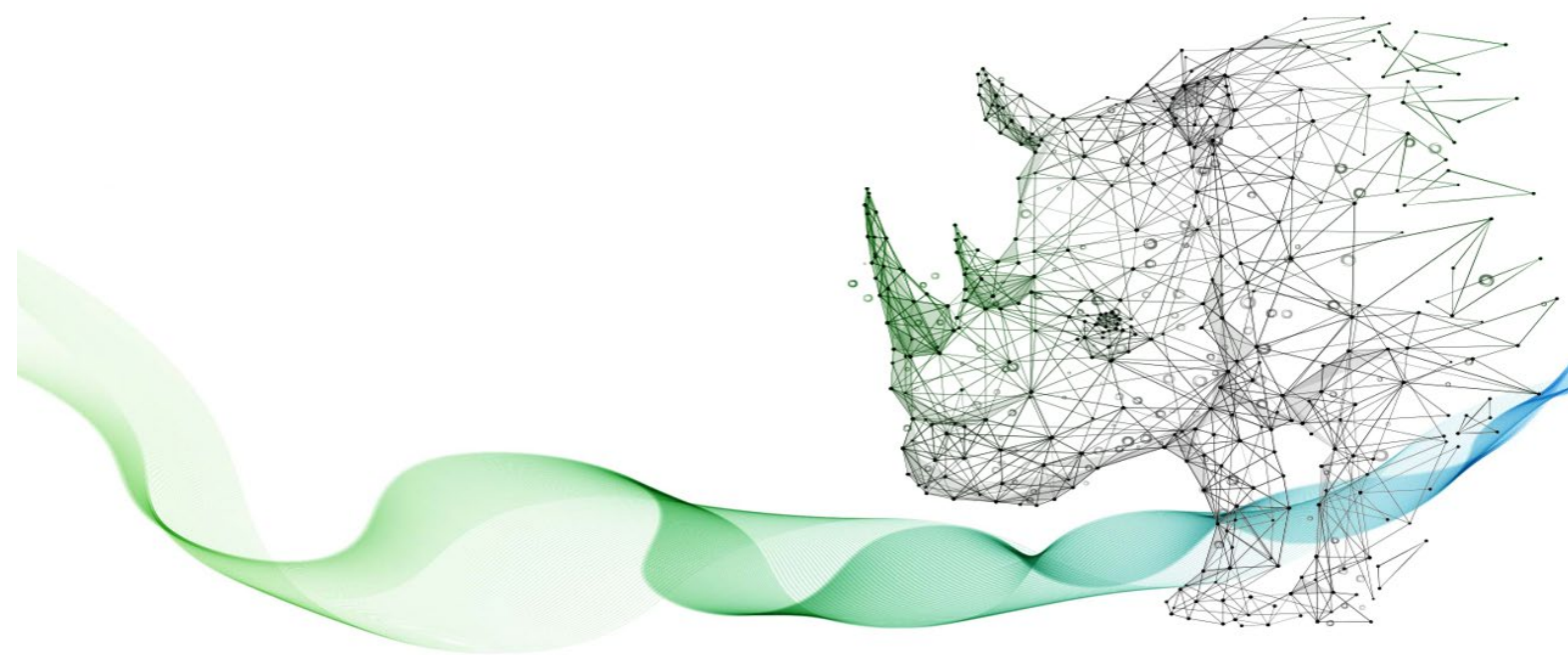


中小企業向け サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策でDXを加速

第2版



東京都産業労働局

第0編 はじめに.....	1
第0章. テキストの活用.....	1
0-1. テキストの目的、想定読者、全体構成、テキストの利用方法など.....	2
0-1-1. テキストの目的、想定読者.....	2
0-1-2. 全体構成.....	2
0-1-3. テキストの利用方法.....	3
第1編 サイバーセキュリティを取り巻く背景【レベル共通】.....	6
第1章. デジタル時代の社会とIT情勢.....	6
1-1. デジタル時代の社会変革とIT情勢の関係性.....	7
第2章. サイバーセキュリティの基礎知識.....	10
2-1. 導入済みと想定するセキュリティ対策機能.....	11
2-2. SECURITY ACTION（セキュリティ対策自己宣言）.....	12
2-2-1. SECURITY ACTION 二つ星レベル.....	12
2-2-2. 情報セキュリティ5か条.....	13
2-2-3. 情報セキュリティ自社診断.....	14
2-2-4. 情報セキュリティ基本方針.....	16
2-3. サイバーセキュリティアプローチ方法.....	18
コラム.....	22
第3章. デジタル社会の方向性と実現に向けた国の方針.....	23
3-1. 国の基本方針および実施計画の要約.....	24
3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題.....	26
3-2-1. デジタル社会の実現に向けた重点計画.....	26
3-2-2. Society5.0.....	30
3-2-3. DXの推進.....	32
第4章. サイバーセキュリティ戦略および関連法令.....	36
4-1. NISC：サイバーセキュリティ戦略.....	37
4-1-1. サイバーセキュリティ戦略.....	37
4-1-2. サイバーセキュリティ2024.....	42
4-2. 企業経営に重要なDX推進とセキュリティ確保の両立.....	45
4-2-1. 企業経営のためのサイバーセキュリティの考え方.....	45
4-2-2. DX with Cybersecurity.....	47
4-3. 関連法令.....	49
4-3-1. 個人情報保護法.....	49
4-3-2. GDPR.....	50
4-3-3. その他関連法令.....	51
編集後記.....	53
第2編 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策【レベル共通】.....	54
第5章. 事例を知る：重大なインシデント発生から課題解決まで.....	54
5-1. 情報セキュリティの概況.....	55
5-1-1. 情報セキュリティの脅威を学ぶ.....	55
5-1-2. IPA：情報セキュリティ白書から見る脅威.....	56
5-1-3. IPA：情報セキュリティ10大脅威.....	58
5-2. 重大インシデント事例から学ぶ課題解決.....	62
5-2-1. インシデント事例から学ぶ.....	62
5-2-2. 最近の攻撃トレンド、および中小企業にも発生しうるサイバー被害事例.....	63

5-2-3. 事案発生->課題の抽出->再発防止策の実施までの流れ	65
5-2-4. インシデントから得た気づきと取組	66
5-2-5. ランサムウェア感染の実態	67
5-3. 実際の被害事例から見るケーススタディー	70
5-3-1. 最近のサイバー被害事例発生の傾向	70
5-3-2. 事例：某港のランサムウェア被害	71
5-3-3. 具体的な対応策	72
第 6 章. 企業経営で重要となる IT 投資と投資としてのサイバーセキュリティ対策	73
6-1. これからの企業経営に必要な観点：社会の動向	74
6-1-1. 現実社会とサイバー空間のつながり	74
6-1-2. IT 活用における課題	77
6-2. 守りの IT 投資と攻めの IT 投資	80
6-2-1. 守りの IT 投資、攻めの IT 投資の概要	80
6-2-2. 経済産業省の DX レポートから見る、「攻めの IT」に取り組む方針について	81
6-2-3. IT を活用した生産性の向上（デジタルオプティマイゼーション）	82
6-2-4. IT を活用した新たなビジネスの展開（DX）	84
6-2-5. 次世代技術を活用したビジネス展開	86
6-3. 経営投資としてのサイバーセキュリティ対策	89
6-3-1. サイバーセキュリティ対策の重要性	89
6-3-2. 経営者が重要視すべき 3 つのポイント	90
編集後記	93
第 3 編 これからの企業経営に必要な IT 活用とサイバーセキュリティ対策 【レベル共通】	94
第 7 章. セキュリティ対策の概要（全容）	94
7-1. 対策基準の策定	95
7-1-1. セキュリティ対策のレベル	95
7-1-2. セキュリティ対策のアプローチ方法	96
第 8 章. 用語定義および関係性と識別方法	102
8-1. 用語の定義、脅威・脆弱性の識別	103
8-1-1. 用語の定義と関係性	103
8-1-2. 脅威の識別	107
8-1-3. 脆弱性の識別	109
コラム	111
編集後記	112
第 4 編 セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施 【レベル 1】	113
第 9 章. 具体的手順の作成（Lv.1 クイックアプローチ）	113
9-1. 【Lv.1 クイックアプローチ】の概要	114
9-2. 【Lv.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順	115
編集後記	120
第 5 編 各種ガイドラインを参考にした対策の実施 【レベル 2】	121
第 10 章. 具体的手順の作成（Lv.2 ベースラインアプローチ）	121
10-1. 【Lv.2 ベースラインアプローチ】の概要	122
10-2. 【Lv.2 ベースラインアプローチ】ガイドラインを参考とした実施手順	123
10-2-1. 情報セキュリティ対策ガイドラインの活用	123
10-2-2. IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の活用	124
10-2-3. NISC「インターネットの安全・安心ハンドブック Ver.5.0」の活用	127
10-2-4. 総務省「テレワークセキュリティガイドライン第 5 版」の活用	128

10-2-5. IPA「中小企業のためのクラウドサービス安全利用の手引き」の活用	130
10-2-6. IPA「情報セキュリティ関連規程」の活用	131
編集後記	134
第 6 編. ISMS などのフレームワークの種類と活用法の紹介 【レベル 3】	135
第 11 章. セキュリティフレームワーク	135
11-1. セキュリティフレームワークの概要	136
11-1-1. セキュリティフレームワークの役割と重要性	136
11-1-2. フレームワーク選択の重要性	137
11-2. 情報セキュリティマネジメントシステム (ISMS) [ISO/IEC27001:2022, 27002:2022]	140
11-3. NIST サイバーセキュリティフレームワーク (CSF)	142
11-3-1. NIST サイバーセキュリティフレームワーク (CSF) の概要	142
11-3-2. NIST SP 800	149
11-3-3. ISMS との関連性	151
11-4. サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF)	152
11-5. サイバーセキュリティ経営ガイドライン	154
11-5-1. サイバーセキュリティ経営ガイドライン	154
11-5-2. サイバーセキュリティ経営ガイドラインの読み方	159
11-5-3. サイバーセキュリティ経営ガイドラインの実践の流れ	161
第 12 章. リスクマネジメント	163
12-1. リスクマネジメント：概要	164
12-1-1. リスクマネジメントプロセス (ISO31000)	164
12-1-2. 情報セキュリティリスクマネジメント (ISO/IEC27005)	165
12-1-3. ISO/IEC 27001 におけるリスクマネジメント手順	167
12-2. リスクマネジメント：リスクアセスメント	168
12-2-1. リスク基準の確立	168
12-2-2. リスクの特定	169
12-2-3. リスクの分析	176
12-2-4. リスクの評価	177
12-3. リスクマネジメント：リスク対応	179
編集後記	182
第 7 編. ISMS の構築と対策基準の策定と実施手順 【レベル 3】	183
第 13 章. ISMS の要求事項と構築 (Lv.3 網羅的アプローチ)	183
13-1. 【Lv.3 網羅的アプローチ】の概要	184
13-2. 【Lv.3 網羅的アプローチ】フレームワークを参考とした実施手順	185
13-2-1. ISMS の概要 (確立・運用・監視)	185
13-2-2. ISMS : 4. 組織の状況	186
13-2-3. ISMS : 5. リーダーシップ	192
13-2-4. ISMS : 6. 計画	196
13-2-5. ISMS : 7. 支援	206
13-2-6. ISMS : 8. 運用	217
13-2-7. ISMS : 9. パフォーマンス評価	221
13-2-8. ISMS : 10. 改善	229
13-3. ISMS 文書体系 (ISMS 構築・導入に必要な文書と記録)	232
13-3-1. ISMS 文書としての策定内容とポイント	232
13-3-2. ISMS の要求事項および管理策	233
13-4. ISO/IEC27001 の審査準備と審査内容	239

13-4-1. ISO/IEC27001 の認証機関の選定と申し込み	239
13-4-2. ISO/IEC27001 の審査事前準備	240
13-4-3. ISO/IEC27001 の審査（第一段・第二段）	241
13-4-4. ISO/IEC27001 の維持審査・再認証審査	243
コラム	244
第 14 章. ISMS の管理策	245
14-1. 管理策の分類と構成	246
14-1-1. 管理策：ISO/IEC 27002	246
14-1-2. 管理策のテーマと属性	247
14-1-3. 対策基準と実施手順の作成方法	250
第 15 章. 組織的対策	251
15-1. 作成する候補となる実施手順書類について	252
15-2. 組織的対策として重要となる実施項目	258
15-2-1. 情報化・サイバーセキュリティ・個人情報保護	258
15-2-2. 脅威インテリジェンス	266
15-2-3. 情報資産台帳作成・維持実施	267
15-2-4. クラウドサービス利用	269
15-2-5. 情報セキュリティインシデント対応	270
15-2-6. 事業継続計画策定	273
15-2-7. 法的、規制および契約上の要件	274
15-2-8. 知的財産、データ、プライバシー	277
15-2-9. セキュリティ対策状況の点検・監査・評価・認証	279
第 16 章. 人的対策	281
16-1. 作成する候補となる実施手順書類について	282
16-2. 人的対策として重要となる実施項目	284
16-2-1. スクリーニング	284
16-2-2. 雇用契約書	284
16-2-3. 懲戒手続き	284
16-2-4. 雇用の終了または変更後の責任	285
16-2-5. 守秘義務または秘密保持契約	285
16-2-6. リモートワーク実施手順	286
16-2-7. 情報セキュリティイベントの報告	287
第 17 章. 物理的対策	288
17-1. 作成する候補となる実施手順書類について	289
17-2. 物理的対策として重要となる実施項目	292
17-2-1. 物理的なセキュリティ境界	292
17-2-2. 入退室認証システム	292
17-2-3. 物理的セキュリティの監視	293
17-2-4. 物理的および環境的脅威からの保護	293
17-2-5. オフプレミスの資産のセキュリティ	295
17-2-6. 機器のメンテナンス	295
17-3. BYOD、MDM	299
17-3-1. BYOD（Bring Your Own Device）導入に向けて	299
17-3-2. MDM（Mobile Device Management）導入のポイント	300
第 18 章. 技術的対策	302
18-1. 作成する候補となる実施手順書類について	303

18-2. 技術的対策として重要となる実施項目	309
18-2-1. エンドポイントデバイス	309
18-2-2. 特権アクセス権	310
18-2-3. アクセス制限	310
18-2-4. 安全な認証	311
18-2-5. キャパシティ管理	311
18-2-6. マルウェアに対する保護	311
18-2-7. 技術的脆弱性の管理	312
18-2-8. 構成管理	312
18-2-9. 情報の削除	313
18-2-10. データ保護	313
18-2-11. バックアップ	314
18-2-12. 冗長化	314
18-2-13. ログイン	315
18-2-14. 監視	315
18-2-15. クロック同期	316
18-2-16. 特権ユーティリティの使用	316
18-2-17. ソフトウェア管理	316
18-2-18. ネットワークセキュリティ	321
18-2-19. ネットワークの分離	322
18-2-20. Web フィルタリング	323
18-2-21. 暗号の使用	323
18-3. 実施手順を適用するセキュリティ概念	325
18-3-1. Security by Design	325
18-3-2. ゼロトラスト、境界防御モデル	329
18-3-3. SASE	336
18-3-4. ネットワーク制御 (Network as a Service)	338
18-3-5. セキュリティ統制 (Security as a Service)	341
18-4. インシデント対応	348
第 19 章. セキュリティ対策状況の有効性評価	352
19-1. 内部監査	353
19-2. 外部監査	354
コラム	356
編集後記	357
第 8 編. 具体的な構築・運用の実践【レベル 3】	358
第 20 章. セキュリティ機能の実装と運用 (IT 環境構築・運用実施手順)	358
20-1. セキュリティ機能の実装と運用	359
20-1-1. デジタル・ガバメント推進標準ガイドラインの概要	359
20-1-2. プロジェクトの管理	366
20-1-3. 予算および執行	373
20-1-4. サービス・業務企画	382
20-1-5. 要件定義	388
20-1-6. 調達	396
20-1-7. 設計・開発	401
20-1-8. サービス・業務の運営と改善	410
20-1-9. 運用および保守	415

20-1-10. システム監査	423
20-2. アジャイル開発	427
20-2-1. アジャイル開発の概要	427
20-2-2. アジャイル開発の実施ポイント	428
第 21 章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施	431
21-1. EC サイトの構築とセキュリティ機能の実装と運用	432
21-1-1. サービス・業務企画	433
21-1-2. 要件定義	437
21-1-3. 調達	485
21-1-4. 設計・開発	491
21-1-5. サービス・業務の運営と改善	493
21-1-6. 運用および保守	498
編集後記	502
第 9 編. 組織として実践するためのスキル・知識と人材育成 【レベル共通】	503
第 22 章. サイバーセキュリティ対策を実践するための知識とスキル	503
22-1. デジタルスキル標準 (DSS)	504
22-1-1. DX リテラシー標準 (DSS-L)	504
22-1-2. DX 推進スキル標準 (DSS-P)	512
22-2. IT スキル標準 (ITSS)	521
22-2-1. 概要	521
22-2-2. キャリア	522
22-2-3. スキル	527
22-3. ITSS+ (プラス)	531
22-3-1. データサイエンス領域	531
22-3-2. アジャイル領域	534
22-3-3. IoT ソリューション領域	535
22-3-4. セキュリティ領域	536
22-4. i コンピテンシ ディクショナリ (iCD)	542
22-4-1. i コンピテンシ ディクショナリ (iCD) の考え方	542
第 23 章. 人材の知識とスキルの認定制度	548
23-1. Di-Lite	549
23-1-1. IT ソフトウェア領域	551
23-1-2. 数理・データサイエンス領域	557
23-1-3. AI・ディープラーニング領域	558
23-2. 情報処理技術者試験	560
23-2-1. 情報セキュリティマネジメント試験	563
23-2-2. 基本情報技術者試験	565
23-2-3. 応用情報技術者試験	565
23-2-4. 各分野スペシャリスト試験	566
23-2-5. 情報処理安全確保支援士試験	569
第 24 章. 各種人材育成カリキュラム	573
24-1. プラス・セキュリティ知識補充講座 カリキュラム例	574
24-1-1. 経営層向けカリキュラム例	576
24-1-2. 部課長級向けカリキュラム例	578
24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3 (レベル 1)】	581
24-3. マナビ DX	586

第 25 章. スキルと知識を持った人材育成・人材確保方法	590
25-1. 「プラス・セキュリティ」の実施計画例	591
25-2. 「リスクリング」「チェンジマインド」の実施計画例	599
25-2-1. 「IT スキル標準」の実施計画例	599
25-2-2. 「デジタルスキル標準」の実施計画例	604
編集後記	621
第 10 編. 全体総括	622
第 26 章. エグゼクティブサマリー	622
26-1. 全体要旨	623
26-2. テキストの活用ポイント	626
第 27 章. 各章のポイント	631
27-1. 第 1 章. デジタル時代の社会と IT 情勢	632
27-2. 第 2 章. サイバーセキュリティの基礎知識	634
27-3. 第 3 章. デジタル社会の方向性と実現に向けた国の方針	637
27-4. 第 4 章. サイバーセキュリティ戦略および関連法令	640
27-5. 第 5 章. 事例を知る：重大なインシデント発生から課題解決まで	643
27-6. 第 6 章. 企業経営で重要となる IT 投資と投資としてのサイバーセキュリティ対策	646
27-7. 第 7 章. セキュリティ対策の概要（全容）	650
27-8. 第 8 章. 用語定義および関係性と識別方法	653
27-9. 第 9 章. 具体的手順の作成（Lv.1 クイックアプローチ）	656
27-10. 第 10 章. 具体的手順の作成（Lv.2 ベースラインアプローチ）	658
27-11. 第 11 章. セキュリティフレームワーク	660
27-12. 第 12 章. リスクマネジメント	663
27-13. 第 13 章. ISMS の要求事項と構築（Lv.3 網羅的アプローチ）	666
27-14. 第 14 章. ISMS の管理策	670
27-15. 第 15 章. 組織的対策	673
27-16. 第 16 章. 人的対策	676
27-17. 第 17 章. 物理的対策	678
27-18. 第 18 章. 技術的対策	681
27-19. 第 19 章. セキュリティ対策状況の有効性評価	685
27-20. 第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）	687
27-21. 第 21 章. 人的、組織的、技術的、物理的対策の実実施手順に基づいた実施	689
27-22. 第 22 章. サイバーセキュリティ対策を実践するための知識とスキル	691
27-23. 第 23 章. 人材の知識とスキルの認定制度	694
27-24. 第 24 章. 各種人材育成カリキュラム	696
27-25. 第 25 章. スキルと知識を持った人材育成・人材確保方法	699
第 28 章. 今後実施すべきこと	701
28-1. 今後のアクション	702
編集後記	712
引用文献	713
参考文献	719
用語集	730
付録：CSF 2.0	749
CSF2.0 の管理策と実装例	750
中小企業向けスタートアップガイドの活用方法	784
付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細	786

経営層向けカリキュラム.....	786
部課長向けカリキュラム.....	789
付録：IT スキル標準レベル1 コマタイトルー覧	796
IT 入門（1）	796
IT 入門（2）	797
パーソナルスキル入門.....	797

第0章. テキストの活用

章の目的

第 0 章では、テキストの目的、想定読者、全体構成、利用方法について理解することを目的とします。

主な達成目標

- テキストの目的、想定読者、全体構成、利用方法を理解すること

0-1. テキストの目的、想定読者、全体構成、テキストの利用方法など

0-1-1. テキストの目的、想定読者

昨今の社会情勢を背景に、日本の中小企業にとってサイバーセキュリティは喫緊の課題となっています。新型コロナウイルスのパンデミックは、リモートワークやオンライン業務の急速な普及をもたらしました。これにより、多くの中小企業がインターネットを介した業務に依存するようになり、[サイバー攻撃](#)のリスクも同時に増加しました。

中小企業は、大企業と比較してセキュリティ対策のリソースが限られていることが多く、サイバー犯罪者にとっては比較的容易な標的となりがちです。フィッシング攻撃や[ランサムウェア](#)攻撃は、これまでにない頻度で中小企業を狙っています。攻撃により業務停止した場合は大きな損失となるため、攻撃者の要求に応じざるを得ない状況に追い込まれることもあります。

また、サイバー攻撃の被害を受けた場合、経済的損失に加えて、企業の信頼やブランド価値にも深刻な影響を与える可能性があります。特に中小企業においては、一度の攻撃で事業継続が困難になることも考えられます。こうした状況を踏まえ、中小企業がセキュリティ対策を講じることは、ビジネスの存続と発展にとって極めて重要です。

本テキストでは、中小企業の経営者や IT 担当者の方々を対象に、包括的なセキュリティ対策に役立つ情報を提供します。

0-1-2. 全体構成

本書の構成は、まず[サイバー攻撃](#)の脅威や実際の被害事例を通じて、リスク認識を深めていただきます。次に、IT およびセキュリティの基礎知識を解説し、セキュリティ対策の要点をまとめています。また、これからの我が国や社会全体の動向についても詳しく解説し、政府や業界団体の取組、最新の技術やトレンドに触れることで、最新の動向への対応力を向上させることを目指しています。さらに、中小企業における IT・セキュリティの課題に焦点を当て、人材不足やビジネス上のリスクに対する具体的な解決策を提示します。また、[ISMS](#) 認証などの代表的な[フレームワーク](#)の習得、組織内でのセキュリティ管理体制の構築や認証取得に向けた手順を解説します。

第 4 編以降ではレベル 1～3 の分類で、セキュリティ対策のレベル感ごとに説明していきます。レベル 1 では、緊急性の高い事例に対処する際の手法を解説します。レベル 2 では、ガイドラインなどを用いて、組織全体として最低限実施すべきセキュリティ対策を解説します。レベル 3 では、セキュリティのフレームワークを用いて、より多くの攻撃や攻撃手法に対して網羅的に対応するための事項を説明します。

最後に、組織としてセキュリティ対策を実施するための知識やスキルおよび、それらを持った人材の育成や確保といった、組織のセキュリティレベル向上を図るにあたって実践的な知識を提供します。

0-1-3. テキストの利用方法

本書は、組織がサイバー攻撃から身を守るための重要なリソースとなりえます。セキュリティ対策の実装、教育、意識向上、最新情報の追跡など、さまざまな方法で利用することができます。

本テキストを通してセキュリティ対策を実践するために、自組織のレベルに応じて、認識すべき事項を把握した上で、参考となる章を選択した活用法が効果的です。以下のアクションに沿って本テキストを活用してください。

1. ポイントの再認識



2. 関係者との共有



3. 社内体制の確立



4. セキュリティ対策の実践

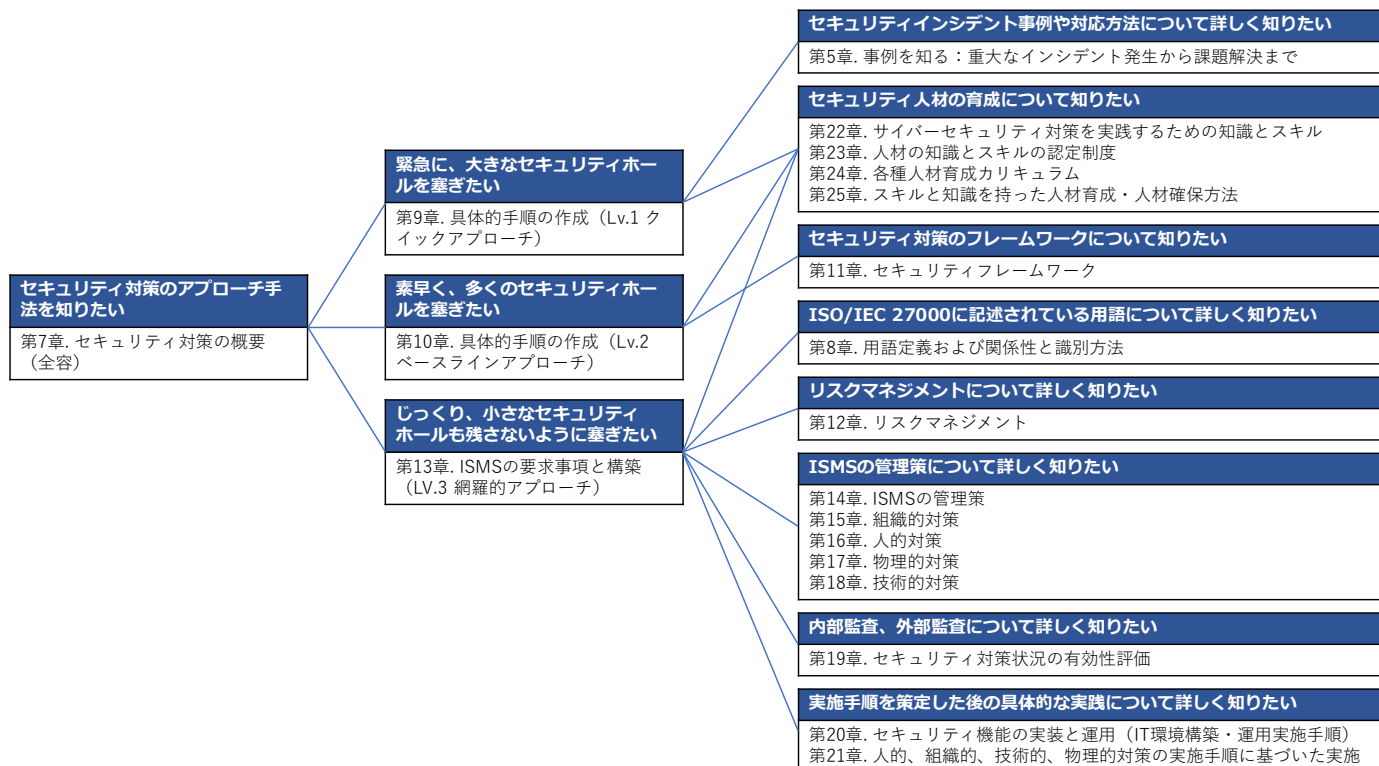
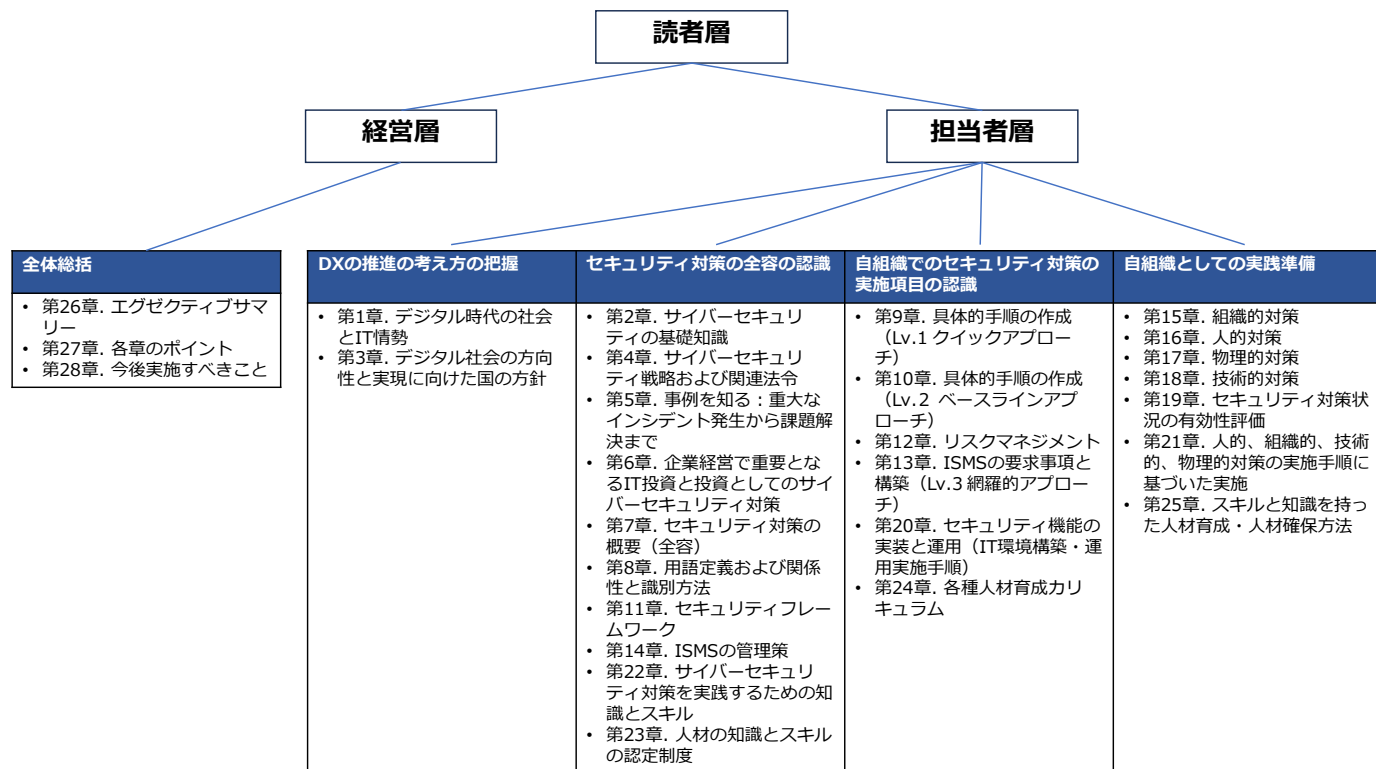
1. ポイントの再認識

「DX の理解からサイバーセキュリティ対策の実践まで」のポイントを再認識します。

各章の内容は以下の通りです。

- DX の推進の考え方の把握
- セキュリティ対策の全容の認識
- 自組織でのセキュリティ対策の実施項目の認識
- 自組織としての実践準備

以下のナビゲーションフローを参照し、自身の役割に応じた内容を確認してください。



2. 関係者との共有

経営者を含めた関係者と、認識したポイントを共有します。「第10編.全体総括」をエグゼクテ

ィブサマリーとして活用してください。重要な点を理解し、経営者および他関係者と共有します。

3. 社内体制の確立

経営者のリーダーシップによって、サイバーセキュリティ対策のための社内体制を確立します。知識やスキルを備えた人材の育成・確保する際は、以下を参照してください。

第9編 組織として実践するためのスキル・知識と人材育成 【レベル共通】
(第22章～第25章)

4. セキュリティ対策の実践

具体的なアクションを起こして、サイバーセキュリティ対策を実践します。情報システムの導入（企画から要件定義、調達、設計・開発、運用保守）の際は、以下の資料などを参考にセキュリティ機能を実装します。

- Security by Design
- 第8編 具体的な構築・運用の実践【レベル3】



図 1. IT 導入プロセスにおけるセキュリティ対策の実施タイミング

第1章. デジタル時代の社会と IT 情勢

章の目的

第 1 章では、現代社会の IT に関する情勢を学ぶことを目的とします。また、日本が Society5.0 の実現を目指す中、企業がビジネスを発展させるために DX を推進していく重要性を明確にすることを目的とします。

主な達成目標

- IT に関する社会の動向を把握し、Society5.0 と DX の関係性を理解すること

1-1. デジタル時代の社会変革と IT 情勢の関係性

社会の現状と今後の動向（Society5.0）

現代社会は、急速な技術革新と経済のグローバル化によって大きな変化を迎えています。この変化の中で、日本では Society5.0 という新たな社会モデルの実現が提唱されています。Society5.0 は、人間とデジタル技術の融合により、持続可能な社会の実現を目指すものです。この概念は、日本が先導する次世代社会のビジョンであり、DX がその実現に向けた重要な手段となることが期待されています。

Society5.0 では、革新的なデジタル技術を活用して、社会の課題を解決し、人々の暮らしを向上させることが求められます。具体的には、AI（人工知能）、ビッグデータ、IoT（Internet of Things）、ロボット工学、クラウドコンピューティングなどのテクノロジーが駆使され、効率的な社会システムや持続可能な産業構造の構築が進められます。

しかしながら、Society5.0 を実現するためには、企業や組織が DX を進め、デジタル化を推進することが不可欠です。DX は、従来のビジネスモデルやプロセスに対する革新的なアプローチであり、さまざまな利点をもたらします。また、大企業と比べ人手や予算などの企業リソースが限定されている中小企業こそ、新たなサービスを創造し、ビジネスを発展させるために、DX を推進することが重要です。

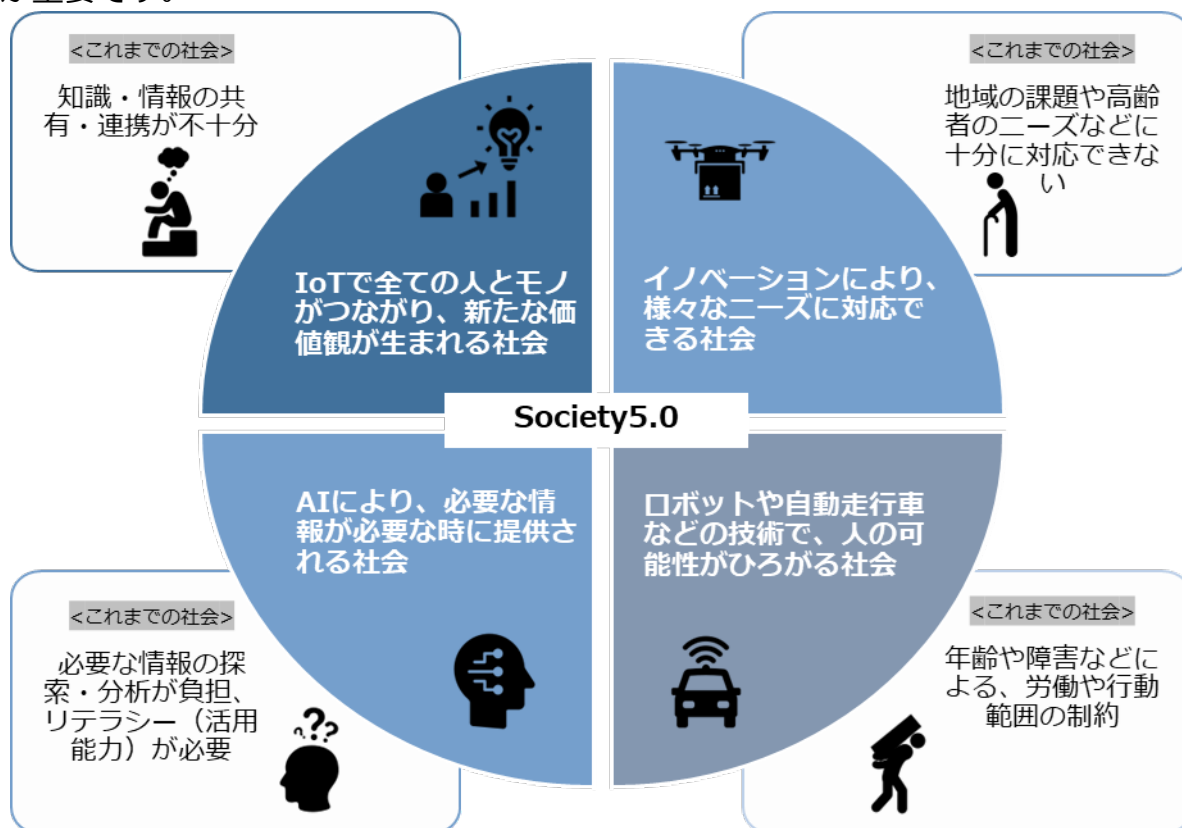


図 2. Society5.0 の概要図

（出典）内閣府、「Society5.0」.https://www8.cao.go.jp/cstp/society5_0

デジタルトランスフォーメーション（DX）とは

ここでは、DX の定義を紹介し、DX の概要を説明します。

DX の定義

DX とは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること¹

DX の概要

DX とは、データやデジタル技術を活用して、顧客視点で新たな価値を創出することです。このためには、ビジネスモデルや企業文化などの変革が必要です。DX を推進するための DX 戦略では、まず経営者が自社の理念や存在意義を明確にし、将来の経営ビジョン（5 年後や 10 年後にどのような企業になりたいか）を具体的に描きます。次に、そのビジョンの実現に向けて関係者を巻き込みながら、現在の状況と目標との差を埋めるために解決すべき課題を整理します。そして、デジタル技術を活用してこれらの課題を解決し、ビジネスモデルや組織、企業文化などを変革することで、経営ビジョンの実現を目指します。

また、DX を推進するにあたり、「知識」「人材」「セキュリティ」の 3 点が重要なキーワードとなります。



DX を進めるにあたり必要な 3 要素

知識

IT の基礎知識のほか、ビッグデータなどを活用するためのデータサイエンスの知識や AI・ブロックチェーンなどの最新技術の知識を取り入れる必要があります。

人材

業務内容に精通し、求められる要件を新たな技術・手法を用いて実装することができるような人材が求められます。

セキュリティ

自宅でのリモートワークやクラウドサービスなどを利用するため必然的にセキュリティの強化が必要となります。

生成 AI とは

令和 4 年 11 月にオープン AI が ChatGPT を公開したことをきっかけに、生成 AI ブームが起きている。ここでは生成 AI とセキュリティの関連について説明します。

¹ 経済産業省, “デジタルガバナンス・コード 2.0”. https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf

生成 AI の概要

生成 AI とは、既存のデータの解析と学習を通じて新たなコンテンツを生成する AI（人工知能）のことです。生成 AI はディープラーニングによって自ら学習したデータをもとに、人が作り出すようなテキスト、画像、音楽、映像などのコンテンツを生み出すことができます。

従来の AI が、大量の学習データをもとに結果を予測し、ある行為を自動的に実行していたのに対して、生成 AI は人間が与えていない情報やデータから新たなコンテンツを生み出すことができる点で大きな違いがあります。

生成 AI の活用

生成 AI はさまざまな業務において実用的に活用できるレベルに進化しています。例えばカスタマーサポートでは生成 AI を用いたチャットボットに 24 時間 365 日対応してもらうことで、顧客の問い合わせに即座に対応できるようになります。広告制作では、バナーやプロモーション用のビジュアルを迅速に、かつ何種類も短時間で生成できます。

このように、生成 AI を活用することによって、多くの業務プロセスを効率化することが可能です。

生成 AI におけるセキュリティの概念

生成 AI は、攻撃者によってフィッシング攻撃の効率を高めるために悪用される可能性があります。生成 AI を使うことで、個々のターゲットに対してパーソナライズされたフィッシングメールを生成することができるため、攻撃の成功率が高まります。また、生成 AI は自然言語処理技術を用いて、より自然で[信頼性](#)の高いメッセージを生成することができるため、受信者が騙されやすくなります。これに対しては、メールの送信元をよく確認する、リンクの URL を不用意にクリックしないなど、従来のフィッシング対策と同様に気をつける必要があります。

また、情報漏えいのリスクもあります。これは、業務上の機密情報や、個人情報を入力してしまうリスクです。生成 AI に送信された情報は、提供元の開発者に見られてしまったり、学習データとして使われたりして、情報漏えいにつながってしまう可能性があります。漏えいしてはいけない情報は、生成 AI には入力しないように気をつけましょう。

第2章. サイバーセキュリティの基礎知識

章の目的

第2章では、サイバーセキュリティの基本的な知識や対策などについて振り返りつつ、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を明確にすることを目的とします。

主な達成目標

- UTM、[EDR](#)の機能を再確認すること
- 企業が自ら実施できる基本的なセキュリティ対策を再確認すること
- リスクと活用可能なリソースを考慮した脅威への対処方法を理解すること

2-1. 導入済みと想定するセキュリティ対策機能

セキュリティ対策は、大企業のみならず中小企業においても重要視されています。特に、ランサムウェアなどのサイバー攻撃のリスクが高まっており、中小企業も十分なセキュリティ対策を講じる必要があります。本テキストの対象読者は、UTM と EDR 相当機能のセキュリティ対策は導入済みであることを想定しています。しかしながら、セキュリティの脅威は常に進化しており、新たな攻撃手法や脆弱性が発見されることがあります。ここでは、UTM、EDR の機能について振り返りますが、さらなるセキュリティ対策についての詳細は本テキストの後半で説明します。

UTM (Unified Threat Management)

UTM は、日本語で「統合脅威管理」と訳されます。UTM は複数のセキュリティ機能を 1 つの機器に集約したもので、ネットワーク全体のトラフィックを監視・管理します。UTM には、ファイアウォール、侵入検知システム、ウイルス対策などが統合されており、内部ネットワークに対する外部からの侵入や攻撃を防御します。そのため、企業・組織内のネットワークセキュリティ対策として UTM の導入は有効な手段です。

EDR (Endpoint Detection and Response)

EDR は、エンドポイント（PC、スマホ、サーバなど）における脅威の検知および対応を可能にします。従来のアンチウイルスソフトウェアでは、ウイルス定義ファイルにないマルウェアは検知できませんでしたが、EDR では、エンドポイント上の不審な動作を検知することができます。また、検知した脅威に対して、悪意のあるプロセスの終了、感染したエンドポイントの隔離などの適切な対応を行います。そのため、EDR を活用することで、セキュリティインシデントの早期発見と迅速な対応が可能になり、エンドポイントの保護が強化されます。

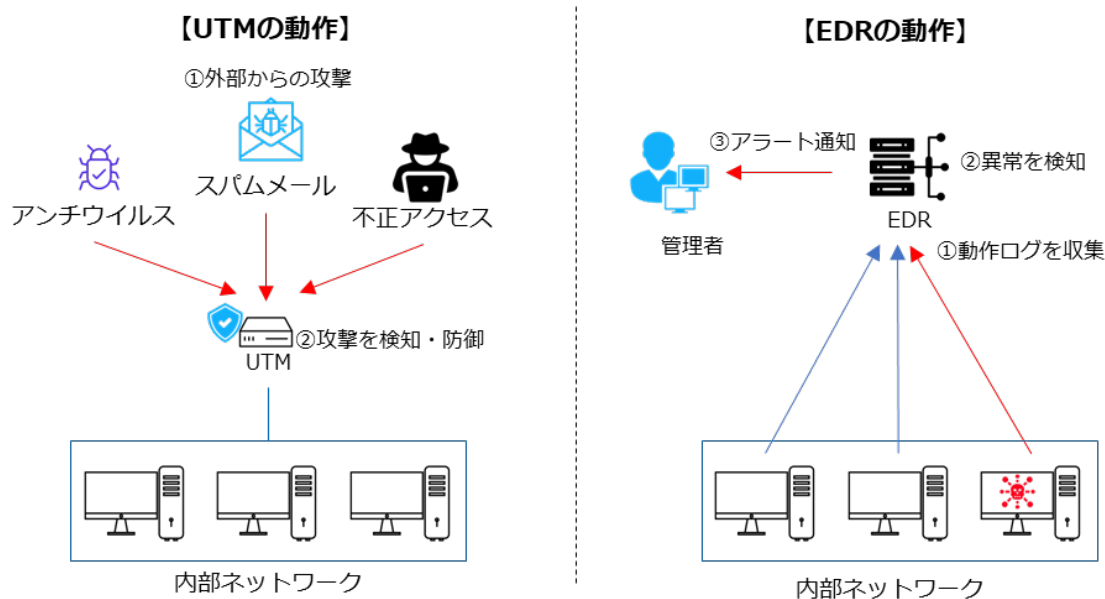


図 3. UTM、EDR の概要図

2-2. SECURITY ACTION（セキュリティ対策自己宣言）

2-2-1. SECURITY ACTION 二つ星レベル

「[SECURITY ACTION](#)」は中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度です。安全・安心な IT 社会を実現するために、独立行政法人情報処理推進機構（IPA）によって創設されました。

宣言企業数（令和 6 年 5 月 31 日時点）：一つ星：302,264 社：二つ星：32,630 社²

★一つ星	「情報セキュリティ 5 か条」に取り組むことを宣言
★★二つ星	「5 分でできる！情報セキュリティ自社診断」で自社の情報を把握 ②情報セキュリティ方針を策定 ③外部に公開したことを宣言

1.使用規約を確認	「ロゴマーク使用規約確認」にて規約を確認します。
2.必要事項を入力	「事業者情報入力」、「自己宣言入力」それぞれの画面で必要事項を入力します。
3.確認メールを受信	「自己宣言受付確認のお知らせ」メールを受信します。 メール本文中の URL を押します。
4.自己宣言 ID のお知らせ	「自己宣言完了のお知らせ」メールにて、ログインに利用する自己宣言 ID をお知らせします。
5.ロゴマークダウンロード	自己宣言完了後、1～2 週間程度でロゴマークのダウンロードに必要な手順をメールでお知らせします。

One Point

取得時における注意点

「SECURITY ACTION」はセキュリティ対策状況などを IPA が認定するものではありません。
「SECURITY ACTION」の取組に関して Web サイトなどにおいて次のような不適切な表現を使用されますと、第三者の誤解を生ずる可能性が懸念されますので、ご注意願います。

- × 「一つ星（二つ星）の認定を受けました」「一つ星（二つ星）を取得しました」
- 「一つ星（二つ星）を宣言しました」

IPA.「SECURITY ACTION セキュリティ対策自己宣言」.<https://www.ipa.go.jp/security/security-action>

詳細理解のため参考となる文献（参考文献）	
SECURITY ACTION セキュリティ対策自己宣言	https://www.ipa.go.jp/security/security-action/

² 経済産業省. “デジタルガバナンス・コード 2.0”. https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf

2-2-2. 情報セキュリティ 5 か条

「情報セキュリティ 5 か条」は、企業の規模に関係なく、重要なセキュリティ対策をまとめたものです。初めてセキュリティ対策に取り組む場合でも、実施しやすい内容となっています。情報セキュリティ 5 か条は、共通する基本的なセキュリティ対策をまとめたものであり、必ず実行することが重要です。

1.OS やソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題が解決されず、悪意のあるウイルスに感染してしまう危険性があるため、最新の状態にします。

対	● パソコンやルータのソフトウェアやファームウェアを最新化します。
策：	● OS やソフトウェアアップデートを実行します。

2.ウイルス対策ソフトを導入しよう！

ID・パスワードを盗まれないようにウイルス対策ソフトを導入し、[ウイルス定義ファイル（パターンファイル）](#) は常に最新の状態になるようにします。

対	● ウイルス定義ファイルが自動更新されるように設定します。
策：	● 統合型のセキュリティ対策ソフトを導入します。

3.パスワードを強化しよう！

パスワードが推測や解析されたり、流出した ID・パスワードが悪用されたりすることで、不正にログインされます。パスワードは長く、複雑に、使い回さないようにします。

対	● 同じ ID、パスワードを複数サービス間で使い回さないようにします。例として、10
策：	文字以上で「大文字」「小文字」「数字」「記号」を含めます。また、「名前」「電話番号」「誕生日」「簡単な英単語」等は使わず、推測できないようにします。

4.共有設定を見直そう！

データ保管等の Web サービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、Web サービスや機器を使うことができるような設定になっていないことを確認します。

対	● Web サービス、ネットワーク接続の複合機・カメラ等の共有範囲を限定します。
策：	● 従業員の異動や退職時には速やかに設定を変更（削除）します。

5.脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送る巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとります。

対	● IPA 等のセキュリティ専門機関の Web サイトやメールマガジンで最新の脅威や攻撃
策：	の手口を知ります。
	● インターネットバンキング やクラウドサービス等が提供する注意喚起を確認します。

(出典) IPA「情報セキュリティ 5 か条」をもとに作成

2-2-3. 情報セキュリティ自社診断

「5分でできる！情報セキュリティ自社診断」を利用することで、自社のセキュリティ対策が、どれくらい実施できているかを把握できます。自社診断は、次ページに示す25項目の設問に答えるだけでセキュリティ対策の実施状況が把握できます。

分類

Part1 基本的対策

No.1~5は企業の規模や形態を問わず、必須の5項目です。いずれも一度行えば良いものではなく、継続的な実施が欠かせないため、運用ルールとして社内に定着させる必要があります。

Part2 従業員としての対策

No.6~18は従業員として注目すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威が日々変化しているので、油断しないように注意する必要があります。

Part3 組織としての対策

No.19~25は組織としての方針を定めた上で、実施すべきセキュリティ対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにします。

診断方法

経営者または情報システム担当や部門長など実施状況を把握している人が記入します。事業所が複数、部署が多いなど一人で記入することが難しい場合は、事業所、部署ごとに記入し、責任者・担当者が集計します。

設問ごとに、以下の点数をつけ、全項目の合計点で組織全体のセキュリティ対策実施状況を確認します。回答が「わからない」となっている項目を確認します。

項目	点数
実施している	4点
一部実施している	2点
実施していない	0点
わからない	-1点



合計得点	現在の状況	次の対策
100 点満点	入門レベルのセキュリティ対策は達成	さらに強化
70~99 点	部分的な対策が不十分	100 点満点への挑戦
50~69 点	対策が不十分	低い項目から改善
49 点以下	事故がいつ起きても不思議ではない	早急に改善

(出典) IPA「5 分でできる！情報セキュリティ自社診断」をもとに作成

詳細理解のため参考となる文献（参考文献）	
5 分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

「5 分でできる！情報セキュリティ自社診断」

No	診断内容
基本的対策	1 パソコンやスマホ等情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2 パソコンやスマホ等にはウイルス対策ソフトを導入し、 ウイルス定義ファイル は最新の状態にしていますか？
	3 パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4 重要情報に対する適切なアクセス制限を行っていますか？
	5 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7 電子メールや FAX の宛先の送信ミスを防ぐ取組みを実施していますか？
	8 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワード等で保護していますか？
	9 無線 LAN を安全に使うために適切な 暗号化 方式を設定する等の対策をしていますか？
	10 インターネットを介したウイルス感染や SNS への書き込み等によるトラブルへの対策をしていますか？
	11 パソコンやサーバのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？

	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫等に安全に保管していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管する等盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
組織としての 対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさない等のルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスや Web サイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成する等準備をしていますか？
	25	情報セキュリティ対策（上記 1～24 等）をルール化し、従業員に明示していますか？

(出典) IPA「5分でできる！情報セキュリティ自社診断」をもとに作成

2-2-4. 情報セキュリティ基本方針

経営者が策定した情報セキュリティに関する基本方針を、従業員や関係者に伝達するために、簡潔な文書を作成する必要があります。基本方針の作成には、特定の書き方が定められているわけではありません。そのため、事業の特徴や顧客の期待などを考慮し、経営者と連携しながら、自社に適した基本方針を策定します。

基本方針は従業員の指針となり、関係者に対して取組を明示するためのものです。そのため、作成した文書は従業員や顧客などの関係者に周知する必要があります。

情報セキュリティ基本方針（サンプル）

株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした/当社の情報資産を事故・災害・犯罪等の脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組めます。

1.経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備

当社は、情報セキュリティの維持および改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取組みを確かなものにします。

4.法令および契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5.違反および事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反および事故が発生した場合には適切に対処し、再発防止に努めます。

制定日：20〇〇年〇月〇日

株式会社〇〇〇〇

代表取締役社長 〇〇〇〇

（出典）IPA「情報セキュリティ基本方針（サンプル）」をもとに作成

情報セキュリティ基本方針の記載項目例

セキュリティ管理体制の整備 / 法令・ガイドラインなどの遵守 / セキュリティ対策の実施 / 継続的改善など

2-3. サイバーセキュリティアプローチ方法

サイバーセキュリティの脅威に対処するためには、効果的な[サイバーセキュリティ戦略](#)を構築し、段階的なアプローチをとることが必要です。(Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ)

自社が直面しているリスク状況および活用できるリソースを考慮し、最適なアプローチ手法を選択します。以下にアプローチ手法を紹介します。

緊急に、大きな セキュリティホール を塞ぐ	Lv.1 クイックアプローチ
	実施手法 報道されるような事象・セキュリティ脅威に緊急対応します。 活用できる文書/ツール名称 (例) ● 情報セキュリティ10 大脅威 (出典：IPA) ● 情報セキュリティ白書 2023 (出典：IPA) ● サイバー攻撃を受けた組織における対応事例 (出典：NISC)
素早く、多くのセキュリティホールを塞ぐ	Lv.2 ベースラインアプローチ
	実施手法 ガイドブック、ひな型を参照し、迅速にセキュリティ対応します。 活用できる文書/ツール名称 (例) ● リスク分析シート (出典：IPA) ● セキュリティ関連費用の可視化 (出典：IPA) ● 中小企業の情報セキュリティ対策ガイドライン第3版 (出典：IPA)
じっくり、小さなセキュリティホールも残さないように塞ぐ	Lv.3 網羅的アプローチ
	実施手法 網羅的なセキュリティ対策が定義されている フレームワーク に沿ってセキュリティ対応します 活用できる文書/ツール名称 (例) ● ISMS (ISO/IEC27001:2022,27002:2022)

	● NIST サイバーセキュリティフレームワーク (CSF) ● サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF)

凡例)「○ : あり / △ : 部分的にあり / × : なし」

Lv.1 クイックアプローチ		網羅性	即時性
Lv.1 クイックアプローチは、サイバーセキュリティにおける即時の対応や緊急事態への対処に適しています。ただし、長期的な戦略や継続的な改善を妨げることなく、将来的なセキュリティの向上を見据えた計画の策定も必要となります。 ● 小規模な対策や修正を迅速に実施可能 ● 低コストでリスクを軽減 ● 進行中の攻撃へ対応することにより、攻撃の拡大や影響を最小限に抑える		×	○
1. 脅威の特定	既知の脅威/過去のインシデントに基づいて、リスクの優先度付けを行いリスクを特定します。		
2. 対応計画	既存のセキュリティ対策の評価を行い、改善点を特定し対応計画を立てます。		
3. 対策の実装	必要な設定変更やアップデートの適用、ポリシーや手順の策定、従業員への教育やトレーニング等の対策を実装します。		
4. 評価・改善	実装した対策の評価を行い、継続的な改善を促進します。		

Lv.2 ベースラインアプローチ		網羅性	即時性
Lv.2 ベースラインアプローチは、セキュリティ対策の基準やガイドラインを定義することにより、組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指します。ただし、追加のセキュリティ対策やリスクに対する適切な対応策を検討し、網羅的なアプローチを推進することが必要となります。 ● セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保		△	△

● 網羅的なアプローチの出発点			
1. ベースラインの定義	セキュリティの基準となるベースラインを定義します。活用できる文書/ツール、内部のセキュリティ目標等に基づいて定義します。		
2. 現状評価	<u>セキュリティポリシー</u> やガイドラインの遵守度に基づき、既存のセキュリティ対策の評価を行います。改善点を特定し対応計画を立てます。		
3. ベースラインの適用	セキュリティポリシーの策定・改訂、ガイドラインの作成、セキュリティ対策の実装等により、ベースラインを適用します。		
4. 教育	定期的な教育活動を通じて、従業員にセキュリティポリシーやガイドラインの重要性を啓発し、遵守を促進します。		
5. 評価・改善	実装した対策の評価を行い、継続的な改善を促進します。		

One Point

即時性を求める場合には、Lv.2 ベースラインアプローチに加えて、Lv.1 クイックアプローチや緊急対応策等を組み合わせることで、より即時の対策を講じることができます。ただし、Lv.2 ベースラインアプローチは継続的な改善を重視するものであり、セキュリティの長期的な維持と向上に焦点を当てています。

凡例)「○：あり / △：部分的にあり / ×：なし」

Lv.3 網羅的アプローチ		網羅性	即時性
Lv.3 網羅的アプローチは、可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなります。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではありません。 ・可能な限り多くの脅威や攻撃手法に対して対策を講じる ・予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持		○	×
1. <u>リスクアセスメント</u>	<u>情報資産</u> を特定し、脅威や <u>脆弱性</u> の評価を実施します。また、リスクの特定と評価を行い、重要度や優先順位を設定します。		
2. 対応計画	<u>リスク評価</u> の結果を基に、セキュリティ対策を設計します。		
3. 対策の実装	組織的な対策（ポリシー、手順整備、教育等）、技術的な対策（ <u>アクセス制御</u> 、 <u>暗号化</u> 等）を実装します。		

4. 教育	定期的な教育活動を通じて、従業員にセキュリティポリシーやガイドラインの重要性を啓発し、遵守を促進します。
5. 評価・改善	実装した対策の評価を行い、継続的な改善を促進します。また、 内部監査 や定期的な監査を実施し、情報セキュリティ管理システム適合性および妥当性を確認します。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ白書 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
リスク分析シート	https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx
セキュリティ関連費用の可視化	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html
中小企業の情報セキュリティ対策ガイドライン第 3.1 版	https://www.ipa.go.jp/security/guide/sme/about.html
ISMS 適合性評価制度	https://isms.jp/isms.html
セキュリティ関連 NIST 文書について	https://www.ipa.go.jp/security/reports/oversea/nist/about.html
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html
セキュリティ関連知識の保管庫（ナレッジベース 2024）	https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/

“情報セキュリティ”と“サイバーセキュリティ”の違いについて

本テキストでは、“情報セキュリティ”と“サイバーセキュリティ”という言葉が随所に出てきます。そこで、両者の違いを説明します。

情報セキュリティは、情報全般の保護を意味します。情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を確保するための対策が目的となります（情報セキュリティの3要素「CIA」）。これには、物理的な文書やデータの保管方法、アクセス制御、暗号化などが含まれます。情報セキュリティは、デジタルに加えて、紙の文書などの非デジタル情報にも関連しています。また、3要素に加えて、真正性（Authenticity）、責任追跡性（説明責任）（Accountability）、否認防止性（Non-Repudation）、信頼性（Reliability）を合わせて情報セキュリティの7要素と呼ぶこともあります。

一方、サイバーセキュリティは、主にインターネットやコンピュータネットワークに関連するリスクに対処することを目的とします。サイバーセキュリティは、クラッキング、マルウェア、DDoS 攻撃などの脅威から情報システムやネットワークを保護するための技術、ポリシー、手順を包括的に扱います。サイバーセキュリティは、コンピュータシステムやネットワーク上の脆弱性に対処するためのテクニカルなアプローチに重点を置いています。

要約しますと、情報セキュリティは広範な情報の保護を対象とし、物理的な文書やデジタルデータを含む一般的なセキュリティの概念を指します。一方、サイバーセキュリティは、インターネットやネットワーク上のリスクに対処するためのテクニカルなアプローチを特に重視しています。

第3章. デジタル社会の方向性と実現に向けた国の方針

章の目的

第3章では、政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶことを目的とします。

主な達成目標

- 国の基本方針にデジタルがどのように影響を与えており、それによりどのような社会を目指しているかを理解すること
- デジタル社会におけるセキュリティ対策の重要性を理解すること

3-1. 国の基本方針および実施計画の要約

国の方針の1つである「経済財政運営と改革の基本方針」は、政府の経済財政政策に関する基本的な方針を示すとともに、経済、財政、行政、社会などの分野における改革の重要性とその方向性を示すものです。この方針は通称「骨太の方針」と言われています。

各省庁の利害を超えて官邸主導で改革を進めるため、内閣総理大臣が議長を務める経済財政諮問会議において毎年策定します。

IT およびセキュリティ関連の施策についてもこの基本方針に沿った形で実施計画が策定されています。

ここでは、令和6年に策定された基本方針の中から、特にIT戦略に関する内容について説明します。

5つのAction

- ①物価上昇を上回る賃上げの定着
- ②構造的価格転嫁の実現
- ③成長分野への戦略的な投資
- ④スタートアップネットワークの形成
- ⑤新技術の徹底した社会実装

5つのVision

- ①社会課題解決をエンジンとした生産性向上と成長機会の拡大
- ②誰もが活躍できる Well-being が高い社会の実現
- ③経済・財政・社会保障の持続可能性の確保
- ④地域ごとの特性・成長資源を活かした持続可能な地域社会の形成
- ⑤海外の成長市場との連結性向上とエネルギー構造転換

IT 戦略に関する施策例

デジタル技術の活用

AI やロボットなどの自動化技術を導入することで、中堅・中小企業の生産性向上と業務効率化を目指しています。特に、人手不足が深刻な業種においては、これらの技術の利用拡大が推奨されています。また、デジタルトランスフォーメーション（DX）を推進することで、新たな市場の開拓や企業間のデータ共有と連携を促進するための基盤整備が進められています。このため、企業情報や支援ニーズを集約したマッチングプラットフォームの運用が2024年度中に開始される予定です。

デジタル・ガバメントの強化

行政サービスのデジタル化も重要な施策の一つです。公的基礎情報のデータベース化や事業者向け共通認証システムの普及により、ワンストップでの行政手続を可能にし、国民の利便性を大幅に向上させることが計画されています。これにより、行政運営の効率化も図られ、地方公共団体や民間企業との連携が強化されることが期待されます。特に、地方公共団体の基幹業務システムの統一・標準化、公共部門のシステムの共通化とモダン化を推進することとされています。

サイバーセキュリティの強化

「サイバーセキュリティ戦略」に基づき、官民連携によるサイバーセキュリティ演習や実践的な侵入テストを実施することで、重要インフラのセキュリティ対策の強化が目指されています。また、フィッシング対策の強化や、IoT 機器のセキュリティ要件の評価制度の導入も進められています。これにより、デジタル社会の安全性が確保され、安心してデジタル技術を利用できる環境が整えられます。さらに、経済安全保障の観点からもセキュリティ対策が強化されています。国際連携を通じて、重要物資の安定供給を確保し、先端技術の流出防止策が講じられます。これにより、日本の産業競争力と経済安全保障が強化され、持続可能な経済成長が目指されています。

(出典) 内閣府「経済財政運営と改革の基本方針 2024」をもとに作成

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

3-2-1. デジタル社会の実現に向けた重点計画

政府は経済財政運営と改革の基本方針で掲げているデジタル社会の実現を目指すにあたって、「デジタル社会の実現に向けた重点計画」を閣議決定しています。

日本が目指すデジタル社会について、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」と定義し、以下の6つの姿を挙げています。³

デジタル社会で目指す6つの姿

1. デジタル化による成長戦略

国・地方公共団体や民間との連携の在り方を含めたアーキテクチャの設計やクラウドサービスの徹底活用、デジタル原則を含む規制改革の徹底、調達改革の推進、データ戦略の推進、データ連携やDXの推進、[AI](#)の適切かつ効果的な活用などにより、我が国全体のデジタル競争力が底上げされ、成長していく持続可能な社会を目指す。

2. 医療・教育・防災・こどもなどの準公共分野のデジタル化

必要なデータの連携などを通じて、国民一人ひとりのニーズやライフスタイルに合ったサービスが提供される豊かな社会、継続的に力強く成長する社会を目指す。

3. デジタル化による地域の活性化

地方の共通基盤を国が支援することなどにより、地域からデジタル改革、デジタル実装を推進、デジタル田園都市国家構想の実現、地域で魅力ある多様な就業機会の創出などを図り、地域の課題が解決され、各地域で培われてきた地域の魅力が向上する社会を目指す。

4. 誰一人取り残されないデジタル社会

地理的な制約、年齢、性別、障害や疾病の有無、国籍、経済的な状況などにかかわらず、誰もが（デジタルに不慣れな方にも・デジタルを利用する方にも）日常的にデジタル化の恩恵を享受でき、さまざまな課題を解決し、豊かさを真に実感できる「誰一人取り残されない」デジタル社会を目指す。

5. デジタル人材の育成・確保

全国民が当事者であるとの認識に立ち、ライフステージに応じた必要な[ICT](#)スキルを継続的に学ぶことで、デジタル人材の底上げと専門性の向上を図り、デジタル人材が育成・確保される社会を目指す。

6. [DFFT](#) (Data Free Flow with Trust) : 「[信頼性](#)のある自由なデータ流通」の推進を始めとする国際戦略

³ デジタル庁「デジタル社会の実現に向けた重点計画」https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/Secac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

国際連携を図ることで、データがもたらす価値を最大限引き出し、国境を越えた自由なデータ流通が可能な社会を目指す。

(出典) デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

デジタル社会の実現に向けた戦略・施策

日本がデジタル社会を実現していくための政府の取組について、7つの戦略的な政策が掲げられています。7つの戦略的な政策の中では、サイバーセキュリティに関する取組も盛り込まれています。サイバーセキュリティの施策が重要視されていることを理解するため、該当の項目について説明していきます。

目指す姿を実現する上で有効な戦略的取組（基本戦略）

1. デジタル社会の実現に向けた構造改革
2. デジタル田園都市国家構想の実現
3. 国際戦略の推進
4. サイバーセキュリティなどの安全・安心の確保
5. 急速な AI の進歩・普及を踏まえた対応
6. 包括的データ戦略の推進と今後の取組
7. Web3.0 の推進

サイバーセキュリティなどの安全・安心の確保

国家安全保障上の課題へと発展していく可能性のある国際情勢の変化、感染症の蔓延、自然災害などへの対応として、国民の生命・財産を守り、国民生活を維持することのできる安全・安心なデジタル社会の構築に取り組みます。

1. サイバーセキュリティの確保

- 令和5年度に、政府情報システムにおけるクラウドサービスの利用拡大などを見据え、政府統一基準を改定。
- デジタル庁は [NISC](#) と連携し、デジタル庁整備・運用システムなどの情報システム整備方針の実装を推進。
- 安全保障などの機微な情報などに係る政府情報システムの取扱いを参照した利用促進。

2. 個人情報などの適正な取扱いの確保

- 改正後の個人情報保護法を踏まえ、個人情報などの適正な取扱いの確保、[個人情報保護委員会](#)の体制強化。

3. 情報通信技術を用いた犯罪の防止

- [不正アクセス](#)の防止などに向けた官民連携。
- 国際連携、サイバー事案の警察への通報促進などの取組を実施。

4.高度情報通信ネットワークの災害対策

- ネットワークの冗長性の確保・電気通信事故の検証、災害発生時における移動電源車などの派遣などを推進。

各分野における基本的な施策

デジタル社会の実現に向け、6つの分野に分けて、基本的な施策が掲げられています。6つの分野における産業のデジタル化には、中小企業を対象とした施策が盛り込まれているため、その分野に焦点を当てて説明していきます。

各分野における基本的な施策

- 1.国民に対する行政サービスのデジタル化
- 2.安全・安心で便利な暮らしのデジタル化
- 3.アクセシビリティの確保
- 4.産業のデジタル化**
- 5.デジタル社会を支えるシステム・技術
- 6.デジタル社会のライフスタイル・人材

産業のデジタル化

行政サービスのデジタル化を通じて事業者にとって利用しやすい環境を整備し、支援を必要とする事業者に迅速に支援が届く環境の実現を目指します。

1.デジタルによる新たな産業の創出・育成

クラウドサービス産業の育成 / IT スタートアップなどの育成

2.事業者向け行政サービスの質の向上に向けた取組

- 電子署名、電子委任状、商業登記電子証明書の普及
- 法人共通認証基盤（[G ビズ ID](#)）の普及
- **事業者に対するオンライン行政サービスの充実**
- レベルに応じた認証の推進
- eKYC（electronic Know Your Customer）などを用いた民間取引などにおける本人確認手法の普及促進

3.中小企業のデジタル化の支援

- **中小企業の事業環境デジタル化サポート**
- **中小企業のサイバーセキュリティ対策の支援**

4.産業全体のデジタルトランスフォーメーション

- 市場評価を通じた DX の推進、産業におけるサイバーセキュリティの強化、データの利活用や規制改革などを通じた産業の DX

(出典) デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

以下では、前述の産業のデジタル化のうち、中小企業を対象とした施策が盛り込まれている「事業者向け行政サービスの質の向上に向けた取組」と「中小企業のデジタル化の支援」について説明します。

事業者向け行政サービスの質の向上に向けた取組

電子署名、電子委任状、商業登記電子証明書の普及

電子署名、電子委任状、商業登記電子証明書について、事業者による活用の機会が増加し、多様化していることから、普及を更に強力に推進する。

法人共通認証基盤（G ビズ ID）の普及

法人が様々なサービスにログインできる認証サービスを実現する「G ビズ ID」について、2023 年度中にマイナンバーカードを利用した審査の効率化、連携行政サービスの拡充などを進める。

事業者に対するオンライン行政サービスの充実

ア：e-Gov の利用促進

安定運用を確保しつつ、クラウドサービス利用による柔軟なリソース活用に向けて、ガバメントクラウドへの移行の整備を 2023 年度中に行うことを目指す。

イ：J グランツの利便性向上と利用補助金の拡大

申請簡素化や事務局の審査プロセス迅速化の観点から、2024 年度（令和 6 年度）を目途に、システムアーキテクチャ及び UI の刷新を行い、申請時の事業者・事務局双方の負担軽減を図る。

ウ：中小企業支援の DX 推進

事業者の申請などデータを一元化し官民で利活用するためのデータ基盤（[ミラサポコネクト](#)）を通じて、自社の経営特性に合った多様な支援がリコmendされる環境を実現する。

最適な支援策や支援者・民間サービスなどについて情報交換できるコミュニティサイトの構築を目指す。

レベルに応じた認証の推進

ア：民間事業者への周知・相談支援の強化

マイナンバーカードの普及などに伴い、利用のインセンティブが大きく高まる民間事業者への周知・相談支援を強化する。

イ：利用要件・利用手続などの改善

民間事業者の視点に立ち、利用要件・利用手続などの継続的な改善を実施する。

eKYC などを用いた民間取引などにおける本人確認手法の普及促進

デジタル空間での安全・安心な民間の取引などにおいて必要となる本人確認について、公的個人認証サービス（JPKI）の利用を促進する。その上で、安全性や信頼性などに配慮しつつ、具体的な課題と方向性を整理し、簡便な手法の一つである eKYC などを用いた本人確認手法の普及を進める。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

中小企業のデジタル化の支援

中小企業の事業環境デジタル化サポート

- デジタル化支援ポータルサイト「みらデジ」の設置
- IT 専門家との相談を受けられる体制の整備
- IT 導入補助金
- 取引全体のデジタル化
- 会計・経理全体のデジタル化
- クラウドサービス利用やハードウェア調達の支援
- 業務効率化や DX に向けた IT ツール導入の支援

中小企業のサイバーセキュリティ対策の支援

- 「サイバーセキュリティお助け隊サービス」の普及促進
- 相談体制の強化
- 情報集約・共有促進機能の強化

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

3-2-2. Society5.0

Society5.0 は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）です。狩猟社会（Society1.0）、農耕社会（Society2.0）、工業社会（Society3.0）、情報社会（Society4.0）に続く、新たな社会を指すもので、第5期科学技術基本計画において我が国が目指すべき未来社会の姿として初めて提唱されました。

Society5.0 では、IoT（Internet of Things）ですべての人とモノがつながり、さまざまな知識や情報を共有することによって、これまでにない新たな価値を生み出すとともに、社会が抱える課題を解決し、困難を克服できます。また、人工知能（AI）、ロボット、自動走行車などの利用によって、少子高齢化、地方の過疎化、貧富の格差などの課題も解決できるでしょう。こうした社会の

変革（イノベーション）が進むことによって、希望の持てる社会、世代を超えて互いに尊重し合う社会、一人一人が快適で活躍できる社会が生まれることが期待されます。

これまでの情報社会（Society4.0）では、人がサイバー空間にあるクラウドサービスにアクセスすることで、情報やデータを入手し、分析を行ってきました。Society5.0 では、フィジカル空間のセンサーから膨大な情報がサイバー空間に集積されます。サイバー空間では、この集積されたデータ（ビッグデータ）を人工知能（AI）が解析し、その結果をフィジカル空間の人間にさまざまな形で、フィードバックしていきます。今までの情報社会では、人間が情報を解析することで、価値が生まれましたが、Society5.0 では、AI が解析した膨大なビッグデータの結果がロボットなどを通して、人間にフィードバックされることで、これまでに実現しなかった新たな価値が産業や社会にもたらされます。⁴

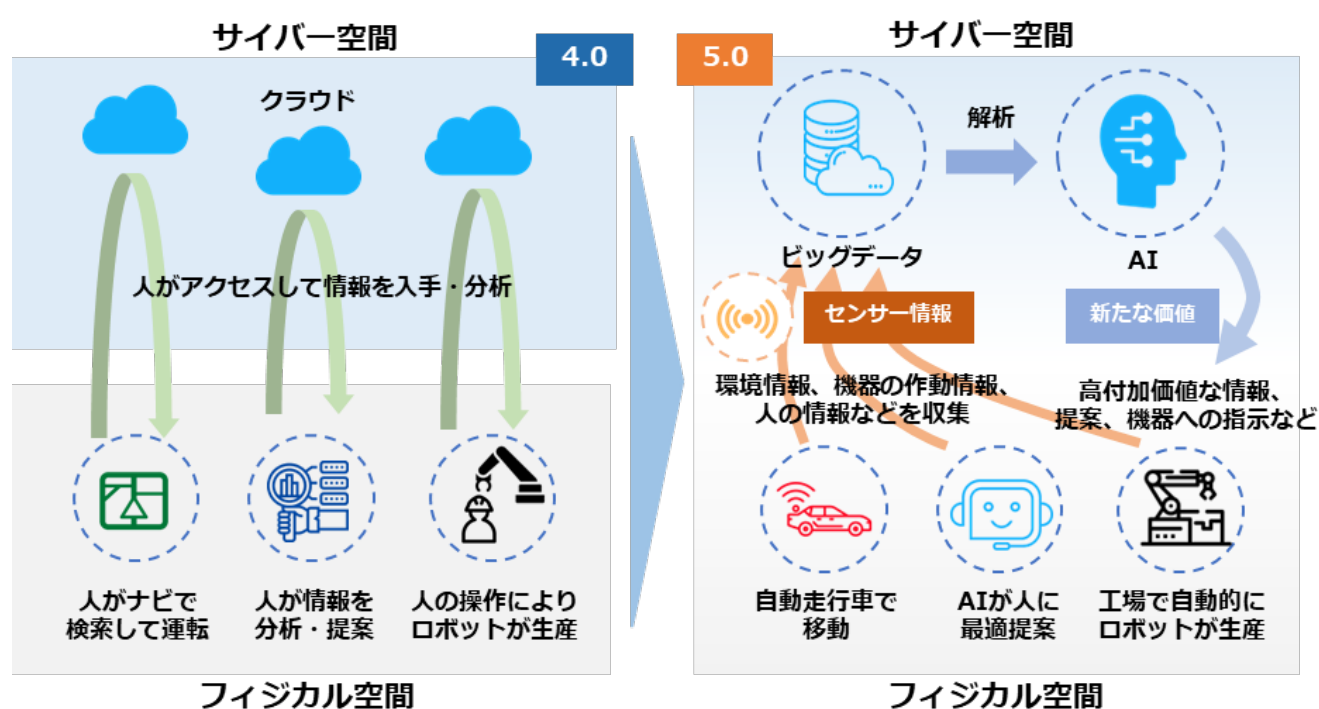


図4. Society4.0 と Society5.0 の比較
（出典）内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0

社会の変化に対するセキュリティ上の脅威

Society5.0 におけるサイバー空間の急激な拡大は、サイバー攻撃の対象が増えることを示しています。サイバー空間とフィジカル空間の相互作用により、サイバー攻撃がフィジカル空間にも影響を及ぼす可能性が高まります。例えば、医療機器やインフラシステムなどがサイバー攻撃によって操作されたり、停止したりすると、人命や社会生活に重大な影響を及ぼす恐れがあります。

Society 5.0 では、多様な人々がサービスの効果を享受できる包摂的な社会を目指していますが、

⁴ 内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0

そのためにはサービスの利用可能性や継続性を確保する必要があります。しかし、サイバー攻撃によってサービスが利用できなくなったり、中断されたりすると、包摂的な社会の実現に支障をきたす可能性があります。また、IoT デバイスやセンサーが収集したデータをサイバー空間で改ざんし、偽情報を拡散するといったフィジカル空間とサイバー空間の情報転送への脅威も考えられます。さらに、IoT や AI などの技術を活用することで、大量のデータが生成されますが、そのデータは個人情報や企業情報などの重要な情報を含む場合が多く、その漏えいや改ざんによってプライバシーや知的財産権などが侵害される危険性が高まります。

また、Society5.0 においては、IoT から得られる大量データの受け渡しなど、サイバー空間とフィジカル空間の融合によって新たな処理が発生します。その新たな処理がサイバー攻撃の対象となる可能性を認識すべきです。Society5.0 においては、サプライチェーンも変化します。サイバー空間とフィジカル空間が融合されることで、サプライチェーンを構成する企業同士の関係が複雑につながります。その結果、サイバー攻撃の影響範囲がこれまで以上に拡大することが予測されます。

Society5.0 における社会の変化	社会の変化に対するセキュリティ上の脅威
大量データの流通・連携	● データの性質に応じた適切な管理の重要性が増大
フィジカル空間とサイバー空間の融合	● サイバー空間からの攻撃がフィジカル空間まで到達 ● フィジカル空間から侵入してサイバー空間へ攻撃を仕掛けるケース ● フィジカル空間とサイバー空間の間における情報の転換作業への介入
複雑につながるサプライチェーン	● サイバー攻撃による影響範囲が拡大

(出典) 経済産業省「サイバー・フィジカル・セキュリティ対策 フレームワーク Ver1.0」をもとに作成

Society5.0 の進展に伴い、セキュリティ対策の重要性が増し、組織や個人がより綿密なセキュリティ対策を講じる必要があります。また、サプライチェーン全体でセキュリティ対策を実施し、企業間で意識を共有することも重要です。

3-2-3. DX の推進

DX の推進における中小企業の優位性について説明します。DX とは、デジタル技術やツールを導入すること自体ではなく、データやデジタル技術を使って、顧客目線で新たな価値を創出していくことです。中小企業の中には、DX を推進し、売上高を 5 倍、利益を 50 倍に増加させた企業が存在します。中小企業ならではの優位性を理解し、積極的に DX に取り組むことで、大きく成長で

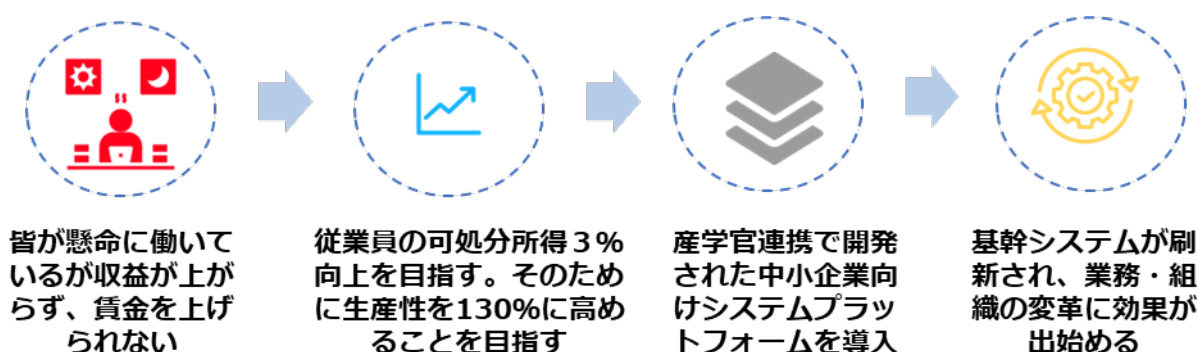
きる可能性があります。以下では、DX を推進する際に、中小企業の優位な点を説明します。そして、優位性を利用してビジネスモデルや企業文化などの変革に取り組んでいる企業の事例を紹介します。

中小企業が DX 推進における優位な点	
参考情報が豊富	DX を既に手掛けている中小企業や、DX を順調に進めている企業のやり方を参考にすることができる
環境が整備されている	先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取り組むことができる
環境の変化に素早く対応しやすい	経営者が即断即決し、新しい取組に臨みやすい利点がある。そのため、変革のスピードにおいて優位性を持つことができる

事例（企業文化の改革）：精密機械部品加工

産学官連携で開発された中小企業向けの共通業務システムプラットフォームを導入し、長年の業務を支えた基幹システムを刷新しました。その結果、無駄な業務や無理な計画などが判明したことに加えて、各部署のデータがつながるようになりました。これにより、各部署がそれぞれ自部署のことにのみを考えていた状態から、他部署に正しいデータを流さなければならないという意識が生まれました。全社で「正しいデータ」を集める意識を持つ企業文化への変革に効果が出始めました。

（出典）経済産業省 「中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き」をもとに作成



データ活用の流れ

顧客視点で新たな価値を創造するためには、製品やサービス、業務の変革が必要です。また、デジタル技術（IoT、ビッグデータ、ロボット、AI など）を用いてデータを活用していくことが大切

です。ここでは、デジタル技術を用いてデータを活用し、製品やサービス、業務を変革していく流れを具体的な事例と合わせて説明します。

以下は、データを活用し、業務を改革していくための手順となります。

手順	概要
1.データの収集	IoT やセンサー、カメラなどの機器を用いて情報を収集します。
2.データの蓄積	収集した膨大なデータ（ビッグデータ）を集積します。
3.データの解析	AI を用いてデータを解析します。
4.解析結果の反映	解析の結果をもとに改革を進めます。

事例（業務改革）：某メーカー

製造現場の加工機にセンサーを設置して、機械の動作を非常に細かい間隔でデータ収集・可視化できる製品を開発しました。また、取得したデータを専門技術者が遠隔で確認し、動作不良の原因調査や製品の適切な使用方法のアドバイスを実施したり、AI によるデータ解析によって使いやすい製品の設計・開発に活用したりすることが可能となりました。

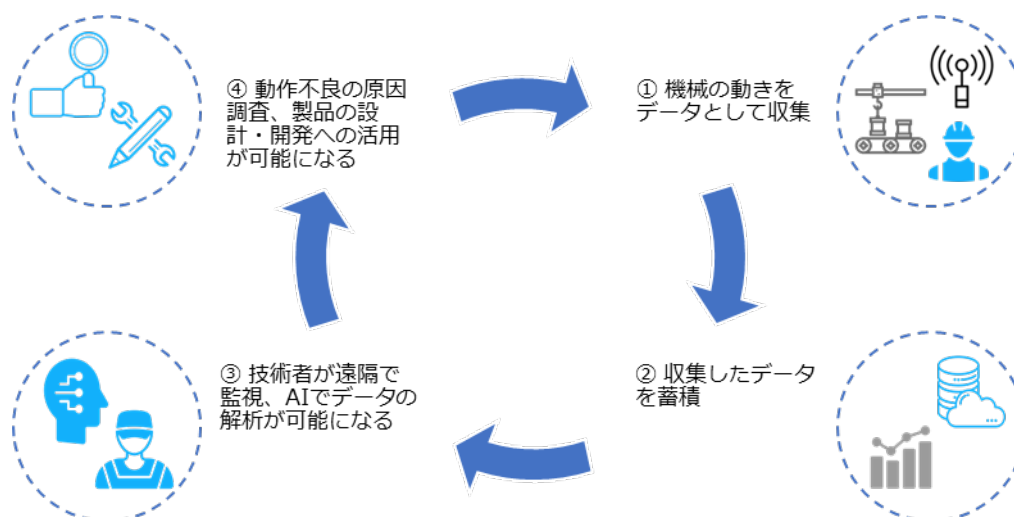


図 5. データ活用による業務改革の流れ

（出典）IPA「製造分野の DX 事例集」.

<https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf>

DX with Cybersecurity の概要

DX を推進していくことで、企業は新たな価値を創造して競争力を強化していくことができます。しかし、DX を推進することは、デジタル技術の利用を拡大することにつながり、サイバー攻撃やデータ漏えいなどのセキュリティ上のリスクが増大することにもなります。そのため、DX を推進すると同時に、セキュリティ対策も強化すること（DX with Cybersecurity）が求められることになります。

DX の推進によって、自社の製品やサービスの価値を向上させることができます。しかし、デジ

タル技術の活用によって増大するセキュリティ上のリスクに対応しなければ、企業の存続を脅かすインシデントが発生するかもしれません。そのため、セキュリティ対策はやむを得ない費用ととらえるのではなく、企業価値や競争力の向上に不可欠なものとしてとらえることが大切です。

DX with Cybersecurity の詳細に関しては、後述のページで説明します。



デジタルトランスフォーメーションの推進

サイバーセキュリティ対策

**デジタルトランスフォーメーションの推進とサイバーセキュリティ対策を
同時に進める必要がある**

第4章. サイバーセキュリティ戦略および関連法令

章の目的

第4章は、[NISC](#)による[サイバーセキュリティ戦略](#)を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法とGDPRについて説明します。

主な達成目標

- 日本におけるサイバーセキュリティに関する方針や施策について理解すること
- サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること
- 個人情報関連の法令を理解すること

4-1. NISC : サイバーセキュリティ戦略

4-1-1. サイバーセキュリティ戦略

サイバーセキュリティ戦略とは、国家レベルでサイバーセキュリティの確保に取り組むための基本的な方針や目標を定めたものです。日本においては、内閣サイバーセキュリティセンター（NISC）が、[サイバーセキュリティ戦略](#)の策定や実施に関する総合調整役を担っています。現行のサイバーセキュリティ戦略は、令和3年9月28日に閣議決定され、「今後3年間に執るべき諸施策の目標や実施方針を示す」ものとされています。この戦略に基づき、政府はサイバーセキュリティの確保に向けた取組を進めています。

サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来
（デジタル改革の推進、新型コロナウイルスの影響、SDGsなど）
サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画
（サイバー攻撃の巧妙化、サイバー空間の公共化、現実世界との相互連関など）

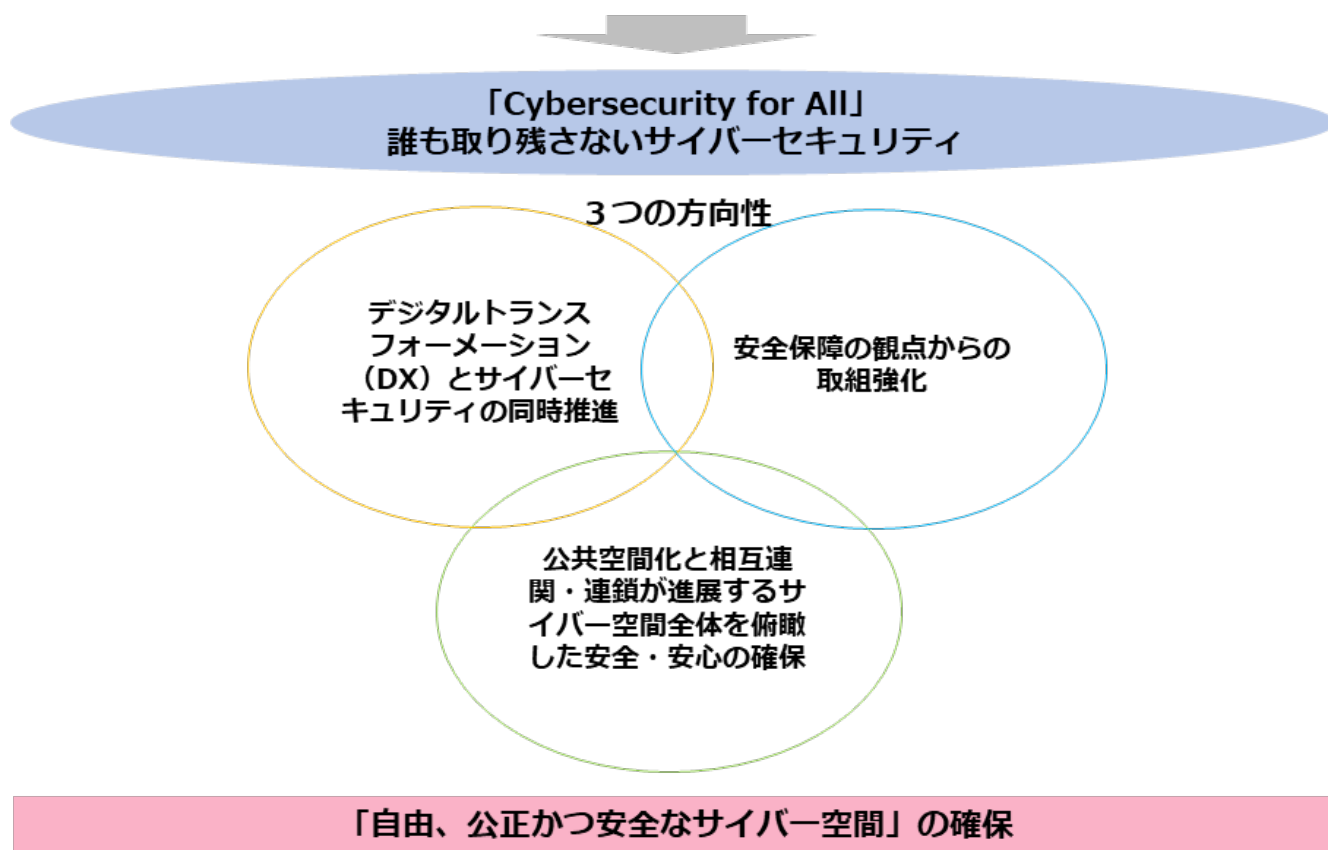


図 6. サイバーセキュリティ戦略の課題と方向性の概要

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

現在、あらゆる人々にとって、サイバーセキュリティの確保が必要とされる時代（Cybersecurity for All）となってきました。また今後、サイバー空間とはつながりのなかった主体も含め、あらゆる主体がサイバー空間に参画することになります。そのため、デジタル化の進歩とともに「誰一人取り残さない」サイバーセキュリティの確保に向けた取組を進める必要があります。この考え方のもと、本戦略では、「自由、公正、かつ安全なサイバー空間」を確保するため、3つの方向性に基づいて施策を推進する方針を示しています。

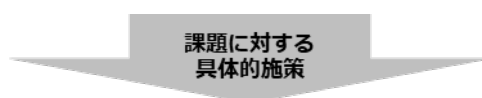
3つの政策目標として、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせるデジタル社会の実現」、「国際社会の平和・安定及び我が国の安全保障への寄与」が掲げられています。これらの目標を達成するために、それぞれの方向性に基づいたさまざまな施策が挙げられています。

経済社会の活力の向上及び持続的発展

方向性	デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進 ➤ デジタル化の進展と併せて、サイバーセキュリティ確保に向けた取組を、あらゆる面で同時に推進

「経済社会の活力の向上及び持続的発展」のためには、「デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進」が必要となります。

課題
● DXの推進が必要とされている中、サイバーセキュリティに対する意識や、サイバー空間を構成する技術基盤やデータなどに対する信頼が醸成されなければ、積極的な参加・コミットメントを得られず、変革を伴わない表層的なデジタル化に留まる恐れがある ● 業務、製品・サービスなどのデジタル化が進む中、サイバーセキュリティの確保は企業価値に直結する重要なものとなっており、製品の企画・設計の段階からセキュリティを考慮する「セキュリティ・バイ・デザイン」が重要視されるなど、デジタル投資とセキュリティ対策を同時に進める必要がある



主な具体的施策
経営層の意識改革 デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化やインセンティブ付けを行い、さらなる取組を促進 地域・中小企業における DX with Cybersecurity の推進

中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業のセキュリティ対策強化の推進

新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり

Society5.0 に対応したフレームワークなども踏まえ、各種取組を推進

- サプライチェーン：産業分野別及び産業横断的なガイドラインなどの策定や活用の促進
- データ流通：送信元のなりすましやデータ改ざんを防止する仕組みの整備
- セキュリティ製品・サービス：第三者検証サービスの普及による信頼性確保の取り組み
- 先端技術：情報収集・蓄積・分析・提供などの共通基盤構築

誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

情報教育推進の中、「デジタル活用支援」と連携して各種取組を推進

(出典) NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

国民が安全で安心して暮らせるデジタル社会の実現

方向性

公共空間化と相互関連・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

- 国は、さまざまな主体と連携しつつ、①自助・共助による自律的なリスクマネジメントが講じられる環境づくりと、②持ち得る手段のすべてを活用した包括的なサイバー防御の展開などを通じて、サイバー空間全体を俯瞰した自助・共助・公助による多層的なサイバー防御体制を構築し、国全体のリスク低減、レジリエンス向上を図る。

「国民が安全で安心して暮らせるデジタル社会の実現」のためには、「公共空間化と相互関連・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保」が必要となります。

課題

- サイバー空間の公共空間化、相互関連・連鎖の深化、サイバー攻撃の組織化・洗練化

課題に対する
具体的施策

主な具体的施策

国民・社会を守るためのサイバーセキュリティ環境の提供

- ① 安全・安心なサイバー空間の利用環境の構築
- ② 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応）
- ③ サイバー犯罪への対策
- ④ 包括的なサイバー防御の展開
- ⑤ サイバー空間の信頼性確保に向けた取組

デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保 経済社会基盤を支える各主体における取組

政府機関など：

- 監査・[CSIRT](#) 訓練・GSOC による監視などを通じたセキュリティ水準の向上
- クラウドサービスの利用拡大を見据えた政府統一基準群の改定
- 運用やクラウド監視に対応した GSOC 機能の強化

重要インフラ：

- 「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」の改定
- 環境変化に対応した防護の強化や経営層のリーダーシップを推進

大学・教育研究機関など：

- 先端情報を保有する大学などへの対策強化支援など
- （リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策）

多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化

（出典）NISC 「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

国際社会の平和・安定及び我が国の安全保障への寄与

方向性

安全保障の観点からの取組強化

- サイバー空間の安全・安定の確保のため、外交・安全保障上のサイバー分野の優先度をこれまで以上に高めるとともに、以下を一層強化する。

「国際社会の平和・安定及び我が国の安全保障への寄与」のためには、「安全保障の観点からの取組強化」が必要となります。

課題

- 我が国を取り巻く安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取などを企図したサイバー攻撃を行っていると思われる
- 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルールなどをめぐる対立などに対して同盟国・同志国などが連携して対抗している

- 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある

課題に対する
具体的施策

主な具体的施策

自由・公正かつ安全なサイバー空間の確保

- サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成）
- サイバー空間におけるルール形成（信頼性のある自由なデータ流通や 5G セキュリティなど）

我が国の防御力・抑止力・状況把握力の強化

- サイバー攻撃に対する防御力の向上（防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、先端技術・防衛産業などのセキュリティ確保のための官民連携・情報共有など）
- サイバー攻撃に対する抑止力の向上（サイバー空間の利用を妨げる能力の活用、外交的手段・刑事訴追などを含めた対応の活用、日米同盟の維持・強化）
- サイバー空間の状況把握力の強化（サイバー攻撃のさらなる実態解明の推進）

国際協力・連携

- 知見の共有・政策調整（国際連携の重層的な枠組みの強化）
- サイバー事案などに係る国際連携の強化（国際サイバー演習の主導などによる国際的なブレイゼンスの向上）
- 能力構築支援（産学官連携や外交・安全保障を含めた ASEAN を含むインド太平洋地域における取組強化）

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

横断的施策

3つの政策目標を達成するためには、サイバーセキュリティ戦略の3つの方向性を意識し、その基盤として、横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組んでいくことが重要です。

サイバーセキュリティ戦略の3つの方向性

デジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進

公共空間化と相互関連・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

安全保障の観点からの取組強化

上記の推進に向け、
横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取り組む

- **研究開発の推進**

産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進

- （1）国際競争力の強化・産学官エコシステムの構築（研究・産学官連携振興施策の活用など）
- （2）実践的な研究開発の推進（サプライチェーンリスクへの対応、攻撃把握・分析・共有基盤、暗号などの研究推進など）
- （3）中長期的な技術トレンドを視野に入れた対応（AI技術の進展、量子技術の進展）

- **人材の確保・育成・活躍促進**

- （1）DX with Cybersecurityの推進（「プラス・セキュリティ」知識を補充できる環境整備など）
- （2）巧妙化・複雑化する脅威への対処（人材育成プログラムの強化、資格制度活用など）
- （3）政府機関における取組み（外部高度人材活用の仕組み強化など）

- **全員参加による協働・普及啓発**

テレワークの増加やクラウドサービスの普及など、近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料などの整備の推進

（出典）NISC「サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成



サイバーセキュリティ基本法

サイバーセキュリティ基本法は、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念や国の責務などを定めています。また、サイバーセキュリティ戦略の策定およびそのほかサイバーセキュリティに関する施策の基本となる事項を規定します。

4-1-2. サイバーセキュリティ 2024

NISC は、国のサイバーセキュリティ対策について、令和 5 年度年次報告・令和 6 年度年次計画

を整理した「サイバーセキュリティ 2024」を公表しています。記載に当たっては、サイバーセキュリティ基本法が定める3つの政策目的と、[サイバーセキュリティ戦略](#)の3つの施策推進の方向性に従って整理されています。

サイバーセキュリティ基本法が定める3つの政策目的

- 経済社会の活力の向上及び持続的発展
- 国民が安全で安心して暮らせる社会の実現
- 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること

サイバーセキュリティ戦略の3つの施策推進の方向性

- デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進
- 公共空間化と相互関連・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保
- 安全保障の観点からの取組強化

本書の中では、中小企業のサイバーセキュリティ対策促進に関する課題や取組などが説明されています。

中小企業のサイバーセキュリティ対策促進

【背景及び課題】

- [サプライチェーン](#)全体の中で対策が相対的に遅れている中小企業を対象とする[サイバー攻撃](#)により、中小企業自身及びその取引先である大企業等への被害が顕在化している。他方で中小企業においては、リスクを自分事として認識していない、あるいは、何をしてもよいかわからない状況が生まれている。
- 予算や人材が不足している中小企業が、それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握し、それを実践できる環境を整備するとともに、中小企業が使いやすいセキュリティサービスを普及・促進していくことが必要である。

【取組の概要】

①手法

- サイバーセキュリティお助け隊サービスについて、2023年度に創設した新たなサービス類型を含め、中小企業等への普及・展開を図る。
- 企業規模やIT資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等を提示する。

- 中小企業等とセキュリティ人材とのマッチングを促す場を構築し、セキュリティ人材のシェアリング促進等、中小企業における人材探索コストの低減を図る。

②取組によって期待される成果・効果

- お助け隊サービスにつき、中規模以上の中小企業等も含めた普及啓発を促進する。
- 費用対効果のあるセキュリティ対策の方法等の提示を図ることで産業界のサプライチェーン全体のセキュリティ対策水準の向上を図る。
- 中小企業における人材探索コストの低減を図ることで企業のサイバーセキュリティ対策を行う側の人材を拡充させる。

【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】

- サプライチェーンは中小企業が支えるところも多く、セキュリティ確保は重要である。
- 中小企業は犯罪者の格好のターゲットになっている。日本産業界のセキュリティ防御の「要」は中小企業にある。
- 政府主導で中小企業のセキュリティ対策支援を積極的に推進すべきである。特に人材と情報共有、補助金支援を中心とした活動に注力すべきである。
- レジリエンス確保は中小企業にとって死活問題になっている。現場の声やニーズに対応して適切な対処方法の提供と普及、それを担う人材の育成等を行う上で「お助け隊サービス」の役割は重要である。
- セキュリティ人材のマッチング、シェアリング等の人材確保支援策にも期待する。

(出典) NISC「サイバーセキュリティ 2024」をもとに作成

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ 2024	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf

4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立

4-2-1. 企業経営のためのサイバーセキュリティの考え方

セキュリティ対策にかかる支出をやむを得ない費用とするのではなく、経営のために必要な投資と位置づけ、自発的にセキュリティ対策に取り組むことが重要です。DX の推進にあたり、IoT などのデジタル技術を積極的に取り入れる中、安全性が高い品質の製品やサービスを実現していく取組は、企業価値や競争力の向上につながります。そのため、DX の推進とセキュリティ対策の強化の両方に取り組むことが大切です。

セキュリティ対策を行うにあたって、以下の基本的認識や留意事項を理解し、自社の現状の IT 活用状況や、セキュリティ対策の取組レベルに応じた対策を行うことが大切です。

2つの基本的認識

<①挑戦>

サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。

<②責任>

すべてがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することになる。

3つの留意事項

<①情報発信による社会的評価の向上>

- セキュリティ対策を、仕方なくやるものではなく、企業価値を高め、品質向上に有効な経営基盤の1つとして位置づけることが必要。
- サイバーセキュリティに関する取組や方針を情報発信することによって、関係者の理解を深め、社会的評価を高めることができる。

<②リスクの一項目としてのサイバーセキュリティ>

- 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。
- 経営層のリーダーシップが必要。

<③サプライチェーン全体でのサイバーセキュリティの確保>

- サプライチェーンでつながるどこかの企業のセキュリティ対策が不十分だと、そこから自社の重要情報が流出してしまうなどの問題が起きる可能性がある。そのため、サプライチェーン全体で一定レベルのサイバーセキュリティの確保が必要。
- 一企業のみでのセキュリティ対策には限界があるため、関係者間での情報共有活動への参

加などが必要。

図 7.IT の活用またはサイバーセキュリティ対策の取組状況に応じた分類と対策
(出典) NISC「企業経営のためのサイバーセキュリティの考え方の策定について」をもとに作成

企業の IT 活用状況、セキュリティ対策の取組のレベルに応じた、実施すべきセキュリティ対策について説明します。企業の IT 活用状況および、セキュリティ対策の意識や実施レベルは、以下の 6 つに分類できます。「理想的」な状態が一番よく、この状態を実現していくためには、自社が置かれているレベルに応じたセキュリティ対策を進めることが重要です。必要なセキュリティ対策の一例を「もっと積極的」、「無駄な投資」、「危険」に該当する分類ごとに紹介します。

レベル	分類	概要・対策
理想的に	1	IT の利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的に IT による革新と高いレベルのセキュリティに挑戦する企業
もっと積極的に	2	IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略としての組み込みはできていない企業 対策：IT を積極的に活用してビジネスの展開を目指すことが重要であり、攻めの IT 投資に関する取組を行うことです。
無駄な投資	3	過剰なセキュリティ意識により、IT の利活用を著しく制限し、競争力強化に活用させていない企業 対策：リスクを再評価して、サイバーセキュリティ対策が過剰になっている部分については見直しを行うことが必要です。
危険	4	サイバーセキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策ができていないにもかかわらず、IT の利活用を進めている企業 対策：情報セキュリティポリシーの策定と実践が必要であり、まずはサイバー攻撃を受けた時のための緊急時対応マニュアルを作成すべきです。
	5	サイバーセキュリティの必要性を理解していない企業や、自らセキュリティ対策を行う上で事業上のリソースの制約が大きい企業 対策：コストがあまりかからない最低限のセキュリティ対策から実施することが重要であり、例えば「情報セキュリティ 5 か条」の対策を行うべきです。
対象外	6	IT を利用していない企業

図 8 IT の活用またはサイバーセキュリティ対策の取組状況に応じた分類と対策
(出典) 東京都「IT およびサイバーセキュリティに関する組織の視点 6 分類」をもとに作成

4-2-2. DX with Cybersecurity

業務や製品・サービスのデジタル化が進む中、サイバーセキュリティの確保は企業の価値に直結する重要な要素となっています。このため、DX とサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が不可欠となっています。しかしながら、中小企業が DX with Cybersecurity を推進するにあたり、人材や予算などのリソース不足などさまざまな課題が存在しています。これらの課題に対処するため、国が実施している施策の一部について説明します。



経営層の意識改革

DX with Cybersecurityの推進に向けた主な施策の分類



新たな価値創出を支える
サプライチェーンなどの信頼性確保に向けた基盤づくり



地域・中小企業における
DX with Cybersecurityの推進

経営層の意識改革

【課題】経営層が主体性を持って DX とセキュリティ対策に取り組むためには、セキュリティの専門家とのコミュニケーションが重要

【施策】経営者が IT やセキュリティに関する専門知識を持っていない場合でも、セキュリティの専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備

地域・中小企業における DX with Cybersecurity の推進

【課題】中小企業は、セキュリティ対策に予算を割くことの必要性を理解する

【施策】中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進

新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり

サプライチェーンの信頼性確保

【課題】サイバー攻撃の起点となりうる箇所の拡大に伴う、リスク管理が重要

【施策】産業分野別、または産業横断的なガイドラインの策定や活用促進を通じて、産業界におけるセキュリティ対策の具体化・実装を促進

データ流通の信頼性確保

【課題】データの真正性や流通基盤の信頼性を確保することが重要

【施策】データマネジメントの定義、送信元のなりすましやデータの改ざんなどを防止する仕組みを整備

セキュリティ製品・サービスの信頼性確保

【課題】市場において提供されるセキュリティ製品・サービスが信頼できるか、客観的な評価が必要

【施策】一定の基準を満たすセキュリティサービスの審査・登録する仕組みを整備

先端技術・イノベーションの社会的実装

【課題】デジタル化の進展に伴い、効率的なセキュリティ対策が必要

【施策】研究機関の知識や技術を民間企業が活用しやすい環境の整備や、企業が社外の知識や技術を取り入れ、組織の改革（セキュリティ対策の強化など）を進められる環境の整備を推進

施策の理解のため参考となる文献（参考文献）	
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/curriculum/

4-3. 関連法令

4-3-1. 個人情報保護法

インターネットが普及し、ネットショッピングなど、さまざまなサービスの利用を通して個人情報のやり取りが当たり前になった現在、個人情報の保護は人々にとって身近なテーマとなりました。企業にとって、個人情報は事業へ有効に活用することのできるものですが、漏えいなどの事故が起きた場合、社会的な信用の失墜に直結するため、事業経営に及ぼす影響は非常に大きいです。

そのため、消費者や取引先から預かっている個人情報を適切に取扱うことは、企業の権利や利益を守ることにつながる非常に重要な取り組みとなります。ここでは、サイバーセキュリティに関連する法令として、個人情報保護法について説明します。

個人情報保護法とは

インターネットの普及や情報技術の進歩などを背景として、個人の権利や利益を守ることを目的として「個人情報保護法」（正式名称：個人情報の保護に関する法律）が平成 17 年 4 月に全面施行されました。施行後も、デジタル技術の進展やグローバル化などの経済・社会情勢の変化や、世の中の個人情報に対する意識の高まりなどに対応するため、今までに 3 度の改正が行われています。

個人情報保護法では、どのような情報が個人情報になるのか、個人の権利や利益を守るためには個人情報をどのように取扱わなければいけないのかなどが規定されています。

個人情報の定義

個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報のことを指します。これには他の情報と容易に照合でき、それにより特定の個人を識別できるものも含まれます。

個人情報を取扱う時の基本ルール

① 取得・利用	② 保管・管理
● 利用目的を特定して、その範囲内で利用する。 ● 利用目的を通知または公表する。	● 漏えいなどが生じないように、安全に管理する。 ● 従業者や委託先にも安全管理を徹底する。
③ 提供	④ 開示請求などへの対応
● 第三者に提供する場合は、あらかじめ本人から同意を得る。 ● 第三者に提供した場合、提供を受けた場合は一定事項を記録する。	● 本人から開示などの請求があった場合はこれに対応する。 ● 苦情に適切かつ迅速に対応する。

個人情報保護法の罰則規定

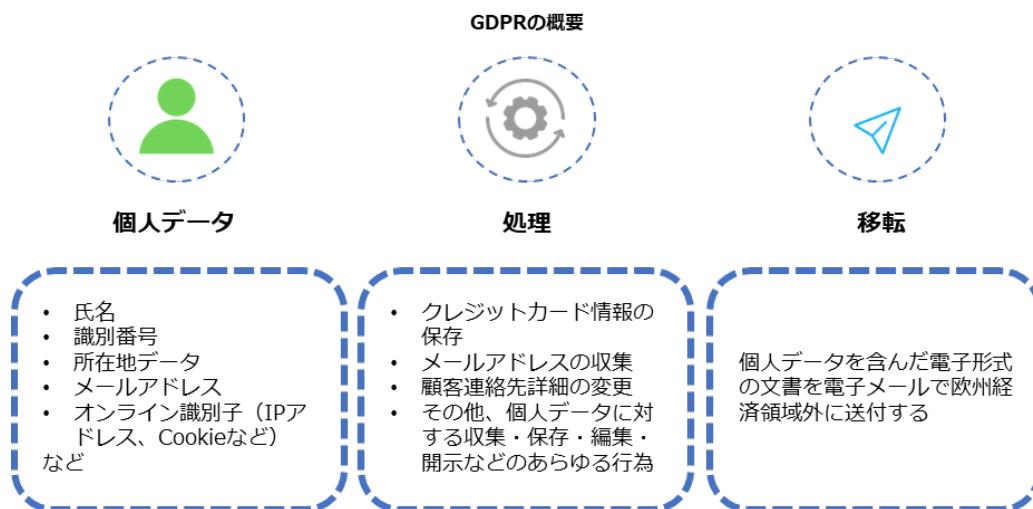
令和 4 年 4 月施行の法改正により、法令違反に対する罰則が強化されました。法人に対しては、個人情報保護委員会の措置命令に違反したり、個人情報データベースを不正流用したりした場合 1 億円以下、報告義務違反の場合 50 万円以下の罰金となっています。

4-3-2. GDPR

GDPR（EU 一般データ保護規則）とは、個人データの保護とプライバシーの権利を強化するために、欧州連合（EU）加盟国に適用される重要な法令です。EU で活動する企業だけではなく、EU 加盟国の居住者の個人データを取扱う企業は、企業規模に関係なく、GDPR が適用されるため、GDPR を理解し遵守することが必要です。以下では、GDPR の概要および日本企業の関わりについて説明します。

GDPR（一般データ保護規則）とは

EU で策定された新しい個人情報保護の枠組みであり、個人データ保護やその取扱いについて詳細に定められた欧州経済領域内の各国に適用される法令のことです。欧州経済領域内で取得した「個人データ」を「処理」し、欧州経済領域外の第三国に「移転」するために満たすべき要件が定められています。GDPR の特徴として、インターネット上で収集できる個人データのほとんどが保護対象となっています。



GDPR と日本企業の関係

GDPR は EU 内で適用される法令ですが、支店など物理的な拠点を EU 内に持っていなくても、インターネットを利用して日本から EU 域内に商品販売やサービス提供、情報収集を行っている企業にも GDPR が適用されます。また、ターゲティング広告を配置した自社サイトに対

して、EU 域内からアクセスがあった際も GDPR の適用対象となる可能性があります。GDPR に違反した場合はかなり重い制裁金が課されるため、適切な対策が求められます。

GDPR に向けた対策例

GDPR では、Cookie が「個人情報」とみなされるため、Web サイトで Cookie を利用する際は、Web サイト閲覧者から Cookie 取得の同意を得る仕組みを構築することが必要です。Cookie についての本人の同意を取得するには、企業とユーザーとの間で個人データの利用における同意の実施・管理を行うツール（CMP）を導入することが推奨されています。

4-3-3. その他関連法令

そのほか、サイバーセキュリティに関連する法令の例を紹介します。

不正競争防止法

事業者間の不正競争の防止を目的の 1 つとしており、ブランドの表示の盗用、商品の形態模倣などととともに、営業秘密や限定データの不正取得・使用などを規制している。

著作権法

プログラムを含む著作物の保護と複製権をはじめとする著作権などについて規定している。

電気通信事業法

サイバー空間における活動の基盤となるインターネットサービスなどの電気通信事業に関する諸規定や、通信の秘密などを規定している。

電子証明および認証業務に関する法律

デジタルデータの流通と情報処理の円滑な利用のため、電子署名や認証業務の法的な取扱いを定めている。

情報処理の促進に関する法律

情報処理の高度利用促進を目的とした法律で、情報処理安全確保支援士や情報処理技術者試験に関する規定、サイバーセキュリティに関する調査や講習を行っている IPA の業務範囲などに関する規定を含んでいる。

国立研究開発法人情報通信研究機構法

NICT の業務においてサイバーセキュリティに関する研究開発など、国や自治体の従業員を対象とする演習の「CYDER」の実施を定めるとともに、時限的な業務として [IoT](#) 機器の調査を行う「NOTICE」に関する規定を措置している。

刑法

不正指令電磁的記録に関する罪（いわゆるウイルス罪）をはじめとするサイバー犯罪を処罰する規定を含む刑罰が規定されている。

不正アクセス行為の禁止などに関する法律

不正ログインといった不正アクセス行為や、いわゆるフィッシング行為を処罰する旨が規定されている。

これらの関連法令を解説した資料として「サイバーセキュリティ関係法定 Q&A ハンドブック」があります。可能な限り平易な表記で記述されており、効率的・効果的なセキュリティ対策・法令遵守を促進するために、参考になります。

施策の理解のため参考となる文献（参考文献）	
サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0	https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook_2.pdf

編集後記

第1編では、社会におけるセキュリティのトレンド、サイバーセキュリティに関する基礎知識、デジタル社会に向けた国の方針などについて紹介をしました。

セキュリティ対策を始める際には、中小企業においては [SECURITY ACTION](#)（セキュリティ対策自己宣言）の中にある一つ星の「情報セキュリティ 5 か条」から実行することをおすすめします。一つ星の取組が完了したら、次は二つ星の「5分でできる！情報セキュリティ自社診断」と「情報セキュリティ基本方針を策定」に取り組みます。もし既にこれらを実行している場合は、サイバーセキュリティアプローチを用いてセキュリティ対策を進めることになります。第2章では「Lv.1 クイックアプローチ」、「Lv.2 ベースラインアプローチ」、「Lv.3 網羅的アプローチ」について簡単に紹介しましたが、第3編以降では具体的な手順も含めて詳しく解説していきます。

第5章. 事例を知る：重大なインシデント発生から課題解決まで

章の目的

第5章では、近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対するセキュリティ対策や、実際に被害に遭ってしまった際の対応方法について学ぶことを目的とします。

主な達成目標

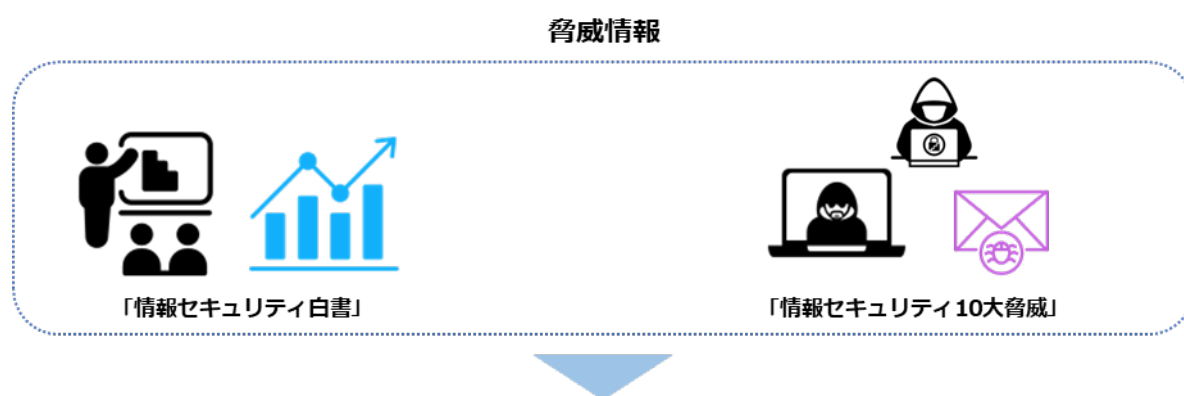
- 近年のサイバー攻撃の傾向や手法を理解すること
- 実際の被害事例を通して脅威に対するセキュリティ対策や予防方法を理解すること
- 脅威の検知から、復旧・再発防止処置までの流れを理解すること

5-1. 情報セキュリティの概況

5-1-1. 情報セキュリティの脅威を学ぶ

情報セキュリティは、個人のユーザーから国の重要インフラやグローバルの通信インフラまで、あらゆるレベルで重要な課題となっています。情報技術（IT）の進歩と普及により、私たちの生活はますます情報システムに依存したものになっています。しかし、便利さの一方で、情報漏えいや不正アクセスといったさまざまな脅威にさらされています。その脅威を理解することは、組織や個人の情報セキュリティレベルの向上に有効です。組織を構成する個人がセキュリティの基本的な知識を持つことで、組織全体の情報セキュリティレベルの向上が期待できます。

どのような脅威があるかは、IPA が公開する「情報セキュリティ白書」や「情報セキュリティ 10 大脅威」が参考になります。「情報セキュリティ白書」は、情報セキュリティの現状とその将来の展望を示し、情報セキュリティの傾向と課題を詳細に解説しています。「情報セキュリティ 10 大脅威」は、1 年間で注目を集めた脅威について事例やセキュリティ対策などを紹介しています。



目的
最新の脅威情報を収集することによって、攻撃の傾向や手法、セキュリティリスクを把握し、適切な予防策やセキュリティ対策を講じること
学べる内容
● 攻撃手法や攻撃者の手口 ● 最近の攻撃傾向 ● 脅威に対するセキュリティ対策方法
活用例
● 攻撃の予防 ● セキュリティリスク管理、対策の強化 ● <u>セキュリティポリシー</u>の改善 ● <u>セキュリティインシデント</u>への対応

- 脅威トレンドの把握、共有
- セキュリティ意識の向上

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ白書 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/10threats2024.html

5-1-2. IPA：情報セキュリティ白書から見る脅威

情報セキュリティ白書は、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックのほか、その年ならではの象徴的なトピックを取り上げています。本書情報セキュリティ白書は、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックのほか、その年ならではの象徴的なトピックを取り上げています。本書を通して、情報セキュリティ分野の全体を把握できます。情報セキュリティ白書は、IPA によって 2 平成 20 年から毎年発行されています。

令和 5 年 7 月に刊行された「情報セキュリティ白書 2023」は、令和 4 年度のサイバー攻撃による実際の被害やセキュリティ対策など、情報を守るための最新情報をまとめています。



図 9. 情報セキュリティ白書 2023

情報セキュリティ白書 2023 の記載内容

- 序章 令和 4 年度の情報セキュリティの概況
- 情報セキュリティインシデント・脆弱性の現状と対策
- 情報セキュリティを支える基盤の動向
- 個別テーマ
- 付録 資料・ツール

サイバー攻撃の内容を知りたい

活用例

- 標的型攻撃やランサムウェア攻撃などの事例、手口やセキュリティ対策を知ることができる
- 社内の注意喚起に利用する

セキュリティ人材の育成方法を知りたい

活用例

- ICSCoE 中核人材育成プログラムやセキュリティ・キャンプの活動を知る

- 人材育成のための国家試験や国家資格について知る

セキュリティ対策の進め方が
知りたい

活用例

- SECURITY ACTION や サイバーセキュリティお助け隊サービス制度 などの活動を知り、自社で取り組む

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ経営ガイドライン Ver. 3.0	https://www.meti.go.jp/policy/netsecurity/mng_guide.html
SECURITY ACTION セキュリティ対策自己宣言	https://www.ipa.go.jp/security/security-action/
サイバーセキュリティお助け隊サービス制度	https://www.ipa.go.jp/security/sme/otasuketai-about.html
セキュリティ・キャンプ	https://www.security-camp.or.jp
ICSCoE 中核人材育成プログラム	https://www.ipa.go.jp/jinzai/ics/core_human_resource

中小企業における情報セキュリティ対策の重要性はますます高まっています。デジタル化の進展により、重要なデータや顧客情報の保護は喫緊の課題となっています。情報セキュリティの重要性が高まる中、私たちが直面する主要なリスクには以下のようなものが挙げられます。

企業、組織への 信頼性低下



重要データの漏えい、改ざん等により、顧客との信頼関係の損失。

サービスの中断



業務やサービスが一時的または永続的に中断。

経済的損失



直接的な経済的損失。
（例：被害の復旧コスト、業務の停止による売上への影響、法的な制裁や罰金等）

法的な制裁



セキュリティ対策が不十分な場合、関連する法的規制や規範に違反

情報セキュリティ白書では、1年間のインシデント状況を紹介しています。それによると情報セキュリティの脅威は年々増加しており、2021年の情報セキュリティインシデント報道件数は769件となり、前年比で43.2%増加しました（図9）。⁵

2019年からの情報セキュリティインシデント報道件数の増加は明らかであり、今後もその数はさらに増加すると見込まれています。

⁵ IPA.“情報セキュリティ白書 2022”. <https://www.ipa.go.jp/publish/wp-security/sec-2022.html>

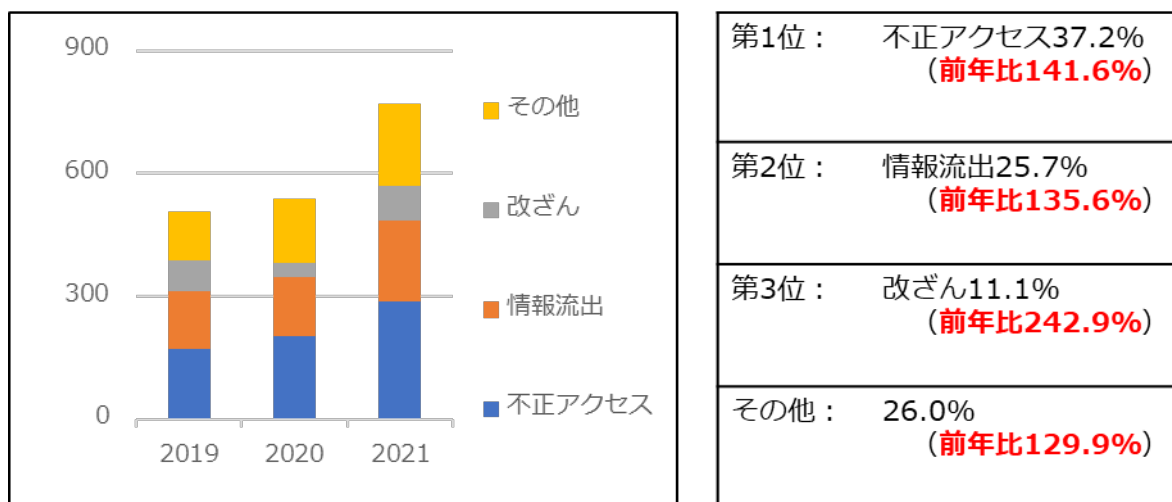


図 10. 情報セキュリティインシデント報道件数
(出典) MBSD 社による集計情報を基に作成

5-1-3. IPA : 情報セキュリティ 10 大脅威

「情報セキュリティ 10 大脅威」は、IPA が毎年発表している、情報セキュリティ分野において特に注意すべき脅威のトップ 10 が「個人」と「組織」に分けてリストアップされています。過去 1 年間に発生したセキュリティインシデントや攻撃の状況をもとに、情報セキュリティ分野の研究者と実務担当者などによる審議・投票によって 10 個の脅威が選定されています。これを活用することで、何を重視してセキュリティ対策を実施すれば良いのかがわかります。

順位に関わらず自身に関係のある脅威に対してセキュリティ対策を行うことが重要です。

情報セキュリティ 10 大脅威の活用法：組織の検討例

1. 「守るべきもの」の明確化	自社の守るべきものを明確にします。 ● 業務プロセス：取引先との受注業務 ● 情報データ：取引先情報や受注先情報 ● システム、サービス、機器：社内 IT システムとその構成機器 ● その他：取引先との信頼関係など
2. 自社にとっての脅威の抽出	情報セキュリティ 10 大脅威を参考にして自社の守るべきものに対する脅威を抽出します。 脅威が生じた場合の被害額を算出し、会社の経営方針を考慮し、優先順位をつけます。 ● <u>ランサムウェア</u>感染による社内 IT システムの使用不能・脅迫（ランサムウェアによる被害） ● 取引先である大企業へのサイバー攻撃の踏み台として悪用（サプライチェーンの弱点を悪用した攻撃）

	従業員による顧客情報や取引情報の不正持ち出し（内部不正による情報漏えい）



3. 対策候補（ベストプラクティス）の洗い出し	抽出した脅威に対する対策候補（ <u>ベストプラクティス</u> ）を洗い出します。
	- 被害の予防：<u>不正アクセス</u>対策、バックアップの取得、基本方針の策定、情報セキュリティの認証取得など - 被害の早期検知：システムの操作履歴の監視など - 被害を受けた後の対応：<u>CSIRT</u>、関係者への連絡、影響調査、バックアップからの復旧、復号ツールの活用など



4. 実施する対策の選定	洗い出した各対策候補に対して現状を整理し、未実施内容に対しての対策を選定します。
	① 実施状況を確認（実施済み、一部実施、要調査など） ② 対応計画を立案 ③ 対策の実施

（出典）IPA「情報セキュリティ 10 大脅威の活用法 2024」をもとに作成

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ 10 大脅威の活用法 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g23i-att/katsuyouhou_2024.pdf

「情報セキュリティ 10 大脅威 2024」の組織向け脅威（1～10 位）を紹介します。

1 位	ランサムウェアによる被害 攻撃者は、PC やサーバをランサムウェアに感染させ、さまざまな脅迫を行い、金銭を要求します。組織の規模や業種に関係なく攻撃が行われているという点に注意が必要です。 事例：<u>VPN (Virtual Private Network)</u> 経由で侵入、ランサムウェアを横展開（某地域購買生協） 11 台のサーバ内の情報がランサムウェアに<u>暗号化</u>されました。暗号化されたデータには約 49 万人の個人情報が含まれていました。攻撃者は、ネットワーク機器の<u>脆弱性</u>を悪用して VPN 経由で侵入し、ランサムウェアを横展開しました。
2 位	サプライチェーンの弱点を悪用した攻撃 直接攻撃が困難な組織に対し、標的組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社などを攻撃し、踏み台にして標的組織に侵入する攻撃です。

	事例：委託先のシステムを介して不正アクセス、顧客情報漏えい（保険会社） 複数の保険会社で、業務委託先から顧客の個人情報が流出しました。流出の規模は、多いところで約 130 万人分におよびました。原因は、業務委託先の適切なセキュリティ対策がされていないサーバへの不正アクセスでした。
3 位	内部不正による情報漏えい等の被害 従業員や元従業員などの組織関係者による機密情報の持ち出しや社内情報の削除などの不正行為が発生しています。 事例：前職場が保有する名刺情報を転職先に提供（人材派遣会社） 従業員は同業他社に転職する直前に、転職元の名刺情報管理システムにログインするための ID とパスワードを転職先の従業員に共有していました。不正に取得された名刺情報は転職先の営業活動に使用されました。
4 位	標的型攻撃による機密情報の窃取 <u>標的型攻撃</u>は、特定の組織（企業、官公庁、民間団体など）を狙う攻撃のことです。攻撃者は社会や働き方の変化に合わせて攻撃手口を変えるなど、組織の状況に応じた巧みな攻撃手法を用いることに注意が必要です。 事例：不正アクセス、機微情報含まず（国立研究開発法人） ネットワーク機器の脆弱性を悪用し、一般業務用の管理サーバに不正アクセスされました。
5 位	修正プログラムの公開前を狙う攻撃（<u>ゼロデイ攻撃</u>） ゼロデイ攻撃は、ソフトウェアの開発ベンダーなどが脆弱性対策情報を公開する前に、脆弱性を悪用する攻撃のことです。事業やサービスが停止するなど、多くのシステムやユーザーに被害が及ぶことがあります。 事例：ファイル圧縮ソフトウェア ファイル圧縮ソフトウェアの一部の脆弱性がゼロデイ攻撃に悪用されていることがわかりました。スクリプトを実行させることが可能になる脆弱性でした。
6 位	不注意による情報漏えい等の被害 システムの設定ミスによる非公開情報の公開や、個人情報を含んだ記憶媒体の紛失など、不注意による機密情報の漏えいが発生しています。 事例：個人情報のコピーした USB メモリを紛失（市民病院） 再委託先担当者が 132 人分の個人情報を含むデータを USB メモリにコピーして持ち

	出し、紛失しました。
7 位	脆弱性対策情報の公開に伴う悪用増加 脆弱性対策の公開情報を悪用して、脆弱性対策の実施が遅れている製品・システムのセキュリティホールを狙うという攻撃が発生しています。近年、情報の公開から攻撃が本格化するまでの時間が短くなっています。 事例：脆弱性を修正した機器へ継続的な攻撃（メールセキュリティ製品） 本脆弱性の修正対応後も、特定の組織では、攻撃者による新たなバックドアの設置や、ネットワーク上での横展開など、継続的な攻撃活動が確認されています。
8 位	ビジネスメール詐欺による金銭被害 悪意のある第三者が標的組織やその取引先の従業員などになりすましてメールを送信し、あらかじめ用意した偽の銀行口座に金銭を振り込ませるといった詐欺です。 事例：信頼できる取引先を騙るメール詐欺（医療製品企業） 支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に総額 2 億円振り込みをしたことを公表しました。
9 位	テレワーク等のニューノーマルな働き方を狙った攻撃 テレワークに活用される VPN サービスなどを狙った攻撃が、引き続き行われています。 事例：在宅勤務用のリモートアクセス経路より侵入の疑い（製造業） 攻撃者がリモートアクセス経路から侵入し、ランサムウェアでデータセンターや国内拠点の一部サーバに保存されていたデータを暗号化しました。結果、約 6 万件の個人情報外部に流出しました。
10 位	犯罪のビジネス化（アンダーグラウンドサービス） アンダーグラウンド市場では、アカウントの ID やパスワード、クレジットカード情報、ウイルスなどが売買されています。話題のサービスのアカウント情報も売買されており、多要素認証を取り入れるなどのセキュリティ対策が重要です。 事例：国内製造業の情報がダークウェブに流出（製造業） ダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明しました。

(出典) IPA「情報セキュリティ 10 大脅威 2024」をもとに作成

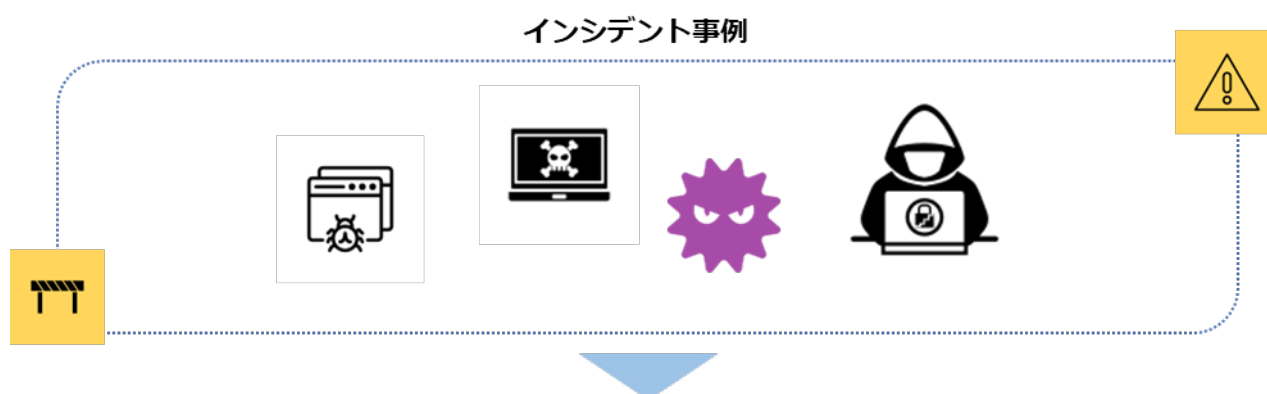
5-2. 重大インシデント事例から学ぶ課題解決

5-2-1. インシデント事例から学ぶ

デジタル社会が急速に発展し、インターネットが日常生活のあらゆる側面に浸透している現代において、情報セキュリティは最優先事項となっています。そのため、過去の重大インシデントから学び、脅威に対抗することが重要です。

不正アクセスやランサムウェアの暗号化による業務停止、システムの損失といった実際の事例から、何がうまくいかなかったのか、どのような手段が用いられたのか、どのような脆弱性が攻撃の対象となったのか理解することができます。これらの失敗から学ぶことは、理論的な知識だけでは得られない実践的な視点を身につけることができます。そして、実践的な視点を身につけることで、インシデントが発生した際の対応手順や新たなセキュリティポリシーの策定といった具体的な行動につながります。

インシデント事例から学ぶことは、情報セキュリティの向上に欠かせません。過去の事例を通じて、脅威に対する対応策の策定や現在使用しているリスク戦略の改善、セキュリティ意識の向上が可能です。その結果、組織や個人の情報を守り、将来起こり得るインシデントに適切な対応を行うことが可能となります。



目的

実際に発生した攻撃事例やセキュリティインシデント事例をケーススタディとして学ぶこと。具体的な知識をもとに実践的なアプローチ手法を習得すること。

学べる内容

- 攻撃手法や攻撃者の手口
- インシデントの影響と被害範囲
- 具体的なインシデント対応と復旧策

活用例

- セキュリティリスク管理、対策の強化
- セキュリティポリシーの改善

- セキュリティインシデント対応の改善
- 脅威トレンドの把握、共有
- セキュリティ意識の向上

5-2-2. 最近の攻撃トレンド、および中小企業にも発生しうるサイバー被害事例

攻撃手法は日々進化しており、中小企業もその標的とされることが増えています。以下では、最新の攻撃トレンドに焦点を当て、中小企業におけるサイバー被害の事例を紹介します。さまざまな攻撃手法や実際の被害事例を通じて、中小企業がより強固なサイバーセキュリティ体制を構築する手助けとなります。

IoT デバイスによるサービス被害

最近、IoT デバイスを標的にしたマルウェアが広まっています。このマルウェアに感染した大量の IoT 機器は、攻撃者によって遠隔操作され、大規模な DDoS 攻撃に利用されます。企業が DDoS 攻撃を受けると、自社の Web サイトが遅延したり、機能停止したりすることがあります。そして、攻撃を停止することと引き換えに、攻撃者から金銭を要求されることもあります。このような攻撃に対抗するためには、Web アプリケーションへの攻撃を防ぐための WAF（Web アプリケーションファイアウォール）や、ネットワーク上の攻撃を防御するための IPS（Intrusion Prevention System）の導入が考えられます。

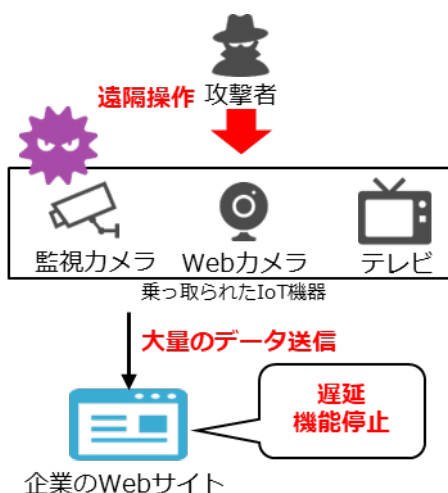


図 11. DDoS 攻撃の概要図

テレワークによるサイバー被害事例

新型コロナウイルスの影響により、テレワークが急速に広まり定着しています。企業では、テレワークを実施するために VPN を利用して社外から社内ネットワークに安全に接続する取組が増えています。しかし、VPN の脆弱性を悪用したサイバー攻撃が確認されています。具体的な事例と

して、某メーカーのインシデントが挙げられます。同社は、VPN 機器において過去に判明した脆弱性に対処するためのアップデートを実施しました。しかし、アップデート前にパスワード情報が漏えいしており、当時から存在していたアカウントがパスワードの変更を行っていなかったため、不正アクセスが行われ、ランサムウェアの被害を受ける事例が発生しました。企業は、VPN のセキュリティ対策に十分な注意を払う必要があります。特に、パスワードの管理や定期的なアップデートの実施が重要です。

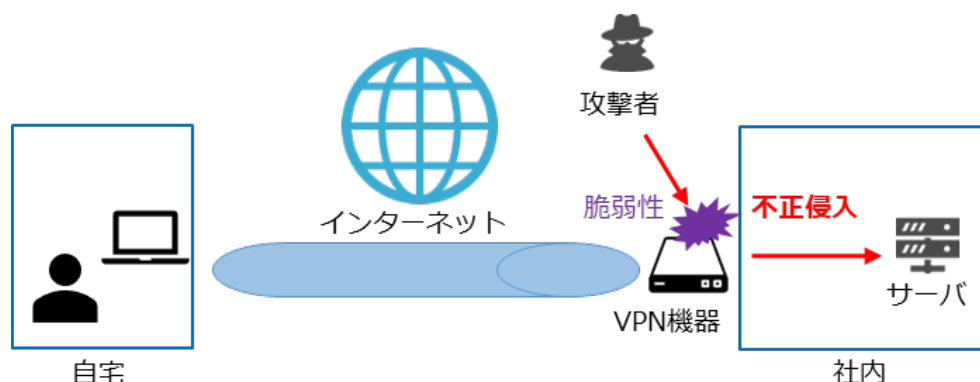


図 12. VPN 機器の脆弱性を利用した攻撃のイメージ

テレワークのセキュリティ対策

総務省は、予算やセキュリティ管理体制が十分でない中小企業などを対象とした「中小企業等担当者向けテレワークセキュリティの手引き」を発行しています。この手引きでは、テレワークを実施する際に中小企業が考慮すべきセキュリティリスクに基づき、実現可能性と優先度の高いセキュリティ対策を具体的に示しています。本書に示されたセキュリティ対策を実施することで、基本的かつ重要なセキュリティ対策を適切に行うことができます。以下の表は、会社が提供する端末を使用して VPN や リモートデスクトップ接続 を利用する際に必要なセキュリティ対策のチェックリストの一部です。

分類	対策内容	想定脅威
資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク端末とその利用者を把握している。	マルウェア感染・不正アクセス盗難・紛失
物理セキュリティ	テレワーク端末に対して覗き見防止フィルタをはり、離席時には <u>スクリーンロック</u> をかけるようルール化している。	情報の盗聴

詳細理解のため参考となる文献（参考文献）	
中小企業等担当者向け テレワークセキュリティの手引き 第3版	https://www.soumu.go.jp/main_content/000816096.pdf

5-2-3. 事案発生->課題の抽出->再発防止策の実施までの流れ

インシデントが発生した場合の基本的な対応方法についての紹介となります。図 8 に示すように、3つのステップで対応します。



図 13. インシデント対応の
3ステップ

① 検 知 ・ 初 動 対 応	検知と連絡受付： インシデントの兆候や実際の発生に気づいた場合は、情報セキュリティ責任者に報告します。責任者は適切な対応が必要と判断した場合には、経営者に報告します。 対応体制の立ち上げ：経営者は事前に策定している対応方針に従い、役割分担を明確にするために責任者と担当者を指名します。これにより、インシデントに迅速かつ効果的に対応する体制を整えます。 初動対応： 被害の拡大を防ぐために、ネットワークの遮断やシステムの停止などの適切な措置を行います。ただし、システム上に記録が残されている場合は、対象機器の電源を切る際に注意し、記録を消去しないようにします。
② 報 告 ・ 公 表	第一報： インシデントが発生したことを、被害の拡大を防ぐために関係者全員に適切なタイミングと内容で通知します。通知が困難な場合は、Web サイトやメディアを通じて公表したり、関係する顧客や消費者に対してはお問い合わせ窓口を開設したりして対応します。 第二報以降・最終報： インシデント復旧の進捗状況や再発防止策などの詳細情報を報告し、被害者に対する損害の補償を行います。個人情報漏えいの場合は、必要に応じて個人情報保護委員会や関連省庁に報告し、犯罪の可能性がある場合は警察に、ウイルス感染や不正アクセスの場合は情報処理推進機構（IPA）に報告します。
③ 復 旧 ・	調査・対応： インシデントの原因や影響範囲を詳しく調査し、適切な対応策を策定します。被害の拡大を止めるために適切な措置をとり、被害の影響を最小限に抑えるよう努めます。 証拠保全：

再 発 防 止	事実関係を裏づける証拠などを収集し、訴訟対応や事件解明、法的手続きに活用します。
	必要に応じて <u>フォレンジック</u> 調査を実施し、証拠の確保と分析を行います。
	復旧： インシデントの修復が確認された後、復旧作業を実施します。システムやデータを正常な状態に戻し、ビジネスの継続性を確保します。復旧作業が完了したら、経営者に報告します。
	再発防止策： 同様のインシデントが再発しないよう、再発防止策を立案・実施します。セキュリティの強化や従業員の教育・訓練の強化などを通じて、将来のインシデントを防止するための措置を講じます。

(出典) IPA「中小企業のためのセキュリティインシデント対応の手引き」をもとに作成

詳細理解のため参考となる文献（参考文献）	
中小企業のためのセキュリティインシデント対応の手引き	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf

5-2-4. インシデントから得た気づきと取組

過去のインシデントから得た知見に基づき、改善取組に焦点を当てていきます。実際に発生した事例を通じて、問題点や課題を明確にし、それに対するセキュリティ対策や予防策を紹介していきます。

サプライチェーンを介した標的型メール攻撃

【事例の概要】

ある企業の工場部門は、取引先企業のメールアカウントが攻撃者に乗っ取られるという被害に遭いました。攻撃者は、取引先企業のフリをして工場部門の担当者に対して、マルウェアが添付されたメールを送信しました。その結果、2台の端末がマルウェアに感染してしまいました。このマルウェアは、通常の定義型ウイルス対策ソフトウェアでは検知することができませんでしたが、EDRを導入していたことで早期に検知し、感染の拡大を食い止めることができました。⁶

【問題点・課題】

- 攻撃者が取引先の正規アカウントを乗っ取っていたため、メール自体に不審な点を見つけることが困難でした。
- 取引先が乗っ取りを受けているため、自社単独では攻撃を完全に防ぐことは困難でした。

⁶ NISC:「サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）」https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf

- 取引先へのセキュリティ支援や[アセスメント](#)の範囲と、それに伴う負担を自社でどの程度検討すべきかについて検討が必要でした。取引先のセキュリティに対する支援やアセスメントの範囲を検討し、自社が負担できる範囲でのセキュリティ対策を考える必要があります。

【対策・予防策】

- 取引先のセキュリティ対策状況を把握するためには、ヒアリングシートやアンケートなどの手法を使用することが重要です。これにより、取引先のセキュリティレベルや[脆弱性](#)を明確にすることができます。
- 工場のセキュリティを強化するためには、国内で最新の工場システムを構築しているベンダーに自社工場のアセスメントを依頼することが有効です。

EDR を導入してマルウェアの[エンドポイントデバイス](#)上での活動を監視し、異常な振る舞いを検知することができます。また既に EDR を導入している場合は、[ゼロトラスト](#)、[SASE](#) の[フレームワーク](#)にある機能の [SWG](#)などを体系的に実装することで、さらにセキュリティを強化することができます。

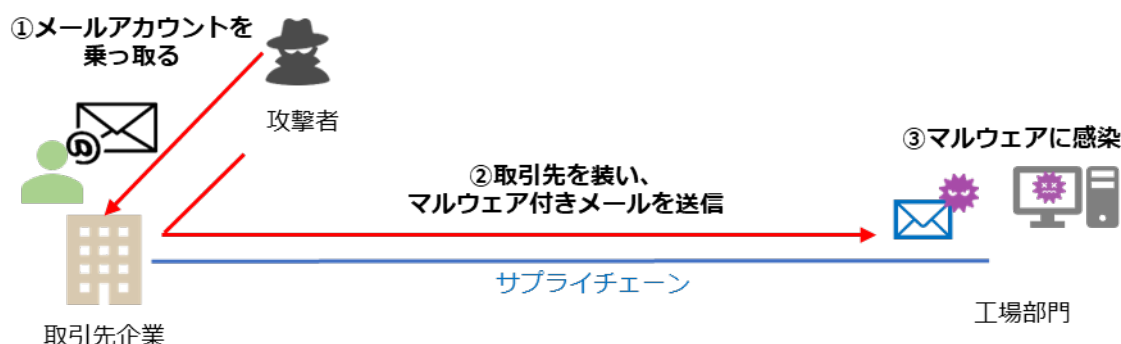


図 14. 攻撃の概要図

(出典) NISC「サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）」をもとに作成

5-2-5. ランサムウェア感染の実態

[ランサムウェア](#)は、PC やサーバのデータを暗号化し、その[暗号化](#)されたデータを復号することを条件に身代金（金銭）を要求する悪意のあるソフトウェアです。令和 5 年における企業や団体の被害件数は合計 197 件であり、被害企業の規模を見ると、大企業が 71 件、中小企業が 102 件、団体などが 24 件でした。ランサムウェアの感染経路については、[VPN](#) 機器からの侵入が 73 件で全体の 63%を占め、リモートデスクトップからの侵入が 21 件で 18%となっています。これらの侵入は、テレワークなどで使用される機器の[脆弱性](#)や弱い認証情報を悪用して行われたものであり、全体の約 82%に上る割合を占めました。⁷

⁷ 警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」。https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

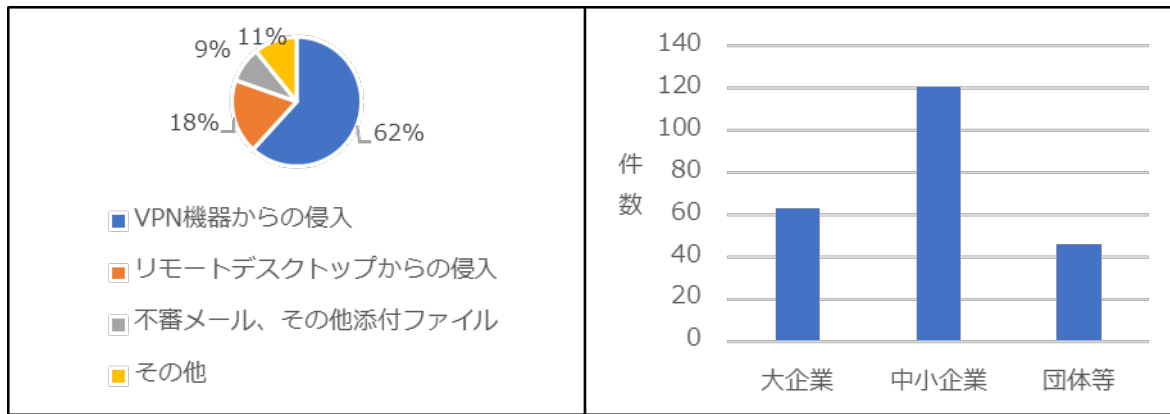


図 15. (令和 5 年) ランサムウェアの感染経路

図 16. (令和 5 年) ランサムウェアの被害件数

(出典) 警察庁「令和 5 年におけるサイバー空間をめぐる脅威の情勢等について」をもとに作成

最近のランサムウェアは、以下のような特徴を持っています。図の①②のように、データの復旧を条件に金銭を要求する脅迫に加えて、暗号化前のデータを窃取し公開するという「二重脅迫」を行うものが存在します。さらに、追加の脅威として③DDoS 攻撃などの追加攻撃を行うことで被害を拡大することもあります。また、さらに高度な手法として、④被害者の利害関係者に連絡し、情報を共有するなどの「四重脅迫」を行うケースも確認されています。

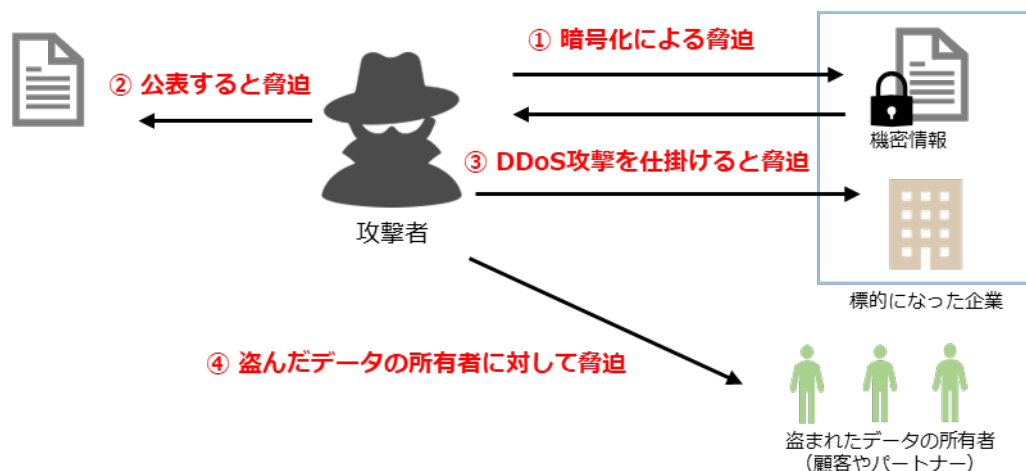


図 17. ランサムウェアの二重、四重脅迫のイメージ図

具体的なランサムウェア攻撃の事例を紹介し、攻撃手法や被害の具体的な内容を解説します。実際のケースを通じてランサムウェアによってもたらされる被害の大きさを理解し、自身や組織のセキュリティ対策を見直すきっかけとしてください。

電子カルテシステムでランサム被害（某市民病院）

事例の概要

外部のインターネットから電子カルテシステムのサーバと一部のクライアントパソコンがランサムウェアに感染しました。サーバの復旧を優先する一方、システムログの保全を行わず再起

動したため、正確な原因究明ができなくなりました。

被害の原因

この事例の原因は、「ルール違反」を犯してインターネットに接続したことにより、外部からウイルスが侵入したことです。また、導入に携わる業者の管理や障害時対応の適切な運用体制が構築、運営されていなかったため、病院のガバナンスにも問題がありました。

この事例から学べること

- [マルウェア](#)対策ソフトウェアの定期的な更新とスキャンは、侵入を防ぐために重要です。
- インターネットに安易に接続してはいけません。拠点間をインターネットで接続する時には安全なVPNを用いるようにしましょう。
- 侵入後のログ保全を行うためには、システムの導入に加えて、適切な運用体制を構築、運営することが重要です。
- 安易にインターネットに接続しないことは、ウイルスを侵入させないために重要です。

VPN 機器に対するランサム攻撃（某容器販売業）

事例の概要

サーバなどに対して第三者による[不正アクセス](#)を受け、ランサムウェアを用いた[サイバー攻撃](#)による被害が発生しました。この攻撃によって、暗号化されたデータには、従業員に加えて、取引先の個人情報が含まれていました。

被害の原因

この事例の被害の原因は、流出したネットワーク機器の認証情報を利用し、VPN 経由で業務サーバを含む複数のサーバへ不正侵入されたことです。この結果、個人情報を含むデータが暗号化されてしまいました。

この事例から学べること

- [多要素認証](#)や[アクセス制御](#)によって接続者を制限することが非常に重要です。
- バックアップの保護や[EDR](#)の導入などのセキュリティ対策を講じることが重要です。また、VPN より高セキュリティな接続方法である[SDP](#)の導入も検討すべきです。

詳細理解のため参考となる文献（参考文献）

コンピュータウイルス・不正アクセスの届出事例

<https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf>

5-3. 実際の被害事例から見るケーススタディー

5-3-1. 最近のサイバー被害事例発生傾向

サプライチェーンを通じて、被害が起きた原因の分析内容および効果的なセキュリティ対策ベストプラクティスを紹介します。

サプライチェーンを通じた被害

被害の概要

某メーカーの取引先企業がサイバー攻撃を受け、システムが使用不能になりました。この攻撃により、某メーカーは部品の調達が可能になり、その結果、複数の工場が停止し、数万個以上の生産が見送られる事態に陥りました。この出来事は、サプライチェーン攻撃のリスクとその被害の大きさを再認識させる上で非常に重要な事例となりました。

被害の原因

ウイルスの侵入経路は、子会社が独自に特定外部事業との専用通信に利用していたリモート接続機器の脆弱性があり、そのことをきっかけとして不正アクセスを受けました。攻撃者はリモート接続機器から子会社内のネットワークに侵入後、さらに親会社のネットワークに侵入して、サーバや PC の一部を暗号化しました。

セキュリティ対策・ベストプラクティス

- VPN 装置は外部のネットワークからアクセス可能な位置に設置されることが多く、外部の攻撃者から攻撃されやすくなります。そのため、VPN 装置のベンダーの Web サイトなどを確認し、未対策の脆弱性がないかを点検することが大切です。
- サイバー攻撃の被害は取引先企業に広がる可能性があります。セキュリティ対策は自社に加えて、サプライチェーンでつながっている会社、取引先企業を含めて考え、実施する必要があります。

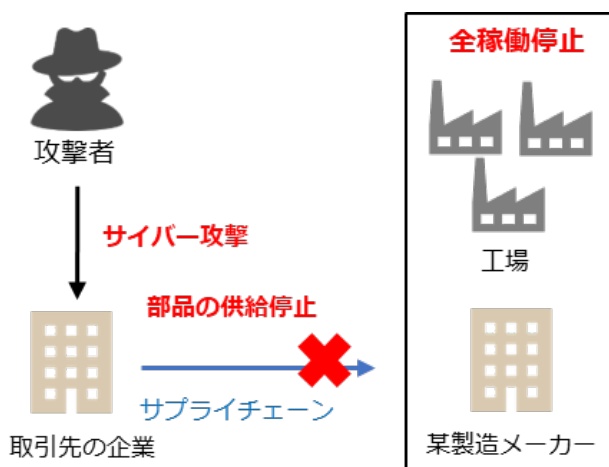


図 18. 攻撃の概要図

5-3-2. 事例：某港のランサムウェア被害

港湾施設のターミナルシステムが大規模なランサムウェアによるサイバー攻撃を受けて停止し、3 日間にわたり、コンテナの搬入、搬出が停止し物流に大きな影響を及ぼしました。

ランサムウェアの感染経路として考えられるのは、VPN 機器からの侵入、USB メモリからのウイルスの持ち込み、事業者間のネットワーク連携で運用している NAT 変換による接続からの侵入があります。しかし、サーバ内のデータがすべて暗号化されているため、ログの解析が困難となり、感染経路を特定することができませんでした。物理サーバがすべて暗号化されていることから VPN 機器からの侵入が行われた可能性が高いと見られています。数か月前から VPN 機器および物理サーバの脆弱性が公表されていたにもかかわらず、IP アドレスの制限をかけていなかったため、ID とパスワードが一致すればどこからでもアクセスできる状況になっていました。

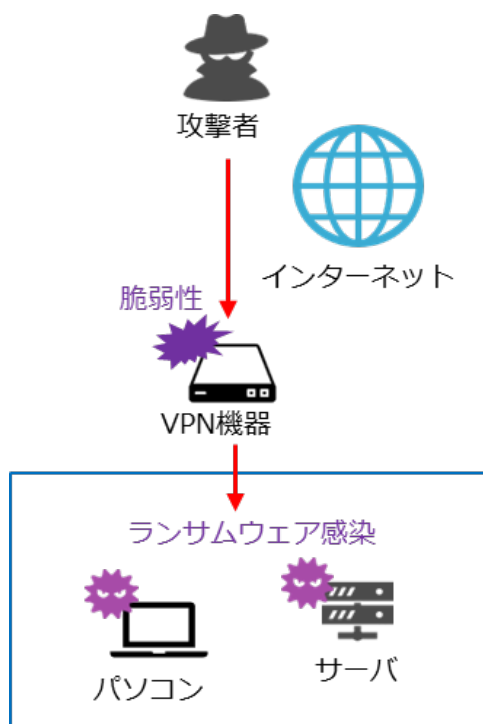


図 19. 攻撃の概要図

問題点

- VPN 装置は導入当初からソフトウェアの更新が行われていなかった。
- 厚生労働省からの注意喚起はあったが、事業者側がリスク評価できず被害を想定できなかった。
- 庶務係が IT 担当者を一人で兼任しており、セキュリティの知識・技術が不十分であった。
- 「VPN 装置を使用すれば外部からのサイバー攻撃を受けない」という誤解があった。
- ベンダーがシステムの動作優先で、セキュリティ対策を考慮していなかった。

教訓

- 取引をしているベンダーと情報交換、コミュニケーションをとる。
- 経営者・担当者のセキュリティレベル向上を図る。
- インシデントが発生した時の被害を想定する。

会社の規模、業種を問わず、ランサムウェアの被害に遭う可能性はあります。大事なことは、「自社が狙われている」という危機感を持つことです。ランサムウェアに限らず、他の事例も含めて、

危機感を持ちセキュリティ対策を総合的に取り組むことが重要です。

詳細理解のため参考となる文献（参考文献）

コンピュータウイルス・不正アクセスの届出事例

<https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf>

5-3-3. 具体的な対応策

ランサムウェア被害のケースを見ると、VPN 機器から不正侵入され、サーバの特権 ID を使用してサーバのデスクトップ上から不正プログラムを実行されるケースが後を絶ちません。セキュリティ対策、運用については、まず、VPN で接続するためのインターネットとの接点を絞りこみ、接続してくる者の身元を確認し、本人であることを証明させる多要素認証の仕組みを講じることが必要となります。それ以外にも、特定の PC やサーバからしか重要なサーバのデスクトップに接続できないような仕組みや、ログの長期保管なども重要な要素となります。

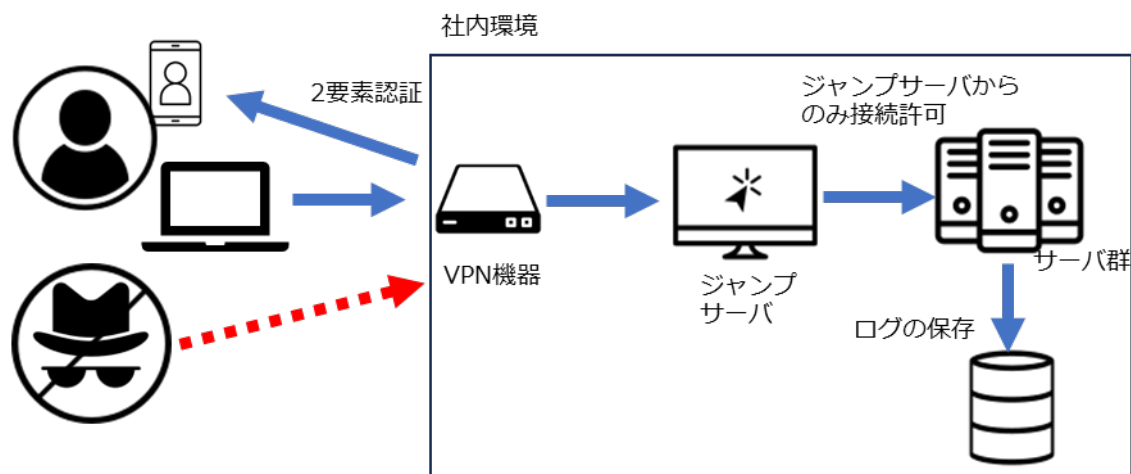


図 20. 対応策の概要図

実施すべきセキュリティ対策と運用

- VPN 接続の認証に多要素認証を実装し、接続する個人の身元を証明します。
- ジャンプサーバを構築し、社内のサーバへのリモートデスクトップはジャンプサーバからの接続のみ許可します。
- サーバの特権アカウントのパスワードを、定期的に変更します。
- PC の Administrator アカウントを無効化するか、LAPS などのツールを用いて定期的に動的なパスワード変更を行います。
- サーバやネットワーク機器のログを長期的に取得し、定期的を確認します。
- 社内では利用しているネットワーク機器やソフトウェアの脆弱性情報について、定期的を確認します。
- ネットワーク機器のファームウェアや、使用している PC の OS、ソフトウェアのセキュリティパッチを適用します。

第6章. 企業経営で重要となる IT 投資と投資としてのサイバーセキュリティ対策

章の目的

第 6 章では、これからの企業経営で必要な観点となる社会の動向、「守りの IT 投資」や「攻めの IT 投資」などの IT 投資について学ぶことを目的とします。また、経営投資としてのセキュリティ対策の重要性を明確にすることを目的とします。

主な達成目標

- 社会の動向を把握し、現実社会とサイバー空間のつながりを理解すること
- IT 投資としての「守りの IT 投資」と「攻めの IT 投資」を理解すること
- 経営投資としてのセキュリティ対策の重要性を理解すること

6-1. これからの企業経営で必要な観点：社会の動向

6-1-1. 現実社会とサイバー空間のつながり

日々の生活や企業活動において、IT の活用は広範囲にわたって浸透しています。インターネット利用率（個人）は平成 9 年には 9.2%でしたが、令和 4 年には 84.9%まで上昇しました。急速な IT の普及により、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革変化をもたらしています。

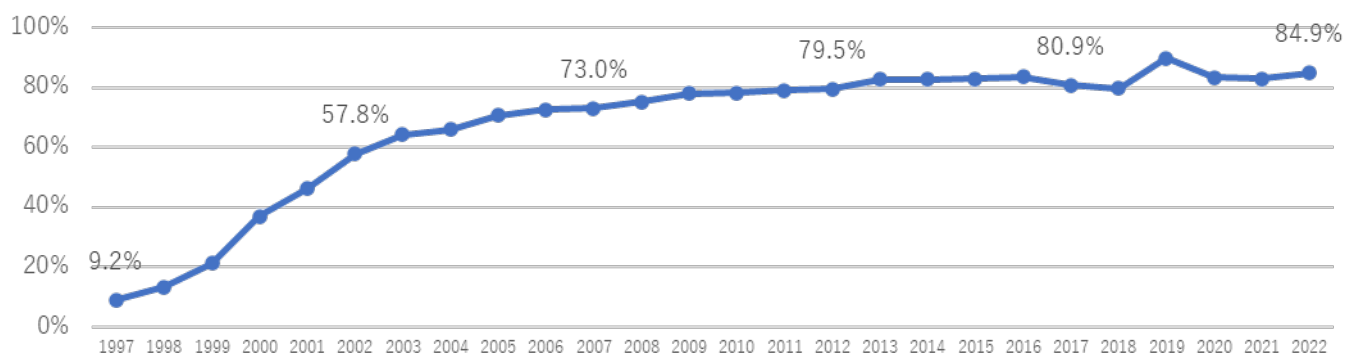


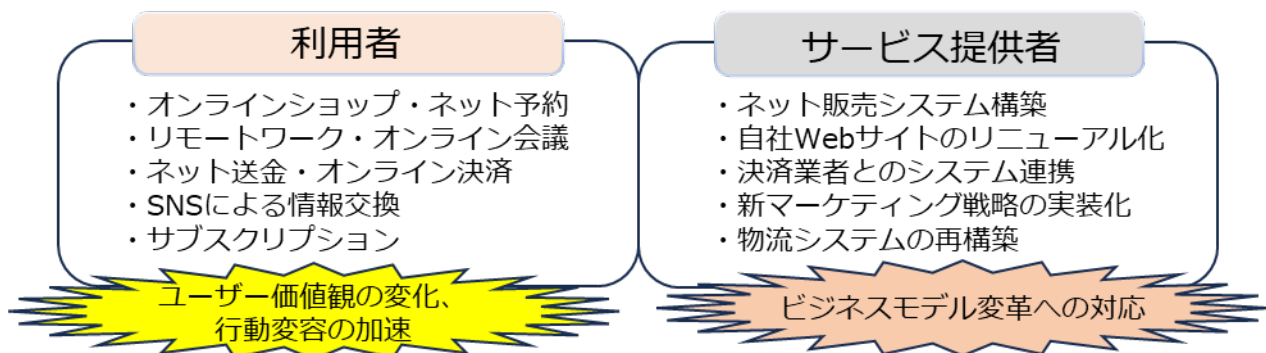
図 21. インターネット利用率（個人）の推移
（出典）総務省「通信利用動向調査」をもとに作成

IT の普及により、私たちはより価値のあるサービスを利用することが可能になりました。例えば、インターネットを介して必要な情報を瞬時に入手したり、オンラインショッピングサイトを利用して、広範囲の商品を比較して購入したりすることができるようになりました。

さらに、スマホなどの普及によって、利用者の意見や情報を即座に国境を超えて交換できるようになりました。SNS やオンラインコミュニティを通じて、個人が持つ意見や情報が一瞬で共有され、世界的な話題になることも少なくありません。社会の意識形成や情報伝達において、IT の果たす役割はより大きくなっていると言えるでしょう。

一方で、IT を活用したサービスの提供を求められています。技術の進化が速く、競争が激化しているため、常に最新のサービスを提供し続ける必要があります。また、企業の経営戦略やビジネスモデルも IT の普及に伴って変化しており、革新的なアイデアと素早い行動が求められる時代になっています。

こうした変化を踏まえ、政府は、さらなる経済発展と社会的課題の解決をするため、サイバー空間とフィジカル空間を融合させたシステムによる新たな社会の姿（[Society5.0](#)）を未来社会のコンセプトとして提唱しています。



Society5.0 で実現する社会では、企業を中心に付加価値を生み出すための一連の活動であるサプライチェーンも変化します。サプライチェーンは、製造、物流、在庫管理、販売などの過程を通じて製品やサービスが供給される経路全体を指します。これまでは、主にサービスが供給される物理的な流れであるフィジカル空間が中心とされていましたが、今後の社会では、サイバー空間とのつながりが重要視されています。

サプライチェーンで利用される技術として、IoT デバイスや AI が挙げられます。IoT デバイスや AI が導入されることにより、製造や物流などのプロセスにおいてセンサーやネットワークが活用され、物理的な動作をサイバー空間で制御・監視できるようになります。さらに、クラウドコンピューティングの普及により、サプライチェーンにおける情報共有やデータのやり取りが容易になり、他社との連携が可能になります。これにより、サプライチェーン全体が可視化され、フィジカル空間とサイバー空間が融合し、サプライチェーンを構成する企業同士の関係は、フィジカル空間に加えて、サイバー空間においても密接になります。

今後の社会では、サプライチェーンにおけるフィジカル空間とサイバー空間とのつながりが重要視されています。そして、Society5.0 に合ったサプライチェーンに変化することで、従来のサプライチェーンもより柔軟で効率的なものになります。

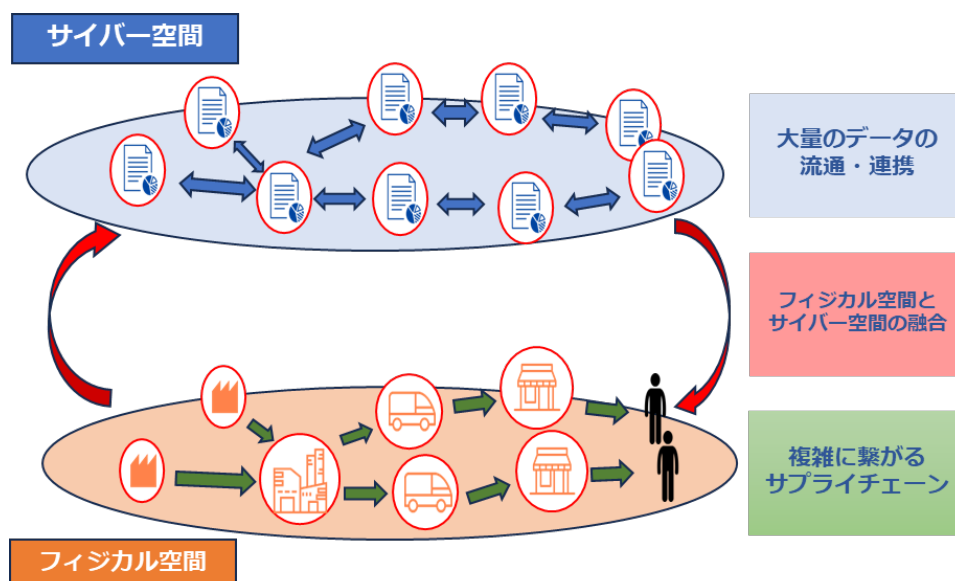


図 22. サイバー空間とフィジカル空間の関係図

(出典) 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク Ver.1.0」をもとに作成

サイバー空間とフィジカル空間を密接に統合する仕組みをCPS(サイバーフィジカルシステム)と呼んでいます。CPSは多様なデータをセンサーネットワークなどで収集し、サイバー空間で分析、知識化を行い、その結果を現実世界に反映させることによって産業の活性化や社会問題の解決を行います。CPS/IoTの利活用分野別の世界市場調査の結果を電子情報技術産業協会(JEITA)が平成29年に公表しました。CPS/IoTの世界市場規模は、平成28年時点で、世界で194兆円、日本で11.1兆円でしたが、令和11年には世界で404.4兆円、日本で19.7兆円とほぼ倍増する見込みです。

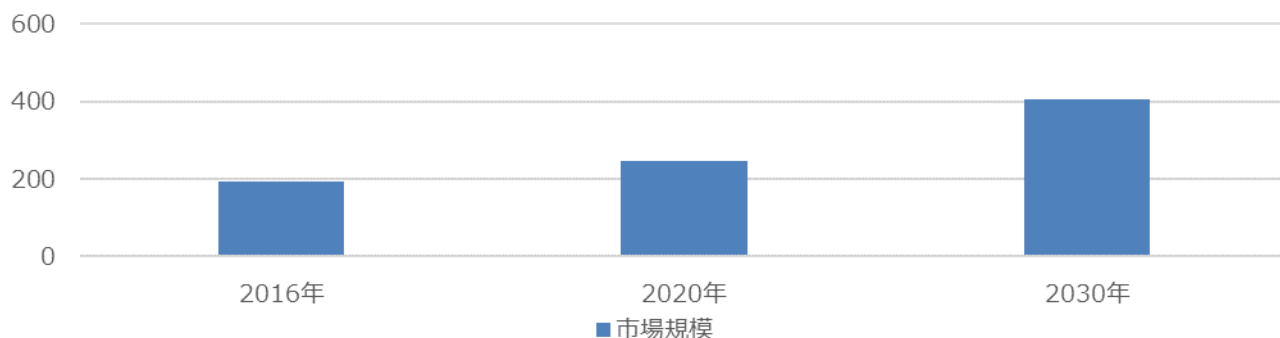


図 23. CPS/IoT の世界市場の推移
(出典) JEITA「CPS/IoTの世界市場の調査結果」をもとに作成

CPS/IoT市場を10の利活用分野別にみた調査結果によると、令和11年時点で最も大きい市場が家庭・個人で106.1兆円です。次いで流通・物流が44.9兆円、製造(FA・自動車)が44兆円、公共が39.3兆円、金融が29.9兆円、放送・通信が25兆円、医療・介護が22.3兆円、農業が7.8兆円、環境・エネルギーが5.4兆円、その他産業が79.8兆円となっています。CPS/流通・物流、製造(FA・自動車)の市場規模が高いことは、製品やサービスが供給される経路全体を指すサプライチェーンとCPSが関わると言えます。世界的にもCPS/IoTの需要額が増加することから、企業は生産性向上や課題の解決のためにCPS/IoTの利活用が重要になります。

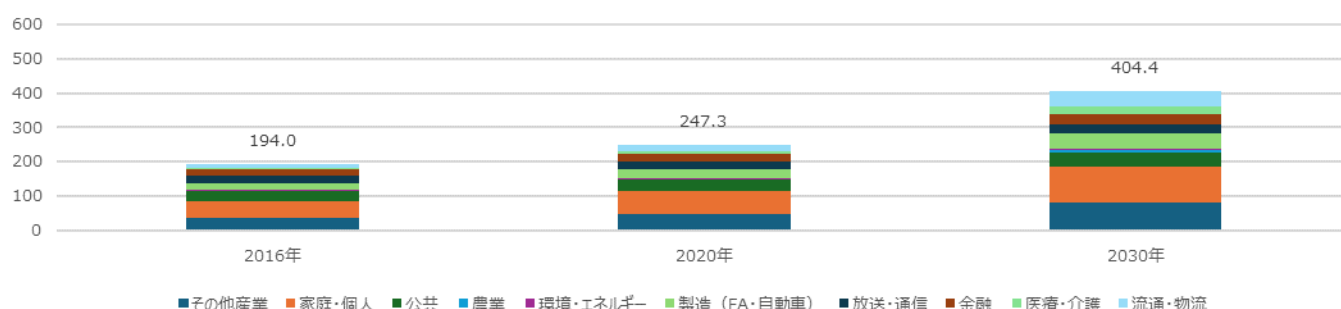


図 24. CPS/IoT の利活用分野別需要額の推移
(出典) JEITA「CPS/IoT世界市場の利活用分野別需要額見通し」をもとに作成

6-1-2. IT 活用における課題

我が国のデジタル化について、デジタルインフラ整備などの一部については世界的に見ても進んでいるものの、全体としては大幅に後れていると言えます。さまざまな理由が複雑に絡み合い、我が国のデジタル化の後れが生じていると考えられます。⁸

ここでは日本社会がデジタル化で後れをとった理由についてみていきます。

我が国がデジタル化で後れをとった 6 つの理由

1. ICT 投資の低迷

我が国における ICT 投資は、1997 年をピークに減少傾向にあります。また、我が国における ICT 投資の 8 割が現行ビジネスの維持・運営に当てられているなど、従来型のシステム（レガシーシステム）が多く残っており、その頃の考え方やアーキテクチャから抜け出せていないと言われています。これらを背景として、我が国では、オープン化やクラウド化への対応、業務やデータの標準化が遅れ、業務効率化やデータ活用が進んでいない状況にあると考えられます。

2. 業務改革等を伴わない ICT 投資

ICT 投資が効果を発揮するためには、業務改革や企業組織の改編などを併せて行うことが重要とされていますが、外部委託に全面的に依存することで、業務改革などをしない形での ICT 導入となり、十分な効果が発揮できなかったため、デジタル化に向けたさらなる ICT 投資が積極的に行われなかった可能性があります。

3. ICT 人材の不足・偏在

我が国の ICT 人材は、量も質も十分ではないとユーザー企業に認識されています。また、その人材についても、外部ベンダーへの依存度が高く、ICT 企業以外のユーザー企業に多く配置されており、ユーザー企業では、組織内で ICT 人材の育成・確保ができていません。

4. 過去の成功体験

我が国は、高度経済成長期を経て、世界有数の経済大国となりましたが、ICT 関連製造業についても生産・輸出が 1985 年頃まで増加傾向にあり、「電子立国」とも称されていました。2000 年代に入ってから、ICT 関連製造業の生産額が減少傾向に転じ、2000 年代後半には輸出額も減少傾向にあります。それ以前の成功体験により、抜本的な変革を行うよりも、個別最適による業務改善が中心となり、デジタル社会の到来に対応できていないと言われています。

5. デジタル化への不安感・抵抗感

デジタル化が進んでいない理由として最も多く挙げられたことが「情報セキュリティやプライバシー漏えいへの不安があるから」（52.2%）でした。また、パーソナルデータの企業などによる不適切な利用、インターネット上に流布する偽情報への対応、慣れないデジタル操作など

⁸ 総務省, “情報通信白書令和 3 年版”, <https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf>

への習熟など、さまざまな要因により、デジタル化に対する不安感・抵抗感が生じる場合があると考えられます。

6. デジタルリテラシーが十分ではない

デジタル化が進んでいない理由として2番目に多く挙げられたことが「利用する人のリテラシーが不足しているから」(44.2%)でした。このようにデジタルリテラシーが十分ではないと考えられることから、デジタル化推進に対して消極的になる場合があると考えられます。

(出典) 総務省「情報通信白書令和3年版」をもとに作成

現在、日本においてDXの取組状況がどのような状態かを確認するため、DXに取り組む企業が多いとされる米国と比較します。

1. DXの取組状況

日本でDXに取り組んでいる企業の割合は令和3年度調査の55.8%から令和4年度調査では69.3%に増加、令和4年度調査の米国の77.9%に近づいており、この1年でDXに取り組む企業の割合は増加しています。ただし、全社戦略に基づいて取り組んでいる割合は米国が68.1%に対して日本が54.2%となっており、全社横断での組織的な取組として、さらに進めていく必要があります。

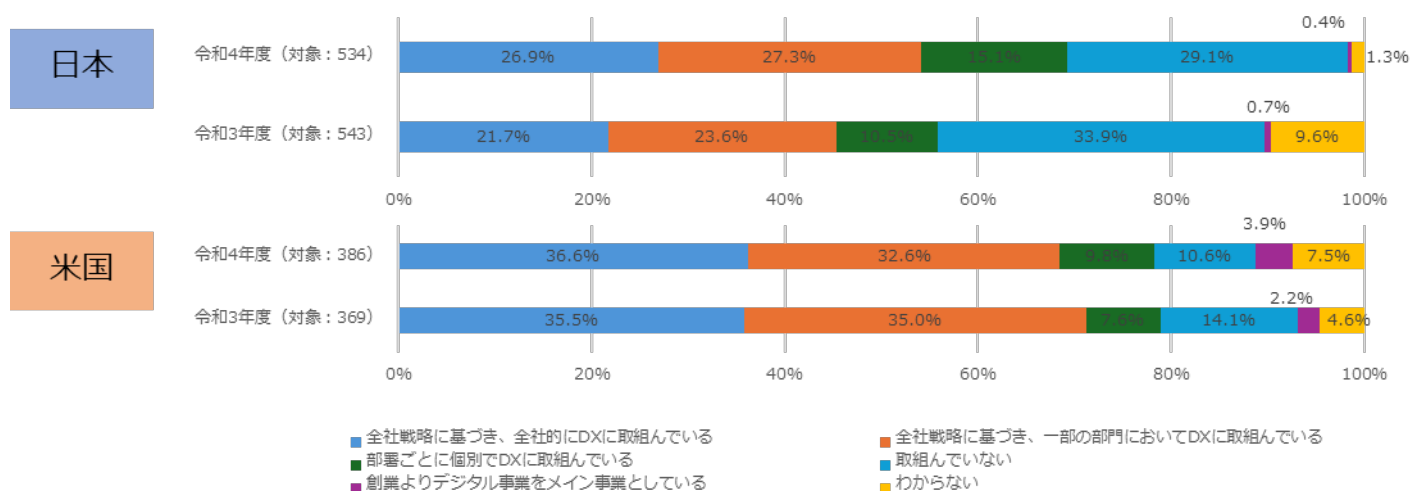


図 25. DXの取組状況

(出典) IPA「DX白書2023」をもとに作成

2. DXの取組の成果

DXの取組において、日本で「成果が出ている」の企業の割合は令和3年度調査の49.5%から令和4年度調査は58.0%に増加しました。一方、米国は89.0%が「成果が出ている」となっており、日本でDXへ取り組む企業の割合は増加しているものの、成果の創出において日米差は依然として大きいです。

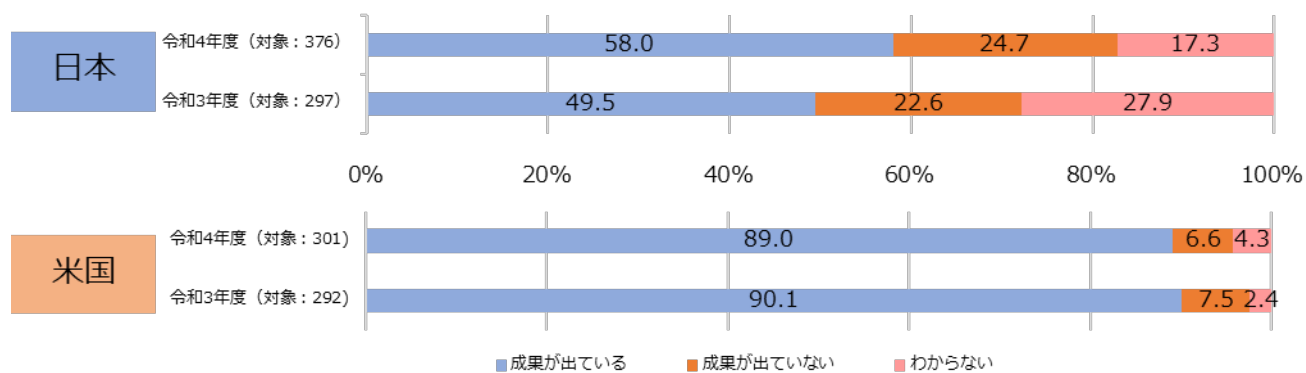


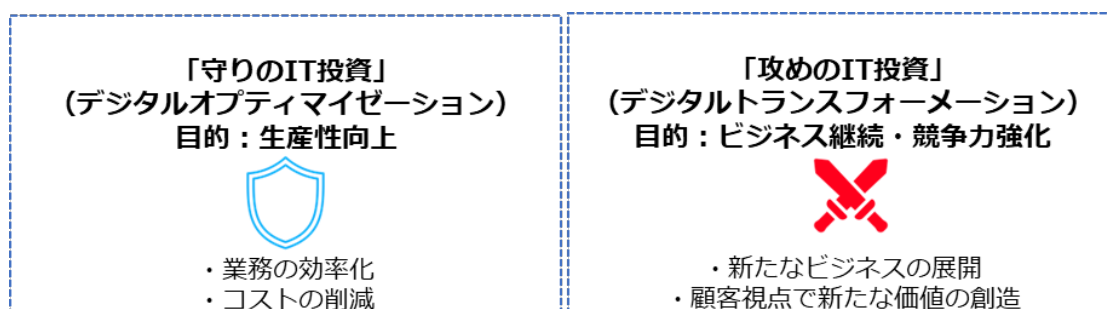
図 26. DX の取組の成果
(出典) IPA「DX 白書 2023」をもとに作成

6-2. 守りの IT 投資と攻めの IT 投資

6-2-1. 守りの IT 投資、攻めの IT 投資の概要

企業の IT 投資は、「守り」と「攻め」の 2 種類に分けて論じられることがあります。「守りの IT 投資」とは、IT による業務の効率化やコスト削減を目的としています。一方、「攻めの IT 投資」とは、IT を活用した既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規顧客獲得、収益拡大、販売力のアップを目指すことです。IT 投資に守りと攻めがあることを意識して、両者のバランスをとることが理想です。日本の企業は「守りの IT 投資」に偏っていると言われていたので、「攻めの IT 投資」に重点を置くと良いでしょう。

ここでは、「守りの IT 投資」（デジタルオプティマイゼーション）と、「攻めの IT 投資」（DX）について紹介します。次に、近年特に重要性が増している攻めの IT 投資に関して、具体的な実施手順を事例とともに説明します。最後に、近年注目されている主要なデジタル技術に対する取り組み方や活用方法を含めて紹介します。



攻めの IT 活用指針

経済産業省は、「攻めの IT 活用指針」を策定しています。この指針を活用することで、自社の現在の IT 活用状況を確認することができます。現状を把握し、これからどのような IT 投資を行っていくかを検討する際の参考になります。

STEP1 IT 導入前の状況
IT を導入していない (例) 口頭連絡、電話、帳簿での業務
STEP2 置き換えステージ
紙や口頭でのやり取りを IT に置き換え (例) 社内メール、会計処理や給与計算に IT を使用
STEP3 効率化ステージ/ 守りの IT 投資 (デジタルオプティマイゼーション)
IT を活用して社内業務を効率化 (例) 顧客・商品・サービス別の売上分析

STEP4 競争力強化ステージ/ 攻めの IT 投資 (DX)

IT を自社の売上向上などの競争力強化に積極的に活用

(例) マーケティング・販路拡大・新商品開発・ビジネスモデル構築

図 27. 攻めの IT 活用指針の概要

(出典) 経済産業省「攻めの IT 活用指針」をもとに作成

6-2-2. 経済産業省の DX レポートから見る、「攻めの IT」に取り組む方針について

2025 年の崖

「2025 年の崖」とは、経済産業省が平成 30 年に発表した「DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～」にて提示されているキーワードです。このレポートでは、令和 7 年は、基幹系システムのサポート終了に伴う維持費の増加や人材不足の深刻化などが集中する年であると予測されています。また、こうした既存の IT システムをめぐる問題を解消しない限りは、DX を本格的に展開することは困難であると指摘しています。さらに、レポートによれば、日本企業が DX を推進できなかった場合の経済的な損失は、年間最大で 12 兆円に上ると算出されています。⁹

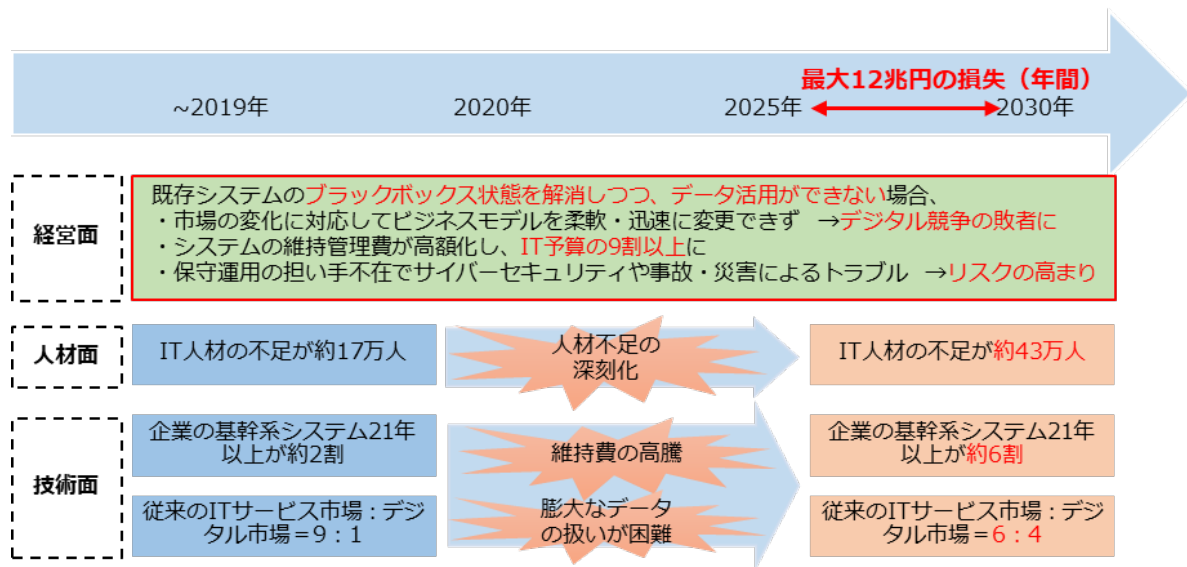


図 28. 「2025 年の崖」の概要図

(出典) 経済産業省「DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～」をもとに作成

「2025 年の崖」に陥らないための対応策

- 「見える化」指標、診断スキームの構築

⁹ 経済産業省「DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～」https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_03.pdf

- DX 推進ガイドラインの策定
- IT システムの刷新
- ユーザー企業・ベンダー企業との新しい関係性構築
- DX 人材の育成・確保

6-2-3. IT を活用した生産性の向上（デジタルオプティマイゼーション）

「守りの IT 投資」：デジタルオプティマイゼーション

現代の市場は絶えず変化し続けており、その市場の変化に迅速に対応するため、業務を変革させ、生産性を向上させることが企業にとって重要な課題となっています。生産性を向上させるためには、IT の活用が不可欠であり、「守りの IT 投資」、デジタルオプティマイゼーションがその 1 つとして注目されています。

必要な理由

業務効率化・コスト削減

デジタル技術の普及により、新たな競合他社が市場に参入し、従来のビジネスの常識が変化しています。この状況下で企業がビジネスを継続していくためには、「攻めの IT 投資」によって、製品・サービスの品質向上や新規開発、ビジネスモデルの変革などを行い、企業の競争力を維持および強化することが必要です。

デジタル活用するための環境整備

DX を実現するには、データの活用が不可欠です。これまでの業務では、表計算ソフトウェアや紙を使用していたため、データを有効に活用することが難しい状況でした。しかし、守りの IT 投資を行うことで、データを収集・利用する環境を整えることが可能です。これにより、将来的に DX を実施する際の障壁を低減することができます。

「守りの IT 投資」には、以下のようなものがあります。

- 定期的なシステム更新サイクル
- IT による業務効率化／コスト削減
- 法規制対応など

進め方

手順 1：業務内容・業務フローの可視化

現在の業務プロセスやフローを明確にし、可視化することで全体像を把握します。

手順 2：削減・短縮可能な業務の洗い出し

可視化された業務から、削減や短縮が可能な業務を特定します。

手順 3：改善や対応の実施
洗い出された業務の中から、優先度や重要度に基づいて順位づけを行い、事前に計画した改善策や対応を実施します。
手順 4：業務改革の実現
業務の効率化や品質向上を実現します。

事例：某旅館（静岡県・宿泊業・飲食サービス業）

社長が就任した平成 27 年は、観光業・宿泊業の市場規模が拡大している時期でした。その一方、人手不足や競合ホテルの増加による清掃業務の委託費高騰など、ホテル経営が厳しい状況でした。少ないコストと労力で生産性を上げるために、アウトソーシングが一般的であった清掃業務に対してデジタル技術を活用し、内製化に取り組みました。この取組によって、お客様満足度も向上しました。

手順 1：業務内容・業務フローの可視化
現在アウトソーシングしている清掃業務について、業務内容を洗い出す。
手順 2：削減・短縮可能な業務の洗い出し
洗い出した内容から以下の目標を立てる。 1.能力の見える化 2.清掃スキルの継承 3.最新状況の共有
手順 3：改善や対応の実施
誰がどのくらい働いているか、労働投入量を可視化 清掃作業がうまい人を動画にし、具体的な手順を可視化・マニュアル化 チャットツールを使って従業員同士の清掃状況の共有
手順 4：業務改革の実現
一部屋あたりの清掃時間を減らすことができ、結果として接客の質も上がり、お客様満足度の点数も上がりました。

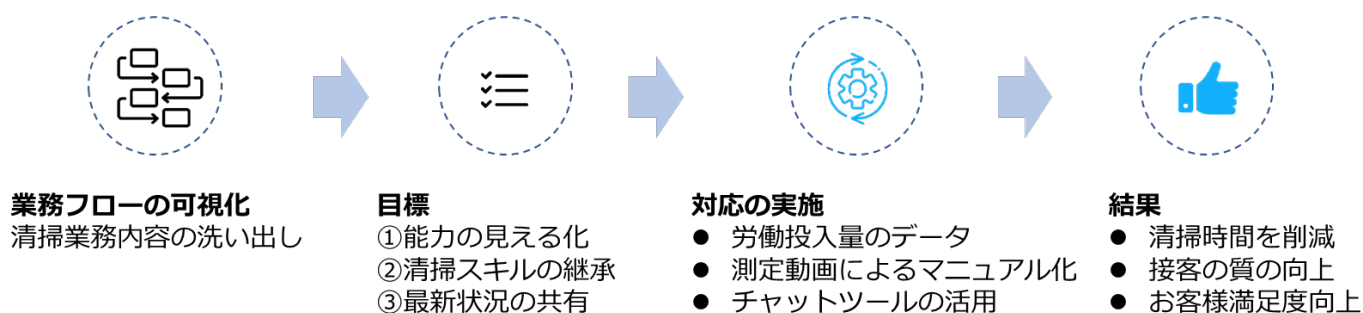


図 29. 業務改革の流れ

（出典）経済産業省「中小企業向け デジタルガバナンス・コード 実践の手引き」をもとに作成

6-2-4. IT を活用した新たなビジネスの展開（DX）

「攻めの IT 投資」：DX

業務効率化やコスト削減のためにデジタル技術やツールに投資する「守りの IT 投資」に加えて、デジタル技術を用いて、ビジネスモデルを変革したり、顧客視点で新たな価値を創出したりする DX を推進させるため、「攻めの IT 投資」を行うことが必要です。

必要な理由

ビジネス環境の急激な変化に対応するため

デジタル技術の普及により、新たな競合他社が市場に参入し、従来のビジネスの常識が変化しています。この状況下で企業がビジネスを継続していくためには、「攻めの IT 投資」によって、製品・サービスの品質向上や新規開発、ビジネスモデルの変革などを行い、企業の競争力を維持および強化することが必要です。

多様化する顧客のニーズに応えるため

デジタル時代において、顧客のニーズや期待は大きく変化しています。そのため、「攻めの IT 投資」によって DX を推進させ、顧客視点で新たな価値を創出し、顧客満足度を高めていくことが必要です。

「攻めの IT 投資」には、以下のようなものがあります。

- 新規事業の立ち上げ、事業発展
- 既存製品の品質向上・新製品やサービスの開発
- ビジネスモデルの変革など

進め方

手順 1：経営ビジョン・戦略の策定

デジタル技術によって市場や顧客のニーズがどのように変化するかを検討した上で、企業の存在意義や企業理念を再認識し、5～10 年後の中長期的な視点で顧客にどのような価値を提供していきたいのか、ビジョンを明確にします。

手順 2：変革の準備・課題の抽出

将来のビジョンと現状のギャップから、課題を抽出します。また、関係者に将来のビジョンを説明し、変革を受け入れてもらえるような意識改革を行い、全社的に取り組める体制を整えます。

手順 3：デジタル技術・業務改革による課題の解決

デジタル技術の活用や業務プロセスの見直し、企業文化の改革などにより、課題を解決していきます。

手順 4：顧客に新たな価値を提供・他社の DX に貢献

新たな価値を創出し、顧客に提供します。さらに、**サプライチェーン**全体に対しても貢献してい

きます。

詳細理解のため参考となる文献（参考文献）

中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/contents.html

事例：某ワイン製造会社（北海道・酒類製造業）

北海道でワイン製造を営む会社が DX の取り組むきっかけは、産地を細分化した高品質なワインを安定化してお客様に届け、農家にもしっかりと利益を還元したいという思いでした。従来ブドウの生産地などはアナログ作業で実施していましたが、業務をデジタル化することによってリアルタイムで管理でき、「産地細分化ワイン」を製造することが可能になりました。

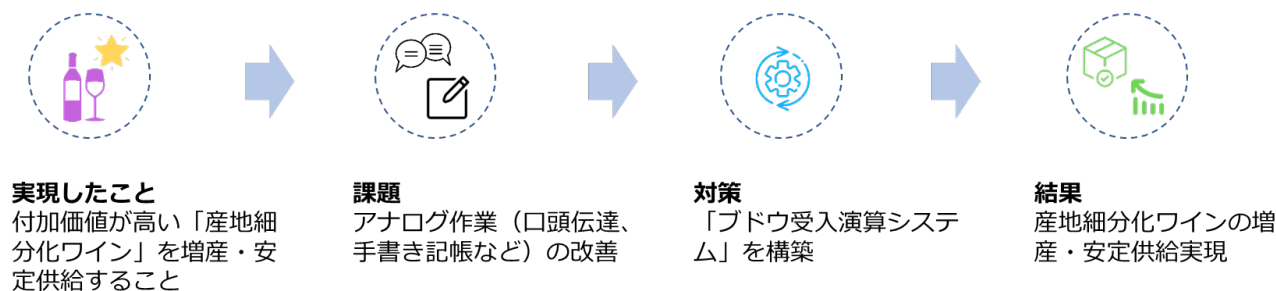


図 30. 業務改革の流れ

（出典）経済産業省「中小企業向け デジタルガバナンス・コード 実践の手引き」をもとに作成

手順 1：実現したいことを明確にする

ワインの価値を決める要素として重要な「産地」を細分化して、高品質なワインを増産・安定供給することを目指します。

手順 2：課題の明確化、関係者の意識改革を実施する

細分化を妨げている要因は、ブドウの受け入れに関わる「口頭伝達」「手書き記帳」などのアナログ作業で、PC には手書き記帳された情報から入力していました。

手順 3：デジタル技術による課題解決

外部の IT ベンダーの力を借り、計測器と専用 PC を連携させてブドウの重量データを送信するとともに、生産農家や品種をコード管理して、生産地などとリンクできるようにしました。

手順 4：顧客に新たな価値を提供・ビジネスモデルの転換

ブドウの重量・品種・産地・生産者をリアルタイムで集約管理し、特定産地のブドウを特定のタンクに貯蔵する、いわゆる「産地細分化ワイン」を製造できるようになりました。
結果、産地細分化ワインの増産・安定供給の実現につながりました。

6-2-5. 次世代技術を活用したビジネス展開

DX を推進していく際、ただ単にデジタル技術を導入すれば良いというわけではありません。自社の実現したいこと（将来のビジョン）から、実現に必要な課題を明確にし、その課題を解決するためにデジタル技術の活用が求められます。現在は、[AI](#)、[IoT](#) など新しいデジタル技術が多くあります。

以下では、主なデジタル技術を紹介します。次に、デジタル技術を活用して自社の課題を解決してもらうための参考情報として、既に DX を実践している企業の事例を紹介します。

デジタル技術は手段であり、導入自体が目的ではない



AI、IoT など最新のデジタル技術を用いて、何かできないかな？



自社の課題を解決するためには、このデジタル技術を活用する必要がある。

項目	概要	活用方法例
AI	AI は膨大な情報を処理し、判断や予測を行うことができます。	● 需要の予測や在庫の最適化 ● 不良品の自動検出 ● 対話型 AI による、問い合わせ対応の自動化（近年、学習したデータをもとに新しいコンテンツを生成できる AI の登場により、複雑な問い合わせにも対応可能）
IoT	現実世界のさまざまなモノが、インターネットとつながることで、収集したデータが、インターネットに送信・蓄積され、データを分析・活用することで、新たな価値の創出につながります。	● 生産設備にセンサーを設置し、振動データを取得し分析することで、部品の故障予知や性能維持が可能 ● 生産設備の稼働状況を可視化したことで、すべての拠点での生産状況をリアルタイムに把握可能
クラウドサービス	自社で機器やシステムを保有しなくても、インターネット経由で、さまざまなサービスを利用できます。	● 社内情報の一元管理、情報共有の利便性向上 ● システムを開発・実行するためのツールや環境構築の作業の省略 ● 場所やデバイスに依存せずに作業の継続ができ、リモートワーカーや複数拠点のチームとの協業が可能

実際にデジタル技術を活用して課題解決、競争力の強化を実践していく際の参考として、既に DX を実践している企業が、どのようにデジタル技術を活用して自社の課題を解決し、競争力を強化しているのか紹介します。

事例 1：不動産売買・仲介・賃貸業（東京都・不動産業）

取組のきっかけ	自社 MISSION を追求すべく、継続に成長できる企業へ邁進していくために、DX によるデジタル技術と活用が急務、かつ必須ととらえたため。
解決への取組	ノーコードツールや RPA を導入するにあたり、情報システム担当者に加えて、各部署 1 名程度エバンジェリスト※を選出し、現場と情報システム部による共創の形をとりました。社長自ら率先して DX の重要性について語ることに加え、社内ブログやコーポレートサイトなどを利用して、広く周知することで、全社として DX に取り組んでいることの本気度を社内外へ示しました。 DX の取り組んだ成果として独自アプリの開発ならびに IoT 技術との連携など、顧客サポートの活性化を推進、また、ノーコードツールならびに RPA を活用し、グループ全体の業務効率化によって年間 8,800 時間の工数削減を実現しました。 ※エバンジェリスト：公益性や中立性を重視して新しいトレンドや技術の啓蒙活動を行う。

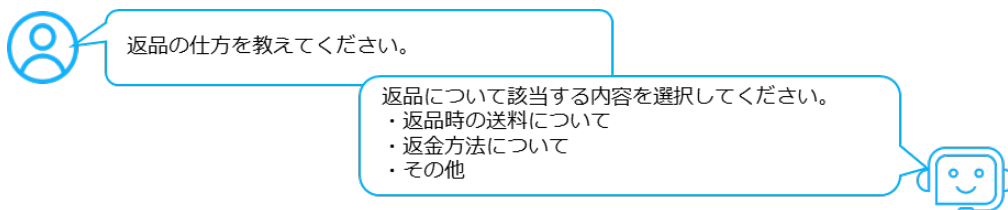
（出典） 経済産業省 「DX Selection 2024」をもとに作成

事例 2：観光客向け飲食、販売業（三重県・飲食・サービス業）

取組のきっかけ	人員不足や独自性の欠如などから、事業縮小が検討されていた。そろばんや手切り食券など効率が悪く、人手不足も問題であった。
解決への取組	現状のままを好む従業員が多くいるため、DX を推進するのは従業員の反対もありました。従業員だけではなく、経営層から自らデジタルを利用し、トップダウン方式で全従業員に浸透させました。年齢層の高い現場スタッフには、抵抗なくデジタルやデータ活用を身近なものにするため、きめ細かいサポートを行いました。 DX 担当者は IT の知識があったわけではなかったもので、勤務時間をすべて勉強に充てて教育しました。他の従業員にも IT や DX に興味があればジョブチェンジを推奨し、ゼロの知識からでもプロの IT 担当へ教育しました。 DX を取り組んだ成果として、自社開発の来客予測・店舗分析システムを用いて、マーケティングなどに活用することで、売上を導入前から 8.5 倍まで伸びました。これから、さらなる発展が見込まれる生成 AI を用いることで、より効率的な経営や運営に取り組んでいます。

チャットボット

チャットボットとは自動会話プログラムのことです。自動で発信・返答を行うプログラムであるチャットボットは、事前に設定したルール、選択肢などに基づいて、文字形式で利用者とコミュニケーションをとることができます。例えば、よくある質問などを設定しておくことで、お問い合わせ対応を自動で行うことができます。そしてチャットボットでは対応できない内容のみオペレータに対応させることで、人的費用を削減することができます。



予想・今後の発展

近年、AIを搭載したチャットボットが登場しています。これまでのチャットボットとは異なり、蓄積されたデータを学習するため、決められた内容や選択肢に限定されず他の質問にも対応できたり、ユーザーからの質問に表現の揺らぎがあった場合でも、一定程度対応できたり、さらには複雑な質問にも回答できるようになっています。

生成 AI の登場

生成 AI とは、さまざまなコンテンツを生成することができる AI のことです。従来の AI が主にデータを分析・学習し、その結果に基づいて予測を行うのに対して、生成 AI は新たなコンテンツの創造を目的として学習します。生成 AI は学習量が多いため、回答の精度や質が従来のものより高く、またコンテンツの生成速度も非常に速いという特徴があります。従来のチャットボットは主にオペレータ業務のサポートなど、お問い合わせ対応に限定されていましたが、生成 AI では以下のような活用ができることが期待されています。

生成AIの活用事例

文章生成



商品やサービスの広告文を作成する際に、商品の特徴やターゲット顧客の特性などを入力するだけで、瞬時に文章を生成することができます。

レポート作成



大量のデータを分析し、要約やレポートを自動的に生成することができます。これにより、データの処理時間を短縮し、意思決定に役立つ情報を迅速に提供することができます。

製品開発と設計



顧客ニーズや市場のトレンド、予算、顧客の意見などの情報を分析させることにより、新製品やサービスのアイデアを効率的に提案することが期待されています。

(出典) 経済産業省「DX Selection 2024」をもとに作成

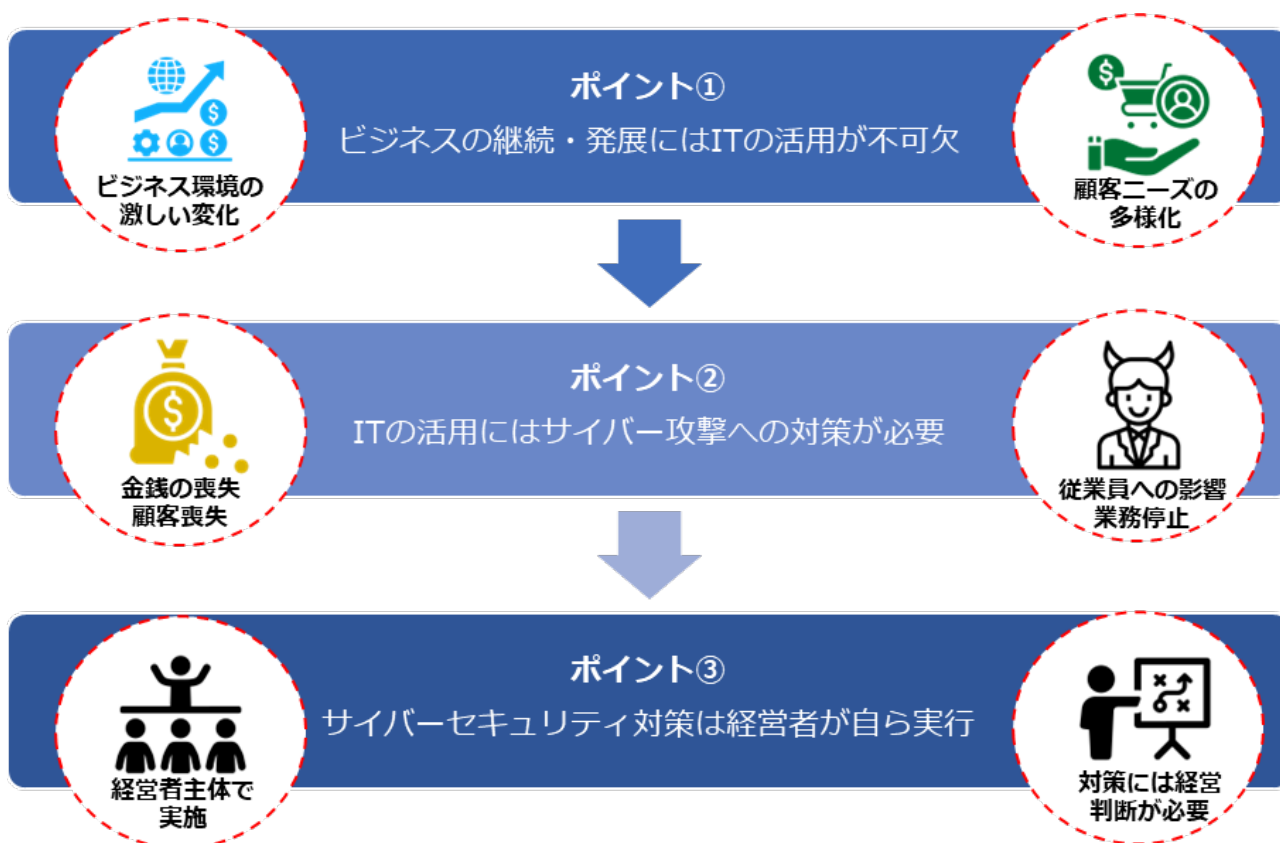
6-3. 経営投資としてのサイバーセキュリティ対策

6-3-1. サイバーセキュリティ対策の重要性

DXを推進していく際に、並行してサイバーセキュリティの確保に取り組むことが重要です。変化の激しい現代社会でビジネスを継続していくためには、従来のITを活用して業務効率化や生産を向上させることに加えて、データやデジタル技術を活用して、顧客視点で新たな価値を創出する、DXを推進していくことが求められています。しかし、データやデジタル技術を活用する際に、セキュリティ対策を行わなければ、サイバー攻撃の標的となり、経営を揺るがすような被害に遭う可能性があります。このような被害を受けないためにも、DXの推進と並行してサイバーセキュリティの確保に取り組むことが重要です。

セキュリティ対策を行うことで、リスクを経営上許容可能な範囲までに減少させることができます。また、セキュリティ対策には経営判断が必要になるため、経営者が主体となって指揮をすることが大切になります。

次のページから、経営者目線でセキュリティ対策を行わなければならない理由を以下のポイントごとに説明していきます。



6-3-2. 経営者が重要視すべき 3 つのポイント

図 31. IT の活用とサイバーセキュリティ対策の関係性

(出典) 東京都産業労働局.“MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響”.

<https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html>

ポイント 1 : ビジネスの継続・発展には IT の活用が不可欠

中小企業にとって、業務や生産の効率化、人材確保は重要な課題です。業務・生産工程などの運用コストの削減・効率化のために、IT の活用が不可欠になっています。また近年では、競争力維持・強化のために、DX を進めることが求められており、IT の活用が必須になっています。

中小企業の課題



ポイント 2 : IT の活用にはサイバー攻撃への対策が必要

図 32. 情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律

(出典) IPA「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」から抜粋

事例：サプライチェーン攻撃による情報流出被害



保険業界

某保険会社は、顧客情報の一部が流出したことを公表し、謝罪しました。情報流出の原因としては、外部委託先の企業のサーバが不正アクセスを受けたことです。顧客の氏名、性別、生年月日、メールアドレスなどの個人情報が数十万人分漏えいしてしまいました。その結果、数億円以上の損害や多くのお客様に対する信頼を低下させてしまう事態となりました。このようにサプライチェーンを介した攻撃では、自社が直接サイバー攻撃を受けていなくても、間接的に被害にあってしまいます。

ポイント3：サイバーセキュリティ対策は経営者が自ら実行

経営者は自ら主体となって指揮をとり、セキュリティ対策を行う必要があります。理由は、主に2つあります。1つ目は、セキュリティ対策を行うにあたり、サイバー攻撃のリスクの許容範囲をどの程度にするのか、セキュリティ投資をどこまで行うのかなど、経営者による経営判断が必要になるからです。2つ目は、セキュリティインシデントが発生した際に、経営者が「法的責任」や「社会的責任」を負わなければならないからです。経営者は民法や会社法により、善管注意義務という「取締役として期待される水準の注意をもって業務を行う義務」を負い、その任務を怠った際に生じた損害を株式会社に対して賠償する責任「任務懈怠」を負うことが規定されています。そのため、セキュリティ対策にベストを尽くさなかった結果、サイバー攻撃による情報漏えいや事業停止が起き、第三者に損害が生じた場合、善管注意義務違反や任務懈怠に基づく損害賠償責任を問われてしまいます。

法令	条項	要約
民法	第 415 条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、会社および第三者に対する、契約違反による賠償義務を負う。
	第 644 条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
	第 562 条 契約不適合責任	請負契約の仕事の目的物（開発システムなど）について、その種類や品質が契約内容に適合しないことが仕事の完成後に判明した場合、会社および第三者に対する契約不適合となる。
	第 709 条 不法行為による損害賠償	故意又は過失によって他人の権利又は法律上

	第 715 条 使用者等の責任	保護される利益を侵害した者は、これによって生じた損害を賠償する義務を負う。
会社法	第 330 条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償責任を負う。
	第 423 条第 1 項 任務懈怠による損害賠償責任	
	第 429 条第 1 項 第三者に対する注意義務違反	

会社法の第三者責任や民法の不法行為責任が認められると、経営者が個人として損害賠償責任を負う場合もあります。このほかにも、法律によっては違反などが発生した場合、経営者に加えて、取締役、担当者に対しても刑罰が科せられることもあります。上記の事態を引き起こさないためにも、セキュリティ対策は経営者が主体となって取り組むことが大切です。

編集後記

第2編では、大きく2つの事項について紹介しました。1つ目は、実際のインシデント事例を通して、近年のサイバー攻撃の傾向や対策などを紹介しました。2つ目は、企業経営で重要なIT投資などについて紹介しました。

サイバー攻撃の中でもランサムウェアやサプライチェーン攻撃は特に深刻な問題となっています。これらの攻撃は企業に対する業務的な影響に加えて、取引先からの信用を損なう社会的な影響も及ぼすことに注意が必要です。近年の攻撃は企業の規模に関係なく行われており、セキュリティ対策の重要性を改めて認識していただきたいと思います。

IT投資は、「守りのIT投資」（デジタルオペティマイゼーション）と、「攻めのIT投資」（DX）があります。ビジネス環境の急激な変化に対応するため「攻めのIT投資」に重点を置き、既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことが大切です。

データやデジタル技術を活用したDXの推進には、十分なセキュリティ対策が必要です。セキュリティ対策が不十分であると、サイバー攻撃の標的となり、経営に大きな被害をもたらす恐れがあるためです。DXの推進と並行してサイバーセキュリティの確保に取り組むことが重要です。

第7章. セキュリティ対策の概要（全容）

章の目的

第 7 章では、ISMS 認証を前提としたセキュリティ対策における基準を 3 段階にレベル分けし、各基準の手法について理解することを目的とします。

主な達成目標

- セキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること
- 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

7-1. 対策基準の策定

7-1-1. セキュリティ対策のレベル

情報セキュリティポリシーは、一般的に「基本方針」「対策基準」「実施手順・運用規則など」で構成されます。「基本方針」には、組織や企業の代表者の情報セキュリティに対する考え、必要性、取扱い方針などの宣言が含まれます。「対策基準」には、各業務や部署におけるセキュリティ対策をまとめた規程を記載します。「実施手順」には、対策基準ごとに内容を具体的な手順として記載します。

以下では、「対策基準」策定方法の考え方について説明します。

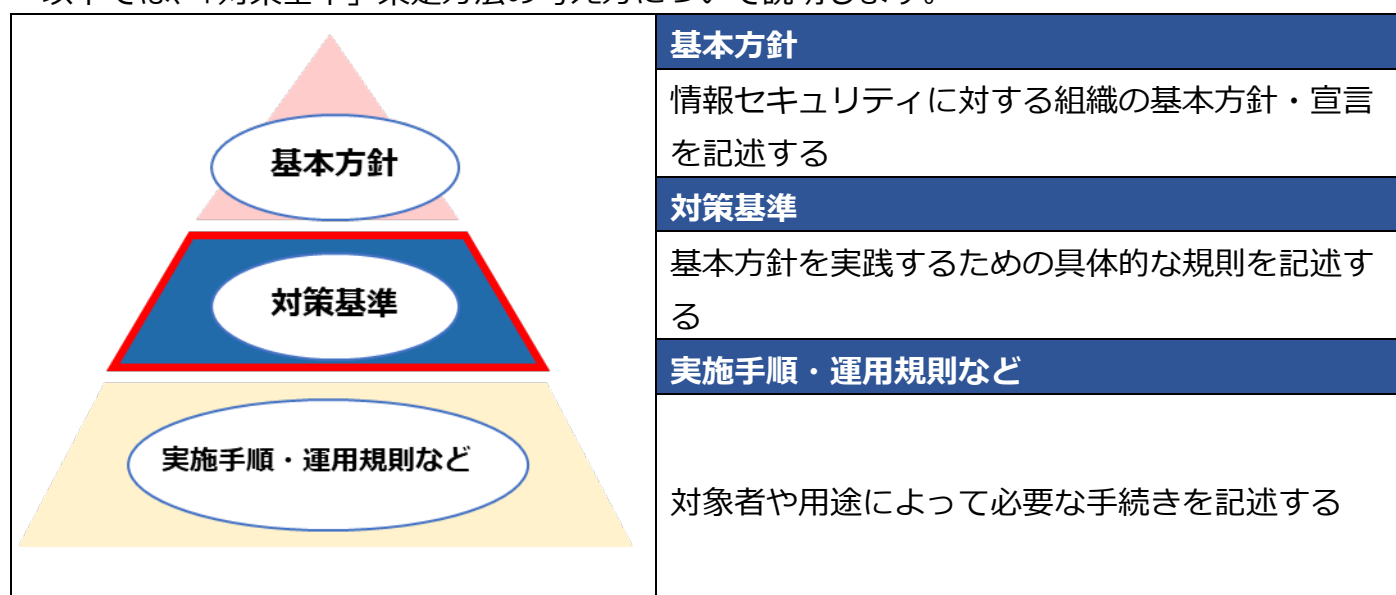


図 33. セキュリティ対策の関係図

(出典) 総務省, “情報セキュリティポリシーの順守”, https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/12/

対策基準外部に公開することにより、セキュリティ対策の実施を内外に示し、説明責任を果たすことができます。ただし、対策基準で記載する内容は抽象度が高いため、具体的に実践で使用することは難しい内容です。実際に運用を行うためには、策定した対策基準に従って、実施手順などを作成する必要があります。

対策基準の内容を定める際は、網羅的なフレームワークを参考にすることが推奨されます。企業の現状、目標に応じてフレームワークを使用せずに段階的な対策基準の策定を行う場合は、「2-3. サイバーセキュリティアプローチ方法の概要」記載のアプローチ方法を参考にすることができます。アプローチ方法はレベルが上がるにつれ、網羅性も上がります。それぞれの特徴を次ページで説明します。

対策基準を策定するためのアプローチ方法



Lv.1
クイックアプローチ
(インシデントベース)



Lv.2
ベースラインアプローチ
(ガイドライン・ひな形ベース)



Lv.3
網羅的アプローチ
(フレームワークベース)

7-1-2. セキュリティ対策のアプローチ方法

Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチの概要、主な特徴と想定される適用ケースを説明します。

アプローチ手法	特徴	想定される適用ケース
Lv.1 クイックアプローチ	即時の対応や緊急事態への対処に適したアプローチ手法。低コスト、短期間で実施可能。包括的ではないが即効性がある。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対して暫定的対策を行う場合。
Lv.2 ベースラインアプローチ	組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。 ガイドラインやひな型を参考とし、対策基準を策定。 規制遵守の観点から一定の安全性が確保できる。 コストパフォーマンスがよい。	組織的に一定以上の対策基準を策定する場合。 包括的な対策は過剰で、基本的な水準の対策が適切だと判断される場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的なセキュリティ対策を講じることを目指すアプローチ手法。 ISMS 認証取得が可能なレベルを目指して、対策基準を策定。	ISMS の <u>フレームワーク</u> に沿った対策基準を策定する場合。 情報システムが重要な組織や <u>機密性</u> の高い情報を扱う組織など、高い水準の情報セキュリティが求められる

	コストが高くなる可能性があるが、組織のニーズに合わせた最適な対策が可能。	場合。

メリット・デメリット

アプローチ手法	メリット	デメリット
Lv.1 クイックアプローチ	● 小規模なセキュリティ対策や修正を迅速に実施可能。 ● 低コストでリスクを軽減でき、コストパフォーマンスがよい。 ● 流行中の攻撃の拡大や影響を最小限に抑えられる。 ● リソースが限られていても実施可能。	● 包括的でないため、抜けが発生する可能性がある。 ● 一時的な対策になりがちで、抜本的な対策にならない。 ● 長期的にみると費用が嵩んでしまう場合がある。
Lv.2 ベースラインアプローチ	● 組織全体で一貫性を確保できる。 ● 最低基準となるセキュリティ対策を講じることができる。 ● ある程度の対策効果が見込め、コストパフォーマンスがよい。	● 最低基準を満たすだけなので、十分なセキュリティ水準が確保できない可能性がある。 ● 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
Lv.3 網羅的アプローチ	● 組織のニーズに合わせた最適な対策が可能。 ● リスクを徹底的に特定・分析できるので、高度なセキュリティ水準が実現できる。 ● 長期的な視点で PDCA サイクルを回せる。 ● 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持できる。	● コスト（特に初期コスト）が高額になってしまふことが多い。 ● リスク分析や対策の詳細設計に時間を要し、全体的なセキュリティ対策の実施が遅くなってしまう。

Lv.1 クイックアプローチ

Lv.1 クイックアプローチでは、さまざまなインシデント事例内容を参考にします。インシデント事例は、報道される事例、情報セキュリティ 10 大脅威、実際のインシデントなどから選択します。自社で発生する可能性が高いと考えられるインシデント事例や、実際に発生したときの被害が大きいと考えられるインシデント事例を参考にして、対策基準を策定することが重要です。以下は、情報セキュリティ 10 大脅威の『組織』に対する脅威で 3 年連続第 1 位になっている、ランサムウェアに対する対策基準の例です。

ランサムウェアに 対する対策基準

対策基準（例）

1. 対象とする脅威
 - ランサムウェアによる情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取など
2. 組織的対策
 - ランサムウェア対応のためにセキュリティ管理体制を確立する
 - インシデント対応のためにセキュリティ管理体制を整備する
3. 人的対策
 - メールの添付ファイル開封や、メールや SMS のリンク、URL のクリックを安易にしない
 - 提供元が不明なソフトウェアを実行しない
 - 適切な報告/連絡/相談を行う
4. 物理的対策
 - 適切なバックアップ運用を行う
5. 技術的対策
 - 公開サーバへの不正アクセス対策
 - 共有サーバなどへのアクセス権の最小化と管理の強化
 - 多要素認証の設定を有効にする
 - サーバやクライアント、ネットワークに適切なセキュリティ対策を行う

詳細理解のため参考となる文献（参考文献）

情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
マルウェア「ランサムウェア」の脅威と対策（対策編）	https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

Lv.2 ベースラインアプローチ

Lv.2 ベースラインアプローチでは、ガイドラインやひな型を参考とし、対策基準を策定します。IPA の「中小企業の情報セキュリティ対策ガイドライン」や以下の【参照資料】を活用することにより、自社にあった対策基準を策定することができます。

【参照資料】

- ・リスク分析シート（出典：IPA）
- ・中小企業の情報セキュリティ対策ガイドライン第 3.1 版（出典：IPA）
- ・情報セキュリティ関連規程（出典：IPA）
- ・自己点検チェックリスト（出典：[個人情報保護委員会](#)）

IPA「情報セキュリティ関連規程（サンプル）」
を活用した対策基準（例）

1	組織的対策	改訂	20yy.mm.dd
適用範囲	全社・全従業員		

1.情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。

詳細理解のため参考となる文献（参考文献）	
リスク分析シート	https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx
中小企業の情報セキュリティ対策ガイドライン第 3.1 版	https://www.ipa.go.jp/security/guide/sme/about.html
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

Lv.3 網羅的アプローチ

Lv.3 網羅的アプローチでは、ISMS 認証取得が可能なレベルを目指して、対策基準を策定します。そのため、ISMS のフレームワークに沿って、技術的対策といった一部の内容ではなく、運用や監査についても対策基準に記載します。

ISMSフレームワークを活用した
対策基準（例）

情報セキュリティ対策基準

93種の管理策ごとに 対策基準を策定

1. 目的
2. 適用範囲
3. 用語の定義
4. 組織的対策
5. 物理的対策
6. 人的対策
7. 技術的対策

93種の管理策を活用（ISMSフレームワーク）
（情報セキュリティマネジメントの確立・運用・監査を含んだ網羅的な管理策）

5.1 組織的対策	5.24 情報セキュリティインシデント監視の仕組みおよび手順
5.2 情報セキュリティの目的および方針	5.25 情報セキュリティ施策の計画および実施
5.3 情報セキュリティの組織および責任	5.26 情報セキュリティインシデントへの対応
5.4 経営者の役割	5.27 情報セキュリティインシデントからの学習
5.5 関係者との連携	5.28 経営者の役割
5.6 専門知識との連携	5.29 事業の中核、経営目的を達成するセキュリティ
5.7 権限管理システム	5.30 事業継続のためのITの確保
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.31 法令、規格および契約上の要求事項
5.9 情報およびその他の資産の保護責任の分担	5.32 契約の管理
5.10 情報およびその他の資産の保護責任の分担	5.33 記録の管理
5.11 資産の分類	5.34 プライバシーおよびITの保護
5.12 情報の分類	5.35 情報セキュリティの向上に資する
5.13 情報の分類	5.36 情報セキュリティのための方針策定、計画および実施の計画
5.14 情報伝送	5.37 運用手続
5.15 アクセス管理	6. 人的対策
5.16 情報資産の管理	6.1 教育
5.17 記録管理	7. 物理的対策
5.18 アクセス権	7.1 物理的セキュリティ確保
5.19 物理環境における情報セキュリティ	7.2 物理的入退
5.20 物理環境における情報セキュリティ	7.3 オフィス、設備および機器のセキュリティ
5.21 物理環境における情報セキュリティ	7.4 物理的セキュリティの確保
5.22 物理環境のカーネルレベルの脆弱性および脆弱性	7.5 物理的および環境的脆弱性からの保護
5.23 クラウドサービス利用における情報セキュリティ	7.6 セキュリティを伴った情報域での作業
	7.7 カラグラフィック・グラフィックス
	7.8 装置の設置および保護
	7.9 機密性のある装置および機器のセキュリティ
	7.10 記録管理
	7.11 ネットワークセキュリティ
	7.12 ネットワークの接続
	7.13 ネットワークの接続
	7.14 ネットワークの接続
	7.15 ネットワークの接続
	7.16 ネットワークの接続
	7.17 ネットワークの接続
	7.18 ネットワークの接続
	7.19 ネットワークの接続
	7.20 ネットワークの接続
	7.21 ネットワークの接続
	7.22 ネットワークの接続
	7.23 ネットワークの接続
	7.24 ネットワークの接続
	7.25 ネットワークの接続
	7.26 ネットワークの接続
	7.27 ネットワークの接続
	7.28 ネットワークの接続
	7.29 ネットワークの接続
	7.30 ネットワークの接続
	7.31 ネットワークの接続
	7.32 ネットワークの接続
	7.33 ネットワークの接続
	7.34 ネットワークの接続
	7.35 ネットワークの接続
	7.36 ネットワークの接続
	7.37 ネットワークの接続
	7.38 ネットワークの接続
	7.39 ネットワークの接続
	7.40 ネットワークの接続
	7.41 ネットワークの接続
	7.42 ネットワークの接続
	7.43 ネットワークの接続
	7.44 ネットワークの接続
	7.45 ネットワークの接続
	7.46 ネットワークの接続
	7.47 ネットワークの接続
	7.48 ネットワークの接続
	7.49 ネットワークの接続
	7.50 ネットワークの接続
	7.51 ネットワークの接続
	7.52 ネットワークの接続
	7.53 ネットワークの接続
	7.54 ネットワークの接続
	7.55 ネットワークの接続
	7.56 ネットワークの接続
	7.57 ネットワークの接続
	7.58 ネットワークの接続
	7.59 ネットワークの接続
	7.60 ネットワークの接続
	7.61 ネットワークの接続
	7.62 ネットワークの接続
	7.63 ネットワークの接続
	7.64 ネットワークの接続
	7.65 ネットワークの接続
	7.66 ネットワークの接続
	7.67 ネットワークの接続
	7.68 ネットワークの接続
	7.69 ネットワークの接続
	7.70 ネットワークの接続
	7.71 ネットワークの接続
	7.72 ネットワークの接続
	7.73 ネットワークの接続
	7.74 ネットワークの接続
	7.75 ネットワークの接続
	7.76 ネットワークの接続
	7.77 ネットワークの接続
	7.78 ネットワークの接続
	7.79 ネットワークの接続
	7.80 ネットワークの接続
	7.81 ネットワークの接続
	7.82 ネットワークの接続
	7.83 ネットワークの接続
	7.84 ネットワークの接続
	7.85 ネットワークの接続
	7.86 ネットワークの接続
	7.87 ネットワークの接続
	7.88 ネットワークの接続
	7.89 ネットワークの接続
	7.90 ネットワークの接続
	7.91 ネットワークの接続
	7.92 ネットワークの接続
	7.93 ネットワークの接続
	7.94 ネットワークの接続
	7.95 ネットワークの接続
	7.96 ネットワークの接続
	7.97 ネットワークの接続
	7.98 ネットワークの接続
	7.99 ネットワークの接続
	7.100 ネットワークの接続

詳細理解のため参考となる文献（参考文献）

情報セキュリティポリシーサンプル改訂版（1.0 版）

<https://www.jnsa.org/result/2016/policy>

第8章. 用語定義および関係性と識別方法

章の目的

第 8 章では、ISO/IEC 27000 に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を理解することを目的とします。

主な達成目標

- ISMS の管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

8-1. 用語の定義、脅威・脆弱性の識別

8-1-1. 用語の定義と関係性

企業や組織にはさまざまなセキュリティ上のリスクが存在しています。これらのリスクを効率的に管理するには、リスクマネジメントを行う必要があります。

リスクマネジメントを理解するために必要となる「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を説明します。次に、リスクを増大させる要因となる「脅威」や「脆弱性」の識別方法を説明します。

主な用語の定義	
脅威	システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。例えば、コンピュータウイルスなどのマルウェア、不正アクセス、DDoS 攻撃、窃盗や破壊行為などの犯罪のような意図的な人為的脅威、機器の故障や操作ミスのような偶発的な人為的脅威、地震や洪水のような環境的脅威がある。
脆弱性	1 つ以上の脅威によって付け込まれる可能性のある、情報システムやネットワーク、アプリケーション、セーフガード（管理策）、施設・設備などに存在する欠陥や弱点。例えば、セキュリティホールと呼ばれるソフトウェアの欠陥・不具合。
インシデント	事故・出来事のこと。セキュリティでは、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象。コンピュータウイルスの感染、不正アクセスの発生、システム障害やネットワーク障害、情報システム関連の内部不正行為、災害や事故によるデータ・設備の損失など。
資産	組織にとって価値があるもの。
情報資産の重要度	機密性・完全性・可用性が損なわれた場合の事業に対する影響や、法律で安全管理義務があるなどの観点から、情報資産の重要度を判断する。
セーフガード（管理策）	脅威から情報資産を守るための対策や管理的・技術的手段。施設の入退室管理、監視カメラの設置、防犯装置の導入などの物理的な対策、ファイアウォール、アンチウイルスソフト、アクセス制御、暗号化、バックアップなどの技術的対策、情報セキュリティポリシーの策定、教育訓練の実施、インシデント対応手順の整備、監査の実施、担当者の資格管理、従業員教育、守

秘義務の徹底などの管理的対策がある。

リスク

目的に対する不確かさの影響。情報セキュリティにおいては、脅威が組織に損害を与える可能性と損害の度合い。

残留リスク

さまざまな対策（セーフガード）を講じた後に残るリスク。残存リスクともいう。

リスク値

リスクの大きさのこと。「情報資産の重要度（あるいはリスクが顕在化したときの被害の大きさ）」と「機密性・完全性・可用性を損なう事象の発生確率」の積で求められる。高、中、低のような段階評価を用いる場合と定量的に計算する場合がある。

脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係をわかりやすく図で表すと以下ようになります。

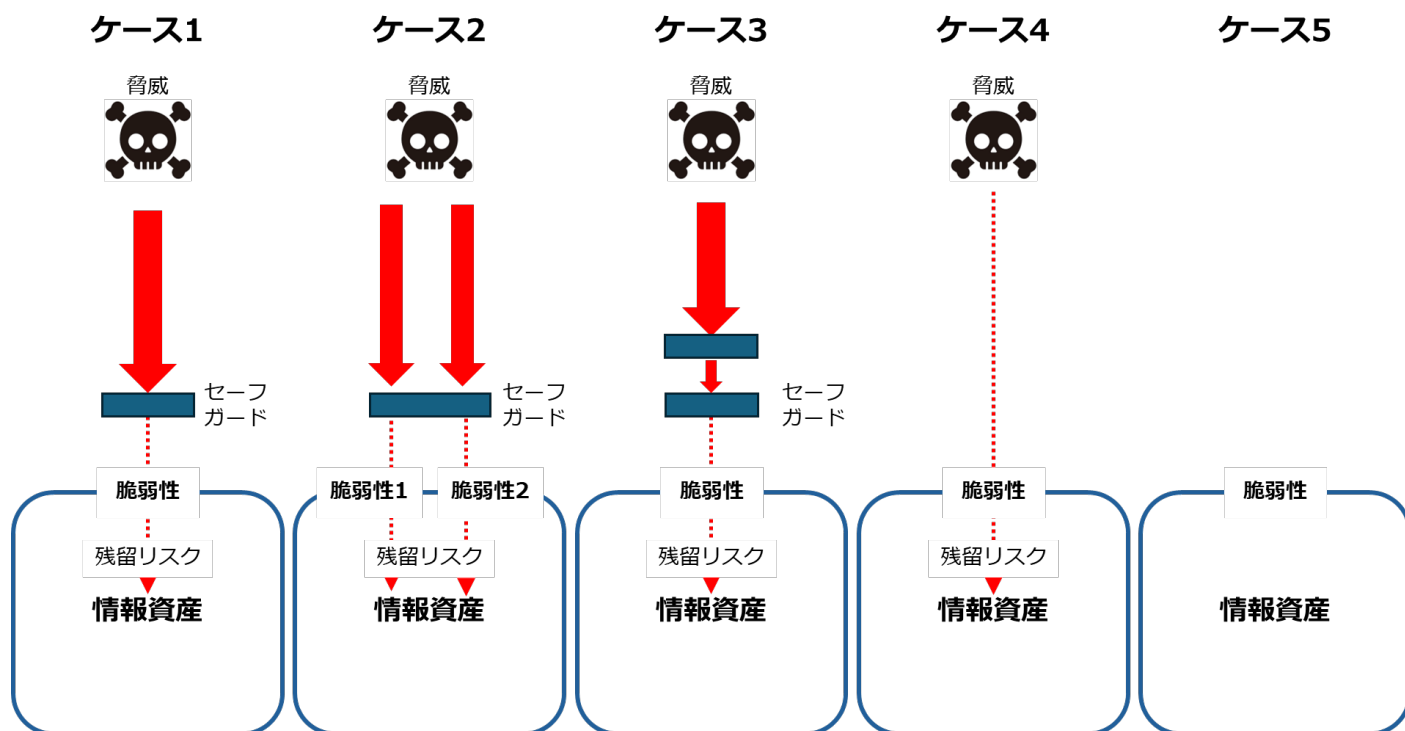


図 34.脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

（出典）「ISO/IEC TR 13335-1」をもとに作成

ケース	図の説明	脅威	脆弱性	セーフガード （管理策）	リスク
ケース 1	1つのセーフガードが、リスクを低減することに効果的と見られる場合	あり	あり	あり	低減
	脆弱性に対応する脅威がありますが、セーフガードがある（セキュリティ対策がなさ				

	れている) ので、リスクは残留リスクまで低減されています。				
ケース 2	1つのセーフガードが、複数の脆弱性を悪用する脅威と関連するリスクを低減することに効果的と見られる場合	あり	あり (複数)	あり	低減
	複数の脆弱性があり、それを悪用する可能性のある脅威がありますが、1つのセーフガード(セキュリティ対策)によってリスクを残留リスクまで低減できるケースです。				
ケース 3	複数のセーフガードの組み合わせが、リスクの低減に有効な場合	あり	あり	あり(多段)	低減
	脆弱性に対応する脅威がありますが、その脅威に対応する複数のセーフガードがあり(複数のセキュリティ対策がなされており) リスクは残留リスクまで低減されているケースです。一般的に、リスクを受容可能なレベルに低減するために、多数のセーフガードが必要になるケースは珍しくありません。				
ケース 4	脆弱性を悪用する可能性がある脅威があるが、そのリスクが受容可能とみなされる場合	あり	あり	あり	受容
	リスクが受容可能なレベル以下であるため、セーフガード(セキュリティ対策)の必要がありません。				
ケース 5	脆弱性に対応する既知の脅威がない場合	なし	あり	あり	不明
	資産をとりまく情報システムなどの環境には脆弱性がありますが、それに対応する既知の脅威がないので、セーフガード(セキュリティ対策)の必要がないケースです(そもそもリスクもないことになります)。				

(例) 業務用ノートパソコン

業務用ノートパソコンに関する脅威や脆弱性、管理策の関係について説明します。

資産	ノートパソコン内の情報
価値	営業業務で必須の情報
脅威	社外持ち出しによるノートパソコンの紛失
リスク	盗難による情報漏えい
脆弱性	不適切なパスワードの設定 (例) わかりやすいパスワード：名前、従業員番号、生年月日など
保護要求事項	● 権限のないものがログインできないようにする ● 不要な持ち出しを防ぐ
管理策	● 複雑なパスワードの設定 (8.5 セキュリティを保った認証) ● 社外の持ち出し管理 (7.9 構外にある装置及び資産のセキュリティ (構外にある資産))

下記の図では「脅威」「脆弱性」「資産の価値」のいずれかが増加することにより、リスクが増大することが示されています。リスクを減少させるためには、まず「脅威」「脆弱性」「資産の価値」を識別し、リスクに対する保護要求事項を明らかにします。そして、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要です。

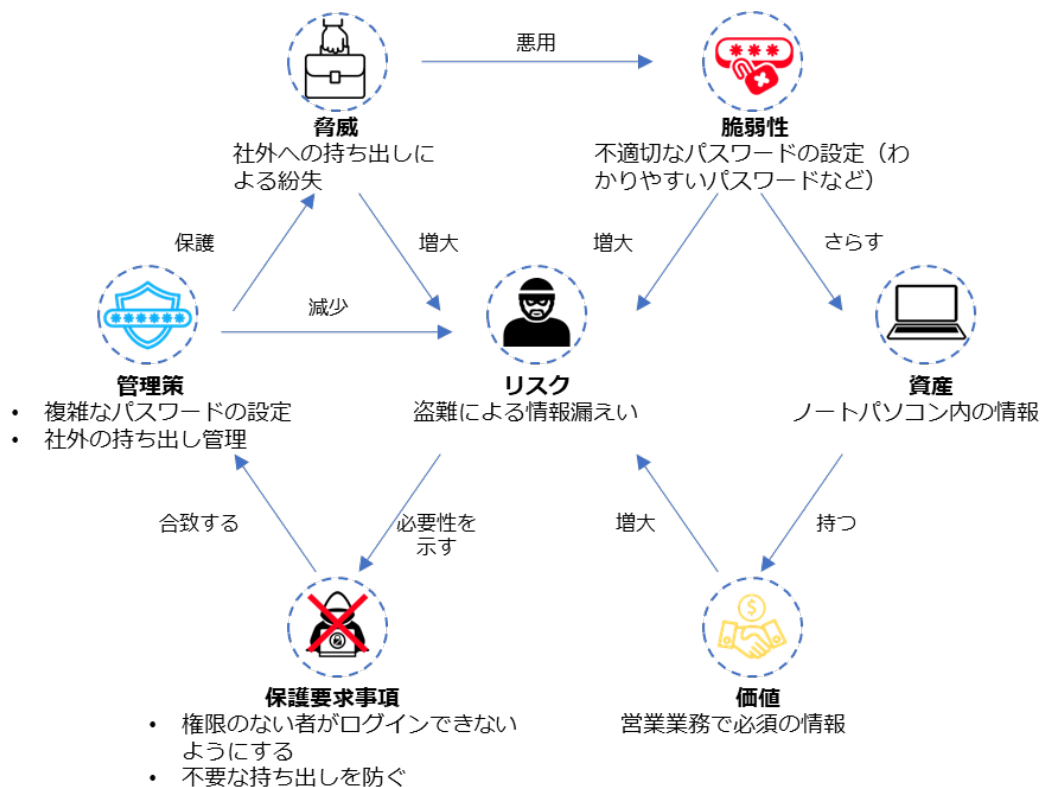


図 35. 脆弱性、リスクの関係の事例

8-1-2. 脅威の識別

脅威は「脆弱性」に付け入り顕在化することにより、組織に損失や損害を与える事故を生じさせます。脅威を、人為的脅威（意図的脅威、偶発的脅威）と環境的脅威に区別して把握することにより、必要なセキュリティ対策を整理しやすくなります。

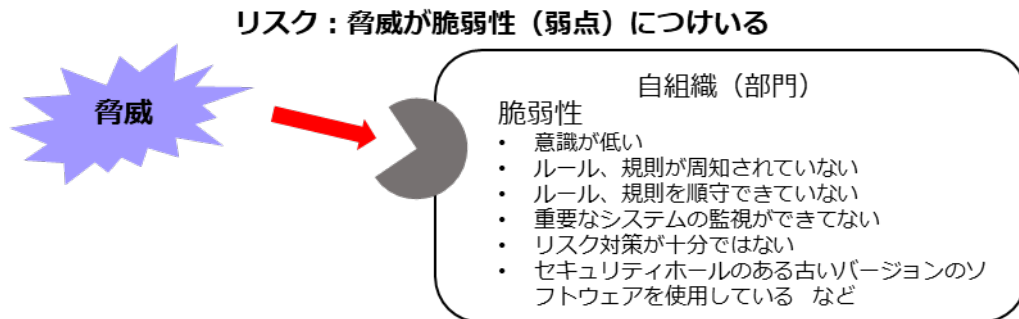


図 36. 脅威と脆弱性の関係

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

類型	脅威	原因
物理的損傷	火災、水害、汚染、大事故、機器や媒体の破壊、粉塵、腐食、凍結	A/D/E
自然現象	気候、地震、火山活動、気象現象、洪水	E
重要なサービスの喪失	空調や給水システムの故障/電気通信機器の故障	A/D
	電力供給の停止	A/D/E
情報を危うくすること	遠隔スパイ行為、盗聴、媒体や文章の盗難、機器の盗難、再利用又は廃棄した媒体からの復元、ハードウェアの改ざん、位置検知	D
	漏えい・信頼できない情報源からのデータ・ソフトウェアの改ざん	A/D
技術的な故障	機器の故障、機器の誤動作、ソフトウェアの誤作動	A
	情報システムの飽和、情報システムの保守に関する違反	A/D
許可されていない行為	許可されていない機器の使用、ソフトウェアの不正コピー、データの破壊、データの違法な処理	D
	海賊版又は（不正）コピーソフトウェアの使用	A/D
機能を危うくすること	使用時のミス	A
	権限の乱用/権限の詐称	A/D
	要員の可用性に関する違反	A/D/E

A：偶発的脅威（Accidental）

D：意図的脅威（Deliberate）

E : 環境的脅威 (Environmental)

脅威の一覧表の例
(出典)「ISO/IEC 27005」をもとに作成

脅威を洗い出すには自組織にある資産に対する脅威を識別して、前ページのようなリストを作成します。その際には、利用者や他の事業部の関係者、外部の専門家などから得られる、脅威に関する情報を活用することが大切です。

脅威の洗い出しの考え方として、意図的脅威は、攻撃の動機や必要なスキル、利用可能なリソースを考慮しつつ、資産の特性や魅力、脆弱性などから、どのような要因が脅威となるかを識別できます。一方で偶発的脅威は、環境や気候、人為的なミスや誤動作などから影響を及ぼす可能性を識別できます。

脅威の種類		想定される被害とセキュリティ対策
環境的脅威 (Environmental → E)		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復することを重視するなどのセキュリティ対策が選択されることになります。
人為的脅威	意図的脅威 (Deliberate → D)	「(内部者が企業秘密を) 漏えいする」という脅威が考えられます。このような脅威については、当該行為が犯罪行為 (不正競争防止法違反) であり、罰せられること、会社は企業規則により漏えい者を罰すること、場合によっては損害賠償請求を行うということを規程で明確に示し、教育を実施するという抑止的なセキュリティ対策が有効になります。漏えいを早期に検知するといったセキュリティ対策も重要になります。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じないように、二回ずつ入力する、一定の範囲の値しか入力できないようにする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

脅威の分類と、被害例と対策
(出典) MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

8-1-3. 脆弱性の識別

脆弱性があるだけでインシデントが発生するわけではありません。しかし、脆弱性は脅威を顕在化させ、インシデントの発生確率を高める可能性があります。脅威と脆弱性がもたらすリスクを低減するためには、適切な管理策を実施する必要があります。脆弱性は管理策の欠如を意味することが多いため、脆弱性を識別することは必要な管理策を識別するのに役立ちます。例えば

ば「アクセス権の誤った割当て」という脆弱性は、「アクセス権の適切な設定」という管理策の欠如を意味しています。

類型	脅威の例	脆弱性の識別
ハードウェア	システムの保守に関する違反	記憶媒体の不十分な保守/不適当な設置
	機器や媒体の破壊	定期的な交換計画の欠如
	粉塵（ダスト）、腐食、凍結	湿気、ホコリ、汚れに対する影響の受けやすさ
	使用時のミス	有効な構成変更管理の欠如
	電力供給の停止	電圧の変化に対する影響の受けやすさ
	気象現象	温度変化に対する影響の受けやすさ
	媒体や文書の盗難	保護されない保管
	媒体や文書の盗難	廃棄時の注意の欠如
	媒体や文書の盗難	管理されないコピー作成
ソフトウェア	不正アクセス	監査証跡の欠如
	不正アクセス	アクセス権の誤った割当て
	使用時のミス	複雑なユーザーインターフェース
	使用時のミス	文書化の欠如
	不正アクセス	ユーザーの識別および認証メカニズムの欠如
	不正アクセス	不十分なパスワード管理
	データの違法な処理	不要なサービスが実行可能
	ソフトウェアの誤作動	効果的な変更管理の欠如
	恐怖、攻撃、妨害行為	管理されていないソフトウェアのダウンロードおよび使用
	装置又はシステムの故障	バックアップコピーの欠如

脆弱性の識別例

（出典）「ISO/IEC 27005」をもとに作成

以下は、脆弱性を識別して一覧表にした例です。脆弱性の一覧表を作成する際は、脅威と関連付

けて整理する必要があります。

脆弱性を識別する際に参考になる情報

- ISO/IEC 27001:2022 の附属書 A「管理目的及び管理策」
- ISO/IEC 27002:2022 の管理策
- 情報セキュリティ管理基準など

脆弱性は、資産の性質から考えることによって簡単に識別できます。例えば、クラウドサービスは、「インターネットがあればどこでも利用可能」、「自社でデータを持たなくていい」といった性質を持ちます。同時にそれらの性質は「不正アクセス」「クラウドサービス停止によるデータの消失」という脅威に対する脆弱性があります。

情報セキュリティの CIA+4 要素

JIS Q 27000:2019 で、情報セキュリティは「機密性 (Confidentiality)」、「完全性 (Integrity)」及び「可用性 (Availability)」を維持することと定義されています。これら 3 つの要素 (CIA) をバランスよく維持することは、セキュリティを担保する上では欠かせません。また、さらに以下の 4 つの要素を追加して、情報セキュリティの 7 要素とする場合もあります。

○真正性 (Authenticity)

情報にアクセスする人や端末が「本当に許可されているか否か」を確実にすることを指します。多要素認証やデジタル署名など、認証方法を強化することがセキュリティ対策として考えられます。

○信頼性 (Reliability)

データやシステムを利用する際、意図した動作と結果が得られることを担保することを指します。不具合がないようにシステム構築を行うことや、ヒューマンエラーが起きないようなルール整備などがセキュリティ対策として考えられます。

○責任追跡性 (Accountability)

情報へのアクセスが、誰によってどのような手順で行われたのかを後から証明できるようにしておくことを指します。ログの取得や、デジタル署名などがセキュリティ対策として考えられます。

○否認防止性 (Non-repudiation)

問題発生後に、その原因となった人物から否定されないよう、後から証明できるようにしておくことを指します。先に説明した責任追跡性を担保することがセキュリティ対策につながります。

CIA の 3 要素に加えて上記の 4 要素も加えることにより、より抜け漏れがないセキュリティ対策が期待できます。

編集後記

第3編では、最初に[セキュリティポリシー](#)の構成（「基本方針」「対策基準」「実施手順・運用規則など」）について説明しました。そして、企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる、レベル感の異なる3つのアプローチ手法（Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ）を紹介しました。

その後、今後解説するリスクマネジメントを理解するために必要となる「リスク」、「脆弱性」、「脅威」といった用語の定義と関係性、さらに「脅威」、「[脆弱性](#)」の識別方法について説明しました。脅威や脆弱性、リスクなどの関係性は、図を用いて表し、具体例も合わせて説明しました。また、「脅威」、「脆弱性」を識別し、一覧表を作成するための考え方を説明しました。

本テキストを通じて、状況に応じて適切なセキュリティ対策のアプローチ手法を選択できるようになり、またリスクマネジメントで使用する用語を理解していただければと思います。

第9章. 具体的手順の作成（Lv.1 クイックアプローチ）

章の目的

第 9 章では、セキュリティインシデント事例を参考にする Lv.1 クイックアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- Lv.1 クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

9-1. 【Lv.1 クイックアプローチ】の概要

対策基準を策定し、具体的な実施手順を明確にすることにより、情報漏えいなどのリスク対策を行います。セキュリティ対策の内容を決めるためのアプローチ手法として、「Lv.1 クイックアプローチ」「Lv.2 ベースラインアプローチ」「Lv.3 網羅的アプローチ」があります。

本章では、「Lv.1 クイックアプローチ」における実施手順の作成方法について説明します。Lv.1 クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。

Lv.1 クイックアプローチ（緊急性の高い事象に対応するための対策）

概要

報道される事例や情報セキュリティ 10 大脅威などから、発生する可能性が高い[セキュリティインシデント](#)事例や、セキュリティインシデントが発生した場合に被害が大きい事例を参考にし、対策基準や実施手順を策定します。

メリット

小規模なセキュリティ対策や修正を迅速に実施可能。
低コストでリスクを軽減でき、コストパフォーマンスがよい。
流行中の攻撃の拡大や影響を最小限に抑えられる。
リソースが限られていても実施可能。

デメリット

包括的でないため、抜けが発生する可能性がある。
一時的な対策になりがちで、抜本的な対策にならない。
長期的にみると費用が嵩んでしまうことがある。



セキュリティインシデント事例をもとに、[リスクアセスメント](#)の実施
(リスク特定、リスク分析、[リスク評価](#))

9-2. 【Lv.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

Lv.1 クイックアプローチ

Lv.1 クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられる[セキュリティインシデント](#)事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。

対策基準・実施手順作成の手順

セキュリティインシデント事例をもとに[リスクアセスメント](#)を実施します。以下は、情報セキュリティ 10 大脅威 2024 にランクインしている「内部不正による情報漏えい」に関するセキュリティインシデント事例です。

事例：内部不正による情報漏えいの疑い（卸売業・小売業、従業員数 6~20 名以下）

被害内容

元従業員が退職前に大量にファイルをダウンロードしました。また、同従業員が使用していた PC の履歴が消去され、専門家でも復旧できない状態になっていました。

機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出しませんでした。しかし、この判断をするまでに 2 年かかりました。その間、弁護士に情報提供するために、多くの作業が必要になりました。例えば、経営者と総務担当は、情報漏えいしたと疑われる膨大なログを確認し、どれが機密情報に該当するかチェックする作業を強いられました。トラブル発生時は、人件費に加えて、心的負担も大きくかかりました。

被害発生の原因

社外からの脅威のセキュリティ対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限などは進めていたが、社内から発生する脅威のセキュリティ対策は不十分であったこと。

セキュリティインシデント事例：内部不正による情報漏えい

(出典) IPA「2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-」をもとに作成

リスク特定（例）

セキュリティインシデント事例を参考に、[情報資産](#)の洗い出しと、「[機密性](#)」「[完全性](#)」「[可用性](#)」の観点から重要度を算出します。セキュリティインシデント事例では、従業員が使用していた PC が悪用されていたため、以下の資産目録の例では「媒体・保存先」で従業員が使用する PC である情報資産を洗い出しています。そして、情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合、事業にどれほど影響があるか評価を行い、「重要度」を判断します。リスクアセスメントの詳細はこの後の「第 12 章. リスクマネジメント」を参照してください。

機密性・完全性・可用性の評価値は、1～3 で記載

重要度は、機密性・完全性・可用性いずれかの最大値

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3

資産目録の例

(出典) IPA 「リスク分析シート」をもとに作成

リスク分析（例）

リスク特定で算出した重要度と、被害発生可能性からリスクレベルを算出します。被害発生可能性は、セキュリティインシデント事例と同様の被害がどの程度起きやすいかを考慮して算出します。

リスクレベルの算出方法	「リスクレベル」 = 「重要度」 × 「被害発生可能性」

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	機密性	完全性	可用性	重要度	被害発生可能性	リスクレベル
人事	社員名簿	社員基本情報	人事部	人事部長	3	3	2	3	3	9
経理	当社宛請求書	過去3年分	経理部	経理部長	3	3	2	3	2	6
営業	顧客リスト	得意先	営業部	営業部長	3	3	3	3	2	6

リスク評価（例）

リスクレベルをもとに、必要なリスク対応を検討します。今回は、例としてリスク低減や回避を選択します。

リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすること
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせたりすること
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすること
リスク受容（保有）	セキュリティ対策を行わずにリスクを受け入れるということ



リスク評価をもとに対策基準・実施手順の作成

対策基準の策定（例）

リスク評価の結果を参考に対策基準を策定します。今回の例では、リスク低減や回避に関する対策基準を決定しています。対策基準の例は以下の通りです。

対策基準（例）
● 社内の機密情報に関する社内規程の策定 ● 重要情報の管理、保護 ● 物理的管理の実施 ● 従業員向け研修の実施

実施手順の作成（例）

情報セキュリティ関連規程を参考に、実施手順を作成します。情報セキュリティ関連規程とは、情報セキュリティに関する社内規則の見本です。情報セキュリティ関連規程から、対策基準に合った規則を選択し、赤字の箇所を自社の状況に合わせて編集することにより、実施手順を作成します。

実施手順の作成（例）
機密情報に関する社内規程の策定 （例）従業員の責務 従業員は以下を遵守する ● 従業員は、当社が営業秘密として管理する情報およびその複製物の一切を許可されていない組織、人に提供してはならない。

- **従業員**は、当社の情報セキュリティ方針および関連規程を遵守する。**違反時の懲戒**については、**就業規則**に準じる。
- **従業員**は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料またはそれらの複製物の一切を退職時に返還する。
- **従業員**は、在職中に知り得た当社の営業秘密または業務遂行上知り得た**技術的機密**を利用して、競合的あるいは競業的行為を行ってはならない。

重要情報の管理、保護

（例）利用者アカウントの管理

利用者の認証に用いるアカウントが不要になる場合、**システム管理者**は、当該アカウントの削除または無効化を、**当該アカウントが不要になった日の翌日までに実施する**。

物理的管理の実施

（例）情報資産の社外持ち出し管理

情報資産を社外に持ち出す場合には、以下を実施する。

- 社外秘の場合は所属部門長の許可を得る。
- 極秘の場合は代表取締役の許可を得る。
- ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。
- スマホ、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
- USB メモリなどの小型電子媒体は、大きなタグをつける/ストラップで体やカバンに固定する/落としてもすぐにわかるように鈴をつける。
- 屋外でネットワークへ接続して極秘または社外秘の情報資産を送受信する場合は、暗号化する。
- 携行中は常に監視可能な距離を保つ。

従業員向けの研修

（例）情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。

対象者：**全従業員**

テーマ：以下は必須とする。

- 情報セキュリティ関連規程の説明（入社時、就業時）
- 最新の脅威に対する注意喚起（随時）
- 関連法令の理解（関連法令の公布・施行時）
- 個人情報の取扱いに関する留意事項
- コンプライアンス教育

編集後記

第4編では、対策基準から実施手順を策定する手法を説明するにあたり、Lv.1 クイックアプローチについて説明しました。

Lv.1 クイックアプローチは、実際の[セキュリティインシデント](#)の事例を踏まえ、自社での発生可能性や被害規模を慎重に検討し、対策基準や実施手順を策定していく手法です。この方法により、特に社会的に影響の大きい事案に対するセキュリティ対策を迅速かつ効果的に行うことができます。

サイバーセキュリティの脅威への対処の最初の段階として、緊急に大きな[セキュリティホール](#)を塞ぐには有効なアプローチとなります。

第5編では、ガイドブックやひな型を参照して迅速に対応できるLv.2 ベースラインアプローチについて解説します。

第10章. 具体的手順の作成（Lv.2 ベースラインアプローチ）

章の目的

第10章では、ガイドラインやひな型などの資料を参考にするLv.2 ベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- Lv.2 ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

10-1. 【Lv.2 ベースラインアプローチ】の概要

「Lv.2 ベースラインアプローチ」における実施手順の作成方法について説明します。Lv.2 ベースラインアプローチは、ガイドラインなどを参考に、対策基準や実施手順を策定するアプローチ手法です。

Lv.2 ベースラインアプローチ（即効性のあるアプローチ手法）

概要

IPA や総務省などが発行しているガイドラインやひな型を参考に、対策基準や実施手順を策定します。

セキュリティ対策のガイドラインやひな型を参考にすることにより、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定します。

メリット

- 組織全体で一貫性を確保できる。
- 最低限実施すべきセキュリティ対策を講じることができる。
- ある程度の対策効果が見込め、コストパフォーマンスがよい。

デメリット

- 最低基準を満たすだけなので、十分なセキュリティ水準を確保できない可能性がある。
- ガイドラインやひな型は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものにするため、追加のセキュリティ対策やリスクに対する適切な対応策を検討する必要がある。

10-2. 【Lv.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

10-2-1. 情報セキュリティ対策ガイドラインの活用

Lv.2 ベースラインアプローチでは、ガイドラインやひな型などの資料を参考に対策基準、実施手順を作成します。次のページから、以下の資料をもとに対策基準、実施手順を作成する流れを説明します。

- IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」
- [NISC「インターネットの安全・安心ハンドブック Ver.5.0」](#)
- 総務省「テレワークセキュリティガイドライン第 5 版」
- IPA「中小企業のためのクラウドサービス安全利用の手引き」
- IPA「情報セキュリティ関連規程」

各資料の概要は以下の通りです。

IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」

「中小企業の情報セキュリティ対策ガイドライン」は、情報セキュリティ対策に取り組む際の、(1) 経営者が認識し実施すべき指針、(2) 社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編で構成されており、中小企業の利用を想定しています。付録の「5分でできる！情報セキュリティ自社診断」や「情報セキュリティハンドブック（ひな形）」を活用することにより、対策基準、実施手順を策定できます。

NISC「インターネットの安全・安心ハンドブック Ver.5.0」

「インターネットの安全・安心ハンドブック」は、サイバーセキュリティに関する基本的な知識を、身近な具体例を取り上げながら説明したものです。子供やシニアの方など、インターネットの一般利用者に加えて、中小企業なども活用できます。中小組織向けにある「インターネットの安全・安心ハンドブック Ver 5.00＜中小組織向け抜粋版＞」を活用することにより、対策基準、実施手順を策定できます。

総務省「テレワークセキュリティガイドライン第 5 版」

「テレワークセキュリティガイドライン」は、企業などがテレワークを導入する際のセキュリティ対策についての考え方や対策例を示したものです。テレワークを既に導入している場合は、自社のテレワーク環境がガイドラインに沿ったものであるのか検証できます。テレワークに関する「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場からそれぞれのセキュリティ対策について対策基準、実施手順を策定できます。

IPA「中小企業のためのクラウドサービス安全利用の手引き」

「中小企業のためのクラウドサービス安全利用の手引き」は、中小企業の情報セキュリティ対策ガイドラインの付録資料です。クラウドサービスを安全に利用するための手引きが記載され

ています。「クラウドサービス安全利用チェックシート」と「解説編」を参考にすることにより、クラウドサービス利用に関する対策基準、実施手順を策定できます。

IPA「情報セキュリティ関連規程」

「情報セキュリティ関連規程」は、自社に適した規程を作成するためのひな型です。ひな型に修正を加えることによって、対策基準、実施手順を策定します。1 から文書化する必要がないため、効率的に策定できます。

10-2-2. IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」の活用

対象者	● 中小企業および小規模事業者（業種は問わず、法人・個人事業主・各種団体も含む）の経営者と情報管理を統括する方 ● セキュリティ対策を部分的に実施してきた企業 ● 情報セキュリティに関する知識を十分に有した人材が不足している企業など
目的	● 情報セキュリティに関する組織的な取組を開始するため

本ガイドラインは、情報セキュリティに関する組織的な取組を行う際に活用できます。

本ガイドラインをもとに実施手順を策定する際は、「1. 実施状況の把握」「2. 対策の決定と周知」の手順で策定します。

1.実施状況の把握

「5分でできる！情報セキュリティ自社診断」を利用し、現在のセキュリティ対策の実施状況を把握します。合計 25 問の設問に答えるだけでセキュリティ対策の実施状況が把握できます。設問の例（一部抜粋）は以下の通りです。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	分からない
Part1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、 ウイルス定義ファイル は最新の状態にしていますか？	4	2	0	-1
	3	パスワードは破られにくい「長く」「複	4	2	0	-1

		雑な」パスワードを設定していますか？				
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	-1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1

自社診断の設問（一部抜粋）

（出典）IPA「5分でできる！情報セキュリティ自社診断」をもとに作成

5分でできる！情報セキュリティ自社診断」の使い方

- 経営者や情報システム担当者、部門長などセキュリティ対策の実施状況がわかる方が、25 問の設問に回答します。
- 事業所が複数ある、部署数が多いなど、1 人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- 実施状況がわからない場合、各従業員に質問して、回答を総合して記入します。
- チェック欄の該当するもの 1 つに○をつけて、「実施している…4 点」「一部実施している…2 点」「実施していない…0 点」「分からない…-1 点」で採点します。
- 全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「分からない」になっている項目を把握します。

詳細理解のため参考となる文献（参考文献）	
中小企業の情報セキュリティ対策ガイドライン第 3.1 版	https://www.ipa.go.jp/security/guide/sme/about.html
5分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf

2.対策の決定と周知

診断結果をもとに「5 分でできる！情報セキュリティ自社診断」（解説編）を参考にし、実行すべきセキュリティ対策を検討・決定します。解説編の例（抜粋）は以下の通りです。

診断編 No.3	パスワード管理
強固なパスワードを使用する	
パスワードが推測や解析されたり、Web サービスから流出した ID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。	
対策例	パスワードは 10 文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。

	同じ ID・パスワードを複数サービス間で使い回さない。 テレワークで VPN やクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。

解説編の一例

(出典) IPA「5分でできる！情報セキュリティ自社診断」をもとに作成

「5分でできる！情報セキュリティ自社診断」（解説編）の使い方

- セキュリティ対策の検討と決定は、責任者・担当者と経営者が行います。
- 診断項目ごとにセキュリティ対策を実施しない場合に考えられる被害・事故や、防止するためのセキュリティ対策例を参考にして検討します。
- 検討するときには従業員の意見を聞き、職場環境や業務に適したセキュリティ対策を決定します。

セキュリティ対策の決定後、「情報セキュリティハンドブック（ひな形）」を利用し、従業員が実行すべき事項を周知します。情報セキュリティハンドブック（ひな形）は、自社診断の解説編に記載されているセキュリティ対策例と連動しています。ひな型を編集して決定したセキュリティ対策の内容を具体的に記述し、従業員に配付します。ひな型の記載例は以下の通りです。

実施手順の例：パスワードの管理

ログインやファイル[暗号化](#)に使うパスワードは、以下に従って設定・利用する。

編集前（ひな型）

○必須	×禁止
10 文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない

編集後

○必須	×禁止
16 文字以上の文字数で構成されている	従業員番号・名前・住所・電話番号・生年月日・辞書に載っている単語・他人に推測されやすい文字列は使わない

ひな形の修正例

(出典) IPA「情報セキュリティハンドブック（ひな形）」をもとに作成

「情報セキュリティハンドブック（ひな形）」の使い方

- 情報セキュリティハンドブックは、責任者・担当者が作成します。
- ひな型に記載された例文を編集して、決定したセキュリティ対策を社内ルールとして明文化

します。

- 完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、セキュリティ対策を周知徹底します。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティハンドブック（ひな形）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu88-att/000108033.pptx

10-2-3. NISC「インターネットの安全・安心ハンドブック Ver.5.0」の活用

対象者	● 全従業員
目的	一人一人が能動的にサイバー空間における脅威を知り、サイバーセキュリティに対する素養・基本的な知識を身につけるため

本ハンドブックは、[サイバー攻撃](#)の手口やリスクを身近な具体例を取り上げながら説明しているため、専門知識を必要とせずセキュリティ対策を知ることができます。インターネットの利用者が実施すべき基本的なセキュリティ対策に加えて、中小組織向けのセキュリティ対策を記載しています。企業経営においてセキュリティ対策に投資すべき理由、企業特有のセキュリティ対策に必要なルール作りといった内容を説明しています。

以下では、第1章の「最低限実施すべきサイバーセキュリティ対策を理解しよう」を用いて、実施手順の作り方を説明します。

（例）①OS やソフトウェアは常に最新の状態にしておこう

インターネットの安全・安心ハンドブック記載

- OS 関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようにする。
- セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにする。
- サイバー攻撃で狙われやすいソフトウェアを重点的に更新する。
- 機器そのものの基本プログラムを更新するファームウェアもアップデートする。
- セキュリティソフトをインストールしている場合は、最新の[ウイルス定義ファイル](#)に自動更新されるよう設定する。
- アップデートが提供されなくなった OS やソフトウェアは[セキュリティホール](#)が見つかったても修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにする。

自社の状況

- OS、セキュリティソフトは法人向けを利用しているため、アップデート管理は情報システム部が担当。
- 情報システム部がブラウザは古いバージョンを使わないように通知している。
- 自宅で使用しているリモート用 PC は、一般向けのソフトウェアがインストールされている。

実施手順

対象 : PC

システム管理者は、アップデート管理として以下を実施する。

- システム管理者は月末に OS、セキュリティソフトの更新プログラムを適用する。緊急な場合は、従業員に通知し、更新プログラムを適用する。
- 従業員は、毎月 OS、セキュリティソフトの更新プログラムを適用する。確認方法はチェックリストを用いる。
- 従業員は、ブラウザのアップデートを適宜行い、バージョン〇〇以前のものは使用しない。
- システム管理者は〇〇日にセキュリティソフトのウイルス定義ファイルの更新を行う。

詳細理解のため参考となる文献（参考文献）	
インターネットの安全・安心ハンドブック Ver.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html

10-2-4. 総務省「テレワークセキュリティガイドライン第5版」の活用

対象者	● 経営者 ● システム・セキュリティ管理者 ● テレワーク勤務者
目的	テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するため

本ガイドラインでは、セキュリティ対策を整理するため、13 個の対策分類にわかれています。「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場から対策分類ごとに具体的に実施すべき事項を示しています。以下では、「6. マルウェア対策」をもとに自社の状況からセキュリティ対策の実施手順の作成例を説明します。

(例) 6. マルウェア対策

システム・セキュリティ管理者が実施すべき対策

- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
- セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能などを用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
- テレワーク端末に [EDR](#) を導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
- テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。

テレワーク勤務者が実施すべき対策

- 少しでも不審を感じたメール（添付ファイルや URL リンクなどを含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

自社の状況

- テレワーク端末には、法人向けのセキュリティ対策ソフトと EDR を導入しており、システム管理者はウイルス定義ファイルの更新などを一元管理できる。
- システム管理者は毎月〇〇日にセキュリティソフトのレポートを確認している。
- 不審なメールが来た場合は、情報システム部と上長に連絡するようにしている。

実施手順

テレワーク端末のマルウェア対策として以下を実施する。

- システム管理者は会社支給のテレワーク端末にセキュリティ対策ソフトと EDR をインストールし、一元管理する。
- システム管理者は、テレワーク端末の [ウイルス定義ファイル](#) の自動更新とリアルタイムスキャンを設定する。
- システム管理者は毎月〇〇日にセキュリティソフトと EDR のレポートを確認し、不審な点

があれば該当のテレワーク端末所有者に対して、確認を行う。

- 従業員は、不審を感じたメール（添付ファイルや URL リンクなどを含む。）は開かず、システム管理者と上長へ連絡する。

詳細理解のため参考となる文献（参考文献）

テレワークセキュリティガイドライン第5版

https://www.soumu.go.jp/main_content/000752925.pdf

10-2-5. IPA「中小企業のためのクラウドサービス安全利用の手引き」の活用

対象者	● クラウドサービスを利用する企業
目的	クラウドサービスを安全に利用するため

本ガイドラインは、クラウドサービスを安全に利用するために活用できるガイドラインです。「利用するクラウドサービスを選定するとき」、「クラウドサービスを運用していくとき」、「クラウドサービスのセキュリティ対策を検討するとき」のタイミングで活用することができます。本ガイドラインの使い方としては、「クラウドサービス安全利用チェックシート」でチェックを行います。また、「解説編」を参考に、利用者としての役割や責任を認識し、実施手順を策定します。

以下は、クラウドサービスの運用に関する設問例となります。

運用するときのポイント	
管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手もとに確保して必要なときに使えるようにしていますか？

解説編をもとに実施手順を作成します。以下は、チェックシートの設問「バックアップに責任を持つ」の実施手順（例）を記載します。自社の状況に合わせて赤字の箇所を修正することによって、自社に適した実施手順を作成できます。

実施手順の例：バックアップに責任を持つ

バックアップの管理

サービス停止やデータの消失・改ざんなどに備え、重要情報を手もとに確保して、必要なとき

に使えるようにする。

会計データやホームページなど、消失や改ざんの影響が大きいものは以下の規則を遵守する

- クラウドサービスの拡張機能にバックアップがある場合は利用する
- 月に1度、社内の専用ハードディスクにバックアップを取得する
- 直前のバックアップよりもさらに過去の状態に遡って復元できるよう、2、3ヶ月前に取得したバックアップを保存しておく

詳細理解のため参考となる文献（参考文献）

付録6：中小企業のためのクラウドサービス安全利用の手引き

<https://www.ipa.go.jp/security/sme/f55m8k0000001wcf-att/000072150.pdf>

10-2-6. IPA「情報セキュリティ関連規程」の活用

対象者	● 中小企業
目的	自社のリスクに応じたセキュリティ対策の規程を作成するため

情報セキュリティ関連規程とは、自社が対応すべきリスクとセキュリティ対策を検討し、文書化した規程のことです。企業をとりまくリスクは、事業内容や取扱う情報、職場環境、ITの利用状況などによって異なるため、汎用的な規程をそのまま使っても、自社に適さない場合があります。そこで情報セキュリティ関連規程を活用することによって、効率的に自社に適した規程を作成できます。

本ガイドラインを用いて、規程を作成する手順を説明します。

1. 対応すべきリスクを特定する

経営者が懸念する情報セキュリティの重大事故などを念頭に、何を起こさないようにするべきかを考えます。このとき、以下のような状況を併せて考えることにより、対応すべきリスクを把握します。

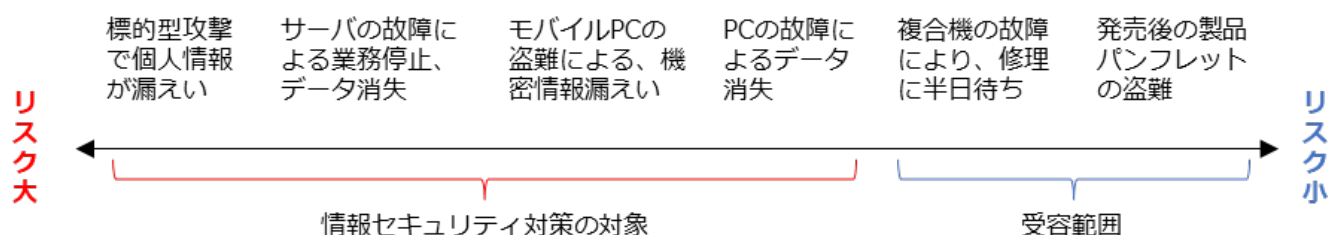
関連する業務や情報に関わる外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）、内部状況（経営方針・情報セキュリティ方針、セキュリティ管理体制、情報システムの利用状況など）

- 例
- 個人情報保護法への対応
 - 取引先のセキュリティに対する要求への対応
 - テレワーク時のセキュリティ対応

- 報道されている新たなサイバー攻撃への対応

2.セキュリティ対策の決定

すべてのリスクに対応しようとする、セキュリティ対策費用が高額になったり、業務に支障をきたしたりする場合があります。そこで、いつ事故が起きてもおかしくない、事故が起きると大きな被害になるなど、リスクが大きなものを優先してセキュリティ対策を実施します。また、事故が起きる可能性が小さい、発生しても被害が軽微であるなど、リスクが小さなものは、現状のまま受容するなど、合理的に対応します。



3.規程の作成

「2. セキュリティ対策の決定」で対象としたリスクに対してセキュリティ対策を実施するため、文書化した規程を作成します。「中小企業の情報セキュリティ対策ガイドライン 付録 5 情報セキュリティ関連規程（サンプル）」を編集することによって、規程を作成することができます。以下では、「サーバの故障による業務停止、データ消失」に対するセキュリティ対策を文書化した規程の例を記載します。赤文字の箇所を修正することにより、自社に適した規程を作成します。

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的を取得する。

機器名	対象	方法	保管先
ファイルサーバ	ユーザーファイル	アプリケーションバックアップ機能	NAS サーバ
Web サーバ	ホームページ	同期ツール	NAS サーバ
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

● NAS サーバ：施錠つきサーバラックに収納



3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的を取得する。

機器名	対象	方法	保管先
DB サーバ	取引先に関するデータ	アプリケーションバックアップ機能	自社サーバ
Web サーバ	ホームページ	同期ツール	自社サーバ
発注管理システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドサービス上のサーバ

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

● 自社サーバ：ハウジングサービスを利用し、サービス事業者の施設内に保管する

情報セキュリティ関連規程の一例
(出典) IPA「情報セキュリティ関連規程（サンプル）」をもとに作成

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

編集後記

第5編では、ガイドラインやひな型などの資料を参考にするLv.2 ベースラインアプローチにおける対策基準・実施手順の策定方法を解説しました。

Lv.2 ベースラインアプローチは、ガイドラインやひな型などの既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができます。

Lv.2 ベースラインアプローチを用いることにより、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定できます。

第6編では、より漏れがないLv.3 網羅的アプローチで用いるISMSや、その他主要な[フレームワーク](#)を解説します。

第11章. セキュリティフレームワーク

章の目的

第 11 章では、ISMS をはじめとしたサイバーセキュリティ対策における代表的なフレームワークを理解し、それぞれの内容について知識を身につけることを目的とします。

主な達成目標

- サイバーセキュリティ対策においてフレームワークを活用することの重要性について理解すること
- 各フレームワークの目的や必要性などの特徴について理解すること

11-1. セキュリティフレームワークの概要

11-1-1. セキュリティフレームワークの役割と重要性

セキュリティフレームワークの概要およびその利用メリットについて説明します。

セキュリティフレームワークとは

セキュリティ対策を行うために定義された指針やセキュリティ対策基準、ガイドライン、[ベストプラクティス](#)集のことを指します。自社におけるセキュリティリスクを評価・管理し、適切なセキュリティ対策を計画、実装、管理するための基盤となります。

セキュリティフレームワークを使用するメリット

効果的なセキュリティ対策

フレームワークを使用することにより、セキュリティ対策の抜け漏れを防ぎ、効果的かつ適切なセキュリティ対策を行うことが可能となります。

信頼性の確保

認証制度が存在する[フレームワーク](#)の場合、そのフレームワークにしたがってセキュリティ対策を実装し、第三者機関から認証を受けることにより、取引先や顧客からの信頼獲得につながります。

代表的なセキュリティフレームワーク

[ISMS](#)（情報セキュリティマネジメントシステム）

ISO/IEC27001:2022、ISO/IEC 27002:2022

- 網羅的なセキュリティフレームワーク

ISO/IEC 27017:2015

- クラウドサービス

サイバーセキュリティフレームワーク ([CSF](#)) 2.0

- 幅広い組織向け

[サイバー・フィジカル・セキュリティ対策フレームワーク \(CPSF\) Ver.1.0](#)

- [Society 5.0](#) における産業社会

サイバーセキュリティ経営ガイドライン Ver3.0

- 経営者を中心としたセキュリティ対策

PCI DSS（国際的なクレジット産業向けのデータセキュリティ基準）v4.0.1

- クレジットカード産業

個人情報保護マネジメントシステム（PMS） JIS Q 15001:2023 準拠 ver1.0

- 個人情報保護

CIS Controls version 8.1

- 具体的な[サイバー攻撃](#)アプローチ

ISA/IEC 62443

- 産業オートメーションおよび制御システム

フレームワーク使用上のポイント

上記のようにフレームワークは数多くの種類がありますが、まずは業種業態を問わず、セキュリティ対策の全体の枠組みと網羅的な対策項目を提示している ISMS をベースとするとよいでしょう。そして必要に応じて、業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークの内容で補完することが大切です。

11-1-2. フレームワーク選択の重要性

ISMS（情報セキュリティマネジメントシステム）

ISO/IEC27001:2022、ISO/IEC 27002:2022

● 網羅的なセキュリティフレームワーク

発行元：ISO/IEC

情報の機密性、完全性、可用性を保護するための体系的な仕組みであり、技術的対策に加えて、従業員の教育や訓練、組織体制の整備などが含まれています。必ずしも、組織全体で適用する必要はなく、組織の必要に応じて、適用範囲を決定できるという特徴があります。¹⁰

ISO/IEC 27017:2015

● クラウドサービス

発行元：ISO/IEC

クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格で、ISO/IEC27002 をベースに作成されています。この規格は、クラウドサービスの提供者とクラウドサービスの利用者の両方を対象としています。クラウドサービスに関するリスクの低減や、クラウドサービスを適切に利用する組織体制を確立できます。

また、情報セキュリティ全般に関するマネジメントシステム規格である ISO/IEC 27001 の取組を ISO/IEC 27017 で強化することによって、クラウドサービスにも対応した情報

サイバーセキュリティフレームワーク (CSF) 2.0

● 幅広い組織向け

発行元：NIST

CSF は、組織がサイバーセキュリティリスクを管理する際の指針を提供するものです。CSF は、組織の規模や業界を問わず（産業界、学術界、政府および非営利組織を含む）組織におけるサイバーセキュリティリスクの管理と低減に役立つよう設計されています。CSF の下位概念に位置づけられているのが SP800 シリーズ（SP 800-53/SP 800-171/SP 800-161 など）となります。CSF2.0、SP800 シリーズの内容については後述します。

¹⁰ ISMS-AC.“ISMS 適合性評価制度”。<https://isms.jp/doc/JIP-ISMS120-62.pdf>

セキュリティ管理体制を構築することができます。	
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）Ver.1.0	サイバーセキュリティ経営ガイドライン Ver3.0
● Society 5.0 における産業社会 発行元：経済産業省 <u>ISMS、CSF の概念を包含したフレームワーク</u> であり、サイバー空間におけるセキュリティ対策から、サイバー空間とフィジカル空間のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理しています。 <u>Society5.0</u> を意識したセキュリティリスクとその対策方法について記述されている特徴があります。 リスク源を適切に捉えるために産業社会を 3 層構造と 6 つの構成要素で捉えており、産業界が自らのセキュリティ対策に活用できるよう、対策例がまとめられています。	● 経営者を中心としたセキュリティ対策 発行元：経済産業省/独立行政法人情報処理推進機構（IPA） サイバー攻撃の多様化・巧妙化に伴い、<u>サイバー攻撃</u>から企業を守るために必要なことをまとめたガイドラインです。ISMS の<u>フレームワーク</u>がベースとなっており、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある 3 原則と、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO など）に指示すべき重要 10 項目をまとめているという特徴があります。¹¹ サイバー攻撃から企業を守る観点で、“サイバーセキュリティは経営問題”と定義し、経営者を中心とした組織的な対策の見直し・強化を求めています。
PCI DSS（国際的なクレジット産業向けのデータセキュリティ基準）v4.0.1	個人情報保護マネジメントシステム（PMS） JIS Q 15001:2023 準拠 ver1.0
● クレジットカード産業 発行元：PCI SSC クレジットカード情報を取扱うすべての事業者に対して国際カードブランド 5 社が共同で策定した、クレジットカードの取扱いにおけるセキュリティの国際基準です（Payment Card Industry Data Security Standard の略）。¹² カード会員情報を適切に管理するため、ネットワークアーキテクチャ、ソフトウェアデザ	● 個人情報保護 発行元：JIPDEC 組織が業務上取扱う個人情報を安全で適切に管理するための仕組みです。JIS Q 15001 によって要求事項が定められています。この規格は、事業者が個人情報を適切に取扱う方法を規定したもので、プライバシーの保護を直接の目的とはしていません。しかし、意図しない個人情報の取扱いが抑制されることにより、結果的にプライバシーも保護されます。¹³

¹¹ 経済産業省,“サイバーセキュリティ経営ガイドラインと支援ツール”, https://www.meti.go.jp/policy/netsecurity/mng_guide.html

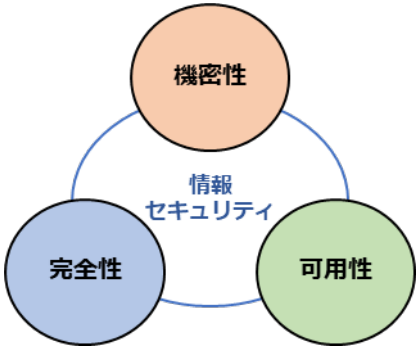
¹² 経済産業省,“クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性”, <https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf>

¹³ JIPDEC,“「個人情報」と「プライバシー」の違い”, <https://privacymark.jp/system/course/theme1/03.html>

イン、セキュリティマネジメント、ポリシー、プロシジャなどに関する基準が 12 の要件として規定されています。	個人情報保護マネジメントシステム（PMS）の基本的な仕組みは、個人情報保護方針を定め、この方針に基づき「PDCA サイクル」を実行することになります。
CIS Controls version 8.1	ISA/IEC 62443
● 具体的なサイバー攻撃アプローチ 発行元：CIS サイバー攻撃の現状と傾向を踏まえて、組織が実施すべきサイバーセキュリティ対策とその優先順位を決めるためのフレームワークで、あらゆる企業が取るべき最も基本的で重要な対応に重点を置いています。ネットワークの詳細設定や、ログの管理など、具体的な技術的な対策が中心となっている特徴があります。 多岐にわたる対策の中から、自社（組織）が実施すべき対策と、その優先順位を導くためのアプローチを提示したフレームワークとなります。	● 産業オートメーションおよび制御システム 発行元：ISA/IEC 産業用自動制御システム（Industrial Automation and Control Systems）に対するセキュリティ対策とプロセス要件を定めた一連の国際標準規格です。ISO/IEC 27001 などではカバーしきれない、工場やプラントにおける制御システムのセキュリティを網羅的に対象としています。また、セキュリティ確保の対象は、ソフトウェア・ハードウェアを含む制御関連のデータ処理基盤であるシステムに加えて、システムの運用に関わる「人」と「業務」も対象となっている特徴があります。

11-2. 情報セキュリティマネジメントシステム（ISMS） 〔ISO/IEC27001:2022, 27002:2022〕

ISMS とは、情報セキュリティマネジメントシステム（Information Security Management System）の略称で、組織の情報セキュリティリスクを適切に管理するための仕組みのことです。ISMS に関する国際規格がフレームワークとして存在していることから、ISMS はセキュリティフレームワークの中でも代表的なものとなっています。ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランスよく維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与えることにあります。¹⁴また、ISMS には技術的対策に加えて、従業員の教育・訓練、組織体制の整備なども含まれます。

情報セキュリティの 3 要素	
機密性（Confidentiality） 権限のない個人、 <u>エンティティ</u> またはプロセスに対して、情報を使用させず、また、開示しないこと（情報に対するアクセスを適切に管理すること）	 図 37. 情報セキュリティの 3 要素 （出典）ISMS-AC「ISMS 適合性評価制度」をもとに作成
完全性（Integrity） 情報が正確であり、完全である状態を保持すること	
可用性（Availability） 情報を必要なときに使えるようにしておくこと	

One Point

情報セキュリティの 7 要素

情報セキュリティには、上記で紹介した 3 要素に加えて、「真正性（Authenticity）」「信頼性（Reliability）」「責任追跡性（Accountability）」「否認防止（non-repudiation）」という 4 つの拡張要素があります。これらは、情報にアクセスする人が本当にアクセスすべき人であることを担保することや、システムが確実に目的の動作をすること、誰がどのような手順で情報にアクセスしたかを追跡できるようにすること、また、情報が後から否定されない状況を作ることにより情報セキュリティを確保するものです。

ISMS のための要求事項をまとめた国際規格が、ISO/IEC 27001 です。組織が ISMS を確立し、

¹⁴ ISMS-AC.“ISMS とは”。<https://isms.jp/isms/>

実施し、維持し、継続的に改善するための要求事項の提供を目的として作成されています。ISMSの確立および実施について、組織の行うべき事項が項目ごとに記述されたものとなっており、この規格は以下のために用いることができます。¹⁵

組織のマネジメントおよび業務プロセスを取り巻くリスクの変化への対応

JIS Q 27001 (ISO/IEC 27001) では、組織は、自らのニーズおよび目的、情報セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模および構造を考慮して、ISMSの確立および実施を行います。これは、多くの情報を取扱うようになっている、現代の組織のマネジメントおよび業務プロセスを取り巻くリスクの変化に対応できるように、組織基盤を構築する抜本的な業務改革をする目的に適しています。

情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準

JIS Q 27001 (ISO/IEC 27001) は、情報セキュリティ要求事項を満たす組織の能力を、パフォーマンス評価および内部監査などにより、組織の内部で評価する基準としても、取引先の顧客などから受ける第三者監査、あるいは、審査登録機関による認証のための第三者監査の基準としても用いることができます。



(出典) ISMS-AC. "ISMS とは". <https://isms.jp/isms>

ISO/IEC 27001 と JIS Q 27001

ISMS に関する規格には、ISO/IEC 27001 とは別に JIS Q 27001 があります。国際規格である ISO/IEC に対して、JIS は日本産業規格となり、日本における任意の国家規格です。JIS Q 27001 は、ISO/IEC 27001 を日本語に訳したものとなり ISO と JIS による規格内容の違いはありません。

¹⁵ ISMS-AC. "ISMS とは". <https://isms.jp/isms/>

11-3. NIST サイバーセキュリティフレームワーク（CSF）

11-3-1. NIST サイバーセキュリティフレームワーク（CSF）の概要

[CSF](#) の概要および [ISMS](#) との関係性について説明します。CSF の最新版は、2.0 です。CSF2.0 は、中小企業を含むあらゆる組織で利用されるよう設計されています。

CSF2.0 は ISMS を補完し、組織のセキュリティ対策を強化するための有用なツールとなります。ISMS を補完する形で、ISMS をベースに必要に応じて CSF を取り込むことが重要です。

CSF2.0 とは

CSF2.0 は、あらゆる組織がサイバーセキュリティリスクを管理する際の指針を提供するものです。CSF2.0 は、どのような組織でもサイバーセキュリティへの取組をより深く理解し、評価し、優先順位をつけ、各方面に周知するために利用できます。CSF2.0 の実施方法は画一的ではなく、組織ごとに異なります。各組織には共通のリスクと固有のリスクの両方があり、また、組織によってリスク選好度やリスク許容度、具体的なミッション、ミッションを達成するための目的もさまざまであるためです。CSF2.0 をしっかりと理解し、自組織に適した形で実施することが重要です。

CSF2.0 の 3 つの構成要素（コア、ティア、プロファイル）

CSF は、組織がセキュリティ対策を継続的に改善するため、①コア（サイバーセキュリティ対策の一覧）、②ティア（対策状況を数値化するための成熟度評価基準）、③プロファイル（サイバーセキュリティ対策の現状とあるべき姿を記述するための[フレームワーク](#)）の 3 つの要素で構成されています。

「コア」の概要

コアとは、一定の分類で定められたセキュリティ管理策の一覧のことです。

コアは、「識別」「防御」「検知」「対応」「復旧」「ガバナンス」の 6 つの機能に分類されます。各機能の下には複数のカテゴリが存在し、各カテゴリはそれぞれ複数のサブカテゴリを有します。

「ティア」の概要

組織におけるサイバーセキュリティガバナンスと管理の成熟度を評価するための階層（tier）です。

指標階層は 4 段階あり、次の通りです。

- ティア 1：実施しているが、まだ部分的／基本的なレベル
- ティア 2：ある程度定型化されているがポリシーにはなっていない
- ティア 3：ポリシーとして確立しており、繰り返し適用可能なレベル

- ティア4：サイバーセキュリティリスク管理が組織文化の一部となっている

「プロファイル」の概要

フレームワークのカテゴリおよびサブカテゴリに基づき、サイバーセキュリティリスクに対する期待される効果を現すものです。

サイバーセキュリティリスクへの対応状況として、「あるべき姿」と「現在の姿」をまとめたものです。「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整します。

詳細理解のため参考となる文献（参考文献）	
The NIST Cybersecurity Framework (CSF) 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

「コア」

コアとは、業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものです。「ガバナンス」「識別」「防御」「検知」「対応」「復旧」の6つの機能に分類されます。

ガバナンス機能は、他の5つの機能（識別、防御、検知、対応、復旧）の目標達成や組織内の優先順位づけをするためのものと定義され、CSF2.0の中心的機能と位置づけられています。

各機能の下には複数のカテゴリが存在し、合計22個あります。また、各カテゴリにはそれぞれ複数のサブカテゴリが存在しており、サブカテゴリは合計で106個あります。

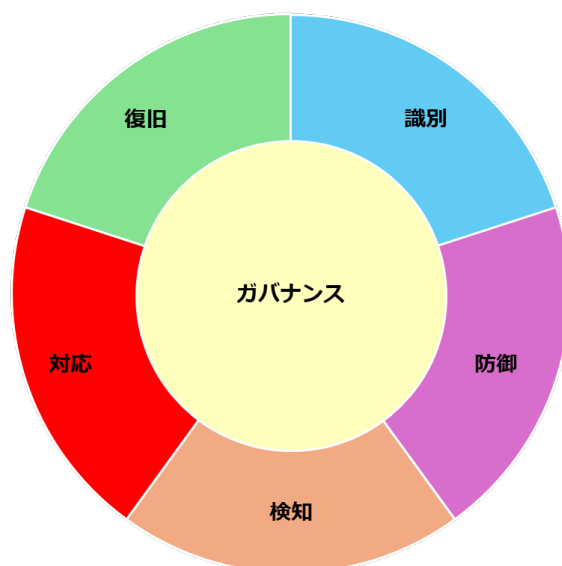


図 38. CSF2.0 のコア

（出典）「The NIST Cybersecurity Framework (CSF) 2.0」をもとに作成

機能	説明	カテゴリ
ガバナンス	組織におけるサイバーセキュリティリスクマネジメントの戦略、期待事項、およびポリシーを確立し、周知し、モニタリングする。	● 組織的文脈 ● リスクマネジメント戦略 ● 役割/責任/権限 ● ポリシー ● 監督 ● サイバーセキュリティサプライチェーンリスクマネジメント
識別	組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。	● 資産管理 ● リスクアセスメント ● 改善
防御	重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。	● アイデンティティ管理とアクセス制御 ● 意識向上およびトレーニング ● データセキュリティ ● プラットフォームセキュリティ ● 技術インフラのレジリエンス
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する。	● 継続的モニタリング ● 有害イベントの分析
対応	サイバーセキュリティインシデント に対処するための適切な対策を検討し実施する。	● インシデントマネジメント ● インシデント分析 ● インシデント対応の報告とコミュニケーション ● インシデント軽減
復旧	サイバーセキュリティインシデントにより影響を受けた機能やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。	● インシデント復旧計画の実行 ● インシデント復旧のコミュニケーション

「ガバナンス」機能のサブカテゴリ（例）

カテゴリ	サブカテゴリ
組織的文脈	GV.OC-01：組織のミッションが理解され、サイバーセキュリティリスクマネジメントについて伝えている。
	GV.OC-02：内部と外部の利害関係者が理解され、サイバーセキュリティリスクマネジメントに関するそれら利害関係者のニーズと期待事項が理解および考慮されている。
	GV.OC-03：サイバーセキュリティに関する法的要求事項、規制上の要求事項、および契約上の要求事項（プライバシーと市民的自由の義務を含む）が理解され管理されている。
	GV.OC-04：外部の利害関係者が組織に依存または期待する重要な目的、能力およびサービスが理解され周知されている。
	GV.OC-05：組織が依存する成果、能力、およびサービスが理解され周知されている。

「ティア」

ティアとは、組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものです。指標は以下の4段階があります。各ティアの定義は、組織に応じて柔軟にアレンジすることが可能です（以下の表は一例です）。また、必ずしもすべてのカテゴリにおいて最高レベル（ティア4）を目指す必要はありません。ビジネス特性や[情報資産](#)の実態などに応じて、カテゴリごとに目指すべきティアを設定しましょう。

ティア1：実施しているが、まだ部分的／基本的なレベル

セキュリティ対策は経験に基づいて実施される。セキュリティ対策は組織として整備されていなく場当たりに実施されている。

ティア2：ある程度定型化されているがポリシーにはなっていない

セキュリティ対策はセキュリティリスクを考慮して実施されているが、組織として方針や標準が定められてはいない、あるいは非公式に存在する。

ティア3：ポリシーとして確立しており、繰り返し適用可能なレベル

セキュリティ対策は組織の方針・標準として定義、周知されており、脅威や技術の変化に伴い方針・標準は定期的に更新される。

ティア4：サイバーセキュリティリスク管理が組織文化の一部となっている

組織で標準化されたセキュリティ対策は、脅威や技術の変化、組織における過去の教訓やセキ

セキュリティ対策に関するメトリックスなどを参考に、継続的かつタイムリーに調整される。

サイバーセキュリティリスクへの対応状況を評価する例

識別：セキュリティ対策が必要なリソースを明確にする

	ティア 1	ティア 2	ティア 3	ティア 4
資産管理 事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が特定され管理されていますか？				

防御：ルールを策定し、セキュリティリスクをコントロールする

	ティア 1	ティア 2	ティア 3	ティア 4
意識向上およびトレーニング サイバーセキュリティ意識向上教育とトレーニングが実施されていますか？				

検知：事故の発生を即時に把握するための仕組みをつくる

	ティア 1	ティア 2	ティア 3	ティア 4
異常とイベント 異常な活動は検知されており、異常がもたらす潜在的な影響を把握していますか？				

対応：事故に対する対策を用意する

	ティア 1	ティア 2	ティア 3	ティア 4
対応計画の策定 検知したセキュリティ事故に対応できるように対応プロセスおよび手順が準備されていますか？				

復旧：システムを正常な状態に戻すための必要なタスクを明確にする

	ティア 1	ティア 2	ティア 3	ティア 4
復旧計画の作成 セキュリティ事故による影響を受けたシステムや資産を復旧できる復旧プロセスおよび				

び手順となっていますか？				

「プロファイル」

プロファイルとは、機能・カテゴリ・サブカテゴリについて、組織ごとに考慮すべき点を踏まえて調整し、整理したものです。組織はプロファイルを用いることにより、サイバーセキュリティ対策の現在の状態（現在の姿）と、目標の状態（あるべき姿）を明らかにすることができます。そして「現在の姿」と「あるべき姿」を比較することによって、サイバーセキュリティマネジメント上の目標を達成する上で、解消が必要なギャップを知ることができます。

「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整します。

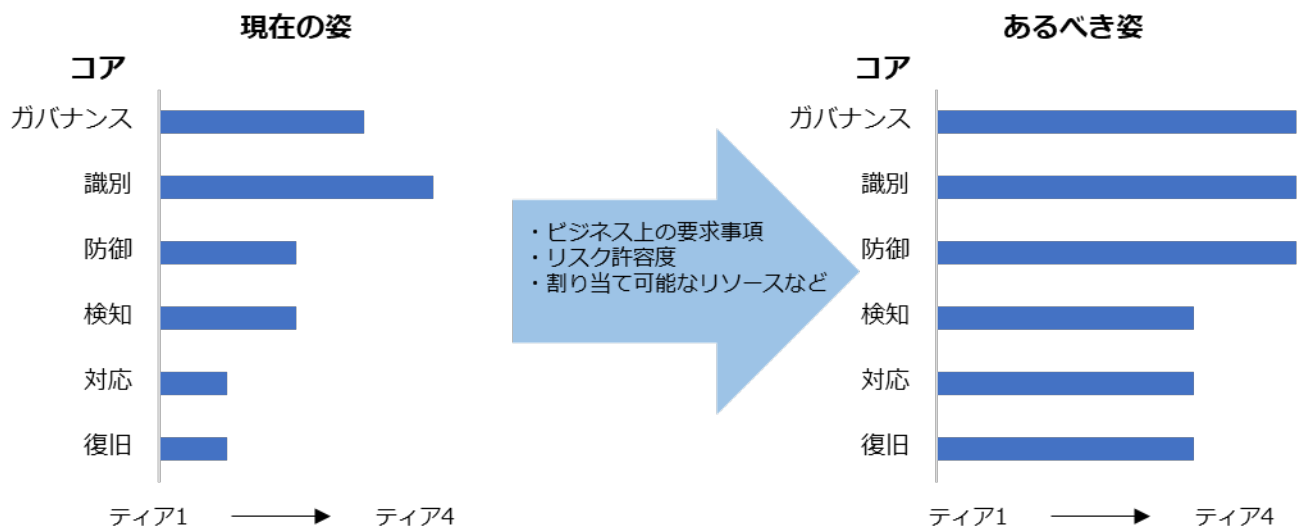


図 39. プロファイルの活用イメージ

（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート」 をもとに作成

NIST サイバーセキュリティフレームワーク（CSF）2.0 の特徴

令和 6 年 2 月 26 日、NIST サイバーセキュリティフレームワークが 1.1 から 2.0 に改訂されました。CSF2.0 の主な特徴は、以下の通りです。

フレームワークの適用範囲の拡大

CSF 2.0 は、組織の規模や業種に関係なく、中小企業を含むあらゆる組織で利用されるよう再設計されました。以前の CSF 1.0, 1.1 は、重要インフラ（病院、発電所など）の安全保障を目的に策定されたものでした。

新たな機能「ガバナンス」の追加

CSF2.0 では、コアの 5 つの機能（特定・防御・検知・対応・復旧）に、「ガバナンス」が新たに追加されました。

ガバナンスは、5つの機能の中心に位置づけられています。ガバナンスは、組織のミッションと利害関係者の期待に沿って、他の5つの機能の成果の達成と優先順位をつけるための方法を示します。

フレームワーク活用のためのコンテンツ強化

CSFの実装を支援するためのさまざまな参考情報が、NISTのWebサイトに公開されました。

- クイック・スタート・ガイド（Quick-Start Guide）

中小企業などの特定のニーズに対応した専用のガイダンスを提供しています。

文書名	利用方法
Small Business Quick-Start Guide	中小企業、特にサイバーセキュリティ計画があまり整っていないまたは全くない企業が、CSF2.0を使用してサイバーセキュリティリスク管理戦略を開始するためのポイントを理解するために利用できます。
A Guide to Creating Community Profiles	フレームワークを実装するために、コミュニティプロファイルの作成と使用に関する考慮事項を理解するために利用できます。コミュニティプロファイルとは、多数の組織間で共有される、サイバーセキュリティリスクを低減するための関心、目標、成果を記述したものです。
Quick-Start Guide for Creating and Using Organizational Profiles	CSF 2.0を実装するための現状および目標プロファイルの作成と使用に関する考慮事項を理解するために利用できます。
Quick-Start Guide for Using the CSF Tiers	CSF 2.0のティアをプロファイルに適用し、自身のサイバーセキュリティリスクのガバナンスおよび管理成果の厳密さを特徴付けるために利用できます。
Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)	サイバーセキュリティサプライチェーンリスク管理（C-SCRM）の概要と、C-SCRMがCSFとどのように関連しているのか理解するために利用できます。 C-SCRMの機能を実装する組織は、このガイドに加えて、参照されている追加文書も併せて確認することが推奨されます。
Enterprise Risk Management Quick-Start Guide	エンタープライズリスクマネジメントの実務者が、組織のサイバーセキュリティリスクマネジメントを改善するために、CSF2.0で提供される成果の活用方法を理解す

るために利用できます。

- 参考情報 (Informative References)

参考情報を利用することにより、目標達成に役立つ他のガイドラインやリソースを知ることができます。

- 実装例 (Implementation Examples)

実装例を利用することにより、特定のサブカテゴリをどのように実装するかは[ベストプラクティス](#) (最良の方法) を知ることができます。

- NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

NIST CSF 2.0 リファレンスツールを利用すると、ユーザーは CSF 2.0 コア (機能、カテゴリ、サブカテゴリ、実装例) を探索できます。このツールは、人間と機械が読み取り可能な形式 (JSON および Excel) でコアを提供します。さらに、ユーザーは主要な検索用語を使用してコアの一部を表示し、エクスポートすることが可能です。これにより、ユーザーは自分のニーズに合わせて情報を探しやすいになります。

サプライチェーンリスクマネジメントの強化

CSF2.0 では、新機能「ガバナンス」の下に新しいカテゴリ (GV.SC : サイバーセキュリティサプライチェーンリスクマネジメント) が設けられました。GV.SC カテゴリの下には 10 個のサブカテゴリが定義され、CSF1.1 に比べて[サプライチェーン](#)のリスク管理に必要な対策が増加しました。

詳細理解のため参考となる文献 (参考文献)	
Small Business Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1300
A Guide to Creating Community Profiles	https://doi.org/10.6028/NIST.CSWP.32.ipd
Quick-Start Guide for Creating and Using Organizational Profiles	https://doi.org/10.6028/NIST.SP.1301
Quick-Start Guide for Using the CSF Tiers	https://doi.org/10.6028/NIST.SP.1302.ipd
Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)	https://doi.org/10.6028/NIST.SP.1305.ipd
Enterprise Risk Management Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1303.ipd
CSF 2.0 Informative References	https://www.nist.gov/informative-references
CSF 2.0 Implementation Examples	https://www.nist.gov/document/csf-20-implementations-pdf
NIST Cybersecurity Framework (CSF) 2.0 Reference Tool	https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters

11-3-2. NIST SP 800

NIST SP 800 シリーズと CSF の関連性

[CSF](#) は、NIST が定義するサイバーセキュリティ対策アプローチの中で最も上位に位置づけられており、セキュリティ管理手法の概念や管理方針・体制の整備など包括的な内容が記載されています。CSF の下位概念に位置づけられているのが、NIST SP 800 シリーズです。実施すべきタスクと手順、推奨技術の特定など、セキュリティ管理の手法について具体的に明記されています。

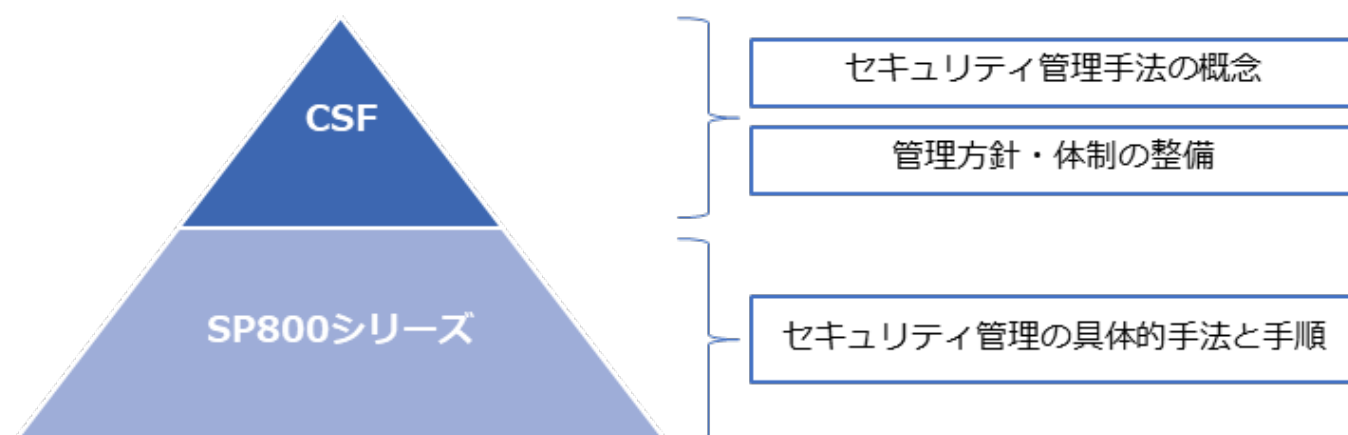


図 40. CSF と SP800 シリーズの関係

NIST SP 800-53、NIST SP 800-171、NIST SP 800-161

NIST SP 800 シリーズの中から、ガイドラインの一部を紹介します。

NIST SP 800-53

米国政府内の情報システムをより安全なものにし、効果的にリスク管理するためのガイドラインのことです。対象は連邦政府機関で、政府の機密情報（CI：Classified information）の保護を目的としています。

NIST SP 800-171

NIST SP 800-53 から民間企業・組織向けに要件を抽出したものです。[サプライチェーン](#)に存在する、業務委託先や関連企業のすべてが準拠すべきセキュリティ基準を示しています。対象は、多くの民間企業・組織で、政府の機密情報以外の重要情報（CUI：Controlled Unclassified Information）の保護を目的としています。

NIST SP 800-161

調達から販売・供給までの一連のサプライチェーンに起因するさまざまなリスクに対して、組織として対応するためのガイドラインです。業務委託先や関連企業におけるセキュリティ対策を目的としています。

NIST SP 800-53 と NIST SP 800-171 は、以下のように保護する情報と対策を行う組織が異なりますが、どちらも密接に関連しているため 2 つ同時に参照する必要があります。

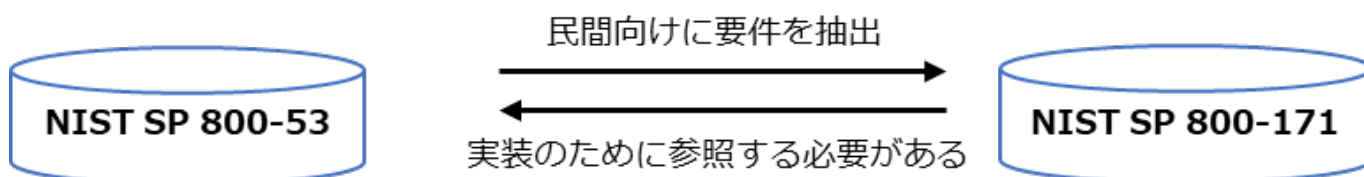


図 41. NIST SP 800-53 と NIST SP 800-171 の関係

11-3-3. ISMS との関連性

CSF と ISMS の主な関係性を説明します。

CSF と ISMS の主な共通点

汎用性が高い

ISMS と CSF は、汎用性が高く、あらゆる組織で使用することができます。まずは ISMS をベースにして情報セキュリティ対策を行い、必要に応じて CSF の内容を取り入れるとよいでしょう。

サイバーセキュリティ対策方法

ISMS と CSF はどちらも「識別」「防御」「検知」「対応」「復旧」といったサイバーセキュリティ対策を挙げています。

任意性がある

ISMS と CSF はどちらも、提示しているすべてのセキュリティ対策を取り入れることは求めているため、何を取り入れるかはそれぞれの組織で決定可能です。

CSF と ISMS の主な相違点

第三者認証制度の有無

ISMS には、第三者機関による認証制度（適合性評価制度）が存在します。これに対して、CSF にはそのような認証制度はありません。そのため、情報セキュリティ対策を行っていることを顧客や取引先に対して客観的に示すためには、ISMS を構築して認証を受けることが有効です。

目標への到達手段

ISMS は、PDCA サイクルをまわすことにより、情報セキュリティマネジメント体制を構築する一方、CSF では特に PDCA サイクルをまわすといった記載はありません。CSF の「プロファイル」では、現在の状況と理想の状況とのギャップを明確にすることにより、取るべき対応策の優先順位を決めて、それにしたがって実施していくことになります。

11-4. サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF)

概要

[Society5.0](#) の到来で、サイバー空間とフィジカル空間が融合することによって、これまでにはなかったさまざまな新たな価値（モノやサービス）が提供されることになります。

[サプライチェーン](#)は、従来の形（例：調達→生産→物流→販売）から、サイバー空間とフィジカル空間のつながりや、サイバー空間のデータのつながりを考える必要がある形へと変化していくことになります。このような新たな形のサプライチェーンは、『価値創造過程（バリュークリエーションプロセス）』と定義されています。

製品を製造して消費者に販売するまでが従来のサプライチェーンだとした場合、バリュークリエーションプロセスでは、消費者の使用データの収集やシステムのアップデートなどを通じて消費者との関係が続きます。サイバー空間とフィジカル空間の接点のすべてが[サイバー攻撃](#)の対象となると考えられ、工場のシステムに加えて、製品そのものに対する攻撃、個人情報などのデータを蓄積した本社に対する攻撃が行われる危険性があります。

このような新たなサプライチェーンの概念に求められるセキュリティへの対応指針として、政府は『[サイバー・フィジカル・セキュリティ対策フレームワーク](#)』（CPSF）を策定しました。

CPSF は、[ISMS](#) や [CSF](#) の [フレームワーク](#) の内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策に対応したフレームワークとなっています。

目的と適用範囲

CPSF の主な目的は、新たな産業社会におけるバリュークリエーションプロセス全体の理解、リスク源の明確化、必要なセキュリティ対策全体像の整理を行うことです。従来のサプライチェーンに適用可能なセキュリティ対策に加えて、新たな産業社会の変化から生じる特有の対策も含まれています。

本フレームワークの適用範囲としては、新たな産業社会におけるバリュークリエーションプロセス全体となります。企業が本フレームワークを参考にし、自社の実態に合わせて、適切なセキュリティ対策を実施することが重要です。

CPSF に含まれる対策

- 従来型サプライチェーンにおいても適用可能な対策
- 新たな産業社会に変化したからこそ新たに対応が必要な対策

- 
- 新たな産業社会におけるバリュークリエーションプロセス全体が適用範囲
 - それぞれの組織に応じてセキュリティ対策を選定することが可能

従来のサプライチェーンに対するセキュリティの考え方では、セキュリティ対応を行っている組織間の取引であれば、サプライチェーン全体の信頼性が確保される「組織マネジメントの信頼性」に基点が置かれていました。

しかしながら、Society5.0 では、従来のサプライチェーンのように、組織のマネジメントの信頼性に基点を置くことだけでは、バリュークリエーションプロセスの信頼性を確保することが困難となります。IoT 機器を使用した場合、フィジカル空間のさまざまな情報はデジタル化され、サイバー空間へ取り込まれ、新たな価値が生まれます。その一方で、マネジメントルールを徹底しただけでは、サイバー空間に取り込んだデータの適切な保護といった信頼性を確保することはできなくなります。

バリュークリエーションプロセスの信頼性を確保するためには、セキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要になります。そのため、CPSF では、バリュークリエーションプロセスが発生する産業社会を 3 つの層、バリュークリエーションプロセスに關与する構成要素を 6 つに整理し、CPSF の基本構成としました。3 つの層でリスク源を洗い出し、6 つの構成要素で各リスク源に対する対策要件および具体的な対策例を示します。

3 層構造モデル

各層における信頼性の基点は以下の通りです。

第 1 層	企業（組織）のマネジメントの信頼性
第 2 層	サイバー空間とフィジカル空間のつながりにおける、要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性
第 3 層	サイバー空間のつながりにおける、データの信頼性

[第 3 層]サイバー空間におけるつながり
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保
[第 2 層]フィジカル空間とサイバー空間のつながり
フィジカル空間・サイバー空間を正確に“転写”する機能の信頼性を確保 (現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラなどの信頼)
[第 1 層]企業間のつながり
適切なマネジメントを基盤に各主体の信頼性を確保

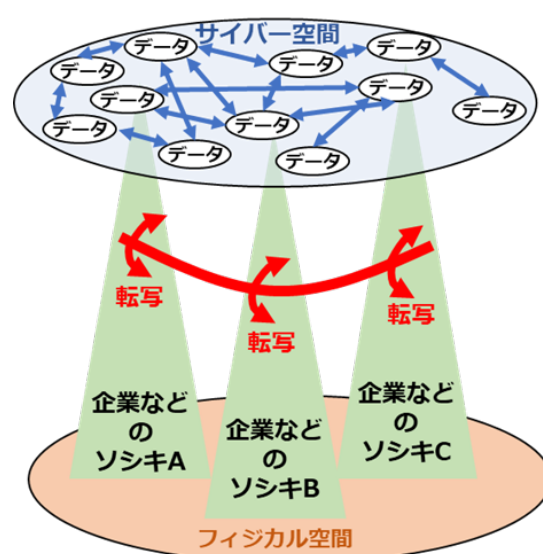


図 42. 層構造モデルと各層における信頼性

(出典) 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークの概要」をもとに作成

11-5. サイバーセキュリティ経営ガイドライン

11-5-1. サイバーセキュリティ経営ガイドライン

経営者が主体となってサイバーセキュリティ対策を実施する際に、経済産業省と独立行政法人情報処理推進機構（IPA）が共同で発行している「サイバーセキュリティ経営ガイドライン」が参考になります。本ガイドラインでは、経営者がサイバーセキュリティ対策を実行する際に認識すべき事項と、サイバーセキュリティ対策の責任者（CISO など）に指示すべき事項を包括的にまとめています。

平成 29 年の Ver2.0 の公開以降、企業のサイバーセキュリティ対策を取り巻く環境が変化しました。そのため、最新の状況への認識と対策の実践が可能となるように内容が見直され、令和 5 年に Ver3.0 が最新版として公開されました。

企業のサイバーセキュリティ対策を取り巻く環境の変化	
テレワークの活用	テレワークなどのデジタル環境の活用を前提とする働き方の多様化
サイバー空間とフィジカル空間のつながり	インターネットなどのサイバー空間と現物の取引を行うフィジカル空間のつながりの緊密化と、それに伴うリスクの顕在化
セキュリティ対象の変化・拡大	<u>情報資産</u> だけでなく、制御系を含むデジタル基盤の保護がサイバーセキュリティの対象となる変化と拡大
<u>ランサムウェア</u> の被害	ランサムウェアによる被害の顕在化により、企業におけるサイバーセキュリティに関する被害は情報漏えいに留まらず、企業の事業活動の停止へと影響が拡大
<u>サプライチェーン</u> を介した被害拡大	国内外のサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、サプライチェーン全体を通じた対策の必要性の高まり
ESG 投資の拡大	ESG（Environment, Society, Governance）投資の拡大により、コーポレートガバナンスおよび ERM（エンタープライズリスクマネジメント）の改善に向けた取組に対する関心の高まり

（出典）経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

次のページからは、サイバーセキュリティ対策に取り組む上で、経営者が認識すべき事項と実行すべき事項を紹介し、経営目線でのサイバーセキュリティ対策について全体像を説明します。また、経営者とセキュリティ担当者それぞれの立場に応じて、具体的に行うべきことについて説明した後、サイバーセキュリティ対策を実践するための手順を説明します。

サイバーセキュリティ対策は企業の価値増大への投資

サイバーセキュリティ対策はやむを得ない「費用」と考えるのではなく、「投資」と位置づけることが重要です。なぜなら、サイバーセキュリティ対策は、企業活動における損失やコストを減らし、企業の価値を維持・増大させるために必要だからです。サイバーセキュリティに関するリスクを経営リスクの一環として取り入れ、適切な対策に投資することによって、リスクを許容可能な範囲まで低減させることができます。企業としては、この取組を通じて社会的責任を果たし、経営者はこの責務を認識する必要があります。

経営者が認識すべき 3 原則

経営者は、以下の 3 原則を認識し、対策を進める必要があります。

原則 1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
原則 2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
原則 3	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営の重要 10 項目

経営者は、以下の重要 10 項目について、サイバーセキュリティ対策を実施する上での責任者や担当部署（CISO、サイバーセキュリティ担当者など）への指示を通じて組織に適した形で確実に実施させる必要があります。これらは、組織のリスクマネジメントの責任を担う経営者が、単なる指示ではなく、自らの役割として発信する必要があります。リスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応など、多くのことを通じてリーダーシップを発揮することが求められます。

経営者がリーダーシップをとったセキュリティ対策の推進

サイバーセキュリティリスクの管理体制構築

指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定

指示 2 サイバーセキュリティリスク管理体制の構築

指示 3 サイバーセキュリティ対策のための資源（予算、人材など）確保

サイバーセキュリティリスクの特定と対策の実装

指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

指示 5 サイバーセキュリティリスクに効果的に対応する仕組みの構築

指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善
インシデント発生に備えた体制構築
指示 7 インシデント発生時の緊急対応体制の整備
指示 8 インシデントによる被害に備えた事業継続・復旧体制の整備
サプライチェーンセキュリティ対策の推進
指示 9 ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握および対策
ステークホルダーを含めた関係者とのコミュニケーションの推進
指示 10 サイバーセキュリティに関する情報の収集、共有および開示の促進

(出典) 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

サイバーセキュリティ経営の重要 10 項目の概要

経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO など）に指示すべき「重要 10 項目」のポイントと、対策例の一部を紹介します。

指示 1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（<u>セキュリティポリシー</u>）を策定させる。 - 策定した対応方針を対外的な宣言として公表させる。 対策例 - 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取ったセキュリティポリシーを策定する。その際、製造、販売、サービス等、事業が立脚している全ての基盤（設備、システム、情報等の資産、流通プロセス等）に影響を及ぼすと考えられるサイバーセキュリティリスクに応じた対応方針を検討する。
指示 2 サイバーセキュリティリスク管理体制の構築
- サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構成させる。 - サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。 対策例 - 役割遂行に求められる責任や専門性、人的資源の状況に応じて、組織内要員で対応すべきものと外部の専門サービスに委託すべきものの切り分けを行う。 - 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを監査する。
指示 3 サイバーセキュリティ対策のための資源（予算、人材等）確保
サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討さ

せ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。

- 全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

対策例

- 事業が立脚している全ての基盤の安全性の担保のために必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。
- 従業員向けやセキュリティ担当者向けなどの研修等のための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門等のあらゆる業務に従事する人材に、「プラス・セキュリティ」知識・スキルの習得を促す。

指示 4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

- 事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダーへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

対策例

- 組織における情報のうち、経営戦略の観点から守るべき情報を特定し、それらがどこに保存され、どこで扱われているかを把握する。その際、自社の営業秘密を外部のクラウドサービスで管理したり、テレワーク等の新しい働き方を導入したりしていることの影響を適切に反映させる。

指示 5 サイバーセキュリティリスクに効果的に対応する仕組みの構築

- サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

対策例

- 重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する。
- 従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

指示 6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

対策例

- 必要に応じて、ISO/IEC 27001 規格に基づく [ISMS](#) など、国際標準となっている PDCA マネジメントシステムの認証を活用する。

指示 7 インシデント発生時の緊急対応体制の整備

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（[CSI](#) [RT](#) 等）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- インシデント発生時の対応について、適宜実践的な演習を実施させる。

対策例

- インシデント発生時の体制整備、ルール整備にあたって、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照しながら、社内理解を深める。
- インシデントの発生を想定した緊急対応に関する演習を役員に対して定期的の実施し、緊急時にどのような手順で初動対応を行うべきかについて、全ての関係者が体験を通じて理解する。

指示 8 インシデントによる被害に備えた事業継続・復旧体制の整備

- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- 制御系も含めた [BCP](#) との連携等、組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
- 業務停止等からの復旧対応について、対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

対策例

- 設備投資計画を立案する際に、事業継続に影響をもたらす要因として、自然災害やパンデミック等にサイバーセキュリティリスクを加え、その対策を要求仕様等に反映させる。
- 定期的な復旧演習の実施により、復旧対応に関わる関係者がその手順について、体験を通じて理解する。

指示 9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

- サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。
- ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

対策例

- 系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等が [SECURITY ACTION](#) を実施していることを確認する。なお、ISMS 等のセキュリティマネジメント認証を取得していることがより効果的である。

指示 10 サイバーセキュリティに関する情報の収集、共有及び開示の促進

- 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
- 入手した情報を有効活用するための環境整備をさせる。

対策例

- 株主やステークホルダーとの対話、広報による一般向け情報開示等の機会において、サイバーセキュリティインシデントに備えた日頃の取組等の情報開示に積極的に取り組む。
- 中小企業の場合は、商工会議所、商工会等を通じて地元で情報共有を行うことのできる相手確保する。
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参考に、インシデントに備え、サイバーセキュリティ専門組織との情報共有や被害に係る情報の公表を行うにあたっての観点について、あらかじめ理解しておく。

詳細理解のため参考となる文献（参考文献）

サイバー攻撃被害に係る情報の共有・公表ガイダンス

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

（出典）経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

11-5-2. サイバーセキュリティ経営ガイドラインの読み方

ここでは「経営者」、「情報セキュリティ対策の責任者（CISO など）」それぞれの立場から、本ガイドラインの内容を実践する際の役割、認識すべきことについて記載します。

対象者	経営者
役割	● 「3 原則」の理解 ● 重要 10 項目について、情報セキュリティ対策の責任者（CISO など）に指示を出す

	● リーダーシップの発揮
認識すべきこと	ERM（エンタープライズリスクマネジメント）にサイバー攻撃のリスクを含めること 現在、企業活動の多くは IT に依存しています。そのため、内部統制システムの構築や、コーポレートガバナンス・コードに基づく開示と対話などにおいて、<u>サイバー攻撃</u>のリスクを考慮する必要があります。 サプライチェーン上のリスクを認識すること 現在、サプライチェーンの多様化が進み、サイバー攻撃の起点は広く拡散しています。したがって、サプライチェーン全体を考慮したリスクマネジメントが必要です。 サイバーセキュリティ対策は担当者に丸投げしてはいけない 経営者は、インシデント発生時に法的・社会的責任を負い、事業停止や新たな脅威に対処するための経営判断を迫られることがあります。そのため、経営者は、サイバーセキュリティ対策を担当者に丸投げせずに、自ら主体的に取り組む必要があります。 サイバーセキュリティ対策は投資と位置づけること サイバーセキュリティ対策への投資では、直接的な収益を算出することは困難です。しかし、サイバーセキュリティ対策への投資は、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、将来の事業活動・成長に必須な投資でもあります。



（出典）経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

ERM（エンタープライズリスクマネジメント）とは
企業が直面するリスクに対して、企業全体で管理することです。国際競争や情報技術の急速な進化により、企業が直面するリスクも多様化しています。このような状況下で、従来の部門ごとにリスクに対して管理するのではなく、企業全体で管理することが重要です。

対象者	情報セキュリティ対策を実施する上で責任者となる担当幹部（CISO など）
役割	● 重要 10 項目を理解すること ● 経営者に対して適宜状況報告を行い、経営者が適切な判断を行うために必要な情報を提供すること

認識すべきこと

経営者から指示される以下の事項に関して、より具体的な取組を検討し、セキュリティ担当者に対して指示する必要があること

- サイバーセキュリティリスクの管理体制構築
- サイバーセキュリティリスクの特定と対策の実装
- インシデント発生に備えた体制を構築
- サプライチェーンセキュリティ対策の推進
- ステークホルダーを含めた関係者とのコミュニケーションの推進

(出典) 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

11-5-3. サイバーセキュリティ経営ガイドラインの実践の流れ

サイバーセキュリティ経営ガイドラインの活用手順

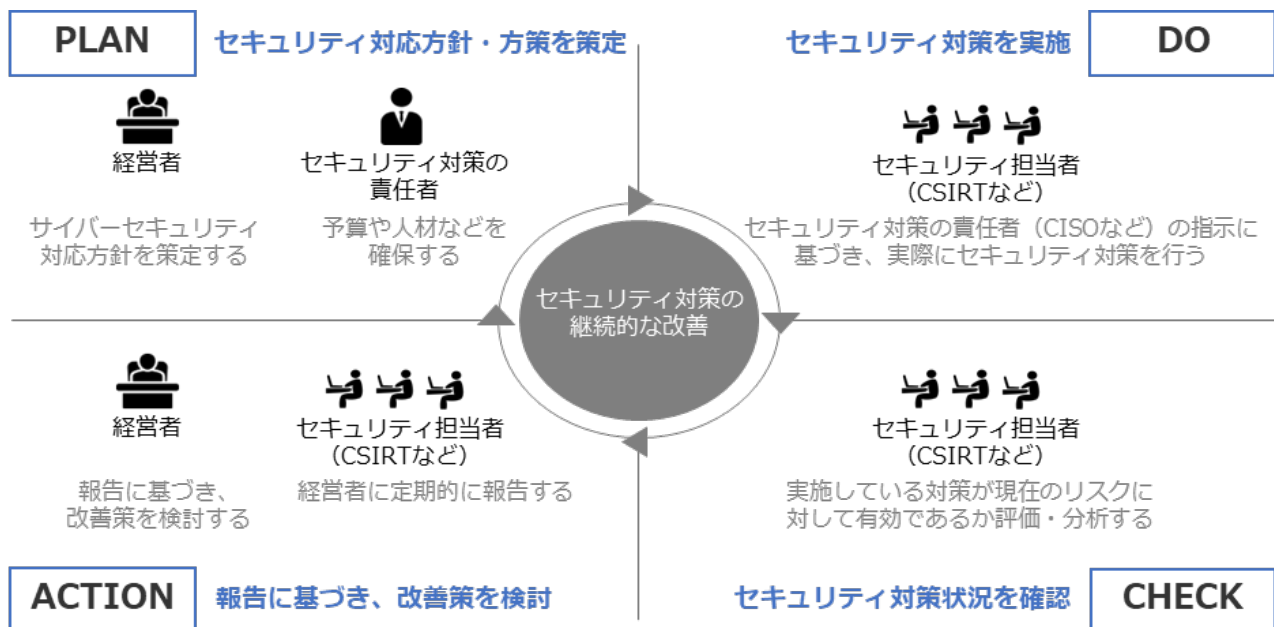


図 43. サイバーセキュリティ経営ガイドラインの全体の流れ

(出典) 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」をもとに作成

PLAN

はじめに、サイバーセキュリティ対応方針・方策を策定します。

- 経営者は、3 原則を認識した上でサイバーセキュリティ対応方針を策定します。
- セキュリティ対策の責任者（CISO など）は、経営者の指示に基づき、リスクを許容範囲内に抑制するための方策を検討し、必要となる資源（予算や人材など）を確保します。

DO

セキュリティ担当者（CSIRT など）は、セキュリティ対策の責任者（CISO など）の指示に基づき、実際にセキュリティ対策を行っていきます。具体的には以下の作業を行います。

- リスクの把握や対応計画の策定
- サイバー攻撃の防御や検知
- 分析などの保護対策の実施
- 緊急時の対応体制を整備、事業継続、復旧体制の整備

CHECK

実施しているセキュリティ対策がリスクに対して有効であるか評価・分析をします。

- セキュリティ担当者（CSIRT など）は、サイバーセキュリティ経営ガイドライン付録の「サイバーセキュリティ経営チェックシート」や「サイバーセキュリティ経営可視化ツール」を活用し、経営者が指示した事項の実践状況をチェックします。

ACTION

セキュリティ担当者（CSIRT など）は、経営者に指示された事項の実践状況について、CISOを通じて経営者に報告し、経営者は報告をもとに改善策を検討します。

- 新たなサイバーセキュリティリスクの発見などにより、追加の対応が必要な場合には、対処方針を修正します。

第12章. リスクマネジメント

章の目的

第 12 章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方について学ぶことを目的とします。

主な達成目標

- リスクマネジメントの意義について理解すること
- リスクマネジメントプロセスの全体像を理解すること
- リスクアセスメント、リスク対応のプロセスを理解すること

12-1. リスクマネジメント：概要

12-1-1. リスクマネジメントプロセス（ISO31000）

企業や組織にはさまざまなリスクが存在しています。これらのリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のことを「リスクマネジメント」と言います。

リスクマネジメントの国際規格として ISO 31000 があります。ISO 31000 では、リスクマネジメントを「原則」「枠組み」「プロセス」の 3 つの要素から構成されるものとして捉えています。

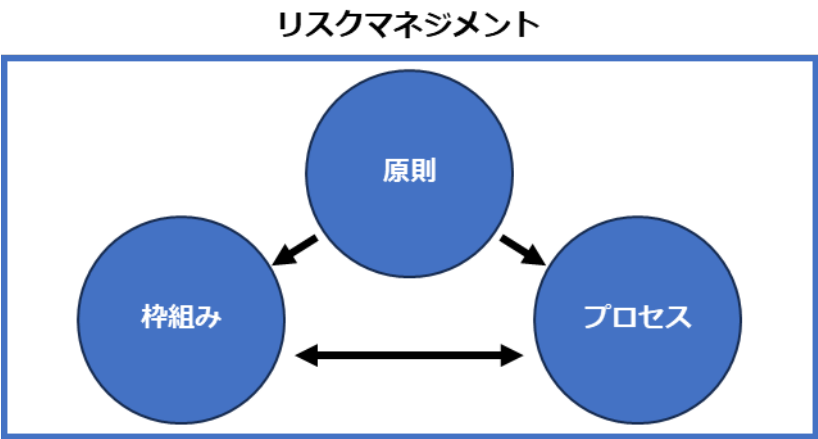


図 44. リスクマネジメントの 3 要素

原則	リスクマネジメントを実施する際に、組織が取り組むべき事項です。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」「利用可能な最善の情報」「人的及び文化的要員」「継続的改善」で構成されています。
枠組み	リスクマネジメントを組織全体に定着させるための仕組みです。 「統合」「設計」「実施」「評価」「改善」で構成されています。
プロセス	リスクマネジメントに取り組む上で実施すべき、一連の活動です。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」「 リスクアセスメント 」「リスク対応」「モニタリング及びレビュー」「記録作成及び報告」で構成されています。

実際にリスクに対応していくにあたっては、リスクマネジメントプロセスにおける「リスクアセスメント」が必須事項となります。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位づけをしていくプロセスのことを表します。リスクアセスメントの実施により、個々の資産が持つリスクと、リスクに対する管理策、および管理策に投じるべき費用の識別が期待できます。また、リスクを評価するということは[情報資産](#)の持つ固有の弱点や脅威を明確にする過程を含みます。そのため、事前にリスクを把握することにより必要な投資額を含め、適切な対策を検討することが可能になります。

12-1-2. 情報セキュリティリスクマネジメント (ISO/IEC27005)

ISO/IEC 27005 は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。先に説明した ISO31000 と整合性がありますが、情報セキュリティに特化した内容になっています。この規格は、組織の情報資産を安全に保つことに焦点が当てられており、情報セキュリティリスクの特定、分析、評価、対応、管理、レビューなどを実施するための手引きになっています。中小企業を含むすべての組織における情報セキュリティリスクのマネジメントに有用です。

ISO/IEC 27005 の情報セキュリティリスクマネジメントプロセスは、ISO 31000 の一般的なリスクマネジメントプロセスに基づいており、リスクの特定、リスクの評価、リスクの対処およびリスクの監視とコントロールに関するステップから構成されます。以下の図で示すように情報セキュリティリスクマネジメントプロセスは循環しており、反復的に実施されるものです。組織を取り巻く環境の変化や組織内の変化に応じて、新しいリスクが発生したり、既存のリスクが変化したりする上に、リスクへの対処法も進化するからです。特に、リスクマネジメントプロセスに含まれているリスクアセスメントは、リスク対応の方策や、対応の優先順位づけの前提になる重要な工程です。

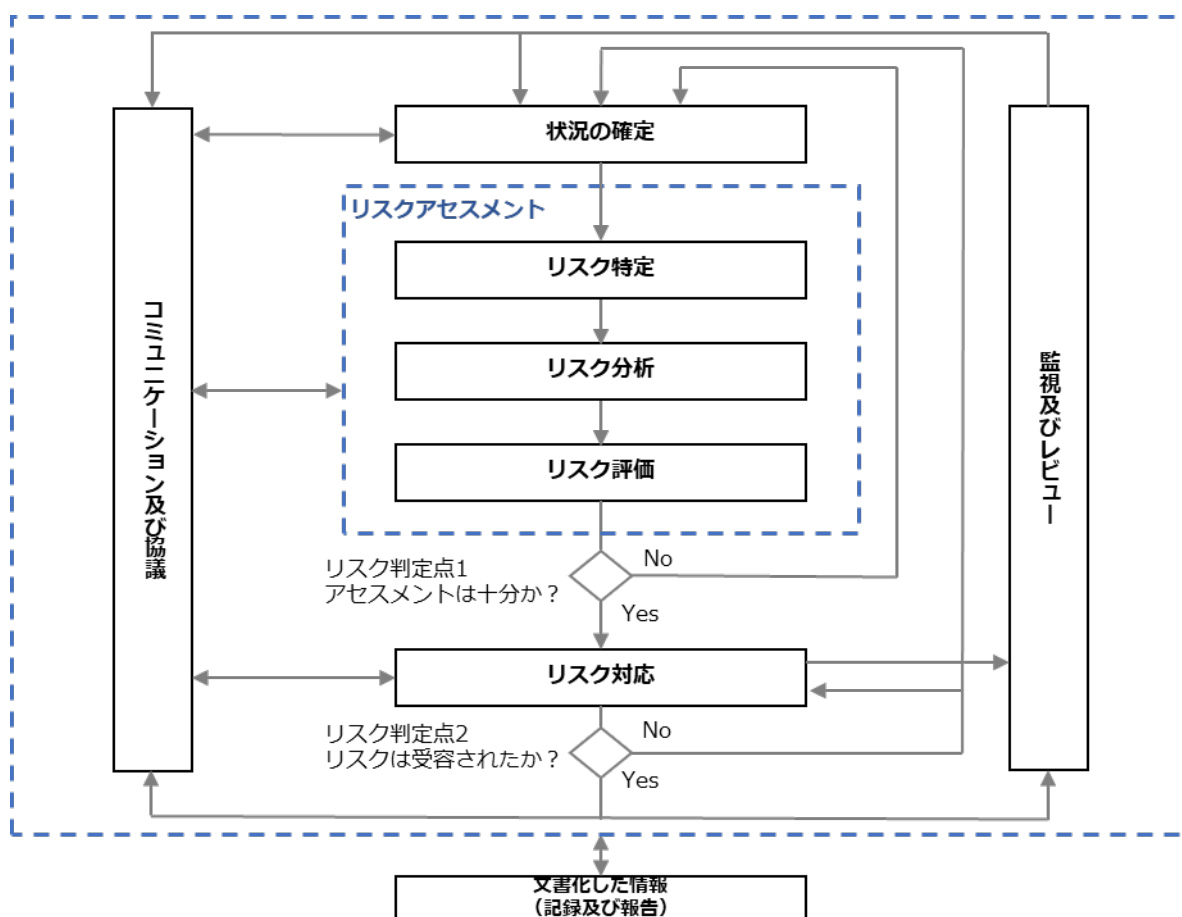


図 45. 情報セキュリティマネジメントプロセスの概要
(出典) ISO/IEC 「ISO/IEC 27005:2022」 をもとに作成

リスクアセスメントからリスク対応までの流れを表す図を記載します。リスク対応を実施する過程では、「低減」「移転」「回避」「受容（保有）」の4つ選択があり、それらの選択は以下の図で示すプロセスで行われます。

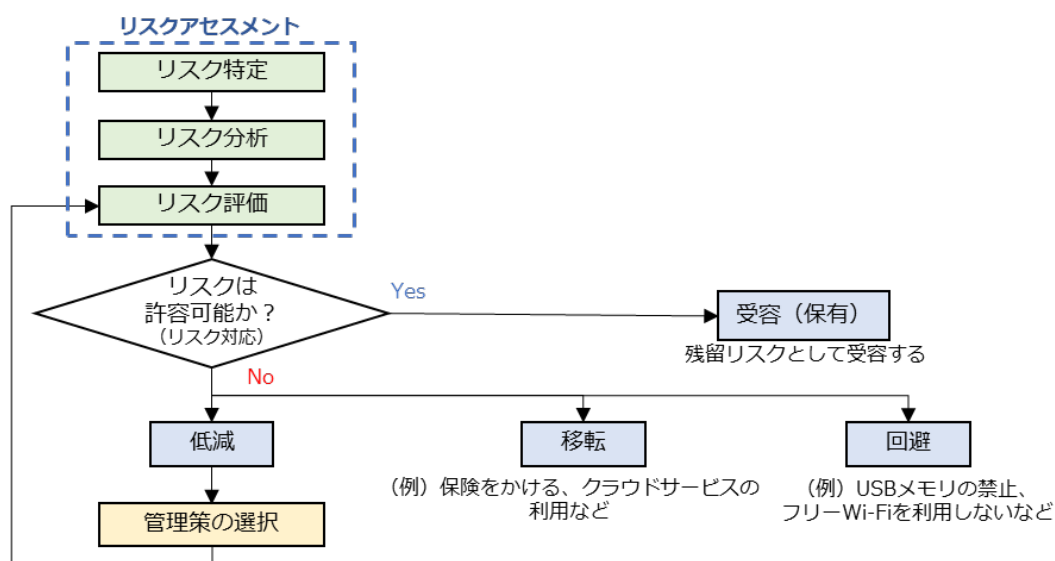


図 46. リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することによって、脆弱性を改善し、事故が起きる可能性を下げます。

リスクを受容（保有）する

事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

（例）

- 従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する。
- インターネットバンキングに使用するパソコンでメールや Web サイトの閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールや Web サイトの閲覧に利用せず、USB メモリ、外付け HDD も接続を禁止する。

リスクレベルが大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できなかったりする場合は「リスクの移転」を検討します。

リスクを移転する

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することにより自社の負担を下げます。

(例)

- 商品を販売する Web サイトではクレジットカード番号を非保持化し、代金の決済はセキュリティ対策を十分行っている外部の決済代行サービスに変更する。
- 社内のサーバで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する。
- 情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する。

(出典) IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」をもとに作成

12-1-3. ISO/IEC 27001 におけるリスクマネジメント手順

ISO/IEC 27005 は、情報セキュリティリスクマネジメントの手法を提供する規格であり、ISO/IEC 27001 (ISMS) は情報セキュリティマネジメントシステムの設計と実装に関する規格です。つまり、ISO/IEC 27001 は情報セキュリティマネジメントシステムの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005 になります。ISO/IEC 27001 ([ISMS](#)) の活動は、ISO/IEC 27005 におけるリスクマネジメントプロセスと関連付けて整理することが可能です。

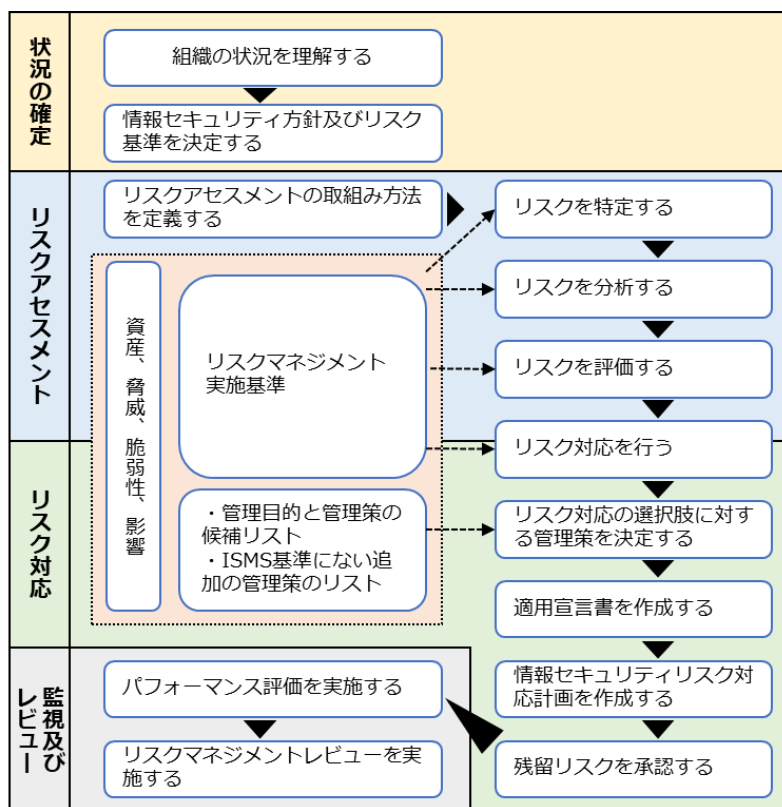


図 47. ISMS におけるリスクアセスメントおよびリスク対応に関する作業の概要

12-2. リスクマネジメント：リスクアセスメント

12-2-1. リスク基準の確立

必要なリスク基準

リスクアセスメントを実施するにあたって、リスクの重大性を評価するための目安となる条件を決める必要があります。その条件のことをリスク基準と言います。ISMSでは、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むよう明示されています。

リスク受容基準

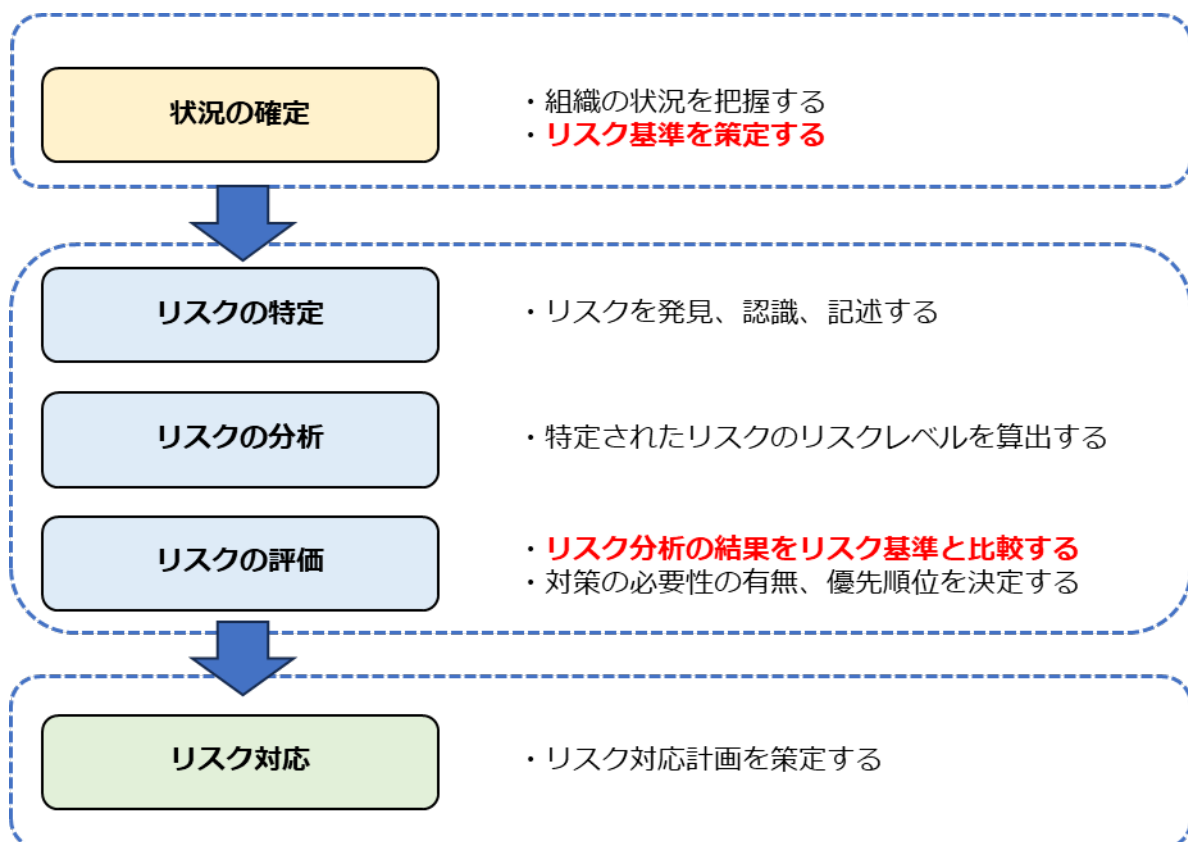
どの程度のリスクであれば受け入れることが可能かの判断基準です。

あるリスクに対して、どの程度のレベル感や優先順位でリスク対応を実施するのか、リスクが顕在化した際にどの程度の大きさまでなら許容するのかを明確にする必要があります。

情報セキュリティリスクアセスメントを実施するための基準

いつ、どのようなときにリスクアセスメントを実施するのかを決める要件です。

リスクアセスメントの実施条件や実施時期、タイミングや頻度などを明確にする必要があります。



12-2-2. リスクの特定

リスク特定

リスクアセスメントの1つ目のプロセスである「リスク特定」について説明します。リスク特定とは、「リスクを発見、認識及び記述するプロセス」¹⁶のことです。リスク特定を実施するために一般的に使用されるアプローチは「資産ベースのアプローチ」および「事象ベースのアプローチ」の2つがあります。

【情報セキュリティリスクの特定および記述】

アプローチ手法	概要	メリット	デメリット
資産ベースのアプローチ	● 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 ● 資産は、その種類及び優先度にしたがって主要資産及び支援資産として特定できる。 ● 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 ● 資産のリストを作成することが望ましい。	● 資産、脅威及び脆弱性のすべての有効な組み合わせをISMSの適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	● 情報資産が増えたときに、資産のリストの行数が多くなる。 ● 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	● 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。	● 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高	● 網羅性において、資産ベースのアプローチに劣る。

16 JISC 日本産業標準調査会。“JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”。<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

	● 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び組織の状況を決定する際に特定された要求事項によって発見できる。	いレベルまたは戦略的なシナリオを確立することができる。	

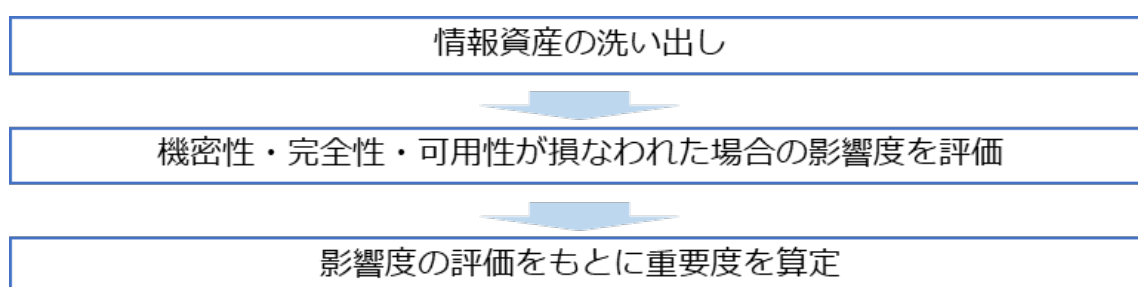
(出典) ISO/IEC「ISO/IEC 27005:2022」をもとに作成



リスク所有者の特定	● 特定されたリスクに対し、リスク所有者を関連付ける。 ● リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする（通常、組織内で一定の権限を持つ人が選ばれる）。

リスク特定（資産ベースのアプローチ）

資産ベースのアプローチでは、はじめに情報資産を洗い出し（資産目録の作成）、その過程でリスク所有者を特定します。リスク所有者とは、リスクが顕在化した際に責任を取る人のことを指します。その後、情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合、事業にどれほど影響があるか評価を行い、重要度を判断します。



情報資産の洗い出し（例）

情報資産の洗い出しでは、業務で利用する電子データや書類などを特定し、資産目録を作成します。洗い出した情報資産は、「営業」「人事」「経理」など管理部門ごとに分類します。企業活動に大きな影響を与えかねない重要な情報を、できる限り漏れないように洗い出すことが重要です。影響がほとんどない情報であれば、漏れても大きな問題はありません。情報資産の洗い出しの粒度は、

細かすぎると管理が大変ですが、逆に粗いと次のリスク分析が難しくなります。そのため、適度な粒度にすることが重要です。以下は、情報資産のリストアップ例です。

No	情報分類	情報資産 名称	備考	利用者範 囲	リスク 所有者	管理 部署	媒体・保 存先
1	人事	従業員名簿	従業員基本情報	人事部	人事部 長	人事 部	事務所 PC
2	人事	健康診断 の結果	雇入時・定期健康診断	人事部	人事部 長	人事 部	書類
3	経理	給与シス テムデー タ	税務署提出用源泉徴収 票	給与計算 担当	経理部 長	人事 部	事務所 PC
4	経理	当社宛請 求書	当社宛請求書の原本 (過去 3 年分)	総務部	経理部 長	総務 部	書類
5	経理	発行済請 求書 控え	当社発行の請求書の控 え (過去 3 年分)	総務部	経理部 長	総務 部	書類
6	営業	顧客リス ト	得意先 (直近 5 年間に 実績があるもの)	営業部	営業部 長	営業 部	可搬電子 媒体
7	営業	受注伝票	受注伝票 (過去 10 年 分)	営業部	営業部 長	営業 部	社内サー バ
8	営業	受注契約 書	受注契約書原本 (過去 10 年分)	営業部	営業部 長	営業 部	書類

資産目録の例

(出典) IPA「リスク分析シート」をもとに作成

電子化された情報を洗い出す際は、「普段パソコンで見ているこのデータは、どこに保存されているのだろう」というように、社内の IT 機器や利用しているクラウドサービスを思い浮かべて記入します。また、複数の組織を持つ企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

資産目録を作成する際、情報資産を情報、情報を支援する資産として「主要/事業資産」と「支援資産」2つのカテゴリに分類して整理する方法も有効です。

「主要/事業資産」

「主要/事業資産」とは、「組織にとって価値のある情報又はプロセス」¹⁷のことです。主要資産

¹⁷ ISO." ISO/IEC 27005:2022". <https://www.iso.org/standard/80585.html>

は、「事業プロセス及び事業活動」と「情報」の2つに分けられます。

「事業プロセス及び事業活動」の例

- その損失又は低下によって、組織の使命達成が不可能となるプロセス
- 機密プロセス又は専有技術を伴っているプロセス
- 修正された場合、組織の使命の達成に大きく影響するプロセス
- 組織が契約、法令又は規則の要求事項を遵守するために必要となるプロセス

「情報」の例

- 組織の使命又は事業の遂行に不可欠の情報
- プライバシーに関する国内法に言う意味で、特別に定義することができる個人情報
- 戦略的方向性によって決定される目的の達成に必要な戦略情報
- 収集、保管、処理、送信に長時間を要する高コスト情報および高い取得費用を伴う情報

「支援資産」

「支援資産」とは、「1 つ以上の事業資産の基礎となる情報システムの構成要素」¹⁸のことです。

「支援資産」の例

- ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織

(出典) MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成



情報資産のグループ化

ISMS 適用範囲に存在する情報資産を洗い出す作業は、負荷が非常に大きくなりやすいです。そこで、資産価値や保管形態、保管期間や用途などが同じものを 1 つのグループとしてまとめて管理することにより、作業負荷を軽減したり、作業を効率化したりすることができます。

(例) 事務所内のパソコンで会計ソフトウェアや表計算ソフトウェアを使って帳簿を作成している場合

・ 仕訳帳 ・ 総勘定元帳 ・ 現金出納帳 ・ 当座預金出納帳 ・ 小口現金出納帳 ・ 仕訳帳 ・ 売上帳	} 情報資産名称：「会計データ」 「会計データバックアップ」 (バックアップを取っている場合) など
	媒体・保存先：「事務所PC」(会計ソフトの保存先) 「可搬電子媒体」 (USBメモリがバックアップ保存先)

機密性・完全性・可用性が損なわれた場合の影響度を評価

情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合の事業への影響度を評価します。

18 ISO." ISO/IEC 27005:2022". <https://www.iso.org/standard/80585.html>

具体例として、以下の評価基準を参考に「機密性」「完全性」「可用性」それぞれの評価値（3～1）を決定します。

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	個人情報（個人情報保護法で定義） 特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている	取引先から秘密として提供された情報
		漏えいすると取引先や顧客に大きな影響がある	取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	自社の独自技術・知識 取引先リスト 特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	自社製品カタログ ホームページ掲載情報
完全性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	個人情報（個人情報保護法で定義） 特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	取引先から処理を委託された会計情報 取引先の口座情報 顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	自社の会計情報 受発注・決済・契約情報 ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	廃版製品カタログデータ
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	顧客に提供している EC サイト 顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響	製品の設計図

		がある	商品・サービスに関するコンテンツ (インターネット向け事業の場合)
	1	利用できなくなっても事業にほとんど 影響はない	廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義

(出典) IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」をもとに作成

影響度の評価をもとに重要度を算定

重要度の算出例を説明します。重要度は「機密性」「完全性」「可用性」いずれかの評価値の最大値で判断します。なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果に関わらず、重要度は3とします。

情報資産の価値・事故の影響の大きさ		
重要度	3	事故が起きると、「法的責任を問われる」「取引先、顧客、個人に大きな影響がある」「事業に深刻な影響を及ぼす」など、企業の存続を左右しかねない
	2	事故が企業の事業に重大な影響を及ぼす
	1	事故が発生しても事業にほとんど影響はない

重要度の判断例：自社のホームページ（電子データ）		評価値
「機密性」	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	⇒ 1
「完全性」	<u>不正アクセス</u> で価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	⇒ 3
「可用性」	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	⇒ 3
➡完全性と可用性の評価値3が最大値なので、重要度は評価値：3		

重要度の判断例

(出典) IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」をもとに作成



重要度を判断する際のポイント

- 重要度の判断は、立場や見識によっても異なることがあるので、情報資産管理台帳に記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
- 情報資産の「重要度」は、時間経過とともに変化することがありますが、現時点の評価値を記入します。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合

は、最大値で評価します。

リスク特定（事象ベースのアプローチ）

事象ベースのアプローチでは、従業員の業務プロセスを起点にリスクを特定します。それにより、詳細なレベルで資産を特定することに多大な時間を費やすことなく、戦略的なシナリオを確立することができます。その結果、組織は自らのリスク対応の取組を、重大なリスクに集中させることができます。

前述の資産ベースのアプローチに比べると網羅性に劣るというデメリットはありますが、その分、日々の業務をもとにして洗い出すため、現実的なリスクを洗い出すことができるというメリットがあります。また、資産ベースのアプローチの際、情報資産の洗い出しにより出てきた主要資産（事業プロセスおよび事業活動）に対しても、事象ベースのアプローチでリスク特定が可能です。

1. リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 （例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」
2. リスク所有者の特定	1. で特定されたリスクの所有者を記載します。

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	〇〇〇〇
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響を及ぼす事象である	3		

事象ベースのアプローチによるリスク特定の例

（出典）MSOA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」をもとに作成

上記内容でリスク特定を実施した後、特定されたリスクおよび「重要度」に対して後述のリスク分析を実施します。

12-2-3. リスクの分析

リスク分析（例）

特定されたリスクに対して「リスク分析」を行います。リスク分析とは、「リスクの性質を理解し、リスクレベルを決定するプロセス」¹⁹のことです。リスクレベル（リスクの大きさ）は、優先的・重点的に対策が必要な情報資産を把握するために使用されます。リスクレベル（リスクの大きさ）を算定するにはさまざまな方法があります。算定方法の一例を以下に示します。

$$\text{「リスクレベル」} = \frac{\text{「重要度」}}{\text{「被害発生可能性」}}$$

※リスク特定で算出方法を説明

被害発生可能性の算出方法

「被害発生可能性」とは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の2つの数値を「被害発生可能性の換算表」に当てはめて算出します。

起こりやすさ（脅威）		つけ込みやすさ（脆弱性）	
3	通常の場合で脅威が発生する （いつ発生してもおかしくない）	3	対策を実施していない （ほぼ無防備）
2	特定の状況で脅威が発生する （年に数回程度）	2	部分的に対策を実施している （一部対策を実施）
1	通常の場合で脅威が発生することはない （通常発生しない）	1	必要な対策をすべて実施している （対策を実施）

被害発生可能性の換算表		つけ込みやすさ（脆弱性）		
		3	2	1
起こりやすさ （脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

¹⁹ JISC 日本産業標準調査会, "JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語", <https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

被害発生可能性の算出例

脅威の起こりやすさ：「2」、脆弱性のつけ込みやすさ：「2」

➡ 被害発生可能性は「1」：通常の場合で被害が発生することはない

脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「2」

➡ 被害発生可能性は「2」：特定の状況で被害が発生する（年に数回程度）

脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「3」

➡ 被害発生可能性は「3」通常の場合で被害が発生する（いつ発生してもおかしくない）

12-2-4. リスクの評価

リスク評価

リスク評価とは、「特定・評価したそれぞれのリスクが、受容可能か否かを評価するプロセス」のことです。リスク分析で算出したリスクレベルを、リスク基準（リスク受容基準）と比較し、リスク対策が必要か否かを判断します。また、リスクレベルをもとに対策の優先順位をつけます。

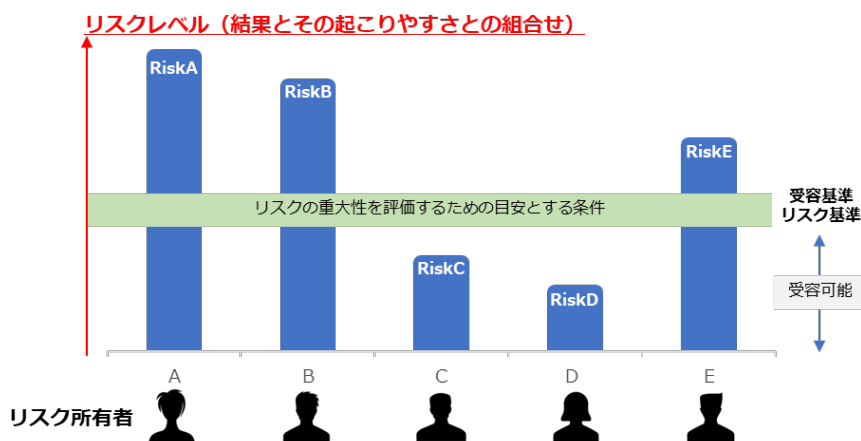


図 48. リスク評価の概要図

（出典）MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

リスク評価（例）

「重要度」 × 「被害発生可能性」でリスクレベルを算出し、リスク評価を行います。例として、算出したリスクレベルを以下の表に当てはめて行います。

リスクレベルの評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

※リスクレベル＝「重要度」×「被害発生可能性」

※赤色、黄色、青色の網掛けは以下のリスク受容基準を示す

リスク受容基準（例）

リスクレベル	リスク評価	記述
低（青）	そのまま受容可能	それ以上の活動なしにリスクを受容可能
中（黄）	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高（赤）	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい。そうでない場合、活動の全部又は一部を拒否することが望ましい

（出典）ISO/IEC「ISO/IEC 27005:2022」をもとに作成

また、情報セキュリティリスクの場合、以下の図で示す考え方をすることが多いです。以下の図では、発生頻度が高く被害が非常に大きいものについては「回避」、発生頻度は低いが被害が大きいものについては「移転」、発生頻度は高いが被害が大きいものについては「低減」を検討するという考え方を示しています。

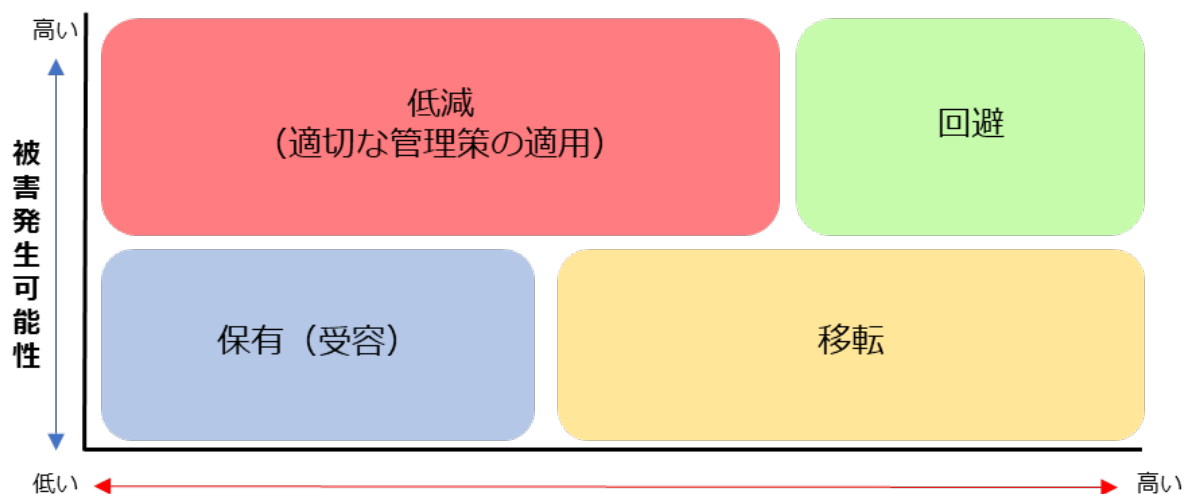


図 49. 情報セキュリティリスクの考え方

（出典）JNSA. “2-4 リスクアセスメントとリスク対応”. <https://www.jnsa.org/ikusei/01/02-04.html>

12-3. リスクマネジメント：リスク対応

リスク対応プロセス

リスク対応とは、「リスクを修正するプロセス」²⁰のことです。[リスクアセスメント](#)プロセスの結果に基づいており、リスク基準に基づき対応すべき優先順位づけされたリスクに対応する内容となります。

1. 適切な情報セキュリティリスク対応の選択肢の選定

リスク対応の選択肢は以下の通りです。

リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。例えば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して自分たちの責任範囲外にし、リスクが顕在化したときの損失を他者に引き受けさせることです。例えばクラウドサービスのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほほない場合が該当します。

2. 情報セキュリティリスク対応の選択肢の実施に必要な全ての管理策の決定

ISO/IEC 27001:2022 の附属書 A、ISO/IEC 27017 などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な全ての管理策を決定します。

3. 決定した管理策と ISO/IEC 27001:2022 附属書 A の管理策との比較

必要な全ての管理策を、ISO/IEC 27001:2022 附属書 A に挙げられている管理策と比較します。

4. 適用宣言書の作成

20 JISC 日本産業標準調査会。“JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”。<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

必要な全ての管理策と、その理由及び実施状況を文書化します。適用宣言書に含まれる全ての管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。

5. 情報セキュリティリスク対応計画

組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。

組織の必要な管理策を実施するためのプロジェクト計画とは、リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画のことです。

6. リスク所有者による承認

リスク所有者は、リスク対応計画を承認します。

7. 残留している情報セキュリティリスクの受容

リスク所有者は、残留リスクが受容可能か否かを判断し、決定します。

(出典) ISO/IEC「ISO/IEC 27005:2022」をもとに作成

リスク対応プロセス（例）

例：自社のホームページ（電子データ）

リスクの内容

不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失ったりする

リスク対応

リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）

対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する

対応する管理策：5.15 アクセス制御

対策基準の策定（対策基準の例）

技術的対策

- 公開サーバへの不正アクセス対策
- 公開サーバへのアクセス権の最小化と管理の強化
- 多要素認証の設定の有効化

残留リスク

残留リスクとは、「リスク対応後に残っているリスク」²¹のことです。残留リスクを受容するためには、リスク所有者の承認が必要になります。受容可能だと判断された残留リスクであっても、資産の価値や脅威、脆弱性など環境の変化に合わせて、リスクレベル（リスクの大きさ）を見直し、必要に応じて追加のリスク対応を行う必要があります。

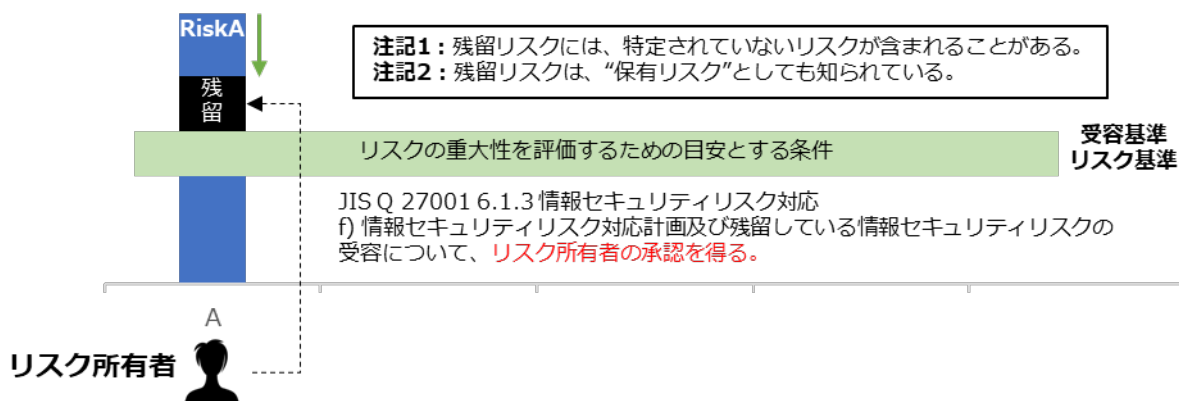


図 50. 残留リスクの概要

(出典) MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

21 JISC 日本産業標準調査会。“JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”。<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

編集後記

第6編では、①ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワーク、②リスクマネジメントやリスクアセスメントの手法、リスク対応の考え方について説明しました。

セキュリティ対策はやみくもに進めると、対策が複雑になり、余計に手間がかかり、内容に抜け漏れが発生する可能性があります。漏れなく効果的に対策を実施するために、セキュリティフレームワークを使用し、自社の課題・目的に即した対応方針を選択する必要があることを、11章を通じて理解していただければと思います。

組織を取り巻く環境や組織が持つ情報資産の変化に応じてリスクもまた流動的に変化するため、リスクマネジメントプロセスを繰り返し実施していくことが重要です。リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることは、容易ではありません。リスクマネジメントプロセスにおける各段階での考え方や手法、フレームワークを用いることにより、円滑なリスク特定、分析と対応策の検討を実施できることを、12章を通じて理解していただければと思います。

今回は、Lv.3 網羅的アプローチで使用する ISMS の要求事項や構築などについて説明します。

第13章. ISMS の要求事項と構築（Lv.3 網羅的アプローチ）

章の目的

第 13 章では、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する Lv.3 網羅的アプローチについて理解することを目的とします。

主な達成目標

- Lv.3 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

13-1. 【Lv.3 網羅的アプローチ】の概要

Lv.3 網羅的アプローチでは、フレームワークとして ISMS を用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。第 13 章では、ISMS における PDCA サイクルを回すために重要となる文書化の方法や、実施すべき事項について焦点を当てて説明していきます。

ISMS の要求事項に関連する文書化は重要ですが、あくまで手段であり目的ではありません。文書化と維持が目的化してしまうと、文書が形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。文書を精細に作り込むことより、ISMS マネジメントプロセスを取り入れ、PDCA サイクルを回していくことが大切です。ISMS に取り組み始めたときには理解できていても、文書作りを始めると文書化が目的になってしまうケースが多いため、注意が必要です。本来、ISMS の認証取得のために作成する文書は、実施すべきことを記述したものではなく、実際に実施していることを記述したものであるべきなのです。

Lv.3 網羅的アプローチ（網羅性のあるアプローチ方法）

概要	メリット	デメリット
網羅的なフレームワークとして ISMS を参考にします。ISMS のフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。	ISMS 要求事項の導入が可能です。	時間とコストがかかる。

13-2. 【Lv.3 網羅的アプローチ】フレームワークを参考とした実施手順

13-2-1. ISMS の概要（確立・運用・監視）

ISO/IEC 27001 各要求事項の概要

「1. 適用範囲」に記述されていますが、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの7項目となっています。

ISO/IEC 27001:2022 の構成	
1. 適用範囲 ISO/IEC 27001 は <u>ISMS</u> 運用のための要求事項を規定しており、本規格に適合するためには4～10に規定されるすべての事項に対応しなければならない。	6. 計画 ISMS の計画を立てる際の要求事項。(PDCA サイクルの P「Plan」)
2. 引用規格 ISO/IEC 27001 は、ISO/IEC 27000 (ISMS の概要と用語) を引用する。	7. 支援 構成員の教育など、ISMS 構築にあたり組織が構成員に行うべきサポートを要求している。
3. 用語および定義 ISO/IEC 27001 で用いる用語および定義は、ISO/IEC 27000 に定めている。	8. 運用 ISMS を実行する際の要求事項。(PDCA サイクルの D「Do」)
4. 組織の状況 組織の内情や取り巻く状況、利害関係者のニーズを把握した上で ISMS の適用範囲を決定することを要求している。	9. パフォーマンス評価 適切な ISMS が構築・運用できているか評価する際の要求事項。(PDCA サイクルの C「Check」)
5. リーダーシップ トップマネジメントが主導して ISMS を構築することを要求している。(トップマネジメントが実施すべきことのまとめ)	10. 改善 ISMS の是正処置やリスク、改善の機会、ISMS 認証の不適合があった場合の対処法。(PDCA サイクルの「Act」)

ISMS の確立、運用、監視

「第11章. セキュリティフレームワーク」でも記載した通り、ISMS は PDCA サイクルに則って運用することになります。Plan で ISMS を確立し、Do で導入および運用、Check で監視および見直し、Act で維持および改善を行います。ISMS の取組により、組織の情報セキュリティをより良くするために管理手段レベルでの解決を目指すことになります。同じ失敗を繰り返さない、ある

いは現状を改善し続けるために、PDCA サイクルによって継続的な改善を図ることが重要です。

本テキストでは、Lv.3 網羅的アプローチとして必要な文書や項目を抜粋し、詳細に説明していきます。なお、ISMS の要求事項を定めている ISO/IEC 27001 の 1 から 3 はそれぞれ「1.適用範囲」「2.引用規格」「3.用語および定義」なので、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの 7 項目となっています。

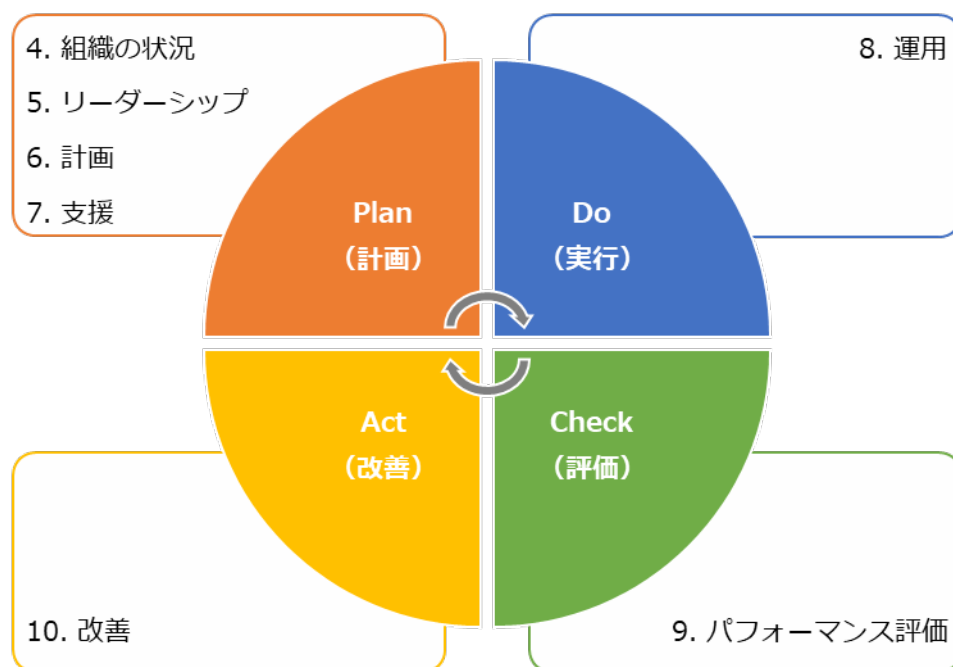


図 51. ISO/IEC 27001 の PDCA サイクル

13-2-2. ISMS : 4. 組織の状況

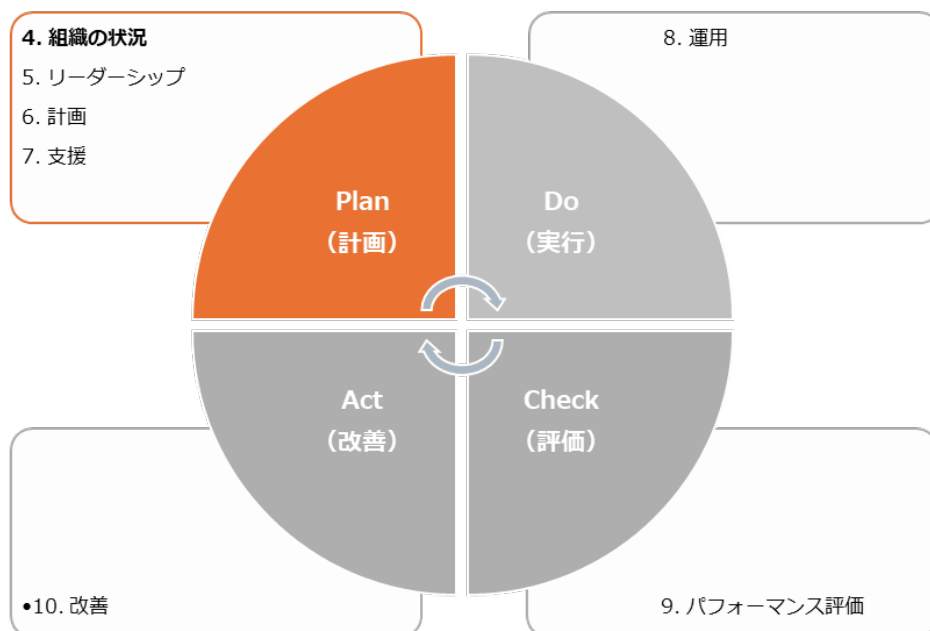
ISMS 構築の第一歩は、組織の状況を把握することにあります。組織が抱えている情報セキュリティ上の課題を明らかにするとともに、組織の利害関係者が情報セキュリティに関してどのようなニーズや期待を持っているのかを整理し、情報セキュリティに取り組む意義を確認します。それを踏まえて、「ISMS の適用範囲」を決定することになります。この「4.組織の状況」は、PDCA サイクルの「Plan（計画）」に位置していますが、組織内外の状況に応じて見直す必要があります。

4. 組織の状況	作成文書（例）
4.1 組織及びその状況の理解 ISMS を構築することにより解決したい課題（組織の目的に関連する内部課題、外部課題）を明確にします。	● 外部及び内部の課題
4.2 利害関係者のニーズ及び期待の理解 ISMS に関係する利害関係者（顧客、従業員、取引先など個人や組織）と、利害関係者から要求される情報セキュリティに関	● 利害関係者のニーズ及び期待

係する要求事項を明確にします。	
4.3 情報セキュリティマネジメントシステムの適用範囲の決定 決定された外部課題・内部課題、利害関係者の要求事項と、業務内容や他の組織との情報のやり取り、ネットワーク構成などを考慮し、ISMS の適用範囲を合理的に決定します。	● ISMS 適用範囲 ● レイアウト図 ● ネットワーク図
4.4 情報セキュリティマネジメントシステム 決定した ISMS の適用範囲を対象に、PDCA サイクルに基づく ISMS を構築・運用します。	—

4.1 組織及びその状況の理解

作成する文書	● 外部および内部の課題



「組織及びその状況の理解」では、組織を取り巻く外部と内部の課題を整理することが求められています。ここで整理した課題を、ISMS の取組を通して解決していきます。また、組織のどの部分に対して ISMS を適用すべきなのかといった適用範囲を確定する際にも、課題を考慮することになります。

外部の課題

組織の外部に原因が存在する課題は、以下の情報をヒントに決定することができます。

- 国際、国内、地方または近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然および競争の環境
- 組織の目的に影響を与える主要な原動力および傾向

- 外部ステークホルダーとの関係並びに外部ステークホルダーの認知および価値観
(例)

課題	リスク	機会
個人情報、機密情報の保護（ウイルス感染、情報漏えい、新たな脅威への対応）	情報セキュリティ事故の発生 →信用低下	情報の活用

内部の課題

組織の内部に原因が存在する課題は、以下の情報をヒントに決定することができます。

- 統治、組織体制、役割およびアカウンタビリティ
- 方針、目的およびこれらを達成するために策定された戦略
- 資源および知識として見た場合の能力（例えば、資本、時間、人員、プロセス、システムおよび技術）
- 情報システム、情報の流れおよび意思決定プロセス（公式および非公式の双方を含む。）
- 内部ステークホルダーとの関係並びに内部ステークホルダーの認知および価値観
- 組織文化
- 組織が採択した規格、指針およびモデル
- 契約関係の形態および範囲

(例)

課題	リスク	機会
ISMS に関する理解の促進	理解不足による情報セキュリティ事故	体制強化
情報（紙、電子データ）の適切な取扱い	紛失、訪問先などに忘れ →信頼喪失	信頼向上
ノウハウ、お客様より預かる機密情報などの保護	機密情報の漏えい、ノウハウの流出	ビジネス機会の拡大

4.2 利害関係者のニーズ及び期待の理解

作成する文書	● 利害関係者のニーズ及び期待

「利害関係者のニーズ及び期待の理解」では、組織の利害関係者と、その利害関係者が要求する情報セキュリティに関する要求事項を明確化することが求められます。利害関係者には、顧客や従業員、取引先など、さまざまな個人や組織が含まれます。利害関係者に該当する範囲は広いいため、組織が管理できる範囲で利害関係者からの要求事項を特定します。また、どの程度のセキュリティレベルで対策するのか、利害関係者とそのニーズから水準を設定することになります。

利害関係者のニーズ及び期待の記入例

利害関係者	情報セキュリティに関する 要求事項	リスク	機会
取引先	適切な情報の取扱い	不適切な取扱いによる信頼低下 →案件減少	適切な対応による信頼向上 →受注の維持/増加
	法令順守	未順守による信頼低下 →案件減少	順守による信頼向上 →受注の維持/増加
株主	<u>セキュリティインシデント</u> の未然防止	セキュリティインシデントの発生 →ブランドイメージの低下	セキュリティインシデント の発生数減少 →ブランドイメージの向上
従業者	情報セキュリティに関する 教育	機密情報/ノウハウの流出	組織の価値向上
	必要な情報へのアクセス	機密情報/ノウハウの流出	効果的・効率的な業務 →競争力アップ
	個人情報の保護	不適切な情報の取扱い →信頼低下	従業者から信頼向上 →人材の確保
国・自治体	法令・その他規範の順守	セキュリティインシデント発生時 の不適切な対応 →社会的信頼の低下	社会的信頼の向上

4.3 情報セキュリティマネジメントシステムの適用範囲の決定

作成する文書	● ISMS 適用範囲 ● レイアウト図 ● ネットワーク図

ISMS の適用範囲は、必ずしも会社全体とする必要はありません。特に大企業の場合には、特定の業務や特定の部門に限定して ISMS を構築することがあります。例えば、ある取引先の要請によって ISMS を構築する場合、その取引先と取引のある部門に適用範囲を限定するケースがあります。

中小企業の場合には、会社全体を適用範囲とすることが多いので、特段の理由がない限り、会社全体を適用範囲にするとよいでしょう。

「情報セキュリティマネジメントシステムの適用範囲の決定」では、ISMS を適用するところと、そうではないところの境界およびその適用される範囲内で、規格の要求事項がどのように適用できるかを決定するよう要求しています。規格などの要求事項によって定められる改善すべき範囲を、

適用範囲といいます。

適用範囲の決定に際しては、考慮しないといけない3つの事項があります。2つはこれまでに説明した「外部および内部の課題」と「要求事項」です。もう1つは、「組織が実施する活動と、他の組織が実施する活動との間のインターフェースおよび依存関係」です。異なる部署や委託先など他の組織との業務プロセスにおける依存度を見ながら、適用範囲を広げるのか、分離しておくのかを検討することになります。

インターフェースおよび依存関係の記入例

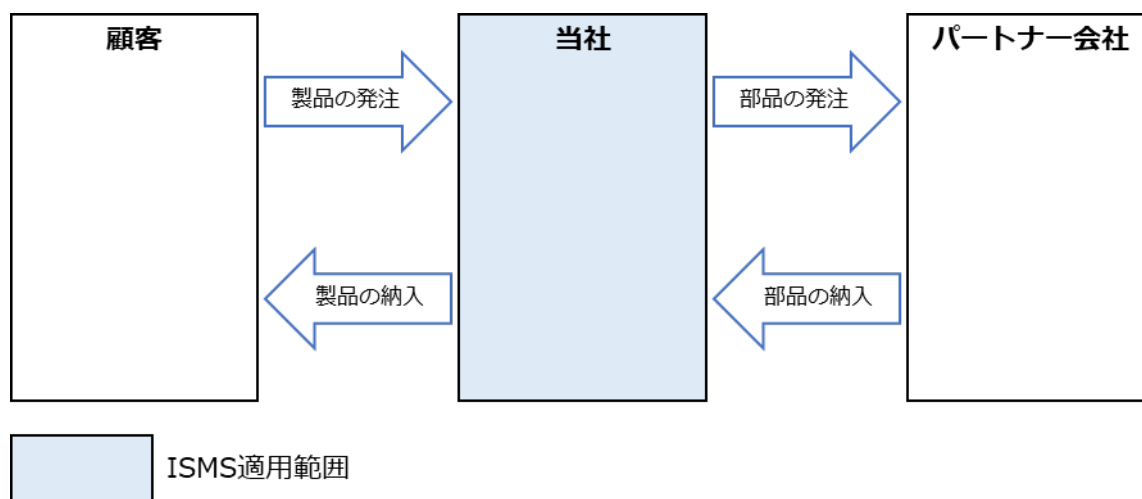


図 52. インターフェースおよび依存関係の記入例

適用範囲を組織の一部とした場合、同じ組織内に適用範囲の内と外という境界ができることになります。適用範囲の境界について、いくつかの観点から明確にしておく必要があります。

人的・組織的境界

組織におけるどの人、どの部門が適用範囲の内側に該当するのかを明確にします。それにより、同じ社内の人であっても、適用範囲外の人を外部の人として扱うといった配慮が必要になる場合があります。

物理的境界

適用範囲とする建物や施設、部屋といった空間を明確にします。扉や壁、パーティションなどの物理的な境界によって仕切られていることが望ましいです。

技術的境界

ネットワークにおいて、対象とする範囲を明確にします。物理的境界と同様に、適用範囲の IT 環境の境界を明らかにし、管理しなければならない情報システムや、ネットワークの対象や範囲を明確にする必要があります。

資産的境界

業務委託を受けていたり、組織の一部を適用範囲にしたりした場合に、資産的境界が生じる場合があります。顧客から情報や資源の提供を受けた際に、それを指定された管理方法により管

理するのか、自組織の管理下となるのかといった場合や、適用範囲内の部門が保有する情報でも、組織全体で共有している場合にはどう管理するのかを明確にする必要があります。

事業的境界

事業（業務）においても対象を明確にします。事業は部門を横断する場合があるため、人的・組織的境界とも合わせて対象を検討し、適用範囲を明確にする必要があります。

物理的境界 レイアウト図（例）

物理的境界では、適用範囲とする空間を明確にし、境界線を記載します。そして境界線により区切られた空間ごとにセキュリティレベルを設定します。

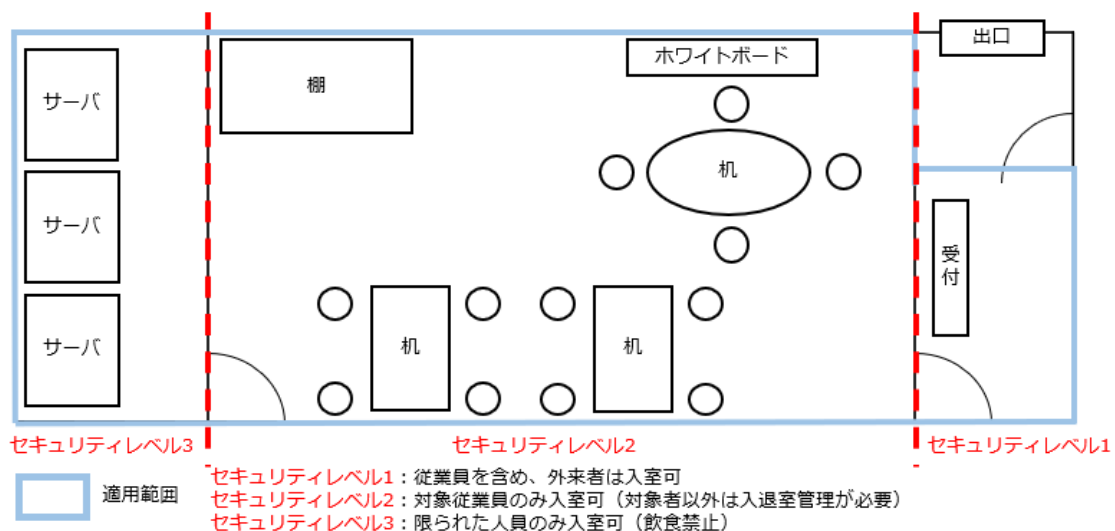


図 53. 適用範囲の例（物理的境界）

技術的境界 ネットワーク図（例）

ネットワークにおいて対象とする範囲を明確にするため、ネットワーク構成図を作成し、境界線を記載します。

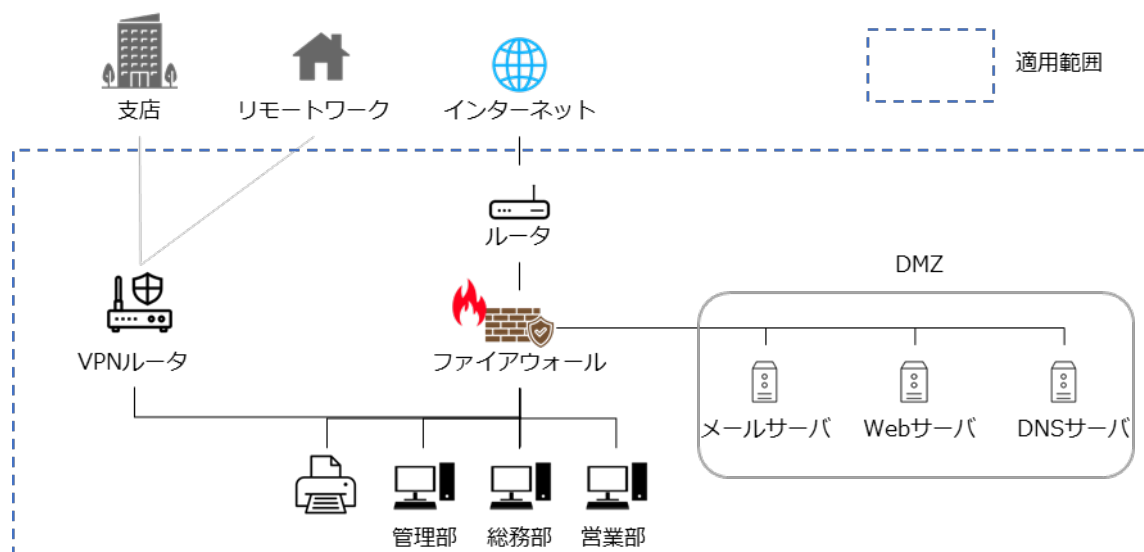
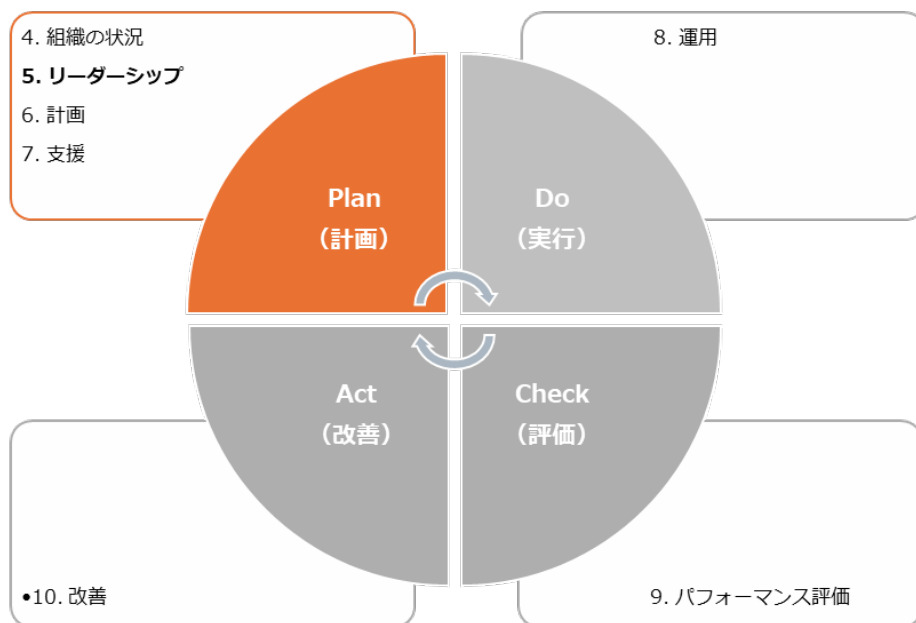


図 54. 適用範囲の例（技術的境界）

13-2-3. ISMS : 5. リーダーシップ

「5. リーダーシップ」は、PDCA サイクルの「Plan（計画）」に位置しており、トップマネジメントに求められる要求事項を示しています。トップマネジメントとは、ISMS の適用範囲における最高責任者のことを指します。多くの場合、トップマネジメントは、組織の社長が担う傾向にあります。「5. リーダーシップ」は、PDCA サイクルの軸であり、PDCA サイクルを回すには、トップマネジメントのコミットメント（関与、制約）が重要になります。



5. リーダーシップ	作成文書（例）
5.1 リーダーシップ及びコミットメント トップマネジメントが責任を持って実行しなければならない事項が記載されています。	—
5.2 方針 トップマネジメントが、ISMS の目的や方向性、実施する内容について文書化し、「情報セキュリティ方針」を作成することを要求しています。	● 情報セキュリティ方針
5.3 組織の役割、責任及び権限 トップマネジメントは、ISMS を運用するために必要な役割や責任、権限を各要員に割り当て、どの要員がどのような役割や責任、権限を持っているかがわかる文書を作成す	● ISMS の運用組織図 ● 責任者または部門の名称と役割を明記した文書

ることを要求しています。	

5.1 リーダーシップ及びコミットメント

「リーダーシップ及びコミットメント」では、ISMS のトップマネジメントが責任を持たなければならないことを要求しています。トップマネジメントは、以下の事項について責任を持って必ず行う必要があります。

トップマネジメントが行う事項（要求事項）
情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする → 組織の事業の方向性に沿った情報セキュリティ方針と、情報セキュリティ目的を策定することを要求しています。※情報セキュリティ方針、情報セキュリティ目的については後述します。
組織のプロセスへの ISMS 要求事項の統合を確実にする → 自社の業務に、情報資産を管理する手順を組み込むことを要求しています。
ISMS に必要な資源が利用可能であることを確実にする → ISMS を構築・運用するために、必要な予算や人員など経営資源を確保しておくことを要求しています。
有効な情報セキュリティマネジメントおよび ISMS 要求事項への適合の重要性を伝達する → 従業員が ISMS を構築・運用し、情報資産を適切に管理することの重要性を十分に認識できるように、周知することを要求しています。
ISMS がその意図した成果を達成することを確実にする → ISMS を構築・運用することにより得られる成果を明確にし、その成果を十分に得られるように取り組んでいくことを要求しています。
ISMS の有効性に寄与するよう人々を指揮し、支援する → ISMS を構築・運用できるようにするため、従業員に対して教育を受けさせたり、定めた決まりを認識・実施させたり、従業員の意見を聞いたりするなど、サポートすることを要求しています。
継続的改善を促進する

→ ISMS を構築・運用するにあたり、従業員が不便に感じていることなど、改善が必要だと考えられる場合には、改善を進めるよう要求しています。

その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する

→ 組織の規模や形態によって、トップマネジメントの指示が従業員に適切に伝わらない可能性があります。そのため、各部門の責任者が主導となり、従業員にトップマネジメントの指示を適切に伝え、ISMS を円滑に構築・運用できるようにすることを要求しています。

5.2 方針

作成する文書

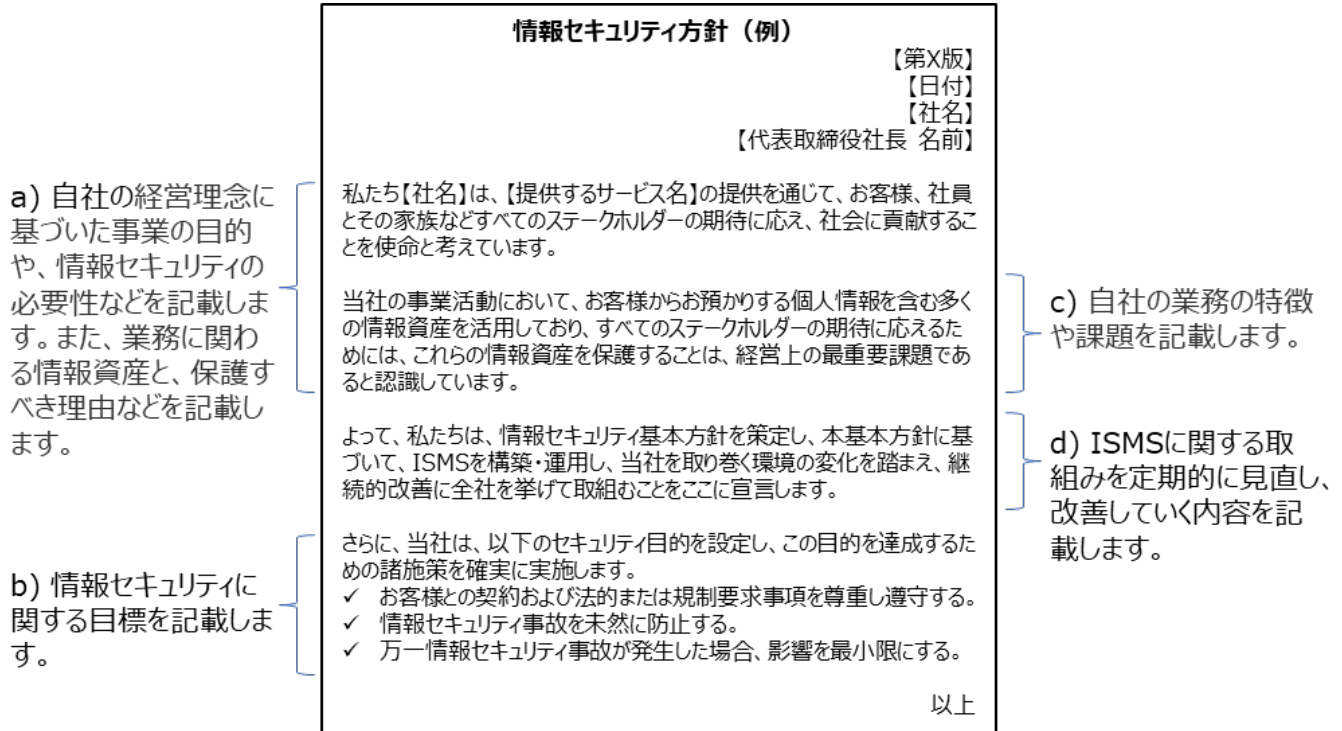
- 情報セキュリティ方針

トップマネジメントは、組織の情報セキュリティに対する考え方や取組の姿勢を利害関係者に示すため、情報セキュリティ方針を文書として作成し、組織内に周知するとともに、必要に応じて、その他の利害関係者が入手できるようにします。例えば、保護すべき情報資産と保護すべき理由を明示し、利害関係者に周知します。

情報セキュリティ方針の作成方法

情報セキュリティ方針が満たさなければならない事項

- 組織の目的に対して適切である
- 情報セキュリティ目的を含むか、または情報セキュリティ目的の設定のための枠組みを示す
- 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む
- ISMS の継続的改善へのコミットメントを含む



5.3 組織の役割、責任及び権限

作成する文書	
	● ISMS 運用組織図 ● 責任者または部門の名称と役割を明記した文書

「組織の役割、責任および権限」とは、ISMS を構築・運用するために、トップマネジメントが、組織内で役割を決め、責任と権限を割り当てることです。

ある程度の規模を超えた組織になると、ISMS の実際の運用担当者や責任者は、トップマネジメントから権限を委譲された人になります。そうすると、情報セキュリティに関する取組の実態を、トップマネジメントが十分把握していないという状況になりがちです。そうならないために、ISMS の実施状況をトップマネジメントに報告する仕組みやルールを作っておく必要があります。

ISMS 運用組織図の作成方法（例）

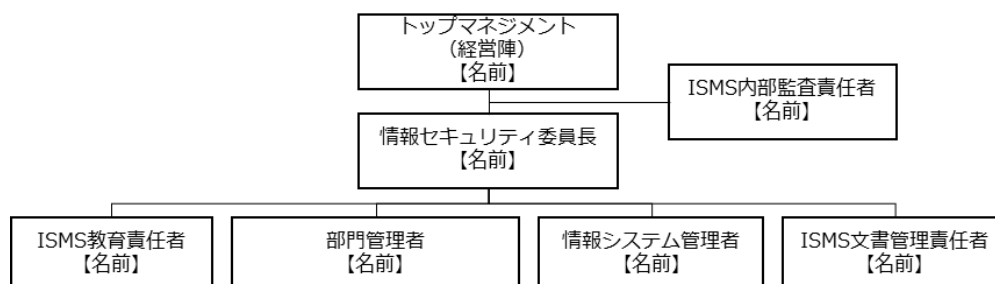


図 55. ISMS 運用組織図の例

ISMS の運用組織図を作成する流れを説明します。

1. トップマネジメントは、情報セキュリティ委員長を任命し、上記の事項に関する権限や責任を持たせる必要があります。そのため、トップマネジメントの下位に、情報セキュリティ委員長を配置します。
2. ISMS 内部監査責任者は、[内部監査](#)を実施する際の最高責任者であり、トップマネジメントの下位に設置します。
3. 情報セキュリティ委員長は、ISMS の実施・運用をするために必要な役割を持つ責任者を任命します。情報セキュリティ委員長の下位に各責任者を配置します。

責任者または部門の名称と役割を明記した文書化の方法（例）

名称	役割
情報セキュリティ委員長	ISMS の実施、運用について統括する
ISMS 内部監査責任者	ISMS とその実施状況に関わる監査を統括する
ISMS 教育責任者	ISMS に関する教育計画の立案と実施を行う
部門管理者（情報セキュリティ委員）	ISMS の部門代表者として、部門を管理する
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規程・規則に従い、ISMS を維持するための安全管理対策を実施する
ISMS 文書管理責任者	ISMS に関する文書と記録などの維持・管理を行う

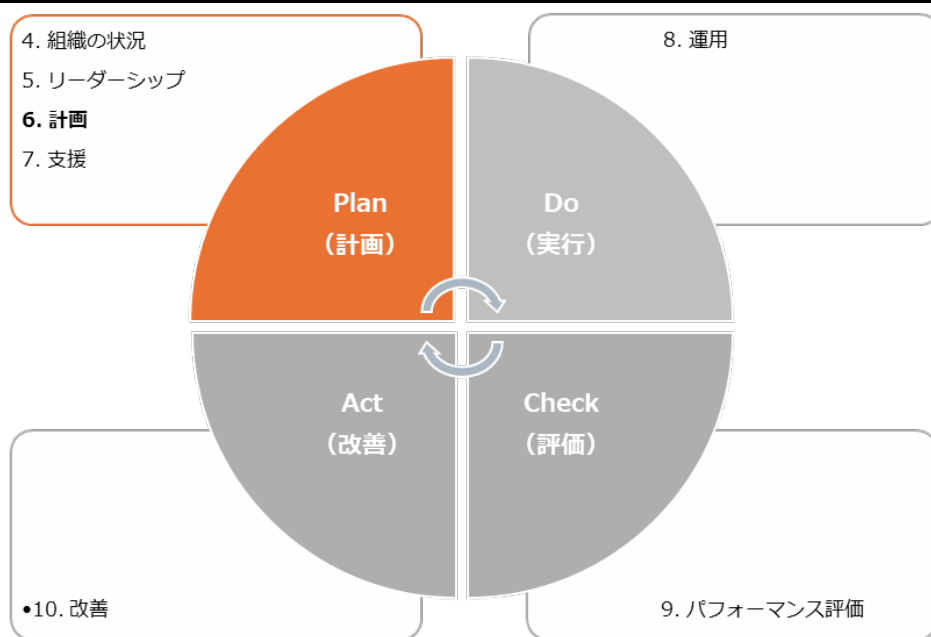
13-2-4. ISMS : 6. 計画

「6. 計画」は、PDCA サイクルの「P（計画）」に位置しており、リスクマネジメントの確立、情報セキュリティにおける[リスクアセスメント](#)、リスク対応、情報セキュリティ目的の管理に関する要求事項を示しています。

本項では、リスクマネジメントで作成する文書化の方法について解説します。リスクマネジメント手順については「12 章. リスクマネジメント」を参照してください。

6. 計画	作成文書（例）
6.1 リスク及び機会に対処する活動 一般	● 資産目録（情報資産管理台帳）

特定した内外部の課題と、利害関係者のニーズおよび期待を考慮して、リスク・機会（期待する状況や結果）を決定し、対処するための活動を明確にすることを要求しています。 情報セキュリティリスクアセスメント 組織や企業の資産に対する、情報セキュリティリスクアセスメントプロセスの確立を要求しています。 情報セキュリティリスク対応 情報セキュリティリスク対応の手順を確立することを要求しています。	● リスクアセスメント結果報告書 ● 適用宣言書 ● リスク対応計画
6.2 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティ目的を確立し、達成するための計画を策定することを要求しています。	● ISMS 有効性評価表
6.3 変更の計画策定 ISMS の変更が必要なときは、計画的な変更を要求しています。	



6.1 リスク及び機会に対処する活動

作成する文書	● 資産目録（情報資産管理台帳） ● リスクアセスメント結果報告書 ● 適用宣言書

「リスク及び機会に対処する活動」とは、「ISMS の意図した成果を達成する」「ISMS の望ましくない影響を防止・低減する」「継続的改善を達成する」の3つを実現するために、妨げとなるような機会やリスクを発見し、対処することです。平たく言えば、情報セキュリティ上のリスクに対して、適切な対策を講じることにより、情報セキュリティを確保するための活動になります。具体的には「リスクアセスメントの実施」「リスク対応策の作成と実施」「リスク対応策の有効性評価」「継続的改善」といった活動が含まれます。

リスクアセスメントは、組織や企業の資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位付けをしていくプロセスになります。リスクアセスメントの実施により、リスクを評価し、事前にリスクを把握することにより必要な投資額を含め、企業が適切な対策を検討することが可能になります。

情報セキュリティのリスク基準を確立し、維持する

リスクアセスメントを実施するにあたり、リスクの重大性を評価するための目安となるリスク基準を決める必要があります。ISMS では、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むように明示されています。

※「12-2-1. リスク基準の確立」を参照

情報セキュリティリスクを特定する

企業が掲げる目的・目標達成を阻害する可能性のあるリスクをすべて洗い出すことです。そのため、リスクの発生可能性や影響の大きさを考慮せず、少しでも企業に影響を与えそうなリスクを洗い出すことが目的となります。リスク特定として最終的な成果はリスク一覧表の作成になります。

※「12-2-2. リスクの特定」を参照

情報セキュリティリスクを分析する

リスク特定により特定されたリスクに対して、リスク分析を行います。リスク分析を行うことで、「企業にとって対応が必要なリスクはどれか」、「優先的に対応しなければならないリスクは何か」といったことを判断します。リスク分析による結果を、「リスクアセスメント結果報告書」に記載します。

※「12-2-3. リスクの分析」を参照

情報セキュリティリスクを評価する

リスク分析により算出したリスクレベルからリスク受容基準と比較し、リスク対策が必要か否かを判断します。また、算出したリスクレベルをもとに優先順位を付けます。

※「12-2-4. リスクの評価」を参照

資産目録（情報資産管理台帳）、リスクアセスメント結果報告書は、ISO/IEC 27001:2022 の管理策「5.9 情報およびその他の関連資産の目録」に対応します。

資産目録（情報資産管理台帳）の作成方法（例）

資産目録（情報資産管理台帳）の作成方法は「12-2-2. リスクの特定」を参照してください。

リスクアセスメント結果報告書の作成方法（例）

作成した資産目録（情報資産管理台帳）から、リスクアセスメントの結果をまとめた「リスクアセスメント結果報告書」について説明します。

※下記表の「対応」の項目を記載するタイミングは、「8.運用」となります。

No	資産 目録 の No	リスク特定					リスク分析 (一次評価)			優先 順位 リスク レベル	リスク対応							二次評価	
		リスク源	影響領域	事象	原因	起こり得る 結果	重要度	被害発生 可能性	保 有		低 減	回 避	移 転	管理策	対 応	重 要 度	被 害 発 生 可 能 性	リ ス ク レ ベ ル	
1	9	モバイル 機器の利 用ルール が十分に 整備され ていない	外部	持出中に重 要な情報を 紛失・盗難 (機密性の 喪失)	【事象】に 対し【リス ク源】であ る	機密情報な どが漏えい し顧客に影 響、信用喪 失	3	2	6	2		●			モバイル機器の利用ルール を整備・強化	予 定	2	1	2
2	40	教育が不 十分なた め従業 者の意識 が低い	全社	誤送信 (機密性の 喪失)	【リスク 源】ため 【事象】が 発生	機密情報な どが漏えい し顧客に影 響、信用喪 失	2	2	4	3		●			教育訓練	予 定	1	1	1
3	10、 11、 13、 26、 55	電子の情 報分類／ 取り扱い が明確で ない	外部	情報の紛 失・盗難 (機密性の 喪失)	【リスク 源】ため 【事象】が 発生	機密情報な どが漏えい し顧客に影 響、信用喪 失	3	3	9	1		●			・ 5. 12 情報の分類、5.13 情報 のラベル付け、分類ごとの 情報の取扱いルール	予 定	2	3	6

リスクアセスメント結果報告書には、以下の内容を記載します。

資産目録の No.		重要資産の項番を記載します。 重要資産は、資産目録（情報資産管理台帳）から「情報セキュリティリスクアセスメントを実施するための基準」で決定した基準をもとに選択します。例えば、機密性、<u>完全性</u>、<u>可用性</u>の項目について、評価値が 1 つでも 3 となった資産を重要資産とします。 ※リスクによっては資産目録の No は複数になることがあります。 ※「情報セキュリティリスクアセスメントを実施するための基準」については、「12-2-1. リスク基準の確立」を参照してください。
リスク源		想定される脅威を記載します。 （例）モバイル機器の利用ルールが十分に整備されていないなど
影響領域		脅威が発生した場合の影響範囲を記載します。 （例）外部、全社など
事象		発生する可能性のある事象を記載します。 （例）持ち出し中に重要な情報を紛失・盗難（機密性の喪失）など
原因		事象が発生する原因を記載します。 （例）【事象】に対し【リスク源】のため【事象】が発生など
起こり得る結果		事象が発生した場合に起きる結果を記載します。 （例）機密情報などが漏えいし顧客に影響、信用喪失など
一次評価	重要度	算出方法は、「12-2-2. リスクの特定」を参照してください。
	被害発生可能性	算出方法は、「12-2-3. リスクの分析」を参照してください。
	リスクレベル	算出方法は、「12-2-3. リスクの分析」を参照してください。
優先順位		リスク受容基準をもとに、リスクレベルから優先順位づけを行います。 （例） 1：早急に対応、2：今期中に対応、3：今期対応が望ましい リスクレベル：9→優先順位：1 リスクレベル：4→優先順位：3 リスクレベル：6→優先順位：2

保有、低減、回避、移転		リスク対応により決定した対応について「●」を記載します。
管理策		リスク対応により決定した内容を記載します。 (例) モバイル機器の利用ルールを整備・強化など ※附属書 A の管理策のリストは包括的なものではないので、必要に応じてリストにない管理策を採用してもかまいません。
対応		管理策の実施状況を記載します。 ● 管理策を実施した場合は「済み」 ● 管理策を実施する予定がある場合は「予定」 ● 管理策を実施する予定が未定の場合は「未定」
二次評価	重要度	算出方法は、「12-2-2. リスクの特定」を参照してください。
	被害発生可能性	算出方法は、「12-2-3. リスクの分析」を参照してください。
	リスクレベル	算出方法は、「12-2-3. リスクの分析」を参照してください。

※「二次評価」とは、リスクに対する管理策の有効性評価をするために行うものです。リスク対応を実施した結果をもとに、[情報資産](#)に対する再評価を実施します。

適用宣言書の作成方法（例）

「適用宣言書」は、ISMS 認証を取得するすべての組織に作成が義務づけられています。認証を取得しない組織では、必須ではありませんが、情報セキュリティに対する取組を明確にするために「適用宣言書」を作成することが望ましいとされています。

適用宣言書は以下の内容を含むように作成します。

- 必要な管理策
- それらの管理策を含めた理由
- それらの管理策を実施しているか否か
- 附属書 A に規定する管理策を除外した理由

管理目的および管理策			適用	実施・未実施	管理策を含めた理由 管理策を除外した理由	規程・手順書
5 組織的管理策						
5.1	情報セキュリティのための方針群	情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行	○	○	情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従	情報セキュリティ方針

		し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューすることが望ましい。			って規定するため	
5.2	情報セキュリティの役割および責任	情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てることが望ましい。	○	○	ISMS の構築・運用を円滑に行うため	情報セキュリティ手順書
5.3	職務の分離	相反する職務および責任範囲は、分離することが望ましい。	○	○	許可されていないもしくは意図しない変更または不正使用の危険性を低減するため	情報セキュリティ手順書
5.4	経営陣の責任	経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求することが望ましい。	○	○	ISMS の取組が、経営陣の経営戦略の一部であることを確実にするため	情報セキュリティ手順書
5.5	関係当局との連絡	組織は関係当局との連絡体制を確立および維持することが望ましい。	○	○	<u>セキュリティインシデント</u> が発生したことを迅速に報告するため	情報セキュリティ手順書
...	...	...	...	...	...	...

適用宣言書には、以下の内容を含めます。

管理目的および管理策	ISO/IEC 27001 の附属書 A の管理策を記載します。 (例) 5.1 情報セキュリティのための方針群など
適用	適用または適用除外を記載します。 (例) ○：適用、×：適用除外
実施・未実施	実施したか否かを記載します。 (例) ○：実施、未：未実施、－：適用除外
管理策を含めた理由または管理策	管理策を行う場合も理由を記載します。

を除外した理由	(例) 情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するためなど
規程・手順書	管理策が含まれている規程または手順書を記載します。 (例) 情報セキュリティ手順書 5.1.1、A-02 情報セキュリティ方針など

情報セキュリティリスク対応計画

「リスク対応計画」は、それぞれのリスクに対して、どのような管理策を、誰が、いつまでに、どのように実施するのかを表にまとめたものになります。

リスク対応計画の作成方法（例）

リスクアセスメント結果報告書から、リスク対応を行う管理策をすべて記載し、それぞれの具体的な内容や、担当者などを記載します。リスク対応を行った場合、実績やリスク対応のステータスを記載する必要があります。

※下記表の「実績」と「ステータス」の項目を記載するタイミングは、「8.運用」となります。

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	ルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
2	教育訓練	ルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-		着手
3	情報の分類定義 分類ごとの情報の 取扱いルール ラベリング	情報の分類定義 分類ごとの取扱い ルール検討 関係者に周知	委員長	20XX/-/-	20XX/-/-			未着手

リスク対応計画では、以下の内容を記載します。

管理策	リスクアセスメント結果報告書の管理策を記載します。 (例) モバイル機器の利用ルールを整備・強化など
タスク	管理策を実施する上で、具体的な業務を記載します。 (例) ルール検討、関係者に周知
担当	管理策の担当者を記載します。

	(例) 委員長
予定	リスク対応予定の開始日と終了日を記載します。 (例) 開始：2024/08/10 終了：2024/09/29
実績	開始の箇所：実際にタスクを開始した日付を記載します。 終了の箇所：実際にタスクが完了した日付を記載します。
ステータス	タスクの進捗状況を記載します。 ● タスクが完了した場合は「終了」 ● タスクを実行中の場合は「着手」 ● タスクに着手していない場合は「未着手」

リスク所有者からの承認/残留している情報セキュリティリスクの受容

リスク対応計画と残留リスク（管理策の適用後に）は、リスク特定で決めたリスク所有者の承認が必要になります。リスク所有者が承認する際は、記録をする必要があるため、ワークフローやチェック欄などを用います。

(例) 承認プロセスとして、作成した書類にチェック欄（電子印欄など）を作成します。

作成	承認

作成者/更新者	【名前】	作成日/更新日	【日付】
承認者	【名前】	承認日	【日付】

6.2 情報セキュリティ目的及びそれを達成するための計画策定

作成する文書	ISMS 有効性評価表

情報セキュリティ目的の基本要件として以下の要件を満たす必要があります。

- 情報セキュリティ方針と整合している
- (実行可能な場合) 測定可能である
- 適用される情報セキュリティ要求事項, 並びにリスクアセスメント及びリスク対応の結果を考慮に入れる
- これを監視する
- これを伝達する
- 必要に応じて、更新する

- 文書化した情報として利用可能な状態にする

情報セキュリティ目的と、それを達成するための計画を ISMS 有効性評価表に記載します。

「8. 運用」で計画を実施し、「9. パフォーマンス評価」で評価を行います。

ISMS 有効性評価表の作成方法（例）

※下記表の「評価」の項目を記載するタイミングは、「9. パフォーマンス評価」となります。

【計画】 情報セキュリティ目的 お客様との契約および法的または規制要求事項を尊重し順守する 情報セキュリティ事故を未然に防止する 情報セキュリティ上の脅威から情報資産を保護する 当社 ISMS の意味を理解した活動の開始 評価指標 ISMS 教育受講／合格 100%（全従業員） 【備考】 取組みの初年度であるため、全従業員が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。 情報セキュリティ目的達成のための計画				
実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業員が ISMS 教育を受講	ISMS 事務局長	20XX 年-月	受講者数および合格者数をカウントし、評価する
【評価】 評価日：【20XX/00/00】 情報セキュリティ目的達成に関する評価結果（凡例 ○：有効 ×：有効ではない） 結果：○ 備考：全従業員 e ラーニングでのテストを 100 点にて合格。有効性があるものと判断する。				

ISMS 有効性評価表では、以下の内容を記載します。

情報セキュリティ目的	適用範囲（組織全体、各部署ごと）でのセキュリティ目的を記載

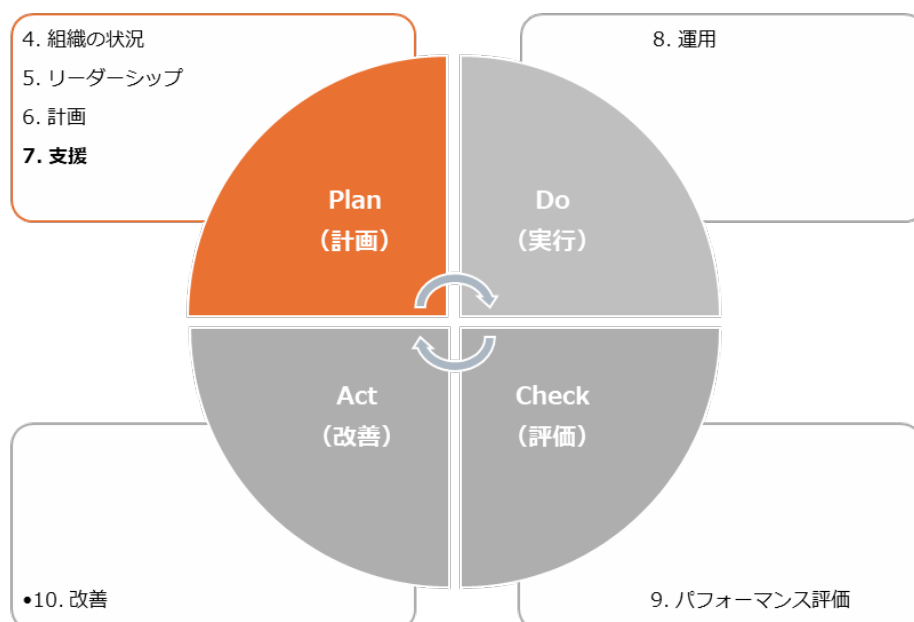
	します。 (例) 重大なセキュリティインシデントを発生させない、 マルウェア感染およびサイバー攻撃によるシステム停止の防止など
評価指標	測定可能な値を記載します。 (例) マルウェア感染の有無、システム停止の有無など
実施事項	情報セキュリティ目的を達成するための実施内容を記載します。 (例) ウイルス対策ソフトのインストール、標的型メール訓練の実施など
必要な資源	計画の責任者を記載します。 (例) 部長各自など
責任者	計画の責任者を記載します。 (例) 部長各自など
達成期限	計画の期限を記載します。 (例) 年度末、2024 年 9 月など
評価方法	具体的な評価方法を記載します。 (例) 年度末に発生したセキュリティインシデントをカウントし、評価するなど
評価	情報セキュリティ目的達成に関する評価結果には、ISMS が有効だったか否かという結果を記載します。

13-2-5. ISMS : 7. 支援

「7. 支援」は、PDCA サイクルの「Plan (計画)」に位置しており、ISMS の運用をサポートするための要求事項が規定されています。

7. 支援	作成文書 (例)
7.1 資源 ISMS に必要な資源 (人、物、金、情報) を決定し、提供します。	—
7.2 力量 ISMS 適用範囲の要員に求められる力量 (知識、技能など) を定義し、要員が力量を備えているか評価を行います。力量評価の結果、	● 力量確認表 ● 教育計画書 ● 理解度確認テスト

力量が不足している場合は、力量を身に付けるための教育を計画し、実施します。教育の実施後、力量を取得・維持できたか確認テストを行います。最後に、実施した教育内容を記録として保持します。	● 教育実施記録
7.3 認識 ISMS 適用範囲のすべての要員に、以下の内容を認識させる必要があります。 ● 情報セキュリティ方針 ● 情報セキュリティパフォーマンスの向上によるメリットや、自身の業務と ISMS の関係、実施すべきセキュリティ対策 ● ISMS によって割り当てられた責任を果たさなかった際の影響	—
7.4 コミュニケーション ISMS を運用するにあたり、必要な意思疎通ができるプロセスを確立する必要があります。	—
7.5 文書化した情報 ISMS に必要な文書化した情報の作成、更新、管理についての要求事項が記載されています。	—



7.1 資源

ISMS の PDCA サイクルを回すために必要な資源を決定し、利用できるようにする必要があります。

す。必要な資源を決定し提供することは、トップマネジメントが行う必要があります。（リーダーシップ及びコミットメントの箇所で要求されています。）



ISMSのPDCAサイクルを回すために必要となる資源を決定し、提供する

資源の具体例を以下に示します。例を参考に、ISMS の PDCA サイクルを回すために自社で必要となる資源を決定し、利用可能にします。

資源	具体例
人	ISMS を構築・運用するために必要となる要員 ISMS の推進体制の確立 必要に応じた外部の専門家など
物	情報を処理するための機器（サーバ、ネットワーク機器など） コミュニケーション手段（パソコン、スマホなど） 活動に必要な施設など
金	人、物の資源を確保するための予算 要員の教育費用 ISMS の維持費など
情報	文書化した情報 ISMS の PDCA サイクルを回すために有用な情報 情報セキュリティに関する最新情報など

7.2 力量

作成する文書	● 力量確認表 ● 教育計画書 ● 理解度確認テスト ● 教育実施記録

ISMS 適用範囲の要員に必要な力量（知識、技能など）を明確にし、実際に要員が力量を備えて

いるか評価を行います。力量が不足している場合、力量を身に付けるための教育を計画し、実施する必要があります。教育の結果、力量が取得できたかを評価します。

力量確認表の作成方法（例）

要員の力量を評価し、確認するための力量確認表を作成する方法について説明します。

以下は、部門管理者の力量評価の例です。以下の手順で赤字の箇所を自社の状況に合わせたものに修正することにより、自社に適した力量確認表を作成できます。

1. 要員ごとに、「組織の役割、責任及び権限」により割り当てられた役割や責任を果たすために必要となる力量を、「必要条件」として定義します。
2. 責任者として任命できるか否かを判断するための任命基準を定義します。
3. 定義された力量をどれほど備えているか、評価基準を決めて評価を行います。
4. 評価の結果、力量が不足している場合は教育・訓練を実施します。
5. 教育・訓練の実施後、どれほど改善できたか評価を行い、任命基準をもとに責任者として任命できるか判断します。

役割	部門管理者	任命基準	A	B	C
氏名	〇〇 〇〇	区分	任命可	改善確認後任命可※	任命不可 再任命

A：項目のすべてが"3"以上。

B：項目の"2"以下について改善の予定がある。

C：項目の"2"以下について改善の予定がない。

※改善確認までは暫定的に任命し、改善確認後に正式任命とする

	必要条件	評価	改善予定日	改善内容	改善後評価	改善確認日
1	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-
2	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-
3	情報セキュリティ全般に関する知識があること	2	20XX/-/-	ISMS 構築作業を通して獲得	3	20XX/-/-

4	公正な判断ができる こと	5				
評価基準		内容				
5		十分な力量がある。指導・教育ができる				
4		力量がある。支援なしに対応ができる				
3		力量がある。他の支援により対応ができる				
2		改善の余地がある				
1		改善が必要				

教育計画書の作成方法（例）

力量評価の結果をもとに、必要な力量を身に付けるための教育を計画します。以下の例をもとに、教育計画書の作成方法を説明します。

教育目的	ISO27001 認証取得のため
教育対象者	全従業者
教育方法	方法：e ラーニングによる自己学習、確認テスト。 委員会より、受講対象者に受講案内のメールを送付。 受講者は、案内にある URL から e ラーニングのシステムにアクセスし、 受講（テキストのダウンロード）／確認テストを行う。
教育内容	ISMS に対する意識向上 当社の方針や手順について（情報セキュリティ基本方針など） ISMS の有効性に対する自らの貢献 ISMS 要求に適合しないことの意味 当社のルールへの順守
実施期間	20XX 年-月-日（-）～20XX 年-月-日（-）
教育の有効性評価	情報セキュリティハンドブックを用いて教育を実施。 教育終了後、アンケート／確認テストを実施し記録に残す。 確認テストは、合格点は 100 点以上とする。 確認テストは、合格点に達するまで繰り返す。

教育計画書には、以下の内容を含めます。

教育目的	教育を実施する目的を記載します。
教育対象者	教育を受ける対象者を記載します。
教育方法	教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、e ラーニングなどさまざまあります。必要な力量を身に付けるために適切と考

	えられる方法を選択します。
教育内容	どのような教育を実施するのか、教育内容を記載します。
実施期間	教育を実施する期間を記載します。
教育の有効性評価	必要な力量を身に付けることができたか評価する方法を記載します。 明確に評価が可能であれば、どのような方法でも問題ないです。例えば、テストやアンケートの実施が挙げられます。次のページでテストの作成方法について説明します。

理解度確認テストの作成方法（例）

教育の実施後、必要な力量を身に付けることができたか評価するため、教育内容に関するテストを行うことが有効です。テストは、理解度が点数という数値で可視化されるため、評価がしやすく、多くの企業が実施しています。テストの作成例は以下の通りです。

次の【 】に入る言葉として最も適したものを選びなさい（各 10 点）

設問			答え
【 】とは、ISMS を構築・運用するための国際規格である。			C
A. ISO9001	B. ISO14001	C. ISO27001	
情報セキュリティという言葉は、一般的に、情報の【 】、 <u>完全性</u> 、 <u>可用性</u> を維持改善することと定義されている。			C
A. 信頼性	B. 整合性	C. 機密性	
2024 年度の当社の情報セキュリティ目標は、【 】である。			A
A. ISMS 教育受講／合格 100 %（全従業員）	B. 予防処置の発行件数を四半期に 1 件以上	C. <u>セキュリティインシデント</u> 発生件数／2 件以内	
【 】とは、企業や個人の情報を盗み取るため、特定の相手（企業組織や社員）をメールなどの手段で狙う攻撃のことです。			A
A. 標的型攻撃	B. ウイルス型攻撃	C. サイバー攻撃	
標的型メール攻撃の特徴はどれか。			B
A. 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。	B. 件名や本文に、組織の担当者の業務に関する内容が記述されている。	C. 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。	

次の文章のうち正しいものには○、間違っているものには×を付けなさい（各 10 点）

設問			答え
⑥ ISMS では、 <u>情報資産</u> とは、書類、データに加えて、ハードウェア、ソフトウェア、設備、ファームウェア（媒体など）、要員までも包括する。			○
⑦ 私物の外部記録媒体（USB メモリ、外づけ HDD など）の使用は原則禁止である。			○
⑧ 当社が重大な損失もしくは不利益を受けるような恐れのある機密情報を社外へ持ち出す場合は、責任者の許可を得て、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。			○
⑨ PC のログインパスワードは英数混合 8 文字以上のパスワードとする。			○
⑩ PC のパスワード付き <u>スクリーンセーバ</u> の設定時間は、15 分以内とする。			×
実施日		氏名	
所属		得点	点/100 点

- ✓ テストは、選択問題や正誤形式にすることにより採点がしやすくなります。
- ✓ 教育内容に合った問題を考え、作成します。例えば、今回の教育内容に「当社のルールへの順守」が含まれているため、⑥～⑩のような設問を作成します。

教育実施記録の作成方法（例）

教育を実施した際、実施記録を文書化する必要があります。以下の例をもとに、教育実施記録の作成方法を説明します。

教育の名称	ISMS 教育（基本方針、目標、ルール）
実施期間	20XX 年-月-日（-）～20XX 年-月-日（-）
実施方法	e ラーニング
使用テキスト	情報セキュリティハンドブック
教育の概要	情報セキュリティハンドブックなどによる ISMS に対する意識向上 ● 当社の方針や手順について（情報セキュリティ基本方針など） ● ISMS の有効性に対する自らの貢献 ● ISMS 要求に適合しないことの意味 ● 当社のルールへの順守 学習後にテスト実施
受講対象者・部門	上記教育実施期間において在籍する全従業員
参加者	別紙：「教育受講者一覧」を参照
備考	特になし

教育実施記録には、以下のような内容を含めます。

教育の名称	どのような教育を実施したのか、教育テーマを記載します。
実施期間	教育を実施する期間を記載します。
教育方法	教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、eラーニングなどさまざまあります。その中で、実際に実施した方法を記載します。
教育の概要	実施した教育の概要や、教育を実施した目的を記載します。
受講対象者・部門	教育を受講する対象者を記載します。
参加者	教育を実際に受講した者を記載します。以下の例のように、「教育の受講者一覧」を別紙で作成し、実施記録と分けて記載するとわかりやすくなります。

No	所属	氏名	受講日
1	営業	〇〇〇〇	20XX/-/-
2	管理	〇〇〇〇	20XX/-/-

7.3 認識

ISMS 適用範囲で働くすべての社員、従業員が情報セキュリティ方針を理解し、それを実現することの重要性を認識する必要があります。逆に、セキュリティ対策を実施せず、セキュリティ方針を実現できなかった場合、どのようなことが起きるのかについて理解する必要もあります。

具体的には、以下の内容について教育を行い、ISMS の重要性を十分理解させる必要があります。

- 情報セキュリティ方針
- 情報セキュリティパフォーマンスの向上によるメリットや、自身の業務と ISMS の関係、実施すべきセキュリティ対策の具体的な内容
- ISMS によって割り当てられた責任を果たさなかった場合の組織に与える影響

これらの内容について認識を持たせるために、教育や訓練を実施します。具体的な教育・訓練の実施手順は、「力量」や「コミュニケーション」で説明します。

力量

上記の内容について、各要員が認識しているか評価を行い、認識が不十分の場合は教育を実施し、認識させます。

コミュニケーション

情報提供・共有によって、上記の内容の認識を深めるようにします。

7.4 コミュニケーション

ISMS の PDCA サイクルを回すためには、内部および外部とのコミュニケーションを円滑に行う必要があります。そのため、組織内および組織外の関係者とコミュニケーションをとる手順などを定め、必要なときに円滑なコミュニケーションが行える体制を整えておくことが重要です。コミュニケーションの手順などには、以下の内容が含まれます。

- コミュニケーションの内容
- コミュニケーションの実施時期
- コミュニケーションの対象者
- コミュニケーションの方法

ISMS に関連するコミュニケーションをとる手順を確立した例を、以下に示します。例を参考に、自社の ISMS に対して PDCA サイクルを回す上で必要なコミュニケーションをとる手順を確立します。

内容	実施時期	対象者	実施者	方法
情報セキュリティ方針の伝達	随時	利害関係者	トップマネジメント（ISMS 事務局）	外部 ・ 当社 HP に公表 内部 ・ ISMS 定期教育にて ・ 当社 HP に公表 ・ 社内掲示
各見直し結果の伝達	見直し後、1 週間以内	従業員	ISMS 事務局	承認後、ISMS 事務局より通達
セキュリティ調査結果の報告	依頼入手時	お客様	ISMS 事務局	・ お客様より調査票などを入手した場合、主管部門にて回答を作成 ・ ISMS 事務局責任者が確認の上、お客様に提出
セキュリティインシデントの伝達	発見時	ISMS 事務局	発見者	「情報セキュリティ手順書：セキュリティインシデント対応フロー」の通り
	適時	トップマネジメント	ISMS 事務局	同上

	適時	関係当局	ISMS 事務局	同上

内容	コミュニケーションで伝える情報
実施時期	伝えるタイミング
対象者	誰に伝えるのか、情報を伝える対象者
実施者	誰に伝えるのか、情報を対象者に伝える者
方法	情報を伝える手段

7.5 文書化した情報

ISMS に必要な文書化した情報の作成、更新、管理方法を決めます。

一般

以下の情報を ISMS に含める必要があります。

- ISO/IEC 27001 が要求する文書化した情報
- ISMS の有効性のために必要であると組織が判断した文書化した情報

以下は、ISO/IEC 27001 が要求する文書化した情報の一覧です。

文書化した情報	作成する項番
ISMS の適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	
力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMS のプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメントレビューの結果	
不適合の内容と処置、処置の結果	「10. 改善」で作成

作成および更新

ISMS に必要な文書化した情報を作成・更新する際に、以下の事項を確実にする必要があります。

1. 適切な識別と記述

文書化した情報を識別できるよう、以下の例のように採番方法を決めたり、各文書には適切なタイトル、作成者、承認者、日付などを記載したりします。

文書の種類	採番方法
基本文書	A-□□（01 から採番を始める）
ISMS マニュアル	B-01
手順書	C-01
記録類	D-01
外部文書	採番せずに文書名、作成社名などの名称にて識別する

2. 適切な形式

文書化する情報を記載する媒体として、紙や電子データなどを指定し、適切な形式（文字、図表など）を用いて読みやすく、簡潔に記載します。

3. 適切なレビューと承認

文書化した情報は、適切な承認とレビューを行い策定します。

文書化した情報の管理

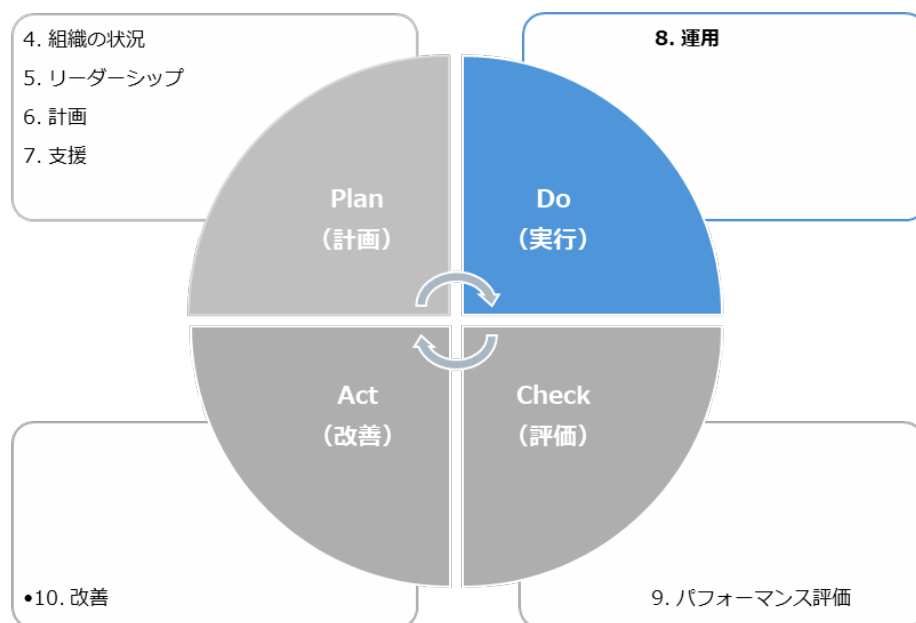
ISMS の文書化した情報を管理する必要があります。

（管理方法の例）

文書化した情報は、ISMS 事務局責任者が、最新版を紙の媒体としてファイリングし、キャビネットにて保管し、適用範囲内の対象者が必要なときに、必要なところで利用可能にする

13-2-6. ISMS : 8. 運用

「8. 運用」は、PDCA サイクルの「Do (実行)」に位置しており、「6. 計画」で計画した活動や、要求事項を満たすための活動を実施し、管理します。そして、計画通りに実施した証拠となる情報を文書化し、保持する必要があります。



8. 運用	作成文書（例）
8.1 運用の計画及び管理 「6. 計画」で計画した活動や、要求事項を満たすための活動の実施状況を管理するための一覧表を作成します。	ISMS 年間計画表
8.2 情報セキュリティリスクアセスメント 「6. 計画」で定めた リスクアセスメント のプロセスを実施し、結果を文書化します。	リスクアセスメント結果報告書
8.3 情報セキュリティリスク対応 「6. 計画」で定めたリスク対応計画を実施し、結果を文書化します。	リスク対応計画

8.1 運用の計画及び管理

作成する文書	● ISMS 年間計画表

「6. 計画で決定した活動」および「要求事項を満たすための活動」を実施するにあたり必要な

プロセスを計画し、ISMS 年間計画表を作成します。ISMS 年間計画表は、「6. 計画で決定した活動」および「要求事項を満たすための活動」の実施状況を管理するための計画表です。

ISMS 年間計画表の作成方法

以下の例は、「6. 計画」で決定した活動に関する計画表の例です。

No	実施事項	文書名	スケジュール							
			2024 年 5 月				2024 年 6 月			
			8	15	22	29	5	12	19	26
6.1	「リスク及び機会に対処する活動」の検討	外部および内部の課題に対する活動の検討								
		資産目録								
		リスクアセスメントの実施								
		リスクアセスメント結果報告書								
		リスク対応のための計画作成								
		(アクションプランの作成)								
6.2	部門ごとに「情報セキュリティ目的及びそれを達成するための計画」を作成	情報セキュリティ手順書								
		ISMS 有効性評価表								

No	ISO/IEC 27001 の要求事項の項番を記載します。
実施事項	行う活動の内容を記載します。
文書名	実施事項で記載した活動を行う際に利用したり、作成したりする文書名を記載します。
スケジュール	実施事項を行う予定日を記載します。

ISMS の要求事項全体を示した計画表の例を紹介します。

前記の計画表は、ISMS の要求事項のうち「6.計画」の箇所だけを抜粋し、作成が必要な文書や、細かいスケジュールを示すことに焦点を当てたものですが、次の計画表は年間を通して実践すべき事項を記載したものとなっています。

期間	月	年に 1 回	月に 1 回	四半期に 1 回	随時
第 1 四	4 月	● 課題に対する活動の検討	● 入退記録の確	● バックアッ	● 「関係当局

半期			認 ● 運用チェックリストによる確認 ● バックアップされていることの確認 ● イベントログの確認 ● 利用者が利用可能なソフトウェアの確認	プされていることの確認 ● イベントログの確認	との連絡」体制の見直し ● 法令規制一覧表の確認
	5月	● リスクアセスメントの実施	同上		
	6月	● リスク対応のための計画作成（アクションプランの作成） ● 管理策（ルール）の検討	同上		
第2四半期	7月	● 「情報セキュリティリスク対応」計画の実行	同上	同上	
	8月	● ISMSの有効性の評価 ● 情報セキュリティパフォーマンス	同上		
	9月	● 資産目録の見直し ● 情報の分類 ● アクセス権限の見直し	同上		
第3四半期	10月	● システム開発の外部委託先の再審査	同上	同上	
	11月	● 情報セキュリティ計画 ● 情報セキュリティ継続の検証・レビュー	同上		
	12月	● 内部監査計画 ● 内部監査の実施	同上		

		● マネジメントレビュー ● 不適合及び是正処置のレビュー			
第4四半期	1月	● 主要メンバーの「力量」の評価・証拠の文書化 ● 定期教育 ● UPSのバッテリーの確認	同上	同上	
	2月	● 外部審査（審査機関による更新審査）の実施	同上		
	3月	● 情報セキュリティのための方針群のレビュー ● 秘密保持契約書の確認	同上		

8.2 情報セキュリティリスクアセスメント

追記する文書

- リスクアセスメント結果報告書

リスクアセスメントを実施する際は、結果を「リスクアセスメント結果報告書」に追記します。

リスクアセスメント結果報告書の追記方法

リスクアセスメント結果報告書の「対応」の箇所に、管理策の実施状況を記載します。
「13-2-4. ISMS：6.計画」を参照してください。

8.3 情報セキュリティリスク対応

追記する文書

- リスク対応計画

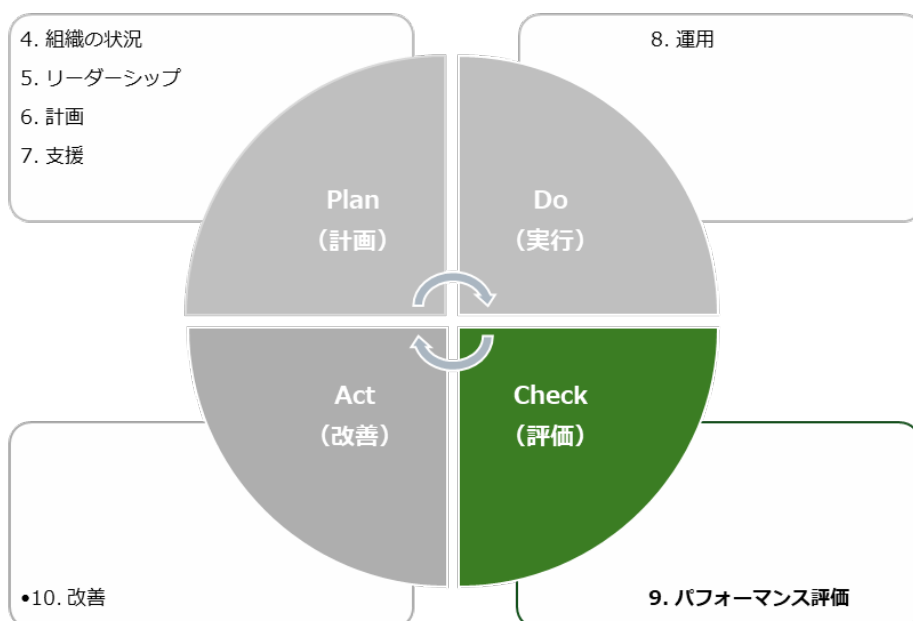
リスク対応を実施する際は、結果を「リスク対応計画」に追記します。

リスク対応計画の追記方法

リスク対応計画の「実績」、「ステータス」の箇所に記載します。
「13-2-4. ISMS：6.計画」を参照してください。

13-2-7. ISMS : 9. パフォーマンス評価

「9. パフォーマンス評価」は、PDCA サイクルの「Check（評価）」に位置しており、定めた情報セキュリティ目標を達成するための取組（構築した ISMS）が有効であるか否かを評価します。



パフォーマンス評価	作成文書（例）
9.1 監視、測定、分析及び評価 情報セキュリティのパフォーマンスと、ISMS の有効性を評価します。	● ISMS 有効性評価表
9.2 内部監査 ISMS の適合性、有効性について、あらかじめ定めた間隔で監査を実施します。	● 内部監査チェックリスト ● 内部監査計画書 ● 内部監査結果報告書
9.3 マネジメントレビュー トップマネジメントが、ISMS の有効性を評価します。	● マネジメントレビュー報告書

9.1 監視、測定、分析及び評価

作成する文書	● ISMS 有効性評価表

ISMS の効果について判断するために、有効性評価を実施します。ISMS に沿って実施している活動が、情報セキュリティ目標の達成に繋がっているのか、有効に作用しているのかを評価し、課題があるのであれば改善することになります。PDCA サイクルによる継続したスパイラルアップに

よって、改善し続けることが重要です。計画時に定めた評価指標および評価方法により、ISMS が有効だったか、そうではなかったかを判断します。この有効性の評価は、マネジメントレビューの際にトップマネジメントが実施することが効果的です。

ISMS 有効性評価表に記載する方法は、「13-2-4. ISMS : 6. 計画」を参照してください。

9.2 内部監査

作成する文書

- 内部監査チェックリスト
- 内部監査計画書
- 内部監査結果報告書

内部監査とは、社内のルールや扱っている文書が ISO/IEC 27001 の要求事項を満たしており、従業員などがそのルールを守って仕事をしているか否かをチェックすることです。内部監査結果報告書をもとに、マネジメントレビューで「自社の ISMS はこのままでいいのか」「自社の ISMS のどこに欠陥があり、どう修復しなくてはならないのか」を経営層が判断し、随時対策をとります。内部監査は一般的に以下のプロセスを進めます。



1. 内部監査員の選定

内部監査とは、組織内部において、専門的知識を持った人が、経営者や役員などの立場にない第三者として、ISMS が適切に構築され、適正に運用されているか否かを評価することです。内部監査員には、監査の公正さや客観性の観点から、監査対象となる部門に所属していない者を任命する必要があります。内部監査員に資格などは不要ですが、下記に当てはまるような人が適任です。社内に適した者がいない場合は、研修により内部監査員を育成したり、外部の専門家へ依頼したりするといった手段をとることが有効です。

- ISMS の内容を理解している人
- ISMS の内部監査の体制や実施方法といった手順に関する知識を有している人
- 自社の ISMS を把握している人
- 監査対象となる部署の業務内容を把握している人

2. 内部監査チェックリストの作成

内部監査員がチェックリストを作成します。事前にチェックリストを作成することにより、監査すべき範囲やポイントが明確になったり、チェック漏れを減らせたり、内部監査員ごとの偏った評価を防止したりといった効果が期待できます。また、チェックリストは内部監査を行った文書記録とすることができます。

内部監査チェックリストの作成方法（例）

ISMS の項目に沿ってチェック事項をまとめ、内部監査を実施の際には確認した ISMS の根拠となる確認結果や文書類を記録します。

監査項目	チェック事項	確認結果・文書類
4. 組織の状況		
4.1 組織及びその状況の理解	組織は、組織の目的に関連し、かつ、その ISMS の意図した成果を達成する組織の能力に影響を与える、外部および内部の課題を決定しているか。	外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解	次の事項を決定したか。 a) ISMS に関連する利害関係者 b) その利害関係者の、情報セキュリティに関連する要求事項	外部および内部の課題
4.3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMS の適用範囲は、文書化されているか。	ISMS マニュアル ISMS 適用範囲 レイアウト図 ネットワーク図
5. リーダーシップ		
5.1 リーダーシップ及びコミットメント	トップマネジメントは、 a) 情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしているか。	情報セキュリティ方針 質問で確認
5.2 方針	情報セキュリティ方針は、 e) 文書化した情報として利用可能であるか。	情報セキュリティ方針

事前に作成する部分

監査時に記載する部分

3. 内部監査の計画立案

内部監査の計画を立てます。いつ、誰が、どの部門の誰に、何についてチェックするか、といったことを事前に段取りしておきます。

内部監査計画書の作成方法（例）

監査概要				
監査名称	ISO27001 認証取得に関する内部監査			
監査目的	ISO/IEC27001:2022 認証取得に向けた当社 ISMS の整備、運用状況を確認			
監査テーマ	● 管理策の運用状況、および有効性の確認 ● 第一段階審査の指摘に対する改善状況の確認			
監査方法	被監査部門に対するヒアリング、文書化された情報の閲覧、およびオフィスの視察			
監査基準	JISQ27001:2022（ISO/IEC27001:2022）の要求事項、当社 ISMS マニュアル、および情報セキュリティ手順書			
詳細監査計画				
No	被監査部門名	監査人	応対者	日時
1	情報システム部	〇〇 〇〇	△△ △△	20XX/-/- 00:00
2	管理部	〇〇 〇〇	△△ △△	20XX/-/- 00:00
3	営業部	〇〇 〇〇	△△ △△	20XX/-/- 00:00
4	総務部	〇〇 〇〇	△△ △△	20XX/-/- 00:00
内部監査結果報告（予定）				
報告予定日		20XX 年〇月		
報告手段		報告会の開催		

監査概要	監査の名称、目的、テーマ、方法、基準を記載します。
詳細監査計画	監査の対象となる部門名、監査人名、監査への対応者名、監査実施の日時といった予定を記載します。
内部監査結果報告（予定）	監査結果の報告予定日と報告手段を記載します。

4. 内部監査の実施

内部監査計画に沿って、内部監査チェックリストを用いて監査を実施します。

5. 内部監査結果報告書の作成

内部監査の結果をとりまとめ、報告書を作成します。どの部署で、どのルールが守られなかったかといったことを明確にしておきます。内部監査結果報告書をもとに、経営層は自社の ISMS をど

のようにするか判断することになるため、内容に不明瞭な点や不足があると、適切な見直しができなくなってしまうため、注意が必要です。

内部監査結果報告書の作成方法（例）

監査名称	ISO27001 認証取得に関する内部監査		
監査実施日時	20XX 年-月		
監査目的	ISO/IEC27001:2022 認証取得に向けた当社 ISMS の整備状況を確認		
監査体制			
被監査部門①	情報システム部	監査人①	【名前】 / 【社名】
被監査部門②	管理部	監査人②	
被監査部門③	営業部	監査人③	
被監査部門④	総務部	監査人④	
監査総評	ISMS の整備状況を確認 当組織での ISMS は、ISO27001:2022 規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されなかった。全体として適切となる有効な仕組みにより運用を開始したと判断できる。 また社員の周知に関しては、ISMS 教育の実施などにより体制や方針などの周知を行っていた。 不適合・観察事項 一部ではあるが、対応が十分でない事項があったため○件を軽微な不適合、○件を観察事項とした。重大な不適合は、検出されなかった。 【軽微な不適合】		
	No	規格	内容
	1	5.2 方針	規格では「情報セキュリティ方針は、次の事項を満たさなければならない。g) 必要に応じて、利害関係者が入手可能である。」としている。しかし、「情報セキュリティ方針」について、お客様などの利害関係者が入手可能であることを確認できなかった。
	【観察事項】		
	No	規格	内容
	1	4.3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMS マニュアルとネットワーク図で適用範囲の表現が同じであることを確認が難しい状況でした。ISMS マニュアルでは、ルータまで。ネットワーク図では、ONU まで。

	2	7.3 認識	実施中の ISMS 教育の終了をお願いします。
備考 (フォローアップなど)	次回の内部監査にて対応のフォローを行う		

9.3 マネジメントレビュー

作成する文書	● マネジメントレビュー報告書

マネジメントレビューとは、経営者（トップマネジメント）が行うレビュー活動です。トップマネジメントは、内部監査の結果や利害関係者からのフィードバックをもとに、組織の ISMS が適切に運用されているか否かを判断し、必要に応じて改善方法を指示します。この活動は、少なくとも年に 1 回定期的実施することが求められています。トップマネジメントに報告した内容（インプット）と、トップマネジメントの指示や提案（アウトプット）を文書化したものが、マネジメントレビュー報告書です。



インプット、アウトプットに含める必要がある内容は以下の通りです。

インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMS に関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMS に関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 ● 不適合および是正処置 ➤ 不適合に対する是正処置の実施状況を報告します。

● 監視および測定の結果 ➤ 情報セキュリティパフォーマンスや、ISMS の有効性についての監視、測定結果を報告します。 ● 監査結果 ➤ 内部監査の結果を報告します。 ● 情報セキュリティ目的の達成 ➤ 情報セキュリティ目的の達成数や未達成数など、情報セキュリティ目的の達成状況を報告します。
5. 利害関係者からのフィードバック 利害関係者から、情報セキュリティに関する要望などについて、対応した結果を報告します。
6. リスクアセスメントの結果およびリスク対応計画の状況 リスクアセスメント により、新しく特定したリスクや、リスク対応計画の進捗状況を報告します。
7. 継続的改善の機会 トップマネジメントに改善策を提案します。
アウトプットに含める必要がある事項
1. 継続的改善の機会 改善すべき内容について指示を記載します。
2. ISMS のあらゆる変更の必要性 ISMS に関して、次年度以降変更すべき内容について指示を記載します。

マネジメントレビュー報告書の作成方法（例）

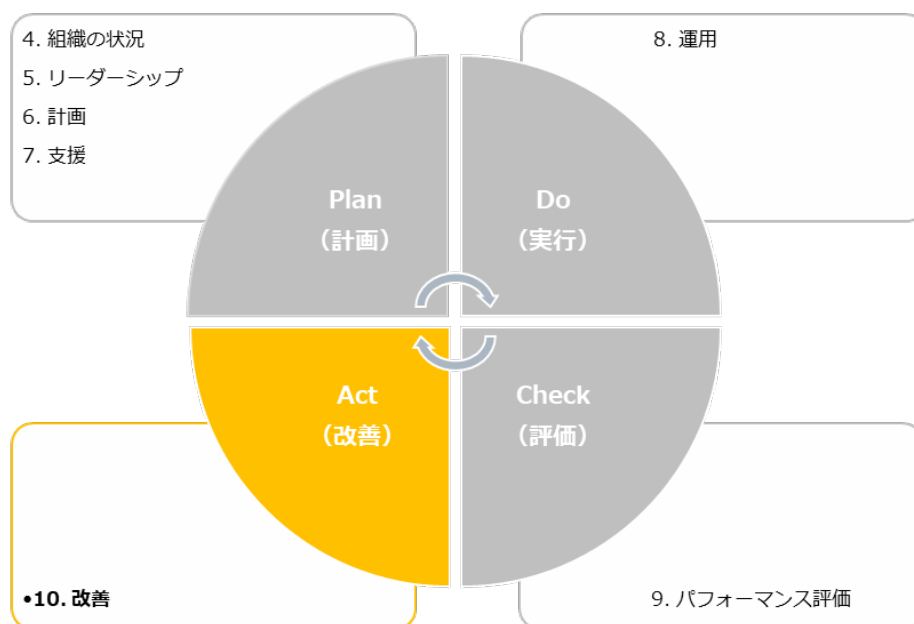
出席者	トップマネジメント	【名前】	日時	20XX 年〇月	
	情報セキュリティ委員長	【名前】			
	ISMS 内部監査責任者	【名前】		00 : 00 ~ 00 : 00	
インプット（報告事項）					
1	前回までの指示事項に対する処置の進捗や結果	初回マネジメントレビューのためありません。			
2	ISMS に関連する外部および内部の課題の変化	「外部および内部の課題」にて報告の通りです。 その後、課題の変化は発生していません。			
3	ISMS に関連する利害関係者のニーズおよび	お客様からの情報セキュリティに関する要求の変化はありませんでした。			

	び期待の変化		
4	情報セキュリティパフォーマンスの実績報告	1) 不適合および是正措置	20XX 年〇月に実施した初回の内部監査により検出された“観察事項”1 件は、是正対応中です。 今月末までに対応を予定しています。 そのほか現在対応中の不適合はありません。
		2) 監視および測定の結果	次回のマネジメントレビューにて測定結果を報告します。
		3) 監査結果	【内部監査】 20XX 年〇月に 1 回目の内部監査を実施し、主に ISMS の文書類整備状況の確認を行いました。 ①ISO27001 規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されませんでした。全体として適切な仕組みにより運用を開始したと判断します。 ②一部ではありますが、対応が十分でない事項があり、観察事項 1 件が検出されました。 詳細は、「内部監査結果報告書」（20XX 年〇月）にて報告の通りです。
		4) 情報セキュリティ目的の達成	次回のマネジメントレビューにて報告します。
5	利害関係者からのフィードバック	お客様からのクレームは現状ありませんでした。	
6	リスクアセスメントの結果およびリスク対応計画の状況	【リスクアセスメントの状況】 「情報リスクアセスメント結果報告書」（20XX 年〇〇月〇〇日）にて報告の通りです。 【リスク対応計画の状況】 ● リスク対応計画にリストアップした管理策：〇件 ● 対応が終了した管理策：〇件 ● 対応が終了していない管理策 2 件は以下の通りです。 ※詳細は、「リスク対応計画」（作成：20XX 年〇〇月〇〇日、見直：20XX 年〇月）にて報告の通りです。	
7	継続的改善の機会	現状は ISMS を従業者が理解するための活動を主として行っています。	
アウトプット（トップマネジメントの指示事項）			
1	継続的改善の機会	現状認識している各課題を確実に実施すること。	
2	ISMS のあらゆる変更の必要性	コンサルタント会社のひな形にとらわれず、より当社の状況を反映した仕組み・ルールに見直しを行っていくこと。	

13-2-8. ISMS : 10. 改善

「10. 改善」は、PDCA サイクルの「Act (改善)」に位置しており、[ISMS](#) の改善を行います。

10. 改善	作成文書 (例)
10.1 継続的改善 ISMS の PDCA サイクル (「4. 組織の状況」から「10. 改善」までの活動) を継続して実施し、情報セキュリティパフォーマンスを向上させるために必要となる改善を行っていきます。具体的には、情報セキュリティ方針や情報セキュリティ目的の計画、 リスクアセスメント やリスク対応をもとに決定した管理策の実施を継続して行い、改善していきます。	—
10.2 不適合及び是正処置 不適合が発生した際には是正処置を実施します。不適合とは、ISMS の要求事項を満たしていないことです。具体的には、管理策の不備や未実施、 セキュリティインシデント の発生などのことです。	● 是正要求書兼回答書



10.2 不適合及び是正処置

作成する文書	● 是正要求書兼回答書

```
graph LR; A[不適合の発生] --> B[不適合を特定する]; B --> C["・ 不適合を管理し、修正するための処置をとる  
・ 不適合によって起こった結果に対処する"]; C --> D[不適合をレビューする]; D --> E[不適合の原因を特定する]; E --> F["・ 類似の不適合が他でも発生しているか調査する  
・ 類似の不適合が発生する可能性を調査する"]; F --> G[必要な処置を決定し、実施する]; G --> H[実施した処置の有効性を評価する]; H --> I[必要に応じて、ISMSを変更する]; I --> A;
```

不適合の発生

修正

不適合を特定する

- ・ 不適合を管理し、修正するための処置をとる
- ・ 不適合によって起こった結果に対処する

是正処置

不適合をレビューする

不適合の原因を特定する

- ・ 類似の不適合が他でも発生しているか調査する
- ・ 類似の不適合が発生する可能性を調査する

必要な処置を決定し、実施する

実施した処置の有効性を評価する

必要に応じて、ISMSを変更する

是正要求書兼回答書の作成方法（例）

整理番号		00-00		対象部門		〇〇〇〇部門		発効日		20XX		年	-	月	-	日	
入力 情報	分類	監査	☒ 内部監査における指摘事項														
			☐ 外部機関が実施した監査における指摘事項（機関名： ）														
			監査年月日			年			月			日		監査者			
			指摘のランク		観察事項						要求事項 項番		7.2 力量				

13-3. ISMS 文書体系（ISMS 構築・導入に必要な文書と記録）

13-3-1. ISMS 文書としての策定内容とポイント

対策基準を策定する際は、ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考にするとよいでしょう。ただし、組織が対策基準を策定する際は、組織の業態や規模によって必要となる管理策は異なるので、取捨選択することが必要です。ISO/IEC 27001:2022 の附属書 A や ISO/IEC 27002:2022 は網羅的に管理策がリストアップされているので、自組織に必要な管理策が含まれています。またその一方、このリストにない管理策が必要となるケースもあることに注意が必要です。自組織におけるサイバーセキュリティリスクを自ら考えて必要な管理策を選択するために、[リスクアセスメント](#)の手法を使用し、対策基準を策定します。

ISO/IEC 27001:2022 附属書 A の管理策		
カテゴリ	項目数（合計 93）	概要
組織的管理策	37	組織として取り組む必要のある管理策。例えば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取り組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。例えば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、 脆弱性 管理、ログ管理、 マルウェア 対策などが含まれます。

対策基準策定時の注意点

[ISMS](#) の認証取得を目標にして情報セキュリティ対策を進めると、文書の整備が目的になり、本来の情報セキュリティ対策がおざなりになってしまい、ISMS が形骸化するケースが少なくありません。策定した管理策が継続的に実行されていくことが重要となります。組織は、情報セキュリティリスクを適切にコントロールするために必要となる管理策の有効性を検討し、対策基準を策定することが大切です。



13-3-2. ISMS の要求事項および管理策

ISO/IEC 27001 の要求事項

ISO/IEC 27001 では、組織が効率的に ISMS の構築・実施・維持・継続的改善を行うとともに、情報セキュリティの リスクアセスメント およびリスク対応を実現するために必要な要求事項を定めています。ISO/IEC 27001 の要求事項は、ISMS 認証を取得するには必ず対応しなければなりません。どのような内容が要求されているのか認識するため、各要求事項の概要について説明します。要求事項は、後述の PDCA サイクルと呼ばれる運用サイクルに落とし込むことにより、情報セキュリティマネジメントを実施することになります。

ISMS の運用プロセス

マネジメントシステムとは、組織の方針や目標を定めて、その目標を達成するために必要な、組織を管理する仕組みのことを指します。情報セキュリティのマネジメントシステムである ISMS も、組織によって定めた目標達成のための取組です。その目標は、情報セキュリティに関することや、会社が抱えている機密情報をどう保護していくのかという内容となります。その目標に向かってマネジメントを行っていくための方法として、要求事項を実施しながら、PDCA (Plan・Do・Check・Act) サイクルを繰り返し、スパイラルアップしていくことが、ISO/IEC 27001 では求められています。

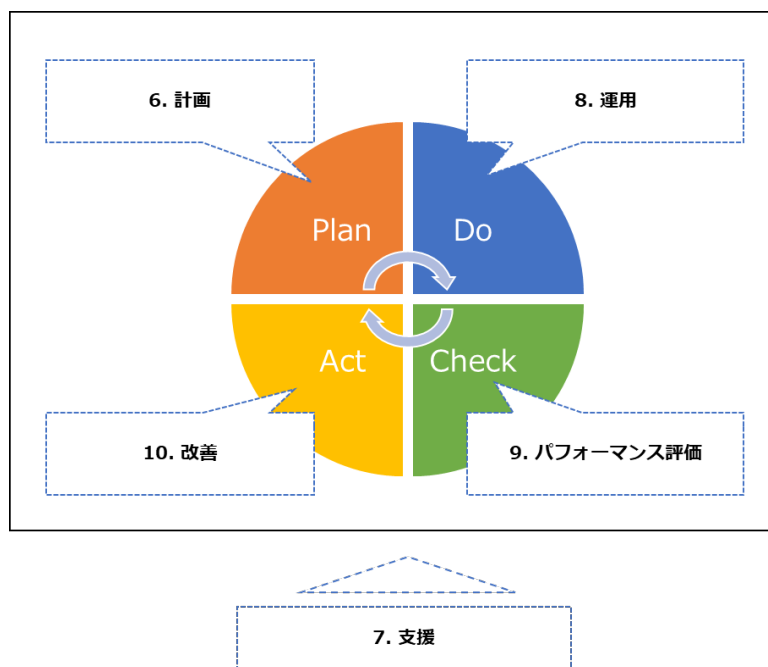


図 56. ISO/IEC 27001 の PDCA サイクル

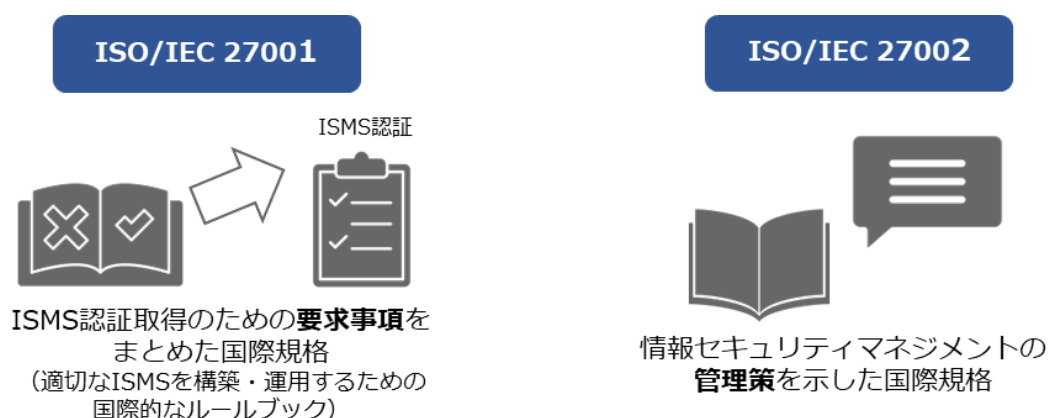
詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

ISMS の管理策

ISO/IEC 27001 に記載されている要求事項をもとに、具体的な情報セキュリティマネジメントの管理策を示した規格として ISO/IEC 27002 があります。ISO/IEC 27001 の付属書 A は、この ISO/IEC 27002 の内容をそのまま取り入れたもので、情報セキュリティ上のリスクを低減するための目的と、その目的を達成するための管理策で構成されています。

付属書 A は、ISMS の本文（ISO/IEC 27001 の規格要求事項）を補完するガイドラインとしての位置づけにあります。業務内容や ISMS の適用範囲によってはすべての管理策を適用することができない場合があります。その際には、適用できない理由を明確にし、採用しないという選択をすることができます。つまり、一律にすべての管理策を適用するのではなく、理由を含めて採用しない管理策を明示する必要があります。

ISO/IEC 27002 では、合計 93 種の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4 カテゴリに分類される形で解説されています。



情報セキュリティ管理策		
カテゴリ	項目数	概要
組織的管理策	37	組織として取り組む必要のある管理策。例えば、情報セキュリティの方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取り組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。例えば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的対策	34	技術面での管理策。ネットワークのセキュリティ、

		データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

ISO/IEC 27002 の箇条 5～8 は、93 種の ISMS 管理策で構成されています。以下の表は、それらの管理策標題の一覧です。詳細については「(別紙) ISO/IEC 27002:2022 管理策と目的」をご確認ください。

組織的管理策	
5.1 情報セキュリティのための方針群	5.19 供給者関係における情報セキュリティ
5.2 情報セキュリティの役割及び責任	5.20 供給者との合意における情報セキュリティの取扱い
5.3 職務の分離	5.21 ICT サプライチェーンにおける情報セキュリティの管理
5.4 経営陣の責任	5.22 供給者のサービス提供の監視、レビュー及び変更管理
5.5 関係当局との連絡	5.23 クラウドサービスの利用における情報セキュリティ
5.6 専門組織との連絡	5.24 情報セキュリティインシデント管理の計画及び準備
5.7 脅威インテリジェンス	5.25 情報セキュリティ事象の評価及び決定
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.26 情報セキュリティインシデントへの対応
5.9 情報及びその他の関連資産の目録	5.27 情報セキュリティインシデントからの学習
5.10 情報及びその他の関連資産の利用の許容範囲	5.28 証拠の収集
5.11 資産の返却	5.29 事業の中断・障害時の情報セキュリティ
5.12 情報の分類	5.30 事業継続のための ICT の備え
5.13 情報のラベル付け	5.31 法令、規制及び契約上の要求事項
5.14 情報転送	5.32 知的財産権
5.15 アクセス制御	5.33 記録の保護
5.16 識別情報の管理	5.34 プライバシー及び PII の保護
5.17 認証情報	5.35 情報セキュリティの独立したレビュー
5.18 アクセス権	5.36 情報セキュリティのための方針群、規則及び

	標準の順守
	5.37 操作手順書

6.人的管理策	
6.1 選考	6.5 雇用の終了又は変更後の責任
6.2 雇用条件	6.6 秘密保持契約又は守秘義務契約
6.3 情報セキュリティの意識向上，教育及び訓練	6.7 リモートワーク
6.4 懲戒手続	6.8 情報セキュリティ事象の報告

7.物理的管理策	
7.1 物理的セキュリティ境界	7.8 装置の設置及び保護
7.2 物理的入退	7.9 構外にある資産のセキュリティ
7.3 オフィス，部屋及び施設のセキュリティ	7.10 記憶媒体
7.4 物理的セキュリティの監視	7.11 サポートユーティリティ
7.5 物理的及び環境的脅威からの保護	7.12 ケーブル配線のセキュリティ
7.6 セキュリティを保つべき領域での作業	7.13 装置の保守
7.7 クリアデスク・クリアスクリーン	7.14 装置のセキュリティを保った処分又は再利用

8.技術的管理策	
8.1 利用者終端装置	8.18 特権的なユーティリティプログラムの使用
8.2 特権的アクセス権	8.19 運用システムに関わるソフトウェアの導入
8.3 情報へのアクセス制限	8.20 ネットワークのセキュリティ
8.4 ソースコードへのアクセス	8.21 ネットワークサービスのセキュリティ
8.5 セキュリティを保った認証	8.22 ネットワークの分離
8.6 容量・能力の管理	8.23 ウェブ・フィルタリング
8.7 マルウェアに対する保護	8.24 暗号の使用
8.8 技術的ぜい弱性の管理	8.25 セキュリティに配慮した開発のライフサイクル
8.9 構成管理	8.26 アプリケーションのセキュリティの要求事項
8.10 情報の削除	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

8.11 データマスキング	8.28 セキュリティに配慮したコーディング
8.12 データ漏えいの防止	8.29 開発及び受入れにおけるセキュリティ試験
8.13 情報のバックアップ	8.30 外部委託による開発
8.14 情報処理施設の冗長性	8.31 開発環境、試験環境及び運用環境の分離
8.15 ログ取得	8.32 変更管理
8.16 監視活動	8.33 試験情報
8.17 クロックの同期	8.34 監査試験中の情報システムの保護

(出典) MSQA「ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド」を基に作成

ISMS の管理策における属性

ISO/IEC 27002 では、2022 年の改訂より「属性」という考え方が新たに追加されました。この「属性」についての各管理策としては「予防（preventive）」、「検知（detective）」、「是正（corrective）」のいずれかに分類され、またその特性によって「機密性」、「完全性」、「可用性」のいずれかに関連付けられています。さらに、サイバーセキュリティ概念、運用機能、セキュリティドメインという 3 つの観点からも属性のグループ分けが行われています。「属性」という考え方が追加された結果、各管理策をより柔軟かつさまざまな場面に採用できるようになりました。

この「属性」という考え方は、他の組織や団体が発行するガイドラインなどとの親和性を高める効果も期待できます。例えば、「サイバーセキュリティ概念」では「識別、防御、検知、対応、復旧」という 5 つの属性値が示されていますが、これは米国国立標準研究所（NIST）が発行している CSF（サイバーセキュリティフレームワーク） でも採用されているものです。また、組織は自らの視点を作るために、独自の属性を作ることも可能です。

管理策タイプ
情報セキュリティインシデントの発生との関係において、リスクをいつどのように修正するかという観点から管理策を見る属性 [属性値] 予防、検知、是正
情報セキュリティ特性
情報のどの特性の維持に寄与するかという観点から管理策を見る属性 [属性値] 機密性、完全性、可用性
サイバーセキュリティ概念
ISO/IEC TS 27119 に記述されているサイバーセキュリティフレームワークで定義された、サイバーセキュリティ概念との関連付けの観点から管理策を見る属性 [属性値] 識別、防御、検知、対応、復旧

運用機能

実践者の情報セキュリティ機能の観点から管理策を見る属性

〔属性値〕ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティを保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、[供給者](#)関係のセキュリティ、法および順守、情報セキュリティ事象管理、情報セキュリティ保証

セキュリティドメイン

情報セキュリティドメインの観点から管理策を見る属性

〔属性値〕ガバナンスおよびエコシステム、保護、防御、対応力

13-4. ISO/IEC27001 の審査準備と審査内容

13-4-1. ISO/IEC27001 の認証機関の選定と申し込み

認証取得の申請先

組織が ISO/IEC 27001 の認証を取得するためには、一般社団法人情報マネジメントシステム認定センター（ISMS-AC）から認定された認証機関からの審査を受け、認証基準に適合していると認められる必要があります。

ISO/IEC27001（ISMS）における「認証」と「認定」は似た用語ですが、英語では“certification”と“accreditation”で異なる意味を持つ用語です。「認証」は組織の情報セキュリティマネジメントシステムが ISO 27001 の規格に適合していることを公的機関が証明することです。一方、「認定」は、審査機関が十分な審査能力をもち、かつ公平な審査が行われていることを証明する仕組みです。日本では ISMS-AC が ISMS の認証機関を認定しています。

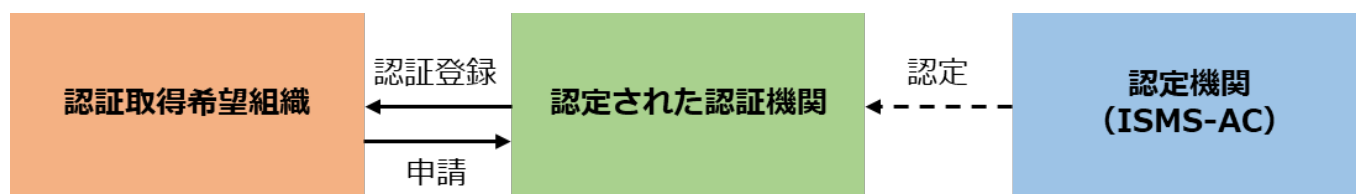


図 57. 認証取得の申請先

（出典）JIPDEC「ISMS/ITSMS/BCMS/CSMS 認証を取得するには」をもとに作成

認証機関の選択

認証取得を希望する組織は認定された認証機関の中から選んで申請します。

認定された認証機関は、ISMS-AC の Web ページに掲載されています。

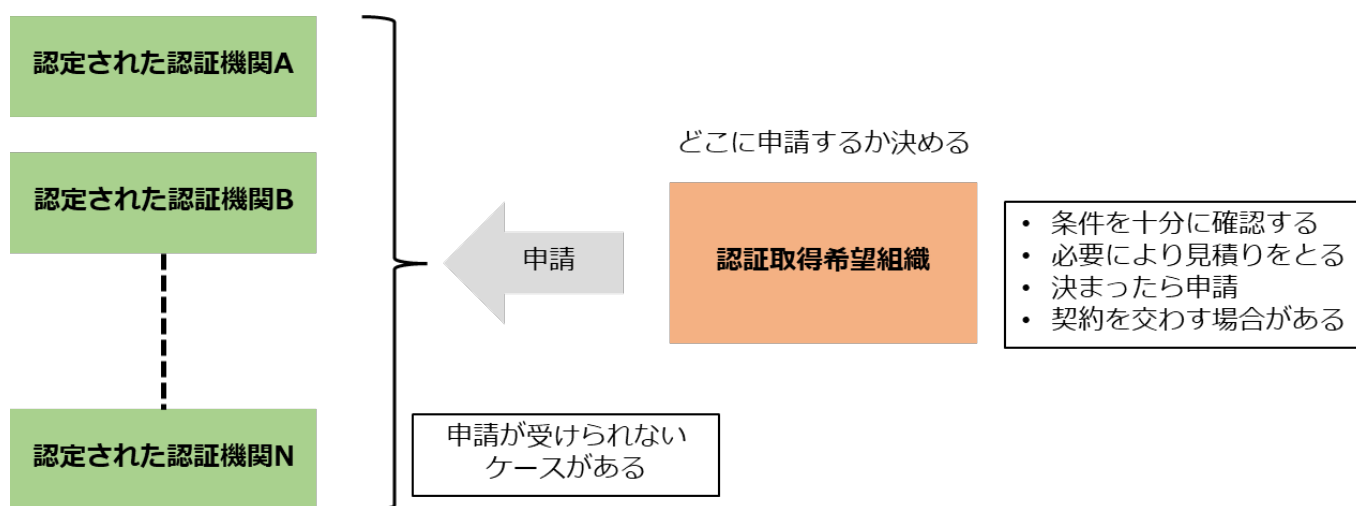


図 58. 認証機関の選択

（出典）JIPDEC「ISMS/ITSMS/BCMS/CSMS 認証を取得するには」をもとに作成

認定された認証機関は、業種による制限はありませんので、どの業種の組織でも審査することができます。しかし、審査において業種特有な専門的知識が必要な場合は、認証機関として審査を受付けない場合がありますので、事前に確認することが大切です。また、利害が絡む場合などでは審査を受付けられない場合があります。

認証機関を選択したら、認証審査・登録に関する条件について事前に確認し、合意されたら申請します。

認証登録に関わる料金は、適用範囲や受審組織の規模などの他、認証機関によっても異なります。見積りをとることもできます。

申請に必要な書類や様式などは、認証機関に確認します。

詳細理解のため参考となる文献（参考文献）	
ISMS 認証機関一覧	https://isms.jp/ist/isr/index.html

13-4-2. ISO/IEC27001 の審査事前準備

ISMS の構築

ISO/IEC 27001 に準拠した [ISMS](#) を実装するには、どのようなステップが必要なのか解説します。実装に際しては ISO/IEC 27001 の認証審査を受けることになります。そのため、審査対象となる ISMS の構築を実施し、実際の運用状況について記録することになります。

ISMS の構築	
ステップ	概要
適用範囲の決定	会社全体だけでなく、特定の部署・拠点のみといったように ISMS の範囲を限定すること も可能なため、まずは適用範囲を決定します。
情報セキュリティ方針の策定	ISMS の基本的な指針として、会社の情報セキュリティ方針を策定します。
体制の確立	ISMS 管理責任者、ISMS 推進事務局、ISMS 内部監査 チームなど、ISMS の運用体制を決定します。
ISMS 文書化	ISMS を運用・維持するための手順やガイドラインを文書化します。従業員や関係者が理解しやすく、利用・実践しやすい形式により作成することが重要です。

リスクアセスメントの実施	会社が持つ情報資産を洗い出し、それらに想定しうるリスクと対策を決定します。リスクアセスメントの結果は記録を作成します。
従業員の教育	ISMS の概要や手順、会社の情報セキュリティ方針について従業員に理解してもらうため、セキュリティ教育を実施します。教育の結果は記録を作成します。
内部監査	ISMS の運用がはじまった後に、定めたルールが適切に運用されているかを確認します。運用が不十分な場合はリスクの指摘やルールの見直しを行い、改善につなげます。内部監査の結果は記録を作成します。
マネジメントレビュー	内部監査の結果をもとに、会社の ISMS についての現状や課題、改善点などを経営陣に報告します。マネジメントレビューの結果は記録を作成します。

13-4-3. ISO/IEC27001 の審査（第一段・第二段）

ISMS 認証と ISMS 適合性評価制度

「ISMS 認証」とは、組織の構築した [ISMS](#) が ISO/IEC 27001 に基づいて適切に運用管理されているかを、第三者である ISMS 認証機関が、利害関係のない公平な立場から審査し証明することです。この認証を公正に運用するために、国際的な枠組みが定められており、これを「ISMS 適合性評価制度」と呼んでいます。この適合性評価制度は、以下の図に示したように「認証機関」「認定機関」「要員認証機関」から構成されています。

ISO/IEC 27001 は、ISMS 適合性評価制度において、第三者である認証機関が ISMS 認証を希望する組織の適合性を評価するための基準となります。認証審査においては、組織の ISMS が ISO/IEC27001 の標準に適合しているかが評価されることになります。

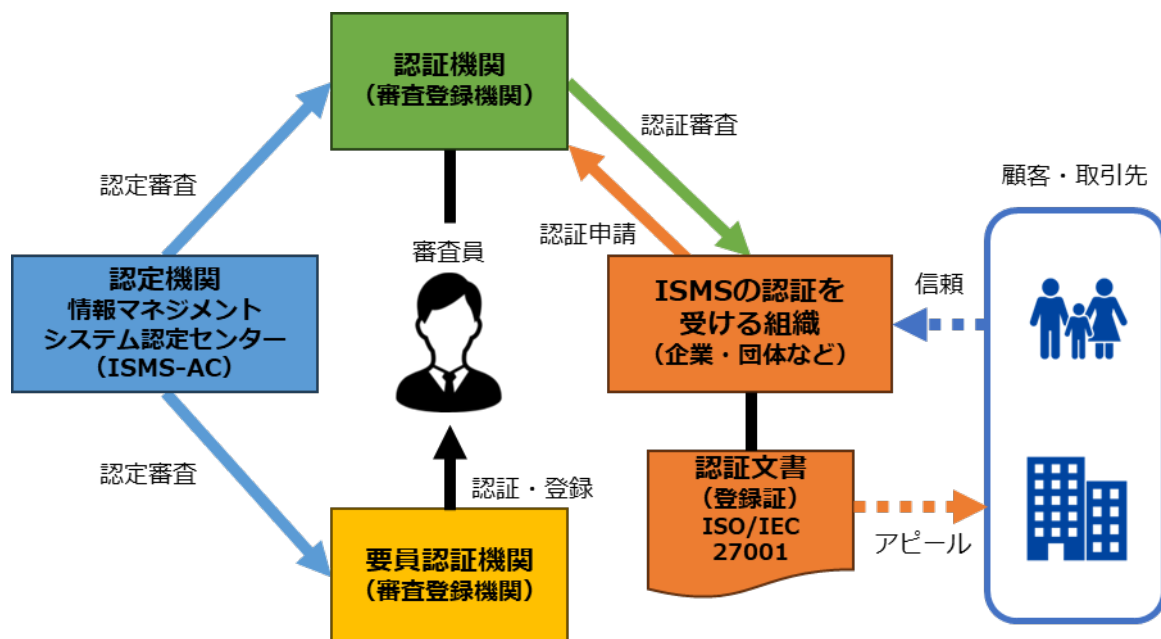


図 59. ISMS 適合性評価制度
 (出典) ISMS-AC「ISMS 適合性評価制度」を基に作成

認定と認証

認定	認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定といいます。日本における ISMS 適合性評価制度の認定機関は ISMS-AC です。ISMS-AC は、認証機関が適切に審査を実施できる体制・能力を持ち、かつ公正な審査を実施しているかを、国際規格に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けた ISMS 認証機関は、適切な ISMS 認証審査を実施することのできる、信頼のおける認証機関であることを意味します。
認証	第三者が文書で保証する手続きを認証といいます。 マネジメントシステム規格への適合性を保証する場合、認証の代わりに特に他と区別するため「審査登録」という用語を用いることがあります。この場合、認証の対象は、製品、サービスあるいはプロセスではなく、組織のマネジメントシステムそのものとなることに注意が必要です。

(出典) MSQA「ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版」を基に作成

ISMS 認証審査プロセス

ISMS の認証審査は、大まかに以下のようなステップで進みます。



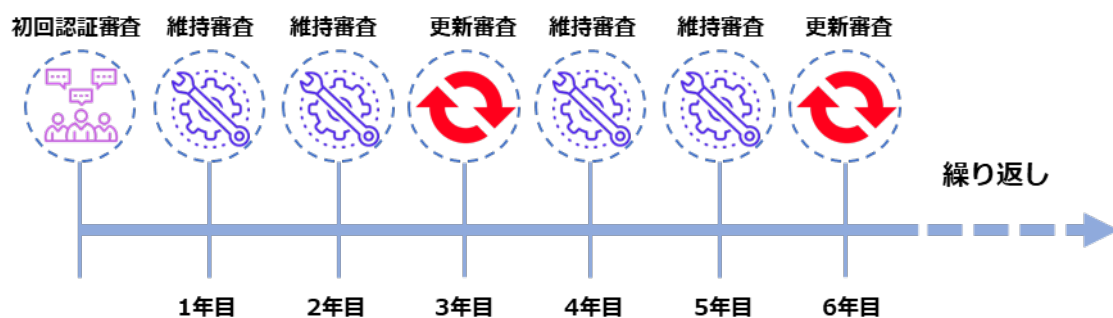
ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受審する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として1次審査と2次審査の2回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページ上で公開されます。

なお、審査に要する期間や工数、申請方法、申請時の準備物、認証登録料金などは、認証機関によって異なります。[ISMS](#) 認証機関は、情報マネジメントシステム認定センター（ISMS-AC）のホームページで公開されているため、申請先選定の際は確認することが大切です。

13-4-4. ISO/IEC27001 の維持審査・再認証審査

ISMS 認証の維持および更新審査プロセス

[ISMS](#) 認証取得後も、維持・更新のための審査があります。年に1回以上の維持審査（サーベイランス審査）と、3年ごとに認証の有効期限を更新するための全面的な審査（再認証審査）です。どちらにおいても、組織のISMSが引き続き規格に適合し、有効に維持されているかが確認されます。



ISMS の導入：成功の鍵とよくある落とし穴

組織が顧客データや機密情報などの[情報資産](#)を守るためには、適切に情報セキュリティを確保する仕組みが必要となります。そのために、ISMS の導入と運用は重要になります。そこで、ISMS を導入・運用していく際に成功の鍵となるポイントと、陥りやすい失敗例をいくつか紹介します。

成功の鍵となるポイント

- トップマネジメントのコミットメント
ISMS の導入には経営陣からのコミットメントが不可欠です。経営層が情報セキュリティの重要性を理解し、リーダーシップを発揮することにより、組織全体が情報セキュリティの確保に向けて協力的になります。
- 従業員の教育と意識向上
従業員への教育は、従業員に基本方針や対策基準などを理解させ、策定された実施手順を実践してもらうために重要です。定期的なトレーニングや教育プログラムを通じて、従業員が脅威に対処できるようにサポートしていくことが大切です。
- リスク評価と適切な対応策
[リスク評価](#)を行い、特定のリスクに対して適切な対応策を策定することにより、情報資産の保護と事業の継続性を確保できます。

陥りやすい失敗例

- 実施手順の抽象性
実施手順が抽象的で理解しづらい場合、従業員は具体的に何を順守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。わかりやすい実施手順を策定し、従業員に浸透させることが重要です。
- 不十分な監査と改善の実施
ISMS の運用において監査と改善を怠ってしまうと、新たな脅威に適応できず、セキュリティ体制が陳腐化してしまいます。定期的な監査と、その結果をもとにした改善活動を継続的に行うことが必要です。

ISMS の導入を成功させるためには、経営層のリーダーシップ、従業員の教育、リスクマネジメントの適切な実施が欠かせません。常に変化するセキュリティ環境に適応する柔軟性や継続的な改善が、組織の情報セキュリティを確保することにつながります。

第14章. ISMS の管理策

章の目的

第 14 章では、ISO/IEC 27002 における管理策の分類と構成について理解することを目的とします。

主な達成目標

- ISMS の管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

14-1. 管理策の分類と構成

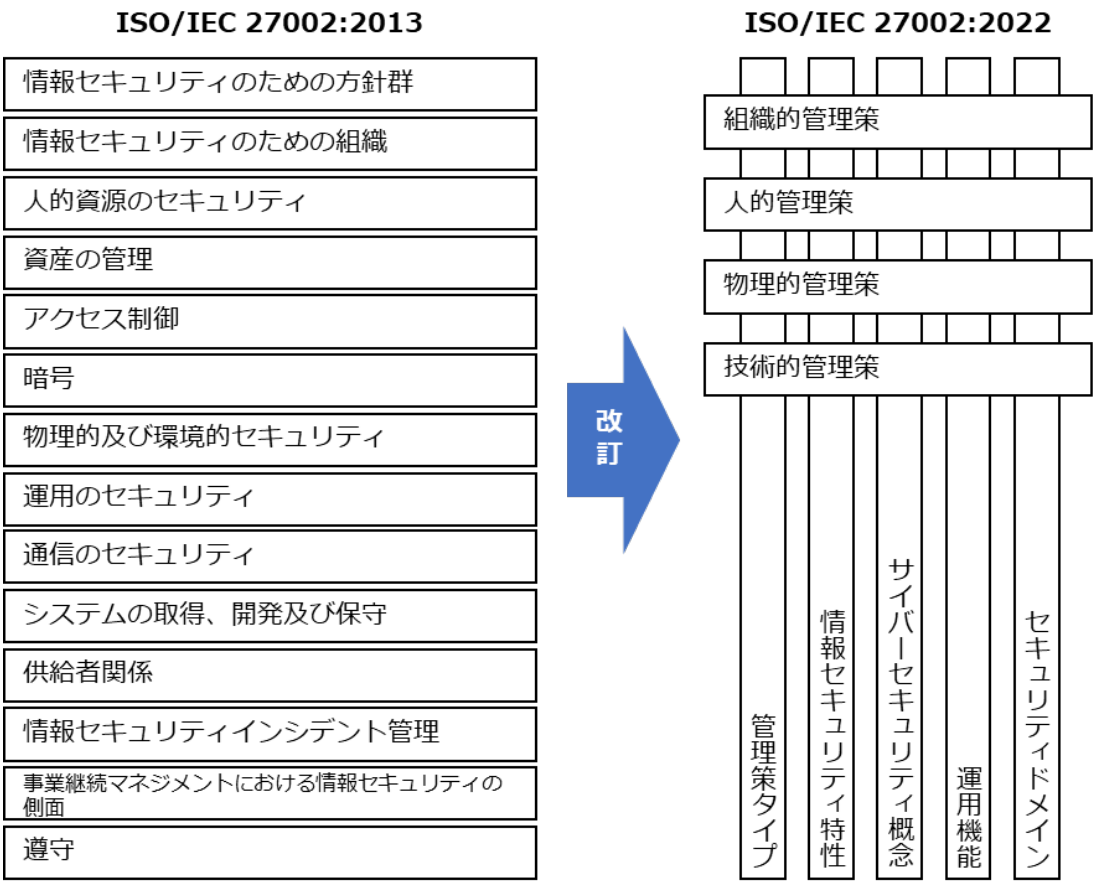
14-1-1. 管理策：ISO/IEC 27002

ISO/IEC 27001 に記載されている要求事項をもとに、さらに具体的な ISMS の管理策を示した規格が ISO/IEC 27002 です。管理策とは、リスク対応策のことを指します。企業は ISMS を導入する際、ISO/IEC 27002 にある管理策から、自社に合ったものを選択し、対策基準として導入することになります。

ISO/IEC 27002 は、2022 年に改訂がありました。その際の変更点としては、管理策の項目数と章立ての変更、テーマおよび属性の導入、全管理策に目的を追加などがあります。管理策の数は、2013 年版では 14 分野 114 項目でしたが、2022 年版ではいくつかが統合されて 82 項目になり、新しく 11 項目が追加され、合計で 93 項目となりました。

2022 年版では、この 93 の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4 カテゴリに分類されています（箇条 5～8）。

また、2022 年版では「属性 (attribute)」という新しい概念が導入されました。各管理策には、属性値がハッシュタグにより表示されるようになっています。例えば、管理策のタイプには、予防・検知・是正の 3 つの属性値があります。この他、情報セキュリティ特性、サイバーセキュリティ概念、運用機能、セキュリティドメインの観点からも属性値が付けられています。これらの属性を参考にして、組織に必要な情報セキュリティ対策を選択することになります。



14-1-2. 管理策のテーマと属性

ISO/IEC 27002 の箇条 5～8 に示される 4 種の管理策での分類（組織的・人的・物理的・技術的）を、テーマと呼びます。管理策の分類はさまざまな考え方がありますが、多くの組織に共通であると考えられる最低限の分類としてこの 4 つが採用されています。テーマとは別の視点で、より細かに管理策を見るのに際しては、属性という機能があります。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。



管理策の属性には、他の組織や団体が発行するガイドラインなどにおける考え方を取り入れているものがあります。「サイバーセキュリティ概念」では、[サイバーセキュリティフレームワーク](#)における、[フレームワークコア](#)の 5 つの機能分類がそのまま属性値となっています。また、「運用機能」の属性値は、2022 年の改訂前における ISO/IEC 27002 での管理策の分類がもとになっています。

管理策の属性	属性値	関連するガイドラインなど
管理策タイプ	予防、検知、是正	—
情報セキュリティ特性	機密性 、 完全性 、 可用性	ISO/IEC 27001:2022
サイバーセキュリティ概念	識別、防御、検知、対応、復旧	サイバーセキュリティフレームワーク
運用機能	ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリ	ISO/IEC 27002:2022

	リケーションのセキュリティ、セキュリティを保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、供給者関係のセキュリティ、法および順守、情報セキュリティ事象管理、情報セキュリティ保証	
セキュリティドメイン	ガバナンスおよびエコシステム、保護、防御、対応力	—

各テーマより管理策の例示（組織的/人的）

【組織的管理策】 5.2 情報セキュリティの役割及び責任

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #対応力

管理策	情報セキュリティの役割及び責任を、組織の要求に従って定め、割り当てることが望ましい。
目的	組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

【人的管理策】 6.8 情報セキュリティ事象の報告

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知	#機密性 #完全性 #可用性	#検知	#情報セキュリティ事象管理	#防御

管理策	組織は、要員が発見した又は疑いを持った情報セキュリティ事象を、適切な連絡経路を通して時機を失せずには報告するための仕組みを設けることが望ましい。

目的	要員が、特定可能な情報セキュリティ事象を、時機を失せず、一貫性をもって効果的に報告することを支援するため。

(出典) MSQA「ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド」を基に作成

各テーマより管理策の例示（物理的/技術的）

【物理的管理策】7.4 物理的セキュリティの監視

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防 #検知	#機密性 #完全性 #可用性	#防御 #検知	#物理的セキュリティ	#保護 #防御

管理策	施設は、認可されていない物理的アクセスについて継続的に監視することが望ましい。
目的	認可されていない物理的アクセスを検知し、抑止するため。

【技術的管理策】8.16 監視活動

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知 #是正	#機密性 #完全性 #可用性	#検知 #対応	#情報セキュリティ事象管理	#防御

管理策	情報セキュリティインシデントの可能性のある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい。
目的	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。

(出典) MSQA「ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド」を基に作成

14-1-3. 対策基準と実施手順の作成方法

管理策から自社に必要な対策を適用宣言書として選択して対策基準を作成し、実施手順を作成できるようにする手順を説明します。

- 管理策の決定：[リスクアセスメント](#)の結果を考慮して、適切なリスク対応を選定します。選定したリスク対応の選択肢に基づいて、実施に必要なすべての管理策を決定します。管理策は、ISO/IEC 27001 の附属書 A から選択できます。附属書 A に適切な管理策がない場合は、独自に追加の管理策を選択できます。
- 管理策の検証：決定した管理策を、ISO/IEC 27001 の附属書 A に規定された管理策と比較し、自社にとって必要な管理策が見落とされていないか検証します。
- 適用宣言書の作成：適用宣言書を作成します。適用宣言書とは、[ISMS](#) に関連してその組織が適用する管理策を記述した、文書化された情報のことです。適用宣言書に含める事項は以下の通りです。
 - 必要な管理策
 - それらの管理策を含めた理由
 - それらの管理策を実施しているか否か
 - 附属書 A に規定する管理策を除外した理由
- 実施手順の作成：管理策（対策基準）をもとに具体的な実施手順を作成します。実施手順は、組織の内部文書として作成します。従業員が具体的に何を順守して行動すればよいか理解できるよう、わかりやすく策定するように心掛けることが大切です。

第15章. 組織的対策

章の目的

第 15 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 組織的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

15-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に記載された合計 93 項目の管理策を参考に、対策基準を策定します。[リスクアセスメント](#)の内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】 採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
5.1 情報セキュリティのための方針群		5.20 供給者との合意におけるセキュリティの取扱い	
5.2 情報セキュリティの役割及び責任		5.21 ICT サプライチェーンにおける情報セキュリティの管理	
5.3 職務の分離		5.22 供給者のサービス提供の監視、レビュー及び変更管理	
5.4 経営陣の責任		5.23 クラウドサービス利用における情報セキュリティ	
5.5 関係当局との連絡		5.24 情報セキュリティインシデント管理の計画策定及び準備	
5.6 専門組織との連絡		5.25 情報セキュリティ事象の評価及び決定	
5.7 脅威インテリジェンス		5.26 情報セキュリティインシデントへの対応	
5.8 プロジェクトマネジメントにおける情報セキュリティ		5.27 情報セキュリティインシデントからの学習	
5.9 情報及びその他の関連資産の目録		5.28 証拠の収集	
5.10 情報及びその他の関連資産の利用の許容範囲		5.29 事業の中断・阻害時の情報セキュリティ	
5.11 資産の返却		5.30 事業継続のための ICT の備え	
5.12 情報の分類		5.31 法令、規制及び契約上の	

		要求事項	
5.13 情報のラベル付け		5.32 知的財産権	
5.14 情報転送		5.33 記録の保護	
5.15 アクセス制御		5.34 プライバシー及び PII の保護	
5.16 識別情報の管理		5.35 情報セキュリティの独立したレビュー	
5.17 認証情報		5.36 情報セキュリティのための方針群、規則及び標準の順守	
5.18 アクセス権		5.37 操作手順書	
5.19 供給者関係における情報セキュリティ			

対策基準の内容は、基本方針とともに公開可能なものとして作成します。[ISMS](#)に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）
5.1 情報セキュリティのための方針群 情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。 5.2 情報セキュリティの役割及び責任 情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。 5.3 職務の分離 相反する職務および責任範囲は、分離しなければならない。 5.4 経営陣の責任 経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従

った情報セキュリティの適用を、すべての要員に要求しなければならない。

5.5 関係当局との連絡

組織は、関係当局との連絡体制を確立および維持しなければならない。

5.6 専門組織との連絡

組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家からの協会・団体との連絡体制を確立し維持しなければならない。

5.7 脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集および分析し、[脅威インテリジェンス](#)を構築しなければならない。

5.8 プロジェクトマネジメントにおける情報セキュリティ

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

5.9 情報及びその他の関連資産の目録

管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。

5.10 情報及びその他の関連資産の利用の許容範囲

情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。

5.11 資産の返却

要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。

5.12 情報の分類

情報は、[機密性](#)、[完全性](#)、[可用性](#)および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。

5.13 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。

5.14 情報転送

情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。

5.15 アクセス制御

情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。

5.16 識別情報の管理

組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。

5.17 認証情報

認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

5.18 アクセス権

情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。

5.19 供給者関係における情報セキュリティ

供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。

5.20 供給者との合意における情報セキュリティの取扱い

供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。

5.21 ICT サプライチェーンにおける情報セキュリティの管理

ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。

5.22 供給者のサービス提供の監視、レビュー及び変更管理

サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。

5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。

5.24 情報セキュリティインシデント管理の計画及び準備

セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。

5.25 情報セキュリティ事象の評価及び決定

情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。

5.26 情報セキュリティインシデントへの対応

セキュリティインシデントに対し、文書化した手順に従って対応しなければならない。

5.27 情報セキュリティインシデントからの学習

セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。

5.28 証拠の収集

情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。

5.29 事業の中断・障害時の情報セキュリティ

事業の中断・障害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。

5.30 事業継続のための ICT の備え

事業継続の目的および ICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。

5.31 法令・規制及び契約上の要求事項

情報セキュリティに関する法令や契約事項を特定・文書化し、順守しなければならない。

5.32 知的財産権

知的財産権を保護するための適切な手順を実施しなければならない。

5.33 記録の保護

記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。

5.34 プライバシー及び PII の保護

適用される法令、規制および契約上の要求事項に従って、プライバシーの維持および PII の保護に関する要求事項を特定し、満たさなければならない。

5.35 情報セキュリティの独立したレビュー

情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。

5.36 情報セキュリティのための方針群、規則及び標準の順守

組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を順守していることを定期的にレビューしなければならない。

5.37 操作手順書

情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。



対策基準を策定する際のポイント

ISO/IEC 27001:2022 附属書 A の中には、中小企業にとっては負担が大きい管理策があります。ISO/IEC 27001:2022 附属書 A に適切な管理策がない場合は、独自の管理策を追加することができます。組織の状況を考慮し、適切な対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

15-2. 組織的対策として重要となる実施項目

管理策(対策基準)をもとに策定されたセキュリティ対策の実施手順例を、それぞれ紹介します。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を順守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対してわかりやすい実施手順を策定するよう心掛けることが大切です。

実施手順を策定する際は、ISO/IEC 27002 に記載されている各管理策の手引きが参考になります。手引きの内容をもとに、実施手順の例を紹介します。この例と、ISO/IEC 27002 の内容を参考に、自社に適した実施手順を策定してください。

15-2-1. 情報化・サイバーセキュリティ・個人情報保護

情報化・サイバーセキュリティ・個人情報保護に関連する実施手順の例を紹介します。

【5.1 情報セキュリティのための方針群】

実施手順（例）

情報セキュリティ委員会は、「情報セキュリティ方針」などの情報セキュリティに関する方針を定義し、トップマネジメント（経営層）の承認を得る。また、情報セキュリティ委員会は、情報セキュリティに関する方針を適用範囲内の全従業員に公表する。また、「情報セキュリティ方針」は外部関係者にも公表する。

情報セキュリティ委員会は、「情報セキュリティ方針」以外の情報セキュリティのための方針群を、本手順において定める。方針群には以下を含める。

- モバイル機器の方針
- テレワーキング
- [アクセス制御](#)方針
- 暗号による管理策の利用方針
- クリアデスク・クリアスクリーン
- 情報転送の方針（および手順）
- セキュリティに配慮した開発のための方針
- [供給者](#)関係のための情報セキュリティの方針

ワンポイントアドバイス

情報セキュリティに関する方針は、関連する従業員および利害関係者に認識されることが大切です。

【5.2 情報セキュリティの役割及び責任】

実施手順（例）

トップマネジメント（経営層）は、情報セキュリティに関連する役割を持つ情報セキュリティ委員会、内部監査責任者に対して、以下の責任および権限を割り当てる。また、トップマネジメント（経営層）は、これらの役割、責任および権限を従業者に伝達する。情報セキュリティの運用に際し、トップマネジメント（経営層）は、情報セキュリティ委員会の設置および運営を実施する。

情報セキュリティ委員会の役割は以下の通り。

- a. リスク対応計画の策定
- b. 情報セキュリティ実行体制の構築
- c. 選択された管理策の実施
- d. 教育・訓練
- e. 運用の管理
- f. 経営資源の管理
- g. 情報セキュリティ事象・セキュリティインシデントの管理
- h. 関連当局との連絡（警察・審査機関・コンサル会社・取引先・委託先など）

情報セキュリティ委員会の役割と、責任および権限は以下の通り。

● 情報セキュリティ委員会責任者

管理策の実施・運用について統括する。管理策の成果をトップマネジメント（経営層）に報告する。

● 教育責任者

管理策に関する教育計画の立案と実施を行う。

● 部門管理者（運用委員）

情報セキュリティの部門代表者として、部門を管理する。

● 情報システム管理者

情報システム部門の管理者で、情報システム管理に関する規定・規則に従い、情報セキュリティを維持するための安全管理対策を実施する。

● 文書管理責任者

管理策に関する文書や記録などの維持・管理を行う。

内部監査責任者の責任および権限は以下の通り。

内部監査責任者は、管理策とその実施状況に関わる監査を統括する責任と権限を有する。

ワンポイントアドバイス

従業員が少ない場合は、文書管理責任者と教育責任者を同じ者にするなど、役割を兼任させて体制を構築することも有効です。

【5.3 職務の分離】

実施手順（例）

- 当組織は、申請者または作業者と、承認者を分離するように組織設計する。
- 従業員の制約により兼任せざるを得ない場合、別部門などから監視を受けることを条件に、兼任できる。

ワンポイントアドバイス

小さな組織で、職務の分離が困難である場合には、他の管理策（例：活動の監視、監査証跡、管理層からの監督）を考慮することが大切です。

【5.4 経営陣の責任】

実施手順（例）

トップマネジメント（経営層）はすべての従業員に対し、情報セキュリティ方針、各実施手順、並びにその他情報セキュリティに関する要求事項の順守を求める。

ワンポイントアドバイス

情報セキュリティ方針、各実施手順、その他情報セキュリティに関する要求事項が、すべての従業員に認識されることが大切です。

【5.5 関係当局との連絡】

実施手順（例）

情報セキュリティ委員会は、関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

ワンポイントアドバイス

セキュリティインシデントを、時機を失せずに報告するために、関係当局の連絡方法を明確にすることが大切です。

連絡先一覧表（例）

関係当局	連絡手段	URL	主目的
【IPA】コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口	ウイルス発見・感染の届出 virus@ipa.go.jp	https://www.ipa.go.jp/security/todokede/crack-virus/about.html	ウイルス感染や、 不正アクセス による被害を報告するため。

	不正アクセスの届出 crack@pa.go.jp		
【IPA】情報セキュリティ安心相談窓口	TEL:03-5978-7509 (受付時間 10:00～12:00、13:30～17:00 土日祝日・年末年始は除く) anshin@ipa.go.jp	https://www.ipa.go.jp/security/anshin/about.html	ウイルス感染や不正アクセスに関する技術的な内容の相談に対して、アドバイスをもらうため。
【警視庁】サイバー犯罪相談窓口	TEL:03-5805-1731 受付時間：午前 8 時 30 分から午後 5 時 15 分まで（平日のみ）	https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html	サイバー犯罪被害について相談するため。
【 個人情報保護委員会 】個人情報・マイナンバーの漏えい報告	Web フォームで報告	https://www.ppc.go.jp/personalinfo/legal/leakAction/	個人情報、マイナンバーの漏えいに対処するため。
【 JPCERT/CC 】インシデント対応依頼	Web フォームまたは、以下のメールアドレスに報告 info@jpcert.or.jp	https://www.jpcert.or.jp/form/	セキュリティインシデント対応を支援してもらうため。

【5.6 専門組織との連絡】

実施手順（例）

情報セキュリティ委員会は、専門組織およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

ワンポイントアドバイス

[脆弱性](#)や攻撃など情報セキュリティに関する情報を適時入手するために、入手方法を明確にすることが大切です。

連絡先一覧表（例）

専門組織	情報の入手方法	URL	主目的
【IPA】重要なセキュリティ情報	Web ページを閲覧	https://www.ipa.go.jp/security/security-alert/2023/index.html	危険性が高いセキュリティ上の問題と対策に関する最新情報を収集

			するため。
【IPA】ランサムウェア対策特設ページ	Web ページを閲覧	https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html	ランサムウェア 対策に関する最新情報を収集するため。
【個人情報保護委員会】注意情報一覧	Web ページを閲覧	https://www.ppc.go.jp/news/careful_information/?category=39	セキュリティ・個人情報・マイナンバーに関する、注意事項を把握するため。
【JPCERT/CC】注意喚起	Web ページを閲覧	https://www.jpcert.or.jp/at/2023.html	脆弱性に関する最新情報を収集するため。

【5.8 プロジェクトマネジメントにおける情報セキュリティ】

実施手順（例）

- プロジェクト管理者は、プロジェクトにおける必要な管理策を特定する。
- プロジェクトにおける必要な管理策は、プロジェクト終了後も考慮する。
- プロジェクト管理者は、情報セキュリティ責任者を任命する。
- 情報システム管理者は、業務用情報システムの導入・改善にあたっては、必要に応じて情報セキュリティ上の要求事項を、要件定義書や提案依頼書などにより文書化する。
文書には下記から必要な事項を含める。
 - 情報システムの設置場所（環境・障害からの対策を含む）に関する事項
 - [無停電電源装置](#)などの[サポートユーティリティ](#)に関する事項
 - 保守契約に関する事項
 - システムの冗長化に関する事項
 - 通信、データの安全対策に関する事項
 - 受け入れテストに関する事項
 - アクセス権限に関する事項

ワンポイントアドバイス

プロジェクトが提供する製品またはサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の個別方針および規制から順守すべき要求事項を決定することが大切です。

【5.12 情報の分類】

実施手順（例）

情報は一般・社外秘・関係者外秘で分類する。

情報セキュリティ委員会は、情報の分類を最低年 1 回見直す。

ワンポイントアドバイス

分類は、情報の侵害が組織に与える影響のレベルによって決定できます。分類体系により定義されたレベルには、分類体系の適用において意味をなすような名称を付けることが大切です。

情報の分類（例）

分類	内容
一般	下記以外
社外秘	関係者外秘以外の機密事項であり、当組織の従業員に対してのみ開示が許されるもの。（取引先に開示する必要があるものは除く。）または情報セキュリティに関わる規定・手順書類。
関係者外秘	情報が外に漏れることによって、当組織が重大な損失もしくは不利益を受けるような恐れのある機密事項であり、職務上の限られた関係者のみに開示を許すもの。関係者が明示的に定められていない場合、関係者とは、情報を直接配布された者を指す。

【5.13 情報のラベル付け】

実施手順（例）

従業員は、取扱う情報が一般・社外秘・関係者外秘の区分のうち、どれに該当するか認識できる必要がある。

書類の分類を容易に認識できない場合は、以下のいずれかの方法により適切なラベル付けを行う。

- 分類をシールなどの色により識別する。
- ファイルなどに分類を記入（またはスタンプ）することで識別する。
- 分類ごとに収納場所を分ける。

ワンポイントアドバイス

ラベル付けは、「5.12 情報の分類」で確立した分類体系を反映していることが大切です。

【5.14 情報転送】

実施手順（例）

- a. 重要な情報を外部に送信する場合は、セキュアなファイル共有サービスを利用する。やむを得ずファイル共有サービスが利用できない場合は、受信者と合意した上で、メールに添付して送信する。
- b. 重要な情報を外部に FAX にて送信する場合は、入力した番号と、名刺や送り状を照合し、間違えないことを確認してからスタートボタンを押す。また頻繁に送信する送り先は短縮ダイヤルに登録する。
- c. 認可されていない者に聞かれる可能性がある場所で、重要な情報を口頭で伝えることは禁じる。
- d. 重要な情報を外部に郵送する場合は、配達記録郵便や宅配便など配達記録が残る手段をとる。
- e. 重要な情報を格納した媒体は、手渡しを原則とし、やむを得ず郵送する場合は、十分な梱包により媒体を保護する。
- f. 個人情報の授受記録
 - 紙や記憶媒体による個人情報の受け渡しに際しては、送付票や受領証などで受け渡しの完了を確認する。
 - 電子メールにより個人情報の受け渡しを行う際には、送信済みメールおよび、受領確認の返信メールのいずれかまたは両方を受け渡し記録とする。
- g. 電子メールの利用
 - 電子メールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定する。
 - 社外メーリングリストへの参加は、原則禁止とする。
 - 重要な情報（社外秘以上）はメール本文に記載して送信せず、a に従う。
- h. 情報転送に関する合意
 - 情報の転送先との間で、情報転送の手段について、あらかじめ合意を得る。
 - 重要な情報を外部にメール添付または FAX にて送信する場合は、必要に応じて送信予告、到着確認の電話を掛ける。
 - 宅配便業者を利用する場合は、会社が指定する業者を利用する。
- i. 電子的メッセージ通信
 - 当組織の Web サイトに入力する情報の通信は、[SSL/TLS](#) により行う。
 - 電子データによる個人情報をインターネット経由で送受信する際は、SSL/TLS などの暗号化対策やパスワード設定などの措置を講じる。

ワンポイントアドバイス

情報転送は、電子的な転送、物理的記憶媒体での送付および口頭での伝達によって行われる場合があります。情報転送の規則、手順を定めることが大切です。

【5.15 アクセス制御】

実施手順（例）

- a. 業務に必要な者のみが情報にアクセスできるようにし、アクセス権限および操作権限は、認められた場合以外は与えないようにする。
- b. 社内 LAN は、情報システム管理者の承認を得た従業員、装置に限り接続する。
- c. 社内の情報システムへの外部からのアクセスは、ファイアウォールなどによって通信を制限する。
- d. 外部から社内のサーバに接続する場合、VPN 接続を使用する。
- e. 無線 LAN は物理的・論理的な認証、通信の暗号化などを施した上で利用する。
- f. サーバ室へ入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。
- g. サーバ室は、常時施錠可能とし、入退資格のない者の立ち入りを禁じる。

ワンポイントアドバイス

アクセス制御規則を定めるには、「明確に許可していないことは、原則的に禁止する」という最も特権の小さい前提に基づいた規則を設定するようにすることが大切です。

【5.16 識別情報の管理】

実施手順（例）

- a. 情報システムの利用者登録および登録削除は、当該利用者の属する部門長が申請し、情報システム管理者の承認を得る。
- b. 利用者登録は業務上必要な範囲で従業者に付与する。

ワンポイントアドバイス

識別情報が不要になった場合、識別情報は時機を失せずは無効化または削除することが大切です。

【5.17 認証情報】

実施手順（例）

- a. 情報システム管理者は、利用者に仮パスワードを発行する場合、利用者本人のみが知ることができる方法で通知する必要がある。
- b. 情報システム管理者は、利用者に対し、仮パスワードを直ちに変更することを要求し、通知する。
- c. 秘密認証情報の利用
 - 利用者は、英数字と記号を混在した 10 文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。利用者は、英数字と記号を混在した 10 文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。

- 他人に容易に推測されるようなわかりやすいパスワードの使用を禁じる。
 - 他のサービスと重複するパスワードの利用を禁じる。
 - 各システムにおける管理者 ID のパスワードは、情報システム管理者において厳重に管理する必要がある。
 - 利用者および情報システム管理者は、パスワードの代替もしくは補完のために、指紋などの生体認証、IC カード認証などの機器による認証方式も採用できるものとする。
- d. パスワード管理システム
- パスワードの入力是对話式とする。
 - パスワードをシステムに記憶させることは禁じる。

ワンポイントアドバイス

パスワードを認証情報として使用する場合、IPA などが推奨している強力なパスワードの作り方を参考にすることが大切です。

【5.18 アクセス権】

実施手順（例）

- 利用者のアクセス権は、重要情報に対しては必要最小限の者がアクセスするという原則のもとに、情報システム管理者が検討し、設定を行う。
- 情報システム管理者は、定期的（最低年 1 回）および必要時にアクセス権限の棚卸および見直しを行う。
- 退職者が発生した際は、業務に支障がないよう調整し、速やかに該当アカウントを削除する必要がある。申請は、当該従業員が最後に所属した部門の長がアクセス権限の削除を申請し、情報システム管理者、またはその指名する従業員が削除する。
- 他部署への移動が生じた際は、a の手順に従い削除する。また、新規のアクセス権限は移動先部門の長が申請し、同様の手順に従い登録する。

ワンポイントアドバイス

物理的および論理的なアクセス権の定期的レビューでは、同じ組織内での異動、昇進、降格、退職後の利用者のアクセス権、および特権的アクセス権の認可について考慮することが大切です。

15-2-2. 脅威インテリジェンス

脅威インテリジェンスに関連する実施手順の例を紹介します。

【5.7 脅威インテリジェンス】

実施手順（例）

既存または新たな脅威に関する情報を、次に示す専門機関から収集する。

- IPA
- [JVN \(Japan Vulnerability Notes\)](#)
- [JPCERT/CC](#)
- [ISAC \(Information Sharing and Analysis Center\)](#)
- [個人情報保護委員会](#)

収集する情報は、以下のようなものとする。

- 変化する脅威の状況に関する情報（例：攻撃者や攻撃の種類）
- 攻撃の方法、使用されるツールや技術に関する情報
- 特定の攻撃に関する詳細な情報

収集した情報を分析する。

脅威が、自組織にどのような影響を及ぼすか把握するために、収集した情報をもとにリスクアセスメントを実施する。

リスク低減の処置を実施する。

[リスクアセスメント](#)の結果をもとに、[ファイアウォール](#)・侵入検知システム・[マルウェア](#)対策ソリューションなど、技術的に予防、検知を行うための管理策を採用する。

ワンポイントアドバイス

情報の収集から、リスク低減処置を実施するまでの手順を明確にすることが大切です。

15-2-3. 情報資産台帳作成・維持実施

情報資産台帳作成・維持実施に関連する実施手順の例を紹介します。

【5.9 情報及びその他の関連資産の目録】

実施手順（例）

情報セキュリティ委員会は「資産目録」を作成し、当組織における重要な資産を識別する。また「資産目録」を「年間計画表」に従い、最低年1回見直す。

情報セキュリティ委員会は「資産目録」において特定した資産に対し、同目録上に管理責任者（リスク所有者）を記載することにより管理責任を明確にする。

ワンポイントアドバイス

資産の管理責任を個人またはグループに割り当て、管理責任を明確にすることが大切です。

【5.10 情報及びその他の関連資産の利用の許容範囲】

実施手順（例）

情報の区分ごとの取扱いルールを以下に示す。

情報の区分は「5.12 情報の分類」で、ラベル表示については「5.13 情報のラベル付け」で定める。

文書・メディアなどの場合

管理区分	関係者外秘	社外秘	一般
ラベル表示	責任者に一任	責任者に一任	不要
利用者	関係する部署・プロジェクトに所属する従業員	当組織の従業員	誰でも可
再配布	関係する部署・プロジェクト内に限る	社内に限る	特別な配慮不要
保管場所	施錠された場所	責任者に一任	
コピーの使用	必要のある者に限定	社内に限る	
FAX 送信	関係する部署・プロジェクト内に限る	社内に限る	
裏紙使用※1	禁止	禁止	
社外便	透かして内容が見えないようにする。※2		
社外での携行	責任者の許可を得た者のみ携行を許可する。※3		
廃棄（文書）※4	シュレッダー・焼却・溶解のいずれか	責任者に一任	
廃棄処（媒体）	廃棄、再利用前の内容を消去する。		

※1 個人情報の記された書類の再利用は禁じる。

※2 紙や記憶媒体による個人情報を、郵便や宅配便などにより移送するときは、誤配、紛失などの危険を最小限にするため、ポストへの施錠、受け取り確認が可能な移送手段の選択などの措置を講じる。

※3 個人情報を外部へ持ち出す際は、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。

※4 紙に記された個人情報の廃棄は、シュレッダーによる裁断・焼却・溶解いずれかの方法により処分する。また、廃棄前の一時保管場所からの紛失・盗難防止のため、重要書類は即廃棄する。

管理区分	関係者外秘	社外秘	一般
アクセス制御	個人またはグループでのアクセス制御	責任者に一任	特別な配慮不要
個人 PC への保管	責任者に一任	責任者に一任	

内 情 報	サーバへの保管	アクセス制限	責任者に一任	
	コピー（複製）※ 1	コピーの管理	責任者に一任	
	メール	添付ファイルにパスワード		
	※1 コピーは、バックアップの必要上および業務上やむを得ない場合の必要最小限の範囲にとどめるものとする。 ※2 取引先との合意がある場合は、その合意に従う。			
ワンポイントアドバイス 許容できる行動、許容できない行動を明確に定めることが大切です。				

【5.11 資産の返却】

実施手順（例）				
情報セキュリティ委員会は、退職者が発生した際に、以下の対応を部門長に要求し、実施されたことを確認する。 名刺、社員証、ID カードなどの返却 会社が支給したノート PC や携帯電話などの返却 紙で保管する書類の返却、または廃棄				
ワンポイントアドバイス 返却するすべての情報およびその他の関連資産を明確に特定し、文書化することが大切です。				

15-2-4. クラウドサービス利用

クラウドサービス利用に関連する実施手順の例を紹介します。

【5.23 クラウドサービスの利用における情報セキュリティ】

実施手順（例）		
クラウドサービスを導入する際、以下の評価表をもとにクラウドサービスを評価し、自社のセキュリティ要件事項を満たしているか確認する。		
評価表		
クラウドサービス提供者名		サービス内容
取得している認証		
☐ ISO/IEC 27001 ☐ ISO/IEC 27017		
セキュリティ対策内容		評価

クラウドサービスに対して、 マルウェア 対策を行っているか。	
クラウドサービスのバックアップを行っているか。	
サービス解約時のデータの取扱い方法が明確になっているか。	
サービス稼働率、障害発生頻度、障害発生時の復旧時間など、サービス品質は問題ないか。	
データがどの国や地域に配置されたサーバに保存されているか確認したか。	
サービスの利用方法について問い合わせることができるか。	
クラウドサービス提供者の責任範囲を確認したか。	
クラウドサービスの セキュリティインシデント 発生時に通知がくるかどうか確認したか。	
ワンポイントアドバイス クラウドサービスの利用は、クラウドサービス提供者とクラウドサービス利用組織との間の情報セキュリティに関する責任の共有および分担、共同作業を伴う可能性があります。クラウドサービス提供者と、クラウドサービス利用組織の両方の責任を適切に定義し、実践することが大切です。	

15-2-5. 情報セキュリティインシデント対応

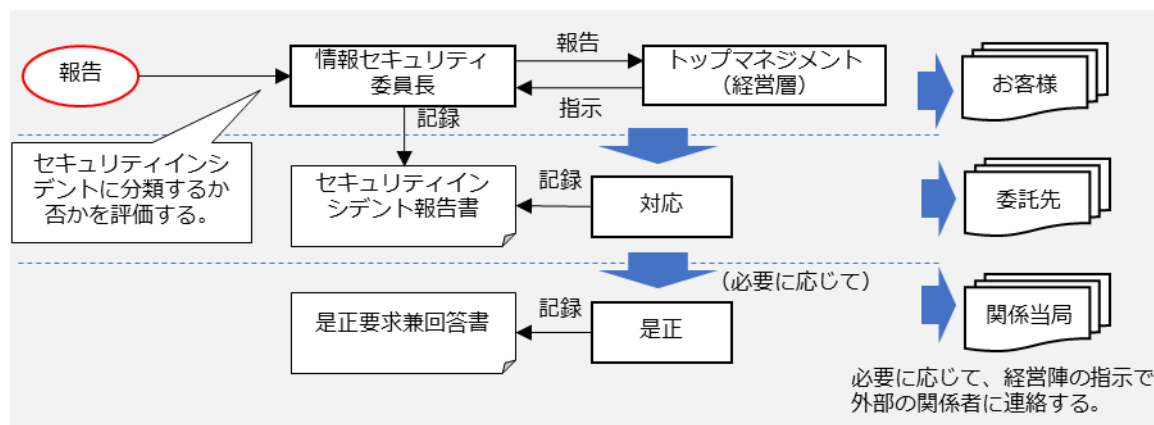
情報**セキュリティインシデント**対応に関連する実施手順の例を紹介します。

【5.24 情報セキュリティインシデント管理の計画策定及び準備】

実施手順（例）

セキュリティインシデントへの対応は、以下の手順で行う。

管理層の責任のもと、以下の手順を関係者に伝達する。



ワンポイントアドバイス

セキュリティインシデントへの対応を実行するために役割および責任を決定し、関連する関係者に効果的に伝達することが大切です。

【5.25 情報セキュリティ事象の評価及び決定】

実施手順（例）

セキュリティの弱点、脅威に気付いた場合もしくは疑いを持った場合は、情報セキュリティ委員会に報告する。この際、自己で解決することよりも報告を優先させる。

情報セキュリティ事象の評価は、以下の表に従い、部門管理者（情報セキュリティ委員会メンバー）が行う。

- ・大、中の項目に該当する情報セキュリティ事象は、セキュリティインシデントとして分類する。
- ・項目の大、中、小の順に優先順位を付ける。

ワンポイントアドバイス

情報セキュリティ事象をセキュリティインシデントに分類する基準を明確に定めることが大切です。

優先順位

項目	小	中	大
分類	ヒヤリハット・事象	インシデント	インシデント
最終的に被害が及ぶ範囲	現状、事件・事故の発生には及ばない。 （将来、被害が発生する可能性がある。）	社員または社内	顧客・取引先
連絡先	情報セキュリティ委員長	情報セキュリティ委員長	情報セキュリティ委員長 トップマネジメント（経営層） 外部関係者

【5.26 情報セキュリティインシデントへの対応】

実施手順（例）

セキュリティインシデントへの対応手順は以下の表に従う。

セキュリティ	影響度	小	中・大
	ウイルス感染時	● 感染した PC を、組織内のネットワークから切り離す。 ● 発生する可能性がある被害をシステム担当者に報告する。	● 感染した PC を、組織内のネットワークから切り離す。 ● 発見した事実をできるだけ速やかに情報システム管理者に連絡する。

インシデントへの対応手順	不正アクセス発生時	● ネットワークを遮断する。 ● 重要なデータを隔離する。 ● ログインできる場合は、早急にパスワードを変更する。 ● 発生する可能性がある被害をシステム担当者に報告する。	● ネットワークを遮断する。 ● 重要なデータを隔離する。 ● ログインできる場合は、早急にパスワードを変更する。 ● システムやアプリケーションを停止する。 ● 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
	情報破壊発生時	● 発見次第、発生する可能性がある被害を部門長に報告する。	● 発見した事実をできるだけ速やかに部門長に連絡する。
	情報改ざん発生時	同上	同上
	情報漏えい発生時	同上	同上
	サービス停止時・機器故障など	同上	同上

ワンポイントアドバイス

セキュリティインシデント対応に関する手順を確立し、すべての関連する利害関係者に伝達することが大切です。

【5.27 情報セキュリティインシデントからの学習】

実施手順（例）

- 情報セキュリティ委員会は、セキュリティインシデントを管理・分析し、問題があれば、計画を立ててトップマネジメント（経営層）へ提議する。計画には、解決に向けての処置方法・費用・実施予定日・責任者を明確にする。
- 将来のセキュリティインシデントの起こりやすさや影響を減らすため、情報セキュリティ委員会は、セキュリティインシデントから得られた知識を活かして「6.3 情報セキュリティの意識向上、教育及び訓練」を強化・改善する。

ワンポイントアドバイス

セキュリティインシデントの形態、規模および費用を定量化および監視するための手順を確立することが大切です。

【5.28 証拠の収集】

実施手順（例）

情報セキュリティ委員会は、情報システムの事故が特定の個人、または組織に起因するもので、事後処置が法的処置に及ぶ可能性のある場合には、必要な証拠の収集、保全に努める。

ワンポイントアドバイス

懲戒処置および法的処置のために情報セキュリティ事象に関連する証拠を取扱う場合は、内部の手順を定めて従うことが大切です。

15-2-6. 事業継続計画策定

事業継続計画策定に関連する実施手順の例を紹介します。

【5.29 事業の中断・阻害時の情報セキュリティ】

実施手順（例）

- a. 資産のリスク分析
- b. 「資産目録（情報資産管理台帳）」で特定した情報資産のうち、可用性の評価値が3の重要資産を情報セキュリティ継続のリスク分析対象とする。
※ 可用性の評価値は、「12-2-2. リスク特定」で記載している方法により算出する。
- c. aにおいて登録した資産に対して、以下のリスクについて考慮する。
 - 地震・火災・洪水などの自然災害
 - 人的なミス
 - システム障害
 - 健康上の問題
- d. bのリスクが生じた際に影響を受ける業務プロセスを特定し、リスクが発生した場合のシナリオを作成する。
- e. リスクが生じた場合の影響度と、リスクが発生する可能性について検討し、検討結果に基づき優先順位を決定する。
- f. dにおいて、優先順位が高いと判断したものに対して「事業継続計画書」を作成し、トップマネジメント（経営層）の承認を得る。
- g. 「事業継続計画書」には以下の内容を含む。
 - 実行開始条件（リスクシナリオの発生）
 - 非常時手順（発生時の連絡手順）
 - 回復手順（復旧のための手順）
 - 回復目標（目標時間を必要に応じて決定）
 - 再開手順（回復後のリハーサル手順）
 - 試験のスケジュール

- 教育（教育が必要な場合はその計画）
- h. 策定した計画および手続きについて試験を実施し、試験の結果、必要があると判断した場合は計画を更新する。試験は以下のいずれかの方法、またはその組み合わせにより行う。
 - 机上試験
 - 模擬試験
 - 技術的回復試験
 - 代替施設における回復試験
 - [供給者施設](#)およびサービスの試験
- i. 情報セキュリティ委員会は、事業継続に関する試験を最低年 1 回、継続的に実施する。

ワンポイントアドバイス

事業の中断または阻害時に、重要な事業プロセスの情報セキュリティを維持または復旧するために、計画を策定、実施、試験、レビューおよび評価することが大切です。

【5.30 事業継続のための ICT の備え】

実施手順（例）

- a. [ビジネスインパクト分析](#)（不測のインシデントによって業務やシステムが停止した場合、会社の事業にどのような影響があるかを分析すること）を行い、事業継続が困難な状況を特定する。
- b. 事業が中断・停止になった際の対応手順を策定し、文書化する。
- c. 策定した対応手順が有効であることを確実にするため、あらかじめ定めた間隔（年 1 回以上）で試験を実施し検証する。

ワンポイントアドバイス

組織が [ICT](#) サービス事業の中断・阻害を管理する方法を詳述した対応および復旧手順を含む ICT 継続計画を、演習および試験を通じて定期的に評価、または経営陣が承認することが大切です。

15-2-7. 法的、規制および契約上の要件

法的、規制および契約上の要件に関連する実施手順の例を紹介します。

【5.19 供給者関係における情報セキュリティ】

実施手順（例）

- a. 当組織における供給者には、以下がある。
- [ISP](#)、電話サービス、IT 機器などのサービス提供者
 - 情報システムの開発・保守における外部委託先
 - 会計、税務、法律などの専門サービス提供者
 - 清掃業者、廃棄業者
 - クラウドサービス
- b. 情報セキュリティ委員会は、部外者・外部組織からのオフィスエリアや情報システムへのアクセスを許可する際に生じる可能性があるリスクを考慮し、情報セキュリティ上の要求事項を明確にする。

ワンポイントアドバイス

[供給者](#)が提供する製品およびサービスの使用に関連するセキュリティリスクに対処するためのプロセスおよび手順を特定し、実施することが大切です。

【5.20 供給者との合意における情報セキュリティの取扱い】

実施手順（例）

- a. 提供されるサービスの利用は、次の手順に従い行う。
1. 「委託先審査票」による評価・選定を行う。
 2. 情報セキュリティ要求事項を考慮し、次の事項を含む契約を締結する。
- 機密保持契約などの情報の取扱いに関する契約
 - 使用許諾に関する取り決め、コードの所有権および知的所有権（開発の場合）
 - 実施される作業場所および入退室管理
 - 外部委託先が不履行となった場合の預託契約に関する取り決め
3. 情報セキュリティ委員会は、「5.19 供給者関係における情報セキュリティ」において検討したリスクを考慮し、必要に応じて第三者との間で契約を締結する。
- b. クラウドサービスを介して重要資産を取扱う際は、利用者は[多要素認証](#)を有効にしてセキュリティを強化する必要がある。

ワンポイントアドバイス

組織と供給者の間で情報セキュリティ要求事項を満たす義務に関し、当事者間で合意を確立し、文書化することが大切です。

【5.21 ICT サプライチェーンにおける情報セキュリティの管理】

実施手順（例）

- a. [ICT](#) 製品・サービスの供給者との契約には、必要に応じて再委託に関する事項を盛り込む。

- b. クラウドサービスの利用にあたっては、クラウドサービス提供者の事業継続性、および以下のサービスに関する情報セキュリティ事項を考慮の上、クラウドサービスを選定する。
- サービスの導入実績、信頼性
 - 利用者サポート機能
 - 利用終了後のデータの扱い
 - サービスの可用性
- c. 暗号化など、通信経路の安全対策

ワンポイントアドバイス

信頼できる供給源から ICT を取得する手順を明確にすることが大切です。

【5.31 法令・規制及び契約上の要求事項】

実施手順（例）

- 情報セキュリティ委員会は、当組織が順守すべき法令、規制、および契約上の要求事項を識別し、「情報セキュリティに関する法令規制一覧表」に記載する。「情報セキュリティに関する法令規制一覧表」は最低年 1 回見直す。
- 情報セキュリティ委員会は、当組織の従業者が「情報セキュリティに関する法令規制一覧表」を、必要に応じていつでも参照できる状態にする。
- 特定した要求事項を満たすために、必要に応じて教育などのテーマとする。
- 暗号化した装置を輸出する場合、または海外に持ち出す場合、該当する法規制について調査を行い、必要であれば対応を行う。

ワンポイントアドバイス

総務省の Web サイト「国民のためのサイバーセキュリティサイト サイバーセキュリティ関連の法律・ガイドライン」で、サイバーセキュリティに関する代表的な法律が紹介されています。

情報セキュリティに関連する法律（例）	概要
特定電子メールの送信の適正化等に関する法律	利用者の同意を得ずに広告、宣伝または勧誘などを目的とした電子メールの送信を禁止している。
電子署名及び認証業務に関する法律	「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定められている。
著作権法	プログラムやマニュアル、ホームページなどは、著

	著作権の対象であり、無断での複製は、著作権法の侵害になる。
不正アクセス禁止法	<u>不正アクセス</u> 行為や、不正アクセス行為につながる識別符号（ID、パスワード）の不正取得・保管行為、不正アクセス行為を助長する行為などを禁止している。
刑法	無断でデータを <u>改ざん</u> ・破壊する行為や、虚偽の金融機関を名乗ったサイトや電子メールを使い、金銭をだまし取るような行為などは、刑法に違反する。

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ関連の法律・ガイドライン	https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal

15-2-8. 知的財産、データ、プライバシー

知的財産、データ、プライバシーに関連する実施手順の例を紹介します。

【5.32 知的財産権】

実施手順（例）

- 知的財産権を保護するためのルールを策定し、組織内で教育・啓発活動を行う。
- 知的財産権を侵害する行為を禁止する。
- 知的財産権を侵害する行為が発生した場合には、速やかに是正措置を講じる。
- ソフトウェアなどの使用許諾計画を順守する。
- 情報システム管理者は、パッケージソフトウェアのライセンス管理を適切に行う。

ワンポイントアドバイス

知的財産権には、ソフトウェアまたは文書の著作権、意匠権、商標権、特許権およびソースコード使用許諾権が含まれます。

【5.33 記録の保護】

実施手順（例）

当組織における記録は、関連する法令に基づき次表の保存期間にわたり、消失、破壊、改ざん、不正なアクセス、流失などがないように適切に保存する。

ワンポイントアドバイス

記録は、記録の種類（会計記録、商取引記録、人事記録、法的記録など）によって分類し、それぞれに保存期間の詳細と、物理的または電子的な保存が可能な保存媒体の種類を記載することが大切です。

記録の種類と保存期間

記録の種類	保存期間
■ 定款 ■ 登記関係書類 ■ 訴訟関係書類 ■ 特許など知的所有権に関する書類 ■ 社則・社規	永久
■ 「商業帳簿」 会計帳簿（日記帳、仕訳帳、総勘定元帳）、貸借対照表、損益計算書、附属明細書 ■ 「営業に関する重要な書類」 株主名簿、社債原簿、株主総会議事録、取締役会議事録、営業報告書、利益処分案（損失処理案）、このほか紛争が生じた場合に重要な証拠となり得る書類（例：契約書）	10 年
■ 仕訳帳、総勘定元帳、現金出納帳、固定資産台帳、売掛帳、買掛帳、経費帳 ■ 棚卸表、貸借対照表、損益計算書、決算に関して作成された書類 ■ 注文書、契約書、送り状、領収書、見積書、その他これらに準ずる書類（例：請求書）	7 年
■ 給与所得者の扶養控除など（異動）申告書 ■ 給与所得者の保険料控除申告書兼給与所得者の配偶者特別控除申告書 ■ 源泉徴収簿	
■ 財産形成非課税貯蓄申込書・移動申請書	
■ 雇用保険被保険者に関する書類	5 年
■ 労働者名簿 ■ 賃金台帳 ■ 雇入・解雇・災害補償・賃金その他労働関係に関する重要な書類	4 年
■ 労働保険料の徴収に関する書類	3 年
■ 労災保険に関する書類	
■ 安全委員会議事録 ■ 衛生委員会議事録 ■ 安全衛生委員会議事録	
■ 健康保険に関する書類	
■ 厚生年金保険に関する書類	
■ 雇用保険に関する書類	2 年

【5.34 プライバシー及び PII の保護】

実施手順（例）

個人情報とは、「5.10 情報およびその他の関連資産の利用の許容範囲」の取扱いルールに従い、厳重に取扱う。

ワンポイントアドバイス

プライバシーの保持および PII 保護のための手順を策定および実施することが大切です。

15-2-9. セキュリティ対策状況の点検・監査・評価・認証

セキュリティ対策状況の点検・監査・評価・認証に関連する実施手順の例を紹介します。

【5.22 供給者のサービス提供の監視、レビュー及び変更管理】

実施手順（例）

- a. 情報セキュリティ委員会は、サービスの供給者に対して、あらかじめ定められた頻度（最低年 1 回）において契約の履行状況ならびに「委託先審査票」による順守状況の確認を行う。
- b. サービスの供給者との間で契約内容やサービスレベルに変更があった場合、変更点を受け入れることができるか否かを検証し、契約内容の見直しを実施する。

ワンポイントアドバイス

サービスの提供において不完全な点があった場合は、適切な処置をとることが大切です。

【5.35 情報セキュリティの独立したレビュー】

実施手順（例）

- a. 年に 1 度、内部監査により独立したレビューを行う。
- b. 以下に例示する、情報セキュリティに影響のある変化が生じた場合も、内部監査により独立したレビューを行う。
 - 事業の追加/変更、業務手順の大幅な変更
 - 住所変更、拠点の新設
 - 情報セキュリティに関する主たる担当者の変更
 - 関係する法令・規制、または契約の大幅な変更

ワンポイントアドバイス

独立したレビューにおいて、情報セキュリティに関して取組が不十分であると明確になった場合には、経営陣は是正処理を発議することが大切です。

【5.36 情報セキュリティのための方針群、規則及び標準の順守】

実施手順（例）

- a. 情報セキュリティ委員会は、セキュリティに関する手順や実施標準が正しく実施されていることを確実にするため、「運用チェックリスト」にて、定期的（3 ヶ月ごと）に点検を行う。
- b. 情報セキュリティ委員会（入退管理責任者）は、入退記録が適切にとられているか否かを月に 1 度確認する。また、入退管理が有効かつ適切に実施されていることを定期的を確認し、不備が発見された場合は速やかに是正の処置をとる必要がある。
- c. 情報システム管理者は、技術的な順守事項が正しく実施されていることを確実にするため、上記の a、b に従い点検する。

ワンポイントアドバイス

是正処置が完了しない場合は、確認時に進捗状況を報告することが大切です。

【5.37 操作手順書】

実施手順（例）

情報処理設備の正確、かつ、セキュリティを保った運用を確実にするために、次の事項を明記した手順書を文書化し、必要に応じて利用者が参照できるようにする。

システムが故障した場合の再起動および回復の手順

- a. 記憶媒体の取扱い手順
- b. バックアップの取得手順
- c. 保守手順
- d. 容量、能力、パフォーマンスおよびセキュリティなどの監視手順

ワンポイントアドバイス

操作手順書は必要に応じてレビューし、更新することが大切です。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

第16章. 人的対策

章の目的

第 16 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 人的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

16-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。[リスクアセスメント](#)の内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】 採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
6.1 選考		6.5 雇用の終了又は変更後の責任	
6.2 雇用条件		6.6 秘密保持契約又は守秘義務契約	
6.3 情報セキュリティの意識向上、教育及び訓練		6.7 リモートワーク	
6.4 懲戒手続		6.8 情報セキュリティ事象 の報告	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。[ISMS](#)に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

6.1 選考

従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。

6.2 雇用条件

雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。

6.3 情報セキュリティの意識向上、教育及び訓練

従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。

6.4 懲戒手続

情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。

6.5 雇用の終了又は変更後の責任

雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。

6.6 秘密保持契約又は守秘義務契約

組織の要求事項を反映した秘密保持契約または守秘義務契約を従業員や外部の関係者と締結しなければならない。

6.7 リモートワーク

要員が遠隔で作業する場合は、セキュリティ対策を実施しなければならない。

6.8 情報セキュリティ事象の報告

情報セキュリティ事象を、適切な連絡経路を通して時機を失せず報告できる仕組みを設けなければならない。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

16-2. 人的対策として重要となる実施項目

管理策(対策基準)をもとに策定されたセキュリティ対策の実施手順例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引きを参考に、自社に適した実施手順を策定してください。

16-2-1. スクリーニング

【6.1 選考】

実施手順（例）

従業員の募集・採用プロセスは以下の点を考慮のうえ行う。

- a. 取得した履歴書、スキルシートなどから業務上の要求事項に対する適合を判断し、選考を行う。
- b. 採用時の面接などにおける態度や言葉遣いなどから倫理観を判断し、選考を行う。
- c. 役員や管理職の採用に関しては、過去の信用情報など、より詳細な調査を行う場合があるが、この際は本人の同意を得たうえで行う。

ワンポイントアドバイス

選考プロセスはフルタイム、パートタイム、臨時スタッフを含むすべての従業員に対して実行することが大切です。

16-2-2. 雇用契約書

【6.2 雇用条件】

実施手順（例）

情報セキュリティに関する責任を理解し、情報セキュリティ方針を守ることが従業員に誓約させるため、雇用契約書に、情報セキュリティに関する事項を盛り込み、誓約書に署名を求める。

ワンポイントアドバイス

従業員に、情報セキュリティに関する雇用条件を同意させることが大切です。

16-2-3. 懲戒手続き

【6.4 懲戒手続】

実施手順（例）

従業員が故意または過失により情報を漏えいした場合、または情報セキュリティ上の遵守事項に違反した場合は、罰則の対象とする。

ワンポイントアドバイス

懲戒手続は、関連する法令、規制、契約および事業上の要求事項を考慮に入れることが大切です。

16-2-4. 雇用の終了または変更後の責任

【6.5 雇用の終了又は変更後の責任】

実施手順（例）

情報セキュリティの観点から、雇用の終了または変更後も従業員が守るべき義務や責任（例えば守秘義務）について定め、雇用時の誓約書に盛り込むと同時に、雇用の終了または変更時に再確認する。

ワンポイントアドバイス

雇用の終了または変更を管理する手続では、終了または変更後にどの情報セキュリティの責任および義務を引き続き有効とすることが望ましいかを定義することが大切です。

16-2-5. 守秘義務または秘密保持契約

【6.6 秘密保持契約又は守秘義務契約】

実施手順（例）

- 当組織の従業者は、当組織との間で機密情報に関する秘密保持の契約を締結する。なお、同契約には原契約の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含める。
- 当組織との委託先との間で、必要に応じて秘密保持の契約を締結する。
- 情報セキュリティ委員会は、年に一度、情報セキュリティ要求事項に照らして、秘密保持契約書の妥当性を検証する。

ワンポイントアドバイス

秘密保持契約または守秘義務契約に関する要求事項は、定期的または要求に影響する変化が発生した場合に、レビューすることが大切です。

【6.3 情報セキュリティの意識向上、教育及び訓練】

実施手順（例）

- すべての従業者は、職務に関連する方針および手順についての適切な、意識向上のための教育および訓練を受ける必要がある。
- 当組織では従業者が次の事項に関して認識を持てるよう教育・訓練を実施する。
 - 情報セキュリティ方針
 - 情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリテ

ィに対する自らの貢献

- ISO/IEC 27001 の要求事項に適合しないことの意味

c. 教育計画は情報セキュリティ委員会が作成し、トップマネジメント（経営層）が承認する。

d. 当組織の主な教育を以下に示す。（以下の教育は「教育実施記録」に残す。）

- 新任部門管理者（運用委員）

新任の情報セキュリティ委員会メンバーに実施する。

- 入社時・社内異動者の教育（適時）

新入社員、中間採用者に対して、入社時にセキュリティ教育を実施する。

- 定期教育（「年間計画表」に基づく）

年に最低 1 回、適用範囲内の従業員に対して、情報セキュリティの理解、再確認と改善、向上のための教育を実施する。

- 再教育

セキュリティ違反者および情報セキュリティに関する低理解度の従業員に対して、再教育を実施し、違反の再発防止に努める。

- 実施した教育の有効性評価

上記の教育実施後理解度調査などを実施し、実施した教育の有効性について評価を行う。

ワンポイントアドバイス

知識が伝わったこと、並びに意識向上、教育および訓練プログラムの有効性を確認するため、意識向上、教育および訓練の活動終了時に、従業員理解の評価を行うことが大切です。

16-2-6. リモートワーク実施手順

【6.7 リモートワーク】

実施手順（例）

- リモートワークは、情報セキュリティ委員長の承認を得たものに限って行える。
- リモートワークにて使用する PC は、会社から貸与した PC とし、家族などの同居人と共有することは禁じる。
- リモートワークにて使用する PC は、アンチウイルスソフトを導入し、「8.7 [マルウェア](#)に対する保護」に準じた設定を行う。
- リモートワークにて使用する PC に、ファイル交換ソフトなどの不正なソフトウェアをインストールすることは禁じる。
- 社内ネットワークへは [VPN](#) にて接続する。

ワンポイントアドバイス

リモートワークで個人所有の PC を使用する場合は、管理方法や接続方法について実施手順を記載することが大切です。

16-2-7. 情報セキュリティイベントの報告

【6.8 情報セキュリティ事象の報告】

実施手順（例）

情報セキュリティ事象は、「5.25 情報セキュリティ事象の評価及び決定」に従って報告し、評価を行う。

ワンポイントアドバイス

すべての従業員が情報セキュリティ事象を報告する連絡先を認識し、報告の仕組みはできるだけ簡単で使いやすく、いつでも利用できるようにすることが大切です。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

第17章. 物理的対策

章の目的

第 17 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 物理的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

17-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。[リスクアセスメント](#)の内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
7.1 物理的セキュリティ境界		7.8 装置の設置及び保護	
7.2 物理的入退		7.9 構外にある資産のセキュリティ	
7.3 オフィス、部屋及び施設のセキュリティ		7.10 記憶媒体	
7.4 物理的セキュリティの監視		7.11 サポートユーティリティ	
7.5 物理的及び環境的脅威からの保護		7.12 ケーブル配線のセキュリティ	
7.6 セキュリティを保つべき領域での作業		7.13 装置の保守	
7.7 クリアデスク・クリアスクリーン		7.14 装置のセキュリティを保った処分又は再利用	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。[ISMS](#)に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

7.1 物理的セキュリティ境界

情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。

7.2 物理的入退

セキュリティを保つべき領域は、適切な入退管理策および立寄り場所によって保護しなければならない。

7.3 オフィス、部屋及び施設のセキュリティ

オフィス、部屋および施設に対する物理的セキュリティを設計し、実装しなければならない。

7.4 物理的セキュリティの監視

施設は、認可されていない物理的アクセスについて継続的に監視しなければならない。

7.5 物理的及び環境的脅威からの保護

自然災害およびその他の意図的または意図的でない、インフラストラクチャーに対する物理的脅威などの物理的および環境的脅威に対する保護を設計し、実装しなければならない。

7.6 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施しなければならない。

7.7 クリアデスク・クリアスクリーン

書類および取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施しなければならない。

7.8 装置の設置及び保護

装置は、セキュリティを保って設置し、保護しなければならない。

7.9 構外にある資産のセキュリティ

構外にある資産を保護しなければならない。

7.10 記憶媒体

記憶媒体は、組織における分類体系および取扱いの要求事項に従って、取得、使用、移送および廃棄のライフサイクルを通して管理しなければならない。

7.11 サポートユーティリティ

情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保

護しなければならない。

7.12 ケーブル配線のセキュリティ

電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。

7.13 装置の保守

装置は、情報の**可用性**、**完全性**、**機密性**を維持することを確実にするために、正しく保守しなければならない。

7.14 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した装置は、処分または再利用する前に、すべての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

17-2. 物理的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順例を紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引きを参考に、自社に適した実施手順を策定してください。

17-2-1. 物理的なセキュリティ境界

【7.1 物理的セキュリティ境界】

実施手順（例）

- a. 当組織は、「レイアウト図」により、セキュリティ境界を定義する。
※レイアウト図は、「13-2-2. [ISMS](#):4. 組織の状況」の「4-3.情報セキュリティマネジメントシステムの適用範囲の決定」内の「物理的境界 レイアウト図（例）」を参照
- b. 重要な[情報資産](#)がある領域の入退を制限し、入退資格を有さない者の立ち入りを制限する。

ワンポイントアドバイス

許可されていない者の物理アクセスを防ぐために、入口に「関係者以外立入禁止」の表示や、入退制限の標識をつけるなどの工夫は効果的です。



17-2-2. 入退室認証システム

【7.2 物理的入退】

実施手順（例）

- a. 入退を行う対象者に対して、入退資格を設け、資格を持たない者の立ち入りを禁じる。入退資格は、従業者証またはセキュリティカードを交付することにより付与し、他人への貸借は禁じる。
- b. 外来者の訪問は、原則として、「入退受付票」に氏名、身元、入退時刻を記録し、面談者が面会確認の押印または署名を行い、退出するまでエスコートする。
- c. 宅配便などの荷物を受け取る場合は、各オフィスの入口より外で行うことを原則とし、例外的にオフィス内への入室を認める場合は、必ず対応者がエスコートする。

ワンポイントアドバイス

荷物の受け取り場所は、重要な情報処理設備から離れた場所に設定することが大切です。

【7.3 オフィス、部屋及び施設のセキュリティ】

実施手順（例）

- a. 各事業場は常時施錠可能とし、入退資格を持たない者の立ち入りを禁じる。やむを得ず施錠可能でない事業場においては、重要な情報はキャビネットに収納し施錠するなど、厳重な管理を行う。
- b. 施錠、開錠は、原則として従業者が行う。
- c. 入退を許可された外来者に対しては、原則として従業者が随行し、立ち入り場所を制限する。
- d. 秘密の情報または活動が外部から見えないう、ブラインドやパーティションを設置する。

ワンポイントアドバイス

活動内容や PC のモニタなどが外部から見えたり、聞こえたりすることがないように、外部来場者の動線ルートを事前に決めておくことが大切です。

17-2-3. 物理的セキュリティの監視

【7.4 物理的セキュリティの監視】

実施手順（例）

- a. 組織の施設は、監視カメラ、侵入者警報を設置し、認可されていないアクセスや、疑わしい行動を検知する。無人の領域には、必ず監視カメラおよび侵入者警報を設置する。
- b. 監視カメラ、侵入者警報の動作確認をするため、3 か月に 1 回点検を実施する。

ワンポイントアドバイス

無人の領域は、警報器を設置することが大切です。

17-2-4. 物理的および環境的脅威からの保護

【7.5 物理的及び環境的脅威からの保護】

実施手順（例）

- a. 各フロアには、火災報知器、消火器を設置する。
- b. サーバ付近に段ボールなどの燃えやすいものを置くことを禁じる。
- c. サーバの転倒対策として設置位置を工夫する。必要に応じて、転倒防止器具を利用するな

どの対策を行う。

ワンポイントアドバイス

ハザードマップなどにより自社の地理的な脅威を把握し、災害時における具体的対策を講じておくことが重要です。

【7.6 セキュリティを保つべき領域での作業】

実施手順（例）

- a. サーバ室には、スマートフォンやボイスレコーダー、カメラなど撮影や録音ができるものや、USB メモリなどサーバの情報をダウンロードできる機器の持ち込みは禁じる。
- b. セキュリティを保つべき領域は常時施錠し、入退資格を持たない者の立ち入りを禁じる。

ワンポイントアドバイス

セキュリティを保つべき領域での作業ルールが適切に守られているか確認することが大切です。

【7.7 クリアデスク・クリアスクリーン】

実施手順（例）

- a. クリアデスク
 - 離席時や帰宅時には、重要情報や個人情報を含む書類や記憶媒体を机上やその周辺に放置しない。
 - 書類やデータは、重要なものとそうでないものを区別して整理する。
 - プリンタ、コピーに出力した印刷分は放置せず速やかに取り出す。
- b. クリアスクリーン
 - 利用者は、食事やトイレ、会議などにより自席を離れる場合には、コンピュータのログアウト（ログオフ）や[スクリーンロック](#)を行い、第三者がコンピュータを操作したり、画面を盗み見たりできないようにする。
 - ログイン ID、パスワードを机上に貼付することは禁じる。

ワンポイントアドバイス

クリアデスク、クリアスクリーンについてのルールが適切に守られているか、チェックシートなどにより徹底することも効果的です。

【7.8 装置の設置及び保護】

実施手順（例）

- a. スイッチ、無線 LAN アクセスポイントなどは、人目につくところや通行量の多い場所を避けて設置する。
- b. サーバは、サーバ室など隔離されたエリアに設置する。隔離されていないエリアに設置する場合は、ラックなどへ収容する。
- c. サーバが設置されたエリアでの飲食、喫煙は禁じる。
- d. サーバが設置されたエリアの温度、湿度を監視し、サーバに悪影響を与えない状態を維持する。

ワンポイントアドバイス

サーバ周辺に水などの配管などが通っていないか、確認することが大切です。

17-2-5. オフプレミスの資産のセキュリティ

【7.9 構外にある資産のセキュリティ】

実施手順（例）

- a. 社外にノート PC などを持ち出す場合は、
 - ① ログインパスワードを設定する。
 - ② 必要のない機密情報、個人情報を格納しない。
 - ③ 格納するファイルは暗号化する（パスワードをつける）。
 - ④ OS・ソフトウェアが最新バージョンになっており、セキュリティソフトが入っていることを確認する。
 - ⑤ ノート PC などが入ったカバンなどを交通機関の網棚などには置かず、常時携帯する。
- b. 公共交通機関を利用する際に、顧客情報や個人情報など、重要な情報をノート PC や社用携帯で閲覧することは禁じる。

ワンポイントアドバイス

公共交通機関を利用する際に、装置（例：スマートフォン、ノート PC など）上の情報をのぞき見られるリスクから保護することが大切です。

17-2-6. 機器のメンテナンス

【7.10 記憶媒体】

実施手順（例）

- a. 外づけの記録媒体を持ち出し・持ち込みする場合は、事前に許可を得た上で行う。また、不使用時は、キャビネットに施錠保管を行う。
- b. 記憶媒体に収納する情報は必要最小限なものとし、必要のない機密情報や個人情報、会社の重要情報は保存しない。
- c. 格納するファイルは暗号化して（パスワードをつけて）保存する。
- d. 外部記憶媒体や、重要な情報が記された文書を机上や、棚上などに放置することは禁じる。
- e. 私有の外部記憶媒体を持ち込む場合、社有の外部記憶媒体を持ち出す場合は、該当部門の責任者および情報システム管理者の許可を得る。
- f. 外部記憶媒体によるデータを受け渡しは、データの内容に応じてセキュリティを確保できるような受け渡し方法をとる。
- g. お客様の USB メモリなどの記憶媒体を預かった場合は、使用する前に必ずアンチウイルスソフトによりスキャンを行う。
- h. 不要な媒体を処分する場合は、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
- i. 媒体を輸送する場合は、必要に応じて梱包などにより保護するとともに、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
- j. サーバ、ネットワーク機器（スイッチ、ルータなど）の設置場所を、情報システム管理者の許可なく移動することは禁じる。
- k. 当組織の資産および顧客から預かった資産を、情報セキュリティ委員長の許可なく無断で持ち出すことは禁じる。

ワンポイントアドバイス

USB メモリやハードディスクなどの記憶媒体に加えて、紙の文書に対してもセキュリティ対策を行うことが大切です。

【7.11 サポートユーティリティ】

実施手順（例）

- a. 情報システム管理者は、必要に応じて無停電電源装置を設置する。無停電電源装置は、ランプの確認などにより、バッテリーの寿命が尽きていないことや、緊急時の切り替えが問題なく行えるかを定期的に確認する。
- b. 情報システム管理者は、フロア（装置の設置場所）が適切な温度に保たれていることを適時確認する。

ワンポイントアドバイス

停電対策として無停電電源装置に加えて、補助発電装置を利用することも有効です。

【7.12 ケーブル配線のセキュリティ】

実施手順（例）

- 人が通る箇所のケーブル配線は、できるだけ床下か天井に配線する。床上に配線する場合には、モール、ケーブルカバーによる保護を行う。
- 配線ケーブルに異常がないか、3 か月に 1 回点検を行う。
- 誤接続を防止するために、ケーブルにラベルをつける、役割ごとに色の異なるケーブルを使う。
- ケーブル配線図を作成するとともに、機器の増設や移設により配線が変更になった場合には配線図を更新する。

ワンポイントアドバイス

周辺機器の増設や移設に際して、ケーブル類の適正化を確認することが大切です。

【7.13 装置の保守】

実施手順（例）

サーバ、ネットワーク機器など主要な装置は、製造元から提供されたマニュアルを参照し、製造元が推奨する頻度にて点検、保守を行い、記録する。

ワンポイントアドバイス

装置の点検・保守が定期的に実施され、記録されているか確認することが大切です。

【7.14 装置のセキュリティを保った処分又は再利用】

実施手順（例）

- PC を処分する場合は、従業員が各自で処理せず、情報システム管理者に処理を依頼する。情報システム管理者は、ハードディスクなどの記憶媒体については、物理的破壊もしくは、完全消去により処分する。
- 上記以外の方法により、処分する必要があると認められる場合、事前に情報セキュリティ委員長の承認を得ることを要するものとする。
- 情報システム管理者は、装置を再利用する場合、不要な情報を完全に消去し、またライセンス供与されたソフトウェアが消去されたことを確認の上、再利用する。

ワンポイントアドバイス

廃棄・再利用する際、情報を消去する責任者と手順を定めることが大切です。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

17-3. BYOD、MDM

17-3-1. BYOD（Bring Your Own Device）導入に向けて

関連する主な管理策

6.3、6.7、7.9、8.1、8.7

BYOD の概念や、導入に向けたポイント、運用手順を説明します。

BYOD（Bring Your Own Device）

BYOD とは、個人が私物として所有している端末（PC やスマートフォンなど）を業務に使う利用形態のことです。従来は、業務で使用する端末は企業が購入し、従業員に貸与することが一般的でした。しかし、使い慣れた端末を利用できることによる働きやすさの実現や、端末購入コストの削減などの観点から、従業員が持つ私物のデバイスを業務に利用する BYOD が導入されるようになりました。

BYOD の主なメリット・デメリット

メリット	デメリット
● コスト削減 企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入替も基本的には個人負担となります。 ● 使い慣れた端末の業務利用 従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率があがります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。	● <u>シャドーIT</u> ルールの整備や技術的な対策を講じないと、シャドーIT が増加してしまう恐れがあります。 ● セキュリティリスク 個人の端末では、さまざまな Web サイトやアプリケーションを利用することがあるため、ウイルス感染や<u>不正アクセス</u>といった被害にあう可能性が高くなります。

BYOD を運用する際のポイント

BYOD を運用する際は、適切なルールを策定し、周知することが重要です。また、ルールに加えて、技術的な対策を講じることも重要です。

運用手順（例）

- a. BYOD に関する使用ルールや禁止事項を決めて周知する。
- b. BYOD で使用する機器については管理者に申請し、許可を得る。
- c. BYOD で使用する機器が紛失した場合の対応フローを策定し、周知する。
- d. BYOD で行える業務範囲やリモートアクセスの権限を設定する。
- e. 社内ネットワークへは、[VPN](#) を利用する場合のみ接続できるようにする。
- f. 必要以上に業務データを蓄積させない。（保存可能なデータに関するルールを決める。）
- g. 業務で使用する PC は、[EDR](#) を導入し、「8.7 [マルウェア](#)に対する保護」に準じた設定を行う。
- h. 業務で使用する PC に、[ファイル共有ソフト](#)などの不正なソフトウェアをインストールすることは禁じる。

17-3-2. MDM（Mobile Device Management）導入のポイント

関連する主な管理策

6.7、7.9、8.1

MDM の概念や、導入に向けたポイント、運用手順について説明します。

MDM（Mobile Device Management）

MDM とは、企業が保有しているモバイル端末（スマートフォンやタブレットなど）を一元管理できるシステムのことです。オフィスの外にあるデバイスも管理できます。ポリシー（パスワードの長さやロック画面の解除方法、インストールできるアプリケーションの制限など）を従業員のモバイル端末に適用し、違反した場合に警告を行ったり管理者に通知したりできます。また、万が一紛失や盗難があった際には、位置情報の確認や遠隔でモバイル端末の画面をロックしたり、リモートワイプ（端末に保存されているデータを遠隔で初期化する機能）したりすることができ、機密情報を守れます。

MDM を導入する際のポイント

コスト・費用	MDM は導入して終わりではなく、維持費がかかります。自社の予算に合わせた確認をすることが大切です。
対応している OS の確認	すべての OS に対応している MDM もあれば、一部のみに対応している MDM もあります。導入する MDM が、自社で使

	用している端末の OS に対応しているか確認することが大切です。
サポート体制	MDM の導入時や導入後の運用サポートなどが受けられるか確認することが大切です。
利用者の意見を反映した社内ルールの策定、および MDM の選定	MDM は情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。例えば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDM による制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定や MDM の選定を進めることが重要です。

MDM の運用手順について説明します。

運用手順（例）

- a. モバイル端末の紛失・盗難時の対応
 1. 従業員は、モバイル端末を紛失・盗難にあった場合は、速やかに情報セキュリティ管理者に報告する。
 2. 情報セキュリティ管理者は、従業員からモバイル端末の紛失・盗難の報告を受けた場合、速やかにリモートでモバイル端末の画面をロックし、位置情報を確認する。
 3. 情報セキュリティ管理者は、モバイル端末の位置情報が確認できず、発見が困難であると想定される場合、リモートワイプを実施し、モバイル端末内のデータを削除する。
- b. 業務で新たにアプリケーションが必要になった場合、情報セキュリティ管理者に連絡し、インストールの許可をもらう。

第18章. 技術的対策

章の目的

第 18 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。また、技術的管理策に関して、テーマごとの対策について学ぶことも目的とします。

主な達成目標

- 技術的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること
- Security by Design、[ゼロトラスト](#)・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること

18-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に掲載された合計 93 項目の管理策を参考に、対策基準を策定します。[リスクアセスメント](#)の内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022 に基づき管理策を決定する（例）

【凡例】 採用：○・不採用：×

項目	採用、 不採用	項目	採用、 不採用
8.1 利用者エンドポイント機器		8.18 特権的なユーティリティプログラムの使用	
8.2 特権的アクセス権		8.19 運用システムに関わるソフトウェアの導入	
8.3 情報へのアクセス制限		8.20 ネットワークのセキュリティ	
8.4 ソースコードへのアクセス		8.21 ネットワークサービスのセキュリティ	
8.5 セキュリティを保った認証		8.22 ネットワークの分離	
8.6 容量・能力の管理		8.23 ウェブ・フィルタリング	
8.7 マルウェア に対する保護		8.24 暗号の使用	
8.8 技術的ぜい弱性の管理		8.25 セキュリティに配慮した開発のライフサイクル	
8.9 構成管理		8.26 アプリケーションのセキュリティの要求事項	
8.10 情報の削除		8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	
8.11 データマスキング		8.28 セキュリティに配慮したコーディング	

8.12 データ漏えいの防止		8.29 開発及び受入れにおけるセキュリティ試験	
8.13 情報のバックアップ		8.30 外部委託による開発	
8.14 情報処理施設の冗長性		8.31 開発環境、試験環境及び運用環境の分離	
8.15 ログ取得		8.32 変更管理	
8.16 監視活動		8.33 試験情報	
8.17 クロックの同期		8.34 監査試験中の情報システムの保護	

対策基準の内容は、基本方針とともに公開可能なものとして作成します。[ISMS](#)に基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022 の文献を参照しながら作成してください。

対策基準（例）

8.1 利用者エンドポイント機器

利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。

8.2 特権的アクセス権

特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。

8.3 情報へのアクセス制限

情報およびその他の関連資産へのアクセスは、確立された[アクセス制御](#)に関するトピック固有の方針に従って、制限しなければならない。

8.4 ソースコードへのアクセス

ソースコード、開発ツール、[ソフトウェアライブラリ](#)への読取りおよび書込みアクセスを、適切に管理しなければならない。

8.5 セキュリティを保った認証

セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関

するトピック固有の方針に基づいて備えなければならない。

8.6 容量・能力の管理

現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。

8.7 マルウェアに対する保護

マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。

8.8 技術的脆弱性の管理

利用中の情報システムの技術的脆弱性に関する情報を獲得しなければならない。また、そのような脆弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

8.9 構成管理

ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立、文書化、実装、監視し、レビューしなければならない。

8.10 情報の削除

情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。

8.11 データマスキング

データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。

8.12 データ漏えいの防止

データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。

8.13 情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。

8.14 情報処理施設の冗長性

情報処理施設・設備は、**可用性**の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。

8.15 ログ取得

活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。

8.16 監視活動

セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。

8.17 クロックの同期

組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。

8.18 特権的なユーティリティプログラムの使用

システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

8.19 運用システムに関わるソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。

8.20 ネットワークのセキュリティ

システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。

8.21 ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。

8.22 ネットワークの分離

情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離し

なければならない。

8.23 ウェブ・フィルタリング

悪意のあるコンテンツにさらされることを減らすために、外部 Web サイトへのアクセスを管理しなければならない。

8.24 暗号の使用

暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。

8.25 セキュリティに配慮した開発のライフサイクル

ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。

8.26 アプリケーションのセキュリティの要求事項

アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。

8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。

8.28 セキュリティに配慮したコーディング

セキュリティに配慮したコーディングの原則を、ソフトウェア開発に適用しなければならない。

8.29 開発及び受入れにおけるセキュリティ試験

セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。

8.30 外部委託による開発

組織は、外部委託したシステム開発に関する活動を指揮、監視し、レビューしなければならない。

8.31 開発環境、試験環境及び運用環境の分離

開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。

8.32 変更管理

情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。

8.33 試験情報

テスト用情報は、適切に選定、保護、管理しなければならない。

8.34 監査試験中の情報システムの保護

運用システムの**アセスメント**を伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

18-2. 技術的対策として重要となる実施項目

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002 に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

18-2-1. エンドポイントデバイス

【8.1 利用者エンドポイント機器】

実施手順（例）

- a. モバイル機器を社外に持ち出す場合、ログインパスワードを設定する。
- b. 必要のない機密情報、個人情報などは、モバイル機器に格納しない。
業務上必要のある機密情報や個人情報をモバイル機器に格納する場合は、暗号化する。（パスワードをつける。）
- c. モバイル機器を利用者が限定されない無償の WiFi スポットなどへ接続することは禁じる。
 - 携帯電話・スマートフォンの管理
社有の携帯電話・スマートフォン（以下「社有携帯電話など」という）を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱う。
 - 社有携帯電話などを使用する者は、使用者本人以外が操作できないよう、パスワードを設定して保護する。
 - 持ち歩く際は、ストラップをつけるなどの紛失・盗難防止策を必要に応じて講じる。
 - 電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮する。
 - 私有の携帯電話・スマートフォンを業務で使用する場合は、情報システム管理者の承認を要する。また、社有携帯電話などと同様の安全対策を実施する。
- d. 利用者はノート PC に対して、パスワード付きのスクリーンセーバを設定し、のぞき見を防止する。スクリーンセーバの設定時間は 10 分以内とする。

ワンポイントアドバイス

利用者端末装置（携帯、スマートフォン、ノート PC など、ユーザーが情報処理サービスにアクセスするために使用するさまざまなデバイス）の取扱いに関する規則を定めることが大切です。

18-2-2. 特権アクセス権

【8.2 特権的アクセス権】

実施手順（例）

- a. 特権的アクセス権は特定の者に付与し、管理対象システムとその保有者を明確にする。
- b. 半年に 1 回、または組織に何か変更があった際、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任、力量の点で今も適格であるか否かを検証する。

ワンポイントアドバイス

特権的アクセス権は一般の利用者よりも多くの権限が付与されているため、悪用されると影響が大きいです。ID 付与に際しては、厳格かつ安全な管理のもとに運用されることが大切です。

18-2-3. アクセス制限

【8.3 情報へのアクセス制限】

実施手順（例）

- a. 情報システム管理者は、取扱いに慎重を要する情報へのアクセス権限を、必要な者のみに割り当てる。
- b. 未知の利用者識別情報または匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。

ワンポイントアドバイス

情報およびその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止することが大切です。

【8.4 ソースコードへのアクセス】

実施手順（例）

ソースコードや設計書、仕様書などの関連書類は、アクセス権で管理されたフォルダに厳重に保管する。

ワンポイントアドバイス

ソースコードが変更される、または開発環境の一部のデータが認可されていない人物によって取り出される可能性をなくするため、ソースコードへのアクセスを適切に制御することが大切です。

18-2-4. 安全な認証

【8.5 セキュリティを保った認証】

実施手順（例）

重要な情報システムにアクセスする際は、パスワードに加えて、多要素認証を使用し、不正アクセスの可能性を減らす。

ワンポイントアドバイス

多要素認証では、知識（パスワード、秘密の質問など）、所持物（スマートフォン、ICカードなど）、生体情報（指紋、声紋など）のうち、2つ以上を組み合わせることで、認可されていないアクセスの可能性を減らします。

18-2-5. キャパシティ管理

【8.6 容量・能力の管理】

実施手順（例）

- a. 情報システム管理者は、コンピュータやネットワークの応答時間など、その負荷状況について、業務を通じて問題がないか否かを確認する。CPU やメモリ、ハードディスクなどの外部記憶装置の使用率など、リソースの使用状況を定期的に監視する。
- b. リソースの使用状況に応じてリソースの割り当てを調整すると同時に、将来必要となる容量や能力を予測し、システムのパフォーマンスを維持するため、必要なリソースを事前に確保する。
- c. 情報システム管理者は、問題が発見された場合、速やかに原因の究明を行い、情報セキュリティ委員会に報告する。
- d. 情報セキュリティ委員会は、情報システム管理者に対策を指示し、必要に応じて経営陣に報告する。
- e. 情報システム管理者は、中長期的な業務量の増減を考慮し、将来的にシステムに必要な容量を予測し、必要であればトップマネジメントに報告する。

ワンポイントアドバイス

クラウドサービスを利用することで、特定のアプリケーションおよびサービスで利用できる資源を、要求に応じて迅速に拡張・削減することができます。

18-2-6. マルウェアに対する保護

【8.7 マルウェアに対する保護】

実施手順（例）

- a. ネットワークに接続するすべてのパソコン、サーバ上に情報システム管理者が指定したアンチウイルスソフトを導入する。
- b. アンチウイルスソフトを常時設定にし、ファイルへのアクセスおよび電子メールの受信時に常時スキャンできる設定を行う。
- c. 常時スキャンに加えて情報システム管理者が指定した期間に一度、ファイル全体に対するスキャンを行う。
- d. 自動でウイルス定義ファイルの更新が行われるように設定する。
- e. 標的型メール対応
 - メールの添付書類やメール中のリンクは、原則として（送信者に確認するなどの方法で）安全が確認できるまで開かない。
 - ファイルの拡張子を表示させる設定とし、添付ファイルの拡張子が、通常使用しない内容の場合、ファイルの参照を禁じる。
通常使用しないファイルの拡張子の例：.exe、.pif、.scr

ワンポイントアドバイス

基本的な対策として、社内パソコンのウイルス定義ファイルが常に最新版に更新されているかの確認を徹底することが重要です。

18-2-7. 技術的脆弱性の管理

【8.8 技術的脆弱性の管理】

実施手順（例）

- a. 情報セキュリティ委員会および情報システム管理者は、技術的な脆弱性のニュースを常に意識し、時期を失せず効果的に外部の攻撃を防御する。
- b. OS やアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法により脆弱性に対処する。

ワンポイントアドバイス

セキュリティパッチは、正当な供給元から取得したもののみを使用することが大切です。

18-2-8. 構成管理

【8.9 構成管理】

実施手順（例）

システムの構成要素とその相互関係を理解し管理するため、台帳や構成管理ツールを用いて、ハードウェア、ソフトウェア、ネットワーク機器、設定ファイルなど、システムを構成するすべての要素の情報を把握する。

ワンポイントアドバイス

ハードウェア・ソフトウェア・サービス・ネットワークが、必要とされるセキュリティ設定により正しく機能し、認可されていない変更や誤った変更によって構成が変えられないようにすることが大切です。

18-2-9. 情報の削除

【8.10 情報の削除】

実施手順（例）

- 業務上必要がなくなったデータは速やかに削除する。
- 記憶媒体上のデータを削除する際は、データ消去ソフトを使用し、復元できないよう、完全に削除する。
- ハードディスクを廃棄する際は、[磁気データ消去装置](#)を用いてハードディスクのデータを削除してから廃棄する。

ワンポイントアドバイス

取扱いに慎重を要する情報などの機密情報については、必要がなくなった時点で速やかに削除することが大切です。情報を保有していることがリスクなので、不要な情報は持ちつづけけないことが重要です。

18-2-10. データ保護

【8.11 データマスキング】

実施手順（例）

保有している情報をマーケティング分析などの目的で二次利用する場合には、個人情報や重要情報が推測できない形に加工した上で利用する。

ワンポイントアドバイス

取扱いに慎重を要するデータ（個人情報や重要情報）の保護が必要である場合、[データマスキング](#)・仮名化・匿名化などの手法を使用して保護することが大切です。これにより、データが万が一漏えいしても、その内容を第三者に理解されることを防げます。

【8.12 データ漏えいの防止】

実施手順（例）

- 漏えいから保護する情報を特定し、分類する。
- [ファイル共有ソフト](#)の使用を禁じる。
- 重要な情報が画面に表示されている場合は、スクリーンショットや写真を撮ることを禁じる。
- [ファイアウォール](#)や [IDS](#)、[IPS](#) などによって [不正アクセス](#) を防止する。「8.20 ネットワークのセキュリティ」に従う。
- 重要データについてアクセス制限を設ける。「8.3 情報へのアクセス制限」に従う。
- 重要データは [暗号化](#) して保管する。「8.24 暗号の使用」に従う。

ワンポイントアドバイス

個人やシステムによる情報の認可されていない開示・抽出を検出し、防止することが大切です。

18-2-11. バックアップ

【8.13 情報のバックアップ】

実施手順（例）

- 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、[不正アクセス](#)、[改ざん](#) などから守るために、必要に応じてシステムおよびデータのバックアップを行う。
- バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。
- 情報システム管理者は、バックアップが確実に実行されており、障害時に復元が可能か否かを月に1度チェックする。

ワンポイントアドバイス

クラウドサービスを利用している場合は、クラウド環境にあるデータのバックアップも作成しているか確認することが大切です。[ランサムウェア](#)対策として、バックアップは2つ作成し、1つはネットワークから隔離したオフサイトで保管することが大切です。

18-2-12. 冗長化

【8.14 情報処理施設の冗長性】

実施手順（例）

- a. 情報システムは、可用性に関する業務上の要求事項を明確にし、必要に応じて予備の機器を用意して二重化を行い、冗長性をもたせる。
- b. 緊急の場合、速やかに予備の機器に切り替えられるよう、動作確認を月に 1 回行う。

ワンポイントアドバイス

冗長な構成要素および処理活動を常に作動させておくか、緊急の場合に自動または手動で作動させるかを確認します。常に作動させておく場合は、稼動状況を確認することが大切です。

18-2-13. ログイン

【8.15 ログ取得】

実施手順（例）

- a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてログの取得を行う。
- b. 情報システム管理者は、必要に応じてログの定期的なチェックを行う。
- c. ログは、情報システム管理者またはその指名する担当がアクセスできるようにする。
- d. 情報システム管理者は、運用担当者がサーバで行った作業を確認する。確認は、作業ログ、または日報・サーバ作業記録の閲覧により行う。

ワンポイントアドバイス

セキュリティインシデントの分析、警告および調査のために、システム間のログを相関づけられるようにすべてのシステムが同期した時刻源（8.17 クロックの同期を参照）を持つことが重要です。

18-2-14. 監視

【8.16 監視活動】

実施手順（例）

ファイアウォール・IDS・IPSのログを常に監視し、異常な動作を検知した場合は速やかに対応する。

ワンポイントアドバイス

通常時およびピーク時のシステム使用率や、各利用者または利用者グループの通常のアクセス時間・アクセス場所・アクセス頻度を考慮して正常な行動・動作の基準を確立し、基準に照らして異常を監視することが大切です。

18-2-15. クロック同期

【8.17 クロックの同期】

実施手順（例）

- a. 情報システム管理者は、クライアント PC やサーバなどすべての情報システムについてクロックを同期させる。
- b. すべての情報システムのクロックを同期させるために、NTP を使用する。

ワンポイントアドバイス

イベントログは、調査や法令や懲戒が関わる場合の証拠として必要となる可能性があり、不正確な監査ログは証拠の信頼性を損なう可能性があります。コンピュータ内のクロックを正しく設定し、イベントログの正確さを確実にすることが重要です。

18-2-16. 特権ユーティリティの使用

【8.18 特権的なユーティリティプログラムの使用】

実施手順（例）

- a. ユーティリティプログラムの使用は、原則として OS 標準機能のみ許可する。
- b. その他のユーティリティプログラムが必要となった場合は、情報システム管理者の承認を得た上で利用する。

ワンポイントアドバイス

情報システムの大半には、パッチ適用・ウイルス対策・バックアップ・ネットワークツールなど、システムやアプリケーションによる制御を無効にできる 1 つ以上のユーティリティプログラムが組み込まれています。不要なユーティリティプログラムは、すべて除去・無効化することが大切です。また、特権的ユーティリティの中には、データベースの中身を、その整合性を気にすることなく強制的に書き換えることができる機能や、他の利用者の権限でデータを操作できる機能をもったものがあります。こうした特権的なユーティリティを野放しにすると組織の情報セキュリティが保てなくなるため、厳しく利用を管理する必要があります。

18-2-17. ソフトウェア管理

【8.19 運用システムに関わるソフトウェアの導入】

実施手順（例）

- a. 運用システムに、開発用のコードを導入しない。
- b. PC を含む社内の情報システムで使用するソフトウェアは、原則情報システム管理者によっ

て指定されたもののみ使用し、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。他社が開発したソフトウェアを利用する場合、その開発会社が要求している条件やスペックを満たす環境で運用する。

- c. 情報システム管理者は、利用者がインストール可能なソフトウェアを定期的に見直す。
- d. 利用者は認可されていないソフトウェアをインストールしてはならず、業務上、必要な場合は、情報システム管理者の承認を得た上でインストールする。
- e. ファイル共有ソフトなど、ウイルス感染や不正アクセスなどの原因となりやすいソフトウェアのインストールを禁じる。

ワンポイントアドバイス

組織は、利用者がインストールできるソフトウェアの種類について、厳密な規則を定めて施行することが大切です。

【8.25 セキュリティに配慮した開発のライフサイクル】

実施手順（例）

セキュリティに配慮した開発のための方針を以下に記す。

- a. 開発の初期段階でセキュリティ要件を明確化する。
- b. 開発環境は、「8.31 開発環境、試験環境及び運用環境の分離」の「b. セキュリティに配慮した開発環境」に従う。
- c. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
- d. 開発したシステムに脆弱性がないかテストする。
- e. 開発文書（仕様書、設計書、テスト仕様など）は、必要最低限の者だけがアクセスできるようにする。
- f. 受託開発または客先への派遣による開発では、クライアントから提示のあったセキュリティの方針・ルールなどに従う。

ワンポイントアドバイス

ソフトウェアやシステムのセキュリティに配慮した開発のための規則を定めることが大切です。

【8.26 アプリケーションのセキュリティの要求事項】

実施手順（例）

- a. アプリケーションを取得する際、リスクアセスメントを通じてアプリケーションの情報セ

セキュリティ要求事項を決定する。必要に応じて、情報セキュリティの専門家の支援を受け、情報セキュリティ要求事項を決定する。

b. セキュリティに配慮したシステムを構築するための原則は、以下の通りとする。

- 情報セキュリティ事象を防止・検知し、対応するために必要な管理策を分析すること。
- 情報セキュリティ要求事項を満たすための費用・時間・複雑さを考慮すること。

ワンポイントアドバイス

ネットワークを介してアクセス可能なアプリケーションは、ネットワークに関連した脅威を受けやすいため、リスクアセスメントの実施や、管理策を決定することが大切です。

【8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則】

実施手順（例）

- a. 社内使用の情報システムおよび外部向けに提供する情報システムの開発に際しては、情報セキュリティ事項を明確にし、要件定義として記録する。
- b. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
- c. 開発したシステムに脆弱性がないかテストする。

ワンポイントアドバイス

セキュリティに配慮したシステム構築の原則および確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするため、定期的にレビューすることが大切です。

【8.28 セキュリティに配慮したコーディング】

実施手順（例）

- a. ユーザーが入力したデータを確認し、問題がある場合は読み込まないようにする。
- b. セキュリティ上の問題を発見しやすくするため、設計は可能な限りシンプルにする。
- c. ユーザーには必要最小限の権限・機能を与える。
- d. 他のシステムに送信するデータは、サニタイズ（特殊文字を一般的な文字に変換すること）を行い、不正操作を防止する。

ワンポイントアドバイス

コーディングの原則が定められていない場合、コードの書き方がそれぞれ異なってしまうことで、コードが読みづらく、脆弱性が生まれる危険性があります。セキュリティに配慮したコー

ディングの規則を定め、コードの書き方を統一することが大切です。

【8.29 開発及び受入れにおけるセキュリティ試験】

実施手順（例）

- a. 情報システムのセキュリティテストは、運用に移行する前に行う。
- b. システムの受入れ試験
 - 情報システムの導入または改修の際は、受入れ時に動作確認を行う。
 - 必要に応じて受入れテストの仕様書を作成し、確認を行う。
 - 必要に応じて、コード分析ツールや脆弱性スキャナのような自動化ツールを利用し、セキュリティに関連する欠陥を修正する。
 - 受入れ試験の結果は、受入れ部門の管理者および情報システム管理者が承認する。

ワンポイントアドバイス

効果的な試験を確実にするために、試験環境、ツール、技術の試験および監視も考慮する必要があります。

【8.30 外部委託による開発】

実施手順（例）

情報システムの開発を外部に委託する場合の手順は以下に従う。

- a. 「委託先審査票」によって委託先を評価、選定、およびあらかじめ定められた頻度（最低年1回）で再審査し、また、契約の履行状況を監視する。
- b. 委託先との契約を締結する。（契約書には情報セキュリティ要求事項を含める。）
- c. 成果物の品質および正確さを評価するため、「8.29 開発及び受入れにおけるセキュリティ試験」に定める「b. システムの受入れ試験」を実施する。

ワンポイントアドバイス

外部委託したシステム開発に関する活動を随時、指導、監視およびレビューすることが大切です。

【8.31 開発環境、試験環境及び運用環境の分離】

実施手順（例）

- a. 情報システムの開発に際しては、開発・テスト環境と本番環境を、物理的・論理的に分割する。

- セキュリティに配慮した開発環境
開発は、開発業務を行わない従業員から分離した場所およびシステムにて行う。また開発環境は、運用環境から分離する。
- ソースコードおよび設定ファイルは、不意の消去や改ざんから保護するため、必要最小限の者だけがアクセスできるようにする。

ワンポイントアドバイス

開発および運用環境に変更を加える際は、組織としての事前レビューおよび承認を徹底することが大切です。

【8.32 変更管理】

実施手順（例）

- a. 変更管理は以下のプロセスで行う。
 1. 変更の承認
変更を行う前にその変更の必要性、変更が及ぼす影響、変更によるリスクの変動について評価し、情報システム管理者の承認を得る。
 2. 変更のテスト
変更を適用する前に、情報システムへの影響を確認するためにテストを行う。
 3. 変更の監査
変更後に変更が適切に行われたか否かを監査によって確認する。
- b. 情報システム管理者は、サーバに周辺機器を接続する場合や、サービスパックを適用する場合、事前に情報収集し、問題の有無を確認する。万が一、適用後に問題が生じた場合は、再インストールすることで問題解決を即座に実施する。
- c. OS やパッケージソフトウェアを変更する際は、情報システム管理者はテスト機や予備機を用いて、現在の情報システムが変更後の OS 上で問題なく動作するかを検証する。
- d. パッケージソフトウェアのカスタマイズを原則として禁じる。万が一、修正を行う場合は、動作上の影響およびベンダーから将来的に受けるサポートへの影響を考慮し、情報システム管理者の許可を得る。

ワンポイントアドバイス

変更管理手順は、情報の機密性、完全性、可用性を確実にするために、設計の初期段階からその後のすべての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装することが大切です。

【8.33 試験情報】

実施手順（例）

- a. テストデータとして個人情報を使用することを禁じる。
- b. 実データをテストデータとして使用する場合は、情報システム管理者の承認を得てから使用する。テスト終了後は、実データを直ちに削除し、情報システム管理者に対して報告する。

ワンポイントアドバイス

テストデータは、注意深く選定し、保護し、管理することが大切です。

【8.34 監査試験中の情報システムの保護】

実施手順（例）

- a. 情報システムの監査は、システム停止のリスクを考慮し、営業時間外もしくは休日を利用して実施することを原則とする。
- b. 情報システムのメンテナンスなどにより情報システムの稼働を停止する場合は、業務への影響を及ぼさない範囲または時間帯で行うように計画する。

ワンポイントアドバイス

運用システムのアセスメントを伴う監査活動およびその他の保証活動を計画し、試験者と管理層の間で合意することが大切です。

18-2-18. ネットワークセキュリティ

【8.20 ネットワークのセキュリティ】

実施手順（例）

- a. ネットワーク図および装置（例：ルータ、スイッチ）の構成ファイルを含む文書を最新に維持する。
- b. 社内ネットワークへ接続する際は、情報システム管理者の承認を受け、指示された手順に従う。
- c. 情報システム管理者は、ネットワークにおける社外との境界には[ファイアウォール](#)を設けるなど、不正侵入対策を施す。
- d. ネットワーク装置のファームウェアの定期的なアップデートを行う。
- e. 他人のID、パスワードで、社内ネットワークに接続することを禁じる。
- f. 一旦、社内ネットワークから切り離れたパソコンなどは、ウイルスチェックなどの安全確認を行ってから再接続する。

- g. 持ち込みおよび私有 PC 利用の場合は、社内ネットワークに接続しない。やむを得ず接続する場合は、情報システム管理者が指定するソフトウェアによりウイルスチェックを行う。
- h. 無線 LAN を使用する場合は、情報システム管理者の承認を得て、暗号化、接続パソコンの認証など、十分な安全対策を実施する。
- i. 不特定が利用できる公衆無線 LAN や WiFi スポットに接続することは禁じる。

ワンポイントアドバイス

ネットワークや、ネットワークをサポートする情報処理施設における情報を、ネットワークを通じた危険から保護することが大切です。

【8.21 ネットワークサービスのセキュリティ】

実施手順（例）

- a. 利用しているネットワークサービスを特定する。
- b. 情報システム管理者は、ネットワークサービスを利用する場合は、ネットワークサービス提供者と SLA を締結する。

ワンポイントアドバイス

ネットワークサービスには、接続・プライベートネットワークサービスおよびネットワークセキュリティ管理のための ソリューション（ファイアウォール、IDS など）が含まれます。

18-2-19. ネットワークの分離

【8.22 ネットワークの分離】

実施手順（例）

- a. インターネットと社内 LAN との境界に ファイアウォール を設置する。
- b. メール、Web サーバなどの公開サーバは、社内のネットワークと分離する。
- c. ゲスト用の無線アクセスネットワークを、社内用の無線アクセスネットワークから分離する。

ワンポイントアドバイス

各領域の境界は、明確に定めることが大切です。ネットワーク領域間のアクセスが認められる場合は、境界にファイアウォールなどを設けて制御することが大切です。

18-2-20. Web フィルタリング

【8.23 ウェブ・フィルタリング】

実施手順（例）

フィルタリングソフトを利用し、業務上不必要な Web サイト、危険性のある Web サイトへアクセスすることを防ぐ。

ワンポイントアドバイス

システムが[マルウェア](#)によって危険にさらされることを防ぐために、認可されていないウェブ資源へのアクセスを防止することが大切です。

18-2-21. 暗号の使用

【8.24 暗号の使用】

実施手順（例）

a. 暗号利用のための規則

- [SSL/TLS](#)

当組織の Web サイトの通信は、SSL/TLS を用いて暗号化する。

- [無線 LAN](#)

無線 LAN の通信は暗号化し、暗号化の規格は[脆弱性](#)の報告されていない安全な方法とする。

b. 鍵の管理

- SSL/TLS

情報システム管理者は、証明書に対する秘密鍵を適切に管理する。

- 無線 LAN

アクセスポイントの管理者画面は、情報システム管理者のみがアクセスでき、そのパスワードを厳重に管理する。

c. 重要データの[暗号化](#)

- 暗号化の対象とするデータを選定する。
- 利用する暗号の種類を決める。
- 暗号鍵のライフサイクルに関する方針を策定する。
- 暗号の管理責任者を定める。

ワンポイントアドバイス

業務や情報セキュリティ要求事項に従い、暗号に関連する法令・規制・契約上の要求事項を考慮し、情報の[機密性](#)・[真正性](#)・[完全性](#)を保護するための暗号の適切かつ効果的な使用を確実に

履行することが大切です。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

18-3. 実施手順を適用するセキュリティ概念

18-3-1. Security by Design

関連する主な管理策

5.1、5.7、5.9、5.19、5.20、5.24、5.26～5.29、5.37、8.9、8.15、8.16、8.22、8.25～8.34

Security by Design とは「情報セキュリティを企画、設計段階から組み込むための方策」で、開発プロセスの最初の段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。従来のように、後づけでセキュリティ機能を追加したり、システムの導入直前に脆弱性診断などを実行したりする方法の場合、手戻りが多発することがあり、結果的に開発コストが増大する可能性があります。企画・設計の段階からセキュリティ対策を行うことで、手戻りが少なくなり、コストの削減につながり、保守性のよいシステム・ソフトウェアになります。



図 60. セキュリティ対策の実施タイミング

Security by Design 導入のメリット

- 手戻りが少なくなり、納期を守れる
- コストを削減できる
- 保守性の高いソフトウェアができる

Security by Design の工程ごとに実施内容を紹介します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
セキュリティリスク分析 ● システムで取扱う重要情報のフローやライフサイクルがわかる内容を記載したシステムプロファイルの作成（ステークホルダー、実施業務、他システムとの連携方法などがわかるように作成） ● システムプロファイルに基づくセキュリティ脅威の特定 ● セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施 ● リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソースなど）	5.1 情報セキュリティのための方針群 5.9 情報及びその他の関連資産の目録
セキュリティ要件定義 ● 遵守すべきセキュリティ標準（セキュリティベースライン）やリスク分析結果などに基づく、システムとして満たすべきセキュリティ要件の定義（機能、非機能面）	8.26 アプリケーションのセキュリティの要求事項
セキュア調達 ● セキュリティ要件に基づいて、調達仕様におけるセキュリティ仕様策定 ● セキュリティ仕様に関する、委託先との責任範囲の明確化 ● 委託先に求めるセキュリティ管理基準の策定 ● セキュリティ仕様を満たす能力を有した安全な委託先の選定 ● 不正侵入の経路となるバックドアなどが含まれていない、継続的なサポートを受けられる安全なプロダクトの	5.19 供給者関係における情報セキュリティ 5.20 供給者との合意における情報セキュリティの取扱い

選定	
セキュリティ設計 ● セキュリティ設計の実施 ➤ アプリケーションセキュリティ ➤ OS セキュリティ ➤ ミドルウェアセキュリティ ➤ ネットワークセキュリティ ➤ クラウドセキュリティ ➤ 物理セキュリティ ➤ セキュリティ運用（平時、有事）	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
セキュリティ実装 ● 設計に基づくシステムにおけるセキュリティ機能の実装 ● セキュリティ設計に基づくアプリケーションのセキュアコーディング ● セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施（堅牢化、要塞化） ➤ OS セキュリティ ➤ ミドルウェアセキュリティ ➤ ネットワークセキュリティ ➤ クラウドセキュリティ ➤ 物理セキュリティ	8.28 セキュリティに配慮したコーディング
セキュリティテスト ● セキュリティ機能テストの実施（単体テスト、結合テスト、システムテストなど） ● 脆弱性診断の実施 ➤ Web アプリケーション脆弱性診断 ➤ プラットフォーム脆弱性診断 ➤ スマートフォンアプリケーション診断 ➤ 高度セキュリティ診断（ペネトレーションテスト、レッドチーム演習など） ● 機能テストで検出されたバグの是正対応 ● 脆弱性診断で検出された脆弱性に対する、リスクベースの是正対応	8.29 開発及び受入れにおけるセキュリティ試験 8.33 試験情報 8.34 監査試験中の情報システムの保護

セキュリティ運用準備 ● セキュリティ運用体制の確立 ● 下記項目に対応したセキュリティ運用手順の整備 平時の運用 ➤ 構成管理、変更管理 ➤ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ➤ 脅威情報収集、自システムへの影響分析 ➤ CVSS などに基づく、リスクに応じた脆弱性対応 ➤ 定期的な脆弱性診断の実施 有事の運用 ➤ インシデント対応 ● システム運用において人的ミスが発生する可能性のある箇所の洗い出し、是正 ● 有事を想定したセキュリティ運用訓練の実施	5.24 情報セキュリティインシデント管理の計画及び準備 5.29 事業の中断・阻害時の情報セキュリティ 8.9 構成管理 8.32 変更管理 8.19 運用システムに関わるソフトウェアの導入
セキュリティ運用 ● セキュリティ運用を行う要員の教育/訓練の実施、重要な情報を取扱う要員のスクリーニング（要員のスキルや行動特性などを考慮） ● セキュリティ運用の実施（下記） 平時の運用 ➤ 構成管理、変更管理 ➤ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ➤ 脅威情報収集、自システムへの影響分析、是正対応 ➤ CVSS などに基づく、リスクに応じた脆弱性対応 ➤ 定期的な脆弱性診断の実施 有事の運用 ➤ インシデント対応	5.7 脅威インテリジェンス 5.26 情報セキュリティインシデントへの対応 5.29 事業の中断・阻害時の情報セキュリティ 5.37 操作手順書 8.9 構成管理 8.15 ログ取得 8.16 監視活動 8.32 変更管理

Security by Design 実施における留意事項

- 工程間でセキュリティ対策の不整合が起きないように注意すること
- 組織として考慮すべきリスクや組織能力を踏まえて実現可能なレベルで実施し、PDCA サイクルを回しながら成熟度を高めていくこと

詳細理解のため参考となる文献（参考文献）	
セキュリティ・バイ・デザイン導入指南書	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf
DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

18-3-2. ゼロトラスト、境界防御モデル

関連する主な管理策

5.9、5.15～5.23、5.29～5.30、8.1～8.3、8.15～8.16、8.21、8.32

ゼロトラストの定義

ゼロトラスト（ZT）は、従来の境界線によるセキュリティ対策とは異なり、ネットワーク内のすべてのデバイスやユーザーを信頼せず、あらゆるアクセスをゼロから検証するという考え方です。これにより、内部からの脅威や、一度内部に侵入された場合の被害を最小限に抑えることを目指します。具体的には、**多要素認証**、最小権限の原則、継続的な監視など、複数のセキュリティ対策を組み合わせることで、**アクセス制御**を強化します。

境界防御モデルとゼロトラストの違い

境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、組織が守るべき**情報資産**は信用する境界内部に存在するという前提をもとに、境界線でセキュリティ対策を講じることで、境界外部からの脅威を防ぐという考え方です。

一方、ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。

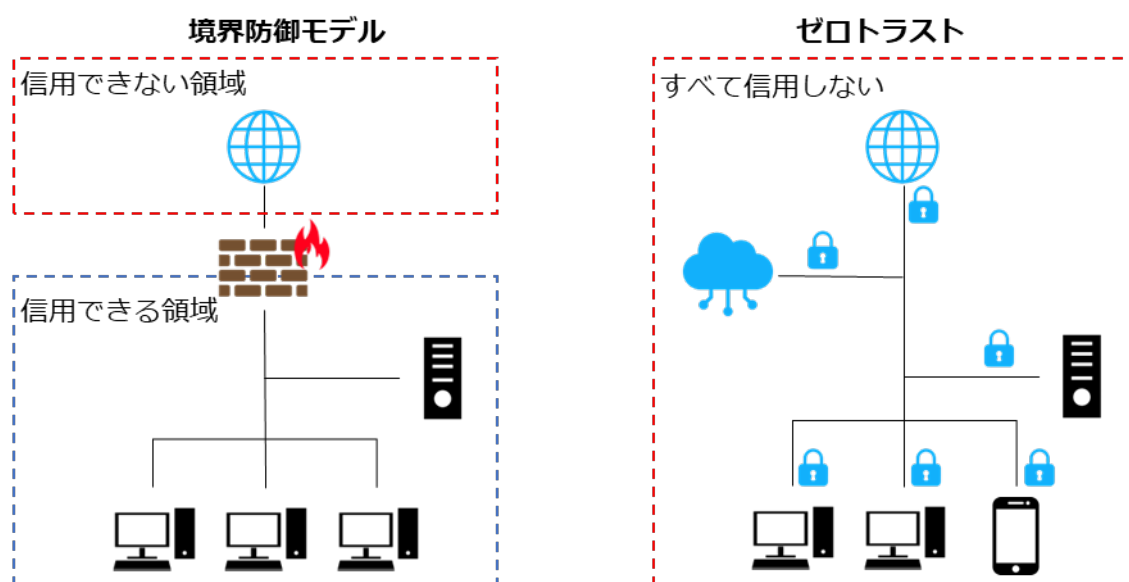


図 61. 境界防御モデルとゼロトラストの概要図

現在、クラウドサービスの普及やモバイル端末の活用、テレワークによる働き方の多様化により、内部と外部を隔てる「境界」そのものが曖昧になりつつあります。その結果、従来の社内・社外の

境界でセキュリティ対策を行う「境界防御モデル」では、サイバー攻撃やマルウェア感染などの脅威から情報資産を守ることが難しくなっています。こうした問題を解決するものとして、「ゼロトラスト」という考え方が注目されています。

One Point

ゼロトラストと境界防御の関係

ゼロトラストは、境界防御モデルで守ることが困難な脅威に対して適用する対策ではあるものの、「境界防御モデルを排除する考え」ではありません。強固なセキュリティを構築するにあたり、すでに用いられている境界防御モデルを活かすことが大切です。

ゼロトラスト導入に向けた進め方

準備工程

ゼロトラストを導入する準備として、資産（デバイスやネットワークなど）、主体（ユーザー・権限など）、ビジネスプロセスについて詳細に理解する必要があります。ゼロトラストを導入する準備として、資産、主体、データフロー、ワークフローの調査を行います。

ゼロトラスト導入プロセス

準備工程を実施した以降は、次のプロセスで進めます。

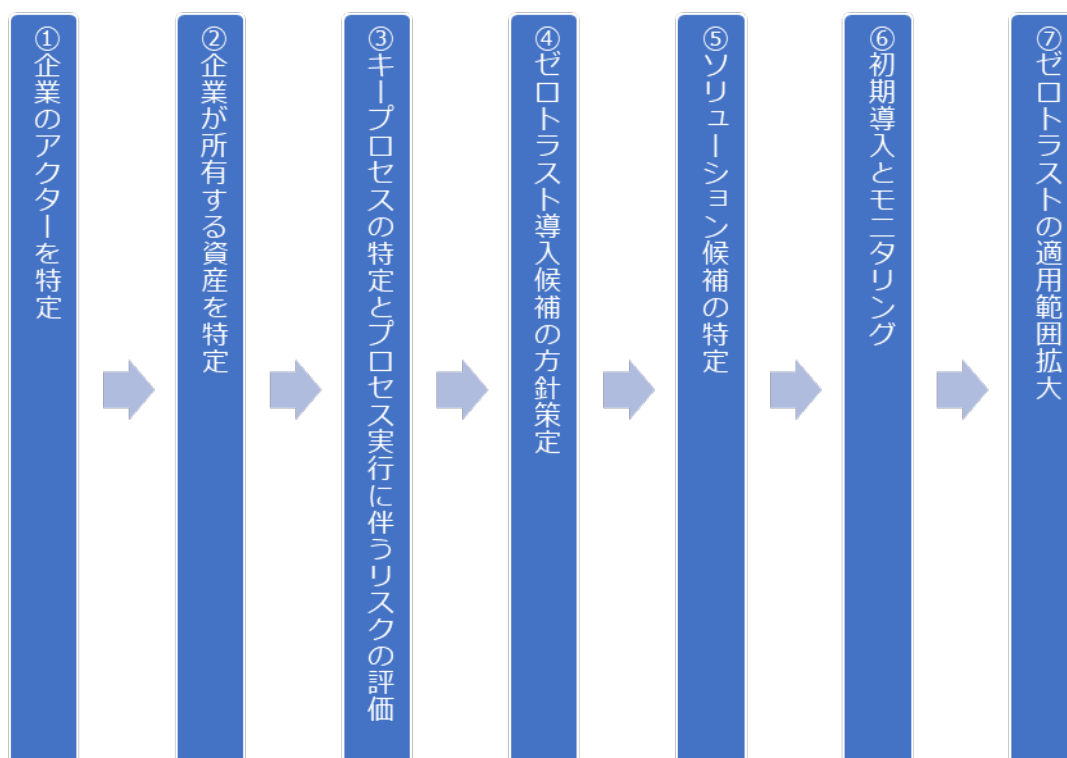


図 62. ゼロトラスト導入プロセス

(出典) IPA「ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～」をもとに作成

詳細理解のため参考となる文献（参考文献）	
ゼロトラスト導入指南書～情報系・制御系システムへのゼロトラスト導入～	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

ゼロトラスト導入の各プロセスで実施すべき内容を説明します。

1.企業のアクターを特定

企業の主体には、ユーザーに紐づいたアカウントと、サービスに紐づいたアカウントの両方が含まれることがあります。どのユーザーにどのレベルの権限を与えるのかは精査が必要です。基本的には、必要な対象に必要な権限だけ与えるという最小権限の考え方で整理します。

2.企業が所有する資産を特定

ゼロトラスト・アーキテクチャ（ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシーなどを含むサイバーセキュリティ計画のこと）は、デバイスを識別して管理する機能が必要であり、企業内のデバイスはもちろん、企業所有ではないデバイスについても識別し、監視する機能が必要です。よって、企業の情報にアクセスするデバイスについては、「[シャドーIT](#)」も含めて可能な限り資産化する必要があります。なお、企業によって可視化されているもの（例：[MAC アドレス](#)、[IP アドレス](#)）と、管理者のデータ入力による追加分も含まれます。

3.キープロセスの特定とプロセス実行に伴うリスクの評価

業務プロセス、データフロー、および組織のミッションにおけるそれらの関係（プロセス）を特定します。次に信用度レベルをつけ、ゼロトラストへ移行するプロセスを決めます。認証・認可の判断を導入することによる失敗のリスクを考慮し、初めはビジネスインパクトの低いビジネスプロセスから開始するとよいでしょう。ある程度、認証・認可の挙動を掴んでから対象を広げていくことで、リスクを抑えることができます。

4.ゼロトラスト導入候補の方針策定

資産またはワークフローを特定したら、影響を受ける対象をすべて特定します。（上流リソース（例：ID 管理システム）、下流リソース（例：セキュリティ監視）、[エンティティ](#)（例：主体ユーザー）。次に企業管理者は、候補となるビジネスプロセスで使用するリソースの信用度レベルの重みを決定します。それらを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定します。

5.ソリューション候補を特定

④で策定した内容をもとに、導入箇所に適するソリューション、製品を検討します。製品、ソリューションについては後述します。

6. 初期導入とモニタリング

初期導入時には、適用したポリシーや初期動作の確認を含め、監視モードで運用することが推奨されます。初期導入後はしばらくシステムの動作を監視し、必要に応じて、システムの安全性を保ちつつ、業務効率を最大化するために調整を行います。

7. ゼロトラストの適用箇所拡大

運用フェーズに入ったら、ネットワークや資産の監視は継続し、トラフィックの記録を行います。これらを実施していく中で、ポリシーの変更や適用箇所の拡大を適宜実施していきます。ポリシー変更などを実施する場合は、深刻な問題にならないように行います。

ゼロトラスト導入に向けた実施手順（例）

「ゼロトラスト導入に向けた進め方」で説明したプロセスをもとに、ゼロトラストを導入するための実施手順を、例を用いて説明します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
準備工程 新たに導入する必要のあるプロセスやシステムを判断すること およびアクセスの認証・認可を正しく行うため、現在の運用状況を把握する。 a. 情報システム管理者は、次の事項を調査し、詳細に理解する。 ● 資産（デバイスやネットワークなど） ● 主体（ユーザー・権限など） b. 経営者は、次の事項を調査し、詳細に理解する。 ● ビジネスプロセス	5.9 情報及びその他の関連資産の目録 5.16 識別情報の管理 5.18 アクセス権 8.2 特権的アクセス権
① 企業のアクターを特定 a. 情報システム管理者は、業務に必要な者のみ情報へアクセスできる権限を与える。 b. アクセス権限および操作権限は、認められた場合以外は与えないようにする。	5.15 アクセス制御 5.16 識別情報の管理 5.17 認証情報 5.18 アクセス権 8.2 特権的アクセス権

	8.3 情報へのアクセス制限
② 企業が所有する資産を特定 a. デバイスを識別して管理する。 企業の情報にアクセスするデバイスは、シャドーITを含めて、すべて識別して管理する。 b. シャドーITは可能な限り資産化する。	5.9 情報及びその他の関連資産の目録 8.1 利用者終端装置
③ キープロセスの特定とプロセス実行に伴うリスクの評価 a. 業務プロセス、データフロー、組織のミッションにおける業務プロセスとデータフローの関係（プロセス）を特定する。 b. 特定したプロセスのうち、ゼロトラストに移行するプロセスを決定する。 認証・認可の判断を導入することによる失敗のリスクを考慮し、初めは組織の事業に与える影響が低いビジネスプロセスを選択し、徐々に対象を広げる。	5.29 事業の中断・阻害時の情報セキュリティ 5.30 事業継続のためのICTの備え
④ ゼロトラスト導入候補の方針策定 a. 資産、プロセスの特定後、ゼロトラストの導入により影響を受ける対象をすべて特定する。 ● 上流リソース（例：ID管理システム） ● 下流リソース（例：セキュリティ監視） ● エンティティ（例：主体ユーザー） b. ゼロトラスト導入候補となるビジネスプロセスで利用されるリソースの重要さを決定する。 c. リソースの重要さを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定する。	5.9 情報及びその他の関連資産の目録
⑤ ソリューション候補を特定 ④で策定した内容をもとに、導入箇所に適するソリューションを検討する。	5.19 供給者関係における情報セキュリティ 5.20 供給者との合意における情報セキュリティの取扱い 5.21 ICT サプライチェーンにおける情報セキュリティ

	の管理 5.22 供給者のサービス提供の監視、レビュー及び変更管理 5.23 クラウドサービスの利用における情報セキュリティ 8.21 ネットワークサービスのセキュリティ
⑥ 初期導入とモニタリング a. ソリューションの初期導入時は、実際に通信の遮断は行わず、適用したポリシーや初期動作の確認を行う。 b. 動作に問題がないことを確認後、運用を開始する。	8.16 監視活動
⑦ ゼロトラストの適用箇所拡大 a. 運用開始後は、ネットワークや資産の監視は継続しつつ、トラフィックの記録を行う。 b. トラフィックを記録していく中で、ポリシーの変更や適用箇所の拡大を適宜実施する。 c. ポリシー変更を実施する場合は、影響が問題にならないように確認する。	8.15 ログ取得 8.16 監視活動 8.32 変更管理

ゼロトラストを実装するための主な技術要素

ゼロトラストを実装するために必要となる主な技術要素（製品、ソリューション）について説明します。

CASB (Cloud Access Security Broker)
CASB とは、クラウドサービスの利活用における情報セキュリティのコンセプトですが、それを実装した製品も CASB と呼ばれます。CASB は、以下の 4 機能を備えています。 ● 可視化 ➤ クラウドストレージへの不審なアップロードやダウンロードの監視や、シャドーITの検知を行います。 ● データセキュリティ ➤ アクセス権限の逸脱や機密情報の持ち出しをチェックし、ブロックします。

- コンプライアンス
 - セキュリティに関する基準やポリシーを満たしていることを監査します。
- 脅威防御
- セキュリティ脅威の検出、分析や防御を行います。

SWG (Secure Web Gateway)

[SWG](#) は、外部ネットワークに対するすべてのアクセスを中継することで、危険なコンテンツをブロック・フィルタリングするセキュリティ製品です。物理的なアプライアンスとして提供されるものもありますが、クラウド型のソリューションが一般的です。利用者によるリスクの高い行為や許可されていない操作をブロックして、[エンドポイントデバイス](#)と社内ネットワークの安全性を保ちます。SWG の主な機能は、次の通りです。

- リスクの高い URL や IP アドレスへのアクセスの遮断
- マルウェアの検出とブロック
- アプリケーション制御

ZTNA (Zero Trust Network Access)

ZTNA は、ユーザー認証によって、特定のサービスやアプリケーションへの安全なアクセスを提供する仕組みです。[VPN](#) と異なり、ネットワーク全体へのアクセスを許可するのではなく、特定のサービスやアプリケーションのみの利用を許可します（ユーザーが許可されていないサービスなどは表示されず、利用もできません）。必要最小限の権限を付与することで、セキュリティを向上することができます。

FWaaS (Firewall as a Service)

FWaaS とは、[ファイアウォール](#)やその他ネットワークセキュリティの機能をクラウドサービスで提供するソリューションです。URL フィルタリングや [IPS](#)、アプリケーション制御の機能を持ち、セキュリティを高めます。FWaaS は、オンプレミス型のファイアウォールよりもネットワークの変更に柔軟に対応できます。

SDP (Software Defined Perimeter)

[SDP](#) の機能はほぼ ZTNA と同じで、ユーザーに特定のサービスやアプリケーションへの安全なリモートアクセスを提供します。SDP は、ネットワークの内部と外部の境界（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する技術のことです。従来のファイアウォールの概念をソフトウェア上に持ち、利用者がどこにいても動的にアクセスを制御します。

18-3-3. SASE

SASE (Secure Access Service Edge) とは、「ネットワーク機能」と「セキュリティ機能」をまとめて提供する仕組みです。「ネットワーク機能」と、接続の安全性を確保する「セキュリティ機能」をまとめて1つの製品として提供します。

SASEに含まれる主な機能に以下のものがあります。

ネットワーク機能

- SD-WAN (Software Defined - Wide Area Network)

※SD-WAN については、「18-3-4. ネットワーク制御 (Network as a Service)」で説明します。

セキュリティ機能

- SWG (Secure Web Gateway)
- CASB (Cloud Access Security Broker)
- FWaaS (Firewall as a Service)
- ZTNA (Zero Trust Network Access)

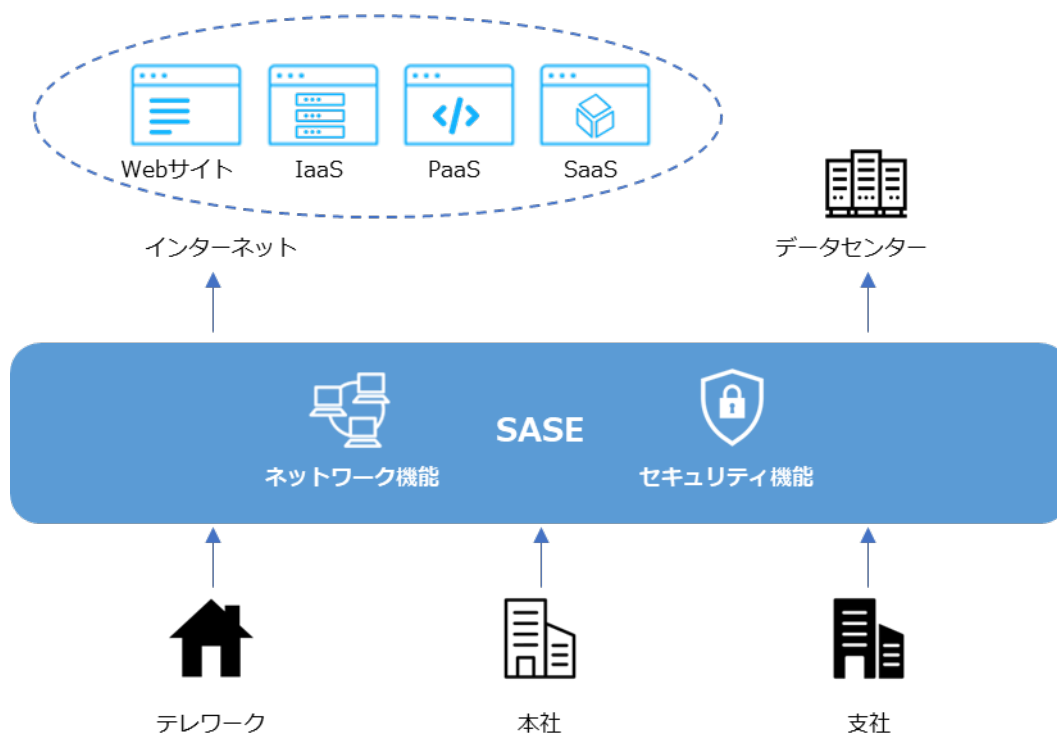


図 63. SASE のイメージ図

ゼロトラスト導入事例

概要

地方銀行は、個人顧客向けサービス以外にも、法人顧客向けサービスの充実を図っています。法人向け営業力強化方策の1つとして、営業職員にモバイル端末を配布し、場所を問わずに行内システムにアクセスを可能にすることになりました。そこで、高いセキュリティが求められる金融機関のリモートアクセス環境として、ゼロトラストネットワークアクセス機能を備えた「ZTNA」を導入しました。結果、安全で安定したリモートアクセスが可能となり、業務効率化と営業力強化を実現しました。

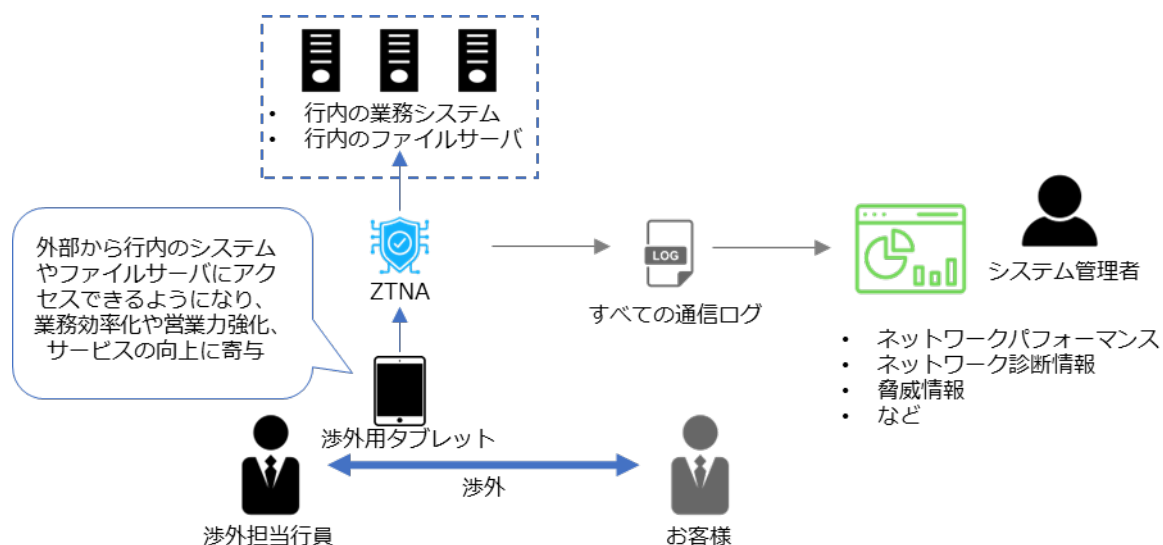


図 64. 事例のイメージ図

導入前の課題

営業力強化に向けてモバイル端末の必要性が高まり、次の課題があげられました。

- 行内だけの運用だったモバイル端末活用を、いつでもどこでも働ける環境に拡大すること。
- 渉外用タブレットは、外から行内システムやファイルサーバにアクセスできる必要があること。
- 外部でモバイル端末を利用するためには、セキュリティや性能の担保が必要であること。

選定の決め手

次の事項が導入の決め手となりました。

- リモートアクセスとセキュリティのゼロトラスト機能が一体になっていること。

- 動作検証でリモートアクセス時の速度・安定性が高いこと。

導入後の効果

導入後の効果は次の通りです。

- 営業職員が行内に戻らず業務を遂行できるようになり、業務が効率化したこと。
- 許容した内容や業務だけの通信に限定できるので、安心して使用できること。
- 今後は渉外用タブレットを活用した業務改革の推進が見込まれること。

詳細理解のため参考となる文献（参考文献）

（参考資料 1）民間企業におけるゼロトラスト導入事例

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

18-3-4. ネットワーク制御（Network as a Service）

関連する主な管理策

5.23、6.7、8.20～8.24

ネットワーク制御を説明するにあたって、クラウドサービスについて説明します。

クラウドサービスとは、サービス事業者がハードウェアの機能（サーバ、ハードディスクなど）、プラットフォームの機能（データベースやプログラム実行環境など）、ソフトウェアなどを、ネットワーク経由で利用者に提供するサービスのことです。利用者は、どの端末からでもさまざまなサービスを利用することができます。クラウドサービスの利用形態には、主に「IaaS＝アイアース」、「PaaS＝パース」、「SaaS＝サーズ」があります。また、「NaaS＝ナース」と呼ばれるネットワークインフラを提供するサービスもあります。

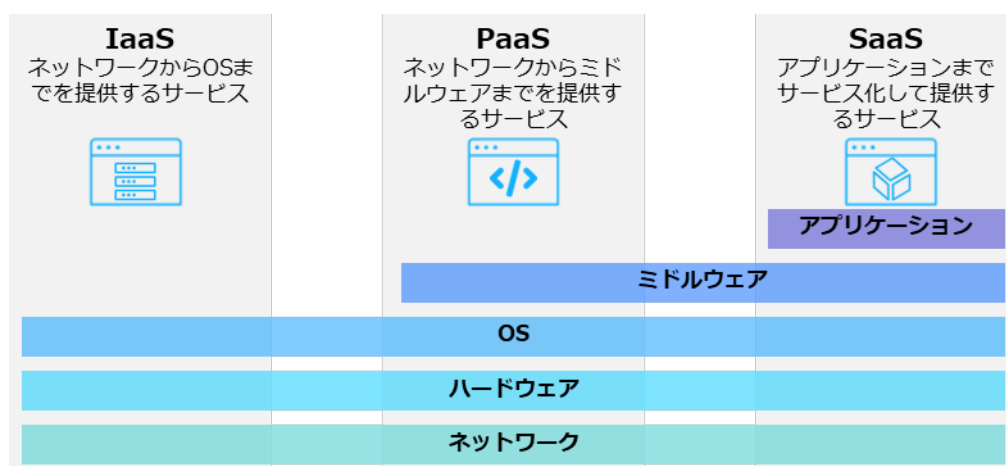


図 65. クラウドサービス利用形態の概要図

IaaS (Infrastructure as a Service)

IaaS とは、インターネット経由でネットワークやサーバ（CPU・メモリ・ストレージ）などのハードウェアやインフラ機能を提供するサービスのことです。IaaS を利用することで、従来は自社で購入、構築し、運用する必要があったハードウェアやインフラの機能を、必要なときに必要なだけ利用できます。

PaaS (Platform as a Service)

PaaS とは、インターネット経由でアプリケーションサーバやデータベースなどのアプリケーションを実行するためのプラットフォーム機能を提供するサービスのことです。PaaS を利用することで、アプリケーションの開発前段階に必要な開発環境の準備（サーバの設置や OS やミドルウェアのインストールと設定、ネットワークの設定など）を省略できます。

SaaS (Software as a Service)

SaaS とは、インターネット経由で電子メール、顧客管理、財務会計などのアプリケーションソフトの機能を提供するサービスのことです。アカウントを持っていれば、インターネット経由でどこからでもアクセスすることができたり、チームでファイルやデータを共有できたりします。

NaaS (Network as a Service)

NaaS とは、インターネット経由でネットワークインフラを提供するサービスのことです。NaaS の導入により、ネットワーク環境の変更に柔軟に対応できるようになります。NaaS に含まれる主要な機能として、SDN、SD-WAN などがあります。

SDN・SD-WAN

クラウドサービスや Web 会議、リモートワークの普及に伴い、ネットワーク回線にアクセスが集中し、通信速度が低下したり、サービスへの接続ができなくなったりするなどの問題があります。その解決策として SDN を応用した SD-WAN があります。SDN、SD-WAN について説明します。

SDN (Software Defined Networking)

SDN とは、ソフトウェアを用いてネットワーク構成を動的に変更することです。ネットワークを構成している機器（ルータやサーバ、スイッチなど）を、ソフトウェアを介して一括制御することで、機器設定やネットワーク構成を柔軟に変更できます。SDN のメリットは、ネットワーク機器に対して一括で設定を行えることです。従来のルータ、スイッチといった物理的なネットワーク機器・製品は、1 台ごとに個別に設定を行う必要があり、大規模なネットワーク構成を変更する際には、大きな作業負荷がかかりました。しかし、SDN を用いてネットワークを制御することで、

管理が 1 か所で行えるようになるため、ネットワーク機器・製品ごとに個別設定が不要になり、作業負荷が大幅に軽減できます。

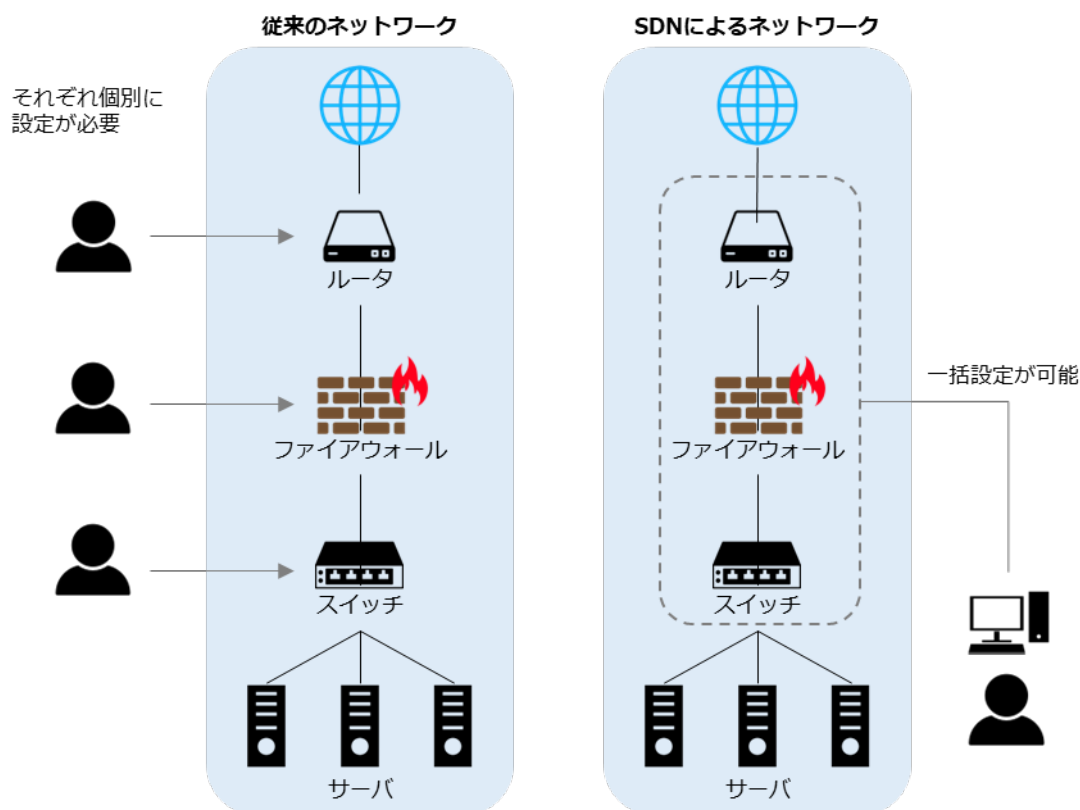


図 66. 従来のネットワークと SDN によるネットワークの比較

SD-WAN (Software Defined-Wide Area Network)

SD-WAN とは、ネットワークをソフトウェアで制御する SDN を、物理的なネットワーク機器で構築した [WAN](#) に適用する技術のことです。企業の拠点間接続や、クラウド接続などにおいて柔軟なネットワーク構成を実現したり、ネットワーク上で発生する通信を適切に制御したりすることができます。

例えば、拠点間の通信には閉域網（不特定多数のユーザーが利用するインターネットとは異なり、関係者のみが接続できる通信回線）を使用し、信頼できるクラウドサービスには直接外部インターネットへ接続するように切り替えることで、[トラフィック](#)の最適化が行えます。

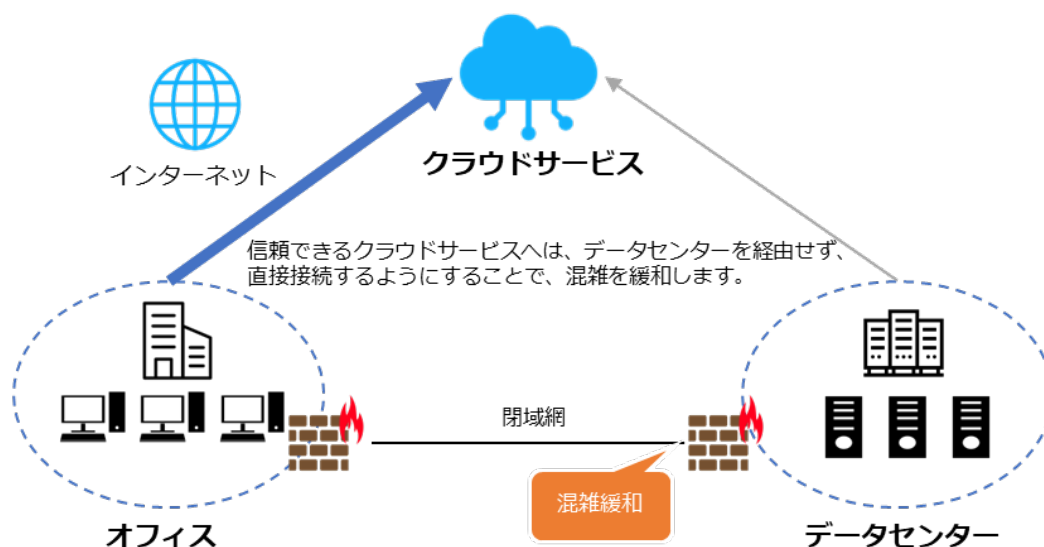


図 67. SD-WAN で実現できることの例

VPN

個人情報などの重要なデータをインターネット経由で扱う機会が増えたことや、サイバー攻撃の手口が年々巧妙化しているなどの状況を背景に、VPN が注目されています。

VPN (Virtual Private Network)

インターネット上で安全性の高い通信を実現するための手法です。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぎます。VPN を使用することで、ユーザーは物理的な専用線で通信しているかのような安全な通信を行えます。

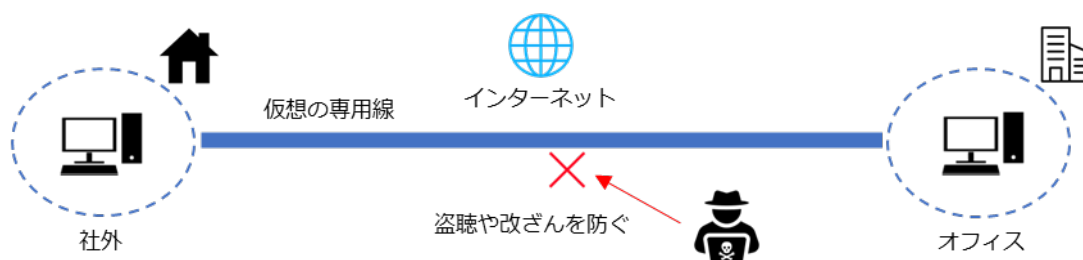


図 68. VPN の概要図

18-3-5. セキュリティ統制 (Security as a Service)

関連する主な管理策

5.1、5.9、5.15～5.18、5.23～5.28、8.1～8.5

セキュリティ統制とは、組織が情報資産を守るために採用するセキュリティ対策や仕組みになります。機密性、完全性、可用性などの情報セキュリティの目標を達成するために監視、記録を行い

統制します。

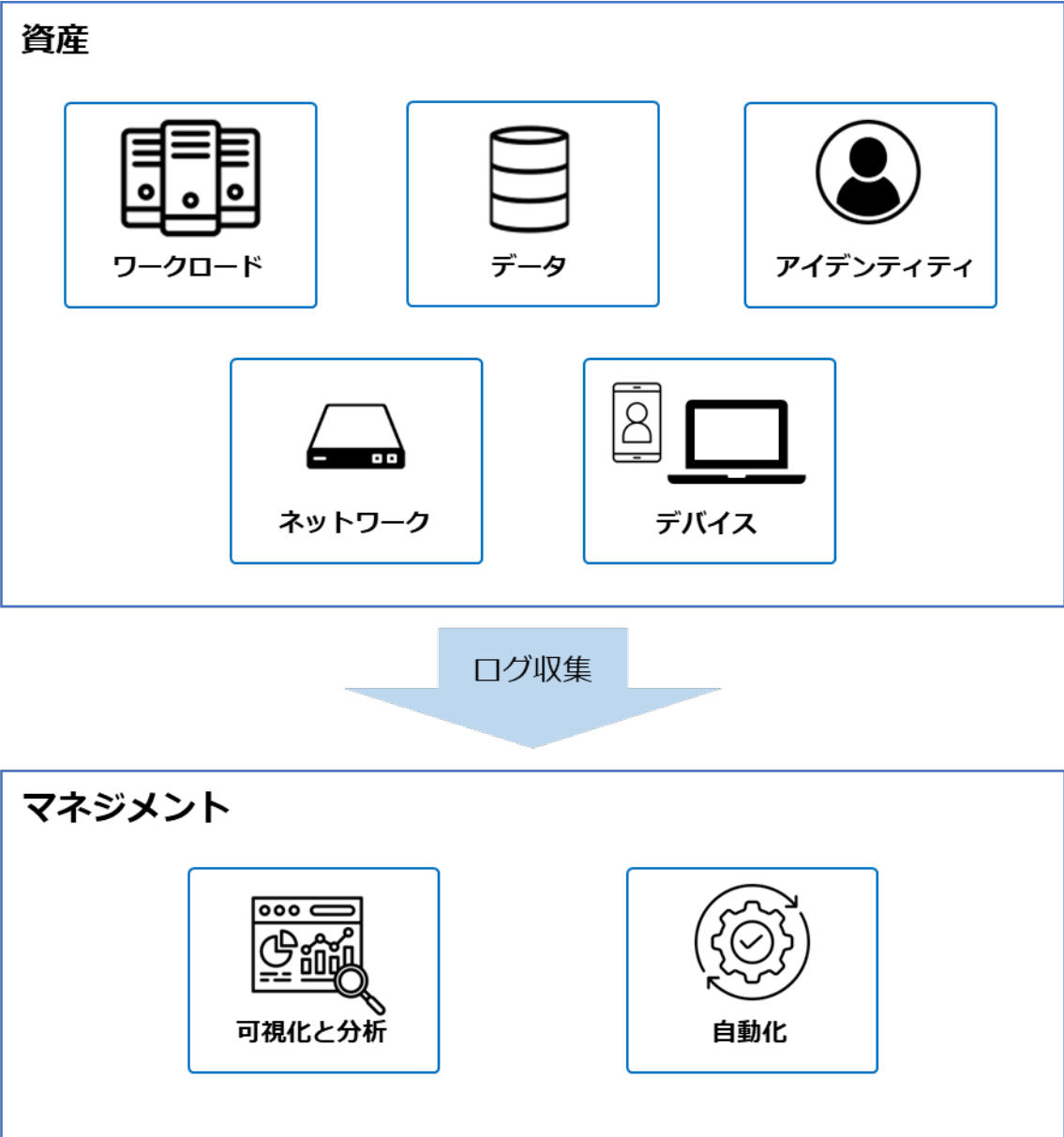


図 69. セキュリティ統制の概要図

以下は、セキュリティ統制を確立するための実施例となります。

実施内容（例）	選択すべき管理策（例）
リスク評価と分析 - 組織内の情報資産やプロセスを評価し、セキュリティリスクを特定 - リスクの重要度や影響を評価し、優先順位づけ	5.9 情報及びその他の関連資産の目録
ポリシーの策定	5.1 情報セキュリティのための

● <u>セキュリティポリシー</u>を作成し、組織内での適用範囲や要件を定義 ● ポリシーは法規制や業界のガイドラインに準拠	方針群
技術的対策の実施 ● 資産に対してセキュリティ対策の実施 ➢ ワークロード ➢ データ ➢ アイデンティティ ➢ ネットワーク ➢ デバイスなど	5.15 <u>アクセス制御</u> 5.16 識別情報の管理 5.17 認証情報 5.18 アクセス権 5.23 クラウドサービスの利用における情報セキュリティ
監視と評価 ● セキュリティ対策の効果を監視し、定期的な評価の実施 ● <u>セキュリティインシデント</u>が発生した場合は、原因を分析し、対策の改善	5.25 <u>情報セキュリティ事象</u> の評価及び決定 5.27 情報セキュリティインシデントからの学習 5.28 証拠の収集 8.15 ログ取得 8.16 監視活動
変更管理 ● システムやポリシーに変更があった場合、セキュリティに影響を与えないように変更管理プロセスを確立	8.32 変更管理
対応計画の策定 ● セキュリティインシデントが発生した場合の対応計画を策定し、迅速かつ効果的に対処	5.24 情報セキュリティインシデント管理の計画及び準備 5.26 情報セキュリティインシデントへの対応

SECaaS (Security as a Service)

SECaaS はセキュリティをサービスとして提供します。組織がセキュリティに関する機能をクラウドベースのサービスプロバイダから提供される形態で利用します。従来では、オンプレミスで利用していたセキュリティ機能をクラウド上に移行し、サブスクリプションで利用することが可能になります。

SECaaS のメリット

- コスト最適化

- スケーラビリティ
- 変化への柔軟な対応
- 冗長性
- 高い可用性
- 障害耐性

セキュリティ統制を確立するために実施することができる技術を紹介します。

ネットワークセキュリティ	
SWG (Secure Web Gateway)	Web アクセスを中継する プロキシ の一種で、危険なサイトやコンテンツへのアクセスを遮断するセキュリティ機能をクラウドサービスとして実施。
SDP (Software Defined Perimeter)	アクセス制御をソフトウェアで制御し、認証とアクセス制御を接続ごとに行うことで、動的なマイクロセグメンテーションおよびセキュアなリモートアクセスを実現。
デバイスセキュリティ	
EDR (Endpoint Detection and Response)	パソコンやサーバ、スマートフォンなどの エンドポイントデバイス に侵入したマルウェアや ランサムウェア などを検出し、通知するシステム。 マルウェア 感染後の被害拡大防止に有効。
EPP (Endpoint Protection Platform)	パソコンやサーバ、スマートフォンなどのエンドポイントデバイスへのマルウェアの侵入を防御する ソリューション 。未知のマルウェアの検知・駆除にも対応。
アイデンティティセキュリティ	
IAM (Identity and Access Management)	情報システムのユーザーID を管理・認証・認可。
FIDO (Fast Identity Online)	ID/パスワード方式に代わる認証技術。指紋や虹彩といった生体情報、公開鍵暗号、端末 ID、ワンタイムパスワードなどを利用した認証方法がある。
ワークロードセキュリティ	

CWPP (Cloud Workload Protection Platform)	クラウド上コンテナ（実行環境）や仮想マシンなどに導入し、クラウドワークロード（クラウド上で実行されるプログラムやアプリケーション）の監視と保護を行うソリューション。
データセキュリティ	
DLP (Data Loss Prevention)	情報漏えい防止を目的とするセキュリティツール。従来のシステムと異なり、データそのものを監視して情報漏えいを防ぐため、高い効果が期待できる。
可視化と分析	
CASB (Cloud Access Security Broker)	クラウドサービスの脆弱性対策ソリューション。クラウドサービスの利用状況を可視化すると同時にクラウド環境への不正アクセス検知と防御も可能。
SIEM (Security Information and Event Management)	ファイアウォールや IDS/IPS などから出力されるログやデータを一元的に集約し、集約したデータを組み合わせることで相関分析を行うことにより、サイバー攻撃やマルウェア感染などのセキュリティインシデントをリアルタイムで検知。
CSPM (Cloud Security Posture Management)	クラウド環境の設定状況を可視化し、あらかじめ設定したルールに基づいて、不適切な設定や脆弱性の有無を検知。
自動化	
SOAR (Security Orchestration Automation and Response)	セキュリティインシデントの監視、データの収集・分析、対応などのセキュリティ運用業務を自動化・効率化する技術。

FIDO (Fast Identity Online)

FIDO は、従来のパスワードによる認証方式に代わる、パスワードを使わない「パスワードレス認証」を実現する技術です。認証には、公開鍵暗号方式を利用したデジタル署名の仕組みが用いられます。

デジタル署名による送信者確認の仕組み

デジタル署名では公開鍵と秘密鍵、2つの鍵を使用します。公開鍵は公開される誰でも取得できる鍵で、秘密鍵は本人だけが保持している鍵です。秘密鍵で署名したデータは、対となる公開鍵で検証できます。この仕組みを利用し、受信者は送られてきたデータが間違いなく送信者本人から送られてきたか確認できます。



図 70. デジタル署名による送信者確認の仕組み

FIDO2

FIDO2 とは、パスワードレス認証の技術仕様です。FIDO2 では、端末で生体認証を行い、利用者を認証します。サーバとは、デジタル署名による本人確認の仕組みを用いて認証します。サーバ側には公開鍵、端末側には秘密鍵が保管され、鍵同士がペアとなります。正式サイトを偽装したフィッシングサイトがログインを求めても、ペアとなる鍵がないためログインを防げます。FIDO2 を利用したパスキーという仕組みでは、認証資格情報を複数の端末で同期できるため、機種変更や端末紛失などの場合に、一からの作成する必要はありません。

メリット

- ・ 認証に必要な秘密情報（秘密鍵）は、認証を行う端末側のみに保存され、利用する際は指紋認証や顔認証などによって本人確認を行うため、パスワードを覚える必要がありません。
- ・ パスワードや認証に必要な機密情報がインターネットに流れず、サーバ側で保存されないため、漏えいのリスクが低減されます。

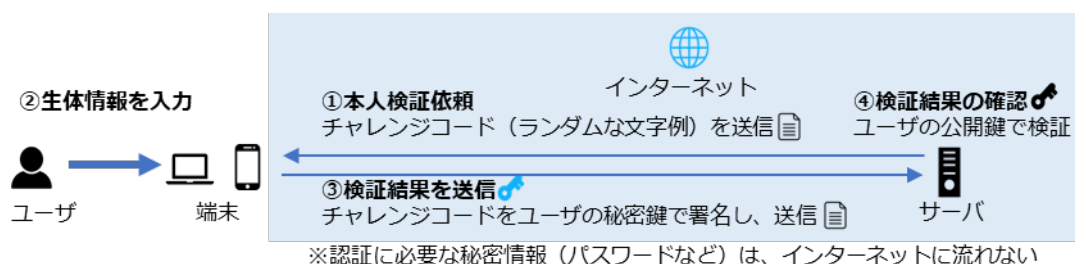


図 71. FIDO2 の仕組み

① 本人検証依頼

サーバは、ユーザーの端末に向けてチャレンジコード（ランダムな文字列）を送信します。

② 生体情報を入力

ユーザーは生体情報を入力し、端末はユーザーを認証します。

③ 検証結果を送信

ユーザーの認証に成功したら、端末はチャレンジコードをユーザーの秘密鍵で署名し、サーバへ送信します。

④ 検証結果の確認

サーバは、署名されたチャレンジコードを受け取ったら、ユーザーの公開鍵で検証します。検証に成功するとユーザーのログインを受入れ、認証完了となります。

18-4. インシデント対応

関連する主な管理策

5.5、5.6、5.24~5.28、6.8

インシデント発生時の対応

セキュリティインシデントが発生した際の基本的な対応の流れは、「第5章. 事例を知る：重大なインシデント発生から課題解決まで」で説明した「1. 検知・初動対応」、「2. 報告・公表」、「3. 復旧・再発防止」です。インシデント対応の実施手順について、ウイルス感染が起きた際の例を用いて説明します。

実施手順（例）

① 検知・ 初動対応	検知と連絡受付： ● パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるため、情報セキュリティ責任者に報告する。 ● ウイルスが添付されたメールを受け取った外部から通知を受けて発覚した場合も、情報セキュリティ責任者に報告する。 ● 内部から外部への不正な通信、外部からの意図しない通信や、一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑う。 初動対応： ● 感染したパソコンやサーバの利用を停止し、ネットワークから切り離す。
② 報告・ 公表	第二報以降・最終報： ● 影響を及ぼした取引先や顧客に対して、セキュリティインシデントに関する報告を行う。 ● ウイルス感染による影響によって、業法などで報告が求められる場合は所管の省庁へ報告する。 ● ウイルス感染やランサムウェア感染の場合は、IPAの届出窓口へ届け出る。
③ 復旧・ 再発防止	調査・対応： ● 他のパソコンやサーバがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックする。 ● ウイルス対策ソフトに従ってウイルスを駆除する。 ● ウイルス駆除ができない場合、OSのクリーンインストールを実施し、すべてのプログラムを入れ直す。

復旧：

- ウイルスの駆除が確認できたら、対象のパソコンやサーバをネットワークに接続し、復旧する。

インシデント対応の実施手順について、ウイルス感染が起きた際の例
(出典) IPA「中小企業のためのセキュリティインシデント対応の手引き」をもとに作成

詳細理解のため参考となる文献（参考文献）

中小企業のためのセキュリティインシデント対応の手引き

<https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf>

フォレンジック

インシデント対応の「復旧・再発防止」のステップでは、訴訟対応などを見越して事実関係を裏づける情報や証拠を保全し、必要に応じてフォレンジックを行います。

フォレンジックとは

フォレンジックとは、セキュリティインシデントが起きた際に、コンピュータやネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を調査・解析する技術・手法・手続きを指します。

フォレンジックを行う際の注意点

フォレンジックを行う必要がある際は、専門の調査会社に依頼する選択肢も考慮することが大切です。なぜなら、フォレンジックには専門知識が必要であり、自社で対応しようとする、証拠となるデータの収集・保全が困難になる可能性があるためです。例えば、データのコピーが客観的証拠として認められない可能性や、誤操作によるデータの破損などがあります。事前に相談する専門の調査会社を決めておくことが大切です。

セキュリティインシデント発生直後の対応についての実施手順策定

フォレンジックに関して、「証拠保全ガイドライン」が参考になります。想定読者として、「フォレンジックに関する専門知識を習得しているとは限らないが、専門事業者または捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」が含まれています。

セキュリティインシデント発生直後の初動対応についての実施手順を、例を用いて説明します。セキュリティインシデントが検知された、または発生していたことが明らかになった直後は、証拠保全を適切かつ円滑に実施するため、次の事項を実施することが大切です。

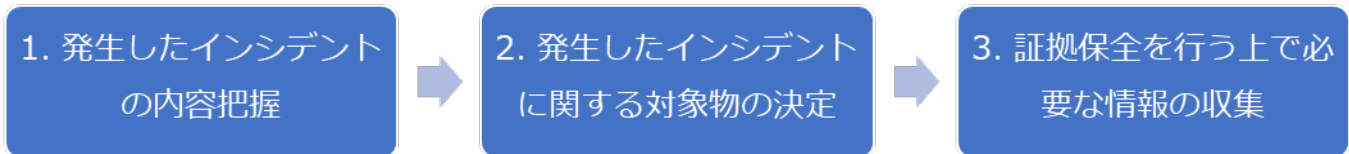


図 72. インシデント発生直後の対応の流れ

詳細理解のため参考となる文献（参考文献）	
証拠保全ガイドライン 第9版	https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf

実施手順（例）

1. 発生したインシデントの内容把握

発生したインシデントを把握します。

インシデントの種類

- 情報流出・データ破壊
- 不正アクセス、不正プログラムの実行
- 操作・設定ミスなど

検知・発覚のきっかけ

- ログのレビュー・監視
- 内部通報
- 不正検知システムなど

発生時刻

- システム時計の正確性について確認

初動対応の開始までの記録

発生したインシデントの検知・発覚から、報告または対応依頼連絡までの時間およびその間のインシデントに対する対応の有無について記録をとります。

- 発生したインシデントを知る人物および人数
- インシデント対象物の確保の有無

インシデントの対象物を確保していた場合

対象物を確保した日時、人物（役職）、場所、確保時の対象物（および周辺）に対する行

為、確保後の対象物に対する対処（の有無）とその内容を記録します。

インシデントの対象物を確保していない場合

対象物を確保する（予定の）日時と場所、確保時の対象物（およびその周辺）の状態を詳細に記録します。

2. 発生したインシデントに関する対象物の決定

対象物に対する情報収集および対象物の絞り込み

- 発生したインシデントに関する対象物の種類および個数を確認します。
 - ・ コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型）
 - ・ ネットワーク機器（ルータ、[ファイアウォール](#)、[IDS](#)、[IPS](#)）
 - ・ HDD、SSD など
- 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。
- 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。
- 発生したインシデントに関する対象物の使用者、および管理者を確認します。
- 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器、および文書の有無を確認します。

対象物の選定と優先順位づけ

- 保全を行う前の対象物（デバイス）を選定し、その理由を明確にします。
- （対象物が複数ある場合）取扱う対象物の優先順位をつけ、その理由を明確にします。

3. 証拠保全を行う上で必要な情報の収集

対象物の情報

- 対象物の形状、個数、物理的な状態を確認します。
 - ・ 対象物のラベル情報（メーカー、型番、モデル名、記憶容量など）
 - ・ ケーブルの接続状況
 - ・ 通常環境下で視認可能な物理的破損、損傷の有無など
- HDD、SSD、ストレージメディアの記憶容量、インタフェースの状況を確認します。
- セキュリティ設定の有無を確認します。
 - ・ HDD、SSD のパスワードロック
 - ・ HDD、SSD 全体[暗号化](#)または一部のファイル・フォルダの暗号化
 - ・ PC 周辺のワイヤストッパー、ロッカーなど

第19章. セキュリティ対策状況の有効性評価

章の目的

第 19 章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。

主な達成目標

- 内部監査および外部監査の重要性について理解すること

19-1. 内部監査

内部監査とは、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実施されているかをチェックすることです。セキュリティのルールを整備して日が浅いうちは、関係者がルールを理解し、遵守しながら仕事ができているかを重視して判断します。運用に慣れてきたら、設けられた社内のルールや使っている文書の内容が適切か、その有効性を判断していきます。内部監査の視点を適合性から有効性へと移していくことで、**ルールが形骸化し、目的が見失われている状態になることを防げる**でしょう。

内部監査の進め方は、「13-2-7. [ISMS](#) : 9. パフォーマンス評価」を参照してください。

19-2. 外部監査

外部監査とは、組織に所属しない外部の監査人が行う監査を指します。セキュリティの外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックすることになります。情報漏えいやサイバー攻撃などのリスクに対して、外部監査を受けることはセキュリティ対策として有効な手段の1つです。近年では取引先企業を乗っ取り、そこを踏み台にしてメインターゲットとなる企業にサイバー攻撃を仕掛ける「サプライチェーン攻撃」が頻繁に起こっており、中小企業が大企業に対する攻撃の踏み台として狙われる可能性が高まっています。

情報セキュリティ監査を受ければ、**自社のセキュリティ対策が正しく行われているか否か確認でき、不十分な点を洗い出して迅速に対処することが可能になります**。顧客や取引先に、セキュリティ対策を適切に行っていることがアピールできるので、会社や事業の規模も考慮しつつ、監査を受けることは重要です。経済産業省は、情報セキュリティの管理・監査について、2つの基準を発表しています。

管理基準・監査基準

情報セキュリティ管理基準

組織における情報セキュリティマネジメントの円滑で効果的な確立を目指し、マネジメントサイクルの構築から具体的な管理策まで、包括的な適用範囲を定めたものです。この管理基準は「マネジメント基準」と「管理策基準」の2項目から構成されています。

マネジメント基準

情報セキュリティマネジメントの計画・実行・点検・処置に必要な実施すべき事項が提示されています。

管理策基準

リスク対応方針に従って管理策を選択する際の選択肢が提示されています。

情報セキュリティ監査基準

情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。監査の品質を一定の水準に保ち、有効かつ効率的に実施できるように「一般基準」「実施基準」「報告基準」の3項目を提示しています。

一般基準

監査人としての適格性および監査業務上の遵守事項を定めています。

実施基準

監査計画の立案および監査手続きの適用方法を中心に、監査実施上の枠組みを定めています。

報告基準

監査報告にかかる留意事項と、監査報告書の記載方式を定めています。

情報セキュリティ管理基準は、JIS Q 27001 をもとに策定されています。そのため、Lv.3 網羅的アプローチを実施することで、外部監査に対応することも可能となります。

実施手順の文書化に関するポイント

実施手順を文書化する際のポイントをいくつか紹介します。

- 明確な手順と責任の割り当て
実施手順を文書化する際、手順が、誰が、いつ、どのように実施するのかを明確にすることが重要です。実施手順が適切に実施されるようにするためには、文書の各手順に関連する責任者を明記することが有効です。
- フローチャートや図の活用
文字に加えて、フローチャートや図などを用いて手順を視覚的に示すことにより、手順の流れや関係性を理解しやすくなります。また、複雑なプロセスをわかりやすく表現できるため、実施者が迷わずに手順を進められるようになります。
- 定期的なレビューと更新
実施手順は、絶えず変化する環境に適応させる必要があります。新たな脅威や法規制などへ対応させていくために、定期的なレビューや更新を行い、実施手順が常に効果的なものである状態を維持していくことが大切です。

実施手順の文書化は、組織がセキュリティ対策を行っていく上で必要です。実施手順を組織全体に浸透させ、形骸化させず有効な状態を維持するためには、責任者を明記したり、視覚的な表現を組み合わせてわかりやすい手順を記載したり、定期的にレビューしたりすることが大切です。

編集後記

第 7 編では、ISMS の管理策を参考に、対策基準・実施手順を策定する手順について解説しました。紹介した対策基準・実施手順の例は、そのまま組織に適用できるものではないため、紹介した例と ISO/IEC 27002 の内容を参考に、自社にあった対策基準・実施手順を策定していただければと思います。文書化・更新は重要ですが、本来の目標は文書化ではなく、効果的なセキュリティ対策の計画と実行にあることを忘れないようにしてください。

第 8 編では、具体的な構築・運用の実践について説明します。

第20章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）

章の目的

第 20 章では、「デジタル・ガバメント推進標準ガイドライン」などが示すサービスシステム構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践に当たっての留意点を理解することを目的とします。

主な達成目標

- 中小企業においても有効なシステム導入工程と、実践に当たっての留意点を理解すること
- システム導入工程に沿って、セキュリティ機能を実装・運用するためポイントを理解すること
- アジャイル開発の概要と実践ポイントを理解すること

20-1. セキュリティ機能の実装と運用

20-1-1. デジタル・ガバメント推進標準ガイドラインの概要

「デジタル社会推進標準ガイドライン群」は、政府向けに作成されており、政府情報システムの整備や管理に際して守るべき共通ルールが記載されています。しかし、システム導入の流れ自体は、政府だけでなく一般企業であっても参考にできます。ガイドラインを通してシステム導入の全体像を認識し、実践する際は必要に応じて取捨選択する形で留意点を把握することが効果的です。

本テキストでは、「デジタル社会推進標準ガイドライン群」におけるシステム導入工程の全体像を網羅的に記載しています。詳細については、ガイドライン本文を参照してください。

「デジタル社会推進標準ガイドライン群」の体系

デジタル社会推進標準ガイドライン群は、サービス・業務改革並びにこれらに伴う政府情報システムの整備および管理についての手続き・手順や、各種技術標準などに関する共通ルールや参考ドキュメントをまとめたものです。

各ドキュメントの位置づけには、次の2種類が存在します。

- Normative（標準ガイドライン）：政府情報システムの整備および管理に関するルールとして順守する内容を定めたドキュメント
- Informative（実践ガイドブック）：参考とするドキュメント

これまでは、「デジタル・ガバメント推進標準ガイドライン群」という名称で各種ガイドラインが策定されていました。しかし、デジタル庁として政府内部に加えて社会全体のデジタル化を推進するという観点から、これらのドキュメント体系の名称を「デジタル社会推進標準ガイドライン群」と変更しました。

主として政府内部の手続き・手順を定めたドキュメントについては、従来と同様に「デジタル・ガバメント」という名称を継続しています。

政府情報システム全般に関するドキュメント

DS-100 デジタル・ガバメント推進標準ガイドライン

ドキュメントの位置づけ：Normative

概要：サービス・業務改革とそれによって利用する政府情報システムの整備および管理についての政府の共通ルールです。手続き・手順についての基本的な方針や政府の各組織における役割などが定められています。

DS-110 デジタル・ガバメント推進標準ガイドライン解説書

ドキュメントの位置づけ：Informative

概要：政府の基本ルールである標準ガイドラインについて解説などを記載した参考文書です。標準ガイドラインの記載内容に関して、趣旨や目的などを読者が理解しやすくするために利用されます。

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

ドキュメントの位置づけ：Informative

概要：標準ガイドライン、標準ガイドライン附属文書、標準ガイドライン解説書に記載された内容に対して知識や教訓などを盛り込んだ、より実践的な参考書です。

DS-121 アジャイル開発実践ガイドブック

ドキュメントの位置づけ：Informative

概要：アジャイル開発がどのようなものかを理解するために必要な、基本的な知識をまとめた文書です。従来の開発スタイルとは別の選択肢としてアジャイル開発を設けるにあたって作成されました。

DS-130 標準ガイドライン群用語集

ドキュメントの位置づけ：Informative

概要：標準ガイドラインの用語集です。

セキュリティに関するドキュメント

DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

ドキュメントの位置づけ：Informative

概要：システムライフサイクルの各工程でのセキュリティ実施内容や要求事項を示し、関係者の役割を定義しています。

DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン～ベースラインと事業被害の組み合わせアプローチ～

ドキュメントの位置づけ：Informative

概要：DS-200「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」のセキュリティリスク分析手順の事例として具体的に示したものです。

DS-202 CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート

ドキュメントの位置づけ：Informative

概要：CI/CD（継続的インテグレーション/継続的デリバリー）パイプラインをセキュリティ観

点から解説し、保護策を検討する際のポイントについて説明しています。

DS-210 ゼロトラストアーキテクチャ適用方針

ドキュメントの位置づけ：Informative

概要：[ゼロトラスト](#)アーキテクチャを適用するための基本方針と導入時の留意点について記載しています。

DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）

ドキュメントの位置づけ：Informative

概要：ゼロトラストの環境下で政府全体のサイバーリスクを把握・低減する CRSA システムについて解説しています。

DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート

ドキュメントの位置づけ：Informative

概要：[アクセス制御](#)モデルの 1 つであり、リソースに付与された属性や環境の情報などを活用した属性ベースアクセス制御に関する俯瞰的な技術的内容を記載しています。

DS-220 政府情報システムにおけるサイバーセキュリティ[フレームワーク](#)導入に関する技術レポート

ドキュメントの位置づけ：Informative

概要：[NIST サイバーセキュリティフレームワーク](#)について解説し、政府情報システムに導入する上での要点を示しています。

DS-221 政府情報システムにおける[脆弱性診断](#)導入ガイドライン

ドキュメントの位置づけ：Informative

概要：[脆弱性診断](#)を効果的に導入するための基準およびガイダンスを記載しています。

DS-231 セキュリティ統制のカタログ化に関する技術レポート

ドキュメントの位置づけ：Informative

概要：セキュリティ統制のカタログ化（独立したセキュリティ管理策に対し一意な識別子を付与し、機械可読形式で分類すること）に関する概要について説明します。

クラウドサービスに関するドキュメント

DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針

ドキュメントの位置づけ：Normative

概要：政府情報システムのシステム方式について、クラウドサービスの採用を第一候補とし、適切に利用するための考え方などを示しています。

データ連携に関するドキュメント

DS-400 政府相互運用性フレームワーク（GIF）

ドキュメントの位置づけ：Informative

概要：GIF（Government Interoperability Framework）は、デジタル庁が公開するデータの連携・交換のためのデータ参照モデルです。

トラストに関するドキュメント

DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン

ドキュメントの位置づけ：Normative

概要：各種行政手続きをデジタル化する際に必要となる、オンラインによる本人確認の手法を示しています。

DS-531 処分通知等のデジタル化に係る基本的な考え方

ドキュメントの位置づけ：Informative

概要：処分通知などのデジタル化を短期的に推進するため、実務で参考にできるよう共通的な考え方や課題への対応方法などを提供します。

その他ドキュメント

DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い

ドキュメントの位置づけ：Normative

概要：安全保障などの機微な情報などを扱う情報システムについて、注意が必要とされるリスクとその対応策、クラウドサービス化の検討、データ連携における留意点など、利用者が検討すべき観点をまとめています。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-110 デジタル・ガバメント推進標準ガイドライン解説書	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9462b2d8/20240605_resources_standard_guidelines_guideline_03.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
DS-121 アジャイル開発実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf
DS-130 標準ガイドライン群用語集	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/83a1ac09/20230331_resources_standard_guidelines_glossary_03.pdf
DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf
DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1b65a1dc/20230411_resources_standard_guidelines_guideline_01.pdf

DS-202 CI/CD パイプラインにおけるセキュリティの留意点に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/33f31336/20240329_resources_standard_guidelines_guideline_01.pdf
DS-210 ゼロトラストアーキテクチャ適用方針	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf
DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ef841b43/20240131_resources_standard_guidelines_guidelines_03.pdf
DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/e5b49450/20230411_resources_standard_guidelines_guideline_03.pdf
DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf
DS-221 政府情報システムにおける脆弱性診断導入ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7f9c9ee/20240206_resources_standard_guidelines_guidelines_01.pdf
DS-231 セキュリティ統制のカタログ化に関する技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9f746654/20230411_resources_standard_guidelines_guideline_07.pdf
DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf
DS-400 政府相互運用性フレームワーク（GIF）	https://github.com/JDA-DM/GIF
DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf
DS-531 処分通知等のデジタル化に係る基本的な考え方	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d92a1cf2/20230411_resources_standard_guidelines_guideline_09.pdf
DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/4d3bf58a/20230719_resources_standard_guidelines_guideline_01.pdf

デジタル・ガバメント推進標準ガイドライン

「デジタル・ガバメント推進標準ガイドライン」は、「デジタル社会推進標準ガイドライン群」における、「政府情報システム全般に関するドキュメント」の標準ガイドラインとして位置づけられています。

「デジタル・ガバメント推進標準ガイドライン」におけるシステム導入工程の全体像は以下の通りです。

プロジェクトの管理

利用者が実感できる効果を目標に設定し、達成に向けて機能するプロジェクト体制を作ります。また、プロジェクト管理を行うチームや担当者（PJMO）自身のモニタリングの結果により、抜本的改善のプロセスに入る場合もあります。

1. プロジェクトの立ち上げ、初動
2. プロジェクト計画書などの作成
3. プロジェクトのモニタリング
4. プロジェクトの終結

予算および執行

予算のための稟議に必要となる主要資料（年間スケジュールなど）を関係者に示し、わかりやすい構成となるように「全体から詳細につながる」資料作成をします。また、コスト削減、見積りの精査を行い適切に執行します。

1. 予算のための稟議の事前準備

2. 予算のための稟議に必要な資料の準備
3. 見積り依頼
4. 見積りの精査
5. 予算を要求する
6. 予算のための稟議後の対応

サービス・業務企画

サービス設計 12 箇条の内容に基づいて、[ペルソナ分析](#)や[ジャーニーマップ](#)といった手法により利用者の立場からサービス・業務の分析を行います。（サービス設計 12 箇条、ペルソナ分析、ジャーニーマップなどについては「サービスデザイン実践ガイドブック」を参照してください）

参考：サービス設計 12 箇条

- [1]利用者のニーズから出発する
- [2]事実を詳細に把握する
- [3]エンドツーエンドで考える
- [4]すべての関係者に気を配る
- [5]サービスはシンプルにする
- [6]デジタル技術を徹底的に活用する
- [7]利用者の日常体験に溶け込む
- [8]自分で作りすぎない
- [9]オープンにサービスを作る
- [10]何度も繰り返す
- [11]一遍にやらず、一貫してやる
- [12]情報システムではなくサービスを作る

1. サービス・業務企画の開始準備
2. 利用者視点でのニーズ把握
3. 業務の現状把握
4. サービス・業務企画内容の検討
5. 軌道修正
6. 新しい業務要件の定義

要件定義

[RFI](#)（Request For Information）や事業者からの情報収集を通して、市場にあるサービス、海外や国内の類似事例、新たな技術の動向や製品のライフサイクル、概算の予算規模、スケジュー

ールなどについて把握を行った上で、機能要件と非機能要件を明確にします。

1. 要件定義の事前準備
2. RFI の実施
3. 要件定義の全体像
4. 機能要件の定義
5. 非機能要件の定義
6. 要件定義終了後の対応

調達

全体機能実現のために、どのような単位に分けて調達するかを調達仕様書の作成を通じて明確化します。調達仕様書には、調達目的、作業内容と納品物、実施体制や発注者としての役割について考え方や注意点を記載します。また、総合評価落札方式では評価点の配分、留意点、事業者から WBS として示される作業内容の精査ポイントを明確化し、事業者の提案を評価します。

1. 調達の事前準備
2. 調達仕様書の作成
3. 調達仕様書以外のドキュメント作成
4. 調達手続きとプロジェクト管理
5. 検収

設計・開発

良い情報システムを作るために、発注者自身が要件を事業者に正しく伝え、関係者間の調整を行い、進捗状況を正しく把握し、情報システムの出来具合をテストする必要があります。設計・開発において発注者自身が実施する業務内容と移行、リハーサル、運用・保守の準備、マニュアルなど、について計画の立て方、ドキュメントの作成方法、注意点について理解し実施します。

1. 設計・開発を開始するための事前準備
2. 設計・開発の計画
3. 設計・開発・テストの管理
4. 見落としがちな活動に注意
5. 新業務の運営を円滑に行うための準備

サービス・業務の運営と改善

外部委託を活用する際の役割分担のコツを理解した上で、サービス・業務の運営を行います。また、蓄積されたさまざまな情報の分析を通してサービスや業務を改善します。

1. 新しいサービス・業務の事前準備
2. 業務の定着と次の備え

3. 業務の改善

運用および保守

情報システムの安定的な稼動を維持することに加え、利用者へのサービスを継続的に改善し、運用コストを低減していくために、運用および保守で実施する代表的な作業項目、会議体の種類と目的、定例会議での報告内容に対する注意点、変更管理、ログなどの蓄積、指標管理、運用業務の改善方法など、従業員が主体的に運用・保守業務を管理するための具体的な知識や技術を確認します。

1. 運用・保守を開始するための事前準備
2. 運用・保守の計画
3. 運用・保守の定着と次への備え
4. 運用・保守の改善と業務の引継ぎ

システム監査

各プロジェクトの取組がその目標達成に正しく向かっているのか、プロジェクトの各フェーズでの実施プロセスは適切かといった観点から、現状を調査し、改善すべき点がないかを第三者の視点で客観的に点検・評価します。

1. システム監査の理解
2. システム監査計画と監査実施計画
3. システム監査の実施
4. 指摘事項を踏まえた改善

「デジタル・ガバメント推進標準ガイドライン」は、さまざまなプロジェクトで発生する多様な状況に対して正確に実施すべき内容を伝えるという性格を持つ文書のため、正確さを優先して記載されています。一方「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」は、読みやすさや実用性を重視しています。

詳細理解のため参考となる文献（参考文献）	
デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

20-1-2. プロジェクトの管理

プロジェクト管理活動全体の流れは以下の通りです。

プロジェクト管理活動の全体の流れ

プロジェクトの立ち上げ、初動

プロジェクトの初動とは、プロジェクトが生み出され、スタートを切ろうとしている際のタイ

ミングです。出だしていくつかの内容を理解し、行動しておくことで、プロジェクトの手戻りを大きく減らせます。

1. 目標とする成果を見定める

- A. 現場で発生している事実をつかんだ上で今後の目標を定める
- B. 上位計画の目標をブレイクダウンし、プロジェクト目標と紐づける

現場で発生している事実をつかんだ上で今後の目標を定めることが重要です。

2. 手段の妥当性を確認する

プロジェクトの立ち上げに当たり、プロジェクトの目標とする成果を定め、その成果を得るための手段が妥当であることを確認します。

3. プロジェクトの投資対効果を算出する

情報システム整備は、利用者の利便性向上・負担軽減などの効果を得ることを目的としているため、投資対効果をしっかりと精査・評価することが重要です。

4. プロジェクトへの投資判断を行う

プロジェクトへの投資判断は、プロジェクトの目標とする成果を明確にした上で、その成果を得るために必要となる経費や人的資源などを見積り、その費用対効果を踏まえた上でプロジェクトを開始することを責任者が意思決定することです。

5. 機能する体制を作る

- A. 制度所管部門、業務実施部門などを含めた [PJMO](#) 体制とする
- B. プロジェクトの規模に見合った体制を組む
- C. 他組織と連携できる体制を作る
- D. 先行経験を持つ人の技術や知識を活用する

プロジェクトの円滑な運営を行うためには、プロジェクトの初期に十分な体制を構築することが重要です。

プロジェクト計画書などの作成

プロジェクトには必ず定めるべき事項が存在します。プロジェクトスタート時点で決められるもの、プロジェクトが進むにつれて具体化されるもの、状況に応じて内容を見直すものなど、さまざまな情報で成り立ちますが、すべてはプロジェクト計画書に記載され、関係者にて共有される必要があります。

1. プロジェクト計画書を作成する

A. プロジェクト計画書は段階的に詳細化する

B. 抜け漏れのない実施計画を作成する

プロジェクト計画書は、最初からすべての計画の詳細を記載するものではありません。初期の段階のプロジェクト計画書は、各項目についての概要を記載した上で、各項目の詳細化を行うタイミングを計画します。実施計画を作成する際には、PJMO が責任範囲を持つ部分のみで計画を立てがちですが、影響を受ける側（業務担当従業員、連携先システム、移行元の既存システムなど）も含めた全体的な計画が必要です。

2. プロジェクト管理要領を作成する

A. 問題に対処できる会議体を構成する

B. 本質的なリスクを事前に予見して、対応を準備する

C. 品質管理を事業者任せにしない

プロジェクト管理要領はその「実施に係るルール」を定義するものです。問題が発生したときだけ相談する形では情報共有が不十分になりがちなので、常日頃からプロジェクトの計画内容、進捗状況、重要課題を関係者が把握できるように進めていく必要があります。

プロジェクトのモニタリング

プロジェクト全体が意図した方向に進んでいるか、包括的な視点で確認するために PJMO 自身によって定期的にモニタリングを行います。

1. プロジェクトをモニタリングし、検証する

A. 目標、経費、進捗、品質などを中心にモニタリングする

B. モニタリングは適時に実施する

C. モニタリングと監査をうまく組み合わせる

D. プロジェクトは状況に応じて停止・改善する

プロジェクトの終結

プロジェクトの実施期間が 10 年を超えるものも珍しくありませんが、期間の長短に関わらずスタートしたプロジェクトはいずれ終わりを迎えます。プロジェクトの終結は、これまでの活動を振り返り、活動の評価を行うことにより、新たなプロジェクトへの糧となる重要なプロセスです。

1. プロジェクトの終結を処理する

A. プロジェクトを完了する

B. プロジェクトを終了する

C. 後続プロジェクトを策定する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

「プロジェクトの立ち上げ、初動」における、プロジェクトの目標設定

新しいプロジェクトを開始する際には、現場における業務の実態と課題を網羅的に把握した上で今後の目標を定めることが大切です。プロジェクトには投資が伴います。投資を行ってまで得たい成果が何なのか。それを具体的な形で明確にすることが重要です。

(例) FAX と電話で受けていた注文業務を、IT を用いてサービス改善するためのプロジェクトにおける目標設定

プロジェクト目標が安易に設定された例（悪い例）

電子注文の実現	課題：顧客が FAX または電話で注文する必要がある 目標：電子注文を実現し、FAX または電話での連絡を不要とする
KPI	指標：電子注文利用率 60% (XX 年度)

プロジェクトの目標設定例（良い例）

受領連絡までの時間短縮	課題：週末の注文受領連絡が週明けになる 目標：(例外を除き) 受領連絡を 12 時間以内に行う
大量注文への対応	課題：FAX は記入内容が多く、電話では話す内容が多い 目標：注文書の簡易化 大量注文向けのデータ一括申請を導入
顧客確認の不要化	課題：注文受領時に顧客台帳から顧客確認が必要なため、注文時に電話番号などによる確認が必要 目標：システム連携により、顧客確認が不要
KPI	受領連絡発信を含む注文完了を 12 時間以内順守率 80% (XX 年度) 100% (XX+2 年度)

<目標設定のポイント>

- 顧客が困っていること（受領連絡までの時間）への対応を優先
- 顧客や注文内容の異なりを捉え、個々のニーズへ対応（大量注文）
- 顧客目線で事前、事後の作業も改善（顧客確認）

- 小さく始める。そして、軌道修正しながら最終目標へ到達する（段階的な [KPI](#)）

悪い例では、目標設定に当たって抜け落ちている観点があります。

誰が何に困っているのか

原点に立ち返り、現場で発生していることをよく見るのが大切です。

顧客は本当に困っているのか、困っている場合は具体的に何に困っているのか確認することが重要です。現場に行き、実際の現場で発生していることを調べると、例えば以下の状況に気づけます。

- 注文受領連絡が遅い
- 大量注文時の作業が煩雑
- 注文のたびに起こる顧客確認

FAX や電話をかけなければならないことよりも、さらに深刻に困っていることがわかります。電子注文を進めることに加えて、他にも対策を打つべきことがあると考えられます。

「顧客は FAX や電話をする手間に困っている」というストーリーは、推測に基づくものでした。現場を知らない人による推測のみで目標を設定するのではなく、現場の流れ、顧客の状況を調べて、本当の「困っていること」を把握することが最初の第一歩です。

顧客の種類

顧客とは誰なのか把握することが重要です。例では、「顧客」という 1 つの言葉で表現していましたが、顧客の中にもさまざまな種類の顧客がいる可能性があります。

- 既存顧客か新規顧客か

注文するのは取引実績のある既存顧客か、初めて取引する新規顧客かを把握することが大切です。新規顧客の場合は、支払い方法・配送先の確認や契約手続きなど、必要書類や事務手続きが異なる可能性があります。

- 配送先が一つか複数か

企業などの法人が注文を行っている場合は、店舗ごとに注文するのではなく、ある程度まとめて一括で注文を行っているかもしれません。

大量の注文を行っている企業は、店舗ごとに FAX 用の注文書を自動出力できるように独自の情報システムを整備済みかもしれません。この場合、拙速に電子注文を進めても、FAX での注文の方が便利であるため、電子注文が使われない可能性があります。

重要なことは、「困っていること」が異なるグループがあれば、個々のグループについて、それぞれの困りごとを把握することです。また、独自の情報システムを整備済みの企業の例のよう

に、「困っていない」グループを把握することも重要です。

例における「顧客」のような、複数のグループを包括する名詞には注意が必要です。ひとまとめに顧客像を捉えてしまうと、特定のグループが困っていることを見落としてしまうおそれがあります。

注文内容の種類

注文内容にもさまざまな種類があります。例えば注文の種類ごとに、確認の内容や必要時間を調べていくと以下のことがわかります。

- 形式的な内容確認のみを行うもの（大部分の注文）

「いつもの商品をいつもの数」注文される場合です。必須記載事項が正しく記載されているかなど形式的な確認のみを行うものが、注文件数の大部分を占めていました。さらに実態を調べていくと、実質的な確認に要する時間は僅かであり、各部門を流れていく際の待ち時間が長いことがわかりました。また、注文を受領した際の確認が十分でなく顧客へ再問い合わせを行うなど、再確認作業にも相当の手間が発生していることがわかりました。

- 受付け担当者が詳細な確認作業を行うもの（一部の注文）

一部の注文については、受付け担当者が詳細な確認作業を行っています。例えば、新規顧客の場合は「支払い方法」「配送先」などを含む初回購入手続きが必要です。他にも、いつもとは違う商品やいつもとは異なる数量の注文と思われる場合には、担当者が確認作業を行ってきました。しかし、上述の形式的な内容確認も同一の担当者が実施しているため、確認に十分な時間が割けない場合があることもわかりました。

エンドツーエンドの視野で、他に問題はないか

業務実施部門の視点で見ると、窓口で申請を受付け、審査を行うという業務は所管業務の重要な一要素です。一方、顧客が注文の事前、事後で作業を行っていることについては、業務実施部門の「担当外」として意識されないことがあります。

しかし、顧客の視点で見ると、事前、事後に必要な作業も同様に重要なプロセスです。そこに、困りごとは発生していないか確認することが大切です。

- 顧客が注文を行う前に必要となる作業

必要物品（購入品目・数量）の取りまとめ、取扱い商品の確認、希望配送日時の確認など

- 顧客が注文受領連絡を受けた後に必要となる作業

配送日時の確認、必要に応じて各店舗への連絡、代金の入金など

顧客視点を重視して現場で発生していることを調べていくと、解決すべき課題にさまざまな種類があることがわかります。

「KGI」「CSF」「KPI」の定義と関係

- 重要目標達成指標（KGI：Key Goal Indicator）
政策目標など、プロジェクトの最終目標を達成するために管理すべき指標
- 重要成功要因（CSF：Critical Success Factor）
KGI を達成する（成功させる）上で重要となる要因
- 重要成果指標（KPI：Key Performance Indicator）
プロジェクトを推進し、新しいサービス・業務を実現することで重要目標達成指標を達成するために管理すべき指標

例：資格試験の合格

資格試験に合格するために勉強するという場面を想定して、具体例を紹介します。

資格試験の合格（例：試験で 70 点以上取得）が KGI となります。

この KGI を達成するための CSF は、「十分な勉強時間を確保すること」（リソースの確保）や、自分の周りでこの資格をすでに取得している人や、この資格の分野に詳しい人を見つけて質問できるようにしておき、「わからないことがあっても解決できるようにすること」（協力体制の確立）、「周りから邪魔されずに集中して勉強できる環境を確保すること」（阻害要因の排除）などが挙げられます。CSF は、これらが揃えば確かに成功（目標を達成）しそうだと思える要因であることが大切です。

KPI は、「1 週間当たりの勉強時間：10 時間以上」、仕事が忙しくて勉強できないということがないように「1 週間当たりの残業時間：5 時間未満」などといった指標を設定します。KPI は、これらが達成されれば CSF（ここでは「十分な勉強時間を確保すること」）が実現できたといえるような指標を設定します。

「プロジェクト管理」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第 3 編 第 2 章 プロジェクトの管理 Step2 プロジェクトの立ち上げ、初動

セキュリティ機能を実装・運用するためポイント

プロジェクトを進める中で発生しやすいリスクとその対応方法について、例を示します。

多数の事業者間をまたいだシステム障害が発生するリスクへの対応

多数の事業者が参画する体制（マルチベンダー体制）においてシステム障害が発生した際に、

各事業者が自身の責任範囲ではないことを主張し、問題を主体的に解決する主体が存在しないことによって、原因究明や対応実施が長期化するというリスク

→リスクを軽減するためには、プロジェクト全体を統括する品質管理チームをプロジェクト管理を行うチームや担当従業員と特定事業者によって構成するなどの対応が考えられます。プロジェクト内でシステム障害などの問題が発生した際には、この品質管理チームが問題解決を統括し、複数事業者をまたがる問題についても問題の切り分けと問題対応者（事業者）の決定を行います。また、各事業者が品質管理チームの指示にしたがって必要な対応を行うことをプロジェクトのルールとしても明示します。

個人情報などの重要情報が漏えいするリスク

個人情報などの重要情報について、本来は参照権限がない利用者が参照してしまったり、外部へ流出してしまったりといった漏えいが発生するリスク

→本番稼動前の段階においてリスクを軽減するためには、情報セキュリティの専門経験を持つ要員がセキュリティ設計を行い、要件定義で定めた情報セキュリティ対策要件の充足性を確認します。また、実作業の中でも本番データを扱うテストにおいて、氏名などの重要情報をマスキング（匿名化）した形で実施するなど、万一の情報流出時にも影響範囲を限定化する対応を行います。

→本番稼動後の段階においてリスクを軽減するためには、運用計画や運用実施要領などの中で重要情報を扱う際の手順を明確に示した上で、実際の実施状況について定期的に確認することや、セキュリティ監査の実施計画を立てて監査の実施とフォローアップを行うなどの対応を行います。

20-1-3. 予算および執行

政府機関における予算活動全体の流れは以下の通りです。

予算活動の全体の流れ

予算のための稟議（予算要求）の事前準備

稟議の直前に作業が集中したり、手戻り作業が発生したりしないように準備を行います。

1. 予算のための稟議を計画的に実施する

- A. 予算のための稟議の年間スケジュールを把握する
- B. 予算のための稟議に向けた作業のポイント

予算のための稟議・編成作業は、各段階において作業の締切り日が厳格に定められているの

で、いつ頃の作業を行うかを意識し、計画を立てて、十分な時間と期間を確保して進めます。

2. 予算のための稟議の対象範囲を早期に決める

- A. プロジェクト計画書を再確認する
- B. 予算のための稟議から漏れがちな項目を理解する
- C. 関係者と役割分担は早期に確認

プロジェクト計画書には、予算のための稟議の対象となる活動が、プロジェクト全体でどう位置づけられ、何を達成し、何の条件を守らないといけないかが書かれています。プロジェクト計画書の内容を理解した上で作業を進めることで、予算のための稟議の内容が具体的になり、第三者にも理解しやすいものとなります。

3. コスト削減の検討

- A. ハードウェア・ソフトウェアのコスト削減観点
- B. アプリケーションのコスト削減観点
- C. 運用業務のコスト削減観点
- D. そのほかのコスト削減観点

見積り依頼

情報システムの見積りには、専門的で見慣れない表現や内容が含まれることがあります。情報システムの見積りの特性を理解した上で、どのように見積り依頼を行えばよい情報を入手できるか理解することが重要です。

1. 見積り依頼書の作成

- A. 要件が未確定な部分を明確にする
- B. プロジェクトの状況によって内訳粒度を変える
- C. 見積りフォーマットを指定する
- D. 工程の名称の違いをなくす
- E. 見積り手法に注意する
- F. できるだけ詳細な要件を書く

2. 事業者への見積り依頼

- A. 見積りしてくれる事業者を探す
- B. 見積り事業者と対話して、発注者の意図を正しく伝える

見積りの精査

見積り金額は、過少でも過大でも問題です。必要十分な金額水準とするために、事業者から受け取った見積りに対して内容の過不足を見つけ、より精度を高めるための作業を実施します。

1. 人件費の見積り精査

- A. 安易な掛け算の精査
- B. 作業重複の精査
- C. 主要成果物との比較
- D. 開発生産性の精査

2. ハードウェアなどの見積り精査

- A. 製品単価を精査する
- B. 高額な製品を中心に、必要性を精査し他製品と比較する
- C. ソフトウェアライセンスを精査する
- D. 保守量を精査する

ハードウェア、ソフトウェアの借料や保守経費は、経費全体の中で大きな比率を占めます。まずは、大前提として製品単位での価格内訳を入手することが大切です。

3. 複数事業者の見積りの比較

予算のための稟議（予算要求）に必要な資料の準備

必要な経費を正確に把握するために事業者に見積りを依頼します。自社のやりたいこと・見積ってほしいことをまとめて伝えるために、見積り依頼資料を提示します。

1. 全体像と要点の明確化

2. 予算のための稟議の資料の作成上の注意点

- A. 「予算のための稟議の概要」の作成ポイント
- B. 「サービス・業務の説明資料」の作成ポイント

概算要求に向けた調整

組織内外の予算のための稟議の関係者に対して、予算の内容、必要性、金額妥当性などの説明を行うことが不可欠です。

- A. [PMO](#) による調整
- B. デジタル庁による調整

予算執行について

予算のための稟議が通ってからがプロジェクトの実質的な始まりです。プロジェクトの実務を計画的に進めるための準備作業を早めから実施します。

1. 執行計画案の作成

予算が決定された後、PJMO は「いつの時期」に「何の調達案件」を「いくら使う」のかについて、記載した 1 年間の執行計画案を作成します。

2. 執行計画案の調整

予算決定以後に生じた事情により、執行計画の内容を変更せざるを得ない場合は、PMO は PJMO から内容を聴取し、必要に応じて資料を徴求するなどして、変更内容が妥当か否か確認し、変更の是非を判断します。また、変更により予算を超過せざるを得ない場合には、プロジェクト間での調整を行うことになります。

3. 予算の移替え・予算執行管理

A. 予算の移替え

B. 予算執行管理

年度途中で事情変更により追加の移替えが必要となる場合には、PMO はデジタル庁に執行計画の変更を行った上で、追加された予算の移替えを受けることになります。PMO は移替えられた予算の範囲内で、各 PJMO が適切に執行しているかについて、予算執行管理を行います。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たったの留意点を説明します。

予算のための稟議に必要な資料の準備

予算のための稟議の過程では、短期間で多くの関係者に対してプロジェクトの目標や予算の必要性などを理解してもらう必要があるため、要点をわかりやすく表現することが求められます。わかりやすい資料を作成することで、事業者からも有意義な提案を受けて的確な見積りを取得できます。

【全体像と要点の明確化】

プロジェクトの内容を第三者に正確に伝えるためには、「全体」から「詳細」につながる構成で説明することが重要です。始めに、サービスや業務の全体を俯瞰した視点を示し、目標を明らかにします。その上で、その中で今回のプロジェクトがどの範囲なのか、今回の予算のための稟議の対象がどの範囲なのかと順を追ってクローズアップしていく構成にすることで、資料の読み手に対して正確にプロジェクトの姿と予算の必要性を伝えられます。

資料の読み手は、予算提案の内容を確認する担当者（PMO、デジタル庁、財務省主計局）だけではなく、PJMO 内部の従業員、利用者や関係者などのステークホルダー、見積り依頼先の事業者なども重要な読み手です。読み手によっては、関心のポイントが異なる部分もあります。しかし、どの読み手も共通して知りたいことは、サービスや業務の全体像です。プロジェクトの前提を間違えて捉えると、的確な判断ができないからです。

サービスや業務の全体像がわかる資料をわかりやすく整理するとともに、プロジェクトの進捗や変化に応じて資料内容をバージョンアップする活動を日常的に行うことで、予算提案に限らず、さまざまな状況でプロジェクトの状況説明を円滑かつ効率的に行えるようになります。

「予算のための稟議」に関する概要作成ポイント

予算のための稟議に関する概要は、プロジェクト計画書の内容を前提に、予算提案を行う範囲についての目標、内容、スケジュール、体制などを要約した資料です。この資料は、予算のための稟議の過程の中で、さまざまな関係者が真っ先に確認する資料となります。

作成時に気をつける点	
全体像と目標の明確化	サービス・業務観点からの全体像と現時点の問題発生状況を明らかにした上で、プロジェクトの目的・目標を示し、サービス・業務の改善後の実現像を示す。
具体的な改善内容の明確化	サービス・業務の改善内容、制度や業務ルール of 改善内容、情報システムの改善内容を明確にする。（情報システムの改善だけの目線にならないように留意する）
主要なスケジュールの明確化	全体スケジュールを作成し、新しいサービス・業務の開始時期を明示するとともに、情報システムの主要な整備スケジュール（要件定義、調達、設計、開発、テストなど）、関連する制度変更のスケジュール、サービス・業務の変更のための手続きなどを明確にする。
体制とステークホルダーの明確化	プロジェクトの体制や、主要なステークホルダーへの影響有無を記述する。また、難易度の高い調整が発生する場合に、今後の調整方法（各ステークホルダーへの調査やヒアリングを通して詳細な分析を行う、ステークホルダーの責任者を集めた会議体を設置するなど）を明らかにする。
前提条件や制約の明確化	プロジェクトを推進する上での前提条件や制約がある場合は、その主要なものについて記述する。また、前提条件や方針などに不明確な箇所がある場合は、この資料にまとめて記述する（業務の説明資料、情報システムの説明資料などの個々の資料にも記載した上で、この資料

	にまとめる)。
費用対効果の考え方の明確化	情報システムの整備により得られる効果を明確にする。「効果」については、恩恵を受ける対象ごとに適切に設定されている必要がある。 また、このような効果はいつまでにどのように把握するのか明確になっていることが重要である。さらに、累積効果がプロジェクト期間全体の投資額（予算のための稟議の経費の総額）を上回るまでの回収期間について明確にする。

「サービス・業務の説明資料」の作成ポイント

サービス・業務の説明資料は、プロジェクトが前提としているサービス・業務の概要を説明する資料です。サービス・業務企画での詳細な検討成果を、予算査定に係るさまざまな関係者にわかりやすく伝えるため、業務自体の概要、業務全体を示す業務フロー（概略）を1枚から数枚程度で簡潔に説明した資料を作成します。

作成時に気をつける点

- 業務（情報のやり取り）が発生する主体を明確化し、矢印などを使ってやり取りする内容を明確にする
- 管理指標と現在の達成状況について、定量的に記述する
- 顕在化している課題を記述する
- 異なる主体であっても業務や取り扱う情報などに共通点がある場合には、一括して記述するなど、図が難解にならないようにする

例として、ECサイトを運営している中小企業を対象とした業務フロー図を紹介します。

業務概要図（サンプル）

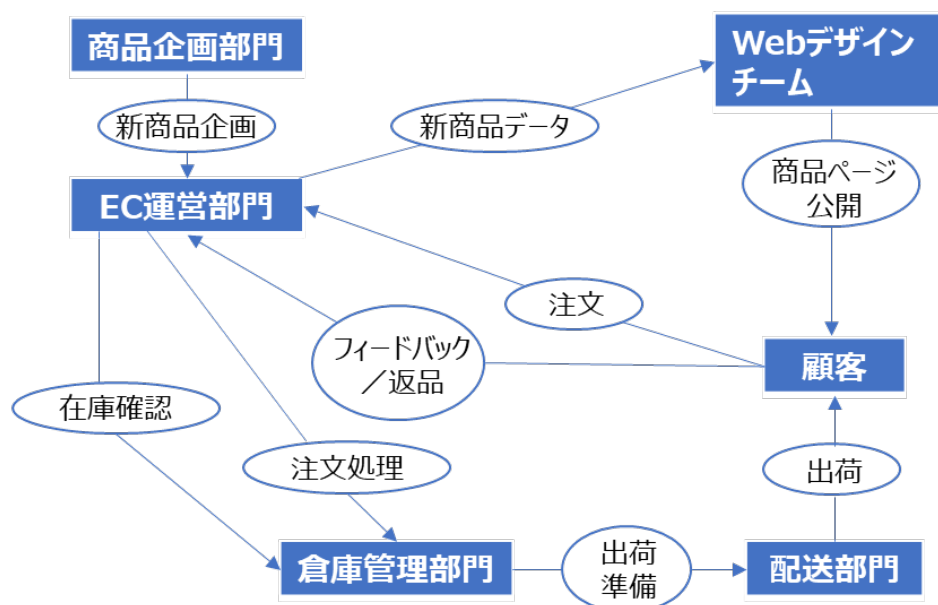


図 73. 業務概要図の例

見積りの精査

情報システムの開発や運用などを委託する事業者は、情報システムを運営していくためのパートナーなため、良好な関係を維持することは重要です。良好な関係とは、業務の一切を事業者任せにする状態ではありません。適切な役割分担の下で、緊張感を持って協働することが良好な関係です。

このことは、事業者が提示する見積りの精査についても当てはまります。発注者側である従業員が見積り内容を十分に理解し、前提条件や取り得る選択肢を理解した上で、実現機能と価格のバランスをとることが求められます。見積り金額を減らせば良いというものでもありません。必要不可欠な項目が抜け落ちてしまうと、システム開発や運用の段階で大きな問題になります。

見積りの精査は、実際には簡単ではありません。ハードウェア、ソフトウェアの見積りには専門的知識がないとわからない横文字が列挙されています。人件費の工数積み上げについても、どのような観点で確認すべきか難しいです。

見積り金額を適切な範囲に収めるとともに、発注者側・事業者側の双方がこの先の工程で円滑に活動ができるために、見積りを精査することが重要です。

One Point

生成 AI 活用による工数削減について

昨今、情報システム開発に生成 AI を活用する事例が増えています。生成 AI の利用で、従来よりも工数を削減できる可能性があります。

- コードの自動生成と補完

開発者が自然言語で指示を出すだけで生成 AI がコードを自動生成するため、手動で書く手間を減らせます。また、未完成のコードを AI が補完してくれるため、コーディングの時間を短縮できます。

- バグ検出と修正

AI はソースコードを自動的にレビューし、潜在的なバグを検出し、修正案を提示します。これにより、開発者はバグ探しや修正作業にかかる時間を短縮できます。

- テストの自動化

テストコードの生成やテストの自動実行も AI によってサポートされるため、手動でのテスト作業に費やす時間を短縮できます。

- ドキュメント生成

ソースコードから自動的にドキュメントを生成する機能により、開発者がドキュメント作成に割く時間を短縮できます。

注意点として、生成 AI の利用によって脆弱なコードが混入する可能性が増加するという指摘もあります。そのため、生成されたコードはしっかりとレビューする必要があります。

人件費の見積り精査

人件費は、工数（「人月」や「人日」）と単価の掛け算で算出できます。

例：4 人体制で 15 日間の作業=60 人日（3 人月）。

人日と人月の換算は、営業日ベースで計算するため、20 人日を 1 人月とすることが標準的です。

【留意点】

- 工数内訳を詳細に確認することが大切です。

見積りの中で、数十人月といった大きな単位で一式としての工数が示される場合、その中にはさまざまな作業が混在して合算されているため、個々の作業工数の妥当性を判断することができません。

- 工数の内訳は、機能や作業単位で分けることが非常に重要です。

数十人月といった大規模作業を、工程単位（設計、開発、試験など）、期間単位（月ごとの工数など）、要員種別単位（プロジェクトマネージャ（PM）、システムエンジニア（SE）、プログラマ（PG））で分けて、一見すると詳細な内訳として提示されることがあります。しかし、このような分け方ではこれ以上精査することが困難です。

- 個々の経費項目について必要性や生産性水準について精査できるようにするためには、実現する機能単位、実際に発生する作業単位での詳細工数が明記された見積りが不可欠です。

このような見積りが提示されていない場合は、事業者に対して見積り精査上の必要性を伝えた

上で、必要な粒度での工数見積りを取得しましょう。

ハードウェアなどの見積り精査

ハードウェア、ソフトウェアの借料や保守経費は、経費全体の中で大きな比率を占めます。

【留意点】

- 大前提として製品単位での価格内訳を入手することが大切です。
予算のための稟議の段階では、「一式」などの形で大括りの見積りが事業者から提示されることがあります。しかし一式の状態では、それ以上に金額の精査が行えません。新規に整備する情報システムであっても、想定する製品に基づいて金額を積算しているはずなので、内容を確認すべきです。また、既存情報システムに対する改修や更改などの案件であれば、なおさら詳細な積算内訳を求めることが重要です。

複数事業者の見積りの比較

複数事業者から見積りを取得した場合は、その内容について比較を行います。

【留意点】

- 比較に際しては、合計金額だけで比較するのではなく、主要な経費項目の単位で比較を行うことで事業者の得意分野、不得意分野などを把握することができます。

One Point

三点見積りによる適正予算の算出

三点見積りとは、例えば5つの事業者から見積りを取得した際に、最高額と最低額を除外した3者で平均して算出した額を指します。見積り経費項目ごとに三点見積りを行い、総合計したものを適正予算額とします。三点見積りは、金額だけではなく工数や期間の算出にも適用できます。

「予算および執行」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第3章 予算および執行 Step.5 予算要求に必要な資料の準備

セキュリティ機能を実装・運用するためポイント

情報システムを構成する製品のサポート終了に付随する経費の考慮

情報システムを構築する際に、主要な作業経費（設計・開発経費やハードウェア関連経費など）が漏れることはまずありません。しかし、付随する作業経費については予算のための稟議の時点で漏れる可能性があります。

情報システムを構成するハードウェア、ソフトウェアなどの製品には、製品供給元からのサポートサービスの提供期限が定められていることが一般的です。特に、各種ソフトウェア（OS、ブラウザ、アプリケーションサーバ用のミドルウェア、データベースサーバ用のミドルウェアなど）については、バージョン別に細かくサポートポリシーが設定されており、注意が必要です。サポートが切れた製品の利用を継続すると、当該製品に対するセキュリティ脆弱性などの問題が発生した際に製品供給元からの対応が行われない可能性があります。そのため、原則として、サポートが終了するまでに後継製品を導入するなどの対応をとることが重要です。

人事異動時の引継ぎ不足を防ぐこと

プロジェクト推進責任者など、プロジェクトの中心となる従業員が人事異動で離れる際、後任者がプロジェクトを円滑に引継げないことで問題になることがあります。これを防ぐために、予算のための稟議などの作業は複数人のグループで行い、常に情報共有することが大切です。異動する従業員は、まず後任の従業員ではなくグループのメンバーへ引継ぐことにより、引継ぐ情報量が少なく済み、円滑に引継ぎができます。1名でプロジェクトを担当する場合は、後任者のために資料をしっかりと作成し、引継ぎを行うことが重要です。



事例：引継ぎ不足により、後日問題が顕在化した

監査を実施した結果、新たに機器・ソフトウェアなどを購入しなければ情報セキュリティ対策ができないことが判明しました。その結果が判明した後、担当者が人事異動で交替しましたが、新たな情報セキュリティ対策用の予算を確保しなければならないことについて、引継ぎが十分に行われていませんでした。

1年後、情報漏えい事案が発生し、原因究明や報道対応を含めたさまざまな対応業務が大量に必要となりました。このとき、監査結果を反映した情報セキュリティ対策が講じられていれば、情報漏えい事案が発生しなかった可能性が高いことが判明しました。しかし、予算担当、会計課、PMOにおいても監査結果から新たな情報セキュリティ対策が必要なこと、そして予算のための稟議が必要だったことを誰も知りませんでした。

20-1-4. サービス・業務企画

サービス・業務企画活動全体の流れは以下の通りです。

サービス・業務企画の全体の流れ

サービス・業務企画の開始準備

サービス・業務企画を開始する前に、今のサービスや業務の現状をよく調べます。誰が何に困っているのか、背景にどのような事象が発生しているのか、事実を正確に把握します。

1. サービスデザイン思考を理解する

A. 心構えと視点（サービス設計 12 箇条）を理解する

利用者視点でのニーズ把握

利用者視点でのニーズを把握するためには、まずどのような利用者が存在するかを把握した上で、利用者の立場に立ってサービスの現状を考えることが重要です。

1. 利用者のことを知る

A. どんな利用者がいるかを調べる

B. 利用者の人数を把握する

「どのような利用者が」「どこに」「どれくらい」いるのか、その利用者は「何のために」「どのように行動し」「何を求めて」いるのかを事実に基づいて把握し、情報を整理していきます。

2. 利用者のニーズを理解する

A. 利用者のニーズから出発する

B. エンドツーエンドで考える

現場を知らない人の推測のみで目標を設定するのではなく、現場の流れ、利用者の状況を調べて、利用者の本当のニーズを把握します。

業務の現状把握

何かを変えようとするときには、まず今がどうなっているかを正確に把握することから始めることが重要です。しかし、むやみに情報をかき集めても、整理しきれず、重要な情報の抜け漏れを招くおそれがあります。現状のサービス内容や業務内容を調査する方法を理解することが重要です。

1. 業務を観察する

A. 事実を詳細に把握する

B. 推測ではなく、現場で発生している事実をみる

C. 1 力所だけの現場分析結果を全体に拡張しない

D. 日常的に業務の課題を収集し、分析に利用する

業務を観察する際には、先入観を持たずに観察することが大切です。細かな粒度で 1 つ 1 つの事実を徹底的に把握していくことで、今までに気づいていなかったものが見えてきます。実際に発生している事実に基づいて問題が可視化し、その問題に対して因果関係の整理を行った上

で具体的な改善策を打つことができます。

2. 実績データを分析する

- A. 平均、合計ではなく、ばらつきを見る
- B. 時間と期間を区別して滞留状況をつかむ
- C. 業務量のピークを捉え、ピークの発生原因を把握する
- D. 問い合わせや要望は、根本原因が同じになる粒度まで分類する

ばらつきを見ると、時間帯や曜日によって利用方法にピーク特性があるなどの実情が見えてきます。また、業務の滞留箇所を探ることで業務処理の中のボトルネックを可視化できます。さらに、実際に発生している事象を確認し、ピークの発生原因を理解することで、業務量のピークを抑えることが可能です。問い合わせ・要望についても詳細な分類をすることで、問い合わせ発生数を時系列で把握できるという点で、業務・サービス改革のために有効な分析が行えます。

3. 業務を可視化する

- A. さまざまな立場の人が理解できる業務フローを作成する
- B. 業務ルールや業務実施方法をまとめる
- C. 入出力情報や管理対象情報をまとめる

業務の分析結果は多くのドキュメントになることがあり、分析した人は内容を理解していても、初めて読む人にとってはポイントを把握するのが難しいです。プロジェクト内部や外部の関係者など多くの人が業務の分析結果を確認する必要があるため、業務フローなどを使って誰にでもわかりやすく可視化した資料を作成することが重要です。

サービス・業務企画内容の検討

現状の業務・システムを調査した結果をもとに、課題を把握し分析します。

1. 課題を整理し、分析する

- A. 優先順位・影響度・費用対効果による分析

課題を原因ごとにグルーピングした後は、それらの課題を利用者への影響度や費用対効果をもとに優先順位づけし、主要課題を抽出していきます。

2. 企画案を作成する

- A. すべての関係者に気を配る
- B. 利用者の日常体験に溶け込む
- C. 縦割り組織にやわらかく横串を刺す
- D. 必要に応じて制度自体を見直す

- E. システムを作る前に、業務を標準化する
- F. 将来の業務フローには、効果を紐づける
- G. 精緻に効果を積算し、主要な効果を実感可能なものとする
- H. オープンにサービスを作る
- I. 企画案を客観的に見直してみる

サービスはさまざまな関係者によって成り立っています。利用者だけでなく、すべての関係者についてどのような影響が発生するかを分析し、企画案を作成する際には既存の活動の中で完結できる方策を検討します。企画に関わる各所とは時間をかけて調整を進めることで、円滑に進められるよう配慮することが必要です。システムを作る前には業務を標準化し、また、システムの効果について業務フローに紐づけることで目指す姿をわかりやすくできます。

軌道修正

プロジェクトの方針は、把握した情報に応じてより良いものに見直されるべきものです。

1. 軌道修正しやすい進め方にする

- A. 一遍にやらず、一貫してやる

開発段階でプロトタイプを作って利用者によるテストを行ったり、本番運用も一度に行うのではなく一部の利用者を対象に実証実験を行ってから本格的に展開したりするなど段階的に整備することによって、利用者の声を取り入れながら軌道修正を積み重ねることができます。

2. 柔軟に軌道修正する

- A. 何度も繰り返す
- B. 無理に継続しない

プロジェクト初期に想定したサービス・業務企画の前提となる課題や仮説が、現状調査の結果と異なっていると判明した場合は、プロジェクト計画全体の軌道修正の検討が必要です。試行的にサービスの提供や業務を実施し、利用者や関係者からのフィードバックを踏まえてサービスの見直しを行うなど、何度も確認と改善のプロセスを繰り返しながら品質を向上させます。また、費用対効果に乏しいと判明したプロジェクトについては無理に継続せず、中止を含めた検討をすることが大切です。

新しい業務要件の定義

「利用者視点でのニーズ把握」「業務の現状把握」で把握した現状をベースに、「サービス・業務企画内容の見当」「軌道修正」で検討した次の業務・システムの方向性に則り、次の新しい業務に関する要件を定めていきます。

- 1. 業務要件をまとめる
- 2. 定義内容を関係者に共有する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：業務の現状把握

実際に発生しているさまざまな事象をしっかりと観察し、把握することが重要です。現状を正しく把握せずにサービス・業務企画を行うと、見た目としては新しいサービスが実現できたように見えても、実際にはサービスが使われなかったり、業務上大きな問題が発生したりするなど、さまざまなトラブルが発生する危険性があります。

事実を詳細に把握するということは、サービス・企画のプロセス全般を通じて根底となる重要な姿勢です。

【事実把握時の留意点】

- 事実把握には「平均や合計ではなく、ばらつきを見る」「推測ではなく、現場の事実を確認する」といった考え方があります。あまりにも当然のことですが、今までに数多くのプロジェクトでトラブルが発生したり、失敗に終わってしまった原因を辿ると、最初の企画時点で事実を詳細に把握できていなかったことに帰結する例が本当に多いです。
- 細かな粒度で事実を徹底的に把握することで、今まで気づいていなかった問題が見えてきます。実際に発生している事実に基づいて問題が可視化されれば、因果関係を整理し、具体的な改善策が導き出せます。問題が可視化されないと、思い込みや仮説に基づいた業務設計となり、問題を解決できません。
- 経験豊富な人ほど、先入観で事実を見過ごしてしまうことがあります。現場を観察し、業務で発生する実データを確認しながら、何が起きているかを先入観なく調べるのが大切です。

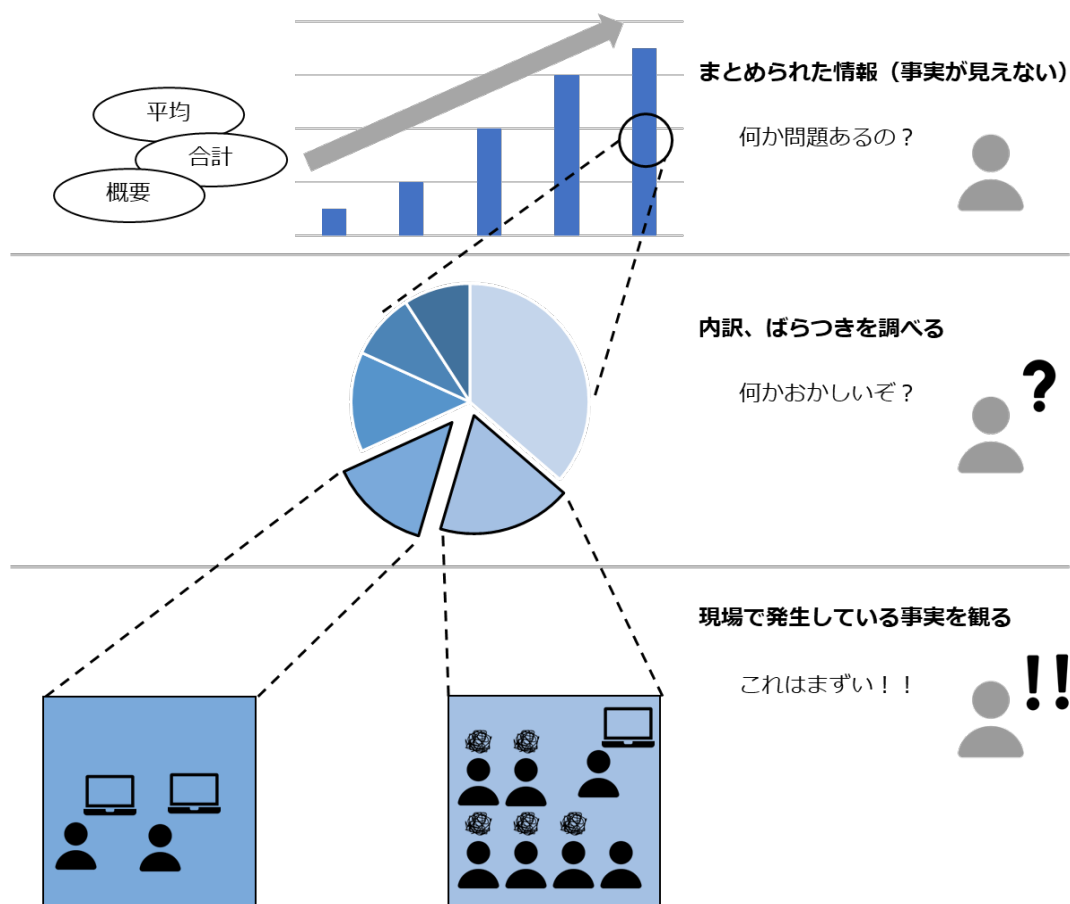


図 74. 事実を詳細に把握するイメージ図

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「サービス・業務企画」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第4章 サービス・業務企画 Step3 利用者視点でのニーズ把握

第3編 第4章 サービス・業務企画 Step4 業務の現状把握

第3編 第4章 サービス・業務企画 Step5 サービス・業務企画内容の検討

セキュリティ機能を実装・運用するためポイント

デジタル技術を徹底的に活用する

デジタル技術は日々進化しています。今までは手間をかけなければできなかったことが、デジタル技術を活用することで効率的に実施できる可能性があります。情報セキュリティとプライバシーを確保する観点からも、IT マネジメント全体を通してリスク管理を適切に行い、情報セキュリティ対策を確実に行うデジタル技術の活用が重要です。

20-1-5. 要件定義

要件定義の活動全体の流れは以下の通りです。

要件定義の全体の流れ

要件定義の事前準備

要件定義を開始するに当たって、まずは、目標、対象範囲、サービス・業務企画の方向性など、実施計画などを把握し、プロジェクトとして達成すべきゴールを把握します。

1. 要件定義で従業員が得た知識は貴重な財産

要件定義を行うことで、サービス・業務の企画内容、情報システムの要件に係る背景、決定経緯、理由、従業員の長年の経験や勘に基づく知識が収集されます。これはプロジェクトを進める上で貴重な財産となります。担当者が異動する場合は、これらの知識がなくならないように十分な引継ぎが必要です。

2. プロジェクト計画や業務要件を把握する

要件定義を開始するに当たっては、目的、目標、対象範囲、サービス・業務企画の方向性など、実施計画などからプロジェクトとして達成すべきゴールを確認し、サービス・業務から見た情報システムに対する要求を理解する必要があります。

RFI の実施

RFI (Request For Information) は、情報システムに関するさまざまな情報を収集するために事業者などに対して、構築しようと考えている情報システムに関わる、技術的な情報や動向、参考事例の提供を依頼する活動です。

要件定義では、RFI などの情報収集を行うことにより、さまざまな情報を複数の事業者から収集し、情報システム構築の方向性や実現性、適用可能な技術などの情報を把握できます。

1. RFI を理解し、必要な資料を準備する

A. RFI の意義と用途を理解する

B. RFI に必要な資料を準備する

2. 公平性を確保したヒアリングを行う

3. 収集した情報をもとに資料を更新する

A. RFI や発注前ヒアリングの結果を整理する

B. 既存の資料を最新化する

要件定義の全体像

要件定義では、業務要件、機能要件、非機能要件で定めた各項目の内容を定義します。

1. 構成要素を把握し要件を定義する
2. 機能の優先順位は改善後の業務で判断する
3. 一貫性を持った論理的な記載とする
4. 要件定義書は継続的にメンテナンスする

機能要件の定義

機能要件を具体的に検討し、ドキュメント化します。

1. 個々の領域について要件を定める
 - A. 機能に関する事項
 - B. 画面に関する事項
 - C. 帳票に関する事項
 - D. データに関する事項
 - E. 外部インターフェースに関する事項
2. 必要な機能を漏れなく抽出し検討する
3. 実現手段ではなく、求める結果を記載する

新しい非機能要件の定義

すでに定められた業務要件に基づき、業務要件を満たすために情報システムの非機能に求められる要件を定義していきます。

1. 個々の領域について要件を定める
 - A. ユーザビリティおよびアクセシビリティに関する事項
 - B. システム方式に関する事項
 - C. 規模に関する事項
 - D. 性能に関する事項
 - E. 信頼性に関する事項
 - F. 拡張性に関する事項
 - G. 上位互換性に関する事項
 - H. 中立性に関する事項
 - I. 継続性に関する事項

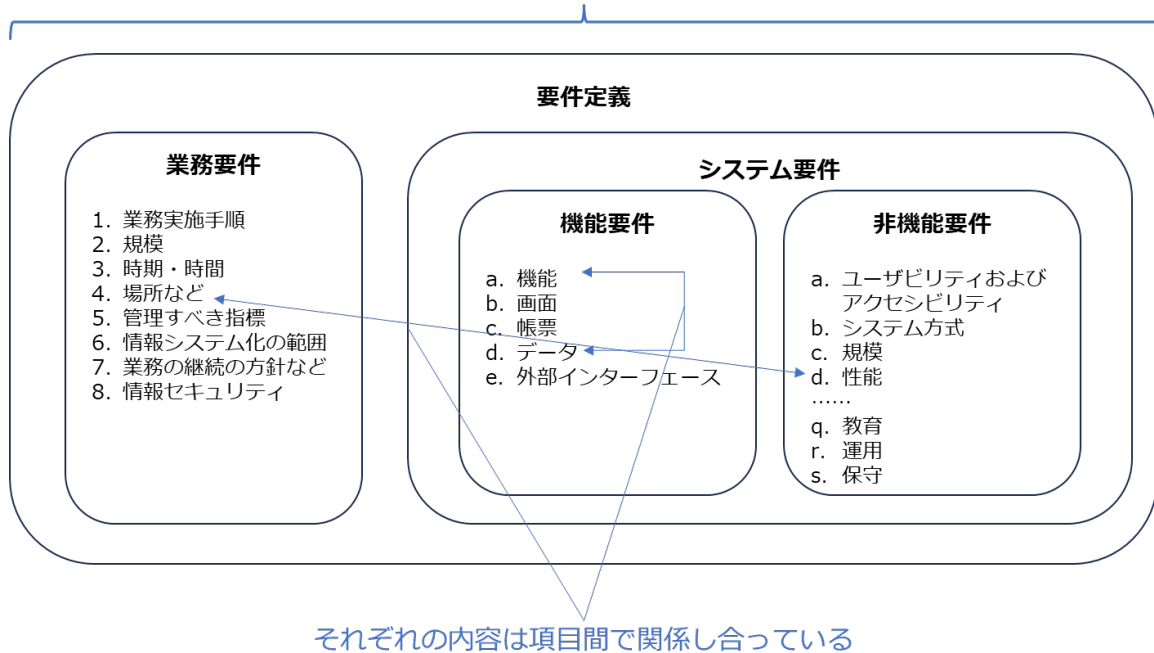
J. 情報セキュリティに関する事項 K. 情報システム稼動環境に関する事項 L. テストに関する事項 M. 移行に関する事項 N. 引継ぎに関する事項 O. 教育に関する事項 P. 運用に関する事項 Q. 保守に関する事項
2. システム方式を決定する
要件定義終了後の対応
関係者へ要件定義内容の共有などを実施します。 1. 定義内容を関係者に共有する 2. プロジェクト計画書に反映して最新化する

要件定義の全体像

要件定義は、業務要件、機能要件、非機能要件で構成されています。各要件には多数の項目が定義されており、それぞれの内容は項目間で影響し合っています。

要件定義の内容は定義する項目が多数あるため、詳細を検討していく中で、どこかで同じ内容を検討していないか、本当に漏れがないか、と不安になることがあります。まずは、要件定義の構造と定義する項目を俯瞰し、要件の上位に当たる、政策目的・実現する目標、達成すべきプロジェクト目標に沿って、何をどこで定義するのか、それぞれの項目がどのように関連しているかを理解することが大切です。要件定義は、各項目の整合性を逐次とりながら定義することで、無駄なく、漏れなく、効率的に検討していくことができます。

これらがすべて揃って要件が網羅的に定義できる



それぞれの内容は項目間で関係し合っている

図 75. 要件定義の構成要素とポイント

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

要件定義を作成する時点では、すべての項目をしっかりと定義することが難しい場合があります。未確定の項目は、後の工程で定義されることとなります。このときに関連する項目に変更がある場合があるため、関連する項目の変更漏れがないように、未確定項目の関係性がわかるようにしておくことが大切です。

定義書が一通り作成された後、以下の観点による最終確認を行うことで、定義漏れを防ぐことができます。

要件定義内容を確認する観点	解説
必要性	政策目的・目標の実現やプロジェクト目標達成への貢献といった有効性の観点および費用対効果の観点を踏まえ、実現すべき機能要件および非機能要件のみが定義されていること。
網羅性	業務要件が漏れなく定義され、その実現のために備えるべき機能要件および非機能要件が漏れなく定義されていること。
具体性	機能要件および非機能要件を実現する複雑さ、難易度、調達コストに影響する不確定要素が可能な限り排除されていること。
定量性	業務および情報システムの規模などが定量的に示され、性能

	などに関する計測可能な指標と具体的な目標値が設定されていること。
整合性	業務要件、機能要件、非機能要件の内容に矛盾がないこと。また、関連する他のプロジェクトの要件定義内容と整合的であること。
中立性	調達コストの削減、透明性向上などを図るため、要件定義内容が特定事業者に不必要に依存したものでないこと。
役割分担の明確性	業務の実施体制が明確であること。また、情報システムのテスト、移行、引継ぎ、運用、保守に関して、関係各所なども含め、自組織と事業者との役割分担が明確であること。
情報セキュリティ	自組織の情報 セキュリティポリシー を順守するために必要な対策が漏れなく定義されていること。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

要件定義プロセスにおける Fit&Gap 分析

情報システム構築においてパッケージソフトウェアや SaaS を利用する場合は、Fit&Gap 分析が必要になります。Fit&Gap 分析とは、導入するパッケージソフトウェアや SaaS などのシステムと、自社の業務要件との適合性を評価する手法です。導入するパッケージソフトウェアや SaaS などのシステムが、どの程度自社の業務要件が満たすか（Fit）、満たされない部分はどの程度あるか（Gap）を明確にします。

Fit&Gap 分析が重要な理由

パッケージソフトウェアや SaaS は、特定の業務ニーズに対応するために設計された汎用的なソリューションです。これらの[ソリューション](#)が、自社の業務要件に完全に適合することは稀であるためです。パッケージソフトウェアや SaaS には標準的な機能が備わっているものの、自社が求めるすべての機能が含まれているわけではありません。Fit&Gap 分析を通じて、自社の業務要件に適合している部分（Fit）と、適合していない部分（Gap）を明確にすることが必要です。ギャップがある場合は、対応方針を検討します。（例えば、パッケージソフトウェアや SaaS をカスタマイズする、別のソリューションを検討するなど）それにより、自社に最適なパッケージ製品の選定や、必要なカスタマイズの範囲が明確になります。Fit&Gap 分析を適切に行うことで、システム導入後のリスクやコストを最小化できます。

Fit&Gap 分析の具体的な手順例：

1. 業務要件の整理

まず、自社の業務要件を整理し、どのような機能やプロセスが必要かをリストアップします。これには、現在の業務プロセスや将来的なニーズも含まれます。

2. パッケージソフトウェアや SaaS の機能確認

導入予定のソフトウェアが提供する標準機能を確認します。製品のドキュメントやデモを通じて、どの機能が自社の要件に対応しているかを評価します。

3. フィット部分の特定 (Fit)

ソフトウェアが業務要件をそのまま満たしている部分を確認します。この部分はカスタマイズなしでそのまま導入可能で、導入コストやリスクが低いです。

4. ギャップ部分の特定 (Gap)

ソフトウェアが業務要件を満たしていない部分（ギャップ）を特定します。これらのギャップが大きい場合、以下のような対応が必要です：

- カスタマイズ：ソフトウェアを自社要件に合わせてカスタマイズする。
- プロセス変更：業務プロセスをソフトウェアに合わせて変更する。
- 追加ツールの導入：足りない機能を補うために別のツールやシステムを導入する。

5. コストとリスクの評価

ギャップ部分の解決にかかるコストやリスクを評価します。カスタマイズやプロセス変更には時間や費用がかかるため、その影響を検討します。

Fit&Gap 分析における考慮事項：

● 標準機能の活用

可能であれば、カスタマイズを避け、標準機能を最大限活用することで、コストや運用の複雑さを抑えることが推奨されます。また、製品やサービスにおけるバージョンアップの観点から（セキュリティの観点からも）安易なカスタマイズを避け、できる限り業務プロセスをパッケージソフトウェアや SaaS に合わせることを推奨されます。

● 長期的視点での検討

将来的なバージョンアップや運用コストも含め、長期的な視点で Fit&Gap 分析を行うことが重要です。

● 業務プロセスの柔軟性

ソフトウェアに合わせた業務プロセスの見直しが可能か否かを検討し、システムの標準機能で対応できる部分が増えるようにすることも一つの方法です。

Fit&Gap 分析の結果に基づく決定

そのまま導入	フィット部分が大きく、カスタマイズなしで導入可能な場合。
部分的にカスタマイズして導入	小規模なギャップがあり、一部カスタマイズやプロセス変更で対応可能な場合。
大幅なカスタマイズまたは導入中止	ギャップが大きく、コストやリスクが許容範囲を超える場合、導入自体を見直す必要があります。

パッケージソフトウェアや SaaS 導入の成否は、この Fit&Gap 分析の精度に大きく依存します。適切な分析を行い、導入計画を立てることが大切です。

「要件定義」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点
第3編 第5章 要件定義 Step5 機能要件の定義
第3編 第5章 要件定義 Step6 非機能要件の定義

セキュリティ機能を実装・運用するためポイント

非機能要件における、情報セキュリティに関する事項について

自組織において定められた情報セキュリティポリシーを順守するために必要な情報セキュリティ対策の内容について、具体的に記載します。

例えば、当該情報システムに実装する機能や画面に対して、利用者の権限に応じた管理レベルを記載します。

No.	機能	利用者区分	アクセス権限	補足
1	〇〇申請処理	一般ユーザー	自申請情報のみ登録・参照・変更・削除可能	
2	〇〇申請処理	一般従業員	自組織が担当する申請者の情報は登録・参照・変更・削除可能。他組織担当の申請者情報は参照のみ	

また、想定されるリスクの概要と対策について記載します。

No.	リスクの区分	リスクの概要と対策	補足
1	…	インターネットからの不正アクセスなど、外部からの攻撃を受ける可能性がある。必要な対策を講じ、不正アクセスなどの悪意あ	

		る攻撃を防ぐ。	
2	...	来訪者エリアと従業員エリアで、同じネットワークを利用するため、来訪者エリアからの進入などの被害につながる可能性がある。ネットワークの論理分割、セグメント分割、 ファイアウォール やDNZなどの設置により、進入を防ぐ。	
3	...	利用者が担当業務に関係のない情報を閲覧し、情報漏えいにつながる可能性がある。必要十分な権限制御を行い、利用者に業務に不必要な情報を閲覧させない。	

最低限記述すべき情報セキュリティ対策要件

(1) セキュリティ機能の装備

【情報システムの構築などを行う場合の記載例】

以下のセキュリティ機能を具体化し、実装すること。

- 本プロジェクトで導入する情報システムへのアクセスを業務上必要な者に限るための機能
- 本プロジェクトで導入する情報システムに対する不正アクセス、ウイルス・不正プログラム感染など、インターネットを経由する攻撃、不正などへの対策機能
- 本プロジェクトで導入する情報システムにおける事故および不正の原因を事後に追跡するための機能（情報システムに含まれる構成要素（サーバ装置・端末など）のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。）

(2) [脆弱性](#)対策の実施

【情報システムの構築などを行う場合の記載例】

以下の脆弱性対策を実施すること。

（第三者による脆弱性検査を必要とする場合）

- 本プロジェクトに基づく改修（新規構築/更改）が影響する範囲について、第三者による脆弱性検査を実施し、その結果を関係各所に書面にて報告すること。

（第三者による脆弱性検査を必要としない場合）

- 本プロジェクトに基づく改修（新規構築/更改）が影響する範囲において、第三者による脆弱性検査を実施し、その結果を関係各所に書面にて報告すること。なお、脆弱性検査ツールを用いるなどにより客観的なテストが可能であれば、受注者で実施することも可とする。
- 構築する情報システムを構成する機器およびソフトウェアの中で、脆弱性対策を実施する

ものを適切に決定すること。

- 脆弱性対策を行うとした機器およびソフトウェアについて、公表されている脆弱性情報および公表される脆弱性情報を把握すること。
- 把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置および影響を納品時に関係各所に書面にて報告すること。

【情報システムの運用・保守・点検を行う場合の記載例】

以下の脆弱性対策を実施すること。

- 機器およびソフトウェアについて、公表される脆弱性情報を常時把握すること。
- 把握した脆弱性情報について、対処の要否、可否につき関係各所と協議し、決定すること。
- 決定した対処または代替措置を実施すること。

(3) 情報セキュリティが侵害された場合の対処

本プロジェクトにおける業務の遂行において情報セキュリティが侵害され、またはそのおそれがある場合には、速やかに関係各所に報告すること。これに該当する場合には、以下の事象を含む。

- 受注者に提供し、または受注者からのアクセスを認める関係各所の情報を外部へ漏えいおよび目的外利用
- 受注者から関係各所のその他の情報へのアクセス

20-1-6. 調達

調達の活動全体の流れは以下の通りです。

調達の全体の流れ

調達の事前準備

適切な外部事業者や製品を選定したり、調達時に不十分な内容に起因する手戻りなどの無駄な手間をかけず、効率的に調達作業を行ったりするためには、事前準備をすることが重要です。

1. 調達の単位・計画を確認する

- A. プロジェクト立ち上げ時点で調達を計画する
- B. さまざまな調達単位があることを理解する
- C. 調達にあった落札方式、評価方式を検討する

D. 調達計画を早めに公開する

E. 契約方式を検討する

調達の計画では、「何の調達を」「どの単位で」「いつ調達するか」を計画します。計画後、それらの調達を「どの単位で行うか」を検討します。複数を1つの調達にまとめることや、1つの単位を分割して複数の調達にすることも可能です。価格以外の技術的な評価を行う場合は、審査に必要なとなる評価基準、審査体制などを十分に検討した上で事業者の選定の準備を整えることが大切です。

2. 調達の注意事項を理解する

A. 調達手続きの基本的なルールを確認し理解する

B. 入札制限を正しく理解する

C. 一者応札の状況を改善する

D. 調達の前にリスクを再確認する

プロジェクト計画の段階で調達に係るルールを理解し、調達に必要な期間を踏まえて準備を行えるように調達の計画をたてることが重要です。

調達仕様書の作成

調達仕様書とは、プロジェクトの目的達成に必要な製品の入手や、必要となる役務を実施する外部事業者を選定するために示す、発注者側の条件を集めたドキュメントです。

1. 関連ドキュメントとの関係性を理解する

A. 調達仕様書と要件定義書の住み分けを理解する

B. 付属文書を活用して可読性を上げ機密性を確保する

C. 既存情報システムの機能改修を行う場合に準備するドキュメントを理解する

2. 調達仕様書の記載内容を理解する

A. 調達の意図や目的を正しく伝える

B. 関連する調達、入札制限を伝える

C. 作業内容・納品物を関連付けて網羅的に記載する

D. 外部事業者の具体的な作業内容を明確にする

E. 作業の実施体制を明確にする

F. 成果物の取扱いに注意する（知的財産権）

G. 再委託に関する事項を定める

H. 納品後に不具合が発覚したときの責任を明確にする（契約不適合責任）

調達仕様書以外のドキュメント作成

調達では、調達仕様書以外にも、提案依頼書や契約書などさまざまなドキュメントを用意する必要があります。

1. プロジェクトに合わせた契約書を作る

A. 調達仕様書と契約書の整合性を確認する

調達仕様書の記載事項には、場合によって契約書に同様の事項を記載することがあります。調達仕様書と契約書でそごが生じている場合、後々問題となることもあるので、契約書を所管する部署と事前に意識合わせを行い、調達仕様書との記述の住み分けを決めておくことが重要です。

2. 提案依頼書の内容を工夫する

A. 具体的な作業計画を評価する

B. 加点の配分を工夫する

提案書の内容だけでは、事業者が本当に調達案件を履行する能力があるか否かを判断するのは難しいです。技術力を適正に評価するためには、具体的な作業計画の案の提出を求めて評価することが効果的です。技術審査を行う際は、当該調達で何を重視するかをよく検討し、重視する項目に対する優れた提案に高い配点がされるように検討する必要があります。

調達手続きとプロジェクト管理

プロジェクトの活動において、調達はそれ以前の活動結果を集約し、その後の活動を方向づけるプロジェクトの結節点ともいえます。このタイミングでのポイントを押さえた上で調達手続きを行うことは、プロジェクト管理の視点からも重要です。

1. 調達手続きに伴うプロジェクト管理作業とは

A. 第一次工程レビューを意識して資料をチェックする

調達仕様書の自己点検を行っておくことで、調達が不落に終わることによる調達事務手続きの手戻りなどの無駄を未然に防ぐことにつながります。

2. 情報システムの調達に特有の注意点

A. ベンダーロックインを理解し、回避する

B. 入札参加要件を緩和する

C. 入札事務手続きを簡素化する

情報システムの調達には特有の注意点があり、これを理解せずに進めると後々問題が発生する可能性があります。問題を防ぐためには、事前にこれらのポイントを把握し、仕様書や契約書に適切な制約を盛り込み、しっかりと管理することが重要です。

検収

調達の結果、外部事業者との契約が締結され、製品の購入手続きも含め委託した作業がスタートします。その結果、製品であれば納品、作業であれば完了報告が行われ、発注者はそれに対して検収を行います。

1. 検収の位置づけと内容を理解する

A. 検収と受入テストの違いを理解する

B. 残存する課題（軽微な瑕疵など）の対応を明確にする

検収の実施者は、発注者側の担当者です。検収の担当者は、調達仕様書および契約書に定められた内容と納品物との突合せを行い、仕様どおりに納品されているのかを確認します。一方、受入れとは、[PJMO](#)を中心として、納品された成果物が今後のサービス・業務の実現に足るかを判断する行為です。検収時点で不具合がわかっている場合は、各々の不具合に対して、「いつまでに」「誰が」責任を持って「どのように」対応するかを改修計画で明確にします。

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たったの留意点を説明します。

例：関連ドキュメントとの関係性を理解する

調達では、調達仕様書以外にも次のようなドキュメントが存在します。それぞれのドキュメントの定義と関係性をあらかじめ理解しておくことが重要です。

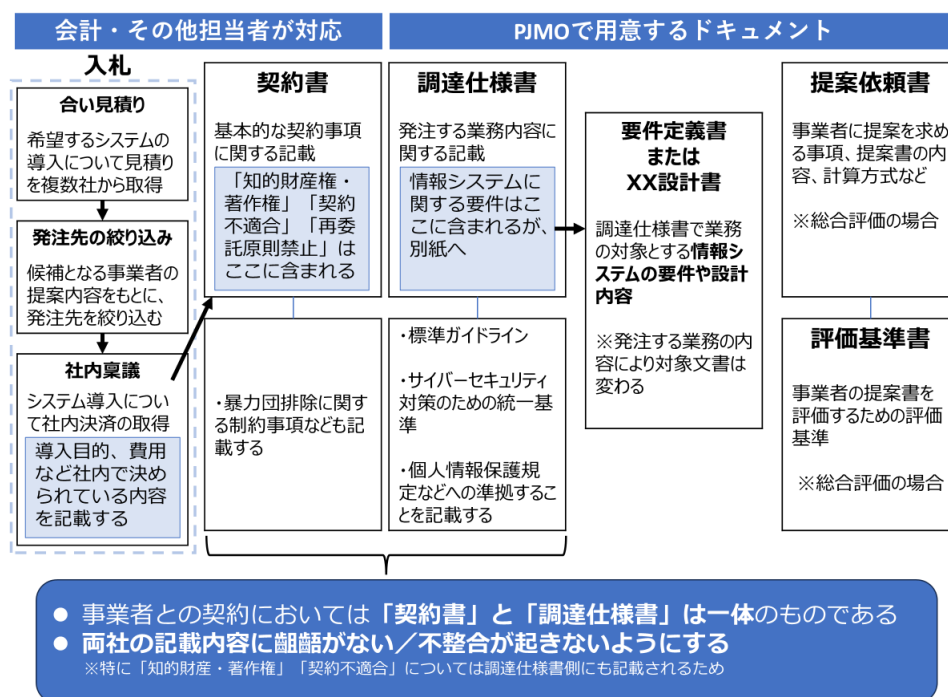


図 76. 調達に必要なドキュメントの関係図

例：「調達の事前準備」における、調達の注意事項を理解

プロジェクト計画の段階で組織の調達ルールをよく理解し、調達に必要な期間を踏まえて準備を行えるように、調達の計画を立てることが重要です。

「調達」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第6章 調達 Step3 調達仕様書の作成

セキュリティ機能を実装・運用するためポイント

再委託先の情報セキュリティ対策に係る規定を確認すること

情報システムの整備においては、プロジェクトの規模が大きくなるほど、さまざまな役割が必要となります。特に、設計・開発工程や運用・保守工程では、情報システムの一部を担う特定の技術や専門分野に特化した外部事業者を活用する機会が多いです。これらの外部事業者は、請負契約を締結している外部事業者からの再委託となることもあります。再委託先が担当する作業内容については、委託先の外部事業者（以下「委託先」という）が責任を持って管理することが原則です。しかし、再委託にまつわる失敗事例は多いです。

事例：再委託に関する失敗例

- 委託先が作成した提案内容を評価し、プロジェクトの委託先として選定したにも関わらず、再委託先が提案内容を遂行するために必要なスキルレベルを十分に持っていないため、成果物の品質低下やスケジュール遅延を招いてしまった。
- 委託先が再委託先に利用者との検討や調整などの作業を丸投げしてしまい、要件や仕様の変更を把握しなかったため、工数超過やスケジュール遅延に発展してしまった。

このような問題を未然に防ぐために、調達仕様の「再委託に関する事項」にて、再委託の制限および再委託を認める場合の条件、承認手続き、再委託先の契約違反などを定め、再委託時の要員の配置や品質、情報管理などに関する責任の所在を明確にします。また、プロジェクト遂行中に発生したさまざまな事情により、請負側の体制変更を図ることがありますが、その際は発注者側と協議の上、請負者の負担と責任において実施することが原則です。

なお、再委託に関する事項は、自組織の情報[セキュリティポリシー](#)における再委託先における情報セキュリティ対策に係る規定も必ず確認することが大切です。

20-1-7. 設計・開発

設計・開発の活動全体の流れは以下の通りです。

設計・開発の全体の流れ

設計・開発を開始するための事前準備

設計・開発を開始する間に、要件を適切に事業者伝える必要があります。また、[PJMO](#)が求める情報システムをトラブルなく構築していくためには、仕様の調整や、できた情報システムを適切に検証することが必要となります。

1. 設計・開発で従業員が行うべきことを理解する

- A. 『要件の内容を伝える役割』
- B. 『要件どおりに情報システムができたかを確認する役割』
- C. 『プロジェクトの進捗状況を正しく把握し適切な調整を行う役割』

要件定義書だけでは読み取れない発注者側の意図や要望について、発注者側は正しく伝達することが必要となります。また、設計をする中で見えてくる課題などの対応方法を決めることも必要です。構築された情報システムが、伝えた要件を満たすものになっているかを確認します。また、新たな情報システムを導入する際には、ほとんどのケースで業務を見直して、手順や内容の変更を行います。

2. 設計・開発全体を通して理解すべき点とは

- A. 要件を理解した従業員の継続的な関与がプロジェクトを安定させる
- B. 要求とコストと納期のバランスをとる
- C. 設計・開発の全体像と流れを理解する
- D. 通常シナリオだけでなく緊急時の対応計画も準備する
- E. メンテナンス性を考慮した成果物の構成、内容を考える

PJMO が、発注者として設計・開発を適切に管理していくために、設計・開発の活動全体を俯瞰的に理解しておく必要があります。例えば、要件定義において、その全体像を理解している従業員はごく一部に限定されます。この従業員をプロジェクトの体制に参画させ続けられるよう、体制の組成時に調整を行うことはプロジェクトを安定させることにつながります。

設計・開発の計画

設計・開発事業者が決まった後、最初にすることは計画を立てることです。設計・開発の活動は、PJMO にとっては、実態が見えにくい活動になりがちで、問題の発覚が遅れて大惨事になることもしばしばあります。設計・開発の活動をブラックボックスにしないようにすることが大切です。

1. 設計・開発の管理の要点を理解する

- A. 定点観測こそ進捗・品質管理の要
- B. 判断に必要な情報を従業員が理解できる説明として事業者に求める

作業の状況を定量値で管理し、継続してその値を把握すると、問題が発生する予兆を捉えられます。その事象を個別に分析することで、原因を捉え必要な対策ができます。また、事業者の資料や説明内容は従業員から見ると専門的でわかりにくいものになりがちのため、内容を理解できるように丁寧な説明や資料のまとめ直しをしてもらうことが大切です。

2. 設計・開発の実施計画を立てる

設計・開発実施計画書は、当該事業者が担当する設計・開発作業の範囲について、PJMO が作成するプロジェクト全体のプロジェクト計画を具体化・詳細化したものです。設計・開発の実施計画を作成する際は、以下のポイントに注意して作成することが重要です。

- A. 2 種類のプロジェクト計画書の相違点を理解する
- B. 意思決定の手順を明確にする
- C. 当初計画からの変更は、必ず関係者で合意する
- D. 他の関係者との役割分担の境界線を定める

- E. WBS で作業計画を確認し進捗を把握する
- F. EVM を用いた進捗管理手法を理解する

3. テストの計画を立てる

- A. V 字モデルと発注者・委託先事業者の役割分担を把握する
- B. テストのレベルや種類を理解する
- C. リスクを踏まえてテストの方針を決める
- D. テストにおける役割分担と必要な環境を明確にする
- E. テストツールを有効活用する
- F. テスト計画を作成する

ウォーターフォール型の開発プロセスでは V 字モデルが一般的です。テスト工程において、発注者側にはテスト計画を確認し、テスト実施状況を管理し、テスト結果を評価するという重要な役割があります。特に、総合テスト以降の工程終盤になればなるほど発注者側の関与が重要であり、受入テストは発注者自身が実施するものです。

設計・開発・テストの管理

設計・開発の大部分の作業は、事業者が行うこととなりますが、PJMO が適切な関与を行わなければ、良い情報システムを構築することはできません。

1. 設計内容を確認・調整する

- A. 基本設計の内容を確実にレビューする
- B. 他の情報システムとのデータ連携には細心の注意を払う

設計書のレビューは、基本的に「基本設計」で作られた成果物を対象とします。基本設計以降は、基本設計に基づいて詳細設計や実装などが行われるため、それらの整合性を確認するのは基本的に事業者の責任範囲となります。情報システムの多くは他の情報システムとデータ連携を行います。そして、このデータ連携では、高い確率でさまざまな問題が発生します。問題を起こさないためには、まずは、他の情報システム側の担当者などとの協力体制を築くことが重要です。

2. 品質管理の考え方を理解する

- A. 見えない品質を見える状態にする

品質は一見すると目に見えない概念です。品質を「見える」形にするために、テストの進捗や障害の発生件数、解決件数などを数値化し、グラフなどで可視化します。これにより、品質を確認できます。

3. 単体テスト・結合テストの品質を評価する

A. 単体テスト留意点

B. 結合テストの留意点

単体テストは開発者が自ら試行錯誤しながら実施するので、不具合件数は過少報告されがちです。結合テストは事業者が主体となって実施する工程ですが、発注者もテスト計画、テスト管理状況、テスト結果などについては積極的に確認する必要があります。

4. 総合テストの品質を評価する

A. 総合テストの留意点

B. 発見できた障害は最大限活用する

総合テストでは、業務観点からのいろいろなシナリオに基づいて機能テストを検証しますが、これに合わせてシステムの性能や信頼性などを検証する非機能テストを行います。総合テストの段階はリリースまでの残り日数が少なくなっていて、単体・結合テストと違って数日の遅延が致命的になるので、特に進捗管理には注意を払います。

5. 受入テストを実施する

A. 受入テストと他のテストとの違いを理解する

B. 受入テストのテスト計画書を作成する

受入テストは、他のテストと異なり、従業員が主体となって行う最終段階のテストです。

「サービス・業務企画や要件定義で想定したとおりに情報システムができているか?」「構築された情報システムを用いて実際のサービス・業務を正しく実施できるか?」という観点で受入テストを行います。

見落としがちな活動に注意

設計・開発でなければいけないことは、情報システムの構築だけではありません。本番で情報システムを稼働させ、サービス・業務の円滑な運営を行っていくためにはさまざまな活動が必要になります。

1. どのプロジェクトでも必ず移行を計画する

A. 移行の種類を理解する

B. リハーサルも考慮した移行計画書を立てる

情報システムの移行は、どのようなプロジェクトでも必ず発生します。既存のサービス・業務や情報システムが存在しない場合でも、本番の情報システムの構築、データの設定、切替え、新規業務の開始に関わる業務の変更などは必ず必要です。移行に関するポイントを理解することが大切です。

2. 次の運用・保守は開発と並行して検討する

A. 指標値を運用作業で取得できるように検討する

B. 運用・保守の計画を立てる

継続的な改善を行い、プロジェクト目標を確実に達成するためには、指標値の評価を容易に行えるようにして定期的に確認していくことが必要不可欠です。運用計画書、運用実施要領、保守計画書、保守実施要領などは、運用・保守事業者の調達仕様書の附属資料になり、運用・保守事業者の調達後に確定されることになります。

3. 種類を理解し揃えるマニュアルを厳選する

A. マニュアルの種類を理解する

新業務の運営を円滑に行うための準備

情報システムを無事に稼働させ、新しいサービス・業務の運営を円滑に行っていくために必要となる最終盤の作業を行います。

1. 本番移行と本番稼働の開始を承認する

A. 移行判定と稼働判定の違いを理解する

2. 正しき引継ぎを行い、トラブルを減らす

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

設計・開発を開始するための事前準備

設計・開発の具体的な活動を行うのは、調達によって選定された事業者です。事業者は、調達仕様書および附属資料である要件定義書をインプットに、設計・開発工程の活動を計画し、活動を行います。設計・開発工程の作業は、情報システムを対象とした専門的なスキル・経験が求められます。

従業員が関与しなければ、作業は順調に進みません。一般的に、従業員の関与が低いほど、設計・開発の成功確率は低下します。『専門的』でわかりづらい設計・開発工程の作業において、『従業員が関与する』ことで効果がある作業とは何かを理解する必要があります。従業員が作業に関与するに当たり、基本的な役割を以下に示します。

『設計・開発』を行う際の従業員の基本的な役割

- 要件の内容を事業者に正しく伝える役割
- 要件どおりに情報システムができたかを確認（テスト）する役割
- プロジェクトの進捗状況を正しく把握し、スケジュールや関係者間において発生する調整を

適切に行う役割

「設計・開発」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第7章 設計・開発 Step3 設計・開発の計画

第3編 第7章 設計・開発 Step4 設計・開発・テストの管理

セキュリティ機能を実装・運用するためポイント

テスト計画の策定

情報システムの設計・開発では、品質の管理が重要であり、そのためには十分なテストが必要です。現在、ウォーターフォール型の開発プロセスではV字モデルが一般的です。開発プロセスには各種の国際標準や国内標準もありますが、「標準ガイドライン」の工程定義に則つると次のように表現できます。

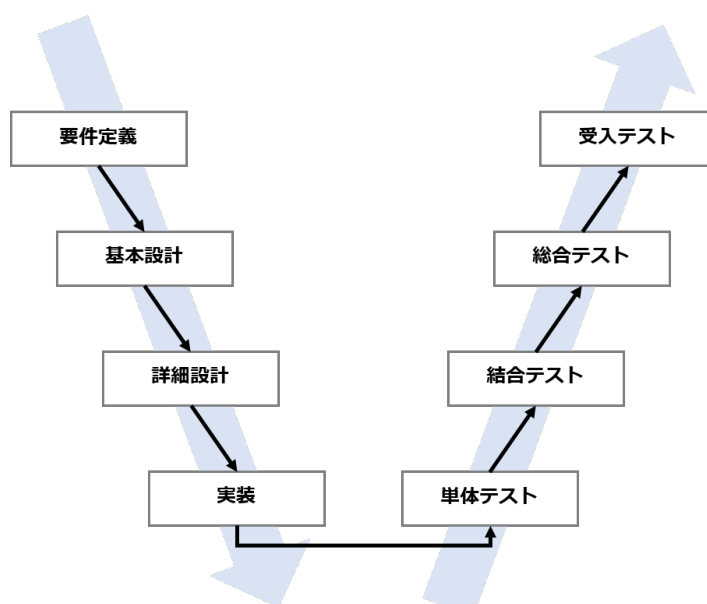


図 77. 標準ガイドラインの定義に則ったソフトウェア開発プロセスのV字モデル
(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

同じ高さにある工程が、それぞれ深く関係しています。例えば、総合テストとは基本設計で定めた要件が充足されているかを確認するテストであり、受入テストとは要件定義との充足性を確認するテストです。

テスト工程において、発注者側にはテスト計画を確認し、テスト実施状況を管理し、テスト結果を評価するという重要な役割があります。特に、総合テスト以降の工程終盤になるほど発注者側の関与が重要であり、受入テストは発注者自身が実施するものであることに留意しましょう。

テストのレベルと種類

情報システムのテストは、段階的に進めていきます。例えば、「個々のプログラムが設計書どおりにできているか?」、「プログラムをつなげて機能としてみたときに、機能の設計を満たしているか?」、「機能同士をつなげてみたときに、要件を満たしているか?」、「要件どおりにできたが、業務が適切に遂行できるか?」など、徐々に確認するレベルを上げていきます。

これは、V字モデルが表しています。標準ガイドラインで定義しているテスト工程では、次のように整理しています。

テスト工程	概要	発注者の関与の仕方
単体テスト	アプリケーションを構成する最小の単位で実施するテストであり、主に機能単位で設計どおりに動作するかを事業者（プログラマ）が確認する。	事業者がテストの実施主体ではあるが、発注者もテスト計画を確認した上で、実施状況の報告を求め、報告書に記載されている実施結果に不足、誤りなどが発生している場合は、課題などを整理し、指摘または指導を行う。
結合テスト	複数の機能を連携させて動作を確認するテストであり、主にユースケース単位で設計どおりに動作するかをテスト担当者が確認する。	（同上）
総合テスト	システム全体が設計のどおりに動作することを確認するテストであり、ユースケースを組み合わせた一連の業務が行えることを機能面や非機能面の観点からテスト担当者が確認する。	上記に加えて、テストシナリオやテスト評価方法の妥当性を確認し、過不足を指摘することで抜け漏れがないテストの内容になるように関与する。
受入テスト	納品されるシステムが要件どおりに動作することを確認するテストであり、発注者が主体となり、事業者と協力して確認する。	発注者が主体となりテストを実施する。実際の利用者がテストに参加することで、サービス・業務が円滑に実施できることを確認する。事前に要件を十分確認できるテストシナリオかを確認し、実際にテストシナリオに基づき情報システムを操作し、テスト結果が要件どおりであることを確認する。

テスト工程とは別に、テスト手法の違いがあります。

テスト手法	概要
ホワイトボックステスト	ホワイトボックステストとは、プログラム（ソースコード）の内部構造、論理構造を理解した上でその構造どおりに実装できているかを確認するテストです。中身が見えている状態で行うテストなので、ホワイトボックスと呼んでいます。プログラムを「作る」人の目線でのテストともいえます。基本的に、上述のテスト工程のうちホワイトボックステストを実施するのは単体テスト工程です。ホワイトボックステストでは、ソースコードがテストされた割合を示す「カバレッジ（網羅率）」が重要な指標となります。しかし、カバレッジには主として3つのレベルがあるので、どのカバレッジレベルを前提としているかについて注意が必要です。 （参考）カバレッジの種類 ● C0 命令網羅率：プログラム内の命令文をどの程度網羅したか ● C1 分岐網羅率：プログラム内の分岐をどの程度網羅したか ● C2 条件網羅率：プログラム内の条件をどの程度網羅したか 長所： ● 期待どおりの処理がされているかを網羅的に確認できます。 短所： ● 仕様自体の間違いや機能が備わっていないバグなどはホワイトボックステストでは検出できません。 ● カバレッジは必ずしも100%を目指す必要はありません。100%に近づくほどコストが増大するので、適切にカバレッジを定める必要があります。
ブラックボックステスト	ブラックボックステストとは、プログラムの内部構造、論理構造に着目するのではなく、プログラムの入出力に着目します。プログラムの外側から見たときに仕様どおりに動作するかを確認するテストです。中身が見えない状態で行うテストなので、ブラックボックスと呼んでいます。プログラムを「使う」人の目線でのテストともいえます。基本的に、ホワイトボックステストの完了後に、さまざまな粒度や観点からブラックボックステストを実施します。 長所： ● レイアウトが崩れていないかなど、実際に使用する観点でテス

	トすることができます。 短所： ● 結果が正しい場合、処理上の不具合があっても見つけることが難しいです。

テストツールの活用

近年、情報システムの品質を向上させるためのツールは多く登場しています。これらを活用することで、設計・開発の活動を効率的に進めたり、効果的に品質を担保・向上させたりすることができます。事業者とも相談しながら、導入を検討することが重要です。

ツールの種類	概要	メリット
ソースコードの静的解析ツール	ソースコードから、機械的にコード規模（コード行、スペース行、コメント行など）、複雑度、複製度/重複度、正当性、セキュリティ観点からの好ましくない行、パターンなどを機械的に抽出するツール。	静的解析ツールは、ソースコードレビュー（インスペクションともいいます）を助け、コード品質の向上、レビューワの負荷軽減、期間短縮に効果を発揮します。 コード特性を可視化することができるため、全体を俯瞰しながら個々の問題や指摘箇所について検討できます。このため、プログラマはツール結果を見ながら自分で問題点を検討し、修正できます。一人では解決できない場合も、レビュー時にレビューワにツール結果を見せることにより、レビューワも問題の特定が容易となり作業負荷の軽減、時間の短縮につながります。
自動テストツール	ソフトウェアテストを行うための作業（テストケースの設計、テストの実行と結果の確認、テストの進捗管	効率よく自動テストを実行するよう、スケジューリングすることで、手動でのテスト工数を削減することが可能で

	理、レポートの作成) またはその一部を自動化するツール。	す。
継続的インテグレーション	コンパイル ・テスト・ デプロイ といったソフトウェア開発のサイクルを頻繁に繰り返し実行する手法。	短期間で品質管理を行うため、問題の早期発見や開発の効率化が可能です。
タスク管理ツール	プロジェクト全体のタスクを管理することができ、進捗の見える化や共有化などにより、タスクを管理しやすくするツール。	タスクのツリー構造を定義し、整理することができます。また、タスクの順序や優先度合いを設定し、スケジュール管理できます。 スケジュールや進捗具合を、自動でガントチャートなどのグラフ化で表現でき、直感的に状況を把握することができます。

20-1-8. サービス・業務の運営と改善

サービス・業務の運営と改善の全体の流れは以下の通りです。

サービス・業務の運営と改善の全体の流れ

新しいサービス・業務の事前準備

新しい情報システムを利用してサービスや業務を実施する際、[PJMO](#) の従業員は情報システムを構築することに意識が行きがちです。一方、利用者にとっては、情報システムが構築直後に「満足な出来」であることは少なく、大なり小なり期待値とのギャップがあります。これを解消するため、利用者からのフィードバックを得ながら、業務と情報システムの双方を改善していく活動を継続していくことが重要です。

1. 運営と改善は、従業員主体の作業である

- A. 『サービス・業務の運営と改善』を外部の事業者に丸投げしない
- B. 『サービス・業務の運営と改善』は他工程の作業と並行で実施する
- C. 関連する業務実施部門との責任分担を意識する

2. 業務手順書はさまざまな用途に有効活用できる
 - A. 業務マニュアルと他のマニュアルとの違いを理解する
3. リハーサル計画・シナリオは従業員目線で
 - A. 移行リハーサルを計画・実施する
 - B. 業務リハーサルを計画・実施する
 - C. サービスの開始や変更を利用者に確実に周知する

業務の定着と次の備え

新しい業務を開始すると、その業務をできるだけ早く現場に定着させ、業務の効率を上げることが求められます。利用者に積極的に使ってもらうための工夫も、定着に向けたカギとなります。また、データマネジメントの観点を意識しながら、業務で取扱うデータの品質を維持していかなければ、肝心なときに必要な情報が取得できなくなり、業務を効率化できない割に運用・保守コストだけがかかるような、使えない情報システムになりかねません。

1. 従業員に継続的な教育を行う
 - A. 研修・教育の準備を十分に行う
 - B. 研修・教育は1回では定着しない
2. 定着には利用者への働きかけが必要
3. 業務で扱うデータの品質を確保する
 - A. 計画どおりにデータを入れないと情報システムの価値はない
 - B. 分析しやすいデータ構造でないと、何かするにも力ネがかかる
4. 業務改善に向け日常業務の事実を蓄積する
 - A. PJMO・従業員がさまざまな情報を収集し、定常的に管理する
 - B. 情報システムのログなど、運用活動に関わる情報を取得可能にする
 - C. 効果測定ができるように [KPI](#) を自動的にとれるようにしておく
 - D. 多数のインシデントや要望などの対応の優先度をつける

業務の改善

業務の改善は、日常的に改善できるものと、情報システムや業務そのものなど、時間をかけて見直すものがあります。

1. 日常業務中でも改善できることを理解する
2. 検討の進め方を理解する

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

（例）：業務の定着と次の備え

新しい情報システムがリリースされると、サービス・業務の運営が始まります。新しいサービス・業務が今までのものと違いがあるほど、リリース直後からしばらくの間はさまざまな問題が発生するかもしれません。業務に関わる従業員は、できるだけ早く業務を現場に定着させようと悪戦苦闘しますが、それ以外にも、より良いサービス・業務となるような活動を併せて行う必要があります。

従業員に継続的な教育を行う

PJMO は、情報システムの設計・開発のリリースが近づいたところで、それまで準備した研修教育資料を用いて、実業務を担当する従業員に対して教育を実施します。

研修・教育の準備を十分に行う

PJMO は、研修資料として、PJMO 主導で作成した業務マニュアルや、事業者主導で作成した情報システムの操作マニュアル、それらをまとめた研修用資料などを準備します。また、可能であれば、デモ環境や研修環境なども用意し、情報システムを実際に触れる環境を提供することも効果的です。

広範囲の従業員が利用する情報システムにおいては、PJMO やヘルプデスクを担当する事業者も、研修・教育の準備期間中に、一般従業員と同じ研修を受講しておくことが望めます。これにより、研修カリキュラムの改善につながることはもちろん、利用者からの問い合わせに的確に対応できるようになります。

情報システム構築の作業進捗状況が遅延すると、研修や教育の回数制限、期間の短縮や、現場担当者が新しい情報システムに触れられる環境の準備が遅れる可能性が出てきます。PJMO は研修や教育に最低限必要な期間は必ず確保できるように、構築事業者の進捗管理をチェックし、安易な計画変更を起こさないようにすることが重要です。

研修・教育は 1 回では定着しない

通常、新しい情報システムのリリース前に行う教育は、開発実施計画を立てる時点でしっかり盛り込まれていれば、作業が抜け漏れることなく実施できます。

研修や教育は、どのぐらいの頻度で実施すれば良いのかといった、計画を立てる際に気をつけるべき注意点を以下に挙げます。

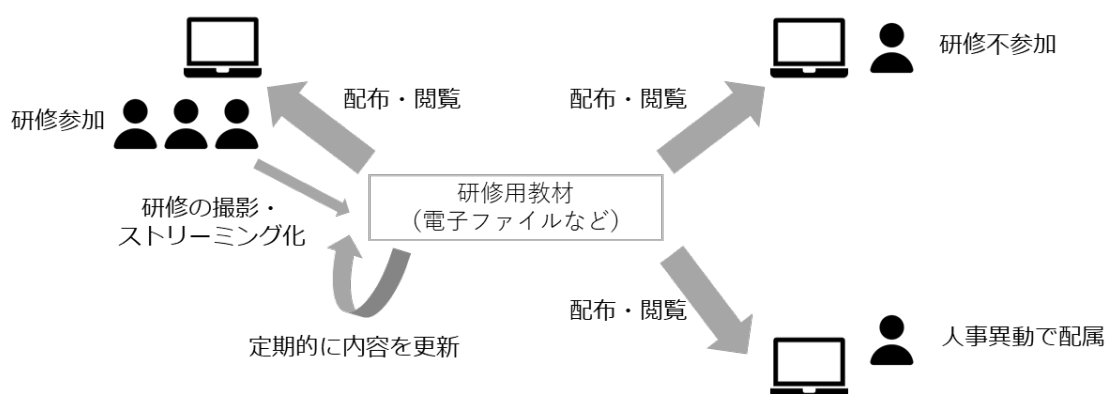
現場への研修・教育を計画する際の注意点

- 大規模システムの場合、全国各地に業務担当者が散らばっていることが多く、実施回数が少ないとそのタイミングで教育を受けられない担当が発生する可能性が出てくる。
- 研修・教育の回数が制限されていると、情報システムリリース後、新しく人事異動で配属された従業員が、正しい情報を把握することができなくなる。
- 教育資料や教育の内容が不十分な場合、そのまま同じように全従業員に情報が伝達されても、全体のレベルが上がらない。

この懸念点を払拭するには、次の対策をとることが効果的です。

懸念点への対策

- 研修を実施した後、受講者にアンケートを配布し、研修の内容・難易度に関する意見をもらい、それをもとに研修のカリキュラムや資料の内容を見直す。
- 研修に用いた教材を関係者が閲覧できるようにする、電子ファイルをダウンロードできるようにするなど、研修に出られない人にも研修の内容が伝わるように工夫する。
- 研修そのものを撮影し、オンラインにてストリーミング配信できるようにする、DVD に焼いて配布するなどの対策を検討する。



いつでも操作・閲覧できるように研修環境を維持することが重要

図 78. 研修・教育の定着化に向けた取組

（出典）「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「サービス・業務の運営と改善」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第 3 編 第 8 章 サービス・業務の運営と改善 Step3 業務の定着と次の備え
 第 3 編 第 8 章 サービス・業務の運営と改善 Step4 業務の改善

セキュリティ機能を実装・運用するためポイント

業務を外部委託する際の注意

サービス・業務を運営する中では、業務・サービスに関連する日常的なオペレーションはもちろんのこと、問い合わせや要望への対応、利用促進のために周知や広報活動を行うなど、さまざまな活動を従業員が主体的に実施します。

ただし、一部の作業については、従業員が正しく作業を切り出し指示や管理をすることを前提に、外部の事業者へ作業を委託できるものがあります。例えば、業務で発生するデータの入力業務や、帳票の仕分け業務などです。

どのような業務が事業者への委託に向いているのか、一般的には、次の図のような考え方ができます。



図 79. 外部委託の向き/不向き判断例

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

業務を外部委託する際の注意点

- 外部委託する業務は、従業員が主体的に行う業務に対する支援や補助となる作業であり、それを行うことで従業員の業務効率が向上するものであること。
- 外部委託した業務成果の正誤や品質状況を従業員が判断できるように、プロセスの透明化と必要十分な報告・記録を確保すること。
- 外部委託した業務の実施方法や、事業者が作成する業務マニュアルなどの内容を適宜確認し、従業員自身も業務の概要を理解し続けること。
- 特定のサービス・業務について、異なる作業範囲や役割を複数の事業者へ外務委託する場合は、緊急時（システム故障や[セキュリティインシデント](#)など）に備えて、できるだけ特定の事業者へ業務統制的な役割を定義しておくこと。

インシデントの優先度つけ

業務に関する問い合わせやインシデント、要望などを取りまとめていくと、膨大な量になり、すべてを対応するのは時間もコストも足りません。そのため、それぞれを整理した上で、優先度をつけて、優先度の高いものから対応していく必要があります。

優先度は、業務遂行上で重要か否かを判断してつけることが大切です。例えば、画面を複数切り替えないと関連する情報が確認できず、件数が多くて作業が非効率ということであれば、情報システムの改善による業務の効率化を検討すべきかもしれません。しかし、単純に画面レイアウトや操作性などについての要望は、個人の好みに依存することが多く、改善効果は見込めません。また、利用者側が業務を遂行できない、または多大な事務作業が発生する不具合に対応できないような場合は、そもそも情報システムの利用を推奨するべきではなく、業務の見直しも含めた検討が必要になります。

インシデントの優先順については、過去のインシデント分析にて、起こっている問題を詳細に分析することで、クリティカルな部分を優先して対策することが効果的です。インシデント分析は、一部をサンプリングして全体を理解するのではなく、全数を調査・分析して全体を捉えることが重要です。サンプリングして行う調査・分析は、コストをかけず実行することができますが、サンプリングから漏れる少数の事実が全体に影響を与える場合があるためです。

20-1-9. 運用および保守

運用および保守活動全体の流れは以下の通りです。

運用および保守の全体の流れ

運用・保守を開始するための事前準備

情報システムが完成したら、サービス・業務を滞りなく提供していくために情報システムをしっかり運用・保守する必要があります。より良い運用・保守を行うためには、事前準備が必要です。

1. 「運用と保守」の位置づけを理解する

- A. サービス・業務をより改善するための活動を行う
- B. 情報システムの運用と保守の活動を理解する
- C. 運用・保守は他のさまざまな活動と連携し、平行で実施する
- D. 運用・保守に、自動化の仕組みを取り入れる
- E. システム間での運用統合を検討する

運用とはサービス・業務を実現するための「情報システムの機能を利用者に提供し続けるための活動」です。効果的なサービス・業務を実現するためには、運用・保守フェーズにおけるヒ

ヤリ・ハット（インシデント）を多く見つけ、改善を繰り返すことが重要です。また、人による体制で運用・保守を行うと人件費がかさみ、運用保守のコスト増となるため通常システム運用管理ツールなどを導入して自動化による効率化を図ります。

2. 作業責任を正しく理解しトラブルを防ぐ

- A. 外部委託事業者へ依頼する作業の内容を明確にする
- B. 指標の基礎データを誰がどのように集めるかを明確にする
- C. 業務実施部門を含めた運用体制を確立する
- D. 障害発生時の役割分担に注意する

「運用」および「保守」に係る作業は、基本的に外部事業者に委託して実施します。外部事業者へ依頼する作業や役割は、調達の段階で調達仕様書に明記しておく必要があります。また、いくつかの指標（[KPI](#)）を用いて判断し、業務の改善や見直しを行います。このほか、情報共有や障害発生時の役割分担などを事前に取り決めておくことが大切です。

運用・保守の計画

運用・保守を実施する事業者が決まったら、最初にすべきことは契約期間中の実施計画を立てることです。

1. 運用と保守の計画を作成する

- A. システムプロファイルに応じた運用・保守レベルにする
- B. セキュリティ関連作業を定期的に確実に実施する
- C. プロジェクトの目標や指標の評価に必要なデータは必ず取得する
- D. 非機能要件に関連するデータを網羅的に詳細に取得する
- E. 会議体は目的を明確にして必要最低限に抑える
- F. 定例会の報告フォーマットを指定して、効率性を上げる
- G. 運用・保守の工数を把握し、人件費をモニタリングする
- H. 運用・保守における変更管理を理解する

運用・保守体制については、システムプロファイルで示した運用・保守レベルを維持できる最低限の体制を基準として、プロジェクトの状況に応じて定期的に見直しを行い、徐々に適切なレベルの保守・運用にしていくように調整します。また、会議や報告の効率化を進めます。

運用・保守の定着と次の備え

運用・保守のほとんどの作業は事業者が実施することになりますが、[PJMO](#) が適切な関与を行わなければ、より良い運用・保守に改善していくことはできません。

1. 運用定例会議を有効活用する

A. 運用保守定例会議で確認する内容を理解する

運用保守定例会議では、運用・保守の計画で定めた報告フォーマットにしたがって、事業者から報告を受けることになります。報告を受け取るだけではなく、報告が不十分なものは、指摘・再提出も求め、改善活動につながる課題や改善点を報告内容から見出すことが大切です。毎回同じ項目が定期的に報告される特徴から、長期間にわたる推移を把握することも可能です。

2. 変更を管理し改善活動などの初動を楽にする

設計書などから現状の情報システムがどのようなになっているかを確認し、プロジェクトの事情に合わせて、効率的に管理できる方法を検討する必要があります。

3. 情報システムで起こった事実を蓄積する

- A. 運用・保守の範囲にとらわれず、意味のある情報を取得する
- B. 情報システムの活用状況を詳細に把握し提供する機能を棚卸する
- C. 情報システムのログやトランザクションデータから改善のための情報を取得できるようにする
- D. 運用・保守実施記録を適切に保管する

運用・保守の改善と業務の引継ぎ

運用・保守の実施中に判明した課題は、定常的な作業の中で改善ができるものは積極的に改善していきます。

- 1. 適切な時期に的確に改善を実行する
- 2. 要員の交替で情報が欠落しないようにする

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：作業責任を正しく理解しトラブルを防ぐ

運用・保守の活動やそれに係る「サービス・業務の運営と改善」などの活動には、さまざまな関係者が関わります。それぞれの作業内容や責任範囲が曖昧になってしまうと、作業漏れや関係者間の意思疎通が不十分となることによる新たな問題が発生するリスクが増大します。悪くすると、情報システムの安定的な稼働への問題発生、改善活動の停滞などを招き、プロジェクトの目標達成に影響が出てしまいかねません。

外部委託事業者へ依頼する作業の内容を明確にする

「運用」および「保守」に係る作業は、基本的に外部事業者へ委託して実施します。その理由は、内容が専門的であることや、手順に沿った定型かつ大量な作業が多いため、PJMO や業務実施部門の従業員が実施すると、かえって非効率になる可能性があるためです。外部事業者と役割を適切に分担することにより、発注者側の従業員は、業務の質向上やコスト削減などの、本来従業員が行う事業者では実施できない作業に、より注力することができます。

外部事業者へ依頼する作業や役割は、調達の段階で調達仕様書に明記しておく必要があります。事業者確定後にこれらの詳細を詰めようとするのは、トラブルの原因となりますので、注意が必要です。

指標の基礎データを誰がどのように集めるかを明確にする

指標に用いるデータを取得するための作業は、標準ガイドライン「第8章サービス・業務の運営と改善」の作業と密接に関連します。サービス・業務の運営と改善では、プロジェクト計画書で定めたプロジェクトの目的・目標が実現できているかに関して、いくつかの指標（KPI（Key Performance Indicator））を用いて判断し、業務の改善や見直しを行います。指標（KPI）は、基礎値の組み合わせによって、表されます。

指標のもととなる各種データは、種類ごとに、取得先、取得手段、取得頻度などについて詳細な検討が必要です。代表的なデータとして、情報システムが稼動している際に作り出されるログやトランザクションデータと呼ばれるものが挙げられます。これらは、従業員が自ら取り出せるもの、運用事業者へ依頼しないと取り出せないものなど、データの取得には制約が発生します。前者であれば、事前に技術的な経験のない従業員でも容易に取得できるように、取得手段が機能化されている必要があります。後者は対象と取得手順が明確に定義されていなければ、定常的な運用作業として継続できません。

これらを踏まえて、取りこぼしが発生しないよう、必要なデータ項目を事前に把握するとともに、外部事業者へ取得を求める場合は調達仕様書に明記しておくことが大切です。

指標は、いざ算出しようとしたときに、算出根拠となる基礎情報が不足していることが判明し、その情報を追加入手するためには想像以上に困難であることに気づくことがあります。特に、ある分析結果からより多角的な分析が必要になった場合、特定の情報に対する付加情報として「区分」や「属性」など、より詳細な情報が求められることがあります。このような情報は、事前に取得・保管する仕組みが備わっていなければ、その時点から遡ってデータを取得することが不可能なこともあります。また、取得可能だったとしても、多くの手間を必要とする場合もあり、そのようなデータは頻繁なモニタリングが敬遠され、結果として指標が適切な時期に算出できず、対策が遅れてしまうことにもつながりかねません。

運用・保守を開始してからトラブルとならないよう、事前に具体的なモニタリングの方法や役割分担を検討し、事業者へ依頼する場合は調達仕様書に作業内容を明記することが重要です。

また、平均値を指標とするときは、集計対象の種類や内容が同種のもので平均値を算出するよう

にし、異なる性質のものを混合して値を算出しないようにすることが重要です。

参考：主な指標とデータの関係例

No	指標名	計算式	単位
1	利用者満足度	「満足」とした回答数 / 「全有効回答数」 × 100	%
2	相談窓口の平均対応時間	相談窓口の平均対応時間	分/回
3	相談窓口における苦情・相談解決率	「相談窓口で解決した件数」 / 「全苦情・相談件数」 × 100	%
4	相談窓口におけるエスカレーション件数の遡減率	(「前年度エスカレーション件数」 - 「当該年度エスカレーション件数」) / 「前年度エスカレーション件数」 × 100	%/年
5	窓口申請に要する費用	窓口申請に要する費用	円
6	オンライン申請に要する費用	オンライン申請に要する費用	円
7	従業員満足度	「満足」とした回答数 / 「全有効回答数」 × 100	%
8	従業員苦情・相談件数	従業員苦情・相談件数	件
9	従業員苦情・相談解決までの平均時間	苦情・相談解決までの平均時間	分/回
10	削減業務処理時間	「現行業務処理時間」 - 「業務・サービス改革実施後の業務処理時間」	時間
11	削減経費	「業務・サービス改革実施前の経費」 - 「業務・サービス改革実施後の経費」	円
12	開発経費削減率	(「基準開発経費」 - 「当該開発経費」) / 「基準開発経費」 × 100	%
13	運用経費削減率	(「基準年度年間運用経費」 - 「当該年度年間運用経費」) / 「基準年度年間運用経費」 × 100	%
14	保守経費削減率	(「基準年度年間保守経費」 - 「当該年度年間保守経費」) / 「基準年度年間保守経費」 × 100	%
15	業務・サービス委託経費削減率	(「基準年度年間委託経費」 - 「当該年度年間委託経費」) / 「基準年度年間委託経費」 × 100	%
16	コンバージョン率	購入者 / サイト訪問者	%

17	売上高の増加率	「今年度総売上高」／「基準年度総売上高」	%
18	利益の増加率	(「今年度総売上」－「今年度年間経費」)／(「基準年度総売上」－「基準年度年間経費」)	%

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

業務実施部門を含めた運用体制を確立する

情報システムの各種テストが完了し、後は本番リリースを迎えるだけという状態に準備が整い、運用・保守フェーズを任せる事業者が確定したら、サービス・業務を利用者に提供するまであと一歩です。運用・保守フェーズでは、最初に司令塔となる PJMO を含んだ運用統制を行うチームを構築し、プロジェクトを管理していくことになります。円滑な運営を進めるためには、注意点があります。業務実施部門（主に当該情報システムの業務統括部門）とのコミュニケーションと役割分担です。

業務実施部門には、情報システムを用いて実際に業務を行う従業員が集まっています。この多くの従業員に、プロジェクトの目的・目標を理解してもらうことは、標準ガイドライン「第8章サービス・業務の運営と改善」で触れています。運営に入ってから次は次の点に気をつけて実施することが重要です。

業務実施部門との役割分担・コミュニケーションで気をつける点

- PJMO には、業務実施部門の担当者が参画するよう、組織を組成します。運用・保守に関わる定期報告会では業務実施部門の担当者（代表者）が参加した上で、常に情報を共有できるようにします。
- 日常的に、現場業務で発生した問題や状況に関する情報が PJMO に伝わるよう業務実施部門の担当者とのコミュニケーションルールを明確にしておきます。

業務実施部門と PJMO との関わりについては、プロジェクト立ち上げ時の PJMO の組成にまでさかのぼります。そこでは、基本的に PJMO には制度所管部門および情報システム部門とともに、業務実施部門の担当者が参画することが望ましいことが言及されています。

これまでは、新しいサービス・業務の要件を定めるために、業務実施部門の従業員から意見・要望を収集することが主でした。しかし、サービス・業務の運営フェーズになると、コミュニケーションの流れが、収集だけではなく、業務実施部門からの情報提供が加わります。

利用者からの意見や要望を把握するためには、最も接点が多い業務実施部門の従業員からの情報提供が欠かせません。また、運用・保守で発生した報告内容には、利用者からの問い合わせや発見した不具合、不具合修正に伴う情報システムの稼働停止連絡など、さまざまな情報が含まれます。これらを業務実施部門と共有することにより、業務実施部門の中で必要な調整や対策を行い、今後問題を引き起こすリスクを低減させることが可能となります。

そのためにも、プロジェクトの情報が集まる PJMO への参画、定期報告会への必要な人員の出席、代表者から業務実施部門の関係者全員への情報伝達手段などを、運用および保守が開始する前に取り決めておくことが重要です。

障害発生時の役割分担に注意する

障害が発生しない情報システムは、ほぼありません。大切なのは、障害が発生した際に適切な対応をとることで被害を最小限に留め、暫定対策から恒久対策を実施し、将来にわたって同じまたは同じような障害を発生させないようにすることです。そのためには、障害対応という急を要する状況の中でも、PJMO、運用の事業者、保守の事業者、そのほかの関係者が適切な役割分担の下に協働して対応を進めていくことが必要になります。運用と保守の事業者が異なる場合や、運用・保守それぞれを複数事業者で分担して実施する場合もあり、役割や責任が曖昧になることで対応が遅くなってしまうことや被害が拡大してしまうことも多いです。

まずは、障害発生時における運用と保守の基本的な役割分担を理解することが重要です。この考え方を踏まえた上で、プロジェクトの体制や特性を踏まえて、詳細を決めていきます。

極端な例ですが、PJMO の体制が 1 名の場合は、24 時間 365 日稼働するサービスへの対応は十分にできません。どのようなタイミングで障害が発生するかは予想できないからです。深夜や休暇取得中など、PJMO が対応できない状況が存在することを前提に、運用事業者・保守事業者と役割分担を検討する必要があります。

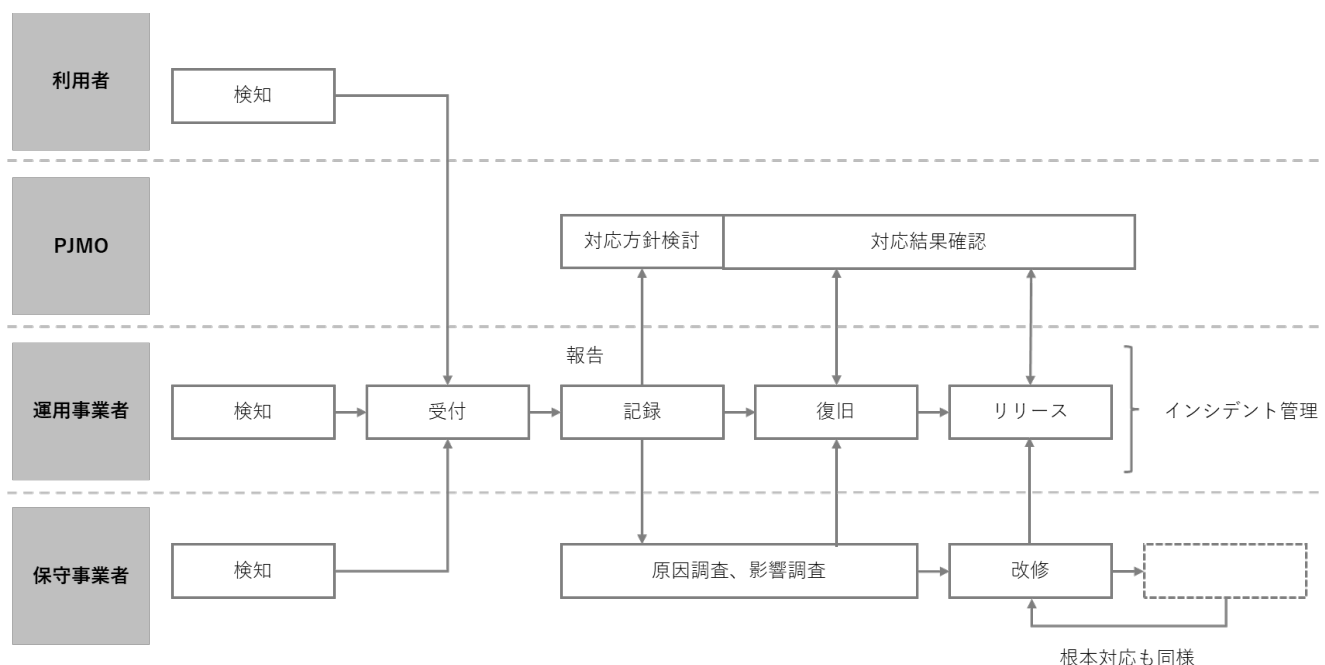


図 80. 障害発生時の運用と保守の役割分担の例

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

「運用および保守」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第9章 運用および保守 Step3 運用・保守の計画

第3編 第9章 運用および保守 Step5 運用・保守の改善と業務の引継ぎ

セキュリティ機能を実装・運用するためポイント

セキュリティ関連作業を定期的に確実に実施すること

セキュリティ管理に関する要件は、非機能要件で示され、運用・保守フェーズでは、その方針に沿ってアプリケーションやインフラでの対策が講じられている状態にあります。昨今のセキュリティに対する脅威は日々増大しており、運用・保守フェーズでは、設計どおりの対策が維持できるよう、日々確実に作業を続ける必要があります。

以下に定期的に実施すべき作業の例を挙げます。

- [セキュリティインシデント](#)発生時の記録、対応、影響範囲の把握
- 脅威と修正パッチ適用計画の立案・調整
- シグニチャ、ブラックリスト（ホワイトリスト含む）の更新
- OS およびプラットフォームなどの緊急修正計画の立案・調整
- セキュリティ向上のための業務改善と利用規制検討
- 中長期的プラットフォーム改善に向けた、システム構成要素の[リスク評価](#)

セキュリティ対策会議の実施

運用・保守フェーズは、複数の従業員や事業者が関わるため、会議体の種類がどうしても多くなる傾向があります。中心的な役割を担う PJMO の従業員や事業者の担当者は、会議出席に拘束されてしまい、本来行うべき作業に手が回らないという状況に陥りがちです。そのような状況にならないために、会議体の目的を整理し、必要な出席者を事前に選抜することが重要です。

- 会議の例：セキュリティ対策会議（月次～四半期）
- 主な目的・内容：
- インシデント発生状況の共有
- 脅威と修正パッチ計画の調整
- シグニチャ、ブラックリスト（ホワイトリスト含む）の更新調整
- OS およびプラットフォームなどの緊急修正計画調整
- セキュリティ向上のための業務改善と利用規制検討・承認

情報システムのアカウントの管理

発注者が運用・保守事業者に対して一定期間の運用・保守実施記録の保管を指示していないなど、情報システムのアカウント管理を運用・保守事業者に丸投げしている場合には、いざという時に必要な記録が参照できず、不正、障害などの原因が究明できないなどの問題が生じる可能性があります。

上記のリスクを低減する方法として、情報システムのログやトランザクションデータを適切に取得・保管することなどが挙げられます。

機密性・完全性・可用性の観点から特に重要な情報を取扱う場合においては、発注者が特権 ID 管理を適切に実施することが重要で、事業者の作業計画に基づいて作業のたびに特権 ID を発注者が事業者が付与する運用とすることが望ましいです。

アカウントの管理や情報の保管は、情報システムの特性に応じて、「政府情報システムにおけるセキュリティ・バイ・デザインガイドライン」や特定非営利活動法人日本ネットワークセキュリティ協会の「【改定新版】特権 ID 管理ガイドライン」を参考にしながら、事前に十分に検討した上で、実施してください。

※特権 ID とは：

特権 ID とは、情報システムを運用・管理するために必要なすべての操作権限を持つ管理者用アカウントのことです。悪意を持った人が特権 ID を使用した場合、不正やセキュリティ上のリスクなどが懸念されるため、発注者の責任下で、特権 ID の取扱いには十分に注意が必要です。

詳細理解のため参考となる文献（参考文献）

DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf
【改定新版】特権 ID 管理ガイドライン	https://www.jnsa.org/result/digitalidentity/2024/index.html

20-1-10. システム監査

システム監査の全体の流れは以下の通りです。

システム監査の全体の流れ

システム監査の理解

システム監査を行う前に、理解すべき監査の目的・活動や、必要な事前準備の内容について理解します。

1. システム監査とは何かを理解する

- A. 監査の種類を理解する
- B. システム監査は問題解決の近道となる
- C. システム監査基準・システム管理基準を理解する

2. システム監査の全体像を理解する

3. 適切な監査が行える体制を作る

システム監査計画と監査実施計画

監査体制は、組織全体のシステム監査計画をもとに対象のプロジェクトを監査するための実施計画を立案します。

1. 複数年の監査計画を立てる

2. システム監査実施計画書を作る

- A. 監査範囲が局所的にならないように注意する
- B. 監査実施方法に注意する

システム監査の実施

監査体制は、システム監査実施計画に則りシステム監査を実施します。

1. 予備調査を踏まえ監査手続きを具体化する

- A. 監査手続書を作成するまでの流れをつかむ

2. 根本原因を究明し改善点を発見する

- A. インタビュー時には情報を上手に引き出す
- B. 改善提案は報告の場で具体的な例を混ぜながら行う
- C. システム監査報告書の様式を把握する

指摘事項を踏まえた改善

[PJMO](#) は、監査実施者からのシステム監査報告書の指摘を踏まえて改善を行います。

1. 改善計画を立て改善を行う

中小企業においても適用することが有効な工程を例にとり、概要と実践に当たっての留意点を説明します。

例：システム監査の理解

監査の種類を理解する

「監査」と聞くと、会計検査院が実施する会計検査や、会社法、金融商品取引法に基づく財務諸表監査を思い出すかもしれません。これらは、会計監査に当たります。標準ガイドラインで扱うシステム監査は、業務監査の一部に位置づけられます。また、監査人が誰かにより監査が分類されることもあります。その分類においては[内部監査](#)に当たります。

また、システム監査と混同しがちな監査に、情報セキュリティ監査があります。情報セキュリティ監査は、元々はシステム監査における監査テーマの一つであり、近年、情報漏えいなど、多くの情報セキュリティに関する事件・事故が多発してきた結果として、情報セキュリティに特化した監査として定着してきているものです。



図 81. 一般的な内部監査における各監査の関係性

(出典)「デジタル・ガバメント推進標準ガイドライン 実践ガイドブック」をもとに作成

システム監査は問題解決の近道となる

システム監査は、中小企業においてもプロジェクトの目標達成を確実にするための重要な活動です。日々の業務に追われ、効率重視のあまり、プロジェクト本来の目的を見失うことがあります。例えば、当初の目的から逸れて手段が目的化してしまうこともあります。このような状態を放置してしまうと、情報システムが意図したどおりに構築・改修されない、不必要な機能構築や人件費の積算、不適切な業務・システム運用の定着、情報漏えいなど、さまざまなリスクが発生し、プロジェクト目標が達成されないおそれがあります。

システム監査は、これらのリスクを未然に防ぐため、プロジェクトの進行状況を客観的に点検・評価し、改善するための活動です。これは、PDCA サイクルにおける「C」（チェック）に該当します。

システム監査では、単に「不具合が発生しているから問題だ」という表面的な評価ではなく、その原因を突き止めます。例えば、「不具合を解決するためのプロセスや体制に問題がある」、「不具

合が発生しやすいプロセスになっている」などの根本的な原因を評価します。

どのような目的で監査を行うか、何を評価するかは、組織内の担当者が決定し、システム監査の組織全体に対する計画である「システム監査計画書」としてまとめます。監査の対象となるプロジェクトもこの中で定めます。

監査の実施に当たってのポイント

規模が小さい企業の場合、大企業（あるいは政府機関）のような内部監査体制を整えることは、事実上困難です。無理にそのような体制を構築すると、中小企業の長所である「小さな組織ならではの効率性」「経営者と従業員の一体感」「迅速な意思決定」「市場などの変化に対する迅速な対応力」などが損なわれる可能性があります。

中小企業が監査を実施するためのポイントを3つ紹介します。

- 経営者の主導と外部専門家の活用

内部監査のもつ意味を正しく理解した経営者自身が監査を行うか、または必要に応じて経営者から委託された外部の専門家（会計士、システム監査士など）を活用することで、効果的な監査を実施できます。

- シンプルで実用的な監査プロセスの導入

チェックリストや定期的なレビューなど、簡易的で中小企業に適した監査プロセスを導入するなど、無理なく監査を継続する仕組みを作ることも効果的です。

- 法令順守とリスク管理に重点を置く

法令順守（コンプライアンス）とリスク管理を中心に監査を行い、企業の安全性と持続可能性を確保することも効果的です。

「システム監査」において、中小企業でも意識すべき重要な観点の詳細は、「DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の以下の箇所を参照してください。

中小企業が意識すべき観点

第3編 第10章 システム監査 Step.2 システム監査の理解

セキュリティ機能を実装・運用するためポイント

情報セキュリティ監査

情報セキュリティ監査は、元々はシステム監査における監査テーマの一つであり、近年、情報漏えいなどの多くの情報セキュリティに関する事件・事故が多発してきた結果として、情報セキュリティに特化した監査として定着してきているものです。

20-2. アジャイル開発

20-2-1. アジャイル開発の概要

アジャイル開発の必要性

現代は、人や組織を取り巻く環境が、複雑さを増し、将来の予測が困難な VUCA (ブーカ) (VUCA: Volatility (変動性)、Uncertainty (不確実性)、Complexity (複雑性)、Ambiguity (曖昧性)) の時代」だといわれています。

複雑な問題を解決する論理的に導ける最適解はありません。従来のような問題を分析して解決する方法ではなく、観察とフィードバックによってあるべき姿に向けて改善、進化し続ける必要があります。こうした背景から「アジャイル開発」が注目されています。

当初アジャイル開発は、ソフトウェアエンジニア主体の開発手法でしたが、近年は不確実さに対応するビジネス戦略としても採用されています。つまり「アジャイル開発」の考え方は、ソフトウェア開発だけでなく、ビジネス戦略などにも活用できるものになっています。

アジャイル開発とは

アジャイル (Agile) とは、直訳すると「敏捷」「素早い」などの意味を持ちます。アジャイル開発は、新しい機能を短時間で継続的にリリースするソフトウェア開発のアプローチです。従来のアプローチ方法は、試行錯誤に向いていません。そのため、状況変化への対応を繰り返す適応するアプローチ方法であるアジャイル開発が有用であると考えられます。

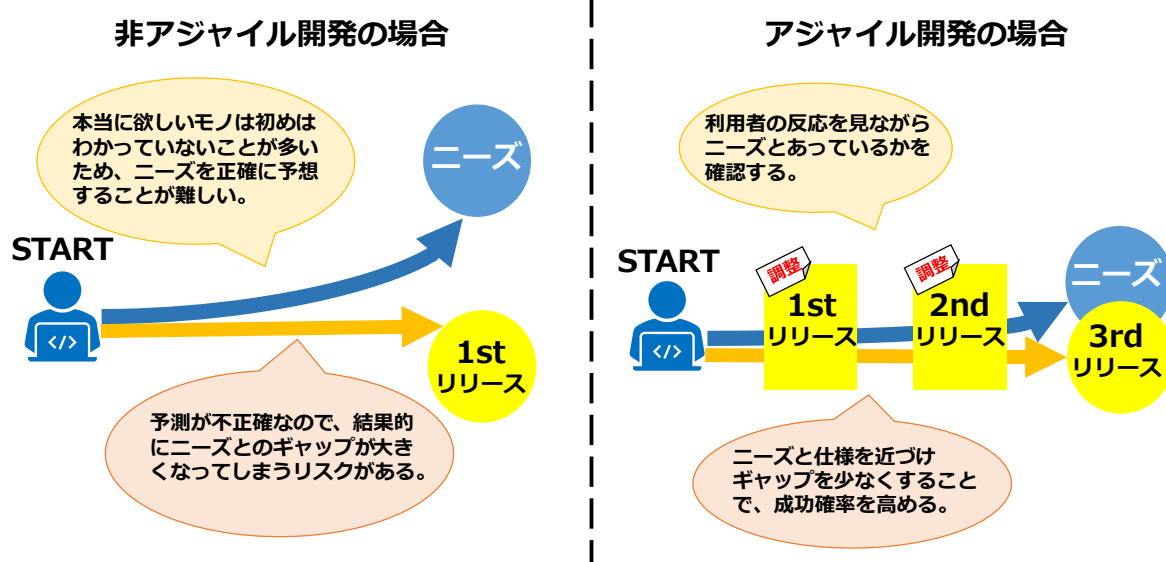


図 82. 非アジャイル開発とアジャイル開発の違い

アジャイル開発では、作成したアウトプットの基づき、情報システムの挙動がどうあるべきかを検討、判断し、その次に取り掛かる開発行為を最適化します。また、アジャイル開発は従来の開発スタイルとは異なり、すべての要求、仕様を言語化し、事前のドキュメントとして整備することなく開発を行うこともできます。ドキュメントで定義しなくとも、短期間のスプリントで得られるアウトプット（インクリメント）が、動くシステムそのものとなり得るためです。ドキュメントの作成にかかる手間を最小限に留め、情報システムそのもので動作確認を行うことで、要求の確認から設計、開発、テストまで、情報システムの機能追加を短い期間で行うことができます。また、アジャイル開発には、下記のような意義があります。

アジャイル開発の 9 つの意義

- ① フィードバックに基づく開発で、目的に適したシステムに近づけていく
- ② 形にすることで、関係者の認識を早期に揃えられる
- ③ システム、プロセス、チームに関する問題に早く気づける
- ④ チームの学習効果が高い
- ⑤ 早く開発を始められる
- ⑥ システムの機能同士の結合リスクを早期に解消できる
- ⑦ 利用開始までの期間を短くできる
- ⑧ 開発のリズムが整えられる
- ⑨ 協働を育み、チームの機能性を高める

前述の 9 つの意義を十分発揮するためには、以下の前提をチームおよび関係者間で確認する必要があります。前提を理解して取り組むことでスムーズに進めることができます。

9 つの意義を十分に発揮するための前提

- ① 常にカイゼンを指向すること
- ② 対話コミュニケーションの重視
- ③ 情報システムの変更容易性を確保し続ける
- ④ 利用者目線で開発を進める

詳細理解のため参考となる文献（参考文献）	
DS-121 アジャイル開発実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf

20-2-2. アジャイル開発の実施ポイント

アジャイル開発を実践するに当たり、まずはプロセスを理解することが大切です。アジャイル開

発の代表格であるスクラムを例に、アジャイル開発のプロセスを説明します。

ポイント

- アジャイル開発は経験者が参画することを前提とします。アジャイル開発に関する資格を有している場合も、一定の知識を有していることは判断できますが、アジャイル開発を実践できるかを判断することができません。参画者がどのようなシステム開発において、どのような役割を果たしたのかを確認することが重要です。
- アジャイル開発の進め方には厳格な決まりごとや規範はありません。本書で説明（例示）する進め方、メンバーの役割（ロール）など、実際のソフトウェア開発プロジェクトでそのまま適用するものではありません。アジャイル開発の基本を習得したのち、実際のプロジェクトや組織に適したやり方を取捨選択し、カスタマイズすることが必要となります。
- 「唯一の正しい」アジャイル開発というものはありません。自分のいる組織に合ったやり方が、その組織のビジネスや活動、文化から自然と育っていくことがアジャイル開発の本質です。

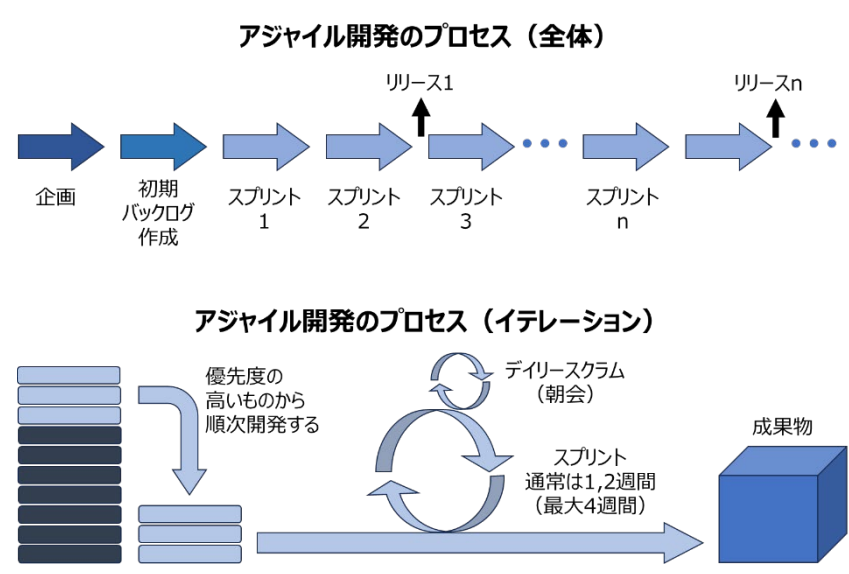


図 83. アジャイル開発のプロセス（スクラムの例）

スクラムのプロセス	特徴
1.プロダクトバックログの作成	プロダクトオーナーがプロジェクトの全体的な要件や機能をリストアップします。このリストは「プロダクトバックログ」と呼ばれ、優先順位がつけられます。
2.スプリントプランニング	チームはスプリント（通常 1～2 週間、長くても 4 週間）ごとに作業する項目を選びます。この選ばれた項目のリストは「スプリントバックログ」と呼ばれます。

3.デイリースクラム (デイリースタンドアップ)	毎日、チームは短いミーティングを行い、進捗状況を共有し、問題点を解決します。このミーティングは通常 15 分以内で行われます。
4.スプリントの実行	チームはスプリントバックログに基づいて作業を進めます。各メンバーは自分のタスクに集中し、協力して目標を達成します。
5.スプリントレビュー	スプリントの終わりに、チームは完成した作業をプロダクトオーナーやステークホルダーにデモンストレーションします。フィードバックを受け取り、次のスプリントに反映させます。スプリントごとにリリースを行うことが理想ですが、業務向けアプリケーションの場合には、エンドユーザーの混乱を避けるため、ある程度まとまった成果物ができた段階でリリースする（複数回のスプリント後にリリースする）ことが多いようです。
6.スプリントレトロスペクティブ	チームはスプリントの振り返りを行い、何がうまくいったか、何が改善できるかを話し合います。このフィードバックをもとに、次のスプリントでの改善策を考えます。

役割（ロール）の名称	役割
プロダクトオーナー	プロダクトのビジョンを持ち、バックログの優先順位を決定します。
スクラムマスター	チームがスクラムのプロセスを正しく実行できるようサポートし、障害を取り除きます。
開発チーム	実際に開発作業を行うメンバーです。
ステークホルダー	エンドユーザー、経営者、総務・経理・法務部門などです。

詳細理解のため参考となる文献（参考文献）	
アジャイル領域へのスキル変革の指針 アジャイル開発の進め方	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

第21章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

章の目的

第 21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明します。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を理解することを目的とします。

主な達成目標

- ❑ 実施例から工程を理解することで、中小企業が主体的に関与するポイントを理解すること
- ❑ 情報システムを導入する工程で、作成すべきドキュメントを理解すること
- ❑ 情報システムを導入する工程の中で、セキュリティ機能を実装、運用するポイントを理解すること

21-1. EC サイトの構築とセキュリティ機能の実装と運用

「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する方法と、セキュリティ機能を実装する方法について説明します。具体的に説明するために、EC サイトの導入を例にとって説明します。

EC サイト導入における全体概要は以下の通りです。

サービス・業務企画
EC サイトの事業目的と提供するサービスの具体的な方向性を定めるフェーズです。 ● サービスの利用者の種類やニーズを特定します。(ペルソナ分析など) ● 現状の業務フローを分析し、サービスの改善点を明確にします。
要件定義
サービスの実現に必要な機能と非機能の要件を定義します。 ● 業務要件と機能要件を定義します。 ● Fit&Gap 分析を実施します。
調達
EC サイト開発に必要なリソースや外部業者を調達します。 ● 調達仕様書を作成します。 ● 適正価格で最適な業者を選定します。
設計・開発
プロジェクトの計画立案とその管理を行います。 ● 設計・開発実施計画書を作成します。 ● テストを管理し、また自社で品質を確認するために受入テストを実施します。
サービス・業務の運営と改善
サービスを運営しながら、必要に応じて改善を行います。 ● EC サイト運営における業務マニュアルを作成します。 ● 研修教育資料（業務マニュアルなど）を用いて、従業員に対して教育を実施します。
運用および保守
システムの安定稼動を維持しつつ、継続的な改善を行います。 ● 運用・保守の詳細な作業内容や実施方法などを検討します。 ● 運用・保守の改善を継続的に実施していきます。

セキュリティに関する要件は、適用宣言書をもとに行います。セキュリティに関する要件を決める流れは以下の通りです。

1. 情報システムで取扱う情報資産に対して、リスクアセスメントを実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。(適用宣言書の作成)
3. 適用宣言書の内容を満たすように、非機能要件などでセキュリティ要件を決定する。

※セキュリティ要件の詳細は「21-1-2.要件定義」で説明します。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

21-1-1. サービス・業務企画

本工程は、規模に関わらずすべての企業にとって重要です。顧客ニーズを理解し、現状の業務を分析した上で、新しいサービスや業務プロセスを計画することは、中小企業の成長と効率化に直結します。

利用者視点でのニーズ把握

サービスを検討するための大前提として、利用者の立場でサービスを受けることを想像し、利用者のニーズがどこにあるかを考えることが大切です。しかし、サービスを提供する側は、どうしても「提供者側の視点」に立ちがちになります。さまざまな利用者のそれぞれの立場でニーズを把握するための手法の1つとして、「ペルソナ分析」があります。

ペルソナ分析

「ペルソナ」とは、サービスの典型的な利用者の、目的、意識、行動などのパターンを構造化し、利用対象者を仮想の人物として定義するものです。例えばサービスのターゲットを「会社員」と抽象的に定義すると、検討チームのメンバーそれぞれが思い描く「会社員」の姿が異なるため、チームとして判断する際にブレが生じてしまいます。ペルソナ分析ではもっと具体的に「氏名、年齢、性別、家族構成、勤務先、仕事内容、そのほかの詳細条件」などを設定します。このような具体的な利用者像をイメージしながら検討を行うことで、利用者が抱える課題や問題を浮き彫りにし、具体性の高いアイデアを創出しやすくなります。

ペルソナの作り方

以下の企業を想定としたペルソナ作成の例を紹介します。

- 地方の特産品を扱う中小企業を想定
- 実店舗がある。
- EC サイトは現在なく、これから構築しようと検討している。

- 実店舗に加えて、販売窓口を増やしたいと考えている。

1.ターゲットとなる利用者に関する情報を収集する

- インタビュー・アンケート

実店舗の来店者に対して、購入動機、どのような商品をオンラインで購入したいか、どのような購入体験を期待しているかを尋ねる。実店舗での顧客に対して、購入理由、購入頻度、地域とのつながりなどをアンケートにより収集する。

- Web 検索や公開調査データ

EC サイトを利用する層（地域外の顧客や新規顧客）について、公開されている市場調査データを収集。

- 店舗の観察・ヒアリング

店舗スタッフからのヒアリングにより、どのような顧客層が頻繁に訪れているのかを確認。

2.収集した情報を分析し、グルーピングする

- 地域住民か観光客か

地域に住んでいるリピーター、観光目的で訪れた一見の顧客。

- 年齢層

若年層、中年層、高齢層

- 購入動機

日常の食材としての購入、贈答品としての購入、観光の記念品としての購入。

- 利用方法

実店舗での対面購入、電話注文、リピーターによる定期購入。

3.グルーピングした情報から利用者像を具現化、ペルソナを作成

ペルソナの例：「地域住民のリピーター」

名前	山田 花子（45 歳）
職業	地元の学校で働くパートタイムスタッフ
居住地	店舗のある地方都市
家族構成	夫と高校生の娘 1 人
趣味	地元のイベントや料理教室に参加すること
価値観	地元の発展に貢献することを大切にしており、地元産品の購入を積極的に行う。 安全で新鮮な食品を求めるため、実店舗で直接商品を見て購入することに安心感を得ている。

利用動機	日常の食材として地元の特産品を購入。特に週末に家族で食事を楽しむため、実店舗で定期的に訪れて新しい商品を見つけるのを楽しみにしている。
購入経路	現在は実店舗での対面購入を利用。EC サイトが構築されれば、忙しいときでもオンラインで注文し、自宅での受け取りや店舗での受け取りができることに興味を持っている。

ペルソナの案を作成後、ターゲットとなる利用者と直に接している人などに、実際の利用者像とかけ離れたところがないか、ターゲットたる利用者としてふさわしいかを確認してもらいます。実際の利用者像と作成したペルソナにかい離が見られた場合は、随時内容を修正してください。

業務の現状把握

業務を観察した結果は、多くのドキュメントとしてまとめられることがあり、分析に関わった人は内容を理解できますが、初めて読む人にはポイントを把握することが難しいことがあります。プロジェクト内部の従業員や外部の関係者、システム開発事業者など、多様な立場の人が内容を確認する必要があるため、業務の状況を誰にでもわかりやすく伝えるために、業務フローなどを用いた視覚的にわかりやすい資料を作成することが重要です。

業務フローの作成

業務フローは、現在行っている業務を「誰が（どの組織が）」「いつ」「何を」「どの順番で」実施しているか、「どの範囲が情報システム化されているか」を可視化するものです。対策の検討や企画後の業務内容の変化箇所を特定するためにも有効です。

業務フローには、現行（AsIs）と将来（ToBe）があります。はじめに作成するのは、現行の業務フローです。業務フローの書き方については、さまざまな表記方法があります。基本的に、関係者にとってわかりやすい表記であれば、どのような表記方法でも問題ないです。縦に流れるフローでも、横に流れるフローでも、どちらでも構いません。

例：お客様が実店舗で商品を購入するフロー

- 地方の特産品を扱う中小企業を想定
- 実店舗での商品購入フロー

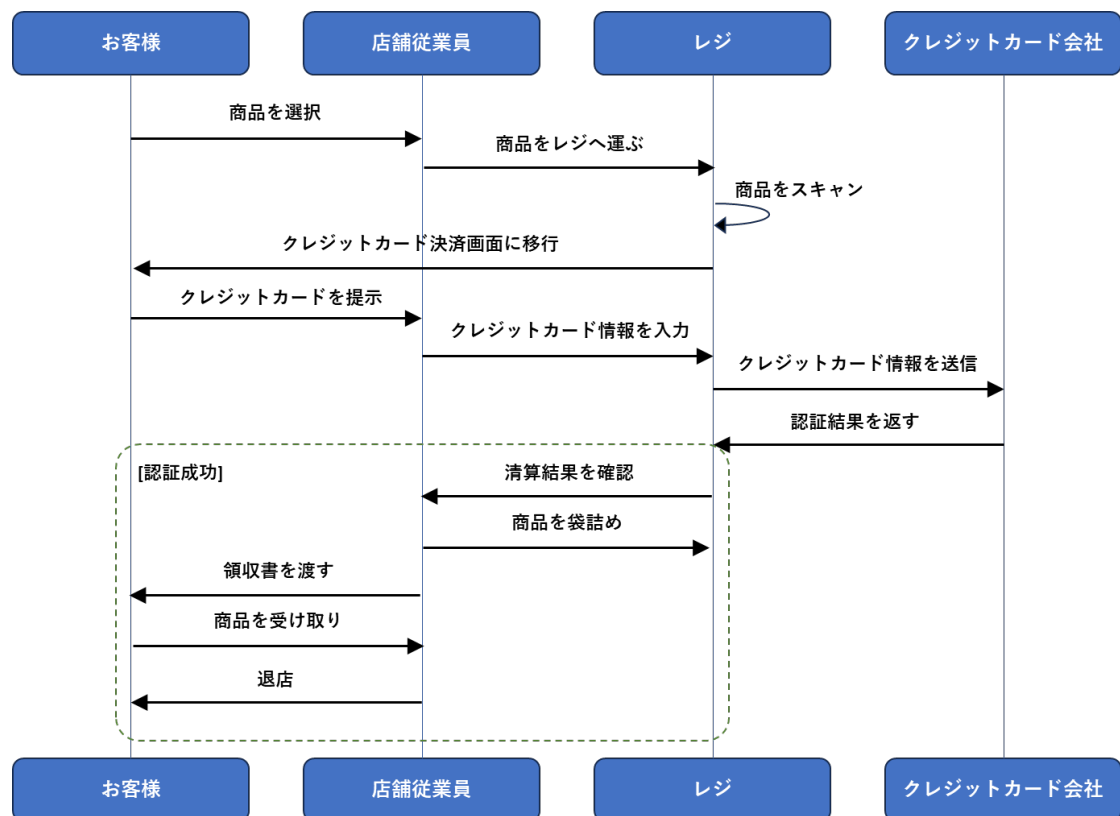


図 84. 実店舗で商品を購入するフロー例

サービス・業務企画内容の検討

現状把握が終わった後は、企画案を練り上げます。企画案の方向性がある程度決まったら、プロジェクト内外の関係者にわかりやすく説明し、改善点のフィードバックを受け取るために、将来（ToBe）の業務フローを活用します。現行（AsIs）の業務フローをもとに、将来どこがどのように変わるのかを明確に示し、変更点とその効果を具体的に示します。関係者と目指す姿を共有できるようにするために、業務フローに吹き出しを付けることは効果的です。

例：お客様が EC サイトで商品を購入するフロー

- 地方の特産品を扱う中小企業を想定
- 実店舗での商品購入フローをもとに、EC サイトでの購入フローを作成

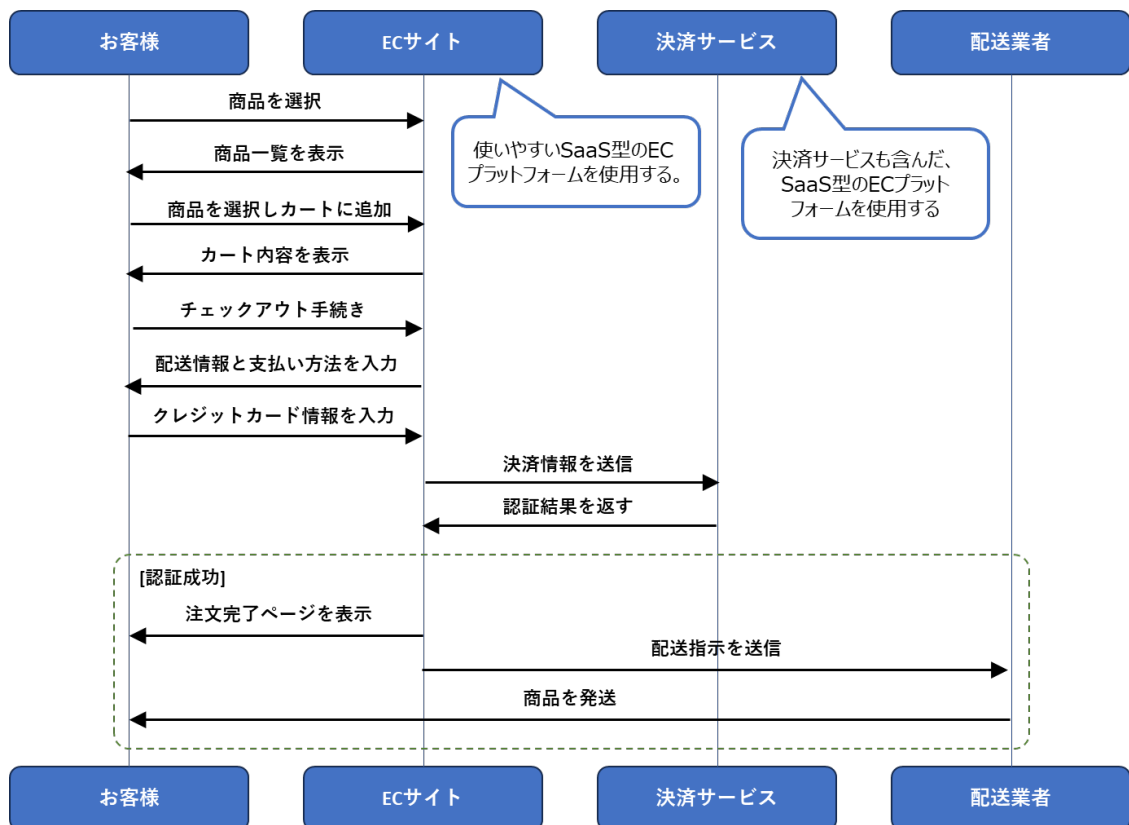


図 85. EC サイトで商品を購入するフロー例

21-1-2. 要件定義

RFI や事業者からの情報収集といった活動を通して、市場にあるサービスや他社の事例などを把握します。その上で、情報システムを導入する際、明確な要件を定義することは中小企業にとっても非常に重要です。必要な機能を確実に実装し、パフォーマンスや信頼性などの非機能要件も満たすことができます。

セキュリティに関する要件については、適用宣言書に基づいて決定することが重要です。

一貫性を持った要件定義書の作成

要件定義の内容を記した文書は、プロジェクト管理を行うチームや担当者と事業者がサービス・業務や情報システムの目指すべき姿を共有するとともに、事業者との契約上の合意文書となる重要なものであるため、誤った定義や曖昧な定義が行われると、後続の工程に重大な影響を与えます。

そのため、要件定義の内容は次に示す点を参考に、正確で一貫性のある記載となるようにし、受託業者の解釈によりブレない内容とすることが重要です。

- 曖昧な用語や一般的な意味と異なる使い方をしている用語などは、プロジェクト関係者間での認識の齟齬を防止するため、用語の定義および機能を定義する粒度や深さについて統一する。

- 要件定義書の「業務要件定義」のインプットであるサービス・業務企画の内容とも整合の取れた区分、順番で機能を記載する。業務の単位ごとに記載する場合も、共通処理機能を識別できるように整理するなど、機能数を把握できるように記載する。
- 機能の説明は、箇条書きなどにして簡潔に記載する。既存のサービス・業務や情報システムの変更を行う際の要件定義では、追加・変更となる要件が明確になるよう、変更箇所の記載ルールを定めて記載を統一する。

機能要件の定義

機能要件として定義しないといけない内容は5つです。

- 機能
- 画面
- 帳票
- データ
- 外部インターフェース

要件定義の対象となる情報システムによっては、このうちの一部を定義しない場合もあります。例えば、他の情報システムと連携しない Web サイトであれば外部インターフェースの定義は不要となります。

機能に関する事項

「機能」とは、情報システムが外部に価値を提供する一連の動作のまとまりのことです。基本的に「入力」・「演算（処理）」・「出力」で構成されます。ボタンを押したら画面に情報が表示されるのも、夜間にバッチ処理で帳票が大量に印刷されるのも、それぞれ1つの機能です。情報システムが提供する形はさまざまですが、それらを「機能」としてリスト化して整理するために用いるものが、「情報システム機能一覧」と呼ばれるドキュメントです。

情報システム機能一覧（例）

NO	機能ID	機能分類	機能名	機能概要			処理方式	利用者区分	現状の機能との差異
				入力	処理	出力			
1	XXX	新規ユーザー登録	新規ユーザー登録機能	記載事項の入力	・・・	・・・	オンライン	新規登録申込者	・・・
2	XXX	新規ユーザー出力	新規ユーザー出力	出力方式の選択	・・・	新規登録申込書の	オンライン	新規登録申込	・・・

			機能			出力		者	

画面に関する事項

情報システムの画面は、利用者が業務の流れの中で情報システムとやり取りを行う窓口となるため、画面上で取扱う情報の種類、画面を構成する要素の配置は、利用者の業務効率や満足度に大きな影響を与えます。

この画面に関する要件を取りまとめるドキュメントは、一般的に画面一覧、画面イメージ（画面モックアップ）、画面遷移図、画面設計方針書（画面設計ポリシー）と呼ばれるもので構成されています。

画面一覧（例）

NO	画面ID	画面分類	画面名	画面概要	画面入出力要件	画面設計要件	該当機能	利用者区分
1	XXXX	新規ユーザー登録画面	新規ユーザー登録作成	新規ユーザー登録の作成画面	表示方法： … 入力操作概要：…	Webブラウザで表示可能であること。	機能ID：XXXX	新規ユーザー
2	XXXX		新規ユーザー登録確認	新規ユーザー登録の作成確認画面	表示方法： … 入力操作概要：…	…	機能ID：XXXX	新規ユーザー

帳票に関する事項

情報システムの帳票とは、サービス・業務で使用するために情報システムから出力した紙やPDF形式などの電子帳票を指します。帳票は、利用者が業務上意識して用いられるものであるため、業務の内容やきっかけと結びついた重要な情報を持ちます。帳票に関する要件を取りまとめるドキュメントは、一般的に帳票一覧、帳票イメージ、帳票設計方針書（帳票設計ポリシー）と呼ばれるもので構成されています。

帳票一覧の例

NO	帳票ID	帳票名	帳票概要	入出力の区分	帳票入出力要件	帳票設計要件	入出力形式	該当機能	利用者区分
1	XX	〇〇申	〇〇	出力	モノクロ	用紙サイズ：	紙	機能ID：	〇〇申

		込書	申込		印刷	A4		XX	込者
2	XX	△△申 込書	△△ 申込	出力	カラー印 刷	用紙サイズ： A4	PDF	機能 ID： XX	△△申 込者

データに関する事項

情報システムで取扱うデータに関して機密性レベル別に分類し、その管理方法を定義しておく必要があります。システム内に存在することになるデータに関して、その機密性を認識し、分類し、またその管理方法を「データ要件」として記述することにより、その後の設計・開発作業に確実につなげていくことができます。データに関する要件を取りまとめる際には、データモデル、データ一覧、データ定義などのドキュメントを整備することが重要です。

データ要件を取りまとめる際に整備するドキュメント（例）

NO	ドキュメント名	説明
1	データモデル	- 画面や帳票などに含まれる情報を抜き出して、意味のある単位（識別キー）ごとにまとめた情報の集合体である「データ」と、他のデータとの関連を1枚に表現した図で、ER（Entity Relationship）図という表記法で記述します。 - 基本的に1つのデータ項目は、必ずどこか1ヶ所のデータのみに属するようにデータを定義します（これを「正規化」といいます）。
2	データ一覧	- データがどのようなまとまりの単位になっているかを一覧形式で示す表で、データモデルやデータ定義の目次として利用されます。 - マスターデータとマスターデータ以外に分け、データの用途や保存期間、データ件数などを定義します。
3	データ定義	データ一覧にあるデータのまとまり単位にそれぞれに含まれるデータ項目の内容・説明を示す表です。

外部インターフェースに関する事項

情報システムの外部インターフェースとは、サービス・業務の内容を実現するために、自分の情報システムが他の情報システムと連携して情報を受け渡す仕組みです。情報連携の内容や形式・仕組みにはさまざまなものがあり、明確に定義する必要がありますが、連携先である他の情報システムの都合もあるため、双方の要件を出し合い、すり合わせる必要があります。この外部インターフェースに関する要件を取りまとめるドキュメントは、一般的に外部インターフェース一覧と呼ばれます。

外部インターフェース一覧（例）

NO	外部インターフェース ID	外部インターフェース名	外部インターフェース概要	相手システム	送受信区分	実装方式	送受信データ	送受信タイミング	送受信の条件
1	XXXX	申込者情報連携	申込の審査に関わる申請者の情報を〇〇システムから日次で取得する	〇〇システム	受信	API	申込者情報	リアルタイム	日次
2	XXXX	申込結果連携	承認された申込情報を〇〇システムに日次で提供する。	〇〇システム	送信	ファイル共有	承認済み申込者情報	リアルタイム	日次

非機能要件の定義

非機能要件として定義しないといけない内容は次に挙げる 17 の事項です。

非機能要件は、安定的なサービスの継続に重要です。

- 情報セキュリティに関する事項
- ユーザビリティおよびアクセシビリティに関する事項
- システム方式に関する事項
- 規模に関する事項
- 性能に関する事項
- 信頼性に関する事項
- 拡張性に関する事項
- 上位互換性に関する事項
- 中立性に関する事項
- 継続性に関する事項
- 情報システム稼動環境に関する事項
- テストに関する事項
- 移行に関する事項
- 引継ぎに関する事項
- 教育に関する事項
- 運用に関する事項

- 保守に関する事項

機能要件の場合は、内容の一部を定義せず、調達時の事業者の提案に委ねることもあります。しかし、非機能要件の場合は基本的にすべての項目を定義します。情報システムやプロジェクトの特性によって、定義すべき内容の量は異なります。

情報セキュリティに関する事項

セキュリティに関する要件の決定は、適用宣言書をもとに行います。セキュリティ要件を決める流れは以下の通りです。

1. 情報システムで取扱う[情報資産](#)に対して、[リスクアセスメント](#)を実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。（適用宣言書の作成）
3. 適用宣言書の内容を満たすように、セキュリティ要件を決定する。

※リスクアセスメントの実施方法の詳細については、「12-2.リスクマネジメント：リスクアセスメント」を参照してください。

EC サイトにおいて、セキュリティ要件を決める例

1. リスクアセスメントの実施

ステップ 1：情報資産の特定

EC サイトで取扱う主な情報資産は以下の通りです。

情報資産名	内容
顧客情報	氏名、住所、電話番号、メールアドレス、クレジットカード情報など
注文情報	商品名、購入日、購入金額など
在庫情報	商品の在庫数、入荷予定など
支払い情報	クレジットカード情報、銀行口座情報など

ステップ 2：リスク特定

各情報資産に対する脅威と脆弱性を特定します。

情報資産名	脅威	脆弱性
顧客情報	データの漏えい、フィッシング攻撃	弱いパスワード、 暗号化 されていないデータ通信

注文情報	改ざん 、 不正アクセス	セキュリティパッチの未適用、不適切なアクセス権限管理
在庫情報	データの改ざん、誤った更新	適切な監査ログがない、 アクセス制御 の欠如
支払い情報	クレジットカード情報の盗難、不正取引	PCI DSS に準拠していないサービスの利用、暗号化されていないストレージ

ステップ 3 : リスク分析

脅威と脆弱性がもたらすリスクを評価し、リスクレベルを「高」「中」「低」に分類します。

情報資産名	リスクレベル
顧客情報の漏えい	高
注文情報の改ざん	中
在庫情報の誤った更新	中
支払い情報の盗難	高

ステップ 4 : リスク評価

リスク分析の結果をもとに、リスクの優先順位を決定し、それに対する対応策（リスク軽減、リスク回避、リスク受容など）を検討します。

2.適用宣言書の作成

リスクアセスメントの結果に基づいて、管理策を導入する適用宣言書を作成します。

※管理策は、[ISMS](#) の管理策だけでなく [CSF2.0](#) の管理策も参考にできます。CSF2.0 の管理策については、「付録 : CSF2.0」を参照してください。

情報資産	リスク内容	リスクレベル	適用する管理策
顧客情報（氏名、住所、電話番号、メールアドレス、クレジットカード情報）	不正アクセスによる個人情報の漏えい	高	情報セキュリティのための方針群（5.1） 個人情報の取扱いに関する方針を策定し、従業員に周知。 アクセス制御（5.15） 顧客情報へのアクセス権を最小限に制限。 暗号の利用（8.24） 顧客情報を保存時・転送時に暗号化。
注文情報（商品名、購入日、購	不正なデータ改ざんや漏えい	中	アクセス制御（5.15） 注文情報へのアクセスを業務上必要な従業員に限

入金額など)			定。 情報 セキュリティインシデント 管理の計画策定および準備 (5.24) 注文情報の改ざんや漏えいが発生した場合の対応手順を整備。
在庫情報 (商品在庫数、入荷予定など)	内部関係者による不正なアクセス	中	情報セキュリティの意識向上、教育および訓練 (6.3) 従業員に対するセキュリティ教育を実施し、在庫情報の取扱いに関するリスクを軽減。 アクセス制御 (5.15) 在庫情報システムへのアクセスを制限。
支払い情報 (クレジットカード情報、銀行口座情報)	クレジットカード情報や銀行口座情報の盗難・不正利用	高	暗号の利用 (8.24) 支払い情報は保存時および転送時に暗号化。 アクセス制御 (5.15) 支払い情報へのアクセスを厳格に制限。 ログ取得 (8.15) 支払い情報に関する操作の記録を保護し、監視を実施。

3.セキュリティ要件の定義

適用宣言書を満たすためのセキュリティ要件を定義します。

セキュリティに関する要件定義の例

1.セキュリティ要件

1.1 顧客情報の保護

要件 1.1.1 : 顧客情報 (氏名、住所、電話番号、メールアドレス、クレジットカード情報) は、すべて暗号化技術を用いて保存および転送すること。

要件 1.1.2 : 顧客情報へのアクセスは、役割ベースで制限し、必要な従業員のみに許可すること。アクセス権は定期的にレビューし、不要な権限は削除すること。

要件 1.1.3 : 顧客情報の取扱いに関する[セキュリティポリシー](#)を文書化し、全従業員に周知すること。ポリシーの順守状況を定期的に監査すること。

1.2 注文情報の保護

要件 1.2.1 : 注文情報 (商品名、購入日、購入金額) は、適切なアクセス制御により保護し、

業務上必要な従業員のみがアクセスできること。

要件 1.2.2：注文情報の改ざんや漏えいが発生した場合のインシデント対応手順を整備し、インシデントの発生時には即座に対応できる体制を構築すること。

1.3 在庫情報の保護

要件 1.3.1：在庫情報（商品在庫数、入荷予定など）へのアクセスは、必要最低限の従業員のみ制限すること。アクセス制御リストは定期的に見直し、不要なアクセス権は削除すること。

要件 1.3.2：在庫情報に関するセキュリティ教育を実施し、従業員が適切に情報を取扱うようにすること。教育内容には、在庫情報の重要性とリスクについても含めること。

1.4 支払い情報の保護

要件 1.4.1：支払い情報（クレジットカード情報、銀行口座情報）は、保存時および転送時に暗号化技術を用いて保護すること。

要件 1.4.2：支払い情報へのアクセスは、業務上必要な従業員に限定し、アクセス権は厳格に管理すること。アクセスログは定期的にレビューすること。

要件 1.4.3：支払い情報に関する操作ログを記録し、改ざんや削除を防ぐための保護を施すこと。ログの保管には、セキュアなストレージを使用し、バックアップを定期的を取得すること。

2. 可用性要件

2.1 システムの高可用性

要件 2.1.1：システムは 24 時間 365 日稼動し続けること。メンテナンスやアップグレード時には、事前に計画を立て、影響を最小限に抑えること。

要件 2.1.2：システム障害発生時の迅速な復旧を支援するために、定期的なバックアップを実施し、災害復旧計画を策定すること。

3. パフォーマンス要件

3.1 応答時間

要件 3.1.1：ユーザーからの要求に対する応答時間は、システムの種類に応じて以下の基準を満たすこと。

Web ページの表示：3 秒以内

データベースクエリの実行：2 秒以内

4. コンプライアンス要件

4.1 法令順守

要件 4.1.1：個人情報保護法、クレジットカード業界の規制、電子商取引に関する規制など、関連する法令や規制を順守するためのプロセスを確立し、定期的な監査を実施すること。

EC サイトの構築時におけるセキュリティ対策要件

IPA が公開している「EC サイト構築・運用セキュリティガイドライン」では、EC サイトの構築時におけるセキュリティ対策要件を示しています。要件ごとに求められるセキュリティの水準に応じて、「必須」、「必要」、「推奨」を定め、それぞれ表中の区分に表記しています。

「必須」は、EC サイト運営事業者が EC サイトのセキュリティを確保する上で早急かつ確実な対策実施が求められるものであり、実装が必須として求められる内容と定義しています。

「必要」は、事業の重要度、対策費用、対策までの期間、対策を実施しないことによる影響度など、または他の代替策を実施するなどを考慮して導入時期を検討した上で実装が求められる内容と定義しています。

「推奨」は、EC サイト運営事業者がサイバー被害を受けるリスクの低減、被害範囲の拡大防止、EC サイトを復旧する場合において、対策実施が求められるものであり、事業の重要度、影響度などを考慮した上で、EC サイト運営事業者が各自の責任において、その実装を検討すべき内容と定義しています。

「必須」の要件については必ず実装することが重要ですが、「必要」、「推奨」の要件については、自社の適用宣言書に基づき、実装を検討することが大切です。

NO	セキュリティ対策要件（構築時）	区分
要件 1	「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」に準拠して、EC サイトを構築する。	必須
要件 2	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須
要件 3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須
要件 4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須
要件 5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須
要件 6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を順守する。	必須
要件 7	サイト利用者情報の登録時およびパスワード入力時における、不正ログイン対策を実施する。	必須
要件 8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須

要件 9	ドメイン名の正当性証明と TLS の利用を行う。	必須
要件 10	サイト利用者のログイン時における二要素認証を導入する。	必要
要件 11	サイト利用者のパスワードの初期化および変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要
要件 12	Web サーバや Web アプリケーションなどのログや、取引データなどのバックアップデータを保管する。	必要
要件 13	保管するログやバックアップデータを保護する。	推奨
要件 14	サーバおよび管理端末において、セキュリティ対策を実施する。	推奨

EC サイトの構築時におけるセキュリティ対策要件一覧
(出典) IPA「EC サイト構築・運用セキュリティガイドライン」をもとに作成

要件 1.「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」に準拠して、EC サイトを構築する。

「詳細理解のため参考となる文献（参考文献）」に掲げた「安全なウェブサイトの作り方」および「セキュリティ実装チェックリスト」では、「ウェブアプリケーションのセキュリティ実装」として、「脆弱性関連情報の届出制度」で届出の多かったものや攻撃による影響度が大きい脆弱性である、SQL インジェクション、OS コマンド・インジェクションやクロスサイト・スクリプティングなど 11 種類の脆弱性を取り上げています。それぞれの脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴などを解説し、脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を期待できる対策を示しています。

また、「ウェブサイトの安全性向上のための取組」として、ウェブサーバのセキュリティ対策やフィッシング詐欺を助長しないための対策など 7 つの項目を取り上げています。主に運用面からウェブサイト全体の安全性を向上させるための方策を示していますので、IPA の「EC サイト構築・運用セキュリティガイドライン」を参考にして EC サイトを構築してください。

なお、EC サイトの構築を委託する場合は、外部委託先事業者ガイドラインを参考にして構築することを依頼してください。

詳細理解のため参考となる文献（参考文献）	
安全なウェブサイトの作り方	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf
セキュリティ実装チェックリスト	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

要件 2.サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。

EC サイトを構築する場合、次のように利用しているソフトウェアへの脆弱性対策を実施するこ

とが重要です。

- 脆弱性情報などセキュリティに関連する情報を公表している EC サイト構築プログラムを選定してください。
- EC サイトを構成するソフトウェア（サーバと管理端末の OS、[ミドルウェア](#)とライブラリ、または、Web アプリケーションなど）を確認の上、一覧にまとめ、それぞれのソフトウェアに関する脆弱性情報などセキュリティに関連する情報を収集して管理し、それらの情報の内容を把握してください。
- EC サイトの構築時に利用しているサーバおよび管理端末の OS、ミドルウェアおよびライブラリ、または、Web アプリケーションや OSS などのソフトウェアについては、その時点の最新バージョンを使用してください。
- 利用しているソフトウェアなどについて、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は公開までにセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響がないことを確認（動作検証）してください。それ以外の脆弱性については、セキュリティパッチの適用や最新版へのバージョンアップを行うか否かを、脆弱性によるシステムへの影響などを考慮して判断してください。

要件 3. EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する

EC サイトを新規に構築した際は、EC サイトを公開するまでに脆弱性対策を実施する期間を確保して、次のような第三者による EC サイトへの脆弱性診断を実施して、EC サイトに脆弱性がないかを確認し、発見された危険度「高」、「中」の脆弱性への対策を行った上で公開してください。

- 脆弱性診断は、原則、第三者（外部委託先事業者、自社以外の第三者）による脆弱性診断を実施し、実施する脆弱性診断は、プラットフォーム診断、Web アプリケーション診断の 2 種類を実施してください。
- Web アプリケーション診断の実施範囲は、最低でも以下の画面について脆弱性診断を実施してください。
 - ログイン画面
 - サイト利用者情報登録/変更画面
 - 商品検索画面
 - 注文・決済画面など
- 脆弱性診断を第三者に依頼する場合は、IPA が公開している「情報セキュリティサービス基準適合サービスリスト」にある「脆弱性診断サービス」に記載されている事業者を選定することを推奨します。
- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、

「中」、「低」の3段階で分類されており、危険度「高」、「中」については、対策を行った上でECサイトを公開してください。



脆弱性診断を実施する上で参考にしていきたいこと

【脆弱性診断の目的】

脆弱性診断は、ECサイトがサイバー攻撃を受けて被害をまねく元となる脆弱性が存在していないかを調べるために行う、とても重要で必要な工程です。もし脆弱性が見つかった場合、脆弱性によるECサイトへの影響度を確認する必要があります。見つかった脆弱性の危険度および、脆弱性によるECサイトへの影響度により、対応の要否を判断して、対応をすることが重要です。

【脆弱性診断の種類】

脆弱性診断は、診断対象、診断方法によって、以下のものがあります。

<診断対象>

- プラットフォーム診断：サーバやネットワーク機器などのOSやミドルウェアを診断します。
- Webアプリケーション診断：Webサーバ上で動作するアプリケーションを診断します。

<診断方法>

- ツールによる診断：ツールにより自動で診断します。ツールによって診断できる範囲が異なります。(ツールには無償のものと有償のものがあります。)
- 手動による診断：人手により診断します。
- ハイブリッド診断：ツールでの診断が難しい箇所(人による判断が必要な場合)を人手で行うといった両者を組み合わせて診断します。

※手動による診断は、ツールによる診断に比べて費用が高額となります。手動による診断は、ツールでは見つけられない脆弱性を発見でき、ツールによる診断と組み合わせることで結果として精度の高い診断が可能です。

【脆弱性診断の実施者】

ツールで自動的に診断できる部分があるとはいえ、ツールの使用や診断結果を判断するため、脆弱性診断を行う人はそれなりのスキルが必要になります。自社に脆弱性診断を実施する技術者がいない場合は、脆弱性診断サービスの利用を検討することが重要です。

要件 4.管理者画面や管理用ソフトウェアへ接続する端末を制限する。

管理者画面や管理用ソフトウェアにアクセスするための ID・パスワードが攻撃者に漏えいすると、サイト利用者の顧客情報や、注文・取引データなどが大量に漏えいすることにつながるおそれがあるため、次のように厳重に管理することが重要です。

- 管理者画面や管理用ソフトウェアにアクセスするための ID・パスワードが不正に取得された場合に備えて、アクセスできる端末を制限するための [IP アドレス](#) 接続制限や、アクセスできる利用者を制限するために、二要素認証（ID とパスワードによる認証後に SMS（ショートメッセージサービス）などでの認証を行う方法）を導入してください。

要件 5. 管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。

管理者画面や管理用ソフトウェアへのアクセスに用いる端末が [マルウェア](#) に感染すると、端末内部および、当該端末がアクセス可能なサーバなどに保管しているサイト利用者の顧客情報や、注文・取引データなどが外部に送信されるおそれがあります。アクセスする端末に対して、マルウェア対策ソフトウェアを導入し、リアルタイム検知の実施および、定義ファイルの更新、端末のフルスキャンなどの定期的（1 回/日を推奨）な実施や、USB メモリなど外部記憶媒体の利用制限を通じて、マルウェア感染防止対策を行うことが重要です。

要件 6. クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を順守する。

クレジットカード決済を提供する場合には、割賦販売法におけるセキュリティ要求事項を反映した、クレジットカード取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」（カード情報の非保持化、カード決済の EMV 3D セキュアの導入など）を順守するとともに、契約するクレジットカード会社および決済代行会社（PSP）とコミュニケーションを取り、常に最新のセキュリティ対策の実施を検討してください。

要件 7. サイト利用者情報の登録時およびパスワード入力時における、不正ログイン対策を実施する。

サイト利用者のパスワードが攻撃者に漏えいすると、サイト利用者の個人情報や、注文・取引データなどの漏えいにつながるおそれがあるため、次のような不正ログイン対策を実施することが重要です。

- サイト利用者がパスワードを登録する際に 10 文字以上、英大文字と小文字、数字、記号を組み合わせ、推測困難なパスワードを登録するようにしてください。また、推測されやすいパスワードは登録できないようにすることが重要です。
- ログイン用の ID とパスワードのすべてのパターンを機械的に繰り返し入力し、EC サイト利用者の ID とパスワードを盗み出すという総当たり攻撃に備えて、パスワードなどの入力間違いの回数が一定数（10 回以下を推奨）を超えた場合はアカウントをロックするように

してください。

要件 8. サイト利用者の個人情報に対して安全管理措置を講じる。

個人情報保護法第二十三条（安全管理措置）に基づき、EC サイトの運用を通じて取扱う個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のために必要かつ適切な措置（個人データの取扱規定の整備、個人データを保存するシステム、機器および電子媒体の盗難、漏えいの防止、システム、機器へのアクセス制御、不正アクセス防止など）を講じる必要があります。

要件 9. ドメイン名の正当性証明と TLS の利用を行う。

EC サイト利用者が ID とパスワードを不正に窃取するフィッシングサイトではないこと（正規のサイトであること）を確認できるようにするためには、TLS/SSL 証明書などを導入し正当性証明を行うこと、および TLS（Transport Layer Security）の利用により通信を暗号化することが重要です。

要件 10. サイト利用者のログイン時における二要素認証を導入する。

なりすましなどによる不正ログインが行われる可能性が高い（ある）と判断した場合には、ID とパスワードを用いたサイト利用者の認証に加えて、安全性を高められる二要素認証（ID とパスワードによる認証後に SMS などでの認証を行う方法）を導入します。

要件 11. サイト利用者のパスワードの初期化および変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。

正規サイトを装ったフィッシングサイトや、パスワードの変更などを行うように不正に誘導するフィッシングメールにだまされて、サイト利用者が気づかないうちに ID とパスワードを盗まれることがあります。そのため、なりすまされて登録情報を変更されたことにサイト利用者が気づくことができるようにするために、EC サイト利用者のメールアドレスの登録および変更、パスワードの初期化および変更、アカウントの登録および削除、決済処理時といった重要な処理を実行した際に、メールや SMS などを用いて、サイト利用者への通知を行うようにします。

要件 12. Web サーバや Web アプリケーションなどのログや、取引データなどのバックアップデータを保管する。

顧客情報の漏えい事故を発生させてしまった場合には、事故の原因究明のために [フォレンジック](#) 調査会社に依頼します。フォレンジック調査で原因究明を徹底的に行うためには、調査に必要なデータが十分に揃っていることが必要となるため、Web サーバや Web アプリケーションのログや、取引データなどのバックアップデータ（該当サーバ以外の外部ストレージサービスや、自社管理のサーバへの保管など）を過去 1 年間分以上保管しておくようにしましょう。

フォレンジック調査の依頼先は、IPA が公開している「情報セキュリティサービス基準適合サービスリスト」にある、「デジタルフォレンジックサービス」に記載されている事業者を参考にする
と良いでしょう。

また、レンタルサーバ事業者を利用する場合は、Web サーバのアクセスログなどの保管および
提供が可能な事業者を選ぶようにしましょう。

要件 13.保管するログやバックアップデータを保護する。

Web サーバのログおよび Web アプリケーションのログ、取引データなどのバックアップデー
タを過去 1 年間分以上保管していても、保管ログおよびデータへの不正アクセスがあれば、前述し
たフォレンジック調査による原因究明に支障が生じ、誤った結果が導かれるおそれがあります。こ
のため、ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対
して、不正アクセスができないような対策を実施する必要があります。

要件 14.サーバおよび管理端末において、セキュリティ対策を実施する。

サーバおよび管理端末自体がマルウェアに感染すると、サーバや管理端末内部に保管しているサ
イト利用者の顧客情報や、注文・取引データなどが外部に送信されるおそれがあるため、マルウェ
ア対策ソフトウェアを導入し、リアルタイム検知の実施および、定義ファイルの更新、ファイル・
メモリのスキャンなどの定期的（1 回/日を推奨）な実施や、USB メモリなど外部記憶媒体の利用
制限を通じて、マルウェア感染防止対策を行うことが必要です。

EC サイトの構築時に有効な CSF2.0 の管理策（例）

セキュリティ対策の要件を決める際は、CSF2.0 の管理策を参考にすることも有効です。

有効な管理策の例

パッチ適用に関する管理策

- GV.SC-09：サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリス
ク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイク
ル全体を通じて監視される。
- ID.RA-01：資産の脆弱性を特定、検証、記録する。
- PR.AT-01：要員は、サイバーセキュリティリスクを念頭において一般的な業務を遂行する
ための知識と技能を有するよう、意識向上とトレーニングを受ける。
- PR.PS-02：ソフトウェアはリスクに見合った保守、交換、削除が行われる。

など

認証に関する管理策

- PR.AA-01：許可されたユーザー、サービス、およびハードウェアの ID とクレデンシャル

が組織によって管理される。

- PR.AA-03 : ユーザー、サービス、ハードウェアを認証する。

など

バックアップに関する管理策

- PR.DS-11 : データのバックアップが作成、保護、維持、およびテストされる。
- RC.RP-03 : バックアップやその他のリストア資産をリストアに使用する前に、その完全性を検証する。

など

※各管理策の詳細は、「付録：CSF2.0」を参照してください。

詳細理解のため参考となる文献（参考文献）	
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html
情報セキュリティサービス基準適合サービスリスト	https://www.ipa.go.jp/security/service_list.html
脆弱性診断サービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_2.pdf
デジタルフォレンジックサービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_3.pdf

ユーザビリティおよびアクセシビリティに関する事項

ユーザビリティとは、利用者がサービス・業務を利用して実施したいことを、ミスなく効率的に行うために必要となる事項であり、アクセシビリティは、目的の情報へのたどり着きやすさを指します。どちらも利用者の年齢、身体的制約、利用環境などの違いによる配慮が必要です。

EC サイト構築におけるユーザビリティの要件（例）

NO	ユーザビリティ分類	ユーザビリティ要件
1	画面の構成 (直観・シンプル)	● 利用者が何をすれば良いか直感的に理解できるデザインにすること。 ● 無駄な情報、凝ったデザイン、不要な機能を排したシンプルでわかりやすい画面にすること。
2	画面の構成 (フォントおよび文字サイズ)	● 十分な視認性のあるフォントおよび文字サイズを使用すること。 ● 画面サイズや位置を変更できること。 ● 一度に膨大な情報を提示して利用者を圧倒しないようにすること。
3	画面の構成 (マルチデバイス対応)	● スマートフォン、タブレット端末により本サービスを利用する利用者を想定し、これら端末の特性を考慮した画

		面にすること。 レスポンシブ Web デザインにより、PC、タブレット端末、スマートフォンなどの利用環境を問わず、同一の情報をグリッドレイアウトなどの適切なレイアウトにより表示できるようにすること。
4	画面遷移	- 利用者が次の処理を想像しやすい画面遷移とすること。 - 無駄な画面遷移を排除し、シンプルな操作とすること。

EC サイト構築におけるアクセシビリティの要件（例）

No	アクセシビリティ分類	アクセシビリティ要件
1	言語対応	本情報システムでは、日本語のほか、XX 語で記載されたコンテンツに対応すること

システム方式に関する事項

「システム方式」では、定義された業務要件のうち、情報システムが処理・実行する範囲について、情報システムとして動作するために必要となる「道具」の具体的な実現方法を明確にします。

EC サイト構築におけるシステム方式に関する事項（例）

No	全体方針の分類	全体方針
1	システムアーキテクチャ	本情報システムのシステムアーキテクチャは、【メインフレーム型／クライアントサーバ型／Web サーバ型／外部サービス利用型／スタンドアロン型】とする
2	アプリケーションプログラムの設計方針	情報システムを構成する各コンポーネント（ソフトウェアの機能を特定単位で分割したまとまり）間の疎結合、再利用性の確保を基本とする
3	ソフトウェア製品の活用方針	広く市場に流通し、利用実績を十分に有するソフトウェア製品を活用する アプリケーションプログラムの動作、性能などに支障をきたさない範囲において、可能な限りオープンソースソフトウェア（OSS）製品（ソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア製品）の活用を図る。ただし、それらのOSS製品のサポートが確実に継続されていることを確認しなければならない
4	システム基盤の方針	クラウドサービス提供者が提供するサービス・機能を最大

		限活用した構成とする

規模に関する事項

「規模」とは、情報システムを使うユーザーの数や取扱う情報量を指します。利用者が多ければ単位時間当たりで多くのリクエストを処理できる能力が必要となりますし、情報量が多ければ、より大容量のデータベースなどが必要になります。要件定義では「利用者は最大 100 人、平日は常時 80 人、土日は基本的に休みのため 10 人未満」といった要件を定量的に示します。

EC サイト構築における利用者数に関する事項（例）

NO	ユーザー区分	ユーザー数
1	想定ユーザー（アクティブユーザー）	5000（人）

EC サイト構築における情報量に関する事項（例）

NO	項目	処理件数	補足
1	業務処理件数（ピーク時）	300（件／分）	1 月 1 日から 1 月 3 日ごろまで、初売りセールのため処理が集中する
2	業務処理件数（通常時）	120（件／分）	平日は 80（件／分）、土日祝日は 100（件／分）

性能に関する事項

「性能」とは、情報システムの能力を指します。能力を測る指標には、応答性能やスループット（処理性能）などがあります。ネットショッピングで例えると、商品を検索し検索結果のリストが表示され、特定の商品を選択すると詳細情報が表示される、という一連の流れが一般的ですが、検索ボタンや選択ボタンを押してから、次の画面が表示されるまでの時間が応答性能です。スループットは、一度にどれだけの量を処理できるかという性能で、通常時でも大量に注文が発生するバーゲンセール開催中でも、定義した応答性能が担保されるということを表します

EC サイト構築における応答性能の事項（例）

NO	指標名	目標値	補足
1	参照系処理	3 秒	画面の読み込み、情報の表示に関する処理
2	更新系処理	5 秒	情報の登録、更新、削除に関する処理

EC サイト構築における処理性能に関する事項（例）

NO	設定対象	指標名	目標値	応答時間達成率

1	〇〇処理	レスポンスタイム	定常時：X 秒以内 ピーク時：X 秒以内	90%
2		ターンアラウンドタイム	定常時：X 秒以内 ピーク時：X 秒以内	90%
3		サーバ処理時間	定常時：X 秒以内 ピーク時：X 秒以内	平均値

信頼性に関する事項

「信頼性」とは、情報システムが持つ故障への耐性の度合いのことを指します。一般的には平均故障間隔（分または時間）で評価します。平均故障間隔の値が小さければ小さいほど信頼性は高いといえます。

EC サイト構築における信頼性に関する事項（例）

NO	指標名	目標値	補足
1	運用時間	24 時間 365 日	以下に該当する時間を除く。 ● 接続回線の計画停止時間 ● 大規模災害などの天災地変に起因する停止時間 ● 連携するサービスまたはクラウドサービスまたはスマートフォン端末の通信キャリアの障害・計画停止・緊急メンテナンスなどに起因する停止時間 ● 本サービスのメンテナンスによる計画停止時間
2	稼働率	99.9%以上	本サービスにおける稼働率を以下の計算式により定義する。 稼働率＝年間実稼働時間／年間予定稼働時間 x100 当該計算式において、年間実稼働時間は「利用者がサービスを利用可能な時間の合計」、年間予定稼働時間は「年間稼働時間（24 時間 365 日）から計画停止時間および大規模災害による停止・縮退時間を除いた時間の合計」とする。

拡張性に関する事項

「拡張性」とは、利用率の増加、データ量の増加などにより、利用資源の規模・性能を拡張する必要が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うことです。また、将来の制度改正などにより機能を拡張する必要が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うことも指します。

EC サイト構築における拡張性に関する事項（例）

基本方針

本システムの利用率の増加、データ量の増加などにより、規模・性能を拡張する必要性が生じた場合に備え、可能な限り性能の拡張を柔軟に行えるよう、設計・開発を行うこと。また、将来の制度改正などにより機能を拡張する必要性が生じた場合に備え、容易に機能追加・変更を行えるよう、設計・開発を行うこと。

マネージドサービスなどの活用

本サービスはクラウドサービスを利用する想定としている。本サービスの構築に当たっては、当該クラウドサービスをマネージドサービスなど可能な限り活用することにより、処理能力などの動的調整を実現することにし、業務量および処理能力の拡張性については特段の拡張性要件を定義しない。

機能の追加

機能の追加や、新たな機能開発の必要性が生じることが想定されることから、将来開発する機能も含めた機能間の連携が十分に図られるようにすること。

本サービスは、連携業務アプリケーションとの一層の連携など、拡張性を備えたシステム・サービスであることが求められる。連携機能などの拡張が必要になった際に拡張が容易となるような構成を取ること。

上位互換性に関する事項

「上位互換性」とは、主にソフトウェア製品において、新しいバージョンの製品で古いバージョンの製品が利用できることを指します。代表的な製品は上位互換性がありますが、バージョンアップに伴い、レイアウトが崩れたり、ブラウザの場合画面のレイアウトや特定のボタンが動作しなくなったりといった、一部の機能に限り上位互換性がないこともあります。

EC サイト構築における上位互換性に関する事項（例）

クラウドサービスのバージョンアップ

システムの構成にクラウドサービスのマネージドサービスを採用する場合、軽微なバージョンアップについては自動適用を前提とする。大規模なバージョンアップについては、アプリケーションへの影響を事前に精査し、適用を検討すること。

OS などへの依存

原則特定バージョンへの依存は避けること。なお、やむを得ず OS、ミドルウェアなどの特定バージョンに依存する場合は、その利用を最低限とすること。

クライアント端末の更新

クライアント端末が更新され、OS や Web ブラウザとして新しいバージョンのものを利用する

場合も、業務運営に極力支障が生じないよう計画されたシステム構成とすること。

中立性に関する事項

「中立性」とは、情報システムを構成する要素が、特定の技術や製品に特化しないことを指します。例えば、新規に情報システムを構築する際に、ある事業者が開発・販売している製品を利用しなければ運用・保守ができない構成にしたとします。その後、運用・保守業務を一般競争入札で調達しようとしても他の事業者ではその製品を入手できないなどの理由により、その製品を導入した事業者による一者応札となってしまいます。このような状態になることを防ぐために、特定の事業者の技術に依存せず、多くの事業者が扱える製品を採用するなど、中立性への配慮が必要です。

EC サイト構築における中立性に関する事項（例）

データの可搬性の担保

データの可搬性の担保に当たっては、以下の要件を満たすこと。

- 情報システム内のデータについては、原則として XML や CSV などの標準的な形式で取り出すことができるものとする。
- 技術的な理由により、提供することが難しいデータ項目がある場合には、代替案を提示することが可能であること。
- 移行用データが満たすべき制約（移行データのデータフォーマットやスキーマなどの要件も含む）を文書化すること。文書については、情報システムの業務要件を理解しているユーザーであれば理解できるように記述すること。なお、システム運用期間中に該当文書の内容に変更が生じる場合は継続して改定を行い最新化できること。
- 移行データに関する文字コードなどは以下に従うこと。
 - 取扱う日本語文字集合の範囲：JIS X 0213
 - 文字コード：ISO/IEC 10646
 - 文字の符号化形式：UTF-8

継続性に関する事項

「継続性」では、当該情報システムを構成する要素（サブシステム、サービスなど）に分解し、情報システム全体での目標復旧時間を踏まえて、各要素の継続性に係る指標や目標値を要件として示します。

クラウドサービスとオンプレミスは継続方法の確保方法が異なります。クラウドサービスを利用する場合には、オンプレミスのように別途保管する必要はなく、クラウドサービス提供者が提供するバックアップサービスを利用すれば良いと考えられます。ただし、バックアップサービスにはさまざまな種類が存在することに鑑み、選択する手法が妥当なものであることを確認しておきましょう。

EC サイト構築における継続性に関する事項（例）

データバックアップ

- バックアップ対象

データバックアップに当たっては、本サービスの稼動に必要な全データを復旧可能とすることを前提として、外部組織から再入手可能なデータの有無を含め、保全対象を精査し、復旧時に必要となるデータを過不足なく保全対象に含めることができるようにすること。なお、クラウドサービスのマネージドサービスを利用することで自動的にバックアップを取得できる部分はあるが、オペレーションミスやアプリケーションのバグなどに起因するデータ破壊に対しても破壊前の時点まで遡れるように、バックアップの実施方法について配慮すること。

- バックアップ頻度

バックアップの取得間隔は、原則日次とする。ただし、障害発生時点への復旧が必要なデータについては、復旧に用いる PITR : Point In Time Recovery/Restore を保存するなどの対応を行うこと。

- 保存期間

万一の障害発生に備え本サービスの稼動に必要な全データを復旧可能とするとともに、過去のシステム処理に問題が発生した場合に原因分析を可能とすることを目的として、日次のバックアップについては、30 日分のデータをバックアップとして保持すること。

情報システム稼動環境に関する事項

「情報システム稼動環境」とは、当該情報システムに係る、クラウドサービスの構成、ハードウェアの構成、ソフトウェア製品の構成、ネットワークの構成、施設・設備要件などを明らかにすることを指します。稼動環境には、運用、保守、研修、検証などに必要な環境も含めます。

EC サイト構築における情報システム稼動環境に関する事項（例）

動作保証対象とする利用端末

NO	端末	OS	バージョン
1	PC	～	Ver〇〇
...	...	...	...

動作保証の対象とするブラウザ

- PC の場合：〇〇ブラウザの最新バージョン
- スマートフォンの場合：□□ブラウザの最新バージョン

- タブレット端末の場合：△△ブラウザの最新バージョン

※動作保証の対象とする OS やブラウザは、想定される利用者に合わせて決定する必要があります。動作保証対象とする OS やブラウザの種類を絞りすぎると、アクセスできない利用者から不満が出る可能性があります。想定される利用者をできるだけ広くカバーできるように動作保証対象を設定することが重要です。

テストに関する事項

情報システムのテストには、ソフトウェアの設計に基づいて事業者が行うテストと、発注者および情報システムの利用者の視点で行うテストが存在します。テストに関する要件には、実施するテストの内容や方法、環境などを示します。

EC サイト構築におけるテストに関する事項（例）

NO	テスト工程	テストの目的・内容	テスト環境	テストデータ	テスト実施主体
1	単体テスト	アプリケーションを構成する最小の単位で実施するテストであり、主に機能単位で設計通りに動作するかを事業者（プログラマ）が確認する。	開発環境	テスト用に作成したデータ	事業主
2	結合テスト	複数の機能を連携させて動作を確認するテストであり、主にユースケース単位で設計通りに動作するかをテスト担当者が確認する。	検証環境	テスト用に作成したデータ	
3	総合テスト	システム全体が設計の通りに動作することを確認するテストであり、ユースケースを組み合わせた一連の業務が行えることを機能面や非機能面の観点からテスト担当者が確認する。	検証環境	テスト用に作成したデータ、または本番データから作成した疑似データ	
4	受入テスト	納品されるシステムが要件通りに動作することを確認するテストであり、発注者が主体	検証または本番環境	本番データ、または本番データから作成した疑	

		となり、事業者と協力して確認する。		似データ	

移行に関する事項

移行には、データ移行、システム移行および業務運用移行の3つの要素があります。業務の安定的な継続が最重要課題であるため、移行の各ステップにおいて状況进行评估し、最悪の場合でも既存の情報システムへ切り戻せるような計画と、プロセスの準備を要求しておくことが必要です。

移行に向けた作業手順および役割分担（例）

No	作業名	主管部	工程管理 支援業者	現行システム 運用保守 事業者	次期システム 設計開発 事業者
1	移行計画の作成	■	●	△	◎
2	移行データ準備・提供	◎・■	●	◎	△
3	移行データ分析	■	●	△	◎
4	移行設計	■	●		◎
5	データ移行サーバ・ツール開発	■	●		◎
6	移行リハーサル	■	●	△	◎
7	移行判定	◎・■	●		◎
8	本番移行	■	●	△	◎
9	稼動判定	◎・■	●		◎

◎：主体者、●：確認者、■：承認者、△：支援者

EC サイト構築における移行対象データ（例）

NO	移行元	移行対象業務	件数	提供方法
1	商品情報	商品テーブル	XX	CSV 形式での提供
2		新規登録ファイル	XX	CSV 形式での提供
3		商品情報	XX	CSV 形式での提供

引継ぎに関する事項

情報システムの構築およびテストが完了し本番運用に移行する際、または年度の節目などで事業者や要員が交代する場合、円滑な業務運営を維持するためには、あらかじめ引継ぎ項目を整理し、想定しておくことが重要です。現在その作業を担当している事業者を「引継ぎ元」と定義し、その

事業者が担当している作業を「引継ぎ内容」として明らかにします。基本的には事業者ごとに作業・成果物などを定義した契約が存在しているため、その内容をもとに整理すると効率的です。引継ぎ期間は1ヶ月程度を設定することが一般的ですが、十分ではないケースが多く見られます。引継ぎ期間が十分でない場合には、他の事業者が参入できなかつたり、その後の業務運営に支障が生じたりするおそれがあるため、十分な期間を確保することが重要です。

EC サイト構築における引継ぎ事項（例）

NO	引継ぎ期間	引継ぎ先	引継ぎ内容	引継ぎ手順
1	令和○年○月○日 ～ 令和○年○月○日	運用・保守事業者 (令和X年度後半 に調達予定)	ソースコード（テスト・構成管理・環境構築などに利用するコード含む）開発環境に必要な各種ツール 各種設計書・ドキュメント類 運用課題（管理簿） 仕様課題（管理簿） インシデント状況（管理簿） 連携業務 AP 対応状況（管理簿） ヘルプデスク作業 各種運用・保守作業 そのほか納品物一式 (クラウドサービスの管理に必要なアカウントや鍵情報、また Infrastructure as Code に基づくシステム構築・管理に係る構成管理ファイルなど情報を漏れなく含む)	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。
2	令和○年○月○日 ～ 令和○年○月○日	連携先システムである●●システムのアプリケーション保守事業者	必要となる知識など	受託者は、引継ぎ計画書の内容に基づいて、引継ぎ作業を行う。

One Point

事業者がソフトウェアライセンスを保有している場合の引継ぎ

事業者が情報システムを構成するソフトウェアのライセンスを保有している場合、事業者が交代する際にソフトウェアライセンスを引継ぎ先の事業者へ譲渡することが必要になります。ソフトウェアライセンスの契約条件によっては譲渡に制約が生じ、引継ぎ先の事業者による運用・保守作業に支障が生じる場合があります。そのため、譲渡可能なソフトウェアライセンスを調達する旨とソフトウェアライセンスの譲渡に関する制約がある場合はその情報を開示する旨を、要件定義書に記載しましょう。落札後、ソフトウェアライセンスの契約条件を発注者・事業者間で合意した上で、ソフトウェアライセンスを調達しましょう。

教育に関する事項

「教育」とは、情報システムの利用者が、その情報システムの機能を理解し、効率的に運用していくために必要となる、利用者に対する操作研修などを指します。

業務要件定義で作成した業務フロー図などを参考に、教育対象者の範囲を定めます。基本的には業務フロー図に表現されているすべてのアクター（役割）が、教育対象者の候補となりますが、対象者の役割、所属する組織、場所などを考慮し、教育効果や費用を考慮して教育内容や用いる教材などについて要件として示します。

EC サイト構築における教育対象者（例）

NO	教育対象者	教育内容	教育対象者数
1	システム部門従業員	運用業務の全体概要、システム部門従業員の業務手順など	XXX
2	業務部門従業員	従業員の業務に関する本システムの操作手順、画面遷移、UI 表示仕様、エラー発生時の対応など	XXX
3	運用・保守事業者	運用・保守業務の全体概要、運用・保守事業者の業務手順、運用・保守要員の業務内容など	XXX

EC サイト構築における教育資料の概要（例）

NO	教材	教材の概要	対象者	補足
1	システム概要資料	情報システムや関連業務の概要を取りまとめた資料	システム部門従業員 業務部門従業員 運用・保守事業者	対象者ごとに教材を作成
2	操作動画	情報システムの操作方法について動画に取りまとめたもの	業務部門従業員	XXX
3	FAQ	よくある質問や回答を取りま	システム部門従業	対象者ごとに教

		とめた資料	員 業務部門従業員 運用・保守事業者	材を作成

運用に関する事項

情報システムの運用とは、稼動状態をあらかじめ定めた品質基準に基づき維持することであり、今ある環境を正常な状態に保ち続ける活動ともいえます。詳細な内容は情報システムの運用設計において検討しますが、運用要件の内容によって、情報システムの機能要件および非機能要件に求める事項が異なることもあるため、基本的な要件はここで定義しておきます。

EC サイトの運用時におけるセキュリティ対策要件

IPA の「EC サイト構築・運用セキュリティガイドライン」には、EC サイト運用時におけるセキュリティ対策要件が記載されています。「必須」、「必要」、「推奨」という区分や定義については、「21-1-2.要件定義」で前述したものと同じです。「必須」の要件については、必ず実装することが重要ですが、「必要」、「推奨」の要件については、自社の適用宣言書に基づいて実装するようにしましょう。

No	セキュリティ対策要件（運用時）	区分
要件 1	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須
要件 2	EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つけた脆弱性を対策する。	必須
要件 3	Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須
要件 4	システムの定期的なバックアップの取得およびアクセスログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。	必須
要件 5	重要な情報はバックアップを取得する。	必須
要件 6	WAF（Web Application Firewall）を導入する。	推奨
要件 7	サイバー保険に加入する。	推奨

EC サイトの運用時におけるセキュリティ対策要件一覧
（出典）IPA「EC サイト構築・運用セキュリティガイドライン」をもとに作成

要件 1.サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。

ソフトウェアを安全な状態で利用するためには、その前提として、脆弱性情報に関する常日頃の

情報収集が大切です。すでに攻撃方法が見つかったり、被害の存在が広く知られていたりするなど、危険度の高い脆弱性に関しては、セキュリティパッチの適用や最新版へのバージョンアップによるアップデートを迅速に行うことが重要です。それ以外の脆弱性に関しては、セキュリティパッチの適用や最新版へのバージョンアップを行うか否かを、脆弱性によるシステムへの影響などを考慮して判断してください。

- EC サイトの構築時に利用している Web サーバなどの OS・ミドルウェア、プラグインおよびライブラリや、Web アプリケーションや OSS のソフトウェアについては、運用時点の最新版を使用してください。
- 利用しているソフトウェアなどについては、EC サイト運営事業者や外部委託先において最新の脆弱性情報を収集することが大切です。セキュリティ情報サイトでの定期的な情報収集をするとともに、ソフトウェアを提供している企業から脆弱性に関する情報収集方法が用意されている場合は必ず登録するようにしてください。
- 利用しているソフトウェアなどで脆弱性が発見された場合、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は、3 ヶ月程度を目途にセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響がないことを確認（動作検証）してください。

要件 2.EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する。

EC サイトを構築後、新たな脆弱性が発見される・新たな脆弱性を作り込む可能性があるため、定期的およびカスタマイズを行った際に脆弱性診断を実施します。

- 新機能の開発・追加やシステム改修などのカスタマイズを行ったときには、その都度 Web アプリケーション診断を実施することが重要です。なお、診断箇所は、最低でも新機能の開発や追加やシステム改修などを行った箇所を対象とした診断を実施してください。
- 上記のような新機能の開発・追加やシステム改修などのカスタマイズを行っていない場合でも、OS やミドルウェアなどの脆弱性は継続的に発見されているため、四半期に 1 回の頻度でプラットフォーム診断を実施することが望めます。
- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、「中」、「低」の 3 段階で分類されており、危険度「高」の脆弱性については、迅速に対策を行うことを推奨しています。また、危険度「中」は、3 ヶ月程度を目途に対策を行うことが推奨されています。

要件 3. Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。

不正アクセスやマルウェア感染により、Web サーバ内部に保管しているサイト利用者の顧客情報や、注文・取引データなどを外部に送信する不正なプログラムが、Web サーバの公開ディレクトリ配下などに仕掛けられた場合でも、それを検知できるように、定期的な差分チェック（ファイル整合性監視）や、Web サイト改ざん検知ツールを利用した監視を行うようにしましょう。

要件 4. システムの定期的なバックアップの取得およびアクセスログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。

不正アクセスやマルウェア感染により、システムを改ざん、破壊された場合、EC サイトでの事業の継続ができなくなる可能性があるため、システムのバックアップを最低 1 回/月取得するようにします。また、EC サイトへの不審なログインの試行が増えたり、システム上で対応されていない不正な注文ができたりするという不正アクセスの予兆が発生している場合もあります。このため、Web サーバのアクセスログを定期的に確認し、確認した結果、不正なアクセス（特定の IP アドレスからの大量のアクセスなど）があれば、[ファイアウォール](#)などのネットワーク機器の設定でアクセスの制限をかけるなどの対策を実施しましょう。

Web サーバのアクセスログの定期的な確認は、IPA が提供する「ウェブサイトの攻撃兆候検出ツール iLogScanner」を利用して確認可能です。

詳細理解のため参考となる文献（参考文献）	
ウェブサイトの攻撃兆候検出ツール iLogScanner	https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

要件 5. 重要な情報はバックアップを取得する。

サイト利用者の顧客情報や仕入先情報、売上情報などの重要な情報が[ランサムウェア](#)によって暗号化されると、EC サイトでの事業の継続ができなくなる可能性があるため、重要な情報は 1 回/日にバックアップを取得（ネットワークに接続されていないオフライン環境へ保管）します。

要件 6. WAF（Web Application Firewall）を導入する。

すでに見つかっている脆弱性に対して対応するまでに期間が必要な場合や、必要となるセキュリティ対策を実装するまでに期間が必要な場合が想定されます。対策をするまでの期間内にサイバー攻撃を受けることがないよう、応急処置として、[WAF](#)（Web Application Firewall）を導入すると良いでしょう。

要件 7. サイバー保険に加入する。

万が一、EC サイトまたは、自社システムがサイバー攻撃による被害を受けた場合に備えて、サ

イバー保険に加入しておきましょう。サイバー保険については、IPA 調査でも顧客情報の漏えい事故を発生させてしまった EC サイトの多くが、被害後に加入していますが、損害賠償や事故対応費用の負担、収益の減少を補う効果が認められることから、被害が発生していない場合でも被害発生に備えて加入することが推奨されます。

EC サイトの運用時に有効な CSF2.0 の管理策（例）

セキュリティ対策の要件を決める際は、CSF2.0 の管理策を参考にすることも有効です。

有効な管理策の例

パッチ適用に関する管理策

- GV.SC-09：サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリスク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイクル全体を通じて監視される。
- ID.RA-01：資産の脆弱性を特定、検証、記録する。
- PR.AT-01：要員は、サイバーセキュリティリスクを念頭において一般的な業務を遂行するための知識と技能を有するよう、意識向上とトレーニングを受ける。
- PR.PS-02：ソフトウェアはリスクに見合った保守、交換、削除が行われる。

など

脆弱性情報に関する管理策

- ID.RA-08：脆弱性の開示を受領、分析、対応するためのプロセスを確立している。

など

ログに関する管理策

- PR.PS-04：ログ記録を作成し、継続的なモニタリングに利用できるようにする。
- DE.CM-02：潜在的に有害な事象を発見するために、物理的環境をモニターする。
- DE.CM-03：潜在的な有害事象を発見するため、従業員の活動および技術利用を監視する。
- DE.AE-02：潜在的有害事象を分析し、関連する活動をよりよく理解する。
- DE.AE-03：情報は複数の情報源から関連付けられている。
- DE.AE-06：有害事象に関する情報は、権限を与えられたスタッフおよびツールに提供される。

など

バックアップに関する管理策

- PR.DS-11：データのバックアップが作成、保護、維持、およびテストされる。

- RC.RP-03 : バックアップやその他のリストア資産をリストアに使用する前に、その完全性を検証する。

など

※各管理策の詳細は、「付録：CSF2.0」を参照してください。

EC サイト構築における運用計画書の記載（例）

NO	項目	補足
1	作業概要	監視・運用・保守作業の対象範囲、管理対象、作業概要を記載する。
2	作業体制に関する事項	運用・保守業務を実施するための体制について、管理体制図、本件受託者の要因（責任者、作業者、役割分担）、連絡手段などについて記載し、全体的な運用管理体制を明確にする。
3	管理対象	受託者は本業務で開発する XXX システムおよびドキュメントについて保守を行うこと。
4	サービスレベル	運用・保守業務で達成目標とするサービスレベル項目およびサービスレベルを主管課が協議の上、決定すること。

主な運用作業例

NO	運用作業の分類	主な運用作業の内容
1	パッチ適用	保守におけるパッチ適用要否の判断結果に基づき、パッチを適用の上、適用後の稼動確認を行う。
2	ログ管理業務	● 操作ログやアクセスログなどのシステムログ、例外事象の発生に関するログを取得すること。 ● ログ解析機能の活用を前提として、適切なキャパシティ管理を行うこと。キャパシティの改善が必要と判断された場合、キャパシティ改善提案を行うこと。 ● 収集したログを一元的に管理し、不正侵入や不正行為の有無の点検・分析を効率的に実施すること。
3	システム監視	● サービスの運用状況を監視し、障害の発生またはその兆候を検知するとともに、障害を検知した際には重要性などで分類した上で、メールなどにより自動で通知する仕組みを構築すること。

		監視には、例として以下のものがある。 ジョブ監視、死活監視、性能監視、リソース監視、障害監視、ログ監視（監視対象のログを監視し、特定の文字列パターンと一致した場合に障害とする方式）、セキュリティ監視、クラウドの構成監視（クラウドサービスを構成する要素を監視する方式）、外形監視（当該システムを利用するユーザーと同じ方法でアクセスし正常に動作しているか監視する方式）など ● 各種監視結果を定期的に集計・分析し、監視方法や閾値、通知の見直しなどが必要な場合は、主管課の承認を得た上でこれに係る設計を行い、対応を実施すること。 ※システムサイジングについても定期的に分析を行い、主管課の承認を得た上で見直すこと。
4	問題管理	● 本サービスに対し、重大な影響を与えるインシデントや将来的に重大なインシデントに発展する可能性がある問題について影響評価を行った上で、緊急度および優先度を定め、根本原因の調査および解決策の立案を行うこと。
5	ヘルプデスク業務	● 本サービスの利用方法に関する問い合わせの受け付けからクローズまでを一元管理するヘルプデスクを設け、本サービス利用者からの問い合わせを受け付けること。 ● 問い合わせの要件は以下に示す ➤ 平均処理時間：6分 ➤ 平均応答速度：20秒 ➤ 一日の問い合わせ想定量：30件 ● ヘルプデスク担当者のスケジュールリングなどの運営を適切に行うこと。 ● ヘルプデスク担当者による対応手順、サービスレベルなどを統一するため、ヘルプデスク運用マニュアルを作成し、主管課の承認を得ること。 ● ヘルプデスク運営の中で FAQ は適宜追加、更新など、メンテナンスを行うこと。 ● 受け付けた問い合わせは、質問、インシデント、サービス要求、作業依頼などに分類した上で、対応日時、問い

		合わせ元、内容、回答状況などとともに記録すること。 なお、具体的な運用方法については、本サービスの設計開始以降に改めて検討する。 ● 問い合わせ記録は受け付け件数、問い合わせ者情報、問い合わせ内容、回率、回答に要した期間、回答内容などを適切な粒度で整理した上で、定期的に問題発生状況を分析し、必要な対応を行うこと。 運用・保守の計画および実施状況について、主管課の定める報告様式に従って取りまとめ、主管課に報告を行うこと。 （原則、月次での報告）

保守に関する事項

「保守」とは機能要件に変更を加えずにプログラム修正のみを行うことです。「機能要件を変えずにプログラム修正する」という特徴があるため、現状の各種ドキュメントを正しく管理することが重要です。運用・保守計画書および運用・保守実施要領に基づき作業をします。

EC サイト構築における保守に関する事項（例）

保守業務の実施	
●	受け付けた問い合わせをインシデントとして管理し、クローズまで、対応を継続すること。
●	障害について対応したときは、障害報告書を作成し、主管課に報告すること。
保守設計	
●	役割分担の整理
➤	保守業務の設計に際し、受託者の責任範囲およびクラウドサービスを含めた関連事業者間の役割分担を整理すること。
➤	新システムがクラウドサービス上で稼動することを踏まえ、各業者間の役割分担を考慮した上で、保守設計を行うこと。
アプリケーションの保守	
●	インシデント管理
➤	運用管理・監視など作業におけるインシデント管理と適切な連携を図ること。
●	是正保守
➤	アプリケーションに起因した障害発生時、監査指摘事項への対応時など、アプリケーションの是正が必要な場合に、是正保守を行うこと。
●	適応保守

- OS、ブラウザ、ミドルウェアなどのバージョンアップ対応など、利用環境の変更への対応が必要な場合、アプリケーションに係る適応保守を行うこと。
- **予防保守**
- アプリケーションに潜在的な問題が発見され、当該問題除去を目的とした変更が必要な場合または新たに脆弱性が報告された場合に、予防保守を行うこと。
- **改善措置**
- アプリケーションに係る機能性、信頼性、使用性、効率性、保守性、移植性などの改善が必要な場合に、対処を行うこと。
- **根本原因の分析**
- 是正保守および予防保守の実施に当たり、障害、監査指摘、潜在する問題などに係る根本原因の分析を行うこと。
- **検証**
- 修正したアプリケーションを本番環境へ展開（デプロイ）する前に、修正が適切に実施されているか否かについて検証環境において検証すること。
- **文章の修正**
- アプリケーション保守に伴い、ドキュメント（設計書、マニュアルなど）の修正を要する場合は、速やかに修正を行うこと。

SaaS 型サービスの選定基準と利用時に必要となる対策

EC サイトの形態の選定において、SaaS 型サービスを選定した場合、以下のセキュリティ対策の実施状況について確認する必要があります。

【SaaS 型サービスの選定基準】

- 選定したサービスがクレジットカードを扱う場合には PCI DSS に準拠していることを確認してください。（当該サービスの運営事業者のホームページやパンフレットなどに情報が公表されていない場合は、サービスの営業窓口にお問い合わせを確認してください）
- CSF2.0 の管理策（ID.RA-09：ハードウェアとソフトウェアの真正性と完全性は、取得および使用前に評価される。）を参考にすることも有効です。ソフトウェアが信頼できるものであるか、セキュリティに問題がないかを導入前に確認することが大切です。

SaaS 型サービスを選択した場合も、セキュリティ対策は必要です。例えば、セキュリティ対策を行わなかった場合、サービスの管理画面を乗っ取られ、EC サイトに不正ログインされる可能性があります。また、カスタマイズした部分（SaaS 型サービス利用で独自の処理を追加したホームページを作成している場合）に関しては、自社構築サイトと同等レベルのセキュリティ対策を行う必要があります。EC サイト運営事業者は、上記を理解した上で以下のセキュリティ対策を必ず実施

することが重要です。

【SaaS 型サービス利用時に注意すべきセキュリティ対策】

- 管理画面の乗っ取りを未然に防ぐため、SaaS 型サービスの管理画面や管理用ソフトウェアへアクセスする管理端末を利用する従業員を極力最低限に限定し、管理端末からのアクセス時は二要素認証と IP アドレスや端末 ID による接続制限の導入などを必須にします。
- 管理端末のサイバー攻撃者からの乗っ取りを防ぐために、セキュリティ対策（マルウェア対策ソフトウェアの導入、USB メモリなど外部記憶媒体の利用制限、OS、ソフトウェアの最新版へのアップデートなど）を実施します。

Fit&Gap 分析

Fit&Gap 分析は、SaaS やパッケージソフトウェアを導入する際に非常に重要なプロセスです。Fit&Gap 分析によって、RFI などの情報収集活動によって選定した SaaS やパッケージソフトウェアと、自社の業務要件との適合性を評価します。

Fit&Gap 分析にはさまざまなやり方がありますが、一般的な実施手順の例を紹介します。

Fit&Gap 分析の実施方法（例）

Fit&Gap 分析の一般的な実施手順（例）

1. 現状分析
2. SaaS、パッケージソフトウェアの機能調査
3. 比較分析
4. ギャップへの対応策検討
5. 費用対効果の分析
6. 実施計画の策定

「3.比較分析」は Fit&Gap 分析の中核をなす重要なステップのため、手順を詳細に説明します。

比較分析の一般的な実施手順（例）

1. 比較項目の設定
2. 評価基準の設定
3. 比較表の作成
4. 詳細比較
5. ギャップの特定と分類
6. フィットの評価

7. 結果の文書化
8. 視覚化（必要があれば実施する）
9. 要件の再検討
10. ステークホルダーレビュー

上記の手順をもとに、実際に Fit & Gap 分析の例を紹介します。

前提条件

企業名：地方の特産品を扱う中小企業「A 社」

現状：

- 実店舗は運営しているが、EC サイトはまだ存在しない。
- 主要な売上は観光客や地元の顧客による実店舗での購入。
- オンラインでの販売に関する経験がない。
- 自社には IT やセキュリティの専門家がいらない。

目標：

パッケージソフトウェアや SaaS を利用し、商品の購入から配送までを管理できる EC サイトを構築する。

1. 現状分析

現在のビジネスプロセスを詳細に文書化します。また、組織の要件を明確にします。

現状分析の例

- 商品仕入れと在庫管理
地元の生産者から商品を仕入れ、表計算ソフトで手動管理している。商品ごとの在庫情報は店舗ごとに管理されている。
- 店舗販売
実店舗での販売が主体で、一般的なレジを使用し、クレジットカード決済は外部の決済端末を利用している。
- 配送対応
電話やメールで受けた注文に対して手動で配送手配を行っている。オンライン販売は行っていない。

ビジネスプロセスをもとに、組織の要件を明確にします。

組織の要件を明確にする例

- ECサイトを構築し、実店舗外の顧客にもアプローチできるようにする。
- 在庫管理、注文管理、配送管理を一元化する。
- ECサイトにはクレジットカード決済機能も追加し、オンラインでも安全な決済を行えるようにする。
- セキュリティ対策を確実に実施する。(PCI-DSS 準拠)

2.パッケージソフトウェア・SaaSの機能調査

パッケージソフトウェアやSaaSが提供する機能を詳細に調査します。また、各機能の仕様や制限を理解します。

ECサイト構築のために適したパッケージソフトウェアやSaaSを調査する例

SaaS サービス A

- 世界的に使用されているECサイト構築プラットフォーム。多言語対応、国際配送、複数の決済オプションをサポートしている。
- PCI-DSSに準拠しており、セキュリティ面で強固な対策が施されている。

SaaS サービス B

- 日本市場向けに特化したEC構築サービス。豊富なカスタマイズ機能を提供している。
- クレジットカード決済機能が統合されており、在庫管理機能も充実している。

パッケージソフトウェア C :

- 中小規模のビジネス向けに使いやすいプラットフォーム。簡単にECサイトを開設でき、決済機能も搭載している。
- セキュリティ面での拡張性は限定的で、標準機能ではPCI-DSSに準拠していない。

3.比較分析

組織の要件とパッケージソフトウェア・SaaSの機能を比較します。また、適合する部分（フィット）と不一致の部分（ギャップ）を特定します。「比較分析」は、Fit&Gap分析の中核をなす重要なステップです。

3-1.比較項目の設定

要件定義の結果を踏まえて、業務プロセス、機能要件、非機能要件、法規制対応など、比較すべき項目を事前に定義します。これらの項目を具体的かつ測定可能な形で記述します。

比較項目の設定例

- 業務プロセス
商品の仕入れ、在庫管理、オンライン販売、決済、配送の各フローを統合して管理できること。
- 機能要件
EC サイト構築、クレジットカード決済の統合、在庫管理、顧客管理、配送管理の機能が含まれていること。
- 非機能要件
システムの稼働率が 99%以上であること、セキュリティ（PCI-DSS 準拠）、ユーザビリティ（初心者でも使いやすい操作画面が備わっていること。）
- 法規制対応
個人情報保護法、特定商取引法、PCI-DSS 対応などの法規制に準拠していること。

3-2.評価基準の設定

各項目に対する評価基準を設定します（例：完全一致、部分一致、不一致）。必要に応じて重要度や優先度を設定します。

評価基準の設定例

- 完全一致：要件がそのまま満たされている場合に該当します。
- 部分一致：要件の大部分が満たされているが、一部の設定やカスタマイズが必要な場合に該当します。
- 不一致：要件を満たしていない場合に該当します。

3-3.比較表の作成

候補となるパッケージソフトウェアや SaaS が複数ある場合は、縦軸に組織の要件、横軸にパッケージソフトウェアや SaaS の機能を配置した比較表を作成します。次に「2.評価基準の設定」で決定した評価基準をもとに、各パッケージソフトウェア・SaaS が組織の要件を満たしているか評価します。これにより、組織の要件とパッケージソフトウェア・SaaS の機能との対応関係を視覚化します。

比較表の例

要件	SaaS サービス A	SaaS サービス B	パッケージソフトウェア C
EC サイト構築	完全一致	完全一致	完全一致
クレジットカード決済の統合	完全一致	完全一致	部分一致
在庫管理	部分一致	完全一致	部分一致
配送管理	完全一致	完全一致	部分一致

顧客管理	完全一致	完全一致	部分一致
稼働率（99%以上）	完全一致	完全一致	完全一致
セキュリティ（PCI-DSS 準拠）	完全一致	完全一致	不一致
法規制対応	完全一致	完全一致	部分一致
操作画面の使いやすさ	完全一致	部分一致	完全一致

3-4. 詳細比較

各要件に対して、パッケージソフトウェアや SaaS が対応する機能を詳細に比較します。機能の有無だけでなく、その実現方法や操作性なども考慮します。

SaaS サービス A をもとに機能を詳細化する例を示します。他のパッケージソフトウェアや SaaS も同様に詳細化し、比較を行います。

SaaS サービス A における詳細比較の例

- EC サイト構築

SaaS サービス A は EC サイト構築において、豊富なテンプレートとカスタマイズ機能を提供しています。操作画面もシンプルで直感的に使えるため、初心者でも容易に利用できます。多言語対応もあり、国際展開を視野に入れている企業にとっては非常に有利です。標準機能でほぼすべての要件に対応しており、カスタマイズの必要がほとんどありません。

- クレジットカード決済の統合

SaaS サービス A は、主要な決済サービスに対応しており、クレジットカード決済の統合がシンプルに行えます。PCI-DSS 準拠の決済システムが組み込まれているため、セキュリティ面も非常に強固です。操作も自動化されており、管理の手間がかかりません。

- 在庫管理

SaaS サービス A には基本的な在庫管理機能があり、在庫数の自動追跡や通知が可能です。実店舗とオンライン店舗の在庫を一元管理できますが、複雑な在庫管理には追加のカスタマイズが必要です。

- 配送管理

SaaS サービス A は主要な配送サービスと連携し、発送手続きや追跡をオンラインで一元管理できます。配送ラベルの自動生成やステータス通知により、手動管理の手間が減少します。操作画面もシンプルで使いやすいです。

- 顧客管理

SaaS サービス A には顧客の購入履歴や連絡先を自動管理する基本的な顧客管理機能があり、リピート顧客向けのプロモーションも可能です。ただし、詳細なデータ分析を行う場合は、追加のカスタマイズが必要です。

- 稼働率

SaaS サービス A はクラウドベースで、99.99%以上の稼働率を提供しており、システムが停止するリスクが非常に低いです。多くのアクセスが集中しても、安定してサイトが動作するため、安心して運用できます。

- セキュリティ（PCI-DSS 準拠）

SaaS サービス A は PCI-DSS に準拠しています。クレジットカード情報が安全に取扱われ、すべての決済データが暗号化されます。また、定期的にセキュリティパッチが更新され、最新の脅威に対応できます。

- 法規制対応

SaaS サービス A は日本の法規制に対応しており、個人情報保護法や特定商取引法の要件に応じたプライバシーポリシーや利用規約の設定が可能です。

- 操作画面の使いやすさ

SaaS サービス A の操作画面は非常に直感的で、初心者でも迷うことなく利用できます。基本的な設定は数クリックで完了し、EC サイト運営の初心者にとって使いやすい設計となっています。

3-5.ギャップの特定と分類

不一致（ギャップ）を見つけたら、その性質を分類します。（例：機能欠如、プロセスの相違、法規制への非対応など）ギャップの影響度や重要度を評価します。

ギャップの特定と分類例

SaaS サービス A のギャップ：在庫管理機能の不足

- 性質：機能欠如

SaaS サービス A は高度な在庫管理（多店舗連携や自動補充）に対応していないため、外部プラグインやカスタマイズが必要です。

- 影響度：

在庫管理はビジネス運営において重要な部分を占めます。標準機能では不足するため、プラグインやカスタマイズが必要ですが、比較的容易に対応できるため業務に大きな影響は与えないと考えられます。

SaaS サービス B のギャップ：操作画面の複雑さ

- 性質：プロセスの相違

SaaS サービス B は操作がやや複雑で、初心者にとっては学習コストが発生しますが、導入初期の対応で解決可能です。

- 影響度：

操作画面の複雑さは導入初期の学習コストを増加させますが、時間と研修によって解消できます。長期的には業務に大きな支障をきたさないため、影響度は低いと考えられます。

パッケージソフトウェア C のギャップ：セキュリティ対応の不足

- 性質：法規制への非対応
パッケージソフトウェア C は PCI-DSS 準拠のセキュリティ対策が不足しており、クレジットカード決済に対する対策が別途必要です。
- 影響度：
セキュリティ対応の不足は、顧客情報の漏えいや法的な問題につながる可能性があるため、ビジネス全体に強い影響を与える可能性があると考えられます。

3-6. フィットの評価

一致している部分（フィット）についても、適合度を評価します。単なる機能の有無だけでなく、使いやすさや効率性も考慮します。

フィットの評価例

SaaS サービス A のフィット評価

- クレジットカード決済の統合
SaaS サービス A は PCI-DSS 準拠であり、セキュリティ面での信頼性が高いです。クレジットカード決済の統合もスムーズで、安全かつ使いやすいシステムを提供しています。
- 稼働率
SaaS サービス A は 99% 以上の稼働率を誇り、安定した運用が可能です。ビジネスが途切れることなく継続できます。
- 操作画面の使いやすさ
操作画面は非常に直感的で、初心者でも簡単に利用可能です。これにより、迅速な導入と運用が可能となります。

SaaS サービス B のフィット評価

- 在庫管理
SaaS サービス B は強力な在庫管理機能を持っており、大量の商品を扱う際に効率的な管理が可能です。この機能は、標準で十分なレベルに達しています。
- クレジットカード決済の統合
SaaS サービス B も PCI-DSS に準拠しており、決済機能が安全に統合されています。法規制対応も含め、安心して利用できる環境が整っています。
- 稼働率
99% 以上の稼働率を持っており、ビジネスの安定運用が確保されています。システムの信頼性が高く、長期的な運用に適しています。

パッケージソフトウェア C のフィット評価

- EC サイト構築

パッケージソフトウェア C はシンプルで使いやすいインターフェースを提供しており、短期間でのサイト構築が可能です。特に中小企業に向いており、導入コストが低いのも魅力です。

- 稼働率

パッケージソフトウェア C も 99%以上の稼働率を誇りますが、大規模運用には適さない場合があります。小規模運用には十分な安定性があります。

- 操作画面の使いやすさ

パッケージソフトウェア C は非常にシンプルな操作画面を提供しており、初心者でも簡単に利用できます。低コストで迅速な運用が可能です。

3-7.結果の文書化

比較結果を詳細に文書化します。フィットとギャップの両方について、具体的な説明を記載します。

結果の文書化例

SaaS サービス A の結果

- フィット：SaaS サービス A は、重要度の高い要件であるクレジットカード決済の統合、セキュリティ（PCI-DSS 準拠）、法規制対応、そして稼働率 99%以上をすべて満たしています。また、操作画面の使いやすさも完全一致しており、操作に慣れていないスタッフでも扱いやすいです。
- ギャップ：在庫管理機能については一部カスタマイズが必要であり、標準機能では自社の要件を完全に満たしません。カスタマイズにより、初期導入コストやシステム設定に追加の手間がかかる可能性があります。

SaaS サービス B の結果

- フィット：SaaS サービス B は、在庫管理、顧客管理、配送管理の各プロセスにおいて高い適合度を示しており、特に中小企業の実務に即した機能が充実しています。重要度の高いセキュリティや法規制対応も完全一致しており、安心して導入できます。稼働率も高く、パフォーマンス面でも良好です。
- ギャップ：操作画面の使いやすさについては、初心者にとってはやや複雑で、導入時にトレーニングが必要となります。ただし、業務に大きな支障はないと考えられます。

パッケージソフトウェア C の結果

- フィット：パッケージソフトウェア C は、導入コストが非常に低く、簡単に EC サイトを

構築できるため、迅速にオンライン販売を開始したい企業には適しています。操作画面の使いやすさにおいても高い評価を受けており、特に IT に不慣れなスタッフでも容易に操作できます。

- **ギャップ**：大きなギャップは、セキュリティ要件が不十分な点です。特に、PCI-DSS 準拠が不足しているため、クレジットカード決済を安全に運用するためには追加のセキュリティ対策が必須となります。また、配送管理や在庫管理の一部機能が標準では不足しており、カスタマイズが必要です。初期の導入コストが低い反面、長期的には追加コストが発生するリスクがあります。

3-8.視覚化（必要があれば実施する）

必要に応じて結果をグラフや図表で表現し、全体像を把握しやすくします。例えば、ヒートマップやレーダーチャートなどを使用します。

3-9.要件の再検討

分析結果に基づき、組織の要件自体の妥当性を再検討します。場合によっては、要件の修正や優先順位の変更を行います。

要件の再検討例

要件 1:EC サイトを構築し、実店舗外の顧客にもアプローチできるようにする。

分析結果の確認：SaaS サービス A、SaaS サービス B、パッケージソフトウェア C すべてが EC サイト構築要件に対して完全一致しており、特に問題がないことが確認できます。

再検討の必要性：なし

要件 2:在庫管理、注文管理、配送管理を一元化する

分析結果の確認：SaaS サービス A とパッケージソフトウェア C は在庫管理や配送管理が部分一致であり、一部カスタマイズや追加機能が必要です。SaaS サービス B は完全に一致しています。

再検討の必要性：在庫管理や配送管理の重要度は高いため、SaaS サービス A やパッケージソフトウェア C を選ぶ場合にはカスタマイズや追加機能導入の検討が必要です。要件自体は妥当ですが、システム選定時にはこれらの要件の優先順位を高く維持するべきです。

要件 3:EC サイトにはクレジットカード決済機能を追加し、オンラインでも安全な決済を行えるようにする

分析結果の確認：SaaS サービス A と SaaS サービス B はクレジットカード決済に完全一致していますが、パッケージソフトウェア C を選択する場合には追加のセキュリティ対策が必要となります。

再検討の必要性：SaaS サービス A と SaaS サービス B は必要ありません。パッケージソフトウェア C を選択する場合は追加のセキュリティコストを考慮する必要があります。

要件 4:セキュリティ対策を確実に実施する（PCI-DSS 準拠）

分析結果の確認：SaaS サービス A と SaaS サービス B は PCI-DSS に完全に準拠していますが、パッケージソフトウェア C はこの要件に不一致であり、セキュリティ対策を強化しなければなりません。

再検討の必要性：パッケージソフトウェア C を選択する場合には、外部セキュリティ対策を追加するコストを考慮しなければなりません。セキュリティは最も重要な要件の一つであり、特にクレジットカード決済においては必須です。

3-10.ステークホルダーレビュー

分析結果を関係者に共有し、フィードバックを得ます。必要に応じて追加の調査や分析を行います。

「1.比較項目の設定」から「10.ステークホルダーレビュー」までの詳細な比較分析により、パッケージソフトウェア・SaaS と組織の要件との適合性を正確に評価し、導入に向けた的確な判断や計画立案が可能になります。

※比較分析の作業において業者に協力を求める場合、当該作業の内容と責任の所在を明確にする必要があります。また、複数の業者からの提案書および Fit&Gap 分析の評価を求める場合は、書式の統一、用語の定義などに配慮し、誤解が生じないようにすることが信頼性の確保につながります。

4.ギャップへの対応策検討

カスタマイズ、ビジネスプロセスの変更、代替ソリューションを検討します。

（可能な限りカスタマイズは避けた方がよく、ビジネスプロセスを変更することで対応することが推奨されます。）

SaaS サービス A を例にとり、説明します。

SaaS サービス A のギャップへの対応策例

ギャップの概要

SaaS サービス A の在庫管理機能が標準では自社の要件に完全には対応していないため、カスタマイズやビジネスプロセスの調整が必要です。

対応策：

- ビジネスプロセスの変更：在庫管理の運用をシンプルにし、SaaS サービス A が標準で提供

している在庫管理機能に適合するようにプロセスを調整できるか検討します。例えば、在庫の更新頻度を増やす、複雑な商品区分を簡略化するなど、システム側に合わせたプロセスの変更で対応可能な部分があるかを確認します。

- カスタマイズ：ビジネスプロセスの変更が難しい場合、在庫管理の不足部分に対して追加のプラグイン導入といったカスタマイズを行います。この際、必要最小限のカスタマイズに留めることが重要です。

5.費用対効果の分析

ギャップへの対応策実施にかかるコストと得られるメリットを評価します。

SaaS サービス A を例にとり、説明します。

費用対効果の分析例

ギャップの概要

SaaS サービス A の在庫管理機能が標準では自社の要件に完全には対応していないため、カスタマイズやビジネスプロセスの調整が必要です。

対応策 1：ビジネスプロセスの変更

コスト

- 初期費用：なし（社内でプロセスを調整）
- 運用費用：低コスト（社内のスタッフによる在庫管理の簡略化）

メリット

- SaaS サービス A の既存の在庫管理機能に合わせてプロセスを調整することで、カスタマイズ不要のため初期費用がかかりません。
- 社内運用のみで対応できるため、カスタマイズのコストが不要です。
- シンプルな運用による管理の効率化が見込まれます。

対応策 2：カスタマイズ（プラグイン導入）

コスト

- 初期費用：中程度（プラグインの導入コストや設定費用がかかる）
- 運用費用：月額 5000 円～10000 円（在庫管理用のプラグイン利用料）

メリット

- カスタマイズにより、標準機能では対応できない在庫管理機能を補完できるため、自社の業務フローに完全に対応することが可能です。
- システム全体の効率性が向上し、在庫管理の自動化やリアルタイムでの在庫情報管理が可能です。

6.実施計画の策定

分析結果に基づいて、具体的な導入計画を立案します。

例では SaaS サービス A の導入を推奨とし、その導入プロセスを具体的に示します。

導入計画の例

1.契約と初期設定（1 週間）

SaaS サービス A の契約を締結し、サイトの基本レイアウトを設定します。

2.商品データと在庫管理（2～3 週間）

商品情報を登録し、在庫管理のカスタマイズを実施します。

3.クレジットカード決済とセキュリティ設定（1～2 週間）

クレジットカード決済機能を設定し、セキュリティ対策を強化します。

4.配送システムの設定（1～2 週間）

配送オプションを設定し、配送業者との連携を行います。

5.テスト運用（1～2 週間）

商品購入から配送までのプロセスをテストし、問題がないか確認します。

6.スタッフトレーニング（1 週間）

SaaS サービス A の操作方法をスタッフに対してトレーニングします。

7.公開とマーケティング（1 週間）

EC サイトを公開し、プロモーションを実施します。

8.運用とメンテナンス

定期的にセキュリティチェックとシステムのメンテナンスを行います。

全体の期間：約 8～10 週間で EC サイトを構築し、運用を開始します。

サービス・パッケージ候補とのギャップを解消するポイント

RFI により提示した要件と提案されたサービス、パッケージ候補とのギャップを、委託候補企業の言いなりにならず、主体的に解消することが重要です。

- 要件の変更

Gap が大きすぎる場合は、最も適合性の高いサービスに合わせて、既存の業務プロセスやシステム要件を見直すことが望ましい。

- サービスのカスタマイズを利用

Gap が小さい場合は、サービス内のカスタマイズを利用することで Gap を埋める方法があります。しかし、セキュリティの観点から安易なカスタマイズは避け、できる限り業務プロセスをパッケージや SaaS に合わせることを望ましい。

- 補完的なサービスを利用

特定の機能のみが不足している場合は、別のパッケージや SaaS を組み合わせることで補完する方法があります。別のシステムを利用することにより専門的な機能の利用や、迅速な導入ができるので、初期投資が低く抑えられます。

独自カスタマイズのリスクについて

GAP を埋めるために、あらかじめ用意されているパッケージソフトウェアや SaaS サービス内のカスタマイズではなく、独自のカスタマイズを行う場合、以下のようなリスクがあります。

- コストの増加

カスタマイズには追加の開発費用がかかります。予算を超える可能性があり、コスト管理が難しくなることがあります。

- 時間の遅延

カスタマイズ作業が予想以上に時間がかかることがあり、プロジェクト全体のスケジュールに影響を与える可能性があります。

- メンテナンスの複雑化

カスタマイズされたシステムは、カスタマイズのないシステムに比べてメンテナンスが難しくなります。将来的なアップデートやバグ修正が困難になる可能性があります。

- 互換性の問題

カスタマイズにより、他のシステムやソフトウェアとの互換性が損なわれる可能性があります。これにより、システム全体のパフォーマンスや安定性に影響を与える可能性があります。

- サポートの制限

カスタマイズされた部分については、ベンダーからのサポートが受けられない場合があります。これにより、問題が発生した際の対応が遅れる可能性があります。

- 品質やセキュリティレベルの低下

カスタマイズが不十分な場合、システムのセキュリティや品質が低下するリスクがあります。これにより、ユーザーの満足度が低下するだけでなく、セキュリティインシデントの発生可能性も高まる可能性があります。

- 将来のアップグレード問題

カスタマイズされたシステムは、将来的なバージョンアップや新機能の追加が難しくなることがあります。最新の技術や機能を利用できなくなるというリスクがあります。

カスタマイズには多くのリスクがあるため、カスタマイズの必要性は慎重に検討し、業務プロセスなどをシステムにあわせて変更することが推奨されます。

どうしても機能などを追加する場合は、本体のシステムに与える影響の少ないアドオン（外側に機能を追加する方法）で対処することが推奨されます。

21-1-3. 調達

調達仕様書の作成方法

要件定義書を含めた調達仕様書の作成方法を説明します。

調達仕様書とは、プロジェクトの目的の達成に必要な製品の入手や、必要となる役務を実施する外部事業者を選定するために示す、発注者側の条件を集めたドキュメントです。

調達仕様書には、発注者側の要望（要件）に加えて、制約となる条件を記載します。実現したいことに加えて、実現を図っていく過程で守るべき前提条件や制約条件を合わせて記載することで、調達仕様書としての完成度を高められます。

調達仕様書の全体像（例）

目次	主要な記載内容
調達案件の概要	背景、目的、効果、業務・情報システムの概要
調達案件および関連調達案件の調達単位、 調達の方式など	調達内容、関連する調達案件、方式、時期
情報システムに求める要件	要件定義の内容
作業の実施内容に求める要件	作業の内容、成果物の範囲、納品期日
作業の実施体制・方法に関する事項	作業実施体制、資格要件、管理の要領
作業の実施に当たっての順守事項	機密保持、資料の取扱い、順守する法令
成果物に関する事項	知的財産権の帰属、契約不適合責任、検収
見積り依頼をする業者の選定に関する事項	業者選定要件
再委託に関する事項	再委託の制限、条件、承認手続き
パッケージソフトウェア、クラウドサービスの選定、利用に関するセキュリティ関連事項（要機密情報を取扱う場合）	パッケージソフトウェア、クラウドサービスの選定・利用に関する共通セキュリティ要件、成果物の取扱い
そのほか特記事項	機器などのセキュリティ確保、制約条件

附属文書	要件定義書など

調達仕様書を作成するときに、特に注意が必要なポイントについて説明します。項目の詳細な説明は、ひな型を参照してください。

調達仕様書を作成するときに、特に注意が必要なポイント

調達の意図や目的を正しく伝える

外部業者からプロジェクトにとって有用な提案をもらうためには、以下の点をしっかり伝える必要があります。

- プロジェクトの背景と目的
このプロジェクトがなぜ必要なのか、達成したい目標を明確に説明します。業者がプロジェクトの意図を理解しやすくなります。
- 調達の経緯と期待する効果
なぜこの調達が必要になったのか、どんな成果や効果を期待しているのかを詳しく説明します。業者が具体的な提案を考えやすくなります。
- プロジェクトの全体像とスケジュール
プロジェクトの全体的な流れやスケジュールを示すことで、業者がプロジェクトの全体像を把握しやすくなります。

これらの情報は、調達仕様書の「調達案件の概要」に記載し、プロジェクト全体のスケジュールも含めることで、業者がより適切で有用な提案をしやすくなります。

作業内容・納品物を関連付けて網羅的に記載する

調達仕様書では、外部事業者の作業内容、納品物をそれぞれ漏れなく定める必要があります。しかし、設計・開発などの調達では多種多様な作業や納品物があるため、漏れなく記載するのは困難です。これらを定義する際は、作業内容、納品物を関連付けて定義していくことで、効果的に抜け漏れを確認していくことができます。作業の実施内容と納品物を関連付けて一覧としてまとめておくと、工程完了時の納品物のチェックにも活用でき、検収時の確認負荷を減らせます。

外部事業者の具体的な作業内容を明確にする

外部事業者が実際に何を実施する必要があるのか理解できるように、作業内容を明確に記載することが重要です。

例えば、「支援」という言葉は人によって解釈が大きく異なります。「マニュアル作成支援」という作業項目があった際、2つの役割分担が考えられます。1つ目は、従業員がもととなる原案や素

材を用意した上で事業者が体裁を整えるという役割分担です。2つ目は、事業者がマニュアルの原案自体を作成して従業員が内容を確認するという役割分担です。このような役割分担の違いによって、事業者が実施する作業範囲や必要工数は大きく変わります。実際に実施する内容が事業者に正確に伝わらない場合、上記の事態をまねくおそれがあるため、事業者に実施を求める内容は正確に記述することが重要です。

作業内容が曖昧な場合に懸念される事態

- 必要な人員のスキルや数について、外部事業者の想定と発注者側の希望や想定がミスマッチとなる場合、契約した後に業務を完遂できない。
- 作業を終えることができて、成果物の品質（機能性、信頼性、使用性、効率性、保守性、移植性）が著しく低下する。
- 契約した外部事業者からの問い合わせや協議などが増加し、発注者側に想定していた以上の作業が発生する。

作業の実施体制を明確にする

調達案件を通じてプロジェクトの活動を円滑に進めていくためには、発注者側であるプロジェクト管理を行うチームや担当者や関係する従業員が、体制や役割分担、責任範囲を明確にし、外部事業者と一緒に協働していくことが大切です。調達仕様書や要件定義書をしっかり記載し、適切な外部事業者を選定することが仮にできたとしても、望んだ情報システムを必ずしも手に入れられるわけではありません。プロジェクトを進めていくと、要件の内容を設計として具体化・詳細化していく中で発注者側が決定しなければならないこと、他の関係者と調整しなければならないことは多く発生します。また、進捗上の課題や問題が発生した場合に発注者側の判断を要する場合があります。

サービス・業務の企画や要件定義のように新しいサービス・業務や情報システムの内容を決定するような活動においては、特に注意が必要です。意思決定の責任は発注者にあることを認識した上で、プロジェクト管理を行うチームや担当者以外の関係者も含めて、適切な判断ができる体制を組成して調達仕様書に明示することが重要です。

成果物の取扱いに注意する（知的財産権）

知的財産権の取扱いについては、設計・開発した文書やアプリケーションプログラムの知的財産権が誰に帰属するかを明確にしておくことが重要です。

- パッケージ製品
全く改変せず採用した場合、その知的財産権は提供もとに帰属します。
- 蓄積データ
パッケージ製品を利用して蓄積されたデータの帰属については、発注者が所有することが一

般的です。

- 機能拡張やクラウド設定

発注者の要望に基づいて拡張した機能や設定の知的財産権については、契約内容により帰属先が変わります。

再委託に関する事項を定める

情報システム整備プロジェクトでは、規模が大きくなると多くの専門的役割が必要となり、特定分野の外部事業者を活用することが増えます。これらの事業者が再委託を行う場合、委託元が再委託先の作業を管理する責任がありますが、再委託に関するトラブルも少なくありません。

再委託の制限や条件、承認手続き、再委託先の契約違反に関する規定を調達仕様書に記載し、責任の所在を明確にすることが重要です。また、プロジェクト遂行中の体制変更も、発注者と協議しながら進める必要があります。再委託に関しては、情報[セキュリティポリシー](#)の規定も確認する必要があります。

納品後に不具合が発覚したときの責任を明確にする（契約不適合責任）

2020 年 4 月に施行された改正民法により、「瑕疵担保責任」が廃止され、代わりに「契約不適合責任」が導入されました。これは、システム納品後の不具合に対する責任を、契約で定められた種類、品質、数量に適合しているか否かに基づいて判断するものです。この改正は、取引の実情に合わせたものであり、特に請負契約において次のような相違点が重要です。

- 救済手段の多様化

契約不適合責任では、契約の解除、損害賠償請求に加えて、修補や代替物の引渡し、報酬減額請求など、多様な救済手段が追加されました。

- 権利行使期間の変更

瑕疵担保責任では瑕疵を知ってから 1 年以内に権利行使をする必要がありましたが、契約不適合責任では不適合を知ったときから 1 年以内に通知すれば救済が可能になりました。

- 「隠れた瑕疵」の要件の廃止

瑕疵担保責任では、発注者が瑕疵の存在について善意無過失であったこと（瑕疵が「隠れた瑕疵」であったこと）が要件とされていましたが、契約不適合責任ではこの要件はなくなり、「隠れた瑕疵」でなくても業者の責任を問うことができるようになりました。

適正な価格で最適な業者の選定

中小企業が適正な価格で最適な業者を選定し、不利益を被らないような、実施可能な手続きについて説明します。

調達仕様書の明確化

中小企業にとって、調達仕様書が曖昧だと、不要な追加コストが発生するリスクが高まります。具体的な要求内容、納品スケジュール、品質基準などを明確に記載し、業者が正確な見積りを行えるようにすることが重要です。また、調達仕様書を適切に作成することで、業者の作業内容を厳密に管理し、不適切な追加請求を防げます。

透明性と公平性の維持

調達プロセス全体において透明性と公平性を確保することは、中小企業が不利益を被らないために不可欠です。提案依頼書や契約書の内容を整合性のあるものにし、期待する成果が正確に伝わるようにすることで、業者との間に不必要な誤解が生じるリスクを軽減します。

複数の見積り取得

中小企業が適正な価格を確保するためには、必ず複数の業者から見積りを取得し、比較検討することが必要です。三点見積りを活用することで、極端な価格設定による影響を排除し、より適正な予算を設定できます。また、特定の業者に依存するリスクを避けるため、依頼する業者を増やす工夫が大切です。

EC サイト構築における、3 点見積りの実施例

中小企業が SaaS やパッケージソフトウェアを用いて EC サイトを構築する際、セキュリティ対策や運用・保守コストを含めた三点見積りを実施する例を説明します。

平均見積りの計算式

平均見積り = (楽観値 + 4 × 最頻値 + 悲観値) / 6

楽観値	最も良い条件が揃った場合の最低コスト。追加コストやリスクが発生せず、プロジェクトが順調に進むことを想定した見積りです。
最頻値	一般的な条件で進行した場合の予測コスト。通常のリスクや変動を含めた、最も現実的な見積りです。
悲観値	最悪の状況が発生した場合の最高コスト。予期しない問題や追加のコストが発生する場合を考慮した見積りです。

この式では最頻値に重きを置き、楽観値と悲観値を考慮してより現実的な平均を算出します。

SaaS 型サービス A（標準プラン）

サービス内容：クラウドベースの EC プラットフォーム。テンプレートを使って簡単にサイトを作成可能。基本的なセキュリティ機能を提供し、月額利用料で運用可能。

楽観値：60 万円（基本プランと最低限のセキュリティ対策）

最頻値：75 万円（追加のカスタマイズと標準的なセキュリティ対策）

悲観値：120 万円（高度なカスタマイズと強化されたセキュリティ対策）

平均見積り：80 万円

パッケージソフトウェア B

サービス内容：自社サーバにインストール可能なソフトウェア。高度なカスタマイズが可能で、独自の機能を追加可能。セキュリティや保守管理が必要。

楽観値：80 万円（シンプルな設定と標準的なセキュリティ対策）

最頻値：100 万円（通常のカスタマイズと強化されたセキュリティ対策）

悲観値：130 万円（広範なカスタマイズと最強のセキュリティ対策）

平均見積り：約 102 万円

SaaS 型サービス C（上位プラン）

サービス内容：上位の SaaS プランで、より多くの機能や強化されたセキュリティ（[WAF](#)、不正利用検知など）を提供。追加のカスタマイズが可能。

楽観値：70 万円（標準プランと基本的なセキュリティ対策）

最頻値：90 万円（カスタマイズ対応と追加セキュリティ機能）

悲観値：170 万円（最上位プランと強化されたセキュリティ対策）

平均見積り：100 万円

三点見積りで比較した結果

SaaS 型サービス A（標準プラン）が、導入コストが最も低く、基本的なセキュリティ対策も標準装備されているため、コストパフォーマンスが最も高い選択肢です。

パッケージソフトウェア B は、カスタマイズ性が高く、独自の機能を追加したい企業に最適ですが、セキュリティや運用にかかる費用が増えるため、予算に余裕がある場合に適しています。

SaaS 型サービス C（上位プラン）は、SaaS の利便性を維持しつつ、セキュリティ機能や機能拡張が必要な場合に選ぶと良いですが、標準プランに比べて費用が増します。

セキュリティやコストバランスを考慮すると、SaaS 型サービス A（標準プラン）が最もバランスが良いと考えられます。

21-1-4. 設計・開発

中小企業でも、プロジェクトの計画立案とその管理は重要です。規模は小さくても、体系的なアプローチを取ることで、効率的な開発と品質の確保が可能になります。

設計・開発の計画

設計・開発事業者が決まれば、最初に行うことは計画を立てることです。設計・開発は実態が見えにくい活動になるため、問題の発覚が遅れて大惨事になることがあるため、しっかりと作成することが重要です。

設計・開発実施要領

プロジェクト・業務・情報システムの概要で、実施されるに当たり知っておくべき内容を記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	コミュニケーション管理	設計・開発事業者が参加すべき会議、開催頻度、議事録などの管理
3	体制管理	作業体制の管理手法
4	工程管理	設計、開発の作業、工程の管理手法
5	品質管理	品質基準、品質管理方法
6	リスク管理	リスクを提示する際の手順や報告様式
7	課題管理	課題を提示する際の手順や報告様式
8	システム構成管理	ハードウェアやソフトウェア製品、ネットワークなどの各資産における管理項目
9	変更管理	管理対象、変更手順、管理手法
10	情報セキュリティ管理	情報セキュリティ確保に必要な対策

設計・開発実施計画書

プロジェクト・業務・情報システムの概要や実施するに当たり手順や内容をまとめたものを記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	設計・開発の対象範囲、作業概要
3	作業体制に関する事項	作業内容および関係者間の関係性、役割分担、責務
4	スケジュールに関する事項	作業内容およびスケジュール、マイルストーン

5	成果物に関する事項	成果物、品質基準、担当者、納入期限、納入方法、納入部数、構成、内容
6	開発形態、開発手法 開発環境、開発ツールなど	開発形態、開発手法、開発環境、開発ツール
7	そのほか	設計・開発の実施の事情に応じて必要な事項

実施計画書のスケジュールに関する事項で作成するスケジュール例を紹介します。

【マイルストーン】

No.	アクティビティの記述	プロジェクトのスケジュール期間				
		5月	7月	9月	11月	1月
1	キックオフ	◆				
2	仕様凍結		◆			
3	連携テスト開始				◆	
4	受入テスト開始					◆
5	リリース					◆

【スケジュール（概略）】

No.	アクティビティの記述	プロジェクトのスケジュール期間				
		5月	7月	9月	11月	1月
1	設計	■				
2	実装		■			
3	結合テスト			■		
4	総合テスト				■	
5	受入テスト					■

設計・開発・テストの管理

設計・開発の大部分の作業は事業者が行いますが、発注者が適切に関わらないと品質が落ちる可能性が高くなります。テストには、「単体テスト」、「結合テスト」、「総合テスト」などがあります。

ここでは、「受入テスト」例を紹介します。受入テストは、システムの妥当性を検証（ユーザーの要件や期待に合致しているか否か、システムが正しく機能するか）、バグや不具合の検出、ユーザーの満足度向上（ユーザーがシステムを実際に操作することによって、使いやすさや機能性に関するフィードバックを得る）のために実施します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	テスト体制	体制、役割、責任範囲

3	テスト環境	実施場所、環境、ツール、前提条件
4	作業内容	テスト対象、実施手順、確認・検証事項
5	作業スケジュール	全体スケジュール、各工程の作業スケジュール
6	テストシナリオ	確認・検証事項、テスト結果の予測
7	合否判定基準	品質基準、合否判定基準

21-1-5. サービス・業務の運営と改善

新しいシステムや業務プロセスを導入した後、それを定着させ、継続的に改善していくことは、中小企業の競争力維持に不可欠です。

業務の定着と次の備え

情報システムの設計・開発のリリースが近づいたところで、研修教育資料（業務マニュアルなど）を用いて、実業務を担当する従業員に対して教育を実施します。

EC サイト運営における業務マニュアル作成例と、作成に当たっての注意点を解説します。

EC サイトの運営業務は、大きく「フロントエンド業務」と「バックエンド業務」の2つに分けられます。

フロントエンド業務

商品の企画や仕入れ、マーケティング、EC サイトの制作など、主に「集客や商品の売上につながる業務」のことを指します。

フロントエンド業務の例

- 商品管理
商品の情報を EC サイトに登録し、在庫数と公開設定を行います。
- 注文処理
受注管理画面で注文を確認し、出荷準備を行い、配送状況を更新します。
- 顧客対応
顧客からの問い合わせや返品・交換リクエストに対応します。
- プロモーション管理
割引キャンペーンや特別オファーを設定し、広告バナーを作成して配置します。
- コンテンツ更新
ブログやニュースの投稿を行い、サイトデザインの変更を実施します。

バックエンド業務

商品情報の登録や受注管理、出荷、アフターサポートなど、「販売を支え、お客様の満足度を高める業務」のことを指します。

バックエンド業務の例

- 受注処理
顧客からの注文内容を確認し、在庫や決済状況をチェックした上で、注文ステータスを更新します。
- 在庫管理
在庫状況を定期的に確認し、補充や棚卸しし、新入荷商品のシステム登録を行います。
- 出荷作業
出荷リストに基づいて商品を梱包し、発送準備を整えて集荷を依頼します。
- 配送作業
商品の配送状況を追跡し、問題が発生した場合には配送業者と連絡を取り、顧客に対応します。
- アフターサービス
返品や交換、顧客クレームに迅速に対応し、顧客満足度を維持します。

バックエンド業務のマニュアル例を紹介します。

バックエンド業務マニュアル（例）

1.目的

このマニュアルは、EC サイトのバックエンド業務に関する標準手順を提供し、業務の効率化と品質向上を目的とします。

2.業務の流れ

2.1 受注処理

目的：顧客からの注文を迅速かつ正確に処理します。

1.注文確認：

- 毎日午前 10 時と午後 3 時にシステム内の「注文管理」画面を確認し、すべての新しい注文をリスト化します。
- 各注文の内容（商品名、数量、配送先）を確認し、備考欄に特記事項があればそれに従います。

2.決済確認：

- 決済状況を確認し、「支払い済み」ステータスでない場合は、決済プロセスをチェックします。

- 決済エラーが発生した場合、顧客に連絡し、再決済や別の支払い方法を提案します。

3.在庫確認：

- 各注文の商品の在庫数をシステム上で確認し、在庫切れが発生していないかを確認します。
- 在庫が不足している場合、直ちに仕入れ担当者に連絡し、在庫補充を手配します。

4.ステータス更新：

注文ステータスを「処理中」に変更し、システムに自動的に反映されるよう設定します。

2.2 在庫管理

目的：適切な在庫管理を行い、欠品を防ぎます。

1.在庫確認：

- 毎週月曜日の午前にシステムで在庫状況を確認します。特に在庫が少ない商品に対しては自動アラートを設定し、タイムリーに補充が行えるようにします。
- 在庫が特定の数値以下になった場合は、即時に仕入れ担当に通知され、発注が行われます。

2.棚卸し：

- 月末に物理的な在庫とシステム上の在庫を照合し、差異がないか確認します。
- 差異が発見された場合は、原因を特定し、システム上で修正します。

3.新入荷処理：

- 新しく入荷した商品が届いた場合、納品書と実際の在庫数を確認し、商品の状態をチェックします。
- 問題がなければ、システムに入荷処理を行い、在庫数を更新します。

2.3 出荷作業

目的：顧客に正確かつ迅速に商品をお届けます。

1.出荷指示：

- システムの「出荷準備」画面から、当日の出荷リストを取得します。
- 各商品を倉庫から取り出し、ピッキングリストに従って確認します。

2.梱包：

- 商品が破損しないよう、適切なサイズの梱包材を使用して商品を梱包します。
- 伝票（納品書や配送伝票）を正しく同梱し、配送業者のステッカーを貼り付けます。

3.発送準備：

発送業者に集荷依頼を出し、翌日集荷の確認が取れたら、システムで発送ステータスを「発送済み」に更新します。

2.4 配送作業

目的：配送状況を確認し、顧客に確実に商品を届けます。

1. 配送確認：

- 発送業者の追跡システムで、すべての配送中の商品のステータスを確認します。
- 配送中に問題が発生した場合は、業者に連絡し、問題解決を図ります。

2. 追跡番号連絡：

配送後、システム上で自動生成された追跡番号を、顧客にメールで通知します。

3. 問題対応：

配送トラブルが発生した場合は、迅速に配送業者と連絡を取り、顧客に問題が解決する見通しを通知します。

2.5 アフターサービス

目的：顧客満足度を向上させ、リピーターを増やします。

1. 返品対応：

- 顧客から返品リクエストがあった場合、商品の状態を確認し、返品の可否を決定します。
- 返品が承認された場合、システム上で返金処理を行い、顧客に返金確認メールを送ります。

2. 交換手続き：

不良品や誤配送が発生した場合、代替商品の発送手配を行い、顧客に交換手続きの詳細を案内します。

3. クレーム対応：

- 顧客からのクレームがあった場合、可能な限り迅速に対応し、問題解決を目指します。
- 必要に応じて、社内での対応策を共有し、再発防止策を講じます。

業務マニュアル作成時の注意点

- 業務マニュアルは、同じ業務に携わる担当者が共通の理解を持つために有効ですが、組織や取扱う情報の種類によっては、同じ業務でも異なるルールが存在する場合があります。いわゆる、ローカルルールと呼ばれるものです。これをすべて業務マニュアルに記載しようとすると、膨大な量となり、マニュアルの更新が追いつかず、現場とのかい離が発生するおそれがあります。同じ業務内で共通化するものと、組織ごとに個別に定めるものとで分けて業務マニュアルを作成することで、その後の保守性を向上させることができます。
- 業務マニュアルは、そのまま従業員向けの教育資料の一部とすることができます。そのことを念頭に、業務マニュアルの内容・構成を検討してください。
- 業務マニュアルには、具体的なシステムの操作手順にとらわれず、業務の流れや手順を中心に記述してください。その流れの説明において、情報システムのどの機能を使うのか、がわ

ければ、使いやすいものになります。情報システムの操作手順や画面説明の詳細はシステム用のマニュアルに任せることで、マニュアルの品質を上げることができます。

- 業務マニュアルは業務全体の業務フローを理解している従業員が作成、またはレビューすることが重要です。マニュアル上の業務説明が途中で途切れたり、内容の重要性に偏りが出たりすることが防げます。マニュアルができ上がったら、業務に初めて携わる従業員がそのマニュアルを読んで業務が行えるか、という観点でチェックすることが重要です。

業務の改善

サービス・業務を運営していく中で発生するさまざまな情報を集め、改善に向けた取組につながっていきます。情報システムの見直しが必要なものは「サービス・業務企画」に立ち戻り、運用保守の見直しが必要なものは「運用および保守」に立ち戻ります。これらに該当しないものは、日常的な改善として対応していく必要があります。具体的には次のようなものに該当します。

日常的に実施する改善事項の例

- 業務の見直し
情報システムに影響を与えない範囲であれば、日常的に実施が可能です。定期的な改善を検討し、その結果は業務手順書などに反映させることが大切です。
- 教育・訓練の見直し
具体的には教育資料の改訂やカリキュラムの改訂に相当します。現状の分析結果を踏まえて、より従業員に遡及できるような教育内容に作り替えていくことが大切です。
- モニタリングの見直し
日常的に把握すべき指標とその仕組みの見直しに相当します。[KPI](#)で取るべき指標値は、業務の状況に応じて変更しても構いませんので、それに応じて値の取得方法や内容を見直し、現状を正確に把握できるようにすることが大切です。

そのほか、利用者からの問い合わせが多い機能や操作などについては、マニュアルの改善やFAQに情報を追加・更新することで改善が図れるため、適宜改善を検討することが大切です。

外部委託先におけるセキュリティ対策の実施状況の定期的確認

外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先に委託する自社のセキュリティ対策を、選定時には実施可能かを確認するとともに、運用時においても継続的に実施状況を確認してください。確認すべきセキュリティ対策は以下の通りです。

- セキュリティ対策要件（運用時）の要件1～5の実施状況を定期的に確認してください。
- 確認頻度の目安としては、以下を参考にしてください。

- （要件 1 の確認頻度）随時
- （要件 2 の確認頻度）プラットフォーム診断は、少なくとも四半期に 1 回程度
Web アプリケーション診断は、新機能の開発や追加やシステム改修などを行ったタイミングで実施
- （要件 3 の確認頻度）少なくとも週に 1 回程度
- （要件 4 の確認頻度）少なくとも週に 1 回程度
- （要件 5 の確認頻度）少なくとも週に 1 回程度

NO	セキュリティ対策要件（運用時）	区分	自社で対応可能な要件	外部委託の活用で対応すべき要件
要件 1	サーバおよび管理端末などで利用しているソフトウェアをセキュリティパッチなどにより最新の状態にする。	必須		
要件 2	EC サイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須		
要件 3	Web サイトのアプリケーションやコンテンツ、設定などの重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須		
要件 4	システムの定期的なバックアップの取得およびアクセスログの定期的な確認を行い不正アクセスなどがあればアクセスの制限などの対策を実施する。	必須		
要件 5	重要な情報はバックアップを取得する。	必須		
要件 6	WAF を導入する。	推奨		
要件 7	サイバー保険に加入する。	推奨		

21-1-6. 運用および保守

システムの安定稼動と継続的な改善は、中小企業にとっても重要です。適切な運用・保守計画を立て、定期的に見直すことで、長期的なコスト削減と効率化が図れます。

運用・保守の計画

運用・保守を担当する事業者が決まったら、事業者とともに調達仕様書で示した内容から、運用・保守の詳細な作業内容や実施方法などを検討し、計画書と実施要領として明文化します。運用・保守の作業はこの計画に基づいて実施することになるため、作業が漏れたり不十分だったりすると後々問題を引き起こすこともあるため、注意が必要です。

運用計画書の作成

運用計画書には、以下のような内容を記載します。

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	運用作業の対象範囲、作業概要
3	作業体制に関する事項	定常時およびインシデント発生時の体制
4	スケジュールに関する事項	運用業務の年次、四半期ごと、月次、週次、日次などのスケジュール
5	成果物に関する事項	成果物、担当者、納入期限、納入方法、納入部数、納入場所など
6	運用形態、運用環境など	運用において採用する運用形態（オンサイト、リモートなど）、定常時および障害発生時における運用環境（本番環境、検証環境、研修環境などの有無）など
7	そのほか	運用を行う上で留意すべき前提条件、運用の時間や予算、品質などに関する制約条件

保守計画書の作成

NO	目次	主要な記載内容
1	はじめに	プロジェクト、業務、情報システムの概要
2	作業概要	保守作業の対象範囲、作業概要
3	作業体制に関する事項	定常時およびインシデント発生時の体制
4	スケジュールに関する事項	提案書などの内容、保守事業者からの情報提供などを踏まえた保守業務のスケジュール
5	成果物に関する事項	成果物、担当者、納入期限、納入方法、納入部数、納入場所など
6	保守形態、保守環境など	保守において採用する保守形態（オンサイト、リモートなど）、アップデートファイル（セキュリティパッチなど）の適用前テストなどを行う検証環境など

7	そのほか	保守を行う上で留意すべき前提条件、保守の時間や予算または品質などに関する制約条件

運用・保守の改善と業務の引継ぎ

運用・保守の改善は、継続的に実施していきます。改善の内容には定常的な作業の範囲内で実施できるものもあれば、契約更新や事業者の交代、ライセンスの切れ目やハードウェアの交換でしか対応できないものなど、さまざまなものがあります。これらは、対応できるタイミングが同一にはなりませんので、以下の点に留意して、確実に改善につなげるようにします。

改善を管理するポイント

- 運用・保守の定常的な作業内で解決が難しい課題は、「デジタル・ガバメント推進標準ガイドライン実践ガイドブック」の第8章「サービス・業務の運営と改善」内の問題管理として、どのタイミングで対応するかを明確に管理する。
- 現行の運用・保守契約期間では対応することが難しい大規模の改善については次回の契約において対応せざるを得ないものもあるので、改善のための予算規模やスケジュールなどについて計画を立て、関係者と事前調整を行うなど、早期から準備を進めておくことが重要である。

ECサイトを運営中の場合において実行すべき取組

ECサイトを運営中の場合においては、いつサイバー被害に遭ってもおかしくない状況を回避または、改善することが必要です。

取組 1. 過去を振り返って、これまでのセキュリティ対策が不十分ではないか自己点検する。

IPAが公開している「安全なウェブサイトの作り方」や、「ECサイト構築・運用セキュリティガイドライン」の付録にあるECサイトの構築時や運用時における講じるべきセキュリティ対策要件をまとめたチェックシートを活用して、自社のECサイトにおけるセキュリティ対策の自己点検を行ってください。

取組 2. セキュリティ対策が不十分であることがわかり、対策までに時間がかかる場合、対策までのサイバー被害リスクを減らすため、応急処置を行う。

セキュリティ対策が不十分であることがわかり、対策実施には時間がかかる場合、その間の攻撃リスクを減らすため、応急処置（例：[WAF](#)実装、サイバー保険への加入）を実施してください。

なお、サイバー保険については、さまざまな種類・プランがあり、万が一の際の補償内容・金額やカバーされる脅威の範囲はもとより、事業性（売上高など）やセキュリティ対策状況、過去のインシデント被害経験などにより保険料が決まるため、詳細は保険会社にご確認ください。

取組 3.セキュリティ対策の不十分な箇所を対策する。

セキュリティ対策の不十分な箇所を対策し、あわせて、長期的（EC サイトの運用を継続する期間）なトータルコストを評価し、SaaS 型サービスやモール型サービスの利用も検討してください。

要員の交代で情報が欠落しないようにする

事業者が交代すると知識やドキュメント化されていない情報が抜け落ちてしまうことで作業効率が下がるリスクがあります。場合によっては、事業者が情報を持ち逃げするリスクもあり、持ち逃げされた情報を取り戻すために費用が発生するような場合もあります。このような事態を避けるためにも、従業員や運用・保守事業者の交代時には、以下の点に注意して、情報が抜け落ちてしまうことを防ぐことが重要です。

従業員や事業者の交代の際に気を付ける点

- 計画時点で作業に対する成果物を明確化する。作業を実施する場合は、基本的に作業手順書を作成し提出するよう、合意する。
- 中間成果物となるようなドキュメント・コンテンツは、維持が必要なもの、維持が不要ないものを明確にしていく。
- 運用・保守作業に関係する事項は、従業員や事業者の特定の担当者が抱え込むことなく、必ずその作業を担当する事業者が管理するドキュメントに記載し管理する。

編集後記

本節では、はじめに「デジタル・ガバメント推進標準ガイドライン」の全体像を説明しました。次に EC サイトを具体例として取り上げ、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する際の流れと、セキュリティ対策の実装および運用のポイントを解説しました。

企画から要件定義、調達、設計・開発、運用保守などの各段階で、中小企業においても役に立つ部分を「デジタル・ガバメント推進標準ガイドライン」からピックアップして紹介しました。特に要件定義におけるセキュリティ要件は、組織で作成した適用宣言書をもとに決定することが重要です。[情報資産](#)におけるリスクを考慮して適切なセキュリティ要件を決めることで、情報システムのセキュリティ対策強化につながります。

「デジタル・ガバメント推進標準ガイドライン」は、政府や地方自治体の情報システム構築を前提としていますが、中小企業でも活用できる重要な部分が数多く記載されています。情報システムを導入する際は、本ガイドラインを参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能です。

第22章. サイバーセキュリティ対策を実践するための知識とスキル

章の目的

技術進歩に伴い次々と新しい脅威が生まれている中で、効果的で漏れのないセキュリティ対策を実践していくためには、IT 全般のスキルや知識を持つ人材の育成と確保が重要です。第 22 章では、各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識について、体系的に理解することを目的とします。

主な達成目標

- 具体的な実施のために必要となる「役割やタスク」「スキルや知識」について、人材育成・人材確保のための各種スキル標準のフレームワークをもとに体系的に理解すること
- 各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること
- スキルや知識の認定制度と活用方法を理解すること

22-1. デジタルスキル標準（DSS）

デジタルスキル標準は「DX リテラシー標準」と「DX 推進スキル標準」の2つの標準で構成されます。「DX リテラシー標準」は、すべてのビジネスパーソンに向けた指針およびそれに応じた学習項目例を定義しています。「DX 推進スキル標準」は、DX を推進する人材の役割（ロール）および必要なスキルを定義しています。

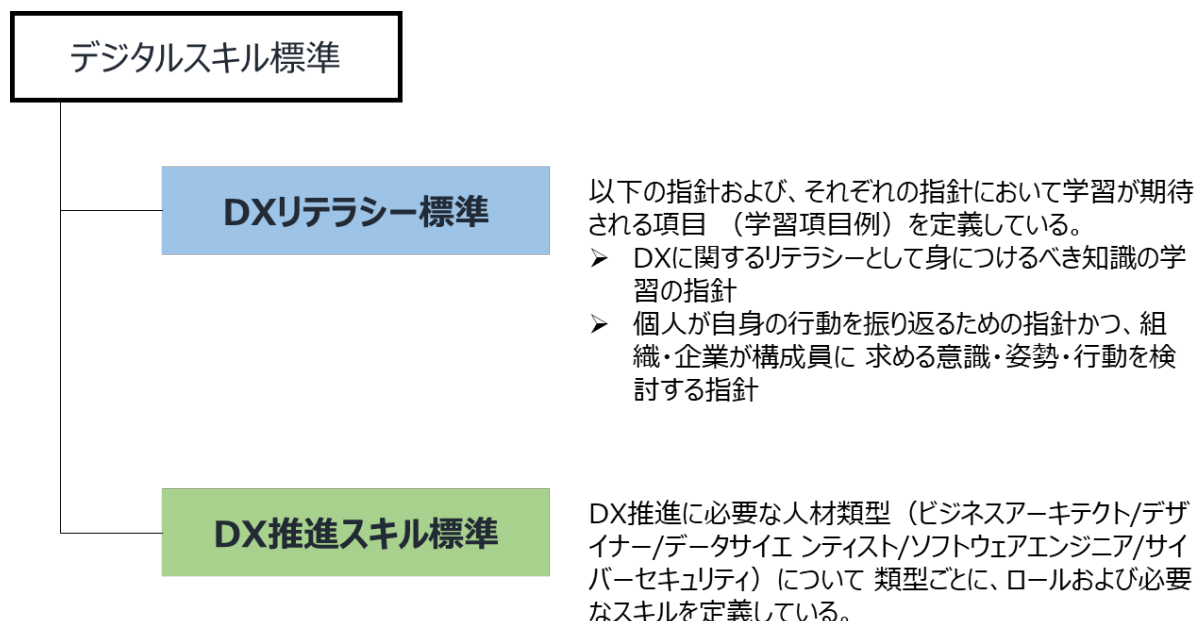


図 86. デジタルスキル標準の構成
(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf

22-1-1. DX リテラシー標準（DSS-L）

「DX リテラシー標準」は、すべてのビジネスパーソンが身につけるべきデジタルトランスフォーメーション（DX）に関する基礎的な知識、スキル、マインドセットの学習指針です。企業は、従業員に対して、DX に関するリテラシーを身につけさせるための指針として活用できます。

DX リテラシー標準は、特定の産業や職種、部署などに依存しない汎用性を重視して作成されています。そのため、企業や組織がこれを適用する際には、自身が属する産業や事業の方向性に合わせる必要があります。

DXリテラシー標準

自社の事業の方向性に
合わせる必要があります

DX リテラシー標準は、「標準策定のねらい」「マインド・スタンス」「Why (DX の背景)」「What (DX で活用されるデータ・技術)」「How (データ・技術の利活用方法)」で構成されています。

急速に普及する生成 AI は、各企業における DX の進展を加速させると考えられ、企業の競争力を向上させる可能性があります。あわせて、ビジネスパーソンに求められるスキルも変化し、より重要になる部分もあると想定されます。DX リテラシー標準は上記の状況に対応するため、令和 5 年 8 月に改訂されました。改訂箇所は、下記の図の太文字と下線で示した箇所です。

標準策定のねらい

ビジネスパーソン一人一人がDXに関するリテラシーを身につけることで、DXを自分事ととらえ、変革に向けて行動できるようになる

Why (DXの背景)

産官学で生成AIの利用が進んでおり、社会環境へ影響を与える可能性があるため、「**社会の変化**」に**人材育成・教育や労働市場の変化等の学習項目例を追加**

What (DXで活用されるデータ・技術)

- ✓ 生成AIは、ビジネスの場で急速に普及・利用されているため、「**AI**」に**生成AIの技術動向や倫理等の学習項目例を追加**
- ✓ 現在の利用状況に鑑み「**ネットワーク**」に**ネットワークの種類、インターネットサービスの学習項目例を追加**
- ✓ 個人や企業等で扱うデータがデジタル技術・サービスに活用されるため、「**データを扱う**」に**活用しやすいデータの入力や整備の手法などの内容・学習項目例を追加**
- ✓ 適切でないデータから生み出される結果は、誤った判断・損害につながり得るため、「**データによって判断する**」に**適切なデータを用いて判断することの重要性などの内容・学習項目例を追加**

How (データ・技術の利活用)

- ✓ 生成AIは、ツールなどの基礎知識や指示（プロンプト）の手法を用いて業務の様々な場面で利用できるため、「**データ・デジタル技術の活用事例**」に**生成AIの活用事例、「ツール利用に生成AIツール概要・利用方法などの学習項目例をそれぞれ追加**
- ✓ 情報漏えいや法規制、利用規約などに正しく対処しながら生成AIを利用することが求められるため、「**モラル**」に**データ流出の危機性等、「コンプライアンス」に法規制や利用規約などの学習項目例をそれぞれ追加**

マインド・スタンス

- ✓ 他項目と比べて**より普遍的な要素を定義**しているため、**生成AI利用においても同様に重要**となる
- ✓ 適切なデータを用いることにより、事実に基づく判断が有効になるため、「**事実に基づく判断**」に**適切なデータ入力の重要性や行動例などを追加**
- ✓ **生成AIをビジネスパーソンとしてのスキルと掛け合わせ生産性向上やビジネス変革などへ適切に利用しようとしていること、生成AI利用における注意点を理解していること、生成AIの影響に対して変化をいとわず学び続けることは、今後、全ビジネスパーソンが身に着けるべきマインド・スタンスとして重要性が増すため、「生成AI利用において求められるマインド・スタンス」として既存項目と分けて追加**

図 87. DX リテラシー標準の全体像

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

項目一覧

Why (DXの背景)	What (DXで活用されるデータ・技術)		How (データ・技術の利活用)		
社会の変化	データ	社会におけるデータ	活用事例・利用方法	データ・デジタル技術の活用事例	
顧客価値の変化		データを読む・説明する		ツール利用	
競争環境の変化		データを扱う	留意点	セキュリティ	
		データによって判断する		モラル	
	デジタル技術	AI		コンプライアンス	
		クラウド			
		ハードウェア・ソフトウェア			
		ネットワーク			
マインド・スタンス					
デザイン思考/アジャイルな働き方	顧客、ユーザへの共感		常識にとらわれない発想	反復的なアプローチ	
新たな価値を生み出す基礎としてのマインド・スタンス	変化への適応		コラボレーション	柔軟な意思決定	事実に基づく判断

図 88. DX リテラシー標準の項目一覧

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

One Point

DX リテラシー標準の学習方法

IPA が運営する「マナビ DX」という、すべての社会人にとって必須であるデジタルスキルを学べるコンテンツを紹介しているポータルサイトがあります。このポータルサイトでは、DX リテラシー標準の各項目ごとに学習できる講座が掲載されており、DX リテラシーを学ぶことができます。

詳細理解のため参考となる文献（参考文献）

マナビ DX

<https://manabi-dx.ipa.go.jp/>

マインド・スタンス

学習のゴール

社会変化の中で新たな価値を生み出すために必要なマインド・スタンスを知り、自身の行動を振り返ることができること。

項目の内容・学習項目

項目	内容	学習項目例
変化への適応	● 環境や仕事・働き方の変化を受け入れ、適応するために自ら主体的に学んでいる ● 自身や組織が持つ既存の価値観について尊重すべき点を認識しつつ、環境変化に応じた新たな価値観、行動様式、知識、スキルを身につけている	● 各自が置かれた環境において目指すべき、具体的な行動や影響例など
コラボレーション	● 価値創造のためには、さまざまな専門性を持った人と社内・社外問わずに協働することが重要であることを理解し、多様性を尊重している	
顧客・ユーザーへの共感	● 顧客・ユーザーに寄り添い、顧客・ユーザーの立場に立ってニーズや課題を発見しようとしている	
常識にとらわれない発想	● 顧客・ユーザーのニーズや課題に対応するためのアイデアを、既存の概念・価値観にとらわれずに考えている ● 従来の物事の進め方について理由を自ら問い、より良い進め方がないか考えている	
反復的なアプローチ	● 新しい取組や改善を、失敗を許容できる範囲の小さいサイクルで行い、顧客・ユーザーのフィードバックを得て反復的に改善している ● 失敗したとしてもその都度軌道修正し、学びを得ることができれば「成	

	果」であると認識している	
柔軟な意思決定	● 既存の価値観に基づく判断が難しい状況においても、価値創造に向けて必要であれば、臨機応変に意思決定を行っている	
事実に基づく判断	● 勘や経験のみではなく、客観的な事実やデータに基づいて、物事を見たり、判断したりしている ● 適切なデータを用いることにより、事実やデータに基づく判断が有効になることを理解し、適切なデータの入力を意識して行っている	

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

Why (DX の背景)

学習のゴール

人々が重視する価値や社会・経済の環境がどのように変化しているか知っており、DX の重要性を理解している

項目の内容・学習項目例

項目	内容	学習項目例
社会の変化	● 世界や日本社会に起きている変化を理解し、変化の中で人々の暮らしをよりよくし、社会課題を解決するためにデータやデジタル技術の活用が有用であることを知っている	● メガトレンド・社会課題とデジタルによる解決 (SDGs など) ● 日本と海外における DX の取組の差、社会・産業の変化に関するキーワード (Society5.0、データ駆動型社会など)
顧客価値の変化	● 顧客価値の概念を理解し、顧客・ユーザーがデジタル技術の発展によりどのように変わってきたか (情報や製品・サービスへのアクセスの多様化、人それぞれのニーズを満たすことへ	● 顧客・ユーザーの行動変化と変化への対応 ● 顧客・ユーザーを取り巻くデジタルサービス

	の欲求の高まり)を知っている	
競争環境の変化	データ・デジタル技術の進展や、社会・顧客の変化によって、既存ビジネスにおける競争力の源泉が変わったり、従来の業種や国境の垣根を超えたビジネスが広がったりしていることを知っている	デジタル技術の活用による競争環境変化の具体的事例

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

What (DXで活用されるデータ・技術)

学習のゴール

DX推進の手段としてのデータやデジタル技術に関する最新の情報を知った上で、その発展の背景への知識を深めることができる

項目の内容・学習項目例

項目	内容	学習項目例
(データ) 社会におけるデータ	「データ」には数値に加えて、文字・画像・音声などさまざまな種類があることや、それらがどのように蓄積され、社会で活用されているか知っている	- データの種類 - 社会におけるデータ活用
(データ) データを読む・説明する	- データの分析手法や結果の読み取り方を理解している - データの分析結果の意味合いを見抜き、分析の目的や受け取り手に応じて、適切に説明する方法を理解している	- データの分析手法(基礎的な確率・統計の知識) - データを読む(比較方法・重複など) - データを説明する(可視化・分析結果の言語化)
(データ) データを扱う	- デジタル技術・サービスに活用しやすいデータの入力や整備の手法を理解している - データ利用には、データ抽出・加工に関するさまざまな手法やデータベースなどの技術が欠かせない場面があることを理解している	- データの入力 - データの抽出・加工(クレンジング・集計など) - データの出力 - データベース(データ

		ベースの種類、構造など)
(データ) データによって判断する	● 業務・事業の構造、分析の目的を理解し、データを分析・利用するためのアプローチを知っている ● 期待していた結果とは異なる分析結果が出たとしても、それ自体が重要な知見となることを理解している ● 分析の結果から、経営や業務に対する改善のアクションを見出し、アクションの結果どうなったかモニタリングする手法を理解している ● 適切なデータを用いることで、データに基づく判断が有効となることを理解している	● データドリブンな判断プロセス ● 分析アプローチ設計 ● モニタリングの手法
(デジタル技術) AI	● AI が生まれた背景や、急速に広まった理由を知っている ● AI の仕組みを理解し、AI ができること、できないことを知っている ● AI 活用の可能性を理解し、精度を高めるためのポイントを知っている ● 組織/社会でよく使われている AI の動向を知っている	● AI の歴史 ● AI を作るための手法・技術 ● AI の得意分野・限界 ● 人間中心の AI 社会原則、ELSI ● 最新の技術動向(生成 AI など)
(デジタル技術) クラウド	● クラウドの仕組みを理解し、クラウドとオンプレミスの違いを知っている ● クラウドサービスの提供形態を知っている	● クラウドの仕組み(データの持ち方、データを守る仕組み) ● クラウドサービスの提供形態 (SaaS、IaaS、PaaS など) ● 最新の技術動向
(デジタル技術) ハードウェア・ソフトウェア	● コンピュータやスマートフォンなどが動作する仕組みを知っている ● 社内システムなどがどのように作られているかを知っている	● ハードウェア(ハードウェアの構成要素、コンピュータの種類) ● ソフトウェア(ソフトウェアの種類、プログ

		ラミング的思考) ● 企業における開発・運用 ● 最新の技術動向
(デジタル技術) ネットワーク	● ネットワークの基礎的な仕組みを知っている ● インターネットの仕組みや代表的なインターネットサービスを知っている	● ネットワークの仕組み (LAN・ WAN 、通信プロトコル) ● インターネットサービス (電子メール) ● 最新の技術動向

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

How (データ・技術の利活用)

学習のゴール

データ・デジタル技術の活用事例を理解し、その実現のための基本的なツールの利用方法を身につけた上で、留意点などを踏まえて実際に業務で利用できる

項目の内容・学習項目例

項目	内容	学習項目例
(活用事例・利用方法) データ・デジタル技術の活用事例	● ビジネスにおけるデータ・デジタル技術の活用事例を知っている ● データ・デジタル技術がさまざまな業務で利用できることを理解し、自身の業務への適用場면을想像できる	● 事業活動におけるデータ・デジタル技術の活用事例 ● 生成 AI の活用事例
(活用事例・利用方法) ツール利用	● ツールの利用方法に関する知識を持ち、日々の業務において、状況に合わせて適切なツールを選択できる	● 日常業務に関するツールの利用方法 ● 生成 AI の利用方法 ● 自動化・効率化に関するデジタルツールの利用方法
(留意点) セキュリティ	● セキュリティ技術の仕組みと個人が取るべき対策に関する知識を持ち、安心してデータやデジタル技術を利用できる	● セキュリティの 3 要素 ● セキュリティ技術 ● 個人が取るべきセキ

		ユリティ対策
(留意点) モラル	● 個人がインターネット上で自由に情報のやり取りができる時代において求められるモラルを持ち、インターネット上で適切にコミュニケーションできる ● 捏造、<u>改ざん</u>、盗用などのデータ分析における禁止事項を知り、適切にデータを利用できる ● データ流出の危険性や影響を想像できる	● ネット被害・SNS・生成 AI などのトラブルの事例・対策 ● データ利用における禁止事項・留意事項
(留意点) コンプライアンス	● プライバシー、知的財産権、著作権の示すものや、その保護のための法律、諸外国におけるデータ規制などについて知っている ● 実際の業務でデータや技術を利用するときに、自身の業務が法規制や利用規約に照らして問題ないか確認できる	● 個人情報の定義と個人情報に関する法律・留意事項 ● 著作権・産業財産権・その他の権利が保護する対象 ● 諸外国におけるデータ規制 ● サービス利用規約を踏まえたデータの利用範囲

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

22-1-2. DX 推進スキル標準 (DSS-P)

DX 推進スキル標準は、人材の種類ごとに必要なスキルの重要度をまとめたものです。人材の種類は、5 つの人材類型（ビジネスアーキテクト/デザイナー/データサイエンティスト/ソフトウェアエンジニア/サイバーセキュリティ）と、その下位区分である 15 のロールに区分されています。一方のスキルは、DX を推進する人材に求められる約 50 のスキルが 5 つのカテゴリ・12 のサブカテゴリに分けられています。このスキルの体系は、すべての人材類型・ロールに共通のものになっており、「共通スキルリスト」と呼ばれています。

人材類型			ビジネスアーキテクト	デザイナー	データサイエンティスト	ソフトウェアエンジニア				サイバーセキュリティ										
ルール (DXの推進において担う責任、主な業務、必要なスキルにより定義)			ビジネスアーキテクト (新規事業開発)	ビジネスアーキテクト (既存事業の高度化)	ビジネスアーキテクト (社内業務の高度化・効率化)	サービスデザイナー	UX/UIデザイナー	グラフィックデザイナー	データビジネスストラテジスト	データエンジニア	データサイエンスプロフェッショナル	フロントエンドエンジニア	バックエンドエンジニア	クラウドエンジニア/SRE	フィジカルコンピューティングエンジニア	サイバーセキュリティマネージャー	サイバーセキュリティエンジニア			
			全人材類型に共通の「共通スキルリスト」から各ロールに必要なスキルを定義																	
			各ロールに必要なスキル			・	・	・								・	・	・	・	
			共通スキルリスト																	
			ビジネスイノベーション			スキル項目...														
データ活用			スキル項目...																	
テクノロジー			スキル項目...																	
セキュリティ			スキル項目...																	
パーソナルスキル			スキル項目...																	

図 89. DX 推進スキル標準の構成

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

※ 5 種類の人材類型のうち「サイバーセキュリティ」のみが、人称ではなく対象分野名となっています。

各人材タイプのロールと、DX 推進において担う責任は以下の通りです。

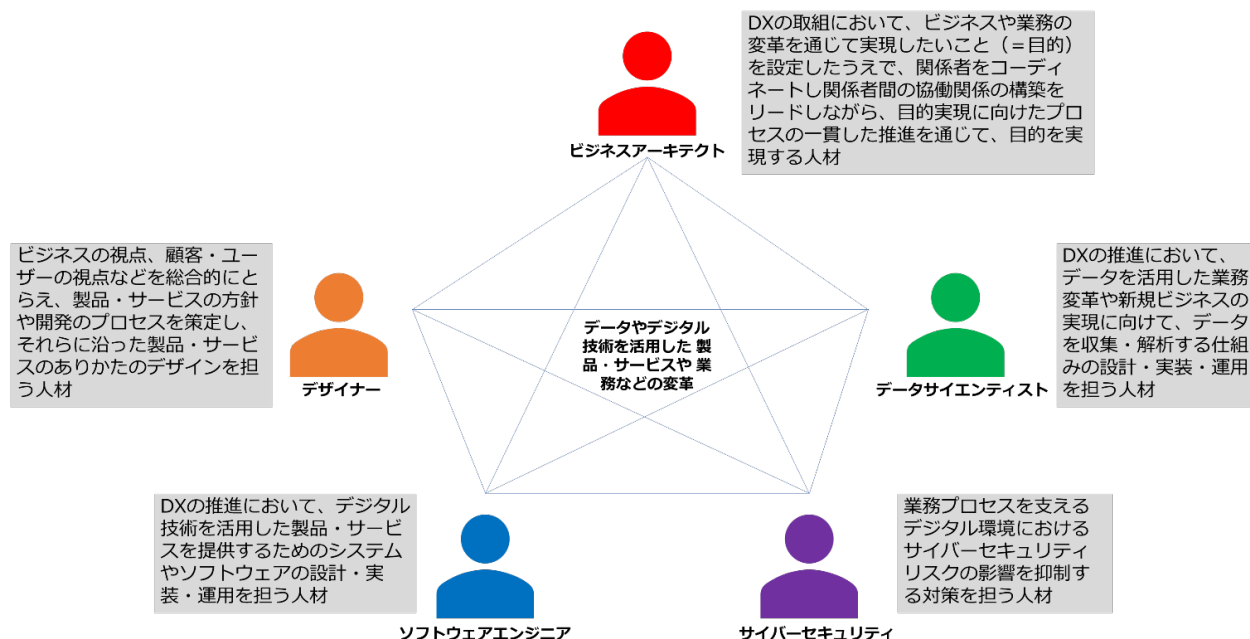


図 90. 人材タイプの定義

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

人材類型	ロール	DX 推進において担う責任
ビジネス アーキテ クト	ビジネスアーキテクト (新規事業開発)	新しい事業、製品・サービスの目的を見出し、新しく定義した目的の実現方法を策定した上で、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
	ビジネスアーキテクト (既存事業の高度化)	既存の事業、製品・サービスの目的を見直し、再定義した目的の実現方法を策定した上で、関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
	ビジネスアーキテクト (社内業務の高度化・効率化)	社内業務の課題解決の目的を定義し、その目的の実現方法を策定した上で関係者をコーディネートし関係者間の協働関係の構築をリードしながら、目的実現に向けたプロセスの一貫した推進を通じて、目的を実現する
デザイナ ー	サービスデザイナー	社会、顧客・ユーザー、製品・サービス提供における社内外関係者の課題や行動から顧客価値を定義し製品・サービスの方針（コンセプト）を策定するとともに、それを継続的に実現するための仕組みのデザインを行う
	UX/UI デザイナー	バリュープロポジションに基づき製品・サービスの顧客・ユーザー体験を設計し、製品・サービスの情報設計や、機能、情報の配置、外観、動的要素のデザインを行う
	グラフィックデザイナー	ブランドのイメージを具現化し、ブランドとして統一感のあるデジタルグラフィック、マーケティング媒体などのデザインを行う
データサイエ ンティスト	データビジネスストラテジスト	事業戦略に沿ったデータの活用戦略を考えるとともに、戦略の具体化や実現を主導し、顧客価値を拡大する業務変革やビジネス創出を実現する
	データサイエンスプロフェッショナル	データの処理や解析を通じて、顧客価値を拡大する業務の変革やビジネスの創出につながる有意義な知見を導出する
	データエンジニア	効果的なデータ分析環境の設計・実装・運用を通じて、顧客価値を拡大する業務変革やビジネス創出を実現する
ソフトウ	フロントエンドエン	デジタル技術を活用したサービスを提供するためのソフト

ウェアエンジニア	エンジニア	ウェアの機能のうち、主にインターフェース（クライアントサイド）の機能の実現に主たる責任を持つ
	バックエンドエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの機能のうち、主にサーバサイドの機能の実現に主たる責任を持つ
	クラウドエンジニア／SRE	デジタル技術を活用したサービスを提供するためのソフトウェアの開発・運用環境の最適化と信頼性の向上に責任を持つ
	フィジカルコンピューティングエンジニア	デジタル技術を活用したサービスを提供するためのソフトウェアの実現において、現実世界（物理領域）のデジタル化を担い、デバイスを含めたソフトウェア機能の実現に責任を持つ
サイバーセキュリティ	サイバーセキュリティマネージャー	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
	サイバーセキュリティエンジニア	事業実施に伴うデジタル活用関連のサイバーセキュリティリスクを抑制するための対策の導入・保守・運用を通じて、顧客価値の高いビジネスの安定的な提供に貢献する

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

共通スキルリストの全体像

全人材類型に共通する「共通スキルリスト」は、DXを推進する人材に求められるスキルを5つのカテゴリ・12のサブカテゴリで整理しています。

各カテゴリは2つか3つのサブカテゴリに分け、1つ目では主要な活動を、2つ目以降ではそれを支える要素技術と手法を、大くりに整理しています。

カテゴリ	サブカテゴリ	スキル項目
ビジネス変革	戦略・マネジメント・システム	ビジネス戦略策定・実行
		プロダクトマネジメント
		変革マネジメント
		システムズエンジニアリング
		エンタープライズアーキテクチャ
		プロジェクトマネジメント

	ビジネス・モデル・プロセス	ビジネス調査
		ビジネスモデル設計
		ビジネスアナリシス
		検証（ビジネス視点）
		マーケティング
		ブランディング
	デザイン	顧客・ユーザー理解
		価値発見・定義
		設計
		検証（顧客・ユーザー視点）
データ活用	データ・ AI の戦略的活用	データ理解・活用
		データ・AI 活用戦略
		データ・AI 活用業務の設計・事業実装・評価
	AI・データサイエンス	数理統計・多変量解析・データ可視化
		機械学習・深層学習
	データエンジニアリング	データ活用基盤設計
		データ活用基盤実装・運用
テクノロジー	ソフトウェア開発	コンピュータサイエンス
		チーム開発
		ソフトウェア設計手法
		ソフトウェア開発プロセス
		Web アプリケーション基本技術
		フロントエンドシステム開発
		クラウドインフラ活用
		SRE プロセス
		サービス活用
	デジタルテクノロジー	フィジカルコンピューティング
		そのほか先端技術
		テクノロジートレンド
セキュリティ	セキュリティマネジメント	セキュリティ体制構築・運営
		セキュリティマネジメント
		インシデント対応と事業継続

	セキュリティ技術	プライバシー保護
		セキュア設計・開発・構築
		セキュリティ運用・保守・監視
パーソナルスキル	ヒューマンスキル	リーダーシップ
		コラボレーション
	コンセプチュアルスキル	ゴール設定
		創造的な問題解決
		批判的思考
		適応力

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

例として、セキュリティカテゴリの詳細を説明します。

カ テ ゴ リ	サ ブ カ テ ゴ リ	スキル項目	内容	学習項目例
セ キ ユ リ テ ィ	セ キ ユ リ テ ィ マ ネ ジ メ ン ト	セキュリティ体制構築・運営	● セキュリティ対策を実施する体制の構築とその維持運営（要員の確保・育成を含む）を円滑に行うためのスキル ● 組織としてのセキュリティカルチャーを企業内で醸成する活動を行うためのスキル	● セキュリティ対応組織（セキュリティ統括機能、SOC、xSIRTなど）との連携手順 ● サービスや機器のセキュリティ対策に関する組織内の役割と責任の明確化 ● 組織におけるセキュリティカルチャーの醸成方法
		セキュリティマネジメント	● 情報、サイバー空間、OT/IoT 環境などのセキュリティマネジメントのプロセスを組織として適切に実施するためのスキル	● セキュリティ関連法制度 ● ポリシー、規程、マニュアルなどの整備 ● <u>脅威インテリジェンス</u>の活用を含むリスクの認知 ● <u>リスクアセスメント</u>手法

セキュリティ技			● セキュリティ要件定義、機能要件としてのセキュリティ機能 ● 認証方式の種類・特徴と選定方法 ● 情報資産管理、構成管理 ● セキュリティ教育・トレーニングと資格・認証制度 ● 情報セキュリティ監査の手法
	インシデント対応と事業継続	● 各種リスク（<u>サイバー攻撃</u>、過失、内部不正、災害、障害など）がデジタル利活用における<u>セキュリティインシデント</u>として顕在化した際の影響を抑制し、事業継続を可能とするためのスキル	● デジタル利活用における事業継続 ● 事業継続計画の整備と訓練 ● インシデント対応と危機管理の連携手順 ● 日常および緊急時の情報共有とコミュニケーション
	プライバシー保護	● パーソナルデータ等のプライバシー情報の保護に求められる要件の理解とその実践に関するスキル	● セキュアシステム設計の概要と実践方法 ● DevSecOps の考え方と実践方法 ● セキュリティ要件およびセキュリティ機能の実現・実装 ● IT/OT/IoT デバイスにおけるセキュリティ対策 ● クラウドサービスおよびネットワーク機器のセキュリティ機能の概要と設定 ● <u>脆弱性</u>の概念と対策・診断方法
	セキュア設計・開発・構築	● デジタルサービス・製品の企画設計を行う際に、サイバー攻撃や各種不正の影響を受けにくくするために遵守すべき基準や要件をもとに設計・開発・構築を行うスキル	● セキュアシステム設計の概要と実践方法 ● DevSecOps の考え方と実践方法 ● セキュリティ要件およびセキュリティ機能の実現・実装 ● IT/OT/IoT デバイスにおけるセ

	術		● デジタルサービス・製品の脆弱性について理解し、診断を適切に実践（委託による実施を含む）するためのスキル	キュリティ対策 ● クラウドサービスおよびネットワーク機器のセキュリティ機能の概要と設定 ● 脆弱性の概念と対策・診断方法
		セキュリティ運用・保守・監視	● デジタルサービスをセキュアに運用するための保守と対策を適切に実践するためのスキル ● セキュリティに関する監視とインシデントの原因究明などを適切に実践するためのスキル	● 脅威情報や脆弱性情報の活用 ● モニタリングの方法と観測データの活用 ● 運用・監視業務への AI 応用 ● インシデント時の影響調査、トリアージ方法 ● デジタルフォレンジックサービスの活用

(出典) IPA「デジタルスキル標準 ver1.2」をもとに作成

生成 AI に関する事項

DX を推進するには、新たに登場するデジタル技術がもたらす変化を捉え、それに対応していくことが重要です。ここでは、生成 AI を例にして、DX を推進する人材に求められる新技術への向き合い方、行動の起こし方などを説明します。

急速に進歩・普及する生成 AI は、各企業における DX を加速すると考えられ、企業の競争力に大きな影響を与える可能性があります。生成 AI の活用によって、新規事業の開発、知的労働や知的労働を伴う肉体労働の生産性向上などが期待できる一方、生成 AI 活用による権利侵害・情報漏えい、倫理的な問題などが発生しないよう十分に注意を払う必要があります。

前提	1 生成AIの特性	■ 生成AIの共通理解を図るため、生成AIの一般的な 特性 （用語の定義も含む）、 有用性、リスク を記載
	2 新技術（生成AI含む）への向き合い方・行動の起こし方	■ ビジネス・業務に変革をもたらすような新技術は、生成AIにとどまらず今後も登場すると想定され、それらへの対応が求められる。そのため、 DXを推進する人材に求められる新技術への向き合い方・行動の起こし方 を定義
生成AIに対するアクション	3 基本的な考え方 【活用する】と【開発、提供する】	■ 生成AIに対するアクションを定義するため、補記④以降の基本的な考え方となる生成AIに対する以下の観点を記載 ✓ 【活用する】：公開されている生成AIの業務での活用／組織・企業の業務プロセスなどに組み込まれた生成AIの活用 ✓ 【開発する、提供する】：ビジネスや組織の業務プロセスに対し、生成AIを組み込んだ製品・サービスを開発し、顧客・ユーザーに提供
	4 詳細定義	■ 生成AIに対するアクションの理解をより促すため、生成AIを 【活用する】【開発する、提供する】 際の、人材類型共通となる具体的な プロセス・内容、留意点 を記載
	5 個人として業務において生成AIを 【活用する】 例	■ 生成AIを 【活用する】 イメージを想起させるため、公開されている生成AIや、組織・企業の業務プロセスに組み込まれた生成AIを 業務で活用する際の例 を記載
	6 ビジネス・業務プロセスの生成AI製品・サービスを 【開発する、提供する】 際の行動例	■ 生成AIを 【開発する、提供する】 イメージを想起させるために、ビジネスや業務における製品・サービスに生成AIを組み込む際の 主要な行動例 を 人材類型別 に記載

図 91. 生成 AI に関する DX 推進スキル標準

(出典) IPA「生成 AI に関する DX 推進スキル標準の改訂 要旨（2024 年 7 月）」をもとに作成

22-2. IT スキル標準（ITSS）

22-2-1. 概要

IT スキル標準（ITSS）は、IT 分野で必要とされるスキルや知識を体系化し、評価するための指標です。経済産業省が 2002 年に策定し、現在は IPA が管理しています。ITSS は、IT 人材の育成に寄与することを目的としており、企業が共通して使用できるスキル指標を提供することで、キャリアパスの明確化やスキルの標準化に役立っています。

IT スキル標準の全体構成

IT スキル標準は、3 部で構成されます。全体構成の決定に際しては、国際規格や JIS 規格などの様式、記述方法を参考にしています。

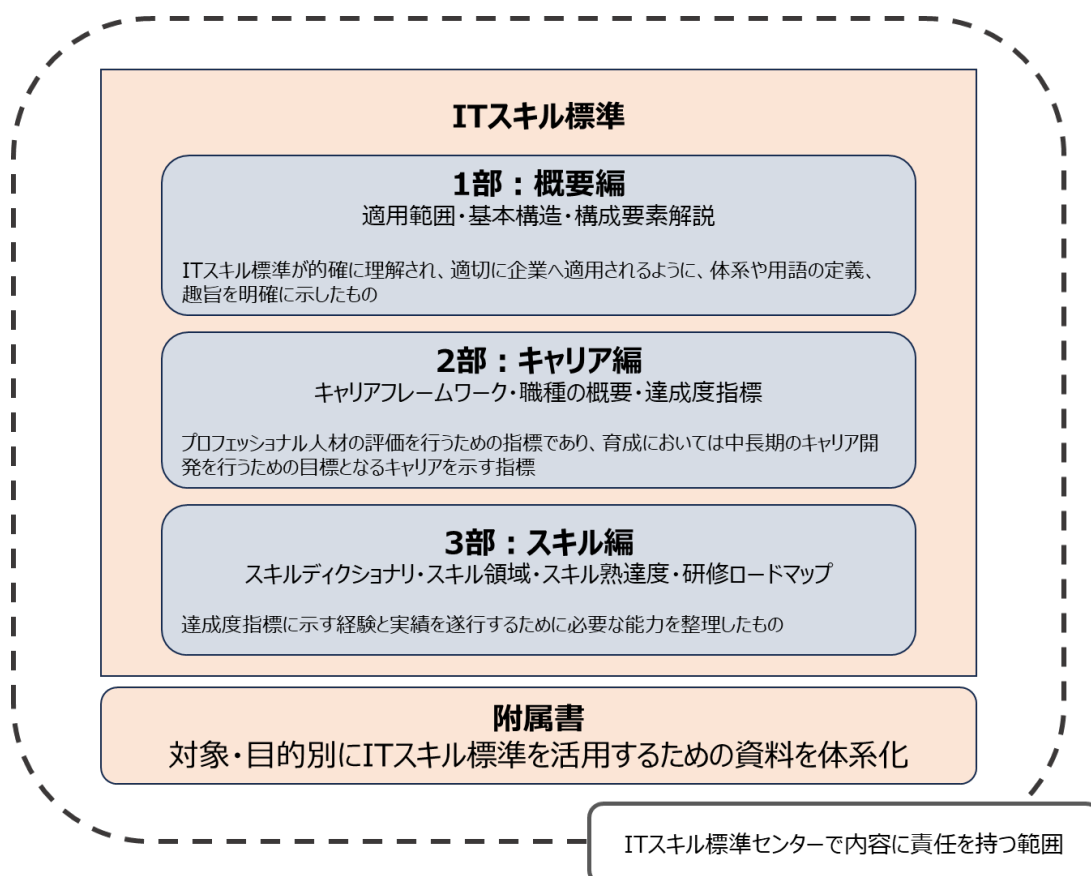


図 92. IT スキル標準の全体構成
(出典) IPA「デジタルスキル標準」をもとに作成

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
IT スキル標準 V3 2011 1部：概要編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf

22-2-2. キャリア

「2部：キャリア編」では、ITスキル標準の構成要素である「キャリアフレームワーク」、「職種の概要」、「達成度指標」を収めています。IT人材のレベル評価は、経験と実績に基づく「達成度指標」によって行うことがITスキル標準の特色です。キャリアフレームワークは横軸に職種区分、縦軸にレベル設定があり、11の職種と35の専門分野を設けています。また、それぞれの専門分野に対応して、各個人の能力や実績に基づく7段階の達成レベルを規定しています。キャリア編で定義したのは、プロフェッショナル人材の評価を行うための指標であり、育成においては中長期のキャリア開発を行うための目標となるキャリアを示す指標です。

キャリアフレームワークの職種と専門分野

職種	専門分野
マーケティング	マーケティングマネジメント
	販売チャネル戦略
	マーケットコミュニケーション
セールス	訪問型コンサルティングサービス
	訪問型製品セールス
	メディア利用型セールス
コンサルタント	インダストリ
	ビジネスファンクション
ITアーキテクト	アプリケーションアーキテクチャ
	インテグレーションアーキテクチャ
	インフラストラクチャアーキテクチャ
プロジェクトマネジメント	システム開発
	ITアウトソーシング
	ネットワークサービス
	ソフトウェア製品開発
ITスペシャリスト	プラットフォーム
	ネットワーク
	データベース
	アプリケーション共通基盤
	システム管理
	セキュリティ
アプリケーションスペシャリスト	業務システム
	業務パッケージ

ソフトウェア開発	基本ソフト
	ミドルソフト
	応用ソフト
カスタマーサービス	ハードウェア
	ソフトウェア
	ファシリティマネジメント
IT サービス管理	運用管理
	システム管理
	オペレーション
	サービスデスク
エデュケーション	研修企画
	インストラクション

(出典) IPA「ITスキル標準V3 2011 2部：キャリア編」をもとに作成

各職種の概要

職種	概要
マーケティング	顧客ニーズに対応するために、企業、事業、製品およびサービスの市場の動向を予測かつ分析し、事業戦略、販売戦略、実行計画、資金計画および販売チャネル戦略などビジネス戦略の企画および立案を実施する。市場分析などを通じて立案したビジネス戦略の投資効果、新規性、顧客満足度に責任を持つ。
セールス	顧客における経営方針を確認し、その実現のための課題解決策の提案、ビジネスプロセス改善支援およびソリューション、製品、サービスの提案を実施し成約する。顧客との良好なリレーションを確立し顧客満足度を高める。
コンサルタント	知的資産、コンサルティングメソドロジーを活用し、顧客の経営戦略やビジネス戦略および IT 戦略策定へのコンサルティング、提言、助言の実施を通じて、顧客のビジネス戦略やビジョンの実現、課題解決に貢献し、IT 投資の経営判断を支援する。提言がもたらす価値や効果、顧客満足度、実現可能性などに責任を持つ。
IT アーキテクト	ビジネスおよび IT 上の課題を分析し、ソリューションを構成する情報システム化要件として再構成する。ハードウ

	エア、ソフトウェア関連技術（アプリケーション関連技術、メソドロジ）を活用し、顧客のビジネス戦略を実現するために情報システム全体の品質（整合性、一貫性など）を保ったITアーキテクチャを設計する。設計したアーキテクチャが課題に対するソリューションを構成することを確認するとともに、後続の開発、導入が可能であることを確認する。また、ソリューションを構成するために情報システムが満たすべき基準を明らかにする。さらに実現性に対する技術リスクについて事前に影響を評価する。
プロジェクトマネジメント	プロジェクトマネジメント関連技術、ビジネスマネジメント技術を活用し、プロジェクトの提案、立上げ、計画、実行、監視コントロール、終結を実施し、計画された納入物、サービスと、その要求品質、コスト、納期に責任を持つ。
ITスペシャリスト	ハードウェア、ソフトウェア関連の専門技術を活用し、顧客の環境に最適なシステム基盤の設計、構築、導入を実施する。構築したシステム基盤の非機能要件（性能、回復性、可用性など）に責任を持つ。
アプリケーションスペシャリスト	業種固有業務や汎用業務において、アプリケーション開発やパッケージ導入に関する専門技術を活用し、業務上の課題解決に関わるアプリケーションの設計、開発、構築、導入、テストおよび保守を実施する。構築したアプリケーションの品質（機能性、回復性、利便性など）に責任を持つ。
ソフトウェアデベロップメント	ソフトウェアエンジニアリング技術を活用し、マーケティング戦略に基づく、市場に受け入れられるソフトウェア製品の企画、仕様決定、設計、開発を実施する。また上位レベルにおいては、ソフトウェア製品に関連したビジネス戦略の立案やコンサルテーションを実施する。開発したソフトウェア製品の機能性、信頼性などに責任を持つ。
カスタマーサービス	ハードウェア、ソフトウェアに関連する専門技術を活用し、顧客の環境に最適なシステム基盤に合致したハードウェア、ソフトウェアの導入、カスタマイズ、保守（遠隔保守含む）、修理を実施するとともに、顧客のシステム基盤

	管理およびサポートを実施する。また IT 施設インフラの設計、構築、導入および管理、運営を実施する。導入したハードウェア、ソフトウェアの品質（使用性、保守容易性など）に責任を持つ。
IT サービスマネジメント	システム運用関連技術を活用し、サービスレベルの設計を行い顧客と合意されたサービスレベルアグリーメント（SLA）に基づき、システム運用リスク管理の側面からシステム全体の安定稼動に責任を持つ。システム全体の安定稼動を目指し、安全性、信頼性、効率性を追及する。またサービスレベルの維持、向上を図るためにシステム稼動情報の収集と分析を実施し、システム基盤管理も含めた運用管理を行う。
エデュケーション	担当分野の専門技術と研修に関連する専門技術を活用し、ユーザーのスキル開発要件に合致した研修カリキュラムや研修コースのニーズの分析、設計、開発、運営、評価を実施する。
共通（レベル 1、2）	担当業務の技術領域に関する基本知識を活用し、上位者の指示の下、あるいは既存の作業標準やガイダンスにしたがい、要求された作業を実施する。自らの担当作業に対する実施責任を持つ。

(出典) IPA「IT スキル標準 V 3 2011 2 部：キャリア編」をもとに作成

達成度指標

達成度指標は、実務能力のレベル評価指標として定義したものです。IT スキル標準では、IT 人材のレベル評価は、経験と実績に基づく「達成度指標」によって行います。達成度指標は、ビジネスを成功させる人材を評価する 2 つの貢献に焦点を当てています。「ビジネス貢献」とは、プロジェクトの成功の経験と実績など、ビジネス成果に対する貢献を示します。「プロフェッショナル貢献」とは、専門技術の向上による社内外への貢献、さらに後進育成や技術の継承といったプロフェッショナルとしての貢献を示します。

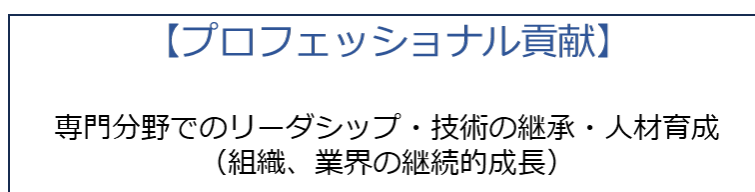
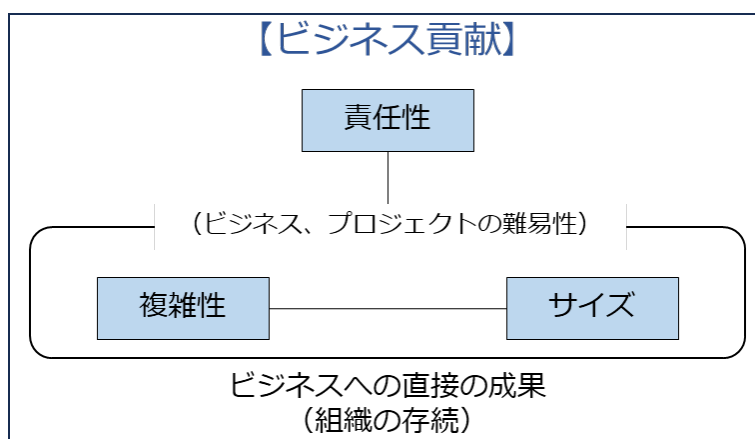


図 93. 達成度指標の構造
(出典) IPA「ITスキル標準 V 3 2011 2部：キャリア編」をもとに作成

レベル\要素	ビジネス貢献		プロフェッショナル貢献			
	責任性	実績回数	専門性の発揮度	技術の継承実績		後進育成
7	チームの責任者として 他をリード	3 回以上	専門領域に関して他を指導できる 高度な専門性保有し、業界を リードしている	5 項以上	☐ 学会、委員会など プロフェッショナル コミュニティ活動 ☐ 著書 ☐ 社外論文掲載 ☐ 社内論文掲載 ☐ 社外講師 ☐ 社内講師 ☐ 特許出願	必須
6		3 回以上	専門領域に関して他を指導できる 高度な専門性保有し、業界に 貢献している	4 項以上		
5		3 回以上	専門領域に関して他を指導できる 高度な専門性保有し、社内に 貢献している	3 項以上		
4		チームのリーダー	2 回以上	専門領域に関して高度の専門性 保有し、後進を指導している		
3	メンバー	1 回以上	専門領域に関して専門性を保有 し、独力で実践している	-		-
2			専門性を踏まえて活動を実施			
1						

(出典) IPA「ITスキル標準 V 3 2011 2部：キャリア編」をもとに作成

IT スキル標準では、ビジネス貢献とプロフェッショナル貢献の両方が重視されています。IT 人材は、ビジネス貢献、およびプロフェッショナル貢献という達成度指標で定められた基準を同時に満たしていることが必要です。

詳細理解のため参考となる文献（参考文献）	
IT スキル標準 V3 2011 2部：キャリア編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf

22-2-3. スキル

「3部：スキル編」では、IT スキル標準で定義されているすべてのスキル項目、知識項目を網羅した「スキルディクショナリ」、職種ごとにスキル項目、知識項目を整理した「スキル領域」と「スキル熟達度」、および IT スキル標準に対応して習得すべき研修科目を職種ごとに明示した「研修ロードマップ」を収めています。スキル編は、達成度指標に示す経験と実績を遂行するために必要な能力を整理したものであり、教育や訓練の設計を行う際の指標として活用するものです。

以下の表は、各職種に求められるスキルの中からセキュリティに関連するスキルを抜き出したものです。

各職種に求められるセキュリティに関するスキル	
全職種共通	● プロジェクト・リスク・マネジメント
マーケティング	● 関連法規に関する知識
セールス	● 最新技術動向
コンサルタント	● ビジネスモデルのリスクコントロールの評価 ● 最新ソリューションの動向 ● 情報技術動向の調査
IT アーキテクト	● 関連技術（IT）動向の把握 ● 統合要件の定義 ● インフラストラクチャ要件（主に非機能要件）の定義 ● インフラストラクチャアーキテクチャ設計
プロジェクトマネジメン ト	● ソフトウェアエンジニアリング ● 最新技術動向 ● セキュリティシステムの実装・検査 ● ネットワーク技術の理解と応用 ● ネットワークシステムの運用、保守、管理 ● リスク・マネジメント計画 ● リスク識別

	● 定性的リスク分析 ● 定量的リスク分析 ● リスク対応計画 ● リスクの監視コントロール
IT スペシャリスト	● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● セキュリティと個人情報 ● IT 基盤構築プロセス ● システム非機能要件基礎 ● コンプライアンスと法規 ● プラットフォーム要件定義手法 ● プラットフォーム設計手法 ● ネットワークシステムの運用・保守・管理 ● 物理データベースの設計技術 ● データベース関連製品の利用技術 ● データベース開発における重要技術 ● アプリケーション共通基盤要件定義手法 ● アプリケーション共通基盤設計手法 ● セキュリティ方針の策定 ● セキュリティ対策基準の策定 ● セキュリティシステムの計画策定 ● セキュリティシステムの要件定義 ● セキュリティシステムの設計 ● セキュリティシステムの実装・検査 ● セキュリティシステム導入支援 ● セキュリティシステムの運用管理 ● セキュリティ障害（事件事故／インシデント）管理 ● セキュリティの分析 ● セキュリティの見直し（セキュリティシステムの評価と改善） ● 情報セキュリティ監査の実施・支援 ● セキュリティシステムの実装・検査 ● 業界固有のセキュリティ要件・事例 ● コンサルティングの実施 ● セキュリティ技術動向

	● セキュリティと個人情報 ● コンピュータ・フォレンジック（証拠保全追跡）
アプリケーションスペシャリスト	● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● システム管理手法 ● データベース開発における重要技術 ● アプリケーションセキュリティ ● セキュリティ技術の理解と応用 ● セキュリティ技術動向 ● セキュリティシステムの実装、検査 ● セキュリティとプライバシー
ソフトウェアデベロップメント	● セキュリティシステムの実践、検査 ● セキュリティとプライバシー ● 最新技術動向 ● ネットワーク技術の理解と応用 ● インターネット技術 ● アプリケーションセキュリティ ● 適合すべき標準の選定 ● リスク管理基礎
カスタマーサービス	● 最新技術動向 ● インターネット技術 ● セキュリティとプライバシー ● ネットワーク技術の理解と応用 ● 関連国際標準および関連規格 ● お客様サポート ● 改善提案 ● ストレージ技術 ● データベース技術 ● セキュリティ技術 ● メンテナンスの準備 ● セキュリティ管理
IT サービスマネジメント	● 基準と標準 ● 人材育成

	● 資産管理 ● セキュリティとプライバシー ● システム運用管理手法 ● リスク管理 ● セキュリティ管理 ● インシデント管理 ● 問題管理 ● 変更管理 ● リリース情報 ● 構成管理 ● ネットワークシステム管理 ● セキュリティ技術 ● 最新セキュリティ情報の収集
エデュケーション	● 最新技術動向

(出典) IPA「IT スキル標準 V3 2011 スキルディクショナリ_20120326」をもとに作成

詳細理解のため参考となる文献（参考文献）	
IT スキル標準 V 3 2011 3部：スキル編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024844.pdf
IT スキル標準 V3 2011 スキルディクショナリ_20120326	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf

22-3. ITSS+（プラス）

ITSS+は、従来のITスキル標準（ITSS）を拡張し、第4次産業革命に向けて求められる新たな領域の新しいスキルをカバーするために策定されました。対象となっている領域は、「[データサイエンス領域](#)」「[アジャイル領域](#)」「[IoTソリューション領域](#)」「[セキュリティ領域](#)」の4つの領域です。

詳細理解のため参考となる文献（参考文献）	
ITSS+（プラス）概要	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

22-3-1. データサイエンス領域

ITSS+（プラス）の「[データサイエンス領域](#)」は、企業などの業務において大量データを分析し、その分析結果を活用するための一連のタスクとそのために習得しておくべきスキルを取りまとめたものです。

タスクは、IPAと「一般社団法人データサイエンティスト協会」スキル定義委員会が協力して策定、見直しを行っています。

スキルは同協会が公開している「スキルチェックリスト」を活用しています。

スキルカテゴリー一覧

スキルカテゴリー一覧			
データサイエンス力	基礎数学	データエンジニアリング力	環境構築
	データの理解・検証		データ収集
	意味合いの抽出・洞察		データ構造
	予測		データ蓄積
	推定・検定		データ加工
	グルーピング		データ共有
	性質・関係性の把握		プログラミング
	サンプリング		ITセキュリティ
	データ加工		AIシステム運用
	データ可視化	ビジネス力	行動規範
	時系列分析		契約・権利保護
	学習		論理的思考
	自然言語処理		着想・デザイン
	画像・映像認識		課題の定義
	音声認識		アプローチ設計

	パターン発見		データ理解
	シミュレーション・データ同化		分析評価
	最適化		事業への実装
			PJ マネジメント
			組織マネジメント

(出典) IPA「データサイエンティスト スキルチェックリスト Ver5.00」をもとに作成

データサイエンティストに必要とされるセキュリティに関するスキル（抜粋）

分野	スキルカテゴリ	サブカテゴリ	内容
ビジネスカ	行動規範	コンプライアンス	個人情報の扱いに関する法令、そのほかのプライバシーの問題、依頼元との契約約款に基づき、明示されていない項目についても仮名化/匿名化すべきデータを選別できる（名寄せにより個人を特定できるもの、依頼元がデータ処理の結果をどのように保持し利用するのかなどの考慮）
	着想・デザイン	デザイン	プライバシー・バイ・デザインやデータガバナンスの考え方を理解した上で、UI 専門家などと協議し、同意取得やプライバシーに配慮したデータ取得設計ができる
	アプローチ設計	アプローチ設計	データの機密度を考慮した上で、内外の AI サービスに対する活用可否を判断し、入出力データの配置先（クラウドストレージへの配置可否や、社内オンプレ環境におけるセキュリティレベルなど）を設計できる
データエンジニアリングカ	IT セキュリティ	基礎知識	セキュリティの 3 要素（ <u>機密性</u> 、 <u>完全性</u> 、 <u>可用性</u> ）について具体的な事例を用いて説明できる
		プライバシー	ハッシュ化、マスキング、k-匿名化、差分プライバシーなどのプライバシー保護の仕組みを理解し適用できる
		攻撃と防御手法	<u>マルウェア</u> などによる深刻なリスクの種類（消失・漏えい・サービスの停止など）を理解している
			OS、ネットワーク、アプリケーション、データなどの各レイヤーに対して、ユーザーごとのアクセスレベルを設定する必要性を理解している
			DoS 攻撃、 <u>不正アクセス</u> 、マルウェア感染や内部不正などの <u>セキュリティインシデント</u> が発覚した場合に既存のルールに

			基づき対応できる
			OS、ネットワーク、アプリケーション、データに対するユーザーごとのアクセスレベルを設計できる
			SQL インジェクションやバッファオーバーフロー攻撃の概要を理解し、防止する対策を判断できる
			なりすまし、 改ざん 、盗聴などのセキュリティ侵害を防御するための対策と セキュリティポリシー を設計し実践できる
			侵入検知システム (IDS) や ファイアウォール 、エンドポイント対策 (EPP/ EDR) などを用いて、外部からの不正アクセスを検知、防御、内部侵入後の対策を行う環境を設計できる
			不正メールの検出、不正通信 トラフィック の自動遮断、ログからの不正検知など AI を活用した サイバー攻撃 などに対する防御 ソリューション の有用性と誤検出などのリスクを評価し導入を判断できる
		暗号化技術	暗号化されていないデータは、不正取得された際に容易に不正利用されるおそれがあることを理解し、データの機密度合いに応じてソフトウェアを使用した暗号化と復号ができる
			なりすましや改ざんされた文書でないことを証明するために、電子署名が用いられることを理解している
			公開鍵暗号化方式において、受信者の公開鍵で暗号化されたデータを復号化するためには受信者の秘密鍵が必要であることを知っている
			ハッシュ関数を用いて、データの改ざんを検出できる
			SSH や SSL/TLS などのセキュアプロトコルの概要と必要性を説明できる
		認証	OAuth に対応したデータ提供サービスに対して、認可サーバから取得したアクセストークンを付与してデータ取得用の REST API を呼び出すことができる
			Kerberos 認証と Radius 認証の違いを理解し、それぞれの認証の特徴やユースケースを説明できる
			SAML や OpenID Connect を用いて一度のログインで複数の Web アプリケーションのログイン認証を連携するシングルサインオンの仕組みを設計できる
		ブロックチェ	ブロックチェーン 技術を用いてストレージに蓄積されたデー

		ーン	タの安全性と品質を保証するシステムを設計できる
		<u>ゼロトラスト</u>	ゼロトラストの概念を理解し、クラウド利用やリモートワークに対応した情報セキュリティの担保と、データ活用の利便性を両立させる環境をサービスを利用して実装できる

(出典) IPA「データサイエンティスト スキルチェックリスト Ver5.00」をもとに作成

詳細理解のため参考となる文献（参考文献）	
データサイエンティスト スキルチェックリスト Ver5.00	https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx
データサイエンティストのためのスキルチェックリスト／タスクリスト概説	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001ity-att/000083733.pdf

22-3-2. アジャイル領域

ITSS+（プラス）の「アジャイル領域」は、アジャイル開発手法に関するスキルを強化するために設けられた領域です。アジャイル開発は、ソフトウェア開発において変化する要件に柔軟に対応し、顧客満足度の高いサービスを迅速かつ継続的に提供する手法の一つです。重要なのは、関係者全員が自律的に考え、ユーザー価値とビジネス価値の最大化を目指して改善を続けることです。スクラム、XP などさまざまな方法論がありますが、重要なのは仮説検証を繰り返し、失敗から学ぶ姿勢にあります。

「アジャイル領域へのスキル変革の指針」は、アジャイル開発の経験が浅い人や非開発者向けに、アジャイルの背景や必要な学びを説明しています。アジャイル開発の成功には、経営層や事業部門の協力が不可欠です。経営層や事業部門もアジャイルの考え方を理解し、開発に深く関わることが重要です。アジャイル開発に関しては IPA からさまざまなドキュメントを公開されていますが、スキル強化のためには、「アジャイル領域」へのスキル変革の指針として公開されている以下の資料が参考になります。

各資料の概要と想定する読者

①「なぜ、いまアジャイルが必要か？」

-概要： [Society5.0](#) 時代になぜアジャイルが必要かを理解します。

Society5.0 時代に直面する問題と従来の問題との違いを踏まえ、いまの時代の問題の解法としてアジャイルが適していることを説明しています。

②「アジャイルソフトウェア開発宣言の読みとき方」

-概要： アジャイル開発のベースにあるマインドセットや原則について理解します。

「アジャイルソフトウェア開発宣言」にある「4 つの価値」と「12 の原則」について検討メンバーの解釈を説明しています。

③「ビジョンとプロダクトの橋渡し」

-概要：いまの時代にプロダクトを価値として届けるために「プロダクト」の責任者に求められる役割を理解します。プロダクト責任者の必要性、役割、振る舞い方について説明しています。

④「アジャイル開発の進め方」

-概要：アジャイル開発のプロセスと開発者の役割について理解します。アジャイル開発プロセスの特徴やチームの特徴、および開発者の学ぶべきスキルについて説明しています。

⑤「アジャイルのさらなる広がり」

-概要：アジャイルの広がりを経営での事例、現場で取組方について説明しています。

◎：主体、○：共同、△：参考

資料	概要	想定読者			
		経営層	事業部門	開発部門／チーム	情報システム部門
①	なぜ、いまアジャイルが必要か？	◎	◎	◎	◎
②	アジャイルソフトウェア開発宣言の読みとき方	○	◎	◎	◎
③	ビジョンとプロダクトの橋渡し	○	◎	○	○
④	アジャイル開発の進め方	△	○	◎	◎
⑤	アジャイルのさらなる広がり	◎	○	○	○

(出典) IPA「アジャイル領域へのスキル変革の指針」をもとに作成

詳細理解のため参考となる文献（参考文献）	
アジャイル領域へのスキル変革の指針	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065571.pdf

22-3-3. IoT ソリューション領域

ITSS+（プラス）の「IoT ソリューション領域」は、IoT 技術の設計、実装、管理に必要なスキルを強化するために設けられた領域です。これは、特に第 4 次産業革命に対応するために必要なスキルセットを提供することを目的としています。主に IT ベンダーとして必要な技術要素や、開発

プロセスなどに焦点を当て、IoT ソリューション開発でのロール（役割）定義や、各ロールにおけるタスクの特徴などについて解説されています。

対象

IoT ソリューション領域へのスキル変革の指針は、以下のような対象者が何を学ぶべきかの羅針盤や、IoT ソリューション領域の特徴の理解などに利用することを想定しています。

- 既存の IT システム開発に携わっているが、これから IoT ソリューション開発に取り組もうとするエンジニア
- すでに IoT ソリューション開発を実施しており、今後のキャリアや強みとする分野を考えようとしているエンジニアなど

(出典) IPA「IoT ソリューション領域へのスキル変革の指針 2021 改訂版」をもとに作成

ドキュメント構成

IoT ソリューション領域のドキュメントは、「①IoT ソリューション領域へのスキル変革の指針」、「②タスクリスト」、「③参考文献」の3部構成になっています。

① IoT ソリューション領域へのスキル変革の指針：

IoT ソリューション領域にこれから取り組もうとする方やスキルチェンジをしようとする技術者などに対して、当該領域の特徴や、活躍するロール（役割）、必要なタスクの概要などを説明しています。

② タスクリスト：

IoT ソリューション領域の仕事を行う上で具体的な業務をタスクとして定義し、大分類・中分類・小分類の階層に分解して示したものです。また、それぞれについてロール（役割）が主に担うタスクについても示しています。

③ 参考文献：

IoT ソリューション領域の仕事を行う上で参考となる書籍や公表資料などを示したものです。

(出典) IPA「IoT ソリューション領域へのスキル変革の指針 2021 改訂版」をもとに作成

詳細理解のため参考となる文献（参考文献）

IoT ソリューション領域へのスキル変革の指針 2021 改訂版

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/000065568.pdf>

22-3-4. セキュリティ領域

ITSS+（プラス）の「セキュリティ領域」は、企業のセキュリティ対策に必要なスキルと知識を体系化し、評価するための枠組みです。この領域は、特にサイバーセキュリティの脅威に対応するために設計されています。「セキュリティ領域」では、企業のセキュリティ対策に必要なとなるセキ

セキュリティ関連業務のまとまりを 17 分野に整理しています。それぞれの分野に求められるセキュリティ知識、スキルの概要を理解することで、セキュリティ体制の構築時と人材育成・配置などに活用することができます。また、セキュリティ専門人材のみならず、セキュリティ以外の業務を生業としている人材の「学び直し」の指針として用い「プラス・セキュリティ人材」を育成できます。（セキュリティを専門としない事業部門、管理部門などの人材で、セキュリティ領域の知識・スキルを身につけた人材を、「プラス・セキュリティ人材」と呼んでいます）。

次の図は、セキュリティ関連タスクを担う分野の概観図です。

ユーザー企業 における 組織の例		サイバーセキュリティ 関連タスクの例	タスクに対応するサイバーセキュリティ関連分野			
			サイバーセキュリティ対策に 関するタスクの割合が高いもの	サイバーセキュリティ以外の タスクが占める割合が高いもの		
経営層	取締役会 執行役員会議	・サイバーセキュリティ意識啓発 ・対策方針指示 ・ポリシー/予算/実施 事項承認	セキュリティ経営 (CISCO)	デジタル経営 (CIO/CDO)	企業経営 (取締役)	
	内部監査部門 (外部監査含む)	・システム監査 ・セキュリティ監査	セキュリティ監査	システム監査		
戦略マネ ジメント層	管理部門 (総務、法務、 広報、調達、 人事 等)	・BCP対応 ・官公庁、法令等遵守対応 ・記者/広報対応 ・調達/契約/検収 ・施設管理/物理セキュリティ ・内部犯行対策		法務		
	セキュリティ 統括室	・リスクアセスメント ・ポリシー・ガイドライン策定・管理 ・サイバーセキュリティ教育 ・社内相談対応 ・インシデントハンドリング	セキュリティ統括	経営リスク マネジメント		
	経営企画部門 事業部門	・事業戦略立案 ・システム企画 ・要件定義・仕様書作成 ・プロジェクトマネジメント		デジタルシステム ストラテジー	事業ドメイン (戦略・企画・ 調達)	
実務者・技術者層	設計・開発・テスト	デジタル部門 ／事業部門 (専門事業者 への外注含む)	・セキュアシステム要件定義 ・セキュアアーキテクチャ設計 ・セキュアソフトウェア方式設計 ・テスト計画	デジタルシステム アーキテクチャ		
			・基本・詳細設計 ・セキュアプログラミング ・テスト・品質保証 ・パッチ開発 ・脆弱性診断	脆弱性診断・ ペネトレーションテ スト	デジタル プロダクト開発	
			・構成管理、運用設定 ・脆弱性対応 ・セキュリティツールの導入・運用 ・監視・検知・対応 ・インシデントレスポンス ・ペネトレーションテスト	脆弱性診断・ ペネトレーションテ スト	デジタル プロダクト運用	事業ドメイン (生産現場・ 事業所管理)
			・現場教育・管理 ・設備管理・保全 ・初動対応・原因究明・ フォレンジック ・マルウェア解析 ・脅威・脆弱性情報の収集・ 分析・活用	セキュリティ 調査分析・ 研究開発		
	運用・保守					
	研究開発					

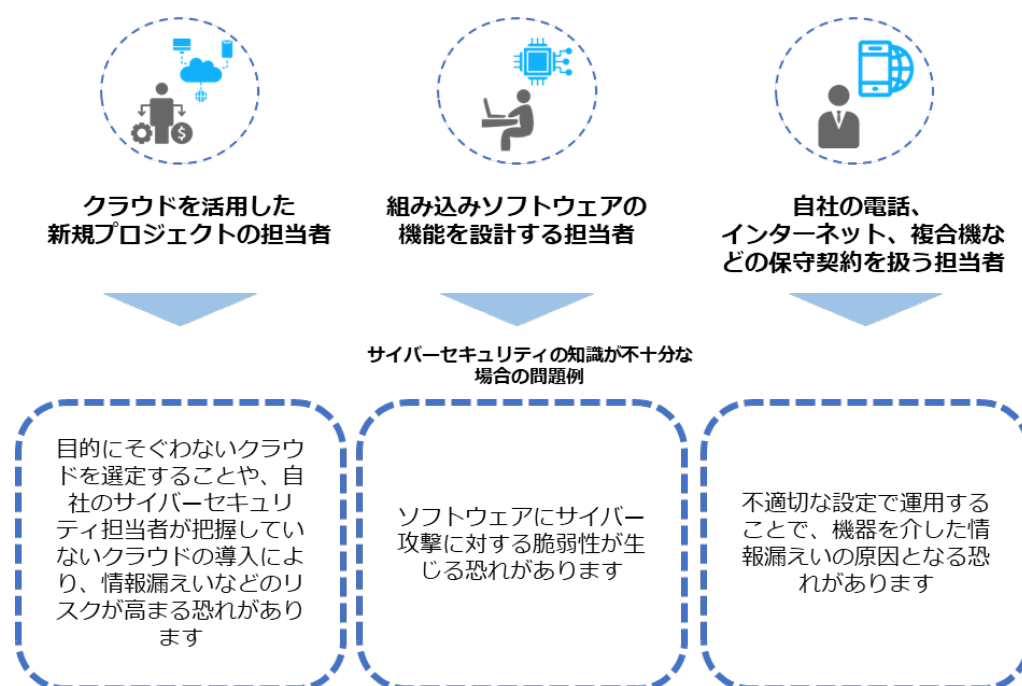
図 94. セキュリティ関連タスクを担う分野の概観図
(出典) IPA「ITSS+（プラス）セキュリティ領域」をもとに作成

プラス・セキュリティ

プラス・セキュリティとは

自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと

企業は、デジタルトランスフォーメーションの推進と並行してサイバーセキュリティへの対策が求められています。この状況の中、経営層をはじめ、法務や広報といった、必ずしも IT やセキュリティに関する専門知識や業務経験を有していない人も「プラス・セキュリティ」知識を習得することが重要です。なぜなら、デジタルトランスフォーメーションが進む中、サイバーセキュリティ担当部署だけでは、サイバーセキュリティ対策への対処が難しい状況になっているためです。そのため、サイバーセキュリティ対策が不十分な場合、インシデントが生じる可能性がある業務を担っている人材には、業務に必要なセキュリティに関する知識・スキルを身につけてもらう必要があります。



プラス・セキュリティ人材の育成

プラス・セキュリティの知識を身につける方法として、主に試験・資格を活用したり、教育プログラムを受けたりする方法があります。ここでは、具体例も含めて紹介します。

試験・資格の活用

各分野の人材がプラス・セキュリティの知識を身につける方法の1つとして、試験や資格の活用が挙げられます。資格を活用することの利点は、特定の役割や業務を担うために必要なスキルを効率よく習得できることです。

(例)

情報セキュリティマネジメント試験

【対象】企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者

【内容】本試験は、情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定するものです。

教育プログラム・コミュニティ活動の活用

[NISC](#)（内閣サイバーセキュリティセンター）は、経営層、管理職、一般従業員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などを紹介しています。

(例)

実践的サイバー防御演習「CYDER」(NICT)

【対象】各組織の情報システム担当者や [CSIRT](#) 要員

【難易度】初学者から準上級者

【内容】実際に[マルウェア](#)感染などの[サイバー攻撃](#)を受けた場合の対処能力の向上を図ることを目的としています。被害の対処をベンダーなど外部委託先に任せている場合であっても、被害発生時に委託先がどのような作業を実施しているかを予め理解・把握しておくことで、円滑なインシデント対応につながります。

実践サイバー演習「RPCI」(NICT)

【対象】経営層、管理職、一般従業員（特に、CISO、CSIRT 管理者、CSIRT メンバー、インシデントが発生した際の対応に携わる方、情報システムの管理・運用・調達・企画・開発に携わる方に向いています）

【難易度】中級～上級

【内容】本番に近いリアルな環境でのインシデント対応を行う演習です。擬似的に発生させたサイバー攻撃にCSIRTとしてチームで対処します。実際の対応に近い体験をすることで、多くの気づきや学びを得ることができます。

そのほかについては、NISCのサイトを参照してください。

詳細理解のため参考となる文献（参考文献）	
実践的サイバー防御演習「CYDER」(NICT)	https://cyder.nict.go.jp
実践サイバー演習「RPCI」(NICT)	https://rpci.nict.go.jp
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/curriculum/

22-4. i コンピテンシ ディクショナリ (iCD)

i コンピテンシ ディクショナリ (iCD) は、組織において IT を利活用するビジネスに求められる業務（タスク）と、それを支える IT 人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものです。具体的には、タスクとスキルをそれぞれ辞書のように参照できる形で構成立ててまとめています。i コンピテンシ ディクショナリを辞書として使用することで、従業員は、自身の業務に必要なスキルを把握できます。組織は目的に応じた人材育成や業務改善・効率化に活かすことができます。

i コンピテンシ ディクショナリ (iCD) に関する重要なポイント

i コンピテンシ ディクショナリ (iCD) において、重要なことは考え方です。タスクやスキルについては、デジタルスキル標準を参照することが大切です。

i コンピテンシ ディクショナリ (iCD) は、網羅的なタスク、スキル、知識の「辞書」として今後も有用ではありますが、デジタルスキル標準 (DSS) と重複する部分が多く、デジタルスキル標準 (DSS) の方が最新情報であるためです。

22-4-1. i コンピテンシ ディクショナリ (iCD) の考え方

i コンピテンシ ディクショナリは、企業、組織および IT 技術者が、人材育成やスキル向上に関わる施策を効率的に立案・推進し、成果を上げるための道具として有用です。

i コンピテンシ ディクショナリは、「タスクディクショナリ」と「スキルディクショナリ」で構成されています。仕事やスキルを構造的に表現して、必要に応じて取捨選択することで、企業や組織のあるべき姿や人材育成のための施策を、根拠を持って効率的に推進できます。

業務遂行における各ディクショナリの働きと関係は以下の通りです。

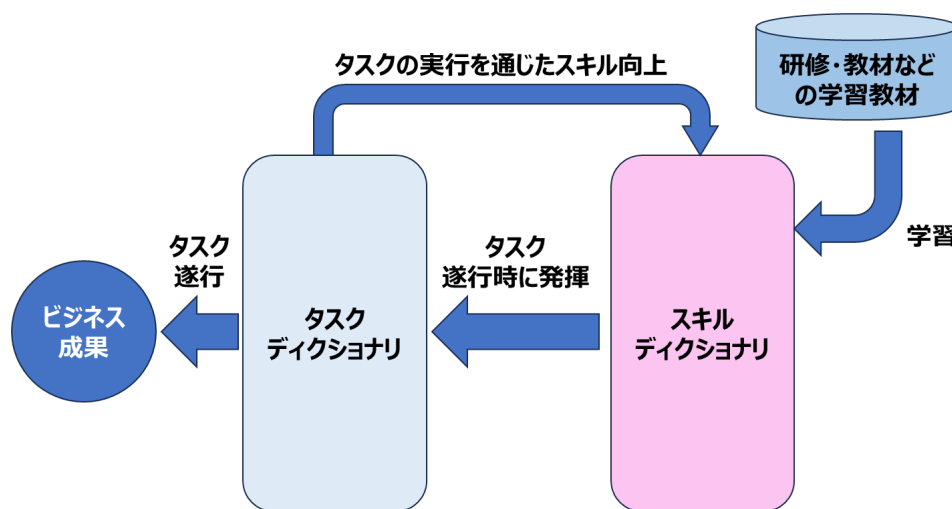


図 95. 業務遂行とディクショナリの働きの関係

(出典) IPA 「i コンピテンシ ディクショナリ解説書」をもとに作成

「タスクディクショナリ」の考え方

タスクディクショナリの広範囲で網羅的なタスク群を参照し、自社・自組織のビジネスモデル、経営戦略や事業計画、および現状の業務に基づいて取捨選択することで、あるべき自社・自組織のタスクを定められます。

タスクを定めることにより、どのような能力を持つ人材がどのくらい必要かを明らかにでき、現状とのギャップも明確となり、効果的な人材育成施策を立案・実施することができます。また、組織の最適化や人員の最適配置など、人材育成に留まらない活用が可能です。

タスクディクショナリには、「タスクディクショナリ構成図」、「タスクプロフィール」が含まれており、自タスクを策定する際の参考情報として利用することを想定しています。

タスクディクショナリを構成する各コンテンツの関係は以下の通りです。

タスクディクショナリの全体像



タスク一覧

タスク大分類 コード	タスク 大分類	タスク中分類 コード	タスク 中分類	タスク小分類 コード	タスク 小分類	評価項目コード	評価項目
ST01	事業戦略 策定	ST01.1	事業環境 の分析	経営方針 の確立	ST01.1.1.1	ST01.1.1.1	自社の基本理念・ビジョン・方針を理解する
					ST01.1.1.2	ST01.1.1.2	新たな事業計画を立案するにあたり、経営方針や経営陣の思いを確認、共有する
					ST01.1.1.3	ST01.1.1.3	事業で達成すべき目標を定めるために、企業目標を把握する
				外部環境 の分析	ST01.1.2.1	ST01.1.2.1	マクロ環境（自社を取り巻く産業や業界）の変化の要因を調査、把握する
					ST01.1.2.2	ST01.1.2.2	自社が所属する業界や自社製品・サービスの市場環境および今後の見通しを調査、把握する
					ST01.1.2.3	ST01.1.2.3	競合他社の市場シェア、収益性、動向を調査、把握する
				内部環境 の分析	ST01.1.3.1	ST01.1.3.1	自社の組織体制、現状人員数、配置状況を把握する
					ST01.1.3.2	ST01.1.3.2	自社の収益性、安全性、生産性等の財務状況を把握する
					ST01.1.3.3	ST01.1.3.3	自社の製品やサービスの売上高、利益率、ライフサイクル上のポジションを把握する
					ST01.1.3.4	ST01.1.3.4	調達、生産、物流、サービス等の自社業務の一連の流れを把握する
					ST01.1.3.5	ST01.1.3.5	事業管理のために必要な情報が自社内のどこに、誰によって、どのように管理されているか把握する

各タスクの属性情報（特性、特徴）



タスクディクショナリ構成図



※タスクディクショナリの把握と保守（タスク追加・更新時の整理）のためのコンテンツ

タスクプロフィール

タスクプロフィール 種別	タスクプロフィール 種別の説明	タスクプロフィール グループ	タスクプロフィールコード	タスクプロフィール	タスクプロフィールの説明
ビジネスタイプ別	組織の立場（ユーザー、ベンダー）や業種によって必要なタスクを識別するもの。	-	A-010-010	自社向け情報システム開発・保守・運用	自社向けシステムの開発・保守・運用を担う部門（IT/非IT企業の情報システム部門）に関連するタスク
			A-010-020	システム受託開発	アプリケーションシステムおよび基幹システムの受託開発を担う企業に関連するタスク
			A-010-030	ソフトウェア製品開発	ソフトウェア製品の企画・開発・販売を担う企業に関連するタスク
			A-010-040	組み込みソフトウェア開発	組み込みソフトウェアの開発を担う企業に関連するタスク
			A-010-050	Webサイト構築・運用	顧客のWebサイトの構築および運用を担う企業に関連するタスク
			A-010-060	システム運用サービス（運用業務受託）	顧客のシステム運用業務を受託して実施する企業に関連するタスク
			A-010-070	システム運用サービス（データセンタ運営）	自社のデータセンタ施設を持ち、顧客のシステム運用業務を受託して実施する企業に関連するタスク
			A-010-080	ITコンサルティング	ITコンサルティング（戦略、企画）を担う企業に関連するタスク

※タスクディクショナリの把握と活用（タスクの選択、役割の定義など）のためのコンテンツ

図 96. タスクディクショナリの構成

(出典) IPA 「i コンピテンシディクショナリ解説書」をもとに作成

「スキルディクショナリ」の考え方

スキルディクショナリは、IT 技術者個人が、スキルディクショナリからスキル項目を選択して、現状把握やスキル向上目標を設定するために利用できます。

タスクディクショナリとの関係情報を利用して、そのスキルが、どのタスクの遂行に有効なのかを判断する使い方もできます。

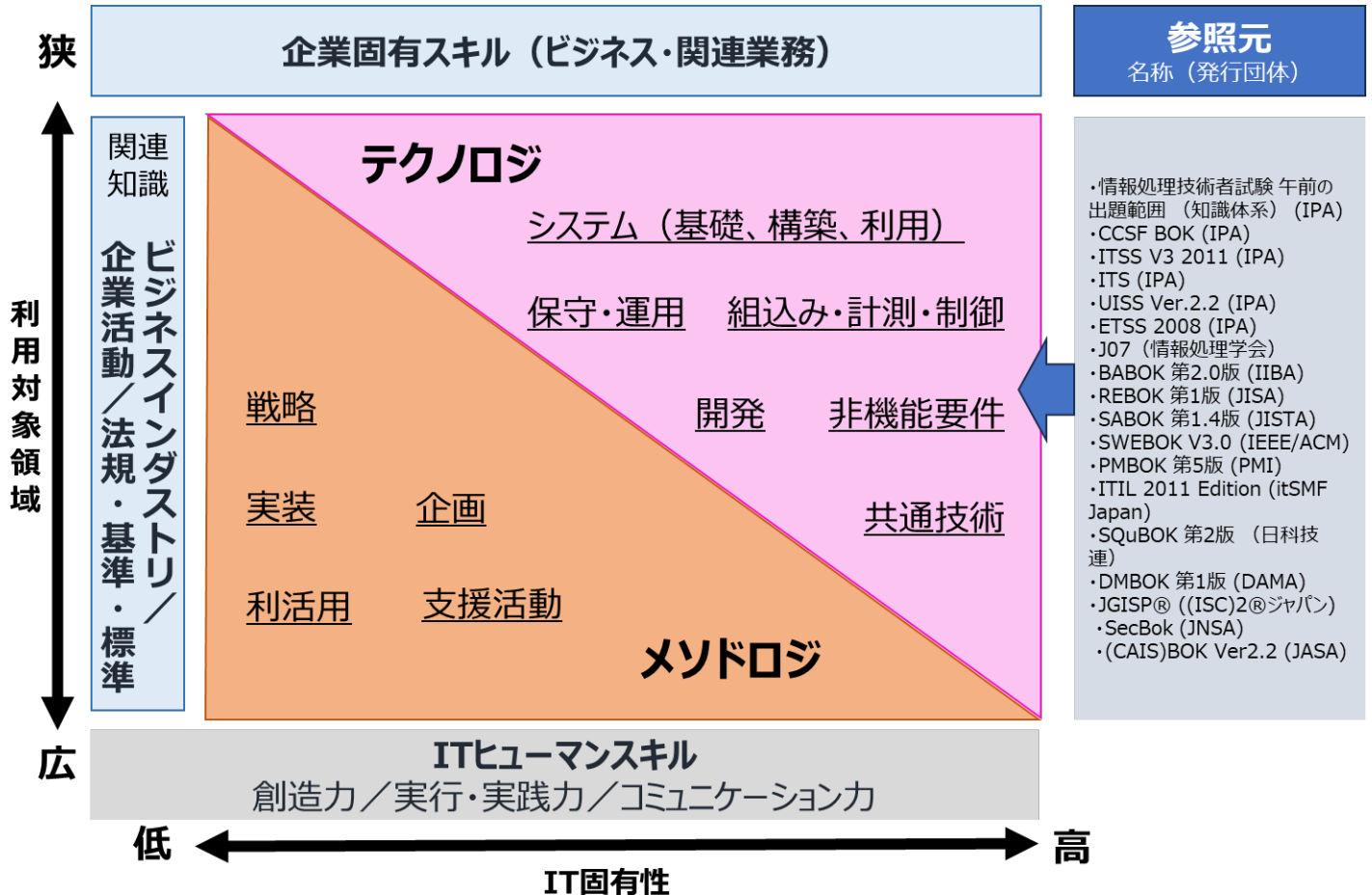


図 97. スキルディクショナリの構成
(出典) IPA 「i コンピテンシディクショナリ解説書」をもとに作成

各項目の詳細は以下の通りです。

システム（基礎、構築、利用）

- ソフトウェア技術
- データベース技術
- ハードウェア技術
- Web システム技術
- プラットフォーム技術
- ネットワーク技術

保守・運用

- IT サービスマネジメント業務管理技術
- IT サービスオペレーション技術
- システム保守・運用・評価
- 障害修理技術
- 施工実務技術
- ファシリティ設計技術
- サポートセンター基盤技術

組込み・計測・制御

- 組込み技術（基礎、構築、利用）
- デジタル技術
- ヒューマンインターフェース技術
- マルチメディア技術
- グラフィック技術
- 計測・制御技術

開発

- システムアーキテクティング技術
- システム開発管理技術

非機能要件

- 非機能要件（可用性、性能・拡張性）
- セキュリティ技術（基礎、構築、利用）

共通技術

- IT 基礎
- ナレッジマネジメント技術

戦略

- 市場機会の評価と選定
- マーケティング
- 製品・サービス戦略
- 販売戦略
- 製品・サービス開発戦略
- システム戦略立案手法
- コンサルティング手法
- 業務動向把握手法

企画

- システム企画立案手法

- セールス事務管理手法
- 要求分析手法
- 非機能要件設計手法

実装

- アーキテクチャ設計手法
- ソフトウェアエンジニアリング手法
- カスタマーサービス手法
- 業務パッケージ活用手法
- データマイニング手法
- 見積り手法
- プロジェクトマネジメント手法

利活用

- サービスマネジメント
- サービスの設計・移行
- サービスマネジメントプロセス
- サービスの運用

支援活動

- 品質マネジメント手法
- リスクマネジメント手法
- IT ガバナンス
- 資産管理手法
- ファシリティマネジメント手法
- 事業継続計画
- システム監査手法
- 標準化・再利用手法
- 人材育成・教育・研修
- 情報セキュリティ

(出典) IPA 「i コンピテンシディクショナリ解説書」をもとに作成

i コンピテンシ ディクショナリ (iCD) の利活用の形態

i コンピテンシディクショナリは、以下の 3 種類の活用形態を利用対象者別に想定しています。

- 企業・組織での利活用
- 個人での利活用
- 学校等教育機関での利活用

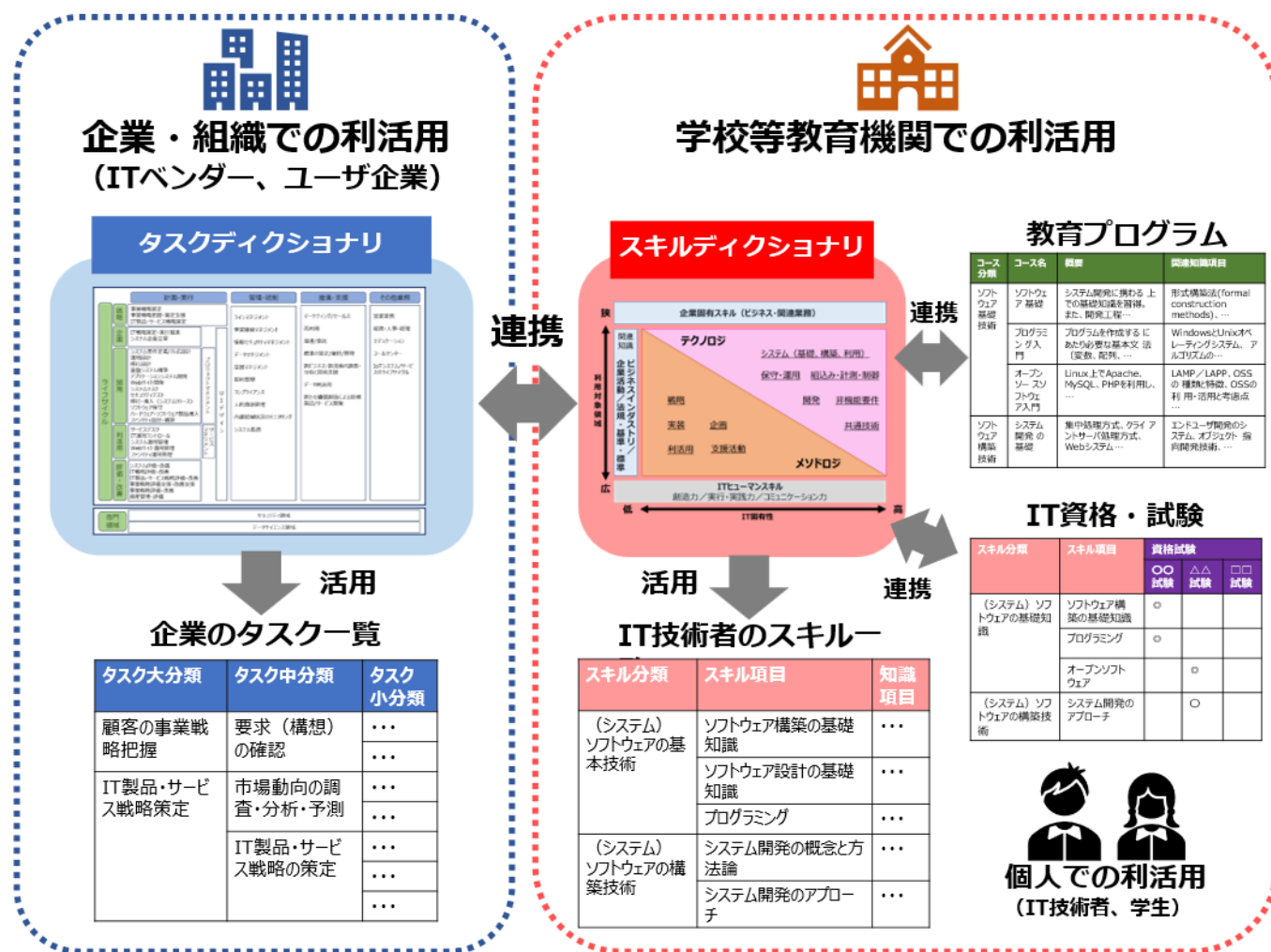


図 98. i コンピテンシ ディクショナリ (iCD) の利活用形態
(出典) IPA「i コンピテンシディクショナリ解説書」をもとに作成

第23章. 人材の知識とスキルの認定制度

章の目的

第 23 章では、IT およびデジタル人材のスキル、知識の認定制度と活用方法を理解することを目的とします。認定制度は、従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段となります。

主な達成目標

- スキルや知識の認定制度と活用方法を理解すること

23-1. Di-Lite

「Di-Lite」とは、デジタルリテラシー協議会が定義する、すべてのビジネスパーソンが持つべきデジタル時代の共通リテラシーのことです。具体的には、以下の3つの領域に関するスキルや知識を指します。

- ① IT・ソフトウェア領域：基本的なITスキルやソフトウェアの使用方法
- ② 数理・データサイエンス領域：データ分析や統計の基礎知識
- ③ 人工知能（AI）・ディープラーニング領域：AI技術やディープラーニングの基礎知識

これらのスキルを身につけることで、デジタル時代におけるビジネスの効率化や競争力の向上が期待されています。学習すべき範囲は、「ITパスポート試験」「G検定」「データサイエンティスト検定」の3つの試験のシラバス範囲になります。

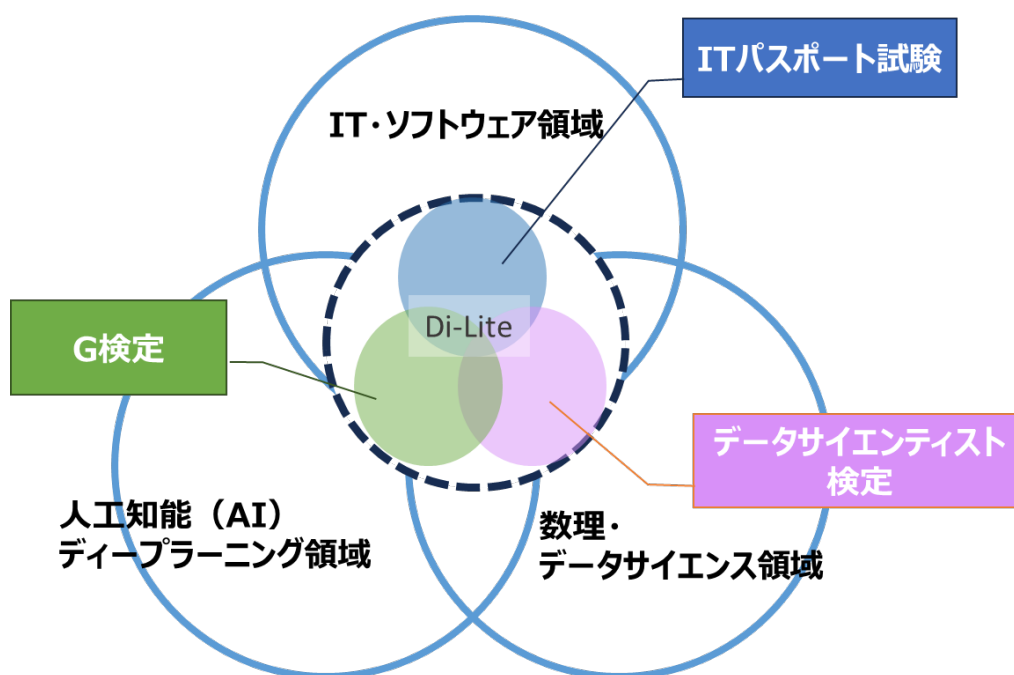
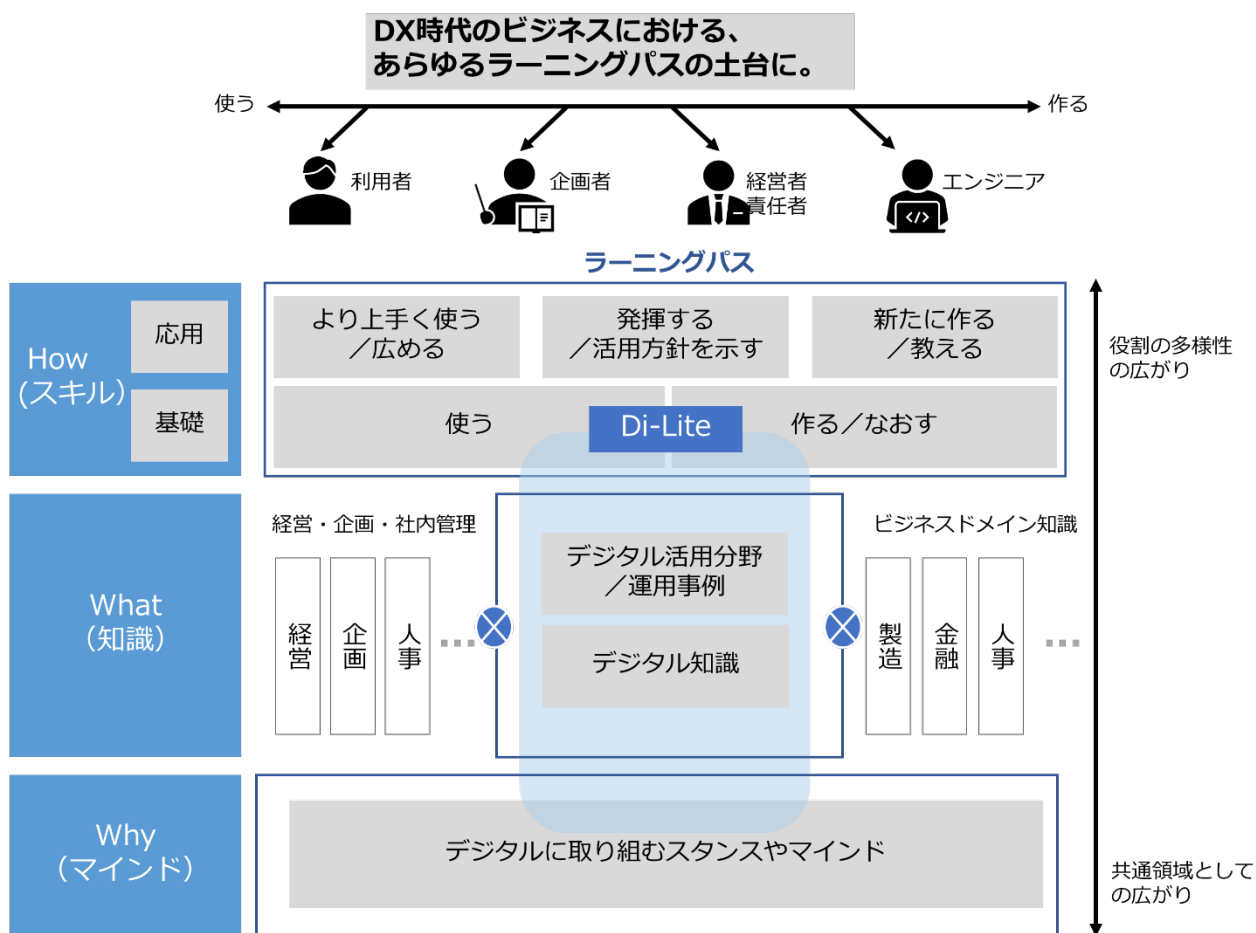


図 99. Di-Lite の 3 つの領域

(出典) デジタルリテラシー協議会「Di-Lite とは」をもとに作成



当協議会が、2021年4月時点で考え方を整理した「デジタルリテラシー・スキルフレームワーク」です。今後協議を進める中で、更新される場合がございます。

図 100. デジタルリテラシー・スキルフレームワーク
(出典) デジタルリテラシー協議会「Di-Lite とは」をもとに作成

DX 推進パスポート

「IT パスポート試験」、「DS 検定 リテラシーレベル」、「G 検定」の3試験の合格数に応じて、デジタルバッジが発行されます。3試験のうちいずれか1種類の合格者には「DX 推進パスポート1」、いずれか2種類に合格すると「DX 推進パスポート2」、3つすべてに合格すると「DX 推進パスポート3」のデジタルバッジが発行されます。

DX 推進パスポートのデジタルバッジ

DX パスポート 3	「IT パスポート」「データサイエンティスト検定」「G 検定」のすべてに合格
DX パスポート 2	「IT パスポート」「データサイエンティスト検定」「G 検定」のいずれか2つに合格
	【デジタルバッジ発行のパターン】

	① 「IT パスポート」と「データサイエンティスト検定」に合格 ② 「IT パスポート」と「G 検定」に合格 ③ 「データサイエンティスト検定」と「G 検定」に合格
DX パスポート 1	「IT パスポート」「データサイエンティスト検定」「G 検定」のいずれか 1 つに合格 【デジタルバッジ発行のパターン】 ① 「IT パスポート」に合格 ② 「データサイエンティスト検定」に合格 ③ 「G 検定」に合格

(出典) デジタルリテラシー協議会「Di-Lite」をもとに作成

詳細理解のため参考となる文献（参考文献）	
Di-Lite	https://www.dilite.jp

23-1-1. IT ソフトウェア領域

Di-Lite の 3 つの領域のうち「IT ソフトウェア領域」における学習範囲「IT パスポート試験」のシラバスについて全体像を説明します。

IT パスポート試験のシラバスは、情報処理技術者試験の一部として、幅広い IT 知識を評価するために設計されています。シラバスは「ストラテジ系」「マネジメント系」「テクノロジー系」の 3 つの主要な領域に分かれています。

IT パスポート（IP）

対象者	職業人およびこれから職業人となる者が備えておくべき、IT に関する共通的な基礎知識を持ち、IT に携わる業務に就くか、担当業務に対して IT を活用していこうとする者

シラバスの全体像は以下の通りです。

ストラテジ系	
大分類 1：企業と法務	
中分類 1：企業活動	
● 経営・組織論 ● 業務分析・データ利活用 ● 会計・財務	

中分類 2 : 法務

- 知的財産権
- セキュリティ関連法規
- 労働関連・取引関連法規
- その他の法律・ガイドライン・情報倫理
- 標準化関連

大分類 2 : 経営戦略

中分類 3 : 経営戦略マネジメント

- 経営戦略手法
- マーケティング
- ビジネス戦略と目標・評価
- 経営管理システム

中分類 4 : 技術戦略マネジメント

- 技術開発戦略の立案・技術開発計画

中分類 5 : ビジネスインダストリ

- ビジネスシステム
- エンジニアリングシステム
- e-ビジネス
- [IoT](#) システム・組込みシステム

大分類 3 : システム戦略

中分類 6 : システム戦略

- 情報システム戦略
- 業務プロセス
- [ソリューション](#)ビジネス
- システム活用促進・評価

中分類 7 : システム企画

- システム化計画
- 要件定義
- 調達計画・実施

マネジメント系

大分類 4 : 開発技術

中分類 8 : システム開発技術

- システム開発技術

中分類 9 : ソフトウェア開発管理技術

- 開発プロセス・手法

大分類 5 : プロジェクトマネジメント

中分類 10 : プロジェクトマネジメント

- プロジェクトマネジメント

大分類 6 : サービスマネジメント

中分類 11 : サービスマネジメント

- サービスマネジメント
- サービスマネジメントシステム
- ファシリティマネジメント

中分類 12 : システム監査

- システム監査
- 内部統制

テクノロジー系

大分類 7 : 基礎理論

中分類 13 : 基礎理論

- 離散数学
- 応用数学
- 情報に関する理論

中分類 14 : アルゴリズムとプログラミング

- データ構造
- アルゴリズムとプログラミング
- プログラム言語
- その他の言語

大分類 8 : コンピュータシステム

中分類 15 : コンピュータ構成要素

- プロセッサ
- メモリ
- 入出力デバイス

中分類 16 : システム構成要素

- システムの構成
- システムの評価指標

中分類 17 : ソフトウェア

- オペレーティングシステム
- ファイルシステム
- オフィスツール
- オープンソースソフトウェア

中分類 18 : ハードウェア

- ハードウェア（コンピュータ・入出力装置）

大分類 9 : 技術要素

中分類 19 : 情報デザイン

- 情報デザイン
- インタフェース設計

中分類 20 : 情報メディア

- マルチメディア技術
- マルチメディア応用

中分類 21 : データベース

- データベース方式
- データベース設計
- データ操作
- トランザクション処理

中分類 22 : ネットワーク

- ネットワーク方式
- 通信プロトコル
- ネットワーク応用

中分類 23 : セキュリティ

- 情報セキュリティ
- 情報セキュリティ管理
- 情報セキュリティ対策・情報セキュリティ実装技術

（出典）IPA「ITパスポート試験シラバス」をもとに作成

「技術要素」に含まれる「情報セキュリティ」について抜粋して詳細に説明します。

情報セキュリティ

1. 情報セキュリティの概念

- 情報セキュリティの基本的な概念と目的

2. 情報資産

- 企業における情報資産の代表的な種類として、顧客情報、営業情報、知的財産関連情報、人事情報などがあること

3. 脅威と脆弱性

- 情報セキュリティの代表的な脅威の種類と基本的な対処法
- [セキュリティインシデント](#)が発生しやすくなる要因である脆弱性

① 人的脅威の種類と特徴

② 技術的脅威の種類と特徴

③ 物理的脅威の種類と特徴

④ 脆弱性

⑤ 不正のメカニズム

4. 攻撃手法

- 情報システム、組織および個人への外部からの不正な行為と手法、およびそれらへの対策の概要

情報セキュリティ管理

1. リスクマネジメント

- リスクマネジメントは、リスクの特定・分析・評価・対応という流れで実施されること
- 事故などが発生した際に対処するために、対応マニュアルの整備や教育・訓練などの準備が必要であること

2. 情報セキュリティ管理

- 情報セキュリティ管理の必要性と情報セキュリティマネジメントシステム（[ISMS](#) : Information Security Management System）の考え方

3. 個人情報保護

- 個人情報保護の必要性、法律やプライバシーマーク制度などの取組の目的

4. 情報セキュリティ組織・機関

- [不正アクセス](#)による被害受けの対応、再発防止のための提言、情報セキュリティに関する啓発活動などを行う情報セキュリティ組織・機関の役割、および関連する制度

5. 各種の基準・ガイドライン

- コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準、システム管理基準などが、情報システムに関する規範として利用されていること

情報セキュリティ対策・情報セキュリティ実装技術

1. 情報セキュリティ対策の種類

- 情報セキュリティ対策としての人的・技術的・物理的セキュリティ対策の基本的な考え

方

① 人的セキュリティ対策

- ・ 人的セキュリティ対策の種類
- ・ 身近な業務における基本的な対策の実行

② 技術的セキュリティ対策

- ・ 技術的セキュリティ対策の種類
- ・ 身近な業務における基本的対策の実行

③ 物理的セキュリティ対策

- ・ 物理的セキュリティ対策の種類
- ・ 組織のルールにしたがった行動の実行

2. 暗号技術

- 情報セキュリティを維持するために必要な暗号技術の基本的な仕組み、暗号化アルゴリズム、暗号強度などの特徴

3. 認証技術

- 認証の必要性、脅威を防止するためにどのような認証技術が用いられるかの概要
- それぞれの認証技術によって何が証明できるかの概要

4. 利用者認証

- 利用者認証のために利用される技術の種類、特徴

5. 生体認証（バイオメトリクス認証）

- 利用者確認に利用される技術の 1 つである生体認証技術の種類、特徴

6. 公開鍵基盤

- 公開鍵基盤の基本的な仕組みと特徴

7. アプリケーションソフトウェア・IoT システムのセキュリティ

- アプリケーションソフトウェア、IoT システム、IoT 機器のセキュリティの対策の種類、特徴

(出典) IPA「IT パスポート試験シラバス」をもとに作成

詳細理解のため参考となる文献（参考文献）

IT パスポート試験シラバス

https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014eh-att/syllabus_ip_ver6_3.pdf

23-1-2. 数理・データサイエンス領域

Di-Lite の 3 つの領域のうち「数理・データサイエンス領域」における学習範囲である「データサイエンティスト検定」のシラバスについて全体像を説明します。

データサイエンティストとは、データサイエンス力、データエンジニアリング力をベースにデータから価値を創出し、ビジネス課題に答えを出すプロフェッショナルです。データサイエンティストに求められるスキルセットはデータサイエンス力・ビジネス力・データエンジニアリング力とされ、検定においても 3 つの領域の力を図ります。

データサイエンティスト検定（リテラシーレベル）

対象者	- データサイエンティスト初学者 - これからデータサイエンティストを目指すビジネスパーソン

試験範囲（3つの領域）

領域	内容
データサイエンス力★1	線形代数基礎、微分・積分基礎、集合論基礎、統計数理基礎、洞察、性質・関係性、推定・検定、アソシエーション分析、因果推論、データ確認、俯瞰・メタ思考、データ理解、サンプリング、データクレンジング、データ加工、特徴量エンジニアリング、方向性定義、軸だし、データ加工、表現・実装技法、意味抽出、回帰・分類、統計的評価、機械学習、深層学習、時系列分析、クラスタリング、ネットワーク分析、レコメンド、自然言語処理、画像認識、映像認識、音声認識、大規模言語モデル
データエンジニアリング力★1	システム企画、システム設計、アーキテクチャ設計、クライアント技術、通信技術、データ抽出、データ収集、データ構造の基礎知識、テーブル定義、DWH、分散技術、クラウド、フィルタリング処理、ソート処理、結合処理、前処理、マッピング処理、サンプリング処理、集計処理、変換・演算処理、データ出力、データ展開、データ連携、基礎プログラミング、拡張プログラミング、AI サービス活用、アルゴリズム、分析プログラム、SQL、IT セキュリティの基礎知識、攻撃と防御手法、暗号化技術、認証、AutoML、MLOps、AIOps、プロンプトエンジニアリング、生成 AI のコーディング支援
ビジネス力★1	ビジネスマインド、データ・AI 倫理、コンプライアンス、MECE、構造化能力、言語化能力、ストーリーライン、ドキュメンテーション、説明能力、AI 活用検討、KPI、スコーピング、データ入手、分析アプローチ設計、生成 AI 活用、統計情報への正しい理解、ビジネス観点での理解、意味合いの抽出・洞察、評価・改善の仕組み、契約、権利保護、プロジェクト発足、リソースマネ

※データサイエンティストに求められるスキルについては、「22-4-1.データサイエンス領域」で説明します。

23-1-3. AI・ディープラーニング領域

Di-Lite の3つの領域のうち「AI・ディープラーニング領域」における学習範囲「G 検定」のシラバスについて全体像を説明します。

G 検定（ジェネラリスト検定）

対象者

- ビジネスに関わるすべての方

G 検定の試験範囲（シラバス）

技術分野

人工知能とは

人工知能の定義、人工知能分野で議論される問題

人工知能をめぐる動向

探索・推論、知識表現とエキスパートシステム、機械学習、ディープラーニング

機械学習の概要

教師あり学習、教師なし学習、強化学習、モデルの選択・評価

ディープラーニングの概要

ニューラルネットワークとディープラーニング、活性化関数、誤差関数、正則化、誤差逆伝播法、最適化手法

ディープラーニングの要素技術

全結合層、畳み込み層、正規化層、プーリング層、スキップ結合、回帰結合層、Attention、オートエンコーダ、データ拡張

ディープラーニングの応用例

画像認識、自然言語処理、音声処理、深層強化学習、データ生成、転移学習・ファインチューニング、マルチモーダル、モデルの解釈性、モデルの軽量化

AI の社会実装に向けて

AI プロジェクトの進め方、データの収集・加工・分析・学習

AI に必要な数理・統計知識

法律倫理分野

AI に関する法律と契約

個人情報保護法、著作権法、特許法、不正競争防止法、独占禁止法、AI 開発委託契約、AI サービス提供契約

AI 倫理・AI ガバナンス

国内外のガイドライン、プライバシー、公平性、安全性とセキュリティ、悪用、透明性、民主主義、環境保護、労働政策、そのほかの重要な価値、AI ガバナンス

(出典) 日本ディープラーニング協会「G 検定とは」をもとに作成

G 検定の試験範囲のうち、セキュリティに関する箇所を抜粋して説明します。

AI 倫理・AI ガバナンス

11. 安全性とセキュリティ

● 安全性に関する論点の所在と代表的な事例を理解している ● セキュリティ上の課題としてどのような攻撃などが存在しているのか理解している ● 安全性やセキュリティの課題への対応手段を理解している	Adversarial Attack (Adversarial Examples)、 セキュリティ・バイ・デザイン、データ汚染、データ窃取、モデル窃取、モデル汚染

(出典) 日本ディープラーニング協会「G 検定 試験出題範囲 (シラバス 2024)」をもとに作成

詳細理解のため参考となる文献 (参考文献)	
G 検定とは	https://www.jdla.org/certificate/general/#
G 検定の試験範囲 (シラバス) と例題	https://www.jdla.org/certificate/general/#general_No03

23-2. 情報処理技術者試験

個人や組織が安全で効果的な IT の活用を進めるためには、IT 業界や IT 職種に限らず、IT を利用する側のすべての人々が IT や情報セキュリティに関する知識を持つことが必要です。また、デジタルトランスフォーメーション（DX）の進展に伴い、IT やセキュリティに関する専門知識や業務経験がない人々にとっても、企業内外でセキュリティの専門人材と協力する機会が増加しています。このような協力関係を築くためにも、IT や情報セキュリティに関する知識を習得しておくことが望まれます。従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段の一つが、情報処理技術者試験の受験です。情報処理技術者試験に合格するには、[IT リテラシー](#)および情報セキュリティに関する基礎知識を習得する必要があります。組織全体で従業員一人一人のセキュリティ意識を高めることは、組織の安全な運営に不可欠です。また、組織内のセキュリティ専門人材不足の問題の解消にも役立ちます。まずは情報処理技術者試験の全体像を紹介します。

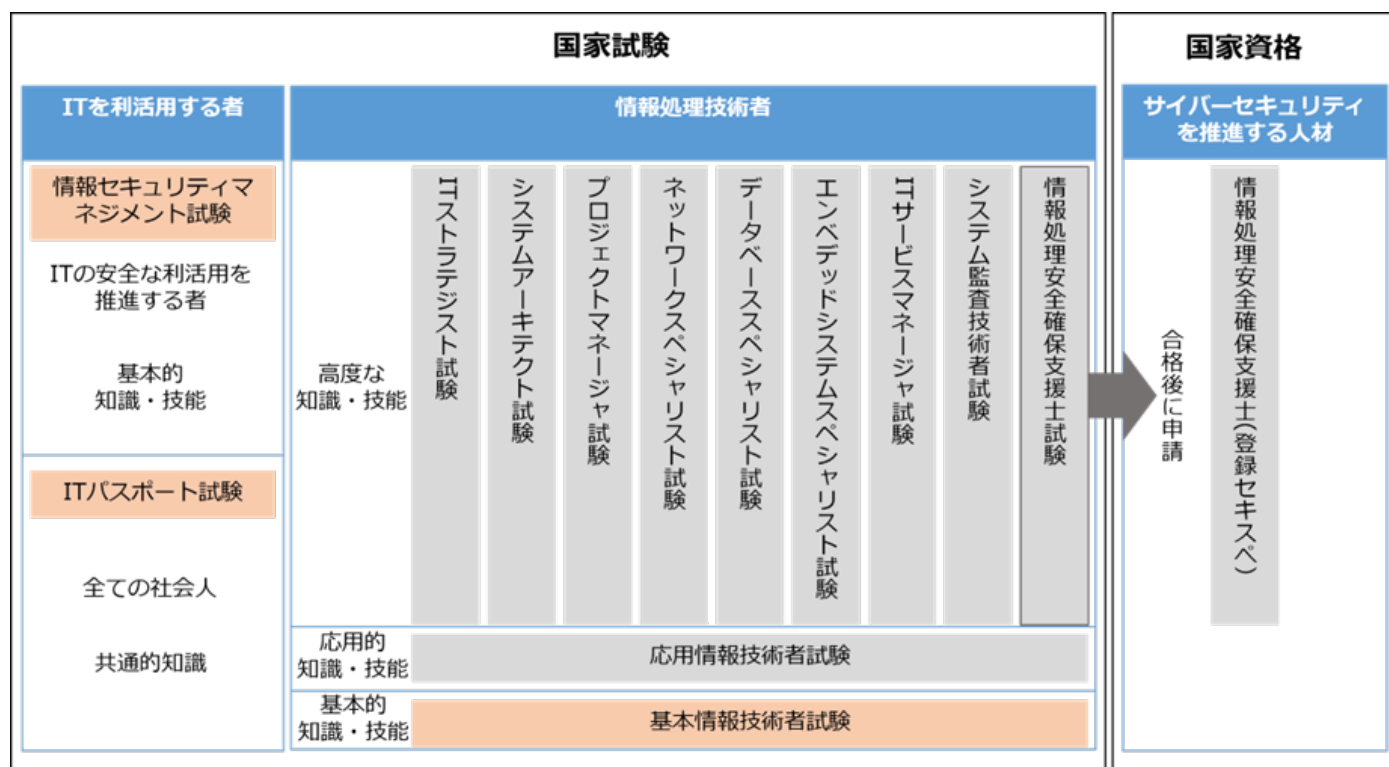


図 101. IT ヒューマンスキル概念図

（出典）IPA「情報処理技術者試験・情報処理安全確保支援士試験 試験要綱」をもとに作成

各試験の出題分野の全体像を以下の表に示します。

※IT パスポート試験については、「22-2-1. IT ソフトウェア領域」を参照してください。

出題分野			試験区分	情報セキュリティマネジメント試験（参考）	基本情報技術者試験（科目 A）	応用情報技術者	高度試験・支援士試験	
							午前 I（共通知識）	午前 II（専門知識）
								情報処理安全確保支援士試験
テクノロジー系	基礎理論	基礎理論			○2	○3	○3	
		アルゴリズムとプログラミング						
	コンピュータシステム	コンピュータ構成要素						
		システム構成要素	○2					
		ソフトウェア						
		ハードウェア						
	技術要素	ユーザーインターフェース			◎2	◎3	◎3	
		情報メディア						
		データベース	○2					○3
		ネットワーク	○2					◎4
		セキュリティ	◎2					◎4
	開発技術	システム開発技術			○2	○3	○3	○3
		ソフトウェア開発管理技術						○3
マネジメント系	プロジェクトマネジメント	プロジェクトマネジメント	○2					
	サービスマネジメント	サービスマネジメント	○2					○3
		システム監査	○2					○3
ストラテジ系	システム戦略	システム戦略	○2					
		システム企画	○2					
	経営戦略	経営戦略マネジメント						
		技術戦略マネジメント						
		ビジネスインダストリ						
	企業と法務	企業活動	○2					
		法務	◎2					

注記 1：○は出題範囲であることを、◎は出題範囲のうちの重点分野であることを表す。

注記 2：2、3、4 は技術レベルを表し、4 が最も高度で、上位は下位を包含する。

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

上記の表の「セキュリティ」分野の内容を詳細に説明します。

大分類	中分類	小分類	知識項目例
技術要素	セキュリティ	情報セキュリティ	情報の <u>機密性</u> ・ <u>完全性</u> ・ <u>可用性</u> 、多層防御、脅威、 <u>マルウェア</u> ・不正プログラム、脆弱性、不正のメカニズム、攻撃者の種類・動機、 <u>サイバー攻撃</u> （SQL インジェクション、クロスサイトスクリプティング、DoS 攻撃、フィッシング、パスワードリスト攻撃、 <u>標的型攻撃</u> 、 <u>AI</u> を悪用した攻撃ほか）、暗号技術（共通鍵、公開鍵、秘密鍵、RSA、AES、ハイブリッド暗号、ハッシュ関数ほか）、認証技術（デジタル署名、メッセージ認証、タイムスタンプほか）、利用者認証（利用者 ID・パスワード、 <u>多要素認証</u> 、パスワードレス認証、アイデンティティ連携（OpenID、SAML）ほか）、生体認証技術、公開鍵基盤（PKI、認証局、デジタル証明書ほか）、政府認証基盤（GPKI、ブリッジ認証局ほか）など
		情報セキュリティ管理	<u>情報資産</u> とリスクの概要、情報資産の調査・分類、リスクの種類、情報セキュリティリスクアセスメントおよびリスク対応、情報セキュリティ継続、情報セキュリティ諸規程（ <u>情報セキュリティポリシー</u> を含む組織内規程）、 <u>ISMS</u> 、情報セキュリティ管理策（組織的管理策、人的管理策、物理的管理策、技術的管理策）、情報セキュリティ組織・機関（ <u>CSIRT</u> 、SOC（Security Operation Center）、エシカルハッカーほか）、コンピュータ <u>不正アクセス</u> 対策基準、コンピュータウイルス対策基準、PCI DSS など
		セキュリティ技術評価	ISO/IEC 15408（コモンクライテリア）、JISEC（IT セキュリティ評価および認証制度）、JCMVP（暗号モジュール試験および認証制度）、 <u>CVSS</u> 、脆弱性検査、 <u>ペネトレーションテスト</u> など
		情報セキュリティ対策	情報セキュリティ啓発（教育、訓練ほか）、組織における内部不正防止ガイドライン、マルウェア・不正プログラム対策、 <u>ランサムウェア</u> 対策、不正アクセス対策、情報漏えい対策、アカウント管理、ログ管理、 <u>脆弱性</u> 管理、入退室管理、 <u>アクセス制御</u> 、侵入検知/侵入防止、検疫ネットワーク、携

			帯端末（携帯電話、スマートフォン、タブレット端末ほか）のセキュリティ、クラウドサービスのセキュリティ、IoTのセキュリティ、AIを使ったセキュリティ技術、AIそのものを守るセキュリティ技術、セキュリティ製品・サービス（ファイアウォール、WAF、DLP、SIEM ほか）、デジタルフォレンジックスなど
		セキュリティ実装技術	セキュアプロトコル（IPsec、SSL/TLS、SSH、WPA3 ほか）、認証・認可技術（SPF、DKIM、SMTP-AUTH、OAuth、DNSSEC ほか）、セキュア OS、ネットワークセキュリティ、データベースセキュリティ、アプリケーションセキュリティ、コンテナセキュリティ、セキュアプログラミングなど

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

詳細理解のため参考となる文献（参考文献）	
情報処理技術者試験 情報処理安全確保支援士 試験要綱	https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf

セキュリティに関する知識やスキルを身につけるためには、以下の試験が推奨されます。

- IT パスポート
- 情報セキュリティマネジメント試験
- 基本情報技術者試験
- 応用情報技術者試験
- 情報処理安全確保支援士試験

上記の試験に焦点を当て、各試験について説明します。

※IT パスポート試験については、「22-2-1. IT ソフトウェア領域」を参照してください。

23-2-1. 情報セキュリティマネジメント試験

対象者	情報システムの利用部門にあって、情報セキュリティリーダーとして、部門の業務遂行に必要な情報セキュリティ対策や組織が定めた情報セキュリティ諸規程（情報セキュリティポリシーを含む組織内諸規程）の目的・内容を適切に理解し、情報および情報システムを安全に活用するために、情報セキュリティが確保

	された状況を実現し、維持・改善する者。
業務と役割	情報システムの利用部門において情報セキュリティが確保された状況を実現し、維持・改善するために、次の業務と役割を果たします。 ① 部門における情報資産の情報セキュリティを維持するために必要な業務を遂行します。 ② 部門の情報資産を特定し、情報セキュリティリスクアセスメントを行い、リスク対応策をまとめます。 ③ 部門の情報資産に関する情報セキュリティ対策および情報セキュリティ継続の要求事項を明確にします。 ④ 部門の業務のIT活用推進に伴う情報システムの調達に際して、利用部門として必要となる情報セキュリティ要求事項を明確にする。また、IT活用推進の一部を利用部門が自ら実現する活動の中で、必要な情報セキュリティ要求事項を提示します。 ⑤ 業務の外部委託に際して、情報セキュリティ対策の要求事項を契約で明確化し、その実施状況を確認します。 ⑥ 部門の情報システムの利用時における情報セキュリティを確保します。 ⑦ 部門のメンバーの情報セキュリティ意識、コンプライアンスを向上させ、内部不正などの情報セキュリティインシデントの発生を未然に防止します。 ⑧ 情報セキュリティインシデントの発生またはそのおそれがあるときに、情報セキュリティ諸規程、法令・ガイドライン・規格などに基づいて、適切に対処します。 ⑨ 部門または組織全体における情報セキュリティに関する意見・問題点について担当部署に提起します。
活用方法	① 部門の情報セキュリティマネジメントの一部を独力で遂行できます。 ② 情報セキュリティインシデントの発生またはそのおそれがあるときに、情報セキュリティリーダーとして適切に対処できます。 ③ IT全般に関する基本的な用語・内容を理解できます。 ④ 情報セキュリティ技術や情報セキュリティ諸規程に関する基本的な知識を持ち、部門の情報セキュリティ対策の一部を独力で、または上位者の指導の下に実現できます。 ⑤ 情報セキュリティ機関、他の企業などから動向や事例を収集し、部門の環境への適用の必要性を評価できます。

23-2-2. 基本情報技術者試験

対象者	IT を活用したサービス、製品、システムおよびソフトウェアを作る人材に必要な基本的知識・技能を持ち、実践的な活用能力を身につけた者。
業務と役割	上位者の指導の下に、次のいずれかの役割を果たします。 ① 組織および社会の課題に対する、IT を活用した戦略の立案、システムの企画・要件定義に参加します。 ② システムの設計・開発、汎用製品の最適組み合わせ（インテグレーション）によって、利用者にとって価値の高いシステムを構築します。 ③ サービスの安定的な運用の実現に貢献します。
活用方法	① IT 全般に関する基本的な事項を理解し、担当する活動に活用できます。 ② 上位者の指導の下に、IT 戦略に関する予測・分析・評価に参加できます。 ③ 上位者の指導の下に、システムまたはサービスの提案活動に参加できます。 ④ 上位者の指導の下に、システムの企画・要件定義に参加できます。 ⑤ 上位者の指導の下に、情報セキュリティの確保を考慮して、システムの設計・開発・運用ができます。 ⑥ 上位者の指導の下に、ソフトウェアを設計できます。 ⑦ 上位者の方針を理解し、自らプログラムを作成できます。

23-2-3. 応用情報技術者試験

対象者	IT を活用したサービス、製品、システムおよびソフトウェアを作る人材に必要な応用的知識・技能を持ち、高度 IT 人材としての方向性を確立した者。
業務と役割	独力で次のいずれかの役割を果たします。 ① 組織および社会の課題に対する、IT を活用した戦略の立案、システムの企画・要件定義を行います。 ② システムの設計・開発、汎用製品の最適組み合わせ（インテグレーション）によって、利用者にとって価値の高いシステムを構築します。

	③ サービスの安定的な運用を実現します。
活用方法	① 経営戦略・IT 戦略の策定に際して、経営者の方針を理解し、経営を取り巻く外部環境を正確に捉え、動向や事例を収集できます。 ② 経営戦略・IT 戦略の評価に際して、定められたモニタリング指標に基づき、差異分析などを行うことができます。 ③ システムまたはサービスの提案活動に際して、提案討議に参加し、提案書の一部を作成できます。 ④ システムの企画・要件定義、アーキテクチャの設計において、システムに対する要求を整理し、適用できる技術の調査を行うことができます。 ⑤ 運用管理チーム、オペレーションチーム、サービスデスクチームなどのメンバーとして、担当分野におけるサービス提供と安定稼働の確保を行うことができます。 ⑥ プロジェクトメンバーとして、プロジェクトマネージャ（リーダー）の下でスコープ、予算、工程、品質などの管理ができます。 ⑦ 情報システム、ネットワーク、データベース、組込みシステムなどの設計・開発・運用・保守において、上位者の方針を理解し、自ら技術的問題を解決できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

23-2-4. 各分野スペシャリスト試験

各分野スペシャリスト試験については、概要を説明します。

IT ストラテジスト試験（ST）

対象者	高度 IT 人材として確立した専門分野を持ち、企業の経営戦略に基づいて、ビジネスモデルや企業活動における特定のプロセスについて、情報技術（IT）を活用して事業を改革・高度化・最適化するための基本戦略を策定・提案・推進する者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

IT ストラテジスト試験は、経営戦略に基づいて IT 戦略を策定し、IT を高度に活用した事業革新、業務改革、および競争優位を獲得する製品・サービスの創出を企画・推進して、ビジネスを成功

に導く CIO や CTO、IT コンサルタントを目指す方に最適な試験です。

システムアーキテクト試験（SA）

対象者	高度 IT 人材として確立した専門分野を持ち、IT ストラテジストからの提案を受けて、情報システムを利用したシステムの開発に必要な要件を定義し、それを実現するためのアーキテクチャを設計し、開発を主導する者。

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

システムアーキテクト試験は、システム開発の上流工程を主導する立場で、豊富な業務知識に基づいて的確な分析を行い、業務ニーズに適した情報システムのグランドデザインを設計し完成に導く、上級エンジニアを目指す方に最適な試験です。

プロジェクトマネージャ試験（PM）

対象者	高度 IT 人材として確立した専門分野を持ち、組織の戦略の実現に寄与することを目的とするシステム開発プロジェクトにおいて、プロジェクトの目的の実現に向けて責任を持ってプロジェクトマネジメント業務を単独でまたはチームの一員として担う者。

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

プロジェクトマネージャ試験は、プロジェクトを取り巻く環境変化やステークホルダの多様な要求に柔軟に対応しながら、プロジェクトを確実に成功に導くマネージャを目指す方に最適な試験です。

ネットワークスペシャリスト試験（NW）

対象者	高度 IT 人材として確立した専門分野を持ち、ネットワークに関係する固有技術を活用し、最適な情報システム基盤の企画・要件定義・開発・運用・保守において中心的な役割を果たすとともに、固有技術の専門家として、情報セキュリティを含む情報システムの企画・要件定義・開発・運用・保守への技術支援を行う者。

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

ネットワークスペシャリスト試験は、ネットワークの固有技術からサービス動向まで幅広く精通し、目的に適合した大規模かつ堅牢なネットワークシステムを構築し運用できるネットワークエンジニアやインフラ系エンジニアを目指す方に最適な試験です。

データベーススペシャリスト試験（DB）

対象者	高度 IT 人材として確立した専門分野を持ち、データベースに関係する固有技術を活用し、最適な情報システム基盤の企画・要件定義・開発・運用・保守において中心的な役割を果たすとともに、固有技術の専門家として、情報システムの企画・要件定義・開発・運用・保守への技術支援を行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

データベーススペシャリスト試験は、企業活動を支える膨大なデータ群を管理し、パフォーマンスの高いデータベースシステムを構築して、顧客のビジネスに活用できるデータ分析基盤を提供するデータベース管理者やインフラ系エンジニアを目指す方に最適な試験です。

エンベデッドシステムスペシャリスト試験（ES）

対象者	高度 IT 人材として確立した専門分野を持ち、 IoT を含む組み込みシステムの開発に関係する広い知識や技能を活用して、市場動向・関連業界の動向を踏まえて最適な組み込みシステムの事業戦略や製品戦略を策定し、ハードウェアとソフトウェアの要求仕様の策定、および要求仕様に基づいた組み込みシステムの設計・構築・製造を主導的に行う者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

エンベデッドシステムスペシャリスト試験は、スマート家電、自動運転などあらゆるモノがつながる IoT が進展する中で、新たな機能を実現するために、ハードウェアとソフトウェアを適切に組み合わせたシステムの企画・開発を推進し、必要な機能・性能・品質・セキュリティなどを確保する、組み込み・IoT 系のフルスタックエンジニアを目指す方に最適な試験です。

IT サービスマネージャ試験（SM）

対象者	高度 IT 人材として確立した専門分野を持ち、サービスの要求事項を満たし、サービスの計画立案、設計、移行、提供および改善のための組織の活動および資源を、指揮し、管理する者。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

IT サービスマネージャ試験は、顧客ニーズを踏まえ、日々の継続的改善を通じて安全性と[信頼性](#)の高い IT サービスを最適なコストで安定的に提供し、IT 投資効果を最大化できる IT サービスマネージャを目指す方に最適な試験です。

システム監査技術者試験（AU）

対象者	高度 IT 人材として確立した専門分野を持ち、高い倫理観の下、監査対象から独立かつ客観的な立場で、情報システムや組込みシステムを総合的に検証・評価して、監査報告の利用者に情報システムのガバナンス、マネジメント、コントロールの適切性などに対する保証を与える、または改善のための助言を行う者。

（出典）IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

システム監査技術者試験は、情報システムに係るリスクを分析し、コントロールを評価・検証することによって、組織体の目標達成に寄与し、利害関係者に対する説明責任を果たす監査人や情報システム責任者などをを目指す方に最適な試験です。

23-2-5. 情報処理安全確保支援士試験

対象者	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し、また、サイバーセキュリティ対策の調査・分析・評価を行い、その結果に基づき必要な指導・助言を行う者。
業務と役割	情報セキュリティマネジメントに関する業務、情報システムの企画・設計・開発・運用におけるセキュリティ確保に関する業務、情報および情報システムの利用におけるセキュリティ対策の適用に関する業務、情報セキュリティインシデント管理に関する業務に従事し、次の役割を主導的に果たすとともに、下位者を指導します。 ① 情報セキュリティ方針および情報セキュリティ諸規程（事業継続計画に関する規程を含む組織内諸規程）の策定、情報セキュリティリスクアセスメントおよびリスク対応などを推進または支援します。 ② システム調達（製品・サービスのセキュアな導入を含む）、システム開発（セキュリティ機能の実装を含む）を、セキュリティの観点から推進または支援します。 ③ 暗号利用、マルウェア対策、脆弱性への対応など、情報および情報システムの利用におけるセキュリティ対策の適用を推進または支援します。 ④ 情報セキュリティインシデントの管理体制の構築、情報セキュリティインシデントへの対応などを推進または支援します。

活用方法	① 情報システムおよび情報システム基盤の脅威分析に関する知識を持ち、セキュリティ要件を抽出できます。 ② 情報セキュリティの動向・事例、およびセキュリティ対策に関する知識を持ち、セキュリティ対策を対象システムに適用するとともに、その効果を評価できます。 ③ 情報セキュリティマネジメントシステム、情報セキュリティリスクアセスメントおよびリスク対応に関する知識を持ち、情報セキュリティマネジメントについて指導・助言できます。 ④ ネットワーク、データベースに関する知識を持ち、暗号、認証、フィルタリング、ロギングなどの要素技術を適用できます。 ⑤ システム開発、品質管理などに関する知識を持ち、それらの業務について、セキュリティの観点から指導・助言できます。 ⑥ 情報セキュリティ方針および情報セキュリティ諸規程の策定、内部不正の防止に関する知識を持ち、情報セキュリティに関する従業員の教育・訓練などについて指導・助言できます。 ⑦ 情報セキュリティ関連の法的要求事項、情報セキュリティインシデント発生時の証拠の収集および分析、情報セキュリティ監査に関する知識を持ち、それらに関連する業務を他の専門家と協力しながら遂行できます。

(出典) IPA「情報処理技術者試験 情報処理安全確保支援士 試験要綱」をもとに作成

国際セキュリティ資格

各情報処理技術者試験で培った IT 知識は、国際セキュリティ資格の学習の基礎となります。また、相乗効果の観点から国際セキュリティ資格の学習を通じて、各情報処理技術者試験の知識を深められたり、より高度な IT ポジションへのキャリアアップが期待できたりします。

CISSP (Certified Information Systems Security Professional)

対象者	情報セキュリティ分野での専門知識と経験を持っている者。
業務と役割	ISC2 が認定を行うベンダーフリー・カントリーフリーの情報セキュリティの専門家資格です。CISSP には、情報セキュリティにおける理論やメカニズムを理解することに加えて、その知識を体系的かつ構造的に整理し、状況に応じた適切な判断を行うための、合理的かつ実践的な「知識」と「理解度」があることを証明します。

活用方法	ANSI（米国規格協会）より、ISO/IEC17024 の認証を受けた厳正な資格開発、運用、運営、維持に加え、米国国防総省のキャリアパスにおいて取得が義務付けられている資格の 1 つにも認定されており、CISSP は知識と実務経験を兼ね備えた、常に最新の知識を持った情報セキュリティプロフェッショナルであることを証明します。

(出典) ISC2「CISSP 8 ドメインガイドブック」をもとに作成

CISM (Certified Information Security Manager)

対象者	主に情報セキュリティガバナンス、プログラムの開発と管理、インシデント管理、およびリスク管理の専門知識を持っていることを証明することを希望する者。
業務と役割	CISM は、情報セキュリティマネジメントの知識と経験を認定する国際的資格であり、日本語名称を『公認情報セキュリティマネージャ』と呼称します。ISACA により、2002 年に資格制度が創設され、2003 年度より試験が開始されました。情報セキュリティマネジメントのチームプレイヤーからリーダーへ、ステップアップしたい方に最適な認定資格です。
活用方法	CISM は、企業・団体などの情報セキュリティプログラムに係る、マネジメント、設計、監督を行う、以下のプロフェッショナルの方をフォーカスしています。 ● セキュリティマネージャ (Security managers) ● 最高情報セキュリティ責任者 (CISO) や最高戦略責任者 (CSO) をはじめとする ● セキュリティ担当役員 (Security directors) ● セキュリティ担当役職者 (Security officers) ● セキュリティコンサルタント (Security consultants) ● コンプライアンス、リスク、プライバシー担当役職者・マネージャ

(出典) ISACA 東京支部ホームページをもとに作成

CISA (Certified Information Systems Auditor)

対象者	企業などで運用されている情報システムの <u>信頼性</u> ・安全性などの検証・評価を行う際に高いスキルを持って対応できると証明することを希望する者。

業務と役割	CISA とは"Certified Information Systems Auditor"の略称であり、「公認情報システム監査人」とも呼ばれています。ISACA（情報システムコントロール協会）が認定する国際的な資格であり、情報システムを監査する者の能力と専門性を証明します。
活用方法	IT/情報システム監査人、コントロール、保証および情報セキュリティの専門家としてのキャリア育成に役立ちます。

(出典) ISACA 東京支部ホームページをもとに作成

詳細理解のため参考となる文献（参考文献）	
CISSP 8 ドメインガイドブック	https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部	https://www.isaca.gr.jp

第24章. 各種人材育成カリキュラム

章の目的

第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を把握することを目的とします。紹介するカリキュラム内容は、具体的な実施計画や実施内容を検討する際の参考資料となります。

主な達成目標

- 「プラス・セキュリティ知識補充講座 カリキュラム例」のカリキュラム内容を理解すること
- 「IT スキル標準モデルカリキュラム」のカリキュラム内容を理解すること
- デジタルスキル習得に関する講座を紹介する「マナビ DX」について概要と活用方法を理解すること

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

「プラス・セキュリティ知識補充講座」は、内閣サイバーセキュリティセンター（[NISC](#)）が提供するプログラムで、特に経営層やデジタルトランスフォーメーション（DX）を推進する部課長向けに設計されています。この講座は、企業内外のセキュリティ専門人材との協働を円滑に行うために必要な知識を補充することを目的としています。

具体的には、以下のように経営層向けと[デジタル化](#)推進部門の部課長級マネジメント層向けの2つのカリキュラムで構成されています。

- 経営層
企業のセキュリティリスクに対する理解を深め、経営判断に役立つ知識を提供。
- デジタル化推進部門の部課長級マネジメント層
業務や製品・サービスのデジタル化を推進する役割を担う部門の管理職向けに、セキュリティリスク管理やデジタル化に伴うセキュリティ対策を強化する知識を提供。

理想とする目標

経営層（必ずしも DX を担当している部署の担当役員などではなく、経営層全体）

- サイバーセキュリティに関する動向が自社のコーポレートリスクに与える影響を的確に把握できる。
- 上記の影響を踏まえ、自社のセキュリティ体制構築・投資の決定・指示を的確に実行できる。
- 万一のインシデント発生時に、的確に経営判断を行い、指示をできる。

業務、製品・サービスのデジタル化を推進する部門のマネジメントを担う部課長級

- サイバーセキュリティに関する動向が自社の担当する事業・自部署に与える影響を的確に把握できる。
- 上記の影響を踏まえつつ、自部署で実施されている対策の現状を理解できる。
- 上記について、経営層が的確な経営判断をできるよう、自ら説明・報告できる。
- 上記を実施するために、社内（情報システム部門など）・社外（ベンダーなど）と、円滑にコミュニケーションできる。

（出典）NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

このカリキュラムは、企業内研修のプログラムを策定する際に参考にできるよう設計されており、対象別の目標・到達レベルは以下の通りです。

カリキュラム受講後の到達レベルは、以下の表の「中」のレベルを想定しています。つまり、専

門家との意見交換ができるレベルを目指したものとなっています。

	理解	コミュニケーション	評価・分析	判断
高	自らの役割に必要な知識を概ね網羅的に習得し、理解している	自ら把握すべきことを洗い出し、専門家を含む適切な対象者に回答を求めることができる	脅威や脆弱性が自組織に及ぼす影響を評価できる	自らの知識のみで、自組織での対応に関する適切な判断ができる
中	自らの役割に必要な知識の全体像を把握した上で、その一部について理解していることを自覚している	専門家との意見交換ができる	脅威や脆弱性がどのように自組織に影響を及ぼすのかを理解できる	専門家の判断について、根拠を理解して合意を与えることができる
低	サイバーセキュリティ関連文書に用いられる用語の意味を理解している	専門家からの説明を概ね理解することができる	脅威や脆弱性とは何かを理解している	自らの知識のみでは判断に関与することが困難

カリキュラム例の構成は以下の通りです。

	経営層向け	部課長級向け	
目標	- サイバーセキュリティが自社のコーポレートリスクに与える影響の把握 - 影響を踏まえた自社のセキュリティ体制構築・投資の決定・指示 - インシデント発生時の適切な経営判断・指示	- サイバーリスクが自部署に与える影響理解 - 自部署で実施されている対策の現状理解 - 上記の経営層への報告	社内外とのコミュニケーション
時間設定	7.5時間（集合講習3時間＋オンデマンド4.5時間（うち必須3時間））	11時間（集合講習4.5時間＋オンデマンド6.5時間（うち必須5.5時間））	
留意点	- 経営会議及び対外対応として実際に起こり得るケースから逆算 - 各コマのインプット項目では、部課長級向けから内容を限定・変更	- 部署内会議やベンダー管理で実際に起こり得るケースから逆算 - 既存のスキルなどフレームワーク（SP800-181等）と紐付けを実施	
1.基礎知識	① デジタルインフラの基本（30分）◇ ② デジタル技術の基盤とリスク（30分）◇ ③ デジタル環境のコストと運用責任（30分）◇	① デジタルインフラ入門（20分）◇	
		② サイバーセキュリティに関する用語の意味（20分）◇ ③ デジタル環境の管理や責任に関するキーワード（20分）◇	
2.脅威と対策	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーションなど）（30分）★	① サイバー攻撃手法とそのトレンド（30分）◆ ② 脅威への対策（30分）◆ ③ 事例紹介（実際のサイバー攻撃事例の紹介、サイバー攻撃のデモンストレーションなど）（30分）★	
		④ 演習1：脅威と対策における“悪い見本”から学ぶ（60分）★	
3.投資	① コーポレートリスクとしてのサイバーセキュリティ（コンプライアンスを含む）（30分）◆ ② 体制構築・人材確保（30分）◆ ③ 演習1：各種対策の費用、損失想定、確率値から必要な投資を検討（70分）★	① サイバーセキュリティのリスクマネジメントの特徴（30分）◆ ② 対策における費用と損失の考え方（30分）◆ ③ リスクマネジメントのケーススタディ（30分）★ ④ 演習2：自部署リスクとその対応策を洗い出し、リスク管理部门などへ説明（60分）★	
4.SHとの関係	① インシデント対応における経営層の役割（30分）◆ ② 通常時の備えと情報開示の在り方（30分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習2：インシデント発生時の模擬記者会見（50分）★	① インシデント対応プロセスとその準備（30分）◆ ② 通常時の備えとインシデント情報の取扱上のポイント（30分）◆ ③ インシデント対応と情報開示の事例から学ぶ（30分）★ ④ 演習3：インシデント発生時の社内外連絡（60分）★	
5.関係法令	-	① サイバーセキュリティに関する国内法令とその読み方（20分）◆ ② サイバーセキュリティに関する基準・規格など（20分）◆ ③ サイバーセキュリティに関するガイドラインなど（20分）◆	

★：集合講習での開催が推奨されるもの（受講必須）

◆：オンライン・オンデマンド形式での実施を想定（受講必須）

◇：オンライン・オンデマンド形式での実施を想定（受講任意）

（出典）NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

24-1-1. 経営層向けカリキュラム例

経営層向けカリキュラム例を紹介します。カリキュラムは、4 単元で構成されます。

経営層向け第1単元	
名称	1.基礎知識 『デジタルシステムとサイバーセキュリティの概要』
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。

経営層向け第2単元	
名称	2.脅威と対策 『サイバー空間における脅威と対策』
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

経営層向け 第3単元	
名称	3.投資 『サイバーセキュリティと投資対効果』
目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。

	セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。

経営層向け 第4単元	
名称	4.ステークホルダーとの関係 『サイバーセキュリティと企業価値』
目標	サイバー<u>セキュリティインシデント</u>の発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。
到達レベル	自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-1-2. 部課長級向けカリキュラム例

部課長級向けカリキュラム例を紹介します。カリキュラムは、5単元で構成されます。

部課長級向け 第1-1単元	
名称	1.基礎知識 『デジタルシステムとサイバーセキュリティの概要（初級編）』
目標	<u>デジタル化</u>を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。

部課長級向け 第1-2単元	
名称	1.基礎知識 『デジタルシステムとサイバーセキュリティの概要（中級編）』

目標	● デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➤ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➤ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念について、第2単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることにする。

部課長級向け 第2単元	
名称	2.脅威 『サイバー空間における脅威と対策』
目標	● 脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

部課長級向け 第3単元	
名称	3.投資 『サイバーセキュリティとリスク対応』
目標	● 自部署におけるサイバーセキュリティリスクのマネジメントに必要なとなる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

部課長級向け 第4単元

名称	4.ステークホルダーとの関係 『サイバーセキュリティ対応における社内外連携』
目標	デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。
到達レベル	自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。

部課長級向け 第5単元

名称	5.関連法令 『サイバーセキュリティに関する法制度』
目標	サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。

（出典）NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

カリキュラム例の詳細については、「付録：プラス・セキュリティ知識補充講座カリキュラム例の詳細」に記載しています。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1）】

IT スキル標準（ITSS）については、22 章で説明しましたが、各種 IT 関連サービスの提供に必要とされる知識やスキルを体系化した指標であり、産学における IT サービス・プロフェッショナルの教育・訓練などに有用な「ものさし」（共通枠組）を提供しようとするものです。

IT スキル標準は、11 の職種と 35 の専門分野を設け、それぞれの専門分野に対応して、各個人の能力や実績に基づく 7 段階の達成レベルを規定しています。

「IT スキル標準モデルカリキュラム」は、IT スキル標準のレベル 1～3 を目指す人向けのカリキュラムとして IPA から公開されているものですが、ここではレベル 1 向けのモデルカリキュラムを紹介します。

このカリキュラムは、職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラムであり、研修ロードマップをもとに、具体的な研修コースを設計・実施する際に参考となる情報がまとめられています。このモデルカリキュラムを履修することにより、IT スキル標準のレベル 1 に相当する知識を修得することができます。

IT スキル標準モデルカリキュラムの構成

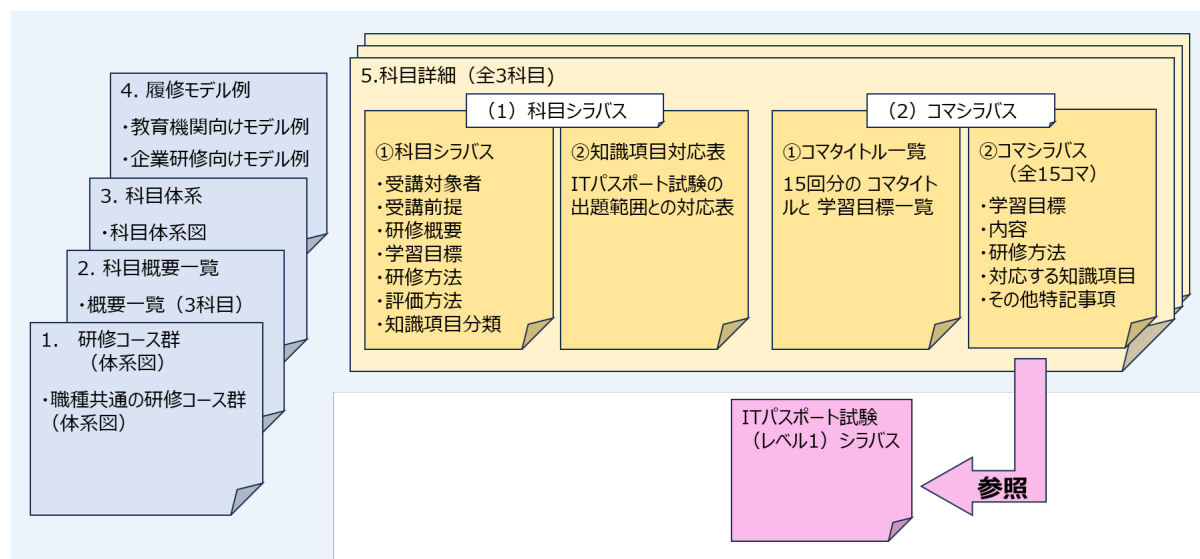


図.102 「IT スキル標準モデルカリキュラムの構成」

（出典）IPA「IT スキル標準モデルカリキュラムーレベル1を目指してー」をもとに作成

IT スキル標準のレベル 1 モデルカリキュラム（科目概要一覧）

対象人材

- ① 本格的な就業経験のない学生
- ② IT に関する基本的な知識を持たない社会人

対象場面	① 企業：IT 系企業を含め企業などの内定者の入社前研修など ② 教育機関：情報系、非情報系のすべての学部、学科における教育。ただし、情報系専門学科においては一般教養課程における教育
特徴	● 特定の製品や分野に偏らない知識と体系的なパーソナルスキルを修得できます。 ● IT パスポート試験の出題範囲と整合し、科目およびコマシラバスごとに知識項目との対応が明らかになっているので、「IT パスポート試験（レベル 1）シラバス」と併用することでより一層の研修効果を図ることができます。

このカリキュラムでは「IT 基本 1」コース群に含まれるコース「IT 入門」と「パーソナルスキル入門」に対応する科目が策定されています。

科目名	概要	受講対象者／ 受講前提	構成	時間
IT 入門（1）	「IT 基本 1」コース群の 1 つとして、ストラテジおよびマネジメント分野の基本的かつ普遍的な知識の修得を目的とする。 具体的には、企業における経営戦略と担当業務の関連、システム開発のライフサイクル、プロジェクトマネジメント、サービスマネジメントおよびシステム監査などの知識を学習する。	IT スキル標準のレベル 1 を目指す者/前提科目は特 にないが、高校卒業程度の知識を有していること	90 分 ×15 回	22.5h
IT 入門（2）	「IT 基本 1」コース群の 1 つとして、テクノロジー分野の基本的な知識の修得を目的とする。具体的には、情報のデジタル化とアルゴリズム、ハードウェア、ソフトウェア、ネットワーク、データベースおよびセキュリティに関する基本的な知識を学習する。	IT スキル標準のレベル 1 を目指す者/「IT 入門（1）」を修了していること、または同等の知識を有していること	90 分 ×15 回	22.5h
パーソナルスキル入門	パーソナルの領域に関して職業人として基本的な要件である、チームワークに基づくリーダーシップ、コミュニケーションの基本（書く、話す、聞く、考える）、プレゼンテーションの基本、論理展開（問題解決）法の基本、基本的なビジネスマナー、	IT スキル標準のレベル 1 を目指す者/前提科目は特 にないが、高校卒業程度の知識を有していること	90 分 ×15 回	22.5h

(出典) IPA「IT スキル標準モデルカリキュラム－レベル1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル1 コマタイトル一覧」に記載しています。

IT 入門（2）

科目シラバス

科目	IT 入門（2）																						
職種	職種共通																						
レベル区分 （対象者）	IT スキル標準のレベル1 を目指す者																						
受講前提	「IT 入門（1）」を修了していること、また同等の知識を有していること																						
学習目標	職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる																						
研修・ 教育方法	講義、演習																						
修得スキルの 評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う																						
カリキュラム構成	1 コマ 90 分×15 回（総時間：22.5 時間）																						
知識項目分類	【分野】 テクノロジ系 <table> <tr> <td>【大分類】 7 基礎理論</td><td>【中分類】 13 基礎理論</td></tr> <tr> <td></td><td>14 アルゴリズムとプログラミング</td></tr> <tr> <td>8 コンピュータシステム</td><td>【中分類】 15 コンピュータ構成要素</td></tr> <tr> <td></td><td>16 システム構成要素</td></tr> <tr> <td></td><td>17 ソフトウェア</td></tr> <tr> <td></td><td>18 ハードウェア</td></tr> <tr> <td>9 技術要素</td><td>【中分類】 19 ヒューマンインタフェース</td></tr> <tr> <td></td><td>20 マルチメディア</td></tr> <tr> <td></td><td>21 データベース</td></tr> <tr> <td></td><td>22 ネットワーク</td></tr> <tr> <td></td><td>23 セキュリティ</td></tr> </table>	【大分類】 7 基礎理論	【中分類】 13 基礎理論		14 アルゴリズムとプログラミング	8 コンピュータシステム	【中分類】 15 コンピュータ構成要素		16 システム構成要素		17 ソフトウェア		18 ハードウェア	9 技術要素	【中分類】 19 ヒューマンインタフェース		20 マルチメディア		21 データベース		22 ネットワーク		23 セキュリティ
【大分類】 7 基礎理論	【中分類】 13 基礎理論																						
	14 アルゴリズムとプログラミング																						
8 コンピュータシステム	【中分類】 15 コンピュータ構成要素																						
	16 システム構成要素																						
	17 ソフトウェア																						
	18 ハードウェア																						
9 技術要素	【中分類】 19 ヒューマンインタフェース																						
	20 マルチメディア																						
	21 データベース																						
	22 ネットワーク																						
	23 セキュリティ																						

(出典) IPA「IT スキル標準モデルカリキュラム－レベル1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル1 コマタイトル一覧」に記載しています。

パーソナルスキル入門

科目シラバス

科目	パーソナルスキル入門
職種	職種共通
レベル区分 (対象者)	IT スキル標準のレベル 1 を目指す者
受講前提	前提科目は特にないが、高校卒業程度の知識を有していること
学習目標	職業人としての基本的なパーソナルスキルの知識を活用し、上位者の指導の下、チームメンバーとして、業務活動に参加することができる
研修・ 教育方法	講義、グループ演習
修得スキルの 評価方法	講義終了後の受講レポート、定量アンケート、知識確認テスト、演習問題の取組状況を総合的に判断して評価を行う
カリキュラ ム構成	1 コマ 90 分×15 回（総時間：22.5 時間）

(出典) IPA「IT スキル標準モデルカリキュラム－レベル1 を目指して－」をもとに作成

コマタイトルの例については、「付録：IT スキル標準レベル1 コマタイトル一覧」に記載しています。

詳細理解のため参考となる文献（参考文献）	
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

24-3. マナビ DX

マナビ DX は、経済産業省と IPA が運営するデジタル人材育成のためのプラットフォームで、デジタルスキル習得に関する講座を紹介するポータルサイトになっています。デジタルスキルを学んだことのない人から、実践的なデジタル知識・スキルを身につけたい人まで、それぞれに適した講座を紹介してくれます。

紹介されている講座

マナビ DX で紹介されている講座には以下のような特徴があります。

- **厳選された信頼できる講座**

デジタルスキル標準（DSS）などのスキル標準への対応を経産省・IPA が審査し、合格した講座のみが掲載されています。

- **種類が豊富**

講座はさまざまなパートナーから提供されており、デジタルリテラシーや基本的な IT スキルを学ぶための講座から実際のビジネスシーンで役立つ実践的なスキルを習得するための講座まで幅広い講座が掲載されています。

- **受講料支援のある講座も掲載**

講座には無料のものと有料のもの（受講料が必要なもの）がありますが、一部の講座では受講料の補助が受けられるものもあります。

- **リスキリングにも活用**

リスキリングに重要なデジタルスキル習得をはじめる方に最適な初学者向け講座も提供されています。

「マナビ DX」には多くの講座が掲載されています。その一部を紹介します。

- **デジタルリテラシー講座**

- IT パスポート試験対策：IT の基本知識を学ぶための講座
- [データサイエンス](#)入門：データ分析の基礎を学ぶための講座
- [AI](#) 活用入門：人工知能の基本概念とその応用方法を学ぶための講座

- **デジタル実践講座**

- AI データ活用実践コース：Web 開発の基礎から AI 技術の応用までを学ぶ講座
- IT エンジニア総合コース：フロントエンドからバックエンド、さらに AI 技術までを網羅する講座
- AI×IoT エンジニア育成コース：Web 開発、AI、[IoT](#) 技術を統合的に学ぶ講座

- **サイバーセキュリティ関連講座**

- SaaS 担当者のためのセキュリティコース
クラウドサービスを利用する際に必要となる情報セキュリティの基礎知識とクラウドサービスにおけるリスク分析手法を学ぶ講座
- サイバーセキュリティ技術者育成コース
サイバーセキュリティ技術を習得するための実践的な高度技術を基礎から体系的に学ぶ講座
- インターネットセキュリティ技術（実習編）
インターネット上のさまざまな脅威について学習し、組織において必要となるセキュリティ対策技術を、実習を通して習得する講座
- 攻撃手法概論
サイバーセキュリティにおける代表的な攻撃手法の概要とその特徴について学ぶ講座
（[サイバー攻撃](#)からシステムや[情報資産](#)を保護するために、まずは攻撃手法の概要を学びたい方におすすめです。）
- 特定のスキルに特化した講座
 - ゼロから始める AI エンジニア講座セット：AI の知識ゼロから E 資格の取得を目指すセット講座
 - IoT エンジニア育成コース A：Web 開発の基礎から IoT 技術までを学ぶ講座

マナビ DX では、スキル標準のレベル定義をもとに 1～4 のレベルに分けて掲載しています。講座レベルは、検索結果や講座ページで確認することができます。

講座レベルは下の表を確認してください。

マナビ DX の講座レベル

レベル 4	DX 推進スキル標準・ITSS・ITSS+ 一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題を発見と解決をリードするレベル。プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献する。
レベル 3	DX 推進スキル標準・ITSS・ITSS+ 要求された作業をすべて独力で遂行するレベル。専門を持つプロフェッショナルを目指し、必要となる応用的知識・技能を有する。
レベル 2	DX 推進スキル標準・ITSS・ITSS+ 要求された作業について、上位者の指導の下、その一部を独力で遂行するレベル。プロフェッショナルに向けて必要となる基本的知識・技能を有する。
レベル 1	DX リテラシー標準 要求された作業について、上位者の指導を受けて遂行するレベル。プロフェッショナル

ナルに向けて必要となる基本知識・技能を有する。

(出典) マナビ DX「マナビ DX での学び方」をもとに作成

マナビ DX での学び方

Point1 キーワードやカテゴリで検索可能

キーワードや「学習できるスキル」や「目指すロール」、「リテラシー講座」といったあらかじめ定義されたカテゴリから講座を探することができます。

- キーワードから探す
どの画面でも、ヘッダーからキーワードで検索することが可能です。具体的なキーワードや講座名があればここから検索してください。また、トレンドキーワードを集めた「注目ワード」を利用することもできます。
- スキルやロールから探す
トップページの「3つのカテゴリ（リテラシー講座・学習できるスキル・目指すロール）」から講座を絞りこむことができます。これらのカテゴリはデジタルスキル標準に準拠しています。
- マナビ DX オススメから探す
具体的なキーワードやカテゴリが想像できない場合は、マナビ DX オススメの視点から講座を選ぶことも可能です。

Point2 自分の「お気に入り」や「学習プラン」の作成が可能

マナビ DX にログインすると、講座を記録することができます。

- 「お気に入り」への登録
学習してみたい講座、気になる講座があれば、「お気に入り」に登録することが可能です。
- 「学習プラン」による計画的な学習の実現
学習したい講座を見つけたら、「学習プラン」を活用し、計画的な研修受講や受講実績を管理することをお勧めします。「学習プラン」は学習したい講座の登録、学習の進捗、研修の受講実績を管理することができ、計画的、継続的な自己研鑽を実現することができます。

Point3 講座は「デジタルスキル標準（DSS）」と紐付け

「デジタルスキル標準（DSS）」を理解し活用しましょう

マナビ DX に掲載されている講座は、「デジタルスキル標準（DSS）」に紐づけされています。

「デジタルスキル標準（DSS）」を活用し、目指すキャリアや習得したい知識・スキルから次の講座を探し、段階的に学習していくことができます。

- 「デジタルスキル標準（DSS）」にはすべてのビジネスパーソンを対象にデジタル技術を理解して活用するスキル（デジタルリテラシー）をまとめた「DX リテラシー標準（DSS-L）」と、高い専門性を持って組織の中で DX を推進するために必要な役割と知識・スキルをまとめた「DX 推進スキル標準（DSS-P）」があります。
- 「デジタルスキル標準（DSS）」を使って、デジタル社会の中でビジネスパーソンに求められている知識・スキルや企業や組織の DX の推進において必要な人材を理解し、自分に必要とされている知識やスキルを整理しましょう。ビジネスパーソンとして必要な知識や習得すべきスキルを、あるいは自分が目指したい人材像や実際の業務を描きながら、現在の自分の強み、弱みを棚卸し、なりたい自分に必要な知識や習得すべきスキルを整理し、学び続けることで、さらなる自己研鑽につなげることができます。

デジタル人材に関する政策や最新テクノロジー情報を知りましょう

学びの継続はとても重要です。ぜひ、マナビ DX の機能を存分に活用し、「もっと知りたい」「もっとスキルアップしたい」を実現するために、計画的、継続的に学ぶことで、自分自身をますます成長させていきましょう。

Point4 最先端の新技术にも対応

デジタルの分野は新しいテクノロジーが次々と出現、進歩していくため、常に最新情報をキャッチし、継続して学び続けることがとても重要です。学び続けることで、更なる自己研鑽をしていきましょう。

- 受講したい研修が見つかったら、講座詳細から、講座提供事業会社のサイトへ進み、研修を申し込みの上、研修を受講しましょう。

（出典）マナビ DX「マナビ DX での学び方」をもとに作成

One Point

デジタル人材育成に関する支援制度から講座を探す方法

マナビ DX では経済産業省を始め、各省庁におけるデジタル人材育成に関する個人、事業者様向けの支援制度を紹介しています。また、第四次産業革命スキル習得講座（経済産業省）、教育訓練給付制度（厚生労働省）、人材開発支援助成金（厚生労働省）などと連携した講座があります。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp
デジタル人材育成政策のご紹介	https://manabi-dx.ipa.go.jp/gov_assist

第25章. スキルと知識を持った人材育成・人材確保方法

章の目的

第 25 章では、カリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を理解することを目的とします。カリキュラムごとに、実践方法を例示します。

主な達成目標

- 「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること
- 「IT スキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること
- 「デジタルスキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること

25-1. 「プラス・セキュリティ」の実施計画例

セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていける必要があります。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。昨今は AI を使った新しい攻撃手法が増加しており、昔のスキルや知識だけでは十分に対応することは困難です。この章の前半では、「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を解説します。

この章の後半ではリスキリングに有効と考えられるカリキュラムを例にして、リスキリングのための研修実施計画の策定について解説します。現在、AI や自動化などの新しい技術の導入が進んでいます。これによって従来の仕事が変わり、新しいスキルが必要になります。中長期で見れば AI などの新技術の普及によって、一部の職業は消滅し、新しい職業が生まれることになるでしょう。そうした変化の中で、個人が市場で競争力を維持するためには、リスキリングを通じて最新の技術や知識を習得し、変化に対応できる能力を高めることが重要です。リスキリングを成功させるためには、チェンジマインド（変革思考）を持つことが非常に重要です。チェンジマインドとは、変化を受け入れ、柔軟に対応する考え方を意味します。リスキリングには新しい知識やスキルを習得するための柔軟な思考が不可欠です。考え方を柔軟に変え、具体的な目標を設定するとともに、信頼できる教材やカリキュラムを選んで、自分にあった学習方法を見つけることが、リスキリング成功の秘訣だと言ってよいでしょう。この章では関係機関が公表しているカリキュラムを参考に、セキュリティに関する学習方法を例示します。

「プラス・セキュリティ知識補充講座 カリキュラム例」の内容を実施するための手順を例示します。

前提条件

中小企業を対象とし、セキュリティ専門家は社内には存在しない。

1. 目標の明確化

単元の目標と、到達レベルを明確にします。（以下の表は、部課長級向けの第3単元（投資『サイバーセキュリティとリスク対応』）の場合です）

目標
自部署におけるサイバーセキュリティリスクのマネジメントに必要な概念と、具体的なアクションについて理解する。
到達レベル

- 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。
- 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

2. 学習方法の検討

カリキュラム内容を学習するための方法を検討します。例えば以下のようなものが挙げられます。

● 専門家の活用

サイバーセキュリティの専門家や、企業向けにトレーニングサービスを提供する企業を活用して学習します。中小企業に対応できる柔軟なサポートを提供するサービスを優先的に検討することが重要です。例えば、企業のセキュリティ状況に応じたカスタマイズされた研修プログラムを依頼したり、専門家によるワークショップを依頼したりすることが効果的です。

● オンライン学習の活用

無料や低価格で利用できるオンライン学習プラットフォームを使って、従業員がセキュリティの基礎を学べるようにします。例えば、セキュリティに関する基礎コースを受講できるオンライン学習サイト（例：マナビ DX など）があります。従業員が自分のペースで学習できるため、業務の合間を利用して学びやすいことがメリットです。

● 内部研修の実施

外部講師を招かず、社内の IT リテラシー が高い従業員が中心となり、セキュリティの基本を他の従業員に教える研修を行います。例えば、社内の担当者が「パスワードの強化方法」や「メールのフィッシング対策」といった実践的な内容を教えることで、全体のセキュリティ意識を高められます。社内の状況に即した内容で実施できるため、企業全体でスムーズに学習が進む点が特徴です。

詳細理解のため参考となる文献（参考文献）

マナビ DX

<https://manabi-dx.ipa.go.jp>

3. 受講者の準備

受講者によってデジタル・ネットワーク技術、サイバーセキュリティに関する知識に差があると考えられます。以下のような方法によって受講の要否を判断することが大切です。

	方法の種類	概要	利点（○）・欠点（×）
①	セルフチェックに基づく受講者判断	「○○について説明できる」といったチェック項目のリストを提供し、「はい」が一定比率以	○ 動画に比べると準備コストが少なく済む × チェック項目が多くなると受

		上の場合は、当該項目の受講を省略できる。	講者にとって判断に要する負担が増大する
②	理解度テストによる判定	受講者の理解度を確認する4択問題を出題し、一定以上の得点を得た受講者は当該項目の受講を省略できる。	○ 提示した方法の中で、最も厳密な判定が可能 × カリキュラムの冒頭で「得点が低いので要受講」を示すのは受講意欲を下げる恐れがある
③	動画視聴に基づく受講者判断	受講者は次ページに示すシナリオの動画を視聴し、理解度十分（同様の場面で適切な判断が可能）と判断した場合は当該項目の受講を省略できる。	○ 受講者にとっては軽い負担で適切な判断を行うことが可能で利便性に優れる × 動画教材の作成にコストがかかる 事前の目的設定が重要
④	（判断支援手段を提供しない）	各項目を受講するか否かを受講者による判断に委ねてしまう。	○ 判断用教材の準備が不要 × 基礎知識不十分なまま集合講習に参加する受講者が生じる可能性がある

（出典）NISC「プラス・セキュリティ知識補講講座 カリキュラム例」をもとに作成

そのほか、受講の可否を判断する手段として以下のものが挙げられます。

- 事前アンケートの実施

セキュリティ知識レベルを把握するために、セルフチェック形式のアンケートを実施します。このアンケートでは、日常的に利用されるデジタルツールやセキュリティ用語の理解度を確認します。アンケートの結果をもとに、カリキュラムを受講する対象者を決定します。部門のマネジメント層で、実際にセキュリティ対応に関与する可能性のあるメンバーを中心に選びます。

4.カリキュラムの実施

カリキュラム内容の実施方法を例示します。（以下は、部課長級向けの第3単元（投資『サイバーセキュリティとリスク対応』）の場合です）

- オンライン研修の実施

オンデマンド形式で提供される次の事項を学習します。

- サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30分）

➤ 対策における費用と損失の考え方（オンデマンド・30分）

この段階では、サイバー攻撃の基礎やリスク管理の基本概念について学びます。

● 集合講習の実施

集合講習で提供される次の事項を学習します。

➤ リスクマネジメントのケーススタディ（集合講習：30分）

集合形式の講習では、講師が具体的なサイバー攻撃事例を紹介し、効果的なセキュリティ対策を解説します。また、参加者同士でディスカッションを行い、演習を通じて理解を深めます。

● 演習の実施

演習2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60分）

演習では、リスク対応策のシミュレーションを行い、サイバーセキュリティにおける投資の費用対効果を検討します。参加者は自社に最も適したリスク対応策を模索し、チームで発表を行います。

5.結果の評価と報告

カリキュラム実施後に評価と報告を行います。

● 結果のフィードバック

集合講習後、各部門に対して研修の成果をフィードバックします。各部門が現状のセキュリティ対策を見直し、改善点を明確にします。

● 最終報告書の作成

すべての受講者の意見や研修結果を反映した最終報告書を作成し、経営層に提出します。この報告書は、今後のセキュリティ体制の強化に向けた重要な資料となります。

6.ガントチャートの作成

上記の手順を実施するためのガントチャートを作成することで、進捗状況の管理が容易になります。

ステップ	タスク	サブタスク	期間	担当者	備考
ステップ1：カリキュラム目標の確認と調整	1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2日	プロジェクトリーダー	単元の目的と目標を確認
		1.2 経営層との初回ミーティング	1日	プロジェクトリーダー、経営層	経営層との合意形成
		1.3 フィードバックの反映	2日	プロジェクトリーダー	ミーティングの結果を反映

		1.4 最終合意の取得	2日	プロジェクトリーダー	経営層からの最終承認
ステップ2: 外部パートナーの選定	2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3日	人事部、セキュリティ担当	ベンダー候補をリスト化
		2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当	各ベンダーに要件を共有
		2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層	提案内容の評価と比較
		2.4 ベンダーの選定	2日	人事部、経営層	最終決定を行い、承認
		2.5 契約の準備と締結	2日	人事部、法務担当	契約書の準備と締結
ステップ3: 受講者の準備	3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント	セルフチェックリストの作成
		3.2 アンケートの配布	1日	人事部	受講対象者へ配布
		3.3 回収と結果の分析	3日	人事部	アンケート結果を集計し分析
		3.4 受講者リストの確定	1日	人事部、セキュリティ担当	受講者リストを最終確定
ステップ4: カリキュラムの実施	4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント	オンデマンド形式の教材準備
		4.2 学習スケジュールの通知	1日	人事部	受講者にスケジュールを周知
		4.3 受講者の進捗確認	7日	人事部	受講進捗の確認とフォロー
		4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント	オンライン研修を終了
	5. 集合講習の実施	5.1 講師の手配	2日	セキュリティコンサルタント	集合講習を担当する講師を確定
		5.2 集合講習の準備	3日	講師、サポートスタッフ	教材、演習の準備
		5.3 集合講習の実	1日	受講者、講師	集合講習で事例紹介と演

		施			習実施
		5.4 演習の実施	1 日	受講者、講師	投資効果分析やリスク対応策を検討
ステップ 5 : 結果の評価と報告	6. 結果のフィードバックと報告	6.1 フィードバックの整理	3 日	各部門マネージャー	受講者からフィードバックを収集
		6.2 改善提案の作成	3 日	各部門マネージャー	改善提案を作成
		6.3 改善提案の実行計画作成	2 日	各部門マネージャー	提案に基づいたアクションプランを策定
	7. 最終報告書の作成	7.1 報告書の初稿作成	3 日	プロジェクトリーダー	研修結果をもとに報告書を作成
		7.2 報告書のレビュー	2 日	各部門マネージャー、経営層	レビューとフィードバック
		7.3 報告書の最終版作成	2 日	プロジェクトリーダー	最終報告書を経営層に提出

タスク	サブタスク	期間	担当者	2024年2月							
				1 日	2 日	3 日	4 日	5 日	6 日	7 日	8 日
1. カリキュラム目標の確認	1.1 カリキュラム内容の確認	2日	プロジェクトリーダー								
	1.2 経営層との初回ミーティング	1日	プロジェクトリーダー、経営層								
	1.3 フィードバックの反映	2日	プロジェクトリーダー								
	1.4 最終合意の取得	2日	プロジェクトリーダー								

タスク	サブタスク	期間	担当者	2024年2月																
				9日	10日	11日	12日	13日	14日	15日	16日	17日	18日	19日	20日	21日	22日			
2. セキュリティベンダーの選定	2.1 セキュリティベンダーリストの作成	3日	人事部、セキュリティ担当																	
	2.2 ベンダーとの初期打ち合わせ	3日	人事部、セキュリティ担当																	
	2.3 ベンダー提案の評価	4日	人事部、セキュリティ担当、経営層																	
	2.4 ベンダーの選定	2日	人事部、経営層																	
	2.5 契約の準備と締結	2日	人事部、法務担当																	

タスク	サブタスク	期間	担当者	2024年2月							3月
				23日	24日	25日	26日	27日	28日	29日	1日
3. 事前アンケートの実施	3.1 アンケート内容の設計	2日	人事部、セキュリティコンサルタント								
	3.2 アンケートの配布	1日	人事部								
	3.3 回収と結果の分析	3日	人事部								
	3.4 受講者リストの確定	1日	人事部、セキュリティ担当								

タスク	サブタスク	期間	担当者	2024年3月											
				2日	3日	4日	5日	6日	7日	8日	9日	10日	11日	12日	13日
4. オンライン研修の実施	4.1 オンライン教材の準備	4日	セキュリティコンサルタント												
	4.2 学習スケジュールの通知	1日	人事部												
	4.3 受講者の進捗確認	7日	人事部												
	4.4 オンライン研修の完了	2日	受講者、セキュリティコンサルタント												

タスク	サブタスク	期間	担当者	2024年3月							
				16日	17日	18日	19日	20日	21日	22日	23日
5. 集合講習の実施	5.1 講師の手配	2日	セキュリティコンサルタント								
	5.2 集合講習の準備	3日	講師、サポートスタッフ								
	5.3 集合講習の実施	1日	受講者、講師								
	5.4 演習の実施	1日	受講者、講師								

タスク	サブタスク	期間	担当者	2024年3月						
				24日	25日	26日	27日	28日	29日	30日
6. 結果のフィードバックと報告	6.1 フィードバックの整理	3日	各部門マネージャー							
	6.2 改善提案の作成	3日	各部門マネージャー							
	6.3 改善提案の実行計画作成	2日	各部門マネージャー							

タスク	サブタスク	期間	担当者	2024年4月							
				1日	2日	3日	4日	5日	6日	7日	8日
7. 最終報告書の作成	7.1 報告書の初稿作成	3日	プロジェクトリーダー								
	7.2 報告書のレビュー	2日	各部門マネージャー、経営層								
	7.3 報告書の最終版作成	2日	プロジェクトリーダー								

ガントチャート作成後の流れ

以下の 3 つのポイントに焦点を当てることで、ガントチャートを活用したプロジェクト管理が効果的に行え、カリキュラム内容のスムーズな実施につながります。

- 進捗確認とスケジュール管理

プロジェクトが計画通りに進んでいるかを定期的を確認し、スケジュールに遅れが生じた場合には迅速に対策を講じます。

- リソースの効率的な活用と調整

限られたリソースを最大限に活用し、必要に応じて適切に調整することで、プロジェクトのスムーズな進行をサポートします。

- リスクの早期特定と対応策の準備

プロジェクトに潜むリスクをあらかじめ特定し、問題が発生する前に対応策を準備しておくことで、予想しないトラブルにも迅速に対応できる体制を整えます。

25-2. 「リスキリング」「チェンジマインド」の実施計画例

25-2-1. 「IT スキル標準」の実施計画例

IT スキル標準レベル1「IT 入門（2）」をもとに実施計画を作成する手順を説明します。

1. 目標の明確化

学習目標を明確にします。

学習目標

職業人として IT（情報技術）の基本的な知識を活用し、上位者の指導の下、業務の分析やシステム化の支援や情報の活用ができる。

（出典）IPA「IT スキル標準モデルカリキュラム－レベル1を目指して－」をもとに作成

2. 目標達成に必要な作業を洗い出す

カリキュラムの知識項目を確認し、学ぶ必要がある項目を整理します。

	タイトル	学習目標	対応する知識項目 （大分類）－（中分類）
第1回	オリエンテーション、 コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。	● 基礎理論 － 基礎理論 ● 技術要素 － マルチメディア
第2回	プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。	● 基礎理論 － アルゴリズムとプログラミング
第3回	コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。	● コンピュータシステム － ハードウェア ● コンピュータシステム － コンピュータ構成要素
第4回	ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。	● コンピュータシステム － ソフトウェア
第5回	システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。	● コンピュータシステム － システム構成要素
第6回	前半のまとめ	前半の講義のまとめを行う。	-

第 7 回	マルチメディアとヒューマンインタフェース	マルチメディアの種類とヒューマンインタフェースの基本的な用語を説明できる。	● 技術要素 - ヒューマンインタフェース ● 技術要素 - マルチメディア
第 8 回	ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。	● 技術要素 - ネットワーク
第 9 回	ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。	● 技術要素 - ネットワーク
第 10 回	データベースの技術①	データベースのモデル化と正規化の方法を説明できる。	● 技術要素 - データベース
第 11 回	データベースの技術②	データベースの表操作の方法を説明できる。	● 技術要素 - データベース
第 12 回	情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。	● 技術要素 - セキュリティ
第 13 回	情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。	● 技術要素 - セキュリティ
第 14 回	後半のまとめ	後半の講義のまとめを行う。	-
第 15 回	まとめ	これまでの講義内容を総括する。	-

(出典) IPA「IT スキル標準モデルカリキュラムーレベル1を目標してー」をもとに作成

3. 学習内容の詳細化

各回で行う内容を具体的に決めます。例として第 13 回で行う内容は、以下の通りです。

第 13 回 情報セキュリティ対策②（講義 70 分+演習 20 分）	
学習目標	セキュリティ対策に関する基本的な用語を説明できる。
内容	1. 技術的なセキュリティ対策 (1) 個人認証技術の種類と特徴 ● ID、パスワード

	● コールバック ● デジタル署名 ● 生体認証技術 (2) <u>暗号化</u>技術の種類と特徴 ● 公開鍵暗号方式の仕組み ● 秘密鍵暗号方式の仕組み (3) 不正侵入・コンピュータウイルス対策 ● 入退出管理 ● アクセス管理、機密管理 ● <u>ファイアウォール</u>・コンピュータウイルスの種類と対策 (4) 演習問題【セキュリティの種類と対策】 2. そのほかの情報セキュリティ対策 (1) 個人情報の漏えい (2) 情報<u>セキュリティポリシー</u> (3) 責任と権限の明確化 (4) 情報セキュリティマネジメントシステム (ISMS)
研修・教育方法 (予定時間)	講義 70 分 演習 20 分
対応する知識項目	<共通キャリア・<u>フレームワーク</u>の大分類／中分類との対応> 技術要素－セキュリティ

(出典) IPA「IT スキル標準モデルカリキュラム－レベル1 を目指して－」をもとに作成

カリキュラムをもとに、学習内容を具体的にします。

具体的な学習内容（例）

1.技術的なセキュリティ対策

(1) 個人認証技術の種類と特徴

個人認証は、システムやネットワークへのアクセスを管理するための基本的な技術です。以下の主要な技術を説明します。

● ID、パスワード

最も一般的な認証方法。ID で個人を特定し、パスワードで本人確認を行います。ただし、パスワードの漏えいリスクや、短い・単純なパスワードの使用がセキュリティの脆弱性となりがちです。

● コールバック

電話やメッセージを使用して本人確認を行う方法。例えば、ログイン時にワンタイムパスワードを送信し、そのパスワードを使用してログインする方法などが含まれます。二要素認証（2FA）の一部として利用されることも多いです。

- デジタル署名

公開鍵暗号方式を利用して、データの改ざんや成りすましを防ぐ技術。電子的な書類やメールの送信者が本人であることを証明する際に使用されます。

- 生体認証技術

指紋、顔認証、虹彩認証など、生体的な特徴を利用して個人を特定します。高いセキュリティを実現できますが、技術の精度やプライバシー問題が課題となることもあります。

（2）暗号化技術の種類と特徴

情報を保護するために、データの暗号化は重要です。主に以下の2つの暗号化方式があります。

- 公開鍵暗号方式

暗号化と復号に異なる鍵（公開鍵と秘密鍵）を使用する方式です。公開鍵で暗号化されたデータは対応する秘密鍵でのみ復号可能であり、安全な通信に使われます。

- 秘密鍵暗号方式

暗号化と復号に同じ鍵を使用する方式。公開鍵暗号に比べて高速で、VPNやWi-Fiのセキュリティなどに使用されますが、鍵の管理が課題となります。

（3）不正侵入・コンピュータウイルス対策

ネットワークやシステムに対する攻撃を防ぐための対策です。

- 入退出管理

システムや施設への物理的・論理的なアクセスを制限し、許可された者のみがアクセスできるようにする対策です。カードキーや生体認証が使用されます。

- アクセス管理、機密管理

特定の情報にアクセスできるユーザーや権限を設定し、無許可のアクセスを防ぎます。これにより、社内のデータ流出や情報漏えいを防ぎます。

- ファイアウォール

ネットワーク間の不正な通信を防ぐための装置またはソフトウェア。パケットフィルタリングやプロキシ機能などを使用し、外部からの攻撃を防ぎます。

- コンピュータウイルス対策

ウイルス対策ソフトウェアの導入や、定期的なアップデート、メール添付ファイルの検査など、ウイルス感染を防ぐための措置が取られます。

(4) 演習問題【セキュリティの種類と対策】

実際の状況を想定したシナリオを使い、各種セキュリティ対策がどのように適用されるかを検討します。

例：新しいウェブサービスを公開する際、どのような認証・暗号化技術を導入すべきかを考察する問題。

2. そのほかの情報セキュリティ対策

(1) 個人情報の漏えい

個人情報の漏えいリスクに対する対策として、データの暗号化、アクセス権限の制限、適切なバックアップの実施が重要です。また、外部とのデータ共有には必ずセキュリティ対策を講じ、セキュアなチャネルを使用することが推奨されます。

(2) 情報セキュリティポリシー

企業や組織が、情報資産をどのように保護するかを明確に定めた規程やガイドラインを「情報セキュリティポリシー」と呼びます。これにより、従業員全員がセキュリティの重要性を理解し、一貫した対策を講じることができます。

(3) 責任と権限の明確化

セキュリティ対策においては、誰がどのような責任を持ち、どのような権限を持つのかを明確にすることが不可欠です。これにより、インシデント発生時の対応がスムーズに進行し、迅速な問題解決が可能となります。

(4) 情報セキュリティマネジメントシステム (ISMS)

ISMS は、企業や組織がセキュリティ管理をシステム的に行うためのフレームワークです。国際規格である ISO/IEC 27001 に準拠して、リスクの評価、管理、改善を繰り返すことで、継続的なセキュリティ強化を図ります。

4. 学習方法の選定

カリキュラム内容を学習するための方法を検討します。学習方法を例示します。

● オンライン学習（e ラーニングなど）の利用

無料や低価格で利用できるオンライン学習プラットフォームを活用します。例えば、「マナビ DX」などで、以下のような内容を学びます：

- パスワードや生体認証技術、暗号化技術の基礎について解説したレッスン
- 不正アクセス対策やウイルス対策の基本を学べる動画やレッスン

➤ 情報セキュリティポリシーや ISMS の基本をカバーする初心者向けのレッスン

● 実践的な演習を取り入れた社内研修

社内で、実際に手を動かして学べる簡単な演習を実施します。例えば、以下のような内容を取り入れます：

- パスワード管理や二要素認証の設定について、従業員が自分で試すハンズオン研修
- 簡単なファイアウォールの設定やアクセス管理の仕組みを学べる実践的な演習
- セキュリティ対策の演習問題の実施

これらの実施により、従業員がすぐに実務に役立てられるスキルを身につけられます。

● 社内ディスカッションと情報共有

定期的に社内でセキュリティに関する話し合いや情報共有の場を設け、従業員同士で意見交換を行います。例えば以下のような事項を取り上げます。

- 個人情報保護やセキュリティポリシーに関する業務上の注意点や実践方法について
- ISMS をどのように社内で実践するか、基本的な導入手順や活用方法についてディスカッションを行います。学んだ内容を業務にどのように適用できるかを従業員同士で考えることで、実践的な理解を深め、セキュリティ対策を現場で活かせるようになります。

5. 学習の進行と進捗管理

学習を開始し、週次または月次で進捗報告を行います。各セッションの進行状況を確認し、従業員が計画に遅れを取っている場合は、すぐに調整を行います。さらに、定期的なテストや確認を設定し、理解度やスキルの定着度を把握します。

6. フィードバック収集とフォローアップの実施

従業員からのフィードバックを定期的に収集し、内容が難しすぎる、または簡単すぎる場合には、カリキュラムの内容を調整します。さらに、トレーニング終了後も、従業員が学んだことを実際の仕事で活用できているかを確認し、必要に応じて追加のサポートや新しい学習計画を提供します。

25-2-2. 「デジタルスキル標準」の実施計画例

「デジタルスキル標準」は、DX に関する基礎的な知識やスキル・マインドを身につけるための指針としての「DX リテラシー標準」と、DX を推進する人材を育成・採用するための指針としての「DX 推進スキル標準」の2種類で構成されています。

DX リテラシー標準

DX リテラシー標準では、あらゆるビジネスパーソンに求められる知識・スキルが定義されてい

ます。学習項目のうち、「How - セキュリティ」を学ぶための手順を例示します。

1. 学習内容の検討

学習する内容を明確にします。「How - セキュリティ」で定義されている内容は以下の通りです。

How - セキュリティの内容

セキュリティ技術の仕組みと個人がとるべき対策に関する知識を持ち、安心してデータやデジタル技術を利用できる。

- データやデジタル技術に対して徒に不安を感じることなく、適切に利用するためには、情報を守る仕組みを知ることが求められる。
- 企業が用意する環境・対策に加えて、個人もセキュリティ対策を行う必要性和その方法を理解する必要がある。

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

学習項目例は以下の通りです。

学習項目例

- セキュリティの3要素
 - ✓ 機密性
 - ✓ 完全性
 - ✓ 可用性
- セキュリティ技術
 - ✓ 暗号
 - ✓ ワンタイムパスワード
 - ✓ ブロックチェーン
 - ✓ 生体認証
- 情報セキュリティマネジメントシステム (ISMS)
- 個人がとるべきセキュリティ対策
 - ✓ ID やパスワードの管理
 - ✓ アクセス権の設定
 - ✓ 覗き見防止
 - ✓ 添付ファイル付きメールへの警戒
 - ✓ 社外メールアドレスへの警戒

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

学習内容を具体的にします。

具体化した学習内容（例）

セキュリティの3要素

- 機密性
情報を許可された人だけがアクセスできる状態を保つこと。例えば、パスワードや[暗号化](#)によってデータを保護します。
- 完全性
情報が正確で、[改ざん](#)や破壊されていない状態を維持すること。例えば、ハッシュ関数を使ったデータ検証により、データの一貫性を確保します。
- 可用性
情報やシステムに必要なときにアクセスできる状態を維持すること。例えば、サーバの冗長化やデータバックアップにより、障害発生時も業務を継続できるようにします。

セキュリティ技術

- 暗号
暗号は、データを「鍵」を使って別の形に変える技術です。この変えられたデータは、正しい「鍵」を持っている人だけがもとの形に戻せる仕組みです。
- ワンタイムパスワード
一度限り有効な使い捨てのパスワード。時間制限や一回の使用で無効になるため、パスワードが盗まれても再利用されるリスクが低いです。
- ブロックチェーン
取引データを分散型の台帳に記録する技術。ブロックチェーンは変更が困難で、データの透明性と[信頼性](#)を高めるために使用されます。
- 生体認証
ユーザーの身体的特徴（指紋、顔、虹彩など）を使用して本人確認を行う技術。これにより、なりすましのリスクを減らします。
- 情報セキュリティマネジメントシステム（ISMS）
組織が情報セキュリティを計画的に管理・運営するための仕組み。ISO 27001 がその基準として有名で、[リスクアセスメント](#)、セキュリティ方針の策定、従業員の教育などが含まれます。

個人がとるべきセキュリティ対策

- ID やパスワードの管理
複雑なパスワードを使用し、使い回しを避ける。パスワードマネージャーを活用することも推奨されます。

- **アクセス権の設定**
必要最低限のアクセス権限を設定し、不要な権限を持たないようにする。例えば、共有フォルダへのアクセス権限を適切に管理することが重要です。
- **覗き見防止**
公共の場所で作業する際に、画面を覗かれないように注意する。プライバシーフィルターなどの物理的な対策も効果的です。
- **添付ファイル付きメールへの警戒**
信頼できない送信者からの添付ファイルは開かない。特に.exe ファイルやスクリプトファイルは注意が必要です。
- **社外メールアドレスへの警戒**
社外からのメールにはフィッシングや詐欺のリスクが伴うことが多いため、注意深くメールの内容やリンクを確認することが重要です。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html

2. 学習方法の選定

社内研修や、オンライン学習（e ラーニングなど）を利用することも有効です。

3. 学習計画の策定

社内研修を実施するための計画を例示します。

学習計画の例

研修期間と目的

期間：半日～1 日（1 セッションあたり 30 分～1 時間）

目的：基本的なセキュリティ知識を学び、実務でのリスクを軽減できるレベルにする。

研修プログラム例

1 日目：セキュリティの基本

内容：セキュリティの 3 要素（機密性、完全性、可用性）の基本説明。

方法：簡単なプレゼンテーションと事例紹介を活用し、各自が自身の業務におけるセキュリティの問題点を考えます。

2 日目：セキュリティ技術の紹介

内容：暗号化、ワンタイムパスワード、生体認証の基本説明。

方法：専門的な用語を避け、従業員が使い慣れている技術やツールを例に出すことで、日常に

どう活かせるかを具体的に説明します。

3 日目：個人がとるべきセキュリティ対策

内容：パスワード管理、メールの警戒、物理的なセキュリティの基本説明。

方法：従業員が今すぐできる行動に絞り、具体的な行動リストを共有します。例えば、「今日から自分のパスワードを強化する」「メールのリンクをクリックする前に URL を確認する」といった実践的な対策を提案します。

計画策定のポイント

- 実践的かつシンプルな内容にする

研修内容は理論に加えて、実際に業務で活かせる具体的な行動を中心に設計します。複雑な専門用語や技術的な話は避け、従業員がすぐに実践できる対策を説明することが重要です。

例：パスワードを複雑に設定し、パスワード管理ツールを使う方法を教える、メールの不審な点を見分けるチェックリストを提供する。

- 短時間で集中できるセッション構成

研修は 30 分～1 時間と短く区切り、1 回のセッションで 1 つのテーマに集中するように構成します。従業員の負担を減らし、重要な内容を確実に理解してもらうために、セッションごとに焦点を絞ることが大切です。

例：1 回目は「パスワード管理」、2 回目は「不審メールへの対応」といった具合に、テーマを分けて短い時間で進める。

- 実施後のフォローアップを重視

研修が終わった後も、理解度や実践状況を確認する仕組みを取り入れることが重要です。例えば、定期的なチェックリストの確認や簡単なクイズで知識の定着を図ります。

例：研修後に「パスワードを強化しましたか？」などのフォローアップメールや、理解度を測るクイズを実施することで、日常的に意識を高める。

4. 学習の実施

計画をもとに、学習を実施する際のポイントを挙げます。

- 参加者の理解度に合わせた進行

参加者のセキュリティに対する知識の違いを考慮し、初心者にも分かりやすい言葉を使い、ゆっくり進めることが大切です。難しい言葉や専門用語は避けて、具体的な例を使いながら説明しましょう。

例：「パスワード管理がなぜ重要か」を説明する際に、複雑な理論ではなく、「簡単なパスワードは悪意のある人に推測されやすい」という形で、わかりやすく説明します。

- 実際の行動を取り入れる

理論に加えて、実際にやってみる活動を含めることで、参加者が実務にどう活かすかを学べるようにします。実際に手を動かしてみることで、学んだ内容が現実の業務に結びつきやすくなります。

例：「不審なメールをどう判断するか」を学んだ後、実際にその場でメールを確認してもらう時間を作り、すぐに対策を実行する体験をさせます。

5.フィードバックの収集とフォローアップ

研修後の確認・フォローアップ・フィードバックは、参加者の理解度を深め、セキュリティ意識を継続的に高め、次回の研修をより効果的にするために重要です。

ポイントを3つ紹介します。

- 理解度の確認

研修内容がしっかりと理解されているかを確認するため、簡単なテストやクイズを実施します。これにより、参加者がどの程度理解しているか、また補足が必要な部分があるかを把握できます。

例：「今日学んだセキュリティ対策を実際にどのように実施するか」を問う簡単な質問や選択式のテストを実施します。

- フォローアップと定期的な確認

研修が終わった後も、継続してセキュリティ意識を高めるために、定期的に復習資料を送ったり、重要なポイントをリマインドするメールを配信したりします。日常的にセキュリティ意識を保つ仕組みを作ることが大切です。

例：毎月1回「パスワードを更新していますか？」や「不審なメールに注意しましょう」といった確認メールを送ります。また、定期的にセキュリティ対策のチェックリストを共有し、従業員が自主的に対策を実践しているか確認します。

- フィードバックの収集

研修後に参加者からのフィードバックを収集し、研修内容や進行方法についての改善点を把握します。これにより、次回の研修がより効果的なものになります。

例：「研修で学んだことは役に立ちましたか？」「今後、さらに知りたいセキュリティの内容はありますか？」といった簡単なアンケートを実施し、感想や要望を集めます。

DX 推進スキル標準

「人材類型：サイバーセキュリティ」の「サイバーセキュリティマネージャー」の育成の例を紹介します。「サイバーセキュリティマネージャー」に必要なスキルを身につけるための教育・研修の実施計画を例示します。

人材類型	サイバーセキュリティ
ロール	サイバーセキュリティマネージャー
DXの推進において担う責任	顧客価値を拡大するビジネスの企画立案に際して、デジタル活用に伴うサイバーセキュリティリスクを検討・評価するとともに、その影響を抑制するための対策の管理・統制の主導を通じて、顧客価値の高いビジネスへの信頼感向上に貢献する
主な業務	● 新規ビジネスにおけるデジタル活用を通じて生じるサイバーセキュリティ、セーフティ、プライバシー保護に関するリスクを評価する ● リスクとリターンのバランスを踏まえ、サイバーセキュリティリスクの影響を抑制するための戦略や、対策の実施体制を検討する ● サイバーセキュリティリスク抑制のための対策の実施状況の管理や監査を行う ● 事業実施に用いているデジタル環境で発生するサイバーセキュリティインシデントへの対応を行う
必要なスキル（高い実践力と専門性が必要のみ抜粋）	カテゴリ：セキュリティ サブカテゴリ：セキュリティマネジメント スキル項目 ● セキュリティ体制構築・運営 ● セキュリティマネジメント ● インシデント対応と事業継続 ● プライバシー保護

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

スキルの詳細は以下の通りです。

「セキュリティマネジメント」サブカテゴリーの構造
● セキュリティ体制構築・運営 セキュリティ対策を実施する体制の構築とその維持運営（要員の確保・育成を含む）を円滑に行うためのスキル、および組織としてのセキュリティカルチャーを企業内で醸成する活動を行うためのスキル

(出典) IPA「デジタルスキル標準 ver.1.2」をもとに作成

- セキュリティマネジメント
情報、サイバー空間、OT/IoT 環境などのセキュリティマネジメントのプロセスを適切に実施するためのスキル
- インシデント対応と事業継続
各種リスク（サイバー攻撃、過失、内部不正、災害、障害など）がデジタル利活用におけるセキュリティインシデントとして顕在化した際の影響を抑制し、事業継続を可能とするためのスキル
- プライバシー保護
パーソナルデータなどのプライバシー情報の保護に求められる要件の理解とその実践に関するスキル

上記のスキルを身につけるための実施計画を例示します。

1. 現状分析と目標設定

現状分析

従業員の現在のセキュリティ知識とスキルを評価します。簡単なテストやアンケートでセキュリティに関する理解度を測定し、各自の強みや弱みを把握します。

テストの例は以下の通りです。

セキュリティに関する理解度テストの例

セキュリティ体制構築・運営

Q1. セキュリティ体制を効果的に構築し、維持運営するために最も重要な要素は次のうちどれですか？

- セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける
- セキュリティソフトウェアを定期的にアップデートする
- IT 部門の従業員だけでセキュリティ体制を構築し、他の従業員には任せない
- 外部ベンダーにすべてのセキュリティ対策を委託する

答え：「a. セキュリティ体制を継続的に見直し、必要に応じて改善するプロセスを設ける」

解説：セキュリティ体制の構築や運営は、一度設けたら終わりではなく、常にリスクや組織の変化に応じて見直し、改善することが求められます。従業員の育成や全員が参加するセキュリティカルチャーの醸成も重要です。

セキュリティマネジメント

Q2. セキュリティマネジメントのプロセスで、最も重要な「リスクアセスメント」とは何です

か？

- a. セキュリティソフトウェアの更新スケジュールを確認すること
- b. 会社のセキュリティ予算を決定すること
- c. 企業が直面するセキュリティリスクを評価・分析すること
- d. セキュリティインシデントの発生回数を計測すること

答え：「c. 企業が直面するセキュリティリスクを評価・分析すること」

解説：リスクアセスメントは、組織の脅威や脆弱性を特定し、どのようなリスクが最も重大であるかを評価するプロセスです。

インシデント対応と事業継続

Q3. サイバー攻撃が発生した場合に、最初に行うべき対応はどれですか？

- a. 影響を受けたシステムを速やかにオフラインにする
- b. すぐに新しいセキュリティソフトウェアをインストールする
- c. メディアにインシデントを報告する
- d. インシデントの原因を調査するためのチームを編成する

答え：「a. 影響を受けたシステムを速やかにオフラインにする」

解説：サイバー攻撃を受けた場合、被害の拡大を防ぐために、まず影響を受けたシステムを隔離することが重要です。

プライバシー保護

Q4. プライバシー保護の観点から、企業が顧客の個人情報进行处理する際に最も重要な点は何ですか？

- a. データの物理的な保存場所を定期的に変更する
- b. データ処理の目的を明確にし、顧客からの同意を得る
- c. データを自動で削除するソフトウェアを購入する
- d. 顧客にデータ処理の手続きを詳細に説明する

答え：「b. データ処理の目的を明確にし、顧客からの同意を得る」

解説：プライバシー保護法において、データ処理の目的を明示し、事前に顧客の同意を得ることは最も基本的かつ重要な要件です。

スキル習得目標の設定

身につけさせたいスキル（セキュリティ体制構築、セキュリティマネジメント、インシデント対

応、プライバシー保護など）を明確にし、何をいつまでに習得するか具体的な目標を設定します。

目標設定の例

1. セキュリティ体制構築・運営

目標：

3ヶ月以内に、基本的なセキュリティポリシーを策定して社内に共有し、従業員全員が日常業務においてそのポリシーを実践できるようにする。

2. セキュリティマネジメント

目標：

3ヶ月以内に、主要なセキュリティリスクを把握し、それに基づいた簡単なリスク評価（例えば、データバックアップやアクセス権管理）を実施できるようにする。

3. インシデント対応と事業継続

目標：

3ヶ月以内に、インシデント発生時の基本的な対応フロー（インシデントの報告、初期対応、関係者への連絡）を整備し、従業員がそのフローに従って行動できるようにする。

4. プライバシー保護

目標：

3ヶ月以内に、顧客データや個人情報の取り扱いに関する基本的なガイドラインを策定し、従業員がデータ保護の基本的な手順を実践できるようにする。

2. 学習計画の作成

目標を達成するための計画を作成します。

計画作成のポイント

- シンプルで実践的な内容にする（即実践できるスキルを重視）
複雑な理論よりも、日常業務で使えるシンプルなスキルを学ばせます。フィッシング対策やパスワード管理など、すぐに役立つ内容を中心にして、従業員がすぐに行動に移せるようにします。
- 段階的な進行と定期的なフィードバック（進捗を段階的に確認し、小さな成功を積み重ねる）
すべてを一度に学ばせるのではなく、段階ごとに小さな成功体験を積み重ねるプランにします。定期的に進捗を確認し、フィードバックを与えて次のステップに進める形にします。

計画作成の例

1. セキュリティ体制構築・運営

目標：3ヶ月以内に、基本的なセキュリティポリシーを全従業員に共有し、日常業務において

実践できるようにする。

第1週 - 第2週

セキュリティポリシーの作成

インターネット上で公開されている無料のセキュリティポリシーテンプレートを活用し、パスワード管理やフィッシング対策を含むシンプルなポリシーを作成します。

ツール例：NIST や中小企業向けサイバーセキュリティポリシーの無料リソースを利用。

第3週 - 第4週

社内で簡単な説明会を開催

経営者や IT 担当者がリーダーとなり、30 分程度の説明会を開催し、セキュリティポリシーの内容を簡単に説明します。

クイズやディスカッション形式で理解を深めます。

第5週 - 第6週

実践トレーニング

タスク：USB デバイスの管理と紙資料の処理に関する簡単な演習を実施。

内容

- USB デバイスの管理：従業員が USB メモリなどを使用する際、デバイスを適切に取り扱い、安全にデータを移動・管理する方法を実演。
例：外部デバイスを使う際のリスクや、使用後のデバイスの安全な保管方法を学びます。
- 紙資料の取り扱い：紙ベースの情報管理について、重要な資料の廃棄方法（シュレッダーの使用）や、デスクの片付け（クリアデスク）の実践演習を行います。
例：印刷された重要書類をどのように処理すべきかを実際に体験させます。

第7週 - 第12週

簡単な社内チェックとフィードバック

月に1度、従業員がセキュリティポリシーを実践できているか簡単なチェックを行い、必要に応じて改善フィードバックを行います。

2. セキュリティマネジメント

目標：3 ヶ月以内に、主要なセキュリティリスクを把握し、簡単なリスク評価を実施できるようにする。

第1週 - 第2週

主要なリスクのリストアップ

経営者と IT 担当者がリーダーとなり、事業に関連するリスク（データ漏えい、内部不正、機器故障など）をリストアップし、シンプルなリスク評価シートを作成します。

第3週 - 第4週

データバックアップの実施指導

各部門で定期的に重要データのバックアップが行われるように指導し、クラウドストレージを

利用してデータ保護を強化します。

第5週 - 第6週

アクセス権限の簡単な見直し

各部門で使用しているファイルやシステムに対して、必要な人だけがアクセスできるよう、アクセス権限を見直します。特別なシステムがない場合は、共有フォルダの権限設定を調整。

第7週 - 第12週

リスク評価結果の共有

各部門が実施したリスク評価の結果を簡単な報告書としてまとめ、全体会議で共有します。大きなリスクに対する対応策を検討し、全従業員に対策を通知。

3. インシデント対応と事業継続

目標：3ヶ月以内に、インシデント発生時の基本的な対応フローを整備し、従業員が対応できるようにする。

第1週 - 第2週

シンプルなインシデント対応フローを作成

報告から初期対応、上司や関係部署への連絡までのシンプルなフローを作成します。例えば、チャットやメールで報告する際のフォーマットを準備。

第3週 - 第4週

インシデント対応説明会

全従業員に対して、インシデント対応フローの説明会を開催し、実際のシナリオを使って報告の練習を行います。

第5週 - 第6週

インシデント対応シミュレーション

簡単なインシデント（例えば、ウイルス感染やデータ損失）を想定したシミュレーションを実施し、従業員がフローに従って報告・対応できるかを確認します。

第7週 - 第12週

定期的なチェックと改善

週に1度、インシデントが発生した場合の報告フローをチェックし、問題がないかを確認し、必要に応じてフローを改善します。

4. プライバシー保護

目標：3ヶ月以内に、顧客データや個人情報の取り扱いガイドラインを策定し、従業員が実践できるようにする。

第1週 - 第2週

シンプルなガイドライン作成

法令（個人情報保護法）を参照しつつ、データの収集、保存、破棄に関する基本的な手順をガイドラインとして作成。データの最小限の収集や、不要なデータの定期的な削除方法などを明

確にします。

第3週 - 第4週

従業員向けガイドラインの共有

ガイドラインを全従業員に配布し、短い説明会を通じてデータ保護の基本的な考え方を共有します。

第5週 - 第6週

データ保護の実践

従業員が日常業務の中で、顧客データの取り扱いやアクセス権の管理を実際に行えるよう指導し、定期的なデータ監査を行います。

第7週 - 第12週

フォローアップと改善

ガイドラインが遵守されているか、簡単なチェックリストを作成し、各部門で確認します。問題点があればすぐに改善策を検討し、再度周知します。

作成した計画をガントチャートにすることで、進捗管理が容易になったり、スケジュール管理が容易になったりするため、効率的に学習を進めることができます。

「セキュリティ体制構築・運営」のガントチャート作成例

タスク ID	タスク名	担当者	開始日	終了日	前提条件	リソース	依存関係	成果の確認ポイント
1	セキュリティポリシーの作成	IT 部門	2024/1/5	2024/1/17	なし	NIST テンプレート	なし	セキュリティポリシー作成完了
2	セキュリティポリシーのレビューと最終化	IT 部門	2024/1/18	2024/1/19	セキュリティポリシーの作成完了	内部リソース	タスク ID 1	ポリシー最終化
3	社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26	ポリシーがレビューされていること	プレゼンテーション資料、共有スペース	タスク ID 2	説明会準備完了

4	社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2	説明会準備完了	参加者、プレゼンテーション資料	タスク ID 3	説明会開催完了
5	USB デバイス管理演習	IT 部門	2024/2/5	2024/2/9	なし	USB メモリ	なし	演習完了
6	紙資料処理演習	総務部	2024/2/13	2024/2/19	USB デバイス管理演習完了	シュレッター、チェックリスト	タスク ID 5	演習完了
7	セキュリティポリシーの実践状況チェック	IT 部門	2024/2/20	2024/3/4	なし	チェックリスト	なし	ポリシー実践確認完了
8	フィードバックと改善提案の作成	IT 部門	2024/3/5	2024/3/25	チェック完了	フィードバックフォーム	タスク ID 7	改善提案完了

タスク名	担当者	開始日	終了日	2024年1月				2024年2月				2024年3月			
				第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週	第1週	第2週	第3週	第4週
セキュリティポリシーの作成	IT部門	2024/1/5	2024/1/17												
セキュリティポリシーのレビューと最終化	IT部門	2024/1/18	2024/1/19												
社内向けセキュリティポリシー説明会の準備	総務部	2024/1/22	2024/1/26												
社内向けセキュリティポリシーの説明会開催	総務部	2024/1/29	2024/2/2												
USBデバイス管理演習	IT部門	2024/2/5	2024/2/9												
紙資料処理演習	総務部	2024/2/13	2024/2/19												
セキュリティポリシーの実践状況チェック	IT部門	2024/2/20	2024/3/4												
フィードバックと改善提案の作成	IT部門	2024/3/5	2024/3/25												

ガントチャート作成のポイント

- タスクを具体的に分解する
プロジェクト全体を小さな作業単位（タスク）に分け、それぞれが具体的に実行可能な内容にします。
例：「セキュリティポリシー作成」「説明会の準備」など
- 依存関係とスケジュールを設定する
各タスクの実行順序と、前のタスクが完了しないと次に進めない場合の依存関係を明示します。また、各タスクの開始日と終了日を設定し、全体のスケジュール管理ができるようにします。
例：「ポリシー作成が終わってから説明会準備を開始」
- 成果物（完了条件）を明確にする
各タスクの完了を確認するための成果物や基準を設定し、進捗状況を評価しやすくします。
例：「セキュリティポリシーの最終版完成」「説明会が無事に開催された」

これら3つのポイントを押さえることで、WBSがシンプルかつ効果的なものになります。

3. 学習計画の周知と実施準備

- 従業員への周知
作成した学習計画を全従業員に共有し、学習目標、内容、進め方について説明します。従業員

が学習計画の重要性を理解し、積極的に参加できるように動機づけることが大切です。

- **学習環境の整備**

e ラーニングの導入や、教材、トレーニング資料の準備を整えます。もし外部講師や専門家を招く場合は、そのスケジュールを確保しておきます。

- **担当者の配置とサポート体制の構築**

プランの進行を管理する担当者を設定し、従業員の学習をサポートする体制を整えます。質問や問題が発生した際にすぐに対応できる窓口を作ることも重要です。

4.学習の実行

- **スケジュールに従ってトレーニングを進行**

作成したカリキュラムやスケジュールに沿って、トレーニングを開始します。各セッションやモジュールが順調に進んでいるかを確認し、必要に応じて進行を調整します。

- **進捗報告の仕組みの導入**

定期的に学習進捗を確認し、例えば週次または月次の進捗報告会を設けて従業員に学習の進捗状況を報告させることは有効です。これにより、モチベーションを維持し、計画の遅れを早期に発見できます。

5.フィードバックと進捗管理

- **定期的なチェックポイントを設定**

学習プランが順調に進んでいるか確認するために、定期的に学習内容のテストや確認を行います。これにより、理解度の確認と学習の定着を測定できます。

- **従業員からのフィードバック収集**

トレーニングの内容や進め方について、従業員からフィードバックを収集します。もし内容が難しすぎる、もしくは簡単すぎる場合には、カリキュラムの調整を検討します。

6.学習プランの調整

- **進捗に応じたプランの見直し**

進捗状況やフィードバックに基づき、学習プランを柔軟に調整します。例えば、理解が進んでいる分野はスピードアップし、苦手な部分には追加トレーニングを提供するなど、個々の従業員のニーズに合わせた調整が必要です。

- **モチベーション向上施策**

成果が見えにくい段階では、従業員のモチベーションが下がる可能性があります。そのため、小さな成功体験や報酬（例えば、社内での称賛や学習ポイントによるインセンティブ）を設定し、モチベーションを維持します。

7.成果の評価とフィードバック

- 成果の測定とフィードバックの提供

学習が一通り終了したら、最終的なテストや評価を行い、どの程度スキルが習得されたかを確認します。各従業員に対して個別のフィードバックを行い、今後の改善点やさらなる学習の方向性を示します。

- 学習効果の測定

学習による効果がどの程度業務に反映されているかも重要です。例えば、セキュリティインシデントの減少や、従業員のセキュリティ対応能力の向上が確認できれば、学習プランが効果的であったと判断できます。

8.フォローアップと継続学習

- 継続的な学習計画の策定

セキュリティは常に進化しているため、1度の学習プランで終わるのではなく、継続的な学習計画を策定します。例えば、最新のサイバーセキュリティ脅威に対応するための定期的なアップデートや新しいツールの習得を含めた継続学習が必要です。

- 従業員の定着度合いのモニタリング

学習内容が業務の中でどの程度実践されているかをモニタリングします。セキュリティインシデント対応やセキュリティガイドラインの実施状況を確認し、従業員が習得したスキルを日常的に活用しているか否かを把握します。

これらのステップを通じて、作成した学習プランが効果的に実行され、従業員が必要なスキルを確実に習得することができます。特に、進捗管理とフィードバックの提供を徹底し、学習の定着を促すことが成功の鍵です。

編集後記

第9編では、組織としてサイバーセキュリティ対策を実践するためのスキルや知識、そしてそれらを備えた人材の育成について紹介しました。本編では、経営層から現場のマネジメント層に至るまで、それぞれの役割に応じた教育プログラムやカリキュラムの具体例を取り上げ、企業が持続的なセキュリティ体制を築くための実践的な指針を提供しています。特に、デジタル時代において求められるスキル標準や人材育成の重要性を強調し、セキュリティリスクの管理や対応において、適切な判断を行うための知識の習得が不可欠であることを解説しています。

さらに、変化の速いこの領域では、リスクリングの取り組みが重要です。従業員が新たな知識やスキルを継続的に学ぶことで、組織全体のセキュリティ対応力が高まり、急速に進化する脅威に柔軟に対応できるようになります。リスクリングを通じて、個々のスキルをアップデートしながら、組織としても最新のセキュリティ標準に適応できる体制を整えることが、今後の競争力強化につながります。

本編で紹介したカリキュラムや講座は一つの例です。業種、企業規模などによって合わない場合もあります。状況に合わせて内容を取捨選択し、自社にあった教育プログラムを作成していただくことで、より効果的・効率的に人材育成が可能です。紹介したカリキュラムを参考に自社のご状況を踏まえたカリキュラム作成、講座の選定をお勧めします。

本編で学んだ内容を活用し、各自が組織のセキュリティを高めるための一歩を踏み出していただければと思います。

第26章. エグゼクティブサマリー

章の目的

テキストの読者が経営者などに説明するために、テキストの全体要旨や活用ポイントなどを提示することを目的とします。これまでの各章のポイントをまとめて振り返りつつ、テキストを読んだ後に実施していただきたいことや、テキストの活用ポイントについて説明します。それぞれの対策における実施概要を再認識していただきたいと思います。

主な達成目標

- 本テキストの全体要旨、活用ポイントをもとに、組織として実践すべき事項と概要を理解すること

26-1. 全体要旨

本テキストでは、中小企業のセキュリティを担う方々への育成のため、サイバーセキュリティ関連の情報や、実践的なセキュリティ対策について解説してきました。

これまでの各章のポイントをまとめて振り返りつつ、テキストを読んだ後に実施してほしいことや、テキストの活用ポイントについて説明します。それぞれの対策における実施概要を再認識していただきたいと思います。また、具体的な対策を講じるにあたっては、本テキストで参考文献としている資料などを入手し、詳細な内容を把握した上で実施していただきたいと思います。

テキストの概要

第 1 編 サイバーセキュリティを取り巻く背景 【レベル共通】

(第 1 章～第 4 章)

サイバーセキュリティを取り巻く背景として、[デジタル化](#)が進む社会と情報技術（IT）活用の動向を解説し、基本的なサイバーセキュリティ知識や UTM・[EDR](#) の活用を振り返りました。また、サイバーセキュリティの脅威に対処する段階的なアプローチ方法を明確にするとともに、[サイバーセキュリティ戦略](#)に関連する国の方針と関連法令、セキュリティ確保と DX 推進の両立の必要性について解説しました。

第 2 編 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策 【レベル共通】

(第 5 章～第 6 章)

実際のインシデント事例を通して、近年の[サイバー攻撃](#)の傾向や対策などを紹介しました。これからの企業経営で必要な観点となる社会の動向、「守りの IT 投資」や「攻めの IT 投資」などの IT 投資や、経営投資としてのセキュリティ対策の重要性を説明しました。

第 3 編 これからの企業経営に必要な IT 活用とサイバーセキュリティ対策 【レベル共通】

(第 7 章～第 8 章)

[ISMS](#) 認証を前提としたセキュリティ対策における基準を 3 段階にレベル分けし、それぞれのアプローチ手法について解説しました。さらに、ISO/IEC 27000 に記述されている「リスク」、「脅威」、「[脆弱性](#)」、「管理策」といった用語の定義とそれらの関係性、脅威や脆弱性の識別方法を説明しました。

第 4 編 セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施 【レベル 1】

(第 9 章)

実際の[セキュリティインシデント](#)の事例を踏まえ、自社での発生可能性や被害規模を慎重に検討し、対策基準や実施手順を策定していく手法である、Lv.1 クイックアプローチについて解説しました。

第 5 編 各種ガイドラインを参考にした対策の実施 【レベル 2】

(第 10 章)

ガイドラインやひな型など既存の手法を参考にして対策基準や実施手順を策定する手法である、Lv.2 ベースラインアプローチについて解説しました。

第 6 編 ISMS などのフレームワークの種類と活用法の紹介 【レベル 3】

(第 11 章～第 12 章)

サイバーセキュリティ対策における代表的な[フレームワーク](#) (ISMS、[CSF2.0](#)、CPSF など) の概要と、リスクマネジメントや[リスクアセスメント](#)の手法、リスク対応の考え方について説明しました。

第 7 編 ISMS の構築と対策基準の策定と実施手順 【レベル 3】

(第 13 章～第 19 章)

ISMS のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する Lv.3 網羅的アプローチについて説明しました。ISMS の管理策（組織的、人的、物理的、技術的管理策）をもとに、対策基準を策定する手順と、策定した対策基準をもとに具体的な実施手順を策定する方法を説明しました。最後に、内部・外部監査によるセキュリティ対策の有効性評価について解説しました。

第 8 編 具体的な構築・運用の実践 【レベル 3】

(第 20 章～第 21 章)

デジタル・ガバメント推進標準ガイドラインなどが示すサービスシステム構築と運用の工程を参考に、中小企業においても有効な情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明しました。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を解説しました。

第 9 編 組織として実践するためのスキル・知識と人材育成 【レベル共通】

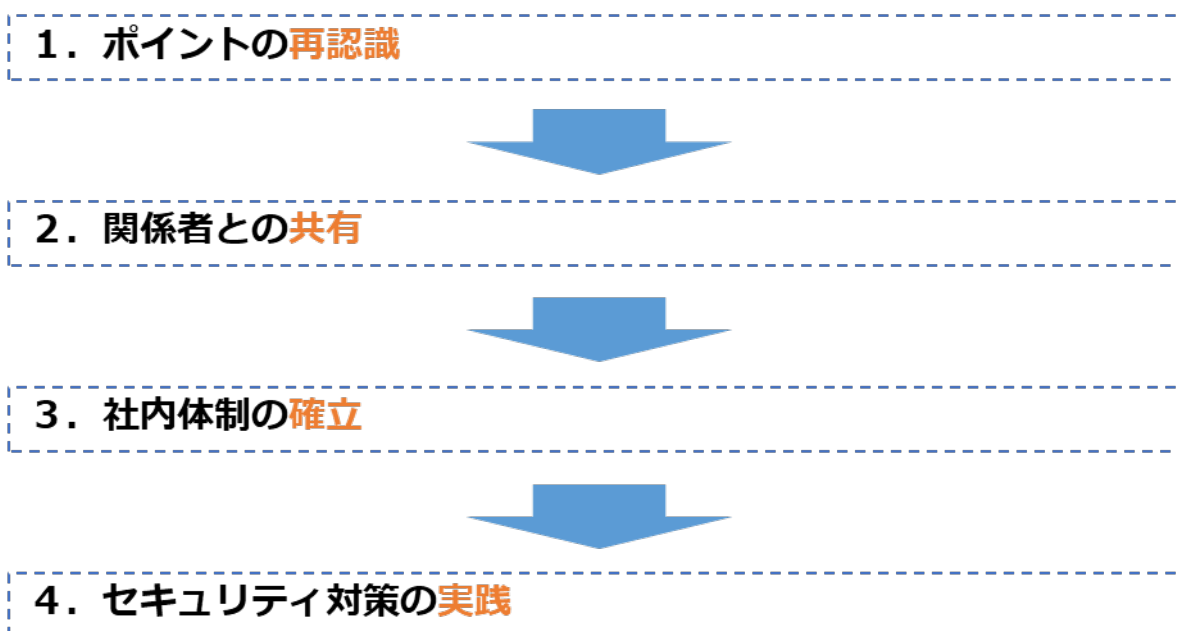
(第 22 章～第 25 章)

各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識、IT およびデジタル人材のスキル、知識の認定制度について解説するとともに、必要な知識やスキルを備えた人材の育成・確保のために、関係機関が公表しているセキュリティ関連のカリキュラムを紹介しました。また紹介したカリキュラムなどを活用して教育・研修計画を作成する方法を解説し

ました。

26-2. テキストの活用ポイント

本テキストを通してセキュリティ対策を実践するために、自組織のレベルに応じて、認識すべき事項を把握した上で、参考となる章を選択した活用法が効果的です。以下のアクションに沿って本テキストを活用してください。



1. ポイントの再認識

「DX の理解からサイバーセキュリティ対策の実践まで」のポイントを再認識します。各章の内容は以下の通りです。

- DX の推進の考え方の把握
- セキュリティ対策の全容の認識
- 自組織でのセキュリティ対策の実施項目の認識
- 自組織としての実践準備

DX の推進の考え方の把握	
第 1 章	技術革新や経済のグローバル化といったビジネス環境の激しい変化に対応し、顧客ニーズに合致した製品・サービスを提供していくためには、DX を推進する必要があること、つまり、データとデジタル技術を活用して、製品やサービスのみならずビジネスモデルや組織、プロセス、企業文化・風土を変革していく必要があることを解説しています。

第3章	国によるデジタル社会に関する方針や政策、 Society5.0 の概要やDX推進における中小企業の優位性とサイバーセキュリティの重要性を解説しています。

セキュリティ対策の全容の認識	
第2章	UTM や EDR の基本的なセキュリティ対策に加え、中小企業向けの「 SECURITY ACTION 」制度や、サイバーセキュリティの脅威に対処するための3つのアプローチ手法について解説しています。
第4章	サイバーセキュリティ戦略 やDX with Cybersecurity の考え方、企業に求められる人材育成とサイバーセキュリティ対策の重要性、サイバーセキュリティに関する法令について解説しています。
第5章	情報セキュリティ白書や情報セキュリティ10大脅威、最近のインシデント事例をもとに、 ランサムウェア やサプライチェーン攻撃などの脅威とその対策や対応方法について解説しています。
第6章	企業が取り組むべき業務効率化やコスト削減といった守りのIT投資と、DX推進に向けた攻めのIT投資の特徴と違い、そして経営者主体のセキュリティ対策の必要性について解説しています。
第7章	セキュリティポリシー の構成（基本方針、対策基準、実施手順・運用規則など）や、企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる3つのアプローチ手法を解説しています。
第8章	リスクマネジメントを理解するために必要となる「リスク」、「 脆弱性 」、「脅威」といった用語の定義と関係性、さらに「脅威」、「脆弱性」の識別方法について解説しています。
第11章	セキュリティ対策を効果的かつ漏れなく行うため、セキュリティ対策に関連する フレームワーク の特徴や概要、そして各フレームワークの要素や要件について解説しています。
第14章	ISO/IEC 27002 に基づく ISMS の管理策の分類と構成、企業が自社のリスクに応じたセキュリティ対策を選定・導入する重要性について解説しています。
第22章	各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要とされるスキルや知識について、体系的に解説しています。
第23章	Di-Lite や情報処理技術者試験、国際セキュリティ資格など、IT およびデ

	デジタル人材のスキル、知識の認定制度と活用方法について解説しています。
自組織でのセキュリティ対策の実施項目の認識	
第 9 章	実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していく、Lv.1 クイックアプローチについて解説しています。
第 10 章	独立行政法人情報処理推進機構（IPA）や総務省などが発行しているガイドラインやひな型など、既存の手法を参考にして対策基準や実施手順を策定していく、Lv.2 ベースラインアプローチについて解説しています。
第 12 章	リスクマネジメントプロセスに沿って、リスク基準の確立、 リスクアセスメント （リスク特定、リスク分析、 リスク評価 ）、リスク対応について手法なども交えながら解説しています。
第 13 章	ISMS のフレームワークに従い、組織全体で適用できるセキュリティ対策基準と手順を整備する Lv.3 網羅的アプローチについて解説しています。
第 20 章	「デジタル・ガバメント推進標準ガイドライン」などが示す政府情報システムの構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を説明しています。
第 24 章	知識やスキルを備えた人材の育成・確保に向けて、具体的な実施計画や実施内容を検討する際の参考となる、セキュリティ関連のカリキュラム内容を解説しています。

自組織としての実践準備	
第 15 章	ISO/IEC 27001:2022 附属書 A の「組織的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 16 章	ISO/IEC 27001:2022 附属書 A の「人的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 17 章	ISO/IEC 27001:2022 附属書 A の「物理的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 18 章	ISO/IEC 27001:2022 附属書 A の「技術的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説して

	います。
第 19 章	ルールの形骸化を防ぎ、目的達成に向けた対策を継続的に改善するために、組織内のルールや手順が適切に守られているかを確認する 内部監査 、第三者による客観的な視点から評価する外部監査について解説しています。
第 21 章	「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを、EC サイトを例にとって解説しています。
第 25 章	関係機関が公表しているカリキュラムや指針などを活用し、チェンジマインド、リスクリングも含めた教育・研修の実施内容および実施計画を作成する手順を解説しています。

2. 関係者との共有

経営者を含めた関係者と、再認識したポイントを共有します。「第 10 編.全体総括」をエグゼクティブサマリーとして活用してください。重要な点を理解し、経営者および他関係者と共有します。

3. 社内体制の確立

経営者のリーダーシップによって、サイバーセキュリティ対策のための社内体制を確立します。知識やスキルを備えた人材の育成・確保をします。人材育成・確保のために、関係機関が公表しているセキュリティ関連のカリキュラムなどを活用し、プラス・セキュリティやチェンジマインド、リスクリングも含めた教育・研修の実施計画および実施内容を作成し、実践します。

経営層をはじめ、法務や広報といった、IT やセキュリティに関する専門知識や業務経験を有していない人材には、プラス・セキュリティ（自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること）が重要です。

実践にあたっては、関係機関が提供している資料を参考にしてください。

人材育成の際に参考となる指針・カリキュラム

DX リテラシー標準	ビジネスパーソン全体が DX に関する基礎的な知識やスキル・マインドを身につけるための指針 ※DX を利用する立場の方向け
DX 推進スキル標準	企業が DX を推進する専門性を持った人材を確保・育成するための指針

	※DX を推進する立場の方向け
プラス・セキュリティ知識補充講座 カリキュラム例	NISC が経営層や DX 推進管理職向けに提供するプログラム。セキュリティ専門家との協働に必要な知識を補充することを目的としています。
IT スキル標準モデルカリキュラム 【IT スキル標準 V3（レベル 1）】	職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラム

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver. 1.2	https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/20240708-p-1.pdf
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

4. セキュリティ対策の実践

具体的なアクションを起こして、サイバーセキュリティ対策を実践します。情報システムの導入（企画から要件定義、調達、設計・開発、運用保守）の際は、以下の資料などを参考にセキュリティ機能を実装します。

- Security by Design
- 「第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）」
- 「第 21 章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施」

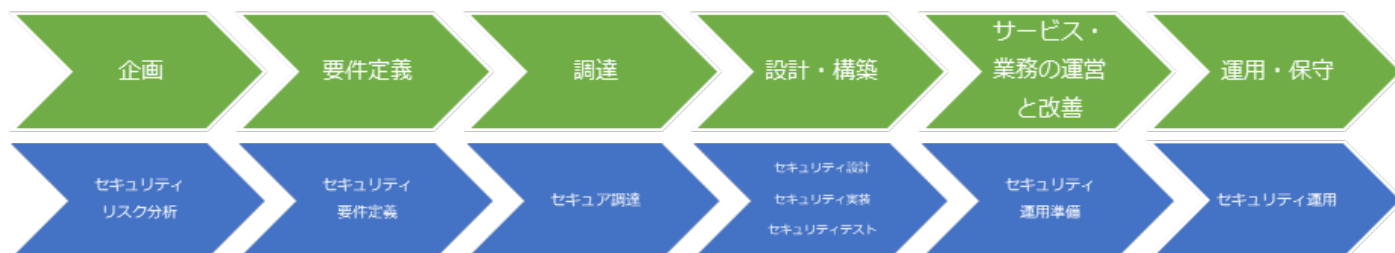


図 103. IT 導入プロセスにおけるセキュリティ対策の実施タイミング

詳細理解のため参考となる文献（参考文献）	
セキュリティ・バイ・デザイン導入指南書	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

第27章. 各章のポイント

章の目的

テキストの読者が各章の内容を実務に活用できるように、各章のポイントを整理し、具体的な知識やスキルを振り返ることを目的とします。これまで学んだ内容を体系的に再確認し、各章が提示するセキュリティ対策の実施方法を明確にすることで、テキストをもとにした実践的な取組を推進できるようにします。

主な達成目標

- 各章ごとに重要なポイントを再確認し、理解すること

27-1. 第 1 章. デジタル時代の社会と IT 情勢

1-1. デジタル時代の社会変革と IT 情勢の関係性

章の目的

第 1 章では、現代社会の IT に関する情勢を学ぶことを目的とします。また、日本が [Society5.0](#) の実現を目指す中、企業がビジネスを発展させるために DX を推進していく重要性を明確にすることを目的とします。

主な達成目標

□ IT に関する社会の動向を把握し、Society5.0 と DX の関係性を理解すること

主なキーワード

Society5.0、DX、生成 AI

要旨

1 章の全体概要

1 章では、技術革新や経済のグローバル化といったビジネス環境の激しい変化に対応し、顧客ニーズに合致した製品・サービスを提供していくためには、DX を推進する必要があること、つまり、データとデジタル技術を活用して、製品やサービスのみならずビジネスモデルや組織、プロセス、企業文化・風土を変革していく必要があることを解説しています。

また、生成 AI は、データ解析を通じて新たなコンテンツを生成し、業務効率化に役立ちますが、[サイバー攻撃](#)に悪用される可能性もあります。生成 AI を利用する際には、機密情報の漏えい防止やセキュリティ意識の向上が重要です。

1-1. デジタル時代の社会変革と IT 情勢の関係性

- 社会の現状と今後の動向（Society5.0）
- DX とは
- 生成 AI とは

訴求ポイント

章を通した気づき・学び

企業や組織は、社会の動向に関する情報を常に収集することが大切です。また、ビジネス環境

の激しい変化に対応するために DX を推進し、デジタル社会に適したビジネスモデル、組織、企業文化に変革していくことが必要です。

生成 AI はさまざまな業務において実用的に活用できるレベルに進化しており、生成 AI を活用することによって、多くの業務プロセスを効率化できます。パブリックな（共同利用型の）生成 AI に送信した情報は、開発者に見られたり学習データとして使用されたりして情報漏えいのリスクがあります。機密情報は入力しないよう注意が必要です。

認識していただきたい実施概要

- 中小企業は、大企業と比べて人手や予算などの企業リソースが限定されており、ビジネス環境の激しい変化に対応するためには、DX を推進し新たなサービスを創造し、ビジネスを発展させることが重要です。
- データやデジタル技術を活用するためには、最新技術の知識、最新技術に精通した人材が必要です。安全にデータやデジタル技術を活用するために、セキュリティ対策を適切に行うことが重要です。
- 生成 AI は業務効率化に役立ちますが、パブリックな（共同利用型の）生成 AI には情報漏えいのリスクもあります。情報漏えいのリスクがある場合には、機密情報を入力しないように活用することが重要です。

詳細理解のため参考となる文献（参考文献）

デジタルガバナンス・コード	https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html
Society5.0	https://www8.cao.go.jp/cstp/society5_0

27-2. 第2章. サイバーセキュリティの基礎知識

2-1. 導入済みと想定するセキュリティ対策機能

2-2. SECURITY ACTION（セキュリティ対策自己宣言）

2-3. サイバーセキュリティアプローチ方法

章の目的

第2章では、サイバーセキュリティの基本的な知識や対策などについて振り返りつつ、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を明確にすることを目的とします。

主な達成目標

- ❑ UTM、EDR の機能を再確認すること
- ❑ 企業が自ら実施できる基本的なセキュリティ対策を再確認すること
- ❑ リスクと活用可能なリソースを考慮した脅威への対処方法を理解すること

主なキーワード

UTM（Unified Threat Management）、EDR（Endpoint Detection and Response）、
SECURITY ACTION

要旨

2章の全体概要

2章では、UTM や EDR の機能など、基本的なセキュリティ対策について解説しています。

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度である「SECURITY ACTION」が推奨されています。「SECURITY ACTION」では、「情報セキュリティ5か条」に取り組んだり、「情報セキュリティ自社診断」を実施したり「情報セキュリティ基本方針」を策定したりします。また、サイバーセキュリティの脅威に対処するためのアプローチ手法「Lv.1 クイックアプローチ」、「Lv.2 ベースラインアプローチ」、「Lv.3 網羅的アプローチ」を解説しています。

2-1. 導入済みと想定するセキュリティ対策機能

UTM、EDR の機能について振り返ります。

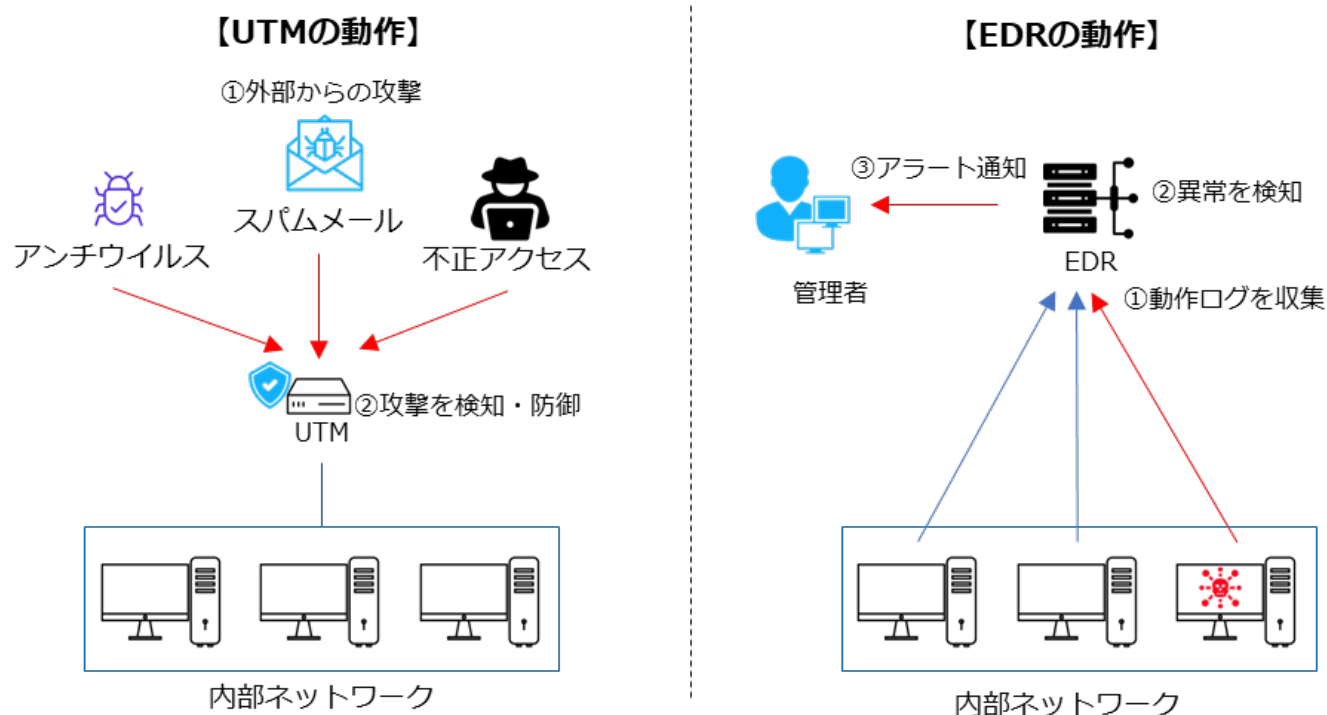


図 104. UTM、EDR の概要図

2-2. SECURITY ACTION（セキュリティ対策自己宣言）

「SECURITY ACTION」に取り組むことで、一つ星・二つ星を宣言でき、従業員のセキュリティに対する意識や対外的な信頼の向上につながります。一つ星・二つ星を宣言するには、次の事項に取り組む必要があります。

- 情報セキュリティ 5 か条
- 情報セキュリティ自社診断
- 情報セキュリティ基本方針

2-3. サイバーセキュリティアプローチ方法

サイバーセキュリティの脅威に対処するアプローチ方法には複数の方法があります。それぞれメリット・デメリットがあるので、自社が直面しているリスク状況および活用できるリソースを考慮し、最適なアプローチ手法を選択するようにしてください。

- Lv.1 クイックアプローチ
- Lv.2 ベースラインアプローチ
- Lv.3 網羅的アプローチ

訴求ポイント

章を通した気づき・学び

セキュリティ対策をはじめると、SECURITY ACTION に取り組み、従業員の意識を高め、対外的な信頼を向上させることが大切です。

認識していただきたい実施概要

- 中小企業が情報セキュリティ対策に取り組むことの宣言として「SECURITY ACTION」という制度があり、従業員の意識を高め、対外的な信頼を向上させるために有効であること。
- サイバーセキュリティの脅威に対処するためには、効果的な 3 種類のアプローチがあること。

詳細理解のため参考となる文献（参考文献）	
SECURITY ACTION セキュリティ対策自己宣言	https://www.ipa.go.jp/security/security-action/
情報セキュリティ 5 か条	https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf
5 分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/guide/sme/5minutes.html
情報セキュリティ基本方針（サンプル）	https://www.ipa.go.jp/security/sme/f55m8k0000001wbv-att/000072146.docx

27-3. 第 3 章. デジタル社会の方向性と実現に向けた国の方針

3-1. 国の基本方針および実施計画の概要

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

章の目的

第 3 章では、政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶことを目的とします。

主な達成目標

- 国の基本方針にデジタルがどのように影響を与えており、それによりどのような社会を目指しているかを理解すること
- デジタル社会におけるセキュリティ対策の重要性を理解すること

主なキーワード

デジタル社会、デジタルトランスフォーメーション（DX）、DX の推進、[サプライチェーン](#)

要旨

3 章の全体概要

3 章では、国によるデジタル社会に関する方針や政策、デジタル分野の取組におけるサイバーセキュリティの位置づけについて解説しています。政府が目指しているデジタル社会として [Society5.0](#) を紹介し、DX 推進における中小企業の優位性について事例を交えて説明しています。

3-1. 国の基本方針および実施計画の要約

IT・セキュリティ関連の施策は、国の方針の 1 つである「経済財政運営と改革の基本方針」に沿った形で実施計画が策定されています。令和 6 年度の方針における IT 戦略に係る施策として「(さまざまな分野における) DX の推進」、「デジタル・ガバメントの強化」、「サイバーセキュリティの強化」があります。

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

政府は「経済財政運営と改革の基本方針」に基づき「デジタル社会の実現に向けた重点計画」

を閣議決定しています。重点計画には、日本がデジタル社会を実現していくための政府の取組として、7つの戦略的な政策が掲げられています。この4番目が「サイバーセキュリティなどの安全・安心の確保」となっています。

デジタル社会を実現していくための7つの戦略的な政策

1. デジタル社会の実現に向けた構造改革
2. デジタル田園都市国家構想の実現
3. 国際戦略の推進
4. サイバーセキュリティなどの安全・安心の確保
5. 急速な [AI](#) の進歩・普及を踏まえた対応
6. 包括的データ戦略の推進と今後の取組
7. Web3.0 の推進

重点計画における、各分野における基本的な施策の4番目「産業の[デジタル化](#)」では「中小企業のDX 推進」や「中小企業のデジタル化の支援」が盛り込まれています。

各分野における基本的な施策

1. 国民に対する行政サービスのデジタル化
2. 安全・安心で便利な暮らしのデジタル化
3. アクセシビリティの確保
4. 産業のデジタル化
5. デジタル社会を支えるシステム・技術
6. デジタル社会のライフスタイル・人材

また、政府が提唱している Society5.0 と DX の推進についても解説しました。

● Society5.0

Society5.0 では、[IoT](#) ですべての人とモノがつながり、知識や情報を共有することによって、これまでにない新たな価値を生み出すとともに、社会が抱えるさまざまな課題を解決の方向に導きます。一方で、Society5.0 におけるサイバー空間の急激な拡大は、[サイバー攻撃](#)の対象が増えることを示しています。サイバー空間とフィジカル空間の相互作用により、サイバー攻撃がフィジカル空間にも影響を及ぼす可能性が高まります。

● DX の推進

DX の推進における中小企業の優位性について説明しています。中小企業の中には、DX を推進し、売上高を5倍、利益を50倍に増加させた企業が存在します。中小企業ならではの優位性を理解し積極的にDXに取り組むことで、大きく成長できる可能性があります。

中小企業が DX 推進における優位な点

参考情報が豊富

DX を既に手掛けている中小企業や、DX を順調に進めている企業のやり方を参考にすることができる

環境が整備されている

先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取り組むことができる

環境の変化に素早く対応しやすい

経営者が即断即決し、新しい取り組みに臨みやすい利点がある。そのため、変革のスピードにおいて優位性を持つことができる

訴求ポイント

章を通した気づき・学び

デジタルの活用が進むとともに、サイバー攻撃などのサイバーセキュリティのリスクも高まっています。自社のデジタル技術の活用を進めつつ、サイバーセキュリティ対策に必要な知識・スキルを身につけた人材を育成・確保することが必要です。

認識していただきたい実施概要

- 政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶこと。
- 中小企業ならではの優位性を理解し、積極的に DX に取り組むことが組織を成長させるために重要であること。

詳細理解のため参考となる文献（参考文献）	
経済財政運営と改革の基本方針 2024	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html
デジタル社会の実現に向けた重点計画	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
Society5.0	https://www8.cao.go.jp/cstp/society5_0
中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

27-4. 第 4 章. サイバーセキュリティ戦略および関連法令

4-1. NISC : サイバーセキュリティ戦略

4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立

4-3. 関連法令

章の目的

第 4 章は、[NISC](#) による[サイバーセキュリティ戦略](#)を通じて、DX とサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法と GDPR について説明します。

主な達成目標

- ❑ 日本におけるサイバーセキュリティに関する方針や施策について理解すること
- ❑ サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること
- ❑ 個人情報関連の法令を理解すること

主なキーワード

サイバーセキュリティ戦略、DX with Cybersecurity、個人情報保護

要旨

4 章の全体概要

4 章では、サイバーセキュリティについては、NISC の「サイバーセキュリティ戦略」を紹介するとともに、DX with Cybersecurity の考え方について解説しています。デジタルの活用が進むとともに、サイバーセキュリティのリスクも高まっています。企業はデジタル技術の活用や DX を進めつつ、必要な知識・スキルを身につけた人材を育成・確保するとともに、適切なサイバーセキュリティ対策を実施することが重要です。

また、個人情報保護法や GDPR（EU 一般データ保護規則）といったサイバーセキュリティに関連する法令を紹介しています。

4-1. NISC : サイバーセキュリティ戦略

サイバーセキュリティ戦略

国家レベルでサイバーセキュリティの確保に取り組むための基本的な方針や目標を定めた「サイバーセキュリティ戦略」について全体概要と、中小企業に関連する内容について説明していま

す。

サイバーセキュリティ 2024

サイバーセキュリティ基本法が定める3つの政策目的と、サイバーセキュリティ戦略の3つの施策推進の方向性に従って整理された「サイバーセキュリティ 2024」について説明しています。

4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立

企業経営のためのサイバーセキュリティの考え方

サイバーセキュリティ対策を行うにあたって、基本的認識や留意事項を理解し、自社の現状のIT活用状況や、セキュリティ対策の取組レベルに応じた対策を行うことが大切です。

DX with Cybersecurity

社会経済のデジタル化が進む中、DXとサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が不可欠になっています。中小企業がDX with Cybersecurityを推進するにあたり、人材やスキル不足などさまざまな課題が存在しています。これらの課題に対する対策として、「デジタルスキル標準（DSS）」、「プラス・セキュリティ」について説明しています。

4-3. 関連法令

個人情報保護法

個人情報保護法は、インターネットの普及や情報技術の進歩などを背景として、個人の権利や利益を守ることを目的として制定された法律です。消費者や取引先から預かっている個人情報を適切に取扱うことは、企業の権利や利益を守ることにつながる非常に重要な取組となります。

GDPR（EU 一般データ保護規則）

GDPRとは、個人データの保護とプライバシーの権利を強化するために、欧州連合（EU）加盟国に適用される重要な法令です。EUで活動する企業だけでなく、EU加盟国の居住者の個人データを取扱う企業は、企業規模に関係なく、GDPRが適用されるため、GDPRを理解し遵守することが必要になります。

訴求ポイント

章を通した気づき・学び

日本政府が打ち出しているサイバーセキュリティ戦略を理解し、関連する知識やスキルを身に

つけることが大切です。

認識していただきたい実施概要

- サイバーセキュリティ戦略によって、国家レベルでのサイバーセキュリティの確保に取り組む方針や目標が定められていることを理解すること。
- サイバーセキュリティ対策にかかる支出をやむを得ない費用とするのではなく、経営のために必要な投資と位置づけ、自発的にサイバーセキュリティ対策に取り組むことが重要であること。
- DX の推進と並行してサイバーセキュリティへの対策が求められている状況の中、必ずしも IT やセキュリティに関する専門知識や業務経験を有していない者も、自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること（プラス・セキュリティ）が重要であること。
- サイバーセキュリティに関連する法令として個人情報保護法や GDPR があり、個人情報はセキュリティレベルの高い情報として適切に取扱うべき情報であること。

詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ	https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
サイバーセキュリティ 2024	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/curriculum/
サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0	https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook_2.pdf
中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
企業経営のためのサイバーセキュリティの考え方の策定について	https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

27-5. 第 5 章. 事例を知る：重大なインシデント発生から課題解決まで

5-1. 情報セキュリティの概況

5-2. 重大インシデント事例から学ぶ課題解決

5-3. 実際の被害事例から見るケーススタディー

章の目的

第 5 章では、近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対するセキュリティ対策や、実際に被害にあった際の対応方法について学ぶことを目的とします。

主な達成目標

- 近年のサイバー攻撃の傾向や手法を理解すること
- 実際の被害事例を通して脅威に対するセキュリティ対策や予防方法を理解すること
- 脅威の検知から、復旧・再発防止処置までの流れを理解すること

主なキーワード

情報セキュリティ白書、情報セキュリティ 10 大脅威、ランサムウェア、サプライチェーン攻撃、テレワーク、脅威、インシデント、サイバー被害

要旨

5 章の全体概要

5 章では情報セキュリティ白書、情報セキュリティ 10 大脅威、最近のインシデント事例をもとに脅威事例を紹介し、脅威への対策や対応方法を説明しています。中でも、ランサムウェアやサプライチェーン攻撃は特に深刻な問題となっています。これらの攻撃は、自社の業務だけでなく取引先からの信用にも悪影響を及ぼす可能性があることに注意する必要があります。近年の攻撃は企業の規模に関係なく行われるため、中小企業にとっても、セキュリティ対策は不可欠なものになっています。

5-1. 情報セキュリティの概況

「情報セキュリティ白書」や「情報セキュリティ 10 大脅威」を用いて、最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握し、適切な予防策や対策を講じることが大切です。

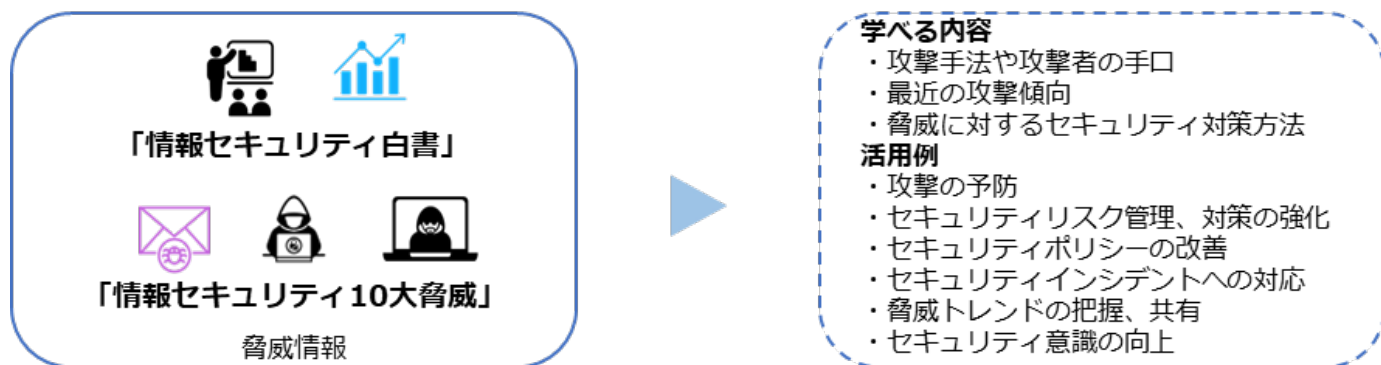


図 105. 情報セキュリティ白書・情報セキュリティ 10 大脅威の活用方法

5-2. 重大インシデント事例から学ぶ課題解決

脅威に対する対応策の策定や、現在使用しているリスク戦略の改善、セキュリティ意識を向上させるには事例を学ぶ方法が有効です。[IoT](#) デバイスへの攻撃、[サプライチェーン](#)を介した[標的型メール攻撃](#)、テレワーク環境での情報漏えい、ランサムウェアへの感染など、過去に発生したさまざまなインシデント事例を紹介しているので、何がうまく行かなかったのか、どのような手段が用いられたのか、どのような脆弱性が攻撃の対象となったのかなどが理解できます。

5-3. 実際の被害事例から見るケーススタディー

実践的な問題解決に役立つスキルを養うため、[不正アクセス](#)やランサムウェアのインシデント事例を通じて、被害が起きた原因の分析内容、効果的なセキュリティ対策や[ベストプラクティス](#)を紹介しています。

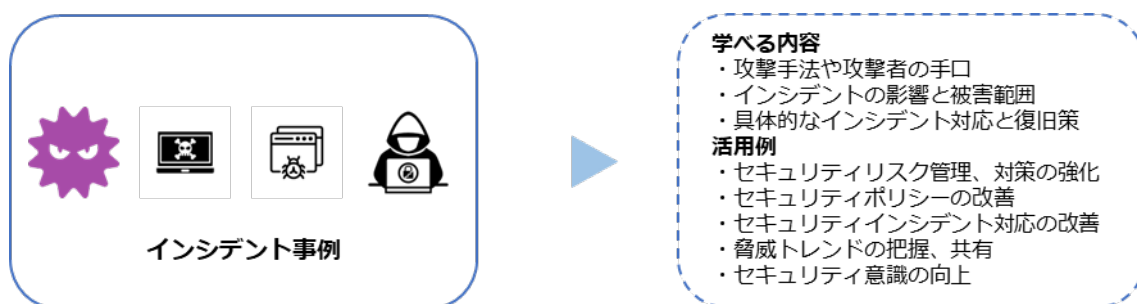


図 106. インシデント事例を通じて学べる内容

訴求ポイント

章を通した気づき・学び

最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握することによって、適切な予防策や対策を講じることが可能になります。また、インシデント事例を学ぶことに

よってセキュリティ意識を高めることもできます。

認識していただきたい実施概要	
● 情報セキュリティ白書や情報セキュリティ 10 大脅威を活用することによって、最新の脆弱性や脅威情報、攻撃の傾向や手法からセキュリティリスクを把握し、適切な予防策や対策を講じることができます。 ● 過去のインシデント事例から対策方法を学ぶことによって、脅威に対する対応策の策定や、現在使用しているリスク戦略の改善、セキュリティ意識の向上、今後起こり得るインシデントに対して適切な対応をすることができます。	

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ白書 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/10threats2024.html

27-6. 第6章. 企業経営で重要となる IT 投資と投資としてのサイバーセキュリティ対策

6-1. これからの企業経営に必要な観点：社会の動向

6-2. 守りの IT 投資と攻めの IT 投資

6-3. 経営投資としてのサイバーセキュリティ対策

章の目的

第6章では、これからの企業経営に必要な観点として、社会の動向、「守りの IT 投資」や「攻めの IT 投資」などの IT 投資について学ぶことを目的とします。また、経営投資としてのセキュリティ対策の重要性を明確にすることを目的とします。

主な達成目標

- 社会の動向を把握し、現実社会とサイバー空間のつながりを理解すること
- IT 投資としての「守りの IT 投資」と「攻めの IT 投資」を理解すること
- 経営投資としてのセキュリティ対策の重要性を理解すること

主なキーワード

守りの IT 投資、攻めの IT 投資

要旨

6 章の全体概要

6章では、社会の動向を踏まえ、企業がセキュリティ対策と同時に進めるべき IT 活用について説明しています。従来の業務効率化やコスト削減といった「守りの IT 投資」と、DX に向けた「攻めの IT 投資」の違いやそれぞれの特徴、主要なデジタル技術の活用方法について簡潔に紹介しています。特に日本企業には「攻めの IT 投資」が不足しており、DX の推進を通じて競争力を強化することが必要だと言われています。

DX 推進と同時に、適切なセキュリティ対策をとる必要があることを鑑み、経営者主体のサイバーセキュリティ対策の必要性とその要点についても解説しています。

6-1. これからの企業経営に必要な観点：社会の動向

社会の動向や、現実社会とサイバー空間のつながり、IT 活用における課題を説明しています。

現実社会とサイバー空間のつながり

個人のインターネット利用率は 1997 年の 9.2% から 2022 年には 84.9% まで上昇し、情報入手やオンラインショッピング、SNS による情報共有が日常化しています。政府は、サイバー空間とフィジカル空間の融合による新しい社会モデルとして [Society5.0](#) を提唱しており、企業は生産性向上や課題解決のために現実空間とサイバー空間をつなぐ CPS（サイバーフィジカルシステム）や [IoT](#) の活用が不可欠となってきました。

IT 活用における課題

日本社会がデジタル化で後れをとった理由は次の 6 つです。

我が国がデジタル化で後れをとった 6 つの理由

1. [ICT](#) 投資の低迷
2. 業務改革等を伴わない ICT 投資
3. ICT 人材の不足・偏在
4. 過去の成功体験
5. デジタル化への不安感・抵抗感
6. デジタルリテラシーが十分ではない

6-2. 守りの IT 投資と攻めの IT 投資

守りの IT 投資と攻めの IT 投資

「攻めの IT 投資」では、IT を活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規市場の創出、収益拡大、販売力のアップを目指します。一方、「守りの IT 投資」では、IT による業務の効率化やコスト削減を目指します。この違いを意識し、「守りの IT 投資」と「攻めの IT 投資」のバランスをとることが大切です。

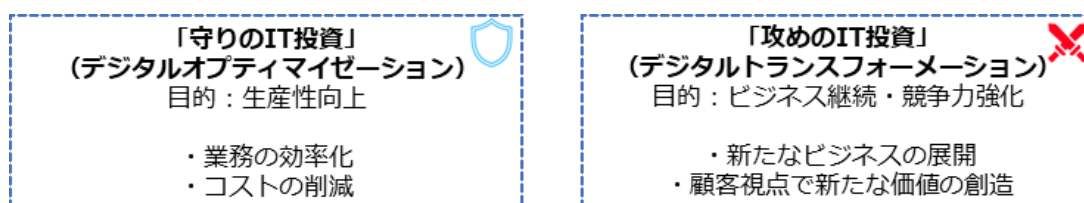


図 107. 守りの IT 投資・攻めの IT 投資

次世代技術を活用したビジネス展開

自社の将来のあるべき姿（将来のビジョン）の実現に必要な課題を明確にし、その課題を解決する必要がありますが、それに役立つのがデジタル技術の活用です。最近では、生成 [AI](#)、IoT、クラウドサービス、チャットボットなどの新しい技術がビジネスで活用されるようになってきて

おり、こうした新しい技術を含めたさまざまな技術やツールをうまく活用していくことが求められています。6章ではデジタル技術の活用成功した企業の例を紹介しています。

6-3. 経営投資としてのサイバーセキュリティ対策

DX 推進と並行してサイバーセキュリティの確保に取り組むことが重要です。サイバーセキュリティ対策をおろそかにすれば、[サイバー攻撃](#)の標的となり、経営を揺るがすような被害にあう可能性があります。サイバーセキュリティ対策には経営判断が必要になるため、経営者がリーダーシップを発揮して対策を進める必要があります。経営者が重視すべきポイントは、次の3つです。

- | |
|---|
| ポイント①：ビジネスの継続・発展には IT の活用が不可欠
ポイント②：IT の活用にはサイバー攻撃への対策が必要
ポイント③：サイバーセキュリティ対策は経営者が自ら実行 |
|---|

訴求ポイント

章を通した気づき・学び

変化の激しい現代社会でビジネスを継続していくためには、従来の IT を活用して業務効率化や生産を向上させることだけでなく、データやデジタル技術を活用して、顧客視点で新たな価値を創出する、DX を推進していくことが求められています。しかし、データやデジタル技術を活用する際に、サイバーセキュリティ対策を行わなければ、サイバー攻撃の標的となり、経営を揺るがすような被害を被ってしまう可能性があります。このような被害を受けないためにも、DX の推進と並行してサイバーセキュリティの確保に取り組むことが不可欠です。このサイバーセキュリティ対策は、経営者自らが主体となって指揮をする必要があります。

認識していただきたい実施概要

- 現実社会とサイバー空間のつながりや、Society5.0 などといった社会の動向を把握することが、これからの企業経営に必要な観点となること。
- IT 投資には「攻め」と「守り」があり、近年特に重要性が増している攻めの IT 投資について理解し、取り組むことが重要であること。
- DX の推進に伴い、データやデジタル技術の活用が進む中、サイバー攻撃の被害を防ぐためには、同時にサイバーセキュリティ対策に取り組むことが重要であること。

詳細理解のため参考となる文献（参考文献）	
情報通信白書令和 3 年版（総務省）	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf
DX 白書 2023	https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
中小企業の情報セキュリティ対策ガイドライン 第 3.1 版	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

27-7. 第 7 章. セキュリティ対策の概要（全容）

7-1. 対策基準の策定

章の目的

第 7 章では、[ISMS](#) 認証を前提としたセキュリティ対策における基準を 3 段階にレベル分けし、各基準の手法について理解することを目的とします。

主な達成目標

- ❑ セキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること
- ❑ 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

主なキーワード

セキュリティ対策基準、Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ

要旨

7 章の全体概要

7 章では、[セキュリティポリシー](#)の構成（「基本方針」「対策基準」「実施手順・運用規則など」）と、企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる、レベル感の異なる 3 つのアプローチ手法（Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ）を説明しています。

7-1. 対策基準の策定

セキュリティ対策基準の概要

情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順・運用規則など」で構成されます。「対策基準」を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせます。対策基準の内容を定める際は、網羅的な[フレームワーク](#)を参考にすることが推奨されます。

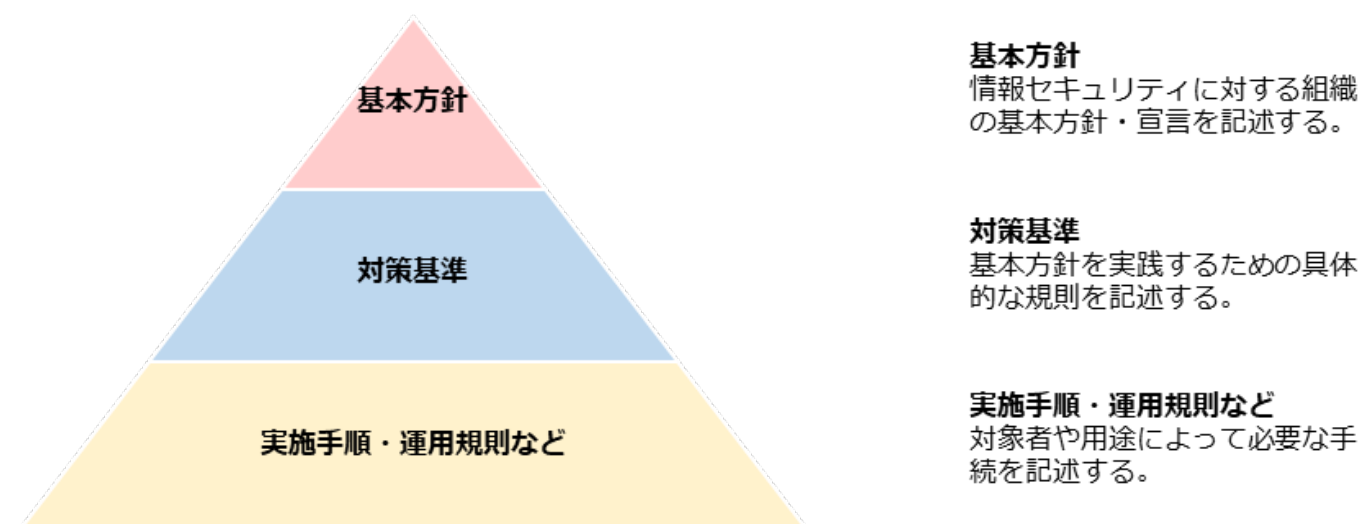


図 108. 情報セキュリティポリシーの全体像

対策基準策定のアプローチ方法

対策基準を作成するアプローチ方法には、レベル感の異なる 3 つの手法（Lv.1 クイックアプローチ、Lv.2 ベースラインアプローチ、Lv.3 網羅的アプローチ）があります。

アプローチ手法	特徴	想定される適用ケース
Lv.1 クイックアプローチ	即時の対応や緊急事態への対処に適したアプローチ手法。 低コスト、短期間で実施可能。包括的ではないが即効性がある。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対して暫定的対策を行う場合。
Lv.2 ベースラインアプローチ	組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。 ガイドラインやひな型を参考とし、対策基準を策定。 規制遵守の観点から一定の安全性が確保できる。 コストパフォーマンスがよい。	組織的に一定以上の対策基準を策定する場合。 包括的な対策は過剰で、基本的な水準の対策が適切だと判断される場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的なセキュリティ対策を講じることを目指すアプローチ手法。 ISMS 認証取得が可能なレベルを目指して、対策基準を策定。 コストが高くなる可能性があるが、組織のニーズに合わせた最適な対策が可能。	ISMS のフレームワークに沿った対策基準を策定する場合。 情報システムが重要な組織や機密性の高い情報を扱う組織など、高い水準の情報セキュリティが求められる場合。

訴求ポイント

章を通した気づき・学び

「基本方針」「対策基準」「実施手順・運用規則など」で構成されるセキュリティポリシーを策定し、セキュリティ対策の実施を内外に示すため、基本方針と対策基準を公開します。同時に、状況に応じて適切なサイバーセキュリティ対策のアプローチ手法を選択し、セキュリティ対策を実施する必要があります。

認識していただきたい実施概要

- 対策基準を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせること。
- 対策基準で記載する内容を具体的に実施するために、策定した対策基準に従って実施手順を作成することが重要であること。
- 対策基準の内容を定める際は、企業の現状や目標に応じてフレームワークを使用せずに「Lv.1 クイックアプローチ」「Lv.2 ベースラインアプローチ」を用いて策定できるが、網羅的なフレームワークである ISMS を参考に策定する「Lv.3 網羅的アプローチ」が推奨されること。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.pdf
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
マルウェア「ランサムウェア」の脅威と対策（対策編）	https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html
リスク分析シート	https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx
中小企業の情報セキュリティ対策ガイドライン第 3.1 版	https://www.ipa.go.jp/security/guide/sme/about.html
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx
自己点検チェックリスト	https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf
情報セキュリティポリシーサンプル改版（1.0 版）	https://www.jnsa.org/result/2016/policy/

27-8. 第 8 章. 用語定義および関係性と識別方法

8-1. 用語の定義、脅威・脆弱性の識別

章の目的

第 8 章では、ISO/IEC 27000 に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を理解することを目的とします。

主な達成目標

- ISMS の管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

主なキーワード

脅威、脆弱性、リスク、セーフガード（管理策）

要旨

8 章の全体概要

8 章では、リスクマネジメントを理解するために必要となる「リスク」、「脆弱性」、「脅威」といった用語の定義とそれらの関係、「脅威」、「脆弱性」の識別方法について説明しています。

8-1. 用語の定義、脅威・脆弱性の識別

用語の定義と関係性

企業や組織にはセキュリティ上のリスクが存在しています。これらのリスクを効率的に管理するには、リスクマネジメントを行う必要があります。リスクマネジメントを理解するために必要となる用語の定義や関係性を説明しています。

脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係をわかりやすく図で表すと以下ようになります。

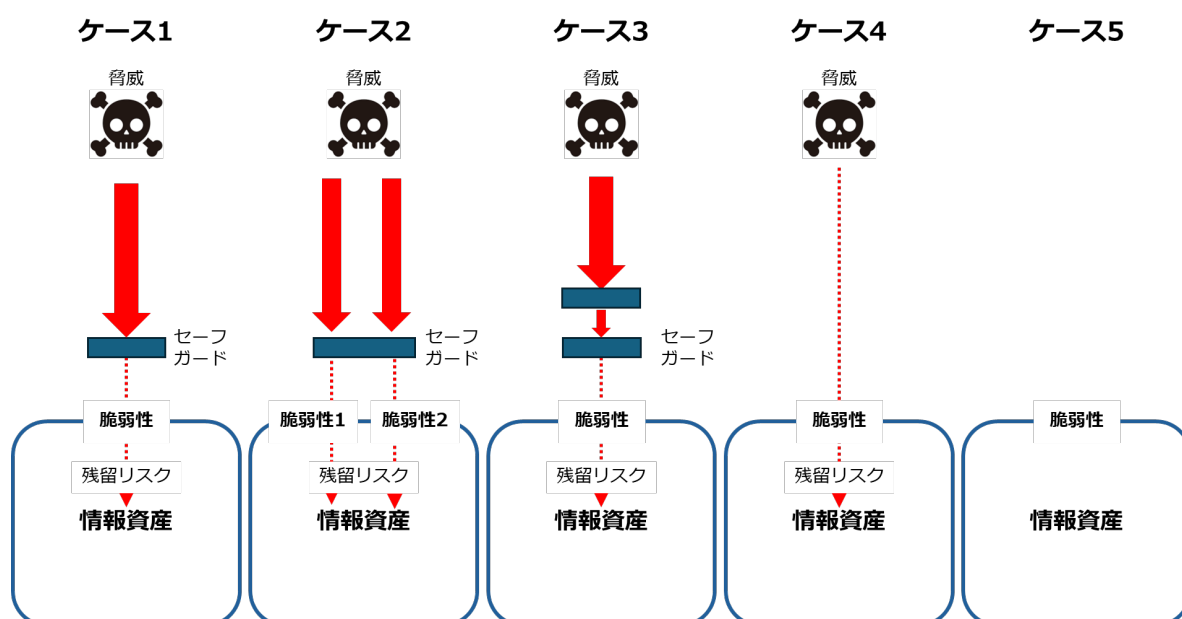


図 109. 脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係
 (出典)「ISO/IEC TR 13335-1」をもとに作成

脅威の識別

脅威は「脆弱性」につけいり顕在化することで、組織に損失や損害を与える事故を生じさせます。脅威を、人為的脅威（意図的脅威、偶発的脅威）と環境的脅威に区別して把握することで、必要なセキュリティ対策を整理しやすくなります。

脅威の種類		想定される被害とセキュリティ対策
環境的脅威（Environmental → E）		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復することを重視するなどのセキュリティ対策が選択されることになります。
人為的脅威	意図的脅威（Deliberate → D）	「（内部者が企業秘密を）漏えいする」という脅威が考えられます。このような脅威については、当該行為が犯罪行為（不正競争防止法違反）であり、罰せられること、会社は企業規則により漏えい者を罰すること、場合によっては損害賠償請求を行うということを規程で明確に示し、教育を実施するという抑止的なセキュリティ対策が有効になります。漏えいを早期に検知す

		るといったセキュリティ対策も重要になります。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じないように、二回ずつ入力する、一定の範囲の値しか入力できないようにする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

脅威の分類と、被害例と対策

(出典) MSQA「ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版」をもとに作成

脆弱性の識別

脆弱性があるだけでインシデントが発生するわけではありません。しかし、脆弱性は脅威を顕在化させ、インシデントの発生確率を高める可能性があります。脆弱性を減らすためには、適切な管理策を実施する必要があります。脆弱性の存在は、管理策の欠如を意味するものでもあるため、脆弱性を識別することは必要な管理策を識別するのに役立ちます。

訴求ポイント

章を通した気づき・学び

リスクマネジメントで使用される「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を理解することは、サイバーセキュリティ対策の第一歩でもあります。また「脅威」、「脆弱性」の識別方法について理解することは、適切なセキュリティ対策の実施に不可欠です。

認識していただきたい実施概要

- 「脅威」「脆弱性」「資産の価値」のいずれかが増加することで、リスクが増大すること。
- リスクを減少させるためには「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明らかにし、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要であること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC TR 13335-1	https://www.iso.org/standard/39066.html
ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html

27-9. 第 9 章. 具体的手順の作成 (Lv.1 クイックアプローチ)

9-1. 【Lv.1 クイックアプローチ】の概要

9-2. 【Lv.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

章の目的

第 9 章では、[セキュリティインシデント](#) 事例を参考にする Lv.1 クイックアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- Lv.1 クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード

Lv.1 クイックアプローチ

要旨

9 章の全体概要

9 章では、Lv.1 クイックアプローチについて説明しています。Lv.1 クイックアプローチは、実際のセキュリティインシデントの事例に基づいて、自社におけるセキュリティインシデントの発生可能性や想定される被害規模を検討し、対策基準や実施手順を策定していく方法です。Lv.1 クイックアプローチは、社会的に影響の大きい事案への対策がとりやすいという特徴があります。

9-1. 【Lv.1 クイックアプローチ】の概要

Lv.1 クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。

報道される事例や情報セキュリティ 10 大脅威などから、発生する可能性が高いセキュリティインシデント事例や、セキュリティインシデントが発生した場合に被害が大きい事例を参考にし、対策基準や実施手順を策定します。

9-2. 【Lv.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

Lv.1 クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定

した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。対策基準・実施手順作成の手順を説明しています。

メリット	デメリット
● 小規模な対策や修正を迅速に実施可能。 ● 低コストでリスクを軽減。	● 短期的な解決策に偏りがちになる。 ● セキュリティインシデント事例ごとに策定するため、網羅性は低い。

訴求ポイント

章を通した気づき・学び

Lv.1 クイックアプローチは、リソースが限られていても実施可能で、低コストでリスクを軽減できるコストパフォーマンスのよい方法です。しかし、包括的でないために抜けが発生する、一時的な対応であり抜本的な対策にならない、長期的に見ると費用が嵩んでしまうことがあるというデメリットがあります。

認識していただきたい実施概要

Lv.1 クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きいまたは緊急性の高い事象への対策がとりやすいこと。

詳細理解のため参考となる文献（参考文献）	
リスク分析シート	https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

27-10. 第 10 章. 具体的手順の作成 (Lv. 2 ベースラインアプローチ)

10-1. 【Lv.2 ベースラインアプローチ】の概要

10-2. 【Lv.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

章の目的

第 10 章では、ガイドラインやひな型などの資料を参考にする Lv.2 ベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- Lv.2 ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード

Lv.2 ベースラインアプローチ

要旨

10 章の全体概要

10 章では、Lv.2 ベースラインアプローチについて説明しています。Lv.2 ベースラインアプローチは、既存のガイドラインやひな型などを参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができます。

10-1. 【Lv.2 ベースラインアプローチ】の概要

Lv.2 ベースラインアプローチとは、既存のガイドラインなどを参考に対策基準や実施手順を策定するアプローチ手法です。IPA や総務省などが公開しているガイドラインやひな型を参考に、自社の対策基準や実施手順を策定します。

10-2. 【Lv.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

IPA が公開している「中小企業の情報セキュリティ対策ガイドライン第 3.1 版」「中小企業のためのクラウドサービス安全利用の手引き」「情報セキュリティ関連規程」、[NISC](#) による「インターネットの安全・安心ハンドブック Ver.5.0」、総務省の「テレワークセキュリティガイドライン第 5 版」などのガイドラインやひな型を参考にして、自社のための対策基準や実施手順を定めます。

この手法によるメリット、デメリットは以下のとおりです。

メリット	デメリット
● 組織全体で一貫性を確保できる。 ● 最低限実施すべきセキュリティ対策を講じることができる。	● 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。 ● ガイドラインやひな型は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものであるか否かを十分に検討する必要がある。

訴求ポイント

章を通した気づき・学び

ガイドラインやひな型を活用することで、中小企業でも効率的かつ効果的にセキュリティ対策を実施することが可能となります。

認識していただきたい実施概要

Lv.2 ベースラインアプローチは、ガイドラインやひな型などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定がしやすいこと。

詳細理解のため参考となる文献（参考文献）	
中小企業の情報セキュリティ対策ガイドライン第 3.1 版	https://www.ipa.go.jp/security/guide/sme/about.html
インターネットの安全・安心ハンドブック Ver.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html
テレワークセキュリティガイドライン第 5 版	https://www.soumu.go.jp/main_content/000752925.pdf
付録 6：中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/sme/f55m8k0000001wcf-att/000072150.pdf
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

27-11. 第 11 章. セキュリティフレームワーク

11-1. セキュリティフレームワークの概要

11-2. 情報セキュリティマネジメントシステム (ISMS) [ISO/IEC27001:2022, 27002:2022]

11-3. NIST サイバーセキュリティフレームワーク (CSF)

11-4. サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF)

11-5. サイバーセキュリティ経営ガイドライン

章の目的

第 11 章では、[ISMS](#) をはじめとしたサイバーセキュリティ対策における代表的なフレームワークを理解し、それぞれの内容について知識を身につけることを目的とします。

主な達成目標

- サイバーセキュリティ対策においてフレームワークを活用することの重要性について理解すること
- 各フレームワークの目的や必要性などの特徴について理解すること

主なキーワード

セキュリティフレームワーク、ISMS、CSF2.0、[CPSF](#)、サイバーセキュリティ経営ガイドライン

要旨

11 章の全体概要

11 章では、セキュリティ対策に関連する[フレームワーク](#)の特徴や概要、各フレームワークの要素や要件について解説しています。セキュリティ対策は、やみくもに進めてしまうとかえって複雑になってしまい、余計に手間がかかり、内容に抜け漏れが発生する可能性があります。漏れのない対策を効率的に実施するためには、セキュリティフレームワークを活用することが最もよい方法です。

11-1. セキュリティフレームワークの概要

次のセキュリティフレームワークの概要、利用メリットについて説明しています。

- ISMS（情報セキュリティマネジメントシステム）ISO/IEC27001:2022、ISO/IEC 27002:2022

- ISO/IEC 27017:2015
- [サイバーセキュリティフレームワーク（CSF） 2.0](#)
- サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） Ver.1.0
- サイバーセキュリティ経営ガイドライン Ver3.0
- PCI DSS（国際的なクレジット産業向けのデータセキュリティ基準） v4.0.1
- 個人情報保護マネジメントシステム（PMS） JIS Q 15001:2023 準拠 ver1.0
- CIS Controls version 8.1
- ISA/IEC 62443

11-2. 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]

ISMS は、情報セキュリティ管理のための体系的な仕組みであり、技術的対策だけでなく、従業員の教育や訓練、組織体制の整備などが含まれています。ISMS は、セキュリティフレームワークの中でも代表的なものです。ISMS が達成すべきことは、リスクマネジメントプロセスを適用することによって情報の[機密性](#)、[完全性](#)および[可用性](#)をバランスよく維持・改善し、リスクの適切な管理を実現し、信頼を利害関係者に与えることです。

11-3. NIST サイバーセキュリティフレームワーク（CSF）

CSF は、NIST が作成した[サイバー攻撃](#)対策に重点を置いたフレームワークであり、防御に留まらず、検知・対応・復旧といったインシデント対応を含んでいます。CSF2.0 は、中小企業を含むあらゆる組織で利用されるよう設計されています。CSF2.0 は ISMS を補完し、組織のセキュリティ対策を強化するための有用なツールとなるので、ISMS をベースにして、必要に応じて CSF を取り込むとよいでしょう。

11-4. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

CPSF は、ISMS や CSF のフレームワークの内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策に対応したフレームワークです。CPSF の主な目的は、新たな産業社会におけるバリュークリエーションプロセス全体の理解、リスク源の明確化、必要なセキュリティ対策全体像の整理を行うことです。従来の[サプライチェーン](#)に適用可能なセキュリティ対策に加えて、新たな産業社会の変化から生じる特有の対策も含まれています。

11-5. サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドラインは、経済産業省と IPA が共同で発行しているガイドラインで、企業がサイバーセキュリティを効果的に経営に取り入れるための指針を提供します。経

営者が認識すべき3原則、サイバーセキュリティ経営の重要10項目など内容を含んでおり、経営者、情報セキュリティ対策の責任者（CISO など）の立場から、セキュリティ対策を実践する際の役割、認識すべきことがまとめられています。このガイドラインは、企業がサイバーセキュリティを経営の一部として位置づけ、組織全体でセキュリティ意識を高めるための基盤として活用できます。

訴求ポイント

章を通した気づき・学び

セキュリティ対策を漏れなく効果的に実施するためには、セキュリティフレームワークを使用することが有効です。さまざまなセキュリティフレームワークがある中、自社の課題や目的に即したものを選択することが大切です。

認識していただきたい実施概要

- 効果的なセキュリティ対策の実施や、取引先や顧客からの信頼を向上させるためには、フレームワークに沿って対策を進めることが有効であること。
- セキュリティ対策を行うためのフレームワークは複数存在するが、まずは業種業態を問わずセキュリティ対策の全体の枠組みと、網羅的な対策項目を提示している ISMS をベースとし、必要に応じて業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークで補完することが有効であること。

詳細理解のため参考となる文献（参考文献）	
ISMS-AC ISMS 適合性評価制度	https://isms.jp/doc/JIP-ISMS120-62.pdf
The NIST Cybersecurity Framework (CSF) 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要	https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.pdf
サイバーセキュリティ経営ガイドライン Ver3.0	https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf

27-12. 第 12 章. リスクマネジメント

12-1. リスクマネジメント：概要

12-2. リスクマネジメント：リスクアセスメント

12-3. リスクマネジメント：リスク対応

章の目的

第 12 章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方について学ぶことを目的とします。

主な達成目標

- リスクマネジメントの意義について理解すること
- リスクマネジメントプロセスの全体像を理解すること
- リスクアセスメント、リスク対応のプロセスを理解すること

主なキーワード

リスクマネジメント、リスクアセスメント

要旨

12 章の全体概要

12 章では、リスクマネジメントプロセスに沿って、リスク基準の確立、[リスクアセスメント](#)、リスク対応について解説しています。リスクマネジメントはセキュリティ対策にとって不可欠な要素です。リスクは、顕在化していないものについても検討する必要があります。リスクマネジメントプロセスにおける各段階での考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できます。

12-1. リスクマネジメント：概要

リスクマネジメントプロセス（ISO 31000）

リスクを効率的に管理し、発生する可能性がある損失を回避、低減するプロセス全体のことを「リスクマネジメント」といいます。リスクマネジメントの国際規格として ISO 31000 があります。リスク対応にあたり、リスクマネジメントプロセスにおける「リスクアセスメント」が必須です。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位付けをしていくプロセスです。

情報セキュリティリスクマネジメント（ISO/IEC 27005）

ISO/IEC 27005 は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。ISO 31000 と整合性があり、情報セキュリティに特化した内容になっています。

ISO/IEC 27001 におけるリスクマネジメント手順

ISO/IEC 27001 は [ISMS](#) の枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているものが、ISO/IEC 27005 です。ISO/IEC 27001 の活動は、ISO/IEC 27005 におけるリスクマネジメントプロセスと関連付けて整理できます。

12-2. リスクマネジメント：リスクアセスメント

12-3. リスクマネジメント：リスク対応

リスクマネジメント全体の流れは下記の図の通りです。リスクアセスメントでは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク基準と比較してリスク対応が必要か否か判断します。リスクの特定には、「資産ベースのアプローチ」と「事象ベースのアプローチ」の2つの方法があります。[情報資産](#)ごとに、その重要度を「[機密性](#)」「[完全性](#)」「[可用性](#)」が損なわれた場合の事業への影響度から決め、重要度と被害発生の可能性からリスクレベルを求めます。この[リスク評価](#)の結果をもとに、受容可能でないものについては、「低減」、「移転」、「回避」、「受容（保有）」からリスク対応を選択します。すべての残留リスクが受容できるレベルになるまで、このリスク評価のプロセスを繰り返します。

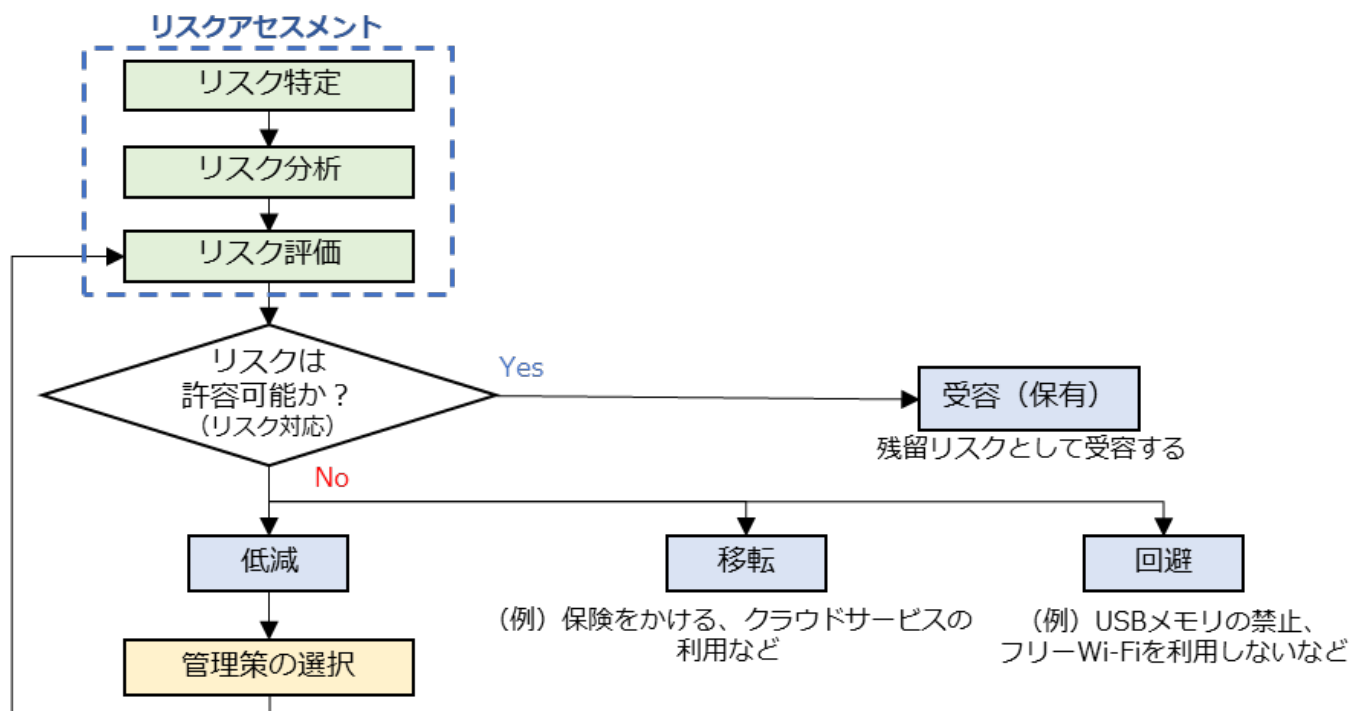


図 110. リスクマネジメント全体の流れと、リスク対応の選択プロセス

訴求ポイント

章を通した気づき・学び

リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることが難しい場合がありますが、「資産ベースのアプローチ」によって網羅的にリスクを特定するようにしましょう。リスクマネジメントプロセスにおける各段階の考え方や手法を用いることで、円滑なリスク特定、分析と対応策の選択と実施が可能になります。このプロセスによってすべてのリスクをコントロールし、残留リスクを受容可能なレベルにすることができます。

認識していただきたい実施概要

- リスク対応にはリスクマネジメントプロセスにおけるリスクアセスメントが必須であること。
- リスクアセスメントは「リスク特定」、「リスク分析」、「リスク評価」を実施すること。
- リスク対応はリスクアセスメントの結果をもとに「リスク回避」、「リスク低減」、「リスク移転」、「リスク受容」から選択すること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html
リスクアセスメントとリスク対応	https://www.jnsa.org/ikusei/01/02-04.html

27-13. 第 13 章. ISMS の要求事項と構築 (Lv.3 網羅的アプローチ)

13-1. 【Lv.3 網羅的アプローチ】の概要

13-2. 【Lv.3 網羅的アプローチ】フレームワークを参考とした実施手順

13-3. ISMS 文書体系 (ISMS 構築・導入に必要な文書と記録)

13-4. ISO/IEC27001 の審査準備と審査内容

章の目的

第 13 章では、情報セキュリティマネジメントシステム (ISMS) のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する Lv.3 網羅的アプローチについて理解することを目的とします。

主な達成目標

□ Lv.3 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード

Lv.3 網羅的アプローチ、PDCA サイクル

要旨

13 章の全体概要

13 章では、情報セキュリティマネジメントシステム (ISMS) を構築するための Lv.3 網羅的アプローチについて説明しています。Lv.3 網羅的アプローチは、ISMS のフレームワークに従い、組織全体で適用できるセキュリティ対策基準と手順を整備する方法です。ISMS の運用では PDCA サイクルを用い、計画・実行・評価・改善のプロセスを通じて継続的に改善を実施します。ISO/IEC 27001 の要求事項に基づき、ISMS に関する文書作成が求められますが、重要なのはセキュリティ対策の策定と実施なので、文書の作成が目的にならないよう注意が必要です。

13-1. 【Lv.3 網羅的アプローチ】の概要

Lv.3 網羅的アプローチ

Lv.3 網羅的アプローチでは、フレームワークとして ISMS を用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。ISMS のフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。ISMS における PDCA サイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項に

ついて焦点を当てて説明しています。

Lv.3 網羅的アプローチのメリットは、ISMS 要求事項の導入によって組織のセキュリティレベルが大幅に向上することです。デメリットは、時間とコストがかかることです。

ISMS の要求事項に関連するドキュメント作成は重要ですが、あくまで手段であり目的ではありません。ドキュメントの作成と維持が目的化してしまうと、ドキュメントが形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。**ドキュメントを精細に作り込むことより、ISMS マネジメントプロセスを取り入れ、PDCA サイクルを回していくことが大切です。**ISMS に取り組みはじめたときには理解できていても、ドキュメントづくりをはじめるとドキュメント作成が目的になってしまうケースが多いため、注意が必要です。

13-2. 【Lv.3 網羅的アプローチ】フレームワークを参考とした実施手順

ISMS は、PDCA サイクルに則って運用することになります。ISMS における PDCA サイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明しています。

ISMS の要求事項を定めている ISO/IEC 27001 の 1 から 3 はそれぞれ「1.適用範囲」「2.引用規格」「3.用語および定義」なので、実質的な要求事項は「4.組織の状況」から「10.改善」までの 7 項目となっています。

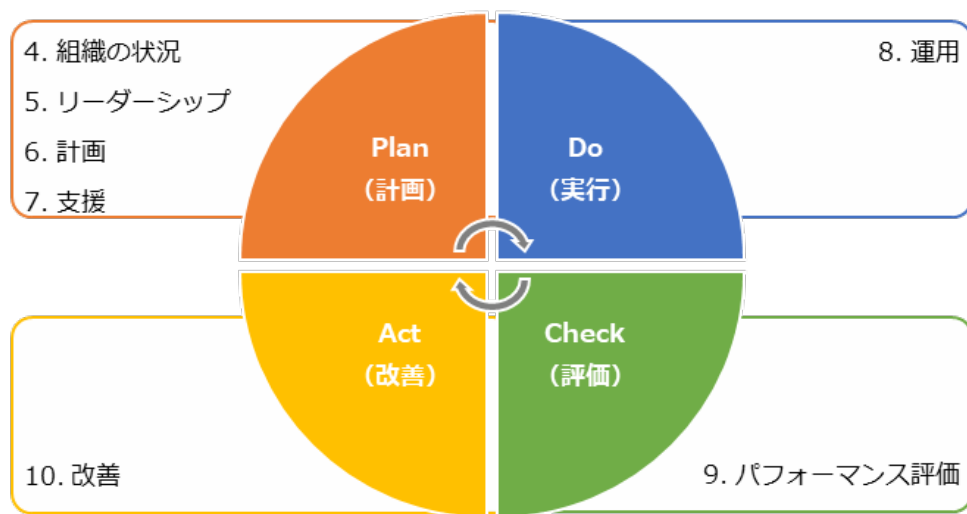


図 111. ISMS の PDCA サイクル

4. 組織の状況

組織の内情や取り巻く状況、利害関係者のニーズを把握した上で ISMS の適用範囲を決定することを要求している。

5. リーダーシップ

トップマネジメントが主導して ISMS を構築することを要求している。(トップマネジメントが

実施すべきことのまとめ)

6. 計画

ISMS の計画を立てる際の要求事項。

7. 支援

従業員の教育など、ISMS 構築にあたり組織が従業員に行うべきサポートを要求している。

8. 運用

ISMS を実行する際の要求事項。

9. パフォーマンス評価

適切な ISMS が構築・運用できているか評価する際の要求事項。

10. 改善

ISMS の是正処置やリスク、改善の機会、ISMS 認証の不適合があった場合の対処法。

13-3. ISMS 文書体系 (ISMS 構築・導入に必要な文書と記録)

ISMS (情報セキュリティマネジメントシステム) の構築や導入に必要な文書と記録の重要性を説明しています。ISMS 文書は、組織内で情報セキュリティの有効な管理を実施するための基本的な要素として、対策や手続きが記載されています。

ISMS 文書体系には、以下のポイントが含まれます:

- **文書の策定内容とその要点:**

対策基準や実施手順が明確に示され、実施状況の確認が可能。

- **管理策:**

ISO/IEC 27001 の要求事項に基づいた文書作成が推奨され、組織全体でのセキュリティ向上を支援します。

13-4. ISO/IEC27001 の審査準備と審査内容

ISO/IEC 27001 認証取得に向けた審査準備や審査の具体的内容について説明しています。主要内容は以下の通りです。

- **認証機関の選定と申し込み:**

認証機関は、ISMS-AC (情報マネジメントシステム認定センター) から認定された組織である必要があり、申請には書類や登録料が異なることを事前に確認します。

- **審査事前準備:**

ISMS 構築のステップを踏まえて、審査対象の範囲や実施手順の文書化が求められます。

- **第一段階・第二段階審査:**

1 次審査は文書レビュー、2 次審査は現地での実施状況確認が行われ、適合が確認されると認証書が発行されます。

- **維持審査・再認証審査:**

年 1 回以上の維持審査と、3 年ごとの再認証審査で、ISMS の有効性が評価されます。

訴求ポイント

章を通した気づき・学び

ISMS を用いる Lv.3 網羅的アプローチを実施することで、単にセキュリティ対策を検討するだけではなく、PDCA サイクルによって ISMS 自体を継続的に改善し、より自社に適した対策を策定・実施できるようになります。

認識していただきたい実施概要

- 「4.組織の状況」から「10.改善」までの 7 項目で必要なドキュメントの作成手順を理解すること。
- ISMS マネジメントプロセスを取り込み、PDCA サイクルを回すこと。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html
ISMS 適合性評価制度	https://isms.jp/isms.html

27-14. 第 14 章. ISMS の管理策

14-1. 管理策の分類と構成

章の目的

第 14 章では、ISO/IEC 27002 における管理策の分類と構成について理解することを目的とします。

主な達成目標

- ISMS の管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

主なキーワード

管理策、ISO/IEC 27002

要旨

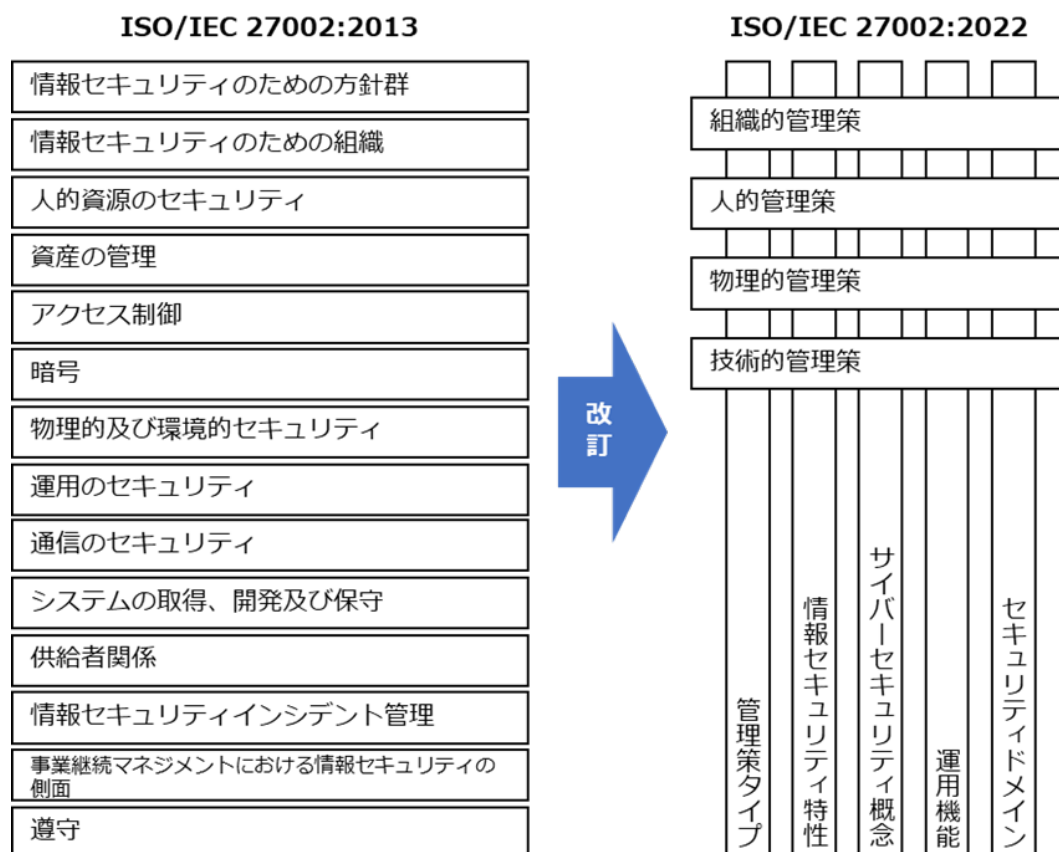
14 章の全体概要

14 章では、ISO/IEC 27002 に基づく [ISMS](#) の管理策について説明しています。企業は、組織的・人的・物理的・技術的な 4 つのカテゴリに分類された 93 項目の管理策から、自社のリスクに応じた適切な管理策を選び、対策基準として導入する必要があります。また、各管理策には目的と属性が追加され、リスクの予防・検知・是正などの観点から策定が求められます。2022 年版の改訂により、管理策の項目数と内容が見直され、組織に適した情報セキュリティ対策の選定と実施が重要視されています。

14-1. 管理策の分類と構成

管理策 : ISO/IEC 27002

管理策の数は、2013 年版では 14 分野 114 項目でしたが、2022 年版ではいくつかが統合されて 82 項目になり、新しく 11 項目が追加され、合計で 93 項目となりました。2022 年版では、この 93 の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4 つのカテゴリに分類されています。また、「属性 (attribute)」という新しい概念が導入されました。この属性という概念が導入されたことで、管理策のフィルタリング、並び替え、提示がしやすくなりました。ISMS を構築する際には、これらの管理策から、自社にあったものを選択し、対策基準として採用します。



管理策のテーマと属性について説明しています。

テーマとは、ISO/IEC 27002 の箇条 5～8 に示される 4 種の管理策での分類（組織的・人的・物理的・技術的）のことです。

属性とは、テーマとは別の視点で、より細かに管理策を見るためのものです。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。



図 112. ISO/IEC 27002:2022 の概要

また、情報セキュリティのために必要な管理策を適用宣言書として選定し、対策基準を作成し、その後に実施手順を策定する方法を説明しています。

- **管理策の決定:**

リスクアセスメントの結果を考慮し、適切なリスク対応策を選び出し、ISO/IEC 27001 の附属書 A から適切な管理策を決定します。

- **管理策の検証:**

決定した管理策が適切であり、見落としがないか ISO/IEC 27001 に基づき検証します。

- **適用宣言書の作成:**

組織が実施する管理策を文書化した適用宣言書を作成し、必要な管理策とその理由を記載します。

- **実施手順の作成:**

管理策をもとに組織内部での具体的な実施手順を作成します。従業員が理解しやすいように、わかりやすい言葉で明確に策定することが重要です。

訴求ポイント

章を通した気づき・学び

企業や組織は ISO/IEC 27002 に示された管理策から組織に必要なものを選択し、対策基準として導入することになります。

認識していただきたい実施概要

- ISMS におけるリスク対応のための対策を指すものとして管理策があり、ISO/IEC 27002:2022 に合計 93 項目示されていること。
- ISO/IEC 27002:2022 で示される管理策には 4 つのテーマと 5 つの属性があり、それらを参考にしながら組織に必要なセキュリティ対策を選択することが重要であること。

詳細理解のため参考となる文献（参考文献）

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

27-15. 第 15 章. 組織的対策

15-1. 作成する候補となる実施手順書類について

15-2. 組織的対策として重要となる実施項目

章の目的

第 15 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 組織的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

主なキーワード

組織的管理策

要旨

15 章の全体概要

15 章では、セキュリティ対策を実施するための具体的な規則としての対策基準と、その実施手順について説明しています。対策基準は、ISO/IEC 27001:2022 附属書 A の合計 93 項目の管理策を参考に策定します。実施手順は ISO/IEC 27002 に記載されている各管理策の手引きを参考に策定することができます。15 章では「組織的管理策」を例にして、対策基準を策定する手順と、それぞれの対策基準に対応する実施手順の例を説明しています。

15-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に記載された 93 項目の管理策を参考に、必要な管理策を選択して対策基準を策定し、実施手順を作成する方法を説明しています。これにより、組織が[リスクアセスメント](#)の結果に基づいて適切な管理策を選び、その基準に従って具体的な手順書を内部文書として作成することが奨励されます。

15-2. 組織的対策として重要となる実施項目

組織が情報セキュリティを強化するために必要な取組について具体的に説明しています。これ

には、組織全体での情報管理の体系化、サイバーセキュリティ対策の適切な実施、個人情報の保護が含まれています。また、外部および内部の脅威情報を収集し、セキュリティ対策に役立てる「脅威インテリジェンス」の導入が推奨され、重要な情報資産を特定して管理するための情報資産管理台帳の作成と更新も重要視されています。

組織的管理策の項目	
5.1 情報セキュリティのための方針群	5.21 ICT サプライチェーンにおける情報セキュリティの管理
5.2 情報セキュリティの役割及び責任	5.22 供給者のサービス提供の監視、レビュー及び変更管理
5.3 職務の分離	5.23 クラウドサービス利用における情報セキュリティ
5.4 経営陣の責任	5.24 情報セキュリティインシデント管理の計画策定及び準備
5.5 関係当局との連絡	5.25 情報セキュリティ事象の評価及び決定
5.6 専門組織との連絡	5.26 情報セキュリティインシデントへの対応
5.7 脅威インテリジェンス	5.27 情報セキュリティインシデントからの学習
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.28 証拠の収集
5.9 情報及びその他の関連資産の目録	5.29 事業の中断・障害時の情報セキュリティ
5.10 情報及びその他の関連資産の利用の許容範囲	5.30 事業継続のための ICT の備え
5.11 資産の返却	5.31 法令、規制及び契約上の要求事項
5.12 情報の分類	5.32 知的財産権
5.13 情報のラベル付け	5.33 記録の保護
5.14 情報転送	5.34 プライバシー及び PII の保護
5.15 アクセス制御	5.35 情報セキュリティの独立したレビュー
5.16 識別情報の管理	5.36 情報セキュリティのための方針群、規則及び標準の順守
5.17 認証情報	5.37 操作手順書
5.18 アクセス権	
5.19 供給者関係における情報セキュリティ	
5.20 供給者との合意におけるセキュリティの取扱い	

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002 の内容を参考に組織的管理策の対策基準を決定し、実施手順を作成することができます。ドキュメントの作成・更新は重要ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- リスクアセスメントの結果をもとに必要な組織的管理策を選択し、対策基準を策定すること。
- 対策基準は、基本方針とともに公開可能なものとして策定すること。
- 決定した対策基準を実行に移すための実施手順を策定すること。
- 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

27-16. 第 16 章. 人的対策

16-1. 作成する候補となる実施手順書類について

16-2. 人的対策として重要となる実施項目

章の目的

第 16 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 人的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

主なキーワード

人的管理策

要旨

16 章の全体概要

16 章では、情報セキュリティ方針に従い、人的対策を中心にセキュリティ対策基準を策定するための方法について説明しています。まず、[リスクアセスメント](#)の結果をもとに適切な管理策を選定し、それを実施手順として組織の内部文書にまとめます。この際、ISO/IEC 27001 の規定に基づいて選定するだけでなく、独自の追加管理策も含めることが推奨されます。具体的な項目としては、雇用契約、守秘義務、リモートワーク手順、懲戒手続などが含まれ、従業員の行動指針として重要な役割を果たします。

16-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に示された 93 項目の管理策を参考に、情報セキュリティにおける実施手順書を策定する方法が説明しています。実施手順書は、リスクアセスメントをもとに選定された管理策を対策基準として採用し、具体的な手順を文書化するための候補を提示します。これにより、組織が適切な管理策を選定し、それをもとに対策基準と具体的な実施手順を策定することが可能になります。

16-2. 人的対策として重要となる実施項目

組織における人的管理策の重要実施項目として、従業員の採用から退職後までのセキュリティ対策を紹介しています。具体的には、情報セキュリティの観点から従業員の選考、雇用契約の内容、セキュリティ教育、守秘義務の遵守などの具体的な項目を取り上げています。懲戒手続や雇用終了後のセキュリティ対策の責任、リモートワーク実施時のセキュリティや情報セキュリティイベントの報告手続に関しても指針を示しています。

人的管理策の項目	
6.1 選考 6.2 雇用条件 6.3 情報セキュリティの意識向上、教育及び訓練 6.4 懲戒手続	6.5 雇用の終了又は変更後の責任 6.6 秘密保持契約又は守秘義務契約 6.7 リモートワーク 6.8 <u>情報セキュリティ事象</u> の報告

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002 の内容を参考にしつつ、雇用契約、守秘義務、リモートワーク手続、懲戒手続など自社に適した管理策を追加して、人的管理策の対策基準を決定し、実施手続を作成することが大切です。

認識していただきたい実施概要

- リスクアセスメントの結果をもとに必要な人的管理策を選択し、対策基準を策定すること。
- 対策基準は、基本方針とともに公開可能なものとして策定すること。
- 決定した対策基準を実行に移すための実施手続を策定すること。
- 実施手続は、組織の内部文書として従業員に対してわかりやすい実施手続を策定するよう心掛けること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

27-17. 第 17 章. 物理的対策

17-1. 作成する候補となる実施手順書類について

17-2. 物理的対策として重要となる実施項目

17-3. BYOD、MDM

章の目的

第 17 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 物理的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること

主なキーワード

物理的管理策、BYOD（Bring Your Own Device）、MDM（Mobile Device Management）

要旨

17 章の全体概要

17 章では、情報セキュリティのために物理的な保護措置を定義する方法について説明しています。まず、組織のレイアウト図を用いて物理的なセキュリティ境界を明確にし、重要な[情報資産](#)があるエリアを保護する必要があります。入退室の管理には、従業員証やセキュリティカードを用い、外来者の訪問については記録とエスコートが求められます。さらに、オフィスや施設のセキュリティを高めるために、施錠や外部からの視線を遮る対策も必要です。施設内では監視カメラや侵入者警報を活用し、無人領域にも監視システムを設置してセキュリティを維持します。また、災害や物理的な脅威への対策として、消火器や火災報知器の設置、サーバの転倒防止措置、情報漏えい防止のためのクリアデスク・クリアスクリーンについても解説しています。

17-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に基づき、物理的セキュリティ対策のための手順書を策定する方法を説明しています。具体的には、[リスクアセスメント](#)結果をもとに適切な管理策を選択

し、対策基準を策定するプロセスを示しています。これにより、組織が必要とする物理的な安全対策を標準化し、実施手順を整えることができます。

17-2. 物理的対策として重要となる実施項目

組織の物理的セキュリティを強化するための重要な実施項目を紹介しています。具体的には、以下のポイントが挙げられます。

物理的管理策の項目	
7.1 物理的セキュリティ境界 7.2 物理的入退 7.3 オフィス、部屋及び施設のセキュリティ 7.4 物理的セキュリティの監視 7.5 物理的及び環境的脅威からの保護 7.6 セキュリティを保つべき領域での作業 7.7 クリアデスク・クリアスクリーン	7.8 装置の設置及び保護 7.9 構外にある資産のセキュリティ 7.10 記憶媒体 7.11 サポートユーティリティ 7.12 ケーブル配線のセキュリティ 7.13 装置の保守 7.14 装置のセキュリティを保った処分又は再利用

17-3. BYOD、MDM

● BYOD (Bring Your Own Device)

BYOD とは、個人が私物として所有している端末（PC やスマートフォンなど）を業務に使う利用形態のことです。BYOD 導入に向けたポイント、運用手順を説明しています。

メリット

- コスト削減
企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入れ替えも基本的には個人負担となります。
- 使い慣れた端末の業務利用
従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率が上がります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。

デメリット

- シャドーIT
ルールの整備や技術的な対策を講じないと、シャドーITが増加してしまう恐れがあります。
- セキュリティリスク
個人の端末では、業務に関係ないWebサイトやアプリケーションを利用されるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなります。

● MDM (Mobile Device Management)

MDM とは、企業で保有しているモバイル端末（スマートフォンやタブレットなど）を一元管理できるシステムのことです。MDM の導入に向けたポイント、運用手順を説明しています。

MDMを導入する際のポイント

- ✓ 利用者の意見を反映した社内ルールの策定、およびMDMの選定

MDMは情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。たとえば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDMによる制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定やMDMの選定を進めることが重要です。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002 の内容を参考にして、自社に適した物理的管理策の対策基準を決定し、実施手順を作成することが大切です。

認識していただきたい実施概要

- リスクアセスメントの結果をもとに必要な物理的管理策を選択し、対策基準を策定すること。
- 対策基準は、基本方針とともに公開可能なものとして策定すること。
- 決定した対策基準を実行に移すための実施手順を策定すること。
- 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。
- BYOD、MDM の概要および運用手順を理解すること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

27-18. 第 18 章. 技術的対策

18-1. 作成する候補となる実施手順書類について

18-2. 技術的対策として重要となる実施項目

18-3. 実施手順を適用するセキュリティ概念

18-4. インシデント対応

章の目的

第 18 章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実実施手順や方法である「実施手順」について学ぶことを目的とします。また、技術的管理策に関して、テーマごとの対策について学ぶことも目的とします。

主な達成目標

- 技術的管理策をもとに、対策基準を策定する手順を理解すること
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること
- Security by Design、[ゼロトラスト](#)・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること

主なキーワード

技術的管理策、Security by Design、ゼロトラスト、ネットワーク制御、セキュリティ統制、インシデント対応

要旨

18 章の全体概要

18 章では、情報セキュリティを実現するための具体的な技術的対策を解説しています。まず、ISO/IEC 27001:2022 に基づき、[リスクアセスメント](#)結果に基づく技術的管理策を策定することが必要です。管理策には、[エンドポイントデバイス](#)の保護、特権アクセス権の管理、アクセス制限の確立、安全な認証技術の導入が含まれます。また、[マルウェア](#)対策や技術的[脆弱性](#)の管理、バックアップと冗長化の設定も重要な要素として挙げられます。さらに、ゼロトラストや SASE などのセキュリティアーキテクチャを取り入れ、インシデント対応を強化することが望まれます。

18-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に基づいて、技術的管理策を用いた対策基準を策定し、その具体的な実施手順を文書化するプロセスを説明しています。リスクアセスメント結果をもとに必要な技術的管理策を選定し、実施手順書を作成することで、組織が情報セキュリティの技術的側面を強化する手段が提供されます。このプロセスにより、情報の安全な取り扱いや[アクセス制御](#)、エンドポイント保護、ネットワーク管理などを含む多様な技術的対策を体系的に導入できます。

18-2. 技術的対策として重要となる実施項目

情報セキュリティを確保するために組織が実施すべき技術的管理策を紹介しています。

技術的管理策の項目	
8.1 利用者エンドポイント機器	8.19 運用システムに関わるソフトウェアの導入
8.2 特権的アクセス権	8.20 ネットワークのセキュリティ
8.3 情報へのアクセス制限	8.21 ネットワークサービスのセキュリティ
8.4 ソースコードへのアクセス	8.22 ネットワークの分離
8.5 セキュリティを保った認証	8.23 ウェブ・フィルタリング
8.6 容量・能力の管理	8.24 暗号の使用
8.7 マルウェアに対する保護	8.25 セキュリティに配慮した開発のライフサイクル
8.8 技術的ぜい弱性の管理	8.26 アプリケーションのセキュリティの要求事項
8.9 構成管理	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構成の原則
8.10 情報の削除	8.28 セキュリティに配慮したコーディング
8.11 データマスキング	8.29 開発及び受入れにおけるセキュリティ試験
8.12 データ漏えいの防止	8.30 外部委託による開発
8.13 情報のバックアップ	8.31 開発環境、試験環境及び運用環境の分離
8.14 情報処理施設の冗長性	8.32 変更管理
8.15 ログ取得	8.33 試験情報
8.16 監視活動	8.34 監査試験中の情報システムの保護
8.17 クロックの同期	
8.18 特権的なユーティリティプログラムの使用	

18-3. 実施手順を適用するセキュリティ概念

この節では、組織が情報セキュリティ対策を実施する際に適用すべきセキュリティ概念を紹介しています。具体的には、以下の5つの主要な概念を取り上げています。

- **Security by Design:**

設計段階からセキュリティを組み込む手法で、開発ライフサイクル全体にわたり、潜在的な脆弱性を排除し、堅牢なシステムを構築することを目指します。

- **ゼロトラストモデル:**

伝統的な境界防御モデルに代わり、常に疑いを持ち、認証を通じてアクセスを制御するアプローチです。ユーザーやデバイスの信頼を前提とせず、厳密なアクセス管理を行います。

- **SASE (Secure Access Service Edge):**

ネットワークとセキュリティ機能を統合し、クラウドサービスを活用して分散された業務環境に適応するセキュリティモデルです。

- **ネットワーク制御 (Network as a Service):**

ネットワーク機能をサービスとして提供し、セキュリティ管理を効率化する取り組みです。

- **セキュリティ統制 (Security as a Service):**

セキュリティ機能をクラウドサービスとして提供し、柔軟な運用を実現します。

18-4. インシデント対応

この節では、情報セキュリティインシデントが発生した際の基本的な対応手順を解説しています。インシデント対応は、「検知・初動対応」「報告・公表」「復旧・再発防止」の3つのステップで構成されます。初動対応では、インシデントを素早く把握し、影響を抑えるための即時対応が求められます。報告・公表の段階では、必要に応じて関係者や関連当局への報告を行います。復旧・再発防止の段階では、影響の調査と是正措置を通じて被害を最小限に抑え、将来的なインシデントを防止するための改善を実施します。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002 の内容を参考に技術的管理策の対策基準を決定し、実施手順を作成することが大切です。特に、Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応などに関するセキュリティ関連技術の動向を把握し、必要な技術的管理策を採用することが重要です。

認識していただきたい実施概要

- リスクアセスメントの結果をもとに必要な技術的管理策を選択し、対策基準を策定するこ

と。

- 対策基準は、基本方針とともに公開可能なものとして策定すること。
- 決定した対策基準を実行に移すための実施手順を策定すること。
- 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。
- 各種テーマごとに概要を理解し、自社に適した実施手順を策定すること。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

27-19. 第 19 章. セキュリティ対策状況の有効性評価

19-1. 内部監査

19-2. 外部監査

章の目的

第 19 章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。

主な達成目標

- 内部監査および外部監査の重要性について理解すること

主なキーワード

内部監査、外部監査

要旨

19 章の全体概要

19 章では、セキュリティ対策の効果を確認するための監査について説明しています。[内部監査](#)とは、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実施されているかをチェックすることです。最初は、内部監査により組織内のルールや手順が適切に守られているかを確認し、運用に慣れたら、その有効性について評価します。次に、外部監査を通じて第三者による客観的な視点から評価し、改善点を見つけることが推奨されます。内部と外部の監査を組み合わせることで、ルールの形骸化を防ぎ、目的達成に向けた対策が継続的に改善されるよう努めます。

19-1. 内部監査

セキュリティのルールを整備したばかりの段階では、関係者がルールを理解し、遵守できているか適合性を重視してチェックします。運用に慣れてきたら、社内のルールや文書の内容が適切か否か有効性をチェックします。内部監査の視点を適合性から有効性へと移していくことで、ルールが形骸化し、目的が見失われる状態を防げるでしょう。

19-2. 外部監査

セキュリティ対策の実施状況について外部監査を受けることは、情報漏えいやサイバー攻撃などのリスクに対する対策が適切かつ有効であるか否かをチェックする手段の1つです。情報セキュリティ監査を受ければ、自社のセキュリティ対策が正しく行われているか確認でき、不十分な点を洗い出して迅速に対処できます。また、顧客や取引先に、セキュリティ対策を適切に行っていることをアピールできます。

訴求ポイント

章を通した気づき・学び

企業や組織は、セキュリティ対策状況の有効性を評価するため、定期的に内部監査・外部監査を実施することが必要です。

認識していただきたい実施概要

- 外部監査を行うことで、第三者視点で企業が保有する情報資産を守るための体制や環境が整っているかをチェックでき、また顧客や取引先に、セキュリティ対策を適切に行っているというアピールにもつながること。
- 内部監査を行うことで、セキュリティのルールや文書の内容が適切か否かの有効性をチェックでき、形骸化し、目的が見失われている状態を防止することにつながる。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

27-20. 第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）

20-1. セキュリティ機能の実装と運用

20-2. アジャイル開発

章の目的

第 20 章では、「デジタル・ガバメント推進標準ガイドライン」などが示すサービスシステム構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を理解することを目的とします。

主な達成目標

- 中小企業においても有効なシステム導入工程と、実践にあたっての留意点を理解すること
- システム導入工程に沿って、セキュリティ機能を実装・運用するためポイントを理解すること
- アジャイル開発の概要と実践ポイントを理解すること

主なキーワード

デジタル・ガバメント推進標準ガイドライン、アジャイル開発

要旨

20 章の全体概要

20 章では、「デジタル・ガバメント推進標準ガイドライン」などに記載されている政府情報システムの構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を説明しています。

また、アジャイル開発の概要と実践ポイントを解説しています。

20-1. セキュリティ機能の実装と運用

「デジタル・ガバメント推進標準ガイドライン」などを参考に、中小企業においても適用することが有効な工程や、セキュリティ機能を実装・運用するためポイントなどを説明しています。

中小企業においても適用することが有効な工程の例として、Fit&Gap 分析が挙げられます。情報システム構築においてパッケージソフトウェアや SaaS を利用する場合は、導入するパッケージソフトウェアや SaaS などのシステムと、自社の業務要件との適合性を評価する Fit&Gap 分析

が重要になります。

20-2. アジャイル開発

アジャイル開発の必要性、概要、実践ポイントを説明しています。

アジャイル開発は、「敏捷」「素早い」といった意味を持ち、新しい機能を短期間で継続的にリリースする開発手法です。この手法は、変化の激しい現代のビジネス環境に適応し、柔軟かつ試行錯誤を許容するアプローチとして有用です。従来の開発手法が試行錯誤に不向きであるのに対し、アジャイル開発は反復的なフィードバックに基づき改善を重ねることで、最適なシステムを目指します。

訴求ポイント

章を通した気づき・学び

「デジタル社会推進標準ガイドライン群」は、政府情報システムの共通ルールを定めたものですが、システム導入の流れ自体は、一般企業であっても参考になります。ガイドラインを通してシステム導入の全体像を認識し、ガイドラインを実践する際は必要に応じてルールを取捨選択する必要があります。

認識していただきたい実施概要

- 「デジタル・ガバメント推進標準ガイドライン」を参考に、中小企業にも適用可能なシステム導入工程や実践時の留意点を理解すること。
- 情報システムの構築と運用の各工程（プロジェクト管理、要件定義、設計・開発、運用など）でセキュリティ機能を実装すること。
- アジャイル開発の重要性を理解すること。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-110 デジタル・ガバメント推進標準ガイドライン解説書	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9462b2d8/20240605_resources_standard_guidelines_guideline_03.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
アジャイル領域へのスキル変革の指針 アジャイル開発の進め方	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

27-21. 第 21 章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

21-1. EC サイトの構築とセキュリティ機能の実装と運用

章の目的

第 21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明します。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を理解することを目的とします。

主な達成目標

- ❑ 実施例から工程を理解することで、中小企業が主体的に関与するポイントを理解すること
- ❑ 情報システムを導入する工程で、作成すべきドキュメントを理解すること
- ❑ 情報システムを導入する工程の中で、セキュリティ機能を実装、運用するポイントを理解すること

主なキーワード

[BCP](#)（事業継続計画）、[CSIRT](#)（Computer Security Incident Response Team）、セキュリティ監査、セキュリティ管理

要旨

21 章の全体概要

21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントについて、EC サイトを例にとって説明しています。

21-1. EC サイトの構築とセキュリティ機能の実装と運用

EC サイトを例にとり、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を解説しています。

非機能要件のうちセキュリティに関する要件は、[リスクアセスメント](#)を実施して作成した適用宣言書をもとに決定します。

SaaS やパッケージソフトウェアを導入する際に非常に重要なプロセスである Fit&Gap 分析については、具体例を含めて解説しています。

訴求ポイント

章を通した気づき・学び

「デジタル・ガバメント推進標準ガイドライン」は、中小企業でも活用できる重要なことが数多く記載されています。情報システムを導入する際は、本ガイドラインを参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能です。

要件定義におけるセキュリティ要件は、組織で作成した適用宣言書をもとに決定することが重要です。情報資産におけるリスクを考慮して適切なセキュリティ要件を決めることで、情報システムのセキュリティ対策を強化することができます。

認識していただきたい実施概要

- 情報システムを導入する際は、「デジタル・ガバメント推進標準ガイドライン」を参考に、セキュリティ機能を実装すること。
- 要件定義では、適用宣言書をもとに情報資産におけるリスクを考慮し、適切なセキュリティ要件を決めること。

詳細理解のため参考となる文献（参考文献）	
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

27-22. 第 22 章. サイバーセキュリティ対策を実践するための知識とスキル

22-1. デジタルスキル標準 (DSS)

22-2. IT スキル標準 (ITSS)

22-3. ITSS+ (プラス)

22-4. i コンピテンシ ディクショナリ (iCD)

章の目的

技術進歩に伴い次々と新しい脅威が生まれている中で、効果的で漏れのないセキュリティ対策を実践していくためには、IT 全般のスキルや知識を持つ人材の育成と確保が重要です。第 22 章では、各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識について、体系的に理解することを目的とします。

主な達成目標

- 具体的な実施のために必要となる「役割やタスク」「スキルや知識」について、人材育成・人材確保のための各種スキル標準のフレームワークをもとに体系的に理解すること
- 各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること
- スキルや知識の認定制度と活用方法を理解すること

主なキーワード

デジタルスキル標準、DX リテラシー標準、IT スキル標準、ITSS+ (プラス)、i コンピテンシ ディクショナリ

要旨

22 章の全体概要

22 章では、サイバーセキュリティ対策を実践するために必要な知識とスキルについて解説しています。必要な知識とスキルを体系的に理解するために有用な [フレームワーク](#) として、デジタルスキル標準 (DSS) や IT スキル標準 (ITSS)、ITSS+ (プラス)、i コンピテンシ ディクショナリなどについて解説しています。

22-1. デジタルスキル標準 (DSS)

デジタルスキル標準は「DX リテラシー標準」と「DX 推進スキル標準」の2つの標準で構成されます。

「DX リテラシー標準」は、すべてのビジネスパーソンが身につけるべき DX に関する基礎的な知識、スキル、マインドセットの学習指針です。企業は、従業員に対して、DX に関するリテラシーを身につけさせるための指針として活用できます。

「DX 推進スキル標準」は、DX を推進する人材の役割（ロール）および必要なスキルを定義しています。

22-2. IT スkill標準（ITSS）

IT スkill標準（ITSS）は、IT 分野で必要とされるスキルや知識を体系化し、評価するための指標です。経済産業省が2002年に策定し、現在はIPAが管理しています。ITSSは、IT人材の育成に寄与することを目的としており、企業が共通して使用できるスキル指標を提供することで、キャリアパスの明確化やスキルの標準化に役立っています。

22-3. ITSS+（プラス）

ITSS+は、従来のIT スkill標準（ITSS）を拡張し、第4次産業革命に向けて求められる新たな領域の新しいスキルをカバーするために策定されました。対象となっている領域は、「[データサイエンス](#)領域」「[アジャイル](#)領域」「[IoT](#)ソリューション領域」「[セキュリティ](#)領域」の4つの領域です。

22-4. i コンピテンシ ディクショナリ（iCD）

i コンピテンシ ディクショナリ（iCD）は、組織においてIT を利活用するビジネスに求められる業務（タスク）と、それを支えるIT 人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものです。

※i コンピテンシ ディクショナリ（iCD）において、重要なことは考え方です。タスクやスキルについては、デジタルスキル標準を参照することが大切です。

訴求ポイント

章を通した気づき・学び

効果的なセキュリティ対策を実践するためには、IT 全般のスキルや知識を持つ人材の育成と確保が必要です。そのためには、各種スキル標準のフレームワークを活用することが有効です。

- デジタルスキル標準や IT スキル標準など各種フレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること。
- 各種スキル標準のフレームワークを活用し、効果的なセキュリティ対策を実践するために必要な IT 全般の知識やスキルを持つ人材を育成・確保すること。

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
IT スキル標準 V3 2011 1部：概要編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf
ITSS+（プラス）概要	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html
i コンピテンシディクショナリ解説書	https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf

27-23. 第 23 章. 人材の知識とスキルの認定制度

23-1. Di-Lite

23-2. 情報処理技術者試験

23-3. 国際セキュリティ資格

章の目的

第 23 章では、IT およびデジタル人材のスキル、知識の認定制度と活用方法を理解することを目的とします。認定制度は、従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段となります。

主な達成目標

- スキルや知識の認定制度と活用方法を理解すること

主なキーワード

Di-Lite、情報処理技術者試験、国際セキュリティ資格

要旨

23 章の全体概要

23 章では、IT およびデジタル人材の知識とスキルを認定する制度の意義と活用方法について解説しています。デジタルリテラシー協議会が提供する「Di-Lite」、情報処理技術者試験や国際セキュリティ資格について解説しています。認定制度は、従業員に IT や情報セキュリティの知識を身につけてもらうための有効な手段となります。

23-1. Di-Lite

「Di-Lite」とは、デジタルリテラシー協議会が定義する、すべてのビジネスパーソンが持つべきデジタル時代の共通リテラシーのことです。具体的には、以下の 3 つの領域に関するスキルや知識を指します。

- 1.IT・ソフトウェア領域：基本的な IT スキルやソフトウェアの使用方法
 - 2.数理・[データサイエンス](#)領域：データ分析や統計の基礎知識
 - 3.人工知能（[AI](#)）・ディープラーニング領域：AI 技術やディープラーニングの基礎知識
- これらのスキルを身につけることで、デジタル時代におけるビジネスの効率化や競争力の向上

が期待されています。

23-2. 情報処理技術者試験

情報処理技術者試験は、IT 分野の基礎から専門知識までをカバーする国家試験で、IPA が運用しています。情報処理技術者試験の受験は、従業員一人一人に IT や情報セキュリティの知識を身につけてもらうための有効な手段になります。

情報処理技術者試験は、初級から高度な IT スキルを持つ人材に対応しており、IT パスポート、基本情報技術者、応用情報技術者、そして情報処理安全確保支援士試験などの区分があります。

組織全体で従業員一人一人のセキュリティ意識を高めることは、組織の安全な運営に不可欠です。また、組織内のセキュリティ専門人材不足の問題の解消にも役立ちます。

23-3. 国際セキュリティ資格

情報セキュリティ分野における国際的な資格（CISSP や CISM、CISA）について説明しています。各情報処理技術者試験で培った IT 知識は、国際セキュリティ資格の学習の基礎となります。また、相乗効果の観点から国際セキュリティ資格の学習を通じて、各情報処理技術者試験の知識を深められたり、より高度な IT ポジションへのキャリアアップが期待できたりします。

訴求ポイント

章を通した気づき・学び

従業員一人一人に IT や情報セキュリティの知識を身につけてもらうためには、IT およびデジタル人材のスキル、知識の認定制度の活用が有効です。

認識していただきたい実施概要

- IT およびデジタル人材のスキルと知識の認定制度を理解すること。
- 情報処理技術者試験や国際資格など IT およびデジタル人材のスキル、知識の認定制度を活用し、人材育成に取り組むこと。

詳細理解のため参考となる文献（参考文献）	
Di-Lite	https://www.dilite.jp/
情報処理技術者試験 情報処理安全確保支援士 試験要綱	https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf
CISSP 8 ドメインガイドブック	https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部	https://www.isaca.gr.jp

27-24. 第 24 章. 各種人材育成カリキュラム

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1）】

24-3. マナビ DX

章の目的

第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を把握することを目的とします。紹介するカリキュラム内容は、具体的な実施計画や実施内容を検討する際の参考資料となります。

主な達成目標

- 「プラス・セキュリティ知識補充講座 カリキュラム例」のカリキュラム内容を理解すること
- 「IT スキル標準モデルカリキュラム」のカリキュラム内容を理解すること
- デジタルスキル習得に関する講座を紹介する「マナビ DX」について概要と活用方法を理解すること

主なキーワード

プラス・セキュリティ知識補充講座、IT スキル標準モデルカリキュラム、マナビ DX、デジタルスキル標準

要旨

24 章の全体概要

24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を解説しています。取り上げたものは、「プラス・セキュリティ知識補充講座 カリキュラム例」、「IT スキル標準モデルカリキュラム IT スキル標準 V3（レベル 1）」、デジタルスキル習得を支援する「マナビ DX」などです。

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

「プラス・セキュリティ知識補充講座」は、内閣サイバーセキュリティセンター（[NISC](#)）が提供するプログラムで、特に経営層や DX を推進する部課長向けに設計されています。この講座

は、企業内外のセキュリティ専門人材との協働を円滑に行うために必要な知識を補充することを目的としています。

具体的には、以下のように経営層向けとデジタル化推進部門の部課長級マネジメント層向けの2つのカリキュラムで構成されています。

24-2. ITスキル標準モデルカリキュラム【ITスキル標準 V3（レベル1）】

「ITスキル標準モデルカリキュラム」は、ITスキル標準のレベル1～3を目指す人向けのカリキュラムとしてIPAから公開されています。

レベル1向けのモデルカリキュラムは、職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラムであり、研修ロードマップをもとに、具体的な研修コースを設計・実施する際に参考となる情報がまとめられています。このモデルカリキュラムを履修することにより、ITスキル標準のレベル1に相当する知識を修得することができます。

24-3. マナビ DX

マナビ DX は、経済産業省とIPAが運営するデジタル人材育成のためのプラットフォームで、デジタルスキル習得に関する講座を紹介するポータルサイトになっています。デジタルスキルを学んだことのない人から、実践的なデジタル知識・スキルを身につけたい人まで、それぞれに適した講座を紹介してくれます。

マナビ DX は、無料や補助付きの講座を含み、リスキリングに重要なデジタルスキル習得をはじめの方に最適な初学者向け講座も提供されています。

訴求ポイント

章を通した気づき・学び

知識やスキルを備えた人材の育成・確保のためには、関係機関が公表しているセキュリティ関連のカリキュラム内容を活用し、実施計画を検討することが重要です。

認識していただきたい実施概要

- 「プラス・セキュリティ知識補充講座 カリキュラム例」や「ITスキル標準モデルカリキュラム ITスキル標準 V3（レベル1）」といった関係機関が公表しているセキュリティ関連のカリキュラム内容を把握すること。
- カリキュラム内容を参考に、具体的な実施計画や実施内容を検討すること。
- マナビ DX を活用し、デジタルスキルの向上を図ること。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
マナビ DX	https://manabi-dx.ipa.go.jp

27-25. 第 25 章. スキルと知識を持った人材育成・人材確保方法

25-1. 「プラス・セキュリティ」の実施計画例

25-2. 「リスキリング」「チェンジマインド」の実施計画例

章の目的

第 25 章では、カリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を理解することを目的とします。カリキュラムごとに、実践方法を例示します。

主な達成目標

- 「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること
- 「IT スキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること
- 「デジタルスキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること

主なキーワード

チェンジマインド、リスキリング、プラス・セキュリティ

要旨

25 章の全体概要

25 章では、既存のカリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を解説しています。

章の前半では、「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を解説しています。

章の後半ではリスキリングに有効と考えられるカリキュラムを例にして、リスキリングのための研修実施計画の策定手順について解説しています。

25-1. 「プラス・セキュリティ」の実施計画例

「プラス・セキュリティ知識補充講座 カリキュラム例」を実施するための手順を例示していま

す。セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていくことが必要です。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。昨今は AI を使った新しい攻撃手法が増加しており、昔のスキルや知識だけでは十分に対応することは困難です。

25-2. 「リスキリング」「チェンジマインド」の実施計画例

IT スキル標準、デジタルスキル標準など、リスキリングに有効と考えられるカリキュラムや指針を参考に、実施計画を策定する手順について例を使って解説しています。生成 AI などの新技術の普及により仕事が変わり、新たなスキルが求められる中、個人が競争力を維持するにはリスキリングが重要です。リスキリングを成功させるには、変化を受け入れるチェンジマインドを持ち、柔軟な思考で具体的な目標を設定し、信頼できる教材やカリキュラムを選び、自分にあった学習方法を見つけることが大切です。

訴求ポイント

章を通した気づき・学び

生成 AI など新しい技術が発展する中で、個人が市場で競争力を維持するためにはリスキリングによって最新のスキルと知識を習得することが重要です。

また、AI を活用した新たな攻撃に対応するため、既にセキュリティを担当している人も含め、新しい技術と考え方を学ぶ必要があります。

認識していただきたい実施概要

- 関係機関が公表しているカリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成し、実施すること。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準モデルカリキュラム－レベル 1 を目指して	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

第28章. 今後実施すべきこと

章の目的

テキストの内容を実践するにあたって行うべき事項を明確化し、具体的な行動計画が策定できるようになることを目的とします。これまで学んだ内容を活用し、自社のセキュリティ体制の向上や課題解決に向けた次のステップを提示します。

主な達成目標

- 学んだ内容をもとにして行動計画を策定できるようになること

28-1. 今後のアクション

本テキストでは、「DX 推進の必要性からセキュリティ対策の実施手順を策定する」ところまでを解説しました。この章では、本テキストの内容を実践するにあたって行うべき事項を列挙し、その概要を説明します。

本テキストの内容を実践するために行うべき事項

- テキストに記載された各章の理解を深め、重要なポイントを経営者も含めた関係者と共有すること
- 経営者のリーダーシップによって社内体制を整備すること
- 整備した社内体制において順次具体的なアクションを実践すること

テキストに記載された各章の理解を深め、重要なポイントを経営者も含めた関係者と共有すること

各章のポイントの理解

- テキストに記載された「セキュリティを考える上で必要となる社会情勢、国の施策に関する情報」、「セキュリティ対策を検討する上で必要となるセキュリティ知識」、「セキュリティ対策を実施するための具体的な手法」を再認識し、理解を深めること

DX 推進の考え方の把握

- 社会情勢、国の施策から DX 推進の方向性を知ること
中小企業においても DX 推進が不可欠です。
- 自組織における DX 推進のための人材育成の必要性を認識すること
DX を推進する人材（DX 推進スキル標準で示されたスキルを有する人材）や、DX を有効に利用できる人材（DX リテラシー標準で示されたスキルを有する人材（※プラス・セキュリティを含む））の確保が必要です。
- 自組織における DX 推進の計画を立案し実施内容を策定すること
DX 推進にあたっては DX with Security（DX の推進にあたり、セキュリティ対策を十分に考慮する）を意識することが重要です。
IT 構築にあたっては Security by Design（設計段階からのセキュリティ対策を考慮する）を意識するとともに「デジタル・ガバメント推進標準ガイドライン」を参考にすることが重要です。

「デジタル・ガバメント推進標準ガイドライン」は、中小企業でも活用できる重要なこと

が数多く記載されています。情報システムを導入する際に参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能になります。

セキュリティ対策の全容の認識

- サイバーセキュリティの脅威に対処するためのアプローチ手法としては「Lv.1 クイックアプローチ」「Lv.2 ベースラインアプローチ」「Lv.3 網羅的アプローチ」があり、それぞれメリット・デメリットがあること

例えば、ISMS などのフレームワークを用いた Lv.3 網羅的アプローチは、時間とコストがかかるというデメリットがあるものの、漏れのない対策が可能であるというメリットがあります。

- ISMS の仕組みや、管理策の全容を理解すること

自組織でのセキュリティ対策の実施項目の認識

- 自組織としての目標設定

自組織のリスクを、経営上および社会的に許容できる範囲まで低減させるセキュリティ対策を実践することが大切です。

- ① リスクアセスメントによって自組織の現状のリスクを把握する。
- ② リスクアセスメントの結果を踏まえ、管理策の中から自組織として実施すべき項目を選定する。
- ③ 実施する管理策に関して、自組織としての実施手順を策定する。

経営者のリーダーシップによって社内体制を整備すること

管理策の実施について

セキュリティポリシー関連文書の整備

組織全体で情報セキュリティを管理・運用するための基盤となるドキュメント（基本方針、対策基準、実施手順など）を作成します。それらを整備することで、セキュリティ対策の指針を明確にし、全社員が一貫した行動を取ることを可能にします。

実施手順の実行準備

実施手順として策定した内容を実行するため、実行性のあるドキュメント（仕様書、運用マニュアルなど）を作成します。

実施手順の実行

実施手順の実行にあたり、セキュリティ担当者とその役割・責任を決める必要があります。セキュリティ担当者とその役割・責任が決まった後、年間計画を作成してそれを実行します。

① 組織体制と役割の決定

セキュリティ対策を実施するための組織体制、役割・責任を決めます。

※13-2-3. ISMS : 5. リーダーシップ「5.3 組織の役割、責任及び権限」を参照。

② 年間を通して実行すべき事項の例示

担当者がその役割・責任において次のような事項を実施します。これらの事項を実行するため、年間計画を作成します。

※13-2-6. ISMS : 8. 運用「8.1 運用の計画及び管理」を参照。

・ リスクアセスメントの実施、リスク対応のための計画作成、管理策の検討 ・ 資産台帳の見直し ・ 事業継続に関する試験 ・ 内部監査 ・ マネジメントレビュー ・ 不適合及び是正処置のレビュー ・ 定期教育	・ 外部審査 ・ 情報セキュリティのための方針群のレビュー ・ 秘密保持契約書の確認 ・ 「関係当局との連絡」体制の見直し ・ 法令規制一覧表の確認 ・ 運用チェックリストによる確認 ・ 入退記録の確認 ・ など



上記の内容を実施するための年間計画を作成



年間計画（例）を紹介します。

期間	月	実施事項			
		年に1回	月に1回	四半期に1回	随時
第1四半期	4月	・課題に対する活動の検討	・入退記録の確認 ・運用チェックリストによる確認 ・バックアップされていることの確認 ・イベントログの確認 ・利用者が利用可能なソフトウェアの確認	・バックアップされていることの確認 ・イベントログのチェック	・「関係当局との連絡」体制の見直し ・法令規制一覧表の確認
	5月	・リスクアセスメントの実施	同上		
	6月	・リスク対応のための計画作成（アクションプランの作成） ・管理策（ルール）の検討	同上		
第2四半期	7月	・「情報セキュリティリスク対応」計画の実行	同上	同上	
	8月	・ISMSの有効性の評価 ・情報セキュリティパフォーマンス	同上		
	9月	・資産目録の見直し ・情報の分類 ・アクセス権限の見直し	同上		
第3四半期	10月	・システム開発の外部委託先の再審査	同上	同上	
	11月	・情報セキュリティ計画 ・情報セキュリティ継続の検証・レビュー	同上		
	12月	・内部監査計画 ・内部監査の実施 ・マネジメントレビュー ・不適合及び是正処置のレビュー	同上		
第4四半期	1月	・主要な従業員の「力量」の評価・証拠の文書化 ・定期教育 ・UPSのバッテリーの確認	同上	同上	
	2月	・外部審査（審査機関による更新審査）の実施	同上		
	3月	・情報セキュリティのための方針群のレビュー ・秘密保持契約書の確認	同上		

情報システム導入の実行について

情報システムの導入にあたり、重要なポイントを紹介します。

Fit&Gap 分析

Fit&Gap 分析は、SaaS やパッケージソフトウェアを導入する際に非常に重要なプロセスです。Fit&Gap 分析によって、[RFI](#) などの情報収集活動によって選定した SaaS やパッケージソフトウェアと、自社の業務要件との適合性を評価します。

Fit & Gap 分析の一般的な実施手順（例）

1. 現状分析
2. SaaS、パッケージソフトウェアの機能調査
3. 比較分析
4. ギャップへの対応策検討
5. 費用対効果の分析
6. 実施計画の策定

※「3.比較分析」は Fit & Gap 分析の中核をなす重要なステップです。

非機能要件における、セキュリティ要件の決め方

セキュリティに関する要件の決定は、適用宣言書をもとに行います。セキュリティ要件を決める流れは以下の通りです。

1. 情報システムで取扱う[情報資産](#)に対して、リスクアセスメントを実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。（適用宣言書の作成）
3. 適用宣言書の内容を満たすように、セキュリティ要件を決定する。

※リスクアセスメントの実施方法の詳細については、「12-2.リスクマネジメント：リスクアセスメント」を参照してください。

※セキュリティ要件の決め方の詳細については、「21-1-2.要件定義」の「非機能要件の定義」における「情報セキュリティに関する事項」を参照してください。

確立した社内体制において順次具体的なアクションを実施すること

管理策を実施するための参考となる情報

組織の中で具体的にどのように実施手順の内容を実践していくか、その際に参考となる各種資料や、実務的な取組例を紹介します。

管理策を実施するための参考となる情報	
ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド	https://isms-society.stores.jp/items/632a57a42e7452256400d84b
ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版	https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

実施手順を具体的に実施していくための取組例

実施手順を具体的に実施していくための取組例を紹介します。

以下は、実施手順を実際の業務として実施していくにあたり、実施手順と主体となって取り組む必要がある担当者に対応付ける例です。

対策基準（例）	5.2 情報セキュリティの役割及び責任	5.5 関係当局との連絡	6.7 リモートワーク	8.15 ログ取得
実施手順（例）	情報セキュリティ委員会を設置する。	関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。	社内ネットワークへはVPNにて接続する。	バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。
トップマネジメント（経営層）	○	—	○	—
情報セキュリティ委員会	—	○	○	—
情報システム管理者	—	—	○	○
一般社員	—	—	○	—

○：主体となって取り組む必要がある。

図 113. 実施手順とメインとなる担当者に対応付ける例

セキュリティ対策を考慮した情報システムを導入するために参考となる情報

セキュリティ対策を考慮した効果的な情報システムをどのように導入するか、その際に参考となる各種資料を紹介します。

セキュリティ対策を考慮した情報システムを導入するために参考となる情報	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf
安全なウェブサイトの作り方	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf
セキュリティ実装チェックリスト	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf
情報セキュリティサービス基準適合サービスリスト	https://www.ipa.go.jp/security/service_list.html
脆弱性診断 サービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_2.pdf
デジタルフォレンジック サービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_3.pdf
ウェブサイトの攻撃兆候検出ツール iLogScanner	https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

継続的な情報収集

本テキストに記載の「①国の方針、社会の現状と今後の動向」、「②IT 活用事例」、「③[セキュリティインシデント](#)事例」における内容は、日々更新されていきます。これらの情報を継続的に学ぶために参考となる文献を紹介します。

国の方針、社会の現状と今後の動向	
デジタルガバナンス・コード	https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html
経済財政運営と改革の基本方針 2024 について	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/2024_basicpolicies_ja.pdf
デジタル社会の実現に向けた重点計画	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
Society5.0	https://www8.cao.go.jp/cstp/society5_0
サイバーセキュリティ 2024 の概要	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf
<u>サイバーセキュリティ戦略</u> Cybersecurity for All 誰も取り残さないサイバーセキュリティ	https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
IT 活用事例	
中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
DX 白書 2023	https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
情報通信白書 令和 6 年版	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/00zentai.pdf
製造分野の DX 事例集	https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf
「DX Selection 2023」選定企業レポート	https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf
セキュリティインシデント事例	
情報セキュリティ白書 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/10threats2024.html

サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
サイバー攻撃を受けた組織における対応事例集 (実事例における学びと気づきに関する調査研究)	https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireis hu.pdf
コンピュータウイルス・不正アクセスの届出事例〔2023 年下半期(7 月～12 月)〕	https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h2-jirei.pdf
令和 4 年におけるサイバー空間をめぐる脅威の情勢等について (警察庁)	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-	https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf

人材育成

セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていける必要があります。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。また、AI や自動化などの新しい技術の導入が進んでいますが、これによって従来の仕事が変わり、新しいスキルが必要になります。中長期で見れば AI などの新技術の普及によって、一部の職業は消滅し、新しい職業が生まれることになるでしょう。そうした変化の中で、個人が市場で競争力を維持するためには、リスクリングを通じて最新の技術や知識を習得し、変化に対応できる能力を高めることが不可欠です。リスクリングを成功させるためには、チェンジマインド（変革思考）を持つことが非常に重要です。考え方を柔軟に変え、具体的な目標を設定するとともに、信頼できる教材やカリキュラムを選んで、自分にあった学習方法を見つけることが、リスクリング成功の秘訣だといえるでしょう。

今後のビジネス発展のためには、人材育成が不可欠となります。人材育成を実施するために参考となる文献を紹介します。

DSS に基づく人材育成	
デジタルスキル標準 Ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf

プラス・セキュリティ人材の育成	
「プラス・セキュリティ知識」について	https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf
サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き～ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第 1.1 版	https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekihontai1.1r.pdf
IT スキル標準に基づく人材育成	
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラムーレベル 1 を目指してー	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
その他	
マナビ DX	https://manabi-dx.ipa.go.jp
デジタル人材育成政策のご紹介	https://manabi-dx.ipa.go.jp/gov_assist
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html

編集後記

第10編では、中小企業におけるサイバーセキュリティ対策を全体的に取りまとめ、各章で取り上げた要点を振り返りつつ、本テキストの内容を実践するにあたって行うべき事項を列挙し、その概要を説明しました。本編では、DXの推進とサイバーセキュリティ対策の両立を目指し、経営層がリーダーシップを発揮して全社的な体制を整備する重要性を強調しています。

セキュリティ対策基準の策定方法として3つのアプローチ手法（クイック、ベースライン、網羅的）を提示し、企業が自らの状況に応じた対策を柔軟に選択できるよう解説しています。また、デジタル時代におけるIT投資のあり方として「守りのIT投資」と「攻めのIT投資」のバランスの重要性を示し、経営判断のもと、セキュリティ対策を経営戦略の一環として実施する必要性を明確にしました。

さらに、実際のインシデント事例や脅威情報を通じて、具体的な課題とその解決策を提示しました。これにより、企業が直面する現実的なリスクへの理解を深め、対策を効果的に実施するための土台を築くことを目指しています。

情報システムの導入にあたっては、本編で紹介した「デジタル・ガバメント推進標準ガイドライン」における中小企業でも活用できる重要な部分を参考にすることで、セキュリティ対策の実装や運用がより円滑に進むことが期待されます。

サイバーセキュリティは一過性の施策ではなく、継続的な改善と人材育成が不可欠です。本編で取り上げた知識や指針をもとに、読者の皆様が自社に最適なセキュリティ体制を構築し、持続的な運用・改善を実施されることを願っています。本テキストが、中小企業を含む社会全体のサイバーセキュリティの向上と、急速に変化するデジタル社会における競争力の強化、DX推進の一助となれば幸いです。

引用文献

Society 5.0

https://www8.cao.go.jp/cstp/society5_0

デジタルガバナンス・コード 2.0

https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html

SECURITY ACTION セキュリティ対策自己宣言

<https://www.ipa.go.jp/security/security-action>

情報セキュリティ 5 か条

https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf

5 分でできる！情報セキュリティ自社診断

<https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf>

情報セキュリティ基本方針（サンプル）

<https://www.ipa.go.jp/security/sme/f55m8k0000001wbv-att/000072146.docx>

経済財政運営と改革の基本方針 2024

<https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html>

デジタル社会の実現に向けた重点計画

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

サイバー・フィジカル・セキュリティ対策 フレームワーク Ver1.0

https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

中堅・中小企業等向けデジタルガバナンス・コード実践の手引き 2.0

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

製造分野の DX 事例集

<https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf>

サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ

<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf>

サイバーセキュリティ 2024

<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>

企業経営のためのサイバーセキュリティの考え方の策定について

<https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf>

IT およびサイバーセキュリティに関する組織の視点 6 分類

<https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/205/index.html>

「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは？

<https://www.gov-online.go.jp/useful/article/201703/1.html>

情報セキュリティ 10 大脅威の活用法 2024

https://www.ipa.go.jp/security/10threats/nq6ept000000g23i-att/katsuyouhou_2024.pdf

中小企業のためのセキュリティインシデント対応の手引き

<https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf>

【NISC】サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）

https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf

令和 5 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

令和 4 年通信利用動向調査の結果

https://www.soumu.go.jp/johotsusintokei/statistics/data/230529_1.pdf

CPS/IoT の利活用分野別世界市場調査の発表について

<https://www.jeita.or.jp/cgi-bin/topics/detail.cgi?n=3455&ca=1>

情報通信白書令和 3 年版（総務省）

<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf>

DX 白書 2023

<https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf>

攻めの IT 活用指針

https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf

DX レポート ～IT システム「2025 年の崖」の克服と DX の本格的な展開～

https://www.meti.go.jp/shingikai/mono_info_service/digital_transformation/pdf/20180907_03.pdf

中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki.pdf

「DX セレクション 2024」選定企業レポート（経済産業省）

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2024report.pdf

MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響

<https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html>

中小企業の情報セキュリティ対策ガイドライン 第 3.1 版

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf>

情報セキュリティポリシーの順守（総務省）

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/security/business/staff/12/

ISO/IEC TR 13335-1

<https://www.iso.org/standard/39066.html>

ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版

<https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOiJEWnZlI0fQ==&pNo=1>

ISO/IEC 27005

<https://www.iso.org/standard/80585.html>

2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-

<https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf>

リスク分析シート

<https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx>

情報セキュリティハンドブック（ひな形）

<https://www.ipa.go.jp/security/sme/ps6vr7000001bu88-att/000108033.pptx>

情報セキュリティ関連規程（サンプル）

<https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx>

ISMS/ITSMS/BCMS/CSMS 認証を取得するには

<https://www.jipdec.or.jp/project/smpo/ninsyou.html>

ISMS 適合性評価制度

<https://isms.jp/isms.html>

ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版

<https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd>

ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド

<https://isms-society.stores.jp/items/632a57a42e7452256400d84b>

ISMS-AC ISMS 適合性評価制度

<https://isms.jp/doc/JIP-ISMS120-62.pdf>

経済産業省 サイバーセキュリティ経営ガイドラインと支援ツール

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

経済産業省 クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性

<https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf>

JIPDEC「個人情報」と「プライバシー」の違い

<https://privacymark.jp/system/course/theme1/03.html>

ISMS-AC ISMS とは

<https://isms.jp/isms/>

デジタル庁 政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

経済産業省 サイバー・フィジカル・セキュリティ対策フレームワークの概要

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.pdf

経済産業省 サイバーセキュリティ経営ガイドライン Ver3.0

<https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf>

JISC 日本産業標準調査会 JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語

<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

JNSA. 2-4 リスクアセスメントとリスク対応

<https://www.jnsa.org/ikusei/01/02-04.html>

ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

アジャイル領域へのスキル変革の指針 アジャイル開発の進め方

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf>

EC サイト構築・運用セキュリティガイドライン

<https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf>

デジタルスキル標準 ver.1.2

<https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf>

生成 AI に関する DX 推進スキル標準の改訂 要旨 (2024 年 7 月)

https://www.ipa.go.jp/jinzai/skill-standard/dss/about_dss-p.html

Di-Lite とは

<https://www.dilite.jp>

G 検定とは

<https://www.jdla.org/certificate/general/#>

G 検定の試験範囲 (シラバス) と例題

https://www.jdla.org/certificate/general/#general_No03

IT スkill標準 V3 2011 1 部 : 概要編

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf>

IT スkill標準 V3 2011 2 部 : キャリア編

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf>

IT スkill標準 V3 2011 スkillディクショナリ_20120326

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf>

データサイエンティスト スkillチェックリスト Ver5.00

https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx

アジャイル領域へのスkill変革の指針

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065571.pdf>

IoT ソリューション領域へのスkill変革の指針 2021 改訂版

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/000065568.pdf>

ITSS+ (プラス) セキュリティ領域

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/security.html>

i コンピテンシディクショナリ解説書

https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf

情報処理技術者試験・情報処理安全確保支援士試験 試験要綱

https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf

CISSP 8 ドメインガイドブック

https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf

ISACA 東京支部

<https://www.isaca.gr.jp>

参考文献

SECURITY ACTION セキュリティ対策自己宣言

<https://www.ipa.go.jp/security/security-action>

情報セキュリティ 5 か条

https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf

5 分でできる！情報セキュリティ自社診断

<https://www.ipa.go.jp/security/sme/f55m8k0000001waj-att/000055848.pdf>

情報セキュリティ白書 2023

<https://www.ipa.go.jp/publish/wp-security/2023.html>

情報セキュリティ 10 大脅威 2024

<https://www.ipa.go.jp/security/10threats/10threats2024.html>

サイバー攻撃対応事例

<https://security-portal.nisc.go.jp/dx/provinatack.html>

リスク分析シート

<https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx>

セキュリティ関連費用の可視化

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html

中小企業の情報セキュリティ対策ガイドライン第 3.1 版

<https://www.ipa.go.jp/security/guide/sme/about.html>

ISMS 適合性評価制度

<https://isms.jp/isms.html>

セキュリティ関連 NIST 文書について

<https://www.ipa.go.jp/security/reports/oversea/nist/about.html>

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

<https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html>

セキュリティ関連知識の保管庫（ナレッジベース 2024）

<https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/>

サイバーセキュリティ 2024

<https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>

サイバーセキュリティ経営ガイドライン Ver 3.0

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

サイバーセキュリティお助け隊サービス制度

<https://www.ipa.go.jp/security/sme/otasuketai-about.html>

セキュリティ・キャンプ

<https://www.security-camp.or.jp>

ICSCoE 中核人材育成プログラム

https://www.ipa.go.jp/jinzai/ics/core_human_resource

情報セキュリティ 10 大脅威の活用法 2024

https://www.ipa.go.jp/security/10threats/nq6ept000000g23i-att/katsuyouhou_2024.pdf

中小企業等担当者向け テレワークセキュリティの手引き 第3版

https://www.soumu.go.jp/main_content/000816096.pdf

中小企業のためのセキュリティインシデント対応の手引き

<https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf>

コンピュータウイルス・不正アクセスの届出事例

<https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf>

マルウェア「ランサムウェア」の脅威と対策（対策編）

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

情報セキュリティ関連規程（サンプル）

<https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx>

自己点検チェックリスト

https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

情報セキュリティポリシーサンプル改版（1.0版）

<https://www.jnsa.org/result/2016/policy>

情報セキュリティハンドブック（ひな形）

<https://www.ipa.go.jp/security/sme/ps6vr7000001bu88-att/000108033.pptx>

インターネットの安全・安心ハンドブック Ver.5.00

<https://security-portal.nisc.go.jp/guidance/handbook.html>

テレワークセキュリティガイドライン第5版

https://www.soumu.go.jp/main_content/000752925.pdf

付録6：中小企業のためのクラウドサービス安全利用の手引き

<https://www.ipa.go.jp/security/sme/f55m8k0000001wcf-att/000072150.pdf>

The NIST Cybersecurity Framework（CSF）2.0

<https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>

Small Business Quick-Start Guide

<https://doi.org/10.6028/NIST.SP.1300>

A Guide to Creating Community Profiles

<https://doi.org/10.6028/NIST.CSWP.32.ipd>

Quick-Start Guide for Creating and Using Organizational Profiles

<https://doi.org/10.6028/NIST.SP.1301>

Quick-Start Guide for Using the CSF Tiers

<https://doi.org/10.6028/NIST.SP.1302.ipd>

Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)

<https://doi.org/10.6028/NIST.SP.1305.ipd>

Enterprise Risk Management Quick-Start Guide

<https://doi.org/10.6028/NIST.SP.1303.ipd>

CSF 2.0 Informative References

<https://www.nist.gov/informative-references>

CSF 2.0 Implementation Examples

<https://www.nist.gov/document/csf-20-implementations-pdf>

NIST Cybersecurity Framework (CSF) 2.0 Reference Tool

<https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters>

サイバー攻撃被害に係る情報の共有・公表ガイダンス

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

ISO/IEC 27002:2022

<https://www.iso.org/standard/75652.html>

ISMS 認証機関一覧

<https://isms.jp/lst/isr/index.html>

サイバーセキュリティ関連の法律・ガイドライン

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal

セキュリティ・バイ・デザイン導入指南書

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf

DS-200 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7e3e30b9/20240131_resources_standard_guidelines_guidelines_01.pdf

ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

(参考資料 1) 民間企業におけるゼロトラスト導入事例

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

証拠保全ガイドライン 第9版

<https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf>

DS-100 デジタル・ガバメント推進標準ガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_resources_standard_guidelines_guideline_01.pdf

DS-110 デジタル・ガバメント推進標準ガイドライン解説書

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9462b2d8/20240605_resources_standard_guidelines_guideline_03.pdf

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

DS-121 アジャイル開発実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9fc931f7/20220422_resources_standard_guidelines_guidebook_01.pdf

DS-130 標準ガイドライン群用語集

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/83a1ac09/20230331_resources_standard_guidelines_glossary_03.pdf

DS-201 政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事

業被害の組み合わせアプローチ～

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1b65a1dc/20230411_resources_standard_guidelines_guideline_01.pdf

DS-202 CI／CD パイプラインにおけるセキュリティの留意点に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/33f31336/20240329_resources_standard_guidelines_guideline_01.pdf

DS-210 ゼロトラストアーキテクチャ適用方針

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5efa5c3b/20220630_resources_standard_guidelines_guidelines_04.pdf

DS-211 常時リスク診断・対処（CRSA）のエンタープライズアーキテクチャ（EA）

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ef841b43/20240131_resources_standard_guidelines_guidelines_03.pdf

DS-212 ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/e5b49450/20230411_resources_standard_guidelines_guideline_03.pdf

DS-220 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

DS-221 政府情報システムにおける脆弱性診断導入ガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/7fefc9ee/20240206_resources_standard_guidelines_guidelines_01.pdf

DS-231 セキュリティ統制のカタログ化に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/9f746654/20230411_resources_standard_guidelines_guideline_01.pdf

nes_guideline_07.pdf

DS-310 政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/5167e265/20230929_resources_standard_guidelines_guideline_01.pdf

DS-400 政府相互運用性フレームワーク（GIF）

<https://github.com/JDA-DM/GIF>

DS-500 行政手続におけるオンラインによる本人確認の手法に関するガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/f1be078e/20220422_resources_standard_guidelines_guideline_07.pdf

DS-531 処分通知等のデジタル化に係る基本的な考え方

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d92a1cf2/20230411_resources_standard_guidelines_guideline_09.pdf

DS-910 安全保障等の機微な情報等に係る政府情報システムの取扱い

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/4d3bf58a/20230719_resources_standard_guidelines_guideline_01.pdf

【改定新版】特権 ID 管理ガイドライン

<https://www.jnsa.org/result/digitalidentity/2024/index.html>

アジャイル領域へのスキル変革の指針 アジャイル開発の進め方

<https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/00065606.pdf>

安全なウェブサイトの作り方

<https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf>

セキュリティ実装チェックリスト

<https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx>

EC サイト構築・運用セキュリティガイドライン

<https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf>

情報セキュリティサービス基準適合サービスリスト

https://www.ipa.go.jp/security/service_list.html
脆弱性診断サービス
https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_2.pdf
デジタルフォレンジックサービス
https://www.ipa.go.jp/security/ug65p90000019fc0-att/20241219_3.pdf
ウェブサイトの攻撃兆候検出ツール iLogScanner
https://www.ipa.go.jp/security/vuln/ilogscanner/index.html
デジタルスキル標準 ver.1.2
https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
マナビ DX
https://manabi-dx.ipa.go.jp
Di-Lite
https://www.dilite.jp
IT パスポート試験シラバス
https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014eh-att/syllabus_ip_ver6_3.pdf
データサイエンティスト検定 リテラシーレベルとは
https://www.datascientist.or.jp/dscertification/what
G 検定とは
https://www.jdla.org/certificate/general/#
G 検定の試験範囲（シラバス）と例題
https://www.jdla.org/certificate/general/#general_No03
IT スキル標準 V3 2011 1 部：概要編
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf
IT スキル標準 V3 2011 2 部：キャリア編
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024842.pdf
IT スキル標準 V3 2011 スキルディクショナリ_20120326
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024846.pdf
IT スキル標準 V 3 2011 3 部：スキル編
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024844.pdf

ITSS+（プラス）概要
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html
データサイエンティスト スキルチェックリスト Ver5.00
https://www.datascientist.or.jp/common/docs/skillcheck_ver5.00_simple.xlsx
データサイエンティストのためのスキルチェックリスト／タスクリスト概説
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001ity-att/00083733.pdf
アジャイル領域へのスキル変革の指針
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/00065571.pdf
IoT ソリューション領域へのスキル変革の指針 2021 改訂版
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i0x-att/00065568.pdf
サイバーセキュリティ体制構築・人材確保の手引き
https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
実践的サイバー防御演習「CYDER」（NICT）
https://cyder.nict.go.jp
実践サイバー演習「RPCI」（NICT）
https://rpci.nict.go.jp
目的や所属・役割から選ぶ施策一覧
https://security-portal.nisc.go.jp/curriculum/
情報処理技術者試験 情報処理安全確保支援士 試験要綱
https://www.ipa.go.jp/shiken/syllabus/nq6ept00000014lt-att/youkou_ver5_3.pdf
CISSP 8 ドメインガイドブック
https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部
https://www.isaca.gr.jp
デジタルスキル標準 ver. 1.2
https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/20240708-p-1.pdf
プラス・セキュリティ知識補充講座 カリキュラム例
https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準モデルカリキュラムーレベル1 を目指してー
https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/0000

24802.pdf
デジタルガバナンス・コード
https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html
Society5.0
https://www8.cao.go.jp/cstp/society5_0/
情報セキュリティ基本方針（サンプル）
https://www.ipa.go.jp/security/sme/f55m8k0000001wbv-att/000072146.docx
経済財政運営と改革の基本方針 2024
https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html
デジタル社会の実現に向けた重点計画
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き 2.0
https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0
https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook_2.pdf
企業経営のためのサイバーセキュリティの考え方の策定について
https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf
情報通信白書令和 3 年版（総務省）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf
DX 白書 2023
https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針
https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
中小企業の情報セキュリティ対策ガイドライン 第 3.1 版
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf
ISO/IEC TR 13335-1
https://www.iso.org/standard/39066.html

ISO/IEC 27005:2022
https://www.iso.org/standard/80585.html
ISMS-AC ISMS 適合性評価制度
https://isms.jp/doc/JIP-ISMS120-62.pdf
サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要
https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.pdf
サイバーセキュリティ経営ガイドライン Ver3.0
https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
リスクアセスメントとリスク対応
https://www.jnsa.org/ikusei/01/02-04.html
i コンピテンシディクショナリ解説書
https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf
IT スキル標準とは -ものさしとしてのスキル標準
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
デジタル人材育成政策のご紹介
https://manabi-dx.ipa.go.jp/gov_assist
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン
https://www.ipa.go.jp/security/anshin/measures/start.html
ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド
https://isms-society.stores.jp/items/632a57a42e7452256400d84b
ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版
https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
経済財政運営と改革の基本方針 2024
https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/2024_basicpolicies_ja.pdf
サイバーセキュリティ 2024 の概要
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf
情報通信白書 令和 6 年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/00zentai.pdf

製造分野の DX 事例集
https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf
「DX Selection 2023」選定企業レポート
https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf
サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）
https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
コンピュータウイルス・不正アクセスの届出事例〔2023 年下半期（7 月～12 月）〕
https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h2-jirei.pdf
令和 4 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集
https://www.ipa.go.jp/security/reports/sme/ug65p900000019djm-att/000098149.pdf
「プラス・セキュリティ知識」とは？
https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf
サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第 1.1 版
https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf

■AI

Artificial Intelligence の略。

「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。

昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第四次 AI ブームに入ったとの見方もある）。

「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている…………… [1-1](#)、[3-1](#)、[3-2-1](#)、[3-2-2](#)、[3-2-3](#)、[6-1-1](#)、[6-2-5](#)、[20-1-3](#)、[22-1-1](#)、[22-1-2](#)、[22-3-1](#)、[23-1](#)、[23-1-2](#)、[23-1-3](#)、[23-2](#)、[24-3](#)、[25-1](#)、[27-1](#)、[27-3](#)、[27-6](#)、[27-23](#)、[27-25](#)

■BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事

態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画…………… [11-5-1](#)、[27-21](#)

■CSIRT（シーサート）

Computer Security Incident Response Team の略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う…………… [4-1-1](#)、[5-1-3](#)、[11-5-1](#)、[11-5-3](#)、[22-3-4](#)、[23-2](#)、[27-21](#)

■CVSS

Common Vulnerability Scoring System の略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSS を用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門

家、管理者、ユーザなどの間で、脆弱性に関して共通の言葉で議論できるようになる…………… [18-3](#)、[23-2](#)

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法…………… [第 2 章コラム](#)、[5-2-2](#)、[5-2-5](#)、[8-1-1](#)

■DFFT

Data Free Flow with Trust の略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している…………… [3-2-1](#)

■EDR

Endpoint Detection and

Response の略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する
..... [2-1](#)、[5-2-4](#)、[5-2-5](#)、[10-2-4](#)、[17-3-1](#)、[18-3-5](#)、[22-3-1](#)、[26-1](#)、[26-2](#)、[27-2](#)

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
..... [3-2-1](#)

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる
..... [3-2-1](#)

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政

法人情報処理推進機構 (IPA) 内に設置された産業サイバーセキュリティセンター (Industrial Cyber Security Center of Excellence, ICSCoE) が実施している人材育成プログラム。制御技術 (OT : Operational Technology) と情報技術 (IT) の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている
..... [5-1-2](#)

■ICT

Information and Communication Technology の略。IT (情報技術) に加えて、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術 (通信技術) を含んでいる
..... [3-2-1](#)、[6-1-2](#)、[13-3-2](#)、[15-1](#)、[15-2-6](#)、[15-2-7](#)、[18-3-2](#)、[27-6](#)、[27-15](#)

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常

な通信をブロックする機能はない

..... [18-2-10](#)、[18-2-14](#)、[18-2-18](#)、[18-3-5](#)、[18-4](#)、[22-3-1](#)

■IoT (アイ・オー・ティー)

Internet of Things の略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

..... [1-1](#)、[3-1](#)、[3-2-2](#)、[3-2-3](#)、[4-2-1](#)、[4-3-3](#)、[5-2-2](#)、[6-1-1](#)、[6-2-5](#)、[11-4](#)、[22-1-2](#)、[22-3](#)、[22-3-3](#)、[23-1-1](#)、[23-2](#)、[23-2-4](#)、[24-3](#)、[25-2-2](#)、[27-3](#)、[27-5](#)、[27-6](#)、[27-22](#)

■IPS

Intrusion Prevention System の略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

..... [5-2-2](#)、[1](#)

[8-2-10](#)、[18-2-14](#)、[18-3-2](#)、[18-3-5](#)、[18-4](#)

■IP アドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。IP アドレスは、127.0.0.1 のように 0～255 までの数字を 4 つ組み合わせたもので、単にアドレスと略されることがある。現在主に使用されているこれら 4 つになる数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量に IP アドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6 では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている
…………… [5-3-2](#)、[18-3-2](#)、[21-1-2](#)

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携を図る組

織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

…………… [15-2-2](#)

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取組。組織が ISMS を構築するための要求事項をまとめた国際規格が ISO/IEC 27001（国内規格は JIS Q 27001）であり、審査機関の審査に合格すると「ISMS 認証」を取得できる

…………… [2-3](#)、[7-1-2](#)、[11-1-1](#)、[11-1-2](#)、[11-2-11-3-1](#)、[11-3-3](#)、[11-4](#)、[11-5-1](#)、[12-1-3](#)、[12-2-1](#)、[12-2-2](#)、[13-1](#)、[13-2-1](#)、[13-2-2](#)、[13-2-3](#)、[13-2-4](#)、[13-2-5](#)、[13-2-6](#)、[13-2-7](#)、[13-2-8](#)、[13-3-1](#)、[13-3-2](#)、[13-4-1](#)、[13-4-2](#)、[13-4-3](#)、[13-4-4](#)、[14-1-1](#)、[14-1-3](#)、[15-1](#)、[16-1](#)、[1](#)

[7-1](#)、[17-2-1](#)、[18-1](#)、[19-1](#)、[21-1-2](#)、[23-1-1](#)、[23-2](#)、[25-2-1](#)、[25-2-2](#)、[26-1](#)、[26-2](#)、[27-7](#)、[27-8](#)、[27-11](#)、[27-12](#)、[27-13](#)、[27-14](#)、[28-1](#)

■ISP

個人や企業などに対してインターネットに接続するためのサービスを提供する事業者のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる
…………… [15-2-7](#)

■IT リテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…………… [23-2](#)、[25-1](#)

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行っている組織。政府機関や企業な

どから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる

…………… [15-2-1](#)、
[15-2-2](#)

■ JVN

Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと

…………… [15-2-2](#)

■ KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの

…………… [20-1-2](#)、
[20-1-8](#)、[20-1-9](#)、[21-1-5](#)、
[23-1-2](#)

■ MAC アドレス

Media Access Control address の略。隣接する機器同士の間で通信を実現するためのアドレスのこと。ネットワーク機

器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

…………… [18-3-2](#)

■ NISC

National center of Incident readiness and Strategy for Cybersecurity の略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

…………… [2-3](#)、[3-2-1](#)、[4-1](#)、[4-1-1](#)、[4-1-2](#)、[10-2-1](#)、[22-3-4](#)、[24-1](#)、[26-2](#)、
[27-4](#)、[27-10-2](#)、[27-24](#)

■ NIST サイバーセキュリティフレームワーク (CSF)

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている。日本においても、今後普及が見込まれる

…………… [2-3](#)、[11-1-1](#)、[11-3-1](#)、[11-3-2](#)、[11-3-3](#)、[11-4](#)、[13-3-2](#)、[14-1-2](#)、

[20-1-1](#)、[21-1-2](#)、[26-1](#)、[27-11-1](#)

■ NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

…………… [18-2-15](#)

■ PII

Personally Identifiable Information の略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と 1 対 1 に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号に加えて、氏名、生年月日、住所、勤務先などの情報も PII に含まれる

…………… [13-3-2](#)、
[15-1](#)、[15-2-8](#)、[27-15](#)

■ PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管

理を行うチームや担当者を指す。

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

…………… [20-1-1](#)、[20-1-2](#)、[20-1-3](#)、[20-1-6](#)、[20-1-7](#)、[20-1-8](#)、[20-1-9](#)、[20-1-10](#)

■PMO

Project Management Office の略。(企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。)組織全体のプロジェクトを横断的に管理する体制を指す。

政府ガイドラインでのPMOは、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる。

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う(例:計画、予算、執行管理、PJMO 支援など)

…………… [20-1-3](#)

■RFI

Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること

…………… [20-1-1](#)、[20-1-5](#)、[21-1-2](#)、[28-1](#)

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

…………… [6-2-5](#)

■SASE (サシー)

Secure Access Service Edge の略。令和元年に提唱されたゼロトラストセキュリティを実現する方法の1つで、IT 環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

…………… [5-2-4](#)、[18-3-3](#)、[27-18](#)

■SDP

Software-Defined Perim

eter の略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPN は、ネットワーク接続前に一度だけ認証を行うのに対し、SDP は、ユーザーの情報(デバイス、場所、OS など)など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

…………… [5-2-5](#)、[18-3-2](#)、[18-3-5](#)

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

…………… [2-2-1](#)、[第4章編集後記](#)、[5-1-2](#)、[11-5-1](#)、[26-2](#)、[27-2](#)

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

…………… [18-2-18](#)、[22-2-2](#)

■Society5.0

日本が目指すべき未来社会の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

…………… [1-1](#)、[3-2-2](#)、[4-1-1](#)、[6-1-1](#)、[11-1-1](#)、[11-1-2](#)、[11-4](#)、[22-1-1](#)、[22-3-2](#)、[26-2](#)、[27-1](#)、[27-3](#)、[27-6](#)、[28-1](#)

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなっている。しかし、歴史的経緯で SSL の用語が広く普及している

ため、本テキストでは「SSL/TLS」と表記しています

…………… [15-2-1](#)、[18-2-21](#)、[22-3-1](#)、[23-2](#)

■SWG

Secure Web Gateway の略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することによりセキュアな通信環境を実現

…………… [5-2-4](#)、[18-3-2](#)、[18-3-3](#)、[18-3-5](#)

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

…………… [5-1-3](#)、[5-2-2](#)、[5-2-5](#)、[5-3-1](#)、[5-3-](#)

[2](#)、[5-3-3](#)、[10-2-2](#)、[15-2-1](#)、[16-2-6](#)、[17-3-1](#)、[18-3-2](#)、[18-3-4](#)、[25-2-1](#)

■WAF（ワフ）

Web Application Firewall の略。従来のファイアウォールが、IP アドレスとポート番号で通信を制御していたことに対して、Web アプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと

…………… [5-2-2](#)、[21-1-2](#)、[21-1-3](#)、[21-1-5](#)、[21-1-6](#)、[23-2](#)

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者

依頼する必要がある

…………… [18-3-4](#)、
[22-1-1](#)

■アクセス制御

特定のデータやファイル、
コンピュータ、ネットワーク
にアクセスできるユーザーを
制限する機能のこと

…………… [2-3](#)、[第2章コラム](#)、[5-2-5](#)、[8-1-1](#)、[11-3-1](#)、[12-3](#)、[13-3-2](#)、[15-1](#)、[15-2-1](#)、[15-2-3](#)、[18-1](#)、[18-3-2](#)、[18-3-5](#)、[20-1-1](#)、[21-1-2](#)、[23-2](#)、[27-15](#)、[27-18](#)

■アセスメント

システムや運用環境などを
客観的に調査・評価すること。
現在の利用状況を把握すること
により、システムの再構築
や運用改善の参考情報となる

…………… [5-2-4](#)、[12-2-2](#)、[18-1](#)

■暗号化

データの内容を変換し、第
三者には、内容を見ても解読
できないようにすること

…………… [2-2-3](#)、[2-3](#)、[第2章コラム](#)、[5-1-3](#)、[5-2-1](#)、[5-2-5](#)、[5-3-1](#)、[5-3-2](#)、[8-1-1](#)、[9-2](#)、[10-2-2](#)、[13-3-1](#)、[13-3-2](#)、[15-2-1](#)、[15-2-7](#)、

[17-2-5](#)、[17-2-6](#)、[18-2-1](#)、[18-2-10](#)、[18-2-18](#)、[18-2-21](#)、[18-3-4](#)、[18-4](#)、[21-1-2](#)、[22-3-1](#)、[23-1-2](#)、[25-2-1](#)、[25-2-2](#)

■アンダーグラウンドサービス

合法ではない非公式な活動
が行われるオンラインの闇市
場やコミュニティでサイバー
攻撃を目的としたツールなど
を販売しているサービス

…………… [5-1-3](#)

■イベントログ

コンピュータシステムに起
こった出来事や、行われた操
作などを時系列に記録したデ
ータのこと

…………… [13-2-6](#)、
[18-2-15](#)

■インターネットバンキング

インターネットを利用して
銀行との取引を行うサービスの
こと。銀行の窓口やATMに
出向かなくても、スマートフ
ォンやパソコンなどを使って、
いつでも利用可能な時間帯に
振り込みや残高照会などの取
引を行うことができる

…………… [2-2-2](#)、[12-1-2](#)

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェア
がマルウェアを検出するた
めの定義情報が入ったファイル。
実世界でいえば顔写真つきの
手配書のようなもの

…………… [2-1](#)、[2-2-2](#)、[2-2-3](#)、[10-2-2](#)、[10-2-3](#)、
[10-2-4](#)

■エンティティ

個人、組織、団体、コンピ
ュータシステム、通信機器など、
多様な実体のこと

…………… [11-2](#)、[18-3-2](#)

■エンドポイントデバイス

ネットワークに接続して、
ネットワークを介して情報を
交換するデバイス（パソコン、
プリンタ、スキャナ、スマート
フォン、仮想マシン、サーバ、
IoT デバイスなど）

…………… [5-2-4](#)、[18-1](#)、[18-3-2](#)、[18-3-5](#)、[27-18](#)

■改ざん

文書や記録などのすべてま
たは一部に対して、無断で修
正・変更を加えること。IT 分

野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

..... [3-2-2](#)、[4-1-1](#)、[4-2-2](#)、[7-1-2](#)、[8-1-1](#)、[8-1-2](#)、[10-2-5](#)、[12-2-2](#)、[15-1](#)、[15-2-5](#)、[15-2-7](#)、[15-2-8](#)、[18-2-11](#)、[18-2-13](#)、[18-2-17](#)、[18-3-4](#)、[21-1-2](#)、[21-1-5](#)、[22-1-1](#)、[22-3-1](#)、[25-2-1](#)、[25-2-2](#)、

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

..... [第 2 章コラム](#)、[8-1-1](#)、[8-1-2](#)、[第 8 章コラム](#)、[9-2](#)、[11-1-2](#)、[11-2](#)、[12-2-2](#)、[13-2-4](#)、[13-2-5](#)、[13-3-2](#)、[14-1-2](#)、[15-1](#)、[15-2-6](#)、[15-2-7](#)、[17-1](#)、[18-1](#)、[18-2-12](#)、[18-2-17](#)、[18-3-5](#)、[20-1-9](#)、[21-1-2](#)、[22-2-2](#)、[22-3-1](#)、[22-4-1](#)、[23-2](#)、[25-2-2](#)、[27-11](#)、[27-12](#)

■完全性

参照する情報が改ざんされていない、正確である特性

..... [第 2 章コラム](#)、[8-1-1](#)、[第 8 章コラム](#)、

[9-2](#)、[11-1-2](#)、[11-2](#)、[12-2-2](#)、[13-2-4](#)、[13-2-5](#)、[13-3-2](#)、[14-1-2](#)、[15-1](#)、[17-1](#)、[18-2-17](#)、[18-2-21](#)、[18-3-5](#)、[20-1-9](#)、[21-1-2](#)、[22-3-1](#)、[23-2](#)、[25-2-2](#)、[27-11](#)、[27-12](#)

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

..... [第 2 章コラム](#)、[7-1-2](#)、[8-1-1](#)、[第 8 章コラム](#)、[9-2](#)、[11-1-2](#)、[11-2](#)、[12-2-2](#)、[13-2-4](#)、[13-2-5](#)、[13-3-2](#)、[14-1-2](#)、[15-1](#)、[17-1](#)、[18-2-17](#)、[18-2-21](#)、[18-3-5](#)、[20-1-6](#)、[20-1-9](#)、[21-1-2](#)、[22-3-1](#)、[23-2](#)、[25-2-2](#)、[27-7](#)、[27-11](#)、[27-12](#)

■脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている

..... [13-3-2](#)、[15-1](#)、[15-2-2](#)、[18-3-1](#)、[22-1-2](#)、[27-15](#)

■供給者

組織に対して、製品・サービスを提供する企業または個人のこと。製品の場合、PC やサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある

..... [13-3-2](#)、[14-1-2](#)、[15-1](#)、[15-2-1](#)、[15-2-6](#)、[15-2-7](#)、[15-2-9](#)、[18-3-1](#)、[18-3-2](#)、[27-15](#)

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

..... [第 2 章コラム](#)

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

..... [18-4](#)

■限定提供データ

不正競争防止法で次のよう

に定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によつては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

…………… [12-2-2](#)

■コーディング

プログラミング言語でソースコードを書くこと

…………… [13-3-2](#)、
[18-1](#)、[18-2-17](#)、[18-3-1](#)、[20-1-3](#)、[23-1-2](#)、[27-18](#)

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行

っている

…………… [3-2-1](#)、[4-3-1](#)、[5-2-3](#)、[7-1-2](#)、[15-2-1](#)、[15-2-2](#)

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

…………… [20-1-7](#)

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまでさまざまである。デジタル社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

…………… [0-1-1](#)、[0-1-2](#)、[0-1-3](#)、[2-1](#)、[2-3](#)、[3-2-2](#)、[3-2-3](#)、[4-1-1](#)、[4-1-2](#)、[4-2-1](#)、[4-2-2](#)、[5-1-2](#)、[5-1-3](#)、[5-2-2](#)、[5-2-5](#)、[5-3-1](#)、[5-3-2](#)、[6-3-1](#)、[6-3-2](#)、[第6章](#) [編集後記](#)、[10-2-3](#)、[10-2-6](#)、

[11-1-1](#)、[11-1-2](#)、[11-4](#)、[11-5-1](#)、[11-5-2](#)、[11-5-3](#)、[12-2-2](#)、[13-2-4](#)、[13-2-5](#)、[18-3-2](#)、[18-3-4](#)、[18-3-5](#)、[19-2](#)、[21-1-2](#)、[22-1-2](#)、[22-3-1](#)、[22-3-4](#)、[23-2](#)、[24-3](#)、[25-1](#)、[25-2-2](#)、[26-1](#)、[27-1](#)、[27-3](#)、[27-5](#)、[27-6](#)、[27-11](#)、[27-19](#)、[27-25](#)、[28-1](#)

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

…………… [5-1-2](#)

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

…………… [2-3](#)、[3-1](#)、[4-1](#)、[4-1-1](#)、[4-1-2](#)、[26-1](#)、

[26-2](#)、[27-4](#)、[28-1](#)

■サイバー・フィジカル・セキュリティ対策フレームワーク (CPSF)

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

…………… [2-3](#)、[11-1-1](#)、[11-1-2](#)、[11-4](#)、[27-11](#)

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

…………… [3-2-2](#)、[4-1-1](#)、[4-1-2](#)、[4-2-1](#)、[4-2-2](#)、[5-1-3](#)、[5-2-4](#)、[5-3-1](#)、[6-1-1](#)、[6-2-4](#)、[6-3-2](#)、第 6 章編集後記、[11-3-1](#)、[11-3-2](#)、[11-4](#)、[11-5-1](#)、[11-5-2](#)、[13-3-2](#)、[27-3](#)、[27-5](#)、[27-11](#)

■サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022 では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調を挙げている

…………… [13-3-2](#)、[15-2-1](#)、[17-1](#)、[17-2-6](#)、[27-17](#)

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

…………… [18-2-9](#)

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

…………… [20-1-1](#)

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業

が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

…………… [17-3-1](#)、[18-3-2](#)

■情報資産

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

…………… [2-2-4](#)、[2-3](#)、[7-1-2](#)、[8-1-1](#)、[9-2](#)、[11-3-1](#)、[11-5-1](#)、[12-1-1](#)、[12-1-2](#)、[12-2-2](#)、[12-2-3](#)、第 6 編編集後記、[13-2-3](#)、[13-2-4](#)、[13-2-5](#)、[13-4-2](#)、第 13 章コラム、[15-2-6](#)、[17-2-1](#)、[18-3-2](#)、[18-3-5](#)、[19-2](#)、[21-1](#)、[21-1-2](#)、第 8 編編集後記、[23-1-1](#)、[23-2](#)、[23-2-1](#)、[24-3](#)、[25-2-1](#)、[27-8](#)、[27-12](#)、[27-15](#)、[27-17](#)、[27-19](#)、[27-21](#)、[28-1](#)

■情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。

情報セキュリティ事象の中

でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される

…………… [13-3-2](#)、[14-1-2](#)、[15-1](#)、[15-2-1](#)、[15-2-5](#)、[16-1](#)、[16-2-7](#)、[18-2-17](#)、[18-3-5](#)、[27-15](#)、[27-16](#)

■情報セキュリティの3要素「CIA」

情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

…………… [第2章コラム](#)、[第8章コラム](#)

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

…………… [第2章コラム](#)、[4-2-2](#)、[第8章コラム](#)、[11-2](#)、[18-2-21](#)、[21-1-2](#)

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

…………… [1-1](#)、[2-2-3](#)、[第2章コラム](#)、[3-2-1](#)、[4-1-1](#)、[4-2-2](#)、[第8章コラム](#)、[11-1-1](#)、[11-2](#)、[11-4](#)、[13-2-5](#)、[15-2-7](#)、[18-2-15](#)、[20-1-5](#)、[20-1-7](#)、[21-1-2](#)、[21-1-3](#)、[22-1-2](#)、[22-2-2](#)、[23-2-4](#)、[23-3-3](#)、[25-2-2](#)

■スクリーンセーバ

離席時にPCの画面の内容を盗み見されることを防ぐ機能のこと。PCに対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

…………… [13-2-5](#)、[18-2-1](#)

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

…………… [5-2-2](#)、[1](#)

[7-2-4](#)

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

…………… [2-1](#)、[2-3](#)、[第2章コラム](#)、[5-1-2](#)、[5-1-3](#)、[5-2-1](#)、[5-2-2](#)、[5-2-4](#)、[5-2-5](#)、[5-3-1](#)、[5-3-2](#)、[5-3-3](#)、[8-1-1](#)、[8-1-2](#)、[8-1-3](#)、[第3編編集後記](#)、[12-1-2](#)、[12-2-2](#)、[12-2-3](#)、[12-3](#)、[13-3-1](#)、[13-3-2](#)、[14-1-2](#)、[15-2-1](#)、[18-1](#)、[18-2-7](#)、[18-2-17](#)、[18-2-21](#)、[18-3-1](#)、[18-3-5](#)、[20-1-1](#)、[20-1-3](#)、[20-1-5](#)、[21-1-2](#)、[21-1-5](#)、[22-1-2](#)、[23-1-1](#)、[23-2](#)、[23-2-5](#)、[24-1](#)、[24-1-1](#)、[24-1-2](#)、[25-2-1](#)、[25-2-2](#)、[26-1](#)、[26-2](#)、[27-5](#)、[27-8](#)、[27-18](#)

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

…………… [18-3-1](#)、[20-1-1](#)、[21-1-2](#)、[21-1-5](#)、[28-1](#)

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

…………… [第 2 章コラム、第 8 章コラム、11-2](#)

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

…………… [2-1、5-1-1、5-1-2、5-1-3、5-2-1、6-3-2、9-1、9-2、第 9 章編集後記、11-3-1、11-5-1、13-2-2、13-2-4、13-2-5、13-2-8、13-3-2、14-1-2、15-1、15-2-1、15-2-4、15-2-5、18-1、18-2-13、18-3-1、18-3-5、18-4、20-1-8、20-1-9、21-1-2、22-1-2、22-3-1、23-1-1、23-2-1、23-2-5、24-1-1、25-2-2、26-1、26-2、27-9、27-15、27-18-4、28-1](#)

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通

過した 22 歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、独立行政法人情報処理推進機構 (IPA) と (一財) セキュリティ・キャンプ協議会が実施している

…………… [5-1-2](#)

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

…………… [2-3、5-1-3、8-1-1、第 9 章編集後記、10-2-3](#)

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載することが一般

的

…………… [2-3、4-2-1、5-1-1、5-2-1、7-1-1、8-1-1、第 3 編編集後記、11-5-1、18-3-5、20-1-5、20-1-6、21-1-2、21-1-3、22-3-1、23-2、23-2-1、25-2-1、25-2-2、26-2、27-7、28-1](#)

■ゼロデイ攻撃

OS やソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

…………… [5-1-3](#)

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

…………… [5-2-4、17-3-2、18-3-2、18-3-3、20-1-1、22-3-1、27-18](#)

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再

利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

..... [18-1](#)

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」

..... [15-2-2](#)、[18-2-18](#)、[18-3-2](#)、[18-3-5](#)、[20-1-5](#)、[21-1-2](#)、[22-2-2](#)、[22-2-3](#)、[22-3-1](#)、[23-1-1](#)、[24-1-2](#)、

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開の Web サイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

..... [5-1-3](#)

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせることで認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広がっている

..... [5-1-3](#)、[5-2-5](#)、[5-3-3](#)、[7-1-2](#)、[第8章コラム](#)、[10-2-2](#)、[12-3](#)、[15-2-7](#)、[18-2-4](#)、[18-3-2](#)、[23-2](#)

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

..... [1-1](#)、[22-1-2](#)、[22-3](#)、[22-3-1](#)、[23-1](#)、[23-1-2](#)、[24-3](#)、[27-22](#)、[27-23](#)

■データーマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする

..... [13-3-2](#)、[18-1](#)、[18-2-10](#)、[27-18](#)

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタルライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタルライゼーションである

..... [1-1](#)、[3-1](#)、[3-2-1](#)、[4-1-1](#)、[4-2-2](#)、[5-1-2](#)、[6-1-2](#)、[6-2-4](#)、[11-4](#)、[20-1-1](#)、[22-1-2](#)、[24-1](#)、[24-1-](#)

[2、24-2、26-1、27-3、27-4、27-6、27-24](#)

■デジタル情報

0、1、2のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の2進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

…………… [第2章コラム](#)

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

…………… [20-1-7](#)

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

…………… [2-1、18-3-2、18-3-4、22-3-1](#)

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する

国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する

…………… [2-3、11-2、13-2-3、13-2-6、13-2-7、13-2-8、13-4-2、15-2-1、15-2-9、19-1、20-1-10、26-2、27-19](#)

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある

…………… [10-2-6](#)

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

…………… [15-2-6](#)

■ビジネスメール詐欺

攻撃者がビジネス用のメー

ルを装い、企業の担当者だまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromise とも略される

…………… [5-1-3](#)

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

…………… [1-1、3-2-2、3-2-3](#)

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

…………… [第2章コラム、第8章コラム](#)

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者へ送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

..... [5-1-2](#)、[5-1-3](#)、[13-2-5](#)、[23-2](#)

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

..... [13-2-5](#)、[27-5](#)

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

..... [2-1](#)、[8-1-1](#)、[15-2-1](#)、[15-2-2](#)、[18-2-10](#)、[18-2-14](#)、[18-2-18](#)、[18-2-19](#)、[18-3-2](#)、[18-3-5](#)、[18](#)

[-4](#)、[20-1-5](#)、[21-1-2](#)、[22-3-1](#)、[23-2](#)、[25-2-1](#)

■ファイル共有ソフト

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある

..... [17-3-1](#)、[18-2-10](#)、[18-2-17](#)

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

..... [5-2-3](#)、[18-4](#)、[21-1-2](#)、[22-1-2](#)、[22-2-3](#)、[23-2](#)、[28-1](#)

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

..... [3-2-1](#)、[4-3-3](#)、[5-1-1](#)、[5-1-3](#)、[5-2-1](#)、[5-2-2](#)、[5-2-3](#)、[5-2-5](#)、[5-3-1](#)、[6-3-2](#)、[7-1-2](#)、[8-1-1](#)、[8-1-3](#)、[12-2-2](#)、[12-3](#)、[15-2-1](#)、[15-2-5](#)、[15-2-7](#)、[17-3-1](#)、[18-2-4](#)、[18-2-10](#)、[18-2-11](#)、[18-2-13](#)、[18-2-17](#)、[18-3-5](#)、[18-4](#)、[20-1-5](#)、[21-1-2](#)、[21-1-5](#)、[22-3-1](#)、[23-1-1](#)、[23-2](#)、[25-2-1](#)、[27-5](#)、[28-1](#)

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵

入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

…………… [5-1-3](#)、[1-9-2](#)

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

…………… [0-1-2](#)、[2-3](#)、[4-1-1](#)、[5-2-4](#)、[7-1-1](#)、[7-1-2](#)、[第5編編集後記](#)、[11-1-1](#)、[11-1-2](#)、[11-2](#)、[11-3-1](#)、[11-4](#)、[第6編編集後記](#)、[13-1](#)、[14-1-2](#)、[20-1-1](#)、[22-2-2](#)

[25-2-1](#)、[26-1](#)、[26-2](#)、[27-7](#)、[27-11](#)、[27-13](#)、[27-22](#)、[28-1](#)

■プロキシ

クライアントとサーバの間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Webサーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

…………… [18-3-5](#)、[25-2-1](#)

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する、オープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

…………… [1-1](#)、[22-3-1](#)、[25-2-2](#)

■ペネトレーションテスト

ネットワークに接続された

システムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する…………… [18-3](#)、[23](#)

[-2](#)

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

…………… [5-1-3](#)、[5-3-1](#)、[11-1-1](#)、[11-3-1](#)、[27-5](#)

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

…………… [20-1-1](#)、[21-1](#)、[21-1-1](#)

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施するこ

とができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

…………… [20-1-6](#)

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

…………… [2-1、第2章コラム、5-2-2、5-2-4、5-2-5、8-1-1、10-2-4、12-2-2、13-2-4、13-3-1、13-3-2、15-2-2、15-2-4、16-2-6、17-3-1、18-1、18-2-6、18-2-20、18-3-2、18-3-5、21-1-2、22-3-1、22-3-4、23-2、23-2-5、27-18](#)

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

…………… [18-3-1、18-3-4、20-1-3、21-1-2](#)

■ミラサポコネク

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネク構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

…………… [3-2-1](#)

■無線 LAN

LAN は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線 LAN を通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

…………… [2-2-3、15-2-1、17-2-4、18-2-18、18-2-21](#)

■無停電電源装置

UPS と呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハー

ドディスク、サーバなどを予期せぬ停電から守れる

…………… [15-2-1、17-2-6](#)

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある

…………… [13-3-2、18-1、18-2-16、27-18](#)

■ランサムウェア

悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

…………… [0-1-1、2-1、5-1-2、5-1-3、5-2-1、5-2-2、5-2-5、5-3-2、5-3-3、第2編編集後記、7-1-2、11-5-1、15-2-1、18-2-11、18-3-5、18-4、21-1-2、23-2、26-2、27-5](#)

■リスクアセスメント

企業や組織が持つ情報資産
に対するリスクの分析・評価
を行うプロセスのこと。具体
的には情報資産の特定、脅威
と脆弱性の特定と評価、リス
クの分析と評価を行う。リス
ク評価の結果、許容できるも
の以外は何らかのセキュリテ
ィ対策を講じる必要がある

…………… [2-3](#)、[9-1](#)、
[9-2](#)、[11-3-1](#)、[12-1-1](#)、[12-1](#)
[-2](#)、[12-2-1](#)、[12-2-2](#)、[12-3](#)、
第 6 編編集後記、[13-2-4](#)、[13](#)
[-2-5](#)、[13-2-6](#)、[13-2-7](#)、[13-](#)

[2-8](#)、[13-3-1](#)、[13-3-2](#)、[13-4](#)
[-2](#)、[14-1-3](#)、[15-1](#)、[15-2-2](#)、
[16-1](#)、[17-1](#)、[18-1](#)、[18-2-1](#)
[7](#)、[21-1](#)、[21-1-2](#)、[22-1-2](#)、
[25-2-2](#)、[26-1](#)、[26-2](#)、[27-1](#)
[2](#)、[27-14](#)、[27-15](#)、[27-16](#)、
[27-17](#)、[27-18](#)、[27-21](#)、[28-](#)
[1](#)

■ リスク評価

組織やプロジェクトにおけ
る特定されたリスクに対して、
重要度や影響度を評価するプ
ロセス

…………… [2-3](#)、[5-3](#)
[-2](#)、[9-1](#)、[9-2](#)、[12-2-4](#)、[12-](#)
[3](#)、第 13 章コラム、[18-3-5](#)、
[20-1-9](#)、[21-1-2](#)、[25-2-2](#)、[2](#)
[6-2](#)、[27-12](#)

■ リモートデスクトップ接続
パソコン、タブレット、スマー
トフォンなどのデバイスを使
用して、遠隔地から特定のパ
ソコンに接続する方法

…………… [5-2-2](#)

中小企業向けサイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

2025 年 4 月 Ver.2.0 初版発行

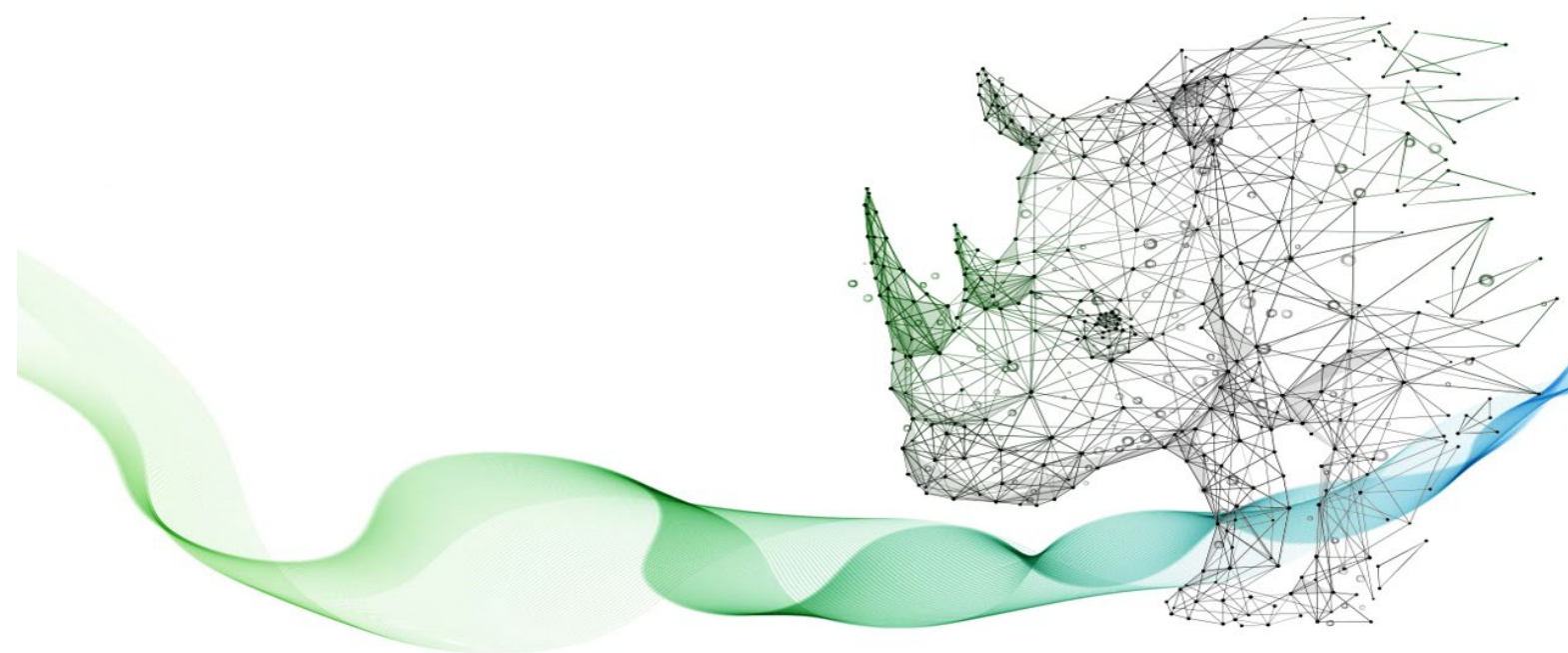
編集・発行 東京都産業労働局商工部経営支援課
新宿区西新宿二丁目 8 番 1 号

電話番号 03-5320-4770

ガイドブックの利用について

このガイドブックは、東京都が著作権を保有しておりますが、利用に際しては、非営利目的、サイバーセ
キュリティ対策の普及・啓発目的であれば、事前の申請等は必要ありません。

全体を利用されるのであればそのままご利用いただけます。



中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速



東京都産業労働局

中小企業向け サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

別添資料



東京都産業労働局

CSF2.0 の管理策と実装例

機能	カテゴリ	サブカテゴリ	実装例
ガバナンス (GV) :組織のサイバーセキュリティリスク管理戦略、期待、ポリシーが確立され、伝達され、監視されている。	組織の状況 (GV.OC) :組織のサイバーセキュリティリスクマネジメントの意思決定を取り巻く状況 (ミッション、利害関係者の期待、依存関係、法律、規制、契約上の要件) が理解されている。	GV.OC-01:組織のミッションが理解され、サイバーセキュリティリスク管理に反映されている。	例 1:組織の使命を（ビジョンや行動指針、マーケティング、サービス戦略などを通じて）共有し、その使命を阻害する可能性のあるリスクを特定するための根拠を事前に提供する。
		GV.OC-02:社内外の利害関係者が理解され、サイバーセキュリティリスク管理に関する彼らのニーズと期待が理解、考慮される。	例 1:関連する社内の利害関係者と、彼らのサイバーセキュリティに関連する期待を特定する（例えば、役員、取締役、顧問に対する実績とリスクに関する予測、従業員に対する文化的な期待）。
			例 2:関連する社外の利害関係者と、彼らのサイバーセキュリティに関する期待を特定する（例えば、顧客のプライバシー、ビジネスパートナーの事業、規制当局のコンプライアンス、社会倫理などへの予測について）。
		GV.OC-03:サイバーセキュリティに関する法的、規制、契約上の要件（プライバシーおよび市民的自由の義務を含む）が理解・管理される。 ※市民的自由:思想・言論・行動の自由など、権利章典によって保証されている自由のこと。	例 1:個人情報の保護について法的・規制要件を追跡・管理プロセスを決定する（医療保険の相互運用性と説明責任に関する法律、カリフォルニア州消費者プライバシー法、一般データ保護規則など）。
			例 2:サプライヤー、顧客、パートナーの情報についてサイバーセキュリティ管理に関する契約要件を追跡し管理するプロセスを決定する。
			例 3:組織のサイバーセキュリティ戦略を、法的・規制・契約的要件と整合させる。
		GV.OC-04:ステークホルダーが組織に依存または期待する重要な目的、能力、サービスを理解し、伝達する。	例 1:社内外のステークホルダーから見た能力とサービスの重要性を判断する基準を確立する。
			例 2:ミッション目標の達成に不可欠な資産および事業活動と、そのような業務の損失（または部分的な損失）による潜在的な影響を判断する（例えば、ビジネスインパクト分析から）。
			例 3:さまざまな運用状態（例:攻撃時、回復時、通常運用時）において、重要な能力とサービスを提供するための回復

			目標（例:回復時間目標）を設定し、伝達する。
		GV.OC-05:組織が依存する成果、能力、サービスが理解、伝達されている。	例 1:組織の外部リソースへの依存度（例:施設、クラウドベースのホスティングプロバイダー）と、組織の資産およびビジネス機能との関係の目録を作成する。
			例 2:組織の重要な機能およびサービスにとって潜在的な障害となる外部依存関係を特定、文書化し、その情報を適切な要員と共有する。
	リスクマネジメント戦略（GV.RM）:組織の優先事項、制約事項、リスクの許容と選好度、前提が設定・伝達され、オペレーショナルリスクの意思決定を支援するために使用される。	GV.RM-01:リスクマネジメントの目標が設定され、組織の利害関係者によって決定・合意される。	例 1:年次戦略計画の一環として、また大きな変更が発生したときに、短期的および長期的なサイバーセキュリティリスク管理目標を更新する。
			例 2:サイバーセキュリティリスク管理のための測定可能な目標を設定する（例:ユーザートレーニングの質を管理する、産業用制御システムの適切なリスク保護を確保する）。
			例 3:シニアリーダーがサイバーセキュリティの目標に合意し、リスクとパフォーマンスの測定・管理に活用している。
		GV.RM-02:リスク選好度およびリスク許容度が設定され、伝達され、維持されている。	例 1:組織にとっての適切なリスクレベルについての期待を伝えるリスク選好度に関する声明を決定し、伝達する。
			例 2:リスク選好度を、具体的かつ測定可能で、広く理解可能なリスク許容度に変換する。
			例 3:既知と残存リスクに基づいて、組織目標とリスク選好度を定期的に見直す。
		GV.RM-03:サイバーセキュリティリスクマネジメントの活動と成果が、企業のリスクマネジメントプロセスに含まれる。	例 1:他の企業リスク（例:コンプライアンス、財務、業務、規制、風評、安全性）とともに、サイバーセキュリティリスクを集約し、管理する。
			例 2:企業のリスク管理計画にサイバーセキュリティリスクマネージャーを含める。
			例 3:企業のリスク管理におけるサイバーセキュリティリスクのエスカレーション基準を設定する。
		GV.RM-04:適切なリスク対応の選択肢を示す戦略的方策を確立し、伝達する。	例 1:さまざまな分類のデータについて、サイバーセキュリティ上のリスクについて受容および回避の基準を明示する。
			例 2:サイバーセキュリティ保険に加入するか否かの判断をする。
			例 3:責任共有モデルが許容される条件を文書化する（例:特定のサイバーセキュリティ機能のアウトソーシング、サード

			パーティが組織に代わって金融取引を実行する、パブリッククラウドベースのサービスを使用する)。
		GV.RM-05:サプライヤーやその他の第三者からのリスクも含め、サイバーセキュリティリスクに関する組織横断的なコミュニケーションラインを確立する。	例 1:上級管理職、取締役、および経営幹部が、組織のサイバーセキュリティ体制について、合意された間隔で更新する方法を決定する。
			例 2:経営陣、業務担当者、内部監査員、法務担当者、買収担当者、物理セキュリティ担当者、人事担当者など、組織全体にまたがるすべての部門が、サイバーセキュリティリスクについてどのように互いにコミュニケーションを図るかを明らかにする。
		GV.RM-06:サイバーセキュリティリスクの算出、文書化、分類、優先順位付けのための標準化された方法を確立し、周知する。	例 1:サイバーセキュリティリスク分析に定量的アプローチを使用するための基準を確立し、確率とエクスポージャーの公式を明示する。
			例 2:サイバーセキュリティリスク情報（リスクの説明、曝露、処置、所有者など）を文書化するためのテンプレート（リスク登録簿など）を作成し、使用する。
			例 3:企業内の適切なレベルでリスクの優先順位付けの基準を確立する。
			例 4:リスクカテゴリーの一貫したリストを使用して、サイバーセキュリティリスクの統合、集約、比較をサポートする。
		GV.RM-07:戦略的機会（すなわち、ポジティブリスク）が特徴づけられ、組織のサイバーセキュリティリスクの議論に含まれる。	例 1:機会を特定し、リスクディスカッションに含めるための、ガイダンスと方法を定義・伝達する（例:強み、弱み、機会、脅威[SWOT]分析）。
			例 2:ストレッチゴールを特定し、文書化する。
			※ストレッチゴール ビジネスにおける部下育成のための目標設定手法である。現在のスキルや経験に加えて最大限の努力が必要な目標を設定することで、背伸びをした目標を設定することができる。
例 3:ポジティブリスクとネガティブリスクを計算、文書化、優先順位付けする。 ※ポジティブリスク 資産、知識、改善、またはデータの潜在的な利益を指す。			

			※ネガティブリスク 潜在的な損失を指す。
	役割、責任、および権限（GV.RR）:サイバーセキュリティの役割、責任、および説明責任、パフォーマンス評価、および継続的な改善を促進するための権限が確立され、伝達される。	GV.RR-01:組織のリーダーシップは、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を醸成する。	例 1:リーダー（取締役など）は、組織のサイバーセキュリティ戦略の策定、実施、評価における各自の役割と責任について合意する。
			例 2:特に、現在の出来事がサイバーセキュリティリスク管理の肯定的または否定的な例を強調する機会を提供する場合安全で倫理的な文化に関するリーダーの期待を共有する。
			例 3:リーダーは CISO に、包括的なサイバーセキュリティリスク戦略を維持し、少なくとも年に一度、および主要なイベント後にそれを見直して更新するように指示する。
			例 4:サイバーセキュリティリスクの管理責任者間で適切な権限と調整を確保するためのレビューを実施する。
		GV.RR-02:サイバーセキュリティリスク管理に関連する役割、責任、および権限が確立され、伝達され、理解され、実施される。	例 1:リスク管理の役割と責任をポリシーに文書化する。
			例 2:サイバーセキュリティリスク管理活動の責任者と説明責任、およびそれらのチームと個人にどのように相談し、通知するかを文書化する。
			例 3:サイバーセキュリティの責任とパフォーマンス要件を人事記述に含める。
			例 4:サイバーセキュリティリスク管理を担当する要員のパフォーマンス目標を文書化し、定期的にパフォーマンスを測定して改善点を特定する。
			例 5:業務、リスク機能、内部監査機能におけるサイバーセキュリティの責任を明確にする。
		GV.RR-03:サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースを配分する。	例 1:定期的なマネジメントレビューを実施し、サイバーセキュリティリスクマネジメントの責任者に必要な権限が与えられていることを確認する。
			例 2:リスク許容度と対応に沿ったリソース配分と投資を特定する。
			例 3:サイバーセキュリティ戦略を支援するために、適切かつ十分な人材、プロセス、技術的リソースを提供する。
		GV.RR-04:サイバーセキュリティは人事慣行に含まれる。	例 1:サイバーセキュリティリスク管理への配慮を人事プロセス（人事審査、入社手続き、変更通知、退社手続きなど）に組み込む。

			例 2:サイバーセキュリティの知識は、雇用、トレーニング、定着の決定においてプラス要因であるとする。
			例 3:機密性の高い役割の従業員をオンボーディングする前に身元調査を実施し、そのような役割の担当者の身元調査を定期的に繰り返す。
			例 4:各自の役割に関連するセキュリティポリシーを認識し、順守し、維持するための要員の義務を定義し、実施する。
	ポリシー（GV.PO）：組織のサイバーセキュリティポリシーが確立され、伝達され、実施される。	GV.PO-01:サイバーセキュリティリスクの管理方針が、組織の状況、サイバーセキュリティ戦略、優先事項に基づいて策定され、周知され、実施される。	例 1:経営陣の意図、期待、方向性を記述した、理解しやすく使いやすいリスク管理ポリシーを作成、普及、維持する。
			例 2:ポリシーとそれをサポートするプロセスと手順を定期的に見直して、リスク管理戦略の目標と優先事項、およびサイバーセキュリティポリシーの高レベルの方向性と一致していることを確認する。
			例 3:ポリシーについて上級管理職の承認を必要とする。
			例 4:サイバーセキュリティリスク管理ポリシーとそれをサポートするプロセスと手順を組織全体に伝達する。
			例 5:最初に採用されたとき、毎年、およびポリシーが更新されるたびに、ポリシーの受領を確認するように担当者に要求する。
		GV.PO-02:サイバーセキュリティリスクの管理方針は、要件、脅威、技術、組織ミッションの変化を反映するよう、見直し、更新、伝達、実施される。	例 1:サイバーセキュリティリスク管理の結果の定期的なレビューに基づいてポリシーを更新し、ポリシーとサポートプロセスと手順がリスクを許容可能なレベルで適切に維持するようにする。
			例 2:組織のリスク環境に対する変更（リスクや組織のミッション目標の変更など）をレビューするためのタイムラインを提供し、推奨されるポリシーの更新を伝える。
			例 3:法的要件および規制要件の変更を反映するようにポリシーを更新する。
			例 4:テクノロジーの変更（人工知能の採用など）とビジネスの変更（新しいビジネスの買収、新しい契約要件など）を反映するようにポリシーを更新する。
	監視（GV.OV）:組織全体のサイバーセキュ	GV.OV-01:サイバーセキュリティリスク管理戦略の成果を	例 1:リスク管理戦略とリスク結果が、リーダーが意思決定を行い、組織の目標を達成するのにどの程度役立ったかを測

	リテリリスク管理活動と実績の結果が、リスク管理戦略の情報提供、改善、調整に利用される。	レビューし、戦略と方向性に反映・調整する。	定する。 例 2:運用やイノベーションを阻害するサイバーセキュリティリスク戦略を調整すべきか否かを検討する。
		GV.OV-02:組織の要求事項とリスクを確実にカバーするために、サイバーセキュリティリスク管理戦略がレビューされ、調整される。	例 1:監査結果を見直して、既存のサイバーセキュリティ戦略が内部および外部の要件への準拠を確保しているか否かを確認する。
			例 2:サイバーセキュリティ関連の役割を担う人々のパフォーマンス監視を見直して、ポリシーの変更が必要か否かを判断する。
			例 3:サイバーセキュリティインシデントを踏まえた戦略の見直し。
	GV.OV-03:組織のサイバーセキュリティリスク管理のパフォーマンスが評価され、必要な調整のために再確認される。		例 1:重要業績評価指標（KPI）を組織全体のポリシーと手順が目標の達成を保証するために再確認する。
			例 2:重要リスク指標（KRI）を見直して、組織が直面するリスク（可能性と潜在的な影響を含む）を特定する。
			例 3:上級管理職にサイバーセキュリティリスク管理に関する指標を収集し、伝達する。
	サイバーセキュリティサプライチェーンリスク管理（GV.SC）:サイバーサプライチェーンのリスク管理プロセスは、組織の利害関係者によって特定、確立、管理、監視、および改善される。	GV.SC-01:サイバーセキュリティのサプライチェーンリスク管理プログラム、戦略、目的、方針、およびプロセスが確立され、組織の利害関係者によって合意されている。	例 1:サイバーセキュリティサプライチェーンリスク管理プログラムの目的を表現する戦略を確立する。
			例 2:プログラムの実施と改善に導く計画（マイルストーンを含む）、ポリシー、手順を含むサイバーセキュリティサプライチェーンリスク管理プログラムを開発し、ポリシーと手順を組織の利害関係者と共有する。
			例 3:組織の利害関係者が合意し、実行する戦略、目的、ポリシー、および手順に基づいて、プログラムプロセスを開発および実装する。
		GV.SC-02:サプライヤー、顧客、パートナーに対するサイバーセキュリティの役割と責	例 4:サイバーセキュリティ、IT、運用、法務、人事、エンジニアリングなど、サイバーセキュリティサプライチェーンのリスク管理に貢献する機能間の整合性を確保するための組織横断的なメカニズムを確立する。
			例 1:サイバーセキュリティサプライチェーンのリスク管理活動の計画、リソース、および実行に責任を持ち、説明責任を負う 1 つ以上の特定の役割またはポジションを特定する。

	任が確立され、伝達され、社内外で調整される。	例 2:サイバーセキュリティサプライチェーンのリスク管理の役割と責任をポリシーに文書化する。
		例 3:サイバーセキュリティサプライチェーンのリスク管理活動の全体の責任と説明責任を誰が負うか、そしてそれらのチームと個人にどのように相談し、通知するかを文書化するための責任マトリックスを作成する。
		例 4:サイバーセキュリティサプライチェーンのリスク管理の責任とパフォーマンス要件を人事記述に含めて、明確にし、また説明責任を向上させる。
		例 5:サイバーセキュリティリスク管理固有の責任を持つ担当者のパフォーマンス目標を文書化し、定期的に測定してパフォーマンスを実証および改善する。
		例 6:サプライヤー、顧客、ビジネスパートナーが、該当するサイバーセキュリティリスクに対する共通の責任に対処するための役割と責任を開発し、それらを組織のポリシーと該当するサードパーティ契約に統合する。
		例 7:サイバーセキュリティサプライチェーンのリスク管理の役割と第三者に対する責任を社内 で伝達する。
		例 8:組織とそのサプライヤー間の情報共有および報告プロセスに関するルールとプロトコルを確立する。
	GV.SC-03:サイバーセキュリティのサプライチェーンリスクマネジメントは、サイバーセキュリティおよび企業のリスクマネジメント、リスク評価、改善プロセスに統合する。	例 1:サイバーセキュリティとエンタープライズリスク管理との整合性と重複する領域を特定する。
		例 2:サイバーセキュリティリスク管理とサイバーセキュリティサプライチェーンリスク管理のための統合制御セットを確立する。
		例 3:サイバーセキュリティサプライチェーンのリスク管理を改善プロセスに統合する。
		例 4:サプライチェーンにおける重大なサイバーセキュリティリスクを上級管理職にエスカレーションし、企業リスク管理レベルで対処する。
	GV.SC-04:サプライヤーを把握し、重要度に応じて優先順位を付ける。	例 1:サプライヤーによって処理または所有されるデータの機密性、組織のシステムへのアクセスの程度、組織のミッションに対する製品またはサービスの重要性などに基づいて、サプライヤーの重要度の基準を作成する。

			例 2:すべてのサプライヤーの記録を保持し、重要度基準に基づいてサプライヤーに優先順位を付ける。
		GV.SC-05:サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件は設定され、順位付けられ、サプライヤーやその他の関連する第三者との契約やその他の合意に組み込まれる。	例 1:サプライヤー、製品、サービスの重要度レベルと、侵害された場合の潜在的な影響に見合ったセキュリティ要件を確立する。
			例 2:第三者が従うべきすべてのサイバーセキュリティおよびサプライチェーン要件と、デフォルトの契約言語で要件の順守を確認する方法を含める。
			例 3:組織とそのサプライヤーおよび契約上のサブ・ティア サプライヤー間の情報共有に関するルールとプロトコルを定義する。
			例 4:セキュリティ要件の重要性と侵害された場合の潜在的な影響に基づいて、セキュリティ要件を契約に含めることでリスクを管理する。
			例 5:サプライヤー関係のライフサイクルを通じて許容可能なセキュリティパフォーマンスについてサプライヤーを監視するためのサービスレベルアグリーメント（SLA）でセキュリティ要件を定義する。
			例 6:契約上、サプライヤーに対して、製品の寿命またはサービスの期間中、自社の製品およびサービスのサイバーセキュリティの特徴、機能、および脆弱性を開示するよう要求する。
			例 7:重要な製品の最新のコンポーネント在庫（ソフトウェアまたはハードウェアの部品表など）を提供し、維持することをサプライヤーに契約上要求する。
			例 8:契約上、サプライヤーに従業員を審査し、インサイダー脅威から保護することを要求する。
			例 9:契約上、サプライヤーに対して、自己証明、既知の標準への準拠、認証、検査などを通じて、許容可能なセキュリティ慣行を実施している証拠を提供するよう要求する。
			例 10:契約およびその他の合意において、潜在的なサイバーセキュリティリスクに関して、組織、そのサプライヤー、およびそれらのサプライチェーンの権利と責任を明記する。

		GV.SC-06:正式なサプライヤーやその他の第三者との関係を結ぶ前に、リスクを低減するための計画やデューデリジェンスが実施されている。 ※デューデリジェンス企業などに要求される当然に実施すべき注意義務および努力のこと。	例 1:調達計画と整合し、各サプライヤーとの関係のリスク、重要性、複雑さのレベルに見合った、見込みサプライヤーに対する徹底的なデューデリジェンスを実施する。
			例 2:テクノロジーとサイバーセキュリティ機能の適合性、および将来のサプライヤーのリスク管理慣行を評価する。
			例 3:ビジネスおよび適用されるサイバーセキュリティ要件に対するサプライヤーリスク評価を実施する。
			例 4:重要な製品を購入して使用する前に、信頼性、完全性、セキュリティを評価する。
		GV.SC-07:サプライヤー、その製品・サービス、その他の第三者によってもたらされるリスクを理解し、記録し、優先順位を付け、評価し、対応し、関係を通じて監視する。	例 1:評価の形式と頻度を、第三者の評判と提供する製品またはサービスの重要性に基づいて調整する。
			例 2:自己証明、保証、認証、その他の成果物など、契約上のサイバーセキュリティ要件に準拠しているという第三者の証拠を評価する。
			例 3:重要なサプライヤーを監視し、検査、監査、テスト、その他の形式の評価など、さまざまな方法と手法を使用して、サプライヤー関係のライフサイクル全体を通じてセキュリティ義務を果たしていることを確認する。
			例 4:重要なサプライヤー、サービス、製品のリスクプロファイルの変化を監視し、それに応じてサプライヤーの重要度とリスクの影響を再評価する。
			例 5:ビジネスの継続性を確保するために、予期しないサプライヤーとサプライチェーン関連の中断を計画する。
		GV.SC-08:インシデント発生時の計画、対応、復旧活動に、関連するサプライヤーやその他の第三者が含まれる。	例 1:インシデント対応と復旧活動、および組織とそのサプライヤー間のステータスを報告するためのルールとプロトコルを定義して使用する。
			例 2:インシデント対応に関する組織とそのサプライヤーの役割と責任を特定し、文書化する。
			例 3:インシデント対応の演習とシミュレーションに重要なサプライヤーを含める。
			例 4:組織とその重要なサプライヤーとの間の危機管理コミュニケーションの方法とプロトコルを定義し、調整する。

			例 5:重要なサプライヤーと共同で教訓セッションを実施する。
		GV.SC-09:サプライチェーンセキュリティの実践が、サイバーセキュリティと企業のリスク管理プログラムに統合され、そのパフォーマンスが技術製品とサービスのライフサイクル全体を通じて監視される。	例 1:ポリシーと手順により、取得したすべてのテクノロジー製品およびサービスの来歴記録を必要とする。
			例 2:買収したコンポーネントが改ざんされていないため、本物であることが証明された方法について、リーダーに定期的にリスクレポートを提供する。
			例 3:サイバーセキュリティのリスクマネージャーと運用担当者間で、認証された信頼できるソフトウェアプロバイダーからのみソフトウェアのバッチ、アップデート、アップグレードを取得する必要があることについて定期的に連絡を取る。
			例 4:ポリシーを見直して、承認されたサプライヤー担当者がサプライヤー製品のメンテナンスを行うことを要求していることを確認する。
			例 5:ポリシーと手順では、重要なハードウェアのアップグレードに不正な変更がないか確認する必要がある。
		GV.SC-10:サイバーセキュリティのサプライチェーンリスクマネジメント計画には、パートナーシップまたはサービス契約締結後に発生する活動に関する規定が含まれる。	例 1:正常な状況と不利な状況の両方で重要な関係を終了するためのプロセスを確立する。
			例 2:コンポーネントの寿命終了時の保守サポートと陳腐化の計画を定義して実装する。
			例 3:組織のリソースへのサプライヤーのアクセスが不要になったときに、すぐに非アクティブ化していることを確認する。
			例 4:組織のデータを含む資産が、タイムリーに、管理された、安全な方法で返却または適切に廃棄されていることを確認する。
			例 5:サプライヤーとの関係を終了または移行するための計画を策定し、実行し、サプライチェーンのセキュリティリスクとレジリエンスを考慮に入れる。
			例 6:サプライヤーの終了によって生じるデータとシステムへのリスクを軽減する。
			例 7:サプライヤーの契約に関連するデータ漏えいリスクを管理する。

識別 (ID) :組織 の現在のサイバー セキュリティリス クを把握する。	資産管理 (ID.AM) : 組織がビジネス目的を 達成できるようにする 資産 (データ、ハード ウェア、ソフトウェ ア、システム、施設、 サービス、人など) は、組織の目標と組織 のリスク戦略に対する 相対的な重要性と一致 して特定および管理さ れる。	ID.AM-01:組織が管理するハ ードウェアのインベントリを 保持する。	例 1:IT、IoT、OT、モバイルデバイスなど、あらゆる種類 のハードウェアの在庫を維持する。
		ID.AM-02:組織が管理するソ フトウェア、サービス、シス テムのインベントリを管理す る。	例 2:ネットワークを常に監視して新しいハードウェアを検 出し、インベントリを自動的に更新する。
			例 1:商用オフザシェルフ、オープンソース、カスタムアプ リケーション、API サービス、クラウドベースのアプリケー ションとサービスなど、あらゆる種類のソフトウェアとサー ビスのインベントリを維持する。
			例 2:コンテナや仮想マシンを含むすべてのプラットフォームを常時監視し、ソフトウェアとサービスのインベントリの 変更を確認する。
		ID.AM-03:組織の許可された ネットワーク通信と内部およ び外部のネットワークデータ フローの表現が維持される。	例 3:組織のシステムのインベントリを維持する。
			例 1:組織の有線および無線ネットワーク内の通信とデータ フローのベースラインを維持する。
			例 2:組織とサードパーティ間のコミュニケーションとデー タフローのベースラインを維持する。
			例 3:組織の IaaS (Infrastructure-as-a-Service) の使用に 関する通信とデータフローのベースラインを維持する。
		ID.AM-04:サプライヤーが提 供するサービスの在庫を管理 する。	例 4:許可されたシステム間で通常使用される予想されるネ ットワークポート、プロトコル、およびサービスのドキュメ ントを維持する。
			例 1:API のおよびそのほかの外部でホストされているアプ リケーションサービス、サードパーティの Infrastructure- as-a-Service (IaaS)、Platform-as-a-Service (PaaS)、 Software-as-a-Service (SaaS) オファリングなど、組織 が使用するすべての外部サービスのインベントリを作成す る。
		ID.AM-05:資産は、分類、重 要度、リソース、ミッション への影響に基づいて優先順位 が付けられる。	例 2:新しい外部サービスを利用する場合はインベントリを 更新して、組織によるそのサービスの使用の適切なサイバー セキュリティリスク管理監視を確保する。
			例 1:各クラスの資産の優先順位付けの基準を定義する。
			例 2:資産に優先順位付け基準を適用する。
			例 3:資産の優先順位を追跡し、定期的に更新するか、組織 に大幅な変更が発生したときに更新する。

		ID.AM-06:[撤回:GV.RR-02、GV.SC-02 に編入する。]	
		ID.AM-07:指定されたデータ型のデータと対応するメタデータのインベントリが維持される。	例 1:指定された関心のあるデータタイプ（個人を特定できる情報、保護医療情報、金融口座番号、組織の知的財産、運用技術データなど）のリストを維持する。
			例 2:アドホックデータを継続的に検出および分析して、指定されたデータタイプの新しいインスタンスを特定する。
			例 3:タグまたはラベルを使用して、指定したデータ型にデータ分類を割り当てる。
			例 4:指定されたデータタイプの各インスタンスの出所、データ所有者、およびジオロケーションを追跡する。
		ID.AM-08: システム、ハードウェア、ソフトウェア、サービス、データは、そのライフサイクル全体を通じて管理される。	例 1:システム、ハードウェア、ソフトウェア、サービスのライフサイクル全体を通じてサイバーセキュリティの考慮事項を統合する。
			例 2:サイバーセキュリティに関する考慮事項を製品ライフサイクルに統合する。
			例 3:ミッション目標を達成するためのテクノロジーの非公式な使用（例:「シャドーIT」）を特定する。
			例 4:組織の攻撃対象領域を不必要に拡大する冗長なシステム、ハードウェア、ソフトウェア、サービスを定期的に特定する。
			例 5:システム、ハードウェア、ソフトウェア、サービスを本番環境に導入する前に、適切に構成し、保護する。
			例 6:システム、ハードウェア、ソフトウェア、およびサービスが組織内で移動または転送されたときにインベントリを更新する。
			例 7:組織のデータ保持ポリシーに基づき、保存されているデータを所定の破棄方法により安全に破棄し、破棄の記録を保持・管理する。
			例 8:ハードウェアが廃止、廃止、再割り当て、または修理や交換のために送られるときに、データストレージを安全に削除する。
			例 9:紙、記憶媒体、その他の物理的なデータストレージを破壊する方法を提供する。

	リスク評価（ID.RA）：組織、資産、および個人に対するサイバーセキュリティリスクは、組織によって理解される。	ID.RA-01:資産の脆弱性を特定、検証、記録する。	例 1:脆弱性管理テクノロジーを使用して、パッチが適用されていないソフトウェアや誤って構成されたソフトウェアを特定する。
			例 2:ネットワークとシステムアーキテクチャを評価し、サイバーセキュリティに影響を与える設計と実装の弱点を検出する。
			例 3:組織が開発したソフトウェアをレビュー、分析、またはテストして、設計、コーディング、およびデフォルト設定の脆弱性を特定する。
			例 4:重要なコンピューティング資産を収容する施設の物理的な脆弱性とレジリエンスの問題を評価する。
			例 5:サイバー脅威インテリジェンスのソースを監視して、製品やサービスの新たな脆弱性に関する情報を入手する。
			例 6:サイバーセキュリティに影響を与えるために悪用される可能性のある弱点について、プロセスと手順を確認する。
		ID.RA-02:情報共有フォーラムや情報源からサイバー脅威インテリジェンスを受け取る。	例 1:サイバーセキュリティツールとテクノロジーを検出または対応機能で構成し、サイバー脅威インテリジェンスフィードを安全に取り込む。
			例 2:現在の脅威アクターとその戦術、技術、手順（TTP）に関するアドバイザリを、信頼できる第三者から受け取り、レビューする。
			例 3:サイバー脅威インテリジェンスのソースを監視して、新興技術が持つ可能性のある脆弱性の種類に関する情報を入手する。
		ID.RA-03:組織に対する内部および外部の脅威を特定し、記録する。	例 1:サイバー脅威インテリジェンスを使用して、組織を標的にする可能性が高い脅威アクターの種類と、彼らが使用する可能性が高い TTP の認識を維持する。
			例 2:脅威ハンティングを実行して、環境内の脅威アクターの兆候を探す。
			例 3:内部の脅威アクターを特定するためのプロセスを実装する。
		ID.RA-04:脆弱性を悪用する脅威の潜在的な影響と可能性を特定し、記録する。	例 1:ビジネスリーダーとサイバーセキュリティリスクマネジメントの実務者が協力して、リスクシナリオの可能性と影響を見積り、リスク登録簿に記録する。

			例 2:組織の通信、システム、およびこれらのシステムで処理される、あるいはこれらのシステムによって処理されるデータへの不正アクセスが、ビジネスに及ぼしうる影響を列挙する。
			例 3:システムのシステムに対する連鎖的な障害の潜在的な影響を考慮する。
		ID.RA-05:脅威、脆弱性、可能性、影響は、固有のリスクを理解し、リスク対応の優先順位付けを通知するために使用される。	例 1:脅威モデルを開発して、データに対するリスクをよりよく理解し、適切なリスク対応を特定する。
			例 2:推定される可能性と影響に基づいて、サイバーセキュリティリソースの割り当てと投資に優先順位を付ける。
		ID.RA-06:リスク対応は選択、優先順位付け、計画、追跡、および伝達される。	例 1:リスクを受け入れるか、移転するか、軽減するか、回避するかを決定するための脆弱性管理計画の基準を適用する。
			例 2:リスクを軽減するための補償制御を選択するための脆弱性管理計画の基準を適用する。
			例 3:リスク対応の実施の進捗状況を追跡する（行動計画とマイルストーン[POA&M]、リスク登録、リスク詳細レポートなど）。
			例 4:リスク評価の結果を使用して、リスク対応の決定とアクションを通知する。
			例 5:影響を受けるステークホルダーに、優先順位を付けて計画されたリスク対応を伝える。
		ID.RA-07:変更と例外は管理され、リスクの影響について評価され、記録され、追跡される。	例 1:提案された変更と要求された例外の正式な文書化、レビュー、テスト、および承認のための手順を実装し、それに従う。
			例 2:提案された各変更を行うか、または行わない場合に発生する可能性のあるリスクを文書化し、変更のロールバックに関するガイダンスを提供する。
			例 3:リクエストされた各例外に関連するリスクと、それらのリスクに対応するための計画を文書化する。
			例 4:計画された将来のアクションまたはマイルストーンに基づいて受け入れられたリスクを定期的に見直す。

		ID.RA-08:脆弱性の開示を受領、分析、対応するためのプロセスを確立している。	例 1:契約で定義されたルールとプロトコルに従って、組織とそのサプライヤー間で脆弱性情報の共有を行う。
			例 2:サプライヤー、顧客、パートナー、政府のサイバーセキュリティ組織によるサイバーセキュリティの脅威、脆弱性、またはインシデントの開示の処理、影響の分析、および対応のための責任を割り当て、手順の実行を確認する。
		ID.RA-09:ハードウェアとソフトウェアの真正性と完全性は、取得および使用前に評価される。	例 1:重要なテクノロジー製品およびサービスを取得して使用する前に、信頼性とサイバーセキュリティを評価する。
		ID.RA-10:重要なサプライヤーは買収前に評価される。	例 1:サプライチェーンを含む、ビジネスおよび適用されるサイバーセキュリティ要件に対してサプライヤーリスク評価を実施する。
	改善（ID.IM）:組織のサイバーセキュリティリスク管理プロセス、手順、および活動の改善は、すべての CSF 機能で特定される。	ID.IM-01:評価から改善点を抽出する。	例 1:現在の脅威と TTP を考慮した重要なサービスの自己評価を実行する。
			例 2:組織のサイバーセキュリティプログラムの有効性に関する第三者評価または独立した監査に投資して、改善が必要な領域を特定する。
			例 3:自動化された手段を通じて、選択したサイバーセキュリティ要件への準拠を常に評価する。
		ID.IM-02:サプライヤーや関連する第三者との連携によるものを含め、セキュリティテストや演習から改善点が特定される。	例 1:インシデント対応評価の結果に基づいて、将来のインシデント対応活動の改善点を特定する（例:机上演習とシミュレーション、テスト、内部レビュー、独立監査）。
			例 2:重要なサービスプロバイダーや製品サプライヤーと連携して実施された演習に基づいて、将来のビジネス継続性、災害復旧、インシデント対応活動の改善点を特定する。
			例 3:必要に応じて、社内の利害関係者（上級管理職、法務部門、人事部など）をセキュリティテストと演習に参加させる。
			例 4:ペネトレーションテストを実施して、リーダーシップによって承認された、選択した高リスクシステムのセキュリティ体制を改善する機会を特定する。
			例 5:製品またはサービスが契約したサプライヤーまたはパートナーから発信されたものではない、または受領前に変更

			されたという発見に対応し、回復するための緊急時対応計画を行使する。
			例 6:セキュリティツールとサービスを使用してパフォーマンスメトリックを収集および分析し、サイバーセキュリティプログラムの改善を通知する。
		ID.IM-03:業務プロセス、手順、活動の実行から改善を特定する。	例 1:サプライヤーとの共同教訓セッションを実施する。
			例 2:サイバーセキュリティのポリシー、プロセス、手順を毎年見直し、学んだ教訓を考慮に入れる。
			例 3:メトリクスを使用して、運用上のサイバーセキュリティパフォーマンスを経時的に評価する。
		ID.IM-04:業務に影響を及ぼすインシデント対応計画およびその他のサイバーセキュリティ計画が策定され、伝達され、維持され、改善される。	例 1:運用に支障をきたす、機密情報を漏えいさせる、または組織の使命と実行可能性を危険にさらす可能性のある有害事象への対応と回復のための緊急時対応計画（インシデント対応、事業継続性、災害復旧など）を確立する。
			例 2:連絡先とコミュニケーションの情報、一般的なシナリオを処理するためのプロセス、優先順位付け、エスカレーション、昇格の基準をすべてのコンティンジェンシープランに含める。
			例 3:脆弱性管理計画を作成して、あらゆる種類の脆弱性を特定および評価し、リスク対応に優先順位を付け、テストし、実装する。
			例 4:サイバーセキュリティ計画（更新を含む）を、その実施責任者および影響を受ける当事者に伝達する。
			例 5:すべてのサイバーセキュリティ計画を毎年、または大幅な改善の必要性が特定された場合に、見直して更新する。
	ビジネス環境（ID.BE）:撤回:GV.OC に編入する。	ID.BE-01:[撤回:GV.OC-05 に編入する。]	
		ID.BE-02:[撤回: GV.OC-01 に編入する。]	
		ID.BE-03:[撤回: GV.OC-01 に編入する。]	
		ID.BE-04:[撤回: GV.OC-04、GV.OC-05 に編入する。]	

		ID.BE-05:[撤回: GV.OC-04 に編入する。]	
	ガバナンス (ID.GV) :撤回:GV に編入する。	ID.GV-01:[撤回:GV.PO、 GV.PO-01、GV.PO-02 に編入 する。]	
		ID.GV-02:[撤回:GV.OC-02、 GV.RR、GV.RR-02 に編入す る。]	
		ID.GV-03:[撤回:GV.OC-03 に 移動する。]	
		ID.GV-04:[撤回:GV.RM-04 に移動する。]	
	リスクマネジメント戦 略 (ID.RM) :撤 回:GV.RM に編入す る。	ID.RM-01:[撤回:GV.RM-01、 GV.RM-06、GV.RR-03 に編入 する。]	
		ID.RM-02:[撤回:GV.RM-02、 GV.RM-04 に編入する。]	
		ID.RM-03:[撤回: GV.RM-02 に移動する。]	
	サプライチェーンリス ク管理 (ID.SC) :撤 回:GV.SC に編入す る	ID.SC-01:[撤回:RM-05、 GV.SC-01、GV.SC-06、 GV.SC-09、GV.SC-10 に編入 する。]	
		ID.SC-02:[撤回: GV.OC-02、 GV.SC-03、GV.SC-04、 GV.SC-07、ID.RA-10 に編入 する。]	
		ID.SC-03:[撤回:GV.SC-05 に 移動する。]	
		ID.SC-04:[撤回:GV.SC-07、 ID.IM-02 に編入する。]	
		ID.SC-05:[撤回:GV.SC-08、 ID.IM-02 に編入する。]	

防御（PR）：組織のサイバーセキュリティリスクを管理するための保護手段が使用される。	ID 管理、認証、およびアクセス制御 （PR.AA）：物理的および論理的な資産へのアクセスは、許可されたユーザー、サービス、およびハードウェアに限定され、不正アクセスの評価されたリスクに見合った方法で管理される。	PR.AA-01:許可されたユーザー、サービス、およびハードウェアの ID とクレデンシャルが組織によって管理される。	例 1:従業員、請負業者、そのほかの新しいアクセスまたは追加のアクセスの要求を開始し、必要に応じてシステムまたはデータ所有者の許可を得て、要求を追跡、レビュー、および実行する。
			例 2:暗号化証明書と ID トークン、暗号化キー（つまり、キー管理）、およびそのほかの資格情報を発行、管理、および取り消す。
			例 3:不変のハードウェア特性から各デバイスの一意の識別子を選択するか、デバイスに安全にプロビジョニングされた識別子を選択する。
			例 4:インベントリとサービスの目的で、承認されたハードウェアに識別子を物理的にラベル付ける。
		PR.AA-02:アイデンティティは、相互作用のコンテキストに基づいて証明され、クレデンシャルにバインドされる。	例 1:登録時に政府発行の ID 資格情報（パスポート、ビザ、運転免許証など）を使用して、個人の主張する ID を確認する。
			例 2:各人に異なる資格情報を発行する（つまり、資格情報を共有しない）。
		PR.AA-03:ユーザー、サービス、ハードウェアを認証する。	例 1:多要素認証を要求する。
			例 2:パスワード、PIN、および同様の認証子の最小強度に関するポリシーを適用する。
			例 3:リスクに基づいてユーザー、サービス、ハードウェアを定期的に再認証する（ゼロトラストアーキテクチャなど）。
			例 4:緊急時下においてセキュリティ確保に必要な不可欠なアカウントにアクセス可能な担当者を確認する。
		PR.AA-04:アイデンティティ・アサーションは保護、伝達、検証される。	例 1:シングルサインオンシステムを通じて認証とユーザー情報の伝達に使用される ID アサーションを保護する。
			例 2:連携システム間で認証とユーザー情報の伝達に使用されるアイデンティティ・アサーションの保護。
			例 3:権限のある担当者が、緊急時の安全を守るために不可欠なアカウントにアクセスできるようにすること。
		PR.AA-05:アクセス許可、資格、および権限がポリシーで定義され、管理され、実施さ	例 1:論理的および物理的なアクセス権限を定期的に、および誰かがロールを変更したり組織を離れたりするたびに確認し、不要になった権限を速やかに取り消す。

		れ、レビューされ、最小特権と職務分離の原則が組み込まれている。	例 2: リクエスターとリクエストされたリソースの属性を認証決定に考慮する（ジオロケーション、曜日/時間、リクエスターエンドポイントのサイバーヘルスなど）。
			例 3: アクセスと権限を必要最小限に制限する（例: ゼロトラストアーキテクチャ）。
			例 4: 重要なビジネス機能に関連する権限を定期的に見直して、職務の適切な分離を確認する。
		PR.AA-06: 資産への物理的なアクセスは、リスクに見合った形で管理、監視、実施される。	例 1: 警備員、防犯カメラ、施錠された入り口、警報システム、およびその他の物理的制御を使用して、施設を監視し、アクセスを制限する。
			例 2: リスクの高い資産を含むエリアに対して、追加の物理的セキュリティ制御を採用する。
			例 3: ビジネスに不可欠な資産を含むエリア内で、ゲスト、ベンダー、その他の第三者をエスコートする。
	意識向上とトレーニング（PR.AT）: 組織の要員は、サイバーセキュリティに関する意識向上とトレーニングを受け、サイバーセキュリティ関連の業務を遂行できるようになる。	PR.AT-01: 要員は、サイバーセキュリティリスクを念頭に置いて一般的な業務を遂行するための知識と技能を有するよう、意識向上とトレーニングを受ける。	例 1: 従業員、請負業者、パートナー、サプライヤー、および組織の非公開リソースのそのほかすべてのユーザーに、基本的なサイバーセキュリティの認識とトレーニングを提供する。
			例 2: ソーシャルエンジニアリングの試みやその他の一般的な攻撃を認識し、攻撃や疑わしい活動を報告し、利用規定を順守し、基本的なサイバーハイジーンタスク（ソフトウェアのパッチ適用、パスワードの選択、資格情報の保護など）を実行するように、従業員を訓練する。
			例 3: サイバーセキュリティポリシー違反の結果について、個々のユーザーと組織全体の両方に説明する。
			例 4: 基本的なサイバーセキュリティの実践に関するユーザーの理解度を定期的に評価またはテストする。
			例 5: 既存のプラクティスを強化し、新しいプラクティスを導入するために、毎年のリフレッシュャーを義務付ける。
		PR.AT-02: 専門的な役割を担う個人が、サイバーセキュリティリスクを念頭に置いて関連業務を遂行するための知識	例 1: 物理的なセキュリティおよびサイバーセキュリティの担当者、財務担当者、上級管理職、ビジネスクリティカルなデータにアクセスできる人など、追加のサイバーセキュリティトレーニングが必要な組織内の専門的な役割を特定する。

		と技能を有するよう、意識向上とトレーニングを提供する。	例 2:請負業者、パートナー、サプライヤー、その他の第三者を含む、専門的な役割を担うすべての人々に、役割ベースのサイバーセキュリティの認識とトレーニングを提供する。
			例 3:ユーザーがそれぞれの専門的な役割におけるサイバーセキュリティの実践を理解しているか否か、定期的に評価またはテストする。
			例 4:既存のプラクティスを強化し、新しいプラクティスを導入するために、毎年のリフレッシュャーを必須にする。
		PR.AT-03:[撤回:PR.AT-01、PR.AT-02 に編入する。]	
		PR.AT-04:[撤回:PR.AT-02 に編入する。]	
		PR.AT-05:[撤回:PR.AT-02 に編入する。]	
	データセキュリティ (PR.DS) :情報の機密性、完全性、可用性を保護するために、組織のリスク戦略に沿ってデータを管理する。	PR.DS-01:静止データの機密性、完全性、可用性を保護する。	例 1:暗号化、デジタル署名、暗号化ハッシュを使用して、ファイル、データベース、仮想マシンディスクイメージ、コンテナイメージ、およびその他のリソースに格納されたデータの機密性と整合性を保護する。
			例 2:フルディスク暗号化を使用して、ユーザーエンドポイントに保存されているデータを保護する。
			例 3:署名の検証によるソフトウェアの整合性を確認する。
			例 4:リムーバブルメディアの使用を制限してデータ流出を防ぐ。
			例 5:暗号化されていない機密情報を含む物理的に安全なリムーバブルメディア（施錠されたオフィスやファイルキャビネット内など）。
		PR.DS-02:転送中のデータの機密性、完全性、および可用性を保護する。	例 1:暗号化、デジタル署名、および暗号化ハッシュを使用して、ネットワーク通信の機密性と整合性を保護する。
			例 2:データの分類に応じて、機密データを含む送信メールやその他の通信を自動的に暗号化またはブロックする。
			例 3:組織のシステムやネットワークから、個人の電子メール、ファイル共有、ファイルストレージサービス、その他の個人のコミュニケーションアプリケーションやサービスへ

			のアクセスをブロックする。
			例 4:本番環境の機密データ（顧客レコードなど）が開発、テスト、そのほかの非本番環境で再利用されるのを防ぐ。
		PR.DS-03:[撤回:ID.AM-08、PR.PS-03 に編入する。]	
		PR.DS-04:[撤回:PR.IR-04 に移動する。]	
		PR.DS-05:[撤回:PR.DS-01、PR.DS-02、PR.DS-10 に編入する。]	
		PR.DS-06:[撤回:PR.DS-01、DE.CM-09 に編入する。]	
		PR.DS-07:[撤回:PR.IR-01 に編入する。]	
		PR.DS-08:[撤回:ID.RA-09、DE.CM-09 に編入する。]	
		PR.DS-10:使用中のデータの機密性、完全性、および可用性が保護されている。	例 1:機密を保持する必要があるデータ（プロセッサやメモリなど）が不要になったらすぐに削除する。
			例 2:同じプラットフォームの他のユーザーやプロセスによるアクセスから使用中のデータを保護する。
		PR.DS-11:データのバックアップが作成、保護、維持、およびテストされる。	例 1:重要なデータをほぼリアルタイムで継続的にバックアップし、他のデータは合意されたスケジュールで頻繁にバックアップする。
			例 2:すべての種類のデータソースのバックアップと復元を少なくとも年に 1 回テストする。
			例 3:一部のバックアップをオフラインおよびオフサイトに安全に保管して、インシデントや災害によって損傷を受けないようにする。
			例 4:データバックアップストレージの地理的な分離と地理的な制限を適用する。
	プラットフォームのセキュリティ (PR.PS):物理ブラ	PR.PS-01:構成管理プラクティスが確立され、適用されている。	例 1:組織のサイバーセキュリティポリシーを適用し、必要な機能のみを提供する強化されたベースラインを確立、テスト、デプロイ、および維持する（つまり、最小機能の原

	ットフォームおよび仮想プラットフォームのハードウェア、ソフトウェア（ファームウェア、オペレーティングシステム、アプリケーションなど）、およびサービスが、組織のリスク戦略に従って管理され、機密性、完全性、および可用性を保護する。		則)。
			例 2:ソフトウェアをインストールまたはアップグレードする際に、サイバーセキュリティに影響を与える可能性のあるすべてのデフォルト設定を確認する。
			例 3:実装されたソフトウェアを監視し、承認されたベースラインからの逸脱がないか確認する。
		PR.PS-02:ソフトウェアはリスクに見合った保守、交換、削除が行われる。	例 1:脆弱性管理計画で指定された期間内に定期的および緊急のパッチ適用を実行する。
			例 2:コンテナイメージを更新し、既存のインスタンスを更新するのではなく、置き換えるために新しいコンテナインスタンスをデプロイする。
			例 3:サポートが終了したソフトウェアとサービスのバージョンを、サポートされ保守されているバージョンに置き換える。
			例 4:過度のリスクをもたらす不正なソフトウェアやサービスをアンインストールして削除する。
			例 5:攻撃者が悪用する可能性のある不要なソフトウェアコンポーネント（オペレーティングシステムユーティリティなど）をアンインストールして削除する。
			例 6:ソフトウェアとサービスの保守サポート終了と陳腐化の計画を定義して実装する。
		PR.PS-03:ハードウェアはリスクに見合った保守、交換、撤去を行う。	例 1:必要なセキュリティ機能がない場合、または必要なセキュリティ機能を備えたソフトウェアをサポートできない場合は、ハードウェアを交換する。
			例 2:ハードウェアのサポート終了と陳腐化の計画を定義して実装する。
			例 3:ハードウェアの廃棄を、安全で責任を持って、監査可能な方法で実行する。
		PR.PS-04:ログ記録を作成し、継続的なモニタリングに利用できるようにする。	例 1:すべてのオペレーティングシステム、アプリケーション、サービス（クラウドベースのサービスを含む）を構成して、ログレコードを生成する。
			例 2:組織のログ記録インフラストラクチャシステムおよびサービスとログを安全に共有するようにログジェネレーターを構成する。

			例 3:ゼロトラストアーキテクチャに必要なデータを記録するようにログジェネレーターを設定する。
		PR.PS-05:不正なソフトウェアのインストールと実行を防止する。	例 1:リスクが正当化される場合は、ソフトウェアの実行を許可された製品のみに制限するか、禁止および許可されていないソフトウェアの実行を拒否する。
			例 2:新しいソフトウェアをインストールする前に、そのソフトウェアの提供元と完全性を確認する。
			例 3:既知の悪意のあるドメインへのアクセスをブロックする承認された DNS サービスのみを使用するようにプラットフォームを構成する。
			例 4:組織が承認したソフトウェアのみのインストールを許可するようにプラットフォームを構成する。
		PR.PS-06:セキュアなソフトウェア開発プラクティスを統合し、ソフトウェア開発ライフサイクル全体を通じてそのパフォーマンスを監視する。	例 1:組織が開発したソフトウェアのすべてのコンポーネントを改ざんや不正アクセスから保護する。
			例 2:組織が作成したすべてのソフトウェアを、リリースの脆弱性を最小限に抑えて保護する。
			例 3:本番環境で使用するソフトウェアをメンテナンスし、不要になったソフトウェアは安全に廃棄する。
	技術基盤の回復力 (PR.IR):資産の機密性、完全性、可用性、および組織の回復力を保護するために、組織のリスク戦略に基づいてセキュリティアーキテクチャを管理する。	PR.IR-01:ネットワークと環境は、不正な論理アクセスや使用から保護されている。	例 1:信頼境界とプラットフォームタイプ (IT、IoT、OT、モバイル、ゲストなど) に従って、組織のネットワークとクラウドベースのプラットフォームを論理的にセグメント化し、セグメント間で必要な通信のみを許可する。
			例 2:組織のネットワークを外部ネットワークから論理的にセグメント化し、必要な通信のみが外部ネットワークから組織のネットワークに入ることを許可する。
			例 4:エンドポイントに運用リソースへのアクセスと使用を許可する前に、エンドポイントのサイバーヘルスを確認する。
			例 4:エンドポイントに運用リソースへのアクセスと使用を許可する前に、エンドポイントのサイバーヘルスを確認する。
		PR.IR-02:組織の技術資産を環境脅威から保護する。	例 1:洪水、火災、風、過度の熱と湿度などの既知の環境脅威から組織の機器を保護する。

			例 2:環境の脅威からの保護と、組織に代わってシステムを運用するサービスプロバイダーの要件に、適切な運用インフラストラクチャに関する規定を含める。
		PR.IR-03:平常時および不利な状況における回復力要件を達成するためのメカニズムが導入されている。	例 1:システムとインフラストラクチャの単一障害点を回避する。
			例 2:負荷分散を使用して容量を増やし、信頼性を向上させる。
			例 3:冗長ストレージや電源などの高可用性コンポーネントを使用して、システムの信頼性を向上させる。
		PR.IR-04:可用性を確保するために十分なリソース容量が維持されていること。	例 1:ストレージ、電源、コンピューティング、ネットワーク帯域幅、その他のリソースの使用状況を監視する。
			例 2:将来のニーズを予測し、それに応じてリソースを拡張する。
	ID 管理、認証、アクセス制御 (PR.AC) :[撤回:PR.AA に移動する。]	PR.AC-01:[撤回:PR.AA-01、PR.AA-05 に編入する。]	
		PR.AC-02:[撤回:PR.AA-06 に移動する。]	
		PR.AC-03:[撤回:PR.AA-03、PR.AA-05、PR.IR-01 に編入する。]	
		PR.AC-04:[撤回: PR.IR-01 に移動する。]	
		PR.AC-05:[撤回:PR.IR-01 に編入する。]	
		PR.AC-06:[撤回: PR.IR-02 に移動する。]	
		PR.AC-07:[撤回: PR.IR-03 に移動する。]	
	情報保護のプロセスと手順 (PR.IP) :[撤回:他のカテゴリー・機能に組み込まれる。]	PR.IP-01:[撤回: PR.PS-01 に編入する。]	
		PR.IP-02:[撤回: ID.AM-08、PR.PS-06 に編入する。]	
		PR.IP-03:[撤回: PR.PS-01、ID.RA-07 に編入する。]	

		PR.IP-04:[撤回:PR.DS-11 に移動する。]	
		PR.IP-05:[撤回:PR.IR-02 に移動する。]	
		PR.IP-06:[撤回:ID.AM-08 に編入する。]	
		PR.IP-07:[撤回:ID.IM、ID.IM-03 に編入する。]	
		PR.IP-08:[撤回:ID.IM-03 に移動する。]	
		PR.IP-09:[撤回: ID.IM-04 に移動する。]	
		PR.IP-10:[撤回:ID.IM-02、ID.IM-04 に編入する。]	
		PR.IP-11:[撤回:GV.RR-04 に移動する。]	
		PR.IP-12:[撤回:ID.RA-01、PR.PS-02 に編入する。]	
	メンテナンス (PR.MA) :撤回:ID.AM-08 に編入する。	PR.MA-01:[撤回:ID.AM-08、PR.PS-03 に編入する。]	
		PR.MA-02:[撤回: ID.AM-08、PR.PS-02 に編入する。]	
	保護技術 (PR.PT) : 撤回:他の保護カテゴリーに組み込まれる。	PR.PT-01:[撤回:PR.PS-04 に編入する。]	
		PR.PT-02:[撤回:PR.DS-01、PR.PS-01 に編入する。]	
		PR.PT-03:[撤回:PR.PS-01 に編入する。]	
		PR.PT-04:[撤回:PR.AA-06、PR.IR-01 に編入する。]	
		PR.PT-05:[撤回:PR.IR-03 に移動する。]	
検知 (DE) :サイバーセキュリティ	継続的モニタリング (DE.CM) :異常、侵	DE.CM-01:ネットワークとネットワークサービスは、潜在	例 1:DNS、BGP、およびその他のネットワークサービスで有害事象を監視する。

攻撃や侵害の可能性を発見し、分析する。	害の指標、そのほかの潜在的な有害事象を発見するために資産を監視する。	的に有害な事象を発見するために監視される。	例 2:有線および無線ネットワークを監視して、許可されていないエンドポイントからの接続を確認する。
			例 3:許可されていないワイヤレスネットワークまたは不正なワイヤレスネットワークのための施設を監視する。
			例 4:実際のネットワークフローをベースラインと比較して、偏差を検出する。
			例 5:ネットワーク通信を監視して、ゼロトラストの目的でセキュリティ体制の変更を特定する。
		DE.CM-02:潜在的に有害な事象を発見するために、物理的環境をモニターする。	例 1:物理的なアクセス制御システム（バッジリーダーなど）からのログを監視して、異常なアクセスパターン（標準からの逸脱など）と失敗したアクセス試行を見つける。
			例 2:物理的なアクセス記録（訪問者登録、サインインシートなど）を確認および監視する。
			例 3:物理的なアクセス制御（ロック、ラッチ、ヒンジピン、アラームなど）を監視して、改ざんの兆候がないか確認する。
			例 4:警報システム、カメラ、警備員を使用して物理的環境を監視する。
		DE.CM-03:潜在的な有害事象を発見するため、従業員の活動および技術利用を監視する。	例 1:行動分析ソフトウェアを使用して異常なユーザーアクティビティを検出し、内部脅威を軽減する。
			例 2:論理アクセス制御システムからのログを監視して、異常なアクセスパターンと失敗したアクセス試行を見つける。
			例 3:ユーザーアカウントを含む欺瞞技術を継続的に監視し、あらゆる使用について監視する。
		DE.CM-04:[撤回。DE.CM-01および DE.CM-09 に編入する。]	
		DE.CM-05:[撤回。DE.CM-01および DE.CM-09 に編入する。]	
		DE.CM-06:外部サービス提供者の活動およびサービスは、	例 1:外部プロバイダーが組織システムに対して実行するリモートおよびオンサイトの管理および保守活動を監視する。

		潜在的に有害な事象を発見するために監視される。	例 2:クラウドベースのサービス、インターネットサービスプロバイダー、およびその他のサービスプロバイダーからのアクティビティを監視して、予想される動作からの逸脱を確認する。
		DE.CM-07:[撤回:DE.CM-01、DE.CM-03、DE.CM-06、DE.CM-09 に編入する。]	
		DE.CM-08:[撤回:ID.RA-01 に編入する。]	
		DE.CM-09:コンピューティングのハードウェアとソフトウェア、ランタイム環境、およびそれらのデータを監視し、潜在的に有害な事象を発見する。	例 1:メール、Web、ファイル共有、コラボレーションサービス、その他の一般的な攻撃ベクトルを監視して、マルウェア、フィッシング、データ漏えいと流出、その他の有害事象を検出する。
			例 2:認証の試行を監視して、資格情報に対する攻撃と資格情報の不正な再利用を特定する。
			例 3:ソフトウェア構成のセキュリティベースラインからの逸脱を監視する。
			例 4:ハードウェアとソフトウェアを改ざんの兆候がないか監視する。
			例 5:エンドポイントに存在するテクノロジーを使用して、サイバーヘルスの問題（パッチの欠落、マルウェア感染、未承認のソフトウェアなど）を検出し、アクセスが承認される前にエンドポイントを修復環境にリダイレクトする。
	有害事象分析 (DE.AE) :異常、侵害の指標、その他の潜在的な有害事象を分析して事象を特徴づけ、サイバーセキュリティインシデントを検出する。	DE.AE-01:[撤回:ID.AM-03 に編入する。]	
		DE.AE-02:潜在的有害事象を分析し、関連する活動をよりよく理解する。	例 1:セキュリティ情報およびイベント管理（SIEM）またはその他のツールを使用して、既知の悪意のあるアクティビティや疑わしいアクティビティのログイベントを継続的に監視する。

			例 2:ログ分析ツールで最新のサイバー脅威インテリジェンスを活用して、検出精度を向上させ、脅威アクター、その方法、および侵害の兆候を特徴づける。
			例 3:自動化では十分に監視できないテクノロジーのログイベントについて、定期的に手動レビューを実施する。
			例 4:ログ分析ツールを使用して、調査結果に関するレポートを生成する。
		DE.AE-03:情報は複数の情報源から関連付けられている。	例 1:他のソースから生成されたログデータを比較的小数のログサーバに常に転送する。
			例 2:イベント関連技術（SIEM など）を使用して、複数のソースから取得した情報を収集する。
			例 3:サイバー脅威インテリジェンスを活用して、ログソース間でイベントを関連付ける。
		DE.AE-04:有害事象の推定影響と範囲が理解されている。	例 1:SIEM またはそのほかのツールを使用して、影響と範囲を見積り、見積りを確認して調整する。
			例 2:人が影響と範囲について自分で見積りを作成する。
		DE.AE-05:[撤回。DE.AE-08に移動する。]	
		DE.AE-06:有害事象に関する情報は、権限を与えられたスタッフおよびツールに提供される。	例 1:サイバーセキュリティソフトウェアを使用してアラートを生成し、セキュリティオペレーションセンター（SOC）、インシデント対応者、インシデント対応ツールに提供する。
			例 2:インシデント対応者およびそのほかの権限のある担当者は、ログ分析の結果にいつでもアクセスできる。
			例 3:特定の種類のアラートが発生したときに、組織のチケットシステムでチケットを自動的に作成して割り当てる。
			例 4:技術スタッフが侵害の兆候を発見したときに、組織のチケットシステムでチケットを手動で作成して割り当てる。
		DE.AE-07:サイバー脅威インテリジェンスとそのほかの文脈情報が分析に統合される。	例 1:サイバー脅威インテリジェンスフィードを検知技術、プロセス、および担当者に安全に提供する。
			例 2:資産インベントリから検出技術、プロセス、人員まで情報を安全に提供する。

			例 3:サプライヤー、ベンダー、サードパーティのセキュリティアドバイザリから組織のテクノロジーの脆弱性開示を迅速に取得して分析する。
		DE.AE-08:インシデントは、有害事象が定義されたインシデント基準を満たす場合に宣言される。	例 1:インシデントを宣言すべきか否かを判断するために、アクティビティの既知および想定される特性にインシデント基準を適用する。
			例 2:インシデント基準を適用する際に既知の誤検知を考慮に入れる。
	検出プロセス (DE.DP) :[撤回:他のカテゴリーおよび機能に編入する。]	DE.DP-01:[撤回:GV.RR-02に編入する。]	
		DE.DP-02:[撤回:DE.AEに編入する。]	
		DE.DP-03:[撤回:ID.IM-02に編入する。]	
		DE.DP-04:[撤回:DE.AE-06に編入する。]	
		DE.DP-05:[撤回:ID.IM、ID.IM-03に編入する。]	
対応 (RS) :検出されたサイバーセキュリティインシデントに関する対応を行う。	インシデント管理 (RS.MA) :検出されたサイバーセキュリティインシデントへの対応を管理する。	RS.MA-01:インシデント対応計画は、インシデントが宣言された後、関連する第三者と連携して実行される。	例 1:検知技術が確認済みのインシデントを自動的に報告する。
			例 2:組織のインシデント対応アウトソーシング業者にインシデント対応支援を依頼する。
			例 3:インシデントごとにインシデントリードを指名する。
			例 4:インシデント対応（ビジネス継続性やディザスタリカバリーなど）をサポートするために、必要に応じて追加のサイバーセキュリティ計画の実行を開始する。
		RS.MA-02:インシデント報告はトリージアされ、検証される。	例 1:インシデントレポートを事前にレビューして、サイバーセキュリティ関連であり、インシデント対応活動が必要であることを確認する。
			例 2:インシデントの重大度を見積る条件を適用する。
		RS.MA-03:インシデントは分類と優先順位付けされる。	例 1:インシデントの種類（データ侵害、ランサムウェア、DDoS、アカウント侵害など）に基づいてインシデントをさらにレビューし、分類する。

			例 2: インシデントの範囲、予想される影響、およびタイムクリティカルな性質に基づいてインシデントに優先順位を付ける。
			例 3: インシデントから迅速に復旧する必要性と、攻撃者を観察したり、より徹底的な調査を実施したりする必要性とのバランスを取ることで、アクティブなインシデントのインシデント対応戦略を選択する。
		RS.MA-04: インシデントは必要に応じてエスカレーションまたは昇格される。	例 1: 進行中のすべてのインシデントのステータスを追跡して検証する。
			例 2: インシデントのエスカレーションまたは昇格を、指定された内部および外部の利害関係者と調整する。
		RS.MA-05: 事故復旧の開始基準が適用される。	例 1: インシデントの既知および想定される特性にインシデント復旧基準を適用して、インシデント復旧プロセスを開始する必要があるか否かを判断する。
			例 2: インシデント復旧活動の運用中断の可能性を考慮に入れる。
	インシデント分析 (RS.AN): 効果的な対応を確保し、フォレンジックと復旧活動をサポートするために調査を実施する。	RS.AN-01: [撤回: RS.MA-02 に編入する。]	
		RS.AN-02: [撤回: RS.MA-02、RS.MA-03、RS.MA-04 に編入する。]	
		RS.AN-03: インシデント発生時に何が起きたか、またその根本原因を特定するために分析を行う。	例 1: インシデント中に発生したイベントのシーケンスと、各イベントに関連した資産とリソースを特定する。
			例 2: インシデントに直接的または間接的に関連した脆弱性、脅威、および脅威アクターの特定を試みる。
			例 3: インシデントを分析して、根底にある体系的な根本原因を見つける。
			例 4: サイバーデセプションテクノロジーで攻撃者の行動に関する追加情報を確認する。
		RS.AN-04: [撤回: RS.MA-03 に移動する。]	
		RS.AN-05: [撤回: ID.RA-08 に移動する。]	

		RS.AN-06:調査中に行われた行為は記録され、記録の完全性と出所は保全される。	例 1:各インシデント対応者と、インシデント対応タスクを実行する他の人（システム管理者、サイバーセキュリティエンジニアなど）に、自分の行動を記録し、記録を不変にするように要求する。
			例 2:インシデントのリーダーにインシデントを詳細に文書化し、文書化の完全性と報告されるすべての情報のソースを維持する責任を持つように要求する。
		RS.AN-07:インシデントデータとメタデータを収集し、その完全性と出所を保全する。	例 1:証拠保全と CoC（Chain of Custody）の手続きに基づいて、関連するすべてのインシデントデータとメタデータ（データソース、収集日時など）の完全性を収集、保存、保護する。
		RS.AN-08:事故の規模を推定し、検証する。	例 1:インシデントのほかの潜在的なターゲットを確認して、侵害の兆候と持続性の証拠を検索する。
			例 2:ターゲットに対してツールを自動的に実行して、侵害の兆候と持続性の証拠を探す。
	インシデントレスポンスの報告とコミュニケーション（RS.CO）：対応活動は、法律、規制、またはポリシーの要求に従って、社内外の利害関係者と調整される。	RS.CO-01:[撤回:PR.AT-01 に編入する。]	
		RS.CO-02:社内外の利害関係者にインシデントを通知する。	例 1:データ侵害インシデントを発見した後、影響を受けた顧客への通知を含む、組織の侵害通知手順に従う。
			例 2:契約上の要件に従って、ビジネスパートナーや顧客にインシデントを通知する。
			例 3:インシデント対応計画の基準と経営陣の承認に基づいて、法執行機関および規制機関にインシデントを通知する。
		RS.CO-03:指定された社内外のステークホルダーと情報を共有する。	例 1:対応計画と情報共有契約に則った情報を安全に共有する。
			例 2:攻撃者が観測した TTP に関する情報を、すべての機密データを削除した状態で、情報共有分析センター（ISAC）と自発的に共有する。
			例 3:悪意のある内部関係者の活動が発生したときに人事部に通知する。
			例 4:重大インシデントの状況について、上級管理職に定期的に最新情報を提供する。
			例 5:組織とそのサプライヤー間のインシデント情報共有に関する契約で定義されているルールとプロトコルに従う。

			例 6:組織とその重要なサプライヤーとの間の危機管理コミュニケーション方法を調整する。
		RS.CO-04:[撤回:RS.MA-01、RS.MA-04 に編入する。]	
		RS.CO-05:[撤回:RS.CO-03 に編入する。]	
	事故の緩和 (RS.MI) :事象の拡大を防ぎ、その影響を緩和するための活動。	RS.MI-01:インシデントを封じ込める。	例 1:サイバーセキュリティ技術（ウイルス対策ソフトウェアなど）と他の技術のサイバーセキュリティ機能（オペレーティングシステム、ネットワークインフラストラクチャデバイスなど）は、自動的に封じ込めアクションを実行する。
			例 2:インシデント対応者が手動で封じ込めアクションを選択して実行できるようにする。
			例 3:第三者（インターネットサービスプロバイダー、マネージドセキュリティサービスプロバイダーなど）が組織に代わって封じ込めアクションを実行できるようにする。
			例 4:侵害されたエンドポイントを修復仮想ローカルエリアネットワーク（VLAN）に自動的に転送する。
		RS.MI-02:インシデントを根絶する。	例 1:サイバーセキュリティ技術と他の技術（オペレーティングシステム、ネットワークインフラストラクチャデバイスなど）のサイバーセキュリティ機能は、自動的に根絶アクションを実行する。
			例 2:インシデント対応者が手動で根絶アクションを選択して実行できるようにする。
			例 3:第三者（マネージドセキュリティサービスプロバイダーなど）が組織に代わって根絶アクションを実行できるようにする。
		RS.MI-03:[ID.RA-06 に編入する。]	
	対応計画 (RS.RP) :[撤回:RS.MA に編入する。]	RS.RP-01:[撤回:RS.MA-01 に編入する。]	
	改善点 (RS.IM) :[撤回:ID.IM に編入する。]	RS.IM-01:[撤回:ID.IM-03、ID.IM-04 に編入する。]	

	る。]	RS.IM-02:[撤回:ID.IM-03 に 編入する。]	
復旧（RC）:サイ バーセキュリティ インシデントの影 響を受けた資産や 業務を復旧させ る。	インシデント復旧計画 の実行（RC.RP）:サイ バーセキュリティイ ンシデントの影響を受 けたシステムとサービ スの運用可用性を確保 するための復旧活動を実 施する。	RC.RP-01:インシデント対応 計画の復旧部分は、インシ デント対応プロセスから開始さ れると実行される。	例 1:インシデント対応プロセス中またはインシデント対応 プロセス後に復旧手順を開始する。 例 2:回復の責任を負うすべての個人に、回復の計画と、計 画の各側面を実装するために必要な権限を認識させる。
		RC.RP-02:復旧アクションの 選択、範囲設定、優先順位付 け、実行を行う。	例 1:インシデント対応計画と利用可能なリソースで定義さ れた基準に基づいて復旧アクションを選択する。 例 2:組織のニーズとリソースの再評価に基づいて計画され た復旧アクションを変更する。
		RC.RP-03:バックアップやそ のほかのリストア資産をリス トアに使用する前に、その完 全性を検証する。	例 1:使用前に、復元資産に侵害、ファイルの破損、そのほ かの整合性の問題の兆候がないか確認する。
		RC.RP-04:重要なミッション 機能とサイバーセキュリティ のリスク管理は、事故後の運 用規範を確立するために考慮 される。	例 1:ビジネスへの影響とシステムの分類レコード（サービ ス提供目標を含む）を使用して、重要なサービスが適切な順 序で復元されていることを検証する。
			例 2:システム所有者と協力して、システムの正常な復元と 通常の運用への復帰を確認する。
			例 3:復元されたシステムのパフォーマンスを監視して、復 元の適切性を確認する。
		RC.RP-05:復旧した資産の完 全性が検証され、システムと サービスが復旧し、正常な運 用状態が確認される。	例 1:復元された資産で侵害の兆候を確認し、本番環境で使 用する前にインシデントの根本原因を修復する。
			例 2:復元されたシステムをオンラインにする前に、実行さ れた復元アクションの正確性と妥当性を確認する。
		RC.RP-06:基準に基づいて事 故復旧の終了が宣言され、事 故関連の文書化が完了する。	例 1:インシデント自体、実行された対応措置と復旧措置、 および学んだ教訓を文書化した事後処理レポートを作成す る。
			例 2:基準が満たされたら、インシデント復旧の終了を宣言 する。
	事故復旧コミュニケー ション（RC.CO）:復	RC.CO-01:[撤回:RC.CO-04 に編入する。]	

	旧活動を社内外の関係者と調整する。	RC.CO-02:[撤回:RC.CO-04に編入する。]	
		RC.CO-03:復旧活動と業務能力回復の進捗状況を、指定された社内外の利害関係者に伝達する。	例 1:復旧の進行状況を含む復旧情報を安全に共有し、対応計画と情報共有契約に則った対応する。
			例 2:重大インシデントの復旧状況と復旧の進捗状況について、上級管理職に定期的に最新情報を提供する。
			例 3:組織とそのサプライヤー間のインシデント情報共有に関する契約で定義されたルールとプロトコルに従う。
			例 4:組織とその重要なサプライヤーとの間の危機管理コミュニケーションを調整する。
	改善点 (RC.IM):撤回:ID.IM に編入する。	RC.CO-04:承認された方法とメッセージングを使用し、事故復旧に関する一般向けの最新情報を共有する。	例 1:データ侵害インシデントから回復するための組織の侵害通知手順に従う。
			例 2:インシデントから回復し、再発を防ぐために実行している手順を説明する。
	改善点 (RC.IM):撤回:ID.IM に編入する。	RC.IM-01:[撤回:ID.IM-03、ID.IM-04 に編入する。]	
		RC.IM-02:[撤回:ID.IM-03 に編入する。]	

詳細理解のため参考となる文献 (参考文献)	
NIST Cybersecurity Framework (CSF) 2.0 Reference Tool	https://csrc.nist.gov/extensions/nudp/services/json/csf/download?olirids=all

中小企業向けスタートアップガイドの活用方法

中小企業が、CSF2.0 を使用してセキュリティ対策を開始するにあたり、クイックスタートガイド (Small Business Quick-Start Guide) が参考になります。このガイドは、セキュリティ対策が十分でない中小企業に対して、セキュリティ対策を始めるための基本的なステップを提供します。ガバナンス、識別、防御、検知、対応、復旧、各機能それぞれにおいて、段階的に対策を進める方法を示しています。

このガイドは、必要に応じて外部の専門家やサービスの利用を検討するための指針にもなります。各機能の活動の中から 1 つを例にとり、どのような内容が記載してあるかを説明します。

ガバナンス

ガバナンス機能は、ビジネスのサイバーセキュリティリスク管理戦略、期待値、ポリシーを確立し、監視するのに役立ちます。

考慮すべきアクション

理解
● サイバーセキュリティリスクが、ビジネスの目標達成をどのように妨げる可能性があるかを理解する。(GV.OC-01) ● 法的、規制上、および契約上のサイバーセキュリティ要件を理解する。(GV.OC-03) ● ビジネス内で誰がサイバーセキュリティ戦略を策定し、実行する責任を負うかを理解する。(GV.RR-02)
評価
● ビジネスにとって大事な資産や運営がすべて、または一部失われた場合にどんな影響が出るかを評価する。(GV.OC-04) ● 自社にサイバーセキュリティ保険が必要か否かを評価する。(GV.RM-04) ● 取引を開始する前に、取引先や他の第三者がもたらすサイバーセキュリティリスクを評価する。(GV.SC-06)
優先
● サイバーセキュリティリスクを、他のビジネスリスクと同じように優先して管理する。(GV.RM-03)
コミュニケーション
● 経営陣がリスクに気を配り、倫理的で常に改善を目指す姿勢をサポートしていることを伝える。(GV.RR-01) ● サイバーセキュリティリスクを管理するためのポリシーを伝達し、実施し、維持する。(GV.PO-01)

サイバーセキュリティ統制の始め方

以下の表を使って、サイバーセキュリティ統制戦略について考え始めることができます。

組織の目的や状況の整理	
組織の使命や目標	
組織の使命や目標の達成を妨げる可能性があるセキュリティリスクは何か？	

セキュリティ要件の文書化	
法的要件をリスト化する	
規制要件をリスト化する	
契約上の要件をリスト化する	

サイバーセキュリティ統制の始め方

(出典) NIST「NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide」をもとに作成

考慮すべきポイント

- ビジネスが成長するにつれて、どのくらいの頻度でサイバーセキュリティ戦略を見直していますか？
- 既存従業員のスキルアップが必要ですか？または、専門知識を持つ新しい人材を採用するか、外部のパートナーと協力してサイバーセキュリティ計画を確立し、管理する必要がありますか？
- 会社のデバイスおよび従業員の私物デバイスが会社の資産にアクセスする際の、適切な利用ポリシーは整っていますか？従業員はこれらのポリシーについて教育を受けていますか？

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide	https://doi.org/10.6028/NIST.SP.1300

経営層向けカリキュラム

経営層向け第1単元	
名称	1.基礎知識 『デジタルシステムとサイバーセキュリティの概要』
目標	● デジタルシステムとそのサイバーセキュリティ対策に関して経営層として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ➢ 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ➢ 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● 関係者とのコミュニケーションにおいて用いられる概念と用語について、コミュニケーションに支障の無い程度の理解を得る。
時間設定・実施方式	1 時間 30 分（オンデマンド・省略可能）
①デジタルインフラの基本（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。受講者の負担軽減の観点から、まとめて学習するほうがよい内容を適宜集約する。 a) デジタルサービスの提供に用いられるハードウェアの概要 b) OS、ミドルウェア、アプリケーション、クラウドの概念説明 c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤー
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェアと脆弱性 b) インターネットの仕組み c) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用

	b) デジタルサービスの約款 c) インシデント時の事業継続

経営層向け第2単元	
名称	2.脅威と対策 『サイバー空間における脅威と対策』
目標	脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。
時間設定・実施方式	1 時間 30 分（オンデマンド 60 分、集合講習 30 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第3単元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法 b) 対策実施上の留意点
③事例紹介（集合講習・30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的にリスクが発現したケースについて被害と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。 - ケース紹介（例：工場停止の影響） - ゲストスピーカーによる説明（例：当事者視点でのインシデント経過の説明）

- ・ デモンストレーション（例：ランサムウェア感染のデモ）

経営層向け 第3単元	
名称	3.投資 『サイバーセキュリティと投資対効果』
目標	● どのような場合にサイバーセキュリティリスクが企業価値の毀損を生じさせるのかを理解し、それを防ぐために日常でサイバーセキュリティ対策としてどのような投資などの方策を行うべきかに関して適切な判断を行えるようになる。
到達レベル	● 自社におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制構築や人材確保・育成に関する指示を行えるようになる。 ● セキュリティ対策の担当者から提示されるセキュリティ対策案について、経営層として妥当性に関する判断を下せるようになる。
時間設定・実施方式	2 時間 10 分（オンデマンド 60 分、集合講習 70 分）
①コーポレートリスクとしてのサイバーセキュリティ（オンデマンド・30 分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。受講者がリスクマネジメントそのものの考え方や保険の仕組みなどは理解していることを前提に、②以降の説明で必要となる概念を確認する。 a) サイバーセキュリティリスクのアセスメント b) リスクへの対応方法 c) 関連法制度とコンプライアンス
②体制構築・人材確保（オンデマンド・30 分）	各種公表資料を参考に、企業の特徴に応じた体制や人材確保・育成に関する考え方を理解する。 a) サイバーセキュリティ対策に関する機能と役割の考え方 b) 外部委託の考え方 c) サイバーセキュリティ体制の構築 d) サイバーセキュリティ対策に従事する人材の確保・育成
③演習 1：各種対策の費用、損失想定、確率値から必要な投資を検討（集合講習：70 分）	サイバーセキュリティ対策における費用対効果分析の基本的な考え方について、事例を踏まえて説明する。受講者 3～4 名で 1 チームを構成し、具体例を想定した上で、ゲーム形式で各種対策の費用、損失想定、確率値から必要な投資を検討し、トータルコストの最小化を競う。

経営層向け 第4単元	
名称	4.ステークホルダーとの関係 『サイバーセキュリティと企業価値』
目標	サイバーセキュリティインシデントの発生時の適切な対応について理解した上で、企業価値を損なわないためにあらかじめ備えておくべきことを自社の事情に応じてイメージできるようになる。
到達レベル	自社におけるインシデント対応を含むサイバーセキュリティ対策に関する取組方針について、対外的に説明や意見交換ができるレベルの理解に到達する。
時間設定・実施方式	2時間 20分（オンデマンド 60分、集合講習 80分）
①インシデント対応における経営層の役割（オンデマンド・30分）	サイバーセキュリティインシデントの対応プロセスにおいて、経営層がどの場面でどのようにかかわるのが適切なのかを理解する。 a) インシデントに備える b) インシデント対応プロセス
②情報開示の在り方（オンデマンド・30分）	サイバーセキュリティ対策を適切に実施していることを取引先や社会に伝えることにより、企業価値の維持・向上を図る方法について理解する。 a) サイバーセキュリティに関する情報開示の考え方 b) サイバーセキュリティが企業価値に及ぼす影響
③インシデント対応と情報開示の事例から学ぶ（集合講習：30分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法等、実践的な内容を説明する。
④演習2：インシデント発生時の模擬記者会見（集合講習：50分）	受講者3～4名で1テーブルとして、経営者役の1名が、マスメディアや企業の広報部門等で記者会見対応に関する経験を有するスタッフが演じるインタビュー役から、自社でのインシデント発生に関する模擬記者会見を行う。

（出典）NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

部課長向けカリキュラム

部課長級向け 第1-1単元	
名称	1.基礎知識

	『デジタルシステムとサイバーセキュリティの概要（初級編）』
目標	デジタル化を推進する部門のマネジメントを担う部課長として中級編の目標に到達するために必要となる、最低限の基礎知識を習得する。
到達レベル	● デジタルシステムとインターネットおよびそれらのセキュリティ対策において用いられる最低限の知識を習得する。
時間設定・実施方式	1 時間（オンデマンド・省略可能）
①デジタルインフラ入門（20 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素について、基本的な用語の意味を理解する。 a) デジタルサービスの提供に用いられるハードウェアの紹介 b) OS、ミドルウェア、アプリケーション、クラウドの用語説明 c) IT/OT/IoT がそれぞれ意味するもの
②サイバーセキュリティに関する用語の意味（20 分）	「セキュリティは難しい」という印象を与える背景として、「脆弱性」など日常で用いられないさまざまな用語が用いられることから、よく用いられるサイバーセキュリティ用語の意味の説明を通じて理解を深める。 なお、サイバーセキュリティ用語を説明する上で必要となる、ソフトウェアやネットワークに関する用語についても併せて説明する。 a) ソフトウェア開発と脆弱性 b) インターネットの仕組み c) デジタルのリスクに関する諸概念
③デジタル環境の管理や責任に関するキーワード（20 分）	インターネットを通じたサービスなどの提供主体と責任に関する用語について説明する。 a) デジタルビジネスの提供者に関する用語 b) 管理と責任の所在

部課長級向け 第 1-2 単元	
名称	1.基礎知識 『デジタルシステムとサイバーセキュリティの概要（中級編）』
目標	デジタル化を推進する部門のマネジメントを担う部課長として次のような場面において適切な判断を行う上で、どのようなことを予め知っておくべきなのかの自覚を促す。 ● 担当者による提案についての、自社のニーズ、競争力、コストなどの面からの妥当性 ● 新たな施策に伴うリスクとその抑制策の妥当性
到達レベル	● デジタルシステムとサイバーセキュリティに関する用語と概念につ

	いて、第2単元目以降の学習を行うために予め習得しておくべきレベルに到達させる。具体的には、対象とする用語と概念を用いて、デジタルシステムやサイバーセキュリティ対策に関するソリューションを提供するベンダーとの実用的な対話に支障の無い程度の理解を得ることとする。
時間設定・実施方式	1 時間 30 分（オンデマンド・必須）
①デジタルインフラの要点（30 分）	ビジネスで用いられるデジタルアーキテクチャの構成要素とその意味について概説する。 a) デジタルサービスの提供に用いられるハードウェアの構成要素 b) OS、ミドルウェア、アプリケーション、クラウドなどの概念説明 c) IT/OT/IoT の違い、クラウド/オンライン会議の仕組み d) デジタルビジネスの主要プレイヤーの役割
②デジタル技術の基盤とリスク（30 分）	デジタル環境の利便性の代償としてシステムトラブルやサイバーセキュリティインシデントがあり、それぞれリスクに応じた対策が用意されているが、一般に対策の効果を高めるほど、利便性又はコストに影響が及ぶ関係にあることを説明する。 a) ソフトウェア開発と脆弱性 b) デジタルリスクとその対策に関する技術的概念
③デジタル環境のコストと運用責任（30 分）	デジタル基盤を快適に利用している中で、どこにどのように費用がかかっているのかについて、課金方法の種類を含めて説明する。また、トラブルが生じたときのベンダーとの責任分界点や、事業継続計画の必要性について説明する。 a) インターネットを安全に利用するための費用 b) デジタルサービスの約款 c) インシデント時の事業継続

部課長級向け 第2単元	
名称	2.脅威 『サイバー空間における脅威と対策』
目標	脅威および脆弱性とその対策に関する理解を通じて、サイバー空間における主要な脅威を事業上のリスクとして適切に把握できるようになる。
到達レベル	● 現在のデジタル環境では脆弱性による影響をゼロにできず、最新の脅威につねに対処していく必要があることを理解し、対策をしなかった場合の自社での被害想定ができるようになる。

時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）
①サイバー攻撃手法とそのトレンド（オンデマンド・30 分）	サイバーセキュリティリスクをもたらす脅威について、誰がどのように影響を及ぼすのかの概要を説明した上で、現在のトレンドから、今後自社にどのようなインパクトを及ぼす脅威が見込まれるのかを、具体的な被害事例を交えて説明する。 a) おもな攻撃手法 b) 脅威の関係主体と攻撃の動向 c) 最新の脅威
②脅威への対策（オンデマンド・30 分）	脅威による影響を抑制する手段としてどのようなものがあるか説明する。第3單元において自社事業の内容に応じたリスクへの対応方法を扱うことを踏まえ、その前提となる基本的な考え方の理解に重点を置く。 a) 対策の具体的な運用方法 b) 対策実施上の留意点
③事例紹介（集合講習：30 分）	①②をオンデマンド教材によって行うことへの補強として、具体的な脅威と対策の事例を紹介し、対策が期待通りに行かないのはどのような場合かなど、実践的な内容を説明する。＜デモンストレーションの実施についても検討＞
④演習 1：脅威と対策における“悪い見本”から学ぶ（集合講習：60 分）	受講者 3～4 名で 1 テーブルとして、仮想の企業が実施する脅威への不適切な事前準備（リスク評価、資産管理、パッチ適用、従業員教育など）に関する動画（8 分程度）を視聴し、どこに問題があるかを理由と共に指摘し合う。なお、本ディスカッションでは問題の抽出のみにとどめ、対策方法には踏み込まない。

部課長級向け 第 3 單元	
名称	3.投資 『サイバーセキュリティとリスク対応』
目標	自部署におけるサイバーセキュリティリスクのマネジメントに必要なとなる概念と、具体的なアクションについて理解する。
到達レベル	● 部署におけるサイバーセキュリティリスクを特定し、対応の優先順位付けや対処方針の選定を行うとともに、その実現に必要な体制や要員の確保・育成を行えるようになる。 ● 担当者や社外ベンダーから提示されるセキュリティ対策案について、組織として妥当性に関する判断を下せるようになる。
時間設定・実施方式	2 時間 30 分（オンデマンド 60 分、集合講習 90 分）

①サイバーセキュリティのリスクマネジメントの特徴（オンデマンド・30分）	サイバーセキュリティリスクは他のコーポレートリスクとどのように異なるかを、対応方法を通じて理解する。 a) サイバーセキュリティにおけるリスクの特徴 b) リスクへの対応方法 c) サイバーセキュリティ対策に関する機能と役割の考え方
②対策における費用と損失の考え方（オンデマンド・30分）	費用をかけてサイバーセキュリティ対策を実施しても、インシデントが生じない場合の効果が見えにくい。その場合に「何も対策をしていなければ」といった仮定により想定される損失額を試算し、妥当性を評価する方法について理解する。 a) サイバーセキュリティインシデントによる損失 b) 発生確率の考え方 c) 費用と効果のバランス
③リスクマネジメントのケーススタディ（集合講習：30分）	①②をオンデマンド教材によって行うことへの補強として、具体的なリスク対応体制の事例を紹介し、発生確率や被害の大きさに関する仮定の置き方によってどのように分析結果が変化するかなど、実践的な内容を説明する。
④演習2：自部署リスクとその対応策を洗い出し、リスク管理部門などへ説明（集合講習：60分）	受講者3～4名で1チームを構成し、各参加者はあらかじめ自業種のビジネスモデルと想定するリスクについて整理したものを持ち寄る。それを他の参加者でサイバーセキュリティリスクがどのようなところにあるかを、第3単元の内容をもとに相互に指摘する。それについて、第3単元で学習したリスクの低減策のうち、どれを適用すべきかを②の内容を踏まえて受講者で議論。1クール12～15分＋講師の講評で構成。

部課長級向け 第4単元	
名称	4.ステークホルダーとの関係 『サイバーセキュリティ対応における社内外連携』
目標	デジタル化を推進していく際のサイバーセキュリティ対策、運用時のインシデントへの適切な対応について理解した上で、その効果を担保するために実施すべき情報開示や連絡の内容と効果的な方法について理解し、実践できるようになる。
到達レベル	● 自部署に係るサイバーセキュリティ対策に関する社内外のコミュニケーション（情報収集、協議、エスカレーションなど）について、実用レベルで実施できる。
時間設定・実施方式	2時間30分（オンデマンド60分、集合講習90分）

①インシデント対応プロセスとその準備（オンデマンド・30分）	サイバーセキュリティインシデントの対応プロセスの一連の流れを理解する。 a) インシデントに備える b) インシデント対応プロセス
②インシデント時の情報の取扱上のポイント（オンデマンド・30分）	即応性や要求されるインシデント発生時に、社内関係者や取引先との間でどのような情報のやりとりが必要になるか、そのために予め準備しておくことは何か、確実性を含む情報をどのように取り扱うべきかなどについて理解する。 a) インシデント時に提供すべき情報の種類と流れ b) 不確実性を含む情報の取扱い
③インシデント対応と情報開示の事例から学ぶ（集合講習：30分）	①②をオンデマンド教材によって行うことへの補強として、インシデント対応と情報開示の事例を紹介し、当初の見通しと異なる状況が生じた場合の適切な対応方法など、実践的な内容を説明する。
④演習3：インシデント発生時の社内外連絡（集合講習：60分）	受講者3～6名で1テーブルとして、社内関係者や取引先の役割を演じる受講者に対し、所管部署の事業を通じて発生したインシデントに関する情報を伝え、不満や混乱を生じさせないためにはどのような点に留意すべきかを工夫する。あらかじめ講師側にてインシデントのシナリオを作成しておき、被害状況やSOCから提供される情報を時間経過に応じて小出しの形で提供する。小出しする方法はカードに記載して提示、あるいはオンライン会議システムのチャット機能で提供するなど工夫してよい。最終的に、判断が適切に行えていたか否かを自己評価し、講師側の評価と対比する。

部課長級向け 第5単元	
名称	5.関連法令 『サイバーセキュリティに関する法制度』
目標	サイバーセキュリティ対策で関連する法律、基準、ガイドラインなどについて、実用上支障が無い程度の理解を得る。
到達レベル	● デジタル化に関連する取組の中で、遵守すべき法律、基準、ガイドラインなどを意識することができる。
時間設定・実施方式	1時間（オンデマンド・必須）
①サイバーセキュリティに関する国内法	サイバーセキュリティ対策の企画・実践に従事する要員が留意すべき法令と具体的な解釈の方法について、『サイバーセキュリティ関係法令

令とその読み方 (20 分)	Q&A ハンドブック』の活用を前提に紹介する。 a) サイバーセキュリティ対策において留意すべき法令 b) 『サイバーセキュリティ関係法令 Q&A ハンドブック』の活用
②サイバーセキュリティに関する基準・規格など (20 分)	サイバーセキュリティ対策を実践する上で留意すべき国際基準や規格などについて紹介する。 a) サイバーセキュリティに関する基準・規格など
③サイバーセキュリティに関するガイドラインなど (20 分)	企業がサイバーセキュリティ対策を実践する上で活用が有益なガイドライン・フレームワークなどを紹介する。 a) サイバーセキュリティに関するガイドライン・フレームワークなど

(出典) NISC「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに作成

IT 入門 (1)

タイトル	学習目標
オリエンテーション、情報化の変遷と代表的な情報システムの特徴	情報化の変遷と代表的な情報システムの特徴を説明できる。
業種別、業務別の代表的なシステムの概要	企業の組織と利用されている業種別、業務別の代表的なシステムの概要を説明できる。
企業活動と企業会計の基本用語	企業活動の成果を評価するための、会計の基本用語を説明できる。
情報化戦略を策定するために必要な基本用語	経営目標から情報化戦略を策定するために必要な、基本的な用語を説明できる。
情報システム戦略の目的と考え方	企業の事業戦略を受けて、情報システム戦略と全体システム化計画策定に必要な手順と用語が説明できる。
業務要件定義と解決策の検討	情報システム戦略を受けて、自部門の業務課題を分析して、業務要件を定義する代表的な手法と用語を説明できる。
企業規範と身近な法律用語	企業の規範、社会・職場で必要となる身近な法律の用語を説明できる。
前半のまとめ	これまでのストラテジ系科目全体の講義のまとめを行う。
ソフトウェア開発プロセスの作業概要と手順	業務要件をもとに、システム要件の定義から稼働までの作業手順と作業項目の用語を説明できる。
代表的なソフトウェア開発手法の概要	代表的な開発手法に関する目的と概要を説明できる。
情報化におけるプロジェクトの種類とプロジェクト遂行の手順	情報化におけるプロジェクトの種類とプロジェクト計画の立案、開発管理、プロジェクトの完了までの手順と用語を説明できる。
システム運用に関する基本用語	IT サービスマネジメントの意義と目的、サービスマネジメントの全体像とシステム運用に関する用語を説明できる。
システム監査の種類と必要性	情報システムの信頼性、安全性、効率性の向上のために行う、システム監査の必要性および監査の種類と用語を説明できる。
後半のまとめ	これまでのマネジメント系科目全体の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラムーレベル1を目指してー」をもとに作成

IT 入門 (2)

タイトル	学習目標
オリエンテーション、コンピュータ上での情報表現	数値や文字情報をコンピュータ上で表現する方法と用語を説明できる。
プログラミングの役割	アルゴリズムとプログラミングとの関係を説明できる。
コンピュータの種類と構成する装置	コンピュータを構成する装置と役割を説明できる。
ソフトウェアの種類と役割	ソフトウェアの種類と役割を説明できる。
システム処理形態と処理方式	システムの処理形態と処理方式の用語を説明できる。
前半のまとめ	前半の講義のまとめを行う。
マルチメディアとヒューマンインタフェース	マルチメディアの種類とヒューマンインタフェースの基本的な用語を説明できる。
ネットワーク技術の活用①	インターネットの仕組みと通信サービスの特徴を説明できる。
ネットワーク技術の活用②	通信網と通信プロトコルに関する用語を説明できる。
データベースの技術①	データベースのモデル化と正規化の方法を説明できる。
データベースの技術②	データベースの表操作の方法を説明できる。
情報セキュリティ対策①	セキュリティ対策に関する基本的な用語を説明できる。
情報セキュリティ対策②	セキュリティ対策に関する基本的な用語を説明できる。
後半のまとめ	後半の講義のまとめを行う。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラム－レベル1を目指して－」をもとに作成

パーソナルスキル入門

タイトル	学習目標
オリエンテーション、職業人に求められるパーソナルスキル	本科目の学習目標や進め方を理解する。職業人として企業で求められるパーソナルスキルの概要を説明できる。
ビジネスマナーの基本①	職業人としてお客様や組織から信頼を得るために必要なビジネスマナーの基本動作が行える。
ビジネスマナーの基本②	職業人として適切な電話対応、報告／連絡／相談、顧客対応が行える。
コミュニケーションの基本(2WAY) ①	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して傾聴やインタビューができる。

コミュニケーションの基本 (2WAY) ②	職業人として求められる基本的な 2WAY コミュニケーションの知識を活用して、上司への業務報告やチームの合意形成ができる。
コミュニケーションの基本 (情報伝達)	職業人として求められる基本的な情報伝達の知識を業務に活用できる。
コミュニケーションの基本 (情報伝達) 文書編①	職業人が現場で実践するビジネス文書の基本的な作成方法を説明できる。
コミュニケーションの基本 (情報伝達) 文書編②	職業人として求められる高品質なビジネス文書の作成方法を理解し、正確でわかりやすいビジネス文書を作成できる。
コミュニケーションの基本 (情報伝達) プ レゼンテーション編①	職業人が現場で実践する情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本 (情報伝達) プレゼンテーシ ョン編②	職業人が現場で実践する情報伝達としての高品質な情報伝達としての基本的なプレゼンテーション方法を説明できる。
コミュニケーションの基本 (情報整理・分析・検索) ①	職業人が現場で実践する基本的なコミュニケーションマネジメントを説明できる。
コミュニケーションの基本 (情報整理・分析・検索) ②	職業人として求められるコミュニケーションマネジメントの知識を活用して円滑な会議を進められる。
リーダーシップの基本	職業人に求められるリーダーシップ基本と原則を説明できる。
ネゴシエーションの基本	職業人に求められるネゴシエーションの基本と原則を説明できる。
まとめ	これまでの講義内容を総括する。

(出典) IPA「IT スキル標準モデルカリキュラムーレベル1 を目指してー」をもとに作成

中小企業向け サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速



令和 6 年 3 月第 1 版 令和 7 年 3 月第 2 版発行

編集・発行 東京都産業労働局商工部経営支援課
新宿区西新宿二丁目 8 番 1 号
電話番号 03(5320)4773

印刷

登録番号 (6) 174

協力 東京中小企業サイバーセキュリティ支援ネットワーク (Tcyss)

ガイドブックの利用について

このガイドブックは、東京都が著作権を保有しておりますが、利用に際しては、非営利目的、サイバーセキュリティ対策の普及・啓発目的であれば、事前の申請等は必要ありません。

全体を利用されるのであればそのままご利用いただけます。また、一部分の「引用・参考・参照・転載」であれば、出典元を明記して頂ければご利用いただけます。

★ガイドブックのライセンス



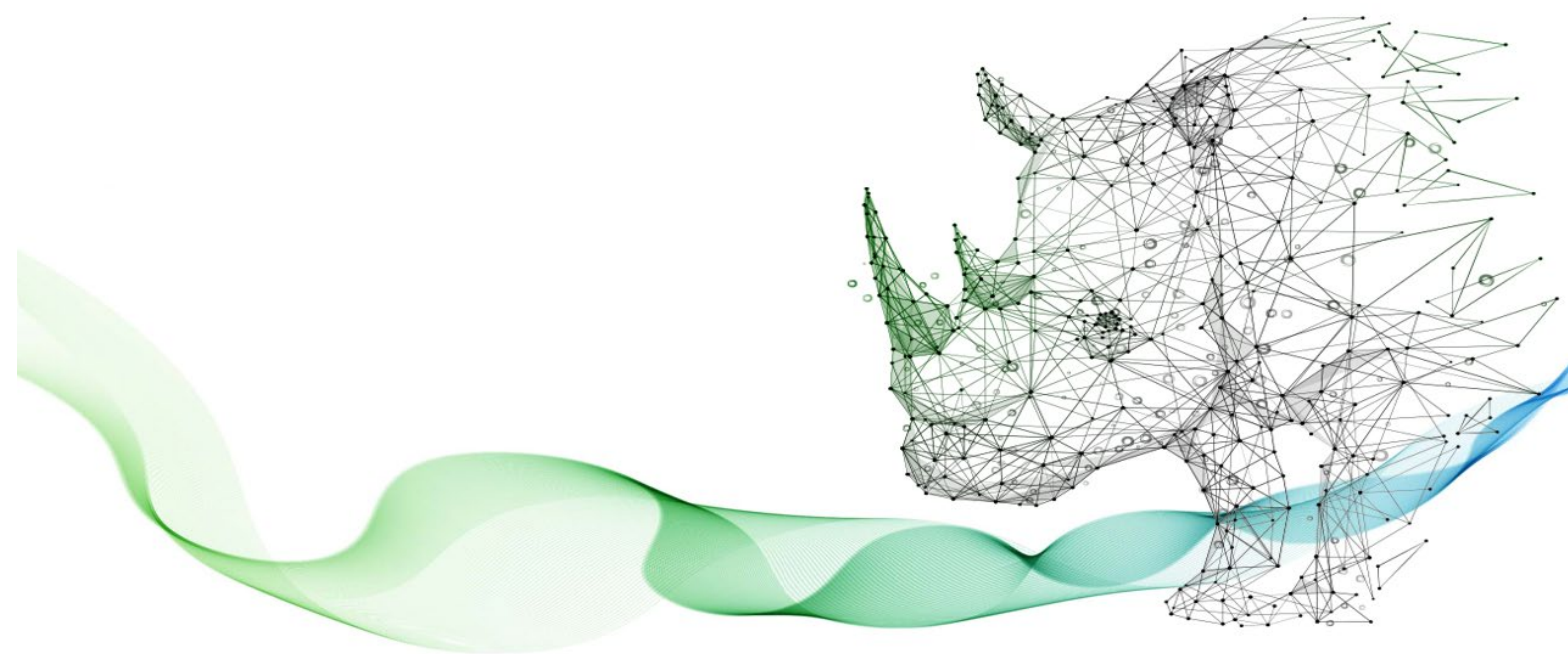
このガイドブックは、利用の条件として、クリエイティブコモンズライセンス「表示-非営利-継承 4.0 国際 (CC BY-NC SA 4.0)」を適用しています。

<https://creativecommons.org/licenses/by-nc-sa/4.0/deed.ja>

VEGETABLE
OIL INK

リサイクル適正
A

※掲載の情報は令和 7 年 3 月現在のものです。



中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速



東京都産業労働局