令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

セミナースライド

東京都産業労働局

講師紹介

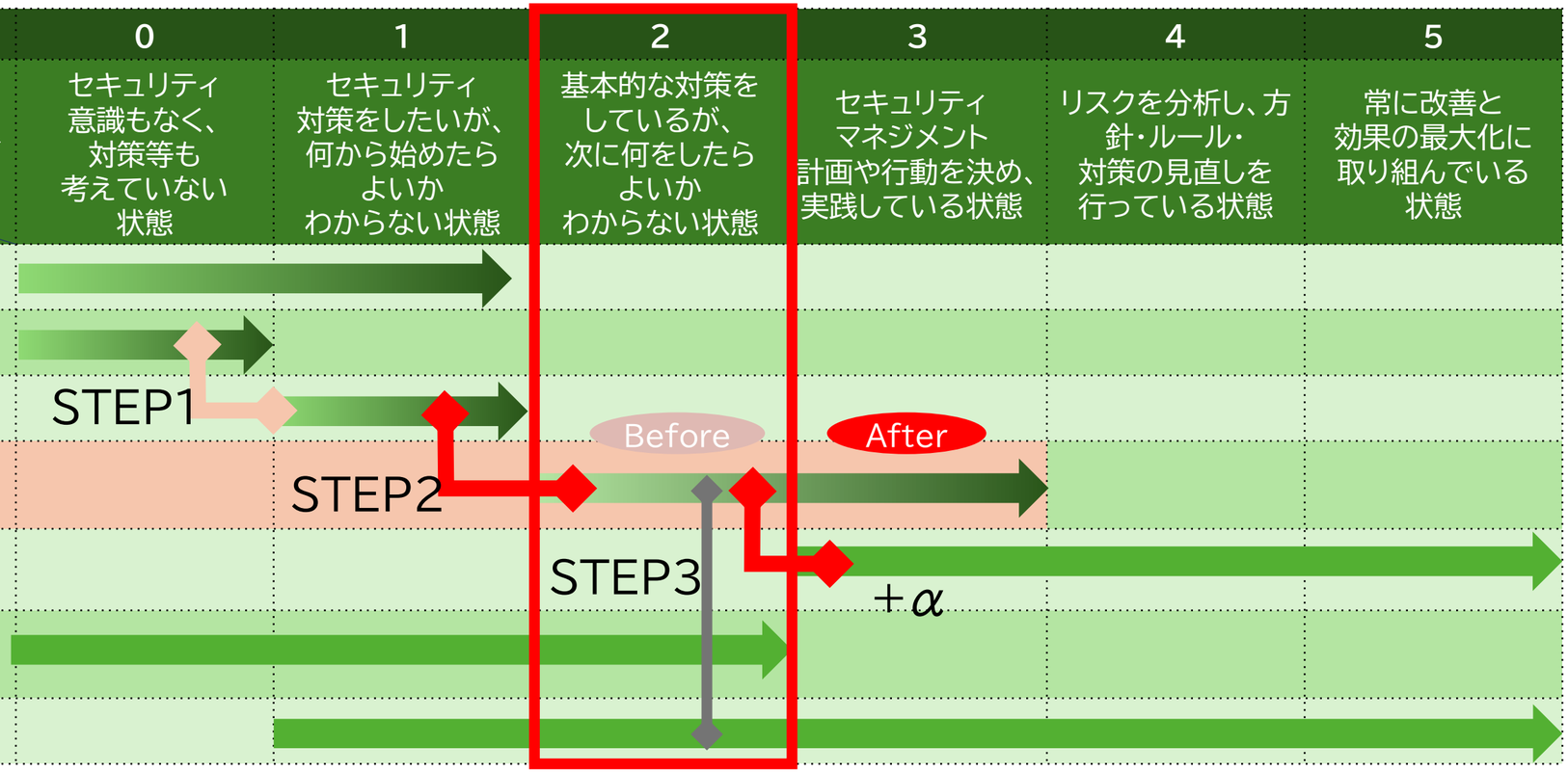
氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。

目的

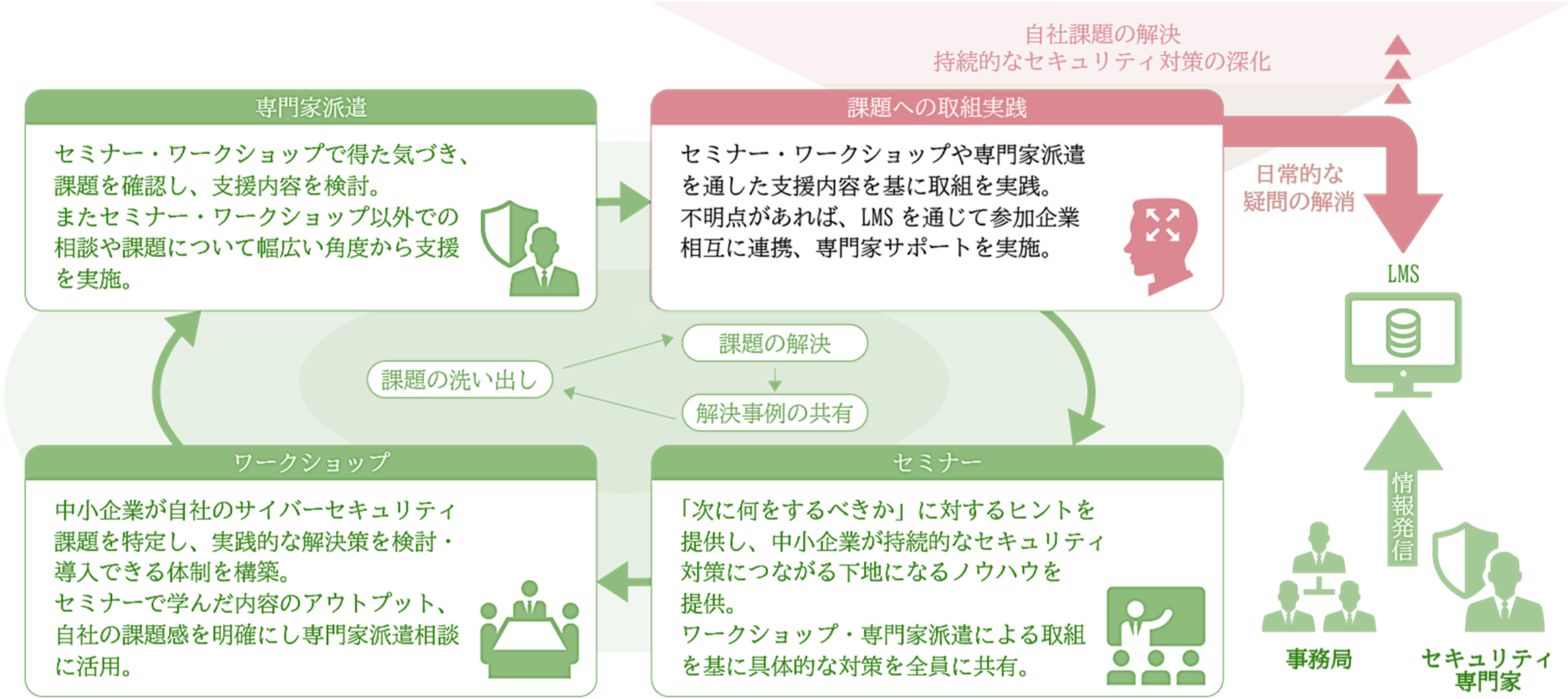
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

東京都他事業と本事業の位置づけ

成熟度レベル　※COBITを援用し設定	0	1	2	3	4	5
ステータス / 事業と主な支援領域	セキュリティ意識もなく、対策等も考えていない状態	セキュリティ対策をしたいが、何から始めたらよいかわからない状態	基本的な対策をしているが、次に何をしたらよいかわからない状態	セキュリティマネジメント計画や行動を決め、実践している状態	リスクを分析し、方針・ルール・対策の見直しを行っている状態	常に改善と効果の最大化に取り組んでいる状態
中小企業サイバーセキュリティの極意						
中小企業サイバーセキュリティ 啓発事業						
中小企業サイバーセキュリティ 基本対策事業						
中小企業サイバーセキュリティ実践力強化プログラム（本事業）						
中小企業サイバーセキュリティインシデント対応力強化						
Tcyss（東京中小企業サイバーセキュリティ支援ネットワーク）						
サイバーセキュリティ対策促進助成金						



支援内容の全体像


自社課題の解決
持続的なセキュリティ対策の深化
専門家派遣
セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談や課題について幅広い角度から支援を実施。
課題への取組実践
セミナー・ワークショップや専門家派遣を通した支援内容を基に取組を実践。
不明点があれば、LMS を通じて参加企業相互に連携、専門家サポートを実施。
日常的な
疑問の解消
LMS
課題の解決
課題の洗い出し
解決事例の共有
ワークショップ
中小企業が自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制を構築。
セミナーで学んだ内容のアウトプット、自社の課題感を明確にし専門家派遣相談に活用。
セミナー
「次に何をするべきか」に対するヒントを提供し、中小企業が持続的なセキュリティ対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組を基に具体的な対策を全員に共有。
情報発信
事務局
セキュリティ専門家

スケジュール

支援内容	7月	8月	9月	10月	11月	12月	1月	2月	3月
セミナー／ワークショップ（全10回）	7/25（金）	8/8（金）	8/27（水）	9/11（木）	9/25（木）	10/10（金）	10/27（月）	11/17（月）	12/12（金）	1/16（金）		
専門家派遣（全4回）	1回目		2回目		3回目		4回目					
事例集								ご参加いただいた企業様への取材	事例集作成期間	公表3月下旬～		

セミナー内容

実施回	編	テーマ
第1回 7/25 （金）	第0編	はじめに
	第1編	サイバーセキュリティを取り巻く背景
	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
第2回 8/8 （金）	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
	第4編	セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施
	第5編	各種ガイドラインを参考にした対策の実施

セミナー内容

実施回		編	テーマ
第3回	8/27(水)	第6編	ISMSなどのフレームワークの種類と活用法の紹介
第4回 第5回	9/11(木) 9/25(木)	第7編	ISMSの構築と対策基準の策定と実施手順
第6回 第7回	10/10(金) 10/27(月)	第8編	具体的な構築・運用の実践
第8回	11/17(月)	第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第9回	12/12(金)	第10編	サイバーレジリエンス能力の育成
第10回	2026年 1/16(金)	第11編	生成AIおよびAIマネジメントシステム
		第12編	全体総括

第0章. テキストの活用

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

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

【参照:テキスト0-1-1.】
P2

テキストの目的、想定読者

- 目的
  中小企業がサイバーセキュリティの重要性と対策について理解を深めるための情報を提供します。

- 中小企業の現状
  - セキュリティ対策のリソースが限られ、大企業よりもサイバー犯罪者に狙われやすい。
  - フィッシング攻撃やランサムウェア攻撃の頻度が増加している。
  - 攻撃により業務停止や経済的損失、企業の信頼・ブランド価値への影響が懸念される。

- 想定読者
  中小企業の経営者やIT担当者。

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

【参照:テキスト0-1-2.】
P2～3

全体構成

- 本書の構成
  - 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る。
  - ITおよびセキュリティの基礎知識と対策の要点を解説。
  - 政府や業界団体の取組、最新の技術やトレンドについて詳しく解説し、対応力を向上させる。
  - 中小企業におけるIT・セキュリティの課題に焦点を当て、具体的な解決策を提示。
  - ISMS認証などの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の手順を解説。

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

【参照:テキスト0-1-2.】
P2～3

全体構成

- 第4編以降では、セキュリティ対策をレベル分けして説明。
  - レベル1： 緊急性の高い事例への対処法を解説。
  - レベル2：ガイドラインを用いて、組織全体で最低限実施すべきセキュリティ対策を解説。
  - レベル3：セキュリティフレームワークを用いて、より多くの攻撃手法に網羅的に対応するための事項を説明。
- セキュリティ対策を実施するための知識やスキル、人材の育成や確保について実践的な知識を提供。

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

【参照:テキスト0-1-3.】
P3～P5

テキストの利用方法

経営層
- 組織として実践すべき事項と概要を知りたい。

システム管理担当者層
- セキュリティに関する動向を知りたい。
- 中小企業に必要な事項を知りたい。
- セキュリティ対策の具体的な手順を知りたい。

現在の対策状況
- 緊急に、大きなセキュリティホールを塞ぎたい。
- 素早く、多くのセキュリティホールを塞ぎたい。
- 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ぎたい。

第1章. デジタル時代の社会とIT情勢

デジタル時代の社会変革とIT情勢の関係性

デジタル時代の社会変革とIT情勢の関係性

【参照:テキスト1-1】
P7～P9

社会の現状と今後の動向

- Society5.0とは
  「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）」
  内閣府「Society 5.0」 https://www8.cao.go.jp/cstp/society5_0/ （参照 2023-07-06）

- Society1.0：狩猟社会
  Society2.0：農耕社会
  Society3.0：工業社会
  Society4.0：情報社会
  Society5.0：未来社会（動画）
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_mirai1.html
  Society5.0　ビックデータ連携がもたらす未来社会像（動画）
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_bigdata1.html

デジタル時代の社会変革とIT情勢の関係性

【参照:テキスト1-1】
P7～P9

デジタルトランスフォーメーション(DX)とは

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。」

経済産業省「デジタルガバナンス・コード3.0」（2023-09-19） p.2脚注
https://www.meti.go.jp/policy/it policy/investment/dgc/dgc3.0.pdf

概要

- DXは、データやデジタル技術を使って新たな価値を生み出すこと。
- DXには、ビジネスモデルや企業文化の変革が必要。
- DX戦略では、経営ビジョンを描き、関係者を巻き込んで課題を解決する。
- DXは「知識」、「人材」、「セキュリティ」が重要な要素。

デジタル時代の社会変革とIT情勢の関係性

【参照:テキスト1-1】
P7～P9

デジタルトランスフォーメーション(DX)とは

DXに必要な3要素

知識

- ITの基礎知識
- データサイエンスの知識
- AI・ブロックチェーンなどの最新の知識

人材

- 業務内容に精通
- 要件を実現させるために、新たな技術・手法を用いることができる

セキュリティ

- リモートワークのためのセキュリティ
- クラウドサービスを利用するためのセキュリティ

デジタル時代の社会変革とIT情勢の関係性

【参照:テキスト1-1】
P7～P9

生成AIとは

概要

- 既存のデータを解析・学習して新しいコンテンツを生成するAI。
- ディープラーニングを用いてテキスト、画像、音楽、映像などを作り出す。
- 従来のAIは大量の学習データをもとに結果を予測し行動を自動化していた。
- 新しい情報やデータから独自のコンテンツを生み出すことができる。

活用

- 生成AIを用いたチャットボットが24時間365日対応している。
- 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、かつ短時間で何種類も生成できる。
- 多くの業務プロセスを効率化できる。

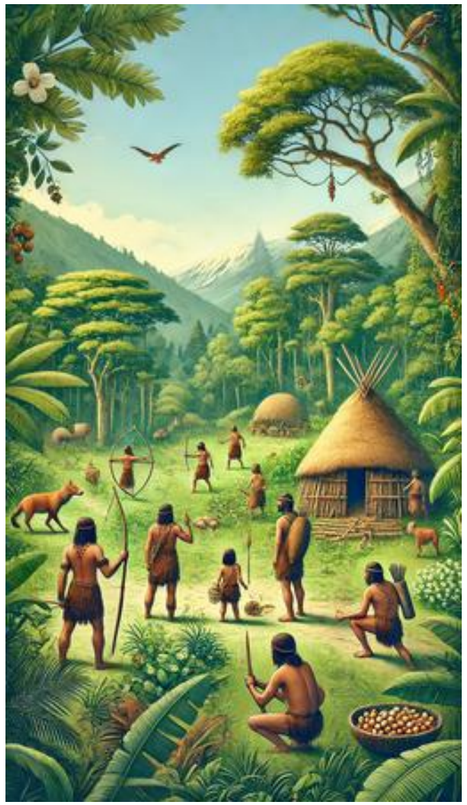
デジタル時代の社会変革とIT情勢の関係性

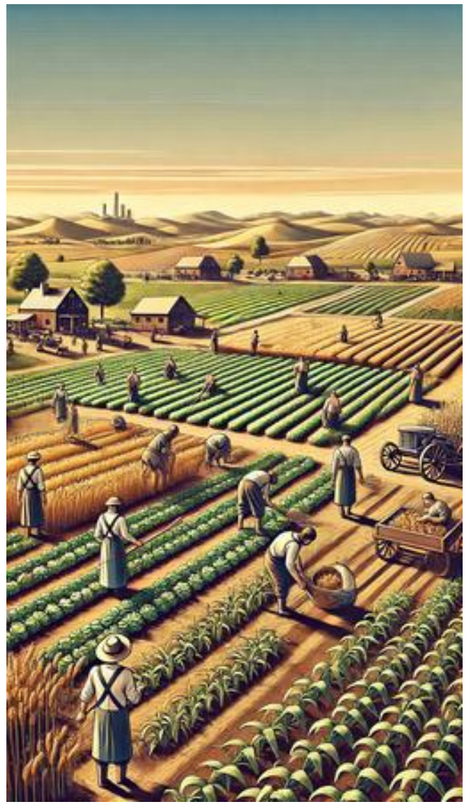
【参照:テキスト1-1】
P7～P9

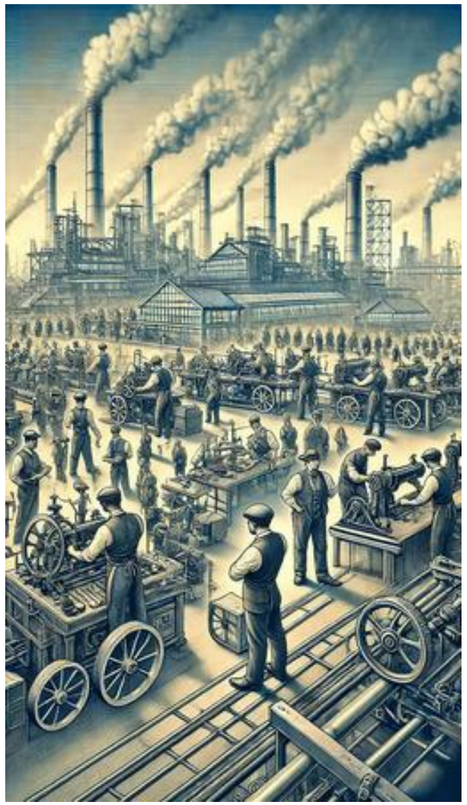
生成AIとは

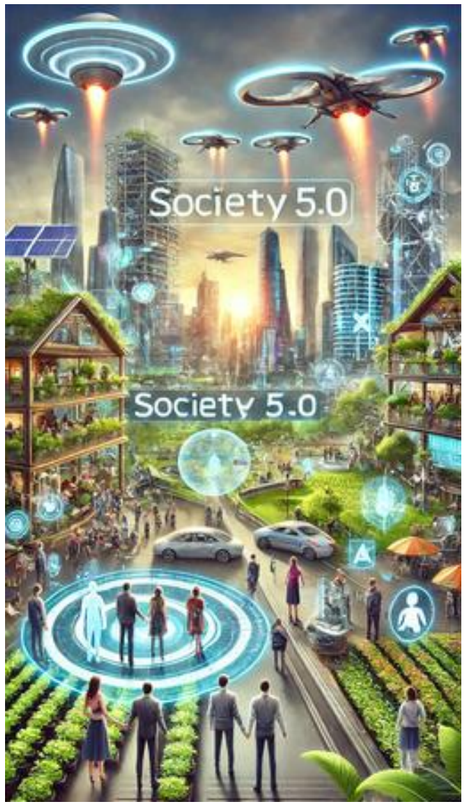
使用例

例えば、Society1.0～5.0のイメージを描かせると、こんな感じ。









第2章. サイバーセキュリティの基礎知識

導入済みと想定するセキュリティ対策機能

SECURITY ACTION（セキュリティ対策自己宣言）

サイバーセキュリティアプローチ方法

導入済みと想定するセキュリティ対策機能

【参照:テキスト2-1.】
P11

UTMとEDRについて

UTM(Unified Threat Management)

- UTM(統合脅威管理)は複数のセキュリティ機能を一つの機器に集約するシステム
- ネットワーク全体のトラフィックを監視・管理する
- 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いる
- 外部からの侵入や攻撃を防御する
- 企業や組織内のネットワークセキュリティ対策として有効

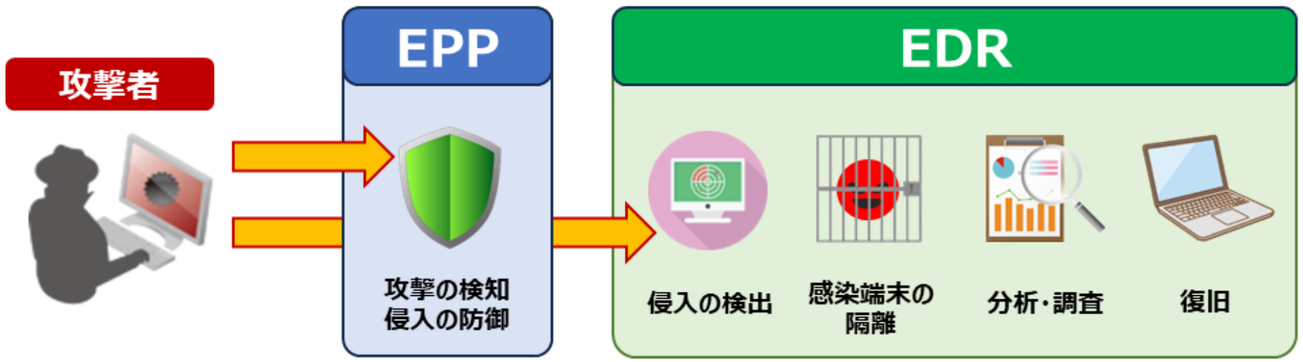
導入済みと想定するセキュリティ対策機能

【参照:テキスト2-1.】
P11

UTMとEDRについて

EDR(Endpoint Detection and Response)

- EDRはエンドポイント(PC、サーバなど)での脅威の検知と対応を可能にする
- 従来のアンチウイルスソフトでは検知できないマルウェアも検知可能
- エンドポイント上の不審な動作を検知する
- 検知した脅威に対して、悪意のあるプロセスの終了や感染したエンドポイントの隔離などの対応を行う
- 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る



SECURITY ACTION 二つ星レベル

【参照:テキスト2-2-1.】
P12～P13

レベルごとの宣言内容

レベル	宣言内容	ロゴマーク
★ 一つ星	「情報セキュリティ5か条」に取り組むことを宣言する	
★★ 二つ星	1.「5分でできる！情報セキュリティ自社診断」で自社のセキュリティ対応状況を把握する 2. 情報セキュリティ方針を策定する 3. 外部に公開したことを宣言する	

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

SECURITY ACTION 二つ星レベル

【参照:テキスト2-2-1.】
P12～P13

宣言プロセス

概要	詳細
1. 使用規約を確認	「ロゴマーク使用規約確認」にて規約を確認する。
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する。
3. 確認メールを受信	「自己宣言受付確認のお知らせ」メールを受信する。メール本文中のURLをクリックする。
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が通知される。
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が、メールで通知される。

SECURITY ACTION 一つ星

【参照:テキスト2-2-2.】
P13～P14

情報セキュリティ5か条

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

SECURITY ACTION 二つ星

【参照:テキスト2-2-3.】
P14～P16

情報セキュリティ自社診断

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するための診断ツール。
25項目の設問に答えるだけで診断できる。

分類

パート	内容
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。
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。
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。

SECURITY ACTION 二つ星

【参照:テキスト2-2-3.】
P14～P16

情報セキュリティ自社診断

診断方法

- 経営者または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する。
- 一人で記入が難しい場合は、事業所、部署ごとに記入し、責任者・担当者が集計する。

点数

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

情報セキュリティ自社診断

【参照:テキスト2-2-3.】
P14～P16

5分でできる！情報セキュリティ自社診断とは

判定

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	部分的に対策が不十分	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

情報セキュリティ基本方針

【参照:テキスト2-2-4.】
P17～P18

情報セキュリティ基本方針とは

- 経営者が情報セキュリティに関する基本方針を策定する。
- 従業員や関係者に基本方針を伝達するため、簡潔な文書を作成する。
- 基本方針の作成には特定の書き方が定められていない。
- 事業の特徴や顧客の期待を考慮して基本方針を策定する。
- 経営者と連携し、自社に適した基本方針を策定する。

情報セキュリティ基本方針

【参照:テキスト2-2-4.】
P17～P18

記載内容

- 継続的改善
- セキュリティ管理体制の整備
- セキュリティ対策の実施
- 法令・ガイドラインなどの遵守
- 違反および事故への対応

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組みます。

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

サイバーセキュリティアプローチ方法

【参照:テキスト2-3.】
P19～P22

対策基準レベルの概要

レベル	概要
Lv.1 クイックアプローチ	緊急に、狙われやすい大きな穴(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	素早く多くの穴を塞ぐ
Lv.3 網羅的アプローチ	じっくりと、小さな穴を残さないように確実に塞ぐ

第3章. デジタル社会の方向性と実現に向けた国の方針

国の基本方針および実施計画の要約

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

国の基本方針および実施計画の要約

【参照:テキスト3-1.】
P25～P27

経済財政運営と改革の基本方針(骨太方針)2024

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Vison

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

※本スライド参照ページは第3版ハンドブックのページに対応するように作成し直したため、
セミナー実施時の参照ページと相違がある場合があります。

国の基本方針および実施計画の要約

【参照:テキスト3-1.】
P25～P27

経済財政運営と改革の基本方針(骨太方針)2024における IT戦略に関係する施策例

- デジタル技術の活用
- 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

※本スライド参照ページは第3版ハンドブックのページに対応するように作成し直したため、
セミナー実施時の参照ページと相違がある場合があります。

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

【参照:テキスト3-2-1.】
P28～P31

デジタル社会の実現に向けた重点計画

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
2. 医療・教育・防災・こどもなどの準公共分野のデジタル化
3. デジタル化による地域の活性化
4. 誰一人取り残されないデジタル社会
5. デジタル人材の育成・確保
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

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

【参照:テキスト3-2-1.】
P28～P31

デジタル社会の実現に向けた戦略・施策

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

① サイバーセキュリティの確保
② 個人情報などの適正な取扱いの確保
③ 情報通信技術を用いた犯罪の防止
④ 高度情報通信ネットワークの災害対策

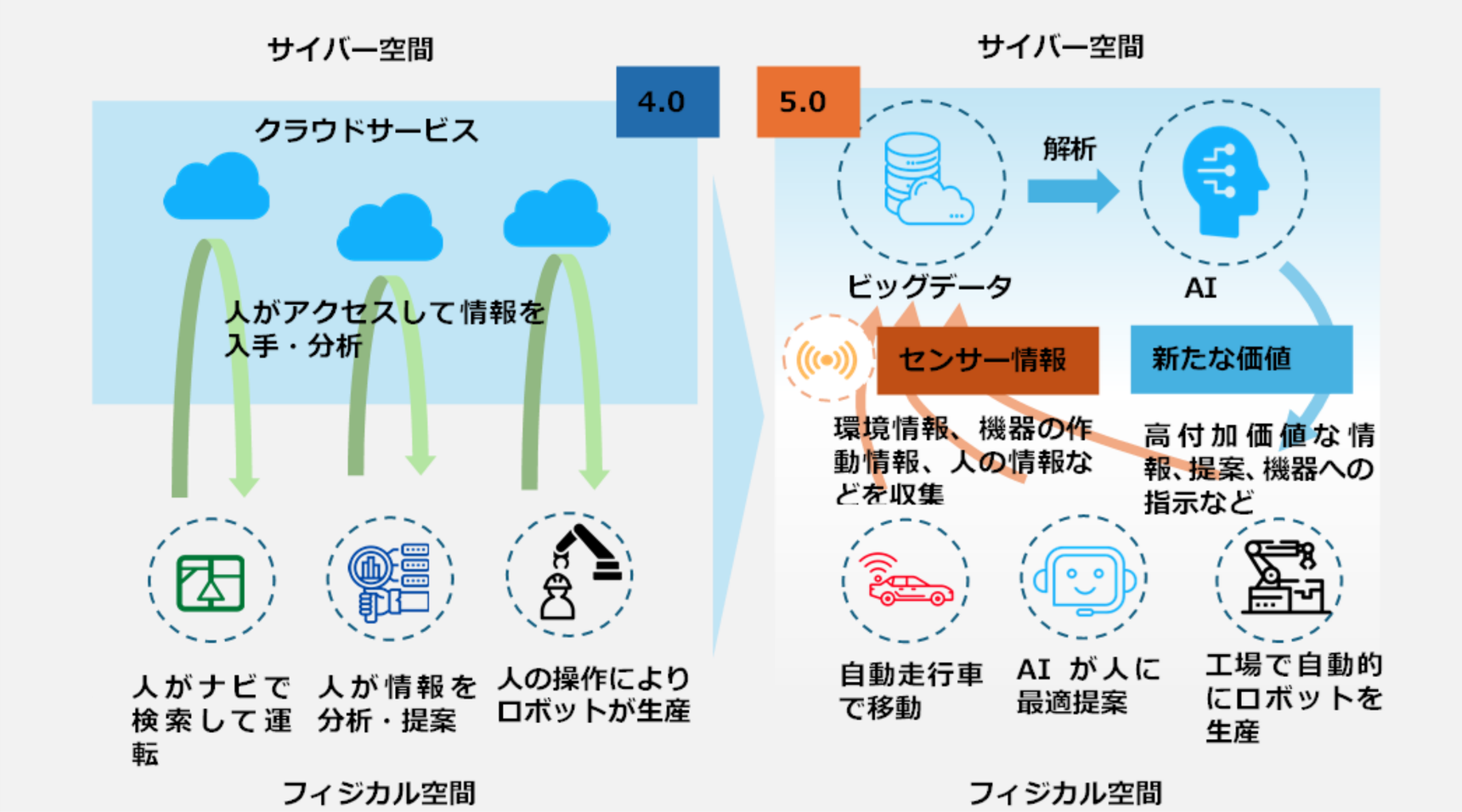
※本スライド参照ページは第3版ハンドブックのページに対応するように作成し直したため、
セミナー実施時の参照ページと相違がある場合があります。

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

【参照:テキスト3-2-3.】
P31～P33

Society 5.0

Society 4.0と5.0の比較



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

【参照:テキスト3-2-3.】
P31～P33

Society 5.0

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

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

【参照:テキスト3-2-4.】
P34～P36

DXの推進

中小企業がDX推進における優位な点

優位点	理由
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

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

【参照:テキスト3-2-4.】
P33～P35

DXの推進

データ活用の流れ

手順	概要
1. データの収取	IoTやセンサー、カメラなどの機器を用いて情報を収集する。
2. データの蓄積	収集した膨大なデータ(ビックデータ)を集積する。
3. データの解析	AIを用いてデータを解析する。
4. 解析結果の反映	解析の結果を基に改革を進める。

DX with Cybersecurityの概要

- デジタル技術の利用拡大に伴い、セキュリティリスクが増大するため、セキュリティ対策の強化が求められる。
- セキュリティ対策はコストではなく、企業価値や競争力の向上に不可欠な要素として重要である。

第4章. サイバーセキュリティ戦略および関連法令

サイバーセキュリティ戦略(NISC→NCO)

- NISC：内閣サイバーセキュリティセンター
  National center of Incident readiness and Strategy for Cybersecurity
- NCO：国家サイバー統括室
  National Cybersecurity Office
  ※ 2025年5月「サイバー対処能力強化法」が成立し、関連法令の整備を受け
  2025年7月1日にNISCを改組し発足

企業経営に重要なDX推進とセキュリティ確保の両立

関連法令

サイバーセキュリティ戦略

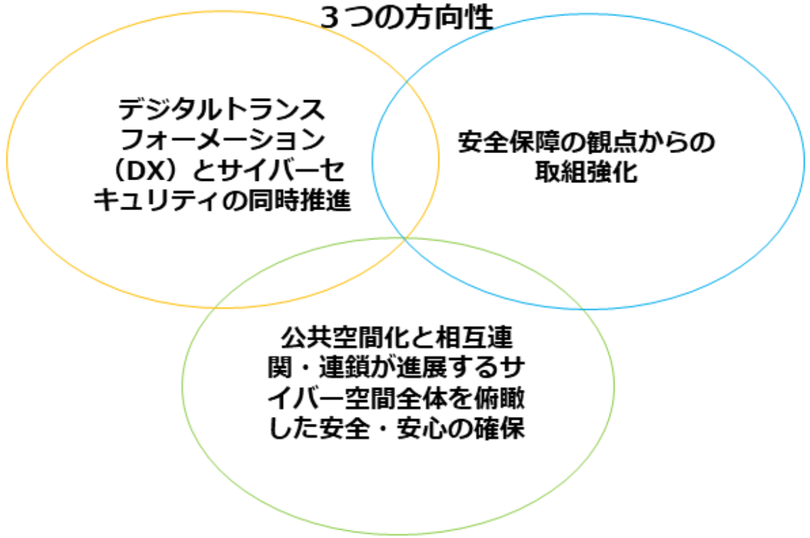
【参照:テキスト4-1-1.】
P38～P43

サイバーセキュリティ戦略の課題と方向性

- サイバーセキュリティ戦略は、国家レベルでのサイバーセキュリティ確保の方針・目標を示す。
- デジタル化の進行とともに、すべての主体がサイバー空間に参加する動きがある。
- 「誰一人取り残さない」セキュリティ確保が必要。
- 戦略では、「自由、公正、かつ安全なサイバー空間」確保のため、3つの方向性をベースに施策推進の方針が示されている。

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）

「Cybersecurity for All」
誰も取り残さないサイバーセキュリティ



「自由、公正かつ安全なサイバー空間」の確保

サイバーセキュリティ戦略

【参照:テキスト4-1-1.】
P38～P43

サイバーセキュリティ戦略の課題と方向性

3つの政策目標

「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」

横断的施策

- 人材育成・確保・活躍推進
- 研究開発の推進
- 全員参加による協働・普及啓発

※本スライド参照ページは第3版ハンドブックのページに対応するように作成し直したため、
セミナー実施時の参照ページと相違がある場合があります。

サイバーセキュリティ戦略

【参照:テキスト4-1-1.】
P38～P43

横断的施策

3つの政策目標を達成するために、横断的・中長期的な視点で取り組む施策。

研究開発
- 国際競争力の強化・産学官エコシステムの構築
- 実践的な研究開発の推進
- 中長期的な技術トレンドを視野に入れた対応

人材の確保・育成・活躍促進
- DX with Cybersecurityの推進
- 巧妙化・複雑化する脅威への対処
- 政府機関における取組

全員参加による協働・普及啓発
- ガイドラインやさまざまな解説資料などの整備の推進

サイバーセキュリティ戦略

【参照:テキスト4-1-2.】
P44～P46

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

- 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

1. 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
2. 公共空間化と相互連関・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
3. 安全保障の観点からの取組強化

企業経営に重要なDX推進とセキュリティ確保の両立

【参照:テキスト4-2-1.】
P47～P48

企業経営のためのサイバーセキュリティの考え方

2つの基本的認識

1. 挑戦
   サイバーセキュリティは、ビジネスの革新や新しい製品・サービス創出の一環として、利益を生み出す戦略として考慮すべきである。
2. 責任
   つながる社会でのサイバーセキュリティへの取組は、社会の要求であり、自社だけでなく、全体の発展にも寄与する。

3つの留意事項

1. 情報発信による社会的評価の向上
2. リスクの一項目としてのサイバーセキュリティ
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

企業経営に重要なDX推進とセキュリティ確保の両立

【参照:テキスト4-2-1.】
P47～P48

サイバーセキュリティ対策の取組レベル

レベル	分類	概要
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
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
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
	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
対象外	6	ITを利用していない企業

企業経営に重要なDX推進とセキュリティ確保の両立

【参照:テキスト4-2-2.】
P49～P50

DX with Cybersecurity

DX with Cybersecurityの推進に向けた主な施策

分類	課題	施策
経営層の意識改革	経営層が主体性を持ってDXとサイバーセキュリティ対策に取り組むためには、専門家とのコミュニケーションが重要	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	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	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	サイバー攻撃の起点となり得る箇所の拡大に伴う、リスク管理が重要	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

関連法令

【参照:テキスト4-3-1.】
P51～P52

個人情報保護法

個人情報保護法とは

- インターネット普及や情報技術の進歩を背景に、「個人情報保護法」が2005年4月に施行。
- デジタル技術の進展や社会情勢の変化を受けて、法律は3度の改正を経ている。
- この法律では、何が個人情報とされるかや、その取り扱い方法を規定。

個人情報の定義

- 「個人情報」は生存する個人に関する情報。
- 氏名、生年月日、住所、顔写真などで個人を特定できる。
- 他の情報と照合し特定可能なものも含む。

関連法令

【参照:テキスト4-3-1.】
P51～P52

個人情報を取扱う時の基本ルール

項番	取扱い種別	ルール
1	取得・利用	・利用目的を特定して、その範囲内で利用する ・利用目的を通知又は公表する
2	保管・管理	・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	・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
4	開示請求などへの対応	・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

<u>個人情報保護法の罰則規定</u>

- 2022年4月の法改正で、罰則強化。
- 個人情報保護委員会の命令違反や不正流用で、1億円以下の罰金。
- 報告義務違反の場合、50万円以下の罰金。

関連法令

【参照:テキスト4-3-2.】
P52～P53

GDPR

GDPR(一般データ保護規則)とは

起源: 欧州連合(EU)で策定された新しい個人情報保護の枠組み。

目的: 個人のプライバシー権を強化し、個人データの処理に関する組織の透明性を増すことを目的としている。

適用範囲: 欧州経済領域(EEA)内で活動するすべての組織に適用され、EEA外の組織もEEAの市民のデータを処理する場合にはこの規則の対象となる。

内容: 個人データの「収集」、「処理」、「保存」、「移転」など、あらゆる側面に関してのルールが定められており、ユーザーには自らのデータに対するアクセス、修正、削除などの権利が保障されている。

罰則: 違反組織には、全世界の年間売上の最大4%以下、または2,000万ユーロ以下(いずれか高い方)の罰金が課せられることが規定されている。
※2,000万ユーロ:約34億円

関連法令

【参照:テキスト4-3-2.】
P52～P53

GDPRと日本企業の関係

- EU内に物理的拠点がない企業も対象となる可能性
  インターネットを利用してEU域内に商品やサービスの提供、情報収集を実施
  EU域内からのアクセスを持つターゲティング広告を配置した自社サイトを保有
- GDPR違反時には重い制裁金が課せられる

対策例

- GDPRにおいて、Cookieは「個人情報」として扱われる
- WebサイトでCookieを使用する場合、閲覧者からの同意取得が必須
- 個人データの利用同意の管理のため、ツール（CMP）の導入が推奨される

関連法令

【参照:テキスト4-3-3.】
P53～P54

その他関連法令

- 不正競争防止法
- 著作権法
- 電気通信事業法
- 電子証明および認証業務に関する法律
- 情報処理の促進に関する法律
- 国立研究開発法人情報通信研究機構法
- 刑法
- 不正アクセス行為の禁止などに関する法律

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

情報セキュリティの概況

重大インシデント事例から学ぶ課題解決

実際の被害事例から見るケーススタディ

情報セキュリティの概況

【参照:テキスト5-1-1.】
P57～P58

情報セキュリティの脅威を学ぶ

目的

- 適切な予防策や対策を講じること

内容

- 攻撃手口の**傾向**を把握する
- 脅威に対する対策方法を理解する

活用するべき代表的な刊行物

- 情報セキュリティ白書
- 情報セキュリティ10大脅威

※本スライド参照ページは第3版ハンドブックのページに対応するように作成し直したため、
セミナー実施時の参照ページと相違がある場合があります。

情報セキュリティの概況

【参照:テキスト5-1-2.】
P58～P59

情報セキュリティ白書

記載内容

- セキュリティインシデントの事例
- セキュリティ対策強化の取組
- サイバーセキュリティ経営ガイドライン
- 国内外のセキュリティの動向
- セキュリティ人材の育成
- 中小企業のセキュリティ対策
- 個別テーマ（IoT、インフラシステム等）のセキュリティ動向
- セキュリティツールの紹介

情報セキュリティの概況

【参照:テキスト5-1-3.】
P60～P64

情報セキュリティ10大脅威 2025[組織編]

順位	組織向け脅威	概要
1	ランサム攻撃による被害	システムを人質に取り、身代金を要求するマルウェア
2	サプライチェーンや委託先を狙った攻撃	取引先や供給業者を通じて攻撃する手口
3	システムの脆弱性を突いた攻撃	ソフトウェアの脆弱性が修正される前に攻撃する手法
4	内部不正による情報漏えい等	従業員や関係者が内部から情報を漏らす行為
5	機密情報等を狙った標的型攻撃	特定の企業や組織を狙った攻撃で機密情報を盗む
6	リモートワーク等の環境や仕組みを狙った攻撃	テレワーク環境を狙った攻撃
7	地政学的リスクに起因するサイバー攻撃	社会的混乱を引き起こすことを目的に国家が行うサイバー攻撃
8	分散型サービス妨害攻撃(DDoS攻撃)	則られた複数の機器から大量のアクセスで攻撃する手法
9	ビジネスメール詐欺	ビジネスメールを装った詐欺によって金銭をだまし取る手口
10	不注意による情報漏えい等	ヒューマンエラーによる情報の漏えい

重大インシデント事例から学ぶ課題解決

【参照:テキスト5-2-1.】
P65～P66

インシデント事例から学ぶ

目的

- 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

- リスク管理、対策の強化、ポリシーの改善、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

重大インシデント事例から学ぶ課題解決

【参照:テキスト5-2-2.】
P66～P67

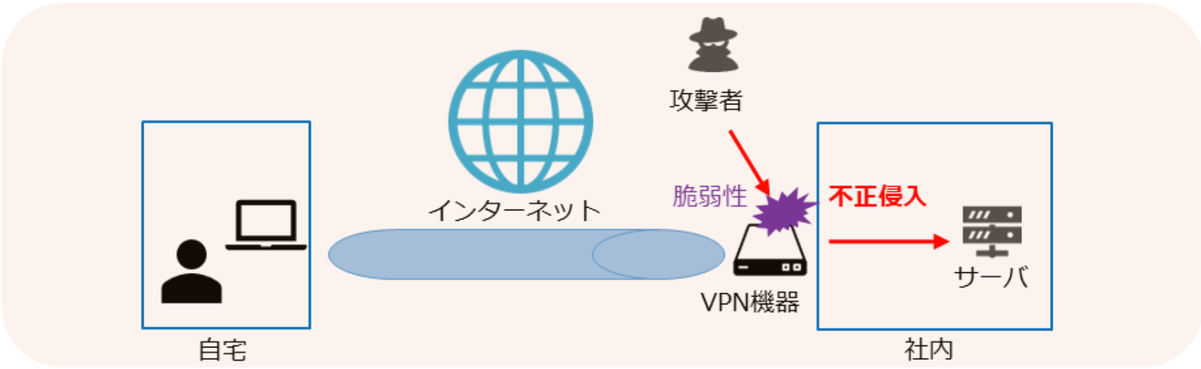
テレワークによるサイバー被害

事例概略

- テレワーク導入のために、社外からVPN接続できるようにした。
- VPN機器の脆弱性対応を実施した。
- すでに接続アカウントは抜かれた後で、そのアカウントを悪用された。

対処ポイント

- 脆弱性を悪用されることで、何が起こるのかを理解する。
- すでに攻撃を受けていることを前提とする。

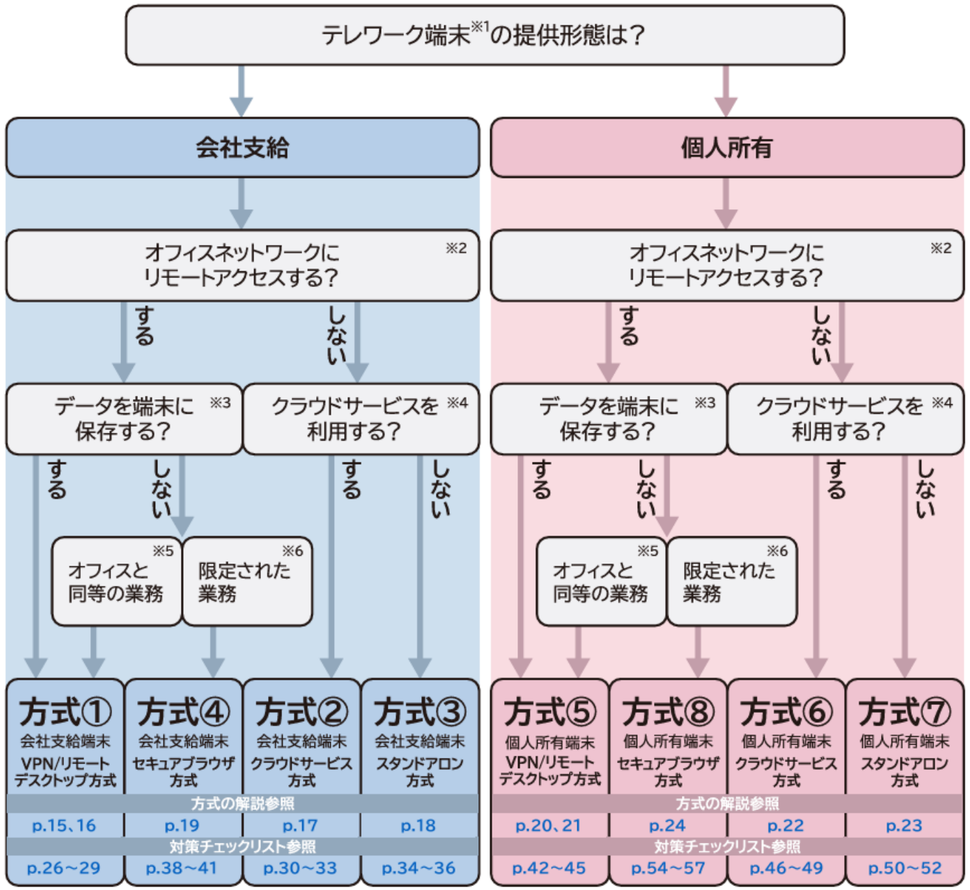


重大インシデント事例から学ぶ課題解決

【参照:テキスト5-2-2.】
P66～P67

テレワークのセキュリティ対策

テレワーク方式概要



No.	方式名
方式1	会社支給端末・VPN/リモートデスクトップ方式
方式2	会社支給端末・クラウドサービス方式
方式3	会社支給端末・スタンドアロン方式
方式4	会社支給端末・セキュアブラウザ方式
方式5	個人所有端末・VPN/リモートデスクトップ方式
方式6	個人所有端末・クラウドサービス方式
方式7	個人所有端末・スタンドアロン方式
方式8	個人所有端末・セキュアブラウザ方式

総務省「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」 https://www.soumu.go.jp/main_content/000816096.pdf

重大インシデント事例から学ぶ課題解決

【参照:テキスト5-2-3.】
P68～P69

インシデント対応の流れ

手順概要

1. 検知・初動対応
2. 報告・公表
3. （調査・対応）復旧・再発防止

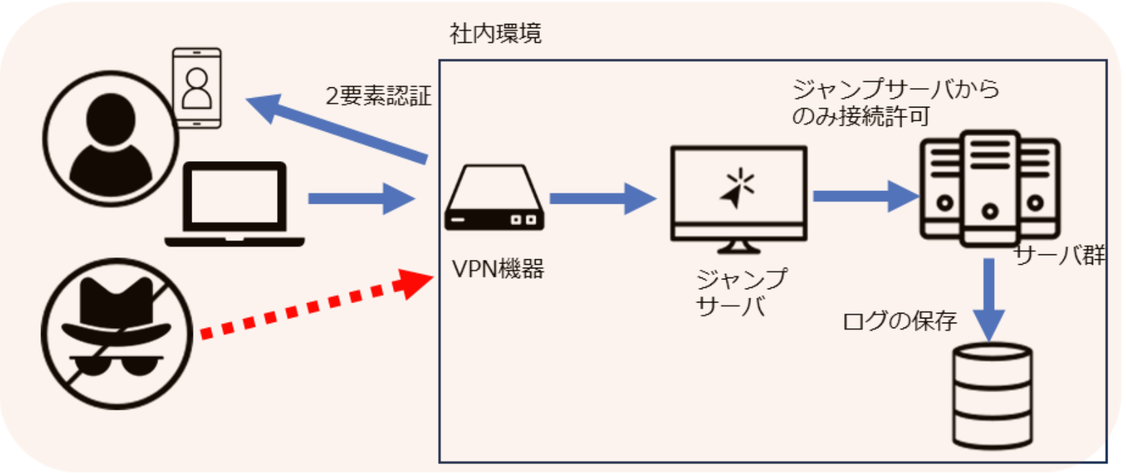
重大インシデント事例から学ぶ課題解決

【参照:テキスト5-3-3.】
P75

具体的な対応策

実施するべき技術的対策

- VPN機器への接続に多要素認証を導入し、接続元の信頼性を上げる。
- 外部から中枢のサーバに対し、VPN経由での直接接続をさせない。
- サーバやPCの特権アカウントのパスワードを定期的に変更する。
- OSのファイアウォール機能を有効にし、接続元を限定する。
- サーバやネットワーク機器のログを取得し、定期的に確認する。
- 脆弱性情報を高い頻度で確認する。
- パッチマネジメントを実施する。
- EDRなどの製品を導入する。



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

これからの企業経営で必要な観点：社会の動向

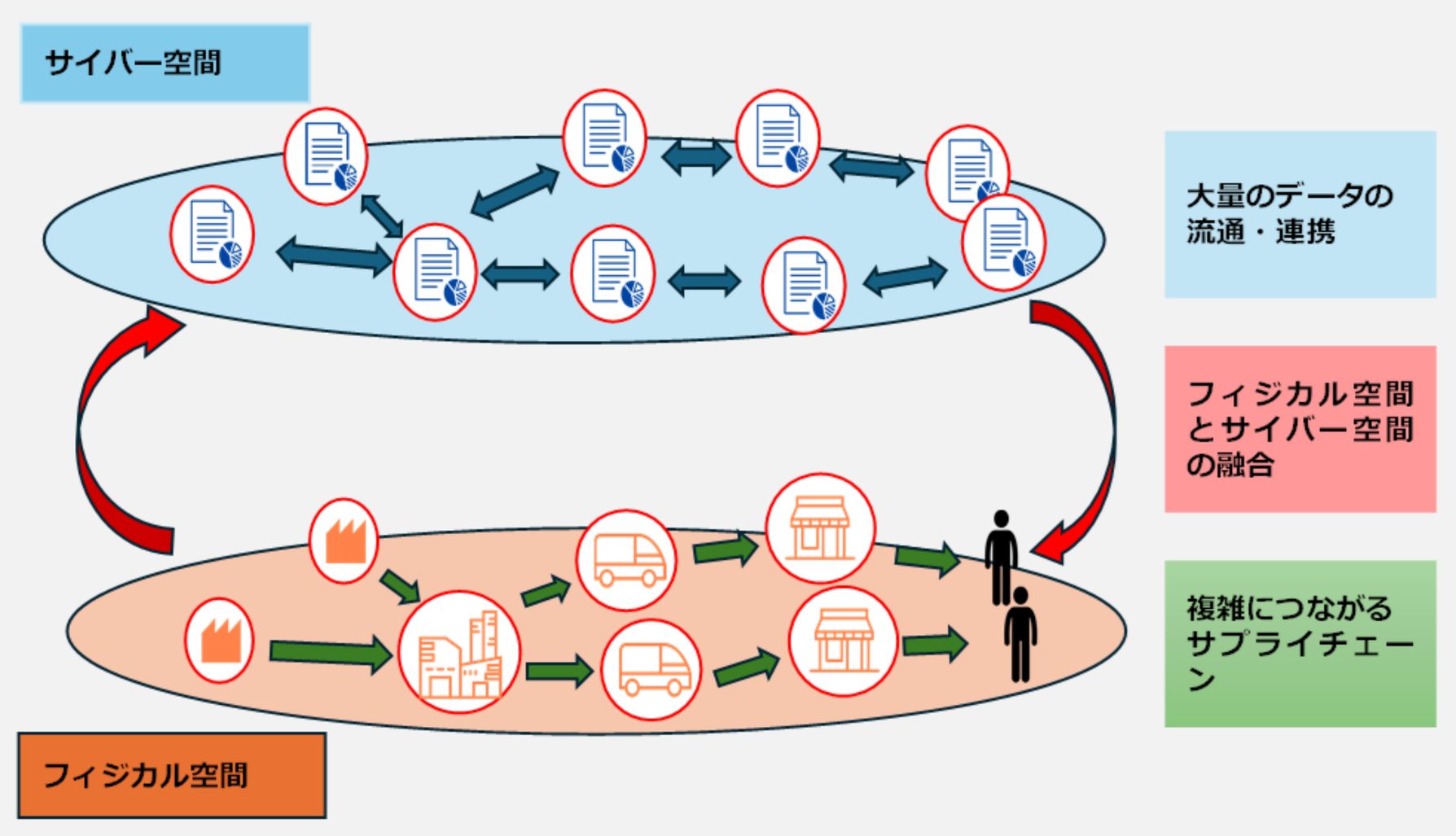
守りのIT投資と攻めのIT投資

経営投資としてのサイバーセキュリティ対策

これからの企業経営で必要な観点：社会の動向

【参照：テキスト6-1-1.】
P77～P79

現実社会とサイバー空間のつながり



これからの企業経営で必要な観点：社会の動向

【参照：テキスト6-1-2.】
P80～P83

IT活用における課題

我が国がデジタル化で後れを取った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

守りのIT投資と攻めのIT投資

【参照:テキスト6-2-1.】
P84～P85

守りのIT投資、攻めのIT投資の概要

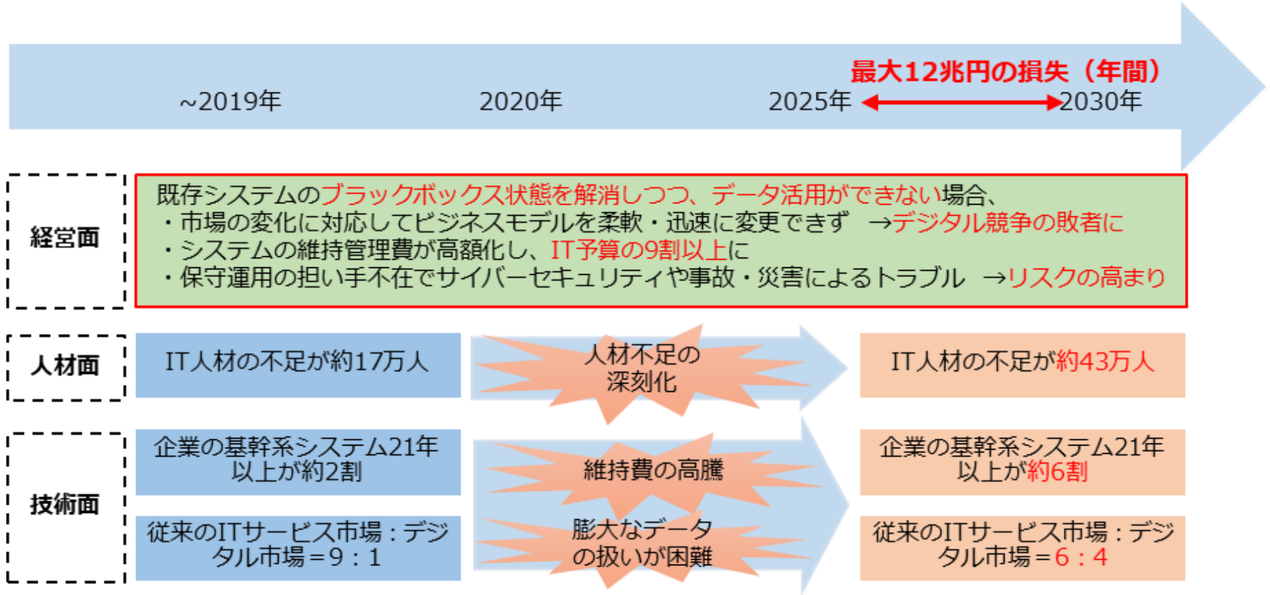
「守りの IT 投資」 （デジタルオプティマイゼーション） 目的：生産性向上	「攻めの IT 投資」 （DX） 目的：ビジネス継続・競争力強化
 • 業務の効率化 • コストの削減	 • 新たなビジネスの展開 • 顧客視点で新たな価値の創造

守りのIT投資と攻めのIT投資

【参照:テキスト6-2-2.】
P85～P86

「攻めのIT」に取り組む方針について

2025年の崖



「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

項番	課題
対策1	「見える化」指標、診断スキームの構築
対策2	DX推進ガイドラインの策定
対策3	ITシステムの刷新
対策4	ユーザー企業・ベンダー企業との新しい関係性構築
対策5	DX人材の育成・確保

守りのIT投資と攻めのIT投資

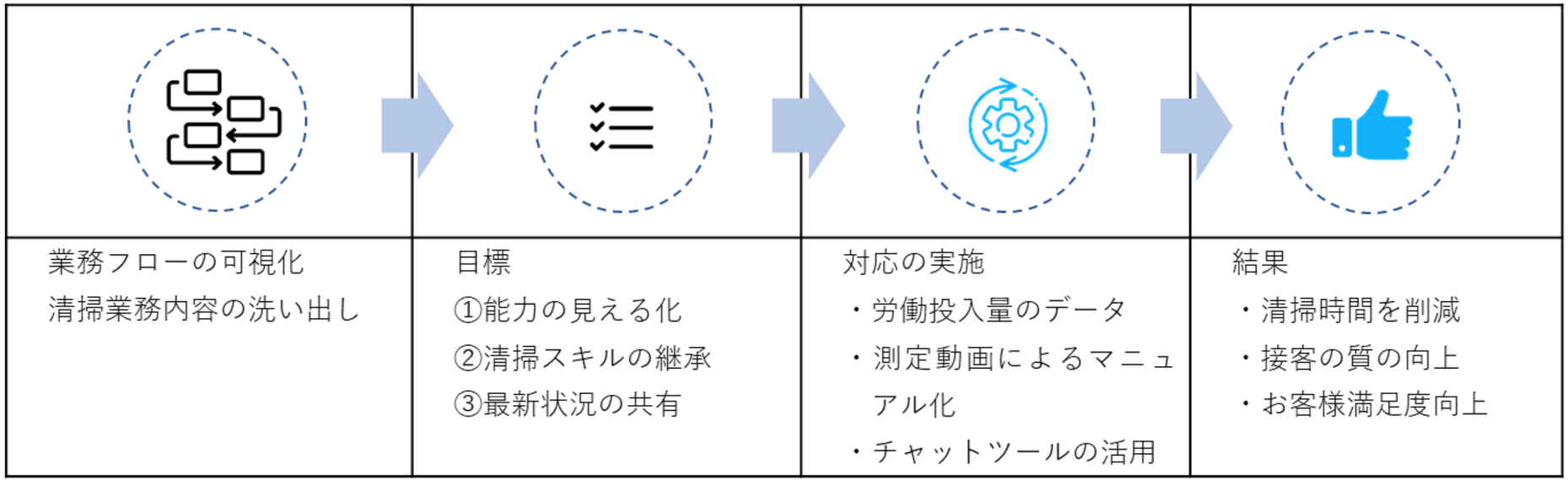
【参照:テキスト6-2-3.】
P86～P87

ITを活用した生産性の向上

「守りのIT投資」:デジタルオプティマイゼーション

- 業務効率化・コスト削減
- デジタル活用するための環境整備

事例:某旅館



業務フローの可視化 清掃業務内容の洗い出し	目標 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	対応の実施 ・労働投入量のデータ ・測定動画によるマニュアル化 ・チャットツールの活用	結果 ・清掃時間を削減 ・接客の質の向上 ・お客様満足度向上

守りのIT投資と攻めのIT投資

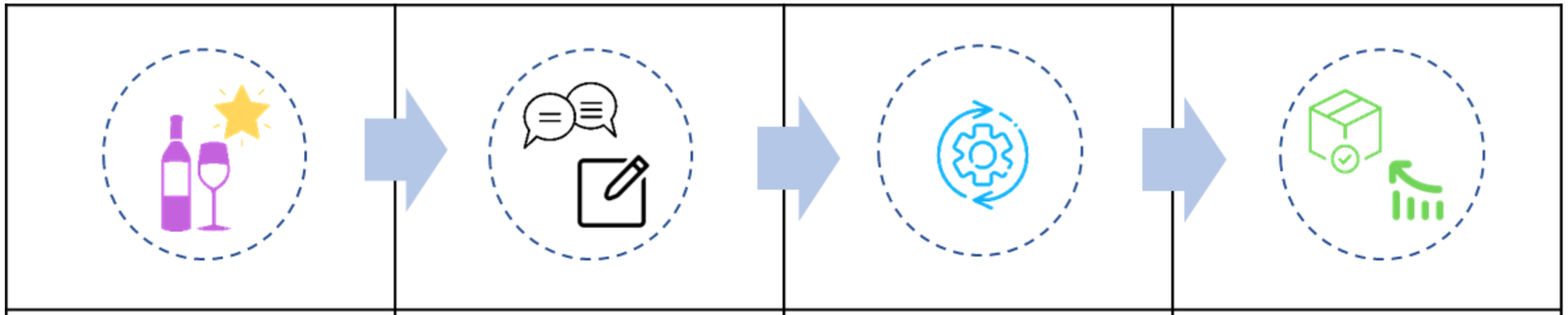
【参照:テキスト6-2-4.】
P88～P89

ITを活用した新たなビジネスの展開

「攻めのIT投資」:DX

- ビジネス環境の急激な変化に対応するため
- 多様化する顧客ニーズに応えるため

事例:某ワイン製造会社



実現したこと	課題	対策	結果
付加価値が高い「産地細分化ワイン」を増産・安定供給すること	アナログ作業（口頭伝達、手書き記帳など）の改善	「ブドウ受入演算システム」を構築	産地細分化ワインの増産・安定供給実現

守りのIT投資と攻めのIT投資

【参照:テキスト6-2-5.】
P90～P92

次世代技術を活用したビジネス展開

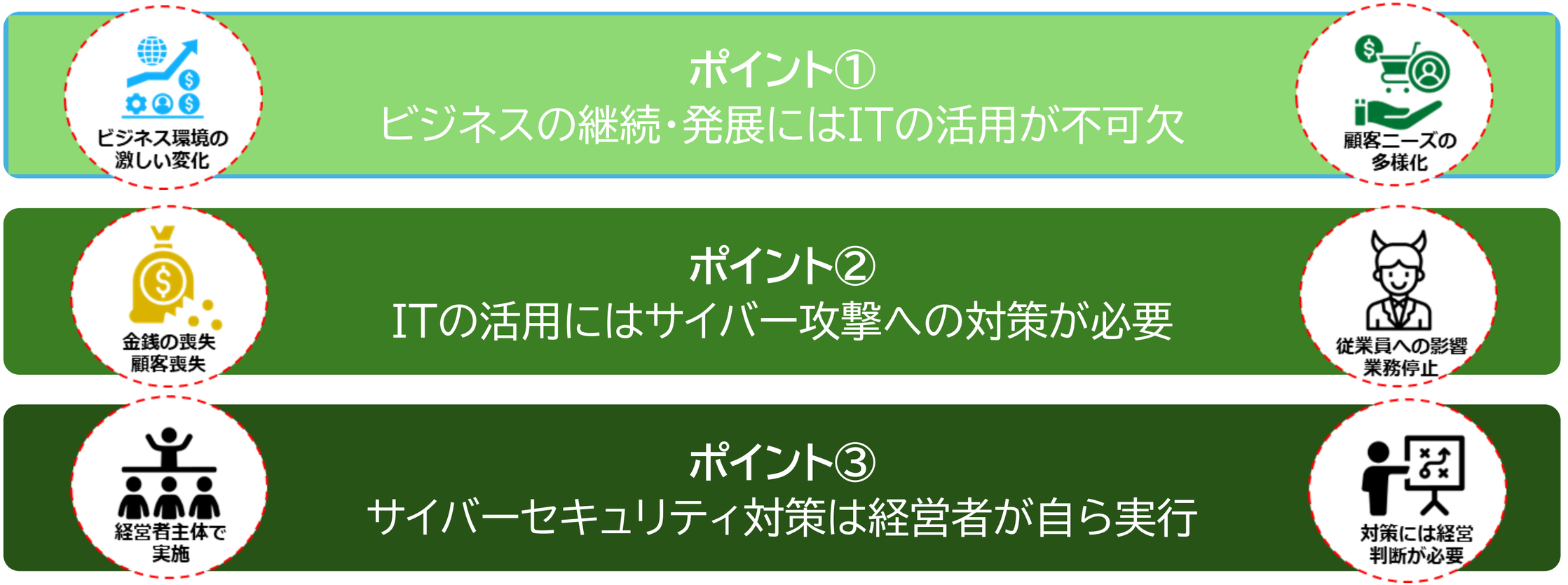
活用する技術

技術	概要	活用方法例
AI	膨大な情報を処理し、判断や予測を行うことができる。	• 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 • コンテンツの生成
IoT	現実世界のさまざまなモノが、インターネットと繋がる。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る。	• 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、全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様々なサービスを利用できる	• 社内情報の一元管理 • システムを開発・実行するためのツールや環境構築作業の省略 • 場所やデバイスに依存せずに作業の継続が可能

経営投資としてのサイバーセキュリティ対策

【参照:テキスト6-3-1.】
P92

経営者が重要視すべき3つのポイント



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」

経営投資としてのサイバーセキュリティ対策

【参照:テキスト6-3-2.】
P93～P94

経営者が重要視すべき3つのポイント

ポイント1:ビジネスの継続・発展にはITの活用が不可欠

【中小企業の重要課題】

- 業務や生産の効率化
- 人材確保

ポイント2:ITの活用にはサイバー攻撃への対策が必要

DX推進のためにはIT活用は必須

⇩

IT活用のためにはインターネットの活用は必須

⇩

インターネットの活用にはサイバーセキュリティ対策は**最優先事項！**

経営投資としてのサイバーセキュリティ対策

【参照:テキスト6-3-2.】
P93～P94

経営者が重要視すべき3つのポイント

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

- 経営者による経営判断が必要
- セキュリティインシデントが発生した際に、経営者が責任を負う

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。
会社法	第330条 取締役の善管注意義務違反 第423条 1項 任務懈怠による損害賠償責任 第429条 1項 第三者に対する注意義務違反	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)に基づく損害賠償義務を負う。

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

第7章. セキュリティ対策の概要（全容）

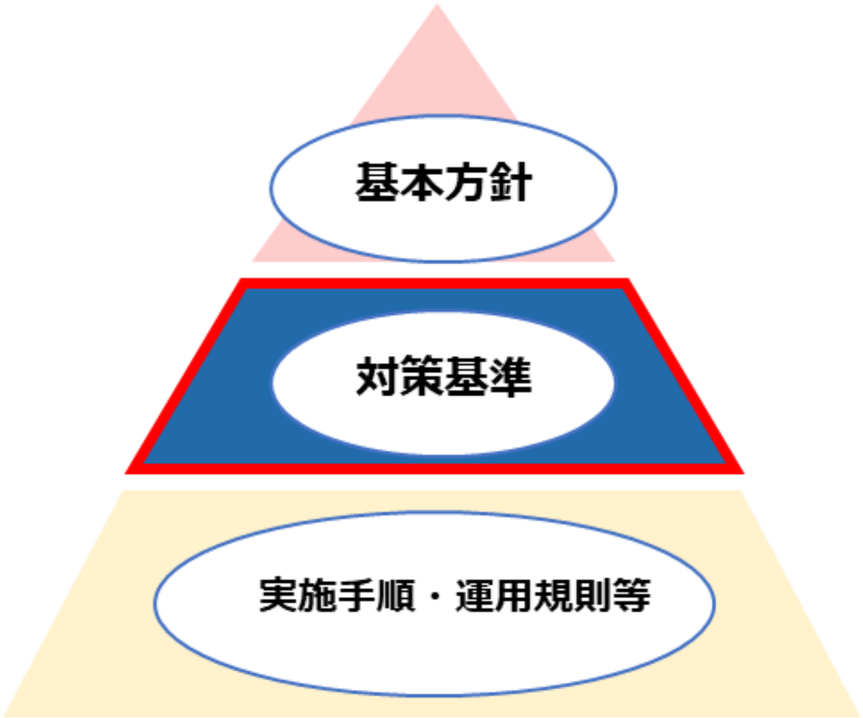
対策基準の策定

対策基準の策定

【参照:テキスト7-1-1.】
P97～P98

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の構成



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」

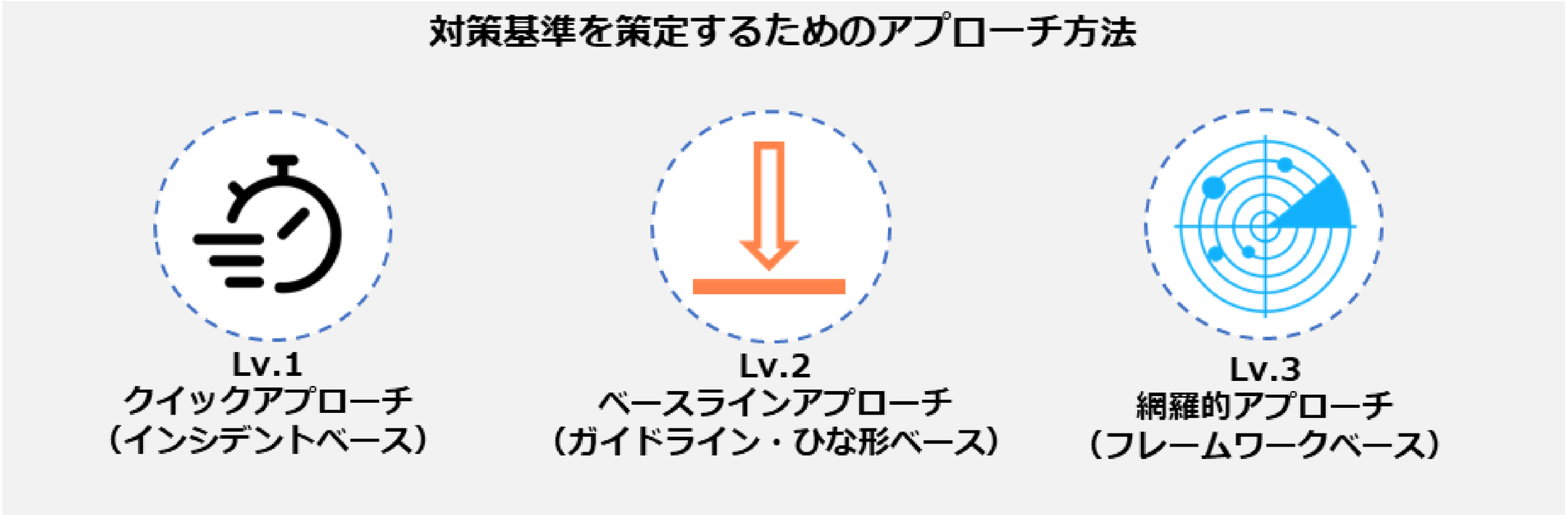
基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

対策基準の策定

【参照:テキスト7-1-1.】
P97～P98

対策基準のアプローチ方法

- 企業の現状を鑑み、次の段階的なアプローチ方法がある
  ① Lv.1　クイックアプローチ
  ② Lv.2　ベースラインアプローチ
  ③ Lv.3　網羅的アプローチ【推奨】



対策基準の策定

【参照:テキスト7-1-2.】
P98～P102

対策基準のアプローチ概要

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。 • さまざまなインシデント事例内容を参考にし、対策基準を策定。	• 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処する場合。
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。	• 組織的に一定以上の対策基準を策定する場合。
Lv.3 網羅的アプローチ	• 脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。 • ISMSなどの認証が可能なレベルを目指して、対策基準を策定。	• ISMSのフレームワークに沿った対策基準を策定する場合。

対策基準の策定

【参照:テキスト7-1-2.】
P98～P102

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	• 小規模な対策や修正を迅速に実施可能。 • 低コストでリスクを軽減。 • 流行中の攻撃の拡大や影響を最小限に抑えられる。	• 詳細な分析や検討が不十分な場合がある。 • 短期的な解決策に偏りがちになる。
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。	• 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	• 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できる。	• 全体的な実施には時間がかかる。

対策基準の策定

【参照:テキスト7-1-2.】
P98～P102

Lv.1 クイックアプローチ

【例】ランサムウェアに対する対策基準を作る

記載項目	内容
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	• 組織としてのランサムウェア対応体制の確立 • インシデント対応体制を整備し対応する
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のクリックを容易にしない • 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

（出典）IPA「情報セキュリティ10大脅威 2025」をもとに作成

対策基準の策定

【参照:テキスト7-1-2.】
P98～P102

Lv.2 ベースラインアプローチ

【例】IPA「情報セキュリティ関連規程」を活用した対策基準

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。

1	組織的対策	改訂	20yy.mm.dd
適用範囲	全社・全従業員		

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。

（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

対策基準の策定

【参照:テキスト7-1-2.】
P98～P102

Lv.3 網羅的アプローチ　※詳細解説は第3回セミナーにて実施

【例】ISMSフレームワークを活用した対策基準
93種の管理策ごとに対策基準を策定する。

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・阻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

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

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

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

第8章. 用語定義および関係性と識別方法

用語の定義、脅威・脆弱性の識別

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-1.】
P104～P107

用語の定義と関係性

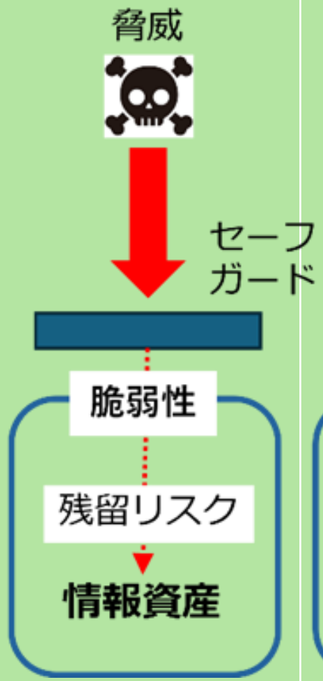
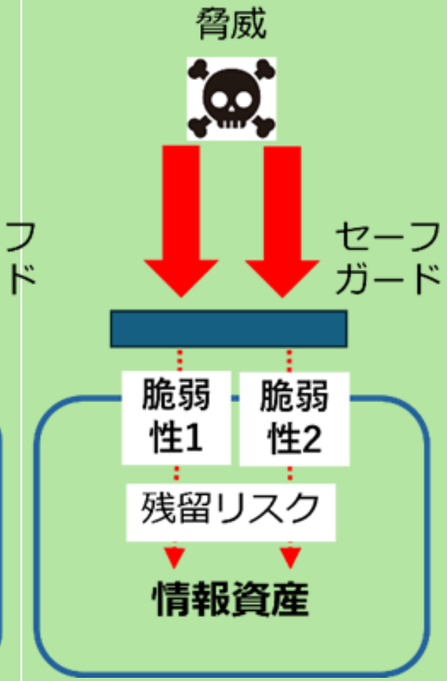
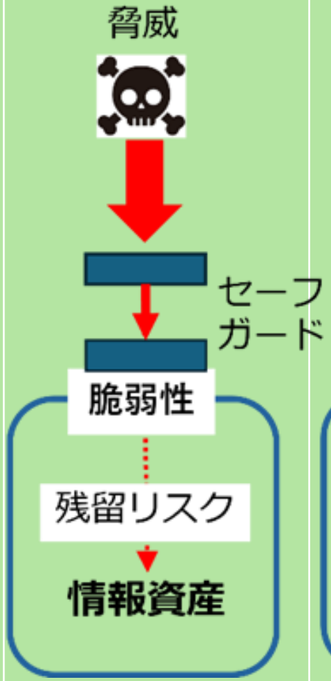
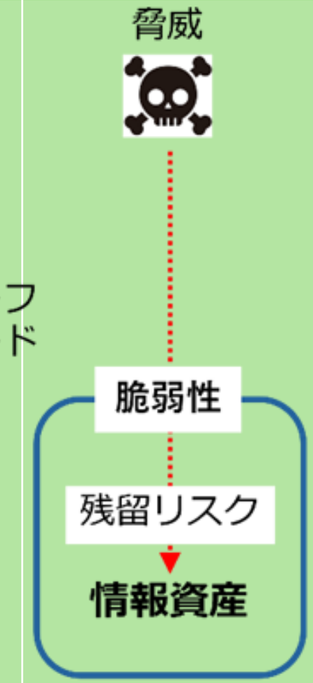
主な用語の定義

- 脅威
- 脆弱性
- インシデント
- 資産
- 資産情報の重要度
- セーフガード(管理策)
- リスク
- 残留リスク
- リスク値

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-1.】
P104～P107

関係図

	ケース1	ケース2	ケース3	ケース4	ケース5
脅威	あり	あり	あり	あり	なし
セーフガード(管理策)	あり	あり	あり(多段)	あり	あり
脆弱性	あり	あり(複数)	あり	あり	あり
リスク対応	低減	低減	低減	受容	不明
関係図					

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-1.】
P104～P107

【例】業務用ノートPCのリスクマネジメント

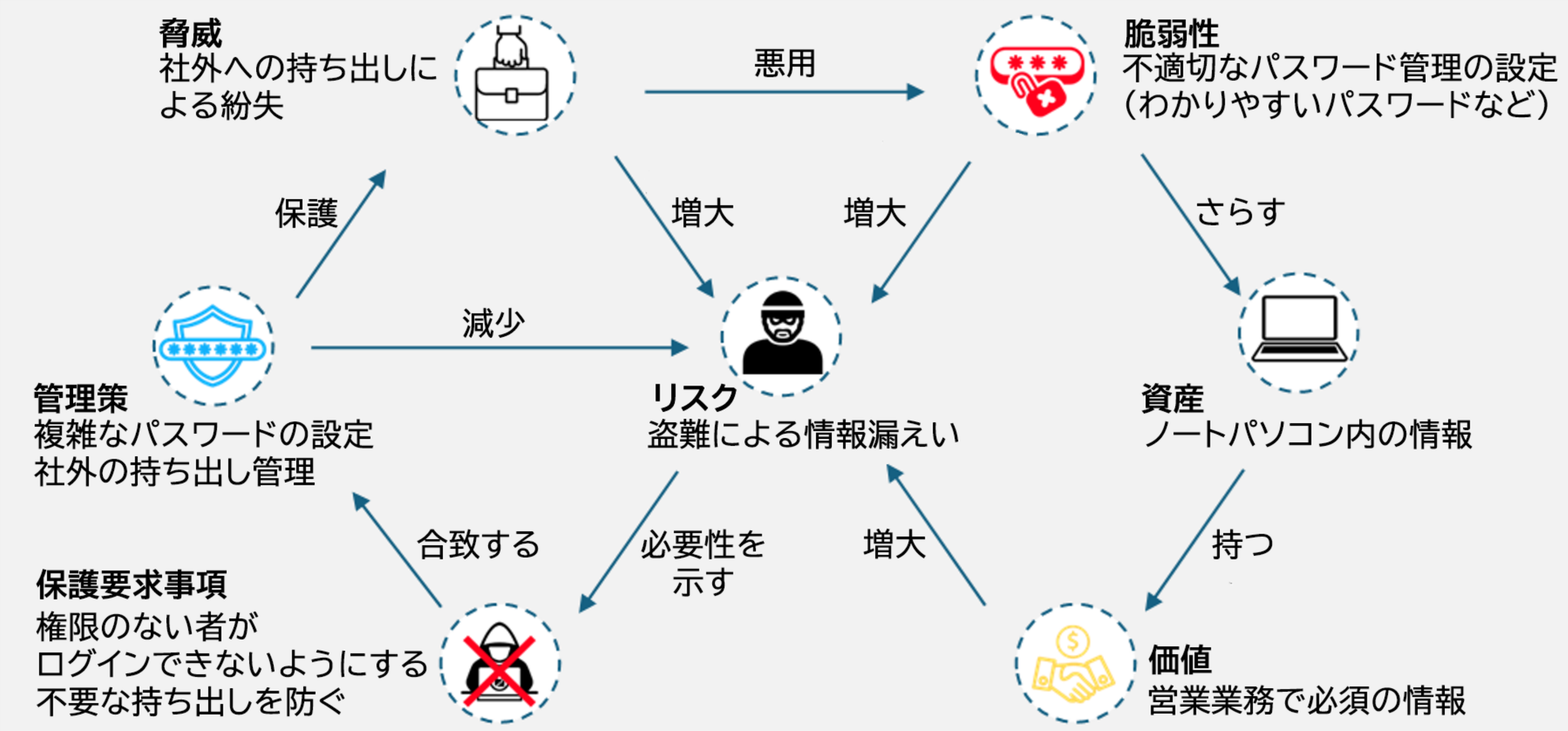
- ノートPCに対して、各要素について検討する

要素	内容
資産	• ノートPC内の情報(データ)
価値	• 営業の業務で必須の情報
脅威	• 社外への持ち出し
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(わかりやすい設定など)
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)

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-1.】
P104～P107

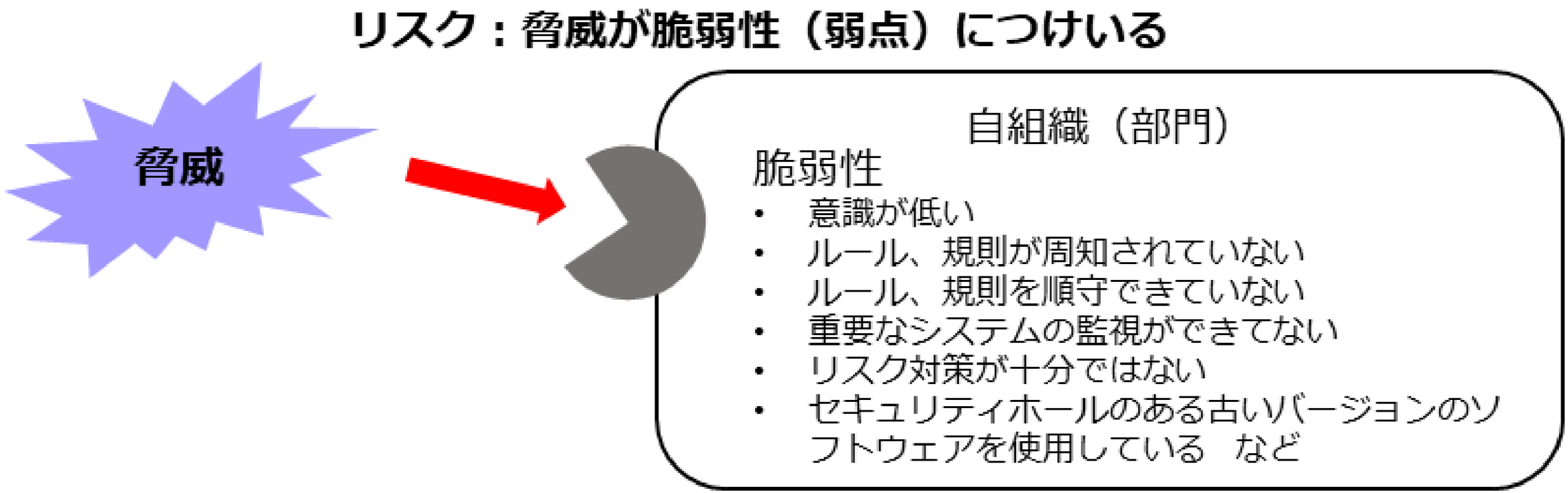
【例】業務用ノートPCのリスクマネジメント



用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-2.】
P108～P109

脅威の識別



（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

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-2.】
P108～P109

脅威の種類

- 脅威を区別することで、セキュリティ対策を整理しやすくなる

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）		被害：建物倒壊や火災による業務停止 対策：地震発生の可能性が低い場所を選択する、 災害からの回復対策を重視する
人為的脅威	意図的脅威 （Deliberate ➡ D）	被害：内部者による企業秘密の漏えい 対策：漏えい者を罰し、場合により損害賠償請求を行う 規程の明示と教育は抑止的対策の実施 漏えいの早期検知
	偶発的脅威 （Accidental ➡ A）	被害：入力ミスなどが原因の損害 対策：入力ミス防止の技術対策 2回入力 値の範囲制限 チェックデジットやチェックサムの設定

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-3.】
P110～P111

脆弱性の識別例

類型	脅威の例	脆弱性
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

用語の定義、脅威・脆弱性の識別

【参照:テキスト8-1-3.】
P110～P111

脆弱性の識別例

類型	脅威の例	脆弱性
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り当て
	使用時のミス	複雑なユーザーインタフェース
	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
	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

第9章. 具体的手順の作成（Lv.1 クイックアプローチ）

【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】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】の概要

【参照:テキスト9-1.】
P115

クイックアプローチ

概要

- 報道される事例や情報セキュリティ10大脅威を参考にする
- 発生する可能性が高いセキュリティインシデント事例を考慮する
- セキュリティインシデント発生時に被害が大きい事例を考慮する

メリット

- 低コストで効果的な対策が可能で、リソースが限られていても実施可能
- 流行中の攻撃に迅速に対応し、影響を最小限に抑えられる

デメリット

- 包括的でないため抜けが発生しやすく、一時的な対策になりがち
- 長期的には費用が増加する可能性がある

セキュリティインシデント事例を参考とした実施手順

【参照:テキスト9-2.】
P116～P119

対策基準・実施手順の作成手順

インシデント事例

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、この判断んをするまでに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。たとえば、経営者と総務担当は、情報漏えいを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、人件費だけでなく、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を参考とした実施手順

【参照:テキスト9-2.】
P116～P119

リスクアセスメントの実施

リスク特定

- 対象となる資産情報の洗い出し
- 機密性、完全性、可用性の評価
- 重要度の算出

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

セキュリティインシデント事例を参考とした実施手順

【参照:テキスト9-2.】
P116～P119

リスクアセスメントの実施

リスク分析

- 重要度と被害発生可能性から、リスクレベルを算出

「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	管理部署	媒体・保存先	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	人事部	人事担当者のPC	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	経理部	経理担当者のPC	3	3	2	3	2	6
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	2	6

セキュリティインシデント事例を参考とした実施手順

【参照:テキスト9-2.】
P116～P119

リスクアセスメントの実施

リスク評価

- リスク対応を検討する

要素	内容
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する
リスク移転	リスクを他者に移す
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
リスク受容(保有)	セキュリティ対策を行わず、リスクを受け入れる

セキュリティインシデント事例を参考とした実施手順

【参照：テキスト9-2.】
P116～P119

対策基準の策定

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

セキュリティインシデント事例を参考とした実施手順

【参照:テキスト9-2.】
P116～P119

実施手順の作成

実施手順(例)

機密情報に関する社内規程の策定

- 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。

＜詳細はテキストP115、P116を参照＞

第10章. 具体的手順の作成（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】の概要

【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

【Lv.2 ベースラインアプローチ】の概要

【参照:テキスト10-1.】
P122

ベースラインアプローチ

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する
- 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する

メリット

- 組織全体で一貫性を確保できる
- コストパフォーマンスよく、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

デメリット

- 十分なセキュリティ水準を確保できない可能性がある
- ひな型は一般的なものであるため、自社に合わせて検討が必要

ガイドラインを参考とした実施手順

【参照:テキスト10-2-1.】
P123～P124

情報セキュリティ対策ガイドラインの活用

参考にするガイドラインの例

- 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」
- NCO「インターネットの安全・安心ハンドブックVer.5.10」
- 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」

ガイドラインを参考とした実施手順

【参照:テキスト10-2-2.】
P124～P126

中小企業の情報セキュリティ対策ガイドラインの活用

対象者

- 中小企業および小規模事業者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

使い方

1. 実施状況の把握
2. 対策の決定と周知

ガイドラインを参考とした実施手順

【参照:テキスト10-2-3.】
P127～P128

インターネットの安全・安心ハンドブックの活用

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る
- サイバーセキュリティ対する素養・基本的な知識を身につける

使い方

1. ハンドブック記載内容を確認する
2. 自社の状況を把握する
3. 新たな実施手順を策定する

ガイドラインを参考とした実施手順

【参照:テキスト10-2-4.】
P128～P129

テレワークセキュリティガイドラインの活用

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する
- 安心してテレワークを導入・活用する

使い方

1. 立場ごとに分類された具体的に実施すべき項目を確認する
2. 自社の状況を把握する
3. 規程や手順に反映させる

ガイドラインを参考とした実施手順

【参照:テキスト10-2-5.】
P130～P131

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

使い方

1. クラウドサービス安全利用チェックシートを活用する
2. 解説編を参考に、利用者としての役割や責任を認識する
3. 実施手順を策定する

ガイドラインを参考とした実施手順

【参照:テキスト10-2-6.】
P131～P133

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

使い方

1. 対応すべきリスクを特定する
2. セキュリティ対策の決定
3. 規程の作成

第11章. セキュリティフレームワーク

セキュリティフレームワークの概要

情報セキュリティマネジメントシステム（ISMS）

サイバー・フィジカル・セキュリティ対策フレームワーク（CSF）

サイバーセキュリティ経営ガイドライン

セキュリティフレームワークの概要

【参照:テキスト11-1-1.】
P136～P137

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定義

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す

セキュリティフレームワークを利用するメリット

- 効果的なセキュリティ対策
- 信頼性の確保

セキュリティフレームワークの概要

【参照:テキスト11-1-1.】
P136～P137

代表的なセキュリティフレームワーク

	フレームワーク名		概要
1	ISMS	別途詳細	[ISO/IEC27001、ISO/IEC27002] 網羅的なセキュリティフレームワーク
2	ISO/IEC27017		クラウドサービス対象のセキュリティフレームワーク
3	CSF	別途詳細	重要インフラ対象のセキュリティフレームワーク
4	CPSF	別途詳細	Society5.0における産業社会が対象のセキュリティフレームワーク
5	サイバーセキュリティ経営ガイドライン	別途詳細	経営者を中心としたセキュリティ対策
6	PCI DSS		クレジットカード産業を対象としたデータセキュリティ基準
7	PMS		個人情報保護
8	CIS Controls		具体的なサイバー攻撃アプローチ
9	ISA/IEC62443		産業オートメーションおよび制御システム

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P137～P139

代表的なセキュリティフレームワークの概要

ISO/IEC27017

- 対象：クラウドサービスの提供者と利用者
- 目的：クラウドサービスのリスク低減、適切な利用のための組織体制の確立
- ISO/IEC27002をベースに作成
- ISO/IEC27001は情報セキュリティのマネジメントシステム規格
- ISO/IEC27017を通じて、ISO/IEC27001を強化し、クラウドサービス向けの情報セキュリティ管理体制の構築が可能

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P137～P139

代表的なセキュリティフレームワークの概要

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）

- 対象：　クレジットカード情報を取扱う全ての事業者
- 名称：　Payment Card Industry Data Security Standard
  （略称：PCI DSS）
- 目的：　カード会員情報の適切な管理
- 基準策定：国際カードブランド5社が共同で策定した国際基準
- 基準内容：ネットワークアーキテクチャ、ソフトウェアデザイン、
  セキュリティマネジメント、ポリシー、プロシジャなど
  12の要件で規定

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P137～P139

代表的なセキュリティフレームワークの概要

PMS（個人情報保護マネジメントシステム）

- 目的：　組織が取扱う個人情報の安全・適切な管理
- 規格：　JIS Q 15001
- 主な内容：　事業者が個人情報を適切に取扱う方法の規定
- プライバシー保護：　直接の目的ではないが、結果的に保護される
- PMSの基本：　個人情報保護方針の設定と、その方針に基づくPDCAサイクルの実行

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P137～P139

代表的なセキュリティフレームワークの概要

CIS Controls

- 目的：　サイバー攻撃の現状・傾向をもとに、組織のサイバーセキュリティ対策と優先順位を決定するフレームワーク
- 重点：　あらゆる企業の最も基本的・重要な対応
- 特徴：　ネットワークの詳細設定、ログ管理などの具体的・技術的対策が中心
- アプローチ：　多岐にわたる対策から、自社の実施すべき対策と優先順位を導出

フレームワーク選択の重要性

【参照：テキスト11-1-2.】
P137～P139

代表的なセキュリティフレームワークの概要

ISA/IEC62443

- 主題：　産業用自動制御システムのセキュリティ対策・プロセス要件の国際標準規格
- カバー範囲：　ISO/IEC 27001では十分にカバーされない工場やプラントの制御システムのセキュリティ
- 対象：　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
- 特徴：　システムだけでなく、運用に関わる「人」と「業務」も対象

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト11-2.】
P140～P141

ISMSの概要

- 定義：　ISMSは情報セキュリティマネジメントシステムの略
- 目的：　組織の情報セキュリティリスクの適切な管理
- 地位：　国際規格の存在により、代表的なセキュリティフレームワークとして認識
- 達成目標：　情報の機密性、完全性、可用性をバランス良く維持・改善し、信頼を提供
- 対策範囲：　技術的対策、従業員教育・訓練、組織体制の整備を含む

情報セキュリティマネジメントシステム(ISMS)

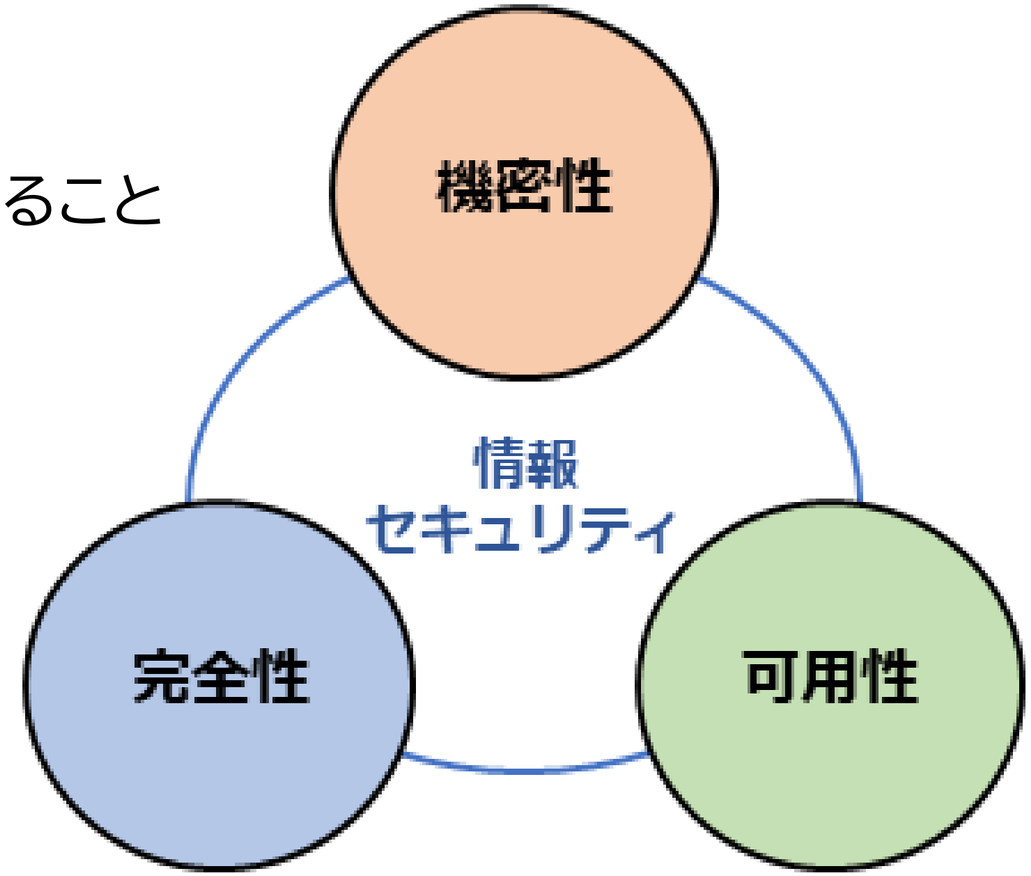
【参照:テキスト11-2.】
P140～P141

情報セキュリティの3要素(情報セキュリティのCIA)

機密性(Confidentiality)
　情報に対するアクセスを適切に管理すること

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)
　情報を必要な時に使えるようにしておくこと



情報セキュリティマネジメントシステム(ISMS)

【参照:テキスト11-2.】
P140～P141

情報セキュリティの7要素　※3要素(CIA)＋追加4要素

真正性(Authenticity)
　情報にアクセスしているユーザー・端末が、許可された人物やシステムであることを明確にする状態

信頼性(Reliability)
　システムの処理やデータ操作が、欠陥や不具合なく実行されること

責任追跡性(Accountability)
　情報やシステムに対する操作が、誰によってどのように行われたのかを明確にすること

否認防止(non-repudiation)
　情報資産に関する問題が発生した際、その原因となる人物が、後から否認できないよう証明すること

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト11-2.】
P140～P141

ISO/IEC27001とJIS Q 27001

ISMSのための要求事項をまとめた国際規格が、ISO/IEC27001
ISO/IEC 27001を日本語訳し、日本産業規格としたものがJIS Q 27001

使用用途

- 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
- 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

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

CSF(Cybersecurity Framework)の概要

- CSFはNIST(米国国立標準技術研究所)が作成したサイバー攻撃対策のフレームワーク
- 防御だけでなく、検知・対応・復旧のインシデント対応が含まれる
- 要求事項は汎用的で、多様な企業に適用可能
- 指示書やノウハウ集ではない
- 利用方法は実施する組織に委ねられている
- CSFを理解し、サイバーセキュリティ対策の検討が必要

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

CSF2.0 の3つの構成要素

「コア」の概要

サイバーセキュリティ対策の一覧

「ティア」の概要

対策状況を数値化するための成熟度評価基準

「プロファイル」の概要

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

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

コアとは

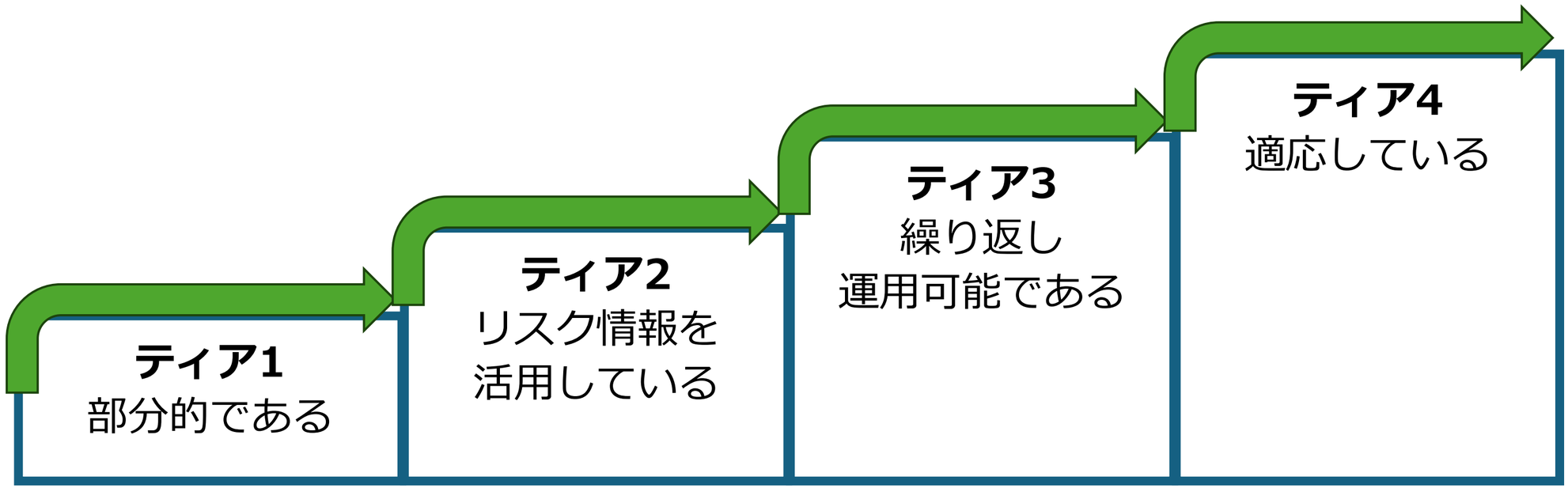
業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものであり、「識別」「防御」「検知」「対応」「復旧」「ガバナンス」の6つの機能に分類される。

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

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ある。
指標はティア1～ティア4まで、下図のように定義が4段階ある。

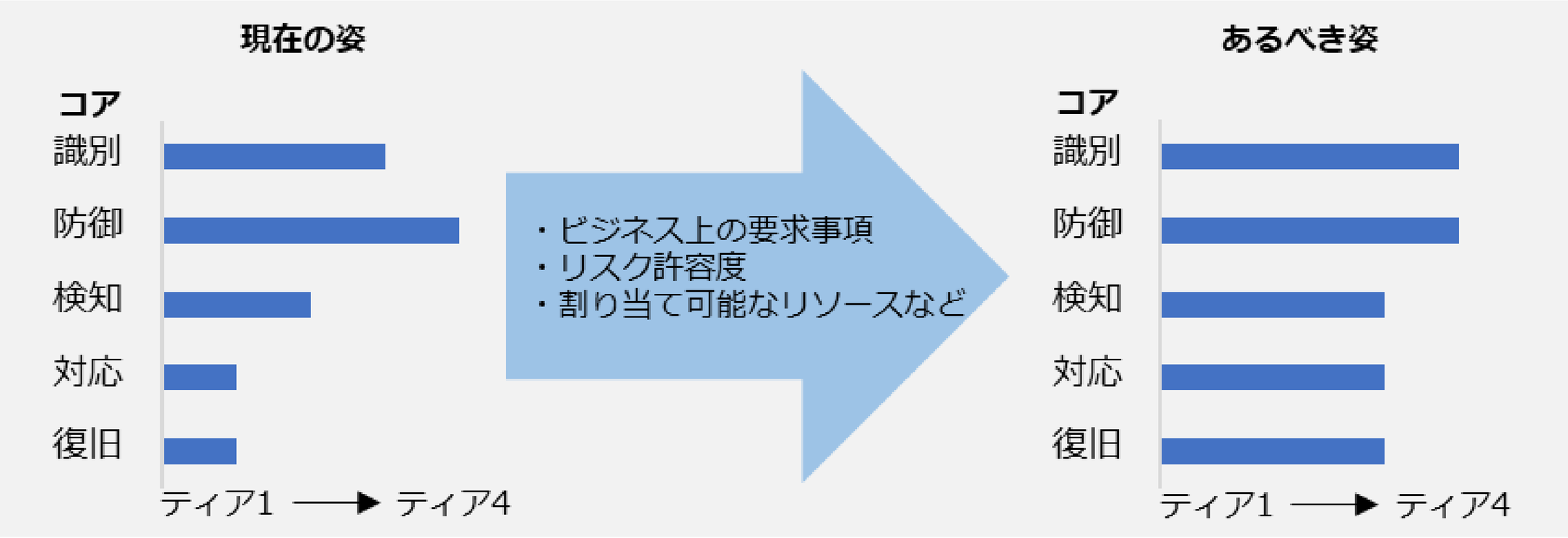


NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

プロファイルとは

組織ごとの考慮点を整理したもので、サイバーセキュリティ対策の現状と目標状態を明示することにより、必要な改善点のギャップを特定できる。
また、「あるべき姿」は、ビジネス要求やリスク許容度、リソースをもとに策定される。



NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-1.】
P142～P149

CSF 2.0 の特徴

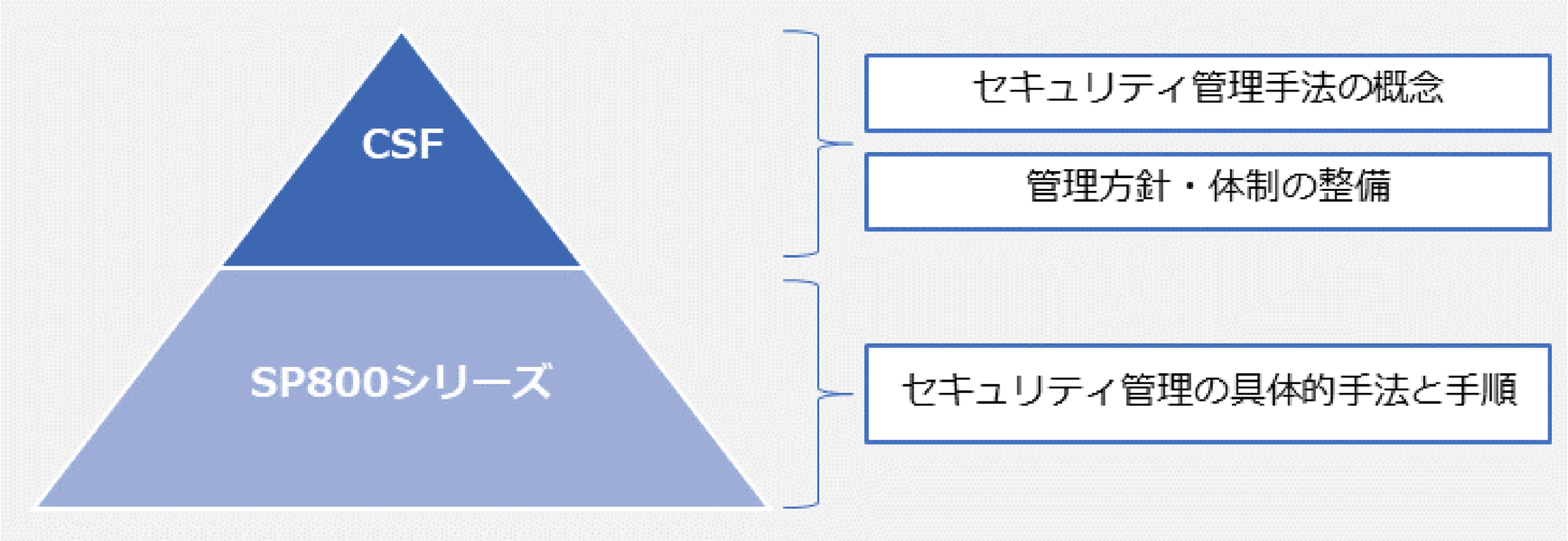
- フレームワークの適用範囲拡大
- 新たな機能「ガバナンス」の追加
- フレームワーク活用のためのコンテンツ強化
- サプライチェーンリスクマネジメントの強化

NISTサイバーセキュリティフレームワーク(CSF)

【参照:テキスト11-3-2.】
P149～P150

NIST SP800シリーズとCSFの関連性

CSFの下位概念に位置づけられているのが、NIST SP800シリーズである。
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る。



NISTサイバーセキュリティフレームワーク（CSF）

【参照：テキスト11-3-3.】
P151

CSFとISMSの関連性

主な共通点

- 汎用性が高い
- サイバーセキュリティ対策方法
- 任意性がある

主な相違点

- 第三者認証制度の有無
- 目標への到達手段

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P152～P153

CPSFの概要

- Society5.0でサイバー空間とフィジカル空間が融合
- サプライチェーンが「価値創造過程」として変化
- 新しいサプライチェーンにはサイバー攻撃のリスク増
- 政府が「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
- CPSFは既存のISMSやCSFをもとに、サイバーとフィジカルの両方のセキュリティ対応

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P152～P153

CPSFの目的と適用範囲

目的

CPSFは新たな産業社会のバリュークリエイションプロセスを理解し、リスクを明確化し、セキュリティ対策を整理すること。

適用範囲

新たな産業社会のバリュークリエイションプロセス全体。

- **新たな産業社会における**バリュークリエイ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

サイバー・フィジカル・セキュリティ対策フレームワーク

【参照:テキスト11-4.】
P152～P153

3層構造モデル

サイバー空間におけるつながり[第3層]

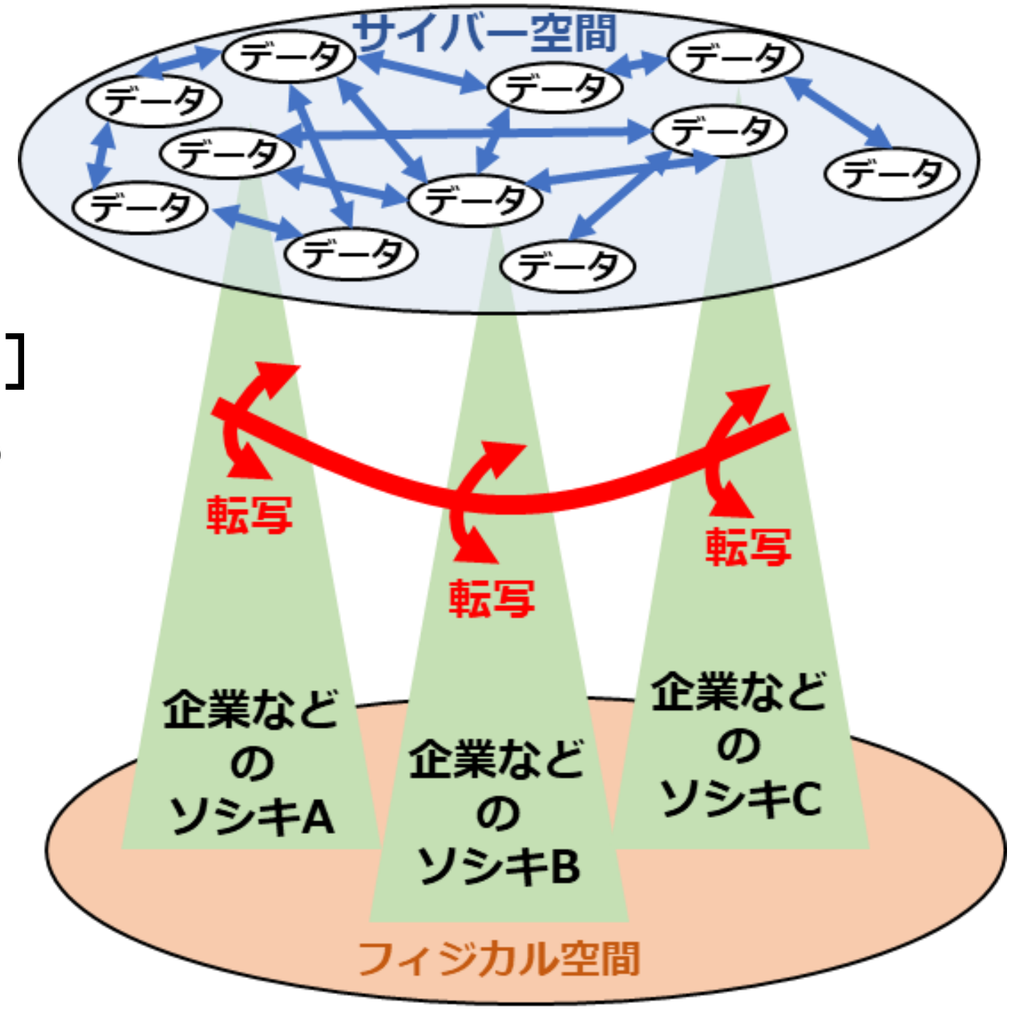
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

フィジカル空間とサイバー空間のつながり[第2層]

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

企業間のつながり[第1層]

適切なマネジメントを基盤に各主体の信頼性を確保



サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-1.】
P154～P159

経営者が認識するべき3原則

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ガイドライン

【参照:テキスト11-5-1.】
P154～P159

経営の重要10項目(指示1～6)

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**

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-1.】
P154～P159

経営の重要10項目(指示7～10)

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**

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-2.】
P159～P160

ガイドラインの読み方（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に指示を出す
- リーダーシップの発揮

認識すべきこと

- ERMにサイバー攻撃のリスクを含めること
- サプライチェーン上のリスクを認識すること
- 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
- 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経営ガイドライン

【参照:テキスト11-5-2.】
P159～P160

ガイドラインの読み方（担当幹部）

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

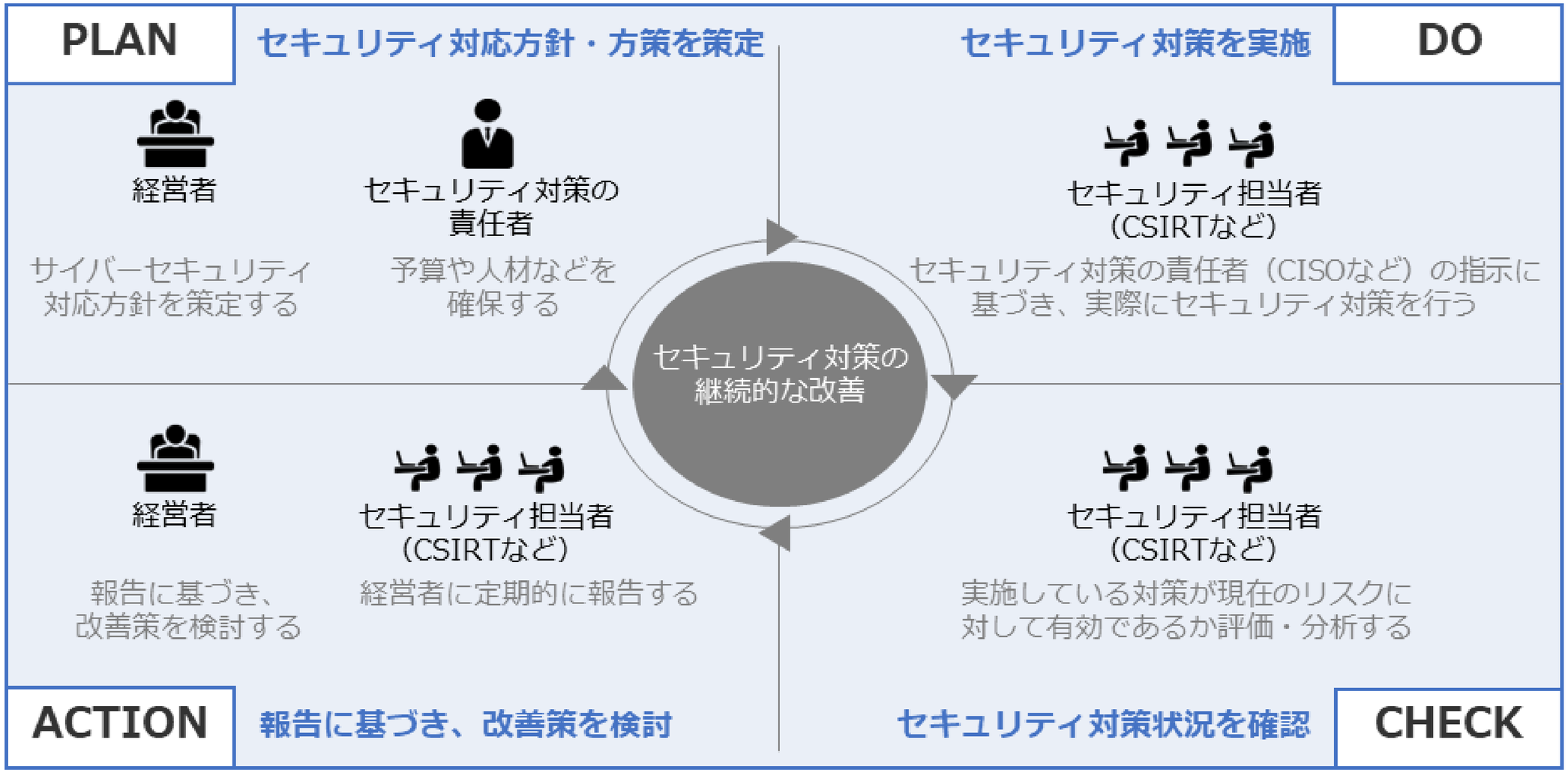
認識すべきこと

- 経営者から指示される内容に関して、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をする必要があること

サイバーセキュリティ経営ガイドライン

【参照:テキスト11-5-3.】
P161～P162

サイバーセキュリティ経営ガイドラインの実践の流れ



第12章. リスクマネジメント

リスクマネジメント：概要

リスクマネジメント：リスクアセスメント

リスクマネジメント：リスク対応

リスクマネジメント：概要

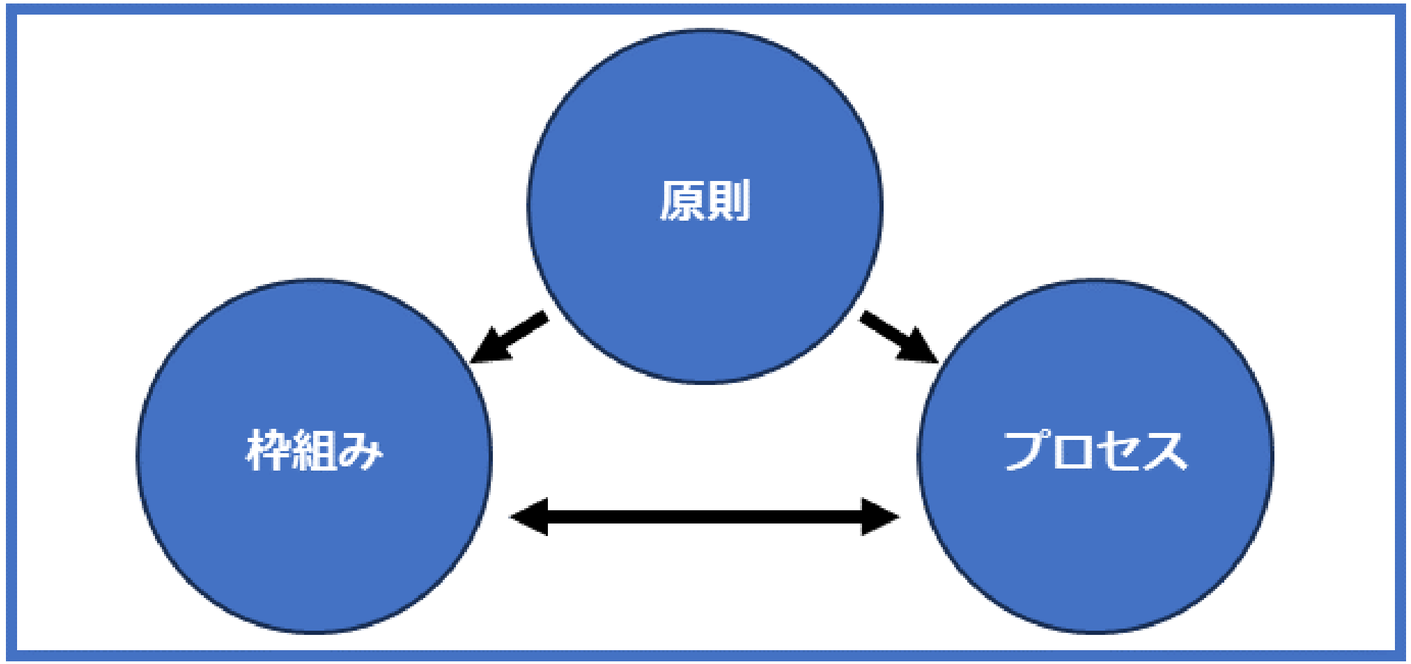
【参照：テキスト12-1-1.】
P164

リスクマネジメントプロセス（ISO31000）

リスクマネジメントとは

存在する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

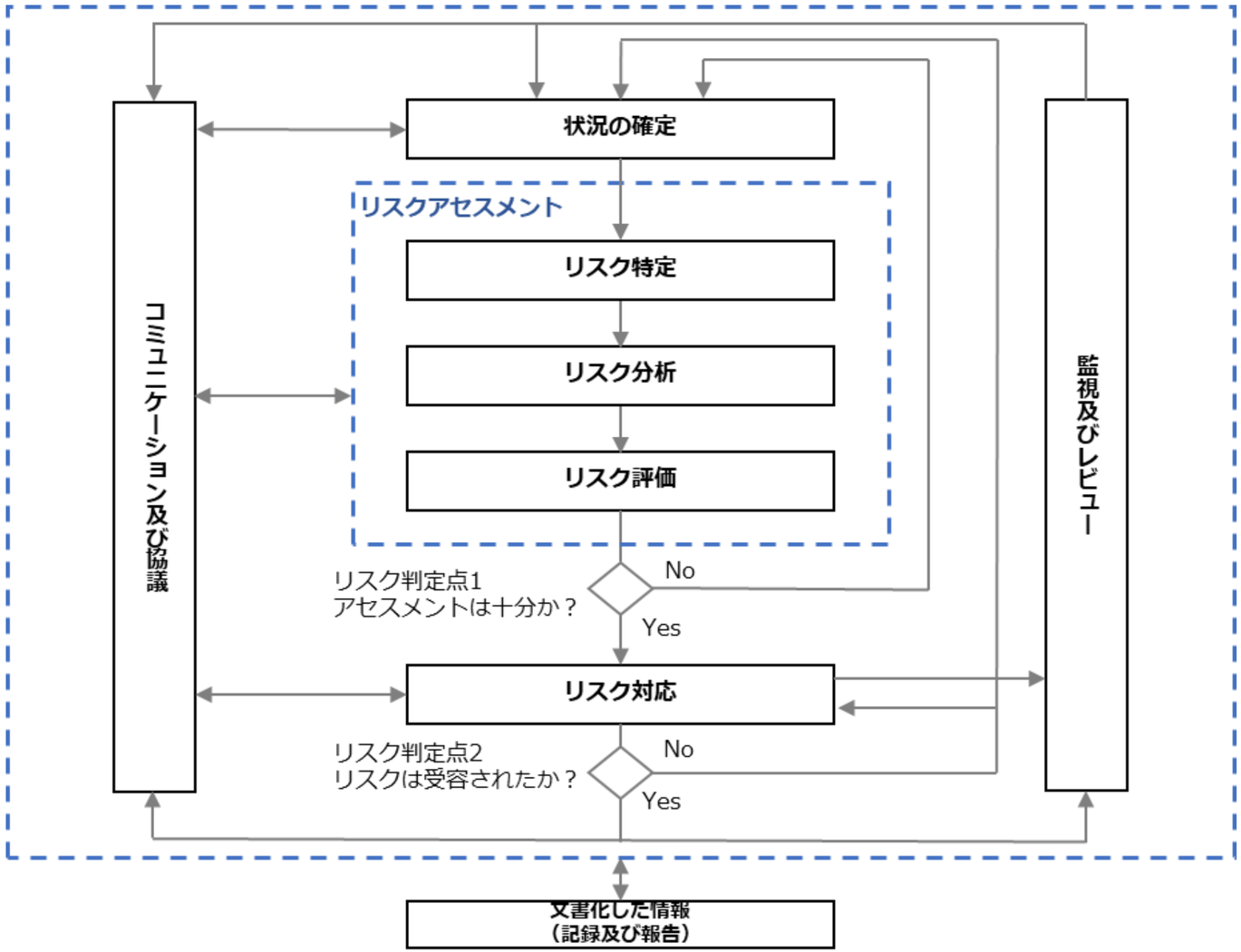
ISO31000での構成要素



リスクマネジメント：概要

【参照：テキスト12-1-2.】
P165～P167

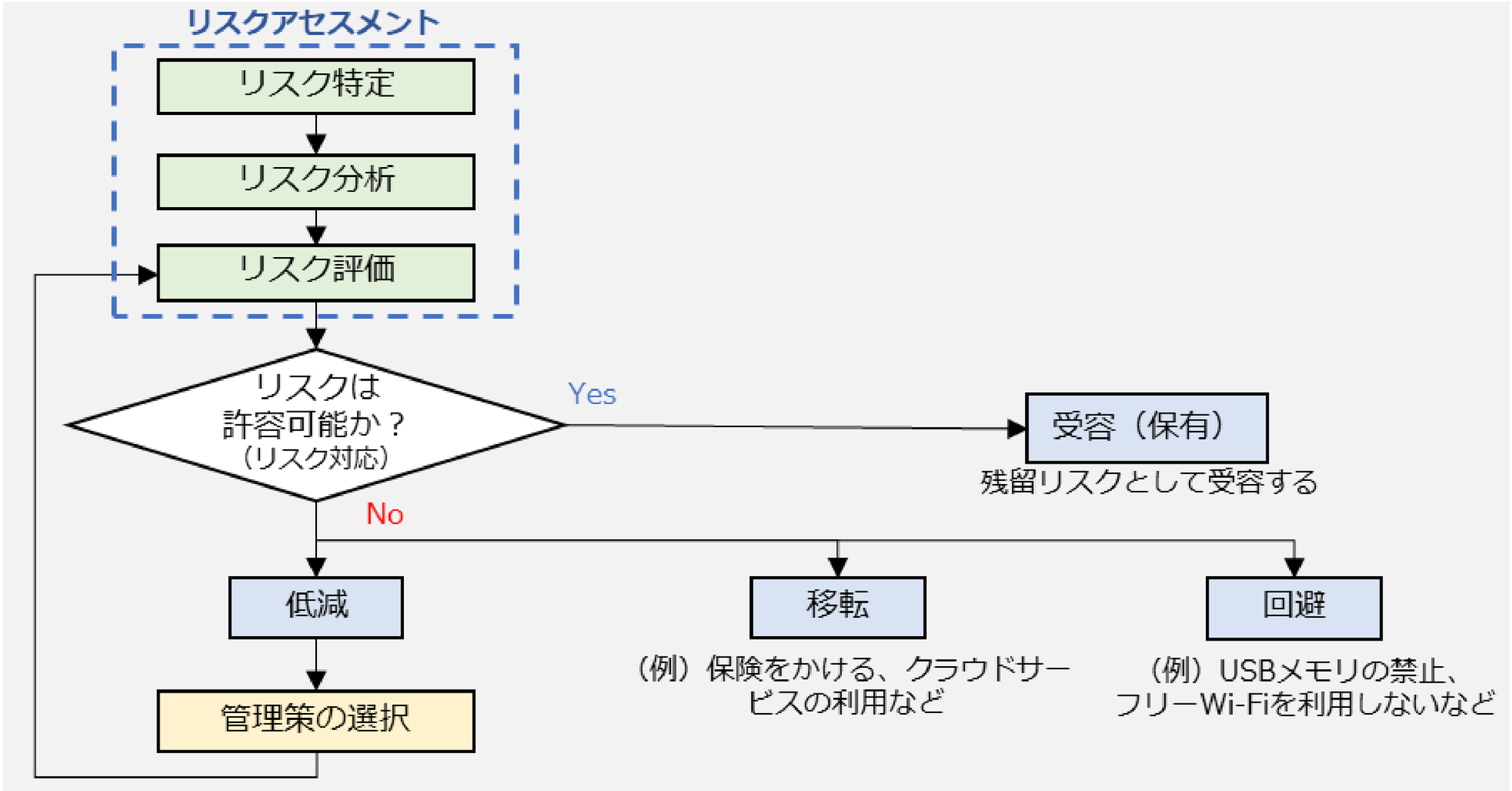
情報セキュリティリスクマネジメント（ISO/IEC27005）



リスクマネジメント：概要

【参照：テキスト12-1-2.】
P165～P167

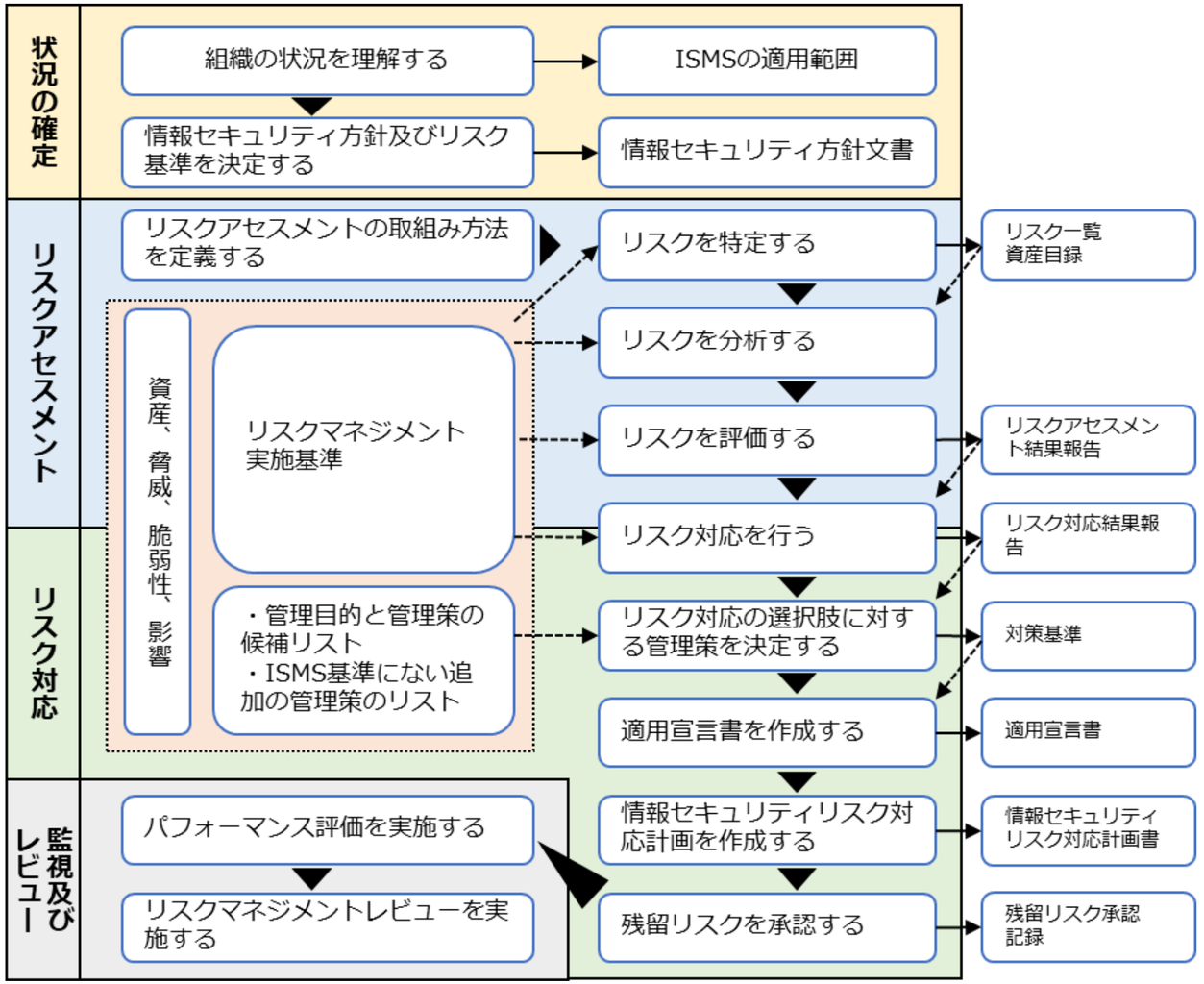
情報セキュリティリスクマネジメント（ISO/IEC27005）



リスクマネジメント：概要

【参照：テキスト12-1-3.】
P167

ISO/IEC 27001におけるリスクマネジメント手順



リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-1.】
P168

リスク基準の確立

必要なリスク基準

状況の確定
- 組織の状況を把握する
- **リスク基準を策定する**

リスクの特定
- リスクを発見、認識、記述する

リスクの分析
- 特定されたリスクのリスクレベルを算出する

リスクの評価
- **リスク分析の結果をリスク基準と比較する**
- **対策の必要性の有無、優先順位を決定する**

リスク対応
- **リスク対応計画を策定する**

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定

アプローチ手法と特徴

- 資産ベースのアプローチ
- 事象ベースのアプローチ
- リスク所有者の特定

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

アプローチ手法

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

情報資産の洗い出し(例)

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
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	顧入時・定期健康診断	人事部	人事部長	人事部	書類
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
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
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
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
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
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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

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 漏えいすると取引先や顧客に大きな影響がある	• 取引先から秘密として提供された情報 • 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・ノウハウ • 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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
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がある	• 製品の設計図 • 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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(資産ベースのアプローチ)

影響度の評価をもとに重要度を算定

重要度	情報資産の価値・事故の影響の大きさ
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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(事象ベースのアプローチ)

アプローチ手法

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) 「ネットワーク生涯により、リモートによる会議が中断もしくは実施できなくないり、取引先や顧客に及ぼす恐れ」

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。

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-2.】
P169～P175

リスク特定(事象ベースのアプローチ)

リスク特定【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

評価値			重要度	リスク所有者
機密性	情報が漏えいする類の事象ではない	1	3	○○○○
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およぼす事象である	3		

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P175～P176

リスクの分析

リスク分析の例

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P175～P176

リスクの分析

被害発生可能性とは

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する （いつ発生してもおかしくない）
2	特定の状況で脅威が発生する （年に数回程度）
1	通常の状況で脅威が発生することはない （通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない （ほぼ無防備）
2	部分的に対策を実施している （一部対策を実施）
1	必要な対策をすべて実施している （対策を実施）

「起こりやすさ（脅威）」と「つけ込みやすさ（脆弱性）」の換算表で算出する

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-3.】
P175～P176

リスクの分析

被害発生可能性の換算表

被害発生可能性		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

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-4.】
P177～P178

リスクの評価

「リスクレベル」＝「重要度」×「被害発生可能性」

リスク評価(例)

リスクレベル評価値		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

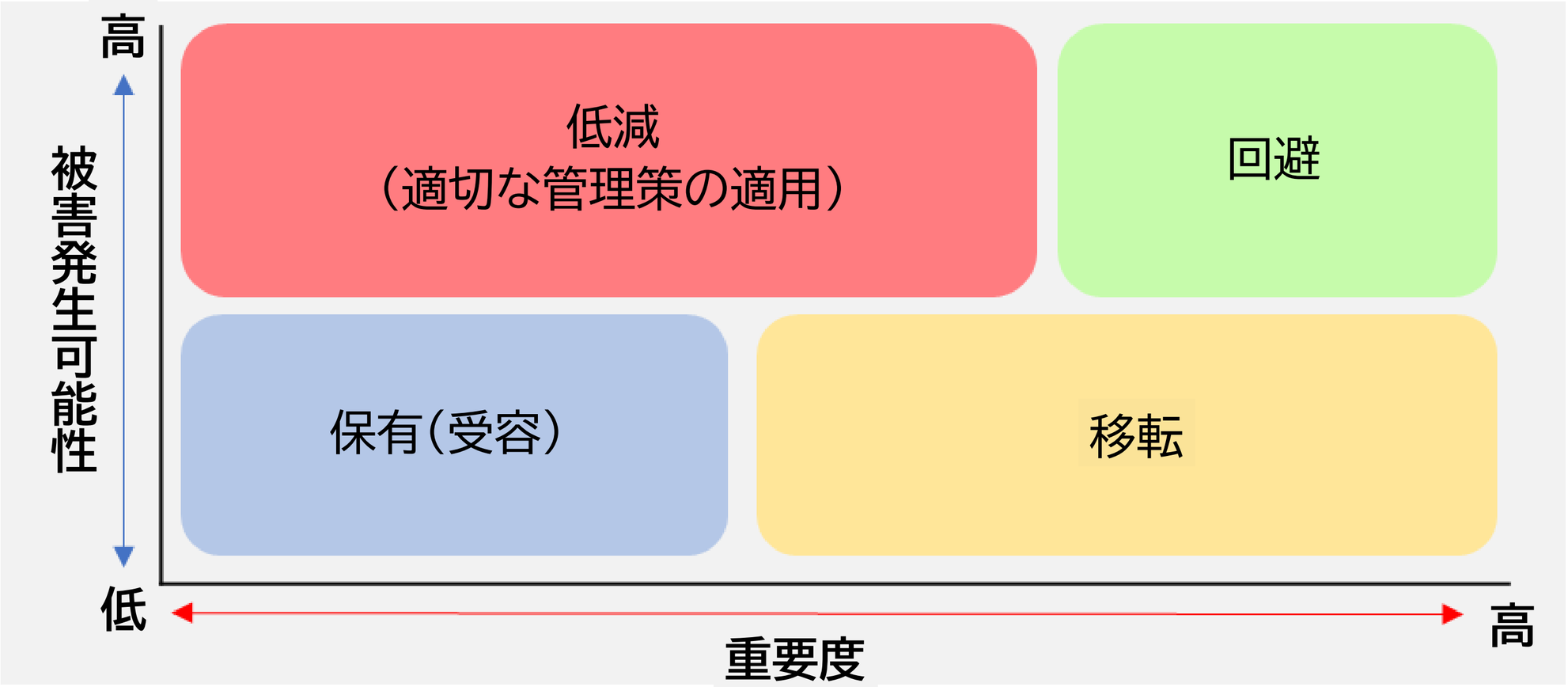
リスクレベル	リスク評価	記述
低	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい そうでない場合、活動の全部又は一部を拒否することが望ましい

リスクマネジメント:リスクアセスメント

【参照:テキスト12-2-4.】
P177～P178

対応策の検討

リスク対応の選択肢の選定方法

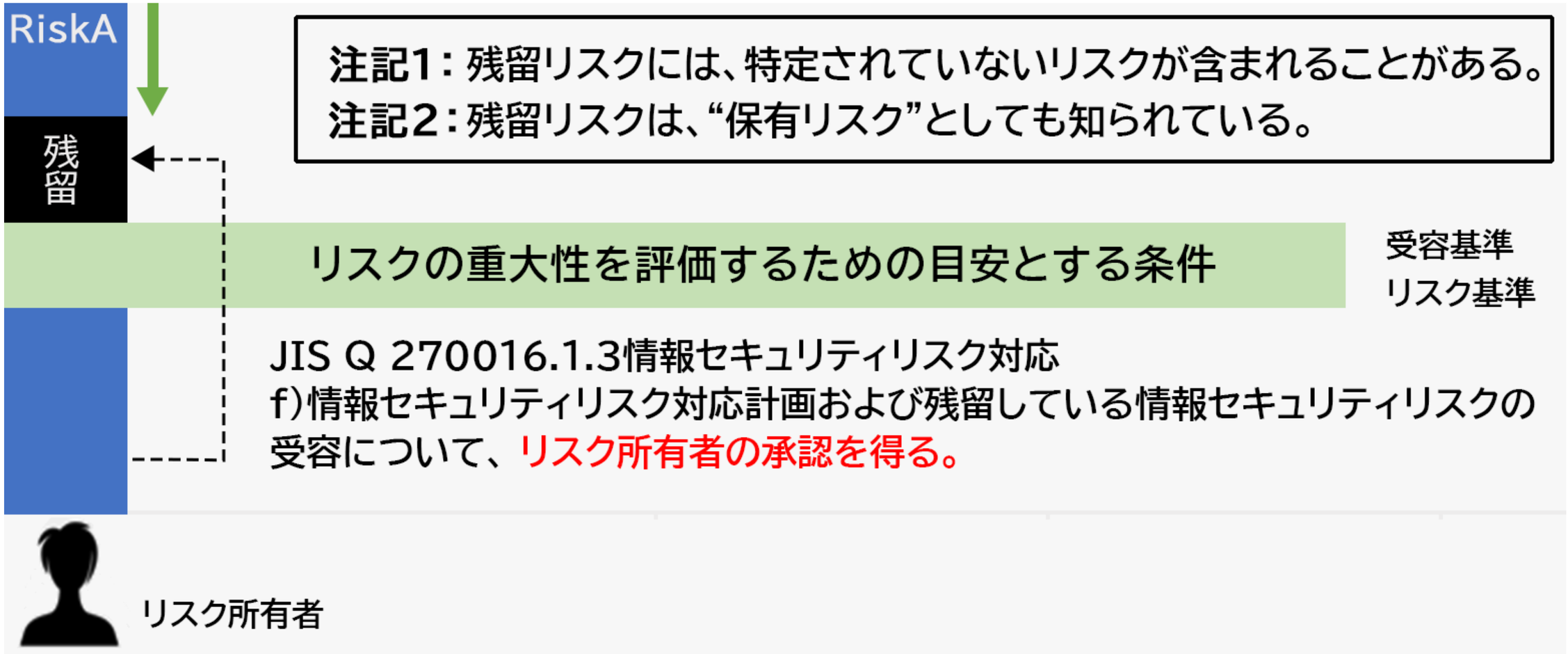


リスクマネジメント:リスクアセスメント

【参照:テキスト12-3.】
P179～P181

対応策の検討

残留リスク



第13章. ISMSの要求事項と構築（LV.3 網羅的アプローチ）

【LV.3 網羅的アプローチ】の概要

【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文書体系（ISMS構築・導入に必要な文書と記録）

ISO/IEC27001の審査準備と審査内容

【LV.3 網羅的アプローチ】の概要

【参照:テキスト13-1.】
P184

概要

特徴

特徴	想定される適用ケース
• 脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法 • ISMSなどの認証が可能なレベルを目指して、対策基準を策定	• ISMSのフレームワークに沿った対策基準を策定する場合

メリット・デメリット

メリット	デメリット
• 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できる	• 全体的な実施には時間がかかる

【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

【参照:テキスト13-2-1.】
P185～P186

ISO/IEC27001 各要求事項の概要

構成		概要
1.	適用範囲	ISMS運用のための要求事項の規程
2.	引用規格	ISO/IEC 27000（ISMSの概要と用語）を引用する
3.	用語および定義	用語および定義は、ISO/IEC 27000に定めている
4.	組織の状況	組織の内情などを把握した上で、適用範囲の決定を要求する
5.	リーダーシップ	トップマネジメントが実施するべきことのまとめ
6.	計画	ISMSの計画を立てる（PDCAのP）
7.	支援	構成員の教育など、組織が行うべきサポートの要求
8.	運用	ISMSを実行する際の要求（PDCAのD）
9.	パフォーマンス評価	適切に構築・運用できているかを評価する（PDCAのC）
10.	改善	是正処置や不適格があった場合の対処法（PDCAのA）

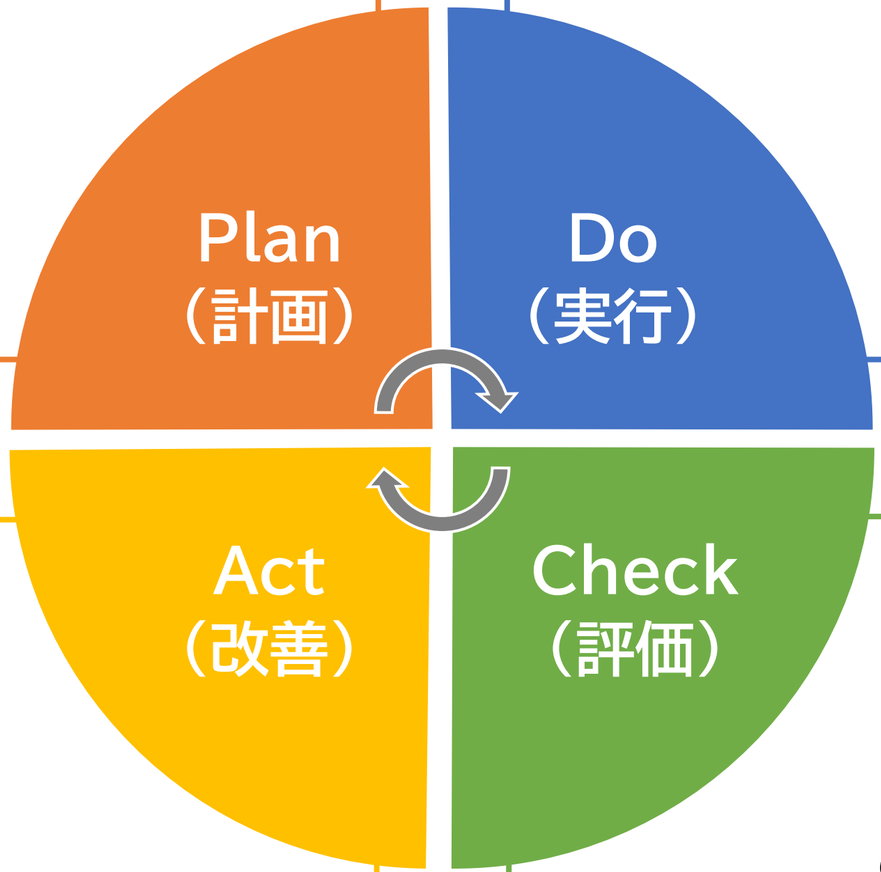
【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

【参照:テキスト13-2-1.】
P185～P186

ISMSの確立、運用、監視

4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援

8. 運用



10. 改善

9. パフォーマンス評価

【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

【参照:テキスト13-2-2.】
P186～P192

ISMS:4. 組織の状況

	作成文書(例)	テキスト
4.1 組織及びその状況の理解 組織の目的に関連する内部・外部課題 (追補1) 気候変動が自社課題となるかを決定することが必要	• 外部及び内部の課題	P187～P188
4.2 利害関係者のニーズ及び期待の理解 利害関係者から要求される情報セキュリティ (追補1) 利害関係者から気候変動対応を求められる可能性	• 利害関係者のニーズ及び期待	P189
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 物理的配置、論理的構成を含め、適用範囲の決定	• ISMS適用範囲 • レイアウト図 • ネットワーク図	P190～P192
4.4 情報セキュリティマネジメントシステム PDCAに基づく運用	―	―

【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

【参照:テキスト13-2-3.】
P192～P196

ISMS:5. リーダーシップ

	作成文書(例)	テキスト
5.1 リーダーシップ及びコミットメント トップが責任を持って実行すること	―	P193～P194
5.2 方針 情報セキュリティ方針の作成	• 情報セキュリティ方針	P194～P195
5.3 組織の役割、責任及び権限 役割と権限の割り当てと組織内への伝達	• 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	P195～P196

【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

【参照:テキスト13-2-4.】
P196～P206

ISMS:6. 計画

	作成文書(例)	テキスト
6.1 リスク及び機会に対する活動 情報資産に対するリスクの決定と対応手順の確立	• 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 • リスク対応計画	P197～P204
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 目的の確立と達成のための計画策定	• ISMS有効性評価表	P204～P206
6.3 変更の計画策定 変更が必要な時は計画的に	―	―

【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

【参照:テキスト13-2-5.】
P206～P215

ISMS:7. 支援

	作成文書(例)	テキスト
7.1 資源 必要資源【人、物、金、情報】の決定	―	P207～P208
7.2 力量 要員の力量を定義し、評価する 結果に応じて教育を計画し実施	• 力量確認表 • 教育計画書 • 理解度確認テスト • 教育実施記録	P208～P212
7.3 認識 適用範囲のすべての要員が認識しなければならない内容	―	P212～P213
7.4 コミュニケーション 意思疎通に必要なプロセスの確立	―	P213～P214
7.5 文書化した情報 文書化した情報の作成、更新、管理	―	P214～P216

【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

【参照:テキスト13-2-6.】
P216～P219

ISMS:8. 運用

	作成文書(例)	テキスト
8.1 運用の計画及び管理 計画した活動の一覧表作成	• ISMS年間計画表	P216～P219
8.2 情報セキュリティリスクアセスメント 実施したリスクアセスメントプロセス結果の文書化	• リスクアセスメント結果報告書	P219
8.3 情報セキュリティリスク対応 実施したリスク対応計画結果の文書化	• リスク対応計画	P219

【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

【参照:テキスト13-2-7.】
P220～P227

ISMS:9. パフォーマンス評価

	作成文書(例)	テキスト
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の有効性の評価	• ISMS有効性評価表	P220～P221
9.2 内部監査 ISMSの適合性、有効性についての監査	• 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	P221～P224
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	• マネジメントレビュー報告書	P225～P227

【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

【参照:テキスト13-2-8.】
P228～P230

ISMS:10. 改善

	作成文書(例)	テキスト
10.1　継続的改善 ISMSのPDCAサイクルを継続して実施し、 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な改善を継続していく	―	―
10.2　不適合及び是正処置 不適合が発生した際の是正処置の実施	• 是正要求書兼回答書	P228～P230

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

【参照:テキスト13-3-1.】
P231

ISMS文書としての策定内容とポイント

ISO/IEC 27001:2022附属書Aの管理策

カテゴリ	項目数	管理策
組織的管理策	37	• 組織として取り組む必要のある管理策 • 組織としてのルールを定めるもの
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 • 情報セキュリティの意識向上や教育など
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 • オフィス、部屋および施設の物理的セキュリティや監視、装置の保守など
技術的管理策	34	• 技術面での管理策 • ネットワーク、システム全般のセキュリティ、データの暗号化、バックアップ、脆弱性管理、ログ管理、マルウェア対策など

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

【参照：テキスト13-3-2.】
P232～P236

ISMSの要求事項

ISO/IEC 27001の要求事項

要求事項	内容
ISMSの構築	組織は、ISMSを計画し、導入する
リスクアセスメント	組織内の情報セキュリティリスクを識別し、そのリスクを評価する
リスク対応策の実施	評価されたリスクに対して、適切な対応策を実施する必要がある
ISMSの維持と改善	ISMSは、PDCAサイクルに従って運用し、継続的に監視・評価され、必要に応じて改善していく
認証取得のための要件遵守	ISO/IEC 27001の認証を取得するには、これらの要求事項をすべて満たす必要がある

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

【参照：テキスト13-3-2.】
P232～P236

ISMSの管理策

- 情報セキュリティマネジメントの具体的な管理策を示す規格が「ISO/IEC 27002」
- ISO/IEC 27002の管理策を取り入れ、リスク低減のための目的と管理策で構成されているもの（リスト）が「ISO/IEC 27001附属書A」
- 「ISO/IEC 27001附属書A」は、要求事項を補完するガイドラインとして位置づけされている。
- 全ての管理策を採用する必要はないが、採用しない理由を明確にしなければならない。

ISMS文書体系（ISMS構築・導入に必要な文書と記録）

【参照：テキスト13-3-2.】
P232～P236

ISMSの管理策における属性

カテゴリ	属性数	属性値
管理策タイプ	3	予防、検知、是正
情報セキュリティ特性	3	機密性、完全性、可用性
サイバーセキュリティ概念	5	識別、防御、検知、対応、復旧
運用機能	15	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のセキュリティ、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管理、脅威およびぜい弱性の管理、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	4	ガバナンスおよびエコシステム、保護、防御、対応力

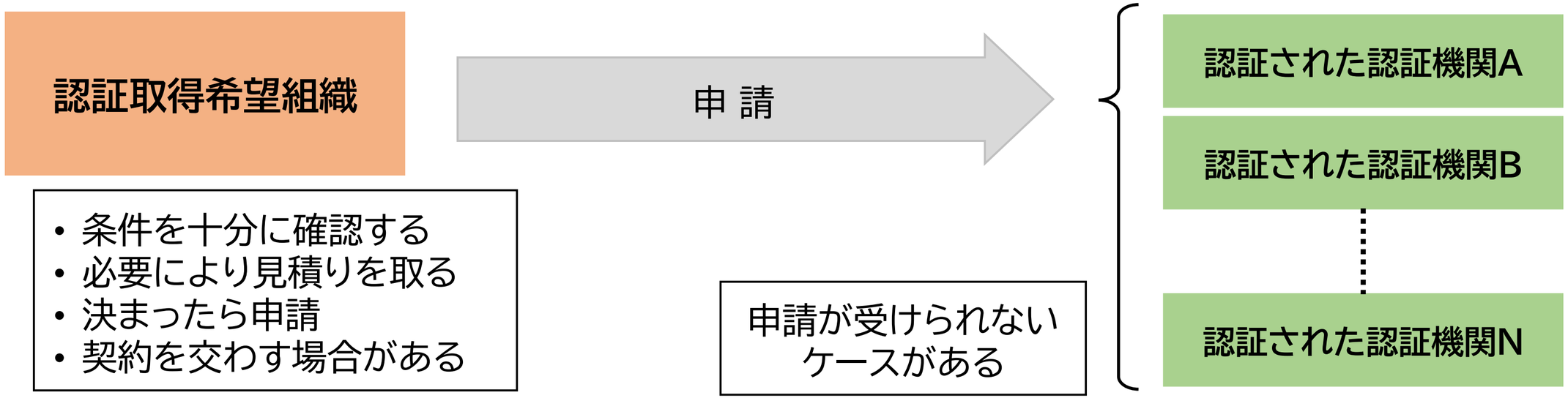
ISO/IEC27001の審査準備と審査内容

【参照:テキスト13-4-1.】
P237～P238

ISO/IEC27001の認証機関の選定と申し込み

認証取得の申請先

認証機関の選択



ISO/IEC27001の審査準備と審査内容

【参照:テキスト13-4-2.】
P238～P239

ISO/IEC27001の審査事前準備

ISMSの構築ステップ

1. 適用範囲の決定
2. 情報セキュリティ方針の策定
3. 体制の確立
4. ISMS文書化
5. リスクアセスメントの実施
6. 従業員の教育
7. 内部監査
8. マネジメントレビュー

ISO/IEC27001の審査準備と審査内容

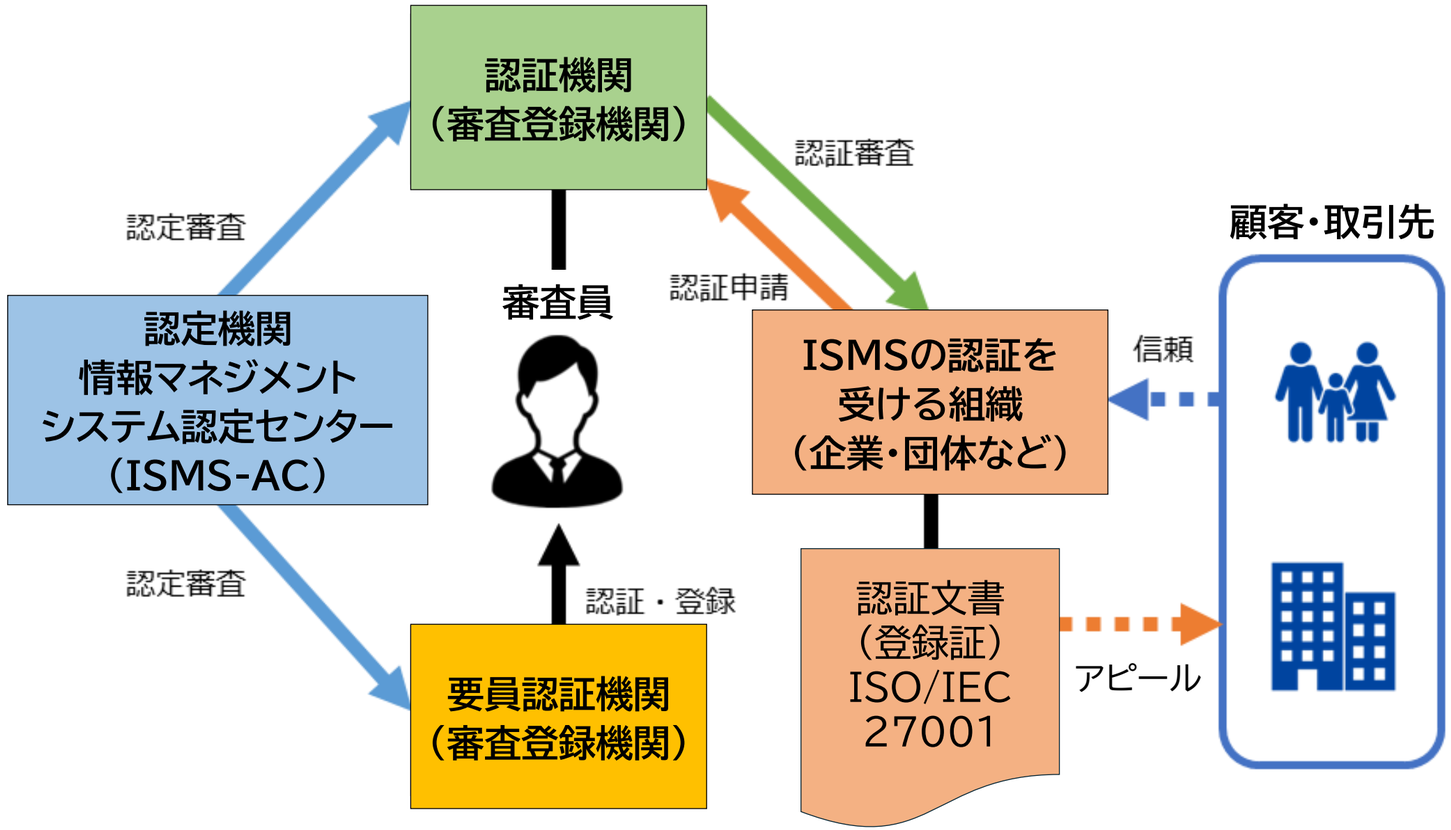
【参照:テキスト13-4-3.】
P239～P241

ISO/IEC27001の審査(第一段・第二段)

「ISMS認証」は、組織のISMSがISO/IEC 27001に準拠しているかを第三者認証機関が審査する制度。この評価は国際的な「ISMS適合性評価制度」のもとで行われる。

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
認証	第三者が文書で保証する手続き



ISO/IEC27001の審査準備と審査内容

【参照:テキスト13-4-3.】
P239～P241

ISO/IEC27001の審査(第一段・第二段)

ISMS認証審査プロセス

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診する場合は、申請が必要	組織と認証機関との間で、審査日程の確認を行う	新規の場合は原則として1次審査と2次審査の2回で実施される	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、登録完了となる	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページで公開される

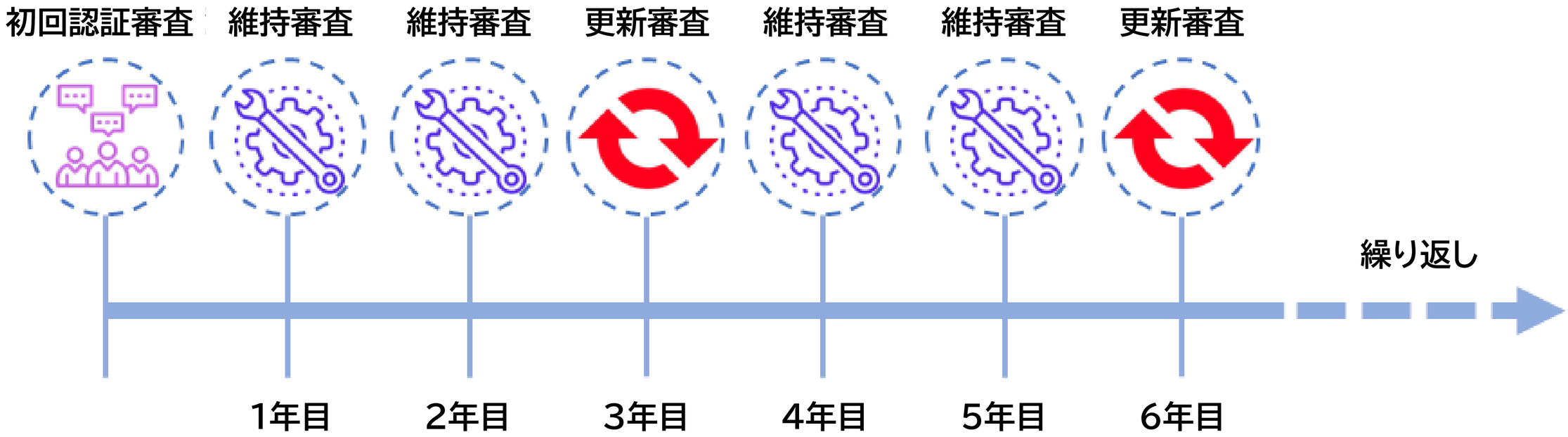
ISO/IEC27001の審査準備と審査内容

【参照:テキスト13-4-4.】
P241

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

- 年に1回以上の維持審査(サーベイランス審査)
- 3年ごとに認証の有効期限を更新するための更新審査



第14章. ISMSの管理策

管理策の分類と構成

管理策の分類と構成

【参照:テキスト14-1-1.】
P244

管理策:ISO/IEC 27002

ISO/IEC 27002:2013

- 情報セキュリティのための方針群
- 情報セキュリティのための組織
- 人的資源のセキュリティ
- 資産の管理
- アクセス制御
- 暗号
- 物理的及び環境的セキュリティ
- 運用のセキュリティ
- 通信のセキュリティ
- システムの取得、開発及び保守
- 供給者関係
- 情報セキュリティインシデント管理
- 事業継続マネジメントにおける情報セキュリティの側面
- 遵守

改訂

ISO/IEC 27002:2022

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

- 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

管理策の分類と構成

【参照:テキスト14-1-2.】
P245～P247

管理策のテーマと属性

カテゴリ	属性数	関連するガイドラインなど
管理策タイプ	3	―
情報セキュリティ特性	3	ISO/IEC 27001
サイバーセキュリティ概念	5	サイバーセキュリティフレームワーク
運用機能	15	ISO/IEC 27002:2022
セキュリティドメイン	4	―

各テーマより管理策の例示

- ISO/IEC 27002 附属書Aに記載
- 使い方は別紙、ISMS管理策の属性説明資料を参照

管理策の分類と構成

【参照:テキスト14-1-3.】
P247～P248

対策基準と実施手順の作成方法

1. 管理策の決定
   a. リスクアセスメント結果を考慮し、適切なリスク対応を選択する
   b. 実施に必要なすべての管理策を決定する

2. 管理策の検証
   a. 必要な管理策の見落としがないか検証する

3. 適用宣言書の作成
   a. 必要な管理策と実施する理由を記載する
   b. 管理策をすでに実施しているかを記載する
   c. 管理策を除外した理由を記載する

4. 実施手順の作成
   a. 具体的な実施手順を作成する

第15章. 組織的対策

作成する候補となる実施手順書類について

組織的対策として重要となる実施項目

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP256】

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、割り当てなければならない。
【実施手順：テキストP257～P258】

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。
【実施手順：テキストP258】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP258】

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。
【実施手順：テキストP258～P259】

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。
【実施手順：テキストP259～P260】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP264～P265】

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。
【実施手順：テキストP260】

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。
【実施手順：テキストP265】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP265～P266】

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。
【実施手順：テキストP266～P267】

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。
【実施手順：テキストP260～P261】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP261】

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。
【実施手順：テキストP261～P262】

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。
【実施手順：テキストP262～P263】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP263】

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。
【実施手順：テキストP263】

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。
【実施手順：テキストP264】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。【実施手順：テキストP272】

5.20 供給者と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。
【実施手順：テキストP272】

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。
【実施手順：テキストP273】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP276】

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。
【実施手順：テキストP267】

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。
【実施手順：テキストP268】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP268～P269】

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。
【実施手順：テキストP269】

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。
【実施手順：テキストP270】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP270】

5.29 事業の中断・阻害時の情報セキュリティ

事業の中断・阻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。
【実施手順：テキストP270～P271】

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。
【実施手順：テキストP271】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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、遵守しなければならない。
【実施手順：テキストP273～P274】

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。
【実施手順：テキストP274】

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。
【実施手順：テキストP274～P275】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP276】

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。
【実施手順：テキストP276】

作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P250～P277

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。
【実施手順：テキストP277】

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。
【実施手順：テキストP277】

第16章. 人的対策

作成する候補実施手順書類について

人的対策として重要となる実施項目

作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P279～P284

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。
【実施手順：テキストP281】

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。
【実施手順：テキストP281】

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。
【実施手順：テキストP282～P283】

作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P279～P284

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。
【実施手順：テキストP281～P282】

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。
【実施手順：テキストP282】

6.6 秘密保持契約又は秘密義務契約

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。
【実施手順：テキストP282】

作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P279～P284

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。
【実施手順：テキストP283】

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に報告できる仕組みを設けなければならない。
【実施手順：テキストP284】

第17章. 物理的対策

作成する候補実施手順書類について

物理的対策として重要となる実施項目

BYOD、MDM

作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P286～P294

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。
【実施手順：テキストP289】

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。
【実施手順：テキストP289】

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。
【実施手順：テキストP290】

作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P286～P294

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。
【実施手順：テキストP290】

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。
【実施手順：テキストP290～P291】

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。
【実施手順：テキストP291】

作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P286～P294

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。
【実施手順：テキストP291】

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。
【実施手順：テキストP291～P292】

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。
【実施手順：テキストP292】

作成する候補となる実施手順書類について

【参照:テキスト17-1、17-2】
P286～P294

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。
【実施手順:テキストP292～P293】

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。
【実施手順:テキストP293】

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。
【実施手順:テキストP293～P294】

作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P286～P294

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。
【実施手順：テキストP294】

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。
【実施手順：テキストP294】

BYOD、MDM

【参照:テキスト17-3-1.】
P295～P296

BYOD導入に向けて

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らない。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る。	**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る。
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る。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る。	**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、ウイルス感染や不正アクセスといった被害にあう可能性が高くなる。

BYOD, MDM

【参照:テキスト17-3-2.】
P296～P297

MDM導入のポイント

MDMを導入する際のポイント

ポイント	概要
コスト・費用	導入費用だけでなく、維持費がかかることを考慮する。
対応しているOSの確認	組織で利用しているPC、貸与しているスマホなど、組織が管理するデバイスのOSを確認する。
サポート体制	導入時や導入後の運用サポートの有無を確認する。
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る。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。

第18章. 技術的対策

作成する候補実施手順書類について
技術的対策として重要となる実施項目
実施手順を適用するセキュリティ概念
インシデント対応

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP305】

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。
【実施手順：テキストP306】

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。
【実施手順：テキストP306】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP306】

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。
【実施手順：テキストP307】

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。
【実施手順：テキストP307】

作成する候補となる実施手順書類について

【参照:テキスト18-1、18-2】
P299～P319

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。
【実施手順:テキストP308】

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。
【実施手順:テキストP308】

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。
【実施手順:テキストP309】

作成する候補となる実施手順書類について

【参照:テキスト18-1、18-2】
P299～P319

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。
【実施手順:テキストP309】

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。
【実施手順:テキストP309～P310】

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。
【実施手順:テキストP310】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP310】

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。
【実施手順：テキストP311】

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。
【実施手順：テキストP311】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP311～P312】

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。
【実施手順：テキストP312】

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。
【実施手順：テキストP312】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP312～P313】

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。
【実施手順：テキストP317～P318】

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。
【実施手順：テキストP318】

作成する候補となる実施手順書類について

【参照:テキスト18-1、18-2】
P299～P319

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。

【実施手順：テキストP318】

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。

【実施手順：テキストP318】

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。

【実施手順：テキストP319】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP313】

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。
【実施手順：テキストP313～P314】

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。
【実施手順：テキストP314】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。

【実施手順：テキストP314】

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。

【実施手順：テキストP315】

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。

【実施手順：テキストP315】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP315～P316】

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。
【実施手順：テキストP316】

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。
【実施手順：テキストP316～P317】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P299～P319

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。
【実施手順：テキストP317】

実施手順を適用するセキュリティ概念

【参照:テキスト18-3-1.】
P320～P323

Security by Design

デジタル・ガバメント推進標準ガイドラインにおける工程名	セキュリティ・バイ・デザインの工程名	概要
サービス・業務企画	セキュリティリスク分析	• システムのセキュリティリスクを特定し、リスク分析を実施する • リスク分析結果をもとにセキュリティ対応方針を決定する
要件定義	セキュリティ要件定義	• 機能面、非機能面で必要となるセキュリティ要件を明確にする
調達	セキュア調達	• セキュリティ仕様を満たす安全な製品やサービス、セキュリティ仕様を満たす能力を有した委託先を選定する
設計・開発	セキュリティ設計	• セキュリティを考慮したシステム設計を行う
	セキュリティ実装	• 設計に基づき、セキュリティ機能を実装する（セキュアコーディングやプラットフォームのセキュリティ設定の実施を含む）
	セキュリティテスト	• 実装されたセキュリティ対策が有効であることを確認する（脆弱性診断を含む）
サービス・業務の運営と改善	セキュリティ運用準備	• システム運用開始前に必要なセキュリティ運用体制と手順を整える
運用および保守	セキュリティ運用	• システム運用中のセキュリティを維持・管理する

導入のメリット

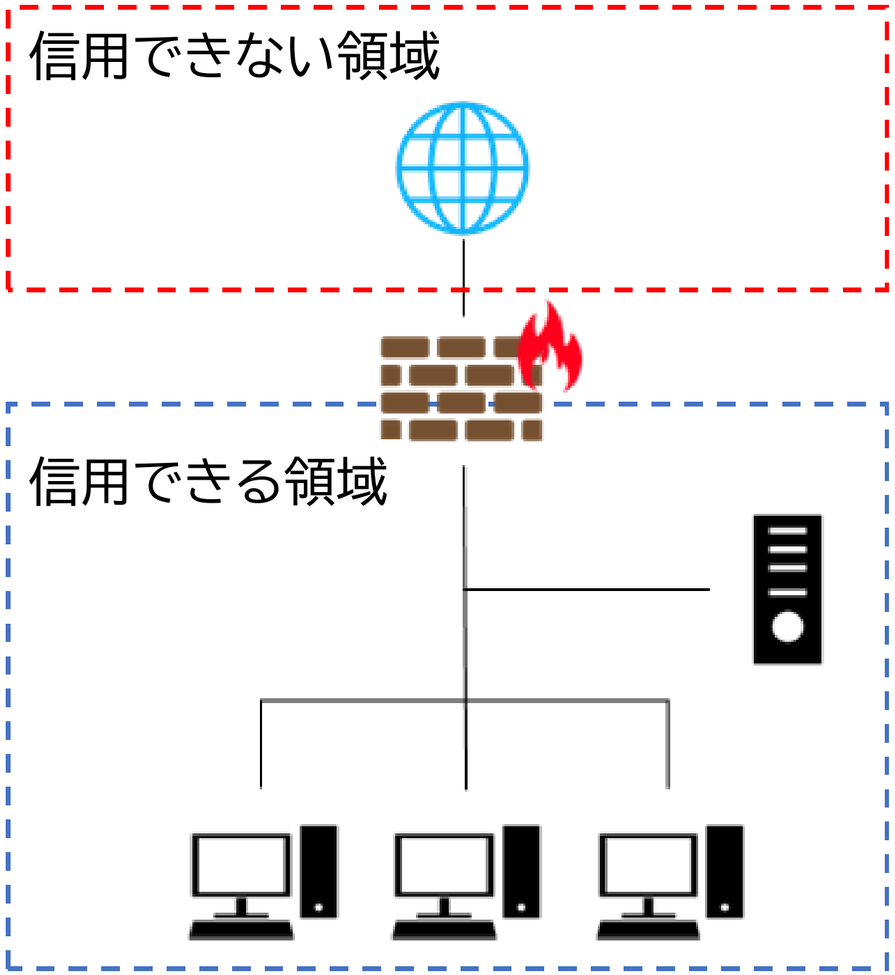
- 手戻りが少なくなり、納期を守れる
- コストを削減できる
- 保守性の高いソフトウェアができる（システムも同様）

ゼロトラスト、境界防御モデル

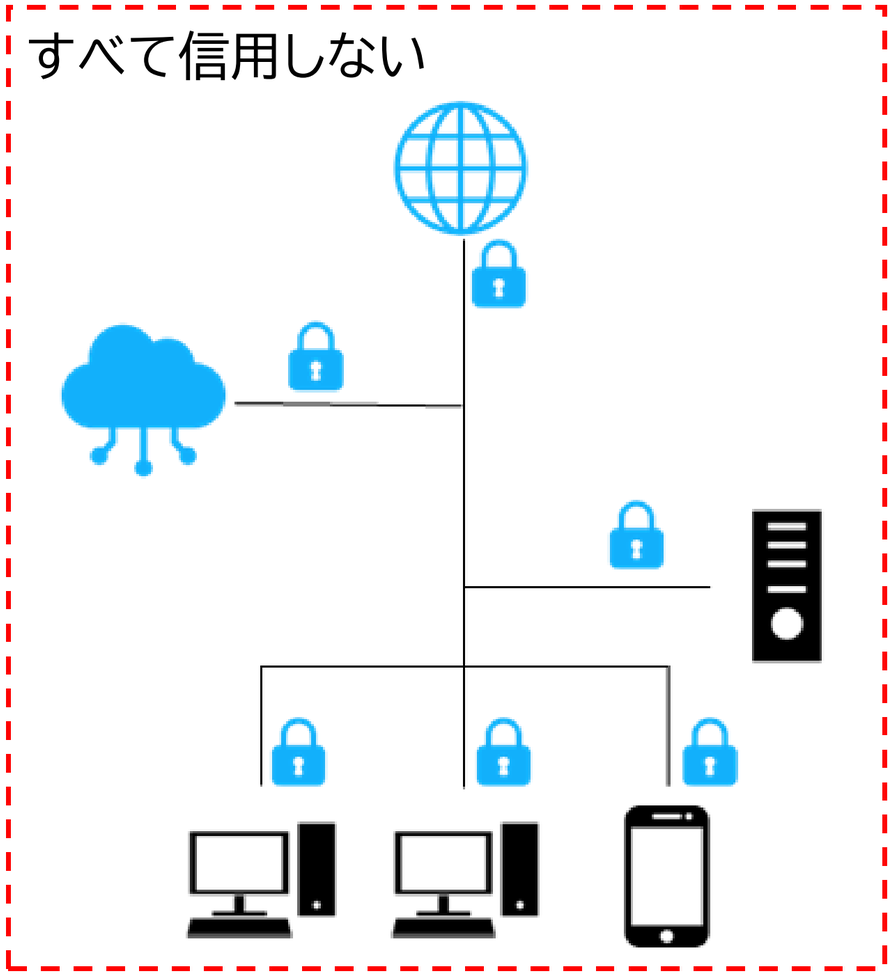
【参照:テキスト18-3-2.】
P324～P330

境界防御モデルとゼロトラストの違い

境界防御モデル



ゼロトラスト



ゼロトラスト導入に向けた進め方

【参照:テキスト18-3-2.】
P324～P330

① 企業のアクターを特定

② 企業が所有する資産を特定

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

④ ゼロトラスト導入候補の方針策定

⑤ ソリューション候補の特定

⑥ 初期導入とモニタリング

⑦ ゼロトラストの適用範囲拡大

ゼロトラストを実装するための主な技術要素

【参照：テキスト18-3-2.】
P324～P330

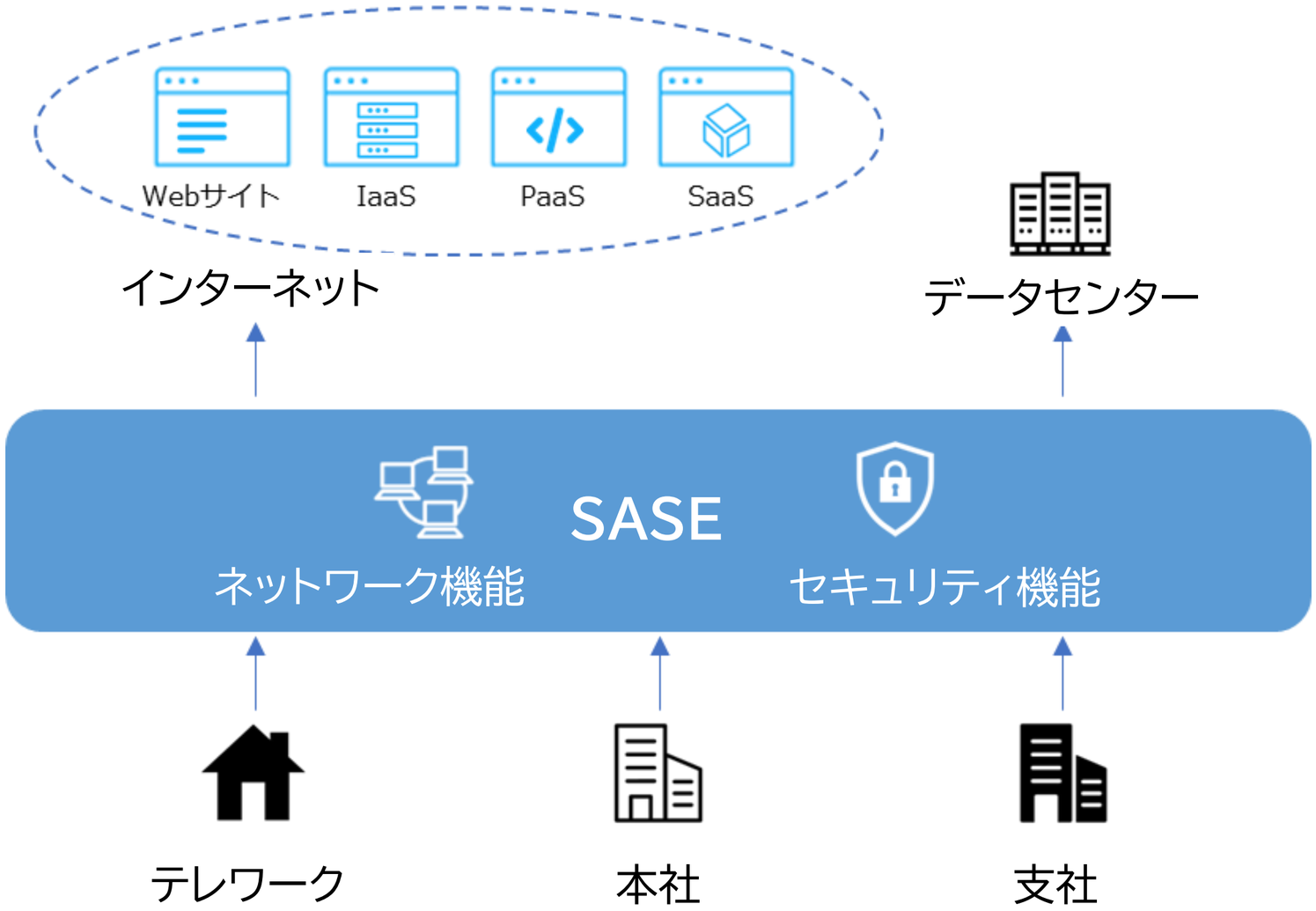
ゼロトラストを実装するために必要な技術要素

- CASB（Cloud Access Security Broker）
- SWG（Secure Web Gateway）
- ZTNA（Zero Trust Network Access）
- FWaaS（Firewall as a Service）
- SDP（Software Defined Perimeter）

ゼロトラスト、境界防御モデル

【参照：テキスト18-3-3.】
P330～P332

SASE

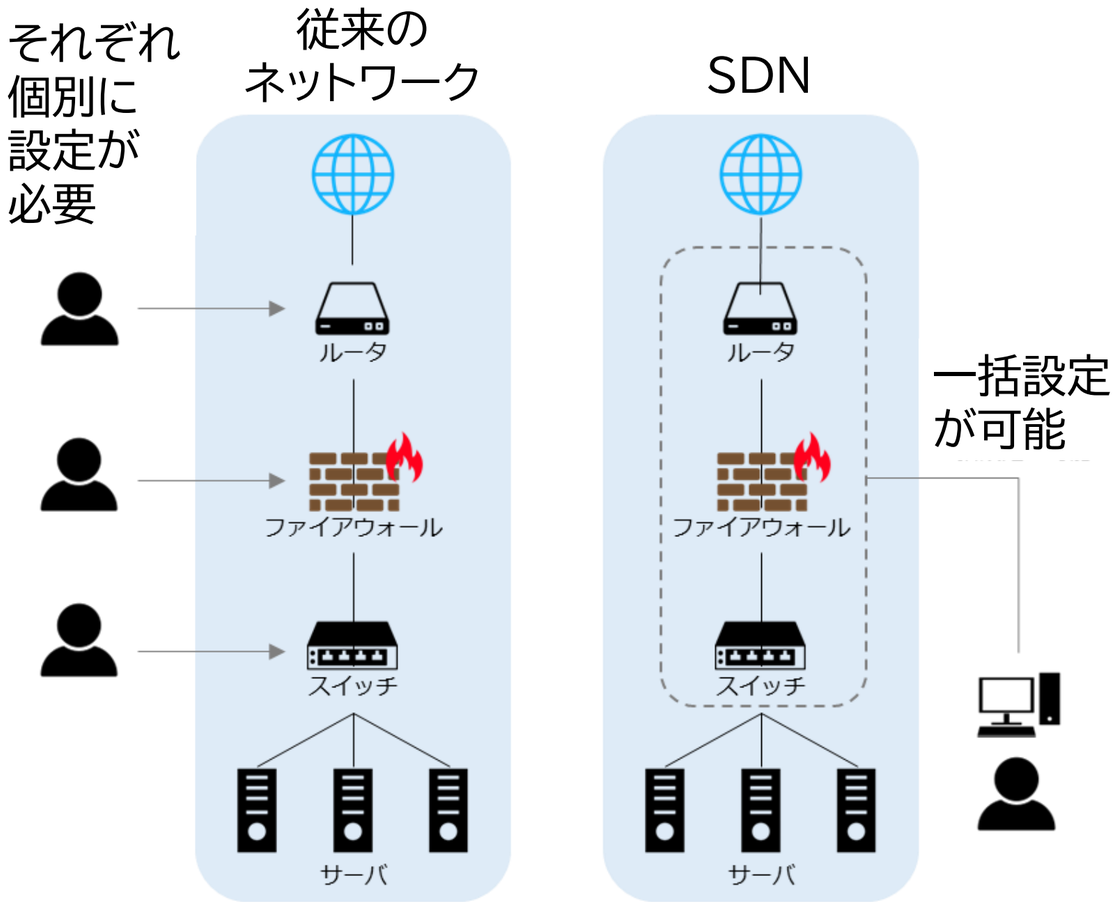


ネットワーク制御

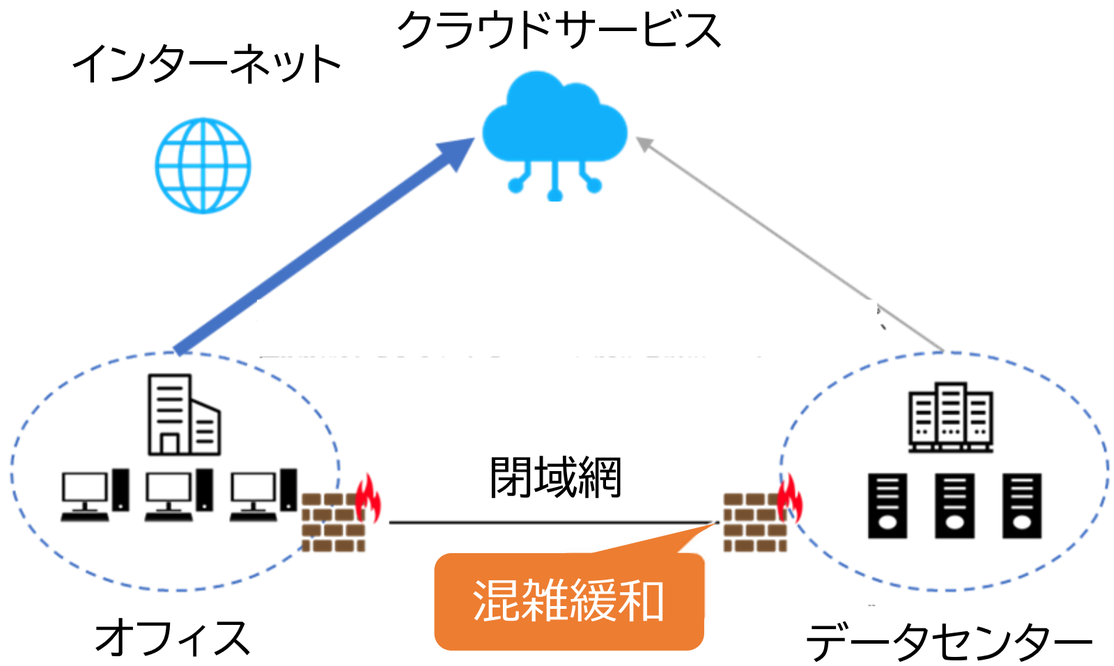
【参照:テキスト18-3-4.】
P333～P336

SDN、SD-WAN

SDN



SD-WAN



信頼できるクラウドサービスへは、データセンターを経由せず、直接接続することで、混雑を緩和します

セキュリティ統制（Security as a Service）

【参照：テキスト18-3-5.】
P336～P342

セキュリティ統制を確立するためのセキュリティ要素

- ネットワークセキュリティ
- デバイスセキュリティ
- アイデンティティセキュリティ
- ワークロードセキュリティ
- データセキュリティ
- 可視化と分析
- 自動化

インシデント対応

【参照:テキスト18-4.】
P343～P346

インシデント発生時の対応

1. 検知・初動対応
2. 報告・発表
3. 復旧・再発防止

フォレンジックの実施手順例

1. 発生したインシデントの内容把握
2. 発生したインシデントに関する対象物の決定
3. 証拠保全を行う上で必要な情報の収集

第19章. セキュリティ対策の有効性評価

内部監査

外部監査

内部監査

【参照:テキスト19-1.】
P348

内部監査は、組織の情報セキュリティ管理が規定通りに運用され、効果的に機能しているかを内部的に確認・評価するプロセスのこと。
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。

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の有効性の評価）	• ISMS有効性評価表
9.2 内部監査 （ISMSの適合性、有効性についての監査）	• 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の有効性を評価する）	• マネジメントレビュー報告書

外部監査

【参照:テキスト19-2.】
P349～P350

外部監査は、第三者機関が、組織の情報セキュリティ管理が国際基準や既定に適合し、適切に運用されているかを独立した視点で確認・評価するプロセスのこと。

管理基準・監査基準

- 情報セキュリティ管理基準
  - マネジメント基準
  - 管理策基準

- 情報セキュリティ監査基準
  - 一般基準
  - 実施基準
  - 報告基準

第20章. セキュリティ機能の実装と運用

セキュリティ機能の実装と運用

アジャイル開発

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン概要

政府情報システム全般に関するドキュメント

文書番号	タイトル
DS-100	デジタル・ガバメント推進標準ガイドライン
DS-110	デジタル・ガバメント推進標準ガイドライン解説書
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
DS-121	アジャイル開発実践ガイドブック
DS-130	標準ガイドライン群用語集

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン概要

セキュリティに関するドキュメント

文書番号	タイトル
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
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～
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
DS-203	政府情報システムにおけるサイバーセキュリティに係る サプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集
DS-210	ゼロトラストアーキテクチャ適用方針
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)

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン概要

セキュリティに関するドキュメント

文書番号	タイトル
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
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
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
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

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン概要

クラウドサービスに関するドキュメント

文書番号	タイトル
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

データ連携に関するドキュメント

文書番号	タイトル
DS-400	政府相互運用性フレームワーク（GIF）

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン概要

トラストに関するドキュメント7.02

文書番号	タイトル
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
DS-531	処分通知等のデジタル化に係る基本的な考え方

その他ドキュメント

文書番号	タイトル
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

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P354～P361

デジタル・ガバメント推進標準ガイドライン

1. プロジェクトの管理
2. 予算および執行
3. サービス・業務企画
4. 要件定義
5. 調達
6. 設計・開発
7. サービス・業務の運営と改善
8. 運用および保守
9. システム監査

プロジェクトの管理

【参照:テキスト20-1-2.】
P361～P368

プロジェクト管理活動の全体の流れ

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

プロジェクトの目標設定におけるポイント

- 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)

プロジェクトの管理

【参照:テキスト20-1-2.】
P361～P368

「KGI」「CSF」「KPI」の定義と関係

- 重要目標達成指標(KGI:Key Goal Indicator)
- 重要成功要因(CSF:Critical Success Factor)
- 重要成果指標(KPI:Key Performance Indicator)

セキュリティ機能を実装・運用するためのポイント

- 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
- 個人情報などの重要情報が漏えいするリスクへの対応

予算および執行

【参照:テキスト20-1-3.】
P368～P376

予算活動の全体の流れ

1. 予算のための稟議(予算要求)の事前準備
2. 見積り依頼
3. 見積りの精査
4. 予算のための稟議(予算要求)に必要な資料の準備
5. 概要要求に向けた調整
6. 予算執行について

セキュリティ機能を実装・運用するためのポイント

- 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
- 人事異動時の引続き不足を防ぐこと

サービス・業務企画

【参照:テキスト20-1-4.】
P376～P381

サービス・業務企画の全体の流れ

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

セキュリティ機能を実装・運用するためのポイント

- デジタル技術を徹底的に活用する

要件定義

【参照:テキスト20-1-5.】
P381～P389

要件定義の全体の流れ

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. 新しい非機能要件の定義
6. 要件定義終了後の対応

要件定義プロセスにおけるFit＆Gap分析

1. 業務要件の整理
2. パッケージソフトやSaaSの機能確認
3. フィット部分の特定（Fit）
4. ギャップ部分の特定（Gap）
5. コストとリスクの評価

要件定義

【参照:テキスト20-1-5.】
P381～P389

Fit＆Gap分析結果に基づく決定

決定	条件
そのまま導入	フィット部分が大きくカスタマイズ不要な場合
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ような場合

セキュリティ機能を実装・運用するためのポイント

- 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
- 想定されるリスクの概要と対策について
- 最低限記載すべき情報セキュリティ対策要件

調達

【参照:テキスト20-1-6.】
P389～P393

調達の全体の流れ

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

セキュリティ機能を実装・運用するためのポイント

- 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

設計・開発

【参照:テキスト20-1-7.】
P393～P402

設計・開発の全体の流れ

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

セキュリティ機能を実装・運用するためのポイント

- テスト計画の策定
- テストのレベルと種類
- テストツールの活用

サービス・業務の運営と改善

【参照:テキスト20-1-8.】
P402～P407

サービス・業務の運営と改善の全体の流れ

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

セキュリティ機能を実装・運用するためのポイント

- 業務を外部委託する際の注意
- インシデントの優先度づけ

運用および保守

【参照:テキスト20-1-9.】
P407～P415

運用および保守の全体の流れ

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・保守の定着と次の備え
4. 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・運用するためのポイント

- セキュリティ関連作業を定期的に確実に実施すること
- セキュリティ対策会議の実施
- 情報システムのアカウントの管理

システム監査

【参照:テキスト20-1-10.】
P415～P418

システム監査の全体の流れ

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

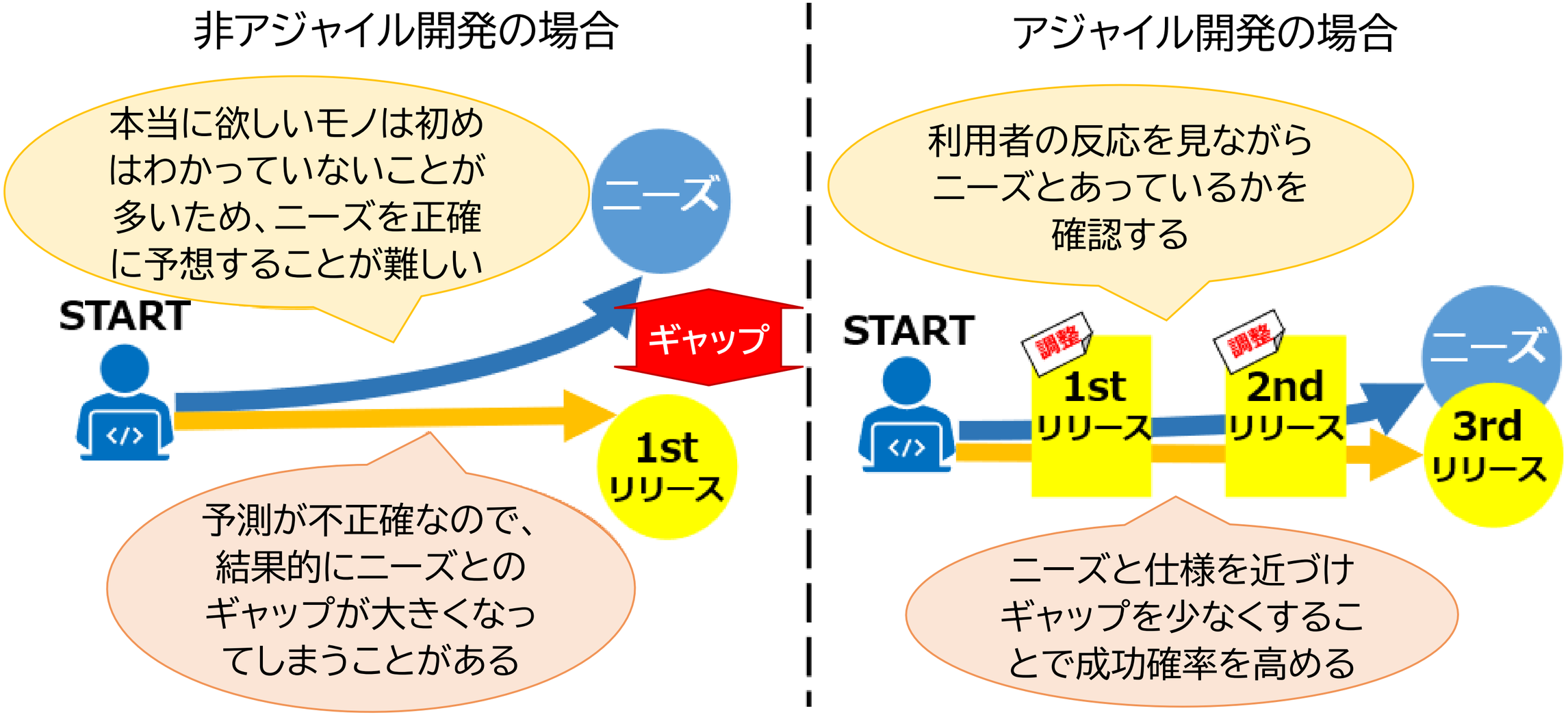
セキュリティ機能を実装・運用するためのポイント

- 情報セキュリティ監査

アジャイル開発

【参照:テキスト20-2-1.】
P419～P420

アジャイル開発の概要

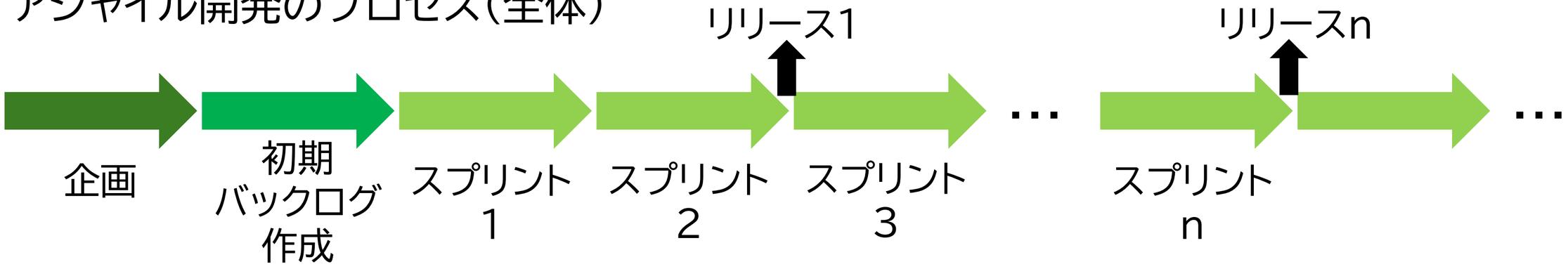


アジャイル開発

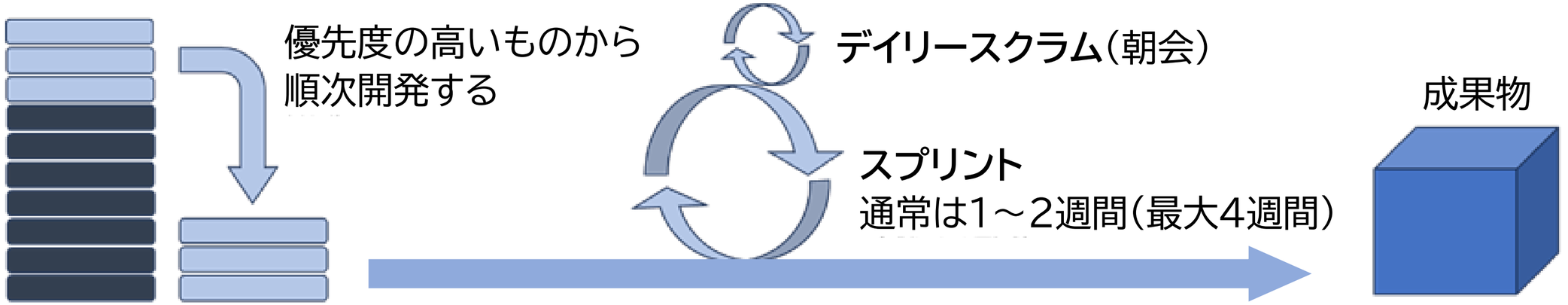
【参照:テキスト20-2-2.】
P420～P422

アジャイル開発の実施ポイント

アジャイル開発のプロセス(全体)



アジャイル開発のプロセス(イテレーション)



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

ECサイトの構築とセキュリティ機能の実装と運用

ECサイトの構築とセキュリティ機能の実装と運用

【参照:テキスト21-1.】
P424～P425

ECサイト導入における全体概要

デジタル・ガバメント推進標準ガイドラインに準拠させた場合

ステップ	概要
1.　サービス・業務企画	事業目的とサービスの具体的な方向性を決める
2.　要件定義	サービスの実現に必要な機能／非機能の要件を定義する
3.　調達	開発に必要なリソースの調達
4.　設計・開発	プロジェクトの計画立案と管理
5.　サービス・業務の運営と改善	運営しながら改善
6.　運用および保守	安定稼動の維持と継続的改善

※セキュリティ要件は、「要件定義」のフェーズで決定する。

サービス・業務企画

【参照:テキスト21-1-1.】
P425～P429

利用者視点でのニーズ把握

ペルソナ分析を活用し、仮想顧客の特徴を具体化することで、利用者が抱える課題等を浮き彫りにし、具体性の高いアイデアを創出する。

ペルソナ分析を活用した、サービス・業務企画のステップ

1. ターゲットとなる利用者に関する情報を収集する
2. 収集した情報を分析し、グルーピングする
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
4. 業務の現状把握
5. サービス・業務企画内容の検討

サービス・業務企画

【参照：テキスト21-1-1.】
P425～P429

業務の現状分析とフロー作成の重要性

現状把握の目的

複数の関係者が理解しやすい形で業務の状況を共有する。

業務フローとは

誰が、何を、どの順番で実施しているかを視覚的に示すツール

- 現行フロー（AsIs）：現在の業務内容を可視化
- 将来フロー（ToBe）：企画後の業務の変化点を明記
- ポイント：関係者にわかりやすい形式で表記する

業務フローの例：

1. 実店舗での購入フロー（テキスト P428 図83 参照）
2. ECサイトでの購入フロー（テキスト P429 図84 参照）

要件定義

【参照:テキスト21-1-2.】
P429～P475

一貫性を持った要件定義書の作成

- プロジェクト管理や契約合意の基盤となる。
- 誤った定義や曖昧な表現は後続工程に重大な影響が出る。

要件定義のポイント

- 用語の統一
- 業務要件の整合性
- 箇条書きで簡潔に

機能要件の定義

- 機能
- 画面
- 帳票
- データ
- 外部インターフェース

要件定義

【参照:テキスト21-1-2.】
P429～P475

機能に関する事項

- 機能とは、システムが何をしてくれるか。

＜テキスト P430 参照＞

画面に関する事項

- 画面とは、システムとやり取りをするための「窓口」のこと。

＜テキスト P431 参照＞

帳票に関する事項

- 帳票とは、システムから出力される書類のこと。

＜テキスト P431 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

データに関する事項

- データとは、システムが扱う情報のこと。

＜テキスト P432 参照＞

外部インターフェースに関する事項

- 外部インターフェースとは、システム同士が連携し情報をやり取りする仕組みのこと。

＜テキスト P432～433 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

非機能要件の定義

- 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
- データマネジメントに関する事項
- 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

要件定義

【参照:テキスト21-1-2.】
P429～P475

情報セキュリティに関する事項

- 情報セキュリティとは、システムに保存されたデータや情報を守るための仕組みやルールのこと。
- セキュリティ要件の決める流れ
  1. リスクアセスメントを実施する。
  2. 必要な管理策を決定する。
  3. セキュリティ要件を決める。
     - IPAが提供しているガイドラインでは、次の3つのレベルで定めている。
       1. 必須
       2. 必要
       3. 推奨
- セキュリティ対策要件(構築時)は、テキスト P436～P444 参照。

※ P442 要件6.中の「クレジットカード・セキュリティガイドライン」がVer6.0に改訂されました。
変更点:EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施など(2025/03/05)

要件定義

【参照:テキスト21-1-2.】
P429～P475

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？

- 使いやすさのこと。

アクセシビリティとは？

- 誰でも目的の情報にたどり着けるか。

＜テキスト P445 参照＞

システム方式に関する事項

システム方式とは？

- システムがどのように動作するか、そのために必要なツールや技術をどう使うかを決めるもの。

＜テキスト P445～446 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

規模に関する事項

規模とは？

- システムがどれくらいのユーザーに使われるか。
- どれくらいの情報量を扱うか。

＜テキスト P446 参照＞

性能に関する事項

性能とは？

- システムが快適に利用できるか。

＜テキスト P447 参照＞

信頼性に関する事項

信頼性とは？

- システムがどれだけ安定して動くか。

＜テキスト P447～448 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

拡張性に関する事項

拡張性とは？

- 性能低下を感じた時に、どのように拡張を実施し、性能を確保するか。

＜テキスト P448 参照＞

上位互換性に関する事項

上位互換性とは？

- ソフトウェアの新しいバージョンが、古いバージョンの機能やデータを問題なく使えるか。

＜テキスト P448～449 参照＞

中立性に関する事項

中立性とは？

- システムが特定の会社や製品に依存しないようにすること。

＜テキスト P449～P450 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

継続性に関する事項

継続性とは？

- システムが問題や災害が起こったときにも、できるだけ早く復旧して再び使えるようにするための能力のこと。

＜テキスト P450 参照＞

情報システム稼働環境に関する事項

情報システム稼働環境とは？

- システムが実際に動くために必要なすべての要素のこと。

＜テキスト P450～451 参照＞

テストに関する事項

テストとは？

- システムが設計通りに動作するか、不具合がないかチェックすること。

＜テキスト P451～452 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

移行に関する事項

移行とは？

- 現在使っているシステムやデータを新しいシステムに引き継いで移動させる作業のこと。

＜テキスト P452 参照＞

引継ぎに関する事項

引継ぎとは？

- 現在の担当者や事業者が行っている作業や業務を、次の担当者や事業者にスムーズに渡すための作業のこと。

＜テキスト P453～454 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

教育に関する事項

教育とは？

- システムの利用者がそのシステムを正しく理解し、効率的に使うために行う研修やトレーニングのこと。

＜テキスト P454～P455 参照＞

運用に関する事項

運用とは？

- 情報システムが常に正常に動き続けるように維持・管理すること。

＜テキスト P455～461 参照＞

保守に関する事項

保守とは？

- システムの現状の機能を維持しつつ問題を修正する作業のこと。

＜テキスト P461～462 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

SaaS型サービスの選定基準と利用時に必要となる対策

SaaS型サービスとは？

- SaaS（Software as a Service）は、インターネットを通じて使うソフトウェアのことです。

＜テキスト P462 参照＞

Fit&Gap 分析

Fit&Gap分析とは？

- SaaSやパッケージソフトを導入する際に、自社の業務要件にどれだけ合っているかと、どこが合わないかを認識するためのプロセスのこと。

＜テキスト P462～P463 参照＞

要件定義

【参照:テキスト21-1-2.】
P429～P475

Fit&Gap分析の実施方法(例)

1. 現状分析
   ＜テキスト P464 参照＞
2. SaaS,パッケージソフトウェアの機能調査
   ＜テキスト P464～467 参照＞
3. 比較分析
   ＜テキスト P465～471 参照＞
4. ギャップへの対応検討
   ＜テキスト P471～472 参照＞
5. 費用対効果の分析
   ＜テキスト P472～473 参照＞
6. 実施計画の策定
   ＜テキスト P473 参照＞

調達

【参照:テキスト21-1-3.】
P475～P480

調達仕様書の作成方法

- 調達仕様書とは？
  プロジェクトに必要な製品やサービスを外部の事業者から調達するときに、発注者側（自分たち）が何を求めているか、どんな条件があるかを詳しくまとめたドキュメントのこと。

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

1. 調達の意図や目的を正しく伝える
2. 作業内容・納品物を関連付けて網羅的に記載する
3. 外部事業者の具体的な作業内容を明確にする
4. 作業の実施体制を明確にする
5. 成果物の取扱いに注意する（知的財産権）
6. 再委託に関する事項を定める
7. 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

【参照:テキスト21-1-3.】
P475～P480

適正な価格で最適な業者の選定

- 調達仕様書の明確化
- 透明性と公平性の維持
- 複数の見積り取得

3点見積りとは

プロジェクトやタスクの時間やコストを予測するための方法の一つ。
3つの異なるシナリオに基づいて予測を行います。それぞれのシナリオは以下の通り

シナリオ	概要
楽観値	最も良い条件がそろった場合の最低コスト
最頻値	一般的な条件で進行した場合の予測コスト
悲観値	最悪の状況が発生した場合の最高コスト

設計・開発

【参照:テキスト21-1-4.】
P480～P483

設計・開発の計画

- 「設計・開発実施要領」の作成
- 「設計・開発実施計画書」の作成

＜テキスト P481～482 参照＞

設計・開発・テストの管理

- 単体テスト
- 結合テスト
- 総合テスト
- 受入テスト

＜テキスト P482～P483 参照＞

サービス・業務の運営と改善

【参照:テキスト21-1-5.】
P483～P488

業務の定着と次の備え

業務の定着とは？

- 新しい情報システムが導入された後、そのシステムを実際の業務でスムーズに使えるようにすること。
- システムのリリースが近づいたら、従業員向けに教育を行い、業務マニュアルを使ってシステムの使い方や業務の流れなどの説明を実施する。

＜テキスト P483～P486 参照＞

業務の改善

業務の改善とは？

- サービスや業務を運営していく中で発生する問題や新しい情報をもとに、より良い運営方法を見つけていくプロセスのこと。

＜テキスト P486～488 参照＞

運用および保守

【参照:テキスト21-1-6.】
P488～P491

運用・保守の計画

運用・保守の計画とは？

- システムが安定して動作し続けるように、日々の運用や修理・メンテナンスをどう進めるかを決める計画のこと。

＜テキスト P488～489 参照＞

運用・保守の改善と業務の引継ぎ

運用・保守の改善とは？

- システムやその運用方法をより効率的に、より安全にするための取り組みのこと。

＜テキスト P489～P491 参照＞

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

デジタルスキル標準（DSS）

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（iCD）

デジタルスキル標準（DSS）

【参照:テキスト22-1.】
P494

デジタルスキル標準

DXリテラシー標準

以下の指針および、それぞれの指針において学習が期待される項目　（学習項目例）を定義している。

- DXに関するリテラシーとして身につけるべき知識の学習の指針
- 個人が自身の行動を振り返るための指針かつ、組織・企業が構成員に 求める意識・姿勢・行動を検討する指針

DX推進スキル標準

DX推進に必要な人材類型（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）について 類型ごとに、ロールおよび必要なスキルを定義している。

DXリテラシー標準（DSS-L）

【参照：テキスト22-1-1.】
P494～P502

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付けることで、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）

社会の変化
顧客価値の変化
競争環境の変化

What（DXで活用されるデータ・技術）

データ	社会におけるデータ
	データを読む・説明する
	データを扱う
	データによって判断する
デジタル技術	AI
	クラウド
	ハードウェア・ソフトウェア
	ネットワーク

How（データ・技術の利活用）

活用方法・利用方法
- データ・デジタル技術の活用事例
- ツール利用

留意点
- セキュリティ
- モラル
- コンプライアンス

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

DXリテラシー標準（DSS-L）

【参照：テキスト22-1-1.】
P494～P502

学習のゴール

要素	ゴール
マインド・スタンス	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
Why DXの背景	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こと
What DXで活用されるデータ・技術	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こと
How データ・技術の利活用	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こと

DX推進スキル標準（DSS-P）

【参照：テキスト22-1-2.】
P502～P509

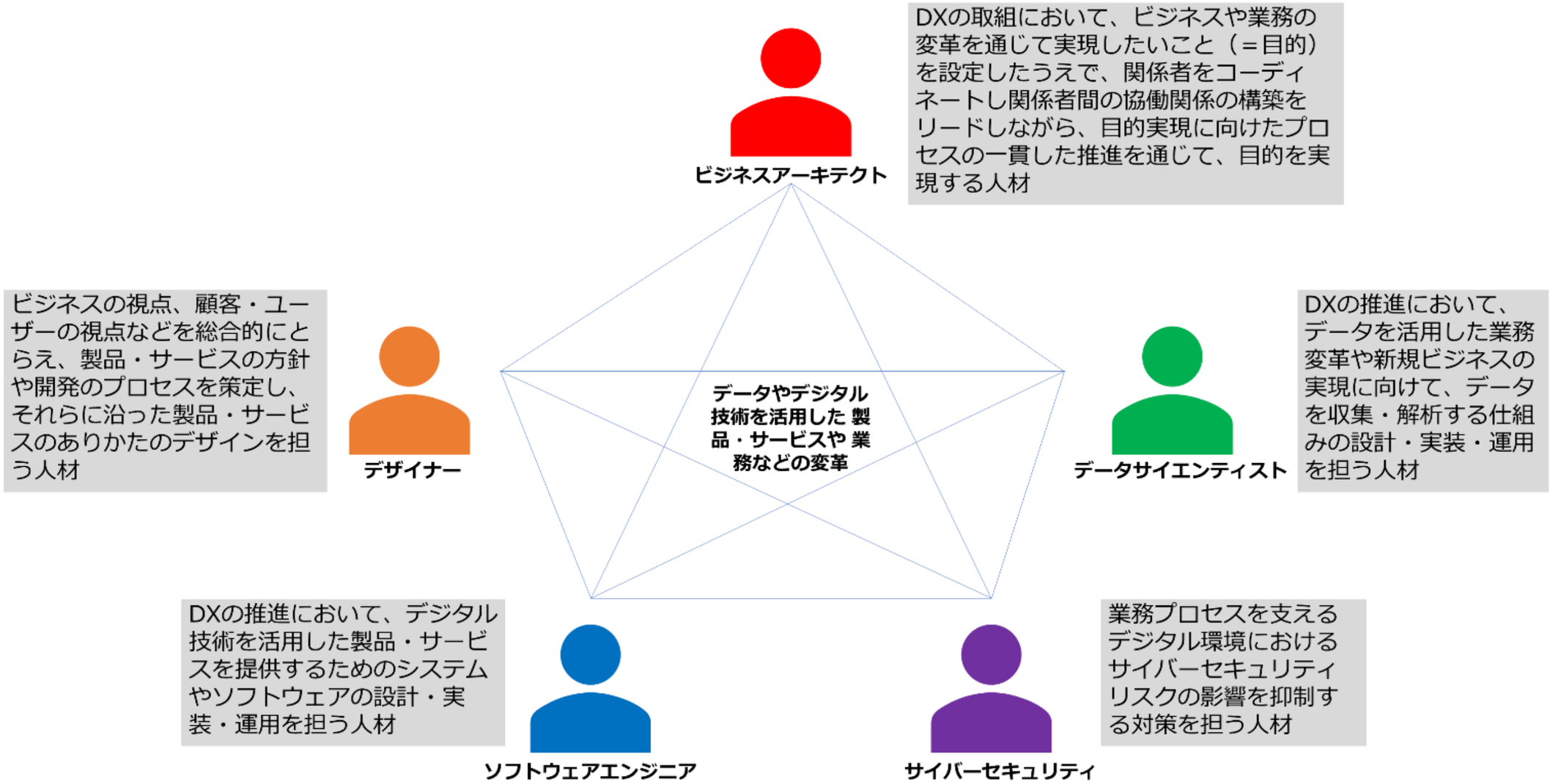
人材類型	ビジネスアーキテクト			デザイナー			データサイエンティスト			ソフトウェアエンジニア				サイバーセキュリティ	
ロール （DXの推進において担う責任、主な業務、必要なスキルにより定義）	ビジネスアーキテクト（新規事業開発）	ビジネスアーキテクト（既存事業の高度化）	ビジネスアーキテクト（社内業務の高度化・効率化）	サービスデザイナー	UX／UIデザイナー	グラフィックデザイナー	データビジネスストラテジスト	データサイエンスプロフェッショナル	データエンジニア	フロントエンドエンジニア	バックエンドエンジニア	クラウドエンジニア／SRE	フィジカルコンピューティングエンジニア	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

共通スキルリスト	
	ビジネスイノベーション
	データ活用
	テクノロジー
	セキュリティ
	パーソナルスキル

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

DX推進スキル標準（DSS-P）

【参照：テキスト22-1-2.】
P502～P509



DX推進スキル標準（DSS-P）

【参照：テキスト22-1-2.】
P502～P509

生成AIに関する事項

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

具体的

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

ITスキル標準（ITSS）

【参照：テキスト22-2-1.】
P510

ITスキル標準

1部：概要編
適用範囲・基本構造・構成要素解説

2部：キャリア編
キャリアフレームワーク・職種の概要・達成度指標

3部：スキル編
スキルディクショナリ・スキル領域・スキル熟達度・研修ロードマップ

附属書
対象・目的別にITスキル標準を活用するための資料を体系化

ITスキル標準センターで内容に責任を持つ範囲

ITスキル標準（ITSS）

【参照：テキスト22-2-2.】
P511～P516

キャリア

IT人材の成長や評価を行うための3つのポイント

1. **キャリアフレームワーク**
   職種ごとにレベルが分かれており、全11種類と35の専門分野がある
   ＜テキスト P511～P512 参照＞

2. **職種の概要**
   それぞれの職種がどんな仕事かの説明
   ＜テキスト P512～514 参照＞

3. **達成度指標**
   各人の経験や実績に基づいて7段階に評価する
   ＜テキスト P514～P515 参照＞

ITスキル標準（ITSS）

【参照：テキスト22-2-3.】
P516～P519

スキル

IT人材が必要とする能力や技術。

1. **スキルディクショナリ**
   ITスキル標準で定義されたすべてのスキルや知識を網羅している

2. **スキル領域とスキル熟練度**
   職種ごとにスキルや知識の整理を行い、それぞれのレベルを示している

3. **研修ロードマップ**
   職種ごとに必要なスキルを習得するための研修科目を明示している

ITSS＋（プラス）

【参照：テキスト22-3.】
P520～P530

従来のITスキル標準（ITSS）を拡張し、第4次産業革命に向けられ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た。

1. **データサイエンス領域**
   大量のデータを分析し、その結果を仕事で活用するために必要なタスクやスキルをまとめたもの
   ＜テキスト P520～P523 参照＞

2. **アジャイル開発領域**
   アジャイル開発のスキルを高めるための分野
   ＜テキスト P523～P524 参照＞

ITSS＋（プラス）

【参照：テキスト22-3.】
P520～P530

従来のITスキル標準（ITSS）を拡張し、第4次産業革命に向けられ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た。

3. IoTソリューション領域
IoT技術に必要なスキルを高めるための分野
＜テキスト P524～P525 参照＞

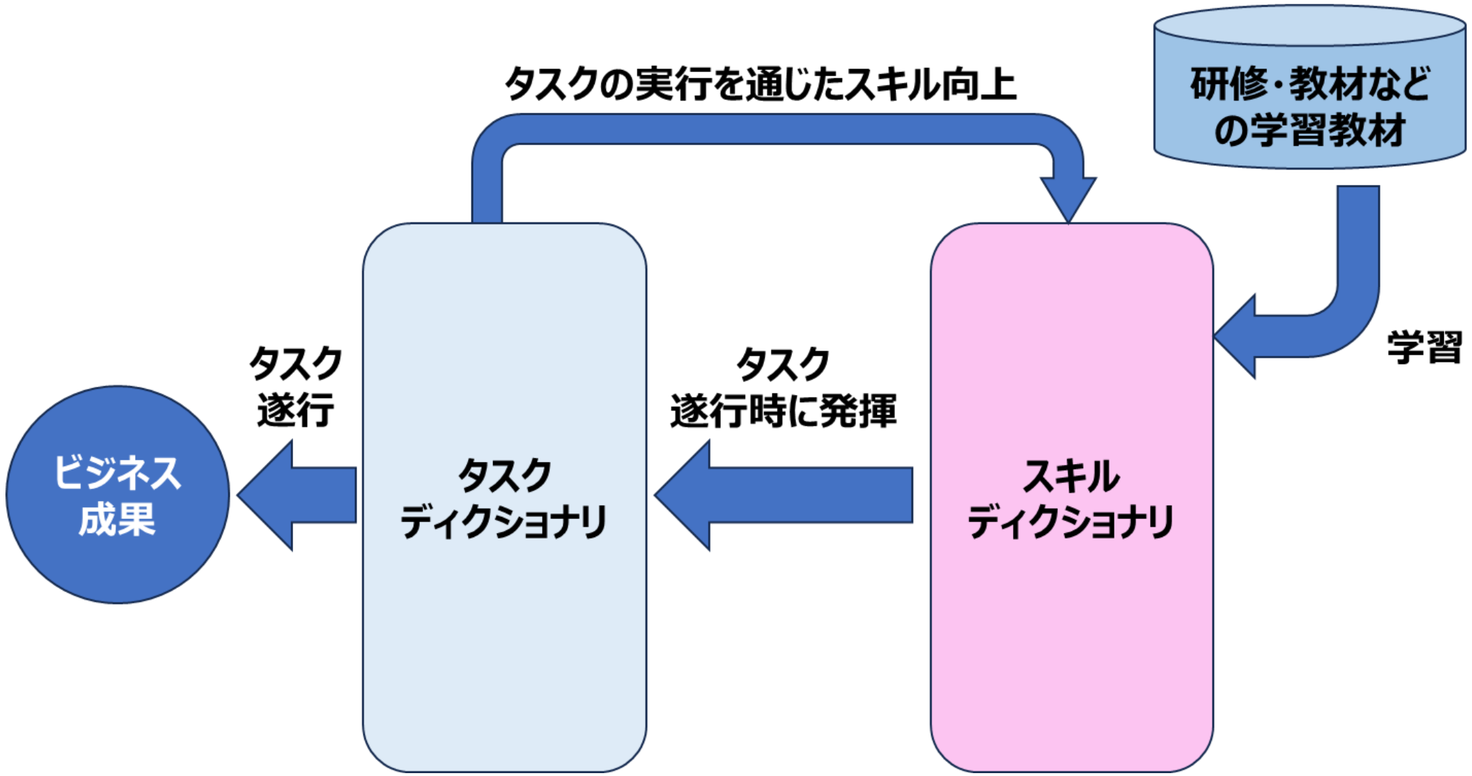
4. セキュリティ領域
企業のセキュリティ対策に必要なスキルや知識を整理・評価するための枠組み
＜テキスト P525～P530参照＞

iコンピテンシ ディクショナリ(iCD)

【参照:テキスト22-4.】
P531～P536

iコンピテンシ ディクショナリの考え方

- 企業やIT技術者が人材育成やスキル向上のために使うツール。
- 「タスクディクショナリ」(仕事の一覧)と「スキルディクショナリ」(必要なスキルの一覧)で構成されている。



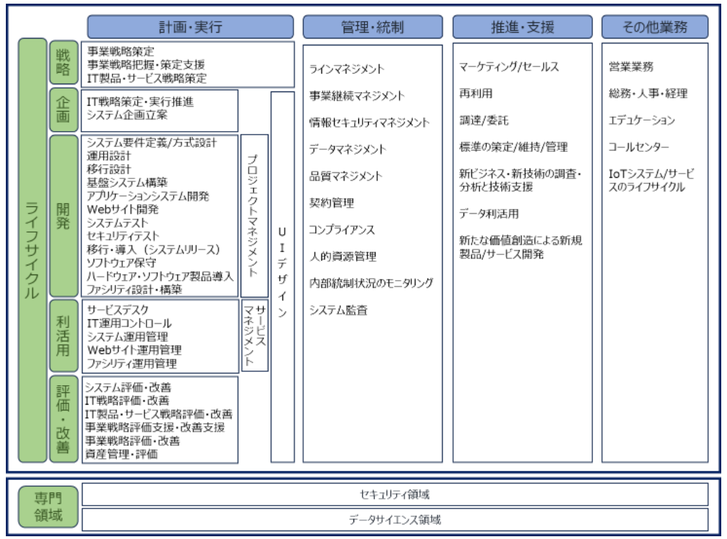
iコンピテンシ ディクショナリ(iCD)

【参照:テキスト22-4.】
P531～P536

「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全体像

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	評価項コード	評価項目
ST01	事業戦略策定	ST01.1	事業環境の分析	ST01.1.1	経営方針の確認	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	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	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
				ST01.1.2	外部環境の分析	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	自社が所属する業界や自社製品・サービスの市場規模および今後の見通しを調査、把握する
						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
				ST01.1.3	内部環境の分析	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	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	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	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	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

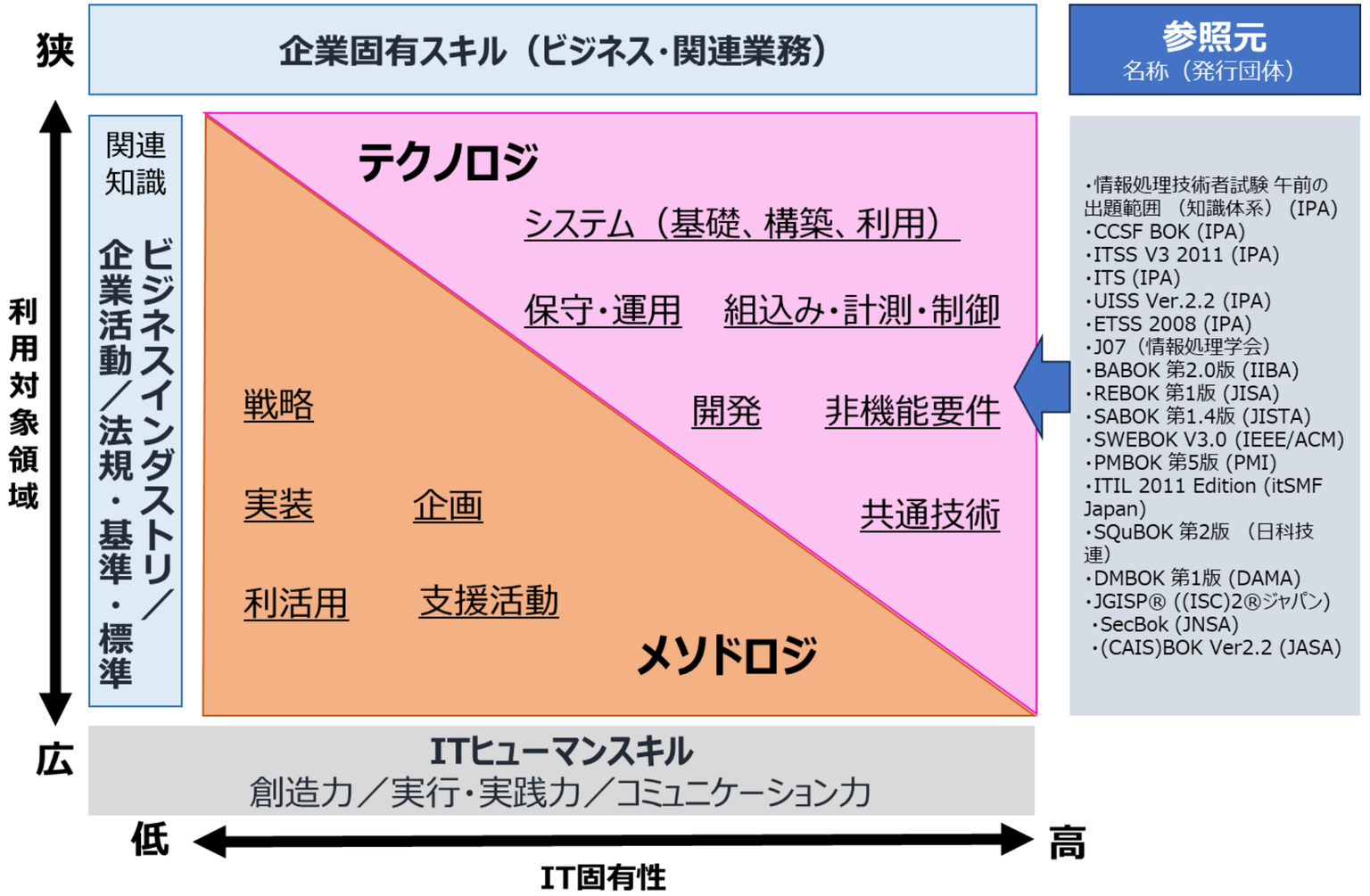
タスクプロフィール種別	タスクプロフィール種別の説明	タスクプロフィールグループ	タスクプロフィールコード	タスクプロフィール	タスクプロフィールの説明
ビジネスタイプ別	組織の立場（ユーザ、ベンダ）や業態によって必要なタスクを識別するもの。 ◎：必要なタスク ○：必要だが、他部門やアウトソースへの委託等が可能なタスク	-	A-010-010	自社向け情報システム開発・保守・運用	自社向けシステムの開発・保守・運用を担う部門（IT/非IT企業の情報システム部門）に関連するタスク
			A-010-020	システム受託開発	アプリケーションシステムおよび基盤システムの受託開発を担う企業に関連するタスク
			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	組込みソフトウェア開発	組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

iコンピテンシ ディクショナリ(iCD)

【参照:テキスト22-4.】
P531～P536

「スキルディクショナリ」の考え方



iコンピテンシ ディクショナリ(iCD)

【参照:テキスト22-4.】
P531～P536

iコンピテンシ ディクショナリ(iCD)の利活用の形態

企業・組織での利活用
ITベンダー
ユーザ企業

タスクディクショナリ

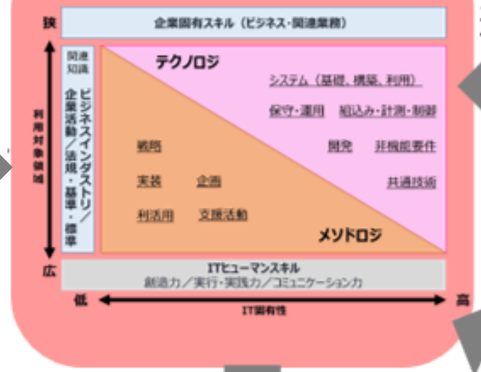
活用

企業のタスク一覧

タスク大分類	タスク中分類	タスク小分類
顧客の事業戦略把握	要求（構想）の確認	・・・
		・・・
IT製品・サービス戦略策定	市場動向の調査・分析・予測	・・・
		・・・
	IT製品・サービス戦略の策定	・・・
		・・・
		・・・

連携

スキルディクショナリ



連携

活用

IT技術者のスキル一

スキル分類	スキル項目	知識項目
（システム）ソフトウェアの基本技術	ソフトウェア構築の基礎知識	・・・
	ソフトウェア設計の基礎知識	・・・
	プログラミング	・・・
（システム）ソフトウェアの構築技術	システム開発の概念と方法論	・・・
	システム開発のアプローチ	・・・

連携

教育プログラム

コース分類	コース名	概要	関連知識項目
ソフトウェア基礎技術	ソフトウェア 基礎	システム開発に携わる 上での基礎知識を習得。また、開発工程…	形式構築法(formal construction methods)、…
	プログラミング入門	プログラムを作成するにあたり必要な基本文 法（変数、配列、…	WindowsとUnixオペレーティングシステム、アルゴリズムの…
	オープンソー スソフトウェア入門	Linux上でApache、MySQL、PHPを利用し、…	LAMP／LAPP、OSSの 種類と特徴、OSSの利 用・活用と考慮点 …
ソフトウェア構築技術	システム開発 の基礎	集中処理方式、クライアントサーバ処理方式、Webシステム…	エンドユーザ開発のシステム、オブジェクト 指向開発技術、…

IT資格・試験

スキル分類	スキル項目	資格試験 ○○試験	△△試験	□□試験
（システム）ソフトウェアの基礎知識	ソフトウェア構築の基礎知識	○		
	プログラミング	○		
	オープンソフトウェア		○	
（システム）ソフトウェアの構築技術	システム開発のアプローチ		○	

個人での利活用
（IT技術者、学生）

学校等教育機関での利活用

第23章. 人材の知識とスキルの認定制度

Di-Lite

情報処理技術者試験

国際セキュリティ資格

Di-Lite

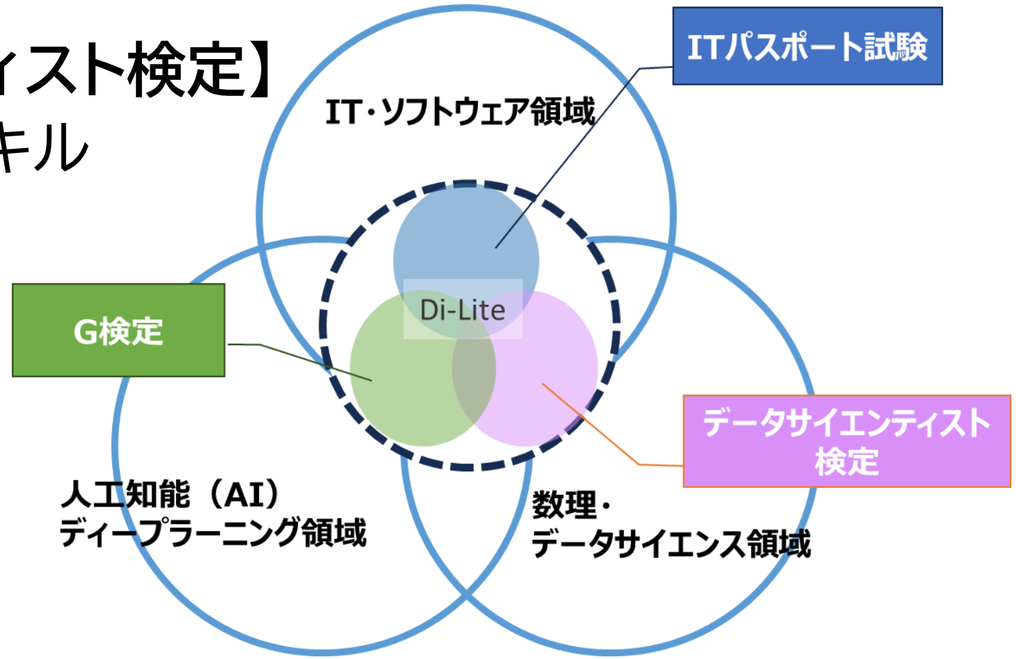
【参照:テキスト23-1.】
P538～P548

デジタル時代を生き抜くための基礎的なスキルセットで、3つの領域を指す

1. **IT・ソフトウェア領域【ITパスポート試験】**
   PCやスマートフォンや、ソフトウェアの使い方に関するスキル
   ＜テキスト P540～545 参照＞

2. **数理・データサイエンス領域【データサイエンティスト検定】**
   データ分析や、統計の基本を理解するためのスキル
   ＜テキスト P545～546 参照＞

3. **AI・ディープラーニング領域【G検定】**
   AI（人工知能）技術の基本的な仕組みや
   考え方を理解するための知識
   ＜テキスト P547～548 参照＞



情報処理技術者試験

【参照：テキスト23-2.】
P549～P559

安全なIT利活用には組織内で業務に携わる全員のIT知識が必要であり、IT知識を身につけてもらうための有効な手段の一つ

- **情報セキュリティマネジメント試験（SG）**
  部門の情報セキュリティを理解し、維持改善する実務リーダー
  ＜テキスト P552～553 参照＞

- **基本情報技術者試験（FE）**
  ITサービスやソフト開発の基礎知識と実践力を備えた人材
  ＜テキスト P553～554 参照＞

- **応用情報技術者試験（AP）**
  高度IT人材として応用的知識と技能を備えた人材
  ＜テキスト P554～555 参照＞

情報処理技術者試験に「ITパスポート試験（IP）」も含まれるが、概要は23-1-1. ITソフトウェア領域を参照のこと

情報処理技術者試験

【参照：テキスト23-2.】
P549～P559

- **各分野スペシャリスト試験**
  ITストラテジスト試験（ST）、システムアーキテクト試験（SA）、
  プロジェクトマネージャ試験（PM）、ネットワークスペシャリスト試験（NW）、
  データベーススペシャリスト試験（DB）、
  エンベデッドシステムスペシャリスト試験（ES）、
- ITサービスマネージャ試験（SM）、
  システム監査技術者試験（AU）
  ＜テキスト P555～557 参照＞

- **情報処理安全確保支援士試験（SC）**
  専門的なセキュリティ知識を基に、組織の安全な情報システムの企画・設計・運用を支援し、対策の分析評価を行い助言できる人材
  ＜テキスト P558～559 参照＞

情報処理技術者試験

【参照:テキスト23-2.】
P549～P559

国際セキュリティ資格

【参照:テキスト23-3.】
P560～P561

各情報処理技術者試験で培った知識は、国際セキュリティ資格の学習を通じて、より高度なITポジションへも期待できる

- **CISSP**(Certified Information System Security Professional)
  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
  ＜テキスト P560 参照＞

- **CISM**(Certified Information Security Manager)
  情報セキュリティの統治・管理全般の専門性を証明したい者
  ＜テキスト P560～561 参照＞

- **CISA**(Certified Information System Auditor)
  情報システムの信頼性や安全性を監査・評価できる能力を証明したい者
  ＜テキスト P561 参照＞

第24章. 各種人材育成カリキュラム

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）】

マナビDX

プラス・セキュリティ知識補充講座

【参照:テキスト24-1.】
P563～P569

カリキュラム構成と目標

経営層（経営層全体）

- サイバーセキュリティ動向が自社リスクに与える影響を正確に把握する
- リスクを考慮して、セキュリティ体制や投資を適切に決定・指示する
- インシデント時に迅速で適切な経営判断と指示を行う

デジタル化推進部門の部課長級マネジメント層

- サイバーセキュリティの動向が自部署や事業に与える影響を正確に理解する
- 自部署で実施中のセキュリティ対策の状況を把握する
- 経営層が適切な判断をできるよう、影響と現状を説明・報告する
- 社内外（情報システム部門やベンダー）とスムーズにコミュニケーションを取る

プラス・セキュリティ知識補充講座

【参照:テキスト24-1.】
P563～P569

対象別の目標・到達レベル

	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

プラス・セキュリティ知識補充講座

【参照:テキスト24-1.】
P563～P569

経営層向けカリキュラム例

単元	目標	到達レベル
1. 基礎知識	経営層として、提案や施策の妥当性を判断するために必要な知識を習得する	関係者との円滑なコミュニケーションができる程度の概念と用語を理解する
2. 脅威と対策	主要な脅威を事業リスクとして適切に把握する能力を身につける	脆弱性が完全に排除できないことを理解し、最新の脅威への対応と被害想定を行う力を養う
3. 投資	セキュリティリスクが企業価値に与える影響を理解し、適切な対策と投資を判断する	• リスクを特定し、優先順位を設定して、必要な体制や人材を確保・育成する • 提示されたセキュリティ対策案の妥当性を経営層として判断する
4. ステークホルダーとの関係	インシデント対応を理解し、企業価値を守るための準備を具体的にイメージする	対策方針について外部と意見交換や説明ができるレベルの理解を持つ

プラス・セキュリティ知識補充講座

【参照:テキスト24-1.】
P563～P569

部課長向けカリキュラム例(その1)

単元	目標	到達レベル
1. 基礎知識（初級編）	部門管理者として必要なデジタル化推進に関する最低限の知識を学ぶ	デジタルシステムやインターネットのセキュリティ対策に関する基本知識を身につける
1. 基礎知識（中級編）	部門管理者として適切な判断を行うために必要な知識を認識する	サイバーセキュリティに関する基本的な用語と概念を習得し、ベンダーと実務的な対話ができるレベルに達する
2. 脅威と対策	主要な脅威を事業リスクとして適切に理解する能力を身につける	脆弱性を完全には排除できないことを理解し、最新の脅威への対応と被害の想定を行えるようになる

プラス・セキュリティ知識補充講座

【参照:テキスト24-1.】
P563～P569

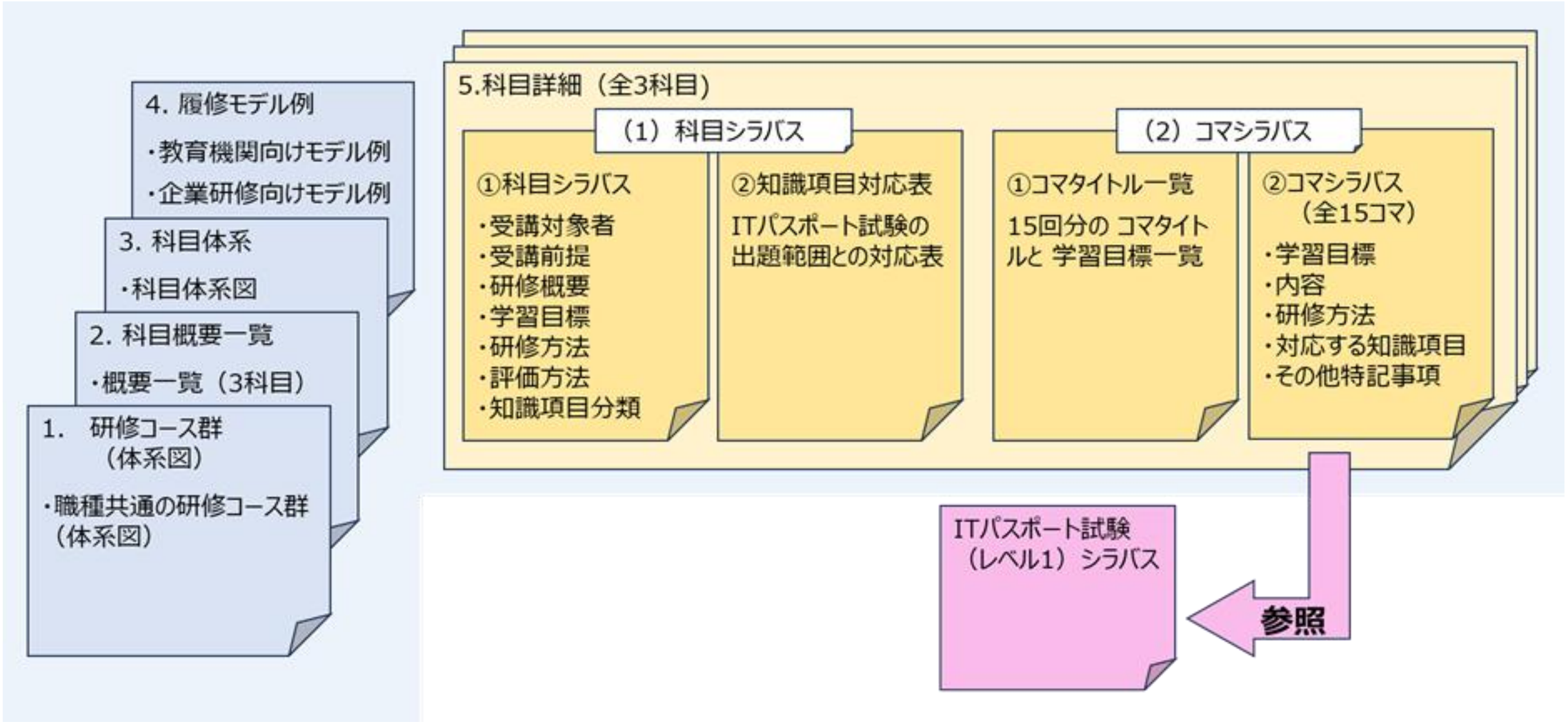
部課長向けカリキュラム例(その2)

単元	目標	到達レベル
3. 投資	サイバーセキュリティリスクの管理に必要な概念と具体的な行動を理解する	• 部署のリスクを特定し、優先順位を設定し、体制や要員の確保・育成を進める • 提示されたセキュリティ対策案の妥当性を判断する能力を持つ
4. ステークホルダーとの関係	サイバーセキュリティ対策やインシデント対応を理解し、情報開示や連絡を効果的に実践する	自部署の対策に関する社内外の情報収集や協議を実務レベルで実施できるようになる
5. 関連法令	サイバーセキュリティに関する法律や基準を実用的に理解する	デジタル化における取組で必要な法律や基準を意識して対応する

ITスキル標準モデルカリキュラム

【参照:テキスト24-2.】
P570～P574

ITスキル標準モデルカリキュラムの構成



ITスキル標準モデルカリキュラム

【参照：テキスト24-2.】
P570～P574

ITスキル標準モデルカリキュラムの構成

対象人材	① 本格的な就業経験の無い学生 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。

プラス・セキュリティ知識補充講座

【参照：テキスト24-2.】
P570～P574

コース概要

科目名	概要	受講対象者／受講前提	シラバス
IT入門（1）	経営戦略、システム開発ライフサイクル、プロジェクト・サービスマネジメント、システム監査の基礎を学ぶ	ITスキル標準レベル1を目指す者	テキスト P136参照
IT入門（2）	デジタル化、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、セキュリティの基礎知識を学ぶ	ITスキル標準レベル1を目指し、「IT入門（1）」修了または同等の知識を有する者	テキスト 137参照
パーソナルスキル入門	チームワーク、コミュニケーション、プレゼン、論理的思考、ビジネスマナー、IT活用に必要なスキルを学ぶ	ITスキル標準レベル1を目指し、高校卒業程度の知識を有する者（前提科目なし）	テキスト P137参照

マナビDX

【参照：テキスト24-3.】
P575～P578

紹介されている講座

- 厳選された信頼できる講座
- 種類が豊富
- 受講料支援のある講座も掲載
- リスキリングにも活用
- デジタルリテラシー講座
- デジタル実践講座
- サイバーセキュリティ関連講座
- 特定のスキルに特化した講座

マナビDX

【参照：テキスト24-3.】
P575～P578

講座のレベル

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+** 要求された作業を全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に向けて必要となる基本知識・技能を有する。

マナビDX

【参照：テキスト24-3.】
P575～P578

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
  - キーワードから探す
  - スキルやロールから探す
  - マナビDXオススメから探す

- Point2 自分の「お気に入り」や「学習プラン」の作成が可能
  - 「お気に入り」への登録
  - 「学習プラン」による計画的な学習の実現

- Point3 講座は「デジタルスキル標準（DSS）」と紐づけ
  - 「デジタルスキル標準（DSS）」を理解し活用する

- Point4 最先端の新技術にも対応

第25章. スキルと知識を持った人材育成・人材確保方法

「プラス・セキュリティ」の実施計画例

「リスキリング」「チェンジマインド」の実施計画例

「プラス・セキュリティ」の実施計画例

【参照:テキスト25-1.】
P580～P587

前提条件

中小企業を対象とし、セキュリティ専門家が社内に存在しない

1. 目標の明確化　＜テキスト P580～P581 参照＞

2. 学習方法の検討　＜テキスト P581参照＞

- 専門家の活用
- オンライン学習の活用
- 内部研修の実施

3. 受講者の準備　＜テキスト P581～582参照＞

- 受講の要否判定
- 事前アンケートの実施

「プラス・セキュリティ」の実施計画例

【参照:テキスト25-1.】
P580～P587

4. カリキュラムの実施　＜テキスト P582～583参照＞

- オンライン研修の実施
- 集合講習の実施
- 演習の実施

5. 結果の評価と報告　＜テキスト P583参照＞

- 結果のフィードバック
- 最終報告書の作成

6. ガントチャートの作成　＜テキスト P583～587参照＞

- 進捗確認とスケジュール管理
- リソースの効率的な活用と調整
- リスクの早期特定と対応策の準備

「リスキリング」「チェンジマインド」の実施計画例

【参照:テキスト25-2-1.】
P588～P608

「ITスキル標準」の実施計画例

1. 目標の明確化　＜テキスト P588 参照＞
2. 目標達成に必要な作業を洗い出す　＜テキスト P588～589 参照＞
3. 学習内容の詳細化　＜テキスト P589～592 参照＞
4. 学習方法の選定　＜テキスト P592～593参照＞
5. 学習の進行と進捗管理　＜テキスト P593 参照＞
6. フィードバック収集とフォローアップの実施　＜テキスト P593 参照＞

「リスキリング」「チェンジマインド」の実施計画例

【参照:テキスト25-2-2.】
P593～P608

「デジタルスキル標準」の実施計画例

DXリテラシー標準

1. 学習内容の検討　＜テキスト P593～596 参照＞
2. 学習方法の選定　＜テキスト P596 参照＞
3. 学習計画の策定　＜テキスト P596～597 参照＞
4. 学習の実施　＜テキスト P597参照＞
5. フィードバックの収集とフォローアップ　＜テキスト P597～598 参照＞

「リスキリング」「チェンジマインド」の実施計画例

【参照:テキスト25-2-2.】
P593～P608

「デジタルスキル標準」の実施計画例

DX推進スキル標準

1. 現状分析と目標設定
   ＜テキスト P599～601 参照＞
2. 学習計画の作成
   ＜テキスト P602～606 参照＞
3. 学習計画の周知と実施準備
   ＜テキスト P606～607 参照＞
4. 学習の実行
   ＜テキスト P607 参照＞
5. フィードバックと進捗管理
   ＜テキスト P607 参照＞
6. 学習プランの調整
   ＜テキスト P607 参照＞
7. 成果の評価とフィードバック
   ＜テキスト P607～P608 参照＞
8. フォローアップと継続学習
   ＜テキスト P608 参照＞

第26章. サイバーレジリエンスの必要性

サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ
ISO/IEC 27002:2022に基づく情報セキュリティインシデント管理策
サイバーレジリエンス戦略としてのNIST CSF 2.0フレームワーク
サイバーレジリエンス能力の育成に向けた体系項立て

サイバーレジリエンスの必要性と情報セキュリティ戦略上の位置づけ

サイバーレジリエンスの基本定義と戦略価値

【参照:テキスト26-1.】
P611～P614

- サイバーレジリエンスとは、サイバー攻撃やシステム障害及び自然災害に直面しても事業を継続し、迅速に復旧する能力を指す
- 侵害を許容しつつ、いかに迅速に立ち直り、事業を継続できるかが重点ポイント
- あらゆる予防策を講じてもセキュリティ侵害を完全に防ぐことは不可能なため、被害発生を前提とした事業継続力が必要

サイバーレジリエンスの必要性と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】
P611～P614

サイバーレジリエンスにおける中小企業の弱点

脅威	影響	中小企業の弱点
ランサムウェア	• 暗号化による業務停止 ➢ IPA「情報セキュリティ10大脅威 2025」	• 復旧体制不足 （専門人材・予算の不足）
サプライチェーン攻撃	• 取引先・委託先への波及被害 • 信頼失墜 ➢ IPA「情報セキュリティ10大脅威 2025」	• 監視体制不足 （委託先管理の不十分さ）
情報漏えい	• 信頼失墜 • 損害賠償リスク ➢ IPA「中小企業のセキュリティ対策に関する実態調査（2024）」	• 初動対応経験不足 • 手順書整備不足 ➢ 新たな脅威の社内共有が不十分（37.9%）
自然災害 （地震・水害・火災・停電）	• 物理設備の損壊・データ破損 • 長期操業停止 • ネットワーク障害 ➢ 経済産業省「中小企業BCP策定状況（2024）」 ➢ 内閣府「業務継続計画（BCP）に関する実態調査」	• 耐災害性の低さ （バックアップの多重化不足） • 停電・浸水などの物理的対策の遅れ • 冗長化・多拠点化が難しい

サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

【参照：テキスト26-1.】

ISO/IEC 27001・27002におけるサイバーレジリエンスの基礎 P611～P614

- サイバーレジリエンスの概念は ISO/IEC 27001の要求事項と密接に関連
- 情報セキュリティの3要素のうち「可用性」の維持がポイント
- ISMSのPDCAにおいて、「改善（Act）」がレジリエンス強化の基盤となる
- 可用性維持の具体的な実装例
  - 情報セキュリティインシデント対応
  - 事業継続計画（BCP）策定
- **ISO/IEC 27002の管理策**の多くは**サイバーレジリエンス能力の中核**をなす

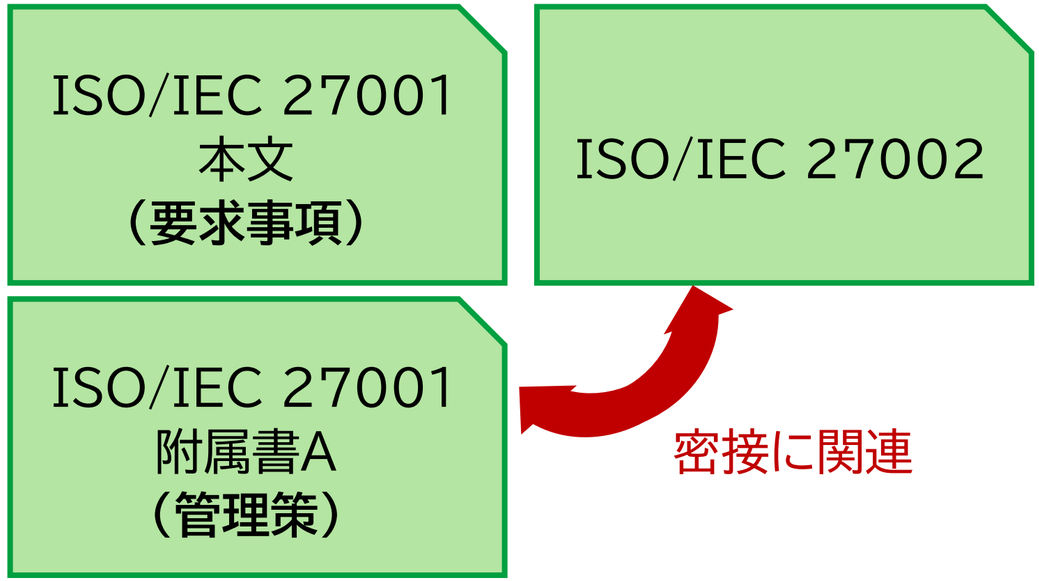


図1. ISO／IEC 27001とISO/IEC 27002の関係図
東京都 「【詳細解説】AI活用とセキュリティガバナンスのための統合規格マネジメント：ISO/IEC 27001, 27002 & 42001 詳細分析レポート」をもとに作成
https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/656/index.html

サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】
P611～P614

サイバーレジリエンスの実践策

1. 事前準備
   - 5.9　情報及びその他の関連資産の目録
   - 5.12　情報分類
   - 8.8　技術的ぜい弱性の管理
   - 8.13　情報のバックアップ

2. 対応
   - 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
   - 5.26　情報セキュリティインシデントへの対応
   - 8.15　ログ取得
   - 5.6　専門組織との連絡

サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】
P611～P614

サイバーレジリエンスの実践策

3. 回復
- 5.29　事業の中断・阻害時の情報セキュリティ
- 5.30　事業継続のための情報セキュリティ
- 8.14　情報処理施設・設備の冗長性

4. 学習と改善
- 5.27　情報セキュリティインシデントからの学習
- 6.3　情報セキュリティの意識向上、教育及び訓練

サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

【参照:テキスト26-1.】
P611～P614

サイバーレジリエンスの実践策のイメージ

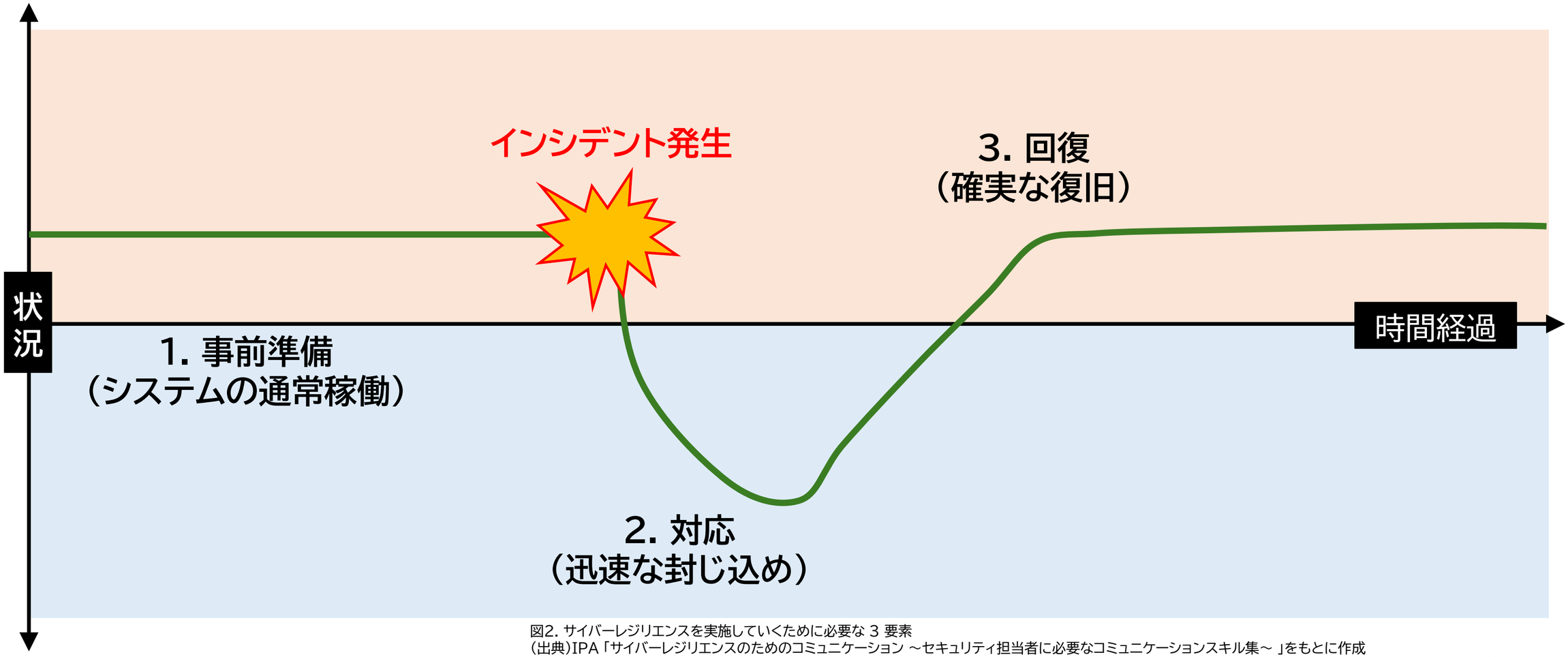


図2. サイバーレジリエンスを実施していくために必要な 3 要素
（出典）IPA「サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～ 」をもとに作成
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k00000070u7-att/f55m8k000000710q.pdf

ISO/IEC 27002に基づく情報セキュリティインシデント管理策

【参照:テキスト26-2.】P615

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の位置づけ

- 情報セキュリティインシデント対応は組織的対策であり、サイバーセキュリティフレームワーク(CSF2.0)の Respond／Recover 機能に対応している

管理策で求められる対応内容

- 対応手順の整備、事象分析、証拠保全、関係者への報告を実施する
- 対応後は教訓を反映し、再発防止策を改善に繋げる

技術的対策

- バックアップや冗長化は Recover の基盤となる
- 有効性は RTO／RPO や訓練結果で評価する

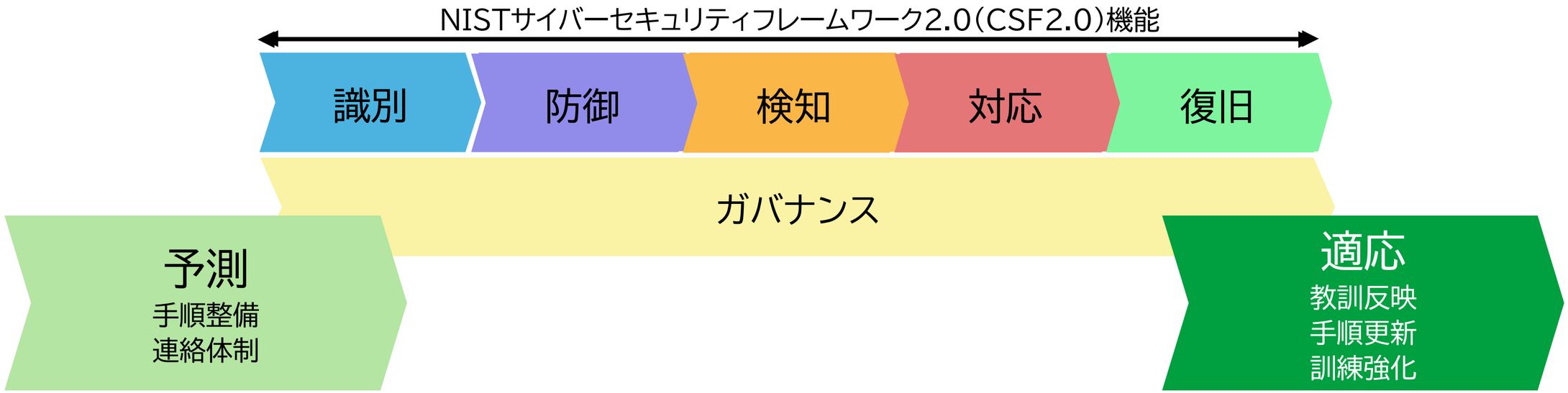
ISO/IEC 27002に基づく情報セキュリティインシデント管理策

【参照:テキスト26-2.】P615

情報セキュリティインシデント対応

マネジメントと改善

- 経営層の統制とリスク判断が不可欠である
- インシデント経験を学習し、手順や教育を継続的に改善することで、レジリエンスの「予測・適応」機能が定着する



情報セキュリティインシデント対応イメージ

図3. 情報セキュリティインシデント対応イメージ
IPA「The NIST Cybersecurity Framework（CSF）2.0（2024年2月）」の翻訳版をもとに作成
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

サイバーレジリエンス戦略としてのNIST CSF 2.0フレームワーク

【参照:テキスト26-3.】P616～P618

サイバーセキュリティフレームワーク(CSF)2.0

NIST CSF 2.0とサイバーレジリエンス

- Govern／Identify／Protect／Detect／Respond／Recover の6機能
- サイバーレジリエンスの中心は Respond(対応) と Recover(復旧)
- Govern は、サイバー対策を経営の責任として組織全体に統合する役割を持つ

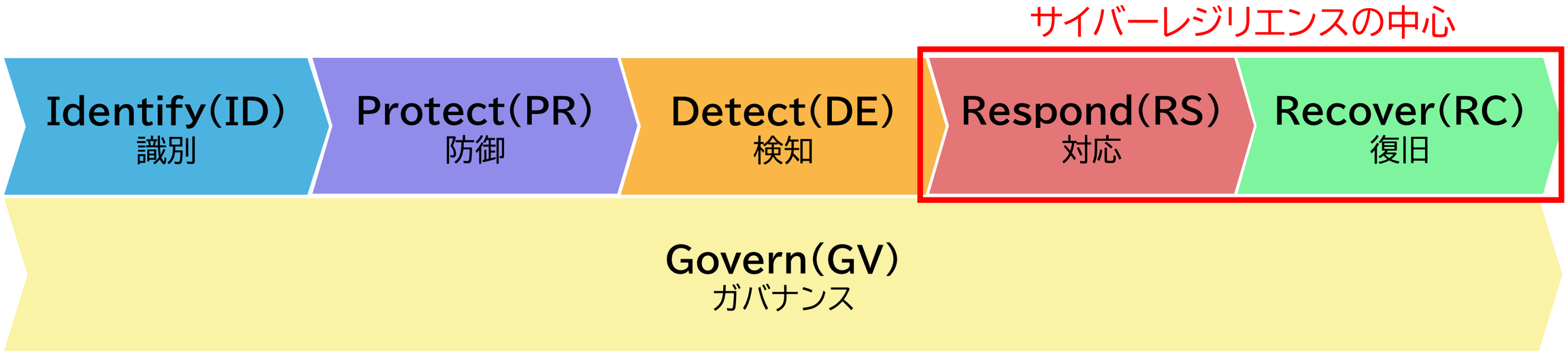


図4. NIST　CSF2.0におけるサイバーレジリエンスの中心
IPA「The NIST Cybersecurity Framework (CSF) 2.0(2024年2月)」の翻訳版をもとに作成
https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf

サイバーレジリエンス戦略としてのNIST CSF 2.0フレームワーク

【参照:テキスト26-3.】P616～P618

中小企業におけるCSF 2.0活用の実践指針

中小企業では、限られたリソースを考慮し、段階的に重点領域を整備することが現実的

CSF Tier	段階	重点機能	主な取り組み	目標
Tier 1～2	初期段階	Identify・Protect	情報資産の把握、アクセス権限の整理、バックアップの確保、クラウドやリモートアクセス環境の安全設定、端末管理と多要素認証の導入	最小限の防御体制の確立
Tier 3	発展段階	Detect・Respond	ログ監視やアラート体制の構築、インシデント報告と対応手順の明文化、定期的な訓練と連絡網の整備、遠隔環境を含む監視強化	迅速な対応体制の整備
Tier 4	成熟段階	Govern・Recover	経営層の定期レビュー、復旧計画と外部連携の統合、復旧訓練の定期化と教訓の反映、KPIに基づく継続改善の仕組みづくり	全社的レジリエンスの定着

サイバーレジリエンス戦略としてのNIST CSF 2.0フレームワーク

【参照:テキスト26-3.】P616～P618

中小企業におけるCSF 2.0活用の実践指針

　中小企業では、特にTier1～2を基盤に整備し、段階的にTier3及びTier4へ拡張していくと過度な負担なく現実的な体制を構築できる。

ガバナンス機能(Govern・GV)

- リスク評価やインシデント状況を定期的に経営層へ報告
- 経営層はリスク許容度・投資方針を決定し、IT計画に反映
- CSFをISMSや経営方針に組み込み、レジリエンスを定着

サイバーレジリエンスの有効性確認のための指標例

- 訓練実施頻度:　年2回以上のインシデント対応訓練を実施
- 復旧時間(MTTR):　主要システムの平均復旧時間を前年より短縮
- 改善策実施率:　年度内に計画した改善項目の80%以上を実施

サイバーレジリエンス能力の育成に向けた体系項立て

【参照:テキスト26-4.】P619～P620

主要フレームワークの機能比較と統合

NIST CSF 2.0の6機能を中核とした体系的なライフサイクルと主たる目的

サイバーレジリエンス ライフサイクル	CSF2.0機能	主たる目的
準備・計画	Govern（GV） Identify（ID）	経営戦略との整合性確保、リスクと資産の特定
防御	Protect（PR）	脅威に対する予防的コントロールの実装
検知	Detect（DE）	異常およびインシデントの早期発見
対応	**Respond（RS）**	**被害の封じ込め、根絶、コミュニケーション**
復旧	**Recover（RC）**	**事業の迅速な回復、サービスの復元**
改善・適応	Govern（GV） Recover（RC）	教訓の反映、体制の強化、継続的改善

サイバーレジリエンス能力の育成に向けた体系項立て

【参照:テキスト26-4.】P619～P620

NIST CSF2.0に基づく段階的育成モデル例

CSF	段階・目標	重点機能	主な取り組み
Tier 1	**Partial** **（部分的対応）** 重大被害の回避	対策が断片的で、明文化された方針が存在しない	最低限の防御・復旧体制を整備（バックアップ、EDR導入、緊急連絡網整備）
Tier 2	**Risk-Informed** **（リスク認識段階）** 継続的対策の開始	リスクを理解し、方針と責任が限定的に共有されている	重要システムのリスク評価を実施し、インシデント通報経路を整備
Tier 3	**Repeatable** **（再現的運用段階）** 継続的運用の確立	手順やルールが組織として整備され、訓練とレビューが定期化されている	年2回以上の訓練実施、ログ監視の標準化、定期的な復旧テスト
Tier 4	**Adaptive** **（適応的高度段階）** 自律的なレジリエンス経営	経営層が主導し、学習と改善を通じて動的にレジリエンスを維持している	改善活動を組織文化に定着させ、経営層がKPIに基づき意思決定

第27章. サイバー攻撃を含む様々な事態に対する総合的な対応計画

サイバーレジリエンスのライフサイクルと対応計画の策定

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

サイバーレジリエンスのライフサイクルと対応計画の策定

サイバーレジリエンス・ライフサイクルと対応計画策定

【参照:テキスト27-1.】P622～P623

総合的な対応計画(IRPとIT-BCPの統合)

- インシデント対応計画(IRP)とIT-BCPを一体化して策定し効率的に運用できる
- サイバーレジリエンスは、予防から復旧までのPDCAサイクルとして能力を強化
- ISO/IEC 27002組織的対策とNIST CSFのRespond・Recoverが基盤となる

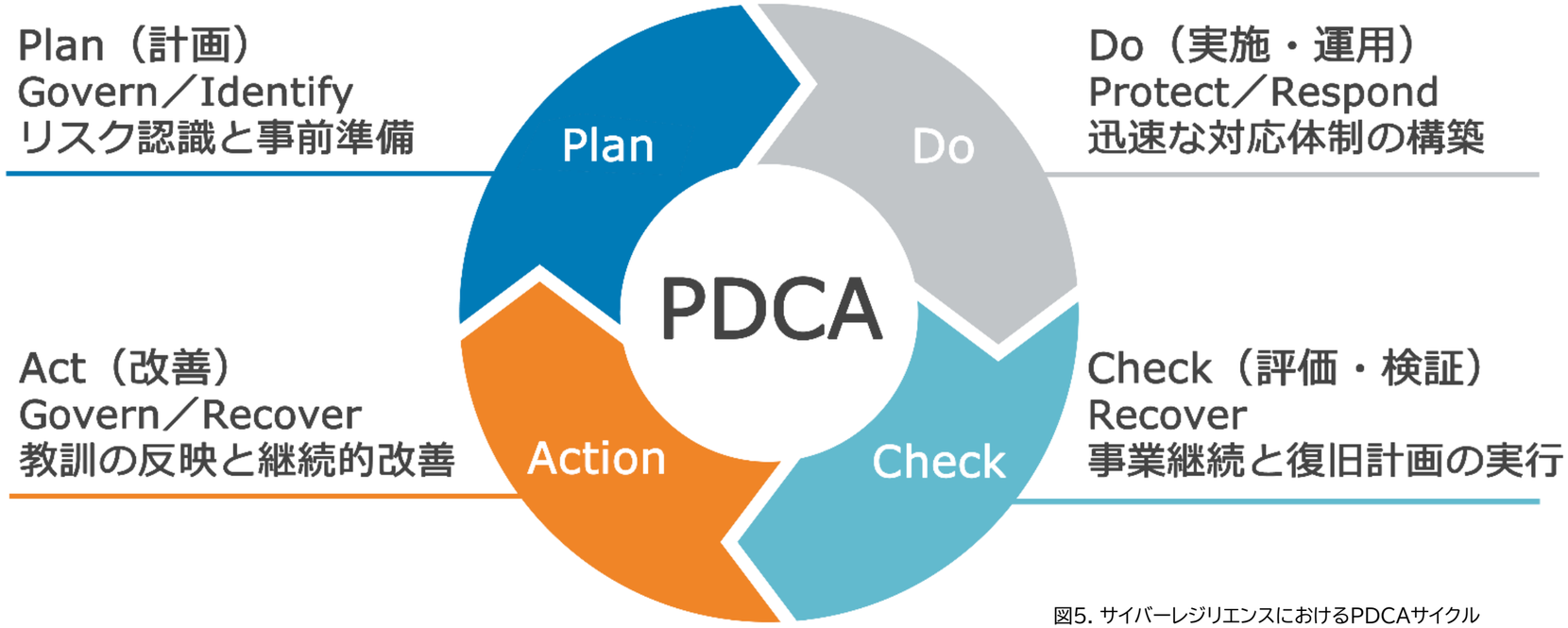


図5. サイバーレジリエンスにおけるPDCAサイクル

サイバーレジリエンスのライフサイクルと対応計画の策定

【参照:テキスト27-1.】P622～P623

サイバーレジリエンス・ライフサイクルモデル例

フェーズ	CSF機能対応と主な目的	実施の要点
Plan 計画	Govern／Identify リスク認識と事前準備	• 経営層とIT担当者が共同でリスクアセスメントを実施し、重要業務・資産・システムを特定する • IRPとIT-BCP を一体化し、RTO（復旧時間目標）とRPO（復旧時点目標）を設定する
Do 実施・運用	Protect／Respond 迅速な対応体制の構築	• インシデント発生時に初動対応を確実に実行するため、手順書と連絡網を整備する • 被害の封じ込め、影響分析、証拠保全を含む対応プロトコルを確立し、クラウド・リモート環境にも適用する
Check 評価・検証	Recover 事業継続と復旧計画の実行	• 定期的なバックアップと冗長化を確保し、復旧手順に従ってサービスを再開する • 関係者への報告や外部連携（取引先、顧客、IPA、NISCなど）を実施し、復旧後の確認テストを行う
Act 改善	Govern／Recover 教訓の反映と継続的改善	• 対応後の評価会議を実施し、再発防止策を策定する • ISMSの「パフォーマンス評価」と連携し、ポリシーや手順書の更新、従業員訓練の見直しを定期的に実施する

サイバーレジリエンスのライフサイクルと対応計画の策定

【参照:テキスト27-1.】 P622～P623

サイバーレジリエンス確立のための3要素

経営層の関与

- レジリエンスは経営リスクであり、トップが方針・優先度・体制を主導する
- NIST CSF 2.0 の Govern機能を組織に定着させる

計画と対応の統合

- IRPとIT-BCPを1つの「総合的対応計画」として統合することで、判断・行動の一貫性と効率的運用を確保する

継続的な改善

- 対応・復旧の教訓を手順書や訓練へ反映する
- PDCAを回し続けることで、レジリエンスが組織文化として定着させる

経営判断、計画統合、継続改善の3つが揃うことで、持続的な事業継続力を高められる。

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

【参照:テキスト27-2.】P624～P625

インシデント管理体制の確立(RS.IM)

RS機能はインシデント発生時に迅速に行動し、影響を封じ込めるための機能であり、混乱を防ぎ組織的に対応するために 初動対応の手順と役割分担の明確化が必須である

対応フロー

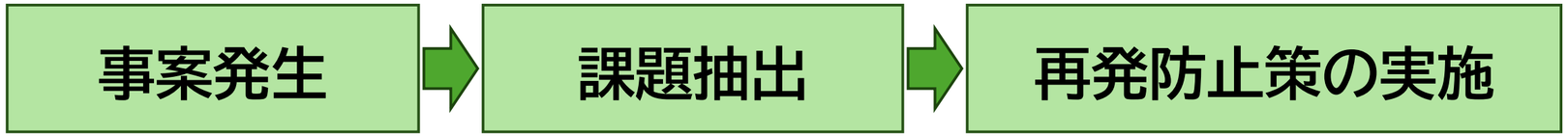


図6. 検知後の対応フロー

中小企業が整備すべきRS.IMにおける4つの領域

- 役割分担の明確化(経営層／IT／現場)
- 報告・判断プロセスの文書化
- 外部機関との連携整備(IPA、JPCERT、ベンダ等)
- 訓練と改善の継続(年1回の机上演習、手順改善)

事後レビューの実施により得られた知見から組織の危機対応力を継続的に強化することで、RS.IMは単なる手順書ではなく、実践的なレジリエンス向上の仕組みとなる。

NIST CSF 2.0 Respond（RS）機能に基づく対応基準

【参照:テキスト27-2.】P624～P625

インシデントの分析と軽減策(RS.AN、RS.MI)

RS.AN(分析能力)におけるインシデント初期対応では、原因究明・影響範囲の特定・証拠保全が最重要となる。分析には ログ(記録)の存在が必須であり、事後分析(フォレンジック)の基盤となるため、長期保存と保護が必要となる。

RS.MI(軽減策)においては、被害拡大を防ぐための封じ込め行動が中心となり、ランサムウェア対策として多要素認証(MFA)やジャンプサーバ経由のアクセス制御などの技術的対策が有効である。

中小企業が整備すべき3つの段階

- 記録　　適切なログ取得と保全
- 封じ込め　　侵入経路遮断・横展開防止
- 改善　　対応後の見直しと継続的強化

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P626～P627

復旧計画の実行(RC.RP)と事業復旧目標の設定

復旧計画(RC.RP)

- 事業継続計画(BCP)の一環としてRTO(目標復旧時間)とRPO(目標復旧時点) を明確に設定する
- RTO/RPO の設定は、経営層がビジネス要件とリスク許容度に基づいて行う戦略的判断となる

復旧の技術基盤

- バックアップと冗長化 が復旧計画の核心である
- 特にバックアップはランサムウェア対策として不可欠で、成功可否を左右する
- CSF 2.0 は、復旧しやすいシステム設計を重視する

RC.RPはバックアップ中心の対策ではなく、経営判断と技術対策を統合したレジリエンス戦略の要であり、中小企業もRTO／RPOの文書化と復旧手順検証が必要である。

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P626～P627

復旧計画の実行(RC.RP)と事業復旧目標の設定

中小企業が整備すべき4つの視点

1. 目標設定(RTO／RPO)

- 業務影響度分析(BIA)に基づき、業務ごとにRTO／RPOを設定し、経営層が承認

2. 優先順位付け・復旧責任

- 全システム同時復旧は困難なため、重要度で復旧順序と代替手段を決定する

3. バックアップ・冗長化

- 3-2-1ルール(3世代・2媒体・1つはオフライン)を基本とする
- 定期的なリストアテストを実施し、クラウドは復旧支援範囲・保持期間を確認する

4. 検証と改善

- 復旧手順演習を年1回以上実施により、PDCAに組み込み継続的に改善させる

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P626～P627

復旧のためのコミュニケーション(RC.CO)

RC.CO(復旧コミュニケーション)の目的

- 復旧時に、内部(従業員・経営)と外部(顧客・規制当局・IPA等)との情報調整を行い、透明性を確保するための機能である
- インシデントの被害状況・初動対応・復旧状況を適切なタイミングで正確に通知することが求められる
- 適切なコミュニケーションは 信頼維持に直結する

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P626～P627

CSF 2.0 対応・復旧機能に基づく対応計画の基準

CSF機能	カテゴリー（RC/RS）	機能の目的	対応基準
Respond（RS）	インシデント管理（RS.IM）	封じ込め、インシデントの管理と追跡	初動対応の実施、ネットワーク遮断措置
	インシデント分析（RS.AN）	原因究明と影響範囲の特定、証拠保全	証拠保全手順の確立、フォレンジック対応
	インシデント軽減（RS.MI）	被害拡大防止と根絶策の実行	特権ID管理、多要素認証、ジャンプサーバ利用
Recover（RC）	復旧計画の実行（RC.RP）	事業継続計画に基づくサービスの復元	RTO/RPOの策定、定期的なバックアップと冗長化
	復旧のためのコミュニケーション（RC.CO）	復旧状況の調整と外部ステークホルダーへの説明責任	関係者への適切な通知と公表手順の確立
	改善（RC.IM）	復旧計画とプロセスへの教訓の反映	事後評価に基づく再発防止策の実施、ポリシー改訂

NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

【参照:テキスト27-3.】P626～P627

復旧のためのコミュニケーション(RC.CO)

中小企業が整備すべきRC.COの3要素

責任体制の明確化

- 技術・広報・顧客対応の責任者を事前に指定する
- 緊急連絡先リストを作成し、オフラインでも参照可能にしておく

外部調整と情報発信

- クラウド・委託先との連絡体制を契約書やSLAに明記し、窓口を共有する
- 顧客・取引先への報告は 事実のみ、推測なしで行う

訓練と改善

- 年1回以上、情報伝達を想定した訓練(報告・連絡・公表)を実施する
- 演習結果を手順書へ反映し、役割理解と精度を向上させる

第28章. IT-BCPの一環としてのインシデントに対応する体制

情報システム継続計画（IT-BCP）の基本要素と体制
インシデント対応体制の確立と初動対応の具体的手順
復旧・回復プロセスと教訓の反映（継続的改善）
サイバーレジリエンス能力向上のための実践的な演習と訓練

情報システム継続計画（IT-BCP）の基本要素と体制

【参照：テキスト28-1.】
P632～P633

サイバーレジリエンスとIT-BCP

サイバーレジリエンスは IT-BCP（情報システム継続計画）と不可分であり、両者を一体として整備することが重要である。また、IT-BCPはサイバー攻撃を含む障害を想定し、事業の早期再開を目的とする組織的対策である。

経営層の役割と計画統合

- レジリエンス体制の構築は経営層のリーダーシップが不可欠である
- CSIRT等の役割・責任を明確化し、インシデント発生時は 経営者が指揮を執る
- 中小企業では、リソース効率化のためIT-BCPとIRPの統合が推奨される

情報システム継続計画（IT-BCP）の基本要素と体制

【参照：テキスト28-1.】
P632～P633

サイバーレジリエンスとIT-BCP

中小企業におけるIT-BCPの3要素

体制の明確化

- 経営層（統括）、IT担当者（技術）、総務（連絡）、外部ベンダ（支援）の役割を整理する

復旧優先順位の設定

- システムの重要度に応じて RTO・RPO を設定し、復旧責任者を決定しておく

訓練と見直し

- NCOや日本シーサート協議会（NCA）の演習資料を活用し、訓練と改善を継続する

【参考】演習資料例

NCA：　「サイバー攻撃演習訓練実施マニュアル」
IPA：　「セキュリティインシデント対応机上演習教材」
NCO：　普及啓発ポータル「みんなで使おうサイバーセキュリティ・ポータルサイト」

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P634～P637

初動対応のフェーズと実践(Respond機能の実装)

- 初動対応は 被害拡大防止・迅速復旧のため極めて重要である。
- 中小企業では専任担当者が不足するため、簡潔・実践的な行動指針を3フェーズの初動対応について整備することが必要である。

初動対応の3フェーズ

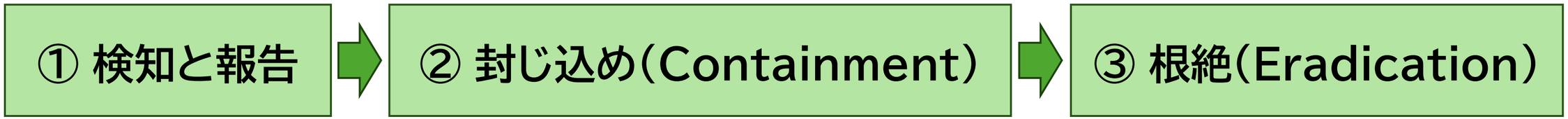


図7. 初動対応の3フェーズ

① 検知と報告

- EDR、ログ監視、従業員通報などで異常を検知したら即座に責任者へ報告
- 「インシデント報告書」に日時・対象・事象・対応状況を記録して共有
- 重大な場合は IPA・JPCERT/CC、個人情報漏えい時は規制当局へ報告

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P634～P637

初動対応のフェーズと実践(Respond機能の実装)

② 封じ込め(Containment)

- 攻撃拡大を防ぐため、感染端末の隔離・ネットワーク遮断を実施
- 証拠保全のため、ログ・記録を消さずに保存
- 必要に応じて、外部ベンダーやクラウド事業者へ支援依頼

③ 根絶(Eradication)

- マルウェア・不正設定・脆弱性などの原因を完全に除去
- 感染ファイル削除、パッチ適用、アカウント再発行、再スキャンで安全性を確認
- 作業記録は「インシデント対応記録」として保存し、復旧計画や再発防止策に活用

根絶後の対応として、事業継続の観点でIT-BCP／IRPに反映し、対応ログをもとに、初動・封じ込め・連絡手順の有効性をレビューし、年次更新を行う。

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P634～P637

ランサムウェア被害からの回復を確実にする技術的対策の実装

ランサムウェアからの確実な復旧には、具体策をサイバーレジリエンスの必須要件として組み込むことが重要である。

多要素認証(MFA)の適用　**アクセス制御の強化**　**バックアップと冗長化**

多要素認証(MFA)の重要性

- VPN・クラウド管理画面など全リモート接続に多要素認証(MFA)を適用し、ID・パスワード漏洩による侵入を遮断する
- 特に、管理者アカウントは必須と考えるべき
- スマートフォンアプリによるワンタイムパスワード(TOTP:Time-based One Time Password)方式や緊急コードの安全管理を推奨する

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-2.】
P634～P637

ランサムウェア被害からの回復を確実にする技術的対策の実装

アクセス制御の強化

- 重要サーバへの接続はジャンプサーバ経由に限定し、横展開を防止する
- 不要なポート閉鎖、共有アカウント廃止、権限分離、アクセスログ保存などを実施する

バックアップと冗長化

- ランサムウェア後の復元には バックアップの完全性の確保が不可欠である
- オフラインバックアップ、クラウド版の過去バージョン保持、複数保存先を確保する
- バックアップデータ保管責任者の明確化が重要である

復旧・回復プロセスと教訓の反映（継続的改善）

【参照：テキスト28-3.】
P638～P640

復旧・回復プロセスと教訓の反映（継続的改善）

　復旧後は、根本原因に基づく恒久的な対策を実施することが不可欠であり、特権アカウント管理や脆弱性確認などの運用改善を手順化し、PDCAで継続強化する。

原因分析と改善策の立案　**改善の実行と記録**　**再発防止計画とレビュー**

原因分析と改善策

- インシデントの原因を 技術的・組織的・人的の3視点で分析。
  - 技術的：　設定不備、脆弱性、更新漏れ
  - 組織的：　連絡体制の不備
  - 人的：　教育不足
- 改善策を明確化し、IT-BCPや対応記録に反映。

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P638～P640

復旧・回復プロセスと教訓の反映（継続的改善）

改善の実行と記録

- 対策は担当・期限・確認方法を決めて実行する
- 技術・運用・教育・外部委託の分類で整理し、効果を記録して見直す

再発防止計画とレビュー

- 改善結果を半期・年次で点検し、未完了項目は翌年へ繰り越す
- 必要に応じて外部専門家の助言を活用する
- 経営層に報告し、IT-BCPの更新に反映する

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P638～P640

教訓の反映と継続的改善（RC.IM）

サイバーレジリエンス向上の基本的な考え方として、インシデント対応で得た 教訓を体系化し改善につなげることが不可欠であり、ISMS の「改善」プロセスを活用し、復旧後の事後評価を必ず実施する。

また、RC.IMは、復旧プロセスに過去の教訓を反映することを要求されており、ポリシー見直し、設計改善、訓練更新を通じてレジリエンスを継続的に向上させる。

成功点と課題の明確化及び教訓の整理

改善項目の管理と反映

継続的改善の仕組み化

インシデント対応体制の確立と初動対応の具体的手順

【参照:テキスト28-3.】
P638～P640

教訓の反映と継続的改善（RC.IM）

成功点・課題の整理（事後レビュー）

- 復旧後に初動～復旧までを振り返り、成功点と課題を明確化する
- 手順・技術・体制の観点で教訓を整理し、「改善記録表」にまとめる

改善項目の管理と反映

- 各改善項目に 担当・期限・確認方法 を設定して管理する
- 改善結果は IT-BCP・手順書・関連文書へ反映し、経営層とも共有する

継続的改善の仕組み化

- 改善効果を確認し、未実施項目は次年度計画へ繰り越す
- 教訓を定例会や研修で共有し、組織全体の意識を向上させる

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】P641～P643

サイバーレジリエンス能力向上のための演習と訓練

文書化された IT-BCP／IRP を実効的にするには、定期的な訓練・演習が必須であり、訓練は、計画の有効性検証、役割の明確化、習熟度向上に直結する。

対象別の訓練の推奨

- 経営層向け:　サイバーリスク判断や対外説明のシミュレーション訓練
- 実務担当者向け:　CYDER・RPCIなどの実践的演習で封じ込め・復旧手順を習得

人材育成の統合

- 非専門人材も初期対応（報告・連絡・封じ込め補助）を行えるよう、「プラス・セキュリティ」などの基礎教育を継続する
- 中小企業では、これが外部専門家との橋渡し役として重要である

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】P641～P643

IT-BCPにおけるインシデント対応(IR)体制の実践ステップと教訓の反映

ステップ	実践内容の概要 (サイバーレジリエンス視点)	サイバーレジリエンス能力への貢献
準備・計画 (Plan)	IT-BCP/IRP策定、RTO/RPO設定、体制構築、演習実施	事態発生時の対応能力と迅速性の確保
検知・分析 (Detect/Analyze)	脅威の早期検知と影響範囲の特定、ログ保全	被害拡大の防止(封じ込め)
復旧・回復 (Recover)	システムの復元、サービス再開、恒久対策の実施	タイムリーな事業の再開
改善・教訓 (Improve)	事後評価に基づく再発防止策の実施、ポリシー改訂、訓練見直し	組織全体のレジリエンス向上と適応性の獲得

サイバーレジリエンス能力向上のための実践的な演習と訓練

【参照:テキスト28-4.】P641～P643

訓練・教育のおける定着のための実践的な手順

訓練・教育の実施方法

- 組織の成熟度に合わせて 机上 → 模擬 → 外部演習 を段階的に導入する
- 訓練目的・対象・頻度(年1回以上)を明確化する

訓練結果の活用

- 訓練後は評価表で改善点(連絡体制・判断・文書整合性)を整理する
- 結果を IT-BCP に添付し、次回改善サイクルへ反映 → レジリエンス向上に直結する

外部支援の活用

- IPA:サイバー演習教材・CYDER
- NCO:演習モデル・訓練シナリオ
- 地域組織:商工会等との合同訓練

外部支援の活用で、小規模でも現実的な訓練環境を構築できる。

第29章.生成AIおよびAIマネジメントシステム

AIの進化とガバナンス・リスクマネジメントの喫緊性
AIガバナンスの国際標準：ISO/IEC 42001の全貌
AIに特有のリスクの特定と体系的な管理
ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用
認証取得の動向と先進企業の事例
AI時代の持続可能な成長に向けた戦略的活用

AIの進化とガバナンス・リスクマネジメントの喫緊性

【参照：テキスト29-1.】
P646～P647

AI普及に伴うリスク

AIにはバイアス、プライバシー侵害、セキュリティリスク、倫理問題が内在しており、自動判断の不透明性や説明困難性は、従来技術より高度な管理を必要としている。また、生成AIでは、誤情報生成、著作権侵害、機密漏洩、攻撃者による悪用といった具体的リスクが顕在化している状況である。

世界的な規制動向とISOの役割

- 欧州AI法（EU AI Act）、NIST AI RMF、米国大統領令など、AI関連規制が各国で急速に整備されている
- ISO/IECは、AIリスク管理と信頼性向上のため国際規格（ISO/IEC 42001）を策定した
- 国際標準は、共通理解の形成と国際取引の円滑化に寄与する

AIの進化とガバナンス・リスクマネジメントの喫緊性

【参照：テキスト29-1.】
P646～P647

AI普及に伴うリスク

AIリスクの複雑性と企業が直面する課題

- AIリスクは技術にとどまらず、社会・倫理・経済など及ぼす効果が多面的である
- 統一的な国際規制は未整備で、各国が異なるリスクアプローチを採用している
- 技術進化が規制を上回るため、企業は 複数の規制への同時対応が必要である

ISO/IEC 42001の意義

- 多様な規制環境下において「AIのガバナンス」「リスク管理」「倫理的配慮」を体系化した国際規格である
- AI導入では、技術力に加え、どの規制に準拠し、どの社会的影響を考慮するかという高度なガバナンス戦略が不可欠である

AIガバナンスの国際標準：ISO/IEC 42001の全貌

【参照：テキスト29-2.】
P648～P650

ISO/IEC 42001とは：AIマネジメントシステム（AIMS）の目的と特徴

2023年に発行された世界初のAIマネジメントシステム規格であり、AIの設計・開発・運用におけるリスク最小化と倫理的・安全なAI活用を目的とした枠組みとなっている。また、企業がAIを「信頼性・透明性・安全性」をもって運用するための国際基準になる。

導入によるメリット（ポイント）

- 信頼性向上：　国際標準準拠を示し、顧客・取引先の信頼を獲得できる
- リスク管理強化：　バイアス・プライバシー・セキュリティなどAI特有リスクを体系的に管理できる
- 規制対応の容易化：EU AI Act 等、多様な国際規制への適合性を高める
- 競争力強化：　認証取得が差別化要因となり、先行優位を確保できる
- ガバナンス確立：　AIの責任体制・プロセスが組織に浸透させられる
- コスト最適化：　効率的な開発とリスク回避で長期的な費用を削減できる

AIガバナンスの国際標準：ISO/IEC 42001の全貌

【参照：テキスト29-2.】
P648～P650

既存のマネジメントシステム規格（ISO 9001など）との整合性

ISO/IEC 42001は ハイレベルストラクチャー（HLS） を採用し、ISO 9001、ISO/IEC 27001、ISO 27701 などと構造が共通であるため、既存のISOを持つ組織は、統合しやすく導入負荷が低いと言える。
※次ページにて図示

▼ 特筆すべきISO/IEC 27001との相乗効果

- 情報セキュリティ管理とAIガバナンスを一体化でき、プロセスの合理化ができる
- 既存の管理手順・文化・専門知識を AIガバナンスに直接応用できる

組織へのメリット（整合性がもたらす効果）

- AI管理を既存の体制に統合することで、効率的なAIガバナンス強化を実現できる
- 部門間の分断を防ぎ、組織全体で一貫したリスクマネジメントを構築できる
- AI導入における国際競争力や信頼性向上に寄与する

AIに特有のリスクの特定と体系的な管理

【参照:テキスト29-3.】
P651～P654

AIがもたらす主なリスクの種類と影響

AIには バイアス、プライバシー侵害、セキュリティ、透明性、責任、教育、競争、公正性、環境など多面的なリスクが存在する。

日本の「AI事業者ガイドライン」は「人間中心のAI社会原則（7つの原則）」をもとに、AIで想定されるリスクを10の原則に細分化しており、項目は次の通りである。

①人間中心	②安全性	③公平性	④プライバシー保護
⑤セキュリティ確保	⑥透明性	⑦アカウンタビリティ	
⑧教育・リテラシー	⑨公正競争確保	⑩イノベーション	

生成AIの追加リスク

- 著作権侵害
- 機密情報漏えい
- 攻撃者の悪用（フィッシング・マルウェア生成）

AIに特有のリスクの特定と体系的な管理

【参照:テキスト29-3.】
P651～P654

ISO/IEC 42001におけるリスクベースアプローチの原則

ISO/IEC 42001は、AIを安全に活用するためのリスクベースアプローチを中核とする国際規格である。

組織に求められる体系的な実施

- AIリスクの特定・分析・評価
- 適切な管理策の選択と実施
- 38の管理策・10の管理目標に基づく統合的管理

  38の管理策・10の管理目標に基づく統合的管理は、AIの特性(用途・影響度)に応じて柔軟に管理策を適用するため、過剰規制を避けつつ高リスクを重点管理できる。

AIに特有のリスクの特定と体系的な管理

【参照:テキスト29-3.】
P651～P654

AIリスクアセスメントと影響度評価の具体的な実践

- AIリスクアセスメント
  バイアス、誤判断、プライバシー侵害、外部要因を分析する
- 影響度評価
  個人・社会・経済への影響(人権・情報漏えい・雇用など)を判断する
- 定性・定量手法を組み合わせ、不確実な領域にも対応している
- 対応策は回避・低減・共有・保有などから選択できる

ISO 31000(リスクマネジメントの指針)との連携と活用

- ISO 31000はリスクマネジメントの国際指針(原則・枠組み・プロセス)である
- 「リスク特定→分析→評価→対応→モニタリング」の一連の流れが体系化されている
- AIリスクに対する事前管理・損失最小化・文書化が強化できる
- ISO/IEC 42001の実践において、ISO 31000は包括的な基盤として機能する

ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】 P655～P660

主要な要求事項と管理策(Annex Aの活用)

ISO/IEC 42001はAIマネジメントシステム(AIMS)の要求事項を定義しているおり、主な要求事項は以下の通り。

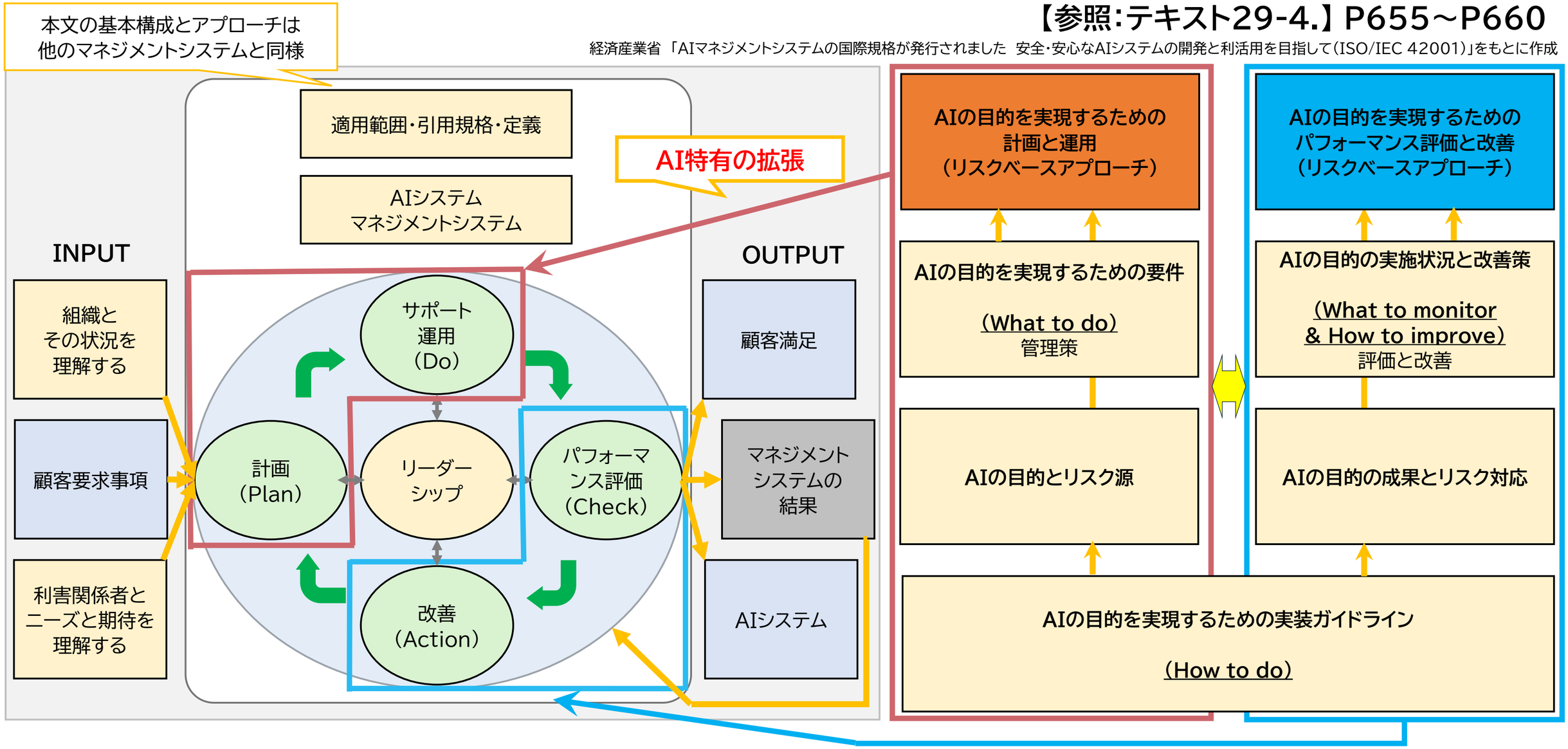
- 組織の文脈:　内部・外部環境、利害関係者ニーズ、AI目的の整理
- リーダーシップ:　責任・権限・AI文化の推進
- 計画:　AIリスク・機会の特定、リスク対応計画
- サポート:　要員・スキル・認識・文書化
- 運用:　AIシステム導入・データ管理・モニタリング・リスク管理
- パフォーマンス評価:　監視・測定・レビュー
- 改善:　評価結果に基づく継続的改善

また、Annex Aでは具体的な管理策の一覧を示し、ガバナンス、リスク管理、データ・アルゴリズム管理、透明性・説明責任、監視・改善といった観点で、AIの安全・公正・説明可能な運用を支える指針となっている。

図：AIマネジメントシステムの構成

【参照：テキスト29-4.】P655～P660

経済産業省 「AIマネジメントシステムの国際規格が発行されました 安全・安心なAIシステムの開発と利活用を目指して（ISO/IEC 42001）」をもとに作成



ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】P655～P660

導入プロセスと実践的なステップ

ISO/IEC 42001導入の一般的な流れ

- ギャップ分析
  現状のAI利用と管理レベルを把握し、不足点を洗い出す
- AIMSの設計・統合
  既存プロセス上にAIマネジメントの枠組みを構築する
- リスク・影響度評価の定期実施
  AIリスクと影響を継続的に評価する
- AI方針・手順の制定
  倫理・プライバシー・データ保護などを網羅する
- プロセスの文書化
  要求事項への適合を示せる記録を整備する
- 外部監査への準備・認証取得
  その後も法令・規制の変化に応じて更新し、内部監査・教育を継続する

ISO/IEC 42001に基づくAIマネジメントシステムの構築と運用

【参照:テキスト29-4.】 P655～P660

既存システムとの統合と効率的な導入

- ISO 9001、ISO/IEC 27001と構造が共通(HLS)で統合しやすい
- プロセスの重複を削減し、コスト・期間の短縮が可能である
- 部分導入(AIリスクアセスメントのみ等)も柔軟に実施できる

導入における課題と解決策

課題

- コスト・専門人材不足、継続運用に対する負荷、柔軟性低下の懸念

解決策

- 段階的導入:リスクアセスメント等、重要要素から順に導入
- 既存ISOシステムとの統合で負荷軽減
- 外部専門家の活用及び経営層コミットメントの強化

第30章. エグゼクティブサマリー

全体要旨

テキストの活用ポイント

全体要旨

【参照:テキスト30-1.】
P663～P665

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。

全体要旨

【参照:テキスト30-1.】
P663～P665

テキストの概要

第3編　これからの企業経営で必要な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5章～第6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。

全体要旨

【参照:テキスト30-1.】
P663～P665

テキストの概要

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。

全体要旨

【参照:テキスト30-1.】
P663～P665

テキストの概要

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。

全体要旨

【参照:テキスト30-1.】
P663～P665

テキストの概要

第10編　サイバーレジリエンス能力の育成【レベル共通】

（第26章～第28章）

サイバー攻撃やシステム障害などの事態が発生した場合でも事業を継続し、速やかに復旧・改善するために必要となるサイバーレジリエンス能力について解説しました。従来の侵入防止を中心とした対策に加え、インシデント対応計画やIT-BCPを含めた対応・復旧・改善の考え方を整理し、中小企業において段階的に取り組むための実践的な方向性を解説しました。

第11編　生成AIおよびAIマネジメントシステム

（第29章）

生成AIの利活用が進展する中で、企業が留意すべきリスクとガバナンスの考え方について解説しました。ISO/IEC 42001などの国際標準を参考に、情報セキュリティ、法令遵守、倫理を含めたAIマネジメントシステムの基本的な枠組みを整理し、組織として適切に生成AIを管理・運用するための方向性を説明しました。

テキスト活用のポイント

【参照:テキスト30-2.】
P666～P670

1. ポイントの再認識
   - DX推進の考え方の把握:＜テキストP666～667参照＞
   - セキュリティ対策の全容の認識:＜テキストP667参照＞
   - 自組織でのセキュリティ対策の実施項目の認識:＜テキストP668参照＞
   - 自組織としての実践準備:＜テキストP668～669参照＞

2. 関係者との共有
   ＜テキストP669参照＞
3. 社内体制の確立
   ＜テキストP669～P670参照＞
4. セキュリティ対策の実践
   ＜テキストP670参照＞

第31章. 各章のポイント

各章のポイント

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ています。

＜テキストP672～P750参照＞

第32章. 今後実施すべきこと

今後のアクション

今後のアクション

【参照:テキスト32-1.】
P752～P761

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、
経営者を含めた関係者と共有すること**

- 各章のポイントの理解
- DX推進の考え方の把握
- セキュリティ対策全容の認識
- 自組織でのセキュリティ対策の実施項目の認識

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。

今後のアクション

【参照:テキスト32-1.】
P752～P761

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

- 実施手順の実行準備
- 実施手順の実行
  1. 組織体制と役割の決定
  2. 年間を通して実行すべき事項の例示

- 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

実施するための年間計画を作成する

今後のアクション

【参照:テキスト32-1.】
P752～P761

Fit&Gap分析

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

非機能要件におけるセキュリティ要件の決め方

1. 情報システムで取扱う情報資産に対し、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。
3. セキュリティ要件を決定する。

今後のアクション

【参照:テキスト32-1.】
P752～P761

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
- ISMS推進マニュアル－活用ガイドブック ISO/IEC 27001:2022対応
- 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」
- ISO/IEC 27002:2022

取組例

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）	○	ー	○	ー
情報セキュリティ委員会	ー	○	○	ー
情報システム管理者	ー	ー	○	○
一般社員	ー	-	○	ー

今後のアクション

【参照:テキスト32-1.】
P752～P761

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

＜テキストP757～758参照＞

継続的な情報収集

＜テキストP758～P760参照＞

人材育成を実施するために参考となる文献

＜テキストP760～P761参照＞

令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

東京都産業労働局