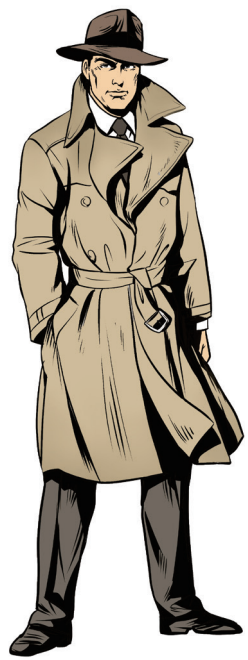
中小企業向け
サイバーセキュリティ対策の極意
Ver 4.0

中小企業向け
サイバーセキュリティ対策の極意

Ver 4.0



冴羽（さいば） 守（まもる）

日本で初めてサイバー探偵事務所を開く。ソフト帽とトレンチコートがトレードマーク。日夜懸命に頑張る中小企業の経営者に対して、客観的な態度と視点を持って依頼人に真に役立つ情報を端的に明言する。「東京をサイバー攻撃から守る」という正義感だけが、今日も彼を突き動かす。

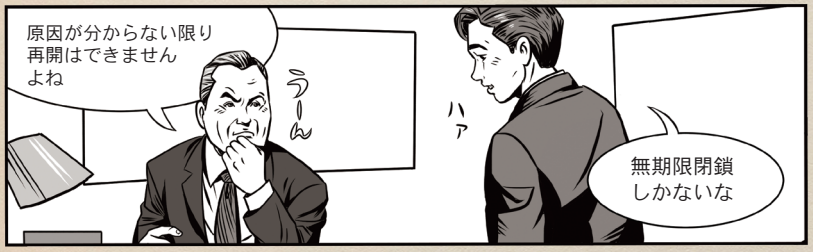
今回、その資質を見込まれ、東京都からの依頼でサイバーセキュリティ対策のコンサルタントとして本冊子のガイド役に任命された。

※本キャラクターはフィクションです

ケーススタディー　1

なぜ、こんな小さな会社が狙われたの？

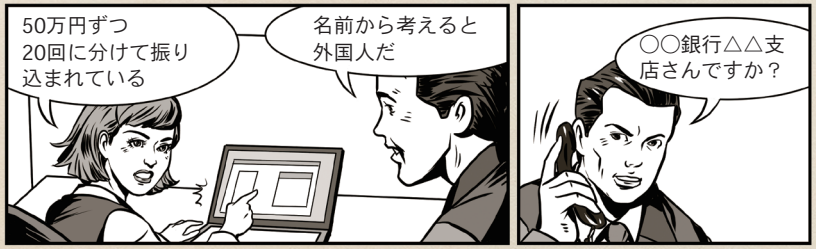
1カ月後　会社での会議



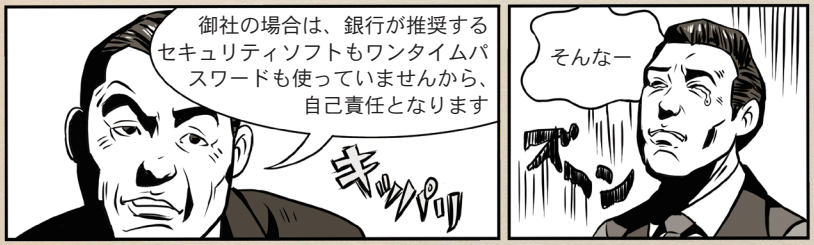
これは実際に起きたケースを基に脚色したものだ。この会社は社員10人ほどの小さな会社で、再開時期が未定のままサイトは閉鎖された。個人情報を窃取するサイバー攻撃の対象は、決して大企業や有名な通販サイトだけでなく、顧客情報の収集などインターネットを何らかの形でビジネスに利用している会社は全て標的になっている。サイバー攻撃による被害によって、事業に致命的なダメージを受ける可能性がある。備えあれば憂いなしだ。

ケーススタディー　2

ある日突然、銀行口座の預金残高が消えた！



数日後、銀行の支店長室で

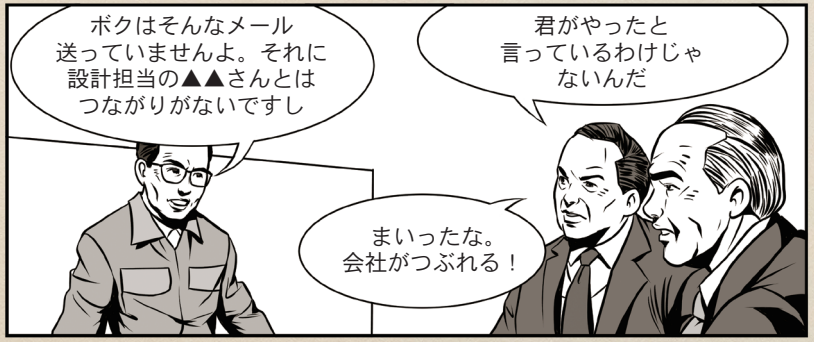


人員不足に悩む中小企業にとって、インターネットバンキングは経理業務の効率化に不可欠なものだが、サイバー攻撃の対象にもなっている。2019 年は、9 月から被害が急増し、発生件数は 1872 件に上った。年間被害総額も 25 億円超の被害が報告されている。

ケーススタディーにもある通り、インターネットバンキングを利用しているからといって、銀行が代弁してくれるとは限らない。基本的には自己防衛だ。

ケーススタディー　3

取引先企業への踏み台にされた

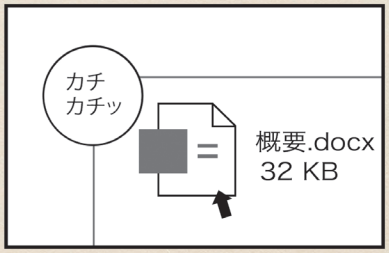


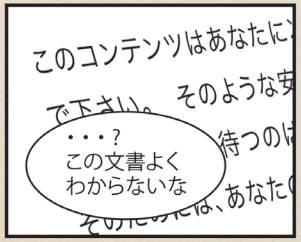
サイバー攻撃は大企業だけを狙っているわけではない。

このケースでは、標的とされた大企業のセキュリティが堅固だったため、攻撃者はその取引先の中小企業を狙ったのだ。なぜなら、中小企業のセキュリティは大企業に比べて甘く、中小企業のセキュリティを突破すれば、取引のメールなどを介して、大企業のシステム内部へ侵入しやすいからだ。こうして踏み台にされた企業にとっては、ビジネスに与える影響は甚大だ。

ケーススタディー　4

企業データが人質に！日常に潜むサイバー攻撃の魔手

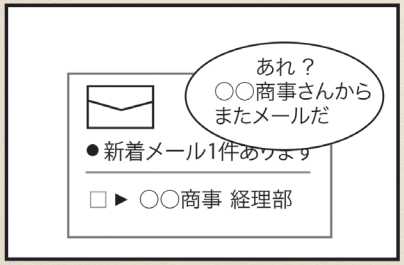




ランサムウェアを使ってパソコンを使用不全にし、身代金要求をするサイバー攻撃が目立つ。そこで中心的役割を果たしたマルウェアの１つに「Emotet（エモテット）」が挙げられる。Emotet は、冒頭のようなやり取りからパソコンや社内システムに忍び込む。そして、感染したパソコンからメール情報やアドレス帳の情報を窃取するほか、ランサムウェアをはじめとする別のマルウェアを呼び込む機能もあり、非常に厄介かつ危険な存在だ。

ケーススタディー　5

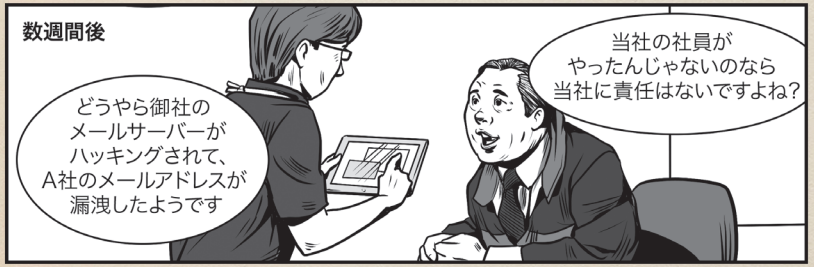
メールで届いた入金指示に従ったら詐欺の被害者に！

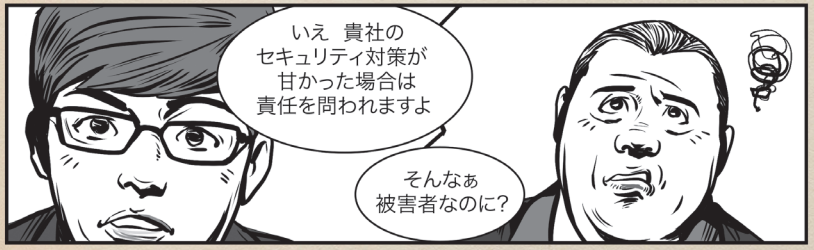


経営幹部や取引先になりすましたメールを送信し、従業員をだまして不正な口座に入金させることで金銭的な被害をもたらすサイバー攻撃が「ビジネスメール詐欺（Business E-mail Compromise ／ BEC）」だ。攻撃者は、標的となる企業の従業員が業務でやり取りしているメールを、何らかの方法で盗み見したり、ネット上の企業情報などを参考にしたりして、標的となる企業のプロジェクトや人間関係を事前に把握することで、送信メールの信憑性を高める。

ケーススタディー　6

セキュリティは サプライチェーン 全体の責任





中小企業はセキュリティ対策予算や人員が不足しがちで、対策も遅れがちだ。サイバー犯罪者はそこを突く。中小企業を取引のある大企業に攻撃する「入り口」として狙うケースも存在する。そうなれば、被害者であると同時にサイバー犯罪の一端を担ってしまう。取引停止だけでなく、損害賠償を請求されることもあるだろう。「中小企業だから狙われない」という甘い考えは通じない。セキュリティはサプライチェーン全体の問題という点を肝に銘じてほしい。

ケーススタディー　7

サイバー保険に入っていれば……

日々進化するサイバー攻撃の脅威。いつ、どのようなタイミングで狙われるかは分からない。もし攻撃の標的になったら？
そのリスクヘッジに備えるのが「サイバー保険」だ。サイバー事故によって生じた第三者に対する「損害賠償責任」や事故の際に必要となる争訟費用等の損害が補償される。ぜひチェックしてほしい。

はじめに

狙われるのは中小企業

サイバー攻撃の標的は政府・自治体や重要インフラだけではありません。
こうした大規模なサイバー攻撃には、数十万台の端末から一斉攻撃をかける手口があり、それに使用される端末は攻撃者に乗っ取られた端末です。そして比較的セキュリティの甘い中小企業の端末が狙われています。
最近では、大企業は防御が厳重なため、防御の甘い取引先の中小企業を狙い、そこから大企業のシステム内部へ侵入するケースも増えています。

セキュリティ対策はなぜ必要なのか？

インターネットが社会生活の隅々まで普及している今、サイバー攻撃は社会機能や国民生活を脅かす大きな問題となっています。個人も企業もセキュリティに関する正しい知識を身に付け、必要な対策を実践していくことがとても重要になっています。
いったんサイバー攻撃を受けて被害を受けると、金銭の損失はもとより、顧客の喪失、業務の喪失など、経営に直結する重大なリスクが発生します。経営者が責任を問われたり、場合によっては株主代表訴訟の対象にもなったりします。

すぐやろう！　サイバーセキュリティ対策

セキュリティ対策は必要だと分かっていても直接利益を生み出すものではない、難しくてよく分からない、社内に IT のことが分かる人材がいないなどの理由から、手つかずのままにしていませんか？
最優先で実施すべき対策はそんなに難しいものではありません。基本的な対策を実施することで多くの攻撃を防ぐことができます。

備えあれば憂いなし

本書は、サイバー攻撃の最新の手口から、中小企業でも実施できる基本的な対策まで分かりやすくまとめました。

INDEX 目次

中小企業向け　サイバーセキュリティ対策の極意 Ver 4.0

ケーススタディー 1　なぜ、こんな小さな会社が狙われたの？…… 2
ケーススタディー 2　ある日突然、銀行口座の預金残高が消えた！…… 4
ケーススタディー 3　取引先企業への踏み台にされた…… 6
ケーススタディー 4　企業データが人質に！日常に潜むサイバー攻撃の魔手 …… 8
ケーススタディー 5　メールで届いた入金指示に従ったら詐欺の被害者に！ …… 10
ケーススタディー 6　セキュリティはサプライチェーン全体の責任…… 12
ケーススタディー 7　サイバー保険に入っていれば……　…… 14
はじめに…… 15
目次…… 16
この冊子の使い方…… 22

TOP SECRET MISSION 1　知っておきたいサイバー攻撃の知識

1・1　標的型攻撃による情報流出…… 24
1・2　ランサムウェアを使った詐欺・恐喝…… 26
1・3　Web サービスからの個人情報の窃取 …… 28
1・4　集中アクセスによるサービス停止…… 30
1・5　内部不正による情報漏えいと業務停止…… 32
1・6　Web サイトの改ざん …… 34
1・7　インターネットバンキングの不正送金…… 36
1・8　悪意のあるスマホアプリ…… 38
1・9　巧妙・悪質化するワンクリック詐欺…… 40
1・10　Web サービスへの不正ログイン …… 42
1・11　公開された脆弱性対策情報の悪用…… 44
1・12　IoT 機器を踏み台にした攻撃 …… 46
1・13　中小企業におけるサイバー攻撃被害の例…… 48
1・14　なりすまし EC サイトの被害と回避策…… 50
1・15　ビジネスメール詐欺（BEC）にご注意！ …… 52

TOP SECRET MISSION 2　すぐやろう！　対サイバー攻撃アクション

今やろう！ 5 ＋ 2 の備えと社内使用パソコンへの対策
2・1　サイバー攻撃に対して何ができるか…… 54
2・2　OS とソフトウェアのアップデート …… 68
2・3　セキュリティ対策ソフト・機器の導入…… 70
2・4　定期的なバックアップ…… 72
2・5　パスワードの管理…… 74
2・6　アクセス管理…… 76
2・7　紛失や盗難による情報漏えい対策…… 78
2・8　テレワーク等での持ち出し・持ち込み機器対策…… 80
今やろう！ 電子メールへの備え
2・9　電子メールの安全利用…… 82
2・10　標的型攻撃メールへの対応…… 84

INDEX

2・11　迷惑メール発信への対応……86
今やろう！ インターネット利用への備え
2・12　安全な Web サイト利用 ……88
2・13　閲覧制限……90
今やろう！
2・14　重要情報の洗い出し……92
2・15　重要情報の保管……94

TOP SECRET MISSION 3　経営者は事前に何を備えればよいのか？

サイバーセキュリティ対策は、事業継続を脅かすリスクの１つ
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…… 100
3・2　サイバー攻撃を受けると企業が被る不利益…… 102
3・3　経営者に問われる責任…… 104
3・4　投資効果（費用対効果）を認識する…… 106
【コラム】セキュリティ対策は経営上の「投資」と位置付ける！ … 107
自社の IT 活用・セキュリティ対策状況を自己診断する
3・5　IT の活用診断 …… 108
3・6　サイバーセキュリティ投資診断…… 110
【コラム】「IT ガバナンス」と 6 つの原則…… 111
3・7　情報セキュリティ対策診断…… 112
ビジネスを継続するために（守りの IT 投資とサイバーセキュリティ対策）
3・8　業務の効率化、サービスの維持のために…… 114
3・9　経営者が認識すべきサイバーセキュリティ経営 3 原則 … 116

3・10　経営者がやらなければならない
サイバーセキュリティ経営の重要 10 項目 …… 118
ビジネスを発展させるために（攻めの IT 投資とサイバーセキュリティ対策）
3・11　次世代技術を活用したビジネス展開…… 130
【コラム】DX 推進はビジネス飛躍のチャンス …… 131
3・12　IoT、ビッグデータ、AI、ロボットの活用 …… 132
【コラム】IoT、ビッグデータ、AI、ロボットはつながっている …… 133
3・13　IoT が果たす役割と効果 …… 134
【コラム】中堅・中小企業の IoT 活用事例 …… 135
3・14　IoT を活用する際のサイバーセキュリティ上の留意点 …… 136
3・15　IoT を活用するための基本ルール …… 138
3・16　ビジネスを発展させるための生成 AI の利活用と、
それに伴うサイバーセキュリティ対策 …… 142

TOP SECRET MISSION 4　もしもマニュアル

4・1　緊急時対応用マニュアルの作成…… 148
4・2　基本事項の決定…… 150
4・3　漏えい・流出発生時の対応…… 152
4・4　改ざん・消失・破壊・サービス停止発生時の対応…… 154
4・5　ウイルス感染時の初期対応…… 157
4・6　届け出および相談…… 159
4・7　大規模災害などによる事業中断と事業継続管理…… 160
4・8　サイバーレジリエンスとは…… 165

TOP SECRET MISSION 5 やってみよう！サイバー攻撃対策シミュレーション

SCENE 01　サイバー攻撃前夜 …… 170
SCENE 02　攻撃発生その瞬間 …… 171
SCENE 03　サイバー攻撃直後 …… 172
SCENE 04　潜入拡大 …… 173
SCENE 05　顧客への被害の拡大　取引先への被害の拡大 …… 174
SCENE 06　サイバー攻撃の発覚 …… 175
SCENE 07　原因が判明　ウイルス感染が原因 …… 177
SCENE 08　再発防止策の作成 …… 179
SCENE 09　復旧回復 …… 181
Attention　大切なのは社内意識の向上！感染を狙うメールに注意 …… 183

TOP SECRET INFORMATION インフォメーション

6・1 ～ 6・8　緊急時対応から恒久的対策への実践ガイド
6・1　もしかしてサイバー攻撃？　緊急時には、ここに連絡を！ 186
6・2　やられる前に、しっかり予防を！ここに相談！…… 192
6・3　経営者の理解のもと、組織としてセキュリティ対策を！ 198
6・4　セキュリティお役立ちリンク…… 200
6・5　中小企業の情報セキュリティ対策の段階的レベルアップ 202
6・6　情報資産台帳の作成と詳細リスク分析…… 210
6・7　情報セキュリティ関連規程に記載すべき項目…… 217
6・8　中小企業のためのクラウドサービス安全利用手引き…… 224

6・9 ～ 6・12　DX 時代に不可欠な人材確保
6・9　DX 時代での経営者の意識改革の方向性 …… 226
6・10　DX 時代に不可欠な人材の確保と育成 …… 228
6・11　デジタル人材の認定・評価制度…… 231
6・12　デジタルリテラシー人材の認定・評価制度…… 232
6・13 ～ 6・15　関係法規、各種規程、フレームワーク等の紹介
6・13　情報セキュリティ関連法令…… 234
6・14　情報管理が不適切な場合の処罰など…… 235
6・15　情報セキュリティに関する各種フレームワークの概要… 237
主な参考文献 …… 239
用語解説インデックス …… 241

本書の用語表記について

本冊子では、日ごろ、サイバー攻撃や情報技術（IT）に接することの少ない方々にもご理解いただくために、できる限り専門用語を使わず、分かりやすい用語に統一しています。

① コンピューターに潜り込んで正常な利用を妨げる不正・有害なプログラムは、近年「マルウェア」(malware) と呼ぶようになっていますが、本冊子では主にウイルスと表現しています。
② ネットワークを通じて他のコンピューターへの感染を広める不正なプログラムが「ワーム」(worm)、利用者に気付かれないように有害な動作を行うプログラムが「トロイの木馬」(Trojan horse) と名付けられていますが、本冊子では全てウイルスと表現しています。
③ 集中アクセスによるサービス停止についても、手口としてはボットネットウイルス、DoS 攻撃、DDoS 攻撃など多様ですが、本冊子では主として「集中攻撃」という形で総称しています。
④ ウイルスを発見し駆除するプログラムについても、ウイルス対策ソフトによって定義ファイルやパターンファイルなど呼び方が異なりますが、本冊子では全て定義ファイルと表現しています。
⑤ 本冊子では「サイバーセキュリティ」と「情報セキュリティ」という 2 つの言葉を使っています。「サイバーセキュリティ」は、コンピューターやインターネットの中に広がる仮想空間に関するセキュリティという意味で使用しています。一方、現実に存在する紙媒体に記載された情報などを含むセキュリティの場合は「情報セキュリティ」を使用しています。
⑥ 本冊子で参照した多くの資料では、セキュリティを脅かす事件や事故を総称して「セキュリティインシデント」と表現していますが、本冊子では「サイバー攻撃被害」と表現しています。

詳しくは巻末の「用語解説インデックス」を参照してください。

この冊子の使い方

どんなサイバー攻撃があるのかを知る
→ [01] 知っておきたいサイバー攻撃の知識

被害を予防するための対策を行う
→ [02] すぐやろう！対サイバー攻撃アクション

経営者が備えるべきことを知る
→ [03] 経営者は事前に何を備えればよいのか？

会社としての対応計画を準備する
→ [04] もしもマニュアル

攻撃シーンを想定して実際に行動する
→ [05] やってみよう！サイバー攻撃対策シミュレーション

本書では、これだけは必ず実践してほしい項目に「すぐやろう」マークを付けました。このマークが付いている項目は優先的に確認し、必ず実施しましょう。

CHECK 今すぐチェックしておくべきこと

POINT 1 攻撃について知っておくべきこと

ACTION 1 対策のために行動するべきこと

TOP SECRET

MISSION 1

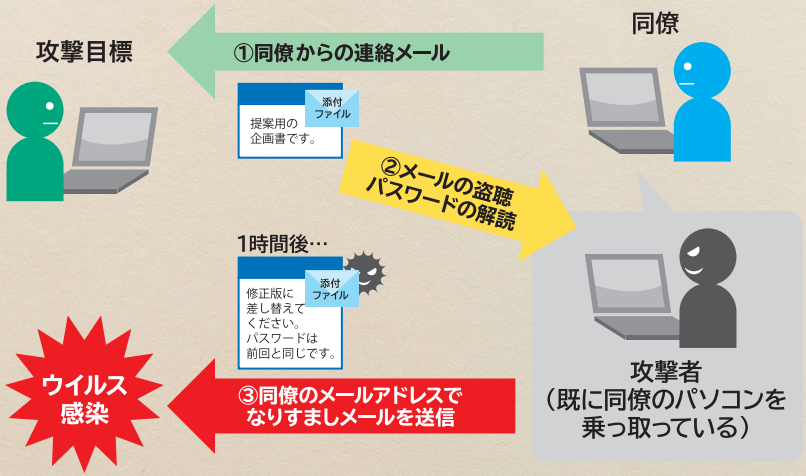
知っておきたい サイバー攻撃の知識

MISSION 1-1 標的型攻撃による情報流出

POINT 1 特定の企業や団体を狙い撃ち！

標的型攻撃とは

標的型攻撃の攻撃者は、特定の個人や企業を狙って、取引先や関係先を装い、仕事に関係しそうな話題の件名や本文のメールを送りつけてきます。メールに添付されているファイルを開いたり、本文の中にある Web サイトのリンク先にアクセスしたりすると、ウイルスに感染してしまいます。



POINT 2 標的型攻撃による被害

- 攻撃者が遠隔操作できるよう、ネットワーク上に組織外部への接続口を勝手に開く
- 感染パソコン内の情報を盗み取って外部に送信する
- 感染パソコンが会社のネットワークに感染を拡大する
- 会社の Web サイトを改ざんする
- 盗み取られたパソコン内部の情報が、次の攻撃に悪用される（例：宛先、差出人、件名、本文、署名などへの利用）

こんなメールに注意だ

- 日本語の言い回しが不自然なメール
- 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なるメール
- これまで届いたことがない公的機関からのお知らせ
- 心当たりのないメールだが、興味をそそられる内容
- 心当たりのない決済や配送通知
- 論理的に自分に送られてくることがおかしいメール

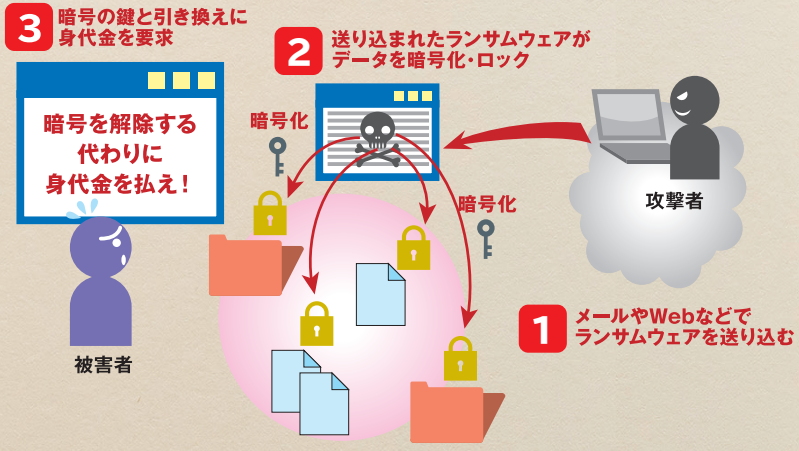
MISSION 1-2

ランサムウェアを使った詐欺・恐喝

POINT 1 パソコンやデータを使用不能にして身代金を要求！

ランサムウェアとは

ランサム（ransom）とは身代金のこと。メールに添付されたランサムウェアを不用意に開くと、パソコンのデータが勝手に暗号化されたり、パソコンがロックされたりして使用不能となります。そして、暗号化されたファイルの復元や、ロック解除の引き換えに金銭を要求されます。



POINT 2 侵入手口はメールとWebサイト

ランサムウェアは、メールの添付ファイルやメール本文に記載されている URL の Web サイトなどから侵入します。不用意に添付ファイルを開いたり、覚えのない URL にアクセスしたりしないことが最大の防御で

POINT 3 世界的脅威として認識されるランサムウェア

ランサムウェアは世界的な脅威となっています。その対抗を目的とした組織として知られるのが、欧州刑事警察機構（ユーロポール）やオランダ警察、セキュリティソフトベンダーなどが立ち上げた「No More Ransom」プロジェクト。2016 年 7 月に組織され、本プロジェクトに参加する各国法執行機関やセキュリティ関連の民間組織等は増え続けて、日本においては情報処理推進機構（IPA）などが参加しています。同プロジェクトは、ランサムウェアで暗号化されたファイルを取り戻すための無料復号ツールを提供する取り組みも継続的に行っています。

対策はバックアップと切り離し保管だ！

ランサムウェアによって、感染したパソコンだけではなく、共有サーバーや外付けハードディスクに保存されているファイルも暗号化される。ウイルス対策ソフトの導入はもちろん、OS※やソフトウェアを常に最新に保つことに加え、小まめにファイルのバックアップを取得し、パソコンやサーバーから切り離して保管しておくべきだ。

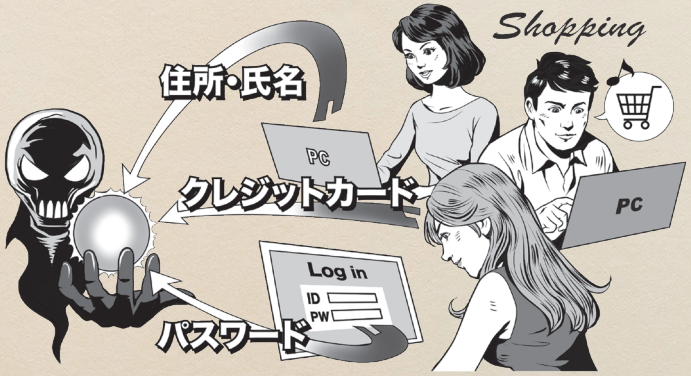
※ Operating System（基本ソフト）

MISSION 1-3

Webサービスからの個人情報の窃取

POINT 1 狙いは個人情報やクレジットカード情報

自社のホームページで、アクセスした顧客の情報を取得するために、個人情報の登録を求める場合があります。また、他社の提供するネットショッピングなどを利用する場合、クレジットカード情報を登録する場合があります。そうしたWebサーバーに登録された個人情報が狙われているのです。



POINT 2 攻撃手口はソフトウェアの脆弱性(ぜいじゃく)※1を狙う

Webサービスに対する攻撃は次の3つです。

・Webサービスでよく使われるソフトウェア※2の脆弱性を狙う
・ブログや電子掲示板などインターネット上で使用されるソフトウェア（Webアプリケーション）の弱点を狙う
・リモート管理用のサービスからの侵入を狙う

※1 セキュリティ上の欠陥（セキュリティホール）
※2 OpenSSL、Apache Struts、WordPressなど

POINT 3 改正割賦販売法への対応で対策が急務に

クレジットカード情報を狙った攻撃増加に伴い、クレジットカードを取り扱う加盟店におけるカード番号等の漏えいや不正使用被害の増加が社会課題となっています。こうした背景から2020年に割賦販売法が改正され、クレジットカード取引におけるセキュリティ対策の強化が事業者側に求められています。対策を怠ると、場合によっては業務改善命令や加盟店登録の取り消しなどの可能性があります。

対策を急ぐべきだ！

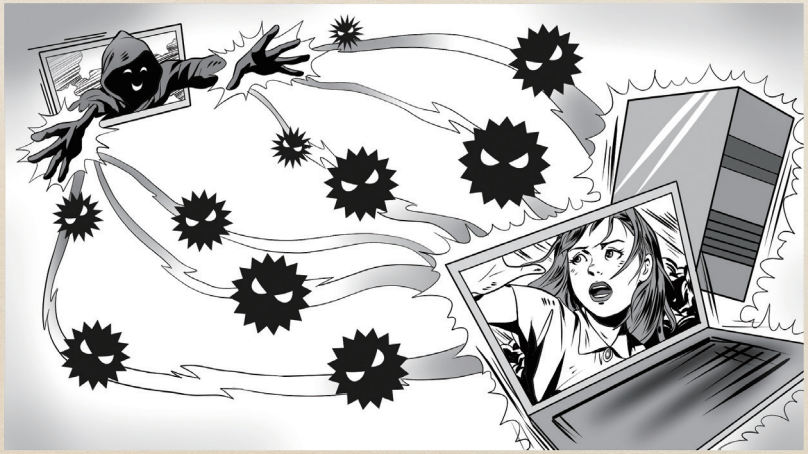
●サービスを提供する場合
・Webサーバーの OS やソフトウェア、Webアプリケーションを最新の状態にする
・Webサイトに対する攻撃を検知・防御するセキュリティソフトの導入と定期的なソフトウェアアップデート
・適切なログの取得と継続的な監視

●サービスを利用する場合
・同じIDやパスワードを使い回ししない
・他社のホームページなどに安易に情報を登録しない
・利用をやめたWebサービスは退会する

MISSION 1-4 集中アクセスによるサービス停止

POINT 1 狙いはサービスの妨害

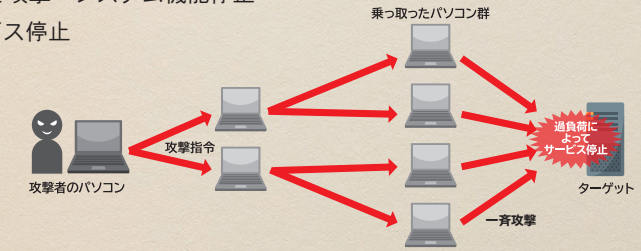
サーバーに処理速度をはるかに上回る大量の要求が集中すると、利用者はそのサーバーにアクセスできない状態になり、最終的にはサーバーがダウンしてしまいます。インターネット回線の容量がオーバーして、接続不能に陥ることもあります。



攻撃者があらかじめ不正に乗っ取った端末から一斉に攻撃を仕掛けます。数万台～数十万台のパソコンを利用した攻撃の事例もあります。最近ではパソコンだけでなく、テレビやネットワークカメラなどインターネットに接続できるデジタル情報家電なども攻撃されています。

POINT 2 攻撃手口は一斉同時集中砲火

1. インターネット経由で攻撃者が脆弱性を攻撃する不正なデータを送信→システム機能停止→サービス停止
2. インターネット経由で攻撃者が大量通信→ネットワークやサーバー処理速度の低下→サービス停止
3. 会社内の端末が感染→社内ネットワークに接続された他端末やサーバーの脆弱性を攻撃→システム機能停止
   →サービス停止



こんな被害が……

被害を受けた組織	発生年月	被害
世界的なWebサービス	2019年3月	DDoS攻撃（ディードス攻撃／Webサイトのサーバーに大量のアクセスを集中させ機能停止に追い込むDoS攻撃よりも悪質な攻撃）を受け断続的にサービスが停止。
ラグビーワールドカップ組織委員会	2019年9月	大会期間中に組織委員会に対してDDoS攻撃が行われ、職員らにもパスワード等の窃取を目的としたフィッシングメールが送信される事案が発生。
東京五輪・パラリンピック大会組織委員会	2021年7月	大会の競技初日及び翌日に攻撃予告とDDoS攻撃が発生。その後開会式、閉会式当日等にもDDoS攻撃が発生。
行政機関	2022年9月	DDoS攻撃により、政府系サイトや主要インフラ企業のウェブサイトの閲覧に障害が発生した。
ライブ配信サービス	2024年1月	DDoS攻撃により、ライブ配信を視聴しづらくなる。トップページが表示されなくなるなどの障害が発生した。

MISSION 1-5 内部不正による情報漏えいと業務停止

POINT 1 内部からも攻撃される！

意図的な情報窃取

個人情報を売買するために、職務で知りえた情報を故意に持ち出すケースです。このケースは情報漏えいというよりも情報窃取です。

うっかりミスや不注意による情報漏えい

自宅で業務を行うために社内規則を守らずに内部情報を持ち出し、紛失してしまったなどのケースです。ほとんどはルールを知りつつ違反しています。

POINT 2 持ち出し手段はUSBメモリーなど

内部情報を持ち出す手段としては USB メモリーが一番多く、そのほかではメール、パソコンです。

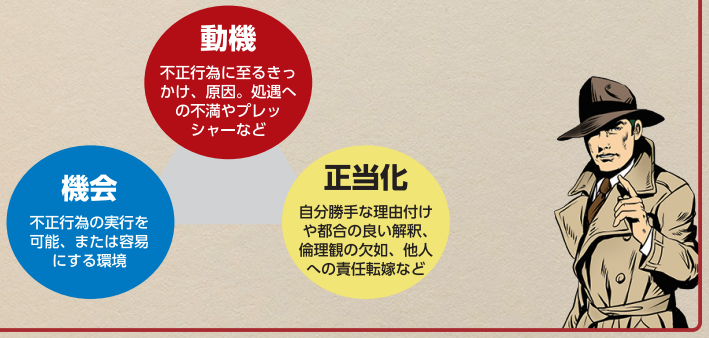
POINT 3 企業の信用が失墜し、賠償が求められる

意図的であれ、うっかりであれ、個人情報の漏えいは企業に重大な打撃を与えます。2024 年の判例では、通信教育会社の顧客情報流出に対する、損害賠償として 3338 人に計 1100 万円の支払いが命じられました。その一方で、日本損害保険協会による「サイバー保険に関する調査 2023」からは、サイバーリスクに対して「特に対策／対処をしていない」と回答した企業が 50% を上回るという傾向が浮かび上がっています。攻撃手法が多様化・悪質化している現在、早急な対策が必要です。

対策は「動機」「機会」を減らすことだ！

●「動機」を減らす
・職場環境や処遇に対する不満を解消する

●「機会」を減らす
・アクセス権の付与を最小限にするとともに管理を厳格にする
・システム操作の記録と監視により管理を強化する
・モニタリングや通報制度などにより「必ず見つかる」と思わせる
・罰則の強化により「利益にならない」と思わせる
・状況に合わせて社内ルールなどの整備・見直しをする



MISSION 1-6

Webサイトの改ざん

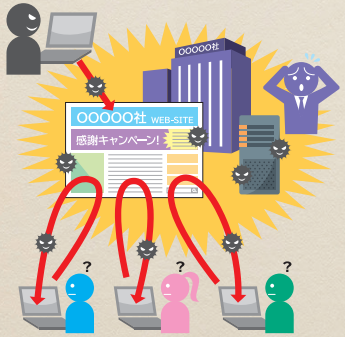
POINT 1 改ざんの目的は2つ

いたずらや主義主張による改ざん

攻撃者がいたずらや主義主張を表示する目的で改ざんするケースです。国際テロ組織の主義主張などが掲載されることもあります。

気付かぬうちにウイルスをばらまくWebサイトに

Web サイトを閲覧しただけでウイルスに感染するように改ざんされるケースです。この場合、Web サイトを改ざんされた企業はウイルス感染に加担した加害者となってしまいます。



POINT 2 ECサイトの脆弱性をついた事案も発生

近年では、EC サイト（インターネットを介した販売サイト）を利用した事業拡大も一般的となりました。しかし、EC サイトを構築するパッケージサービスの脆弱性等を突く形で、Web サイトが改ざんされ、クレジットカード番号等が窃取される被害が起きています。経済産業省によると、2019 年までに約 14 万件のクレジットカード番号等の漏えいが報告されています。

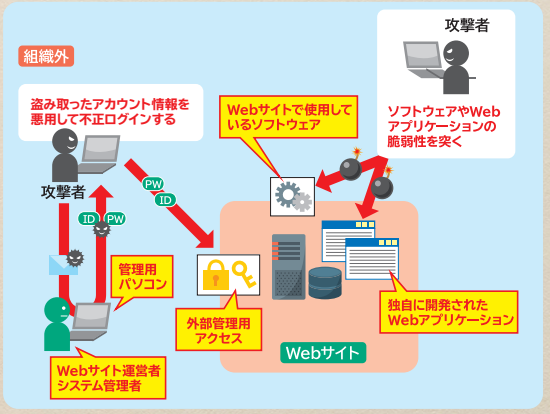
POINT 3 手口は脆弱性攻撃と管理用アカウントの乗っ取り

脆弱性を狙った攻撃による改ざん

Web サーバーに存在する脆弱性を攻撃することにより、改ざんを行います。直接コンテンツの改ざんを行う方法と、秘密の出入り口をつくるなどして遠隔操作で改ざんを行う方法の 2 つがあります。

管理用アカウントの乗っ取りによる改ざん

管理者の ID・パスワードが盗まれ、攻撃者が管理者として Web サイトを操作して改ざんしてしまうやり方です。正規の Web サイト操作により改ざんが行われるため、被害にほとんど気付きません。



対策を急ぐべきだ！

- サーバーの OS や Web アプリケーションを最新の状態にする
- サーバーに使用しているソフトウェアを更新する
- 管理用アカウントを厳重に管理する
- 改ざんを早期に検知する対策を行う

MISSION 1-7 インターネットバンキングの不正送金

POINT 1 銀行口座が狙われている！

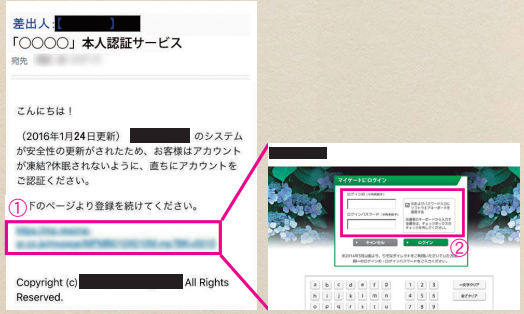
インターネットバンキング不正送金の被害は大手銀行の対策が進み、2016 年に被害額はいったん減少したものの、中小企業が利用する金融機関の法人口座の被害などにおいても増加傾向が続いています。警察庁発表によると、2019 年に発生したインターネットバンキングの不正送金事案は 1872 件。被害総額は約 25 億 2100 万円（いずれも前年度増）となっており、事態の深刻さがうかがえます。

POINT 2 手口はフィッシング詐欺と不正送金ウイルス

フィッシング詐欺

①銀行を装い、「本人認証サービスの確認」といった内容でフィッシングサイト（偽サイト）の URL を送りつける

②偽のログインページにアカウント情報を入力させる

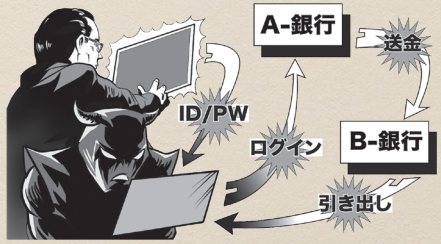


不正送金ウイルス

・攻撃者は改ざんした Web サイトやメールの添付ファイルなどから不正送金ウイルスを侵入させる

・不正送金ウイルスは、ユーザーがインターネットバンキングを利用する際、本来の画面とよく似た偽のポップアップ画面を表示し、認証情報（ID、パスワードなど）を入力させ、攻撃者に送信する

・攻撃者は、入手した認証情報を利用してインターネットバンキングにログインし、第三者の口座に送金を行う



不正送金を阻止するには

・金融機関が推奨するセキュリティソフトを導入する

・対策ソフトを最新状態に更新し、定期的なウイルススキャンを実施

・OS やインストールされているソフトウェアは常に最新の状態を保つ

・インターネットバンキングにアクセスした際にいつもと違う画面等が表示された場合、ID・パスワードを入力しない

・ID・パスワードを求めるメール等が来ても無視する

・ワンタイムパスワードを受信している場合、パソコンではなく、携帯電話やスマートフォンのメールで受信できるように登録する

・不正なログインや覚えのない送金等の履歴がないか小まめに確認

MISSION 1-8

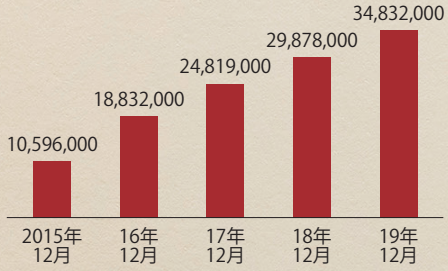
悪意のあるスマホアプリ

POINT 1 不正アプリでスマートフォンは乗っ取られる！

スマートフォンではさまざまなアプリをダウンロードして使用することができますが、中にはインストールされたスマートフォンのデータをのぞき見したり、カメラなどを遠隔で勝手に作動させたりする機能を持つ不正アプリがあります。

Androidの不正アプリが累計3400万個を突破

2010 年 8 月に最初の Android 不正アプリが検出されて以来、2019 年 12 月時点で 3400 万個に到達しました（トレンドマイクロ社調べ）。
Android では自由にアプリを配布・インストールすることができます。スマートフォンには、電話番号やメールアドレスなどの個人情報をはじめ、クレジットカードや銀行口座の情報を入れている人も多いでしょう。不正なアプリには十分注意してください。また不正アプリのアカウント削除数



（トレンドマイクロ社調べ）

POINT 2 不正アプリによる被害

- ワンクリック詐欺やフィッシング詐欺により、個人情報などを盗まれたり、アカウントの乗っ取りや不正利用で金銭を奪われたりする
- 写真や住所、電話番号などの個人情報を抜き取られて勝手にネット上に掲載されたり、自分のいる場所を追跡してストーキングをされたりして精神的な被害を受ける
- スマートフォン向けのランサムウェアで端末にロックをかけられて身代金を要求される

スマートフォンにもセキュリティ対策が必要だ！

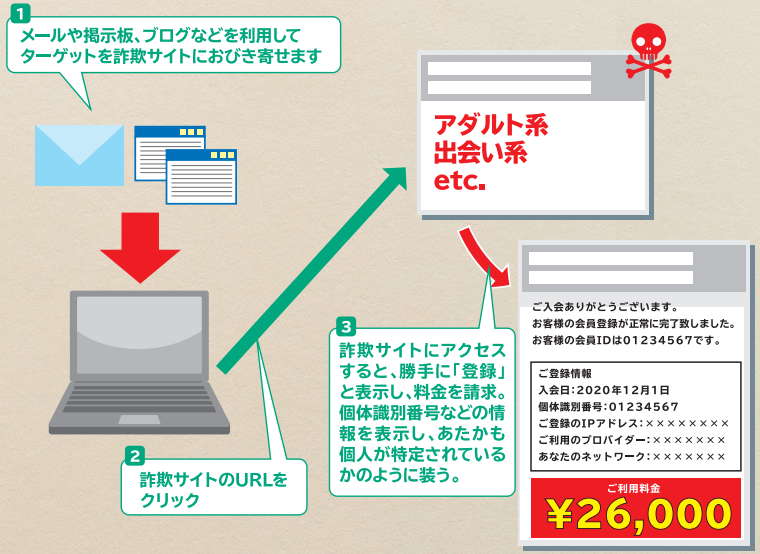
スマートフォンの OS・ソフトウェアはアップデートし、ウイルス対策ソフトも導入・更新しよう。また、公式サイト以外からアプリをインストールせず、アカウントやクレジット情報などの入力は慎重に行うことだ。さらに、重要データのバックアップを実施し、盗難・紛失に備えて画面ロックなどを設定し、「GPS（位置情報サービス）」と「端末を探す」機能を有効にしておくとよいだろう。

MISSION 1-9

巧妙・悪質化する ワンクリック詐欺

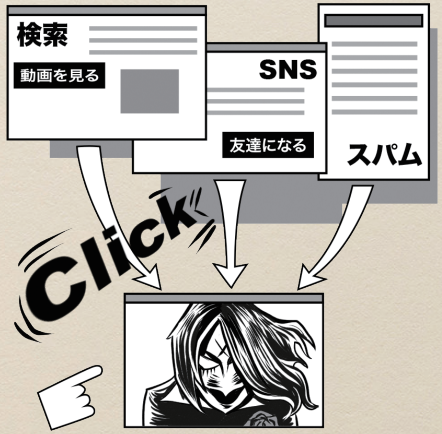
POINT 1 サイトを見ただけで請求！

アダルトサイトや出会い系サイトなどにアクセスさせ、金銭を不当に請求する攻撃です。これまでは利用者のクリックをきっかけにして請求画面が表示されるものでしたが、2016 年にはクリックすることなく Web サイトを見ただけで勝手に「登録」させて請求画面が表示される「ゼロクリック詐欺」などが出現しており、今後も注意が必要です。



POINT 2 手口は巧妙化している！

- ワンクリック詐欺に誘導するメールが届く
- パソコンなどに常駐して定期的に料金を要求する画面を表示する
- 懸賞サイトや占いサイト、音楽のダウンロードサイトなどを装う
- 合法的なコミュニティーサイトで知り合いになり、詐欺サイトに誘う
- 個人情報を盗み取り、データを削除するための金銭を要求する
- ウイルス感染の警告画面を表示して、対策ソフトを売りつけたり、パソコンのデータを盗み取ったりする
- 相談窓口を装ったサイトで解決料を請求する
- 裁判所に訴える、というメールが届く



請求には応じるな！

ワンクリック請求が来ても慌てる必要はない。料金の請求には一切応じず、とにかく無視することが最善の対処法だ。「登録完了」と表示されても、ワンクリックでは契約が成立せず、料金の支払い義務はない。
不安な場合は、国民生活センターや消費生活センターなどに相談だ。

MISSION 1-10

Webサービスへの不正ログイン

POINT 1 個人情報の窃取やオンラインショッピングでの不正注文が狙いだ！

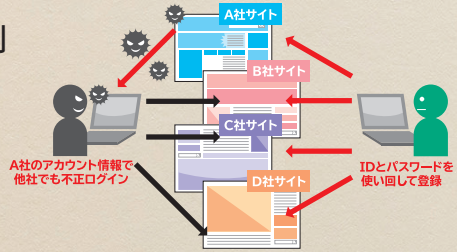
Web サービスから盗み取った ID とパスワードを悪用し、ほかのサイトに不正ログインして、なりすましを行ったり、不正な注文をしたりする攻撃です。

サービス提供者の被害例

・サービス提供しているサイトから情報を盗み取り、不正な注文やポイントの不正使用を実行
・利用者の個人情報の閲覧、窃取
・登録している利用者にサイトを装ったメールを不正送信

サービス利用者の被害例

・なりすましによるインターネットバンキングでの不正送金やオンラインショッピングでの不正注文



POINT 2 代表的な攻撃手法の特徴

パスワードの推測や情報漏えい型のウイルス

名前や誕生日、ID と同一の文字列、連続した英数字など使われやすい文字列を攻撃者が入力し、不正ログインされます。以下が主な攻撃手法の一例です。また、情報漏えいを引き起こすタイプのウイルス感染によってもユーザー ID やパスワードが不正利用される確率が高まります。

・パスワードリスト型攻撃
別の Web サービスから窃取した ID やパスワードを使い不正ログイン。

・総当たり攻撃
攻撃者側がツール等を用いて考えられる全てのパターンを試す、文字通り「総当たり」の不正ログイン手法。

・ソーシャルエンジニアリング攻撃
主要な攻撃手法の 1 つ。例えば、パソコン画面等ののぞき見によって ID やパスワードを窃取する手法です。

不正ログインを防ぐ対策はこれだ！

●サービス提供者
・簡単なパスワード、容易に推測できるパスワードを許可しない
・多要素認証を導入（Web とスマートフォンを使ったログインなど）

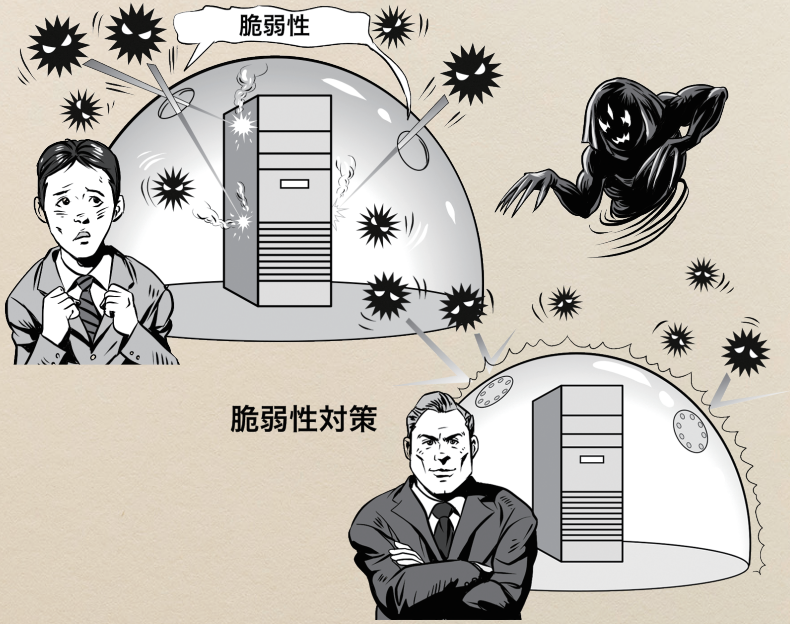
●サービス利用者
・複数の Web サービスで同一パスワードを使い回さない
・パスワード管理は他人に知られず、自分でも忘れないよう徹底する
・パスワードのほか多要素認証（ログイン時に事前登録されている電話番号との連携を通じた認証など）を採用しているサイトを利用する
・離席時のログアウトなどパソコン画面ののぞき見防止策を講じる
・パスワードが流出したと疑われるときには速やかに変更する

MISSION 1-11

公開された脆弱性対策情報の悪用

POINT 1 セキュリティ対策ができていない企業を狙い撃ち

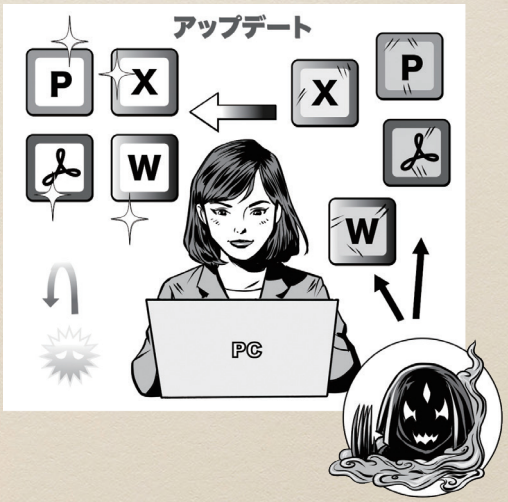
OS やソフトウェアの脆弱性が発見されると、開発したメーカーから更新プログラムが提供されます。攻撃者は、更新プログラムを実施していない利用者を探し出し、攻撃を仕掛けます。



POINT 2 こんな企業が狙われる！

・脆弱性対策情報を知らない
・利用している製品が影響を受けることを知らない
・公開された対策をすぐに実施していない

つまり、OS やソフトウェアをいつも最新の状態にしていない企業がターゲットなのです。



対策はこれだ！

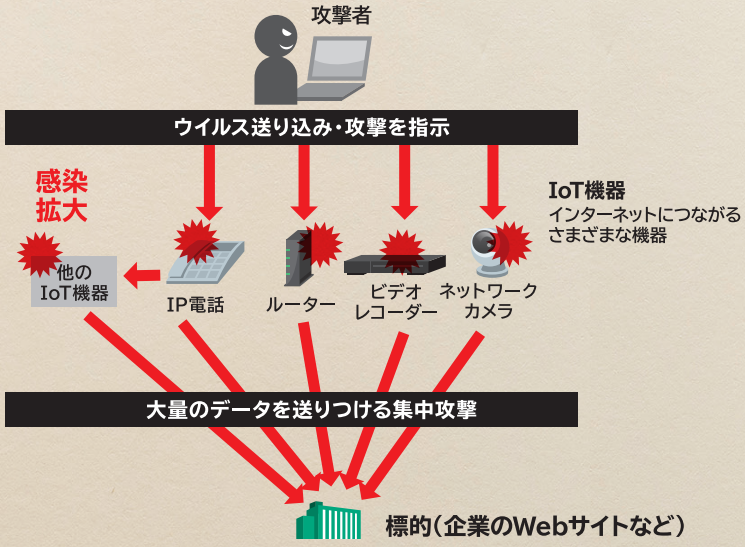
・社内で使用しているソフトウェアの全てについて、自動更新が設定されているものと設定されていないものを把握する
・使っているソフトウェアに関する脆弱性情報を「脆弱性対策情報ポータルサイト」（Japan Vulnerability Notes）などで入手する
・使っているソフトウェアに脆弱性が発見された場合に備えて、会社全体のソフトウェアを更新する手順を作成しておく
・脆弱性が発見されたら、全てのソフトウェアの更新を確認し、実行する

MISSION 1-12

IoT機器を踏み台にした攻撃

POINT 1 狙われているのはパソコンやサーバーだけではない！

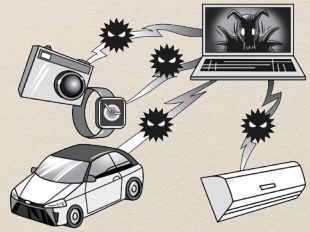
昨今は自動車やネットワークカメラ、情報家電などもインターネットにつながるようになっています（IoT※機器）。攻撃者はインターネット越しにこれらIoT機器の脆弱性や設定不備などを突いて攻撃を行い、不正アクセスやウイルス感染、さらにデータの改ざんや情報漏えい、機器操作などを行います。



※ IoT（Internet of Things）：モノをインターネットにつなげて動作させること

POINT 2 IoT機器向けウイルスの猛威

2016年にはIoT機器向けウイルス「Mirai」による攻撃により、複数の大手ネットサービスが長時間にわたって接続しにくくなるトラブルが発生しました。初期パスワードのまま使用されているネットワークカメラなどのIoT機器が「Mirai」に感染したことが原因でした。



POINT 3 脅威を増すIoT機器へのサイバー攻撃

IoT機器普及につれて、これらを狙ったサイバー攻撃の脅威も増しています。そのため、総務省や情報通信研究機構（NICT）、インターネットプロバイダが連携し、サイバー攻撃に悪用されるおそれのあるIoT機器の調査や注意喚起を行う「NOTICE」という取り組みが行われています。

● NOTICE　https://notice.go.jp/

対策はこれだ！

- IoT機器を社内ネットワークに接続するリスクとルールを周知させる
- IoT機器の管理者を明確にする
- インターネットにつながっているIoT機器を把握する
- 必要がない場合はIoT機器をインターネットに接続しない（または電源を切る）
- 管理画面にアクセスするためのIDとパスワードを確実に管理する（複雑なものに変更するなど）
- 制御用ソフトウェアの更新を定期的にチェックし、常に最新の状態にする

中小企業における サイバー攻撃被害の例

リモートワーク等の環境や仕組みを狙ったサイバー攻撃

ICT を活用した柔軟な働き方の普及により、リモートワークが定着しています。そんな中、リモートワーク用の端末や VPN 機器等のデバイスを標的とした攻撃が増加しており、社内システムへのマルウェア感染等様々な不正アクセスの被害が起きています。

中小企業を含むサプライチェーンや委託先を狙ったサイバー攻撃

大企業などの標的組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社等を攻撃し、その組織が保有する標的組織の機密情報等を窃取するサイバー攻撃が増加しています。

内部不正や不注意による情報漏えい等

個人情報などの機密情報を取り扱う従業員や元従業員等、規定の不備等により、意図的もしくは不注意による情報漏えいが度々発生しています。

最近の事例

発生地	主な要因	概要
神奈川県	古いOSの使用	古いOSでしか動作しないソフトウェアを利用するためマルウェア対策ソフト未導入の端末を使用。社内プリンターを利用する際に社内LANに接続し、インターネット接続を介してマルウェアに感染した。
愛知県	私物端末の利用	社内の特定端末から不正な通信先に通信が行われていた。社員の私物端末が会社のWi-Fiに無断接続されていたことに起因。当該端末からの不正送信先は過去にマルウェアやランサムウェア配布に利用されていることが確認されている攻撃者サーバーであった。
奈良県	ネットワーク機器の脆弱性	ネットワーク機器の脆弱性を悪用され、VPN経由で侵入を許し、サーバーがランサムウェアに感染し、大量の個人情報が暗号化された。
東京都	データを削除せずHDDを廃棄	開発保守の業務委託先従業員が、私物の外付けHDDを業務に使用し、データを削除せずに廃棄。顧客情報も含まれていることが判明した。
群馬県	サプライチェーン攻撃	取引先企業のメールサーバーがサイバー攻撃を受けたことにより、メールアドレスが漏えい。複数のアドレスから当該企業に向けてマルウェアが仕込まれたメールが送信された。メール内容は賞与支払いや請求書の支払い等を装うなりすましメールであり、サプライチェーンを通じた攻撃であった。

参考：経済産業省「昨今のサイバー攻撃事案を踏まえた注意喚起と報告のお願い」に対する報告結果 及び「中小企業向けサイバーセキュリティ事後対応支援実証事業（いわゆる「サイバーセキュリティお助け隊」）」の事業報告を踏まえた昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について」（2020年6月）IPA 情報セキュリティ10大脅威 2025

MISSION 1-14 なりすましECサイトの被害と回避策

POINT 1 なりすましECサイトに注意！

実在するサイトの外観を装った「なりすまし EC サイト」。その被害が増加して
います。これらは既存の EC サイトの模倣などによって消費者を誤認させ、商品代金を騙しとったり、模倣品、海賊版その他購入しようとした品と全く別個の物を送りつけてきたりします。また、こうした手口だけでなく、クレジットカード決済ができるかのように見せかけて消費者側のカード情報等を入力させ

典型事例

その他の特徴としては、「支払い方法が銀行振り込みのみになっている」「問い合わせ先のメールアドレスがフリーメールアドレス」「フォームの崩れやリンク切れなど Web サイトの作り方に粗雑な点が見られる」などが挙げられま

出典：セーファーインターネット協会／なりすまし EC 対策協議会「なりすまし EC サイトに注意！」よ

POINT 2 なりすましECサイトの対策を怠ると企業側も大きな不利益を被る可能性が…

なりすまし EC サイトの被害者は、消費者だけではありません。なりすまされた企業側にも大きな不利益が生じる可能性があります。なりすまし EC サイトへの対策を放置すると、

・売上減少
・信頼失墜
・被害者からのクレーム・問い合わせ殺到

といった事態が生まれる可能性があります。EC サイトの来訪者への注意喚起など積極的な対策が重要で

なりすましECサイトを撃退せよ！

なりすまし EC サイトを撃退するには、積極的なアクションが重要だ。より具体的には、

・来訪者への注意喚起
・迅速な問い合わせ対応
・プロバイダへの削除要請

の 3 つが考えられる。また、警察に情報提供することで、当該サイトの銀行口座の停止やウイルス対策ソフトやフィルタリング製品への反映がされる場合があり、被害拡大防止が期待できる。

● 一般社団法人セーファーインターネット協会／なりすまし EC サイト対策協議会「なりすまし EC サイト対策マニュアル」（2015 年 3 月）

https://www.saferinternet.or.jp/wordpress/wp-content/uploads/narisumashi_manual.pdf

ビジネスメール詐欺(BEC)にご注意!

巧妙なBECの罠

ケーススタディー 5 (P10) でもご紹介した「BEC 攻撃」。「取引先から振込先口座変更の指示を電子メールで受信した」などのように、ビジネス関係者を装ったサイバー攻撃が中小企業を狙っています。

BEC被害の事例

BEC 攻撃は世界的にも大きな被害を生んでいます。「取引先との請求書の偽装」「経営者などへのなりすまし」「窃取メールアカウントの悪用」「弁護士など社外の権威ある第三者へのなりすまし 」「詐欺の準備行為」の大きく 5 つのタイプに分類できます。

セキュリティ意識を高め対策を確実に!

- 取引先とメール以外の方法で確認
- 電信送金に関する社内規程の整備
- 普段とは異なる表現のメールやフリーメールに注意
- 不審なメールは組織内外で情報共有
- ウイルス・不正アクセス対策はしっかりと
- 電子署名を活用しよう

TOP SECRET

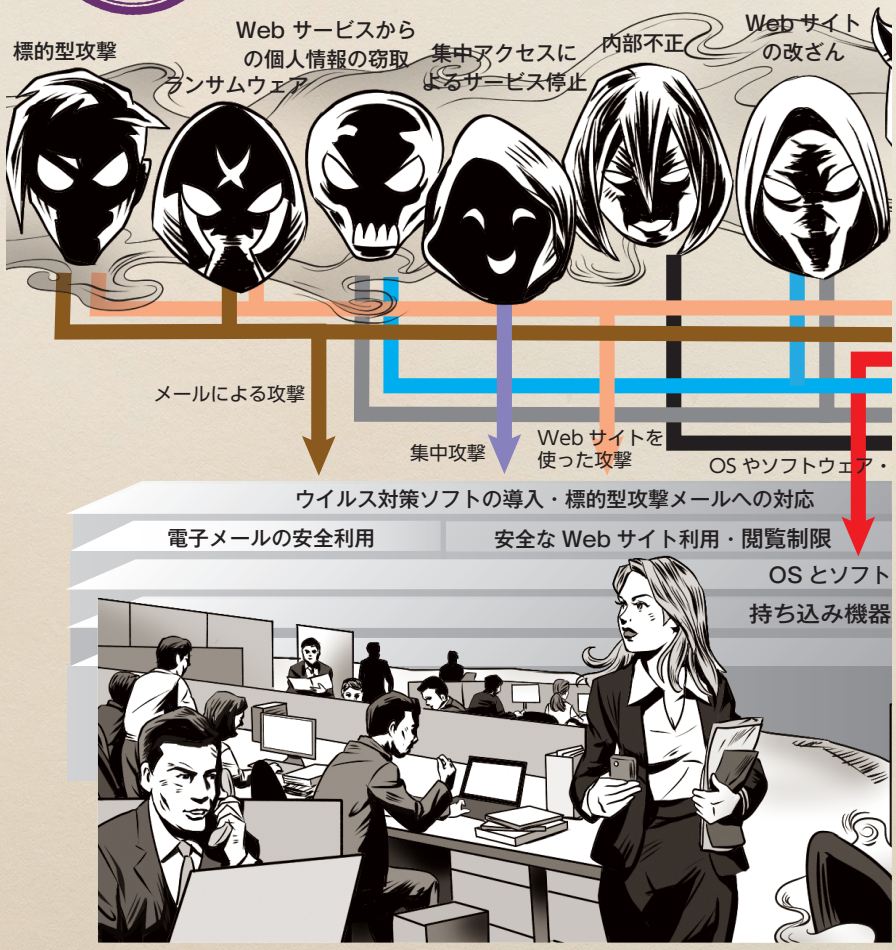
MISSION 2

すぐやろう！ 対サイバー攻撃アクション

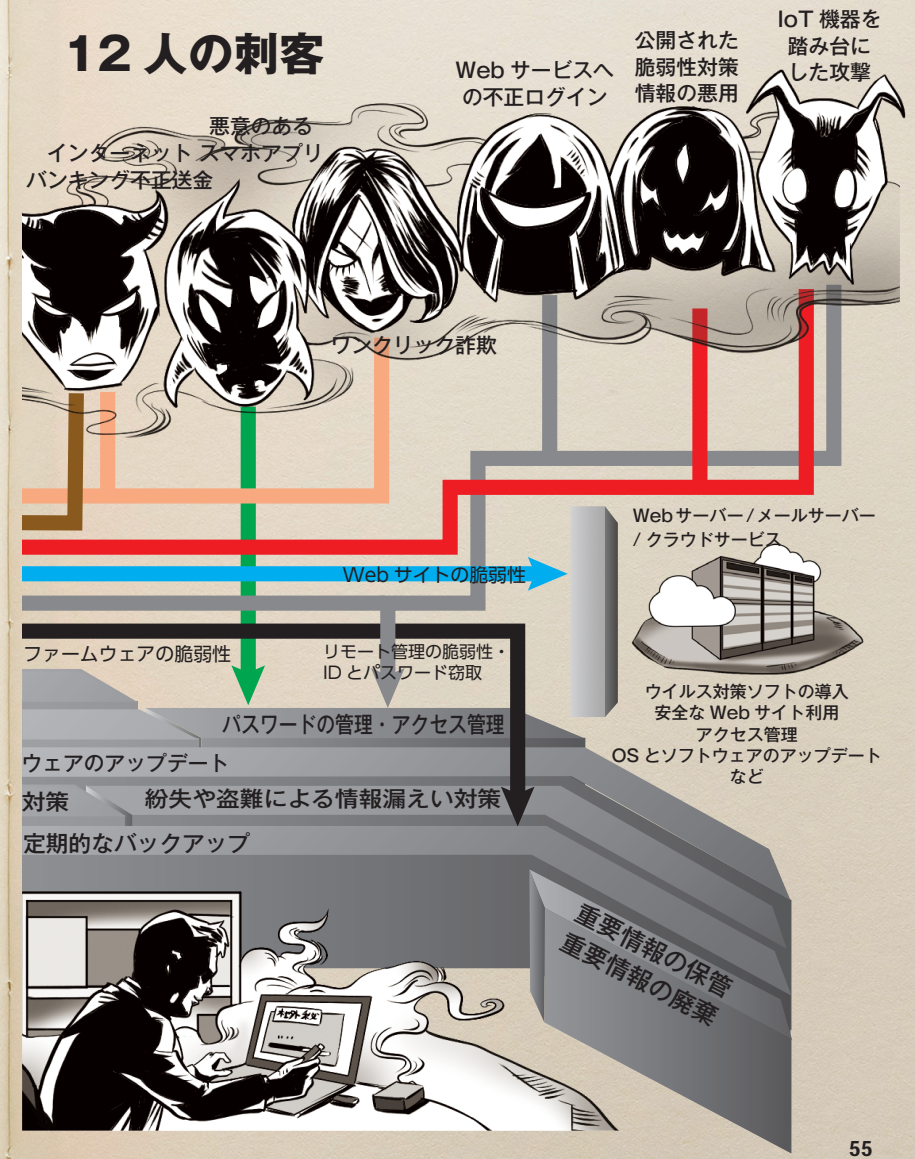
MISSION 2-1

今やろう！ 5+2の備えと社内使用パソコンへの対策

サイバー攻撃に対して何ができるか

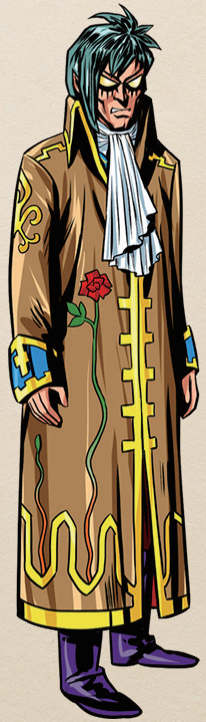


12 人の刺客



12 人の刺客：ドッペルゲンガー
標的型攻撃

我が文章はまさに芸術。
この最高傑作、
果たして見破れるかな



＜名前の由来＞
標的型による成りすましで本人そっくりのメールを送る技術に長け、「生き写し」と呼ばれる。

＜プロフィール＞
自分自身は直接ウイルスの作成は行わず、攻撃対象に対してウイルスを潜り込ませるための標的型攻撃メールを作成するスペシャリスト。複数の国の言語・文化に精通しており、作成する文章はネイティブ並みで不自然さは感じられない。さらに送信元の人物の文体のクセまで模倣するため、送られくるメールの文章はまさに生き写し。
職人気質で自分の攻撃メールがどの程度相手をだませるかが重要で、結果的に得られる金銭的利益にはあまり興味がない。
Emotet と呼ばれるウィルスを何処からか入手して、世界中に拡散を試みている。

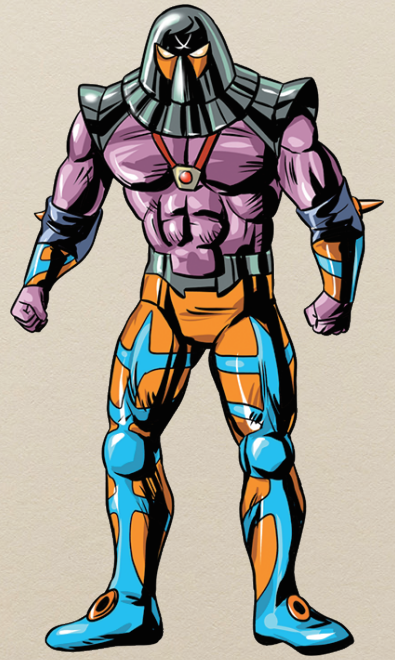
＜事例＞
某お菓子メーカーは、社員を装ったメールに添付された Word ファイルを開き、「編集を有効にする」をクリックし、ウイルスに感染。

12 人の刺客：ハインリッヒ
ランサムウェア

＜名前の由来＞
高額の身代金を奪う技量を持つ。名前の由来はイングランドのリチャード王を拘束し、高額の身代金を得た神聖ローマ皇帝ハインリヒ6世から。

まあ、そのデータを諦めるなら、それはそれでよし。
ただ、この程度の金銭を惜しむのかね？

＜プロフィール＞
重要なデータを人質に金銭を要求するランサムウェアを使って荒稼ぎをする。絶対に取り戻さないと業務に支障があるデータを有する組織を狙って、データを使えなくし、高額な金銭を要求することが多い。現時点での1件当たりのランサムウェア被害額の最高記録は自分が保持していると主張している。最近は宗旨替えをして、この金額なら払っても惜しくはないか、と思える絶妙な金額を要求し、数で稼ぐこともやっている。



＜事例＞
某病院では、ランサムウェアにより、電子カルテなどの端末と関連するサーバのデータが暗号化され、患者の診察記録が閲覧できなくなり、病院の機能が停止。
通常の診療を再開するまでに数か月を要した。

12 人の刺客：フラー
個人情報窃取

フェイクとは違うんだよ！
フェイクとは！

＜名前の由来＞

脆弱性を突いて個人情報を窃取するのが得意。名前の由来は「奇襲の原則」を記述した軍事理論家フラーから。

＜プロフィール＞

主に EC サイトを狙い、Web サーバに登録されている顧客情報を密かに窃取することを得意とする。狙う対象は、Web サイトを構築するソフトウェアの脆弱性やブログ及び電子掲示板等の Web アプリケーションの脆弱性を改善しないまま公開している EC サイト。一見してフェイクと被るが、情報を窃取された企業が日々マスコミから法的・社会的責任を追及される姿をしり目に、窃取した情報を基にパスワードリスト攻撃といった二次的犯行を繰り返す血も涙もないところはまさに外道。Web サイトの改ざんで満足するフェイクがかわいいくらいだ。企業としては絶対に敵に回したくない相手の一人だろう。

＜事例＞

某大手フリーマーケット会社は、サイバー攻撃により顧客情報約 275 万件が流出した可能性があることを発表した。

12 人の刺客：サガー
集中アクセスによるサービス停止

＜名前の由来＞

ＤＤｏｓ攻撃に長け、物量で押し切る。第４次中東戦争で強力なイスラエル戦車部隊を数量で圧倒したソ連製対戦車ミサイル「サガー」の名を名乗る。

ふへへ、次はどのサイトを
落としてやろうかな

＜プロフィール＞

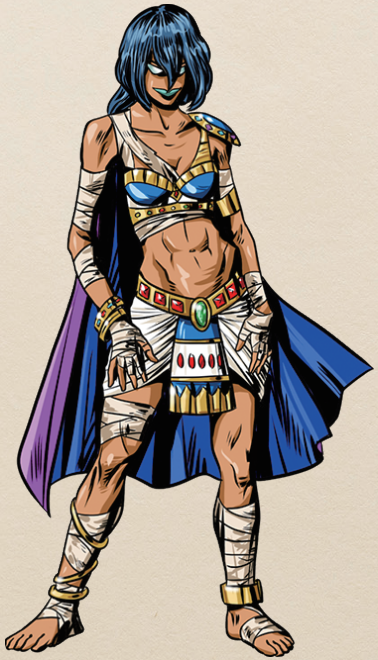
政府や企業のサイトにＤＤＯＳ攻撃を仕掛けて、サイト閲覧をできなくする愉快犯。他人のあたふたした姿を見るのが目的なので、攻撃相手は選ばない。サイトを落とすぞと脅迫して金銭を要求することもある。本人の能力は実はたいしたことがないようだが、闇サイトで調達した攻撃ツールを使って、とにかく数で押し切ってくる。ＳＮＳの捨てアカウントで犯行予告やあおりをすることも多い。過去に犯行予告をした際にズボンのチャックが全開のままの姿を投稿したことがある。

＜事例＞

某ライブ配信サービスでは DDos 攻撃によりサービスにアクセスしづらくなる。トップページが表示されなくなる。などの被害が発生した。攻撃は1週間以上つづきました。

12 人の刺客：ユダ
内部不正

動機・機会・正当化こそ
私を突き動かす力の源だ！



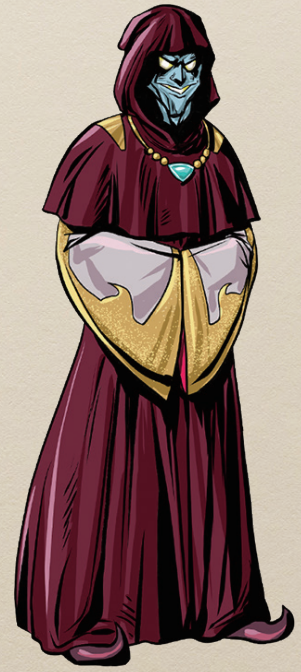
＜名前の由来＞
組織内部に裏切り者「ユダ」を作る能力に長ける。

＜プロフィール＞
サイバー空間を介さず、人間の心に直接アクセスできる能力を有するエスパーゴースト。しかし、その実態は、不正三種の神器である『動機の鏡』『機会の勾玉』『正当化の剣』を駆使して人間を操るゴースト界きってのエース。人間の心理を突いてくるその攻撃は、高価なセキュリティ設備の導入をもってしても完全に防ぐことは難しく、企業にとっては常に警戒しなくてはならない存在である。そのため、ユダとの戦いを制することは、サイバーセキュリティを制するといってもても過言ではないだろう。

＜事例＞
卸・小売業を営む某中小企業にて、元従業員が退職前に大量にファイルをダウンロードしたうえに、使用していた PC の履歴を消去。専門家でも復旧できない状態となり、機密情報を持ち出した確定的な証拠を得ることができず、結果的には被害届を提出できなかった。

12 人の刺客：フェイク
Web サイトの改ざん

表面しか更新していない
サイトはタイトルを
『フェイク様カッコいい』
にしてやんよ



＜名前の由来＞
WEBサイトを改ざんし本物と見分けがつかない偽物（フェイク）を作るのが得意。

＜プロフィール＞
脆弱性のある古い OS やソフトウェアを更新しないまま使用し続けている Web サーバを見つけ出し、その脆弱性を狙って Web サイトを改ざんすることを得意とする。ただ、改ざんとはいってもフェイク自身に技術力がないため、レージィが作成した攻撃ツールを使用してサイトのタイトルを改ざんすることが精一杯である。他のサイバーゴーストからは『スクリプトキディ』というあだ名をもらい、その単語の響きからカッコいいと思っていたが、最近インターネットで意味を知ってしまい、落ち込んでいる。得意技は標的サイトの情報を露見させる「ダブルゲット」。

＜事例＞
大手動画ストリーミングサービスにおいて、人気アーティストのミュージックビデオのタイトルやサムネイル画像が改ざんされる事例が発生した。

12 人の刺客：ベラム
インターネットバンキング不正送金

＜名前の由来＞
フィッシングの王。アーサー王伝説の漁夫王（フィッシャーキング）の名から。

＜プロフィール＞
インターネットバンキングの不正送金を利用して、経済的利益を追求する金銭目的の犯罪者。個人から法人まで手広く狙う。フィッシングサイト及び不正送金ウイルスによる偽の入力画面表示でＩＤ・パスワードを窃取する。特にフィッシングサイトの作成に長け、人呼んで "phisher king"。自己顕示欲が強く用済みのフィッシングサイトには自らのコスチューム姿を表示し、被害者をあざ笑う。

＜事例＞
某大手銀行からのＥメールを装い、「アカウント保全のため」などの内容で本物そっくりの偽サイトへ誘導。ID・パスワードを入力させ、その情報を利用して不正送金を行う。

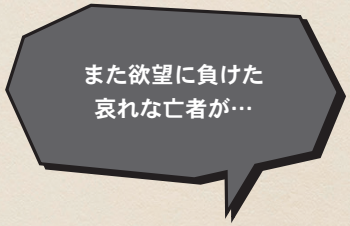
12 人の刺客：バッドアップル
悪意のあるスマホアプリ

＜名前の由来＞
正規のアプリ群に紛れ込む腐ったリンゴ。

＜プロフィール＞
人気のアプリを発見すると、そのアプリに酷似した『不正アプリ』を作成して、インターネット上にばらまき、正規のアプリと勘違いしてインストールしたターゲットの端末から、電話帳や登録されているクレジット番号をはじめとした、様々な個人情報を抜き取っていく。その様は、まさにゴースト界の諜報員だ。かつて、その諜報能力の高さから某英国スパイ組織に所属していたこともある。嘘である。安易に野良アプリをインストールすれば彼の思うつぼとなるところだろう。

＜事例＞
不正アプリには、利用者を盗聴するトロイの木馬、端末内の情報や位置情報をサーバーに送信するスパイウェアなどを含むものが見つかっている。

12 人の刺客：テラー
ワンクリック詐欺



＜名前の由来＞

閲覧者の恐怖心を煽り、巧みに金銭を要求。

＜プロフィール＞

人の好奇心・欲望につけ込み、様々なサイトにクリックすると金銭を要求する画面を仕込む。そのサイトを見たことを知られたくない、早く何とかしないと大変なことになるという恐怖心を巧みにあおって被害者を支配する。金銭を直接巻き上げるだけでなく、個人情報を聞き出して、カモリストとして闇サイトで売り出すこともする。本人の美学として、自発的にクリックさせて罠にかけることにこだわりがあり、ゼロクリックは邪道だと思っている。いかがわしいサイトを見たことを糊塗するために右往左往する被害者の姿をみるのが無上の喜び。

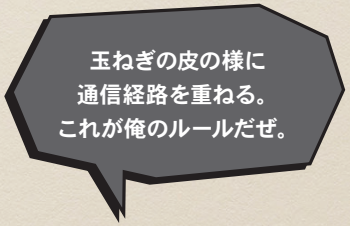
＜事例＞

スマートフォンでサイトを閲覧中、「24 時間以内にお金を支払ってください」という内容のメッセージが画面に表示され、サイト上で退会を選択したものの翌日にサイトの関係者を名乗る人物から電話があり、登録料等として金銭の支払いを請求された。

12 人の刺客：ウルトラ
Web サービスの不正ログイン

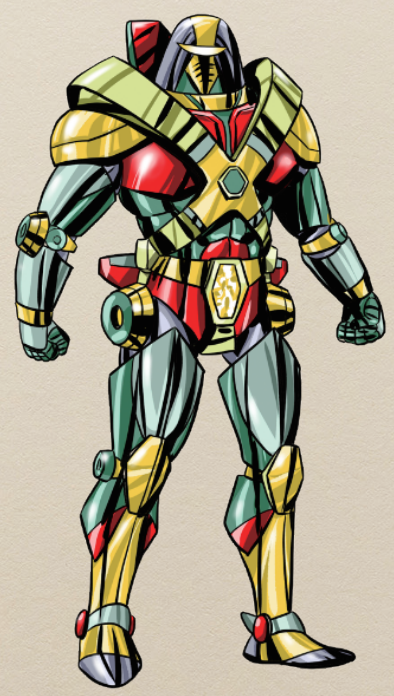
＜名前の由来＞

パスワード解読に長ける。名前は、第２次世界大戦時に解読不能と言われたエニグマの解読グループから。



＜プロフィール＞

ログイン ID の持ち主の情報を基にした、パスワード推測能力は非常に高く、周囲からは「パスワードが分からなければウルトラに聞け」と言われるほどであり、名前や誕生日、辞書に載っているような文字列をパスワードを設定していればウルトラの恰好の餌食となる。また、不正ログイン時にはアクセス元を辿られないよう、通信経路を重ねることを信条としているが、最近は経路を増やしすぎたせいで通信が重くなり、お気に入りのまとめサイトが閲覧できない状態が続くなど、信条と趣味との間で葛藤をし続けている。



＜事例＞

某ショッピングサービスでは、第３者が正規利用者のアカウント情報を用いて不正ログインし、正規利用者とは関係ない宛先へ商品を届ける不正な注文をおこなった。注文金額の総額は約 300 万円以上。

12 人の刺客：レージィ
公開された脆弱性情報の悪用

＜名前の由来＞

脆弱性情報を放置する企業への攻撃を得意とする。７つの大罪の一つ「怠惰」を見逃さない。

＜プロフィール＞

各国のセキュリティ警告情報を監視し、新たに報告された脆弱性情報を使った不正プログラムの作成を得意とする。効率重視で無駄な努力が嫌いなため、ユーザー数が多いソフトウェアの致命的な欠陥を利用することが多い。折角警告が出ているのにその情報を放置するユーザーが被害に遭うのは自業自得だと考えており容赦がない。脆弱性情報を利用するという手口の性格上、様々なプログラムに精通しており、技術力もなかなかのもの。

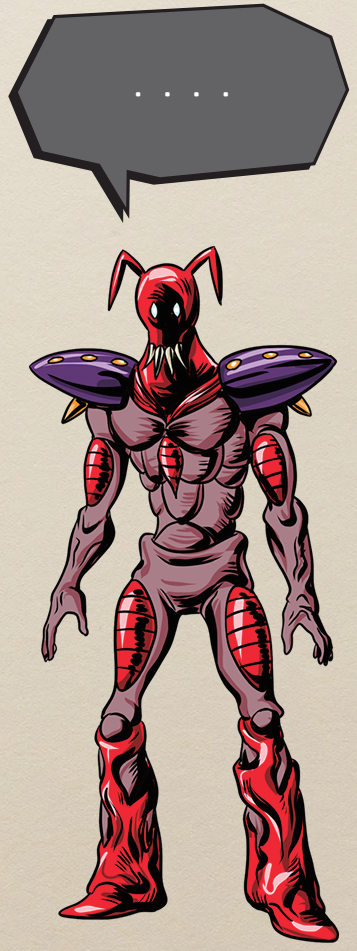
＜事例＞

広く利用されているファイル圧縮ソフトに複数の脆弱性が存在しており、一部の脆弱性が悪用された。アーカイブファイル内の画像ファイルやテキストファイルのプレビューを行おうとすると、同名のフォルダ内に配置されたスクリプトを実行させることが可能になるという脆弱性であった。

12 人の刺客：ユビキタス
ＩｏＴ機器を踏み台にした攻撃

＜名前の由来＞

ありとあらゆるＩｏＴ機器を乗っ取り、「いつでもどこでも存在」するネットの神。



＜プロフィール＞

ネットワークカメラやルーターなどの IoT 機器の乗っ取りを得意とする。乗っ取った機器は仲間に横流しすることもあり、直接・間接の影響力は大きい。セキュリティという概念が組み込まれていない旧式の機器や初期状態のまま稼働している機器は恰好の餌食となっている。感情を表すことはなく、常に淡々と乗っ取りを実行する。サイバーゴースト内でも浮いた存在で、対面していても直接話をすることはなく、チャットアプリでしか意思疎通しない。

＜事例＞

IoT 機器向けウイルスによる攻撃により、複数の大手ネットサービスが長時間にわたって接続しにくくなるトラブルが発生した。初期パスワードのまま使用されているネットワークカメラなどの IoT 機器が感染したことが原因。

MISSION 2-2

今やろう！ 5+2の備えと社内使用パソコンへの対策

OSとソフトウェアのアップデート

すぐやろう

■パソコンの OS は可能な限り自動更新にする
■インストールしているソフトウェアは、常に最新の状態にする

＜OSのアップデート＞

●パソコンの OS は可能な限り最新の状態を保つようにする。自動更新が利用できる場合は、自動更新機能を有効にする。
●サポートが終了した古い OS は使わない※。
●業務に利用するスマートフォンの OS は機種ごとの情報を常に調べて手動で更新する。

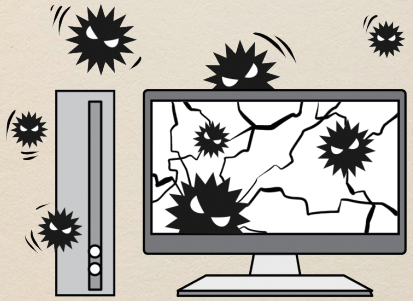
※ Windows8.1のサポートは2023年1月10日に終了。Windows10については2025年10月14日に終了。可能な限り早く最新のWindows環境への移行をお勧めします。やむを得ず継続利用する場合には、ベンダーサポートに相談するなどし、適切な対応を図ってください

＜ソフトウェアのアップデート＞

●全てのソフトウェアを最新版にする。
●自動更新機能がある場合は必ず設定する。
●自動更新が設定できないものについては、定期的に脆弱性情報をチェックする。

セキュリティ上の脆弱性が攻撃対象に！

OS は、日々新たなセキュリティ上の脆弱性が発見されています。サイバー攻撃はこの脆弱性を利用してウイルスを潜入・繁殖・拡散させます。



また、OS だけでなく、Microsoft Office 製品や Adobe Acrobat Reader など、多くの人が使用している製品のセキュリティホールも攻撃の対象となっています。OS もソフトウェアも常に最新版にしておくことが大切です。

※ Adobe Flash Playerは2020年12月31日でサポートが終了しました。直ちにアンインストールすることが、メーカーから強く推奨されています

脆弱性情報はここから入手

JPCERT コーディネーションセンターが運営・提供している脆弱性に関するメーリングリストや JVN（脆弱性対策情報ポータルサイト）などから、自分が使っているソフトウェアに関する脆弱性情報を入手だ。

MISSION 2-3

今やろう！ 5+2の備えと社内使用パソコンへの対策

セキュリティ対策ソフト・機器の導入

すぐやろう

■セキュリティ対策ソフトがインストールされているか、また最新バージョンになっているかを確認する

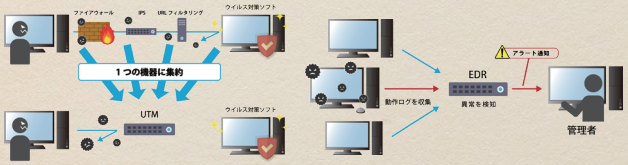
＜個別のパソコンに導入するタイプ＞

個別のパソコンに導入するセキュリティ対策ソフトには自動的に更新する機能が付いています。最近のセキュリティ対策ソフトは脆弱性スキャンや Web 脅威対策、URL フィルターなど多くの機能が付いています。

※ パソコンを購入した際に、セキュリティ対策ソフトの試用版がインストールされている場合がありますが、一定期間を過ぎると、利用できなくなったり、更新できなくなったりするものがあります

＜ネットワークの出入り口に設置するタイプ＞

オフィスのネットワークとインターネット網との間の出入り口部分に、統合型セキュリティ機器（UTM）を導入することで、二重にセキュリティを強め外部への情報漏えいや被害拡大を防ぐことができます。UTM は複数のセキュリティ機能を 1 つのハードウェアに統合し、集中的に管理します。また、EDR というシステムでは、PC やスマートフォン、サーバーなどのネットワークに接続されている末端機器（エンドポイント）における不審な動作を検知できます。



セキュリティ対策ソフトは必ず最新のものに

パソコンに脅威を与える悪意あるソフトウェア（マルウェア）は毎日たくさんの新種が登場している。そのために、セキュリティ対策ソフトを新しいマルウェアに対応できる状態に保つ必要がある。セキュリティ対策ソフトには、マルウェアを発見して駆除するプログラムを自動的に更新する機能が付いている。この機能を利用するか、更新プログラムがないか毎日チェックするかのどちらかだ。

メールの添付ファイル、ダウンロードしたファイル、USB メモリーや CD・DVD などの外部記憶媒体に格納されたファイルも、必ずセキュリティチェックを行ってから使うほうがよい。

MISSION 2-4

今やろう！ 5+2の備えと社内使用パソコンへの対策

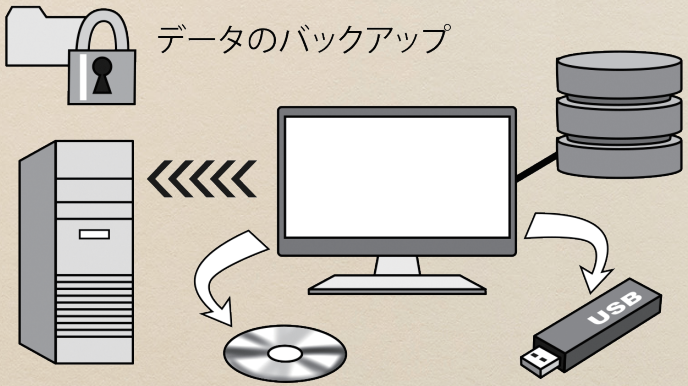
定期的なバックアップ

すぐやろう

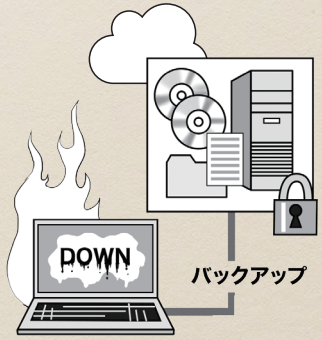
■重要データは、定期的に別媒体へバックアップを取って保存する

＜バックアップの方法＞

●ハードディスク（HDD）や DVD などの外部記憶媒体に保存。
●重要情報はネットワークと切り離して保存。
●保管方法を決めておく（保管場所や保管媒体など）。
●バックアップ媒体のセキュリティ対策も同時に実施。
●必要に応じて１つ前のデータも保存。



定期的バックアップの重要性



ビジネスで利用するデータは、削除誤りなどの人的ミスやハードウェア障害、ソフトウェア障害など多様な要因によって破損する危険があります。これらのリスクから業務データを守るためには、定期的なバックアップが不可欠です。

重要なデータのバックアップがあれば、万が一データが消失してしまっても、速やかにビジネスを復旧させることができます。

バックアップには、使っている PC が壊れたときのために重要なデータを外付けの HDD などにバックアップする方法や、クラウドへバックアップする方法があります。クラウドの場合、保管するデータセンターの場所が会社から遠いところにあったり、複数のデータセンターで相互にバックアップしていたりと、社内で保管するより安心な場合もあります。

クラウドの活用に際しては、管理担当者の選定や利用範囲と権限の明確化、利用者が使うパスワードなどの認証機能を適切に設定・管理するなどの点に留意が必須です。

Windowsのバックアップ機能を活用だ！

定期的バックアップのために市販のバックアップソフトウェアを使う方法もあるが、Windows には自動バックアップ機能が付いている。一度設定すれば指定したフォルダーを定期的にバックアップしてくれる。保管場所としてはネットワークから切り離すことができる外付けのハードディスクがお薦めだ。

MISSION 2-5

今やろう！ 5+2の備えと社内使用パソコンへの対策

パスワードの管理

すぐやろう

■パスワードを強化する
■ID・パスワードを盗まれないようにする

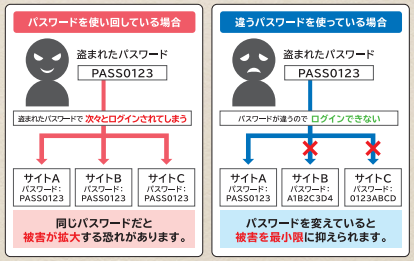
＜パスワードの強化＞

他人に推測されやすいパスワード（ニックネームや誕生日など）は使わない。

●長いパスワード（推奨は 10 桁以上）にする。
●推測しづらく自分が忘れないパスワードにする。
●他人の目に触れるような場所に、パスワードを残さない。
●いろいろな Web サービスで同じ ID・パスワードを使い回さない。

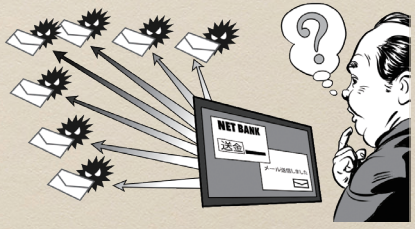
パスワードの使い回しは危険

パソコン本体はもちろん、メールや SNS、各種アプリや会員サイトなどの Web サービスを使うときに必要となるのが ID(アカウント)とパスワード。1 つのパスワードを使い回している場合、それが流出すると、ほかのサービスも乗っ取られてしまう可能性が高くなります。



対策を講じないと……

ID やパスワードを盗まれて不正にログインされることで、会社にも個人にもさまざまな被害が発生します。



・自分が利用しているインターネットバンキングから知らない口座に振り込まれた
・ショッピングサイトで勝手に高額な買い物をされた
・知らないうちに迷惑メールを大量に送信させられた

など、他人に迷惑をかけることになるケースもあります。

多要素認証でより安全に

通常は ID とパスワードを使って本人であることを確認するが、さらにもう 1 つ別のパスワードで認証する方法がさまざまなオンラインサービスで使われている。また複数の要素を使って認証する多要素認証も多く使われている（P43 を参照）。

MISSION 2-6

今やろう！ 5+2の備えと社内使用パソコンへの対策

アクセス管理

すぐやろう

■データや社内ネットワークへのアクセスについて利用者の制限やIDの管理を行う
■職務や業務、役割によってもIT機器や情報に対してアクセスの管理・制限を行う

＜ネットワークなどへのアクセス管理＞

●社内のパソコンやIT機器、ネットワークなどへアクセスする場合、職務を実施するために必要な情報に限定したり利用者を制限したりする。
●職務の変更や人事異動があったら、利用者のアクセス権限を見直す。

＜情報へのアクセス管理＞

●会社の重要情報を機密性※1、完全性※2、可用性※3の観点から評価し、情報資産の重要度を仕分ける。
●情報ごとにアクセス権を設定する。
●アクセス権の設定ではID・パスワードの使い回しを禁止する。

※1 アクセスを許可された者だけが必要な情報にアクセスできること
※2 情報および処理方法が正確であること、かつ完全であること
※3 認可された利用者が必要なときに情報および関連する資産にアクセスできること

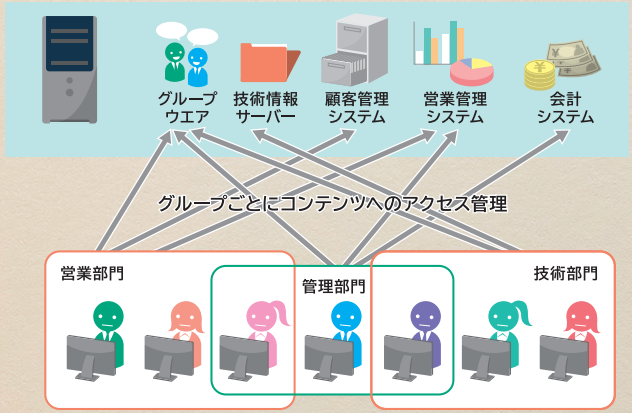
アクセス管理の例

	極秘文書	機密文書	営業データ	技術データ
役　員	○	○	△	△
部　長	△	○	△	△
営業部門	×	×	○	×
技術部門	×	×	×	○

○は読み書き可
△は閲覧のみ可
×は閲覧・編集とも不可

何が防げるの？

例えば「社外秘」の情報はアクセスできる利用者も制限する必要があります。つまり、この情報を利用できるのは誰かを決め、それ以外の人は利用不可とするのがアクセス権の設定です。
ネットワーク上の共有フォルダーやWebページにアクセス権を設定すると、特定のユーザーだけが利用するので、重要なデータを保護できます。



無線LANのアクセスに注意だ

社内で無線LAN（Wi-Fi）を使う会社が飛躍的に増えている。しかし「簡単に接続できる」「社内の人しか使わないから」といった理由で、接続時のパスワードを設定していない企業も少なくない。無線LANが社内ネットワークに直結している場合、誰でも簡単に侵入できる可能性がある。無線LANには必ずパスワードを設定し、接続できる権限を持った人間と端末を決めておくべきだ。

MISSION 2-7

今やろう！ 5+2の備えと社内使用パソコンへの対策

紛失や盗難による情報漏えい対策

すぐやろう

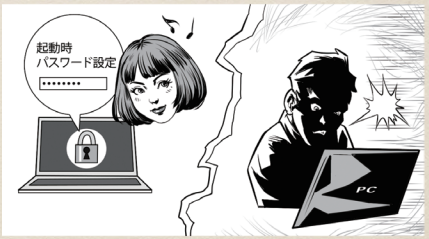
■原則は情報の持ち出し禁止
■パソコンや USB メモリーなどの記憶媒体やデータを外部に持ち出す場合、盗難・紛失などに備えて、パスワード設定や暗号化などの対策を実施する

＜情報持ち出しの対策＞

●パソコンや記憶媒体を持ち出す場合の規定を設ける。
●利用者の認証（ID･パスワード設定､USB キーや IC カード認証､指紋認証など）を行う。
●保存されているデータに対して、重要度に応じて HDD 暗号化、パスワード設定などの技術的対策を実施する。
●紛失情報が何かを正確に把握するため、持ち出し情報の一覧を作り、管理を行う。
●ノートパソコンまたはタブレット端末に保存するデータは最小限にする。
●電子媒体はケースに入れ、USB メモリーはタグ、ストラップ、鈴などを付ける。
●不要な場所に持ち出さない。
●携帯時には注意する。
・電車内では肌身離さず、網棚に置かない
・自動車内には保管しない
・他者からのぞき見されない状態で扱う

紛失・盗難対策の基本はパスワード

パソコンやモバイル端末などの情報が収められた機器は、起動の際にパスワードをかけたり、ファイルそのものにもパスワードを設定したりするなどの対策を事前に行っておくことで、盗難・紛失時に情報を簡単に見られないようにすることができます。



街なかのフリーWi-Fiに注意だ

公共施設をはじめ街なかには多くの AP（アクセスポイント）が設置されている。だが、AP すべてが万全のセキュリティ対策を講じているとは限らない。中には利便性を追求し最低限の対策に留める AP も存在し、使い方によっては通信内容を盗まれる可能性がある。

また必ずしも『暗号化＝安心』というわけではない。例えば「偽 AP」だ。この場合、暗号化に関係なく通信内容が盗まれる。

便利なフリー Wi-Fi だが利用する際、少なくとも次の点は確認だ。

・接続するフリー Wi-Fi の AP 名の確認
・接続後、ID・パスワード等の入力画面になった場合、URL が「https://」で始まっているか
・ブラウザーに鍵マークが表示されているか

特にテレワーク等、機微な情報を扱う際は不特定の AP は避けるべきだ。

MISSION 2-8

今やろう！ 5+2の備えと社内使用パソコンへの対策

テレワーク等での持ち出し・持ち込み機器対策

すぐやろう

■テレワーク等で機器を社外に持ち出す際や私物機器類を会社に持ち込む場合には、セキュリティと使い方のルール（例）を設ける

＜使い方ルール＞

情報機器の種類	順守事項
パソコン ※自宅のパソコンで業務を行う場合も含む 	・データや情報を持ち出す場合は会社ルール（P78参照）に準拠する ・ウイルス対策ソフトおよびアプリケーションなどは会社指定のものを導入 ・情報セキュリティ事故の発生に備えて担当者への連絡体制を確認する ・作業開始前に端末のOSやソフトウェアが最新か確認 ・機密情報を送信する際には暗号化する ・テレワークなどで会社機器を社外に持ち出す場合、フリーWi-Fiなどには接続しない ・基本的に私物機器は社内に無断で持ち込まない ・私物機器は社内LANへの接続を禁止する ・家族や友人への会社機器の貸与を禁止する
スマートフォン タブレット端末 携帯電話など 	・会社で指定したアプリケーション以外は使わない ・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする ・ウイルス対策ソフトなどは会社指定のものを導入 ・業務情報と私的な情報を混在させない ・家族や友人への貸与を禁止する
USBメモリー 外付けHDD	・社内パソコンに接続する前には必ずウイルス対策ソフトでチェックする
共通	・個人のメールアドレスに業務用データを添付して送信しない ・社用メールアドレスで受信したメールを個人のアドレスに転送することを禁止する

私物端末による脅威とは

●感染した私物端末が不正プログラムなどで遠隔操作される。
●私物端末でデータを持ち出される。
●感染した私物端末から社内のネットワークに感染が広がる。
●感染した私物端末のテザリング機能を利用して外部への通信が行われ、情報が漏えいする。

持ち込み機器にもウイルス対策ソフトを

私物の機器は原則として持ち込み禁止にするのが安全だが、実際には私物端末を業務に利用するニーズも増えている。その場合は持ち込みを許可する端末に必ずウイルス対策ソフトをインストールする。ソフトによっては、USB メモリーなどを差し込んだら自動的にチェックを求める機能が付いているものもある。

MISSION 2-9

今やろう！ 電子メールへの備え

電子メールの安全利用

すぐやろう

- 誤送信しないように宛先や内容、添付ファイルの確認をする
- 原則としてファイルを添付しない
- 万一必要な場合は、添付ファイルを暗号化する

＜誤送信対策＞

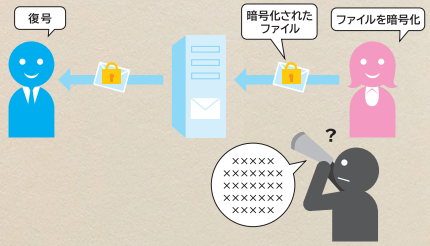
●送信ボタンを押す前に、必ず宛先を再確認する。いったん送信トレイに保存するように設定すれば、送信前に宛先を再確認できる（メールソフトとバージョンによって異なります）。

●大量のアドレスへ同報メールを送るときなどはそれぞれの受信者にアドレスが分からないように BCC を使う。

＜添付ファイルの暗号化＞

メールを安全に送受信するために添付ファイルを簡単に暗号化できます。

●アプリケーションソフトにある暗号化機能を利用する。



●圧縮・解凍ソフトの暗号化機能を利用する（パスワードを設定する）。

なお、パスワード付き ZIP ファイルなどをメール添付で送り、後からパスワードを別のメールで送ることは、「Emotet などのマルウェアに悪用される」「受信者の作業負荷を高める」といった理由で、禁止する動きが広がっています。

＜電子メールのなりすまし対策＞

ビジネスツールとして広く普及する電子メール。しかし、近年は「なりすまし」や標的型攻撃も登場しています。その対策手段の１つが「送信ドメイン認証技術」の導入です。この中には、送信元のメールサーバーの IP アドレスを認証に用いる「SPF」と、暗号化技術を用いて認証する電子署名方式の「DKIM」の２方式があり、さらに両者の結果を利用する「DMARC」があります。

対策を講じないと…

送信設定間違いによる重要情報の漏えい事故や、同報メールの送信方法の誤りによるメールアドレスの漏えい事故につながる可能性があります。

誤送信対策をする一方で、受信対策、すなわち迷惑メール対策もしっかり行いましょう。下記のサイトが参考になります。

● 迷惑メール相談センター

https://www.dekyo.or.jp/soudan/

添付ファイルはなるべく減らす！

電子メールを使ったサイバー攻撃の多くは、添付ファイルに仕込まれたウイルスや不正プログラムによるものだ。

だからビジネス上のやり取りでは添付ファイルを減らすことが、防御の第一歩だ。

ファイルを送るには Web 上で提供されている無料転送サービスも使うことができる。

添付ファイルを減らすことは、メールサーバーや通信回線の負荷の軽減にもつながる。

MISSION 2-10

今やろう！ 電子メールへの備え

標的型攻撃メールへの対応

すぐやろう

■ 不審な電子メールは開かない
■ 標的型攻撃メールを見分ける

入り口対策	
ウイルスの侵入防御	□OSやアプリケーションの脆弱性の解消 □スパムメールのフィルタリング □従業員教育 ・不審なメールを開かない ・ウイルス対策ソフトを適切に導入

▼

潜伏期間対策	
ウイルスの早期発見	□ウイルス対策ソフトによる各機器の感染チェック □不審な通信などの監視

▼

出口対策	
外部への情報漏えい防止	□統合型セキュリティ機器（UTM）によるデータ送信のチェック

巧妙な標的型攻撃メールの事例

これは、とある会社の社員に届いたメールです。その会社が加盟する健康保険組合からの「医療費通知のお知らせ」というメールだったので、添付されていた「医療費通知のお知らせ」というファイルを開きました。クリックした途端に不正プログラムが動きだし、遠隔操作ツールが実行されてしまいました。添付ファイルはワードのアイコンになっていましたが、拡張子は「doc」でも「docx」でもなく、「医療費通知のお知らせ .exe」という不正プログラムだったのです。

これは実際にあった事例です。同じように、取引先を偽装して、「請求明細」や「明細書」というタイトルの不正プログラムが送られてきた事例もあります。

※警察庁発表によると 2019 年には、確認された標的型攻撃メールは 5300 を超える

こんな添付ファイルに注意だ

・件名に「緊急」など、ことさらに添付ファイルの開封を促すメール
・日ごろメールでやり取りすることのない種類のファイルが添付されているメール
・ID やパスワードなどの入力を要求する添付ファイルや URL が記載されたメール

メールについての注意点は P 24 参照

MISSION 2-11

今やろう！ 電子メールへの備え

迷惑メール発信への対応

すぐやろう

■ ウイルス対策ソフトで迷惑メールをブロック
■ 統合型セキュリティ機器（UTM）※で迷惑メールの送信をチェック

※ P71 参照

最近ではスマートフォンなどへの迷惑メールが日常茶飯事となっているため、その危険性があまり言われなくなっていますが、迷惑メールはサイバー攻撃の予兆の１つであることを認識しましょう。

＜迷惑メールの発信は受け取り拒否につながる＞

迷惑メールと判断された送信元の IP アドレスを管理する「ブラックリスト」といわれるデータベースがあります。ウイルス対策ソフトの中には、このブラックリストを参照して、このリストに登録されたメールサーバーからのメールは受け取りを拒否する機能を持ったものもあります。もし、あなたの会社が迷惑メールを発信してブラックリストに登録され取引先で受け取り拒否されたら、事業に大きな支障が生じます。

＜万が一ブラックリストに登録されてしまったら＞

取引先で受け取り拒否されたら、拒否した理由が記されたメールが送られてきます。そこに参照したブラックリスト名と URL が記載されています。
ブラックリストを登録・管理している団体の Web サイトに行き、送信元 IP アドレスを入力し、リストから削除するための手順を確認してください。ただし、ブラックリストを管理している団体のほとんどは海外の団体ですから、削除依頼は英語で行う必要があります。

迷惑メールを発信していないかをチェック！

もし、あなたの会社のメールサーバーが迷惑メール発信の踏み台にされていると疑わしく思ったら、すぐにメールサーバーの通信量を調べよう。迷惑メールの踏み台となっている場合は、毎日数十万通のメールを発信しているはずだ。

MISSION 2-12

今やろう！ インターネット利用への備え

安全なWebサイト利用

すぐやろう

■不用意に信頼できないサイトへアクセスしないようにする
■パスワードをブラウザー※に保存しない

※ Microsoft Edge や Google Chrome などのインターネット閲覧ソフト

＜フィッシングサイト＞

●メールの送信者欄（From アドレス）は偽装できるため、なりすましメールに注意する。
●必要に応じて、金融機関が推奨するセキュリティソフトなどの導入も検討する。
●カード番号や暗証番号を入力するような依頼がメールで来ることはなく、もしそのようなメールが金融機関などから届いた場合は、送信元に電話で問い合わせたり、ホームページを見たりして真偽を確認する。

＜ワンクリック詐欺（不正請求）につながるサイト＞

●信頼できないサイトにはアクセスしない。
●アクセスしても安易なダウンロードはしない。
●ウイルス対策ソフトなどの警告画面が表示された場合は次に進まない。

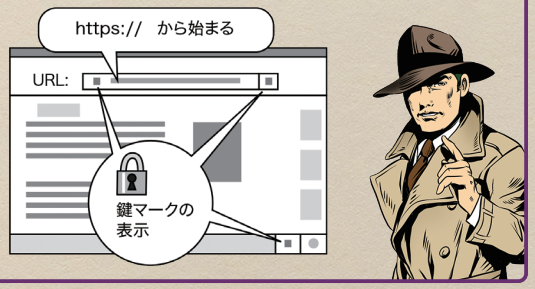
詐欺サイトにご注意を！

フィッシングサイトなどの詐欺サイトが巧妙化している。正式なものと「URL が 1 文字だけ」違うといった騙されやすいサイトもあるので要注意だ。検索などで調べた場合でも、該当のサイト名や URL スペルが合っているかをよく確かめよう。

同時に鍵マークが URL 表示窓に出ているかも確認しよう。この鍵マークをクリックするとサイト運営組織の実在を証明する電子証明書※の内容を確認することができる。しかし、鍵マークがあっても詐欺サイトの可能性がある。

また、詐欺サイトへの誘導にはメールや SMS も使われる。メールや SMS に記載された URL や電話番号を安易にクリックしてはいけない。メールソフトや Web ブラウザーにフィッシングサイト判別機能があればこれらを活用するのも 1 つの手だ。

※ 信頼できる第三者（認証局）が本人であることを証明するインターネットにおける証明書で、「運転免許証」や「印鑑証明書」のようなもの



MISSION 2-13

今やろう！ インターネット利用への備え

閲覧制限

すぐやろう

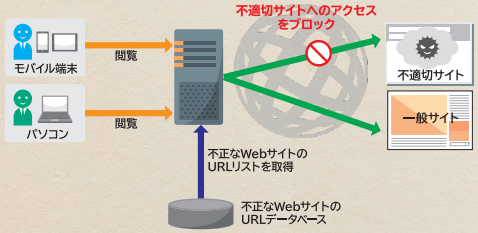
■業務に不要な Web サイトへのアクセスを制限する

＜URLフィルタリング＞

特定の URL アドレスを持つ Web サイトとのアクセスを制限します。アクセス制限には次のような方法があります。

●商用サービスとURLデータベースを使った規制

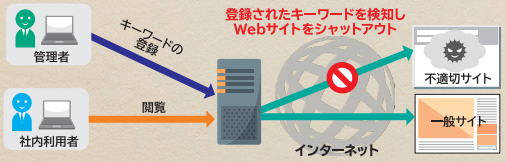
フィッシングサイトやウイルスを配布するような不正な Web サイトのアドレスを URL データベースから取得し、Web（URL）のフィルタリングを行うことで、アクセスを制限します。



＜キーワードによる規制＞

●キーワードによる規制

ブラウザーに対し入力するキーワードを管理者が事前に規制します。

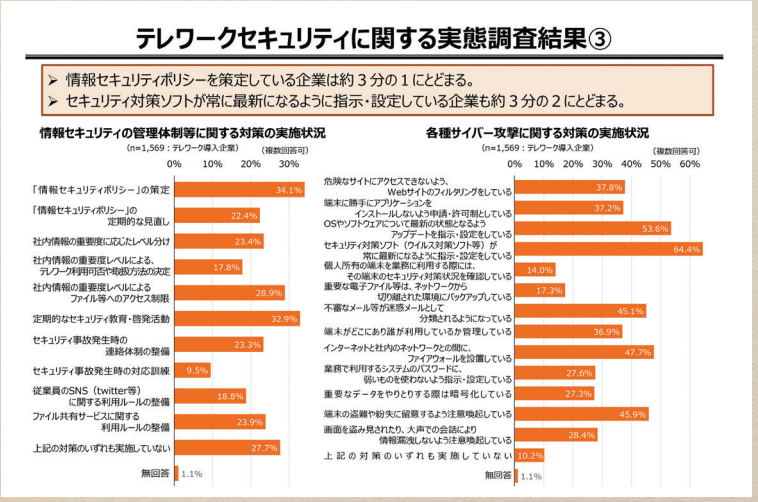


何が防げるの？

インターネットの業務外利用を制限することによって、安全でない Web サイトの利用や不正プログラムのダウンロードを防ぐことができます。

閲覧制限への対策は比較的手薄!?

2020 年の新型コロナ禍に際して、感染拡大防止の観点から多くの企業でテレワークが導入された。しかし、総務省が実施した「テレワークセキュリティに関する実態調査」(2020 年 10 月)からは、テレワーク導入に際しての経営課題がセキュリティの確保にある点が分かる。また、同調査の「各種サイバー攻撃に関する対策の実施状況」からは、Web サイトのフィルタリングなどの閲覧制限対策が比較的手薄になっている姿も浮かび上がる。



引用：総務省「テレワークセキュリティに関する実態調査」（2020 年 10 月）より

MISSION 2-14

今やろう！

重要情報の洗い出し

すぐやろう

■機密性、完全性、可用性の観点から重要度を評価する

＜情報セキュリティの三大要件＞

適切な情報管理を行うために３つの観点から重要度を評価し、重要度の高いものを優先して対策を行いましょう。

	説明	対策の例
機密性	アクセスを許可された者だけが情報にアクセスできる	情報漏えい防止、アクセス権の設定
安全性	情報と処理方法が正確でかつ完全である	改ざん防止・検出
可用性	許可された利用者が必要なときに情報と関連資産にアクセスできる	電源対策、システムの二重化

●個人情報とは

①氏名　②住所　③電話番号
④メールアドレス　⑤生年月日
⑥性別　など

●これも個人情報（紙媒体／データベース）

①各種会員の申込書
②顧客の氏名が表記される売上伝票
③顧客氏名や会員コードが入っているもの
④アンケートなど氏名を記入させるもの
⑤特定の個人を識別できるメールアドレス情報
⑥防犯・監視カメラに記録された本人と判別できる映像　など

Mission2

企業の各部門で保有している情報資産の例

経営企画部門	**経営戦略に関する情報資産** 経営計画、目標、戦略、新規事業計画、M&A計画など
総務・人事部門	**管理に関する情報資産** 従業員個人情報、マイナンバー、人事評価など
法務・知的財産部門	**知的財産などに関する情報資産** 各種契約情報、公開前の知的財産情報、共同研究情報、係争関連情報など
情報システム部門	**情報システムに関する情報資産** 社内システム情報（ユーザーID、権限情報）、システム構築情報、セキュリティ情報など
営業部門	**顧客・営業に関する情報資産** 顧客個人情報、売買契約情報、販売協力・協業先情報、仕入先情報、仕入価格情報など
研究開発部門	**研究開発技術に関する情報資産** 共同研究情報、研究者情報、素材情報、図面情報、製造技術情報、技術ノウハウなど

「サイバーセキュリティ経営ガイドライン解説書」（情報処理推進機構）より作成

MISSION 2-15

今やろう！

重要情報の保管

すぐやろう

- ■オフィスへの入退室を管理する
- ■クリアデスク・クリアスクリーンを徹底する
- ■重要情報を一元管理する
- ■保管室への入退室を管理する
- ■重要書類の持ち出しを管理する
- ■重要情報廃棄の基本ルールを徹底する

＜オフィス全体の入退室管理＞

最終退室者は以下を行います。

●全員のパソコンがシャットダウンされ、プリンターなど周辺機器の電源が切られているか確認する。

●全ての出入り口の施錠を確認する。

●退室時刻と退室者氏名を管理簿に記録する。

＜入退室管理（訪問者）＞

オフィスに見知らぬ人がいることは、セキュリティ上問題があります。整理整頓が行き届いていたとしても、見ず知らずの人に勝手に情報を盗み見されたり、持ち出されたりすることもあるかもしれません。

●訪問記録に記入してもらう。

●名刺をもらう。

●知らない人には声をかける。

●訪問した人をオフィスに１人で残さない。

＜クリアデスク・クリアスクリーンの徹底＞

●重要書類、スマートフォン、重要な情報を保存したUSBメモリーやCDなどの電子媒体を業務以外のときは机上に放置せず、クリアデスクを徹底する。

●離席時にはパソコンの画面をロックし、クリアスクリーンを徹底する。

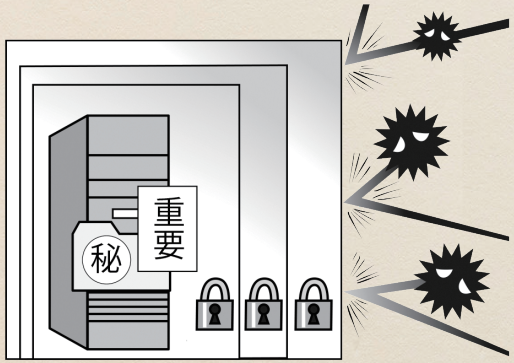
・スクリーンセーバーの起動時間を10分以内に設定し、パスワードを設定

・スリープモードの起動時間を10分以内に設定し、解除時のパスワード保護を設定

・離席時には［Windows］+［L］キーを押してパソコンをロック（Windowsの場合）

＜重要情報の一元管理＞

机の上に放置した情報は、誰かに持ち去られたり、盗み見られたりする危険にさらされています。関係者以外が見たり、触れたりすることができないように、重要情報は放置せず、一元管理する必要があります。保管場所を定め、作業に必要な場合のみ持ち出し、終了後に戻すようにしましょう。



＜保管室への入退室管理＞

●保管室への入退室者を制限する。
●施錠忘れを防ぐために入退室者と時間の記録を残す。
●机の上をチェックする。
●パソコン（モニターも）や機器の電源をチェックする。
●消灯をチェックする。
●施錠をチェックする。

＜重要書類の持ち出し＞

ルールについては P78 参照。

＜スタンドアロンのパソコンによる管理＞

ネットワークを経由した感染と情報流出を防ぐために、最重要情報についてはネットワークに接続をしていないスタンドアロンのパソコンで管理し常時ネットワークには接続しない。

＜重要情報廃棄の基本ルール＞

媒体	廃棄方法
サーバー・パソコン ※リース物件返却・売却含む	・システム担当がハードディスクを取り出し破壊 ・システム担当がデータ抹消ツールにより完全消去 ・専門のデータ消去サービスを利用する。ただし、依頼先の会社の信頼度も考慮して業者を選定する
外付け ハードディスク	・システム担当が破壊 ・システム担当がデータ抹消ツールにより完全消去
CD・DVDなどの ディスク	・利用者がシュレッダーで細断 ・利用者がディスクの両面にカッターなどでキズを入れる
USBメモリー	・システム担当がデータ抹消ツールにより完全消去
重要書類	・利用者がシュレッダーで細断 ・大量の場合はシステム担当が溶解処分を専門業者に依頼し、廃棄証明書を取得

これらの方法を企業・組織の情報資産の重要度に応じて組み合わせ、最適な方法をとることが重要です。次ページでは、情報資産の廃棄に関連して発生した近年の重大事案をご紹介します。

廃棄資産の転売で行政情報流出の危機に

2019 年 11 月、個人情報を含む神奈川県の大量の行政データが蓄積されたハードディスク（HDD）が転売される事案が明らかになった。

これは、リース契約満了によって県が返却した HDD のデータ消去（物理破壊）を委託された企業の社員がデータ消去の不十分な状態で一部を持ち出し、ネットオークションで販売したために発生した。

この事案を受け、神奈川県庁は同年 12 月 16 日に再発防止検討チームを発足。外部に出た HDD は 21 日までに全て回収し、2020 年 1 月 27 日に情報流出防止策を決定した。同月、総務省も「県情報を保存するために使用した情報機器からの情報流出防止策」を発出。原因特定とデータ抹消措置の作業完了まで県職員が立ち会い確認するなどの今後の再発に向けた具体的な防止策を明らかにした。

TOP SECRET

MISSION 3

経営者は事前に何を備えればよいのか？

MISSION 3-1

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

サイバーセキュリティ対策が経営に与える重大な影響

POINT 1 ビジネスの継続のためにはITの活用は不可欠

中小企業にとって、業務の効率化、生産の効率化、人材確保は重要な課題であり、業務、生産工程などの運用コストの削減・効率化のために、ITは大きな柱として活用されています。より一層の業務効率の改善や生産力向上を目指して、モバイル端末の活用や外部クラウドサービスの活用も進んでいます。

POINT 2 ITの活用にはサイバー攻撃などへの備えが必要

ITを活用してどんなに利便性の高いサービスを提供しても、どんなに業務を効率化しても、緊急事態（自然災害、大火災、感染症、テロ、サイバー攻撃など）で事業資産や社会的信用が失われて早期復旧ができない場合は、事業の継続が困難になり、組織の存立さえも脅かされる可能性があります。
サイバー攻撃は事前のセキュリティ対策によって、防御が可能です。

POINT 3 サイバーセキュリティ対策は経営者が自ら実行

サイバーセキュリティリスクは経営に重大な影響を及ぼす可能性がある一方で、投資効果が見えにくいものです。サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップを発揮することが必要不可欠です。

MISSION 3-2

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

サイバー攻撃を受けると企業が被る不利益

金銭の損失

顧客の個人情報や取引先などから預かった機密情報を万一漏えいした場合は、多大な損害賠償が発生します。また、インターネットバンキングの不正送金などで直接的な損失を被る企業も増えています。

顧客の喪失

サイバー攻撃を受けた企業は管理責任を問われ、社会的評価は低下し、顧客離れなど大きなダメージを受けることになります。風評被害がいつまでも続き、イメージが回復せず事業の存続が困難になる場合もあります。

業務の喪失

サイバー攻撃を受けると、被害の拡大を防止するため、システムを停止する措置が必要です。その間はメールすら使えなくなり、営業機会を喪失するとともに、社内の業務も停滞してしまいます。

従業員への影響

内部不正が容易に行えるような職場環境は、従業員のモラルを低下させます。また、従業員の個人情報が適切に保護されなければ、従業員から訴訟を起こされることも考えられます。

MISSION 3-3

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

経営者に問われる責任

POINT 1 経営者などに問われる法的責任

ITを利活用する際には、顧客の個人情報を収集・活用する、他社への差別化として技術情報を活用するなど、さまざまな重要情報を取り扱います。そのため、企業とその経営者には高い責任が求められます。

企業が個人情報などを適切に管理していなかった場合、経営者や役員、担当者は刑事罰やその他の責任を問われます。場合によっては、経営者が個人として損害賠償責任を負うこともあります。

POINT 2 関係者や社会に対する責任

情報漏えいを引き起こした企業の経営者には、法的責任だけでなく、その情報の提供者や顧客に対して損害賠償や謝罪などが求められます。

また、会社を代表して、社会に対して情報漏えいの原因や再発防止策を明らかにする義務があります。さらに、営業機会の喪失・売上高の減少・企業のイメージダウン・取引先との信頼関係の喪失などを引き起こすことにより、事業に大きなダメージを与え、経営者としての経営責任を果たすことができなくなります。

POINT 3 海外の法律への対応も必要

サイバーセキュリティへの注目は世界中で高まっており、関連法案が世界各国・地域で施行されています。近年はWebなどで個人情報を比較的容易に収集でき、海外との直接取引も容易です。事業展開の中でこうした活動を行っている場合には、諸外国の法律に抵触しないように注意が必要です。

（例）・欧州連合（EU）：EU 一般データ保護規則
（General Data Protection Regulation：GDPR）
・中華人民共和国：中国サイバーセキュリティ法（CS法）
・アメリカ合衆国：「NIST SP800-171」
（米国政府の調達品に関するセキュリティガイドライン）

POINT 4 サイバーセキュリティ対策の情報開示

５G、IoTやAIをはじめとしたICT利活用が社会・経済のあらゆる場面に浸透しつつある中、有効なサイバーセキュリティ対策を講じることは企業の経営課題となっています。加えて、企業の社会的責任を果たし、ステークホルダーからの信頼を得るためには、それらの情報を適切に開示することも重要な視点となっています。

Mission3

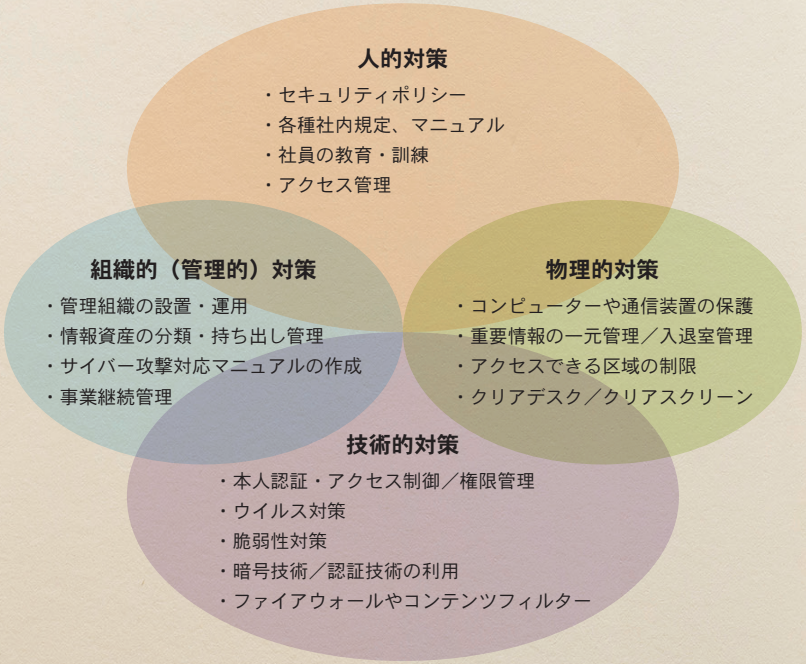
MISSION 3-4

サイバーセキュリティ対策は、事業継続を脅かすリスクの1つ

投資効果（費用対効果）を認識する

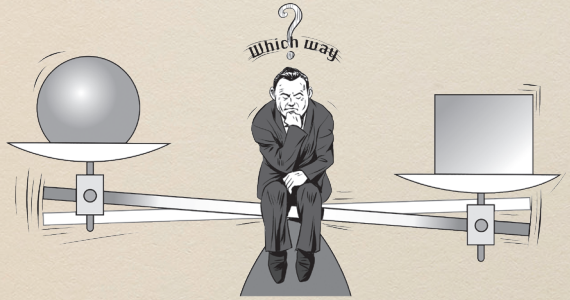
POINT 1 サイバーセキュリティ対策にかかる費用の項目

サイバー攻撃に対するセキュリティ対策には、次のような項目があります。これらの項目を実現するためには、当然費用が発生します。



POINT 2 セキュリティ対策の投資効果を考える

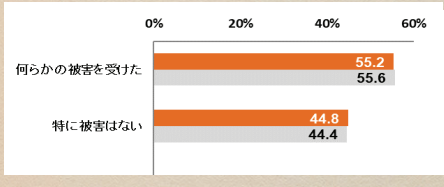
あなたの会社のインターネット接続と業務システムが1週間停止した場合のビジネスへの影響度を考えたことがありますか？　当然その間はメールもやり取りできないため、営業機会はなくなります。また、この時代にメールも送受信できないということで取引先との信頼関係もなくなります。それらの損失を数字に置き換えたものがセキュリティ対策の投資効果です。



コラム セキュリティ対策は経営上の「投資」と位置付ける！

IDC Japanが2020年1月に実施した国内企業878社の情報セキュリティ対策の実態調査結果によると、2020年度の情報セキュリティ投資見込みについて38%の企業が2019年度を上回ると回答しています。総務省「通信利用動向調査（令和元年）」においても55.2%の企業が「何らかの被害を受けた」と回答。対策には相応のコストが必要なものの、近年は中小企業を含むサプライチェーンを狙った攻撃も増えています。こうした観点も鑑み、やむを得ない「経費」でなく、ITを利活用した積極的な経営への「投資」と位置付けることが重要です。

情報通信ネットワークの利用の際に発生した過去1年間のセキュリティ状況の被害



引用：総務省「通信利用動向調査（令和元年）」より

MISSION 3-5

自社のIT活用・セキュリティ対策状況を自己診断する

ITの活用診断

POINT 1 自社のIT活用状況を診断する

IT化において中小企業が注意したいのは、「IT化の範囲を一気に広げ過ぎない」という点です。中小企業が短期間であらゆる業務にITを導入しようとすると、コストの増大だけでなく、スケジュールが煩雑になり結果的に中途半端なクオリティーのシステムになるリスクがあります。下記の診断ツールが利用できます。

IT活用診断ツール

中小企業基盤整備機構：IT経営簡易診断
情報処理推進機構：DX推進指標

POINT 2 IT活用診断のカギは費用対効果

IT導入の目的は、既存ビジネスの効率化や新ビジネス展開などであり、IT化のための投資が、それによって得られる利益を上回っている場合は、投資を削減すべきです（参考「ITガバナンス」P111参照）。

IT化による想定利益＞IT化投資額
（IT導入、運用、セキュリティ対策費）

ITおよびサイバーセキュリティに関する組織の視点6分類

【理想的】

【分類1】ITの利活用を事業戦略上に位置付け、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】

【分類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、積極的な事業戦略に組み込むところまでは位置付けていない企業

【無駄な投資】

【分類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】

【分類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

【分類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】

【分類6】ITを利用していない企業

Mission3

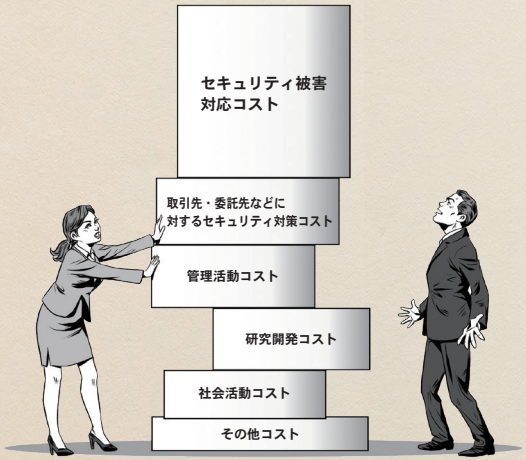
MISSION 3-6

自社のIT活用・セキュリティ対策状況を自己診断する

サイバーセキュリティ投資診断

POINT 1 サイバーセキュリティ投資（コスト）とは

サイバーセキュリティの投資（コスト）としては、P106に示した対策費用以外にも、さまざまなコストがあります。



POINT 2 サイバーセキュリティ対策はどこまでやればよいのか

これで万全というサイバーセキュリティはありません。特に、技術的対策にどれだけ投資してもリスクは残ります。管理的対策や人的対策を優先する方が効果的です。想定被害額を上回るセキュリティ対策費を費やすことは現実的ではありません。セキュリティ対策費が、セキュリティ侵害による想定被害額を上回っている場合は、対策費を削減すべきです。

セキュリティ侵害による想定被害額（経済的損失、社会的信用） ＞ **セキュリティ対策費**

問題は残ったリスク（残留リスク）によって発生した被害の想定被害額が、支出可能な対策費を上回っている場合は、事業継続が困難になりますので、支出可能な対策費に収まるように残留リスクを下げる対策を講じるか、支出可能な対策費を捻出する必要があります。

セキュリティ侵害発生時に支出可能な対策費 ＞ **残留リスクによる想定被害額**

残留リスクをどこまで許容できるかは、まさに経営者の判断です。

コラム「ITガバナンス」と6つの原則

IT活用は今や企業戦略の中で不可欠となっています。この観点から経営層には組織価値を高め、ITシステム戦略の策定や運用に必要となる組織能力である「ITガバナンス」が求められています。その成功には、経営層が次の6原則を実践することが肝要とされています。以下、要約して紹介します。

1. **責任**：役割に責任を負う人は、その遂行権限を持つ
2. **戦略**：情報システム戦略は現在と将来を考慮して、そのニーズを満たす必要がある
3. **取得**：情報システムの導入は短期・長期の両面で効果・リスク・資源のバランスを考慮した意思決定に基づく必要がある
4. **パフォーマンス**：情報システムは現在および将来のニーズを満たす必要がある
5. **適合**：情報システムは関連する全ての法律および規制に適合する必要がある
6. **人間行動**：情報システムのパフォーマンス維持に関わる人間行動を尊重する必要がある

参考：経済産業省「システム管理基準」
https://www.meti.go.jp/policy/netsecurity/sys-kansa/sys-kanri-2023.pdf

MISSION 3-7

自社のIT活用・セキュリティ対策状況を自己診断する

情報セキュリティ対策診断

POINT 1 情報セキュリティ対策を診断する

企業（組織）はセキュリティ上の脅威に取り囲まれています。

・個人、顧客、企業（組織）情報を脅威から守る

・会社内の設備を脅威から守る

情報セキュリティ対策は常に新たな脅威に対応する必要があり、継続的に自社の対策状況を診断する必要があります。

POINT 2 やってみよう！ 情報セキュリティ対策診断

・わが社のセキュリティ対策は大丈夫か？

・セキュリティ対策予算を増額したいが、どこにどう使ったらいいのか分からない

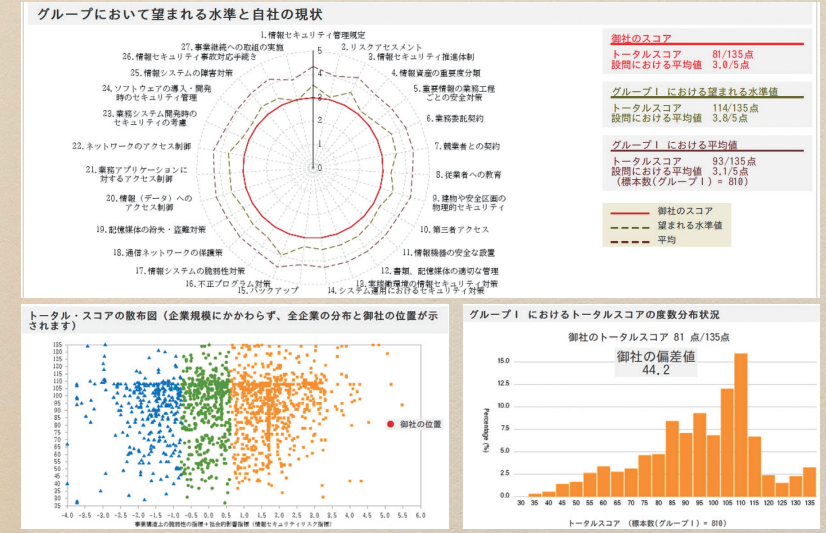
・まだ取り組んでいないセキュリティ対策を考えたい

・自社の情報セキュリティ対策状況はどこが弱点で、どこが強いのか知りたい

こうした要望に応えて、情報処理推進機構（IPA）では、「情報セキュリティ対策ベンチマーク」を提供しています。

情報セキュリティ対策ベンチマークは、設問に答えるだけで、自社のセキュリティレベルを他社との比較で診断することのできるシステムです。

散布図、レーダーチャート、スコア（点数）などの診断結果が自動的に表示されます。



「情報セキュリティ対策ベンチマーク」（IPA）より転載（一部加工）

MISSION 3-8

ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

業務の効率化、サービスの維持のために

POINT 1 守りのIT投資と攻めのIT投資

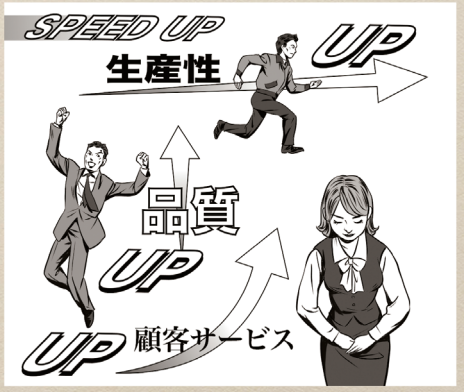
守りのIT投資という言葉を聞いたことがありますか。
従来、IT活用は業務効率化やコスト削減を目的として、定型業務の自動化に集中していました。近年、売り上げ増加を目指したIT投資を「攻めのIT投資」と呼ぶようになり、従来のIT投資を「守りのIT投資」と呼んでいます。
いわゆる、「新たな価値の創出」と「既存事業の業務生産性向上や働き方の変革」という二つのアプローチです。
「既存事業の業務生産性向上や働き方の変革」で得られた原資を「新たな価値の創出」に向けた活動に充当していくことで、企業の競争力と経営体力を高めながら、環境変化にも 対応することが可能となります。

POINT 2 業務の効率化にITを活用

経営者のみなさんが重視している経営課題の1つは、業務効率化やコスト削減です。
改善活動による業務効率化という手法は以前から展開されています。IT活用は、受発注業務や経理業務など、定型・繰り返しが多い業務プロセスを自動化、簡便化することに適しています。

POINT 3 生産性の向上やサービス向上のためにITを活用

ITを活用すれば、コスト削減だけでなく、業務のスピードアップ、品質向上、ミス低減など、生産性の向上にもつながります。また、生産状況の見える化などを通して、工程管理や生産管理など生産性を大幅に向上することも可能です。また、顧客サービスのスピードアップなどを通して、サービス力の向上にもつながります。



MISSION 3-9

ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

経営者が認識すべきサイバーセキュリティ経営3原則

原則 1　サイバーセキュリティ対策は経営者のリーダーシップで進める

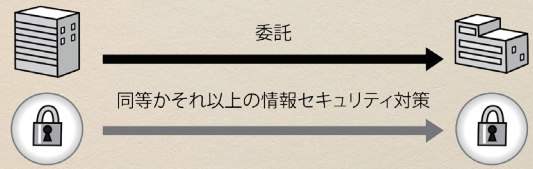
サイバー攻撃のリスクをどの程度容認するのか、セキュリティ投資をどこまでやるのか、経営者が決めなければサイバーセキュリティ対策はスタートしません。

従業員は安心して業務に集中できる環境を求めますが、利便性が低下し、面倒な作業を伴う対策には積極的に取り組めないこともあります。経営者が自らリーダーシップを発揮しなければ、サイバーセキュリティ対策は進みません。

原則 2　サプライチェーン全体にわたりサイバーセキュリティ対策に目を配る

サプライチェーンとしてつながる国内外の拠点やあらゆる委託先等においてサイバーセキュリティ対策が不十分であった場合、それらのセキュリティが弱い組織を踏み台にしたサイバー攻撃による重要情報の流出等、サプライチェーン全体の機能が停止する恐れがあります。自社の対策不十分であれば、自社がサプライチェーンの他企業にとっての加害者の立場になる可能性もあります。

対策を推進することは、サプライチェーン全体のリスクを下げるため、企業規模を問わずサプライチェーンに参加する全ての企業の経営者の責務です。



原則 3　関係者とのサイバーセキュリティに関するコミュニケーションはどんなときにも怠らない

顧客、取引先、委託先、代理店、利用者、株主などからの信頼を高めるには、普段からサイバーセキュリティ対策についての情報開示に努め、社内・社外を問わず関係者との適切なコミュニケーションを図ることが必要です。

MISSION 3-10

ビジネスを継続するために（守りのIT投資とサイバーセキュリティ対策）

経営者がやらなければならないサイバーセキュリティ経営の重要10項目

経済産業省と情報処理推進機構（IPA）がまとめた「サイバーセキュリティ経営ガイドライン Ver 3.0」を基に、経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者（CISO）」に指示すべき重要10項目をまとめました。

重要10項目とは

経営者がリーダーシップをとったセキュリティ対策の推進	**サイバーセキュリティリスクの管理体制構築**	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
		2	サイバーセキュリティリスク管理体制の構築
		3	サイバーセキュリティ対策のための資源（予算、人材等）確保
	サイバーセキュリティリスクの特定と対策の実装	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
		5	サイバーセキュリティリスクに対応するための仕組みの構築
		6	PDCAサイクルによるサイバーセキュリティ対策の継続的改善
	インシデント発生に備えた体制構築	7	インシデント発生時の緊急対応体制の整備
		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		9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
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		10	サイバーセキュリティに関する情報の収集、共有及び開示の促進

指示 1

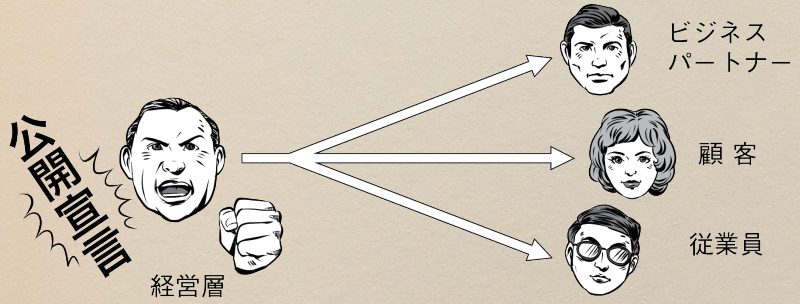
サイバーセキュリティリスクの認識、組織全体での対応方針の策定

POINT 1 指示すべきことはこれだ

・サイバーセキュリティリスクを経営リスクの1つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる

POINT 2 やるべきことはこれだ

・組織全体の対応方針を組織の内外に宣言できるよう、セキュリティポリシーを策定
・セキュリティポリシーを従業員へ周知徹底
・セキュリティポリシーを一般公開することでステークホルダーや社会に対する企業としての姿勢を示す



指示2 サイバーセキュリティリスク管理体制の構築

POINT 1 指示すべきことはこれだ

・サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる

POINT 2 やるべきことはこれだ

・CISOは、責任範囲を明確にしたサイバーセキュリティリスク管理体制を構築
・取締役、監査役はサイバーセキュリティリスク管理体制を監査
・セキュリティ・バイ・デザインの観点を踏まえて体制を構築
・経営者のリーダーシップの下で体制を構築

指示3 サイバーセキュリティ対策のための資源（予算、人材等）確保

POINT 1 指示すべきことはこれだ

・サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる

POINT 2 やるべきことはこれだ

・サイバーセキュリティ対策に必要な費用の確保
・セキュリティ対策に必要な人材の確保
・セキュリティ人材育成、キャリアパスを設計検討
・外部の組織が提供するセキュリティ研修等の活用を検討
・各部門においてもセキュリティを意識した業務遂行ができるようにする

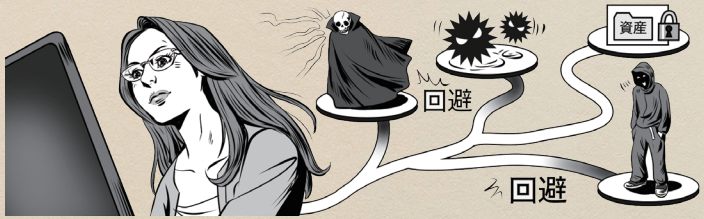
指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

POINT 1 指示すべきことはこれだ

・経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる
・その際、サイバー保険の活用や守るべき情報について専門ベンダーへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる

POINT 2 やるべきことはこれだ

・経営戦略の観点から守るべき情報を特定し把握
・守るべき情報に対して、発生しうるサイバーセキュリティリスクを把握
・把握したリスクに対して、実施するサイバーセキュリティ対策を検討（リスクの低減策、回避策、移転策）
・実施できない場合は、残留リスクとしての識別も
・法令上の取り扱いも考慮したリスクの特定と緊急時の情報の保護が行えるような対策も検討
・製品・サービス等においても、セキュリティ・バイ・デザインの観点を踏まえて、対策を考慮



指示5 サイバーセキュリティリスクに対応するための仕組みの構築

POINT 1 指示すべきことはこれだ

・サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる
・構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる

POINT 2 やるべきことはこれだ

・重要業務を行う端末、ネットワーク、システムまたはサービス（クラウドサービスを含む）には、多層防御を実施
・アクセスログや通信ログ等からサイバー攻撃を監視・検知する仕組みを構築
・従業員に対する教育を行い、適切な対応が行えるよう日頃から備える
・製品・サービス等においても、セキュリティバイデザインの観点を踏まえて、企画・設計段階からサイバーセキュリティ対策を考慮
・クラウドサービスの利用にあたっては、提供されるセキュリティ機能を考慮して選定し、アクセス制限やアカウント管理など適切な維持・管理を行う

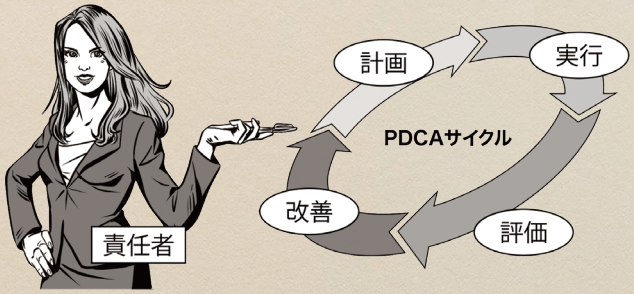
指示6 PDCAサイクルによるサイバーセキュリティ対策の継続的改善

POINT 1 指示すべきことはこれだ

・計画を確実に実施し、改善していくため、サイバーセキュリティ対策をPDCAサイクルとして実施させる
・その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる

POINT 2 やるべきことはこれだ

・サイバーセキュリティリスクに継続して対応可能な体制（プロセス）を整備する（PDCAの実施体制の整備）
・サイバーセキュリティリスク管理に関するKPIを定め、組織内の経営リスクに関する委員会においてその状況を経営者に報告する
・新たなサイバーセキュリティリスクの発見等により、追加的に対応が必要な場合には、速やかに対処方針を修正する
・サイバーセキュリティ対策の状況について、情報セキュリティ報告書、CSR報告書等への記載を通じて開示を検討する



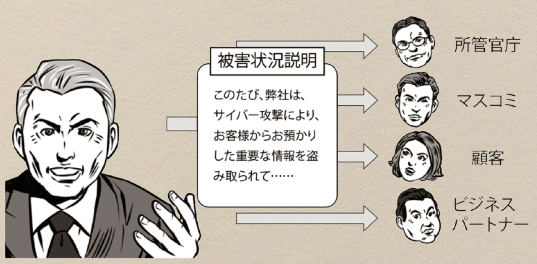
指示7 インシデント発生時の緊急対応体制の整備

POINT 1 指示すべきことはこれだ

・影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる
・被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明できる体制を整備させる

POINT 2 やるべきことはこれだ

・緊急時において、以下を実施できるような対応体制を構築する
・サイバー攻撃による被害を受けた場合、速やかな各種ログの保全や感染端末の確保等の証拠保全が行える体制を構築する
・インシデント収束後の再発防止策の策定、所管省庁等への報告手順も含めて演習を行う
・緊急連絡網として社外を含む情報開示の通知先一覧を整備し、対応に従事するメンバーに共有しておく
・緊急時に組織内各部署が速やかに協力できるよう予め取り決めをしておく
・関係法令を確認し、法的義務が履行されるよう手続きを確認しておく
・インシデントに関する被害状況、他社への影響等について経営者に報告する



指示8 インシデントによる被害に備えた事業継続・復旧体制の整備

POINT 1 指示すべきことはこれだ

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

POINT 2 やるべきことはこれだ

・業務停止等に至った場合に、以下を実施できるような復旧体制を構築する
・サイバー攻撃により業務停止に至った場合、関係機関との連携や復旧作業を実施できるよう指示する。また、対応担当者には復旧手順に従った演習を実施させる
・演習内容や組織の関係者の役割を踏まえて検討することが望ましい
・重要な業務をいつまでに復旧すべきかの目標について、組織全体として整合をとる（例えばBCPで定めている目標との整合等）
・自社内に限定せず、企業間をまたがった演習の実施も考慮する

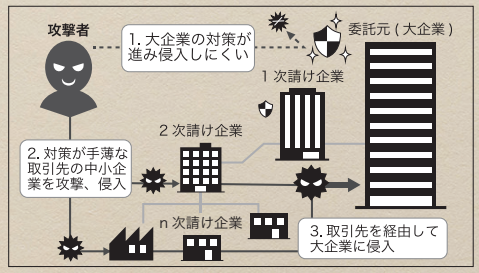
指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

POINT 1 指示すべきことはこれだ

・ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる
・システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる

POINT 2 やるべきことはこれだ

・系列企業やサプライチェーンのビジネスパートナーやシステム管理の委託先等のサイバーセキュリティ対策の内容を明確にした上で契約を交わす
・個人情報や技術情報等の重要な情報を委託先に預ける場合は、情報の安全性の確保が可能であるかどうかを定期的に確認する
・系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先等がSECURITY_ACTIONを　実施していることを確認する
・緊急時に備え、委託先がサイバー保険に加入していることが望ましい



出典：日経コンピュータ 2018年9月27日号より、一部を改変して作成

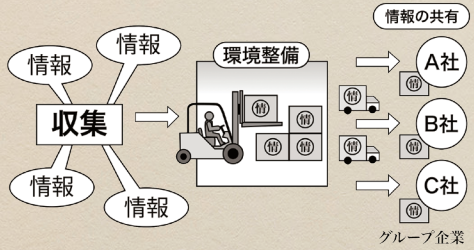
指示10 サイバーセキュリティに関する情報の収集、共有及び開示の促進

POINT 1 指示すべきことはこれだ

・社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる
・入手した情報を有効活用するための環境整備をさせる
・有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる

POINT 2 やるべきことはこれだ

・情報共有を通じたサイバー攻撃の防御につなげていくため、情報を入手するのみならず、積極的に情報を提供する
・IPAやJPCERT/CC等による脆弱性情報などの注意喚起情報を、自社のサイバーセキュリティ対策に生かす
・CSIRT間における情報共有や、日本シーサート協議会等のコミュニティ活動への参加による情報収集
・IPAに対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基準）に基づいてウイルス情報や不正アクセス情報の届出をする
・JPCERT/CCにインシデントに関する情報提供を行い、必要に応じて調整を依頼する



◆開示・報告先における注意点

開示・報告先	開示・報告時の留意点
所管官庁	・事前に先方の窓口を確認し、誰が報告するか決めておく
サイバーセキュリティ関係機関（IPA、JPCERT/CC）	・サイバー攻撃の内容、実施していた対策、被害の概要などを報告する ・同種の攻撃手法による二次被害を避けるため、至急報告する
報道機関／マスメディア	・窓口を一本化し、対外的な情報に不整合が起こらないようにする ・世評の影響も踏まえて、法務部門、広報部門などと連携し、適切な公表時期を慎重に判断する ・SNSなどのソーシャルメディアにより、社会的にどのように受け止められているか動向を確認する ・被害の状況に応じて、経営者が記者会見を行うことを想定し、公表する内容を検討する
顧客	・被害者に至急その事実を通知しおわびするとともに、個人情報（顧客情報）漏えいの場合は、詐欺や迷惑行為などの被害に遭わないように注意喚起する ・被害者に連絡する方法（メーリングリストで一斉送信など）を確認・整備しておく
ビジネスパートナー／同業者	・対処に必要な情報を速やかに関係者と共有する（外部委託先や、提携しているクレジットカード会社など） ・同業種を狙った一斉攻撃の可能性があるため、攻撃手法などを同業者間で共有する

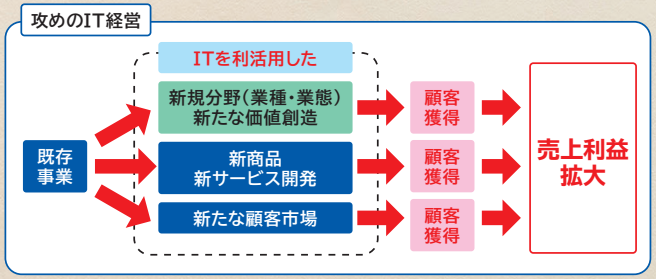
MISSION 3-11

ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

次世代技術を活用したビジネス展開

POINT 1 攻めのIT投資とは？

ITを活用して製品・サービス開発に取り組み、ビジネスモデルを変革することや新たな価値を創出することが「攻めのIT経営」です。柔軟かつ大企業に先駆けて IT関連の次世代技術やデジタル情報を活用していくことが中小企業の発展につながります。 デジタル情報や IT技術の進展を受け入れ、それを活用して顧客サービスの強化を図る企業に今大きなビジネスチャンスが訪れています。



「攻めのIT経営中小企業百選」（経済産業省）より

POINT 2 各種の支援策も充実

感染症対策や働き方改革の必要性が高まる中、テレワーク等の実現のためにデジタルツールに関心があっても、導入・定着に至らない中小企業に向けた支援も充実しています。その1つが「中小企業デジタル化応援隊事業」（2020年9月開始）。全国の中小企業とIT専門家をマッチングし、デジタル化・IT化を促進しています。

コラム DX推進はビジネス飛躍のチャンス

これから目指す社会は、「超スマート社会」いわゆる「Society5.0」

政府は、サイバー空間（仮想空間）とフィジカル空間（現実空間）を連携し、すべての物、情報、人を1つにつなぐ「サイバー・フィジカル・システム」（CPS）によって量と質の全体最適を図る社会像として「Society5.0）を提唱し、その考えが「デジタル社会の実現に向けた改革の基本方針」（2020年12月閣議決定）の背景となっています。IoTやビッグデータ、ロボット、AI、5Gなどの技術革新（いわゆる第4次産業革命）により、Society5.0は現実になりつつあります。

DXは、新たな技術を活用したビジネスの変革

新しいITおよびデジタル情報を活用して、ビジネスを変革させるのが「デジタルトランスフォーメーション（DX）」です。DXにより新時代に対応した新たなサービスを創造し、ビジネスを飛躍させることができます。

DX推進のためには、セキュリティも強化

一方、どんなに良いサービスを展開しても、セキュリティ侵害があっては事業が継続できません。ITシステム運用継続計画（IT-BCP）を明確にして、サービス設計の段階から十分なセキュリティ対策を考慮することが重要です。

中小企業のビジネスの拡大・発展に向けて

そのためには、ビジネス、デジタルのスキルとともに、セキュリティ対策のスキルを併せ持った人材が必要です。DXに対応した新たなビジネスの拡大・発展のためには、経営者は、業務や組織、企業風土の変革を含めて、明確なビジョンを持ち、「攻めのIT投資」を牽引する強いリーダーシップが求められます。

引用：内閣府「Society5.0」より

MISSION 3-12

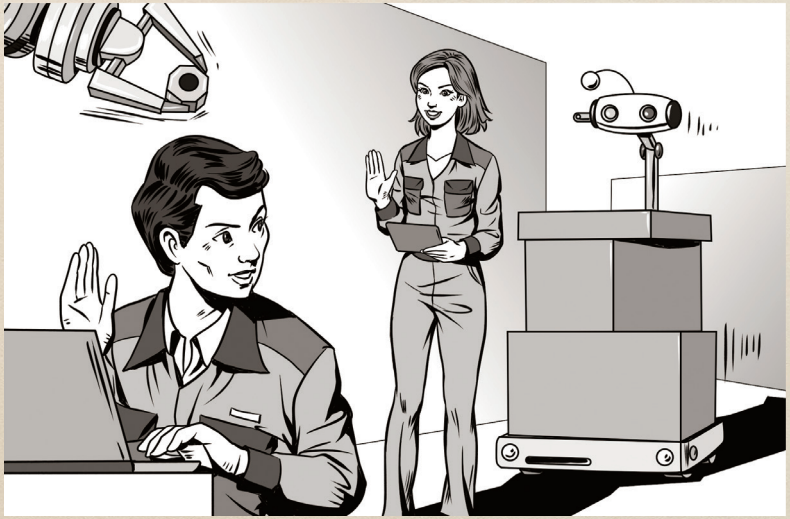
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

IoT、ビッグデータ、AI、ロボットの活用

POINT 1 業務・サービスの効率性を追求

あらゆる機器がインターネットに接続することで、人が行ってきたことをセンサー化し、センサーからの膨大なデータを瞬時に分析できます。その結果を踏まえて業務やサービスを効率的、効果的に行うことが始まっています。IoT(Internet of Things／モノのインターネット)※、ビッグデータ※、AI(Artificial Intelligence／人工知能)※、ロボットの活用は、人手不足に対応した省力化や、自動化のための投資という面でも期待されています。

※ IoT、ビッグデータはP134を、AIはP136を参照

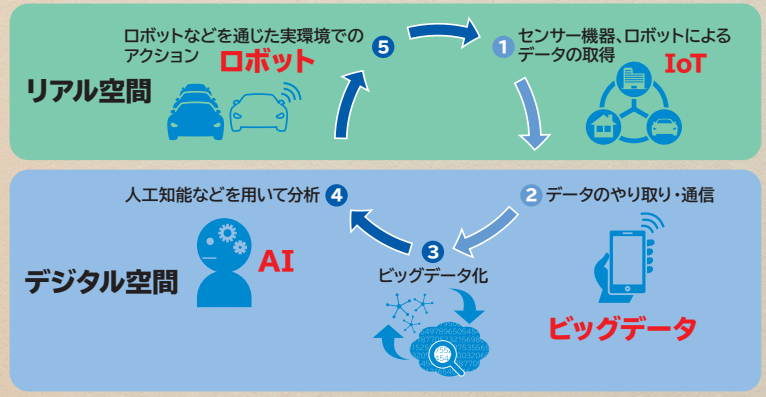


コラム IoT、ビッグデータ、AI、ロボットはつながっている

IoT、ビッグデータ、人工知能（AI）、ロボットなどの技術革新によって社会のあらゆる活動、情報がデータ化され、ネットワークによってつながることが可能な時代になりました。これらを組み合わせた機器やサービスが普及するとともに利活用を実現する事例が増えています。リアルタイムに分析を行い、新たなサービスや製品を生み出すことが可能になると、データそのものが創造の源泉になります。

商品やサービスの提供は個々のニーズに合わせてカスタマイズされ、個々のニーズとの効率的なマッチングが可能になります。AIやロボットはますます人間の役割をサポートし、部分的に代替するようになります。こうした状況にどう対応するかは、事業者にとっても重要なテーマです。商品・サービスの開発や生産、さらには流通、アフターサービスなど、事業活動に上手に取り込むことができれば、将来の成長の大きな助けになります。

急速な技術革新により、大量データの取得、分析、実行の循環が可能に



出典：「IoT、AI、ロボットに関する経済産業省の施策について」（経済産業省）より

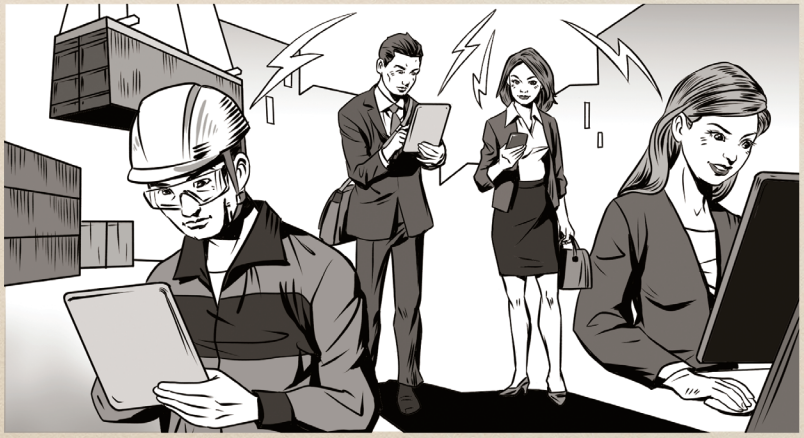
MISSION 3-13

ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

IoTが果たす役割と効果

POINT 1 IoTは中小企業にとって大きなビジネスチャンス

「5G」に代表される次世代通信技術などによってIoTデバイスは急速に普及し、2024年には10兆円を超える国内市場となる予測もあります。さらに政府が目指す「Society5.0」実現に向けた動きも追い風となり、ビジネスシーンにおいては、IoTがもたらすビッグデータ（蓄積された膨大なデータ）が新たな価値を見いだす資源として注目されています。中小企業にとっても、IoTは、例えば医療・介護、物流、製造業、交通、農業などさまざまな分野での活用が期待でき、大きなビジネスチャンスになるのです。



コラム 中堅・中小企業のIoT活用事例

製造業（東京都墨田区）社員数：50名
各種装置・機械の設計開発等

3DCADをクラウド環境で離れたところから利用可能に

事例ポイント

専門ソフトウェアの導入によって一般的なノートPCで、社内のハイスペックPCを高性能のままにリモート操作可能とした。客先や工場内など遠隔地のどこからでも社内の３DCADソフトをシームレスに利用して設計データの確認や修正が実現できる環境を構築した。

概要

- 当該企業は板金加工を中心とした金属加工による部品製造や機械装置設計開発業務に従事。設計開発では3DCAD等のソフトウェアを利用。一般的なオフィスソフトを動作させるPCスペックでは足りずハイスペックな環境が必要であり、場所も設計者の机に限定されている
- 設計に関して客先での打ち合わせや工場内確認を行う場合、3DCADのデータ参照が必要であり、設計者の机以外の場所で利用することができない。3DCADデータをプリントアウトした紙媒体を多く用いていた。修正や改編の度に紙とCADを行き来しなければならず膨大な手間が発生していた。修正ミスが起こる可能性も高い状況にあった

効果・メリット

客先や工場内など遠隔地のどこからでも社内の3DCADソフトを利用して設計データの確認や修正を迅速に反映。情報セキュリティ面から見ても、データそのものや紙媒体を持ち運ぶ必要がなくなり、情報漏えいのリスクを最小限に抑えた形で外部での設計対応が可能に。

「中堅・中小製造業のIoT活用事例一覧」（ロボット革命・産業IoTイニシアティブ協議会）より抜粋・要約して作成

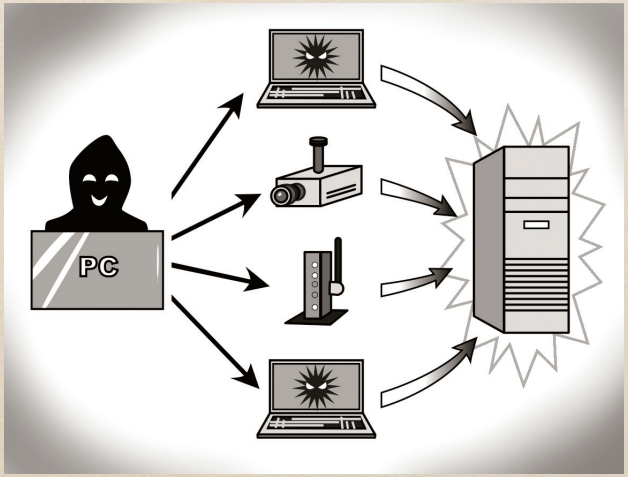
MISSION 3-14

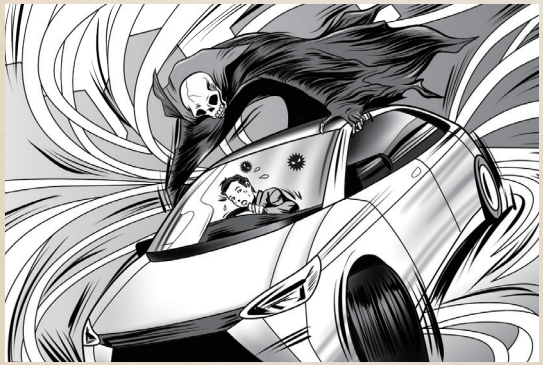
ビジネスを発展させるために(攻めのIT投資とサイバーセキュリティ対策)

IoTを活用する際のサイバーセキュリティ上の留意点

POINT 1 IoTへの脅威

次世代通信技術である5Gの進歩などを背景に、これから飛躍的に活用場面の増加が予想されるIoT機器ですが、一方でセキュリティ対策が十分とはいえないのが現状です。また、5Gが社会浸透していく中では、これまで以上にさまざまなリスクが生まれ、脅威の在り方もさらに多様化・複雑化することが予想されます。そのため、IoT機器をターゲットとしたサイバー攻撃が増大することも懸念されています。利用する際には、それを前提とした対策が欠かせません。（対策はP140参照）





インターネットから自動車の脆弱性を突かれ、ハンドルやエンジンなどが遠隔操作される

ホテルの部屋に設置してある通信機器・設備が不正に遠隔操作される

ペースメーカーや植え込み型除細動器が不正操作される

MISSION 3-15

ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

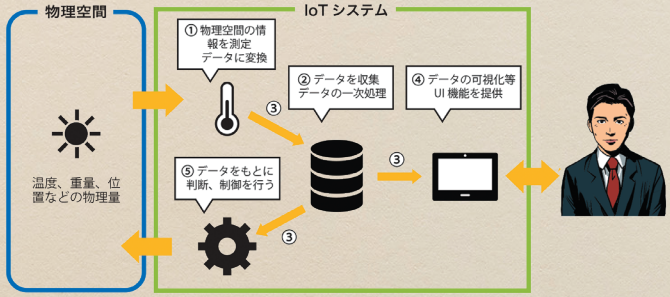
IoTを活用するための基本ルール

POINT 1 IoTのセキュリティは製造サービス提供側とサービス利用者側の双方の意識が大切

製造業を中心にIoTを利活用する動きが加速しています。

IoT機器はインターネットに接続しているネットワーク機器の一種。そのためパソコンと同様にサイバー攻撃のリスクがありますが、セキュリティ面がなおざりにされているものもあります。それらを利用するとサイバー攻撃によってシステムが使えなくなる、あるいは第三者への攻撃の踏み台となるかもしれません。

IoTのセキュリティは、製造サービス提供側とサービス利用者側の双方が注意を払わなくてはならないのです。



出典；JPCERT/CC「IoTセキュリティチェックリスト利用説明書」（2019年6月）より作成

POINT 2 IoT機器やシステム、サービスの提供にあたっての指針

■ 指針1　IoTの性質を考慮した基本方針を定める

IoT機器が原因で情報流出や社会インフラの停止などが起こった場合は、IoT機器やシステム、サービスの提供側の経営責任が問われることもあります。リスクを認識し、内部不正やミスに備えることが必要です。

■ 指針2　IoTのリスクを認識する

他の機器とつながることで、影響が広範囲になるリスクを想定することが大切です。不正操作や、廃棄機器からの情報漏えいリスクも考慮します。

■ 指針3　守るべきものを守る設計を考える

つながる相手や状況に応じてつなぎ方を判断できる設計を検討しましょう。安全安心を実現するために設計が妥当かどうかの評価も必要です。

■ 指針4　ネットワーク上での対策を考える

セキュアなゲートウェイを利用するなど、ネットワーク構成やセキュリティ機能の検討を行いましょう。初期設定もセキュリティに留意し、利用者にも注意喚起を行います。

■ 指針5　安全安心な状態を維持し、情報発信・共有を行う

出荷・リリース後も安全安心な状態を維持できるようソフトウェアをアップデートする手段を確保します。脆弱性について情報発信し、セキュリティに関する重要事項はユーザーへあらかじめ説明しましょう。

参考：IoT推進コンソーシアム「IoTセキュリティガイドラインver1.0」（平成28年7月）より

POINT 3 IoT機器の一般利用者のためのルール

ルール 1 問い合わせ窓口やサポートのない機器やサービスの購入・利用を控える

機器やサービスの問い合わせ窓口やサポートがない場合は、不都合が生じたとしても、適切に対処することが困難になります。サービスの購入・利用は控えましょう。

ルール 2 初期設定に気を付ける

機器を初めて使用する際には、IDやパスワードの設定を適切に行います。パスワードの設定では、「機器購入時のパスワードを必ず変更する」「他の人とパスワードを共有しない」「他のパスワードを使い回さない」「不要なサービスや機能は有効化しない」に気を付けましょう。また、取扱説明書などの手順に従って、自分でアップデートを実施しましょう。

ルール 3 使用しなくなった機器については電源を切る

使用しなくなった機器や不具合が生じた機器をインターネットに接続したまま放置すると、不正利用されるおそれがあります。使用しなくなったWebカメラやルーターなどをそのまま放置せず、電源プラグを抜きましょう。

ルール 4 使用しなくなった機器は必ずデータを消す

情報が他の人に漏れることのないよう、機器廃棄・下取りなどのときは、事前にデータを削除しましょう。

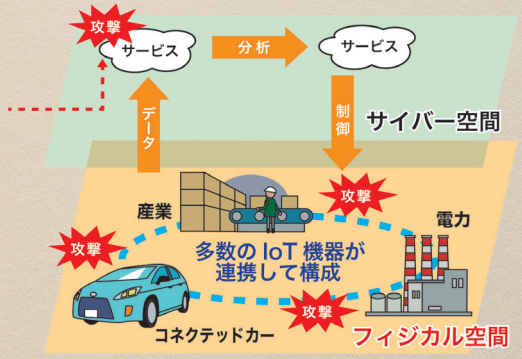
参考：「IoTセキュリティガイドライン」（総務省 経済産業省 平成28 年7月）より

POINT 4 Society5.0とIoT

Society5.0が目指す社会では、IoTによってPCやスマートフォンだけでなく家電製品や車、建物などあらゆるモノがサイバー（仮想）空間とフィジカル（現実）空間で融合されます。このため、IoT機器へのサイバー攻撃が成功すると、フィジカル空間にも影響を与える可能性が高まります。

例えば、IoT製品などに感染するウイルス「Mirai」によりWebサイトが大規模なサイバー攻撃を受けました。さらに重要インフラや生産設備への攻撃による大規模な被害も発生しています。

IoT製品をはじめ、インターネット接続される多様な機器に適切なセキュリティ対策が行われず、インターネット上に晒されアクセス可能な状態にある製品を監視し被害を防止するために、「NOTICE（National Operation Towards IoT Clean Environment）」が行われています（P47参照）。これはサイバー攻撃に悪用されるおそれのあるIoT機器の調査および当該機器の利用者への注意喚起を行うもので、総務省、国立研究開発法人情報通信研究機構（NICT）および一般社団法人ICT-ISAC が主体となって実施されています。



出典：内閣府「IoT社会に対応したサイバー・フィジカル・セキュリティ『サイバー・フィジカル・セキュリティ対策基盤』の研究開発」より作成

MISSION 3-16

ビジネスを発展させるために（攻めのIT投資とサイバーセキュリティ対策）

ビジネスを発展させるための生成AIの利活用と、それに伴うサイバーセキュリティ対策

AI（人工知能）技術の進化は目覚ましく、中小企業にとっても、業務効率化や新規事業創出の大きなチャンスをもたらしています。しかし、その恩恵を最大限に享受し、企業としての信頼を守りながら成長していくためには、AIセキュリティへの適切な対応が不可欠です。

POINT 1 AI導入の現状とメリット

AIは、「業務の自動化によるコスト削減」や「顧客データの分析による新たなサービス開発」など、具体的な成功事例が増えています。国内外の中小企業でもAI導入の動きが広がり、今後もこの流れは加速すると見込まれます。

■ メリット

・業務効率化とコスト削減：ルーティン作業の自動化により、人手不足の解消や人件費の最適化が期待できます。
・新規事業創出：データ分析を通じて、これまで見えなかった市場ニーズを発見し、新しい商品やサービスを生み出すことが可能です。

AIの活用が広がるにつれて、AI特有のセキュリティリスクも顕在化しています。データ漏洩や不正アクセスといった従来の脅威に加え、「AIモデルへの攻撃」や「AIの誤動作・判断の偏り（バイアス）」など、新たなリスクへの対応が求められます。これらのリスクを放置することは、企業の信頼性やブランドイメージを大きく損なうことにつながりかねません。また、個人情報保護法や不正競争防止法といった法規制への対応も重要です。

POINT 2 AI導入前の準備と計画

AI導入を成功させる第一歩は、その目的と達成目標（KPI）を明確にすることです。その上で、セキュリティ要件を定義し、潜在的なリスクを評価する「リスクアセスメント」を実施します。
そのためにはまず、社内体制の構築が必要です。AI活用の担当者を明確にし、責任体制を確立するとともに、委員会を設置するなどAIの公平性や透明性を確保するための組織を構築します。
また、AIサービスを選定する際には、サービス提供元（プロバイダー）のセキュリティ体制をしっかり確認することが重要です。

POINT 3 IoT機器の一般利用者のためのルール

AIは大量のデータを使って学習するため、データの管理は極めて重要です。
まず、データ管理を徹底するにあたって、データの収集・管理・保管・廃棄それぞれで対策を実施します。データ収集時には、適切な同意の取得を徹底し、不要な情報は集めないようにします。
個人情報や機密データは、匿名化・仮名化し、暗号化することが基本です。また、アクセス権限は厳密に管理します。
そして、不要になったデータは安全に削除します。
次に、データ品質と安全確保という観点より、AI学習用データが改ざんされていないかチェックし、「データポイズニング」と呼ばれる悪意のある攻撃を防ぐ対策が必要です。そして、データに偏り（バイアス）がないかを確認し、公正なAIの判断を妨げないように是正します。

※データポイズニング：攻撃者がAIモデルの学習データに悪意のあるデータや誤解を招くデータを意図的に混入させること

POINT 4 AIモデル・システムのセキュリティ対策

AIの核となるモデル自体にも対策が必要です。
まず、モデルの脆弱性対策として、AIを騙して誤作動させる「敵対的攻撃」からモデルを防御する必要があります。そのため、常にAIの判断理由を人間が理解できるようにする「透明性・説明可能性」を確保することで、モデルの挙動を適切に管理し、モデルの性能と安全性を定期的に検証・評価しましょう。
また、AIシステムへのアクセス制御と監視を徹底し、セキュリティパッチの適用や脆弱性診断を定期的に行いましょう。

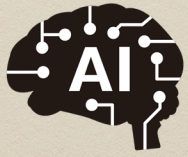
POINT 5 従業員向け教育と啓発

AIセキュリティは、担当者だけでなく、全従業員が一丸となって取り組むべき課題です。そのため、全従業員向けの基本教育を実施し、AIセキュリティに関する知識やAIを悪用したフィッシング詐欺などの手口と対策を周知・共有することが重要です。また、AI担当者を対象とし、AIサービスの適切な利用方法や社内ガイドラインの順守、不審なAIシステムへの対応方法を教育しましょう。

POINT 6 人間中心のAI社会原則

AIの適切な社会実装について方針を与えるものが「AI社会原則」です。組織でのAI活用を推進するための指標として理解しましょう。

1．人間中心の原則
2．教育・リテラシーの原則
3．プライバシー確保の原則
4．セキュリティ確保の原則
5．公正競争確保の原則
6．公平性、説明責任及び透明性の原則
7．イノベーションの原則



POINT 7 生成AIの誤情報（ハルシネーション）対策について

生成AIの誤情報（ハルシネーション）とは、AIが、実在しない法律や統計データ、架空の人物・出来事など、「もっともらしいが事実ではない情報」を生成してしまう現象のことです。この現象はAIの仕組み上、避けられないため「必ず発生するもの」として運用体制を整えることが重要です。

■ 原因

誤情報（ハルシネーション）が発生する主な原因としては、学習データの偏りや古さ、曖昧な質問や誘導的なプロンプト、AIが事実確認をせず統計的に自然な文章を生成する仕組み、利用者がAIの出力を無批判に信じてしまう過信が挙げられます。

■ 対処方法

誤情報（ハルシネーション）に対処するためには、事実かどうかを確認するファクトチェックが必要です。特に重要な意思決定や対外発信資料は、専門知識を持つ担当者が一次情報や公式ソースと突き合わせて確認しましょう。他にも異なる複数のAIに対して同じ質問を投げかけて回答を比較するクロスチェックやAIファクトチェックツールの活用などの方法があります。
誤情報（ハルシネーション）の発生を抑えるという観点から、投げかける質問をできるだけ具体的・明確にすること、そして根拠や出展を記載するように指示を加えることも有効です。

POINT 8 人間中心のAI社会原則

生成AIの誤情報（ハルシネーション）は避けられないものとして、最終責任は人間が負うという原則を徹底しましょう。AI活用のルールやガイドラインの明文化・定期的な教育や研修を行い、AIのメリットを享受することで、持続的な成長と信頼性の高い企業経営を実現しましょう。

MEMO

TOP SECRET

MISSION 4

もしもマニュアル

緊急時対応用マニュアルの作成

サイバー攻撃を受けたときのために、あらかじめ緊急時対応用マニュアルを作成しておきましょう。

作成に当たっては、情報処理推進機構（IPA）が中小企業・小規模事業者向けに提供している「中小企業の情報セキュリティ対策ガイドライン第3版」付録5の「10 情報セキュリティインシデント対応ならびに事業継続管理」を参考にすれば、自社に合った情報セキュリティポリシーを簡単に作成することができます。

緊急時対応用マニュアルは定期的に見直すことも必要です。

マニュアルに記載すべき事項

緊急時対応用マニュアルには次の項目を記載します。

記載すべき項目	記載すべき内容	本書の参照ページ
対応体制	一次対応者、対応責任者、最高責任者を決めます。	P150
サイバー攻撃被害の影響範囲と対応者	サイバー攻撃が発生した場合に対応策を決めるため、サイバー攻撃被害の影響範囲のレベルと対応者を決めます。	P150
サイバー攻撃被害の連絡および報告体制	サイバー攻撃が発生した場合の連絡・報告手順を決めます。	P151
対応手順	サイバー攻撃被害の内容ごとに、影響範囲のレベルごとの対応手順を決めます。	P151
漏えい・流出発生時の対応	社外秘または極秘情報資産の盗難、流出、紛失の場合の対応を決めます。	P152
改ざん・消失・破壊・サービス停止発生時の対応	情報資産の意図しない改ざん、消失、破壊や情報資産が必要なときに利用できない場合の対応を決めます。	P154
ウイルス感染時の初期対応	悪意のあるソフトウェアに感染した場合の対応を決めます。	P157
届け出および相談 ＜届け出・相談先＞	サイバー攻撃被害対応後に届け出または相談する機関を検討しておきます。	P159
大規模災害などによる事業中断と事業継続管理	大規模災害などの影響により事業が中断した場合に備えて、対応策を決めておきます。	P160

MISSION 4-2 基本事項の決定

ACTION 1 対応体制を決める

サイバー攻撃を受けたときに会社として対応する体制を決めます。
対応体制として一次対応者、対応責任者、最高責任者を決めます。

最高責任者	代表取締役
対応責任者	サイバー攻撃対応責任者
一次対応者	発見者または情報システム管理者

ACTION 2 サイバー攻撃被害の影響範囲と対応者を決める

サイバー攻撃被害の影響範囲のレベルと対応者を決めます。サイバー攻撃被害が発生した場合、被害レベルを判断して対応を決めます。

被害レベル	影響範囲	対応者
3	顧客、取引先、株主などに影響が及ぶとき 個人情報が漏えいしたとき	最高責任者
2	事業に影響が及ぶとき	対応責任者
1	従業員の業務遂行に影響が及ぶとき	情報システム管理者
0	影響はないが、将来においてサイバー攻撃が発生する可能性がある事象が発見されたとき	情報システム管理者

ACTION 3 サイバー攻撃被害の連絡および報告体制を決める

サイバー攻撃が発生した場合の連絡・報告手順を決めます。

レベル1以上の被害が発生した場合、発見者は以下の連絡網に従い、対応者に速やかに報告し、指示を仰ぐ。

被害レベル	最終対応者	緊急連絡先
3	最高責任者	携帯電話：090-****-**** メールアドレス：president@*****.co.jp
2	対応責任者	携帯電話：090-****-**** メールアドレス：incident@*****.co.jp
1	情報システム管理者	携帯電話：090-****-**** メールアドレス：system@*****.co.jp

ACTION 4 対応手順を決める

サイバー攻撃を認知した際、確認事項や連絡系統を一元化し迅速な対応をするための対応手順を決めます。

区分	サイバー攻撃被害の状況
漏えい・流出	社外秘または極秘情報資産の盗難、流出、紛失
改ざん・消失・破壊 サービス停止	情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない
ウイルス感染	悪意のあるソフトウェアに感染

Mission4

対応手順1

漏えい・流出発生時の対応

被害レベル3の場合

STEP1	発生の報告	漏えいや流出の事実を発見したり、外部から連絡を受けたりした者は即座に対応責任者および最高責任者に報告します。	発見者、一次対応者
STEP2	原因の特定と二次被害の防止	対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行します。	対応責任者
STEP3	被害者対応の準備	個人情報が流出した場合、漏えい・流出した個人情報の本人（被害者）への対応を準備します。	対応責任者
STEP4	問い合わせ対応の準備	被害者本人や関係先からの問い合わせ対応を準備します。	対応責任者
STEP5	報道発表の準備	対応責任者は影響範囲・被害の大きさによって総務部に報道発表の準備を申請します。	対応責任者
STEP6	被害届の提出	対応責任者はサイバー攻撃などの不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出ます。	対応責任者
STEP7	監督官庁への届け出	対応責任者は個人情報の漏えいの場合には監督官庁に届け出ます。	対応責任者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

被害レベル2の場合

STEP1	発生の報告	発見者は発見次第、システム管理者に報告します。	発見者
STEP2	漏えい先の調査と報告	システム管理者は漏えい先を調査し、対応責任者に報告します。	システム管理者
STEP3	社内への通知	システム管理者は社内関係者に周知します。	システム管理者

対応手順2

改ざん・消失・破壊・サービス停止発生時の対応

被害レベル3の場合

STEP1	発生の報告	発見者は即座に対応責任者および最高責任者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者
	対応結果および対策を公表	最高責任者は、社内および影響範囲の全ての組織・人に対応結果および対策を公表します。	最高責任者

被害レベル2の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者
STEP3	社内周知と担当部署への連絡	対応責任者は社内に周知するとともに総務部情報システム担当に連絡します。	対応責任者
STEP4	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP5	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

被害レベル1の場合

STEP1	発生の報告	発見者はシステム管理者に報告します。	発見者
STEP2	原因の特定と応急措置の実施	システム管理者は原因を特定し、応急処置を実行します。	システム管理者

STEP3	復旧措置	電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行します。	システム管理者
		機器の場合はシステム管理者が修理、復旧、交換などの手続きを行います。	システム管理者
		書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復します。	情報セキュリティ部門責任者
STEP4	原因対策の実施	システム管理者は原因対策を実施します。	システム管理者

ACTION 4 被害レベル0の場合

発見者は発見次第、発生可能性のあるサイバー攻撃と想定される被害をシステム管理者に報告

MISSION 4-5

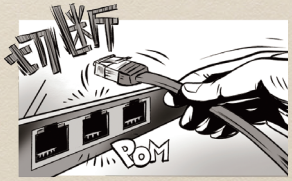
対応手順3

ウイルス感染時の初期対応

ACTION 1 従業員が対応可能な場合

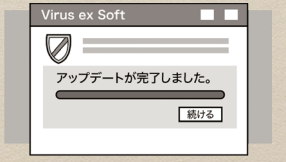
従業員は、業務に利用しているパソコン、サーバーまたはスマートフォン、タブレット（以下「コンピューター」といいます）がウイルスに感染した場合には、次の手順を実行します。

STEP1 ネットワークからコンピューターを切断します。

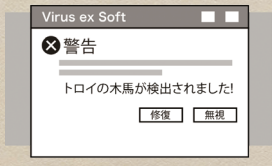


STEP2 システム管理者に連絡します。

STEP3 ウイルス対策ソフトの定義ファイルを最新版に更新します。



STEP4 ウイルス対策ソフトを実行しウイルス名を確認します。



STEP5 ウイルス対策ソフトで駆除可能な場合は駆除します。

STEP6 駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認します。

STEP7 システム管理者に報告します。

ACTION 2 従業員が対応できない場合

従業員自身で対応できないと判断する場合はシステム管理者に問い合わせます。

・ウイルス対策ソフトで駆除できない
・システムファイルが破壊・改ざんされている
・ファイルが改ざん・暗号化・削除されている

MISSION 4-6 対応手順4 届け出および相談

システム管理者は、サイバー攻撃被害への対応後に以下の機関への届け出または相談を検討します。

＜届け出・相談先＞

独立行政法人 情報処理推進機構セキュリティセンター（IPA/ISEC）

ウイルスにかかってしまったり、不正アクセスをされたりした場合は、下記URLを参照してにIPA/ISECに届け出をしてください。
https://www.ipa.go.jp/security/todokede/crack-virus/about.html

IPA/ISECでは、情報セキュリティの相談窓口も開設しています。
https://www.ipa.go.jp/security/anshin/about.html

個人情報保護委員会

個人情報や特定個人情報（マイナンバー）の漏えいなどの事案が発覚した場合は、速やかに下記URLを参照して個人情報保護委員会などに対して報告してください。
https://www.ppc.go.jp/

大規模災害などによる事業中断と事業継続管理

企業にとって、大規模な自然災害をはじめとする緊急事態に備えた事業継続のための計画（BCP）を策定することはとても重要です。

一方、情報システムの活用が進むこれからは、このBCPにプラスして情報システム運用継続計画（IT-BCP）も大切となってきています。

STEP1　環境整備

基本方針を決定し、実施・運用体制を構築する。

STEP2　情報の収集・前提の整理

危機的事象を特定し、特定した事象の顕在化がもたらす被害状況を想定する。

STEP3　分析、課題の抽出

情報システムの復旧優先度を設定し、運用継続に必要なリソースを整理する。

STEP4　計画の策定

事前対策計画、非常時の対応計画、教育訓練計画・維持改善計画を検討する。

STEP5　実施（評価・改善）

平常時にIT-BCPが発動されることはないため、定期的な訓練を通じて組織・個人における習熟度を維持し、計画に問題があれば見直しを図る。

※IT-BCPの策定には「情報システム部門」と「業務部門」等の関連部門間で適切な連携を図り、既存のBCPとの整合性を確保することが大切です
参考：IT-BCP 策定モデル（内閣官房情報セキュリティセンター（NISC））

＜各作業の進め方と留意事項＞

STEP 1 ：環境整備

ACTION 1 基本方針の決定

計画の適用範囲と基本方針を定める。
（検討事項・考え方）
・代替拠点に設置されている情報システムを活用する場合、業務を実施するためにそれらが危機的事象発生時に利用可能であるか。
・適用範囲には非常時優先業務を支える情報システムである、メールやWeb、SNS 等の情報収集・共有・伝達手段、基幹LAN やクラウドサービス等の外部サービスにアクセスするための認証基盤等を含める。

ACTION 2 策定・運用体制の構築

計画の策定・運用に係る体制を構築する。
（検討事項・考え方）
・基本方針で定めた適用範囲を踏まえて必要な担当者を定める。また、各部署との連携体制を構築する。
・代替拠点に設置されている情報システムを活用する場合、業務を実施するためにそれらが危機的事象発生時に利用可能であるか。

STEP 2 ：情報の収集・前提の整理

ACTION 1 危機的事象の特定

計画の対象とする危機的事象を調査・検討し、特定する。
（検討事項・考え方）
・危機的事象発生時の前提条件は厳しい条件を想定し、必要な検討に漏れが生じないようにする。

・外部環境等の変化に応じ、情報システム運用継続計画が対象とする危機的事象は変化することを考慮する。

ACTION 2 被害状況の想定

危機的事象が発生した場合の情報システムの被害状況を想定する。
（検討事項・考え方）
・情報システムの設置拠点が複数存在する場合は、拠点ごとに環境が異なることを考慮し、拠点ごとの被害を想定する。なお、クラウドサービス等の外部サービスを利用している場合は、外部サービス事業者のサービス提供環境も考慮する。
・情報システムの抱えるリスクの算定が複雑となることから、細かすぎる被害想定を避ける。

STEP 3 ：分析、課題の抽出

ACTION 1 復旧優先度の設定

非常時優先業務を確認した上で、対象の情報システムとの関連性を整理する。非常時優先業務の目標復旧時間と、情報システム停止時の影響や代替手段を踏まえ、情報システムの復旧優先度を設定する。
（検討事項・考え方）
・個々の業務、情報システムごとに対応を考えるのではなく、情報システムの運用において非常時優先業務をどのように継続させるかの検討を行う。
・時間の経過とともに対象の情報システムの重要性が変わる可能性があることから、復旧優先度は定期的に見直す。

ACTION 2 必要な構成要素の整理

危機的事象発生時に必要な情報システムを支える構成要素を整理する。構成要素ごとに、情報システムの復旧優先度に応じた目標対策レベルを設定する。
（検討事項・考え方）
・非常時優先業務を支える情報システム、部署横断で連携する重要な情報システム、メールやWeb、SNS 等の情報収集・共有・伝達手段、基幹LANや外部サービス及びこれらにアクセスするための認証基盤を対象として、情報システムを支える構成要素を明確化する。
・復旧優先度に応じて必要となる対策を、現状の情報システム環境を踏まえながら実施していくことに留意する。

STEP 4 ：計画の策定

ACTION 1 事前対策の計画とその実施

現状の対策を確認し、リスクを評価、整理する。リスクの評価を踏まえ、「事前対策計画」を作成する。
（検討事項・考え方）
・情報システムの運用継続作業を困難とさせるリスクについて評価しておく。
・現状の対策を目標対策レベルに近づけるための方針（事前対策実施方針）を情報システムごとに定める。

ACTION 2 危機的事象発生時の対応計画の検討

現危機的事象発生時に情報システムの運用を継続させるために必要となる体制・役割を決定し、具体的な対応方法を対応計画として整理する。

Mission4

（検討事項・考え方）
・危機的事象発生時に責任者及び担当者に連絡がとれない可能性を考慮し、代行者を定める。
・知見を有している前任者等による応援も考慮する。
・特定の担当者に作業が集中しないように配慮し、危機的事象発生の影響が長期化することが想定される場合は、担当者が交代で勤務ができるようなチーム編成による交代制勤務等を考慮する。

ACTION 3 教育訓練・維持改善の計画とその実施

対応計画の実効性を高めるため、「教育訓練計画」を作成する。また定期的に見直しを行うための「維持改善計画」を作成する。
（検討事項・考え方）
・情報システムの運用体制に委託先が含まれる場合には、教育訓練計画の実施対象者として委託先を含めて検討する。
・見直し時期は予算編成の検討時期を踏まえ設定することに留意する。

STEP 5 ：実施（評価・改善）

・運用段階においては、策定された事前対策計画と教育訓練計画に則り、計画の実施と維持改善を行う。また、適宜見直しを行い、計画の陳腐化を防ぎ、常に計画の最新化を維持するように努める。
・計画の見直し時には、関連部局や組織のレビューを必要に応じて受ける。

参考：政府機関等における情報システム運用継続計画ガイドライン第３版（内閣官房情報セキュリティセンター（NISC））

MISSION 4-8 サイバーレジリエンスとは

現代のサイバー攻撃は、もはや「防げる」レベルを超え、企業の存続を脅かす主要なリスクとなっています。特にリソースが限られる中小企業にとって、一度のランサムウェア感染やシステム停止は致命的になりかねません。
中小企業の経営者・担当者向けに、従来の「防御」を超えた新しい考え方である「サイバーレジリエンス」の概念、その重要性、そしてそれを確立するために経営層が果たすべき役割を含めた具体的な行動計画を理解しましょう。

POINT 1 サイバーレジリエンスとは何か

サイバーレジリエンスとは、企業がサイバー攻撃やシステム障害といった多様な事態に直面した際に、被害を最小限に食い止め、迅速に回復し、事業を継続する能力のことです。

区分	従来のセキュリティ	サイバーレジリエンス
基本的な考え方	侵入を完全に防ぐ	侵入されることを前提とし、被害を最小化する
戦略的重点	予防	検知、対応、復旧、適応

この考え方は、企業が有害なサイバー事象が発生したとしても、中核的なビジネス活動を継続的に提供できる能力を確保するための戦略です。

POINT 2 サイバーレジリエンスの重要性

現代のサイバー攻撃は、もはや「防げる」レベルを超え、企業の存続を脅かす主要なリスクとなっています。特にリソースが限られる中小企業にとって、一度のランサムウェア感染やシステム停止は致命的になりかねません。

■ 攻撃を受ける前提での防御（弾力性）

攻撃を完全に防ぐことは困難なため、「侵入を許容しつつ、いかに迅速に立ち直れるか」に戦略の重点を置く必要があります。これが企業の「弾力性」です。攻撃を防ぐための壁を高くするだけではなく、壁が破られた後のための防火シャッターとして、ネットワーク隔離や検知システムといった対策を準備して

■ 復旧の要としてのバックアップ

ランサムウェア攻撃を受けた場合、システムとデータが暗号化され、使用不能になります。この際、身代金を払わずに事業を再開するためにも、バックアップが重要な手段です。なお、バックアップデータも攻撃者に暗号化されないよう、ネットワークから切り離してオフラインで保管しましょう。

POINT 3 経営者の参画の重要性

サイバーレジリエンスは、IT部門任せでは機能しません。経営層の責任として、役割を果たす必要があります。

■ 戦略的な意思決定

「事業が停止してからいつまでに復旧させるか（目標復旧時間：RTO）」、「どの程度のデータ損失なら許容できるか（RPO）」といった目標設定は、ビジネス上の判断であり、経営層が責任をもって決定する必要があります。

■ 全社的な体制構築

セキュリティへの投資予算、従業員教育の義務化、インシデント発生時の社内外への報告・対応体制の構築は、経営層からのトップダウンの指示が不可欠です。サイバーセキュリティを組織のミッションやリスク管理戦略に統合することが求められます。

POINT 4 レジリエンス確立のために企業が実施すべきこと

サイバーレジリエンス能力を育成・強化するためには、次の6つの機能からなる体系的なアプローチを採用することが重要です。

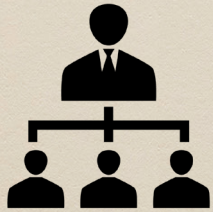
出典：NIST「The NIST Cybersecurity Framework (CSF) 2.0」より作成

Mission4

- **統治（Govern）**：経営戦略との整合性の確保。経営層が関与し、責任者と予算を明確にする。
- **特定（Identify）**：守るべき資産の把握。事業に不可欠なシステムとデータ（顧客情報など）を特定し、リスク評価を行う。
- **防御（Protect）**：予防的対策の実装。OSやソフトウェアのパッチ適用を徹底し、VPN接続や重要なシステムへのアクセスには多要素認証（MFA）を導入する。
- **検知（Detect）**：異常の早期発見。アクセスログを確実に取得・監視し、不審な挙動を素早く検知する体制を構築する。
- **対応（Respond）**：被害の封じ込めと分析。インシデント発生時の初動対応計画（誰が、何を、誰に報告するか）を策定し、定期的に訓練を実施する。
- **復旧（Recover）**：事業の迅速な回復。策定したRTO/RPOに基づき、バックアップを定期的に実行し、必ずネットワークから隔離して保管する。

POINT 5 組織としてのサイバーレジリエンス

サイバーレジリエンスは、中小企業が現代のサイバー脅威から事業を守り抜くための「保険であり、同時に競争力を維持するための「投資」です。重要なのは、「防御の限界」を認識し、経営層がリスクと復旧目標を決定し、バックアップと訓練を通じて「迅速に立ち直る能力」を組織全体で身につけることです。この継続的な改善サイクルこそが、攻撃に打ち勝つ、しなやかな企業体質の構築につながります。

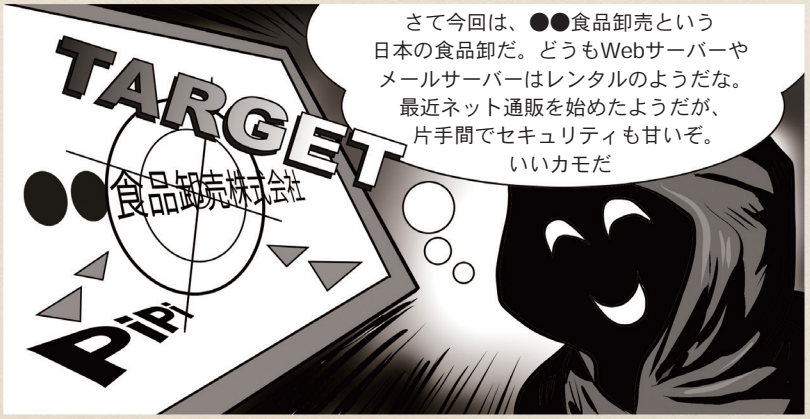


TOP SECRET

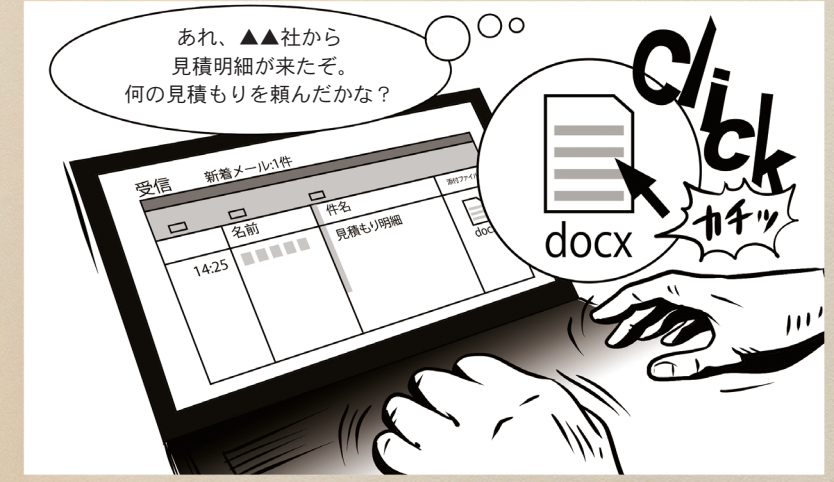
MISSION 5

やってみよう! サイバー攻撃対策シミュレーション

サイバー攻撃前夜



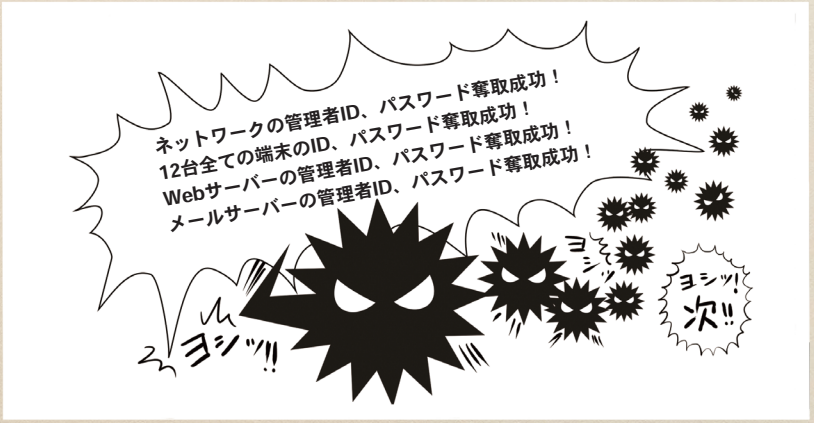
攻撃発生その瞬間



Mission5

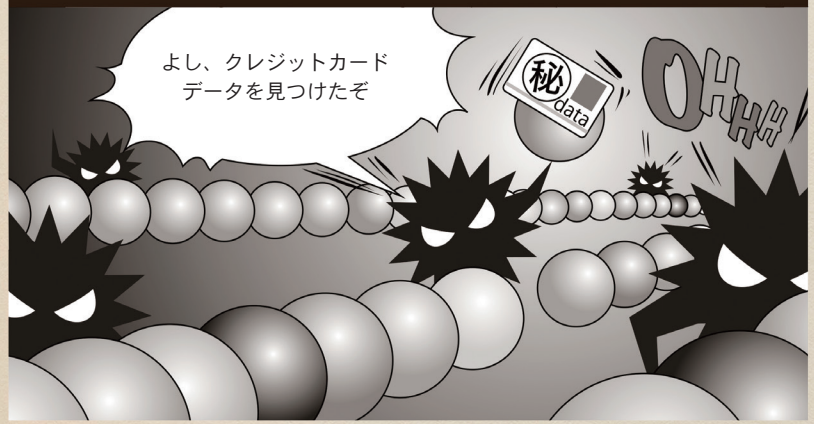
サイバー攻撃直後

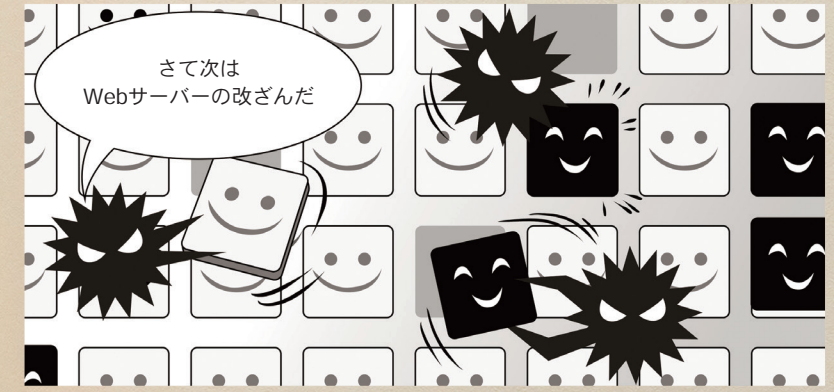
よおし、標的型メールを開いたぞ。
さあ、活動開始だ



潜入拡大

クレジットカードの個人情報を取得。クレジットカードを自由に使うために
セキュリティコードなどを盗み取る





顧客への被害の拡大
取引先への被害の拡大

フィッシングサイトでセキュリティコード情報を窃取。
取得した個人情報を使ってキャッシングで現金を引き出す

●●食品卸売株式会社からの請求明細のメールを装い、
標的型メールの攻撃

サイバー攻撃の発覚

さあ、あなたならどうしますか？

ACTION 1 原因と被害範囲の調査を自社で実施できるかどうかを判断する

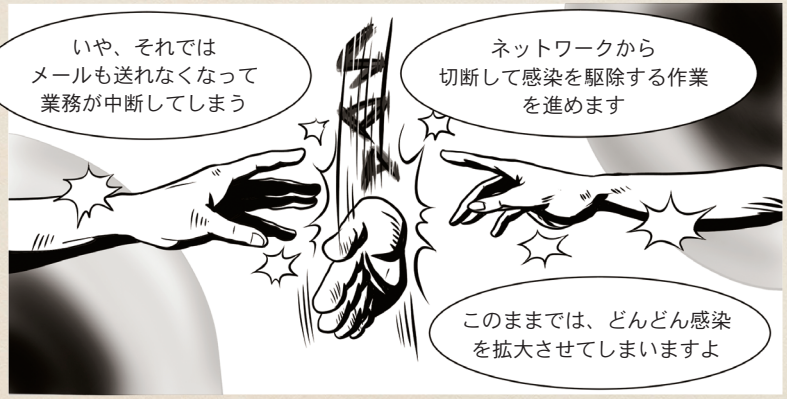
標的型攻撃に代表される企業ネットワークに対する外部からの攻撃や、Webアプリケーションの改ざん、不正アクセスなどのサイバー攻撃の発生時に、本格的な調査（フォレンジック〈法的〉調査、ウイルスの不正プログラムの解析、ログの分析など）、復旧支援と再発防止策のアドバイスを支援するセキュリティ会社があります。

ACTION 2 原因と被害範囲の調査を依頼する

SCENE 07 原因が判明 ウイルス感染が原因

さあ、あなたならどうしますか？

ACTION 1 ネットワークからの切断



ACTION 2 感染ウイルス・不正プログラムの駆除

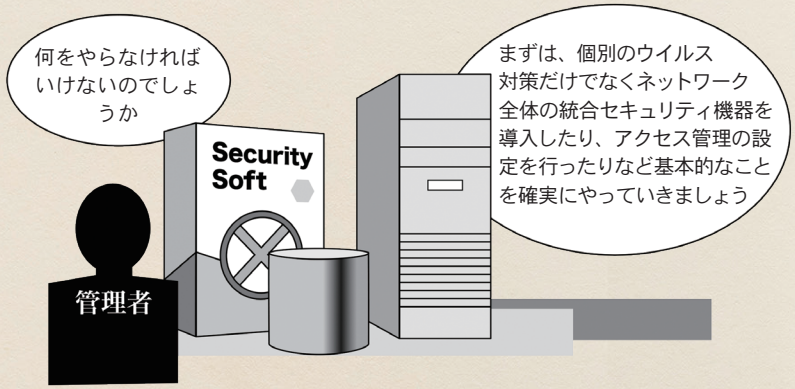
- OS は最新バージョン自動更新をチェック
- アプリケーションも最新の状態に
- データは必ずウイルス対策ソフトで複数チェック

ACTION 3 各機関への連絡・関係先への報告

SCENE 08 再発防止策の作成

さあ、あなたならどうしますか？

ACTION 1 物理的および環境的セキュリティを再検討する



ACTION 2 社員教育など人的セキュリティを強化する

SCENE 09 復旧回復

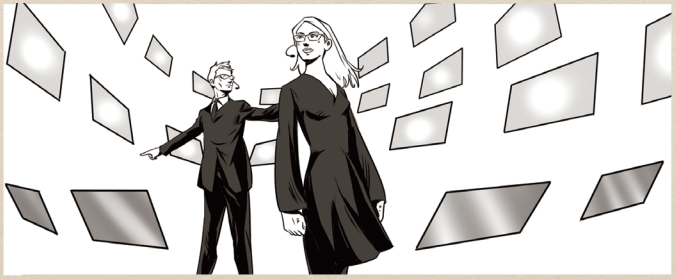
さあ、あなたならどうしますか？

ACTION 1 情報漏えいについての発表

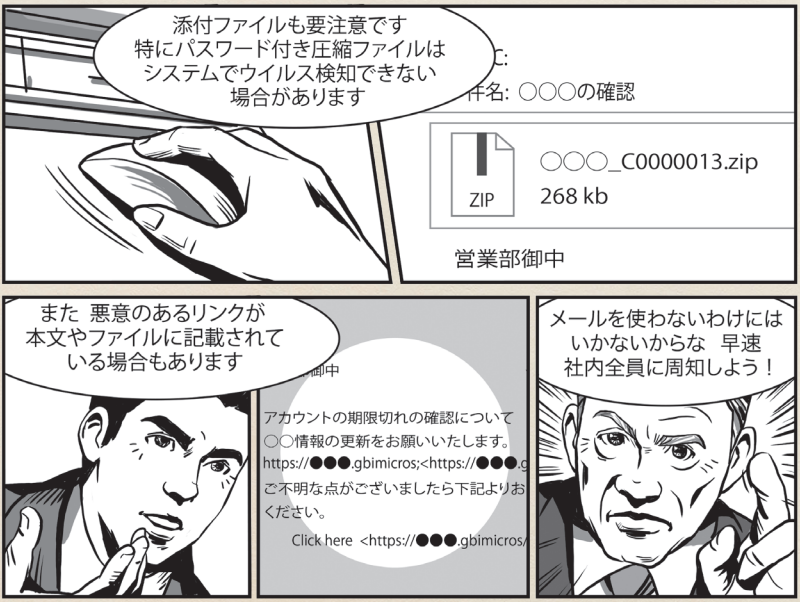
ACTION 2 再発防止の恒久的対策

ACTION 3 不審なログオンや通信の監視

不自然な通信をしているプログラムがないか、外部から不正なログオンが行われていないか、監視します。



ATTENTION 大切なのは社内意識の向上！
～感染を狙うメールに注意～



経営者にとってメールの安全な運用は他人事ではない!

コンピューターウイルスやマルウェアは、以下のような経路から感染する。

・USB 機器からの感染
・ファイル共有、アプリからの感染
・ウェブ閲覧からの感染　など

これらは、システム設定などにより使用を禁止することで回避できる。しかし、ビジネスツールであるメールを一切禁止することは現実的ではない。加えて、メールを悪用した攻撃の中には人の心理的な隙や行動ミスをついた、システム設定だけでは対応が難しい手口も存在する。

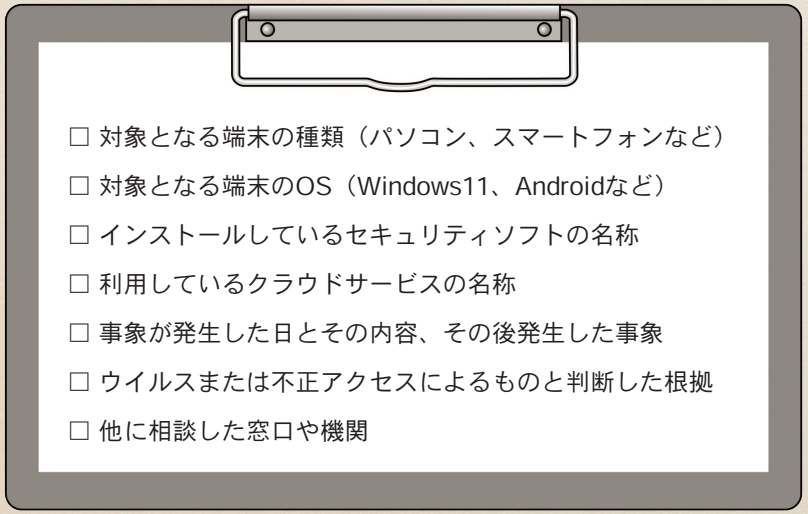
メールを発端とするサイバー攻撃の中には、企業の事業継続に多大な影響を与えるものもある。自社がそのような当事者にならないためにも、定期的な勉強会や訓練を実施するほか、経営者自身も率先して参加するなど、社内全体で危機意識を共有し、個々のリテラシー向上を図っていくことが何より大切だろう。

TOP SECRET
INFORMATION
インフォメーション

INFORMATION 6-1 もしかしてサイバー攻撃？緊急時には、ここに連絡を！

CHECK 問合わせる前に被害状況を整理しましょう

サイバー攻撃を受けた可能性がある場合は、事前に次のような情報を整理して緊急連絡先に連絡しましょう。



- ☐ 対象となる端末の種類（パソコン、スマートフォンなど）
- ☐ 対象となる端末のOS（Windows11、Androidなど）
- ☐ インストールしているセキュリティソフトの名称
- ☐ 利用しているクラウドサービスの名称
- ☐ 事象が発生した日とその内容、その後発生した事象
- ☐ ウイルスまたは不正アクセスによるものと判断した根拠
- ☐ 他に相談した窓口や機関

CHECK サイバー犯罪の可能性？

●警視庁 サイバー犯罪対策課

サイバーセキュリティに関連した犯罪の可能性がある場合の連絡先。

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/cyber_sodan.html
TEL　03-5805-1731
受付時間：平日8:30−17:15

CHECK サイバー犯罪の届出

●所轄の警察署

犯罪の証拠となる資料（エビデンス）を用意して届け出ましょう。

https://www.keishicho.metro.tokyo.lg.jp/about_mpd/shokai/ichiran/index.html
TEL　03-3581-4321（交換で、管轄の警察署名を確認して電話を転送してもらう。）

CHECK インシデントが発生していることの報告・届け出

●JPCERT/CC

サイトの改ざん箇所の特定や、改ざんされた際の復旧手順復旧方法などのインシデント対応の依頼・相談が可能です。

https://www.jpcert.or.jp/menu_reporttojpcert.html
TEL　03-6271-8901

●IPA J-CRAT／標的型サイバー攻撃特別相談窓口

標的型サイバー攻撃を受けている組織は支援を依頼・相談することができます。

https://www.ipa.go.jp/security/todokede/tokubetsu.html
TEL　03-5978-7599
E-mail　tokusou@ipa.go.jp

CHECK 個人情報の取り扱いに関する相談

●個人情報保護委員会

https://www.ppc.go.jp/
TEL　03-6457-9849

info

CHECK 一般的な情報セキュリティ相談

●独立行政法人 情報処理推進機構（IPA）情報セキュリティ安心相談窓口

可能な限り公開されている「よくあるご相談」（https://www.ipa.go.jp/security/anshin/about.html#1faq）を参照してから相談しましょう。

https://www.ipa.go.jp/security/anshin/about.html
TEL　03-5978-7509　FAX　03-5978-7518
受付時間：10:00－12:00　13:30－17:00（土日祝日・年末年始を除く）
E-mail　anshin@ipa.go.jp

CHECK 迷惑メールが送られてきた

●迷惑メールとは

「広告宣伝メール」、「架空請求メール」、「不当請求メール」、「ウイルスメール」、「お金儲けのメール」、「チェーンメール」等、受け取る人の意思に関わらず、勝手に送りつけられてくるメールです。メール内のリンク、添付ファイルは絶対に開かないで、削除してください。

●自分のメールアドレス等からの脅迫メール

迷惑メールの中には、自分のメールアドレス等から、暗号資産（ビットコイン）を要求する脅迫メールが送られてくるような事例も確認されています。

参考情報：日本サイバー犯罪対策センター　脅威情報
https://www.jc3.or.jp/threats/topics/article-160

●一般財団法人日本データ通信協会　迷惑メール相談センター

不特定多数へ同意を得ずに送られる広告宣伝目的メールに関する相談受付

https://www.dekyo.or.jp/soudan/index.html

CHECK 不審なメールが届いた・不審なサイトを発見した

●警視庁 フィッシング110番

警視庁は、フィッシングと思われる不審なメールが届いたり、フィッシングと思われる不審なサイトを発見した場合やフィッシングの被害に遭ってしまったという方は、フィッシング110番まで。

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/security/cyber406.html

●フィッシング対策協議会

フィッシングメールやフィッシングサイトに関する情報提供を受け付けており、フィッシング詐欺に関する事例情報、技術情報が公開されています。

https://www.antiphishing.jp/

●サポート詐欺

サポート詐欺とは「ウイルス感染した」などと偽の警告画面を表示させて不安をあおり、問題解決のためのサポートを行うふりをして、不必要なセキュリティソフトを購入させたりする詐欺です。
警告画面が表示されたら、サポート詐欺を疑ってください。

参考情報：警視庁　よく寄せられる相談事例
https://www.keishicho.metro.tokyo.lg.jp/sodan/nettrouble/jirei/warning_screen.html

●ビジネスメール詐欺

メールなどを組織・企業に送り付け、従業員を騙して送金取引に係る資金を詐取するといった、直接的に金銭を狙うサイバー攻撃です。
何らかの形でのメール等のやりとりを盗み見て、相手になりすまして偽の取引へ誘導しようとします。判明した際は、まずメールがどちらから漏えいしたのかを確認する必要があります。

参考情報：IPA_J-CSIP/ビジネスメース詐欺「BEC」に関する事例と注意喚起
https://www.ipa.go.jp/archive/files/000058478.pdf

CHECK ウィルスに感染した･不正アクセスされた

●ランサムウェアに感染した場合

感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求されることがあります。

被害として、バックアップがなかった場合のデータ復旧に要する多大なコスト、感染したことによる社会的信用の失墜、流失したデータが公開された場合の損害賠償等、ビジネスの継続が困難になることなどが考えられます。

●IPAコンピュータウイルス・不正アクセスに関する届出窓口

届出様式をダウンロードし、判明している範囲で構いませんので、被害の状況や対応した内容等を記入の上、メールで送付してください。

https://www.ipa.go.jp/security/todokede/crack-virus/about.html

●ランサムウェア被害の届出

独立行政法人情報処理推進機構 セキュリティセンター

コンピュータウイルス届出窓口

E-mail　virus@ipa.go.jp

●不正アクセスの届出

独立行政法人情報処理推進機構 セキュリティセンター

コンピュータ不正アクセス届出窓口

E-mail　crack@ipa.go.jp

CHECK なりすましECサイトを作られた

●なりすましECサイト

実在のサイトに似せたサイトを作成して、消費者を誤認させ、商品代金をだましとったり、模倣品、海賊版やその他購入しようとした品と全く別個の物を送りつけるサイトのことです。

参考情報：東京都　セキュリティの部屋　なりすましECサイトに注意！
https://www.cybersecurity.metro.tokyo.lg.jp/topics/43/

●なりすまされた事業者の緊急対応

①問い合わせには誠実に対応し、記録に残す。

だまされてしまった利用者には、きちんと事情を説明し、誠実に対応しましょう。

②自社サイト内で注意喚起

なりすましECサイトが存在している旨を説明し、自社とは関係がないサイトであることを明記しましょう。

③プロバイダに削除要請。被害届けは、事業者から提出する。

なりすましECサイトが公開されているプロバイダ等に削除要請を行いましょう。

●利用者の緊急対応

経済的被害等があった場合は、警視庁サイバー犯罪対策課、管轄の警察署へ被害相談をしましょう。

●なりすましECサイト対策協議会【セーファインターネット協会】

https://www.saferinternet.or.jp/e-commerce/narisumash
対策マニュアル：https://www.saferinternet.or.jp/e-commerce/narisumashi/
違法情報の通報：https://www.safe-line.jp/report/

INFORMATION 6-2 やられる前に、しっかり予防を！ ここに相談！

CHECK 専門機関に相談する前に、まずは、組織の対策状況を確認する

専門機関に相談する前に、まずは、公開情報を参考に、現在、どの程度の対策ができているかを把握し、できるところから段階的に対策の実施を検討しましょう。

中小企業の情報セキュリティ対策ガイドライン（IPA)
https://www.ipa.go.jp/security/guide/sme/about.html

CHECK 自社の対策状況から見て、緊急に対策すべき脅威と対策の概要を知る

●知っておきたいサイバー攻撃の知識について
参考情報：本ガイドブックMISSION1-1〜1-15

●基本的なセキュリティ対策
OS（オペレーティングシステム）の設定や利用状況を整理しましょう。
参考情報：NCO_OS(オペレーティングシステム）の設定や利用
https://security-portal.nisc.go.jp/cybersecuritymonth/2022/basics/OS/index.html
家庭用無線LANルーターの設定や利用に注意しましょう。
参考情報：NCO_家庭用無線LANルータの設定・利用
https://security-portal.nisc.go.jp/cybersecuritymonth/2022/basics/router/index.html

CHECK 予防策、改善策を専門機関に相談する

●経営とIT化の全般に関して相談したい
ITコーディネータ協会 「経営とIT化相談」窓口
https://www.itc.or.jp/
東京都中小企業振興公社ワンストップ総合相談
https://www.hataraku.metro.tokyo.lg.jp/madoguchi/telework-center/
TEL.03-3251-7881

●テレワーク等の運用に関して相談したい
テレワーク相談センター
https://telework.mhlw.go.jp/info/map/
TEL.0120-861009

●情報セキュリティ対策に関してのセミナー、イベント、教材等を探したい
「みんなで使おうサイバーセキュリティ・ポータルサイト」(NCO)
https://security-portal.nisc.go.jp/linkindex.html

info

●情報セキュリティ対策に関してのプレゼンターを探したい
IPAセキュリティプレゼンター検索（IPA)
https://www.ipa.go.jp/security/sme/presenter/index.html

●情報セキュリティ対策を支援してくれるサービスを探したい
情報セキュリティサービス基準適合サービスリスト（IPA）
https://www.ipa.go.jp/security/service_list.html

●サイバーインシデント発生時に対応を依頼できる企業を探したい
サイバーインシデント緊急対応企業一覧　(JNSA)
https://www.jnsa.org/emergency_response/

CHECK 助成制度を活用したい

●IT化・セキュリティ対策助成制度等

中小企業向けサイバーセキュリティお助け隊
（サイバーセキュリティ事後対応支援実証事業）(IPA)
https://www.ipa.go.jp/security/sme/otasuketai-about.html

サイバーセキュリティお助け隊サービス(IPA)
https://www.ipa.go.jp/security/otasuketai-pr/

サイバーセキュリティ対策促進助成金（東京都中小企業振興公社）
https://www.tokyo-kosha.or.jp/support/josei/setsubijosei/cyber.html
助成金活用例：https://cybersecurity.metro.tokyo.lg.jp/torikumi/47

CHECK 日常的に、最新情報をウオッチする！

●X

・警視庁サイバーセキュリティ対策本部
https://x.com/MPD_cybersec

・IPA（情報セキュリティ安心相談窓口）
https://x.com/IPA_anshin

・IPA（ICATalerts）
https://x.com/ICATalerts

・国家サイバー統括室(注意・警戒情報)
https://x.com/nisc_forecast

・JVN 脆弱性レポート
https://x.com/jvnjp

・JPCERTコーディネーションセンター
https://x.com/jpcert

・フィッシング対策協議会
https://x.com/antiphishing_jp

・JNSA
https://x.com/jnsa

●Webページ

・JC3 情報提供 注意喚起情報
https://www.jc3.or.jp/info/heads-up.html

・JPCERT/CC　注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

CHECK 恒久的対策を行うための情報源

情報セキュリティ対策支援サイト（IPA）
https://security-shien.ipa.go.jp/

セキュリティプレゼンター支援（IPA）
https://security-shien.ipa.go.jp/presenter/

情報セキュリティサービス基準適合サービスリスト（IPA）
https://www.ipa.go.jp/security/service_list.html

サイバーインシデント緊急対応企業一覧（JNSA）
https://www.jnsa.org/emergency_response/

経営とIT化相談窓口（ITコーディネータ協会）
https://www.itc.or.jp/management/diagnosis/

東京テレワーク推進センター | TOKYOはたらくネット
https://www.hataraku.metro.tokyo.lg.jp/madoguchi/telework-center/

テレワーク相談センター

https://telework.mhlw.go.jp/info/map/

テレワークのセキュリティあんしん相談窓口（LAC）
https://www.lac.co.jp/telework/security.html

ワンストップ総合相談窓口（東京都中小企業振興公社）
https://www.tokyo-kosha.or.jp/support/shien/soudan/

CHECK 東京都による情報源

東京都と警視庁、中小企業支援機関、サイバーセキュリティ対策機関などが連携して開設した、中小企業のための相談窓口

https://www.cybersecurity.metro.tokyo.lg.jp/support/
TEL　03-5320-4773
窓口　東京都産業労働局商工部（東京都西新宿2-8-1 都庁第一本庁舎20階北側）
受付時間：都庁開庁日の9:00～12:00、13:00～17:00

東京中小企業支援 サイバーセキュリティ
https://www.sangyo-rodo.metro.tokyo.lg.jp/chushou/shoko/cyber/

「中小企業向けサイバーセキュリティの極意」ポータルサイト
https://cybersecurity-tokyo.jp/

東京都の取組
https://www.cybersecurity.metro.tokyo.lg.jp/torikumi/#page1

CHECK 被害が発生している可能性がある場合

違法・有害情報（セーファーインターネット協会）
https://www.safe-line.jp/

違法・有害情報（インターネット違法・有害情報相談センター）
https://www.ihaho.jp/

違法・有害情報（インターネット・ホットラインセンター）
https://www.internethotline.jp/

個人情報（個人情報保護委員会）
https://www.ppc.go.jp/

嫌がらせ・ネットストーカー（管轄の警察署の生活安全課）
Webブラウザーで「警察署一覧」で検索

人権侵害（法務省人権擁護局 みんなの人権110番）
https://www.moj.go.jp/JINKEN/index_soudan.html

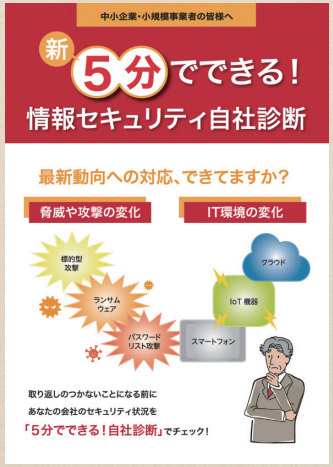
INFORMATION 6-3 経営者の理解のもと組織としてセキュリティ対策を！

CHECK セキュリティ対策は、どんな手順で進めるべきか？

ACTION 1 まずは、自社の現状を把握する

取り急ぎ、簡単に診断してみる

「5分でできる！情報セキュリティ自社診断」(IPA)
https://www.ipa.go.jp/security/guide/ps6vr70000011jhl-att/000055848.pdf



ACTION 2 経営者に理解を求めること

自社の対策状況から見て、緊急に対策すべき脅威と対策の概要を知る
基本的なセキュリティ対策

OS（オペレーティングシステム）の設定や利用（NCO）
https://security-portal.nisc.go.jp/cybersecuritymonth/2022/basics/OS/index.html

企業経営のためのサイバーセキュリティに係る基本的な考え方

企業経営のためのサイバーセキュリティの考え方の策定について（国家サイバー統括室）

https://www.nisc.go.jp/pdf/policy/kihon-1/keiei.pdf

経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するためガイドライン

「サイバーセキュリティ経営ガイドライン」（経済産業省）
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

脅威を認識してもらう（セキュリティ被害の状況）

「情報セキュリティ10大脅威 2025」（IPA）
https://www.ipa.go.jp/security/10threats/10threats2025.html

ACTION 3 具体的な対策を進めるには

- 経営者が率先して段階的に対策に取り組むために、経営者が情報セキュリティ全般を統括する「最高情報セキュリティ責任者（CISO）」等に指示すべき重要項目を把握する。
- どんな情報資産を保有し、それぞれの情報資産に対してどのような情報セキュリティリスクがあるかを把握するためリスク分析を活用する。
- リスク分析をそれをもとに定めたセキュリティ対策を文書化した規程を効率的に作成する。

ACTION 4 具体的な対策の実施

具体的な対策は、ガイドラインを参考にして効率的に実施しましょう

「中小企業の情報セキュリティ対策ガイドライン」（IPA）
https://www.ipa.go.jp/security/guide/sme/about.html

info

セキュリティお役立ちリンク

中小企業のDX、セキュリティ対策の推進に関連する情報を提供している主なポータルサイトを紹介します。用途に応じて活用してください。

CHECK サイバーセキュリティ関連（ユーザ向け）

みんなで使おうサイバーセキュリティ・ポータルサイト	NCO	サイバーセキュリティに関する様々な情報への入り口。相談窓口の紹介、最新動向などを広く網羅。
情報セキュリティ・ポータルサイト（ここからセキュリティ！）	IPA	個人から組織まで幅広い層に向けた情報セキュリティ対策、ハンドブック、最新の脅威情報などを提供。
国民のためのサイバーセキュリティサイト	総務省	インターネットとサイバーセキュリティの知識や、利用方法に応じたサイバーセキュリティ対策を講じるための基本となる情報などを公開。
インシデントの報告受付、対応支援、手口分析、再発防止策の助言	JPCER T/CC	コンピュータセキュリティインシデントに関する報告の受付、対応支援、脆弱性情報、注意喚起を行う日本のCSIRTの中心的組織。
中小企業向けサイバーセキュリティ対策の極意ポータルサイト	東京都	東京都が都内中小企業向けに提供するサイバーセキュリティ対策ポータル。「極意」ガイドブックの公開、脅威情報、相談窓口の紹介など。
サイバーセキュリティインフォメーション	警視庁	警視庁がサイバーセキュリティに関する注目情報、被害者・加害者にならないための情報、ケースごとの対策情報など掲載。

CHECK サ各府省の情報セキュリティ関連ポータル（政府政策・基準関連）

国家サイバー統括室	NCO	サイバーセキュリティ戦略、統一基準群など、政府全体の基本方針や法制度に関する情報を掲載。
経済産業省 情報セキュリティ関連施策	経済産業省	産業界の情報セキュリティ対策、サイバー攻撃への対応、セキュリティポリシーに関するガイドライン、産業分野別施策やAI事業者ガイドラインなどを公開。

CHECK DX・AI（生成AI含む）のフレームワーク・ガイドライン関連

DX推進ポータル	IPA	「DX推進指標」や「DX認定制度」など、企業がDXを測るためのフレームワークと指標を解説。
マナビDX（デラックス）	IPA	デジタル知識・能力を身につけるための実践的な学習コンテンツを集約したプラットフォーム。「デジタルスキル標準」に基づいた信頼できる講座を掲載し、デジタル人材育成を支援。
経済産業省/総務省 AI事業者ガイドライン関連情報	経済産業省	「AI事業者ガイドライン」など、AIを開発・提供・利用する事業者が自主的に取り組むべき事項や、リスク管理の考え方に関するガイドラインを公開。
AIセキュリティ情報発信ポータル	総務省	AI開発の各工程で注意すべきセキュリティのポイントを体系化した「AIセキュリティ・マトリックス」など、生成AIのセキュリティリスクに関するフレームワークを提供。
J-Net21（中小企業ビジネス支援サイト）	中小企業基盤整備機構	中小企業向けのビジネス支援情報。DX推進やIT活用に関する支援策、成功事例、専門家への相談窓口などを重点的に紹介。

INFORMATION 6-5

中小企業の情報セキュリティ対策の段階的レベルアップ

CHECK

情報セキュリティ対策の進め方

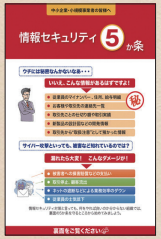
情報技術の進歩・普及に伴い経営効率が向上した一方、重要情報の漏えいや消失、改ざんなど技術特有の不利益が発生する機会も増してきています。
これら不利益が対策の不備により生じた場合、経営者は取引先や従業員などへの社会的・道義的責任に加え、法的責任も追及されるおそれがあります。

近年は企業情報を狙うサイバー脅威も日々巧妙化しています。自社を守るためには、経営者が率先して対策に取り組むことが大切です。

●中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html

情報セキュリティ対策を推進する際に参考にしたいのが、「中小企業の情報セキュリティ対策ガイドライン」（情報処理推進機構〈IPA〉）です。
このガイドラインは情報の安全管理の重要性や企業の保有する機微な情報を各種の脅威から保護するための対策の考え方や段階的に実現するための方策を紹介する目的で作成されたものです。まずはこのガイドラインを参考に、自社に適した対策を実践していくとよいでしょう。

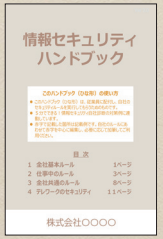
●「中小企業の情報セキュリティ対策ガイドライン」



●付録1
「情報セキュリティ5か条」

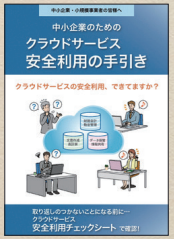
●付録2
「情報セキュリティ基本方針（サンプル）」

●付録3
「5分でできる！ 情報セキュリティ自社診断」



●付録4
「情報セキュリティハンドブック（ひな形）」

●付録5
「情報セキュリティ関連規程（サンプル）」



●付録6
中小企業のためのクラウドサービス安全利用の手引き

●付録7
リスク分析シート

●付録8
中小企業のためのセキュリティインシデント対応の手引き

info

ACTION 1 最低限のルール「情報セキュリティ5か条」

資金や人材が限られる中小企業にとって、最初から全ての対策に取り組むことは容易ではありません。まずは、基本的な対策を取りまとめた「情報セキュリティ５か条」に取り組むことからはじめ、段階的に対策を講じていきましょう。

1 OSやソフトウェアは常に最新の状態にしよう！

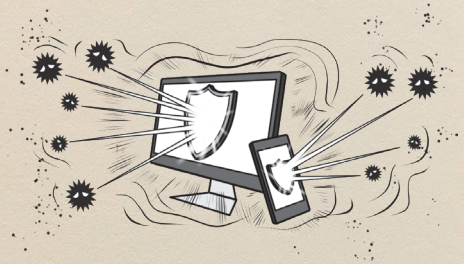
Windows OS、Mac OS、Androidなどはいずれも常に最新バージョンに！
Office、Adobe Readerなど利用中のソフトウェアも常に最新バージョンに！

☑ **「自動アップデート」は必ずONに！**

2 ウイルス対策ソフトを導入しよう！

ウイルス定義ファイルは自動更新に設定！
ファイアウォールや脆弱性対策なども可能な統合型セキュリティ対策ソフトを導入！

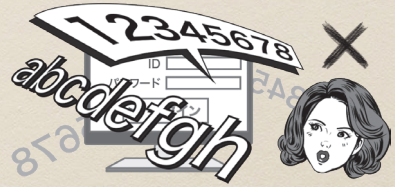
☑ **ウイルス対策ソフトも常に最新に！**



3 パスワードを強化しよう！

ID・パスワードは推測や解析、ウェブサービスから流出することで不正ログインに悪用される恐れがある！
「長く」「複雑」「使い回さない」を徹底しよう！

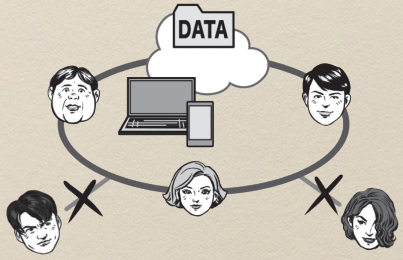
☑ **パスワードは使い回さない！**



4 共有設定を見直そう！

クラウドサービスの共有を限定的に！
ネットワーク接続の複合機、カメラ、ハードディスク、NASなどの共有を限定的に！
従業員の異動や退職時に設定の変更や削除漏れがないように！

☑ **利用者は必要な人だけに！**



5 脅威や攻撃の手口を知ろう！

セキュリティ専門機関から常に最新の脅威情報を収集！
利用中のネットバンクやクラウドサービスからの注意喚起を確認！

☑ **最新情報で対策を！**

ACTION 2 組織的な対策に取り組む

基本的対策の次は組織的な対策です。「中小企業の情報セキュリティ対策ガイドライン」とその付録を参考に自社に適した基本方針を作成し、社内関係者に周知します。また、自社のセキュリティ診断を実施して、取り得る対策を検討していきましょう。

1　情報セキュリティ基本方針の作成と周知

従業員の指針であり、関係者に対して取り組みを表明するための情報セキュリティに関する基本方針を経営者が定め、簡潔な文書にまとめて周知します。
「中小企業の情報セキュリティ対策ガイドライン」と付録2の「情報セキュリティ基本方針（サンプル）」を参考に、経営者と連携して自社に適した基本方針を作成しましょう。

2　実施状況の把握

付録3の「5分でできる！情報セキュリティ自社診断」を利用して、情報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しましょう。

3　対策の決定と周知

「5分でできる！情報セキュリティ自社診断」の結果を基に、解説編を参考にして実施すべき情報セキュリティを検討しましょう。

ACTION 3 本格的に対策に取り組む

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

1　管理体制の構築

情報セキュリティ基本方針を具体的に実現するために、情報セキュリティ責任者、情報部門責任者、システム管理者、教育責任者、点検責任者を任命して責任分担と連絡体制を整備しましょう。また、情報セキュリティ事故が発生した場合など、緊急時対応体制も整備しておきましょう。

2　デジタルトランスフォーメーション（DX）の推進と情報セキュリティの予算化

中小企業においても競争力維持・強化のために、デジタルトランスフォーメーション（DX）を進めていくことが求められています。昨今はクラウドサービスなどデジタル技術やインターネットの活用が多様化し、それに伴いリスクも複雑化しています。そこで、より有効なセキュリティ対策のために、自社の情報システムについて、インターネットとの接続状況を図にするなどして対策を検討するとともに、予算を確保しましょう。

3　情報セキュリティ規程の作成

事業内容や取り扱う情報、職場環境、IT利活用の状況に応じて、「中小企業の情報セキュリティ対策ガイドライン」付録5の「情報セキュリティ関連規程（サンプル）」を参考に、情報セキュリティ規程を作成しましょう。（1）対応するリスクの特定、（2）対策の決定、（3）規程の作成の順に進めます。

4　委託時の対策

業務の一部または全部を外部に委託したり、レンタルサーバーやクラウドサービスなどの外部サービスを利用したりして、重要な情報を渡したり処理を依頼したりする場合には、委託先に実施してもらう情報セキュリティ対策も決めましょう。取引条件のひとつとして、契約書や覚書に具体的な対策を明記しましょう。

5　点検と改善

「情報セキュリティ5か条」や「5分でできる！情報セキュリティ自社診断」、自社の情報セキュリティ対策に関するルール・規程を基準に、情報セキュリティ対策が、計画通りに実行されているか、見落としている対策はないか、対策がセキュリティ事故防止の役に立っているかを確認しましょう。

ACTION 4　対策をより強固にする

本格的な対策に取り組んでいても、必要な対策を追加して強固にしましょう。

1　情報収集と共有

情報セキュリティに関する脅威や攻撃の手口を知り、社内や取引先、同業者と共有することで対策レベルの向上につなげましょう。

2　ウェブサイトの情報セキュリティ

情報漏えいや改ざんなどの被害が発生する攻撃の対象になりやすいWebサイトの運営形態、構築、運営それぞれの段階に応じた対策を講じましょう。

3　クラウドサービスの情報セキュリティ

クラウドサービスに適した情報セキュリティ対策について、サービスの選定、運用、セキュリティ対策の3段階で検討しましょう。

4　テレワークの情報セキュリティ

テレワークのセキュリティ対策について、方針検討、セキュリティ対策、運用の３段階で検討しましょう。

5　セキュリティインシデント対応

インシデント発生時の対応について、検知初動対応、報告・公表、復旧・再発防止の３段階に分けて検討しましょう。

6　情報セキュリティサービスの活用

（1）情報資産の洗い出し、（2）リスク値の算定、（3）情報セキュリティ対策の決定の順で、リスクの洗い出しと対策の検討を行いましょう。

INFORMATION 6-6 資産管理台帳の作成と詳細リスク分析

CHECK リスク分析を活用する

自社に適した対策を実行して効果をあげるには、まず、自社にどのような情報セキュリティリスクがあるかを把握する必要があります。
リスク分析を通じて、適切な対策を導き出しましょう。

CHECK リスク分析によるセキュリティ対策決定までの流れ

手順1　情報資産管理台帳を作成する

自社で保有している情報を<ツールAリスク分析シート>の「情報資産管理台帳」シートへ記入例に従い書き出し、それぞれの重要度を判定してください。

重要度2　事故が起きると事業に深刻な影響がある
重要度1　事故が起きると事業に重大な影響がある
重要度0　事故が起きても事業に影響はない

手順2　リスク値の算定

<ツールAリスク分析シート>の「脅威の状況」シートで想定される脅威を指定し、「対策状況チェック」シートで自社の対策状況を指定すると情報資産ごとのリスク値が計算されて対策が必要な情報資産が分かります。

リスク値4～6　大　重点的に対策を実施
リスク値1～3　中　対策を実施
リスク値　0　小　現状維持

手順3　情報セキュリティ対策を決定

<ツールAリスク分析シート>の「対策状況チェック」シートで自社の対策状況を以下から選択すると、「診断結果」シートに診断結果と自社で策定すべく情報セキュリティポリシーが表示されます。

1：実施している　…対策を実施済みの場合
2：一部実施している　…対策を実施しているが、十分でない場合
3：実施してない／わからない　…対策を実施していないか、関連情報がない場合
4：自社には該当しない　…当該項目に該当する業務を行っていない場合

リスク分析シートはIPAの中小企業の情報セキュリティ対策ガイドラインのページからダウンロード。
https://www.ipa.go.jp/security/guide/sme/about.html

ACTION 1 情報資産管理台帳を作成する

情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つです。日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。
情報資産管理台帳を作成する際は、
・情報資産の洗い出し
・情報資産ごとの機密性・完全性・可用性の影響度評価
・影響度の評価をもとに重要度を算定
の順で行います。

●情報資産の洗い出し

情報資産の洗い出しでは、業務で利用する電子データや書類などを特定し、資産目録を作成します。洗い出した情報資産は、「営業」「人事」「経理」など管理部門ごとに分類します。企業活動に大きな影響を与えかねない重要な情報を、できる限り漏れないように洗い出すことが重要です。影響がほとんどない情報であれば、漏れても大きな問題はありません。情報資産の洗い出しの粒度は、細かすぎると管理が大変ですが、逆に粗いと次のリスク分析が難しくなります。そのため、適度な粒度にすることが重要です。

業務分類	情報資産名簿	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	雇入時・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）	税務部	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）	税務部	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

資産目録の記載例

●情報資産ごとの機密性・完全性・可用性の影響度評価

機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、評価基準を参考に評価値3〜1を記入します。

評価値		評価基準	該当する情報の例
機密性 アクセスを許可された者だけが情報にアクセスできる	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供給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	●見積書に、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性 情報や情報の処理方法が正確で完全である	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 ●受注先・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性 許可された者が必要な時に情報資産にアクセスできる	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

●影響度の評価をもとに重要度を算定

重要度は「機密性」「完全性」「可用性」いずれかの評価値の最大値で判断します。なお、事故が起きると法的責任を問われたり、取引先、顧客、個人に大きな影響があったり、事業に深刻な影響を及ぼすなど、企業の存続を左右しかねない場合や、個人情報を含む場合は、前項の算定結果に関わらず、重要度は3とします。

判断基準	重要度
機密性・完全性・可用性評価値のうち最大値が「3」の情報資産	3
機密性・完全性・可用性評価値のうち最大値が「2」の情報資産	2
機密性・完全性・可用性評価値すべてが「1」の情報資産	1

情報資産の「重要度」は、時間経過とともに変化することがありますが、現時点の評価値を記入します。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。

（重要度の判断例）

①独自技術に基づいた設計図（書類）機密性の3が最大なので重要度は3

機密性：評価＝3

主力製品の設計図であり、流出すると他社との差別化ができなくなり、売上が減少する

完全性：評価＝2

改ざんや無断の変更があると、製造に支障がある

可用性：評価＝1

原本のCADデータはサーバーに保存してあり、必要なときに閲覧や再印刷が可能なので、利用できなくなっても困ることはない

②自社のホームページ（電子データ）完全性と可用性の3が最大なので重要度は3

機密性：評価＝1

公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない

完全性：評価＝3

不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う

可用性：評価＝3

サーバーの障害などでアクセスできなくなると、来店客が減少し、売上も減少する

info

ACTION 2 リスク値の算定

洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定します。

リスク値を算定するにはいろいろな方法がありますが、「重要度」と「被害発生可能性」の2つの数値の掛け算で行います。

リスク値 ＝ 重要度 × 被害発生可能性

重要度 ＝ 手順１にて算定

被害発生可能性 ＝ 脅威・脆弱性から算定

「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の2つの数値から算出します。これは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。

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）

換算表で算出

被害発生可能性の換算表		つけ込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

重要度は手順1で算定した3～1の数値、被害発生可能性、脅威、脆弱性は3～1の数値、リスク値は算定結果を大・中・小で表します。

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

リスク値		
	9～6 大	深刻な事故が起きる可能性大
	4　中	重大な事故が起きる可能性有
	3～1 小	事故が起きる可能性小、起きても被害は受容範囲

また、情報セキュリティリスクの場合は、発生頻度が高く被害が非常に大きいものについては「回避」、発生頻度は低いが被害が大きいものについては「移転」、発生頻度は高いが被害が大きくないものについては「低減」を検討するという対応策の整理を行います。

ACTION 3 情報セキュリティ対策を決定

リスク値の大きいものから対策を検討し、自社に適した対策を決定します。

①リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくすることです。「軽減」「修正」と呼ばれることもあります。

②リスクを保有する

対策を行わずにリスクを受け入れるということです。事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

③リスクを回避する

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

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

④リスクを移転する

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

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

INFORMATION 6-7 情報セキュリティ関連規程に記載すべき項目

企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ITの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。リスク分析とそれをもとに定めたセキュリティ対策を文書化した規程を効率的に作成する方法を紹介します。

	名 称	概 要
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等の IT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。 委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。

CHECK 組織的対策

管理体制の構築や点検、情報共有などのルールを定めます。

●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します。情報セキュリティ委員会は、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します。

●情報セキュリティ取組みの監査・点検

監査・点検責任者は、情報セキュリティ関連規程の実施状況について、監査・点検/点検結果を情報セキュリティ委員会に報告します。情報セキュリティ委員会は、報告に基づき、必要に応じて改善計画を立案します。

●情報セキュリティに関する情報共有

情報セキュリティ責任者は、新たな脅威及び脆弱性に関する警戒情報及び個人情報の保護に関する情報を専門機関等から適時に入手し、委員会で共有します。

CHECK 人的対策

取締役及び従業員の責務や教育、人材育成などのルールを定めます。

●雇用条件

従業員を雇用する際には秘密保持契約を締結します。

●情報セキュリティ教育・人材育成

教育責任者は、情報セキュリティに関する教育計画を年度単位で立案します。また推奨資格の取得による従業員の情報セキュリティに対する意識向上を年度単位で計画します。計画には関連テキストの配付、公開セミナーへの派遣、受験費用の予算を含めます。

CHECK 情報資産管理

情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。

●情報資産の管理

事業に必要で価値がある情報及び個人情報など情報資産を特定し、「情報資産管理台帳」に記載します。情報資産を社外に持ち出す場合には、情報資産の重要度に応じた許可と管理手順に従って実施します。

●バックアップ

情報システム管理者は、各機器で処理するデータのバックアップを定期的に取得します。利用する機器及び媒体の保管は、所定の手順に従います。クラウドサービスを利用し、外部のサーバーにバックアップを保存する場合は、各サービス要件を確認し、情報セキュリティ責任者の許可を得て導入します。

CHECK アクセス制御及び認証

情報資産に対するアクセス制御方針や認証のルールを定めます。

●利用者の認証・利用者アカウントの登録

社外秘又は極秘の情報資産を扱う社内情報システムは、重要度に従った方針に基づいて利用者の認証を行います。利用者の認証に用いるアカウントは、代表取締役又は情報セキュリティ責任者の承認に基づき登録します。

●利用者アカウントの管理

利用者の認証に用いるアカウントが不要になった場合、情報システム管理者は、当該アカウントの削除又は無効化を、当該アカウントが不要になる日の翌日までに実施します。

従業員以外の者にアカウントを発行する場合は、代表取締役又は情報セキュリティ責任者の承認を得たうえで、秘密保持契約を締結します。

●パスワードの設定

利用者の認証に用いるパスワードは以下に注意して設定します。

・十分な強度のあるパスワードを用いる
・他者に知られないようにする

CHECK 物理的対策

セキュリティ領域の設定や領域内での注意事項などのルールを定めます。

●セキュリティ領域の設定

扱う情報資産の重要度に応じて、社内の領域を区分し、利用者、施錠、設置可能情報機器、制限事項、部外者管理、管理記録、侵入検知、来客用名札、火災対策等の対策方法を設定します。

●セキュリティ領域内注意事項

セキュリティ領域では区分にかかわらずセキュリティ上注意すべき事項があれば明記します。

CHECK IT機器利用

IT機器やソフトウェアの利用などのルールを定めます。

●ソフトウェアの利用

情報システム管理者は、利用者の業務に不要な機能をあらかじめ取除いて提供します。従業員は、業務に不要なシステムユーティリティやインストールされているソフトウェアを利用しません。情報システム管理者は、適宜ウイルスに関する情報を収集し、重大な被害を与えるウイルスに対しては、対応策及び対応に必要な修正プログラムを社内に公開及び通知します。

●クリアデスク・クリアスクリーン

従業員は、社外秘又は極秘の書類及び電子データを保存したノートパソコン、USBメモリ、HDD、CD等の持ち運び可能な機器や媒体の扱いについて明記します。持ち運び可能な機器や媒体は机の上などに放置せず適切に管理してください。

●インターネット・電子メール等の利用

従業員は、インターネットで提供されているサービスを業務で利用する場合は、情報システム管理者の許可を得ます。

誤送信、メールアドレス漏えい、傍受による漏えい等の防止する方法、添付ファイル暗号化、クラウド型メール等の利用方法を明記する。標的型攻撃メール等によるウイルス感染を防止するため、疑わしいメールの要件に合致する場合は十分に注意し、添付ファイルを開く、又はリンクを参照するなどしません。

CHECK IT基盤運用管理

サーバーやネットワーク等のITインフラに関するルールを定めます。

●管理体制

情報システム管理者は、IT基盤の運用に当たり情報セキュリティ対策を考慮し製品又はサービスを選択します。

●IT基盤の情報セキュリティ対策

IT基盤の運用を行う際に情報システム管理者が実施すべき事項を明記します。

IT基盤で利用するサーバー機器に求める情報セキュリティ要件は、情報システム管理者が決定します。

IT基盤で利用するサーバー機器に導入するソフトウェアは、情報システム管理者が標準ソフトウェアを選定します。

IT基盤で利用するネットワーク機器に求める情報セキュリティ要件は、情報システム管理者が決定します。

●クラウドサービスの導入

IT基盤の一部としてクラウドサービス等の外部サービスを導入する場合は、情報システム管理者がサービスプロバイダの情報セキュリティ対策をあらかじめ評価したうえで選定します。

●IT基盤標準

サーバー機器、IT基盤標準ソフトウェア、標準ネットワーク機器、ネットワーク機器の種別毎に、情報セキュリティ要件を明記します。

サービスプロバイダを設定するに当たっての要件及び利用に当たっての条件となる適合性評価制度を明記します。

●廃棄・返却・譲渡

情報システム管理者は、IT基盤で利用した機器を返却、廃棄、譲渡を行う場合は、データを完全に消去し、情報セキュリティ責任者の承認を得たうえで返却、廃棄、譲渡を行います。内部記憶媒体の破壊又はデータの完全消去を、外部に委託する場合は、破壊又はデータの完全消去を実行したことの証明書を取得します。

CHECK システムの開発及び保守

独自に開発及び保守を行う情報システムに関するルールを定めます。

●新規システム開発・改修
情報システムの開発・改修を行う際には、設定された各工程を経て実施し、各工程の完了時に情報システム管理者の承認を得ます。

●脆弱性への対処
情報システムのソフトウェア開発を行う際には、当該情報システムの利用環境に応じて設計時に技術的な脆弱性を識別し、対策を講じます。脆弱性に対する対策の有効性は情報システム管理者が判断し、承認します。

●情報システムの開発環境
情報システムの開発及び改修を行う環境は、運用環境とは分離します。新たに情報システムの開発を行った場合や、情報システムの改修を行った場合は、当該情報システムの運用を開始する前に、必要な情報セキュリティ対策が講じられていることを確認し、情報システム管理者の承認を得ます。

●情報システムの保守
情報システムの保守を、開発元又は外部の組織に委託することができない場合、実施すべき事項を明確にし、情報システムに既知の脆弱性が存在しない状態で運用します。使用しているハード・ソフトのサポート終了が予定されている場合、再構築またはシステム利用停止を検討し、システム管理者の承認を得ます。

●情報システムの変更
情報システムのハードウェア又はソフトウェアの変更を行う際には、設定された工程を経て実施します。各工程の完了時に情報システム管理者の承認を得ます。

CHECK 委託管理

業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書に機密保持条項を定め、「委託先情報セキュリティ対策状況リスト」等委託先チェックリストによる評価結果に基づき委託先を選定・評価します。

●委託先評価基準
情報セキュリティ部門責任者は「情報資産管理台帳」の重要度が1以上である情報資産の取り扱う業務を、外部の組織に委託する場合は、委託先の情報セキュリティ管理について、委託先評価基準に基づいて評価します。

●委託先の選定
評価結果に基づき委託先を選定し、情報セキュリティ責任者の承認を得ます。

●委託契約の締結
委託契約書には、守られるべき事項を明記します。

●委託先の評価
委託開始後には、「委託先情報セキュリティ対策状況確認リスト」により、委託先における情報セキュリティ対策の実施状況について定期的に評価する機会を設けます。

●再委託
委託先が他の組織又は個人に再委託する場合には、事前に書面による報告を委託先に求めます。

CHECK 情報セキュリティインシデント対応ならびに事業継続管理

●対応体制
情報セキュリティインシデントが発生した場合の対応体制を明記します。

●情報セキュリティインシデントの影響範囲と対応者
情報セキュリティインシデントが発生した場合、影響範囲に対応した事故レベル(顧客や業務・組織に与える影響の程度を評価する基準）を設定し、対応責任者を明記します。

●インシデントの連絡及び報告
事故レベル１（従業員の業務遂行に影響が及ぶとき）以上のインシデントが発生した場合、発見者は連絡網に従い対応者又は責任者に速やかに報告し、指示を仰ぎます。

●対応手順
漏えい・流出発生時の事故レベル毎に対応手順を明記します。
情報システム管理者は、インシデント対応後に届け出、報告又は相談する機関を明記します。

●情報セキュリティインシデントによる事業中断と事業継続管理
代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合を想定し明記します。被害の対象毎に、復旧責任者、関係者連絡先を明記します。

INFORMATION 6-8 中小企業のためのクラウドサービス安全利用手引き

CHECK クラウドサービスとは

インターネットを通じてソフトウェアやハードウェアを利用する情報システムサービスをクラウドサービスと呼びます。クラウドサービスの利用は、情報システムの構築や管理といった手間が省けるなど、自社での所有・運用と比較して業務の効率化やコストダウンを図れるといったメリットがあります。

CHECK 利用前の確認

クラウドサービスの利用を検討する際は、情報セキュリティ対策の一部がサービス提供事業者に依存してしまうことや、クラウドサービス固有のリスクがある点についても考慮する必要があります。『クラウドサービス安全利用の手引き』（情報処理推進機構＜IPA＞）では、サービスを選択するときのポイントについて事例をあげて解説しています。

●中小企業のためのクラウドサービス安全利用の手引き

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

CHECK パブリッククラウドとプライベートクラウド

クラウドには大きく「パブリッククラウド」と「プライベートクラウド」があり、前者は、企業・個人を問わず必要なときにサーバーやサービス活用が可能です。後者は、企業・組織が専用環境を構築して社内各部署などにサービス提供する形を指します。しかし、各々メリット・デメリットがあり、両者を統合して利用する「ハイブリッドクラウド」の活用が増えつつあります。

CHECK クラウドサービス利用時の確認事項

●選択するときのポイント

1	どの業務で利用するか明確にする	どの業務クラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取り扱う情報の重要度を確認する	クラウドサービスで取り扱う情報が漏えい、改ざん、消失したり、サービスが停止したりした場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？

●運用するときのポイント

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

●セキュリティ管理のポイント

11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

No15 クラウドサービスのサーバーは日本国外に設定されている場合もありますが、扱うデータによってサーバーの設置国・地域の法規制が適用されることがあります。No 6、11、12、13はスマートSMEサポーター（認定情報処理支援機関）開示情報で確認できます。

出典：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」より

INFORMATION 6-9 DX 時代での経営者の意識改革の方向性

CHECK 経営者の「チェンジマネジメント」の重要性の認識

DXがうまく進まない大きな要因の一つに「人の変化に対する抵抗」の存在が挙げられます。
変化に対する抵抗は、「今のままでもうまくいっている」「変化の必要性を感じない」といった「現状肯定」と、「ITやデジタル化についていけない」「自分の立場や仕事を失うかもしれない」という「将来不安」から形成されます。

CHECK 社員の能力再開発「リスキリング」

DXの本質は、デジタル技術を活用して、今のビジネスモデルの革新をはかることです。現場で働く多種多様な人々がおしなべて、新しいスキルを身につけることが求められます。
成果を発揮し続けられるように新たなスキルを獲得することが「リスキリング」。働く人々にどんな新しいスキルを獲得してほしいのかを示し、リスキリングの基盤を構築する責任が企業にあると言えます。「価値を提供する新しいデジタルな方法を理解し使いこなせる」ことが重要です。

CHECK 中小企業における人材育成の戦略

企業のIT 投資は、「攻め」と「守り」に分けることができます。経営者は、守りのIT・セキュリティ対策に留まらず、事業を発展させるための攻めのIT・セキュリティ対策を講じるための人材の育成を推進するべきなのです。

「攻めのIT 投資」とは、IT を活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規顧客獲得、収益拡大、販売力のアップを目指すことです。一方、「守りの IT 投資」とは、IT による業務の効率化やコスト削減を目的としています。

●守りのIT・セキュリティ対策

これまで組織のITシステムは、業務の改善や効率化によるコスト削減により、経営を安定化させることに重きが置かれ、サービスの維持が図られてきました。現状のサービスを維持だけであっても、競争力を維持するためには効率化は必須であり、新たなIT技術への対応と、新たな脅威への対処のためのセキュリティ対策が必要です。

【進め方】
手順１：業務内容・業務フローの可視化
手順２：削減・短縮可能な業務の洗い出し
手順３：改善や対応の実施
手順４：業務改革の実現

●攻めのIT・セキュリティ対策

一方でサービスの維持だけでは、ビジネスの競争に勝ち残れません。時代のニーズに対応した高付加価値の新たな取り組みにより、サービスを向上させていかなければ、組織の発展はおろか、継続も見込めなくなることが予想されます。より先進的な技術を活用した新たなサービスを、他社に先駆けて提供していくことが望まれるのです。そのためにも、組織人として、ITやデジタルを利活用できるデジタルリテラシーの習得が求められます。

【進め方】
手順１：経営ビジョン・戦略の策定
手順２：変革の準備・課題の抽出
手順３：デジタル技術・業務改革による課題解決
手順４：顧客に新たな価値を提供

info

DX 時代に不可欠な人材の確保と育成

デジタルリテラシーを持った人材の確保

昨今の企業は、ビジネスの展開の中で、サスティナブルな企業価値の創造が求められています。
そのような環境において、ビジネスを発展していくためには、ビジネスの変革が必要であり、IoTやビッグデータ、ロボット、AI、5Gなどの新しいIT及びデジタルの活用が不可欠です。
新しいIT及びデジタル技術を活用するためには、従来からのITリテラシーに留まらず、IT・データサイエンス・AIの三方面からデジタルリテラシーを持った人材の育成・確保が重要になります。

デジタル人材の確保

●「デジタルを作る人材」の確保

DX時代のIT・デジタル活用では、データをクラウド環境からIoT等により収集し、ビッグデータを学習データとして、AIにより分析して知識として活用したり、付加価値を付けた情報として提供するようなビジネスモデルが想定されます。
DXに対応するためには、「デジタルを作る人材」であるシステム関連部門では、従来からのITスキルに加えて、データサイエンス・AIを生かせるスキル、知識等が必要です。更に、それらを実践で生かせるマインド、素養を含めてデジタルリテラシーを持つ人材の確保と育成が不可欠となります。

●「デジタルを使う人材」だけでなく「デジタルを使う人材」の育成も必須

DXの推進には、「デジタルを使う人材」である事業担当部門でも、基礎的なデジタルリテラシーを持つことが必要です。

●「リスキリング」：システム関連部署だけでなく、全員がデジタルリテラシーを持つ

「デジタルを作る人材」、「デジタルを使う人材」は、「リスキリング」等により、現状にプラスするデジタルリテラシーを持った人材へとスキルアップすることが効果的です。

●網羅的な素養を確保：人材育成が困難な場合は、外部の人材を積極的に活用

業務を担うために必要な人材を確保できなければ、その役割は経営者、責任者が担わなければなりません。業務及びシステムに必要な素養を一人で全てを兼ね備えることは困難です。リスキリング等によっても十分に確保できない人材は、外部の組織に支援を求め、事業全体で、スキル・知識の網羅性を確保することが重要です。その際においても、外部委託を担当する従業員は、対等に指示できるレベルのデジタルリテラシーが必要になります。

サイバーセキュリティ対策人材

●DX with Security：サービスの向上のためセキュリティ対策は必須

ITやデジタル情報を活用してどんな利便性の高いサービスを提供しても、どんなに業務を効率化しても、セキュリティ侵害が発生し早期に復旧ができなければ、事業の継続が困難になります。
セキュリティ対策の必要性の認識のみならず、具体的なセキュリティ対策を実施する必要があるのです。

info

しかしながら、ITの活用に関しての知識を持たずに、具体的なセキュリティ対応を行うことは困難です。まず、ITリテラシーを備えた上で、「プラス・セキュリティ」として、セキュリティに関する知識を習得することが有効です。

CHECK 役割毎に必要な素養・スキル・知識のレベル

必要な素養を組織の中で確保が困難な場合が多いと思われるが、外部要員も含めて、全体で全ての役割をに担えることが重要です。

	概　要	経営者層	企画管理部門	システム構築実務者	サービス提供実務者	サービス利用者
IT リテラシー（IT パスポートレベル）	社会人として、IT 及びデジタルを操作するために必要な最低限のリテラシー	◎	◎	◎	◎	◎
プラス・セキュリティ	ITSS＋（セキュリティ領域）を理解できるレベルのセキュリティ知識	○	◎	◎	◎	◎
デジタルリテラシー（Di-Lite）レベル	IT 及びデジタルを利活用する全ての社会人が、今後、持つべきコア・リテラシー	○	○	◎	◎	○
基本情報技術者レベル	システム担当として持つべき、基本的な IT 関連スキル・知識			◎	△	
応用情報技術者レベル	システム管理者として持つべき、応用的な IT 関連スキル・知識			◎		
専門情報技術者（スペシャリスト）レベル	システム関連の各役割の専門家として持つべき、高度な IT 関連スキル・知識			○		

INFORMATION 6-11 デジタルリテラシー人材の認定・評価制度

CHECK 「デジタルリテラシー」の習得

デジタル時代の人材育成は国全体の重要な課題となっており、全てのビジネスパーソンがデジタル時代のコア・リテラシーを身につけていくことが求められています。DXの推進には、これまでの「デジタルを作る人材」だけでなく、「デジタルを使う人材」が必要ですが、中小企業においては、まず、「デジタルを使う人材」の育成に力を入れましょう。

CHECK 各種スキル標準

●ITSS+（プラス）

ITSS+は、第4次産業革命に向けて求められる新たな領域の"学び直し"の指針 として策定されました。情報システム部門の従事者等のスキル強化を図る取 組みに活用されることを想定しています。

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

●情報システムユーザースキル標準（UISS）

情報システムユーザー企業における情報システムの利用に関する課題の解決に必要とされる課題解決に必要な能力の指標です。

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/uiss.html

●ITスキル標準（ITSS）

各種IT関連サービスの提供に必要とされる能力を明確化・体系化した指標です。

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/index.html

INFORMATION 6-12

セキュリティ人材の確保と育成

CHECK セキュリティ人材育成と考え方の変化

企業規模等によっても異なりますが、セキュリティ対策の中心となるのは、セキュリティ統括分野やセキュリティ監視・運用分野等を担うセキュリティ人材です。さらに、ITを利活用して社会を変えるSociety5.0の進展など、時代の変化を受け、本来の業務の中でITを利活用する人材にもセキュリティに関するスキルが求められるようになっています。

CHECK 求められる「プラス・セキュリティ人材」

企業におけるあらゆる業務でデジタルトランスフォーメーション（DX）が進んでいますが、DXによる利便性はサイバー攻撃にも悪用されやすいため、DXを活用する企業ではセキュリティを意識して必要な対策を総合的に実施することが求められます。

一方、IPAなどによる調査では、そうしたセキュリティ人材の量的・質的不足が大きな課題となっています。セキュリティ対策がセキュリティ人材だけでは対処できなくなっているため、デジタル部門、事業部門、管理部門など、セキュリティ対策が不十分な場合にセキュリティ上の問題が生じるような業務を担っている人材にも、セキュリティに関する意識を養い、対策の実施に求められる知識・スキルを積極的に身に付けてもらう必要があります。

こうした「プラス・セキュリティ人材」の育成がこれからの企業には求められます。

CHECK 「プラス・セキュリティ人材」の育成

「プラス・セキュリティ人材」を育成する際には、経済産業省が定めている、セキュリティ領域のIT人材に求められる個人のIT関連能力を明確化・体系化し、スキルやキャリア（職業）を示した指標である「ITSS+（セキュリティ領域）」を活用し、関連部門でセキュリティ関連タスクを担う人材の特定・育成・配置等を検討するとよいでしょう。

●ITSS+（プラス）・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報
https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/index.html

●サイバーセキュリティ体制構築・人材確保の手引き（経済産業省）
https://www.meti.go.jp/policy/netsecurity/tebiki_taisei_jinzai.html

info

情報セキュリティ関連法令

企業の情報セキュリティに関連する国内の法令は、下記のように多岐にわたります。また、海外に子会社や支店、営業所などを有し、日本から海外に商品やサービスを提供している企業や海外から個人データの処理について委託を受けている事業など、業務の内容によっては、EU域内の各国に適用される個人データ保護を規定したEU一般データ保護規則（GDPR：General Data Protection Regulation）などの海外法令への対応も必要になります。

・サイバーセキュリティ基本法
・不正アクセス禁止法
・個人情報保護法
・民法、刑法
・その他のセキュリティ関連法規（電子署名及び認証業務等に関する法律、プロバイダ責任制限法、特定電子メール法）
・知財関連法規（著作権法、産業財産権法、不正競争防止法）
・労働関連・取引関連法規（労働基準法、労働者派遣法、男女雇用機会均等法、公益通報者保護法、労働安全衛生法、下請法、特定商取引法、電子消費者契約法）
・海外法令（GDPR等）
・その他の法律・ガイドライン・技術者倫理
・「非連邦政府組織およびシステムにおける管理対象非機密情報CUIの保護（SP800-171）」
・行政手続における特定の個人を識別するための番号の利用等に関する法律
・デジタル社会形成基本法

国家サイバー統括室（NCO）は、関連法令をQ&A形式で解説する「サイバーセキュリティ関係法令Q&Aハンドブック」を公開しています。自社の業務と照らし合わせながら、効率的・効果的なサイバーセキュリティ対策・法令遵守を実践するとよいでしょう。

●国家サイバー統括室（NCO）関係法令等
https://www.nisc.go.jp/law/

情報管理が不適切な場合の処罰など

個人情報などの法的な管理義務がある情報を適切に管理していなかった場合には、企業の経営者や役員、担当者は下記の表に示すような責任を問われ、処罰されることになります。

法令	条項	処罰など
個人情報保護法 個人情報の保護に関する法律	第173条 委員会からの命令に違反	1年以下の懲役又は100万円以下の罰金
	第179条 個人情報データベース等不正提供罪	1年以下の懲役又は50万円以下の罰金
	第182条 報告及び立入検査 委員会への虚偽の報告など	50万円以下の罰金
	184条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても1億円以下の罰金
マイナンバー法（番号法） 行政手続における特定の個人を識別するための番号の利用等に関する法律	48条 正当な理由なく特定個人情報ファイルを提供	4年以下の懲役若しくは200万円以下の罰金又は併科
	49条 不正な利益を図る目的で、個人番号を提供又は盗用	3年以下の懲役若しくは150万円以下の罰金又は併科
	50条 情報提供ネットワークシステムに関する秘密を漏えい又は盗用	同上
	第51条 不正な手段で個人番号を取得	3年以下の懲役又は150万円以下の罰金
	53条 委員会からの命令に違反	2年以下の懲役又は50万円以下の罰金
	54条 委員会への虚偽の報告など	1年以下の懲役又は50万円以下の罰金
	55条 偽りその他不正の手段により個人番号カード等を取得	6月以下の懲役又は50万円以下の罰金
	57条 両罰規定	従業者等が業務に関し違反行為をした場合、法人に対しても1億円以下の罰金又は各本条が定める罰金

法令	条項	処罰など
不正競争防止法 営業秘密・限定提供データに係る不正行為の防止など	第3条 差止請求権	利益を侵害された者からの侵害の停止又は予防の請求
	第4条 損害賠償	利益を侵害した者は損害を賠償する責任
	第14条 信頼回復措置	信用を害された者からの信用回復措置請求
金融商品取引法 インサイダー取引の規制など	175条 課徴金	違反者の経済的利得相当額
著作権法	第119条1号 著作権等の侵害者 著作者人格権、著作権、出版権、実演家人格権又は著作権隣接権を侵害した者	10年以下の懲役又は1000万円以下の罰金（法人は、3億円以下の罰金（「著作者人格権」「実演家人格権」を除く。））
不正アクセス行為の禁止等に関する法律	第3条 不正アクセス行為の禁止 第4条 不正アクセスにつながる識別符号の不正取得の禁止 第5条 不正アクセス行為を助長する行為の禁止 第6条 不正アクセスにつながる識別符号の保管の禁止	コンピュータに対する不正アクセスや、不正アクセスにつながるID・パスワード等の識別符号の不正取得・保管行為、不正アクセスを助長する行為等をした場合、不正アクセスは3年以下の懲役又は100万円以下の罰金。その他は1年以下の懲役又は50万円等の罰金。
刑法 **不正指令電磁的記録に関する罪（ウイルス作成罪）**	第168条の2 第168条の3 不正指令電磁的記録作成罪等	正当な理由なく、他人のコンピュータにおいて実行させる目的でウイルスを作成・提供・実行した場合、3年以内の懲役又は50万円以下の罰金。保管した場合は、2年以下の懲役又は30万円以下の罰金。
一般データ保護規則（General Data Protection Regulation：GDPR）	EU域内の個人データ取り扱いの制限	EU域内の個人データ保護について規定する。EU域内の個人データを扱う場合はEU以外の企業も対象になる。違反内容によっては高額な制裁金になる。

※参考：「中小企業情報セキュリティ対策ガイドライン第3.1版」を基に最新の情報に更新

情報セキュリティに関する各種フレームワークの概要

フレームワークの有用性

情報セキュリティは、顧客データや機密情報などの重要な情報資産を守るために不可欠です。適切なセキュリティ対策を実施するためには、フレームワークの活用が効果的です。フレームワークを活用することで、リスク管理を体系的に進め、組織のセキュリティレベルを向上させることができます。一方で、フレームワークには様々な種類が存在し、各フレームワークが、どれも必要な全ての対策を網羅しているわけではありません。企業のセキュリティ対策の目的、状況に応じてそれぞれのフレームワークを補完して活用することが望ましいと言えます。

情報セキュリティマネジメントシステム（ISMS）

ISMSは、「Information Security Management System」の略称です。ISMSに関する国際規格が存在していることから、ISMSはセキュリティフレームワークの中でも代表的なものとなっており、業種業態を問わず、セキュリティ対策の全体の枠組みと網羅的な対策項目を提示しています。

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

CHECK サイバーセキュリティフレームワーク(CSF)

CSFは「Cybersecurity Framework」の略称です。NIST（米国国立標準技術研究所）が定義するサイバーセキュリティ対策アプローチの中で最も上位に位置付けられており、重要インフラを主な対象としています。サイバーセキュリティを企業リスクの一つと位置づけ、経営層の主導で対策と改善を行うことを推奨し、セキュリティ管理手法の概念や管理方針・体制の整備など包括的な内容が記載されています。

CHECK サイバー・フィジカルセキュリティ対策フレームワーク（CPSF）

CPSFは、ISMSやCSFのフレームワークの内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策を整理するためのフレームワークです。Society5.0を意識したセキュリティリスクとその対策方法について記述されている点が特徴です。

CHECK 代表的なセキュリティフレームワーク

・ISO/IEC27017
　クラウドサービス提供者とクラウドサービス利用者の双方を対象にした規格。

・PMS（個人情報保護マネジメントシステム）
　組織が業務上取扱う個人情報を安全で適切に管理するための仕組み。

・サイバーセキュリティ経営ガイドライン
　サイバー攻撃から企業を守るために必要な事をまとめたガイドライン

主な参考文献

発行元	タイトル
国家サイバー統括室 (NCO 旧:NISC)	・国家サイバー統括室 ・サイバーセキュリティ基本法 (e-Gov法令検索) ・個人情報の保護に関する法律 (e-Gov法令検索) ・サイバーセキュリティ戦略 ・サイバーセキュリティ 2025 (2024年度年次報告・2025年度年次計画) ・重要インフラのサイバーセキュリティの確保に関する主な資料 ・政府機関等のサイバーセキュリティ対策のための統一基準群 ・政府機関等における情報システム運用継続計画ガイドライン ・関係法令Q&Aハンドブック ・サイバーセキュリティポータル 目的や所属・役割から選ぶ施策一覧 ・サイバー攻撃対応事例 ・インターネットの安全・安心ハンドブック
内閣府	・経済財政運営と改革の基本方針 2025 ・知的財産戦略本部 ・デジタル社会形成基本法 (e-Gov法令検索) ・Society 5.0 ・サイバー・フィジカル・セキュリティ対策検討ガイドブック
デジタル庁	・デジタル社会の実現に向けた重点計画 ・デジタル社会推進標準ガイドライン ・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 ・ゼロトラストアーキテクチャ 適用方針 ・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
総務省	・情報通信白書 ・DX時代における企業のプライバシーガバナンスガイドブック ・サイバー攻撃被害に係る情報の共有・公表ガイダンス ・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
文部科学省	・科学技術・イノベーション白書

発行元	タイトル
経済産業省	・サイバーセキュリティ政策 ・サイバーセキュリティ経営ガイドライン ・産業界のデジタルトランスフォーメーション（DX） ・AI事業者ガイドライン ・情報セキュリティ監査基準及び情報セキュリティ管理基準について ・サイバー・フィジカル・セキュリティ対策フレームワーク ・ASM導入ガイダンス
独立行政法人 情報処理推進機構 (IPA)	・情報セキュリティ白書 ・DX動向2025 ・情報処理技術者試験・情報処理安全確保支援士試験 ・デジタルスキル標準 ・iコンピテンシ ディクショナリ (iCD) ・情報システム・モデル取引・契約書 ・セキュリティ関連費用の可視化 ・サイバーセキュリティ経営可視化ツール ・ECサイト構築・運用セキュリティガイドライン ・中小企業の情報セキュリティ対策ガイドライン ・情報セキュリティ10大脅威
個人情報保護委員会	・EU（外国制度）GDPR（General Data Protection Regulation：一般データ保護規則）
JPCERT/CC	・インシデントハンドリングマニュアル
日本情報経済社会推進協会 (JIPDEC)	・ISMS適合性評価制度 ・ISMS/ITSMS/BCMS認証に関するガイド類 ・個人情報保護法規則/ガイドライン改正の実務対応のポイント
米国国立標準技術研究所(NIST)規格	・Cybersecurity and privacy ・Cybersecurity Framework (CSF)
東京都	・中小企業向け サイバーセキュリティ対策の極意ポータル ・文章生成AI利活用ガイドライン・活用事例集

用語解説インデックス

【A】AI 132,142

Android 38
スマートフォン用のOSの1つ

【B】BEC 11,52
Business Email Compromise（ビジネスメール詐欺）

【C】CISO 118,199
Chief Information Security Officer（最高情報セキュリティ責任者）

CPS 131
Cyber-Physical System

CSIRT 125,128
Computer Security Incident Response Team

CSR 124
corporate social responsibility（企業の社会的責任）

【D】DDoS攻撃 31
複数のネットワークに分散する大量のコンピューターが一斉に特定の対象に送信し、通信容量をあふれさせて機能を停止させてしまう攻撃

DKIM 83

DMARC 83

DoS攻撃 31
Denial of Servicesの略。企業や組織のWebシステムに大量の通信パケットを送りつけて利用できなくする攻撃

DX 108,131,207,226,228,232
Digital Transformation（デジタル変革）

【E】ECサイト 34,50,191
Electronic Commerceの略でインターネット上で商品やサービスの売買を行うサイト

【G】GDPR 234
General Data Protection Regulation：EU一般データ保護規則

【I】ICカード 78

ID 29,42,74,76,78,140
Identificationの略。コンピューターシステムで利用者を識別するための符号

IoT 46,132,134,136,138,143,228

IPアドレス 83,86
Internet Protocol Addressの略で、ネットワーク上にあるコンピューターや通信機器を判別するための番号

IT 21,76,100,108,114,130,221
Information Technologyの略で情報技術の総称

IT-BCP 131,160
IT-Business Continuity Plan（ITにおける事業継続計画）

ITSS+ 231
IT skill standard +（ITスキル標準プラス）

ITガバナンス 111
IT governance：企業がITへの投資や効果、リスクを継続的に最適化するために構築する組織的な仕組み

【N】NAS 205
Network Attached Storageの略でネットワークに接続された記憶装置

NIST 105,238
National Institute of Standards and Technology（米国国立標準技術研究所）

NOTICE 47,143

【O】OS 27,68
Operating Systemの略。パソコンを動かすための基本ソフトウェア

【P】PDCA 118,124
Plan（計画）、Do（実行）、Check（評価）、Act（改善）の繰り返しで管理業務を円滑に進める手法の1つ

【S】SECURITY ACTION 127

SNS 75,161

Society5.0 131,134,141
狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すもの

SPF 83

【U】URL 27,36,85,87,89
URLとは、インターネット上に存在する情報の位置を記述するためのデータ形式

USBメモリー 32,71,78
Universal Serial Bus。パソコンなどに周辺機器を簡単に接続するための記憶媒体

UTM 71,86

【W】Webアプリケーション 29

Webサーバー 28
ホームページや情報・機能を提供するコンピューター

Webサービス 28,42,74
Webアプリケーションを使い、ネットワークを通じてソフトウェアの機能を利用できるようにしたもの

【あ】アカウント 35
ユーザーがネットワークやコンピューターにログインするための権利

アクセス権 33,76
コンピューターやネットワーク、データベースなどを利用する権利

アップデート 39,68
ソフトウェアやアプリケーションを最新の状態にすること

アプリ 38
スマートフォンなどで、さまざまな機能を提供するプログラム

暗号化 26,78,82
データの内容を他人には分からなくするための方法

暗号化技術（SSL） 83

【い】インシデント 21,118,223
コンピューターやネットワークのセキュリティを脅かす事象。セキュリティインシデントとも呼ぶ

インターネットバンキング 5,36
コンピューターを使ってインターネット経由で銀行などの金融機関のサービスを利用すること

【う】ウイルス 6,21

【か】可用性 76,92

完全性 76,92

【き】機密性 76,92

共有サーバー 27
情報や機能を共有で使用するサーバー

共有設定 205
プリンターやデータなどを複数人で共有できるよう設定すること

【く】クラウドサービス 123,209,224

クリアスクリーン 94,220

クリアデスク 94,220

【こ】個人情報保護法 142,234

コンテンツ 35
WebサイトやDVD、CD-ROMに含まれる情報の内容

コンテンツフィルター 106
業務上不要または有害な内容を含むWebサイトへの接続を制限する機能

【さ】サイバー空間(仮想空間) 131,238

サイバーセキュリティ 21,105

残留リスク 111,121

【し】指紋認証 78
指紋を利用する生体認証

情報資産 76,93,211,219

情報セキュリティ 21

【す】スクリーンセーバー 95
パソコン操作をしない間、画面を図形や模様などで隠す機能

スタンドアロン 97

スパムメール 84
不特定多数に対して送信される広告や詐欺的な内容を主としたメール

スリープモード 95
パソコン操作をしない間、省電力のため画面が暗くなる機能。第三者による操作やのぞき見防止にもなる

【せ】脆弱性（ぜいじゃくせい） 28,34,44,69

セキュリティコード 173
クレジットカード裏面に印字されている3桁の番号

セキュリティ・バイ・デザイン 120
Security by Design：企画・設計段階から必要なセキュリティ対策を施しておくという考え方

セキュリティホール 29,69
ソフトウェアの設計ミスなどによって生じたセキュリティ上の弱点

セキュリティポリシー 106,119

センサー 132
音や光、温度、振動などを検出して信号に変える装置

【そ】ソーシャルエンジニアリング 43
social engineering：人間の心理的な隙や、行動のミスにつけ込んで、IT技術を使用せずに秘密情報を入手する方法

外付けハードディスク 27
パソコン本体にケーブルで接続するタイプのハードディスク装置

ソフトウェア 27,28,68
コンピューターを動作させる命令や処理手順のまとまり

【た】第4次産業革命 131
蒸気機関（第1次）、電気機器（第2次）、コンピュータ（第3次）に続くAI等の技術、デジタル情報を活用した産業構造の変革を示す

多要素認証 43,75
サービス利用時の利用者の認証を、複数の要素を用いて行うもの

【て】定義ファイル 21
コンピューターウイルスの特徴を記録したファイル

テザリング 81
スマートフォンなどを経由してパソコンをインターネットに接続する方法

テレワーク 80,91
ICT機器等を活用して、時間や場所の制約を受けずに、柔軟に働くことができる形態

電子証明書 89
信頼できる第三者（認証局）が本人であることを証明するもの

【と】同報メール 82
同じ内容のメールを複数の人へ同時に送付すること

トロイの木馬 21
正体を偽ってコンピューターへ侵入し、破壊活動を行うプログラム

【な】なりすまし 42,52
他人のIDとパスワードを使用し、その人のふりをして活動すること

【ね】ネットワークカメラ 46
主にネットワーク上に設置されたカメラ。監視カメラなどに用いられる

【は】パターンファイル 21
定義ファイルと同じ

ハッキング 2
他人のコンピューターや通信システムを不正な手段で勝手に操作したり、不正に機密情報を入手したりすること

バックアップ 27,72,166,219
データの破損や損失に備えて複製を作成して保管すること

【ひ】ビッグデータ 132,134,228

標的型攻撃 24,84

【ふ】ファイアウォール 106,204
外部から送られてくる通信を制御・監視し安全を保持するための仕組み

5G 131,134,136
5th Generation（第5世代移動通信システム）

フィジカル空間（現実空間） 131,141

フィッシング詐欺 36

フィルタリング 51,90
特定のWebサイトや迷惑メールなどを選別・閲覧制限する仕組み

踏み台 6,46
外部の第三者に乗っ取られ、不正アクセスの中継地点や迷惑メールの発信源などに利用されてしまうこと

プラス・セキュリティ人材 232
本来の業務を担いながらITを利活用する中でセキュリティスキルも必要となる人材

【へ】ベンチマーク 113
比較のために用いる指標

【ほ】ボットネットウイルス 21
ボットはロボットの略。攻撃者が遠隔から操作して、別のコンピューターへの攻撃の踏み台にする。ボットネットは、外部からの指令で一斉に攻撃を行わせるネットワークのこと

ポップアップ画面 37
Webページ上に、自動的に新しいウインドウが開いて表示される画面

【ま】マイナンバー 159
住民票を有する個人に割り当てられた12桁の番号

マルウェア 21,71
Malicious software（悪意のあるソフトウェア）の略語。コンピューターの正常な利用を妨げたり、利用者やコンピューターに害を成す不正な動作を行うソフトウェアの総称

【め】メーリングリスト 69,129
あらかじめ登録した複数の人に同じメールを同時配信できる仕組み

メールサーバー 83,86
メールの送受信を行うためのサーバーのこと

【も】モバイル端末 79,100
インターネットに接続できる携帯電話やタブレット端末などの通信機器

【よ】溶解処分 97
紙の重要情報を主に水と機械で溶かして処分する方法。専門業者に依頼

【ら】ランサムウェア 26

【り】リモート管理 29
離れた場所にあるコンピューターを通信回線などを通じて管理すること

【ろ】ログ 29,123
コンピューターなどの内部で起こった出来事についての情報を時系列に記録・蓄積したデータ

【わ】ワーム 21
自立的に動作する不正プログラムで、コンピューターに侵入し、破壊活動や別のコンピューターへの侵入などを行う

ワンクリック詐欺 40,89

ワンタイムパスワード 5,37
認証方法の1つで、ワンタイム（＝1回）限りで短時間のみ有効な"使い捨て"パスワードのこと

中小企業向け
サイバーセキュリティ対策の極意 Ver 4.0

平成29年11月第1.0版　令和8年3月第4.0版 発行
編集・発行　東京都産業労働局商工部経営支援課
新宿区西新宿二丁目8番1号
電話番号　03（5320）4770

印刷　株式会社　シンソークリエイト

登録番号　（5）155

協力
東京中小企業サイバーセキュリティ支援ネットワーク（Tcyss）

※掲載の情報は令和7年12月現在のものです

VEGETABLE OIL INK

リサイクル適性Ⓐ
この印刷物は、印刷用の紙へリサイクルできます

中小企業向け

サイバーセキュリティ対策の極意

Ver 4.0

東京都