

第１編　サイバーセキュリティを取り巻く背景

第２編　中小企業に求められるサイバーセキュリティ対策

令和6年度

中小企業サイバーセキュリティ

社内体制整備事業

[第0編. はじめに 4](#_Toc174086561)

[第0章. テキストの活用 4](#_Toc174086562)

[0-1. テキストの目的、想定読者、全体構成、テキストの利用方法など 5](#_Toc174086563)

[0-1-1. テキストの目的、想定読者 5](#_Toc174086564)

[0-1-2. 全体構成 5](#_Toc174086565)

[0-1-3. テキストの利用方法 6](#_Toc174086566)

[第1編. サイバーセキュリティを取り巻く背景【レベル共通】 7](#_Toc174086567)

[第1章. デジタル時代の社会とIT情勢 7](#_Toc174086568)

[1-1. デジタル時代の社会変革とIT情勢の関係性 8](#_Toc174086569)

[第2章. サイバーセキュリティの基礎知識 11](#_Toc174086570)

[2-1. 導入済みと想定するセキュリティ対策機能 12](#_Toc174086571)

[2-2. SECURITY ACTION（セキュリティ対策自己宣言） 13](#_Toc174086572)

[2-2-1. SECURITY ACTION 二つ星レベル 13](#_Toc174086573)

[2-2-2. 情報セキュリティ5か条 14](#_Toc174086574)

[2-2-3. 情報セキュリティ自社診断 15](#_Toc174086575)

[2-2-4. 情報セキュリティ基本方針 17](#_Toc174086576)

[2-3. サイバーセキュリティアプローチ方法 19](#_Toc174086577)

[コラム 23](#_Toc174086578)

[第3章. デジタル社会の方向性と実現に向けた国の方針 24](#_Toc174086579)

[3-1. 国の基本方針および実施計画の要約 25](#_Toc174086580)

[3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題 27](#_Toc174086581)

[3-2-1. デジタル社会の実現に向けた重点計画 27](#_Toc174086582)

[3-2-2. Society5.0 31](#_Toc174086583)

[3-2-3. DXの推進 33](#_Toc174086584)

[第4章. サイバーセキュリティ戦略および関連法令 37](#_Toc174086585)

[4-1. NISC：サイバーセキュリティ戦略 38](#_Toc174086586)

[4-1-1. サイバーセキュリティ戦略 38](#_Toc174086587)

[4-1-2. サイバーセキュリティ2024 43](#_Toc174086588)

[4-2. 企業経営に重要なDX推進とセキュリティ確保の両立 46](#_Toc174086589)

[4-2-1. 企業経営のためのサイバーセキュリティの考え方 46](#_Toc174086590)

[4-2-2. DX with Cybersecurity 48](#_Toc174086591)

[4-3. 関連法令 50](#_Toc174086592)

[4-3-1. 個人情報保護法 50](#_Toc174086593)

[4-3-2. GDPR 51](#_Toc174086594)

[4-3-3. その他関連法令 52](#_Toc174086595)

[編集後記 54](#_Toc174086596)

[第2編. 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策【レベル共通】 55](#_Toc174086597)

[第5章. 事例を知る：重大なインシデント発生から課題解決まで 55](#_Toc174086598)

[5-1. 情報セキュリティの概況 56](#_Toc174086599)

[5-1-1. 情報セキュリティの脅威を学ぶ 56](#_Toc174086600)

[5-1-2. IPA：情報セキュリティ白書から見る脅威 57](#_Toc174086601)

[5-1-3. IPA：情報セキュリティ10大脅威 59](#_Toc174086602)

[5-2. 重大インシデント事例から学ぶ課題解決 64](#_Toc174086603)

[5-2-1. インシデント事例から学ぶ 64](#_Toc174086604)

[5-2-2. 最近の攻撃トレンド、および中小企業にも発生しうるサイバー被害事例 65](#_Toc174086605)

[5-2-3. 事案発生->課題の抽出->再発防止策の実施までの流れ 67](#_Toc174086606)

[5-2-4. インシデントから得た気づきと取組 68](#_Toc174086607)

[5-2-5. ランサムウェア感染の実態 69](#_Toc174086608)

[5-3. 実際の被害事例から見るケーススタディー 72](#_Toc174086609)

[5-3-1. 最近のサイバー被害事例発生の傾向 72](#_Toc174086610)

[5-3-2. 事例：某港のランサムウェア被害 73](#_Toc174086611)

[5-3-3. 具体的な対応策 74](#_Toc174086612)

[第6章. 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策 75](#_Toc174086613)

[6-1. これからの企業経営で必要な観点：社会の動向 76](#_Toc174086614)

[6-1-1. 現実社会とサイバー空間のつながり 76](#_Toc174086615)

[6-1-2. IT活用における課題 78](#_Toc174086616)

[6-2. 守りのIT投資と攻めのIT投資 82](#_Toc174086617)

[6-2-1. 守りのIT投資、攻めのIT投資の概要 82](#_Toc174086618)

[6-2-2. 経済産業省のDXレポートから見る、「攻めのIT」に取り組む方針について 83](#_Toc174086619)

[6-2-3. ITを活用した生産性の向上（デジタルオプティマイゼーション） 84](#_Toc174086620)

[6-2-4. ITを活用した新たなビジネスの展開（DX） 86](#_Toc174086621)

[6-2-5. 次世代技術を活用したビジネス展開 88](#_Toc174086622)

[6-3. 経営投資としてのサイバーセキュリティ対策 92](#_Toc174086623)

[6-3-1. サイバーセキュリティ対策の重要性 92](#_Toc174086624)

[6-3-2. 経営者が重要視すべき3つのポイント 93](#_Toc174086625)

[編集後記 95](#_Toc174086626)

[引用文献 96](#_Toc174086627)

[参考文献 99](#_Toc174086628)

[用語集 101](#_Toc174086629)

# はじめに

## テキストの活用

|  |
| --- |
| 章の目的 |
| 第0章では、テキストの目的、想定読者、全体構成、利用方法について理解することを目的とします。 |
| 主な達成目標 |
| * テキストの目的、想定読者、全体構成、利用方法を理解すること |

### テキストの目的、想定読者、全体構成、テキストの利用方法など

#### テキストの目的、想定読者

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

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

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

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

#### 全体構成

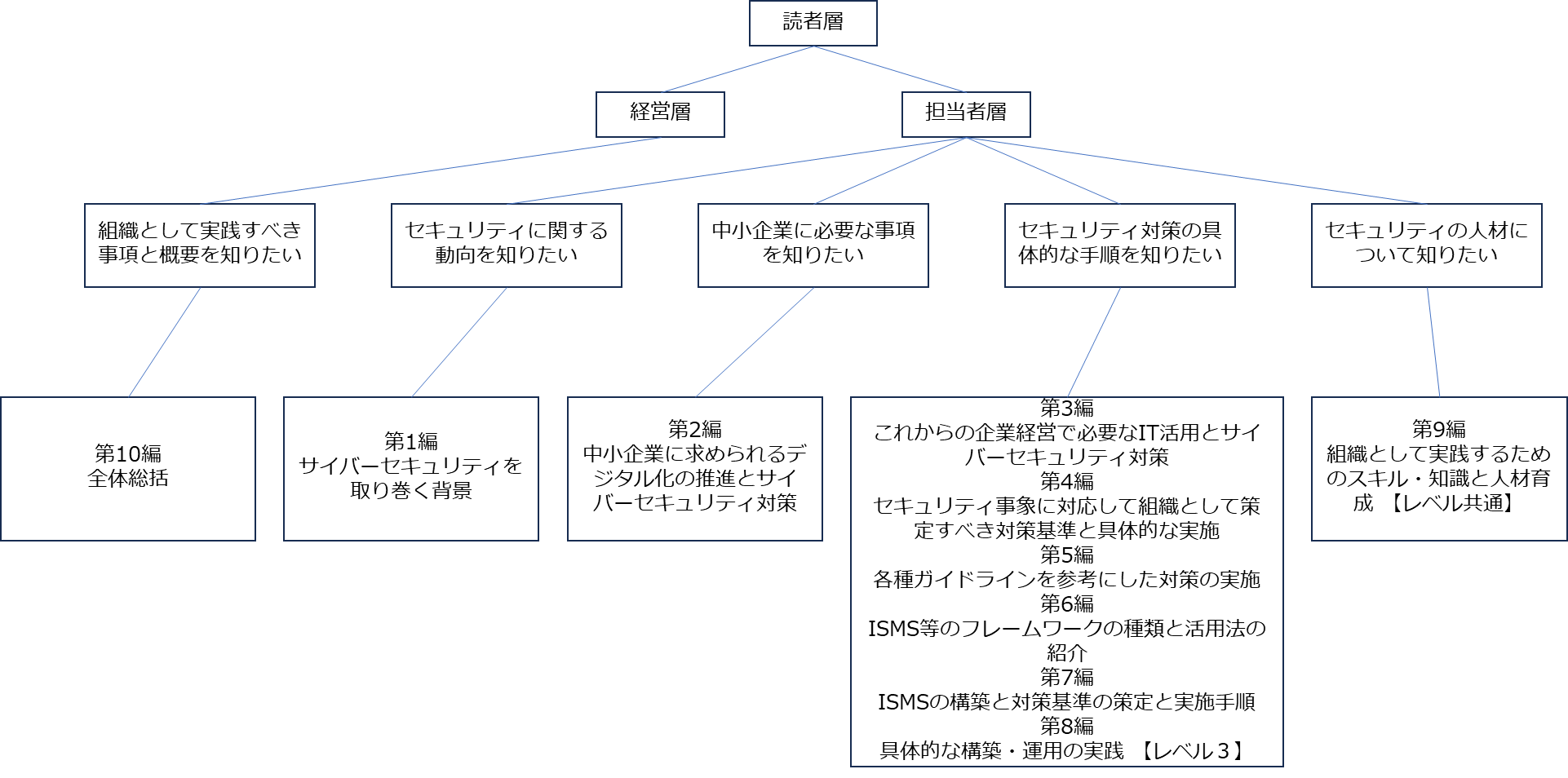
本書の構成は、まずサイバー攻撃の脅威や実際の被害事例を通じて、リスク認識を深めていただきます。次に、ITおよびセキュリティの基礎知識を解説し、セキュリティ対策の要点をまとめています。また、これからの我が国や社会全体の動向についても詳しく解説し、政府や業界団体の取組、最新の技術やトレンドに触れることで、最新の動向への対応力を向上させることを目指しています。さらに、中小企業におけるIT・セキュリティの課題に焦点を当て、人材不足やビジネス上のリスクに対する具体的な解決策を提示します。また、ISMS認証などの代表的なフレームワークの習得、組織内でのセキュリティ管理体制の構築や認証取得に向けた手順を解説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

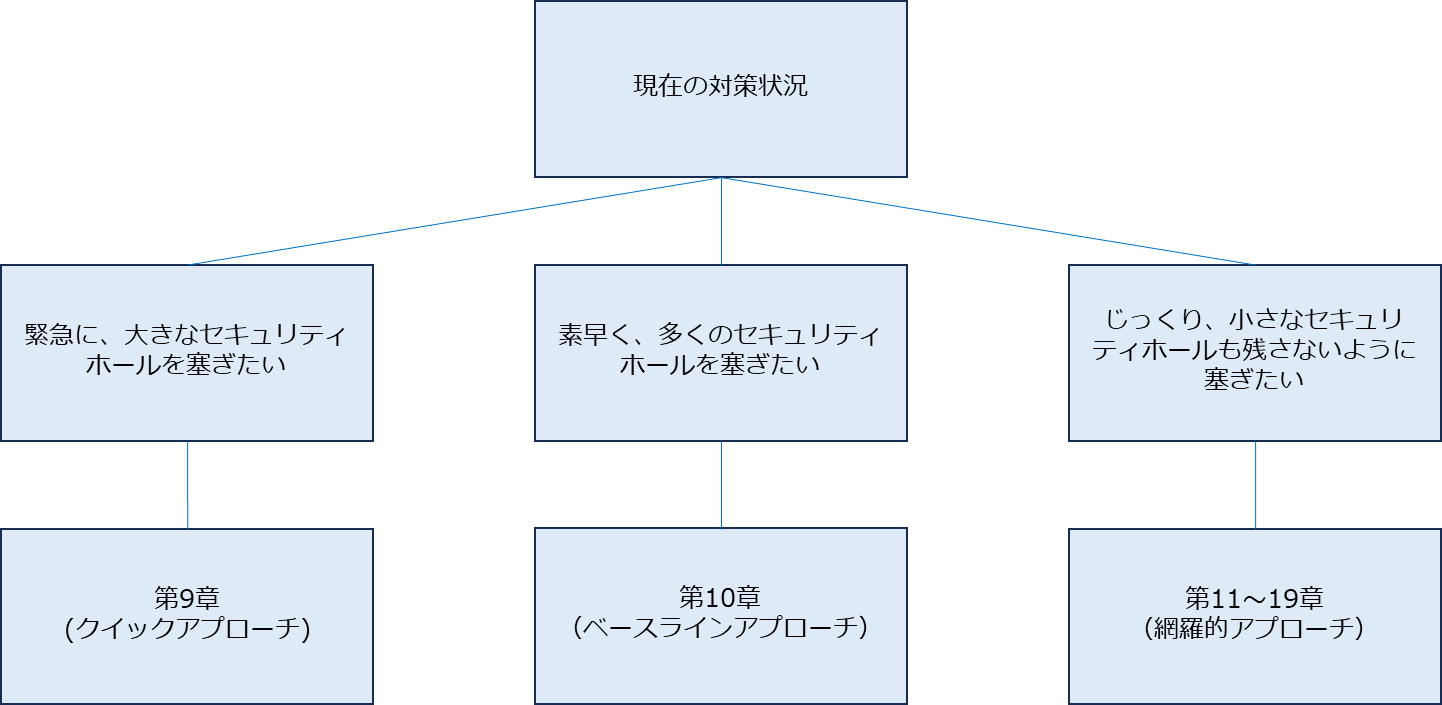
第4編以降ではレベル1～3の分類で、セキュリティ対策のレベル感ごとに説明していきます。レベル1では、緊急性の高い事例に対処する際の手法を解説します。レベル2では、ガイドラインなどを用いて、組織全体として最低限実施すべきセキュリティ対策を解説します。レベル3では、セキュリティのフレームワークを用いて、より多くの攻撃や攻撃手法に対して網羅的に対応するための事項を説明します。

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

#### テキストの利用方法

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

以下に示すナビゲーションフローを参照して、自分に特に重要な内容が記載されている箇所を確認してください。



# サイバーセキュリティを取り巻く背景【レベル共通】

## デジタル時代の社会とIT情勢

|  |
| --- |
| 章の目的 |
| 第1章では、現代社会のITに関する情勢を学ぶことを目的とします。また、日本がSociety5.0の実現を目指す中、企業がビジネスを発展させるためにDXを推進していく重要性を明確にすることを目的とします。 |
| 主な達成目標 |
| * ITに関する社会の動向を把握し、Society5.0とDXの関係性を理解すること |

### デジタル時代の社会変革とIT情勢の関係性

##### 社会の現状と今後の動向（Society5.0）

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

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

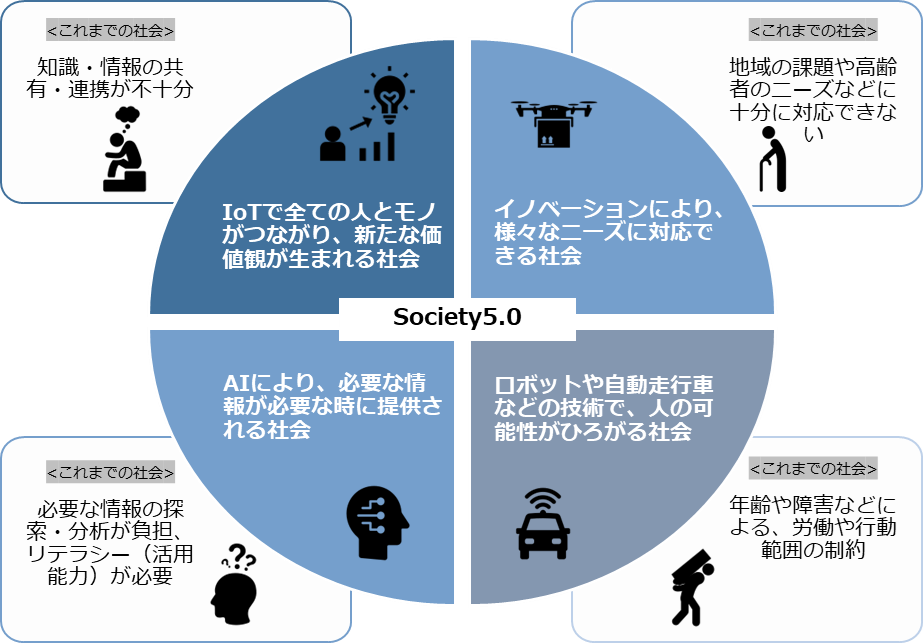
しかしながら、Society5.0を実現するためには、企業や組織がDXを進め、デジタル化を推進することが不可欠です。DXは、従来のビジネスモデルやプロセスに対する革新的なアプローチであり、さまざまな利点をもたらします。また、大企業と比べ人手や予算などの企業リソースが限定されている中小企業こそ、新たなサービスを創造し、ビジネスを発展させるために、DXを推進することが重要です。

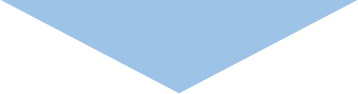
図1. Society5.0の概要図

（出典）内閣府.”Society5.0”.<https://www8.cao.go.jp/cstp/society5_0>

##### デジタルトランスフォーメーション（DX）とは

ここでは、DXの定義を紹介し、DXの概要を説明します。

|  |
| --- |
| DXの定義 |
| DXとは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズをもとに、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること[[1]](#footnote-2) |
| DXの概要 |
| DXとは、データやデジタル技術を活用して、顧客視点で新たな価値を創出することです。このためには、ビジネスモデルや企業文化などの変革が必要です。DXを推進するためのDX戦略では、まず経営者が自社の理念や存在意義を明確にし、将来の経営ビジョン（5年後や10年後にどのような企業になりたいか）を具体的に描きます。次に、そのビジョンの実現に向けて関係者を巻き込みながら、現在の状況と目標との差を埋めるために解決すべき課題を整理します。そして、デジタル技術を活用してこれらの課題を解決し、ビジネスモデルや組織、企業文化などを変革することで、経営ビジョンの実現を目指します。  また、DXを推進するにあたり、「知識」「人材」「セキュリティ」の3点が重要なキーワードとなります。 |



|  |  |  |
| --- | --- | --- |
| DXを進めるにあたり必要な3要素 | | |
| 知識  ITの基礎知識のほか、ビッグデータなどを活用するためのデータサイエンスの知識やAI・ブロックチェーンなどの最新技術の知識を取り入れる必要があります。 | 人材  業務内容に精通し、求められる要件を新たな技術・手法を用いて実装することができるような人材が求められます。 | セキュリティ  自宅でのリモートワークやクラウドサービスなどを利用するため必然的にセキュリティの強化が必要となります。 |

##### 生成AIとは

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

|  |
| --- |
| 生成AIの概要 |
| 生成AIとは、既存のデータの解析と学習を通じて新たなコンテンツを生成するAI（人工知能）のことです。生成AIはディープラーニングによって自ら学習したデータをもとに、人が作り出すようなテキスト、画像、音楽、映像などのコンテンツを生み出すことができます。  従来のAIが、大量の学習データをもとに結果を予測し、ある行為を自動的に実行していたのに対して、生成AIは人間が与えていない情報やデータから新たなコンテンツを生み出すことができる点で大きな違いがあります。 |
| 生成AIの活用 |
| 生成AIはさまざまな業務において実用的に活用できるレベルに進化しています。例えばカスタマーサポートでは生成AIを用いたチャットボットに24時間365日対応してもらうことで、顧客の問い合わせに即座に対応できるようになります。広告制作では、バナーやプロモーション用のビジュアルを迅速に、かつ何種類も短時間で生成できます。  このように、生成AIを活用することによって、多くの業務プロセスを効率化することが可能です。 |
| 生成AIにおけるセキュリティの概念 |
| 生成AIは、攻撃者によってフィッシング攻撃の効率を高めるために悪用される可能性があります。生成AIを使うことで、個々のターゲットに対してパーソナライズされたフィッシングメールを生成することができるため、攻撃の成功率が高まります。また、生成AIは自然言語処理技術を用いて、より自然で信頼性の高いメッセージを生成することができるため、受信者が騙されやすくなります。これに対しては、メールの送信元をよく確認する、リンクのURLを不用意にクリックしないなど、従来のフィッシング対策と同様に気をつける必要があります。  また、情報漏えいのリスクもあります。これは、業務上の機密情報や、個人情報を生成AIに入力してしまうリスクです。生成AIに送信された情報は、提供元の開発者に見られてしまったり、学習データとして使われたりして、情報漏えいにつながってしまう可能性があります。漏えいしてはいけない情報は、生成AIには入力しないように気をつけましょう。 |

## サイバーセキュリティの基礎知識

|  |
| --- |
| 章の目的 |
| 第2章では、サイバーセキュリティの基本的な知識や対策などについて振り返りつつ、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を明確にすることを目的とします。 |
| 主な達成目標 |
| * UTM、EDRの機能を再確認すること * 企業が自ら実施できる基本的なセキュリティ対策を再確認すること * リスクと活用可能なリソースを考慮した脅威への対処方法を理解すること |

### 導入済みと想定するセキュリティ対策機能

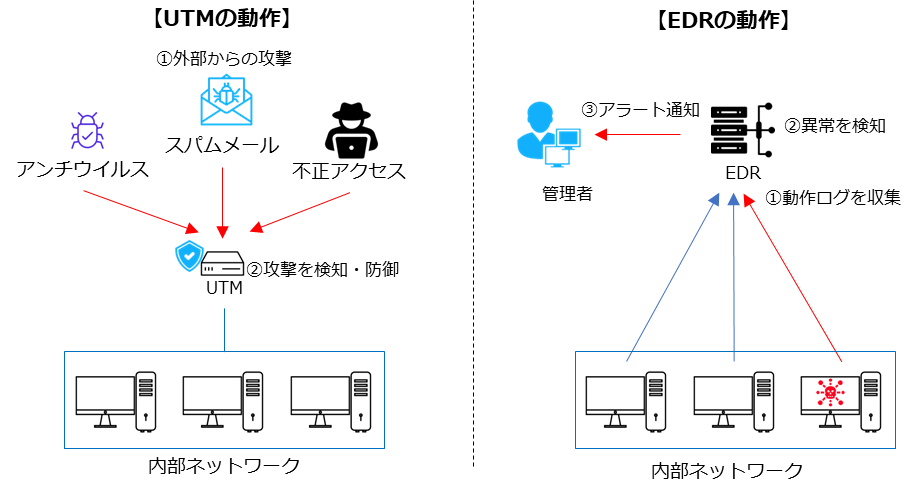
セキュリティ対策は、大企業のみならず中小企業においても重要視されています。特に、ランサムウェアなどのサイバー攻撃のリスクが高まっており、中小企業も十分なセキュリティ対策を講じる必要があります。本テキストの対象読者は、UTMとEDR相当機能のセキュリティ対策は導入済みであることを想定しています。しかしながら、セキュリティの脅威は常に進化しており、新たな攻撃手法や脆弱性が発見されることがあります。ここでは、UTM、EDRの機能について振り返りますが、さらなるセキュリティ対策についての詳細は本テキストの後半で説明します。

図2. UTM、EDRの概要図

|  |
| --- |
| UTM（Unified Threat Management） |
| UTMは、日本語で「統合脅威管理」と訳されます。UTMは複数のセキュリティ機能を1つの機器に集約したもので、ネットワーク全体のトラフィックを監視・管理します。UTMには、ファイアウォール、侵入検知システム、ウイルス対策などが統合されており、内部ネットワークに対する外部からの侵入や攻撃を防御します。そのため、企業・組織内のネットワークセキュリティ対策としてUTMの導入は有効な手段です。 |
| EDR（Endpoint Detection and Response） |
| EDRは、エンドポイント（PC、スマホ、サーバなど）における脅威の検知および対応を可能にします。従来のアンチウイルスソフトウェアでは、ウイルス定義ファイルにないマルウェアは検知できませんでしたが、EDRでは、エンドポイント上の不審な動作を検知することができます。また、検知した脅威に対して、悪意のあるプロセスの終了、感染したエンドポイントの隔離などの適切な対応を行います。そのため、EDRを活用することで、セキュリティインシデントの早期発見と迅速な対応が可能になり、エンドポイントの保護が強化されます。 |

### SECURITY ACTION（セキュリティ対策自己宣言）

#### SECURITY ACTION 二つ星レベル

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

宣言企業数（令和6年5月31日時点）：一つ星：302,264社：二つ星：32,630社[[2]](#footnote-3)

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

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

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

|  |
| --- |
| 取得時における注意点  「SECURITY ACTION」はセキュリティ対策状況などをIPAが認定するものではありません。「SECURITY ACTION」の取組に関してWebサイトなどにおいて次のような不適切な表現を使用されますと、第三者の誤解を生ずる可能性が懸念されますので、ご注意願います。  ×「一つ星（二つ星）の認定を受けました」「一つ星（二つ星）を取得しました」  〇「一つ星（二つ星）を宣言しました」 |

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

#### 情報セキュリティ5か条

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

(出典) IPA「情報セキュリティ5か条」をもとに作成

|  |  |
| --- | --- |
| 1.OSやソフトウェアは常に最新の状態にしよう！  OSやソフトウェアを古いまま放置していると、セキュリティ上の問題が解決されず、悪意のあるウイルスに感染してしまう危険性があるため、最新の状態にします。 | |
| 対策: | * パソコンやルータのソフトウェアやファームウェアを最新化します。 * OSやソフトウェアアップデートを実行します。 |
| 2.ウイルス対策ソフトを導入しよう！  ID・パスワードを盗まれないようにウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにします。 | |
| 対策: | * ウイルス定義ファイルが自動更新されるように設定します。 * 統合型のセキュリティ対策ソフトを導入します。 |
| 3.パスワードを強化しよう！  パスワードが推測や解析されたり、流出したID・パスワードが悪用されたりすることで、不正にログインされます。パスワードは長く、複雑に、使い回さないようにします。 | |
| 対策: | * 同じID、パスワードを複数サービス間で使い回さないようにします。例として、10文字以上で「大文字」「小文字」「数字」「記号」を含めます。また、「名前」「電話番号」「誕生日」「簡単な英単語」等は使わず、推測できないようにします。 |
| 4.共有設定を見直そう！  データ保管等のWebサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、Webサービスや機器を使うことができるような設定になっていないことを確認します。 | |
| 対策: | * Webサービス、ネットワーク接続の複合機・カメラ等の共有範囲を限定します。 * 従業員の異動や退職時には速やかに設定を変更（削除）します。 |
| 5.脅威や攻撃の手口を知ろう！  取引先や関係者と偽ってウイルス付きのメールを送る巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとります。 | |
| 対策: | * IPA等のセキュリティ専門機関のWebサイトやメールマガジンで最新の脅威や攻撃の手口を知ります。 * インターネットバンキングやクラウドサービス等が提供する注意喚起を確認します。 |

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| 情報セキュリティ5か条 | https://www.ipa.go.jp/security/security-action/download/5point\_poster.pdf |

#### 情報セキュリティ自社診断

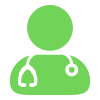
「5分でできる！情報セキュリティ自社診断」を利用することで、自社のセキュリティ対策が、どれくらい実施できているかを把握できます。自社診断は、次ページに示す25項目の設問に答えるだけでセキュリティ対策の実施状況が把握できます。

##### 分類

|  |
| --- |
| Part1 基本的対策  No.1~5は企業の規模や形態を問わず、必須の5項目です。いずれも一度行えば良いものではなく、継続的な実施が欠かせないため、運用ルールとして社内に定着させる必要があります。 |
| Part2 従業員としての対策  No.6~18は従業員として注目すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威が日々変化しているので、油断しないように注意する必要があります。 |
| Part3 組織としての対策  No.19~25は組織としての方針を定めた上で、実施すべきセキュリティ対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにします。 |

##### 診断方法

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

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

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

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

(出典) IPA「 5分でできる！情報セキュリティ自社診断」をもとに作成

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

##### 「5分でできる！情報セキュリティ自社診断」

|  |  |  |
| --- | --- | --- |
| No | | 診断内容 |
| 基本的対策 | 1 | パソコンやスマホ等情報機器のOSやソフトウェアは常に最新の状態にしていますか？ |
| 2 | パソコンやスマホ等にはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？ |
| 3 | パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？ |
| 4 | 重要情報に対する適切なアクセス制限を行っていますか？ |
| 5 | 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？ |
| 従業員としての対策 | 6 | 電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？ |
| 7 | 電子メールやFAXの宛先の送信ミスを防ぐ取組みを実施していますか？ |
| 8 | 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワード等で保護していますか？ |
| 9 | 無線LANを安全に使うために適切な暗号化方式を設定する等の対策をしていますか？ |
| 10 | インターネットを介したウイルス感染やSNSへの書き込み等によるトラブルへの対策をしていますか？ |
| 11 | パソコンやサーバのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？ |
| 12 | 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫等に安全に保管していますか？ |
| 13 | 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？ |
| 14 | 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？ |
| 15 | 関係者以外の事務所への立ち入りを制限していますか？ |
| 16 | 退社時にノートパソコンや備品を施錠保管する等盗難防止対策をしていますか？ |
| 17 | 事務所が無人になる時の施錠忘れ対策を実施していますか？ |
| 18 | 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？ |
| 組織としての対策 | 19 | 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさない等のルールを守らせていますか？ |
| 20 | 従業員にセキュリティに関する教育や注意喚起を行っていますか？ |
| 21 | 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？ |
| 22 | 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？ |
| 23 | クラウドサービスやWebサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？ |
| 24 | セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成する等準備をしていますか？ |
| 25 | 情報セキュリティ対策（上記1～24等）をルール化し、従業員に明示していますか？ |

(出典) IPA「 5分でできる！情報セキュリティ自社診断」をもとに作成

#### 情報セキュリティ基本方針

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

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

|  |
| --- |
| 情報セキュリティ基本方針（サンプル）  株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪等の脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取組みます。  1.経営者の責任  当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。  2.社内体制の整備  当社は、情報セキュリティの維持および改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。  3.従業員の取組み  当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取組みを確かなものにします。  4.法令および契約上の要求事項の遵守  当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。  5.違反および事故への対応  当社は、情報セキュリティに関わる法令違反、契約違反および事故が発生した場合には適切に対処し、再発防止に努めます。  制定日：20○○年○月○日  株式会社○○○○  代表取締役社長 ○○○○ |

(出典) IPA「情報セキュリティ基本方針（サンプル）」をもとに作成

情報セキュリティ基本方針の記載項目例

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

### サイバーセキュリティアプローチ方法

サイバーセキュリティの脅威に対処するためには、効果的なサイバーセキュリティ戦略を構築し、段階的なアプローチをとることが必要です。（Lv1.クイックアプローチ、Lv2.ベースラインアプローチ、Lv3.網羅的アプローチ）

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

|  |  |
| --- | --- |
| 緊急に、大きなセキュリティホールを塞ぐ | Lv.1 クイックアプローチ |
| 実施手法  報道されるような事象・セキュリティ脅威に緊急対応します。 |
| 活用できる文書/ツール名称（例）   * 情報セキュリティ10大脅威（出典：IPA） * 情報セキュリティ白書2023（出典：IPA） * サイバー攻撃を受けた組織における対応事例（出典：NISC） |

|  |  |
| --- | --- |
| 素早く、多くのセキュリティホールを塞ぐ | Lv2. ベースラインアプローチ |
| 実施手法  ガイドブック、ひな型を参照し、迅速にセキュリティ対応します。 |
| 活用できる文書/ツール名称（例）   * リスク分析シート（出典：IPA） * セキュリティ関連費用の可視化（出典：IPA） * 中小企業の情報セキュリティ対策ガイドライン第3版（出典：IPA） |

|  |  |
| --- | --- |
| じっくり、小さなセキュリティホールも残さないように塞ぐ | Lv3. 網羅的アプローチ |
| 実施手法  網羅的なセキュリティ対策が定義されているフレームワークに沿ってセキュリティ対応します |
| 活用できる文書/ツール名称（例）   * ISMS（ISO/IEC27001:2022,27002:2022） * NIST サイバーセキュリティフレームワーク（CSF） * サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） |

**凡例）「〇:あり / △：部分的にあり / ×:なし」**

|  |  |  |  |
| --- | --- | --- | --- |
| Lv.1 クイックアプローチ | | 網羅性 | 即時性 |
| クイックアプローチは、サイバーセキュリティにおける即時の対応や緊急事態への対処に適しています。ただし、長期的な戦略や継続的な改善を妨げることなく、将来的なセキュリティの向上を見据えた計画の策定も必要となります。   * 小規模な対策や修正を迅速に実施可能 * 低コストでリスクを軽減 * 進行中の攻撃へ対応することにより、攻撃の拡大や影響を最小限に抑える | | × | 〇 |
| 1．脅威の特定 | 既知の脅威/過去のインシデントに基づいて、リスクの優先度付けを行いリスクを特定します。 | | |
| 2．対応計画 | 既存のセキュリティ対策の評価を行い、改善点を特定し対応計画を立てます。 | | |
| 3．対策の実装 | 必要な設定変更やアップデートの適用、ポリシーや手順の策定、従業員への教育やトレーニング等の対策を実装します。 | | |
| 4．評価・改善 | 実装した対策の評価を行い、継続的な改善を促進します。 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Lv2. ベースラインアプローチ | | 網羅性 | 即時性 |
| ベースラインアプローチは、セキュリティ対策の基準やガイドラインを定義することにより、組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指します。ただし、追加のセキュリティ対策やリスクに対する適切な対応策を検討し、網羅的なアプローチを推進することが必要となります。   * セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保 * 網羅的なアプローチの出発点 | | △ | △ |
| 1．ベースラインの定義 | セキュリティの基準となるベースラインを定義します。活用できる文書/ツール、内部のセキュリティ目標等に基づいて定義します。 | | |
| 2．現状評価 | セキュリティポリシーやガイドラインの遵守度に基づき、既存のセキュリティ対策の評価を行います。改善点を特定し対応計画を立てます。 | | |
| 3．ベースラインの適用 | セキュリティポリシーの策定・改訂、ガイドラインの作成、セキュリティ対策の実装等により、ベースラインを適用します。 | | |
| 4．教育 | 定期的な教育活動を通じて、従業員にセキュリティポリシーやガイドラインの重要性を啓発し、遵守を促進します。 | | |
| 5．評価・改善 | 実装した対策の評価を行い、継続的な改善を促進します。 | | |

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

**凡例）「〇:あり / △：部分的にあり / ×:なし」**

|  |  |  |  |
| --- | --- | --- | --- |
| Lv3. 網羅的アプローチ | | 網羅性 | 即時性 |
| 網羅的アプローチは、可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなります。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではありません。  ・可能な限り多くの脅威や攻撃手法に対して対策を講じる  ・予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持 | | 〇 | × |
| 1．リスクアセスメント | 情報資産を特定し、脅威や脆弱性の評価を実施します。また、リスクの特定と評価を行い、重要度や優先順位を設定します。 | | |
| 2．対応計画 | リスク評価の結果を基に、セキュリティ対策を設計します。 | | |
| 3．対策の実装 | 組織的な対策（ポリシー、手順整備、教育等）、技術的な対策（アクセス制御、暗号化等）を実装します。 | | |
| 4．教育 | 定期的な教育活動を通じて、従業員にセキュリティポリシーやガイドラインの重要性を啓発し、遵守を促進します。 | | |
| 5．評価・改善 | 実装した対策の評価を行い、継続的な改善を促進します。また、内部監査や定期的な監査を実施し、情報セキュリティ管理システム適合性および妥当性を確認します。 | | |

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| 情報セキュリティ白書2023 | https://www.ipa.go.jp/publish/wp-security/2023.html |
| 情報セキュリティ10大脅威 2024 | https://www.ipa.go.jp/security/10threats/10threats2024.html |
| サイバー攻撃対応事例 | <https://security-portal.nisc.go.jp/dx/provinatack.html> |
| リスク分析シート | https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx |
| セキュリティ関連費用の可視化 | <https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/visualization-costs.html> |
| 中小企業の情報セキュリティ対策ガイドライン第3.1版 | <https://www.ipa.go.jp/security/guide/sme/about.html> |
| ISMS適合性評価制度 | <https://isms.jp/isms.html> |
| セキュリティ関連NIST文書について | <https://www.ipa.go.jp/security/reports/oversea/nist/about.html> |
| サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） | <https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html> |
| セキュリティ関連知識の保管庫（ナレッジベース2024） | <https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/> |

コラム

|  |
| --- |
| “情報セキュリティ”と“サイバーセキュリティ”の違いについて |
| 本テキストでは、“情報セキュリティ”と“サイバーセキュリティ”という言葉が随所に出てきます。そこで、両者の違いを説明します。  情報セキュリティは、情報全般の保護を意味します。情報の機密性（Confidentiality） 、完全性（Integrity） 、可用性（Availability） を確保するための対策が目的となります（情報セキュリティの3要素「CIA」）。これには、物理的な文書やデータの保管方法、アクセス制御、暗号化などが含まれます。情報セキュリティは、デジタルに加えて、紙の文書などの非デジタル情報にも関連しています。また、3要素に加えて、真正性（Authenticity）、責任追跡性（説明責任）（Accountability） 、否認防止性（Non-Repudation） 、信頼性（Reliability） を合わせて情報セキュリティの7要素と呼ぶこともあります。  一方、サイバーセキュリティは、主にインターネットやコンピュータネットワークに関連するリスクに対処することを目的とします。サイバーセキュリティは、クラッキング、マルウェア、DDoS攻撃などの脅威から情報システムやネットワークを保護するための技術、ポリシー、手順を包括的に扱います。サイバーセキュリティは、コンピュータシステムやネットワーク上の脆弱性に対処するためのテクニカルなアプローチに重点を置いています。  要約しますと、情報セキュリティは広範な情報の保護を対象とし、物理的な文書やデジタルデータを含む一般的なセキュリティの概念を指します。一方、サイバーセキュリティは、インターネットやネットワーク上のリスクに対処するためのテクニカルなアプローチを特に重視しています。 |

## デジタル社会の方向性と実現に向けた国の方針

|  |
| --- |
| 章の目的 |
| 第3章では、政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶことを目的とします。 |
| 主な達成目標 |
| * 国の基本方針にデジタルがどのように影響を与えており、それによりどのような社会を目指しているかを理解すること * デジタル社会におけるセキュリティ対策の重要性を理解すること |

### 国の基本方針および実施計画の要約

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

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

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

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

|  |
| --- |
| 5つのAction |
| ①物価上昇を上回る賃上げの定着  ②構造的価格転嫁の実現  ③成長分野への戦略的な投資  ④スタートアップネットワークの形成  ⑤新技術の徹底した社会実装 |
| 5つのVision |
| ①社会課題解決をエンジンとした生産性向上と成長機会の拡大  ②誰もが活躍できるWell-beingが高い社会の実現  ③経済・財政・社会保障の持続可能性の確保  ④地域ごとの特性・成長資源を活かした持続可能な地域社会の形成  ⑤海外の成長市場との連結性向上とエネルギー構造転換 |

IT戦略に関係する施策例

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

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

（出典）内閣府「経済財政運営と改革の基本方針 2024」をもとに作成

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

### 政府機関が目指す社会の方向性とサイバーセキュリティ課題

#### デジタル社会の実現に向けた重点計画

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

日本が目指すデジタル社会について、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」と定義し、以下の6つの姿を挙げています。[[3]](#footnote-4)

|  |
| --- |
| デジタル社会で目指す6つの姿 |
| 1.デジタル化による成長戦略  国・地方公共団体や民間との連携の在り方を含めたアーキテクチャの設計やクラウドサービスの徹底活用、デジタル原則を含む規制改革の徹底、調達改革の推進、データ戦略の推進、データ連携やDXの推進、AIの適切かつ効果的な活用などにより、我が国全体のデジタル競争力が底上げされ、成長していく持続可能な社会を目指す。 |
| 2.医療・教育・防災・こどもなどの準公共分野のデジタル化  必要なデータの連携などを通じて、国民一人ひとりのニーズやライフスタイルに合ったサービスが提供される豊かな社会、継続的に力強く成長する社会を目指す。 |
| 3.デジタル化による地域の活性化  地方の共通基盤を国が支援することなどにより、地域からデジタル改革、デジタル実装を推進、デジタル田園都市国家構想の実現、地域で魅力ある多様な就業機会の創出などを図り、地域の課題が解決され、各地域で培われてきた地域の魅力が向上する社会を目指す。 |
| 4.誰一人取り残されないデジタル社会  地理的な制約、年齢、性別、障害や疾病の有無、国籍、経済的な状況などにかかわらず、誰もが（デジタルに不慣れな方にも・デジタルを利用する方にも）日常的にデジタル化の恩恵を享受でき、さまざまな課題を解決し、豊かさを真に実感できる「誰一人取り残されない」デジタル社会を目指す。 |
| 5.デジタル人材の育成・確保  全国民が当事者であるとの認識に立ち、ライフステージに応じた必要なICTスキルを継続的に学ぶことで、デジタル人材の底上げと専門性の向上を図り、デジタル人材が育成・確保される社会を目指す。 |
| 6.DFFT（Data Free Flow with Trust）：「信頼性のある自由なデータ流通」の推進を始めとする国際戦略  国際連携を図ることで、データがもたらす価値を最大限引き出し、国境を越えた自由なデータ流通が可能な社会を目指す。 |

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

##### デジタル社会の実現に向けた戦略・施策

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

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

##### サイバーセキュリティなどの安全・安心の確保

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

|  |
| --- |
| 1.サイバーセキュリティの確保 |
| * 令和5年度に、政府情報システムにおけるクラウドサービスの利用拡大などを見据え、政府統一基準を改定。 * デジタル庁はNISCと連携し、デジタル庁整備・運用システムなどの情報システム整備方針の実装を推進。 * 安全保障などの機微な情報などに係る政府情報システムの取扱いを参照した利用促進。 |
| 2.個人情報などの適正な取扱いの確保 |
| * 改正後の個人情報保護法を踏まえ、個人情報などの適正な取扱いの確保、個人情報保護委員会の体制強化。 |
| 3.情報通信技術を用いた犯罪の防止 |
| * 不正アクセスの防止などに向けた官民連携。 * 国際連携、サイバー事案の警察への通報促進などの取組を実施。 |
| 4.高度情報通信ネットワークの災害対策 |
| * ネットワークの冗長性の確保・電気通信事故の検証､災害発生時における移動電源車などの派遣などを推進。 |

##### 各分野における基本的な施策

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

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

##### 産業のデジタル化

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

|  |
| --- |
| 1.デジタルによる新たな産業の創出・育成 |
| クラウドサービス産業の育成 / ITスタートアップなどの育成 |
| 2.事業者向け行政サービスの質の向上に向けた取組 |
| * 電子署名、電子委任状、商業登記電子証明書の普及 * 法人共通認証基盤（GビズID）の普及 * 事業者に対するオンライン行政サービスの充実 * レベルに応じた認証の推進 * eKYC（electronic Know Your Customer）などを用いた民間取引などにおける本人確認手法の普及促進 |
| 3.中小企業のデジタル化の支援 |
| * 中小企業の事業環境デジタル化サポート * 中小企業のサイバーセキュリティ対策の支援 |
| 4.産業全体のデジタルトランスフォーメーション |
| * 市場評価を通じたDXの推進、産業におけるサイバーセキュリティの強化、データの利活用や規制改革などを通じた産業のDX |

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

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

##### 事業者向け行政サービスの質の向上に向けた取組

|  |
| --- |
| 電子署名、電子委任状、商業登記電子証明書の普及 |
| 電子署名、電子委任状、商業登記電子証明書について、事業者による活用の機会が増加し、多様化していることから、普及を更に強力に推進する。 |
| 法人共通認証基盤（GビズID）の普及 |
| 法人が様々なサービスにログインできる認証サービスを実現する「GビズID」について、2023年度中にマイナンバーカードを利用した審査の効率化、連携行政サービスの拡充などを進める。 |
| 事業者に対するオンライン行政サービスの充実 |
| ア：e-Gov の利用促進  安定運用を確保しつつ、クラウドサービス利用による柔軟なリソース活用に向けて、ガバメントクラウドへの移行の整備を2023年度中に行うことを目指す。  イ：J グランツの利便性向上と利用補助金の拡大  申請簡素化や事務局の審査プロセス迅速化の観点から、2024年度（令和６年度）を目途に、システムアーキテクチャ及びUIの刷新を行い、申請時の事業者・事務局双方の負担軽減を図る。  ウ：中小企業支援のDX推進  事業者の申請などデータを一元化し官民で利活用するためのデータ基盤（ミラサポコネクト）を通じて、自社の経営特性に合った多様な支援がリコメンドされる環境を実現する。  最適な支援策や支援者・民間サービスなどについて情報交換できるコミュニティサイトの構築を目指す。 |
| レベルに応じた認証の推進 |
| ア：民間事業者への周知・相談支援の強化  マイナンバーカードの普及などに伴い、利用のインセンティブが大きく高まる民間事業者への周知・相談支援を強化する。  イ：利用要件・利用手続などの改善  民間事業者の視点に立ち、利用要件・利用手続などの継続的な改善を実施する。 |
| eKYCなどを用いた民間取引などにおける本人確認手法の普及促進 |
| デジタル空間での安全・安心な民間の取引などにおいて必要となる本人確認について、公的個人認証サービス（JPKI）の利用を促進する。その上で、安全性や信頼性などに配慮しつつ、具体的な課題と方向性を整理し、簡便な手法の一つであるeKYCなどを用いた本人確認手法の普及を進める。 |

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

##### 中小企業のデジタル化の支援

|  |
| --- |
| 中小企業の事業環境デジタル化サポート |
| * デジタル化支援ポータルサイト「みらデジ」の設置 * IT専門家との相談を受けられる体制の整備 * IT導入補助金 * 取引全体のデジタル化 * 会計・経理全体のデジタル化 * クラウドサービス利用やハードウェア調達の支援 * 業務効率化やDXに向けたITツール導入の支援 |
| 中小企業のサイバーセキュリティ対策の支援 |
| * 「サイバーセキュリティお助け隊サービス」の普及促進 * 相談体制の強化 * 情報集約・共有促進機能の強化 |

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

#### Society5.0

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

Society5.0では、IoT（Internet of Things）ですべての人とモノがつながり、さまざまな知識や情報を共有することによって、これまでにない新たな価値を生み出すとともに、社会が抱える課題を解決し、困難を克服できます。また、人工知能（AI）、ロボット、自動走行車などの利用によって、少子高齢化、地方の過疎化、貧富の格差などの課題も解決できるでしょう。こうした社会の変革（イノベーション）が進むことによって、希望の持てる社会、世代を超えて互いに尊重し合う社会、一人一人が快適で活躍できる社会が生まれることが期待されます。

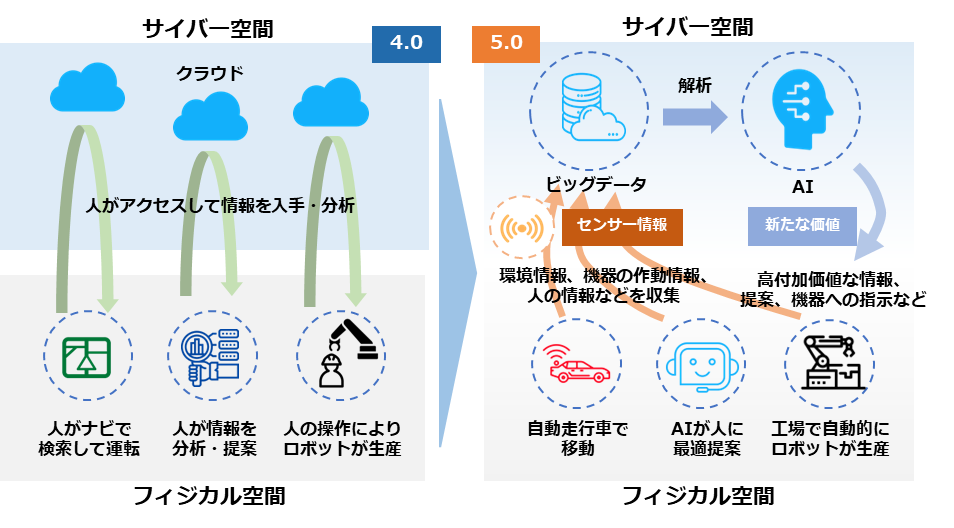
これまでの情報社会（Society4.0）では、人がサイバー空間にあるクラウドサービスにアクセスすることで、情報やデータを入手し、分析を行ってきました。Society5.0では、フィジカル空間のセンサーから膨大な情報がサイバー空間に集積されます。サイバー空間では、この集積されたデータ（ビッグデータ）を人工知能（AI）が解析し、その結果をフィジカル空間の人間にさまざまな形で、フィードバックしていきます。今までの情報社会では、人間が情報を解析することで、価値が生まれましたが、Society5.0では、AIが解析した膨大なビッグデータの結果がロボットなどを通して、人間にフィードバックされることで、これまでに実現しなかった新たな価値が産業や社会にもたらされます。[[4]](#footnote-5)

図3. Society4.0とSociety5.0の比較

（出典）内閣府.”Society5.0”.https://www8.cao.go.jp/cstp/society5\_0

##### 社会の変化に対するセキュリティ上の脅威

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

Society 5.0では、多様な人々がサービスの効果を享受できる包摂的な社会を目指していますが、そのためにはサービスの利用可能性や継続性を確保する必要があります。しかし、サイバー攻撃によってサービスが利用できなくなったり、中断されたりすると、包摂的な社会の実現に支障をきたす可能性があります。また、IoTデバイスやセンサーが収集したデータをサイバー空間で改ざんし、偽情報を拡散するといったフィジカル空間とサイバー空間の情報転送への脅威も考えられます。さらに、IoTやAIなどの技術を活用することで、大量のデータが生成されますが、そのデータは個人情報や企業情報などの重要な情報を含む場合が多く、その漏えいや改ざんによってプライバシーや知的財産権などが侵害される危険性が高まります。

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

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

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

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

#### DXの推進

DXの推進における中小企業の優位性について説明します。DXとは、デジタル技術やツールを導入すること自体ではなく、データやデジタル技術を使って、顧客目線で新たな価値を創出していくことです。中小企業の中には、DXを推進し、売上高を5倍、利益を50倍に増加させた企業が存在します。中小企業ならではの優位性を理解し、積極的にDXに取り組むことで、大きく成長できる可能性があります。以下では、DXを推進する際に、中小企業の優位な点を説明します。そして、優位性を利用してビジネスモデルや企業文化などの変革に取り組んでいる企業の事例を紹介します。

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

##### 事例（企業文化の改革）：精密機械部品加工

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

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

##### データ活用の流れ

顧客視点で新たな価値を創造するためには、製品やサービス、業務の変革が必要です。また、デジタル技術（IoT、ビッグデータ、ロボット、AIなど）を用いてデータを活用していくことが大切です。ここでは、デジタル技術を用いてデータを活用し、製品やサービス、業務を変革していく流れを具体的な事例と合わせて説明します。

以下は、データを活用し、業務を改革していくための手順となります。

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

##### 事例（業務改革）：某メーカー

図4. データ活用による業務改革の流れ  
（出典）IPA”製造分野のDX事例集”.

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

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

##### DX with Cybersecurityの概要

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

DXの推進によって、自社の製品やサービスの価値を向上させることができます。しかし、デジタル技術の活用によって増大するセキュリティ上のリスクに対応しなければ、企業の存続を脅かすインシデントが発生するかもしれません。そのため、セキュリティ対策はやむを得ない費用ととらえるのではなく、企業価値や競争力の向上に不可欠なものとしてとらえることが大切です。

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

## サイバーセキュリティ戦略および関連法令

|  |
| --- |
| 章の目的 |
| 第4章は、NISCによるサイバーセキュリティ戦略を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法とGDPRについて説明します。 |
| 主な達成目標 |
| * 日本におけるサイバーセキュリティに関する方針や施策について理解すること * サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること * 個人情報関連の法令を理解すること |

### NISC：サイバーセキュリティ戦略

#### サイバーセキュリティ戦略

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

##### サイバーセキュリティ戦略の課題と方向性

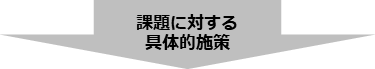
図5.サイバーセキュリティ戦略の課題と方向性の概要  
（出典）NISC「 サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

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

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

##### 経済社会の活力の向上及び持続的発展

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

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

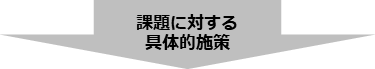
|  |
| --- |
| 課題 |
| * DXの推進が必要とされている中、サイバーセキュリティに対する意識や、サイバー空間を構成する技術基盤やデータなどに対する信頼が醸成されなければ、積極的な参加・コミットメントを得られず、変革を伴わない表層的なデジタル化に留まる恐れがある * 業務、製品・サービスなどのデジタル化が進む中、サイバーセキュリティの確保は企業価値に直結する重要なものとなっており、製品の企画・設計の段階からセキュリティを考慮する「セキュリティ・バイ・デザイン」が重要視されるなど、デジタル投資とセキュリティ対策を同時に進める必要がある |

|  |
| --- |
| 主な具体的施策 |
| 経営層の意識改革  デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化やインセンティブ付けを行い、さらなる取組を促進  地域・中小企業におけるDX with Cybersecurityの推進  中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業のセキュリティ対策強化の推進  新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり  Society5.0に対応したフレームワークなども踏まえ、各種取組を推進   * サプライチェーン：産業分野別及び産業横断的なガイドラインなどの策定や活用の促進 * データ流通：送信元のなりすましやデータ改ざんを防止する仕組みの整備 * セキュリティ製品・サービス：第三者検証サービスの普及による信頼性確保の取り組み * 先端技術：情報収集・蓄積・分析・提供などの共通基盤構築   誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着  情報教育推進の中、「デジタル活用支援」と連携して各種取組を推進 |

##### 国民が安全で安心して暮らせるデジタル社会の実現

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

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

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

|  |
| --- |
| 課題 |
| * サイバー空間の公共空間化、相互連関・連鎖の深化、サイバー攻撃の組織化・洗練化 |

|  |
| --- |
| 主な具体的施策 |
| 国民・社会を守るためのサイバーセキュリティ環境の提供   1. 安全・安心なサイバー空間の利用環境の構築 2. 新たなサイバーセキュリティの担い手との協調（クラウドサービスへの対応） 3. サイバー犯罪への対策 4. 包括的なサイバー防御の展開 5. サイバー空間の信頼性確保に向けた取組   デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保  経済社会基盤を支える各主体における取組  政府機関など：   * 監査・CSIRT訓練・GSOCによる監視などを通じたセキュリティ水準の向上 * クラウドサービスの利用拡大を見据えた政府統一基準群の改定 * 運用やクラウド監視に対応したGSOC機能の強化   重要インフラ：   * 「重要インフラの情報セキュリティ対策に係る第4次行動計画」の改定 * 環境変化に対応した防護の強化や経営層のリーダーシップを推進   大学・教育研究機関など：   * 先端情報を保有する大学などへの対策強化支援など * （リスクマネジメント・事案対応に関する研修・訓練や、サプライチェーンリスク対策）   多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化 |

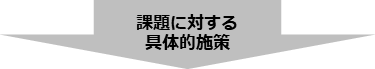
（出典）NISC「 サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

##### 国際社会の平和・安定及び我が国の安全保障への寄与

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

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

|  |
| --- |
| 課題 |
| * 我が国を取り巻く安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取などを企図したサイバー攻撃を行っているとみられている * 一方、同盟国・同志国においても、サイバー脅威に対応するため、サイバー軍や対処能力の強化が進められており、サイバー事案やサイバー空間に関する国際ルールなどをめぐる対立などに対して同盟国・同志国などが連携して対抗している * 加えて、安全保障の裾野が経済・技術分野にも一層拡大している中で、サイバー空間に関する技術基盤やデータをめぐる争いに対しても、同盟国・同志国が連携して対抗し、「自由、公正かつ安全なサイバー空間」を確保するため、我が国の基本的な理念に沿った国際ルールを形成していく必要がある |

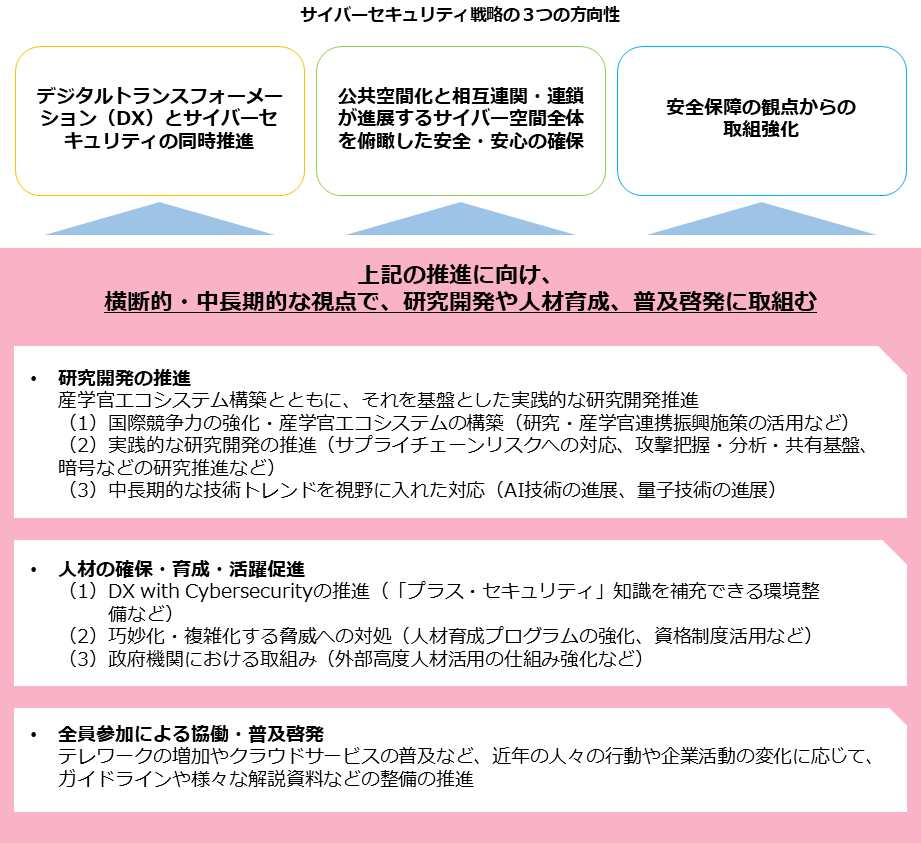


|  |
| --- |
| 主な具体的施策 |
| ⾃由・公正かつ安全なサイバー空間の確保   * サイバー空間における法の支配の推進（我が国の安全保障に資するルール形成） * サイバー空間におけるルール形成（信頼性のある自由なデータ流通や5Gセキュリティなど）   我が国の防御⼒・抑⽌⼒・状況把握⼒の強化   * サイバー攻撃に対する防御力の向上（防衛省・自衛隊におけるサイバー防衛能力の抜本的強化、先端技術・防衛産業などのセキュリティ確保のための官民連携・情報共有など） * サイバー攻撃に対する抑止力の向上（サイバー空間の利用を妨げる能力の活用、外交的手段・刑事訴追などを含めた対応の活用、日米同盟の維持・強化） * サイバー空間の状況把握力の強化（サイバー攻撃のさらなる実態解明の推進）   国際協⼒・連携   * 知見の共有・政策調整（国際連携の重層的な枠組みの強化） * サイバー事案などに係る国際連携の強化（国際サイバー演習の主導などによる国際的なプレゼンスの向上） * 能力構築支援（産学官連携や外交･安全保障を含めたASEANを含むインド太平洋地域における取組強化） |

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

##### 横断的施策

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



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

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

#### サイバーセキュリティ2024

NISCは、国のサイバーセキュリティ対策について、令和5年度年次報告・令和6年度年次計画を整理した「サイバーセキュリティ2024」を公表しています。記載に当たっては、サイバーセキュリティ基本法が定める３つの政策目的と、サイバーセキュリティ戦略の３つの施策推進の方向性に従って整理されています。

|  |
| --- |
| サイバーセキュリティ基本法が定める３つの政策目的 |
| * 経済社会の活力の向上及び持続的発展 * 国民が安全で安心して暮らせる社会の実現 * 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること |

|  |
| --- |
| サイバーセキュリティ戦略の３つの施策推進の方向性 |
| * デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進 * 公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保 * 安全保障の観点からの取組強化 |

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

|  |
| --- |
| 中小企業のサイバーセキュリティ対策促進 |
| 【背景及び課題】   * サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。他方で中小企業においては、リスクを自分事として認識していない、あるいは、何をしてよいか分からない状況が生まれている。 * 予算や人材が不足している中小企業が、それぞれの規模や業種、事業上の事情等に照らして自らに最も効果的なセキュリティ対策の水準を把握し、それを実践できる環境を整備するとともに、中小企業が使いやすいセキュリティサービスを普及・促進していくことが必要である。   【取組の概要】  ①手法   * サイバーセキュリティお助け隊サービスについて、2023年度に創設した新たなサービス類型を含め、中小企業等への普及・展開を図る。 * 企業規模やIT資産の内容等に応じて、ガイドラインとも紐付けながら、費用対効果のある方法等を提示する。 * 中小企業等とセキュリティ人材とのマッチングを促す場を構築し、セキュリティ人材のシェアリング促進等、中小企業における人材探索コストの低減を図る。   ②取組によって期待される成果・効果   * お助け隊サービスにつき、中規模以上の中小企業等も含めた普及啓発を促進する。 * 費用対効果のあるセキュリティ対策の方法等の提示を図ることで産業界のサプライチェーン全体のセキュリティ対策水準の向上を図る。 * 中小企業における人材探索コストの低減を図ることで企業のサイバーセキュリティ対策を行う側の人材を拡充させる。   【サイバーセキュリティ戦略本部有識者本部員の主な受け止め】   * サプライチェーンは中小企業が支えるところも多く、セキュリティ確保は重要である。 * 中小企業は犯罪者の格好のターゲットになっている。日本産業界のセキュリティ防御の「要」は中小企業にある。 * 政府主導で中小企業のセキュリティ対策支援を積極的に推進すべきである。特に人材と情報共有、補助金支援を中心とした活動に注力すべきである。 * レジリエンス確保は中小企業にとって死活的問題になっている。現場の声やニーズに対応して適切な対処方法の提供と普及、それを担う人材の育成等を行う上で「お助け隊サービス」の役割は重要である。 * セキュリティ人材のマッチング、シェアリング等の人材確保支援策にも期待する。 |

(出典) NISC「サイバーセキュリティ2024」をもとに作成

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

### 企業経営に重要なDX推進とセキュリティ確保の両立

#### 企業経営のためのサイバーセキュリティの考え方

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

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

|  |
| --- |
| 2つの基本的認識 |
| <①挑戦>  サイバーセキュリティは、利益を生み出し、ビジネスモデルを革新するものであり、新しい製品やサービスを創造するための戦略の一環として考えていく必要がある。 |
| <②責任>  すべてがつながる社会において、サイバーセキュリティに取り組むことは社会的な要求・要請であり、自社のみならず社会全体の発展にも寄与することになる。 |

|  |
| --- |
| 3つの留意事項 |
| <①情報発信による社会的評価の向上>   * セキュリティ対策を、仕方なくやるものではなく、企業価値を高め、品質向上に有効な経営基盤の1つとして位置づけることが必要。 * サイバーセキュリティに関する取組や方針を情報発信することによって、関係者の理解を深め、社会的評価を高めることができる。 |
| <②リスクの一項目としてのサイバーセキュリティ>   * 提供する機能やサービスを全うする（機能保証）という観点から、リスクの一項目としてのサイバーセキュリティの視点も踏まえ、リスクを分析し、総合的に判断。 * 経営層のリーダーシップが必要。 |
| <③サプライチェーン全体でのサイバーセキュリティの確保>   * サプライチェーンでつながるどこかの企業のセキュリティ対策が不十分だと、そこから自社の重要情報が流出してしまうなどの問題が起きる可能性がある。そのため、サプライチェーン全体で一定レベルのサイバーセキュリティの確保が必要。 * 一企業のみでのセキュリティ対策には限界があるため、関係者間での情報共有活動への参加などが必要。 |

図6.ITの活用またはサイバーセキュリティ対策の取組み状況に応じた分類と対策

（出典）NISC「企業経営のためのサイバーセキュリティの考え方の策定について」をもとに作成

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

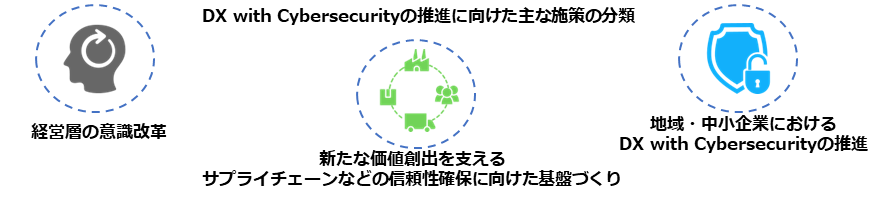
|  |  |  |
| --- | --- | --- |
| レベル | 分類 | 概要・対策 |
| 理想的に | 1 | ITの利活用を事業戦略上に位置づけ、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業 |
| もっと積極的に | 2 | IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略としての組み込みはできていない企業 |
| 対策：ITを積極的に活用してビジネスの展開を目指すことが重要であり、攻めのIT投資に関する取組を行うことです。 |
| 無駄な投資 | 3 | 過剰なセキュリティ意識により、ITの利活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

図7 ITの活用またはサイバーセキュリティ対策の取組状況に応じた分類と対策

（出典）東京都「 ITおよびサイバーセキュリティに関する組織の視点6分類」をもとに作成

#### DX with Cybersecurity

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



|  |
| --- |
| 経営層の意識改革 |
| 【課題】経営層が主体性を持ってDXとセキュリティ対策に取り組むためには、セキュリティの専門家とのコミュニケーションが重要  【施策】経営者がITやセキュリティに関する専門知識を持っていない場合でも、セキュリティの専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備 |
| 地域・中小企業におけるDX with Cybersecurityの推進 |
| 【課題】中小企業は、セキュリティ対策に予算を割くことの必要性を理解する  【施策】中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進 |
| 新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり |
| サプライチェーンの信頼性確保  【課題】サイバー攻撃の起点となりうる箇所の拡大に伴う、リスク管理が重要  【施策】産業分野別、または産業横断的なガイドラインの策定や活用促進を通じて、産業界におけるセキュリティ対策の具体化・実装を促進  データ流通の信頼性確保  【課題】データの真正性や流通基盤の信頼性を確保することが重要  【施策】データマネジメントの定義、送信元のなりすましやデータの改ざんなどを防止する仕組みを整備  セキュリティ製品・サービスの信頼性確保  【課題】市場において提供されるセキュリティ製品・サービスが信頼できるか、客観的な評価が必要  【施策】一定の基準を満たすセキュリティサービスの審査・登録する仕組みを整備  先端技術・イノベーションの社会的実装  【課題】デジタル化の進展に伴い、効率的なセキュリティ対策が必要  【施策】研究機関の知識や技術を民間企業が活用しやすい環境の整備や、企業が社外の知識や技術を取り入れ、組織の改革（セキュリティ対策の強化など）を進められる環境の整備を推進 |

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

### 関連法令

#### 個人情報保護法

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

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

|  |
| --- |
| 個人情報保護法とは |
| インターネットの普及や情報技術の進歩などを背景として、個人の権利や利益を守ることを目的として「個人情報保護法」（正式名称：個人情報の保護に関する法律）が平成17年4月に全面施行されました。施行後も、デジタル技術の進展やグローバル化などの経済・社会情勢の変化や、世の中の個人情報に対する意識の高まりなどに対応するため、今までに3度の改正が行われています。  個人情報保護法では、どのような情報が個人情報になるのか、個人の権利や利益を守るためには個人情報をどのように取扱わなければいけないのかなどが規定されています。 |

##### 個人情報の定義

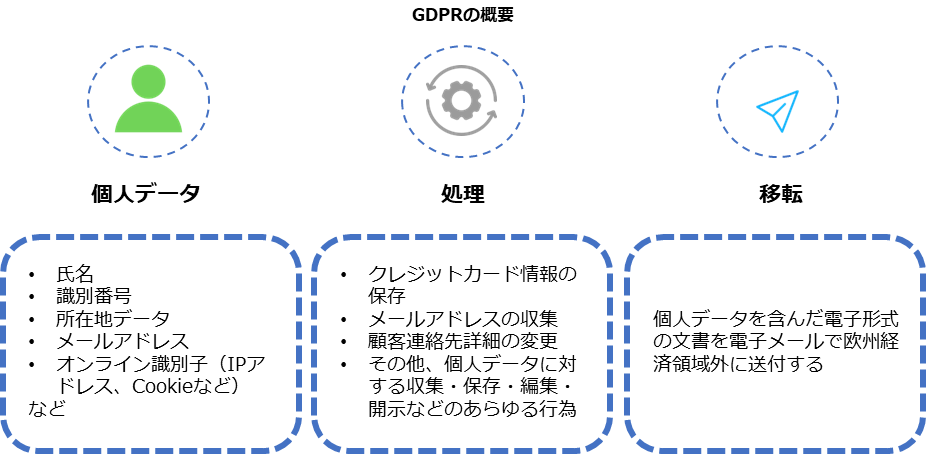
|  |
| --- |
| 個人情報保護法において「個人情報」とは、生存する個人に関する情報で、氏名、生年月日、住所、顔写真などにより特定の個人を識別できる情報のことを指します。これには他の情報と容易に照合でき、それにより特定の個人を識別できるものも含まれます。 |

##### 個人情報を取扱う時の基本ルール

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

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

#### GDPR

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

|  |
| --- |
| GDPR（一般データ保護規則）とは |
| EUで策定された新しい個人情報保護の枠組みであり、個人データ保護やその取扱いについて詳細に定められた欧州経済領域内の各国に適用される法令のことです。欧州経済領域内で取得した「個人データ」を「処理」し、欧州経済領域外の第三国に「移転」するために満たすべき要件が定められています。GDPRの特徴として、インターネット上で収集できる個人データのほとんどが保護対象となっています。 |

|  |
| --- |
| GDPRと日本企業の関係 |
| GDPRはEU内で適用される法令ですが、支店など物理的な拠点をEU内に持っていなくても、インターネットを利用して日本からEU域内に商品販売やサービス提供、情報収集を行っている企業にもGDPRが適用されます。また、ターゲティング広告を配置した自社サイトに対して、EU域内からアクセスがあった際もGDPRの適用対象となる可能性があります。GDPRに違反した場合はかなり重い制裁金が課されるため、適切な対策が求められます。 |
| GDPRに向けた対策例 |
| GDPRでは、Cookieが「個人情報」とみなされるため、WebサイトでCookieを利用する際は、Webサイト閲覧者からCookie取得の同意を得る仕組みを構築することが必要です。Cookieについての本人の同意を取得するには、企業とユーザーとの間で個人データの利用における同意の実施・管理を行うツール（CMP）を導入することが推奨されています。 |

#### その他関連法令

そのほか、サイバーセキュリティに関連する法令の例を紹介します。

|  |
| --- |
| 不正競争防止法 |
| 事業者間の不正競争の防止を目的の1つとしており、ブランドの表示の盗用、商品の形態模倣などとともに、営業秘密や限定データの不正取得・使用などを規制している。 |
| 著作権法 |
| プログラムを含む著作物の保護と複製権をはじめとする著作権などについて規定している。 |
| 電気通信事業法 |
| サイバー空間における活動の基盤となるインターネットサービスなどの電気通信事業に関する諸規定や、通信の秘密などを規定している。 |
| 電子証明および認証業務に関する法律 |
| デジタルデータの流通と情報処理の円滑な利用のため、電子署名や認証業務の法的な取扱いを定めている。 |
| 情報処理の促進に関する法律 |
| 情報処理の高度利用促進を目的とした法律で、情報処理安全確保支援士や情報処理技術者試験に関する規定、サイバーセキュリティに関する調査や講習を行っているIPAの業務範囲などに関する規定を含んでいる。 |
| 国立研究開発法人情報通信研究機構法 |
| NICTの業務においてサイバーセキュリティに関する研究開発など、国や自治体の従業員を対象とする演習の「CYDER」の実施を定めるとともに、時限的な業務としてIoT機器の調査を行う「NOTICE」に関する規定を措置している。 |
| 刑法 |
| 不正指令電磁的記録に関する罪（いわゆるウイルス罪）をはじめとするサイバー犯罪を処罰する規定を含む刑罰が規定されている。 |
| 不正アクセス行為の禁止などに関する法律 |
| 不正ログインといった不正アクセス行為や、いわゆるフィッシング行為を処罰する旨が規定されている。 |

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

|  |  |
| --- | --- |
| 施策の理解のため参考となる文献（参考文献） | |
| サイバーセキュリティ関係法令Q&AハンドブックVer2.0 | https://security-portal.nisc.go.jp/guidance/pdf/law\_handbook/law\_handbook\_2.pdf |

編集後記

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

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

# 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策【レベル共通】

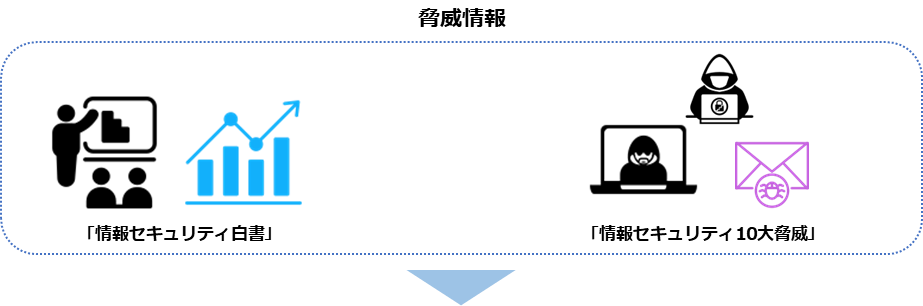
## 事例を知る：重大なインシデント発生から課題解決まで

|  |
| --- |
| 章の目的 |
| 第5章では、近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対するセキュリティ対策や、実際に被害に遭ってしまった際の対応方法について学ぶことを目的とします。 |
| 主な達成目標 |
| * 近年のサイバー攻撃の傾向や手法を理解すること * 実際の被害事例を通して脅威に対するセキュリティ対策や予防方法を理解すること * 脅威の検知から、復旧・再発防止処置までの流れを理解すること |

### 情報セキュリティの概況

#### 情報セキュリティの脅威を学ぶ

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

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

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

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

#### IPA：情報セキュリティ白書から見る脅威

|  |
| --- |
| 情報セキュリティ白書は、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックのほか、その年ならではの象徴的なトピックを取り上げています。本書情報セキュリティ白書は、情報セキュリティに関する国内外の政策や脅威の動向、インシデントの発生状況、被害実態など定番トピックのほか、その年ならではの象徴的なトピックを取り上げています。本書を通して、情報セキュリティ分野の全体を把握できます。情報セキュリティ白書は、IPAによって2平成20年から毎年発行されています。  令和5年7月に刊行された「情報セキュリティ白書2023」は、令和4年度のサイバー攻撃による実際の被害やセキュリティ対策など、情報を守るための最新情報をまとめています。 |



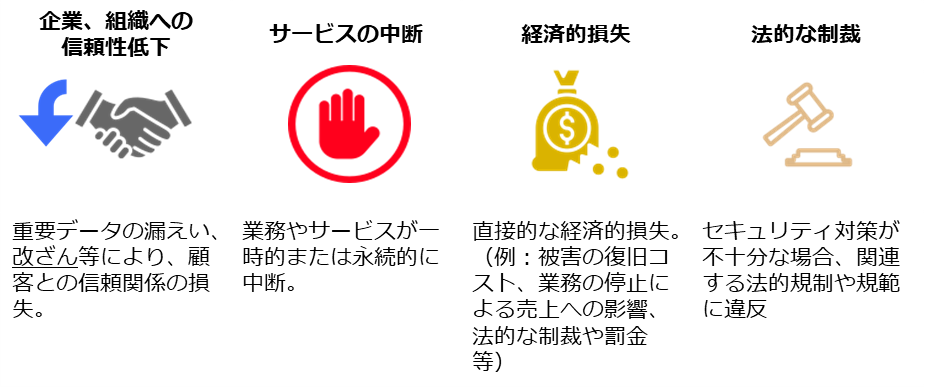
図8. 情報セキュリティ白書2023

|  |
| --- |
| 情報セキュリティ白書2023の記載内容 |
| * 序章 令和4年度の情報セキュリティの概況 * 情報セキュリティインシデント・脆弱性の現状と対策 * 情報セキュリティを支える基盤の動向 * 個別テーマ * 付録 資料・ツール |

|  |  |  |
| --- | --- | --- |
| サイバー攻撃の内容を知りたい |  | 活用例 |
| * 標的型攻撃やランサムウェア攻撃などの事例、手口やセキュリティ対策を知ることができる * 社内の注意喚起に利用する |
|  |  |  |
| セキュリティ人材の育成方法を知りたい |  | 活用例 |
| * ICSCoE中核人材育成プログラムやセキュリティ・キャンプの活動を知る * 人材育成のための国家試験や国家資格について知る |

|  |  |  |
| --- | --- | --- |
| セキュリティ対策の進め方が知りたい |  | 活用例 |
| * SECURITY ACTIONやサイバーセキュリティお助け隊サービス制度などの活動を知り、自社で取り組む |

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

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

情報セキュリティ白書では、1年間のインシデント状況を紹介しています。それによると情報セキュリティの脅威は年々増加しており、2021年の情報セキュリティインシデント報道件数は769件となり、前年比で43.2%増加しました（図9）。[[5]](#footnote-6)

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

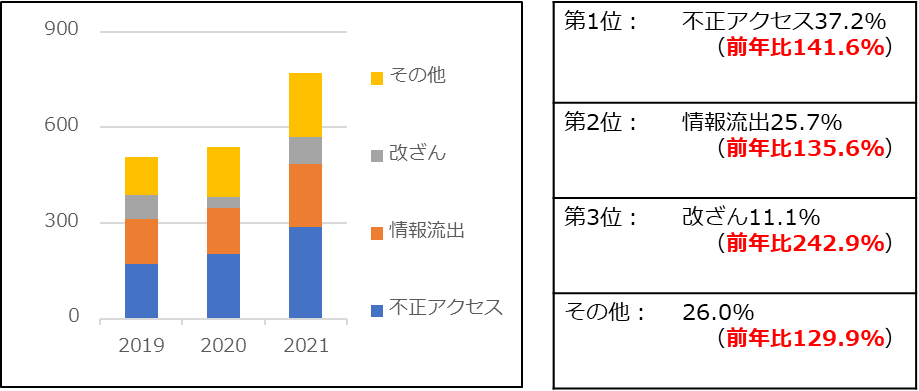


図9. 情報セキュリティインシデント報道件数

(出典) MBSD社による集計情報を基に作成

#### IPA：情報セキュリティ10大脅威

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

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

|  |  |
| --- | --- |
| 情報セキュリティ10大脅威の活用法：組織の検討例 | |
| 1．「守るべきもの」の明確化 | 自社の守るべきものを明確にします。 |
| * 業務プロセス：取引先との受注業務 * 情報データ：取引先情報や受注先情報 * システム、サービス、機器：社内ITシステムとその構成機器 * その他：取引先との信頼関係など |

|  |  |
| --- | --- |
| 2．自社にとっての脅威の抽出 | 情報セキュリティ10大脅威を参考にして自社の守るべきものに対する脅威を抽出します。  脅威が生じた場合の被害額を算出し、会社の経営方針を考慮し、優先順位をつけます。 |
| * ランサムウェア感染による社内ITシステムの使用不能・脅迫（ランサムウェアによる被害） * 取引先である大企業へのサイバー攻撃の踏み台として悪用（サプライチェーンの弱点を悪用した攻撃） * 従業員による顧客情報や取引情報の不正持ち出し（内部不正による情報漏えい） |

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

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

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

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| 情報セキュリティ 10 大脅威の活用法2024 | https://www.ipa.go.jp/security/10threats/nq6ept000000g23i-att/katsuyouhou\_2024.pdf |

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

(出典) IPA「情報セキュリティ10大脅威 2024」をもとに作成

|  |  |
| --- | --- |
| 1位 | ランサムウェアによる被害  攻撃者は、PCやサーバをランサムウェアに感染させ、さまざまな脅迫を行い、金銭を要求します。組織の規模や業種に関係なく攻撃が行われているという点に注意が必要です。  事例：VPN（Virtual Private Network）経由で侵入、ランサムウェアを横展開（某地域購買生協）  11台のサーバ内の情報がランサムウェアに暗号化されました。暗号化されたデータには約49万人の個人情報が含まれていました。攻撃者は、ネットワーク機器の脆弱性を悪用してVPN経由で侵入し、ランサムウェアを横展開しました。 |
| 2位 | サプライチェーンの弱点を悪用した攻撃  直接攻撃が困難な組織に対し、標的組織よりもセキュリティが脆弱な取引先や委託先、国内外の子会社などを攻撃し、踏み台にして標的組織に侵入する攻撃です。  事例：委託先のシステムを介して不正アクセス、顧客情報漏えい（保険会社）  複数の保険会社で、業務委託先から顧客の個人情報が流出しました。流出の規模は、多いところで約130万人分におよびました。原因は、業務委託先の適切なセキュリティ対策がされていないサーバへの不正アクセスでした。 |
| 3位 | 内部不正による情報漏えい等の被害  従業員や元従業員などの組織関係者による機密情報の持ち出しや社内情報の削除などの不正行為が発生しています。  事例：前職場が保有する名刺情報を転職先に提供（人材派遣会社）  従業員は同業他社に転職する直前に、転職元の名刺情報管理システムにログインするためのIDとパスワードを転職先の従業員に共有していました。不正に取得された名刺情報は転職先の営業活動に使用されました。 |
| 4位 | 標的型攻撃による機密情報の窃取  標的型攻撃は、特定の組織（企業、官公庁、民間団体など）を狙う攻撃のことです。攻撃者は社会や働き方の変化に合わせて攻撃手口を変えるなど、組織の状況に応じた巧みな攻撃手法を用いることに注意が必要です。  事例：不正アクセス、機微情報含まず（国立研究開発法人）  ネットワーク機器の脆弱性を悪用し、一般業務用の管理サーバに不正アクセスされました。 |
| 5位 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）  ゼロデイ攻撃は、ソフトウェアの開発ベンダーなどが脆弱性対策情報を公開する前に、脆弱性を悪用する攻撃のことです。事業やサービスが停止するなど、多くのシステムやユーザーに被害が及ぶことがあります。  事例：ファイル圧縮ソフトウェア  ファイル圧縮ソフトウェアの一部の脆弱性がゼロデイ攻撃に悪用されていることがわかりました。スクリプトを実行させることが可能になる脆弱性でした。 |
| 6位 | 不注意による情報漏えい等の被害  システムの設定ミスによる非公開情報の公開や、個人情報を含んだ記憶媒体の紛失など、不注意による機密情報の漏えいが発生しています。  事例：個人情報をコピーしたUSBメモリを紛失（市民病院）  再委託先担当者が132人分の個人情報を含むデータをUSBメモリにコピーして持ち出し、紛失しました。 |
| 7位 | 脆弱性対策情報の公開に伴う悪用増加  脆弱性対策の公開情報を悪用して、脆弱性対策の実施が遅れている製品・システムのセキュリティホールを狙うという攻撃が発生しています。近年、情報の公開から攻撃が本格化するまでの時間が短くなっています。  事例：脆弱性を修正した機器へ継続的な攻撃（メールセキュリティ製品）  本脆弱性の修正対応後も、特定の組織では、攻撃者による新たなバックドアの設置や、ネットワーク上での横展開など、継続的な攻撃活動が確認されています。 |
| 8位 | ビジネスメール詐欺による金銭被害  悪意のある第三者が標的組織やその取引先の従業員などになりすましてメールを送信し、あらかじめ用意した偽の銀行口座に金銭を振り込ませるという詐欺です。  事例：信頼できる取引先を騙るメール詐欺（医療製品企業）  支払口座の変更依頼が書かれた、取引先の名を騙るメールに従い、虚偽の銀行口座に総額2億円振り込みをしたことを公表しました。 |
| 9位 | テレワーク等のニューノーマルな働き方を狙った攻撃  テレワークに活用されるVPNサービスなどを狙った攻撃が、引き続き行われています。  事例：在宅勤務用のリモートアクセス経路より侵入の疑い（製造業）  攻撃者がリモートアクセス経路から侵入し、ランサムウェアでデータセンターや国内拠点の一部サーバに保存されていたデータを暗号化しました。結果、約6万件の個人情報が外部に流出しました。 |
| 10位 | 犯罪のビジネス化（アンダーグラウンドサービス）  アンダーグラウンド市場では、アカウントのIDやパスワード、クレジットカード情報、ウイルスなどが売買されています。話題のサービスのアカウント情報も売買されており、多要素認証を取り入れるなどのセキュリティ対策が重要です。  事例：国内製造業の情報がダークウェブに流出（製造業）  ダークウェブ上にアカウント情報や機密文書がアップロードされていることが判明しました。 |

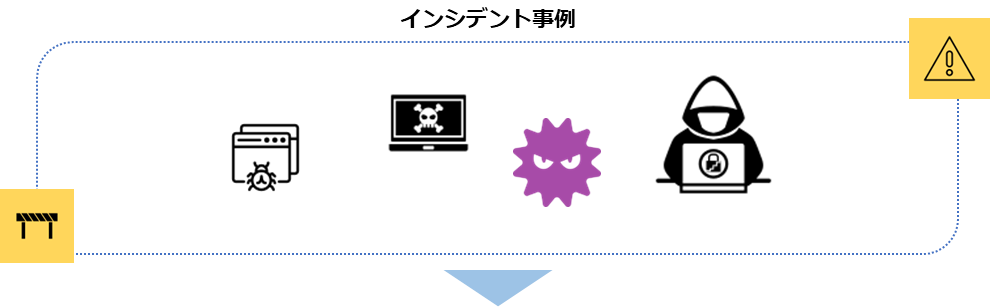
(出典) IPA「情報セキュリティ10大脅威 2024」をもとに作成

### 重大インシデント事例から学ぶ課題解決

#### インシデント事例から学ぶ

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

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

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

|  |
| --- |
| 目的 |
| 実際に発生した攻撃事例やセキュリティインシデント事例をケーススタディーとして学ぶこと。具体的な知識をもとに実践的なアプローチ手法を習得すること。 |
| 学べる内容 |
| * 攻撃手法や攻撃者の手口 * インシデントの影響と被害範囲 * 具体的なインシデント対応と復旧策 |
| 活用例 |
| * セキュリティリスク管理、対策の強化 * セキュリティポリシーの改善 * セキュリティインシデント対応の改善 * 脅威トレンドの把握、共有 * セキュリティ意識の向上 |

#### 最近の攻撃トレンド、および中小企業にも発生しうるサイバー被害事例

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

##### IoTデバイスによるサービス被害

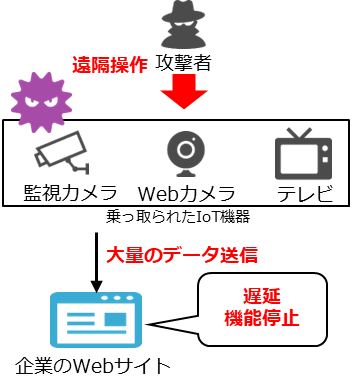
最近、IoTデバイスを標的にしたマルウェアが広まっています。このマルウェアに感染した大量のIoT機器は、攻撃者によって遠隔操作され、大規模なDDoS攻撃に利用されます。企業がDDoS攻撃を受けると、自社のWebサイトが遅延したり、機能停止したりすることがあります。そして、攻撃を停止することと引き換えに、攻撃者から金銭を要求されることもあります。このような攻撃に対抗するためには、Webアプリケーションへの攻撃を防ぐためのWAF（Webアプリケーションファイアウォール）や、ネットワーク上の攻撃を防御するためのIPS（Intrusion Prevention System）の導入が考えられます。

図10. DDoS攻撃の概要図

##### テレワークによるサイバー被害事例

新型コロナウイルスの影響により、テレワークが急速に広まり定着しています。企業では、テレワークを実施するためにVPNを利用して社外から社内ネットワークに安全に接続する取組が増えています。しかし、VPNの脆弱性を悪用したサイバー攻撃が確認されています。具体的な事例として、某メーカーのインシデントが挙げられます。同社は、VPN機器において過去に判明した脆弱性に対処するためのアップデートを実施しました。しかし、アップデート前にパスワード情報が漏えいしており、当時から存在していたアカウントがパスワードの変更を行っていなかったため、不正アクセスが行われ、ランサムウェアの被害を受ける事例が発生しました。企業は、VPNのセキュリティ対策に十分な注意を払う必要があります。特に、パスワードの管理や定期的なアップデートの実施が重要です。

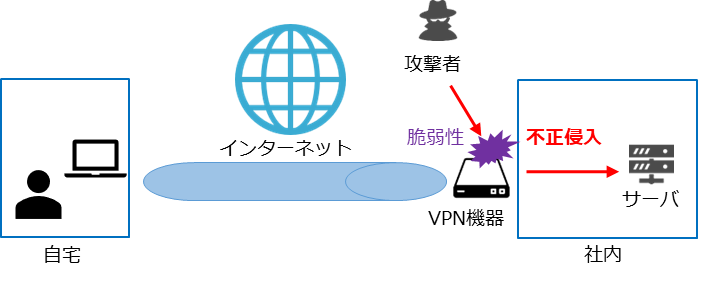


図11. VPN機器の脆弱性を利用した攻撃のイメージ

##### テレワークのセキュリティ対策

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

|  |  |  |
| --- | --- | --- |
| 分類 | 対策内容 | 想定脅威 |
| 資産・構成管理 | 許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク端末とその利用者を把握している。 | マルウェア感染・不正アクセス盗難・紛失 |
| 物理セキュリティ | テレワーク端末に対して覗き見防止フィルタをはり、離席時には[スクリーンロック](#_bookmark290)をかけるようルール化している。 | 情報の盗聴 |

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

#### 事案発生->課題の抽出->再発防止策の実施までの流れ

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



図12. インシデント対応の３ステップ

|  |  |
| --- | --- |
| ①検知  ・初動対応 | 検知と連絡受付：  インシデントの兆候や実際の発生に気づいた場合は、情報セキュリティ責任者に報告します。責任者は適切な対応が必要と判断した場合には、経営者に報告します。  対応体制の立ち上げ：経営者は事前に策定している対応方針に従い、役割分担を明確にするために責任者と担当者を指名します。これにより、インシデントに迅速かつ効果的に対応する体制を整えます。  初動対応：  被害の拡大を防ぐために、ネットワークの遮断やシステムの停止などの適切な措置を行います。ただし、システム上に記録が残されている場合は、対象機器の電源を切る際に注意し、記録を消去しないようにします。 |
| ②報告・公表 | 第一報：  インシデントが発生したことを、被害の拡大を防ぐために関係者全員に適切なタイミングと内容で通知します。通知が困難な場合は、Webサイトやメディアを通じて公表したり、関係する顧客や消費者に対してはお問い合わせ窓口を開設したりして対応します。  第二報以降・最終報：  インシデント復旧の進捗状況や再発防止策などの詳細情報を報告し、被害者に対する損害の補償を行います。個人情報漏えいの場合は、必要に応じて[個人情報保護委員会](#_bookmark289)や関連省庁に報告し、犯罪の可能性がある場合は警察に、ウイルス感染や不正アクセスの場合は情報処理推進機構（IPA）に報告します。 |
| ③復旧・再発防止 | 調査・対応：  インシデントの原因や影響範囲を詳しく調査し、適切な対応策を策定します。被害の拡大を止めるために適切な措置をとり、被害の影響を最小限に抑えるよう努めます。  証拠保全：  事実関係を裏づける証拠などを収集し、訴訟対応や事件解明、法的手続きに活用します。必要に応じて[フォレンジック](#_bookmark293)調査を実施し、証拠の確保と分析を行います。  復旧：  インシデントの修復が確認された後、復旧作業を実施します。システムやデータを正常な状態に戻し、ビジネスの継続性を確保します。復旧作業が完了したら、経営者に報告します。  再発防止策：  同様のインシデントが再発しないよう、再発防止策を立案・実施します。セキュリティの強化や従業員の教育・訓練の強化などを通じて、将来のインシデントを防止するための措置を講じます。 |

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

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| 中小企業のためのセキュリティインシデント対応の手引き | <https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf> |

#### インシデントから得た気づきと取組

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

##### サプライチェーンを介した標的型メール攻撃

|  |
| --- |
| 【事例の概要】  ある企業の工場部門は、取引先企業のメールアカウントが攻撃者に乗っ取られるという被害に遭いました。攻撃者は、取引先企業のフリをして工場部門の担当者に対して、マルウェアが添付されたメールを送信しました。その結果、2台の端末がマルウェアに感染してしまいました。このマルウェアは、通常の定義型ウイルス対策ソフトウェアでは検知することができませんでしたが、EDRを導入していたことで早期に検知し、感染の拡大を食い止めることができました。[[6]](#footnote-7) |
| 【問題点・課題】   * 攻撃者が取引先の正規アカウントを乗っ取っていたため、メール自体に不審な点を見つけることが困難でした。 * 取引先が乗っ取りを受けているため、自社単独では攻撃を完全に防ぐことは困難でした。 * 取引先へのセキュリティ支援やアセスメントの範囲と、それに伴う負担を自社でどの程度検討すべきかについて検討が必要でした。取引先のセキュリティに対する支援やアセスメントの範囲を検討し、自社が負担できる範囲でのセキュリティ対策を考える必要があります。 |
| 【対策・予防策】   * 取引先のセキュリティ対策状況を把握するためには、ヒアリングシートやアンケートなどの手法を使用することが重要です。これにより、取引先のセキュリティレベルや脆弱性を明確にすることができます。 * 工場のセキュリティを強化するためには、国内で最新の工場システムを構築しているベンダーに自社工場のアセスメントを依頼することが有効です。   EDRを導入してマルウェアのエンドポイントデバイス上での活動を監視し、異常な振る舞いを検知することができます。また既にEDRを導入している場合は、ゼロトラスト、SASEのフレームワークにある機能のSWGなどを体系的に実装することで、さらにセキュリティを強化することができます。 |

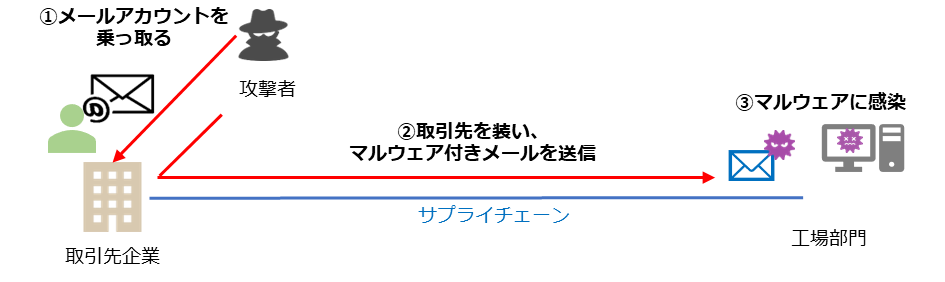
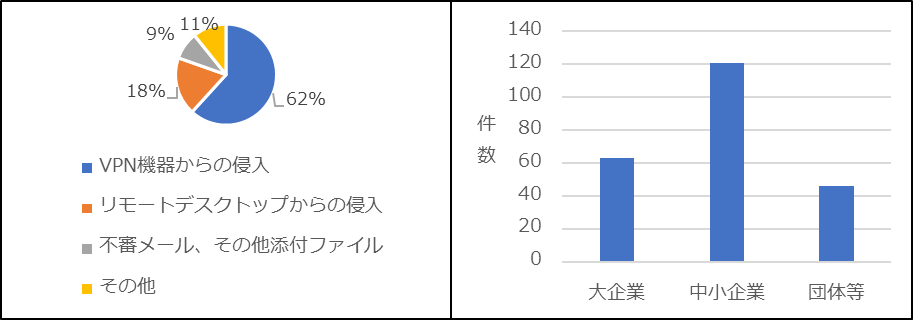


図13. 攻撃の概要図

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

#### ランサムウェア感染の実態

ランサムウェアは、PCやサーバのデータを暗号化し、その暗号化されたデータを復号することを条件に身代金（金銭）を要求する悪意のあるソフトウェアです。令和5年における企業や団体の被害件数は合計197件であり、被害企業の規模を見ると、大企業が71件、中小企業が102件、団体などが24件でした。ランサムウェアの感染経路については、VPN機器からの侵入が73件で全体の63%を占め、リモートデスクトップからの侵入が21件で18%となっています。これらの侵入は、テレワークなどで使用される機器の脆弱性や弱い認証情報を悪用して行われたものであり、全体の約82%に上る割合を占めました。[[7]](#footnote-8)



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

図15.（令和5年）ランサムウェアの被害件数

図14.（令和5年）ランサムウェアの感染経路

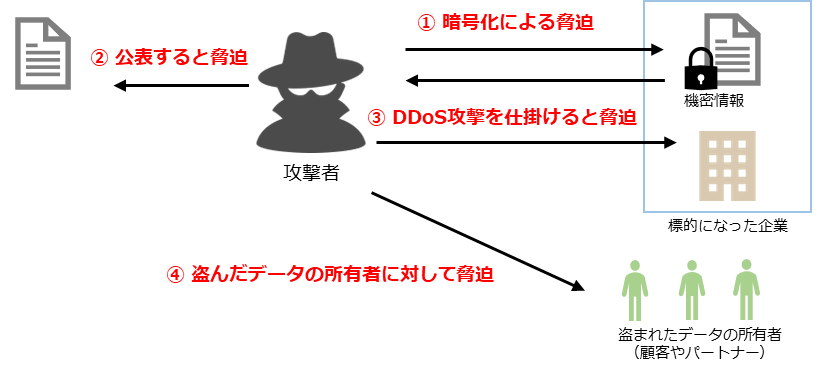
最近のランサムウェアは、以下のような特徴を持っています。図の①②のように、データの復旧を条件に金銭を要求する脅迫に加えて、暗号化前のデータを窃取し公開するという「二重脅迫」を行うものが存在します。さらに、追加の脅威として③DDoS攻撃などの追加攻撃を行うことで被害を拡大することもあります。また、さらに高度な手法として、④被害者の利害関係者に連絡し、情報を共有するなどの「四重脅迫」を行うケースも確認されています。

図16. ランサムウェアの二重、四重脅迫のイメージ図

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

##### 電子カルテシステムでランサム被害（某市民病院）

|  |
| --- |
| 事例の概要  外部のインターネットから電子カルテシステムのサーバと一部のクライアントパソコンがランサムウェアに感染しました。サーバの復旧を優先する一方、システムログの保全を行わず再起動したため、正確な原因究明ができなくなりました。 |
| 被害の原因  この事例の原因は、「ルール違反」を犯してインターネットに接続したことにより、外部からウイルスが侵入したことです。また、導入に携わる業者の管理や障害時対応の適切な運用体制が構築、運営されていなかったため、病院のガバナンスにも問題がありました。 |
| この事例から学べること   * マルウェア対策ソフトウェアの定期的な更新とスキャンは、侵入を防ぐために重要です。 * インターネットに安易に接続してはいけません。拠点間をインターネットで接続する時には安全なVPNを用いるようにしましょう。 * 侵入後のログ保全を行うためには、システムの導入に加えて、適切な運用体制を構築、運営することが重要です。 * 安易にインターネットに接続しないことは、ウイルスを侵入させないために重要です。 |

##### VPN機器に対するランサム攻撃（某容器販売業）

|  |
| --- |
| 事例の概要  サーバなどに対して第三者による不正アクセスを受け、ランサムウェアを用いたサイバー攻撃による被害が発生しました。この攻撃によって、暗号化されたデータには、従業員に加えて、取引先の個人情報が含まれていました。 |
| 被害の原因  この事例の被害の原因は、流出したネットワーク機器の認証情報を利用し、VPN経由で業務サーバを含む複数のサーバへ不正侵入されたことです。この結果、個人情報を含むデータが暗号化されてしまいました。 |
| この事例から学べること   * [多要素認証](#_bookmark292)やアクセス制御によって接続者を制限することが非常に重要です。 * バックアップの保護やEDRの導入などのセキュリティ対策を講じることが重要です。また、VPNより高セキュリティな接続方法である[SDP](#_bookmark287)の導入も検討すべきです。 |

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| コンピュータウイルス・不正アクセスの届出事例 | https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf |

### 実際の被害事例から見るケーススタディー

#### 最近のサイバー被害事例発生の傾向

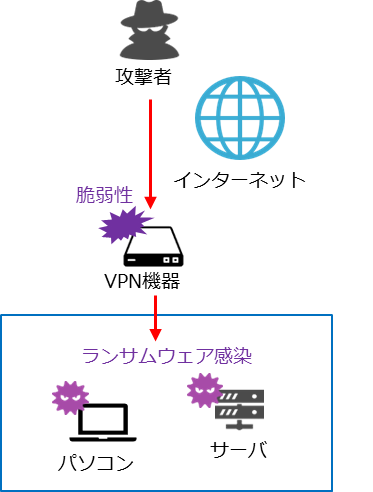
サプライチェーンを通じて、被害が起きた原因の分析内容および効果的なセキュリティ対策ベストプラクティスを紹介します。

##### サプライチェーンを通じた被害

|  |
| --- |
| 被害の概要  某メーカーの取引先企業がサイバー攻撃を受け、システムが使用不能になりました。この攻撃により、某メーカーは部品の調達が不可能になり、その結果、複数の工場が停止し、数万個以上の生産が見送られる事態に陥りました。この出来事は、サプライチェーン攻撃のリスクとその被害の大きさを再認識させる上で非常に重要な事例となりました。 |
| 被害の原因  ウイルスの侵入経路は、子会社が独自に特定外部事業との専用通信に利用していたリモート接続機器の脆弱性があり、そのことをきっかけとして不正アクセスを受けました。攻撃者はリモート接続機器から子会社内のネットワークに侵入後、さらに親会社のネットワークに侵入して、サーバやPCの一部を暗号化しました。 |
| セキュリティ対策・ベストプラクティス   * VPN装置は外部のネットワークからアクセス可能な位置に設置されることが多く、外部の攻撃者から攻撃されやすくなります。そのため、VPN装置のベンダーのWebサイトなどを確認し、未対策の脆弱性がないかを点検することが大切です。 * サイバー攻撃の被害は取引先企業に広がることがあります。セキュリティ対策は自社に加えて、サプライチェーンでつながっている会社、取引先企業を含めて考え、実施する必要があります。 |

図17. 攻撃の概要図

#### 事例：某港のランサムウェア被害

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

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

図18. 攻撃の概要図

|  |
| --- |
| 問題点   * VPN装置は導入当初からソフトウェアの更新が行われていなかった。 * 厚生労働省からの注意喚起はあったが、事業者側がリスク評価できず被害を想定できなかった。 * 庶務係がIT担当者を一人で兼任しており、セキュリティの知識・技術が不十分であった。 * 「VPN装置を使用すれば外部からのサイバー攻撃を受けない」という誤解があった。   ベンダーがシステムの動作優先で、セキュリティ対策を考慮していなかった。 |
| 教訓   * 取引をしているベンダーと情報交換、コミュニケーションをとる。 * 経営者・担当者のセキュリティレベル向上を図る。 * インシデントが発生した時の被害を想定する。 |

会社の規模、業種を問わず、ランサムウェアの被害に遭う可能性はあります。大事なことは、「自社が狙われている」という危機感を持つことです。ランサムウェアに限らず、他の事例も含めて、危機感を持ちセキュリティ対策を総合的に取り組むことが重要です。

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| コンピュータウイルス・不正アクセスの届出事例 | https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf |

#### 具体的な対応策

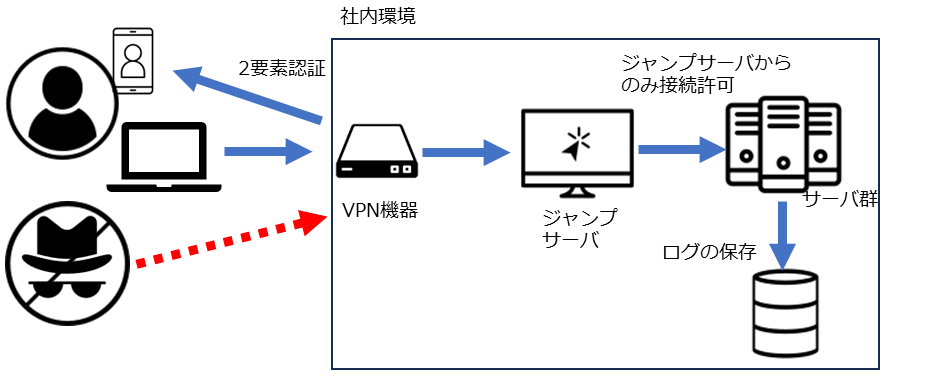
ランサムウェア被害のケースを見ると、VPN機器から不正侵入され、サーバの特権IDを使用してサーバのデスクトップ上から不正プログラムを実行されるケースが後を絶ちません。セキュリティ対策、運用については、まず、VPNで接続するためのインターネットとの接点を絞りこみ、接続してくる者の身元を確認し、本人であることを証明させる多要素認証の仕組みを講じることが必要となります。それ以外にも、特定のPCやサーバからしか重要なサーバのデスクトップに接続できないような仕組みや、ログの長期保管なども重要な要素となります。

図19. 対応策の概要図

実施するべきセキュリティ対策と運用

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

## 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

|  |
| --- |
| 章の目的 |
| 第6章では、これからの企業経営で必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資について学ぶことを目的とします。また、経営投資としてのセキュリティ対策の重要性を明確にすることを目的とします。 |
| 主な達成目標 |
| * 社会の動向を把握し、現実社会とサイバー空間のつながりを理解すること * IT投資としての「守りのIT投資」と「攻めのIT投資」を理解すること * 経営投資としてのセキュリティ対策の重要性を理解すること |

### これからの企業経営で必要な観点：社会の動向

#### 現実社会とサイバー空間のつながり

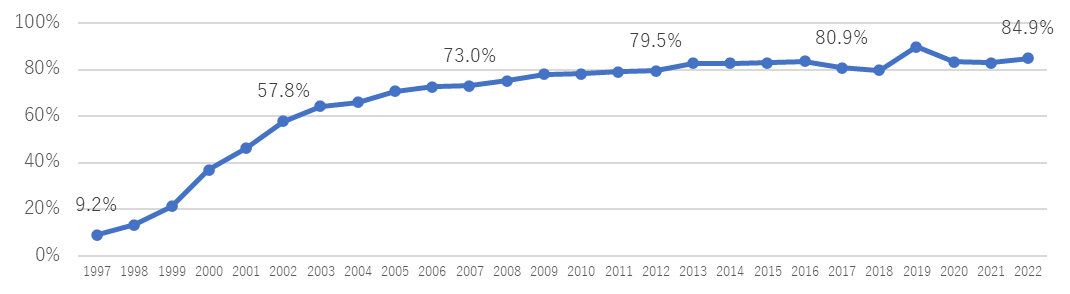
日々の生活や企業活動において、ITの活用は広範囲にわたって浸透しています。インターネット利用率（個人）は平成9年には9.2%でしたが、令和4年には84.9%まで上昇しました。急速なITの普及により、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革変化をもたらしています。

図20. インターネット利用率（個人）の推移

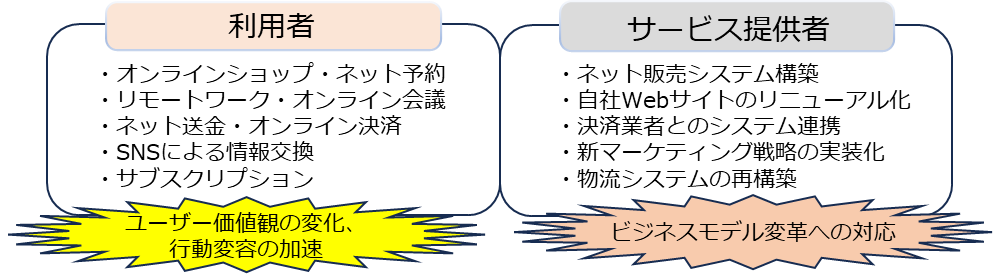
（出典） 総務省「通信利用動向調査」をもとに作成

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

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

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

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



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

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

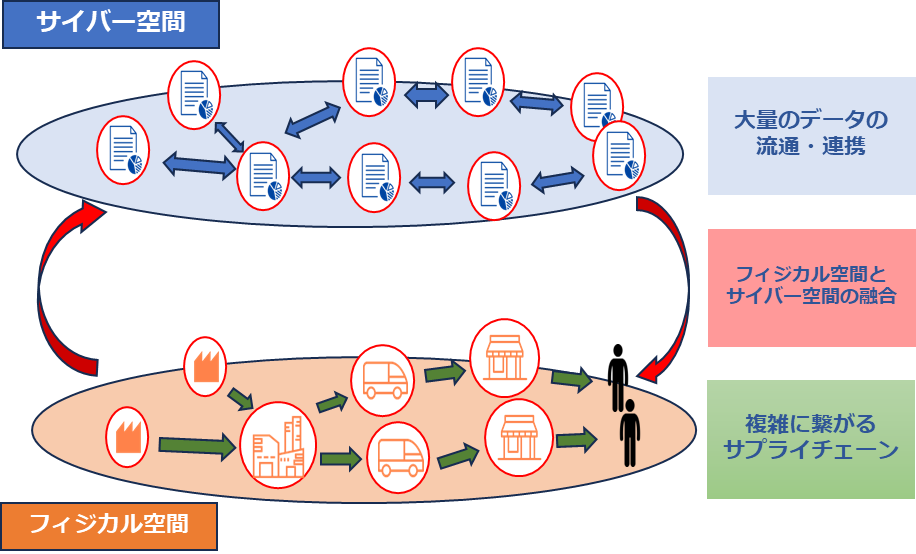
今後の社会では、サプライチェーンにおけるフィジカル空間とサイバー空間とのつながりが重要視されています。そして、Society5.0に合ったサプライチェーンに変化することで、従来のサプライチェーンもより柔軟で効率的なものになります。

図21. サイバー空間とフィジカル空間の関係図

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

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

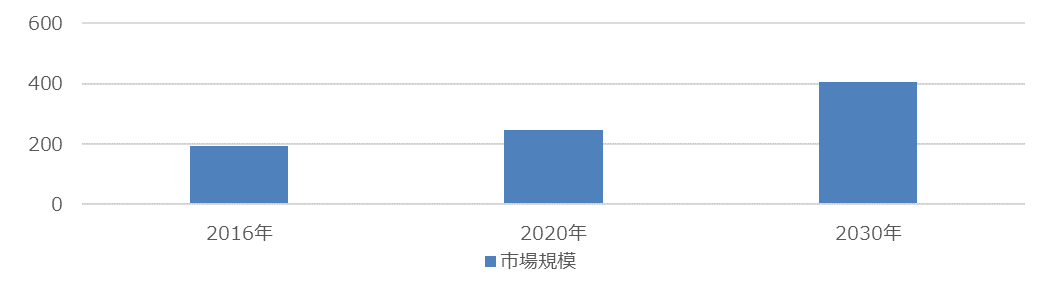


図22. CPS／IoTの世界市場の推移

（出典） JIETA「CPS／IoTの世界市場の調査結果」をもとに作成

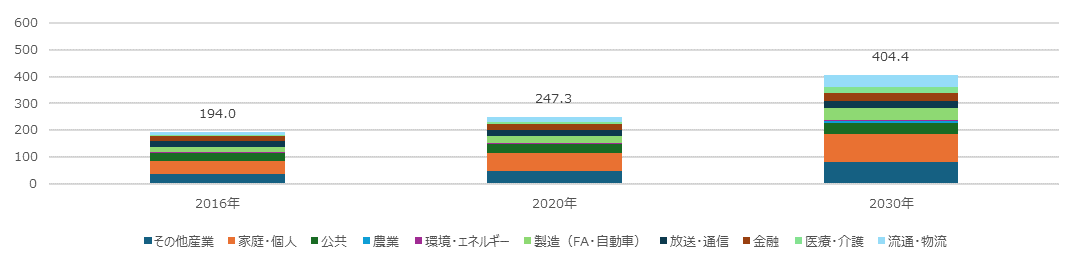
CPS/IoT市場を10の利活用分野別にみた調査結果によると、令和11年時点で最も大きい市場が家庭・個人で106.1兆円です。次いで流通・物流が44.9兆円、製造（FA・自動車）が44兆円、公共が39.3兆円、金融が29.9兆円、放送・通信が25兆円、医療・介護が22.3兆円、農業が7.8兆円、環境・エネルギーが5.4兆円、その他産業が79.8兆円となっています。CPS/流通・物流、製造（FA・自動車）の市場規模が高いことは、製品やサービスが供給される経路全体を指すサプライチェーンとCPSが関わると言えます。世界的にもCPS/IoTの需要額が増加することから、企業は生産性向上や課題の解決のため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

図23. CPS／IoTの利活用分野別需要額の推移

（出典） JIETA「CPS／IoT世界市場の利活用分野別需要額見通し」をもとに作成

#### IT活用における課題

我が国のデジタル化について、デジタルインフラ整備などの一部については世界的に見ても進んでいるものの、全体としては大幅に後れていると言えます。さまざまな理由が複雑に絡み合い、我が国のデジタル化の後れが生じていると考えられます。[[8]](#footnote-9)

ここでは日本社会がデジタル化で後れをとった理由についてみていきます。

##### 我が国がデジタル化で後れをとった6つの理由

|  |
| --- |
| 1. ICT投資の低迷 |
| 我が国におけるICT投資は、1997年をピークに減少傾向にあります。また、我が国におけるICT投資の8割が現行ビジネスの維持・運営に当てられているなど、従来型のシステム（レガシーシステム）が多く残っており、その頃の考え方やアーキテクチャから抜け出せていないと言われています。これらを背景として、我が国では、オープン化やクラウド化への対応、業務やデータの標準化が遅れ、業務効率化やデータ活用が進んでいない状況にあると考えられます。 |
| 2. 業務改革等を伴わないICT投資 |
| ICT投資が効果を発揮するためには、業務改革や企業組織の改編などを併せて行うことが重要とされていますが、外部委託に全面的に依存することで、業務改革などをしない形でのICT導入となり、十分な効果が発揮できなかったため、デジタル化に向けたさらなるICT投資が積極的に行われなかった可能性があります。 |
| 3. ICT人材の不足・偏在 |
| 我が国のICT人材は、量も質も十分ではないとユーザー企業に認識されています。また、その人材についても、外部ベンダーへの依存度が高く、ICT企業以外のユーザー企業に多く配置されており、ユーザー企業では、組織内でICT人材の育成・確保ができていません。 |
| 4. 過去の成功体験 |
| 我が国は、高度経済成長期を経て、世界有数の経済大国となりましたが、ICT関連製造業についても生産・輸出が1985年頃まで増加傾向にあり、「電子立国」とも称されていました。2000年代に入ってからは、ICT関連製造業の生産額が減少傾向に転じ、2000年代後半には輸出額も減少傾向にありますが、それ以前の成功体験により、抜本的な変革を行うよりも、個別最適による業務改善が中心となり、デジタル社会の到来に対応できていないと言われています。 |
| 5. デジタル化への不安感・抵抗感 |
| デジタル化が進んでいない理由として最も多く挙げられたことが「情報セキュリティやプライバシー漏えいへの不安があるから」（52.2%）でした。また、パーソナルデータの企業などによる不適切な利用、インターネット上に流布する偽情報への対応、慣れないデジタル操作などへの習熟など、さまざまな要因により、デジタル化に対する不安感・抵抗感が生じる場合があると考えられます。 |
| 6. デジタルリテラシーが十分ではない |
| デジタル化が進んでいない理由として2番目に多く挙げられたことが「利用する人のリテラシーが不足しているから」（44.2%）でした。このようにデジタルリテラシーが十分ではないと考えられることから、デジタル化推進に対して消極的になる場合があると考えられます。 |

（出典） 総務省「情報通信白書令和3年版」をもとに作成

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

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

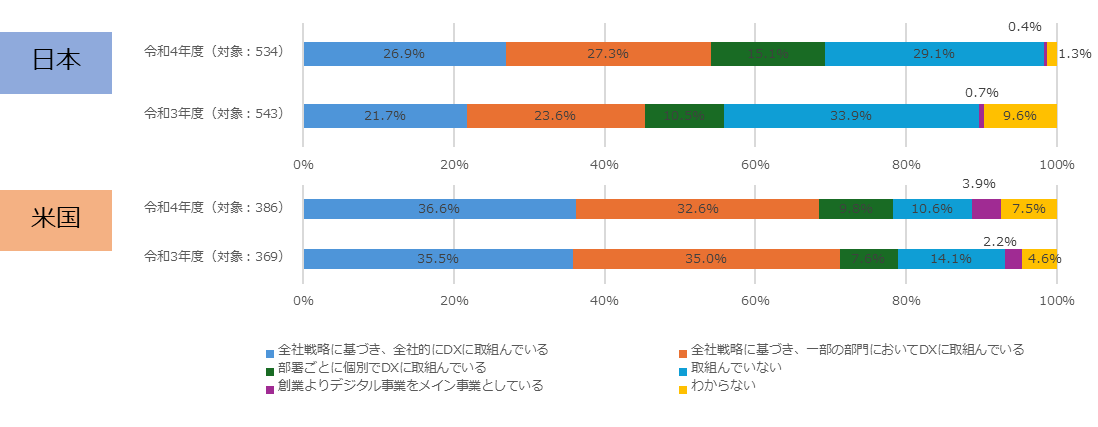


図24. DXの取組状況

（出典）IPA「DX白書2023」をもとに作成

|  |
| --- |
| 2. DXの取組の成果 |
| DXの取組において、日本で「成果が出ている」の企業の割合は令和3年度調査の49.5%から令和4年度調査は58.0%に増加しました。一方、米国は89.0%が「成果が出ている」となっており、日本でDXへ取り組む企業の割合は増加しているものの、成果の創出において日米差は依然として大きいです。 |

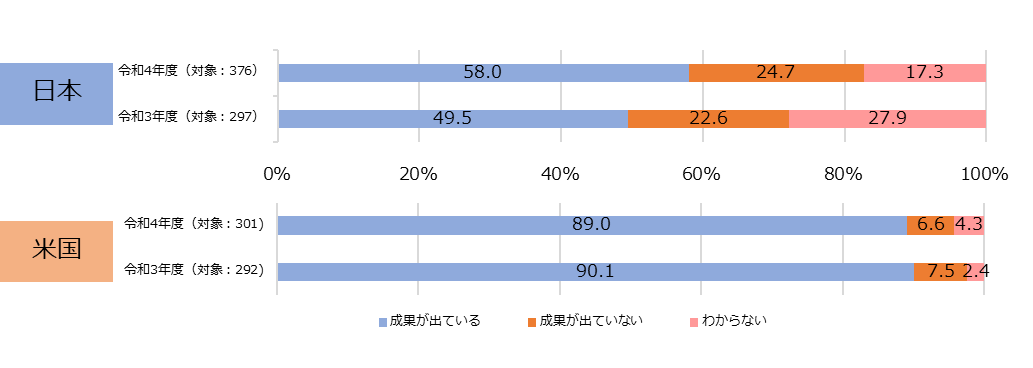


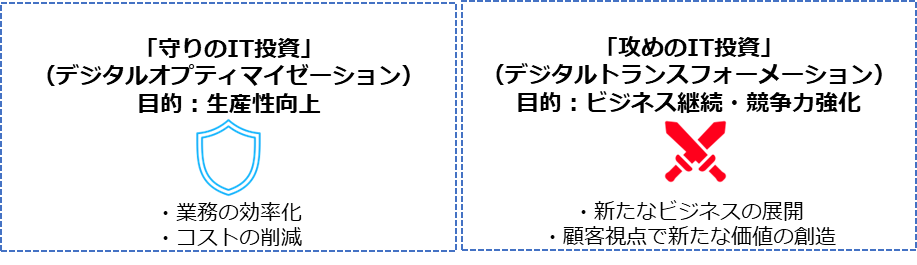
図25. DXの取組の成果

（出典）IPA「DX白書2023」をもとに作成

### 守りのIT投資と攻めのIT投資

#### 守りのIT投資、攻めのIT投資の概要

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

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

攻めのIT活用指針

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

|  |
| --- |
| STEP1 IT導入前の状況 |
| ITを導入していない  （例）口頭連絡、電話、帳簿での業務 |
| STEP2 置き換えステージ |
| 紙や口頭でのやり取りをITに置き換え  （例）社内メール、会計処理や給与計算にITを使用 |
| STEP3 効率化ステージ/ 守りのIT投資（デジタルオプティマイゼーション） |
| ITを活用して社内業務を効率化  （例）顧客・商品・サービス別の売上分析 |
| STEP4 競争力強化ステージ/ 攻めのIT投資（DX） |
| ITを自社の売上向上などの競争力強化に積極的に活用  （例）マーケティング・販路拡大・新商品開発・ビジネスモデル構築 |

図26. 攻めのIT活用指針の概要

（出典）経済産業省「攻めのIT活用指針」をもとに作成

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

##### 2025年の崖

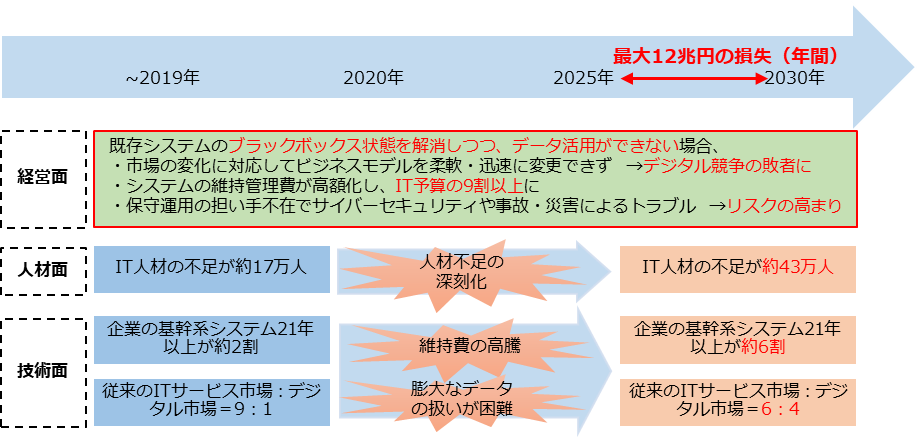
「2025年の崖」とは、経済産業省が平成30年に発表した「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」にて提示されているキーワードです。このレポートでは、令和7年は、基幹系システムのサポート終了に伴う維持費の増加や人材不足の深刻化などが集中する年であると予測されています。また、こうした既存のITシステムをめぐる問題を解消しない限りは、DXを本格的に展開することは困難であると指摘しています。さらに、レポートによれば、日本企業がDXを推進できなかった場合の経済的な損失は、年間最大で12兆円に上ると算出され

図27. 「2025年の崖」の概要図

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

ています。[[9]](#footnote-10)

「2025年の崖」に陥らないための対応策

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

#### ITを活用した生産性の向上（デジタルオプティマイゼーション）

##### 「守りのIT投資」：デジタルオプティマイゼーション

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

##### 必要な理由

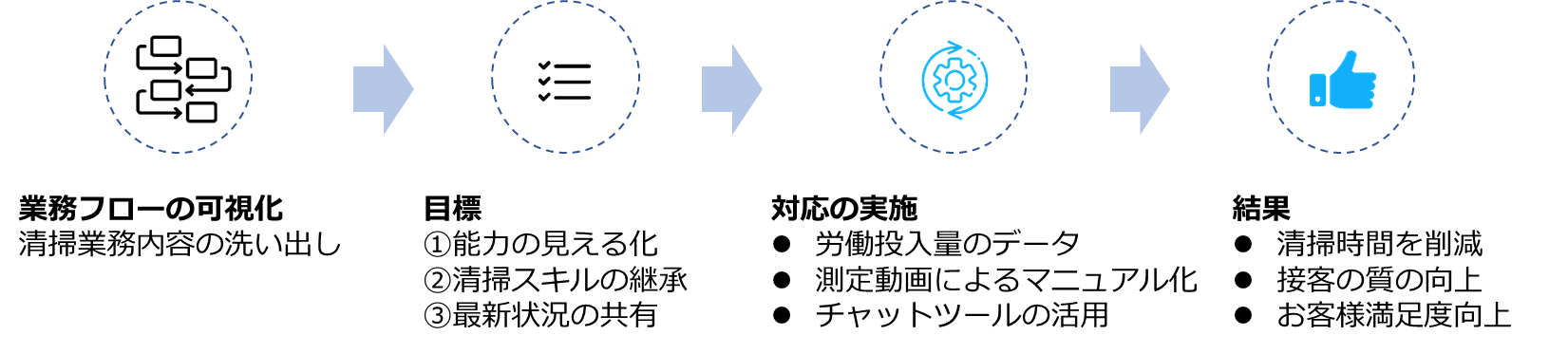
|  |
| --- |
| 業務効率化・コスト削減  デジタル技術の普及により、新たな競合他社が市場に参入し、従来のビジネスの常識が変化しています。この状況下で企業がビジネスを継続していくためには、「攻めのIT投資」によって、製品・サービスの品質向上や新規開発、ビジネスモデルの変革などを行い、企業の競争力を維持および強化することが必要です。 |
| デジタル活用するための環境整備  DXを実現するには、データの活用が不可欠です。これまでの業務では、表計算ソフトウェアや紙を使用していたため、データを有効に活用することが難しい状況でした。しかし、守りのIT投資を行うことで、データを収集・利用する環境を整えることが可能です。これにより、将来的にDXを実施する際の障壁を低減することができます。 |
| 「守りのIT投資」には、以下のようなものがあります。   * 定期的なシステム更新サイクル * ITによる業務効率化／コスト削減 * 法規制対応など |

##### 進め方

|  |
| --- |
| 手順1：業務内容・業務フローの可視化 |
| 現在の業務プロセスやフローを明確にし、可視化することで全体像を把握します。 |
| 手順2：削減・短縮可能な業務の洗い出し |
| 可視化された業務から、削減や短縮が可能な業務を特定します。 |
| 手順3：改善や対応の実施 |
| 洗い出された業務の中から、優先度や重要度に基づいて順位づけを行い、事前に計画した改善策や対応を実施します。 |
| 手順4：業務改革の実現 |
| 業務の効率化や品質向上を実現します。 |

##### 事例：某旅館（静岡県・宿泊業・飲食サービス業）

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



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

図28. 業務改革の流れ

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

#### ITを活用した新たなビジネスの展開（DX）

##### 「攻めのIT投資」：DX

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

##### 必要な理由

|  |
| --- |
| ビジネス環境の急激な変化に対応するため  デジタル技術の普及により、新たな競合他社が市場に参入し、従来のビジネスの常識が変化しています。この状況下で企業がビジネスを継続していくためには、「攻めのIT投資」によって、製品・サービスの品質向上や新規開発、ビジネスモデルの変革などを行い、企業の競争力を維持および強化することが必要です。 |
| 多様化する顧客のニーズに応えるため  デジタル時代において、顧客のニーズや期待は大きく変化しています。そのため、「攻めのIT投資」によってDXを推進させ、顧客視点で新たな価値を創出し、顧客満足度を高めていくことが必要です。 |
| 「攻めのIT投資」には、以下のようなものがあります。   * 新規事業の立ち上げ、事業発展 * 既存製品の品質向上・新製品やサービスの開発 * ビジネスモデルの変革など |

##### 進め方

|  |
| --- |
| 手順1：経営ビジョン・戦略の策定 |
| デジタル技術によって市場や顧客のニーズがどのように変化するのかを検討した上で、企業の存在意義や企業理念を再認識し、5～10年後の中長期的な視点で顧客にどのような価値を提供していきたいのか、ビジョンを明確にします。 |
| 手順2：変革の準備・課題の抽出 |
| 将来のビジョンと現状のギャップから、課題を抽出します。また、関係者に将来のビジョンを説明し、変革を受け入れてもらえるような意識改革を行い、全社的に取り組める体制を整えます。 |
| 手順3：デジタル技術・業務改革による課題の解決 |
| デジタル技術の活用や業務プロセスの見直し、企業文化の改革などにより、課題を解決していきます。 |
| 手順4：顧客に新たな価値を提供・他社のDXに貢献 |
| 新たな価値を創出し、顧客に提供します。さらに、サプライチェーン全体に対しても貢献していきます。 |

|  |  |
| --- | --- |
| 詳細理解のため参考となる文献（参考文献） | |
| 中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き | <https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/contents.html> |

##### 事例：某ワイン製造会社（北海道・酒類製造業）

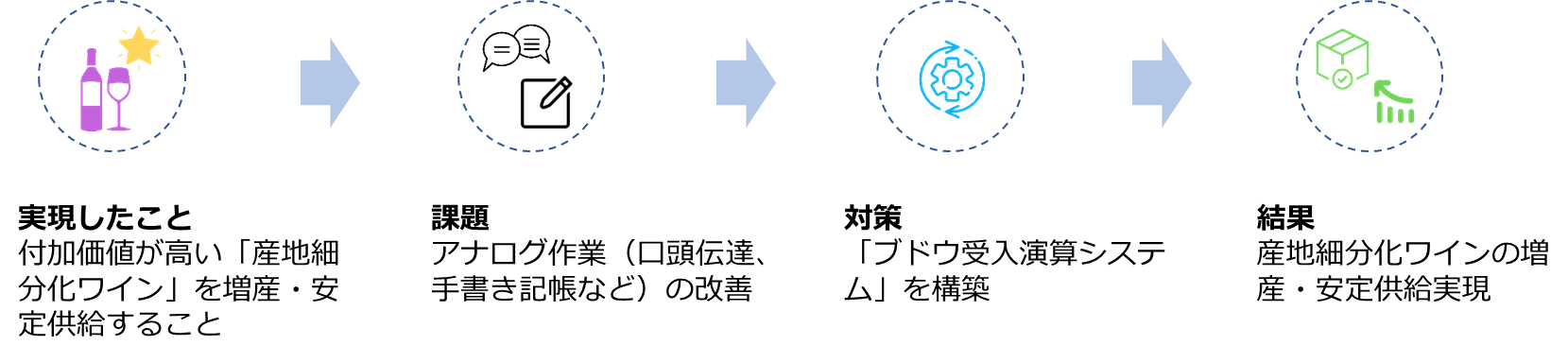
北海道でワイン製造を営む会社がDXの取り組むきっかけは、産地を細分化した高品質なワインを安定化してお客様に届け、農家にもしっかりと利益を還元したいという思いでした。従来ブドウの生産地などはアナログ作業で実施していましたが、業務をデジタル化することによってリアルタイムで管理でき、「産地細分化ワイン」を製造することが可能になりました。

図29. 業務改革の流れ

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

|  |
| --- |
| 手順1：実現したいことを明確にする |
| ワインの価値を決める要素として重要な「産地」を細分化して、高品質なワインを増産・安定供給することを目指します。 |
| 手順2：課題の明確化、関係者の意識改革を実施する |
| 細分化を妨げている要因は、ブドウの受け入れに関わる「口頭伝達」「手書き記帳」などのアナログ作業で、PCには手書き記帳された情報から入力していました。 |
| 手順3：デジタル技術による課題解決 |
| 外部のITベンダーの力を借り、計測器と専用PCを連携させてブドウの重量データを送信するともに、生産農家や品種をコード管理して、生産地などとリンクできるようにしました。 |
| 手順4：顧客に新たな価値を提供・ビジネスモデルの転換 |
| ブドウの重量・品種・産地・生産者をリアルタイムで集約管理し、特定産地のブドウを特定のタンクに貯蔵する、いわゆる「産地細分化ワイン」を製造できるようになりました。  結果、産地細分化ワインの増産・安定供給の実現につながりました。 |

#### 次世代技術を活用したビジネス展開

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

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



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

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

##### 事例1：不動産売買・仲介・賃貸業（東京都・不動産業）

（出典） 経済産業省 「DX Selection 2024」をもとに作成

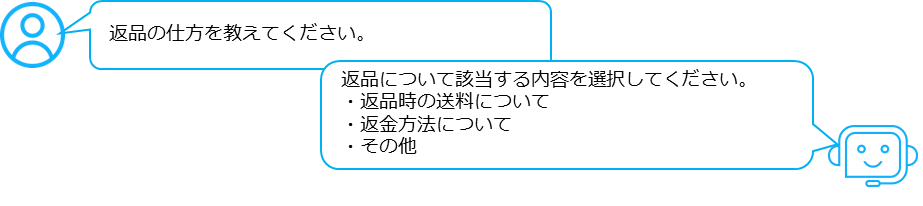
|  |  |
| --- | --- |
| 取組のきっかけ | 自社MISSIONを追求すべく、継続に成長できる企業へ邁進していくために、DXによるデジタル技術と活用が急務、かつ必須ととらえたため。 |
| 解決への取組 | ノーコードツールやRPAを導入するにあたり、情報システム担当者に加えて、各部署1名程度エバンジェリスト※を選出し、現場と情報システム部による共創の形をとりました。社長自ら率先してDXの重要性について語ることに加え、社内ブログやコーポレートサイトなどを利用して、広く周知することで、全社としてDXに取り組んでいることの本気度を社内外へ示しました。  DXの取り組んだ成果と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

##### 事例2：観光客向け飲食、販売業（三重県・飲食・サービス業）

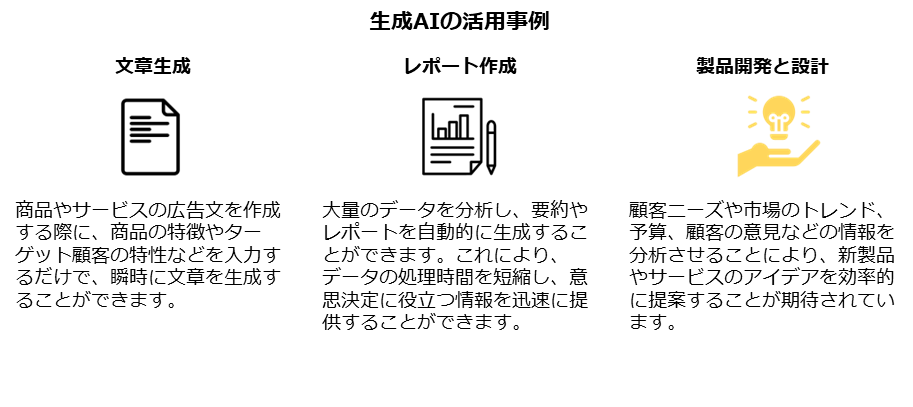
（出典） 経済産業省 「DX Selection 2024」をもとに作成

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

##### チャットボット

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

|  |
| --- |
| 予想・今後の発展 |
| 近年、AIを搭載したチャットボットが登場しています。これまでのチャットボットとは異なり、蓄積されたデータを学習するため、決められた内容や選択肢に限定されず他の質問にも対応できたり、ユーザーからの質問に表現の揺らぎがあった場合でも、一定程度対応できたり、さらには複雑な質問にも回答できるようになっています。  生成AIの登場  生成AIとは、さまざまなコンテンツを生成することができるAIのことです。従来のAIが主にデータを分析・学習し、その結果に基づいて予測を行うのに対して、生成AIは新たなコンテンツの創造を目的として学習します。生成AIは学習量が多いため、回答の精度や質が従来のものより高く、またコンテンツの生成速度も非常に速いという特徴があります。従来のチャットボットは主にオペレータ業務のサポートなど、お問い合わせ対応に限定されていましたが、生成AIでは以下のような活用ができることが期待されています。 |



### 経営投資としてのサイバーセキュリティ対策

#### サイバーセキュリティ対策の重要性

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

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

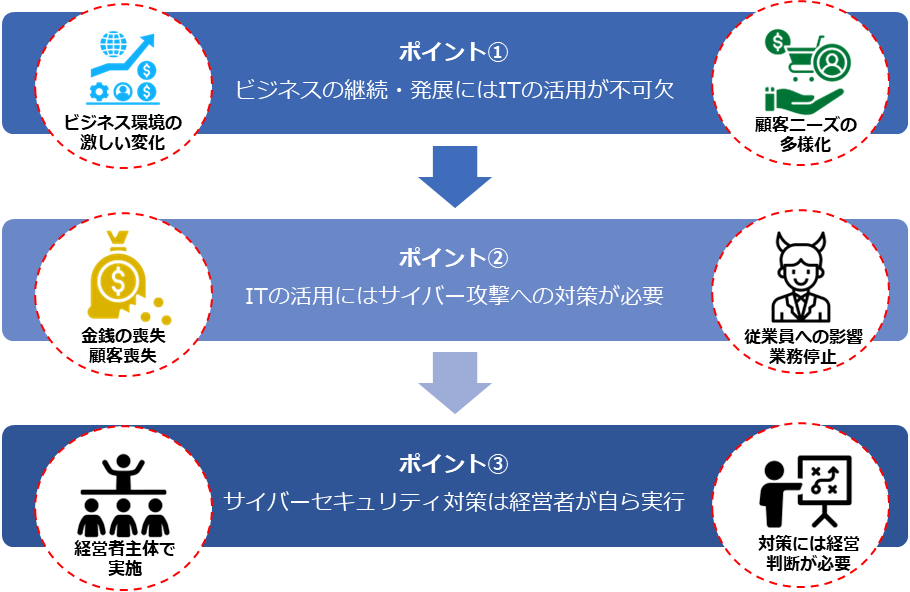
次のページから、経営者目線でセキュリティ対策を行わなければならない理由を以下のポイントごとに説明していきます。

図30. ITの活用とサイバーセキュリティ対策の関係性

（出典） 東京都産業労働局.” MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響”. <https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html>

#### 経営者が重要視すべき3つのポイント

|  |
| --- |
| ポイント1：ビジネスの継続・発展にはITの活用が不可欠 |
| 中小企業にとって、業務や生産の効率化、人材確保は重要な課題です。業務・生産工程などの運用コストの削減・効率化のために、ITの活用が不可欠になっています。また近年では、競争力維持・強化のために、DXを進めることが求められており、ITの活用が必須になっています。 |
| 中小企業の課題 |
| ポイント2：ITの活用にはサイバー攻撃への対策が必要 |
| 事例：サプライチェーン攻撃による情報流出被害  保険業界  某保険会社は、顧客情報の一部が流出したことを公表し、謝罪しました。情報流出の原因としては、外部委託先の企業のサーバが不正アクセスを受けたことです。顧客の氏名、性別、生年月日、メールアドレスなどの個人情報が数十万人分漏えいしてしまいました。その結果、数億円以上の損害や多くのお客様に対する信頼を低下させてしまう事態となりました。このようにサプライチェーンを介した攻撃では、自社が直接サイバー攻撃を受けていなくても、間接的に被害にあってしまいます。 |
| ポイント3：サイバーセキュリティ対策は経営者が自ら実行 |
| 経営者は自ら主体となって指揮をとり、セキュリティ対策を行う必要があります。理由は、主に2つあります。1つ目は、セキュリティ対策を行うにあたり、サイバー攻撃のリスクの許容範囲をどの程度にするのか、セキュリティ投資をどこまで行うのかなど、経営者による経営判断が必要になるからです。2つ目は、セキュリティインシデントが発生した際に、経営者が「法的責任」や「社会的責任」を負わなければならないからです。経営者は民法や会社法により、善管注意義務という「取締役として期待される水準の注意をもって業務を行う義務」を負い、その任務を怠った際に生じた損害を株式会社に対して賠償する責任「任務懈怠」を負うことが規定されています。そのため、セキュリティ対策にベストを尽くさなかった結果、サイバー攻撃による情報漏えいや事業停止が起き、第三者に損害が生じた場合、善管注意義務違反や任務懈怠に基づく損害賠償責任を問われてしまいます。 |

図31. 情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律

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

|  |  |  |
| --- | --- | --- |
| 法令 | 条項 | 要約 |
| 民法 | 第415条 債務不履行による損害賠償責任 | サイバー攻撃により仕事が停滞した場合、会社および第三者に対する、契約違反による賠償義務を負う。 |
| 第644条 取締役の善管注意義務違反 | 企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。 |
| 第562条 契約不適合責任 | 請負契約の仕事の目的物（開発システムなど）について、その種類や品質が契約内容に適合しないことが仕事の完成後に判明した場合、会社および第三者に対する契約不適合となる。 |
| 第709条 不法行為による損害賠償  第715条 使用者等の責任 | 故意又は過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する義務を負う。 |
| 会社法 | 第330条 取締役の善管注意義務違反 | 企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償責任を負う。 |
| 第423条第1項 任務懈怠による損害賠償責任 |
| 第429条第1項 第三者に対する注意義務違反 |

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

編集後記

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

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

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

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

引用文献

|  |
| --- |
| Society 5.0 |
| https://www8.cao.go.jp/cstp/society5\_0 |
| デジタルガバナンス・コード2.0 |
| https://www.meti.go.jp/policy/it\_policy/investment/dgc/dgc.html |
| SECURITY ACTION セキュリティ対策自己宣言 |
| https://www.ipa.go.jp/security/security-action |
| 情報セキュリティ5か条 |
| https://www.ipa.go.jp/security/security-action/download/5point\_poster.pdf |
| 5分でできる！情報セキュリティ自社診断 |
| https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf |
| 情報セキュリティ基本方針（サンプル） |
| https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072146.docx |
| 経済財政運営と改革の基本方針2024 |
| https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html |
| デジタル社会の実現に向けた重点計画 |
| https://www.digital.go.jp/assets/contents/node/basic\_page/field\_ref\_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609\_policies\_priority\_outline\_05.pdf |
| サイバー・フィジカル・セキュリティ対策 フレームワークVer1.0 |
| https://www.meti.go.jp/policy/netsecurity/wg1/CPSF\_ver1.0.pdf |
| 中堅・中小企業等向けデジタルガバナンス・コード実践の手引き2.0 |
| https://www.meti.go.jp/policy/it\_policy/investment/dx-chushoguidebook/tebiki2-0.pdf |
| 製造分野のDX事例集 |
| https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf |
| サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ |
| https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf |
| サイバーセキュリティ2024 |
| https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf |
| 企業経営のためのサイバーセキュリティの考え方の策定について |
| https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf |
| ITおよびサイバーセキュリティに関する組織の視点6分類 |
| https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/205/index.html |
| 「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは？ |
| https://www.gov-online.go.jp/useful/article/201703/1.html |
| 情報セキュリティ 10 大脅威の活用法2024 |
| https://www.ipa.go.jp/security/10threats/nq6ept000000g23i-att/katsuyouhou\_2024.pdf |
| 中小企業のためのセキュリティインシデント対応の手引き |
| https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf |
| 【NISC】サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究） |
| https://www.nisc.go.jp/pdf/policy/inquiry/kokai\_jireishu.pdf |
| 令和5年におけるサイバー空間をめぐる脅威の情勢等について（警察庁） |
| https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05\_cyber\_jousei.pdf |
| 令和4年通信利用動向調査の結果 |
| https://www.soumu.go.jp/johotsusintokei/statistics/data/230529\_1.pdf |
| CPS/IoTの利活用分野別世界市場調査の発表 |
| https://www.jeita.or.jp/cgi-bin/topics/detail.cgi?n=3455&ca=1 |
| 情報通信白書令和3年版（総務省） |
| https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf |
| DX白書2023 |
| https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf |
| 攻めのIT活用指針 |
| https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki\_1.pdf |
| DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～ |
| https://www.meti.go.jp/shingikai/mono\_info\_service/digital\_transformation/pdf/20180907\_03.pdf |
| 中堅・中小企業等向け『デジタルガバナンス・コード』実践の手引き |
| https://www.meti.go.jp/policy/it\_policy/investment/dx-chushoguidebook/tebiki.pdf |
| 「DXセレクション2024」選定企業レポート （経済産業省） |
| https://www.meti.go.jp/policy/it\_policy/investment/dx-selection/dxselection2024report.pdf |
| MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響 |
| https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html |
| 中小企業の情報セキュリティ対策ガイドライン 第3.1版 |
| https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf |

参考文献

|  |
| --- |
| SECURITY ACTION セキュリティ対策自己宣言 |
| https://www.ipa.go.jp/security/security-action |
| 情報セキュリティ5か条 |
| https://www.ipa.go.jp/security/security-action/download/5point\_poster.pdf |
| 5分でできる！情報セキュリティ自社診断 |
| https://www.ipa.go.jp/security/guide/sme/5minutes.html |
| 情報セキュリティ白書2023 |
| https://www.ipa.go.jp/publish/wp-security/2023.html |
| 情報セキュリティ10大脅威 2024 |
| https://www.ipa.go.jp/security/10threats/10threats2024.html |
| サイバー攻撃対応事例 |
| https://security-portal.nisc.go.jp/dx/provinatack.html |
| リスク分析シート |
| https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-att/000055518.xlsx |
| セキュリティ関連費用の可視化 |
| https://www.ipa.go.jp/jinzai/ics/core\_human\_resource/final\_project/2022/visualization-costs.html |
| 中小企業の情報セキュリティ対策ガイドライン第3.1版 |
| https://www.ipa.go.jp/security/guide/sme/about.html |
| ISMS適合性評価制度 |
| https://isms.jp/isms.html |
| セキュリティ関連NIST文書について |
| https://www.ipa.go.jp/security/reports/oversea/nist/about.html |
| サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF） |
| https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html |
| セキュリティ関連知識の保管庫（ナレッジベース2024） |
| https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/ |
| サイバーセキュリティ 2024 |
| https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf |
| サイバーセキュリティ経営ガイドラインVer 3.0 |
| https://www.meti.go.jp/policy/netsecurity/mng\_guide.html |
| サイバーセキュリティお助け隊サービス制度 |
| https://www.ipa.go.jp/security/sme/otasuketai-about.html |
| セキュリティ・キャンプ |
| https://www.security-camp.or.jp |
| ICSCoE中核人材育成プログラム |
| https://www.ipa.go.jp/jinzai/ics/core\_human\_resource |
| コンピュータウイルス・不正アクセスの届出事例 |
| https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf |

用語集

■AI

Artificial Intelligenceの略。

「AI（人工知能）」という言葉は、昭和31年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和25年代後半から昭和35年代が第一次AIブーム、昭和55年代が第二次AIブーム、現在は平成20年代から始まる第三次AIブームである（近年の大規模言語モデルなどの登場を契機に、第4次AIブームに入ったとの見方もある）。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

■CSIRT（シーサート）

Computer Security Incident Response Teamの略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

■DDoS攻撃（ディードスこうげき）

Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■DFFT

Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

■EDR

Endpoint Detection and Responseの略。パソコンやスマホ、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

■ICSCoE中核人材育成プログラム

平成29年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■ICT

Information and Communication Technologyの略。IT（情報技術）に加えて、コンピュータやスマホなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

■IoT（アイ・オー・ティー）

Internet of Thingsの略。日本語では「モノのインターネット」。インターネットにコンピュータやセンサー、カメラ、産業機械、家電などさまざまな「モノ」が接続され、データを収集したり、相互に情報をやり取りしたりする概念や仕組み、技術のこと

■IPアドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。 IPアドレスは、127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。 現在主に使用されているこれらの4つの数字の組み合わせによるアドレス体系は、IPv4（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加に加えて、情報セキュリティ機能の追加などの改良も加えられている

■ISMS

Information Security Management Systemの略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取り組み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる

■NISC

National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当

■NIST サイバーセキュリティフレームワーク（CSF）

米国政府機関の重要インフラの運用者を対象として誕生し、防御に留まらず、検知・対応・復旧といった、インシデント対応が含まれている、日本においても、今後普及が見込まれる

■SASE（サシー）

Secure Access Service Edgeの略。令和元年に提唱したゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウドサービス上で統合して提供するサービス、また、その考え方・概念

■SDP

Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、すべての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザーの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

■Society5.0

日本が目指すべき未来社会の姿として、2016年に閣議決定された「第5期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている

■SWG

Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現

■VPN

Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。VPNを使用することで、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと

■アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することで、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマホやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

セキュリティソフトウェアがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真つきの手配書のようなもの

■エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT分野においては、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■可用性

許可された者だけが必要な時にいつでも情報や情報資産にアクセスできる特性

■完全性

参照する情報が改ざんされていなく、正確である特性

■機密性

許可された者だけが情報や情報資産にアクセスできる特性

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などを行うこと

■個人情報保護委員会

個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱いを確保することを任務とする、独立性の高い行政機関（組織的には内閣府の外局）。個人情報保護法およびマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱いに関する監視・監督、認定個人情報保護団体に関する事務などの業務を行っている

■サイバー攻撃

インターネットを通じて、別の企業や組織、国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマホから、企業のサーバやデータベース、国の重要インフラまでさまざまである。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。IPAが中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

単純なサイバー空間（仮想空間）におけるセキュリティ対策から、サイバー空間とフィジカル空間（現実空間）のそれぞれにおけるリスクを洗い出し、そのセキュリティ対策を整理するためのフレームワーク

■サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

■情報セキュリティの3要素「CIA」

情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ

■真正性

情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある

■信頼性

システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性

■スクリーンロック

デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっている時は、パスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない

■脆弱性

情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）におけるセキュリティ上の欠陥のこと

■責任追跡性

情報資産に対する参照や変更などの操作を、どのユーザーが行ったものかを確認することができる特性

■セキュリティインシデント

セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当

■セキュリティ・キャンプ

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している

■セキュリティホール

情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある

■セキュリティポリシー

企業や組織において実施するセキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するためのセキュリティ管理体制、運用規定、基本方針、対策基準などを具体的に記載することが一般的

■ゼロデイ攻撃

OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと

■ゼロトラスト

従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、すべてのネットワーク通信を信用できない領域として扱い、すべての通信を検知し認証するという新しいセキュリティの考え方

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマホの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■データサイエンス

数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである

■デジタル情報

0、1、2のような離散的に（数値として）変化する量

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者を騙して、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得したり、本人に認証させたりすることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトウェアに付いているもの、専用のハードウェアになっているものなど形態はさまざまである

■不正アクセス

利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入する時に、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■フォレンジック

犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組を指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録するオープンな分散型台帳。ビットコインなどの暗号資産に使われている仕組み

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準に従って最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論

■マルウェア

パソコンやスマホなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる

■無線LAN

LANはLocal Area Networkの略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットなどのネットワークにアクセスすることができる

■ランサムウェア

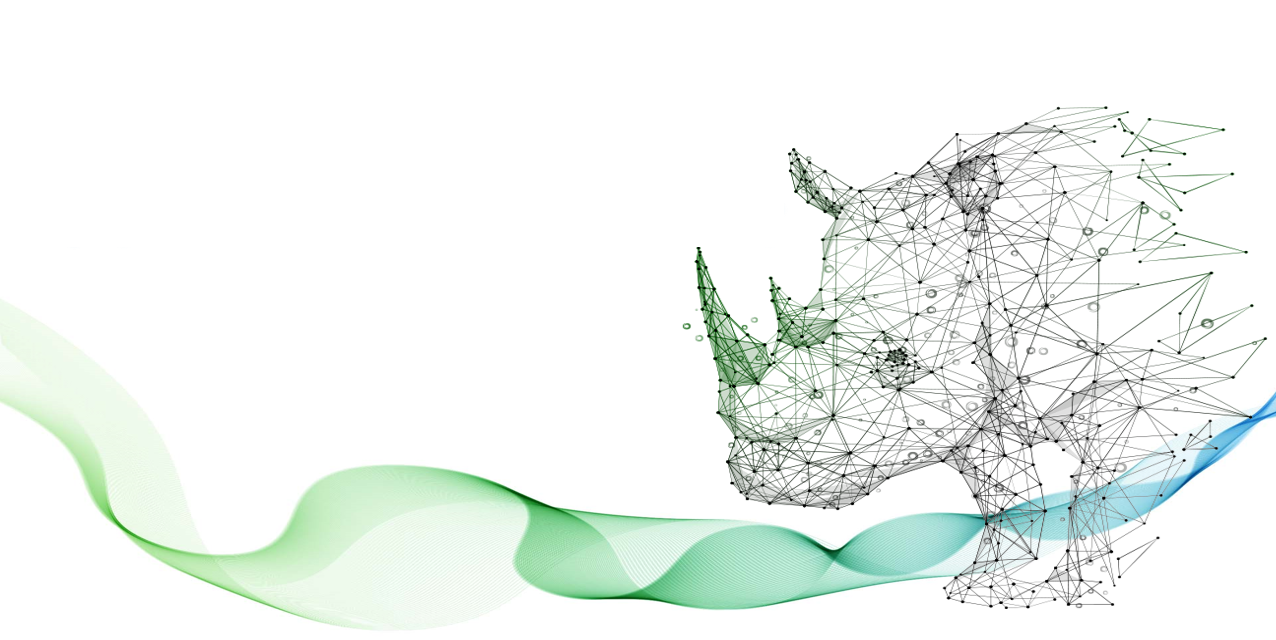
悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する

■リスク評価

組織やプロジェクトにおける特定されたリスクに対して、重要度や影響度を評価するプロセス

■リモートデスクトップ接続

パソコン、タブレット、スマホなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法



1. 経済産業省. “デジタルガバナンス・コード2.0”. https://www.meti.go.jp/policy/it\_policy/investment/dgc/dgc2.pdf [↑](#footnote-ref-2)
2. 経済産業省. “デジタルガバナンス・コード2.0”. https://www.meti.go.jp/policy/it\_policy/investment/dgc/dgc2.pdf [↑](#footnote-ref-3)
3. デジタル庁.”デジタル社会の実現に向けた重点計画”.https://www.digital.go.jp/assets/contents/node/basic\_page/field\_ref\_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609\_policies\_priority\_outline\_05.pdf [↑](#footnote-ref-4)
4. 内閣府.”Society5.0”.https://www8.cao.go.jp/cstp/society5\_0 [↑](#footnote-ref-5)
5. IPA.”情報セキュリティ白書2022”. https://www.ipa.go.jp/publish/wp-security/sec-2022.html [↑](#footnote-ref-6)
6. NISC.”サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）”https://www.nisc.go.jp/pdf/policy/inquiry/kokai\_jireishu.pdf [↑](#footnote-ref-7)
7. 警察庁.”令和5年におけるサイバー空間をめぐる脅威の情勢等について”. https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05\_cyber\_jousei.pdf [↑](#footnote-ref-8)
8. 総務省.”情報通信白書令和3年版”. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf [↑](#footnote-ref-9)
9. 経済産業省.” DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～”.https://www.meti.go.jp/shingikai/mono\_info\_service/digital\_transformation/pdf/20180907\_03.pdf [↑](#footnote-ref-10)