中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

東京都産業労働局

第0章. テキストの活用

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

0-1. テキストの目的、想定読者、全体構成、テキストの利用方法など

0-1-1. テキストの目的、想定読者

昨今の社会情勢を背景に、日本の中小企業にとってサイバーセキュリティは喫緊の課題となっています。ビジネスの成長には DX の推進が不可欠であり、特に生成 AI の活用は重要な要素です。しかし、DX の進展とともにサイバーセキュリティのリスクも増大するため、各局面で適切な対策を講じることが求められます。この対策は、組織の責任者のリーダーシップのもと、実務担当者が連携して実施していくことで、企業の安全なデジタル化を実現できます。

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。攻撃を受けた中小企業だけでなく、その取引先にも影響を与え、サプライチェーン全体に影響が広がることで、当該企業の業務停止による損失だけではなく、業界全体の業務が停滞するリスクがあります。

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

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

0-1-2. 全体構成

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

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

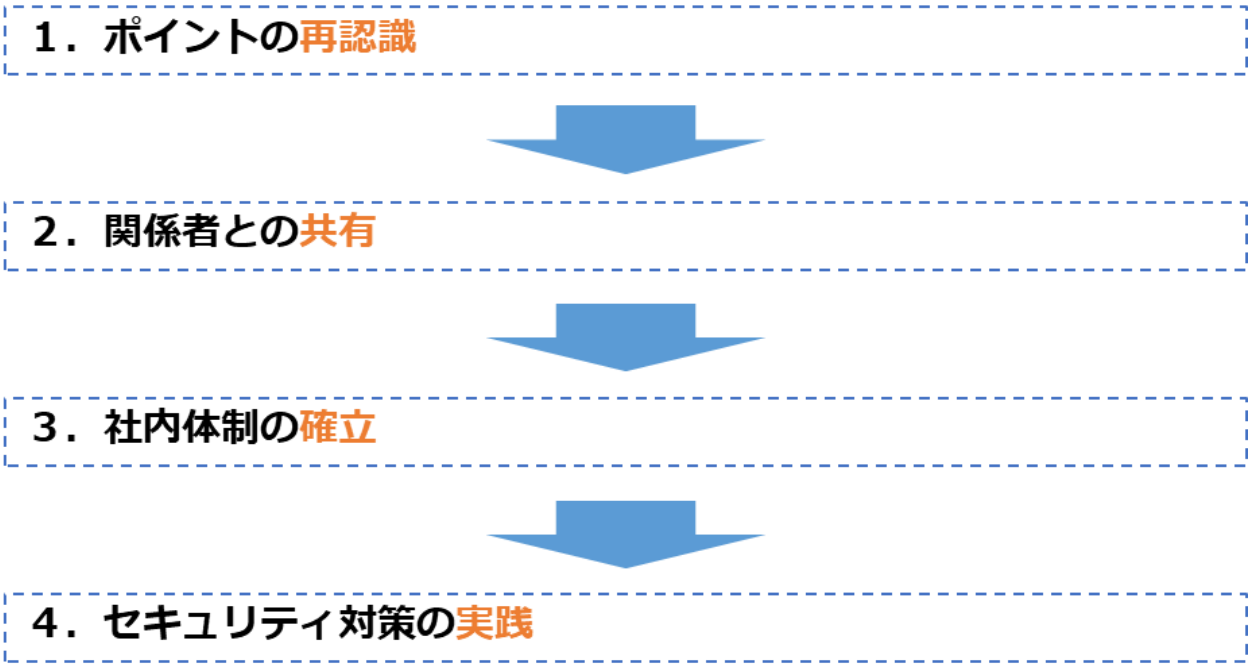
最後に、組織としてセキュリティ対策を実施するための知識やスキルおよび、それらを持った人材の育成や確保といった、組織のセキュリティレベル向上を図るにあたって実践的な知識を提供し

ます。

0-1-3. テキストの利用方法

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

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



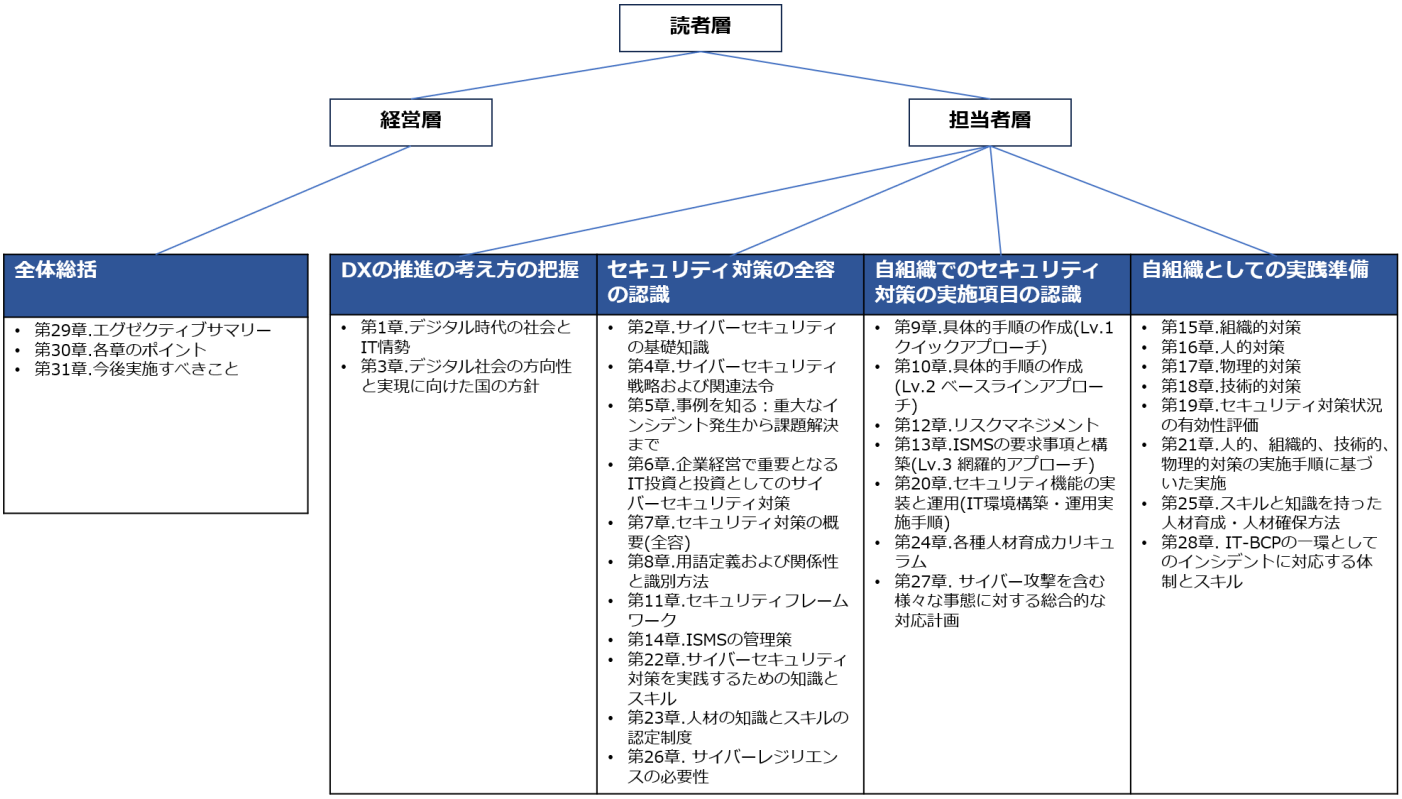
1．ポイントの再認識

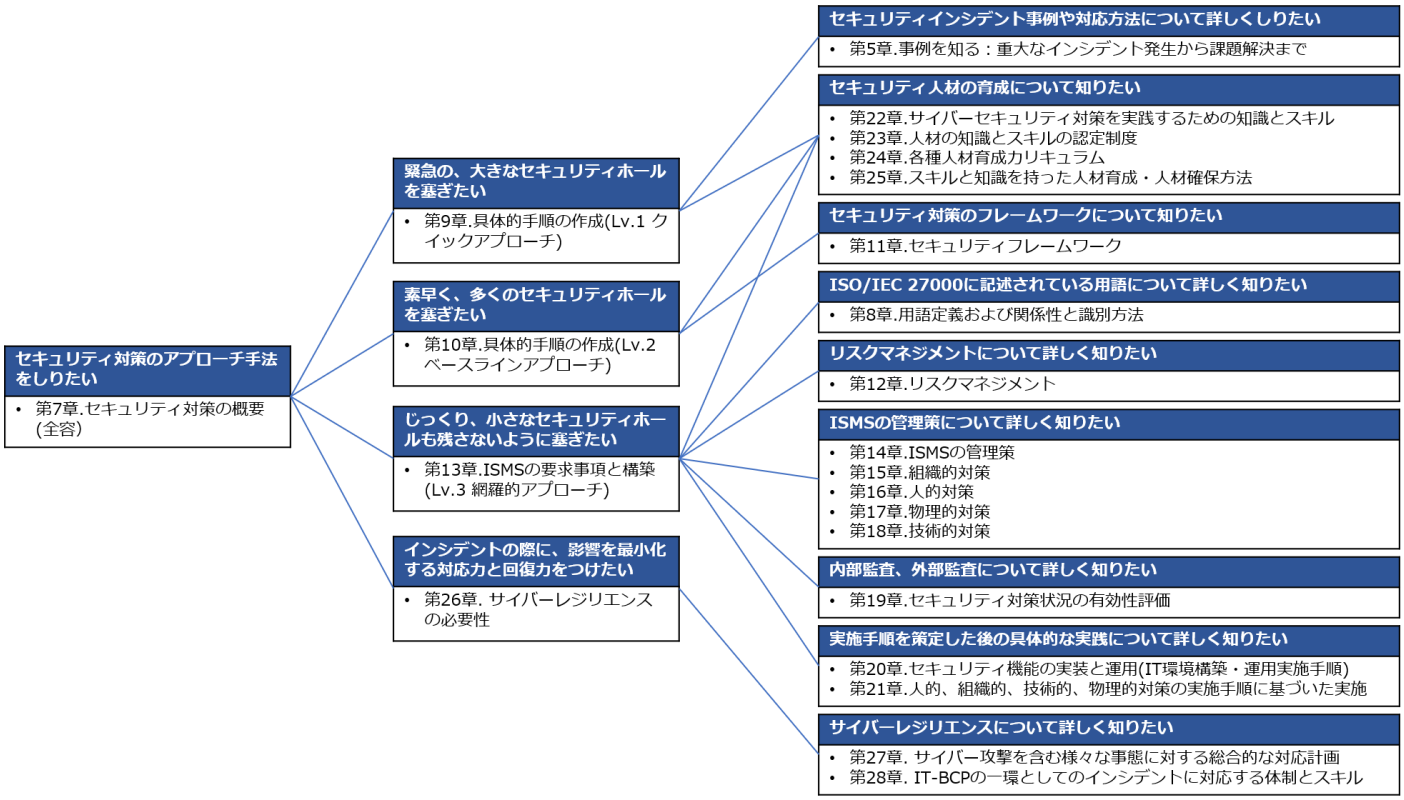
「DX の理解からサイバーセキュリティ対策の実践まで」のポイントを再認識します。

各章の内容は以下の通りです。

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

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


読者層
経営層
担当者層
全体総括
• 第29章,エグゼクティブサマリー
• 第30章,各章のポイント
• 第31章,今後実施すべきこと
DXの推進の考え方の把握
• 第1章,デジタル時代の社会とIT情勢
• 第3章,デジタル社会の方向性と実現に向けた国の方針
セキュリティ対策の全容の認識
• 第2章,サイバーセキュリティの基礎知識
• 第4章,サイバーセキュリティ戦略および関連法令
• 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
• 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
• 第7章,セキュリティ対策の概要(全容)
• 第8章,用語定義および関係性と識別方法
• 第11章,セキュリティフレームワーク
• 第14章,ISMSの管理策
• 第22章,サイバーセキュリティ対策を実践するための知識とスキル
• 第23章,人材の知識とスキルの認定制度
• 第26章, サイバーレジリエンスの必要性
自組織でのセキュリティ対策の実施項目の認識
• 第9章,具体的手順の作成(Lv.1 クイックアプローチ)
• 第10章,具体的手順の作成(Lv.2 ベースラインアプローチ)
• 第12章,リスクマネジメント
• 第13章,ISMSの要求事項と構築(Lv.3 網羅的アプローチ)
• 第20章,セキュリティ機能の実装と運用(IT環境構築・運用実施手順)
• 第24章,各種人材育成カリキュラム
• 第27章, サイバー攻撃を含む様々な事態に対する総合的な対応計画
自組織としての実践準備
• 第15章,組織的対策
• 第16章,人的対策
• 第17章,物理的対策
• 第18章,技術的対策
• 第19章,セキュリティ対策状況の有効性評価
• 第21章,人的、組織的、技術的、物理的対策の実施手順に基づいた実施
• 第25章,スキルと知識を持った人材育成・人材確保方法
• 第28章, IT-BCPの一環としてのインシデントに対応する体制とスキル


セキュリティ対策のアプローチ手法をしりたい
• 第7章,セキュリティ対策の概要(全容)
緊急の、大きなセキュリティホールを塞ぎたい
• 第9章,具体的手順の作成(Lv.1 クイックアプローチ)
素早く、多くのセキュリティホールを塞ぎたい
• 第10章,具体的手順の作成(Lv.2 ベースラインアプローチ)
じっくり、小さなセキュリティホールも残さないように塞ぎたい
• 第13章,ISMSの要求事項と構築(Lv.3 網羅的アプローチ)
インシデントの際に、影響を最小化する対応力と回復力をつけたい
• 第26章, サイバーレジリエンスの必要性
セキュリティインシデント事例や対応方法について詳しくしりたい
• 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
セキュリティ人材の育成について知りたい
• 第22章,サイバーセキュリティ対策を実践するための知識とスキル
• 第23章,人材の知識とスキルの認定制度
• 第24章,各種人材育成カリキュラム
• 第25章,スキルと知識を持った人材育成・人材確保方法
セキュリティ対策のフレームワークについて知りたい
• 第11章,セキュリティフレームワーク
ISO/IEC 27000に記述されている用語について詳しく知りたい
• 第8章,用語定義および関係性と識別方法
リスクマネジメントについて詳しく知りたい
• 第12章,リスクマネジメント
ISMSの管理策について詳しく知りたい
• 第14章,ISMSの管理策
• 第15章,組織的対策
• 第16章,人的対策
• 第17章,物理的対策
• 第18章,技術的対策
内部監査、外部監査について詳しく知りたい
• 第19章,セキュリティ対策状況の有効性評価
実施手順を策定した後の具体的な実践について詳しく知りたい
• 第20章,セキュリティ機能の実装と運用(IT環境構築・運用実施手順)
• 第21章,人的、組織的、技術的、物理的対策の実施手順に基づいた実施
サイバーレジリエンスについて詳しく知りたい
• 第27章, サイバー攻撃を含む様々な事態に対する総合的な対応計画
• 第28章, IT-BCPの一環としてのインシデントに対応する体制とスキル

2. 関係者との共有

経営者を含めた関係者と、認識したポイントを共有します。「第 10 編.全体総括」をエグゼクティブサマリーとして活用してください。重要な点を理解し、経営者および他関係者と共有します。

3. 社内体制の確立

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

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

4. セキュリティ対策の実践

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

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

図 1. IT 導入プロセスにおけるセキュリティ対策の実施タイミング

第1章. デジタル時代の社会と IT 情勢

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

1-1. デジタル時代の社会変革と IT 情勢の関係性

社会の現状と今後の動向（Society5.0）

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

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

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

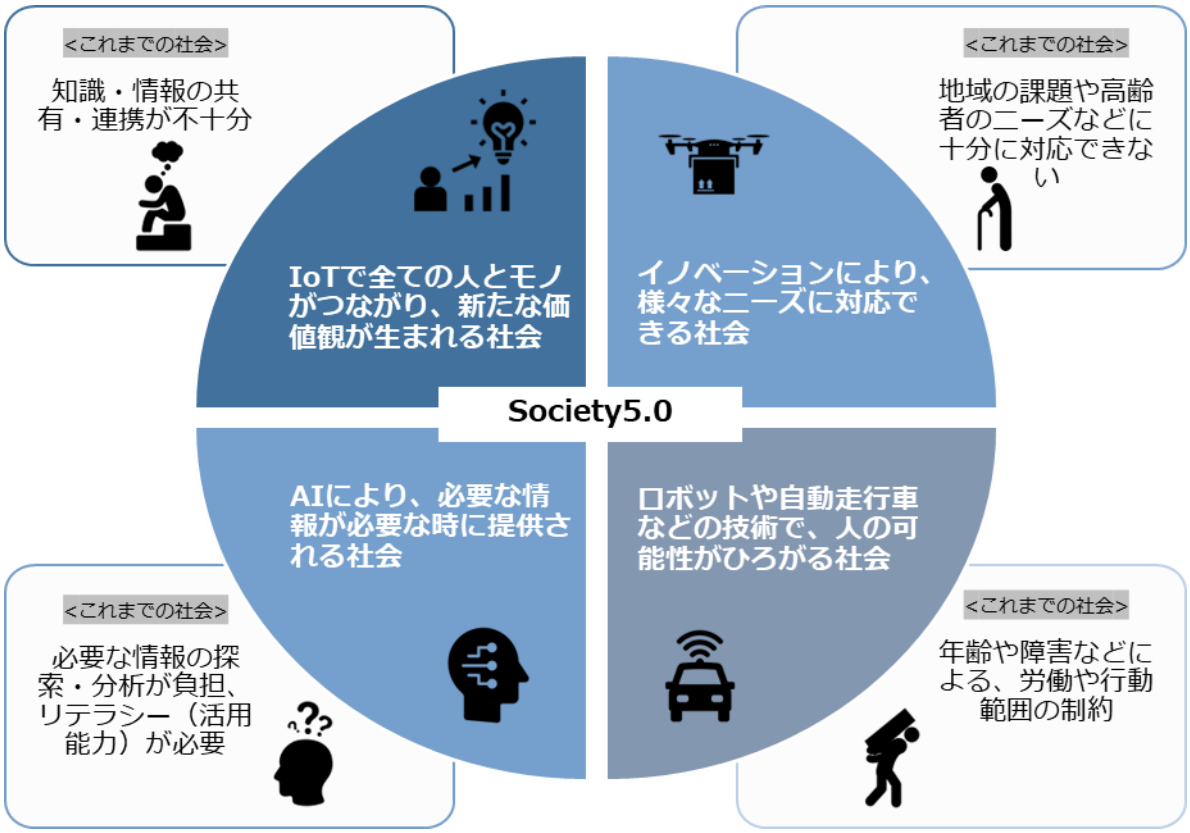


図 2. Society5.0 の概要図

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

デジタルトランスフォーメーション（DX）とは

ここでは、DX の定義を紹介し、DX の概要を説明します。

DX の定義
DX とは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズをもとに、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]
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。

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

生成 AI とは

令和 4 年 11 月に OpenAI 社が 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。

第2章. サイバーセキュリティの基礎知識

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

2-1. 導入済みと想定するセキュリティ対策機能

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

UTM（Unified Threat Management）

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

EDR（Endpoint Detection and Response）

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

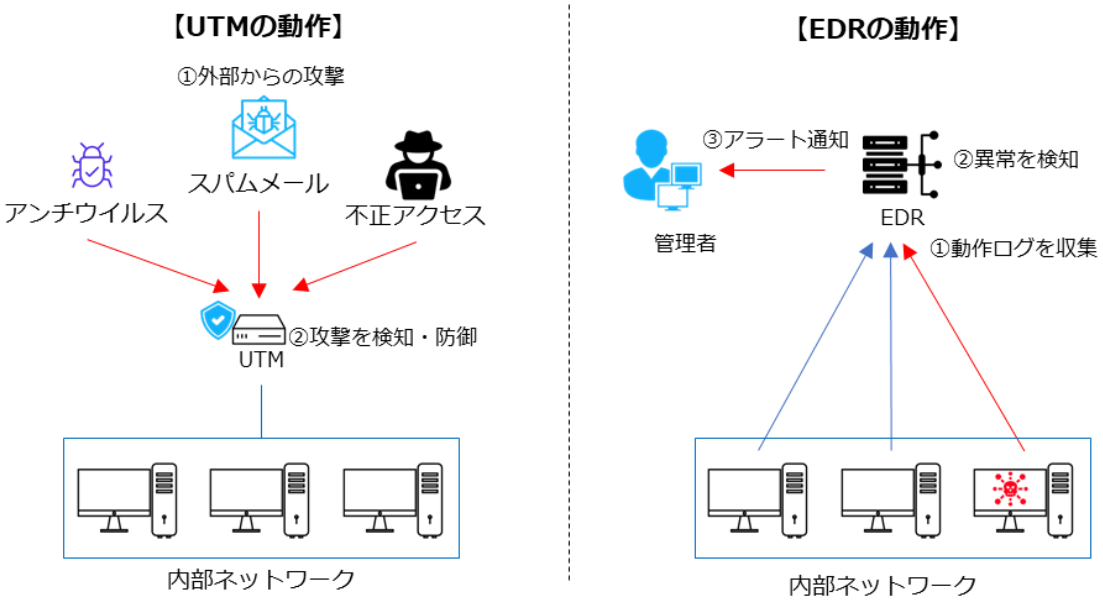


図 3. UTM、EDR の概要図

2-2. SECURITY ACTION（セキュリティ対策自己宣言）

2-2-1. SECURITY ACTION 二つ星レベル

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

SECURITY ACTION の自己宣言企業数：40 万社を突破（令和 7 年 4 月 23 日発表）

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

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

One Point

取得時における注意点

「SECURITY ACTION」はセキュリティ対策状況などを IPA が認定するものではありません。

「SECURITY ACTION」の取組に関して Web サイトなどにおいて次のような不適切な表現を使用されますと、第三者の誤解を生ずる可能性が懸念されますので、ご注意願います。

×「一つ星（二つ星）の認定を受けました」「一つ星（二つ星）を取得しました」

○「一つ星（二つ星）を宣言しました」

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

経済産業省では、中小企業を含めたサプライチェーンにおけるセキュリティ対策の重要性を踏まえ、各企業のセキュリティ対策状況を可視化する仕組み（サプライチェーン強化に向けたセキュリティ対策評価制度）の構築を検討しています。各企業のサプライチェーンにおける重要性や影響度

を踏まえ、求められるセキュリティ対策について区分を★3、★4、★5 の 3 つに分けることを想定しています。先行する自己評価制度の仕組みである「SECURITY　ACTION」にて一つ星、二つ星の区分を設けているため、★3 からの区分としています。なお、この仕組みは 2026 年度からの制度開始を目指しています。

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/
サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ	https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

2-2-2. 情報セキュリティ 5 か条

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

1.OS やソフトウェアは常に最新の状態にしよう！ OS やソフトウェアを古いまま放置していると、セキュリティ上の問題が解決されず、悪意のあるウイルスに感染してしまう危険性があるため、最新の状態にします。	
対策：	● パソコンやルーター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。	

(出典) IPA「情報セキュリティ 5 か条」をもとに作成

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

2-2-3. 情報セキュリティ自社診断

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

分類

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

診断方法

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

設問ごとに、以下の点数をつけ、全項目の合計点で組織全体のセキュリティ対策実施状況を確認

します。回答が「わからない」となっている項目を確認します。

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

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

(出典) IPA「 5 分でできる！情報セキュリティ自社診断」をもとに作成

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

「5 分でできる！情報セキュリティ自社診断」

No		診断内容
基本的対策	1	パソコンやスマホ等情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホ等にはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取組みを実施していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書い

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

(出典) IPA「 5 分でできる！情報セキュリティ自社診断」をもとに作成

2-2-4. 情報セキュリティ基本方針

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

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

情報セキュリティ基本方針（サンプル）

株式会社○○○○（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

2-3. サイバーセキュリティアプローチ方法

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

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

緊急に、大きなセキュリティホールを塞ぐ	**Lv.1 クイックアプローチ** **実施手法** 報道されるような事象・セキュリティ脅威に緊急対応します。 **活用できる文書/ツール名称（例）** ● 情報セキュリティ 10 大脅威（出典：IPA） ● 情報セキュリティ白書 2024（出典：IPA） ● サイバー攻撃を受けた組織における対応事例（出典：NISC）

素早く、多くのセキュリティホールを塞ぐ	**Lv.2 ベースラインアプローチ** **実施手法** ガイドブック、ひな型を参照し、迅速にセキュリティ対応します。 **活用できる文書/ツール名称（例）** ● リスク分析シート（出典：IPA） ● セキュリティ関連費用の可視化（出典：IPA） ● 中小企業の情報セキュリティ対策ガイドライン第 3.1 版（出典：IPA）

じっくり、小さなセキュリティホールも残さないように塞ぐ	**Lv.3 網羅的アプローチ** **実施手法** 網羅的なセキュリティ対策が定義されているフレームワークに沿ってセキュリティ対応します **活用できる文書/ツール名称（例）** ● ISMS（ISO/IEC27001:2022,27002:2022） ● NIST サイバーセキュリティフレームワーク（CSF）

	● サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

凡例）「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**
Lv.1 クイックアプローチは、サイバーセキュリティにおける即時の対応や緊急事態への対処に適しています。ただし、長期的な戦略や継続的な改善を妨げることなく、将来的なセキュリティの向上を見据えた計画の策定も必要となります。 ● 小規模な対策や修正を迅速に実施可能 ● 低コストでリスクを軽減 ● 進行中の攻撃へ対応することにより、攻撃の拡大や影響を最小限に抑える		×	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。		

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

ンの定義	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。

One Point

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

凡例）「〇：あり / △：部分的にあり / ×：なし」

Lv.3 網羅的アプローチ	**網羅性**	**即時性**
Lv.3 網羅的アプローチは、可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなります。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではありません。 ・可能な限り多くの脅威や攻撃手法に対して対策を講じる ・予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持	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 2024	https://www.ipa.go.jp/publish/wp-security/eid2eo0000007gv4-att/2024_ALL.pdf
情報セキュリティ 10 大脅威 2025（組織編）	https://www.ipa.go.jp/security/10threats/10threats2025.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 2024-2025）	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（Non-Repudation）、信頼性（Reliability）を合わせて情報セキュリティの 7 要素と呼ぶこともあります。

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

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

第3章. デジタル社会の方向性と実現に向けた国の方針

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

3-1. 国の基本方針および実施計画の要約

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

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

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

ここでは、令和 6 年に策定された基本方針の中から、特に IT 戦略に関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。

サイバーセキュリティの強化

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

（出典）内閣府「経済財政運営と改革の基本方針 2024」をもとに作成

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

3-2-1. デジタル社会の実現に向けた重点計画

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

日本が目指すデジタル社会について、「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」と定義し、以下の 6 つの姿を挙げています。[2]

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

[2] 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

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

G ビズ ID とは事業者（法人、個人事業主）が 1 つのアカウントで様々な事業者向け行政手続システムにログインできるサービスである。G ビズ ID は、2020 年の運用開始より利用者数と接続先サービス数を順調に伸ばしており、補助金申請、社会保険手続、その他許認可等の行政手続へ G ビズ ID でログインが可能になり、事業者向け行政手続のオンライン化に寄与している。

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を 2024 年 8 月に行った。事業者は e-Gov により各省庁が所管する行政手続きについて申請や届出を行うことができる。

イ：J グランツの利便性向上と利用補助金の拡大

デジタル庁では、2025 年度以降の全ての事業者向け補助金申請について、原則電子化を目指し、事業者や行政機関の J グランツ利用開始を支援する取り組みを進めている。令和 7 年 1 月 31 日より、J グランツで代理申請が可能となった。

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順次進めている。

レベルに応じた認証の推進

ア：民間事業者への周知・相談支援の強化

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

イ：利用要件・利用手続などの改善

民間事業者の視点に立ち、利用要件・利用手続などの継続的な改善を実施する。

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

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

中小企業のデジタル化の支援

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

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」をもとに作成

3-2-2. 統合イノベーション戦略推進会議

国は、統合イノベーション戦略推進会議の下に AI 戦略会議と AI 制度研究会を設置しました。ここでは、イノベーションの推進とリスクへの適切な対応の両立を重視しており、限られた経営資源の中で生成 AI を安全かつ効果的に活用するための道筋を示すことが重要視されています 。AI が我が国の発展に大きく貢献する可能性がある一方、様々なリスクが表面化している現状を踏まえ、急速に進展し、中小企業を含む様々なビジネス主体にとって身近になりつつある生成 AI 技術の利活用を促進するとともに、その利用に伴うセキュリティリスクへのための制度的対応を検討しています。

3-2-3. 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。[3]

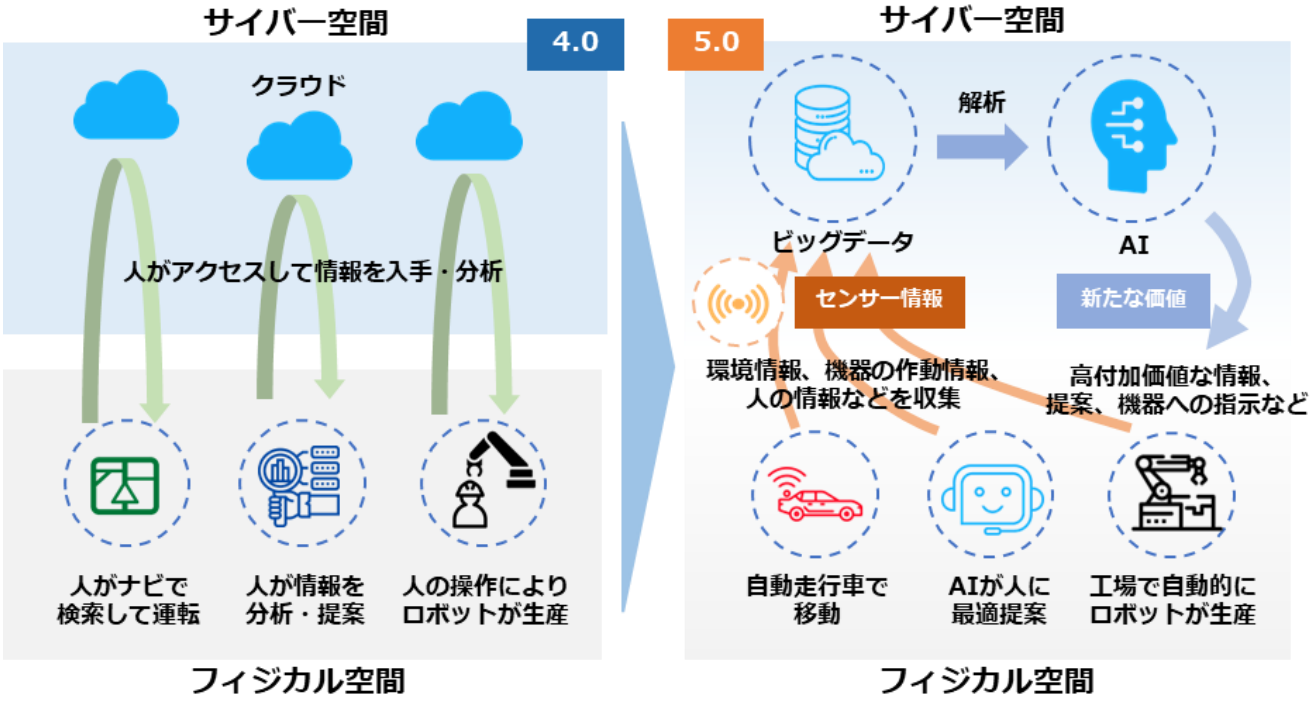


図 4. Society4.0 と Society5.0 の比較

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

[3] 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。

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

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

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

3-2-4. DX の推進

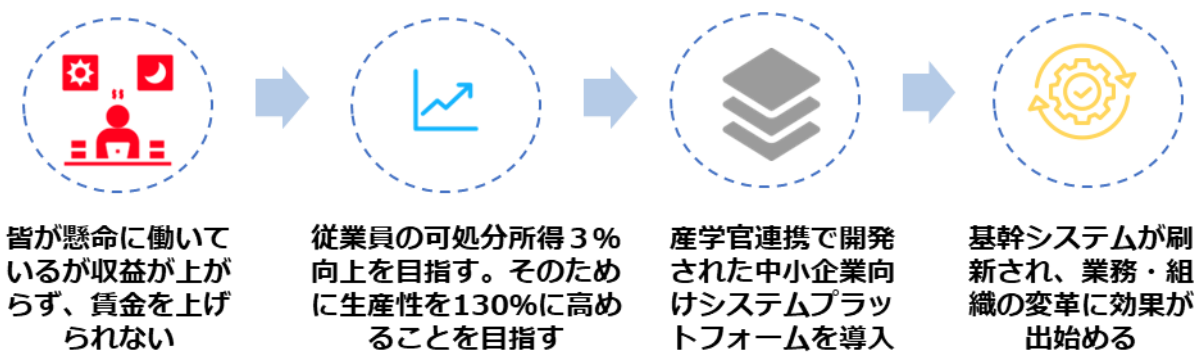
DX の推進における中小企業の優位性について説明します。DX とは、デジタル技術やツールを導入すること自体ではなく、データやデジタル技術を使って、顧客目線で新たな価値を創出していくことです。中小企業の中には、DX を推進し、売上高を 5 倍、利益を 50 倍に増加させた企業が存在します。中小企業ならではの優位性を理解し、積極的に DX に取り組むことで、大きく成長できる可能性があります。以下では、DX を推進する際に、中小企業の優位な点を説明します。そして、優位性を利用してビジネスモデルや企業文化などの変革に取り組んでいる企業の事例を紹介します。

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

事例（企業文化の改革）：精密機械部品加工

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

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



データ活用の流れ

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

以下は、データを活用し、業務を改革していくための手順となります。

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

事例（業務改革）：某メーカー

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

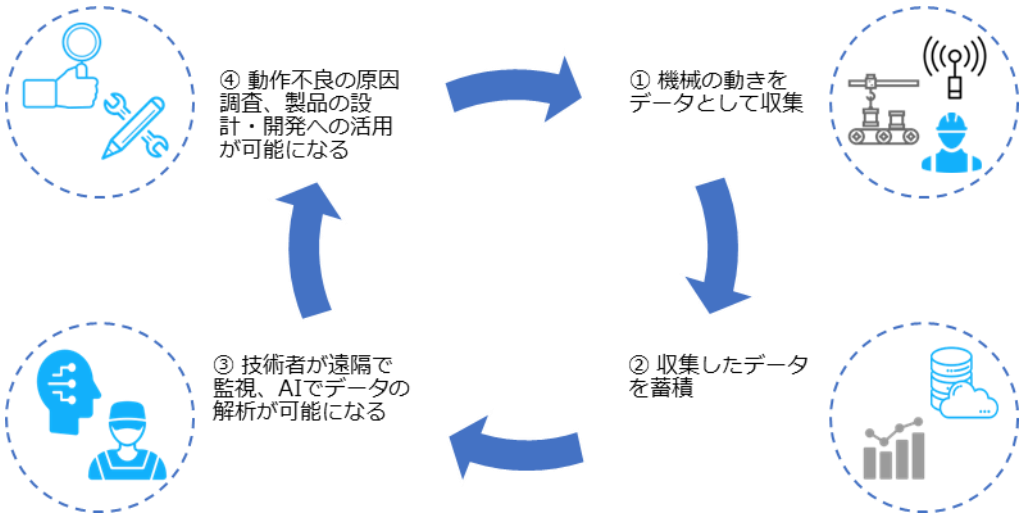


図 5. データ活用による業務改革の流れ

（出典）IPA"製造分野の DX 事例集".

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

DX with Cybersecurity の概要

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

すると同時に、セキュリティ対策も強化すること（DX with Cybersecurity）が求められることになります。

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

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

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

第4章. サイバーセキュリティ戦略および関連法令

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

4-1. NISC：サイバーセキュリティ戦略

4-1-1. サイバーセキュリティ戦略

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

サイバーセキュリティ戦略の課題と方向性

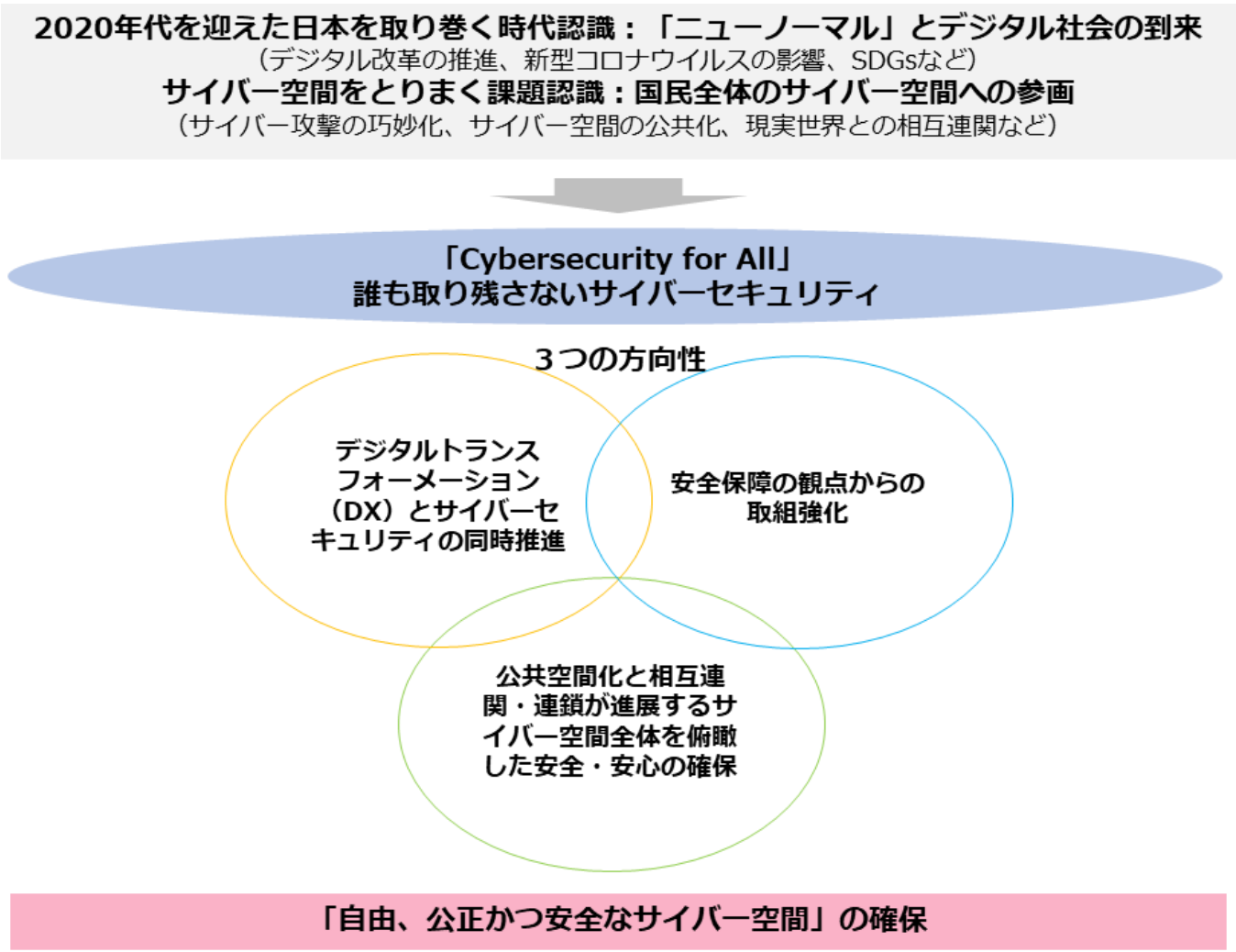


図 6.サイバーセキュリティ戦略の課題と方向性の概要
（出典）NISC「 サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ」をもとに作成

現在、あらゆる人々にとって、サイバーセキュリティの確保が必要とされる時代（Cybersecurity

for All）となってきています。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

課題に対する
具体的施策

主な具体的施策

経営層の意識改革

デジタル経営に向けた行動指針の実践を通じ、サイバーセキュリティ経営のガイドラインに基づく取組の可視化やインセンティブ付けを行い、さらなる取組を促進

地域・中小企業における DX with Cybersecurity の推進

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

新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり

Society5.0 に対応したフレームワークなども踏まえ、各種取組を推進

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

誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

情報教育推進の中、「デジタル活用支援」と連携して各種取組を推進

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

国民が安全で安心して暮らせるデジタル社会の実現

方向性	**公共空間化と相互連関・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

課題に対する具体的施策

主な具体的施策

国民・社会を守るためのサイバーセキュリティ環境の提供

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

デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保

経済社会基盤を支える各主体における取組

政府機関など：

- 監査・CSIRT 訓練・GSOC による監視などを通じたセキュリティ水準の向上

- クラウドサービスの利用拡大を見据えた政府統一基準群の改定
- 運用やクラウド監視に対応した GSOC 機能の強化

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

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

多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化

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

国際社会の平和・安定及び我が国の安全保障への寄与

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

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

課題

- 我が国を取り巻く安全保障環境は厳しさを増し、サイバー空間は、地政学的緊張も反映した国家間の競争の場となっている。中国・ロシア・北朝鮮は、サイバー能力の構築・増強を行い、情報窃取などを企図したサイバー攻撃を行っているとみられている
- 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）

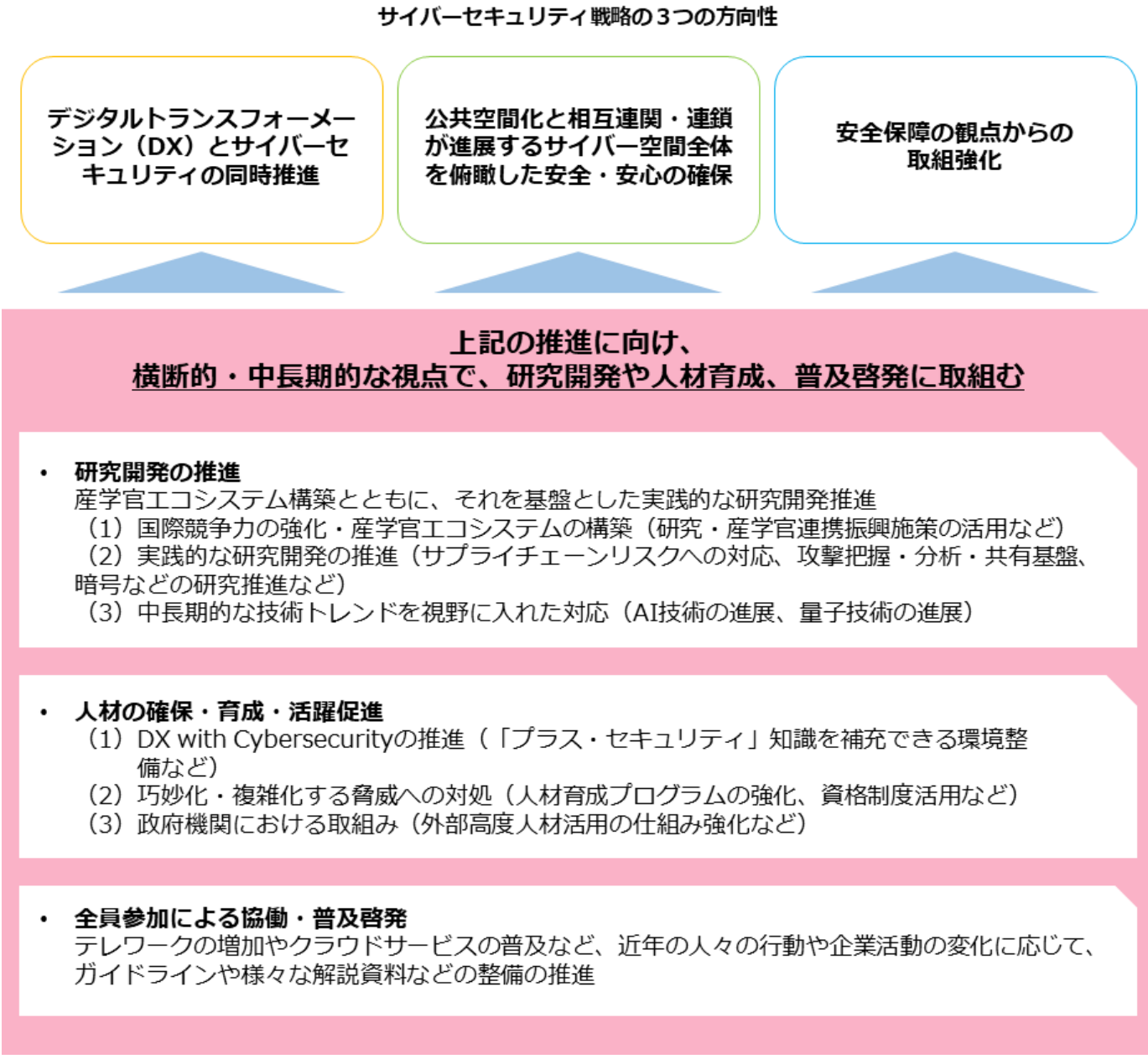
国際協力・連携

- 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

One Point

サイバーセキュリティ基本法

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

4-1-2. サイバーセキュリティ 2024

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

に従って整理されています。

サイバーセキュリティ基本法が定める３つの政策目的

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

サイバーセキュリティ戦略の３つの施策推進の方向性

- デジタル改革を踏まえたデジタルトランスフォーメーション（DX）とサイバーセキュリティの同時推進
- 公共空間化と相互連関・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

4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立

4-2-1. 企業経営のためのサイバーセキュリティの考え方

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

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

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

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

図 7.IT の活用またはサイバーセキュリティ対策の取組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 8 IT の活用またはサイバーセキュリティ対策の取組状況に応じた分類と対策
（出典）東京都「IT およびサイバーセキュリティに関する組織の視点 6 分類」をもとに作成

4-2-2. DX with Cybersecurity

業務や製品・サービスのデジタル化が進む中、サイバーセキュリティの確保は企業の価値に直結

する重要な要素となっています。このため、DX とサイバーセキュリティ確保に向けた取組を同時に推進すること（DX with Cybersecurity）が不可欠になっています。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/

4-3. 関連法令

4-3-1. 個人情報保護法

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

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

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

個人情報の定義

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

個人情報を取扱う時の基本ルール

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

One Point

個人情報保護法の罰則規定

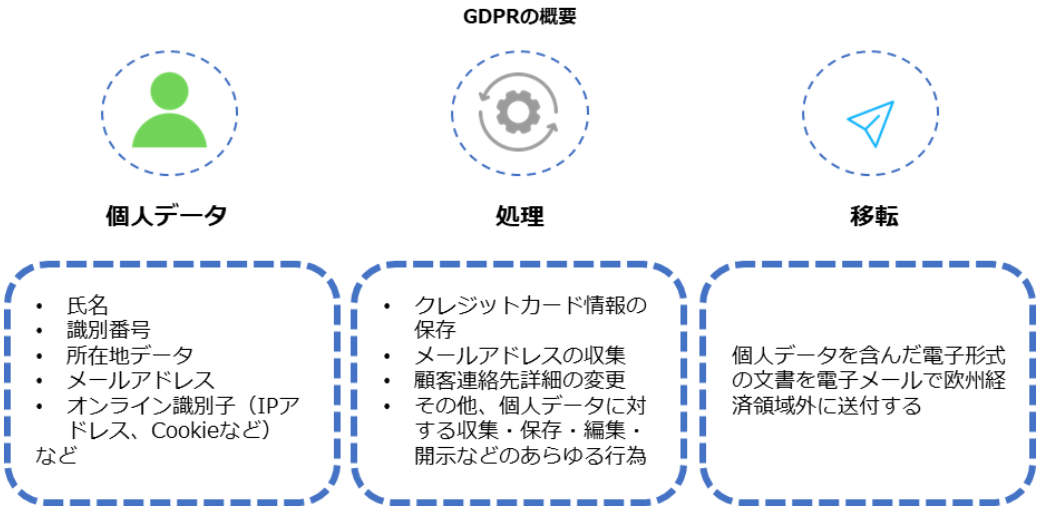
令和 4 年 4 月施行の法改正により、法令違反に対する罰則が強化されました。法人に対しては、個人情報保護委員会の措置命令に違反したり、個人情報データベースを不正流用したりした場合 1 億円以下、報告義務違反の場合 50 万円以下の罰金となっています。

4-3-2. GDPR

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

GDPR（一般データ保護規則）とは

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



GDPR と日本企業の関係

GDPR は EU 内で適用される法令ですが、支店など物理的な拠点を EU 内に持っていなくても、インターネットを利用して日本から EU 域内に商品販売やサービス提供、情報収集を行っている企業にも GDPR が適用されます。また、ターゲティング広告を配置した自社サイトに対して、EU 域内からアクセスがあった際も GDPR の適用対象となる可能性があります。GDPR に違反した場合はかなり重い制裁金が課されるため、適切な対策が求められます。

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

4-3-3. その他関連法令

そのほか、サイバーセキュリティに関連する法令の例を紹介します。

不正競争防止法
事業者間の不正競争の防止を目的の 1 つとしており、ブランドの表示の盗用、商品の形態模倣などとともに、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 ハンドブックポータルサイト	https://security-portal.nisc.go.jp/guidance/law_handbook.html
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
サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0　誤記修正箇所	https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/seigo.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。

なお、第 2 章の中で「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。

第5章. 事例を知る：重大なインシデント発生から課題解決まで

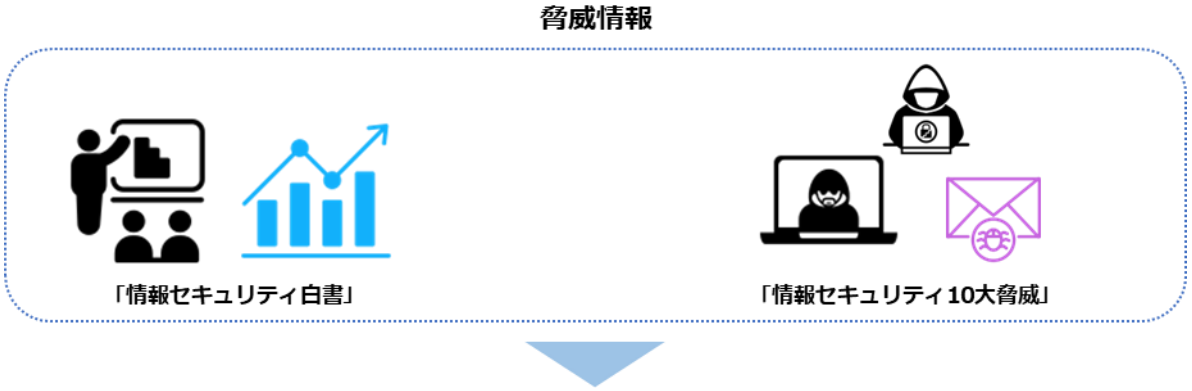
章の目的
第 5 章では、近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対するセキュリティ対策や、実際に被害に遭ってしまった際の対応方法について学ぶことを目的とします。
主な達成目標
□ 近年のサイバー攻撃の傾向や手法を理解すること □ 実際の被害事例を通して脅威に対するセキュリティ対策や予防方法を理解すること □ 脅威の検知から、復旧・再発防止処置までの流れを理解すること

5-1. 情報セキュリティの概況

5-1-1. 情報セキュリティの脅威を学ぶ

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

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



目的
最新の脅威情報を収集することによって、攻撃の傾向や手法、セキュリティリスクを把握し、適切な予防策やセキュリティ対策を講じること
学べる内容
● 攻撃手法や攻撃者の手口 ● 最近の攻撃傾向 ● 脅威に対するセキュリティ対策方法
活用例
● 攻撃の予防 ● セキュリティリスク管理、対策の強化 ● 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 2024	https://www.ipa.go.jp/publish/wp-security/eid2eo0000007gv4-att/2024_ALL.pdf
情報セキュリティ 10 大脅威 2025	https://www.ipa.go.jp/security/10threats/10threats2025.html

5-1-2. IPA：情報セキュリティ白書から見る脅威

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

図 9. 情報セキュリティ白書 2023

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。

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

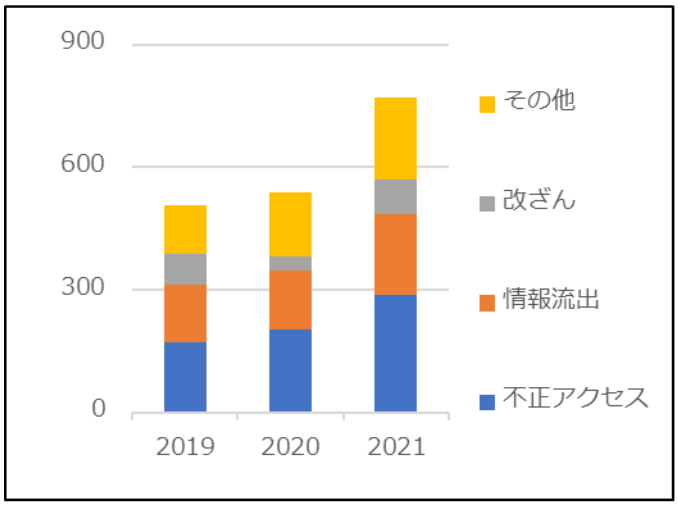
詳細理解のため参考となる文献（参考文献）	
サイバーセキュリティ経営ガイドライン Ver 3.0	https://www.meti.go.jp/policy/netsecurity/mng_guide.html
SECURITY ACTION セキュリティ対策自己宣言	https://www.ipa.go.jp/security/security-action/
サイバーセキュリティお助け隊サービス制度	https://www.ipa.go.jp/security/sme/otasuketai-about.html
セキュリティ・キャンプ	https://www.security-camp.or.jp
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 10）。[4]

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。

[4] IPA.”情報セキュリティ白書 2022”. https://www.ipa.go.jp/publish/wp-security/sec-2022.html



第1位：	不正アクセス37.2% （**前年比141.6%**）
第2位：	情報流出25.7% （**前年比135.6%**）
第3位：	改ざん11.1% （**前年比242.9%**）
その他：	26.0% （**前年比129.9%**）

図 10. 情報セキュリティインシデント報道件数

(出典) MBSD 社による集計情報を基に作成

5-1-3. IPA：情報セキュリティ 10 大脅威

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

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

情報セキュリティ 10 大脅威の活用法：組織の検討例	
1.「守るべきもの」の明確化	自社の守るべきものを明確にします。 ● 業務プロセス：取引先との受注業務 ● 情報データ：取引先情報や受注先情報 ● システム、サービス、機器：社内 IT システムとその構成機器 ● その他：取引先との信頼関係など
2. 自社にとっての脅威の抽出	情報セキュリティ 10 大脅威を参考にして自社の守るべきものに対する脅威を抽出します。 脅威が生じた場合の被害額を算出し、会社の経営方針を考慮し、優先順位をつけます。 ● 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

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

（出典）IPA「情報セキュリティ 10 大脅威の活用法 2025」をもとに作成

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ 10 大脅威の活用法［組織編］	https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/katsuyouhou_2025_soshiki.pdf

「情報セキュリティ 10 大脅威 2025」の組織向け脅威（1~10 位）を紹介します。

1 位	**ランサムウェアによる被害** 攻撃者は、PC やサーバー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：RaaS が利用された国内事例（某ソフトウェア開発・支援企業） サーバーの脆弱性および VPN ルーターの設定不備を悪用して、攻撃者が社内ネットワークに侵入し、複数のサーバーに対してデータの暗号化を行いました。10 万件以上の個人情報漏えいの可能性がありましたが、事件から約 2 か月経過しても外部への流出や二次被害は確認されていません。この事例では、RaaS の一種である「Phobos（フォボス）」を用いた攻撃だったことも確認されています。 ※ RaaS（Ransomware as a Service）：サービスとして提供されるランサムウェアを指し、攻撃者は対価を払って利用し攻撃を行う。ランサムウェアの攻撃自体がビジネス化している。
2 位	**サプライチェーンや委託先を狙った攻撃** 商品の企画、開発から、調達、製造、在庫管理、物流、販売までの一連のプロセス、およびこの商流に関わる組織群をサプライチェーンと呼びます。このような

	「ビジネス上の繋がり」を悪用した攻撃は、自組織の対策のみでは防ぐことが難しいため、取引先や委託先も含めたセキュリティ対策が必要な脅威と言えます。 事例：業務委託先業者からの顧客情報漏えい（複数の保険会社） 　原因は委託先業者サーバーへの不正アクセスであり、不正アクセスされたサーバーには適切なセキュリティ対策が施されていなかったことが発覚しました。流出した個人情報は海外の Web サイトに掲載されており、流出の規模は保険会社により異なりますが最大で約 130 万人に及ぶ情報が流出し、調査や対処に追われました。
3 位	**システムの脆弱性を突いた攻撃** 製品開発ベンダー等による脆弱性対策情報の公開は、脆弱性の存在や対策必要性を広く呼び掛けることができるが、攻撃者はその情報を悪用し脆弱性対策が講じられていないシステムを狙って攻撃を行うこと（ゼロデイ攻撃）があります。脆弱性が発見されてから、それを悪用した攻撃が発生するまでの時間が短くなっているため、脆弱性の対策情報が公開された場合には早急な対策の実施が求められます。 事例：Windows 上の PHP の脆弱性を悪用した攻撃 　Windows 上で動作する PHP には既存の脆弱性に対する保護がありますが、この保護を回避できる OS コマンドインジェクション（OS のコマンドを不正に実行させる攻撃）に対する脆弱性が発見され、情報公開がなされました。この公開された脆弱性を悪用し、webshell（Web サーバーの遠隔操作を行える悪意のあるスクリプト）が設置されるといった被害や、ランサムウェア「TellYouThePass」の感染活動に悪用された事例が確認されています。
4 位	**内部不正による情報漏えい等** 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：顧客情報を転職先に持ち出し、営業活動に使用（某保険会社） 元社員が退職時に秘密保持の誓約書に署名していたにもかかわらず、顧客情報（契約者・被保険者）約 980 件を印刷した紙で不正に持ち出し、転職先で一部を使用していました。
5 位	**機密情報等を狙った**標的型攻撃 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：マルウェア感染による情報漏えい（某情報通信企業）

	原因はマルウェアによるものと推測されますが、高度な手法で様々な偽装を行い検知されにくくしてあったため、発見が非常に困難であった事例です。通信ログや操作ログから、個人情報を含むファイルが社外に持ち出されている可能性がありました。
6 位	**リモートワーク等の環境や仕組みを狙った攻撃** リモートワークの実現に必要な環境や仕組みを狙ったサイバー攻撃が多発していいます。攻撃を受けるとマルウェア感染や情報漏えい等、様々な不正アクセスが行われ、組織の事業が停止するなど重大な結果を招くおそれがあります。 事例： VPN 機器を介した個人情報の流失（某エネルギー関連システム子会社） 不正アクセスにより同社の保有する個人情報、約 416 万人分が流出した可能性があると公表されました。攻撃者が社内に設置された VPN 機器から社内ネットワークに侵入していると公表されたものの、侵入のきっかけとなった VPN 機器についての脆弱性有無などについてはセキュリティの関係で公表されませんでした。
7 位	**地政学的リスクに起因するサイバー攻撃** 政治的に対立する周辺国に対して、社会的な混乱を引き起こすことを目的にサイバー攻撃を行う国家が存在します。そのような国家は、自国の産業の競争優位性を確保するために周辺国の機密情報等の窃取を目的とした攻撃や、政治体制維持のために外貨獲得のための攻撃を行うことがあります。このような国家からの攻撃に備えて、組織として常にサイバー攻撃への対策を強化していく必要があります。 事例：日本の個人や組織に対する標的型攻撃 日本の学術機関、シンクタンク、政治家等に関係する個人や組織に対するサイバー攻撃を、海外の国家の関与が疑われるサイバー攻撃グループ MirrorFace が行っていたことを、警察庁および内閣サイバーセキュリティセンターが確認しました。この攻撃では、ANEL と呼ばれるマルウェアをダウンロードするリンクを記載したメールが送信されており、主に日本の安全保障や先端技術に係る情報窃取を目的とした組織的なサイバー攻撃活動であることも公表されています。
8 位	**分散型サービス妨害攻撃（DDoS 攻撃）** 攻撃者に乗っ取られた複数の機器から構成されるネットワーク（ボットネット）から、インターネット上のサービス（サーバー）に対して大量のアクセスを一斉に仕掛けることで高負荷状態にさせる他、回線帯域を占有してサービスを利用不能にする等の分散型サービス妨害攻撃（DDoS 攻撃）が行われています。標的にされたサーバーでは Web サイト等の応答遅延や機能停止が発生するおそれがあります。 事例：某航空会社や複数の金融機関への DDoS 攻撃

	大規模な DDoS 攻撃を受けた航空会社は一部のシステムに障害が発生し、この障害により当日の国内線・国際線のチケット販売が一時停止する等の影響が出ました。また、同時期に複数の金融機関においてインターネットバンキングが利用できない事態も発生し、この原因も DDoS 攻撃によるものでした。 今回の攻撃はいずれも、想定されていないパケットも用いられる混成型 DDoS 攻撃であり、これまでの一般的な対策では止められないものだったことが確認されています。
9 位	ビジネスメール詐欺 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：生成 AI を利用したビジネスメール詐欺 セキュリティ企業である Vipre Security Group は、過去 1 年間に世界中で 18 億通の電子メールを処理し、2 億 2600 万件のスパムメールを検出したと公表しました。検出されたスパムメールの 49%がビジネスメール詐欺（BEC）で、標的は CEO、人事部門と IT 部門の順に多く、その 40%は AI によって生成されていました。生成 AI 技術がより多くの攻撃者に使用されることで、BEC の量は飛躍的に増加するおそれがあると警告しています。
10 位	**不注意による情報漏えい等** 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：教育機関における意図しない個人情報漏えい（複数の公立学校） 教諭が会議で使用するデータを Teams（Microsoft 社の会議ツール）にアップロードしました。約 1 か月後、他校の生徒から共有のアカウントで閲覧可能との指摘があり、そのデータの公開範囲がパブリックであったことが判明しました。別の事象では体力テストアプリのログイン情報一覧が、誰でも閲覧可能な状態となっていることが保護者の指摘で判明しました。学校側と委託業者の双方で、ログイン情報一覧の削除を失念していたことが原因でした。

(出典) IPA「情報セキュリティ 10 大脅威 2025」をもとに作成

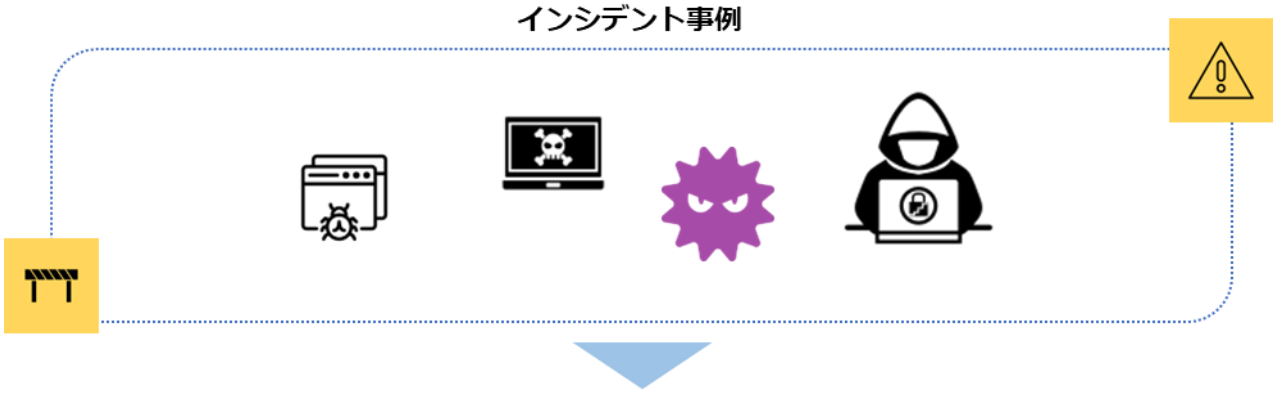
5-2. 重大インシデント事例から学ぶ課題解決

5-2-1. インシデント事例から学ぶ

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

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

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



目的
実際に発生した攻撃事例やセキュリティインシデント事例をケーススタディーとして学ぶこと。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

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

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

IoT デバイスによるサービス被害

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

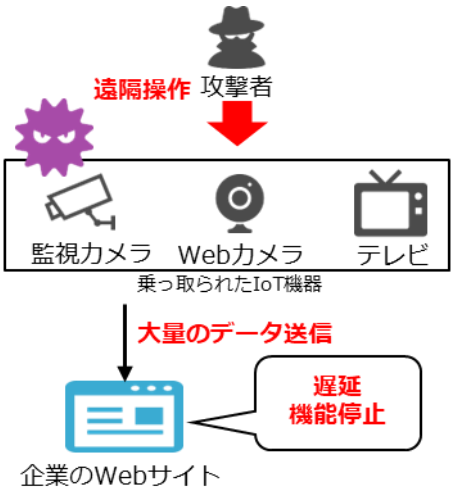


図 11. DDoS 攻撃の概要図

テレワークによるサイバー被害事例

新型コロナウイルスの影響により、テレワークが急速に広まり定着しています。企業では、テレワークを実施するために VPN を利用して社外から社内ネットワークに安全に接続する取組が増えています。しかし、VPN の脆弱性を悪用したサイバー攻撃が確認されています。具体的な事例として、某メーカーのインシデントが挙げられます。同社は、VPN 機器において過去に判明した脆弱性に対処するためのアップデートを実施しました。しかし、アップデート前にパスワード情報が

漏えいしており、当時から存在していたアカウントがパスワードの変更を行っていなかったため、不正アクセスが行われ、ランサムウェアの被害を受ける事例が発生しました。企業は、VPN のセキュリティ対策に十分な注意を払う必要があります。特に、パスワードの管理や定期的なアップデートの実施が重要です。

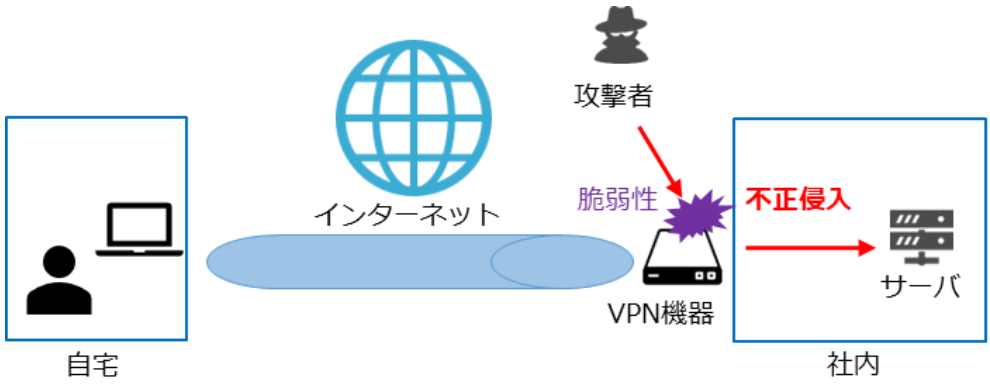


図 12. VPN 機器の脆弱性を利用した攻撃のイメージ

テレワークのセキュリティ対策

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

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

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

5-2-3. 事案発生->課題の抽出->再発防止策の実施までの流れ

インシデントが発生した場合の基本的な対応方法についての紹介となります。図 13 に示すように、3 つのステップで対応します。

図 13. インシデント対応の
3 ステップ

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

防止	復旧： インシデントの修復が確認された後、復旧作業を実施します。システムやデータを正常な状態に戻し、ビジネスの継続性を確保します。復旧作業が完了したら、経営者に報告します。 再発防止策： 同様のインシデントが再発しないよう、再発防止策を立案・実施します。セキュリティの強化や従業員の教育・訓練の強化などを通じて、将来のインシデントを防止するための措置を講じます。

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

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

5-2-4. インシデントから得た気づきと取組

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

サプライチェーンを介した標的型メール攻撃

【事例の概要】

ある企業の工場部門は、取引先企業のメールアカウントが攻撃者に乗っ取られるという被害に遭いました。攻撃者は、取引先企業のフリをして工場部門の担当者に対して、マルウェアが添付されたメールを送信しました。その結果、2 台の端末がマルウェアに感染してしまいました。このマルウェアは、通常の定義型ウイルス対策ソフトウェアでは検知することができませんでしたが、EDR を導入していたことで早期に検知し、感染の拡大を食い止めることができました。[5]

【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。

[5] 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

【対策・予防策】

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

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

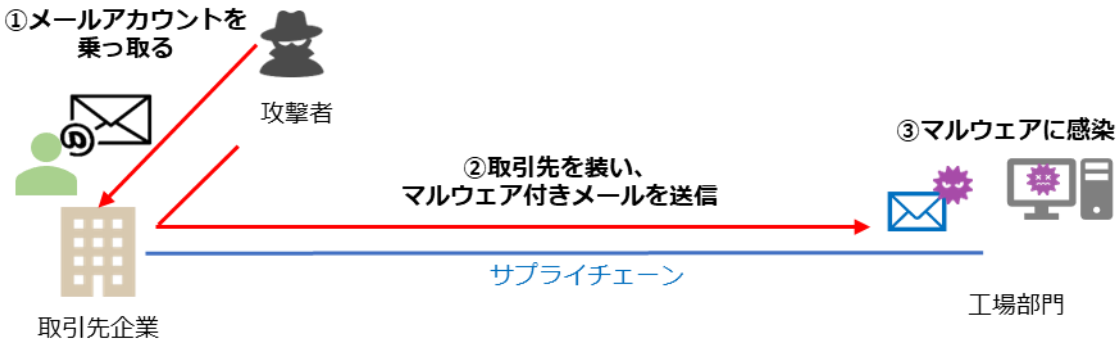


図 14. 攻撃の概要図

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

5-2-5. ランサムウェア感染の実態

ランサムウェアは、PC やサーバー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 6 年における企業や団体の被害件数は合計 222 件であり、被害企業の規模を見ると、大企業が 61 件、中小企業が 140 件、団体などが 21 件でした。ランサムウェアの感染経路については、有効回答 100 件に対して、VPN 機器からの侵入が 55 件、リモートデスクトップからの侵入が 31 件となっています。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 8 割以上の割合を占めました。[6]

[6] 警察庁.”令和 6 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/R6/R06_cyber_jousei.pdf

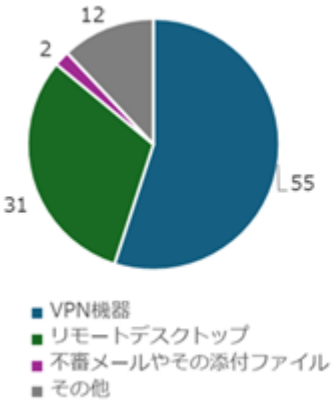


図 15.（令和 6 年）ランサムウェアの感染経路（件数）

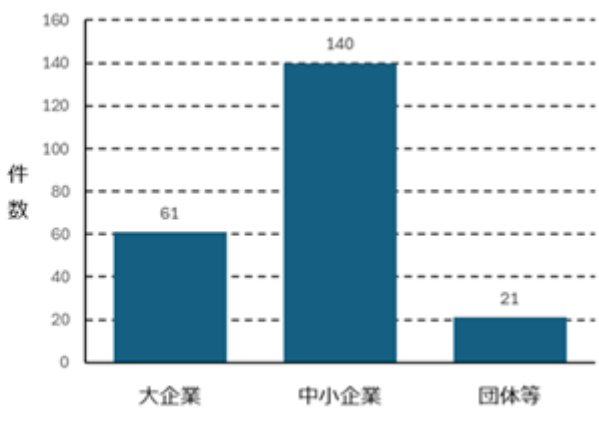


図 16.（令和 6 年）ランサムウェアの被害件数

（出典）警察庁「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について」をもとに作成

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

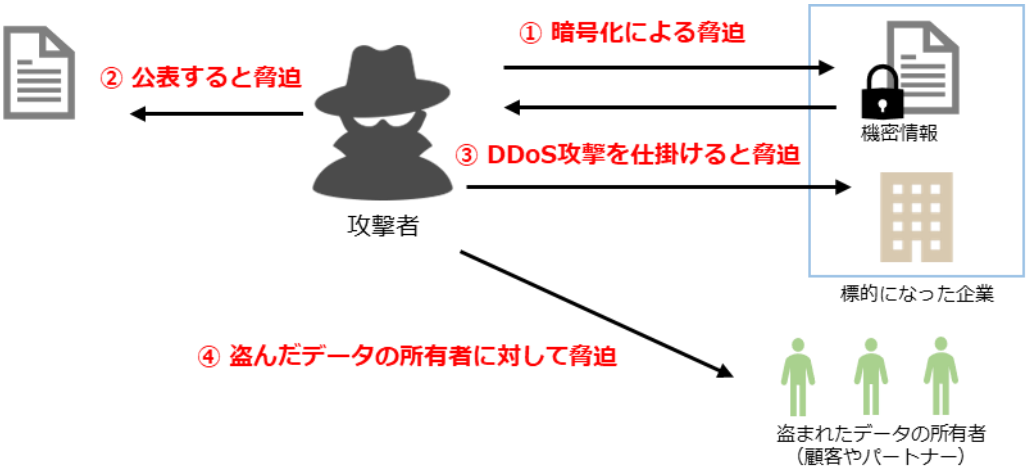


図 17. ランサムウェアの二重、四重脅迫のイメージ図

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

電子カルテシステムでランサム被害（某市民病院）

事例の概要

外部のインターネットから電子カルテシステムのサーバー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。サーバー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

サーバー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 経由で業務サーバーを含む複数のサーバーへ不正侵入されたことです。この結果、個人情報を含むデータが暗号化されてしまいました。

この事例から学べること

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

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

5-3. 実際の被害事例から見るケーススタディー

5-3-1. 最近のサイバー被害事例発生の傾向

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、サーバーや 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。

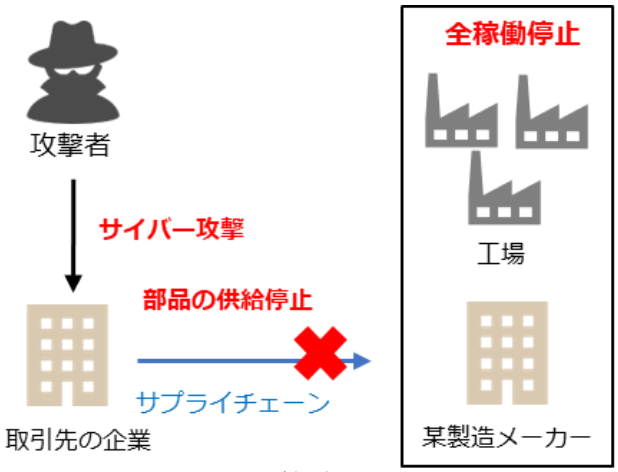


図 18. 攻撃の概要図

5-3-2. 事例：某港のランサムウェア被害

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

ランサムウェアの感染経路として考えられるのは、VPN 機器からの侵入、USB メモリからのウイルスの持ち込み、事業者間のネットワーク連携で運用している NAT 変換による接続からの侵入があります。しかし、サーバー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。物理サーバー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ー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。

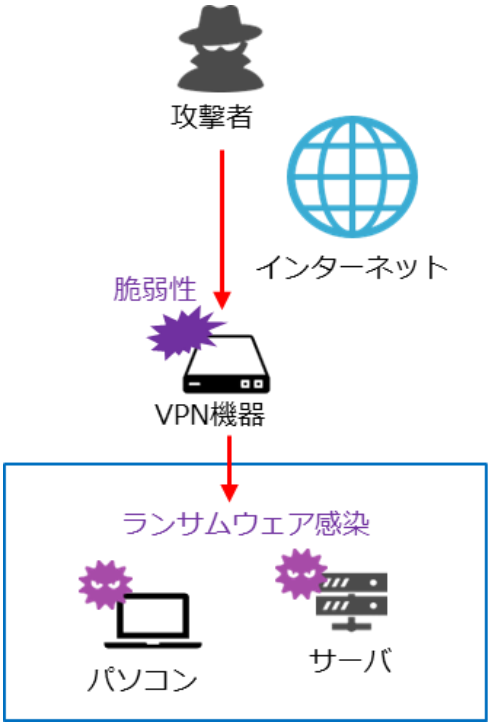


図 19. 攻撃の概要図

問題点

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

教訓

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

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

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

5-3-3. 具体的な対応策

ランサムウェア被害のケースを見ると、VPN 機器から不正侵入され、サーバーの特権 ID を使用してサーバー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 やサーバーからしか重要なサーバーのデスクトップに接続できないような仕組みや、ログの長期保管なども重要な要素となります。

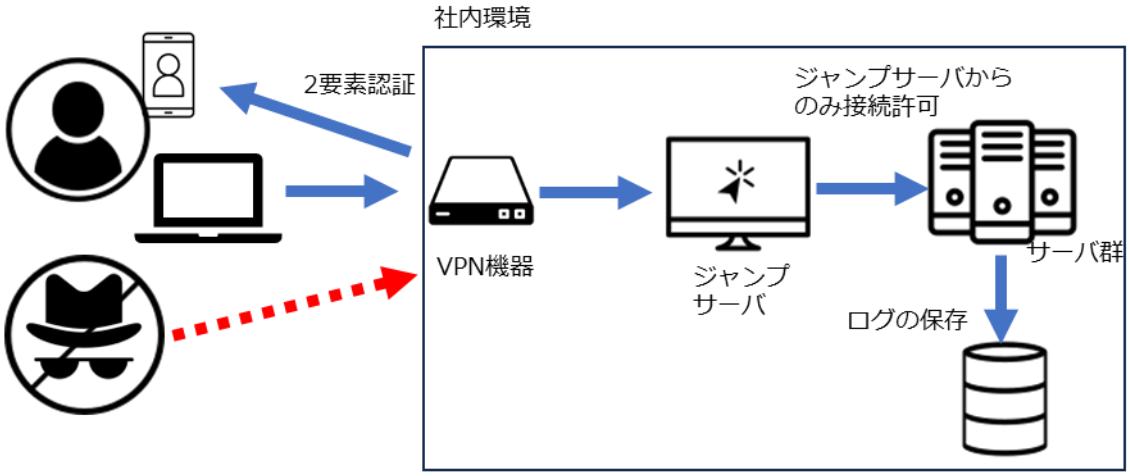


図 20. 対応策の概要図

実施す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、社内のサーバー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。
- サーバー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。
- サーバー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。

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

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

6-1. これからの企業経営で必要な観点：社会の動向

6-1-1. 現実社会とサイバー空間のつながり

日々の生活や企業活動において、IT の活用は広範囲にわたって浸透しています。インターネット利用率（個人）は平成 9 年には 9.2%でしたが、令和 5 年には 86.2%まで上昇しました。急速な IT の普及により、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革変化をもたらしています。

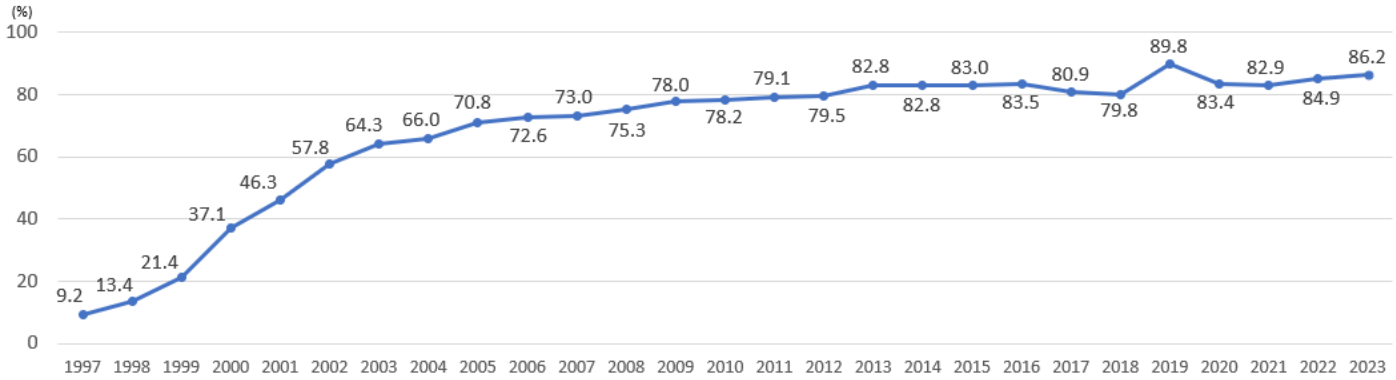


図 21. インターネット利用率（個人）の推移

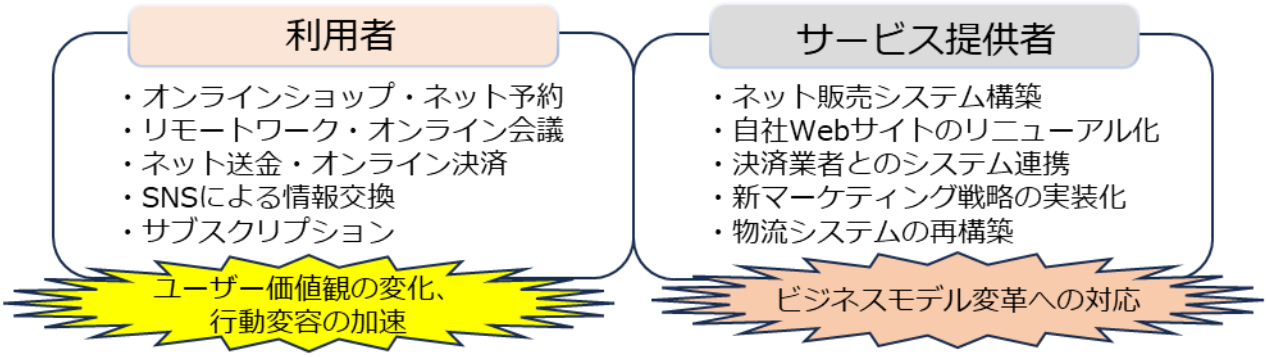
（出典） 総務省「通信利用動向調査」をもとに作成

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

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

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

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



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

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

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

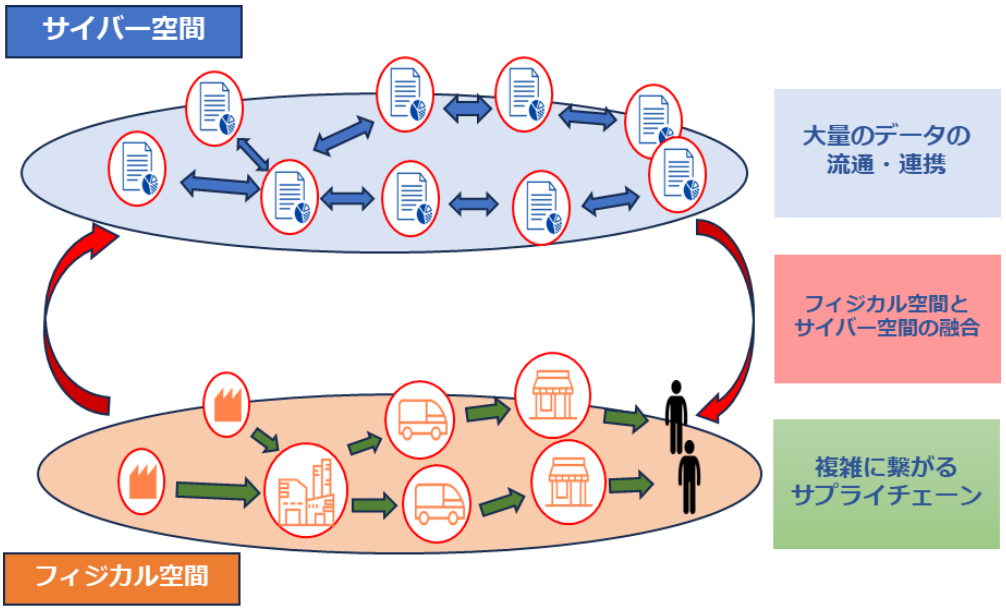


図 22. サイバー空間とフィジカル空間の関係図

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

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

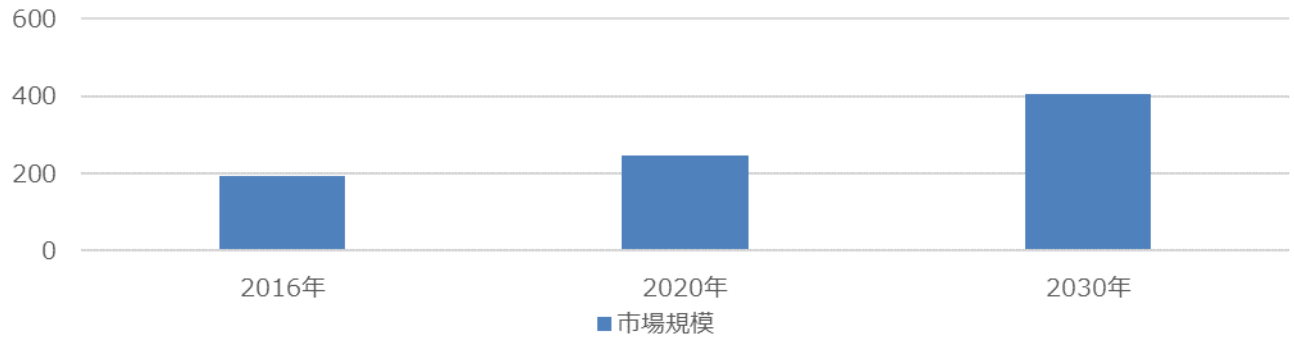


図 23. CPS／IoT の世界市場の推移

（出典） 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。

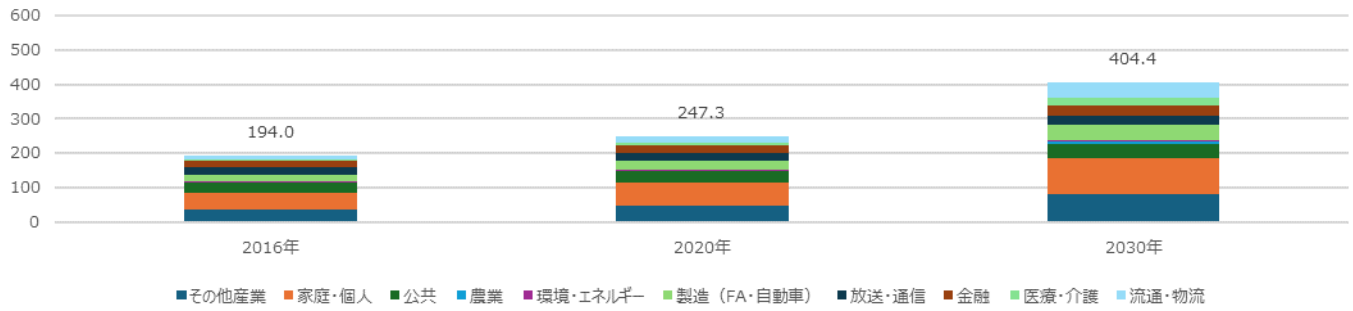


図 24. CPS／IoT の利活用分野別需要額の推移

（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

6-1-2. IT 活用における課題

我が国のデジタル化について、デジタルインフラ整備などの一部については世界的に見ても進んでいるものの、全体としては大幅に後れていると言えます。さまざまな理由が複雑に絡み合い、我が国のデジタル化の後れが生じていると考えられます。[7]

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

[7] 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

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。

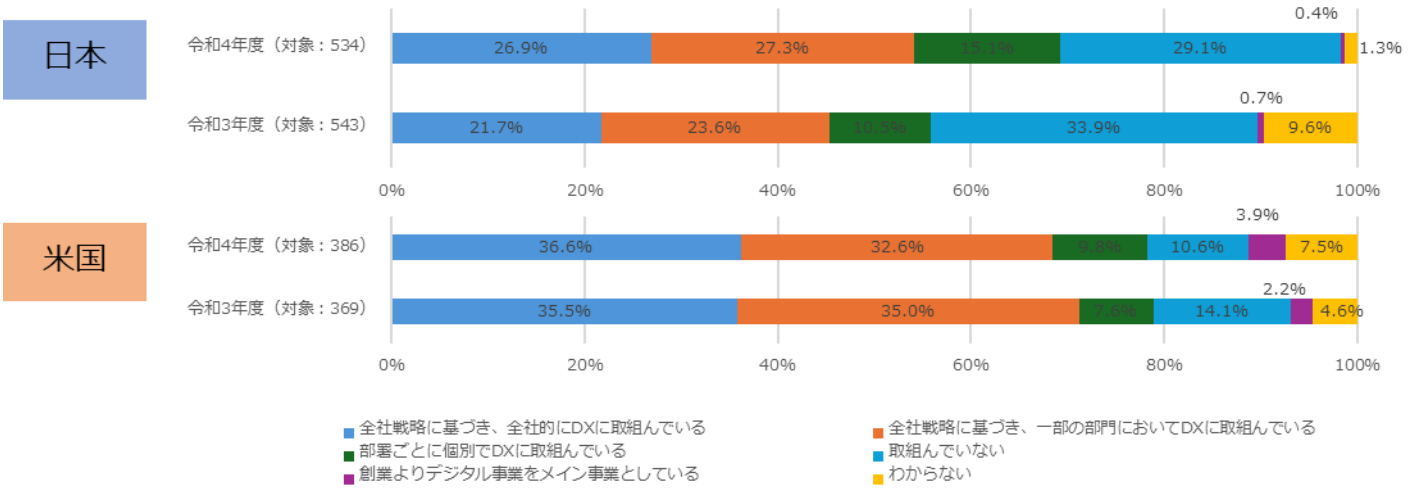


図 25. DX の取組状況

（出典）IPA「DX 白書 2023」をもとに作成

2. DX の取組の成果

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

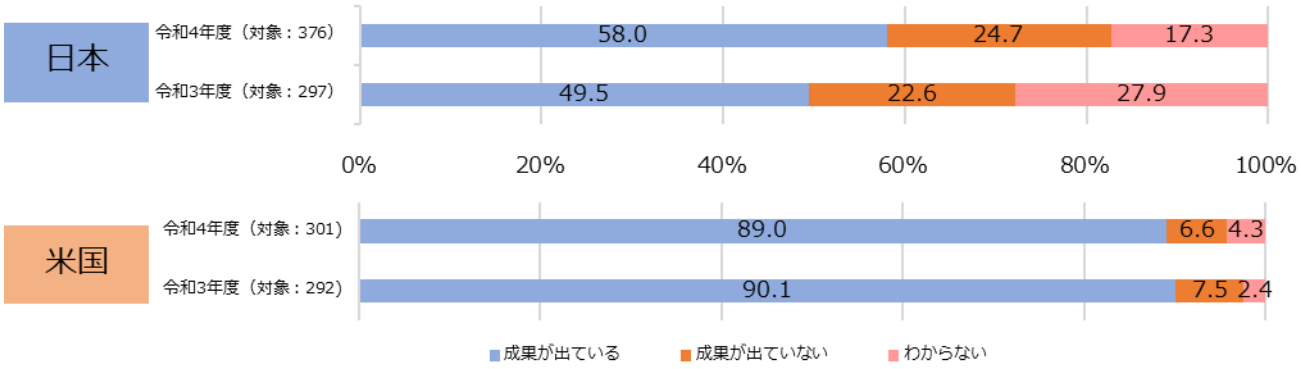


図 26. DX の取組の成果

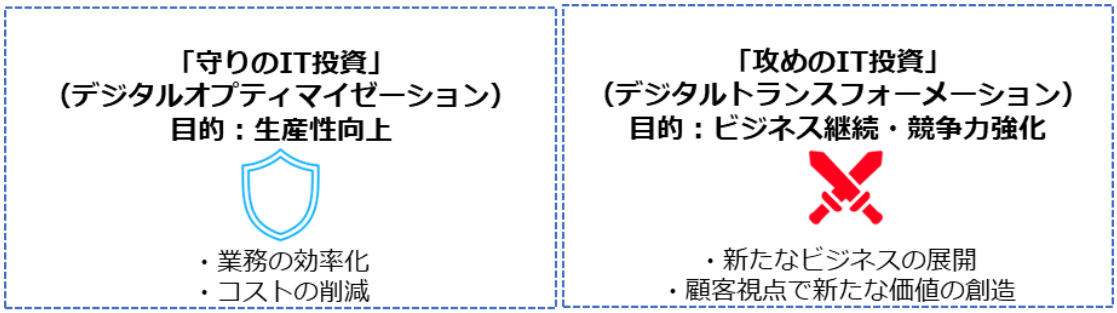
（出典）IPA「DX 白書 2023」をもとに作成

6-2. 守りの IT 投資と攻めの IT 投資

6-2-1. 守りの IT 投資、攻めの IT 投資の概要

企業の IT 投資は、「守り」と「攻め」の 2 種類に分けて論じられることがあります。「守りの IT 投資」とは、IT による業務の効率化やコスト削減を目的としています。一方、「攻めの IT 投資」とは、IT を活用した既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規顧客獲得、収益拡大、販売力のアップを目指すことです。IT 投資に守りと攻めがあることを意識して、両者のバランスをとることが理想です。日本の企業は「守りの IT 投資」に偏っていると言われているので、「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 27. 攻めの IT 活用指針の概要

（出典）経済産業省「攻めの IT 活用指針」をもとに作成

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

2025 年の崖

「2025 年の崖」とは、経済産業省が平成 30 年に発表した「DX レポート～IT システム「2025 年の崖」の克服と DX の本格的な展開～」にて提示されているキーワードです。このレポートでは、令和 7 年は、基幹系システムのサポート終了に伴う維持費の増加や人材不足の深刻化などが集中する年であると予測されています。また、こうした既存の IT システムをめぐる問題を解消しない限りは、DX を本格的に展開することは困難であると指摘しています。さらに、レポートによれば、日本企業が DX を推進できなかった場合の経済的な損失は、年間最大で 12 兆円に上ると算出されています。[8]

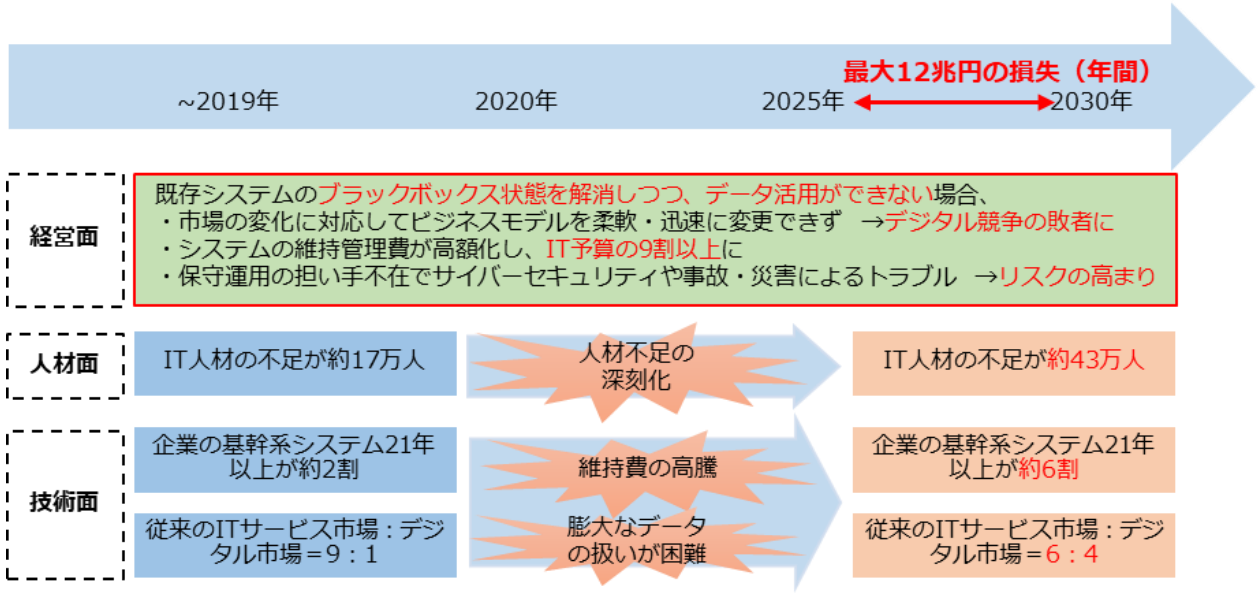


図 28. 「2025 年の崖」の概要図

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

「2025 年の崖」に陥らないための対応策

- 「見える化」指標、診断スキームの構築

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

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

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

「守りの IT 投資」：デジタルオプティマイゼーション

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

必要な理由

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

進め方

手順 1：業務内容・業務フローの可視化
現在の業務プロセスやフローを明確にし、可視化することで全体像を把握します。
手順 2：削減・短縮可能な業務の洗い出し
可視化された業務から、削減や短縮が可能な業務を特定します。

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

事例：某旅館（静岡県・宿泊業・飲食サービス業）

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

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

業務フローの可視化
清掃業務内容の洗い出し

目標
①能力の見える化
②清掃スキルの継承
③最新状況の共有

対応の実施
- 労働投入量のデータ
- 測定動画によるマニュアル化
- チャットツールの活用

結果
- 清掃時間を削減
- 接客の質の向上
- お客様満足度向上

図 29. 業務改革の流れ

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

6-2-4. IT を活用した新たなビジネスの展開（DX）

「攻めの IT 投資」：DX

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

必要な理由

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

進め方

手順 1：経営ビジョン・戦略の策定
デジタル技術によって市場や顧客のニーズがどのように変化する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。

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。

実現したこと
付加価値が高い「産地細分化ワイン」を増産・安定供給すること

課題
アナログ作業（口頭伝達、手書き記帳など）の改善

対策
「ブドウ受入演算システム」を構築

結果
産地細分化ワインの増産・安定供給実現

図 30. 業務改革の流れ

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

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

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

6-2-5. 次世代技術を活用したビジネス展開

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

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

デジタル技術は手段であり、導入自体が目的ではない

AI、IoT など最新のデジタル技術を用いて、何かできないかな？

自社の課題を解決するためには、このデジタル技術を活用する必要がある。

項目	概要	活用方法例
AI	AI は膨大な情報を処理し、判断や予測を行うことができます。	● 需要の予測や在庫の最適化 ● 不良品の自動検出 ● 対話型 AI による、問い合わせ対応の自動化（近年、学習したデータをもとに新しいコンテンツを生成できる AI の登場により、複雑な問い合わせにも対応可能）
IoT	現実世界のさまざまなモノが、インターネットとつながることです。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）

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

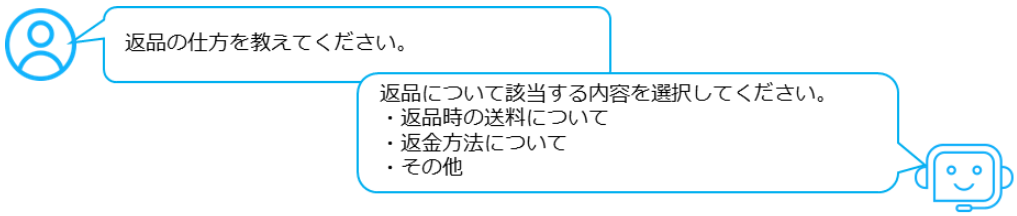
（出典） 経済産業省 「DX Selection 2024」をもとに作成

事例 2：観光客向け飲食、販売業（三重県・飲食・サービス業）

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

チャットボット

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



予想・今後の発展

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

生成 AI の登場

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

生成AIの活用事例

文章生成

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

レポート作成

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

製品開発と設計

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

（出典） 経済産業省 「DX Selection 2024」をもとに作成

6-3. 経営投資としてのサイバーセキュリティ対策

6-3-1. サイバーセキュリティ対策の重要性

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

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

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

図 31. IT の活用とサイバーセキュリティ対策の関係性

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

6-3-2. 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ーが不正アクセスを受けたことです。顧客の氏名、性別、生年月日、メールアドレスなどの個人情報が数十万人分漏えいしてしまいました。その結果、数億円以上の損害や多くのお客様に対する信頼を低下させてしまう事態となりました。このようにサプライチェーンを介した攻撃では、自社が直接サイバー攻撃を受けていなくても、間接的に被害にあってしまいます。

ポイント 3：サイバーセキュリティ対策は経営者が自ら実行

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

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

図 32. 情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律
（出典）IPA「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」から抜粋

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/dgc2.pdf
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
「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 [組織編]
https://www.ipa.go.jp/security/10threats/eid2eo0000005231-att/katsuyouhou_2025_soshiki.pdf
中小企業のためのセキュリティインシデント対応の手引き
https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
【NISC】サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）
https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
令和6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/R6/R06_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
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
IPA 情報セキュリティ白書 2022
https://www.ipa.go.jp/publish/wp-security/sec-2022.html
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
総務省　通信利用動向調査
https://www.soumu.go.jp/johotsusintokei/statistics/data/240607_1.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 2024
https://www.ipa.go.jp/publish/wp-security/eid2eo0000007gv4-att/2024_ALL.pdf
情報セキュリティ10大脅威 2025（組織編）
https://www.ipa.go.jp/security/10threats/10threats2025.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
サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ
https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html
目的や所属・役割から選ぶ施策一覧
https://security-portal.nisc.go.jp/curriculum/
サイバーセキュリティ関係法令Q&Aハンドブックポータルサイト
https://security-portal.nisc.go.jp/guidance/law_handbook.html
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
サイバーセキュリティ関係法令Q&AハンドブックVer2.0　誤記修正箇所
https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/seigo.pdf
中小企業等担当者向け テレワークセキュリティの手引き 第3版
https://www.soumu.go.jp/main_content/000816096.pdf
中小企業のためのセキュリティインシデント対応の手引き
https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf

■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。

0-1-1、0-1-2、1-1、3-1、3-2-1、3-2-2、3-2-3、4-2-1、5-1-3、6-1-1、6-2-5

■CSIRT（シーサート）

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

4-1-1、5-1-3

■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。

2章コラム、5-1-3、5-2-2、5-2-5

■DFFT

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

3-2-1

■EDR（イーディーアール）

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

2-1、5-2-4、5-2-5

■eKYC（イーケイワイシー）

electronic Know Your Customerの略で、オンライン上で本人確認を完結させる仕組みのこと。従来、金融機関やその他のサービスで必要だった本人確認書類の郵送や窓口での手続きを、インターネット上で行うことを指す。

3-2-1

■G ビズ ID

すべての事業者を対象とした共通認証システム。1つのID・パスワードで、複数の行政サービス にログインでき、補助金申請、社会保険手続、各種認可申請など業務上の電子届出や申請に使用できる。ID発行時に一度だけ代表者の身元確認を行えば、その後の各手続での本人確認書類提出が不要になる。

3-2-1

■ICSCoE 中核人材育成プログラム

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

5-1-2

■ICT

Information and Communication Technologyの略。IT（情報技術）に加えて、コンピュータやスマ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。

3-2-1、6-1-2

■IoT（アイオーティー）

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

1-1、3-1、3-2-3、3-2-4、4-2-1、4-3-3、5-2-2、6-1-1、6-2-5

■IPS（アイピーエス）

Intrusion Prevention System（不正侵入防止システム）の略で、ネットワークやサーバーへの不正アクセスをリアルタイムで検知し、遮断するセキュリティシステム。ネットワーク型とホスト型がある。

5-2-2

■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。

5-3-2

■ISMS

Information Security Management System の略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的なセキュリティ対策を含む、経営者を頂点とした総合的で組織的な取り組み。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。

0-1-2、2-3

■NISC（ニスク）

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

2-3、3-2-1、4-1、4-1-1、4-1-2

■NIST サイバーセキュリティフレームワーク（CSF）

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

2-3

■RPA（アールピーエー）

Robotic Process Automation の略称。人間がPCを用いて日常的に行う一連の作業を、AIなどの技術を活用して自動化するソフトウェアロボットを指す。人手を介さず高速かつ正確に事務作業が実行できるため、生産性向上や人手不足の解消といったメリットがある。

6-2-5

■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。

5-2-4

■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。

5-2-5

■SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度。

2-2-1、4章編集後記、5-1-2

■Society 5.0

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。

1章、1-1、3-2-3、4-1-1、6-1-1

■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。

5-2-4

■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。

5-1-3、5-2-2、5-2-5、5-3-1、5-3-2、5-3-3

■WAF（Web アプリケーションファイアウォール）

Web Application Firewallの略で、「Webアプリケーションの脆弱性を悪用した攻撃」からWebサイトを保護するセキュリティ対策。Webサーバーの前段に設置して通信を解析・検査し、攻撃と判断した通信を遮断することで、Webサイトを保護する。

5-2-2

■アクセス制御

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

2章コラム、2-3、5-2-5

■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。

5-2-4

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること。

2-2-3、2-3、2章コラム、5-1-3、5-2-1、5-3-2

■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。

2-2-2、5-1-3

■ウイルス定義ファイル（パターンファイル）

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

2-1、2-2-2、2-2-3

■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、サーバーなど）

5-2-4

■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。

3-2-3、4-1-1、4-2-2

■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。

2章コラム

■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。

2章コラム

■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。

2章コラム

■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・サーバー攻撃・情報システムの破壊などを行うこと。

2章コラム

■個人情報保護委員会

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

3-2-1、4-3-1、5-2-3

■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、企業のサーバーやデータベース、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。

0-1-1、0-1-2、0-1-3、2-1、2-3、3-2-3、3-2-4、4-1-1、4-1-2、4-2-1、4-2-2、5章、5-1-2、5-1-3、5-2-2、5-2-5、5-3-1、5-3-2、6-3-1、6-3-2、2編-編集後記

■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において中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている。

5-1-2

■サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ。

2-3、3-1、4章、4-1-1、4-1-2

■サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

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

2-3

■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。

0-1-1、2-2-1、3-2-3、4-1-1、4-1-2、4-2-1、4-2-2、5-

1-3、5-2-4、5-3-1、6-1-1、6-2-4、6-3-2、２編-編集後記

■情報資産

企業や組織などが所有している情報全般のこと。情報資産には顧客情報や販売情報などの情報自体に加え、ファイルやデータベースといったデータ、CD-ROMやUSBメモリなどの記録メディア、紙媒体の資料も含まれる。

2-2-4、2-3

■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。

2章コラム

■真正性

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

2章コラム、4-2-2

■信頼性

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

1-1、2-2-3、2章コラム、3-2-1、4-1-1、4-2-2

■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。

5-2-2

■脆弱性

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

2-1、2-3、2章コラム、5-1-2、5-1-3、5-2-1、5-2-2、5-2-4、5-2-5、5-3-1、5-3-2、5-3-3

■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。

2章コラム

■セキュリティインシデント

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

2-1、5-1-1、5-1-2、5-1-3、5-2-1、6-3-2

■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。

5-1-2

■セキュリティホール

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

2-3

■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。

2-3、4-2-1、5-1-1、5-2-1

■ゼロデイ攻撃

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

5-1-3

■ゼロトラスト

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

5-2-4

■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。

5-2-5、5-3-3

■データサイエンス

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

1-1

■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。

0-1-1、1-1、3-1、3-2-1、4-1-1、4-2-2、5-1-2、6-1-2、6-2-4

■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。

2章コラム

■トラフィック

通信回線やネットワーク上で送受信される信号やデータのことやその量や密度のことを表す。もともとは交通量、通行量などの意味を持つ英単語である。

2-1

■内部監査

組織内部の独立した部門が、組織の業務が適切かつ効率的に行われているかを評価し、改善を促す活動。不正行為の防止や業務効率の向上、経営目標の達成を支援することを目的とする。

2-3

■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。

5-1-3

■ビッグデータ

全体を把握することが困難な程膨大な規模のデータ群。

1-1、3-2-3、3-2-4

■否認防止

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。

2章コラム

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（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。

5-1-2、5-1-3

■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。

5-2-4

■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。

2-1、5-2-2

■不正アクセス

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

3-2-1、4-3-3、5-1-1、5-1-3、5-2-1、5-2-2、5-2-3、5-2-5、5-3-1、6-3-2

■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。

5-1-3

■フォレンジック

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

5-2-3

■フレームワーク

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

0-1-2、2-3、4-1-1、5-2-4

■ブロックチェーン

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

1-1

■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。

5-1-3、5-3-1

■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。

2-1、2章コラム、5-1-3、5-2-2、5-2-4、5-2-5

■ミラサポコネクト

中小企業支援コミュニティの活性化に向けて、補助金や認定計画等のデータを蓄積したデータベース。

3-2-1

■無線 LAN

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

2-2-3

■ランサムウェア

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

0-1-1、2-1、5-1-2、5-1-3、5-2-1、5-2-2、5-2-5、5-3-2、5-3-3

■リスクアセスメント

組織に存在するリスクを認識し、リスクの大きさの評価を行い、そのリスクが許容できるかどうかを決定するプロセスを指す。リスク対応を行うときの優先度の根拠となるリスクレベルを決定する活動である。

2-3

■リスク評価

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

2-3、5-3-2

■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。

5-2-2、5-2-5、5-3-3

東京都産業労働局