


令和5年度 中小企業サイバーセキュリティ対策 継続支援事業

**サイバーセキュリティを取り巻く環境および
中小企業に求められるサイバーセキュリティ対策**



**サイバーセキュリティ
人材育成
社内体制整備支援**

目次

はじめに

第1章. デジタル時代の社会とIT情勢

1-1. デジタル時代の社会変革とIT情勢の関係性

1-1-1. 社会の現状と今後の動向

第2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

2-1. 情報セキュリティの概況

2-1-1. 情報セキュリティの脅威を学ぶ

2-1-2. IPA：情報セキュリティ白書から見る脅威

2-1-3. IPA：情報セキュリティ10大脅威

2-2. 重大インシデント事例から学ぶ課題解決

2-2-1. インシデント事例から学ぶ

2-2-2. 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

2-2-3. 事案発生->課題の抽出->再発防止策の実施までの流れ

2-2-4. インシデントから得た気付きと取組み

2-2-5. ランサムウェア感染の実態

2-3. 実際の被害事例からみるケーススタディ

2-3-1. 最近のサイバー被害事例発生の傾向

2-3-2. 事例：徳島県の某病院

2-3-3. 具体的な対応策

第3章. サイバーセキュリティの基礎知識

3-1. 導入済と想定するセキュリティ対策機能

3-1-1. UTM、EDRの概要

3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

3-2-1. 情報処理技術者向け国家試験体系

3-3. Security Action（セキュリティ対策自己宣言）

3-3-1. Security Action 二つ星レベル

3-3-2. 情報セキュリティ5か条

3-3-3. 情報セキュリティ自社診断

3-3-4. 情報セキュリティ基本方針

3-4. サイバーセキュリティアプローチ方法

3-4-1. サイバーセキュリティアプローチ方法の概要

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

編集後記

引用文献・参考文献・用語集

はじめに

新型コロナウイルス感染症の蔓延の影響もあり、社会経済のデジタル化が急速に進行しました。サイバーセキュリティ対策はデジタル化に不可欠なものです。特に中小企業においては、十分な対策が講じられていない状況にあります。このため、東京都ではサイバーセキュリティ対策の普及啓発活動に加え、セキュリティ機器の設置等を進めています。中小企業において、継続的なサイバーセキュリティ対策を実現するには、人材やノウハウの面でリソースが不足しているという大きな課題があります。この課題解決のため、サイバーセキュリティ人材の育成支援や実践的な課題解決を通じて、セキュリティ対策の継続性を確保し、サプライチェーンのセキュリティ対策に役立つテキストを作成しました。

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、包括的なサイバーセキュリティ対策に役立つ情報を提供します。現代のビジネス環境では、サイバー攻撃が日々進化し、企業の資産や顧客情報、信頼性が危険にさらされています。本テキストでは、その重要性を明確にし、対策の方法論を解説します。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み、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体制の構築や認証取得に向けた手順を解説します。

最後に、本テキストでは、実際のセキュリティ対策の実施手順を具体的に解説します。リスクアセスメントから対策計画の策定、セキュリティ運用や監視の手順まで、段階的なアプローチで実践的な知識体系を提供します。

第1章. デジタル時代の社会とIT情勢

1-1. デジタル時代の社会変革とIT情勢の関係性

第1章. デジタル時代の社会とIT情勢

1-1. デジタル時代の社会変革とIT情勢の関係性

1-1-1. 社会の現状と今後の動向

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、様々な利点をもたらします。また、大企業と比べ人手や予算等の企業リソースが限定されている中小企業こそ、新たなサービスを創造し、ビジネスを発展させるために、DXを推進することが重要です。

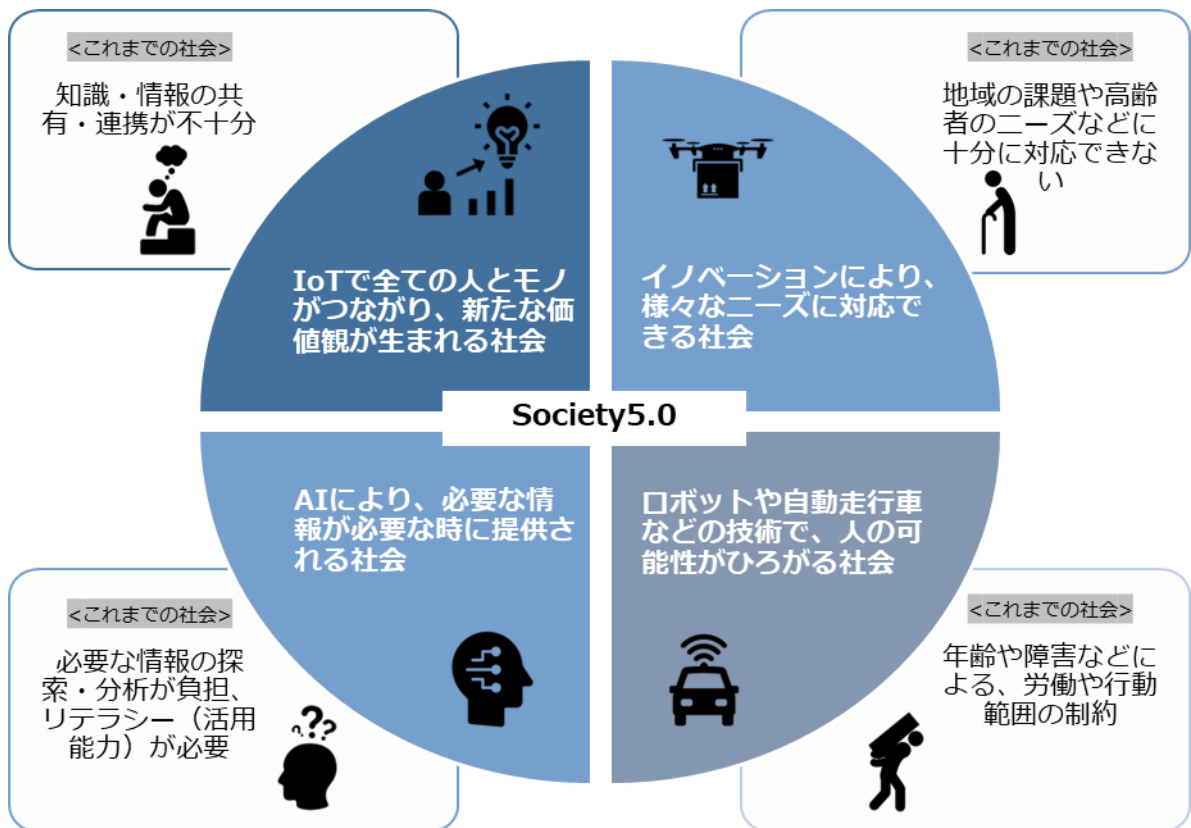


図1. Society5.0の概要図
 (出典) 内閣府. "Society5.0". https://www8.cao.go.jp/cstp/society5_0/, (2023-06-30).

第1章. デジタル時代の社会とIT情勢

1-1. デジタル時代の社会変革とIT情勢の関係性

1-1-1. 社会の現状と今後の動向

デジタルトランスフォーメーション（DX）とは

ここでは、DX（デジタルトランスフォーメーション）の定義を紹介し、DXの概要を説明します。

DXの定義

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

DXの概要

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

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

DXを進めるにあたり必要な3要素

知識

ITの基礎知識の他、ビッグデータ等を活用するためのデータサイエンスの知識やAI・ブロックチェーン等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等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, (2023-07-06).

第2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

2-1. 情報セキュリティの概況

2-2. 重大インシデント事例から学ぶ課題解決

2-3. 実際の被害事例からみるケーススタディ

第2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

2-1. 情報セキュリティの概況

2-1-1. 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。現代の情報技術の進歩により、私たちの生活はますますデジタル化されており、情報の安全保障は社会の安定と発展を支える要素となっています。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様々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のレベルを向上させるのにも有効で、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が向上します。

どのような脅威があるかは、情報処理推進機構（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説明しています。そして、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対策等を紹介しています。

脅威情報



目的

脅威情報を把握することで、攻撃の傾向や手法、そして最新の脆弱性情報からセキュリティリスクを把握し、適切な予防策や対策を講じること

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2022

<https://www.ipa.go.jp/publish/wp-security/sec-2022.html>

情報セキュリティ10大脅威 2023

<https://www.ipa.go.jp/security/10threats/10threats2023.html>

第2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
2-1. 情報セキュリティの概況

2-1-2. 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現状や課題、脅威、対策について包括的な情報を提供することを目的として、独立行政法人情報処理推進機構（IPA）によって、2008年から毎年発行されています。

2022年7月に刊行された「情報セキュリティ白書2022」は、2021年までのサイバー攻撃による実際の被害や対策等、情報を守るための最新情報をまとめており、対象は情報セキュリティの専門家、企業、行政機関を想定しています。



図2. 情報セキュリティ白書2022
(出典) IPA. “情報セキュリティ白書2022”. <https://www.ipa.go.jp/publish/wp-security/sec-2022.html>, (2023-06-30).

情報セキュリティ白書の記載内容

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

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等の事例、手口や対策方法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等の活動を知り、自社で取組む

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

第2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

2-1. 情報セキュリティの概況

2-1-2. IPA：情報セキュリティ白書から見る脅威

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

企業、組織への信頼性低下



重要データの漏えい、改ざん等により、顧客との信頼関係の損失。

サービスの中断



業務やサービスが一時的または永続的に中断。

経済的損失



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

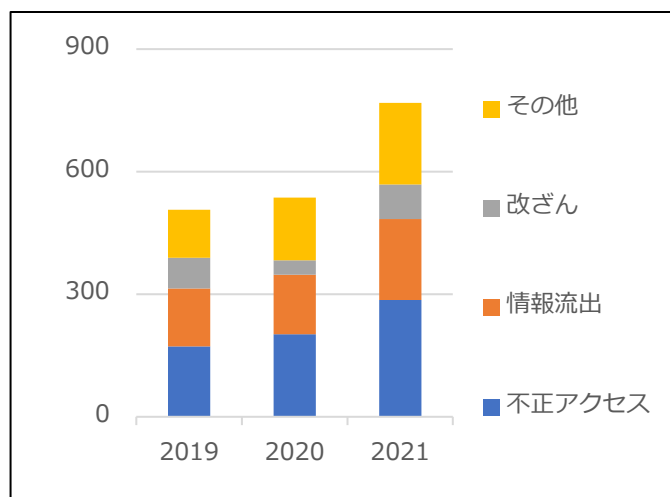
法的な制裁



セキュリティ対策が不十分な場合、関連する法的規制や規範に違反

情報セキュリティ白書では、1年間のインシデント状況を紹介しています。それによると情報セキュリティの脅威は年々増加しており、2021年の情報セキュリティインシデント報道件数は769件となり、前年比で43.2%増加しました（図3）。^[2]

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。



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3. 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

[2]:IPA.“情報セキュリティ白書2022”. <https://www.ipa.go.jp/publish/wp-security/sec-2022.html>, (2023-07-06).

第2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

2-1. 情報セキュリティの概況

2-1-3. 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、情報セキュリティ専門家を中心に作成された資料です。情報セキュリティの研究者と実務担当者が、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元に脅威を抽出し、審議・投票によって「個人」と「組織」に分けて、10個の脅威が選定されています。^[3]

10大脅威を活用することで、どのようなこと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。1年間の状況を反映して作成され、テレワークに関連した脅威や注目を集めた脅威についてのサイバー攻撃事例や対策が紹介されています。これらを有効活用して、自社のセキュリティ対策に役立てます。

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	<p>自社にとっての守るべきものを明確にします。</p> <ul style="list-style-type: none"> ・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等
2. 自社にとっての脅威の抽出	<p>10大脅威を参考にし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、優先順位を付けます。</p> <ul style="list-style-type: none"> ・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	<p>自社にとっての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。</p> <ul style="list-style-type: none"> ・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等 ・被害の早期検知：システムの操作履歴の監視等 ・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、復号ツールの活用等
4. 実施する対策の選定	<p>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。</p> <ol style="list-style-type: none"> ①実施状況を確認（実施済み、一部実施、要調査等） 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」を基に作成

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





https://www.ipa.go.jp/security/10threats/ps6vr7000009r2t-att/katsuyouhou_2023.pdf

[3]:IPA.“情報セキュリティ10大脅威 2023”. https://www.ipa.go.jp/security/10threats/ps6vr7000009r2f-att/kaisetsu_2023.pdf, (2023-07-06).

第2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

2-1. 情報セキュリティの概況

2-1-3. IPA：情報セキュリティ10大脅威

<p>1位</p>	<p>ランサムウェアによる被害 情報が暗号化され、復旧と引き換えに金銭を要求されます。また金銭を支払わなければ、情報を公開すると脅迫する二重脅迫も確認されています。 事例：攻撃者はWebサービス上にランサムウェアを自動的に配布するファイルを配置し、自動更新時にファイルを実行させることで、ランサムウェア感染を引き起こしました。（2021年年末）^[4]</p>	
<p>2位</p>	<p>サプライチェーンの弱点を悪用した攻撃 直接攻撃が困難な大企業に対し、セキュリティレベルが低い取引先や子会社を攻撃し、踏み台にして標的に侵入する攻撃です。 事例：某自動車メーカーが取引先のシステム障害により国内全工場を停止しました。（2022年3月）^[5]</p>	
<p>3位</p>	<p>標的型攻撃による機密情報の窃取 特定の企業を標的にし、業務関連のメールを装ったウイルス付きメールを送りつけることで行われます。受信者がメールを開くと、PCやサーバに感染が広がります。そして、攻撃者は組織内部に潜入し、機密情報を窃取する等の活動を行います。 事例：某和菓子メーカーは、他社の社員を装ったメールに添付されたWordファイルを開き、「編集を有効にする」をクリックし、ウイルスに感染しました。（2020年9月）^[6]</p>	
<p>4位</p>	<p>内部不正による情報漏えい 企業の従業員や元従業員等が、会社で保管する情報を不正に持ち出し、外部に公開したり、競合他社へ情報提供したりすることで情報が漏えいすることがあります。 事例：住宅販売を手がける某工務店は、元従業員が同社顧客情報を不正に持ち出し、転職先に提供していたことを明らかにしました。（2023年3月）^[7]</p>	
<p>5位</p>	<p>テレワーク等のニューノーマルな働き方を狙った攻撃 Web会議を覗き見されたり、テレワーク用の端末にウイルスを感染させられたり、VPNの脆弱性を悪用して不正アクセスされ、情報を搾取されるおそれがあります。 事例：某自動車部品メーカーは、テレワークの負荷により過去に利用したVPN機器を再度稼働させたところ、未修正の脆弱性が存在しており、IDとパスワードが窃取されました。（2020年8月）^[8]</p>	

(出典) IPA「情報セキュリティ10大脅威」を基に作成

[4]:株式会社ヴィアックス.“動怠管理システムサーバに対する攻撃について”.<https://www.viax.co.jp/pdf/20220601.pdf>, (2023-07-06).

[5]:小島プレス工業株式会社.“ウイルス感染被害によるシステム停止事業発生のお知らせ”.<https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/ウイルス感染被害によるシステム停止事業発生のお知らせ-2.pdf>, (2023-07-06).

[6]:亀屋良長.“弊社を装った不正メールが届いた際のご対応方法のお知らせ”.<https://kameya-yoshinaga.com/f/single?p=1848>, (2023-07-06).






[7]:アイ工務店.“お客様情報の流出に関するお詫びとご報告”.<https://www.ai-kouruten.co.jp/topics/news/37241/>, (2023-07-06).

[8]:平田機工株式会社.“情報セキュリティインシデントについて”.https://www.hirata.co.jp/files/optionallink/ns_20200825.pdf, (2023-07-06).

第2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

2-1. 情報セキュリティの概況

2-1-3. IPA：情報セキュリティ10大脅威

6位	<p>修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） ソフトウェアに脆弱性が存在することが判明し、脆弱性の修正プログラムがベンダーから提供される前に、その脆弱性を悪用してサイバー攻撃されることがあります。 事例：Microsoftは、Microsoft Edgeのゼロデイ脆弱性を解消するアップデートを準備しており、それまで影響を軽減する機能の活用を呼びかけています。（2023年6月）^[9]</p>	
7位	<p>ビジネスメール詐欺による金銭被害 従業員のメールアドレスを乗っ取り、取引実績がある組織の担当者へ偽の請求等を送りつけ、攻撃者の用意した口座に金銭を振込ませるような攻撃です。 事例：国内企業と海外取引先企業の間で行われるやり取りにおいて、攻撃者が取引先を装い、銀行口座証明書を偽造し、書類の真正性に気付かずに誤って偽造口座へ送金した事案が発生しました。（2021年3月）^[10]</p>	
8位	<p>脆弱性対策情報の公開に伴う悪用増加 ベンダーが脆弱性対策情報の公開をして利用者に広く呼びかける際、攻撃者がその情報を悪用し、当該製品へ脆弱性対策を講じていないシステムを狙って攻撃を行うことがあります。 事例：給食委託業者は、VPN機器の公開された修正プログラムを更新しなかったため、ランサムウェアによるサイバー攻撃を受けました。（2022年10月）^[11]</p>	
9位	<p>不注意による情報漏えい等の被害 メールの誤送信、記録端末や記録媒体の紛失等、従業員のセキュリティ意識の低さ、不注意によるミス等によって重要情報を漏えいすることがあります。 事例：某新聞社は、メールマガジンの送信時にミスがあり、登録者のメールアドレスが流出しました。（2023年5月）^[12]</p>	
10位	<p>犯罪のビジネス化（アンダーグラウンドサービス） 企業から不正に窃取した情報が、ブラックマーケットで売買され悪用されています。認証情報を入手し、企業のWebサービス等に不正ログインされることがあります。 事例：某パチンコホール経営企業はサイバー攻撃を受け、その後、口座情報を含む一部の個人情報ダークウェブ上で公開されたことが判明しました。（2022年9月）^[13]</p>	

(出典) IPA「情報セキュリティ10大脅威」を基に作成

[9]:Microsoft." Microsoft Edge セキュリティ更新プログラムのリリースノート". <https://learn.microsoft.com/ja-jp/deployedge/microsoft-edge-relnotes-security>, (2023-07-06).[10]:IPA."ビジネスメール詐欺（BEC）の詳細事例2～銀行口座証明書類を偽造し振込先口座変更を依頼してきた事例". <https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000103087.pdf>, (2023-07-06).[11]:大阪急性期・総合医療センター."情報セキュリティインシデント調査委員会報告書について". <https://www.gh.opho.jp/important/785.html>, (2023-07-06).[12]:産経新聞社."メールアドレス漏えいのお詫び". https://www.sankei.jp/wp-content/uploads/2023/05/メールアドレス漏えいのお詫び_20230510.pdf, (2023-07-06).[13]:株式会社ダイナムジャパンホールディングス."当社サバーへの不正アクセスについて（第3報）". https://www.dyjh.co.jp/news/pdf/221101_dyjh.pdf, (2023-07-06).

第2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

2-2. 重大インシデント事例から学ぶ課題解決

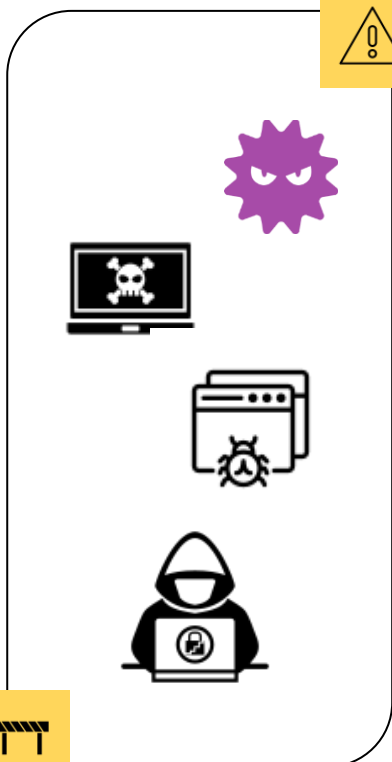
2-2-1. インシデント事例から学ぶ

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、何がうまく行かなかったのか、どのような手段が用いられたのか、どのような脆弱性が攻撃の対象となったのか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。

インシデント事例



目的

インシデント事例を通して、実際に発生した攻撃事例やセキュリティインシデントをケーススタディを通じて学びます。具体的な知識を基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

第2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

2-2. 重大インシデント事例から学ぶ課題解決

2-2-2. 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。様々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がっています。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。

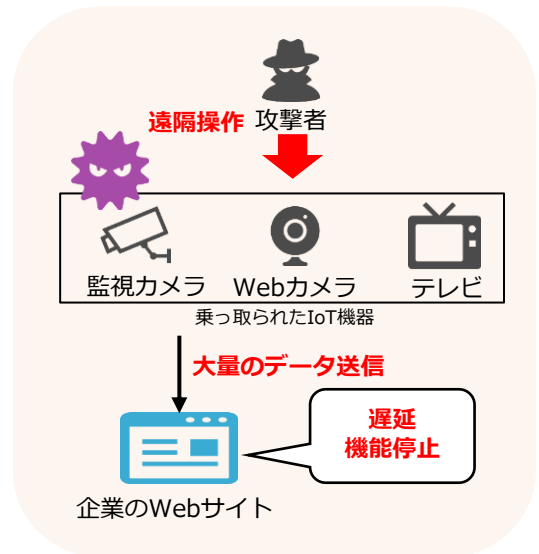


図4. DDoS攻撃の概要図

サプライチェーンによるサービス被害

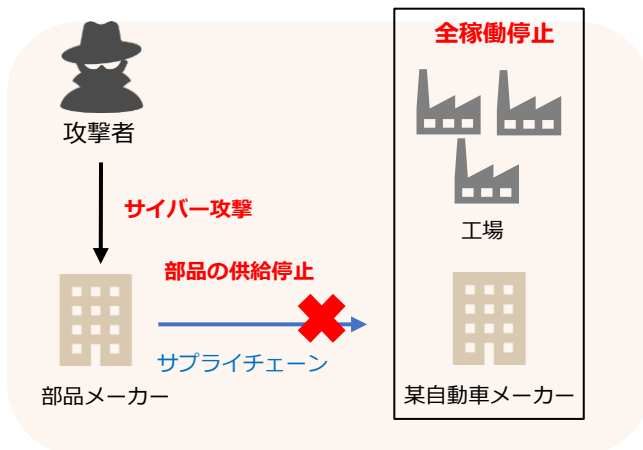


図5. 某自動車メーカーで起きたサプライチェーン攻撃の概要図

2022年2月、某自動車メーカーの取引先である部品メーカーがサイバー攻撃を受け、その結果、システムが使用不能になりました。この攻撃により、某自動車メーカーは部品の調達が不可能になり、その結果、14の工場の28のラインが停止し、約1万3000台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。

[14]

[14]:小島プレス工業株式会社.“ウイルス感染被害によるシステム停止事案発生のお知らせ”. <https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/ウイルス感染被害によるシステム停止事案発生のお知らせ-2.pdf>, (2023-07-06).

第2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
2-2. 重大インシデント事例から学ぶ課題解決

2-2-2. 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

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みが増えています。しかし、2022年9月には、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、エンジンバルブ某製造業のインシデントが挙げられます。同社は、VPN装置において2021年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いため、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。^[15]

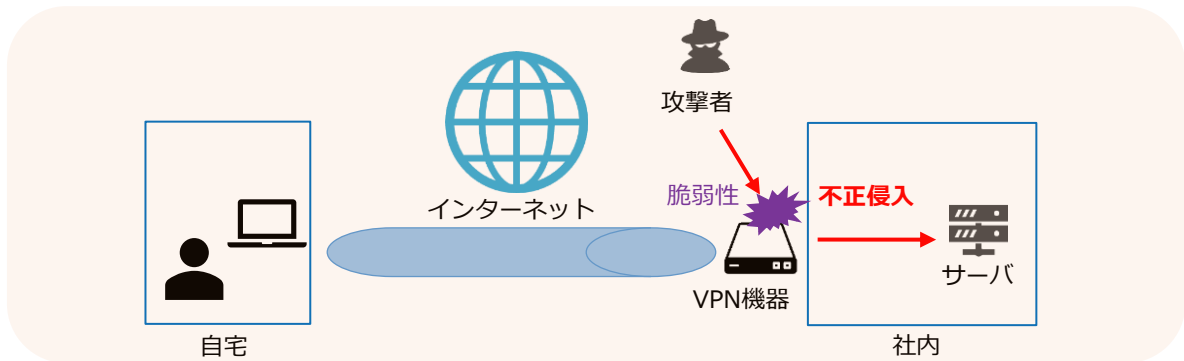


図6. VPN機器の脆弱性を利用した攻撃のイメージ

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体制が十分でない中小企業等を対象とした「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。本書に示された対策を実施することで、基本的かつ重要な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

https://www.soumu.go.jp/main_content/000753141.pdf

[15]:株式会社NITTAN.“当社サーバへの不正アクセスに関するお知らせ（第3報）”。<https://contents.xj-storage.jp/xcontents/AS05830/d773ba09/280a/4cde/879c/0e4c785b44a8/140120221031553846.pdf>, (2023-07-06).

第2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
2-2. 重大インシデント事例から学ぶ課題解決

2-2-3. 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7に示すように、3つのステップで対応します。

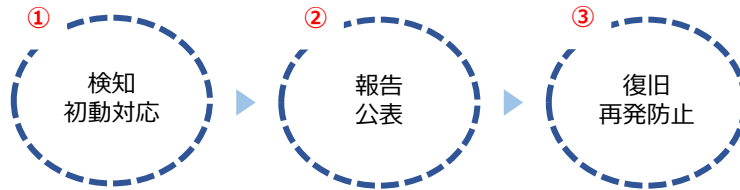


図7. インシデント対応の3ステップ

① 検知・ 初動対応	<p>検知と連絡受付： インシデントの兆候や実際の発生に気付いた場合は、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。</p> <p>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等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。</p>
② 報告・ 公表	<p>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て対応します。</p> <p>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等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。</p>
③ 復旧・ 再発防止	<p>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。</p> <p>証拠保全： 事実関係を裏付ける証拠等を収集し、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。</p> <p>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。</p> <p>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・訓練の強化等を通じて、将来のインシデントを防止するための措置を講じます。</p>

(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」を基に作成

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

第2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

2-2. 重大インシデント事例から学ぶ課題解決

2-2-4. インシデントから得た気づきと取組み

過去のインシデントから得た知見に基づき、改善取組み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、通常の設定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。^[16]

【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対策を考える必要があります。

【対策・予防策】

- ・ 取引先のセキュリティ対策状況を把握するためには、ヒアリングシートやアンケート等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な対策です。
- ・ 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。

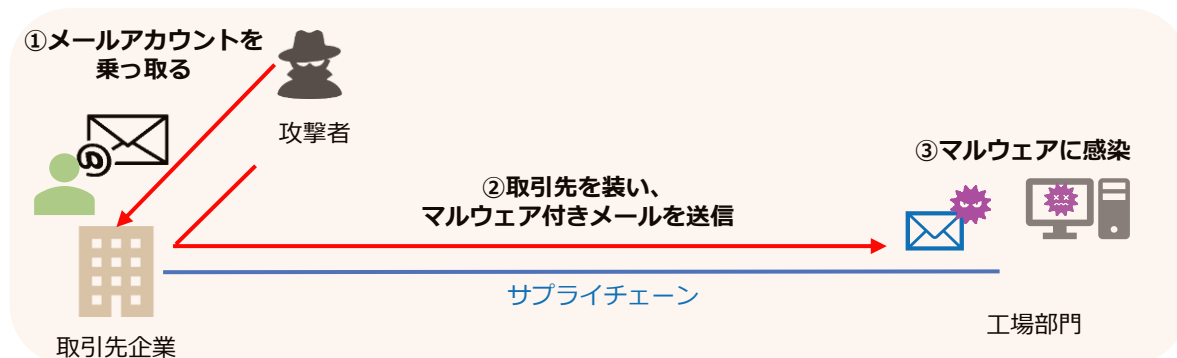


図8. 攻撃の概要図

(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）」を基に作成

[16]: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, (2023-07-06).

第2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

2-2. 重大インシデント事例から学ぶ課題解決

2-2-5. ランサムウェア感染の実態

ランサムウェアは、PCやサーバのデータを暗号化し、その暗号化されたデータを復号することを条件に身代金（金銭）を要求する悪意のあるソフトウェアです。令和4年における企業や団体の被害件数は合計230件であり、被害企業の規模を見ると、大企業が63件、中小企業が121件、団体等が46件でした。ランサムウェアの感染経路については、VPN機器からの侵入が63件で全体の62%を占め、リモートデスクトップからの侵入が19件で18%となっています。これらの侵入は、テレワーク等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80%に上る割合を占めました。^[17]

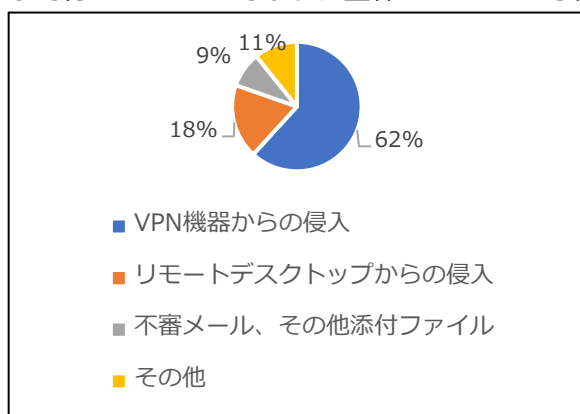


図9. (令和4年) ランサムウェアの感染経路

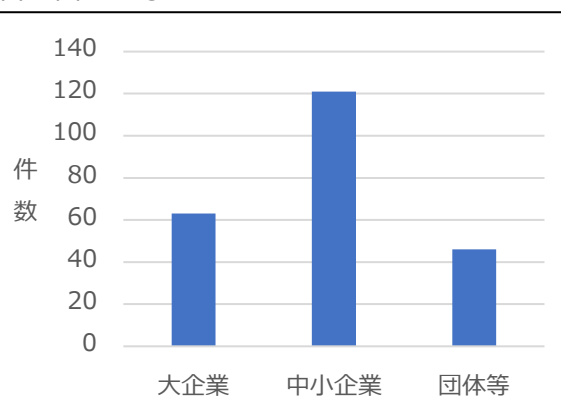


図10. (令和4年) ランサムウェアの被害件数

(出典) 警察庁「令和4年におけるサイバー空間をめぐる脅威の情勢等について」を基に作成

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、金銭を要求するだけでなく、データの復旧を条件にすると同時に、暗号化前のデータを窃取し、情報を公開するという「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③ DDoS攻撃等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、情報を共有する等の「四重脅迫」を行うケースも確認されています。

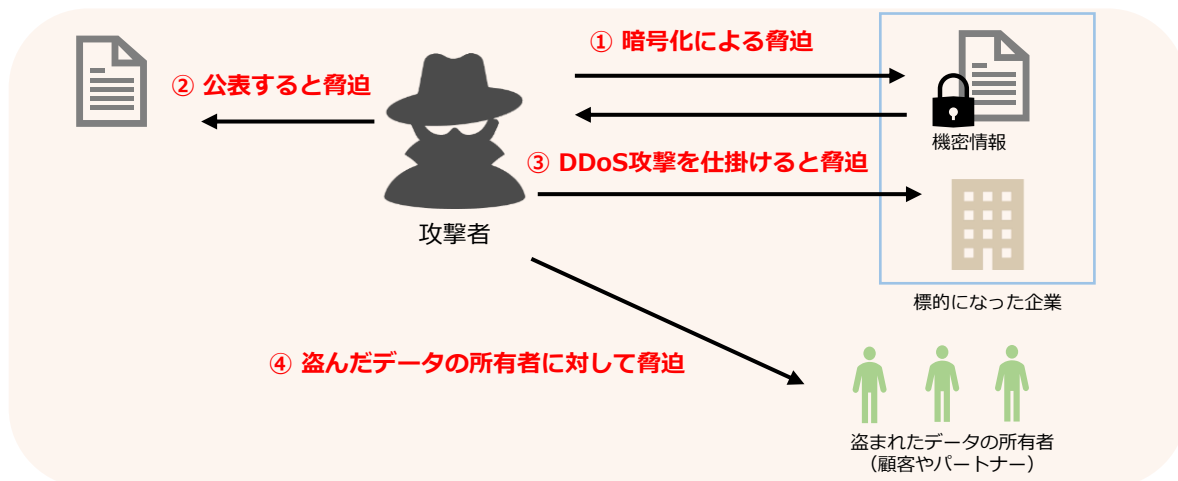


図11. ランサムウェアの二重、四重脅迫のイメージ図

[17]:警察庁,“令和4年におけるサイバー空間をめぐる脅威の情勢等について”.https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf, (2023-07-06).

第2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

2-2. 重大インシデント事例から学ぶ課題解決

2-2-5. ランサムウェア感染の実態

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することが重要です。

基幹システムでランサム被害（某食品包装メーカー）



事例の概要

2023年3月において、サーバが第三者による不正アクセスを受け、個人情報が増えいた可能性が判明しました。この攻撃者はVPN経由でリモートアクセス機能に侵入、社内サーバに侵入してランサムウェアを実行し、ファイルを暗号化したと考えられています。[18]

被害の原因

この事例の原因は、利用していたVPNの脆弱性による不正アクセスでした。さらに、不審な動きを監視するソフトウェアの最新化が不十分であり、侵入後の被害拡大を防ぐことができませんでした。

この事例から学べること

- ・マルウェア対策ソフトの定期的な更新と定期スキャンは、侵入を防ぐために重要です。
- ・侵入後の被害拡大を防ぐためには、早期の侵入検知と隔離を行うソリューションの導入、データへのアクセス制御、ログの保存等が重要です。

多数システムでランサム被害（某市民生協）



事例の概要

2020年10月、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、約49万人の個人情報が含まれていました。その中には既に脱退した会員の情報も含まれていました。[19]

被害の原因

この事例の被害の原因は、第三者によりネットワーク機器の脆弱性を突かれ、VPN経由で基幹システムサーバを含む複数のサーバへ不正侵入されたことです。この結果、ほとんどの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

- ・VPNからの不正侵入を防止するためには、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の導入等、セキュリティ強化の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）

サイバー攻撃を受けた組織における対応事例集

https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf

[18]:株式会社ギンパック, "不正アクセス及びこれに伴うシステム障害に関するお知らせ", <https://www.ginpack.co.jp/ng-wp/wp-content/uploads/2023/03/notice20230324.pdf>, (2023-07-06).

[19]:ならこープ, "重大なシステムトラブルに伴う個人情報についてのお知らせ", <https://www.naracoop.or.jp/naranews/cat2/4628.html>, (2023-07-06).

第2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

2-3. 実際の被害事例からみるケーススタディ

2-3-1. 最近のサイバー被害事例発生の傾向

不正アクセスによって引き起こされるインシデントを通じて、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とベストプラクティスを紹介します。

テレワーク対応時の脆弱性対策の不備により不正アクセスされた事例

被害の概要

ある企業がファイアウォールとVPN機能を備えた装置を導入しました。最初は、ファイアウォールの機能のみ利用していましたが、テレワークを実現するためにVPNを有効化した結果、存在していた脆弱性が悪用され、不正アクセスが行われました。その結果、装置の設定ファイルやログファイル、さらにはIPアドレスを含む設定情報が盗まれ、ダークWeb上で公開されてしまいました。^[20]

被害の原因

VPNの脆弱性情報が公開された際には、VPN機能を無効にしていたため、対策は必要ないと判断されていました。しかし、テレワークに対応するためにVPN機能を有効にしたことで、脆弱性が露呈し、不正アクセスが行われました。このように、機器の利用用途が変わった場合には、必要なセキュリティ対策も変わる可能性があることを考慮していなかったことが、不正アクセスの一因とされています。

対策・ベストプラクティス

- ・システムの構成変更や機器の設定変更が行われる際には、利用用途の変更等も考慮し、適切なセキュリティ設定や脆弱性対策が行われているかを確認することが重要です。必要に応じて脆弱性診断を受けることも有効な対策の1つです。
- ・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サイト等を確認し、未対策の脆弱性がないかを点検することが大切です。

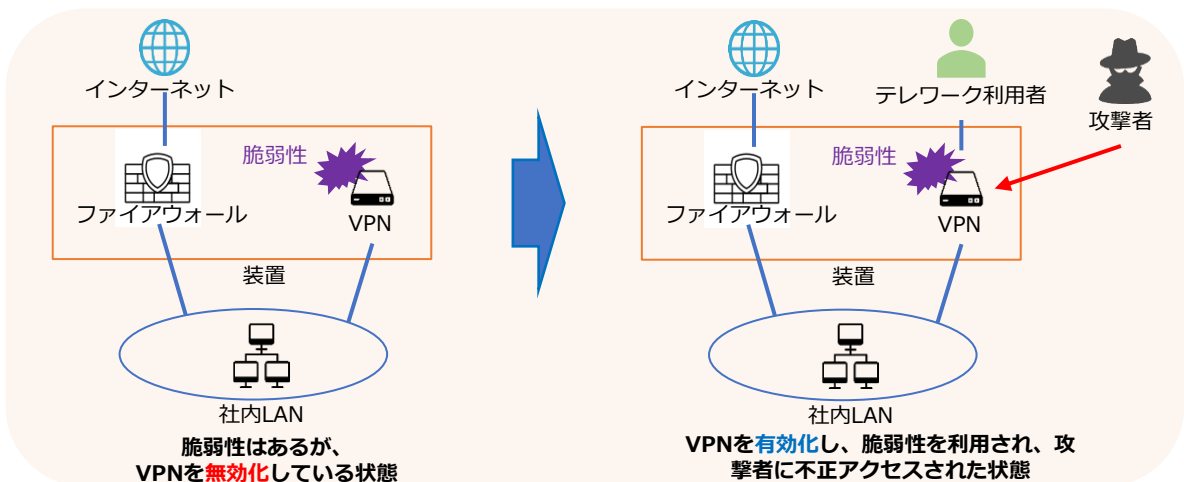


図12. 攻撃の概要図

(出典) IPA「コンピュータウイルス・不正アクセスの届出事例【2022年下半年（7月～12月）】」を基に作成*22

[20]:IPA,「コンピュータウイルス・不正アクセスの届出事例【2020年下半年（7月～12月）】」。 <https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000088780.pdf>, (2023-07-06).

第2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

2-3. 実際の被害事例からみるケーススタディ

2-3-2. 事例：徳島県の某病院

令和3年10月31日未明、病院内で重大なインシデントが発生しました。複数のプリンタが同時に犯行声明を印刷し、LockBit2.0ランサムウェアに感染したことが判明しました。この攻撃により、電子カルテ等の端末と関連するサーバのデータが暗号化され、患者の診察記録が閲覧できなくなり、病院の機能は停止しました。侵入経路は、導入されているVPN装置の脆弱性を悪用したものと考えられ、これは過去に話題になった脆弱性と同じものでした。病院は事前に策定されたBCP（事業継続計画）を発動し、迅速な対応を行い、徳島県警察本部への相談や関係機関の連携を行いました。

対策方針として全体の状況把握や情報漏えいの特定よりも、データの復元やシステムの再構築に取組みました。フォレンジックを担当した事業者が一部のデータを復元することができ、復元端末の初期化やセキュリティの見直しを行い、令和4年1月4日に通常の診療を再開することができました。^[21]

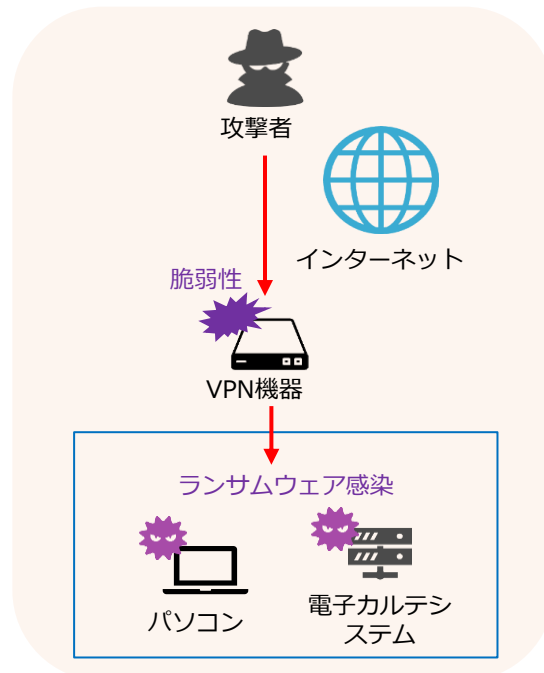


図13. 攻撃の概要図

問題点

- ・ Fortinet社製の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、病院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ときの被害を想定する。

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>

[21]:徳島県つるぎ町立半田病院.“徳島県つるぎ町立半田病院 コンピュータウイルス感染事案 有識者会議調査報告書”. https://www.handahospital.jp/topics/2022/0616/report_01.pdf, (2023-07-06).

第2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

2-3. 実際の被害事例からみるケーススタディ

2-3-3. 具体的な対応策

ランサムウェア被害のケースをみると、VPN機器から不正侵入され、サーバの特権IDを使用してサーバのデスクトップ上から不正プログラムを実行されるケースが後を絶ちません。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、本人であることを証明させる多要素認証の仕組みを講じることが必要となります。それ以外にも、特定のPCやサーバからしか重要なサーバのデスクトップに接続できないような仕組みや、ログの長期保管なども重要な要素となります。

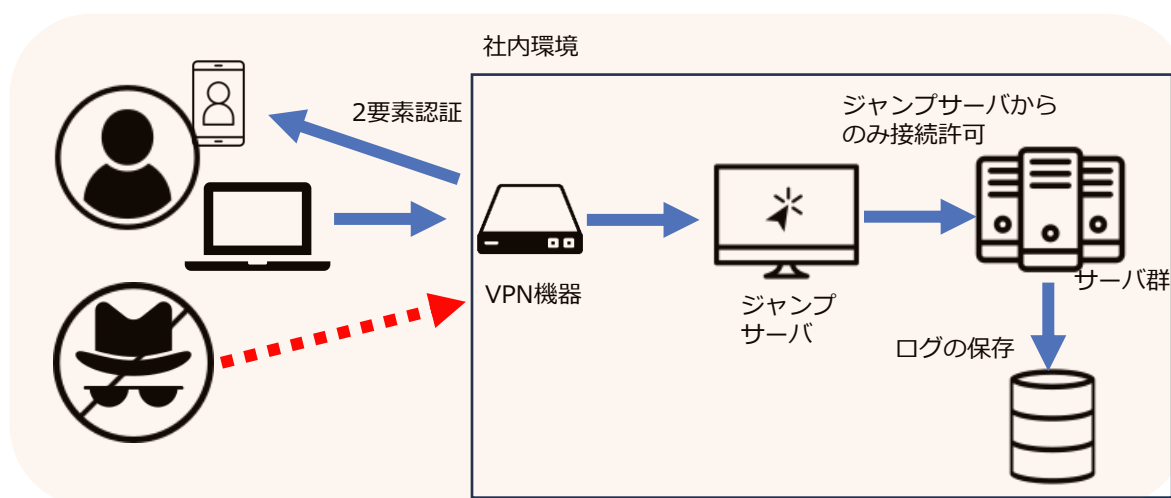


図14. 対応策の概要図

実施すべき対策と運用

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

第3章. サイバーセキュリティの基礎知識

3-1. 導入済と想定するセキュリティ対策機能

3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-4. サイバーセキュリティアプローチ方法

第3章. サイバーセキュリティの基礎知識

3-1. 導入済と想定するセキュリティ対策機能

3-1-1. UTM、EDRの概要

サイバー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一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、スマートフォン、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。

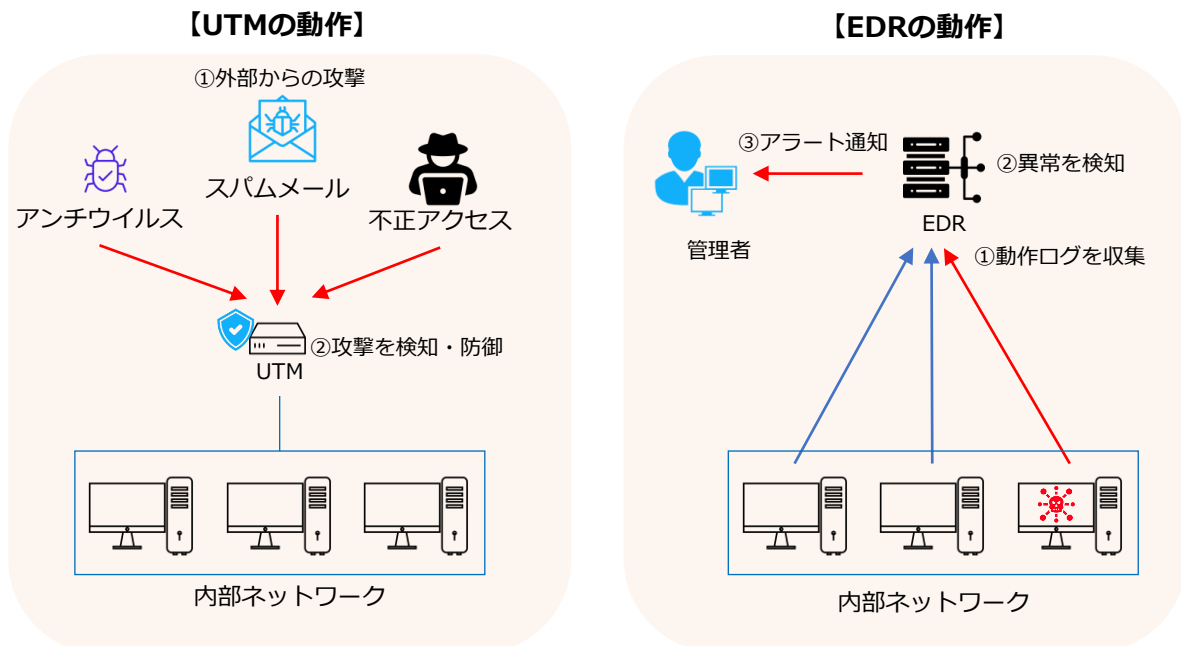


図15. UTM、EDRの概要図

第3章. サイバーセキュリティの基礎知識

3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

3-2-1. 情報処理技術者向け国家試験体系

情報処理技術者試験の全体像を紹介し、その後、最初に受験すべき3つの試験について、対象者や取得目的、そして活用方法等を紹介します。

現代社会において、安全で効果的なITの活用を進めるためには、IT業界やIT職種に限らず、広範な範囲の人々がITや情報セキュリティに関する知識を持つことが欠かせません。また、デジタルトランスフォーメーション（DX）の進展に伴い、ITやセキュリティに関する専門知識や業務経験を持っていない人々にとっても、企業内外でセキュリティ専門の人材と協力する必要性が増しています。このような協力関係を築くためには、必要な知識を補完する必要があります。そこで、従業員一人ひとりにITや情報セキュリティの知識を身につけてもらうための有効な手段として、情報技術者試験を受験することが挙げられます。情報技術者試験を受験することで、ITリテラシーおよび情報セキュリティに関する基礎知識を習得することができます。組織全体で従業員一人ひとりのセキュリティ意識を高めることは、組織の安全な運営に不可欠です。また、この試験の合格により、組織内のセキュリティ専門人材不足の問題を解消する可能性もあります。まずは情報技術者試験の全体像を紹介します。

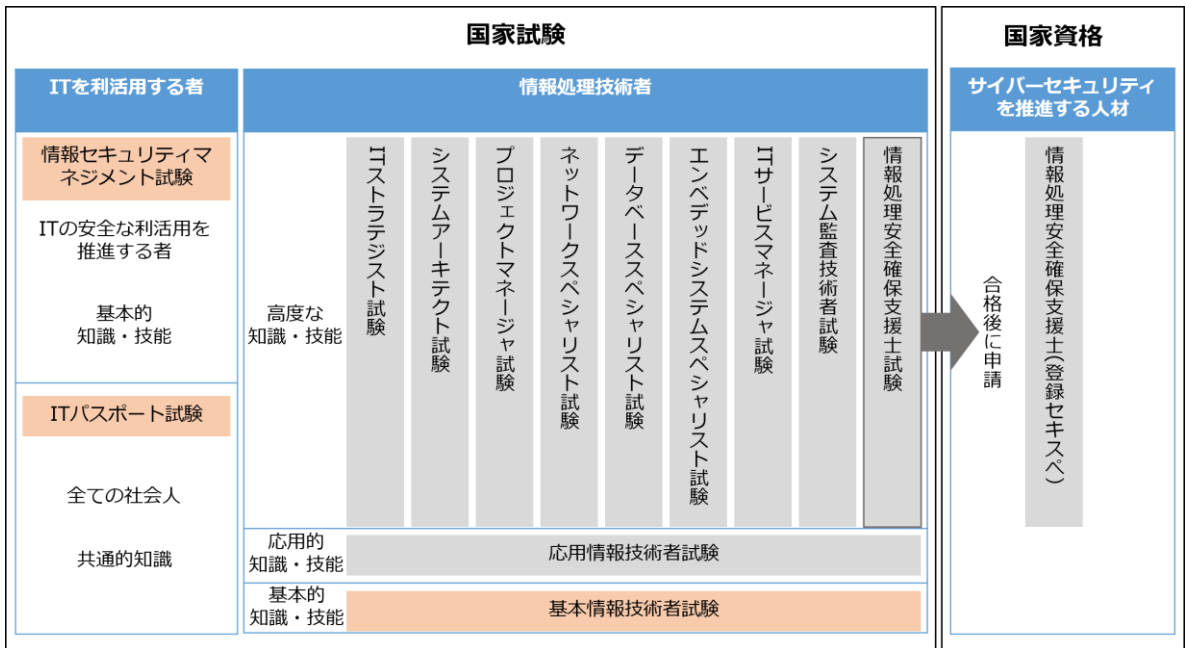


図16. 情報処理技術者試験の一覧
(出典) IPA「試験区分一覧」を基に作成

詳細理解のため参考となる文献（参考文献）

試験区分一覧

<https://www.ipa.go.jp/shiken/kubun/list.html>

第3章. サイバーセキュリティの基礎知識

3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

3-2-1. 情報処理技術者向け国家試験体系

ITの国家試験の中で、全ての社会人にとって必要なITパスポート試験（IP）、ITの安全な利活用を目的とした情報セキュリティマネジメント試験（SG）、ITの基本的知識・技能を有する水準となる基本情報技術者試験（FE）について紹介します。^[22]

ITパスポート試験（IP）

対象者	ITを活用する全ての方（ITを使う社会人や学生等）
取得目的	現代の社会人に必要とされる、ITに関する知識、企業活動、経営戦略、マーケティング・財務・法務等の幅広い知識をバランス良く習得し、業務の課題把握力やITを活用した課題解決力を身につけたり、ビジネスパーソンとしてのスキルの向上や仕事を効率化させます。
活用シーン	<ul style="list-style-type: none"> ・情報セキュリティや情報モラルに関する知識が身につくことで、インターネット、電子メール、社内システムを利用する際に、機密情報の漏えいやウイルス感染等様々なリスクがあることを理解できるようになります。 ・知的財産権等に関する法律の知識や、企業コンプライアンスに関する知識が身につくことで、著作権侵害・商標権侵害等の法令違反や個人情報漏えい等のリスクが理解できるようになります。
補足	試験時間：60分 出題数：100問 出題形式：多肢選択式



情報セキュリティマネジメント試験（SG）

対象者	<ul style="list-style-type: none"> ・業務で個人情報を取り扱う全ての方 ・業務部門・管理部門で情報管理の担当者 ・外部委託先に対する情報セキュリティ評価・確認を行う全ての方 ・情報セキュリティ管理の知識・スキルを身につけたい全ての方 ・ITパスポート試験合格から、さらにステップアップしたい全ての方
取得目的	情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを身につけます。また、より実践的なセキュリティの対策方法への理解を深めます。
活用シーン	<ul style="list-style-type: none"> ・部門全体の情報セキュリティ意識を高め、情報漏えいのリスクを低減することができるようになります。 ・トラブルが発生しても、適切な事後対応により、被害を最小限にとどめることができるようになります。 ・情報セキュリティが確保され、より安全で積極的なITの利活用を推進することができるようになります。
補足	試験時間：午前 120分 午後 120分 出題数：午前 60問 午後 60問 出題形式：午前 多肢選択式（四肢択一） 午後 多肢選択式



[22]:IPA.“試験要綱 Ver.5.1”. https://www.ipa.go.jp/shiken/syllabus/ps6vr7000000htyh-att/youkou_ver5_1.pdf, (2023-07-06).

第3章. サイバーセキュリティの基礎知識

3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

3-2-1. 情報処理技術者向け国家試験体系

基本情報技術者試験 (FE)



対象者	<ul style="list-style-type: none"> ・デジタル人材 (DX を主導・実行する人材) ・ビジネス職の方 ・エンジニア職の方
取得目的	ITパスポートよりさらに詳しく、ITや情報セキュリティの基礎知識を身につけます。また、基礎知識を身につけることで専門家とのコミュニケーションがスムーズになります。
活用シーン	・セキュリティに関する基礎的な知識とスキルを習得することにより、情報システムやネットワークのセキュリティに関する業務やプロジェクトに参加し、セキュリティリスクを最小限に抑えるための役割を果たすことができます。
補足	試験時間：午前 120分 午後 120分 出題数：午前 60問 午後 60問 出題形式：午前 多肢選択式 (四肢択一) 午後 多肢選択式

詳細理解のため参考となる文献 (参考文献)

ITパスポート試験	https://www.ipa.go.jp/shiken/kubun/ip.html
情報セキュリティマネジメント試験	https://www.ipa.go.jp/shiken/kubun/sg.html
基本情報技術者試験	https://www.ipa.go.jp/shiken/kubun/fe.html

第3章. サイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-3-1. Security Action 二つ星レベル

「SECURITY ACTION」は中小企業自らが、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です。安全・安心なIT社会を実現するために、IPAによって創設されました。宣言企業数（2023年6月7日時点）：一つ星：225252社 二つ星：25143社^[23]

★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	①「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」は情報セキュリティ対策状況等を、IPAが認定するものではありません。

「SECURITY ACTION」の取組みに関してWebサイト等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/>,(参照 2023-06-30)

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/>

[23]:IPA.“SECURITY ACTION セキュリティ対策自己宣言”.<https://www.ipa.go.jp/security/security-action/>, (2023-06-30).

第3章. サイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-3-2. 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: パソコンやルータのソフトウェアやファームウェアを最新化します。
WindowsUpdateやソフトウェアアップデートを実行します。

2. ウイルス対策ソフトを導入しよう！

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

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

3. パスワードを強化しよう！

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

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

4. 共有設定を見直そう！

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

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

5. 脅威や攻撃の手口を知ろう！

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

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

(出典) IPA「情報セキュリティ5か条」を基に作成

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5か条

https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf

第3章. サイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-3-3. 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、自社の情報セキュリティ対策が、どれくらい実施できているかを把握できます。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情報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等実施状況を把握している人が記入します。事業所が複数、部署が多い等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」を基に作成

詳細理解のため参考となる文献（参考文献）

5分でできる！情報セキュリティ自社診断

<https://www.ipa.go.jp/security/guide/sme/5minutes.html>

第3章. サイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-3-3. 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」

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

(出典) IPA「5分でできる！情報セキュリティ自社診断」を基に作成

第3章. サイバーセキュリティの基礎知識

3-3. Security Action (セキュリティ対策自己宣言)

3-3-4. 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等を考慮し、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みを明示するためのものです。したがって、作成した文書は従業員や顧客等の関係者に周知する必要があります。

情報セキュリティ基本方針 (サンプル)

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

1. 経営者の責任

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

2. 社内体制の整備

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

3. 従業員の取組み

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

4. 法令および契約上の要求事項の遵守

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

5. 違反および事故への対応

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

制定日：20〇〇年〇月〇日

株式会社〇〇〇〇

代表取締役社長 〇〇〇〇

(出典) IPA「情報セキュリティ基本方針 (サンプル)」を基に作成

情報セキュリティ基本方針の記載項目例

管理体制の整備 / 法令・ガイドライン等の遵守 / セキュリティ対策の実施 / 継続的改善 等

第3章. サイバーセキュリティの基礎知識

3-4. サイバーセキュリティアプローチ方法

3-4-1. サイバーセキュリティアプローチ方法の概要

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

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

①

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2022（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）

②

素早く、多くの
セキュリティホール
を塞ぐ

Lv2. ベースラインアプローチ

実施手法

ガイドブック、ひな形を参照し、迅速にセキュリティ対応します

活用できる文書/ツール名称（例）

- ・リスク分析シート（出典：IPA）
- ・セキュリティ関連費用の可視化（出典：IPA）
- ・中小企業の情報セキュリティ対策ガイドライン第3版（出典：IPA）

③

じっくり、小さな
セキュリティホール
も残さないように塞
ぐ

Lv3. 網羅的アプローチ

実施手法

網羅的な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)

第3章. サイバーセキュリティの基礎知識
3-4. サイバーセキュリティアプローチ方法

3-4-1. サイバーセキュリティアプローチ方法の概要

凡例) 「○:あり / △:部分的にあり / ×:なし」

Lv.1 クイックアプローチ		網羅性	即時性
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。 <ul style="list-style-type: none"> ・小規模な対策や修正を迅速に実施可能 ・低コストでリスクを軽減 ・進行中の攻撃へ対応することにより、攻撃の拡大や影響を最小限に抑える 		×	○
1. 脅威の特定	既知の脅威/過去のインシデントに基づいて、リスクの優先度付けを行いリスクを特定します。		
2. 対応計画	既存のセキュリティ対策の評価を行い、改善点を特定し対応計画を立てます。		
3. 対策の実装	必要な設定変更やアップデートの適用、ポリシーや手順の策定、従業員への教育やトレーニング等の対策を実装します。		
4. 評価・改善	実装した対策の評価を行い、継続的な改善を促進します。		

Lv2. ベースラインアプローチ		網羅性	即時性
ベースラインアプローチは、セキュリティ対策の基準やガイドラインを定義することにより、組織全体で一貫性を確保し、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。 <ul style="list-style-type: none"> ・セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保 ・網羅的なアプローチの出発点 		△	△
1. ベースラインの定義	セキュリティの基準となるベースラインを定義します。活用できる文書/ツール、内部のセキュリティ目標等に基づいて定義します。		
2. 現状評価	セキュリティポリシーやガイドラインの遵守度に基づき、既存のセキュリティ対策の評価を行います。改善点を特定し対応計画を立てます。		
3. ベースラインの適用	セキュリティポリシーの策定・改訂、ガイドラインの作成、セキュリティ対策の実装等により、ベースラインを適用します。		
4. 教育	定期的な教育活動を通じて、従業員にセキュリティポリシーやガイドラインの重要性を啓発し、遵守を促進します。		
5. 評価・改善	実装した対策の評価を行い、継続的な改善を促進します。		



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

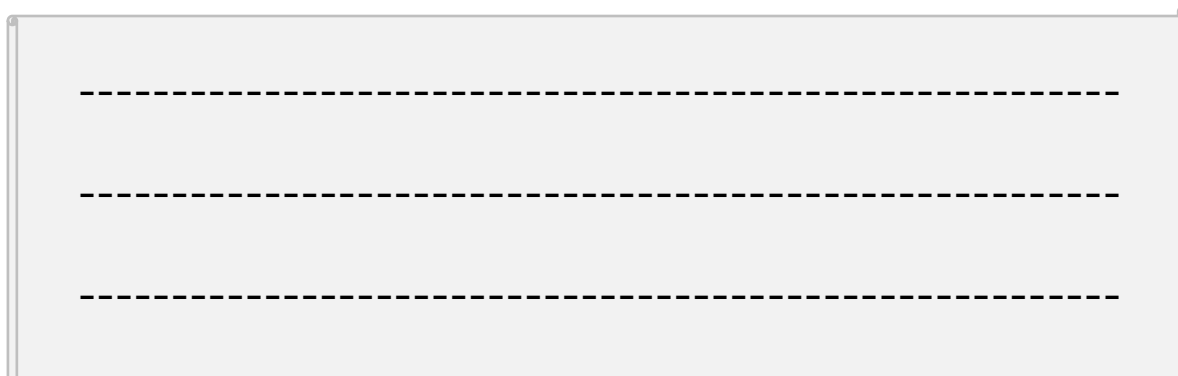
第3章. サイバーセキュリティの基礎知識
3-4. サイバーセキュリティアプローチ方法

3-4-1. サイバーセキュリティアプローチ方法の概要

凡例) 「○:あり / △:部分的にあり / ×:なし」

Lv3. 網羅的アプローチ		網羅性	即時性
網羅的アプローチは、可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなります。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではありません。 ・可能な限り多くの脅威や攻撃手法に対して対策を講じる ・予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持		○	×
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2022	https://www.ipa.go.jp/publish/wp-security/sec-2022.html
情報セキュリティ10大脅威 2023	https://www.ipa.go.jp/security/10threats/10threats2023.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/guide/sme/ug65p90000019cbk-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2023）	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、暗号化等が含まれます。情報セキュリティは、デジタルだけでなく、紙の文書等の非デジタル情報にも関連しています。また、3要素に加えて、真正性（Authenticity）、責任追跡性（説明責任）（Accountability）、否認防止性（Non-Repudation）、信頼性（Reliability）を合わせて情報セキュリティの7要素と呼ぶこともあります。

一方、サイバーセキュリティは、主にインターネットやコンピュータネットワークに関連するリスクに対処することを目的とします。サイバーセキュリティは、クラッキング、マルウェア、DDoS攻撃等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。

編集後記

セミナー1日目では、情報セキュリティ白書、情報セキュリティ10大脅威、最近の事例、Security Action（セキュリティ対策自己宣言）について紹介をしました。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だけでなく、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、サイバー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。

また、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。一つ星の取組みが完了したら、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」に取り組めます。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対策を進めることとなります。本テキストでは「クイックアプローチ」、「ベースラインアプローチ」、「網羅的アプローチ」について簡単に紹介しましたが、次回以降のテキストでは具体的な手順も含めて詳しく解説していきます。

引用文献

Society 5.0

https://www8.cao.go.jp/cstp/society5_0

デジタルガバナンス・コード2.0

https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html

情報セキュリティ白書2022

<https://www.ipa.go.jp/publish/wp-security/qv6pgp0000000vgi-att/000100472.pdf>

情報セキュリティ10大脅威 2023

https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

情報セキュリティ10大脅威の活用法

https://www.ipa.go.jp/security/10threats/ps6vr70000009r2t-att/katsuyouhou_2023.pdf

勤怠管理システムサーバに対する攻撃について

<https://www.viax.co.jp/pdf/20220601.pdf>

ウイルス感染被害によるシステム停止事案発生のお知らせ

<https://www.kojima-tns.co.jp/wp-content/uploads/2022/08/ウイルス感染被害によるシステム停止事案発生のお知らせ-2.pdf>

弊社を装った不正メールが届いた際のご対応方法のお知らせ

<https://kameya-yoshinaga.com/f/single?p=1848>

お客様情報の流出に関するお詫びとご報告

<https://www.ai-koumuten.co.jp/topics/news/37241/>

情報セキュリティインシデントについて

https://www.hirata.co.jp/files/optionallink/ns_20200825.pdf

Microsoft Edge セキュリティ更新プログラムのリリースノート

<https://learn.microsoft.com/ja-jp/deployedge/microsoft-edge-relnotes-security>

ビジネスメール詐欺（BEC）の詳細事例 2 ～銀行口座証明書類を偽造し振込先口座変更を依頼してきた事例

<https://www.ipa.go.jp/security/bec/hjuojm0000003c8r-att/000103087.pdf>

情報セキュリティインシデント調査委員会報告書

<https://www.gh.opho.jp/important/785.html>

メールアドレス漏洩のお詫び

https://www.sankei.jp/wp-content/uploads/2023/05/メールアドレス漏洩のお詫び_20230510.pdf

引用文献

当社サーバへの不正アクセスについて（第3報）

https://www.dyjh.co.jp/news/pdf/221101_dyjh.pdf

当社サーバへの不正アクセスに関するお知らせ（第3報）

<https://contents.xj-storage.jp/xcontents/AS05830/d773ba09/280a/4cde/879c/0e4c785b44a8/140120221031553846.pdf>

中小企業のためのセキュリティインシデント対応の手引き

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf>

【NISC】サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）

https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf

令和4年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf

不正アクセスおよびこれに伴うシステム障害に関するお知らせ

<https://www.ginpack.co.jp/ng-wp/wp-content/uploads/2023/03/notice20230324.pdf>

重大なシステムトラブルに伴う個人情報についてのお知らせ

<https://www.naracoop.or.jp/naranews/cat2/4628.html>

コンピュータウイルス・不正アクセスの届出事例【2020年下半年（7月～12月）】

<https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000088780.pdf>

徳島県つるぎ町立半田病院 コンピュータウイルス感染事案 有識者会議調査報告書

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

試験区分一覧

<https://www.ipa.go.jp/shiken/kubun/list.html>

試験要綱 Ver.5.1

https://www.ipa.go.jp/shiken/syllabus/ps6vr7000000htyh-att/youkou_ver5_1.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/guide/sme/ug65p90000019cbk-att/000055848.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/security-action/download/5point_poster.pdf

引用文献

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>

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

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/downloadfiles/guide_v3.0.pdf

ICSCoE中核人材育成プログラム

https://www.ipa.go.jp/jinzai/ics/core_human_resource

セキュリティ・キャンプ

<https://www.security-camp.or.jp>

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>

中小企業等担当者向け テレワークセキュリティの手引き

https://www.soumu.go.jp/main_content/000753141.pdf

iパスWebサイト

<https://www3.jitec.ipa.go.jp/JitesCbt/index.html>

ITパスポート試験

<https://www.ipa.go.jp/shiken/kubun/ip.html>

情報セキュリティマネジメント試験

<https://www.ipa.go.jp/shiken/kubun/sg.html>

基本情報技術者試験

<https://www.ipa.go.jp/shiken/kubun/fe.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/guide/sme/ug65p90000019cbk-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

参考文献

中小企業の情報セキュリティ対策ガイドライン第3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

<https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html>

セキュリティ関連知識の保管庫（ナレッジベース2023）

<https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/>

用語集

■ AI

Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956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。最近AIは目覚ましい研究結果を出すようになってきていて、ブームとなっている。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

…………… 1-1-1

■ BCP

Business Continuity Plan（事業継続計画）の略。企業が災害やテロ攻撃などの緊急事態に直面した際に、被害を最小限に抑え、企業の存続に関わる最も重要な事業を継続または早期復旧するための計画

…………… 2-3-2

■ 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

…………… 2-1-3

■ 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

…………… 2-2-2、
2-2-5、第一回コラム

■ EDR

Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な挙動を検知し、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

…………… 2-2-4、
2-2-5

■ Fortinet

セキュリティ製品の開発、製造を行う米国のメーカー。ファイアウォールやセキュリティソフトを提供している

…………… 2-3-2

■ ICSCoE中核人材育成プログラム

制御システム（OT：Operational Technology）と情報システム（IT）、双方にわたるスキルを核とした上で、サイバーセキュリティ対策の必要性を把握し、プロジェクトを強力に推進していく力をバランス良く備えた人材など将来企業などの経営層と現場担当者をつなぐ、中核となる人材を育成すること

…………… 2-1-2

■ IoT

Internet of Thingsの略。あらゆるモノ（物理デバイスや機器）をインターネットに

接続する技術のこと。相互に通信し、データをやり取りすることを可能にする技術のこと

…………… 1-1-1、
2-1-2、2-2-2

■ IPS

Intrusion Prevention Systemの略。不正侵入防止システムとも呼ばれるセキュリティ確保の仕組み。

IPSは、異常を検知した場合、管理者に通知するだけではなく、その通信を遮断する

…………… 2-2-2

■ 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、今後情報家電等で大量に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検討されている。なお、IPv6では、アドレス空間の増加だけでなく、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

…………… 2-3-1

用語集

■ ISMS

Information Security Management Systemの略称。ISMSは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
…………… 3-4-1

■ ITリテラシー

コンピュータやインターネットをはじめとする情報技術（IT）を適切に活用する基礎的な知識や技能
…………… 3-2-1

■ LockBit2.0

「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…………… 2-3-2

■ 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、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本においても、今後普及が見込まれる
…………… 3-4-1

■ SASE（サッシー）

Secure Access Service

Edgeの略。ガートナー社が2019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上で統合して提供するサービス、また、その考え方・概念
…………… 2-2-4

■ SDP

Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、全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
…………… 2-2-5

■ SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取組むことを自己宣言する制度
…………… 2-1-2、3-2-1

■ Society 5.0

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）
…………… 1-1-1

■ 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

…………… 2-2-4

■ 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。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…………… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3

■ WAF（ワフ）

Web Application Firewallの略。WAFとは、従来のファイアウォールが、IPアドレスとポート番号で通信を制御していたことに対して、Webアプリケーションの脆弱性を狙うサイバー攻撃を防ぐことを目的として、アプリケーションレベルで通信を制御（分析・検知・遮断）するファイアウォールのこと
…………… 2-2-2

■ アクセス制御

コンピュータやネットワークにアクセスできるユーザを制限する機能のこと
…………… 2-2-5、
第一回コラム

用語集

■アセスメント

システムや運用環境等を客観的に調査・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
…………… 2-2-4

■暗号化

データの内容を変換し、利用者以外には、内容を見ても解読できないようにすること。利用者自身は、データを元の状態に戻すことができる
…………… 2-1-3、2-2-1、2-2-5、2-3-2、3-2-3、3-3-1、第一回コラム

■アンダーグラウンドサービス

合法ではない非公式な活動が行われるオンラインの闇市場やコミュニティでサイバー攻撃を目的としたツールなどを販売しているサービス
…………… 2-1-3

■インターネットバンキング

インターネットを利用した銀行や金融機関との取引を行うサービスのこと。銀行の窓口やATMに出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振込や残高照会などの取引を行うことができる
…………… 3-3-2

■ウイルス定義ファイル（パターンファイル）

セキュリティソフト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付きの手配書のようなもの
…………… 3-3-2、

3-2-3

■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、サーバ等）
…………… 2-2-4

■改ざん

文書や記録などの全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
…………… 2-1-2

■可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性
…………… 第一回コラム

■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
…………… 第一回コラム

■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
…………… 第一回コラム

■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・サーバ攻撃・情報システムの破壊などの行為を行うこと
…………… 第一回コ

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、独立した機関のこと。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う行政機関（組織的には内閣府の外局）
…………… 2-2-3

■サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまで様々である。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、個人等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。
…………… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2

■サイバーセキュリティお助け隊サービス制度

中小企業のサイバー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で安価に提供するサービス
…………… 2-1-2

用語集

■ **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

…………… 3-4-1

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

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

…………… 3-4-1

■ **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

…………… 2-1-3、
2-2-2、2-2-4

■ **情報資産**

営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

…………… 3-4-1

■ **情報セキュリティの3要素「CIA」**

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

…………… 第一回コ

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

…………… 2-1-3、
第一回コラム

■ **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

…………… 第一回コ
ラム

■ **スクリーンロック**

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

…………… 2-2-2

■ **脆弱性**

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

…………… 2-1-1、
2-1-3、2-2-1、2-2-2、2-
2-4、2-2-5、2-3-1、2-3-2、
2-3-3、3-4-1、第一回コ
ラム

■ **脆弱性診断**

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

…………… 2-3-1

■ **責任追跡性**

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

…………… 第一回コ
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等がインシデントに該当

…………… 2-1-1、
2-1-2、2-1-3、2-2-1

■ **セキュリティ・キャンプ**

情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、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

…………… 2-1-2

■ **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

…………… 3-4-1

用語集

■セキュリティポリシー

企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的
…………… 2-1-1、2-2-1、3-4-1

■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
…………… 2-1-3

■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、全てのネットワーク通信を信用できない領域として扱い、全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
…………… 2-2-4

■ソリューション

問題や課題を解決するための具体的な解決策や手段を指す。ある特定の課題やニーズに対して提供される解決方法やアプローチのことを指すことが一般的で、ビジネスシーンにおけるソリューションの意味とは「顧客が抱える問題や課題を解決すること」
…………… 2-2-5

■ダークウェブ

特別な手法でないとアクセスできない、匿名性の高い非公開のWebサイトのこと。漏えいした個人情報や機密情報、危険な商品、クラッキングツールなど、違法なものが取引されている
…………… 2-1-3

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせることで認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年ではFIDO2と呼ばれる、デバイスを使用したパスワードによる認証により、パスワードレスでの認証が広まっている
…………… 2-2-5、2-3-3

■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
…………… 1-1-1

■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ル化（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタルライゼーション

（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードをCD（コンパクトディスク）にするのがデジタルイゼーション、音楽をダウンロード販売するのがデジタルライゼーションである
…………… 1-1-1、2-1-1、2-2-1、3-4-1

■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
…………… 第一回コラム

■内部監査

内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する
…………… 3-4-1

■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、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Email Compromiseとも略される
…………… 2-1-3

■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
…………… 1-1-1

用語集

■否認防止性

システムに対する操作・通信のログを取得したり、本人に認証させることにより行動を否認させないようとする特性
…………… 第一回コラム

■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、組織の担当者へ送付する手口が知られている。従来は府省庁や大手企業を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
…………… 2-1-2、2-1-3

■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
…………… 2-2-4

■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

様々である

…………… 2-3-1

■不正アクセス

利用権限を持たない悪意のあるユーザが、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、2000年2月に施行された不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）により、法律で固く禁じられている

…………… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、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

…………… 2-1-3

■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みを指す。

「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
…………… 2-2-3、2-3-2

■ブラックマーケット

広義には、不法な取引が行われる市場。不正に入手した個人情報などを売買するネット上の市場（闇市）
…………… 2-1-3

■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様々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「ひな形」としてまとめたもの
…………… 2-2-4、3-3-1

■ブロックチェーン

複数のコンピュータを使用し、分散的にデータをブロック単位にまとめて鎖（チェーン）のように記録する仕組み
…………… 1-1-1

■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、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論
…………… 2-1-3、2-3-1

用語集

■ マルウェア

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

…………… 2-2-2、
2-2-4、2-2-5、第一回コラム

■ 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にアクセスすることができる

…………… 3-3-3

■ 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

…………… 2-1-2、
2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3

■ リスクアセスメント

企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外については何らかの対策を講じる必要がある

…………… 3-4-1

■ リスク評価

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

…………… 2-3-2、
3-3-1

■ リモートデスクトップ接続

パソコン、タブレット、スマートフォン等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

…………… 2-2-2



**令和5年度
中小企業サイバーセキュリティ対策
継続支援事業**
