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

目次

目次

目次

目次

目次

目次

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が、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などを進めています。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、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

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

1-1-1. 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などの企業リソースが限定されている中小企業こそ、新たなサービスを創造し、ビジネスを発展させるために、DXを推進することが重要です。

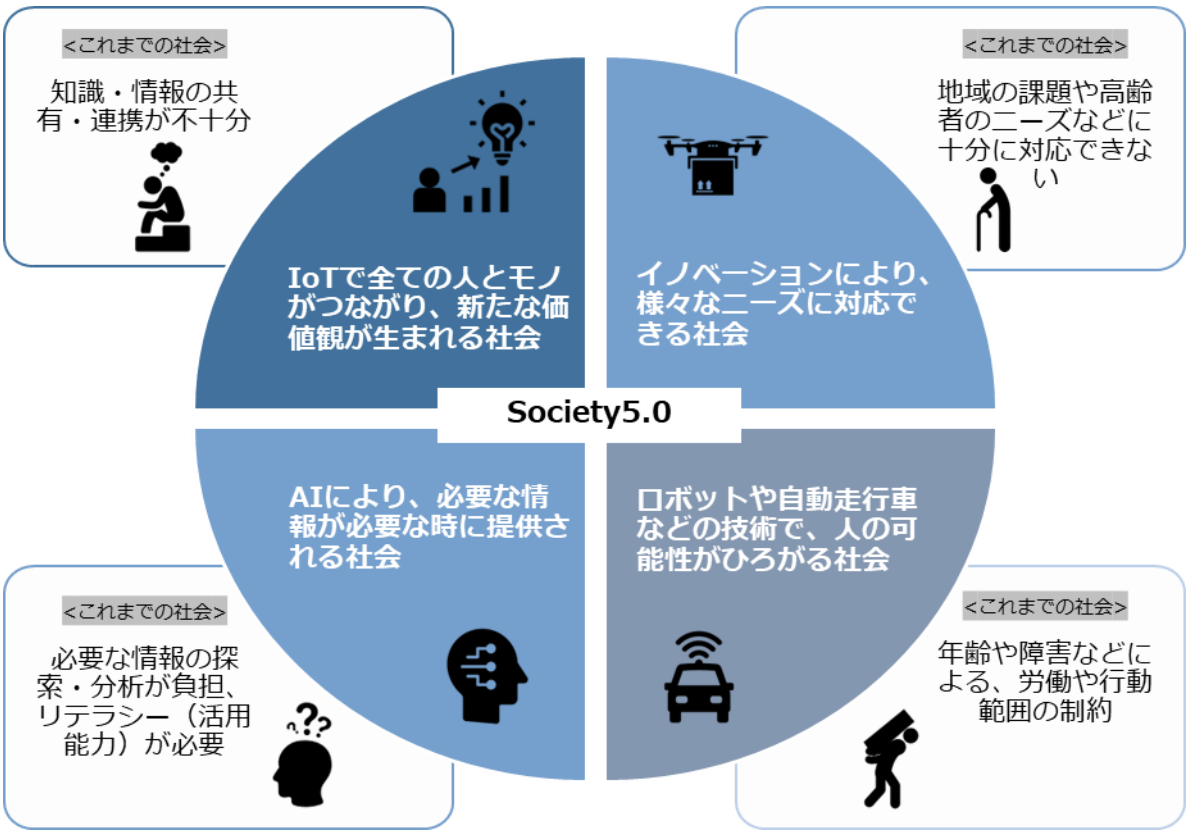


図1. Society5.0の概要図
（出典）内閣府.”Society5.0”.https://www8.cao.go.jp/cstp/society5_0,(2023-06-30).

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 ,(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

章の目的
第2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

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などを紹介しています。

脅威情報

「情報セキュリティ白書」

「情報セキュリティ10大脅威」

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

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など、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
- 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、インフラシステムなど）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などの事例、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などの活動を知り、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

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、改ざんなどにより、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、法的な制裁や罰金など）

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。

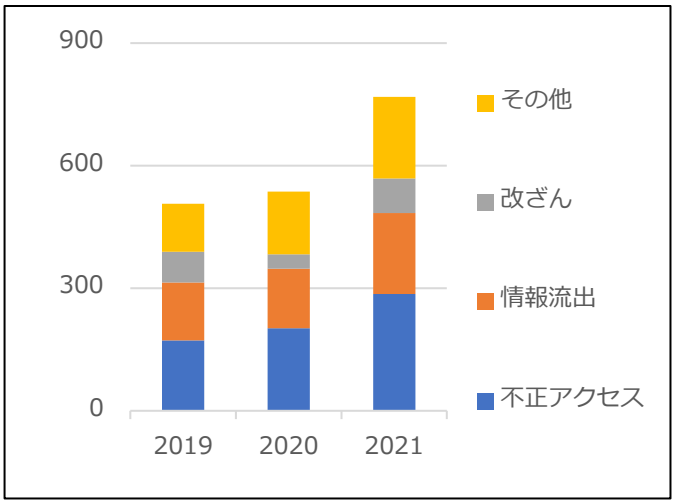


図3. 情報セキュリティインシデント報道件数
(出典) MBSD社による集計情報を基に作成

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%**）

[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).

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	自社にとって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	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。 ・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	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。 ・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」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/ps6vr70000009r2t-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/ps6vr70000009r2f-att/kaisetsu_2023.pdf , (2023-07-06).

2-1-3. IPA：情報セキュリティ10大脅威

1位	**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。
2位	**サプライチェーンの弱点を悪用した攻撃** 直接攻撃が困難な大企業に対し、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：某製造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。
3位	**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などの活動を行います。 事例：某お菓子メーカーは、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。
4位	**内部不正による情報漏えい** 企業の従業員や元従業員などが、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：某住宅メーカーは、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。
5位	**テレワークなど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：某製造メーカーは、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。

(出典) IPA「情報セキュリティ10大脅威」を基に作成

2-1-3. IPA：情報セキュリティ10大脅威

6位	**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：某ベンダーは、ブラウザ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。
7位	**ビジネスメール詐欺による金銭被害** 従業員のメールアカウントを乗っ取り、取引実績がある組織の担当者へ偽の請求などを送りつけ、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。
8位	**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：某食品メーカーは、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。
9位	**不注意による情報漏えいなどの被害** メールの誤送信、記録端末や記録媒体の紛失など、従業員のセキュリティ意識の低さ、不注意によるミスなどによって重要情報を漏えいすることがあります。 事例：某マスコミは、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。
10位	**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サービスなどに不正ログインされることがあります。 事例：某施設運営会社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がダークウェブ上で公開されたことが判明しました。

(出典) IPA「情報セキュリティ10大脅威」を基に作成

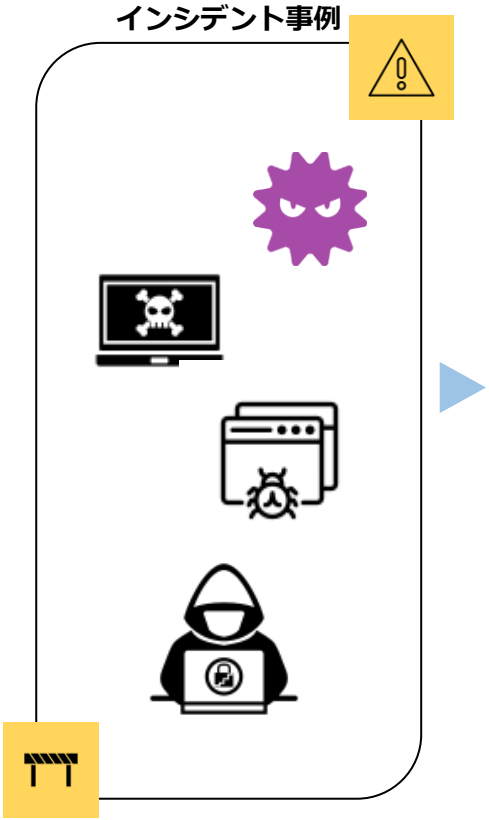
2-2-1. インシデント事例から学ぶ

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

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。

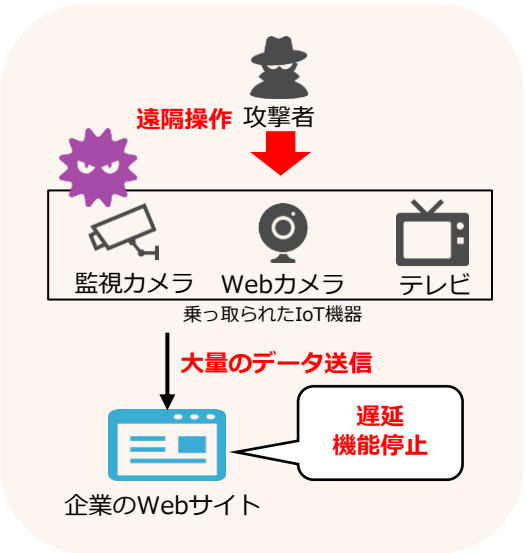


図4. DDoS攻撃の概要図

サプライチェーンによるサービス被害

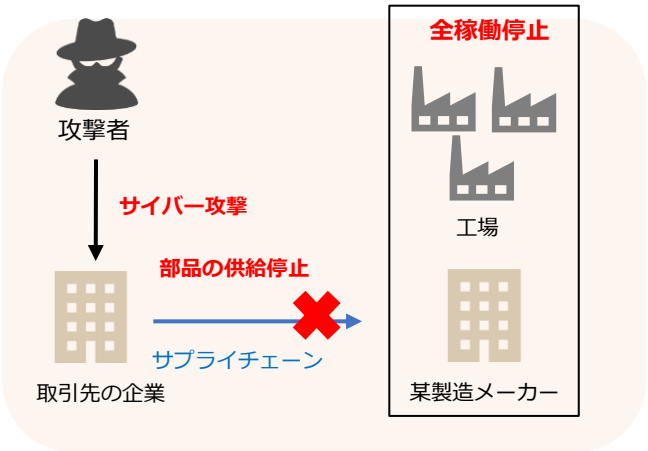


図5. 某製造メーカーで起きたサプライチェーン攻撃の概要図

某製造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、某製造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。

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、某製造メーカーのインシデントが挙げられます。同社は、VPN装置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。

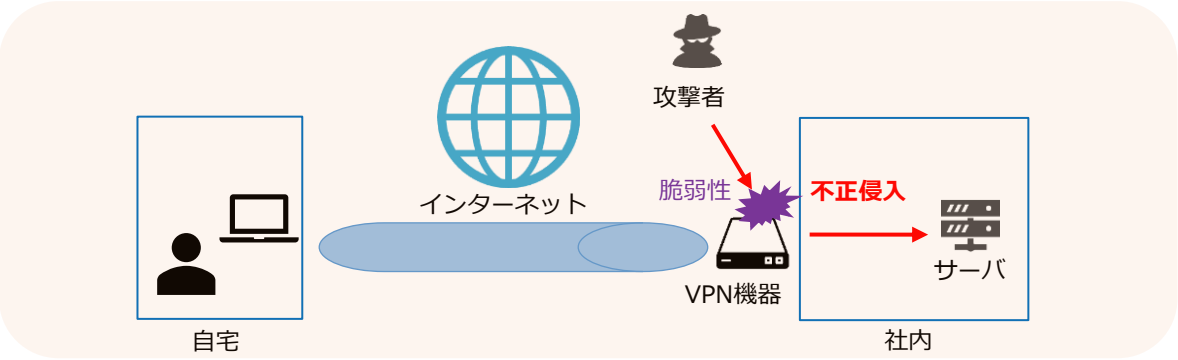


図6. VPN機器の脆弱性を利用した攻撃のイメージ

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などを対象とした「中小企業など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

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。

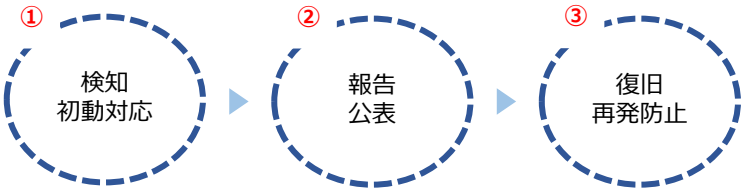


図7. インシデント対応の３ステップ

①検知・初動対応	**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。 **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・再発防止	**調査・対応：** インシデントの原因や影響範囲を詳しく調査し、適切な対応策を策定します。被害の拡大を止めるために適切な措置をとり、被害の影響を最小限に抑えるよう努めます。 **証拠保全：** 事実関係を裏付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。 **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

2-2-4. 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。[4]

【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。

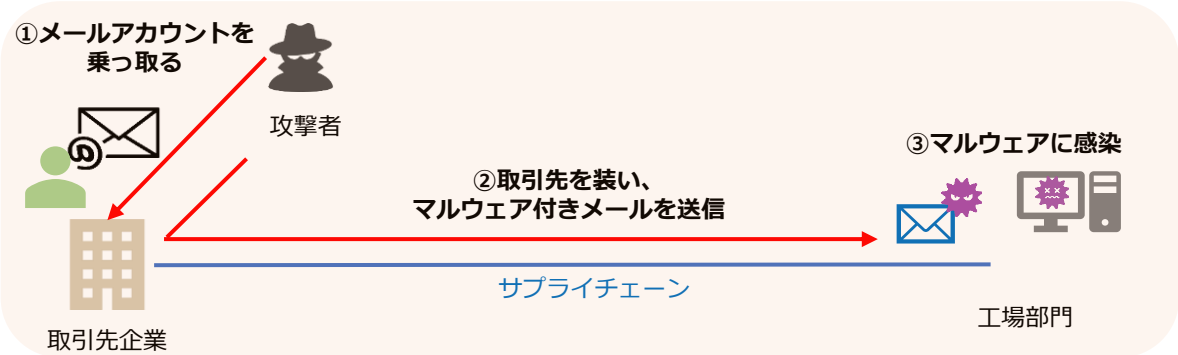


図8. 攻撃の概要図
(出典) NISC「サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）」を基に作成

[4]: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).

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、団体などが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80%に上る割合を占めました。[5]

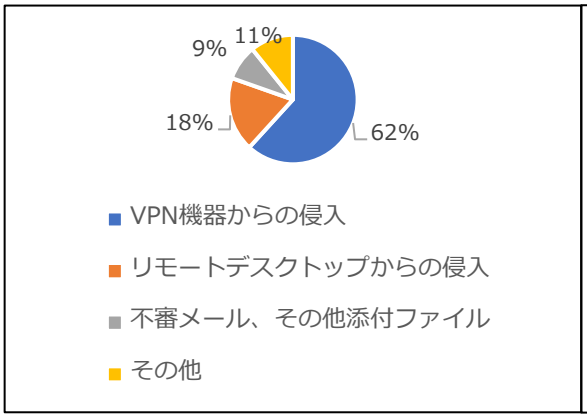


図9.（令和４年）ランサムウェアの感染経路

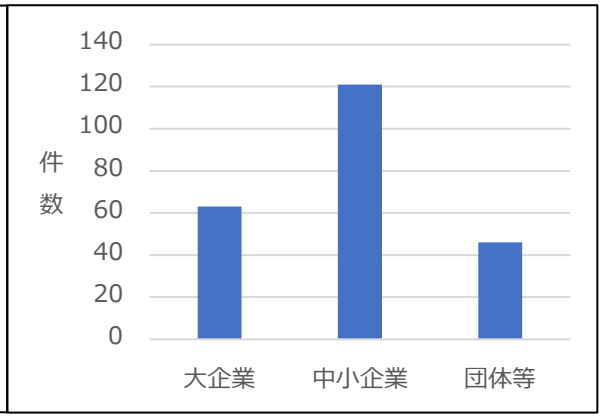


図10.（令和４年）ランサムウェアの被害件数

（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。

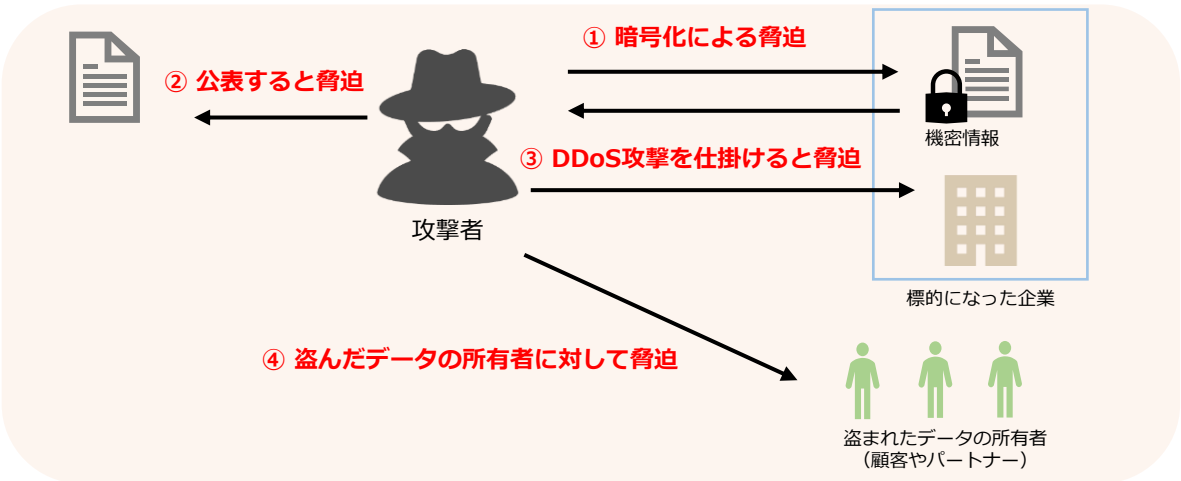


図11. ランサムウェアの二重、四重脅迫のイメージ図

[5]: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).

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（某製造メーカー）

事例の概要
サーバが第三者による不正アクセスを受け、個人情報が漏えいし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。

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、ログの保存などが重要です。

多数システムでランサム被害（某組合）

事例の概要
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、数十万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。

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の導入など、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

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。[6]

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、利用用途の変更なども考慮し、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。

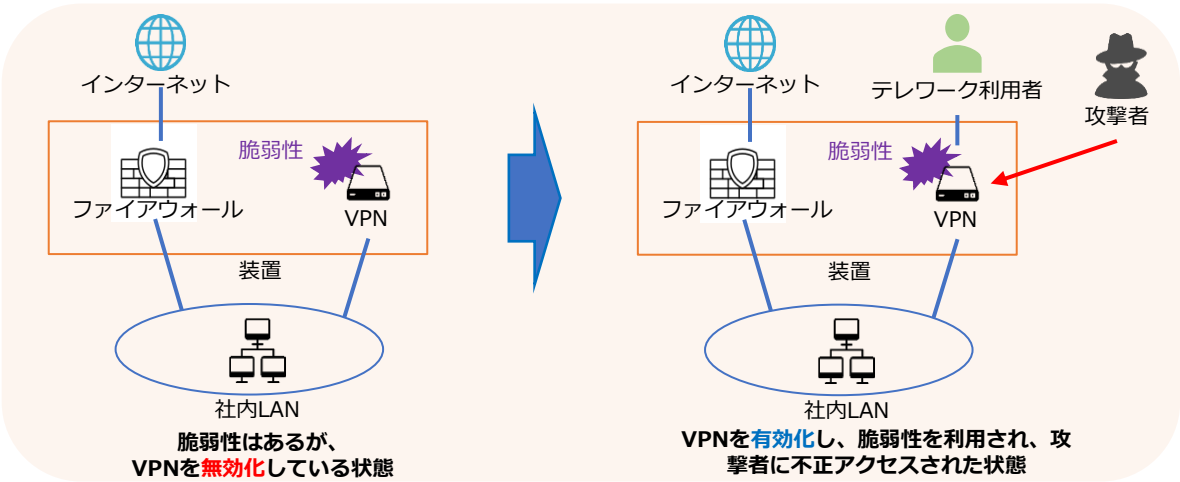


図12. 攻撃の概要図
(出典) IPA「コンピュータウイルス・不正アクセスの届出事例［2022年下半期（7月～12月）］」を基に作成

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

2-3-2. 事例：某病院のランサムウェア被害

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、電子カルテなどの端末と関連するサーバのデータが暗号化され、患者の診察記録が閲覧できなくなり、病院の機能は停止しました。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、警察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、数か月後に通常の診療を再開することができました。

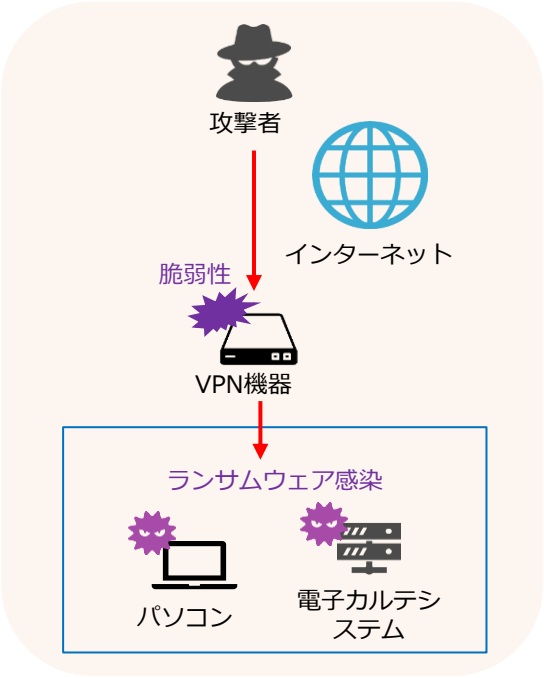


図13. 攻撃の概要図

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、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

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。

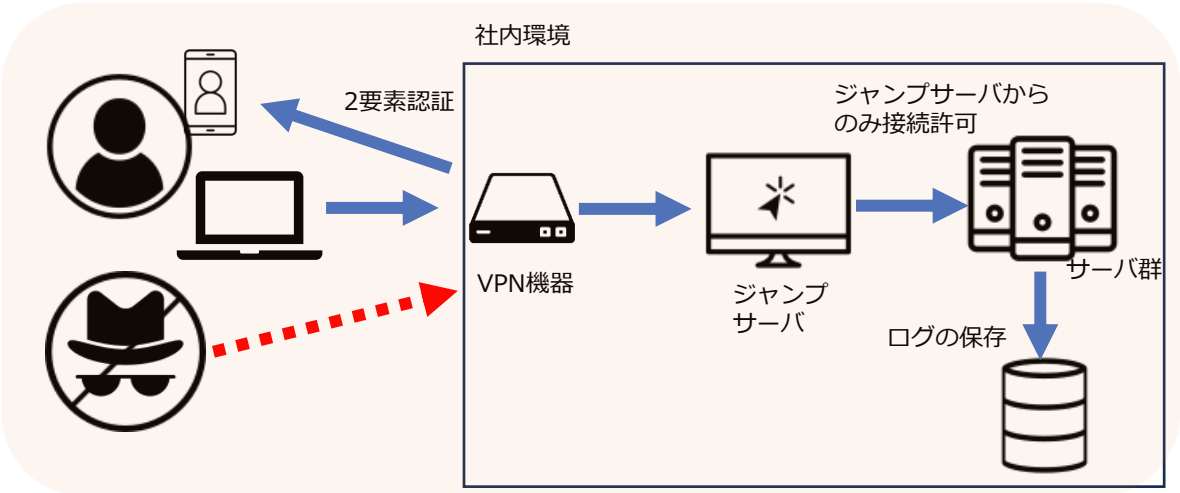


図14. 対応策の概要図

実施するべき対策と運用

- 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

章の目的
第3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
◘ サイバーセキュリティに関する基礎知識を身に付ける方法を確認すること
◘ 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

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。

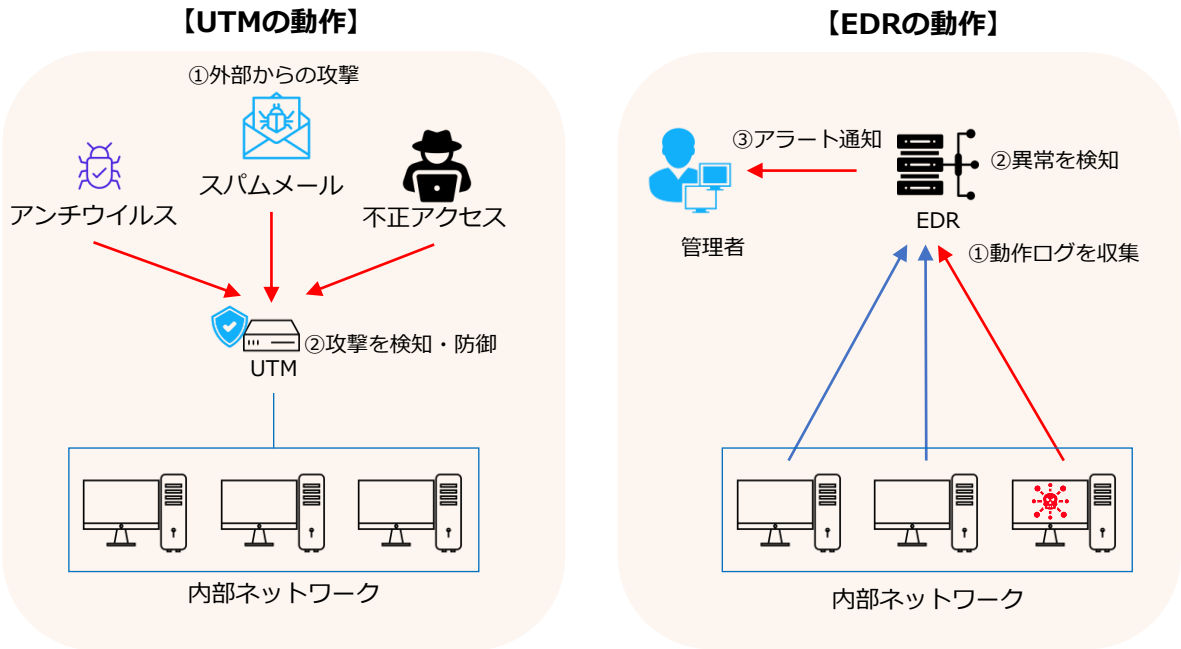


図15. UTM、EDRの概要図

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、そして活用方法などを紹介します。

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。

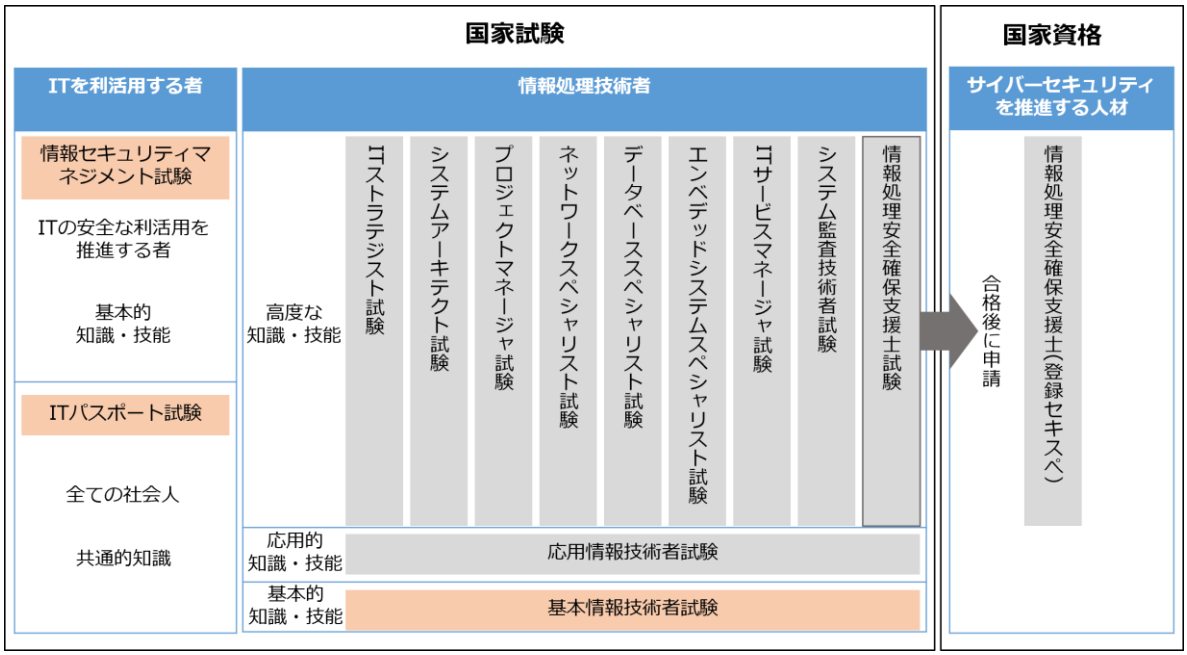


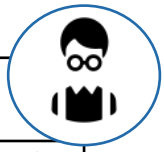
図16. 情報処理技術者試験の一覧
(出典) IPA「試験区分一覧」を基に作成

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

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、すべて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。[7]

ITパスポート試験（IP）



対象者	ITを利活用するすべての方（ITを使う社会人や学生など）
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・法務など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	・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など様々なリスクがあることを理解できるようになります。 ・知的財産権など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・商標権侵害などの法令違反や個人情報漏えいなど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	・業務で個人情報を取扱うすべての方 ・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・確認を行うすべての方 ・情報セキュリティ管理の知識・スキルを身につけたいすべての方 ・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すべての方
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	・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

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

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	・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

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[8]

★一つ星	「情報セキュリティ5か条」に取組むことを宣言
★★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,(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/

[8]: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).

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」などは使わず、推測できないようにします。
４．共有設定を見直そう！ データ保管などの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・カメラなど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など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など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

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

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	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなど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など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など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への書き込みなど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、書庫など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など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など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サイトの運用など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など準備をしていますか？
	25	情報セキュリティ対策（上記 1 ～ 24 など）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

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。したがって、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・犯罪などの脅威から守り、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
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・ガイドラインなどの遵守 / セキュリティ対策の実施 / 継続的改善など

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）

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）「O:あり / △：部分的にあり / ×:なし」

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

Lv2. ベースラインアプローチ		網羅性	即時性
ベースラインアプローチは、セキュリティ対策の基準やガイドラインを定義することにより、組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指します。ただし、追加のセキュリティ対策やリスクに対する適切な対応策を検討し、網羅的なアプローチを推進することが必要となります。 ・セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保 ・網羅的なアプローチの出発点		△	△
1. ベースラインの定義	セキュリティの基準となるベースラインを定義します。活用できる文書/ツール、内部のセキュリティ目標など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などにより、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、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など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。

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）「O: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		O	×
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、教育など）、技術的な対策（アクセス制御、暗号化など）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、暗号化などが含まれます。情報セキュリティは、デジタルだけでなく、紙の文書などの非デジタル情報にも関連しています。また、3要素に加えて、真正性（Authenticity）、責任追跡性（説明責任）（Accountability）、否認防止性（Non-Repudation）、信頼性（Reliability）を合わせて情報セキュリティの7要素と呼ぶこともあります。

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

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

第4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

4-1.これからの企業経営で必要な観点：社会の動向

4-2. 守りのIT投資と攻めのIT投資

4-3. 経営投資としてのサイバーセキュリティ対策

章の目的
第4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、経営投資としてのサイバー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繋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
◘ 経営投資としてのサイバーセキュリティ対策の重要性を理解すること

4-1-1. 現実社会とサイバー空間の繋がり

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1997年には9.2%でしたが、2022年には84.9%まで上昇しました。急速なITの普及により、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革をもたらしています。

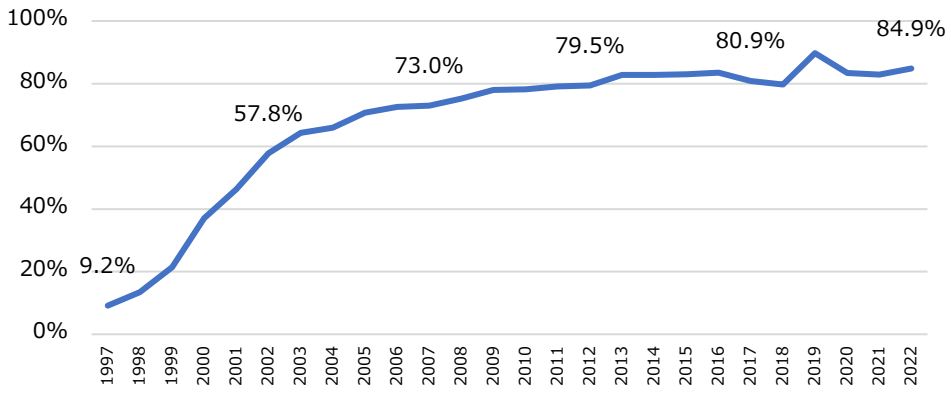


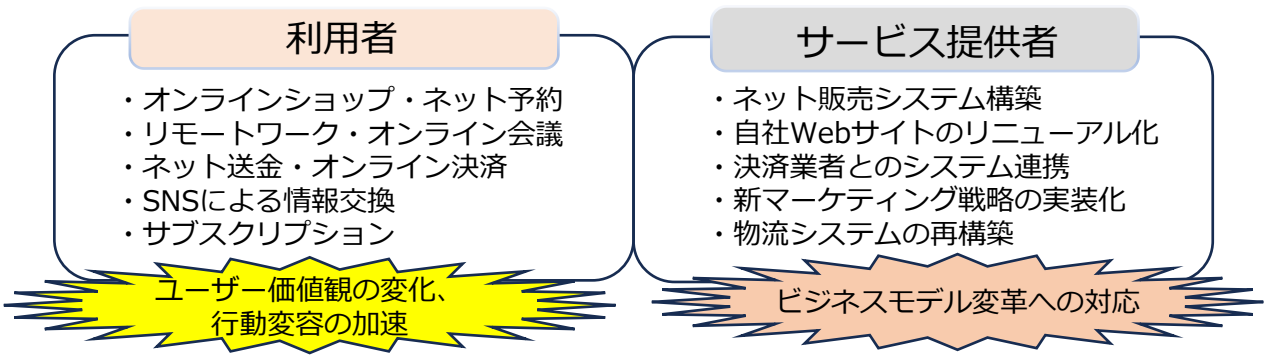
図17. インターネット利用率（個人）の推移
（出典） 総務省「通信利用動向調査」を基に作成

ITの普及により、サービスの利用者はより価値のあるサービスを選択することが可能になりました。たとえば、インターネットを介して情報を瞬時に入手したり、オンラインショッピングで広範囲の商品を比較したりすることができます。このように、より便利で効率的な方法でサービスを利用できるようになりました。

さらに、スマートフォンなどの普及により、利用者の意見や情報が即座に国境を超えて広がることが可能になりました。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。これにより、社会の意識形成や情報伝達において、ITの役割がより大きくなっています。

一方で、ITサービスの提供者は、新たなサービスの提供が日々求められます。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。それに伴い、企業の経営戦略やビジネスモデルも変化しており、革新的なアイディアと素早い行動が求められる時代と言えます。

また、今後の社会では、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）が提唱されています。



4-1-1. 現実社会とサイバー空間の繋がり

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、サイバー空間との繋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、フィジカル空間だけでなく、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繋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。

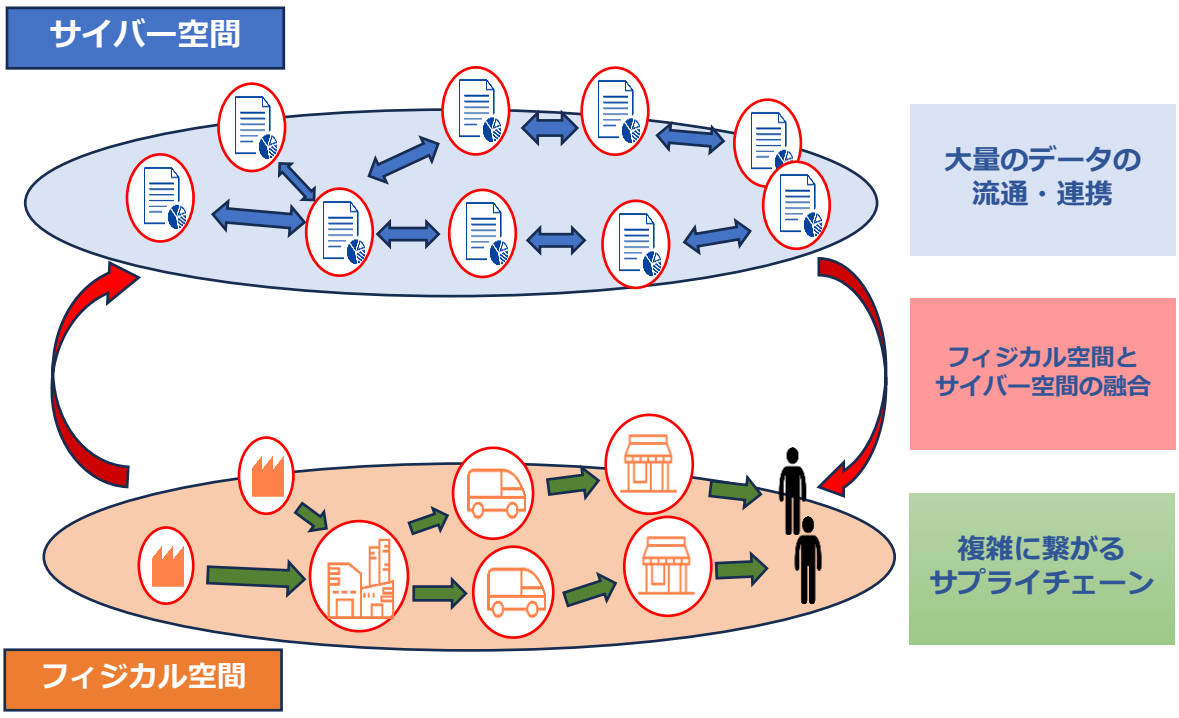


図18. サイバー空間とフィジカル空間の関係図
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

4-1-2. 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。様々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。[9]
ここでは日本社会がデジタル化で後れを取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取った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. 業務改革などを伴わない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更なる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のが「情報セキュリティやプライバシー漏えいへの不安があるから」（52.2%）でした。また、パーソナルデータの企業などによる不適切な利用、インターネット上に流布する偽情報への対応、慣れないデジタル操作などへの習熟など、様々な要因により、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のが「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」を基に作成

[9]: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, (2023-07-25).

4-1-2. IT活用における課題

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に取組んでいる企業の割合は2021年度調査の55.8%から2022年度調査では69.3%に増加、2022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。

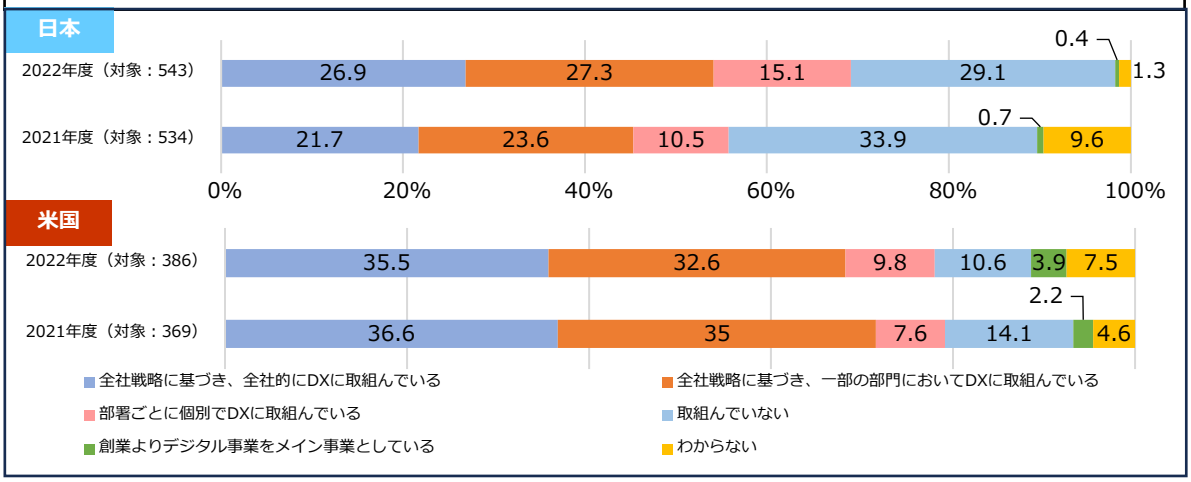


図19. DXの取組状況
（出典）IPA「DX白書2023」を基に作成

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2021年度調査の49.5%から2022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。

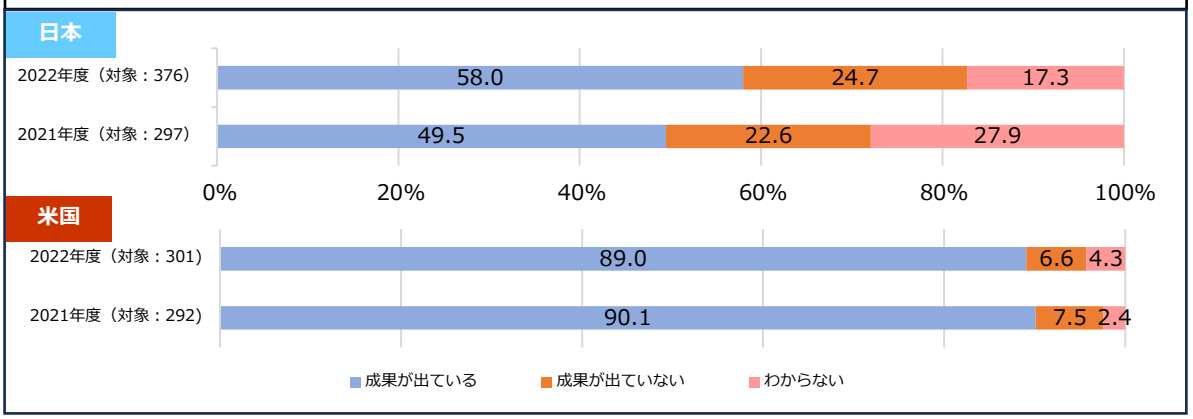


図20. DXの取組の成果
（出典）IPA「DX白書2023」を基に作成

4-2-1. 守りのIT投資、攻めのIT投資の概要

企業のIT投資は、「攻め」と「守り」の2種類に分けて論じられることがあります。「攻めのIT投資」とは、ITを活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規顧客獲得、収益拡大、販売力のアップを目指すことです。一方、「守りのIT 投資」とは、ITによる業務の効率化やコスト削減を目的としています。IT投資に攻めと守り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、従来より「攻めのIT投資」に重点を置くとよいでしょう。

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」（デジタルトランスフォーメーション）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組み方や活用方法を含めて紹介します。

「守りのIT投資」
（デジタルオプティマイゼーション）
目的：生産性向上

・業務の効率化
・コストの削減

「攻めのIT投資」
（デジタルトランスフォーメーション）
目的：ビジネス継続・競争力強化

・新たなビジネスの展開
・顧客視点で新たな価値の創造

One Point

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（デジタルトランスフォーメーション）
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21. 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」を基に作成

4-2-2. 経済産業省のDXレポートから見る、「攻めのIT」に取組む方針について

2025年の崖

「2025年の崖」とは、経済産業省が2018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、2025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システムを巡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。[10]

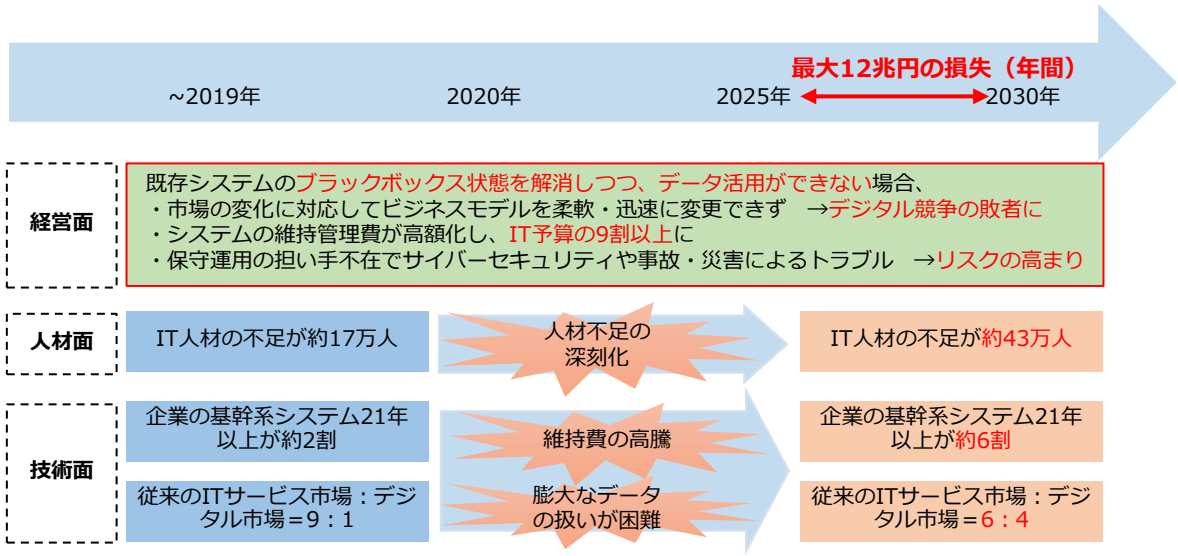


図22.「2025年の崖」の概要図
（出典）経済産業省「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」を基に作成

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

[10]: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, (2023-07-12).

4-2-3. 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一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

たとえば請求業務はこれまで、表計算ソフトウェアや紙などを使用して手作業で業務を行ってきましたが、その業務には時間がかかってしまう課題が生じていました。そこで、たとえば電子契約サービスを導入することで、紙で文書を作成し、その文書に直接押印するというプロセスを省くことができ、業務プロセスを効率化することが期待できます。この改善により、従来の業務にかかっていた時間を短縮し、その削減された時間を他の業務に充てることが可能になります。

デジタル活用するための環境整備

デジタルトランスフォーメーションを実現するには、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、将来的にデジタルトランスフォーメーション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付けを行い、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。

4-2-3. 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）

事例：某エンジニア商社（東京都・製造業）

東京のオフィスに通勤していましたが、新型コロナウイルスの影響により、テレワークへの切り替えを迫られました。書類処理のため、交代で出社しなければならない問題がありましたが、出社が必要な業務をRPAに切り替えていくことができたため、暫定的にテレワークに移行することができました。その後、問題が特に生じなかったため、三つの拠点を一つに統合し、一つの拠点とテレワークに集約することができました。

手順１：業務内容・業務フローの可視化
問題となる業務は、「会社に出社し、お客様や仕入れ先様からFAXで届いた見積書や注文書に対して、紙で返信する業務」であることが判明しました。
手順2：削減・短縮可能な業務の洗い出し
紙ベースの書類を電子データに切り替えることで、出社する手間を削減しました。
手順3：改善や対応の実施
RPAを導入し、FAXデータをPDFファイルに変更しサーバに保存することで、パソコンからどこからでもアクセス可能になりました。
手順4：業務改革の実現
出社する必要が激減し、完全テレワークが実現しました。

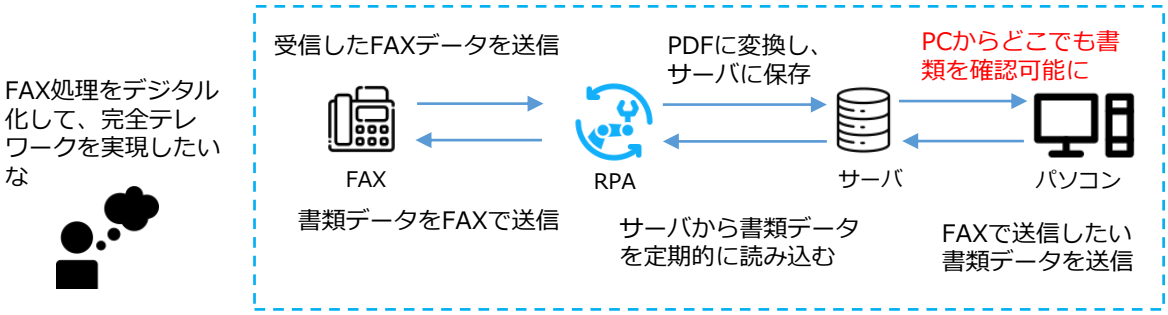


図23. RPAのイメージ図

4-2-4. ITを活用した新たなビジネスの展開（デジタルトランスフォーメーション）

「攻めのIT投資」：デジタルトランスフォーメーション

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」だけでなく、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するデジタルトランスフォーメーションを推進させるため、「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」によってデジタルトランスフォーメーションを推進させ、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、全社的に取組める体制を整えます。

手順3：デジタル技術・業務改革による課題の解決

デジタル技術の活用や業務プロセスの見直し、企業文化の改革などにより、課題を解決していきます。

手順4：顧客に新たな価値を提供・他社のDXに貢献

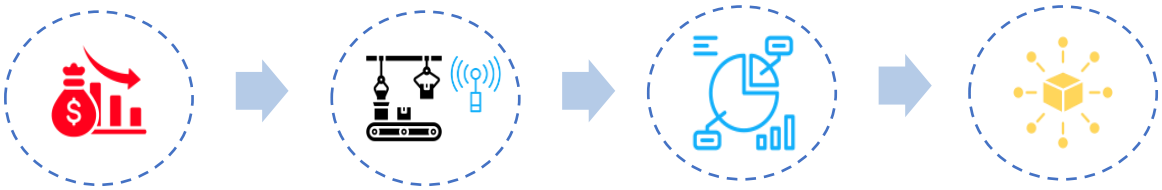
新たな価値を創出し、顧客に提供します。さらに、サプライチェーン全体に対しても貢献していきます。

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

4-2-4. ITを活用した新たなビジネスの展開（デジタルトランスフォーメーション）

事例：某金属製作所（大阪府・製造業）

2008年の米金融危機により受注が半減し、従来の受注を待つだけの機械加工ではビジネスの継続が困難であるという危機感から、自らサービスを提供できるビジネスモデルへの転換に着手しました。自社の機械加工プロセスのデータを分析することで、新規事業の展開に繋がりました。結果、自社の経営を立て直し、自社だけでなく、他社のものづくりを担う人材を育成することに貢献できるようになりました。[11]



（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」を基に作成

手順１：実現したいことを明確にする
ビジネスモデルを、受注を待つだけでなく自らサービス提供していくモデルへ転換することに設定しました。
手順2：課題の明確化、関係者の意識改革を実施する
機械加工による製品の開発や販売だけでなく、自ら市場を開拓できるような新たな価値の創出を課題として挙げました。
手順3：デジタル技術による、課題解決
機械加工を行う機器にデータを計測するセンサーをつけ、加工データをリアルタイムで計測してデータを抽出し分析して得た情報をもとに、新規事業の展開に繋げました。
手順4：顧客に新たな価値を提供・ビジネスモデルの転換
機械加工の現場における生産性の向上や品質の改善、人材の育成などの課題を解決するサービスを提供できるようになり、受注だけに頼らないビジネスモデルを構築できました。

[11]: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". https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf, (2023-07-10).

4-2-5. 次世代技術を活用したビジネス展開

デジタルトランスフォーメーションを推進していく際、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、既にデジタルトランスフォーメーション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な

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、学習したデータを元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	現実世界の様々なモノが、インターネットと繋がることです。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繋がります。	• 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、様々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可能。リモートワーカーや複数拠点のチームとの協業がしやすくなる

4-2-5. 次世代技術を活用したビジネス展開

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自社の課題に対して、どのようにデジタル技術を活用して解決し、競争力を強化しているのか紹介します。

事例1：ユニット型制御基板製造企業（愛媛県・製造業）

課題	システム開発において、設計時に仕様変更がかなり多く、適切な情報共有ができないため、製造工程のやり直しや製品の品質低下の恐れがあること。
解決への取組	社内SNSとしての機能を備え、情報共有がしやすく、簡単にシステムを構築できるクラウドサービスを導入しました。それにより、システムを短期間で開発することが可能となり、業務の変化に応じて修正を即座に反映できるようになりました。その結果、情報の共有、工程管理の効率化を実現しました。さらに、この一連の経験を同じ地域の製造業者に共有するために、他の企業と協力してワークショップを開催しました。その結果、ある企業から、効率化システムのコンサルティング、開発の依頼を受注することができました。これらの経験を生かし、地域のDX推進事業をビジネスとすることを目指しています。

（出典）経済産業省 「DX Selection 2022」を基に作成

事例2：マッシュルーム生産販売業（山形県・農業、販売業）

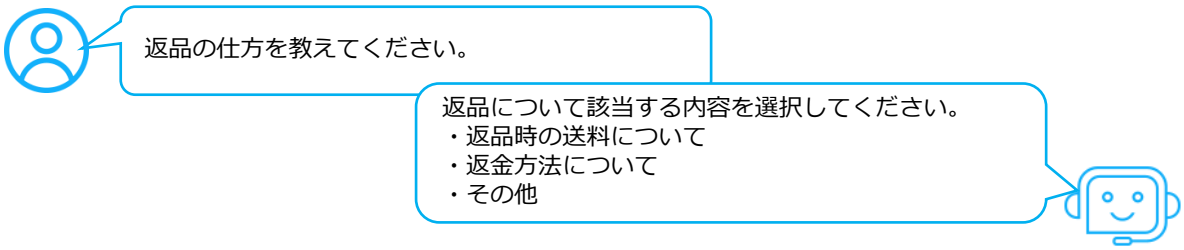
課題	「つくる力」と「とどける力」を将来にわたってさらに強化するために、管理面の強化を行うこと。
解決への取組	作業の安全性や生産性の向上、栽培作業の平準化を目的に栽培ハウスの温湿度やCo2などの栽培環境の点検作業をIoTを用いて自動化することにしました。IoT導入にあたり、電子機械に詳しい人材を確保し、機器の設置や保守、従業員へのIoTに関する知識の向上や理解を深める指導を行いました。また、システムの使い方を担当者に熟知してもらうために、IoT機器を設置するだけでなく、どのように活用するかの検証やマニュアルづくりを、実際に現場で作業する人員と一体となって進めました。結果、栽培ハウスの点検システムの自動化により、リアルタイムで栽培ハウスのデータを把握でき、勘と経験に頼らない栽培作業の平準化が可能になりました。また、測定で得られたデータをAIを用いて分析することで、最適な栽培条件を絞り込み、マッシュルームの品質向上、栽培作業の平準化、生産量の増大が期待できるようになりました。

（出典）経済産業省 「DX Selection 2023」を基に作成

4-2-5. 次世代技術を活用したビジネス展開

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。たとえば、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、様々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。

4-3-1. サイバーセキュリティ対策の重要性

デジタルトランスフォーメーション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だけでなく、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、デジタルトランスフォーメーション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、サイバー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を被ってしま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、デジタルトランスフォーメーションの推進と並行してサイバーセキュリティの確保に取組むことが重要です。

サイバー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、サイバー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、経営者目線でサイバー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。

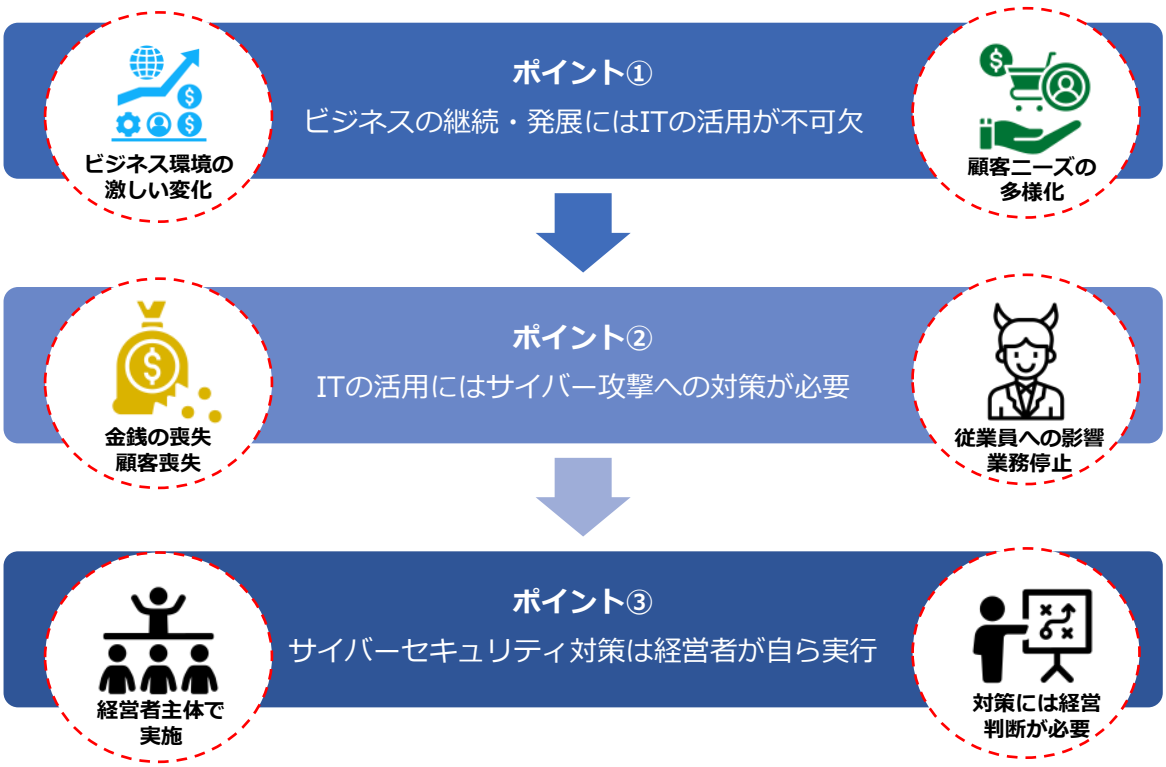


図24. ITの活用とサイバーセキュリティ対策の関係性
（出典） 東京都産業労働局.” MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響”.
https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/201/index.html,(参照 2023-07-10).

4-3-2. 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、デジタルトランスフォーメーション（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

ITの活用が不可欠な中、サイバーセキュリティ対策を行うことが必須となっています。サイバーセキュリティ対策を怠ることで、金銭・顧客の喪失、法的責任、事業の中断・停止、従業員への悪影響など、経営を揺るがすような被害を引き起こす可能性があります。近年は、サプライチェーンを介して、セキュリティ対策が不十分な企業を踏み台にして攻撃されることもあります。攻撃を受けた企業だけが責任を追及されるだけでなく、踏み台にされた企業も加害者として責任を追及されてしまいます。

事例：サプライチェーン攻撃による情報流出被害
保険業界

某保険会社は、顧客情報の一部が流出したことを公表し、謝罪しました。情報流出の原因としては、外部委託先の企業のサーバが不正アクセスを受けたことです。顧客の氏名、性別、生年月日、メールアドレスなどの個人情報が数十万人分漏えいしてしまいました。その結果、数億円以上の損害や多くのお客様に対する信頼を低下させてしまう事態となりました。このようにサプライチェーンを介した攻撃では、自社が直接サイバー攻撃を受けていなくても、間接的に被害にあってしまいます。

4-3-2. 経営者が重要視すべき3つのポイント

ポイント3：サイバーセキュリティ対策は経営者が自ら実行

経営者は自ら主体となって指揮をとり、サイバー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、サイバー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、会社及び第三者に対する、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、会社及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	故意または過失によって他人の権利また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25. 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。この他にも、法律によっては違反などが発生した場合、経営者だけでなく、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、サイバーセキュリティ対策は経営者が主体となって取組むことが大切です。

第5章. デジタル社会の方向性と実現に向けた国の方針

5-1. 国の基本方針および実施計画の要約

5-2. 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

章の目的

第5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サイバーセキュリティ対策の重要性を理解すること

5-1-1. 経済財政運営と改革の基本方針2023

国の方針の一つである「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及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。2023年の骨太の方針では、本文中だけで50回以上「デジタル」という言葉が使われており、デジタル技術の活用やデジタル社会の構築に向けた変革が重要な課題になっていることがわかります。

ここでは、2023年に策定された基本方針の中から、「新しい資本主義の加速」を構成する「投資の拡大と経済社会改革の実行」に掲げられているいくつかの施策において、特にIT戦略に関係する内容について説明します。

投資の拡大と経済社会改革の実行（2023年度方針）

①官民連携による国内投資拡大と**サプライチェーンの強靭化**
②GX、**DXなどの加速**
③スタートアップの推進と新たな産業構造への転換、インパクト投資の促進
④官民連携を通じた科学技術・イノベーションの推進
⑤インバウンド戦略の展開

IT戦略に関係する施策例

サプライチェーンの強靭化

国際環境の不確実性が増す中にあって、海外からヒト、モノ、カネ、アイデアを積極的に呼び込むことで、国内全体の投資を拡大させ、イノベーション力を高めることを目指します。特に、次世代半導体を含めたグローバルサプライチェーンの中核となることを目指し、政府を挙げて投資拡大に取組んでいきます。 ITは、サプライチェーンを支える重要な役割になると同時に、セキュリティリスクへの対策も併せて重要です。

DXの加速

新型コロナウイルス感染症が拡大したことによって、日本国内において様々な課題が浮き彫りとなりました。デジタル化やオンライン化の遅れもその一つであり、2020年度の「経済財政運営と改革の基本方針」以降、DX（デジタルトランスフォーメーション）の推進が謳われるようになりました。2023年度の方針においても同様に、DXの加速が謳われています。

DXへの対応については、デジタルの力を活用して国が地方を支える事を目指しての行政サービスの見直しや、マイナンバーカードの制度における安全・信頼確保および利便性・機能向上への取組などが掲げられています。また、中堅・中小企業の活力を向上させるため、DX、人手不足などの事業環境変化への対応を後押しすることが明記されています。

また、「サイバーセキュリティ戦略」に基づく取組を進める旨が記載されており、日本のDX方針にサイバーセキュリティの観点が組み込まれている事が確認できます。中堅・中小企業に対して、インボイス制度の円滑な導入、サイバーセキュリティ対策を支援することが謳われています。サイバーセキュリティ戦略の詳細については後述します。

（出典）内閣府「経済財政運営と改革の基本方針 2023」を基に作成

5-2-1. 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。 [12]

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、様々な課題を解決し、豊かさを真に実感できる「誰一人取り残されない」デジタル社会を目指す。
5. デジタル人材の育成・確保 全国民が当事者であるとの認識に立ち、ライフステージに応じた必要なICTスキルを継続的に学ぶことで、デジタル人材の底上げと専門性の向上を図り、デジタル人材が育成・確保される社会を目指す。
6. DFFT（Data Free Flow with Trust）：「信頼性のある自由なデータ流通」の推進を始めとする国際戦略 国際連携を図ることで、データがもたらす価値を最大限引き出し、国境を越えた自由なデータ流通が可能な社会を目指す。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

[12]: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, （2023-07-28）.

5-2-1. デジタル社会の実現に向けた重点計画

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み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組みます。

1. サイバーセキュリティの確保

・ 2023年度（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。

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

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」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

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

事業者向け行政サービスの質の向上に向けた取組

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

（出典） デジタル庁「デジタル社会の実現に向けた重点計画」を基に作成

5-2-1. デジタル社会の実現に向けた重点計画

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」を基に作成

5-2-2. 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、様々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、一人ひとり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様々な形で、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。[13]

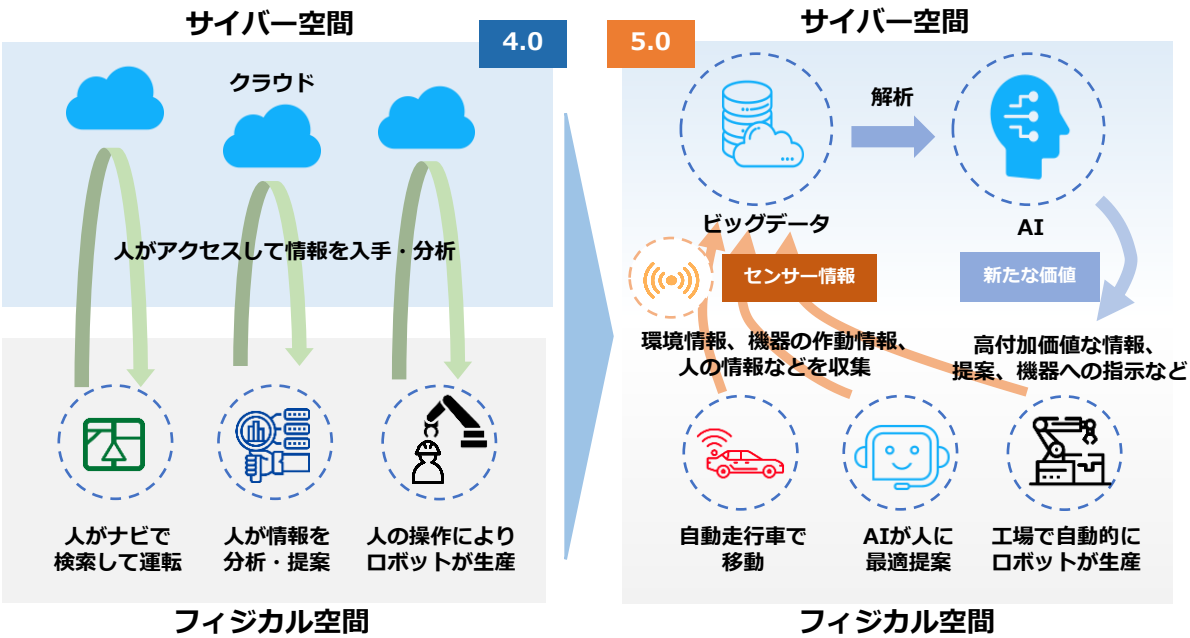


図26. Society4.0とSociety5.0の比較
（出典）内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

[13]:内閣府.“Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

5-2-2. 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。たとえば、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繋がります。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
複雑に繋がる 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」を基に作成

Society5.0の進展に伴い、サイバー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サイバー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。

5-2-3. DXの推進

デジタルトランスフォーメーション（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。デジタルトランスフォーメーションとは、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、デジタルトランスフォーメーションを推進し、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、積極的にデジタルトランスフォーメーションに取組むことで、大きく成長できる可能性があります。以下では、デジタルトランスフォーメーションを推進する際に、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組んでいる企業の事例を紹介します。

中小企業がデジタルトランスフォーメーション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、デジタルトランスフォーメーション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

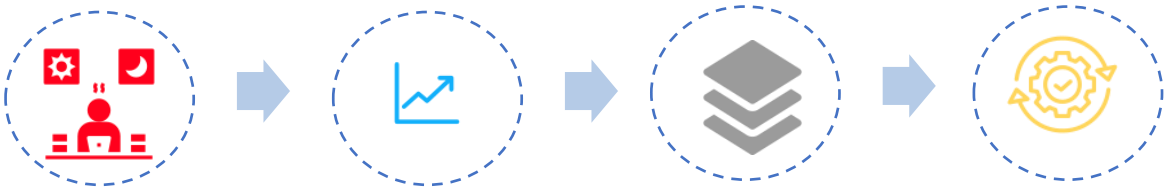
環境の変化に素早く対応しやすい

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だけでなく、各部署のデータが繋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」を基に作成



皆が懸命に働いているが収益が上がらず、賃金を上げられない

従業員の可処分所得３％向上を目指す。そのために生産性を130%に高めることを目指す

産学官連携で開発された中小企業向けシステムプラットフォームを導入

基幹システムが刷新され、業務・組織の変革に効果が出始める

5-2-3. DXの推進

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）：製造メーカー

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・可視化出来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指導を実施したり、AIによるデータ解析によって使いやすい製品の設計・開発にいかすことが可能となりました。

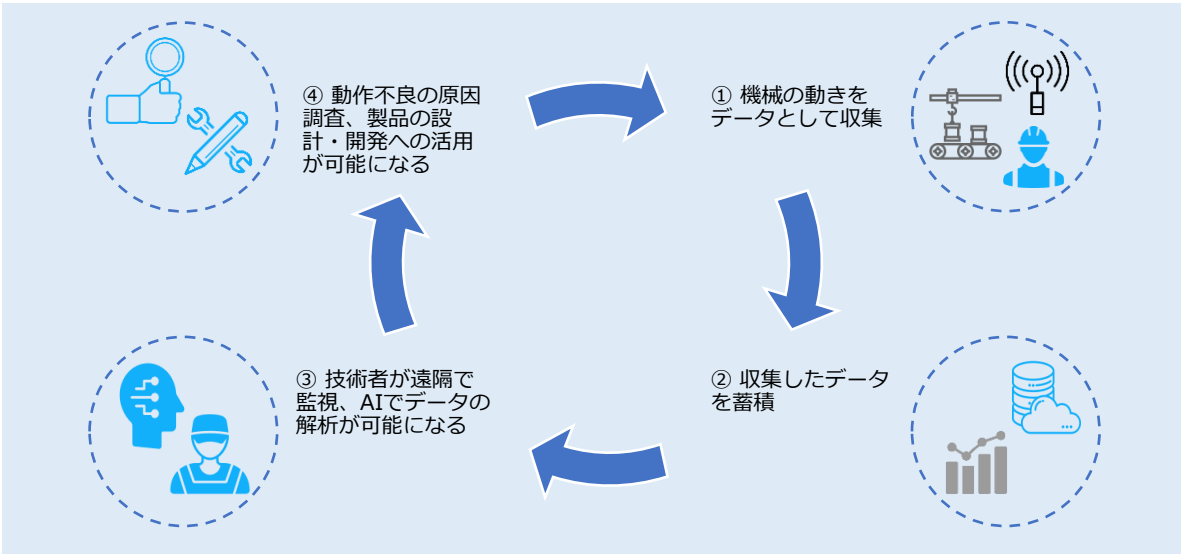


図27. データ活用による業務改革の流れ
（出典）IPA"製造分野のDX事例集".
https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf,
（参照 2023-07-28）.

5-2-3. DXの推進

DX with Cybersecurityの概要

デジタルトランスフォーメーション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、デジタルトランスフォーメーションを推進することは、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。したがって、デジタルトランスフォーメーションを推進すると同時に、サイバー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。

デジタルトランスフォーメーションの推進によって、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。したがって、サイバー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6章. サイバーセキュリティ戦略および関連法令

6-1. NISC：サイバーセキュリティ戦略

6-2. 関連法令

章の目的
第6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

6-1-1. サイバーセキュリティ戦略

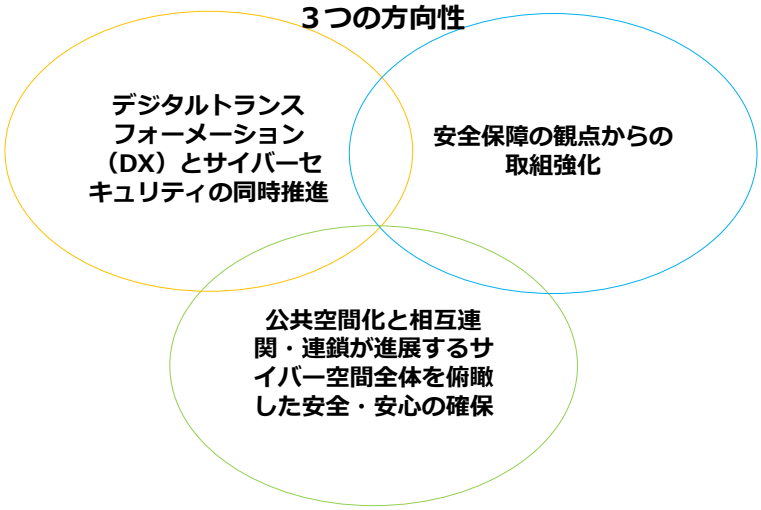
サイバーセキュリティ戦略とは、国家レベルでサイバーセキュリティの確保に取組むための基本的な方針や目標を定めたものです。日本においては、内閣サイバーセキュリティセンター（NISC）が、サイバーセキュリティ戦略の策定や実施に関する総合調整役を担っています。現行のサイバーセキュリティ戦略は、2021年9月28日に閣議決定され、「今後3年間に執るべき諸施策の目標や実施方針を示す」ものとされています。この戦略に基づき、政府はサイバーセキュリティの確保に向けた取組を進めています。

サイバーセキュリティ戦略の課題と方向性

2020年代を迎えた日本を取り巻く時代認識：「ニューノーマル」とデジタル社会の到来
（デジタル改革の推進、新型コロナウイルスの影響、SDGsなど）
サイバー空間をとりまく課題認識：国民全体のサイバー空間への参画
（サイバー攻撃の巧妙化、サイバー空間の公共化、現実世界との相互連関など）

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

３つの方向性



「自由、公正かつ安全なサイバー空間」の確保

図28.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」を基に作成

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、サイバー空間とは繋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共に「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。

6-1-1. サイバーセキュリティ戦略

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様々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おそれがある

・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、更なる取組を促進

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組
・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」を基に作成

6-1-1. サイバーセキュリティ戦略

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、様々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

（1）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

（2）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

（3）経済社会基盤を支える各主体における取組

① 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
② 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
③ 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）

（4）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」を基に作成

6-1-1. サイバーセキュリティ戦略

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

・我が国をとりま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

課題に対する具体的施策

主な具体的施策

（1） 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）

（2）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（サイバー攻撃の更なる実態解明の推進）

（3） 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」を基に作成

6-1-1. サイバーセキュリティ戦略

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、普及啓発に取組んでいくことが重要です。

サイバーセキュリティ戦略の３つの方向性

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	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

上記の推進に向け、
横断的・中長期的な視点で、研究開発や人材育成、普及啓発に取組む

- **研究開発の推進**
  産学官エコシステム構築とともに、それを基盤とした実践的な研究開発推進
  （1）国際競争力の強化・産学官エコシステムの構築（研究・産学官連携振興施策の活用など）
  （2）実践的な研究開発の推進（サプライチェーンリスクへの対応、攻撃把握・分析・共有基盤、暗号などの研究推進など）
  （3）中長期的な技術トレンドを視野に入れた対応（AI技術の進展、量子技術の進展）

- **人材の確保・育成・活躍促進**
  （1）DX with Cybersecurityの推進（「プラス・セキュリティ」知識を補充できる環境整備など）
  （2）巧妙化・複雑化する脅威への対処（人材育成プログラムの強化、資格制度活用など）
  （3）政府機関における取組（外部高度人材活用の仕組み強化など）

- **全員参加による協働・普及啓発**
  テレワークの増加やクラウドサービスの普及など、近年の人々の行動や企業活動の変化に応じて、ガイドラインや様々な解説資料などの整備の推進

（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」を基に作成

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他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。

6-1-1. サイバーセキュリティ戦略

サイバーセキュリティ2023

NISCは、サイバーセキュリティ戦略に基づく今年度の2022年度年次報告・2023年度年次計画を整理した「サイバーセキュリティ2023」を策定しています。サイバーセキュリティ戦略に基づく施策を的確に実施するため、各年度の施策の進捗状況を検証し、次年度の計画に反映することとしています。

2023年度の「サイバー空間を巡る状況変化と情勢、及び政策課題」と「今後の取組の方向性（今年度特に強力に取組む施策について）」は以下の通りです。

サイバー空間を巡る状況変化と情勢、及び政策課題

- **昨今の状況変化**
  - ・サイバー空間への依存度の高まり/情報システムの利用拡大/サプライチェーンの多様化・複雑化の進展/生成AIなどの新たな技術普及
  - ・新たな技術・サービスの普及に伴うサイバー攻撃を受けるシステム側の侵入口（セキュリティホール）増加
  - ・サイバー攻撃手法の変化（深刻化・巧妙化）/サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取
- **サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～**
  - ・ランサムウェアが依然とした脅威、不正プログラムEmotetが活動と停止の繰り返し/暗号資産交換業者もサイバー攻撃の対象
- **昨今の状況変化を踏まえた政策課題**
  - ・政府による「国家安全保障戦略」の策定：サイバー空間の安全かつ安定した利用、特に国や重要インフラなどの安全などを確保
  - ・実効的なサイバーセキュリティ対策を実現するための課題：①各主体による対策の強化・対処能力の向上/②政府による支援などの充実・強化/③国際連携・協力の強化が政策課題に

今後の取組の方向性（今年度特に強力に取組む施策について）

1. 経済社会の活力の向上及び持続的発展 ～DXの推進に向けたリスク対策の強化～
- ✓ これまでICTの利活用に必ずしも積極的ではなかった地域・中小企業における対策の促進
- ✓ サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組強化

2. 国民が安心して暮らせるデジタル社会の実現 ～政府機関や重要インフラのレジリエンスの向上～
- ✓ サイバー空間における脅威動向の把握・対処や分析能力の向上を通じた政府情報システムのレジリエンス向上
- ✓ 重要インフラ分野において、組織全体でのサイバーセキュリティ対応の促進・インシデント発生時の初動対応支援などを進めている医療分野など

3. 国際社会の平和・安定及び我が国の安全保障への寄与 ～同盟国・同志国との国際連携・協力の推進～
- ✓ 同盟国・同志国とのサイバー協議や対話の実施
- ✓ 日米豪印における協力、ランサムウェア対策を推進するための同志国間の協力枠組みの推進

サイバーセキュリティ2023のポイント
（出典）NISC「サイバーセキュリティ２０２３の概要」を基に作成

6-1-1. サイバーセキュリティ戦略

「今後の取組の方向性（今年度特に強力に取組む施策について）」に記載がある「１. 経済社会の活力の向上及び持続的発展～DXの推進に向けたリスク対策の強化～」の中で、中小企業に主に関連する内容を説明します。

[１] 中小企業のサイバーセキュリティ対策促進

１．背景及び課題

✓ サプライチェーンの中で比較的弱い中小企業へのサイバー攻撃を経由して、発注元の大企業も被害を受けている実態への取組強化が必要である。

✓ 他方で、その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にある中小企業や、対策費用や人材の確保に課題を感じている中小企業も多数存在する。

✓ 中小企業の経営者の意識改革や中小企業が使いやすいセキュリティサービスの普及促進・運用改善、大企業が取引先の中小企業に対してセキュリティ対策の支援・要請を行う際の関係法令の適用関係にかかる懸念の払拭を更に進めていくことが必要である。

２．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」につき、サービス基準の改定による同サービスの拡充などを通じて、中小企業側の様々なニーズに応え、個々の中小企業の要望に応じたサイバーセキュリティ対策の支援を実現する。

✓ こうした取組を、サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）とも連携して実施し、中小企業への対策の浸透を図る。

②取組によって期待される成果・効果

✓ お助け隊サービスの普及を通じて、中小企業のセキュリティが向上するとともに、中小企業におけるサイバー攻撃被害の実態について、サービス提供事業者を通じて把握することが可能になる。あわせて、関係機関への通報や共有が促進されることも期待される。

✓ サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）との連携により、産業界全体のサイバーセキュリティ強化が期待される。

[２] サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取組

１．背景及び課題

✓ サイバー空間とフィジカル空間が密接に関係していく世界にあって、サイバー攻撃のリスクも増大する中、これに対応するための考え方を整理したフレームワークを整備しているところであり、この社会実装を進めることでセキュリティ対策のレベルを向上させることが必要である。

✓ 特に、ソフトウェアを構成する部品情報を管理し、脆弱性管理などに活用可能なSBOM導入の重要性に対する認識が米国を中心に広まっていることから、こうした動きに対応しつつ、SBOMが有するメリットを生かしていくための仕組み作りや様々な分野への普及が重要である。

✓ 通信システムのソフトウェアでのOSSの普及拡大に伴って多発するサイバー攻撃への対処のため、通信分野におけるSBOM導入が急務である。

２．取組の概要

①手法

✓ 脆弱性管理の効率化などを図るため、脆弱性情報とSBOMの紐付けを機械的に行う手法の実証など、2022年度までの取組を深化する。

✓ 代表的な通信システムを対象にSBOMを作成・評価するなど、通信分野でのSBOM導入に向けた取組を進める。

②取組によって期待される成果・効果

✓ SBOMに関する知見の整理、契約モデルなどのツールの整備などを通じた、安心してソフトウェア活用を行うことができる環境の構築、ひいてはあらゆる産業で生産性の向上や新たなサービスの創出といった付加価値の増大が見込まれる。

✓ 通信分野でのSBOM導入により、OSSなどのソフトウェア部品の脆弱性が確認された際の対応の迅速化などが期待される。

サイバーセキュリティ2023のポイント
（出典）NISC「サイバーセキュリティ２０２３の概要」を基に作成

6-1-2. 企業経営のためのサイバーセキュリティの考え方

企業経営のためのサイバーセキュリティの考え方

サイバー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付け、自発的にサイバーセキュリティ対策に取組むことが重要です。デジタルトランスフォーメーションの推進にあたり、IoTなどのデジタル技術を積極的に取り入れる中、安全性が高い品質の製品やサービスを実現していく取組は、企業価値や競争力の向上に繋がります。そのため、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の強化の両方に取組むことが大切です。

サイバー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となる。

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一つとして位置付けることが必要。
・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29.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」を基に作成

6-1-2. 企業経営のためのサイバーセキュリティの考え方

企業のIT活用状況、サイバーセキュリティ対策の取組のレベルに応じた、実施すべき対策について説明します。企業のIT活用状況および、サイバー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」な状態が一番良く、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対策を進めることが重要です。必要な対策の一例を「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付け、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業**	
もっと積極的に	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とき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、たとえば「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30.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）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」を基に作成

6-1-3. 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、デジタルトランスフォーメーション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】経営層が主体性をもってデジタルトランスフォーメーションとサイバーセキュリティ対策に取組むためには、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事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得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

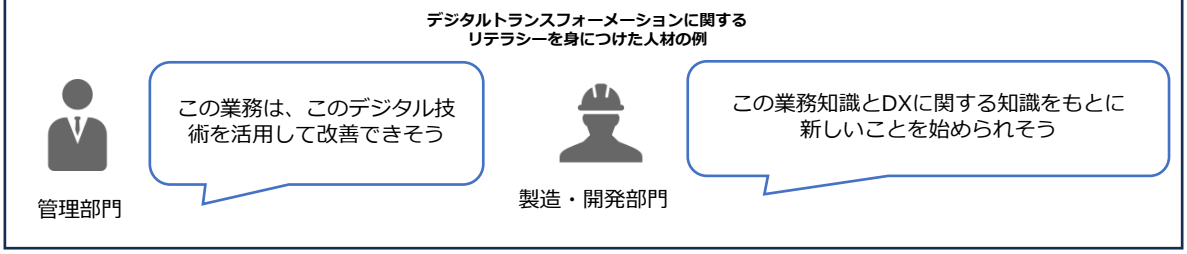
施策の理解のため参考となる文献（参考文献）	
目的や所属・役割から選ぶ施策一覧	https://security-portal.nisc.go.jp/curriculum/

6-1-3. DX with Cybersecurity

ここからは、デジタルトランスフォーメーションを推進するために必要なスキルや人材について説明します。デジタルトランスフォーメーションを進めていくには、社内にデジタルトランスフォーメーションの素養を持った人材が必要ですが、中小企業において重要なのは、デジタルトランスフォーメーションに関する高度な知識を持った人材を確保・育成することよりも、まずは経営層を含め社内のすべての人々がデジタルトランスフォーメーションに理解や関心を持ち、自らの業務を変革して新たな付加価値を生み出そうとするような意識を持つことです。そのために必要となるデジタルトランスフォーメーションに関するリテラシー（基礎的な知識やスキル、マインドセット）を説明していきます。

DXに関するリテラシーを身につけたことによる効果（個人）

世の中で起きているDXや最新の技術へのアンテナを広げ、日々生まれている新たな技術、キーワードなどにも興味を向けられるようになります。
知らない内容に接した際は、自ら調べてDXの知識を広げていけるようになります。



DXに関するリテラシーを身につけたことによる効果（会社）

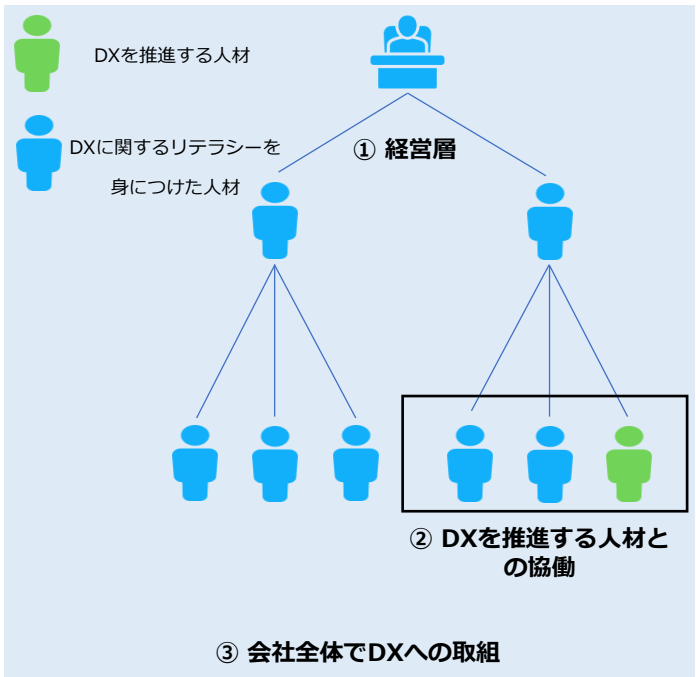


図31. DXリテラシー標準に沿った学びによる効果の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.0 」を基に作成

①経営層

社会やビジネス環境の変化において有益な技術・考え方を知ることで、自社のDXの方向性を思案し、社員に示すことができる

②DXを推進する人材との協働

事業内容に知見がある人材とDXを推進する人材（DXに関する専門性が高い人材）との協働が進み、企業としてのDXが進みやすくなる

③会社全体でDXへの取組

社員全員がDXに関するリテラシーを身につけることで、DX推進に伴う組織内の変化に対する受容性が高くなる

6-1-3. DX with Cybersecurity

デジタルスキル標準（DSS）

経済産業省とIPAがまとめた「デジタルスキル標準（DSS）」では、すべてのビジネスパーソンがデジタルトランスフォーメーションに関する基礎的な知識、スキル、マインドセットを身につけるための学習指針を「DXリテラシー標準」として策定しています。企業は、社員に対して、デジタルトランスフォーメーションに関するリテラシーを身につけさせるための育成方法を検討する際に、指針として活用することができます。

DXリテラシー標準は、特定の産業や職種、部署などに依存しない汎用性を重視して作成されています。そのため、企業や組織がこれを適用する際には、自身が属する産業や事業の方向性に合わせる必要があります。

DXリテラシー標準 → **自社の事業の方向性に合わせることが必要**

DXリテラシー標準は、以下のように構成されています。

標準策定のねらい
ビジネスパーソン一人ひとりがDXに関するリテラシーを身につけることで、DXを自分事ととらえ、変革に向けて行動できるようになる

Why
（DXの背景）
DXの重要性を理解するために必要な、社会、顧客・ユーザー、競争環境の変化に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする）

What
（DXで活用されるデータ・技術）
ビジネスの場で活用されているデータやデジタル技術に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

How
（データ・技術の利活用）
ビジネスの場でデータやデジタル技術を利用する方法や、活用事例、留意点に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

マインド・スタンス
社会変化の中で新たな価値を生み出すために必要な意識・姿勢・行動を定義

→個人が自身の行動を振り返るための指針かつ、組織・企業がDX推進や持続的成長を実現するために、構成員に求める意識・姿勢・行動を検討する指針とする

項目一覧

Why（DXの背景）	What（DXで活用されるデータ・技術）		How（データ・技術の利活用）	
社会の変化	データ	社会におけるデータ	活用事例・利用方法	データ・デジタル技術の活用事例
顧客価値の変化		データを読む・説明する		ツール利用
競争環境の変化		データを扱う	留意点	セキュリティ
		データによって判断する		モラル
	デジタル技術	AI		コンプライアンス
		クラウド		
		ハードウェア・ソフトウェア		
		ネットワーク		

マインド・スタンス				
デザイン思考/アジャイルな働き方	顧客、ユーザへの共感	常識にとらわれない発想	反復的なアプローチ	
新たな価値を生み出す基礎としてのマインド・スタンス	変化への適応	コラボレーション	柔軟な意思決定	事実に基づく判断

図32.DXリテラシー標準の全体像
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

6-1-3. DX with Cybersecurity

デジタルスキル標準の改訂について

急速に普及する生成AIは、各企業におけるDXの進展を加速させると考えられ、企業の競争力を向上させる可能性があります。あわせて、ビジネスパーソンに求められるスキル・リテラシーも変化し、より重要になる部分もあると想定されます。その状況に対応するため、2023年８月にDXリテラシー標準に関する内容が改定されました。

追加された生成AIに関する内容を以下の図で説明します。

DXリテラシー標準策定のねらい

「DXを自分事ととらえ、変革に向けて行動できるようになる」という位置付けは不変

Why DXの背景

- ✓ 産官学で生成AIの利用が進んでおり、社会環境へ影響を与える可能性があるため、「社会の変化」に人材育成・教育や労働市場の変化などの学習項目例を追加

What DXで活用されるデータ・技術

- ✓ 生成AIは、ビジネスの場で急速に普及・利用されているため、「AI」に生成AIの技術動向や倫理などの学習項目例を追加
- ✓ 現在の利用状況に鑑み「ネットワーク」にネットワークの種類、インターネットサービスの学習項目例を追加
- ✓ 個人や企業などで扱うデータがデジタル技術・サービスに活用されるため、「データを扱う」に活用しやすいデータの入力や整備の手法などの内容・学習項目例を追加
- ✓ 適切でないデータから生み出される結果は、誤った判断・損害につながり得るため、「データによって判断する」に適切なデータを用いて判断することの重要性などの内容・学習項目例を追加

How データ・技術の利活用

- ✓ 生成AIは、ツールなどの基礎知識や指示（プロンプト）の手法を用いて業務の様々な場面で利用できるため、「データ・デジタル技術の活用事例」に生成AIの活用事例、「ツール利用」に生成AIツールの概要、指示（プロンプト）の手法などの学習項目例をそれぞれ追加
- ✓ 情報漏えいや法規制、利用規約などに正しく対処しながら生成AIを利用することが求められるため、「モラル」にデータ流出の危険性など、「コンプライアンス」に法規制や利用規約などの学習項目例をそれぞれ追加

マインド・スタンス

- ✓ 他項目と比べてより普遍的な要素を定義しているため、生成AI利用においても同様に重要となる
- ✓ 適切なデータを用いることにより、事実に基づく判断が有効になるため、「事実に基づく判断」に適切なデータ入力の重要性や行動例などを追加
- ✓ 生成AIをビジネスパーソンとしてのスキルと掛け合わせ生産性向上やビジネス変革などへ適切に利用しようとしていること、生成AI利用における注意点を理解していること、生成AIの影響に対して変化をいとわず学び続けることは、今後、全ビジネスパーソンが身に着けるべきマインド・スタンスとして重要性が増すため、「生成AI利用において求められるマインド・スタンス」として既存項目と分けて追加

図33.DXリテラシー標準の改訂（ 2023年８月）の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

One Point

DXリテラシー標準の学習方法

「マナビDX」という、すべての社会人にとって必須であるデジタルスキルを学べるコンテンツを紹介しているポータルサイトがあります。このポータルサイトでは、DXリテラシー標準の各項目ごとに学習できる講座が掲載されており、DXリテラシーを学ぶことができます。

6-1-3. DX with Cybersecurity

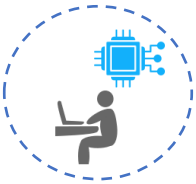
プラス・セキュリティ

プラス・セキュリティとは

自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと[14]

企業は、デジタルトランスフォーメーションの推進と並行してサイバーセキュリティへの対策が求められています。この状況の中、経営層をはじめ、法務や広報といった、必ずしもITやセキュリティに関する専門知識や業務経験を有していない人も「プラス・セキュリティ」知識を習得することが重要です。なぜなら、デジタルトランスフォーメーションが進む中、サイバーセキュリティ担当部署だけでは、サイバーセキュリティ対策への対処が難しい状況になっているためです。そのため、サイバーセキュリティ対策が不十分な場合、インシデントが生じる可能性がある業務を担っている人材には、業務に必要なセキュリティに関する知識・スキルを身につけてもらう必要があります。

クラウドを活用した新規プロジェクトの担当者



組み込みソフトウェアの機能を設計する担当者

自社の電話、インターネット、複合機などの保守契約を扱う担当者

サイバーセキュリティの知識が不十分な場合の問題例

- 目的にそぐわないクラウドを選定することや、自社のサイバーセキュリティ担当者が把握していないクラウドの導入により、情報漏えいなどのリスクが高まる恐れがあります
- ソフトウェアにサイバー攻撃に対する脆弱性が生じる恐れがあります
- 不適切な設定で運用することで、機器を介した情報漏えいの原因となる恐れがあります

[14]:経済産業省.”サイバーセキュリティ経営ガイドラインVer2.0付録Fサイバーセキュリティ体制構築・人材確保の手引き～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1.1版”. https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf, （2023-07-28）.

6-1-3. DX with Cybersecurity

プラス・セキュリティ人材の育成

プラスセキュリティの知識を身につける方法として、主に試験・資格を活用したり、教育プログラムを受けたりする方法があります。ここでは、具体例も含めて紹介します。

試験・資格の活用

各分野の人材がプラスセキュリティの知識を身につける方法の1つとして、試験や資格の活用が挙げられます。資格を活用することの利点は、特定の役割や業務を担うために必要なスキルを効率よく習得できることです。

（例）

- **情報セキュリティマネジメント試験**

【対象】企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者
【内容】本試験は、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認定するものです。

教育プログラム・コミュニティ活動の活用

NISC（内閣サイバーセキュリティセンター）では、経営層、管理職、一般社員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などが紹介されています。

（例）

- **戦略マネジメント系セミナー（IPA）**

【対象】管理職、一般社員（特に、「セキュリティ統括責任者」である部課長級の責任者層、今後責任者層になることが期待される実務者層・技術者層、「プラス・セキュリティ」人材の方に向いています）
【難易度】中級
【内容】セキュリティ統括責任者として認識しておくべき事項を、「有識者講演」、「プログラム講義」、「ディスカッション（グループワーク）」の３つのプログラムで学習するセミナーです。
座学だけでなく、受講者間でのディスカッション・意見交換の場を設け、より実践的で深い理解が得られるアクティブラーニングの機会を提供しています。

- **実践サイバー演習「RPCI」**（NICT）

【対象】経営層、管理職、一般社員（特に、CISO、CSIRT管理者、CSIRTメンバー、インシデントが発生した際の対応に携わる方、情報システムの管理・運用・調達・企画・開発に携わる方に向いています）
【難易度】中級～上級
【内容】本番に近いリアルな環境でのインシデント対応を行う演習です。擬似的に発生させたサイバー攻撃にCSIRTとしてチームで対処します。実際の対応に近い体験をすることで、多くの気づきや学びを得ることができます。

6-2-1. 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、様々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繋がる非常に重要な取組となります。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2005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り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。

（出典）内閣府大臣官房政府広報室.”「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,（2023-07-28）.

One Point

個人情報保護法の罰則規定

2022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。

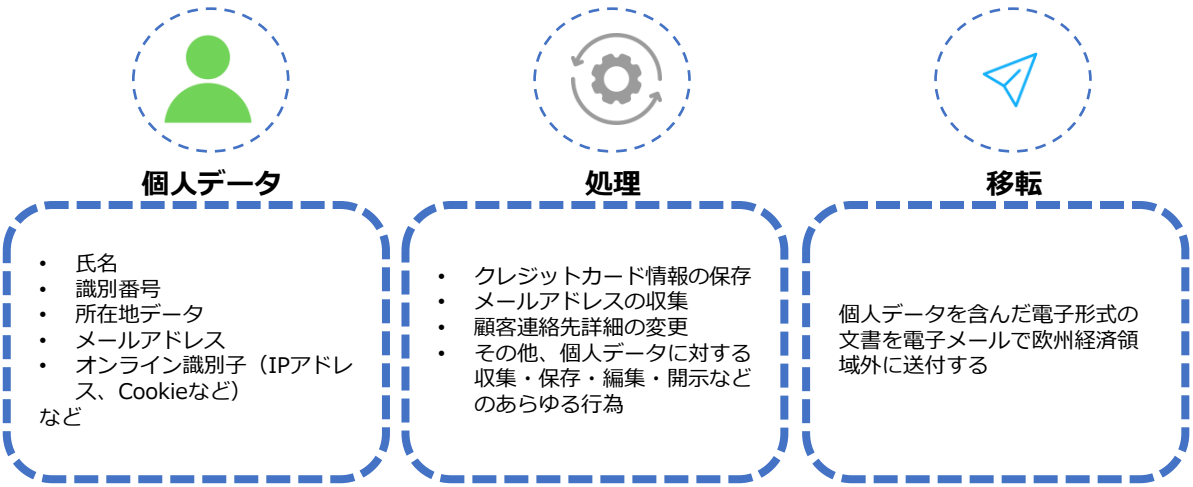
6-2-2. GDPR

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の概要



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。

コラム

“デジタルトランスフォーメーション”と“デジタル化”の関係について

テキスト内では、国の方針や計画を解説する中で”デジタルトランスフォーメーション”という言葉が随所に出てきます。それと同時に、 ”デジタル化”という言葉もあります。両者は異なる定義の言葉ですが、無関係なものではありません。

“デジタルトランスフォーメーション”は、データとデジタル技術を活用してビジネスモデルを変革し、新たな価値を創出することを指します。

”デジタル化”に含まれる概念には、「デジタイゼーション」と「デジタライゼーション」があります。本テキストの用語集”デジタル化”に説明がありますが、デジタイゼーションはアナログや物理的な情報をデジタル化すること、デジタライゼーションはビジネスプロセスをデジタル化することを意味します。
紙で管理していた情報をシステム上に入力することでデータをデジタル化すること、紙資料で行っていたプレゼンテーションをタブレットで行うようにすることなどがデジタイゼーション、それにより業務のやり方が変化し、効率化されるなどの変化がデジタライゼーションです。

“デジタルトランスフォーメーション”は、デジタイゼーション、デジタライゼーションといった”デジタル化”の先にあるものです。”デジタル化”により課題をクリアした後に、新たな価値を創出することが”デジタルトランスフォーメーション”となります。”デジタルトランスフォーメーション”の実現に向けて、”デジタル化”は不可欠なステップです。

第7章. セキュリティフレームワーク

7-1. セキュリティフレームワークの概要

7-2.情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]

7-3. NIST サイバーセキュリティフレームワーク（CSF）

7-4. 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）

7-5. サイバーセキュリティ経営ガイドライン

章の目的
第7章では、ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークを理解し、それぞれの内容について知識を身につけることを目的とします。

主な達成目標
◘ サイバーセキュリティ対策においてフレームワークを活用することの重要性について理解すること ◘ 各フレームワークの目的や必要性などの特徴について理解すること

7-1-1. セキュリティフレームワークの役割と重要性

セキュリティフレームワークの概要およびその利用メリットについて説明します。

セキュリティフレームワークとは

セキュリティ対策を行うために定義された指針やセキュリティ対策基準、ガイドライン、ベストプラクティス集のことを指します。自社におけるセキュリティリスクを評価・管理し、適切なセキュリティ対策を計画、実装、管理するための基盤となります。

セキュリティフレームワークを使用するメリット

**効果的な
セキュリティ対策**

フレームワークを使用することで、対策の抜け漏れを防ぎ、効果的かつ適切なセキュリティ対策を行うことが可能となります。

**信頼性の
確保**

認証制度が存在するフレームワークの場合、そのフレームワークに従ってセキュリティ対策を実装し、第三者機関から認証を受けることで、取引先や顧客からの信頼獲得につながります。

<代表的なセキュリティフレームワーク>

ISMS（情報セキュリティマネジメントシステム）
[ISO/IEC27001,27002]
☛ **網羅的なセキュリティフレームワーク**

ISO/IEC27017
☛ **クラウドサービス**

CSF（サイバーセキュリティフレームワーク）
☛ **重要インフラ**

CPSF
（サイバー・フィジカル・セキュリティ対策フレームワーク）
☛ **Society 5.0における産業社会**

サイバーセキュリティ経営ガイドライン
☛ **経営者を中心としたセキュリティ対策**

PCI DSS
（国際的なクレジット産業向けのデータセキュリティ基準）
☛ **クレジットカード産業**

PMS
（個人情報保護マネジメントシステム）
☛ **個人情報保護**

CIS Controls
☛ **具体的なサイバー攻撃アプローチ**

ISA/IEC62443
☛ **産業オートメーションおよび制御システム**

フレームワーク使用上のポイント

上記のようにフレームワークは数多くの種類がありますが、まずは業種業態を問わず、セキュリティ対策の全体の枠組みと網羅的な対策項目を提示しているISMSをベースとするとよいでしょう。そして必要に応じて、業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークの内容で補完することが大切です。

7-1-2. フレームワーク選択の重要性

→フレームワークの発行元

ISO/IEC

ISMS（情報セキュリティマネジメントシステム）[ISO/IEC27001,27002]
☛ 網羅的なセキュリティフレームワーク

情報の機密性、完全性、可用性を保護するための体系的な仕組みであり、技術的対策だけでなく、従業員の教育や訓練、組織体制の整備などが含まれています。必ずしも、組織全体で適用する必要はなく、組織の必要に応じて、適用範囲を決定できるという特徴があります。[15]

ISO/IEC

ISO/IEC27017
☛ クラウドサービス

クラウドサービスに関する情報セキュリティ対策を実施するためのガイドライン規格で、ISO/IEC27002をベースに作成されています。この規格は、クラウドサービスの提供者とクラウドサービスの利用者の両方を対象としています。クラウドサービスに関するリスクの低減や、クラウドサービスを適切に利用する組織体制を確立できます。

また、情報セキュリティ全般に関するマネジメントシステム規格であるISO/IEC 27001の取組をISO/IEC 27017で強化することで、クラウドサービスにも対応した情報セキュリティ管理体制を構築することができます。

NIST

CSF（サイバーセキュリティフレームワーク）
☛ 重要インフラ

CSFの正式名称は「重要インフラのサイバーセキュリティを改善するためのフレームワーク」となり、重要インフラ向けのセキュリティフレームワークとして発行されました。NISTが定義するサイバーセキュリティ対策アプローチの中で最も上位に位置付けられており、セキュリティ管理手法の概念や管理方針・体制の整備など包括的な内容が記載されています。

CSFの下位概念に位置付けられているのがSP800シリーズ（SP 800-53/SP 800-171/SP 800-161など）となり、 SP800シリーズの内容については後述します。

経済産業省

CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）
☛ Society 5.0における産業社会

ISMS、CSFの概念を包含したフレームワークであり、サイバー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しています。Society5.0を意識したセキュリティリスクとその対策方法について記述されている特徴があります。

リスク源を適切に捉えるために産業社会を3層構造と6つの構成要素で捉えており、産業界が自らのセキュリティ対策に活用できるよう、対策例がまとめられています。

経済産業省/IPA

サイバーセキュリティ経営ガイドライン
☛ 経営者を中心としたセキュリティ対策

サイバー攻撃の多様化・巧妙化に伴い、サイバー攻撃から企業を守るために必要なことをまとめたガイドラインです。 ISMSのフレームワークがベースとなっており、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある3原則と、経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISOなど）に指示すべき重要10項目をまとめているという特徴があります。[16]

サイバー攻撃から企業を守る観点で、“サイバーセキュリティは経営問題”と定義し、経営者を中心とした組織的な対策の見直し・強化を求めています。

[15]:ISMS-AC.”ISMS適合性評価制度”. https://isms.jp/doc/JIP-ISMS120-62.pdf, （2023-08-10）.
[16]:経済産業省.”サイバーセキュリティ経営ガイドラインと支援ツール”. https://www.meti.go.jp/policy/netsecurity/mng_guide.html, （2023-08-10）.

7-1-2. フレームワーク選択の重要性

→フレームワークの発行元

PCI SSC

PCI DSS (国際的なクレジット産業向けのデータセキュリティ基準)
☛ **クレジットカード産業**

クレジットカード情報を取扱うすべての事業者に対して国際カードブランド5社が共同で策定した、クレジットカードの取扱いにおけるセキュリティの国際基準です（Payment Card Industry Data Security Standard の略）。[17]
カード会員情報を適切に管理するため、ネットワークアーキテクチャ、ソフトウェアデザイン、セキュリティマネジメント、ポリシー、プロシジャなどに関する基準が12の要件として規定されています。

JIPDEC

PMS（個人情報保護マネジメントシステム）
☛ **個人情報保護**

組織が業務上取扱う個人情報を安全で適切に管理するための仕組みです。JIS Q 15001によって要求事項が定められています。この規格は、事業者が個人情報を適切に取扱う方法を規定したもので、プライバシーの保護を直接の目的とはしていません。しかし、意図しない個人情報の取扱いが抑制されることで、結果的にプライバシーも保護されます。[18]
PMSの基本的な仕組みは、個人情報保護方針を定め、この方針に基づき「PDCAサイクル」を実行することとなります。

CIS

CIS Controls
☛ **具体的なサイバー攻撃アプローチ**

サイバー攻撃の現状と傾向を踏まえて、組織が実施すべきサイバーセキュリティ対策とその優先順位を決めるためのフレームワークで、あらゆる企業がとるべき最も基本的で重要な対応に重点を置いています。ネットワークの詳細設定や、ログの管理など、具体的で技術的な対策が中心となっている特徴があります。
多岐にわたる対策の中から、自社（組織）が実施すべき対策と、その優先順位を導くためのアプローチを提示したフレームワークとなります。

ISA/IEC

ISA/IEC62443
☛ **産業オートメーションおよび制御システム**

産業用自動制御システム（Industrial Automation and Control Systems）に対するセキュリティ対策とプロセス要件を定めた一連の国際標準規格です。ISO/IEC 27001などではカバーしきれない、工場やプラントにおける制御システムのセキュリティを網羅的に対象としています。また、セキュリティ確保の対象は、ソフトウェア・ハードウェアを含む制御関連のデータ処理基盤であるシステムだけでなく、システムの運用に関わる「人」と「業務」も対象となっている特徴があります。

[17]:経済産業省."クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性".
https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf, （2023-08-17）.
[18]:JIPDEC."「個人情報」と「プライバシー」の違い". https://privacymark.jp/wakaru/kouza/theme1_03.html, （2023-08-10）.

7-2-1. ISMSの概要

ISMSとは、情報セキュリティマネジメントシステム（Information Security Management System）の略称で、組織の情報セキュリティリスクを適切に管理するための仕組みのことです。 ISMSに関する国際規格がフレームワークとして存在していることから、ISMSはセキュリティフレームワークの中でも代表的なものとなっています。ISMSが達成すべきことは、**リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランス良く維持・改善し、リスクを適切に管理しているという信頼を利害関係者に与える**ことにあります。[19]また、ISMSには技術的対策だけでなく、従業員の教育・訓練、組織体制の整備なども含まれます。

情報セキュリティの3要素

機密性（Confidentiality）
権限のない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しないこと（情報に対するアクセスを適切に管理すること）

完全性（Integrity）
情報が正確であり、完全である状態を保持すること

可用性（Availability）
情報を必要なときに使えるようにしておくこと

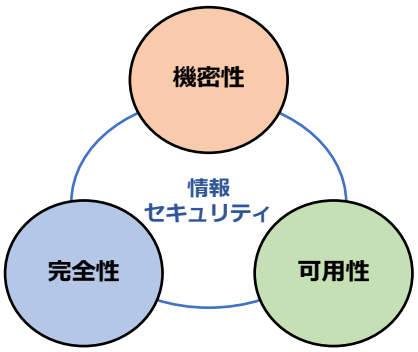


図34. 情報セキュリティの3要素
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

One Point

情報セキュリティの7要素
情報セキュリティには、上記で紹介した3要素に加えて、「真正性（Authenticity）」「信頼性（Reliability）」「責任追跡性（Accountability）」「否認防止（non-repudiation）」という4つの拡張要素があります。これらは、情報にアクセスする人が本当にアクセスするべき人であるかを担保することや、システムが確実に目的の動作をすること、誰がどのような手順で情報にアクセスしたかを追跡できるようにすること、また、情報が後から否定されない状況を作ることで情報セキュリティを確保するものです。

---

[19]:ISMS-AC.”ISMSとは”.https://isms.jp/isms/, （2023-08-09）

7-2-1. ISMSの概要

ISMSのための要求事項をまとめた国際規格が、 ISO/IEC 27001です。組織がISMSを確立し、実施し、維持し、継続的に改善するための要求事項の提供を目的として作成されています。ISMSの確立および実施について、組織の行うべき事項が項目ごとに記述されたものとなっており、この規格は以下のために用いることができます。[20]

組織のマネジメントおよび業務プロセスを取り巻くリスクの変化への対応
JIS Q 27001（ISO/IEC 27001）では、組織は、自らのニーズおよび目的、情報セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模および構造を考慮して、ISMSの確立および実施を行います。これは、多くの情報を取扱うようになっている、現代の組織のマネジメントおよび業務プロセスを取り巻くリスクの変化に対応できるように、組織基盤を構築する抜本的な業務改革をする目的に適しています。
情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準
JIS Q 27001（ISO/IEC 27001）は、情報セキュリティ要求事項を満たす組織の能力を、パフォーマンス評価および内部監査などにより、組織の内部で評価する基準としても、取引先の顧客などから受ける第二者監査、あるいは、審査登録機関による認証のための第三者監査の基準としても用いることができます。

（出典）ISMS-AC.”ISMSとは”.https://isms.jp/isms ,（参照 2023-08-09）

One Point

ISO/IEC 27001とJIS Q 27001

ISMSに関する規格には、ISO/IEC 27001とは別にJIS Q 27001があります。国際規格であるISO/IECに対して、JISは日本産業規格となり、日本における任意の国家規格です。JIS Q 27001は、ISO/IEC 27001を日本語に訳したものとなりISOとJISによる規格内容の違いはありません。

---

[20]:ISMS-AC.”ISMSとは”.https://isms.jp/isms/ ,（2023-08-09）

7-2-2. ISMSの要素と要件

ISO/IEC 27001の要求事項

ISO/IEC 27001では、組織が効率的にISMSの構築・実施・維持・継続的改善を行うとともに、情報セキュリティのリスクアセスメントおよびリスク対応を実現するために必要な要求事項を定めています。**ISO/IEC 27001の要求事項は、ISMS認証を取得するには必ず対応しなければなりません。**どのような内容が要求されているのか認識するため、各要求事項の概要について説明します。要求事項は、後述のPDCAサイクルと呼ばれる運用サイクルに落とし込んで、情報セキュリティマネジメントを実施することとなります。

ISO/IEC 27001 各要求事項の概要

「1. 適用範囲」に記述されていますが、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの7項目となっています。

1. 適用範囲
ISO/IEC 27001はISMS運用のための要求事項を規定しており、本規格に適合するためには4～10に規定されるすべての事項に対応しなければならない。

2. 引用規格
ISO/IEC 27001は、ISO/IEC 27000（ISMSの概要と用語）を引用する。

3. 用語および定義
ISO/IEC 27001で用いる用語および定義は、ISO/IEC 27000に定めている。

4. 組織の状況
組織の内情や取り巻く状況、利害関係者のニーズを把握した上でISMSの適用範囲を決定することを要求している。

5. リーダーシップ
トップマネジメントが主導してISMSを構築することを要求している。（トップマネジメントが実施するべきことのまとめ）

6. 計画
ISMSの計画を立てる際の要求事項。（PDCA サイクルの P「Plan」）

7. 支援
構成員の教育など、ISMS 構築にあたり組織が構成員に行うべきサポートを要求している。

8. 運用
ISMSを実行する際の要求事項。（PDCA サイクルの D「Do」）

9. パフォーマンス評価
適切なISMSが構築・運用できているか評価する際の要求事項。（PDCA サイクルの C「Check」）

10. 改善
ISMSの是正処置やリスク、改善の機会、ISMS認証の不適格があった場合の対処法。（PDCA サイクルの「Act」）

7-2-2. ISMSの要素と要件

ISMSの運用プロセス

マネジメントシステムとは、組織の方針や目標を定めて、その目標を達成するために必要な、組織を管理する仕組みのことを指します。情報セキュリティのマネジメントシステムであるISMSも、組織によって定めた目標達成のための取組です。その目標は、情報セキュリティに関することや、会社が抱えている機密情報をどう保護していくのかという内容となります。その目標に向かってマネジメントを行っていくための方法として、**要求事項を実施しながら、PDCA（Plan・Do・Check・Act）サイクルを繰り返し、スパイラルアップしていく**ことが、ISO/IEC 27001では求められています。

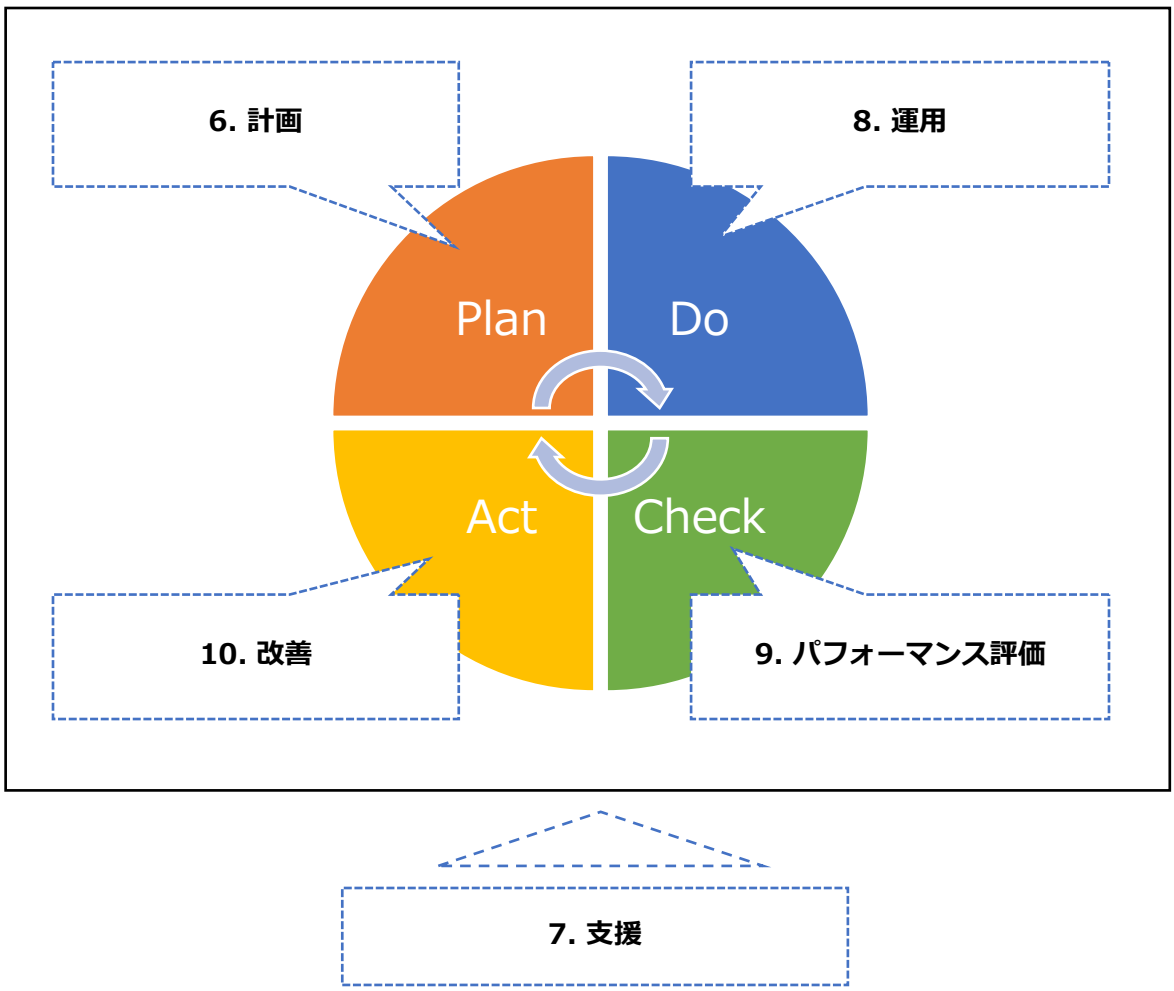


図35. ISO/IEC 27001のPDCAサイクル

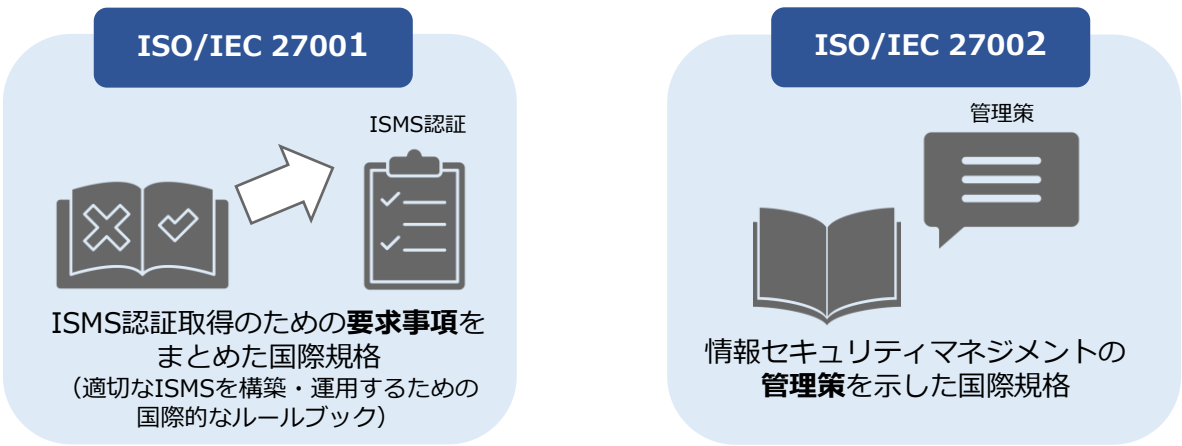
7-2-2. ISMSの要素と要件

ISMSの管理策

ISO/IEC 27001に記載されている要求事項をもとに、具体的な情報セキュリティマネジメントの管理策を示した規格としてISO/IEC 27002があります。 ISO/IEC 27001の付属書Aは、このISO/IEC 27002の内容をそのまま取り入れたもので、情報セキュリティ上のリスクを低減するための目的と、その目的を達成するための管理策で構成されています。

付属書Aは、ISMSの本文（ISO/IEC 27001の規格要求事項）を補完するガイドラインとしての位置付けにあります。業務内容やISMSの適用範囲によってはすべての管理策を適用することができない場合があり、その際には、適用できない理由を明確にし、採用しないという選択をすることができます。つまり、一律にすべての管理策を適用するのではなく、理由を含めて採用しない管理策を明示する必要があります。

ISO/IEC 27002では、合計93種の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」 の4つのカテゴリに分類される形で解説されています。



情報セキュリティ管理策		
カテゴリ	**項目数**	**概要**
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティの方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

7-2-2. ISMSの要素と要件

ISO/IEC 27002の箇条5～8は、93種のISMS管理策で構成されています。以下の表は、それらの管理策標題の一覧です。詳細については別添資料の「ISO/IEC 27002:2022 管理策と目的」をご確認ください。

5.組織的管理策	5.24 情報セキュリティインシデント管理の計画及び準備
5.1 情報セキュリティのための方針群	5.25 情報セキュリティ事象の評価及び決定
5.2 情報セキュリティの役割及び責任	5.26 情報セキュリティインシデントへの対応
5.3 職務の分離	5.27 情報セキュリティインシデントからの学習
5.4 経営陣の責任	5.28 証拠の収集
5.5 関係当局との連絡	5.29 事業の中断・阻害時の情報セキュリティ
5.6 専門組織との連絡	5.30 事業継続のためのICTの備え
5.7 脅威インテリジェンス	5.31 法令、規制及び契約上の要求事項
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.32 知的財産権
5.9 情報及びその他の関連資産の目録	5.33 記録の保護
5.10 情報及びその他の関連資産の利用の許容範囲	5.34 プライバシ及びPIIの保護
5.11 資産の返却	5.35 情報セキュリティの独立したレビュー
5.12 情報の分類	5.36 情報セキュリティのための方針群、規制及び標準の順守
5.13 情報のラベル付け	5.37 操作手順書
5.14 情報転送	**6.人的管理策**
5.15 アクセス制御	6.1 選考
5.16 識別情報の管理	6.2 雇用条件
5.17 認証情報	6.3 情報セキュリティの意識向上、教育及び訓練
5.18 アクセス権	6.4 懲戒手続き
5.19 供給者関係における情報セキュリティ	6.5 雇用の終了または変更後の責任
5.20 供給者との合意におけるセキュリティの取扱い	6.6 秘密保持契約または守秘義務契約
5.21 ICTサプライチェーンにおける情報セキュリティの管理	6.7 リモートワーク
5.22 供給者のサービス提供の監視、レビュー及び変更管理	6.8 情報セキュリティ事象の報告
5.23 クラウドサービス利用における情報セキュリティ	

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

7-2-2. ISMSの要素と要件

7.物理的管理策	8.10 情報の削除
7.1 物理的セキュリティ境界	8.11 データマスキング
7.2 物理的入退	8.12 データ漏えいの防止
7.3 オフィス、部屋及び施設のセキュリティ	8.13 情報のバックアップ
7.4 物理的セキュリティの監視	8.14 情報処理施設の冗長性
7.5 物理的及び環境的脅威からの保護	8.15 ログ取得
7.6 セキュリティを保つべき領域での作業	8.16 監視活動
7.7 クリアデスク・クリアスクリーン	8.17 クロックの動機
7.8 装置の設置及び保護	8.18 特権的なユーティリティプログラムの使用
7.9 構外にある資産のセキュリティ	8.19 運用システムに関わるソフトウェアの導入
7.10 記憶媒体	8.20 ネットワークのセキュリティ
7.11 サポートユーティリティ	8.21 ネットワークサービスのセキュリティ
7.12 ケーブル配線のセキュリティ	8.22 ネットワークの分離
7.13 装置の保守	8.23 ウェブ・フィルタリング
7.14 装置のセキュリティを保った処分または再利用	8.24 暗号の使用
8.技術的管理策	8.25 セキュリティに配慮した開発のライフサイクル
8.1 利用者エンドポイント機器	8.26 アプリケーションのセキュリティの要求事項
8.2 特権的アクセス権	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
8.3 情報へのアクセス制限	8.28 セキュリティに配慮したコーディング
8.4 ソースコードへのアクセス	8.29 開発及び受け入れにおけるセキュリティ試験
8.5 セキュリティを保った認証	8.30 外部委託による開発
8.6 容量・能力の管理	8.31 開発環境、試験環境及び運用環境の分離
8.7 マルウェアに対する保護	8.32 変更管理
8.8 技術的脆弱性の管理	8.33 試験情報
8.9 構成管理	8.34 監査試験中の情報システムの保護

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

7-2-2. ISMSの要素と要件

ISMSの管理策における属性

ISO/IEC 27002では、2022年の改訂より「属性」という考え方が新たに追加されました。この「属性」についての各管理策としては「予防（ preventive ）」、「検知（ detective ）」、「是正（ corrective ）」のいずれかに分類され、またその特性によって「機密性」、「完全性」、「可用性」のいずれかに関連付けられています。さらに、サイバーセキュリティ概念、運用機能、セキュリティドメインという3つの観点からも属性のグループ分けが行われています。「属性」という考え方が追加された結果、各管理策をより柔軟かつ様々な場面に採用できるようになりました。

この「属性」という考え方は、他の組織や団体が発行するガイドラインなどとの親和性を高める効果も期待できます。たとえば、「サイバーセキュリティ概念」では「識別、防御、検知、対応、復旧」という5つの属性値が示されていますが、これは米国国立標準研究所（NIST）が発行しているCSF（サイバーセキュリティフレームワーク）でも採用されているものです。また、組織は自らの視点を作るために、独自の属性を作ることも可能です。

管理策タイプ
情報セキュリティインシデントの発生との関係において、リスクをいつどのように修正するかという観点から管理策を見る属性 ［属性値］予防、検知、是正
情報セキュリティ特性
情報のどの特性の維持に寄与するかという観点から管理策を見る属性 ［属性値］機密性、完全性、可用性
サイバーセキュリティ概念
ISO/IEC TS 27119に記述されているサイバーセキュリティフレームワークで定義された、サイバーセキュリティ概念との関連付けの観点から管理策を見る属性 ［属性値］識別、防御、検知、対応、復旧
運用機能
実践者の情報セキュリティ機能の観点から管理策を見る属性 ［属性値］ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティを保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、供給者関係のセキュリティ、法および順守、情報セキュリティ事象管理、情報セキュリティ保証
セキュリティドメイン
情報セキュリティドメインの観点から管理策を見る属性 ［属性値］ガバナンスおよびエコシステム、保護、防御、対応力

7-2-3. ISMSの実装と認証

ISMSの構築

ISO/IEC 27001に準拠したISMSを実装するには、どのようなステップが必要なのか解説します。実装に際してはISO/IEC 27001の認証審査を受けることになります。そのため、審査対象となるISMSの構築を実施し、実際の運用状況の記録をつけることとなります。

ISMSの構築	
ステップ	**概要**
適用範囲の決定	会社全体だけでなく、特定の部署・拠点のみといったようにISMSの範囲を限定することも可能なため、まずは適用範囲を決定します。
情報セキュリティ方針の策定	ISMSの基本的な指針として、会社の情報セキュリティ方針を策定します。
体制の確立	ISMS管理責任者、ISMS推進事務局、ISMS内部監査チームなど、ISMSの運用体制を決定します。
ISMS文書の作成	ISMSを運用・維持するための手順やガイドラインを文書化します。従業員や関係者が理解しやすく、利用・実践しやすい形式で作成することが重要です。
リスクアセスメントの実施	会社が持つ情報資産を洗い出し、それらに想定しうるリスクと対策を決定します。リスクアセスメントの結果は記録を作成します。
従業員の教育	ISMSの概要や手順、会社の情報セキュリティ方針について従業員に理解してもらうため、セキュリティ教育を実施します。教育の結果は記録を作成します。
内部監査	ISMSの運用がはじまった後に、定めたルールが適切に運用されているかを確認します。運用が不十分な場合はリスクの指摘やルールの見直しを行い、改善につなげます。内部監査の結果は記録を作成します。
マネジメントレビュー	内部監査の結果をもとに、会社のISMSについての現状や課題、改善点などを経営陣に報告します。マネジメントレビューの結果は記録を作成します。

7-2-3. ISMSの実装と認証

ISMS認証とISMS適合性評価制度

「ISMS認証」とは、組織の構築したISMSがISO/IEC 27001に基づいて適切に運用管理されているかを、第三者であるISMS認証機関が、利害関係のない公平な立場から審査し証明することです。この認証を公正に運用するために、国際的な枠組みが定められており、これを「ISMS適合性評価制度」と呼んでいます。この適合性評価制度は、以下の図のように「認証機関」「認定機関」「要員認証機関」から構成されています。

ISO/IEC 27001は、 ISMS適合性評価制度において、第三者である認証機関がISMS認証を希望する組織の適合性を評価するための基準となります。**認証審査においては、組織のISMSがISO/IEC27001の標準に適合しているか**が評価されることとなります。

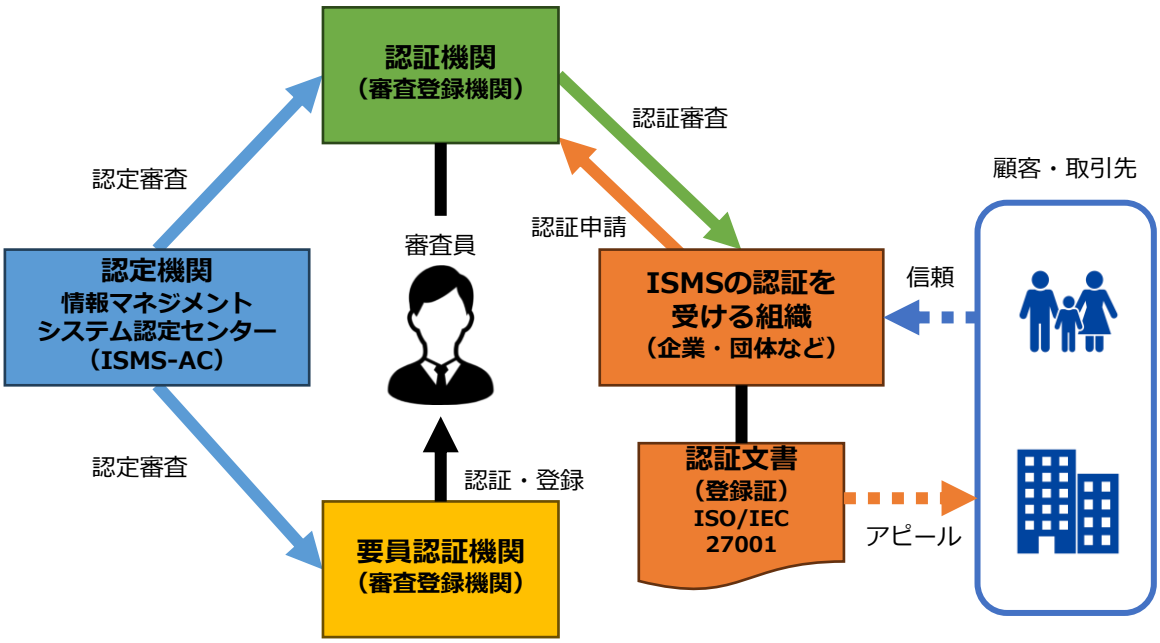


図36. ISMS適合性評価制度
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

認定と認証

認定	**認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定**と言います。日本におけるISMS適合性評価制度の認定機関は情報マネジメントシステム認定センター（ISMS-AC）です。ISMS-ACは、認証機関が適切に審査を実施できる体制・能力を持っているかを、国際規格に照らして審査し、適合していると認められる機関を認定して、「認定シンボル」の使用を許可しています。そのため、認定を受けたISMS認証機関は、適切なISMS認証審査を実施することのできる、信頼のおける認証機関であることを意味します。
認証	**第三者が文書で保証する手続きを認証**と言います。 マネジメントシステム規格への適合性を保証する場合、認証の代わりに特に他と区別するため「審査登録」という用語を用いることがあります。この場合、認証の対象は、製品、サービスあるいはプロセスではなく、組織のマネジメントシステムそのものとなることに注意が必要です。

（出典）MSQA「ISMS推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応1.0版」を基に作成

7-2-3. ISMSの実装と認証

ISMS認証審査プロセス

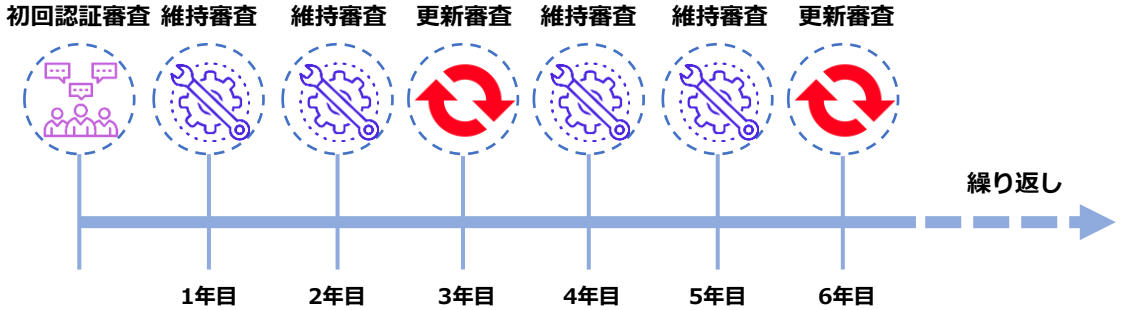
ISMSの認証審査は、大まかに以下のようなステップで進みます。

ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受診する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として1次審査と2次審査の2回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページで公開されます。

なお、審査に要する期間や工数、申請方法、申請時の準備物、認証登録料金などは、認証機関によって異なります。 ISMS認証機関は、情報マネジメントシステム認定センター（ISMS-AC）のホームページで公開されているため、申請先の選定の際は確認することが大切です。

ISMS認証の維持および更新審査プロセス

ISMS認証取得後も、維持・更新のための審査があります。**年に1回以上の維持審査（サーベイランス審査）**と、**3年ごとに認証の有効期限を更新するための更新審査**です。どちらにおいても、組織のISMSが引き続き規格に適合し、有効に維持されているかが確認されます。



7-3-1. NIST サイバーセキュリティフレームワーク（CSF）の概要

サイバーセキュリティフレームワーク（CSF）の概要およびISMSとの関係性について説明します。

NIST サイバーセキュリティフレームワーク（CSF）とは

CSFは、NISTが作成したサイバー攻撃対策に重点を置いたフレームワークであり、防御にとどまらず、検知・対応・復旧といったインシデント対応が含まれています。
また、多様な企業に適用できるように要求事項が汎用的になっています。指示書やノウハウ集ではありません。CSFをどのように利用するかは、実施する組織に委ねられているため、CSFをしっかりと理解した上で、サイバーセキュリティ対策を検討することが大切です。

CSFの3つの構成要素（コア、ティア、プロファイル）

CSFは、組織がセキュリティ対策を継続的に改善するため、①コア（サイバーセキュリティ対策の一覧）、②ティア（対策状況を数値化するための成熟度評価基準）、③プロファイル（サイバーセキュリティ対策の現状とあるべき姿を記述するためのフレームワーク）の3つの要素で構成されています。

「コア」の概要

すべての重要インフラ分野に共通するサイバーセキュリティ対策、期待される成果、適用可能な参考情報を定義したもの。

✓ 「識別」「防御」「検知」「対応」「復旧」の5つの機能に分類される。各機能の下には複数のカテゴリが存在し、各カテゴリはそれぞれ複数のサブカテゴリを有する。

「ティア」の概要

組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したもの。

✓ 指標は4段階あり、次のとおり。 ① ティア１：部分的である ② ティア２：リスク情報を活用している ③ ティア３：繰り返し適用可能である ④ ティア４：適応している

「プロファイル」の概要

フレームワークのカテゴリ及びサブカテゴリに基づき、サイバーセキュリティリスクに対する期待される効果を現すもの。

✓ サイバーセキュリティリスクへの対応状況として、「あるべき姿」と「現在の姿」をまとめたもの。

✓ 「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整する。

（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

7-3-2. NIST サイバーセキュリティフレームワーク（CSF）の構成

「コア」

コアとは、業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものです。 「識別」「防御」「検知」「対応」「復旧」の5つの機能に分類され、各機能の下には複数のカテゴリが存在し、合計23個あります。また、各カテゴリにはそれぞれ複数のサブカテゴリが存在しており、サブカテゴリは合計で108個あります。

機能	説明	カテゴリ
識別	組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。	• 資産管理 • ビジネス環境 • ガバナンス • リスク評価 • リスク管理戦略 • サプライチェーンリスク管理
防御	重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。	• アクセス制御 • 意識向上およびトレーニング • データセキュリティ • 情報を保護するためのプロセスおよび手順 • 保守 • 保護技術
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する。	• 異常とイベント • セキュリティの継続的なモニタリング • 検知プロセス
対応	サイバーセキュリティインシデントに対処するための適切な対策を検討し実施する。	• 対応計画 • コミュニケーション • 分析 • 低減 • 改善
復旧	サイバーセキュリティインシデントにより影響を受けた機能やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。	• 復旧計画 • 改善 • コミュニケーション

コアの構成
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

サブカテゴリ（例）

カテゴリ	サブカテゴリ
資産管理	自組織内の物理デバイスとシステムが、目録作成されている。
	自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。
	組織内の通信とデータフロー図が、作成されている。
	外部情報システムが、カタログ作成されている。
	リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。
	全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。

7-3-2. NIST サイバーセキュリティフレームワーク（CSF）の構成

コアの各カテゴリとISMSの管理策は、以下の通りに対応しています。

CSF	ISMS
ID.GVガバナンス	リーダーシップおよびコミットメント・方針・認識・情報セキュリティのための方針群・経営陣の責任
ID.BEビジネス環境	組織の役割、責任および権限・情報セキュリティの役割および責任・職務の分離
ID.AM資産管理 PR.AT意識向上およびトレーニング	資源・力量
ID.RAリスクアセスメント ID.RMリスクマネジメント戦略	リスクおよび機会に対処する活動・情報セキュリティ目的およびそれを達成するための計画策定・情報セキュリティリスクアセスメント・情報セキュリティリスク対応・脅威インテリジェンス・情報およびその他の関連資産の目録・情報およびその他の関連資産の利用の許容範囲・情報の分類・知的財産権
PR.ACアイデンティティ管理、認証／アクセス制御 PR.DSデータセキュリティ PR.IP情報を保護するためのプロセスおよび手順 PR.PT保護技術	文書化した情報・情報のラベル付け・情報転送・アクセス制御・識別情報の管理・認証情報・アクセス権・記録の保護・プライバシーおよびPIIの保護・操作手順書・人的管理策・物理的管理策・技術的管理策
PR.MA保守 DE.AE異常とイベント DE.CMセキュリティの継続的なモニタリング DE.DP検知プロセス	コミュニケーション・運用の計画および管理・監視、測定、分析および評価・内部監査・マネジメントレビュー・継続的改善・不適合および是正処置・プロジェクトマネジメントにおける情報セキュリティ・資産の返却・法令、規則および契約上の要求事項・情報セキュリティの独立したレビュー・情報セキュリティのための方針群、規則および標準の順守
RS.RP対応計画 RS.AN分析 RS.MI低減 RS.IM改善	情報セキュリティインシデント管理の計画および準備・情報セキュリティ事象の評価および決定・情報セキュリティインシデントへの対応・情報セキュリティインシデントからの学習・証拠の収集
RC.RP復旧計画 RC.IM改善	事業の中断・阻害時の情報セキュリティ・事業継続のためのICTの備え
ID.SCサプライチェーンリスクマネジメント	運用の計画および管理・供給者関係における情報セキュリティ・供給者との合意におけるセキュリティの取扱い・ICTサプライチェーンにおける情報セキュリティの管理・供給者のサービス提供の監視、レビューおよび変更管理・クラウドサービスの利用における情報セキュリティ
RS.COコミュニケーション RC.COコミュニケーション	関係当局との連絡・専門組織との連絡

CSFとISMSの対応関係
（出典）経済産業省 「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

7-3-2. NIST サイバーセキュリティフレームワーク（CSF）の構成

「ティア」

ティアとは、組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものです。指標は以下の4段階があります。各ティアの定義は、組織に応じて柔軟にアレンジすることが可能です（以下の表は一例です）。また、必ずしもすべてのカテゴリにおいて最高レベル（ティア4）を目指す必要はありません。ビジネス特性や情報資産の実態などに応じて、カテゴリごとに目指すべきティアを設定しましょう。

ティア1：部分的である （Partial） セキュリティ対策は経験に基づいて実施される。 セキュリティ対策は組織として整備されておらず場当たり的に実施されている。
ティア2：リスク情報を活用している （Risk Informed） セキュリティ対策はセキュリティリスクを考慮して実施されているが、組織として方針や標準が定められてはいない、あるいは非公式に存在する。
ティア3：繰り返し適用可能である （Repeatable） セキュリティ対策は組織の方針・標準として定義、周知されており、脅威や技術の変化に伴い方針・標準は定期的に更新される。
ティア4：適応している （Adoptive） 組織で標準化されたセキュリティ対策は、脅威や技術の変化、組織における過去の教訓やセキュリティ対策に関するメトリックスなどを参考に継続的かつタイムリーに調整される。

（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

「プロファイル」

プロファイルとは、機能・カテゴリ・サブカテゴリについて、組織ごとに考慮すべき点を踏まえて調整し、整理したものです。組織はプロファイルを用いることで、サイバーセキュリティ対策の現在の状態（現在の姿）と、目標の状態（あるべき姿）を明らかにすることができます。そして「現在の姿」と「あるべき姿」を比較することで、サイバーセキュリティマネジメント上の目標を達成する上で、解消が必要なギャップを知ることができます。

「あるべき姿」の策定については、組織のビジネス上の要求、リスク許容度、割当可能なリソースに基づき、コアの機能、カテゴリ、サブカテゴリの到達地点を調整します。

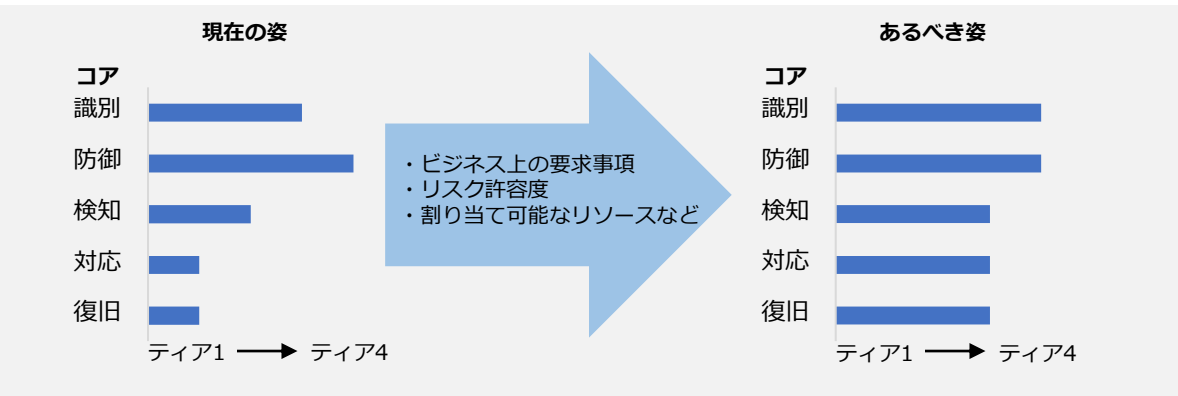


図37.プロファイルの活用イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

7-3-3. NIST SP 800

NIST SP 800シリーズとCSFの関連性

CSFは、NISTが定義するサイバーセキュリティ対策アプローチの中で最も上位に位置付けられており、セキュリティ管理手法の概念や管理方針・体制の整備など包括的な内容が記載されています。CSFの下位概念に位置付けられているのが、NIST SP 800シリーズです。実施すべきタスクと手順、推奨技術の特定など、セキュリティ管理の手法について具体的に明記されています。

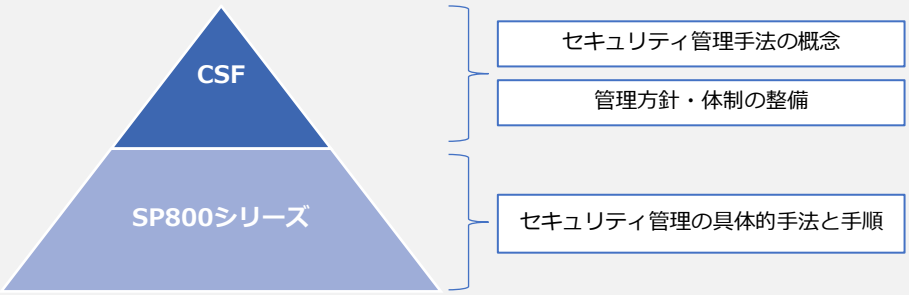


図38. CSFとSP800シリーズの関係

NIST SP 800-53、NIST SP 800-171、NIST SP 800-161

NIST SP 800シリーズの中から、ガイドラインの一部を紹介します。

NIST SP 800-53
米国政府内の情報システムをより安全なものにし、効果的にリスク管理するためのガイドラインのことです。対象は連邦政府機関で、政府の機密情報（CI:Classified information）の保護を目的としています。
NIST SP 800-171
NIST SP 800-53から民間企業・組織向けに要件を抽出したものです。サプライチェーンに存在する、業務委託先や関連企業のすべてが準拠すべきセキュリティ基準を示しています。対象は、多くの民間企業・組織で、政府の機密情報以外の重要情報（CUI:Controlled Unclassified Information）の保護を目的としています。
NIST SP 800-161
調達から販売・供給までの一連のサプライチェーンに起因する様々なリスクに対して、組織として対応するためのガイドラインです。業務委託先や関連企業におけるセキュリティ対策を目的としています。

NIST SP 800-53とNIST SP 800-171は、以下のように保護する情報と対策を行う組織が異なりますが、どちらも密接に関連しているため2つ同時に参照する必要があります。

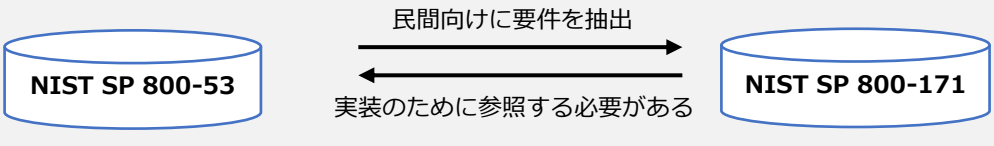


図39. NIST SP 800-53とNIST SP 800-171の関係

7-3-4. ISMSとの関連性

CSFとISMSの関連性

CSFとISMSの主な共通点

汎用性が高い
　ISMSとCSFは、汎用性が高く、あらゆる組織で使用することができます。まずはISMSをベースにして情報セキュリティ対策を行い、必要に応じてCSFの内容を取り入れるとよいでしょう。

サイバーセキュリティ対策方法
　ISMSとCSFはどちらも「識別」「防御」「検知」「対応」「復旧」といったサイバーセキュリティ対策を挙げています。

任意性がある
　ISMSとCSFはどちらも、提示しているすべてのセキュリティ対策を取り入れることは求めておらず、何を取り入れるかはそれぞれの組織で決定可能です。

CSFとISMSの主な相違点

第三者認証制度の有無
　ISMSには、第三者機関による認証制度（適合性評価制度）が存在します。これに対して、CSFにはそのような認証制度はありません。そのため、情報セキュリティ対策を行っていることを顧客や取引先に対して客観的に示すためには、ISMSを構築して認証を受けることが有効です。

目標への到達手段
　ISMSは、PDCAサイクルをまわすことで、情報セキュリティマネジメント体制を構築する一方、CSFでは特にPDCAサイクルをまわすといった記載はありません。CSFの「プロファイル」では、現在の状況と理想の状況とのギャップを明確にすることで、とるべき対応策の優先順位を決めて、それに従って実施していくことになります。

7-4-1. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）の概要

概要

Society5.0の到来に従い、サイバー空間とフィジカル空間が融合することで、これまでにはなかった様々な新たな価値（モノやサービス）が提供されることになります。
サプライチェーンは、従来の形（例：調達→生産→物流→販売）から、サイバー空間とフィジカル空間のつながりや、サイバー空間のデータのつながりを考える必要がある形へと変化していくことになります。このような新たな形のサプライチェーンは、『**価値創造過程（バリュークリエイションプロセス）**』と定義されています。

製品を製造して消費者に販売するまでが従来のサプライチェーンだとした場合、バリュークリエイションプロセスでは、消費者の使用データの収集やシステムのアップデートなどを通じて消費者との関係が継続します。サイバー空間とフィジカル空間の接点のすべてがサイバー攻撃の対象となると考えられ、工場のシステムだけでなく、製品そのものに対する攻撃、個人情報などのデータを蓄積した本社に対する攻撃が行われる危険性があります。

このような新たなサプライチェーンの概念に求められるセキュリティへの対応指針として、政府は『サイバー・フィジカル・セキュリティ対策フレームワーク』（CPSF）を策定しました。

CPSFは、ISMSやCSFのフレームワークの内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策に対応したフレームワークとなっています。

目的と適用範囲

CPSFの主な目的は、新たな産業社会におけるバリュークリエイションプロセス全体の理解、リスク源の明確化、必要なセキュリティ対策全体像の整理を行うことです。従来のサプライチェーンに適用可能なセキュリティ対策に加えて、新たな産業社会の変化から生じる特有の対策も含まれています。

本フレームワークの適用範囲としては、新たな産業社会におけるバリュークリエイションプロセス全体となります。企業が本フレームワークを参考にし、自社の実態に合わせて、適切なセキュリティ対策を実施することが重要です。

CPSFに含まれる対策

従来型サプライチェーンにおいても適用可能な対策	新たな産業社会に変化したからこそ新たに対応が必要な対策

- **新たな産業社会における**バリュークリエイションプロセス全体が適用範囲
- それぞれの組織に応じてセキュリティ対策を選定することが可能

7-4-1. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）の概要

従来のサプライチェーンに対するセキュリティの考え方では、セキュリティ対応を行っている組織間の取引であれば、サプライチェーン全体の信頼性が確保される「組織マネジメントの信頼性」に基点が置かれていました。

しかしながら、 Society5.0では、従来のサプライチェーンのように、組織のマネジメントの信頼性に基点を置くことだけでは、バリュークリエイションプロセスの信頼性を確保することが困難となります。IoT機器を使用した場合、フィジカル空間の様々な情報はデジタル化され・サイバー空間へ取り込まれ、新たな価値が生み出されます。その一方で、マネジメントルールを徹底しただけでは、サイバー空間に取り込んだデータの適切な保護といった信頼性を確保することはできなくなります。

バリュークリエイションプロセスの信頼性を確保するためには、セキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要になります。そのため、CPSFでは、バリュークリエイションプロセスが発生する産業社会を3つの層、バリュークリエイションプロセスに関与する構成要素を6つに整理し、CPSFの基本構成としました。3つの層でリスク源を洗い出し、6つの構成要素で各リスク源に対する対策要件および具体的な対策例を示します。

3層構造モデル

各層における信頼性の基点は以下の通りです。
- 第1層では、企業（組織）のマネジメントの信頼性
- 第2層では、サイバー空間とフィジカル空間のつながりにおける、要求される情報の正確性に応じて適切な正確さで情報が変換される “転写”機能の信頼性
- 第3層では、サイバー空間のつながりにおける、データの信頼性

サイバー空間におけるつながり

[第3層]

自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

フィジカル空間とサイバー空間のつながり

[第2層]

フィジカル空間・サイバー空間を正確に”転写”する機能の信頼性を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラなどの信頼）

企業間のつながり

[第1層]

適切なマネジメントを基盤に各主体の信頼性を確保

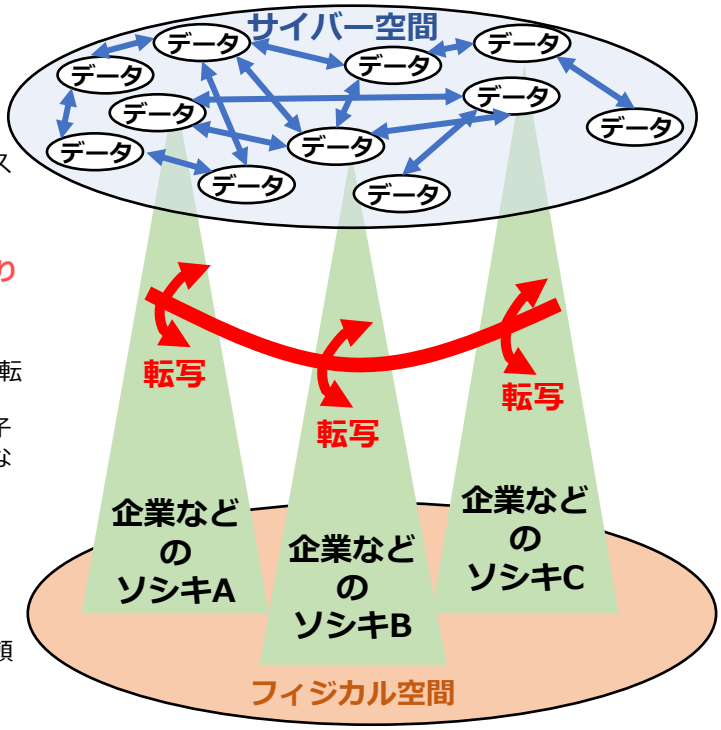


図40.3層構造モデルと各層における信頼性
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

7-5-1. サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドライン

経営者が主体となってサイバーセキュリティ対策を実施する際に、経済産業省とIPAが共同で発行している「サイバーセキュリティ経営ガイドライン」が参考になります。本ガイドラインでは、経営者がサイバーセキュリティ対策を実行する際に認識するべき事項と、サイバーセキュリティ対策の責任者（CISOなど）に指示するべき事項を包括的にまとめています。

平成29年のVer2.0の公開以降、企業のサイバーセキュリティ対策を取り巻く環境が変化しました。そのため、最新の状況への認識と対策の実践が可能となるように内容が見直され、令和5年にVer3.0が最新版として公開されました。

企業のサイバーセキュリティ対策を取り巻く環境の変化	
テレワークの活用	テレワークなどのデジタル環境の活用を前提とする働き方の多様化
サイバー空間とフィジカル空間のつながり	インターネットなどのサイバー空間と現物の取引を行うフィジカル空間のつながりの緊密化と、それに伴うリスクの顕在化
セキュリティ対象の変化・拡大	情報資産だけでなく、制御系を含むデジタル基盤の保護がサイバーセキュリティの対象となる変化と拡大
ランサムウェアの被害	ランサムウェアによる被害の顕在化により、企業におけるサイバーセキュリティに関する被害は情報漏えいにとどまらず、企業の事業活動の停止へと影響が拡大
サプライチェーンを介した被害拡大	国内外のサプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、サプライチェーン全体を通じた対策の必要性の高まり
ESG投資の拡大	ESG（Environment, Society, Governance）投資の拡大により、コーポレートガバナンスおよびERM（エンタープライズリスクマネジメント）の改善に向けた取組に対する関心の高まり

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

次のページからは、サイバーセキュリティ対策に取組む上で、経営者が認識するべき事項と実行するべき事項を紹介し、経営目線でのサイバーセキュリティ対策について全体像を説明します。また、経営者とセキュリティ担当者それぞれの立場に応じて、具体的に行うべきことについて説明した後、サイバーセキュリティ対策を実践するための手順を説明します。

One Point

サイバーセキュリティ対策は企業の価値増大への投資

サイバーセキュリティ対策はやむを得ない「費用」と考えるのではなく、「投資」と位置付けることが重要です。なぜなら、サイバーセキュリティ対策は、企業活動における損失やコストを減らし、企業の価値を維持・増大させるために必要だからです。サイバーセキュリティに関するリスクを経営リスクの一環として取り入れ、適切な対策に投資することで、リスクを許容可能な範囲まで低減させることができます。企業としては、この取組を通じて社会的責任を果たし、経営者はこの責務を認識する必要があります。

7-5-1. サイバーセキュリティ経営ガイドライン

経営者が認識するべき3原則

経営者は、以下の3原則を認識し、対策を進める必要があります。

原則1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップの元で対策を進めることが必要
原則2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
原則3	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営の重要10項目

経営者は、以下の重要10項目について、サイバーセキュリティ対策を実施する上での責任者や担当部署（CISO、サイバーセキュリティ担当者など）への指示を通じて組織に適した形で確実に実施させる必要があります。これらは、組織のリスクマネジメントの責任を担う経営者が、単なる指示ではなく、自らの役割として発信する必要があります。リスク対策に関する実施方針の検討、予算や人材の割当、実施状況の確認や問題の把握と対応など、多くのことを通じてリーダーシップを発揮することが求められます。

経営者がリーダーシップをとったセキュリティ対策の推進

サイバーセキュリティリスクの管理体制構築
指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示２ サイバーセキュリティリスク管理体制の構築
指示３ サイバーセキュリティ対策のための資源（予算、人材など）確保

サイバーセキュリティリスクの特定と対策の実装
指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示６ PDCAサイクルによるサイバーセキュリティ対策の継続的改善

インシデント発生に備えた体制構築
指示７ インシデント発生時の緊急対応体制の整備
指示８ インシデントによる被害に備えた事業継続・復旧体制の整備

サプライチェーンセキュリティ対策の推進

指示９ ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握および対策

ステークホルダーを含めた関係者とのコミュニケーションの推進

指示１０ サイバーセキュリティに関する情報の収集、共有および開示の促進

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

7-5-1. サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営の重要10項目の概要

経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISOなど）に指示すべき「重要10項目」のポイントと、対策例の一部を紹介します。

指示１ サイバーセキュリティリスクの認識、組織全体での対応方針の策定

- ✓ サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定させる。
- ✓ 策定した対応方針を対外的な宣言として公表させる。

対策例

- 経営者が組織全体の対応方針を組織の内外に宣言できるよう、企業の経営方針と整合を取ったセキュリティポリシーを策定する。その際、製造、販売、サービスなど、事業が立脚しているすべての基盤（設備、システム、情報などの資産、流通プロセスなど）に影響を及ぼすと考えられるサイバーセキュリティリスクに応じた対応方針を検討する。

指示２ サイバーセキュリティリスク管理体制の構築

- ✓ サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構成させる。
- ✓ サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

対策例

- 役割遂行に求められる責任や専門性、人的資源の状況に応じて、組織内要員で対応すべきものと外部の専門サービスに委託すべきものとの切り分けを行う。
- 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを監査する。

指示３ サイバーセキュリティ対策のための資源（予算、人材など）確保

- ✓ サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材など）を確保した上で、具体的な対策に取組ませる。
- ✓ すべての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

対策例

- 事業が立脚しているすべての基盤の安全性の担保のために必要なサイバーセキュリティ対策を明確にし、それに要する費用を確保する。
- 従業員向けやセキュリティ担当者向けなどの研修などのための予算を確保し、継続的に役割に応じたセキュリティ教育を実施する。
- セキュリティ対策業務に従事する人材のみならず、デジタル部門、事業部門、管理部門などのあらゆる業務に従事する人材に、「プラス・セキュリティ」知識・スキルの習得を促す。

指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

- ✓ 事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- ✓ サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

対策例

- 組織における情報のうち、経営戦略の観点から守るべき情報を特定し、それらがどこに保存され、どこで扱われているかを把握する。その際、自社の営業秘密を外部のクラウドサービスで管理したり、テレワークなどの新しい働き方を導入したりしていることの影響を適切に反映させる。

指示５ サイバーセキュリティリスクに効果的に対応する仕組みの構築

- ✓ サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- ✓ 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

対策例

- 重要業務を行う端末、ネットワーク、システムまたはサービス（クラウドサービスを含む）には、多層防御を実施する。
- 従業員に対する教育を定期的に行い、適切な対応が行えるよう日頃から備える。

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

7-5-1. サイバーセキュリティ経営ガイドライン

指示６ PDCAサイクルによるサイバーセキュリティ対策の継続的改善

- ✓ リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえたPDCAサイクルを運用させる。
- ✓ 経営者は対策の状況を定期的に報告させることなど通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- ✓ 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

対策例

- 必要に応じて、ISO/IEC 27001規格に基づくISMSなど、国際標準となっているPDCAマネジメントシステムの認証を活用する。

指示７ インシデント発生時の緊急対応体制の整備

- ✓ 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRTなど）を整備させる。
- ✓ 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- ✓ インシデント発生時の対応について、適宜実践的な演習を実施させる。

対策例

- インシデント発生時の体制整備、ルール整備に当たって、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参照しながら、社内理解を深める。
- インシデントの発生を想定した緊急対応に関する演習を役員や職員に対して定期的に実施し、緊急時にどのような手順で初動対応を行うべきかについて、すべての関係者が体験を通じて理解する。

指示８ インシデントによる被害に備えた事業継続・復旧体制の整備

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

対策例

- **設**備投資計画を立案する際に、事業継続に影響をもたらす要因として、自然災害やパンデミックなどにサイバーセキュリティリスクを加え、その対策を要求仕様などに反映させる。
- 定期的な復旧演習の実施により、復旧対応に関わる関係者がその手順について、体験を通じて理解する。

指示９ ビジネスパートナーや委託先などを含めたサプライチェーン全体の状況把握及び対策

- ✓ サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先などを含めた対策状況の把握を行わせる。
- ✓ ビジネスパートナーなどとの契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施など、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

対策例

- 系列企業、サプライチェーンのビジネスパートナーやシステム管理の委託先などがSECURITY ACTIONを実施していることを確認する。なお、ISMSなどのセキュリティマネジメント認証を取得していることがより効果的である。

指示１０ サイバーセキュリティに関する情報の収集、共有及び開示の促進

- ✓ 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
- ✓ 入手した情報を有効活用するための環境整備をさせる。

対策例

- 株主やステークホルダーとの対話、広報による一般向け情報開示などの機会において、サイバーセキュリティインシデントに備えた日頃の取組などの情報開示に積極的に取組む。
- 中小企業の場合は、商工会議所、商工会などを通じて地元で情報共有を行うことのできる相手を確保する。
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を参考に、インシデントに備え、サイバーセキュリティ専門組織との情報共有や被害に係る情報の公表を行うに当たっての観点について、あらかじめ理解しておく。

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

詳細理解のため参考となる文献（参考文献）	
サイバー攻撃被害に係る情報の共有・公表ガイダンス	https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

7-5-2. サイバーセキュリティ経営ガイドラインの読み方

ここでは「経営者」、「情報セキュリティ対策の責任者（CISOなど）」それぞれの立場から、本ガイドラインの内容を実践する際の役割、認識するべきことについて記載します。

対象者	経営者
役割	・「3原則」の理解 ・重要１０項目について、情報セキュリティ対策の責任者（CISOなど）に指示を出す ・リーダーシップの発揮
認識すべきこと	**ERM（エンタープライズリスクマネジメント）にサイバー攻撃のリスクを含めること** 現在、企業活動の多くはITに依存しています。そのため、内部統制システムの構築や、コーポレートガバナンス・コードに基づく開示と対話などにおいて、サイバー攻撃のリスクを考慮する必要があります。 **サプライチェーン上のリスクを認識すること** 現在、サプライチェーンの多様化が進み、サイバー攻撃の起点は広く拡散しています。したがって、サプライチェーン全体を考慮したリスクマネジメントが必要です。 **サイバーセキュリティ対策は担当者に丸投げしてはいけない** 経営者は、インシデント発生時に法的・社会的責任を負い、事業停止や新たな脅威に対処するための経営判断を迫られることがあります。そのため、経営者は、サイバーセキュリティ対策を担当者に丸投げせずに、自ら主体的に取組む必要があります。 **サイバーセキュリティ対策は投資と位置付けること** サイバーセキュリティ対策への投資では、直接的な収益を算出することは困難です。しかし、サイバーセキュリティ対策への投資は、企業活動におけるコストや損失を減らすために必要不可欠な投資であるとともに、将来の事業活動・成長に必須な投資でもあります。

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

One Point

ERM（エンタープライズリスクマネジメント）とは

企業が直面するリスクに対して、企業全体で管理することです。国際競争や情報技術の急速な進化により、企業が直面するリスクも多様化しています。このような状況下で、従来の部門ごとにリスクに対して管理するのではなく、企業全体で管理することが重要です。

7-5-2. サイバーセキュリティ経営ガイドラインの読み方

対象者	情報セキュリティ対策を実施する上で責任者となる担当幹部（CISOなど）
役割	・重要10項目を理解すること ・経営者に対して適宜状況報告を行い、経営者が適切な判断を行うために必要な情報を提供すること
認識すべきこと	**経営者から指示される以下の事項に関して、より具体的な取組み方を検討し、セキュリティ担当者に対して指示する必要があること** ・サイバーセキュリティリスクの管理体制構築 ・サイバーセキュリティリスクの特定と対策の実装 ・インシデント発生に備えた体制を構築 ・サプライチェーンセキュリティ対策の推進 ・ステークホルダーを含めた関係者とのコミュニケーションの推進

（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

7-5-3. サイバーセキュリティ経営ガイドラインの実践の流れ

サイバーセキュリティ経営ガイドラインの活用手順

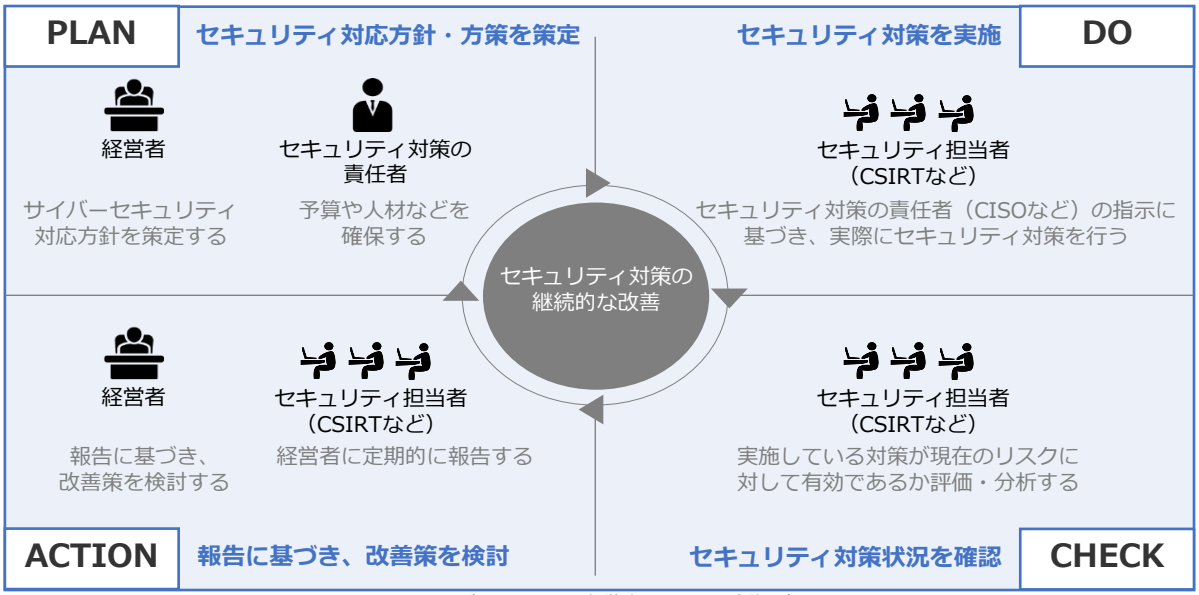


図41. サイバーセキュリティ経営ガイドラインの全体の流れ
（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

PLAN

はじめに、サイバーセキュリティ対応方針・方策を策定します。
・経営者は、3原則を認識した上でサイバーセキュリティ対応方針を策定します。
・セキュリティ対策の責任者（CISOなど）は、経営者の指示に基づき、リスクを許容範囲内に抑制するための方策を検討し、必要となる資源（予算や人材など）を確保します。

DO

セキュリティ担当者（CSIRTなど）は、セキュリティ対策の責任者（CISOなど）の指示に基づき、実際にセキュリティ対策を行っていきます。具体的には以下の作業を行います。
・リスクの把握や対応計画の策定
・サイバー攻撃の防御や検知
・分析などの保護対策の実施
・緊急時の対応体制を整備、事業継続、復旧体制の整備

CHECK

実施しているセキュリティ対策がリスクに対して有効であるか評価・分析をします。
・セキュリティ担当者（CSIRTなど）は、サイバーセキュリティ経営ガイドライン付録の「サイバーセキュリティ経営チェックシート」や「サイバーセキュリティ経営可視化ツール」を活用し、経営者が指示した事項の実践状況をチェックします。

ACTION

セキュリティ担当者（CSIRTなど）は、経営者に指示された事項の実践状況について、CISOを通じて経営者に報告し、経営者は報告をもとに改善策を検討します。
・新たなサイバーセキュリティリスクの発見などにより、追加の対応が必要な場合には、対処方針を修正します。

コラム

ISMS[ISO/IEC 27001]認証の取得にあたって

ISMSの国際規格であるISO/IEC 27001の認証を取得している企業の数は、この20年間ほどで著しく増加しています。2002年には、約140社だった取得企業数は、2015年には約4,600社、そして2023年8月現在では約7,400社となっております。この推移から、情報セキュリティの重要度が高まっており、各企業がセキュリティ対策に乗り出していることが窺えます。
そのようなISO/IEC 27001ですが、取得することでどのようなメリットがあり、考慮すべきポイントがあるのでしょうか。

メリットについては、テキスト内でも説明しているように、顧客や取引先といった利害関係者へ信頼を与えられることとなります。一定の水準以上を満たした管理体制を証明できるため、公共案件の入札や、取引先からの取引要件を満たすことにつながり、商談機会の拡大が期待できます。
また、リスクマネジメント体制の確立により、事故防止に役立ちます。ISO/IEC 27001を満たすように社内のルールを守ることや、事業変化に応じたリスクアセスメント、継続的な改善の実施により、事故の防止活動がされている状態となります。また、個人情報保護法といった情報保護関係の法令順守にもつながります。

一方で、費用面では、コンサル費用、申請費用、審査費用などがかかるため、必要な予算を確保して準備を進める必要があります。状況によっては、予算確保が容易ではない場合があるかもしれません。また、取得までの作業や、取得後の定期的な運用の手間を考慮する必要があります。

ただし、一度ISO/IEC 27001に準拠する体制を確立すれば、法令への準拠や安全管理策は仕組み化されます。また、事故防止による経済的損失の抑止効果があることや、顧客や取引先などのステークホルダーの信頼を獲得できることなど、将来の事業活動や成長に必要な費用だということを考えれば、ISMS認証取得に必要な経費は、中長期的に回収可能な投資だと考えることができます。

第8章. セキュリティ対策基準の策定

8-1. 対策基準の策定

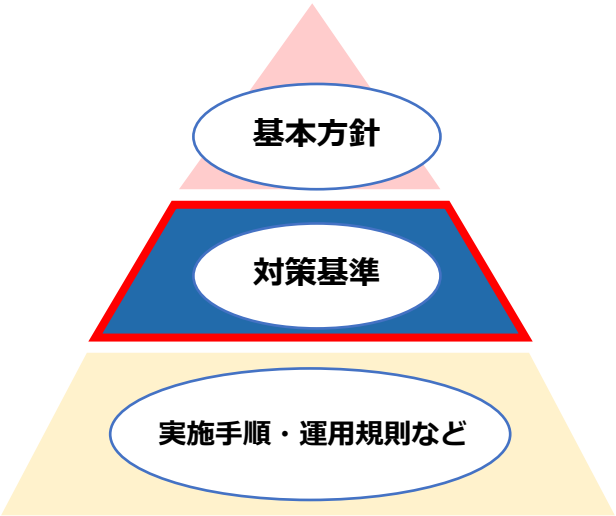
章の目的
第8章では、ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法について理解することを目的とします。

主な達成目標
◘ サイバーセキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること ◘ 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

8-1-1. セキュリティ対策基準の概要

情報セキュリティポリシーは、一般的に「基本方針」「対策基準」「実施手順・運用規則など」で構成されます。「基本方針」には、組織や企業の代表者による情報セキュリティに対する考え、必要性、取り扱い方針などの宣言が含まれます。「対策基準」には、各業務や部署におけるセキュリティ対策をまとめた規定を記載します。「実施手順」には、対策基準ごとに、対策内容を具体的な手順として記載します。

以下では、「対策基準」策定方法の考え方について、説明します。



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

図42. セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”.
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-3.html,(参照 2023-08-21).

対策基準を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たすことができます。ただし、対策基準で記載する内容は抽象度が高いため、具体的に実践で使用することは難しい内容です。実際に運用を行うためには、策定した対策基準に従って、実施手順などを作成する必要があります。

対策基準の内容を定める際は、網羅的なフレームワークを参考にすることが推奨されます。企業の現状、目標に応じてフレームワークを使用せずに段階的な対策基準の策定を行う場合は、「3-4-1. サイバーセキュリティアプローチ方法の概要」記載のアプローチ方法を参考にすることができます。アプローチ方法はレベルが上がるにつれ、網羅性も上がります。それぞれの特徴を次ページで説明します。

対策基準を策定するためのアプローチ方法

Lv.1
クイックアプローチ
（インシデントベース）

Lv.2
ベースラインアプローチ
（ガイドライン・ひな形ベース）

Lv.3
網羅的アプローチ
（フレームワークベース）

8-1-2. 対策基準策定のアプローチ方法

クイックアプローチ、ベースラインアプローチ、網羅的アプローチの概要、主な特徴と想定される適用ケースを説明します。

アプローチ手法	特徴	想定される適用ケース
Lv.1 クイックアプローチ	即時の対応や緊急事態への対処に適したアプローチ手法。 様々なインシデント事例内容を参考にし、対策基準を策定。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対処する場合。
Lv.2 ベースラインアプローチ	組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。 ガイドラインやひな形を参考とし、対策基準を策定。	組織的に一定以上の対策基準を策定する場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。 ISMSなどの認証が可能なレベルを目指して、対策基準を策定。	ISMSのフレームワークに沿った対策基準を策定する場合。

メリット・デメリット

アプローチ手法	メリット	デメリット
Lv.1 クイックアプローチ	• 小規模な対策や修正を迅速に実施可能。 • 低コストでリスクを軽減。 • 進行中の攻撃の拡大や影響を最小限に抑えられる。	• 詳細な分析や検討が不十分な場合がある。 • 短期的な解決策に偏りがちになる。
Lv.2 ベースラインアプローチ	• 組織全体で一貫性を確保できる。 • 最低基準となるセキュリティ対策を講じることができる。	• 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
Lv.3 網羅的アプローチ	• 可能な限り多くの脅威や攻撃手法に対して対策を講じる。 • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持できる。	• 全体的な実施には時間がかかる。

8-1-2. 対策基準策定のアプローチ方法

Lv.1 クイックアプローチ

Lv.1 クイックアプローチでは、様々なインシデント事例内容を参考にします。インシデント事例は、報道される事例、情報セキュリティ10大脅威、実際のインシデントなどから選択します。自社で発生する可能性が高いと考えられるインシデント事例や、実際に発生したときの被害が大きいと考えられるインシデント事例を参考にして、対策基準を策定することが重要です。以下は、情報セキュリティ10大脅威の『組織』に対する脅威で3年連続第1位になっている、ランサムウェアに対する対策基準の例です。

対策基準（例）

1. 対象とする脅威
ランサムウェアによる情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取など

2. 組織的対策
- 組織としてのランサムウェア対応体制の確立 ・インシデント対応体制を整備し対応する

3. 人的対策
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 提供元が不明なソフトウェアを実行しない
- 適切な報告/連絡/相談を行う

4. 物理的対策
- 適切なバックアップ運用を行う

5. 技術的対策
- 公開サーバーへの不正アクセス対策
- 共有サーバーなどへのアクセス権の最小化と管理の強化
- 多要素認証の設定を有効にする
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

(出典) IPA「情報セキュリティ10大脅威 2023」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 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
マルウェア「ランサムウェア」の脅威と対策（対策編）	https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

8-1-2. 対策基準策定のアプローチ方法

Lv.2 ベースラインアプローチ

Lv.2 ベースラインアプローチでは、ガイドラインやひな形を参考とし、対策基準を策定します。IPAの「中小企業の情報セキュリティ対策ガイドライン」や以下の【参照資料】を活用することで、自社にあった対策基準を策定することできます。

【参照資料】
・リスク分析シート（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）
・情報セキュリティ関連規程（出典：IPA）
・自己点検チェックリスト（出典：個人情報保護委員会）

IPA「情報セキュリティ関連規程（サンプル）」を活用した対策基準（例）

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1.情報セキュリティのための組織
情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。

(出典) IPA「情報セキュリティ関連規程（サンプル）」を基に作成

詳細理解のため参考となる文献（参考文献）	
リスク分析シート	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
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
情報セキュリティ関連規程	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx
自己点検チェックリスト	https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

8-1-2．対策基準策定のアプローチ方法

Lv.3 網羅的アプローチ

Lv.3 網羅的アプローチでは、ISMSなどの認証が可能なレベルを目指して、対策基準を策定します。そのため、ISMSのフレームワークに沿って、技術的対策といった一部の内容ではなく、運用や監査についても対策基準に記載します。

ISMSフレームワークを活用した対策基準（例）

情報セキュリティ対策基準

1.目的

2. 適用範囲

3. 用語の定義

4. 組織的対策

5. 物理的対策

6. 人的対策

7. 技術的対策

93種の管理策を活用（ISMSフレーワーク）（情報セキュリティマネジメントの確立・運用・監査を含んだ網羅的な管理策）

93種の管理策ごとに対策基準を策定

5.組織的管理策	5.24 情報セキュリティインシデント管理の計画および準備	
5.1 情報セキュリティのための方針群	5.25 情報セキュリティ事象の評価および決定	
5.2 情報セキュリティの役割および責任	5.26 情報セキュリティインシデントへの対応	
5.3 職務の分離	5.27 情報セキュリティインシデントからの学習	
5.4 経営陣の責任	5.28 証拠の収集	
5.5 関係当局との連絡	5.29 事業の中断・阻害時の情報セキュリティ	
5.6 専門組織との連絡	5.30 事業継続のためのICTの備え	
5.7 脅威インテリジェンス	5.31 法令、規制および契約上の要求事項	
5.8 プロジェクトマネジメントにおける情報セキュリティ	5.32 知的財産権	
5.9 情報およびその他の関連資産の目録	5.33 記録の保護	
5.10 情報および その他の関連資産の利用の許容範囲	5.34 プライバシーおよび PII の保護	
5.11 資産の返却	5.35 情報セキュリティの独立したレビュー	
5.12 情報の分類	5.36 情報セキュリティのための方針群、規則および標準の順守	
5.13 情報のラベル付け	5.37 操作手順書	
5.14 情報転送	6.人的管理策	
5.15 アクセス制御	6.1 審査	
5.16 識別情報の管理	7.物理的管理策	8.10 情報の削除
5.17 認証情報	7.1 物理的セキュリティ境界	8.11 データマスキング
5.18 アクセス権	7.2 物理的入退	8.12 データ漏えいの防止
5.19 供給者関係における情報セキュリティ	7.3 オフィス、部屋および施設のセキュリティ	8.13 情報のバックアップ
5.20 供給者との合意におけるセキュリティの取扱い	7.4 物理的セキュリティの監視	8.14 情報処理施設の冗長性
5.21 ICTサプライチェーンにおける情報セキュリティの取扱い	7.5 物理的および環境的脅威からの保護	8.15 ログ取得
5.22 供給者のサービス提供の監視およびレビューおよび変更管理	7.6 セキュリティを保つべき領域での作業	8.16 監視活動
5.23 クラウドサービス利用における情報セキュリティ	7.7 クリアデスク・クリアスクリーン	8.17 クロックの同期
	7.8 装置の設置および保護	8.18 特権的なユーティリティプログラムの使用
	7.9 構外にある装置および資産のセキュリティ	8.19 運用システムに関わるソフトウェアの導入
	7.10 記憶媒体	8.20 ネットワークのセキュリティ
	7.11 サポートユーティリティ	8.21 ネットワークサービスのセキュリティ
	7.12 ケーブル配線のセキュリティ	8.22 ネットワークの分離
	7.13 装置の保守	8.23 ウェブ・フィルタリング
	7.14 装置のセキュリティを保った処分又は再利用	8.24 暗号の使用
	8.技術的管理策	8.25 セキュリティに配慮した開発のライフサイクル
	8.1 利用者エンドポイント機器	8.26 アプリケーションのセキュリティの要求事項
	8.2 特権的アクセス権	8.27 セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則
	8.3 情報へのアクセス制限	8.28 セキュリティに配慮したコーディング
	8.4 ソースコードへのアクセス	8.29 開発および受け入れにおけるセキュリティ試験
	8.5 セキュリティを保った認証	8.30 外部委託による開発
	8.6 容量・能力の管理	8.31 開発環境、試験環境および運用環境の分離
	8.7 マルウェアに対する保護	8.32 変更管理
	8.8 技術的脆弱性の管理	8.33 試験情報
	8.9 構成管理	8.34 監査試験中の情報システムの保護

詳細理解のため参考となる文献（参考文献）	
情報セキュリティポリシーサンプル改版（1.0版）	https://www.jnsa.org/result/2016/policy/

第9章. 管理策のテーマと属性

9-1. 管理策の分類と構成

章の目的
第9章では、ISO/IEC 27002における管理策の分類と構成について理解することを目的とします。

主な達成目標
◘ ISMSの管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

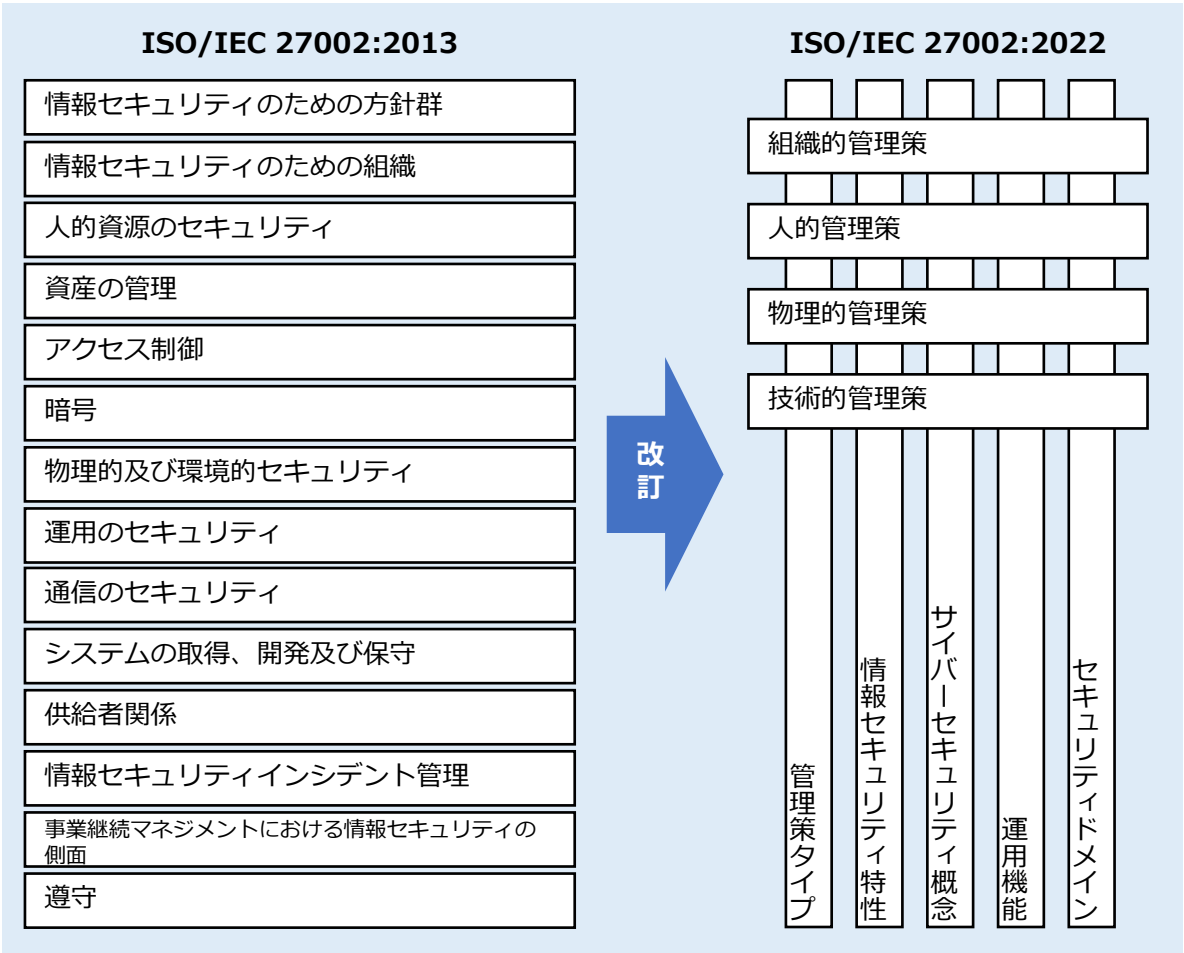
9-1-1. 管理策：ISO/IEC 27002

ISO/IEC 27001に記載されている要求事項をもとに、さらに具体的なISMSの管理策を示した規格がISO/IEC 27002です。管理策とは、リスク対応のための対策のことを指します。企業はISMSを導入する際、ISO/IEC 27002にある管理策から、自社に合ったものを選択し、対策基準として導入することになります。

ISO/IEC 27002は、2022年に改訂がありました。その際の変更点としては、管理策の項目数と章立ての変更、テーマおよび属性の導入、全管理策への目的の追加などがあります。管理策の数は、2013年版では14分野114項目でしたが、2022年版ではいくつかが統合されて82項目になり、新しく11項目が追加され、合計で93項目となりました。

2022年版では、この93の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4つのカテゴリに分類されています（箇条5～8 ）。

また、2022年版では「属性（attribute） 」という新しい概念が導入されました。各管理策には、属性値がハッシュタグで表示されるようになっています。たとえば、管理策のタイプには、予防・検知・是正の3つの属性値があります。この他、情報セキュリティ特性、サイバーセキュリティ概念、運用機能、セキュリティドメインの観点からも属性値がつけられています。 これらの属性を参考にして、組織に必要な情報セキュリティ対策を選択することになります。



9-1-2. 管理策のテーマと属性

ISO/IEC 27002の箇条5～8に示される4種の管理策での分類（組織的・人的・物理的・技術的）を、テーマと呼びます。管理策の分類は様々な考え方がありますが、多くの組織に共通であると考えられる最低限の分類としてこの4つが採用されています。テーマとは別の視点で、より細かに管理策を見るのに際しては、属性という機能があります。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。

管理策の属性には、他の組織や団体が発行するガイドラインなどにおける考え方を取り入れているものがあります。「サイバーセキュリティ概念」では、サイバーセキュリティフレームワークにおける、フレームワークコアの5つの機能分類がそのまま属性値となっています。また、「運用機能」の属性値は、2022年の改訂前におけるISO/IEC 27002の管理策の分類がもとになっています。

管理策の属性	属性値	関連するガイドラインなど
管理策タイプ	予防、検知、是正	―
情報セキュリティ特性	機密性、完全性、可用性	**ISO/IEC 27001**
サイバーセキュリティ概念	識別、防御、検知、対応、復旧	**サイバーセキュリティフレームワーク**
運用機能	ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティを保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、供給者関係のセキュリティ、法および遵守、情報セキュリティ事象管理、情報セキュリティ保証	**ISO/IEC 27002:2013**
セキュリティドメイン	ガバナンスおよびエコシステム、保護、防御、対応力	―

9-1-2. 管理策のテーマと属性

各テーマより管理策の例示（組織的/人的）

【組織的管理策】5.2 情報セキュリティの役割及び責任

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #対応力

管理策	情報セキュリティの役割及び責任を、組織の要求に従って定め、割り当てることが望ましい。
目的	組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

【人的管理策】6.8 情報セキュリティ事象の報告

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知	#機密性 #完全性 #可用性	#検知	#情報セキュリティ事象管理	#防御

管理策	組織は、要員が発見したまたは疑いを持った情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けることが望ましい。
目的	要員が、特定可能な情報セキュリティ事象を時機を失せず、一貫性をもって効果的に報告することを支援するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

9-1-2. 管理策のテーマと属性

各テーマより管理策の例示（物理的/技術的）

【物理的管理策】7.4 物理的セキュリティの監視

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#予防 #検知	#機密性 #完全性 #可用性	#防御 #検知	#物理的セキュリティ	#保護 #防御

管理策	施設は、認可されていない物理的アクセスについて継続的に監視することが望ましい。
目的	認可されていない物理的アクセスを検知し、抑止するため。

【技術的管理策】8.16 監視活動

管理策タイプ	情報セキュリティ特性	サイバーセキュリティ概念	運用機能	セキュリティドメイン
#検知 #是正	#機密性 #完全性 #可用性	#検知 #対応	#情報セキュリティ事象管理	#防御

管理策	情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい。
目的	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

第10章. 脅威、脆弱性、リスクの定義と関係性

10-1. 用語の定義および関係性と識別方法

章の目的
第10章では、ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を理解することを目的とします。

主な達成目標
◘ ISMSの管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

10-1-1. 用語の定義と関係性

企業や組織には様々なセキュリティ上のリスクが存在しています。これらのリスクを効率的に管理するには、リスクマネジメントを行う必要があります。

リスクマネジメントを理解するために必要となる「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を説明します。次に、リスクを増大させる要因となる「脅威」や「脆弱性」の識別方法を説明します。

主な用語の定義

- ✓ **脅威**：システムまたは組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。たとえば、不正アクセス、DDoS攻撃のような意図的な人為的脅威、機器の故障や操作ミスのような偶発的な人為的脅威、地震や洪水のような環境的脅威がある。
- ✓ **脆弱性**：1つ以上の脅威によって付け込まれる可能性のある、資産または管理策の弱点。たとえば、セキュリティホールと呼ばれるソフトウェアの欠陥・不具合。
- ✓ **情報資産の重要度**：機密性・完全性・可用性が損なわれた場合の事業に対する影響や、法律で安全管理義務があるなどの観点から、情報資産の重要度を判断する。
- ✓ **セーフガード（管理策）**：リスクを修正する対策。具体的には、リスクを除去あるいは許容できる範囲に制御するための手順や仕組みのこと。
- ✓ **リスク**：目的に対する不確かさの影響。情報セキュリティにおいては、脅威が組織に損害を与える可能性。
- ✓ **リスク値**：リスクの大きさのこと。「情報資産の重要度」と「機密性・完全性・可用性を損なう事象の発生確率」の積で求められる。

脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係を分かりやすく図で表すと以下のようになります。

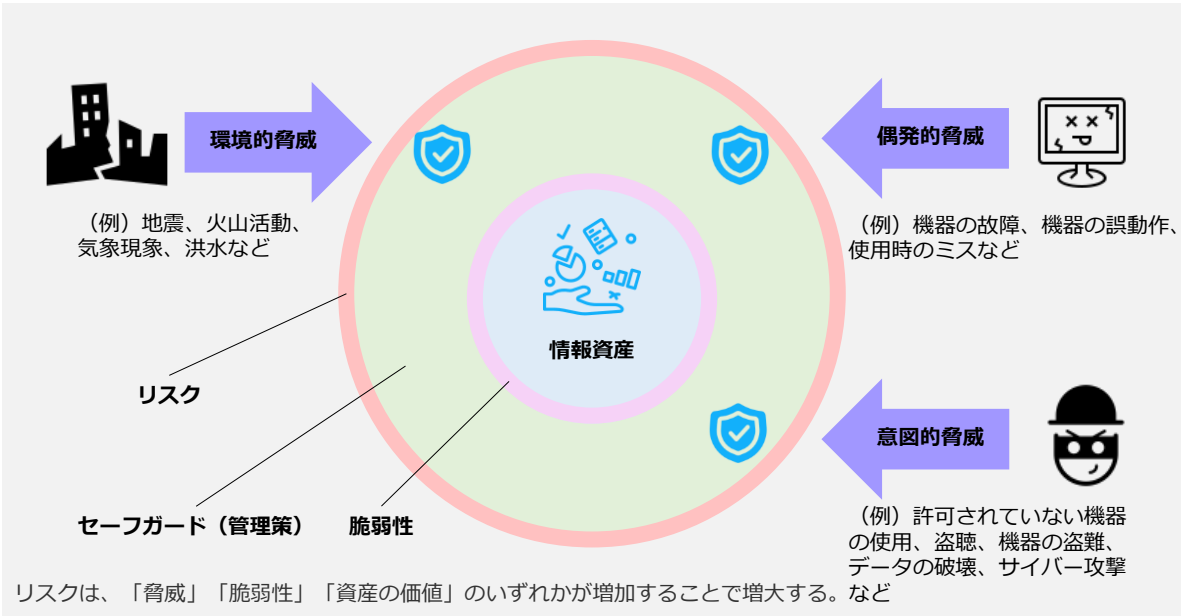


図43.脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

10-1-1. 用語の定義と関係性

（例）業務用ノートパソコン

業務用ノートパソコンに関する脅威や脆弱性、管理策の関係について説明します。

資産	ノートパソコン内の情報
価値	営業の業務で必須の情報
脅威	社外への持ち出しによるノートパソコンの紛失
リスク	盗難による情報漏えい
脆弱性	不適切なパスワードの設定（例）わかりやすいパスワード：名前、社員番号、生年月日など
保護要求事項	• 権限のないものがログインできないようにする • 不要な持ち出しを防ぐ
管理策	• 複雑なパスワードの設定（8.5 セキュリティを保った認証） • 社外の持ち出し管理（7.9 構外にある装置及び資産のセキュリティ（構外にある資産））

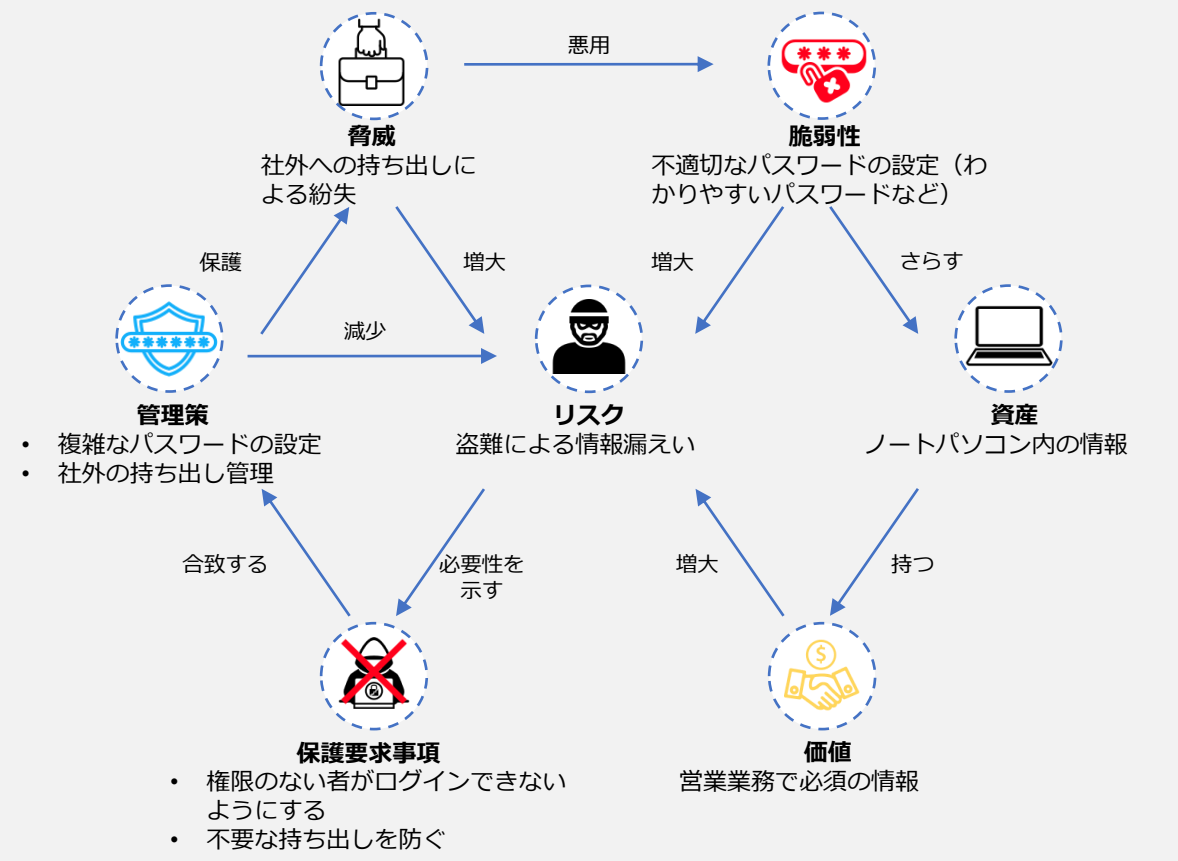


図44. 脆弱性、リスクの関係の事例

上記の図では「脅威」「脆弱性」「資産の価値」のいずれかが増加することで、リスクが増大することが示されています。リスクを減少させるためには、まず「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明らかにします。そして、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要です。

10-1-2. 脅威の識別

脅威の識別

脅威は「脆弱性」につけいり顕在化することで、組織に損失や損害を与える事故を生じさせます。脅威を、人為的脅威（意図的脅威、偶発的脅威）と環境的脅威に区別して把握することで、必要なセキュリティ対策を整理しやすくなります。

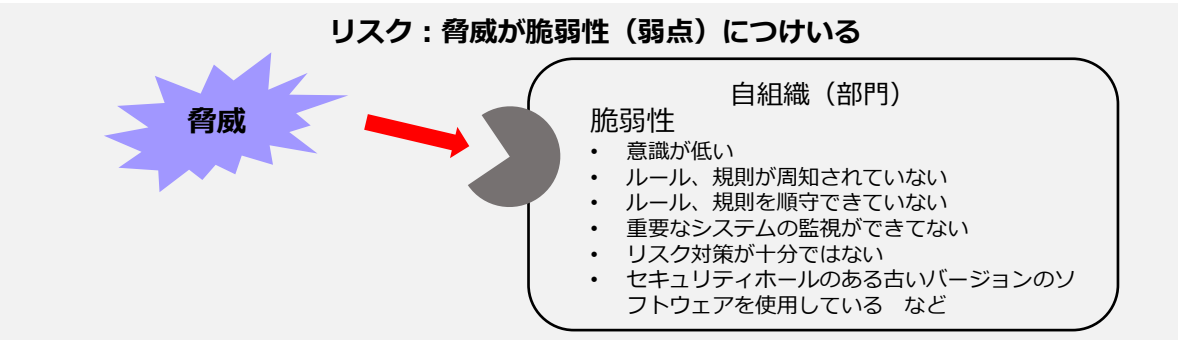


図45. 脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

類型	脅威	原因
物理的損傷	火災、水害、汚染、大事故、機器や媒体の破壊、粉塵、腐食、凍結	A/D/E
自然現象	気候、地震、火山活動、気象現象、洪水	E
重要なサービスの喪失	空調や給水システムの故障/電気通信機器の故障	A/D
	電力供給の停止	A/D/E
情報を危うくすること	遠隔スパイ行為、盗聴、媒体や文章の盗難、機器の盗難、再利用または廃棄した媒体からの復元、ハードウェアの改ざん、位置検知	D
	漏えい・信頼できない情報源からのデータ・ソフトウェアの改ざん	A/D
技術的な故障	機器の故障、機器の誤動作、ソフトウェアの誤作動	A
	情報システムの飽和、情報システムの保守に関する違反	A/D
認可されていない行為	許可されていない機器の使用、ソフトウェアの不正コピー、データの破壊、データの違法な処理	D
	海賊版または（不正）コピーソフトウェアの使用	A/D
機能を危うくすること	使用時のミス	A
	権限の乱用/権限の詐称	A/D
	要員の可用性に関する違反	A/D/E

A：偶発的脅威（Accidental）　D：意図的脅威（Deliberate）　E：環境的脅威（Environmental）

脅威の一覧表の例
（出典）「ISO/IEC 27005」を基に作成

10-1-2. 脅威の識別

脅威を洗い出すには自組織にある資産に対する脅威を識別して、前ページのようなリストを作成します。その際には、利用者や他の事業部の関係者、外部の専門家などから得られる、脅威に関する情報を活用することが大切です。

脅威の洗い出しの考え方として、意図的脅威は、攻撃の動機や必要なスキル、利用可能なリソースを考慮しつつ、資産の特性や魅力、脆弱性などから、どのような要因が脅威となるかを識別できます。一方で偶発的脅威は、環境や気候、人為的なミスや誤動作などから影響を及ぼす可能性を識別できます。

脅威の種類		想定される被害とセキュリティ対策
環境的脅威 (Environmental → E)		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を重視する、などのセキュリティ対策が選択されることになります。
人為的脅威	**意図的脅威 (Deliberate → D)**	「（内部者が企業秘密を）漏えいする」という脅威が考えられます。この様な脅威については、当該行為が犯罪行為（不正競争防止法違反）であり、罰せられること、会社は企業規則により漏えい者を罰すること、場合によっては損害賠償請求を行うということを規程で明確に示し、教育を実施するという抑止的な対策が有効になります。漏えいを早期に検知するといった対策も重要になります。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じない様に、二回ずつ入力する、一定の範囲の値しか入力できない様にする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

10-1-3. 脆弱性の識別

脆弱性の識別

脆弱性があるだけでインシデントが発生するわけではありません。しかし、脆弱性は脅威を顕在化させ、インシデントの発生確率を高める可能性があります。脆弱性を減らすためには、適切な管理策を実施する必要があります。脆弱性は管理策の欠如を同時に意味しているため、脆弱性を識別することは必要な管理策を識別するのに役立ちます。たとえば「アクセス権の誤った割当て」という脆弱性は、「アクセス権の適切な設定」という管理策の欠如を意味しています。

以下は、脆弱性を識別して一覧表にした例です。脆弱性の一覧表を作成する際は、脅威と関連付けて整理する必要があります。

類型	脆弱性の例	脅威の例
ハードウェア	記憶媒体の不十分な保守/不適当な設置	システムの保守に関する違反
	定期的な交換計画の欠如	機器や媒体の破壊
	湿気、ホコリ、汚れに対する影響の受けやすさ	粉塵（ダスト）、腐食、凍結
	有効な構成変更管理の欠如	使用時のミス
	電圧の変化に対する影響の受けやすさ	電力供給の停止
	温度変化に対する影響の受けやすさ	気象現象
	保護されない保管	媒体や文書の盗難
	廃棄時の注意の欠如	媒体や文書の盗難
	管理されないコピー作成	媒体や文書の盗難
ソフトウェア	監査証跡の欠如	不正アクセス
	アクセス権の誤った割当て	不正アクセス
	複雑なユーザインタフェース	使用時のミス
	文書化の欠如	使用時のミス
	ユーザの識別及び認証メカニズムの欠如	不正アクセス
	不十分なパスワード管理	不正アクセス
	不要なサービスが実行可能	データの違法な処理
	効果的な変更管理の欠如	ソフトウェアの誤作動
	管理されてないソフトウェアのダウンロード及び使用	恐怖。攻撃，妨害行為
	バックアップコピーの欠如	装置又はシステムの故障

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

脆弱性を識別する際に参考になる情報

- ISO/IEC 27001:2022の附属書A「管理目的及び管理策」
- ISO/IEC 27002:2022の管理策
- 情報セキュリティ管理基準　など

脆弱性は、資産の性質から考えることで簡単に識別できます。たとえば、クラウドサービスは、「インターネットがあればどこでも利用可能」、「自社でデータを持たなくていい」といった性質を持ちます。同時にそれらの性質は「不正アクセス」「クラウドサービス停止によるデータの消失」という脅威に対する脆弱性があります。

コラム

情報セキュリティのCIA＋4要素

JIS Q 27000:2019で、情報セキュリティは「機密性（Confidentiality）」、「完全性（Integrity）」及び「可用性（Availability）」を維持することと定義されています。これら３つの要素（CIA）をバランスよく維持することは、セキュリティを担保する上では欠かせません。また、さらに以下の4つの要素を追加して、情報セキュリティの7要素とする場合もあります。より高度なISMSの構築につながる要素のため、ここで紹介します。

〇真正性 (Authenticity)
情報にアクセスする人や端末が「本当に許可されているかどうか」を確実にすることを指します。多要素認証やデジタル署名など、認証方法を強化することが対策として考えられます。

〇信頼性 (Reliability)
データやシステムを利用する際、意図した動作と結果が得られることを担保することを指します。不具合がないようにシステム構築を行うことや、ヒューマンエラーが起きないようなルール整備などが対策として考えられます。

〇責任追跡性 (Accountability)
情報へのアクセスが、誰によってどのような手順で行われたのかを後から証明できるようにしておくことを指します。ログの取得や、デジタル署名などが対策として考えられます。

〇否認防止性 (Non-repudiation)
問題発生後に、その原因となった人物から否定されないよう、後から証明できるようにしておくことを指します。先に説明した責任追跡性を担保することが対策につながります。

CIAの3要素だけでなく、上記の4要素も加えることで、より抜け漏れがないセキュリティ対策が期待できます。

第11章. リスクマネジメント

11-1. リスクマネジメント：概要

11-2. リスクマネジメント：リスクアセスメント

11-3. リスクマネジメント：リスク対応

章の目的
第11章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方について学ぶことを目的とします。

主な達成目標
◘ リスクマネジメントの意義について理解すること ◘ リスクマネジメントプロセスの全体像を理解すること ◘ リスクアセスメント、リスク対応のプロセスを理解すること

11-1-1. リスクマネジメントプロセス（ISO31000）

企業や組織にはさまざまなリスクが存在しています。これらのリスクを効率的に管理し、発生する可能性がある損失を回避したり低減したりするプロセス全体のことを「**リスクマネジメント**」と言います。

リスクマネジメントの国際規格として**ISO 31000**があります。ISO 31000では、リスクマネジメントを「原則」「枠組み」「プロセス」の3つの要素から構成されるものとして捉えています。

リスクマネジメント

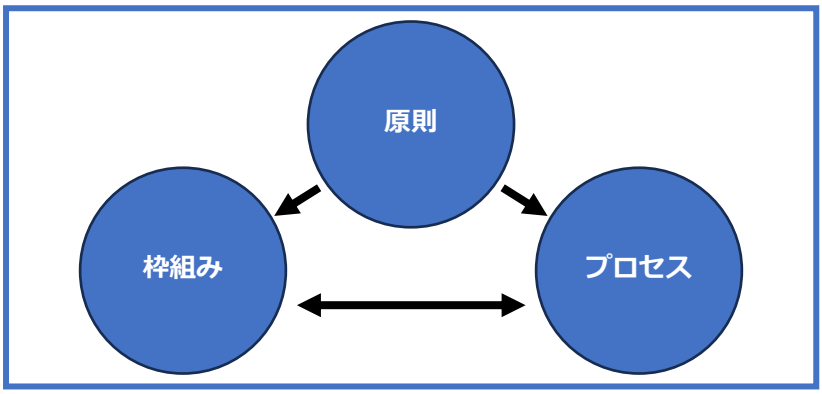


図46. リスクマネジメントの3要素

原則	リスクマネジメントを実施する際に、組織が取組むべき事項です。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」「利用可能な最善の情報」「人的及び文化的要員」「継続的改善」で構成されています。
枠組み	リスクマネジメントを組織全体に定着させるための仕組みです。 「統合」「設計」「実施」「評価」「改善」で構成されています。
プロセス	リスクマネジメントに取組む上で実施すべき、一連の活動です。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」「記録作成及び報告」で構成されています。

実際にリスクに対応していくにあたっては、リスクマネジメントプロセスにおける「**リスクアセスメント**」が必須事項となります。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位づけをしていくプロセスのことを表します。リスクアセスメントの実施により、個々の資産が持つリスクと、リスクに対する管理策、および管理策に投じるべき費用の識別が期待できます。また、リスクを評価するということは情報資産の持つ固有の弱点や脅威を明確にする過程を含みます。そのため、事前にリスクを把握することで必要な投資額を含め、適切な対策を検討することが可能になります。

11-1-2. 情報セキュリティリスクマネジメント（ISO/IEC27005）

ISO/IEC 27005は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。先に説明したISO31000と整合性がありますが、情報セキュリティに特化した内容になっています。この規格は、組織の情報資産を安全に保つことに焦点が当てられており、情報セキュリティリスクの特定、分析、評価、対応、管理、レビューなどを実施するための手引きになっています。中小企業を含むすべての組織における情報セキュリティリスクのマネジメントに有用です。

ISO/IEC 27005の情報セキュリティリスクマネジメントプロセスは、ISO 31000の一般的なリスクマネジメントプロセスに基づいており、リスクの特定、リスクの評価、リスクの対処、およびリスクの監視とコントロールに関するステップから構成されます。以下の図で示すように情報セキュリティリスクマネジメントプロセスは循環しており、反復的に実施されるものです。組織を取り巻く環境の変化や組織内の変化に応じて、新しいリスクが発生したり、既存のリスクが変化したりする上に、リスクへの対処法も進化するからです。特に、リスクマネジメントプロセスに含まれているリスクアセスメントは、リスク対応の方策や、対応の優先順位づけの前提になる重要な工程です。

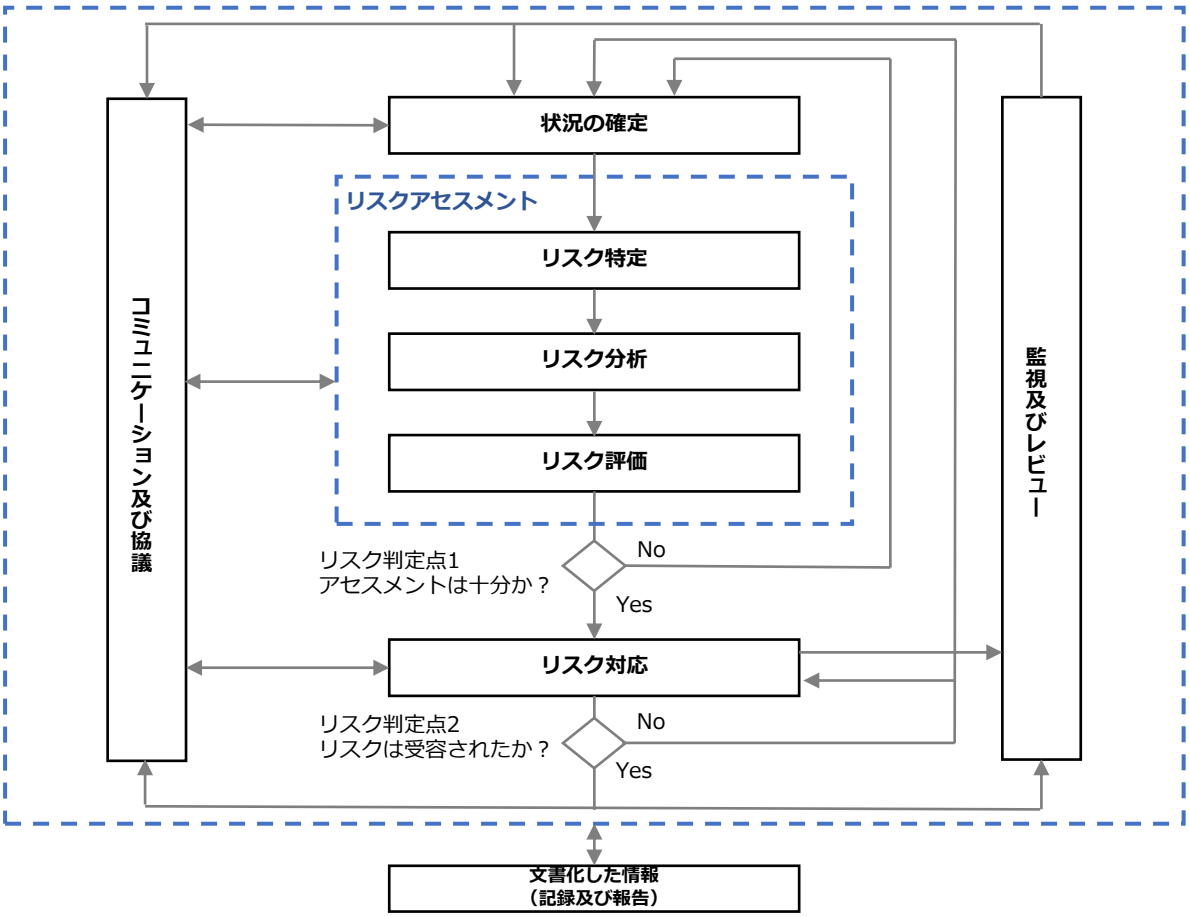


図47. 情報セキュリティマネジメントプロセスの概要
（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

11-1-2. 情報セキュリティリスクマネジメント（ISO/IEC27005）

リスクアセスメントからリスク対応までの流れを表す図を記載します。リスク対応を実施する過程では、「低減」「移転」「回避」「受容（保有）」の4つ選択があり、それらの選択は以下の図で示すプロセスで行われます。

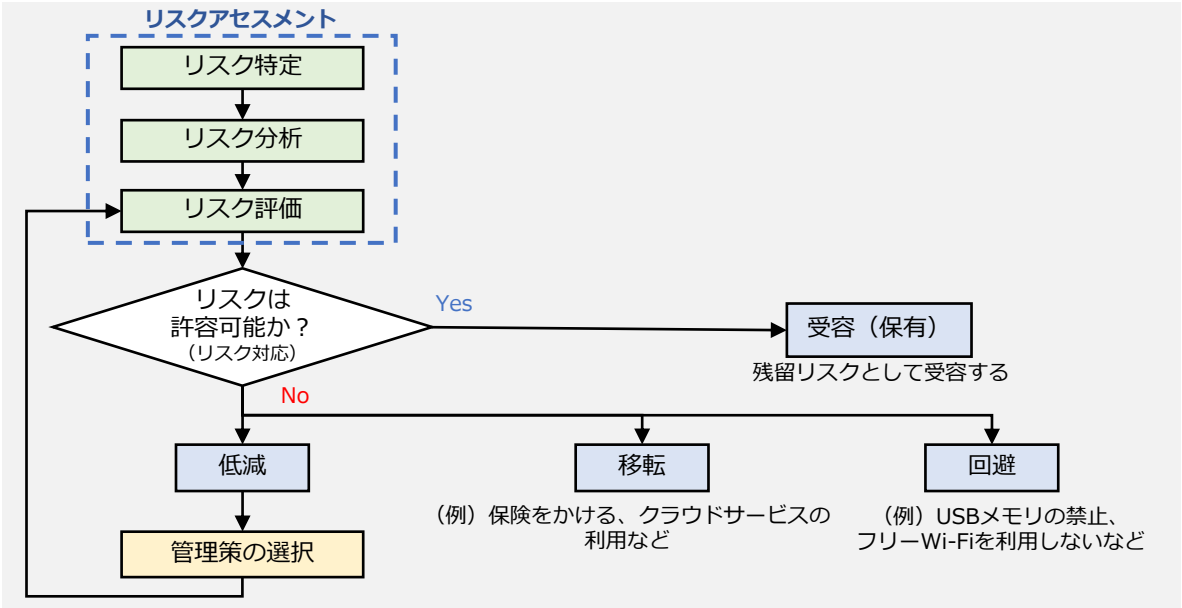


図48. リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

リスクを受容（保有）する

事故が発生しても受容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。
（例）
・従来は商品の発送先である住所や氏名などの個人情報を発送完了後もパソコンに保存し続けていたが、保存中の漏えいを避けるために、利用後はすぐに消去する
・インターネットバンキングに使用するパソコンでメールやウェブ閲覧をしていたが、ウイルスに感染しないようにインターネットバンキング専用のパソコンを設置し、ウイルス感染の原因となるメールやウェブ閲覧に利用せず、USBメモリ、外付けHDDも接続を禁止する
また、リスクレベルが大きく自社の対策だけでは不十分であったり、多額の費用がかかり、実施できなかったりする場合は「リスクの移転」を検討します。

リスクを移転する

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げます。
（例）
・商品を販売するウェブサイトではクレジットカード番号を非保持化し、代金の決済はセキュリティ対策を十分行っている外部の決済代行サービスに変更する
・社内のサーバで運用していた業務システムをセキュリティ対策の充実した外部クラウドサービスに移行する
・情報漏えい、システム障害などの事故発生に伴う損失に対して保険金が支払われる情報セキュリティに関連した保険商品に加入する

（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」を基に作成

11-1-3. ISO/IEC 27001におけるリスクマネジメント手順

ISO/IEC 27005は、情報セキュリティ**リスクマネジメント**の手法を提供する規格であり、ISO/IEC 27001（ISMS）は情報セキュリティ**マネジメントシステム**の設計と実装に関する規格です。つまり、ISO/IEC 27001は情報セキュリティマネジメントシステムの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005になります。

ISO/IEC 27001（ISMS）の活動は、ISO/IEC 27005におけるリスクマネジメントプロセスと関連付けて整理することが可能です。

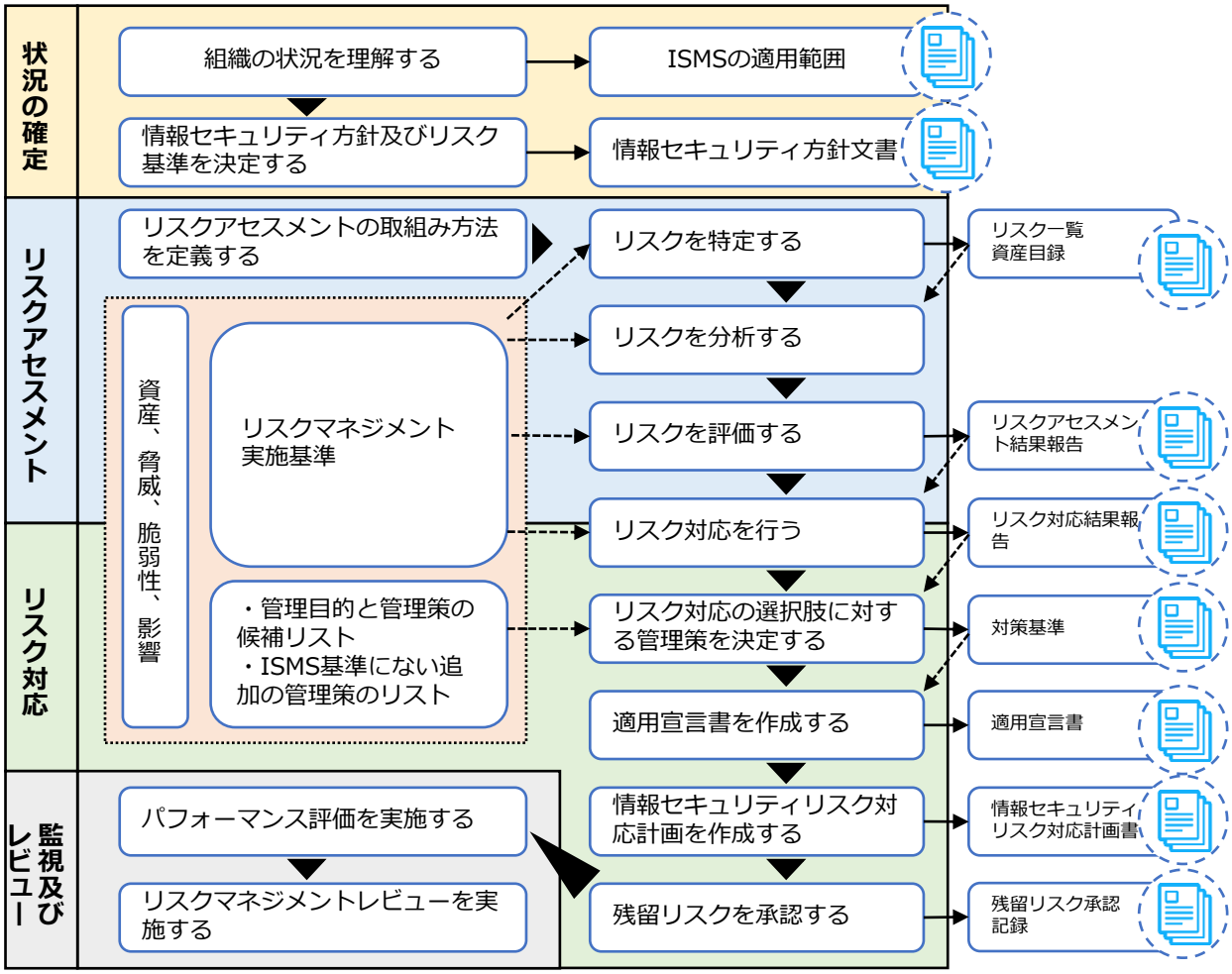


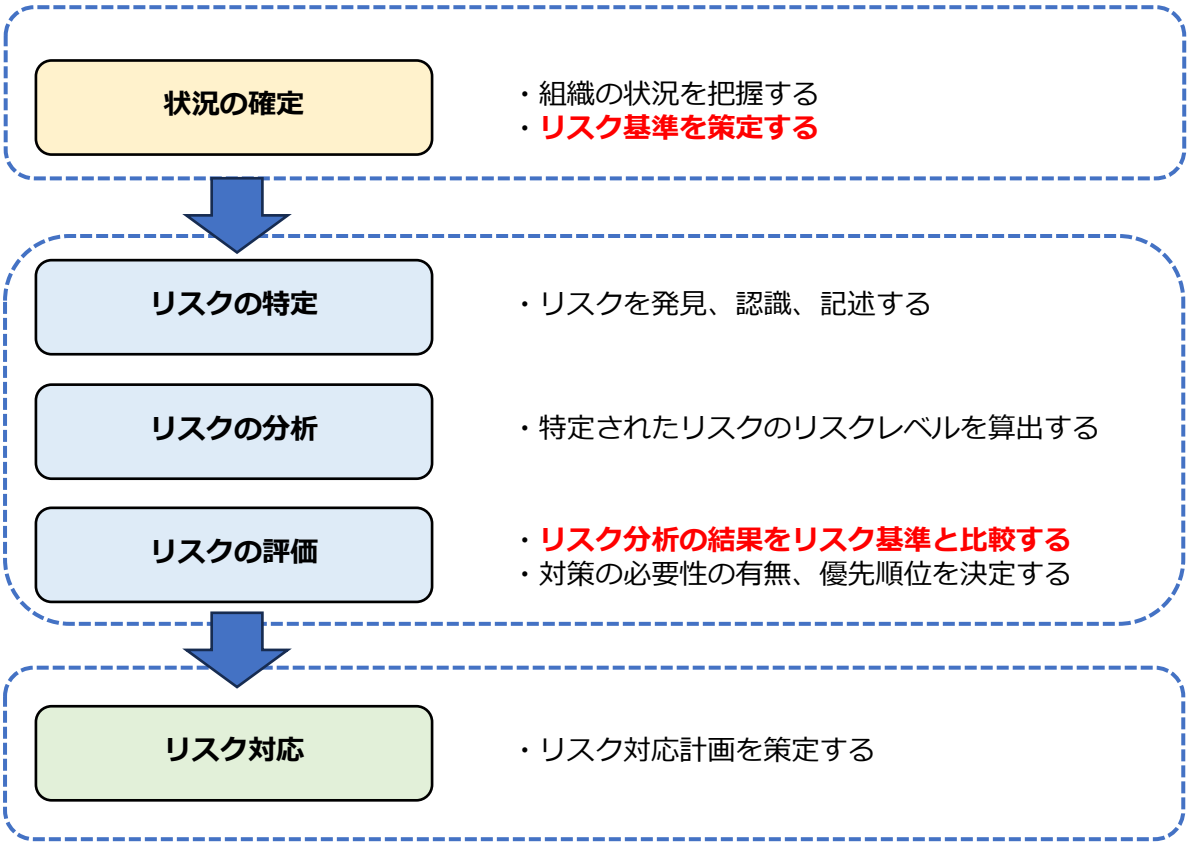
図49. ISMSにおけるリスクアセスメントおよびリスク対応に関する作業の概要

11-2-1. リスク基準の確立

必要なリスク基準

リスクアセスメントを実施するにあたって、リスクの重大性を評価するための目安となる条件を決める必要があります。その条件のことをリスク基準と言います。ISMSでは、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むよう明示されています。

リスク受容基準
どの程度のリスクであれば受け入れることが可能かの判断基準です。 あるリスクに対して、どの程度のレベル感や優先順位でリスク対応を実施するのか、リスクが顕在化した際にどの程度の大きさまでなら許容するのかを明確にする必要があります。
情報セキュリティリスクアセスメントを実施するための基準
いつ、どのようなときにリスクアセスメントを実施するのかを決める要件です。 リスクアセスメントの実施条件や実施時期、タイミングや頻度などを明確にする必要があります。



11-2-2. リスクの特定

リスク特定

リスクアセスメントの1つ目のプロセスである「リスク特定」について説明します。リスク特定とは、「リスクを発見、認識及び記述するプロセス」[21]のことです。リスク特定を実施するために一般的に使用されるアプローチは「資産ベースのアプローチ」および「事象ベースのアプローチ」の2つがあります。

【情報セキュリティリスクの特定および記述】

アプローチ手法	概要	メリット	デメリット
資産ベースのアプローチ	• 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 • 資産は、その種類及び優先度に従って主要資産及び支援資産として特定できる。 • 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 • 資産のリストを作成することが望ましい。	• 資産、脅威及び脆弱性のすべての有効な組合せをISMSの適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	• 情報資産が増えたときに、資産のリストの行数が多くなる。 • 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	• 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。 • 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び組織の状況を決定する際に特定された要求事項によって発見できる。	• 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルまたは戦略的なシナリオを確立することができる。	• 網羅性において、資産ベースのアプローチに劣る。

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスク所有者の特定	・特定されたリスクに対し、リスク所有者を関連付ける。 ・リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする。（通常、組織内で一定の権限を持つ人が選ばれる）

[21]: JISC 日本産業標準調査会."JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語". https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

資産ベースのアプローチでは、はじめに情報資産を洗い出し（資産目録の作成）、その過程でリスク所有者を特定します。リスク所有者とは、リスクが顕在化した際に責任を取る人のことを指します。その後、情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合、事業にどれほど影響があるか評価を行い、重要度を判断します。

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

情報資産の洗い出し（例）

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

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部長	人事部	書類
経理	給与システムデータ	税務署提出用 源泉徴収票	給与計算担当	経理部長	人事部	事務所PC
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	経理部長	総務部	書類
経理	発行済請求書控え	当社発行の請求書の控え（過去3年分）	総務部	経理部長	総務部	書類
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部長	営業部	可搬電子媒体
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部長	営業部	社内サーバ
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部長	営業部	書類

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

電子化された情報を洗い出す際は、「普段パソコンで見ているこのデータは、どこに保存されているのだろう」というように、社内のIT機器や利用しているクラウドサービスを思い浮かべて記入します。また、複数の組織を持つ企業の場合、管理部署ごとにシートを分けて作成すると、内容の見直しの際に便利です。

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

資産目録を作成する際、情報資産を情報、情報を支援する資産として「主要/事業資産」と「支援資産」2つのカテゴリに分類して整理する方法も有効です。

「主要/事業資産」

「主要/事業資産」とは、「組織にとって価値のある情報またはプロセス」[22]のことです。主要資産は、「事業プロセス及び事業活動」と「情報」の2つに分けられます。

「事業プロセス及び事業活動」の例

- その損失または低下によって、組織の使命達成が不可能となるプロセス
- 機密プロセスまたは専有技術を伴っているプロセス
- 修正された場合、組織の使命の達成に大きく影響するプロセス
- 組織が契約、法令または規則の要求事項を遵守するために必要となるプロセス

「情報」の例

- 組織の使命または事業の遂行に不可欠の情報
- プライバシーに関する国内法にいう意味で、特別に定義することができる個人情報
- 戦略的方向性によって決定される目的の達成に必要となる戦略情報
- 収集、保管、処理、送信に長時間を要する高コスト情報及び高い取得費用を伴う情報

「支援資産」

「支援資産」とは、「1つ以上の事業資産の基礎となる情報システムの構成要素」[23]のことです。

「支援資産」の例

- ハードウェア、ソフトウェア、ネットワーク、要員、サイト、組織

（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

One Point

情報資産のグループ化

ISMS適用範囲に存在する情報資産を洗い出す作業は、負荷が非常に大きくなりやすいです。そこで、資産価値や保管形態、保管期間や用途などが同じものを1つのグループとしてまとめて管理することで、作業負荷を軽減したり、作業を効率化したりすることができます。

（例）事務所内のパソコンで会計ソフトや表計算ソフトを使って帳簿を作成している場合

- 仕訳帳
- 総勘定元帳
- 現金出納帳
- 当座預金出納帳
- 小口現金出納帳
- 仕訳帳
- 売上帳

情報資産名称：「会計データ」
「会計データバックアップ」
（バックアップを取っている場合）など

媒体・保存先：「事務所PC」（会計ソフトの保存先）
「可搬電子媒体」
（USBメモリがバックアップ保存先）

[22][23]: ISO.” ISO/IEC 27005:2022”. https://www.iso.org/standard/80585.html, （2023-09-21）.

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

情報資産ごとに「機密性」「完全性」「可用性」が損なわれた場合の事業への影響度を評価します。具体例として、以下の評価基準を参考に「機密性」「完全性」「可用性」それぞれの評価値（3～1）を決定します。

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失またはき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	●取引先から秘密として提供された情報 ●取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	●自社の独自技術・ノウハウ ●取引先リスト ●特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	●見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	●自社製品カタログ ●ホームページ掲載情報
完全性	3	法律で安全管理（漏えい、滅失またはき損防止）が義務付けられている	●個人情報（個人情報保護法で定義） ●特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	●取引先から処理を委託された会計情報 ●取引先の口座情報 ●顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	●自社の会計情報 ●受発注・決済・契約情報 ●ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	●廃版製品カタログデータ
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	●顧客に提供しているECサイト ●顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	●製品の設計図 ●商品・サービスに関するコンテンツ　（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	●廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義
（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」を基に作成

11-2-2. リスクの特定

リスク特定（資産ベースのアプローチ）

影響度の評価をもとに重要度を算定

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

	情報資産の価値・事故の影響の大きさ	
重要度	3	事故が起きると、「 法的責任を問われる」「 取引先、顧客、個人に大きな影響がある」「 事業に深刻な影響を及ぼす」など、企業の存続を左右しかねない
	2	事故が企業の事業に重大な影響を及ぼす
	1	事故が発生しても事業にほとんど影響はない

重要度の判断例：自社のホームページ（電子データ）		評価値
「機密性」	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	⇒ 1
「完全性」	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	⇒ 3
「可用性」	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	⇒ 3
➡ 完全性と可用性の評価値3が最大値なので、**重要度は評価値：3**		

重要度の判断例
（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」を基に作成

One Point

重要度を判断する際のポイント

- 重要度の判断は、立場や見識によっても異なることがあるので、情報資産管理台帳に記入する前に「重要ではない」と判断するのではなく、記入した後に組織的に重要度を判断します。
- 情報資産の「重要度」は、時間経過とともに変化することがありますが、現時点の評価値を記入します。また時間経過に伴う重要度の変化を台帳上で更新することが難しい場合は、最大値で評価します。

11-2-2. リスクの特定

リスク特定（事象ベースのアプローチ）

事象ベースのアプローチでは、従業者の業務プロセスを起点にリスクを特定します。それにより、詳細なレベルで資産を特定することに多大な時間を費やすことなく、戦略的なシナリオを確立することができます。その結果、組織は自らのリスク対応の取組を、重大なリスクに集中させることができます。

前述の資産ベースのアプローチに比べると網羅性に劣るというデメリットはありますが、その分、日々の業務をもとにして洗い出すため、現実的なリスクを洗い出すことができるというメリットがあります。また、資産ベースのアプローチの際、情報資産の洗い出しにより出てきた主要資産（事業プロセスおよび事業活動）に対しても、事象ベースのアプローチでリスク特定が可能です。

① リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 （例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」

② リスク所有者の特定	①で特定されたリスクの所有者を記載します。

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	○○○○
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響をおよぼす事象である	3		

事象ベースのアプローチによるリスク特定の例
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

上記内容でリスク特定を実施した後、特定されたリスクおよび「重要度」に対して後述のリスク分析を実施します。

11-2-3. リスクの分析

リスク分析（例）

特定されたリスクに対して「リスク分析」を行います。リスク分析とは、「リスクの性質を理解し、リスクレベルを決定するプロセス」[24]のことです。リスクレベル（リスクの大きさ）は、優先的・重点的に対策が必要な情報資産を把握するために使用されます。リスクレベル（リスクの大きさ）を算定するにはさまざまな方法があります。算定方法の一例を以下に示します。

「リスクレベル」 ＝ 「重要度」 ※リスク特定で算出方法を説明 × 「被害発生可能性」

「被害発生可能性」とは、脅威が脆弱性を利用して、どの程度被害をもたらす可能性があるかを示す指標です。「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の2つの数値を「被害発生可能性の換算表」に当てはめて算出します。

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

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

換算表で算出

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

（例）
- 脅威の起こりやすさ：「2」、 脆弱性のつけ込みやすさ：「2」
  ➡ 被害発生可能性は**「1」：**通常の状況で被害が発生することはない
- 脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「2」
  ➡ 被害発生可能性は**「2」：**特定の状況で被害が発生する（年に数回程度）
- 脅威の起こりやすさ：「3」、脆弱性のつけ込みやすさ：「3」
  ➡ 被害発生可能性は**「3」**通常の状況で被害が発生する（いつ発生してもおかしくない）

[24]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-2-4. リスクの評価

リスク評価

リスク評価とは、「特定・評価したそれぞれのリスクが、受容可能かどうかを評価するプロセス」のことです。リスク分析で算出したリスクレベルを、リスク基準（リスク受容基準）と比較し、リスク対策が必要かどうか判断します。また、リスクレベルをもとに対策の優先順位をつけます。

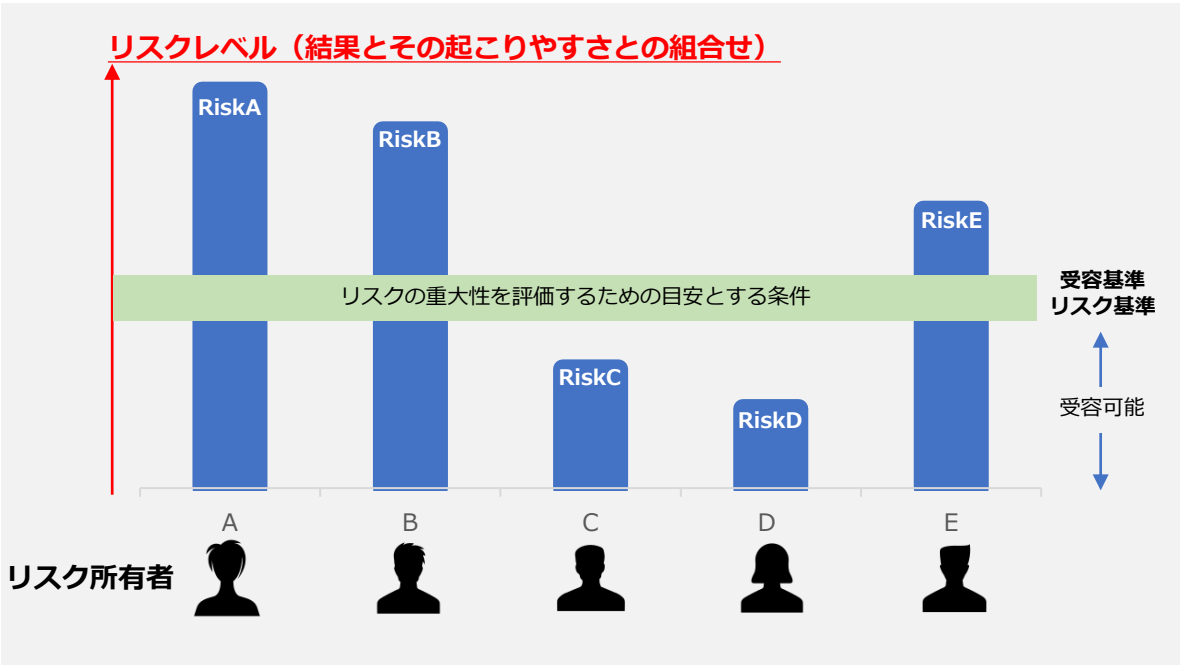


図50. リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

11-2-4. リスクの評価

リスク評価（例）

「重要度」 × 「被害発生可能性」でリスクレベルを算出し、リスク評価を行います。例として、算出したリスクレベルを以下の表に当てはめて行います。

リスクレベル 評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

※リスクレベル=「重要度」 × 「被害発生可能性」　※赤色、黄色、青色の網掛けは以下の「リスク受容基準」を示す

リスク受容基準（例）

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

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

また、情報セキュリティリスクの場合、以下の図で示す考え方をすることが多いです。以下の図では、発生頻度が高く被害が非常に大きいものについては「回避」、発生頻度は低いが被害が大きいものについては「移転」、発生頻度は高いが被害が大きくないものについては「低減」を検討するという考え方を示しています。

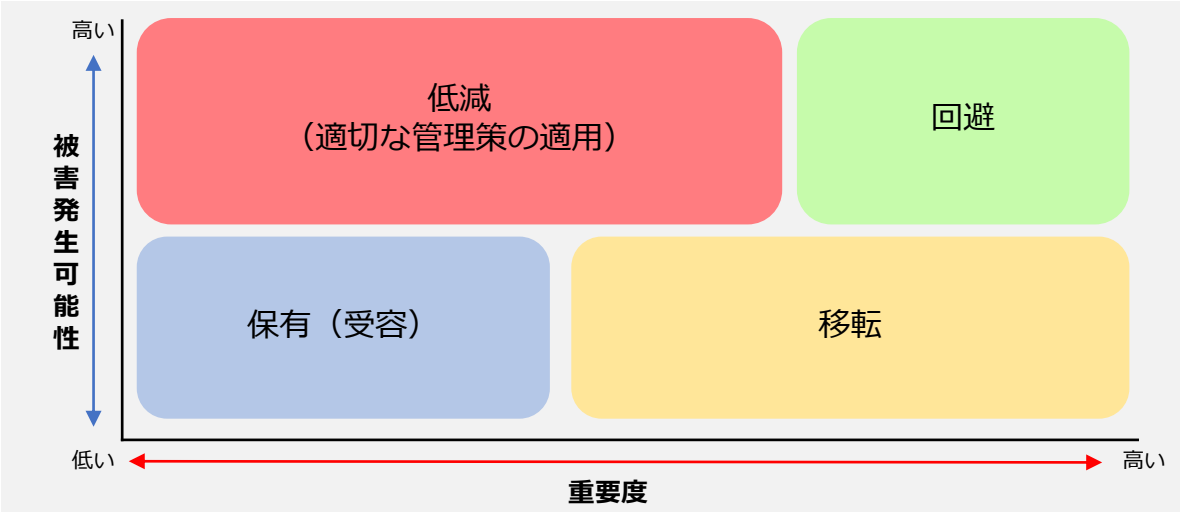


図51. 情報セキュリティリスクの考え方
（出典）JNSA.”2-4 リスクアセスメントとリスク対応”. https://www.jnsa.org/ikusei/01/02-04.html,（参照 2023-09-21）

11-3-1. 対策案の検討

リスク対応プロセス

リスク対応とは、「リスクを修正するプロセス」[25]のことです。リスクアセスメントプロセスの結果に基づいており、リスク基準に基づき対応すべき優先順位づけされたリスクに対応する内容となります。

1. 適切な情報セキュリティリスク対応の選択肢の選定	
リスク対応の選択肢は以下の通りです。	
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。
2. 情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定	
ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要なすべての管理策を決定します。	
3. 決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較	
必要なすべての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。	
4. 適用宣言書の作成	
必要なすべての管理策と、その理由及び実施状況を文書化します。適用宣言書に含まれるすべての管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。	
5. 情報セキュリティリスク対応計画	
組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。 - 組織の必要な管理策を実施するためのプロジェクト計画 - リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画	
6. リスク所有者による承認	
リスク所有者は、リスク対応計画を承認します。	
7. 残留している情報セキュリティリスクの受容	
リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。	

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

[25]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

11-3-1. 対策案の検討

リスク対応プロセス（例）

例：自社のホームページ（電子データ）

リスクの内容

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

リスク対応

リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）

対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する

対応する管理策：5.15アクセス制御

対策基準の策定（対策基準の例）

技術的対策

- 公開サーバへの不正アクセス対策
- 公開サーバへのアクセス権の最小化と管理の強化
- 多要素認証の設定の有効化

残留リスク

残留リスクとは、「リスク対応後に残っているリスク」[26]のことです。残留リスクを受容するためには、リスク所有者の承認が必要になります。受容可能だと判断された残留リスクであっても、資産の価値や脅威、脆弱性など環境の変化に合わせて、リスクレベル（リスクの大きさ）を見直し、必要に応じて追加のリスク対応を行う必要があります。

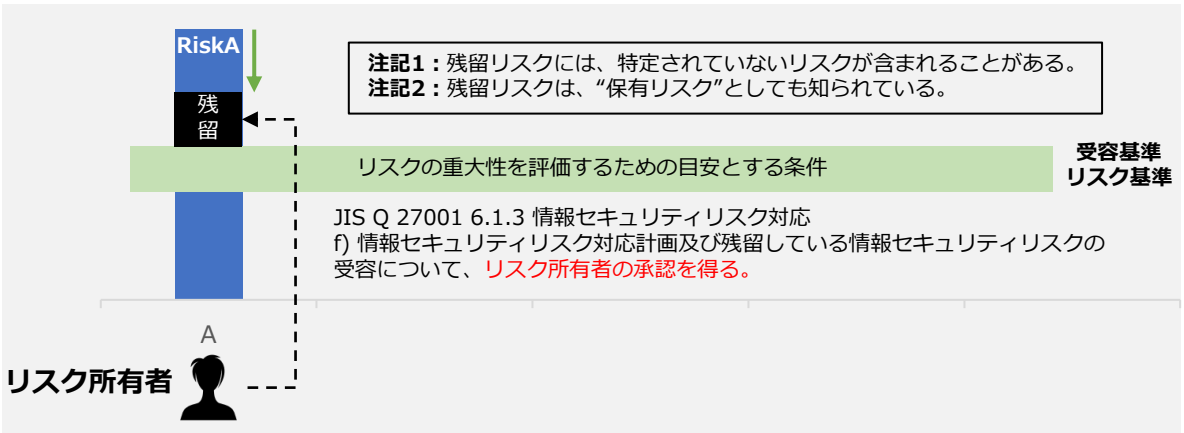


図52. 残留リスクの概要
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

[26]: JISC 日本産業標準調査会.”JIS Q 27000:2019 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語”. https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000, （2023-09-21）.

第12章. 具体的手順の作成（LV.1 クイックアプローチ/LV.2 ベースラインアプローチ）

12-1. 【LV.1 クイックアプローチ】【LV.2 ベースラインアプローチ】の概要

12-2. 【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

12-3. 【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

章の目的
第12章では、セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。
主な達成目標
◘ クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること ◘ ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

12-1-1. クイックアプローチ・ベースラインアプローチ

セキュリティ対策基準を策定し、具体的な実施手順を明確にすることで、情報漏えいなどのリスク対策を行います。対策内容を決めるためのアプローチ手法として、「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」があります。

本章では、「LV.1 クイックアプローチ」と「LV.2 ベースラインアプローチ」における実施手順の作成方法について説明します。LV.1 クイックアプローチは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。LV.2 ベースラインアプローチは、ガイドラインなどを参考に、対策基準や実施手順を策定するアプローチ手法です。

LV.1 クイックアプローチ（緊急性の高い事象に対応するための対策）

概要

報道される事例や情報セキュリティ10大脅威などから、発生する可能性が高いセキュリティインシデント事例や、セキュリティインシデントが発生した場合に被害が大きい事例を参考にし、対策基準や実施手順を策定します。

メリット

- 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。

デメリット

- 短期的な解決策に偏りがちになる。
- セキュリティインシデント事例ごとに策定するため、網羅性は低い。

LV.2 ベースラインアプローチ（即効性のあるアプローチ方法）

概要

IPAや総務省などが発行しているガイドラインやひな形を参考に、対策基準や実施手順を策定します。セキュリティ対策のガイドラインやひな形を参考にすることで、組織全体で一貫性があり、セキュリティの最低基準を満たす対策基準や実施手順を策定します。

メリット

- 組織全体で一貫性を確保できる。
- 最低限実施すべきセキュリティ対策を講じることができる。

デメリット

- 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
- ガイドラインやひな形は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものであるかどうかを十分に検討する必要があります。

12-2-1. セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（1/3）

クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。

対策基準・実施手順作成の手順

セキュリティインシデント事例をもとにリスクアセスメントを実施します。以下は、情報セキュリティ10大脅威2023にランクインしている「内部不正による情報漏えい」に関するセキュリティインシデント事例です。

事例：内部不正による情報漏えいの疑い（卸売業・小売業、従業員数6~20名以下）

被害内容

元従業員が退職前に大量にファイルをダウンロードしました。また、同従業員が使用していたPCの履歴が消去され、専門家でも復旧できない状態になっていました。

機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出しませんでした。しかし、この判断をするまでに2年かかりました。その間、弁護士に情報提供するために、多くの作業が必要になりました。たとえば、経営者と総務担当は、情報漏えいしたと疑われる膨大なログを確認し、どれが機密情報に該当するかチェックする作業を強いられました。トラブル発生時は、人件費だけでなく、心的負担も大きくかかりました。

被害発生の原因

社外からの脅威の対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限などは進めていたが、社内から発生する脅威の対策は不十分であったこと。

セキュリティインシデント事例：内部不正による情報漏えい
(出典) IPA「2021年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集- 」を基に作成

セキュリティインシデント事例をもとに、リスクアセスメントの実施
（リスク特定、リスク分析、リスク評価）

リスク特定（例）

セキュリティインシデント事例を参考に、情報資産の洗い出しと、「機密性」「完全性」「可用性」の観点から重要度を算出します。セキュリティインシデント事例では、従業員が使用していたPCが悪用されていたため、以下の資産目録の例では「媒体・保存先」が従業員が使用するPCである情報資産を洗い出しています。機密性・完全性・可用性の評価値と、重要度は「11-2-2. リスクの特定」で解説した方法で算出します。リスクアセスメントの詳細は「第11章. リスクマネジメント」を参照してください。

機密性・完全性・可用性の評価値は、1~3で記載
重要度は、機密性・完全性・可用性いずれかの最大値

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

12-2-1. セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（2/3）

リスク分析（例）

リスク特定で算出した重要度と、被害発生可能性からリスクレベルを算出します。被害発生可能性は、セキュリティインシデント事例と同様の被害がどの程度起きやすいかを考慮して算出します。被害発生可能性・リスクレベルの詳しい算出方法は、「11-2-3. リスクの分析」を参照してください。

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクレベルの算出方法

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度	被害発生可能性	リスクレベル
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3	3	9
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3	2	6
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3	2	6

リスク評価（例）

リスクレベルをもとに、必要なリスク対応を検討します。今回は、例としてリスク低減や回避を選択します。

リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすること
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせたりすること
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすること
リスク受容（保有）	対策を行わずにリスクを受け入れるということ

リスク評価をもとに対策基準・実施手順の作成

対策基準の策定（例）

リスク評価の結果を参考に対策基準を策定します。今回の例では、リスク低減や回避に関する対策基準を決定しています。対策基準の例は以下の通りです。

対策基準（例）

- 社内の機密情報に関する社内規定の策定
- 重要情報の管理、保護
- 物理的管理の実施
- 従業員向け研修の実施

12-2-1. セキュリティインシデント事例を参考とした実施手順

LV.1 クイックアプローチ（3/3）

実施手順の作成（例）

情報セキュリティ関連規程を参考に、実施手順を作成します。情報セキュリティ関連規程とは、情報セキュリティに関する社内規則の見本です。情報セキュリティ関連規程から、対策基準に合った規則を選択し、赤字の箇所を自社の状況に合わせて編集することで、実施手順を作成します。

実施手順の作成（例）

- **機密情報に関する社内規定の策定**
  （例）従業員の責務
  従業員は以下を遵守する
  ・従業員は、当社が営業秘密として管理する情報およびその複製物の一切を許可されていない組織、人に提供してはならない。
  ・従業員は、当社の情報セキュリティ方針および関連規程を遵守する。違反時の懲戒については、就業規則に準じる。
  ・従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料またはそれらの複製物の一切を退職時に返還する。
  ・従業員は、在職中に知り得た当社の営業秘密または業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

- **重要情報の管理、保護**
  （例）利用者アカウントの管理
  利用者の認証に用いるアカウントが不要になる場合、システム管理者は、当該アカウントの削除または無効化を、当該アカウントが不要になった日の翌日までに実施する。

- **物理的管理の実施**
  （例）情報資産の社外持ち出し管理
  情報資産を社外に持ち出す場合には、以下を実施する。
  ・社外秘の場合は所属部門長の許可を得る。
  ・極秘の場合は代表取締役の許可を得る。
  ・ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。
  ・スマホ、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
  ・USBメモリなどの小型電子媒体は、大きなタグをつける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴をつける。
  ・屋外でネットワークへ接続して極秘または社外秘の情報資産を送受信する場合は、暗号化する。
  ・携行中は常に監視可能な距離を保つ。

- **従業員向けの研修**
  （例）情報セキュリティ教育
  教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。
  対象者：全従業員
  テーマ：以下は必須とする。
  ・情報セキュリティ関連規程の説明（入社時、就業時）
  ・最新の脅威に対する注意喚起（随時）
  ・関連法令の理解（関連法令の公布・施行時）
  ・個人情報の取扱いに関する留意事項
  ・コンプライアンス教育

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（1/8）

ベースラインアプローチでは、ガイドラインやひな形などの資料を参考に対策基準、実施手順を作成します。次のページから、以下の資料をもとに対策基準、実施手順を作成する流れを説明します。

- 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」
- NISC「インターネットの安全・安心ハンドブックVer.5.0」
- 総務省「テレワークセキュリティガイドライン第5版」
- IPA「中小企業のためのクラウドサービス安全利用の手引き」
- IPA「情報セキュリティ関連規程」

各資料の概要は以下の通りです。

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」

「中小企業の情報セキュリティ対策ガイドライン」は、情報セキュリティ対策に取組む際の、（1）経営者が認識し実施すべき指針、（2）社内において対策を実践する際の手順や手法をまとめたものです。経営者編と実践編で構成されており、中小企業の利用を想定しています。付録の「5分でできる！情報セキュリティ自社診断」や「情報セキュリティハンドブック（ひな形）」を活用することで、対策基準、実施手順を策定できます。

NISC「インターネットの安全・安心ハンドブックVer.5.0」

「インターネットの安全・安心ハンドブック」は、サイバーセキュリティに関する基本的な知識を、身近な具体例を取り上げながら説明したものです。子供やシニアの方など、インターネットの一般利用者だけでなく、中小企業なども活用できます。中小組織向けにある「インターネットの安全・安心ハンドブックVer 5.00＜中小組織向け抜粋版＞」を活用することで、対策基準、実施手順を策定できます。

総務省「テレワークセキュリティガイドライン第5版」

「テレワークセキュリティガイドライン」は、企業などがテレワークを導入する際のセキュリティ対策についての考え方や対策例を示したものです。テレワークを既に導入している場合は、自社のテレワーク環境がガイドラインに沿ったものであるのか検証できます。テレワークに関する「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場からそれぞれのセキュリティ対策について対策基準、実施手順を策定できます。

IPA「中小企業のためのクラウドサービス安全利用の手引き」

「中小企業のためのクラウドサービス安全利用の手引き」は、中小企業の情報セキュリティ対策ガイドラインの付録資料です。クラウドサービスを安全に利用するための手引きが記載されています。「クラウドサービス安全利用チェックシート」と「解説編」を参考にすることで、クラウドサービス利用に関する対策基準、実施手順を策定できます。

IPA「情報セキュリティ関連規程」

「情報セキュリティ関連規程」は、自社に適した規程を作成するためのひな形です。ひな形に修正を加えることで、対策基準、実施手順を策定します。1から文書化する必要がないため、効率的に策定できます。

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（2/8）

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」の活用

対象者	• 中小企業および小規模事業者（業種は問わず、法人・個人事業主・各種団体も含む）の経営者と情報管理を統括する方 • 情報セキュリティ対策を部分的に実施してきた企業 • 情報セキュリティに関する知識を十分に有した人材が不足している企業など
目的	情報セキュリティに関する組織的な取組を開始するため

本ガイドラインは、情報セキュリティに関する組織的な取組を行う際に活用できます。本ガイドラインをもとに実施手順を策定する際は、「1. 実施状況の把握」「2. 対策の決定と周知」の手順で策定します。

1. 実施状況の把握

「5分でできる！情報セキュリティ自社診断」を利用し、現在の情報セキュリティ対策の実施状況を把握します。合計25問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。設問の例（一部抜粋）は以下の通りです。

診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	分からない
Part1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	-1
	2	パソコンやスマホなど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？	4	2	0	-1
	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	2	0	-1
	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？	4	2	0	-1
	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？	4	2	0	-1

自社診断の設問（一部抜粋）
(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

「5分でできる！情報セキュリティ自社診断」の使い方

- ✓ 経営者や情報システム担当者、部門長など情報セキュリティ対策の実施状況が分かる方が、25問の設問に回答します。
- ✓ 事業所が複数ある、部署数が多いなど、1人で記入することが難しい場合には、事業所や部署ごとに記入し、責任者・担当者が集計します。
- ✓ 実施状況が分からない場合、各従業員に質問して、回答を総合して記入します。
- ✓ チェック欄の該当するもの1つに〇をつけて、「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」「分からない…-1点」で採点します。
- ✓ 全項目の合計点で、組織全体のセキュリティ対策の実施状況と、回答が「分からない」になっている項目を把握します。

詳細理解のため参考となる文献（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3.1版	https://www.ipa.go.jp/security/guide/sme/about.html
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

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（3/8）

2.対策の決定と周知

診断結果をもとに「5分でできる！情報セキュリティ自社診断」（解説編）を参考にし、実行すべき情報セキュリティ対策を検討・決定します。解説編の例（抜粋）は以下の通りです。

診断編　No.3	パスワード管理
強固なパスワードを使用する	
パスワードが推測や解析されたり、Webサービスから流出した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る被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。	
対策例	• パスワードは10文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、推測できないようにする。 • 同じID・パスワードを複数サービス間で使い回さない。 • テレワークでVPNやクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。

解説編の一例
(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

「5分でできる！情報セキュリティ自社診断」（解説編）の使い方

✓ 対策の検討と決定は、責任者・担当者と経営者が行います。
✓ 診断項目ごとに対策を実施しない場合に考えられる被害・事故や、防止するための対策例を参考にして検討します。
✓ 検討するときには従業員の意見を聞き、職場環境や業務に適した対策を決定します。

対策の決定後、「情報セキュリティハンドブック（ひな形）」を利用し、従業員が実行するべき事項を周知します。情報セキュリティハンドブック（ひな形）は、自社診断の解説編に記載されている対策例と連動しています。ひな形を編集して決定した対策内容を具体的に記述し、従業員に配付します。ひな形の記載例は以下の通りです。

実施手順の例：パスワードの管理
ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

編集前（ひな形）

○必須	×禁止
10文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない

編集後

○必須	×禁止
16文字以上の文字数で構成されている	社員番号・名前・住所・電話番号・生年月日・辞書に載っている単語・他人に推測されやすい文字列は使わない

ひな形の修正例
(出典) IPA「情報セキュリティハンドブック（ひな形）」を基に作成

「情報セキュリティハンドブック（ひな形）」の使い方

✓ 情報セキュリティハンドブックは、責任者・担当者が作成します。
✓ ひな形に記載された例文を編集して、決定した対策を社内ルールとして明文化します。
✓ 完成した情報セキュリティハンドブックを全従業員に配付し、必要に応じて説明する機会を設けるなどして、情報セキュリティ対策を周知徹底します。

詳細理解のため参考となる文献（参考文献）	
情報セキュリティハンドブック（ひな形）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（4/8）

NISC「インターネットの安全・安心ハンドブックVer.5.0」の活用

対象者	• 全社員
目的	一人ひとりが能動的にサイバー空間における脅威を知り、サイバーセキュリティに対する素養・基本的な知識を身につけるため

本ハンドブックは、サイバー攻撃の手口やリスクを身近な具体例を取り上げながら説明しているため、専門知識を必要とせずサイバーセキュリティ対策を知ることができます。インターネットの利用者が実施すべき基本的なサイバーセキュリティ対策に加えて、中小組織向けのサイバーセキュリティ対策を記載しています。企業経営においてセキュリティ対策に投資すべき理由、企業特有のサイバーセキュリティ対策に必要なルール作りといった内容を説明しています。

以下では、第1章の「最低限実施すべきサイバーセキュリティ対策を理解しよう」を用いて、サイバーセキュリティ対策の実施手順の作り方を説明します。

（例）①OSやソフトウェアは常に最新の状態にしておこう

インターネットの安全・安心ハンドブック記載
- OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出るようにする。
- セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにする。
- サイバー攻撃で狙われやすい、ソフトウェアを重点的に更新する。
- 機器そのものの基本プログラムを更新するファームウェアもアップデートする。
- セキュリティソフトをインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定する。
- アップデートが提供されなくなったOSやソフトウェアはセキュリティホールが見つかっても修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにする。

自社の状況
- OS、オフィス系ソフト、セキュリティソフトは法人向けを利用しているため、アップデート管理は情報システム部が担当。
- 情報システム部がブラウザは古いバージョンを使わないように通知している。
- 自宅で使用しているリモート用PCは、一般向けのソフトがインストールされている。

実施手順

対象：PC
システム管理者は、アップデート管理として以下を実施する。
- システム管理者は月末にOS、オフィス系ソフト、セキュリティソフトの更新プログラムを適用する。緊急に対策が必要な場合は、従業員に通知し、更新プログラムを適用する。
- 従業員は、毎月OS、オフィス系ソフトの更新プログラムを適用する。確認方法はチェックリストを用いる。
- 従業員は、ブラウザのアップデートを適宜行い、バージョン○○以前のものは使用しない。
- システム管理者は○○日にセキュリティソフトのウイルス定義ファイルの更新を行う。

詳細理解のため参考となる文献（参考文献）	
インターネットの安全・安心ハンドブックVer.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（5/8）

総務省「テレワークセキュリティガイドライン第5版」の活用

対象者	• 経営者 • システム・セキュリティ管理者 • テレワーク勤務者
目的	テレワークを業務に活用する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するため

本ガイドラインでは、セキュリティ対策を整理するため、13個の対策分類に分かれています。「経営者」、「システム・セキュリティ管理者」、「テレワーク勤務者」の立場から対策分類ごとに具体的に実施すべき事項を示しています。

以下では、「6.マルウェア対策」をもとに、自社の状況からセキュリティ対策の実施手順の作成例を説明します。

（例）6. マルウェア対策

システム・セキュリティ管理者が実施すべき対策
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。
- セキュリティ対策ソフト（ウイルス対策ソフト）やメールサービスに付属しているフィルタリング機能やフィッシング対策機能などを用いて、テレワーク勤務者がマルウェアの含まれたファイルを開いたり、危険なサイトにアクセスしたりしないように設定する。
- テレワーク端末にEDRを導入し、未知のマルウェアを含めた不審な挙動を検知し、マルウェア感染後の対応を迅速に行えるようにする。
- テレワーク勤務者が利用するテレワーク端末のセキュリティ対策ソフト（ウイルス対策ソフト）について、定義ファイルの更新状況やマルウェアの検知状況が一元管理できるようにする。

テレワーク勤務者が実施すべき対策
- 少しでも不審を感じたメール（添付ファイルやURLリンクなどを含む。）は開かず、必要に応じて送信者に送信状況の確認を行うほか、システム・セキュリティ管理者へ速やかに報告する。報告の是非について判断に迷う場合は報告することを心がける。
- テレワーク端末にセキュリティ対策ソフト（ウイルス対策ソフト）をインストールし、定義ファイルの自動更新やリアルタイムスキャンが行われるようにする。

自社の状況
- テレワーク端末には、法人向けのセキュリティ対策ソフトとEDR製品を導入しており、システム管理者はウイルス定義ファイルの更新などを一元管理できる。
- システム管理者は毎月○○日にセキュリティソフトのレポートを確認している。
- 不審なメールが来た場合は、情報システム部と上長に連絡するようにしている。

実施手順

テレワーク端末のマルウェア対策として以下を実施する。
- システム管理者は会社支給のテレワーク端末にセキュリティ対策ソフトとEDR製品をインストールし、一元管理する。
- システム管理者は、テレワーク端末のウイルス定義ファイルの自動更新とリアルタイムスキャンを設定する。
- システム管理者は毎月○○日にセキュリティソフトとEDR製品のレポートを確認し、不審な点があれば該当のテレワーク端末所有者に対して、確認を行う。
- 従業員は、不審を感じたメール（添付ファイルやURLリンクなどを含む。）は開かず、システム管理者と上長へ連絡する。

詳細理解のため参考となる文献（参考文献）	
テレワークセキュリティガイドライン第5版	https://www.soumu.go.jp/main_content/000752925.pdf

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（6/8）

IPA「中小企業のためのクラウドサービス安全利用の手引き」の活用

対象者	• クラウドサービスを利用する企業
目的	クラウドサービスを安全に利用するため

本ガイドラインは、クラウドサービスを安全に利用するために活用できるガイドラインです。「利用するクラウドサービスを選定するとき」、「クラウドサービスを運用していくとき」、「クラウドサービスのセキュリティ対策を検討するとき」のタイミングで活用することができます。本ガイドラインの使い方としては、「クラウドサービス安全利用チェックシート」でチェックを行います。また、「解説編」を参考に、利用者としての役割や責任を認識し、実施手順を策定します。

以下は、クラウドサービスの運用に関する設問例となります。

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

クラウドサービス安全利用チェックシートの例（一部抜粋）
(出典) IPA「中小企業のためのクラウドサービス安全利用の手引き」を基に作成

解説編をもとに実施手順を作成します。 以下は、チェックシートの設問「バックアップに責任を持つ」の実施手順（例）を記載します。自社の状況に合わせて赤文字の箇所を修正することで、自社に適した実施手順を作成できます。

実施手順の例：バックアップに責任を持つ

バックアップの管理
サービス停止やデータの消失・改ざんなどに備え、重要情報を手もとに確保して、必要なときに使えるようにする。

会計データやホームページなど、消失や改ざんの影響が大きいものは以下の規則を遵守する

- クラウドサービスの拡張機能にバックアップがある場合は利用する
- 月に1度、社内の専用ハードディスクにバックアップを取得する
- 直前のバックアップよりもさらに過去の状態に遡って復元できるよう、2、3ヶ月前に取得したバックアップを保存しておく

詳細理解のため参考となる文献（参考文献）	
付録6：中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（7/8）

IPA「情報セキュリティ関連規程」の活用

対象者	• 中小企業
目的	自社のリスクに応じた対策規程を作成するため

情報セキュリティ関連規程とは、自社が対応すべきリスクと対策を検討し、文書化した規程のことです。企業を取り巻くリスクは、事業内容や取扱う情報、職場環境、ITの利用状況などによって異なるため、汎用的な規程をそのまま使っても、自社に適さない場合があります。そこで情報セキュリティ関連規程を活用することで、効率的に自社に適した規程を作成できます。

本ガイドラインを用いて、規程を作成する手順を説明します。

1. 対応すべきリスクを特定する

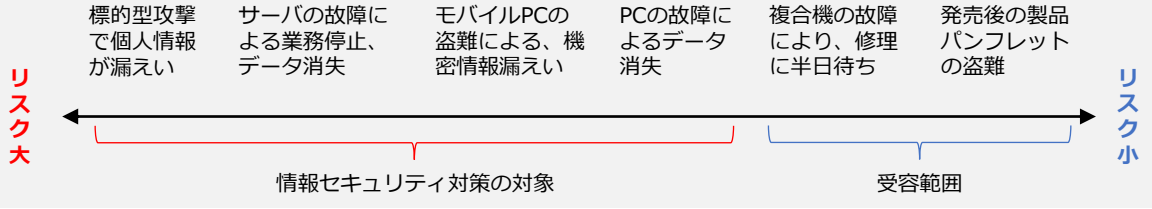
経営者が懸念する情報セキュリティの重大事故などを念頭に、何を起こさないようにするべきかを考えます。このとき、以下のような状況を併せて考えることで、対応すべきリスクを把握します。

- ✓ 関連する業務や情報に関わる外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）
- ✓ 内部状況（経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など）

（例）
- 個人情報保護法への対応
- 取引先のセキュリティに対する要求への対応
- テレワーク時のセキュリティ対応
- 報道されている新たなサイバー攻撃への対応

2. 対策の決定

すべてのリスクに対応しようとすると、対策費用が高額になったり、業務に支障をきたしたりする場合があります。そこで、いつ事故が起きてもおかしくない、事故が起きると大きな被害になるなど、リスクが大きなものを優先して対策を実施します。また、事故が起きる可能性が小さい、発生しても被害が軽微であるなど、リスクが小さなものは、現状のまま受容するなど、合理的に対応します。



12-3-1. 情報セキュリティ対策ガイドラインの活用

LV.2 ベースラインアプローチ（8/8）

3. 規程の作成

「2. 対策の決定」で情報セキュリティ対策の対象としたリスクに対して対策を実施するため、文書化した規程を作成します。「中小企業の情報セキュリティ対策ガイドライン 付録5情報セキュリティ関連規程（サンプル）」を編集することで、規程を作成することができます。以下では、「サーバの故障による業務停止、データ消失」に対する対策を文書化した規程の例を記載します。赤文字の箇所を修正することで、自社に適した規程を作成します。

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバ	ユーザーファイル	アプリケーションバックアップ機能	NASサーバ
Webサーバ	ホームページ	同期ツール	NASサーバ
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

- NASサーバ：施錠つきサーバラックに収納

情報セキュリティ関連規程の一例
(出典) IPA「情報セキュリティ関連規程（サンプル）」を基に作成

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
DBサーバ	取引先に関するデータ	アプリケーションバックアップ機能	自社サーバ
Webサーバ	ホームページ	同期ツール	自社サーバ
発注管理システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウド上のサーバ

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

<保管>

- 自社サーバ：ハウジングサービスを利用し、サービス事業者の施設内に保管する

詳細理解のため参考となる文献（参考文献）	
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

第13章. ISMSの要求事項と構築（LV.3 網羅的アプローチ）

13-1. 【LV.3 網羅的アプローチ】の概要

13-2. 【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

章の目的
第13章では、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて理解することを目的とします。

主な達成目標
◘ 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

13-1-1. LV.3 網羅的アプローチ

網羅的アプローチでは、フレームワークとしてISMSを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。第13章では、ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明していきます。

ISMSの要求事項に関連するドキュメント作成は重要ですが、あくまで手段であり目的ではありません。ドキュメントの作成と維持が目的化してしまうと、ドキュメントが形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。**ドキュメントを精細に作り込むことより、ISMSマネジメントプロセスを取り入れ、PDCAサイクルを回していくことが大切です。**ISMSに取組み始めたときには理解できていても、ドキュメント作りを始めるとドキュメント作成が目的になってしまうケースが多いため、注意が必要です。

LV.3 網羅的アプローチ（網羅性のあるアプローチ方法）

概要
網羅的なフレームワークとしてISMSを参考にします。ISMSのフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。

メリット
- ISMS要求事項の導入が可能です。

デメリット
- 時間とコストがかかる。

13-2-1. ISMSの概要（確立・運用・監視）

ISMSの確立、運用、監視

「第7章. セキュリティフレームワーク」でも記載した通り、ISMSはPDCAサイクルに則って運用することとなります。PlanでISMSを確立し、Doで導入および運用、Checkで監視および見直し、Actで維持および改善を行います。ISMSの取組で、組織の情報セキュリティをより良くするために管理手段レベルでの解決を目指すことになります。同じ失敗を繰り返さない、あるいは現状を改善し続けるために、PDCAサイクルによって継続的な改善を図ることが重要です。

本テキストでは、網羅的アプローチとして必要なドキュメントや項目を抜粋し、詳細に説明していきます。なお、ISMSの要求事項を定めているISO/IEC 27001の1から3はそれぞれ「1.適用範囲」「2.引用規格」「3.用語および定義」なので、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの7項目となっています。

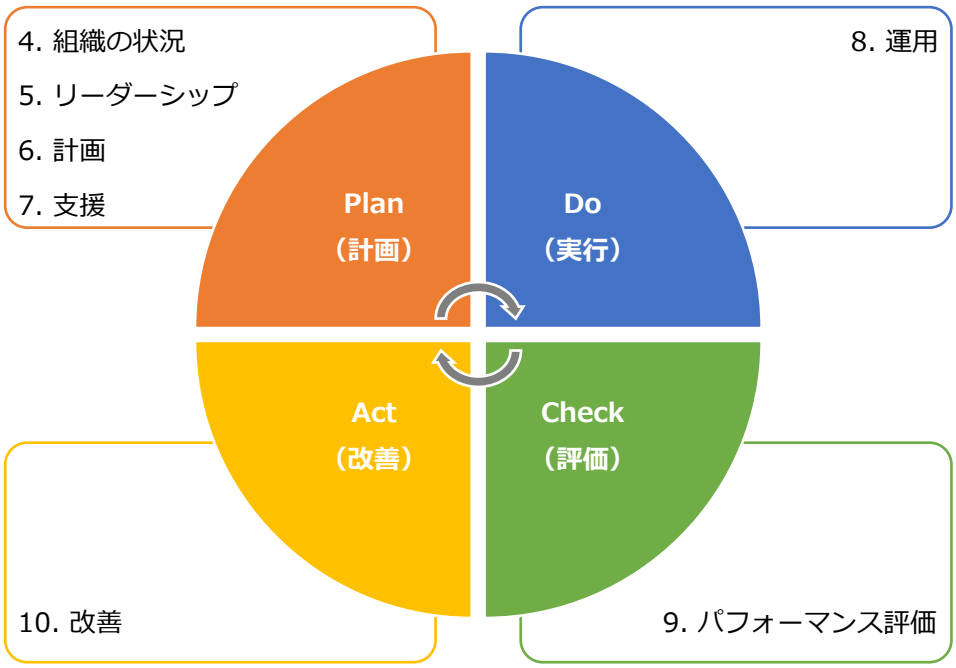
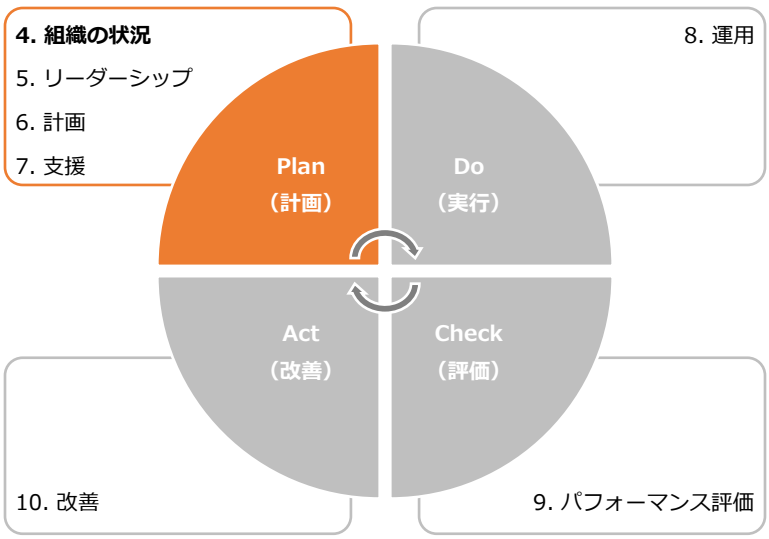


図53. ISO/IEC 27001のPDCAサイクル

13-2-2. ISMS：4. 組織の状況

ISMS構築の第一歩は、組織の状況を把握することにあります。 組織が抱えている情報セキュリティ上の課題を明らかにするとともに、組織の利害関係者が情報セキュリティに関してどのようなニーズや期待を持っているのかを整理し、情報セキュリティに取組む意義を確認します。それを踏まえて、「ISMSの適用範囲」を決定することになります。この「4.組織の状況」は、PDCAサイクルの「Plan（計画）」に位置していますが、組織の内外の状況に応じて見直す必要があります。

4. 組織の状況	作成ドキュメント（例）
4.1 組織及びその状況の理解 ISMSを構築することで解決したい課題（組織の目的に関連する内部課題、外部課題）を明確にします。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解 ISMSに関係する利害関係者（顧客、従業員、取引先など個人や組織）と、利害関係者から要求される情報セキュリティに関係する要求事項を明確にします。	• 利害関係者のニーズ及び期待
4.3 情報セキュリティマネジメントシステムの適用範囲の決定 決定された外部課題・内部課題、利害関係者の要求事項と、業務内容や他の組織との情報のやり取り、ネットワーク構成などを考慮し、ISMSの適用範囲を合理的に決定します。	• ISMS適用範囲 • レイアウト図 • ネットワーク図
4.4 情報セキュリティマネジメントシステム 決定したISMSの適用範囲を対象に、PDCAサイクルに基づくISMSを構築・運用します。	ー



13-2-2. ISMS：4. 組織の状況

4.1 組織及びその状況の理解

作成するドキュメント
- 外部および内部の課題

「組織及びその状況の理解」では、組織を取り巻く外部と内部の課題を整理することが求められています。ここで整理した課題を、ISMSの取組を通して解決していきます。また、組織のどの部分に対してISMSを適用すべきなのかといった適用範囲を確定する際にも、課題を考慮することとなります。

外部の課題

組織の外部に原因が存在する課題は、以下の情報をヒントに決定することができます。
- 国際、国内、地方または近隣地域を問わず、文化、社会、政治、法律、規制、金融、技術、経済、自然および競争の環境
- 組織の目的に影響を与える主要な原動力および傾向
- 外部ステークホルダーとの関係並びに外部ステークホルダーの認知および価値観

（例）

課題	リスク	機会
個人情報、機密情報の保護（ウイルス感染、情報漏えい、新たな脅威への対応）	情報セキュリティ事故の発生 →信用低下	情報の活用

内部の課題

組織の内部に原因が存在する課題は、以下の情報をヒントに決定することができます。
- 統治、組織体制、役割およびアカウンタビリティ
- 方針、目的およびこれらを達成するために策定された戦略
- 資源および知識として見た場合の能力（たとえば、資本、時間、人員、プロセス、システムおよび技術）
- 情報システム、情報の流れおよび意思決定プロセス（公式および非公式の双方を含む。）
- 内部ステークホルダーとの関係並びに内部ステークホルダーの認知および価値観
- 組織文化
- 組織が採択した規格、指針およびモデル
- 契約関係の形態および範囲

（例）

課題	リスク	機会
ISMSに関する理解の促進	理解不足による情報セキュリティ事故	体勢強化
情報(紙、電子データ)の適切な取扱い	紛失、訪問先などで置忘れ →信頼喪失	信頼向上
ノウハウ、お客様より預かる機密情報などの保護	機密情報の漏えい、ノウハウの流出	ビジネス機会の拡大

13-2-2. ISMS：4. 組織の状況

4.2 利害関係者のニーズ及び期待の理解

作成するドキュメント
- 利害関係者のニーズ及び期待

「利害関係者のニーズ及び期待の理解」では、組織の利害関係者と、その利害関係者が要求する情報セキュリティに関する要求事項を明確化することが求められます。利害関係者には、顧客や従業員、取引先など、さまざまな個人や組織が含まれます。利害関係者に該当する範囲は広いため、組織が管理できる範囲で利害関係者からの要求事項を特定します。また、どの程度のセキュリティレベルで対策するのか、利害関係者とそのニーズから水準を設定することになります。

利害関係者のニーズ及び期待の記入例

利害関係者	情報セキュリティに関する要求事項	リスク	機会
取引先	適切な情報の取扱い	不適切な取扱いで信頼低下 →案件減少	適切な対応で信頼向上 →受注の維持/増加
	法令遵守	未遵守による信頼低下 →案件減少	遵守による信頼向上 →受注の維持/増加
株主	セキュリティインシデントの未然防止	セキュリティインシデントの発生 →ブランドイメージの低下	セキュリティインシデントの発生数減少 →ブランドイメージの向上
従業者	情報セキュリティに関する教育	機密情報/ノウハウの流出	組織の価値向上
	必要な情報へのアクセス	機密情報/ノウハウの流出	効果的・効率的な業務 →競争力アップ
	個人情報の保護	不適切な情報の取扱い →信頼低下	従業者から信頼向上 →人材の確保
国・自治体	法令・その他規範の遵守	セキュリティインシデント発生時の不適切な対応 →社会的信頼の低下	社会的信頼の向上

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（1/3）

作成するドキュメント
- ISMS適用範囲
- レイアウト図
- ネットワーク図

ISMSの適用範囲は、必ずしも会社全体とする必要はありません。特に大企業の場合には、特定の業務や特定の部門に限定してISMSを構築することがあります。たとえば、ある取引先の要請によってISMSを構築する場合、その取引先と取引のある部門に適用範囲を限定するケースがあります。

中小企業の場合には、会社全体を適用範囲とすることが多いので、特段の理由がない限り、会社全体を適用範囲にするとよいでしょう。

「情報セキュリティマネジメントシステムの適用範囲の決定」では、ISMSを適用するところと、そうではないところの境界およびその適用される範囲内で、規格の要求事項がどのように適用できるかを決定するよう要求しています。規格などの要求事項によって定められる改善すべき範囲を、適用範囲と言います。

適用範囲の決定に際しては、考慮しないといけない3つの事項があります。2つはこれまでに説明した「外部および内部の課題」と「要求事項」です。もう1つは、「組織が実施する活動と、他の組織が実施する活動との間のインターフェースおよび依存関係」です。異なる部署や委託先など他の組織との業務プロセスにおける依存度を見ながら、適用範囲を広げるのか、分離しておくのかを検討することになります。

インターフェースおよび依存関係の記入例

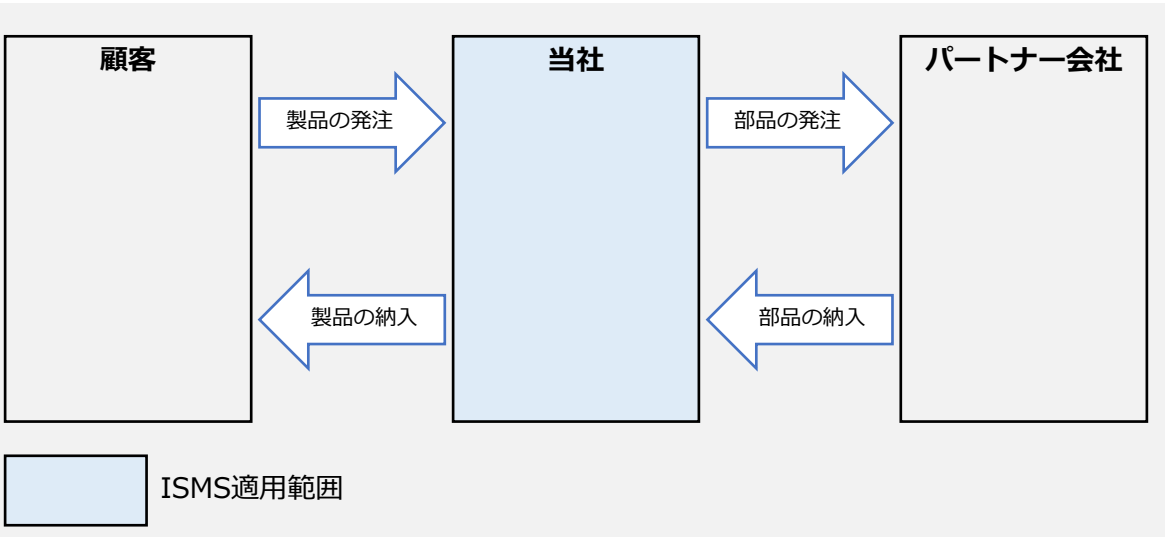


図54. インターフェースおよび依存関係の記入例

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（2/3）

適用範囲を組織の一部とした場合、同じ組織内に適用範囲の内と外という境界ができることになります。適用範囲の境界について、いくつかの観点から明確にしておく必要があります。

人的・組織的境界

組織におけるどの人、どの部門が適用範囲の内側に該当するのかを明確にします。それにより、同じ社内の人であっても、適用範囲外の人を外部の人として扱うといった配慮が必要になる場合があります。

物理的境界

適用範囲とする建物や施設、部屋といった空間を明確にします。扉や壁、パーティションなどの物理的な境界によって仕切られていることが望ましいです。

技術的境界

ネットワークにおいて、対象とする範囲を明確にします。物理的境界と同様に、適用範囲のIT環境の境界を明らかにし、管理しなければならない情報システムや、ネットワークの対象や範囲を明確にする必要があります。

資産的境界

業務委託を受けていたり、組織の一部を適用範囲にしたりした場合に、資産的境界が生じる場合があります。顧客から情報や資源の提供を受けた際に、それを指定された管理方法で管理するのか、自組織の管理下となるのかといった場合や、適用範囲内の部門が保有する情報でも、組織全体で共有している場合にはどう管理するのかを明確にする必要があります。

事業的境界

事業（業務）においても対象を明確にします。事業は部門を横断する場合があるため、人的・組織的境界とも合わせて対象を検討し、適用範囲を明確にする必要があります。

13-2-2. ISMS：4. 組織の状況

4.3 情報セキュリティマネジメントシステムの適用範囲の決定（3/3）

物理的境界 レイアウト図（例）

物理的境界では、適用範囲とする空間を明確にし、境界線を記載します。そして境界線で区切られた空間ごとにセキュリティレベルを設定します。

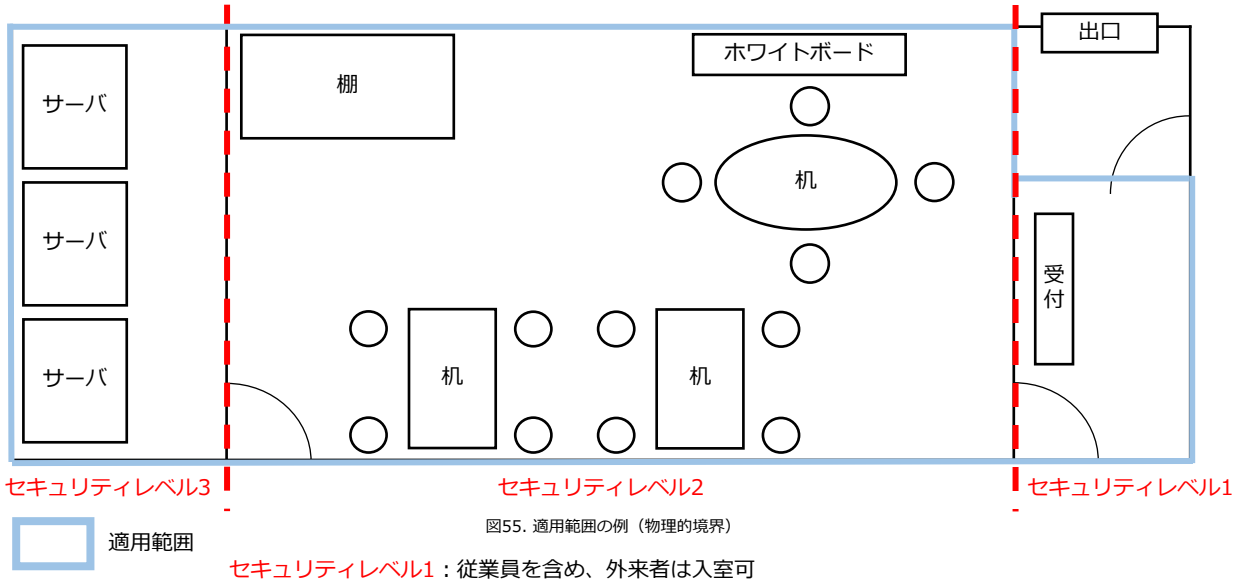


図55. 適用範囲の例（物理的境界）

セキュリティレベル1：従業員を含め、外来者は入室可
セキュリティレベル2：対象従業員のみ入室可（対象者以外は入退室管理が必要）
セキュリティレベル3：限られた人員のみ入室可（飲食禁止）

技術的境界 ネットワーク図（例）

ネットワークにおいて対象とする範囲を明確にするため、ネットワーク構成図を作成し、境界線を記載します。

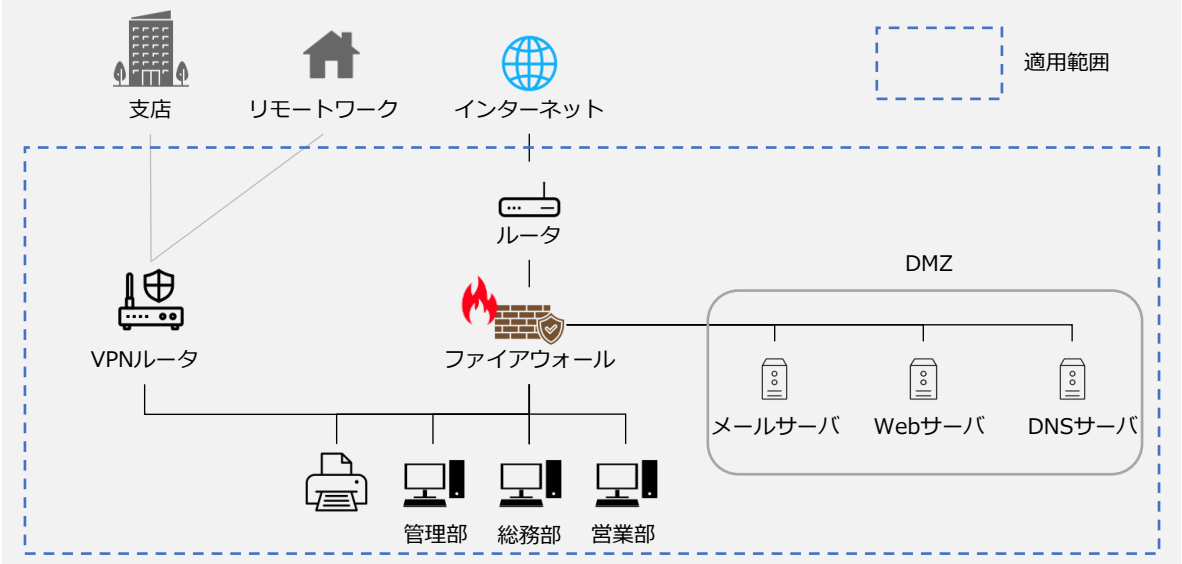
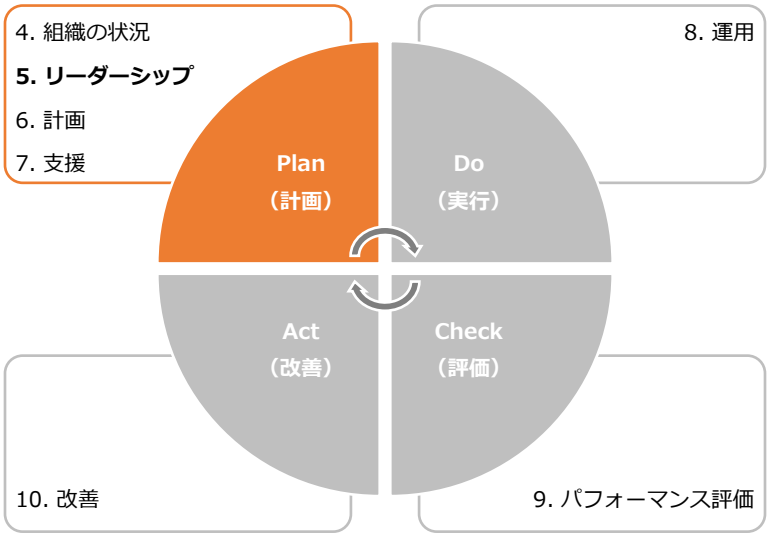


図56. 適用範囲の例（技術的境界）

13-2-3. ISMS：5. リーダーシップ

「5. リーダーシップ」は、PDCAサイクルの「Plan（計画）」に位置しており、トップマネジメントに求められる要求事項を示しています。トップマネジメントとは、ISMSの適用範囲における最高責任者のことを指します。多くの場合、トップマネジメントは、組織の社長が担う傾向にあります。「5. リーダーシップ」は、PDCAサイクルの軸であり、PDCAサイクルを回すには、トップマネジメントのコミットメント（関与、制約）が重要になります。

5. リーダーシップ	作成ドキュメント（例）
5.1 リーダーシップ及びコミットメント トップマネジメントが責任を持って実行しなければならない事項が記載されています。	―
5.2 方針 トップマネジメントが、ISMSの目的や方向性、実施する内容について文書化し、「情報セキュリティ方針」を作成することを要求しています。	• 情報セキュリティ方針
5.3 組織の役割、責任及び権限 トップマネジメントは、ISMSを運用するために必要な役割や責任、権限を各要員に割り当て、どの要員がどのような役割や責任、権限を持っているかが分かる文書を作成することを要求しています。	• ISMSの運用組織図 • 責任者または部門の名称と役割を明記した文書



13-2-3. ISMS：5. リーダーシップ

5.1 リーダーシップ及びコミットメント

「リーダーシップ及びコミットメント」では、ISMSのトップマネジメントが責任を持たなければならないことを要求しています。トップマネジメントは、以下の事項について責任を持って必ず行う必要があります。

トップマネジメントが行う事項（要求事項）
情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする → 組織の事業の方向性に沿った情報セキュリティ方針と、情報セキュリティ目的を策定することを要求しています。※情報セキュリティ方針、情報セキュリティ目的については後述します。
組織のプロセスへのISMS要求事項の統合を確実にする → 自社の業務に、情報資産を管理する手順を組み込むことを要求しています。
ISMSに必要な資源が利用可能であることを確実にする → ISMSを構築・運用するために、必要な予算や人員など経営資源を確保しておくことを要求しています。
有効な情報セキュリティマネジメントおよびISMS要求事項への適合の重要性を伝達する → 従業員がISMSを構築・運用し、情報資産を適切に管理することの重要性を十分に認識できるよう、周知することを要求しています。
ISMSがその意図した成果を達成することを確実にする → ISMSを構築・運用することで得られる成果を明確にし、その成果を十分に得られるように取組んでいくことを要求しています。
ISMSの有効性に寄与するよう人々を指揮し、支援する → ISMSを構築・運用できるようにするため、従業者に対して教育を受けさせたり、定めた決まりを認識・実施させたり、従業員の意見を聞いたりするなど、サポートすることを要求しています。
継続的改善を促進する → ISMSを構築・運用するにあたり、従業員が不便に感じていることなど、改善が必要だと考えられる場合には、改善を進めるよう要求しています。
その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する → 組織の規模や形態によって、トップマネジメントの指示が従業員に適切に伝わらない可能性があります。そのため、各部門の責任者が主導となり、従業員にトップマネジメントの指示を適切に伝え、ISMSを円滑に構築・運用できるようにすることを要求しています。

13-2-3. ISMS：5. リーダーシップ

5.2 方針

作成するドキュメント
- 情報セキュリティ方針

トップマネジメントは、組織の情報セキュリティに対する考え方や取組の姿勢を利害関係者に示すため、情報セキュリティ方針を文書として作成し、組織内に周知するとともに、必要に応じて、その他の利害関係者が入手できるようにします。たとえば、保護するべき情報資産と保護すべき理由を明示し、利害関係者に周知します。

情報セキュリティ方針の作成方法

情報セキュリティ方針は、以下の事項を満たす必要があります。しかし、規格の内容をそのまま記載するのではなく、内容を理解した上で組織内部の従業員や、利害関係者にとって分かりやすい方針を作成する必要があります。

情報セキュリティ方針が満たさなければならない事項

a) 組織の目的に対して適切である
b) 情報セキュリティ目的を含むか、または情報セキュリティ目的の設定のための枠組みを示す
c) 情報セキュリティに関連する適用される要求事項を満たすことへのコミットメントを含む
d) ISMS の継続的改善へのコミットメントを含む

a) 自社の経営理念に基づいた事業の目的や、情報セキュリティの必要性などを記載します。また、業務に関わる情報資産と、保護すべき理由などを記載します。

b) 情報セキュリティに関する目標を記載します。

情報セキュリティ方針（例）

【第X版】
【日付】
【社名】
【代表取締役社長　名前】

私たち【社名】は、【提供するサービス名】の提供を通じて、お客様、社員とその家族などすべてのステークホルダーの期待に応え、社会に貢献することを使命と考えています。

当社の事業活動において、お客様からお預かりする個人情報を含む多くの情報資産を活用しており、すべてのステークホルダーの期待に応えるためには、これらの情報資産を保護することは、経営上の最重要課題であると認識しています。

よって、私たちは、情報セキュリティ基本方針を策定し、本基本方針に基づいて、ISMSを構築・運用し、当社を取り巻く環境の変化を踏まえ、継続的改善に全社を挙げて取組むことをここに宣言します。

さらに、当社は、以下のセキュリティ目的を設定し、この目的を達成するための諸施策を確実に実施します。
✓ お客様との契約および法的または規制要求事項を尊重し遵守する。
✓ 情報セキュリティ事故を未然に防止する。
✓ 万一情報セキュリティ事故が発生した場合、影響を最小限にする。

以上

c) 自社の業務の特徴や課題を記載します。

d) ISMSに関する取組を定期的に見直し、改善していく内容を記載します。

13-2-3. ISMS：5. リーダーシップ

5.3 組織の役割、責任及び権限

作成するドキュメント
- ISMS運用組織図
- 責任者または部門の名称と役割を明記した文書

「組織の役割、責任および権限」とは、ISMSを構築・運用するために、トップマネジメントが、組織内で役割を決め、責任と権限を割り当てることです。

ある程度の規模以上の組織になると、ISMSの実際の運用担当者や責任者は、トップマネジメントから権限を委譲された人になります。そうすると、情報セキュリティに関する取組の実態を、トップマネジメントが十分把握していないという状況になりがちです。そうならないために、ISMSの実施状況をトップマネジメントに報告する仕組みやルールを作っておく必要があります。

ISMS運用組織図の作成方法（例）

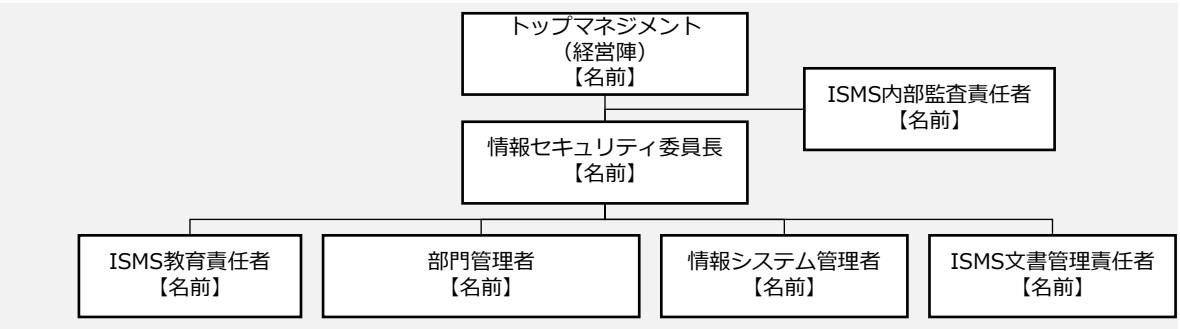


図57. ISMS運用組織図の例

ISMSの運用組織図を作成する流れを説明します。

1. トップマネジメントは、情報セキュリティ委員長を任命し、上記の事項に関する権限や責任を持たせる必要があります。そのため、トップマネジメントの下位に、情報セキュリティ委員長を配置します。
2. ISMS内部監査責任者は、内部監査を実施する際の最高責任者であり、トップマネジメントの下位に設置します。
3. 情報セキュリティ委員長は、ISMSの実施・運用のために必要な役割を持つ責任者を任命します。情報セキュリティ委員長の下位に各責任者を配置します。

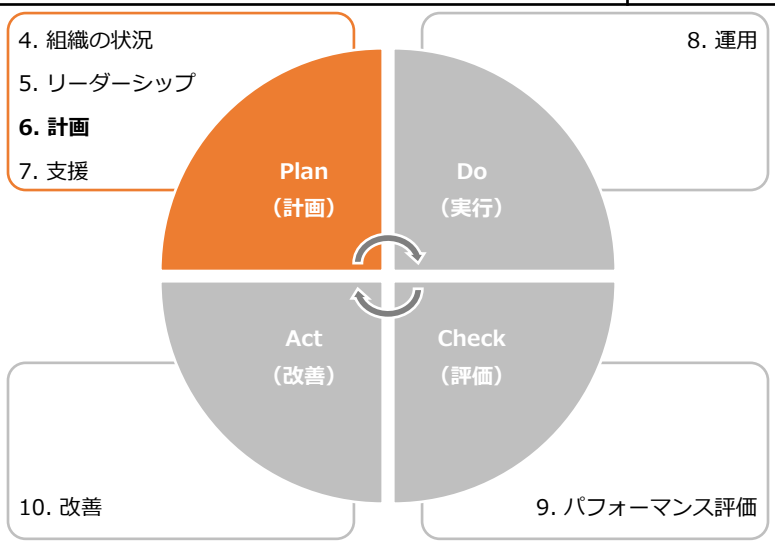
責任者または部門の名称と役割を明記した文書の作成方法（例）

名称	役割
情報セキュリティ委員長	ISMSの実施、運用について統括する
ISMS内部監査責任者	ISMSとその実施状況に関わる監査を統括する
ISMS教育責任者	ISMSに関する教育計画の立案と実施を行う
部門管理者(情報セキュリティ委員)	ISMSの部門代表者として、部門を管理する
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規程・規則に従い、ISMSを維持するための安全管理対策を実施する
ISMS文書管理責任者	ISMSに関する文書と記録などの維持・管理を行う

13-2-4. ISMS：6. 計画

「6. 計画」は、PDCAサイクルの「P（計画）」に位置しており、リスクマネジメントの確立、情報セキュリティにおけるリスクアセスメント、リスク対応、情報セキュリティ目的の管理に関する要求事項を示しています。

6. 計画	作成ドキュメント（例）
6.1 リスク及び機会に対処する活動 ① **一般** 特定した内外部の課題と、利害関係者のニーズおよび期待を考慮して、リスク・機会（期待する状況や結果）を決定し、対処するための活動を明確にすることを要求しています。 ② **情報セキュリティリスクアセスメント** 組織や企業の資産に対する、情報セキュリティリスクアセスメントプロセスの確立を要求しています。 ③ **情報セキュリティリスク対応** 情報セキュリティリスク対応の手順を確立することを要求しています。	• 資産目録（情報資産管理台帳） • リスクアセスメント結果報告書 • 適用宣言書 • リスク対応計画
6.2 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティ目的を確立し、達成するための計画を策定することを要求しています。	• ISMS有効性評価表
6.3 変更の計画策定 ISMSの変更が必要なときは、計画的な変更を要求しています。	―



13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（1/9）

作成するドキュメント
- 資産目録（情報資産管理台帳）
- リスクアセスメント結果報告書

「リスク及び機会に対処する活動」とは、「ISMSの意図した成果を達成する」「ISMSの望ましくない影響を防止・低減する」「継続的改善を達成する」の3つを実現するために、妨げとなるような機会やリスクを発見し、対処することです。

平たく言えば、情報セキュリティ上のリスクに対して、適切な対策を講じることで、情報セキュリティを確保するための活動になります。

具体的には「リスクアセスメントの実施」「リスク対応策の作成と実施」「リスク対応策の有効性評価」「継続的改善」といった活動が含まれます。

リスクアセスメントは、組織や企業の資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位づけをしていくプロセスになります。リスクアセスメントの実施により、リスクを評価し、事前にリスクを把握することで必要な投資額を含め、企業が適切な対策を検討することが可能になります。

情報セキュリティのリスク基準を確立し、維持する

リスクアセスメントを実施するにあたり、リスクの重大性を評価するための目安となるリスク基準を決める必要があります。ISMSでは、リスク基準に「リスク受容基準」と「情報セキュリティリスクアセスメントを実施するための基準」を含むように明示されています。
※「11-2-1. リスク基準の確立」を参照

情報セキュリティリスクを特定する

企業が掲げる目的・目標の達成を阻害する可能性のあるリスクをすべて洗い出すことです。そのため、リスクの発生可能性や影響の大きさを考慮せず、少しでも企業に影響を与えそうなリスクを洗い出すことが目的となります。リスク特定として最終的な成果はリスク一覧表の作成になります。
※「11-2-2. リスクの特定」を参照

情報セキュリティリスクを分析する

リスク特定で特定されたリスクに対して、リスク分析を行います。リスク分析を行うことで、「企業にとって対応が必要なリスクはどれか」、「優先的に対応しなければならないリスクは何か」といったことを判断します。リスク分析で求めた結果を、「リスクアセスメント結果報告書」に記載します。
※「11-2-3. リスクの分析」を参照

情報セキュリティリスクを評価する

リスク分析で算出したリスクレベルからリスク受容基準と比較し、リスク対策が必要かどうかを判断します。また、算出したリスクレベルをもとに優先順位をつけます。
※「11-2-4. リスクの評価」を参照

本項では、資産目録（情報資産管理台帳）とリスクアセスメント結果報告書を作成します。2つのドキュメントは、ISO/IEC 27001:2022の管理策「5.9 情報およびその他の関連資産の目録」に対応します。

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（2/9）

資産目録（情報資産管理台帳）の作成方法は「 11-2. リスクマネジメント：リスクアセスメント」で説明しました。作成した資産目録（情報資産管理台帳）から、リスクアセスメントの結果をまとめた「リスクアセスメント結果報告書」について説明します。

リスク特定における、リスクアセスメント結果報告書の作成方法（例）

以下の手順で、リスク一覧表となるリスクアセスメント結果報告書を作成します。

1. 資産目録（情報資産管理台帳）から、「情報セキュリティリスクアセスメントを実施するための基準」で決定した基準をもとに、重要資産を選択します。例では、機密性、完全性、可用性の項目の評価値が1つでも3となった資産を重要資産としています。選択した重要資産を「リスクアセスメント結果報告書」に記載し、リスク一覧表を作成します。

No	資産目録のNo	リスク特定				
		リスク源	影響領域	事象	原因	起こり得る結果
1	9	モバイル機器の利用ルールが十分に整備されていない	外部	持ち出し中に重要な情報を紛失・盗難(機密性の喪失)	【事象】に対し【リスク源】である	機密情報などが漏えいし、顧客に影響、信用喪失
2	40	教育が不十分なため従業者の意識が低い	全社	誤送信(機密性の喪失)	【リスク源】ため【事象】が発生	機密情報などが漏えいし、顧客に影響、信用喪失
3	10、11、13、26、55	電子の情報分類／取扱いが明確でない	外部	情報の紛失・盗難(機密性の喪失)	【リスク源】ため【事象】が発生	機密情報などが漏えいし、顧客に影響、信用喪失

リスクアセスメント結果報告書には、以下の内容を記載します。

- ✓ **資産目録のNo**
  作成した資産目録に対応する項番を記載します。
  ※リスクによっては資産目録のNoは複数になることもあります。
- ✓ **リスク源**
  想定される脅威を記載します。
  （例）モバイル機器の利用ルールが十分に整備されていない　など
- ✓ **影響領域**
  脅威が発生した場合の影響範囲を記載します。
  （例）外部、全社　など
- ✓ **事象**
  発生する可能性のある事象を記載します。
  （例）持ち出し中に重要な情報を紛失・盗難(機密性の喪失)　など
- ✓ **原因**
  事象が発生する原因を記載します。
  （例）【事象】に対し【リスク源】である、【リスク源】ため【事象】が発生　など
- ✓ **起こり得る結果**
  事象が発生した場合に起きる結果を記載します。
  （例）機密情報などが漏えいし顧客に影響、信用喪失　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（3/9）

リスク分析・リスク評価における、リスクアセスメント結果報告書の作成方法（例）

事象	原因	起こり得る結果	リスク分析			優先順位
			重要度	被害発生可能性	リスクレベル	
持ち出し中に重要な情報を紛失・盗難（機密性の喪失）	【事象】に対し【リスク源】である	機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2
誤送信（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3
情報の紛失・盗難（機密性の喪失）	【リスク源】ため【事象】が発生	機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1

具体的には、以下の内容を記載します。

✓ **重要度**
「機密性」「完全性」「可用性」いずれかの最大値で判断します。
（例）機密性：1、完全性：2、可用性：3 →　重要度：3
　　機密性：2、完全性：1、可用性：1 →　重要度：2

✓ **被害発生可能性**
脅威の起こりやすさと脆弱性のつけ込みやすさから換算表に当てはめて算出します。

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

起こりやすさ：2、つけ込みやすさ：1 → 被害発生可能性：1
起こりやすさ：3、つけ込みやすさ：3 → 被害発生可能性：3

✓ **リスクレベル**
重要度と被害発生可能性から算出します。
（例）重要度：3、被害発生可能性：1 →　リスクレベル：3
　　重要度：2、被害発生可能性：3 →　リスクレベル：6

✓ **優先順位**
リスク受容基準をもとに、リスクレベルから優先順位づけを行います。

（例）1：早急に対応、2：今期中に対応、3:：今期対応が望ましい
リスクレベル：9　→　優先順位：1
リスクレベル：4　→　優先順位：3
リスクレベル：6　→　優先順位：2

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（4/9）

作成するドキュメント
- リスクアセスメント結果報告書
- 適用宣言書
- リスク対応計画

リスクアセスメントにおいて、自社の情報セキュリティリスクを洗い出します。リスク対応では、洗い出したそれぞれのリスクに対してどう対策するのか、ISMSの管理策を実施の有無を含めて検討します。リスク対応は以下のプロセスになります。

リスク対応のプロセス

1.適切な情報セキュリティリスク対応の選択肢の選定
リスク対応の選択肢（リスクの回避、低減、移転、受容（保有））から選定する。
2.情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定
ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要なすべての管理策を決定します。
3.決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較
必要なすべての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。
4.適用宣言書の作成
必要なすべての管理策と、その理由および実施状況を文書化します。適用宣言書に含まれるすべての管理策の実施状況は、“実施された”、“一部実施された”または“実施されていない”として記述できます。
5.情報セキュリティリスク対応計画
組織がリスクに対応する必要性を含んだリスク対応計画を作成します。リスク対応計画とは、組織のリスク受容基準を満たすようにリスクを修正するための計画のことです。 - 組織の必要な管理策を実施するためのプロジェクト計画 - リスクを修正するために管理策が環境と相互にどのように作用するかを記述した設計計画
6.リスク所有者による承認
リスク所有者は、リスク対応計画を承認します。
7.残留している情報セキュリティリスクの受容
リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。

本項では、リスクアセスメント結果報告書、適用宣言書、リスク対応計画とISMS有効性評価表を作成します。リスクアセスメント結果報告書は、リスクアセスメントで作成したドキュメントにリスク対応と二次評価を記載します。

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（5/9）

1.適切な情報セキュリティリスク対応の選択肢の選定

リスク対応には、以下の4つがあります。

リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくしたりすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせたりすることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり、盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。

2.選択肢の実施に必要なすべての管理策の決定

リスク対応を実施することが決まった場合は、管理策を決める必要があります。管理策は、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な管理策をすべて決定します。

リスク対応における、リスクアセスメント結果報告書の作成方法（例）

リスク対応した結果を、リスクアセスメント結果報告書に記載します。

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	

具体的には、以下の内容を記載します。

✓ **保有、低減、回避、移転**
リスク対応で決定した対応について「●」を記載します。

✓ **管理策**
リスク対応で決定した内容を記載します。
（例）モバイル機器の利用ルールを整備・強化　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（6/9）

3.決定した管理策とISO/IEC 27001:2022附属書A の管理策との比較

附属書Aは、ISO/IEC 27001で記載されている要求事項をもとに情報セキュリティ上のリスクを低減するための目的と、その目的を達成するための管理策で構成されています。ISO/IEC 27001:2022では、合計93種の管理策が、以下の4つのカテゴリに分類されています。

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

リスク対応で決定した管理策を附属書Aと比較し、必要な管理策を見落としていないか確認します。附属書Aの管理策のリストは包括的なものではないので、必要に応じてリストにない管理策を採用してもかまいません。

（例）
リスクアセスメント結果報告書で記載の管理策：
- 情報の分類定義
- 分類ごとの情報の取扱いルール
- ラベリング

附属書Aに記載の管理策：
- 5.12 情報の分類
- 5.13 情報のラベル付け

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（7/9）

4.適用宣言書の作成

「適用宣言書」は、ISMS認証を取得するすべての組織に作成が義務づけられています。認証を取得しない組織では、 必須ではありませんが、情報セキュリティに対する取組を明確にするために「適用宣言書」を作成することが望ましいとされています。

適用宣言書は以下の内容を含むように作成します。

- 必要な管理策
- それらの管理策を含めた理由
- それらの管理策を実施しているか否か
- 附属書Aに規定する管理策を除外した理由

管理目的および管理策			適用	実施・未実施	管理策を含めた理由 管理策を除外した理由	規程・手順書
5 組織的管理策						
5.1	情報セキュリティのための方針群	情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューすることが望ましい。	○	○	情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するため	情報セキュリティ方針
5.2	情報セキュリティの役割および責任	情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てることが望ましい。	○	○	ISMSの構築・運用を円滑に行うため	情報セキュリティ手順書
5.3	職務の分離	相反する職務および責任範囲は、分離することが望ましい。	○	○	許可されていないもしくは意図しない変更または不正使用の危険性を低減するため	情報セキュリティ手順書
5.4	経営陣の責任	経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求することが望ましい。	○	○	ISMSの取組が、経営陣の経営戦略の一部であることを確実にするため	情報セキュリティ手順書
5.5	関係当局との連絡	組織は関係当局との連絡体制を確立および維持することが望ましい。	○	○	セキュリティインシデントが発生したことを迅速に報告するため	情報セキュリティ手順書
…	…	…	…	…	…	…

適用宣言書には、以下の内容を含めます。

✓ **管理目的および管理策**
ISO/IEC 27001の附属書Aの管理策を記載します。
（例）5.1 情報セキュリティのための方針群　など

✓ **適用**
適用または適用除外を記載します。
（例）○：適用、×：適用除外

✓ **実施・未実施**
実施したか否かを記載します。
（例）○：実施、未：未実施、ー：適用除外

✓ **管理策を含めた理由または管理策を除外した理由**
管理策を行う場合も理由を記載します。
（例）情報セキュリティのための経営層の方向性および支持を、事業上の要求事項、関連する法令および規則に従って規定するため　など

✓ **規程・手順書**
管理策が含まれている規程または手順書を記載します。
（例）情報セキュリティ手順書5.1.1、A-02 情報セキュリティ方針　など

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（8/9）

5.情報セキュリティリスク対応計画

「リスク対応計画」は、それぞれのリスクに対して、どのような管理策を、誰が、いつまでに、どのように実施するのかを表にまとめたものになります。表には、対策の実績やステータスを記載する欄もありますが、これらの欄については「8. 運用」で説明します。

リスク対応計画の作成方法（例）

リスクアセスメント結果報告書から、リスク対応を行う管理策をすべて記載し、それぞれの具体的な内容や、担当者などを記載します。リスク対応を行った場合、実績やリスク対応のステータスを記載する必要があります。
※実績とステータスは、「8.運用」で記載します。

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			
2	教育訓練	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			
3	• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	• 情報の分類定義 • 分類ごとの取扱いルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			

リスク対応計画では、以下の内容を記載します。

✓ **管理策**
リスクアセスメント結果報告書の管理策を記載します。
（例）モバイル機器の利用ルールを整備・強化　など

✓ **タスク**
管理策を実施する上で、具体的な業務を記載します。
（例）ルール検討
　　関係者に周知

✓ **担当**
管理策の担当者を記載します。
（例）委員長

✓ **予定**
リスク対応予定の開始日と終了日を記載します。
（例）開始：2023/08/10
　　終了：2023/09/29

13-2-4. ISMS：6. 計画

6.1 リスク及び機会に対処する活動（9/9）

二次評価

「二次評価」とは、リスクに対する管理策の有効性評価のために行うものです。
リスク対応を実施した結果は、二次評価としてリスクアセスメント結果報告書に記載します。リスク分析で使用した値を用いて、リスク対応を実施した結果をもとに、情報資産に対する再評価を実施します。

リスク対応における、リスクアセスメント結果報告書の作成方法（例）

優先順位	リスク対応						二次評価		
	保有	低減	回避	移転	管理策	対応	重要度	被害発生可能性	リスクレベル
2		●			モバイル機器の利用ルールを整備・強化	済	2	1	2
3		●			教育訓練	済	1	1	1
1		●			情報の分類定義 分類ごとの情報の取扱いルール ラベリング	済	2	3	6

具体的には、以下の内容を記載します。

- ✓ **重要度（係数）**
  「機密性」「完全性」「可用性」いずれかの最大値で判断します。
  （例）機密性：1、完全性：2、可用性：3 →　重要度：3
  　　機密性：2、完全性：1、可用性：1 →　重要度：2
- ✓ **被害発生可能性**
  脅威の起こりやすさと脆弱性のつけ込みやすさから換算表に当てはめて算出します。
  （例）起こりやすさ：2、つけ込みやすさ：1 → 被害発生可能性：1
  　　起こりやすさ：3、つけ込みやすさ：3 → 被害発生可能性：3
- ✓ **リスクレベル**
  重要度と被害発生可能性から算出します。
  （例）重要度：3、被害発生可能性：1 →　リスクレベル：3
  　　重要度：2、被害発生可能性：3 →　リスクレベル：6

6.リスク所有者による承認/7.残留している情報セキュリティリスクの受容

リスク対応計画と残留リスク（管理策の適用後に）は、リスク特定で決めたリスク所有者の承認が必要になります。リスク所有者が承認する際は、記録をする必要があるため、ワークフローやチェック欄などを用います。

（例）
承認プロセスとして、作成した書類にチェック欄（電子印欄など）を作成します。

作成者／更新者	【名前】	作成日／更新日	【日付】
承認者	【名前】	承認日	【日付】

作成	承認

13-2-4. ISMS：6. 計画

6.2 情報セキュリティ目的及びそれを達成するための計画策定

作成するドキュメント
- ISMS有効性評価表

情報セキュリティ目的の基本要件として以下の要件を満たす必要があります。

a. 情報セキュリティ方針と整合
b. 測定可能
c. 適用される情報セキュリティ要求事項、並びにリスクアセスメントおよびリスク対応の結果を考慮
d. 伝達すること
e. 必要に応じて、更新すること

情報セキュリティ目的と、それを達成するための計画をISMS有効性評価表に記載します。「8. 運用」で計画を実施し、「9. パフォーマンス評価」で評価を行います。評価結果の記載方法は、「9. パフォーマンス評価」で説明します。

ISMS有効性評価表の作成方法（例）

【計画】

情報セキュリティ目的：
・お客様との契約および法的または規制要求事項を尊重し遵守する
・情報セキュリティ事故を未然に防止する
・情報セキュリティ上の脅威から情報資産を保護する
・当社ISMSの意味を理解した活動の開始

評価指標：
ISMS教育受講／合格　100%(全従業者)
【備考】
取組の初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者がISMS教育を受講	ISMS事務局長	20XX年-月	受講者数および合格者数をカウントし、評価する

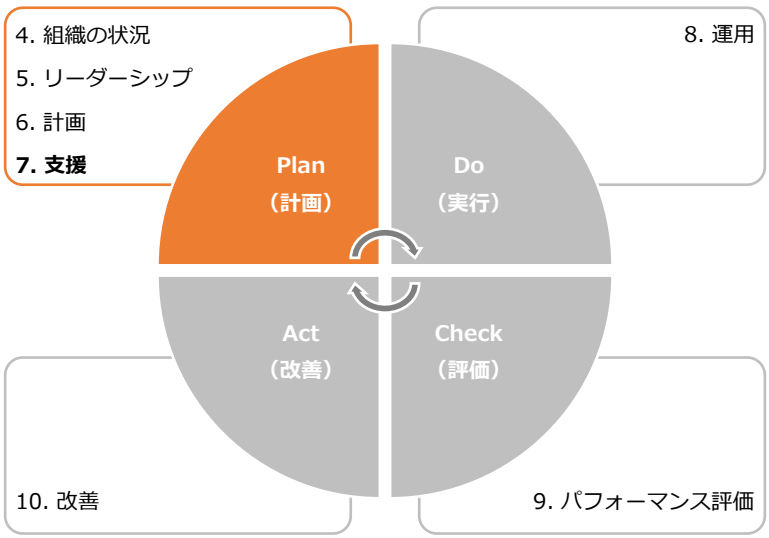
ISMS有効性評価表では、以下の内容を記載します。

- **情報セキュリティ目的**
  適用範囲（組織全体、各部署ごと）でのセキュリティ目的を記載します。
  （例）
  重大なセキュリティインシデントを発生させない、マルウェア感染およびサイバー攻撃によるシステム停止の防止　など
- **評価指標**
  測定可能な値を記載します。
  （例）マルウェアの感染の有無、システム停止の有無　など
- **実施事項**
  情報セキュリティ目的を達成するための実施内容を記載します。
  （例）ウイルス対策ソフトのインストール、標的型メール訓練の実施　など
- **必要な資源**
  実施事項のために必要な資源を記載します。
  （例）ウイルス対策ソフト、標的型メール訓練　など
- **責任者**
  計画の責任者を記載します。
  （例）部長各自　など
- **達成期限**
  計画の期限を記載します。
  （例）年度末、2023年9月　など
- **評価方法**
  具体的な評価方法を記載します。
  （例）年度末に発生したセキュリティインシデントをカウントし、評価する　など

13-2-5. ISMS：7. 支援

「7. 支援」は、PDCAサイクルの「Plan（計画）」に位置しており、ISMSの運用をサポートするための要求事項が規定されています。

7. 支援	作成ドキュメント（例）
7.1 資源 ISMSに必要な資源（人、物、金、情報）を決定し、提供します。	ー
7.2 力量 ISMS適用範囲の要員に求められる力量（知識、技能など）を定義し、要員が力量を備えているか評価を行います。力量評価の結果、力量が不足している場合は、力量を身につけるための教育を計画し、実施します。教育の実施後、力量を取得・維持できたか確認テストを行います。最後に、実施した教育内容を記録として保持します。	• 力量確認表 • 教育計画書 • 理解度確認テスト • 教育実施記録
7.3 認識 ISMS適用範囲のすべての要員に、以下の内容を認識させる必要があります。 ・情報セキュリティ方針 ・情報セキュリティパフォーマンスの向上によるメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策 ・ISMSによって割り当てられた責任を果たさなかった際の影響	ー
7.4 コミュニケーション ISMSを運用するにあたり、必要な意思疎通ができるプロセスを確立する必要があります。	ー
7.5 文書化した情報 ISMSに必要な文書化した情報の作成、更新、管理についての要求事項が記載されています。	**ー**



13-2-5. ISMS：7. 支援

7.1 資源

ISMSのPDCAサイクルを回すために必要な資源を決定し、利用できるようにする必要があります。必要な資源を決定し提供することは、トップマネジメントが行う必要があります。（リーダーシップ及びコミットメントの箇所で要求されています。）

ISMSのPDCAサイクルを回すために必要となる資源を決定し、提供する

資源の具体例を以下に示します。例を参考に、ISMSのPDCAサイクルを回すために自社で必要となる資源を決定し、利用可能にします。

資源	具体例
人	• ISMSを構築・運用するために必要となる要員 • ISMSの推進体制の確立 • 必要に応じた外部の専門家　など
物	• 情報を処理するための機器（サーバ、ネットワーク機器など） • コミュニケーション手段（パソコン、スマホなど） • 活動に必要な施設　など
金	• 人、物の資源を確保するための予算 • 要員の教育費用 • ISMSの維持費　など
情報	• 文書化した情報 • ISMSのPDCAサイクルを回すために有用な情報 • 情報セキュリティに関する最新情報　など

13-2-5. ISMS：7. 支援

7.2 力量（1/4）

作成するドキュメント
- 力量確認表
- 教育計画書
- 理解度確認テスト
- 教育実施記録

ISMS適用範囲の要員に必要な力量（知識、技能など）を明確にし、実際に要員が力量を備えているか評価を行います。力量が不足している場合、力量を身につけるための教育を計画し、実施する必要があります。教育の結果、力量が取得できたかを評価します。

力量確認表の作成方法（例）

要員の力量を評価し、確認するための力量確認表を作成する方法について説明します。

以下は、部門管理者の力量評価の例です。以下の手順で赤文字の箇所を自社の状況に合わせたものに修正することで、自社に適した力量確認表を作成できます。

1. 各要員ごとに、「組織の役割、責任及び権限」で割り当てられた役割や責任を果たすために必要となる力量を、「必要条件」として定義します。
2. 責任者として任命できるかどうか判断するための任命基準を定義します。
3. 定義された力量をどれほど備えているか、評価基準を決めて評価を行います。
4. 評価の結果、力量が不足している場合は教育・訓練を実施します。
5. 教育・訓練の実施後、どれほど改善できたか評価を行い、任命基準をもとに責任者として任命できるか判断します。

役　割	部門管理者
氏　名	○○ ○○

任命基準	A	B	C
区分	任命可	改善確認後任命可※	任命不可 再任命

A：項目のすべてが"3"以上。
B：項目の"2"以下について改善の予定がある。
C：項目の"2"以下について改善の予定がない。

※改善確認までは暫定的に任命し、改善確認後に正式任命とする

	必要条件	評価	改善予定日	改善内容	改善後評価	改善確認日
1	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
2	ISMSに関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
3	情報セキュリティ全般に関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
4	公正な判断ができること	5				

評価基準	内容
5	十分な力量がある。指導・教育ができる
4	力量がある。支援なしに対応ができる
3	力量がある。他の支援により対応ができる
2	改善の余地がある
1	改善が必要

13-2-5. ISMS：7. 支援

7.2 力量（2/4）

教育計画書の作成方法（例）

力量評価の結果をもとに、必要な力量を身につけるための教育を計画します。以下の例をもとに、教育計画書の作成方法を説明します。

教育目的	ISO27001認証取得のため
教育対象者	全従業者
教育方法	方法：eラーニングによる自己学習、確認テスト。 委員会より、受講対象者に受講案内のメールを送付。 受講者は、案内にあるURLからeラーニングのシステムにアクセスし、受講(テキストのダウンロード)／確認テストを行う。
教育内容	ISMSに対する意識向上 ・　当社の方針や手順について（情報セキュリティ基本方針など） ・　ISMSの有効性に対する自らの貢献 ・　ISMS要求に適合しないことの意味 ・　当社のルールの遵守
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
教育の有効性評価	情報セキュリティハンドブックを用いて教育を実施。 教育終了後、アンケート／確認テストを実施し記録に残す。 確認テストは、合格点は100点以上とする。 確認テストは、合格点に達するまで繰り返す。

教育計画書には、以下の内容を含めます。

✓ **教育目的**
教育を実施する目的を記載します。

✓ **教育対象者**
教育を受ける対象者を記載します。

✓ **教育方法**
教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、eラーニングなどさまざまあります。必要な力量を身につけるために適切と考えられる方法を選択します。

✓ **教育内容**
どのような教育を実施するのか、教育内容を記載します。

✓ **実施期間**
教育を実施する期間を記載します。

✓ **教育の有効性評価**
必要な力量を身につけることができたか評価する方法を記載します。
明確に評価が可能であれば、どのような方法でも問題ないです。たとえば、テストやアンケートの実施が挙げられます。次のページでテストの作成方法について説明します。

13-2-5. ISMS：7. 支援

7.2 力量（3/4）

理解度確認テストの作成方法（例）

教育の実施後、必要な力量を身につけることができたか評価するため、教育内容に関するテストを行うことが有効です。テストは、理解度が点数という数値で可視化されるため、評価がしやすく、多くの企業が実施しています。テストの作成例は以下の通りです。

次の【　　】に入る言葉として最も適したものを選びなさい（各10点）

設問			答え
①【　　】とは、ISMSを構築・運用するための国際規格である。			C
A. ISO9001	B.ISO14001	C.ISO27001	
② 情報セキュリティという言葉は、一般的に、情報の【　　】、完全性、可用性を維持改善することと定義されている。			C
A. 信頼性	B.整合性	C.機密性	
③ 2023年度の当社の情報セキュリティ目標は、【　　】である。			A
A.ISMS教育受講／合格　100%(全従業者)	B.予防処置の発行件数を四半期に1件以上	C.セキュリティインシデント発生件数／2件以内	
④【　　】とは、企業や個人の情報を盗みとるため、特定の相手（企業組織や社員）をメールなどの手段で狙う攻撃のことです。			A
A. 標的型攻撃	B. ウイルス型攻撃	C. サイバー攻撃	
⑤ ④【　　】メールの特徴はどれか。			B
A. 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。	B. 件名や本文に、組織の担当者の業務に関係する内容が記述されている。	C. 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。	

次の文章のうち正しいものには○、間違っているものには×をつけなさい（各10点）

設問	答え
⑥ ISMSでは、情報資産とは、書類、データだけでなく、ハードウェア、ソフトウェア、設備、ファームウェア（媒体など）、要員までも包括する。	○
⑦ 私物の外部記録媒体(USBメモリ、外づけHDDなど)の使用は原則禁止である。	○
⑧ 当社が重大な損失もしくは不利益を受けるような恐れのある機密情報を社外へ持ち出す場合は、責任者の許可を得て、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。	○
⑨ PCのログインパスワードは英数混合8文字以上のパスワードとする。	○
⑩ PCのパスワードつきスクリーンセーバの設定時間は、15分以内とする。	×

実施日：	
所属：	
氏名：	
点数：	点/100点

✓ テストは、選択問題や正誤形式にすることで採点がしやすくなります。
✓ 教育内容に合った問題を考え、作成します。たとえば、今回の教育内容に「当社のルールの遵守」が含まれているため、⑥～⑩のような設問を作成します。

13-2-5. ISMS：7. 支援

7.2 力量（4/4）

教育実施記録の作成方法（例）

教育を実施した際、実施記録を文書化する必要があります。以下の例をもとに、教育実施記録の作成方法を説明します。

教育の名称	ISMS教育（基本方針、目標、ルール）
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
実施方法	eラーニング
使用テキスト	情報セキュリティハンドブック
教育の概要	情報セキュリティハンドブックなどによるISMSに対する意識向上 ・当社の方針や手順について（情報セキュリティ基本方針など） ・ISMSの有効性に対する自らの貢献 ・ISMS要求に適合しないことの意味 ・当社のルールの遵守 学習後にテスト実施
受講対象者・部門	上記教育実施期間において在籍する全従業者
参加者	別紙：「教育受講者一覧」を参照
備考	特になし

教育実施記録には、以下のような内容を含めます。

✓ **教育の名称**
どのような教育を実施したのか、教育テーマを記載します。

✓ **実施期間**
教育を実施する期間を記載します。

✓ **教育方法**
教育・訓練方法は、集合研修や、職場訓練（OJT）、資格試験の受験、eラーニングなどさまざまあります。その中で、実際に実施した方法を記載します。

✓ **教育の概要**
実施した教育の概要や、教育を実施した目的を記載します。

✓ **受講対象者・部門**
教育を受講する対象者を記載します。

✓ **参加者**
教育を実際に受講した者を記載します。以下の例のように、「教育の受講者一覧」を別紙で作成し、実施記録と分けて記載すると分かりやすくなります。

No	所属	氏　　名	受講日
1	営業	○○○○	20XX/-/-
2	管理	○○○○	20XX/-/-

13-2-5. ISMS：7. 支援

7.3 認識

ISMS適用範囲で働くすべての社員、従業員が情報セキュリティ方針を理解し、それを実現することの重要性を認識する必要があります。逆に、セキュリティ対策を実施せず、セキュリティ方針を実現できなかった場合、どのようなことが起きるのかについて理解する必要もあります。

具体的には、以下の内容について教育を行い、ISMSの重要性を十分理解させる必要があります。

- **情報セキュリティ方針**
- **情報セキュリティパフォーマンスの向上によるメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策の具体的な内容**
- **ISMSによって割り当てられた責任を果たさなかった場合の組織に与える影響**

これらの内容について認識を持たせるために、教育や訓練を実施します。
具体的な教育・訓練の実施手順は、「力量」や「コミュニケーション」で説明します。

力量

上記の内容について、各要員が認識しているか評価を行い、認識が不十分の場合は教育を実施し、認識させます。

コミュニケーション

情報提供・共有によって、上記の内容の認識を深めるようにします。

13-2-5. ISMS：7. 支援

7.4 コミュニケーション

ISMSのPDCAサイクルを回すためには、内部および外部とのコミュニケーションを円滑に行う必要があります。そのため、組織内および組織外の関係者とコミュニケーションをとる手順などを定め、必要なときに円滑なコミュニケーションが行える体制を整えておくことが重要です。コミュニケーションの手順などには、以下の内容が含まれます。

- コミュニケーションの内容
- コミュニケーションの実施時期
- コミュニケーションの対象者
- コミュニケーションの方法

ISMSに関連するコミュニケーションをとる手順を確立した例を、以下に示します。例を参考に、自社のISMSのPDCAサイクルを回す上で必要なコミュニケーションをとる手順を確立します。

内容	実施時期	対象者	実施者	方法
情報セキュリティ方針の伝達	随時	利害関係者	トップマネジメント（ISMS事務局）	外部 ・当社HPに公表 内部 ・ISMS定期教育にて ・当社HPに公表 ・社内掲示
各見直し結果の伝達	見直後、1週間以内	従業者	ISMS事務局	承認後、ISMS事務局より通達
セキュリティ調査結果の報告	依頼入手時	お客様	ISMS事務局	・お客様より調査票などを入手した場合、主管部門にて回答を作成 ・ISMS事務局責任者が確認の上、お客様に提出
セキュリティインシデントの伝達	発見時	ISMS事務局	発見者	「情報セキュリティ手順書：セキュリティインシデント対応フロー」の通り
	適時	トップマネジメント	ISMS事務局	同上
	適時	関係当局	ISMS事務局	同上

✓ **内容**：コミュニケーションで伝える情報

✓ **実施時期**：伝えるタイミング

✓ **対象者**：誰に伝えるのか、情報を伝える対象者

✓ **実施者**：誰が伝えるのか、情報を対象者に伝える者

✓ **方法**：情報を伝える手段

13-2-5. ISMS：7. 支援

7.5 文書化した情報

ISMSに必要な文書化した情報の作成、更新、管理方法を決めます。

一般

以下の情報をISMSに含める必要があります。

- ISO/IEC 27001が要求する文書化した情報
- ISMSの有効性のために必要であると組織が判断した文書化した情報

以下は、ISO/IEC 27001が要求する文書化した情報の一覧です。

文書化した情報	作成する項番
ISMSの適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	
力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMSのプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメントレビューの結果	
不適合の内容と処置、処置の結果	「10. 改善」で作成

作成および更新

ISMSに必要な文書化した情報を作成・更新する際に、以下の事項を確実にする必要があります。

1. 適切な識別と記述

文書化した情報を識別できるよう、以下の例のように採番方法を決めたり、各文書には適切なタイトル、作成者、承認者、日付などを記載したりします。

文書の種類	採番方法
基本文書	A-□□（01から採番を始める）
ISMSマニュアル	B-01
手順書	C-01
記録類	D-01
外部文書	採番せずに文書名、作成社名などの名称にて識別する

2. 適切な形式

文書化する情報を記載する媒体として、紙や電子データなどを指定し、適切な形式（文字、図表など）を用いて読みやすく、簡潔に記載します。

3. 適切なレビューと承認

文書化した情報は、適切な承認とレビューを行い策定します。

文書化した情報の管理

ISMSの文書化した情報を管理する必要があります。

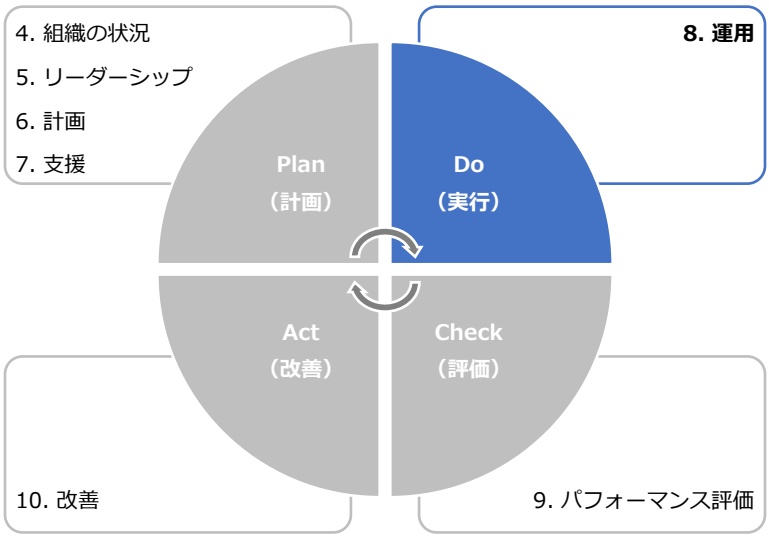
（管理方法の例）

- 文書化した情報は、ISMS事務局責任者が、最新版を紙の媒体としてファイリングし、キャビネットにて保管し、適用範囲内の対象者が必要なときに、必要なところで利用可能にする

13-2-6. ISMS：8. 運用

「8. 運用」は、PDCAサイクルの「Do（実行）」に位置しており、「6. 計画」で計画した活動や、要求事項を満たすための活動を実施し、管理します。そして、計画通りに実施した証拠となる情報を文書化し、保持する必要があります。

8. 運用	作成ドキュメント（例）
8.1 運用の計画及び管理 「6. 計画」で計画した活動や、要求事項を満たすための活動の実施状況を管理するための一覧表を作成します。	• ISMS年間計画表
8.2 情報セキュリティリスクアセスメント 「6. 計画」で定めたリスクアセスメントのプロセスを実施し、結果を文書化します。	• リスクアセスメント結果報告書
8.3 情報セキュリティリスク対応 「6. 計画」で定めたリスク対応計画を実施し、結果を文書化します。	• リスク対応計画



13-2-6. ISMS：8. 運用

8.1 運用の計画及び管理

作成するドキュメント
- ISMS年間計画表

「6. 計画で決定した活動」および「要求事項を満たすための活動」を実施するにあたり必要なプロセスを計画し、ISMS年間計画表を作成します。　ISMS年間計画表は、「6. 計画で決定した活動」および「要求事項を満たすための活動」の実施状況を管理するための計画表のことです。

ISMS年間計画表の作成方法

以下の例は、「6. 計画」で決定した活動に関する計画表の例です。

No	実施事項		文書名	スケジュール							
				2023年5月				2023年6月			
				8	15	22	29	5	12	19	26
6.1	「リスク及び機会に対処する活動」の検討	外部および内部の課題に対する活動の検討	外部および内部の課題								
		リスクアセスメントの実施	資産目録								
			リスクアセスメント結果報告書								
		リスク対応のための計画作成	適用宣言書								
		（アクションプランの作成）	リスク対応計画								
		管理策(ルール)の検討	情報セキュリティ手順書								
6.2	部門ごとに「情報セキュリティ目的及びそれを達成するための計画」を作成		ISMS有効性評価表								

- ✓ **No**：ISO/IEC 27001の要求事項の項番を記載します。
- ✓ **実施事項**：行う活動の内容を記載します。
- ✓ **文書名**：実施事項で記載した活動を行う際に利用したり、作成したりする文書名を記載します。
- ✓ **スケジュール**：実施事項を行う予定日を記載します。

13-2-6. ISMS：8. 運用

ISMSの要求事項全体を示した計画表の例を紹介します。
前記の計画表は、ISMSの要求事項のうち「6.計画」の箇所だけを抜粋し、作成が必要な文書や、細かいスケジュールを示すことに焦点を当てたものですが、次の計画表は年間を通して実践すべき事項を記載したものとなっています。

<table>
<tr><th rowspan="2">期間</th><th rowspan="2">月</th><th colspan="4">実施事項</th></tr>
<tr><th>年に1回</th><th>月に1回</th><th>四半期に1回</th><th>随時</th></tr>
<tr><td rowspan="3">第1四半期</td><td>4月</td><td>・課題に対する活動の検討</td><td>・入退記録の確認
・運用チェックリストによる確認
・バックアップされていることの確認
・イベントログの確認
利用者が利用可能なソフトウェアの確認</td><td rowspan="3">・バックアップされていることの確認
・イベントログのチェック</td><td rowspan="12">・「関係当局との連絡」体制の見直し
・法令規制一覧表の確認</td></tr>
<tr><td>5月</td><td>・リスクアセスメントの実施</td><td>同上</td></tr>
<tr><td>6月</td><td>・リスク対応のための計画作成（アクションプランの作成）
・管理策（ルール）の検討</td><td>同上</td></tr>
<tr><td rowspan="3">第2四半期</td><td>7月</td><td>・「情報セキュリティリスク対応」計画の実行</td><td>同上</td><td rowspan="3">同上</td></tr>
<tr><td>8月</td><td>・ISMSの有効性の評価
・情報セキュリティパフォーマンス</td><td>同上</td></tr>
<tr><td>9月</td><td>・資産目録の見直し
・情報の分類
・アクセス権限の見直し</td><td>同上</td></tr>
<tr><td rowspan="3">第3四半期</td><td>10月</td><td>・システム開発の外部委託先の再審査</td><td>同上</td><td rowspan="3">同上</td></tr>
<tr><td>11月</td><td>・情報セキュリティ計画
・情報セキュリティ継続の検証・レビュー</td><td>同上</td></tr>
<tr><td>12月</td><td>・内部監査計画
・内部監査の実施
・マネジメントレビュー
・不適合及び是正処置のレビュー</td><td>同上</td></tr>
<tr><td rowspan="3">第4四半期</td><td>1月</td><td>・主要メンバーの「力量」の評価・証拠の文書化
・定期教育
・UPSのバッテリーの確認</td><td>同上</td><td rowspan="3">同上</td></tr>
<tr><td>2月</td><td>・外部審査（審査機関による更新審査）の実施</td><td>同上</td></tr>
<tr><td>3月</td><td>・情報セキュリティのための方針群のレビュー
・秘密保持契約書の確認</td><td>同上</td></tr>
</table>

13-2-6. ISMS：8. 運用

8.2 情報セキュリティリスクアセスメント

追記するドキュメント
- リスクアセスメント結果報告書

リスクアセスメントを実施する際は、結果を「リスクアセスメント結果報告書」に追記します。

リスクアセスメント結果報告書の追記方法

リスクアセスメント結果報告書の「対応」の箇所に記載します。

✓ **対応**：管理策の実施状況を記載します。
- ・管理策を実施した場合は「済み」
- ・管理策を実施する予定がある場合は「予定」
- ・管理策を実施する予定が未定の場合は「未定」

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	済み
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	予定
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	未定

8.3 情報セキュリティリスク対応

追記するドキュメント
- リスク対応計画

リスク対応を実施する際は、結果を「リスク対応計画」に追記します。

リスク対応計画の追記方法

リスク対応計画の「実績」、「ステータス」の箇所に記載します。

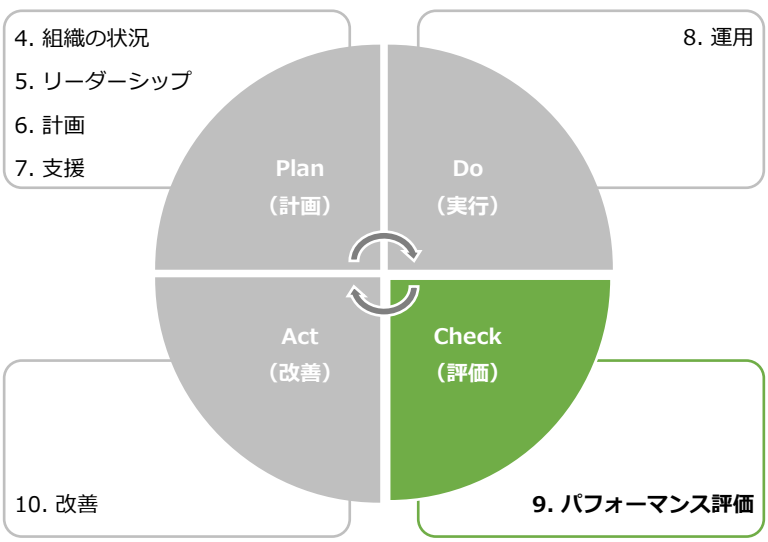
✓ **実績の開始の箇所**：実際にタスクを開始した日付を記載します。
✓ **実績の終了の箇所**：実際にタスクが完了した日付を記載します。
✓ **ステータスの箇所**：タスクの進捗状況を記載します。
- ・タスクが完了した場合は「終了」
- ・タスクを実行中の場合は「着手」
- ・タスクに着手していない場合は「未着手」

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
2	教育訓練	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-		着手
3	• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	• 情報の分類定義 • 分類ごとの取扱いルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-			未着手

13-2-7. ISMS：9. パフォーマンス評価

「9. パフォーマンス評価」は、PDCAサイクルの「Check（評価）」に位置しており、定めた情報セキュリティ目標を達成するための取組（構築したISMS）が有効であるかどうかを評価します。

パフォーマンス評価	作成ドキュメント（例）
9.1 監視、測定、分析及び評価 情報セキュリティのパフォーマンスと、ISMSの有効性を評価します。	• ISMS有効性評価表
9.2 内部監査 ISMSの適合性、有効性について、あらかじめ定めた間隔で監査を実施します。	• 内部監査チェックリスト • 内部監査計画書 • 内部監査結果報告書
9.3 マネジメントレビュー トップマネジメントが、ISMSの有効性を評価します。	• マネジメントレビュー報告書



13-2-7. ISMS：9. パフォーマンス評価

9.1 監視、測定、分析及び評価

作成するドキュメント
- ISMS有効性評価表

ISMSの効果について判断するために、有効性評価を実施します。ISMSに沿って実施している活動が、情報セキュリティ目標の達成に繋がっているのか、有効に作用しているのかを評価し、課題があるのであれば改善することになります。　前項で説明した通り、PDCAサイクルによる継続したスパイラルアップによって、改善し続けることが重要です。計画時に定めた評価指標および評価方法により、ISMSが有効だったか、そうではなかったかを判断します。この有効性の評価は、マネジメントレビューの際にトップマネジメントが実施するのが効果的です。

【計画】
情報セキュリティ目的：・お客様との契約および法的または規制要求事項を尊重し遵守する
・情報セキュリティ事故を未然に防止する
・情報セキュリティ上の脅威から情報資産を保護する
・当社ISMSの意味を理解した活動の開始

評価指標：　ISMS教育受講／合格　100%(全従業者)
【備考】
取組の初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者がISMS教育を受講	ISMS事務局長	20XX年00月	受講者数および合格者数をカウントし、評価する

【評価】　**評価日：【20XX/00/00】**

情報セキュリティ目的達成に関する評価結果　**凡例　○：有効　×：有効ではない**

結果	備考
○	全従業員eラーニングでのテストを100点にて合格。有効性があるものと判断する。

✓ 情報セキュリティ目的達成のための計画には、計画時に定める実施事項、必要な資源、責任者、達成期限、評価方法を記載します。
※【計画】の詳しい記載方法については、「6. 計画」で説明しています。

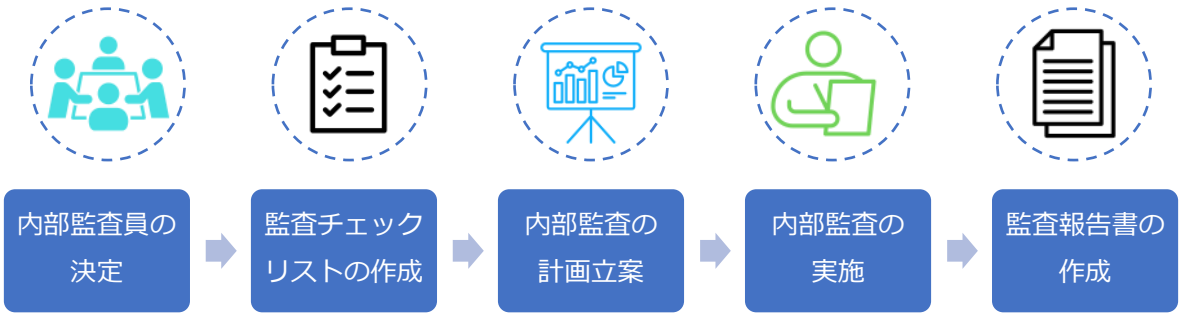
✓ 情報セキュリティ目的達成に関する評価結果には、ISMSが有効だったか否かという結果を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（1/4）

作成するドキュメント
- 内部監査チェックリスト
- 内部監査計画書
- 内部監査結果報告書

内部監査とは、社内のルールや扱っている文書がISO/IEC 27001の要求事項を満たしており、従業員などがそのルールを守って仕事をしているかどうかをチェックすることです。内部監査結果報告書をもとに、マネジメントレビューで「自社のISMSはこのままでいいのか」「自社のISMSのどこに欠陥があり、どう修復しなくてはならないのか」を経営層が判断し、随時対策をとります。内部監査は一般的に以下のプロセスで進めます。



13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（2/4）

1. 内部監査員の選定

内部監査とは、組織内部において、専門的知識を持った人が、経営者や役員などの立場にない第三者として、ISMSが適切に構築され、適正に運用されているかどうかを評価することです。内部監査員には、監査の公正さや客観性の観点から、監査対象となる部門に所属していない者を任命する必要があります。内部監査員に資格などは不要ですが、下記に当てはまるような人が適任です。社内に適した者がいない場合は、研修により内部監査員を育成したり、外部の専門家へ依頼したりするといった手段をとることが有効です。

・ISMSの内容を理解している人
・ISMSの内部監査の体制や実施方法といった手順に関する知識を有している人
・自社のISMSを把握している人
・監査対象となる部署の業務内容を把握している人

2. 内部監査チェックリストの作成

内部監査員がチェックリストを作成します。事前にチェックリストを作成することで、監査するべき範囲やポイントが明確になったり、チェック漏れを減らせたり、内部監査員ごとの偏った評価を防止したりといった効果が期待できます。また、チェックリストは内部監査を行った文書記録とすることができます。

内部監査チェックリストの作成方法（例）

ISMSの項目に沿ってチェック事項をまとめ、内部監査を実施の際には確認したISMSの根拠となる確認結果や文書類を記録します。

監査項目	チェック事項	確認結果・文書類
4. 組織の状況		
4.1 組織及びその状況の理解	組織は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部および内部の課題を決定しているか。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解	次の事項を決定したか。 a) ISMSに関連する利害関係者 b) その利害関係者の、情報セキュリティに関連する要求事項	• 外部および内部の課題
4.3 情報セキュリティマネジメントシステムの適用範囲の決定	ISMSの適用範囲は、文書化されているか。	• ISMSマニュアル • ISMS適用範囲 • レイアウト図 • ネットワーク図
5. リーダーシップ		
5.1 リーダージップ及びコミットメント	トップマネジメントは、 a） 情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしているか。	• 情報セキュリティ方針 • 質問で確認
5.2 方針	情報セキュリティ方針は、 e) 文書化した情報として利用可能であるか。	• 情報セキュリティ方針

事前に作成する部分　　**監査時に記載する部分**

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（3/4）

3. 内部監査の計画立案

内部監査の計画を立てます。いつ、誰が、どの部門の誰に、何についてチェックするか、といったことを事前に段取りしておきます。

内部監査計画書の作成方法（例）

監査概要	
監査名称	ISO27001認証取得に関する内部監査
監査目的	ISO/IEC27001:2022認証取得に向けた当社ISMSの整備、運用状況を確認
監査テーマ	・管理策の運用状況、および有効性の確認 ・第一段階審査の指摘に対する改善状況の確認
監査方法	被監査部門に対するヒアリング、文書化された情報の閲覧、およびオフィスの視察
監査基準	JISQ27001:2022（ISO/IEC27001:2022)の要求事項、当社ISMSマニュアル、および情報セキュリティ手順書

詳細監査計画				
No	被監査部門名	監査人	応対者	日時
1	情報システム部	○○　○○	△△　△△	20XX/-/- 00:00
2	管理部	○○　○○	△△　△△	20XX/-/- 00:00
3	営業部	○○　○○	△△　△△	20XX/-/- 00:00
4	総務部	○○　○○	△△　△△	20XX/-/- 00:00

内部監査結果報告（予定）	
報告予定日	20XX年〇月
報告手段	報告会の開催

✓ **監査概要**：監査の名称、目的、テーマ、方法、基準を記載します。

✓ **詳細監査計画**：監査の対象となる部門名、監査人名、監査への対応者名、監査実施の日時といった予定を記載します。

✓ **内部監査結果報告（予定）**：監査結果の報告予定日と報告手段を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.2 内部監査（4/4）

4. 内部監査の実施

内部監査計画に沿って、内部監査チェックリストを用いて監査を実施します。

5. 内部監査結果報告書の作成

内部監査の結果をとりまとめ、報告書を作成します。どの部署で、どのルールが守られなかったかといったことを明確にしておきます。　内部監査結果報告書をもとに、経営層は自社のISMSをどのようにするか判断することになるため、内容に不明瞭な点や不足があると、適切な見直しができなくなってしまうため、注意が必要です。

内部監査結果報告書の作成方法（例）

<table>
<tr><td>監査名称</td><td colspan="3">ISO27001認証取得に関する内部監査</td></tr>
<tr><td>監査実施日時</td><td colspan="3">20XX年-月</td></tr>
<tr><td>監査目的</td><td colspan="3">ISO/IEC27001:2022認証取得に向けた当社ISMSの整備状況を確認</td></tr>
<tr><td colspan="4">監査体制</td></tr>
<tr><td>被監査部門①</td><td>情報システム部</td><td>監査人①</td><td>【名前】/【社名】</td></tr>
<tr><td>被監査部門②</td><td>管理部</td><td>監査人②</td><td></td></tr>
<tr><td>被監査部門③</td><td>営業部</td><td>監査人③</td><td></td></tr>
<tr><td>被監査部門④</td><td>総務部</td><td>監査人④</td><td></td></tr>
<tr><td>監査総評</td><td colspan="3">
ISMSの整備状況を確認
当組織でのISMSは、ISO27001:2022規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されなかった。全体として適切な有効な仕組みにより運用を開始したと判断できる。
また社員の周知に関しては、ISMS教育の実施などにより体制や方針などの周知を行っていた。

不適合・観察事項
一部ではあるが、対応が十分でない事項があったため○件を軽微な不適合、○件を観察事項とした。重大な不適合は、検出されなかった。

【軽微な不適合】
<table>
<tr><th>No</th><th>規格</th><th>内容</th></tr>
<tr><td>1</td><td>5.2 方針</td><td>規格では「情報セキュリティ方針は、次の事項を満たさなければならない。g) 必要に応じて、利害関係者が入手可能である。」としている。しかし、「情報セキュリティ方針」について、お客様などの利害関係者が入手可能であることを確認できなかった。</td></tr>
</table>
【観察事項】
<table>
<tr><th>No</th><th>規格</th><th>内容</th></tr>
<tr><td>1</td><td>4.3 情報セキュリティマネジメントシステムの適用範囲の決定</td><td>ISMSマニュアルとネットワーク図で適用範囲の表現が同じであることの確認が難しい状況でした。ISMSマニュアルでは、ルータまで。ネットワーク図では、ONUまで。</td></tr>
<tr><td>2</td><td>7.3 認識</td><td>実施中のISMS教育の終了をお願いします。</td></tr>
</table>
</td></tr>
<tr><td>備考
（フォローアップなど）</td><td colspan="3">次回の内部監査にて対応のフォローを行う</td></tr>
</table>

13-2-7. ISMS：9. パフォーマンス評価

9.3 マネジメントレビュー（1/2）

作成するドキュメント
- マネジメントレビュー報告書

マネジメントレビューとは、経営者（トップマネジメント）が行うレビュー活動です。トップマネジメントは、内部監査の結果や利害関係者からのフィードバックをもとに、組織のISMSが適切に運用されているかどうかを判断し、必要に応じて改善方法を指示します。この活動は、少なくとも年に1回定期的に実施することが求められています。トップマネジメントに報告した内容（インプット）と、トップマネジメントの指示や提案（アウトプット）を文書化したものが、マネジメントレビュー報告書です。

インプット、アウトプットに含める必要がある内容は以下の通りです。

インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMSに関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMSに関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 • 不適合および是正処置 不適合に対する是正処置の実施状況を報告します。 • 監視および測定の結果 情報セキュリティパフォーマンスや、ISMSの有効性についての監視、測定結果を報告します。 • 監査結果 内部監査の結果を報告します。 • 情報セキュリティ目的の達成 情報セキュリティ目的の達成数や未達成数など、情報セキュリティ目的の達成状況を報告します。
5. 利害関係者からのフィードバック 利害関係者から、情報セキュリティに関する要望などについて、対応した結果を報告します。
6. リスクアセスメントの結果およびリスク対応計画の状況 リスクアセスメントにより、新しく特定したリスクや、リスク対応計画の進捗状況を報告します。
7. 継続的改善の機会 トップマネジメントに改善策を提案します。
アウトプットに含める必要がある事項
1. 継続的改善の機会 改善すべき内容について指示を記載します。
2. ISMSのあらゆる変更の必要性 ISMSに関して、次年度以降変更すべき内容について指示を記載します。

13-2-7. ISMS：9. パフォーマンス評価

9.3 マネジメントレビュー（2/2）

マネジメントレビュー報告書の作成方法（例）

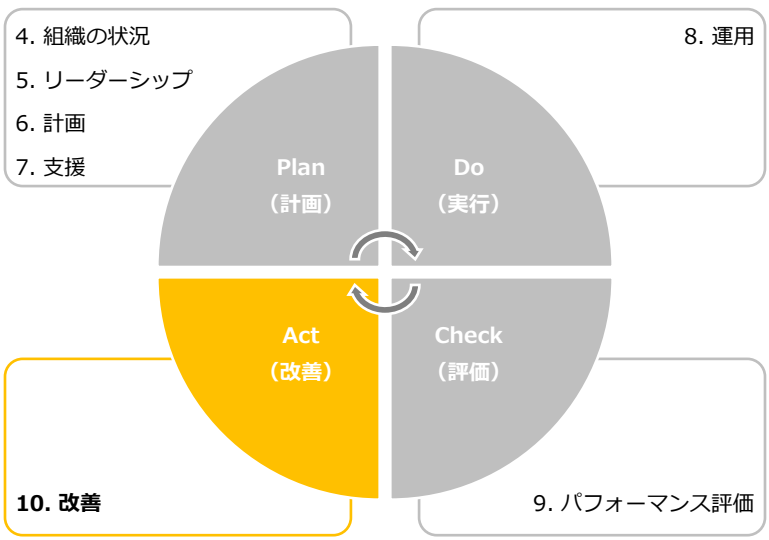
出席者	トップマネジメント	【名前】	日時	20XX年〇月	
	情報セキュリティ委員長	【名前】		00：00　～　00：00	
	ISMS内部監査責任者	【名前】			

インプット（報告事項）			
1	前回までの指示事項に対する処置の進捗や結果	初回マネジメントレビューのためありません。	
2	ISMSに関連する外部および内部の課題の変化	「外部および内部の課題」にて報告の通りです。 その後、課題の変化は発生しておりません。	
3	ISMSに関連する利害関係者のニーズおよび期待の変化	お客様からの情報セキュリティに関する要求の変化はありませんでした。	
4	情報セキュリティパフォーマンスの実績報告	1）不適合および是正処置	20XX年〇月に実施した初回の内部監査で検出された“観察事項”1件は、是正対応中です。 今月末までに対応を予定しています。 そのほか現在対応中の不適合はありません。
		2）監視および測定の結果	次回のマネジメントレビューにて測定結果を報告します。
		3）監査結果	【内部監査】 20XX年〇月に1回目の内部監査を実施し、主にISMSの文書類整備状況の確認を行いました。 ①ISO27001規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されませんでした。全体として適切な仕組みにより運用を開始したと判断します。 ②一部ではありますが、対応が十分でない事項があり、観察事項1件が検出されました。 詳細は、「内部監査結果報告書」(20XX年〇月)にて報告の通りです。
		4）情報セキュリティ目的の達成	次回のマネジメントレビューにて報告します。
5	利害関係者からのフィードバック	お客様からのクレームは現状ありませんでした。	
6	リスクアセスメントの結果およびリスク対応計画の状況	【リスクアセスメントの状況】 「情報リスクアセスメント結果報告書」(20XX年〇〇月〇〇日)にて報告の通りです。 【リスク対応計画の状況】 ・リスク対応計画にリストアップした管理策：〇件 ・対応が終了した管理策：〇件 ・対応が終了していない管理策2件は以下の通りです。 対応：予定 サービス供給者の管路：今月下旬 情報セキュリティ継続：今月下旬 ※詳細は、「リスク対応計画」(作成：20XX年〇〇月〇〇日、見直：20XX年〇月)にて報告の通りです。	
7	継続的改善の機会	現状はISMSを従業者が理解するための活動を主として行っています。	
アウトプット（トップマネジメントの指示事項）			
1	継続的改善の機会	現状認識している各課題を確実に実施すること。	
2	ISMSのあらゆる変更の必要性	コンサルタント会社のひな形にとらわれず、より当社の状況を反映した仕組み・ルールに見直しを行っていくこと。	

13-2-8. ISMS：10. 改善

「10. 改善」は、PDCAサイクルの「Act（改善）」に位置しており、ISMSの改善を行います。

10. 改善	作成ドキュメント（例）
10.1 継続的改善 ISMSのPDCAサイクル（「4. 組織の状況」から「10. 改善」までの活動）を継続して実施し、情報セキュリティパフォーマンスを向上させるために必要となる改善を行っていきます。具体的には、情報セキュリティ方針や情報セキュリティ目的の計画、リスクアセスメントやリスク対応をもとに決定した管理策の実施を継続して行い、改善していきます。	―
10.2 不適合及び是正処置 不適合が発生した際に是正処置を実施します。不適合とは、ISMSの要求事項を満たしていないことです。具体的には、管理策の不備や未実施、セキュリティインシデントの発生などのことです。	• 是正要求書兼回答書

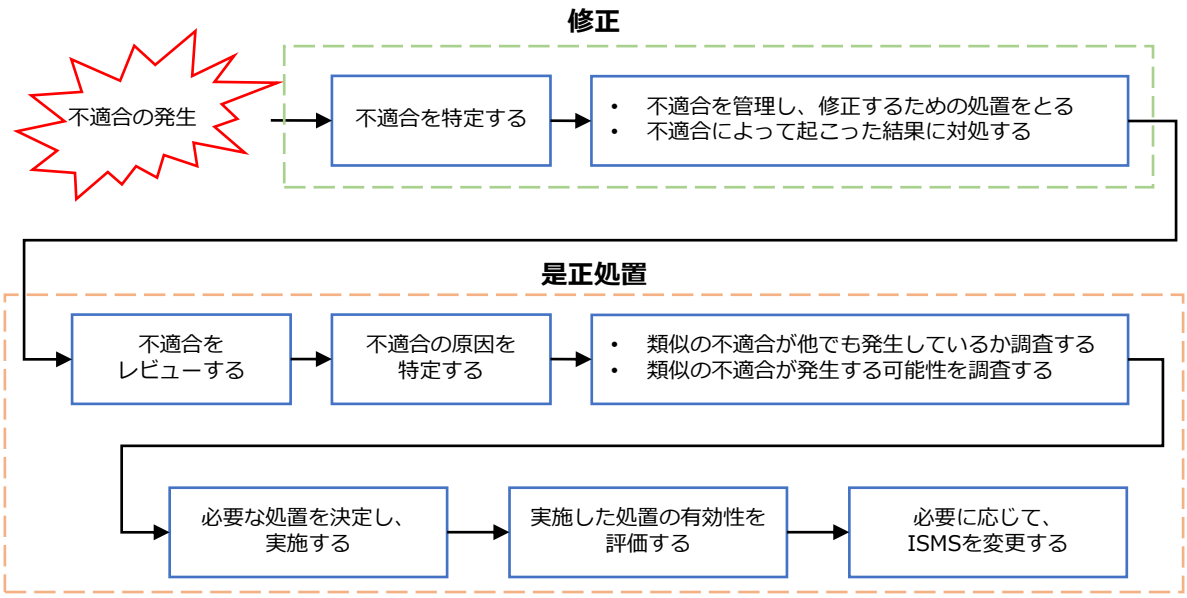


13-2-8. ISMS：10. 改善

10.2 不適合及び是正処置（1/2）

作成するドキュメント
- 是正要求書兼回答書

審査でISMSに不適合が検出された場合は、是正処置をしなければなりません。是正処置とは、不適合について、その原因を取り除き、再発防止を図る処置を指します。是正処置は以下の図のようなプロセスで実施されます。



「不適合の性質および講じた処置」と「是正処置の結果」について、文書化した情報を残さなければなりません。そのため、内部監査で不適合が出た際は、是正要求書とその回答書を記載して保存することになります。

13-2-8. ISMS：10. 改善

10.2 不適合及び是正処置（2/2）

是正要求書兼回答書の作成方法（例）

前ページで説明した「不適合の性質および講じた処置」と「是正処置の結果」についての内容を記載します。

整理番号	00-00	対象部門	○○○○部門	発効日	20XX 年 - 月 - 日

入力情報	分類	監査	■	内部監査における指摘事項											
			□	外部機関が実施した監査における指摘事項　(機関名：　　)											
			監査年月日		年		月		日	監査者					
			指摘のランク	観察事項						要求事項項番	7.2 力量				
		監査以外	□	セキュリティインシデントの関連した改善事項											
			□	外部の利害関係者からのニーズに基づく改善事項											
			□	内部において提案された改善事項											
			□	その他（　　）											
	内容	一部情報セキュリティ委員会担当者が仮任命のため、今後本任命を行っていく。												承認	作成
処置計画	修正	力量の確認。任命力量確認表の更新。													
		実施予定日		年		月		日							
	評価	類似の不適合の有無		無	発生する可能性	無									
		原因	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。												
		原因を除去するための計画の必要性		有	※有の場合原因除去の計画を記載										
	原因除去	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。												承認	作成
		実施予定日		年		月		日							
実施報告	内容	上記の通り、「ISMS年間計画書」を修正し、運用チェックリストによる点検を実施した。												承認	作成
		実施完了日		年		月		日							
処置確認	確認	「ISMS年間計画表」の修正、運用チェックリストによる点検記録を確認した。												承認	作成
		確認日		年		月		日							
	有効性	セキュリティ手順の実行、および技術的遵守について、点検漏れのリスクが低減された。													
		評価日		年		月		日	フォロー監査の要・不要						

コラム

ISMSの導入：成功の鍵とよくある落とし穴

組織が顧客データや機密情報などの情報資産を守るためには、適切に情報セキュリティを確保する仕組みが必要となります。そのために、ISMSの導入と運用は重要になります。そこで、ISMSを導入・運用していく際に成功の鍵となるポイントと、陥りやすい失敗例をいくつか紹介します。

成功の鍵となるポイント

■ トップマネジメントのコミットメント
ISMSの導入には経営陣からのコミットメントが不可欠です。経営層が情報セキュリティの重要性を理解し、リーダーシップを発揮することで、組織全体が情報セキュリティの確保に向けて協力的になります。

■ 従業員の教育と意識向上
従業員への教育は、従業員に基本方針や対策基準などを理解させ、策定された実施手順を実践してもらうために重要です。定期的なトレーニングや教育プログラムを通じて、従業員が脅威に対処できるようにサポートしていくことが大切です。

■ リスク評価と適切な対応策
リスク評価を行い、特定のリスクに対して適切な対応策を策定することで、情報資産の保護と事業の継続性を確保できます。

陥りやすい失敗例

■ 実施手順の抽象性
実施手順が抽象的で理解しづらい場合、従業員は具体的に何を遵守して行動すればよいか分からず、セキュリティ対策が不十分になってしまいます。分かりやすい実施手順を策定し、従業員に浸透させることが重要です。

■ 不十分な監査と改善の実施
ISMSの運用において監査と改善を怠ってしまうと、新たな脅威に適応できず、セキュリティ体制が陳腐化してしまいます。定期的な監査と、その結果をもとにした改善活動を継続的に行うことが必要です。

ISMSの導入を成功させるためには、経営層のリーダーシップ、従業員の教育、リスクマネジメントの適切な実施が欠かせません。常に変化するセキュリティ環境に適応する柔軟性や継続的な改善が、組織の情報セキュリティを確保することに繋がります。

第14章. 組織的管理策

14-1. 組織的管理策を参考とした対策基準・実施手順の策定

章の目的
第14章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 組織的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

14-1-1. 対策基準の策定

対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にすることができます。
組織が対策基準を策定する際は、組織の業態や規模によって重視するべき管理策は異なり、適用の必要性がない管理策も存在します。一方で、ISO/IEC 27001:2022の附属書AやISO/IEC 27002:2022にない管理策が必要となるケースもあることをご留意ください。
自組織にとってのリスクを自ら考えて必要な管理策を選択するために、リスクアセスメントの手法を使用し、対策基準を策定します。

ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	**項目数（合計93）**	**概要**
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

対策基準策定時の注意点
ISMSの認証取得を目標にして情報セキュリティ対策を進めると、ドキュメントの整備が目的になり、本来の情報セキュリティ対策がなおざりになってしまい、ISMSが形骸化するケースが少なくありません。策定した管理策が継続的に実行されていくことが重要となります。

組織は、情報セキュリティリスクを適切にコントロールするために必要となる管理策を念入りに検討し、対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

14-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）　【凡例】採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
5.1 情報セキュリティのための方針群		5.20 供給者との合意におけるセキュリティの取扱い	
5.2 情報セキュリティの役割及び責任		5.21 ICTサプライチェーンにおける情報セキュリティの管理	
5.3 職務の分離		5.22 供給者のサービス提供の監視、レビュー及び変更管理	
5.4 経営陣の責任		5.23 クラウドサービス利用における情報セキュリティ	
5.5 関係当局との連絡		5.24 情報セキュリティインシデント管理の計画策定及び準備	
5.6 専門組織との連絡		5.25 情報セキュリティ事象の評価及び決定	
5.7 脅威インテリジェンス		5.26 情報セキュリティインシデントへの対応	
5.8 プロジェクトマネジメントにおける情報セキュリティ		5.27 情報セキュリティインシデントからの学習	
5.9 情報及びその他の関連資産の目録		5.28 証拠の収集	
5.10 情報及びその他の関連資産の利用の許容範囲		5.29 事業の中断・阻害時の情報セキュリティ	
5.11 資産の返却		5.30 事業継続のためのICTの備え	
5.12 情報の分類		5.31 法令、規制及び契約上の要求事項	
5.13 情報のラベル付け		5.32 知的財産権	
5.14 情報転送		5.33 記録の保護	
5.15 アクセス制御		5.34 プライバシー及びPIIの保護	
5.16 識別情報の管理		5.35 情報セキュリティの独立したレビュー	
5.17 認証情報		5.36 情報セキュリティのための方針群、規則及び標準の順守	
5.18 アクセス権		5.37 操作手順書	
5.19 供給者関係における情報セキュリティ			

14-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

5.1 情報セキュリティのための方針群
情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。

5.2 情報セキュリティの役割及び責任
情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。

5.3 職務の分離
相反する職務および責任範囲は、分離しなければならない。

5.4 経営陣の責任
経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。

5.5 関係当局との連絡
組織は、関係当局との連絡体制を確立および維持しなければならない。

5.6 専門組織との連絡
組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家による協会・団体との連絡体制を確立し維持しなければならない。

5.7 脅威インテリジェンス
情報セキュリティの脅威に関連する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。

One Point

対策基準を策定する際のポイント
ISO/IEC 27001:2022附属書Aの中には、中小企業にとっては負担が大きい管理策があります。ISO/IEC 27001:2022附属書Aに適切な管理策がない場合は、独自の管理策を追加することができます。組織の状況を考慮し、適切な対策基準を策定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

14-1-1. 対策基準の策定

対策基準（例）

5.8 プロジェクトマネジメントにおける情報セキュリティ
情報セキュリティをプロジェクトマネジメントに組み入れなければならない。

5.9 情報及びその他の関連資産の目録
管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。

5.10 情報及びその他の関連資産の利用の許容範囲
情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。

5.11 資産の返却
要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。

5.12 情報の分類
情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。

5.13 情報のラベル付け
情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。

5.14 情報転送
情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。

5.15 アクセス制御
情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。

5.16 識別情報の管理
組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。

5.17 認証情報
認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。

5.18 アクセス権
情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。

14-1-1. 対策基準の策定

対策基準（例）

5.19 供給者関係における情報セキュリティ
供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。

5.20 供給者との合意における情報セキュリティの取扱い
供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。

5.21 ICTサプライチェーンにおける情報セキュリティの管理
ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。

5.22 供給者のサービス提供の監視、レビュー及び変更管理
サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。

5.23 クラウドサービスの利用における情報セキュリティ
クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。

5.24 情報セキュリティインシデント管理の計画及び準備
セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。

5.25 情報セキュリティ事象の評価及び決定
情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。

5.26 情報セキュリティインシデントへの対応
セキュリティインシデントに対し、文書化した手順に従って対応しなければならない。

5.27 情報セキュリティインシデントからの学習
セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。

5.28 証拠の収集
情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。

14-1-1. 対策基準の策定

対策基準（例）

5.29 事業の中断・阻害時の情報セキュリティ
事業の中断・阻害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。

5.30 事業継続のためのICTの備え
事業継続の目的およびICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。

5.31 法令・規制及び契約上の要求事項
情報セキュリティに関する法令や契約事項を特定・文書化し、遵守しなければならない。

5.32 知的財産権
知的財産権を保護するための適切な手順を実施しなければならない。

5.33 記録の保護
記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。

5.34 プライバシー及びPIIの保護
適用される法令、規制および契約上の要求事項に従って、プライバシーの維持およびPIIの保護に関する要求事項を特定し、満たさなければならない。

5.35 情報セキュリティの独立したレビュー
情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。

5.36 情報セキュリティのための方針群、規則及び標準の順守
組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を遵守していることを定期的にレビューしなければならない。

5.37 操作手順書
情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

14-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を遵守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対してわかりやすい実施手順を策定するよう心掛けることが大切です。

実施手順を策定する際は、ISO/IEC 27002に記載されている各管理策の手引が参考になります。手引の内容をもとに、実施手順の例を紹介します。この例と、ISO/IEC 27002の内容を参考に、自社に適した実施手順を策定してください。

5.1 情報セキュリティのための方針群

実施手順（例）

情報セキュリティ委員会は、「情報セキュリティ方針」などの情報セキュリティに関する方針を定義し、トップマネジメント（経営層）の承認を得る。また、情報セキュリティ委員会は、情報セキュリティに関する方針を適用範囲内の全従業者に公表する。また、「情報セキュリティ方針」は外部関係者にも公表する。

情報セキュリティ委員会は、「情報セキュリティ方針」以外の情報セキュリティのための方針群を、本手順において定める。方針群には以下を含める。

a. モバイル機器の方針
b. テレワーキング
c. アクセス制御方針
d. 暗号による管理策の利用方針
e. クリアデスク・クリアスクリーン
f. 情報転送の方針（および手順）
g. セキュリティに配慮した開発のための方針
h. 供給者関係のための情報セキュリティの方針

ワンポイントアドバイス

情報セキュリティに関する方針は、関連する従業員および利害関係者に認識されることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

14-1-2. 実施手順の策定

5.2 情報セキュリティの役割及び責任

実施手順（例）

トップマネジメント（経営層）は、情報セキュリティに関連する役割を持つ情報セキュリティ委員会、内部監査責任者に対して、以下の責任および権限を割り当てる。また、トップマネジメント（経営層）は、これらの役割、責任および権限を従業者に伝達する。情報セキュリティの運用に際し、トップマネジメント（経営層）は、情報セキュリティ委員会の設置および運営を実施する。

情報セキュリティ委員会の役割は以下の通り。
a. リスク対応計画の策定
b. 情報セキュリティ実行体制の構築
c. 選択された管理策の実施
d. 教育・訓練
e. 運用の管理
f. 経営資源の管理
g. 情報セキュリティ事象・セキュリティインシデントの管理
h. 関連当局との連絡（警察・審査機関・コンサル会社・取引先・委託先など）

情報セキュリティ委員会の責任および権限は以下の通り。

役割	責任および権限
情報セキュリティ委員会責任者	管理策の実施・運用について統括する。 管理策の成果をトップマネジメント（経営層）に報告する。
教育責任者	管理策に関する教育計画の立案と実施を行う。
部門管理者（運用委員）	情報セキュリティの部門代表者として、部門を管理する。
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規定・規則に従い、情報セキュリティを維持するための安全管理対策を実施する。
文書管理責任者	管理策に関する文書や記録などの維持・管理を行う。

内部監査責任者の責任および権限は以下の通り。
内部監査責任者は、管理策とその実施状況に関わる監査を統括する責任と権限を有する。

ワンポイントアドバイス
従業員が少ない場合は、文書管理責任者と教育責任者を同じ者にするなど、役割を兼任させて体制を構築することも有効です。

14-1-2. 実施手順の策定

5.3 職務の分離

実施手順（例）

a. 当組織は、申請者または作業者と、承認者を分離するように組織設計する。
b. 従業員の制約により兼任せざるを得ない場合、別部門などによる監視を行うことを条件に、兼任できる。

ワンポイントアドバイス
小さな組織で、職務の分離が困難である場合には、他の管理策（例：活動の監視、監査証跡、管理層による監督）を考慮することが大切です。

5.4 経営陣の責任

実施手順（例）

トップマネジメント（経営層）はすべての従業者に対し、情報セキュリティ方針、各実施手順、並びにその他情報セキュリティに関する要求事項の遵守を求める。

ワンポイントアドバイス
情報セキュリティ方針、各実施手順、その他情報セキュリティに関する要求事項が、すべての従業員に認識されることが大切です。

5.5 関係当局との連絡

実施手順（例）

情報セキュリティ委員会は、関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

関係当局	連絡手段	URL	主目的
【IPA】コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口	ウイルス発見・感染の届出 virus@ipa.go.jp 不正アクセスの届出 crack@pa.go.jp	https://www.ipa.go.jp/security/todokede/crack-virus/about.html	ウイルス感染や、不正アクセスによる被害を報告するため。
【IPA】情報セキュリティ安心相談窓口	TEL:03-5978-7509（受付時間10:00～12:00、13:30～17:00 土日祝日・年末年始は除く） anshin@ipa.go.jp	https://www.ipa.go.jp/security/anshin/about.html	ウイルス感染や不正アクセスに関する技術的な内容の相談に対して、アドバイスをもらうため。
【警視庁】サイバー犯罪相談窓口	TEL:03-5805-1731 受付時間：午前8時30分から午後5時15分まで（平日のみ）	https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html	サイバー犯罪被害について相談するため。
【個人情報保護委員会】個人情報・マイナンバーの漏えい報告	Webフォームで報告	https://www.ppc.go.jp/personalinfo/legal/leakAction/	個人情報、マイナンバーの漏えいに対処するため。
【JPCERT/CC】インシデント対応依頼	Webフォームまたは、以下のメールアドレスに報告 info@jpcert.or.jp	https://www.jpcert.or.jp/form/	セキュリティインシデント対応を支援してもらうため。

ワンポイントアドバイス
セキュリティインシデントを時機を失せずに報告するために、関係当局の連絡方法を明確にすることが大切です。

14-1-2. 実施手順の策定

5.6 専門組織との連絡

実施手順（例）

情報セキュリティ委員会は、専門組織およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。

専門組織	情報の入手方法	URL	主目的
【IPA】重要なセキュリティ情報	Webページを閲覧	https://www.ipa.go.jp/security/security-alert/2023/index.html	危険性が高いセキュリティ上の問題と対策に関する最新情報を収集するため。
【IPA】ランサムウェア対策特設ページ	Webページを閲覧	https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html	ランサムウェア対策に関する最新情報を収集するため。
【個人情報保護委員会】注意情報一覧	Webページを閲覧	https://www.ppc.go.jp/news/careful_information/?category=39	セキュリティ・個人情報・マイナンバーに関する、注意事項を把握するため。
【JPCERT/CC】注意喚起	Webページを閲覧	https://www.jpcert.or.jp/at/2023.html	脆弱性に関する最新情報を収集するため。

ワンポイントアドバイス
脆弱性や攻撃など情報セキュリティに関する情報を適時入手するために、入手方法を明確にすることが大切です。

5.7 脅威インテリジェンス

実施手順（例）

1. 既存または新たな脅威に関する情報を、次に示す専門機関から収集する。
   ・IPA
   ・JVN（Japan Vulnerability Notes）
   ・JPCERT/CC
   ・ISAC (Information Sharing and Analysis Center)
   ・個人情報保護委員会
   収集する情報は、以下のようなものとする。
   ・変化する脅威の状況に関する情報（例：攻撃者や攻撃の種類）
   ・攻撃の方法、使用されるツールや技術に関する情報
   ・特定の攻撃に関する詳細な情報
2. 収集した情報を分析する。
   脅威が、自組織にどのような影響を及ぼすか把握するために、収集した情報をもとにリスクアセスメントを実施する。
3. リスク低減の処置を実施する。
   リスクアセスメントの結果をもとに、ファイアウォール・侵入検知システム・マルウェア対策ソリューションなど、技術的に予防、検知を行うための管理策を採用する。

ワンポイントアドバイス
情報の収集から、リスク低減処置を実施するまでの手順を明確にすることが大切です。

14-1-2. 実施手順の策定

5.8 プロジェクトマネジメントにおける情報セキュリティ

実施手順（例）
a. プロジェクト管理者は、プロジェクトにおける必要な管理策を特定する。 b. プロジェクトにおける必要な管理策は、プロジェクト終了後も考慮する。 c. プロジェクト管理者は、情報セキュリティ責任者を任命する。 d. 情報システム管理者は、業務用情報システムの導入・改善にあたっては、必要に応じて情報セキュリティ上の要求事項を、要件定義書や提案依頼書などにより文書化する。文書には下記から必要な事項を含める。 ・情報システムの設置場所（環境・障害からの対策を含む）に関する事項 ・無停電電源装置などのサポートユーティリティに関する事項 ・保守契約に関する事項 ・システムの冗長化に関する事項 ・通信、データの安全対策に関する事項 ・受け入れテストに関する事項 ・アクセス権限に関する事項
ワンポイントアドバイス プロジェクトが提供する製品またはサービスの情報セキュリティ要求事項は、情報セキュリティ方針、トピック固有の個別方針および規制から遵守すべき要求事項を決定することが大切です。

5.9 情報及びその他の関連資産の目録

実施手順（例）
a. 情報セキュリティ委員会は「資産目録」を作成し、当組織における重要な資産を識別する。また「資産目録」を「年間計画表」に従い、最低年1回見直す。 b. 情報セキュリティ委員会は「資産目録」において特定した資産に対し、同目録上に管理責任者（リスク所有者）を記載することで管理責任を明確にする。
ワンポイントアドバイス 資産の管理責任を個人またはグループに割り当て、管理責任を明確にすることが大切です。

14-1-2. 実施手順の策定

5.10 情報及びその他の関連資産の利用の許容範囲

実施手順（例）

情報の区分ごとの取扱いルールを以下に示す。
情報の区分は「5.12 情報の分類」で、ラベル表示については「5.13 情報のラベル付け」で定める。

【文書・メディアなどの場合】

管理区分	関係者外秘	社外秘	一般
ラベル表示	責任者に一任	責任者に一任	不要
利用者	関係する部署・プロジェクトに所属する従業者	当組織の従業者	誰でも可
再配布	関係する部署・プロジェクト内に限る	社内に限る	特別な配慮不要
保管場所	施錠された場所	責任者に一任	
コピーの使用	必要のある者に限定	社内に限る	
FAX送信	関係する部署・プロジェクト内に限る	社内に限る	
裏紙使用※1	禁止	禁止	
社外便	透かして内容が見えないようにする。※2		
社外での携行	責任者の許可を得た者のみ携行を許可する。※3		
廃棄（文書）※4	シュレッダー・焼却・溶解のいずれか	責任者に一任	
廃棄処（媒体）	廃棄、再利用前の内容を消去する。		

※1 個人情報の記された書類の再利用は禁じる。
※2 紙や記憶媒体による個人情報を、郵便や宅配便などにより移送するときは、誤配、紛失などの危険を最小限にするため、ポストへの施錠、受け取り確認が可能な移送手段の選択などの措置を講じる。
※3 個人情報を外部へ持ち出す際は、目的地以外へ立ち寄らず、手放さない、車中に放置しないよう徹底する。
※4 紙に記された個人情報の廃棄は、シュレッダーによる裁断・焼却・溶解いずれかの方法で処分する。また、廃棄前の一時保管場所からの紛失・盗難防止のため、重要書類は即廃棄する。

【システム内情報】

管理区分	関係者外秘	社外秘	一般
アクセス制御	個人またはグループでのアクセス制御	責任者に一任	特別な配慮不要
個人PCへの保管	責任者に一任	責任者に一任	
サーバへの保管	アクセス制限	責任者に一任	
コピー(複製)※1	コピーの管理	責任者に一任	
メール	添付ファイルにパスワード※2		

※1　コピーは、バックアップの必要上および業務上やむを得ない場合の必要最小限の範囲にとどめるものとする。
※2　取引先との合意がある場合は、その合意に従う。

ワンポイントアドバイス
許容できる行動、許容できない行動を明確に定めることが大切です。

14-1-2. 実施手順の策定

5.11 資産の返却

実施手順（例）

情報セキュリティ委員会は、退職者が発生した際に、以下の対応を部門長に要求し、実施されたことを確認する。
a. 名刺、社員証、IDカードなどの返却
b. 会社が支給したノートPCや携帯電話などの返却
c. 紙で保管する書類の返却、または廃棄

ワンポイントアドバイス
返却するすべての情報およびその他の関連資産を明確に特定し、文書化することが大切です。

5.12 情報の分類

実施手順（例）

情報は一般・社外秘・関係者外秘で分類する。
情報セキュリティ委員会は、情報の分類を最低年1回見直す。

分類	内容
一般	下記以外
社外秘	関係者外秘以外の機密事項であり、当組織の従業者に対してのみ開示が許されるもの。（取引先に開示する必要があるものは除く。）または情報セキュリティに関わる規定・手順書類。
関係者外秘	情報が外に漏れることによって、当組織が重大な損失もしくは不利益を受けるような恐れのある機密事項であり、職務上の限られた関係者のみに開示を許すもの。関係者が明示的に定められていない場合、関係者とは、情報を直接配布された者を指す。

ワンポイントアドバイス
分類は、情報の侵害が組織に与える影響のレベルによって決定できます。分類体系で定義されたレベルには、分類体系の適用において意味をなすような名称を付けることが大切です。

5.13 情報のラベル付け

実施手順（例）

従業員は、取扱う情報が一般・社外秘・関係者外秘の区分のうち、どれに該当するか認識できる必要がある。
書類の分類を容易に認識できない場合は、以下のいずれかの方法により適切なラベル付けを行う。

a. 分類をシールなどの色により識別する。
b. ファイルなどに分類を記入（またはスタンプ）することで識別する。
c. 分類ごとに収納場所を分ける。

ワンポイントアドバイス
ラベル付けは、「5.12 情報の分類」で確立した分類体系を反映していることが大切です。

14-1-2. 実施手順の策定

5.14 情報転送

実施手順（例）

a. 重要な情報を外部に送信する場合は、セキュアなファイル共有サービスを利用する。やむを得ずファイル共有サービスが利用できない場合は、受信者と合意したうえで、メールに添付して送信する。
b. 重要な情報を外部にFAXにて送信する場合は、入力した番号と、名刺や送り状を照合し、間違えがないことを確認してからスタートボタンを押す。また頻繁に送信する送り先は短縮ダイヤルに登録する。
c. 認可されていない者に聞かれる可能性がある場所で、重要な情報を口頭で伝えることは禁じる。
d. 重要な情報を外部に郵送する場合は、配達記録郵便や宅配便など配達記録が残る手段をとる。
e. 重要な情報を格納した媒体は、手渡しを原則とし、やむを得ず郵送する場合は、十分な梱包により媒体を保護する。
f. 個人情報の授受記録
  ・紙や記憶媒体による個人情報の受け渡しに際しては、送付票や受領証などで受け渡しの完了を確認する。
  ・電子メールにより個人情報の受け渡しを行う際には、送信済みメールおよび、受領確認の返信メールのいずれかまたは両方を受け渡し記録とする。
g. 電子メールの利用
  ・電子メールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定する。
  ・社外メーリングリストへの参加は、原則禁止とする。
  ・重要な情報（社外秘以上）はメール本文に記載して送信せず、aに従う。
h. 情報転送に関する合意
  ・情報の転送先との間で、情報転送の手段について、あらかじめ合意を得る。
  ・重要な情報を外部にメール添付またはFAXにて送信する場合は、必要に応じて送信予告、到着確認の電話を掛ける。
  ・宅配便業者を利用する場合は、会社が指定する業者を利用する。
i. 電子的メッセージ通信
  ・当組織のWebサイトに入力する情報の通信は、SSL/TLSにより行う。
  ・電子データによる個人情報をインターネット経由で送受信する際は、SSL/TLSなどの暗号化対策やパスワード設定などの措置を講じる。

ワンポイントアドバイス
情報転送は、電子的な転送、物理的記憶媒体での送付および口頭での伝達によって行われる場合があります。情報転送の規則、手順を定めることが大切です。

14-1-2. 実施手順の策定

5.15 アクセス制御

実施手順（例）
a. 業務に必要な者のみが情報にアクセスできるようにし、アクセス権限および操作権限は、認められた場合以外は与えないようにする。 b. 社内LANは、情報システム管理者の承認を得た従業員、装置に限り接続する。 c. 社内の情報システムへの外部からのアクセスは、ファイアウォールなどによって通信を制限する。 d. 外部から社内のサーバに接続する場合、VPN接続を使用する。 e. 無線LANは物理的・論理的な認証、通信の暗号化などを施したうえで利用する。 f. サーバ室へ入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。 g. サーバ室は、常時施錠可能とし、入退資格のない者の立ち入りを禁じる。
ワンポイントアドバイス アクセス制御規則を定めるには、「明確に許可していないことは、原則的に禁止する」という最も特権の小さい前提に基づいた規則を設定するようにすることが大切です。

5.16 識別情報の管理

実施手順（例）
a. 情報システムの利用者登録および登録削除は、当該利用者の属する部門長が申請し、情報システム管理者の承認を得る。 b. 利用者登録は業務上必要な範囲で従業者に付与する。
ワンポイントアドバイス 識別情報が不要になった場合、識別情報は時機を失せずに無効化または削除することが大切です。

14-1-2. 実施手順の策定

5.17 認証情報

実施手順（例）
a. 情報システム管理者は、利用者に仮パスワードを発行する場合、利用者本人のみが知ることができる方法で通知する必要がある。 b. 情報システム管理者は、利用者に対し、仮パスワードを直ちに変更することを要求し、通知する。 c. 秘密認証情報の利用 ・利用者は、英数字と記号を混在した10文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。 ・他人に容易に推測されるようなわかりやすいパスワードの使用を禁じる。 ・他のサービスと重複するパスワードの利用を禁じる。 ・各システムにおける管理者IDのパスワードは、情報システム管理者において厳重に管理する必要がある。 ・利用者および情報システム管理者は、パスワードの代替もしくは補完のために、指紋などの生体認証、ICカード認証などの機器による認証方式も採用できるものとする。 d. パスワード管理システム ・パスワードの入力は対話式とする。 ・パスワードをシステムに記憶させることは禁じる。
ワンポイントアドバイス パスワードを認証情報として使用する場合、IPAなどが推奨している強力なパスワードの作り方を参考にすることが大切です。

5.18 アクセス権

実施手順（例）
a. 利用者のアクセス権は、重要情報に対しては必要最小限の者がアクセスするという原則のもとに、情報システム管理者が検討し、設定を行う。 b. 情報システム管理者は、定期的（最低年1回）および必要時にアクセス権限の棚卸および見直しを行う。 c. 退職者が発生した際は、業務に支障がないよう調整し、速やかに該当アカウントを削除する必要がある。申請は、当該従業員が最後に所属した部門の長がアクセス権限の削除を申請し、情報システム管理者、またはその指名する従業員が削除する。 d. 他部署への移動が生じた際は、aの手順に従い削除する。また、新規のアクセス権限は移動先部門の長が申請し、同様の手順に従い登録する。
ワンポイントアドバイス 物理的および論理的なアクセス権の定期的レビューでは、同じ組織内での異動、昇進、降格、退職後の利用者のアクセス権、および特権的アクセス権の認可について考慮することが大切です。

14-1-2. 実施手順の策定

5.19 供給者関係における情報セキュリティ

実施手順（例）

a. 当組織における供給者には、以下がある。
- ISP、電話サービス、IT機器などのサービス提供者
- 情報システムの開発・保守における外部委託先
- 会計、税務、法律などの専門サービス提供者
- 清掃業者、廃棄業者
- クラウドサービス

b. 情報セキュリティ委員会は、部外者・外部組織によるオフィスエリアや情報システムへのアクセスを許可する際に生じる可能性があるリスクを考慮し、情報セキュリティ上の要求事項を明確にする。

ワンポイントアドバイス
供給者が提供する製品およびサービスの使用に関連するセキュリティリスクに対処するためのプロセスおよび手順を特定し、実施することが大切です。

5.20 供給者との合意における情報セキュリティの取扱い

実施手順（例）

a. 提供されるサービスの利用は、次の手順に従い行う。
1. 「委託先審査票」による評価・選定を行う。
2. 情報セキュリティ要求事項を考慮し、次の事項を含む契約を締結する。
- 機密保持契約などの情報の取扱いに関する契約
- 使用許諾に関する取り決め、コードの所有権および知的所有権（開発の場合）
- 実施される作業場所および入退室管理
- 外部委託先が不履行となった場合の預託契約に関する取り決め

3. 情報セキュリティ委員会は、「5.19 供給者関係における情報セキュリティ」において検討したリスクを考慮し、必要に応じて第三者との間で契約を締結する。

b. クラウドサービスを介して重要資産を取扱う際は、利用者は多要素認証を有効にしてセキュリティを強化する必要がある。

ワンポイントアドバイス
組織と供給者の間で情報セキュリティ要求事項を満たす義務に関し、当事者間で合意を確立し、文書化することが大切です。

14-1-2. 実施手順の策定

5.21 ICTサプライチェーンにおける情報セキュリティの管理

実施手順（例）
a. ICT製品・サービスの供給者との契約には、必要に応じて再委託に関する事項を盛り込む。 b. クラウドサービスの利用にあたっては、クラウドサービス提供者の事業継続性、および以下のサービスに関する情報セキュリティ事項を考慮のうえ、クラウドサービスを選定する。 ・サービスの導入実績、信頼性 ・利用者サポート機能 ・利用終了後のデータの扱い ・サービスの可用性 ・暗号化など、通信経路の安全対策
ワンポイントアドバイス 信頼できる供給源からICTを取得する手順を明確にすることが大切です。

5.22 供給者のサービス提供の監視、レビュー及び変更管理

実施手順（例）
a. 情報セキュリティ委員会は、サービスの供給者に対して、あらかじめ定められた頻度（最低年1回）において契約の履行状況ならびに「委託先審査票」による遵守状況の確認を行う。 b. サービスの供給者との間で契約内容やサービスレベルに変更があった場合、変更点を受け入れることができるか否かを検証し、契約内容の見直しを実施する。
ワンポイントアドバイス サービスの提供において不完全な点があった場合は、適切な処置をとることが大切です。

14-1-2. 実施手順の策定

5.23 クラウドサービスの利用における情報セキュリティ

実施手順（例）

クラウドサービスを導入する際、以下の評価表をもとにクラウドサービスを評価し、自社のセキュリティ要件事項を満たしているか確認する。

クラウドサービス提供者名	サービス内容

取得している認証
□ ISO/IEC 27001 □ ISO/IEC 27017

セキュリティ対策内容	評価
クラウドサービスに対して、マルウェア対策を行っているか。	
クラウドサービスのバックアップを行っているか。	
サービス解約時のデータの取扱い方法が明確になっているか。	
サービス稼働率、障害発生頻度、障害発生時の復旧時間など、サービス品質は問題ないか。	
データがどの国や地域に配置されたサーバに保存されているか確認したか。	
サービスの利用方法について問い合わせることができるか。	
クラウドサービス提供者の責任範囲を確認したか。	
クラウドサービスのセキュリティインシデント発生時に通知がくるかどうか確認したか。	

（評価）○：できている　△：部分的にできている　×：できていない

ワンポイントアドバイス

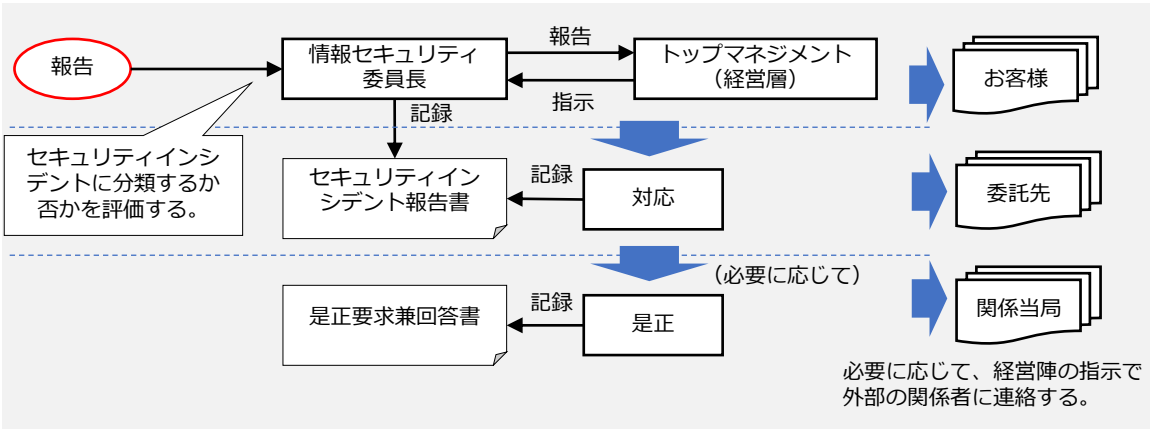
クラウドサービスの利用は、クラウドサービス提供者とクラウドサービス利用組織との間の情報セキュリティに関する責任の共有および分担、共同作業を伴う可能性があります。クラウドサービス提供者と、クラウドサービス利用組織の両方の責任を適切に定義し、実践することが大切です。

14-1-2. 実施手順の策定

5.24 情報セキュリティインシデント管理の計画策定及び準備

実施手順（例）

セキュリティインシデントへの対応は、以下の手順で行う。
管理層の責任のもと、以下の手順を関係者に伝達する。



ワンポイントアドバイス
セキュリティインシデントへの対応を実行するために役割および責任を決定し、関連する関係者に効果的に伝達することが大切です。

5.25 情報セキュリティ事象の評価及び決定

実施手順（例）

a. セキュリティの弱点、脅威に気付いた場合もしくは疑いを持った場合は、情報セキュリティ委員会に報告する。この際、自己で解決することよりも報告を優先させる。
b. 情報セキュリティ事象の評価は、以下の表に従い、部門管理者（情報セキュリティ委員会メンバー）が行う。
・大、中の項目に該当する情報セキュリティ事象は、セキュリティインシデントとして分類する。
・項目の大、中、小の順に優先順位を付ける。

項目	小	中	大
分類	ヒヤリハット・事象	インシデント	インシデント
最終的に被害が及ぶ範囲	現状、事件・事故の発生には及ばない。（将来、被害が発生する可能性がある。）	社員または社内	顧客・取引先
連絡先	情報セキュリティ委員長	情報セキュリティ委員長	情報セキュリティ委員長 トップマネジメント（経営層） 外部関係者

ワンポイントアドバイス
情報セキュリティ事象をセキュリティインシデントに分類する基準を明確に定めることが大切です。

14-1-2. 実施手順の策定

5.26 情報セキュリティインシデントへの対応

実施手順（例）

セキュリティインシデントへの対応手順は以下の表に従う。

影響度	小	中・大
ウイルス感染時	• 感染したPCを、組織内のネットワークから切り離す。 • 発生する可能性がある被害をシステム担当者に報告する。	• 感染したPCを、組織内のネットワークから切り離す。 • 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
不正アクセス発生時	• ネットワークを遮断する。 • 重要なデータを隔離する。 • ログインできる場合は、早急にパスワードを変更する。 • 発生する可能性がある被害をシステム担当者に報告する。	• ネットワークを遮断する。 • 重要なデータを隔離する。 • ログインできる場合は、早急にパスワードを変更する。 • システムやアプリケーションを停止する。 • 発見した事実をできるだけ速やかに情報システム管理者に連絡する。
情報破壊発生時	発見次第、発生する可能性がある被害を部門長に報告する。	発見した事実をできるだけ速やかに部門長に連絡する。
情報改ざん発生時	同上	同上
情報漏えい発生時	同上	同上
サービス停止時・機器故障など	同上	同上

ワンポイントアドバイス
セキュリティインシデント対応に関する手順を確立し、すべての関連する利害関係者に伝達することが大切です。

14-1-2. 実施手順の策定

5.27 情報セキュリティインシデントからの学習

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティインシデントを管理・分析し、問題があれば、計画を立ててトップマネジメント（経営層）へ提議する。計画には、解決に向けての処置方法・費用・実施予定日・責任者を明確にする。 b. 将来のセキュリティインシデントの起こりやすさや影響を減らすため、情報セキュリティ委員会は、セキュリティインシデントから得られた知識を活かして「6.3 情報セキュリティの意識向上、教育及び訓練」を強化・改善する。
ワンポイントアドバイス セキュリティインシデントの形態、規模および費用を定量化および監視するための手順を確立することが大切です。

5.28 証拠の収集

実施手順（例）
情報セキュリティ委員会は、情報システムの事故が特定の個人、または組織に起因するもので、事後処置が法的処置に及ぶ可能性のある場合には、必要な証拠の収集、保全に努める。
ワンポイントアドバイス 懲戒処置および法的処置のために情報セキュリティ事象に関連する証拠を取扱う場合は、内部の手順を定めて従うことが大切です。

14-1-2. 実施手順の策定

5.29 事業の中断・阻害時の情報セキュリティ

実施手順（例）

a. 資産のリスク分析
「資産目録（情報資産管理台帳）」で特定した情報資産のうち、可用性の評価値が3の重要資産を情報セキュリティ継続のリスク分析対象とする。
※可用性の評価値は、「11-2-2. リスク特定」で記載している方法で算出する。

b. aにおいて登録した資産に対して、以下のリスクについて考慮する。
・地震・火災・洪水などの自然災害
・人的なミス
・システム障害
・健康上の問題

c. bのリスクが生じた際に影響を受ける業務プロセスを特定し、リスクが発生した場合のシナリオを作成する。

d. リスクが生じた場合の影響度と、リスクが発生する可能性について検討し、検討結果に基づき優先順位を決定する。

e. dにおいて、優先順位が高いと判断したものに対して「事業継続計画書」を作成し、トップマネジメント（経営層）の承認を得る。
「事業継続計画書」には以下の内容を含む。
・実行開始条件（リスクシナリオの発生）
・非常時手順（発生時の連絡手順）
・回復手順（復旧のための手順）
・回復目標（目標時間を必要に応じて決定）
・再開手順（回復後のリハーサル手順）
・試験のスケジュール
・教育（教育が必要な場合はその計画）

f. 策定した計画および手続について試験を実施し、試験の結果、必要があると判断した場合は計画を更新する。試験は以下のいずれかの方法、またはその組み合わせにより行う。
・机上試験
・模擬試験
・技術的回復試験
・代替施設における回復試験
・供給者施設およびサービスの試験

g. 情報セキュリティ委員会は、事業継続に関する試験を最低年1回、継続的に実施する。

ワンポイントアドバイス
事業の中断または阻害時に、重要な事業プロセスの情報セキュリティを維持または復旧するために、計画を策定、実施、試験、レビューおよび評価することが大切です。

14-1-2. 実施手順の策定

5.30 事業継続のためのICTの備え

実施手順（例）
a. ビジネスインパクト分析（不測のインシデントによって業務やシステムが停止した場合、会社の事業にどのような影響があるかを分析すること）を行い、事業継続が困難な状況を特定する。 b. 事業が中断・停止になった際の対応手順を策定し、文書化する。 c. 策定した対応手順が有効であることを確実にするため、あらかじめ定めた間隔（年1回以上）で試験を実施し検証する。
ワンポイントアドバイス 組織がICTサービス事業の中断・阻害を管理する方法を詳述した対応および復旧手順を含むICT継続計画を、演習および試験を通じて定期的に評価、または経営陣が承認することが大切です。

14-1-2. 実施手順の策定

5.31 法令・規制及び契約上の要求事項

実施手順（例）

a. 情報セキュリティ委員会は、当組織が遵守すべき法令、規制、および契約上の要求事項を識別し、「情報セキュリティに関する法令規制一覧表」に記載する。「情報セキュリティに関する法令規制一覧表」は最低年1回見直す。
b. 情報セキュリティ委員会は、当組織の従業者が「情報セキュリティに関する法令規制一覧表」を、必要に応じていつでも参照できる状態にする。
c. 特定した要求事項を満たすために、必要に応じて教育などのテーマとする。
d. 暗号化した装置を輸出する場合、または海外に持ち出す場合、該当する法規制について調査を行い、必要であれば対応を行う。

情報セキュリティに関連する法律（例）	概要
特定電子メールの送信の適正化などに関する法律	利用者の同意を得ずに広告、宣伝または勧誘などを目的とした電子メールの送信を禁止している。
電子署名及び認証業務に関する法律	「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定められている。
著作権法	プログラムやマニュアル、ホームページなどは、著作権の対象であり、無断での複製は、著作権法の侵害になる。
不正アクセス禁止法	不正アクセス行為や、不正アクセス行為につながる識別符号（ID、パスワード）の不正取得・保管行為、不正アクセス行為を助長する行為などを禁止している。
刑法	無断でデータを改ざん・破壊する行為や、虚偽の金融機関を名乗ったサイトや電子メールを使い、金銭をだまし取るような行為などは、刑法に違反する。

ワンポイントアドバイス
総務省のWebサイト「国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン」で、サイバーセキュリティに関する代表的な法律が紹介されています。

詳細理解のため参考となる文献（参考文献）	
国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン	https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal.html

14-1-2. 実施手順の策定

5.32 知的財産権

実施手順（例）
a. 知的財産権を保護するためのルールを策定し、組織内で教育・啓発活動を行う。 b. 知的財産権を侵害する行為を禁止する。 c. 知的財産権を侵害する行為が発生した場合には、速やかに是正措置を講じる。 d. ソフトウェアなどの使用許諾計画を遵守する。 e. 情報システム管理者は、パッケージソフトのライセンス管理を適切に行う。
ワンポイントアドバイス 知的財産権には、ソフトウェアまたは文書の著作権、意匠権、商標権、特許権およびソースコード使用許諾権が含まれます。

14-1-2. 実施手順の策定

5.33 記録の保護

実施手順（例）

当組織における記録は、関連する法令に基づき次表の保存期間にわたり、消失、破壊、改ざん、不正なアクセス、流失などがないように適切に保存する。

記録の種類	保存期間
■定款 ■登記関係書類 ■訴訟関係書類 ■特許など知的所有権に関する書類 ■社則・社規	永久
■「商業帳簿」 会計帳簿（日記帳、仕訳帳、総勘定元帳）、貸借対照表、損益計算書、附属明細書 ■「営業に関する重要な書類」 株主名簿、社債原簿、株主総会議事録、取締役会議事録、営業報告書、利益処分案 （損失処理案）、このほか紛争が生じた場合に重要な証拠となり得る書類（例：契約書）	10年
■仕訳帳、総勘定元帳、現金出納帳、固定資産台帳、売掛帳、買掛帳、経費帳 ■棚卸表、貸借対照表、損益計算書、決算に関して作成された書類 ■注文書、契約書、送り状、領収書、見積書、その他これらに準ずる書類（例：請求書）	7年
■給与所得者の扶養控除など（異動）申告書 ■給与所得者の保険料控除申告書兼給与所得者の配偶者特別控除申告書 ■源泉徴収簿	
■財産形成非課税貯蓄申込書・移動申請書	5年
■雇用保険被保険者に関する書類	4年
■労働者名簿 ■賃金台帳 ■雇入・解雇・災害補償・賃金その他労働関係に関する重要な書類	3年
■労働保険料の徴収に関する書類	
■労災保険に関する書類	
■安全委員会議事録 ■衛生委員会議事録 ■安全衛生委員会議事録	
■健康保険に関する書類	2年
■厚生年金保険に関する書類	
■雇用保険に関する書類	

ワンポイントアドバイス
記録は、記録の種類（会計記録、商取引記録、人事記録、法的記録など）によって分類し、それぞれに保存期間の詳細と、物理的または電子的な保存が可能な保存媒体の種類を記載することが大切です。

5.34 プライバシー及びPIIの保護

実施手順（例）

個人情報は、「5.10 情報およびその他の関連資産の利用の許容範囲」の取扱いルールに従い、厳重に取扱う。

ワンポイントアドバイス
プライバシーの保持およびPII保護のための手順を策定および実施することが大切です。

14-1-2. 実施手順の策定

5.35 情報セキュリティの独立したレビュー

実施手順（例）

a. 年に1度、内部監査により独立したレビューを行う。
b. 以下に例示する、情報セキュリティに影響のある変化が生じた場合も、内部監査により独立したレビューを行う。
・事業の追加/変更、業務手順の大幅な変更
・住所変更、拠点の新設
・情報セキュリティに関する主たる担当者の変更
・関係する法令・規制、または契約の大幅な変更

ワンポイントアドバイス
独立したレビューにおいて、情報セキュリティに関して取組が不十分であると明確になった場合には、経営陣は是正処理を発議することが大切です。

5.36 情報セキュリティのための方針群、規則及び標準の順守

実施手順（例）

a. 情報セキュリティ委員会は、セキュリティに関する手順や実施標準が正しく実施されていることを確実にするため、「運用チェックリスト」にて、定期的（3ヶ月ごと）に点検を行う。
b. 情報セキュリティ委員会（入退管理責任者）は、入退記録が適切にとられているかどうかを月に1度確認する。また、入退管理が有効かつ適切に実施されていることを定期的に確認し、不備が発見された場合は速やかに是正の処置をとる必要がある。
c. 情報システム管理者は、技術的な遵守事項が正しく実施されていることを確実にするため、上記のa、bに従い点検する。

ワンポイントアドバイス
是正処置が完了しない場合は、確認時に進捗状況を報告することが大切です。

5.37 操作手順書

実施手順（例）

情報処理設備の正確、かつ、セキュリティを保った運用を確実にするために、次の事項を明記した手順書を文書化し、必要に応じて利用者が参照できるようにする。
a. システムが故障した場合の再起動および回復の手順
b. 記憶媒体の取扱い手順
c. バックアップの取得手順
d. 保守手順
e. 容量、能力、パフォーマンスおよびセキュリティなどの監視手順

ワンポイントアドバイス
操作手順書は必要に応じてレビューし、更新することが大切です。

第15章. 人的管理策

15-1. 人的管理策を参考とした対策基準・実施手順の策定

章の目的
第15章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標
◘ 人的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

15-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
6.1 選考		6.5 雇用の終了または変更後の責任	
6.2 雇用条件		6.6 秘密保持契約または守秘義務契約	
6.3 情報セキュリティの意識向上、教育及び訓練		6.7 リモートワーク	
6.4 懲戒手続		6.8 情報セキュリティ事象の報告	

15-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

6.1 選考
従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。

6.2 雇用条件
雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。

6.3 情報セキュリティの意識向上、教育及び訓練
従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。

6.4 懲戒手続
情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。

6.5 雇用の終了または変更後の責任
雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。

6.6 秘密保持契約または守秘義務契約
組織の要求事項を反映した秘密保持契約または守秘義務契約を従業員や外部の関係者と締結しなければならない。

6.7 リモートワーク
要員が遠隔で作業する場合は、セキュリティ対策を実施しなければならない。

6.8 情報セキュリティ事象の報告
情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告できる仕組みを設けなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

15-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

6.1 選考

実施手順（例）
従業者の募集・採用プロセスは以下の点を考慮のうえ行う。 a. 取得した履歴書、スキルシートなどから業務上の要求事項への適合を判断し、選考を行う。 b. 採用時の面接などにおける態度や言葉遣いなどから倫理観を判断し、選考を行う。 c. 役員や管理職の採用に関しては、過去の信用情報など、より詳細な調査を行う場合があるが、この際は本人の同意を得たうえで行う。
ワンポイントアドバイス 選考プロセスはフルタイム、パートタイム、臨時スタッフを含むすべての従業員に対して実行することが大切です。

6.2 雇用条件

実施手順（例）
情報セキュリティに関する責任を理解し、情報セキュリティ方針を守ることを従業員に誓約させるため、雇用契約書に、情報セキュリティに関する事項を盛り込み、誓約書に署名を求める。
ワンポイントアドバイス 従業員に、情報セキュリティに関する雇用条件を同意させることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

15-1-2. 実施手順の策定

6.3 情報セキュリティの意識向上、教育及び訓練

実施手順（例）

a. すべての従業者は、職務に関連する方針および手順についての適切な、意識向上のための教育および訓練を受ける必要がある。
b. 当組織では従業者が次の事項に関して認識を持てるよう教育・訓練を実施する。
・情報セキュリティ方針
・情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティに対する自らの貢献
・ISO/IEC 27001の要求事項に適合しないことの意味
c. 教育計画は情報セキュリティ委員会が作成し、トップマネジメント（経営層）が承認する。
d. 当組織の主な教育を以下に示す。（以下の教育は「教育実施記録」に残す。）
・新任部門管理者（運用委員）
新任の情報セキュリティ委員会メンバーに実施する。
・入社時・社内異動者の教育（適時）
新入社員、中間採用者に対して、入社時にセキュリティ教育を実施する。
・定期教育（「年間計画表」に基づく）
年に最低1回、適用範囲内の従業者に対して、情報セキュリティの理解、再確認と改善、向上のための教育を実施する。
・再教育
セキュリティ違反者および情報セキュリティに関する低理解度の従業者に対して、再教育を実施し、違反の再発防止に努める。
・実施した教育の有効性評価
上記の教育実施後理解度調査などを実施し、実施した教育の有効性の評価を行う。

ワンポイントアドバイス
知識が伝わったこと、並びに意識向上、教育および訓練プログラムの有効性を確認するため、意識向上、教育および訓練の活動終了時に、従業員理解の評価を行うことが大切です。

15-1-2. 実施手順の策定

6.4 懲戒手続

実施手順（例）
従業者が故意または過失により情報を漏えいした場合、または情報セキュリティ上の遵守事項に違反した場合は、罰則の対象とする。
ワンポイントアドバイス 懲戒手続は、関連する法令、規制、契約および事業上の要求事項、並びに必要に応じてその他の要素を考慮に入れることが大切です。

6.5 雇用の終了または変更後の責任

実施手順（例）
情報セキュリティの観点から、雇用の終了または変更後も従業員が守るべき義務や責任（たとえば守秘義務）について定め、雇用時の誓約書に盛り込むと同時に、雇用の終了または変更時に再確認する。
ワンポイントアドバイス 雇用の終了または変更を管理する手続では、終了または変更後にどの情報セキュリティの責任および義務を引き続き有効とすることが望ましいかを定義することが大切です。

6.6 秘密保持契約または守秘義務契約

実施手順（例）
a. 当組織の従業者は、当組織との間で機密情報に関する秘密保持の契約を締結する。なお、同契約には原契約の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含める。 b. 当組織との委託先との間で、必要に応じて秘密保持の契約を締結する。 c. 情報セキュリティ委員会は、年に一度、情報セキュリティ要求事項に照らして、秘密保持の契約書の妥当性を検証する。
ワンポイントアドバイス 秘密保持契約または守秘義務契約に関する要求事項は、定期的または要求に影響する変化が発生した場合に、レビューすることが大切です。

15-1-2. 実施手順の策定

6.7 リモートワーク

実施手順（例）
a. リモートワークは、情報セキュリティ委員長の承認を得たものに限って行える。 b. リモートワークにて使用するPCは、会社から貸与したPCとし、家族などの同居人と共有することは禁じる。 c. リモートワークにて使用するPCは、アンチウイルスソフトを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。 d. リモートワークにて使用するPCに、ファイル交換ソフトなどの不正なソフトウェアをインストールすることは禁じる。 e. 社内ネットワークへはVPNにて接続する。
ワンポイントアドバイス リモートワークで個人所有のPCを使用する場合は、管理方法や接続方法について実施手順を記載することが大切です。

6.8 情報セキュリティ事象の報告

実施手順（例）
情報セキュリティ事象は、「5.25 情報セキュリティ事象の評価及び決定」に従って報告し、評価を行う。
ワンポイントアドバイス すべての社員が情報セキュリティ事象を報告する連絡先を認識し、報告の仕組みはできるだけ簡単で使いやすく、いつでも利用できるようにすることが大切です。

第16章. 物理的管理策

16-1. 物理的管理策を参考とした対策基準・実施手順の策定

16-2. 各種テーマごとの対策

章の目的

　第16章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。

主な達成目標

- 物理的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

16-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）

【凡例】採用：〇・不採用：×

項目	採用、不採用	項目	採用、不採用
7.1 物理的セキュリティ境界		7.8 装置の設置及び保護	
7.2 物理的入退		7.9 構外にある資産のセキュリティ	
7.3 オフィス、部屋及び施設のセキュリティ		7.10 記憶媒体	
7.4 物理的セキュリティの監視		7.11 サポートユーティリティ	
7.5 物理的及び環境的脅威からの保護		7.12 ケーブル配線のセキュリティ	
7.6 セキュリティを保つべき領域での作業		7.13 装置の保守	
7.7 クリアデスク・クリアスクリーン		7.14 装置のセキュリティを保った処分または再利用	

16-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

7.1 物理的セキュリティ境界
情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。

7.2 物理的入退
セキュリティを保つべき領域は、適切な入退管理策および立寄り場所によって保護しなければならない。

7.3 オフィス、部屋及び施設のセキュリティ
オフィス、部屋および施設に対する物理的セキュリティを設計し、実装しなければならない。

7.4 物理的セキュリティの監視
施設は、認可されていない物理的アクセスについて継続的に監視しなければならない。

7.5 物理的及び環境的脅威からの保護
自然災害およびその他の意図的または意図的でない、インフラストラクチャーに対する物理的脅威などの物理的および環境的脅威に対する保護を設計し、実装しなければならない。

7.6 セキュリティを保つべき領域での作業
セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施しなければならない。

7.7 クリアデスク・クリアスクリーン
書類および取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施しなければならない。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

16-1-1. 対策基準の策定

対策基準（例）

7.8 装置の設置及び保護
装置は、セキュリティを保って設置し、保護しなければならない。

7.9 構外にある資産のセキュリティ
構外にある資産を保護しなければならない。

7.10 記憶媒体
記憶媒体は、組織における分類体系および取扱いの要求事項に従って、取得、使用、移送および廃棄のライフサイクルを通して管理しなければならない。

7.11 サポートユーティリティ
情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。

7.12 ケーブル配線のセキュリティ
電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。

7.13 装置の保守
装置は、情報の可用性、完全性、機密性を維持することを確実にするために、正しく保守しなければならない。

7.14 装置のセキュリティを保った処分または再利用
記憶媒体を内蔵した装置は、処分または再利用する前に、すべての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

16-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を紹介します。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

7.1 物理的セキュリティ境界

実施手順（例）

a. 当組織は、「レイアウト図」により、セキュリティ境界を定義する。
※レイアウト図は、第13章 4.3 情報セキュリティマネジメントシステムの適用範囲の決定（3/3）の物理的境界レイアウト図（例）を参照
b. 重要な情報資産のある領域の入退を制限し、入退資格を有さない者の立ち入りを制限する。

ワンポイントアドバイス
許可されていない者の物理アクセスを防ぐために、入口に「関係者以外立入禁止」の表示や、入退制限の標識をつけるなどの工夫は効果的です。

7.2 物理的入退

実施手順（例）

a. 入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。入退資格は、従業者証またはセキュリティカードを交付することにより付与し、他人への貸借は禁じる。
b. 外来者の訪問は、原則として、「入退受付票」に氏名、身元、入退時刻を記録し、面談者が面会の確認印の押印または署名を行い、退出するまでエスコートする。
c. 宅配便などの荷物の受け取りは、各オフィスの入口より外で行うことを原則とし、例外的にオフィス内への入室を認める場合は、必ず応対者がエスコートする。

ワンポイントアドバイス
荷物の受け取り場所は、重要な情報処理設備から離れた場所に設定することが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

16-1-2. 実施手順の策定

7.3 オフィス、部屋及び施設のセキュリティ

実施手順（例）
a. 各事業場は常時施錠可能とし、入退資格のない者の立ち入りを禁じる。やむを得ず施錠可能でない事業場においては、重要な情報はキャビネットに収納し施錠するなど、厳重な管理を行う。 b. 施錠、開錠は、原則として従業者が行う。 c. 入退を許可された外来者に対しては、原則として従業者が随行し、立ち入り場所を制限する。 d. 秘密の情報または活動が外部から見えないよう、ブラインドやパーティションを設置する。
ワンポイントアドバイス 活動内容やPCのモニタなどが外部から見えたり、聞こえたりすることがないよう、外部来場者の動線ルートを事前に決めておくことが大切です。

7.4 物理的セキュリティの監視

実施手順（例）
a. 組織の施設は、監視カメラ、侵入者警報を設置し、認可されていないアクセスや、疑わしい行動を検知する。無人の領域には、必ず監視カメラおよび侵入者警報を設置する。 b. 監視カメラ、侵入者警報の動作確認をするため、3か月に1回点検を実施する。
ワンポイントアドバイス 無人の領域は、警報器を設置することが大切です。

7.5 物理的及び環境的脅威からの保護

実施手順（例）
a. 各フロアには、火災報知器、消火器を設置する。 b. サーバ付近に段ボールなどの燃えやすいものを置くことを禁じる。 c. サーバの転倒対策として設置位置を工夫する。必要に応じて、転倒防止器具を利用するなどの対策を行う。
ワンポイントアドバイス ハザードマップなどで自社の地理的な脅威を把握し、災害時における具体的対策を講じておくことが重要です。

16-1-2. 実施手順の策定

7.6 セキュリティを保つべき領域での作業

実施手順（例）

a. サーバ室には、スマートフォンやボイスレコーダー、カメラなど撮影や録音ができるものや、USBメモリなどサーバの情報をダウンロードできる機器の持ち込みは禁じる。
b. セキュリティを保つべき領域は常時施錠し、入退資格のない者の立ち入りを禁じる。

ワンポイントアドバイス
セキュリティを保つべき領域での作業ルールが適切に守られているか確認することが大切です。

7.7 クリアデスク・クリアスクリーン

実施手順（例）

a. クリアデスク
・離席時や帰宅時には、重要情報や個人情報を含む書類や記憶媒体を机上やその周辺に放置しない。
・書類やデータは、重要なものとそうでないものを区別して整理する。
・プリンタ、コピーに出力した印刷分は放置せず速やかに取り出す。
b. クリアスクリーン
・利用者は、食事やトイレ、会議などで自席を離れる場合には、コンピュータのログアウト（ログオフ）やスクリーンロックを行い、第三者がコンピュータを操作したり、画面を盗み見たりできないようにする。
・ログインID、パスワードを机上に貼付することは禁じる。

ワンポイントアドバイス
クリアデスク、クリアスクリーンについてのルールが適切に守られているか、チェックシートなどで徹底することも効果的です。

7.8 装置の設置及び保護

実施手順（例）

a. スイッチ、無線LANアクセスポイントなどは、人目につくところや通行量の多い場所を避けて設置する。
b. サーバは、サーバ室など隔離されたエリアに設置する。隔離されていないエリアに設置する場合は、ラックなどへ収容する。
c. サーバが設置されたエリアでの飲食、喫煙は禁じる。
d. サーバが設置されたエリアの温度、湿度を監視し、サーバに悪影響を与えない状態を維持する。

ワンポイントアドバイス
サーバ周辺に水などの配管などが通っていないか、確認することが大切です。

16-1-2. 実施手順の策定

7.9 構外にある資産のセキュリティ

実施手順（例）

a. 社外にノートPCなどを持ち出す場合は、
①ログインパスワードを設定する。
②必要のない機密情報、個人情報を格納しない。
③格納するファイルは暗号化する（パスワードをつける）。
④OS・ソフトウェアが最新バージョンになっており、セキュリティソフトが入っていることを確認する。
⑤ノートPCなどが入ったカバンなどを交通機関の網棚などには置かず、常時携帯する。
b. 公共交通機関を利用する際に、顧客情報や個人情報など、重要な情報をノートPCや社用携帯で閲覧することは禁じる。

ワンポイントアドバイス
公共交通機関を利用する際に、装置（例：スマートフォン、ノートPCなど）上の情報をのぞき見られるリスクから保護することが大切です。

7.10 記憶媒体

実施手順（例）

a. 外づけの記録媒体の持ち出し・持ち込みは、事前に許可を得た上で行う。また、不使用時は、キャビネットに施錠保管を行う。
b. 記憶媒体に収納する情報は必要最小限なものとし、必要のない機密情報や個人情報、会社の重要情報は保存しない。
c. 格納するファイルは暗号化して（パスワードをつけて）保存する。
d. 外部記憶媒体や、重要な情報が記された文書を机上や、棚上などに放置することは禁じる。
e. 私有の外部記憶媒体を持ち込む場合、社有の外部記憶媒体を持ち出す場合は、該当部門の責任者および情報システム管理者の許可を得る。
f. 外部記憶媒体でデータを受け渡す場合は、データの内容に応じてセキュリティを確保できるような受け渡し方法をとる。
g. お客様のUSBメモリなどの記憶媒体を預かった場合は、使用する前に必ずアンチウイルスソフトによりスキャンを行う。
h. 不要な媒体を処分する場合は、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
i. 媒体を輸送する場合は、必要に応じて梱包などにより保護するとともに、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。
j. サーバ、ネットワーク機器（スイッチ、ルータなど）の設置場所を、情報システム管理者の許可なく移動することは禁じる。
k. 当組織の資産および顧客から預かった資産を、情報セキュリティ委員長の許可なく無断で持ち出すことは禁じる。

ワンポイントアドバイス
USBメモリやハードディスクなどの記憶媒体だけでなく、紙の文書に対しても対策を行うことが大切です。

16-1-2. 実施手順の策定

7.11 サポートユーティリティ

実施手順（例）

a. 情報システム管理者は、必要に応じて無停電電源装置を設置する。無停電電源装置は、ランプの確認などにより、バッテリーの寿命が尽きていないことや、緊急時の切り替えが問題なく行えるかを定期的に確認する。
b. 情報システム管理者は、フロア（装置の設置場所）が適切な温度に保たれていることを適時確認する。

ワンポイントアドバイス
停電対策として無停電電源装置だけでなく、補助発電装備を利用することも有効です。

7.12 ケーブル配線のセキュリティ

実施手順（例）

a. 人が通る箇所のケーブル配線は、できるだけ床下か天井に配線する。床上に配線する場合には、モール、ケーブルカバーによる保護を行う。
b. 配線ケーブルに異常がないか、3か月に1回点検を行う。
c. 誤接続を防止するために、ケーブルにラベルをつける、役割ごとに色の異なるケーブルを使う。
d. ケーブル配線図を作成するとともに、機器の増設や移設で配線が変更になった場合には配線図を更新する。

ワンポイントアドバイス
周辺機器の増設や移設に際して、ケーブル類の適正化を確認することが大切です。

7.13 装置の保守

実施手順（例）

サーバ、ネットワーク機器など主要な装置は、製造元から提供されたマニュアルを参照し、製造元が推奨する頻度にて点検、保守を行い、記録する。

ワンポイントアドバイス
装置の点検・保守が定期的に実施され、記録されているか確認することが大切です。

7.14 装置のセキュリティを保った処分または再利用

実施手順（例）

a. PCを処分する場合は、従業員が各自で処理せず、情報システム管理者に処理を依頼する。情報システム管理者は、ハードディスクなどの記憶媒体については、物理的破壊もしくは、完全消去により処分する。
b. 上記以外の方法により、処分する必要があると認められる場合、事前に情報セキュリティ委員長の承認を得ることを要するものとする。
c. 情報システム管理者は、装置を再利用する場合、不要な情報を完全に消去し、またライセンス供与されたソフトウェアが消去されたことを確認の上、再利用する。

ワンポイントアドバイス
廃棄・再利用する際、情報を消去する責任者と手順を定めることが大切です。

16-2-1. BYOD（Bring Your Own Device）

関連する主な管理策
6.3、6.7、7.9、8.1、8.7

BYODの概念や、導入に向けたポイント、運用手順を説明します。

BYOD（Bring Your Own Device）

BYODとは、個人が私物として所有している端末（PCやスマートフォンなど）を業務に使う利用形態のことです。従来は、業務で使用する端末は企業が購入し、従業員に貸与することが一般的でした。しかし、使い慣れた端末を利用できる働きやすさや、端末購入コストの削減などの観点から、従業員が持つ私物のデバイスを業務に利用することが普及しました。

BYODの主なメリット・デメリット

メリット

- コスト削減
  企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入れ替えも基本的には個人負担となります。
- 使い慣れた端末の業務利用
  従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率があがります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。

デメリット

- シャドーIT
  ルールの整備や技術的な対策を講じないと、シャドーITが増加してしまう恐れがあります。
- セキュリティリスク
  個人の端末では、さまざまなWebサイトやアプリケーションを利用することがあるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなります。

BYODを運用する際のポイント

BYODを運用する際は、適切なルールを策定し、周知することが重要です。また、ルールだけでなく、技術的な対策を講じることも重要です。

運用手順（例）

a. BYODに関する使用ルールや禁止事項を決めて周知する。
b. BYODで使用する機器については管理者に申請し、許可を得る。
c. BYODで使用する機器が紛失した場合の対応フローを策定し、周知する。
d. BYODで行える業務範囲やリモートアクセスの権限を設定する。
e. 社内ネットワークへは、VPNを利用する場合のみ接続できるようにする。
f. 必要以上に業務データを蓄積させない。（保存可能なデータに関するルールを決める。）
g. 業務で使用するPCは、EDRを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。
h. 業務で使用するPCに、ファイル共有ソフトなどの不正なソフトウェアをインストールすることは禁じる。

16-2-2. MDM（Mobile Device Management）

関連する主な管理策
6.7、7.9、8.1

MDMの概念や、導入に向けたポイント、運用手順について説明します。

MDM（Mobile Device Management）

MDMとは、企業で保有しているモバイル端末 (スマート フォンやタブレットなど) を一元管理できるシステムのことです。オフィスの外にあるデバイスも管理できます。ポリシー（パスワードの長さやロック画面の解除方法、インストールできるアプリケーションの制限など）を従業員のモバイル端末に適用し、違反した場合に警告を行ったり管理者に通知したりできます。また、万が一紛失や盗難があった際には、位置情報の確認や遠隔でモバイル端末の画面をロックしたり、リモートワイプ（端末に保存されているデータを遠隔で初期化する機能）したりすることができ、機密情報を守れます。

MDMを導入する際のポイント

- ✓ コスト・費用
  MDMは導入して終わりではなく、維持費がかかります。自社の予算に合わせた確認をすることが大切です。
- ✓ 対応しているOSの確認
  すべてのOSに対応しているMDMもあれば、一部のみに対応しているMDMもあります。導入するMDMが、自社で使用している端末のOSに対応しているか確認することが大切です。
- ✓ サポート体制
  MDMの導入時や導入後の運用サポートなどが受けられるか確認することが大切です。
- ✓ 利用者の意見を反映した社内ルールの策定、およびMDMの選定
  MDMは情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。たとえば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDMによる制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定やMDMの選定を進めることが重要です。

MDMの運用手順について説明します。

運用手順（例）

a. モバイル端末の紛失・盗難時の対応
   1. 従業員は、モバイル端末を紛失・盗難にあった場合は、速やかに情報セキュリティ管理者に報告する。
   2. 情報セキュリティ管理者は、従業員からモバイル端末の紛失・盗難の報告を受けた場合、速やかにリモートでモバイル端末の画面をロックし、位置情報を確認する。
   3. 情報セキュリティ管理者は、モバイル端末の位置情報が確認できず、発見が困難であると想定される場合、リモートワイプを実施し、モバイル端末内のデータを削除する。

b. 業務で新たにアプリケーションが必要になった場合、情報セキュリティ管理者に連絡し、インストールの許可をもらう。

第17章. 技術的管理策

17-1. 技術的管理策を参考とした対策基準・実施手順の策定

17-2. 各種テーマごとの対策

章の目的
第17章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について学ぶことを目的とします。また、技術的管理策に関して、テーマごとの対策について学ぶことも目的とします。
主な達成目標
◘ 技術的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。 ◘ Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること。

17-1-1. 対策基準の策定

ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

ISO/IEC27001:2022に基づき管理策を決定する（例）　【凡例】採用：○・不採用：×

項目	採用、不採用	項目	採用、不採用
8.1 利用者エンドポイント機器		8.18 特権的なユーティリティプログラムの使用	
8.2 特権的アクセス権		8.19 運用システムに関わるソフトウェアの導入	
8.3 情報へのアクセス制限		8.20 ネットワークのセキュリティ	
8.4 ソースコードへのアクセス		8.21 ネットワークサービスのセキュリティ	
8.5 セキュリティを保った認証		8.22 ネットワークの分離	
8.6 容量・能力の管理		8.23 ウェブ・フィルタリング	
8.7 マルウェアに対する保護		8.24 暗号の使用	
8.8 技術的脆弱性の管理		8.25 セキュリティに配慮した開発のライフサイクル	
8.9 構成管理		8.26 アプリケーションのセキュリティの要求事項	
8.10 情報の削除		8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	
8.11 データマスキング		8.28 セキュリティに配慮したコーディング	
8.12 データ漏えいの防止		8.29 開発及び受入れにおけるセキュリティ試験	
8.13 情報のバックアップ		8.30 外部委託による開発	
8.14 情報処理施設の冗長性		8.31 開発環境、試験環境及び運用環境の分離	
8.15 ログ取得		8.32 変更管理	
8.16 監視活動		8.33 試験情報	
8.17 クロックの同期		8.34 監査試験中の情報システムの保護	

17-1-1. 対策基準の策定

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

対策基準（例）

8.1 利用者エンドポイント機器
利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。

8.2 特権的アクセス権
特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。

8.3 情報へのアクセス制限
情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。

8.4 ソースコードへのアクセス
ソースコード、開発ツール、ソフトウェアライブラリへの読取りおよび書込みアクセスを、適切に管理しなければならない。

8.5 セキュリティを保った認証
セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。

8.6 容量・能力の管理
現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。

8.7 マルウェアに対する保護
マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。

8.8 技術的脆弱性の管理
利用中の情報システムの技術的脆弱性に関する情報を獲得しなければならない。また、そのような脆弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

8.9 構成管理
ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立、文書化、実装、監視し、レビューしなければならない。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

17-1-1. 対策基準の策定

対策基準（例）

8.10 情報の削除
情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。

8.11 データマスキング
データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。

8.12 データ漏えいの防止
データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。

8.13 情報のバックアップ
合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。

8.14 情報処理施設の冗長性
情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。

8.15 ログ取得
活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。

8.16 監視活動
セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。

8.17 クロックの同期
組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。

8.18 特権的なユーティリティプログラムの使用
システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。

17-1-1. 対策基準の策定

対策基準（例）

8.19 運用システムに関わるソフトウェアの導入
運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。

8.20 ネットワークのセキュリティ
システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。

8.21 ネットワークサービスのセキュリティ
ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。

8.22 ネットワークの分離
情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離しなければならない。

8.23 ウェブ・フィルタリング
悪意のあるコンテンツにさらされることを減らすために、外部Webサイトへのアクセスを管理しなければならない。

8.24 暗号の使用
暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。

8.25 セキュリティに配慮した開発のライフサイクル
ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。

8.26 アプリケーションのセキュリティの要求事項
アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。

8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。

17-1-1. 対策基準の策定

対策基準（例）

8.28 セキュリティに配慮したコーディング
セキュリティに配慮したコーディングの原則を、ソフトウェア開発に適用しなければならない。

8.29 開発及び受入れにおけるセキュリティ試験
セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。

8.30 外部委託による開発
組織は、外部委託したシステム開発に関する活動を指揮、監視し、レビューしなければならない。

8.31 開発環境、試験環境及び運用環境の分離
開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。

8.32 変更管理
情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。

8.33 試験情報
テスト用情報は、適切に選定、保護、管理しなければならない。

8.34 監査試験中の情報システムの保護
運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

次ページ以降では、策定した対策基準をもとに作成する実施手順について説明します。

17-1-2. 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介します。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引の内容を参考に、自社に適した実施手順を策定してください。

8.1 利用者エンドポイント機器

実施手順（例）

a. モバイル機器を社外に持ち出す場合、ログインパスワードを設定する。
b. 必要のない機密情報、個人情報などは、モバイル機器に格納しない。
業務上必要のある機密情報や個人情報をモバイル機器に格納する場合は、暗号化する。（パスワードをつける。）
c. モバイル機器を利用者が限定されない無償のWiFiスポットなどへ接続することは禁じる。
d. 携帯電話・スマートフォンの管理
・社有の携帯電話・スマートフォン（以下「社有携帯電話など」という）を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱う。
・社有携帯電話などを使用する者は、使用者本人以外が操作できないよう、パスワードを設定して保護する。
・持ち歩く際は、ストラップをつけるなどの紛失・盗難防止策を必要に応じて講じる。
・電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮する。
・私有の携帯電話・スマートフォンを業務で使用する場合は、情報システム管理者の承認を要する。また、社有携帯電話などと同様の安全対策を実施する。
e. 利用者はノートPCに対して、パスワードつきのスクリーンセーバを設定し、のぞき見を防止する。スクリーンセーバの設定時間は10分以内とする。

ワンポイントアドバイス
利用者終端装置（携帯、スマートフォン、ノートPCなど、ユーザが情報処理サービスにアクセスするために使用するさまざまなデバイス）の取扱いに関する規則を定めることが大切です。

8.2 特権的アクセス権

実施手順（例）

a. 特権的アクセス権は特定の者に付与し、管理対象システムとその保有者を明確にする。
b. 半年に1回、または組織に何か変更があった際、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任、力量の点で今も適格であるかどうかを検証する。

ワンポイントアドバイス
特権的アクセス権は一般の利用者よりも多くの権限が付与されているため、悪用されると影響が大きいです。ID付与に際しては、厳格かつ安全な管理のもとに運用されることが大切です。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

17-1-2. 実施手順の策定

8.3 情報へのアクセス制限

実施手順（例）
a. 情報システム管理者は、取扱いに慎重を要する情報へのアクセス権限を、必要な者のみに割り当てる。 b. 未知の利用者識別情報または匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。
ワンポイントアドバイス 情報およびその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止することが大切です。

8.4 ソースコードへのアクセス

実施手順（例）
ソースコードや設計書、仕様書などの関連書類は、アクセス権で管理されたフォルダに厳重に保管する。
ワンポイントアドバイス ソースコードが変更される、または開発環境の一部のデータが認可されていない人物によって取り出される可能性をなくすため、ソースコードへのアクセスを適切に制御することが大切です。

8.5 セキュリティを保った認証

実施手順（例）
重要な情報システムにアクセスする際は、パスワードだけでなく、多要素認証を使用し、不正アクセスの可能性を減らす。
ワンポイントアドバイス 多要素認証では、知識（パスワード、秘密の質問など）、所持物（スマートフォン、ICカードなど）、生体情報（指紋、声紋など）のうち、2つ以上を組み合わせて認証することで、認可されていないアクセスの可能性を減らします。

17-1-2. 実施手順の策定

8.6 容量・能力の管理

実施手順（例）

a. 情報システム管理者は、コンピュータやネットワークの応答時間など、その負荷状況について、業務を通じて問題がないかどうかを確認する。CPUやメモリ、ハードディスクなどの外部記憶装置の使用率など、リソースの使用状況を定期的に監視する。
b. リソースの使用状況に応じてリソースの割り当てを調整すると同時に、将来必要となる容量や能力を予測し、システムのパフォーマンスを維持するため、必要なリソースを事前に確保する。
c. 情報システム管理者は、問題が発見された場合、速やかに原因の究明を行い、情報セキュリティ委員会に報告する。
d. 情報セキュリティ委員会は、情報システム管理者に対策を指示し、必要に応じて経営陣に報告する。
e. 情報システム管理者は、中長期的な業務量の増減を考慮し、将来的にシステムに必要な容量を予測し、必要であればトップマネジメントに報告する。

ワンポイントアドバイス
クラウドサービスを利用することで、特定のアプリケーションおよびサービスで利用できる資源を、要求に応じて迅速に拡張・削減することができます。

8.7 マルウェアに対する保護

実施手順（例）

a. ネットワークに接続するすべてのパソコン、サーバ上に情報システム管理者が指定したアンチウイルスソフトを導入する。
b. アンチウイルスソフトを常時設定にし、ファイルへのアクセスおよび電子メールの受信時に常時スキャンできる設定を行う。
c. 常時スキャンだけでなく情報システム管理者が指定した期間に一度、ファイル全体に対するスキャンを行う。
d. 自動でウイルス定義ファイルの更新が行われるように設定する。
e. 標的型メール対応
・メールの添付書類やメール中のリンクは、原則として（送信者に確認するなどの方法で）安全が確認できるまで開かない。
・ファイルの拡張子を表示させる設定とし、添付ファイルの拡張子が、通常使用しない内容の場合、ファイルの参照を禁じる。
通常使用しないファイルの拡張子の例：.exe、.pif、.scr

ワンポイントアドバイス
基本的な対策として、社内パソコンのウイルス定義ファイルが常に最新版に更新されているかの確認を徹底することが重要です。

17-1-2. 実施手順の策定

8.8 技術的脆弱性の管理

実施手順（例）
a. 情報セキュリティ委員会および情報システム管理者は、技術的な脆弱性のニュースを常に意識し、時期を失せず効果的に外部の攻撃を防御する。 b. OSやアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法で脆弱性に対処する。
ワンポイントアドバイス セキュリティパッチは、正当な供給元から取得したもののみを使用することが大切です。

8.9 構成管理

実施手順（例）
システムの構成要素とその相互関係を理解し管理するため、台帳や構成管理ツールを用いて、ハードウェア、ソフトウェア、ネットワーク機器、設定ファイルなど、システムを構成するすべての要素の情報を把握する。
ワンポイントアドバイス ハードウェア・ソフトウェア・サービス・ネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更や誤った変更によって構成が変えられないようにすることが大切です。

8.10 情報の削除

実施手順（例）
a. 業務上必要がなくなったデータは速やかに削除する。 b. 記憶媒体上のデータを削除する際は、データ消去ソフトを使用し、復元できないよう、完全に削除する。 c. ハードディスクを廃棄する際は、磁気データ消去装置を用いてハードディスクのデータを削除してから廃棄する。
ワンポイントアドバイス 取扱いに慎重を要する情報などの機密情報については、必要がなくなった時点で速やかに削除することが大切です。情報を保有していることがリスクなので、不要な情報は持ちつづけないことが重要です。

8.11 データマスキング

実施手順（例）
保有している情報をマーケティング分析などの目的で二次利用する場合には、個人情報や重要情報が推測できない形に加工した上で利用する。
ワンポイントアドバイス 取扱いに慎重を要するデータ（個人情報や重要情報）の保護が必要である場合、データマスキング・仮名化・匿名化などの手法を使用して保護することが大切です。これにより、データが万が一漏えいしても、その内容を第三者に理解されることを防げます。

17-1-2. 実施手順の策定

8.12 データ漏えいの防止

実施手順（例）
a. 漏えいから保護する情報を特定し、分類する。 b. ファイル共有ソフトの使用を禁じる。 c. 重要な情報が画面に表示されている場合は、スクリーンショットや写真を撮ることを禁じる。 d. ファイアウォールやIDS、IPSなどによって不正アクセスを防止する。「8.20 ネットワークのセキュリティ」に従う。 e. 重要データについてアクセス制限を設ける。「8.3 情報へのアクセス制限」に従う。 f. 重要データは暗号化して保管する。「8.24 暗号の使用」に従う。
ワンポイントアドバイス 個人やシステムによる情報の認可されていない開示・抽出を検出し、防止することが大切です。

8.13 情報のバックアップ

実施手順（例）
a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてシステムおよびデータのバックアップを行う。 b. バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。 c. 情報システム管理者は、バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。
ワンポイントアドバイス クラウドサービスを利用している場合は、クラウド環境にあるデータのバックアップも作成しているか確認することが大切です。ランサムウェア対策として、バックアップは2つ作成し、1つはネットワークから隔離したオフサイトで保管することが大切です。

8.14 情報処理施設の冗長性

実施手順（例）
a. 情報システムは、可用性に関する業務上の要求事項を明確にし、必要に応じて予備の機器を用意して二重化を行い、冗長性をもたせる。 b. 緊急の場合、速やかに予備の機器に切り替えられるよう、動作確認を月に1回行う。
ワンポイントアドバイス 冗長な構成要素および処理活動を常に作動させておくか、緊急の場合に自動または手動で作動させるかを確認します。常に作動させておく場合は、稼動状況を確認することが大切です。

17-1-2. 実施手順の策定

8.15 ログ取得

実施手順（例）
a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてログの取得を行う。 b. 情報システム管理者は、必要に応じてログの定期的なチェックを行う。 c. ログは、情報システム管理者またはその指名する担当がアクセスできるようにする。 d. 情報システム管理者は、運用担当者がサーバで行った作業を確認する。確認は、作業ログ、または日報・サーバ作業記録の閲覧により行う。
ワンポイントアドバイス セキュリティインシデントの分析、警告および調査のために、システム間のログを相関づけられるようにすべてのシステムが同期した時刻源（8.17 クロックの同期を参照）を持つことが重要です。

8.16 監視活動

実施手順（例）
a. ファイアウォール・IDS・IPSのログを常に監視し、異常な動作を検知した場合は速やかに対応する。
ワンポイントアドバイス 通常時およびピーク時のシステムの使用率や、各利用者または利用者グループの通常のアクセス時間・アクセス場所・アクセス頻度を考慮して正常な行動・動作の基準を確立し、基準に照らして異常を監視することが大切です。

8.17 クロックの同期

実施手順（例）
a. 情報システム管理者は、クライアントPCやサーバなどすべての情報システムのクロックを同期させる。 b. すべての情報システムのクロックを同期させるために、NTPを使用する。
ワンポイントアドバイス イベントログは、調査や法令や懲戒が関わる場合の証拠として必要となる可能性があり、不正確な監査ログは証拠の信頼性を損なう可能性があります。コンピュータ内のクロックを正しく設定し、イベントログの正確さを確実にすることが重要です。

17-1-2. 実施手順の策定

8.18 特権的なユーティリティプログラムの使用

実施手順（例）

a. ユーティリティプログラムの使用は、原則としてOS標準機能のみ許可する。
b. その他のユーティリティプログラムが必要となった場合は、情報システム管理者の承認を得た上で利用する。

ワンポイントアドバイス

情報システムの大半には、パッチ適用・ウイルス対策・バックアップ・ネットワークツールなど、システムやアプリケーションによる制御を無効にできる1つ以上のユーティリティプログラムが組み込まれています。不要なユーティリティプログラムは、すべて除去・無効化することが大切です。また、特権的ユーティリティのなかには、データベースの中身を、その整合性を気にすることなく強制的に書き換えることができる機能や、他の利用者の権限でデータを操作できる機能をもったものがあります。こうした特権的なユーティリティを野放しにすると組織の情報セキュリティが保てなくなるため、厳しく利用を管理する必要があります。

8.19 運用システムに関わるソフトウェアの導入

実施手順（例）

a. 運用システムに、開発用のコードを導入しない。
b. PCを含む社内の情報システムで使用するソフトウェアは、原則情報システム管理者によって指定されたもののみ使用し、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。他社が開発したソフトウェアを利用する場合、その開発会社が要求している条件やスペックを満たす環境で運用する。
c. 情報システム管理者は、利用者がインストール可能なソフトウェアを定期的に見直す。
d. 利用者は認可されていないソフトウェアをインストールしてはならず、業務上、必要な場合は、情報システム管理者の承認を得た上でインストールする。
e. ファイル共有ソフトなど、ウイルス感染や不正アクセスなどの原因となりやすいソフトウェアのインストールを禁じる。

ワンポイントアドバイス

組織は、利用者がインストールできるソフトウェアの種類について、厳密な規則を定めて施行することが大切です。

17-1-2. 実施手順の策定

8.20 ネットワークのセキュリティ

実施手順（例）
a. ネットワーク図および装置（例：ルータ、スイッチ）の構成ファイルを含む文書を最新に維持する。 b. 社内ネットワークへ接続する際は、情報システム管理者の承認を受け、指示された手順に従う。 c. 情報システム管理者は、ネットワークにおける社外との境界にはファイアウォールを設けるなど、不正侵入対策を施す。 d. ネットワーク装置のファームウェアの定期的なアップデートを行う。 e. 他人のID、パスワードで、社内ネットワークに接続することを禁じる。 f. 一旦、社内ネットワークから切り離したパソコンなどは、ウイルスチェックなどの安全確認を行ってから再接続する。 g. 持ち込みおよび私有PC利用の場合は、社内ネットワークに接続しない。やむを得ず接続する場合は、情報システム管理者が指定するソフトウェアによりウイルスチェックを行う。 h. 無線LANを使用する場合は、情報システム管理者の承認を得て、暗号化、接続パソコンの認証など、十分な安全対策を実施する。 i. 不特定が利用できる公衆無線LANやWiFiスポットに接続することは禁じる。
ワンポイントアドバイス ネットワークや、ネットワークをサポートする情報処理施設における情報を、ネットワークを通じた危険から保護することが大切です。

8.21 ネットワークサービスのセキュリティ

実施手順（例）
a. 利用しているネットワークサービスを特定する。 b. 情報システム管理者は、ネットワークサービスを利用する場合は、ネットワークサービス提供者とSLAを締結する。
ワンポイントアドバイス ネットワークサービスには、接続・プライベートネットワークサービスおよびネットワークセキュリティ管理のためのソリューション（ファイアウォール、IDSなど）が含まれます。

8.22 ネットワークの分離

実施手順（例）
a. インターネットと社内LANとの境界にファイアウォールを設置する。 b. メール、Webサーバなどの公開サーバは、社内のネットワークと分離する。 c. ゲスト用の無線アクセスネットワークを、社内用の無線アクセスネットワークから分離する。
ワンポイントアドバイス 各領域の境界は、明確に定めることが大切です。ネットワーク領域間のアクセスが認められる場合は、境界にファイアウォールなどを設けて制御することが大切です。

17-1-2. 実施手順の策定

8.23 ウェブ・フィルタリング

実施手順（例）
フィルタリングソフトを利用し、業務上不必要なWebサイト、危険性のあるWebサイトへのアクセスを防ぐ。
ワンポイントアドバイス システムがマルウェアによって危険にさらされることを防ぐために、認可されていないウェブ資源へのアクセスを防止することが大切です。

8.24 暗号の使用

実施手順（例）
a. 暗号利用のための規則 ・SSL/TLS 当組織のWebサイトの通信は、SSL/TLSを用いて暗号化する。 ・無線LAN 無線LANの通信は暗号化し、暗号化の規格は脆弱性の報告されていない安全な方法とする。 b. 鍵の管理 ・SSL/TLS 情報システム管理者は、証明書に対する秘密鍵を適切に管理する。 ・無線LAN アクセスポイントの管理者画面は、情報システム管理者のみがアクセスでき、そのパスワードを厳重に管理する。 c. 重要データの暗号化 ・暗号化の対象とするデータを選定する。 ・利用する暗号の種類を決める。 ・暗号鍵のライフサイクルに関する方針を策定する。 ・暗号の管理責任者を定める。
ワンポイントアドバイス 業務や情報セキュリティ要求事項に従い、暗号に関連する法令・規制・契約上の要求事項を考慮し、情報の機密性・真正性・完全性を保護するための暗号の適切かつ効果的な使用を確実に履行することが大切です。

17-1-2. 実施手順の策定

8.25 セキュリティに配慮した開発のライフサイクル

実施手順（例）

セキュリティに配慮した開発のための方針を以下に記す。
a. 開発の初期段階でセキュリティ要件を明確化する。
b. 開発環境は、「8.31 開発環境、試験環境及び運用環境の分離」の「b. セキュリティに配慮した開発環境」に従う。
c. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
d. 開発したシステムに脆弱性がないかテストする。
e. 開発ドキュメント（仕様書、設計書、テスト仕様など）は、必要最低限の者だけがアクセスできるようにする。
f. 受託開発または客先への派遣による開発では、クライアントから提示のあったセキュリティの方針・ルールなどに従う。

ワンポイントアドバイス
ソフトウェアやシステムのセキュリティに配慮した開発のための規則を定めることが大切です。

8.26 アプリケーションのセキュリティの要求事項

実施手順（例）

a. アプリケーションを取得する際、リスクアセスメントを通じてアプリケーションの情報セキュリティ要求事項を決定する。必要に応じて、情報セキュリティの専門家の支援を受け、情報セキュリティ要求事項を決定する。
b. セキュリティに配慮したシステムを構築するための原則は、以下の通りとする。
・情報セキュリティ事象を防止・検知し、対応するために必要な管理策を分析すること。
・情報セキュリティ要求事項を満たすための費用・時間・複雑さを考慮すること。

ワンポイントアドバイス
ネットワークを介してアクセス可能なアプリケーションは、ネットワークに関連した脅威を受けやすいため、リスクアセスメントの実施や、管理策を決定することが大切です。

8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

実施手順（例）

a. 社内使用の情報システムおよび外部向けに提供する情報システムの開発に際しては、情報セキュリティ事項を明確にし、要件定義として記録する。
b. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
c. 開発したシステムに脆弱性がないかテストする。

ワンポイントアドバイス
セキュリティに配慮したシステム構築の原則および確立した構築手順は、構築プロセスにおけるセキュリティレベルの向上に有効に寄与していることを確実にするため、定期的にレビューすることが大切です。

17-1-2. 実施手順の策定

8.28 セキュリティに配慮したコーディング

実施手順（例）

a. ユーザが入力したデータを確認し、問題がある場合は読み込まないようにする。
b. セキュリティ上の問題を発見しやすくするため、設計は可能な限りシンプルにする。
c. ユーザには必要最小限の権限・機能を与える。
d. 他のシステムに送信するデータは、サニタイズ（特殊文字を一般的な文字に変換すること）を行い、不正操作を防止する。

ワンポイントアドバイス
コーディングの原則が定められていない場合、コードの書き方がバラバラになり、コードが読みづらく、脆弱性が生まれる危険性があります。セキュリティに配慮したコーディングの規則を定め、コードの書き方を統一することが大切です。

8.29 開発及び受入れにおけるセキュリティ試験

実施手順（例）

a. 情報システムのセキュリティテストは、運用に移行する前に行う。
b. システムの受入れ試験
・情報システムの導入または改修の際は、受入れ時に動作確認を行う。
・必要に応じて受入れテストの仕様書を作成し、確認を行う。
・必要に応じて、コード分析ツールや脆弱性スキャナのような自動化ツールを利用し、セキュリティに関連する欠陥を修正する。
・受入れ試験の結果は、受入れ部門の管理者および情報システム管理者が承認する。

ワンポイントアドバイス
効果的な試験を確実にするために、試験環境、ツール、技術の試験および監視も考慮する必要があります。

8.30 外部委託による開発

実施手順（例）

情報システムの開発を外部に委託する場合の手順は以下に従う。
a. 「委託先審査票」によって委託先を評価、選定、およびあらかじめ定められた頻度（最低年1回）で再審査し、また、契約の履行状況を監視する。
b. 委託先との契約を締結する。（契約書には情報セキュリティ要求事項を含める。）
c. 成果物の品質および正確さを評価するため、「8.29 開発及び受入れにおけるセキュリティ試験」に定める「b. システムの受入れ試験」を実施する。

ワンポイントアドバイス
外部委託したシステム開発に関する活動を随時、指導、監視およびレビューすることが大切です。

17-1-2. 実施手順の策定

8.31 開発環境、試験環境及び運用環境の分離

実施手順（例）

a. 情報システムの開発に際しては、開発・テスト環境と本番環境を、物理的・論理的に分割する。
b. セキュリティに配慮した開発環境
・開発は、開発業務を行わない従業員から分離した場所およびシステムにて行う。また開発環境は、運用環境から分離する。
・ソースコードおよび設定ファイルは、不意の消去や改ざんから保護するため、必要最小限の者だけがアクセスできるようにする。

ワンポイントアドバイス
開発および運用環境に変更を加える際は、組織としての事前レビューおよび承認を徹底することが大切です。

8.32 変更管理

実施手順（例）

a. 変更管理は以下のプロセスで行う。
    1. 変更の承認
    変更を行う前にその変更の必要性、変更が及ぼす影響、変更によるリスクの変動について評価し、情報システム管理者の承認を得る。
    2. 変更のテスト
    変更を適用する前に、情報システムへの影響を確認するためにテストを行う。
    3. 変更の監査
    変更後に変更が適切に行われたかどうかを監査によって確認する。
b. 情報システム管理者は、サーバに周辺機器を接続する場合や、サービスパックを適用する場合、事前に情報収集し、問題の有無を確認する。万が一、適用後に問題が生じた場合は、再インストールすることで問題解決を即座に実施する。
c. OSやパッケージソフトを変更する際は、情報システム管理者はテスト機や予備機を用いて、現在の情報システムが変更後のOS上で問題なく動作するかを検証する。
d. パッケージソフトウェアのカスタマイズを原則として禁じる。万が一、修正を行う場合は、動作上の影響およびベンダーから将来的に受けるサポートへの影響を考慮し、情報システム管理者の許可を得る。

ワンポイントアドバイス
変更管理手順は、情報の機密性、完全性、可用性を確実にするために、設計の初期段階からその後のすべての保守作業までのシステム開発のライフサイクル全体にわたって文書化し、実装することが大切です。

17-1-2. 実施手順の策定

8.33 試験情報

実施手順（例）
a. テストデータとして個人情報を使用することを禁じる。 b. 実データをテストデータとして使用する場合は、情報システム管理者の承認を得てから使用する。テスト終了後は、実データを直ちに削除し、情報システム管理者に対して報告する。
ワンポイントアドバイス テストデータは、注意深く選定し、保護し、管理することが大切です。

8.34 監査試験中の情報システムの保護

実施手順（例）
a. 情報システムの監査は、システム停止のリスクを考慮し、営業時間外もしくは休日を利用して実施することを原則とする。 b. 情報システムのメンテナンスなどにより情報システムの稼動を停止する場合は、業務への影響を及ぼさない範囲または時間帯で行うように計画する。
ワンポイントアドバイス 運用システムのアセスメントを伴う監査活動およびその他の保証活動を計画し、試験者と管理層の間で合意することが大切です。

17-2-1. Security by Design

関連する主な管理策
5.1、5.7、5.9、5.19、5.20、5.24、5.26~5.29、5.37、8.9、8.15、8.16、8.22、8.25~8.34

Security by Designとは「情報セキュリティを企画、設計段階から組み込むための方策」で、開発プロセスの早い段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。従来のように、後づけでセキュリティ機能を追加したり、システムの導入直前に脆弱性診断などを実行したりする方法の場合、手戻りが多発することがあり、結果的に開発コストが増大する可能性があります。設計・企画段階からセキュリティ対策を行うことで、手戻りが少なくなり、コストの削減につながり、保守性のよいシステム・ソフトウェアになります。

図58. セキュリティ対策の実施タイミング

Security by Design導入のメリット
- 手戻りが少なくなり、納期を守れる
- コストを削減できる
- 保守性の高いソフトウェアができる

17-2-1. Security by Design

Security by Designの工程ごとに実施内容を紹介します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
セキュリティリスク分析 • システムで取扱う重要情報、アクター、実施業務、他システムとの連携方法など、システムで取扱う重要情報のフローやライフサイクルが分かる内容を記載したシステムプロファイルの作成 • システムプロファイルに基づくセキュリティ脅威の特定 • セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施 • リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソースなど）	• 5.1 情報セキュリティのための方針群 • 5.9 情報及びその他の関連資産の目録
セキュリティ要件定義 • 遵守すべきセキュリティ標準（セキュリティベースライン）や、詳細リスク分析結果などに基づいた、システムとして満たすべきセキュリティ要件の定義（機能、機能面）	• 8.26 アプリケーションのセキュリティの要求事項
セキュア調達 • セキュリティ要件に基づき、調達仕様書のセキュリティ仕様策定 • セキュリティ仕様に関する、委託先との責任範囲の明確化 • 委託先に求めるセキュリティ管理基準の策定 • セキュリティ仕様を満たす能力を有した安全な委託先の選定 • 不正侵入の経路となるバックドアなどが含まれていない、サポートを受けられる安全なプロダクトの選定	• 5.19 供給者関係における情報セキュリティ • 5.20 供給者との合意における情報セキュリティの取扱い
セキュリティ設計 • セキュリティ設計の実施 ➢ アプリケーションセキュリティ ➢ OSセキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ ➢ セキュリティ運用（平時、有事）	• 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
セキュリティ実装 • 設計に基づくシステムにおけるセキュリティ機能の実装 • セキュリティ設計に基づくアプリケーションのセキュアコーディング • セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施 ➢ OS セキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ	• 8.28 セキュリティに配慮したコーディング

17-2-1. Security by Design

実施手順（例）	選択すべき管理策（例）
セキュリティテスト • セキュリティ機能テストの実施 ➢ 単体テスト ➢ 結合テスト ➢ システムテストなど • 脆弱性診断の実施 ➢ Webアプリケーション脆弱性診断 ➢ プラットフォーム脆弱性診断 ➢ スマートフォンアプリケーション診断 ➢ 高度セキュリティ診断（ペネトレーションテストなど） ➢ 機能テストで検出されたバグの是正対応 ➢ 脆弱性診断で検出された脆弱性に対するリスクベースの是正対応	• 8.29 開発及び受入れにおけるセキュリティ試験 • 8.33 試験情報 • 8.34 監査試験中の情報システムの保護
セキュリティ運用準備 • セキュリティ運用体制の確立 • 下記項目に対応したセキュリティ運用手順の整備 ➢ 平時の運用 ✓ 構成管理、変更管理 ✓ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ✓ 脅威情報収集、自システムへの影響分析 ✓ CVSSなどに基づくリスクに応じた脆弱性対応 ✓ 定期的な脆弱性診断の実施 ➢ 有事の運用 ✓ インシデント対応 • 有事を想定したセキュリティ運用訓練の実施	• 5.24 情報セキュリティインシデント管理の計画及び準備 • 5.29 事業の中断・阻害時の情報セキュリティ • 8.9 構成管理 • 8.32 変更管理 • 8.19 運用システムに関わるソフトウェアの導入
セキュリティ運用 • セキュリティ運用の実施 ➢ 平時の運用 ✓ 構成管理、変更管理 ✓ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ✓ 脅威情報収集、自システムへの影響分析 ✓ CVSSなどに基づくリスクに応じた脆弱性対応 ✓ 定期的な脆弱性診断の実施 ➢ 有事の運用 ✓ インシデント対応	• 5.7 脅威インテリジェンス • 5.26 情報セキュリティインシデントへの対応 • 5.29 事業の中断・阻害時の情報セキュリティ • 5.37 操作手順書 • 8.9 構成管理 • 8.15 ログ取得 • 8.16 監視活動 • 8.32 変更管理

詳細理解のため参考となる文献（参考文献）	
セキュリティ・バイ・デザイン導入指南書	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf
政府情報システムにおけるセキュリティ・バイ・デザインガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2a169f83/20220630_resources_standard_guidelines_guidelines_01.pdf

17-2-2. ゼロトラスト・境界防御モデル

関連する主な管理策
5.9、5.15~5.23、5.29~5.30、8.1~8.3、8.15~8.16、8.21、8.32

ゼロトラストの定義
ゼロトラスト（ZT）は、ネットワークが侵害されている場合であっても、情報システムやサービスにおいて、各リクエストを正確かつ最小の権限となるようにアクセス判断する際の不確実性を最小化するために設計された概念とアイデアの集合体のことです。

境界防御モデルとゼロトラストの違い
　境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、組織が守るべき情報資産は信用する境界内部に存在するという前提をもとに、境界線でセキュリティ対策を講じることで、境界外部からの脅威を防ぐという考え方です。
　一方、ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。

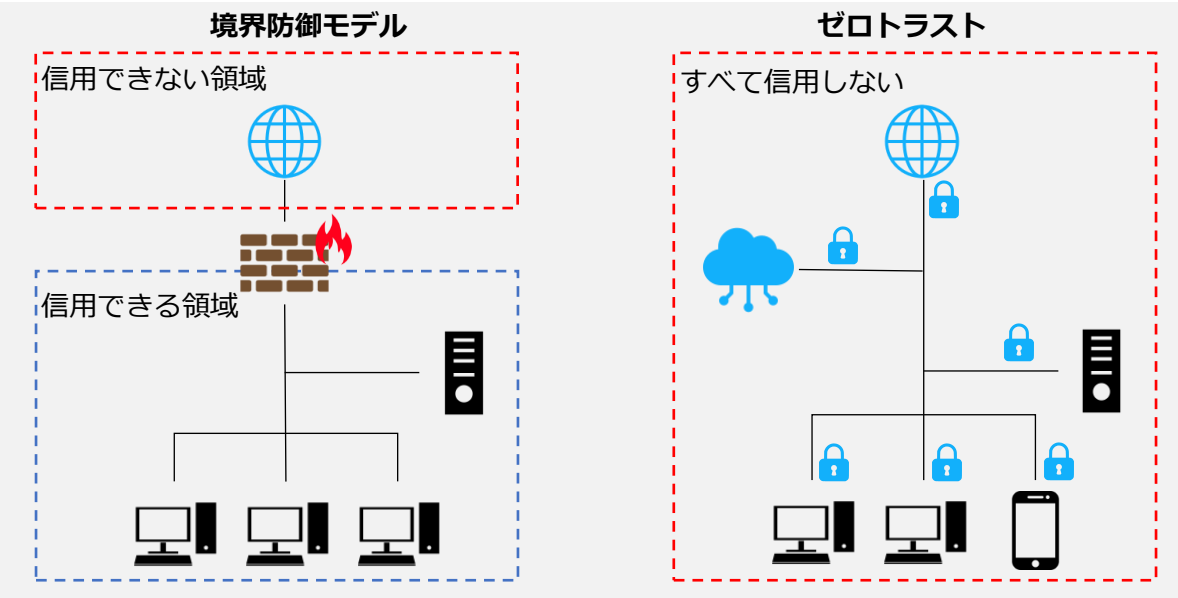


図59. 境界防御モデルとゼロトラストの概要図

　現在、クラウドサービスの普及やモバイル端末の活用、テレワークによる働き方の多様化により、内部と外部を隔てる「境界」そのものが曖昧になりつつあります。その結果、従来の社内・社外の境界でセキュリティ対策を行う「境界防御モデル」では、サイバー攻撃やマルウェア感染などの脅威から情報資産を守ることが難しくなってきています。こうした問題を解決するものとして、「ゼロトラスト」という考え方が注目されています。

One Point

ゼロトラストと境界防御の関係
　ゼロトラストは、境界防御モデルで守ることが困難な脅威に対して適用する対策ではあるものの、「境界防御モデルを排除する考え」ではありません。強固なセキュリティを構築するにあたり、すでに用いられている境界防御モデルを活かすことが大切です。

17-2-2. ゼロトラスト・境界防御モデル

ゼロトラスト導入に向けた進め方

準備工程

ゼロトラストを導入する準備として、資産 (デバイスやネットワークなど) 、主体 (ユーザ・権限など) 、ビジネスプロセスについて詳細に理解する必要があります。ゼロトラストを導入する準備として、資産、主体、データフロー、ワークフローの調査を行います。

ゼロトラスト導入プロセス

準備工程を実施した以降は、次のプロセスで進めます。

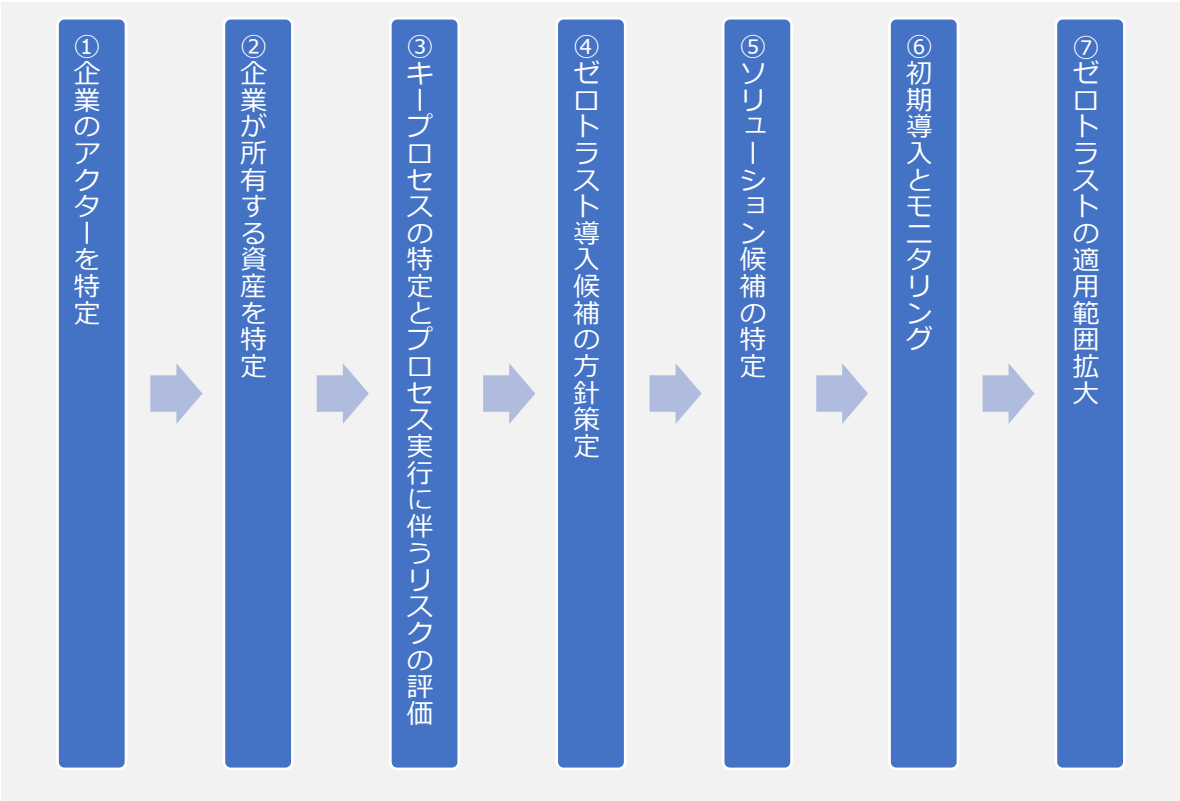


図60. ゼロトラスト導入プロセス
（出典）IPA「ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～ 」を基に作成

詳細理解のため参考となる文献（参考文献）	
ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

17-2-2. ゼロトラスト・境界防御モデル

ゼロトラスト導入の各プロセスで実施すべき内容を説明します。

① 企業のアクターを特定

企業の主体には、ユーザに紐づいたアカウントと、サービスに紐づいたアカウントの両方が含まれることがあります。どのユーザにどのレベルの権限を与えるのかは精査が必要です。基本的には、必要な対象に必要な権限だけ与えるという最小権限の考え方で整理します。

② 企業が所有する資産を特定

ゼロトラスト・アーキテクチャ（ゼロトラストの概念を利用し、コンポーネントの関係、ワークフロー計画、アクセスポリシーなどを含むサイバーセキュリティ計画のこと ）は、デバイスを識別して管理する機能が必要であり、企業内のデバイスはもちろん、企業所有ではないデバイスについても識別し、監視する機能が必要です。よって、企業の情報にアクセスするデバイスについては、「シャドーIT」も含めて可能な限り資産化する必要があります。なお、企業によって可視化されているもの (例：MACアドレス、IPアドレス) と、管理者のデータ入力による追加分も含まれます。

③ キープロセスの特定とプロセス実行に伴うリスクの評価

業務プロセス、データフロー、および組織のミッションにおけるそれらの関係（プロセス）を特定します。次に信用度レベルをつけ、ゼロトラストへ移行するプロセスを決めます。認証・認可の判断を導入することによる失敗のリスクを考慮し、初めはビジネスインパクトの低いビジネスプロセスから開始するとよいでしょう。ある程度、認証・認可の挙動を掴んでから対象を広げていくことで、リスクを抑えることができます。

④ ゼロトラスト導入候補の方針策定

資産またはワークフローを特定したら、影響を受ける対象をすべて特定します。（上流リソース (例:ID管理システム) 、下流リソース (例:セキュリティ監視) 、エンティティ (例:主体ユーザ))。次に企業管理者は、候補となるビジネスプロセスで使用されるリソースの信用度レベルの重みを決定します。それらを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定します。

⑤ ソリューション候補を特定

④で策定した内容をもとに、導入箇所に適するソリューション、製品を検討します。製品、ソリューションについては後述します。

⑥ 初期導入とモニタリング

初期導入時には、適用したポリシーや初期動作の確認を含め、監視モードで運用することが推奨されます。初期導入後はしばらくシステムの動作を監視し、必要に応じて、システムの安全性を保ちつつ、業務効率を最大化するために調整を行います。

⑦ ゼロトラストの適用箇所拡大

運用フェーズに入ったら、ネットワークや資産の監視は継続し、トラフィックの記録を行います。これらを実施していくなかで、ポリシーの変更や適用箇所の拡大を適宜実施していきます。ポリシー変更などを実施する場合は、深刻な問題にならないように行います。

17-2-2. ゼロトラスト・境界防御モデル

ゼロトラスト導入に向けた実施手順（例）

「ゼロトラスト導入に向けた進め方」で説明したプロセスをもとに、ゼロトラストを導入するための実施手順を、例を用いて説明します。また、実施手順を策定する上で、選択すべき管理策の例を紹介します。

実施手順（例）	選択すべき管理策（例）
準備工程 新たに導入する必要のあるプロセスやシステムを判断することおよびアクセスの認証・認可を正しく行うため、現在の運用状況を把握する。 a. 情報システム管理者は、次の事項を調査し、詳細に理解する。 ・資産 (デバイスやネットワークなど) ・主体 (ユーザ・権限など) b. 経営者は、次の事項を調査し、詳細に理解する。 ・ビジネスプロセス	• 5.9 情報及びその他の関連資産の目録 • 5.16 識別情報の管理 • 5.18 アクセス権 • 8.2 特権的アクセス権
① 企業のアクターを特定 a. 情報システム管理者は、業務に必要な者のみ情報へアクセスできる権限を与える。 b. アクセス権限および操作権限は、認められた場合以外は与えないようにする。	• 5.15 アクセス制御 • 5.16 識別情報の管理 • 5.17 認証情報 • 5.18 アクセス権 • 8.2 特権的アクセス権 • 8.3 情報へのアクセス制限
② 企業が所有する資産を特定 デバイスを識別して管理する。 a. 企業の情報にアクセスするデバイスは、シャドーITを含めて、すべて識別して管理する。 b. シャドーITは可能な限り資産化する。	• 5.9 情報及びその他の関連資産の目録 • 8.1 利用者終端装置
③ キープロセスの特定とプロセス実行に伴うリスクの評価 a. 業務プロセス、データフロー、組織のミッションにおける業務プロセスとデータフローの関係（プロセス）を特定する。 b. 特定したプロセスのうち、ゼロトラストに移行するプロセスを決定する。 認証・認可の判断を導入することによる失敗のリスクを考慮し、初めは組織の事業に与える影響が低いビジネスプロセスを選択し、徐々に対象を広げる。	• 5.29 事業の中断・阻害時の情報セキュリティ • 5.30 事業継続のためのICT の備え

17-2-2. ゼロトラスト・境界防御モデル

実施手順（例）	選択すべき管理策（例）
④ ゼロトラスト導入候補の方針策定 a. 資産、プロセスの特定後、ゼロトラストの導入により影響を受ける対象をすべて特定する。 ・上流リソース（例:ID管理システム） ・下流リソース（例:セキュリティ監視） ・エンティティ（例:主体ユーザ） b. ゼロトラスト導入候補となるビジネスプロセスで使用されるリソースの重要さを決定する。 c. リソースの重要さを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定する。	• 5.9 情報及びその他の関連資産の目録
⑤ ソリューション候補を特定 ④で策定した内容をもとに、導入箇所に適するソリューションを検討する。	• 5.19 供給者関係における情報セキュリティ • 5.20 供給者との合意における情報セキュリティの取扱い • 5.21 ICTサプライチェーンにおける情報セキュリティの管理 • 5.22 供給者のサービス提供の監視、レビュー及び変更管理 • 5.23 クラウドサービスの利用における情報セキュリティ • 8.21 ネットワークサービスのセキュリティ
⑥ 初期導入とモニタリング a. ソリューションの初期導入時は、実際に通信の遮断は行わず、適用したポリシーや初期動作の確認を行う。 b. 動作に問題がないことを確認後、運用を開始する。	• 8.16 監視活動
⑦ ゼロトラストの適用箇所拡大 a. 運用開始後は、ネットワークや資産の監視は継続しつつ、トラフィックの記録を行う。 b. トラフィックを記録していくなかで、ポリシーの変更や適用箇所の拡大を適宜実施する。 c. ポリシー変更を実施する場合は、影響が問題にならないように確認する。	• 8.15 ログ取得 • 8.16 監視活動 • 8.32 変更管理

17-2-2. ゼロトラスト・境界防御モデル

ゼロトラストを実装するための主な技術要素

ゼロトラストを実装するために必要となる主な技術要素（製品、ソリューション）について説明します。

CASB（Cloud Access Security Broker）

CASBとは、クラウドサービスの利活用における情報セキュリティのコンセプトですが、それを実装した製品もCASBと呼ばれます。CASBは、以下の4つの機能を備えています。

- 可視化
  クラウドストレージへの不審なアップロードやダウンロードの監視や、シャドーITの検知を行います。
- データセキュリティ
  アクセス権限の逸脱や機密情報の持ち出しをチェックし、ブロックします。
- コンプライアンス
  セキュリティに関する基準やポリシーを満たしていることを監査します。
- 脅威防御
  セキュリティ脅威の検出、分析や防御を行います。

SWG (Secure Web Gateway)

SWGは、外部ネットワークへのすべてのアクセスを中継することで、危険なコンテンツをブロック・フィルタリングするセキュリティ製品です。物理的なアプライアンスとして提供されるものもありますが、クラウド型のソリューションが一般的です。利用者のリスクの高い行為や許可されていない操作をブロックして、エンドポイントデバイスと社内ネットワークの安全性を保ちます。SWGの主な機能は、次の通りです。

- リスクの高いURLやIPアドレスへのアクセスの遮断
- マルウェアの検出とブロック
- アプリケーション制御

ZTNA（Zero Trust Network Access）

ZTNAは、ユーザ認証によって、特定のサービスやアプリケーションへの安全なアクセスを提供する仕組みです。VPNと異なり、ネットワーク全体へのアクセスを許可するのではなく、特定のサービスやアプリケーションのみの利用を許可します（ユーザが許可されていないサービスなどは表示されず、利用もできません）。必要最小限の権限を付与することで、セキュリティを向上することができます。

FWaaS（Firewall as a Service）

FWaaSとは、ファイアウォールやその他ネットワークセキュリティの機能をクラウドサービスで提供するソリューションです。URLフィルタリングやIPS、アプリケーション制御の機能を持ち、セキュリティを高めます。FWaaSは、オンプレミス型のファイアウォールよりもネットワークの変更に柔軟に対応できます。

SDP (Software Defined Perimeter)

SDPの機能はほぼZTNAと同じで、ユーザに特定のサービスやアプリケーションへの安全なリモートアクセスを提供します。SDPは、ネットワークの内部と外部の境界（Perimeter）をソフトウェア上で構築、集中的に制御し、アクセス制御に関わる設定を柔軟に動的に変更することにより安全にデータを転送する技術のことです。従来のファイアウォールの概念をソフトウェア上に持ち、利用者がどこにいても動的にアクセスを制御します。

17-2-2. ゼロトラスト・境界防御モデル

SASE (Secure Access Service Edge)

SASEとは、「ネットワーク機能」と「セキュリティ機能」をまとめて提供する仕組みです。「ネットワーク機能」と、接続の安全性を確保する「セキュリティ機能」をまとめて1製品として提供します。

SASEに含まれる主な機能に以下のものがあります。

ネットワーク機能
- SD-WAN（Software Defined - Wide Area Network）
  ※SD-WANについては、「17-2-3. ネットワーク制御」で説明します。

セキュリティ機能
- SWG（Secure Web Gateway）
- CASB（Cloud Access Security Broker）
- FWaaS（Firewall as a Service）
- ZTNA（Zero Trust Network Access）

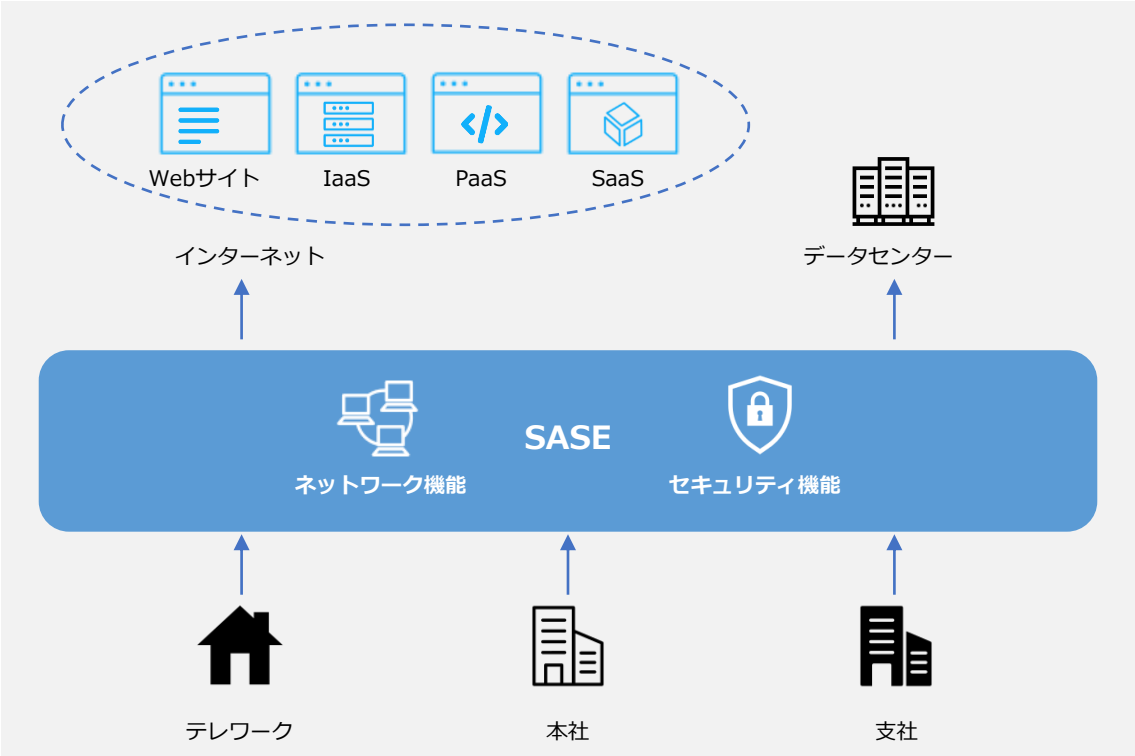


図61. SASEのイメージ図

17-2-2. ゼロトラスト・境界防御モデル

ゼロトラスト導入事例

概要

地方銀行は、個人顧客向けサービス以外にも、法人顧客向けサービスの充実を図っています。法人向け営業力強化の方策の1つとして、営業職員にモバイル端末を配布し、場所を問わずに行内システムにアクセスを可能にすることになりました。そこで、高いセキュリティが求められる金融機関のリモートアクセス環境として、ゼロトラストネットワークアクセス機能を備えた「ZTNA」を導入しました。結果、安全で安定したリモートアクセスが可能となり、業務効率化と営業力強化を実現しました。

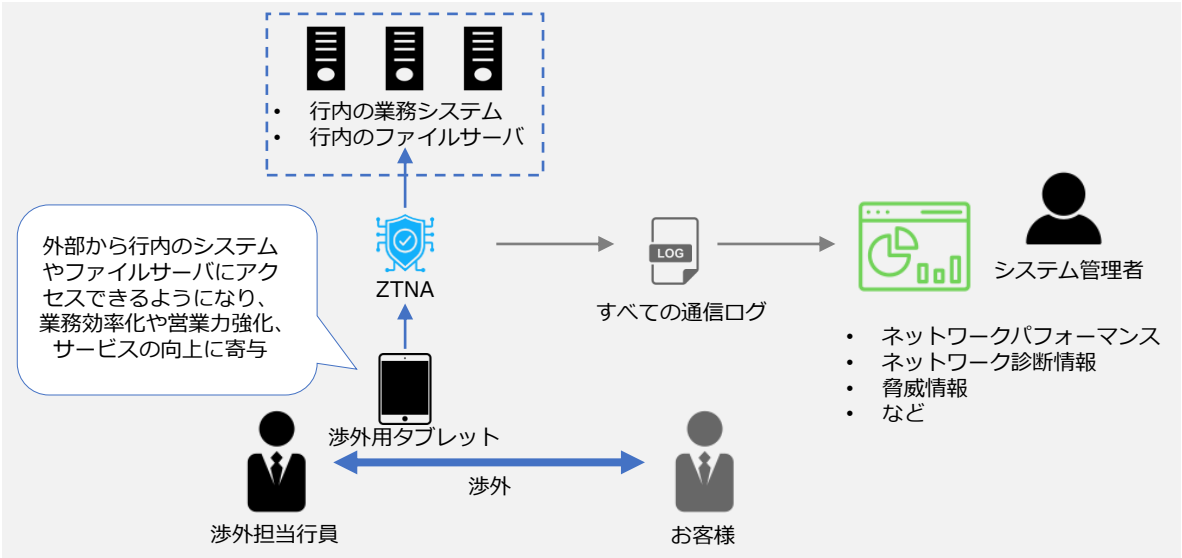


図62. 事例のイメージ図

導入前の課題

営業力強化に向けてモバイル端末の必要性が高まり、次の課題があげられました。
- 行内だけの運用だったモバイル端末活用を、いつでもどこでも働ける環境に拡大すること。
- 渉外用タブレットは、外から行内システムやファイルサーバにアクセスできる必要があること。
- 外部でモバイル端末を利用するためには、セキュリティや性能の担保が必要であること。

選定の決め手

次の事項が導入の決め手となりました。
- リモートアクセスとセキュリティのゼロトラスト機能が一体になっていること。
- 動作検証でリモートアクセス時の速度・安定性が高いこと。

導入後の効果

導入後の効果は次の通りです。
- 営業職員が行内に戻らず業務を遂行できるようになり、業務が効率化したこと。
- 許容した内容や業務だけの通信に限定できるので、安心して使用できること。
- 今後は渉外用タブレットを活用した業務改革の推進が見込まれること。

詳細理解のため参考となる文献（参考文献）	
（参考資料1）民間企業におけるゼロトラスト導入事例	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.pdf

17-2-3. ネットワーク制御

関連する主な管理策
5.23、6.7、8.20~8.24

ネットワーク制御を説明するにあたって、クラウドサービスについて説明します。
クラウドサービスとは、サービス事業者がハードウェアの機能（サーバ、ハードディスクなど）、プラットフォームの機能（データベースやプログラム実行環境など）、ソフトウェアなどを、ネットワーク経由で利用者に提供するサービスのことです。利用者は、どの端末からでもさまざまなサービスを利用することができます。クラウドサービスの利用形態には、主に「IaaS＝アイアース」、「PaaS＝パース」、「SaaS＝サーズ」があります。また、「NaaS＝ナース」と呼ばれるネットワークインフラを提供するサービスもあります。

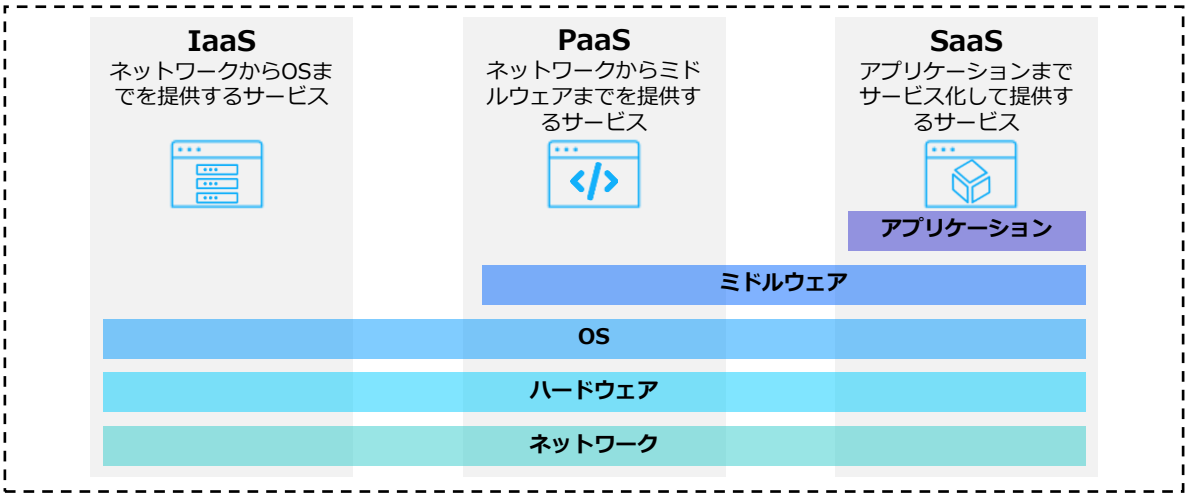


図63. クラウドサービス利用形態の概要図

IaaS（Infrastructure as a Service）

IaaSとは、インターネット経由でネットワークやサーバ（CPU・メモリ・ストレージ）などのハードウェアやインフラ機能を提供するサービスのことです。IaaSを利用することで、従来は自社で購入、構築し、運用する必要があったハードウェアやインフラの機能を、必要なときに必要なだけ利用できます。

PaaS（Platform as a Service）

PaaSとは、インターネット経由でアプリケーションサーバやデータベースなどのアプリケーションを実行するためのプラットフォーム機能を提供するサービスのことです。PaaSを利用することで、アプリケーションの開発前段階で必要な開発環境の準備（サーバの設置やOSやミドルウェアのインストールと設定、ネットワークの設定など）を省略できます。

SaaS（Software as a Service）

SaaSとは、インターネット経由で電子メール、顧客管理、財務会計などのアプリケーションソフトの機能を提供するサービスのことです。アカウントを持っていれば、インターネット経由でどこからでもアクセスすることができたり、チームでファイルやデータを共有できたりします。

NaaS（Network as a Service）

NaaSとは、インターネット経由でネットワークインフラを提供するサービスのことです。
NaaSの導入により、ネットワーク環境の変更に柔軟に対応できるようになります。NaaSに含まれる主要な機能として、SDN、SD-WANなどがあります。

17-2-3. ネットワーク制御

SDN・SD-WAN

クラウドサービスやWeb会議、リモートワークの普及に伴い、ネットワーク回線にアクセスが集中し、通信速度が低下したり、サービスへの接続ができなくなったりするなどの問題があります。その解決策としてSDNを応用したSD-WANがあります。SDN、SD-WANについて説明します。

SDN（Software Defined Networking）

SDNとは、ソフトウェアを用いてネットワーク構成を動的に変更することです。ネットワークを構成している機器（ルータやサーバ、スイッチなど）を、ソフトウェアを介して一括制御することで、機器設定やネットワーク構成を柔軟に変更できます。SDNのメリットは、ネットワーク機器に対して一括で設定を行えることです。従来のルータ、スイッチといった物理的なネットワーク機器・製品は、1台ごとに個別に設定を行う必要があり、大規模なネットワーク構成を変更する際には、大きな作業負荷がかかりました。しかし、SDNを用いてネットワークを制御することで、管理が1か所で行えるようになるため、ネットワーク機器・製品ごとに個別設定が不要になり、作業負荷が大幅に軽減できます。

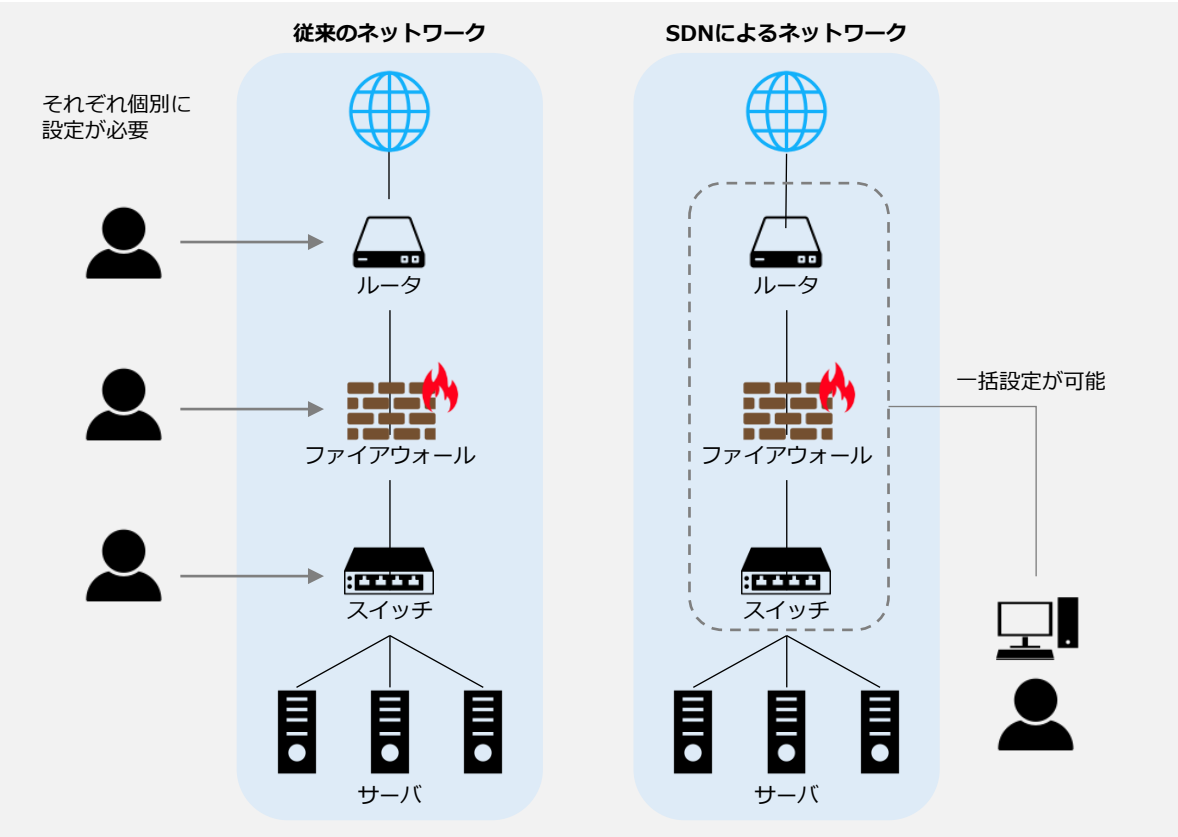


図64. 従来のネットワークとSDNによるネットワークの比較

17-2-3. ネットワーク制御

SD-WAN（Software Defined-Wide Area Network）

SD-WANとは、ネットワークをソフトウェアで制御するSDNを、物理的なネットワーク機器で構築したWANに適用する技術のことです。企業の拠点間接続や、クラウド接続などにおいて柔軟なネットワーク構成を実現したり、ネットワーク上で発生する通信を適切に制御したりすることができます。

たとえば、拠点間の通信には閉域網（不特定多数のユーザが利用するインターネットとは異なり、関係者のみが接続できる通信回線）を使用し、信頼できるクラウドサービスには直接外部インターネットへ接続するように切り替えることで、トラフィックの最適化が行えます。

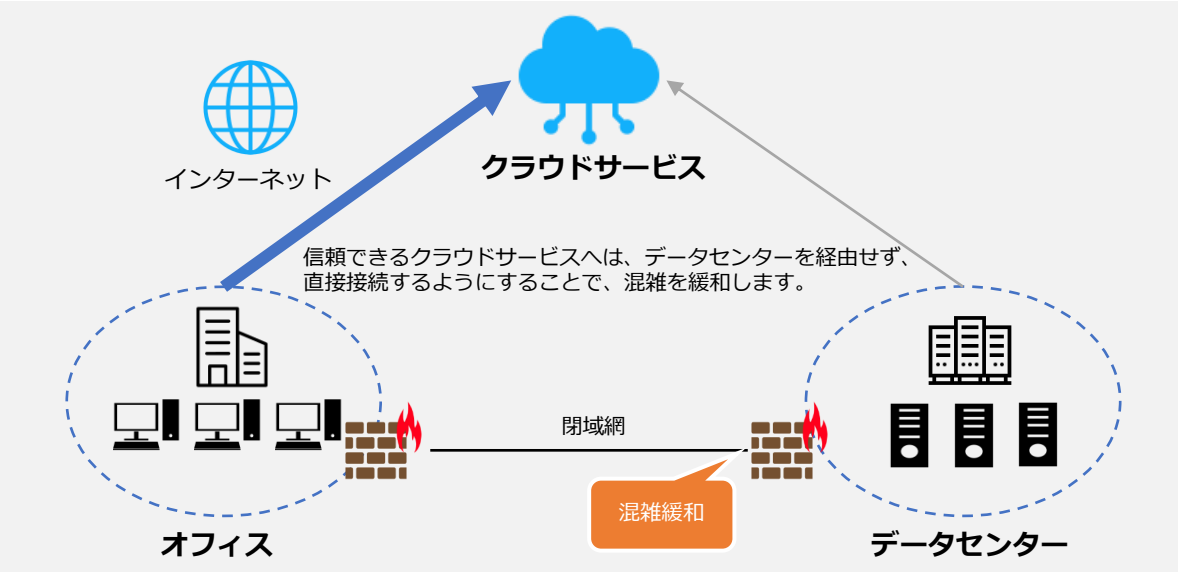


図65. SD-WANで実現できることの例

VPN

個人情報などの重要なデータをインターネット経由で扱う機会が増えたことや、サイバー攻撃の手口が年々巧妙化しているなどの状況を背景に、VPNが注目されています。

VPN（Virtual Private Network）

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です。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ぎます。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えます。

図66. VPNの概要図

17-2-4. セキュリティ統制

関連する主な管理策
5.1、5.9、5.15～5.18、5.23～5.28、8.1～8.5

セキュリティ統制とは、組織が情報資産を守るために採用するセキュリティ対策や仕組みになります。機密性、完全性、可用性などの情報セキュリティの目標を達成するために監視、記録を行い統制します。

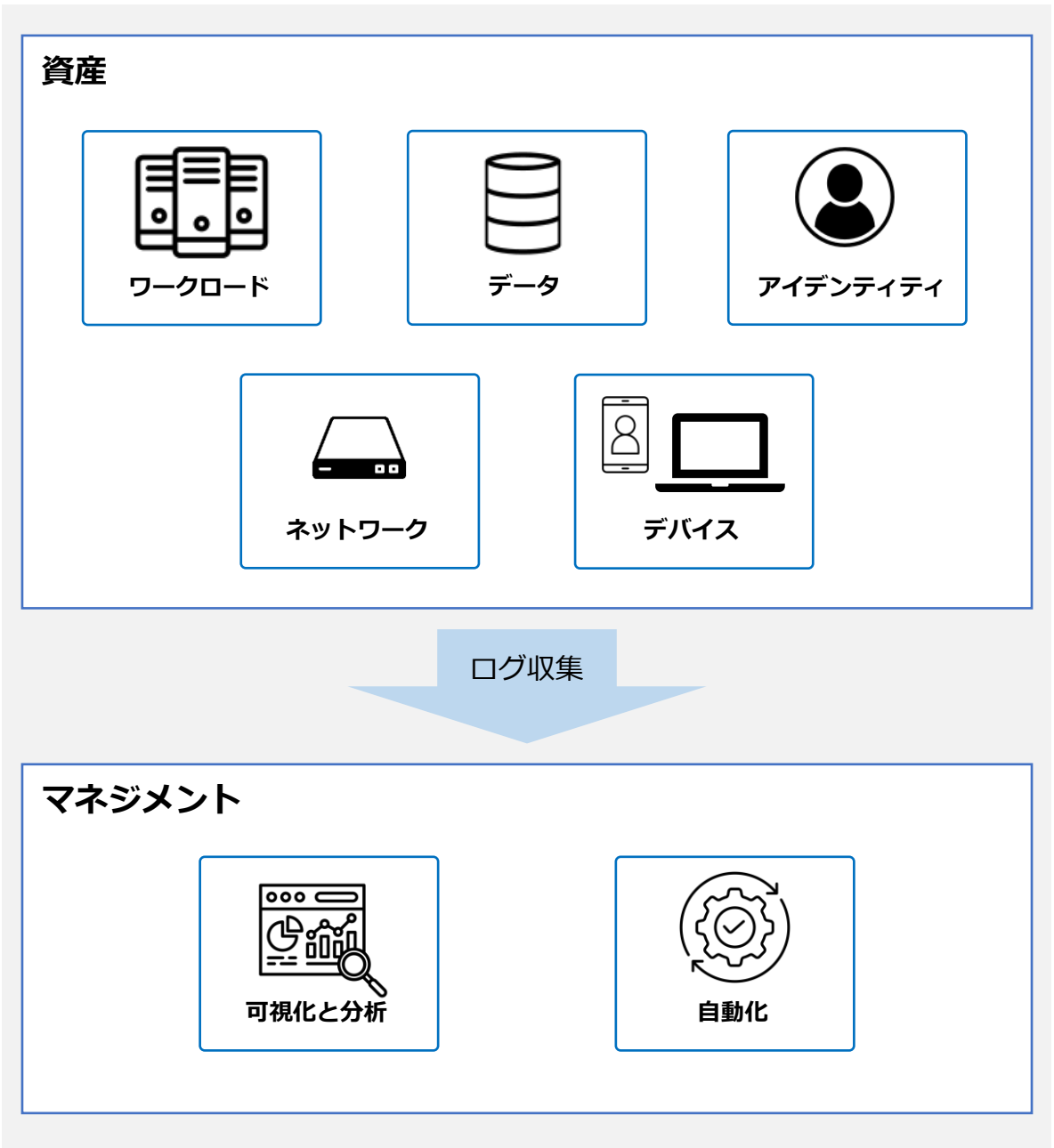


図67. セキュリティ統制の概要図

17-2-4. セキュリティ統制

以下は、セキュリティ統制を確立するための実施例となります。

実施内容（例）	選択すべき管理策（例）
リスク評価と分析 • 組織内の情報資産やプロセスを評価し、セキュリティリスクを特定 • リスクの重要度や影響を評価し、優先順位づけ	• 5.9 情報及びその他の関連資産の目録
ポリシーの策定 • セキュリティポリシーを作成し、組織内での適用範囲や要件を定義 • ポリシーは法規制や業界のガイドラインに準拠	• 5.1 情報セキュリティのための方針群
技術的対策の実施 • 資産に対してセキュリティ対策の実施 ➢ ワークロード ➢ データ ➢ アイデンティティ ➢ ネットワーク ➢ デバイス　など	• 5.15 アクセス制御 • 5.16 識別情報の管理 • 5.17 認証情報 • 5.18 アクセス権 • 5.23 クラウドサービスの利用における情報セキュリティ
監視と評価 • セキュリティ対策の効果を監視し、定期的な評価の実施 • セキュリティインシデントが発生した場合は、原因を分析し、対策の改善	• 5.25 情報セキュリティ事象の評価及び決定 • 5.27 情報セキュリティインシデントからの学習 • 5.28 証拠の収集 • 8.15 ログ取得 • 8.16 監視活動
変更管理 • システムやポリシーに変更があった場合、セキュリティに影響を与えないように変更管理プロセスを確立	• 8.32 変更管理
対応計画の策定 • セキュリティインシデントが発生した場合の対応計画を策定し、迅速かつ効果的に対処	• 5.24 情報セキュリティインシデント管理の計画及び準備 • 5.26 情報セキュリティインシデントへの対応

SECaaS（Security as a Service）

SECaaSはセキュリティをサービスとして提供します。組織がセキュリティに関する機能をクラウドベースのサービスプロバイダから提供される形態で利用します。従来では、オンプレミスで利用していたセキュリティ機能をクラウドに移行し、サブスクリプションで利用することが可能になります。

SECaaSのメリット
- コスト最適化
- スケーラビリティ
- 変化への柔軟な対応
- 冗長性
- 高い可用性
- 障害耐性

17-2-4. セキュリティ統制

セキュリティ統制を確立するために実施することができる技術を紹介します。

ネットワーク・セキュリティ	
SWG（Secure Web Gateway）	Webアクセスを中継するプロキシの一種で、危険なサイトやコンテンツへのアクセスを遮断するセキュリティ機能をクラウドサービスとして実施。（第17章 27ページを参照）
SDP（Software Defined Perimeter）	アクセス制御をソフトウェアで制御し、認証とアクセス制御を接続ごとに行うことで、動的なマイクロセグメンテーションおよびセキュアなリモートアクセスを実現。（第17章 27ページを参照）
デバイスセキュリティ	
EDR（Endpoint Detection and Response）	パソコンやサーバ、スマートフォンなどのエンドポイントデバイスに侵入したマルウェアやランサムウェアなどを検出し、通知するシステム。マルウェア感染後の被害拡大防止に有効。（第3章 2ページを参照）
EPP（Endpoint Protection Platform）	パソコンやサーバ、スマートフォンなどのエンドポイントデバイスへのマルウェアの侵入を防御するソリューション。未知のマルウェアの検知・駆除にも対応。
アイデンティティセキュリティ	
IAM（Identity and Access Management）	情報システムのユーザIDの管理・認証・認可。
FIDO（Fast Identity Online）	ID/パスワード方式に代わる認証技術。指紋や虹彩といった生体情報、公開鍵暗号、端末ID、ワンタイムパスワードなどを利用した認証方法がある。
ワークロードセキュリティ	
CWPP（Cloud Workload Protection Platform）	クラウド上コンテナ（実行環境）や仮想マシンなどに導入し、クラウドワークロード（クラウド上で実行されるプログラムやアプリケーション）の監視と保護を行うソリューション。
データ・セキュリティ	
DLP（Data Loss Prevention）	情報漏えい防止を目的とするセキュリティツール。従来のシステムと異なり、データそのものを監視して情報漏えいを防ぐため、高い効果が期待できる。
可視化と分析	
CASB（Cloud Access Security Broker）	クラウドサービスの脆弱性対策ソリューション。クラウドサービスの利用状況を可視化すると同時にクラウドへの不正アクセスの検知と防御も可能。（第17章 27ページを参照）
SIEM（Security Information and Event Management）	ファイアウォールやIDS/IPSなどから出力されるログやデータを一元的に集約し、集約したデータを組み合わせて相関分析を行うことにより、サイバー攻撃やマルウェア感染などのセキュリティインシデントをリアルタイムで検知。
CSPM（Cloud Security Posture Management）	クラウド環境の設定状況を可視化し、あらかじめ設定したルールに基づいて、不適切な設定や脆弱性の有無を検知。
自動化	
SOAR（Security Orchestration Automation and Response）	セキュリティインシデントの監視、データの収集・分析、対応などのセキュリティ運用業務を自動化・効率化する技術。

17-2-4. セキュリティ統制

FIDO（Fast Identity Online）

FIDOは、従来のパスワードによる認証方式に代わる、パスワードを使わない「パスワードレス認証」を実現する技術です。認証には、公開鍵暗号方式を利用したデジタル署名の仕組みが用いられます。

デジタル署名による送信者確認の仕組み

デジタル署名では公開鍵と秘密鍵、2つの鍵を使用します。 公開鍵は公開される誰でも取得できる鍵で、秘密鍵は本人だけが保持している鍵です。秘密鍵で署名したデータは、対となる公開鍵で検証できます。この仕組みを利用し、受信者は送られてきたデータが間違いなく送信者本人から送られてきたか確認できます。

図68. デジタル署名による送信者確認の仕組み

FIDO2

FIDO2とは、パスワードレス認証の技術仕様のことです。FIDO2では、端末で生体認証行い、利用者を認証します。サーバとは、デジタル署名による本人確認の仕組みを用いて認証します。サーバ側には公開鍵、端末側には秘密鍵が保管され、鍵同士がペアとなります。正式サイトを偽装したフィッシングサイトがログインを求めても、ペアとなる鍵がないためログインを防げます。FIDO2を利用したパスキーという仕組みでは、認証資格情報を複数の端末で同期できるため、機種変更や端末紛失などの場合に、一からの作成する必要はありません。

メリット

- 認証に必要な秘密情報（秘密鍵）は、認証を行う端末側のみに保存され、利用する際は生体認証を行うため、パスワードを覚える必要がありません。
- パスワードや認証に必要な機密情報がインターネットに流れず、サーバ側で保存されないため、漏えいのリスクが低減されます。

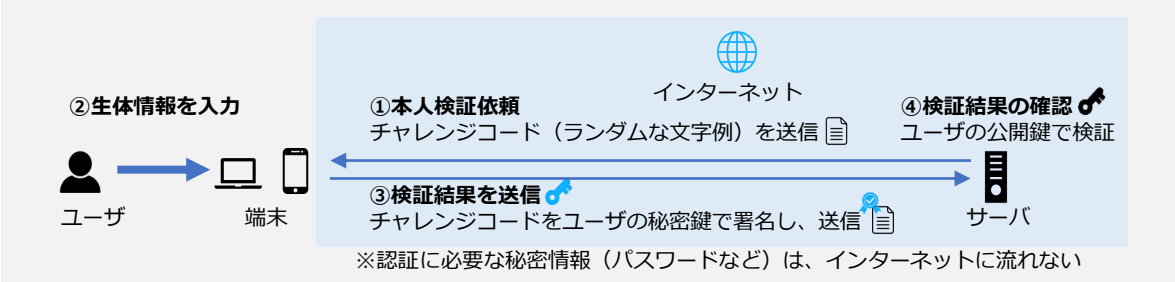


図69. FIDO2の仕組み

①本人検証依頼
サーバは、ユーザの端末に向けてチャレンジコード（ランダムな文字列）を送信します。
②生体情報を入力
ユーザは生体情報を入力し、端末はユーザを認証します。
③検証結果を送信
ユーザの認証に成功したら、端末はチャレンジコードをユーザの秘密鍵で署名し、サーバへ送信します。
④検証結果の確認
サーバは、署名されたチャレンジコードを受け取ったら、ユーザの公開鍵で検証します。検証に成功するとユーザのログインを受け入れ、認証完了となります。

17-2-5. インシデント対応

関連する主な管理策
5.5、5.6、5.24~5.28、6.8

インシデント発生時の対応

セキュリティインシデントが発生した際の基本的な対応の流れは、「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」で説明した「1. 検知・初動対応」、「2. 報告・公表」、「3. 復旧・再発防止」です。インシデント対応の実施手順について、ウイルス感染が起きた際の例を用いて説明します。

実施手順（例）	
①検知・初動対応	検知と連絡受付： • パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるため、情報セキュリティ責任者に報告する。 • ウイルスが添付されたメールを受け取った外部から通知を受けて発覚した場合も、情報セキュリティ責任者に報告する。 • 内部から外部への不正な通信、外部からの意図しない通信や、一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑う。 初動対応： • 感染したパソコンやサーバの利用を停止し、ネットワークから切り離す。
②報告・公表	第二報以降・最終報： • 影響を及ぼした取引先や顧客に対して、セキュリティインシデントに関する報告を行う。 • ウイルス感染による影響によって、業法などで報告が求められる場合は所管の省庁へ報告する。 • ウイルス感染やランサムウェア感染の場合は、IPAの届出窓口へ届け出る。
③復旧・再発防止	調査・対応： • 他のパソコンやサーバがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックする。 • ウイルス対策ソフトに従ってウイルスを駆除する。 • ウイルス駆除ができない場合、OSのクリーンインストールを実施し、すべてのプログラムを入れ直す。 復旧： • ウイルスの駆除が確認できたら、対象のパソコンやサーバをネットワークに接続し、復旧する。

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

17-2-5. インシデント対応

フォレンジック

インシデント対応の「復旧・再発防止」のステップでは、訴訟対応などを見越して事実関係を裏づける情報や証拠を保全し、必要に応じてフォレンジックを行います。

フォレンジックとは

フォレンジックとは、セキュリティインシデントが起きた際に、コンピュータ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調査・解析する技術・手法・手続きを指します。

フォレンジックを行う際の注意点

フォレンジックを行う必要がある際は、専門の調査会社に依頼する選択肢も考慮することが大切です。なぜなら、フォレンジックには専門知識が必要であり、自社で対応しようとすると、証拠となるデータの収集・保全が困難になる可能性があるためです。たとえば、データのコピーが客観的証拠として認められない可能性や、誤操作によるデータの破損などがあります。事前に相談する専門の調査会社を決めておくことが大切です。

セキュリティインシデント発生直後の対応についての実施手順策定

フォレンジックに関して、「証拠保全ガイドライン」が参考になります。想定読者として、「フォレンジックに関する専門知識を習得しているとは限らないが、専門事業者または捜査機関に引き継ぐために証拠保全手続きを行う可能性のある担当者」が含まれています。

セキュリティインシデント発生直後の初動対応についての実施手順を、例を用いて説明します。セキュリティインシデントが検知された、または発生していたことが明らかになった直後は、証拠保全を適切かつ円滑に実施するため、次の事項を実施することが大切です。

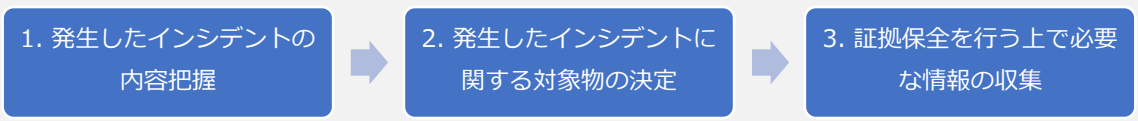


図70. インシデント発生直後の対応の流れ

詳細理解のため参考となる文献（参考文献）	
証拠保全ガイドライン 第9版	https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf

17-2-5. インシデント対応

実施手順（例）

1. 発生したインシデントの内容把握

発生したインシデントを把握します。

インシデントの種類

- ✓ 情報流出・データ破壊
- ✓ 不正アクセス、不正プログラムの実行
- ✓ 操作・設定ミスなど

検知・発覚のきっかけ

- ✓ ログのレビュー・監視
- ✓ 内部通報
- ✓ 不正検知システムなど

発生時刻

- ✓ システム時計の正確性の確認

初動対処の開始までの記録

発生したインシデントの検知・発覚から、報告または対処依頼の連絡までの時間およびその間のインシデントに対する対処の有無について記録をとります。

- ✓ 発生したインシデントを知る人物および人数
- ✓ インシデントの対象物の確保の有無

インシデントの対象物を確保していた場合
対象物を確保した日時、人物（役職）、場所、確保時の対象物（および周辺）に対する行為、確保後の対象物に対する対処（の有無）とその内容を記録します。

インシデントの対象物を確保していない場合
対象物を確保する（予定の）日時と場所、確保時の対象物（およびその周辺）の状態を詳細に記録します。

2. 発生したインシデントに関する対象物の決定

対象物に対する情報収集および対象物の絞り込み

- ✓ 発生したインシデントに関する対象物の種類および個数を確認します。
  - ・コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型）
  - ・ネットワーク機器（ルータ、ファイアウォール、IDS、IPS）
  - ・HDD、SSDなど
- ✓ 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。
- ✓ 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。
- ✓ 発生したインシデントに関する対象物の使用者、および管理者を確認します。
- ✓ 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器、およびドキュメントの有無を確認します。

対象物の選定と優先順位づけ

- ✓ 保全を行う前の対象物（デバイス）を選定し、その理由を明確にします。
- ✓ （対象物が複数ある場合）取扱う対象物の優先順位をつけ、その理由を明確にします。

3. 証拠保全を行う上で必要な情報の収集

対象物の情報

- ✓ 対象物の形状、個数、物理的な状態を確認します。
  - ・対象物のラベル情報（メーカー、型番、モデル名、記憶容量など）
  - ・ケーブルの接続状況
  - ・通常環境下で視認可能な物理的破損、損傷の有無など
- ✓ HDD、SSD、ストレージメディアの記憶容量、インタフェースの状況を確認します。
- ✓ セキュリティ設定の有無を確認します。
  - ・HDD、SSDのパスワードロック
  - ・HDD、SSD全体暗号化または一部のファイル・フォルダの暗号化
  - ・PC周辺のワイヤストッパー、ロッカーなど

第18章. セキュリティ対策状況の有効性評価

18-1. 内部監査・外部監査

章の目的
第18章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。
主な達成目標
◘ 内部監査および外部監査の重要性について理解すること。

18-1-1. 内部監査

内部監査とは、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実施されているかをチェックすることです。　セキュリティのルールを整備して日が浅いうちは、関係者がルールを理解し、遵守しながら仕事ができているかを重視して判断します。運用に慣れてきたら、設けられた社内のルールや使っている文書の内容が適切か、その有効性を判断していきます。内部監査の視点を適合性から有効性へと移していくことで、**ルールが形骸化し、目的が見失われている状態になることを防げる**でしょう。

内部監査の進め方については、第7回のテキストで説明している内容をご参照ください。

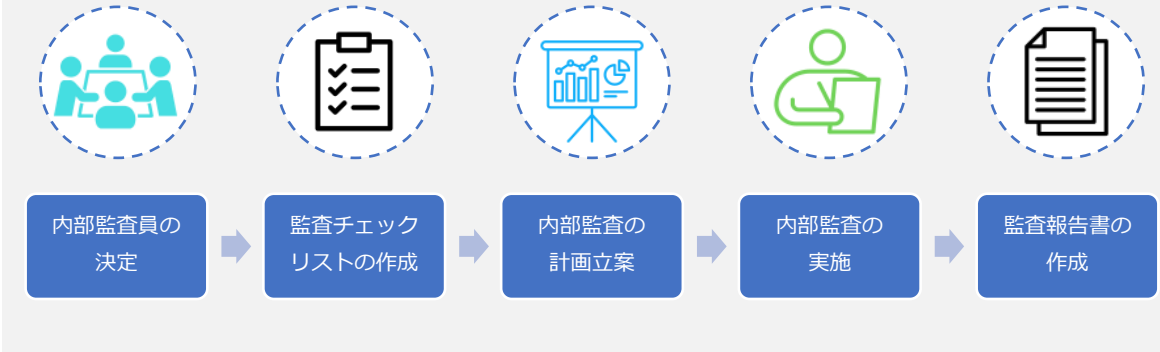


図71. 内部監査の進め方

18-1-2. 外部監査

外部監査とは、組織に所属しない外部の監査人が行う監査を指します。セキュリティの外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックすることになります。情報漏えいやサイバー攻撃などのリスクに対して、外部監査を受けることはセキュリティ対策として有効な手段の1つです。近年では取引先企業を乗っ取り、そこを踏み台にしてメインターゲットとなる企業にサイバー攻撃を仕掛ける「サプライチェーン攻撃」が頻繁に起こっており、中小企業が大企業への攻撃の踏み台として狙われる可能性が高まっています。

情報セキュリティ監査を受ければ、**自社のセキュリティ対策が正しく行われているかどうか確認でき、不十分な点を洗い出して迅速に対処することが可能になります**。顧客や取引先に、セキュリティ対策を適切に行っていることがアピールできるので、会社や事業の規模も考慮しつつ、監査を受けることは重要です。経済産業省は、情報セキュリティの管理・監査について、2つの基準を発表しています。

管理基準・監査基準

情報セキュリティ管理基準

組織における情報セキュリティマネジメントの円滑で効果的な確立を目指し、マネジメントサイクルの構築から具体的な管理策まで、包括的な適用範囲を定めたものです。この管理基準は「マネジメント基準」と「管理策基準」の2項目から構成されています。

マネジメント基準……情報セキュリティマネジメントの計画・実行・点検・処置に必要な実施すべき事項が提示されています。
管理策基準……リスク対応方針に従って管理策を選択する際の選択肢が提示されています。

情報セキュリティ監査基準

情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。監査の品質を一定の水準に保ち、有効かつ効率的に実施できるように「一般基準」「実施基準」「報告基準」の3項目を提示しています。

一般基準……監査人としての適格性および監査業務上の遵守事項を定めています。
実施基準……監査計画の立案および監査手続きの適用方法を中心に、監査実施上の枠組みを定めています。
報告基準……監査報告にかかる留意事項と、監査報告書の記載方式を定めています。

情報セキュリティ管理基準は、JIS Q 27001をもとに策定されています。そのため、本セミナーで解説した網羅的アプローチを実施することで、外部監査に対応することも可能となります。

コラム

実施手順の文書化に関するポイント
実施手順を文書化する際のポイントをいくつか紹介します。

■ 明確な手順と責任の割り当て
実施手順を文書化する際、手順が誰が、いつ、どのように実施するのかを明確にすることが重要です。実施手順が適切に実施されるようにするためには、文書の各手順に関連する責任者を明記することが有効です。

■ フローチャートや図の活用
文字だけでなく、フローチャートや図などを用いて手順を視覚的に示すことで、手順の流れや関係性を理解しやすくできます。また、複雑なプロセスを分かりやすく表現できるため、実施者が迷わずに手順を進められるようになります。

■ 定期的なレビューと更新
実施手順は、絶えず変化する環境に適応させる必要があります。新たな脅威や法規制などへ対応させていくために、定期的なレビューや更新を行い、実施手順が常に効果的なものである状態を維持していくことが大切です。

実施手順の文書化は、組織がセキュリティ対策を行っていく上で必要です。実施手順を組織全体に浸透させ、形骸化させず有効な状態を維持するためには、責任者を明記したり、視覚的な表現を組み合わせて分かりやすい手順を記載したり、定期的にレビューしたりすることが大切です。

第19章. 総括編

19-1. 全体要旨

19-2. 各章のポイント

19-3. 読者に今後行ってほしいこと

章の目的
第19章では、各章のポイントを振り返り、テキスト読後に実施してほしいことや、テキストの活用ポイントについて学ぶことを目的とします。

主な達成目標
◘ 各章ごとに振り返り、重要なポイントを再確認し、その概要を理解すること。
◘ 本テキストに記載の実施手順を活用し、今後、読者が自組織においてセキュリティ対策を実践するために必要な考え方、参考になる文献を把握すること。
◘ 情報セキュリティ担当者、情報システム管理者、経営者など、それぞれの立場で担うべき本テキストの活用方法を理解すること。

19-1-1. テキストの活用

活用のポイント

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. 「DXの理解から対策の実践まで」のポイントを**再認識する**

↓

2. 経営者を含めた関係者と**共有する**

↓

3. 経営者のリーダーシップによって**社内体制を確立する**

↓

4. 具体的なアクションを起こして一歩ずつ**実践する**

19-1-1. テキストの活用

1. 「DXの理解から対策の実践まで」のポイントを再認識する

☛ 「DXの理解から対策の実践まで」の各章の内容は以下の通りです。

DXの推進の考え方の把握	
第1章	現代社会のITに関する情勢、Society5.0やDXについて紹介
第5章	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・課題について紹介

セキュリティ対策の全容の認識	
第2章	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対策や、実際に被害にあってしまった際の対応方法を紹介
第3章	サイバーセキュリティの基本的な知識や対策や、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紹介
第4章	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、経営投資としてのサイバーセキュリティ対策の重要性を紹介
第6章	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、サイバーセキュリティに関連する法令（個人情報保護法とGDPR）について紹介
第7章	ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークの特徴を紹介
第8章	ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法を紹介
第9章	ISO/IEC 27002における管理策の分類と構成について紹介
第10章	ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を紹介

自組織でのセキュリティ対策の実施項目の認識	
第11章	リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を紹介
第12章	セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法を紹介
第13章	情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて紹介

自組織として実践準備	
第14章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、組織的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第15章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、人的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第16章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、物理的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第17章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、技術的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第18章	セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組である監査について紹介

19-1-1. テキストの活用

2. 経営者を含めた関係者と共有する

☛ 本テキストの「第19章. 総括編」をエグゼクティブサマリとして活用してください。記載内容を理解し、経営者および他関係者と共有します。

3. 経営者のリーダーシップによって社内体制を整備する

☛ Security by Designの観点で、ITの導入（企画・計画・仕様策定・調達・運用・保守など）を実践するためのIT人材を育成します。

人材育成の指針を検討する際は、デジタルスキル標準に示された指針を参考にすることが有効です。デジタルスキル標準は、「DXリテラシー標準」と「DX推進スキル標準」の2種類で構成されています。

デジタルスキル標準	**DXリテラシー標準**	ビジネスパーソン全体がDXに関する基礎的な知識やスキル・マインドを身につけるための指針 ※DXを利用する立場の方向け
	DX推進スキル標準	企業がDXを推進する専門性を持った人材を確保・育成するための指針 ※DXを推進する立場の方向け

経営層をはじめ、法務や広報といった、必ずしもITやセキュリティに関する専門知識や業務経験を有していない人材には、プラス・セキュリティ（自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力）を習得させることが重要です。実践にあたっては、関係機関が提供している資料や市販の参考書を参考にしてください。

参考文献）・デジタルスキル標準Ver.1.1 2023年8月（出典：IPA）
・「プラス・セキュリティ知識」とは？（出典：経済産業省）

4. 具体的なアクションを起こして一歩ずつ実践する

☛ Security by Designを実践します。DX化、具体的なIT導入にあたって、セキュリティ対策を含めた実践を行います。

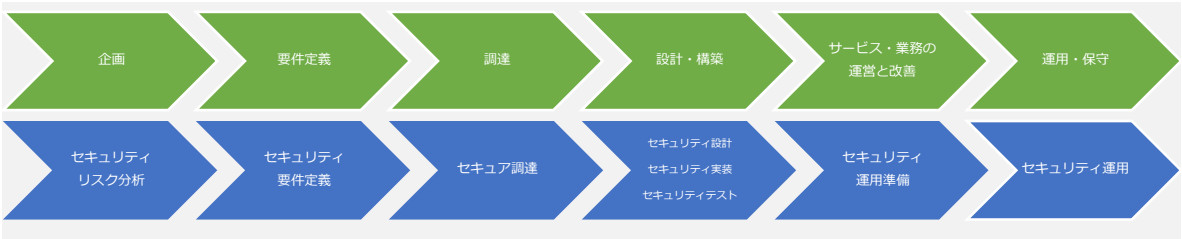


図72. IT導入プロセスにおけるセキュリティ対策の実施タイミング

実践にあたっては、関係機関が提供している資料、市販の参考書を参考にしてください。

参考文献）・セキュリティ・バイ・デザイン導入指南書（出典：IPA）

実践のために参考となる文献（参考文献）	
デジタルスキル標準Ver.1.1 2023年8月	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf
「プラス・セキュリティ知識」とは？	https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf
セキュリティ・バイ・デザイン導入指南書	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf

19-1-2. 中小企業の情報セキュリティ対策

これまでの振り返り

本テキストでは、中小企業のセキュリティを担う方々への育成のため、サイバーセキュリティ関連の情報や、実践的なセキュリティ対策について解説してきました。

第19章では、これまでの各章のポイントをまとめて振り返りつつ、テキストを読んだ後に実施してほしいことや、テキストの活用ポイントについて説明します。

本章を通して、それぞれの対策における実施概要を再認識していただきたいと思います。また、具体的な対策を講じるにあたっては、本テキストで参考文献としている資料などを入手し、詳細な内容を把握した上で実施していただきたいと思います。

テキスト各章の概要	
第1章	現代社会のITに関する情勢、Society5.0の概要やDX推進の重要性について紹介
第2章	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対策や、実際に被害にあってしまった際の対応方法を紹介
第3章	サイバーセキュリティの基本的な知識や対策や、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紹介
第4章	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、経営投資としてのサイバーセキュリティ対策の重要性を紹介
第5章	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・課題について紹介
第6章	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、サイバーセキュリティに関連する法令（個人情報保護法とGDPR）について紹介
第7章	ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークの特徴を紹介
第8章	ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法を紹介
第9章	ISO/IEC 27002における管理策の分類と構成について紹介
第10章	ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を紹介
第11章	リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を紹介
第12章	セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法を紹介
第13章	情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて紹介
第14章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、組織的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第15章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、人的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第16章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、物理的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第17章	情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、技術的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介
第18章	セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組である監査について紹介

19-2-1. 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

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、日本の政府がSociety5.0の方向性を示す中で、企業がビジネスを発展させるためにDX（デジタルトランスフォーメーション）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。

主なキーワード
Society5.0、DX

要旨

1章の全体概要

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おり、日本政府はSociety5.0という新たな社会モデルの実現を提唱しています。Society5.0では、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。AI、ビッグデータなど最新技術が駆使され、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。Society5.0を実現するために、企業にはDX（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）の推進が求められています。

➢ **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という新たな社会モデルが提唱されており、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を進めるには、最新技術の知識、人材確保、セキュリティが重要になります。

訴求ポイント

章を通した気づき・学び

企業や組織は、社会の動向に関する情報を常に収集することが大切です。また、ビジネス環境の激しい変化に対応するためにDXを推進し、デジタル社会に適したビジネスモデル、組織、企業文化に変革していくことが必要です。

認識していただきたい実施概要

✓ 中小企業は、大企業と比べて人手や予算などの企業リソースが限定されており、ビジネス環境の激しい変化に対応するためには、DXを推進し新たなサービスを創造し、ビジネスを発展させることが重要です。

✓ データやデジタル技術を活用するためには、最新技術の知識、最新技術に精通した人材が必要です。安全にデータやデジタル技術を活用するために、セキュリティ対策を適切に行うことが重要です。

実践のために参考となる文献（参考文献）	
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

19-2-2. 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

章の目的
第2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対策や、実際にインシデントが発生した場合の対応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
☐ 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。

主なキーワード
情報セキュリティ白書、情報セキュリティ10大脅威、ランサムウェア、サプライチェーン攻撃、テレワーク、脅威、インシデント、サイバー被害

要旨

2章の全体概要
情報セキュリティ白書、情報セキュリティ10大脅威、最近のインシデント事例をもとに脅威事例を紹介し、対策や対応方法を説明しています。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、自社の業務だけでなく取引先からの信用にも悪影響を及ぼす可能性があることに注意する必要があります。近年の攻撃は企業の規模に関係なく行われるため、中小企業にとっても、セキュリティ対策は不可欠なものになっています。

➢ **2-1. 情報セキュリティの概況**
「情報セキュリティ白書」や「情報セキュリティ10大脅威」を用いて、最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握し、適切な予防策や対策を講じることが大切です。

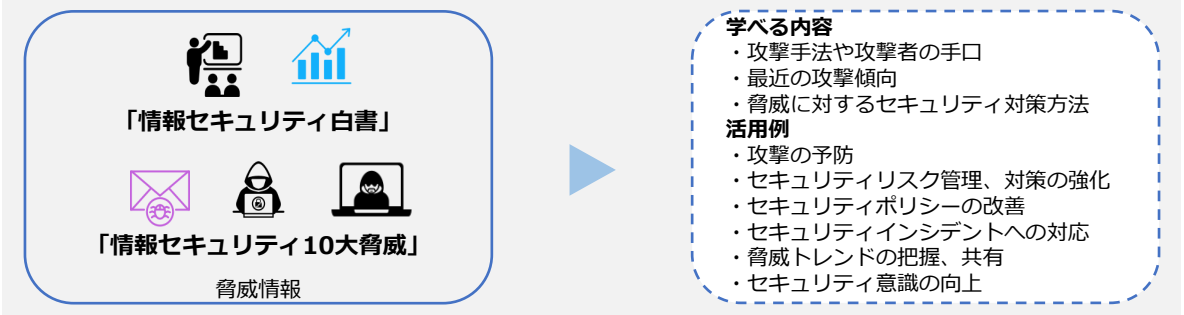


図73. 情報セキュリティ白書・情報セキュリティ10大脅威の活用方法

19-2-2. 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**
  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、セキュリティ意識を向上させるため、IoTデバイスへの攻撃、サプライチェーンを介した標的型メール攻撃、テレワーク環境での情報漏えい、ランサムウェアへの感染など、過去に発生したさまざまなインシデント事例から、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などを理解することが大切です。

- **2-3. 実際の被害事例からみるケーススタディ**
  実践的な問題解決に役立つスキルを養うため、不正アクセスやランサムウェアのインシデント事例を通じて、被害が起きた原因の分析内容、効果的なセキュリティ対策やベストプラクティスを紹介しています。

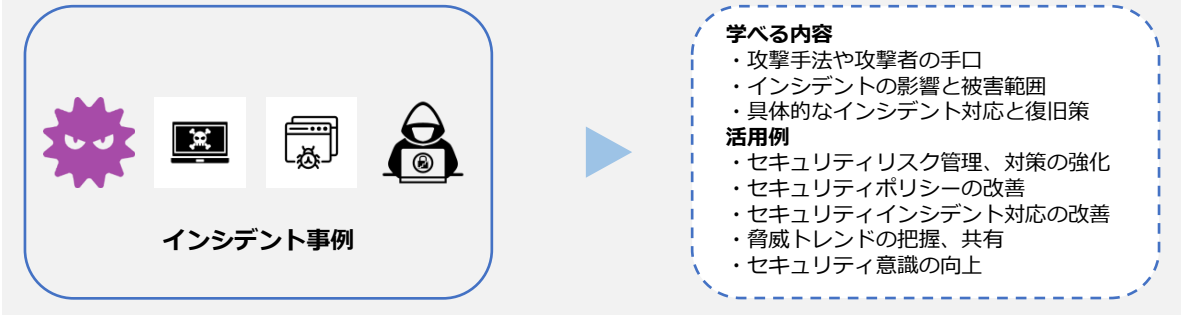


図74. インシデント事例を通じて学べる内容

訴求ポイント

章を通した気づき・学び
最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握し、適切な予防策や対策を講じることが大切です。また、インシデント事例を通して、自社でも起こり得るインシデントに対して適切な対応策を検討し、実施することが大切です。

認識していただきたい実施概要
- ✓ 最新の脆弱性や脅威情報、攻撃の傾向や手法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ためには、情報セキュリティ白書や情報セキュリティ10大脅威を活用することが有効です。
- ✓ 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、今後起こり得るインシデントに対して適切な対応をするためには、過去のインシデント事例から対策方法を学ぶことが有効です。
- ✓ セキュリティ対策の必要性を理解するためには、インシデントが発生した原因や、対策・ベストプラクティスを学ぶことが有効です。

実践のために参考となる文献（参考文献）	
情報セキュリティ白書2022	https://www.ipa.go.jp/publish/wp-security/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

19-2-3. 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

章の目的

第3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。
- サイバーセキュリティに関する基礎知識を身につける方法を確認すること。
- 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。

主なキーワード
UTM、EDR、情報処理技術者試験、SECURITY ACTION

要旨

3章の全体概要
UTM、EDRの機能や、ITやセキュリティに関する網羅的な知識の取得状況を確認するために有効な情報処理技術者試験を紹介しています。中小企業がセキュリティ対策を進めるにあたり、SECURITY ACTION（セキュリティ対策自己宣言）に取組むことを推奨します。その後、サイバーセキュリティの脅威に対処するための3つの段階的なアプローチ手法を用いて対策を進めましょう。

➢ **3-1.導入済と想定するセキュリティ対策機能**
UTM、EDRの機能について振り返ります。

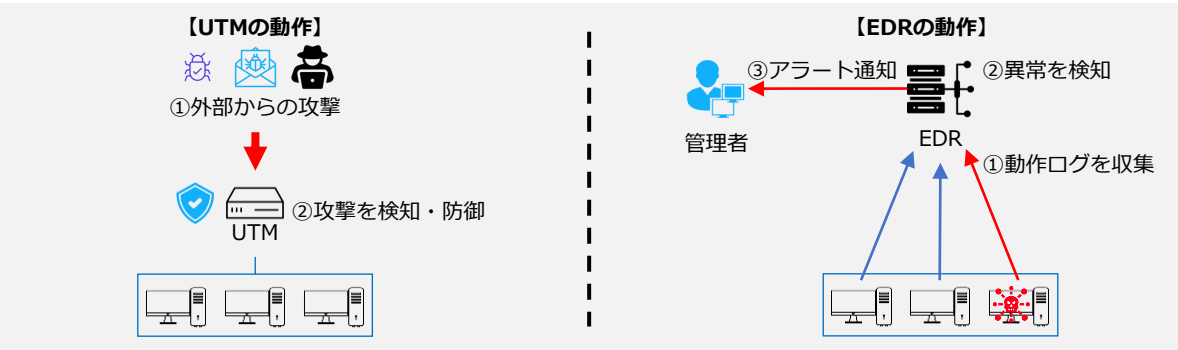


図75. UTM・EDRの概要図

19-2-3. 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**

ITやセキュリティの知識を身につけることは重要です。従業員一人ひとりがITやセキュリティの知識を身につけることで、組織の安全な運営や、組織のセキュリティレベルの向上に繋がります。ITやセキュリティに関する網羅的な知識の取得状況を確認するために、情報処理技術者試験などを受験するとよいでしょう。

- ITパスポート試験（IP）
- 情報セキュリティマネジメント試験（SG）
- 基本情報技術者試験（FE）

➢ **3-3. Security Action（セキュリティ対策自己宣言）**

「SECURITY ACTION」に取組むことで、一つ星・二つ星を宣言でき、従業員のセキュリティに対する意識や対外的な信頼の向上に繋がります。一つ星・二つ星を宣言するには、次の事項に取組む必要があります。

- 情報セキュリティ5か条
- 5分でできる！情報セキュリティ自社診断
- 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**

サイバーセキュリティの脅威に対処するために、段階的なアプローチ手法をとることが重要です。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することが大切です。

- 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

訴求ポイント

章を通した気づき・学び

ITや情報セキュリティの知識を身につけ、企業内外でセキュリティ専門の人材と協力できるようになることが大切です。セキュリティ対策をはじめるにあたり、SECURITY ACTIONに取組み、従業員の意識を高め、対外的な信頼を向上させることが大切です。

認識していただきたい実施概要

✓ ITやセキュリティに関する網羅的な知識の取得状況を確認するために、情報処理技術者試験などを受験することが有効であること。

✓ 中小企業が情報セキュリティ対策に取組むことの宣言として「SECURITY ACTION」という制度があり、従業員の意識を高め、対外的な信頼を向上させるために有効であること。

✓ 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3段階のアプローチがあること。

実践のために参考となる文献（参考文献）	
試験区分一覧	https://www.ipa.go.jp/shiken/kubun/list.html
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

19-2-4. 第4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

4-1. これからの企業経営で必要な観点：社会の動向
4-2. 守りのIT投資と攻めのIT投資
4-3. 経営投資としてのサイバーセキュリティ対策

章の目的
第4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投資について理解することを目的とします。また、経営投資としてのサイバー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繋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
- 経営投資としてのサイバーセキュリティ対策の重要性を理解すること

主なキーワード
守りのIT投資、攻めのIT投資

要旨

4章の全体概要
社会の動向を踏まえ、企業がセキュリティ対策と同時に進めるべきIT活用について説明しています。従来の業務効率化やコスト削減といった守りのIT投資と、DXに向けた攻めのIT投資の特徴や違い、主要なデジタル技術の活用方法について簡潔に紹介しています。経営者主体のサイバーセキュリティ対策の必要性と要点を説明しています。

➢ 4-1.これからの企業経営で必要な観点：社会の動向

社会の動向や、現実社会とサイバー空間の繋がり、IT活用における課題を説明しています。

- 現実社会とサイバー空間の繋がり
  現代社会では、技術の進化が速く、競争が激化しています。企業の経営戦略やビジネスモデルも変化しており、革新的なアイディアと素早い行動が求められています。さらなる経済発展と社会的課題の解決をするため、Society5.0が提唱されています。
- IT活用における課題
  日本社会がデジタル化で後れをとった理由と、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が進んでいる米国と比較します。

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
2. 業務改革などを伴わないICT投資
3. ICT人材の不足・偏在
4. 過去の成功体験
5. デジタル化への不安感・抵抗感
6. デジタルリテラシーが十分ではない

19-2-4. 第4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

➢ 4-2. 守りのIT投資と攻めのIT投資

- 守りのIT投資と攻めのIT投資
  「攻めのIT投資」では、ITを活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規市場の創出、収益拡大、販売力のアップを目指します。一方、「守りのIT 投資」では、ITによる業務の効率化やコスト削減を目指します。攻めと守りを意識し、両者のバランスをとることが大切です。

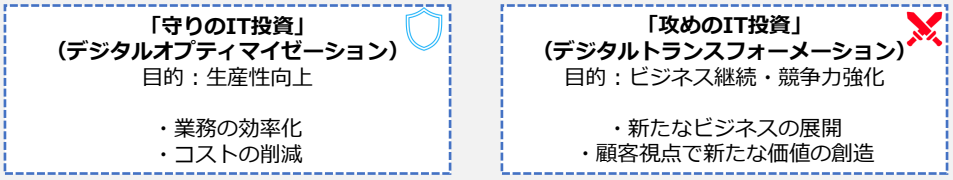


図76. 守りのIT投資・攻めのIT投資

- 次世代技術を活用したビジネス展開
  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、解決するためにデジタル技術の活用が求められます。最近では、AI、クラウド、チャットボットなどの新しい技術がビジネスで活用されるようになってきており、こうした新しい技術を含め、自社に適した技術やツールをうまく活用していくことが求められています。

➢ 4-3. 経営投資としてのサイバーセキュリティ対策

DX推進と並行してサイバーセキュリティの確保に取組むことが重要です。サイバーセキュリティ対策をおろそかにすれば、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あう可能性があります。サイバー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です。経営者が重視すべきポイントは、次の3つです。

ポイント①：ビジネスの継続・発展にはITの活用が不可欠
ポイント②：ITの活用にはサイバー攻撃への対策が必要
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

訴求ポイント

章を通した気づき・学び

Society5.0が提唱される中、企業はデジタル技術を用いてビジネスモデルを変革し、顧客視点で新たな価値を創出するDXを推進するため、「攻めのIT投資」を行うことが大切です。サイバーセキュリティ対策は、経営者が主体となって指揮をすることが大切です。

認識していただきたい実施概要

- ✓ 現実社会とサイバー空間の繋がりや、Society5.0などといった社会の動向を把握することが、これからの企業経営で必要な観点となること。
- ✓ IT投資には「攻め」と「守り」があり、近年特に重要性が増している攻めのIT投資について理解し、取組むことが重要であること。
- ✓ DXの推進に伴い、データやデジタル技術の活用が進む中、サイバー攻撃の被害を防ぐためには、同時にサイバーセキュリティ対策に取組むことが重要であること。

実践のために参考となる文献（参考文献）	
攻めのIT活用指針	https://www.smrj.go.jp/doc/tool/guide4youshiki_1.pdf

19-2-5. 第5章. デジタル社会の方向性と実現に向けた国の方針

5-1. 国の基本方針および実施計画の要約
5-2. 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

章の目的
第5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、デジタル技術の活用やサイバーセキュリティ対策の方向性・課題について理解する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サイバーセキュリティ対策の重要性を理解すること

主なキーワード
デジタル社会、DXの推進、サプライチェーン、DX

要旨

5章の全体概要
国によるデジタル社会に関する方針や政策、デジタル分野の取組におけるサイバーセキュリティの位置付けについて解説しています。政府が目指しているデジタル社会としてSociety5.0を取り上げ、DXについては事例を交えて中小企業の優位性を説明しています。

➢ **5-1. 国の基本方針および実施計画の要約**
IT・セキュリティ関連の施策は、国の方針の1つである「経済財政運営と改革の基本方針」に沿った形で実施計画が策定されています。たとえば、2023年度の方針では「サプライチェーンの強靭化」、「DXの加速」が盛り込まれています。

➢ **5-2. 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**

- 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」に基づき「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。この重点計画の中の各分野における基本的な施策の4番目の「産業のデジタル化」では「中小企業のDX 推進」や「中小企業のデジタル化の支援」が盛り込まれています。

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

19-2-5. 第5章. デジタル社会の方向性と実現に向けた国の方針

「デジタル社会の実現に向けた重点計画」には、日本がデジタル社会を実現していくための政府の取組として、7つの戦略的な政策が掲げられています。この4番目が「サイバーセキュリティなどの安全・安心の確保」となっています。

デジタル社会を実現していくための7つの戦略的な政策

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

また第5章では、政府が提唱しているSociety5.0とDXの推進についても解説しました。

- Society5.0
  Society5.0では、IoTですべての人とモノが繋がり、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、社会が抱えるさまざまな課題を解決の方向に導きます。一方で、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。
- 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ています。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に取組むことで、大きく成長できる可能性があります。

中小企業がデジタルトランスフォーメーション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、デジタルトランスフォーメーション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

訴求ポイント

章を通した気づき・学び

デジタルの活用が進むとともに、サイバー攻撃などのサイバーセキュリティのリスクも高まっています。企業は自社のIT活用状況を認識しつつ、必要な知識・スキルを身につけた人材を育成・確保することが必要です。

認識していただきたい実施概要

- ✓ 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。
- ✓ 中小企業ならではの優位性を理解し、積極的にDXに取組むことが組織を成長させるために重要であること。

実践のために参考となる文献（参考文献）	
経済財政運営と改革の基本方針2023	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf
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
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

19-2-6. 第6章. サイバーセキュリティ戦略および関連法令

6-1. NISC：サイバーセキュリティ戦略
6-2. 関連法令

章の目的
第6章は、NISCの「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について説明しています。

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

主なキーワード
サイバーセキュリティ戦略、DX with Cybersecurity、個人情報保護

要旨

6章の全体概要
サイバーセキュリティについては、NISCの「サイバーセキュリティ戦略」を紹介するとともに、DX with Cybersecurityの考え方について解説しています。デジタルの活用が進むとともに、サイバーセキュリティのリスクも高まっています。企業は自社のIT活用状況を認識しつつ、必要な知識・スキルを身につけた人材を育成・確保するとともに、適切なサイバーセキュリティ対策を実施することが重要です。

➢ **6-1. NISC：サイバーセキュリティ戦略**

- サイバーセキュリティ戦略
  国家レベルでサイバーセキュリティの確保に取組むための基本的な方針や目標を定めた「サイバーセキュリティ戦略」について全体概要と、中小企業に関連する内容について説明しています。
- 企業経営のためのサイバーセキュリティの考え方
  サイバーセキュリティ対策を行うにあたって、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。
- DX with Cybersecurity
  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。中小企業がDX with Cybersecurityを推進するにあたり、人材やスキル不足などさまざまな課題が存在しています。これらの課題に対する対策として、「デジタルスキル標準（DSS）」、「プラス・セキュリティ」について説明しています。

19-2-6. 第6章. サイバーセキュリティ戦略および関連法令

- デジタルスキル標準（DSS）
  デジタルスキル標準（DSS）では、すべてのビジネスパーソンがDXに関する基礎的な知識、スキル、マインドセットを身につけるための学習指針を「DXリテラシー標準」として策定しています。社員に対して、DXに関するリテラシーを身につけさせるための育成方法を検討する際に、指針として活用することができます。
- プラス・セキュリティ
  プラス・セキュリティとは、「自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと」です。
  サイバーセキュリティ体制を適切に機能させるため、経営者は、デジタル部門、事業部門、管理部門などの従業員にサイバーセキュリティに対する意識を高め、業務遂行に必要なセキュリティ対策を実施できる能力を身につけさせるよう育成することが大切です。具体的には、自社で実施しなければならないサイバーセキュリティ関連タスクの一部を担っていること、およびその責任・権限を組織として明確化し、担当者に自覚させることが重要です。

➢ 6-2. 関連法令

- 個人情報保護法
  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繋がる非常に重要な取組となります。
- GDPR（EU一般データ保護規則）
  GDPR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になります。

訴求ポイント

章を通した気づき・学び
日本政府が打ち出しているサイバーセキュリティ戦略を理解し、関連する知識やスキルを身につけることが大切です。

認識していただきたい実施概要

- ✓ サイバーセキュリティ戦略によって、国家レベルでのサイバーセキュリティの確保に取組む方針や目標が定められていることを理解すること。
- ✓ サイバー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付け、自発的にサイバーセキュリティ対策に取組むことが重要であること。
- ✓ DXの推進と並行してサイバーセキュリティへの対策が求められている状況の中、必ずしもITやセキュリティに関する専門知識や業務経験を有していない者も、自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力（プラス・セキュリティ）を身につけることが重要であること。
- ✓ 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やGDPRがあり、個人情報はレベルの高い情報として取扱うべきであること。

実践のために参考となる文献（参考文献）	
サイバーセキュリティ体制構築・人材確保の手引き（第2.0版）	http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf
デジタルスキル標準Ver.1.1 2023年8月	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.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

19-2-7. 第7章. セキュリティフレームワーク

7-1. セキュリティフレームワークの概要
7-2. 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]
7-3. NIST サイバーセキュリティフレームワーク（CSF）
7-4. 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）
7-5. サイバーセキュリティ経営ガイドライン

章の目的

第7章では、ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークを理解し、それぞれの内容について知識を身につけることを目的とします。

主な達成目標

- サイバーセキュリティ対策においてフレームワークを活用することの重要性について理解すること
- 各フレームワークの目的や必要性などの特徴について理解すること

主なキーワード
セキュリティフレームワーク、ISMS

要旨

7章の全体概要

セキュリティ対策に関連するフレームワークの特徴や概要、そして各フレームワークの要素や要件について解説しています。セキュリティ対策は、やみくもに進めてしまうとかえって複雑になってしまい、余計に手間がかかり、内容に抜け漏れが発生する可能性があります。漏れなく効果的に対策を実施するために、企業はセキュリティフレームワークを使用し、自社の課題・目的に即した対応方針を選択することが重要です。

➢ **7-1. セキュリティフレームワークの概要**

次のセキュリティフレームワークの概要、利用メリットについて説明しています。

- ISMS（情報セキュリティマネジメントシステム）[ISO/IEC27001, 27002]
- ISO/IEC27017
- CSF（サイバーセキュリティフレームワーク）
- CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）
- サイバーセキュリティ経営ガイドライン
- PCI DSS
- PMS（個人情報保護マネジメントシステム）
- CIS Controls
- ISA/IEC62443

➢ **7-2.情報セキュリティマネジメントシステム（ISMS）**

ISMSとは、組織の情報セキュリティリスクを適切に管理するための仕組みのことです。 ISMSは、セキュリティフレームワークの中でも代表的なものです。ISMSが達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランスよく維持・改善し、リスクの適切な管理を実現し、信頼を利害関係者に与えることです。

19-2-7. 第7章. セキュリティフレームワーク

- **7-3. NIST サイバーセキュリティフレームワーク（CSF）**
  サイバーセキュリティフレームワーク（CSF）は、NISTが作成したサイバー攻撃対策に重点をおいたフレームワークであり、防御にとどまらず、検知・対応・復旧といったインシデント対応が含まれています。多様な企業に適用できるように要求事項が汎用的になっています。CSFは、組織がセキュリティ対策を継続的に改善するため、①コア（サイバーセキュリティ対策の一覧）、②ティア（対策状況を数値化するための成熟度評価基準）、③プロファイル（サイバーセキュリティ対策の現状とあるべき姿を記述するためのフレームワーク）の3つの要素で構成されています。

- **7-4. 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）**
  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）は、ISMSやCSFのフレームワークの内容を包含しつつ、サイバー空間とフィジカル空間双方のセキュリティ対策に対応したフレームワークです。

- **7-5. サイバーセキュリティ経営ガイドライン**
  サイバーセキュリティ経営ガイドラインは、経営者がサイバーセキュリティ対策を実行する際に認識するべき事項と、サイバーセキュリティ対策の責任者（CISOなど）に指示するべき事項を包括的にまとめています。経営者が主体となってサイバーセキュリティ対策を実施する際に参考にできます。

訴求ポイント

章を通した気づき・学び
セキュリティ対策を漏れなく効果的に実施するためには、セキュリティフレームワークを使用することが有効です。さまざまなセキュリティフレームワークがある中、自社の課題や目的に即したものを選択することが大切です。

認識していただきたい実施概要
- ✓ 効果的なセキュリティ対策の実施や、取引先や顧客からの信頼を向上させるためには、フレームワークに沿って対策を進めることが有効であること。
- ✓ セキュリティ対策を行うためのフレームワークは複数存在するが、まずは業種業態を問わずセキュリティ対策の全体の枠組みと、網羅的な対策項目を提示しているISMSをベースとし、必要に応じて業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークで補完することが有効であること。

実践のために参考となる文献（参考文献）	
ISMS適合性評価制度	https://isms.jp/doc/JIP-ISMS120-62.pdf
サイバーセキュリティ経営ガイドライン Ver3.0	https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf
政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

19-2-8. 第8章. セキュリティ対策基準の策定

8-1. 対策基準の策定

章の目的

第8章では、ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法について理解することを目的とします。

主な達成目標

- サイバーセキュリティ対策における複数のアプローチ方法と、それぞれのアプローチ手法の特徴について理解すること
- 各アプローチ手法について理解し、どのアプローチ手法を実施するべきか選択できるようになること

主なキーワード
セキュリティ対策基準、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

要旨

8章の全体概要
最初にセキュリティポリシーの構成（「基本方針」「対策基準」「実施手順・運用規則など」）について説明しています。企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる、レベル感の異なる3つのアプローチ手法（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）を紹介しています。

➢ **8-1. 対策基準の策定**

- セキュリティ対策基準の概要
  情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順・運用規則など」で構成されます。「対策基準」を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせます。対策基準の内容を定める際は、網羅的なフレームワークを参考にすることが推奨されます。

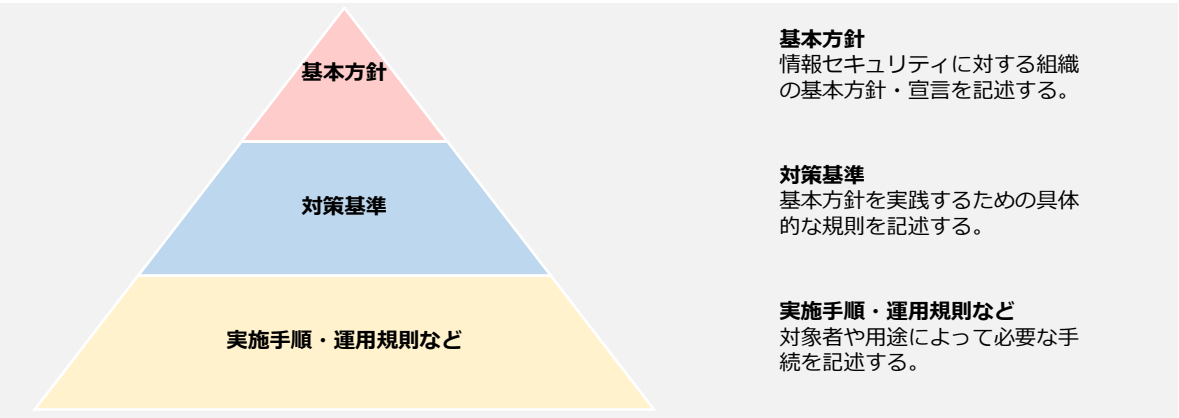


図77. 情報セキュリティポリシーの全体像

19-2-8. 第8章. セキュリティ対策基準の策定

- 対策基準策定のアプローチ方法
  対策基準を作成するアプローチ方法には、レベル感の異なる3つの手法（ 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）があります。

アプローチ手法	特徴	想定される適用ケース
LV.1 クイックアプローチ	インシデント事例内容を参考にして、対策基準を策定する方法。即時の対応や緊急事態への対処に適したアプローチ手法。	自社で発生する可能性が高い、または、発生したときの被害が大きいと考えられるインシデントに対処する場合。
LV.2 ベースラインアプローチ	ガイドラインやひな形を参考にして、対策基準を策定する方法。組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ方法。	組織的に一定以上の対策基準を策定する場合。
LV.3 網羅的アプローチ	ISMSなどの既存のフレームワークを用いて、さまざまな脅威や攻撃手法に対して、網羅的な対策を講じることを目指すアプローチ手法。	ISMSの認証取得を目指す場合、あるいは、ISMSの認証取得が可能なレベルを目指す場合。

訴求ポイント

章を通した気づき・学び
　状況に応じて適切なサイバーセキュリティ対策のアプローチ手法を選択し、セキュリティ対策の実施を内外に示すため、対策基準を策定することが大切です。

認識していただきたい実施概要
- ✓ 対策基準を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせること。
- ✓ 対策基準で記載する内容を具体的に実践するために、策定した対策基準に従って実施手順を作成することが重要であること。
- ✓ 対策基準の内容を定める際は、企業の現状や目標に応じてフレームワークを使用せずに 「クイックアプローチ」「ベースラインアプローチ」を用いて策定できるが、 網羅的なフレームワークであるISMSを参考に策定する「網羅的アプローチ」が推奨されること。

実践のために参考となる文献（参考文献）	
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
情報セキュリティ関連規程	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx
自己点検チェックリスト	https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf
情報セキュリティポリシーサンプル改版（1.0版）	https://www.jnsa.org/result/2016/policy/

19-2-9. 第9章. 管理策のテーマと属性

9-1. 管理策の分類と構成

章の目的

第9章では、ISO/IEC 27002における管理策（リスク対応のための対策）の分類と構成について理解することを目的とします。

主な達成目標

- ISMSの管理策について、テーマと属性という観点を学んだ上で管理策の構成を理解すること

主なキーワード
管理策、ISO/IEC 27002

要旨

9章の全体概要
ISMSの管理策を示した規格であるISO/IEC 27002について説明しています。

➢ 9-1. 管理策の分類と構成

- 管理策：ISO/IEC 27002
  管理策の数は、2013年版では14分野114項目でしたが、2022年版ではいくつかが統合されて82項目になり、新しく11項目が追加され、合計で93項目となりました。2022年版では、この93の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の 4つのカテゴリに分類されています。また、「属性（attribute）」という新しい概念が導入されました。この属性という概念が導入されたことで、管理策のフィルタリング、並び替え、提示がしやすくなりました。ISMSを構築する際には、これらの管理策から、自社にあったものを選択し、対策基準として採用します。

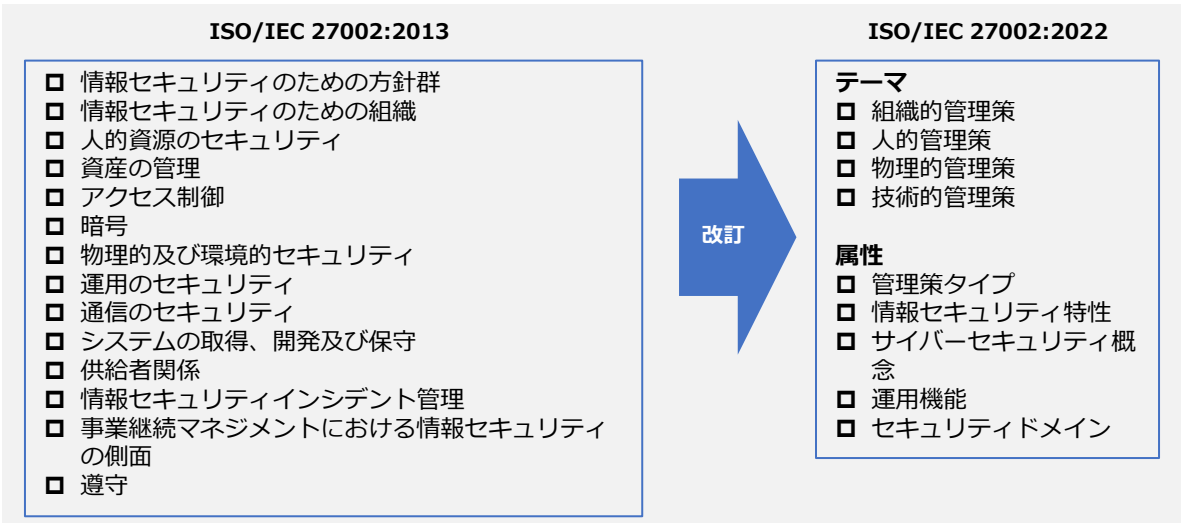


図78. ISO/IEC 27002の改定内容

19-2-9. 第9章. 管理策のテーマと属性

- 管理策のテーマと属性
  管理策のテーマと属性について説明しています。
  テーマとは、ISO/IEC 27002の箇条5～8に示される4種の管理策での分類（組織的・人的・物理的・技術的）のことです。
  属性とは、テーマとは別の視点で、より細かに管理策をみるためのものです。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。

図79. ISO/IEC 27002:2022の概要

訴求ポイント

章を通した気づき・学び
企業や組織はISO/IEC 27002に示された管理策から組織に必要なものを選択することが重要です。

認識していただきたい実施概要
- ✓ ISMSにおけるリスク対応のための対策を指すものとして管理策があり、ISO/IEC 27002:2022に合計93項目示されていること。
- ✓ ISO/IEC 27002:2022で示される管理策には4つのテーマと5つの属性があり、それらを参考にしながら組織に必要なセキュリティ対策を選択することが重要であること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

19-2-10. 第10章. 脅威、脆弱性、リスクの定義と関係性

10-1. 用語の定義および関係性と識別方法

章の目的

第10章では、ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を理解することを目的とします。

主な達成目標

- ISO/IEC 27000に定義されている「リスク」、「脅威」、「脆弱性」、「管理策」の定義を理解すること
- 「リスク」、「脅威」、「脆弱性」などの関係性を理解すること
- 脆弱性、脅威の識別方法を理解すること

主なキーワード
脅威、脆弱性、リスク

要旨

10章の全体概要
リスクマネジメントを理解するために必要となる「リスク」、「脆弱性」、「脅威」といった用語の定義と関係性、さらに「脅威」、「脆弱性」の識別方法について説明しています。

➢ 10-1. 用語の定義および関係性と識別方法

- 用語の定義と関係性
  企業や組織にはセキュリティ上のリスクが存在しています。これらのリスクを効率的に管理するには、リスクマネジメントを行う必要があります。リスクマネジメントを理解するために必要となる「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を説明しています。
  （例）業務用ノートパソコンに関する脅威や脆弱性、管理策の関係

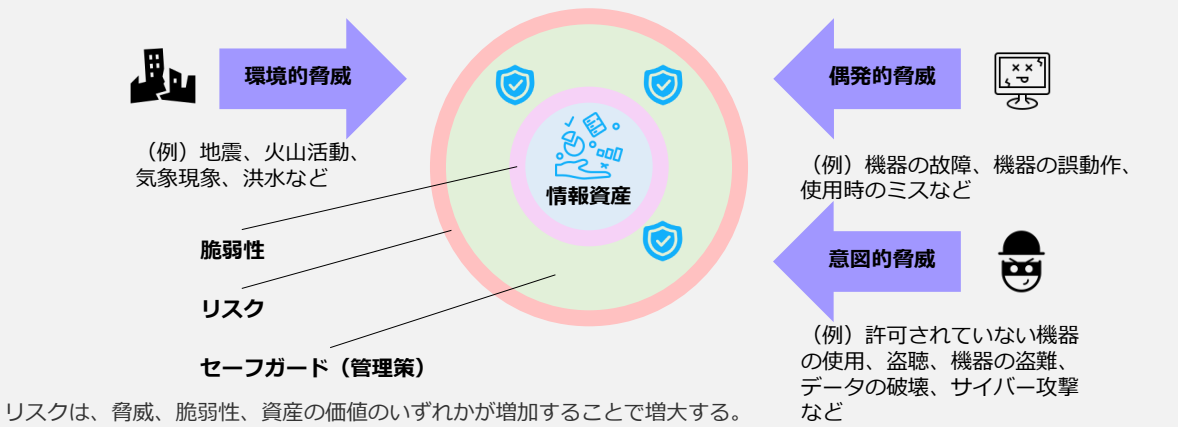


図80. 「脅威」「脆弱性」「リスク」「管理策」の関係性

19-2-10. 第10章. 脅威、脆弱性、リスクの定義と関係性

- 脅威の識別
  脅威は「脆弱性」につけいり顕在化することで、組織に損失や損害を与える事故を生じさせます。脅威を、人為的脅威（意図的脅威、偶発的脅威）と環境的脅威に区別して把握することで、必要なセキュリティ対策を整理しやすくなります。

脅威の種類		想定される被害とセキュリティ対策
環境的脅威 (Environmental → E)		環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を検討して実施する、などのセキュリティ対策が選択されることになります。
人為的脅威	意図的脅威 (Deliberate → D)	悪意のある者によるサイバー攻撃（不正アクセスや標的型攻撃、DDoS攻撃など）があります。対策としては、OSやソフトウェアのアップデートを適宜実施する、EDRやUTMなどのセキュリティ製品を導入する、従業員へ教育の実施などがあげられます。サイバー攻撃により、個人情報や機密情報の漏えい、サービスの停止などの被害にあう可能性があるため、適切なセキュリティ対策を実施することが重要です。
	偶発的脅威 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じないように、2回ずつ入力する、一定の範囲の値しか入力できないようにする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。

- 脆弱性の識別
  脆弱性があるだけでインシデントが発生するわけではありません。しかし、脆弱性は脅威を顕在化させ、インシデントの発生確率を高める可能性があります。脆弱性を減らすためには、適切な管理策を実施する必要があります。脆弱性は管理策の欠如を同時に意味しているため、脆弱性を識別することは必要な管理策を識別するのに役立ちます。

訴求ポイント

章を通した気づき・学び
リスクマネジメントで使用される「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を理解することが大切です。また「脅威」、「脆弱性」の識別方法について理解することが大切です。

認識していただきたい実施概要
✓ 「脅威」「脆弱性」「資産の価値」のいずれかが増加することで、リスクが増大すること。

✓ リスクを減少させるためには「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明らかにし、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要であること。

実践のために参考となる文献（参考文献）	
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

19-2-11. 第11章. リスクマネジメント

11-1. リスクマネジメント：概要
11-2. リスクマネジメント：リスクアセスメント
11-3. リスクマネジメント：リスク対応

章の目的
第11章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を理解することを目的とします。

主な達成目標
◘ リスクマネジメントの意義について理解すること
◘ リスクマネジメントプロセスの全体像を理解すること
◘ リスクアセスメント、リスク対応のプロセスを理解すること

主なキーワード
リスクマネジメント、リスクアセスメント

要旨

11章の全体概要
リスクマネジメントプロセスに沿って、リスク基準の確立、リスクアセスメント、リスク対応について手法なども交えながら解説しています。リスクマネジメントはセキュリティ対策にとって必要ですが、顕在化していないリスクについて考えることが難しい場合もあるでしょう。リスクマネジメントプロセスにおける各段階での考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できます。

➢ 11-1. リスクマネジメント：概要

- リスクマネジメントプロセス（ISO 31000）
  リスクを効率的に管理し、発生する可能性がある損失を回避、低減するプロセス全体のことを「リスクマネジメント」と言います。リスクマネジメントの国際規格としてISO 31000があります。リスク対応にあたり、リスクマネジメントプロセスにおける「リスクアセスメント」が必須です。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位付けをしていくプロセスです。
- 情報セキュリティリスクマネジメント（ISO/IEC 27005）
  ISO/IEC 27005は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。ISO 31000と整合性があり、情報セキュリティに特化した内容になっています。
- ISO/IEC 27001におけるリスクマネジメント手順
  ISO/IEC 27001はISMSの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005です。ISO/IEC 27001の活動は、ISO/IEC 27005におけるリスクマネジメントプロセスと関連付けて整理できます。

19-2-11. 第11章. リスクマネジメント

- **11-2. リスクマネジメント：リスクアセスメント**
- **11-3. リスクマネジメント：リスク対応**

リスクマネジメント全体の流れは下記の図の通りです。リスクアセスメントでは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク基準と比較してリスク対応が必要かどうか判断します。リスク評価の結果をもとに、「低減」、「移転」、「回避」、受容（保有）」からリスク対応を選択します。

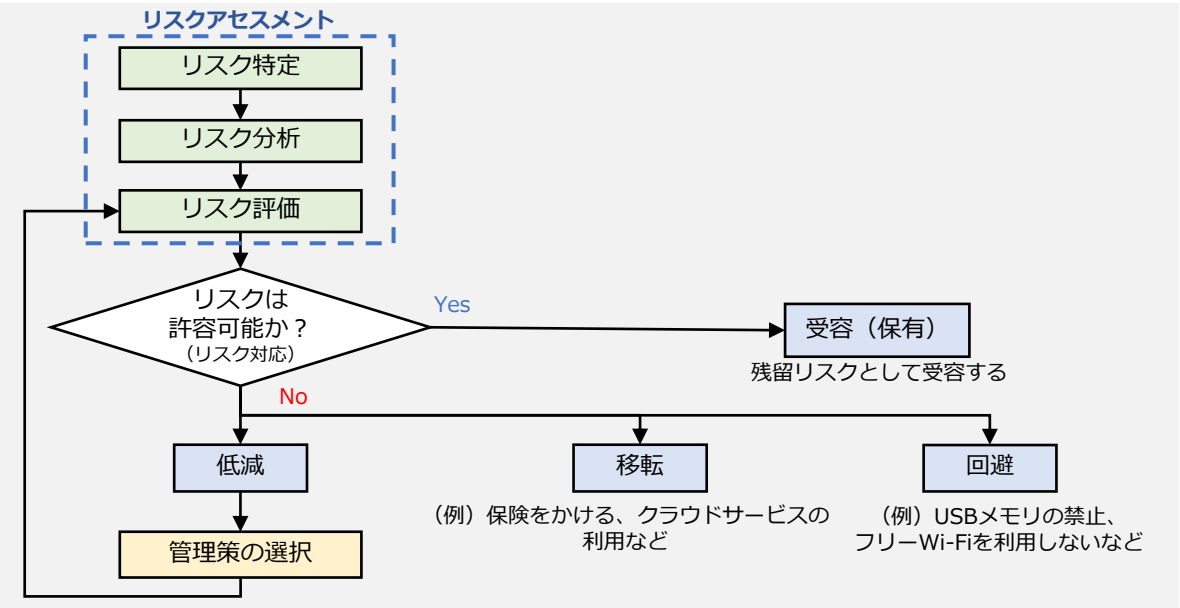


図81. リスクマネジメント全体の流れと、リスク対応の選択プロセス

訴求ポイント

章を通した気づき・学び

リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることが難しい場合もあります。リスクマネジメントプロセスにおける各段階の考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できます。

認識していただきたい実施概要

- ✓ リスク対応にはリスクマネジメントプロセスにおけるリスクアセスメントが必須であること。
- ✓ リスクアセスメントは「リスク特定」、「リスク分析」、「リスク評価」を実施すること。
- ✓ リスク対応はリスクアセスメントの結果をもとに「リスク回避」、「リスク低減」、「リスク移転」、「リスク受容」から選択すること。

実践のために参考となる文献（参考文献）	
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html

19-2-12. 第12章. 具体的手順の作成（LV.1 クイックアプローチ/LV2. ベースラインアプローチ）

12-1. 【LV.1 クイックアプローチ】【LV.2 ベースラインアプローチ】の概要
12-2. 【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順
12-3. 【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

章の目的
第12章では、セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること
- ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード
クイックアプローチ、ベースラインアプローチ

要旨

12章の全体概要
クイックアプローチ、ベースラインアプローチについて説明しています。クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きい事案への対策がとりやすいでしょう。ベースラインアプローチは、ガイドラインやひな形などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができるでしょう。

➢ 12-1. 【LV.1 クイックアプローチ】【LV.2 ベースラインアプローチ】の概要

- LV.1 クイックアプローチ・LV.2 ベースラインアプローチ
  セキュリティ対策基準を策定し、具体的な実施手順を明確にすることで、情報漏えいなどのリスク対策を行います。
  LV.1 クイックアプローチとは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。
  LV.2 ベースラインアプローチとは、ガイドラインなどを参考に対策基準や実施手順を策定するアプローチ手法です。

19-2-12. 第12章. 具体的手順の作成（LV.1 クイックアプローチ/LV2. ベースラインアプローチ）

➢ 12-2.【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順

- セキュリティインシデント事例を参考とした実施手順
  クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。対策基準・実施手順作成の手順を説明しています。

メリット
- 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。

デメリット
- 短期的な解決策に偏りがちになる。
- セキュリティインシデント事例ごとに策定するため、網羅性は低い。

➢ 12-3.【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順

- 情報セキュリティ対策ガイドラインの活用
  ベースラインアプローチは、ガイドラインやひな形などの資料を参考に対策基準、実施手順を作成するという方法です。

メリット
- 組織全体で一貫性を確保できる。
- 最低限実施すべきセキュリティ対策を講じることができる。

デメリット
- 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
- ガイドラインやひな形は、一般的な組織を想定したものであるため、自社の組織やシステム、環境に見合ったものであるかどうかを十分に検討する必要がある。

訴求ポイント

章を通した気づき・学び
緊急性や即効性についてはクイックアプローチ、ベースラインアプローチが勝りますが、じっくりと対策を検討する余裕がある場合、網羅的アプローチに取組むことが大切です。

認識していただきたい実施概要
- ✓ クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きいまたは緊急性の高い事象への対策がとりやすいこと。
- ✓ ベースラインアプローチは、ガイドラインやひな形などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定がしやすいこと。

実践のために参考となる文献（参考文献）	
リスク分析シート	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx
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
インターネットの安全・安心ハンドブックVer.5.0	https://security-portal.nisc.go.jp/guidance/handbook.html
テレワークセキュリティガイドライン第5版	https://www.soumu.go.jp/main_content/000752925.pdf
中小企業のためのクラウドサービス安全利用の手引き	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

19-2-13. 第13章. ISMSの要求事項と構築（LV3. 網羅的アプローチ）

13-1. 【LV.3 網羅的アプローチ】の概要
13-2. 【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順

章の目的
第13章では、情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて理解することを目的とします。
主な達成目標
□ 網羅的アプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード
網羅的アプローチ、PDCAサイクル

要旨

13章の全体概要
網羅的アプローチは、ISMSなどのフレームワークを利用して、対策基準や実施手順を策定する方法です。時間はかかりますが、会社としてセキュリティを確保するにあたって高いレベルでのセキュリティ対策ができるでしょう。緊急性や即効性についてはクイックアプローチ、ベースラインアプローチが勝りますが、じっくりと対策を検討する余裕がある場合、網羅的アプローチを推奨します。

➢ 13-1. 【LV.3 網羅的アプローチ】の概要

- LV.3 網羅的アプローチ
  網羅的アプローチでは、フレームワークとしてISMSを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。ISMSのフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明していきます。
  網羅的アプローチのメリットは、ISMS要求事項の導入が可能なことです。デメリットは、時間とコストがかかることです。

ISMSの要求事項に関連するドキュメント作成は重要ですが、あくまで手段であり目的ではありません。ドキュメントの作成と維持が目的化してしまうと、ドキュメントが形骸化し、情報セキュリティ対策としての意味がほとんどなくなってしまう場合があります。**ドキュメントを精細に作り込むことより、ISMSマネジメントプロセスを取り入れ、PDCAサイクルを回していくことが大切です。**ISMSに取組みはじめたときには理解できていても、ドキュメントづくりをはじめるとドキュメント作成が目的になってしまうケースが多いため、注意が必要です。

19-2-13. 第13章. ISMSの要求事項と構築（LV3. 網羅的アプローチ）

➢ **13-2. 【LV.3 網羅的アプローチ】フレームワークを参考とした実施手順**

ISMSは、PDCAサイクルに則って運用することとなります。ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明しています。

ISMSの要求事項を定めているISO/IEC 27001の1から3はそれぞれ「1.適用範囲」「2.引用規格」「3.用語及び定義」なので、実質的な要求事項は「4. 組織の状況」から「10. 改善」までの7項目となっています。

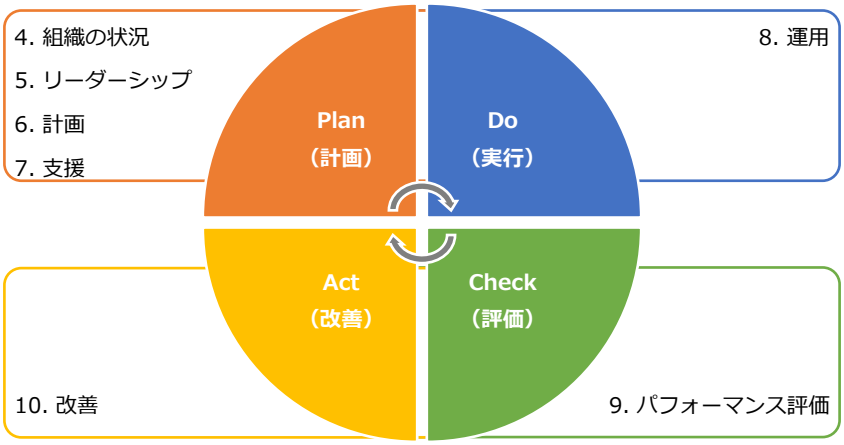


図82. ISMSのPDCAサイクル

4. 組織の状況
組織の内情や取り巻く状況、利害関係者のニーズを把握した上でISMSの適用範囲を決定することを要求している。
5. リーダーシップ
トップマネジメントが主導してISMSを構築することを要求している。（トップマネジメントが実施するべきことのまとめ）
6. 計画
ISMSの計画を立てる際の要求事項。
7. 支援
構成員の教育など、ISMS 構築にあたり組織が構成員に行うべきサポートを要求している。
8. 運用
ISMSを実行する際の要求事項。
9. パフォーマンス評価
適切なISMSが構築・運用できているか評価する際の要求事項。
10. 改善
ISMSの是正処置やリスク、改善の機会、ISMS認証の不適格があった場合の対処法。

訴求ポイント

章を通した気づき・学び

ISMSを用いる網羅的アプローチを実施することで、単にセキュリティ対策を検討するだけではなく、PDCAサイクルによってISMS自体を継続的に改善し、より自社に適した対策を検討できるようになります。

認識していただきたい実施概要
✓ 「4. 組織の状況」から「10. 改善」までの7項目で必要なドキュメントの作成手順を理解すること。
✓ ISMSマネジメントプロセスを取り込み、PDCAサイクルを回すこと。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

19-2-14. 第14章. 組織的管理策

14-1. 組織的管理策を参考とした対策基準・実施手順の策定

章の目的
第14章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。
主な達成目標
◘ 組織的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード
組織的管理策

要旨

14章の全体概要
対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説しています。管理策は、「組織的管理策」、「人的管理策」、「物理的管理策」、「技術的管理策」の4つのカテゴリに分類できます。14章では「組織的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。

➢ **14-1. 組織的管理策を参考とした対策基準・実施手順の策定**

- 対策基準の策定
  ISO/IEC 27001:2022附属書Aの組織的管理策（37項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。
  対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。
- 実施手順の策定
  管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を遵守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対して具体的でわかりやすい実施手順を策定するよう心掛けることが大切です。
  実施手順を策定する際は、ISO/IEC 27002に記載されている各管理策の手引きが参考になります。手引きの内容をもとに、実施手順の例を紹介しています。この例と、ISO/IEC 27002の内容を参考に、自社に適した実施手順を策定しましょう。

19-2-14. 第14章. 組織的管理策

組織的管理策の項目	
5.1 情報セキュリティのための方針群 5.2 情報セキュリティの役割及び責任 5.3 職務の分離 5.4 経営陣の責任 5.5 関係当局との連絡 5.6 専門組織との連絡 5.7 脅威インテリジェンス 5.8 プロジェクトマネジメントにおける情報セキュリティ 5.9 情報及びその他の関連資産の目録 5.10 情報及びその他の関連資産の利用の許容範囲 5.11 資産の返却 5.12 情報の分類 5.13 情報のラベル付け 5.14 情報転送 5.15 アクセス制御 5.16 識別情報の管理 5.17 認証情報 5.18 アクセス権 5.19 供給者関係における情報セキュリティ 5.20 供給者との合意におけるセキュリティの取扱い	5.21 ICTサプライチェーンにおける情報セキュリティの管理 5.22 供給者のサービス提供の監視、レビュー及び変更管理 5.23 クラウドサービス利用における情報セキュリティ 5.24 情報セキュリティインシデント管理の計画策定及び準備 5.25 情報セキュリティ事象の評価及び決定 5.26 情報セキュリティインシデントへの対応 5.27 情報セキュリティインシデントからの学習 5.28 証拠の収集 5.29 事業の中断・阻害時の情報セキュリティ 5.30 事業継続のためのICTの備え 5.31 法令、規制及び契約上の要求事項 5.32 知的財産権 5.33 記録の保護 5.34 プライバシー及びPIIの保護 5.35 情報セキュリティの独立したレビュー 5.36 情報セキュリティのための方針群、規則及び標準の順守 5.37 操作手順書

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に組織的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は重要ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な組織的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

19-2-15. 第15章. 人的管理策

15-1. 人的管理策を参考とした対策基準・実施手順の策定

章の目的
第15章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。

主な達成目標
□ 人的管理策をもとに、対策基準を策定する手順を理解すること。 □ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード
人的管理策

要旨

15章の全体概要
対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説しています。15章では「人的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。

➢ **15-1. 人的管理策を参考とした対策基準・実施手順の策定**

- 対策基準の策定
  ISO/IEC 27001:2022附属書Aの人的管理策（8項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。
  対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。
- 実施手順の策定
  管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

人的管理策の項目	
6.1 選考 6.2 雇用条件 6.3 情報セキュリティの意識向上、教育及び訓練 6.4 懲戒手続	6.5 雇用の終了または変更後の責任 6.6 秘密保持契約または守秘義務契約 6.7 リモートワーク 6.8 情報セキュリティ事象の報告

19-2-15. 第15章. 人的管理策

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に人的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な人的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

19-2-16. 第16章. 物理的管理策

16-1. 物理的管理策を参考とした対策基準・実施手順の策定
16-2. 各種テーマごとの対策

章の目的
第16章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。

主な達成目標
◘ 物理的管理策をもとに、対策基準を策定する手順を理解すること。 ◘ 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード
物理的管理策、BYOD、MDM

要旨

16章の全体概要
対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説しています。16章では「物理的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。またテーマごとの対策として、「BYOD」、「MDM」を紹介しています。

➢ **16-1. 物理的管理策を参考とした対策基準・実施手順の策定**

- 対策基準の策定
  ISO/IEC 27001:2022附属書Aの物理的管理策（14項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。
  対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。
- 実施手順の策定
  管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

物理的管理策の項目	
7.1 物理的セキュリティ境界	7.8 装置の設置及び保護
7.2 物理的入退	7.9 構外にある資産のセキュリティ
7.3 オフィス、部屋及び施設のセキュリティ	7.10 記憶媒体
7.4 物理的セキュリティの監視	7.11 サポートユーティリティ
7.5 物理的及び環境的脅威からの保護	7.12 ケーブル配線のセキュリティ
7.6 セキュリティを保つべき領域での作業	7.13 装置の保守
7.7 クリアデスク・クリアスクリーン	7.14 装置のセキュリティを保った処分または再利用

19-2-16. 第16章. 物理的管理策

➢ **16-2. 各種テーマごとの対策**

テーマごとに、概要や関連する管理策、運用手順などについて説明しています。

- BYOD（Bring Your Own Device）

BYODとは、個人が私物として所有している端末（PCやスマートフォンなど）を業務に使う利用形態のことです。BYOD導入に向けたポイント、運用手順を説明しています。

メリット

- コスト削減
  企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入れ替えも基本的には個人負担となります。
- 使い慣れた端末の業務利用
  従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率があがります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。

デメリット

- シャドーIT
  ルールの整備や技術的な対策を講じないと、シャドーITが増加してしまう恐れがあります。
- セキュリティリスク
  個人の端末では、業務に関係ないWebサイトやアプリケーションを利用されるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなります。

- MDM（Mobile Device Management）

MDMとは、企業で保有しているモバイル端末 (スマート フォンやタブレットなど) を一元管理できるシステムのことです。MDMの導入に向けたポイント、運用手順を説明しています。

MDMを導入する際のポイント

✓ 利用者の意見を反映した社内ルールの策定、およびMDMの選定
MDMは情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。たとえば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDMによる制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定やMDMの選定を進めることが重要です。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に物理的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

✓ リスクアセスメントの結果をもとに必要な物理的管理策を選択し、対策基準を策定すること。
✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。
✓ BYOD、MDMの概要および運用手順を理解すること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

19-2-17. 第17章. 技術的管理策

17-1. 技術的管理策を参考とした対策基準・実施手順の策定
17-2. 各種テーマごとの対策

章の目的

第17章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。また、技術的管理策に関して、テーマごとの対策について理解することも目的とします。

主な達成目標

- 技術的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。
- Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること。

主なキーワード
技術的管理策、Security by Design、ゼロトラスト、ネットワーク制御、セキュリティ統制、インシデント対応

要旨

17章の全体概要

ISMSの管理策を参考に、対策基準・実施手順を策定する手順について解説しています。17章では「技術的管理策」を参考に対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。またテーマごとの対策として、「Security by Design」、「ゼロトラスト」、「ネットワーク制御」、「セキュリティ統制」、「インシデント対応」を紹介しています。

➢ 17-1. 技術的管理策を参考とした対策基準・実施手順の策定

- 対策基準の策定
  ISO/IEC 27001:2022附属書Aの技術的管理策（34項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。
  対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。
- 実施手順の策定
  管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

19-2-17. 第17章. 技術的管理策

技術的管理策の項目	
8.1 利用者エンドポイント機器	8.19 運用システムに関わるソフトウェアの導入
8.2 特権的アクセス権	8.20 ネットワークのセキュリティ
8.3 情報へのアクセス制限	8.21 ネットワークサービスのセキュリティ
8.4 ソースコードへのアクセス	8.22 ネットワークの分離
8.5 セキュリティを保った認証	8.23 ウェブ・フィルタリング
8.6 容量・能力の管理	8.24 暗号の使用
8.7 マルウェアに対する保護	8.25 セキュリティに配慮した開発のライフサイクル
8.8 技術的脆弱性の管理	8.26 アプリケーションのセキュリティの要求事項
8.9 構成管理	8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則
8.10 情報の削除	8.28 セキュリティに配慮したコーディング
8.11 データマスキング	8.29 開発及び受入れにおけるセキュリティ試験
8.12 データ漏えいの防止	8.30 外部委託による開発
8.13 情報のバックアップ	8.31 開発環境、試験環境及び運用環境の分離
8.14 情報処理施設の冗長性	8.32 変更管理
8.15 ログ取得	8.33 試験情報
8.16 監視活動	8.34 監査試験中の情報システムの保護
8.17 クロックの同期	
8.18 特権的なユーティリティプログラムの使用	

➢ 17-2. 各種テーマごとの対策

テーマごとに、概要や関連する管理策、実施手順などについて説明しています。

- ✓ **Security by Design**
  開発プロセスの早い段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。
- ✓ **境界防御モデル・ゼロトラスト**
  境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、境界線でセキュリティ対策を講じることで境界外部からの脅威を防ぐという考え方です。
  ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。
- ✓ **ネットワーク制御**
  クラウドサービス、SDN、SD-WANについて説明しています。
- ✓ **セキュリティ統制**
  組織が情報資産を守るために採用するセキュリティ対策や仕組みのことです。セキュリティ統制を確立するために実施することができる技術を紹介しています。
- ✓ **インシデント対応**
  インシデント対応の実施手順、フォレンジックについて説明しています。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に技術的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な技術的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。
- ✓ 各種テーマごとに概要を理解し、自社に適した実施手順を策定すること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

19-2-18. 第18章. セキュリティ対策状況の有効性評価

18-1. 内部監査・外部監査

章の目的

第18章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組として、監査について理解することを目的とします。

主な達成目標

- 内部監査および外部監査の重要性について理解すること。

主なキーワード
内部監査、外部監査

要旨

18章の全体概要

セキュリティ対策状況の有効性評価として、内部監査と外部監査について説明しています。内部監査では、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実際されているかをチェックします。外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックします。

➢ 18-1. 内部監査・外部監査

- 内部監査
  セキュリティのルールを整備したばかりの段階では、関係者がルールを理解し、遵守できてるか適合性を重視してチェックします。運用に慣れてきたら、社内のルールや文書の内容が適切かどうか有効性をチェックします。内部監査の視点を適合性から有効性へと移していくことで、ルールが形骸化し、目的が見失われる状態を防げるでしょう。
- 外部監査
  セキュリティ対策の実施状況について外部監査を受けることは、情報漏えいやサイバー攻撃などのリスクに対する対策が適切かつ有効であるかどうかをチェックする手段の1つです。情報セキュリティ監査を受ければ、自社のセキュリティ対策が正しく行われているか確認でき、不十分な点を洗い出して迅速に対処できます。また、顧客や取引先に、セキュリティ対策を適切に行っていることをアピールできます。

訴求ポイント

章を通した気づき・学び

企業や組織は、セキュリティ対策状況の有効性評価として定期的に内部・外部監査を実施することが重要です。

認識していただきたい実施概要

- ✓ 外部監査を行うことで、第三者視点で企業が保有する情報資産を守るための体制や環境が整っているかをチェックでき、また顧客や取引先に、セキュリティ対策を適切に行っているというアピールにも繋がること。
- ✓ 内部監査を行うことで、セキュリティのルールや文書の内容が適切かどうかの有効性をチェックでき、形骸化し、目的が見失われている状態を防止することに繋がること。

実践のために参考となる文献（参考文献）	
ISO/IEC 27001:2022	https://www.iso.org/standard/27001

19-3-1. 今後のアクション

本テキストでは、「DX推進の必要性からセキュリティ対策の実施手順を策定する」ところまでを解説しました。本テキストの内容を実践するにあたって行うべき事項を列挙し、概要を説明します。

本テキストの内容を実践するために行うべき事項

- テキストに記載された各章の理解を深め、経営者を含めた関係者と共有すること
- 経営者のリーダーシップによって社内体制を整備すること
- 整備した社内体制において順次具体的なアクションを実践すること

テキストに記載された各章の理解を深め、経営者を含めた関係者と共有すること

➢ **各章のポイントの理解**

テキストに記載された「セキュリティを考える上で必要となる社会情勢、国の施策に関する情報」、「セキュリティ対策を検討する上で必要となるセキュリティ知識」、「セキュリティ対策を実施するための具体的な手法」を再認識し、理解を深めること。

➢ **DX推進の考え方の把握**

- 社会情勢、国の施策からDX推進の方向性
  中小企業においてもDX推進が必要であること。
- 自組織におけるDX推進のための人材育成の必要性
  DXを推進する人材（DX推進スキル標準で示されたスキルを有する人材）や、DXを有効に利用できる人材（DXリテラシー標準で示されたスキルを有する人材（※プラスセキュリティを含む））の確保が必要であること。
- 自組織としてのDX推進の計画立案・実施内容の認識
  DX推進にあたってはDX with Security（DXの推進にあたり、セキュリティ対策を十分に考慮する）、IT構築にあたってはSecurity by Design（設計段階からのセキュリティ対策を考慮する）を意識すること。

➢ **セキュリティ対策の全容の認識**

サイバーセキュリティの脅威に対処するためのアプローチ手法としては「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」があり、それぞれのアプローチ方法には長所・短所があること。たとえば、ISMSなどのフレームワークを用いた網羅的アプローチは、時間とコストがかかるという短所があるものの、漏れのない対策が可能であるという長所があること。ISMSの仕組みや、管理策の全容を理解すること。

➢ **自組織でのセキュリティ対策の実施項目の認識**

- 自組織としての目標設定
  自組織のリスクを、経営上および社会的に許容できる範囲まで低減させるセキュリティ対策を実践すること。

1. リスクアセスメントによって自組織の現状のリスクを把握する。
2. リスクアセスメントの結果を踏まえ、管理策の中から自組織として実施すべき項目を選定する。
3. 実施する管理策に関して、自組織としての実施手順を策定する。

19-3-1. 今後のアクション

経営者のリーダーシップによって社内体制を整備すること

実施手順の実践準備

実施手順として策定した内容を実践するため、実行性のあるドキュメント（仕様書、運用マニュアルなど）を作成します。

実施手順の実践

実践にあたり、セキュリティ担当者とその役割・責任を決める必要があります。セキュリティ担当者とその役割・責任が決まった後、年間計画を作成して実践を行います。

①組織体制と役割の決定

セキュリティ対策を実施するための組織体制、役割・責任を決めます。

※第13章13ページ「管理策：5.3 組織の役割、責任及び権限」を参照。

②年間を通して実践すべき事項の例示

担当者がその役割・責任において次のような事項を実施します。これらの事項を実践するため、年間計画を作成します。

※第13章35ページ「管理策：8.1 運用の計画及び管理」を参照。

- リスクアセスメントの実施、リスク対応のための計画作成、管理策の検討
- 資産台帳の見直し
- 事業継続に関する試験
- 内部監査
- マネジメントレビュー
- 不適合及び是正処置のレビュー
- 定期教育
- 外部審査
- 情報セキュリティのための方針群のレビュー
- 秘密保持契約書の確認
- 「関係当局との連絡」体制の見直し
- 法令規制一覧表の確認
- 運用チェックリストによる確認
- 入退記録の確認
- など

上記の内容を実施するための年間計画を作成

19-3-1. 今後のアクション

年間計画（例）を紹介します。

期間	月	実施事項			
		年に1回	月に1回	四半期に1回	随時
第1四半期	4月	・課題に対する活動の検討	・入退記録の確認 ・運用チェックリストによる確認 ・バックアップされていることの確認 ・イベントログの確認 利用者が利用可能なソフトウェアの確認	・バックアップされていることの確認 ・イベントログのチェック	・「関係当局との連絡」体制の見直し ・法令規制一覧表の確認
	5月	・リスクアセスメントの実施	同上		
	6月	・リスク対応のための計画作成（アクションプランの作成） ・管理策（ルール）の検討	同上		
第2四半期	7月	・「情報セキュリティリスク対応」計画の実行	同上	同上	
	8月	・ISMSの有効性の評価 ・情報セキュリティパフォーマンス	同上		
	9月	・資産目録の見直し ・情報の分類 ・アクセス権限の見直し	同上		
第3四半期	10月	・システム開発の外部委託先の再審査	同上	同上	
	11月	・情報セキュリティ計画 ・情報セキュリティ継続の検証・レビュー	同上		
	12月	・内部監査計画 ・内部監査の実施 ・マネジメントレビュー ・不適合及び是正処置のレビュー	同上		
第4四半期	1月	・主要メンバーの「力量」の評価・証拠の文書化 ・定期教育 ・UPSのバッテリーの確認	同上	同上	
	2月	・外部審査（審査機関による更新審査）の実施	同上		
	3月	・情報セキュリティのための方針群のレビュー ・秘密保持契約書の確認	同上		

図83. 年間計画（例）

19-3-1. 今後のアクション

確立した社内体制において順次具体的なアクションを実践すること

管理策を実践するための参考となる情報

組織の中で具体的にどのように実施手順の内容を実践していくか、その際に参考となる各種資料や、実務的な取組例を紹介します。

管理策を実践するための参考となる情報	
ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド	https://isms-society.stores.jp/items/632a57a42e7452256400d84b
ISMS推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応1.0版	https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

実施手順を具体的に実践していくための取組例を紹介します。
以下は、実施手順を実際の業務として実践していくにあたり、実施手順と主体となって取組む必要がある担当者を対応付ける例です。

対策基準（例）	5.2 情報セキュリティの役割及び責任	5.5 関係当局との連絡	6.7 リモートワーク	8.15 ログ取得
実施手順（例）	情報セキュリティ委員会を設置する。	関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。	社内ネットワークへはVPNにて接続する。	バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。
トップマネジメント（経営層）	○	－	○	－
情報セキュリティ委員会	－	○	○	－
情報システム管理者	－	－	○	○
一般社員	－	-	○	－

図84. 実施手順とメインとなる担当者を対応付ける例

○：主体となって取組む必要がある。

19-3-1. 今後のアクション

継続的な情報収集

本テキストに記載の「①国の方針、社会の現状と今後の動向」、「②IT活用事例」、「③セキュリティインシデント事例」における内容は、日々更新されていきます。これらの情報を継続的に学ぶために参考となる文献を紹介します。

①国の方針、社会の現状と今後の動向	
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
経済財政運営と改革の基本方針2023	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf
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
Society5.0	https://www8.cao.go.jp/cstp/society5_0
サイバーセキュリティ2023の概要	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.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
②IT活用事例	
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
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/doc/tool/guide4youshiki_1.pdf
情報通信白書 令和2年版	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf
製造分野のDX事例集	https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf
「DX Selection 2023」選定企業レポート	https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf
③セキュリティインシデント事例	
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
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
コンピュータウイルス・不正アクセスの届出事例［2022年下半期（7月～12月）］	https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.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
2021年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-	https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf

人材育成

今後のビジネス発展のためには、人材育成が不可欠となります。人材育成を実践するために参考となる文献を紹介します。

①DSSに基づく人材育成	
デジタルスキル標準Ver.1.1 2023年8月	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf
②プラス・セキュリティ人材の育成	
「プラス・セキュリティ知識」とは？	https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf
サイバーセキュリティ経営ガイドラインVer2.0付録F サイバーセキュリティ体制構築・人材確保の手引き～ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1版	https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

おわりに

本テキストでは、「継続的に社内のセキュリティ対策ができる人材を育成し、実践的な課題解決で社内セキュリティ体制を強化すること」を目的とし、中小企業向けにセキュリティに関するさまざまな知識を解説いたしました。
ITの世界は日進月歩であり、常に企業を取り巻く環境が変化しています。定期的にテキストの内容を復習していただくとともに、参考文献などから常に最新の情報を収集し、セキュリティ対策を見直すことが大切です。

本テキストを通して、セキュリティ対策に関する幅広い選択肢と考え方を提供できたことを願っています。限定された対策ではなく、多様な選択肢から最適なセキュリティ対策を選び出すことの重要性を理解していただけたなら幸いです。選択する際には、自社のビジネス目標と照らし合わせ、最も適切な対策を見極めることが大切です。

セキュリティ対策を成功させるには、経営者との連携が欠かせません。対策費用の捻出や体制構築などは、経営者が主体となって行う必要があります。経営者と協力し、ビジネス目標に即したセキュリティ対策を策定し、実施することが今後のセキュリティ強化に向けての重要なステップとなります。

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

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

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

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

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

https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

DX白書2023

https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf

引用文献

【本編07】中小企業が組織として実施すべきサイバーセキュリティ対策【実施手順・実務者マニュアルレベル】＜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/464/index.html

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

サイバーセキュリティ経営ガイドライン Ver3.0

https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.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

攻めのIT活用指針

https://www.smrj.go.jp/doc/tool/guide4youshiki_1.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/tebiki2-0.pdf

「DX Selection 2022」選定企業レポート

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dx-selection2022-2.pdf

「DX Selection 2023」選定企業レポート

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf

経済財政運営と改革の基本方針2023　加速する新しい資本主義～未来への投資の拡大と構造的賃上げの実現～

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf

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

Society5.0

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

情報通信白書 令和2年版

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.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

MISSION 3-12 IoT、ビッグデータ、AI、ロボットの活用

https://www.cybersecurity.metro.tokyo.lg.jp/security/guidebook/212/index.html

製造分野のDX事例集

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

引用文献

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2023の概要

https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.pdf

企業経営のためのサイバーセキュリティの考え方の策定について

https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

ITおよびサイバーセキュリティに関する組織の視点6分類別に実施すべき対策

https://www.cybersecurity.metro.tokyo.lg.jp/security/docs/Sec01-11-02.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

デジタルスキル標準ver.1.1 2023年8月

https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf

「プラス・セキュリティ知識」とは？

https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf

サイバーセキュリティ経営ガイドラインVer2.0付録Fサイバーセキュリティ体制構築・人材確保の手引き
～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1版

https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.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

ISMS適合性評価制度

https://isms.jp/doc/JIP-ISMS120-62.pdf

サイバーセキュリティ経営ガイドラインと支援ツール

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性

https://www.meti.go.jp/policy/economy/consumer/credit/2022060221001.pdf

「個人情報」と「プライバシー」の違い

https://privacymark.jp/wakaru/kouza/theme1_03.html

ISMSとは

https://isms.jp/isms

ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド

https://isms-society.stores.jp/items/632a57a42e7452256400d84b

ISMS推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応1.0版

https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd

引用文献

政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_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Ver.1.0の概要

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.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Ver.1.0

https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

情報セキュリティポリシーの内容

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_executive_04-3.html

情報セキュリティ関連規程

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」

https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000

国民のためのサイバーセキュリティサイト | 用語辞典

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/glossary/glossary_01.html

JIPDEC ISMSユーザーズガイド –JIS Q 27001:2014(ISO/IEC 27001:2013)対応- -リスクマネジメント編-

https://m-p-o.co.jp/mpo/wp-content/uploads/2020/05/b823443df9d0ab703dd07bd352244f1d.pdf

MSQA ISMS推進マニュアル活用ガイドブック2022_第1.0版

https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOjEwNzI0fQ==&pNo=1

ISO/IEC 27005:2022

https://www.iso.org/standard/80585.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

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 付録7 リスク分析シート（全7シート）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx

JNSA 2-4 リスクアセスメントとリスク対応

https://www.jnsa.org/ikusei/01/02-04.html

2021年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-

https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf

情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

引用文献

中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

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

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

参考文献

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/

目的や所属・役割から選ぶ施策一覧

https://security-portal.nisc.go.jp/curriculum/

サイバー攻撃被害に係る情報の共有・公表ガイダンス

https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.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

マルウェア「ランサムウェア」の脅威と対策（対策編）

https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/ransomware_taisaku.html

情報セキュリティ関連規程（サンプル）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

自己点検チェックリスト

https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf

情報セキュリティポリシーサンプル改版（1.0版）

https://www.jnsa.org/result/2016/policy/

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

情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055529.pptx

インターネットの安全・安心ハンドブックVer 5.00

https://security-portal.nisc.go.jp/guidance/handbook.html

テレワークセキュリティガイドライン第5版

https://www.soumu.go.jp/main_content/000752925.pdf

中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

ISO/IEC 27001:2022

https://www.iso.org/standard/27001

ISO/IEC 27002:2022

https://www.iso.org/standard/75652.html

参考文献

国民のためのサイバーセキュリティサイト　サイバーセキュリティ関連の法律・ガイドライン

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/basic_legal.html

セキュリティ・バイ・デザイン導入指南書

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf

政府情報システムにおけるセキュリティ・バイ・デザインガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/2a169f83/20220630_resources_standard_guidelines_guidelines_01.pdf

ゼロトラスト導入指南書 ～情報系・制御系システムへのゼロトラスト導入～

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/ngi93u0000002klo-att/000092243.pdf

（参考資料1）民間企業におけるゼロトラスト導入事例

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5805a275-3e16-4296-8a94-6557b58c6a4c/dd52a824/20231124_meeting_network_casestudie_03.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

証拠保全ガイドライン 第9版

https://digitalforensic.jp/wp-content/uploads/2023/02/shokohoznGL9.pdf

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。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代からはじまる第三次AIブームである。
「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
…… 1-1-1、4-1-1、4-2-5、5-2-1、5-2-2、5-2-3、6-1-1、6-1-3、19-2-1、19-2-4、19-2-5

■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、6-1-3、7-5-3

■CVSS
Common Vulnerability Scoring Systemの略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSSを用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門家、管理者、ユーザなどの間で、脆弱性に関して共通の言葉で議論できるようになる
…… 17-2-1

■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3章コラム、10-1-1、19-2-10

■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
…… 5-2-1

■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
…… 2-2-4、2-2-5、3-1-1、12-3-1、16-2-1、17-2-4、19-2-3、19-2-10

■eKYC
electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと
…… 5-2-1

■GビズID
行政手続きなどにおいて手続を行う法人を認証するための仕組み。1つのID・パスワードで本人確認書類なしに様々な政府・自治体の法人向けオンライン申請が可能になる
…… 5-2-1

■ICSCoE中核人材育成プログラム
2017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
…… 2-1-2

用語集

■ICT
Information and Communication Technologyの略。IT（情報技術）だけでなく、コンピュータやスマートフォン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
…… 4-1-2、5-2-1、6-1-1、7-2-2、7-3-2、14-1-1、14-1-2、17-2-2、19-2-4、19-2-14

■IDS
Intrusion Detection Systemの略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPSと異なり、不正アクセスや異常な通信をブロックする機能はない。
…… 17-1-2、17-2-4、17-2-5

■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、家電など様々な「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
…… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5、5-2-2、5-2-3、6-1-2、7-4-1、19-2-2、19-2-5

■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、17-1-2、17-2-2、17-2-4、17-2-5

■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になる数字の組み合わせ。 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4つになる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、6-2-2、17-2-2

■ISAC
Information Sharing and Analysis Centerの略。業界内での情報共有・連携の取組み推進を図る組織のこと。国内では、金融や交通、電力、ICTなどの分野にISACがある。ICT-ISACでは、ICT分野の情報セキュリティに関する情報(インシデント情報を含む。)の収集・調査・分析を行っている。
…… 14-1-2

■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、法令的な対策を含む、経営者を頂点とした総合的で組織的な取組。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、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-2、7-3-4、7-4-1、7-5-1、第7章コラム、8-1-2、9-1-1、第10章コラム、11-1-3、11-2-1、11-2-2、13-1-1、13-2-1、13-2-2、13-2-3、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、第13章コラム、14-1-1、15-1-1、16-1-1、17-1-1、19-1-1、19-1-2、19-2-7 、19-2-8 、19-2-9 、19-2-11 、19-2-13 、19-2-14 、19-2-15 、19-2-16 、19-2-17 、19-3-1

■ISP
個人や企業などに対してインターネットに接続するためのサービスを提供する事業者のこと。ユーザはISPと契約し、回線を用いてISPが運営するネットワークに接続することで、インターネット上のサーバーなどへアクセスできる。
…… 14-1-2

■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
…… 3-1-1

用語集

■JPCERT/CC
日本におけるセキュリティインシデントなどの報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取組んでいる。
…… 14-1-2

■JVN
Japan Vulnerability Notesの略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと。…… 14-1-2

■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

■MACアドレス
Media Access Control addressの略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器やPC、ルータなどについている固有の識別番号で、一般的に12桁の16進数で「00-00-00-XX-XX-XX」などと表される。
…… 17-2-2

■NISC
National center of Incident readiness and Strategy for Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…… 5-2-1、6-1-3、12-3-1、19-1-1、19-2-6

■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、日本も今後普及が見込まれる
…… 3-4-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4、7-4-1、19-2-7

■NTP
Network Time Protocolの略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている。
…… 17-1-2

■PII
Personally Identifiable Informationの略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と1対1に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号だけでなく、氏名、生年月日、住所、勤務先などの情報もPIIに含まれる。
…… 14-1-1、14-1-2、19-2-14

■RPA
Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…… 4-2-3

■SASE（サシー）
Secure Access Service Edgeの略。2019年に提唱され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、17-2-2

■SBOM（エスボム）
Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…… 6-1-1

用語集

■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、17-2-2、17-2-4

■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、3-3-1、19-2-3

■SLA
Service Level Agreementの略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの。
…… 17-1-2

■Society5.0
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、4-1-1、5-2-2、6-1-1、7-1-2、7-4-1、19-1-1、19-1-2、19-2-1、19-2-4、19-2-5、19-3-1

■SSL/TLS
WebサーバとWebブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去にはSSLが使われていたが、脆弱性が発見されたため、TLS（v.1.2以降）への移行が進んでおり、今ではSSLは使われなくなってきている。しかし、歴史的経緯でSSLの用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する。
…… 14-1-2、17-1-2

■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、17-2-2、17-2-4

■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、12-3-1、13-2-2、14-1-2、15-1-2、16-2-1、17-2-2、17-2-3、19-3-1

■WAF（ワフ）
Web Application Firewallの略。 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

■WAN
Wide Area Networkの略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。
一方、狭義には、物理的に離れた場所にあるLAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザしかアクセスできない。このプライベートなWANを構築する場合には、通信事業者に依頼する必要がある。
…… 17-2-3

■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を制限する機能のこと
…… 2-2-5、第3章コラム、7-2-2、7-3-2、9-1-1、14-1-1、14-1-2、17-1-1、17-2-2、17-2-4、19-2-9、19-2-14

用語集

■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
…… 2-2-4、11-1-2、17-1-1、17-1-2

■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
…… 2-1-3、2-2-1、2-2-5、2-3-2、3-3-3、3-4-1、第3章コラム、7-2-2、12-2-1、12-3-1、14-1-1、14-1-2、16-1-2、17-1-2、17-2-3、17-2-5

■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

■イベントログ
コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと。
…… 13-2-6、17-1-2、19-3-1

■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、11-1-2

■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
…… 3-1-1、3-3-2、3-3-3、12-3-1、17-1-2

■エンティティ
個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと
…… 7-2-1、17-2-2

■エンドポイントデバイス
ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…… 2-2-4、17-1-1、17-2-2、17-2-4

■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分野では、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、5-2-2、6-1-3、8-1-2、10-1-2、11-2-2、11-3-1、12-3-1、14-1-1、14-1-2、17-1-2、17-2-3

■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3章コラム、7-1-2、7-2-1、7-2-2、9-1-2 、10-1-1、第10章コラム、11-2-2、12-2-1、13-2-4、13-2-5、 14-1-1 、14-1-2、 16-1-1 、17-1-1、17-1-2、17-2-4、19-2-7

■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3章コラム、7-1-2、7-2-1、7-2-2、9-1-2、10-1-1、第10章コラム、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1、16-1-1、17-1-2、17-2-4 、19-2-7

■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3章コラム、7-1-2、7-2-1、7-2-2、9-1-2、10-1-1、第10章コラム、11-2-2、12-2-1、13-2-4、13-2-5、 14-1-1、16-1-1、17-1-2、17-2-4、19-2-7

■脅威インテリジェンス
サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている。
…… 7-2-2、7-3-2、14-1-1、14-1-2、17-2-1、19-2-14

用語集

■供給者
組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PCやサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある。
…… 7-2-2、7-3-2、9-1-1、9-1-2、13-2-7、14-1-1、14-1-2、17-2-1、17-2-2、19-2-9、19-2-14

■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
…… 第3章コラム

■クリーンインストール
すでにインストールされているOSを削除したうえで、新しくOSを再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある。
…… 17-2-5

■限定提供データ
不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」
…… 11-2-2

■コーディング
プログラミング言語でソースコードを書くこと。
…… 7-2-2、17-1-1、17-1-2、17-2-1、19-2-17

■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、5-2-1、6-2-1、8-1-2、14-1-2

■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。
…… 2-1-2、2-1-3、2-2-2、2-2-5、2-3-2、3-1-1、3-4-1、4-3-1、4-3-2、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-1、7-1-2、7-3-1、7-4-1、7-5-1、7-5-2、7-5-3、10-1-1、11-2-2、12-3-1、13-2-4、13-2-5、17-2-2、17-2-3、17-2-4、18-1-2、19-1-1、19-1-2、19-2-2、19-2-4、19-2-5、19-2-7、19-2-10、19-2-18、19-3-1

■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

■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、5-1-1、6-1-1、19-1-1、19-1-2、19-2-6、19-3-1

■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、7-1-1、7-1-2、7-4-1、19-2-7

用語集

■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、4-1-1、4-2-4、4-3-2、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3、7-2-2、7-3-2、7-3-3、7-4-1、7-5-1、7-5-2、14-1-1、14-1-2、17-2-2、18-1-2、19-2-2、19-2-5、19-2-14

■サポートユーティリティ
情報システムを運用する施設の稼動に不可欠な設備やライフライン、公共インフラのこと。ISO/IEC 27002:2022では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調をあげている。
…… 7-2-2、16-1-1、16-1-2、19-2-16

■磁気データ消去装置
ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる。
…… 17-1-2

■シャドーIT
従業員が業務に使用するIT機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの。
…… 16-2-1、17-2-2、19-2-16

■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、7-2-3、7-3-2、7-5-1、8-1-2、10-1-1、11-1-1、11-1-2、11-2-2、11-2-3、12-2-1、12-3-1、13-2-3、13-2-4、13-2-5、13-2-7、第13章コラム、14-1-2、16-1-2、17-2-2、17-2-4、18-1-2、19-2-10 、19-2-17 、19-2-18

■情報セキュリティ事象
情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。
情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される。
…… 7-2-2、7-3-2、9-1-2、14-1-1、14-1-2、15-1-1、15-1-2、17-1-2、17-2-4、19-2-14、19-2-15

■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3章コラム、第10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
…… 2-1-3、第3章コラム、6-1-3、7-2-1、第10章コラム、17-1-2

■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
…… 第3章コラム、6-1-1、6-1-3、7-2-1、7-4-1、第10章コラム、13-2-5、14-1-2、17-1-2

■スクリーンセーバ
離席時にPCの画面の内容を盗み見されることを防ぐ機能のこと。PCに対して一定時間ユーザによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする。
…… 13-2-5、17-1-2

■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、16-1-2

用語集

■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
…… 2-1-1、2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-1-1、3-4-1、第3章コラム、6-1-1、6-1-3、7-2-2、9-1-2、10-1-1、10-1-2、10-1-3、11-1-2、11-1-3、11-2-2、11-2-3、11-3-1、13-2-4、14-1-1、14-1-2、17-1-1、17-1-2、17-2-1、17-2-4、19-1-1、19-1-2、19-2-2、19-2-10

■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、17-2-1

■責任追跡性
情報資産に対する参照や変更などの操作を、どのユーザが行ったものかを確認することができる特性
…… 第3章コラム、7-2-1 、第10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。たとえば、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
…… 2-1-1、2-1-2、2-1-3、2-2-1、3-1-1、4-3-2、7-2-2、7-3-2、7-5-1、9-1-1、9-1-2、12-1-1、12-2-1、13-2-2、13-2-4、13-2-5、13-2-8、14-1-1、14-1-2、17-1-1、17-1-2、17-2-1、17-2-4、17-2-5、19-1-1、19-1-2、19-2-2、19-2-9、19-2-12、19-2-14、19-3-1

■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、6-1-1、10-1-1、10-1-2、12-3-1

■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、6-1-2、7-5-1、8-1-1、17-2-4、19-2-2、19-2-8

■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、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
…… 2-2-4、17-2-2、19-2-17

■ソフトウェアライブラリ
プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1から作る必要がなくなり、効率的に開発を行うことができる。
…… 17-1-1

■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、14-1-2、17-1-2、17-2-2、17-2-4

用語集

■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て認証する安全性が高い認証方法。たとえば、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
…… 2-2-5、2-3-3、8-1-2、第10章コラム、11-3-1、12-3-1、14-1-2、17-1-2

■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

■データマスキング
個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（アスタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする。
…… 7-2-2、17-1-1、17-1-2、19-2-17

■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）にするのがデジタイゼーション、音楽をダウンロード販売するのがデジタライゼーションである
…… 1-1-1、2-1-1、2-1-2、4-1-2、4-2-3、5-1-1、5-2-1、6-1-1、6-1-3、第6章コラム、7-4-1、19-2-1、19-2-4、19-2-5

■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3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、データ量のこと。
…… 3-1-1、17-2-2、17-2-3

■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、7-2-1、7-2-3、7-3-2、13-2-3、13-2-6、13-2-7、13-2-8、14-1-2、18-1-1、19-2-18、19-3-1

■ハウジングサービス
データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある。
…… 12-3-1

■ビジネスインパクト分析
災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てるうえで実行する必要がある。
…… 14-1-2

■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

用語集

■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、5-2-2、5-2-3、19-2-1

■否認防止性
システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性
…… 第3章コラム 、第10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
…… 2-1-2、2-1-3、12-3-1、13-2-5、19-2-10

■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、19-2-2

■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、3-1-1、13-2-2、14-1-2、17-1-2、17-2-2、17-2-3、17-2-4、17-2-5

■ファイル共有ソフト
複数の利用者によるネットワークでのファイルのやりとりを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトは、使用を禁止する必要がある。
…… 16-2-1、17-1-2

■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
…… 2-1-1、2-1-2、2-1-3、2-2-1、2-2-2、2-2-3、2-2-5、2-3-1、3-1-1、4-3-2、5-2-1、8-1-2、10-1-1、10-1-3、11-2-2、11-3-1、14-1-2、16-2-1、17-1-2、17-2-4、17-2-5、19-2-2、19-2-10、19-2-16、19-3-1

■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、4-3-2、18-1-2

■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
…… 2-2-3、2-3-2、17-2-5、19-2-17

用語集

■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を指す。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、3-4-1、6-1-1、7-1-1、7-1-2、7-2-1、7-2-2、7-3-1、7-4-1、8-1-1、8-1-2、9-1-2、13-1-1、13-2-1、19-1-1、19-1-2、19-2-7、19-2-8、19-2-13、19-3-1

■プロキシ
クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。
プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Webサーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる。
…… 17-2-4

■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よい成果をもたらす方法論
…… 2-1-3、2-3-1、7-1-1、19-2-2

■ペネトレーションテスト
ネットワークに接続されたシステムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する。
…… 17-2-1

■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、3-1-1、第3章コラム、7-2-2、11-2-2、12-3-1、13-2-4、14-1-1、14-1-2、15-1-2、16-2-1、17-1-1、17-1-2、17-2-2、17-2-4、19-2-17

■ミドルウェア
OSとアプリケーションの中間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやりとりをミドルウェアが担うことで複雑な処理を行うことができる。
…… 17-2-1、17-2-3

■ミラサポコネクト
ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤
…… 5-2-1

■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にアクセスできる
…… 3-3-3、14-1-2、16-1-2、17-1-2

■無停電電源装置
UPSとも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる。
…… 14-1-2、16-1-2

■ユーティリティプログラム
コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある。
…… 7-2-2、17-1-1、17-1-2、19-2-17

用語集

■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、3-1-1、6-1-1、7-5-1、8-1-2、14-1-2、17-1-2、17-2-4、17-2-5、19-2-2

■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は何らかの対策を講じる必要がある
…… 3-4-1、7-2-2、7-3-2、第7章コラム、11-1-1、11-1-2、11-1-3、11-2-1、11-2-2、11-3-1、12-2-1、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、14-1-1、14-1-2、15-1-1、16-1-1、17-1-1、17-1-2、19-1-1、19-1-2、19-2-11、19-2-14、19-2-15、19-2-16、19-2-17、19-3-1

■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、3-4-1、7-3-2、11-1-2、11-2-4、11-3-1、12-2-1、13-2-4、第13章コラム、17-2-4、19-2-11

■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
…… 2-2-2

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

2024年4月 Ver.1.0 初版発行

編集・発行　東京都産業労働局商工部経営支援課
新宿区西新宿二丁目8番1号

電話番号　03-5320-4770

監修　前川 徹
東京通信大学 情報マネジメント学部 教授
肩書は発行当時

ガイドブックの利用について
このガイドブックは、東京都が著作権を保有しておりますが、利用に際しては、非営利目的、サイバーセキュリティ対策の普及・啓発目的であれば、事前の申請などは必要ありません。
全体を利用されるのであればそのままご利用いただけます。
また、一部分の「引用・参考・参照・転載」であれば、出典元を明記して頂ければご利用いただけます。

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

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

別添資料

東京都産業労働局

目次

概要

「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」で紹介した内容の補足や、参考となる情報を紹介します。

本書を通して、テキスト本体で紹介した内容の理解をさらに深めていただきたいと思います。

1. ISO/IEC 27002:2022 管理策と目的

5.組織的管理策		
標題	**管理策**	**目的**
5.1 情報セキュリティのための方針群	情報セキュリティ方針及びトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員及び関連する利害関係者へ伝達し認識され、計画した間隔で及び重要な変化が発生した場合にレビューすることが望ましい。	事業、法令、規制及び契約上の要求事項に従って、経営陣の方向性の継続的な適合性、適切性、有効性、及び情報セキュリティのサポートを確実にするため。
5.2 情報セキュリティの役割及び責任	情報セキュリティの役割及び責任を、組織の要求に従って定め、割り当てることが望ましい。	組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。
5.3 職務の分離	相反する職務及び責任範囲は、分離することが望ましい。	情報セキュリティ管理策の不正、エラー及び回避のリスクを軽減するため。
5.4 経営陣の責任	経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針及び手順に従った情報セキュリティの適用を、すべての要員に要求することが望ましい。	経営陣が、情報セキュリティにおける自らの役割を理解し、すべての要員が自らの情報セキュリティの責任を認識し、果たすことを確実にすることを目的として行動することを確実にするため。
5.5 関係当局との連絡	組織は関係当局との連絡体制を確立及び維持することが望ましい。	組織と、関連する法務、規制及び監督当局との間で、情報セキュリティに関して適切な情報の流通が行われることを確実にするため。
5.6 専門組織との連絡	組織は、情報セキュリティに関する研究会または会議、及び情報セキュリティの専門家による協会・団体との連絡体制を確立し維持することが望ましい。	情報セキュリティに関して適切な情報流通が行われることを確実にするため。
5.7 脅威インテリジェンス	情報セキュリティの脅威に関連する情報を収集及び分析し、脅威インテリジェンスを構築することが望ましい。	適切なリスク低減処置を講じることができるように、組織の脅威環境についての認識をもつため。
5.8 プロジェクトマネジメントにおける情報セキュリティ	情報セキュリティをプロジェクトマネジメントに組み入れることが望ましい。	プロジェクト及び成果物に関連する情報セキュリティリスクが、プロジェクトのライフサイクル全体を通じてプロジェクトマネジメントで効果的に対処されることを確実にするため。
5.9 情報及びその他の関連資産の目録	管理責任者を含む情報及びその他の関連資産の目録を作成し、維持することが望ましい。	組織の情報及びその他の関連資産を特定し、それらの情報セキュリティを維持し、適切な管理責任を割り当てるため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

5.組織的管理策		
標題	**管理策**	**目的**
5.10 情報及びその他の関連資産の利用の許容範囲	情報及びその他の関連資産の利用並びに取扱手順の許容範囲に関する規則は、明確にし、文書化し、実施することが望ましい。	情報及びその他の関連資産が適切に保護、利用及び取扱いされることを確実にするため。
5.11 資産の返却	要員及び必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却することが望ましい。	雇用、契約、または合意を変更または終了するプロセスの一環として、組織の資産を保護するため。
5.12 情報の分類	情報は、機密性、完全性、可用性及び関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類することが望ましい	組織における情報の重要度に従って、情報の保護の要件を特定及び理解することを確実にするため。
5.13 情報のラベル付け	情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施することが望ましい。	情報の分類の伝達を容易にし、情報の処理及び管理の自動化を支援するため。
5.14 情報転送	情報転送の規則、手順または合意を、組織内及び組織と他の関係者との間のすべての種類の転送設備に関して備えることが望ましい。	組織内及び外部の利害関係者との間で転送される情報のセキュリティを維持するため。
5.15 アクセス制御	情報及びその他の関連資産への物理的及び論理的アクセスを制御するための規則を、業務及び情報セキュリティの要求事項に基づいて確立し、実施することが望ましい。	情報及びその他の関連資産への認可されたアクセスを行わせ、認可されていないアクセスを防ぐことを確実にするため。
5.16 識別情報の管理	識別情報のライフサイクル全体を管理することが望ましい。	組織の情報及びその他の関連資産にアクセスする個人及びシステムを一意に特定できるようにし、アクセス権を適切に割り当てることができるようにするため。
5.17 認証情報	認証情報の割当て及び管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理することが望ましい。	適切なエンティティ認証を確実にし、認証プロセスの失敗を防ぐため。
5.18 アクセス権	情報及びその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針及び規則に従って、提供、レビュー、変更及び削除することが望ましい。	情報及びその他の関連資産へのアクセスが、業務上の要求事項に従って定義及び認可されることを確実にするため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

5.組織的管理策		
標題	**管理策**	**目的**
5.19 供給者関係における情報セキュリティ	供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセス及び手順を定義し実施することが望ましい。	供給者関係において合意したレベルの情報セキュリティを維持するため。
5.20 供給者との合意における情報セキュリティの取扱い	供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意することが望ましい。	供給者関係において合意したレベルの情報セキュリティを維持するため。
5.21 ICTサプライチェーンにおける情報セキュリティの管理	ICT 製品及びサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順を定義し実施することが望ましい。	供給者関係において合意したレベルの情報セキュリティを維持するため。
5.22 供給者のサービス提供の監視、レビュー及び変更管理	組織は、供給者の情報セキュリティの実践及びサービス提供の変更を定常的に監視し、レビューし、評価し、管理することが望ましい。	供給者との合意に沿って、合意したレベルの情報セキュリティ及びサービス提供を維持するため。
5.23 クラウドサービス利用における情報セキュリティ	クラウドサービスの取得、利用、管理及び終了のプロセスを、組織の情報セキュリティ要求事項に従って確立することが望ましい。	クラウドサービスの利用における情報セキュリティを規定及び管理するため。
5.24 情報セキュリティインシデント管理の計画及び準備	組織は、情報セキュリティインシデント管理のプロセス、役割及び責任を定義、確立及び伝達することによって、情報セキュリティインシデント管理を計画及び準備することが望ましい。	情報セキュリティ事象に関する伝達を含む、情報セキュリティインシデントへの迅速で、効果的で、一貫性があり、かつ秩序のある対応を確実にするため。
5.25 情報セキュリティ事象の評価及び決定	組織は情報セキュリティ事象を評価し、それらを情報セキュリティインシデントに分類するか否かを決定することが望ましい。	情報セキュリティ事象の効果的な分類及び優先順位付けを確実にするため。
5.26 情報セキュリティインシデントへの対応	情報セキュリティインシデントは、文書化した手順に従って対応することが望ましい。	情報セキュリティインシデントへの効率的かつ効果的な対応を確実にするため。
5.27 情報セキュリティインシデントからの学習	情報セキュリティインシデントから得られた知識は、情報セキュリティ管理策を強化し、改善するために用いることが望ましい。	将来のインシデントの起こりやすさまたは影響を減らすため。
5.28 証拠の収集	組織は、情報セキュリティ事象に関連する証拠の特定、収集、取得及び保存のための手順を確立し、実施することが望ましい。	懲戒処置及び法的処置の目的で、情報セキュリティインシデントに関連する証拠の一貫した効果的な管理を確実にするため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

5.組織的管理策		
標題	**管理策**	**目的**
5.29 事業の中断・阻害時の情報セキュリティ	組織は、事業の中断・阻害時に情報セキュリティを適切なレベルに維持する方法を計画することが望ましい。	事業の中断・阻害時に情報及びその他の関連資産を保護するため。
5.30 事業継続のためのICTの備え	事業継続の目的及び ICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持及び試験することが望ましい。	事業の中断・阻害時に組織の情報及びその他の関連資産の可用性を確実にするため。
5.31 法令、規制及び契約上の要求事項	情報セキュリティに関連する法令、規制及び契約上の要求事項、並びにこれらの要求事項を満たすための組織の取組を特定し、文書化し、また、最新に保つことが望ましい。	情報セキュリティに関連する法令、規制及び契約上の要求事項の順守を確実にするため。
5.32 知的財産権	組織は知的財産権を保護するための適切な手順を実施することが望ましい。	知的財産権及び権利関係のある製品の利用に関連する、法令、規制及び契約上の要求事項の順守を確実にするため。
5.33 記録の保護	記録は、消失、破壊、改ざん、認可されていないアクセス及び不正な流出から保護することが望ましい。	法令、規制及び契約上の要求事項、並びに記録の保護及び可用性に関連する共同体または社会の期待の順守を確実にするため。
5.34 プライバシー及びPIIの保護	組織は、適用される法令、規制及び契約上の要求事項に従って、プライバシーの維持及び PII の保護に関する要求事項を特定し、満たすことが望ましい。	PIIの保護の情報セキュリティの側面に関連する法令、規制及び契約上の要求事項の順守を確実にするため。
5.35 情報セキュリティの独立したレビュー	人、プロセス及び技術を含む、情報セキュリティ及びその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施することが望ましい。	情報セキュリティを管理するための組織の取組の継続的な適切性、十分性及び有効性を確実にするため。
5.36 情報セキュリティのための方針群、規制および標準の順守	組織の情報セキュリティ方針、トピック固有の個別方針、規則及び標準を順守していることを定期的にレビューすることが望ましい。	情報セキュリティが組織の情報セキュリティ方針、トピック固有の個別方針、規則及び標準に従って実施及び運用されることを確実にするため。
5.37 操作手順書	情報処理設備の操作手順は、文書化し、必要とする要員に対して利用可能とすることが望ましい。	情報処理設備の正確かつセキュリティに配慮した操作を確実にするため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

6.人的管理策		
標題	**管理策**	**目的**
6.1 選考	要員になるすべての候補者についての経歴などの確認は、組織に加わる前に、適用される、規制及び倫理を考慮に入れて継続的に行うことが望ましい。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うことが望ましい。	すべての要員が、予定する役割に対して適格かつ適切であり、雇用中に適格かつ適切であり続けることを確実にするため。
6.2 雇用条件	雇用契約書には、情報セキュリティに関する要員及び組織の責任を記載することが望ましい。	要員が、予定する役割における自らの情報セキュリティの責任を理解することを確実にするため。
6.3 情報セキュリティの意識向上、教育及び訓練	組織の要員及び関連する利害関係者は、職務に関連する組織の情報セキュリティ方針、トピック固有の個別方針及び手順についての、適切な、情報セキュリティに関する意識向上、教育及び訓練を受け、また、定めに従ってその更新を受けることが望ましい。	要員及び関連する利害関係者が自らの情報セキュリティの責任を意識し、それを果たすことを確実にするため。
6.4 懲戒手続	情報セキュリティ方針違反を犯した要員及びその他の関連する利害関係者に対して処置をとるために、懲戒手続を正式に定め、伝達することが望ましい。	要員及びその他の関連する利害関係者が情報セキュリティ方針違反の結果を理解すること、違反を阻止すること、及びそれを犯した要員及びその他の関連する利害関係者を適切に扱うことを確実にするため。
6.5 雇用の終了または変更後の責任	雇用の終了または変更の後もなお有効な情報セキュリティに関する責任及び義務を定め、実施し、関連する要員及びその他の利害関係者に伝達することが望ましい。	雇用または契約を変更または終了する手続の一部として、組織の利益を保護するため。
6.6 秘密保持契約または守秘義務契約	情報保護に対する組織の要求事項を反映する秘密保持契約または守秘義務契約は、特定し、文書化し、定めに従ってレビューし、要員及びその他の関連する利害関係者が署名することが望ましい。	要員または外部の関係者がアクセスできる情報の秘密保持を維持するため。
6.7 リモートワーク	組織の施設外でアクセス、処理または保存される情報を保護するために、要員が遠隔で作業している場合に、セキュリティ対策を実施することが望ましい。	要員が遠隔で作業している場合に情報のセキュリティを確実にするため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

6.人的管理策		
標題	**管理策**	**目的**
6.8 情報セキュリティ事象の報告	組織は、要員が発見した又は疑いをもった情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告するための仕組みを設けることが望ましい。	要員が、特定可能な情報セキュリティ事象を時機を失せず、一貫性をもって効果的に報告することを支援するため。
7.物理的管理策		
標題	**管理策**	**目的**
7.1 物理的セキュリティ境界	情報及びその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いることが望ましい。	組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷及び干渉を防ぐため。
7.2 物理的入退	セキュリティを保つべき領域は、適切な入退管理策及び立寄り場所によって保護することが望ましい。	組織の情報及びその他の関連資産に、認可された物理的アクセスだけがなされることを確実にするため。
7.3 オフィス、部屋及び施設のセキュリティ	オフィス、部屋及び施設に対する物理的セキュリティを設計し、実装することが望ましい。	オフィス、部屋及び施設内の組織の情報及びその他の関連資産への認可されていない物理的アクセス、損傷、並びに干渉を防ぐため。
7.4 物理的セキュリティの監視	施設は、認可されていない物理的アクセスについて継続的に監視することが望ましい	認可されていない物理的アクセスを検知し、抑止するため。
7.5 物理的および環境的脅威からの保護	基盤に対する、自然災害及びその他の意図的または意図的でない物理的脅威などの物理的及び環境的脅威に対する保護を設計し実装することが望ましい。	物理的及び環境的脅威に起因する事象の結果を防止または低減するため。
7.6 セキュリティを保つべき領域での作業	セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実装することが望ましい。	セキュリティを保つべき領域にある情報及びその他の関連資産を、これらの領域で働く要員による損傷及び認可されていない干渉から保護するため。
7.7 クリアデスク・クリアスクリーン	書類及び取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定義し、適切に実施させることが望ましい。	通常の勤務時間内及び時間外の、机、スクリーン及びその他のアクセス可能な場所にある情報への認可されていないアクセス、情報の消失及び損傷のリスクを低減するため。
7.8 装置の設置および保護	装置は、セキュリティを保って設置し、保護することが望ましい。	物理的及び環境的脅威、並びに認可されていないアクセス及び損傷によるリスクを低減するため。
7.9 構外にある資産のセキュリティ	構外にある資産を保護することが望ましい。	構外にある装置の紛失、損傷、盗難または侵害、及び組織の業務の中断を防止するため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

7.物理的管理策		
標題	**管理策**	**目的**
7.10 記憶媒体	記憶媒体は、組織における分類体系及び取扱いの要求事項に従って、取得、使用、移送及び廃棄のライフサイクルを通じて管理することが望ましい。	記憶媒体上の情報に対して認可された開示、変更、移動または破棄だけがなされることを確実にするため。
7.11 サポートユーティリティ	情報処理施設は、サポートユーティリティの不具合による、停電、その他の故障から保護することが望ましい。	サポートユーティリティの故障及び事業の中断・阻害による情報及びその他の関連資産の消失、損傷若しくは侵害、または組織の運用の中断を防止するため。
7.12 ケーブル配線のセキュリティ	電源ケーブル、データ伝送ケーブルまたは情報サービスをサポートするケーブルの配線は、傍受、妨害または損傷から保護することが望ましい。	通信ケーブル及び電源ケーブルの配線に関連した、情報及びその他の関連資産の消失、損傷、盗難または侵害、並びに組織の運用の中断を防止するため。
7.13 装置の保守	装置は、情報の可用性、完全性及び機密性を維持することを確実にするために、正しく保守することが望ましい。	保守の不足による、情報及びその他の関連資産の消失、損傷、盗難または侵害、並びに組織の運用の中断を防止するため。
7.14 装置のセキュリティを保った処分又は再利用	記憶媒体を内蔵した装置は、処分又は再利用する前に、すべての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又はセキュリティを保って上書きしていることを確実にするために、検証することが望ましい。	処分または再利用する装置からの情報漏えいを防止するため。
8.技術的管理策		
標題	**管理策**	**目的**
8.1 利用者エンドポイント機器	利用者終端装置に保存し、そこで処理し、またはそれを通じてアクセス可能な情報を保護することが望ましい。	利用者終端装置を使用することによってもたらされるリスクから情報を保護するため。
8.2 特権的アクセス権	特権的アクセス権の割当て及び利用は、制限し、管理することが望ましい。	認可された利用者、ソフトウェア構成要素及びサービスだけに特権的アクセス権が与えられることを確実にするため。
8.3 情報へのアクセス制限	情報及びその他の関連資産へのアクセスは、アクセス制御に関する確立されたトピック固有の個別方針に従って、制限することが望ましい。	情報及びその他の関連資産への認可されたアクセスだけを確実にし、認可されていないアクセスを防止するため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

8.技術的管理策		
標題	**管理策**	**目的**
8.4 ソースコードへのアクセス	ソースコード、開発ツール、及びソフトウェアライブラリへの読取り及び書込みアクセスを適切に管理することが望ましい。	認可されていない機能が入り込むことを防止し、意図しないまたは悪意のある変更を回避し、価値の高い知的財産の機密性を維持するため。
8.5 セキュリティを保った認証	セキュリティを保った認証技術及び手順を、情報アクセス制限、及びアクセス制御に関するトピック固有の個別方針に基づいて備えることが望ましい。	システム、アプリケーション及びサービスへのアクセスを許可するときに、利用者またはエンティティをセキュリティを保って認証することを確実にするため。
8.6 容量・能力の管理	現在の及び予測される容量・能力の要求事項に合わせて、資源の利用を監視し調整することが望ましい。	情報処理施設、人的資源、オフィス及びその他の施設で必要とされる容量・能力の確保を確実にするため。
8.7 マルウェアに対する保護	マルウェアに対する保護は、利用者の適切な認識によって実施及び支援することが望ましい。	情報及びその他の関連資産をマルウェアに対して保護することを確実にするため。
8.8 技術的脆弱性の管理	利用中の情報システムの技術的脆弱性に関する情報を獲得することが望ましい。また、そのような脆弱性に組織がさらされている状況を評価することが望ましい。さらに、適切な手段をとることが望ましい。	技術的脆弱性の悪用を防止するため。
8.9 構成管理	ハードウェア、ソフトウェア、サービス及びネットワークのセキュリティ構成を含む構成を確立し、文書化し、実装し、監視及びレビューすることが望ましい。	ハードウェア、ソフトウェア、サービス及びネットワークが、必要とされるセキュリティ設定で正しく機能し、認可されていない変更または誤った変更によって構成が変えられないことを確実にするため。
8.10 情報の削除	情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった場合は削除することが望ましい。	取扱いに慎重を要する情報の不必要な漏えいを防止し、情報の削除に関する法令、規制及び契約上の要求事項を順守するため。
8.11 データマスキング	データマスキングは、適用される法律を考慮して、アクセス制御に関する組織のトピック固有の個別方針及びその他の関連するトピック固有の個別方針、並びに業務要求事項に従って使用することが望ましい。	PII を含む、取扱いに慎重を要するデータの開示を制限し、法令、規制及び契約上の要求事項を順守するため。
8.12 データ漏えいの防止	データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存または送信するシステム、ネットワーク及びその他の装置に適用することが望ましい。	個人またはシステムによる情報の認可されていない開示及び抽出を検出し防止するため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

8.技術的管理策		
標題	**管理策**	**目的**
8.13 情報のバックアップ	合意されたバックアップに関するトピック固有の個別方針に従って、情報、ソフトウェア及びシステムのバックアップを維持し、定期的に検査することが望ましい。	データまたはシステムの損失からの回復を可能にするため。
8.14 情報処理施設の冗長性	情報処理施設は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい。	情報処理施設の継続的な運用を確実にするため。
8.15 ログ取得	活動、例外処理、過失及びその他の関連事象を記録したログを取得し、保存し、保護し、分析することが望ましい。	事象を記録し、証拠を生成し、ログ情報の完全性を確実にし、認可されていないアクセスを防止し、情報セキュリティインシデントにつながる可能性のある情報セキュリティ事象を特定し、調査を支援するため。
8.16 監視活動	情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい。	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。
8.17 クロックの同期	組織が使用する情報処理システムのクロックは、広く認められた時刻源と同期させることが望ましい。	セキュリティ関連の事象及びその他の記録されたデータの関係付け及び分析を可能にし、情報セキュリティインシデントの調査を支援するため。
8.18 特権的なユーティリティプログラムの使用	システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理することが望ましい。	ユーティリティプログラムの使用が、システム及びアプリケーションについての情報セキュリティ管理策に害を与えないことを確実にするため。
8.19 運用システムに関わるソフトウェアの導入	運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順及び対策を実施することが望ましい。	運用システムの完全性の維持を確実にし、技術的脆弱性の悪用を防止するため。
8.20 ネットワークのセキュリティ	システム及びアプリケーション内の情報を保護するために、ネットワーク及びネットワーク装置のセキュリティを保ち、管理し、制御することが望ましい。	ネットワーク及びそれをサポートする情報処理施設における情報を、ネットワークを通じた危険から保護するため。
8.21 ネットワークサービスのセキュリティ	ネットワークサービスについて、セキュリティ機能、サービスレベル及びサービスの要求事項を特定し、実装し、監視することが望ましい。	ネットワークサービスの使用におけるセキュリティを確実にするため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

8.技術的管理策		
標題	**管理策**	**目的**
8.22 ネットワークの分離	情報サービス、利用者及び情報システムは、組織のネットワーク上で、グループごとに分離することが望ましい。	業務の要求に基づいて、ネットワークをセキュリティ境界で分割し、それらの間のトラフィックを管理するため。
8.23 ウェブ・フィルタリング	悪意のあるコンテンツにさらされることを減らすために、外部ウェブサイトへのアクセスを管理することが望ましい。	システムがマルウェアによって危険にさらされることを防ぎ、認可されていないウェブ資源へのアクセスを防止するため。
8.24 暗号の使用	暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実装することが望ましい。	業務及び情報セキュリティの要求事項に従い、暗号に関連する法令、規制及び契約上の要求事項を考慮して、情報の機密性、真正性または完全性を保護するための暗号の適切かつ効果的な使用を確実にするため。
8.25 セキュリティに配慮した開発のライフサイクル	ソフトウェア及びシステムのセキュリティに配慮した開発のための規則を確立し、適用することが望ましい。	情報セキュリティを、ソフトウェア及びシステムのセキュリティに配慮した開発ライフサイクルにおいて設計し、実装することを確実にするため。
8.26 アプリケーションのセキュリティの要求事項	アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認することが望ましい。	アプリケーションを開発または取得する場合、すべての情報セキュリティ要求事項を特定し、対応することを確実にするため。
8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則	セキュリティに配慮したシステムを構築するための原則を確立し、文書化し、維持し、すべての情報システムの開発活動に対して適用することが望ましい。	情報システムが、開発のライフサイクルにおいてセキュリティに配慮して設計、実装及び運用されることを確実にするため。
8.28 セキュリティに配慮したコーディング	セキュリティに配慮したコーディングの原則をソフトウェア開発に適用することが望ましい。	ソフトウェアがセキュリティに配慮して書かれ、それによってソフトウェアの潜在的な情報セキュリティの脆弱性の数を減らすことを確実にするため。
8.29 開発及び受け入れにおけるセキュリティ試験	セキュリティ試験のプロセスを開発のライフサイクルにおいて定義し実施することが望ましい。	アプリケーションまたはコードを運用環境に導入するときに、情報セキュリティ要求事項が満たされているかどうかの妥当性確認をするため。
8.30 外部委託による開発	組織は、外部委託したシステム開発に関する活動を指導、監視及びレビューすることが望ましい。	組織が要求する情報セキュリティ対策が、外部委託したシステム開発で実施されることを確実にするため。
8.31 開発環境、試験環境及び運用環境の分離	開発環境、試験環境及び運用環境は、分離してセキュリティを保つことが望ましい。	開発活動及び試験活動による危険から運用環境及びそのデータを保護するため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

1. ISO/IEC 27002:2022 管理策と目的

8.技術的管理策		
標題	**管理策**	**目的**
8.32 変更管理	情報処理施設及び情報システムの変更は、変更管理手順に従うことが望ましい。	変更を実行するときに情報セキュリティを維持するため。
8.33 試験情報	試験情報は、注意深く選定し、保護し、管理することが望ましい。	試験の適切な実施、及び試験に使用する運用情報の保護を確実にするため。
8.34 監査試験中の情報システムの保護	運用システムのアセスメントを伴う監査試験及びその他の保証活動を計画し、試験者と適切な管理層の間で合意することが望ましい。	監査及びその他の保証活動が運用システム及び業務プロセスに与える影響を最小限に抑えるため。

（出典）JSA「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護－情報セキュリティ管理策」を基に作成

2. パスワードの作り方と管理方法

【複雑さを持つパスワードの作り方】

1. 単語ではなく、文章にする
　単語の場合、ディクショナリ検索でヒットする確率が上がるため、文章として考える

【例】
Cyber Security Keizoku Shien
↓
CyberSecurityKeizokuShien

2. 数字を入れる

CyberSecurityKeizokuShien0725

3. 単語の母音を削除し、読めなくする(aiueo)

CyberSecurityKeizokuShien0725
↓
CybrScrtyKzkShn0725

4. 特殊記号を数文字入れる
　#、%、@を単語の区切りに入れる

CybrScrtyKzkShn0725
↓
Cybr**#**Scrty**%**Kzk**@**Shn0725

5. サービス識別文字を入れる

【例】
　Tokyo ： t5
t5Cybr#Scrty%Kzk@Shn0725

6. 自分にしかわからない固定文字を入れる

　例　イニシャル
　　SH　→　$H
$Ht5Cybr#Scrty%Kzk@Shn0725

メモはベース部分のみ

$Ht5Cybr#Scrty%Kzk@Shn0725

【認証方式と管理】

- パスワードマネージャー（ソフトウェア）
  複雑なパスワードを生成し、管理するためのソフトウェア。
  端末間の同期を行うことで、複数のデバイスで共有できる。
- ワンタイムパスワード
  定期的に更新され、1度しか使用できないパスワード。
  パスワードは、専用のデバイスやソフトウェアで確認できる。
- PINコード方式
  パスワードとは異なり、デバイスに対する認証となるため、ネットワーク上を流れることがない。
- 公開鍵方式のパスキー
  公開鍵と秘密鍵を用いた2種類の鍵ペアで認証を行う方式

3. サイバーセキュリティフレームワーク参考資料

識別（ID）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
資産管理（ID.AM） 自組織が事業目的を達成することを可能にするデータ、人員、デバイス、システム、施設が、識別され、組織の目的と自組織のリスク戦略における相対的な重要性に応じて管理されている。		適用範囲における自組織の資産の一部のみ目録化（台帳管理）しているが、大部分は記憶や慣習において管理している。	適用範囲における自組織の資産は目録化（台帳管理）にて、管理している。	適用範囲における目録（台帳管理）を定期的に更新している。	適用範囲における目録（台帳管理）が定期的に更新されており、より良い管理に向けて、効率化や最適化の検討を行っている。
ID.AM-1:	自組織内の物理デバイスとシステムが、目録作成されている。				
ID.AM-2:	自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。				
ID.AM-3:	組織内の通信とデータフロー図が、作成されている。				
ID.AM-4:	外部情報システムが、カタログ作成されている。				
ID.AM-5:	リソース（例:ハードウェア、デバイス、データ、時間、人員、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。				
ID.AM-6:	全労働力と利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。				

3. サイバーセキュリティフレームワーク参考資料

識別（ID）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
ビジネス環境（ID.BE） 自組織のミッション、目標、利害関係者、活動が、理解され、優先順位付けが行われている。この情報は、サイバーセキュリティ上の役割、責任、リスクマネジメント上の意思決定を伝えるために使用されている。		従業員に対して、会社が目指すミッションや目標の伝達方法が曖昧となっている。そのため、役割、責任、リスクマネジメント上の意思決定も曖昧なまま活動している。	従業員に対して、会社が目指すミッションやビジン・目標が伝達され、従業員も理解した上で、役割、責任、リスクマネジメント上の意思決定が行われている。	従業員は、会社が目指すミッションやビジョン・目標に従って行動や判断を行なえるように周知などの機会を定期的に用意するよう努め、役割、責任、リスクマネジメント上の意思決定に最新の情報が使用されている。	組織は時勢に合わせたミッションやビジョン・目標を立案し、従業員が知る機会やアップデートする機会をもうけ、役割、責任、リスクマネジメント上の意思決定に最新の情報が使用されている。
ID.BE-1:	サプライチェーンにおける自組織の役割が、識別され、周知されている。				
ID.BE-2:	重要インフラとその産業分野における自組織の位置付けが、識別され、周知されている。				
ID.BE-3:	組織のミッション、目標、活動の優先順位が、定められ、周知されている。				
ID.BE-4:	重要サービスを提供する上での依存関係と重要な機能が、定められている。				
ID.BE-5:	重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。				
ガバナンス（ID.GV） 自組織に対する規制、法律、リスク、環境、運用上の要求事項を、管理し、モニタリングするためのポリシー、手順、プロセスが理解されており、経営層にサイバーセキュリティリスクについて伝えている。		組織のポリシー・手順・プロセスが策定されていない（または制定されていても認識されていない）ため、それぞれの思う方法で対応している。	組織のポリシー・手順・プロセスが策定されており、作成されたポリシー・手順・プロセスに則った方法で対応している。	組織のポリシー・手順・プロセスの見直しを定期的に行なっている。	組織のポリシー・手順・プロセスが現場の声を反映し、組織が目指す理想の姿の実現に向けた最適な方法となるように検討している。
ID.GV-1:	組織のサイバーセキュリティポリシーが、定められ、周知されている。				
ID.GV-2:	サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。				
ID.GV-3:	プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。				
ID.GV-4:	ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している				

3. サイバーセキュリティフレームワーク参考資料

識別（ID）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
リスクアセスメント（ID.RA） 自組織は、（ミッション、機能、イメージ、評判を含む）組織の業務、組織の資産、個人に対するサイバーセキュリティリスクを把握している。		適用範囲において組織の資産が網羅的に特定できていないため、守る対象や想定される脅威、脆弱性が一部のみで判断している。適用範囲に対して組織の資産は特定できているが、脆弱性や脅威の想定・把握が部分的となっており、リスクアセスメントの結果にばらつきが発生している。	適用範囲において組織の資産が網羅され、脅威・脆弱性の情報が管理されており、リスクアセスメントの結果リスクを把握している。資産の洗いだし方法や脅威・脆弱性の収集方法が文書化され管理されている。	資産の洗いだし方法や脅威・脆弱性の収集が文書化された方法で実施され、資産に対してリスクアセスメントが定期的に実行されている。	資産の洗いだし方法や脅威・脆弱性の収集をより良い方法となるように文書の見直しが行われ、情報を能動的に取得するとともに、システムの入れ替え等が発生した場合にも早期に必要な情報が収集できている。
ID.RA-1:	資産の脆弱性が、識別され、文書化されている。				
ID.RA-2:	サイバー脅威に関する情報が、複数の情報共有フォーラムおよび複数のソースから入手されている。				
ID.RA-3:	内部および外部からの脅威が、識別され、文書化されている。				
ID.RA-4:	ビジネスに対する潜在的な影響とその発生可能性が、識別されている。				
ID.RA-5:	脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。				
ID.RA-6:	リスク対応が、識別され、優先順位付けされている。				
リスクマネジメント戦略（ID.RM） 自組織の優先順位、制約、リスク許容度、想定が、定められ、運用リスクに対する意思決定を支援するために利用されている。		リスクの管理方法や許容度の指標が策定されていない（または制定されていても認識されていない）ため、それぞれの思う方法で判断・対応している。	リスクの管理方法や許容度の指標が定まっており、判断材料として活用されている。	同等事業の中でリスク管理方法を活用し、運用リスクの判断を行なっている。	組織の社会的地位の変化や、提供サービスの変化、DXを見据えた変化においても、現行のリスク管理プロセスを参考として、新事業や新システム導入などの変化に対応しリスク管理プロセスを実行している。
ID.RM-1:	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。				
ID.RM-2:	組織のリスク許容度が、決定され、明確に表現されている。				
ID.RM-3:	自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。				

3. サイバーセキュリティフレームワーク参考資料

識別（ID）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
サプライチェーンリスクマネジメント（ID.SC） 自組織の優先順位、制約、リスク許容度、想定が、定められ、サプライチェーンリスクマネジメントに関連するリスクに対する意思決定を支援するために利用されている。自組織は、サプライチェーンリスクを識別し、分析・評価し、管理するためのプロセスを定め、実装している。		自組織・利害関係者双方がセキュリティに対しての意識が低く、サプライチェーンとしてのセキュリティに対して担当者依存となっている。	自組織・利害関係者双方がセキュリティに対しての意識を持ち、必要な確認作業などに協力している。	サプライチェーンに加わることに対してセキュリティの取り組みを理解し、協力しあえる利害関係者を選定している。	サプライチェーンの安全性を高めるために日頃から協力しあい、啓発活動などを連携している。
ID.SC-1:	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。				
ID.SC-2:	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。				
ID.SC-3:	サプライヤーおよび第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。				
ID.SC-4:	サプライヤーおよび第三者であるパートナーが、監査、テストの結果、またはその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。				
ID.SC-5:	対応・復旧計画の策定とテストが、サプライヤーおよび第三者プロバイダーと共に行なわれている。				

3. サイバーセキュリティフレームワーク参考資料

防御（PR）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
アイデンティティ管理、認証／アクセス制御（PR.AC） 物理的・論理的資産および関連施設へのアクセスが、認可されたユーザ、プロセス、デバイスに限定されている。また、これらのアクセスは、認可された活動およびトランザクションに対する不正アクセスのリスクアセスメントと一致して、管理されている。		細かい制限等がなされていないため、全従業員といったような設定となっている。最新（または推奨）の技術を用いた通信や通信設備の管理が部分的なシステムで行われている。（組織のすべてのシステムで実施されていない。）	必要な資産に対して、適切な制限のもと、制限をかけるための手順や基準が体系化している。組織内の資産・システムにおいて、最新（または推奨）の技術を用いた通信や通信設備の管理が行われている。	資産に対しての制限が定期的に見直され、定める期間内において変更が実施されている。最新（または推奨）の技術の情報を把握し、更新手順やスケジュール立案が円滑に行われている。	脅威や資産価値に即したアクセス制限方法を検討し、検討の結果を基にした実施方法を実現するための計画や手順として体系化されている。
PR.AC-1:	認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。				
PR.AC-2:	資産に対する物理アクセスが、管理され、保護されている。				
PR.AC-3:	リモートアクセスが、管理されている。				
PR.AC-4:	アクセスの許可および認可が、最小権限の原則および役割の分離の原則を組み入れて、管理されている。				
PR.AC-5:	ネットワークの完全性が、保護されている（例：ネットワークの分離、ネットワークのセグメント化）。				
PR.AC-6:	IDは、ID利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。				
PR.AC-7:	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例：個人のセキュリティおよびプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例：一要素、多要素）が行われている。				

3. サイバーセキュリティフレームワーク参考資料

防御（PR）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
意識向上およびトレーニング （PR.AT） 自組織の人員およびパートナーは、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育とトレーニングが実施されている。		関連するポリシー、手順、契約などが理解されておらず、各自の判断で義務と責任を果たそうとしている。または果たしている。	教育・トレーニングが実行されており、関連するポリシー、手順、契約を理解した上で、義務と責任が果たされている。	関連するポリシー、手順、契約を理解した上で、義務と責任を果たすために、教育・トレーニングが会社の課題などに紐づき、企画から行われ実行されている。	関連するポリシー、手順、契約を理解した上で、義務と責任を果たすために、教育・トレーニングの企画・実施の方法が見直しされている。
PR.AT-1:	すべてのユーザは、情報が周知され、トレーニングが実施されている。				
PR.AT-2:	権限を持つユーザが、自身の役割と責任を理解している。				
PR.AT-3:	第三者である利害関係者（例：サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している				
PR.AT-4:	上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。				
PR.AT-5:	物理セキュリティおよびサイバーセキュリティの担当者が、自身の役割と責任を理解している。				

3. サイバーセキュリティフレームワーク参考資料

防御（PR）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
データセキュリティ（PR.DS） 情報と記録（データ）が、情報の機密性、完全性、可用性を保護するための自組織のリスク戦略に従って管理されている。		適用範囲において、資産の撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化は一部の情報と記録（データ）のみに適用している。	適用範囲において、情報と記録（データ）が目録化（台帳管理）され、資産のリスクアセスメントに基づいた撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化を実施している。	適用範囲において、情報と記録（データ）の変化があった際に、定めた期間内に目録化（台帳管理）され、資産のリスクアセスメントに基づいた撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得、暗号化を実施している。	適用範囲において、情報と記録（データ）の変化があった際に、すぐに目録化（台帳管理）が更新され資産のリスクアセスメントを行い、撤去、譲渡、廃棄のプロセス・ルール・手順、その他バックアップの取得暗号化を実施している。
PR.DS-1:	保存されているデータが、保護されている。				
PR.DS-2:	伝送中のデータが、保護されている。				
PR.DS-3:	資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。				
PR.DS-4:	可用性を確保するのに十分な容量が、維持されている。				
PR.DS-5:	データ漏えいに対する防御対策が、実装されている。				
PR.DS-6:	完全性チェックメカニズムが、ソフトウェア、ファームウェア、および情報の完全性を検証するために使用されている。				
PR.DS-7:	開発・テスト環境が、実稼働環境から分離されている。				
PR.DS-8:	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。				

3. サイバーセキュリティフレームワーク参考資料

防御（PR）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
情報を保護するためのプロセスおよび手順（PR.IP） （目的、範囲、役割、責任、経営コミットメント、組織間の調整について記した）セキュリティポリシー、プロセス、手順が、維持され、情報システムと資産の防御の管理に使用されている。		セキュリティポリシー、プロセス、手順が体系化されておらず、適用範囲内の情報システムと資産が担当者の判断により保護されいる。	適用範囲内のすべての情報システムと資産が、セキュリティポリシー、プロセス、手順が維持管理され、定められた対応手順に従って運用している。	適用範囲内のすべての情報システムと資産に更新がある場合には、セキュリティポ リシー、プロセス、手順が維持管理され、定めた期間内で見直しを行なっている。	事業変更やリスク分析などにより即時の変更が求められる場合には、セキュリティポリシー、プロセス、手順を直ちに見直し、見直されたプロセス、手順で情報システムと資産の保護を実施している。
PR.IP-1:	情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例：最低限の機能性の概念）を組み入れて、定められ、維持されている。				
PR.IP-2:	システムを管理するためのシステム開発ライフサイクルが、実装されている。				
PR.IP-3:	構成変更管理プロセスは、策定されている。				
PR.IP-4:	情報のバックアップが、実施され、維持され、テストされている。				
PR.IP-5:	組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。				
PR.IP-6:	データは、ポリシーに従って破壊されている。				
PR.IP-7:	防御プロセスは、改善されている。				
PR.IP-8:	防御技術の有効性に関する情報が、共有されている。				
PR.IP-9:	（インシデント対応および事業継続）対応計画と（インシデントからの復旧および災害復旧）復旧計画が、策定され、管理されている。				
PR.IP-10:	対応計画と復旧計画が、テストされている。				
PR.IP-11:	サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。				
PR.IP-12:	脆弱性管理計画が、作成され、実装されている。				

3. サイバーセキュリティフレームワーク参考資料

防御（PR）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
保守（PR.MA） 産業用制御システムと情報システムのコンポーネントの保守と修理が、ポリシーと手順に従って実施されている。		適用範囲において、システム関係の保守契約がなされていない。または保守契約がシステムの目的を達成するための内容・方法になっている。保守と修理がポリシーや手順に文書化されておらず、担当者の経験や勘により対応されている。	適用範囲において、システム関係の保守と修理がポリシーや手順に文書化されており、文書に基づいたシステムが果たすべき目的を達成するための内容・方法となっている。	保守と修理が求められるシステム関係が追加・更新された際には、ポリシーや手順に基づき、システムが果たすべき目的を達成するための内容・方法となっていることを確認している。	導入される各システムは定められたポリシーや手順の保守条件を満たすものであり、条件が満たされない場合には、リスクアセスメントなどを行い適切な対応を行なっている。
PR.MA-1:	組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。				
PR.MA-2:	組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。				
保護技術（PR.PT） 技術的なセキュリティソリューションが、関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンスを確保するために管理されている。		適用範囲において、ポリシーやルールが明確でないかつ、導入されている機器や資産の機能を把握できていないため、ほとんどの機能がデフォルトの設定のまま利用している。	適用範囲において、ポリシーやルールに定められた重要度や影響度に従って機器や資産の設定や保護方法を実施している。	適用範囲において、ポリシーやルールに定められた重要度や影響度をリスクアセスメントとともに見直し、リスクアセスメントの結果を踏まえた設定や保護方法へ更新している。	機器や資産保護方法を提供するサービスなどの選定をポリシーやルールに基づき行い、必要な設定や保護方法を実装するソリューションを導入している。
PR.PT-1:	監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。				
PR.PT-2:	リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。				
PR.PT-3:	最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。				
PR.PT-4:	通信（情報）ネットワークと制御ネットワークが、保護されている。				
PR.PT-5:	メカニズム（例：フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。				

3. サイバーセキュリティフレームワーク参考資料

検知（DE）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
異常とイベント（DE.AE） 異常な活動は、検知されており、イベントがもたらす潜在的な影響が、把握されている。		何をもって異常と判断するかの閾値が組織内で熟慮されておらず、担当者の経験や勘により異常・正常の判断をしている。	異常と正常の判断を行う指標（閾値など）が定まり文書化しており、それらの指標が及ぼす影響度を認識している。	異常と正常の判断を行う指標（閾値など）は異常がもたらす影響度などにより見直しを行っている。	脅威の情報やリスクアセスメントの結果などに基づき、異常の定義を見直し、検知できるようにしている。
DE.AE-1:	ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。				
DE.AE-2:	検知したイベントは、攻撃の標的と手法を理解するために分析されている。				
DE.AE-3:	イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。				
DE.AE-4:	イベントがもたらす影響が、判断されている。				
DE.AE-5:	インシデント警告の閾値が、定められている。				

3. サイバーセキュリティフレームワーク参考資料

検知（DE）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
セキュリティの継続的なモニタリング（DE.CM） 情報システムと資産は、サイバーセキュリティイベントを識別し、保護対策の有効性を検証するために、モニタリングされている。		適用範囲における、ネットワーク・物理環境・個人の活動・外部サービスプロバイダの活動などをモニタリングが一部のみで実施されている。（モニタリングされていないイベントや対象がある。）	適用範囲において、ネットワーク、物理環境、個人の活動、外部サービスプロバイダの活動がモニタリングされ、ログとして保管し不審・悪質なものが検知されている。	適用範囲において、対象のモニタリングが適切に行われているかを確認するため、チェックを行うとともに、脆弱性診断等を行い、システムの健全性を確認している。	脅威の情報やリスクアセスメントなどに基づき、モニタリング対象や内容を定期的に見直ししている。
DE.CM-1:	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。				
DE.CM-2:	物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。				
DE.CM-3:	人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。				
DE.CM-4:	悪質なコードは、検知されている。				
DE.CM-5:	不正なモバイルコードは、検知されている。				
DE.CM-6:	外部サービスプロバイダの活動は、潜在的なサイバーセキュリティイベントを検知できるようにモニタリングされている。				
DE.CM-7:	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。				
DE.CM-8:	脆弱性スキャンが、実施されている。				

3. サイバーセキュリティフレームワーク参考資料

検知（DE）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
検知プロセス（DE.DP） 検知プロセスおよび手順が、異常なイベントに確実に気付くために維持され、テストされている。		検知した情報を異常として判断するプロセス・手順・報告体制が定まっておらず、担当者の経験と勘で実施している。	検知した情報を異常として判断するプロセス・手順・報告体制が定まり、異常の判断ができている。	異常な判断に気づくプロセス・方法がテストされ、異常な状態がないことが正常であることを確認している。	異常な状態を検知する仕組みを脅威の情報やインシデントなどに基づき見直ししている。
DE.DP-1:	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。				
DE.DP-2:	検知活動は、該当するすべての要求事項を準拠している。				
DE.DP-3:	検知プロセスが、テストされている。				
DE.DP-4:	イベント検知情報が、周知されている。				
DE.DP-5:	検知プロセスが、継続的に改善されている				

3. サイバーセキュリティフレームワーク参考資料

対応（RS）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
対応計画（RS.RP） 対応プロセスおよび手順が、検知したサイバーセキュリティインシデントに対応できるように実施され、維持されている。		インシデント発生時の基本的な対応手順が組織内で定まっておらず、場当たり的な対応になっている。 インシデント発生時の基本的な対応手順が定まっているが、組織に浸透していないため、担当者によって対応方法が異なる。	インシデント発生時の基本的な対応手順が組織内で定まっており、手順は組織に浸透している。	インシデント発生時の基本的な対応手順を、従業員は発生した事象に合わせて実施することができる。	未知のインシデントに対して蓄積・手順化した組織の知見から、対応方針や対応手法を協議し対応を行なっている。
RS.RP-1:	対応計画が、インシデントの発生中または発生後に実行されている。				
コミュニケーション（RS.CO） 対応活動が、内外の利害関係者との間で調整されている（例：法執行機関からの支援）。		組織図などを作成しておらず、その場その場で必要な人や連絡先を考えて調整から行なっている。	対応活動を行うための関係者が整理されており、連絡が取り合えるように調整がされている。	定期的に有事の際を想定したコミュニケーション手法（連絡先や方法）を日頃から確認している。	組織体制の最適化や関係者を巻き込んだプロセスの改善の検討を日頃から行なっている。
RS.CO-1:	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。				
RS.CO-2:	インシデントが、定められた基準に沿って報告されている。				
RS.CO-3:	対応計画に従って、情報が共有されている。				
RS.CO-4:	利害関係者との間で調整が、対応計画に従って行なわれている。				
RS.CO-5:	サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。				

3. サイバーセキュリティフレームワーク参考資料

対応（RS）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
分析 （RS.AN） 分析は、効果的な対応を確実にし、復旧活動を支援するために実施されている。		取得しているログの期間が短い、網羅性がないため、必要な情報が必要なときに準備ができないため、経験や勘に頼った分析をしている。	取得するログの範囲や上記の取得期間等のルールが文書化されており、ログが正しく取得できていることを確認している。	必要なログを定める期間に従い確認しており、ログの精査を行うことで、自社のリスク分析に活用している。	円滑なインシデント対応ができるために、対応・復旧などの手順に紐づいた見直し・改善を行なっている。
RS.AN-1:	検知システムからの通知は、調査されている。				
RS.AN-2:	インシデントがもたらす影響は、把握されている。				
RS.AN-3:	フォレンジックが、実施されている。				
RS.AN-4:	インシデントは、対応計画に従って分類されている。				
RS.AN-5:	プロセスは、内外のソース（例：内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。				
低減（RS.MI） 活動は、イベントの拡大を防ぎ、その影響を緩和し、インシデントを解決するために実施されている。		適用範囲において、インシデントによる影響を正しく把握・認識しておらず、原因究明の為の対応に集中している。インシデントの対応が場当たり的になっており、担当者の経験や知識のみで判断を行なっている。	インシデントによる影響を最小限に抑えるために担当者が意識を持って対応している。（原因究明や攻撃手法解析などに集中したインシデント対応となっていない。）	インシデント発生時に注意する点などが文書化されており、インシデント発生時にスムーズにインシデント対応に入り、対応を開始している。	リスクアセスメントの結果や脅威の状況、被害実態などの情報を収集し、インシデントを封じ込め、緩和するために必要な行動や注意点を更新している。
RS.MI-1:	インシデントは、封じ込められている。				
RS.MI-2:	インシデントは、緩和されている。				
RS.MI-3:	新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。				
改善（RS.IM） 組織の対応活動は、現在と過去の検知/対応活動から学んだ教訓を取り入れることで改善されている。		対応の為の活動の履歴や記録を文書化しておらず、担当者の記憶に頼っている	手順が文書化されており、活動の振り返りを行なっている。	振り返りを元に、改善を行い、手順等を更新している。	模擬訓練や検知で得た情報などをもとに振り返りを行い、改善し手順等を更新している。
RS.IM-1:	対応計画は、学んだ教訓を取り入れられている。				
RS.IM-2:	対応戦略は、更新されている。				

3. サイバーセキュリティフレームワーク参考資料

復旧（RC）		ティア1 部分的である (Partial) 場当たり的、属人的である	ティア2 リスク情報を活用している (Risk Information) 初期プロセスが整備されている	ティア3 繰り返し適用可能である (Responsible) プロセスが継続的に回っている	ティア4 適応している (Adaptive) プロセス自身の継続的改善に努めている
復旧計画（RC.RP） 復旧プロセスおよび手順は、サイバーセキュリティインシデントによる影響を受けたシステムや資産を復旧できるよう実行され、維持されている。		インシデント発生時の基本的な復旧手順が文書化されておらず、担当者の経験と知識で対応している。	インシデント発生時の基本的な復旧手順が定まっており、文書化している。	従業員はインシデント発生時の基本的な復旧手順を理解しており、発生した事象に合わせて復旧手順を実施している。	想定外の事象に対して蓄積・手順化した組織の知見から、対応方針や対応手法を協議し対応を行なっている。
RC.RP-1:	復旧計画が、サイバーセキュリティインシデントの発生中または発生後に実施されている。				
改善（RC.IM） 復旧計画およびプロセスが、学んだ教訓を将来の活動に取り入れることで改善されている。		復旧の為の活動の履歴や記録を文書化しておらず、担当者の記憶に頼っている	手順が文書化されており、活動の振り返りを行なっている。	振り返りを元に、改善を行い、手順等を更新している	模擬訓練などを定期的に行う中で振り返りを行い、改善し手順等を更新している。
RC.IM-1:	復旧計画は、学んだ教訓を取り入れている。				
RC.IM-2:	復旧戦略は、更新されている。				
コミュニケーション（RC.CO） 復旧活動は、内外の関係者（例：コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、他組織のCSIRT、ベンダ）との間で調整されている。		組織図などを作成しておらず、その場その場で必要な人や連絡先を考えて調整から行なっている。	復旧活動を行うための関係者が整理されており、連絡が取り合えるように調整がされている。	定期的に有事の際を想定したコミュニケーション手法（連絡先や方法）を確認している。	組織体制の最適化や関係者を巻き込んだプロセスの改善の検討を日頃から行なっている。
RC.CO-1:	広報活動が、管理されている。				
RC.CO-2:	評判は、インシデント発生後に回復されている。				
RC.CO-3:	復旧活動は、内外の利害関係者だけでなく役員と経営陣にも周知されている。				

4. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）参考資料

想定読者および全体構成

CPSFの想定読者は、Society5.0という新たな社会において、セキュリティ担当者やサプライチェーンに関わる担当者になります。CPSFは、必要な見直しを迅速かつ柔軟に行うことを視野に入れた構成とするため、全体を以下のような三部構成とし、A~Eまでの5つの添付資料で成り立っています。添付資料A、Bは第Ⅱ部、添付資料Cは第Ⅲ部、添付資料D、Eは全体に対する参考資料という位置付けとなります。

＜添付資料＞
添付 A ユースケース
添付 B リスク源と対策要件の対応関係
添付 C 対策要件に応じたセキュリティ対策例
添付 D 海外の主要規格との対応関係
添付 E 用語集

第Ⅰ部[コンセプト]
サイバーセキュリティの観点からリスク源を整理するためのモデル（3層構造と6つの構成要素）を提示
※テキストの「7-4-1. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）の概要」で説明しています。

第Ⅱ部[ポリシー]
第Ⅰ部で示したモデルを活用したリスク源を整理するとともに、リスク源に対応する対策要件を提示

第Ⅲ部[メソッド]
第Ⅱ部で示した対策要件を対策の種類に応じて整理

想定読者	第Ⅰ部 [コンセプト]	第Ⅱ部 [ポリシー]	第Ⅲ部 [メソッド]
CISO（最高情報セキュリティ責任者）	○	○	
サプライチェーンマネジメントに関わる戦略・企画部門の担当者	○	○	
バリュークリエイションプロセスに関わる企業・団体などのセキュリティ担当者		○	○
情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者		○	○
データマネジメントの担当者		○	○
各産業分野におけるセキュリティ対策のガイドラインなどを策定する業界団体の担当者	○	○	○

（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の概要」を基に作成

CPSFを活用することで期待される効果

・セキュリティ対策の実行によるバリュークリエイションプロセスの信頼性確保
・製品・サービスのセキュリティ品質を差別化要因（価値）にまで高めることによる競争力の強化

4. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）参考資料

第Ⅰ部[コンセプト]

コンセプトの詳細につきましては、テキストの「7-4-1. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）の概要」で説明しています。第Ⅰ部[コンセプト]については、テキストの補足として、6つの構成要素について説明します。

6つの構成要素

CPSFでは、バリュークリエイションプロセスが動的に柔軟に構成されることから、資産を固定的に捉えることが難しく、構成要素について一定の抽象化を行って捉えることが必要となります。セキュリティ対策を講じる上で最適な最小単位として、6つの構成要素が定義されています。

構成要素	定義
ソシキ	バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	ソシキに属する人、およびバリュークリエイションプロセスに直接参加する人
モノ	ハードウェア、ソフトウェアおよびそれらの部品（操作する機器を含む）
データ	フィジカル空間にて収集された情報、および共有・分析・シミュレーションを通じて加工された情報
プロシージャ	定義された目的を達成するための一連の活動の手続き
システム	目的を実現するためにモノで構成される仕組み・インフラ

（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」を基に作成

第Ⅱ部[ポリシー]

3層構造モデルと6つの構成要素を活用したリスクマネジメント

リスクマネジメントにおける標準的なプロセス（例：JIS Q 31000:2010、 JIS Q 27001:2014）も踏まえ、CPSFに基づくセキュリティリスクマネジメントの流れを整理します。 3層構造モデル、6つの構成要素の考え方を活用し、バリュークリエイションプロセスの特徴を捉えたセキュリティリスクマネジメントが可能になります。

1. 分析対象の明確化
2. 想定されるセキュリティインシデントおよび事業被害レベルの設定
3. リスク分析の実施
4. リスク対応の実施

CPSFの考え方を踏まえたリスクマネジメントで考慮すべき観点

- バリュークリエイションプロセスに関わるステークホルダーとの関係
- IoT機器を介したサイバー空間とフィジカル空間の融合
- 組織を跨るデータの流通
- 各層における信頼性の基点の確保

1. 分析対象の明確化（3層構造モデルへの落とし込み）

各層の特性および機能・役割を理解した上で分析範囲および資産を整理します。
分析対象のシステムによっては第2層の機能と第3層の機能を併せ持つ内容もあります。

階層	特性	機能・役割	分析対象	分析対象の具体的イメージ
第1層	各組織の適切なガバナンスマネジメント	各組織のセキュリティマネジメント [信頼性の基点] 組織・マネジメント	• 組織で管理されるモノ・システム • 組織内で流通するデータ など	• 社員、従業員 • 企業のIT資産 • 企業のセキュリティポリシー など
第2層	IoT機器を介して、フィジカル空間とサイバー空間のつながり拡大	フィジカル空間とサイバー空間との間のデータのやり取り [信頼性の基点]ルールに沿って正しくフィジカル空間とサイバー空間を転写する機能	• データを転写するモノ・システム • 転写されるデータ など	• センサ • アクチュエータ • 3Dプリンタ • 監視カメラ など
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	データの送受信、加工・分析、保管 [信頼性の基点]データ	• データを送受信／加工・分析／保管するモノ・システム • 組織を超えて流通するデータ など	• サーバ • ルータ • スマートメータ • オープンデータ など

（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の概要」を基に作成

2. 想定されるセキュリティインシデントおよび事業被害レベルの設定

各層の機能に対する悪影響のイメージ

3層構造モデルにおける各層の特性などを踏まえ、各層の機能（守るべきもの）とそれに対する悪影響のイメージを整理します。

階層	各層の機能（守るべきもの）	機能（守るべきもの）に対する悪影響のイメージ
第1層	• 各組織のセキュリティマネジメント	• 法制度への不準拠 • セキュリティインシデントの発生（営業秘密の漏えい） • セキュリティインシデントによる影響の拡大（被害拡大による事業影響）
第2層	• フィジカル空間とサイバー空間との間のデータのやりとり	• 機器の機能停止（IoT機器の稼動停止） • 信頼性の低い稼動（IoT機器の意図しない稼動）
第3層	• データの送受信、加工・分析、保管	• データ保護に係る法制度などへの不準拠 • セキュアでない稼動（データ処理側での情報資産の棄損） • 信頼性の低い稼動（データ関連サービスの意図しない稼動）

（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の概要」を基に作成

想定されるセキュリティインシデントの設定

各層の機能および機能に対する悪影響の観点を踏まえ、3層構造の各層で発生を回避すべき一般的なセキュリティインシデントを整理します。

階層	想定されるセキュリティインシデントの例
第1層	• 平時のリスクマネジメントプロセスに支障があり、セキュリティインシデント（情報資産の漏えい／改ざん／破壊／利用停止）が発生する • セキュリティに係る法制度などの規定内容を遵守できない • セキュリティインシデントによる被害が拡大し、適切に事業継続できない　など
第2層	• 内部に不正アクセスされたIoT機器が意図しない動作 • IoT機器の動作による安全面に問題のある事象の発生 • 改ざんされたIoT機器による正確でないデータの送信などが発生 など
第3層	• サイバー空間にて取り扱われる保護すべきデータの漏えい • サイバー空間にて取り扱われる保護すべきデータの改ざん • なりすましされた機器などから不適切なデータを受領 • サイバー空間上のデータの取扱いに係る法規制や一部の関係者のみで共有するデータについて求められるセキュリティ水準を満たさない など

（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の概要」を基に作成

3. リスク分析・リスク対応の実施（添付Bの活用）

想定されるセキュリティインシデントおよび事業被害レベルの設定にて実施した内容を踏まえ、添付Bでは、抽出したセキュリティインシデントに対して、当該インシデントの発生を助長、あるいは発生したインシデントの被害を拡大させる可能性がある脅威および典型的な脆弱性を整理します。脆弱性を6つの構成要素で捉えることで、バリュークリエイションプロセスにおけるリスク源の洗い出しが可能となります。また、リスク分析を実施する際に、検討するリスク源の抽出および過不足のチェックなどに活用できます。添付Bでは、対応するセキュリティ対策要件が整理されており、リスク対応として回避、低減、移転、保有のうち、低減を実施する場合は、これらを参照することで対策要件の選択が可能になります。

機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件ID
		脅威	脆弱性ID	脆弱性		
下記すべてに関わる • データを加工・分析する機能 • データを保管する機能 • データを送受信する機能	サービス拒否攻撃により、関係する他組織における自組織のデータを取扱うシステムが停止する	システムを構成するサーバなどの電算機器、通信機器などに対するDDoS攻撃	L3_3_b_ORG	[ソシキ] データの収集先、加工・分析などの依頼先の組織の信頼を契約前、契約後に確認していない	サービスやシステムの運用において、サービスマネジメントを効率的、効果的に運営管理するサービスサプライヤーを選定する	CPS.SC-2

脆弱性は、6つの構成要素別に記載。

対策要件IDで添付Cの詳細な対策例を参照可能。

（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の概要」を基に作成

機能	各層の機能に対する悪影響のイメージの表で整理した3層構造モデルにおける各層の機能
想定されるセキュリティインシデント	想定されるセキュリティインシデントの設定の表で整理した「機能」に記載した各層の機能を侵害する可能性のあるセキュリティインシデント
リスク源	それ自体または他との組み合わせにより、リスクを生じさせる力を潜在的にもっている要素
脅威	システムまたは組織に損害を与える可能性がある望ましくないインシデントの潜在的な原因
脆弱性ID	添付Bの固有の識別子（ID）
脆弱性	脅威によって付け込まれる可能性のある、資産または管理策の弱点
対策要件	対応策となる見込みの高い要件
対策要件ID	添付Bの固有の識別子（ID）

第Ⅲ部[メソッド]

4. 対策要件および対策例集を活用したリスク対応

添付Cでは、添付Bで示した対策要件に対して、CSFを参考にカテゴリ分けを行い整理します。各対策要件に対して、具体的な対策例を記載します。

リスクアセスメントの結果に応じて、第Ⅲ部に記載された対策要件および、添付Cに記載されたセキュリティ対策例を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントが改善されます。

<添付C>

添付Bの脆弱性に対応。

他の国際規格などとの対応関係。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	NIST SP800-171	NIST SP800-53	ISO/IEC 27001 付属書A
CPS.AM-1	…	L1_1_a_COM L1_1_b_COM L1_1_c_COM L2_1_a_ORG L2_3_b_ORG	<H-Advanced>	O/S	○	○	―
			<Advanced>	O/S	○	○	○
			<Basic>	O			

・添付Bの対策要件をNIST CSFを参考に整列。
・対策要件IDで添付Bの記載へ参照が可能

対策例を実施する主体を記載。
S: システムに実装される対策
O:組織に実装される対策

対策例を3つのレベルに分けて記載。
High Advanced、Advanced、Basic

（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の概要」を基に作成

CPSFにおける他の国際規格などとの対応関係

第Ⅲ部、添付Cおよび添付Dにおいて、主要な国際規格などとの対応関係を記載します。またCFS、NIST SP800-171、ISO/IEC 27001付属書Aについては、各規格などから見た場合の対応関係を整理します。

<添付C> CPSF → 他の国際規格など

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	NIST SP800-171	NIST SP800-53	ISO/IEC 27001付属書A
CPS.AM-1	…	L1_1_a_COM, L1_1_b_COM, …	<H-Advanced>	O/S	○	○	―
			<Advanced>	O/S	○	○	○

<添付D> 他の国際規格など → CPSF

NIST Cybersecurity Framework v1.1のサブカテゴリ → CPSF

NIST Cybersecurity Framework v1.1			サイバー・フィジカル・セキュリティ対策フレームワーク	
機能	サブカテゴリID	サブカテゴリ	対策要件ID	対策要件
特定（ID）	AM-1	…	CPS.AM-1	…

NIST SP 800-171の要求事項 → CPSF

NIST SP 800-171			NIST SP800-171 から参照される NIST SP800-53	サイバー・フィジカル・セキュリティ対策フレームワーク		
ファミリ	管理策ID	要求事項	管理策名称	対策要件ID	対策要件	対策例
アクセス制御	3.1.1	…	・AC-2 アカウント管理 …	CPS.AC-9	…	…

ISO/IEC 27001の管理策群 → CPSF

ISO/IEC 27001:2013 付属書A		サイバー・フィジカル・セキュリティ対策フレームワーク		
管理策ID	要求事項	対策要件ID	対策要件	対策例
3.1.1	…	CPS.BE-2	…	…

（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の概要」を基に作成

4. CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク）参考資料

対策要件のカテゴリとNIST Cybersecurity Framework との対応関係

カテゴリ名称	略称	NIST Cybersecurity Framework Ver1.1 の対応カテゴリ
資産管理	CPS.AM	ID.AM（Asset Management）
ビジネス環境	CPS.BE	ID.BE（Business Environment）
ガバナンス	CPS.GV	ID.GV（Governance）
リスク評価	CPS.RA	ID.RA（Risk Assessment）
リスク管理戦略	CPS.RM	ID.RM（Risk Management Strategy）
サプライチェーンリスク管理	CPS.SC	ID.SC（Supply Cain Risk Management）
アイデンティティ管理、認証および アクセス制御	CPS.AC	PR.AC（Identity Management and Access Control）
意識向上およびトレーニング	CPS.AT	PR.AT（Awareness and Training）
データセキュリティ	CPS.DS	PR.DS（Data Security）
情報を保護するためのプロセスおよび 手順	CPS.IP	PR.IP（Information Protection Processes and Procedures）
保守	CPS.MA	PR.MA（Maintenance）
保護技術	CPS.PT	PR.PT（Protective Technology）
異変とイベント	CPS.AE	DE.AE（Anomalies and Events）
セキュリティの継続的なモニタリング	CPS.CM	DE.CM（Security Continuous Monitoring）
検知プロセス	CPS.DP	DE.DP（Detection Processes）
対応計画	CPS.RP	RS.RP（Response Planning） RC.RP（Recovery Planning）
伝達	CPS.CO	RS.CO（Communications） RC.CO（Communications）
分析	CPS.AN	RS.AN（Analysis）
低減	CPS.MI	RS.MI（Mitigation）
改善	CPS.IM	RS.IM（Improvements） RC.IM（Improvements）

（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」を基に作成

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