令和5年度
中小企業サイバーセキュリティ対策
継続支援事業

サイバーセキュリティ対策におけるフレームワークの体系

サイバーセキュリティ
人材育成
社内体制整備支援

目次

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の取組みを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全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**

組織が業務上取り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り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

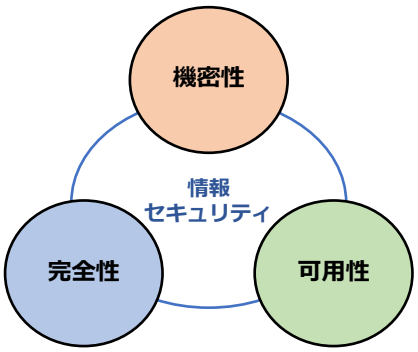


図34. 情報セキュリティの3要素
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

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、多くの情報を取り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に規定される全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みです。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。

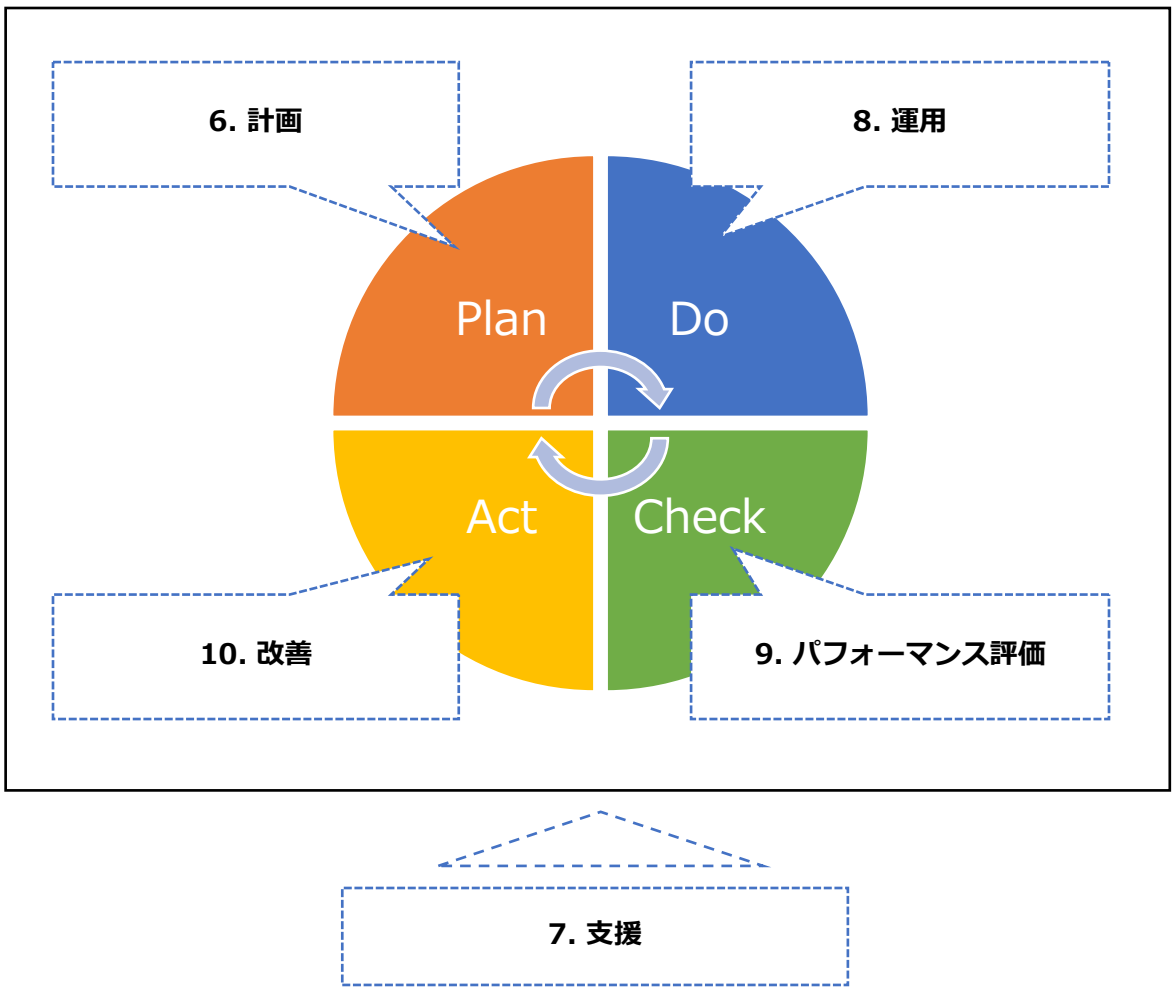


図35. ISO/IEC 27001のPDCAサイクル

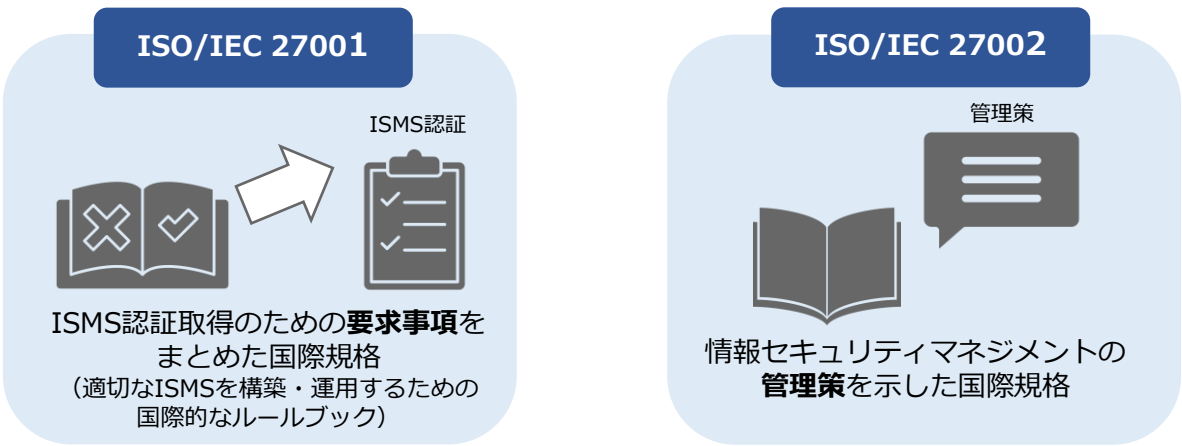
7-2-2. ISMSの要素と要件

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全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、一律に全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。例えば、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。例えば、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「（別紙）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、規制および標準の順守
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 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、教育および訓練
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 雇用の終了又は変更後の責任
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 秘密保持契約又は守秘義務契約
5.21 ICTサプライチェーンにおける情報セキュリティの取扱い	6.7 リモートワーク
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	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、部屋およ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 物理的およ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

（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。例えば、「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。

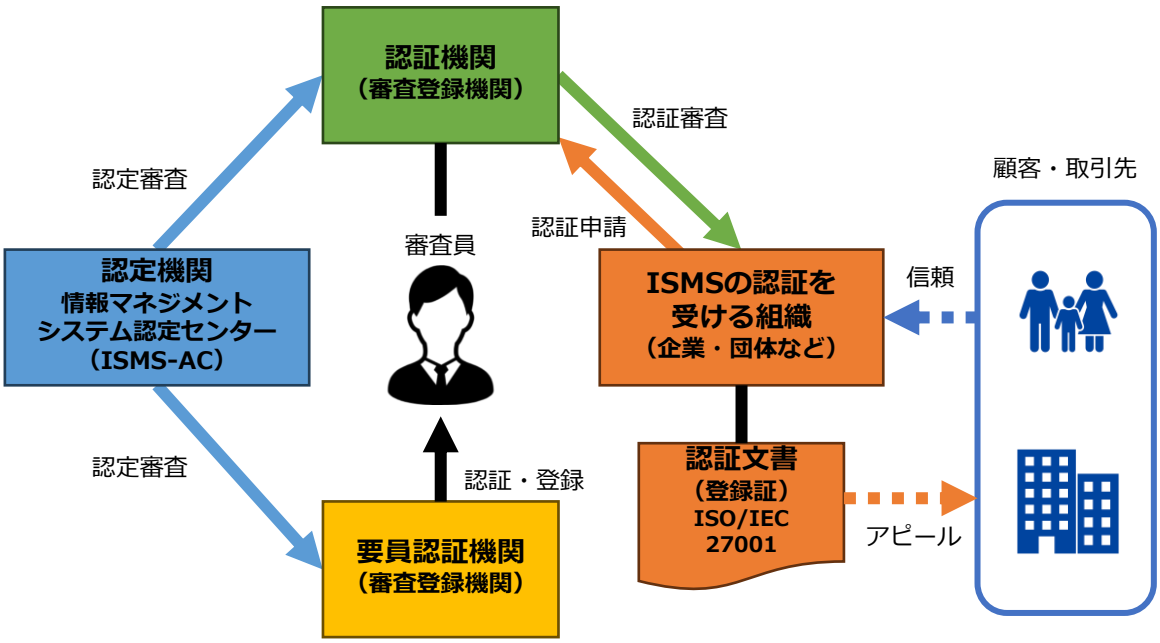


図36. ISMS適合性評価制度
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

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

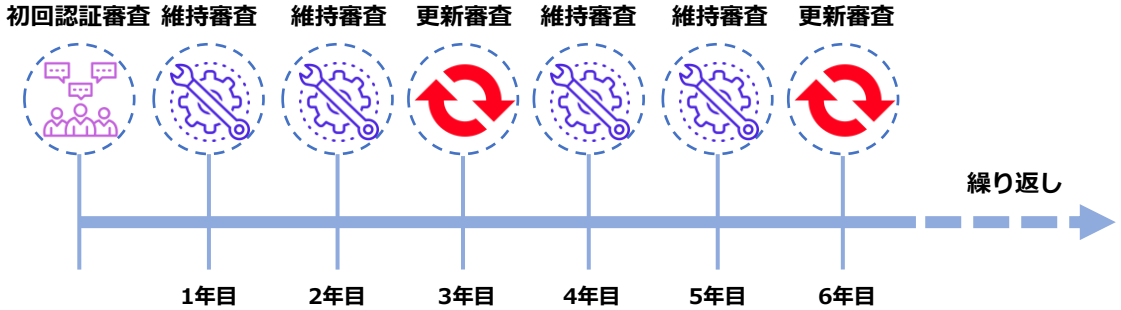
ISMSの認証審査は、大まかに以下のようなステップで進みます。

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、必ずしも全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。

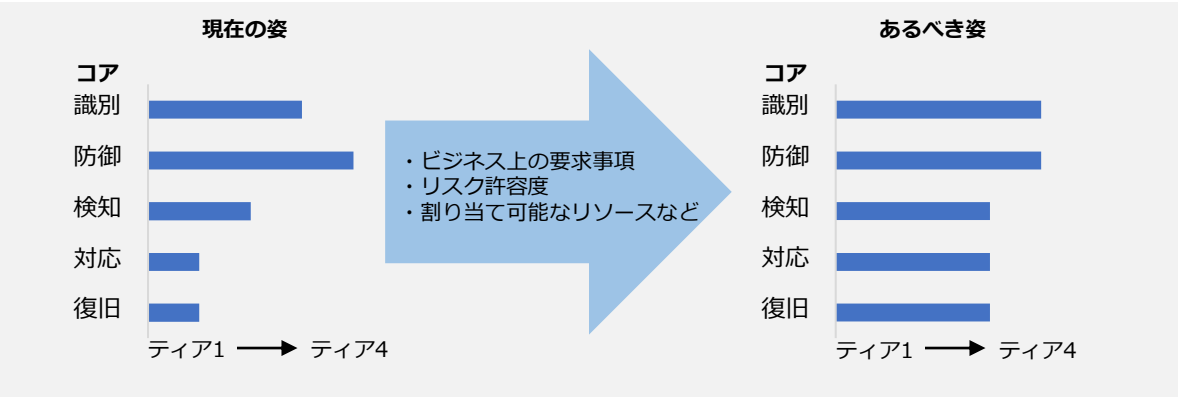


図37.プロファイルの活用イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

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。

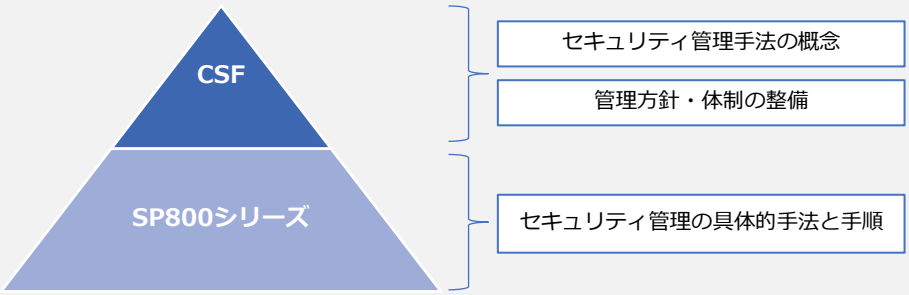


図38. CSFとSP800シリーズの関係

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。

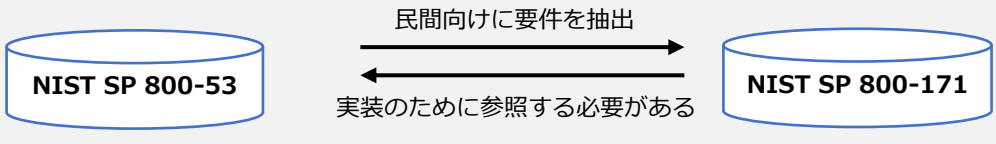


図39. NIST SP 800-53とNIST SP 800-171の関係

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、提示している全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全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

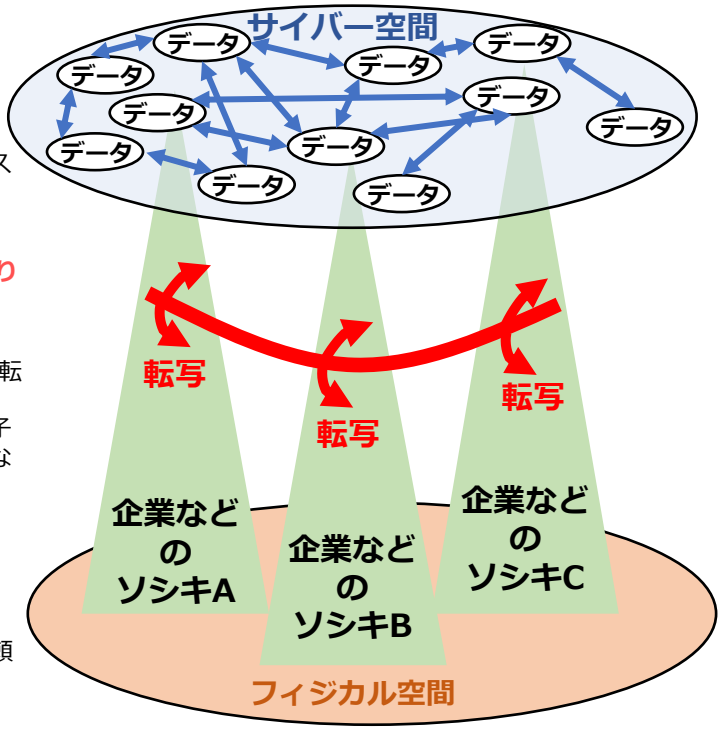


図40.3層構造モデルと各層における信頼性
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

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、この取組み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等）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、サービス等、事業が立脚している全ての基盤（設備、システム、情報等の資産、流通プロセス等）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、人材等）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、人材等）を確保した上で、具体的な対策に取り組ませる。
- ✓ 全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全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等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、管理部門等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、テレワーク等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、システム又はサービス（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等を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等）を整備させる。
- ✓ 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明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、全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等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- ✓ 制御系も含めたBCPとの連携等、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。
- ✓ 業務停止等からの復旧対応について、対象をIT系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

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等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等に反映させる。
- 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等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等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等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

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等がSECURITY ACTIONを実施していることを確認する。なお、ISMS等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等の機会において、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等の情報開示に積極的に取り組む。
- 中小企業の場合は、商工会議所、商工会等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

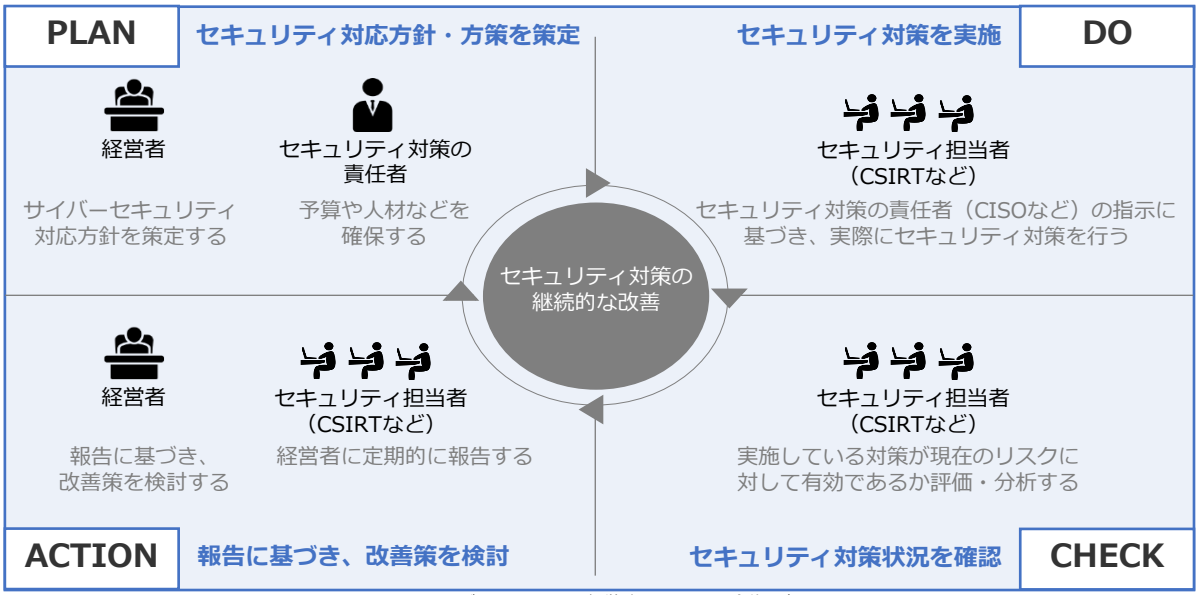


図41. サイバーセキュリティ経営ガイドラインの全体の流れ
（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

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。

編集後記

セミナー4日目では、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ました。セキュリティ対策は、やみくもに進めることで、複雑になり、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必要があることを、今回のセミナーを通じて理解していただければと思います。

本テキストでは、最初にセキュリティフレームワークの全体像について説明を行い、網羅的なセキュリティフレームワークであるISMSを取り上げました。その後に、各フレームワーク（CSF、NIST SP 800、CPSF、サイバーセキュリティ経営ガイドライン）の概要について説明を行いました。ISMSの管理策であるISO/IEC 27002の「サイバーセキュリティ概念（識別、防御、検知、対応、復旧）」がCSFの「コア」と共通していることを説明し、ISMSが他のフレームワークについても共通した概念を持ったフレームワークであることについても触れました。セキュリティ対策を推進する上では、網羅性を持ったISMSのフレームワークをベースとしつつ、自社に合った管理策などを他のフレームワークから選定して対策に取組むことが重要となります。次回は、フレームワークに基づいて、サイバーセキュリティ対策の詳細について解説していきます。

（別紙）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、全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、全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又は会議、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 情報およ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

（別紙）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 情報およ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、契約又は合意の変更又は終了時に、自らが所持する組織の資産の全てを返却することが望ましい。	雇用、契約、又は合意を変更又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、手順又は合意を、組織内及び組織と他の関係者との間の全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

（別紙）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	供給者の製品又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取扱い	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およびレビューおよび変更管理	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および準備	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および決定	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又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

（別紙）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、規制およ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又は社会の期待の順守を確実にするため。
5.34 プライバシーおよび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、又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

（別紙）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	要員になる全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。	全ての要員が、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、教育および訓練	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 雇用の終了又は変更後の責任	雇用の終了又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。	雇用又は契約を変更又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 秘密保持契約又は守秘義務契約	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又は守秘義務契約は、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。	要員又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、処理又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

（別紙）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、部屋およ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又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又は低減するため。
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 構外にある装置および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、盗難又は侵害、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

（別紙）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、移動又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、又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又は情報サービスをサポートするケーブルの配線は、傍受、妨害又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、盗難又は侵害、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、盗難又は侵害、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、全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。	処分又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、又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

（別紙）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、意図しない又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、利用者又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又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、装置又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、保存又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。	個人又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

（別紙）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。	データ又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

（別紙）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、真正性又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又は取得する場合、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又は取得する場合、全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およ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、全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 開発およ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。	アプリケーション又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、試験環境および運用環境の分離	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

（別紙）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

引用文献

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

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

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

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

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

■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

■DDoS攻撃（ディードスこうげき）
Distributed Denial of Service Attackの略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることで、過剰な負荷をかけてサービスを利用できなくする攻撃手法
…… 2-2-2、2-2-5、第一回コラム

■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、3-4-1

■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で様々な政府・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

■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、7-2-2、7-3-2

用語集

■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

■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、3-4-2

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

■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み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる
…… 3-4-1、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-4、7-4-1

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

■LockBit2.0
「Your files are encrypted by LockBit」というメッセージを表示させ、身代金を要求するマルウェア（ランサムウェア）。感染するとファイルが暗号化され、拡張子が「.LockBit」に変更される
…… 2-3-2

■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

■NIST サイバーセキュリティフレームワーク（CSF）
米国政府機関の重要インフラの運用者を対象として誕生し、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本においても、今後普及が見込まれる
…… 3-4-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4

■OSS
Open Source Softwareの略。利用者の目的を問わず、誰でもソースコードの使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称。
…… 6-1-1

■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年に提唱したゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…… 2-2-4

用語集

■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

■SDP
Software-Defined Perimeterの略。ゼロトラストを実現するための仕組みで、全ての通信をチェックおよび認証する。VPNは、ネットワーク接続前に一度だけ認証を行うのに対し、SDPは、ユーザの情報（デバイス、場所、OSなど）など複数の要素からネットワーク接続前、接続中、接続後で検証と認証を行う
…… 2-2-5

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

■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、7-1-1、7-4-1

■SWG
Secure Web Gatewayの略。社内と社外のネットワーク境界で通信を中継する役割を持っている。また、やり取りしているデータを分析し、悪意のあるデータを遮断することでセキュアな通信環境を実現
…… 2-2-4

■UTM
複数のセキュリティ対策機能を1つに集約した製品のこと。ウイルスや不正アクセスなど外部からの脅威から、内部のネットワークを包括的に保護することができる
…… 3-1-1

■VPN
Virtual Private Networkの略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することで、盗聴やデータの改ざんを防ぐ。このようにVPNを使用することで、ユーザは物理的な専用線で通信しているかのような安全な通信を行うことができる
…… 2-1-3、2-2-2、2-2-5、2-3-1、2-3-2、2-3-3

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

■アクセス制御
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、第一回コラム、7-2-2、7-3-2

■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

■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、3-2-3、3-4-1、第一回コラム

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

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

用語集

■ウイルス定義ファイル（パターンファイル）
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…… 3-3-2、3-3-3

■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

■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

■改ざん
文書や記録などの全てまたは一部に対して、無断で修正・変更を加えること。IT分野においては、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為
…… 2-1-2、5-2-2、6-1-3

■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
…… 第一回コラム、7-1-2、7-2-1、7-2-2

■完全性
参照する情報が改ざんされていなく、正確である特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2

■機密性
許可された者だけが情報や情報資産にアクセスできる特性
…… 第一回コラム、7-1-2、7-2-1、7-2-2

■クラッキング
悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為を行うこと
…… 第一回コラム

■個人情報保護委員会
個人情報の有用性を考慮しながらも、個人の権利や利益を保護するために、個人情報の適切な取扱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

■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、3-3-1、4-3-1、4-3-2、5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-2、7-3-1、7-4-1、7-5-2、7-5-3

■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

■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

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

■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

■情報セキュリティの3要素「CIA」
情報セキュリティの3つの要素、機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の頭文字をとって「CIA」と呼ぶ
…… 第一回コラム

■真正性
情報セキュリティマネジメントの付加的な要素で、利用者、プロセス、システム、情報などが、主張どおりであることを確実にする特性のこと。真正性を低下させる例としては、なりすまし行為などがある
…… 2-1-3、第一回コラム、6-1-3、7-2-1

■信頼性
システムが実行する処理に欠陥や不具合がなく、想定した通りの処理が実行される特性
…… 第一回コラム、6-1-1、6-1-3、7-2-1

■スクリーンロック
デバイスの誤動作や勝手に操作されることを防ぐための機能。スクリーンロック画面になっているときはパスワードやロックパターンの入力、指紋や顔の認証をしなければ解除することができない
…… 2-2-2

■脆弱性
情報システム（ハードウェア、ソフトウェア、ネットワークなどを含む）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、3-4-1、第一回コラム、6-1-3、7-2-2

■脆弱性診断
システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること
…… 2-3-1

■責任追跡性
情報資産に対する参照や変更などの操作を、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
…… 第一回コラム、7-2-1

■セキュリティインシデント
セキュリティの事故・出来事のこと。単に「インシデント」とも呼ばれる。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象などがインシデントに該当
…… 2-1-1、2-1-2、2-1-3、2-2-1、4-3-2、7-2-2、7-3-2

■セキュリティ・キャンプ
情報セキュリティに関する高度な技術と倫理に関する講習・演習を行う合宿。審査に通過した22歳以下の学生・生徒が対象。次代を担う情報セキュリティ人材を発掘・育成するために、情報処理推進機構（IPA）と（一財）セキュリティ・キャンプ協議会が実施している
…… 2-1-2

■セキュリティホール
情報システムにおけるセキュリティ上の欠陥のこと。「脆弱性」とほぼ同義であるが、セキュリティホールは、ソフトウェアの設計上のミスやプログラムの不具合によって発生するセキュリティ上の脆弱性のみを指す場合がある
…… 3-4-1

用語集

■セキュリティポリシー
企業や組織において実施する情報セキュリティ対策の方針や行動指針のこと。社内規定といった組織全体のルールから、どのような情報資産をどのような脅威からどのように守るのかといった基本的な考え方、情報セキュリティを確保するための体制、運用規定、基本方針、対策基準などを具体的に記載するのが一般的
…… 2-1-1、2-2-1、3-4-1、6-1-2、7-5-1

■ゼロデイ攻撃
OSやソフトウェアに存在する脆弱性が公開された後、修正プログラムや回避策がベンダーから提供されるまでの間に、その脆弱性を悪用して行われるサイバー攻撃のこと
…… 2-1-3

■ゼロトラスト
従来の「社内を信用できる領域、社外を信用できない領域」という考え方とは異なり、社内外を問わず、全てのネットワーク通信を信用できない領域として扱い、全ての通信を検知し認証するという新しいセキュリティの考え方
…… 2-2-4、4-1-3

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

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

■多要素認証
多要素認証は、サービス利用時において利用者の認証を行うために、3つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも2つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマ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

■データサイエンス
数学、統計、人工知能などの技術を用いて、大量のデータを解析し、ビジネスに有益な知見を抽出すること
…… 1-1-1

■デジタル化
紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（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、3-3-1、4-1-2、4-2-3、5-1-1、6-1-1、6-1-3、7-4-1

■デジタル情報
0、1、2のような離散的に（数値として）変化する量
…… 第一回コラム

■内部監査
内部の独立した監査組織が業務やシステムの評価、監査、アドバイスを行う活動である。情報セキュリティマネジメントシステム（ISMS）に関する国際規格であるISO27001の監査では、ポリシーや規定、手順に適合し、各情報資産が確実に守られているか確認する
…… 3-4-1、7-2-1、7-3-2

■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

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

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

■標的型メール攻撃
特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある
…… 2-2-4

■ファイアウォール
本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを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、3-4-1、3-4-2

■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、4-3-2、5-2-1

■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

■フォレンジック
犯罪捜査における分析や鑑識を意味する言葉。サイバーセキュリティの分野で使われる「フォレンジック」とは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取組みを指す。「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…… 2-2-3、2-3-2

■ブラックマーケット
広義には、不法な取引が行われる市場を指す。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、7-1-1、7-1-2、7-2-1、7-3-1、7-4-1

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

用語集

■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

■マルウェア
パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる
…… 2-2-2、2-2-4、2-2-5、第一回コラム、7-2-2

■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することができる
…… 3-3-3

■ランサムウェア
悪意のあるマルウェアの一種。パソコンなどのファイルを暗号化し利用不可能な状態とし、解除と引き換えに被害者から身代金（ransom）を要求する
…… 2-1-2、2-1-3、2-2-1、2-2-2、2-2-5、2-3-2、2-3-3、7-5-1

■リスクアセスメント
企業や組織が持つ情報資産に対するリスクの分析・評価を行うプロセスのこと。具体的には情報資産の特定、脅威と脆弱性の特定と評価、リスクの分析と評価を行う。リスク評価の結果、許容できるもの以外については何らかの対策を講じる必要がある
…… 3-4-1、7-3-2、第4回コラム

■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

■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

令和5年度
中小企業サイバーセキュリティ対策
継続支援事業