中小企業向け

サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策で DX を加速

東京都産業労働局

第28章. サイバーレジリエンスの必要性

章の目的
第 28 章では、サイバーレジリエンス確保に不可欠な情報システム継続計画（IT-BCP）を独立した柱として位置づけ、その中にインシデント対応体制・復旧プロセス・教訓の反映および訓練を一体的に組み込み、中小企業でも現実的に運用可能な仕組みとして定着させることを目的とします。

主な達成目標
◘ IT-BCP と IRP を統合したインシデント対応体制の基本構造を理解すること ◘ RTO・RPO 設定や復旧優先順位に基づく復旧・回復プロセスを設計できること ◘ ランサムウェア対策を含む技術的対策と証拠保全・記録の実務要点を把握できること ◘ 教訓の反映と継続的改善サイクルを運用し、訓練・演習及び外部支援を活用しながら IT-BCP を日常業務に定着させる方法を理解すること

28-4. サイバーレジリエンス能力向上のための実践的な演習と訓練

関連項目
5-2-3、22-3-4、24-1、24-1-1、

文書化された IT-BCP/IRP の実効性を確保するためには、定期的な訓練と演習が必須です。訓練は、計画が緊急時に機能するかを検証し、全関係者の役割の明確化と習熟度向上に寄与します。

対象別訓練の推奨

【経営層向け】

サイバーリスクを伴う経営判断や、対外的なコミュニケーションをシミュレーションする訓練が必要です。

【実務担当者向け】

実践的サイバー防御演習（CYDER、RPCI など）を活用し、インシデント封じ込めや復旧の具体的な技術手順を習得させます。

人材育成の統合

セキュリティ専門人材以外の全従業員がインシデント発生時の初期対応（報告、連絡、封じ込め支援）を適切に行えるよう、「プラス・セキュリティ」知識補充講座などを活用した継続的なスキル育成が必要です。この非専門人材の育成は、リソースが限定的な中小企業にとって、外部の専門家との連携を円滑にする「橋渡し役」の確保につながります。

IT-BCP におけるインシデント対応（IR）体制の実践ステップと教訓の反映

ステップ	実践内容の概要（サイバーレジリエンス視点）	ハンドブック内参照基準	サイバーレジリエンス能力への貢献
準備・計画（Plan）	IT-BCP/IRP 策定、RTO/RPO 設定、体制構築、演習実施	15-2-6. 事業継続計画策定 24-1. 知識補充講座カリキュラム例	事態発生時の対応能力と迅速性の確保
検知・分析（Detect/Analyze）	脅威の早期検知と影響範囲の特定、ログ保全	5-2-3. 事案発生→課題の抽出… 18-2-13. ロギング	被害拡大の防止（封じ込め）
復旧・回復（Recover）	システムの復元、サービス再開、恒久対策の	5-3-3. 具体的な対応策	タイムリーな事業の再開

	実施	18-2-11. バックアップ	
改善・教訓 (Improve)	事後評価に基づく再発防止策の実施、ポリシー改訂、訓練見直し	5-2-4. インシデントから得た気づきと取組 13-2-8. ISMS:10. 改善	組織全体のレジリエンス向上と適応性の獲得

IT-BCP の訓練・教育を定着させる実践的な手順

IT-BCP（情報システム継続計画）における訓練と教育を、日常業務に定着させるための実践的な手順を示します。

訓練・教育実施案の立案

訓練は組織の成熟度に応じ、段階的に導入します。初期は「計画理解と連携確認」を目的とした机上訓練を実施し、その後、模擬訓練や外部演習（CYDER 等）へ発展させます。

- 机上訓練（基本）：報告手順・判断ルートの確認
- 模擬訓練（応用）：シナリオに沿った実践的対応
- 外部演習（発展）：他機関との合同訓練による対応力強化

この段階的アプローチにより、無理のない訓練体制を構築できます。

訓練計画と役割分担例

訓練実施にあたっては、目的・対象・頻度を明確に設定します。

- 目的：初動対応の確認、連絡体制検証、復旧手順の確認
- 対象：経営層、IT 担当者、従業員など役割に応じて区分
- 頻度：年 1 回以上を基本とし、体制変更時に追加実施

訓練の進行・記録は IT 担当者が兼務しても構いません。小規模組織でも実施しやすい形に簡略化することが重要です。

結果の記録と改善への反映

訓練後は、評価表や実施記録を作成し、改善点を整理します。

- 連絡体制の有効性（報告遅延や情報漏れの有無）
- 判断・指示の妥当性（優先度や対応順の適切さ）
- 文書整合性（計画書との乖離）

結果は IT-BCP 文書に添付し、次回の改善サイクルに反映します。この継続的な記録が、組織のレジリエンス向上に直結します。

外部支援の活用

自組織のみでの訓練実施が困難な場合は、外部支援を積極的に利用します。

- IPA：中小企業向けサイバー演習教材、CYDER プログラム
- NCO：演習モデル・訓練シナリオの提供
- 地域：商工会・情報セキュリティ連携組織との合同訓練など

これらの支援を組み合わせることで、継続的で現実的な訓練環境を整備できます。

詳細理解のため参考となる文献（参考文献）	
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf
セキュリティインシデント対応机上演習教材	https://www.ipa.go.jp/security/sec-tools/ttx.html
中小企業支援セミナー（IPA 主催）	https://www.ipa.go.jp/security/seminar/sme/supportseminar.html?utm_source=chatgpt.com

編集後記

第 10 編では、サイバーレジリエンスを実務に落とし込むうえで中心的な位置づけとなる IT-BCP とインシデント対応計画（IRP）の統合、復旧プロセスの確立について紹介しました。特に、中小企業が限られたリソースの中で現実的に取り組むためには、予防から復旧までのプロセスを一貫した体系として扱うことが重要である点を改めて確認しました。本編では、この 2 つの計画を一体として整理し、実務に即した体制として構築するための視点を中心に解説しています。

さらに、Respond 機能に基づく初動対応の重要性についても取り上げました。検知・報告・封じ込め・根絶という流れは、どの組織においてもインシデント対応の共通の骨格となります。その実効性を支えるのは、日常的なログ管理や役割分担の明確化といった基本的な仕組みです。外部機関との連携、机上訓練の実施、発生時の記録の徹底など、平常時に整えるべき要素が多く存在することもお伝えしています。さらに、復旧段階では、RTO 及び RPO を事前に設定しておくことでが企業活動の再開速度を大きく左右すること、バックアップの取得だけでなく、復元可能性を確認するための定期的な検証、復旧後の教訓をどのように手順書や訓練へ反映していくかについても触れ、改善のプロセスが組織の適応力そのものにつながることを解説しています。

サイバーレジリエンスの強化は、計画の文書化、連絡体制の整備、訓練の実施、バックアップ検証、教訓の反映といった、ひとつひとつの取り組みを確実に積み上げることで、組織の復旧力と継続力は大きく向上します。本編が、皆さまの組織で取り組むべき項目を見直すきっかけとなり、日常の業務からサイバーレジリエンスに取り組むきっかけとなれば幸いです。

第29章. 生成 AI および AI マネジメントシステム

章の目的
第 29 章では、生成 AI の利活用に伴うリスクとガバナンスの要点を理解し、組織としての AI 運用方針を確立すること及び AI 倫理、情報セキュリティ、法的遵守を統合した管理体制を構築し、安全かつ信頼できる生成 AI 活用を実現することを目的とします。

主な達成目標
◘ 生成 AI 利用における情報管理とリスクの仕組みを理解すること ◘ ISO/IEC 42001（AI マネジメントシステム）の構成と適用範囲を把握すること ◘ 自社の AI 活用を統制する方針策定と運用手順を検討できるようにすること

29-1. AI の進化とガバナンス・リスクマネジメントの喫緊性

人工知能（AI）技術は、その急速な普及と進化により、ビジネスと社会に計り知れない変革をもたらしています。この革新的な可能性の裏側には、潜在的なリスクと倫理的な課題が内在しており、その適切な管理が喫緊の課題として浮上しています。例えば、AI の活用においては、学習データのバイアス、個人のプライバシー侵害、システムへのセキュリティリスク、そして倫理的な問題といった多岐にわたる懸念が指摘されています。

特に、AI がもたらす自動的な意思決定、その非透明性、および判断プロセスの非説明可能性といった AI 固有の特性は、従来のシステム開発や運用におけるアプローチとは異なる、新たな考慮事項を提起しています。さらに、近年注目される生成 AI の活用においては、不正確な情報生成、既存著作物の模倣による著作権侵害、企業内の機密情報や個人情報の漏洩、さらには攻撃者が生成 AI を悪用することによるフィッシングメールやマルウェア開発といったセキュリティ攻撃の助長など、具体的なリスクが顕在化しており、早急な対策が求められています。

このような AI 技術の進化とそれに伴うリスクの増大を受け、世界各国では AI に関する規制の整備が急速に進んでいます。例えば、欧州連合（EU）の AI Act、米国国立標準技術研究所（NIST）の AI リスクマネジメントフレームワーク（AI RMF）、米国大統領令などが挙げられ、企業は AI の適切な開発・運用方法について新たな課題に直面しています。このような国際的な規制動向に対応し、AI の責任ある利用に関する共通の枠組みを提供するために、国際標準化機構（ISO）と国際電気標準会議（IEC）が協力して ISO 規格の開発を進めてきました。ISO 規格は、AI に関するリスクを回避するための要件や、リスクが発生した場合の対応を含む信頼性の高いマネジメントシステムを構築することを可能にし、より安全・安心な AI システムの普及拡大に貢献することが期待されています。国際標準に準拠することは、AI システムの開発・提供・使用を行う事業者間で共通理解を促進し、ひいては AI システムの国際取引を円滑にするという戦略的なメリットももたらします。

AI がもたらすリスクは、単なる技術的な欠陥に留まらず、社会、倫理、経済、心理といった広範な領域に影響を及ぼす多面的な不確実性として認識されています。この複雑なリスクプロファイルに対して、国際社会はまだ統一された規制アプローチを確立しておらず、各国がそれぞれの価値観や産業構造に基づいた多様なリスクベースアプローチを模索している段階にあります。これは、企業が国際的な AI ビジネスを展開する上で、単一の規制遵守だけでなく、複数の異なる規制枠組みへの適合性を考慮する必要があることを示唆しています。AI の技術的進歩が規制の進歩を上回る速度で進行しているため、規制当局は常に後追いにならざるを得ない状況にあります。このスピードギャップが、各国の規制アプローチの多様性と、国際標準化の重要性を加速させています。ISO 規格は、このギャップを埋め、国際的な相互運用性を促進するための共通言語としての役割を担っ

ていると言えます。結果として、企業が AI を導入する際、技術選定だけでなく、その AI がどの国の規制に準拠する必要があるか、どのような倫理的・社会的影響を考慮すべきかといった、より高度なガバナンス戦略が不可欠となります。ISO/IEC 42001 は、この複雑な状況下で、企業が国際的な信頼性を獲得し、競争力を維持するための羅針盤となり得ます。

29-2. AI ガバナンスの国際標準：ISO/IEC 42001 の全貌

29-2-1. ISO/IEC 42001 とは：AI マネジメントシステム(AIMS)の目的と特徴

ISO/IEC 42001 は、AI を安全かつ効果的に管理するための「AI マネジメントシステム（AIMS: AI Management System）」に関する国際標準であり、2023 年 12 月に正式に発行された世界初の AI マネジメントシステム認証規格です。この規格の主たる目的は、組織が AI を適切に管理するための堅牢なフレームワークを提供し、AI の設計・開発・運用におけるリスクを最小化しつつ、倫理的かつ効果的に AI 技術を活用することにあります。

メリット項目	内容	意義
AI の信頼性向上	企業の AI システムが国際標準に準拠していることを示し、顧客や取引先の信頼を獲得できる。	グローバル市場での競争優位性を確立し、ブランド価値を高める。
リスク管理の強化	AI のバイアス、プライバシー、セキュリティリスクを体系的に管理し、法的・倫理的なトラブルを未然に防ぐ。	予期せぬ事態による事業中断や風評被害を最小限に抑える。
国際規制への対応容易化	EU の AI 規制（AI Act）や GDPR といったグローバルな規制への適合性を高め、国際ビジネス展開を円滑にする。	法的リスクを低減し、新たな市場への参入障壁を下げる。
競争力の向上	AI 管理体制が国際基準に適合していることを示し、市場における独自の強みとしてアピールできる。	認証取得が業界標準となる可能性を見据え、先行者利益を確保する。
ガバナンスの確立・強化	AI に関する明確な責任体制とプロセスを構築し、組織全体の AI に対する意識と統制力を高める。	組織全体で一貫した AI 利用方針を徹底し、内部統制を強化する。
コスト削減と効率向上	AI マネジメントシステムを効率的に構築し、開発期間の短縮と潜在的な損失回避	長期的な視点で AI 投資の費用対効果を最大化する。

	によりコストを削減する。	
イノベーションと責任のバランス	AI 導入を戦略的決定として促し、事業目標とリスク管理戦略の整合性を確保することで、イノベーションを推進しつつ責任ある利用を両立させる。	AI の可能性を最大限に引き出しつつ、社会からの信頼を維持する。

この表は、企業が ISO/IEC 42001 導入を検討する際の経営層への説得材料として極めて価値が高いです。単なる技術標準ではなく、事業戦略や競争優位性、社会的責任といった多角的な視点からその重要性を一目で理解できるためです。特に、コスト削減や効率向上といった実利的な側面も示すことで、投資対効果を意識する意思決定者にとって魅力的な情報となります。AI の持つ強力な潜在能力を「暴れ馬」に例える見方もありますが、この規格はそれを手なずけ、イノベーションを阻害せずに責任ある利用を可能にするというバランスの取れたアプローチを示しており、AI 導入の潜在的な障壁を乗り越えるための具体的な論拠を提供します。

29-2-2. 既存のマネジメントシステム規格（ISO 9001 など）との整合性

ISO/IEC 42001 は、ISO 9001（品質マネジメントシステム）、ISO/IEC 27001（情報セキュリティマネジメントシステム）、ISO/IEC 27701（プライバシー情報マネジメントシステム）、ISO 13485（医療機器品質マネジメントシステム）など、既に広く確立されている既存のマネジメントシステム規格と同様の「ハイレベルストラクチャー（HLS）」を採用しています。この共通構造により、既に他の ISO マネジメントシステムを導入している組織は、比較的容易に AI マネジメントシステムを導入・統合することが可能となります。

特に、ISO/IEC 27001 の認証を取得している組織にとっては、ISO/IEC 42001 との統合は共通のメリットを提供し、プロセスを合理化し、情報セキュリティと AI ガバナンスの効率化を促進します。ISO/IEC 42001 は、既存規格の実施を前提条件とはしていませんが、これらの規格との互換性を持つことで、組織モデルが全体的なアプローチを採用し、各マネジメントシステムが特定の目的を追求することを示唆しています。

既存のマネジメントシステムを保有する企業にとって、ISO/IEC 42001 の導入は、単なる追加のコンプライアンス負担ではなく、既存の強みを活かした「効率的な AI ガバナンス強化」の機会となります。これは、AI 導入の障壁を下げ、既に確立された組織文化やプロセスを通じて、責任ある AI の原則を迅速に浸透させる戦略的な優位性を生み出すものです。HLS の採用は、ISO が新しい技術領域の標準化において、既存の成功モデルを横展開し、企業側の導入負荷を軽減しようとする明確な意図を示しています。これにより、AI の急速な進化に対応しつつ、規格の普及を加速させる効果が期待できます。結果として、企業は、ISO/IEC 42001 の導入を、既存の ISMS や QMS

の延長線上と捉えることで、部門間の連携を強化し、情報セキュリティや品質管理の専門知識を AI ガバナンスに応用できます。これにより、組織やシステムが部署ごとに孤立し、情報やデータが十分に共有・連携されず、全体として最適化されていない状態となってしまう、いわゆる「サイロ化」を防ぎ、組織全体で一貫したリスクマネジメント体制を構築することが可能となります。

29-3. AI に特有のリスクの特定と体系的な管理

29-3-1. AI がもたらす主なリスクの種類と影響（バイアス、プライバシー、セキュリティ、倫理的課題など）

AI の活用には、バイアス、プライバシー、セキュリティ、倫理的課題などの多様なリスクが伴います。経済産業省・総務省の「AI 事業者ガイドライン」では、日本が 2019 年に公表した「人間中心の AI 社会原則」（7 つの原則）をもとに、AI で想定されるリスクを 10 の原則に細分化し、それぞれの主なリスクを整理しています。

項目	共通の指針	主なリスク
1) 人間中心	人間の尊厳及び個人の自律、AI による意思決定・感情の操作等への留意、偽情報等への対策、多様性・包摂性の確保、利用者支援、持続可能性の確保	● 人間の尊厳及び個人の自律を損なうリスク（プロファイリング時の配慮の必要性等） ● AI により意思決定・感情の操作をされてしまうリスク ● 偽情報などのリスク ● 多様性や包摂性が確保されないリスク ● 地球環境への影響のリスク
2) 安全性	人間の生命・身体・財産、精神及び環境への配慮、適正利用、適正学習	● 動作が止まる、低下するリスク ● 意図しない動作のリスク ● ステークホルダーがリスクを知らないリスク ● 目的外に利用してしまうリスク ● 学習データに十分な品質がないリスク ● 学習データのコンプライアンスリスク
3) 公平性	AI モデルの各構成技術に含まれるバイアスへの配慮、人間の判断の介在	● バイアスによる公平性を損なうリスク（潜在的なバイアスを含む） ● 人間の介在が不足するリスク ● バイアスの評価プロセスが不十分なリスク
4) プライバシー保護	AI システム・サービス全般におけるプライバシーの保護	● プライバシーを侵害するリスク
5) セキュリティ	AI システム・サービスに影響す	● 不正操作のリスク

確保	るセキュリティ対策、最新動向への留意	● AI システム自体へのセキュリティ侵害へのリスク ● 不正データが使われるリスク
6) 透明性	検証可能性の確保、関連するステークホルダーへの情報提供、合理的かつ誠実な対応、関連するステークホルダーへの説明可能性・解釈可能性の向上によりコストを削減する。	● 検証ができないリスク ● ステークホルダーに十分な情報提供がされないリスク ● 合理的な情報提供を求められるリスク
7) アカウンタビリティ	トレーサビリティの向上、「共通の指針」の対応状況の説明、責任者の明示、関係者間の責任の分配、ステークホルダーへの具体的な対応、文書化	● トレーサビリティ情報が入手できないリスク ● 共通の指針への対応状況が報告されないリスク ● 責任が明確にならないリスク ● ステークホルダーと適切なコミュニケーションが取れないリスク ● 各種情報をドキュメンテーションできていないリスク
8) 教育・リテラシー	AI リテラシーの確保、教育・リスキリング、ステークホルダーへのフォローアップ	● AI 利用者が判断能力を持たないリスク ● AI により雇用が奪われるリスク ● ステークホルダーが技術などの進化に追随できないリスク
9) 公正競争確保		● AI に関して公正な競争が阻害されるリスク
10) イノベーション	オープンイノベーション等の推進、相互接続性・相互運用性への留意、適切な情報提供	● AI のイノベーションが阻害されるリスク ● 相互運用性が確保されないリスク ● AI に関する情報が十分に伝達されないリスク

この表は、企業が AI リスクを網羅的に特定し、評価するための実用的なチェックリストとして機能します。多様なリスクを体系的に理解することで、見落としを防ぎ、効果的なリスクアセスメントの基盤を築くことができます。特に、技術的リスクだけでなく、倫理的・社会的・経済的リスクまで含めることで、AI ガバナンスの全体像を把握し、多角的な視点から対策を検討する上で不可欠な情報となります。

特に生成 AI 特有のセキュリティリスクとして、著作権侵害のリスク、ビジネスデータの漏洩リ

スク（機密情報や個人情報の入力による）、攻撃者による生成 AI 悪用によるセキュリティ攻撃の助長（フィッシングメールやマルウェア開発）が挙げられます。リスクは、ISO 31000 では「物事の不確実性に影響があるもの」と定義されており、これはネガティブな影響だけでなく、ポジティブな影響（機会）も含む概念です。欧州 AI 法（EU AI Act）では、AI のリスクレベルを「受け入れがたいリスク」「ハイリスク」「限定的なリスク」「ミニマムリスク」の 4 段階に分類し、それぞれに応じた規制アプローチを検討しています。

29-3-2. ISO/IEC 42001 におけるリスクベースアプローチの原則

ISO/IEC 42001 は、AI システムを適切に開発、提供、または使用するために必要なマネジメントシステムを構築する際に遵守すべき要求事項を、リスクベースアプローチによって規定しています。このアプローチは、組織が AI システムに内在するリスクを特定し、軽減するための体系的な方法を提供することを目的としています。ISO/IEC 42001 は、リスク評価プロセスから、適切な処置オプションの選択、必要な管理策の実施に至るまで、リスクを積極的に最小化し、AI システムの回復力を強化するために必要なツールを組織に提供します。規格は、組織が AI 関連のリスクに包括的に対処するために、38 の管理策と 10 の管理目標（付録参照）の実施を求めています。

AI の急速な進化とそれに伴うリスクの多様性は、一律の厳格な法規制では対応しきれないという課題を提起します。この状況において、ISO/IEC 42001 がリスクベースアプローチを中核に据えていることは、非常に戦略的な意味合いを持ちます。これは、組織が個々の AI システムの特性、利用目的、および潜在的な影響度に基づいて、リスクを評価し、それに応じた管理策を柔軟に適用することを可能にします。これにより、過剰な規制によるイノベーションの阻害を防ぎつつ、高リスクな AI システムに対しては厳格な管理を求めるという、バランスの取れたアプローチが実現されます。このような柔軟性は、技術の進歩が速い AI 分野において、規格が陳腐化することなく、長期的にその有効性を維持するための重要な要素となります。

29-3-3. AI リスクアセスメントと影響度評価の具体的な実践

ISO/IEC 42001 では、AI リスクアセスメントと AI システム影響度評価が重要な要素として位置づけられています。AI リスクアセスメントは、AI に関連するリスクの重要性と範囲を特定し、分析し、評価するプロセスです。これには、バイアス、プライバシー侵害、誤判断などのリスクを特定することが含まれます。リスクの特定にあたっては、自社の管理下にあるか否かを問わず、災害など外部で発生する可能性のあるリスクも考慮することが望ましいとされています。

AI システム影響度評価は、AI システムの開発、提供、および使用が個人、グループ、社会に与える潜在的な影響を評価するものです。例えば、人権侵害、情報漏洩、雇用減少といった課題が挙げられます。この評価は、AI リスクアセスメントの際に実施することが推奨されています。

これらの取り組みは、ISO/IEC 42001 の「6. 計画」段階でプロセスを設計し、「7. 支援」段階で必要な文書を作成し、「8. 運用」段階で実行することが求められています。リスク分析においては、意見の相違や先入観による影響を避け、不確かで複雑な事象に対しては定性・定量など複数の手法を組み合わせて分析を行うことが重要です。リスク対応策としては、リスク回避、リスク追求、リスク除去、確率変更、結果変更、リスク共有、リスク保有といった選択肢が挙げられます。

29-3-4. ISO 31000（リスクマネジメントの指針）との連携と活用

ISO 31000 は、リスクマネジメントの指針を示した国際規格であり、組織がリスクを適切に管理し、事業運営の信頼性を高めるためのフレームワークを提供します。この規格は、リスクマネジメントのベストプラクティスを学ぶ上で活用できます。ISO 31000 は、リスクマネジメントの全体を「原則」、「枠組み」、「プロセス」で説明しており、そのプロセスには、コミュニケーションおよび協議、組織の状況の確定、リスク特定、リスク分析、リスク評価、リスク対応、モニタリングおよびレビュー、記録作成および報告が含まれます。

ISO 31000 の指針を使用することで、リスクの洗い出しからリスク対応計画の策定までのプロセスを体系的に行うことができます。これにより、リスク発生時の損失を最小化し、リスクに対する事前管理を整えることが可能になります。また、ISO 31000 に準拠することで、危機管理体制が必要十分であることを社外へ発信しやすくなるメリットも得られます。AI 特有のリスクを特定し管理する上で、ISO 31000 が提供する包括的なリスクマネジメントの枠組みは、ISO/IEC 42001 の実践において強力な基盤となります。

29-4. ISO/IEC 42001 に基づく AI マネジメントシステムの構築と運用

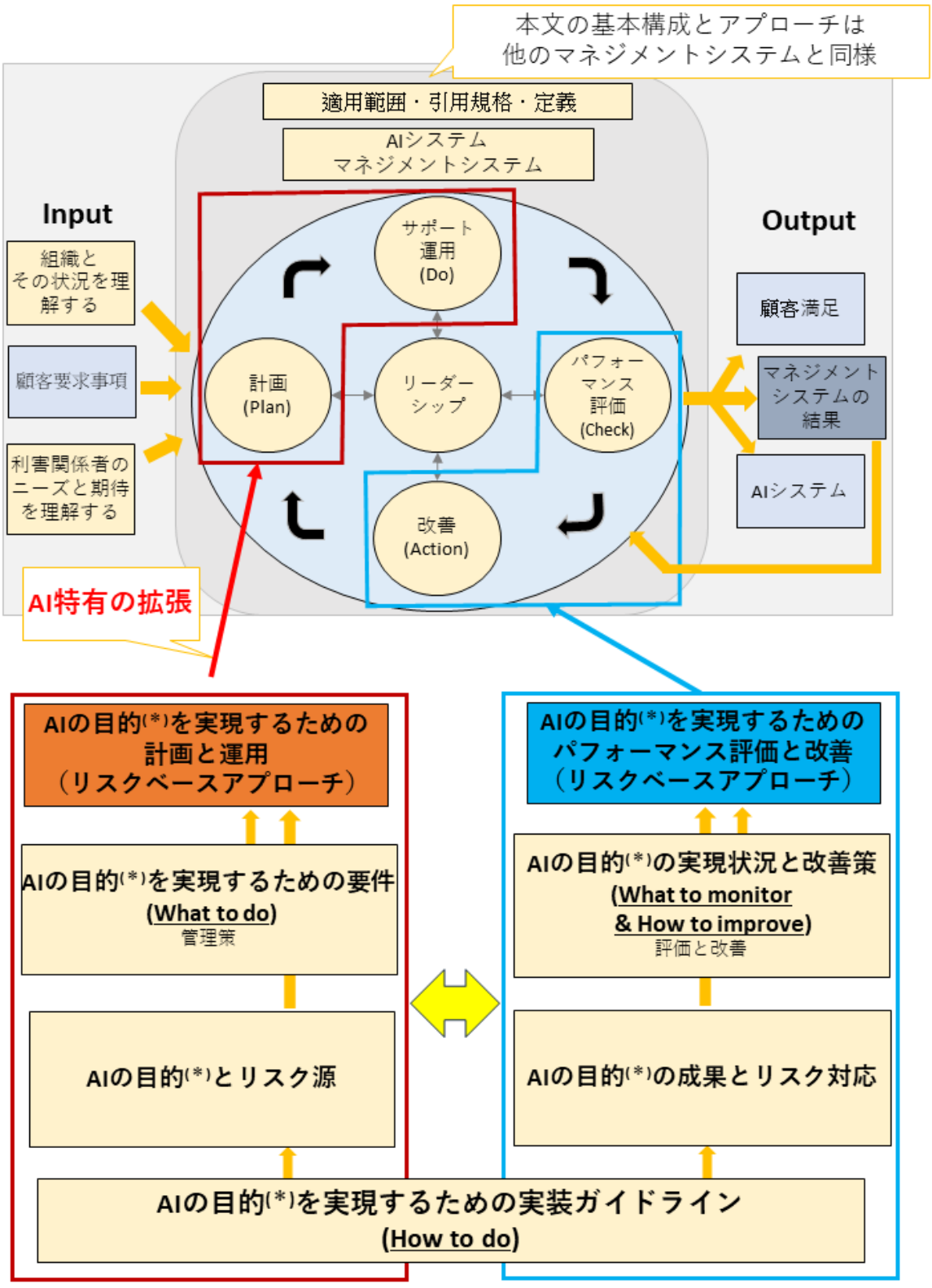


図. AI マネジメントシステムの構

（転載）経済産業省「AI マネジメントシステムの国際規格が発行されました」

https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html

29-4-1. 主要な要求事項と管理策（Annex A の活用）

ISO/IEC 42001 は、他の ISO マネジメントシステム規格と同様に、全 10 章からなるハイレベルストラクチャー（HLS）で構成されています。このうち、実質的な実装は第 4 章「組織の状況」から第 10 章「改善」までが中心となります。

主要な要求事項は以下の通りです。

組織の文脈（コンテキスト）

内部および外部要因の理解、利害関係者のニーズと期待の理解、AI 関連の目的の決定、そして組織内の AI マネジメントシステムの目的を定めます。

リーダーシップ

コミットメント、責任、および AI に関する情報文化の促進を求めます。

計画策定

AI の機会とリスクの特定、目的の定義、AI に関連するリスク軽減と対応のための行動計画を策定します。AI リスクアセスメントや AI システム影響度評価といった AI 固有の活動のプロセス設計がこの段階で行われます。

サポート

AI の責任ある管理に必要な資源、技能、認識、コミュニケーションの提供を規定します。計画された活動に必要な文書の作成がこの段階で行われます。

運用

AI システムの導入、データ管理、パフォーマンス・モニタリング、リスク管理を行います。計画されたプロセスの実行がこの段階で行われます。

パフォーマンス評価

AI のパフォーマンスを監視・測定し、目標に照らして評価し、マネジメントレビューを実施します。

改善

評価とフィードバックに基づき、AI システムおよび AI マネジメントシステムそのものを改善するための継続的な措置を講じます。

巻末には 4 つの付属書（Annex）が掲載されており、特に「付属書 A（規範的）参照コントロール目標およびコントロール」は、AI マネジメントシステムにおける具体的な管理策の指針を提供

します。これらの管理策は、AI の設計・開発・運用におけるリスクを軽減し、透明性と説明責任を確保するための具体的な手段であり、企業が AI を適切に活用し、社会的な信頼を得るためのガイドラインとなります。

付属書 A の管理策は、大きく以下の 5 つのカテゴリに分けられます。

1. AI のガバナンス管理策（リーダーシップ・責任の明確化）

組織全体のガバナンス体制整備が重要であり、AI ガバナンスの方針策定、責任者の明確化、規制・法令遵守体制の整備が求められます。例えば、AI 倫理委員会の設置が挙げられます。

2. リスクマネジメントに関する管理策（リスクアセスメント・対応策）

バイアス、プライバシー侵害、誤判断などのリスク特定のための AI リスク評価の実施、影響の大きいリスクに対する適切なリスク低減策の導入、AI の誤作動や不正利用発生時の緊急対応計画の策定が求められます。バイアス検知ツールの導入などが例として挙げられます。

3. データとアルゴリズムの管理策（バイアス防止・品質管理）

AI のトレーニングデータが正確かつ公平であることの確認（データの品質管理）、AI が特定のグループを差別しないようにする仕組み（バイアス防止策）、AI の出力が予期せぬ動作をしないようテスト実施（アルゴリズムの安全性検証）が求められます。AI の公平性を評価するダッシュボードの開発が例示されます。

4. AI の透明性と説明責任に関する管理策（意思決定の透明性）

AI の決定に対する異議申し立ての仕組み導入が求められます。AI の判断理由をユーザーがリクエストできる機能の実装などが例として挙げられます。

5. 継続的な監視と改善のための管理策（モニタリング・フィードバック）

AI のパフォーマンス評価の実施、新しいリスクや課題発生時の AI の調整、第三者機関による外部監査の実施が求められます。

29-4-2. 導入プロセスと実践的なステップ

ISO/IEC 42001 への準拠を達成することは、AI システムを倫理的、安全かつ透明性をもって管理することを目指す組織にとって戦略的なステップです。導入のための一般的なステップは以下の通りです。

1. ギャップ分析の実施

ISO 42001 の要求事項に対する現在の慣行を特定し、修正が必要な箇所を理解します。AI 活

用状況や既存の管理体制を把握し、AI に関するリスク評価の現状や社内ポリシーの有無などを精査します。この段階で経営層や関係部門へのヒアリングを実施し、トップの意識醸成を図ることも重要です。

2. **AI マネジメントシステムの開発**
   AI マネジメントシステムを既存の組織プロセスに統合します。

3. **リスク評価と影響度評価の定期的な実施**
   潜在的なリスクと相対的なインパクトを特定するために、AI システムのリスクおよび影響評価を定期的に実施します。

4. **AI 方針および/または手順の導入**
   AI の側面（倫理、データ保護、プライバシー）をカバーするために、AI 方針および/または手順を導入します。

5. **プロセスの文書化**
   すべてのプロセスの文書化を行います。

6. **外部監査への準備**
   認証取得のため、外部監査への準備を行います。

認証取得後も、組織は変化する法律や規制を把握し、方針と手順を確実に更新し、定期的な内部監査を実施し、従業員に研修を受けさせることで、規格へのコンプライアンスを維持することが重要です。

29-4-3.既存システムとの統合と効率的な導入

ISO/IEC 42001 は、ISO 9001 や ISO/IEC 27001 などの既存のマネジメントシステム規格と共通の HLS を採用しているため、他の ISO マネジメントシステムとの統合を見据えた設計や構築支援が可能です。既にこれらの認証を取得している組織にとっては、AI マネジメントシステムの導入は既存の管理構造への組み込みが容易であり、プロセスを合理化し、情報セキュリティと AI ガバナンスの効率化を促進します。

この統合により、AI マネジメントシステムを効率的に構築でき、開発期間の短縮とコスト削減につながります。また、AI リスクアセスメントの考え方のみを取り込むなど、組織の都合に合わせて当該規格の一部分だけを採用した整備・導入支援も可能です。

29-4-4. 導入における課題と解決策

ISO/IEC 42001 は新しい規格であるため、導入にはいくつかの課題が伴います。

導入コストと工数の増加

対応する体制づくりやドキュメントの整備に時間とコストがかかります。特に中小企業にとっては、専門人材の確保が課題となることもあります。

継続的な運用負担

一度認証を取得しても、年次監査や定期的な見直しが求められるため、継続的なリソースの投入が必要です。AI の技術進化に追随する体制も整えておく必要があります。

過度な規制による柔軟性の低下

AI の倫理やリスク管理に重きを置くため、開発スピードや柔軟性を犠牲にする場面が出る可能性があります。イノベーションとのバランスをどう取るかが重要です。

これらの課題に対する解決策として、以下が考えられます。

段階的な導入

規格の全体を一度に導入するのではなく、AI リスクアセスメントや AI システム影響度評価といった特定の要素から部分的に導入を始めることが可能です。これにより、組織はリソースを効率的に配分し、段階的に AI ガバナンスを強化できます。

既存システムとの統合

既に ISO 9001 や ISO 27001 などのマネジメントシステムを運用している組織は、その共通の HLS を活用し、AI マネジメントシステムを既存の枠組みに統合することで、導入コストと運用負担を軽減できます。

外部専門家の活用

専門人材の確保が困難な場合、コンサルティングサービスなどを活用することで、ギャップ分析からシステム構築、文書化、監査準備までの一連のプロセスを効率的に進めることができます。

トップマネジメントのコミットメント

経営層が AI ガバナンスの重要性を理解し、積極的に関与することで、組織全体の意識が高まり、導入・運用が円滑に進みます。

ISO/IEC 42001 の導入は、AI 技術の急速な進化とそれに伴う不確実性の中で、組織がリスクを管理し、イノベーションを継続するための「適応的ガバナンス」を構築する機会を提供します。規

格が提供するフレームワークは、単にリスクを抑制するだけでなく、組織が AI の機会を戦略的に捉え、責任ある方法でその恩恵を最大化するための指針となります。この柔軟なアプローチは、AI 技術の特性（自動的な意思決定、非透明性、非説明可能性など）に適応し、組織が AI 特有の課題に対応するための具体的な対策を講じることを可能にします。結果として、ISO/IEC 42001 は、AI の導入を単なる技術的な選択ではなく、事業目標やリスク管理戦略に深く統合された戦略的決定として位置づけ、情報に基づいた意思決定プロセスを促進し、イノベーションと責任のダイナミックなバランスを育むことに貢献します。

詳細理解のため参考となる文献（参考文献）	
東京都　AI 時代の信頼性を築く：ISO/IEC 42001 等の ISO 関連規格に基づく AI ガバナンスとリスクマネジメントの活用戦略	https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/619/index.html
経済産業省　AI マネジメントシステムの国際規格が発行されました	https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html
講演レポート「AI 規制について --欧米の動向と日本の状況--」 | JIPDEC	https://www.jipdec.or.jp/library/report/20240722-r01.html

編集後記

第 11 編では、AI 技術の急速な進展が、社会に多大な恩恵をもたらす一方で、倫理的、プライバシー、セキュリティ、公平性といった多岐にわたる新たなリスクを顕在化させていることを整理しました。これらのリスクは、従来の IT システム管理の枠を超え、AI 固有の特性（非透明性、非説明可能性など）に起因する複雑な課題を提起しています。国際社会は、この複雑なリスクプロファイルに対し、多様な規制アプローチを模索しており、企業は国際的な AI ビジネスを展開する上で、複数の異なる規制枠組みへの適合性を考慮する必要があります。

このような背景のもと、ISO/IEC 42001 は、AI マネジメントシステム（AIMS）に関する世界初の国際標準として、その重要性を増しています。この規格は、AI の安全かつ効果的な管理のための堅牢なフレームワークを提供し、信頼性、透明性、説明責任を備えた AI システムの開発と利用を促進することを目的としています。ISO/IEC 42001 は、既存の ISO マネジメントシステム規格（ISO 9001、ISO 27001 など）と共通のハイレベルストラクチャー（HLS）を採用しているため、既にこれらのシステムを導入している組織は、比較的容易に AI ガバナンスを既存の枠組みに統合し、効率的な導入と運用を実現できます。これは、AI 導入の障壁を下げ、責任ある AI の原則を迅速に浸透させる戦略的な優位性を生み出します。

ISO/IEC 42001 の導入は、AI の信頼性向上、リスク管理の強化、国際規制への対応容易化、競争力の向上、ガバナンスの確立・強化、コスト削減と効率向上、そしてイノベーションと責任のバランスといった多岐にわたるメリットを組織にもたらします。特に、AI の急速な進化とそれに伴う不確実性の中で、組織がリスクを管理し、イノベーションを継続するための「適応的ガバナンス」を構築する機会を提供します。この規格が提供するフレームワークは、単にリスクを抑制するだけでなく、組織が AI の機会を戦略的に捉え、責任ある方法でその恩恵を最大化するための指針となります。

結論として、AI 時代の持続可能な成長を追求する企業にとって、ISO/IEC 42001 の導入は不可欠な戦略的投資です。この規格を積極的に活用し、AI マネジメントシステムを構築・運用することで、組織は AI がもたらす潜在的なリスクを効果的に管理しつつ、その革新的な可能性を最大限に引き出し、国際市場における競争優位性を確立できるでしょう。

第30章. 全体総括エグゼクティブサマリー

章の目的
テキストの読者が経営者などに説明するために、テキストの全体要旨や活用ポイントなどを提示することを目的とします。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いただきたいことや、テキストの活用ポイントについて説明します。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。
主な達成目標
□ 本テキストの全体要旨、活用ポイントをもとに、組織として実践すべき事項と概要を理解すること

30-1. 全体要旨

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。

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。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。

テキストの概要
第 1 編 サイバーセキュリティを取り巻く背景 【レベル共通】 **（第 1 章～第 4 章）** サイバーセキュリティを取り巻く背景として、デジタル化が進む社会と情報技術（IT）活用の動向を解説し、基本的なサイバーセキュリティ知識や UTM・EDR の活用を振り返りました。また、サイバーセキュリティの脅威に対処する段階的なアプローチ方法を明確にするとともに、サイバーセキュリティ戦略に関連する国の方針と関連法令、セキュリティ確保と DX 推進の両立の必要性について解説しました。
第 2 編 中小企業に求められるデジタル化の推進とサイバーセキュリティ対策 【レベル共通】 **（第 5 章～第 6 章）** 実際のインシデント事例を通して、近年のサイバー攻撃の傾向や対策などを紹介しました。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 投資や、経営投資としてのセキュリティ対策の重要性を説明しました。
第 3 編 これからの企業経営で必要な IT 活用とサイバーセキュリティ対策 【レベル共通】 **（第 7 章～第 8 章）** ISMS 認証を前提とした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、それぞれのアプローチ手法について解説しました。さらに、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とそれらの関係性、脅威や脆弱性の識別方法を説明しました。
第 4 編 セキュリティ事象に対応して組織として策定すべき対策基準と具体的な実施 【レベル 1】 **（第 9 章）** 実際のセキュリティインシデントの事例を踏まえ、自社での発生可能性や被害規模を慎重に検討し、対策基準や実施手順を策定していく手法である、Lv.1 クイックアプローチについて解説しました。

第 5 編 各種ガイドラインを参考にした対策の実施 【レベル 2】

（第 10 章）

ガイドラインやひな型など既存の手法を参考にして対策基準や実施手順を策定する手法である、Lv.2 ベースラインアプローチについて解説しました。

第 6 編 ISMS などのフレームワークの種類と活用法の紹介 【レベル 3】

（第 11 章～第 12 章）

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（ISMS、CSF2.0、CPSF など）の概要と、リスクマネジメントやリスクアセスメントの手法、リスク対応の考え方について説明しました。

第 7 編 ISMS の構築と対策基準の策定と実施手順 【レベル 3】

（第 13 章～第 19 章）

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 Lv.3 網羅的アプローチについて説明しました。ISMS の管理策（組織的、人的、物理的、技術的管理策）をもとに、対策基準を策定する手順と、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説明しました。最後に、内部・外部監査によるセキュリティ対策の有効性評価について解説しました。

第 8 編 具体的な構築・運用の実践 【レベル 3】

（第 20 章～第 21 章）

デジタル・ガバメント推進標準ガイドラインなどが示すサービスシステム構築と運用の工程を参考に、中小企業においても有効な情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明しました。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を解説しました。

第 9 編 組織として実践するためのスキル・知識と人材育成 【レベル共通】

（第 22 章～第 25 章）

各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識、IT およびデジタル人材のスキル、知識の認定制度について解説するとともに、必要な知識やスキルを備えた人材の育成・確保のために、関係機関が公表しているセキュリティ関連のカリキュラムを紹介しました。また紹介したカリキュラムなどを活用して教育・研修計画を作成する方法を解説しました。

第 10 編 サイバーレジリエンス能力の育成

（第 26 章～第 28 章）

サイバー攻撃やシステム障害などの事態が発生した場合でも事業を継続し、速やかに復旧・改善するために必要となるサイバーレジリエンス能力について解説しました。従来の侵入防止を

中心とした対策に加え、インシデント対応計画や IT-BCP を含めた対応・復旧・改善の考え方を整理し、中小企業において段階的に取り組むための実践的な方向性を解説しました。

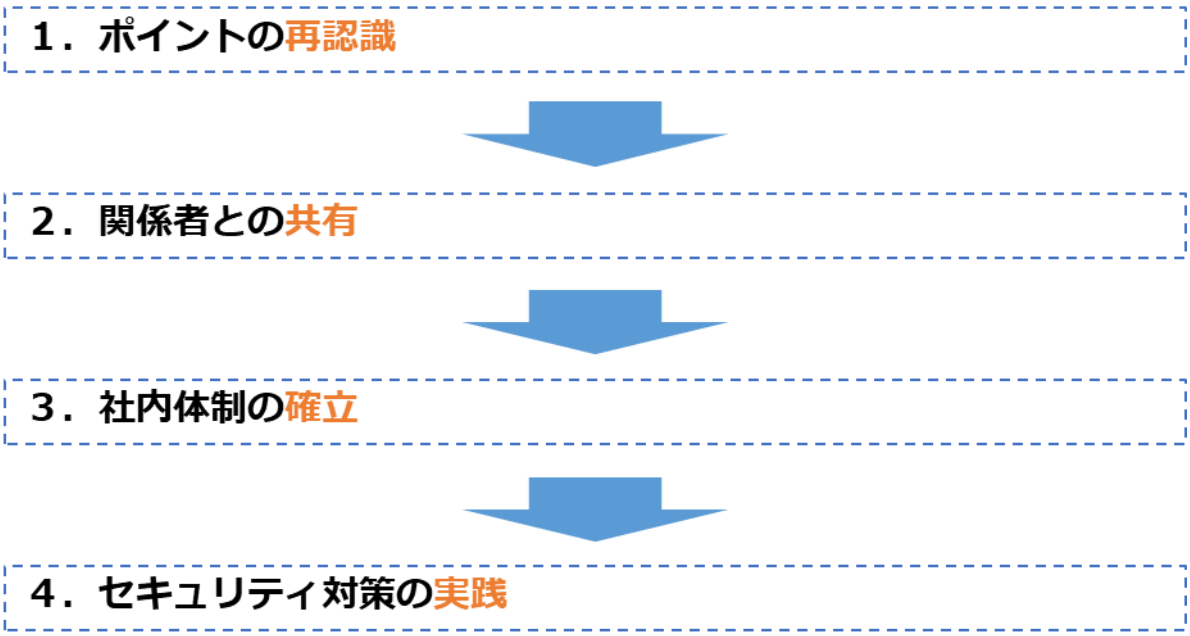
第 11 編生成 AI および AI マネジメントシステム

（第 29 章）

生成 AI の利活用が進展する中で、企業が留意すべきリスクとガバナンスの考え方について解説しました。ISO/IEC 42001 などの国際標準を参考に、情報セキュリティ、法令遵守、倫理を含めた AI マネジメントシステムの基本的な枠組みを整理し、組織として適切に生成 AI を管理・運用するための方向性を説明しました。

30-2. テキストの活用ポイント

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．ポイントの再認識

「DX の理解からサイバーセキュリティ対策の実践まで」のポイントを再認識します。各章の内容は以下の通りです。

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

DX の推進の考え方の把握	
第 1 章	技術革新や経済のグローバル化といったビジネス環境の激しい変化に対応し、顧客ニーズに合致した製品・サービスを提供していくためには、DX を推進する必要があること、つまり、データとデジタル技術を活用して、製品やサービスのみならずビジネスモデルや組織、プロセス、企業文化・風土を変革していく必要があることを解説しています。
第 3 章	国によるデジタル社会に関する方針や政策、Society5.0 の概要や DX 推進における中小企業の優位性とサイバーセキュリティの重要性を解説しています。

第 29 章	生成 AI の普及を背景に、企業が直面する AI 特有のリスクと、それに対応するためのガバナンスや AI マネジメントの考え方を解説しています。

セキュリティ対策の全容の認識	
第 2 章	UTM や EDR の基本的なセキュリティ対策に加え、中小企業向けの「SECURITY ACTION」制度や、サイバーセキュリティの脅威に対処するための 3 つのアプローチ手法について解説しています。
第 4 章	サイバーセキュリティ戦略や DX with Cybersecurity の考え方、企業に求められる人材育成とサイバーセキュリティ対策の重要性、サイバーセキュリティに関する法令について解説しています。
第 5 章	情報セキュリティ白書や情報セキュリティ 10 大脅威、最近のインシデント事例をもとに、ランサムウェアやサプライチェーン攻撃などの脅威とその対策や対応方法について解説しています。
第 6 章	企業が取り組むべき業務効率化やコスト削減といった守りの IT 投資と、DX 推進に向けた攻めの IT 投資の特徴と違い、そして経営者主体のセキュリティ対策の必要性について解説しています。
第 7 章	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）や、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 3 つのアプローチ手法を解説しています。
第 8 章	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解説しています。
第 11 章	セキュリティ対策を効果的かつ漏れなく行うため、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。
第 14 章	ISO/IEC 27002 に基づく ISMS の管理策の分類と構成、企業が自社のリスクに応じたセキュリティ対策を選定・導入する重要性について解説しています。
第 22 章	各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要とされるスキルや知識について、体系的に解説しています。
第 23 章	Di-Lite や情報処理技術者試験、国際セキュリティ資格など、IT およびデジタル人材のスキル、知識の認定制度と活用方法について解説しています。
第 26 章	中小企業におけるサイバーレジリエンスの必要性を整理し、その定義と情報セキュリティ戦略上の位置づけを解説しています。

自組織でのセキュリティ対策の実施項目の認識	
第 9 章	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、Lv.1 クイックアプローチについて解説しています。
第 10 章	独立行政法人情報処理推進機構（IPA）や総務省などが発行しているガイドラインやひな型など、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、Lv.2 ベースラインアプローチについて解説しています。
第 12 章	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（リスク特定、リスク分析、リスク評価）、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。
第 13 章	ISMS のフレームワークに従い、組織全体で適用できるセキュリティ対策基準と手順を整備する Lv.3 網羅的アプローチについて解説しています。
第 20 章	「デジタル・ガバメント推進標準ガイドライン」などが示す政府情報システムの構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を説明しています。
第 24 章	知識やスキルを備えた人材の育成・確保に向けて、具体的な実施計画や実施内容を検討する際の参考となる、セキュリティ関連のカリキュラム内容を解説しています。
第 27 章	サイバー攻撃を含む様々な事態に対して、中小企業が組織として対応・復旧を行うための総合的な対応計画の考え方を解説しています。

自組織としての実践準備	
第 15 章	ISO/IEC 27001:2022 附属書 A の「組織的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 16 章	ISO/IEC 27001:2022 附属書 A の「人的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 17 章	ISO/IEC 27001:2022 附属書 A の「物理的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 18 章	ISO/IEC 27001:2022 附属書 A の「技術的管理策」を参考に、対策基準を策定する手順や、対策基準それぞれに対応する実施手順の例を解説しています。
第 19 章	ルールの形骸化を防ぎ、目的達成に向けた対策を継続的に改善するために、組織内のルールや手順が適切に守られているかを確認する内部監査、

	第三者による客観的な視点から評価する外部監査について解説しています。
第 21 章	「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを、EC サイトを例にとって解説しています。
第 25 章	関係機関が公表しているカリキュラムや指針などを活用し、チェンジマインド、リスキリングも含めた教育・研修の実施内容および実施計画を作成する手順を解説しています。
第 28 章	情報システム継続計画（IT-BCP）を軸に、インシデント対応、復旧・回復、訓練・演習を一体的に運用する方法を解説しています。

2. 関係者との共有

経営者を含めた関係者と、再認識したポイントを共有します。「第 12 編.全体総括」をエグゼクティブサマリーとして活用してください。重要な点を理解し、経営者および他関係者と共有します。

3. 社内体制の確立

経営者のリーダーシップによって、サイバーセキュリティ対策のための社内体制を確立します。知識やスキルを備えた人材の育成・確保をします。人材育成・確保のために、関係機関が公表しているセキュリティ関連のカリキュラムなどを活用し、プラス・セキュリティやチェンジマインド、リスキリングも含めた教育・研修の実施計画および実施内容を作成し、実践します。

経営層をはじめ、法務や広報といった、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身につけること）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を参考にしてください。

人材育成の際に参考となる指針・カリキュラム

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
プラス・セキュリティ知識補充講座カリキュラム例	NCO が経営層や DX 推進管理職向けに提供するプログラム。セキュリティ専門家との協働に必要な知識を補充することを目的としています。

IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1）】	職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラム

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver. 1.2	https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/20240708-p-1.pdf
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.cyber.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

4. セキュリティ対策の実践

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

- Security by Design
- 「第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）」
- 「第 21 章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施」

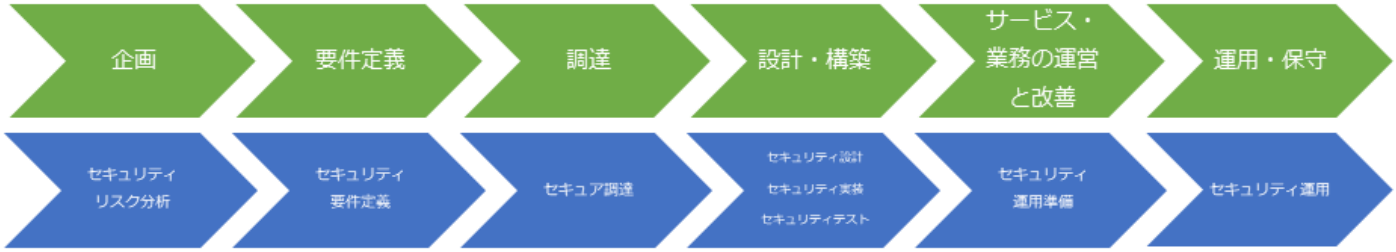


図 103. IT 導入プロセスにおけるセキュリティ対策の実施タイミング

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
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ae9a37b7/20250619_resources_standard_guidelines_guideline_05.pdf

第31章. 各章のポイント

章の目的
テキストの読者が各章の内容を実務に活用できるように、各章のポイントを整理し、具体的な知識やスキルを振り返ることを目的とします。これまで学んだ内容を体系的に再確認し、各章が提示するセキュリティ対策の実施方法を明確にすることで、テキストをもとにした実践的な取組を推進できるようにします。
主な達成目標
◘　各章ごとに重要なポイントを再確認し、理解すること

31-1. 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

主なキーワード
Society5.0、DX、生成 AI

要旨

1 章の全体概要

1 章では、技術革新や経済のグローバル化といったビジネス環境の激しい変化に対応し、顧客ニーズに合致した製品・サービスを提供していくためには、DX を推進する必要があること、つまり、データとデジタル技術を活用して、製品やサービスのみならずビジネスモデルや組織、プロセス、企業文化・風土を変革していく必要があることを解説しています。

また、生成 AI は、データ解析を通じて新たなコンテンツを生成し、業務効率化に役立ちますが、サイバー攻撃に悪用される可能性もあります。生成 AI を利用する際には、機密情報の漏えい防止やセキュリティ意識の向上が重要です。

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）
- DX とは
- 生成 AI とは

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。

生成 AI はさまざまな業務において実用的に活用できるレベルに進化しており、生成 AI を活用

することによって、多くの業務プロセスを効率化できます。パブリックな（共同利用型の）生成 AI に送信した情報は、開発者に見られたり学習データとして使用されたりして情報漏えいのリスクがあります。機密情報は入力しないよう注意が必要です。

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。
- 生成 AI は業務効率化に役立ちますが、パブリックな（共同利用型の）生成 AI には情報漏えいのリスクもあります。情報漏えいのリスクがある場合には、機密情報を入力しないように活用することが重要です。

詳細理解のため参考となる文献（参考文献）	
デジタルガバナンス・コード	https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html
Society5.0	https://www8.cao.go.jp/cstp/society5_0

31-2. 第 2 章. サイバーセキュリティの基礎知識

2-1. 導入済みと想定するセキュリティ対策機能
2-2. SECURITY ACTION（セキュリティ対策自己宣言）
2-3. サイバーセキュリティアプローチ方法

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

主なキーワード
UTM（Unified Threat Management）、EDR（Endpoint Detection and Response）、SECURITY ACTION

要旨

2 章の全体概要

２章では、UTM や EDR の機能など、基本的なセキュリティ対策について解説しています。

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度である「SECURITY ACTION」が推奨されています。「SECURITY ACTION」では、「情報セキュリティ 5 か条」に取り組んだり、「情報セキュリティ自社診断」を実施したり「情報セキュリティ基本方針」を策定したりします。また、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「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」を解説しています。

2-1. 導入済み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。

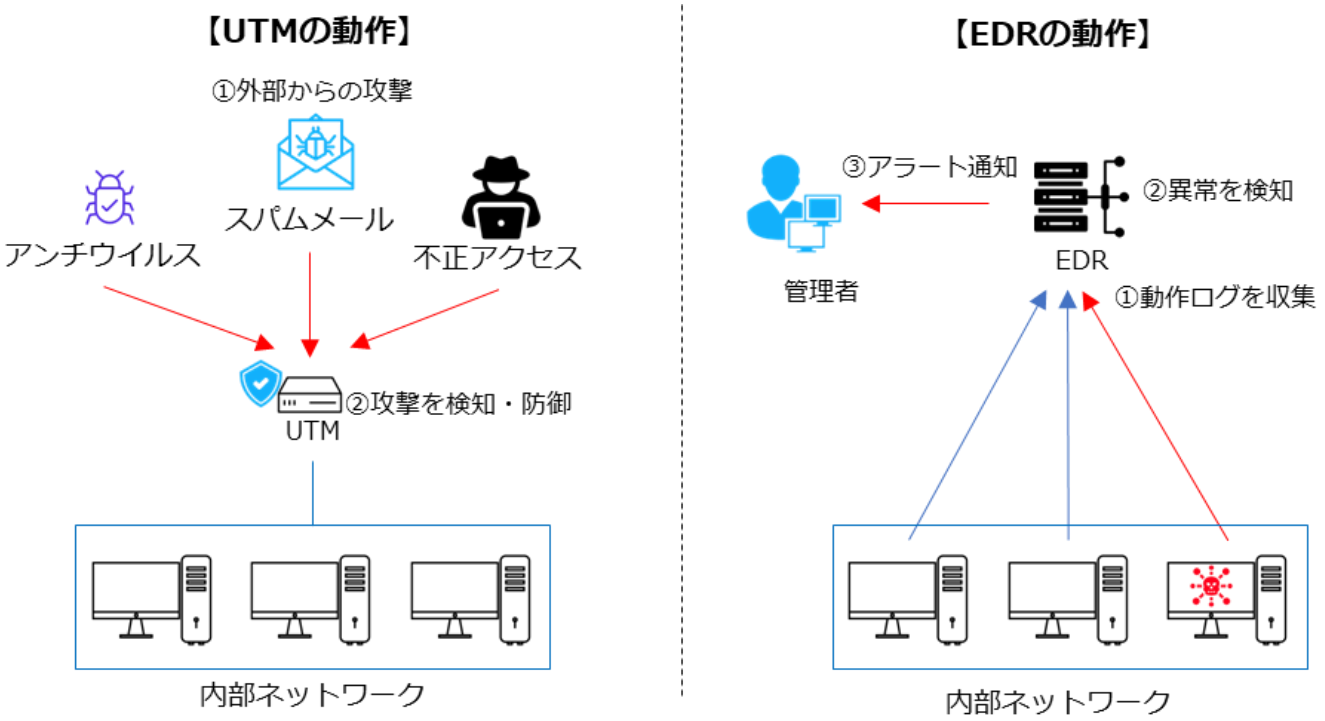


図 104. UTM、EDR の概要図

2-2. SECURTY ACTION （セキュリティ対策自己宣言）

「SECURITY ACTION」に取り組むことで、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つながります。一つ星・二つ星を宣言するには、次の事項に取り組む必要があります。

- 情報セキュリティ 5 か条
- 情報セキュリティ自社診断
- 情報セキュリティ基本方針

2-3. サイバーセキュリティアプローチ方法

サイバーセキュリティの脅威に対処するアプローチ方法には複数の方法があります。それぞれメリット・デメリットがあるので、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ようにしてください。

- 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

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はじめるにあたり、SECURITY ACTION に取り組み、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

- 中小企業が情報セキュリティ対策に取り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 種類のアプローチがあること。

詳細理解のため参考となる文献（参考文献）	
SECURITY ACTION セキュリティ対策自己宣言	https://www.ipa.go.jp/security/security-action/
情報セキュリティ 5 か条	https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf
5 分でできる！情報セキュリティ自社診断	https://www.ipa.go.jp/security/guide/sme/5minutes.html
情報セキュリティ基本方針（サンプル）	https://www.ipa.go.jp/security/sme/f55m8k0000001wbv-att/000072146.docx

31-3. 第 3 章. デジタル社会の方向性と実現に向けた国の方針

3-1. 国の基本方針および実施計画の概要

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

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

主なキーワード

デジタル社会、デジタルトランスフォーメーション（DX）、DX の推進、サプライチェーン

要旨

3 章の全体概要

３章では、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づ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 を紹介し、DX 推進における中小企業の優位性について事例を交えて説明しています。

3-1. 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。「骨太の方針 2025」に基づく、中小企業の DX・セキュリティ関連事項として「柱 1. 物価上昇を上回る賃上げの普及・定着」「柱 3. 「投資立国」及び「資産運用立国」」「柱 4. 国民の安心・安全の確保」が示されています。

3-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

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」を閣議決定しました。策定された「デジタル社会の実現に向けた重点計画」において、「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 6 つの姿を挙げています。

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 2. 医療・教育・防災・こどもなどの準公共分野のデジタル化 3. デジタル化による地域の活性化 4. 誰一人取り残されないデジタル社会 5. デジタル人材の育成・確保 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

「デジタル社会の実現に向けた重点計画」で記載されている中でも、『４、安全・安心なデジタル社会の形成に向けた取組』は、デジタル社会の急速な進展に伴い、国民・企業が安心してデジタル技術を活用できる環境を整備するための政策が体系的に示されています。中小企業にとっても、特に重要となる章であり、5 つのポイントが示されています。

安全・安心なデジタル社会の形成に向けた取組（要約）　5 つのポイント
1. デジタルリテラシーの向上 2. アクセシビリティの確保 3. 偽・誤情報等対策 4. サイバー犯罪対策 5. サイバーセキュリティの確保

また、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つながり、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 に取り組むことで、大きく成長できる可能性があります。

中小企業が DX 推進における優位な点
参考情報が豊富 DX を既に手掛けている中小企業や、DX を順調に進めている企業のやり方を参考にすることができる

環境が整備されている 先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取り組むことができる
環境の変化に素早く対応しやすい 経営者が即断即決し、新しい取り組み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。自社のデジタル技術の活用を進めつつ、サイバーセキュリティ対策に必要な知識・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 に取り組むことが組織を成長させるために重要であること。

詳細理解のため参考となる文献（参考文献）	
経済財政運営と改革の基本方針 2025	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2025/2025_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/cd4e0324/20250613_policies_priority_outline_03.pdf
Society5.0	https://www8.cao.go.jp/cstp/society5_0
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 2.1	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/dxtebikihontai2.1.pdf

31-4. 第 4 章. サイバーセキュリティ戦略および関連法令

4-1. NCO：サイバーセキュリティ戦略
4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立
4-3. 関連法令

章の目的
第 4 章は、NCO 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

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

4 章の全体概要

４章では、サイバーセキュリティについては、NCO 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。企業はデジタル技術の活用や DX を進めつつ、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。

また、個人情報保護法や GDPR（EU 一般データ保護規則）といったサイバーセキュリティに関連する法令を紹介しています。

4-1. NCO：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り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。

サイバーセキュリティ 2025

サイバーセキュリティ基本法が定める 3 つの政策目的と、サイバーセキュリティ戦略の 3 つの施策推進の方向性に従って整理された「サイバーセキュリティ 2025」について説明しています。

4-2. 企業経営に重要な DX 推進とセキュリティ確保の両立

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

社会経済のデジタル化が進む中、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。

4-3. 関連法令

個人情報保護法

個人情報保護法は、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制定された法律です。消費者や取引先から預かっている個人情報を適切に取扱うことは、企業の権利や利益を守ることにつながる非常に重要な取組となります。

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り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づけ、自発的にサイバーセキュリティ対策に取り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を身につけること（プラス・セキュリティ）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、個人情報はセキュリティレベルの高い情報として適切に取扱うべき情報であること。

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.cyber.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
サイバーセキュリティ 2025	https://www.cyber.go.jp/pdf/policy/kihon-s/250627cs2025.pdf
目的や所属・役割から選ぶ施策一覧	https://security-portal.cyber.go.jp/curriculum/
サイバーセキュリティ関係法令 Q&A ハンドブック Ver2.0	https://security-portal.cyber.go.jp/guidance/pdf/law_handbook/law_handbook_2.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 2.1	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/dxtebikihontai2.1.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.cyber.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

31-5. 第 5 章. 事例を知る：重大なインシデント発生から課題解決まで

5-1. 情報セキュリティの概況
5-2. 重大インシデント事例から学ぶ課題解決
5-3. 実際の被害事例から見るケーススタディー

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

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

5 章の全体概要

5 章では情報セキュリティ白書、情報セキュリティ 10 大脅威、最近のインシデント事例をもとに脅威事例を紹介し、脅威への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。

5-1. 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。

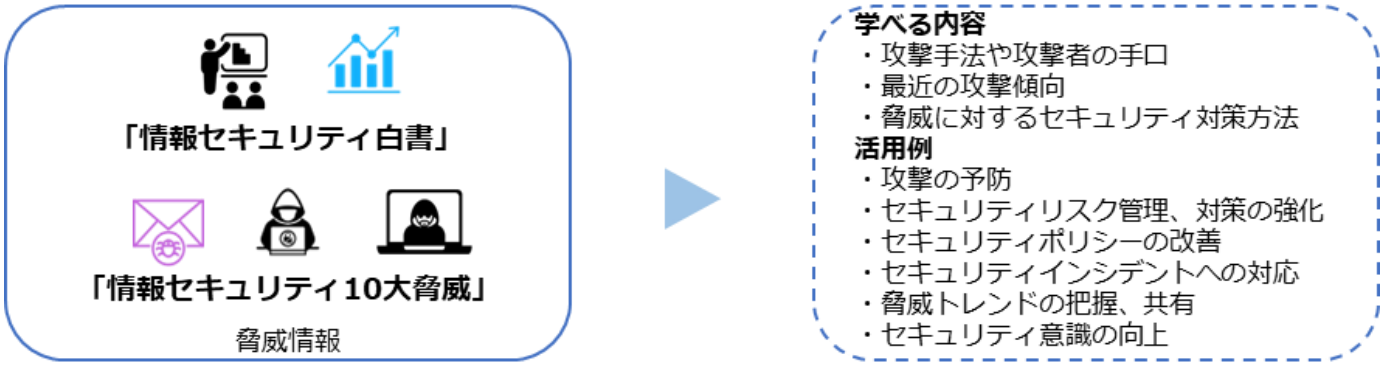


図 105. 情報セキュリティ白書・情報セキュリティ 10 大脅威の活用方法

5-2. 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には事例を学ぶ方法が有効です。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を紹介しているので、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が理解できます。

5-3. 実際の被害事例から見るケーススタディー

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。

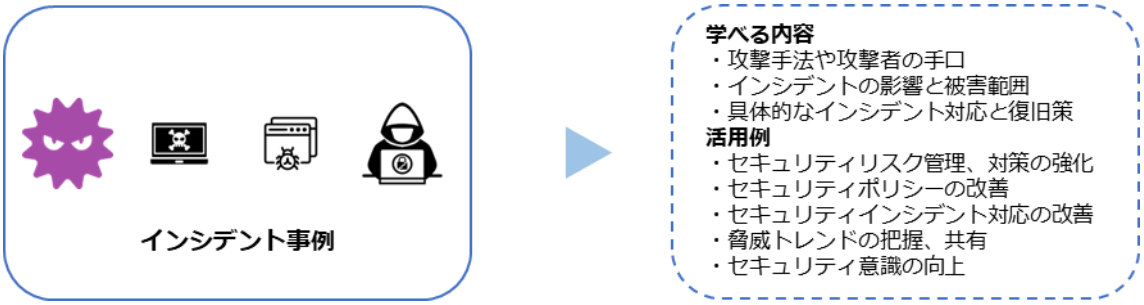


図 106. インシデント事例を通じて学べる内容

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することによって、適切な予防策や対策を講じることが可能になります。また、インシデント事例を学ぶことによってセキュリティ意識を高めることもできます。

認識していただきたい実施概要

- 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によって、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ことができます。
- 過去のインシデント事例から対策方法を学ぶことによって、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、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ことができます。

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 2025	https://www.ipa.go.jp/publish/wp-security/2025.html
情報セキュリティ 10 大脅威 2025	https://www.ipa.go.jp/security/10threats/10threats2025.html

31-6. 第 6 章. 企業経営で重要となる IT 投資と投資としてのサイバーセキュリティ対策

6-1. これからの企業経営で必要な観点：社会の動向
6-2. 守りの IT 投資と攻めの IT 投資
6-3. 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 6 章では、これからの企業経営に必要な観点として、社会の動向、「守りの IT 投資」や「攻めの IT 投資」などの IT 投資について学ぶことを目的とします。また、経営投資としてのセキュリティ対策の重要性を明確にすることを目的とします。
主な達成目標
□ 社会の動向を把握し、現実社会とサイバー空間のつながりを理解すること □ IT 投資としての「守りの IT 投資」と「攻めの IT 投資」を理解すること □ 経営投資としてのセキュリティ対策の重要性を理解すること

主なキーワード
守りの IT 投資、攻めの IT 投資

要旨

6 章の全体概要

6 章では、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」の違いやそれぞれの特徴、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。特に日本企業には「攻めの IT 投資」が不足しており、DX の推進を通じて競争力を強化することが必要だと言われています。

DX 推進と同時に、適切なセキュリティ対策をとる必要があることを鑑み、経営者主体のサイバーセキュリティ対策の必要性とその要点についても解説しています。

6-1.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つながり、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つながり

個人のインターネット利用率は 1997 年の 9.2%から令和 5 年には 86.2%まで上昇し、情報入手やオンラインショッピング、SNS による情報共有が日常化しています。政府は、サイバー空間

とフィジカル空間の融合による新しい社会モデルとして Society5.0 を提唱しており、企業は生産性向上や課題解決のために現実空間とサイバー空間をつなぐ CPS（サイバーフィジカルシステム）や IoT の活用が不可欠となってきています。

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は次の 6 つです。

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. 業務改革等を伴わない 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

6-2. 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。この違いを意識し、「守りの IT 投資」と「攻めの IT 投資」のバランスをとることが大切です。

図 107. 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

自社の将来のあるべき姿（将来のビジョン）の実現に必要な課題を明確にし、その課題を解決する必要がありますが、それに役立つのがデジタル技術の活用です。最近では、生成 AI、IoT、クラウドサービス、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たさまざまな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。6 章ではデジタル技術の活用に成功した企業の例を紹介しています。

6-3. 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り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、経営者がリーダーシップを発揮して対策を進める必要があります。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

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、DX を推進していくことが求められています。しかし、データやデジタル技術を活用する際に、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、DX の推進と並行してサイバーセキュリティの確保に取り組むことが不可欠です。このサイバーセキュリティ対策は、経営者自らが主体となって指揮をする必要があります。

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つながりや、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、取り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り組むことが重要であること。

詳細理解のため参考となる文献（参考文献）	
情報通信白書令和 7 年版（総務省）	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/pdf/00zentai.pdf
DX 動向 2025	https://www.ipa.go.jp/digital/chousa/dx-trend/tbl5kb0000001mn2-att/dx-trend-2025.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.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	https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

31-7. 第 7 章. セキュリティ対策の概要（全容）

7-1. 対策基準の策定

章の目的
第 7 章では、ISMS 認証を前提とした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
◘ 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、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

要旨

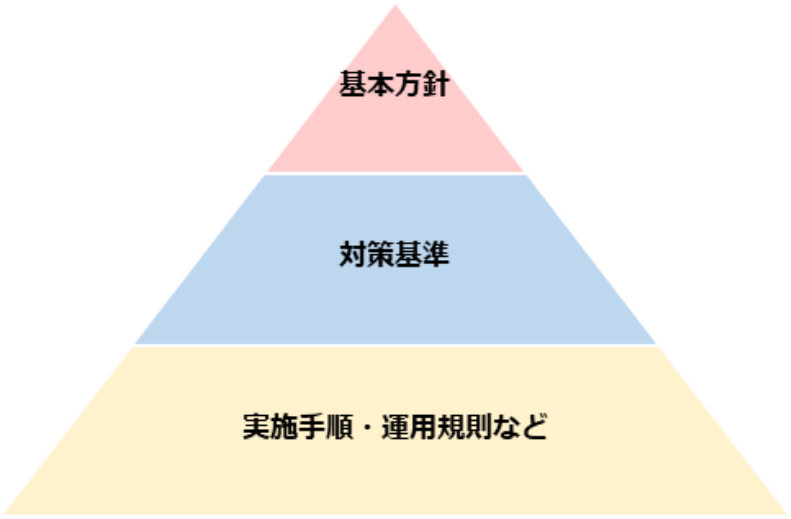
7 章の全体概要

7 章では、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」）と、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）を説明しています。

7-1. 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。



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を記述する。

図 108. 情報セキュリティポリシーの全体像

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	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。 低コスト、短期間で実施可能。包括的ではないが即効性がある。	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して暫定的対策を行う場合。
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型を参考とし、対策基準を策定。 規制遵守の観点から一定の安全性が確保できる。 コストパフォーマンスがよい。	組織的に一定以上の対策基準を策定する場合。 包括的な対策は過剰で、基本的な水準の対策が適切だと判断される場合。
Lv.3 網羅的アプローチ	脅威や攻撃手法に対して、網羅的なセキュリティ対策を講じることを目指すアプローチ手法。 ISMS 認証取得が可能なレベルを目指して、対策基準を策定。 コストが高くなる可能性があるが、組織のニーズに合わせた最適な対策が可能。	ISMS のフレームワークに沿った対策基準を策定する場合。 情報システムが重要な組織や機密性の高い情報を扱う組織など、高い水準の情報セキュリティが求められる場合。

訴求ポイント

章を通した気づき・学び

「基本方針」「対策基準」「実施手順・運用規則など」で構成されるセキュリティポリシーを策定し、セキュリティ対策の実施を内外に示すため、基本方針と対策基準を公開します。同時に、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、セキュリティ対策を実施する必要があります。

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施するために、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「Lv.1 クイックアプローチ」「Lv.2 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「Lv.3 網羅的アプローチ」が推奨されること。

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 2025	https://www.ipa.go.jp/security/10threats/10threats2025.html
サイバー攻撃対応事例	https://security-portal.cyber.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
リスク分析シート	https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-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（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-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/

31-8. 第 8 章. 用語定義および関係性と識別方法

8-1. 用語の定義、脅威・脆弱性の識別

章の目的
第 8 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

主なキーワード
脅威、脆弱性、リスク、セーフガード（管理策）

要旨

8 章の全体概要

８章では、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それらの関係、「脅威」、「脆弱性」の識別方法について説明しています。

8-1. 用語の定義、脅威・脆弱性の識別

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用語の定義や関係性を説明しています。

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

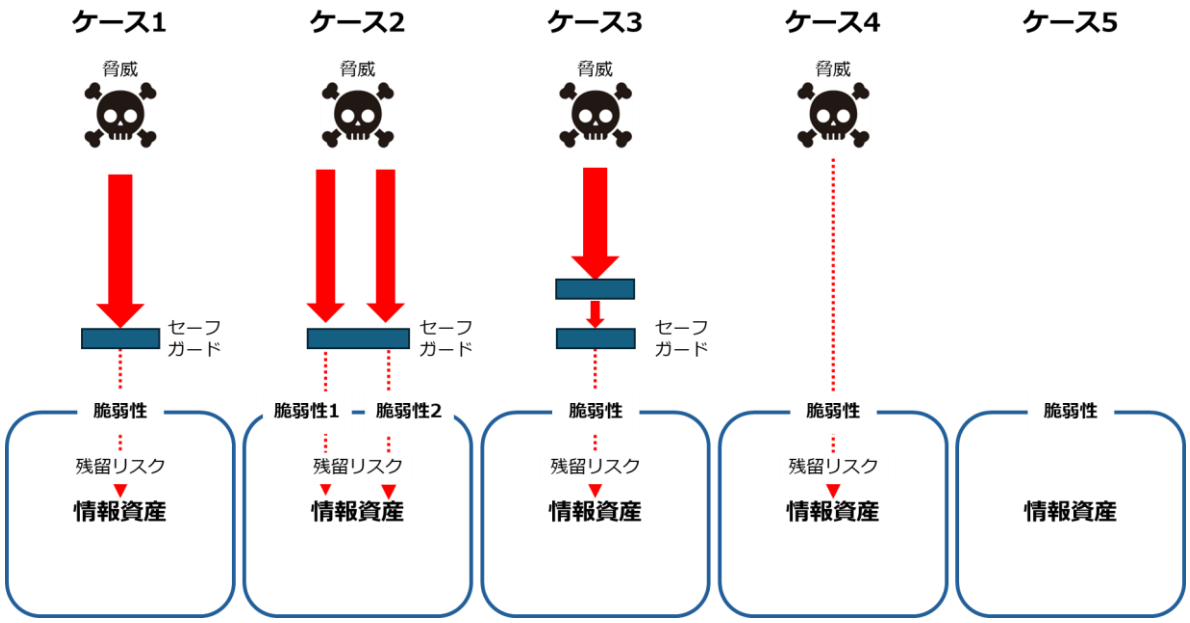


図 109. 脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

（出典）「ISO/IEC TR 13335-1」をもとに作成

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、災害から回復すること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。このような脅威については、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セキュリティ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セキュリティ対策も重要になります。
	偶発的脅威	「入力ミス」がありますが、入力ミスが生じないよう

	(Accidental → A)	に、二回ずつ入力する、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。

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」をもとに作成

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。脆弱性の存在は、管理策の欠如を意味するものでもあるため、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は、サイバーセキュリティ対策の第一歩でもあります。また「脅威」、「脆弱性」の識別方法について理解することは、適切なセキュリティ対策の実施に不可欠です。

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。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC TR 13335-1	https://www.iso.org/standard/39066.html
ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html

31-9. 第 9 章. 具体的手順の作成（Lv.1 クイックアプローチ）

9-1. 【Lv.1 クイックアプローチ】の概要
9-2. 【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

章の目的
第 9 章では、セキュリティインシデント事例を参考にする Lv.1 クイック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
□ Lv.1 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

主なキーワード
Lv.1 クイックアプローチ

要旨

9 章の全体概要

9 章では、Lv.1 クイックアプローチについて説明しています。Lv.1 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基づいて、自社におけるセキュリティインシデントの発生可能性や想定される被害規模を検討し、対策基準や実施手順を策定していく方法です。Lv.1 クイックアプローチは、社会的に影響の大きい事案への対策がとりやすいという特徴があります。

9-1. 【Lv.1 クイックアプローチ】の概要

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。

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。

9-2.【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

Lv.1 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	デメリット
● 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。	● 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。

訴求ポイント

章を通した気づき・学び

Lv.1 クイックアプローチは、リソースが限られていても実施可能で、低コストでリスクを軽減できるコストパフォーマンスのよい方法です。しかし、包括的でないために抜けが発生する、一時的な対応であり抜本的な対策にならない、長期的に見ると費用が嵩んでしまうことがあるというデメリットがあります。

認識していただきたい実施概要
Lv.1 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。

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/sme/f55m8k0000001wd3-att/000055518.xlsx
情報セキュリティ関連規程（サンプル）	https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-att/000055794.docx

31-10. 第 10 章. 具体的手順の作成（Lv. 2 ベースラインアプローチ）

10-1. 【Lv.2 ベースラインアプローチ】の概要
10-2. 【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 10 章では、ガイドラインやひな型などの資料を参考にする Lv.2 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
□ Lv.2 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
Lv.2 ベースラインアプローチ

要旨

10 章の全体概要

10 章では、Lv.2 ベースラインアプローチについて説明しています。Lv.2 ベースラインアプローチは、既存のガイドラインやひな型など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ます。

10-1. 【Lv.2 ベースラインアプローチ】の概要

Lv.2 ベースラインアプローチとは、既存の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。IPA や総務省などが公開しているガイドラインやひな型を参考に、自社の対策基準や実施手順を策定します。

10-2.【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

IPA が公開している「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」「中小企業のためのクラウドサービス安全利用の手引き」「情報セキュリティ関連規程」、NCO による「インターネットの安全・安心ハンドブック Ver.5.10」、総務省の「テレワークセキュリティガイドライン第 5 版」などのガイドラインやひな型を参考にして、自社のための対策基準や実施手順を定めます。

この手法によるメリット、デメリットは以下のとおりです。

メリット	デメリット
● 組織全体で一貫性を確保できる。	● 追加のセキュリティ対策やリスクに対する

● 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。	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型は、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否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

ガイドラインやひな型を活用することで、中小企業でも効率的かつ効果的にセキュリティ対策を実施することが可能となります。

認識していただきたい実施概要
Lv.2 ベースラインアプローチは、ガイドラインやひな型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。

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
インターネットの安全・安心ハンドブック Ver.5.10	https://security-portal.cyber.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
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/sme/f55m8k0000001wcf-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/sme/ps6vr7000001bu8m-att/000055794.docx

31-11. 第 11 章. セキュリティフレームワーク

11-1. セキュリティフレームワークの概要
11-2. 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]
11-3. NIST サイバーセキュリティフレームワーク（CSF）
11-4. 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）
11-5. サイバーセキュリティ経営ガイドライン

章の目的
第 11 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、CSF2.0、CPSF、サイバーセキュリティ経営ガイドライン

要旨

11 章の全体概要

11 章では、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、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。漏れのない対策を効率的に実施するためには、セキュリティフレームワークを活用することが最もよい方法です。

11-1. 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/IEC27001:2022、ISO/IEC 27002:2022
- ISO/IEC 27017:2015
- サイバーセキュリティフレームワーク（CSF）2.0
- 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）Ver.1.0

- サイバーセキュリティ経営ガイドライン Ver3.0
- 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）v4.0.1
- 個人情報保護マネジメントシステム（PMS）JIS Q 15001:2023 準拠 ver1.0
- CIS Controls version 8.1
- ISAIEC 62443

11-2. 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]

ISMS は、情報セキュリティ管理の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。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。

11-3. NIST サイバーセキュリティフレームワーク（CSF）

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、防御に留まらず、検知・対応・復旧といったインシデント対応を含んでいます。CSF2.0 は、中小企業を含むあらゆる組織で利用されるよう設計されています。CSF2.0 は ISMS を補完し、組織のセキュリティ対策を強化するための有用なツールとなるので、ISMS をベースにして、必要に応じて CSF を取り込むとよいでしょう。

11-4. 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）

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。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。

11-5. 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、経済産業省と IPA が共同で発行しているガイドラインで、企業がサイバーセキュリティを効果的に経営に取り入れるための指針を提供します。経営者が認識するべき 3 原則、サイバーセキュリティ経営の重要 10 項目など内容を含んでおり、経営者、情報セキュリティ対策の責任者（CISO など）の立場から、セキュリティ対策を実践する際の役割、認識するべきことがまとめられています。このガイドラインは、企業がサイバーセキュリティを経営の一部として位置づけ、組織全体でセキュリティ意識を高めるための基盤として活用できます。

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。

詳細理解のため参考となる文献（参考文献）	
ISMS-AC ISMS 適合性評価制度	https://isms.jp/doc/JIP-ISMS120-62.pdf
The NIST Cybersecurity Framework (CSF) 2.0	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.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（CPSF）の概要	https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.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/policy/netsecurity/downloadfiles/guide_v3.0.pdf

31-12. 第 12 章. リスクマネジメント

12-1. リスクマネジメント：概要
12-2. リスクマネジメント：リスクアセスメント
12-3. リスクマネジメント：リスク対応

章の目的
第 12 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

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

12 章の全体概要

12 章では、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不可欠な要素です。リスクは、顕在化していないものについても検討する必要があります。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。

12-1. 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」といいます。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ものが、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。

12-2. リスクマネジメント：リスクアセスメント

12-3. 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否か判断します。リスクの特定には、「資産ベースのアプローチ」と「事象ベースのアプローチ」の 2 つの方法があります。情報資産ごとに、その重要度を「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から決め、重要度と被害発生の可能性からリスクレベルを求めます。このリスク評価の結果をもとに、受容可能でないものについては、「低減」、「移転」、「回避」、「受容（保有）」からリスク対応を選択します。すべての残留リスクが受容できるレベルになるまで、このリスク評価のプロセスを繰り返します。

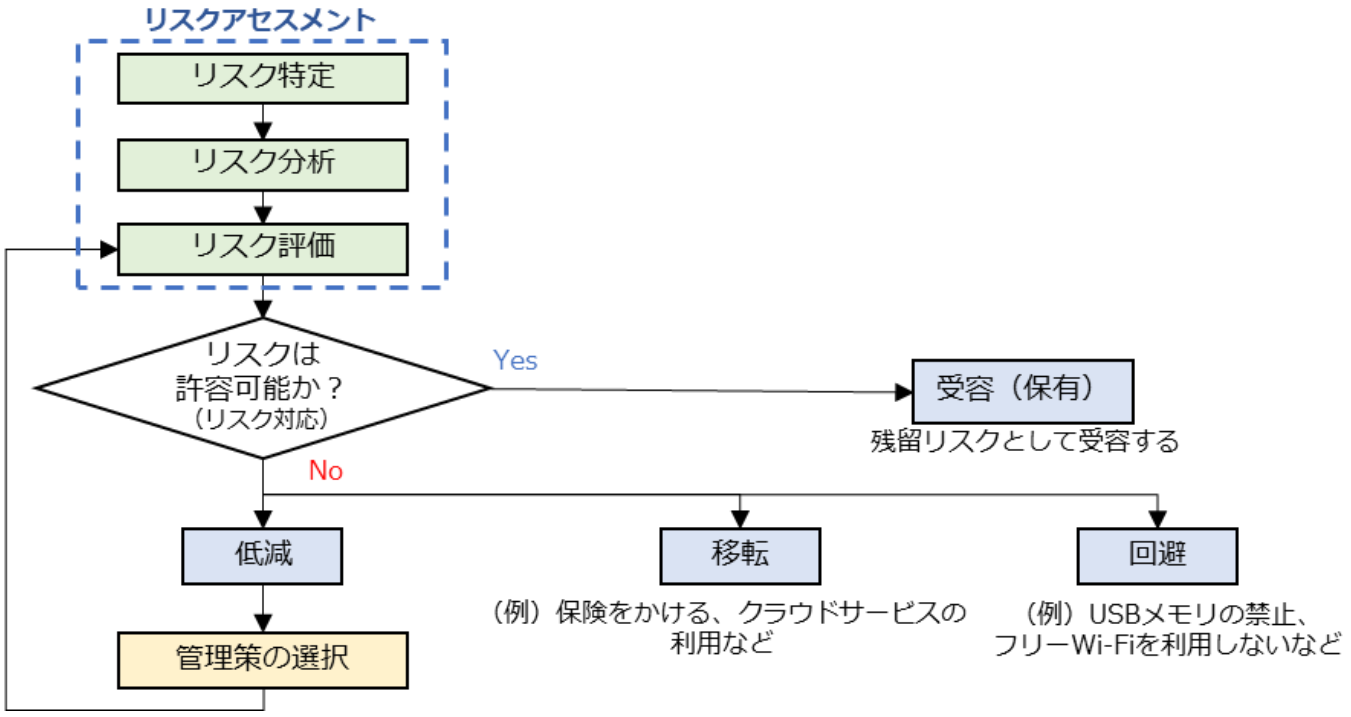


図 110. リスクマネジメント全体の流れと、リスク対応の選択プロセス

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が、「資産ベースのアプローチ」によって網羅的にリスクを特定するようにしましょう。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、分析と対応策の選択と実施が可能になります。このプロセスによってすべてのリスクをコントロールし、残留リスクを受容可能なレベルにすることができます。

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。

詳細理解のため参考となる文献（参考文献）	
ISO/IEC 27005:2022	https://www.iso.org/standard/80585.html
リスクアセスメントとリスク対応	https://www.jnsa.org/ikusei/01/02-04.html

31-13. 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
13-3. ISMS 文書体系（ISMS 構築・導入に必要な文書と記録）
13-4. ISO/IEC27001 の審査準備と審査内容

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 Lv.3 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
□ Lv.3 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
Lv.3 網羅的アプローチ、PDCA サイクル

要旨

13 章の全体概要

13 章では、情報セキュリティマネジメントシステム（ISMS）を構築するための Lv.3 網羅的アプローチについて説明しています。Lv.3 網羅的アプローチは、ISMS のフレームワークに従い、組織全体で適用できるセキュリティ対策基準と手順を整備する方法です。ISMS の運用では PDCA サイクルを用い、計画・実行・評価・改善のプロセスを通じて継続的に改善を実施します。ISO/IEC 27001 の要求事項に基づき、ISMS に関する文書作成が求められますが、重要なのはセキュリティ対策の策定と実施なので、文書の作成が目的にならないよう注意が必要です。

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

Lv.3 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ます。

Lv.3 網羅的アプローチのメリットは、ISMS 要求事項の導入によって組織のセキュリティレベルが大幅に向上することです。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 に取り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。

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になります。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。

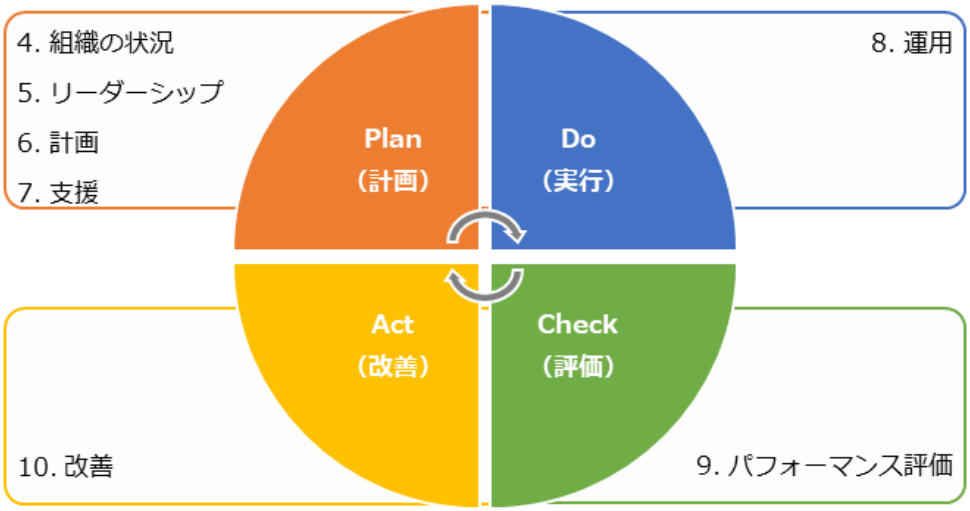


図 111. ISMS の PDCA サイクル

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
従業員の教育など、ISMS 構築にあたり組織が従業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。

13-3. ISMS 文書体系（ISMS 構築・導入に必要な文書と記録）

ISMS（情報セキュリティマネジメントシステム）の構築や導入に必要な文書と記録の重要性を説明しています。ISMS 文書は、組織内で情報セキュリティの有効な管理を実施するための基本的な要素として、対策や手続きが記載されています。

ISMS 文書体系には、以下のポイントが含まれます:

- **文書の策定内容とその要点:**
  対策基準や実施手順が明確に示され、実施状況の確認が可能。
- **管理策:**
  ISO/IEC 27001 の要求事項に基づいた文書作成が推奨され、組織全体でのセキュリティ向上を支援します。

13-4. ISO/IEC27001 の審査準備と審査内容

ISO/IEC 27001 認証取得に向けた審査準備や審査の具体的内容について説明しています。主要な内容は以下の通りです。

- **認証機関の選定と申し込み**:
  認証機関は、ISMS-AC（情報マネジメントシステム認定センター）から認定された組織である必要があり、申請には書類や登録料が異なることを事前に確認します。
- **審査事前準備**:
  ISMS 構築のステップを踏まえて、審査対象の範囲や実施手順の文書化が求められます。
- **第一段階・第二段階審査**:
  1 次審査は文書レビュー、2 次審査は現地での実施状況確認が行われ、適合が確認されると認証書が発行されます。
- **維持審査・再認証審査**:
  年 1 回以上の維持審査と、3 年ごとの再認証審査で、ISMS の有効性が評価されます。

訴求ポイント

章を通した気づき・学び

ISMS を用いる Lv.3 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策

定・実施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。

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
ISMS 適合性評価制度	https://isms.jp/isms.html

31-14. 第 14 章. ISMS の管理策

14-1. 管理策の分類と構成

章の目的
第 14 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

主なキーワード
管理策、ISO/IEC 27002

要旨

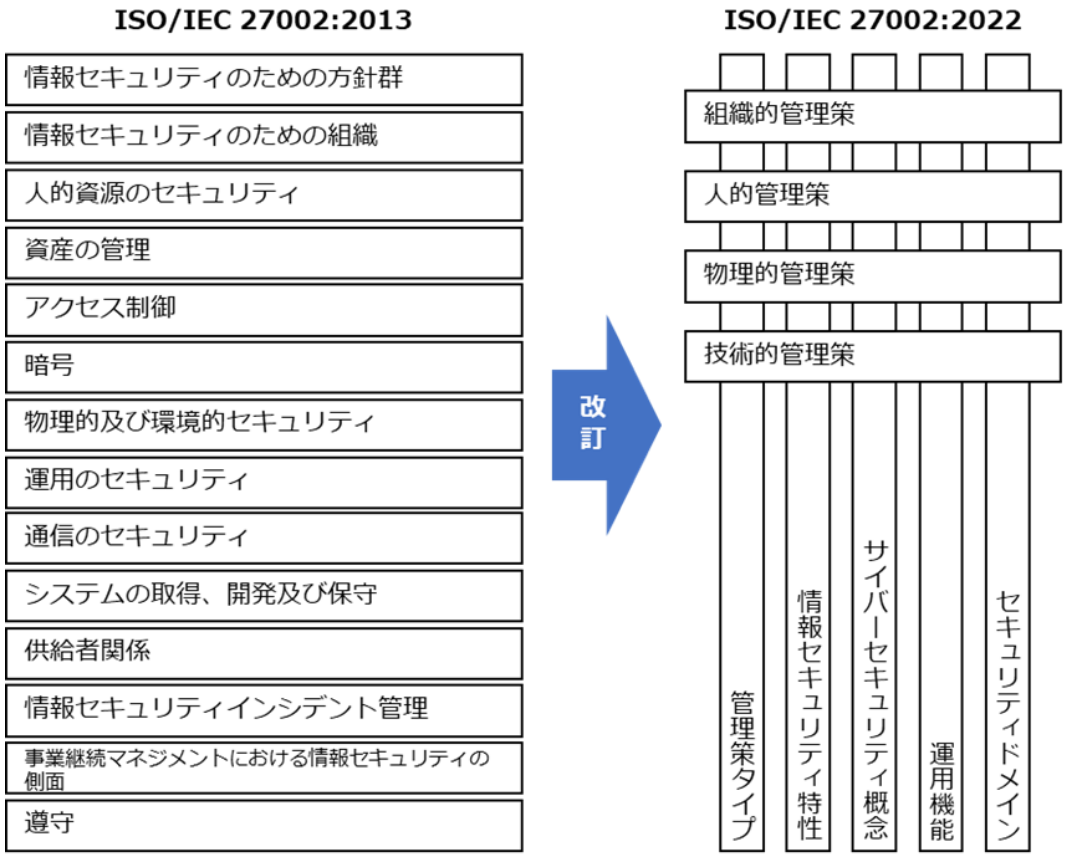
14 章の全体概要

14 章では、ISO/IEC 27002 に基づく ISMS の管理策について説明しています。企業は、組織的・人的・物理的・技術的な 4 つのカテゴリに分類された 93 項目の管理策から、自社のリスクに応じた適切な管理策を選び、対策基準として導入する必要があります。また、各管理策には目的と属性が追加され、リスクの予防・検知・是正などの観点から策定が求められます。2022 年版の改訂により、管理策の項目数と内容が見直され、組織に適した情報セキュリティ対策の選定と実施が重要視されています。

14-1. 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。



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見るためのものです。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 112. ISO/IEC 27002:2022 の概要

また、情報セキュリティのために必要な管理策を適用宣言書として選定し、対策基準を作成し、その後に実施手順を策定する方法を説明しています。

- **管理策の決定**:
  リスクアセスメントの結果を考慮し、適切なリスク対応策を選び出し、ISO/IEC 27001 の附属書 A から適切な管理策を決定します。
- **管理策の検証**:
  決定した管理策が適切であり、見落としがないか ISO/IEC 27001 に基づき検証します。
- **適用宣言書の作成**:
  組織が実施する管理策を文書化した適用宣言書を作成し、必要な管理策とその理由を記載します。
- **実施手順の作成**:
  管理策をもとに組織内部での具体的な実施手順を作成します。従業員が理解しやすいように、わかりやすい言葉で明確に策定することが重要です。

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し、対策基準として導入することになります。

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。

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

31-15. 第 15 章. 組織的対策

15-1. 作成する候補となる実施手順書類について

15-2. 組織的対策として重要となる実施項目

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
◘ 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

15 章の全体概要

15 章では、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、その実施手順について説明しています。対策基準は、ISO/IEC 27001:2022 附属書 A の合計 93 項目の管理策を参考に策定します。実施手順は ISO/IEC 27002 に記載されている各管理策の手引きを参考に策定することができます。15 章では「組織的管理策」を例にして、対策基準を策定する手順と、それぞれの対策基準に対応する実施手順の例を説明しています。

15-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に記載された 93 項目の管理策を参考に、必要な管理策を選択して対策基準を策定し、実施手順を作成する方法を説明しています。これにより、組織がリスクアセスメントの結果に基づいて適切な管理策を選び、その基準に従って具体的な手順書を内部文書として作成することが奨励されます。

15-2. 組織的対策として重要となる実施項目

組織が情報セキュリティを強化するために必要な取組について具体的に説明しています。これには、組織全体での情報管理の体系化、サイバーセキュリティ対策の適切な実施、個人情報の保護が含まれています。また、外部および内部の脅威情報を収集し、セキュリティ対策に役立てる「脅威インテリジェンス」の導入が推奨され、重要な情報資産を特定して管理するための情報資

産管理台帳の作成と更新も重要視されています。

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できます。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実行に移す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。

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

31-16. 第 16 章. 人的対策

16-1. 作成する候補となる実施手順書類について

16-2. 人的対策として重要となる実施項目

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
◘ 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

16 章の全体概要

16 章では、情報セキュリティ方針に従い、人的対策を中心にセキュリティ対策基準を策定するための方法について説明しています。まず、リスクアセスメントの結果をもとに適切な管理策を選定し、それを実施手順として組織の内部文書にまとめます。この際、ISO/IEC 27001 の規定に基づいて選定するだけでなく、独自の追加管理策も含めることが推奨されます。具体的な項目としては、雇用契約、守秘義務、リモートワーク手順、懲戒手続などが含まれ、従業員の行動指針として重要な役割を果たします。

16-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に示された 93 項目の管理策を参考に、情報セキュリティにおける実施手順書を策定する方法が説明しています。実施手順書は、リスクアセスメントをもとに選定された管理策を対策基準として採用し、具体的な手順を文書化するための候補を提示します。これにより、組織が適切な管理策を選定し、それをもとに対策基準と具体的な実施手順を策定することが可能になります。

16-2. 人的対策として重要となる実施項目

組織における人的管理策の重要実施項目として、従業員の採用から退職後までのセキュリティ

対策を紹介しています。具体的には、情報セキュリティの観点から従業員の選考、雇用契約の内容、セキュリティ教育、守秘義務の遵守などの具体的な項目を取り上げています。懲戒手続や雇用終了後のセキュリティ対策の責任、リモートワーク実施時のセキュリティや情報セキュリティイベントの報告手順に関しても指針を示しています。

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 雇用の終了又は変更後の責任 6.6 秘密保持契約又は守秘義務契約 6.7 リモートワーク 6.8 情報セキュリティ事象の報告

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002 の内容を参考にしつつ、雇用契約、守秘義務、リモートワーク手順、懲戒手続など自社に適した管理策を追加して、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。

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実行に移す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。

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

31-17. 第 17 章. 物理的対策

17-1. 作成する候補となる実施手順書類について

17-2. 物理的対策として重要となる実施項目

17-3. BYOD、MDM

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。
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（Bring Your Own Device）、MDM（Mobile Device Management）

要旨

17 章の全体概要

17 章では、情報セキュリティのために物理的な保護措置を定義する方法について説明しています。まず、組織のレイアウト図を用いて物理的なセキュリティ境界を明確にし、重要な情報資産があるエリアを保護する必要があります。入退室の管理には、従業員証やセキュリティカードを用い、外来者の訪問については記録とエスコートが求められます。さらに、オフィスや施設のセキュリティを高めるために、施錠や外部からの視線を遮る対策も必要です。施設内では監視カメラや侵入者警報を活用し、無人領域にも監視システムを設置してセキュリティを維持します。また、災害や物理的な脅威への対策として、消火器や火災報知器の設置、サーバの転倒防止措置、情報漏えい防止のためのクリアデスク・クリアスクリーンについても解説しています。

17-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 附属書 A に基づき、物理的セキュリティ対策のための手順書を策定する方法を説明しています。具体的には、リスクアセスメント結果をもとに適切な管理策を選択し、対策基準を策定するプロセスを示しています。これにより、組織が必要とする物理的な安全対策を標準化し、実施手順を整えることができます。

17-2. 物理的対策として重要となる実施項目

組織の物理的セキュリティを強化するための重要な実施項目を紹介しています。具体的には、以下のポイントが挙げられます。

物理的管理策の項目	
7.1 物理的セキュリティ境界 7.2 物理的入退 7.3 オフィス、部屋及び施設のセキュリティ 7.4 物理的セキュリティの監視 7.5 物理的及び環境的脅威からの保護 7.6 セキュリティを保つべき領域での作業 7.7 クリアデスク・クリアスクリーン	7.8 装置の設置及び保護 7.9 構外にある資産のセキュリティ 7.10 記憶媒体 7.11 サポートユーティリティ 7.12 ケーブル配線のセキュリティ 7.13 装置の保守 7.14 装置のセキュリティを保った処分又は再利用

17-3. BYOD、MDM

- **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 の内容を参考にして、自社に適した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。

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実行に移す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。

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

31-18. 第 18 章. 技術的対策

章の目的
第 18 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

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

18 章の全体概要

18 章では、情報セキュリティを実現するための具体的な技術的対策を解説しています。まず、ISO/IEC 27001:2022 に基づき、リスクアセスメント結果に基づく技術的管理策を策定することが必要です。管理策には、エンドポイントデバイスの保護、特権アクセス権の管理、アクセス制限の確立、安全な認証技術の導入が含まれます。また、マルウェア対策や技術的脆弱性の管理、バックアップと冗長化の設定も重要な要素として挙げられます。さらに、ゼロトラストや SASE などのセキュリティアーキテクチャを取り入れ、インシデント対応を強化することが望まれます。

18-1. 作成する候補となる実施手順書類について

ISO/IEC 27001:2022 の附属書 A に基づいて、技術的管理策を用いた対策基準を策定し、その具体的な実施手順を文書化するプロセスを説明しています。リスクアセスメント結果をもとに必要な技術的管理策を選定し、実施手順書を作成することで、組織が情報セキュリティの技術的側面を強化する手段が提供されます。このプロセスにより、情報の安全な取り扱いやアクセス制御、エンドポイント保護、ネットワーク管理などを含む多様な技術的対策を体系的に導入できます。

18-2. 技術的対策として重要となる実施項目

情報セキュリティを確保するために組織が実施すべき技術的管理策を紹介しています。

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 技術的ぜい弱性の管理	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成の原則
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	

18-3. 実施手順を適用するセキュリティ概念

この節では、組織が情報セキュリティ対策を実施する際に適用すべきセキュリティ概念を紹介しています。具体的には、以下の 5 つの主要な概念を取り上げています。

- **Security by Design:**
  設計段階からセキュリティを組み込む手法で、開発ライフサイクル全体にわたり、潜在的な脆弱性を排除し、堅牢なシステムを構築することを目指します。
- **ゼロトラストモデル:**
  伝統的な境界防御モデルに代わり、常に疑いを持ち、認証を通じてアクセスを制御するアプローチです。ユーザーやデバイスの信頼を前提とせず、厳密なアクセス管理を行います。
- **SASE (Secure Access Service Edge):**
  ネットワークとセキュリティ機能を統合し、クラウドサービスを活用して分散された業務環境に適応するセキュリティモデルです。
- **ネットワーク制御 (Network as a Service):**
  ネットワーク機能をサービスとして提供し、セキュリティ管理を効率化する取り組みです。
- **セキュリティ統制 (Security as a Service):**
  セキュリティ機能をクラウドサービスとして提供し、柔軟な運用を実現します。

18-4. インシデント対応

この節では、情報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手順を解説しています。インシデント対応は、「検知・初動対応」「報告・公表」「復旧・再発防止」の 3 つのステップで構成されます。初動対応では、インシデントを素早く把握し、影響を抑えるための即時対応が求められます。報告・公表の段階では、必要に応じて関係者や関連当局への報告を行います。復旧・再発防止の段階では、影響の調査と是正措置を通じて被害を最小限に抑え、将来的なインシデントを防止するための改善を実施します。

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。特に、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、インシデント対応などに関するセキュリティ関連技術の動向を把握し、必要な技術的管理策を採用することが重要です。

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実行に移す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。

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

31-19. 第 19 章. セキュリティ対策状況の有効性評価

19-1. 内部監査

19-2. 外部監査

章の目的
第 19 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

19 章の全体概要

19 章では、セキュリティ対策の効果を確認するための監査について説明しています。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。最初は、内部監査により組織内のルールや手順が適切に守られているかを確認し、運用に慣れたら、その有効性について評価します。次に、外部監査を通じて第三者による客観的な視点から評価し、改善点を見つけることが推奨されます。内部と外部の監査を組み合わせることで、ルールの形骸化を防ぎ、目的達成に向けた対策が継続的に改善されるよう努めます。

19-1. 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、遵守できてい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否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。

19-2. 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否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を評価するため、定期的に内部監査・外部監査を実施することが必要です。

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つながること。 ● 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否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つながること。

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

31-20. 第 20 章. セキュリティ機能の実装と運用（IT 環境構築・運用実施手順）

20-1. セキュリティ機能の実装と運用

20-2. アジャイル開発

章の目的
第 20 章では、「デジタル・ガバメント推進標準ガイドライン」などが示すサービスシステム構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を理解することを目的とします。
主な達成目標
◘ 中小企業においても有効なシステム導入工程と、実践にあたっての留意点を理解すること ◘ システム導入工程に沿って、セキュリティ機能を実装・運用するためポイントを理解すること ◘ アジャイル開発の概要と実践ポイントを理解すること

主なキーワード

デジタル・ガバメント推進標準ガイドライン、アジャイル開発

要旨

20 章の全体概要

20 章では、「デジタル・ガバメント推進標準ガイドライン」などに記載されている政府情報システムの構築と運用の工程を参考に、中小企業においても適用することが有効な工程と、実践にあたっての留意点を説明しています。

また、アジャイル開発の概要と実践ポイントを解説しています。

20-1. セキュリティ機能の実装と運用

「デジタル・ガバメント推進標準ガイドライン」などを参考に、中小企業においても適用することが有効な工程や、セキュリティ機能を実装・運用するためポイントなどを説明しています。

中小企業においても適用することが有効な工程の例として、Fit&Gap 分析が挙げられます。情報システム構築においてパッケージソフトウェアや SaaS を利用する場合は、導入するパッケージソフトウェアや SaaS などのシステムと、自社の業務要件との適合性を評価する Fit&Gap 分析が重要になります。

20-2. アジャイル開発

アジャイル開発の必要性、概要、実践ポイントを説明しています。

アジャイル開発は、「敏捷」「素早い」といった意味を持ち、新しい機能を短期間で継続的にリリースする開発手法です。この手法は、変化の激しい現代のビジネス環境に適応し、柔軟かつ試行錯誤を許容するアプローチとして有用です。従来の開発手法が試行錯誤に不向きであるのに対し、アジャイル開発は反復的なフィードバックに基づき改善を重ねることで、最適なシステムを目指します。

訴求ポイント

章を通した気づき・学び

「デジタル社会推進標準ガイドライン群」は、政府情報システムの共通ルールを定めたものですが、システム導入の流れ自体は、一般企業であっても参考になります。ガイドラインを通してシステム導入の全体像を認識し、ガイドラインを実践する際は必要に応じてルールを取捨選択する必要があります。

認識していただきたい実施概要
● 「デジタル・ガバメント推進標準ガイドライン」を参考に、中小企業にも適用可能なシステム導入工程や実践時の留意点を理解すること。 ● 情報システムの構築と運用の各工程（プロジェクト管理、要件定義、設計・開発、運用など）でセキュリティ機能を実装すること。 ● アジャイル開発の重要性を理解すること。

詳細理解のため参考となる文献（参考文献）	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf
DS-110 デジタル・ガバメント推進標準ガイドライン解説書	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/573c839f/20250619_resources_standard_guidelines_guideline_03.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ae9a37b7/20250619_resources_standard_guidelines_guideline_05.pdf
アジャイル領域へのスキル変革の指針　アジャイル開発の進め方	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

31-21. 第 21 章. 人的、組織的、技術的、物理的対策の実施手順に基づいた実施

21-1. EC サイトの構築とセキュリティ機能の実装と運用

章の目的
第 21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントを説明します。EC サイトを例にとり、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を理解することを目的とします。
主な達成目標
◘ 実施例から工程を理解することで、中小企業が主体的に関与するポイントを理解すること ◘ 情報システムを導入する工程で、作成すべきドキュメントを理解すること ◘ 情報システムを導入する工程の中で、セキュリティ機能を実装、運用するポイントを理解すること

主なキーワード

BCP（事業継続計画）、CSIRT（Computer Security Incident Response Team）、セキュリティ監査、セキュリティ管理

要旨

21 章の全体概要

21 章では、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で情報システムを導入する流れと、セキュリティ対策の実装と運用ポイントについて、EC サイトを例にとって説明しています。

21-1. EC サイトの構築とセキュリティ機能の実装と運用

EC サイトを例にとり、「デジタル・ガバメント推進標準ガイドライン」に準拠した手順で、企画から要件定義、調達、設計・開発、運用保守までの流れと、セキュリティ機能の実装方法を解説しています。

非機能要件のうちセキュリティに関する要件は、リスクアセスメントを実施して作成した適用宣言書をもとに決定します。

SaaS やパッケージソフトウェアを導入する際に非常に重要なプロセスである Fit&Gap 分析については、具体例を含めて解説しています。

訴求ポイント

章を通した気づき・学び

「デジタル・ガバメント推進標準ガイドライン」は、中小企業でも活用できる重要なことが数多く記載されています。情報システムを導入する際は、本ガイドラインを参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能です。

要件定義におけるセキュリティ要件は、組織で作成した適用宣言書をもとに決定することが重要です。情報資産におけるリスクを考慮して適切なセキュリティ要件を決めることで、情報システムのセキュリティ対策を強化することができます。

認識していただきたい実施概要
● 情報システムを導入する際は、「デジタル・ガバメント推進標準ガイドライン」を参考に、セキュリティ機能を実装すること。 ● 要件定義では、適用宣言書をもとに情報資産におけるリスクを考慮し、適切なセキュリティ要件を決めること。

詳細理解のため参考となる文献（参考文献）	
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ae9a37b7/20250619_resources_standard_guidelines_guideline_05.pdf
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

31-22. 第 22 章. サイバーセキュリティ対策を実践するための知識とスキル

22-1. デジタルスキル標準（DSS）
22-2. IT スキル標準（ITSS）
22-3. ITSS+（プラス）
22-4. i コンピテンシ ディクショナリ（iCD）

章の目的
技術進歩に伴い次々と新しい脅威が生まれている中で、効果的で漏れのないセキュリティ対策を実践していくためには、IT 全般のスキルや知識を持つ人材の育成と確保が重要です。第 22 章では、各種スキル標準のフレームワークをもとに、必要とされる新しいスキルや知識について、体系的に理解することを目的とします。
主な達成目標
◘ 具体的な実施のために必要となる「役割やタスク」「スキルや知識」について、人材育成・人材確保のための各種スキル標準のフレームワークをもとに体系的に理解すること ◘ 各種スキル標準のフレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること ◘ スキルや知識の認定制度と活用方法を理解すること

主なキーワード
デジタルスキル標準、DX リテラシー標準、IT スキル標準、ITSS+（プラス）、i コンピテンシ ディクショナリ

要旨

22 章の全体概要

22 章では、サイバーセキュリティ対策を実践するために必要な知識とスキルについて解説しています。必要な知識とスキルを体系的に理解するために有用なフレームワークとして、デジタルスキル標準（DSS）や IT スキル標準（ITSS）、ITSS+（プラス）、i コンピテンシ ディクショナリなどについて解説しています。

22-1. デジタルスキル標準（DSS）

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 つの標準で構成されます。

「DX リテラシー標準」は、すべてのビジネスパーソンが身につけるべき DX に関する基礎的な知識、スキル、マインドセットの学習指針です。企業は、従業員に対して、DX に関するリテラシーを身につけさせるための指針として活用できます。

「DX 推進スキル標準」は、DX を推進する人材の役割（ロール）および必要なスキルを定義しています。

22-2. IT スキル標準（ITSS）

IT スキル標準（ITSS）は、IT 分野で必要とされるスキルや知識を体系化し、評価するための指標です。経済産業省が 2002 年に策定し、現在は IPA が管理しています。ITSS は、IT 人材の育成に寄与することを目的としており、企業が共通して使用できるスキル指標を提供することで、キャリアパスの明確化やスキルの標準化に役立っています。

22-3. ITSS＋（プラス）

ITSS+は、従来の IT スキル標準（ITSS）を拡張し、第 4 次産業革命に向けて求められる新たな領域の新しいスキルをカバーするために策定されました。対象となっている領域は、「データサイエンス領域」「アジャイル領域」「IoT ソリューション領域」「セキュリティ領域」の 4 つの領域です。

22-4. i コンピテンシ ディクショナリ（iCD）

i コンピテンシ ディクショナリ（iCD）は、組織において IT を利活用するビジネスに求められる業務（タスク）と、それを支える IT 人材の能力や素養（スキル）を「タスクディクショナリ」、「スキルディクショナリ」として体系化したものです。

※i コンピテンシ ディクショナリ（iCD）において、重要なことは考え方です。タスクやスキルについては、デジタルスキル標準を参照することが大切です。

訴求ポイント

章を通した気づき・学び

効果的なセキュリティ対策を実践するためには、IT 全般のスキルや知識を持つ人材の育成と確保が必要です。そのためには、各種スキル標準のフレームワークを活用することが有効です。

認識していただきたい実施概要

- デジタルスキル標準や IT スキル標準など各種フレームワークをもとに、サイバーセキュリティ対策を実践するために必要なスキルや知識について体系的に理解すること。
- 各種スキル標準のフレームワークを活用し、効果的なセキュリティ対策を実践するために必要な IT 全般の知識やスキルを持つ人材を育成・確保すること。

詳細理解のため参考となる文献（参考文献）	
デジタルスキル標準 ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
IT スキル標準 V3 2011 1 部：概要編	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf
ITSS+（プラス）概要	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html
i コンピテンシディクショナリ解説書	https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf

31-23. 第 23 章. 人材の知識とスキルの認定制度

23-1. Di-Lite
23-2. 情報処理技術者試験
23-3. 国際セキュリティ資格

章の目的
第 23 章では、IT およびデジタル人材のスキル、知識の認定制度と活用方法を理解することを目的とします。認定制度は、従業員一人一人に 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なります。
主な達成目標
□ スキルや知識の認定制度と活用方法を理解すること

主なキーワード
Di-Lite、情報処理技術者試験、国際セキュリティ資格

要旨

23 章の全体概要

23 章では、IT およびデジタル人材の知識とスキルを認定する制度の意義と活用方法について解説しています。デジタルリテラシー協議会が提供する「Di-Lite」、情報処理技術者試験や国際セキュリティ資格について解説しています。認定制度は、従業員に 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なります。

23-1. Di-Lite

「Di-Lite」とは、デジタルリテラシー協議会が定義する、すべてのビジネスパーソンが持つべきデジタル時代の共通リテラシーのことです。具体的には、以下の 3 つの領域に関するスキルや知識を指します。

1.IT・ソフトウェア領域：基本的な IT スキルやソフトウェアの使用方法
2.数理・データサイエンス領域：データ分析や統計の基礎知識
3.人工知能（AI）・ディープラーニング領域：AI 技術やディープラーニングの基礎知識

これらのスキルを身につけることで、デジタル時代におけるビジネスの効率化や競争力の向上が期待されています。

23-2. 情報処理技術者試験

情報処理技術者試験は、IT 分野の基礎から専門知識までをカバーする国家試験で、IPA が運用しています。情報処理技術者試験の受験は、従業員一人一人に 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になります。

情報処理技術者試験は、初級から高度な IT スキルを持つ人材に対応しており、IT パスポート、基本情報技術者、応用情報技術者、そして情報処理安全確保支援士試験などの区分があります。

組織全体で従業員一人一人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、組織内のセキュリティ専門人材不足の問題の解消にも役立ちます。

23-3. 国際セキュリティ資格

情報セキュリティ分野における国際的な資格（CISSP や CISM、CISA）について説明しています。各情報処理技術者試験で培った IT 知識は、国際セキュリティ資格の学習の基礎となります。また、相乗効果の観点から国際セキュリティ資格の学習を通じて、各情報処理技術者試験の知識を深められたり、より高度な IT ポジションへのキャリアアップが期待できたりします。

訴求ポイント

章を通した気づき・学び

従業員一人一人に IT や情報セキュリティの知識を身につけてもらうためには、IT およびデジタル人材のスキル、知識の認定制度の活用が有効です。

認識していただきたい実施概要
● IT およびデジタル人材のスキルと知識の認定制度を理解すること。 ● 情報処理技術者試験や国際資格など IT およびデジタル人材のスキル、知識の認定制度を活用し、人材育成に取り組むこと。

詳細理解のため参考となる文献（参考文献）	
Di-Lite	https://www.dilite.jp/
情報処理技術者試験 情報処理安全確保支援士 試験要綱	https://www.ipa.go.jp/shiken/syllabus/nl10bi0000007smr-att/youkou_ver5_4.pdf
CISSP 8 ドメインガイドブック	https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf
ISACA 東京支部	https://www.isaca.gr.jp

31-24. 第 24 章. 各種人材育成カリキュラム

24-1. プラス・セキュリティ知識補充講座 カリキュラム例
24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1）】
24-3. マナビ DX

章の目的
第 24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を把握することを目的とします。紹介するカリキュラム内容は、具体的な実施計画や実施内容を検討する際の参考資料となります。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」のカリキュラム内容を理解すること ◘ 「IT スキル標準モデルカリキュラム」のカリキュラム内容を理解すること ◘ デジタルスキル習得に関する講座を紹介する「マナビ DX」について概要と活用方法を理解すること

主なキーワード
プラス・セキュリティ知識補充講座、IT スキル標準モデルカリキュラム、マナビ DX、デジタルスキル標準

要旨

24 章の全体概要

24 章では、知識やスキルを備えた人材の育成・確保に向けて、関係機関が公表しているセキュリティ関連のカリキュラム内容を解説しています。取り上げたものは、「プラス・セキュリティ知識補充講座 カリキュラム例」、「IT スキル標準モデルカリキュラム IT スキル標準 V3（レベル 1）」、デジタルスキル習得を支援する「マナビ DX」などです。

24-1. プラス・セキュリティ知識補充講座 カリキュラム例

「プラス・セキュリティ知識補充講座」は、国家サイバー統括室（NCO）が提供するプログラムで、特に経営層や DX を推進する部課長向けに設計されています。この講座は、企業内外のセキュリティ専門人材との協働を円滑に行うために必要な知識を補充することを目的としています。

具体的には、以下のように経営層向けとデジタル化推進部門の部課長級マネジメント層向けの2つのカリキュラムで構成されています。

24-2. IT スキル標準モデルカリキュラム【IT スキル標準 V3（レベル 1）】

「IT スキル標準モデルカリキュラム」は、IT スキル標準のレベル 1～3 を目指す人向けのカリキュラムとして IPA から公開されています。

レベル 1 向けのモデルカリキュラムは、職業人として備えておくべき、情報技術に関する共通的な基礎知識を修得することを目指す社会人や学生を対象としたカリキュラムであり、研修ロードマップをもとに、具体的な研修コースを設計･実施する際に参考となる情報がまとめられています。このモデルカリキュラムを履修することにより、IT スキル標準のレベル 1 に相当する知識を修得することができます。

24-3. マナビ DX

マナビ DX は、経済産業省と IPA が運営するデジタル人材育成のためのプラットフォームで、デジタルスキル習得に関する講座を紹介するポータルサイトになっています。デジタルスキルを学んだことのない人から、実践的なデジタル知識・スキルを身につけたい人まで、それぞれに適した講座を紹介してくれます。

マナビ DX は、無料や補助付きの講座を含み、リスキリングに重要なデジタルスキル習得をはじめる方に最適な初学者向け講座も提供されています。

訴求ポイント

章を通した気づき・学び

知識やスキルを備えた人材の育成・確保のためには、関係機関が公表しているセキュリティ関連のカリキュラム内容を活用し、実施計画を検討することが重要です。

認識していただきたい実施概要
● 「プラス・セキュリティ知識補充講座 カリキュラム例」や「IT スキル標準モデルカリキュラム IT スキル標準 V3（レベル 1）」といった関係機関が公表しているセキュリティ関連のカリキュラム内容を把握すること。 ● カリキュラム内容を参考に、具体的な実施計画や実施内容を検討すること。 ● マナビ DX を活用し、デジタルスキルの向上を図ること。

詳細理解のため参考となる文献（参考文献）	
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.cyber.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
マナビ DX	https://manabi-dx.ipa.go.jp

31-25. 第 25 章. スキルと知識を持った人材育成・人材確保方法

25-1. 「プラス・セキュリティ」の実施計画例
25-2. 「リスキリング」「チェンジマインド」の実施計画例

章の目的
第 25 章では、カリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を理解することを目的とします。カリキュラムごとに、実践方法を例示します。

主な達成目標
◘ 「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること ◘ 「IT スキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること ◘ 「デジタルスキル標準」をもとに、教育・研修の実施内容および実施計画を作成する手順を理解すること

主なキーワード
チェンジマインド、リスキリング、プラス・セキュリティ

要旨

25 章の全体概要

25 章では、既存のカリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成方法を解説しています。

章の前半では、「プラス・セキュリティ知識補充講座 カリキュラム例」をもとに、教育・研修の実施内容および実施計画を解説しています。

章の後半ではリスキリングに有効と考えられるカリキュラムを例にして、リスキリングのための研修実施計画の策定手順について解説しています。

25-1. 「プラス・セキュリティ」の実施計画例

「プラス・セキュリティ知識補充講座 カリキュラム例」を実施するための手順を例示しています。セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていくことが必要です。技術は常に進化しており、過去の対策や古い

考え方では、最新のサイバー攻撃に対応することが難しいためです。昨今は AI を使った新しい攻撃手法が増加しており、昔のスキルや知識だけでは十分に対応することは困難です。

25-2. 「リスキリング」「チェンジマインド」の実施計画例

IT スキル標準、デジタルスキル標準など、リスキリングに有効と考えられるカリキュラムや指針を参考に、実施計画を策定する手順について例を使って解説しています。生成 AI などの新技術の普及により仕事が変化し、新たなスキルが求められる中、個人が競争力を維持するにはリスキリングが重要です。リスキリングを成功させるには、変化を受け入れるチェンジマインドを持ち、柔軟な思考で具体的な目標を設定し、信頼できる教材やカリキュラムを選び、自分にあった学習方法を見つけることが大切です。

訴求ポイント

章を通した気づき・学び

生成 AI など新しい技術が発展する中で、個人が市場で競争力を維持するためにはリスキリングによって最新のスキルと知識を習得することが重要です。

また、AI を活用した新たな攻撃に対応するため、既にセキュリティを担当している人も含め、新しい技術と考え方を学ぶ必要があります。

認識していただきたい実施概要
● 関係機関が公表しているカリキュラムなどを活用し、チェンジマインド、リスキリングも含めた実施計画および教育・研修の実施内容の作成し、実施すること。

詳細理解のため参考となる文献（参考文献）	
マナビ DX	https://manabi-dx.ipa.go.jp
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html
プラス・セキュリティ知識補充講座 カリキュラム例	https://security-portal.cyber.go.jp/dx/pdf/plussecurity_curriculum.pdf
IT スキル標準モデルカリキュラム－レベル 1 を目指して	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf

31-26. 第 26 章.サイバーレジリエンスの必要性

26-1. サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ
26-2. ISO/IEC 27002:2022 に基づく情報セキュリティインシデント管理策
26-3. サイバーレジリエンス戦略としての NIST CSF 2.0 フレームワーク
26-4. サイバーレジリエンス能力の育成に向けた体系項立て

章の目的
第 26 章では、中小企業におけるサイバーレジリエンスの必要性とその定義を理解し、ISO/IEC 27001/27002 や NIST CSF 2.0 との関係を把握することで、自組織の情報セキュリティ戦略や IT-BCP と統合したレジリエンスを段階的に構築するための基礎を身につけることを目的とします。
主な達成目標
◘ サイバーレジリエンスの概念と、防御だけでなく回復・適応を重視する戦略的必要性を理解すること ◘ ISO/IEC 27001/27002 および ISMS の PDCA との関連を踏まえ、可用性維持と継続的改善がレジリエンスの基盤であることを説明できること ◘ NIST CSF 2.0 の 6 機能、とくに Respond／Recover の重要性を理解し、中小企業向けの段階的導入方法を整理できること サイバーレジリエンスライフサイクル（準備・防御・検知・対応・復旧・改善）を体系的に把握し、自社の取り組みへ適用できること

主なキーワード
サイバーレジリエンス、可用性、ISO/IEC 27001/27002、NIST CSF 2.0、Respond、Recover

要旨

26 章の全体概要

26 章では、中小企業におけるサイバーレジリエンスの必要性を整理し、その定義と情報セキュリティ戦略上の位置づけについて解説しています。

従来の「侵入を防ぐこと」を中心としたサイバーセキュリティ対策に加え、インシデントの発生を前提として、迅速な対応・復旧・改善を含めた事業継続能力の確保が重要であることを示しています。

章の前半では、サイバーレジリエンスの基本概念を整理し、ISO/IEC 27001/27002（ISMS）における可用性および継続的改善との関係を解説しています。

章の後半では、NIST Cybersecurity Framework（CSF）2.0 をサイバーレジリエンス戦略の枠組みとして位置づけ、特に Respond および Recover 機能を中心とした体系的な考え方と、中小企業における段階的な能力育成の考え方を整理しています。

26-1. サイバーレジリエンスの定義と情報セキュリティ戦略上の位置づけ

サイバーレジリエンスを、サイバー攻撃やシステム障害などの事態が発生した場合でも、影響を最小限に抑え、迅速に回復し、事業を継続するための能力として定義しています。

ISO/IEC 27001 における情報セキュリティの三要素のうち、特に可用性の維持と、PDCA サイクルによる継続的改善が、サイバーレジリエンスの基盤となることを示しています。

26-2. ISO/IEC 27002:2022 に基づく情報セキュリティインシデント管理策

ISO/IEC 27002 に基づく管理策を、事前準備、対応、回復、学習・改善の観点から整理し、サイバーレジリエンス能力を構成する具体的な要素として解説しています。

情報資産管理、バックアップ、インシデント対応体制、復旧計画および教訓の反映といった管理策が、組織の回復力を高めるために重要であることを示しています。

26-3. サイバーレジリエンス戦略としての NIST CSF 2.0 フレームワーク

NIST CSF 2.0 を、サイバーレジリエンス戦略を体系的に整理するための枠組みとして位置づけています。

6 つの機能（Govern、Identify、Protect、Detect、Respond、Recover）のうち、特に Respond および Recover 機能が、インシデント発生後の対応力と事業復旧能力の中核であることを解説しています。

また、Govern 機能を通じて、サイバーレジリエンスが経営レベルのリスク管理として位置づけられる必要性を示しています。

26-4. サイバーレジリエンス能力の育成に向けた体系項立て

サイバーレジリエンスを、防御から復旧、改善に至るライフサイクルとして捉え、NIST CSF 2.0 の機能と既存のハンドブック記載内容を統合した体系を整理しています。

中小企業においては、限られたリソースの中で段階的に取り組むことが重要であり、成熟度に応じた育成モデルを用いることで、現実的な能力向上が可能であることを示しています。

訴求ポイント

章を通した気づき・学び

サイバー攻撃やシステム障害を完全に防ぐことは困難であるという前提に立ち、迅速な対応と回復を含めたサイバーレジリエンスの確保が、事業継続と経営リスク低減に不可欠であることを理解することが重要です。

特に中小企業においては、ISO/IEC 27001/27002 や NIST CSF 2.0 といった公的枠組みを活用し、段階的に能力を高めていくことが現実的なアプローチとなります。

認識していただきたい実施概要

- ISO/IEC 27001/27002 および NIST CSF 2.0 といった公的に整理されたフレームワークを活用し、防御だけでなく対応・復旧・改善を含めたサイバーレジリエンスを情報セキュリティ戦略に組み込むこと。
- 中小企業の実情に応じて、段階的な導入と優先順位付けを行い、事業継続力の向上を図ること。

詳細理解のため参考となる文献（参考文献）	
経済産業省「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
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）」	https://www.ipa.go.jp/security/guide/sme/about.html
総務省「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
IPA サイバーレジリエンスのためのコミュニケーション ～セキュリティ担当者に必要なコミュニケーションスキル集～	https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2024/f55m8k00000070u7-att/f55m8k000000710q.pdf
NIST Cybersecurity Framework (CSF) 2.0（2024）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
JISC「JIS Q 27000：情報セキュリティマネジメントシステム－用語」	https://kikakurui.com/q/Q27000-2019-01.html
デジタル庁「デジタル・ガバメント推進標準ガイドライン（2025 年 5 月）」	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf

31-27. 第 27 章.サイバー攻撃を含む様々な事態に対する総合的な対応計画

27-1. サイバーレジリエンスのライフサイクルと対応計画の策定
27-2. NIST CSF 2.0 Respond（RS）機能に基づく対応基準
27-3. NIST CSF 2.0 Recover（RC）機能に基づく復旧基準

章の目的
第 27 章では、インシデント対応計画（IRP）と IT-BCP を統合し、ISO/IEC 27002 および NIST CSF 2.0 を基盤とした、予防から対応・復旧・改善まで一体となった総合的な対応計画とサイバーレジリエンス・ライフサイクルの構築方法を学ぶことを目的とします。

主な達成目標
◘ IRP と IT-BCP を連携させた総合的対応計画の枠組みを理解すること ◘ NIST CSF 2.0 の Respond／Recover 機能に基づく対応・復旧基準を把握すること ◘ RTO・RPO 設定やバックアップ等による事業復旧プロセスを設計できること RC.CO による復旧時のコミュニケーションと信頼維持の要点を理解すること

主なキーワード
サイバーレジリエンス、IRP（インシデント対応計画）、IT-BCP、NIST CSF 2.0、Respond、Recover、RTO／RPO

要旨

27 章の全体概要

27 章では、サイバー攻撃を含む様々な事態に対して、中小企業が組織として対応・復旧を行うための総合的な対応計画について解説しています。

インシデント対応計画（IRP）と情報システム継続計画（IT-BCP）を統合し、ISO/IEC 27002 および NIST Cybersecurity Framework（CSF）2.0 を基盤とした、予防から対応、復旧、改善までを一体として捉える考え方を示しています。

章の前半では、サイバーレジリエンス・ライフサイクルに基づく対応計画の策定方法を整理し、章の後半では、NIST CSF 2.0 の Respond および Recover 機能に基づく具体的な対応・復旧基準を解説しています。

27-1. サイバーレジリエンスのライフサイクルと対応計画の策定

サイバーレジリエンスを、計画、実施、評価、改善の PDCA サイクルとして捉え、インシデント対応計画（IRP）と IT-BCP を一体化した総合的な対応計画の策定方法を解説しています。

経営層の関与のもと、重要業務や情報資産を特定し、RTO（復旧時間目標）および RPO（復旧時点目標）を設定することが、実効性ある対応計画の基礎となることを示しています。

27-2. NIST CSF 2.0 Respond(RS)機能に基づく対応基準

インシデント発生時の初動対応、分析、被害軽減を担う Respond 機能について解説しています。

インシデント管理体制の確立、封じ込め、証拠保全、原因分析および軽減策の実施といった対応を、組織的に実行するための基準を整理しています。

また、中小企業においては、役割分担の明確化、外部機関との連携、定期的な訓練を通じて、対応力を維持・向上させることが重要であることを示しています。

27-3. NIST CSF 2.0 Recover (RC)機能に基づく復旧基準

インシデントの影響を受けたシステムや業務を迅速に復旧するための Recover 機能について解説しています。

復旧計画の実行にあたり、RTO および RPO を明確に設定し、バックアップや冗長化を含む復旧基盤を整備することの重要性を示しています。

また、復旧過程における関係者とのコミュニケーションや、復旧後の教訓の反映を通じた継続的改善が、サイバーレジリエンス能力の向上につながることを整理しています。

訴求ポイント

章を通した気づき・学び

サイバー攻撃やシステム障害への対応は、個別の手順対応にとどまらず、IRP と IT-BCP を統合した総合的な対応計画として整備することが重要です。

NIST CSF 2.0 の Respond および Recover 機能を活用することで、対応から復旧、改善までを一貫したプロセスとして整理でき、事業継続力の向上につながります。

認識していただきたい実施概要
● インシデント対応計画（IRP）と IT-BCP を統合し、サイバー攻撃を含む様々な事態に対応できる総合的な対応計画を策定・運用すること。 ● ISO/IEC 27002 および NIST CSF 2.0 を参照し、対応・復旧・改善を含めたサイバーレジリエンス・ライフサイクルを組織に定着させること。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
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）」	https://www.ipa.go.jp/security/guide/sme/about.html
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
JPCERT/CC「インシデント対応依頼フォーム」	https://www.jpcert.or.jp/form/
経済産業省「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
IPA「情報セキュリティ 10 大脅威 2025」	https://www.ipa.go.jp/security/10threats/

31-28. 第 28 章. 情報システム継続計画（IT-BCP）の一環としてのインシデントに対応する体制

28-1. 情報システム継続計画（IT-BCP）の基本要素と体制
28-2. インシデント対応体制の確立と初動対応の具体的手順
28-3. 復旧・回復プロセスと教訓の反映（継続的改善）
28-4. サイバーレジリエンス能力向上のための実践的な演習と訓練

章の目的
第 28 章では、サイバーレジリエンス確保に不可欠な情報システム継続計画（IT-BCP）を独立した柱として位置づけ、その中にインシデント対応体制・復旧プロセス・教訓の反映および訓練を一体的に組み込み、中小企業でも現実的に運用可能な仕組みとして定着させることを目的とします。
主な達成目標
◘ IT-BCP と IRP を統合したインシデント対応体制の基本構造を理解すること ◘ RTO・RPO 設定や復旧優先順位に基づく復旧・回復プロセスを設計できること ◘ ランサムウェア対策を含む技術的対策と証拠保全・記録の実務要点を把握できること 教訓の反映と継続的改善サイクルを運用し、訓練・演習及び外部支援を活用しながら IT-BCP を日常業務に定着させる方法を理解すること

主なキーワード
IT-BCP、インシデント対応体制、初動対応、ランサムウェア対策、復旧・回復、継続的改善、訓練・演習

要旨

28 章の全体概要

28 章では、サイバーレジリエンス確保に不可欠な情報システム継続計画（IT-BCP）を軸として、インシデント対応体制、復旧・回復プロセス、教訓の反映および訓練・演習を一体的に運用する方法を解説しています。

サイバー攻撃を含む様々な事態を想定し、中小企業でも現実的に運用可能な体制として、IT-BCP とインシデント対応計画（IRP）を統合して構築・定着させる考え方を示しています。

章の前半では、IT-BCP の基本要素と体制を整理し、章の後半では、初動対応、技術的対策、復旧後の改善および訓練・演習を通じた継続的な能力向上について解説しています。

28-1. 情報システム継続計画（IT-BCP）の基本要素と体制

IT-BCP を、情報システムとデータの継続を担保する独立した計画として位置づけ、その基本要素と体制を解説しています。

経営層のリーダーシップのもとで、インシデント対応体制の役割と責任を明確化し、復旧優先順位や RTO（復旧時間目標）・RPO（復旧時点目標）を設定することが、実効性ある IT-BCP の基盤となることを示しています。

28-2. インシデント対応体制の確立と初動対応の具体的手順

インシデント発生時の被害拡大を防ぐため、検知・報告、封じ込め、根絶といった初動対応の具体的な手順を解説しています。

中小企業においては、専任人材が限られることを前提に、簡潔で実践的な行動指針を定め、外部支援機関との連携を含めた体制整備が重要であることを示しています。

28-3. 復旧・回復プロセスと教訓の反映（継続的改善）

復旧・回復後に再発防止策を実施し、インシデント対応から得られた教訓を IT-BCP や手順書に反映する重要性を解説しています。

原因分析、改善策の立案・実施、記録およびレビューを通じて、PDCA サイクルを継続的に回すことが、サイバーレジリエンス能力の向上につながることを整理しています。

28-4. サイバーレジリエンス能力向上のための実践的な演習と訓練

IT-BCP およびインシデント対応体制の実効性を確保するため、定期的な訓練・演習の必要性を解説しています。

経営層、実務担当者、一般従業員それぞれを対象とした訓練を段階的に実施し、訓練結果を改善に反映することで、組織全体の対応力を維持・向上させる考え方を示しています。

訴求ポイント

章を通した気づき・学び

IT-BCP は文書を整備するだけではなく、体制の明確化、初動対応の実践、復旧後の改善、訓練・演習を通じて継続的に運用することが重要です。

中小企業においては、限られたリソースの中で実行可能な範囲から取り組みを積み重ねることで、サイバーレジリエンス能力を現実的に高めることができます。

認識していただきたい実施概要
● IT-BCP を軸に、インシデント対応体制、復旧・回復プロセス、教訓の反映および訓練を一

体として整備・運用すること。

- 公的機関が公表しているガイドラインや演習資料を活用し、継続的な改善を通じて IT-BCP を日常業務に定着させること。

詳細理解のため参考となる文献（参考文献）	
NIST Cybersecurity Framework（CSF）2.0（2024 年版）	https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf
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）」	https://www.ipa.go.jp/security/guide/sme/about.html
中小企業庁「中小企業 BCP 策定運用指針」	https://www.chusho.meti.go.jp/bcp/
国家サイバー統括室（NCO）「2023 年度 分野横断的演習 実施報告」	https://www.cyber.go.jp/pdf/policy/infra/NISC_enshu_20240327.pdf
日本シーサート協議会「サイバー攻撃演習訓練実施マニュアル」	https://www.nca.gr.jp/activity/pub_doc/drill_manual.html
CSIRT スタータキット	https://www.nca.gr.jp/activity/pub_doc/csirtstarterkit.html
CSITR スタータキット ver3.0	https://www.nca.gr.jp/activity/pub_doc/imgs_u/CSIRTstarterkit_v3.pdf
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」	https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf
IPA「情報セキュリティ 10 大脅威 2025」	https://www.ipa.go.jp/security/10threats/
中小企業支援セミナー（IPA 主催）	https://www.ipa.go.jp/security/seminar/sme/supportseminar.html?utm_source=chatgpt.com

31-29. 第 29 章. 生成 AI および AI マネジメントシステム

29-1. AI の進化とガバナンス・リスクマネジメントの喫緊性
29-2. AI ガバナンスの国際標準：ISO/IEC 42001 の全貌
29-3. AI に特有のリスクの特定と体系的な管理
29-4. ISO/IEC 42001 に基づく AI マネジメントシステムの構築と運用

章の目的
第 29 章では、生成 AI の利活用に伴うリスクとガバナンスの要点を理解し、組織としての AI 運用方針を確立すること及び AI 倫理、情報セキュリティ、法的遵守を統合した管理体制を構築し、安全かつ信頼できる生成 AI 活用を実現することを目的とします。

主な達成目標
◘ 生成 AI 利用における情報管理とリスクの仕組みを理解すること ◘ ISO/IEC 42001（AI マネジメントシステム）の構成と適用範囲を把握すること ◘ 自社の AI 活用を統制する方針策定と運用手順を検討できるようにすること

主なキーワード
生成 AI、AI マネジメントシステム、ISO/IEC 42001、AI リスク、ガバナンス、説明責任

要旨

29 章の全体概要

29 章では、生成 AI の急速な普及を背景に、企業が直面する AI 特有のリスクとガバナンスの必要性について解説しています。

生成 AI の利活用に伴い、情報セキュリティ、プライバシー、倫理、法令遵守などの課題が顕在化する中で、組織としてリスクを把握し、体系的に管理するための枠組みとして、AI マネジメントシステムの考え方を整理しています。

章の前半では、AI の進化とリスクマネジメントの重要性を整理し、章の後半では、ISO/IEC 42001 を中心とした国際標準を参照しながら、AI リスクの特定、評価、管理およびマネジメントシステムの構築・運用について解説しています。

29-1. AI の進化とガバナンス・リスクマネジメントの喫緊性

生成 AI を含む AI 技術の進化により、業務効率化や新たな価値創出が可能になる一方で、従来の IT リスク管理では十分に対応できない課題が生じていることを整理しています。

このような状況において、AI の利活用を進めるためには、技術面だけでなく、ガバナンスおよびリスクマネジメントの観点から、組織的な対応が必要であることを示しています。

29-2. AI ガバナンスの国際標準：ISO/IEC 42001 の全貌

AI マネジメントシステムの国際標準である ISO/IEC 42001 について、その目的、適用範囲および基本構造を解説しています。

AI のライフサイクル全体を対象とし、方針策定、役割と責任の明確化、リスク管理、運用管理および継続的改善を通じて、信頼できる AI 利用を実現する枠組みであることを整理しています。

29-3. AI に特有のリスクの特定と体系的な管理

AI に特有のリスクとして、バイアス、プライバシー侵害、セキュリティ上の問題、倫理的課題などを整理しています。

ISO/IEC 42001 におけるリスクベースアプローチの原則に基づき、AI リスクの特定、アセスメント、影響度評価を行い、ISO 31000 のリスクマネジメントの指針と連携させて管理する考え方を解説しています。

29-4. ISO/IEC 42001 に基づく AI マネジメントシステムの構築と運用

ISO/IEC 42001 の要求事項および Annex A の管理策を活用し、AI マネジメントシステムを構築・運用するための基本的な手順を解説しています。

既存の情報セキュリティマネジメントシステムやリスクマネジメントと統合することで、効率的かつ実務に即した導入が可能であることを整理しています。

訴求ポイント

章を通した気づき・学び

生成 AI の活用を安全かつ継続的に進めるためには、AI 特有のリスクを正しく認識し、国際標準に基づいたガバナンスとリスクマネジメントを組織として整備することが重要です。

ISO/IEC 42001 を活用することで、AI 利用を統制しながら価値創出につなげるための共通の枠組みを理解することができます。

認識していただきたい実施概要
● 生成 AI の利活用に伴うリスクを把握し、AI ガバナンスおよびリスクマネジメントの観点から組織的に管理すること。

- ISO/IEC 42001 および ISO 31000 などの国際標準を参考に、既存のマネジメントシステムと統合した AI マネジメント体制を構築・運用すること。

詳細理解のため参考となる文献（参考文献）	
東京都　AI 時代の信頼性を築く：ISO/IEC 42001 等の ISO 関連規格に基づく AI ガバナンスとリスクマネジメントの活用戦略	https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/619/index.html
経済産業省　AI マネジメントシステムの国際規格が発行されました	https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html
講演レポート「AI 規制について --欧米の動向と日本の状況--」 | JIPDEC	https://www.jipdec.or.jp/library/report/20240722-r01.html

第32章. 今後実施すべきこと

章の目的
テキストの内容を実践するにあたって行うべき事項を明確化し、具体的な行動計画が策定できるようになることを目的とします。これまで学んだ内容を活用し、自社のセキュリティ体制の向上や課題解決に向けた次のステップを提示します。

主な達成目標
□　学んだ内容をもとにして行動計画を策定できるようになること

32-1. 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。この章では、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、その概要を説明します。

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、重要なポイントを経営者も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、重要なポイントを経営者も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 推進の方向性を知ること
  中小企業においても DX 推進が不可欠です。
- 自組織における DX 推進のための人材育成の必要性を認識すること
  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））の確保が必要です。
- 自組織における DX 推進の計画を立案し実施内容を策定すること
  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）を意識することが重要です。
  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）を意識するとともに「デジタル・ガバメント推進標準ガイドライン」を参考にすることが重要です。
  「デジタル・ガバメント推進標準ガイドライン」は、中小企業でも活用できる重要なことが数多く記載されています。情報システムを導入する際に参考にすることで、セキュリティ対策を考慮した、効果的な情報システムの導入が可能になります。

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「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、それぞれメリット・デメリットがあること
  例えば、ISMS などのフレームワークを用いた Lv.3 網羅的アプローチは、時間とコストがかかるというデメリットがあるものの、漏れのない対策が可能であるというメリットがあります。
- 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が大切です。
  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。

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

管理策の実施について

セキュリティポリシー関連文書の整備

組織全体で情報セキュリティを管理・運用するための基盤となるドキュメント（基本方針、対策基準、実施手順など）を作成します。それらを整備することで、セキュリティ対策の指針を明確にし、全社員が一貫した行動を取ることを可能にします。

実施手順の実行準備

実施手順として策定した内容を実行するため、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。

実施手順の実行

実施手順の実行にあたり、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それを実行します。

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。

※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」を参照。

② 年間を通して実行すべき事項の例示

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。これらの事項を実行するため、年間計画を作成します。

※13-2-6. ISMS：8. 運用「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

年間計画（例）を紹介します。

<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>・主要な従業員の「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>

情報システム導入の実行について

情報システムの導入にあたり、重要なポイントを紹介します。

Fit&Gap 分析

Fit&Gap 分析は、SaaS やパッケージソフトウェアを導入する際に非常に重要なプロセスです。Fit&Gap 分析によって、RFI などの情報収集活動によって選定した SaaS やパッケージソフトウェアと、自社の業務要件との適合性を評価します。

Fit＆Gap 分析の一般的な実施手順（例）

1. 現状分析
2. SaaS、パッケージソフトウェアの機能調査
3. 比較分析
4. ギャップへの対応策検討
5. 費用対効果の分析
6. 実施計画の策定

※「3.比較分析」は Fit＆Gap 分析の中核をなす重要なステップです。

非機能要件における、セキュリティ要件の決め方

セキュリティに関する要件の決定は、適用宣言書をもとにして行います。セキュリティ要件を決める流れは以下の通りです。

1. 情報システムで取扱う情報資産に対して、リスクアセスメントを実施する。
2. リスクアセスメントの結果をもとに、必要な管理策を決定する。（適用宣言書の作成）
3. 適用宣言書の内容を満たすように、セキュリティ要件を決定する。

※リスクアセスメントの実施方法の詳細については、「12-2.リスクマネジメント：リスクアセスメント」を参照してください。

※セキュリティ要件の決め方の詳細については、「21-1-2.要件定義」の「非機能要件の定義」における「情報セキュリティに関する事項」を参照してください。

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施すること

管理策を実施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。

管理策を実施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.3.0 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施していくための取組例

実施手順を具体的に実施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施していくにあたり、実施手順と主体となって取り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	―	-	○	―

○：主体となって取り組む必要がある。

図 113. 実施手順とメインとなる担当者を対応付ける例

セキュリティ対策を考慮した情報システムを導入するために参考となる情報

セキュリティ対策を考慮した効果的な情報システムをどのように導入するか、その際に参考となる各種資料を紹介します。

セキュリティ対策を考慮した情報システムを導入するために参考となる情報	
DS-100 デジタル・ガバメント推進標準ガイドライン	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf
DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ae9a37b7/20250619_resources_standard_guidelines_guideline_05.pdf
安全なウェブサイトの作り方	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000017316.pdf
セキュリティ実装チェックリスト	https://www.ipa.go.jp/security/vuln/websecurity/ug65p900000196e2-att/000044403.xlsx
EC サイト構築・運用セキュリティガイドライン	https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf
情報セキュリティサービス基準適合サービスリスト	https://www.ipa.go.jp/security/service_list.html
脆弱性診断サービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20251223_2.pdf
デジタルフォレンジックサービス	https://www.ipa.go.jp/security/ug65p90000019fc0-att/20251223_3.pdf
ウェブサイトの攻撃兆候検出ツール iLogScanner	https://www.ipa.go.jp/security/vuln/ilogscanner/index.html

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。

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	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 2025 について	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2025/2025_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/cd4e0324/20250613_policies_priority_outline_03.pdf
Society5.0	https://www8.cao.go.jp/cstp/society5_0
サイバーセキュリティ 2025 の概要	https://www.cyber.go.jp/pdf/policy/kihon-s/cs2025_abstract.pdf
サイバーセキュリティ戦略	https://www.cyber.go.jp/pdf/policy/kihon-s/cs_strategy2025.pdf
IT 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 2.1	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/dxtebikihontai2.1.pdf
DX 動向 2025	https://www.ipa.go.jp/digital/chousa/dx-trend/tbl5kb0000001mn2-att/dx-trend-2025.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
情報通信白書 令和 7 年版	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/pdf/01hyoshi.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 2025」選定企業レポート	https://www.meti.go.jp/policy/it_policy/investment/dx-chukenchushotebiki/dx-chukenchushotebiki_2025.pdf
セキュリティインシデント事例	
情報セキュリティ白書 2025	https://www.ipa.go.jp/publish/wp-security/2025.html
情報セキュリティ 10 大脅威 2025	https://www.ipa.go.jp/security/10threats/10threats2025.html
サイバー攻撃対応事例	https://security-portal.cyber.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.cyber.go.jp/policy/inquiry/index.html
コンピュータウイルス・不正アクセスの届出事例［2023 年下半期（7 月～12 月）］	https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h2-jirei.pdf

令和７年上半期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/R7kami/R07_kami_cyber_jyosei.pdf
2024 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 -業種ごとの効果的な取組事例集-	https://www.ipa.go.jp/security/reports/sme/nl10bi000000fbw9-att/sme-kouka-jirei2024.pdf

人材育成

セキュリティに詳しくない人に加えて、既にセキュリティを担当している人も、新しい技術を学び、考え方を最新にしていくことが必要です。技術は常に進化しており、過去の対策や古い考え方では、最新のサイバー攻撃に対応することが難しいためです。また、AI や自動化などの新しい技術の導入が進んでいますが、これによって従来の仕事が変化し、新しいスキルが必要になります。中長期で見れば AI などの新技術の普及によって、一部の職業は消滅し、新しい職業が生まれることになるでしょう。そうした変化の中で、個人が市場で競争力を維持するためには、リスキリングを通じて最新の技術や知識を習得し、変化に対応できる能力を高めることが不可欠です。リスキリングを成功させるためには、チェンジマインド（変革思考）を持つことが非常に重要です。考え方を柔軟に変え、具体的な目標を設定するとともに、信頼できる教材やカリキュラムを選んで、自分にあった学習方法を見つけることが、リスキリング成功の秘訣だといってよいでしょう。

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。人材育成を実施するために参考となる文献を紹介します。

DSS に基づく人材育成	
デジタルスキル標準 Ver.1.2	https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000083ki-att/000106872.pdf
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」について	https://security-portal.cyber.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 ～ 変化するサイバーセキュリティリスクに対処するための組織の在り方と従事	https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

する人材の配置・役割分担 ～第 2 版	
IT スキル標準に基づく人材育成	
IT スキル標準とは -ものさしとしてのスキル標準	https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html
IT スキル標準モデルカリキュラム－レベル 1 を目指して－	https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.pdf
その他	
マナビ DX	https://manabi-dx.ipa.go.jp
デジタル人材育成政策のご紹介	https://manabi-dx.ipa.go.jp/gov_assist
【ほぼ 15 秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン	https://www.ipa.go.jp/security/anshin/measures/start.html

編集後記

第 12 編では、中小企業におけるサイバーセキュリティ対策を全体的に取りまとめ、各章で取り上げた要点を振り返りつつ、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、その概要を説明しました。本編では、DX の推進とサイバーセキュリティ対策の両立を目指し、経営層がリーダーシップを発揮して全社的な体制を整備する重要性を強調しています。

セキュリティ対策基準の策定方法として 3 つのアプローチ手法（クイック、ベースライン、網羅的）を提示し、企業が自らの状況に応じた対策を柔軟に選択できるよう解説しています。また、デジタル時代における IT 投資のあり方として「守りの IT 投資」と「攻めの IT 投資」のバランスの重要性を示し、経営判断のもと、セキュリティ対策を経営戦略の一環として実施する必要性を明確にしました。

さらに、実際のインシデント事例や脅威情報を通じて、具体的な課題とその解決策を提示しました。これにより、企業が直面する現実的なリスクへの理解を深め、対策を効果的に実施するための土台を築くことを目指しています。

情報システムの導入にあたっては、本編で紹介した「デジタル・ガバメント推進標準ガイドライン」における中小企業でも活用できる重要な部分を参考にすることで、セキュリティ対策の実装や運用がより円滑に進むことが期待されます。

サイバーセキュリティは一過性の施策ではなく、継続的な改善と人材育成が不可欠です。本編で取り上げた知識や指針をもとに、読者の皆様が自社に最適なセキュリティ体制を構築し、持続的な運用・改善を実施されることを願っています。本テキストが、中小企業を含む社会全体のサイバーセキュリティの向上と、急速に変化するデジタル社会における競争力の強化、DX 推進の一助となれば幸いです。

引用文献

東京都　AI時代の信頼性を築く：ISO/IEC 42001等のISO関連規格に基づくAIガバナンスとリスクマネジメントの活用戦略

https://www.cybersecurity.metro.tokyo.lg.jp/security/KnowLedge/619/index.html

経済産業省　AIマネジメントシステムの国際規格が発行されました

https://www.meti.go.jp/press/2023/01/20240115001/20240115001.html

講演レポート「AI規制について --欧米の動向と日本の状況--」 | JIPDEC

https://www.jipdec.or.jp/library/report/20240722-r01.html

参考文献

デジタルスキル標準 ver. 1.2

https://www.meti.go.jp/policy/it_policy/jinzai/skill_standard/20240708-gp-1.pdf

プラス・セキュリティ知識補充講座 カリキュラム例

https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

ITスキル標準モデルカリキュラム－レベル1を目指して－

https://www.ipa.go.jp/archive/jinzai/skill-standard/itss/qv6pgp000000buc8-att/000024802.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/ngi93u000002kef-att/000100451.pdf

DS-100 デジタル・ガバメント推進標準ガイドライン

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/d4e68a9b/20250619_resources_standard_guidelines_guideline_01.pdf

DS-120 デジタル・ガバメント推進標準ガイドライン実践ガイドブック

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/ae9a37b7/20250619_resources_standard_guidelines_guideline_05.pdf

デジタルガバナンス・コード

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

Society5.0

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

SECURITY ACTION セキュリティ対策自己宣言

https://www.ipa.go.jp/security/security-action/

情報セキュリティ5か条

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

5分でできる！情報セキュリティ自社診断

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

情報セキュリティ基本方針（サンプル）

https://www.ipa.go.jp/security/sme/f55m8k0000001wbv-att/000072146.docx

経済財政運営と改革の基本方針 2025

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2025/2025_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/cd4e0324/20250613_policies_priority_outline_03.pdf

中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き2.1

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/dxtebikihontai2.1.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.cyber.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf

サイバーセキュリティ2025

https://www.cyber.go.jp/pdf/policy/kihon-s/250627cs2025.pdf

目的や所属・役割から選ぶ施策一覧

https://security-portal.nisc.go.jp/curriculum/

サイバーセキュリティ関係法令Q&AハンドブックVer2.0

https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook_2.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.cyber.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

情報セキュリティ白書2025

https://www.ipa.go.jp/publish/wp-security/2025.html

情報セキュリティ10大脅威2025

https://www.ipa.go.jp/security/10threats/10threats2025.html

情報通信白書令和7年版（総務省）

https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/pdf/00zentai.pdf

DX動向2025

https://www.ipa.go.jp/digital/chousa/dx-trend/tbl5kb0000001mn2-att/dx-trend-2025.pdf

攻めのIT活用指針

https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.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

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

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

リスク分析シート
https://www.ipa.go.jp/security/sme/f55m8k0000001wd3-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（サンプル）
https://www.ipa.go.jp/security/sme/ps6vr7000001bu8m-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/
ISO/IEC TR 13335-1
https://www.iso.org/standard/39066.html
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/about.html
インターネットの安全・安心ハンドブックVer.5.10
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
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/sme/f55m8k0000001wcf-att/000072150.pdf
ISMS-AC ISMS適合性評価制度
https://isms.jp/doc/JIP-ISMS120-62.pdf
The NIST Cybersecurity Framework (CSF) 2.0
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.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（CPSF）の概要
https://www.meti.go.jp/policy/netsecurity/wg1/cpsf_ver1.o_gaiyou.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/policy/netsecurity/downloadfiles/guide_v3.0.pdf
リスクアセスメントとリスク対応
https://www.jnsa.org/ikusei/01/02-04.html
ISO/IEC 27001:2022
https://www.iso.org/standard/27001

ISO/IEC 27002:2022

https://www.iso.org/standard/75652.html

DS-110 デジタル・ガバメント推進標準ガイドライン解説書

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/573c839f/20250619_resources_standard_guidelines_guideline_03.pdf

アジャイル領域へのスキル変革の指針　アジャイル開発の進め方

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/ps6vr70000001i7c-att/000065606.pdf

ECサイト構築・運用セキュリティガイドライン

https://www.ipa.go.jp/security/guide/vuln/ps6vr7000000acvt-att/000109337.pdf

ITスキル標準V3 2011 1部：概要編

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/ps6vr70000004x60-att/000024840.pdf

ITSS+（プラス）概要

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itssplus/about.html

i コンピテンシディクショナリ解説書

https://www.icda.or.jp/wp-content/uploads/2021/03/iCD_guidebook-1.pdf

Di-Lite

https://www.dilite.jp/

情報処理技術者試験 情報処理安全確保支援士 試験要綱

https://www.ipa.go.jp/shiken/syllabus/nl10bi0000007smr-att/youkou_ver5_4.pdf

CISSP 8 ドメインガイドブック

https://japan.isc2.org/files/MAR-CISSP_Guidebook-JP-RB-2023.pdf

ISACA 東京支部

https://www.isaca.gr.jp

プラス・セキュリティ知識補充講座 カリキュラム例

https://security-portal.nisc.go.jp/dx/pdf/plussecurity_curriculum.pdf

ITスキル標準とは -ものさしとしてのスキル標準

https://www.ipa.go.jp/jinzai/skill-standard/plus-it-ui/itss/itss2.html

マナビDX

https://manabi-dx.ipa.go.jp

【ほぼ15秒アニメ】子ブタと学ぼう！情報セキュリティ対策のキホン

https://www.ipa.go.jp/security/anshin/measures/start.html

■AI

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

29-1、30-2、31-1、31-6、31-23、31-25

■AI マネジメントシステム（AIMS）

AI Management System の略。AI を開発・提供・利用する組織が、AI に関わるリスクや責任を適切に管理し、信頼性・透明性・説明責任を確保するための管理の仕組み。国際規格「ISO/IEC 42001」に基づき、AI のライフサイクル全体を通じたリスク評価やガバナンス体制、継続的な改善を行い、生成 AI を含む AI の責任ある活用を支援する。

29-2-1、29-4-1、29-4-3、30-1

■BCP

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

31-21

■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。

31-21

■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。

31-3

■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。

30-1、30-2、31-2

■GDPR

General Data Protection Regulation の略。欧州連合（EU）における個人データ保護とプライバシーを目的とした一般データ保護規則。個人データの取得・利用・保存・移転に関する厳格なルールを定めており、EU 域内外を問わず、EU 居住者の個人データを取り扱う組織に適用される。生成 AI を含むデータ活用においても、適切なデータ管理とプライバシー保護を求める国際的に重要な規制である。

29-2-1、31-4

■ICT

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

31-6、31-15

■IoT（アイ・オー・ティー）

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

31-3、31-5、31-6、31-22

■IRP

Incident Response Plan：インシデント対応計画の略。サイバー攻撃や情報漏洩などのセキュリティインシデントが発生した際に、被害を最小限に抑え、迅速な復旧と再発防止を図るための文書化された計画。誰が・何を・どの順序で・どのように対応するかを明確に定め、組織が混乱なく行動できるようにすることを目的とする。企業や組織にとって不可欠な文書であり、事前の準備と定期的な見直しが重要とされる。

28-4、第 10 編-編集後記、31-27、31-28

■ISMS

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

29-2-2、30-1、30-2、31-7、31-8、31-11、31-12、31-13、31-14、31-26、32-1

■IT-BCP

IT Business Continuity Plan の略。企業の事業継続計画（BCP）の一部として策定する、災害やサイバー攻撃、システム障害などによって IT システムが停止した場合でも、業務を継続・早期復旧できるようにするための計画。企業の重要な情報資産やシステムの保護、損失の最小化を目的とし、復旧目標（RTO/RPO）や代替手段、バックアップ、システムの冗長化、クラウド活用などの対策が含まれる。IT への依存度が高まる現代において、定期的な見直しと訓練を通じて実効性を高めることが求められる。

28-4、第 10 編-編集後記、30-1、30-2、31-26、31-27、31-28

■NCO

National Cybersecurity Office の略。国家サイバー統括室の略。2025 年 5 月に成立したサイバー対処能力強化法および同整備法を受け、内閣サイバーセキュリティーセンター（NISC）を改組し、同年 7 月 1 日、内閣官房に設置された。サイバーセキュリティ戦略本部の事務局として、サイバーセキュリティの確保に関する総合調整の役割を担う。

28-4、30-2、31-4、31-10、31-24

■NIST サイバーセキュリティフレームワーク（CSF）

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

においても、今後普及が見込まれる。
30-1、31-11、31-26、31-27

■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、銀行口座番号に加えて、氏名、生年月日、住所、勤務先などの情報も PII に含まれる。
31-15

■RFI
Request For Information の略。情報提供依頼のこと。発注者が依頼をする候補となるシステム開発会社に対して、技術情報や製品情報の提供を依頼すること。
32-1

■RPO
Recovery Point Objective の略。システム障害やサイバー攻撃などのインシデント発生時に、どの時点までのデータを復旧対象とするかを定める指標。インシデント発生前のどれだけのデータ損失を許容できるかを示し、バックアップの頻度や保管方法、データ保全の厳格さを決める基準となる。適切な RPO の設定により、データ損失の影響を最小限に抑え、迅速な復旧と事業継続を支えるための重要な指標として、サイバーレジリエンスの領域でも重視されている。
10 編-編集後記、31-27、31-28

■RTO
システム障害やサイバー攻撃などのインシデント発生後、業務やサービスを再開するまでに許容される最大の停止時間を定める指標。復旧に必要な時間の上限を示し、システム構成、復旧手順、代替手段の設計における重要な基準となる。 適切な RTO の設定により、業務への影響を最小限に抑え、迅速なサービス復旧と事業継続を実現する。RPO（Recovery Point Objective）と併せて、可用性やサイバーレジリエンスを評価する際の重要な指標とされる。
10 編-編集後記、31-27、31-28

■SASE（サシー）
Secure Access Service Edge の略。令和元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サービス上で統合して提供するサービス、また、その考え方・概念。
31-18

■SECURITY ACTION
中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度。
30-2、31-2

■Society5.0
日本が目指すべき未来社会の姿として、平成 28 年に閣議決定された「第 5 期科学技術基本計画」において内閣府が提唱した概念。サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）で、狩猟社会、農業社会、工業社会、情報社会の次にくる社会として位置づけられている。
30-2、31-1、31-3、31-6
32-1

■アカウンタビリティ
組織や個人が、自らの行動や意思決定、その結果について、関係者に対して説明し、責

任を果たすこと。
29-3-1

■アクセス制御
特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザーを制限する機能のこと。
31-15、31-18

■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。
31-29

■アルゴリズム
AI が入力データを処理し、判断や予測、出力を行うための計算手順やルールの集合。
29-4-1

■イノベーション
新しい技術や仕組み、価値を創出し、社会やビジネスに変化をもたらすこと。
29-2-1、29-3-1、29-4-4

■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（パソコン、プリンタ、スキャナ、スマートフォン、仮想マシン、サーバ、IoT デバイスなど）
31-18

■オープンイノベーション
企業や組織が自社の技術や知見にとどまらず、大学・研究機関・他企業・スタートアップなど外部の知識や人材、アイデアを積極的に活用して、新たな価値を創出する考え方。生成 AI や AI マネジメントの分野では、外部技術やサービスとの連携によりイノベーションを推進しつつ、リスクや責任を適切に管理することが重要とされる。
29-3-1

■ガバナンス
組織が目標を達成するために、方針やルールを定め、意思決定や行動を適切に統制・管理する仕組みや体制。生成 AI や AI マネジメントの分野では、リスク管理や責任の明確化、法令・倫理への対応を通じて、AI を適切かつ信頼性のある形で活用するための重要な考え方とされている。
29-1、29-2-1、29-3-1、29-4-1、29-4-3、29-4-4、11 編-編集後記、30-1、31-29

■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。
31-11、31-12、31-26

■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。
31-11、31-12

■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。
31-7、31-11、31-12

■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。
31-15

■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。
31-15

■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。
31-18

■国際電気標準会議（IEC）
International Electrotechnical Commission の略。 電気・電子技術分野の国際規格を策定する非政府組織で、電力、電子機器、情報通信技術（ICT）などにおける安全性や互換性を確保する基準を提供している。 ISO と連携して情報技術分野の標準化も進めており、AI マネジメントシステムに関する国際規格「ISO/IEC 42001」は、両機関の合同専門委員会（JTC1）により策定された。
29-1

■国際標準化機構（ISO）
International Organization for Standardization の略。スイス・ジュネーブに本部を置く、国際的な標準化を推進する非政府組織。製品やサービス、マネジメントシステムの品質・安全性・効率性を確保するための国際規格を策定しており、品質管理（ISO 9001）、情報セキュリティ（ISO/IEC 27001）、AI マネジメント（ISO/IEC 42001）などが広く利用されている。これらの規格は、生成 AI を含む企業活動の信頼性向上や経営管理の高度化、取引先・社会からの信頼確保に寄与する共通の枠組みを提供する。
29-1

■コミットメント
方針や目標の実現に向けて、責任を持って関与し、継続的に取り組む姿勢や意思を指す。
29-4-4

■コンテキスト
AI マネジメントシステムの構築・運用に影響を与える、組織の内部および外部の状況、利害関係者の期待などの背景要因。
29-4-1

■コンプライアンス
法令や規則、業界ガイドライン、社内ルールなどを遵守すること。生成 AI や AI マネジメントの分野では、個人情報保護、知的財産、AI 規制、倫理原則などへの適合が求められ、リスク低減や社会的信頼の確保において重要な要素とされる。
29-2-2、29-3-1、29-4-2

■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さまざまである。デジタル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。
30-1、31-1、31-3、31-5、31-6、31-11、31-19、31-25、31-26、31-27、31-28、32-1

■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。
30-1、30-2、31-4、32-1

■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。
30-1、31-11

■サイバーレジリエンス

サイバー攻撃やシステム障害が発生しても、業務の継続性を維持しながら影響を最小限に抑え、迅速に回復・適応できる能力を指す。従来の「防御中心」のサイバーセキュリティに対し、攻撃を受けることを前提に「備える・耐える・回復する・適応する」といった一連の対応力を含む概念であり、組織の事業継続性と信頼性を高めるための重要な要素として NIST CSF2.0 でも位置づけられている。

10 編-編集後記、30-1、30-2、31-26、31-27、31-28

■サイロ化

サイロ化とは、組織やシステムが部署や部門ごとに分断され、情報やデータ、意思決定が十分に共有・連携されない状態を指す。その結果、全体最適が図れず、リスク管理や業務効率、意思決定の質が低下する要因となる。

29-2-2

■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。

30-2、31-3、31-5、31-11、31-15

■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、空調を挙げている。

31-17

■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。

31-8、31-12、31-15、31-17、31-19、31-21、31-26、31-27、32-1

■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。

31-15、31-16

■ステークホルダー

組織の活動や意思決定、システムの導入・運用によって影響を受ける、または影響を与える利害関係者のこと。

29-3-1

■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。

30-1、30-2、31-5、31-8 31-18

■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。

32-1

■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。

28-4、10 編-編集後記、30-1、30-2、31-5、31-7、31-8、31-9、31-15、31-18、31-26、31-27、31-28、32-1、12 編

■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ことが一般的。

30-2、31-7

■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。

31-18

■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」。

31-22

■ダイナミック

状況や環境の変化に応じて、柔軟かつ迅速に対応し、継続的に調整・改善される性質や状態を指す。AI マネジメントの文脈では、技術の進化や社会的要請、リスクの変化に応じて、リスク管理とイノベーションのバランスを固定的にせず、継続的に見直し・改善を行う姿勢を表す際に用いられる。

29-4-4

■ダッシュボード

AI システムの動作や出力結果を可視化し、性能や公平性、バイアスの有無などを評価・監視するためのツール。AI マネジメントでは、透明性や説明責任を確保する手段として、ダッシュボードの活用が推奨されている。

29-4-1

■多様性

多様性とは、年齢、性別、国籍、文化、価値観、能力など、人々が持つさまざまな違いが尊重される状態を指す。AI の分野では、特定の属性や集団に偏らない設計や判断を行うことで、差別や不公平な扱いといったリスクを低減するための重要な考え方とされる。

29-1、29-3-1、29-3-2

■陳腐化

技術や制度、ルールなどが環境の変化や進歩に追いつけず、価値や有効性を失ってしまうこと。

29-3-2

■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。

31-22、31-23

■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。

31-18

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション

（digitization）と、デジタル技術を用いてビジネスプロセスを自動化・合理化するデジタライゼーション（digitalization）がある。音楽ビジネスでいえば、アナログ記録のレコードを CD（コンパクトディスク）にすることがデジタイゼーション、音楽をダウンロード販売することがデジタライゼーションである。
30-1、31-4、31-6、31-24

■ドキュメンテーション

ドキュメンテーションとは、AI システムの設計・開発・運用に関する情報や判断の根拠、プロセスを文書として整理・記録・管理すること。アカウンタビリティ（説明責任）を果たすための基盤となり、トレーサビリティの確保やステークホルダーへの説明、リスク対応の透明性向上に不可欠とされる。十分なドキュメンテーションが行われていない場合、責任の所在が不明確となり、信頼性や法的対応力の低下につながるおそれがある。
29-3-1

■トップマネジメント

組織を指揮・統制し、最終的な意思決定責任を持つ経営層を指す。AI マネジメントにおいては、AI ガバナンスの方針決定や資源配分を通じて、AI の活用を事業戦略やリスク管理と整合させる重要な役割を担う。
29-4-4、31-13

■トレーサビリティ

AI システムの設計・開発・運用における判断や処理の過程を追跡・記録し、後から確認・説明できるようにする仕組み。アカウンタビリティ（説明責任）を支える要素の一つであり、AI の意思決定プロセスやデータの流れを可視化・文書化することで、責任の所在を明確にし、信頼性や法的対応力を高める役割を果たす。
29-3-1

■トレーニングデータ

AI モデルを学習させるために使用されるデータのこと。AI の性能や公平性に大きな影響を与えるため、正確性、完全性、代表性、偏りの有無などを確認し、品質を適切に管理することが求められる。
29-4-1

■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。
29-4-2、30-2、31-19

■バイアス

AI の学習データや設計、運用上の要因により、特定の属性や条件に対して偏った判断や結果が生じること。生成 AI においては、不公平な扱い、差別的な出力、誤った意思決定につながるリスクがあり、法的・倫理的な問題を引き起こす可能性がある。そのため、AI ガバナンスや AI マネジメントにおいては、バイアスを重要なリスクの一つとして把握し、継続的に管理・低減することが求められる。
29-1、29-2-1、29-3-1、29-3-3、29-4-1、31-29

■ハイレベルストラクチャー（HLS）

High Level Structure の略。ISO が策定した、すべてのマネジメントシステム規格に共通する構造と基本要素の枠組み。規格間の整合性を高め、品質（ISO 9001）、情報セキュリティ（ISO/IEC 27001）、AI マネジメント（ISO/IEC 42001）など、複数の ISO 規格を効率的に統合・運用できるよう設

計されている。 組織が一貫した方針とプロセスでマネジメントを行うための基盤となっている。
29-2-2、29-4-1、11 編-編集後記

■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。
31-5

■フィッシングメール
実在する企業や組織、人物を装い、受信者に偽のリンクや添付ファイルを開かせることで、個人情報や認証情報を不正に取得しようとする詐欺メール。報漏えいやマルウェア感染を引き起こすおそれがあり、サイバーセキュリティ上の代表的な脅威の一つとされる。近年では生成 AI の活用により、文法的に自然で本物そっくりのメールが自動生成されるなど、従来の対策では見抜くことが難しくなっている。
29-1、29-3-1

■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。
32-1

■不確実性
将来の結果や影響を事前に正確に予測・把握することが難しい状態を指す。
29-1、29-3-1、29-4-4、11 編-編集後記

■不正アクセス
利用権限を持たない悪意のあるユーザーが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、平成12年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている。
31-5、32-1

■プライバシー侵害
個人の意思に反して、個人情報や私的な情報が不適切に取得・利用・公開されること。
29-1、29-3-3、29-4-1、31-29

■フレームワーク
フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃などさまざまなセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな型」としてまとめたもの。
29-2-1、29-3-4、29-4-4、11 編-編集後記、30-1、30-2、31-7、31-11、31-13、31-22、31-26、32-1

■プロファイリング
プロファイリングとは、個人の行動履歴や属性データなどをもとに、傾向や特徴を自動的に分析・分類する手法。
AI によるプロファイリングは、利便性の向上やサービスの最適化に活用される一方、本人の知らないうちに判断が下されることで、人間の尊厳や個人の自立を損なうリスク

がある。そのため「人間中心のAI社会原則」では、プロファイリングに対する配慮の重要性が示されている。
29-3-1

■ベストプラクティス
何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例や良い成果をもたらす方法論。
29-3-4、31-5

■包摂性
年齢、性別、障がいの有無、文化的・社会的背景などにかかわらず、すべての人が平等に参加し、恩恵を受けられるようにする考え方。AIの設計や運用においては、特定の集団が排除されたり不利益を被ったりしないよう、意図的に配慮された仕組みづくりが求められる。
29-3-1

■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。
29-1、29-3-1、31-18

■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。
31-18

■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。
30-2、31-5

■リスキリング
技術や環境の変化に対応するために、新たな知識やスキルを習得し直すこと。AIの活用が進む中では、生成AIを含む新しい技術を理解・活用できる人材を育成するため、教育や研修を通じた継続的なリスキリングが重要とされる。
29-3-1、30-2、31-24、31-25、32-1

■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は何らかのセキュリティ対策を講じる必要がある。
29-3-1、29-3-3、29-4-1、29-4-3、29-4-4、30-1、30-2、31-12、31-14、31-15、31-16、31-17、31-18、31-21、32-1

■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。
29-3-2、29-3-4、29-4-1、29-4-2、30-2、31-12

■リスクプロファイル
組織やシステムが直面するリスクの種類、発生可能性、影響度などを整理し、全体像として把握したもの。生成AIやAIマネジメントの分野では、技術的リスクに加え、法令・倫理・社会的影響なども含めて評価し、リスク対応の優先順位付けや管理方針の策定に活用される。

29-1、11 編-編集後記

■リスクベースアプローチ

想定されるリスクの大きさや影響度、発生可能性に応じて、対策や管理の優先順位を決める考え方。AI マネジメントや国際規格（ISO/IEC 42001 等）において、信頼性や安全性を確保するための基本的な枠組みとして重視されている。

29-1、29-3-2、31-29

■リテラシー

情報や技術を正しく理解し、適切に活用するための知識や能力。AI 分野では、仕組みやリスクを理解した上で、倫理的・法的な観点も踏まえて活用する力を指す。

29-3-1

■ログ（記録）

ログとは、コンピュータシステム、ネットワーク機器、アプリケーションなどで発生する操作履歴やイベント情報を時系列で記録したデータのこと。ユーザー操作、アクセス履歴、認証情報、設定変更、エラーや障害などを把握でき、インシデントの原因調査や不正アクセスの検知、監査証跡として活用される。適切なログの取得・保管・分析は、インシデントの早期発見や原因特定、再発防止に不可欠であり、サイバーセキュリティ対策の基盤となる。

28-4、31-18

付録：ISO/IEC 42001 附属書 A 管理目標・管理策（参考）

本付録は、ISO/IEC 42001:2023 附属書 A に規定されている 10 の管理目標および 38 の管理策について、公開されている解説資料を基に要約・整理した参考情報です。正式な規格文書は ISO または日本規格協会が発行する原文を参照ください。

管理策はすべてを適用することを要求するものではなく、組織の AI 利用状況およびリスク評価に基づき、適用・非適用を判断することが想定されています。

管理目標および管理策一覧

管理目標	概要	管理策（項目）
A.2：AI に関する方針	組織が AI をどのように活用し、どのような倫理観を持つべきかの「憲法」を定めます。	(A.2.1) AI 方針 (A.2.2) AI 方針のレビュー
A.3：内部組織	AI を適切に管理するための責任体制とガバナンスを構築します。	(A.3.1) AI の役割と責任 (A.3.2) 報告ライン
A.4：AI システムの資源	AI のライフサイクルを支えるために必要なリソースを適切に管理します。	(A.4.1) 人的資源 (A.4.2) データ資源 (A.4.3) 計算資源
A.5：AI システムの影響評価	AI が社会、個人、環境に及ぼす潜在的な影響を分析します。	(A.5.1) 影響評価プロセス (A.5.2) 影響評価の実施 (A.5.3) 影響評価の記録
A.6：AI システムライフサイクル	企画から開発、運用、廃棄までの各段階で品質と安全性を確保します。	(A.6.1) ライフサイクルプロセスの管理 (A.6.2) 目標の策定 (A.6.3) 設計と開発 (A.6.4) 検証と妥当性確認 (A.6.5) 展開（リリース） (A.6.6) 運用と関し (A.6.7) 変更管理 (A.6.8) 廃棄
A.7： データと情報	AI の精度と信頼性の源泉である「データ」を厳格に管理します。	(A.7.1) データの取得 (A.7.2) データの準備 (A.7.3) データの品質 (A.7.4) データのバイアス (A.7.5) データの機密性 (A.7.6) データの出所管理

A.8：利用者への情報提供	AI の透明性を高め、利用者との信頼関係を築きます。	(A.8.1) 利用者への説明 (A.8.2) 説明可能性 (A.8.3) 情報の提供
A.9：AI システムの利用	他社から提供される AI ツールやサービスを利用する際のリスクを管理します。	(A.9.1) 外部 AI システムの利用方針 (A.9.2) 供給者（ベンダー）の評価 (A.9.3) 供給者との合意 (A.9.4) 外部 AI システムの監視
A.10：関係者とのコミュニケーション	社会的な説明責任を果たし、ステークホルダーとの信頼を維持します。	(A.10.1) 外部への報告 (A.10.2) 利害関係者との対話 (A.10.3) インシデントの通知
A.11：改善	PDCA サイクルを通じて、AI マネジメントを継続的に進化させます。	(A.11.1) 不適合と是正処置 (A.11.2) 継続的改善 (A.11.3) AI システムの再学習 (A.11.4) モニタリング結果の活用

東京都産業労働局