令和６年度

中小企業サイバーセキュリティ

社内体制整備事業

第 10 編　全体総括

第26章. 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。

26-1. 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。

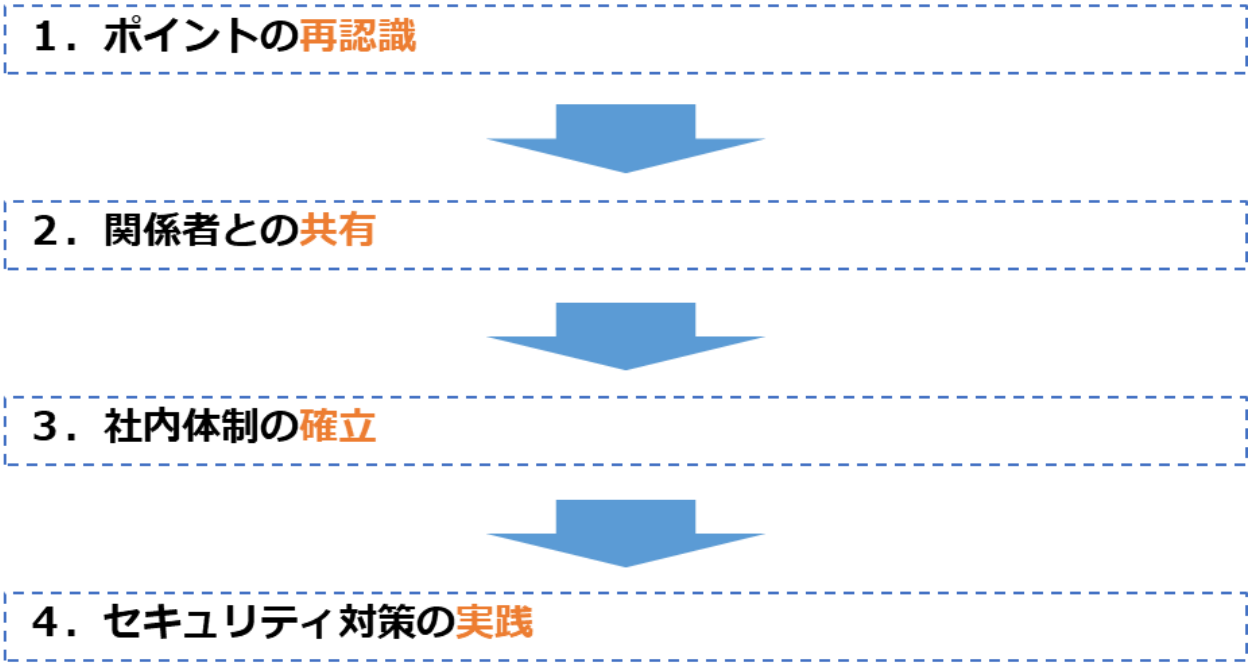
第 9 編 組織として実践するためのスキル・知識と人材育成 【レベル共通】

（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。

26-2. 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。

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。

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。

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。

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 10 編.全体総括」をエグゼクティブサマリーとして活用してください。重要な点を理解し、経営者および他関係者と共有します。

3. 社内体制の確立

経営者のリーダーシップによって、サイバーセキュリティ対策のための社内体制を確立します。知識やスキルを備えた人材の育成・確保をします。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	NISC 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.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

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」

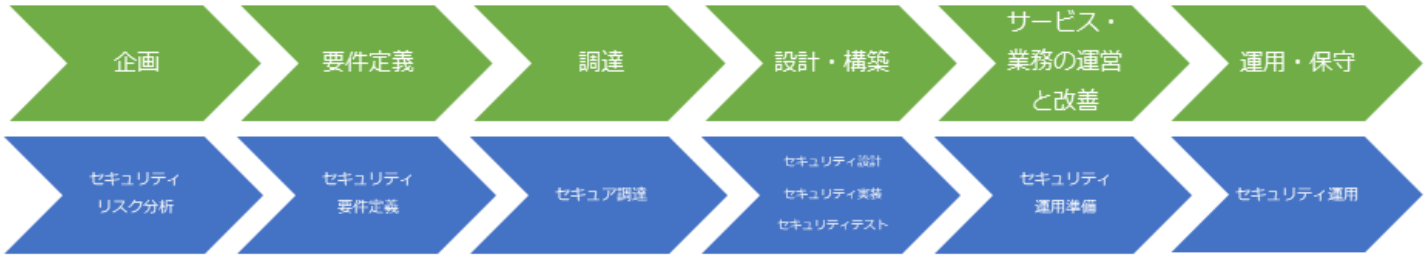


図 102. IT 導入プロセスにおけるセキュリティ対策の実施タイミング

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/1fc6722a/20240605_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/d85eeb55/20240605_resources_standard_guidelines_guideline_05.pdf

第27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。

27-1. 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

27-2. 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。

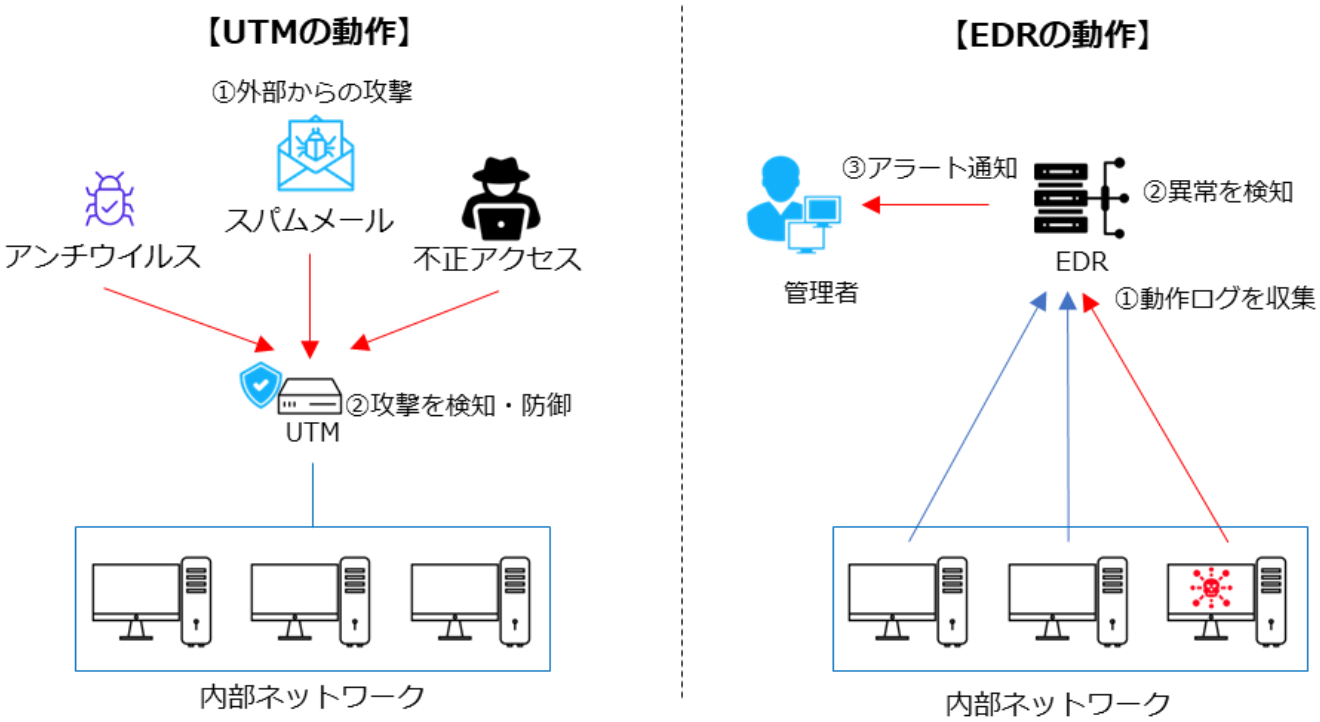


図 103. UTM、EDR の概要図

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。

- Lv1. クイックアプローチ
- Lv2. ベースラインアプローチ
- Lv3. 網羅的アプローチ

訴求ポイント

章を通した気づき・学び

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

27-3. 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。令和 6 年度の方針における IT 戦略に関係する施策として「（さまざまな分野における）DX の推進」、「デジタル・ガバメントの強化」、「サイバーセキュリティの強化」があります。

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」に基づき「デジタル社会の実現に向けた重点計画」を閣議決定しています。重点計画には、日本がデジタル社会を実現していくための政府の取組として、7 つの戦略的な政策が掲げられています。この 4 番目が「サイバーセキュリティなどの安全・安心

の確保」となっています。

デジタル社会を実現していくための 7 つの戦略的な政策
1. デジタル社会の実現に向けた構造改革
2. デジタル田園都市国家構想の実現
3. 国際戦略の推進
4. サイバーセキュリティなどの安全・安心の確保
5. 急速な AI の進歩・普及を踏まえた対応
6. 包括的データ戦略の推進と今後の取組
7. Web3.0 の推進

重点計画における、各分野における基本的な施策の 4 番目「産業のデジタル化」では「中小企業の DX 推進」や「中小企業のデジタル化の支援」が盛り込まれています。

各分野における基本的な施策
1. 国民に対する行政サービスのデジタル化
2. 安全・安心で便利な暮らしのデジタル化
3. アクセシビリティの確保
4. 産業のデジタル化
5. デジタル社会を支えるシステム・技術
6. デジタル社会のライフスタイル・人材

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 2024	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html
デジタル社会の実現に向けた重点計画	https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
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 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

27-4. 第 4 章. サイバーセキュリティ戦略および関連法令

4-1. NISC：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、NISC によるサイバーセキュリティ戦略を通じて、DX とサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法と GDPR について説明します。
主な達成目標
◘ 日本におけるサイバーセキュリティに関する方針や施策について理解すること ◘ サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること ◘ 個人情報関連の法令を理解すること

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、NISC の「サイバーセキュリティ戦略」を紹介するとともに、DX with Cybersecurity の考え方について解説しています。デジタルの活用が進むとともに、サイバーセキュリティのリスクも高まっています。企業は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. NISC：サイバーセキュリティ戦略

サイバーセキュリティ戦略

国家レベルでサイバーセキュリティの確保に取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 2024

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 2024」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.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
サイバーセキュリティ 2024	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf
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
中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
企業経営のためのサイバーセキュリティの考え方の策定について	https://www.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf

27-5. 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。

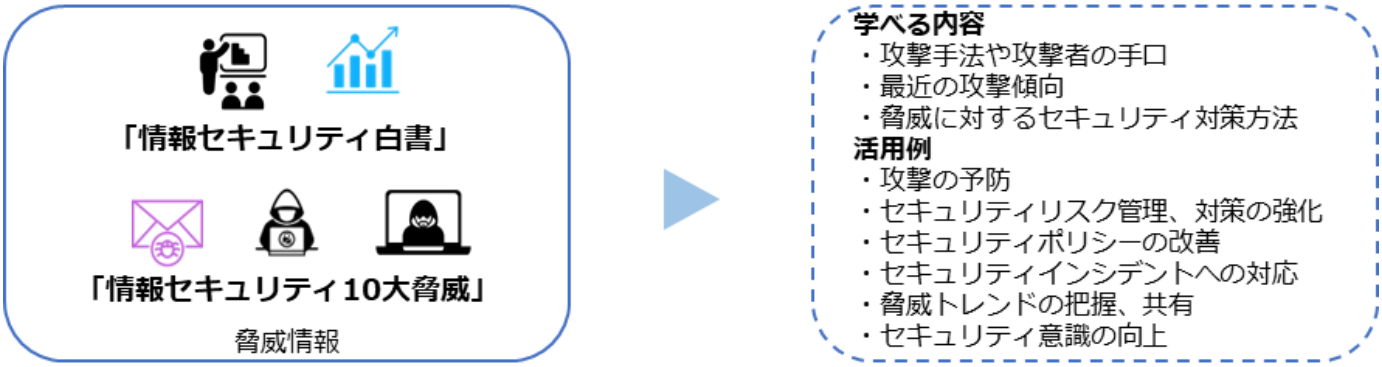


図 104. 情報セキュリティ白書・情報セキュリティ 10 大脅威の活用方法

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。

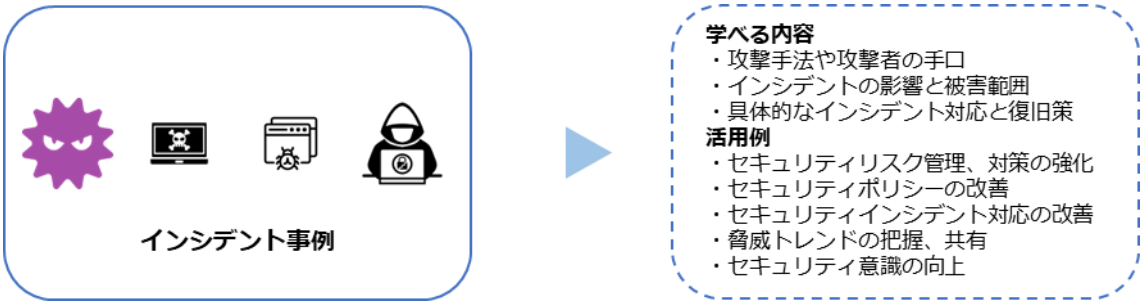


図 105. インシデント事例を通じて学べる内容

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 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/10threats2024.html

27-6. 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 2022 年には 84.9%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。

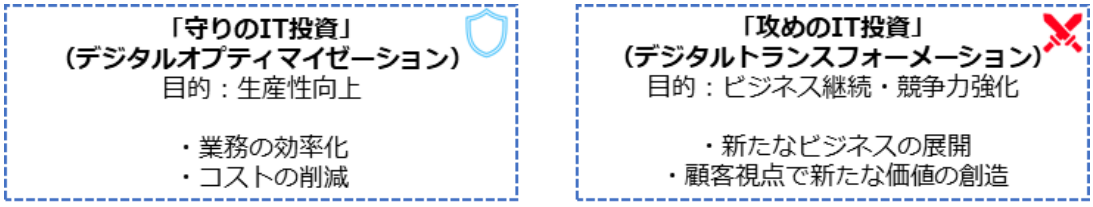


図 106. 守りの IT 投資・攻めの IT 投資

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 3 年版（総務省）	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf
DX 白書 2023	https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
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

27-7. 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。

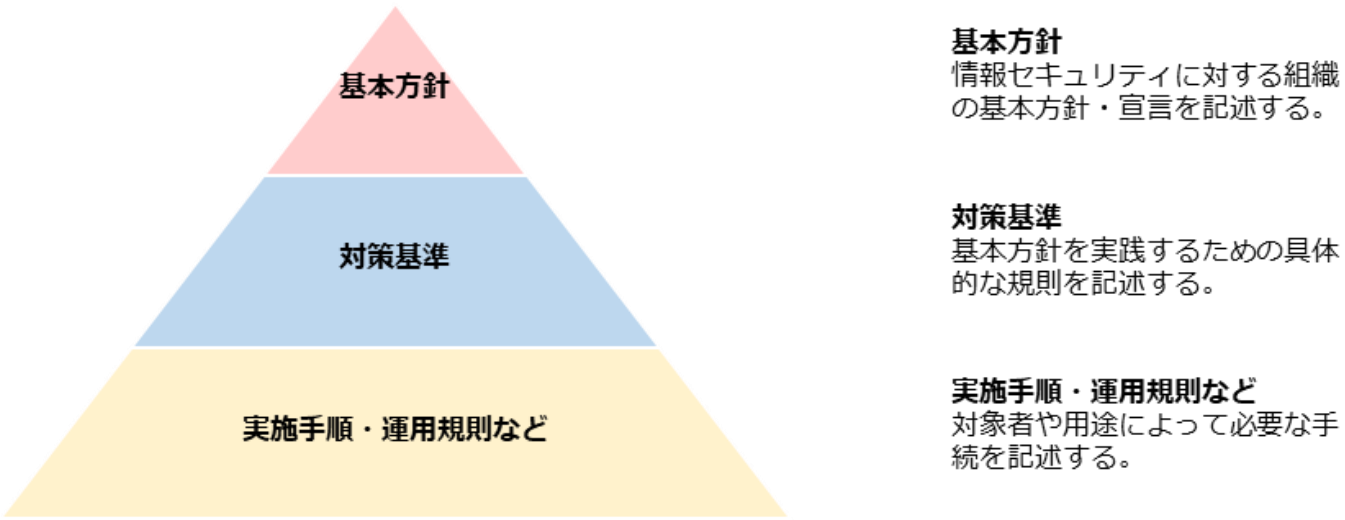


図 107. 情報セキュリティポリシーの全体像

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 2024	https://www.ipa.go.jp/security/10threats/nq6ept000000g22h-att/kaisetsu_2024.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/

27-8. 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。

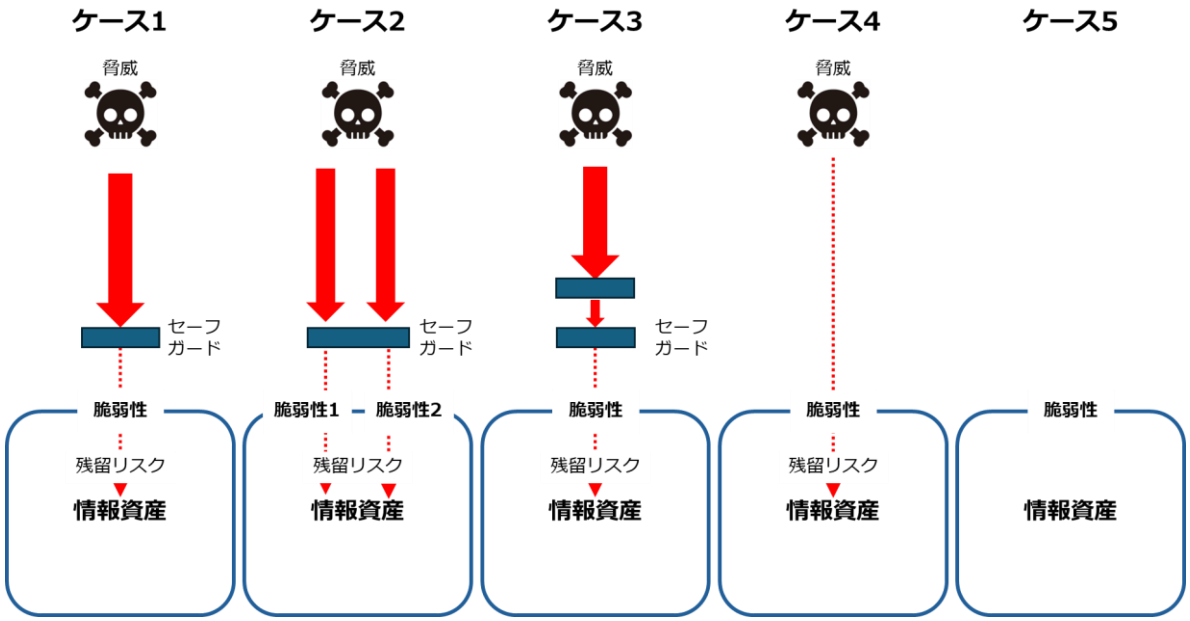


図 108. 脅威、脆弱性、情報資産、セーフガード（管理策）、リスクの関係

（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 (Accidental → A)	「入力ミス」がありますが、入力ミスが生じないように、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

27-9. 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

27-10. 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」、NISC による「インターネットの安全・安心ハンドブック Ver.5.0」、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。 • 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。	• 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。 • ガイドラインやひな型は、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.5.00	https://security-portal.nisc.go.jp/guidance/handbook.html
テレワークセキュリティガイドライン第 5 版	https://www.soumu.go.jp/main_content/000752925.pdf
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

27-11. 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
- ISA/IEC 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/press/2022/03/20230324002/20230324002-1.pdf

27-12. 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。

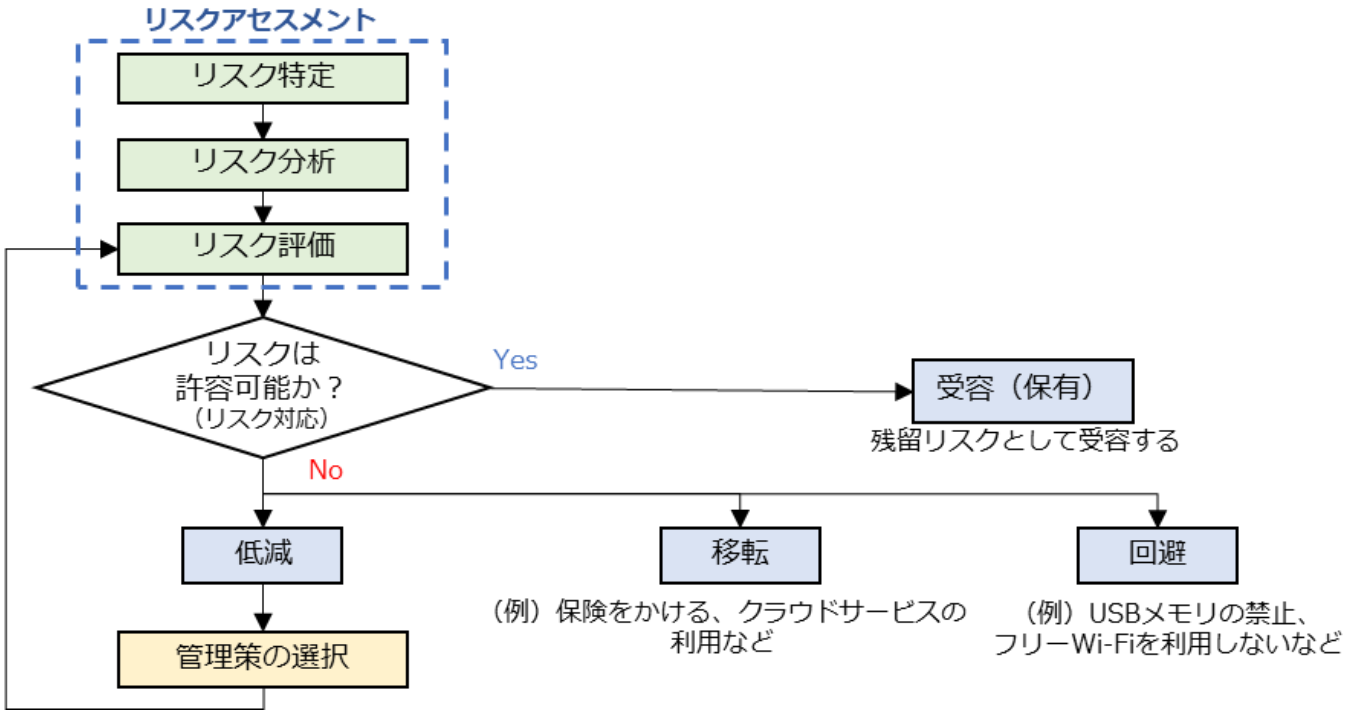


図 109. リスクマネジメント全体の流れと、リスク対応の選択プロセス

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

27-13. 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。

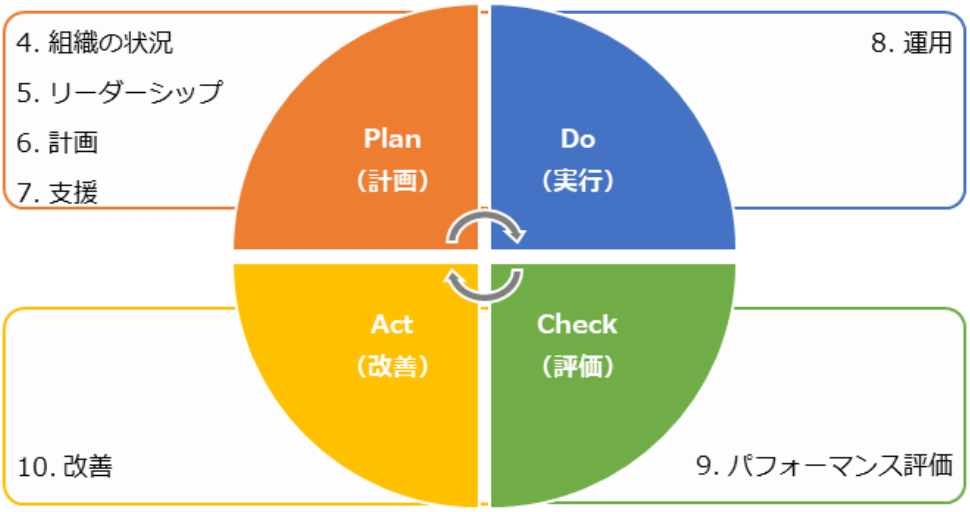


図 110. ISMS の PDCA サイクル

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

27-14. 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

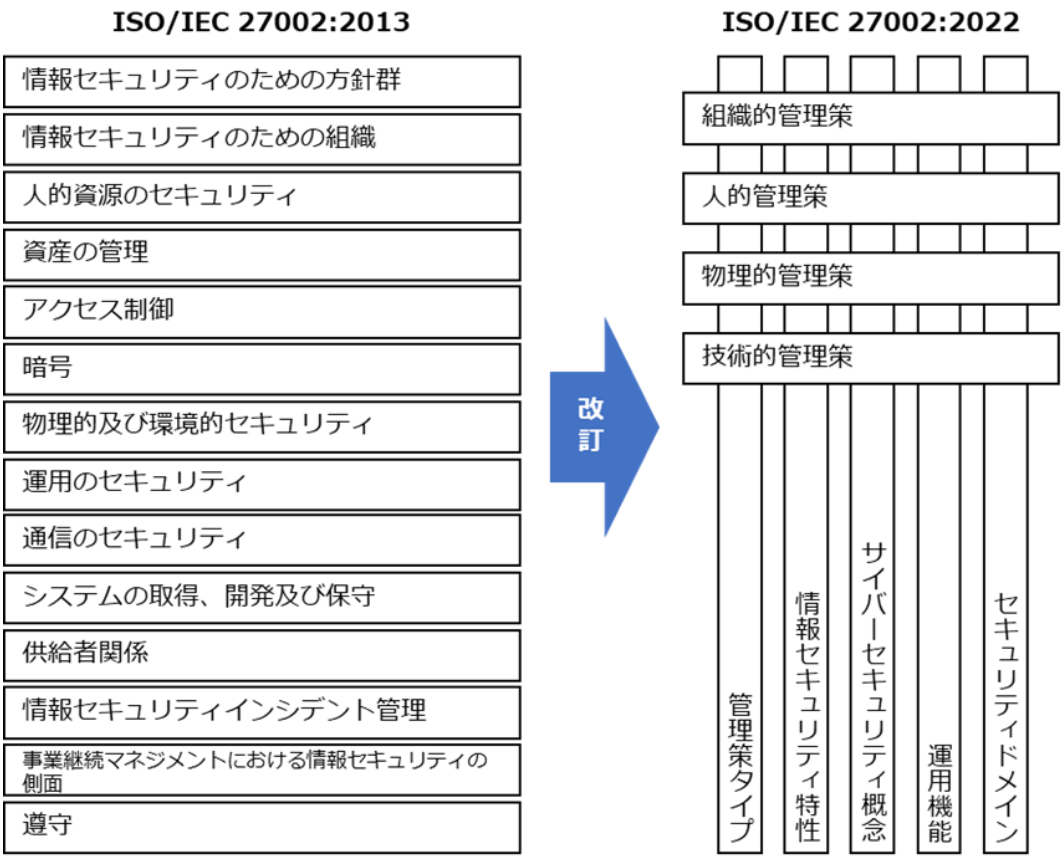
14 章の全体概要

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 111. 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

27-15. 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

27-16. 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

27-17. 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

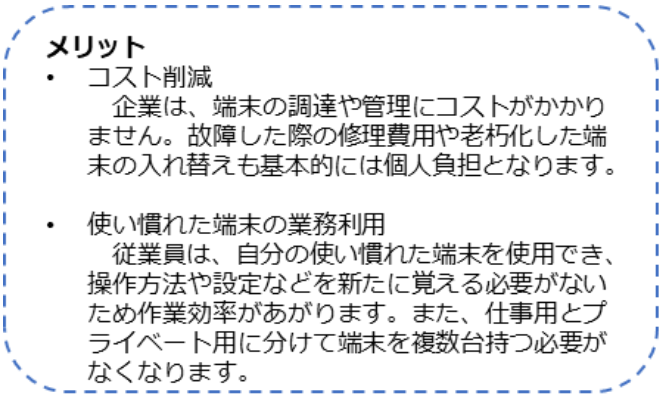
組織の物理的セキュリティを強化するための重要な実施項目を紹介しています。具体的には、以下のポイントが挙げられます。

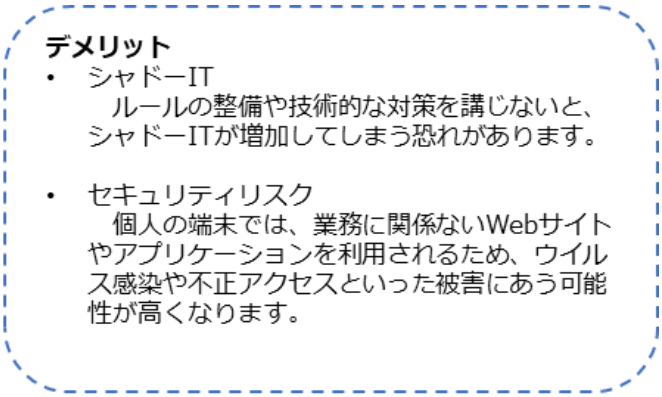
物理的管理策の項目	
7.1 物理的セキュリティ境界 7.2 物理的入退 7.3 オフィス、部屋及び施設のセキュリティ 7.4 物理的セキュリティの監視 7.5 物理的及び環境的脅威からの保護 7.6 セキュリティを保つべき領域での作業 7.7 クリアデスク・クリアスクリーン	7.8 装置の設置及び保護 7.9 構外にある資産のセキュリティ 7.10 記憶媒体 7.11 サポートユーティリティ 7.12 ケーブル配線のセキュリティ 7.13 装置の保守 7.14 装置のセキュリティを保った処分又は再利用

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。





- **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

27-18. 第 18 章. 技術的対策

18-1. 作成する候補となる実施手順書類について
18-2. 技術的対策として重要となる実施項目
18-3. 実施手順を適用するセキュリティ概念
18-4. インシデント対応

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	
8.9 構成管理	8.26 アプリケーションのセキュリティの要求事項
8.10 情報の削除	
8.11 データマスキング	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
8.12 データ漏えいの防止	
8.13 情報のバックアップ	8.28 セキュリティに配慮したコーディング
8.14 情報処理施設の冗長性	8.29 開発及び受入れにおけるセキュリティ試験
8.15 ログ取得	8.30 外部委託による開発
8.16 監視活動	8.31 開発環境、試験環境及び運用環境の分離
8.17 クロックの同期	8.32 変更管理
8.18 特権的なユーティリティプログラムの使用	8.33 試験情報
	8.34 監査試験中の情報システムの保護

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

27-19. 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

27-20. 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/1fc6722a/20240605_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/9462b2d8/20240605_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/d85eeb55/20240605_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

27-21. 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/d85eeb55/20240605_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

27-22. 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

27-23. 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。

①IT・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/nq6ept00000014lt-att/youkou_ver5_3.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

27-24. 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、内閣サイバーセキュリティセンター（NISC）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、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.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
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

27-25. 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.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

第28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。

28-1. 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="10">・「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 1.0 版	https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd
JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」	https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
ISO/IEC 27002:2022	https://www.iso.org/standard/75652.html

実施手順を具体的に実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 112. 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	https://www.digital.go.jp/assets/contents/node/bas

ライン	ic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/1fc6722a/20240605_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/d85eeb55/20240605_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/20241009_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/20241009_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 2024 について	https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/2024_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/b

	24ac613/20230609_policies_priority_outline_05.pdf
Society5.0	https://www8.cao.go.jp/cstp/society5_0
サイバーセキュリティ 2024 の概要	https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf
サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ	https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
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 2.0	https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
DX 白書 2023	https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針	https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
情報通信白書 令和 6 年版	https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/00zentai.pdf
製造分野の DX 事例集	https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf
「DX Selection 2023」選定企業レポート	https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf
セキュリティインシデント事例	
情報セキュリティ白書 2023	https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024	https://www.ipa.go.jp/security/10threats/10threats2024.html
サイバー攻撃対応事例	https://security-portal.nisc.go.jp/dx/provinatack.html
サイバー攻撃を受けた組織における対応事例集 （実事例における学びと気づきに関する調査研究）	https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
コンピュータウイルス・不正アクセスの届出事例［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 4 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）	https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
2021 年度 中小企業における情報セ	https://www.ipa.go.jp/security/reports/sme/ug65p90000019

キュリティ対策に関する実態調査 -事例集-	djm-att/000098149.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.nisc.go.jp/dx/pdf/about_plussecurity.pdf
サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き～ ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第 1.1 版	https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf
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	https://www.ipa.go.jp/archive/jinzai/skill-

ラム－レベル 1 を目指して－	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 10 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

ISO/IEC TR 13335-1
https://www.iso.org/standard/39066.html
ISMS 推進マニュアル活用ガイドブック 2022 年 1.0 版
https://msqa.actibookone.com/content/detail?param=eyJjb250ZW50TnVtIjo3ODgwMSwiY2F0ZWdvcnlOdW0iOjEwNzI0fQ==&pNo=1

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.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/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/1fc6722a/20240605_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/d85eeb55/20240605_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 2024

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/decision0621.html

デジタル社会の実現に向けた重点計画
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf
中堅・中小企業等向け デジタルガバナンス・コード 実践の手引き 2.0
https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf
サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ
https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf
サイバーセキュリティ 2024
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf
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.nisc.go.jp/pdf/council/cs/dai09/09shiryou07.pdf
情報セキュリティ白書 2023
https://www.ipa.go.jp/publish/wp-security/2023.html
情報セキュリティ 10 大脅威 2024
https://www.ipa.go.jp/security/10threats/10threats2024.html
情報通信白書令和 3 年版（総務省）
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r03/pdf/01honpen.pdf
DX 白書 2023
https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf
攻めの IT 活用指針
https://www.smrj.go.jp/supporter/tool/guidebook/guidebook1/fbrion000000206n-att/guide4youshiki_1.pdf
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
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
インターネットの安全・安心ハンドブック Ver.5.00
https://security-portal.nisc.go.jp/guidance/handbook.html
テレワークセキュリティガイドライン第 5 版
https://www.soumu.go.jp/main_content/000752925.pdf
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/press/2022/03/20230324002/20230324002-1.pdf
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
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
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/9462b2d8/20240605_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/nq6ept00000014lt-att/youkou_ver5_3.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
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
ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド
https://isms-society.stores.jp/items/632a57a42e7452256400d84b
ISMS 推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応 1.0 版
https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd

JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」
https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000
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
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/20241009_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/20241009_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
経済財政運営と改革の基本方針 2024 について
https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2024/2024_basicpolicies_ja.pdf
サイバーセキュリティ 2024 の概要
https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024_gaiyou.pdf
情報通信白書 令和 6 年版
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/pdf/00zentai.pdf
製造分野の DX 事例集
https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf
「DX Selection 2023」選定企業レポート
https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf
サイバー攻撃を受けた組織における対応事例集（実事例における学びと気づきに関する調査研究）
https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf
コンピュータウイルス・不正アクセスの届出事例［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 4 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf
2021 年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-
https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf
「プラス・セキュリティ知識」について
https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf
サイバーセキュリティ経営ガイドライン Ver2.0 付録 F サイバーセキュリティ体制構築・人材確保の手引き ～ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～ 第 1.1 版
https://www.meti.go.jp/policy/netsecurity/downloadfiles/tekibihontai1.1r.pdf

■AI

Artificial Intelligence の略。

「AI（人工知能）」という言葉は、昭和 31 年に米国の計算機科学研究者ジョン・マッカーシーが初めて使った言葉。昭和 25 年代後半から昭和 35 年代が第一次 AI ブーム、昭和 55 年代が第二次 AI ブーム、現在は平成 20 年代から始まる第三次 AI ブームである（近年の大規模言語モデルなどの登場を契機に、第四次 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

■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

■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

■DDoS 攻撃（ディードスこうげき）

Distributed Denial of Service Attack の略。攻撃者が複数のコンピュータを操作し、標的となるコンピュータに対して同時に大量の問い合わせを送ることにより、過剰な負荷をかけてサービスを利用できなくする攻撃手法

■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

■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

■eKYC

electronic Know Your Customer の略称。オンラインで完結可能な本人確認方法のこと

■G ビズ ID

行政手続きなどにおいて手続きを行う法人を認証するための仕組み。1 つの ID・パスワードで本人確認書類なしにさまざまな政府・自治体の法人向けオンライン申請が可能になる

■ICSCoE 中核人材育成プログラム

平成 29 年 4 月に独立行政法人情報処理推進機構（IPA）内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence, ICSCoE）

が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

■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

■IDS

Intrusion Detection System の略。不正アクセスや異常な通信を検知して管理者に通知するシステムのこと。IPS と異なり、不正アクセスや異常な通信をブロックする機能はない

■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

■IPS

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

IPS は、異常を検知した場合、管理者に通知するに加えて、その通信を遮断する

■IP アドレス

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

■ISAC

Information Sharing and Analysis Center の略。業界内での情報共有・連携を図る組織のこと。国内では、金融や交通、電力、ICT などの分野に ISAC がある。ICT-ISAC では、ICT 分野の情報セキュリティに関する情報（インシデント情報を含む。）の収集・調査・分析を行っている

■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

■ISP

個人や企業などに対してインターネットに接続するためのサービスを提供する事業者

のこと。ユーザーは ISP と契約し、回線を用いて ISP が運営するネットワークに接続することで、インターネット上のサーバなどへアクセスできる

■IT リテラシー

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

■JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討やアドバイスなどを、技術的な立場から行っている組織。政府機関や企業などから独立した中立の組織として、日本における情報セキュリティ対策活動の向上に積極的に取り組んでいる

■JVN

Japan Vulnerability Notes の略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと

■KPI

Key Performance Indicator の略。目標・戦略を実現するために設定した具体的な業務プロセスをモニタリングするために設定される指標（業績評価指標：Performance Indicators）のうち、特に重要なもの

■LockBit2.0

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

■MAC アドレス

Media Access Control address の略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器や PC、ルータなどについている固有の識別番号で、一般的に 12 桁の 16 進数で「00-00-00-XX-XX-XX」などと表される

■NISC

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

■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

■NTP

Network Time Protocol の略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている

■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

■PJMO

Project Management Office の略。プロジェクトの進捗管理やタスク管理などを行う組織のこと。プロジェクト管理を行うチームや担当者を指す。

例えば、プロジェクト管理を行うチームは、情報システム部門の担当者に加え、実務部門の担当者、調達担当者、業務委託先が決定した後はその担当者も含めた体制で構成する

■PMO

Project Management Office の略。（企業組織やプロジェクト規模によっては、Program Management Office、Portfolio Management Office とも呼ばれる。）組織全体のプロジェクトを横断的に管理する体制を指す。

政府ガイドラインでの PMO は、府省全体の管理となっているが、一般企業においては、企業全体のプロジェクトの管理と読み替えられる。

PJMO が個々のプロジェクト計画を定めるのに対し、PMO は全プロジェクトについて、横断的に管理・支援を行う（例：計画、予算、執行管理、PJMO 支援など）

■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

■RPA

Robotic Process Automation の略。定型的な業務をソフトウェアのロボットにより自動化すること

■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

■SBOM（エスボム）

Software Bill of Materials の略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOM は、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOM は、ソフトウェアのリスクを把握・管理するのに役立つ

■SDP

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

■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

■SLA

Service Level Agreement の略。サービス提供者と利用者の間で結ばれるサービスの品質に関して合意する契約のこと。サービスを提供する事業者が利用者に対して、どの程度の品質を保証できるのかを明示したもの

■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

■SSL/TLS

Web サーバと Web ブラウザとの通信において、データを暗号化して送受信する仕組みのこと。これにより、通信の途中で情報の盗聴・改ざんや、なりすましを防ぐことができる。過去には SSL が使われていたが、脆弱性が発見されたため、TLS（v.1.2 以降）への移行が進んでおり、今では SSL は使われなくなってきている。しかし、歴史的経緯で SSL の用語が広く普及しているため、本テキストでは「SSL/TLS」と表記する

■SWG

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

■VPN（Virtual Private Network）

Virtual Private Network の略。インターネット上で安全性の高い通信を実現するための手法。通信データを暗号化し、送信元から送信先までの通信を保護することにより、盗聴やデータの改ざんを防ぐ。VPN（Virtual Private Network）を使用することによって、ユーザーは物理的に独立した専用線で通信しているかのような安全な通信を行うことができる

■WAF（ワフ）

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

■WAN

Wide Area Network の略。広義には、広い地域をカバーするネットワークのことで、インターネットとほぼ同義の言葉として使われる。

一方、狭義には、物理的に離れた場所にある LAN（オフィスのフロアや建物内など狭いエリアで構築されたネットワーク）同士を接するネットワークを指し、特定のユーザーしかアクセスできない。このプライベートな WAN を構築する場合には、通信事業者に依頼する必要がある

■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

■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により、システムの再構築や運用改善の参考情報となる

■暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること

■アンダーグラウンドサービス

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

■イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと

■インターネットバンキング

インターネットを利用して銀行との取引を行うサービスのこと。銀行の窓口や ATM に出向かなくても、スマートフォンやパソコンなどを使って、いつでも利用可能な時間帯に振り込みや残高照会などの取引を行うことができる

■ウイルス定義ファイル（パターンファイル）

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

■エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと

■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）

■改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT 分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為

■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

■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

■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

■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

■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

■クラッキング

悪意を持って情報システムに侵入し、データの改ざん・機密情報の盗み出し・サーバ攻撃・情報システムの破壊などの行為

■クリーンインストール

すでにインストールされている OS を削除した上で、新しく OS を再インストールする方法のこと。記憶領域にあるデータはすべて消去されるので、データはバックアップから復元する必要がある

■限定提供データ

不正競争防止法で次のように定義されている。「業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、および管理されている技術上または営業上の情報（秘密として管理されているものを除く。）をいう。」

■個人情報保護委員会

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

■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

■コンパイル

プログラミング言語で書かれたプログラムを機械語に変換する作業

■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。

■サイバーセキュリティお助け隊サービス制度

「サイバーセキュリティお助け隊サービス」は、中小企業のセキュリティ対策に不可欠な各種サービスをワンパッケージにまとめた、民間事業者による安価なサービス。独立行政法人情報処理推進機構（IPA）は中小企業向けセキュリティサービスが満たすべき基準を設定しており、同基準を充足するサービスに「お助け隊マーク」を付与し、同サービスの普及促進活動を行っている

■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

■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

■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

■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

■磁気データ消去装置

ハードディスクに強力な磁気を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる

■ジャーニーマップ

一人のユーザーが目的を達成するための道のり（プロセス）を表に表したもの。

カスタマージャーニーマップともいう

■シャドーIT

従業員が業務に使用する IT 機器やサービスのうち、企業が把握していないものを指す。具体的には、普段プライベートで使用しているオンラインストレージといったクラウドサービス、個人所有のデバイスなどで、組織の許可なく業務に利用しているもの

■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

■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

■情報セキュリティの 3 要素「CIA」

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

■真正性

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

■信頼性

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

■スクリーンセーバ

離席時に PC の画面の内容を盗み見されることを防ぐ機能のこと。PC に対して一定時間ユーザーによる操作がなかった場合、自動的にアニメーションや写真などを表示し、作業中の情報を見せないようにする

■スクリーンロック

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

■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

■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

■責任追跡性

情報資産に対する参照や変

更などの操作を、どのユーザーが行ったものかを確認することができる特性

■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

■セキュリティ・キャンプ

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

■セキュリティホール

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

■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

■ゼロデイ攻撃

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

■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

■ソフトウェアライブラリ

プログラムにおいてよく利用される機能を切り出し、再利用しやすいようにまとめたもので、プログラム作成のための部品のこと。ライブラリを利用することで、1 から作る必要がなくなり、効率的に開発を行うことができる

■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」

■ダークウェブ

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

■多要素認証

多要素認証は、サービス利用時において利用者の認証を行うために、3 つの要素（①利用者だけが知っている情報②利用者の所有物③利用者の生体情報）のうち、少なくとも 2

つ以上の要素を組み合わせて認証する安全性が高い認証方法。例えば、利用者が知っている情報としてはパスワード、利用者の所有物としては、スマートフォンの電話番号を用いたメッセージ認証、利用者の生体情報としては指紋認証や顔認識などがある。また、近年では FIDO2 と呼ばれる、デバイスを使用したパスキーによる認証により、パスワードレスでの認証が広まっている

■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

■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

■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

■デジタル情報

0、1、2 のような離散的に（数値として）変化する量で表現できる情報のこと。一般的にコンピュータ内部では「0」と「1」の 2 進数で表現されている。デジタル情報は劣化することがなく、整理・検索が容易であるという特徴がある

■デプロイ

実行ファイルをサーバ上に配置することで、ユーザーが利用できるようにすること

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと

■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

■ハウジングサービス

データセンターのラック（サーバを収容する鍵のついた棚）とサーバに接続する回線や電源を貸し出すサービスのこと。自社が所有しているサーバを、物理的にセキュリティが強固なデータセンターに設置し、運用できるため、セキュリティを強化できるメリットがある

■ビジネスインパクト分析

災害など不測の事態によって業務やシステムが停止した場合に、会社の事業に与える影響度を評価すること。BCP（事業継続計画）を立てる上で実行する必要がある

■ビジネスメール詐欺

攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などの原因となる攻撃。BEC（ベック）Business Em

ail Compromise とも略される

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようにする特性

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルスつきメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている

■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

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンの OS に付随しているもの、セキュリティソフトウェアについているもの、専用のハードウェアになっているものなど形態はさまざまである

■ファイル共有ソフトウェア

複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェアのこと。不特定多数でファイルを共有するソフトウェアは、自動的にファイルを送受信する仕組みであるため、ウイルスの感染によって、公開したくないファイルがインターネットに流出するトラブルなどが多く発生している。不特定多数でファイルを共有するファイル共有ソフトウェアは、使用を禁止する必要がある

■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

■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

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元の IP アドレスによって、犯人が特定されてしまう可能

性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することにより、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

■ブラックマーケット

広義には、不法な取引が行われる市場を指す。不正に入手した個人情報などを売買するインターネット上の市場（闇市）

■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

■プロキシ

クライアントとサーバの中間で、両者の通信を中継する役割を担うサーバのこと。

プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Web サーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる

■ブロックチェーン

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

■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

■ペルソナ分析

理想とする顧客像を具体化し、典型的なユーザーのプロファイル分析をすること

■ベンダーロックイン

ソフトウェアの機能改修やバージョンアップ、ハードウェアのメンテナンスなど、情報システムを使い続けるために必要な作業を、それを導入した事業者以外が実施することができないために、特定の事業者（ベンダー）を利用し続けなくてはならない状態のこと

■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

■ミドルウェア

OS とアプリケーションの中間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやり取りをミドルウェアが担うことで複雑な処理を行うことができる

■ミラサポコネクト

ビッグデータを活用して事業を伸ばしたい中小企業を応援するための「ミラサポコネクト構想」をもとにした、行政、

支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供するための、官民データ連携基盤

■無線 LAN

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

■無停電電源装置

UPS とも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる

■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

■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

■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

■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

■リモートデスクトップ接続

パソコン、タブレット、スマートフォンなどのデバイスを使用して、遠隔地から特定のパソコンに接続する方法