

令和5年度 中小企業サイバーセキュリティ対策 継続支援事業

全体総括

サイバーセキュリティ
人材育成
社内体制整備支援

目次

第19章. 総括編

19-1. 全体要旨

19-1-1. テキストの活用

19-1-2. 中小企業の情報セキュリティ対策

19-2. 各章のポイント

19-2-1. 第1章. デジタル時代の社会とIT情勢

19-2-2. 第2章. 事例を知る：重大なインシデント発生から課題解決まで

19-2-3. 第3章. サイバーセキュリティの基礎知識

19-2-4. 第4章. 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

19-2-5. 第5章. デジタル社会の方向性と実現に向けた国の方針

19-2-6. 第6章. サイバーセキュリティ戦略および関連法令

19-2-7. 第7章. セキュリティフレームワーク

19-2-8. 第8章. セキュリティ対策基準の策定

19-2-9. 第9章. 管理策のテーマと属性

19-2-10. 第10章. 脅威、脆弱性、リスクの定義と関係性

19-2-11. 第11章. リスクマネジメント

19-2-12. 第12章. 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

19-2-13. 第13章. ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

19-2-14. 第14章. 組織的管理策

19-2-15. 第15章. 人的管理策

19-2-16. 第16章. 物理的管理策

19-2-17. 第17章. 技術的管理策

19-2-18. 第18章. セキュリティ対策状況の有効性評価

19-3. 読者に今後行ってほしいこと

19-3-1. 今後のアクション

おわりに

引用文献・参考文献・用語集

第19章. 総括編

19-1. 全体要旨

19-2. 各章のポイント

19-3. 読者に今後行ってほしいこと

章の目的

第19章では、各章のポイントを振り返り、テキスト読後に実施してほしいことや、テキストの活用ポイントについて学ぶことを目的とします。

主な達成目標

- 各章ごとに振り返り、重要なポイントを再確認し、その概要を理解すること。
- 本テキストに記載の実施手順を活用し、今後、読者が自組織においてセキュリティ対策を実践するために必要な考え方、参考になる文献を把握すること。
- 情報セキュリティ担当者、情報システム管理者、経営者など、それぞれの立場で担うべき本テキストの活用方法を理解すること。

19-1-1. テキストの活用

活用のポイント

本テキストを通してセキュリティ対策を実践するために、自組織のレベルに応じて、認識すべき事項を把握した上で、参考となる章を選択した活用法が効果的です。以下のアクションに沿って本テキストを活用してください。

1. 「DXの理解から対策の実践まで」のポイントを**再認識する**



2. 経営者を含めた関係者と**共有する**



3. 経営者のリーダーシップによって**社内体制を確立する**



4. 具体的なアクションを起こして**一歩ずつ実践する**

19-1-1. テキストの活用

1. 「DXの理解から対策の実践まで」のポイントを再認識する

- 「DXの理解から対策の実践まで」の各章の内容は以下の通りです。

| DXの推進の考え方の把握 | |
|-----------------------|-------------------------------------------------------------------------------------------|
| 第1章 | 現代社会のITに関する情勢、Society5.0やDXについて紹介 |
| 第5章 | 政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について紹介 |
| セキュリティ対策の全容の認識 | |
| 第2章 | 近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通じて把握し、それらの脅威に対する対策や、実際に被害にあった際の対応方法を紹介 |
| 第3章 | サイバーセキュリティの基本的な知識や対策や、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を紹介 |
| 第4章 | これからの企業経営で必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資、経営投資としてのサイバーセキュリティ対策の重要性を紹介 |
| 第6章 | NISCによるサイバーセキュリティ戦略を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性、サイバーセキュリティに関連する法令（個人情報保護法とGDPR）について紹介 |
| 第7章 | ISMSをはじめとしたサイバーセキュリティ対策における代表的なフレームワークの特徴を紹介 |
| 第8章 | ISMSを前提としたサイバーセキュリティ対策における基準を3段階にレベル分けし、各基準の手法を紹介 |
| 第9章 | ISO/IEC 27002における管理策の分類と構成について紹介 |
| 第10章 | ISO/IEC 27000に記述されている「リスク」、「脅威」、「脆弱性」、「管理策」といった用語の定義、それらの用語の関係性、脅威や脆弱性の識別方法を紹介 |
| 自組織でのセキュリティ対策の実施項目の認識 | |
| 第11章 | リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を紹介 |
| 第12章 | セキュリティインシデント事例を参考にクイックアプローチと、ガイドラインやひな形などの資料を参考にベースラインアプローチにおける対策基準・実施手順の策定方法を紹介 |
| 第13章 | 情報セキュリティマネジメントシステム（ISMS）のフレームワークを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成する網羅的アプローチについて紹介 |
| 自組織として実践準備 | |
| 第14章 | 情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、組織的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介 |
| 第15章 | 情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、人的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介 |
| 第16章 | 情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、物理的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介 |
| 第17章 | 情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則として、技術的管理策を用いた「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について紹介 |
| 第18章 | セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組みである監査について紹介 |

19章. 総括編 19-1. 全体要旨

19-1-1. テキストの活用

2. 経営者を含めた関係者と共有する

■ 本テキストの「第19章. 総括編」をエグゼクティブサマリとして活用してください。記載内容を理解し、経営者および他関係者と共有します。

3. 経営者のリーダーシップによって社内体制を整備する

■ Security by Designの観点で、ITの導入（企画・計画・仕様策定・調達・運用・保守など）を実践するためのIT人材を育成します。

人材育成の指針を検討する際は、デジタルスキル標準に示された指針を参考にすることが有効です。デジタルスキル標準は、「DXリテラシー標準」と「DX推進スキル標準」の2種類で構成されています。

| デジタルスキル標準 | DXリテラシー標準 | ビジネスパーソン全体がDXに関する基礎的な知識やスキル・マインドを身につけるための指針 ※DXを利用する立場の方向け |
|-----------|-----------|---------------------------------------------------------------|
| | DX推進スキル標準 | 企業がDXを推進する専門性を持った人材を確保・育成するための指針 ※DXを推進する立場の方向け |

経営層をはじめ、法務や広報といった、必ずしもITやセキュリティに関する専門知識や業務経験を有していない人材には、プラス・セキュリティ（自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力）を習得させることが重要です。実践にあたっては、関係機関が提供している資料や市販の参考書を参考にしてください。

参考文献) ・デジタルスキル標準Ver.1.1 2023年8月（出典：IPA）

・「プラス・セキュリティ知識」とは？（出典：経済産業省）

4. 具体的なアクションを起こして一歩ずつ実践する

■ Security by Designを実践します。DX化、具体的なIT導入にあたって、セキュリティ対策を含めた実践を行います。

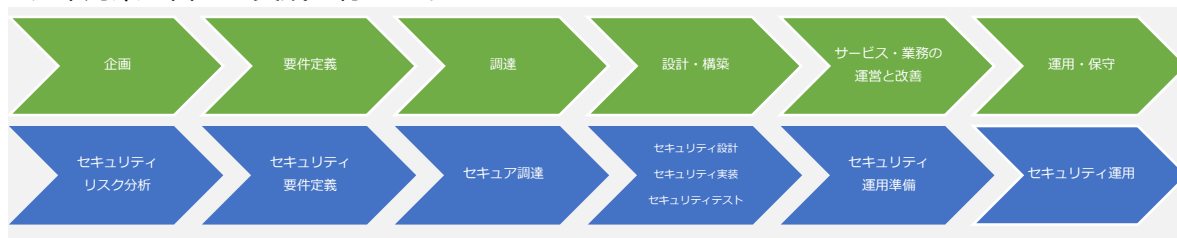


図72. IT導入プロセスにおけるセキュリティ対策の実施タイミング

実践にあたっては、関係機関が提供している資料、市販の参考書を参考にしてください。
参考文献) ・セキュリティ・バイ・デザイン導入指南書（出典：IPA）

| 実践のために参考となる文献（参考文献） | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デジタルスキル標準Ver.1.1 2023年8月 | https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf |
| 「プラス・セキュリティ知識」とは？ | https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf |
| セキュリティ・バイ・デザイン導入指南書 | https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf |

19-1-2. 中小企業の情報セキュリティ対策

これまでの振り返り

本テキストでは、中小企業のセキュリティを担う方々への育成のため、サイバーセキュリティ関連の情報や、実践的なセキュリティ対策について解説してきました。

第19章では、これまでの各章のポイントをまとめて振り返りつつ、テキストを読んだ後に実施してほしいことや、テキストの活用ポイントについて説明します。

本章を通して、それぞれの対策における実施概要を再認識していただきたいと思います。また、具体的な対策を講じるにあたっては、本テキストで参考文献としている資料などを入手し、詳細な内容を把握した上で実施していただきたいと思います。

| テキストの概要 | |
|--------------------|------------------------------------------------------------------------------------------------|
| 第1回 (第1章～第3章) | 情報セキュリティ白書、情報セキュリティ10大脅威、最近の事例、Security Actionについて紹介し、現代社会のIT情勢や、サイバー攻撃の傾向、脅威への対処方法について解説しました。 |
| 第2回 (第4章) | 企業経営の観点で、ITの普及によるサプライチェーンの変化や、IT活用の課題、「守り」と「攻め」という2種類のIT投資、サイバーセキュリティ確保の重要性について解説しました。 |
| 第3回 (第5章～第6章) | 日本政府がDXによってどのような社会を目指しているのか、サイバーセキュリティをどのように実現しようとしているのかについて解説しました。 |
| 第4回 (第7章) | サイバーセキュリティ対策におけるフレームワークについて、特にISMS、CSF、CPSF、サイバーセキュリティ経営ガイドラインについてピックアップして解説しました。 |
| 第5回 (第8章～第10章) | ISMSを前提に、セキュリティ対策基準とその策定方法、セキュリティ対策を示した管理策、「リスク」「脅威」「脆弱性」とは何かについて解説しました。 |
| 第6回 (第11章) | リスクを管理し、損失を回避、低減するためのリスクマネジメントに関して、その意義や、リスクアセスメントやリスク対応についてのプロセスを解説しました。 |
| 第7回 (第12章～第13章) | セキュリティ対策基準や、その具体的な実施手順を策定するにあたってのアプローチ方法として、クイックアプローチ、ベースラインアプローチ、網羅的アプローチを解説しました。 |
| 第8回 (第14章～第15章) | セキュリティ対策の具体的な規則としての「対策基準」と、その具体的な方法である「実施手順」について、組織的管理策、人的管理策をもとに解説しました。 |
| 第9回 (第16章～第18章) | セキュリティ対策の具体的な規則としての「対策基準」と、その具体的な方法である「実施手順」について、物理的管理策、技術的管理策をもとに解説し、対策状況の評価として監査についても解説しました。 |

19章. 総括編

19-2. 各章のポイント

19-2-1. 第1章. デジタル時代の社会とIT情勢

1-1. デジタル時代の社会変革とIT情勢の関係性

章の目的

第1章では、現代社会のITに関する情勢を学ぶことを目的とします。また、日本の政府がSociety5.0の方向性を示す中で、企業がビジネスを発展させるためにDX（デジタルトランスフォーメーション）を推進していく重要性を明確にすることを目的とします。

主な達成目標

□ ITに関する社会の動向を把握し、Society5.0とDXの関係性を理解すること。

主なキーワード 🔍
Society5.0、DX

要旨

1章の全体概要

現代社会は、急速な技術革新と経済のグローバル化によって大きな変化を迎えており、日本政府はSociety5.0という新たな社会モデルの実現を提唱しています。Society5.0では、デジタル技術を活用して社会の課題を解決し、人々の暮らしを向上させることが求められます。AI、ビッグデータなど最新技術が駆使され、効率的な社会システムや持続可能な産業構造の構築が進められます。Society5.0を実現するために、企業にはDX（データやデジタル技術を活用して、顧客視点で新たな価値を創出すること）の推進が求められています。

➤ 1-1. デジタル時代の社会変革とIT情勢の関係性

- 社会の現状と今後の動向
Society5.0という新たな社会モデルが提唱されており、実現するためには企業や組織がDXを進め、デジタル化を推進することが不可欠です。DXを進めるには、最新技術の知識、人材確保、セキュリティが重要になります。

訴求ポイント

章を通した気づき・学び

企業や組織は、社会の動向に関する情報を常に収集することが大切です。また、ビジネス環境の激しい変化に対応するためにDXを推進し、デジタル社会に適したビジネスモデル、組織、企業文化に変革していくことが必要です。

認識していただきたい実施概要

- ✓ 中小企業は、大企業と比べて人手や予算などの企業リソースが限定されており、ビジネス環境の激しい変化に対応するためには、DXを推進し新たなサービスを創造し、ビジネスを発展させることが重要です。
- ✓ データやデジタル技術を活用するためには、最新技術の知識、最新技術に精通した人材が必要です。安全にデータやデジタル技術を活用するために、セキュリティ対策を適切に行うことが重要です。

実践のために参考となる文献（参考文献）

デジタルガバナンス・コード2.0

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

19-2-2. 第2章. 事例を知る：重大なインシデント発生から課題解決まで

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

章の目的

第2章では、近年のサイバー攻撃の傾向や手法を、実際のインシデント事例など通して把握し、それらの脅威に対する対策や、実際にインシデントが発生した場合の対応方法について理解することを目的とします。

主な達成目標

- 近年のサイバー攻撃の傾向や手法を理解すること。
- 実際の被害事例を通して脅威に対する対策や予防方法を理解すること。
- 脅威の検知から、復旧・再発防止処置までの流れを理解すること。

主なキーワード

情報セキュリティ白書、情報セキュリティ10大脅威、ランサムウェア、サプライチェーン攻撃、テレワーク、脅威、インシデント、サイバー被害

要旨

2章の全体概要

情報セキュリティ白書、情報セキュリティ10大脅威、最近のインシデント事例をもとに脅威事例を紹介し、対策や対応方法を説明しています。中でも、ランサムウェアやサプライチェーン攻撃は特に深刻な問題となっています。これらの攻撃は、自社の業務だけでなく取引先からの信用にも悪影響を及ぼす可能性があることに注意する必要があります。近年の攻撃は企業の規模に関係なく行われるため、中小企業にとっても、セキュリティ対策は不可欠なものになっています。

➤ 2-1. 情報セキュリティの概況

「情報セキュリティ白書」や「情報セキュリティ10大脅威」を用いて、最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握し、適切な予防策や対策を講じることが大切です。

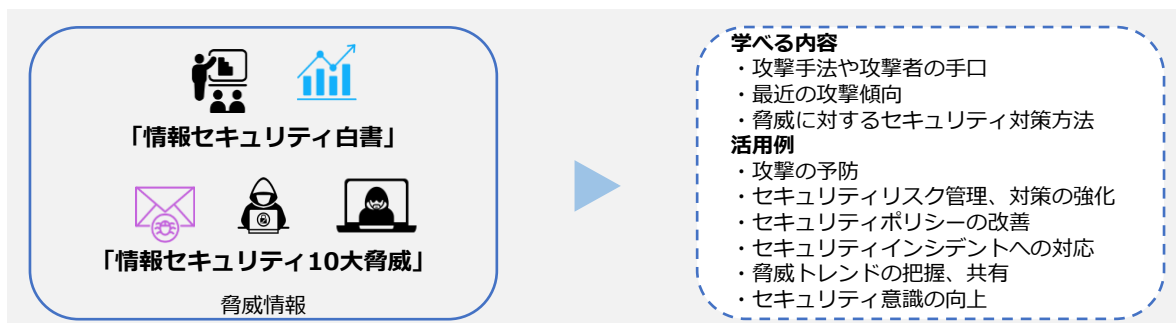


図73. 情報セキュリティ白書・情報セキュリティ10大脅威の活用方法

19-2-2. 第2章. 事例を知る：重大なインシデント発生から課題解決まで

➤ 2-2. 重大インシデント事例から学ぶ課題解決

脅威に対する対応策の策定や、現在使用しているリスク戦略の改善、セキュリティ意識を向上させるため、IoTデバイスへの攻撃、サプライチェーンを介した標的型メール攻撃、テレワーク環境での情報漏えい、ランサムウェアへの感染など、過去に発生したさまざまなインシデント事例から、何がうまく行かなかったのか、どのような手段が用いられたのか、どのような脆弱性が攻撃の対象となったのかなどを理解することが大切です。

➤ 2-3. 実際の被害事例からみるケーススタディ

実践的な問題解決に役立つスキルを養うため、不正アクセスやランサムウェアのインシデント事例を通じて、被害が起きた原因の分析内容、効果的なセキュリティ対策やベストプラクティスを紹介しています。

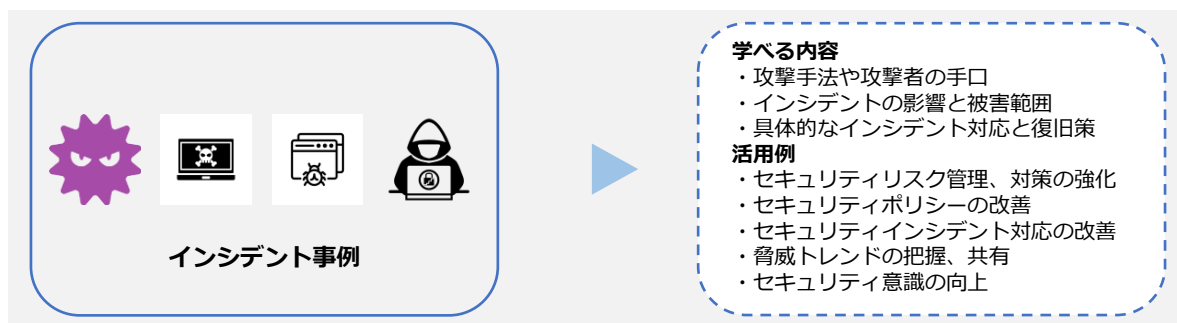


図74. インシデント事例を通じて学べる内容

訴求ポイント

章を通じた気づき・学び

最新の脅威・脆弱性情報、攻撃の傾向や手法、セキュリティリスクなどを把握し、適切な予防策や対策を講じることが大切です。また、インシデント事例を通して、自社でも起こり得るインシデントに対して適切な対応策を検討し、実施することが大切です。

認識していただきたい実施概要

- ✓ 最新の脆弱性や脅威情報、攻撃の傾向や手法からセキュリティリスクを把握し、適切な予防策や対策を講じるためには、情報セキュリティ白書や情報セキュリティ10大脅威を活用することが有効です。
- ✓ 脅威に対する対応策の策定や、現在使用しているリスク戦略の改善、セキュリティ意識の向上、今後起こり得るインシデントに対して適切な対応をするためには、過去のインシデント事例から対策方法を学ぶことが有効です。
- ✓ セキュリティ対策の必要性を理解するためには、インシデントが発生した原因や、対策・ベストプラクティスを学ぶことが有効です。

実践のために参考となる文献（参考文献）

情報セキュリティ白書2022 <https://www.ipa.go.jp/publish/wp-security/qv6pgp0000000vgi-att/000100472.pdf>

情報セキュリティ10大脅威 2023 https://www.ipa.go.jp/security/10threats/ps6vr70000009r2f-att/kaisetsu_2023.pdf

19-2-3. 第3章. サイバーセキュリティの基礎知識

- 3-1. 導入済と想定するセキュリティ対策機能
- 3-2. 各種資格試験から得るサイバーセキュリティの基礎知識
- 3-3. Security Action (セキュリティ対策自己宣言)
- 3-4. サイバーセキュリティアプローチ方法

章の目的

第3章では、サイバーセキュリティの基本的な知識や対策などについて振り返りつつ、自社のリスク状況や活用可能なリソースを考慮した、脅威に対する最適な対処方法を明確にすることを目的とします。

主な達成目標

- UTM、EDRの機能を再確認すること。
- サイバーセキュリティに関する基礎知識を身につける方法を確認すること。
- 企業が自ら実施できる基本的なセキュリティ対策を再確認すること。
- リスクと活用可能なリソースを考慮した脅威への対処方法を理解すること。

主なキーワード

UTM、EDR、情報処理技術者試験、SECURITY ACTION

要旨

3章の全体概要

UTM、EDRの機能や、ITやセキュリティに関する網羅的な知識の取得状況を確認するために有効な情報処理技術者試験を紹介しています。中小企業がセキュリティ対策を進めるにあたり、SECURITY ACTION (セキュリティ対策自己宣言) に取り組むことを推奨します。その後、サイバーセキュリティの脅威に対処するための3つの段階的なアプローチ手法を用いて対策を進めましょう。

➤ 3-1. 導入済と想定するセキュリティ対策機能

UTM、EDRの機能について振り返ります。



図75. UTM・EDRの概要図

19章. 総括編

19-2. 各章のポイント

19-2-3. 第3章. サイバーセキュリティの基礎知識

➤ 3-2. 各種資格試験から得るサイバーセキュリティの基礎知識

ITやセキュリティの知識を身につけることは重要です。従業員一人ひとりがITやセキュリティの知識を身につけることで、組織の安全な運営や、組織のセキュリティレベルの向上に繋がります。ITやセキュリティに関する網羅的な知識の取得状況を確認するために、情報処理技術者試験などを受験するとよいでしょう。

- ITパスポート試験 (IP)
- 情報セキュリティマネジメント試験 (SG)
- 基本情報技術者試験 (FE)

➤ 3-3. Security Action (セキュリティ対策自己宣言)

「SECURITY ACTION」に取り組むことで、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繋がります。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
- 5分でできる！情報セキュリティ自社診断
- 情報セキュリティ基本方針

➤ 3-4. サイバーセキュリティアプローチ方法

サイバーセキュリティの脅威に対処するために、段階的なアプローチ手法をとることが重要です。自社が直面しているリスク状況および活用できるリソースを考慮し、最適なアプローチ手法を選択することが大切です。

- LV1. クイックアプローチ
- LV2. ベースラインアプローチ
- LV3. 網羅的アプローチ

訴求ポイント

章を通した気づき・学び

ITや情報セキュリティの知識を身につけ、企業内外でセキュリティ専門の人材と協力できるようにすることが大切です。セキュリティ対策をはじめると同時に、SECURITY ACTIONに取り組む、従業員の意識を高め、対外的な信頼を向上させることが大切です。

認識していただきたい実施概要

- ✓ ITやセキュリティに関する網羅的な知識の取得状況を確認するために、情報処理技術者試験などを受験することが有効であること。
- ✓ 中小企業が情報セキュリティ対策に取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段階のアプローチがあること。

実践のために参考となる文献 (参考文献)

| | |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 試験区分一覧 | https://www.ipa.go.jp/shiken/kubun/list.html |
| SECURITY ACTION セキュリティ対策自己宣言 | https://www.ipa.go.jp/security/security-action/ |
| 情報セキュリティ5か条 | https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf |
| 5分でできる！情報セキュリティ自社診断 | https://www.ipa.go.jp/security/guide/sme/5minutes.html |

19-2-4. 第4章. 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

- 4-1. これからの企業経営に必要な観点：社会の動向
- 4-2. 守りのIT投資と攻めのIT投資
- 4-3. 経営投資としてのサイバーセキュリティ対策

章の目的

第4章では、これからの企業経営に必要な観点となる社会の動向、「守りのIT投資」や「攻めのIT投資」などのIT投資について理解することを目的とします。また、経営投資としてのサイバーセキュリティ対策の重要性を明確にすることを目的とします。

主な達成目標

- 社会の動向を把握し、現実社会とサイバー空間の繋がりを理解すること
- IT投資としての「守りのIT投資」と「攻めのIT投資」を理解すること
- 経営投資としてのサイバーセキュリティ対策の重要性を理解すること

主なキーワード

守りのIT投資、攻めのIT投資

要旨

4章の全体概要

社会の動向を踏まえ、企業がセキュリティ対策と同時に進めるべきIT活用について説明しています。従来の業務効率化やコスト削減といった守りのIT投資と、DXに向けた攻めのIT投資の特徴や違い、主要なデジタル技術の活用方法について簡潔に紹介しています。経営者主体のサイバーセキュリティ対策の必要性と要点を説明しています。

➤ 4-1. これからの企業経営に必要な観点：社会の動向

- 社会の動向や、現実社会とサイバー空間の繋がり、IT活用における課題を説明しています。
- 現実社会とサイバー空間の繋がり
現代社会では、技術の進化が速く、競争が激化しています。企業の経営戦略やビジネスモデルも変化しており、革新的なアイデアと素早い行動が求められています。さらなる経済発展と社会的課題の解決をするため、Society5.0が提唱されています。
 - IT活用における課題
日本社会がデジタル化で後れをとった理由と、現在日本においてDXの取組み状況がどのような状態かを確認するため、DXが進んでいる米国と比較します。

我が国がデジタル化で後れをとった6つの理由

1. ICT投資の低迷
2. 業務改革等を伴わない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

19-2-4. 第4章. 企業経営で重要となるIT投資と投資としてのサイバーセキュリティ対策

➤ 4-2. 守りのIT投資と攻めのIT投資

• 守りのIT投資と攻めのIT投資

「攻めのIT投資」では、ITを活用して既存のビジネスの変革、新たな事業展開や新しいビジネスモデルの創出を行うことによって、新規市場の創出、収益拡大、販売力のアップを目指します。一方、「守りのIT投資」では、ITによる業務の効率化やコスト削減を目指します。攻めと守りを意識し、両者のバランスをとることが大切です。

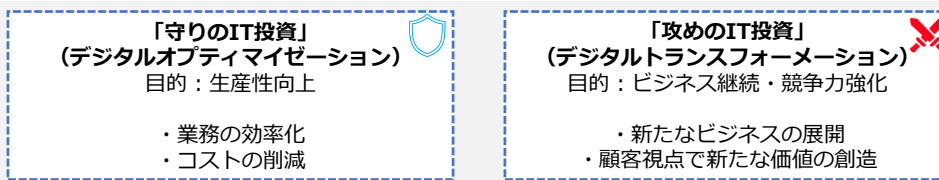


図76. 守りのIT投資・攻めのIT投資

• 次世代技術を活用したビジネス展開

自社の実現したいこと（将来のビジョン）から実現に必要な課題を明確にし、解決するためにデジタル技術の活用が求められます。最近では、AI、クラウド、チャットボットなどの新しい技術がビジネスで活用されるようになってきており、こうした新しい技術を含め、自社に適した技術やツールをうまく活用していくことが求められています。

➤ 4-3. 経営投資としてのサイバーセキュリティ対策

DX推進と並行してサイバーセキュリティの確保に取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、経営者が主体となって指揮をすることが大切です。経営者が重視すべきポイントは、次の3つです。

- ポイント①：ビジネスの継続・発展にはITの活用が不可欠
- ポイント②：ITの活用にはサイバー攻撃への対策が必要
- ポイント③：サイバーセキュリティ対策は経営者が自ら実行

訴求ポイント

章を通じた気づき・学び

Society5.0が提唱される中、企業はデジタル技術を用いてビジネスモデルを変革し、顧客視点で新たな価値を創出するDXを推進するため、「攻めのIT投資」を行うことが大切です。サイバーセキュリティ対策は、経営者が主体となって指揮をすることが大切です。

認識していただきたい実施概要

- ✓ 現実社会とサイバー空間の繋がりや、Society5.0などといった社会の動向を把握することが、これからの企業経営に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。

19-2-5. 第5章. デジタル社会の方向性と実現に向けた国の方針

5-1. 国の基本方針および実施計画の要約

5-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

章の目的

第5章では、政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル技術の活用やサイバーセキュリティ対策の方向性・課題について理解することを目的とします。

主な達成目標

- 国の基本方針にデジタルがどのように影響を与えており、それによりどのような社会を目指しているかを理解すること
- デジタル社会におけるサイバーセキュリティ対策の重要性を理解すること

主なキーワード

デジタル社会、DXの推進、サプライチェーン、DX

要旨

5章の全体概要

国によるデジタル社会に関する方針や政策、デジタル分野の取組みにおけるサイバーセキュリティの位置付けについて解説しています。政府が目指しているデジタル社会としてSociety5.0を取り上げ、DXについては事例を交えて中小企業の優位性を説明しています。

➤ 5-1. 国の基本方針および実施計画の要約

IT・セキュリティ関連の施策は、国の方針の1つである「経済財政運営と改革の基本方針」に沿った形で実施計画が策定されています。たとえば、2023年度の方針では「サプライチェーンの強靱化」、「DXの加速」が盛り込まれています。

➤ 5-2. 政府機関が目指す社会の方向性とサイバーセキュリティ課題

- デジタル社会の実現に向けた重点計画

政府は「経済財政運営と改革の基本方針」に基づき「デジタル社会の実現に向けた重点計画」を閣議決定しています。この重点計画の中の各分野における基本的な施策の4番目の「産業のデジタル化」では「中小企業のDX 推進」や「中小企業のデジタル化の支援」が盛り込まれています。

各分野における基本的な施策

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

19章. 総括編

19-2. 各章のポイント

19-2-5. 第5章. デジタル社会の方向性と実現に向けた国の方針

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

デジタル社会を実現していくための7つの戦略的な政策

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

また第5章では、政府が提唱しているSociety5.0とDXの推進についても解説しました。

• Society5.0

Society5.0では、IoTですべての人とモノが繋がり、知識や情報を共有することによって、これまでにない新たな価値を生み出すとともに、社会が抱えるさまざまな課題を解決の方向に導きます。一方で、Society5.0におけるサイバー空間の急激な拡大は、サイバー攻撃の対象が増えることを示しています。サイバー空間とフィジカル空間の相互作用により、サイバー攻撃がフィジカル空間にも影響を及ぼす可能性が高まります。

• DXの推進

DXの推進における中小企業の優位性について説明しています。中小企業の中には、DXを推進し、売上高を5倍、利益を50倍に増加させた企業が存在します。中小企業ならではの優位性を理解し積極的にDXに取り組むことで、大きく成長できる可能性があります。

中小企業がデジタルトランスフォーメーション推進における優位点

参考情報が豊富

DXを既に手掛けている中小企業や、デジタルトランスフォーメーションを順調に進めている企業のやり方を参考にすることができる

環境が整備されている

先行者や大企業などにより既に整備されたプラットフォームを利用し、新たなビジネスに取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。企業は自社のIT活用状況を認識しつつ、必要な知識・スキルを身につけた人材を育成・確保することが必要です。

認識していただきたい実施概要

- ✓ 政府が発表している国の基本方針や、国が目指している社会を実現するための計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題について学ぶこと。
- ✓ 中小企業ならではの優位性を理解し、積極的にDXに取り組むことが組織を成長させるために重要であること。

実践のために参考となる文献（参考文献）

| | |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 経済財政運営と改革の基本方針2023 | https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf |
| デジタル社会の実現に向けた重点計画 | https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabff870/b24ac613/20230609_policies_priority_outline_05.pdf |
| 中堅・中小企業等向けデジタルカバナンス・コード実践の手引き2.0 | https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf |

19-2-6. 第6章. サイバーセキュリティ戦略および関連法令

6-1. NISC : サイバーセキュリティ戦略

6-2. 関連法令

章の目的

第6章は、NISCの「サイバーセキュリティ戦略」を通じて、DXとサイバーセキュリティの確保を同時に推進する重要性について理解することを目的とします。また、サイバーセキュリティに関連する法令として、個人情報保護法とGDPRについて説明しています。

主な達成目標

- 日本におけるサイバーセキュリティに関する方針や施策について理解すること
- サイバーセキュリティに関する知識やスキルを身につける必要性について理解すること
- 個人情報関連の法令を理解すること

主なキーワード 🔍

サイバーセキュリティ戦略、DX with Cybersecurity、個人情報保護

要旨

6章の全体概要

サイバーセキュリティについては、NISCの「サイバーセキュリティ戦略」を紹介するとともに、DX with Cybersecurityの考え方について解説しています。デジタルの活用が進むとともに、サイバーセキュリティのリスクも高まっています。企業は自社のIT活用状況を認識しつつ、必要な知識・スキルを身につけた人材を育成・確保するとともに、適切なサイバーセキュリティ対策を実施することが重要です。

➤ 6-1. NISC : サイバーセキュリティ戦略

- サイバーセキュリティ戦略
国家レベルでサイバーセキュリティの確保に取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。
- 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り組みレベルに応じた対策を行うことが大切です。
- DX with Cybersecurity
DXとサイバーセキュリティ確保に向けた取り組みを同時に推進すること（DX with Cybersecurity）が不可欠になっています。中小企業がDX with Cybersecurityを推進するにあたり、人材やスキル不足などさまざまな課題が存在しています。これらの課題に対する対策として、「デジタルスキル標準（DSS）」、「プラス・セキュリティ」について説明しています。

19章. 総括編

19-2. 各章のポイント

19-2-6. 第6章. サイバーセキュリティ戦略および関連法令

- デジタルスキル標準 (DSS)
デジタルスキル標準 (DSS) では、すべてのビジネスパーソンがDXに関する基礎的な知識、スキル、マインドセットを身につけるための学習指針を「DXリテラシー標準」として策定しています。社員に対して、DXに関するリテラシーを身につけさせるための育成方法を検討する際に、指針として活用することができます。
- プラス・セキュリティ
プラス・セキュリティとは、「自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと」です。
サイバーセキュリティ体制を適切に機能させるため、経営者は、デジタル部門、事業部門、管理部門などの従業員にサイバーセキュリティに対する意識を高め、業務遂行に必要なセキュリティ対策を実施できる能力を身につけさせるよう育成することが大切です。具体的には、自社で実施しなければならないサイバーセキュリティ関連タスクの一部を担っていること、およびその責任・権限を組織として明確化し、担当者に自覚させることが重要です。

➤ 6-2. 関連法令

- 個人情報保護法
消費者や取引先から預かっている個人情報を適切に取扱うことは、企業の権利や利益を守ることに繋がる非常に重要な取組みとなります。
- 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となります。

訴求ポイント

章を通じた気づき・学び

日本政府が打ち出しているサイバーセキュリティ戦略を理解し、関連する知識やスキルを身につけることが大切です。

認識していただきたい実施概要

- ✓ サイバーセキュリティ戦略によって、国家レベルでのサイバーセキュリティの確保に取組む方針や目標が定められていることを理解すること。
- ✓ サイバーセキュリティ対策にかかる支出をやむを得ない費用とするのではなく、経営のために必要な投資と位置付け、自発的にサイバーセキュリティ対策に取組むことが重要であること。
- ✓ DXの推進と並行してサイバーセキュリティへの対策が求められる状況の中、必ずしもITやセキュリティに関する専門知識や業務経験を有していない者も、自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力 (プラス・セキュリティ) を身につけることが重要であること。
- ✓ サイバーセキュリティに関連する法令として個人情報保護法やGDPRがあり、個人情報レベルの高い情報として取扱うべきであること。

実践のために参考となる文献 (参考文献)

| | |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サイバーセキュリティ体制構築・人材確保の手引き (第2.0版) | http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf |
| デジタルスキル標準Ver.1.1 2023年8月 | https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf |
| 「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは? | https://www.gov-online.go.jp/useful/article/201703/1.html |

19-2-7. 第7章. セキュリティフレームワーク

7-1. セキュリティフレームワークの概要

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

7-3. NIST サイバーセキュリティフレームワーク (CSF)

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

7-5. サイバーセキュリティ経営ガイドライン

章の目的

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

主な達成目標

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

主なキーワード

セキュリティフレームワーク、ISMS

要旨

7章の全体概要

セキュリティ対策に関連するフレームワークの特徴や概要、そして各フレームワークの要素や要件について解説しています。セキュリティ対策は、やみくもに進めてしまうとかえって複雑になってしまい、余計に手間がかかり、内容に抜け漏れが発生する可能性があります。漏れなく効果的に対策を実施するために、企業はセキュリティフレームワークを使用し、自社の課題・目的に即した対応方針を選択することが重要です。

➤ 7-1. セキュリティフレームワークの概要

次のセキュリティフレームワークの概要、利用メリットについて説明しています。

- ISMS (情報セキュリティマネジメントシステム) [ISO/IEC27001, 27002]
- ISO/IEC27017
- CSF (サイバーセキュリティフレームワーク)
- CPSF (サイバー・フィジカル・セキュリティ対策フレームワーク)
- サイバーセキュリティ経営ガイドライン
- PCI DSS
- PMS (個人情報保護マネジメントシステム)
- CIS Controls
- ISA/IEC62443

➤ 7-2. 情報セキュリティマネジメントシステム (ISMS)

ISMSとは、組織の情報セキュリティリスクを適切に管理するための仕組みのことです。ISMSは、セキュリティフレームワークの中でも代表的なものです。ISMSが達成すべきことは、リスクマネジメントプロセスを適用することによって情報の機密性、完全性および可用性をバランスよく維持・改善し、リスクの適切な管理を実現し、信頼を利害関係者に与えることです。

19章. 総括編

19-2. 各章のポイント

19-2-7. 第7章. セキュリティフレームワーク

➤ 7-3. NIST サイバーセキュリティフレームワーク (CSF)

サイバーセキュリティフレームワーク (CSF) は、NISTが作成したサイバー攻撃対策に重点をおいたフレームワークであり、防御にとどまらず、検知・対応・復旧といったインシデント対応が含まれています。多様な企業に適用できるように要求事項が汎用的になっています。CSFは、組織がセキュリティ対策を継続的に改善するため、①コア（サイバーセキュリティ対策の一覧）、②ティア（対策状況を数値化するための成熟度評価基準）、③プロファイル（サイバーセキュリティ対策の現状とあるべき姿を記述するためのフレームワーク）の3つの要素で構成されています。

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

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

➤ 7-5. サイバーセキュリティ経営ガイドライン

サイバーセキュリティ経営ガイドラインは、経営者がサイバーセキュリティ対策を実行する際に認識すべき事項と、サイバーセキュリティ対策の責任者（CISOなど）に指示すべき事項を包括的にまとめています。経営者が主体となってサイバーセキュリティ対策を実施する際に参考にできます。

訴求ポイント

章を通した気づき・学び

セキュリティ対策を漏れなく効果的に実施するためには、セキュリティフレームワークを使用することが有効です。さまざまなセキュリティフレームワークがある中、自社の課題や目的に即したものを選択することが大切です。

認識していただきたい実施概要

- ✓ 効果的なセキュリティ対策の実施や、取引先や顧客からの信頼を向上させるためには、フレームワークに沿って対策を進めることが有効であること。
- ✓ セキュリティ対策を行うためのフレームワークは複数存在するが、まずは業種業態を問わずセキュリティ対策の全体の枠組みと、網羅的な対策項目を提示しているISMSをベースとし、必要に応じて業種業態や重点領域ごとに特に注力すべき内容が詳細化されている各種フレームワークで補完することが有効であること。

| 実践のために参考となる文献（参考文献） | |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISMS適合性評価制度 | https://isms.jp/doc/JIP-ISMS120-62.pdf |
| サイバーセキュリティ経営ガイドライン Ver3.0 | https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf |
| 政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート | https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf |

19-2-8. 第8章. セキュリティ対策基準の策定

8-1. 対策基準の策定

章の目的

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

主な達成目標

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

主なキーワード

セキュリティ対策基準、クイックアプローチ、ベースラインアプローチ、網羅的アプローチ

要旨

8章の全体概要

最初にセキュリティポリシーの構成（「基本方針」「対策基準」「実施手順・運用規則など」）について説明しています。企業が現在の状況や目標に合わせた「対策基準」を策定する際に活用できる、レベル感の異なる3つのアプローチ手法（LV.1 クイックアプローチ、LV.2 ベースラインアプローチ、LV.3 網羅的アプローチ）を紹介しています。

➤ 8-1. 対策基準の策定

• セキュリティ対策基準の概要

情報セキュリティポリシーは、「基本方針」「対策基準」「実施手順・運用規則など」で構成されます。「対策基準」を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせます。対策基準の内容を定める際は、網羅的なフレームワークを参考にすることが推奨されます。

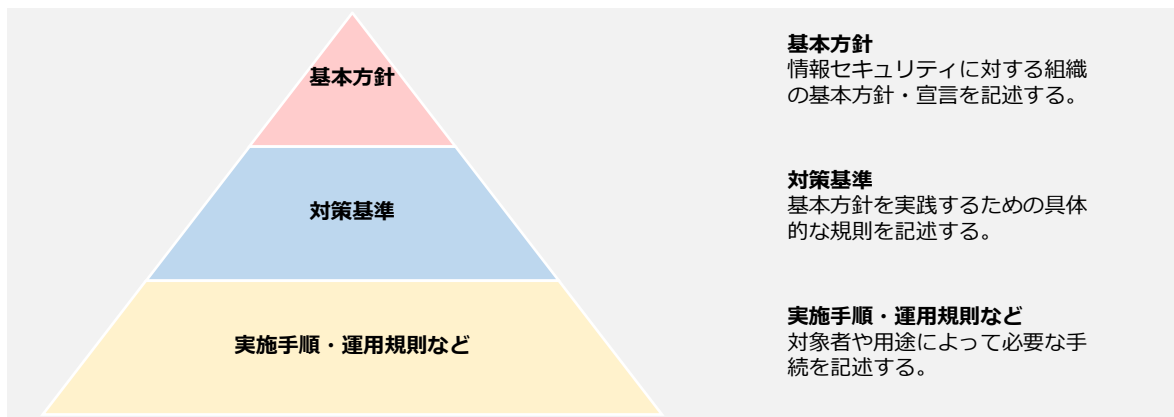


図77. 情報セキュリティポリシーの全体像

19章. 総括編

19-2. 各章のポイント

19-2-8. 第8章. セキュリティ対策基準の策定

- 対策基準策定のアプローチ方法
対策基準を作成するアプローチ方法には、レベル感の異なる3つの手法（LV.1 クイックアプローチ、LV.2 ベースラインアプローチ、LV.3 網羅的アプローチ）があります。

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

訴求ポイント

章を通した気づき・学び

状況に応じて適切なサイバーセキュリティ対策のアプローチ手法を選択し、セキュリティ対策の実施を内外に示すため、対策基準を策定することが大切です。

認識していただきたい実施概要

- ✓ 対策基準を外部に公開することで、セキュリティ対策の実施を内外に示し、説明責任を果たせること。
- ✓ 対策基準で記載する内容を具体的に実践するために、策定した対策基準に従って実施手順を作成することが重要であること。
- ✓ 対策基準の内容を定める際は、企業の現状や目標に応じてフレームワークを使用せずに「クイックアプローチ」「ベースラインアプローチ」を用いて策定できるが、網羅的なフレームワークであるISMSを参考に策定する「網羅的アプローチ」が推奨されること。

| 実践のために参考となる文献（参考文献） | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| サイバー攻撃対応事例 | https://security-portal.nisc.go.jp/dx/provinatack.html |
| 情報セキュリティ関連規程 | https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx |
| 自己点検チェックリスト | https://www.ppc.go.jp/files/pdf/Self_assessment_checklist.pdf |
| 情報セキュリティポリシーサンプル改版（1.0版） | https://www.jnsa.org/result/2016/policy/ |

19-2-9. 第9章. 管理策のテーマと属性

9-1. 管理策の分類と構成

章の目的

第9章では、ISO/IEC 27002における管理策（リスク対応のための対策）の分類と構成について理解することを目的とします。

主な達成目標

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

主なキーワード

管理策、ISO/IEC 27002

要旨

9章の全体概要

ISMSの管理策を示した規格であるISO/IEC 27002について説明しています。

➤ 9-1. 管理策の分類と構成

• 管理策：ISO/IEC 27002

管理策の数は、2013年版では14分野114項目でしたが、2022年版ではいくつかが統合されて82項目になり、新しく11項目が追加され、合計で93項目となりました。2022年版では、この93の管理策が「組織的管理策」「人的管理策」「物理的管理策」「技術的管理策」の4つのカテゴリに分類されています。また、「属性 (attribute)」という新しい概念が導入されました。この属性という概念が導入されたことで、管理策のフィルタリング、並び替え、提示がしやすくなりました。ISMSを構築する際には、これらの管理策から、自社にあったものを選択し、対策基準として採用します。

ISO/IEC 27002:2013

- 情報セキュリティのための方針群
- 情報セキュリティのための組織
- 人的資源のセキュリティ
- 資産の管理
- アクセス制御
- 暗号
- 物理的及び環境的セキュリティ
- 運用のセキュリティ
- 通信のセキュリティ
- システムの取得、開発及び保守
- 供給者関係
- 情報セキュリティインシデント管理
- 事業継続マネジメントにおける情報セキュリティの側面
- 遵守

ISO/IEC 27002:2022

テーマ

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

属性

- 管理策タイプ
- 情報セキュリティ特性
- サイバーセキュリティ概念
- 運用機能
- セキュリティドメイン

改訂

図78. ISO/IEC 27002の改定内容

19章. 総括編 19-2. 各章のポイント

19-2-9. 第9章. 管理策のテーマと属性

- 管理策のテーマと属性
管理策のテーマと属性について説明しています。
テーマとは、ISO/IEC 27002の箇条5～8に示される4種の管理策での分類（組織的・人的・物理的・技術的）のことです。
属性とは、テーマとは別の視点で、より細かに管理策をみるためのものです。各管理策に属性が付与されたことにより、検索性が向上し、管理策のフィルタリング、並び替え、提示がしやすくなりました。



図79. ISO/IEC 27002:2022の概要

訴求ポイント

章を通した気づき・学び

企業や組織はISO/IEC 27002に示された管理策から組織に必要なものを選択することが重要です。

認識していただきたい実施概要

- ✓ ISMSにおけるリスク対応のための対策を指すものとして管理策があり、ISO/IEC 27002:2022に合計93項目示されていること。
- ✓ ISO/IEC 27002:2022で示される管理策には4つのテーマと5つの属性があり、それらを参考にしながら組織に必要なセキュリティ対策を選択することが重要であること。

実践のために参考となる文献（参考文献）

ISO/IEC 27002:2022

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

19-2-10. 第10章. 脅威、脆弱性、リスクの定義と関係性

10-1. 用語の定義および関係性と識別方法

章の目的

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

主な達成目標

- ISO/IEC 27000に定義されている「リスク」、「脅威」、「脆弱性」、「管理策」の定義を理解すること
- 「リスク」、「脅威」、「脆弱性」などの関係性を理解すること
- 脆弱性、脅威の識別方法を理解すること

主なキーワード 🔍

脅威、脆弱性、リスク

要旨

10章の全体概要

リスクマネジメントを理解するために必要となる「リスク」、「脆弱性」、「脅威」といった用語の定義と関係性、さらに「脅威」、「脆弱性」の識別方法について説明しています。

➤ 10-1. 用語の定義および関係性と識別方法

• 用語の定義と関係性

企業や組織にはセキュリティ上のリスクが存在しています。これらのリスクを効率的に管理するには、リスクマネジメントを行う必要があります。リスクマネジメントを理解するために必要となる「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を説明しています。

(例) 業務用ノートパソコンに関する脅威や脆弱性、管理策の関係

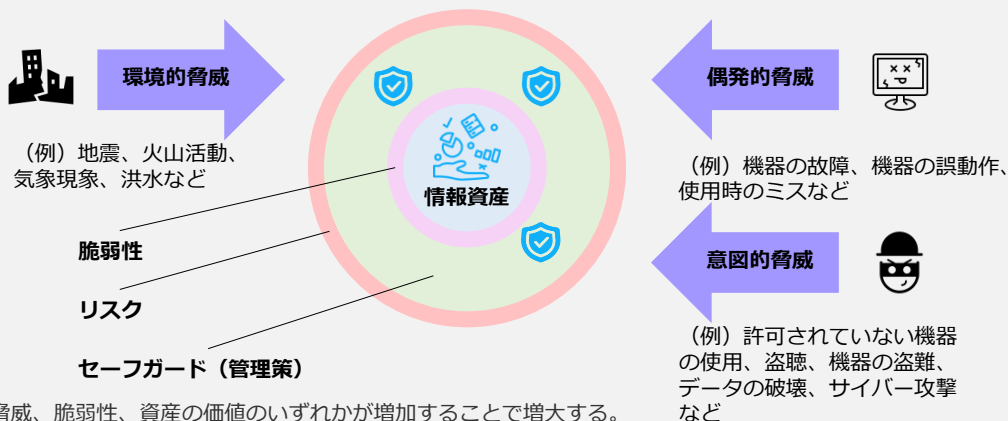


図80. 「脅威」「脆弱性」「リスク」「管理策」の関係性

19章. 総括編

19-2. 各章のポイント

19-2-10. 第10章. 脅威、脆弱性、リスクの定義と関係性

・ 脅威の識別

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

| 脅威の種類 | | 想定される被害とセキュリティ対策 |
|------------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 環境的脅威 (Environmental → E) | | 環境的脅威として地震や高潮がありますが、地震や高潮の発生そのものをコントロールすることはできません。従って、地震の発生可能性が低い場所を選択する、地震が発生した場合に素早く検知し、災害から回復する対策を検討して実施する、などのセキュリティ対策が選択されることとなります。 |
| 人為的脅威 | 意図的脅威 (Deliberate → D) | 悪意のある者によるサイバー攻撃（不正アクセスや標的型攻撃、DDoS攻撃など）があります。対策としては、OSやソフトウェアのアップデートを適宜実施する、EDRやUTMなどのセキュリティ製品を導入する、従業員へ教育の実施などがあげられます。サイバー攻撃により、個人情報や機密情報の漏えい、サービスの停止などの被害にありう可能性があるため、適切なセキュリティ対策を実施することが重要です。 |
| | 偶発的脅威 (Accidental → A) | 「入力ミス」がありますが、入力ミスが生じないように、2回ずつ入力する、一定の範囲の値しか入力できないようにする、チェックデジットやチェックサムを設けるといった技術対策が有効となります。 |

・ 脆弱性の識別

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

訴求ポイント

章を通した気づき・学び

リスクマネジメントで使用される「脅威」、「脆弱性」、「リスク」といった用語の定義や関係性を理解することが大切です。また「脅威」、「脆弱性」の識別方法について理解することが大切です。

認識していただきたい実施概要

- ✓ 「脅威」「脆弱性」「資産の価値」のいずれかが増加することで、リスクが増大すること。
- ✓ リスクを減少させるためには「脅威」、「脆弱性」、「資産の価値」を識別し、リスクに対する保護要求事項を明らかにし、保護要求事項に合致するセーフガード（管理策）を適切に実施することが必要であること。

実践のために参考となる文献（参考文献）

JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」

<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

19-2-11. 第11章. リスクマネジメント

- 11-1. リスクマネジメント：概要
- 11-2. リスクマネジメント：リスクアセスメント
- 11-3. リスクマネジメント：リスク対応

章の目的

第11章では、リスクマネジメントの概要と、リスクマネジメントプロセスにおけるリスクアセスメントの手法やリスク対応の考え方を理解することを目的とします。

主な達成目標

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

主なキーワード 🔍

リスクマネジメント、リスクアセスメント

要旨

11章の全体概要

リスクマネジメントプロセスに沿って、リスク基準の確立、リスクアセスメント、リスク対応について手法なども交えながら解説しています。リスクマネジメントはセキュリティ対策にとって必要ですが、顕在化していないリスクについて考えることが難しい場合もあるでしょう。リスクマネジメントプロセスにおける各段階での考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できます。

➤ 11-1. リスクマネジメント：概要

- リスクマネジメントプロセス (ISO 31000)
リスクを効率的に管理し、発生する可能性がある損失を回避、低減するプロセス全体のことを「リスクマネジメント」と言います。リスクマネジメントの国際規格としてISO 31000があります。リスク対応にあたり、リスクマネジメントプロセスにおける「リスクアセスメント」が必須です。リスクアセスメントとは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク対応の優先順位付けをしているプロセスです。
- 情報セキュリティリスクマネジメント (ISO/IEC 27005)
ISO/IEC 27005は、情報セキュリティにおけるリスクマネジメントに関する国際規格です。ISO 31000と整合性があり、情報セキュリティに特化した内容になっています。
- ISO/IEC 27001におけるリスクマネジメント手順
ISO/IEC 27001はISMSの枠組みを提供し、その中で必要となるリスクマネジメントの具体的な手法やプロセスの詳細を提供しているのが、ISO/IEC 27005です。ISO/IEC 27001の活動は、ISO/IEC 27005におけるリスクマネジメントプロセスと関連付けて整理できます。

19章. 総括編 19-2. 各章のポイント

19-2-11. 第11章. リスクマネジメント

➤ 11-2. リスクマネジメント：リスクアセスメント

➤ 11-3. リスクマネジメント：リスク対応

リスクマネジメント全体の流れは下記の図の通りです。リスクアセスメントでは、組織や企業が抱える資産に対するリスクの洗い出しや分析、評価を行い、リスク基準と比較してリスク対応が必要かどうか判断します。リスク評価の結果をもとに、「低減」、「移転」、「回避」、受容（保有）」からリスク対応を選択します。

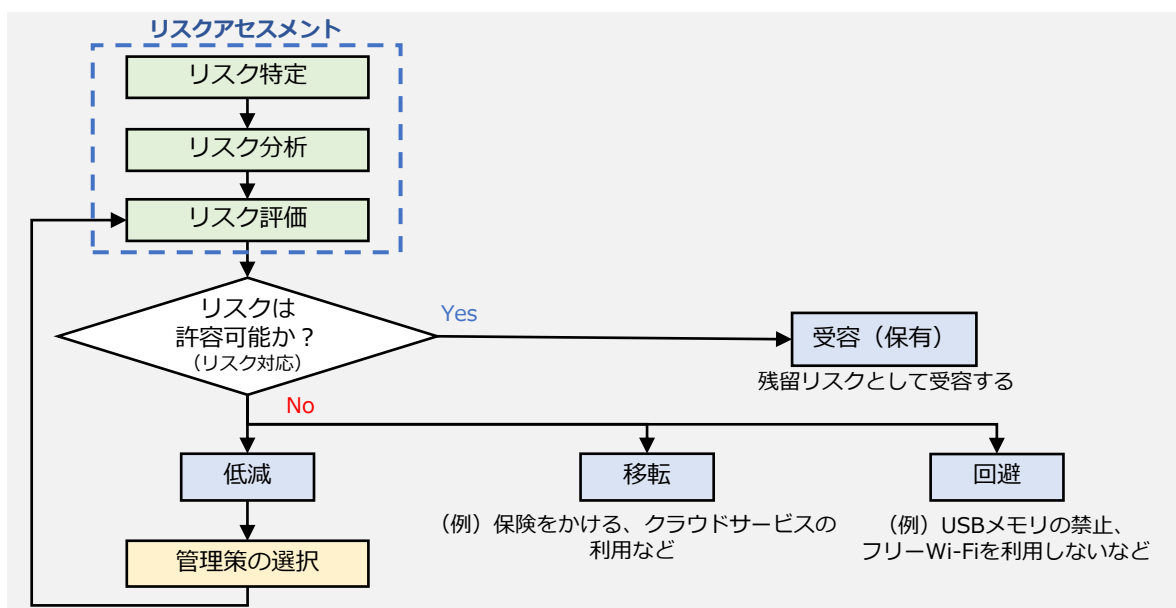


図81. リスクマネジメント全体の流れと、リスク対応の選択プロセス

訴求ポイント

章を通した気づき・学び

リスクマネジメントはセキュリティ対策にとって欠かせないものですが、顕在化していないリスクについて考えることが難しい場合もあります。リスクマネジメントプロセスにおける各段階の考え方や手法を用いることで、円滑なリスク特定、分析と対応策の検討を実施できます。

認識していただきたい実施概要

- ✓ リスク対応にはリスクマネジメントプロセスにおけるリスクアセスメントが必須であること。
- ✓ リスクアセスメントは「リスク特定」、「リスク分析」、「リスク評価」を実施すること。
- ✓ リスク対応はリスクアセスメントの結果をもとに「リスク回避」、「リスク低減」、「リスク移転」、「リスク受容」から選択すること。

実践のために参考となる文献（参考文献）

JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」

<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

ISO/IEC 27005:2022

<https://www.iso.org/standard/80585.html>

19-2-12. 第12章. 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

- 12-1. 【LV.1 クイックアプローチ】 【LV.2 ベースラインアプローチ】 の概要
- 12-2. 【LV.1 クイックアプローチ】 セキュリティインシデント事例を参考とした実施手順
- 12-3. 【LV.2 ベースラインアプローチ】 ガイドラインを参考とした実施手順

章の目的

第12章では、セキュリティインシデント事例を参考にするクイックアプローチと、ガイドラインやひな形などの資料を参考にするベースラインアプローチにおける対策基準・実施手順の策定方法の理解を目的とします。

主な達成目標

- クイックアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること
- ベースラインアプローチ手法を用いて、対策基準・実施手順を策定する方法を理解すること

主なキーワード

クイックアプローチ、ベースラインアプローチ

要旨

12章の全体概要

クイックアプローチ、ベースラインアプローチについて説明しています。クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きい事案への対策がとりやすいでしょう。ベースラインアプローチは、ガイドラインやひな形などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定ができるでしょう。

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

- LV.1 クイックアプローチ・LV.2 ベースラインアプローチ
セキュリティ対策基準を策定し、具体的な実施手順を明確にすることで、情報漏えいなどのリスク対策を行います。
LV.1 クイックアプローチとは、即時の対応や緊急事態への対処が必要な事例に対して、対策基準や実施手順を策定していくアプローチ手法です。
LV.2 ベースラインアプローチとは、ガイドラインなどを参考に対策基準や実施手順を策定するアプローチ手法です。

19章. 総括編

19-2. 各章のポイント

19-2-12. 第12章. 具体的手順の作成 (LV.1 クイックアプローチ/LV2. ベースラインアプローチ)

- **12-2. 【LV.1 クイックアプローチ】セキュリティインシデント事例を参考とした実施手順**
- **セキュリティインシデント事例を参考とした実施手順**
クイックアプローチでは、自社で発生する可能性が高い、または実際に発生したときの被害が大きいと考えられるセキュリティインシデント事例を参考に、対策基準を策定します。決定した対策基準をもとに、具体的に実施する内容（実施手順）を作成します。対策基準・実施手順作成の手順を説明しています。

メリット

- 小規模な対策や修正を迅速に実施可能。
- 低コストでリスクを軽減。

デメリット

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

- **12-3. 【LV.2 ベースラインアプローチ】ガイドラインを参考とした実施手順**
- **情報セキュリティ対策ガイドラインの活用**
ベースラインアプローチは、ガイドラインやひな形などの資料を参考に対策基準、実施手順を作成するという方法です。

メリット

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

デメリット

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

訴求ポイント

章を通した気づき・学び

緊急性や即効性についてはクイックアプローチ、ベースラインアプローチが勝りますが、じっくりと対策を検討する余裕がある場合、網羅的アプローチに取り組むことが大切です。

認識していただきたい実施概要

- ✓ クイックアプローチは、実際のセキュリティインシデントの事例について、自社での発生可能性や被害規模を検討した上で対策基準や実施手順を策定していくため、社会的に影響の大きいまたは緊急性の高い事象への対策がとりやすいこと。
- ✓ ベースラインアプローチは、ガイドラインやひな形などによる既存の手法を参考にして対策基準や実施手順を策定していくため、自社に適した参考元があれば、それをもとに簡易な手順で策定がしやすいこと。

| 実践のために参考となる文献（参考文献） | |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| リスク分析シート | https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx |
| 中小企業の情報セキュリティ対策ガイドライン第3.1版 | https://www.ipa.go.jp/security/guide/sme/about.html |
| インターネットの安全・安心ハンドブックVer.5.0 | https://security-portal.nisc.go.jp/guidance/handbook.html |
| テレワークセキュリティガイドライン第5版 | https://www.soumu.go.jp/main_content/000752925.pdf |
| 中小企業のためのクラウドサービス安全利用の手引き | https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf |
| 情報セキュリティ関連規程（サンプル） | https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx |

19-2-13. 第13章. ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

13-1. 【LV.3 網羅的アプローチ】の概要

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

章の目的

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

主な達成目標

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

主なキーワード

網羅的アプローチ、PDCAサイクル

要旨

13章の全体概要

網羅的アプローチは、ISMSなどのフレームワークを利用して、対策基準や実施手順を策定する方法です。時間はかかりますが、会社としてセキュリティを確保するにあたって高いレベルでのセキュリティ対策ができるでしょう。緊急性や即効性についてはクイックアプローチ、ベースラインアプローチが勝りますが、じっくりと対策を検討する余裕がある場合、網羅的アプローチを推奨します。

➤ 13-1. 【LV.3 網羅的アプローチ】の概要

• LV.3 網羅的アプローチ

網羅的アプローチでは、フレームワークとしてISMSを用いて、体系的・網羅的にセキュリティ対策基準、実施手順を作成します。ISMSのフレームワークに沿うため、技術的対策といった一部の内容に限らず、運用や監査についても含めて対策基準、実施手順を策定します。ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明していきます。

網羅的アプローチのメリットは、ISMS要求事項の導入が可能なことです。デメリットは、時間とコストがかかることです。

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

19章. 総括編

19-2. 各章のポイント

19-2-13. 第13章. ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

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

ISMSは、PDCAサイクルに則って運用することとなります。ISMSにおけるPDCAサイクルを回すために重要となるドキュメントの作成方法や、実施すべき事項について焦点を当てて説明しています。

ISMSの要求事項を定めているISO/IEC 27001の1から3はそれぞれ「1.適用範囲」「2.引用規格」「3.用語及び定義」なので、実質的な要求事項は「4.組織の状況」から「10.改善」までの7項目となっています。

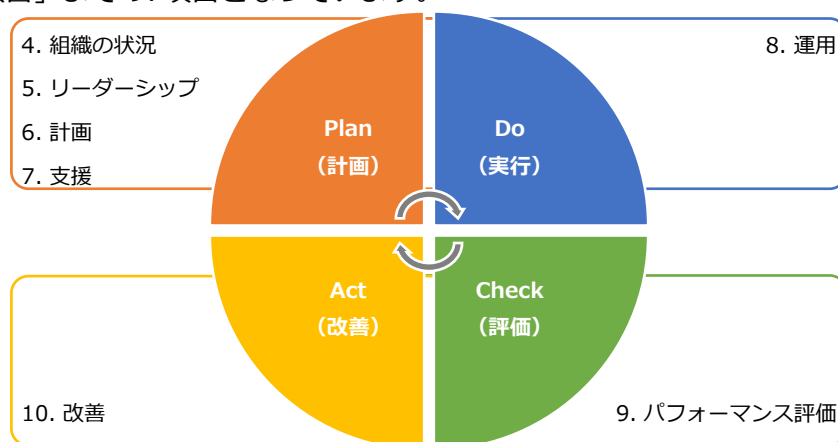


図82. ISMSのPDCAサイクル

4. 組織の状況

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

5. リーダーシップ

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

6. 計画

ISMSの計画を立てる際の要求事項。

7. 支援

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

8. 運用

ISMSを実行する際の要求事項。

9. パフォーマンス評価

適切なISMSが構築・運用できているか評価する際の要求事項。

10. 改善

ISMSの是正処置やリスク、改善の機会、ISMS認証の不適合があった場合の対処法。

訴求ポイント

章を通した気づき・学び

ISMSを用いる網羅的アプローチを実施することで、単にセキュリティ対策を検討するだけではなく、PDCAサイクルによってISMS自体を継続的に改善し、より自社に適した対策を検討できるようになります。

認識していただきたい実施概要

- ✓ 「4. 組織の状況」から「10. 改善」までの7項目で必要なドキュメントの作成手順を理解すること。
- ✓ ISMSマネジメントプロセスを取り込み、PDCAサイクルを回すこと。

実践のために参考となる文献 (参考文献)

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

19-2-14. 第14章. 組織的管理策

14-1. 組織的管理策を参考とした対策基準・実施手順の策定

章の目的

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

主な達成目標

- 組織的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード 🔍
組織的管理策

要旨

14章の全体概要

対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説しています。管理策は、「組織的管理策」、「人的管理策」、「物理的管理策」、「技術的管理策」の4つのカテゴリに分類できます。14章では「組織的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。

➤ 14-1. 組織的管理策を参考とした対策基準・実施手順の策定

• 対策基準の策定

ISO/IEC 27001:2022附属書Aの組織的管理策（37項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

• 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。実施手順は、組織の内部文書として作成します。実施手順が抽象的で理解しづらい場合、従業員は具体的に何を遵守して行動すればよいかわからず、セキュリティ対策が不十分になってしまいます。従業員に対して具体的でわかりやすい実施手順を策定するよう心掛けることが大切です。

実施手順を策定する際は、ISO/IEC 27002に記載されている各管理策の手引きが参考になります。手引きの内容をもとに、実施手順の例を紹介しています。この例と、ISO/IEC 27002の内容を参考に、自社に適した実施手順を策定しましょう。

19章. 総括編

19-2. 各章のポイント

19-2-14. 第14章. 組織的管理策

組織的管理策の項目

| | |
|------------------------------|---------------------------------|
| 5.1 情報セキュリティのための方針群 | 5.21 ICTサプライチェーンにおける情報セキュリティの管理 |
| 5.2 情報セキュリティの役割及び責任 | 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 |
| 5.3 職務の分離 | 5.23 クラウドサービス利用における情報セキュリティ |
| 5.4 経営陣の責任 | 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 |
| 5.5 関係当局との連絡 | 5.25 情報セキュリティ事象の評価及び決定 |
| 5.6 専門組織との連絡 | 5.26 情報セキュリティインシデントへの対応 |
| 5.7 脅威インテリジェンス | 5.27 情報セキュリティインシデントからの学習 |
| 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 | 5.28 証拠の収集 |
| 5.9 情報及びその他の関連資産の目録 | 5.29 事業の中断・阻害時の情報セキュリティ |
| 5.10 情報及びその他の関連資産の利用の許容範囲 | 5.30 事業継続のためのICTの備え |
| 5.11 資産の返却 | 5.31 法令、規制及び契約上の要求事項 |
| 5.12 情報の分類 | 5.32 知的財産権 |
| 5.13 情報のラベル付け | 5.33 記録の保護 |
| 5.14 情報転送 | 5.34 プライバシー及びPIIの保護 |
| 5.15 アクセス制御 | 5.35 情報セキュリティの独立したレビュー |
| 5.16 識別情報の管理 | 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 |
| 5.17 認証情報 | 5.37 操作手順書 |
| 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 | |

訴求ポイント

章を通じた気づき・学び

ISO/IEC 27002の内容を参考に組織的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は重要ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な組織的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。

実践のために参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

ISO/IEC 27002:2022

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

19-2-15. 第15章. 人的管理策

15-1. 人的管理策を参考とした対策基準・実施手順の策定

章の目的

第15章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。

主な達成目標

- 人的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード 🔍 人的管理策

要旨

15章の全体概要

対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説しています。15章では「人的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。

➤ 15-1. 人的管理策を参考とした対策基準・実施手順の策定

- 対策基準の策定
ISO/IEC 27001:2022附属書Aの人的管理策（8項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。
対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。
- 実施手順の策定
管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

人的管理策の項目

| | |
|--------------------------|--------------------|
| 6.1 選考 | 6.5 雇用の終了又は変更後の責任 |
| 6.2 雇用条件 | 6.6 秘密保持契約又は守秘義務契約 |
| 6.3 情報セキュリティの意識向上、教育及び訓練 | 6.7 リモートワーク |
| 6.4 懲戒手続 | 6.8 情報セキュリティ事象の報告 |

19-2-15. 第15章. 人的管理策

訴求ポイント

章を通じた気づき・学び

ISO/IEC 27002の内容を参考に人的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な人的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。

実践のために参考となる文献（参考文献）

| | |
|--------------------|-----------------------------------------------------------------------------------------------|
| ISO/IEC 27001:2022 | https://www.iso.org/standard/27001 |
| ISO/IEC 27002:2022 | https://www.iso.org/standard/75652.html |

19-2-16. 第16章. 物理的管理策

16-1. 物理的管理策を参考とした対策基準・実施手順の策定

16-2. 各種テーマごとの対策

章の目的

第16章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。

主な達成目標

- 物理的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。

主なキーワード

物理的管理策、BYOD、MDM

要旨

16章の全体概要

対策基準を策定する際は、ISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできます。管理策を参考に、対策基準・実施手順を策定する手順について解説していません。16章では「物理的管理策」を参考に、対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。またテーマごとの対策として、「BYOD」、「MDM」を紹介しています。

➤ 16-1. 物理的管理策を参考とした対策基準・実施手順の策定

• 対策基準の策定

ISO/IEC 27001:2022附属書Aの物理的管理策（14項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

• 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

物理的管理策の項目

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

19章. 総括編

19-2. 各章のポイント

19-2-16. 第16章. 物理的管理策

➤ 16-2. 各種テーマごとの対策

テーマごとに、概要や関連する管理策、運用手順などについて説明しています。

• BYOD (Bring Your Own Device)

BYODとは、個人が私物として所有している端末（PCやスマートフォンなど）を業務に使う利用形態のことです。BYOD導入に向けたポイント、運用手順を説明しています。

メリット

- コスト削減
企業は、端末の調達や管理にコストがかかります。故障した際の修理費用や老朽化した端末の入れ替えも基本的には個人負担となります。
- 使い慣れた端末の業務利用
従業員は、自分の使い慣れた端末を使用でき、操作方法や設定などを新たに覚える必要がないため作業効率があがります。また、仕事用とプライベート用に分けて端末を複数台持つ必要がなくなります。

デメリット

- シャドーIT
ルールの整備や技術的な対策を講じないと、シャドーITが増加してしまう恐れがあります。
- セキュリティリスク
個人の端末では、業務に関係ないWebサイトやアプリケーションを利用されるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなります。

• MDM (Mobile Device Management)

MDMとは、企業で保有しているモバイル端末（スマートフォンやタブレットなど）を一元管理できるシステムのことです。MDMの導入に向けたポイント、運用手順を説明しています。

MDMを導入する際のポイント

- ✓ 利用者の意見を反映した社内ルールの策定、およびMDMの選定
MDMは情報セキュリティの向上や業務効率化に役立ちますが、いくつか注意点があります。たとえば、紛失・盗難されたデバイスがネットワークに接続されていない場合には、初期化などのリモート制御ができません。また、MDMによる制限が厳しくなりすぎると、使い勝手が悪くなり利用者から不満がでる可能性があります。利用者の意見を聞きながら、社内ルールの策定やMDMの選定を進めることが重要です。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に物理的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な物理的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定しよう心掛けること。
- ✓ BYOD、MDMの概要および運用手順を理解すること。

実践のために参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

ISO/IEC 27002:2022

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

19-2-17. 第17章. 技術的管理策

17-1. 技術的管理策を参考とした対策基準・実施手順の策定

17-2. 各種テーマごとの対策

章の目的

第17章では、情報セキュリティ方針に従ってセキュリティ対策を実施するための具体的な規則としての「対策基準」と、セキュリティ対策の実施手順や方法である「実施手順」について理解することを目的とします。また、技術的管理策に関して、テーマごとの対策について理解することも目的とします。

主な達成目標

- 技術的管理策をもとに、対策基準を策定する手順を理解すること。
- 策定した対策基準をもとに、具体的な実施手順を策定する方法を理解すること。
- Security by Design、ゼロトラスト・境界防御モデル、ネットワーク制御、セキュリティ統制、インシデント対応について理解すること。

主なキーワード

技術的管理策、Security by Design、ゼロトラスト、ネットワーク制御、セキュリティ統制、インシデント対応

要旨

17章の全体概要

ISMSの管理策を参考に、対策基準・実施手順を策定する手順について解説しています。17章では「技術的管理策」を参考に対策基準を策定する手順について説明し、対策基準それぞれに対応する実施手順の例を説明しています。またテーマごとの対策として、「Security by Design」、「ゼロトラスト」、「ネットワーク制御」、「セキュリティ統制」、「インシデント対応」を紹介しています。

➤ 17-1. 技術的管理策を参考とした対策基準・実施手順の策定

• 対策基準の策定

ISO/IEC 27001:2022附属書Aの技術的管理策（34項目）を参考に、対策基準を策定します。リスクアセスメントの内容をもとに必要な管理策を選択し、決定した管理策を対策基準とします。

対策基準の内容は、基本方針とともに公開可能なものとして作成します。ISMSに基づく管理策を用いて対策基準を策定する際は、ISO/IEC 27001:2022の文献を参照しながら作成してください。

• 実施手順の策定

管理策（対策基準）をもとに策定されたセキュリティ対策の実施手順の例を、それぞれ紹介しています。紹介する例と、ISO/IEC 27002に記載されている各管理策の手引きの内容を参考に、自社に適した実施手順を策定しましょう。

19章. 総括編

19-2. 各章のポイント

19-2-17. 第17章. 技術的管理策

| 技術的管理策の項目 | |
|--------------------------|----------------------------------------|
| 8.1 利用者エンドポイント機器 | 8.19 運用システムに関わるソフトウェアの導入 |
| 8.2 特権的アクセス権 | 8.20 ネットワークのセキュリティ |
| 8.3 情報へのアクセス制限 | 8.21 ネットワークサービスのセキュリティ |
| 8.4 ソースコードへのアクセス | 8.22 ネットワークの分離 |
| 8.5 セキュリティを保った認証 | 8.23 ウェブ・フィルタリング |
| 8.6 容量・能力の管理 | 8.24 暗号の使用 |
| 8.7 マルウェアに対する保護 | 8.25 セキュリティに配慮した開発のライフサイクル |
| 8.8 技術的ぜい弱性の管理 | 8.26 アプリケーションのセキュリティの要求事項 |
| 8.9 構成管理 | 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則 |
| 8.10 情報の削除 | 8.28 セキュリティに配慮したコーディング |
| 8.11 データマスキング | 8.29 開発及び受入れにおけるセキュリティ試験 |
| 8.12 データ漏えいの防止 | 8.30 外部委託による開発 |
| 8.13 情報のバックアップ | 8.31 開発環境、試験環境及び運用環境の分離 |
| 8.14 情報処理施設の冗長性 | 8.32 変更管理 |
| 8.15 ログ取得 | 8.33 試験情報 |
| 8.16 監視活動 | 8.34 監査試験中の情報システムの保護 |
| 8.17 クロックの同期 | |
| 8.18 特権的なユーティリティプログラムの使用 | |

➤ 17-2. 各種テーマごとの対策

テーマごとに、概要や関連する管理策、実施手順などについて説明しています。

✓ Security by Design

開発プロセスの早い段階からセキュリティを考慮することで、開発システムのセキュリティを確保するという考え方です。

✓ 境界防御モデル・ゼロトラスト

境界防御モデルは、信用する領域（社内）と信用しない領域（社外）に境界を設け、境界線でセキュリティ対策を講じることで境界外部からの脅威を防ぐという考え方です。

ゼロトラストは、「境界」の概念をなくし、守るべき情報資産にアクセスするものはすべて確認し、認証・認可を行うことで脅威を防ぐという考え方です。

✓ ネットワーク制御

クラウドサービス、SDN、SD-WANについて説明しています。

✓ セキュリティ統制

組織が情報資産を守るために採用するセキュリティ対策や仕組みのことです。セキュリティ統制を確立するために実施することができる技術を紹介しています。

✓ インシデント対応

インシデント対応の実施手順、フォレンジックについて説明しています。

訴求ポイント

章を通した気づき・学び

ISO/IEC 27002の内容を参考に技術的管理策の対策基準を決定し、実施手順を作成することが大切です。ドキュメントの作成・更新は大切ですが、本来の目標は、効果的な情報セキュリティ対策の計画と実行にあることを忘れないことが重要です。

認識していただきたい実施概要

- ✓ リスクアセスメントの結果をもとに必要な技術的管理策を選択し、対策基準を策定すること。
- ✓ 対策基準は、基本方針とともに公開可能なものとして策定すること。
- ✓ 決定した対策基準をもとに、具体的に実践するための実施手順を策定すること。
- ✓ 実施手順は、組織の内部文書として従業員に対してわかりやすい実施手順を策定するよう心掛けること。
- ✓ 各種テーマごとに概要を理解し、自社に適した実施手順を策定すること。

実践のために参考となる文献（参考文献）

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

ISO/IEC 27002:2022

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

19-2-18. 第18章. セキュリティ対策状況の有効性評価

18-1. 内部監査・外部監査

章の目的

第18章では、セキュリティ対策をした結果、効果があったのか、目標に近づいているかを判断するための取組みとして、監査について理解することを目的とします。

主な達成目標

- 内部監査および外部監査の重要性について理解すること。

主なキーワード 🔍
内部監査、外部監査

要旨

18章の全体概要

セキュリティ対策状況の有効性評価として、内部監査と外部監査について説明しています。内部監査では、セキュリティのルールや扱っている文書などが、自社で規定した要求事項を満たしており、決められたルールに沿って業務が実際されているかをチェックします。外部監査では、企業が保有する情報資産を守るための体制や環境が整っているかを第三者がチェックします。

➤ 18-1. 内部監査・外部監査

・ 内部監査

セキュリティのルールを整備したばかりの段階では、関係者がルールを理解し、遵守できて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どうか有効性をチェックします。内部監査の視点を適合性から有効性へと移していくことで、ルールが形骸化し、目的が見失われる状態を防げるでしょう。

・ 外部監査

セキュリティ対策の実施状況について外部監査を受けることは、情報漏えいやサイバー攻撃などのリスクに対する対策が適切かつ有効であるかどうかをチェックする手段の1つです。情報セキュリティ監査を受ければ、自社のセキュリティ対策が正しく行われているか確認でき、不十分な点を洗い出して迅速に対処できます。また、顧客や取引先に、セキュリティ対策を適切に行っていることをアピールできます。

訴求ポイント

章を通した気づき・学び

企業や組織は、セキュリティ対策状況の有効性評価として定期的に内部・外部監査を実施することが重要です。

認識していただきたい実施概要

- ✓ 外部監査を行うことで、第三者視点で企業が保有する情報資産を守るための体制や環境が整っているかをチェックでき、また顧客や取引先に、セキュリティ対策を適切に行っているというアピールにも繋がること。
- ✓ 内部監査を行うことで、セキュリティのルールや文書の内容が適切かどうかの有効性をチェックでき、形骸化し、目的が見失われている状態を防止することに繋がること。

19章. 総括編

19-3 読者に今後行ってほしいこと

19-3-1. 今後のアクション

本テキストでは、「DX推進の必要性からセキュリティ対策の実施手順を策定する」ところまでを解説しました。本テキストの内容を実践するにあたって行うべき事項を列挙し、概要を説明します。

本テキストの内容を実践するために行うべき事項

- テキストに記載された各章の理解を深め、経営者を含めた関係者と共有すること
- 経営者のリーダーシップによって社内体制を整備すること
- 整備した社内体制において順次具体的なアクションを実践すること

テキストに記載された各章の理解を深め、経営者を含めた関係者と共有すること

➤ 各章のポイントの理解

テキストに記載された「セキュリティを考える上で必要となる社会情勢、国の施策に関する情報」、「セキュリティ対策を検討する上で必要となるセキュリティ知識」、「セキュリティ対策を実施するための具体的な手法」を再認識し、理解を深めること。

➤ DX推進の考え方の把握

- 社会情勢、国の施策からDX推進の方向性
中小企業においてもDX推進が必要であること。
- 自組織におけるDX推進のための人材育成の必要性
DXを推進する人材（DX推進スキル標準で示されたスキルを有する人材）や、DXを有効に利用できる人材（DXリテラシー標準で示されたスキルを有する人材（※プラスセキュリティを含む））の確保が必要であること。
- 自組織としてのDX推進の計画立案・実施内容の認識
DX推進にあたってはDX with Security（DXの推進にあたり、セキュリティ対策を十分に考慮する）、IT構築にあたってはSecurity by Design（設計段階からのセキュリティ対策を考慮する）を意識すること。

➤ セキュリティ対策の全容の認識

サイバーセキュリティの脅威に対処するためのアプローチ手法としては「クイックアプローチ」「ベースラインアプローチ」「網羅的アプローチ」があり、それぞれのアプローチ方法には長所・短所があること。たとえば、ISMSなどのフレームワークを用いた網羅的アプローチは、時間とコストがかかるという短所があるものの、漏れない対策が可能であるという長所があること。ISMSの仕組みや、管理策の全容を理解すること。

➤ 自組織でのセキュリティ対策の実施項目の認識

- 自組織としての目標設定
自組織のリスクを、経営上および社会的に許容できる範囲まで低減させるセキュリティ対策を実践すること。

1. リスクアセスメントによって自組織の現状のリスクを把握する。
2. リスクアセスメントの結果を踏まえ、管理策の中から自組織として実施すべき項目を選定する。
3. 実施する管理策に関して、自組織としての実施手順を策定する。

19-3-1. 今後のアクション

経営者のリーダーシップによって社内体制を整備すること

実施手順の実践準備

実施手順として策定した内容を実践するため、実行性のあるドキュメント（仕様書、運用マニュアルなど）を作成します。

実施手順の実践

実践にあたり、セキュリティ担当者とその役割・責任を決める必要があります。セキュリティ担当者とその役割・責任が決まった後、年間計画を作成して実践を行います。

①組織体制と役割の決定

セキュリティ対策を実施するための組織体制、役割・責任を決めます。

※第13章13ページ「管理策：5.3 組織の役割、責任及び権限」を参照。

②年間を通して実践すべき事項の例示

担当者がその役割・責任において次のような事項を実施します。これらの事項を実践するため、年間計画を作成します。

※第13章35ページ「管理策：8.1 運用の計画及び管理」を参照。

- リスクアセスメントの実施、リスク対応のための計画作成、管理策の検討
- 資産台帳の見直し
- 事業継続に関する試験
- 内部監査
- マネジメントレビュー
- 不適合及び是正処置のレビュー
- 定期教育
- 外部審査
- 情報セキュリティのための方針群のレビュー
- 秘密保持契約書の確認
- 「関係当局との連絡」体制の見直し
- 法令規制一覧表の確認
- 運用チェックリストによる確認
- 入退記録の確認
- など

上記の内容を実施するための年間計画を作成



19章. 総括編
19-3 読者に今後行ってほしいこと

19-3-1. 今後のアクション

年間計画（例）を紹介します。

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

図83. 年間計画（例）

19章. 総括編

19-3 読者に今後行ってほしいこと

19-3-1. 今後のアクション

確立した社内体制において順次具体的なアクションを実践すること

管理策を実践するための参考となる情報

組織の中で具体的にどのように実施手順の内容を実践していくか、その際に参考となる各種資料や、実務的な取組み例を紹介します。

| 管理策を実践するための参考となる情報 | |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ISO/IEC 27002:2022 対応 情報セキュリティ管理策実践ガイド | https://isms-society.stores.jp/items/632a57a42e7452256400d84b |
| ISMS推進マニュアル - 活用ガイドブック ISO/IEC 27001:2022 対応1.0版 | https://isms-society.stores.jp/items/6427f4b51d175c002b8ee1cd |
| JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」 | https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000 |
| ISO/IEC 27002:2022 | https://www.iso.org/standard/75652.html |

実施手順を具体的に実践していくための取組み例を紹介します。
以下は、実施手順を実際の業務として実践していくにあたり、実施手順と主体となって取り組む必要がある担当者に対応付ける例です。

| 対策基準 (例) | 5.2 情報セキュリティの役割及び責任 | 5.5 関係当局との連絡 | 6.7 リモートワーク | 8.15 ログ取得 |
|-----------------|---------------------|----------------------------------------------------|----------------------|--------------------------------------------|
| 実施手順 (例) | 情報セキュリティ委員会を設置する。 | 関係当局およびその連絡先を「連絡先一覧表」に特定し、必要時に容易に連絡がとれる体制を確立・維持する。 | 社内ネットワークへはVPNにて接続する。 | バックアップが確実に行われており、障害時に復元が可能かどうかを月に1度チェックする。 |
| トップマネジメント (経営層) | ○ | — | ○ | — |
| 情報セキュリティ委員会 | — | ○ | ○ | — |
| 情報システム管理者 | — | — | ○ | ○ |
| 一般社員 | — | — | ○ | — |

図84. 実施手順とメインとなる担当者に対応付ける例

○：主体となって取り組む必要がある。

19章. 総括編

19-3 読者に今後行ってほしいこと

19-3-1. 今後のアクション

継続的な情報収集

本テキストに記載の「①国の方針、社会の現状と今後の動向」、「②IT活用事例」、「③セキュリティインシデント事例」における内容は、日々更新されていきます。これらの情報を継続的に学ぶために参考となる文献を紹介します。

| ①国の方針、社会の現状と今後の動向 | |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デジタルガバナンス・コード2.0 | https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc.html |
| 経済財政運営と改革の基本方針2023 | https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf |
| デジタル社会の実現に向けた重点計画 | https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf |
| Society5.0 | https://www8.cao.go.jp/cstp/society5_0 |
| サイバーセキュリティ2023の概要 | https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.pdf |
| サイバーセキュリティ戦略 Cybersecurity for All 誰も取り残さないサイバーセキュリティ | https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf |
| ②IT活用事例 | |
| 中堅・中小企業等向け「デジタルガバナンス・コード」実践の手引き | https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/contents.html |
| DX白書2023 | https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf |
| 攻めのIT活用指針 | https://www.smrj.go.jp/doc/tool/guide4youshiki_1.pdf |
| 情報通信白書 令和2年版 | https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf |
| 製造分野のDX事例集 | https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf |
| 「DX Selection 2023」選定企業レポート | https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf |
| ③セキュリティインシデント事例 | |
| 情報セキュリティ白書2022 | https://www.ipa.go.jp/publish/wp-security/sec-2022.html |
| 情報セキュリティ10大脅威 2023 | https://www.ipa.go.jp/security/10threats/10threats2023.html |
| サイバー攻撃対応事例 | https://security-portal.nisc.go.jp/dx/provinatack.html |
| サイバー攻撃を受けた組織における対応事例集 (実事例における学びと気づきに関する調査研究) | https://www.nisc.go.jp/pdf/policy/inquiry/kokai_jireishu.pdf |
| コンピュータウイルス・不正アクセスの届出事例 [2022年下半年(7月~12月)] | https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf |
| 令和4年におけるサイバー空間をめぐる脅威の情勢等について (警察庁) | https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf |
| 2021年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集- | https://www.ipa.go.jp/security/reports/sme/ug65p90000019djm-att/000098149.pdf |

人材育成

今後のビジネス発展のためには、人材育成が不可欠となります。人材育成を実践するために参考となる文献を紹介します。

| ①DSSIに基づく人材育成 | |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| デジタルスキル標準Ver.1.1 2023年8月 | https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf |
| ②プラス・セキュリティ人材の育成 | |
| 「プラス・セキュリティ知識」とは? | https://security-portal.nisc.go.jp/dx/pdf/about_plussecurity.pdf |
| サイバーセキュリティ経営ガイドラインVer2.0付録F サイバーセキュリティ体制構築・人材確保の手引き~ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成~第1版 | https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf |

おわりに

Society5.0の実現に向けて、社会のデジタル化が着実に進んでいます。それと同時に、ビジネス環境におけるサイバー攻撃によるリスクも大きくなってきています。大企業を中心としたサプライチェーン網においては、比較的セキュリティ対策の弱い中小企業を狙った攻撃事例も増加しているため、セキュリティ対策は中小企業にとっても喫緊の課題であることを強く意識していただければと思います。

本テキストでは中小企業向けに、社会のセキュリティ動向から、具体的なセキュリティ対策まで、セキュリティに関する実践的な知識を解説いたしました。是非、定期的に全10回の内容を復習していただくとともに、必要に応じて、参考文献などからより多くの情報を集めるようにしてください。またITの世界は日進月歩であり、常に企業を取り巻く環境が変化していることを忘れず、常に最新の情報を収集し、セキュリティ対策を定期的に見直すことも忘れないでください。自組織に必要なセキュリティ関連の知識を充実させることで、課題への対応力の向上や、セキュリティ体制の強化をしていけると思います。セキュリティ対策は会社の健全な成長に不可欠なものであると捉え、積極的に取り組んでいただくことを期待しております。

参考文献

「プラス・セキュリティ知識」とは？

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

セキュリティ・バイ・デザイン導入指南書

https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2022/ngi93u0000002kef-att/000100451.pdf

デジタルスキル標準Ver.1.1 2023年8月

<https://www.ipa.go.jp/jinzai/skill-standard/dss/ps6vr700000080fg-att/000106869.pdf>

デジタルガバナンス・コード2.0

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

情報セキュリティ白書2022

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

情報セキュリティ10大脅威 2023

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

試験区分一覧

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

SECURITY ACTION セキュリティ対策自己宣言

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

情報セキュリティ5か条

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

5分でできる！情報セキュリティ自社診断

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

攻めのIT活用指針

https://www.smrj.go.jp/doc/tool/guide4youshiki_1.pdf

経済財政運営と改革の基本方針2023

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2023/2023_basicpolicies_ja.pdf

デジタル社会の実現に向けた重点計画

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5ecac8cc-50f1-4168-b989-2bcaabffe870/b24ac613/20230609_policies_priority_outline_05.pdf

中堅・中小企業等向けデジタルガバナンス・コード実践の手引き2.0

https://www.meti.go.jp/policy/it_policy/investment/dx-chushoguidebook/tebiki2-0.pdf

サイバーセキュリティ体制構築・人材確保の手引き（第2.0版）

<http://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf>

「個人情報保護法」をわかりやすく解説 個人情報の取扱いルールとは？

<https://www.gov-online.go.jp/useful/article/201703/1.html>

参考文献

ISMS適合性評価制度

<https://isms.jp/doc/JIP-ISMS120-62.pdf>

サイバーセキュリティ経営ガイドライン Ver3.0

<https://www.meti.go.jp/press/2022/03/20230324002/20230324002-1.pdf>

政府情報システムにおけるサイバーセキュリティフレームワーク導入に関する技術レポート

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/e2a06143-ed29-4f1d-9c31-0f06fca67afc/a84dbb17/20230411_resources_standard_guidelines_guideline_05.pdf

サイバー攻撃対応事例

<https://security-portal.nisc.go.jp/dx/provinatack.html>

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 27002:2022

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

JISC「JIS Q 27000 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－用語」

<https://www.jisc.go.jp/app/jis/general/GnrJISNumberNameSearchList?show&jisStdNo=Q27000>

ISO/IEC 27005:2022

<https://www.iso.org/standard/80585.html>

リスク分析シート

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055518.xlsx>

中小企業の情報セキュリティ対策ガイドライン第3.1版

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

インターネットの安全・安心ハンドブックVer.5.0

<https://security-portal.nisc.go.jp/guidance/handbook.html>

テレワークセキュリティガイドライン第5版

https://www.soumu.go.jp/main_content/000752925.pdf

中小企業のためのクラウドサービス安全利用の手引き

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf>

情報セキュリティ関連規程（サンプル）

<https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx>

ISO/IEC 27001:2022

<https://www.iso.org/standard/27001>

参考文献

Society5.0

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

サイバーセキュリティ2023の概要

https://www.nisc.go.jp/pdf/policy/kihon-s/cs2023_gaiyou.pdf

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

<https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf>

DX白書2023

<https://www.ipa.go.jp/publish/wp-dx/gmcbt8000000botk-att/000108041.pdf>

情報通信白書 令和2年版

<https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r02/pdf/02honpen.pdf>

製造分野のDX事例集

<https://www.ipa.go.jp/digital/dx/mfg-dx/ug65p90000001kqv-att/000087633.pdf>

「DX Selection 2023」選定企業レポート

https://www.meti.go.jp/policy/it_policy/investment/dx-selection/dxselection2023report.pdf

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

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

コンピュータウイルス・不正アクセスの届出事例 [2022年下半年（7月～12月）]

<https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/000108764.pdf>

令和4年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

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

2021年度 中小企業における情報セキュリティ対策に関する実態調査 -事例集-

<https://www.ipa.go.jp/security/reports/sme/ug65p900000019djm-att/000098149.pdf>

サイバーセキュリティ経営ガイドラインVer2.0付録Fサイバーセキュリティ体制構築・人材確保の手引き
～ユーザー企業におけるサイバーセキュリティ対策のための組織づくりと従事する人材の育成～第1版

<https://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf>

用語集

■ AI

Artificial Intelligenceの略。「AI（人工知能）」という言葉は、1956年に米国の計算機科学者ジョン・マッカーシーが初めて使った言葉。1950年代後半から1960年代が第一次AIブーム、1980年代が第二次AIブーム、現在は2000年代からはじまる第三次AIブームである。「AI」に関する確立した定義はないが、人間の思考プロセスと同じような形で動作するプログラム、あるいは人間が知的と感じる情報処理・技術といった広い概念で理解されている

…………… 1-1-1、4-1-1、4-2-5、5-2-1、5-2-2、5-2-3、6-1-1、6-1-3、19-2-1、19-2-4、19-2-5

■ BCP

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

…………… 2-3-2

■ CSIRT（シーサート）

Computer Security Incident Response Teamの略。コンピュータセキュリティにかかるインシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動を行う

…………… 2-1-3、6-1-3、7-5-3

■ CVSS

Common Vulnerability

Scoring Systemの略。情報システムの脆弱性に対するオープンで汎用的な評価手法のこと。ベンダーに依存しない共通の評価方法を提供している。CVSSを用いると、脆弱性の深さを同一の基準の下で定量的に比較できるようになる。ベンダー、セキュリティ専門家、管理者、ユーザなどの間で、脆弱性に関して共通の言葉で議論できるようになる。

…………… 17-2-1

■ DDoS攻撃（ディードスこ上げき）

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

…………… 2-2-2、2-2-5、第一回コラム、7-4-4、19-2-10

■ DFFT

Data Free Flow with Trustの略。日本が提案したコンセプトであり、ビジネスや社会的な課題を解決するために、データの国際的な自由な流れを促進すると同時に、プライバシー、セキュリティ、知的財産権に対する信頼を確保することを目指している

…………… 5-2-1

■ EDR

Endpoint Detection and Responseの略。パソコンやスマートフォン、サーバなどのエンドポイントにおける不審な動作を検知し、迅速な対応を支援するソリューション。

従来のツールやソリューションでは防げなかった未知のマルウェアや不正アクセスを検知し被害の拡大を防止する

…………… 2-2-4、2-2-5、3-1-1、3-4-1、12-3-1、16-2-1、17-2-4、19-2-3、19-2-10

■ eKYC

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

…………… 5-2-1

■ GビズID

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

…………… 5-2-1

■ ICSCoE中核人材育成プログラム

2017年4月にIPA内に設置された産業サイバーセキュリティセンター（Industrial Cyber Security Center of Excellence ICSCoE）が実施している人材育成プログラム。制御技術（OT：Operational Technology）と情報技術（IT）の両方の知識・スキルを有し、社会インフラ・産業基盤へのサイバーセキュリティリスクに対応できる人材の育成を目的としている

…………… 2-1-2

用語集

■ ICT

Information and Communication

Technologyの略。IT（情報技術）だけでなく、コンピュータやスマートフォンなどを用いて行うコミュニケーションを実現する技術（通信技術）を含んでいる

…………… 4-1-2、5-2-1、7-2-2、7-3-1、14-1-1、14-1-2、17-2-2、19-2-4、19-2-14

■ IDS

Intrusion Detection

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

…………… 17-1-2、17-2-4、17-2-5

■ IoT（アイ・オー・ティー）

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

…………… 1-1-1、2-1-2、2-2-2、4-1-1、4-2-5、5-2-2、5-2-3、6-1-2、7-4-3、7-4-4、19-2-2、19-2-5

■ IPS

Intrusion Prevention

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

IPSは、異常を検知した場合、

管理者に通知するだけでなく、その通信を遮断する

…………… 2-2-2、3-4-2、17-1-2、17-2-2、17-2-4、17-2-5

■ IPアドレス

コンピュータをネットワークで接続するために、それぞれのコンピュータに割り振られた一意になる数字の組み合わせ。IPアドレスは、

127.0.0.1のように0～255までの数字を4つ組み合わせたもので、単にアドレスと略されることがある。現在主に使用されているこれら4つになる数字の組み合わせによるアドレス体系は、IPv4

（アイ・ピー・ブイフォー）と呼ばれている。また、今後情報家電などで大量にIPアドレスが消費される時代に備えて、次期規格として、IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が進みつつある。なお、IPv6では、アドレス空間の増加だけでなく、情報セキュリティ機能の追加などの改良も加えられている

…………… 2-3-1、6-2-2、17-2-2

■ ISAC

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

…………… 14-1-2

■ ISMS

Information Security

Management Systemの略称。情報セキュリティを確保するための、組織的、人的、運用的、物理的、技術的、法令的な対策を含む、経営者を頂点とした総合的で組織的な取り組み。組織がISMSを構築するための要求事項をまとめた国際規格がISO/IEC 27001（国内規格はJIS Q 27001）であり、審査機関の審査に合格すると「ISMS認証」を取得できる

…………… 3-3-1、7-1-1、7-1-2、7-2-2、7-2-3、7-3-1、7-3-4、7-4-1、8-1-2、9-1-1、11-1-3、13-1-1、13-2-1、13-2-2、13-2-3、13-2-4、13-2-5、13-2-6、13-2-7、13-2-8、第七回コラム、14-1-1、15-1-1、16-1-1、17-1-1、19-1-1、19-1-2、19-2-7、19-2-8、19-2-9、19-2-11、19-2-13、19-2-14、19-2-15、19-2-16、19-2-17、19-3-1

■ ISP

個人や企業などに対してインターネットに接続するためのサービスを提供する事業者のこと。ユーザはISPと契約し、回線を用いてISPが運営するネットワークに接続することで、インターネット上のサーバーなどへアクセスできる。

…………… 14-1-2

■ ITリテラシー

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

…………… 3-1-1

用語集

■ JPCERT/CC

日本におけるセキュリティインシデントなどの報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行なっている組織。政府機関や企業等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。
…………… 14-1-2

■ JVN

Japan Vulnerability Notesの略。日本で使用されているソフトウェアなどの脆弱性関連情報と対策情報を提供する、脆弱性対策情報ポータルサイトのこと。
…………… 14-1-2

■ LockBit2.0

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

■ MACアドレス

Media Access Control addressの略。隣接する機器同士の通信を実現するためのアドレスのこと。ネットワーク機器やPC、ルータなどについている固有の識別番号で、一般的に12桁の16進数で「00-00-00-XX-XX-XX」などと表される。
…………… 17-2-2

■ NISC

National center of Incident readiness and Strategy for

Cybersecurityの略。内閣サイバーセキュリティセンターの略称。サイバーセキュリティに関する施策の立案や実施、行政各部の情報システムに対するセキュリティ対策の強化を担当
…………… 5-2-1、6-1-3、12-3-1、19-1-1、19-2-6

■ NIST サイバーセキュリティフレームワーク (CSF)

米国政府機関の重要インフラの運用者を対象として誕生し、防御にとどまらず、検知・対応・復旧といったステップも含み、インシデント対応を含めており、日本も今後普及が見込まれる
…………… 3-3-1、7-1-1、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-3-4、19-2-7

■ NTP

Network Time Protocolの略。あらゆる機器の時刻情報を同期するためのプロトコル（通信規約）のこと。時刻情報を配信するサーバと、時刻合わせを行うクライアント間、およびサーバ間の通信方法を定めている。
…………… 17-1-2

■ PII

Personally Identifiable Informationの略。「個人を特定できる情報」と訳されることが多いが、実際には個人を特定するために使用される情報のこと。個人と1対1に紐づいているマイナンバー、メールアドレス、携帯電話番号、銀行口座番号だけでなく、氏名、生年月日、住所、勤務先などの情報もPIIに含まれ

る。
…………… 14-1-1、14-1-2、17-1-2、19-2-14

■ RPA

Robotic Process Automationの略。定型的な業務をソフトウェアのロボットにより自動化すること
…………… 4-2-3、19-2-14

■ SASE (サシー)

Secure Access Service Edgeの略。2019年に提唱されたゼロトラストセキュリティを実現する方法の1つで、IT環境のネットワークの機能とセキュリティの機能をクラウド上で統合して提供するサービス、また、その考え方・概念
…………… 2-2-4、17-2-2

■ SBOM (エスボム)

Software Bill of Materialsの略。ソフトウェアを構成する要素を一覧できるリストのこと。SBOMは、ソフトウェアの構成要素の名称やバージョン情報、開発者、依存関係などの情報を含む。SBOMは、ソフトウェアのリスクを把握・管理するのに役立つ
…………… 6-1-1

用語集

■ SDP

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

…………… 2-2-5、
17-2-2、17-2-4

■ SECURITY ACTION

中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度

…………… 2-1-2、
3-3-1、19-1-2、19-2-3

■ SLA

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

…………… 17-1-2

■ Society5.0

サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）

…………… 1-1-1、
4-1-1、5-2-2、6-1-1、7-1-1、7-4-1、7-4-2、7-4-3、
19-1-1、19-2-1、19-2-4、
19-2-5、19-3-1

■ SSL/TLS

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

…………… 14-1-2、
17-1-2

■ SWG

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

…………… 2-2-4、
17-2-2、17-2-4

■ VPN

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

…………… 2-1-3、
2-2-2、2-2-5、2-3-1、2-3-2、2-3-3、12-3-1、13-2-2、14-1-2、15-1-2、

16-2-1、17-2-2、17-2-3、
19-3-1

■ WAF（ワフ）

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

…………… 2-2-2

■ WAN

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

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

…………… 17-2-3

■ アクセス制御

特定のデータやファイル、コンピュータ、ネットワークにアクセスできるユーザを制限する機能のこと

…………… 2-2-5、
第一回コラム、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、
9-1-1、14-1-1、14-1-2、
17-1-1、17-2-2、17-2-4、
19-2-9、19-2-14

用語集

■ アセスメント

システムや運用環境などを客観的に調査・評価すること。現在の利用状況を把握することで、システムの再構築や運用改善の参考情報となる
…………… 2-2-4、7-3-1、7-4-5、11-1-2、17-1-1、17-1-2

■ 暗号化

データの内容を変換し、第三者には、内容を見ても解読できないようにすること
…………… 2-1-3、2-2-1、2-2-5、2-3-2、3-3-3、3-4-1、第一回コラム、12-2-1、12-3-1、14-1-1、14-1-2、16-1-2、17-1-2、17-2-3、17-2-5

■ アンダーグラウンドサービス

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

■ イベントログ

コンピュータシステムに起こった出来事や、行われた操作などを時系列に記録したデータのこと。
…………… 17-1-2、19-3-1

■ インターネットバンキング

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

…………… 3-2-2、11-1-2

■ ウイルス定義ファイル（パターンファイル）

セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの
…………… 3-2-2、3-3-3、12-3-1、17-1-2

■ エンティティ

個人、組織、団体、コンピュータシステム、通信機器など、多様な実体のこと
…………… 7-2-1、17-2-2

■ エンドポイントデバイス

ネットワークに接続して、ネットワークを介して情報を交換するデバイス（デスクトップコンピュータ、仮想マシン、サーバなど）
…………… 2-2-4、17-1-1、17-2-2、17-2-4

■ 改ざん

文書や記録などのすべてまたは一部に対して、無断で修正・変更を加えること。IT分野では、権限を持たない者が管理者に無断でコンピュータにアクセスし、データの書き換え・作成・削除などをする行為
…………… 2-1-2、5-2-2、6-1-3、7-4-4、8-1-2、11-2-2、11-3-1、12-3-1、14-1-1、14-1-2、17-1-2、17-2-3

…………… 2-1-2、5-2-2、6-1-3、7-4-4、8-1-2、11-2-2、11-3-1、12-3-1、14-1-1、14-1-2、17-1-2、17-2-3

■ 可用性

許可された者だけが必要なときにいつでも情報や情報資産にアクセスできる特性

…………… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1、14-1-2、16-1-1、17-1-1、17-1-2、17-2-4、19-2-7

■ 完全性

参照する情報が改ざんされていない、正確である特性
…………… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1、16-1-1、17-1-2、17-2-4、19-2-7

■ 機密性

許可された者だけが情報や情報資産にアクセスできる特性
…………… 第一回コラム、7-1-2、7-2-1、7-2-2、9-1-2、11-2-2、12-2-1、13-2-4、13-2-5、14-1-1、16-1-1、17-1-2、17-2-4、19-2-7

■ 脅威インテリジェンス

サイバー攻撃などの脅威への対応を支援することを目的として、収集・分析・蓄積された情報のこと。一部の産業では、企業横断的にこうした情報（インテリジェンス）を共有する活動が行われている。
…………… 14-1-1、14-1-2、17-2-1、19-2-14

用語集

■ 供給者

組織に対して、製品・サービスを供給する企業または個人のこと。製品の場合、PCやサーバ、通信機器などがある。サービスの場合、クラウドサービス、インターネット接続サービス、業務の委託、物流、教育などがある。

…………… 14-1-1、
14-1-2、17-2-1、17-2-2、
19-2-9、19-2-14

■ クラッキング

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

…………… 第一回コラム

■ クリーンインストール

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

…………… 17-2-5

■ 限定提供データ

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

…………… 11-2-2

■ 個人情報保護委員会

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

…………… 2-2-3、
5-2-1、6-2-1、8-1-2、14-1-2

■ コーディング

プログラミング言語でソースコードを書くこと。

…………… 17-1-1、
17-1-2、17-2-1、19-2-17

■ サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、個人が所有するパソコンやスマートフォンから、企業のサーバやデータベース、国の重要インフラまで様々である。ネット社会となった現代では、インターネット空間をサイバー空間と呼ぶ。サイバー空間において、敵対する国家、企業、集団、個人などを攻撃する行為やその防御をサイバー戦争と呼ぶこともある。

…………… 2-1-2、
2-1-3、2-2-2、2-2-5、2-3-2、3-3-1、4-3-1、4-3-2、
5-2-2、5-2-3、6-1-1、6-1-2、6-1-3、7-1-2、7-3-4、
7-4-1、7-5-2、7-5-3、12-3-1、13-2-4、13-2-5、
14-1-2、17-2-2、17-2-3、
17-2-4、18-1-2、19-1-1、

19-1-2、19-2-2、19-2-4、
19-2-5、19-2-7、19-2-8、
19-2-10、19-2-18、19-3-1

■ サイバーセキュリティお助け隊サービス制度

中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービス

…………… 2-1-2

■ サイバーセキュリティ戦略

組織や企業がセキュリティに関する目標を達成するための計画やアプローチ

…………… 3-3-1、
5-1-1、6-1-1、19-1-1、
19-2-6、19-3-1

■ サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

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

…………… 3-3-1、
7-1-1、7-1-2、7-4-1、7-4-2、7-4-3、7-4-4、7-4-5、
19-1-2、19-2-7

用語集

■ サプライチェーン

製品やサービスの供給に関わる一連のプロセスのこと。具体的には、原材料や部品の調達、生産、物流、販売など、製品やサービスが最終的に消費者に届くまでの流れを指す。サプライチェーンは、製造業者、卸売業者、小売業者などが協力して構築される

…………… 2-1-3、
2-2-2、2-2-4、4-1-1、4-2-4、4-3-2、5-1-1、5-2-2、6-1-1、6-1-2、6-1-3、7-1-2、7-2-2、7-3-1、7-3-2、7-3-3、7-4-1、7-4-2、7-4-3、7-4-5、7-5-1、7-5-2、14-1-1、14-1-2、17-2-2、18-1-2、19-1-2、19-2-2、19-2-5、19-2-14

■ サポートユーティリティ

情報システムを運用する施設の稼動に不可欠な設備やライブライン、公共インフラのこと。ISO/IEC 27002:2022では、サポートユーティリティの例として、電気、通信サービス、給水、ガス、下水、換気、空調をあげている。

…………… 16-1-1、
16-1-2、19-2-16

■ シャドーIT

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

…………… 16-2-1、
17-2-2、19-2-16

■ 磁気データ消去装置

ハードディスクに強力な磁気

を照射することで、ハードディスク内の磁気記録領域に記録されている情報を破壊する装置のこと。短時間で効率よく、大量のハードディスクのデータを完全に消去できる。
…………… 17-1-2

■ 情報資産

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

…………… 3-3-1、
7-2-1、7-2-2、7-3-4、7-4-4、7-5-1、8-1-2、11-1-1、11-1-2、11-2-2、11-2-3、12-2-1、12-3-1、13-2-3、13-2-4、13-2-5、13-2-7、第七回コラム、14-1-2、16-1-2、17-2-2、17-2-4、18-1-2、19-2-10、19-2-17、19-2-18

■ 情報セキュリティ事象

情報セキュリティ上よくない、システムやサービス、ネットワークの状態のこと。情報セキュリティ事象の中でも、事業運営を危うくしたり、情報セキュリティを脅かしたりする可能性が高いものは、セキュリティインシデントに分類される。

…………… 14-1-1、
14-1-2、15-1-1、15-1-2、17-1-2、17-2-4、19-2-14、19-2-15

■ 情報セキュリティの3要素「CIA」

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

ラム、第五回コラム

■ 真正性

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

…………… 2-1-3、
第一回コラム、6-1-3、7-2-1、第五回コラム、17-1-2

■ 信頼性

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

…………… 第一回コラム、6-1-1、6-1-3、7-2-1、7-4-2、7-4-3、7-4-4、第五回コラム、13-2-5、14-1-2、17-1-2

■ スクリーンセーバ

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

…………… 17-1-2

■ スクリーンロック

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

…………… 2-2-2、
16-1-2

用語集

■脆弱性

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

…………… 2-1-1、
2-1-3、2-2-1、2-2-2、2-2-4、2-2-5、2-3-1、2-3-2、2-3-3、3-3-1、第一回コラム、6-1-3、7-2-2、7-4-4、7-4-5、9-1-2、10-1-1、11-1-2、11-1-3、11-2-2、11-2-3、11-3-1、13-2-4、14-1-1、14-1-2、17-1-1、17-1-2、17-2-1、17-2-4、19-1-1、19-1-2、19-2-2、19-2-10

■脆弱性診断

システムや機器などにおいて、セキュリティ上の欠陥がないか診断すること

…………… 2-3-1、
17-2-1

■責任追跡性

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

…………… 第一回コラム、7-2-1、第五回コラム

■セキュリティインシデント

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

…………… 2-1-1、
2-1-2、2-1-3、2-2-1、4-1-1、7-2-2、7-3-1、7-4-4、9-1-1、9-1-2、12-1-1、12-2-1、13-2-2、13-2-4、

13-2-5、13-2-8、14-1-1、14-1-2、17-1-1、17-1-2、17-2-1、17-2-4、17-2-5、19-1-1、19-2-2、19-2-9、19-2-12、19-2-14、19-3-1

■セキュリティ・キャンプ

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

…………… 2-1-2

■セキュリティホール

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

…………… 3-3-1

■セキュリティポリシー

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

…………… 2-1-1、
2-2-1、3-3-1、6-1-2、7-4-4、8-1-1、17-2-4、19-2-2、19-2-8

■ゼロデイ攻撃

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

…………… 2-1-3

■ゼロトラスト

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

…………… 2-2-4、
17-2-2、19-2-17

■ソフトウェアライブラリ

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

…………… 17-1-1

■ソリューション

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

…………… 2-2-5、
14-1-2、17-1-2、17-2-2、
17-2-4

用語集

■ダークウェブ

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

…………… 2-1-3

■多要素認証

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

…………… 2-2-5、
2-3-3、8-1-2、第五回コラム、11-3-1、12-3-1、14-1-2、17-1-2

■データサイエンス

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

…………… 1-1-1

■データマスキング

個人情報や機密情報が含まれるデータを扱う際に、特定の部位のみを無意味な符号（ア

スタリスク「※」など）に置き換える処理のこと。もとのデータの一部を秘匿化し、個人や機密情報を識別できないようにすることで、データ分析やテストデータなどに利用可能とする。

…………… 17-1-1、
17-1-2、19-2-17

■デジタル化

紙などで管理されてきた情報（非デジタル情報）をデジタル化するデジタイゼーション（digitization）と、デジタル技術を用いてビジネス・プロセスを自動化・合理化するデジタルイゼーション（digitalization）がある。

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

…………… 1-1-1、
2-1-1、2-1-2、3-3-1、4-1-2、4-2-3、5-1-1、6-1-1、6-1-3、7-4-3、19-2-1、19-2-4、19-2-5

■デジタル情報

0、1、2のような離散的に（数値として）変化する量…………… 第一回コラム

■トラフィック

通信回線やネットワーク上で送受信される信号やデータ、データ量のこと。

…………… 17-2-2、
17-2-3

■内部監査

内部の独立した監査組織が業

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

…………… 3-3-1、
7-2-1、7-3-1、13-2-3、13-2-7、13-2-8、14-1-2、18-1-1、19-2-18、19-3-1

■ハウジングサービス

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

…………… 12-3-1

■ビジネスインパクト分析

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

…………… 14-1-2

■ビジネスメール詐欺

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

…………… 2-1-3

用語集

■ビッグデータ

全体を把握することが困難な程、膨大な規模のデータ群
…………… 1-1-1、
5-2-2、5-2-3、19-2-1

■否認防止性

システムに対する操作・通信のログを取得や本人に認証させることにより行動を否認させないようとする特性
…………… 第一回コラム、第五回コラム

■標的型攻撃

機密情報を盗み取ることなどを目的として、特定の個人や組織を狙った攻撃。業務関連のメールを装ったウイルス付きメール（標的型攻撃メール）を、組織の担当者に送付する手口が知られている。従来は府省庁や大手企業が中心に狙われてきたが、最近では地方公共団体や中小企業もそのターゲットとなっている
…………… 2-1-2、
2-1-3、12-3-1、13-2-5、
19-2-10

■標的型メール攻撃

特定の個人や組織を標的にしたフィッシング攻撃の一種。一般のフィッシング攻撃とは異なり、業界ニュースや社内情報といった情報を利用するため、業務上のメールと見分けがつかない内容や、業務で付き合いがある人物の名前で送られることもある
…………… 2-2-4、
19-2-2

■ファイアウォール

本来は「防火壁」のことだが、情報セキュリティの世界では、外部のネットワークからの攻

撃や不正なアクセスから企業や組織のネットワークやコンピュータ、データなどを守るためのソフトウェアやハードウェアを指す。パソコンのOSに付随しているもの、セキュリティソフトに付いているもの、専用のハードウェアになっているものなど形態は様々である

…………… 2-3-1、
3-4-1、3-4-2、13-2-2、
14-1-2、17-1-2、17-2-2、
17-2-3、17-2-4、17-2-5

■ファイル共有ソフト

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

…………… 16-2-1、
17-1-2

■不正アクセス

利用権限を持たない悪意のあるユーザが、企業や組織で管理されている情報システムやサービスに不正にアクセスすること。不正アクセスにより、正規の個人情報の窃取やデータの改ざんや破壊などの危険がある。日本では、2000年2月に施行された不正アクセス行為の禁止などに関する法律（不正アクセス禁止法）により、法律で固く禁じられている

…………… 2-1-1、
2-1-2、2-1-3、2-2-1、2-
2-2、2-2-3、2-2-5、2-3-1、
4-3-2、5-2-1、7-4-4、8-
1-2、11-2-2、11-3-1、
14-1-2、16-2-1、17-1-2、
17-2-2、17-2-5、19-2-2、
19-2-10、19-2-16、19-3-
1

■踏み台

不正侵入の中継地点として利用されるコンピュータのこと。他人のコンピュータに侵入するときに、直接自分のコンピュータから接続すると、接続元のIPアドレスによって、犯人が特定されてしまう可能性がある。そこで、いくつかのコンピュータを経由してから、目的のコンピュータに接続することで、犯人が自分のコンピュータを探しにくくする。このように、現実的な被害はないけれども、不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と呼ぶ

…………… 2-1-3、
4-3-2、18-1-2

■フォレンジック

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

「デジタル・フォレンジック」や「コンピュータ・フォレンジック」などと呼ばれる
…………… 2-2-3、
2-3-2、17-2-5、19-2-17

用語集

■ブラックマーケット

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

■フレームワーク

フレームワーク（サイバーセキュリティフレームワーク）とは、マルウェアやサイバー攻撃など様々なセキュリティ上の脅威から、情報システムやデータを守るために、システム上の仕組みや人的な体制の整備を整える方法を「ひな形」としてまとめたもの
…………… 2-2-4、
3-4-1、7-1-1、7-1-2、7-2-1、7-3-1、7-3-2、7-4-1、8-1-1、8-1-2、9-1-2、13-1-1、19-1-1、19-1-2、19-2-7、19-2-8、19-2-13、19-3-1

■プロキシ

クライアントとサーバの間で、両者の通信を中継する役割を担うサーバのこと。プロキシは、クライアントからのリクエストやサーバからの応答をすべて把握することが可能なため、詳細な通信内容をログとして記録したり、Webサーバから送られてきたコンテンツをチェックし、不正なコードやマルウェアが含まれていないかをチェックしたりできる。
…………… 17-2-4

■ブロックチェーン

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

■ペネトレーションテスト

ネットワークに接続されたシステムの安全性を検証するテスト手法。すでに知られているサイバー攻撃手法を使って実際にシステムに侵入や攻撃を試みることで攻撃耐性を確認する。
…………… 17-2-1

■ベストプラクティス

何かを行う方法や工程、その実践例の中で、ある基準にしたがって最も優れていると評価されたもののこと。実績や経験に基づいて確立された成功例やよい成果をもたらす方法論
…………… 2-1-3、
2-3-1、7-1-1、19-2-2

■マルウェア

パソコンやスマートフォンなどのデバイスやサービス、ネットワークに害を与えたり、悪用したりすることを目的として作成された悪意のあるソフトウェアの総称。コンピュータウイルスやワームなどが含まれる
…………… 2-2-2、
2-2-4、2-2-5、第一回コラム、7-2-2、12-3-1、13-2-4、14-1-1、14-1-2、15-1-2、16-2-1、17-1-1、17-1-2、17-2-2、17-2-4、19-2-17

■ミラサポコネク

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「ミラサポコネク構想」をもとにした、行政、支援者、民間事業者に分散して保有されているデータ（法人情報、決算情報、経営カルテなど）を連携し、経営課題解決に資する支援を提供する

ための、官民データ連携基盤
…………… 5-2-1

■ミドルウェア

OSとアプリケーションの間に位置するソフトウェアのこと。アプリケーションが業務に関する処理を行う際、データベースやサーバのやりとりをミドルウェアが担うことで複雑な処理を行うことができる。
…………… 17-2-1、
17-2-3

■無線LAN

LAN（は Local Area Network の略。物理的なケーブルを使わず、電波を利用してネットワークに接続する仕組み。この無線LANを通じて、コンピュータはインターネットにアクセスできる
…………… 3-2-3、
14-1-2、16-1-2、17-1-2

■無停電電源装置

UPSとも呼ばれる。停電が起きてしまったときに電気を一定時間供給し続けるための装置のこと。パソコンやハードディスク、サーバなどを予期せぬ停電から守れる。
…………… 16-1-2

■ユーティリティプログラム

コンピュータで、システムの運用を支援するプログラムのこと。具体的には、記憶媒体間のデータ転送、ファイルの複写・削除・整理などの処理を行うためのプログラムのこと。システムおよびアプリケーションによる制御を無効にすることのできるものもある。
…………… 17-1-1、
17-1-2、19-2-17

用語集

■ ランサムウェア

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

…………… 2-1-2、
2-1-3、2-2-1、2-2-2、2-
2-5、2-3-2、2-3-3、7-5-1、
8-1-2、14-1-2、17-1-2、
17-2-4、17-2-5、19-2-2

■ リスクアセスメント

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

…………… 3-3-1、
7-3-1、7-4-5、第四回コ
ラム、11-1-1、11-1-2、11-
1-3、11-2-1、11-2-2、
11-3-1、12-2-1、13-2-4、
13-2-5、13-2-6、13-2-7、
13-2-8、14-1-1、14-1-2、
15-1-1、16-1-1、17-1-1、
17-1-2、19-1-1、19-1-2、
19-2-11、19-2-14、19-2-
15、19-2-16、19-2-17、
19-3-1

■ リスク評価


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

…………… 2-3-2、
3-4-1、7-3-2、7-4-5、11-
1-2、11-2-4、11-3-1、
12-2-1、13-2-4、第七回コ
ラム、17-2-4、19-2-11

■ リモートデスクトップ接続

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

…………… 2-2-2



**令和5年度
中小企業サイバーセキュリティ対策
継続支援事業**
