# 令和7年度
# 中小企業サイバーセキュリティ
# 実践力強化プログラム

## 第5回

第7編：ISMSの構築と対策基準の策定と実施手順
その2（第14章～第19章）


東京都産業労働局

# 講師紹介

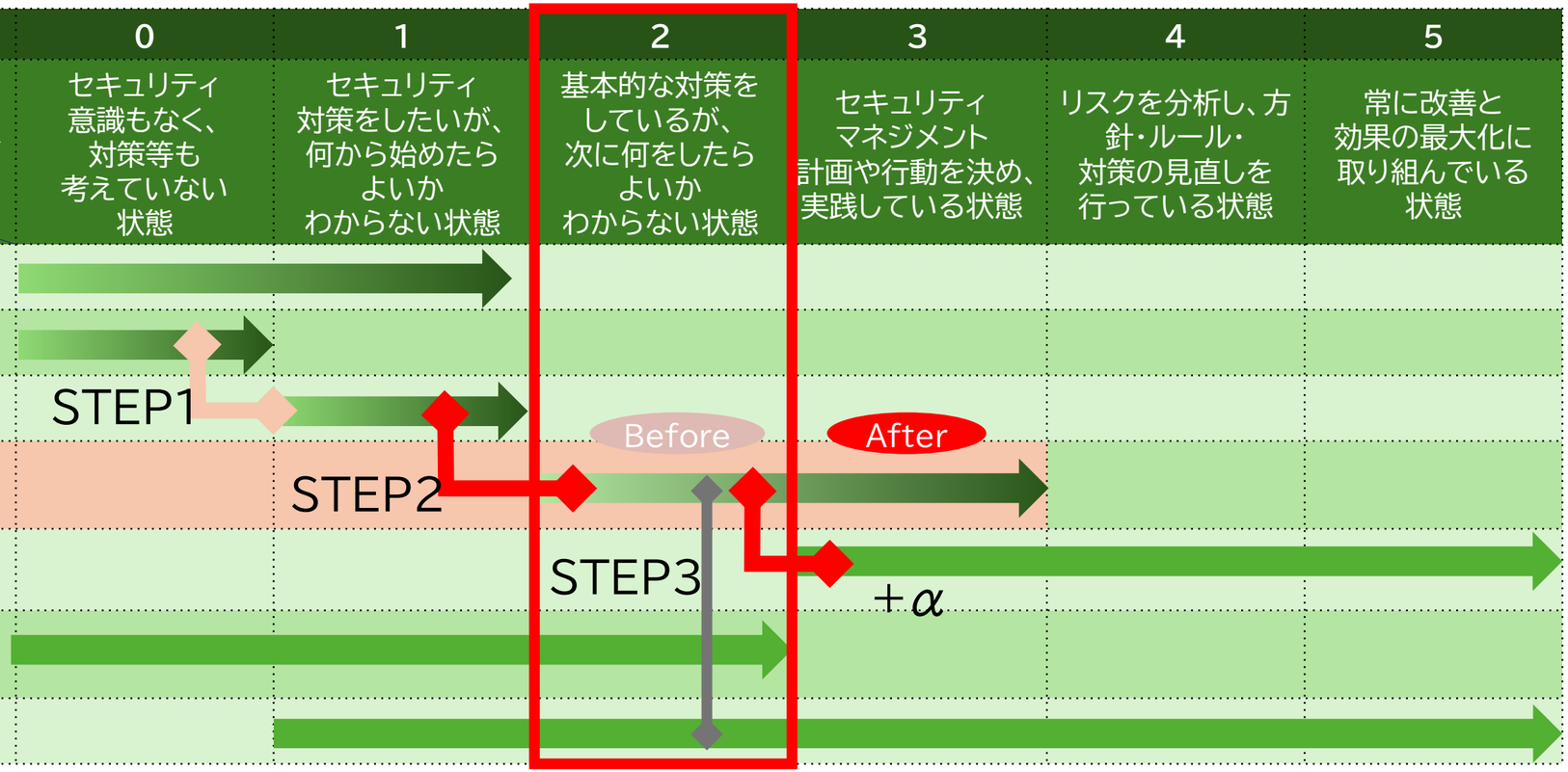
| | |
|---|---|
| 氏名 | 矢野　泰広（やの　よしひろ） |
| 業務経歴 | 26年（セキュリティ経験：15年） |
| 専門分野 | 情報セキュリティ、DX、ICT、クラウド技術、<br>ネットワーク技術、DB設計・構築、プロジェクト<br>マネジメント、WEBシステム設計・構築、<br>サーバ設計・構築 |
| 保有資格 | 情報処理安全確保支援士（第004005号）<br>経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、<br>情報処理技術者第一種、情報処理技術者第二種<br>インターネット検定 .com Master ADVANCE★★<br>生成AIパスポート<br>家電製品アドバイザー（AV情報家電・生活家電） |
| コメント | 中小企業を中心にDX、ネットワーク、クラウド技術および情報セキュリティに関する構築や導入支援やコンサルティングの経験が豊富。併せて長年にわたり大手通信事業者のSE（技術営業）を対象に指導を行ってきた事から、幅広い業種、業態の企業の状況を認識しており、中小企業の課題点を的確に捉え、各企業が取り組みやすい解決策を提示する対応力に定評がある。 |

# 目的

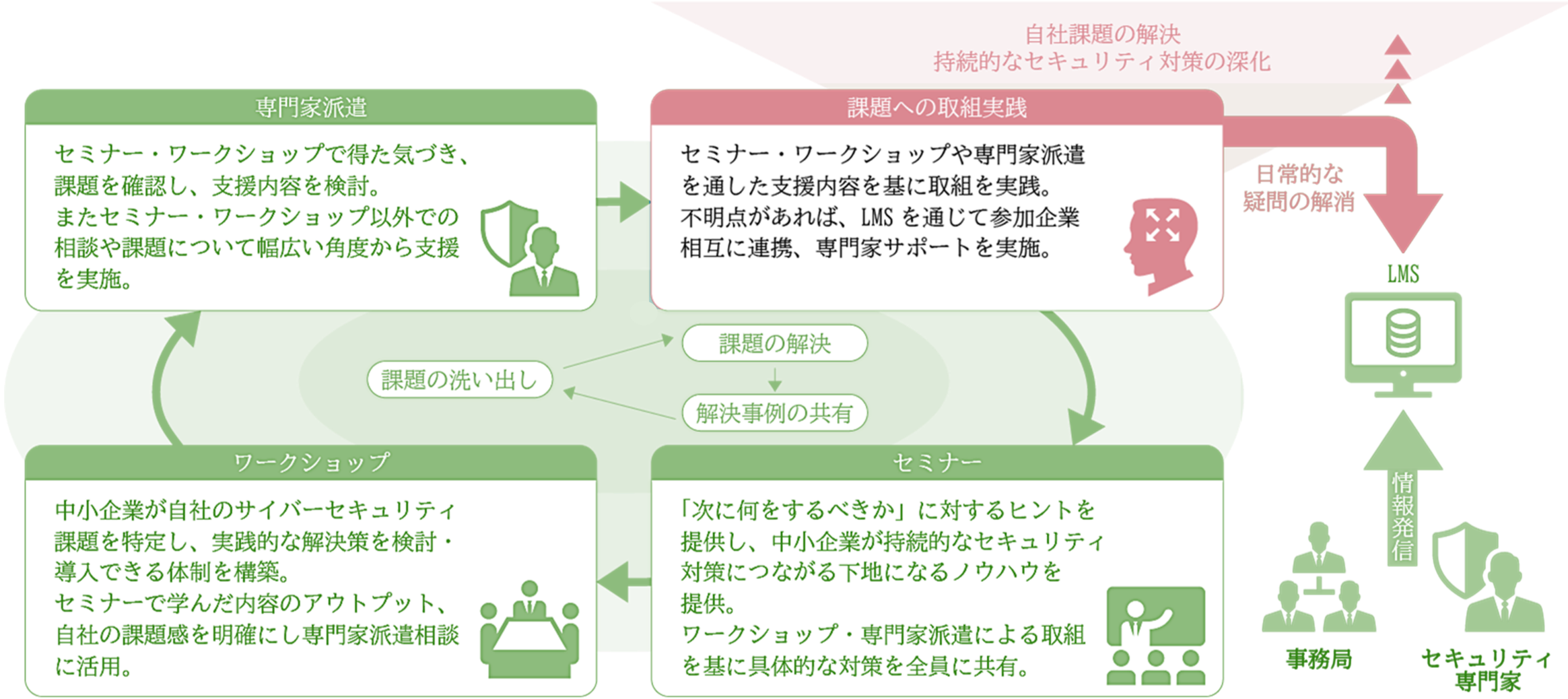
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

## 東京都他事業と本事業の位置づけ

| 成熟度レベル　※COBITを援用し設定 | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| ステータス / 事業と主な支援領域 | セキュリティ意識もなく、対策等も考えていない状態 | セキュリティ対策をしたいが、何から始めたらよいかわからない状態 | 基本的な対策をしているが、次に何をしたらよいかわからない状態 | セキュリティマネジメント計画や行動を決め、実践している状態 | リスクを分析し、方針・ルール・対策の見直しを行っている状態 | 常に改善と効果の最大化に取り組んでいる状態 |
| 中小企業サイバーセキュリティの極意 | | | | | | |
| 中小企業サイバーセキュリティ 啓発事業 | | | | | | |
| 中小企業サイバーセキュリティ 基本対策事業 | | | | | | |
| 中小企業サイバーセキュリティ実践力強化プログラム（本事業） | | | | | | |
| 中小企業サイバーセキュリティインシデント対応力強化 | | | | | | |
| Tcyss（東京中小企業サイバーセキュリティ支援ネットワーク） | | | | | | |
| サイバーセキュリティ対策促進助成金 | | | | | | |



# 支援内容の全体像


自社課題の解決
持続的なセキュリティ対策の深化
専門家派遣
セミナー・ワークショップで得た気づき、課題を確認し、支援内容を検討。
またセミナー・ワークショップ以外での相談や課題について幅広い角度から支援を実施。
課題への取組実践
セミナー・ワークショップや専門家派遣を通した支援内容を基に取組を実践。
不明点があれば、LMS を通じて参加企業相互に連携、専門家サポートを実施。
日常的な
疑問の解消
LMS
課題の解決
課題の洗い出し
解決事例の共有
ワークショップ
中小企業が自社のサイバーセキュリティ課題を特定し、実践的な解決策を検討・導入できる体制を構築。
セミナーで学んだ内容のアウトプット、自社の課題感を明確にし専門家派遣相談に活用。
セミナー
「次に何をするべきか」に対するヒントを提供し、中小企業が持続的なセキュリティ対策につながる下地になるノウハウを提供。
ワークショップ・専門家派遣による取組を基に具体的な対策を全員に共有。
情報発信
事務局
セキュリティ専門家

# スケジュール

| 支援内容 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
|---|---|---|---|---|---|---|---|---|---|
| セミナー・ワークショップ（全10回） | 7/25（金） | 8/8（金） 8/27（水） | 9/11（木） 9/25（木） | 10/10（金） 10/27（月） | 11/17（月） | 12/12（金） | 1/16（金） | | |
| 専門家派遣（全4回） | 1回目 | | 2回目 | 3回目 | | 4回目 | | | |
| 事例集 | | | | | | ご参加いただいた企業様への取材 | 事例集作成期間 | 公表3月下旬～ | |

# セミナー内容

| 実施回 | 編 | テーマ |
|---|---|---|
| 第1回<br>7/25<br>（金） | 第0編 | はじめに |
| | 第1編 | サイバーセキュリティを取り巻く背景 |
| | 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 |
| 第2回<br>8/8<br>（金） | 第3編 | これからの企業経営に必要なIT活用とサイバーセキュリティ対策 |
| | 第4編 | セキュリティ事象に対応して組織として対策すべき対策基準と具体的な実施 |
| | 第5編 | 各種ガイドラインを参考にした対策の実施 |

# セミナー内容

| 実施回 | | 編 | テーマ |
|---|---|---|---|
| 第3回 | 8/27(水) | 第6編 | ISMSなどのフレームワークの種類と活用法の紹介 |
| 第4回<br>第5回 | 9/11(木)<br>9/25(木) | 第7編 | ISMSの構築と対策基準の策定と実施手順 |
| 第6回<br>第7回 | 10/10(金)<br>10/27(月) | 第8編 | 具体的な構築・運用の実践 |
| 第8回 | 11/17(月) | 第9編 | 中小企業が組織として実践するためのスキル・知識と人材育成 |
| 第9回 | 12/12(金) | 第10編 | サイバーレジリエンス能力の育成 |
| 第10回 | 2026年<br>1/16(金) | 第11編 | 全体総括 |

# 第14章. ISMSの管理策

## 管理策の分類と構成

# 管理策の分類と構成

【参照:テキスト14-1-1.】
P2

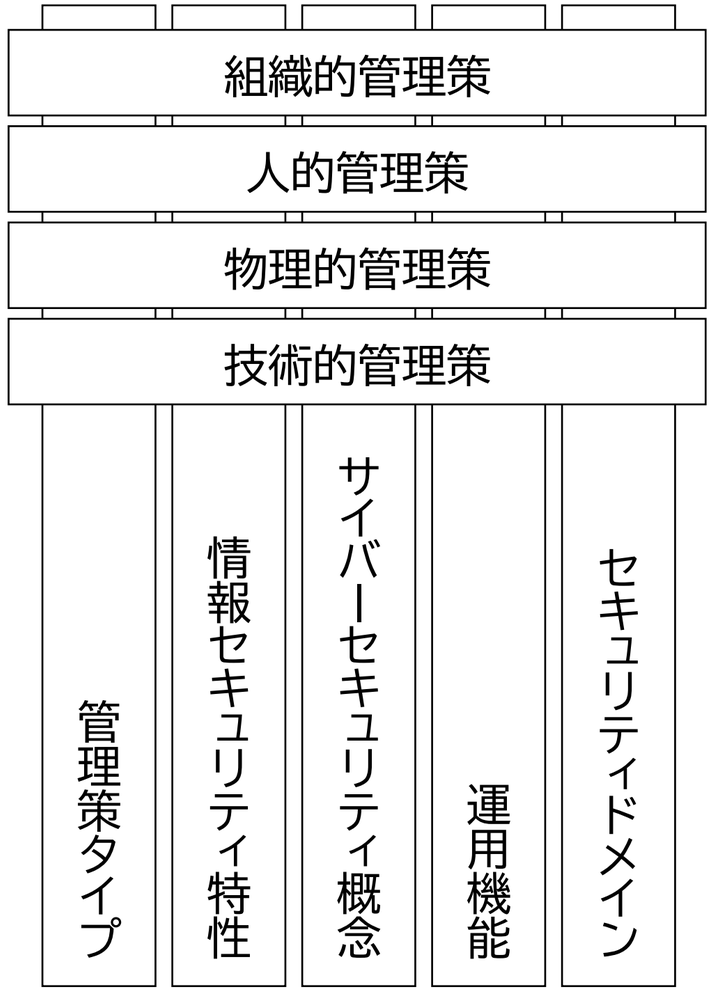
## 管理策:ISO/IEC 27002

### 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

改訂

### ISO/IEC 27002:2022



# 管理策の分類と構成

【参照:テキスト14-1-2.】
P3～P5

## 管理策のテーマと属性

| カテゴリ | 属性数 | 関連するガイドラインなど |
|---|---|---|
| 管理策タイプ | 3 | ― |
| 情報セキュリティ特性 | 3 | ISO/IEC 27001 |
| サイバーセキュリティ概念 | 5 | サイバーセキュリティフレームワーク |
| 運用機能 | 15 | ISO/IEC 27002:2022 |
| セキュリティドメイン | 4 | ― |

## 各テーマより管理策の例示

- ISO/IEC 27002 附属書Aに記載
- 使い方は別紙、ISMS管理策の属性説明資料を参照

# 管理策の分類と構成

【参照:テキスト14-1-3.】
P5～P6

## 対策基準と実施手順の作成方法

1. 管理策の決定
   a. リスクアセスメント結果を考慮し、適切なリスク対応を選択する
   b. 実施に必要なすべての管理策を決定する

2. 管理策の検証
   a. 必要な管理策の見落としがないか検証する

3. 適用宣言書の作成
   a. 必要な管理策と実施する理由を記載する
   b. 管理策をすでに実施しているかを記載する
   c. 管理策を除外した理由を記載する

4. 実施手順の作成
   a. 具体的な実施手順を作成する

# 第15章. 組織的対策

作成する候補となる実施手順書類について

組織的対策として重要となる実施項目

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.1 情報セキュリティのための方針群

情報セキュリティ方針およびトピック固有の個別方針は、これを定義し、経営陣によって承認され、発行し、関連する要員および関連する利害関係者へ伝達し認識され、計画した間隔でおよび重要な変化が発生した場合にレビューしなければならない。
【実施手順：テキストP14】

## 5.2 情報セキュリティの役割および責任

情報セキュリティの役割および責任を、組織の要求に従って定め、割り当てなければならない。
【実施手順：テキストP14～P15】

## 5.3 職務の分離

相反する職務および責任範囲は、分離しなければならない。
【実施手順：テキストP16】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.4 経営陣の責任

経営陣は、組織の確立された情報セキュリティ方針、トピック固有の個別方針および手順に従った情報セキュリティの適用を、すべての要員に要求しなければならない。
【実施手順：テキストP16】

## 5.5 関係当局との連絡

組織は、関係当局との連絡体制を確立および維持しなければならない。
【実施手順：テキストP16】

## 5.6 専門組織との連絡

組織は、情報セキュリティに関する研究会または会議、および情報セキュリティの専門家からの協会・団体との連絡体制を確立し維持しなければならない。
【実施手順：テキストP17～P18】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.7 脅威インテリジェンス

情報セキュリティの脅威に関連する情報を収集および分析し、脅威インテリジェンスを構築しなければならない。
【実施手順：テキストP22～P23】

## 5.8 プロジェクトマネジメントにおける情報セキュリティ

情報セキュリティをプロジェクトマネジメントに組み入れなければならない。
【実施手順：テキストP18】

## 5.9 情報及びその他の関連資産の目録

管理責任者を含む情報およびその他の関連資産の目録を作成し、維持しなければならない。
【実施手順：テキストP23】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.10 情報及びその他の関連資産の利用の許容範囲

情報およびその他の関連資産の利用並びに取扱い手順の許容範囲に関する規則は、明確にし、文書化し、実施しなければならない。
【実施手順：テキストP23～P24】

## 5.11 資産の返却

要員および必要に応じてその他の利害関係者は、雇用、契約または合意の変更または終了時に、自らが所持する組織の資産のすべてを返却しなければならない。
【実施手順：テキストP24～P25】

## 5.12 情報の分類

情報は、機密性、完全性、可用性および関連する利害関係者の要求事項に基づく組織の情報セキュリティの要求に従って分類しなければならない。
【実施手順：テキストP18～P19】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.13 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は、「5.12 情報の分類」で確立した分類体系に従って策定し、実施しなければならない。
【実施手順：テキストP19】

## 5.14 情報転送

情報転送の規則、手順または合意を、組織内および組織と他の関係者との間のすべての種類の転送設備に関して備えなければならない。
【実施手順：テキストP19～P20】

## 5.15 アクセス制御

情報およびその他の関連資産への物理的および論理的アクセスを制御するための規則を、業務および情報セキュリティの要求事項に基づいて確立し、実施しなければならない。
【実施手順：テキストP20～P21】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.16 識別情報の管理

組織の情報およびその他の関連資産にアクセスする個人およびシステムを一意に特定できるようにし、アクセス権を適切に割り当てなければならない。
【実施手順：テキストP21】

## 5.17 認証情報

認証情報の割り当ておよび管理は、認証情報の適切な取扱いについて要員に助言することを含む管理プロセスによって管理しなければならない。
【実施手順：テキストP21】

## 5.18 アクセス権

情報およびその他の関連資産へのアクセス権は、アクセス制御に関する組織のトピック固有の個別方針および規則に従って、提供、レビュー、変更および削除しなければならない。
【実施手順：テキストP22】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.19 供給者関係における情報セキュリティ

供給者の製品またはサービスの使用に関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定義し実施しなければならない。【実施手順：テキストP30】

## 5.20 供給者と合意における情報セキュリティの取扱い

供給者関係の種類に応じて、各供給者と、関連する情報セキュリティ要求事項を確立し合意をとらなければならない。
【実施手順：テキストP30】

## 5.21 ICTサプライチェーンにおける情報セキュリティの管理

ICT 製品およびサービスのサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセスおよび手順を定め、実施しなければならない。
【実施手順：テキストP31】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.22 供給者のサービス提供の監視、レビュー及び変更管理

サービスの供給者の情報セキュリティの実践およびサービス提供の変更を定常的に監視し、レビューし、評価し、管理しなければならない。
【実施手順：テキストP34】

## 5.23 クラウドサービスの利用における情報セキュリティ

クラウドサービスの取得、利用、管理および終了のプロセスを、組織の情報セキュリティ要求事項に従って定めなければならない。
【実施手順：テキストP25】

## 5.24 情報セキュリティインシデント管理の計画及び準備

セキュリティインシデント管理のプロセス、役割および責任を定義、確立および伝達し、セキュリティインシデント管理の計画を定めなければならない。
【実施手順：テキストP26】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.25 情報セキュリティ事象の評価及び決定

情報セキュリティ事象に対して、セキュリティインシデントに分類するか否かを決定するための評価を実施しなければならない。
【実施手順：テキストP26～P27】

## 5.26 情報セキュリティインシデントへの対応

セキュリティインシデントに対し、文書化した手順に従って対応しなければならない。
【実施手順：テキストP27～P28】

## 5.27 情報セキュリティインシデントからの学習

セキュリティインシデントから得られた知識を、情報セキュリティ管理策を強化し、改善するために用いなければならない。
【実施手順：テキストP28】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.28 証拠の収集

情報セキュリティ事象に関連する証拠の特定、収集、取得および保存のための手順を定め、実施しなければならない。
【実施手順：テキストP28】

## 5.29 事業の中断・阻害時の情報セキュリティ

事業の中断・阻害時に情報セキュリティを適切なレベルに維持するための方法を定めなければならない。
【実施手順：テキストP28～P29】

## 5.30 事業継続のためのICTの備え

事業継続の目的およびICT 継続の要求事項に基づいて、ICT の備えを計画、実施、維持および試験しなければならない。
【実施手順：テキストP29～P30】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.31 法令・規制及び契約上の要求事項

情報セキュリティに関する法令や契約事項を特定・文書化し、遵守しなければならない。
【実施手順：テキストP31～P32】

## 5.32 知的財産権

知的財産権を保護するための適切な手順を実施しなければならない。
【実施手順：テキストP32】

## 5.33 記録の保護

記録を、消失、破壊、改ざん、認可されていないアクセスおよび不正な流出から保護しなければならない。
【実施手順：テキストP32～P33】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.34 プライバシー及びPIIの保護

適用される法令、規制および契約上の要求事項に従って、プライバシーの維持およびPII の保護に関する要求事項を特定し、満たさなければならない。
【実施手順：テキストP34】

## 5.35 情報セキュリティの独立したレビュー

情報セキュリティおよびその実施の管理に対する組織の取組について、あらかじめ定めた間隔で、または重大な変化が生じた場合に、独立したレビューを実施しなければならない。
【実施手順：テキストP34】

# 作成する候補となる実施手順書類について

【参照：テキスト15-1,15-2】
P8～P35

## 5.36 情報セキュリティのための方針群、規則及び標準の順守

組織の情報セキュリティ方針、トピック固有の個別方針、規則および標準を順守していることを定期的にレビューしなければならない。
【実施手順：テキストP34～P35】

## 5.37 操作手順書

情報処理設備の操作手順を文書化し、必要な要員に対して利用可能な状態としなければならない。
【実施手順：テキストP35】

# 第16章. 人的対策

作成する候補実施手順書類について

人的対策として重要となる実施項目

# 作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P37～P42

## 6.1 選考

従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。
【実施手順：テキストP39】

## 6.2 雇用条件

雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。
【実施手順：テキストP39】

## 6.3 情報セキュリティの意識向上、教育及び訓練

従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。
【実施手順：テキストP40～P41】

# 作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P37～P42

## 6.4 懲戒手続

情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。
【実施手順：テキストP39～P40】

## 6.5 雇用の終了又は変更後の責任

雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。
【実施手順：テキストP40】

## 6.6 秘密保持契約又は秘密義務契約

組織の要求事項を反映した秘密保持契約または守秘義務契約を従業員や外部の関係者と締結しなければならない。
【実施手順：テキストP40】

# 作成する候補となる実施手順書類について

【参照：テキスト16-1、16-2】
P37～P42

## 6.7 リモートワーク

要員が遠隔で作業する場合は、セキュリティ対策を実施しなければならない。
【実施手順：テキストP41】

## 6.8 情報セキュリティ事象の報告

情報セキュリティ事象を、適切な連絡経路を通して時機を失せずに報告できる仕組みを設けなければならない。
【実施手順：テキストP42】

# 第17章. 物理的対策

作成する候補実施手順書類について

物理的対策として重要となる実施項目

BYOD、MDM

# 作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P44～P52

## 7.1 物理的セキュリティ境界

情報およびその他の関連資産のある領域を保護するために、物理的セキュリティ境界を定め、かつ、用いなければならない。
【実施手順：テキストP47】

## 7.2 物理的入退

セキュリティを保つべき領域は、適切な入退管理策および立寄り場所によって保護しなければならない。
【実施手順：テキストP47】

## 7.3 オフィス、部屋及び施設のセキュリティ

オフィス、部屋および施設に対する物理的セキュリティを設計し、実装しなければならない。
【実施手順：テキストP48】

# 作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P44～P52

## 7.4 物理的セキュリティの監視

施設は、認可されていない物理的アクセスについて継続的に監視しなければならない。
【実施手順：テキストP48】

## 7.5 物理的及び環境的脅威からの保護

自然災害およびその他の意図的または意図的でない、インフラストラクチャーに対する物理的脅威などの物理的および環境的脅威に対する保護を設計し、実装しなければならない。
【実施手順：テキストP48】

## 7.6 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関するセキュリティ対策を設計し、実施しなければならない。
【実施手順：テキストP49】

# 作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P44～P52

## 7.7 クリアデスク・クリアスクリーン

書類および取外し可能な記憶媒体に対するクリアデスクの規則、並びに情報処理設備に対するクリアスクリーンの規則を定め、適切に実施しなければならない。
【実施手順：テキストP49】

## 7.8 装置の設置及び保護

装置は、セキュリティを保って設置し、保護しなければならない。
【実施手順：テキストP49～P50】

## 7.9 構外にある資産のセキュリティ

構外にある資産を保護しなければならない。
【実施手順：テキストP50】

# 作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P44～P52

## 7.10 記憶媒体

記憶媒体は、組織における分類体系および取扱いの要求事項に従って、取得、使用、移送および廃棄のライフサイクルを通して管理しなければならない。
【実施手順：テキストP50～P51】

## 7.11 サポートユーティリティ

情報処理施設・設備は、サポートユーティリティの不具合による、停電、その他の中断から保護しなければならない。
【実施手順：テキストP51】

## 7.12 ケーブル配線のセキュリティ

電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。
【実施手順：テキストP51～P52】

# 作成する候補となる実施手順書類について

【参照：テキスト17-1、17-2】
P44～P52

## 7.13 装置の保守

装置は、情報の可用性、完全性、機密性を維持することを確実にするために、正しく保守しなければならない。
【実施手順：テキストP52】

## 7.14 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した装置は、処分または再利用する前に、すべての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。
【実施手順：テキストP52】

# BYOD, MDM

【参照:テキスト17-3-1.】
P53～P54

## BYOD導入に向けて

主なメリット・デメリット

| メリット | デメリット |
| --- | --- |
| **コスト削減**<br>企業は、端末の調達や管理にコストがかからない。故障した際の修理費用や老朽化した端末の入替も基本的には個人負担となる。 | **シャドーIT**<br>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る。 |
| **使い慣れた端末の業務利用**<br>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上がる。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る。 | **セキュリティリスク**<br>個人の端末では、さまざまなWebサイトやアプリケーションを利用することがあるため、ウイルス感染や不正アクセスといった被害にあう可能性が高くなる。 |

# BYOD, MDM

【参照：テキスト17-3-2.】
P54～P55

## MDM導入のポイント

MDMを導入する際のポイント

| ポイント | 概要 |
|---|---|
| コスト・費用 | 導入費用だけでなく、維持費がかかることを考慮する。 |
| 対応しているOSの確認 | 組織で利用しているPC、貸与しているスマホなど、組織が管理するデバイスのOSを確認する。 |
| サポート体制 | 導入時や導入後の運用サポートの有無を確認する。 |
| 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る。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。 |

# 第18章. 技術理的対策

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

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.1 利用者エンドポイント機器

利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。
【実施手順：テキストP63】

## 8.2 特権的アクセス権

特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。
【実施手順：テキストP64】

## 8.3 情報へのアクセス制限

情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。
【実施手順：テキストP64】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.4 ソースコードへのアクセス

ソースコード、開発ツール、ソフトウェアライブラリへの読取りおよび書込みアクセスを、適切に管理しなければならない。
【実施手順：テキストP64】

## 8.5 セキュリティを保った認証

セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。
【実施手順：テキストP65】

## 8.6 容量・能力の管理

現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。
【実施手順：テキストP65】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.7 マルウェアに対する保護

マルウェアに対する保護を実施し、利用者の適切な認識によって支援しなければならない。

【実施手順：テキストP66】

## 8.8 技術的脆弱性の管理

利用中の情報システムの技術的脆弱性に関する情報を獲得しなければならない。また、そのような脆弱性に組織がさらされている状況を評価し、適切な手段をとらなければならない。

【実施手順：テキストP66】

## 8.9 構成管理

ハードウェア、ソフトウェア、サービスおよびネットワークのセキュリティ構成を含む構成を確立、文書化、実装、監視し、レビューしなければならない。

【実施手順：テキストP67】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.10 情報の削除

情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。
【実施手順：テキストP67】

## 8.11 データマスキング

データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。
【実施手順：テキストP67～P68】

## 8.12 データ漏えいの防止

データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。
【実施手順：テキストP68】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.13 情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。
【実施手順：テキストP68】

## 8.14 情報処理施設の冗長性

情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。
【実施手順：テキストP69】

## 8.15 ログ取得

活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。
【実施手順：テキストP69】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.16 監視活動

セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。
【実施手順：テキストP69】

## 8.17 クロックの同期

組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。
【実施手順：テキストP70】

## 8.18 特権的なユーティリティプログラムの使用

システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。
【実施手順：テキストP70】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.19 運用システムに関わるソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。
【実施手順：テキストP70～P71】

## 8.20 ネットワークのセキュリティ

システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。
【実施手順：テキストP75～P76】

## 8.21 ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。
【実施手順：テキストP76】

# 作成する候補となる実施手順書類について

【参照:テキスト18-1、18-2】
P57～P77

## 8.22 ネットワークの分離

情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離しなければならない。

【実施手順：テキストP76】

## 8.23 ウェブ・フィルタリング

悪意のあるコンテンツにさらされることを減らすために、外部Webサイトへのアクセスを管理しなければならない。

【実施手順：テキストP76】

## 8.24 暗号の使用

暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。

【実施手順：テキストP77】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.25 セキュリティに配慮した開発のライフサイクル

ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。
【実施手順：テキストP71】

## 8.26 アプリケーションのセキュリティの要求事項

アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。
【実施手順：テキストP71～P72】

## 8.27 セキュリティに配慮したシステムアーキテクチャ及びシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。
【実施手順：テキストP72】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.28 セキュリティに配慮したコーディング

セキュリティに配慮したコーディングの原則を、ソフトウェア開発に適用しなければならない。

【実施手順：テキストP72】

## 8.29 開発及び受入れにおけるセキュリティ試験

セキュリティテストのプロセスを開発のライフサイクルにおいて定め、実施しなければならない。

【実施手順：テキストP73】

## 8.30 外部委託による開発

組織は、外部委託したシステム開発に関する活動を指揮、監視し、
レビューしなければならない。

【実施手順：テキストP73】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.31 開発環境、試験環境及び運用環境の分離

開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。
【実施手順：テキストP73～P74】

## 8.32 変更管理

情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。
【実施手順：テキストP74】

## 8.33 試験情報

テスト用情報は、適切に選定、保護、管理しなければならない。
【実施手順：テキストP74～P75】

# 作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P57～P77

## 8.34 監査試験中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。
【実施手順：テキストP75】

# 実施手順を適用するセキュリティ概念

【参照:テキスト18-3-1.】
P78～P81

## Security by Design

| デジタル・ガバメント推進標準ガイドラインにおける工程名 | セキュリティ・バイ・デザインの工程名 | 概要 |
|---|---|---|
| サービス・業務企画 | セキュリティリスク分析 | • システムのセキュリティリスクを特定し、リスク分析を実施する<br>• リスク分析結果をもとにセキュリティ対応方針を決定する |
| 要件定義 | セキュリティ要件定義 | • 機能面、非機能面で必要となるセキュリティ要件を明確にする |
| 調達 | セキュア調達 | • セキュリティ仕様を満たす安全な製品やサービス、セキュリティ仕様を満たす能力を有した委託先を選定する |
| 設計・開発 | セキュリティ設計 | • セキュリティを考慮したシステム設計を行う |
| | セキュリティ実装 | • 設計に基づき、セキュリティ機能を実装する（セキュアコーディングやプラットフォームのセキュリティ設定の実施を含む） |
| | セキュリティテスト | • 実装されたセキュリティ対策が有効であることを確認する（脆弱性診断を含む） |
| サービス・業務の運営と改善 | セキュリティ運用準備 | • システム運用開始前に必要なセキュリティ運用体制と手順を整える |
| 運用および保守 | セキュリティ運用 | • システム運用中のセキュリティを維持・管理する |

### 導入のメリット

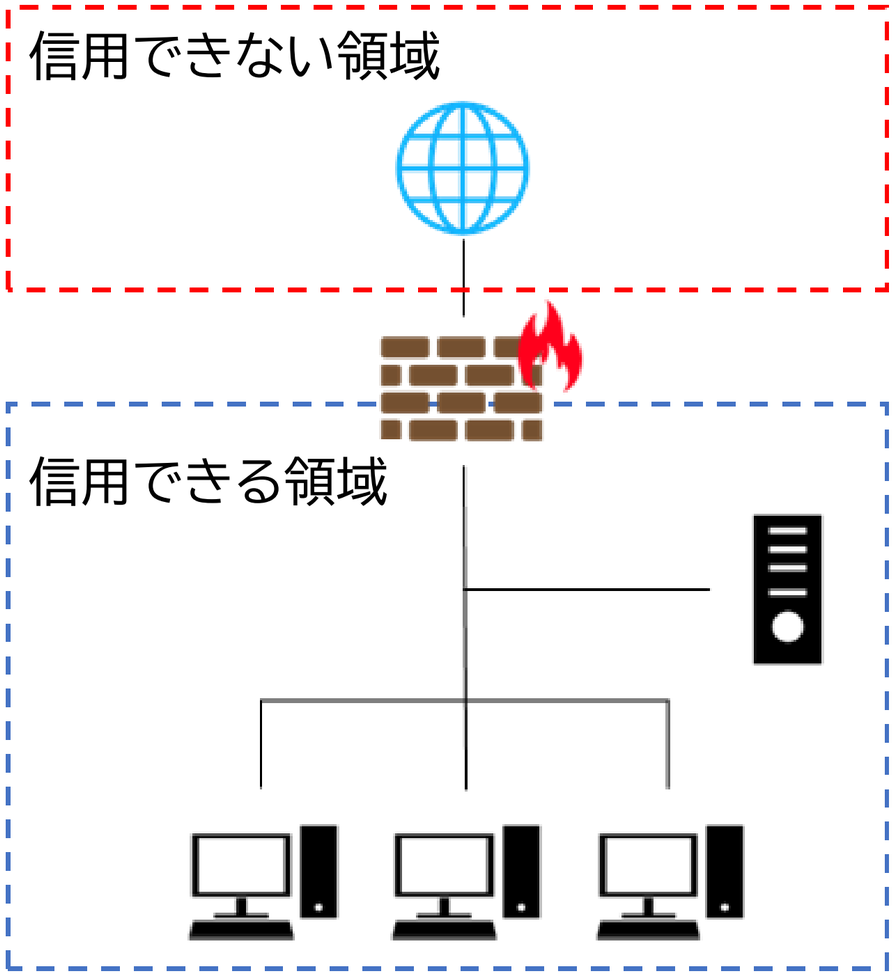
- 手戻りが少なくなり、納期を守れる
- コストを削減できる
- 保守性の高いソフトウェアができる（システムも同様）

# ゼロトラスト、境界防御モデル

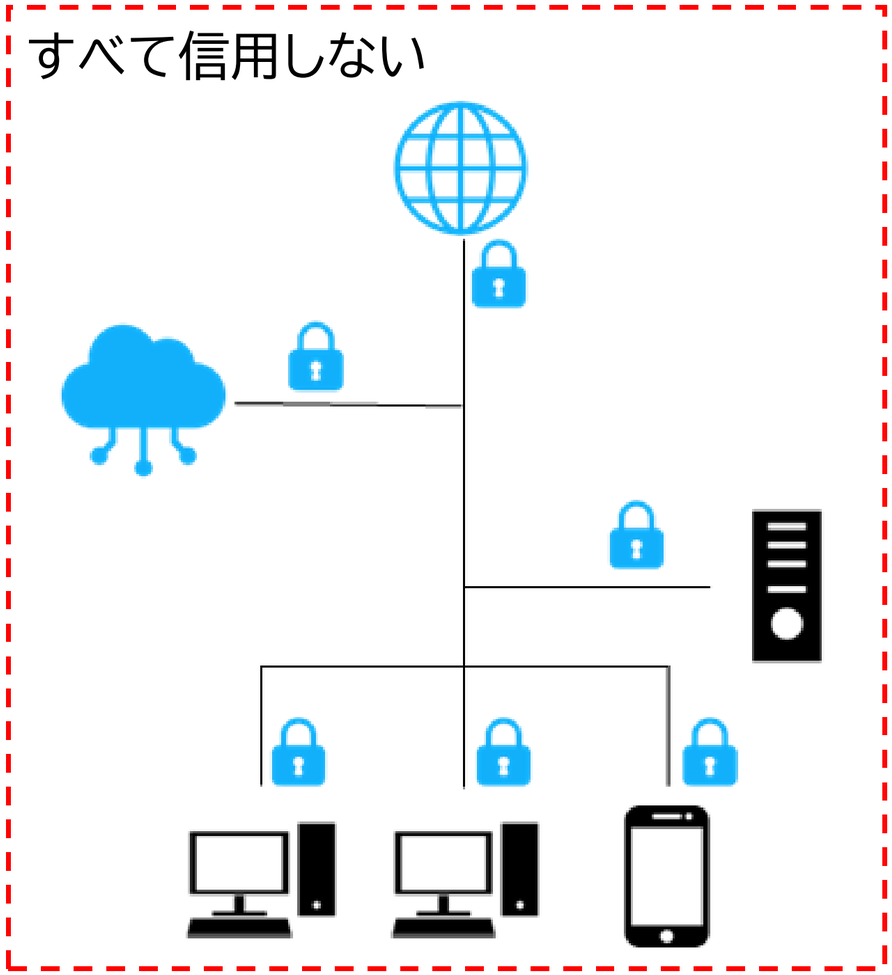
【参照：テキスト18-3-2.】
P82～P88

## 境界防御モデルとゼロトラストの違い

### 境界防御モデル




### ゼロトラスト



# ゼロトラスト導入に向けた進め方

【参照:テキスト18-3-2.】
P82～P88

① 企業のアクターを特定

② 企業が所有する資産を特定

③ キープロセスの特定とプロセス実行に伴うリスクの評価

④ ゼロトラスト導入候補の方針策定

⑤ ソリューション候補の特定

⑥ 初期導入とモニタリング

⑦ ゼロトラストの適用範囲拡大

# ゼロトラストを実装するための主な技術要素

【参照：テキスト18-3-2.】
P82～P88

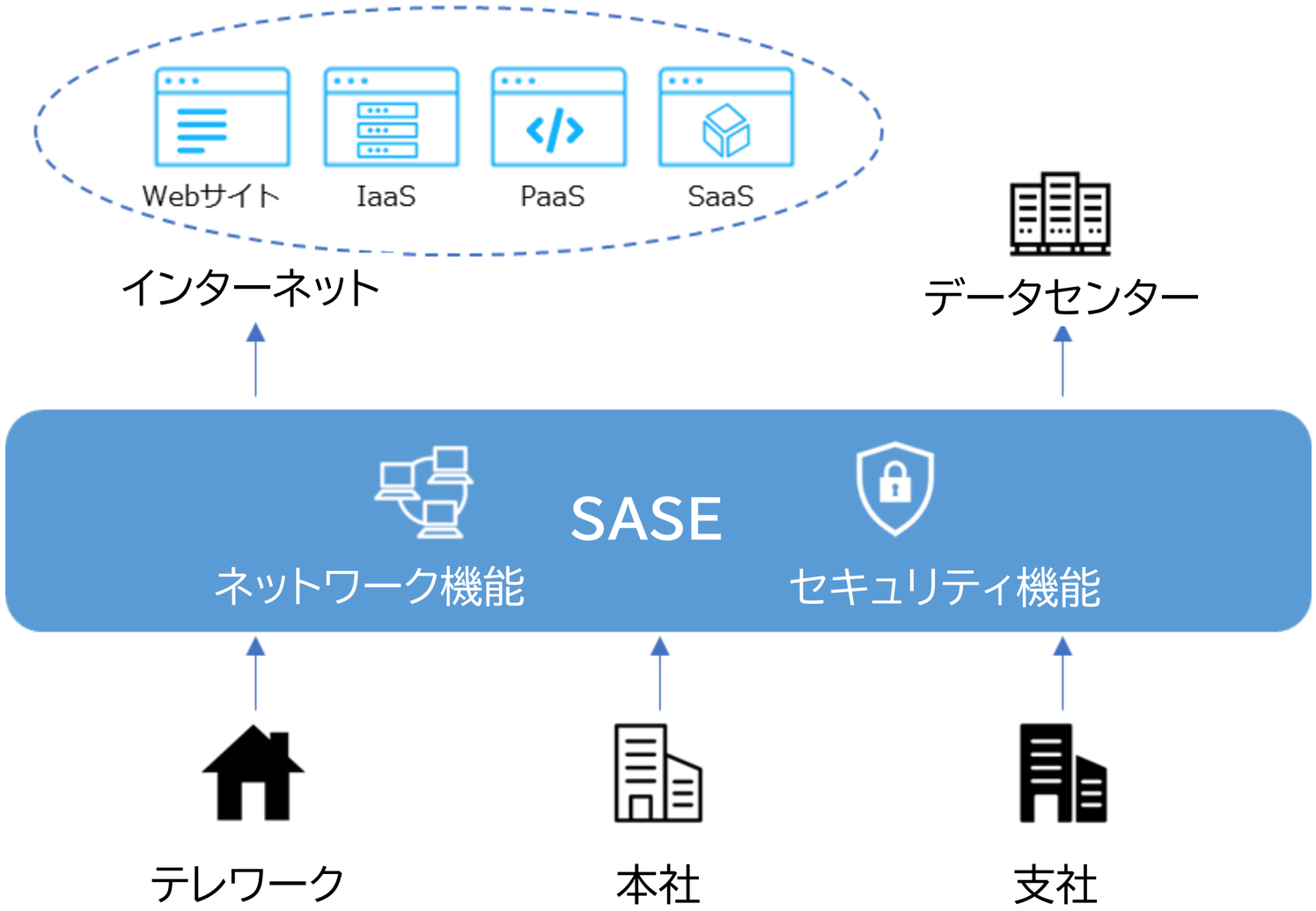
ゼロトラストを実装するために必要な技術要素

- CASB（Cloud Access Security Broker）
- SWG（Secure Web Gateway）
- ZTNA（Zero Trust Network Access）
- FWaaS（Firewall as a Service）
- SDP（Software Defined Perimeter）

# ゼロトラスト、境界防御モデル

【参照：テキスト18-3-3.】
P88～P90

## SASE

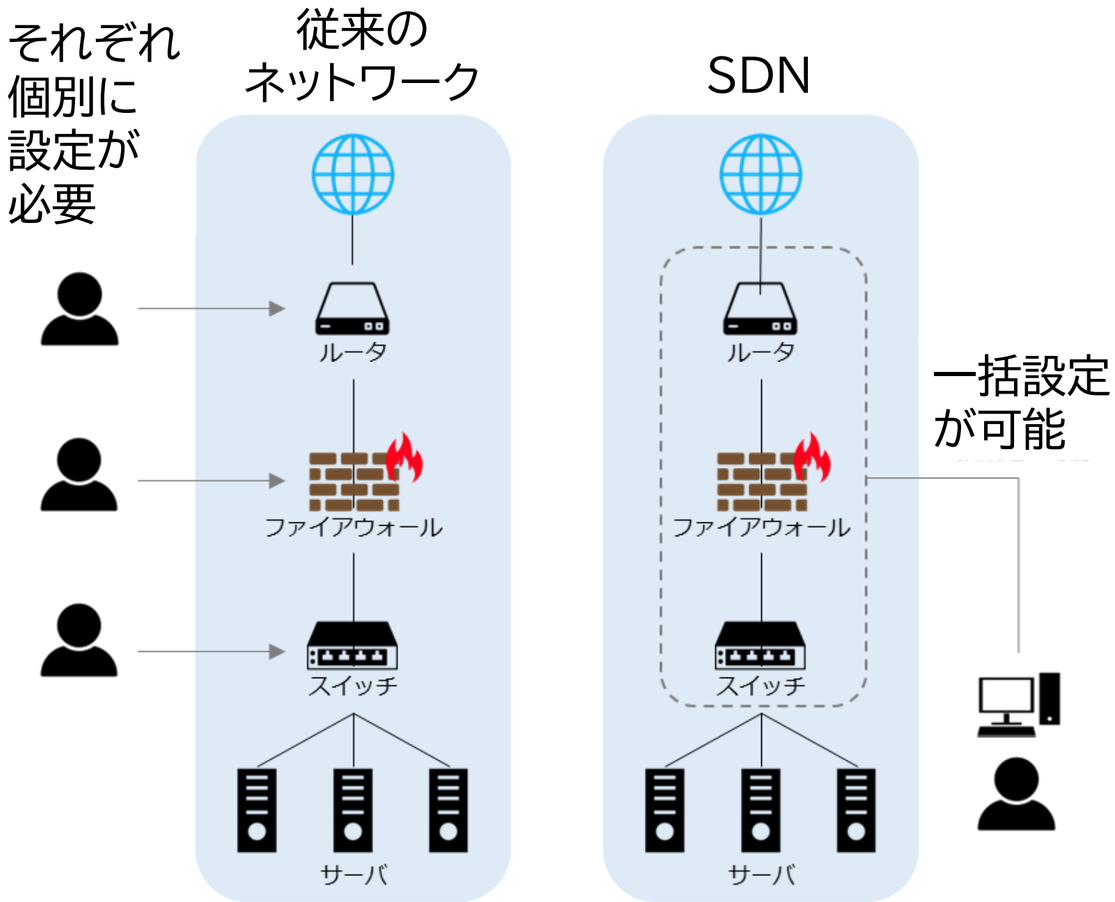


# ネットワーク制御

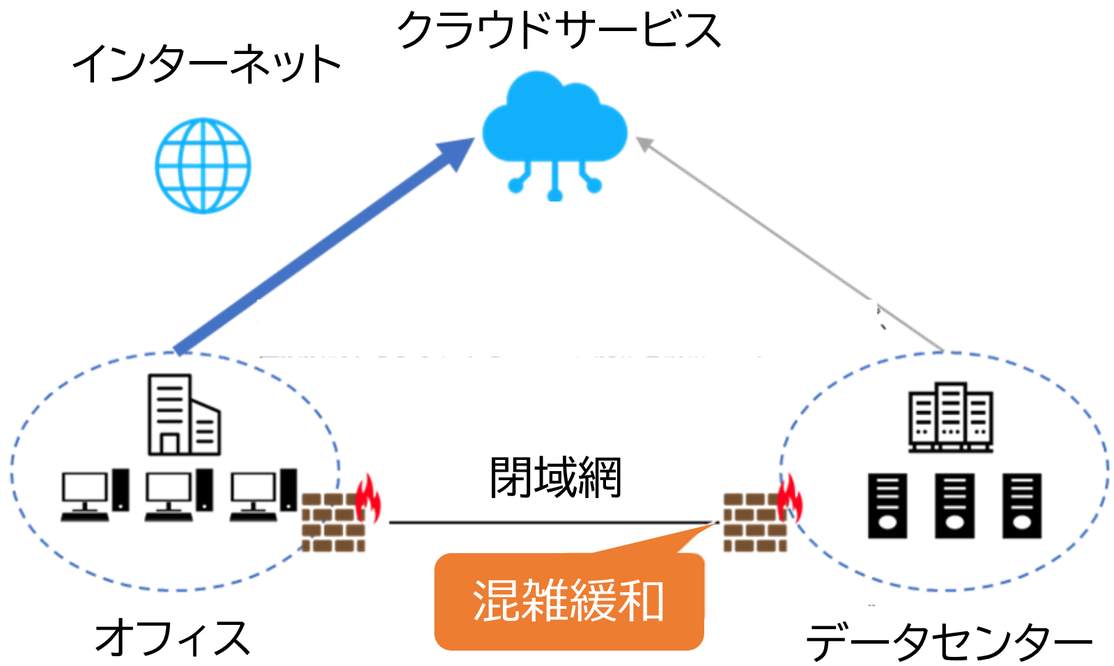
【参照:テキスト18-3-4.】
P91～P94

## SDN、SD-WAN

### SDN




### SD-WAN




信頼できるクラウドサービスへは、データセンターを経由せず、直接接続することで、混雑を緩和します

# セキュリティ統制（Security as a Service）

【参照：テキスト18-3-5.】
P94～P99

セキュリティ統制を確立するためのセキュリティ要素

- ネットワークセキュリティ
- デバイスセキュリティ
- アイデンティティセキュリティ
- ワークロードセキュリティ
- データセキュリティ
- 可視化と分析
- 自動化

# インシデント対応

【参照:テキスト18-4.】
P100～P103

## インシデント発生時の対応

1. 検知・初動対応
2. 報告・発表
3. 復旧・再発防止

## フォレンジックの実施手順例

1. 発生したインシデントの内容把握
2. 発生したインシデントに関する対象物の決定
3. 証拠保全を行う上で必要な情報の収集

# 第19章. セキュリティ対策の有効性評価

## 内部監査

## 外部監査

# 内部監査

【参照:テキスト19-1.】
P105

内部監査は、組織の情報セキュリティ管理が規定通りに運用され、効果的に機能しているかを内部的に確認・評価するプロセスのこと。
内部監査の進め方は「13-2-7. ISMS:9.パフォーマンス評価」を参照。

| パフォーマンス評価 | 作成文書（例） |
|---|---|
| 9.1 監視、測定、分析及び評価<br>（情報セキュリティのパフォーマンスとISMSの有効性の評価） | • ISMS有効性評価表 |
| 9.2 内部監査<br>（ISMSの適合性、有効性についての監査） | • 内部監査チェックリスト<br>• 内部監査計画書<br>• 内部監査結果報告書 |
| 9.3 マネジメントレビュー<br>（トップマネジメントが、ISMSの有効性を評価する） | • マネジメントレビュー報告書 |

# 外部監査

【参照：テキスト19-2.】
P106～P107

外部監査は、第三者機関が、組織の情報セキュリティ管理が国際基準や既定に適合し、適切に運用されているかを独立した視点で確認・評価するプロセスのこと。

## 管理基準・監査基準

- 情報セキュリティ管理基準
  - マネジメント基準
  - 管理策基準

- 情報セキュリティ監査基準
  - 一般基準
  - 実施基準
  - 報告基準

# 令和7年度
# 中小企業サイバーセキュリティ
# 実践力強化プログラム


東京都産業労働局