令和6年度
中小企業サイバーセキュリティ
社内体制整備事業

第5回

第7編：ISMSの構築と対策基準の策定と実施手順【レベル3】

セミナー内容

編	テーマ
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

編	テーマ
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7編	ISMSの構築と対策基準の策定と実施手順
第8編	具体的な構築・運用の実践
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10編	全体総括

セミナー内容

第16章. 人的対策

第17章. 物理的対策

第18章. 技術的対策

第19章. セキュリティ対策状況の有効性評価

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.】
P4

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P6】

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P6】

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P7】

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.】
P5

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P6】

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P7】

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P7】

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.】
P5

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P8】

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P9】

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.】
P11, P12

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P14】

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P14】

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P15】

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.】
P12

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P15】

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P15】

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17-1.】
P12

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P16】

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P16】

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P17】

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.】
P12, P13

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P17】

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P18】

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17-1.】
P12, P13

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P19】

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P19】

BYOD, MDM

BYOD導入に向けて

【参照：テキスト17-3.】
P21

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 企業は、端末の調達や管理にコストがかかりません。故障した際の修理費用や老朽化した端末の入替も基本的には個人負担となります。	**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。
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。	**セキュリティリスク** 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ります。

BYOD, MDM

MDM導入のポイント

【参照：テキスト17-3.】
P21

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.】
P26

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P31】

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P32】

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P32】

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.】
P26, P27

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P32】

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P33】

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18-1.】
P27

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P34】

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P34】

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P35】

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.】
P27

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P35】

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P35】

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P36】

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.】
P27, P28

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P36】

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P37】

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P37】

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.】
P28

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P37】

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P38】

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P38】

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.】
P28

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P39】

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P43】

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P44】

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.】
P28, P29

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P44】

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P45】

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P45】

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.】
P29

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P39】

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P40】

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18-1.】
P29

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P40】

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P41】

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18-1.】
P29, P30

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P42】

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P42】

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P43】

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.】
P30

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P43】

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.】
P47

Security by Design

デジタル・ガバメント推進標準ガイドラインおける工程名	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 ● 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

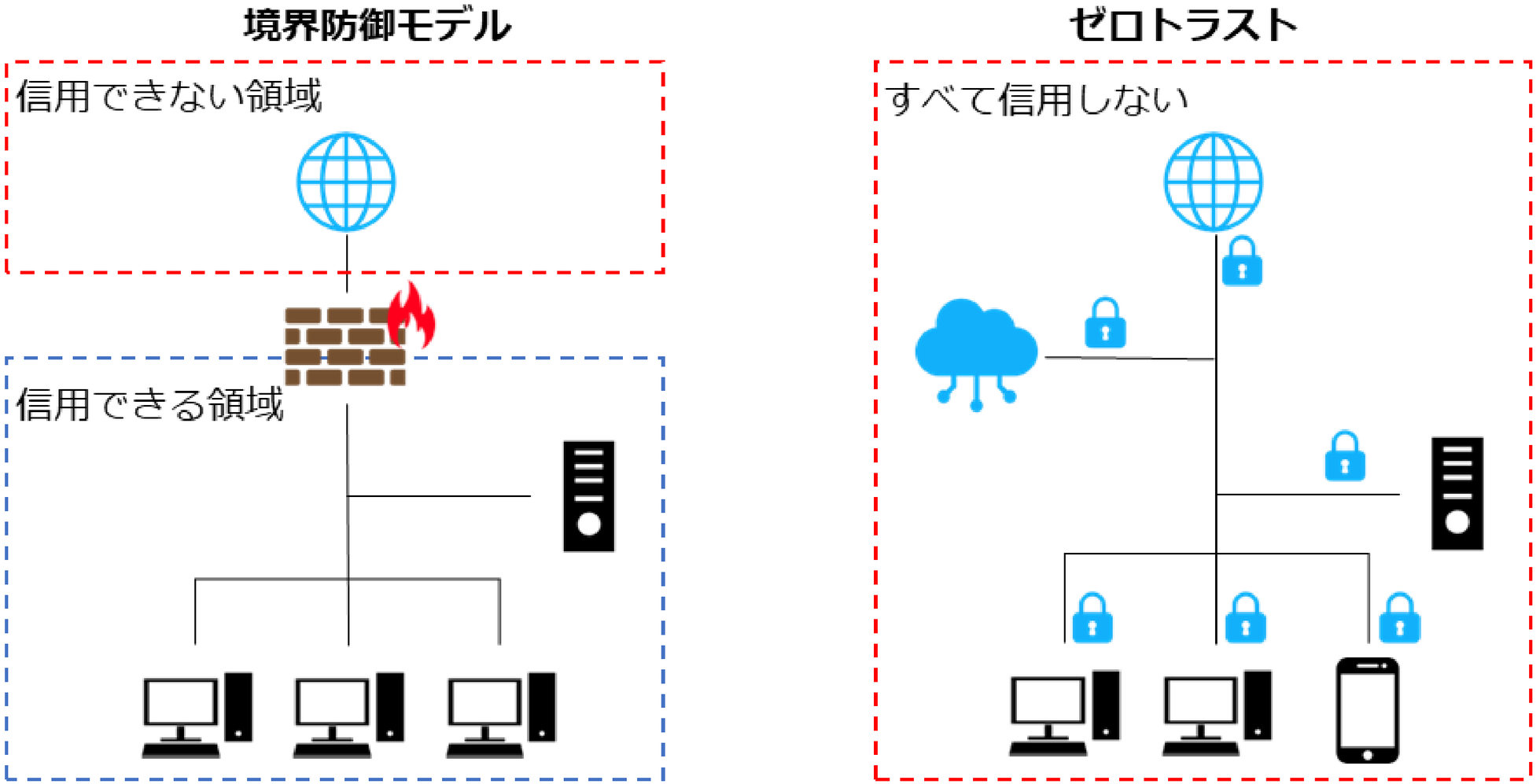
導入のメリット

- 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

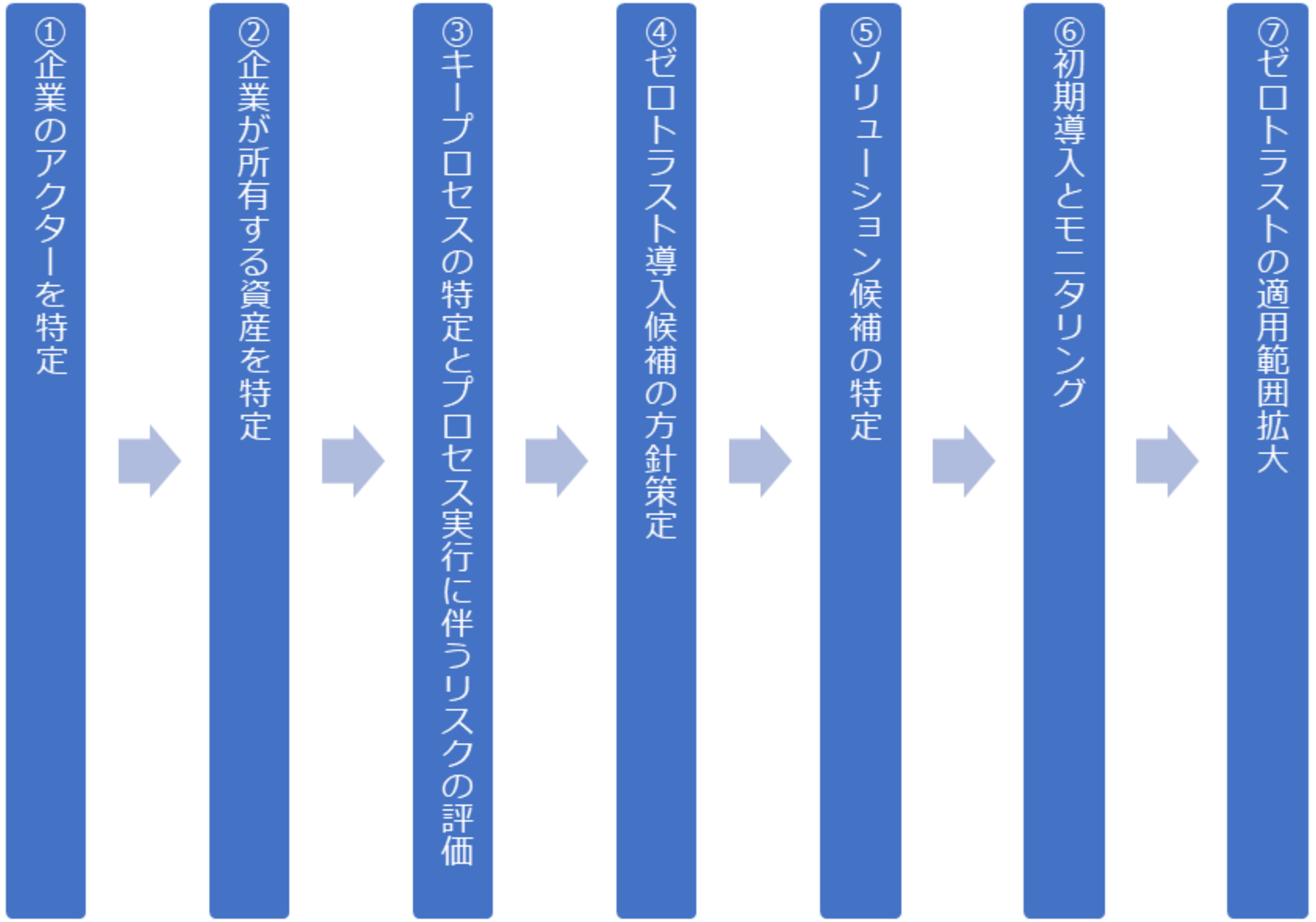
境界防御モデルとゼロトラストの違い

【参照：テキスト18-3-2.】
P51



ゼロトラスト導入に向けた進め方

【参照：テキスト18-3-2.】
P52



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.】
P56

ゼロトラストを実装するために必要な技術要素

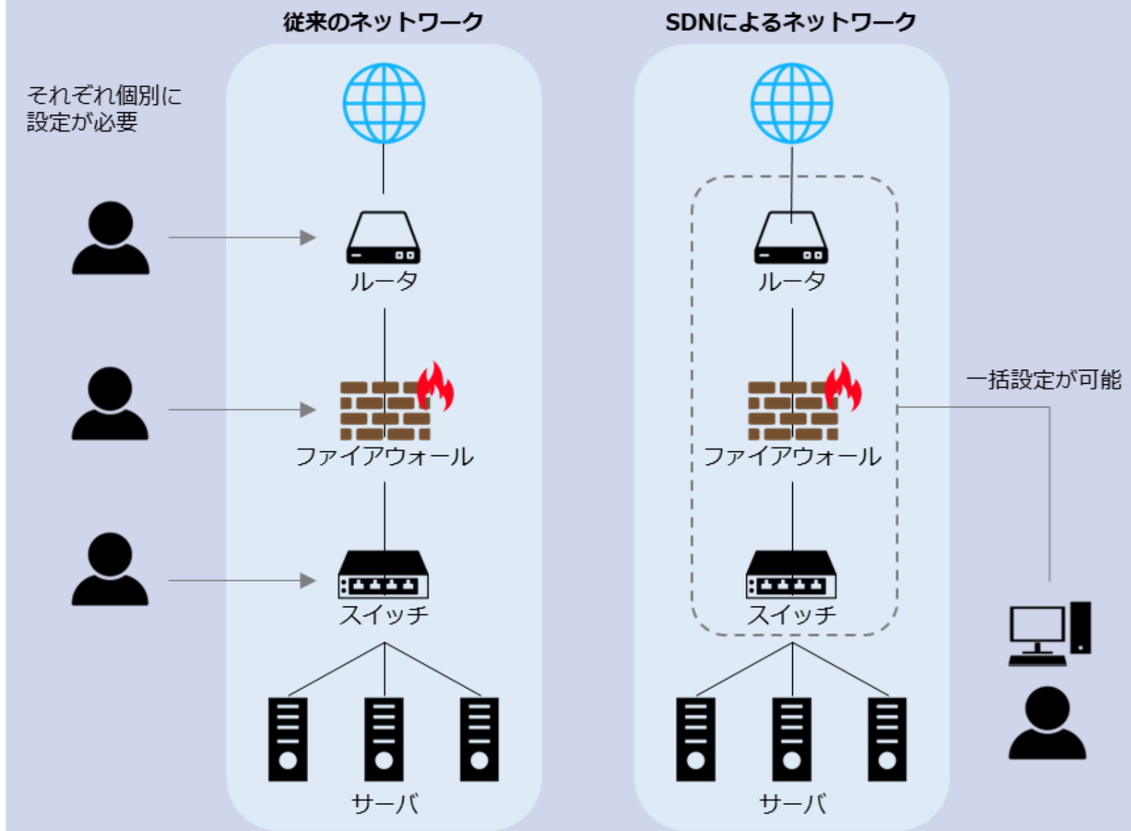
- CASB（Cloud Access Security Broker）
- SWG（Secure Web Gateway）
- ZTNA（Zero Trust Network Access）
- FWaaS（Firewall as a Service）
- SDP（Software Defined Perimeter）

ネットワーク制御

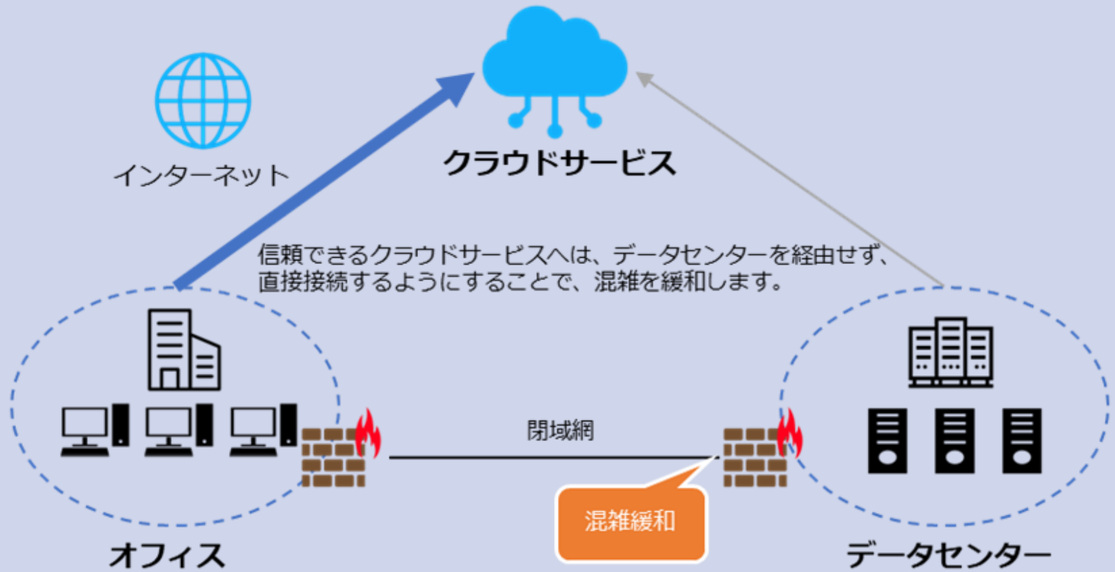
SDN、SD-WAN

【参照：テキスト18-3-4.】
P61, P62, P63

SDN



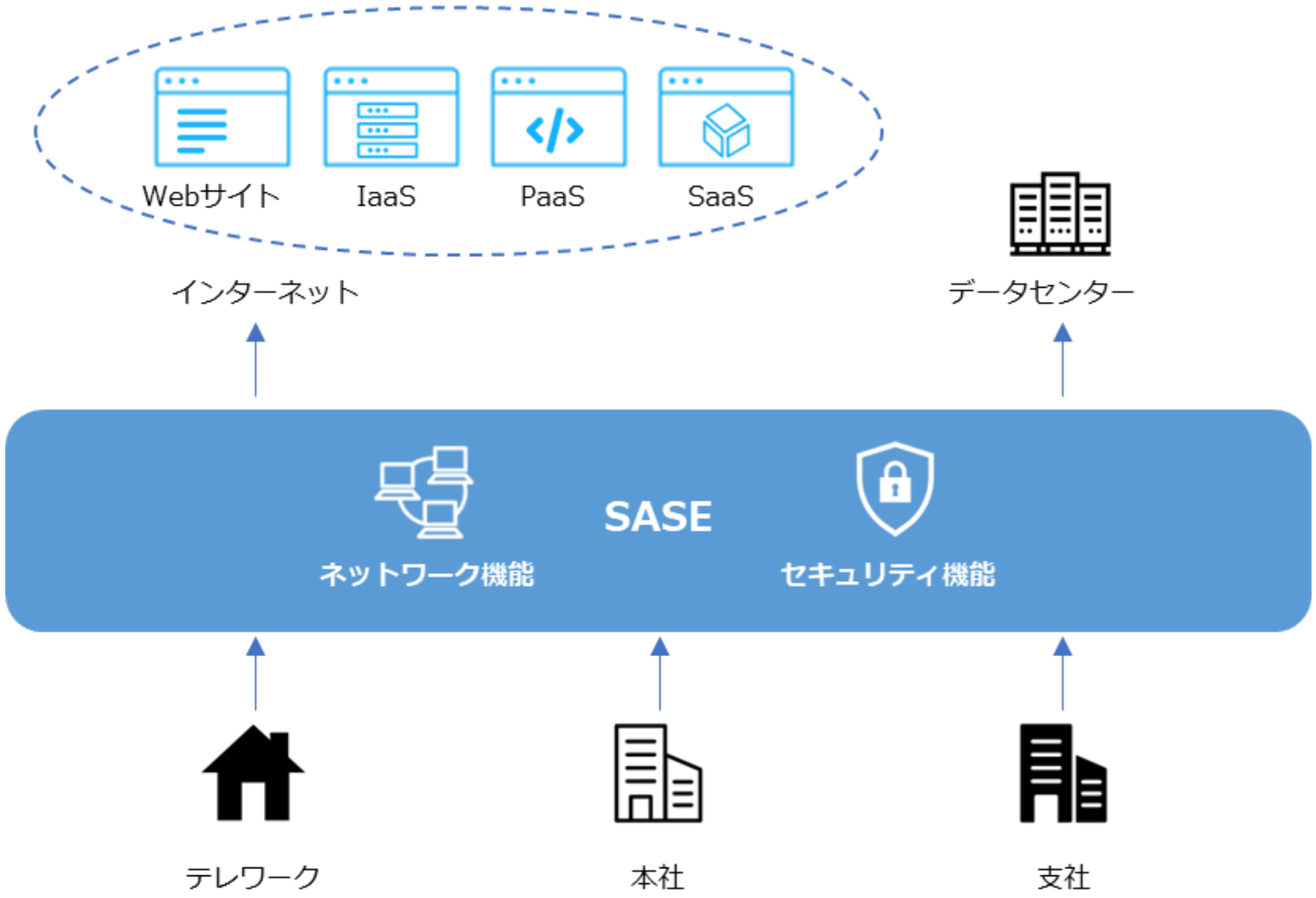
SD-WAN



ゼロトラスト、境界防御モデル

SASE

【参照：テキスト18-3-3.】
P58



セキュリティ統制（Security as a Service）

【参照：テキスト18-3-5.】
P66, P67

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.】
P70, P71, P72, P73

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.】
P75

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 （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 （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 • 内部監査計画書 • 内部監査結果報告書
9.3 マネジメントレビュー （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

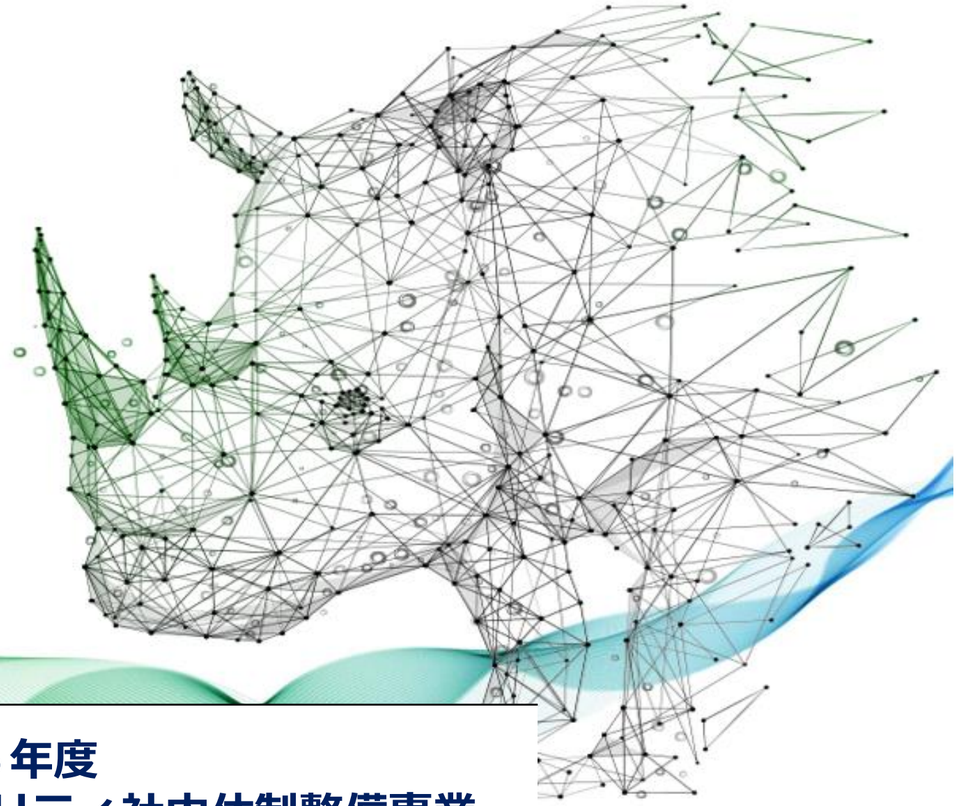
【参照：テキスト19-2.】
P76, P77

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６年度
中小企業サイバーセキュリティ社内体制整備事業