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

技術的対策と物理的対策およびセキュリティ対策状況の有効性評価
【実施手順・実施者マニュアルレベル③】

サイバーセキュリティ
人材育成
社内体制整備支援

セミナー内容

回数	テーマ
第1回	サイバーセキュリティを取り巻く環境および中小企業に 求められるサイバーセキュリティ対策
第2回	これからの企業経営で必要な攻めと守りのIT活用および サイバーセキュリティ対策
第3回	サイバーセキュリティに関する国の方針・施策および サイバー脅威の動向
第4回	サイバーセキュリティ対策におけるフレームワークの体系
第5回	組織として策定すべき対策基準及び情報セキュリティの 三大要素【対策基準レベル①】

セミナー内容

回数	テーマ
第6回	セキュリティリスク評価及び対策基準に記載されるべき管理策【対策基準レベル②】
第7回	組織として実施すべき具体的な対策事項・手順【実施手順・実施者マニュアルレベル①】
第8回	組織的対策と人的対策【実施手順・実施者マニュアルレベル②】
第9回	技術的対策と物理的対策およびセキュリティ対策状況の有効性評価【実施手順・実施者マニュアルレベル③】
第10回	全体総括

１．物理的管理策

物理的管理策を参考とした対策基準・実施手順の策定

各種テーマごとの対策

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-1.】
第16章 - 02

対策基準の策定

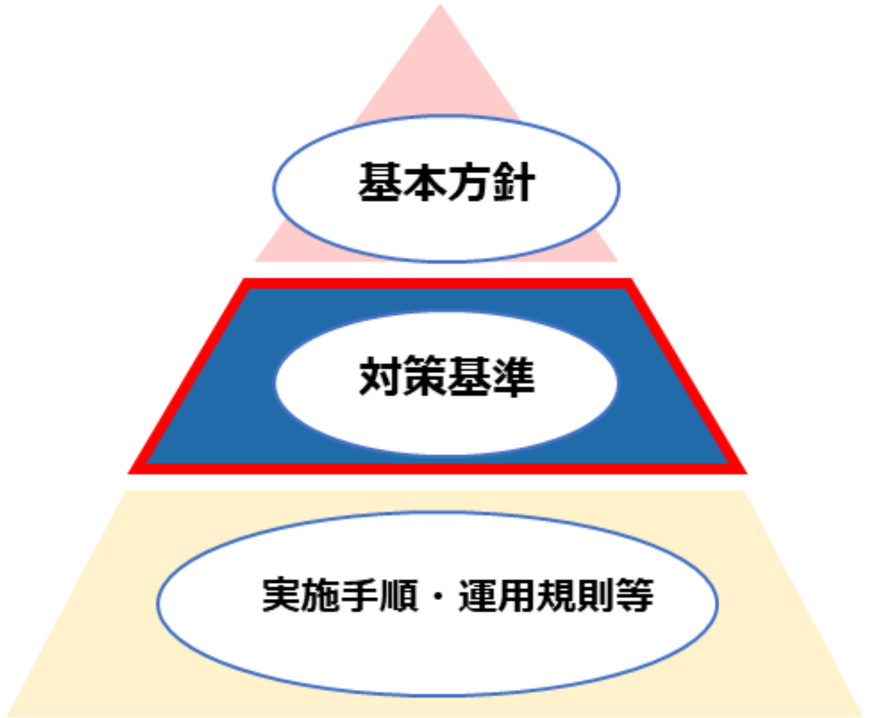
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

物理的管理策を参考とした対策基準・実施手順の策定

【復習】

対策基準の策定

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-1.】
第16章 - 03

対策基準（例）

対策基準（例）
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。 **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。 **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。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-1.】
第16章 - 03

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-1.】
第16章 - 04

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-1.】
第16章 - 04

対策基準（例）

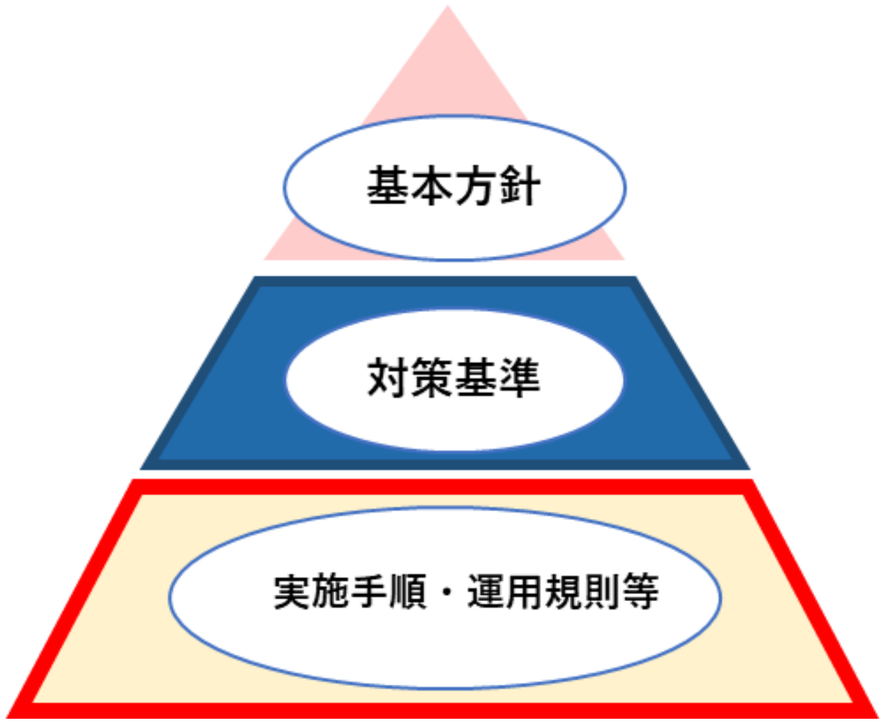
対策基準（例）
7.12 ケーブル配線のセキュリティ 電源ケーブル、データ伝送ケーブルまたは情報サービスを支援するケーブルの配線は、傍受、妨害または損傷から保護しなければならない。 **7.13 装置の保守** 装置は、情報の可用性、完全性、機密性を維持することを確実にするために、正しく保守しなければならない。 **7.14 装置のセキュリティを保った処分又は再利用** 記憶媒体を内蔵した装置は、処分または再利用する前に、すべての取扱いに慎重を要するデータおよびライセンス供与されたソフトウェアを消去していること、またはセキュリティを保てるよう上書きしていることを確実にするために、検証しなければならない。

物理的管理策を参考とした対策基準・実施手順の策定

【復習】

実施手順の策定

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 05

7.1 物理的セキュリティ境界

実施手順（例）
a. 当組織は、「レイアウト図」により、セキュリティ境界を定義する。 ※レイアウト図は、第13章 4.3 情報セキュリティマネジメントシステムの適用範囲の決定（3/3）の物理的境界 レイアウト図（例）を参照 b. 重要な情報資産のある領域の入退を制限し、入退資格を有さない者の立ち入りを制限する。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 05

7.2 物理的入退

実施手順（例）
a. 入退を行う対象者に対して、入退資格を設け、資格のない者の立ち入りを禁じる。入退資格は、従業者証またはセキュリティカードを交付することにより付与し、他人への貸借は禁じる。 b. 外来者の訪問は、原則として、「入退受付票」に氏名、身元、入退時刻を記録し、面談者が面会の確認印の押印または署名を行い、退出するまでエスコートする。 c. 宅配便などの荷物の受け取りは、各オフィスの入口より外で行うことを原則とし、例外的にオフィス内への入室を認める場合は、必ず応対者がエスコートする。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 06

7.3 オフィス、部屋及び施設のセキュリティ

実施手順（例）

a. 各事業場は常時施錠可能とし、入退資格のない者の立ち入りを禁じる。やむを得ず施錠可能でない事業場においては、重要な情報はキャビネットに収納し施錠するなど、厳重な管理を行う。
b. 施錠、開錠は、原則として従業者が行う。
c. 入退を許可された外来者に対しては、原則として従業者が随行し、立ち入り場所を制限する。
d. 秘密の情報または活動が外部から見えないよう、ブラインドやパーティションを設置する。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 06

7.4 物理的セキュリティの監視

実施手順（例）
a. 組織の施設は、監視カメラ、侵入者警報を設置し、認可されていないアクセスや、疑わしい行動を検知する。無人の領域には、必ず監視カメラおよび侵入者警報を設置する。 b. 監視カメラ、侵入者警報の動作確認をするため、3か月に1回点検を実施する。

7.5 物理的及び環境的脅威からの保護

実施手順（例）
a. 各フロアには、火災報知器、消火器を設置する。 b. サーバ付近に段ボールなどの燃えやすいものを置くことを禁じる。 c. サーバの転倒対策として設置位置を工夫する。必要に応じて、転倒防止器具を利用するなどの対策を行う。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 07

7.6 セキュリティを保つべき領域での作業

実施手順（例）
a. サーバ室には、スマートフォンやボイスレコーダー、カメラなど撮影や録音ができるものや、USBメモリなどサーバの情報をダウンロードできる機器の持ち込みは禁じる。 b. セキュリティを保つべき領域は常時施錠し、入退資格のない者の立ち入りを禁じる。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 07

7.7 クリアデスク・クリアスクリーン

実施手順（例）

a. クリアデスク
- 離席時や帰宅時には、重要情報や個人情報を含む書類や記憶媒体を机上やその周辺に放置しない。
- 書類やデータは、重要なものとそうでないものを区別して整理する。
- プリンタ、コピーに出力した印刷分は放置せず速やかに取り出す。

b. クリアスクリーン
- 利用者は、食事やトイレ、会議などで自席を離れる場合には、コンピュータのログアウト（ログオフ）やスクリーンロックを行い、第三者がコンピュータを操作したり、画面を盗み見たりできないようにする。
- ログインID、パスワードを机上に貼付することは禁じる。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 07

7.8 装置の設置及び保護

実施手順（例）

a. スイッチ、無線LANアクセスポイントなどは、人目につくところや通行量の多い場所を避けて設置する。
b. サーバは、サーバ室など隔離されたエリアに設置する。隔離されていないエリアに設置する場合は、ラックなどへ収容する。
c. サーバが設置されたエリアでの飲食、喫煙は禁じる。
d. サーバが設置されたエリアの温度、湿度を監視し、サーバに悪影響を与えない状態を維持する。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 08

7.9 構外にある資産のセキュリティ

実施手順（例）

a. 社外にノートPC等を持ち出す場合は、
①ログインパスワードを設定する。
②必要のない機密情報、個人情報を格納しない。
③格納するファイルは暗号化する（パスワードをつける）。
④OS・ソフトウェアが最新バージョンになっており、セキュリティソフトが入っていることを確認する。
⑤ノートPCなどが入ったカバンなどを交通機関の網棚などには置かず、常時携帯する。

b. 公共交通機関を利用する際に、顧客情報や個人情報など、重要な情報をノートPCや社用携帯で閲覧することは禁じる。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 08

7.10 記憶媒体

実施手順（例）
a. 外づけの記録媒体の持ち出し・持ち込みは、事前に許可を得た上で行う。また、不使用時は、キャビネットに施錠保管を行う。 b. 記憶媒体に収納する情報は必要最小限なものとし、必要のない機密情報や個人情報、会社の重要情報は保存しない。 c. 格納するファイルは暗号化して（パスワードをつけて）保存する。 d. 外部記憶媒体や、重要な情報が記された文書を机上や、棚上などに放置することは禁じる。 e. 私有の外部記憶媒体を持ち込む場合、社有の外部記憶媒体を持ち出す場合は、該当部門の責任者および情報システム管理者の許可を得る。 f. 外部記憶媒体でデータを受け渡す場合は、データの内容に応じてセキュリティを確保できるような受け渡し方法をとる。 g. お客様のUSBメモリなどの記憶媒体を預かった場合は、使用する前に必ずアンチウイルスソフトによりスキャンを行う。 h. 不要な媒体を処分する場合は、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。 i. 媒体を輸送する場合は、必要に応じて梱包などにより保護するとともに、「5.10 情報及びその他の関連資産の利用の許容範囲」のルールに従う。 j. サーバ、ネットワーク機器（スイッチ、ルータなど）の設置場所を、情報システム管理者の許可なく移動することは禁じる。 k. 当組織の資産および顧客から預かった資産を、情報セキュリティ委員長の許可なく無断で持ち出すことは禁じる。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 09

7.11 サポートユーティリティ

実施手順（例）

a. 情報システム管理者は、必要に応じて無停電電源装置を設置する。無停電電源装置は、ランプの確認などにより、バッテリーの寿命が尽きていないことや、緊急時の切り替えが問題なく行えるかを定期的に確認する。
b. 情報システム管理者は、フロア（装置の設置場所）が適切な温度に保たれていることを適時確認する。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 09

7.12 ケーブル配線のセキュリティ

実施手順（例）

a. 人が通る箇所のケーブル配線は、できるだけ床下か天井に配線する。床上に配線する場合には、モール、ケーブルカバーによる保護を行う。
b. 配線ケーブルに異常がないか、3か月に1回点検を行う。
c. 誤接続を防止するために、ケーブルにラベルをつける、役割ごとに色の異なるケーブルを使う。
d. ケーブル配線図を作成するとともに、機器の増設や移設で配線が変更になった場合には配線図を更新する。

物理的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト16-1-2.】
第16章 - 09

7.13 装置の保守

実施手順（例）
サーバ、ネットワーク機器など主要な装置は、製造元から提供されたマニュアルを参照し、製造元が推奨する頻度にて点検、保守を行い、記録する。

7.14 装置のセキュリティを保った処分又は再利用

実施手順（例）
a. PCを処分する場合は、従業員が各自で処理せず、情報システム管理者に処理を依頼する。情報システム管理者は、ハードディスクなどの記憶媒体については、物理的破壊もしくは、完全消去により処分する。 b. 上記以外の方法により、処分する必要があると認められる場合、事前に情報セキュリティ委員長の承認を得ることを要するものとする。 c. 情報システム管理者は、装置を再利用する場合、不要な情報を完全に消去し、またライセンス供与されたソフトウェアが消去されたことを確認の上、再利用する。

各種テーマごとの対策

【参照：テキスト16-2-1.】
第16章 - 10

BYOD（Bring Your Own Device）

関連する主な管理策
6.3、6.7、7.9、8.1、8.7

運用手順（例）

a. BYODに関する使用ルールや禁止事項を決めて周知する。
b. BYODで使用する機器については管理者に申請し、許可を得る。
c. BYODで使用する機器が紛失した場合の対応フローを策定し、周知する。
d. BYODで行える業務範囲やリモートアクセスの権限を設定する。
e. 社内ネットワークへは、VPNを利用する場合のみ接続できるようにする。
f. 必要以上に業務データを蓄積させない。（保存可能なデータに関するルールを決める。）
g. 業務で使用するPCは、EDRを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。
h. 業務で使用するPCに、ファイル共有ソフトなどの不正なソフトウェアをインストールすることは禁じる。

各種テーマごとの対策

【参照：テキスト16-2-2.】
第16章 - 11

MDM（Mobile Device Management）

関連する主な管理策
6.7、7.9、8.1

運用手順（例）

a. モバイル端末の紛失・盗難時の対応
   1. 従業員は、モバイル端末を紛失・盗難にあった場合は、速やかに情報セキュリティ管理者に報告する。
   2. 情報セキュリティ管理者は、従業員からモバイル端末の紛失・盗難の報告を受けた場合、速やかにリモートでモバイル端末の画面をロックし、位置情報を確認する。
   3. 情報セキュリティ管理者は、モバイル端末の位置情報が確認できず、発見が困難であると想定される場合、リモートワイプを実施し、モバイル端末内のデータを削除する。

b. 業務で新たにアプリケーションが必要になった場合、情報セキュリティ管理者に連絡し、インストールの許可をもらう。

2. 技術的管理策

技術的管理策を参考とした対策基準・実施手順の策定

各種テーマごとの対策

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 02

対策基準の策定

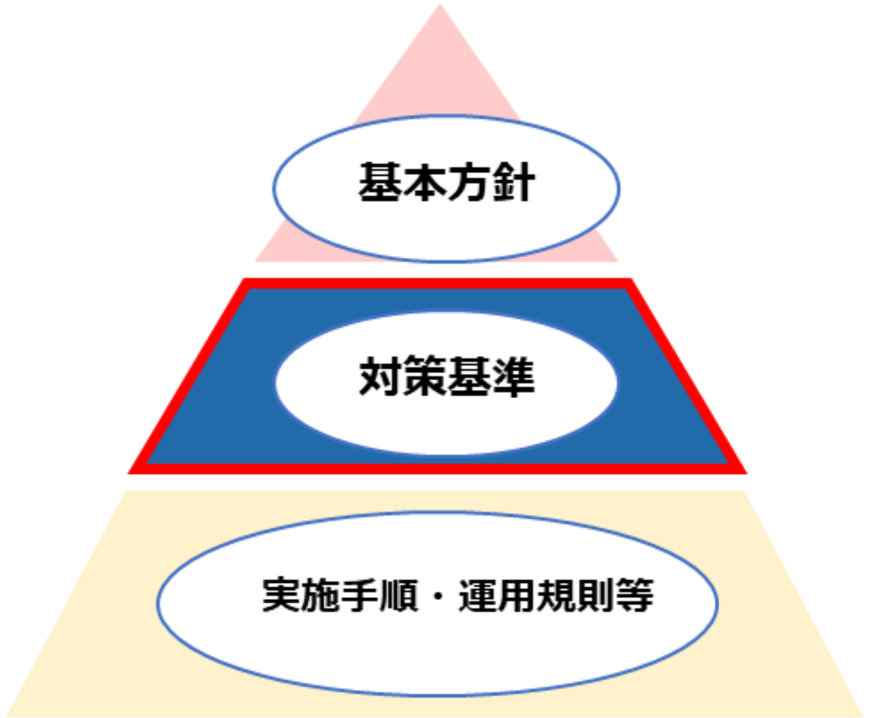
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理策。ネットワークのセキュリティ、データの暗号化、データのバックアップ、脆弱性管理、ログ管理、マルウェア対策などが含まれます。

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

【復習】

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 03

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 03

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 04

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 04

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 05

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 05

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 06

対策基準（例）

対策基準（例）
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。 **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。 **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。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 06

対策基準（例）

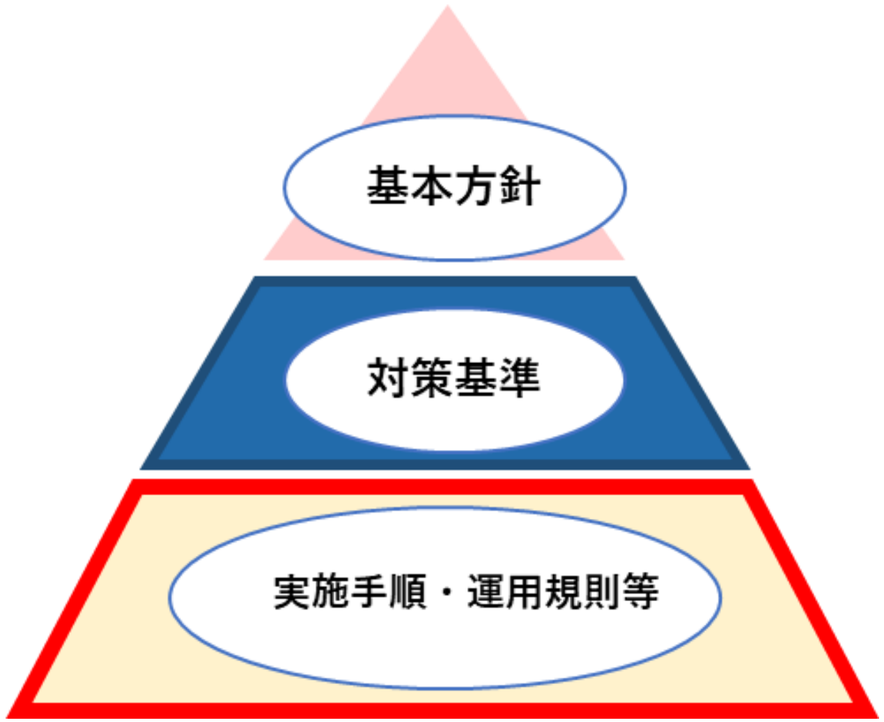
対策基準（例）
8.31 開発環境、試験環境及び運用環境の分離 開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。 **8.32 変更管理** 情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。 **8.33 試験情報** テスト用情報は、適切に選定、保護、管理しなければならない。 **8.34 監査試験中の情報システムの保護** 運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

技術的管理策を参考とした対策基準・実施手順の策定

実施手順の策定

【復習】

情報セキュリティポリシーの構成



セキュリティ対策の関係図
（出典）総務省.”情報セキュリティポリシーの内容”

基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 07

8.1 利用者エンドポイント機器

実施手順（例）

a. モバイル機器を社外に持ち出す場合、ログインパスワードを設定する。
b. 必要のない機密情報、個人情報などは、モバイル機器に格納しない。
業務上必要のある機密情報や個人情報をモバイル機器に格納する場合は、暗号化する。（パスワードをつける。）
c. モバイル機器を利用者が限定されない無償のWiFiスポットなどへ接続することは禁じる。
d. 携帯電話・スマートフォンの管理
・社有の携帯電話・スマートフォン（以下「社有携帯電話など」という）を使用する者は、紛失、破損しないよう丁寧かつ慎重に扱う。
・社有携帯電話などを使用する者は、使用者本人以外が操作できないよう、パスワードを設定して保護する。
・持ち歩く際は、ストラップをつけるなどの紛失・盗難防止策を必要に応じて講じる。
・電車やバスの中、その他公共の場所における使用は控え、個人情報やその他機密情報を他者に聞かれないよう十分配慮する。
・私有の携帯電話・スマートフォンを業務で使用する場合は、情報システム管理者の承認を要する。また、社有携帯電話などと同様の安全対策を実施する。
e. 利用者はノートPCに対して、パスワードつきのスクリーンセーバを設定し、のぞき見を防止する。スクリーンセーバの設定時間は10分以内とする。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 07

8.2 特権的アクセス権

実施手順（例）
a. 特権的アクセス権は特定の者に付与し、管理対象システムとその保有者を明確にする。 b. 半年に1回、または組織に何か変更があった際、特権的アクセス権を用いて作業する利用者をレビューし、特権的アクセス権を用いた作業に関して、その利用者が職務、役割、責任、力量の点で今も適格であるかどうかを検証する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 08

8.3 情報へのアクセス制限

実施手順（例）
a. 情報システム管理者は、取扱いに慎重を要する情報へのアクセス権限を、必要な者のみに割り当てる。 b. 未知の利用者識別情報または匿名の者による、取扱いに慎重を要する情報へのアクセスを許可しない。

8.4 ソースコードへのアクセス

実施手順（例）
ソースコードや設計書、仕様書などの関連書類は、アクセス権で管理されたフォルダに厳重に保管する。

8.5 セキュリティを保った認証

実施手順（例）
重要な情報システムにアクセスする際は、パスワードだけでなく、多要素認証を使用し、不正アクセスの可能性を減らす。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 09

8.6 容量・能力の管理

実施手順（例）

a. 情報システム管理者は、コンピュータやネットワークの応答時間など、その負荷状況について、業務を通じて問題がないかどうかを確認する。CPUやメモリ、ハードディスクなどの外部記憶装置の使用率など、リソースの使用状況を定期的に監視する。
b. リソースの使用状況に応じてリソースの割り当てを調整すると同時に、将来必要となる容量や能力を予測し、システムのパフォーマンスを維持するため、必要なリソースを事前に確保する。
c. 情報システム管理者は、問題が発見された場合、速やかに原因の究明を行い、情報セキュリティ委員会に報告する。
d. 情報セキュリティ委員会は、情報システム管理者に対策を指示し、必要に応じて経営陣に報告する。
e. 情報システム管理者は、中長期的な業務量の増減を考慮し、将来的にシステムに必要な容量を予測し、必要であればトップマネジメントに報告する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 09

8.7 マルウェアに対する保護

実施手順（例）

a. ネットワークに接続するすべてのパソコン、サーバ上に情報システム管理者が指定したアンチウイルスソフトを導入する。
b. アンチウイルスソフトを常時設定にし、ファイルへのアクセスおよび電子メールの受信時に常時スキャンできる設定を行う。
c. 常時スキャンだけでなく情報システム管理者が指定した期間に一度、ファイル全体に対するスキャンを行う。
d. 自動でウイルス定義ファイルの更新が行われるように設定する。
e. 標的型メール対応
   ・メールの添付書類やメール中のリンクは、原則として（送信者に確認するなどの方法で）安全が確認できるまで開かない。
   ・ファイルの拡張子を表示させる設定とし、添付ファイルの拡張子が、通常使用しない内容の場合、ファイルの参照を禁じる。
   通常使用しないファイルの拡張子の例：.exe、.pif、.scr

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 10

8.8 技術的脆弱性の管理

実施手順（例）
a. 情報セキュリティ委員会および情報システム管理者は、技術的な脆弱性のニュースを常に意識し、時期を失せず効果的に外部の攻撃を防御する。 b. OSやアプリケーションには常に最新のセキュリティパッチを適用する。ただし、検証の結果、業務上支障があると認められる場合には、他の方法で脆弱性に対処する。

8.9 構成管理

実施手順（例）
システムの構成要素とその相互関係を理解し管理するため、台帳や構成管理ツールを用いて、ハードウェア、ソフトウェア、ネットワーク機器、設定ファイルなど、システムを構成するすべての要素の情報を把握する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 10

8.10 情報の削除

実施手順（例）
a. 業務上必要がなくなったデータは速やかに削除する。 b. 記憶媒体上のデータを削除する際は、データ消去ソフトを使用し、復元できないよう、完全に削除する。 c. ハードディスクを廃棄する際は、磁気データ消去装置を用いてハードディスクのデータを削除してから廃棄する。

8.11 データマスキング

実施手順（例）
保有している情報をマーケティング分析などの目的で二次利用する場合には、個人情報や重要情報が推測できない形に加工した上で利用する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 11

8.12 データ漏えいの防止

実施手順（例）
a. 漏えいから保護する情報を特定し、分類する。 b. ファイル共有ソフトの使用を禁じる。 c. 重要な情報が画面に表示されている場合は、スクリーンショットや写真を撮ることを禁じる。 d. ファイアウォールやIDS、IPSなどによって不正アクセスを防止する。「8.20 ネットワークのセキュリティ」に従う。 e. 重要データについてアクセス制限を設ける。「8.3 情報へのアクセス制限」に従う。 f. 重要データは暗号化して保管する。「8.24 暗号の使用」に従う。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 11

8.13 情報のバックアップ

実施手順（例）
a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてシステムおよびデータのバックアップを行う。 b. バックアップ情報は、主事業所の災害による被害から免れるために、十分離れた安全でセキュリティを保った場所に保管する。 c. 情報システム管理者は、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。

8.14 情報処理施設の冗長性

実施手順（例）
a. 情報システムは、可用性に関する業務上の要求事項を明確にし、必要に応じて予備の機器を用意して二重化を行い、冗長性をもたせる。 b. 緊急の場合、速やかに予備の機器に切り替えられるよう、動作確認を月に1回行う。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 12

8.15 ログ取得

実施手順（例）

a. 情報システム管理者は、サーバ内に保存された重要データを障害による破壊や、不正アクセス、改ざんなどから守るために、必要に応じてログの取得を行う。
b. 情報システム管理者は、必要に応じてログの定期的なチェックを行う。
c. ログは、情報システム管理者またはその指名する担当がアクセスできるようにする。
d. 情報システム管理者は、運用担当者がサーバで行った作業を確認する。確認は、作業ログ、または日報・サーバ作業記録の閲覧により行う。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 12

8.16 監視活動

実施手順（例）
a. ファイアウォール・IDS・IPSのログを常に監視し、異常な動作を検知した場合は速やかに対応する。

8.17 クロックの同期

実施手順（例）
a. 情報システム管理者は、クライアントPCやサーバなどすべての情報システムのクロックを同期させる。 b. すべての情報システムのクロックを同期させるために、NTPを使用する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 13

8.18 特権的なユーティリティプログラムの使用

実施手順（例）
a. ユーティリティプログラムの使用は、原則としてOS標準機能のみ許可する。 b. その他のユーティリティプログラムが必要となった場合は、情報システム管理者の承認を得た上で利用する。

8.19 運用システムに関わるソフトウェアの導入

実施手順（例）
a. 運用システムに、開発用のコードを導入しない。 b. PCを含む社内の情報システムで使用するソフトウェアは、原則情報システム管理者によって指定されたもののみ使用し、それ以外のソフトウェアを使用する場合は、事前に許可を得るものとする。他社が開発したソフトウェアを利用する場合、その開発会社が要求している条件やスペックを満たす環境で運用する。 c. 情報システム管理者は、利用者がインストール可能なソフトウェアを定期的に見直す。 d. 利用者は認可されていないソフトウェアをインストールしてはならず、業務上、必要な場合は、情報システム管理者の承認を得た上でインストールする。 e. ファイル共有ソフトなど、ウイルス感染や不正アクセスなどの原因となりやすいソフトウェアのインストールを禁じる。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 14

8.20 ネットワークのセキュリティ

実施手順（例）

a. ネットワーク図および装置（例：ルータ、スイッチ）の構成ファイルを含む文書を最新に維持する。
b. 社内ネットワークへ接続する際は、情報システム管理者の承認を受け、指示された手順に従う。
c. 情報システム管理者は、ネットワークにおける社外との境界にはファイアウォールを設けるなど、不正侵入対策を施す。
d. ネットワーク装置のファームウェアの定期的なアップデートを行う。
e. 他人のID、パスワードで、社内ネットワークに接続することを禁じる。
f. 一旦、社内ネットワークから切り離したパソコンなどは、ウイルスチェックなどの安全確認を行ってから再接続する。
g. 持ち込みおよび私有PC利用の場合は、社内ネットワークに接続しない。やむを得ず接続する場合は、情報システム管理者が指定するソフトウェアによりウイルスチェックを行う。
h. 無線LANを使用する場合は、情報システム管理者の承認を得て、暗号化、接続パソコンの認証など、十分な安全対策を実施する。
i. 不特定が利用できる公衆無線LANやWiFiスポットに接続することは禁じる。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 14, 15

8.21 ネットワークサービスのセキュリティ

実施手順（例）
a. 利用しているネットワークサービスを特定する。 b. 情報システム管理者は、ネットワークサービスを利用する場合は、ネットワークサービス提供者とSLAを締結する。

8.22 ネットワークの分離

実施手順（例）
a. インターネットと社内LANとの境界にファイアウォールを設置する。 b. メール、Webサーバなどの公開サーバは、社内のネットワークと分離する。 c. ゲスト用の無線アクセスネットワークを、社内用の無線アクセスネットワークから分離する。

8.23 ウェブ・フィルタリング

実施手順（例）
フィルタリングソフトを利用し、業務上不必要なWebサイト、危険性のあるWebサイトへのアクセスを防ぐ。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 15

8.24 暗号の使用

実施手順（例）

a. 暗号利用のための規則
- SSL/TLS
  当組織のWebサイトの通信は、SSL/TLSを用いて暗号化する。
- 無線LAN
  無線LANの通信は暗号化し、暗号化の規格は脆弱性の報告されていない安全な方法とする。

b. 鍵の管理
- SSL/TLS
  情報システム管理者は、証明書に対する秘密鍵を適切に管理する。
- 無線LAN
  アクセスポイントの管理者画面は、情報システム管理者のみがアクセスでき、そのパスワードを厳重に管理する。

c. 重要データの暗号化
- 暗号化の対象とするデータを選定する。
- 利用する暗号の種類を決める。
- 暗号鍵のライフサイクルに関する方針を策定する。
- 暗号の管理責任者を定める。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 16

8.25 セキュリティに配慮した開発のライフサイクル

実施手順（例）

セキュリティに配慮した開発のための方針を以下に記す。

a. 開発の初期段階でセキュリティ要件を明確化する。
b. 開発環境は、「8.31 開発環境、試験環境及び運用環境の分離」の「b. セキュリティに配慮した開発環境」に従う。
c. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。
d. 開発したシステムに脆弱性がないかテストする。
e. 開発ドキュメント（仕様書、設計書、テスト仕様など）は、必要最低限の者だけがアクセスできるようにする。
f. 受託開発または客先への派遣による開発では、クライアントから提示のあったセキュリティの方針・ルールなどに従う。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 16

8.26 アプリケーションのセキュリティの要求事項

実施手順（例）
a. アプリケーションを取得する際、リスクアセスメントを通じてアプリケーションの情報セキュリティ要求事項を決定する。必要に応じて、情報セキュリティの専門家の支援を受け、情報セキュリティ要求事項を決定する。 b. 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は、以下の通りとする。 ・情報セキュリティ事象を防止・検知し、対応するために必要な管理策を分析すること。 ・情報セキュリティ要求事項を満たすための費用・時間・複雑さを考慮すること。

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

実施手順（例）
a. 社内使用の情報システムおよび外部向けに提供する情報システムの開発に際しては、情報セキュリティ事項を明確にし、要件定義として記録する。 b. 開発の各段階でセキュリティレビューを行い、セキュリティ要件が満たされているかを確認する。 c. 開発したシステムに脆弱性がないかテストする。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 17

8.28 セキュリティに配慮したコーディング

実施手順（例）
a. ユーザが入力したデータを確認し、問題がある場合は読み込まないようにする。 b. セキュリティ上の問題を発見しやすくするため、設計は可能な限りシンプルにする。 c. ユーザには必要最小限の権限・機能を与える。 d. 他のシステムに送信するデータは、サニタイズ（特殊文字を一般的な文字に変換すること）を行い、不正操作を防止する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 17

8.29 開発及び受入れにおけるセキュリティ試験

実施手順（例）

a. 情報システムのセキュリティテストは、運用に移行する前に行う。
b. システムの受入れ試験
- 情報システムの導入または改修の際は、受入れ時に動作確認を行う。
- 必要に応じて受入れテストの仕様書を作成し、確認を行う。
- 必要に応じて、コード分析ツールや脆弱性スキャナのような自動化ツールを利用し、セキュリティに関連する欠陥を修正する。
- 受入れ試験の結果は、受入れ部門の管理者および情報システム管理者が承認する。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 17, 18

8.30 外部委託による開発

実施手順（例）

情報システムの開発を外部に委託する場合の手順は以下に従う。

a. 「委託先審査票」によって委託先を評価、選定、およびあらかじめ定められた頻度（最低年1回）で再審査し、また、契約の履行状況を監視する。
b. 委託先との契約を締結する。（契約書には情報セキュリティ要求事項を含める。）
c. 成果物の品質および正確さを評価するため、「8.29 開発及び受入れにおけるセキュリティ試験」に定める「b. システムの受入れ試験」を実施する。

8.31 開発環境、試験環境及び運用環境の分離

実施手順（例）

a. 情報システムの開発に際しては、開発・テスト環境と本番環境を、物理的・論理的に分割する。
b. セキュリティに配慮した開発環境
・開発は、開発業務を行わない従業員から分離した場所およびシステムにて行う。また開発環境は、運用環境から分離する。
・ソースコードおよび設定ファイルは、不意の消去や改ざんから保護するため、必要最小限の者だけがアクセスできるようにする。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 18

8.32 変更管理

実施手順（例）

a. 変更管理は以下のプロセスで行う。
   1. 変更の承認
      変更を行う前にその変更の必要性、変更が及ぼす影響、変更によるリスクの変動について評価し、情報システム管理者の承認を得る。
   2. 変更のテスト
      変更を適用する前に、情報システムへの影響を確認するためにテストを行う。
   3. 変更の監査
      変更後に変更が適切に行われたかどうかを監査によって確認する。

b. 情報システム管理者は、サーバに周辺機器を接続する場合や、サービスパックを適用する場合、事前に情報収集し、問題の有無を確認する。万が一、適用後に問題が生じた場合は、再インストールすることで問題解決を即座に実施する。

c. OSやパッケージソフトを変更する際は、情報システム管理者はテスト機や予備機を用いて、現在の情報システムが変更後のOS上で問題なく動作するかを検証する。

d. パッケージソフトウェアのカスタマイズを原則として禁じる。万が一、修正を行う場合は、動作上の影響およびベンダーから将来的に受けるサポートへの影響を考慮し、情報システム管理者の許可を得る。

技術的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト17-1-1.】
第17章 – 19

8.33 試験情報

実施手順（例）
a. テストデータとして個人情報を使用することを禁じる。 b. 実データをテストデータとして使用する場合は、情報システム管理者の承認を得てから使用する。テスト終了後は、実データを直ちに削除し、情報システム管理者に対して報告する。

8.34 監査試験中の情報システムの保護

実施手順（例）
a. 情報システムの監査は、システム停止のリスクを考慮し、営業時間外もしくは休日を利用して実施することを原則とする。 b. 情報システムのメンテナンスなどにより情報システムの稼動を停止する場合は、業務への影響を及ぼさない範囲または時間帯で行うように計画する。

各種テーマごとの対策

【参照：テキスト17-2-1.】
第17章 - 20

Security by Design

関連する主な管理策

5.1、5.7、5.9、5.19、5.20、5.24、5.26~5.29、5.37、8.9、8.15、8.16、8.22、8.25~8.34

各種テーマごとの対策

【参照：テキスト17-2-1.】
第17章 - 21

Security by Design 実施手順例1

実施手順（例）	選択すべき管理策（例）
セキュリティリスク分析 • システムで取扱う重要情報、アクター、実施業務、他システムとの連携方法など、システムで取扱う重要情報のフローやライフサイクルが分かる内容を記載したシステムプロファイルの作成 • システムプロファイルに基づくセキュリティ脅威の特定 • セキュリティ脅威の発生可能性、システムへの影響度を踏まえたリスク分析の実施 • リスク分析結果を踏まえたセキュリティ対応方針の決定（リスク対応優先度、遵守すべきセキュリティ標準、検証方法、対応リソースなど）	• 5.1 情報セキュリティのための方針群 • 5.9 情報及びその他の関連資産の目録
セキュリティ要件定義 • 遵守すべきセキュリティ標準（セキュリティベースライン）や、詳細リスク分析結果等に基づいた、システムとして満たすべきセキュリティ要件の定義（機能、機能面）	• 8.26 アプリケーションのセキュリティの要求事項
セキュア調達 • セキュリティ要件に基づき、調達仕様書のセキュリティ仕様策定 • セキュリティ仕様に関する、委託先との責任範囲の明確化 • 委託先に求めるセキュリティ管理基準の策定 • セキュリティ仕様を満たす能力を有した安全な委託先の選定 • 不正侵入の経路となるバックドア等が含まれていない、サポートを受けられる安全なプロダクトの選定	• 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情報セキュリティの取扱い

各種テーマごとの対策

【参照：テキスト17-2-1.】
第17章 - 21

Security by Design 実施手順例2

実施手順（例）	選択すべき管理策（例）
セキュリティ設計 • セキュリティ設計の実施 ➢ アプリケーションセキュリティ ➢ OSセキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ ➢ セキュリティ運用（平時、有事）	• 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
セキュリティ実装 • 設計に基づくシステムにおけるセキュリティ機能の実装 • セキュリティ設計に基づくアプリケーションのセキュアコーディング • セキュリティ設計に基づくプラットフォームのセキュリティ設定の実施 ➢ OS セキュリティ ➢ ミドルウェアセキュリティ ➢ ネットワークセキュリティ ➢ クラウドセキュリティ ➢ 物理セキュリティ	• 8.28 セキュリティに配慮したコーディング

各種テーマごとの対策

【参照：テキスト17-2-1.】
第17章 - 22

Security by Design 実施手順例3

実施手順（例）	選択すべき管理策（例）
セキュリティテスト • セキュリティ機能テストの実施 ➢ 単体テスト ➢ 結合テスト ➢ システムテストなど • 脆弱性診断の実施 ➢ Webアプリケーション脆弱性診断 ➢ プラットフォーム脆弱性診断 ➢ スマートフォンアプリケーション診断 ➢ 高度セキュリティ診断（ペネトレーションテストなど） ➢ 機能テストで検出されたバグの是正対応 ➢ 脆弱性診断で検出された脆弱性に対するリスクベースの是正対応	• 8.29 開発及び受入れにおけるセキュリティ試験 • 8.33 試験情報 • 8.34 監査試験中の情報システムの保護

各種テーマごとの対策

【参照：テキスト17-2-1.】
第17章 - 22

Security by Design 実施手順例4

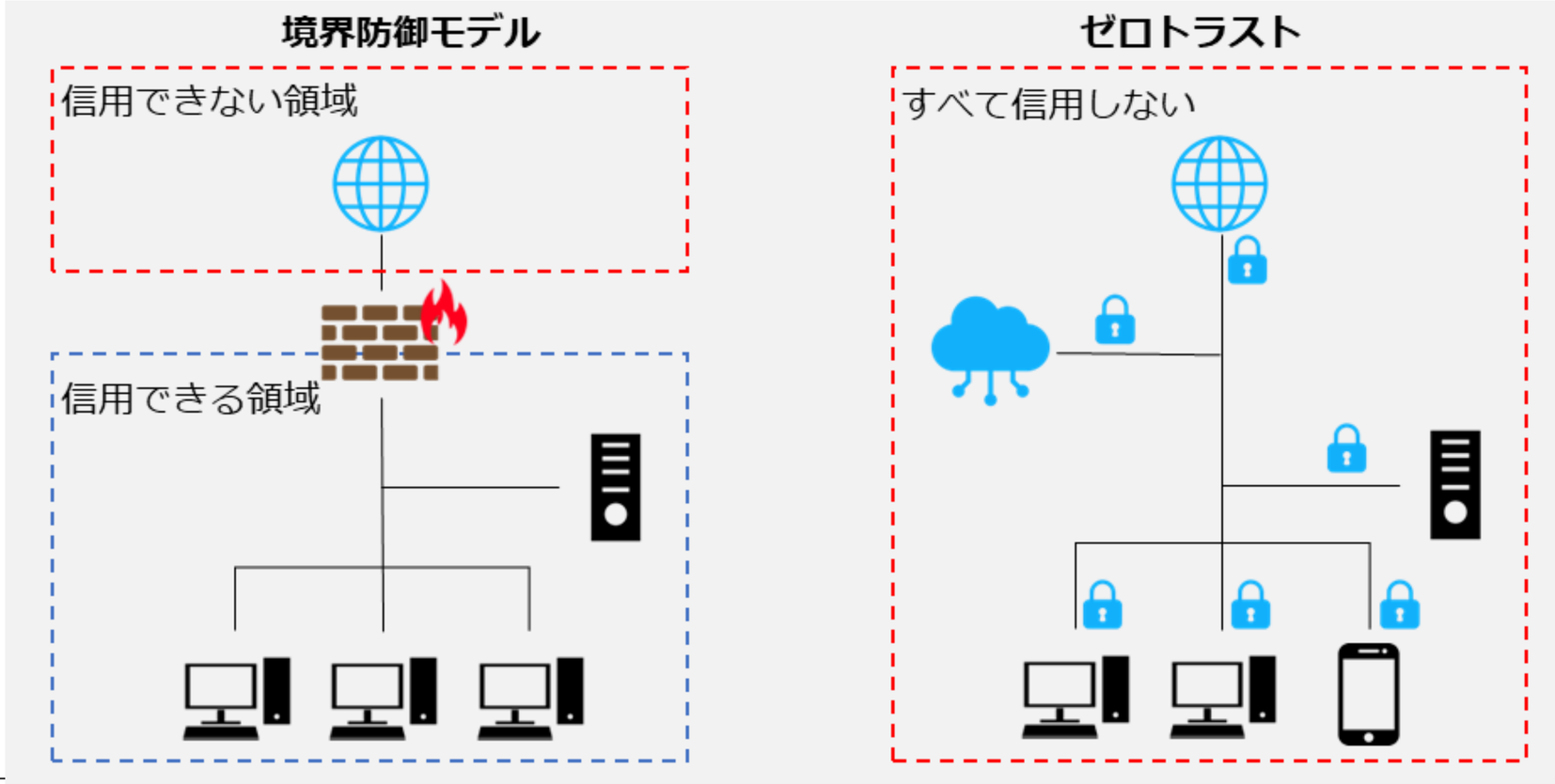
実施手順（例）	選択すべき管理策（例）
セキュリティ運用準備 • セキュリティ運用体制の確立 • 下記項目に対応したセキュリティ運用手順の整備 ➢ 平時の運用 ✓ 構成管理、変更管理 ✓ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ✓ 脅威情報収集、自システムへの影響分析 ✓ CVSSなどに基づくリスクに応じた脆弱性対応 ✓ 定期的な脆弱性診断の実施 ➢ 有事の運用 ✓ インシデント対応 • 有事を想定したセキュリティ運用訓練の実施	• 5.24 情報セキュリティインシデント管理の計画及び準備 • 5.29 事業の中断・阻害時の情報セキュリティ • 8.9 構成管理 • 8.32 変更管理 • 8.19 運用システムに関わるソフトウェアの導入
セキュリティ運用 • セキュリティ運用の実施 ➢ 平時の運用 ✓ 構成管理、変更管理 ✓ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ✓ 脅威情報収集、自システムへの影響分析 ✓ CVSSなどに基づくリスクに応じた脆弱性対応 ✓ 定期的な脆弱性診断の実施 ➢ 有事の運用 ✓ インシデント対応	• 5.7 脅威インテリジェンス • 5.26 情報セキュリティインシデントへの対応 • 5.29 事業の中断・阻害時の情報セキュリティ • 5.37 操作手順書 • 8.9 構成管理 • 8.15 ログ取得 • 8.16 監視活動 • 8.32 変更管理

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 23

ゼロトラスト・境界防御モデル

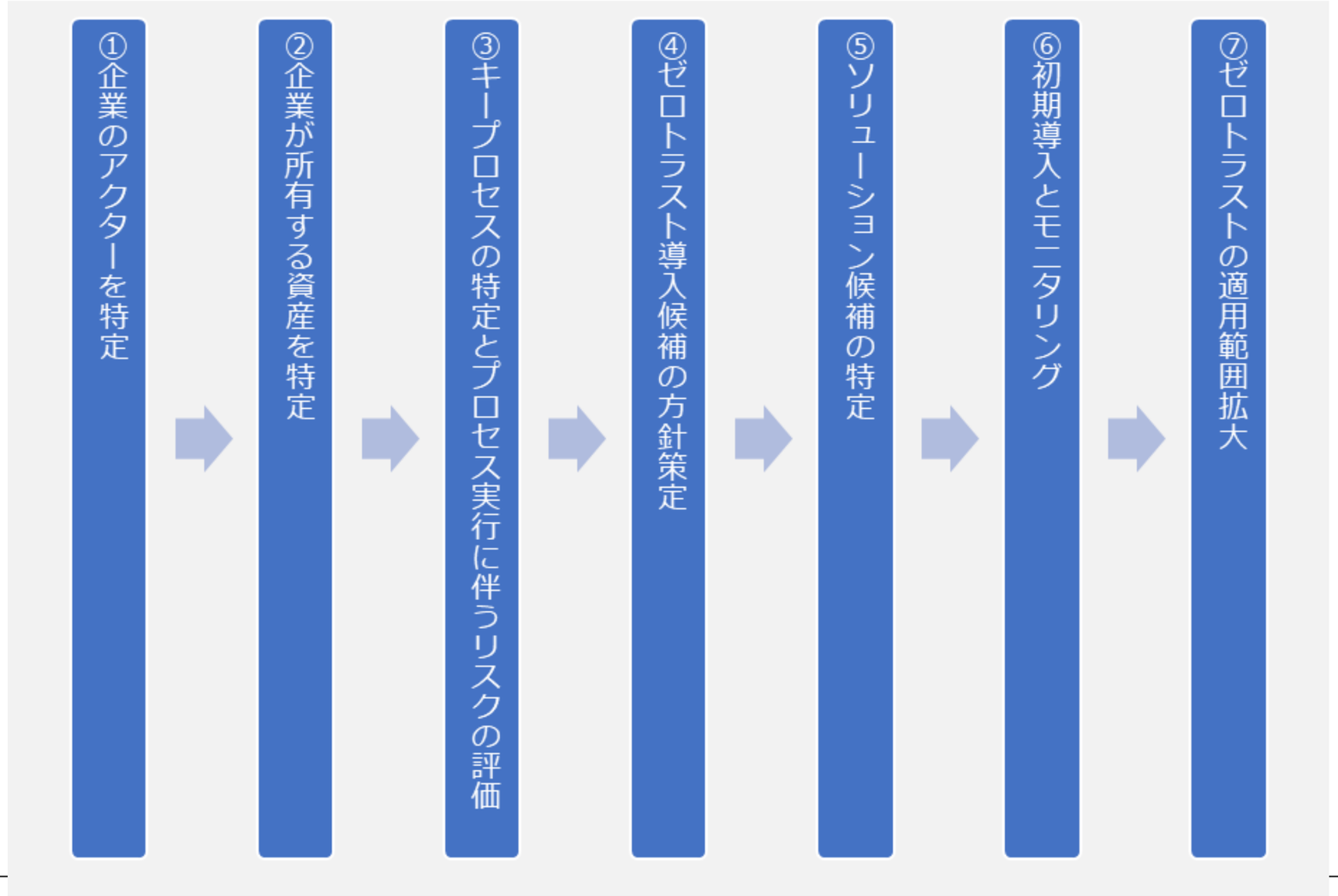
関連する主な管理策
5.9、5.15~5.23、5.29~5.30、8.1~8.3、8.15~8.16、8.21、8.32



各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 24

ゼロトラスト・境界防御モデル



各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 26

ゼロトラスト導入に向けた実施手順例1

実施手順（例）	選択すべき管理策（例）
準備工程 新たに導入する必要のあるプロセスやシステムを判断することおよびアクセスの認証・認可を正しく行うため、現在の運用状況を把握する。 a. 情報システム管理者は、次の事項を調査し、詳細に理解する。 ・資産 (デバイスやネットワークなど) ・主体 (ユーザ・権限など) b. 経営者は、次の事項を調査し、詳細に理解する。 ・ビジネスプロセス	• 5.9 情報及びその他の関連資産の目録 • 5.16 識別情報の管理 • 5.18 アクセス権 • 8.2 特権的アクセス権
① 企業のアクターを特定 a. 情報システム管理者は、業務に必要な者のみに情報にアクセスできる権限を与える。 b. アクセス権限および操作権限は、認められた場合以外は与えないようにする。	• 5.15 アクセス制御 • 5.16 識別情報の管理 • 5.17 認証情報 • 5.18 アクセス権 • 8.2 特権的アクセス権 • 8.3 情報へのアクセス制限

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 26

ゼロトラスト導入に向けた実施手順例2

実施手順（例）	選択すべき管理策（例）
② 企業が所有する資産を特定 デバイスを識別して管理する。 a. 企業の情報にアクセスするデバイスは、シャドーITを含めて、すべて識別して管理する。 b. シャドーITは可能な限り資産化する。	• 5.9 情報及びその他の関連資産の目録 • 8.1 利用者終端装置
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 a. 業務プロセス、データフロー、組織のミッションにおける業務プロセスとデータフローの関係（プロセス）を特定する。 b. 特定したプロセスのうち、ゼロトラストに移行するプロセスを決定する。認証・認可の判断を導入することによる失敗のリスクを考慮し、初めは組織の事業に与える影響が低いビジネスプロセスを選択し、徐々に対象を広げる。	• 5.29 事業の中断・阻害時の情報セキュリティ • 5.30 事業継続のためのICTの備え

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 27

ゼロトラスト導入に向けた実施手順例3

実施手順（例）	選択すべき管理策（例）
④ ゼロトラスト導入候補の方針策定 a. 資産、プロセスの特定後、ゼロトラストの導入により影響を受ける対象をすべて特定する。 ・上流リソース（例:ID管理システム） ・下流リソース（例:セキュリティ監視） ・エンティティ（例:主体ユーザ） b. ゼロトラスト導入候補となるビジネスプロセスで使用されるリソースの重要さを決定する。 c. リソースの重要さを踏まえて、何を対象に、どこへゼロトラストの機能を導入するのかを決定する。	• 5.9 情報及びその他の関連資産の目録
⑤ ソリューション候補を特定 ④で策定した内容をもとに、導入箇所に適するソリューションを検討する。	• 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情報セキュリティの取扱い • 5.21 ICTサプライチェーンにおける情報セキュリティの管理 • 5.22 供給者のサービス提供の監視、レビュー及び変更管理 • 5.23 クラウドサービスの利用における情報セキュリティ • 8.21 ネットワークサービスのセキュリティ

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 27

ゼロトラスト導入に向けた実施手順例4

実施手順（例）	選択すべき管理策（例）
⑥ 初期導入とモニタリング a. ソリューションの初期導入時は、実際に通信の遮断は行わず、適用したポリシーや初期動作の確認を行う。 b. 動作に問題がないことを確認後、運用を開始する。	• 8.16 監視活動
⑦ ゼロトラストの適用箇所拡大 a. 運用開始後は、ネットワークや資産の監視は継続しつつ、トラフィックの記録を行う。 b. トラフィックを記録していくなかで、ポリシーの変更や適用箇所の拡大を適宜実施する。 c. ポリシー変更を実施する場合は、影響が問題にならないように確認する。	• 8.15 ログ取得 • 8.16 監視活動 • 8.32 変更管理

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 – 28,29

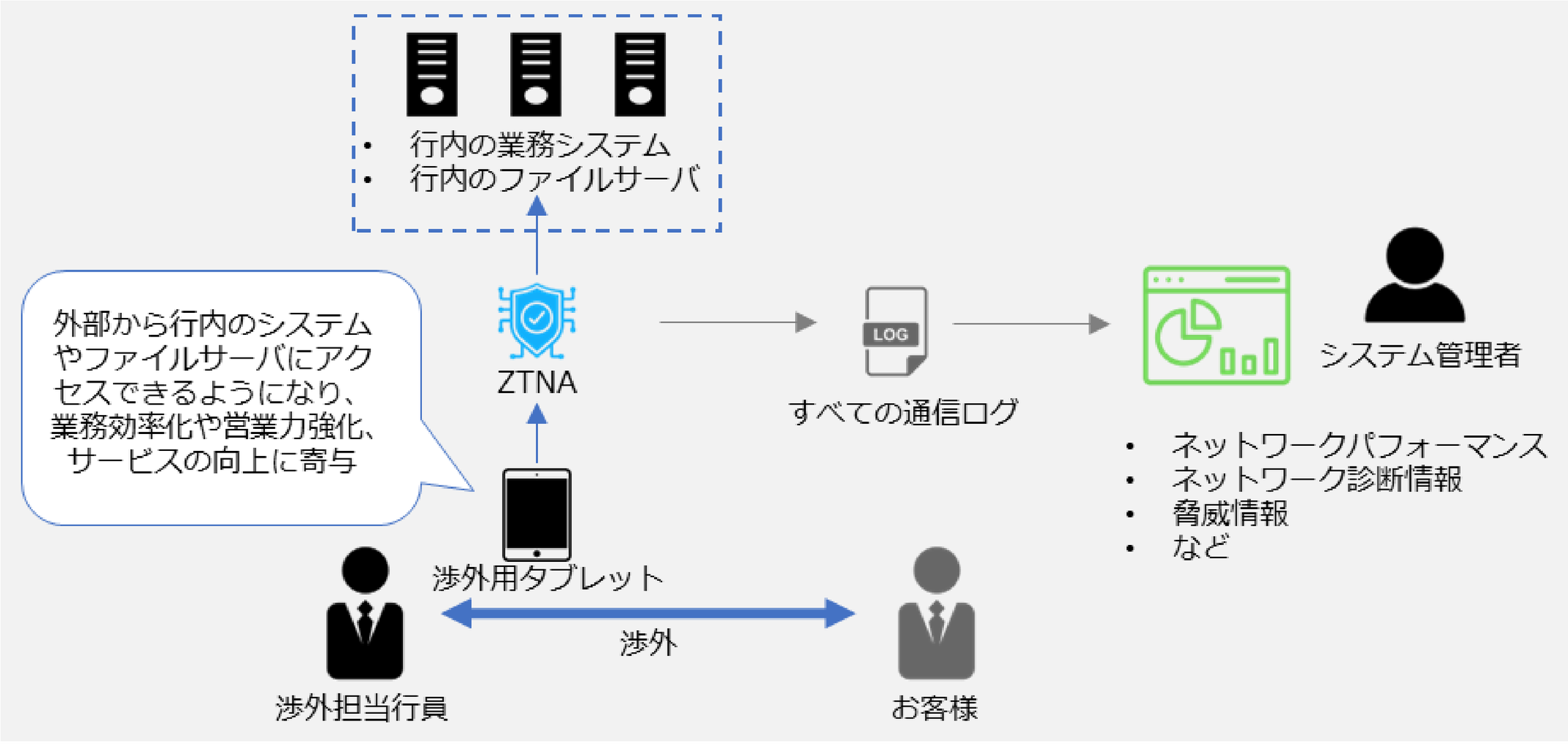
ゼロトラストを実装するための主な技術要素

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

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 - 30

ゼロトラスト導入事例

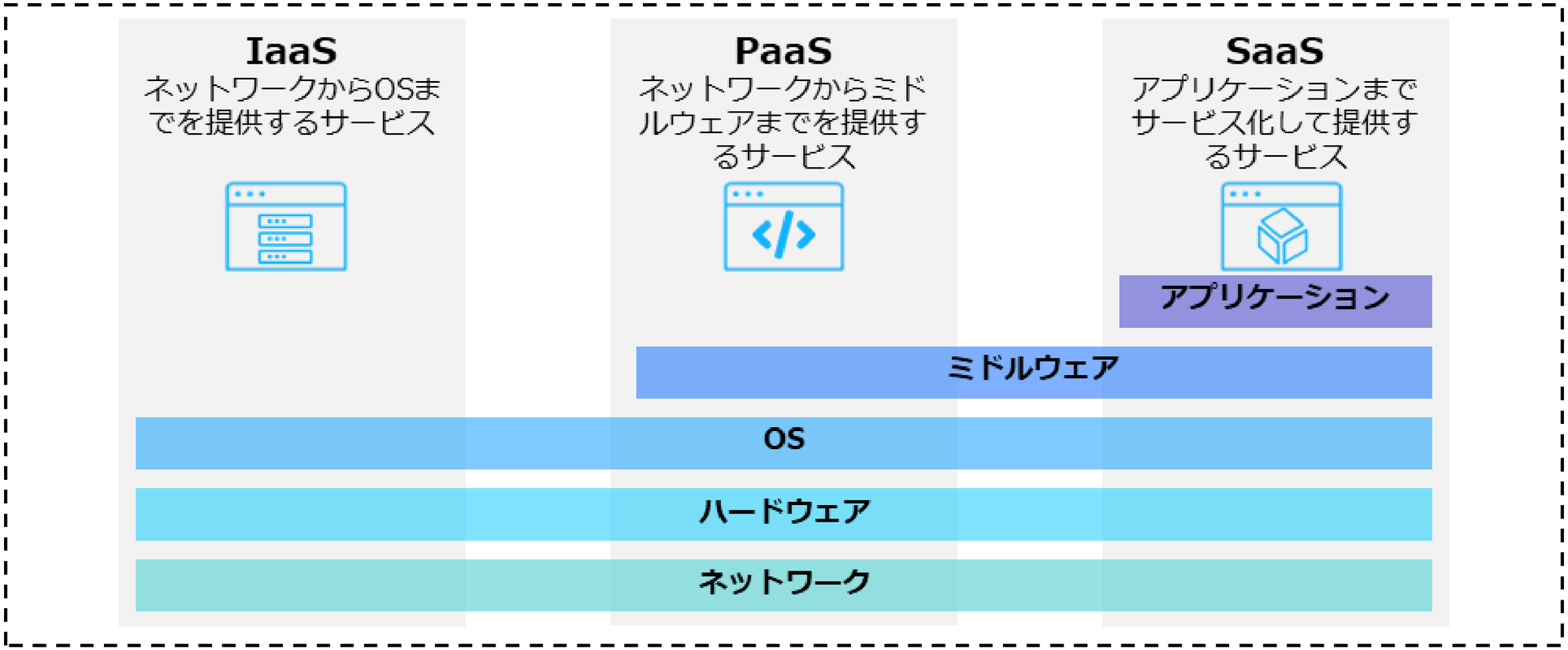


各種テーマごとの対策

【参照：テキスト17-2-3.】
第17章 - 31

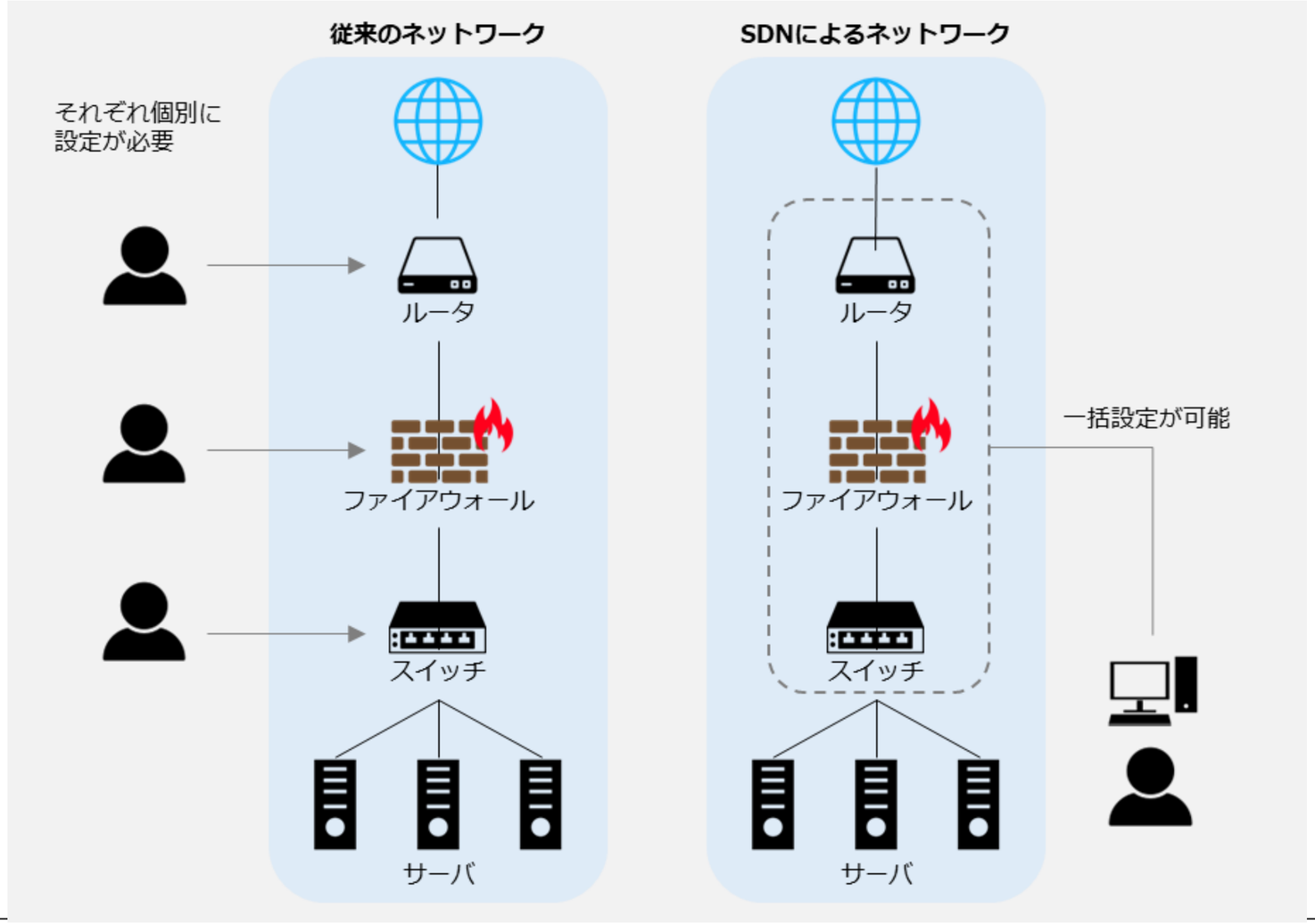
ネットワーク制御

関連する主な管理策
5.23、6.7、8.20~8.24



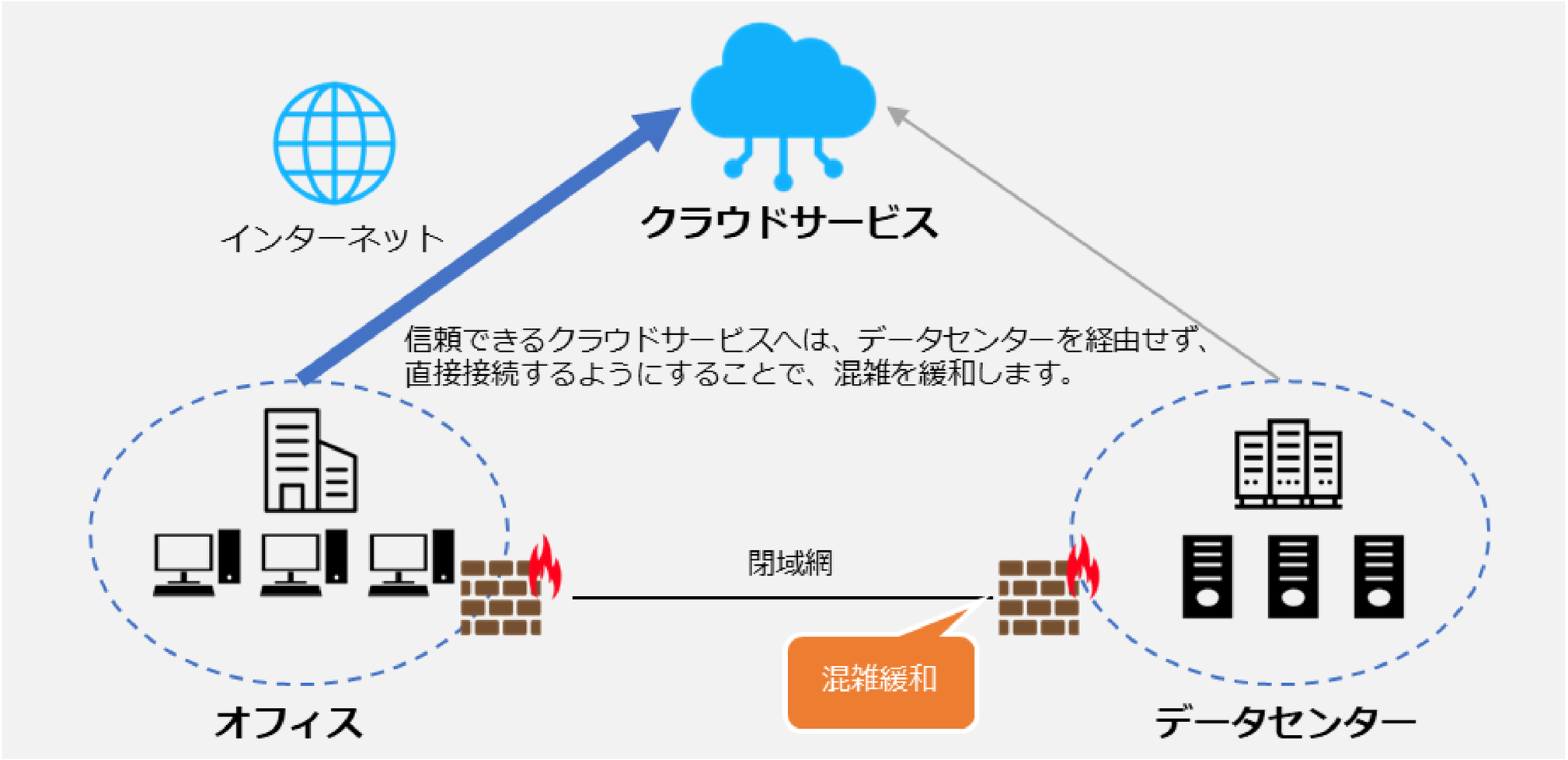
各種テーマごとの対策

SDN（Software Defined Networking）



各種テーマごとの対策

SD-WAN（Software Defined –Wide Area Network）



各種テーマごとの対策

【参照：テキスト17-2-4.】
第17章 - 35

セキュリティ統制

関連する主な管理策
5.1、5.9、5.15～5.18、5.23～5.28、8.1～8.5

実施内容（例）	選択すべき管理策（例）
リスク評価と分析 • 組織内の情報資産やプロセスを評価し、セキュリティリスクを特定 • リスクの重要度や影響を評価し、優先順位づけ	• 5.9 情報及びその他の関連資産の目録
ポリシーの策定 • セキュリティポリシーを作成し、組織内での適用範囲や要件を定義 • ポリシーは法規制や業界のガイドラインに準拠	• 5.1 情報セキュリティのための方針群
技術的対策の実施 • 資産に対してセキュリティ対策の実施 ➢ ワークロード ➢ データ ➢ アイデンティティ ➢ ネットワーク ➢ デバイス　など	• 5.15 アクセス制御 • 5.16 識別情報の管理 • 5.17 認証情報 • 5.18 アクセス権 • 5.23 クラウドサービスの利用における情報セキュリティ

各種テーマごとの対策

【参照：テキスト17-2-4.】
第17章 - 35

セキュリティ統制

実施内容（例）	選択すべき管理策（例）
監視と評価 • セキュリティ対策の効果を監視し、定期的な評価の実施 • セキュリティインシデントが発生した場合は、原因を分析し、対策の改善	• 5.25 情報セキュリティ事象の評価及び決定 • 5.27 情報セキュリティインシデントからの学習 • 5.28 証拠の収集 • 8.15 ログ取得 • 8.16 監視活動
変更管理 • システムやポリシーに変更があった場合、セキュリティに影響を与えないように変更管理プロセスを確立	• 8.32 変更管理
対応計画の策定 • セキュリティインシデントが発生した場合の対応計画を策定し、迅速かつ効果的に対処	• 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 • 5.26 情報セキュリティインシデントへの対応

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 – 36

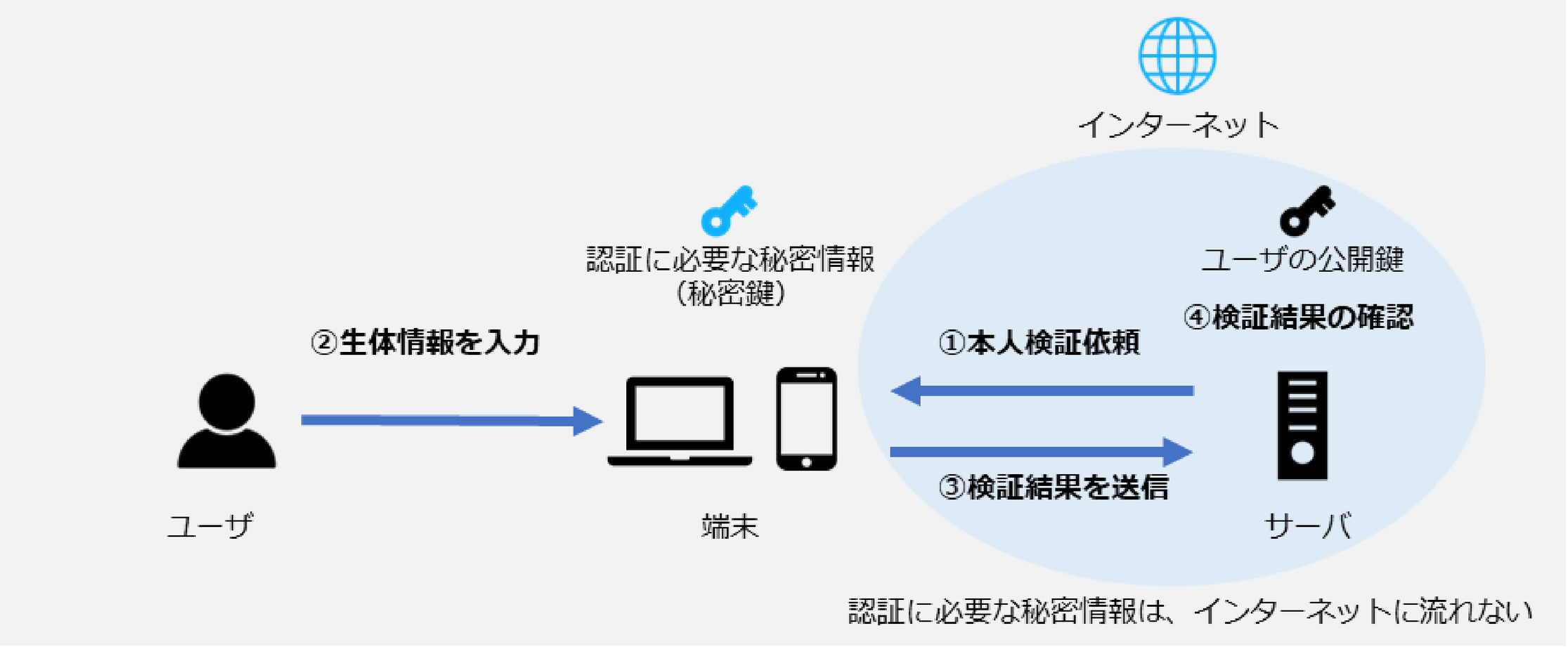
セキュリティ統制を確立するための技術

- SWG（Secure Web Gateway）
- SDP（Software Defined Perimeter）
- EDR（Endpoint Detection and Response）
- EPP（Endpoint Protection Platform）
- IAM（Identity and Access Management）
- FIDO（Fast Identity Online）
- CWPP（Cloud Workload Protection Platform）
- DLP（Data Loss Prevention）
- CASB（Cloud Access Security Broker）
- SIEM（Security Information and Event Management）
- CSPM（Cloud Security Posture Management）
- SOAR（Security Orchestration Automation and Response）

各種テーマごとの対策

【参照：テキスト17-2-4.】
第17章 - 37

FIDO（Fast Identity Online）



FIDO2の認証の仕組み

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 – 38

インシデント発生時の対応

関連する主な管理策
5.5、5.6、5.24~5.28、6.8

実施手順（例）	
①検知・初動対応	検知と連絡受付： • パソコンの動作異常やウイルス対策ソフトの警告が表示された場合、ウイルス感染の可能性があるため、情報セキュリティ責任者に報告する。 • ウイルスが添付されたメールを受け取った外部から通知を受けて発覚した場合も、情報セキュリティ責任者に報告する。 • 内部から外部への不正な通信、外部からの意図しない通信や、一時的な大量の通信、ウイルスに関係する特定サイトへのアクセスなどは、ウイルス感染を疑う。 初動対応： • 感染したパソコンやサーバの利用を停止し、ネットワークから切り離す。
②報告・公表	第二報以降・最終報： • 影響を及ぼした取引先や顧客に対して、セキュリティインシデントに関する報告を行う。 • ウイルス感染による影響によって、業法などで報告が求められる場合は所管の省庁へ報告する。 • ウイルス感染やランサムウェア感染の場合は、IPAの届出窓口へ届け出る。
③復旧・再発防止	調査・対応： • 他のパソコンやサーバがウイルスに感染していないか、ウイルス対策ソフトの定義ファイルを最新にしてからチェックする。 • ウイルス対策ソフトに従ってウイルスを駆除する。 • ウイルス駆除ができない場合、OSのクリーンインストールを実施し、すべてのプログラムを入れ直す。 復旧： • ウイルスの駆除が確認できたら、対象のパソコンやサーバをネットワークに接続し、復旧する。

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 – 39

フォレンジック

フォレンジックとは

フォレンジックとは、セキュリティインシデントが起きた際に、コンピュータ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調査・解析する技術・手法・手続きを指します。

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

各種テーマごとの対策

【参照：テキスト17-2-2.】
第17章 – 40

インシデント対応手順例1

実施手順（例）
1. 発生したインシデントの内容把握
発生したインシデントを把握します。 **インシデントの種類** ✓ 情報流出・データ破壊 ✓ 不正アクセス、不正プログラムの実行 ✓ 操作・設定ミスなど **検知・発覚のきっかけ** ✓ ログのレビュー・監視 ✓ 内部通報 ✓ 不正検知システムなど **発生時刻** ✓ システム時計の正確性の確認 **初動対処の開始までの記録** 発生したインシデントの検知・発覚から、報告または対処依頼の連絡までの時間およびその間のインシデントに対する対処の有無について記録をとります。 ✓ 発生したインシデントを知る人物および人数 ✓ インシデントの対象物の確保の有無 インシデントの対象物を確保していた場合 対象物を確保した日時、人物（役職）、場所、確保時の対象物（および周辺）に対する行為、確保後の対象物に対する対処（の有無）とその内容を記録します。 インシデントの対象物を確保していない場合 対象物を確保する（予定の）日時と場所、確保時の対象物（およびその周辺）の状態を詳細に記録します。

各種テーマごとの対策

インシデント対応手順例2

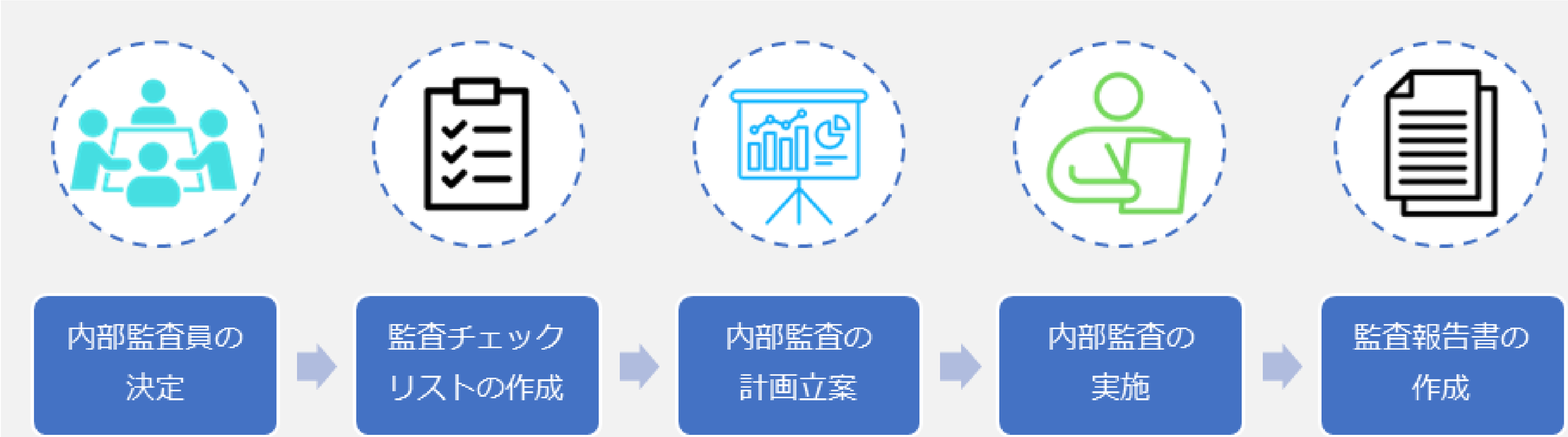
実施手順（例）
2. 発生したインシデントに関する対象物の決定
対象物に対する情報収集および対象物の絞り込み ✓ 発生したインシデントに関する対象物の種類および個数を確認します。 ・コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型） ・ネットワーク機器（ルータ、ファイアウォール、IDS、IPS） ・HDD、SSDなど ✓ 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。 ✓ 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。 ✓ 発生したインシデントに関する対象物の使用者、および管理者を確認します。 ✓ 発生したインシデントに関する対象物を円滑に証拠保全するための周辺機器、およびドキュメントの有無を確認します。 **対象物の選定と優先順位づけ** ✓ 保全を行う前の対象物（デバイス）を選定し、その理由を明確にします。 ✓ （対象物が複数ある場合）取扱う対象物の優先順位をつけ、その理由を明確にします。
3. 証拠保全を行う上で必要な情報の収集
対象物の情報 ✓ 対象物の形状、個数、物理的な状態を確認します。 ・対象物のラベル情報（メーカー、型番、モデル名、記憶容量など） ・ケーブルの接続状況 ・通常環境下で視認可能な物理的破損、損傷の有無など ✓ HDD、SSD、ストレージメディアの記憶容量、インタフェースの状況を確認します。 ✓ セキュリティ設定の有無を確認します。 ・HDD、SSDのパスワードロック ・HDD、SSD全体暗号化または一部のファイル・フォルダの暗号化 ・PC周辺のワイヤストッパー、ロッカーなど

3. セキュリティ対策状況の有効性評価

内部監査・外部監査

内部監査

【参照：テキスト18-1-1.】
第18章 – 02



外部監査

【参照：テキスト18-1-1.】
第18章 – 03

管理基準・監査基準

情報セキュリティ管理基準

組織における情報セキュリティマネジメントの円滑で効果的な確立を目指し、マネジメントサイクルの構築から具体的な管理策まで、包括的な適用範囲を定めたものです。この管理基準は「マネジメント基準」と「管理策基準」の2項目から構成されています。

マネジメント基準……情報セキュリティマネジメントの計画・実行・点検・処置に必要な実施すべき事項が提示されています。
管理策基準……リスク対応方針に従って管理策を選択する際の選択肢が提示されています。

情報セキュリティ監査基準

情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範です。監査の品質を一定の水準に保ち、有効かつ効率的に実施できるように「一般基準」「実施基準」「報告基準」の3項目を提示しています。

一般基準……監査人としての適格性および監査業務上の遵守事項を定めています。
実施基準……監査計画の立案および監査手続きの適用方法を中心に、監査実施上の枠組みを定めています。
報告基準……監査報告にかかる留意事項と、監査報告書の記載方式を定めています。

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