中小企業向け
サイバーセキュリティ実践ハンドブック
中小企業も安心！セキュリティ対策でDXを加速

セミナースライド

東京都産業労働局

講師紹介

氏名	星野 樹昭（ほしの しげあき）
業務経歴	25年（セキュリティ経験：19年）
専門分野	ITインフラ設計 / 構築 / テスト 移行設計 セキュリティ製品導入支援 ISMS導入支援
保有資格	情報処理安全確保支援士（登録番号 第002047号） MCP
コメント	官公庁や金融機関などの大規模環境から、中小零細企業規模まで、オンプレ/クラウド問わず様々な環境のITインフラ環境導入・移行の経験あり。 セキュリティ製品の導入支援では、DB暗号化ソフトウェアやWeb Application Firewall、クライアントPCのセキュリティ対応など、実績豊富。 現在はISMSコンサルも実施しており、活動は多岐にわたる。

目的

- 継続的な社内のセキュリティ対策ができる人材を育成する
- 実践的な課題解決で社内セキュリティ体制を強化する

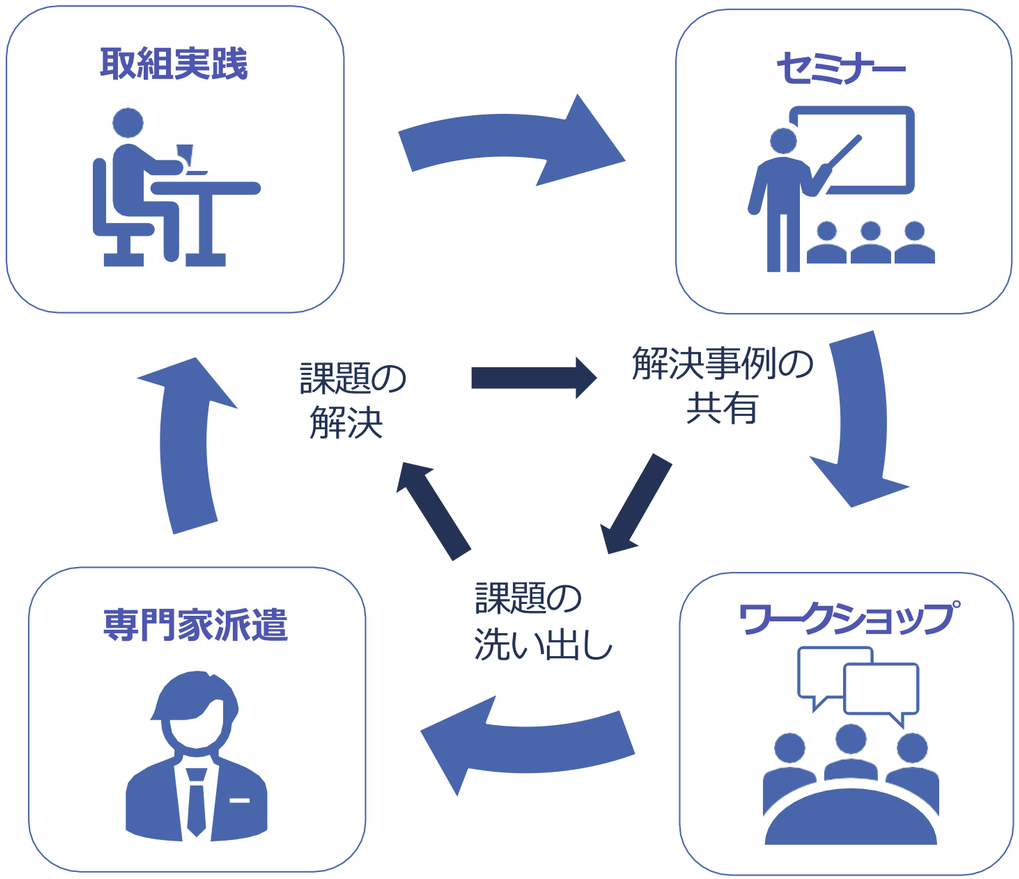
東京都他事業と本事業の位置づけ

【支援領域】 組織的支援 人的支援 技術的支援

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実施しないといけないと思っている状態	セキュリティに関する方針・ルール、対策を決めている状態	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	最適化や習慣化がされている状態
中小企業サイバーセキュリティの極意	組織的支援 人的支援	→	→				
中小企業サイバーセキュリティ向上支援事業	組織的支援 技術的支援		→				
中小企業サイバーセキュリティ対策強化サポート事業	技術的支援		→				
中小企業サイバーセキュリティ対策継続支援事業（本事業）	組織的支援 人的支援			Before →	After →		
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）	組織的支援	→	→	→			
サイバーセキュリティ対策促進助成金	技術的支援		→	→	→	→	→

支援内容

セミナーで得た知見やワークショップの事例を参考に、専門家と決めた取組を実践します。不明点や不安点などは、コミュニティを通して質問を行い、専門家だけでなく、参加企業同士でフォローします。



導入済みのセキュリティ機器の日常的な運用方法や、業務内容に沿ったセキュリティルールの策定方法など、中小企業の皆様が自主的にセキュリティ対策業務を運営する上で生じる疑問点の解決に直接役立つ、実践的な知識・ノウハウを講義形式でお伝えします。

ワークショップで洗い出した課題やセミナー・ワークショップの気づきをもとに、企業が直面しているセキュリ ティ上の問題点解決や、社内体制構築へ向けた支援を行います。

参加企業の皆様同士で、それぞれの課題に一緒に取り組み、解決策を考えます。自社の問題だけでなく、他社の事例に触れることで、様々な課題の解決に向けた引き出しとなる知識を得られます。

セミナー内容

1. デジタル時代の社会とIT情勢
   デジタル時代の社会変革とIT情勢の関係性

2. 事例を知る：重大インシデント発生から課題解決まで
   情報セキュリティの概況
   重大インシデント事例から学ぶ課題解決

3. サイバーセキュリティの基礎知識
   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
   Security Action（セキュリティ対策自己宣言）
   サイバーセキュリティ対策基準レベル

1. デジタル時代の社会とIT情勢

デジタル時代の社会変革とIT情勢の関係性

デジタル時代の社会変革とIT情勢の関係性 【参照：テキスト1-1-1.】

社会の現状と今後の動向（Society5.0）

- Society5.0とは
  「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）」
  内閣府. “Society 5.0” https://www8.cao.go.jp/cstp/society5_0/ , (参照 2023-07-06)

- Society1.0：狩猟社会
  Society2.0：農耕社会
  Society3.0：工業社会
  Society4.0：情報社会
  Society5.0：未来社会
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_mirai1.html
  Society5.0 ビックデータ連携がもたらす未来社会像
  https://wwwc.cao.go.jp/lib_006/society5_0/society5_0_bigdata1.html

デジタル時代の社会変革とIT情勢の関係性 【参照：テキスト1-1-1.】

デジタルトランスフォーメーション(DX)とは

【定義】

「DXとは、企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。」

経済産業省. “デジタルガバナンス・コード2.0” https://www.meti.go.jp/policy/it_policy/investment/dgc/dgc2.pdf , (2023-07-06)

【概要】

- DXは、データやデジタル技術を使って新たな価値を生み出すこと。
- DXには、ビジネスモデルや企業文化の変革が必要。
- DX戦略では、経営ビジョンを描き、関係者を巻き込んで課題を解決する。
- DXは「知識」、「人材」、「**セキュリティ**」が重要な要素。

デジタル時代の社会変革とIT情勢の関係性 【参照：テキスト1-1-1.】

IT化とDXの違いって？？

ことば	意味	視点
IT化	情報技術を活用して業務プロセスなどを効率化し、コスト削減すること。	社内
DX	ITを含むデジタル技術を駆使してビジネスを変革し、新しい価値を生み出すこと。	顧客 社会

デジタル社会の三方良し
「売り手良し」⇒「社内」
「買い手良し」⇒「顧客」
「世間良し」　⇒「社会」

デジタル時代の社会変革とIT情勢の関係性

サイバーセキュリティ経営ガイドライン

経営者が認識するべき3原則

1. 「経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要」

2. 「サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要」

3. 「平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要」

経済産業省. “サイバーセキュリティ経営ガイドライン Ver 2.0” https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf , (2023-07-06)

2. 事例を知る：重大インシデント発生から課題解決まで

情報セキュリティの概況

重大インシデント事例から学ぶ課題解決

情報セキュリティの概況 【参照：テキスト2-1-1.】

情報セキュリティの脅威を学ぶ

【目的】

- 適切な予防策や対策を講じること

【内容】

- 攻撃手口の**傾向**を把握する
- 脅威に対する対策方法を理解する

【活用するべき代表的な刊行物】

- 情報セキュリティ白書

  情報セキュリティに関する現状や課題、脅威、対策について包括的に学ぶことができる。毎年発行されている。

- 情報セキュリティ10大脅威

  1年間の状況を反映して作成され、何を重視して対策を実施するべきかを学ぶことができる。毎年発行されている。

IPA.”情報セキュリティ白書2022”.
https://www.ipa.go.jp/publish/wp-security/sec-2022.html
(参照 2023-07-06).

IPA.”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
(参照 2023-07-06).

情報セキュリティの概況 【参照：テキスト2-1-2.】

情報セキュリティ白書

【記載内容】

- セキュリティインシデントの事例
- セキュリティ対策強化の取組み
- サイバーセキュリティ経営ガイドライン
- 国内外のセキュリティの動向
- セキュリティ人材の育成
- 中小企業のセキュリティ対策
- 個別テーマ（IoT、インフラシステム等）のセキュリティ動向
- セキュリティツールの紹介

情報セキュリティの概況 【参照：テキスト2-1-3.】

情報セキュリティ10大脅威 [組織編]

順位	前年順位	組織
1	1	ランサムウェアによる被害
2	3	サプライチェーンの弱点を悪用した攻撃
3	2	標的型攻撃による機密情報の窃取
4	5	内部不正による情報漏洩
5	4	テレワーク等のニューノーマルな働き方を狙った攻撃
6	7	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	8	ビジネスメール詐欺による金銭被害
8	6	脆弱性対策の公開に伴う悪用増加
9	10	不注意による情報漏えい等の被害
10	圏外	犯罪のビジネス化（アンダーグラウンドサービス）

IPA.”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 (参照 2023-07-06).

情報セキュリティの概況 【参照：テキスト2-1-3.】

情報セキュリティ対策の基本

攻撃の糸口	対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・糸口を知る	手口から重要視するべき対策を理解する

備える対象	対策の基本＋α	目的
インシデント全般	責任範囲の明確化	クラウドサービスを契約する際に、インシデント発生時は誰が対応する責任があるのかを明確化する
クラウドの停止	代替案の準備	業務が停止しないように代替案を準備する
クラウドの仕様変更	設定の見直し	更新情報を定期的に確認し、仕様変更により意図せず変更された設定を適切な設定に直す

IPA.”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 (参照 2023-07-06).

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-1.】

インシデント事例から学ぶ

【目的】

- 予防策の理解と強化
- リスクの認識
- 教育／訓練の材料
- 事後対応の改善

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

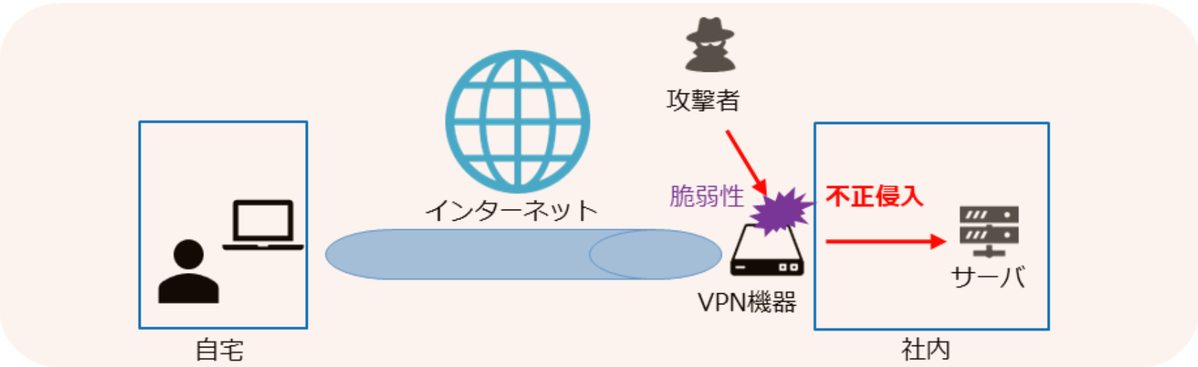
テレワークによるサイバー被害

【事例概略】

- テレワーク導入のために、社外からVPN接続できるようにした。
- VPN機器の脆弱性対応を実施した。
- すでに接続アカウントは抜かれた後で、そのアカウントを悪用された。

【対処ポイント】

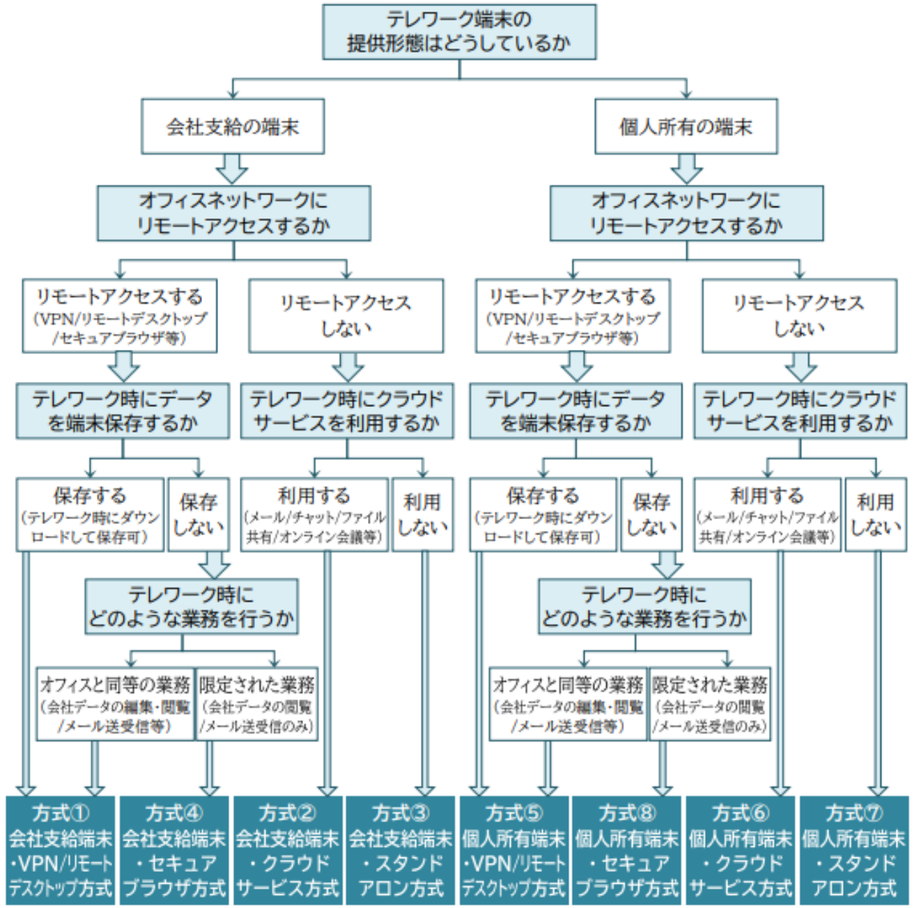
- 脆弱性を悪用されることで、何が起こるのかを理解する。
- すでに攻撃を受けていることを前提とする。



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【テレワーク方式概要】



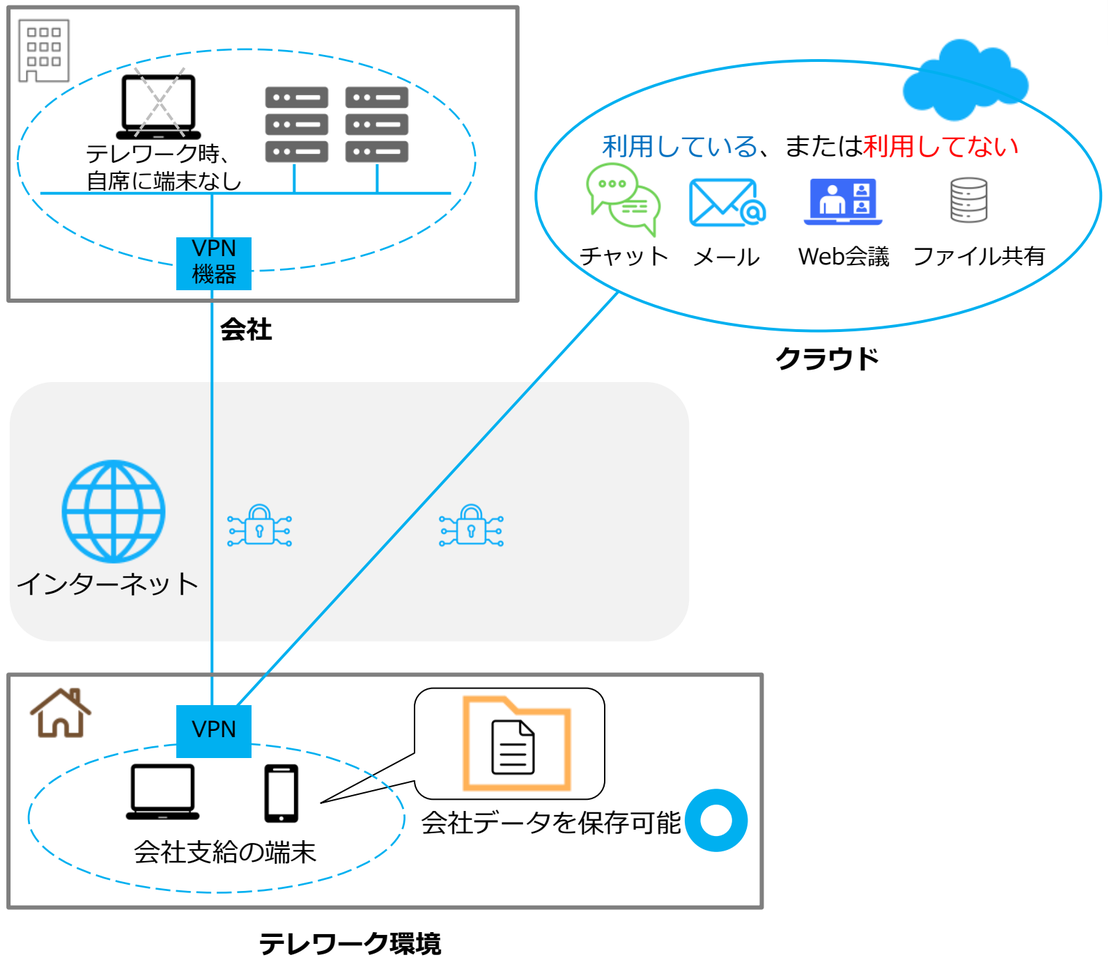
No	方式名
方式1	会社支給端末・VPN/リモートデスクトップ方式
方式2	会社支給端末・クラウドサービス方式
方式3	会社支給端末・スタンドアロン方式
方式4	会社支給端末・セキュアブラウザ方式
方式5	個人所有端末・VPN/リモートデスクトップ方式
方式6	個人所有端末・クラウドサービス方式
方式7	個人所有端末・スタンドアロン方式
方式8	個人所有端末・セキュアブラウザ方式

総務省. ”中小企業等担当者向けテレワークセキュリティの手引き”. https://www.soumu.go.jp/main_content/000753141.pdf (参照 2023-07-06).

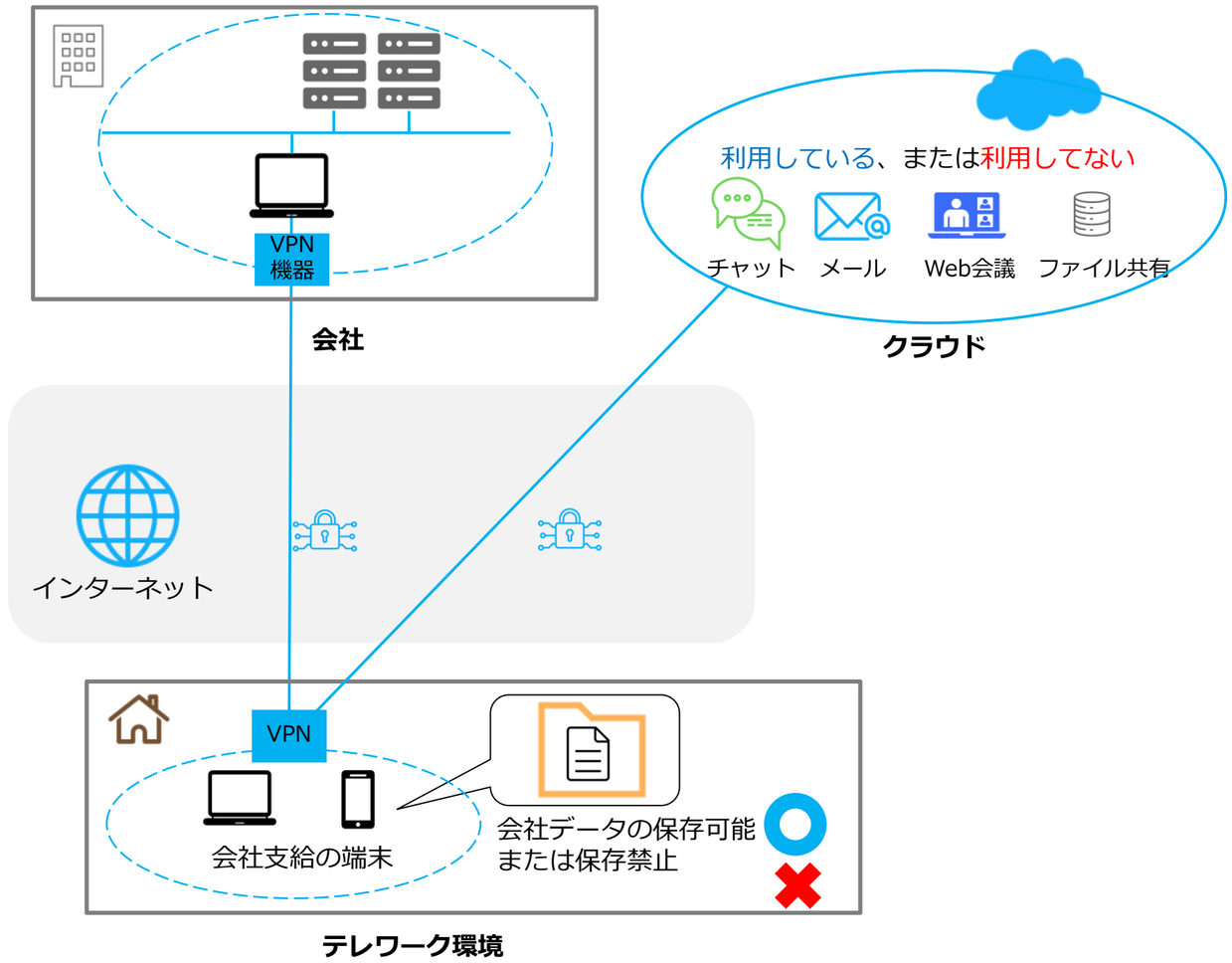
重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【VPN方式】



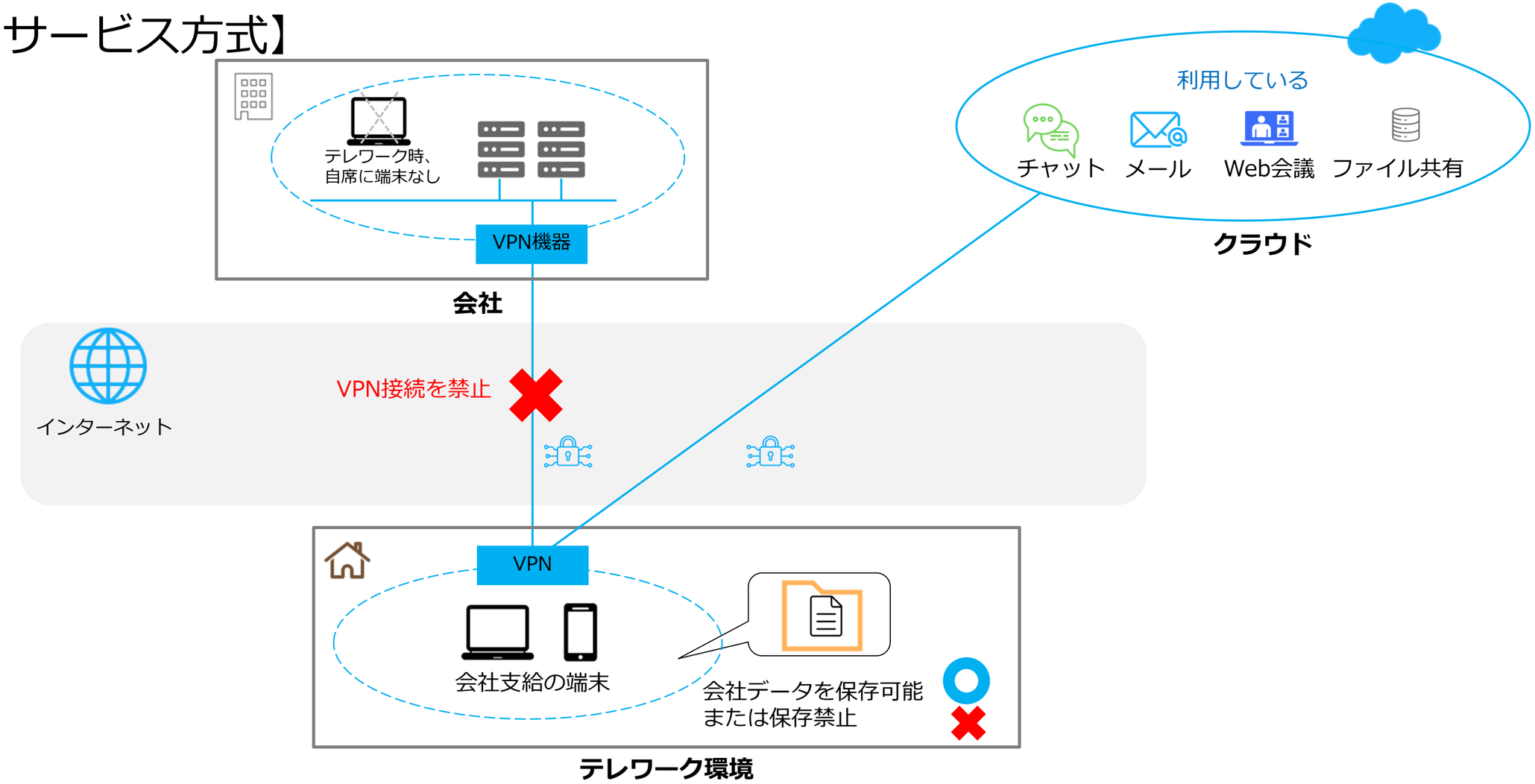
【リモートデスクトップ方式】



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

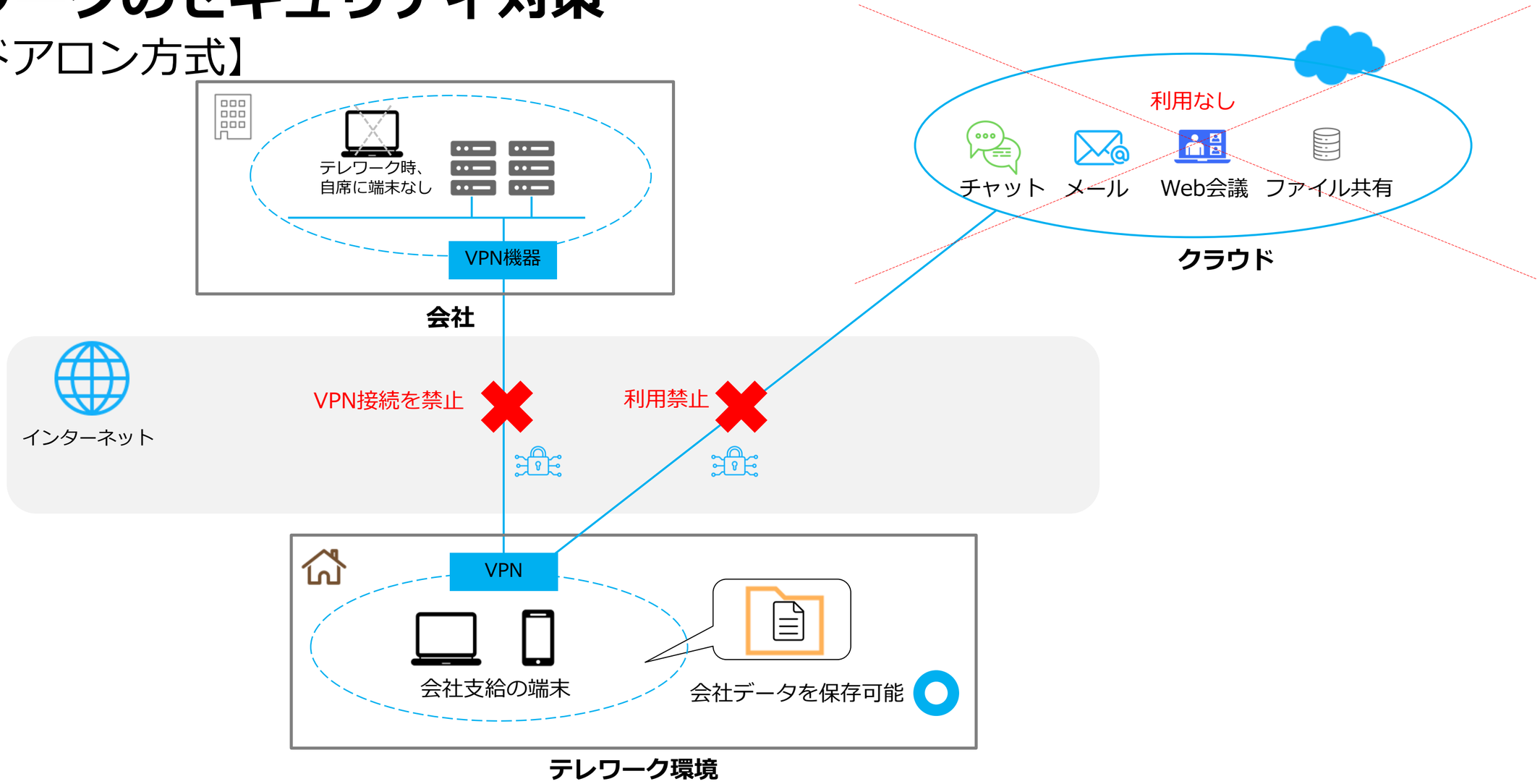
【クラウドサービス方式】



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

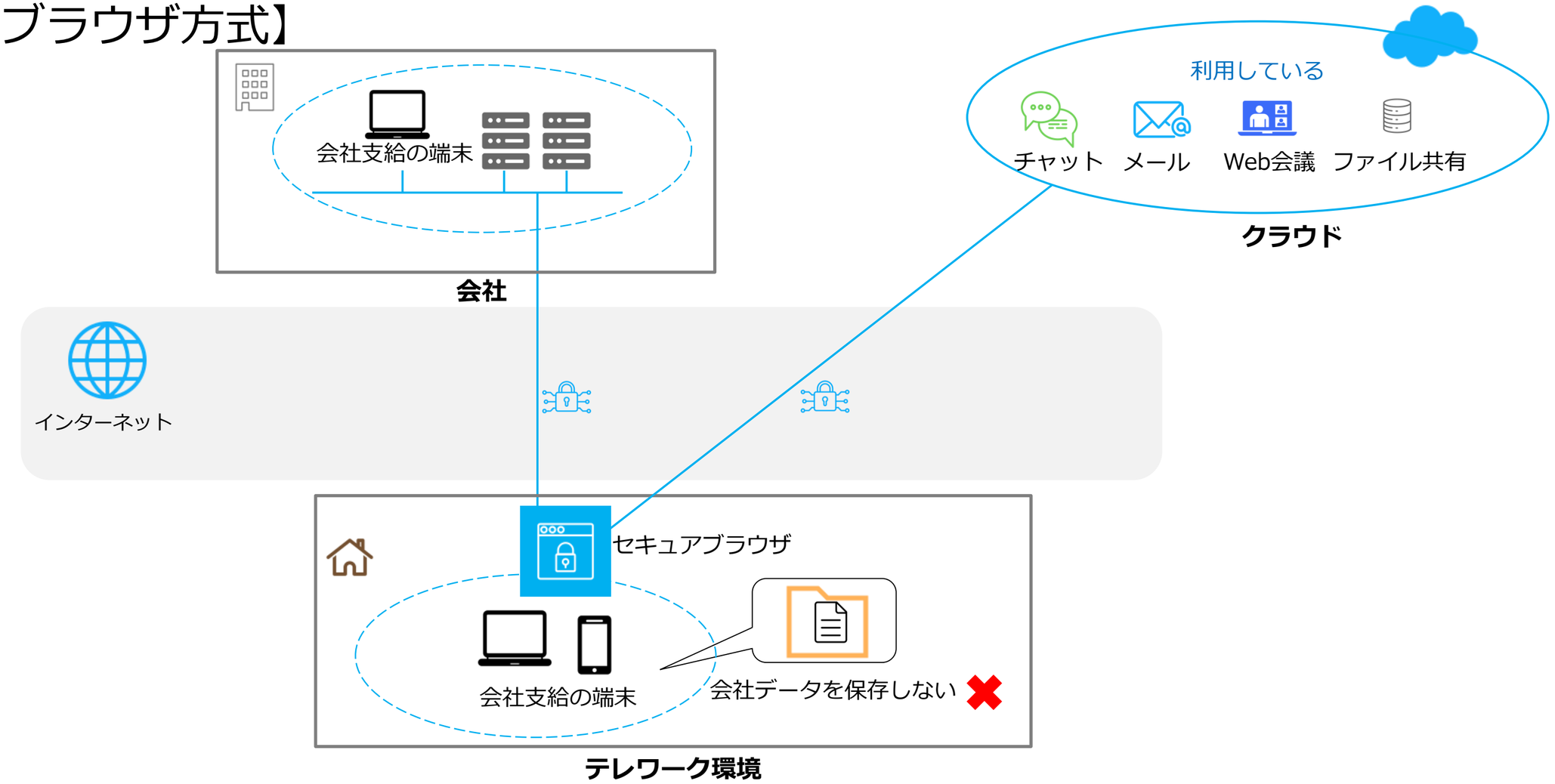
【スタンドアロン方式】



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【セキュアブラウザ方式】



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威】

- マルウェア感染
- 不正アクセス
- 端末の紛失・盗難
- 情報の盗難

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威の起因と対策】

脅威の起因	想定される対策
マルウェア感染 • 添付ファイル付きのメールを受信し開封 • 悪意のあるサイトを閲覧し、ソフトをダウンロード • USBメモリの接続	**マルウェア感染** • 検知製品（EPP）の導入 →不十分 • 挙動監視・対応支援製品（EDR）の導入 • UTM（マルウェア検知機能）の導入 • USBの利用制限 • USB自動実行の禁止
不正アクセス • VPN機器の脆弱性 • パスワードの使いまわし • 強度の弱いパスワード設定	**不正アクセス** • 脆弱性の確認とパッチ適用 • サイトやサービスごとにパスワード変更 • 10文字以上の複雑なパスワード作成 • MFA（多要素認証）の導入 • UTM（IPS/IDS機能）の導入

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【想定される脅威の起因と対策】

脅威の起因	想定される対策
端末の紛失・盗難 • サテライトオフィスに端末を忘れて帰って紛失 • 電車やタクシー置き忘れ、紛失 • カフェ等で離籍した際に盗難	**端末の紛失・盗難** • 社内ルールの徹底 →出しっぱなしにしない お酒を飲むときは持ち歩かない タクシーでは荷物を出口側に置く • ケンジントンロックの利用
情報の盗難 • Web会議のURL不正利用 • 覗き見 • フリーWifiの利用	**情報の盗難** • Web会議の入室にパスワードを設ける • 覗き見防止フィルターを付ける • Windows Firewallを有効にする

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-2.】

テレワークのセキュリティ対策

【チェックリストの活用】

- テレワーク方式ごとのチェックシートが用意されている
- チェックシートは、2種類の優先度ごとに記載されている
  優先度：◎
  　セキュリティ対策の重要性が高いもののうち、実施難易度が低い（専門知識、追加コストの観点で懸念が小さい）もの
  優先度：○
  　セキュリティ対策の重要性が高いもののうち、実施難易度が中程度（ITセキュリティに関する知識を必要とするが、実施困難ではない）もの
- 具体的な設定内容については、設定一覧を活用する

重大インシデント事例から学ぶ課題解決 【参照：テキスト3-1-1.】

EPPとEDR、UTMについて

EPP（Endpoint Protection Platform）の役割

- マルウェアの**感染を防止**することに特化したソフトウェア製品
  →パターンマッチングや振る舞い解析による検知製品

EDR（Endpoint Detection and Response）の役割

- マルウェア**感染後の対応**を支援するソフトウェア製品
  →感染後、攻撃が始まる前に脅威を検知し、原因の削除や対処法を提供する。

UTM（Unified Threat Management）の役割

- 多くのセキュリティ機能を一元化させたハードウェア製品
  →ファイアウォール、IPS/IDS、アンチウイルスなどの機能が含まれる。

重大インシデント事例から学ぶ課題解決 【参照：テキスト2-2-4.】

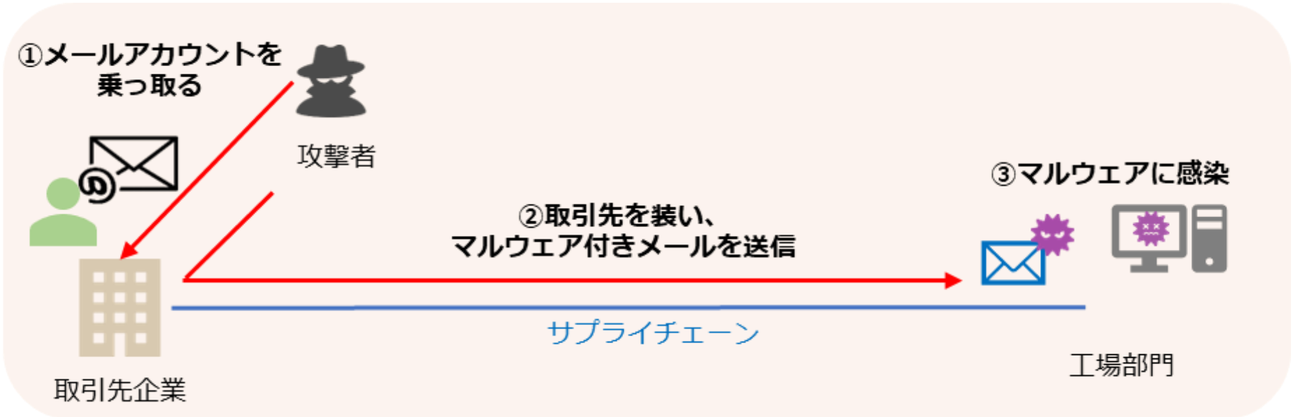
サプライチェーンを介した標的型メール攻撃

【事例概略】

- 取引先企業のメールアカウントが乗っ取られる。
- 攻撃者が取引先企業のふりをして、マルウェアが添付されたメールを送信してきた。
- 受信したPCのうち、2台がマルウェアに感染した。
- EPPでは検知できず、EDRによって早期検知ができ、感染拡大を食い止めた。

【問題点・課題】

- 攻撃者は正規アカウントを乗っ取っているため、不審な点を見つけにくい



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-3-2.】

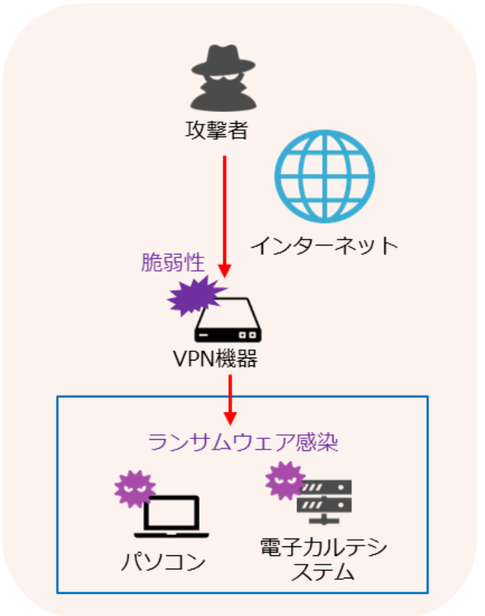
ランサムウェアによる電子カルテシステムの停止

【事例概略】

- リモートメンテナンス用のVPN機器の脆弱性が悪用され、不正アクセスされる。
- LockBit2.0が仕掛けられ、電子カルテ関連サーバが暗号化される。
- 事前に策定していたBCPを発動し、発生当初から災害級の扱いでインシデント対応にあたった。

【問題点・課題】

- VPN機器の脆弱性が放置されていた。
- 脆弱なパスワードが使用されており、簡単に特権アカウントでシステムに接続できた。
- ベンダー側のセキュリティ知識が不足していた。



重大インシデント事例から学ぶ課題解決 【参照：テキスト2-3-3.】

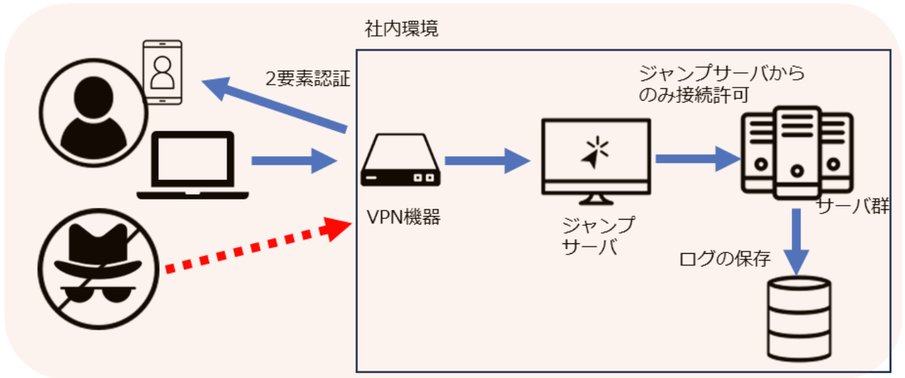
具体的な対策

【考え方】

- アクセス元の信頼性を重視し、すべてのアクセスを監視する。

【実施するべき技術的対策】

- VPN機器への接続に多要素認証を導入し、接続元の信頼性を上げる。
- 外部から中枢のサーバに対し、VPN経由での直接接続をさせない。
- サーバやPCの特権アカウントのパスワードを定期的に変更する。
- OSのファイアウォール機能を有効にし、接続元を限定する。
- サーバやネットワーク機器のログを取得し、定期的に確認する。
- 脆弱性情報を高い頻度で確認する。
- パッチマネジメントを実施する。
- EDRなどの製品を導入する。



重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【複雑さを持つパスワードの作り方】

1.単語ではなく、文章にする
単語の場合、ディクショナリ検索でヒットする確率が上がるため、
文章として考える

Cyber Security Keizoku Shien
↓
CyberSecurityKeizokuShien

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

2. 数字を入れる

CyberSecurityKeizokuShien**0725**

3.単語の母音を削除し、読めなくする（aiueo）

Cyb**e**rS**e**c**u**r**i**tyK**ei**z**o**k**u**Sh**ie**n0725

↓

CybrScrtyKzkShn0725

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

4. 特殊記号を数文字入れる
   #、%、@を単語の区切りに入れる

CybrScrtyKzkShn0725

↓

Cybr#Scrty%Kzk@Shn0725

ベースパスワード完成！

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

5. サービス識別文字を入れる

例

Amazon ： a6

FaceBook ： f8

a6Cybr#Scrty%Kzk@Shn0725

f6Cybr#Scrty%Kzk@Shn0725

重大インシデント事例から学ぶ課題解決

パスワードの使いまわしをしないために

【パスワードの作り方】

6. 自分にしかわからない固定文字を入れる

例　イニシャル
SH　→　$H

$Ha6Cybr#Scrty%Kzk@Shn0725
$Hf6Cybr#Scrty%Kzk@Shn0725

メモするときはベース部分のみをメモする
$Ha6**Cybr#Scrty%Kzk@Shn0725**

重大インシデント事例から学ぶ課題解決

認証方式と管理

- パスワードマネージャー（ソフトウェア）
  複雑なパスワードを生成し、管理するためのソフトウェア。
  端末間の同期を行うことで、複数のデバイスで共有できる。
- ワンタイムパスワード
  定期的に更新され、1度しか使用できないパスワード。
  パスワードは、専用のデバイスやソフトウェアで確認できる。
- PINコード方式
  パスワードとは異なり、デバイスに対する認証となるため、ネットワーク上を流れることがない。
- 公開鍵方式のパスキー
  公開鍵と秘密鍵の2種類の鍵のペアで認証を行う方式

3. サイバーセキュリティの基礎知識

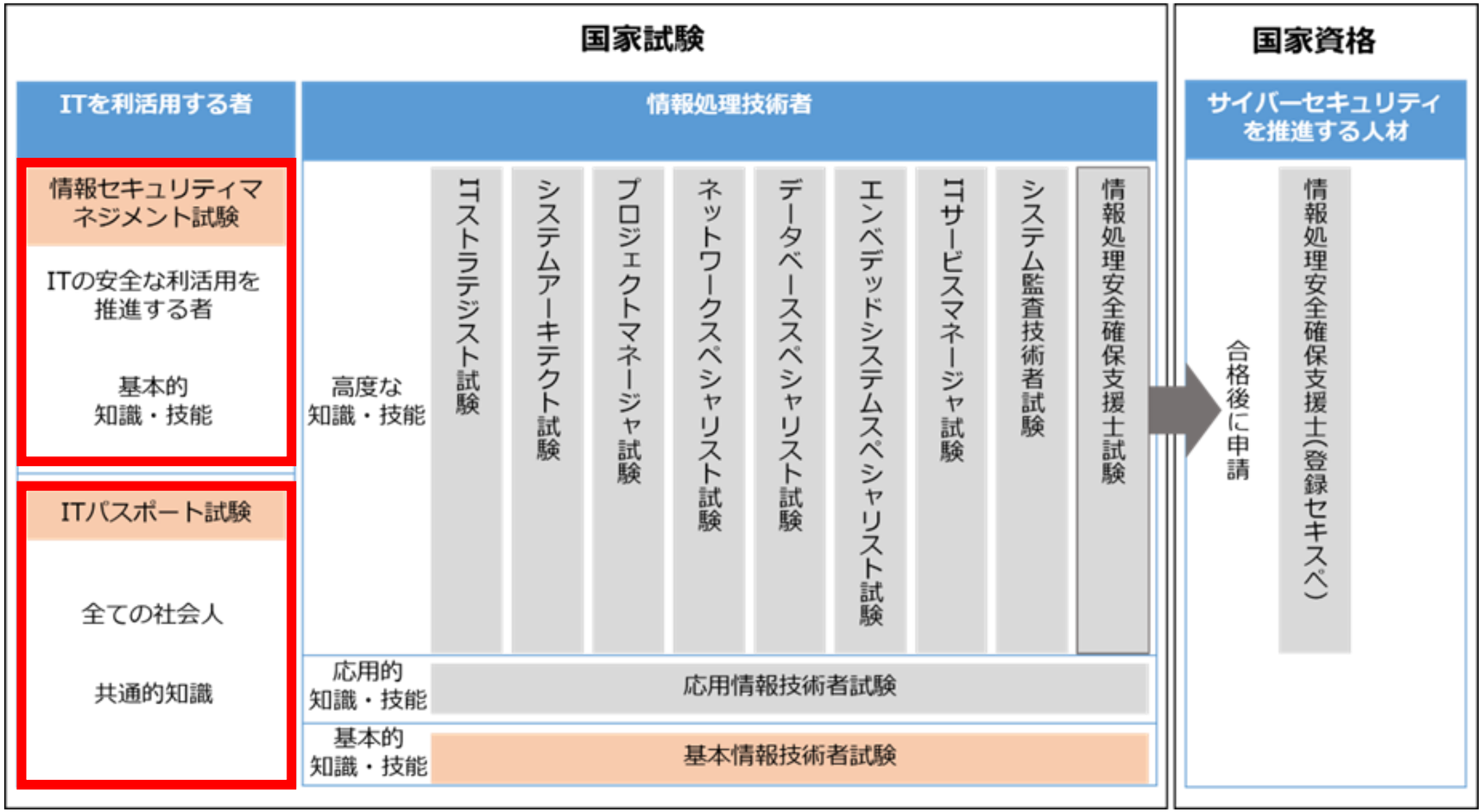
各種資格試験から得るサイバーセキュリティの基礎知識

Security Action（セキュリティ対策自己宣言）

サイバーセキュリティ対策基準レベル

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 【参照：テキスト3-2-1.】

社員に取得させたい資格



IPA.”試験区分一覧”を基に作成. https://www.ipa.go.jp/shiken/kubun/list.html (参照 2023-07-06).

Security Action 宣言　二つ星レベル 【参照：テキスト3-3-1.】

レベルごとの宣言内容

レベル	宣言内容
★ 1つ星	次の情報セキュリティ5か条に取り組むことを宣言する 1. OSやソフトウェアは常に最新の状態にしよう！ 2. ウイルス対策ソフトウェアを導入しよう！ 3. パスワードを強化しよう！ 4. 共有設定を見直そう！ 5. 脅威や攻撃の手口を知ろう！
★★ 2つ星	• 5分でできる！情報セキュリティ自社診断で自社のセキュリティ対応状況を把握する • 情報セキュリティ方針を策定する （理念、指針、原則、目標等を表した「方針書」「宣言書」等を指す）

セキュリティ対策自己宣言

IPA. ”SECURITY ACTION セキュリティ対策自己宣言”. https://www.ipa.go.jp/security/security-action , (参照 2023-07-06).

サイバーセキュリティ対策基準レベル 【参照：テキスト3-4-1.】

対策基準レベルの概要

レベル	概要
Lv.1 クイック アプローチ	緊急に、狙われやすい大きな穴（セキュリティホール）を塞ぐ
Lv.2 ベースライン アプローチ	素早く多くの穴を塞ぐ
Lv.3 網羅的 アプローチ	じっくりと、小さな穴を残さないように確実に塞ぐ

サイバーセキュリティ対策基準レベル 【参照：テキスト3-4-1.】

Lv.1 クイックアプローチ

項目	説明
内容	様々なインシデント事案の対応内容を参考として、「リスクが大きい（発生頻度が高い、被害が大きい）」と思われる事例から、重要な対策を実施していく。 何から実施していいかわからない。という組織は、まずはここから。
参考資料	• 徳島県つるぎ町立半田病院 コンピュータウイルス感染事案有識者会議調査報告書について • 大阪急性・総合医療センター 情報セキュリティインシデント調査委員会報告書について • 【IPA】情報セキュリティ10大脅威2023 • 【NISC】サイバー攻撃を受けた組織における対応事例集（事実例における学びと気づきに関する調査研究） など

サイバーセキュリティ対策基準レベル 【参照：テキスト3-4-1.】

Lv.2 ベースラインアプローチ

項目	説明
内容	セキュリティ対策の基準やガイドラインを定義することにより、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。ただし、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し、網羅的なアプローチを推進することが必要となる。 • セキュリティの基準となるベースラインを定義し、組織全体で一貫性を確保 • 網羅的なアプローチの出発点
参考資料	• 【IPA】中小企業の情報セキュリティ対策ガイドライン第3版 • 情報セキュリティハンドブック（ひな形） • 中小企業のためのクラウドサービス安全利用の手引書 • 情報セキュリティ関連規程（サンプル）

サイバーセキュリティ対策基準レベル 【参照：テキスト3-4-1.】

Lv.3 網羅的アプローチ

項目	説明
内容	可能な限り多くの脅威や攻撃手法に対して対策を講じることを目指すアプローチとなる。ただし、全体的な実施には時間がかかるため、即時性を重視するアプローチではない。 • 可能な限り多くの脅威や攻撃手法に対して対策を講じる • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持する
フレームワーク	ISMS CIS Controls など

１． 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

これからの企業経営で必要な観点：社会の動向

守りのIT投資と攻めのIT投資

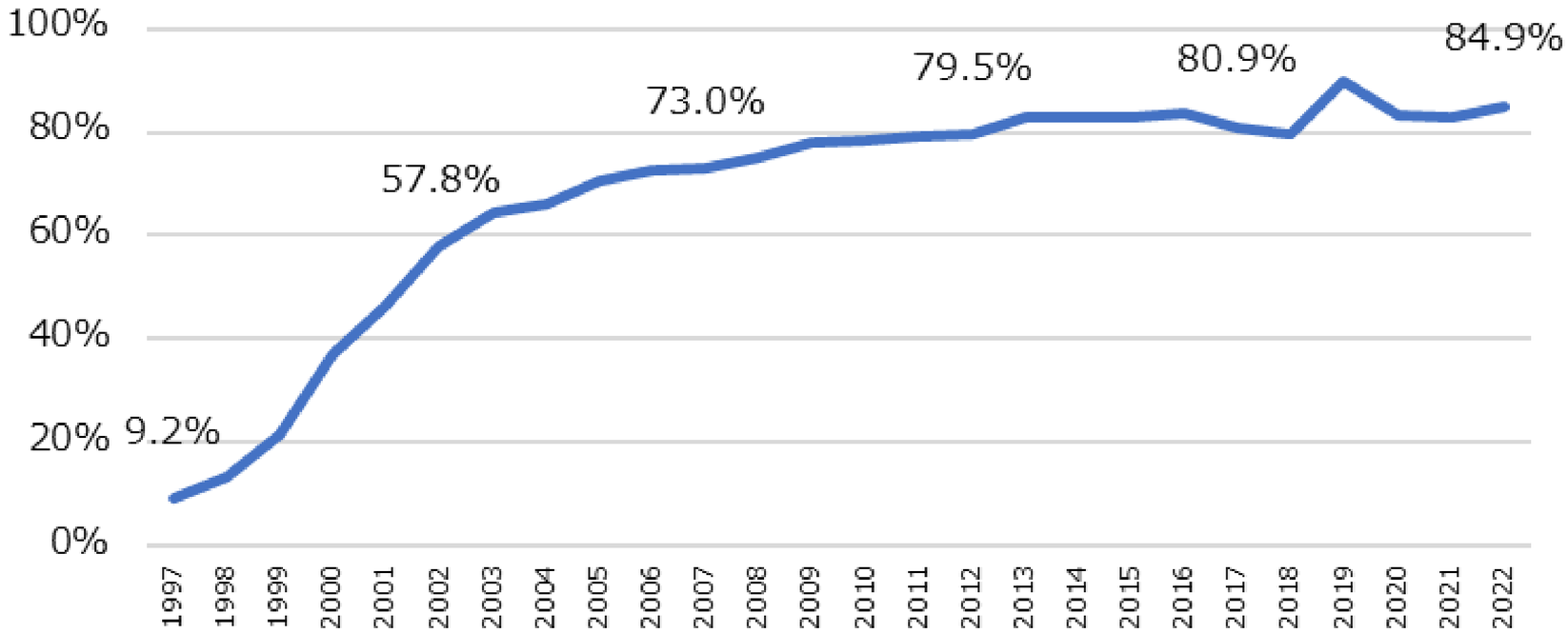
経営投資としてのサイバーセキュリティ対策

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-1.】

インターネットの利用率

インターネットの普及とともに、現実社会とサイバー空間が密接に結びつき、私たちの生活やビジネスに大きな変革をもたらしている。



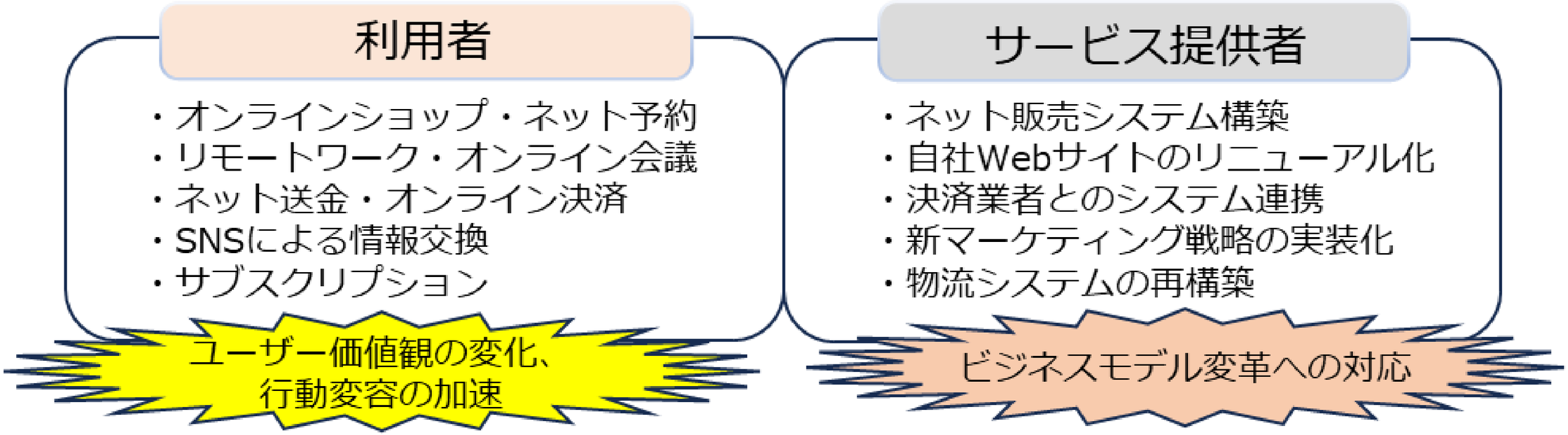
インターネット利用率（個人）の推移
（出典） 総務省「通信利用動向調査」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-1.】

デジタル時代の競争：革新と選択肢の拡大

インターネットの普及とともに、利用者はより価値あるサービスを選択することが可能になった。
ITサービス提供者は、常に最新のサービス提供が求められるため、革新的なアイディアと素早い行動が求められる。

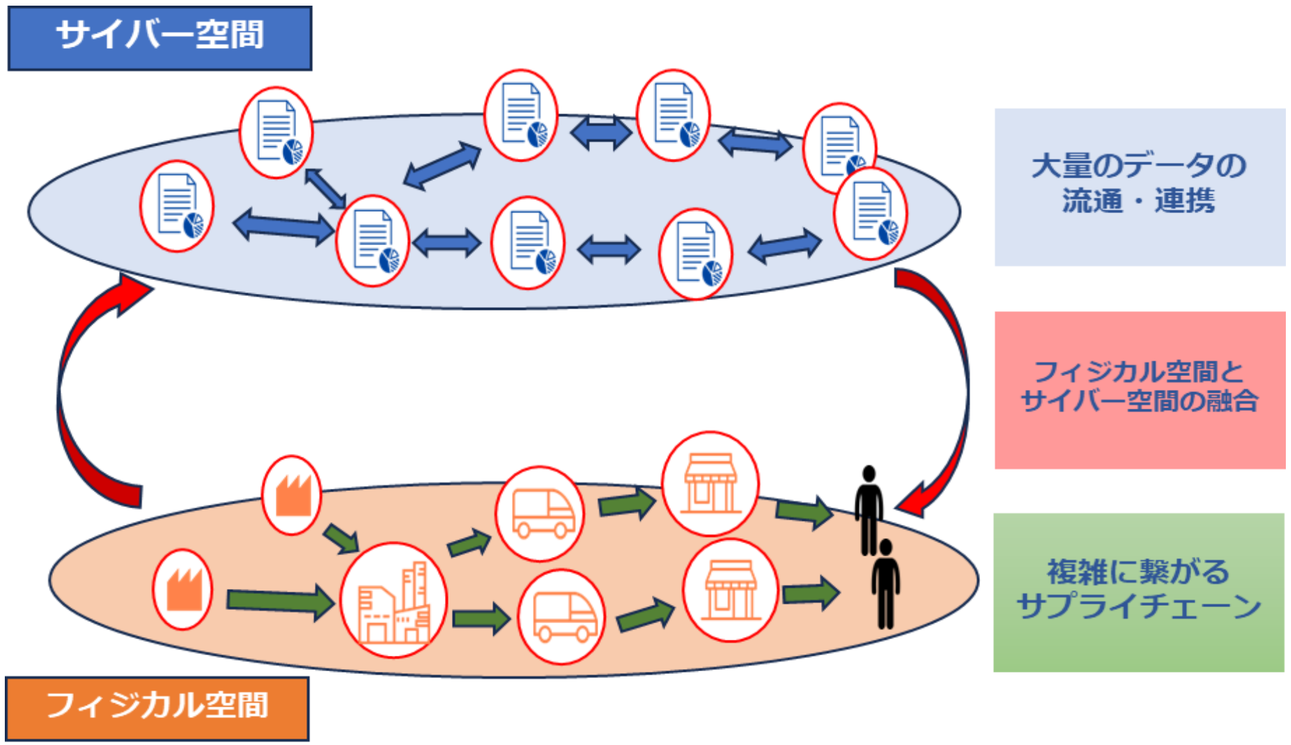


これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-1.】

フィジカル空間とサイバー空間の融合

Society5.0で実現する社会では、サプライチェーンにIoTやAIが導入され、製造や物流がサイバー空間で監視・制御されるようになる。また、クラウドの普及に伴い情報共有が容易になることで、**サプライチェーンが可視化**され、フィジカルとサイバー空間が密接に融合する。



サイバー空間とフィジカル空間の関係図
（出典） 経済産業省「サイバー・フィジカル・セキュリティ対策フレームワークVer.1.0」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

日本のデジタル化は後れている！！

後れをとった6つの理由

1. ICT投資の低迷
2. 業務改革などを伴わないICT投資
3. ICT人材不足・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

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

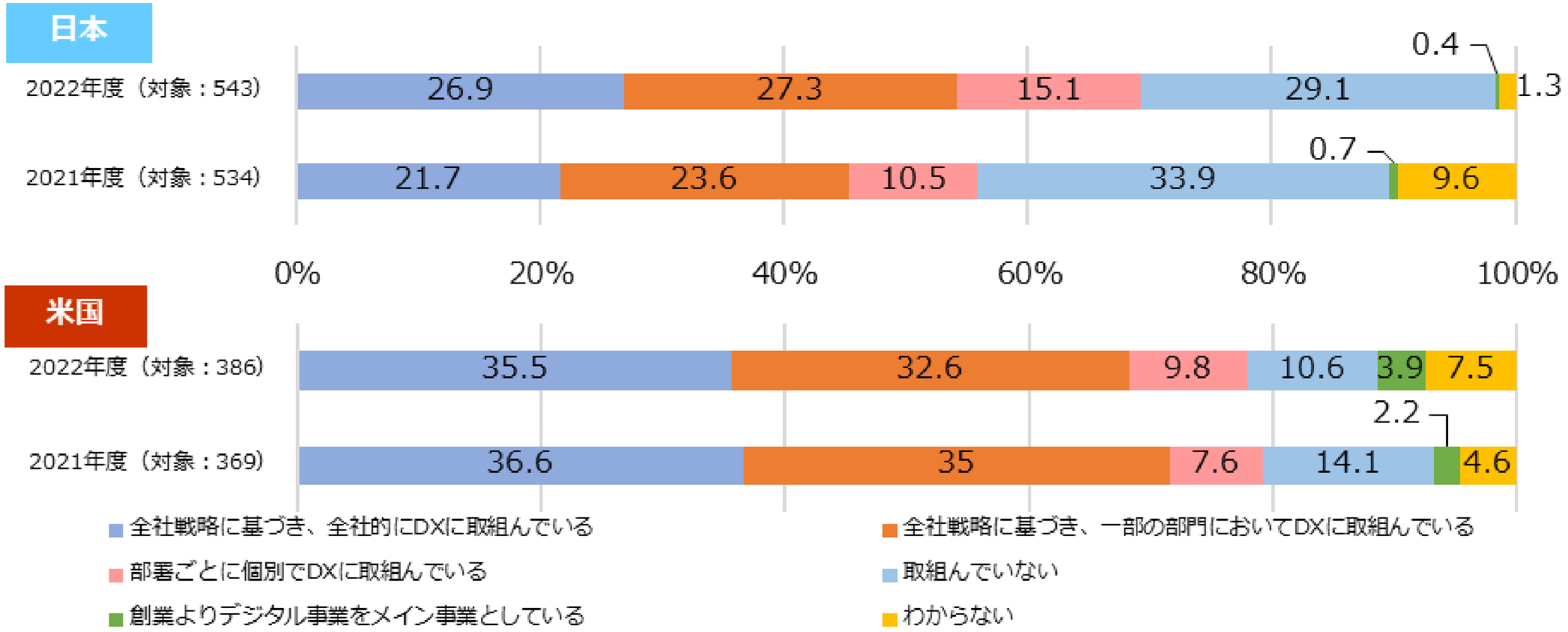
1. ICT投資の低迷

- 我が国のICT投資は1997年をピークに減少中。
- ICT投資の8割は現行ビジネス維持・運営に使われ、レガシーシステムが多い。
- 現代の変化に適応するアジャイル開発が推奨されるが、ウォーターフォール型が主流でアジャイル導入が遅れている。
- オープン化、クラウド化、業務・データ標準化の対応が遅れ、業務効率化・データ活用が不十分。

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

DXの取組状況

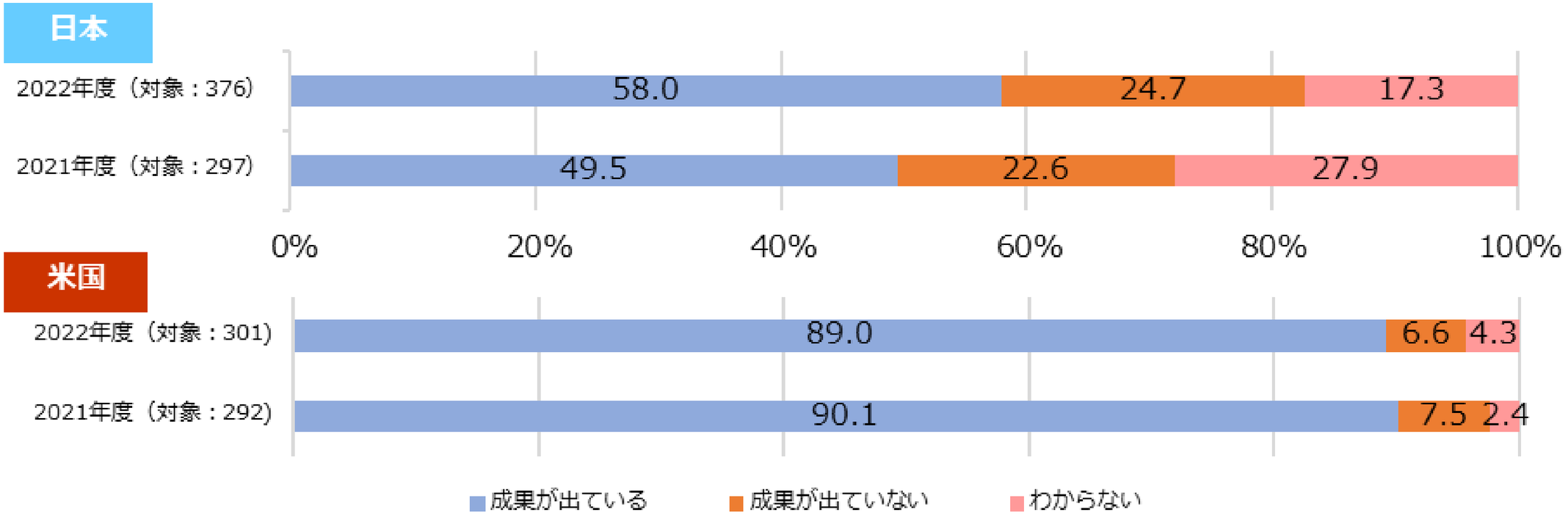


DXの取組状況
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

DXの取組の成果



DXの取組の成果
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

2. 業務改革などを伴わないICT投資

- 我が国のICT導入は、主に業務の効率化の手段として使用される。
- 情報システム開発はコア業務とは見なされず、外部企業への依存が高まっている。
- この外部委託の依存により、ノウハウやスキルの蓄積が委託元企業で不足。
- 業務改革を伴わないICT導入が多く、十分な効果が発揮されず、デジタル化への更なる投資が後れている。
- ICT投資の効果を最大化するには業務改革や組織の改編が必要。

これからの企業経営で必要な観点：社会の動向

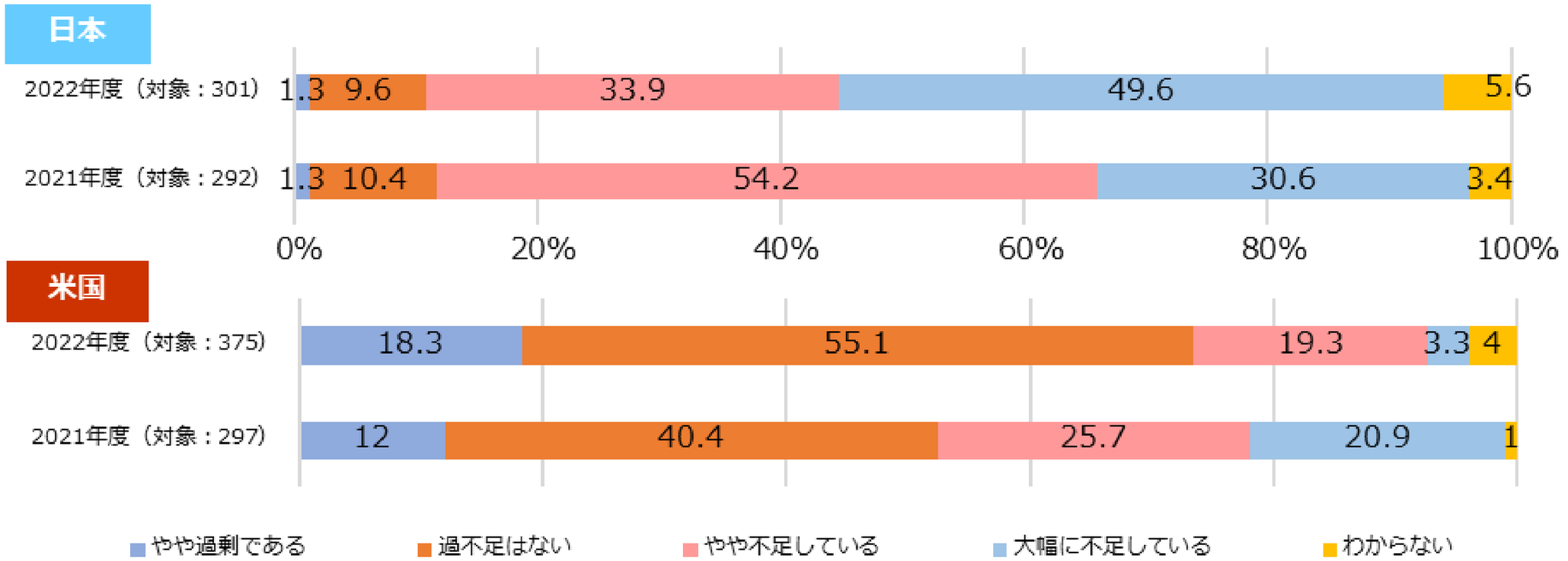
【参照：テキスト4-1-2.】

3. ICT人材不足・偏在

- ICT人材はデジタル化の推進に不可欠。
- IPAの2022年度調査：IT人材の量について、83.5%が「大幅に不足」または「やや不足」と回答。
- 時代に応じて変わるICT人材の要件：情報セキュリティやアジャイル開発などの高度なスキルが求められる。
- IT人材の質に関しても、86.1%が「大幅に不足」または「やや不足」と回答。
- 我が国のユーザー企業は、ICT人材の量・質ともに不足していると認識。
- 我が国では外部ベンダーへの依存度が高く、ユーザー企業内でのICT人材の育成・確保が不十分。

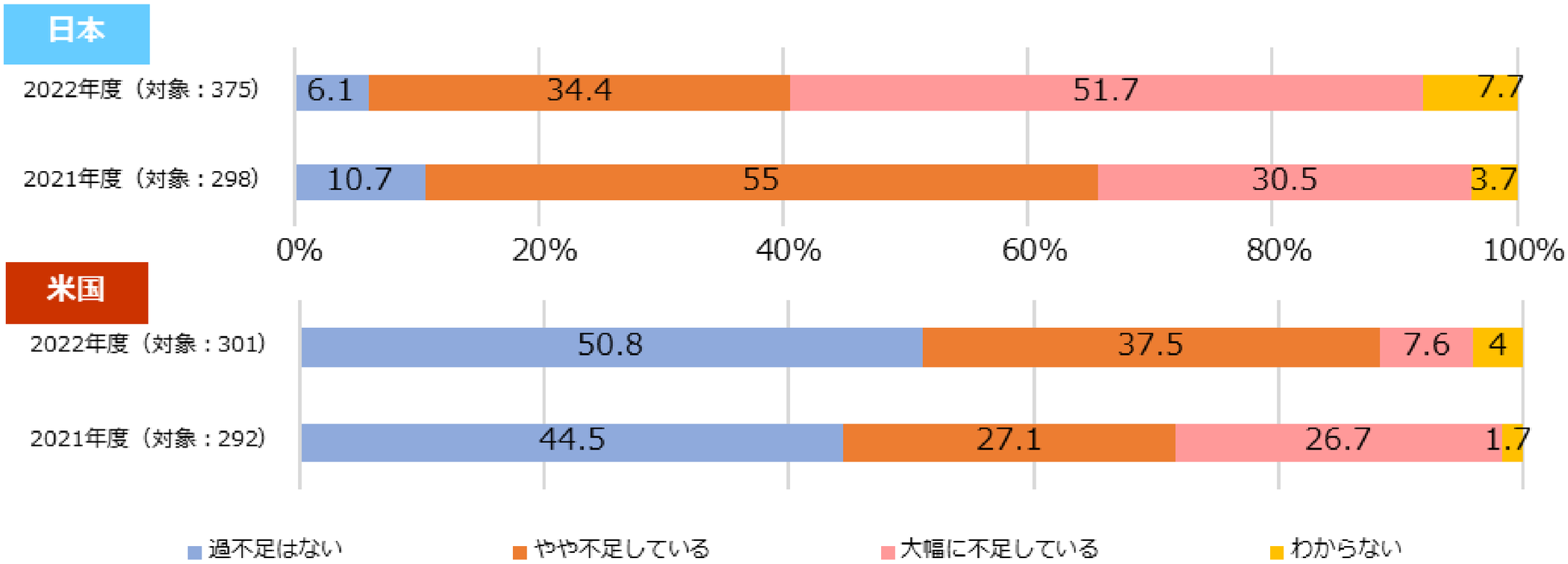
これからの企業経営で必要な観点：社会の動向

DXを推進する人材の「量」の確保



DXを推進する人材の「量」の確保
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向
DXを推進する人材の「質」の確保



DXを推進する人材の「質」の確保
（出典） IPA「DX白書2023」を基に作成

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

4. 過去の成功体験

- 我が国は高度経済成長期後、世界の経済大国となり、「電子立国」と称された。
- 2000年代に、ICT関連製造業の生産・輸出が減少。
- 以前の成功に固執し、デジタル化への適応が不十分。
- 国民生活・社会活動は維持できており、デジタル化の緊急性を感じていない。
- 技術での解決を、人材の質・量で補っている。
- デジタル化による生産性向上の余地があるが、「ゆでガエル現象」の可能性。
- 新興国では、制約の少ないデジタル環境で「リープフロッグ」が起きている。

これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

5. デジタル化への不安感・抵抗感

- デジタル化に対する不安感・抵抗感を持つ人が存在する。
- デジタル化により、情報セキュリティなどの新しい脅威が出現。
- 総務省調査：デジタル化が進んでいない主な理由は「情報セキュリティやプライバシー漏洩への不安」（52.2%）。
- パーソナルデータの不適切な利用、ネット上の偽情報、デジタル操作への不慣れなどが不安感・抵抗感の要因。

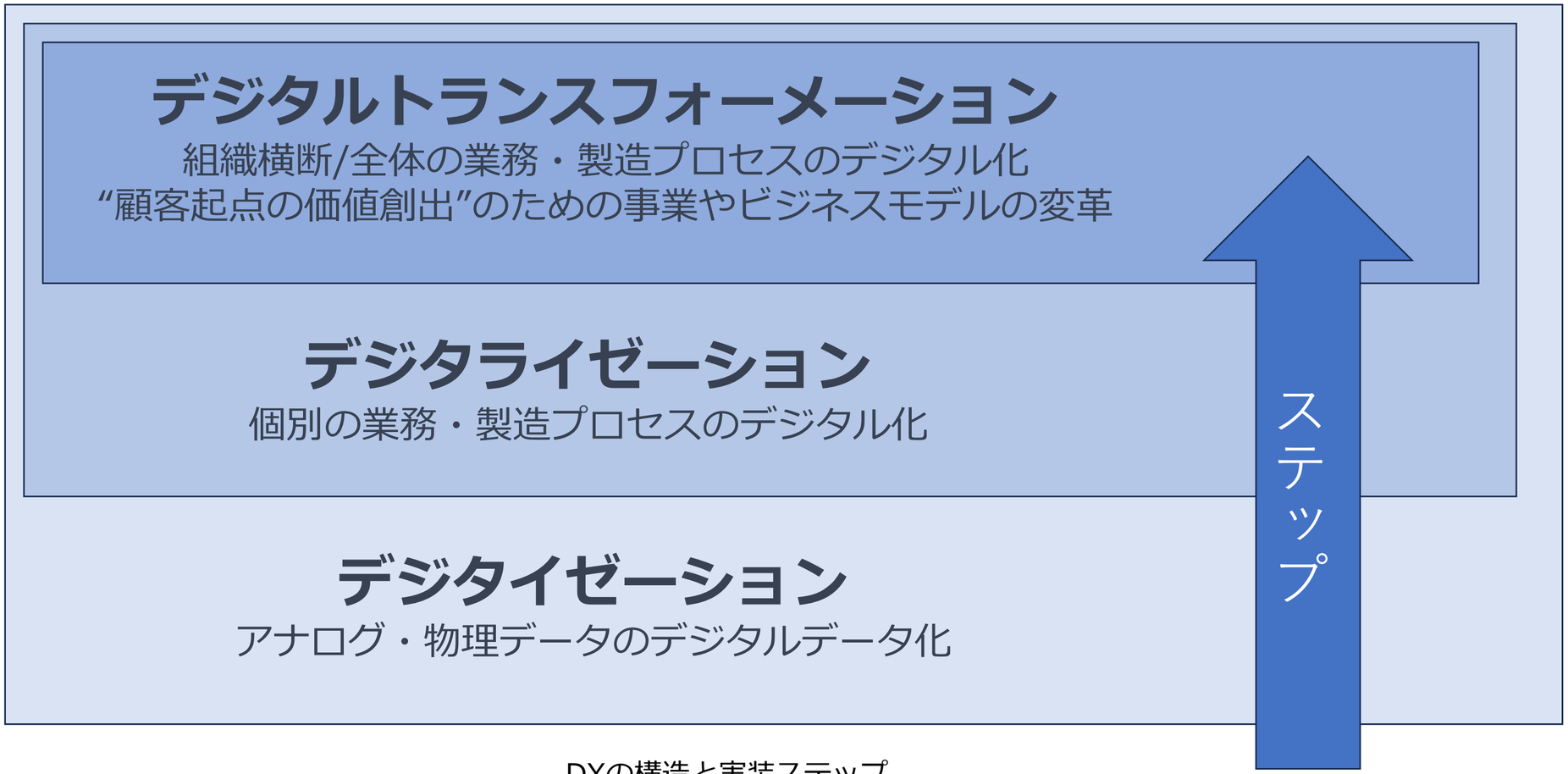
これからの企業経営で必要な観点：社会の動向

【参照：テキスト4-1-2.】

6. デジタルリテラシーが十分ではない

- 情報セキュリティや偽情報対応には情報リテラシーが必要。
- 総務省の調査: デジタル化未進の理由の2番目は「利用者のリテラシー不足」(44.2%)。
  ※1番目は前述の「情報セキュリティやプライバシー漏洩への不安」（52.2%）。
- デジタルリテラシー不足は、デジタル化推進への消極的態度の原因となる可能性。

守りのIT投資、攻めのIT投資
DXの構造と実装STEPを理解する



DXの構造と実装ステップ
（出典） 経済産業省「DXレポート2」を基に作成

守りのIT投資、攻めのIT投資

DXフレームワーク

	未着手	デジタイゼーション	デジタライゼーション	デジタルトランスフォーメーション
ビジネスモデルのデジタル化				ビジネスモデルのデジタル化
製品／サービスのデジタル化	非デジタル製品/サービス	デジタル製品	製品へのデジタルサービス付加	製品を基礎とするデジタルサービス デジタルサービス
業務のデジタル化	紙ベース・人手作業	業務/製造プロセスの電子化	業務/製造プロセスのデジタル化	顧客とのE2Eでのデジタル化
プラットフォームのデジタル化	システムなし	従来型ITプラットフォームの整備		デジタルプラットフォームの整備
DXを進める体制の整備	ジョブ型人事制度 リカレント教育	CIO/CDXOの強化 リモートワーク環境整備	内製化	

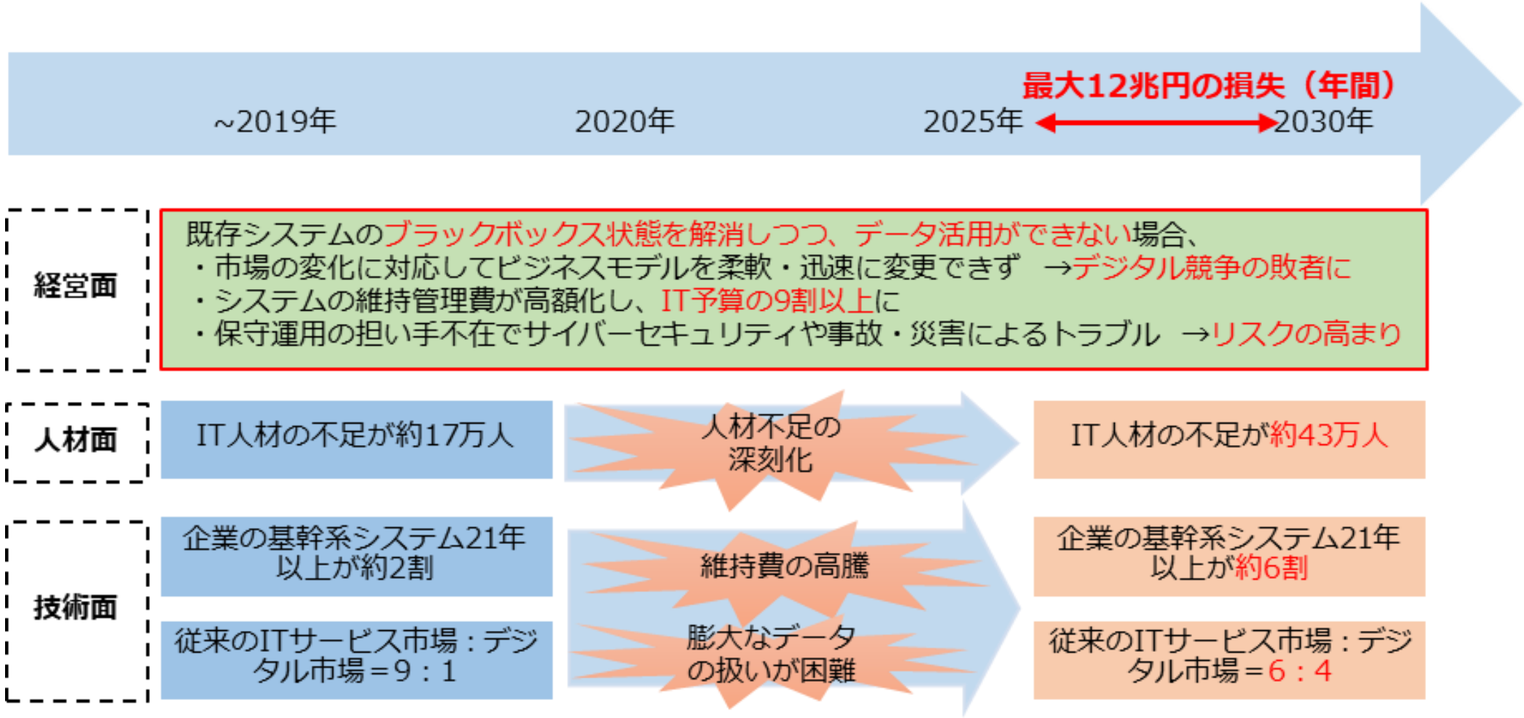
DXフレームワーク
（出典） 経済産業省「DXレポート2」を基に作成

2025年の崖

【参照：テキスト4-2-2.】

2025年の崖が示す課題

項番	課題
課題1	既存システムのレガシーシステム化
課題2	IT人材不足の深刻化
課題3	システム維持費の高騰
課題4	サイバーセキュリティや災害リスクの高まり
課題5	各種システムのサポート終了



「2025年の崖」の概要図
（出典）経済産業省「DXレポート ～ITシステム「2025年の崖」の克服とDXの本格的な展開～」を基に作成

2025年の崖

【参照：テキスト4-2-2.】

2025年の崖の解決策

項番	課題
解決策1	DX推進システムガイドラインの策定
解決策2	「見える化」指標、診断スキームの構築
解決策3	ITシステムの刷新
解決策4	DX人材の育成・確保
解決策5	ユーザー企業・ベンダー企業との新しい関係性構築

守りのIT投資、攻めのIT投資

【参照：テキスト4-2-1.】

守りのIT投資（デジタルオプティマイゼーション）

- ITによる業務効率化
- コスト削減

攻めのIT投資（デジタルトランスフォーメーション）

- 新しい事業展開
- 新しいビジネスモデル創出

守りのIT投資、攻めのIT投資

【参照：テキスト4-2-3.】

守りのIT投資

【投資目的】

- 業務効率化・コスト削減
- デジタル活用するための環境整備

【進め方】

1. 業務内容・業務フローの可視化
2. 削減・短縮可能な業務の洗い出し
3. 改善や対応の実施
4. 業務改革の実現

守りのIT投資、攻めのIT投資

【参照：テキスト4-2-3.】

守りのIT投資事例

課題

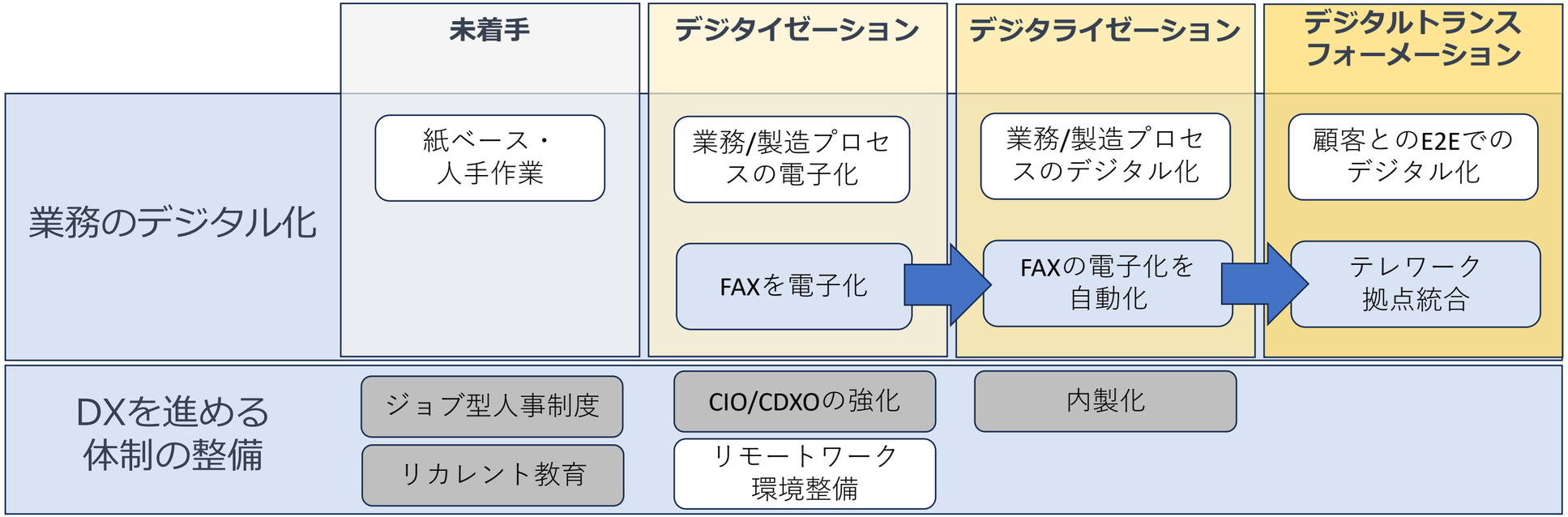
- 新型コロナウイルス対応のため、テレワークへの切り替え
- 書類処理のための出社

【進め方】

手順１：業務内容・業務フローの可視化
問題となる業務は、「お客様や仕入れ先様からFAXで届いた見積書や注文書に対して、紙で返信する業務」であることが判明
手順２：削減・短縮可能な業務の洗い出し
紙ベースの書類を電子データに切り替えることで、出社する手間を削減
手順３：改善や対応の実施
RPAを導入し、FAXデータをPDFファイルに自動変更しサーバに保存
手順４：業務改革の実現
出社回数が激減し、完全テレワークが実現

守りのIT投資、攻めのIT投資

守りのIT投資事例とフレームワーク



守りのIT投資、攻めのIT投資

【参照：テキスト4-2-4.】

攻めのIT投資

【投資目的】

- ビジネス環境の急激な変化に対応するため
- 多様化する顧客のニーズに応えるため

【進め方】

1. 経営ビジョン・戦略の策定
2. 変革の準備・課題の抽出
3. デジタル技術・業務改革による課題の解決
4. 顧客に新たな価値を提供・他社のDXに貢献

守りのIT投資、攻めのIT投資

【参照：テキスト4-2-4.】

攻めのIT投資事例

課題

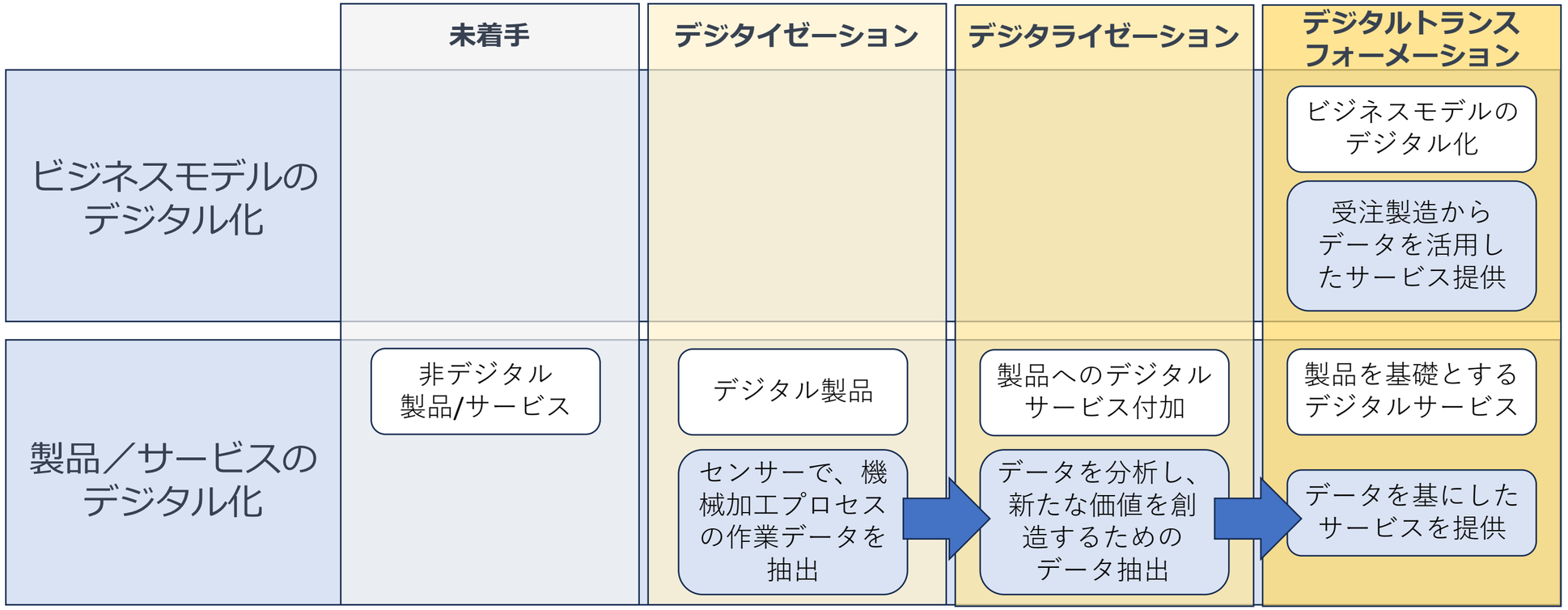
- 従来の機械加工ではビジネスの継続が困難

【進め方】

手順１：実現したいことを明確にする
ビジネスモデルを、自らサービス提供していくモデルへ転換することに設定した。
手順２：課題の明確化、関係者の意識改革を実施する
機械加工による製品の開発や販売だけでなく、自ら市場を開拓できるような新たな価値の創出を課題として挙げた。
手順３：デジタル技術による、課題解決
機械加工を行う機器にデータを計測するセンサーをつけ、加工データをリアルタイムで計測してデータを抽出し分析して得た情報をもとに、新規事業の展開に繋げた。
手順４：顧客に新たな価値を提供・ビジネスモデルの転換
機械加工の現場における生産性の向上や品質の改善、人材の育成などの課題を解決するサービスを提供できるようになり、受注だけに頼らないビジネスモデルを構築できた。

守りのIT投資、攻めのIT投資

攻めのIT投資事例とフレームワーク



次世代技術を活用したビジネス展開

【参照：テキスト4-2-5.】

活用する技術

技術	概要	活用方法例
AI	膨大な情報を処理し、判断や予測を行うことができる。	• 需要の予測や在庫の最適化 • 不良品の自動検出 • 対話型AIによる、問い合わせ対応の自動化 • コンテンツの生成
IoT	現実世界の様々なモノが、インターネットと繋がる。収集したデータが、インターネットに送信・蓄積され、データを分析・活用することで、新たな価値の創出に繋がる。	• 生産設備にセンサーを設置し、振動データを取得し分析することで、部品の故障予知や性能維持が可能 • 生産設備の稼働状況を可視化したことで、全ての拠点での生産状況をリアルタイムに把握可能
クラウドサービス	自社で機器やシステムを保有しなくても、インターネット経由で様々なサービスを利用できる	• 社内情報の一元管理 • システムを開発・実行するためのツールや環境構築作業の省略 • 場所やデバイスに依存せずに作業の継続が可能

次世代技術を活用したビジネス展開

【参照：テキスト4-2-5.】

次世代技術の活用事例 1

【課題】
- システム開発において、仕様変更が多すぎる。
- 適切な情報共有ができない。

【解決への取り組み】
- 情報共有のための社内SNSを利用。
- クラウドサービス（Iaas）を導入し、システム構築を簡略化。

【結果】
- システムを短期間で開発可能となる。
- 修正を即座に反映できるようになる。
- 情報の共有、工程管理の効率化を実現。

【＋α】
- 地域の製造業者に共有することで、効率化のコンサルティング、開発依頼の受注。

想定すべきセキュリティリスク
- 社内SNSへの攻撃による情報漏洩・サービス停止
- 個人用スマホからの情報漏洩
- 社用PC以外のPCからの利用による情報漏洩
- クラウド（Iaas）環境への攻撃による情報漏洩・サービス停止
- データ連携時の情報漏洩

次世代技術を活用したビジネス展開

次世代技術の活用事例１（リスク対策）

項番	想定すべきセキュリティリスク	一般的なリスク対策
1	社内SNSへの攻撃による 情報漏洩・サービス停止	• Web Application Firewall（WAF）サービスの導入 • 多要素認証の導入（利用者の特定） • 定期的なアカウント棚卸 • データの暗号化
2	個人用スマホからの情報漏洩	• 会社用スマホの支給＋Mobile Device Management（MDM） • Mobile Application Management（MAM）サービスの導入
3	社用PC以外のPCからの 情報漏洩	• テレワーク用持ち出しPCの支給 • 外部リモートデスクトップ接続用、社内端末の設置 • 社内SNSサービスの接続元IP固定化＋VPN接続
4	クラウド環境への攻撃による 情報漏洩・サービス停止	• 管理画面のログインに多要素認証の導入 • ファイアウォールの適切な設定 • 仮想サーバへのSSH、RDPの接続元IP固定 • 社内とクラウド環境の拠点間VPN
5	データ連携時の情報漏洩	• 社内とクラウド環境の拠点間VPN（経路の暗号化） • データの暗号化

次世代技術を活用したビジネス展開

【参照：テキスト4-2-5.】

次世代技術の活用事例２

【課題】

- 「つくる力」と「とどける力」を強化するため、管理面を強化する。

【解決への取組み】

- 農家における栽培環境の点検作業にIoTを導入し、自動化することを決定。
- IoT導入のために、電子機械に詳しい人材の確保。
- IoT活用方法を検証し、マニュアル作りを実施。

【結果】

- 栽培環境における点検作業の自動化に成功。
- 勘と経験に頼らない栽培作業の平準化に成功。

【＋α】

- 計測データをAI分析することで、最適な栽培条件の絞り込みができるようになる。
- 品質向上、作業の平準化、生産量の拡大が期待できるようになる。

想定すべきセキュリティリスク

- IoT機器への攻撃による情報漏洩・機器停止・データ改ざん
- Wifiアクセスポイントへの攻撃による機能停止
- 制御システムへの攻撃による情報漏洩・サービス停止
- IoT機器から制御システムへのデータ連携時の情報漏洩

次世代技術を活用したビジネス展開

次世代技術の活用事例2（リスク対策）

項番	想定すべきセキュリティリスク	一般的なリスク対策
1	IoT機器への攻撃による情報漏洩・機器停止・データ改ざん	• ファイアウォールの適切な設定 • 接続アカウントとパスワードの適切な設定 • ファームウェアのアップデート運用
2	Wifiアクセスポイントへの攻撃による機能停止	• SSIDをデフォルトから変更 • パスフレーズの適切な設定 • WPA2以上の暗号化強度を使用 • ファームウェアのアップデート運用
3	制御システムへの攻撃による情報漏洩・サービス停止	• WAFの導入 • ファイアウォールの適切な設定 • 管理画面のログインに多要素認証の導入 • データの暗号化
4	IoT機器から制御システムへのデータ連携時の情報漏洩	• データ転送経路の暗号化（SSLなど） • データの暗号化

次世代技術を活用したビジネス展開

【参照：テキスト4-2-5.】

チャットボットとは

- 自動会話プログラム
- 事前に設定したルール、選択肢などに基づいて利用者と文字形式でコミュニケーションをとることができる

【利用シーン】

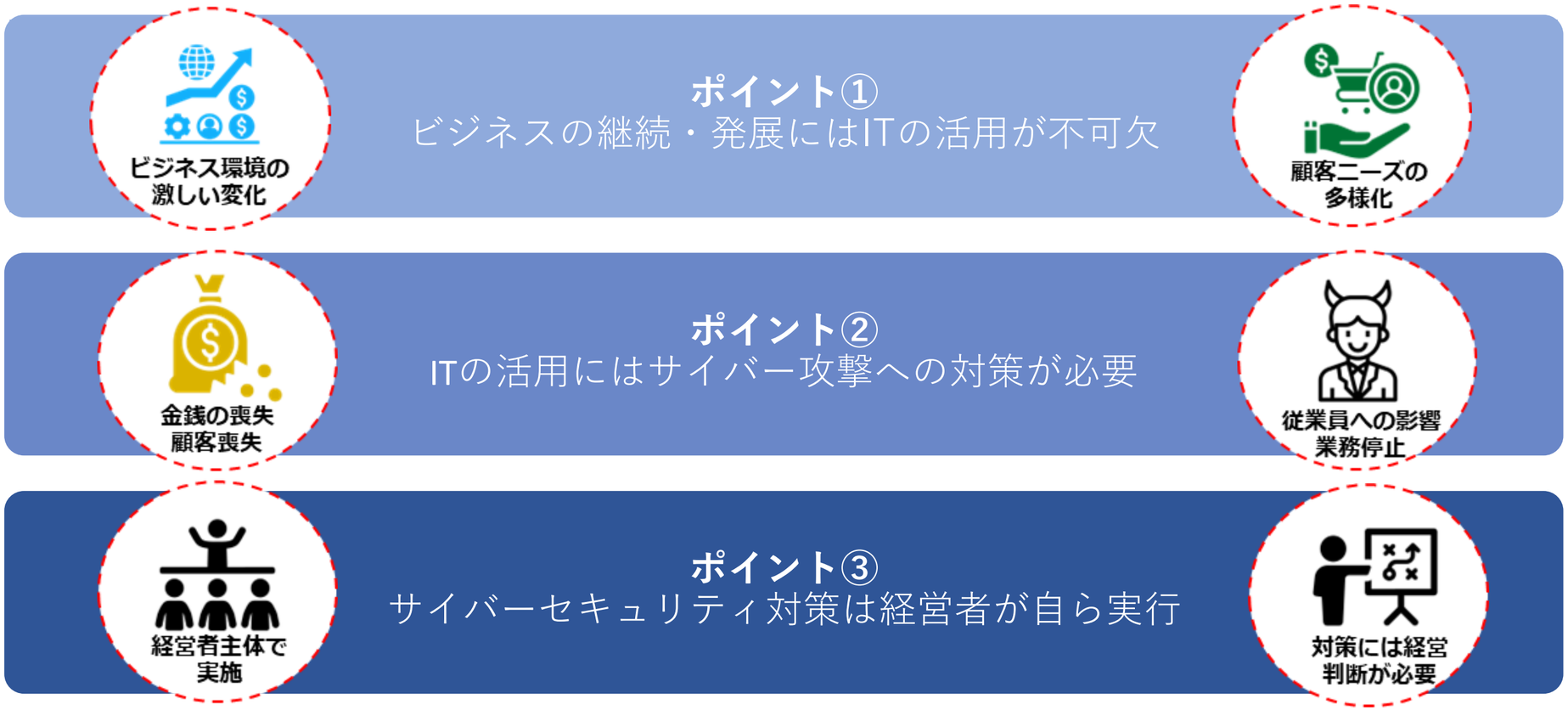
- サポートサイトのFAQ
- 社内SNSの自動応答

【今後の発展】

- チャットボットのAI連携

サイバーセキュリティ対策の重要性
経営者が重要視すべき3つのポイント

【参照：テキスト4-3-1.】



ITの活用とサイバーセキュリティ対策の関係性
（出典） 東京都産業労働局 「MISSION 3-1 サイバーセキュリティ対策が経営に与える重大な影響」

経営者が重要視すべき3つのポイント

【参照：テキスト4-3-2.】

ポイント１：ビジネスの継続・発展にはITの活用が不可欠

【中小企業の重要課題】

- 業務の効率化
- 生産性の効率化
- 人材確保
- DX化

【課題解決のアプローチ】

- 運用コストの削減・効率化のために、デジタルオプティマイゼーション
- 競争力維持・強化のために、デジタルトランスフォーメーション

経営者が重要視すべき3つのポイント

【参照：テキスト4-3-2.】

ポイント２：ITの活用にはサイバー攻撃への対策が必要

DX推進のためにはIT活用は必須

⇩

IT活用のためにはインターネットの活用は必須

⇩

インターネットの活用にはサイバーセキュリティ対策は**最優先事項！**

守りや攻めのIT投資によってDXを推進しても、たった1度のサイバー攻撃による被害で、すべてを失います。

経営者が重要視すべき3つのポイント

【参照：テキスト4-3-2.】

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

【その理由】

- 経営者による経営判断が必要
  - サイバー攻撃のリスクの許容範囲をどの程度にするのか
  - セキュリティ投資をどこまで行うのか
- セキュリティインシデントが発生した際に、経営者が責任を負う

法令	条項	要約
民法	415条 債務不履行による損害賠償責任	サイバー攻撃により仕事が停滞した場合、 会社および第三者に対する、契約違反による賠償義務を負う。
	644条 取締役の善管注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対して、善管注意義務違反による賠償義務を負う。
会社法	330条 取締役の善管注意義務違反 423条 1項 任務懈怠による損害賠償責任 429条 1項 第三者に対する注意義務違反	企業のセキュリティ体制が規模や業務内容に鑑みて適切でなく、サイバー攻撃により企業や第三者に損害が発生した場合、取締役は会社に対する、善管注意義務違反による任務懈怠（けたい）に基づく損害賠償義務を負う。

情報セキュリティ対策が不備の場合に責任追及の根拠とされる主な法律
（出典） IPA 「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」から抜粋

１．デジタル社会の方向性と実現に向けた国の方針

国の基本方針および実施計画の要約

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

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

経済財政運営と改革の基本方針

- 国の基本的な政策方針を示すもので、通称「骨太の方針」と呼ばれる
- 官邸主導での改革を目的とし、内閣総理大臣が議長を務める経済財政諮問会議で毎年策定される
- ITとセキュリティ関連の施策もこの方針に基づいて計画される
- 2023年の方針では、「デジタル」が50回以上使用され、デジタル技術の活用とデジタル社会構築が協調される

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

新しい資本主義の取組み

- 官民連携による国内投資拡大と**サプライチェーンの強靭化**
- グリーントランスフォーメーション（GX）、デジタルトランスフォーメーション（DX）などの加速
- スタートアップの推進と新たな産業構造への転換、インパクト投資の促進
- 官民連携を通じた化学技術・イノベーションの推進
- インバウンド戦略の展開

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

官民連携による国内投資拡大とサプライチェーンの強靭化

1. 新しい資本主義の下の変化
2. 挑戦と方針
3. 日本経済の再生のための方針
4. 投資拡大の方策
5. 雇用と人材の課題への対応
6. 強靭な経済構造の構築
7. 国際協力と投資拡大の推進

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

GX、DXなどの加速

GXの加速

1. 日本の脱炭素政策
2. エネルギー政策の推進
3. 環境友好的な輸出と生活の推進

DXの加速

1. デジタル行政の実現
2. 市場環境の整備
3. 先進技術と国際連携

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

スタートアップの推進と新たな産業構造への転換、インパクト投資の促進

スタートアップの促進と新たな産業構造への展開

1. 参入と再チャレンジの際の障壁を低くする
2. 「スタートアップ育成5か年計画」を通じて、参入・退出の円滑化

インパクト投資の促進

1. インパクトスタートアップへの支援を強化
2. 社会的起業家の認証制度の設立

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

官民連携を通じた科学技術・イノベーションの推進

1. 科学技術・イノベーションの推進
2. 高等教育と研究の強化
3. 教育の国際化と人材の育成

経済財政運営と改革の基本方針2023

【参照：テキスト5-1-1.】

インバウンド戦略の展開

1. 持続可能な形での観光立国の復活
2. 高度人材の受入れ
3. 技能実習制度および特定技能制度の在り方の検討
4. 資産運用立国・国際金融センター等の実現

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

重点計画とは

1. データの重要性増大
2. デジタル社会実現の必要性
3. 重点計画の策定
4. 計画の役割
5. PDCAサイクルの徹底
6. 施策の進捗公開

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

デジタル社会で目指す6つの姿

1. デジタル化による成長戦略
2. 医療・教育・防災・こどもなどの準公共分野のデジタル化
3. デジタル化による地域活性化
4. 誰一人取り残されないデジタル社会
5. デジタル人材の育成・確保
6. DFFT（Data Free Flow with Trust）：「信頼性のある自由なデータ流通」の推進をはじめとする国際戦略

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

デジタル社会の実現に向けた戦略・施策

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み
7. Web3.0の推進

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

サイバーセキュリティなどの安全・安心の確保

1. サイバーセキュリティの確保
2. 個人情報などの適正な取扱いの確保
3. 情報通信技術を用いた犯罪の防止
4. 高度情報通信ネットワークの災害対策

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

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

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

産業のデジタル化

1. デジタルによる新たな産業の創出・育成
   クラウドサービス産業の育成／ITスタートアップなどの育成
2. 事業者向け行政サービスの質の向上に向けた取組み　【別ページで解説】
3. 中小企業のデジタル化の支援　【別ページで解説】
4. 産業全体のデジタルトランスフォーメーション

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

事業者向け行政サービスの質の向上に向けた取組み

1. 電子署名、電子委任状、商業登記電子証明書の普及
2. 法人共通認証基盤（GビズID）の普及
3. 事業者に対するオンライン行政サービスの充実
4. レベルに応じた認証の推進
5. eKYCなどを用いた民間取引などにおける本人確認手法の普及促進

デジタル社会の実現に向けた重点計画

【参照：テキスト5-2-1.】

中小企業のデジタル化の支援

1. 中小企業の事業環境デジタル化サポート
   ・IT専門家との相談を受けられる体制の整備、IT導入補助金　など

2. 中小企業のサイバーセキュリティ対策の支援
   ・「サイバーセキュリティお助け隊サービス」の普及促進
   ・相談体制の強化、情報集約、共有促進機能の強化　など

Society5.0

【参照：テキスト5-2-2.】

Society5.0の特徴と期待される未来

1. IoTを利用
   ・全ての人とモノが繋がり、知識や情報を共有する
   ・新たな価値の創出や社会の課題の解決が可能となる

2. AI、ロボット、自動走行車を利用
   ・少子高齢化、地方の過疎化、貧富の格差などの課題への対応が期待される
   ・希望を持てる社会や、世代間で互いに尊重し合う社会、個人が快適に活躍できる社会の実現が期待される

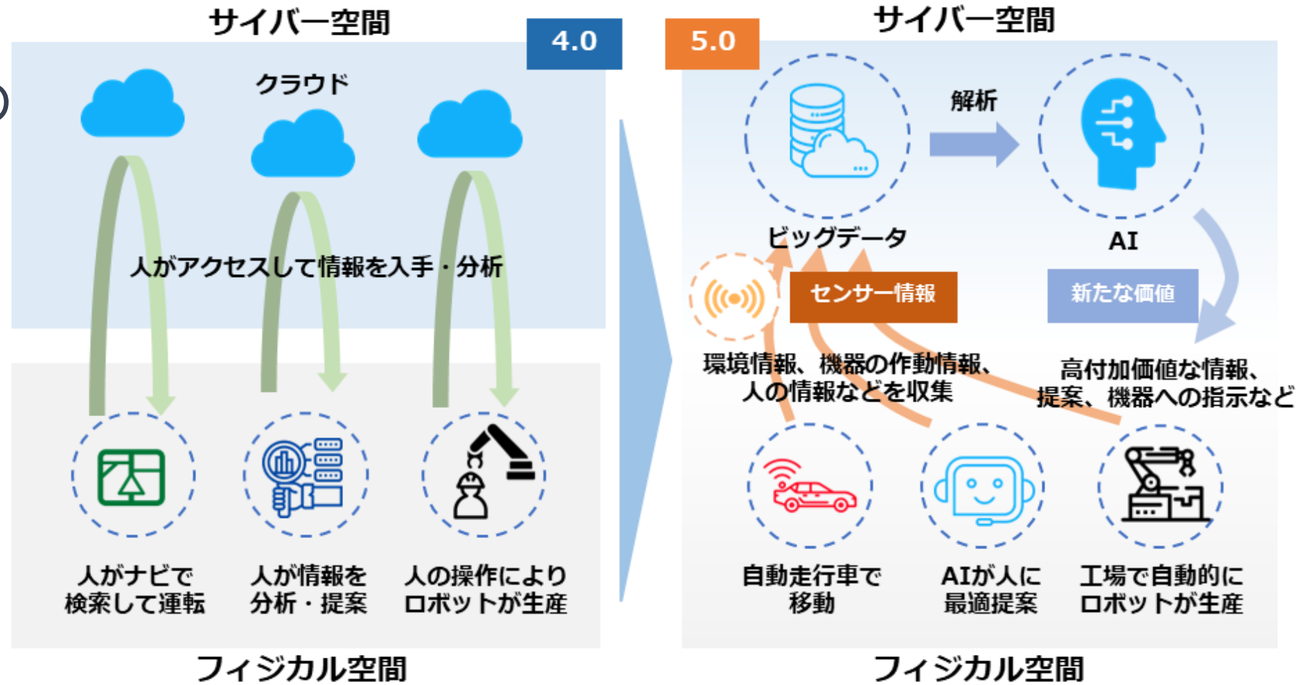
Society5.0

【参照：テキスト5-2-2.】

Society5.0とこれまでの情報社会（Society4.0）の違い

- Society4.0：
  人がクラウドサービスにアクセスし、情報やデータを取得・分析
- Society5.0：
  フィジカル空間のセンサーから取得した膨大な情報がサイバー空間に集積

※ Society4.0では人間が情報の解析で価値を生んでいたが、Society5.0ではAIによる解析結果が人間にフィードバックされ、新しい価値が産業や社会にもたらされる



Society4.0とSociety5.0の比較
（出典）内閣府.”Society5.0”.https://www8.cao.go.jp/cstp/society5_0,（2023-08-03）.

Society5.0

【参照：テキスト5-2-2.】

社会の変化に対するセキュリティ上の脅威

1. サイバー攻撃によりサービス利用の中断または利用不可能
2. データがサイバー空間で改ざんされ、偽情報が拡散されるリスク
3. 情報の漏えいや改ざんによるプライバシー侵害や知的財産権侵害のリスク増加
4. サイバー空間とフィジカル空間の融合による新たな処理がサイバー攻撃の新しい対象となる
5. サプライチェーンの変化に伴うサイバー攻撃の影響範囲が拡大するリスク

DXの推進

【参照：テキスト5-2-3.】

中小企業がDX推進における優位な点

1. 参考情報が豊富
2. 環境が整備されている
3. 環境の変化に素早く対応しやすい

DXの推進

【参照：テキスト5-2-3.】

データ活用の流れ

1. データの収集
   IoTやセンサー、カメラなどの機器を用いて情報を収集する。
2. データの蓄積
   収集した膨大なデータ（ビックデータ）を集積する。
3. データの解析
   AIを用いてデータを解析する。
4. 解析結果の反映
   解析の結果を基に改革を進める。

2．サイバーセキュリティ戦略および関連法令

NISC：サイバーセキュリティ戦略

※NISC
（National center of Incident readiness and Strategy for Cybersecurity）

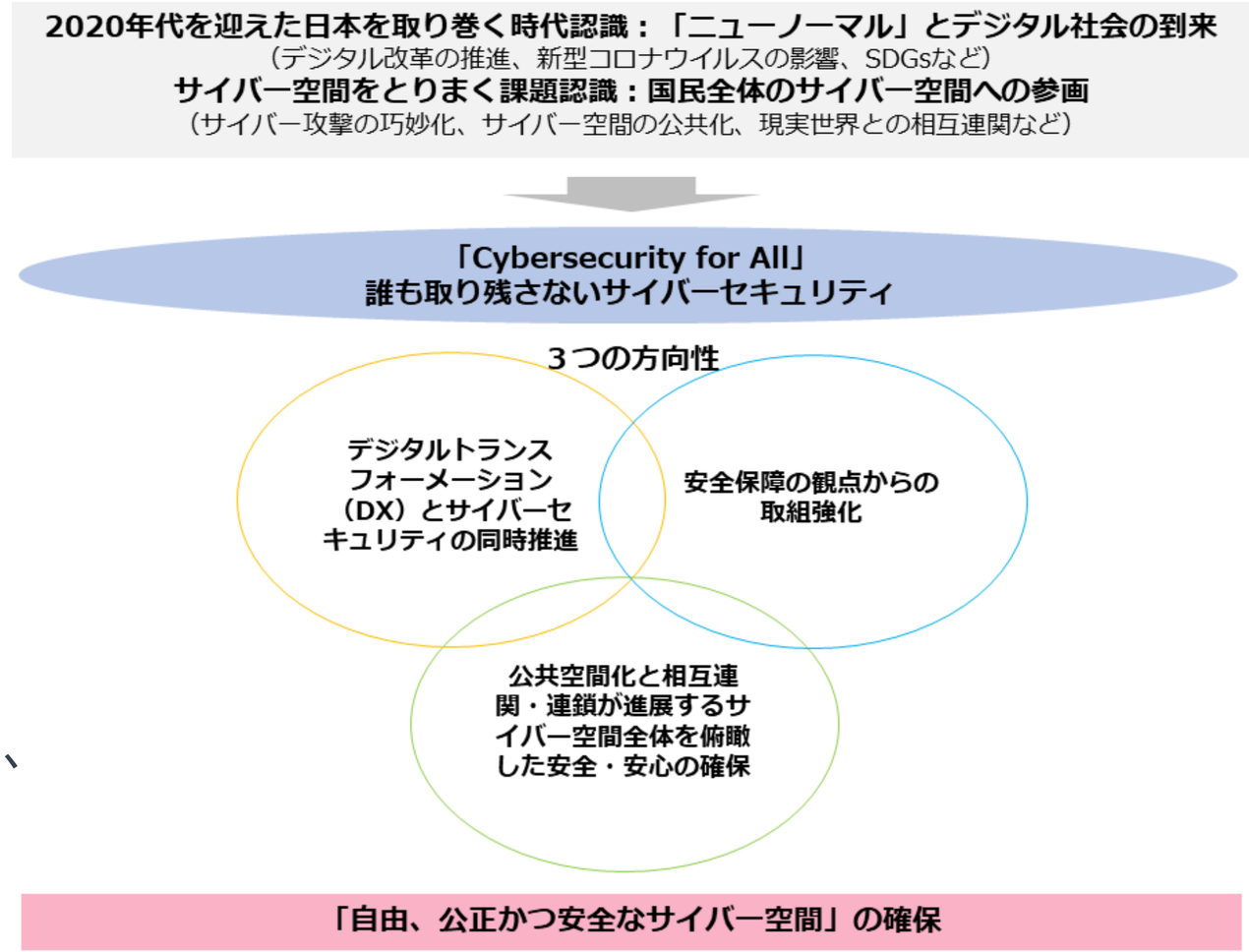
関連法令

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

サイバーセキュリティ戦略の課題と方向性

- サイバーセキュリティ戦略は、国家レベルでのサイバーセキュリティ確保の方針・目標を示す。
- デジタル化の進行とともに、すべての主体がサイバー空間に参加する動きがある。
- 「誰一人取り残さない」セキュリティ確保が必要。
- 戦略では、「自由、公正、かつ安全なサイバー空間」確保のため、3つの方向性をベースに施策推進の方針が示されている。



サイバーセキュリティ戦略の課題と方向性の概要
（出典）NISC「 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」を基に作成

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

3つの政策目標と横断的施策

3つの政策目標

「経済社会の活力の向上及び持続的発展」
「国民が安全で安心して暮らせるデジタル社会の実現」
「国際社会の平和、安定及び我が国の安全保障への寄与」

横断的施策

- 人材育成・確保・活躍推進
- 研究開発の推進
- 全員参加による協働・普及啓発

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

経済社会の活力の向上及び持続的発展

方向性

DXとサイバーセキュリティの同時推進

課題

- DXの進行中、サイバーセキュリティの意識と技術・データへの信頼が不足すると、表層的なデジタル化のリスクが高まる
- デジタル化が進展しているが、セキュリティ確保は企業価値にリンクし、「セキュリティ・バイ・デザイン」の考慮と、デジタルとセキュリティの投資が同時に必要である

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

経済社会の活力の向上及び持続的発展

主な具体的施策

1. 経営層の意識改革
2. 地域・中小企業におけるDX with Cybersecurityの推進
3. 新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり
   - ➢ サプライチェーン、データ流通、セキュリティ製品・サービス、先端技術
4. 誰も取り残さないデジタル／セキュリティ・リテラシーの向上と定着

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

国民が安全で安心して暮らせるデジタル社会の実現

方向性

公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保

課題

- サイバー空間の公共空間化、相互連関、連鎖の深化
- サイバー攻撃の組織化、洗練化

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

国民が安全で安心して暮らせるデジタル社会の実現

主な具体的施策

1. 国民・社会を守るためのサイバーセキュリティ環境の提供
2. デジタル庁を司令塔とするデジタル改革と一体となったサイバーセキュリティの確保
3. 経済社会基盤を支える各主体における取組み
4. 多様な主体による情報共有・連携と大規模サイバー攻撃事態などへの対処体制強化

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

国際社会の平和・安定及びわが国の安全保障への寄与

方向性

安全保障の観点からの取組み強化

課題

- 我が国の安全保障環境が厳しく、中国・ロシア・北朝鮮がサイバー能力を増強し、情報窃取を試みるサイバー攻撃を行っているとの認識がある。
- 同盟国や同志国はサイバー脅威への対応を強化しており、サイバー空間のルールに関する対立に連携して立ち向かっている。
- 安全保障の範囲が経済や技術分野にも広がっているため、同盟国や同志国と連携し、自由で公正なサイバー空間の確保と国際ルールの形成が必要である。

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

国際社会の平和・安定及びわが国の安全保障への寄与

主な具体的施策

1. 自由・公正かつ安全なサイバー空間の確保
   - サイバー空間における法の支配の推進
   - サイバー空間におけるルール形成

2. 我が国の防御力・抑止力・状況把握力の強化
   - サイバー攻撃に対する防御力の向上
   - サイバー攻撃に対する抑止力の向上
   - サイバー空間の状況把握力の強化

3. 国際協力・連携
   - 知見の共有・政策調整
   - サイバー事案などに係る国際連携の強化
   - 能力構築支援

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

横断的施策

3つの政策目標を達成するために、横断的・中長期的な視点で取り組む施策。

研究開発
- 国際競争力の強化・産学官エコシステムの構築
- 実践的な研究開発の推進
- 中長期的な技術トレンドを視野に入れた対応

人材の確保・育成・活躍促進
- DX with Cybersecurityの推進
- 巧妙化・複雑化する脅威への対処
- 政府機関における取組み

全員参加による協働・普及啓発
- ガイドラインや様々な解説資料などの整備の推進

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

サイバーセキュリティ2023

サイバー空間を巡る状況変化と情勢、及び政策課題

- 昨今の状況変化
  - ➢ サイバー空間への依存度の高まり/情報システムの利用拡大/サプライチェーンの多様化・複雑化の進展/生成AIなどの新たな技術普及　など

- サイバー空間の現下の情勢 ～サイバー攻撃の深刻化・巧妙化～
  - ➢ ランサムウェアが依然とした脅威、不正プログラムEmotetが活動と停止の繰り返し/暗号資産交換業者もサイバー攻撃の対象　など

- 昨今の状況変化を踏まえた政策課題
  - ➢ 政府による「国家安全保障戦略」の策定　など

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

サイバーセキュリティ2023

今後の取組みの方向性

1. 経済社会の活力の向上及び持続的発展
   - **ICTの利活用に積極的ではなかった地域・中小企業における対策の促進**
   - **サプライチェーンリスクの増大を踏まえたソフトウェアセキュリティの高度化に関する取組み強化**
2. 国民が安心して暮らせるデジタル社会の実現
3. 国際社会の平和・安定及び我が国の安全保障への寄与

サイバーセキュリティ戦略

【参照：テキスト6-1-1.】

サイバーセキュリティ2023

今後の取組みの方向性

1. 中小企業のサイバーセキュリティ対策促進
   - 「サイバーセキュリティお助け隊サービス」の普及
   - サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）との連携

2. サプライチェーンリスクを踏まえたソフトウェアセキュリティの高度化に関する取組強化
   - 脆弱性情報とSBOMの紐付けを機械的に行う手法の実証
   - 通信分野でのSBOM導入に向けた取組

サイバーセキュリティ戦略

【参照：テキスト6-1-2.】

企業経営のためのサイバーセキュリティの考え方

2つの基本的認識

1. 挑戦
   サイバーセキュリティは、ビジネスの革新や新しい製品・サービス創出の一環として、利益を生み出す戦略として考慮すべきである。
2. 責任
   つながる社会でのサイバーセキュリティへの取組みは、社会の要求であり、自社だけでなく、全体の発展にも寄与する。

サイバーセキュリティ戦略

【参照：テキスト6-1-2.】

企業経営のためのサイバーセキュリティの考え方

3つの留意事項

1. 情報発信による社会的評価の向上
2. リスクの一項目としてのサイバーセキュリティ
3. サプライチェーン全体でのサイバーセキュリティの確保

サイバーセキュリティ戦略

【参照：テキスト6-1-2.】

サイバーセキュリティ対策の取組みレベル

レベル	分類	概要
理想的に	1	ITの利活用を事業戦略上に位置付け、サイバーセキュリティを強く意識し、積極的にITによる革新と高いレベルのセキュリティに挑戦する企業
もっと積極的に	2	IT・サイバーセキュリティの重要性は理解しているものの、積極的な事業戦略としての組み込みはできていない企業
無駄な投資	3	過剰なセキュリティ意識により、ITの利活用を著しく制限し、競争力強化に活用させていない企業
危険	4	サイバーセキュリティ対策の必要性は理解しているが、必要十分なセキュリティ対策ができていないにもかかわらず、ITの利活用を進めている企業
	5	サイバーセキュリティの必要性を理解していない企業や、自らセキュリティ対策を行う上で事業上のリソースの制約が大きい企業
対象外	6	ITを利用していない企業

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

DX with Cybersecurity

DX with Cybersecurityの推進に向けた主な施策

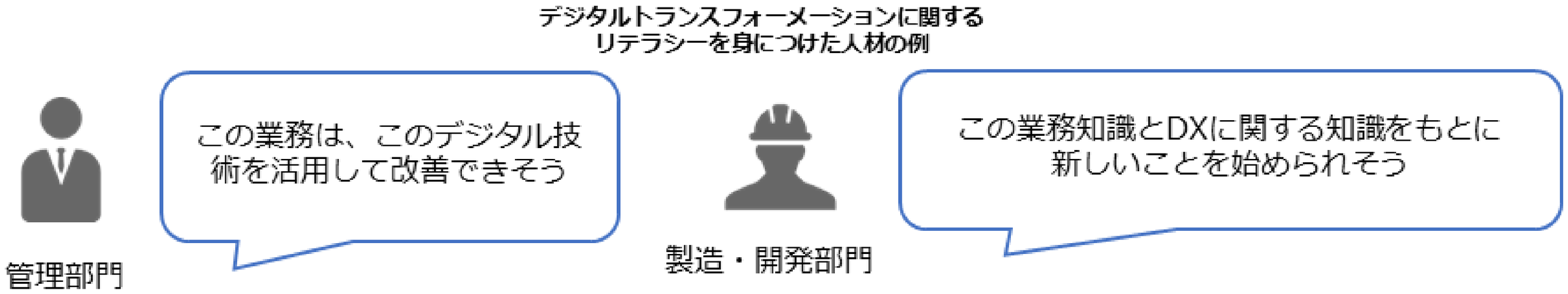
分類	課題	施策
経営層の意識改革	経営層が主体性をもってDXとサイバーセキュリティ対策に取組むためには、専門家とのコミュニケーションが重要	経営者がITやセキュリティに関する専門知識を持っていない場合でも、セキュリティ専門家と協力し、「プラス・セキュリティ」知識を習得する環境を整備
地域・中小企業におけるDX with Cybersecurityの推進	中小企業は、セキュリティ対策に予算を割く事の必要性を理解する	中小企業が利用しやすい安価かつ効果的なセキュリティサービス・保険の普及など、中小企業向けセキュリティ施策を推進
新たな価値創出を支えるサプライチェーンなどの信頼性確保に向けた基盤づくり	サイバー攻撃の起点となり得る箇所の拡大に伴う、リスク管理が重要	産業分野別、または産業横断的なガイドラインの策定や活用促進を通じて、産業界におけるセキュリティ対策の具体化・実装を促進

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

DXに関するリテラシーを身につけたことによる効果（個人）

- 世の中のDXと最新技術にアンテナを広げる
- 新技術やキーワードに興味を持つ
- 知らない内容に遭遇した時、自ら調査しDXの知識を深める



サイバーセキュリティ戦略

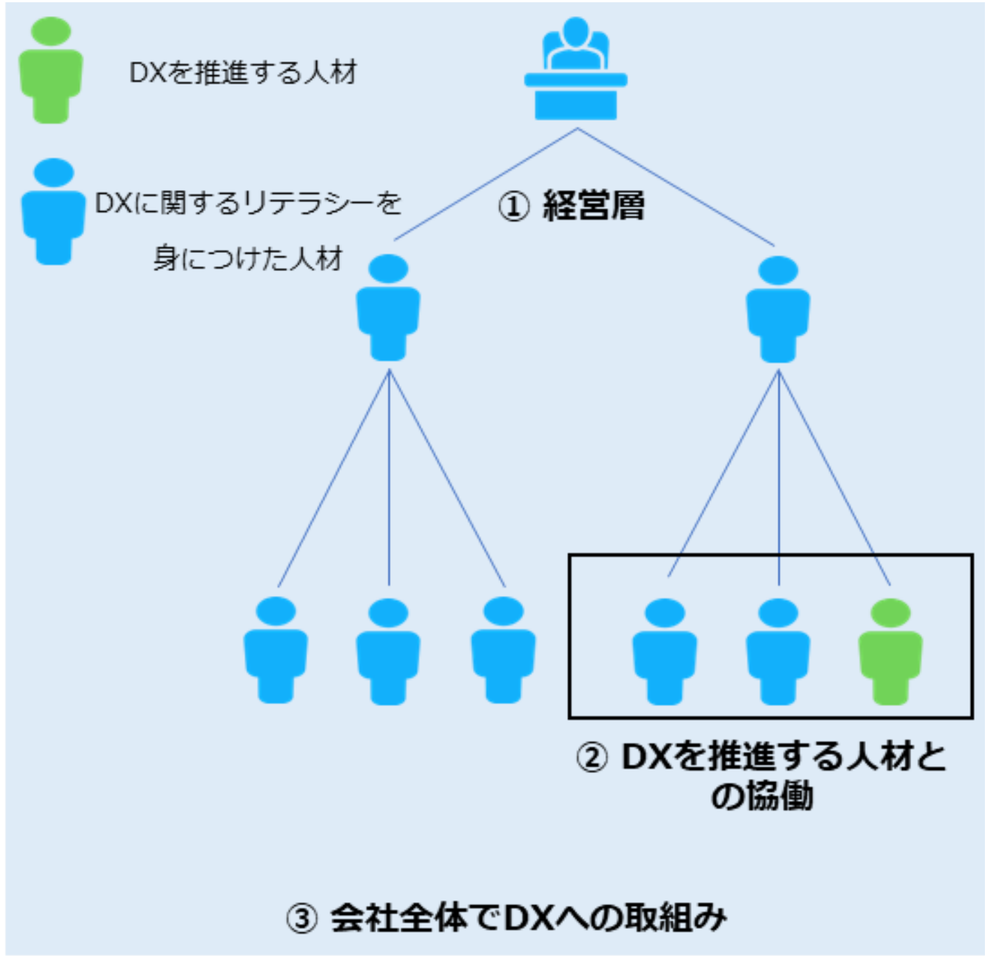
【参照：テキスト6-1-3.】

DXに関するリテラシーを身につけたことによる効果（会社）

経営層
- 社会・ビジネス環境の変化を把握
- 有益な技術・考え方を獲得
- 自社のDXの方向性を社員に示す

DXを推進する人材との協働
- 事業知見を持つ人材との協力
- DX専門の人材との連携
- これにより企業のDXが進展しやすくなる

会社全体でDXへの取組み
- 社員全員がDXリテラシーを習得
- 組織内の変化に対する理解が増加
- DXの推進が受け入れられやすくなる



DXリテラシー標準に沿った学びによる効果の概要
（出典）IPA、経済産業省「デジタルスキル標準ver.1.0 」を基に作成

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

デジタルスキル標準（DSS）

「DXリテラシー標準」は、自身が属する産業や事業の方向性に合わせる必要がある

標準策定のねらい

ビジネスパーソン一人ひとりがDXに関するリテラシーを身につけることで、
DXを自分事ととらえ、変革に向けて行動できるようになる

Why
（DXの背景）
DXの重要性を理解するために必要な、社会、顧客・ユーザー、競争環境の変化に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする）

What
（DXで活用されるデータ・技術）
ビジネスの場で活用されているデータやデジタル技術に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

How
（データ・技術の利活用）
ビジネスの場でデータやデジタル技術を利用する方法や、活用事例、留意点に関する知識を定義

→ DXに関するリテラシーとして身につけるべき知識の学習の指針とする

マインド・スタンス

社会変化の中で新たな価値を生み出すために必要な意識・姿勢・行動を定義

→個人が自身の行動を振り返るための指針かつ、組織・企業がDX推進や持続的成長を実現するために、構成員に求める意識・姿勢・行動を検討する指針とする

DXリテラシー標準の全体像
（出典）IPA、経済産業省「デジタルスキル標準ver.1.1 」を基に作成

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

デジタルスキルの学習方法

マナビDXとは

- DXに関する講座を案内するサービス
- https://manabi-dx.ipa.go.jp/

取り扱い講座

- 経済産業省の審査基準を満たしたDXに関するもの
- 掲載講座数：457件
  有償：360件　無償：97件　（2023/8/27現在）

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

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。

クラウドを活用した
新規プロジェクトの担当者

組み込みソフトウェアの
機能を設計する担当者

自社の電話、
インターネット、複合機な
どの保守契約を扱う担当者

サイバーセキュリティの知識が不十分な
場合の問題例

目的にそぐわないクラウドを選定することや、自社のサイバーセキュリティ担当者が把握していないクラウドの導入により、情報漏洩などのリスクが高まる恐れがあります

ソフトウェアにサイバー攻撃に対する脆弱性が生じる恐れがあります

不適切な設定で運用することで、機器を介した情報漏えいの原因となる恐れがあります

サイバーセキュリティ戦略

【参照：テキスト6-1-3.】

プラス・セキュリティ人材の育成

試験・資格の活用

- 各分野の人材がセキュリティ知識を習得する手段として、資格や試験がある。
- 資格の利点は、特定の業務に必要なスキルを効率的に学べること。

情報セキュリティマネジメント試験

対象：企業の戦略マネジメント層や実務者層のサイバーセキュリティ担当者
内容：組織の情報セキュリティを確保し、脅威から保護するための計画・運用・評価・改善のスキルを認定する。

教育プログラム・コミュニティ活動の活用

NISCでは、経営層、管理職、一般社員ごとにそれぞれ初級、中級、上級で難易度が分けられたプラス・セキュリティ知識を補充できる研修、セミナー、講義などが紹介されています。
https://security-portal.nisc.go.jp/#strategiclist

関連法令

【参照：テキスト6-2-1.】

個人情報保護法

<u>個人情報保護法とは</u>

- インターネット普及や情報技術の進歩を背景に、「個人情報保護法」が2005年4月に施行。
- デジタル技術の進展や社会情勢の変化を受けて、法律は3度の改正を経ている。
- この法律では、何が個人情報とされるかや、その取り扱い方法を規定。

<u>個人情報の定義</u>

- 「個人情報」は生存する個人に関する情報。
- 氏名、生年月日、住所、顔写真などで個人を特定できる。
- 他の情報と照合し特定可能なものも含む。

関連法令

【参照：テキスト6-2-1.】

個人情報を取り扱う時の基本ルール

項番	取扱い種別	ルール
1	取得・利用	・利用目的を特定して、その範囲内で利用する ・利用目的を通知又は公表する
2	保管・管理	・漏えいなどが生じないように、安全に管理する ・従業者や委託先にも安全管理を徹底する
3	提供	・第三者に提供する場合は、あらかじめ本人から同意を得る ・第三者に提供した場合、提供を受けた場合は一定事項を記録する
4	開示請求などへの対応	・本人から開示などの請求があった場合はこれに対応する ・苦情に適切かつ迅速に対応する

<u>個人情報保護法の罰則規定</u>

- 2022年4月の法改正で、罰則強化。
- 個人情報保護委員会の命令違反や不正流用で、1億円以下の罰金。
- 報告義務違反の場合、50万円以下の罰金。

関連法令

【参照：テキスト6-2-2.】

GDPR

GDPR（一般データ保護規則）とは

起源: EU（欧州連合）で策定された新しい個人情報保護の枠組み。

目的: 個人のプライバシー権を強化し、個人データの処理に関する組織の透明性を増すことを目的としている。

適用範囲: 欧州経済領域（EEA）内で活動するすべての組織に適用され、EEA外の組織もEEAの市民のデータを処理する場合にはこの規則の対象となる。

内容: 個人データの「収集」、「処理」、「保存」、「移転」など、あらゆる側面に関してのルールが定められており、ユーザーには自らのデータに対するアクセス、修正、削除などの権利が保障されている。

罰則: 違反組織には、全世界の年間売上の最大4%以下、または2,000万ユーロ以下（いずれか高い方）の罰金が課せられることが規定されている。

※1ユーロ：¥158.09（2023/8/27日現在）
2,000万ユーロ：約31.6億円

関連法令

【参照：テキスト6-2-2.】

GDPRと日本企業の関係

- EU内に物理的拠点がない企業も対象となる可能性
  インターネットを利用してEU域内に商品やサービスの提供、情報収集を実施
  EU域内からのアクセスを持つターゲティング広告を配置した自社サイトを保有
- GDPR違反時には重い制裁金が課せられる

対策例

- GDPRにおいて、Cookieは「個人情報」として扱われる
- WebサイトでCookieを使用する場合、閲覧者からの同意取得が必須
- 個人データの利用同意の管理のため、ツール（CMP）の導入が推奨される

１．セキュリティフレームワーク

セキュリティフレームワークの概要

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

NISTサイバーセキュリティフレームワーク（CSF）

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）

サイバーセキュリティ経営ガイドライン

セキュリティフレームワークの概要

【参照：テキスト7-1-1.】
第7章 - 02

セキュリティフレームワークの役割と重要性

セキュリティフレームワークの定義

セキュリティ対策を行うために定義された指針やセキュリティ対策基準、ガイドライン、ベストプラクティス集のことを指します。

セキュリティフレームワークを利用するメリット

効果的なセキュリティ対策

信頼性の確保

セキュリティフレームワークの概要

【参照：テキスト7-1-1.】
第7章 - 02

代表的なセキュリティフレームワークの紹介

項番	フレームワーク名	概要
1	ISMS 別途詳細	[ISO/IEC27001,27002] 網羅的なセキュリティフレームワーク
2	ISO/IEC27017	クラウドサービス対象のセキュリティフレームワーク
3	CSF 別途詳細	重要インフラ対象のセキュリティフレームワーク
4	CPSF 別途詳細	Society5.0における産業社会が対象のセキュリティフレームワーク
5	サイバーセキュリティ経営ガイドライン 別途詳細	経営者を中心としたセキュリティ対策
6	PCI DSS	クレジットカード産業を対象としたデータセキュリティ基準
7	PMS	個人情報保護
8	CIS Controls	具体的なサイバー攻撃アプローチ
9	ISA/IEC62443	産業オートメーションおよび制御システム

セキュリティフレームワークの選択の重要性

【参照：テキスト7-1-2.】
第7章 - 03

代表的なセキュリティフレームワークの概要

ISO/IEC27017

- クラウドサービスの情報セキュリティ対策のガイドライン規格が存在。
- ISO/IEC27002をベースに作成。
- 対象：クラウドサービスの提供者と利用者。
- 目的：クラウドサービスのリスク低減、適切な利用のための組織体制の確立。
- ISO/IEC 27001は情報セキュリティのマネジメントシステム規格。
- ISO/IEC 27017を通じて、ISO/IEC 27001を強化し、クラウドサービス向けの情報セキュリティ管理体制の構築が可能。

セキュリティフレームワークの選択の重要性

【参照：テキスト7-1-2.】
第7章 - 04

代表的なセキュリティフレームワークの概要

PCI/DSS（国際的なクレジット産業向けのデータセキュリティ基準）

- 国際カードブランド5社が共同で策定した国際基準。
- 対象：クレジットカード情報を取扱う全ての事業者。
- 名称：Payment Card Industry Data Security Standard (略称：PCI DSS)。
- 目的：カード会員情報の適切な管理。
- 基準内容：ネットワークアーキテクチャ、ソフトウェアデザイン、セキュリティマネジメント、ポリシー、プロシジャ。
- 12の要件で規定。

セキュリティフレームワークの選択の重要性

【参照：テキスト7-1-2.】
第7章 - 04

代表的なセキュリティフレームワークの概要

PMS（個人情報保護マネジメントシステム）

- 目的：組織が取り扱う個人情報の安全・適切な管理。
- 規格：JIS Q 15001。
- 主な内容：事業者が個人情報を適切に取り扱う方法の規定。
- プライバシー保護：直接の目的ではないが、結果的に保護される。
- PMSの基本：個人情報保護方針の設定と、その方針に基づくPDCAサイクルの実行。

セキュリティフレームワークの選択の重要性
代表的なセキュリティフレームワークの概要

【参照：テキスト7-1-2.】
第7章 - 04

CIS Controls

- 目的：サイバー攻撃の現状・傾向を基に、組織のサイバーセキュリティ対策と優先順位を決定するフレームワーク。
- 重点：あらゆる企業の最も基本的・重要な対応。
- 特徴：ネットワークの詳細設定、ログ管理などの具体的・技術的対策が中心。
- アプローチ：多岐にわたる対策から、自社の実施すべき対策と優先順位を導出。

セキュリティフレームワークの選択の重要性
代表的なセキュリティフレームワークの概要

【参照：テキスト7-1-2.】
第7章 - 04

ISA/IEC62443

- 主題：産業用自動制御システムのセキュリティ対策・プロセス要件の国際標準規格。
- カバー範囲：ISO/IEC 27001では十分にカバーされない工場やプラントの制御システムのセキュリティ。
- 対象：ソフトウェア・ハードウェアを含む制御関連のデータ処理基盤。
- 特徴：システムだけでなく、運用に関わる「人」と「業務」も対象。

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-1.】
第7章 - 05

ISMSの概要

- 定義：ISMSは情報セキュリティマネジメントシステムの略。
- 目的：組織の情報セキュリティリスクの適切な管理。
- 地位：国際規格の存在により、代表的なセキュリティフレームワークとして認識。
- 達成目標：情報の機密性、完全性、可用性をバランス良く維持・改善し、信頼を提供。
- 対策範囲：技術的対策、従業員教育・訓練、組織体制の整備を含む。

情報セキュリティマネジメントシステム（ISMS）

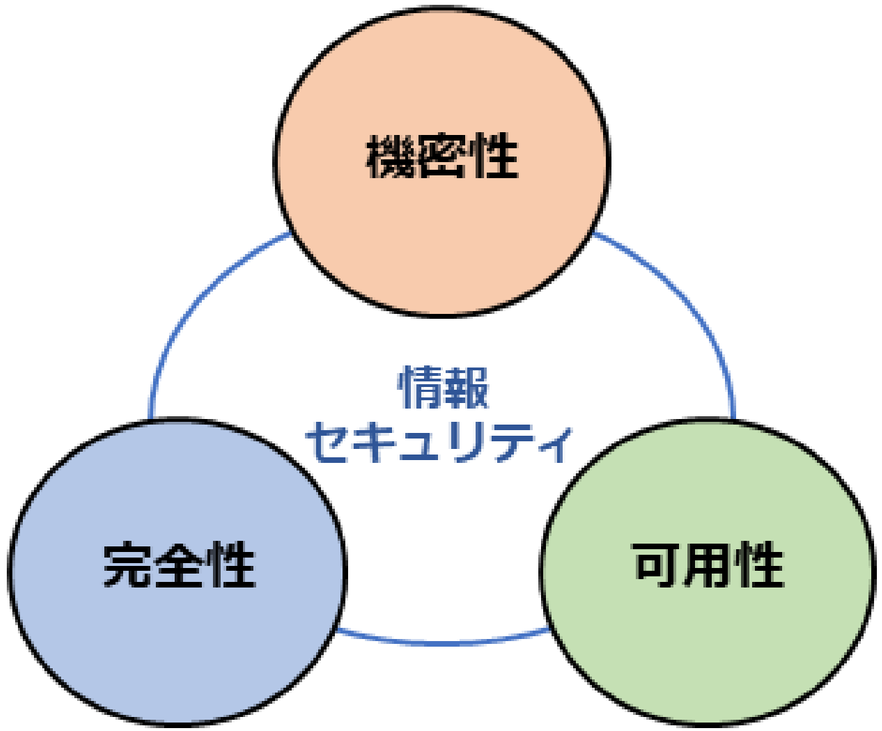
【参照：テキスト7-2-1.】
第7章 - 05

情報セキュリティの3要素

機密性（Confidentiality）
　情報に対するアクセスを適切に管理すること

完全性（Integrity）
　情報が正確であり、完全である状態を保持すること

可用性（Availability）
　情報を必要な時に使えるようにしておくこと



情報セキュリティの3要素
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-1.】
第7章 - 06

ISO/IEC 27001とJIS Q 27001

ISMSのための要求事項をまとめた国際規格が、ISO/IEC 27001
ISO/IEC 27001を日本語訳し、日本産業規格としたものが
JIS Q 27001

使用用途

- 組織のマネジメントおよび業務プロセスを取り巻くリスクの変化への対応
- 情報セキュリティ要求事項を満たす組織の能力を内外で評価するための基準

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-2.】
第7章 - 07

ISMSの要求事項

ISMS認証取得するために必ず対応し、PDCAの運用サイクルで
情報セキュリティマネジメントを実施すること

要求事項
1. 適用範囲
2. 引用規格
3. 用語および定義

4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

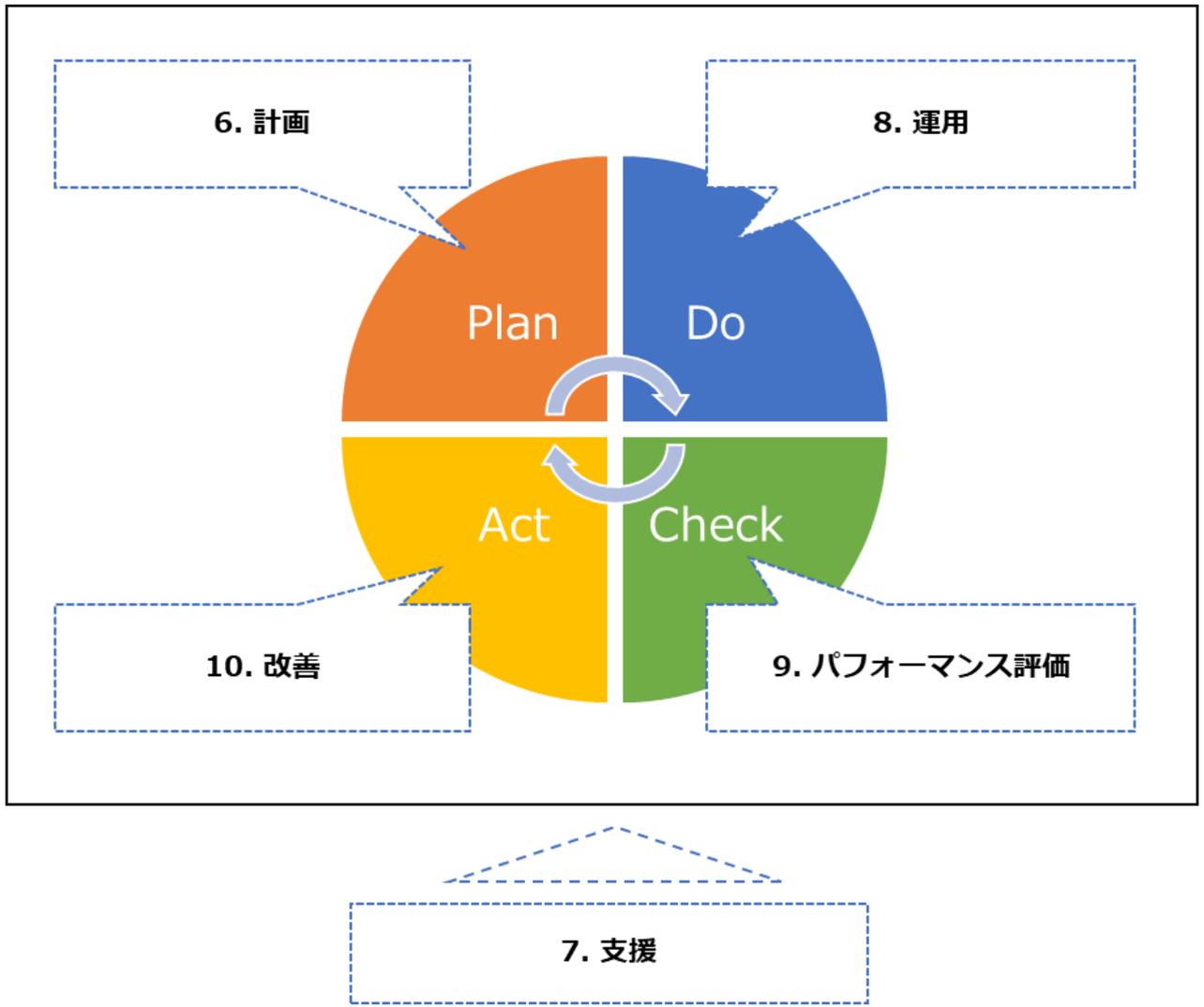
実質的な要求事項

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-2.】
第7章 - 08

ISMSの運用プロセス

マネジメントシステムは組織の目標達成のための管理の仕組み。ISMSは情報セキュリティと機密情報の保護を目的とし、そのための方法としてPDCAサイクルを繰り返してスパイラルアップすることがISO/IEC 27001で要求される。



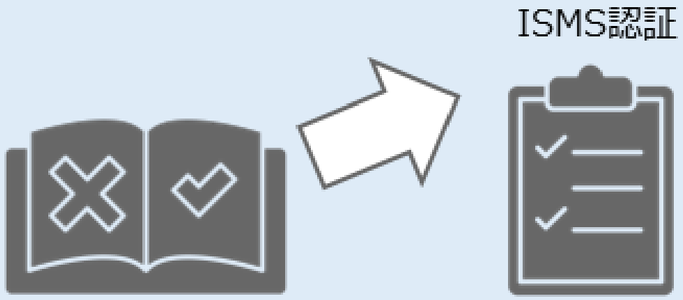
情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-2.】
第7章 - 09

ISO/IEC 27001 と ISO/IEC 27002

ISO/IEC 27002は情報セキュリティの管理策を示す規格で、ISO/IEC 27001の付属書Aに反映されている。管理策は具体的な状況に応じて選択・適用され、93の管理策は4つのカテゴリに分けられている。

ISO/IEC 27001



ISMS認証取得のための**要求事項**をまとめた国際規格
（適切なISMSを構築・運用するための国際的なルールブック）

ISO/IEC 27002

情報セキュリティマネジメントの**管理策**を示した国際規格

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-2.】
第7章 - 09

ISMSの管理策

管理策は次の4つのテーマにグループ分けされるようになった。

情報セキュリティ管理策		
テーマ	項目数	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。例えば、情報セキュリティの方針、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。例えば、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。

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-2.】
第7章 - 12

ISMSの管理策における属性

ISO 27002 の最新版では、カテゴリー分類をしやすくするため、
管理策に5種類の「属性」が追加されている。

管理策における属性	
属性	**概要**
管理策のタイプ	予防、検知、是正
情報セキュリティ資産	機密性、完全性、可用性
サイバーセキュリティの概念	識別、防御、検知、対応、復旧
運用能力	ガバナンス、資産管理、情報保護、人的資産のセキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティなど
セキュリティドメイン	ガバナンスとエコシステム、保護、防御、対応力

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-3.】
第7章 - 13

ISMSの構築

ISMS実装のためのステップ

1. 適用範囲の決定
2. 情報セキュリティ方針の策定
3. 体制の確立
4. ISMS文書の作成
5. リスクアセスメントの実施
6. 従業員の教育
7. 内部監査
8. マネジメントレビュー

情報セキュリティマネジメントシステム（ISMS）

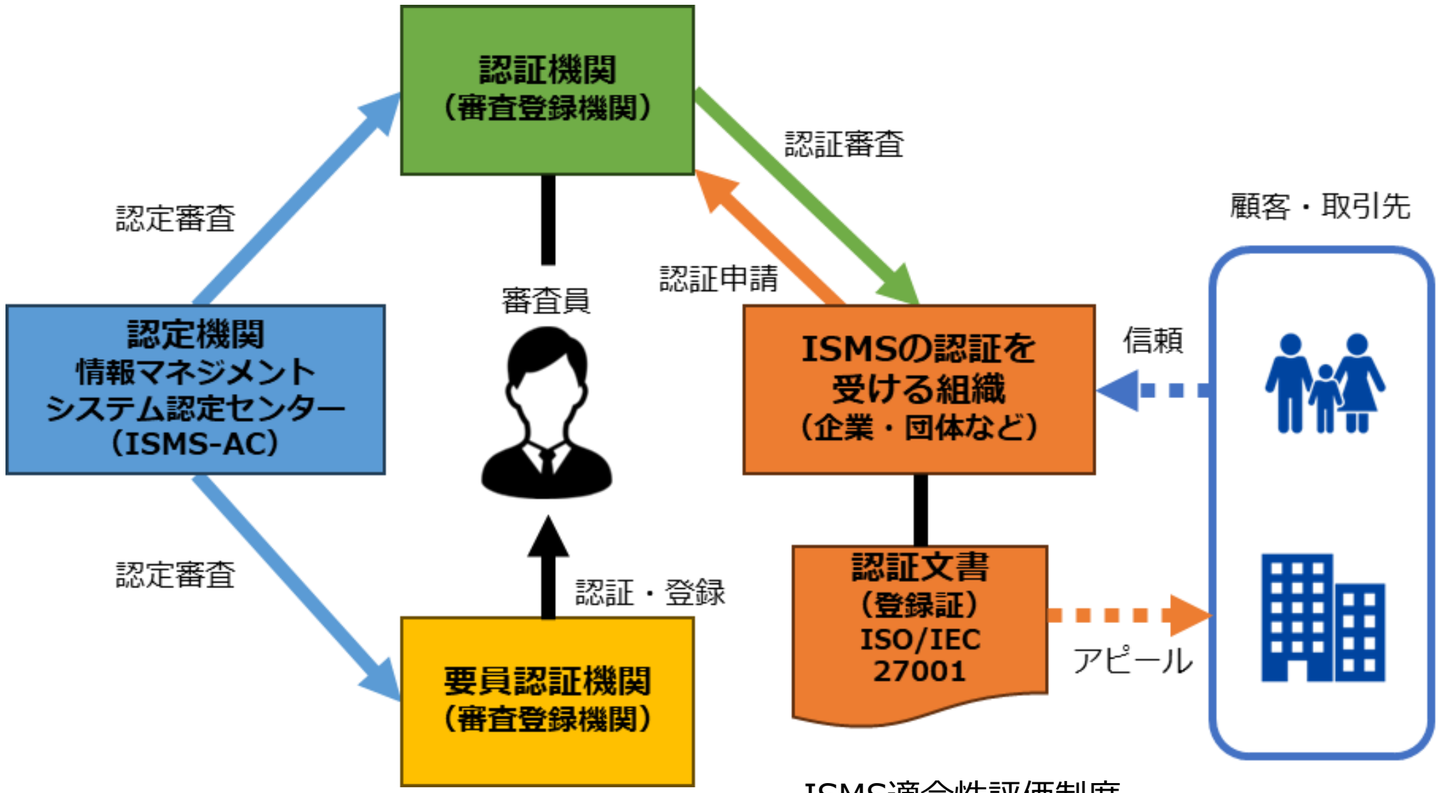
【参照：テキスト7-2-3.】
第7章 - 14

ISMSの実装と認証

「ISMS認証」は、組織のISMSがISO/IEC 27001に準拠しているかを第三者認証機関が審査する制度。この評価は国際的な「ISMS適合性評価制度」のもとで行われます。

認定と認証

認定	認定機関が認証機関を審査し、認証を遂行する能力のあることを公式に承認する行為を認定と言います。
認証	第三者が文書で保証する手続きを認証と言います。



ISMS適合性評価制度
（出典）ISMS-AC「ISMS適合性評価制度」を基に作成

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-3.】
第7章 - 15

ISMS認証審査プロセス

ISMSの認証審査は、次のようなステップで実施されます。

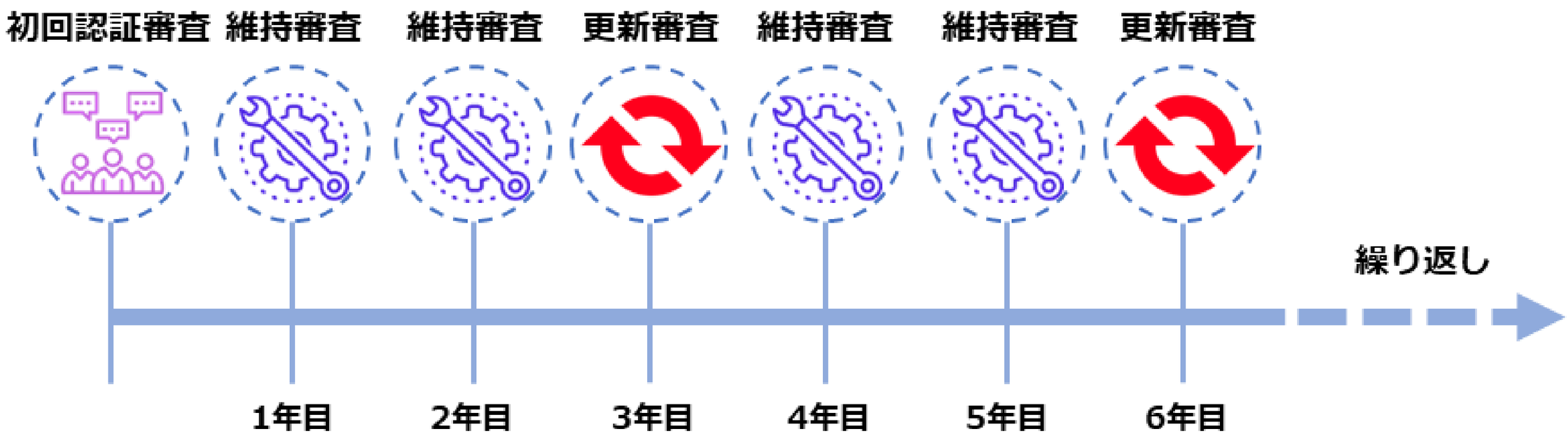
ステップ	申請	審査日程の確認	初回認証審査	認証登録	報告・公開
概要	新規取得する際、今までと異なる認証機関で受診する場合は、申請が必要です。	組織と認証機関との間で、審査日程の確認を行います。	新規の場合は原則として1次審査と2次審査の2回で実施されます。	審査の結果、適合していることが確認されると認証書が発行され、登録完了となります。	認証された旨が認証機関からISMS-ACに報告され次第、ISMS-ACホームページで公開されます。

情報セキュリティマネジメントシステム（ISMS）

【参照：テキスト7-2-3.】
第7章 - 15

ISMS認証の維持、更新審査プロセス

- 年に1回以上の維持審査（サーベイランス審査）
- 3年ごとに認証の有効期限を更新するための更新審査



NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-1.】
第7章 - 16

NISTサイバーセキュリティフレームワーク（CSF）の概要

- CSFはNISTが作成したサイバー攻撃対策のフレームワーク。
- 防御だけでなく、検知・対応・復旧のインシデント対応が含まれる。
- 要求事項は汎用的で、多様な企業に適用可能。
- 指示書やノウハウ集ではない。
- 利用方法は実施する組織に委ねられている。
- CSFを理解し、サイバーセキュリティ対策の検討が必要。

NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-1.】
第7章 - 16

CSFの3つの構成要素（コア、ティア、プロファイル）

「コア」の概要
サイバーセキュリティ対策の一覧

「ティア」の概要
対策状況を数値化するための成熟度評価基準

「プロファイル」の概要
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

NISTサイバーセキュリティフレームワーク コアとは

【参照：テキスト7-3-2.】
第7章 - 17

業種・業態や企業規模に依存しない共通のサイバーセキュリティ対策の一覧を定義したものです

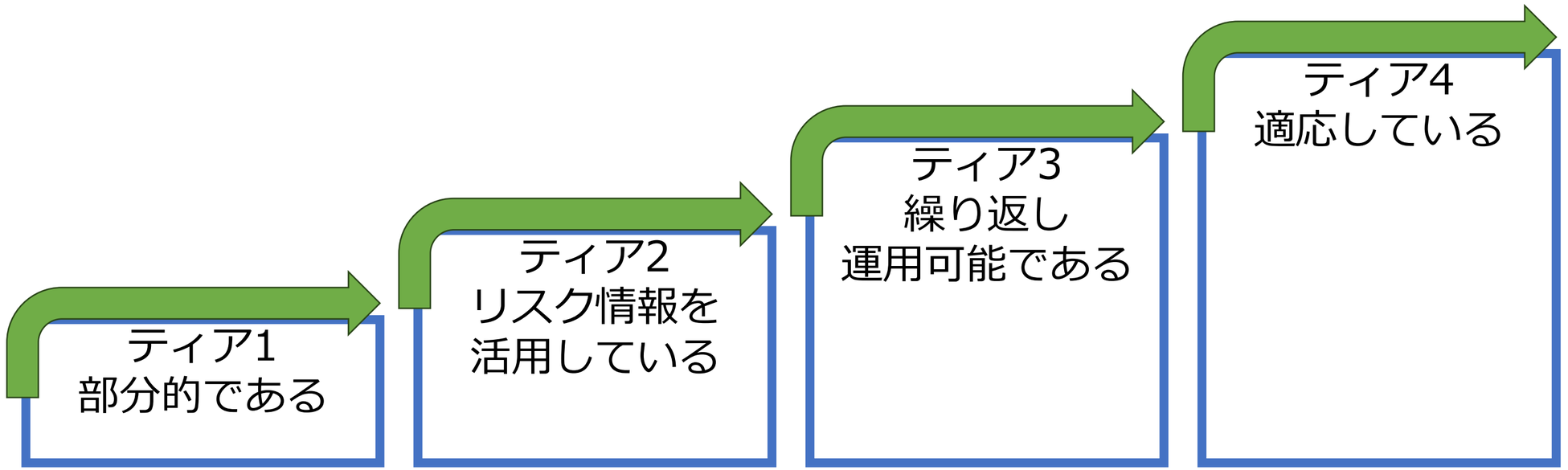
機能	説明	カテゴリ	サブカテゴリ
識別	組織の資産（情報システム、人、データ・情報など）、組織を取り巻く環境、重要な機能を支えるリソース、関連するサイバーセキュリティリスクを特定し理解を深める。	合計23	合計108
防御	重要サービスの提供が確実に行われるよう適切な保護対策を検討し実施する。		
検知	サイバーセキュリティイベントの発生を検知するための適切な対策を検討し実施する。		
対応	サイバーセキュリティインシデントに対処するための適切な対策を検討し実施する。		
復旧	サイバーセキュリティインシデントにより影響を受けた機能やサービスをインシデント発生前の状態に戻すための適切な対策を検討し実施する。これには、レジリエンスを実現するための計画の策定・維持も含む。		

NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-2.】
第7章 - 19

ティアとは

組織におけるサイバーセキュリティリスクへの対応状況を評価する際の指標を定義したものです。指標はティア1～ティア4までの4段階があります。



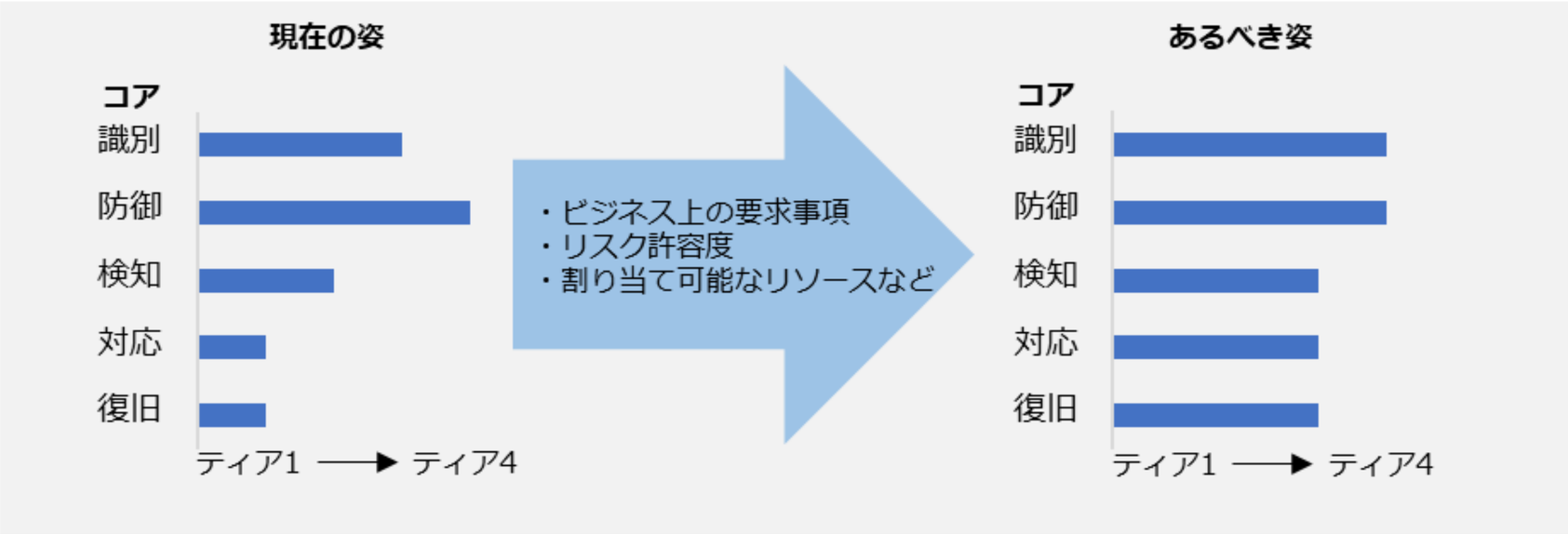
ティアの成熟度イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-2.】
第7章 - 19

プロファイルとは

組織ごとの考慮点を整理したもので、サイバーセキュリティ対策の現状と目標状態を明示します。これにより、必要な改善点のギャップを特定できます。「あるべき姿」は、ビジネス要求やリスク許容度、リソースを基に策定されます。



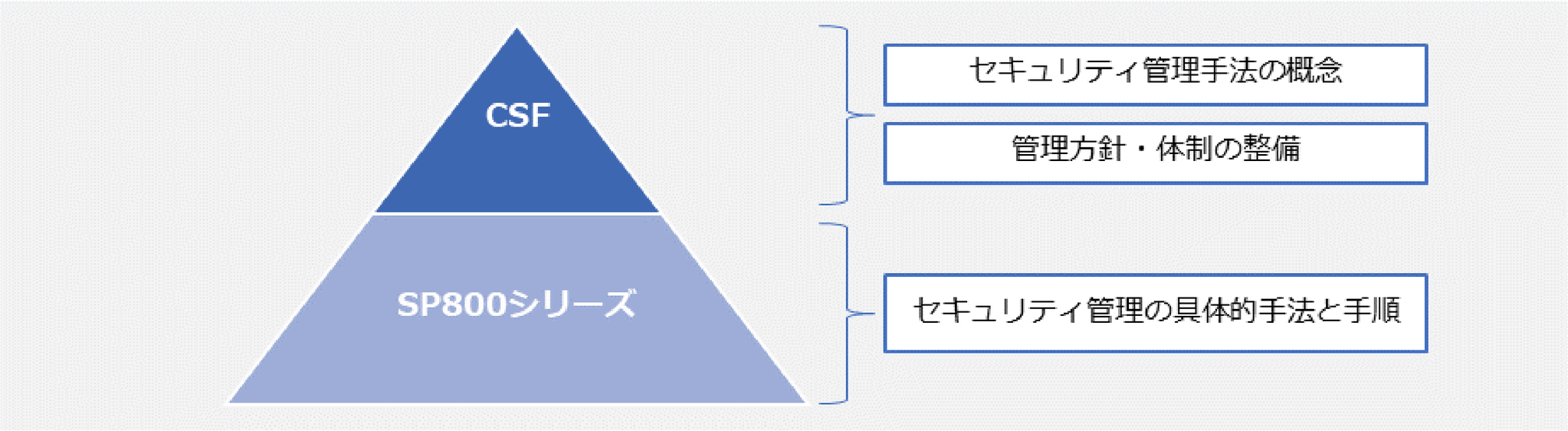
プロファイルの活用イメージ
（出典）デジタル庁 「政府情報システムにおける サイバーセキュリティフレームワーク導入に関する 技術レポート 」を基に作成

NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-3.】
第7章 - 20

NIST SP 800シリーズとCSFの関連性

CSFの下位概念に位置付けられているのが、NIST SP 800シリーズです。実施すべきタスクと手順、推奨技術の特定など、セキュリティ管理の手法について具体的に明記されています。



CSFとSP800シリーズの関係

NISTサイバーセキュリティフレームワーク

【参照：テキスト7-3-4.】
第7章 - 21

CSFとISMSの関連性

主な共通点

- 汎用性が高い
- サイバーセキュリティ対策方法
- 任意性がある

主な相違点

- 第三者認証制度の有無
- 目標への到達手段

サイバー・フィジカル・セキュリティ対策フレームワーク

CPSFの概要

【参照：テキスト7-4-1.】
第7章 - 22

- Society5.0でサイバー空間とフィジカル空間が融合。
- サプライチェーンが『価値創造過程』として変化。
- 新しいサプライチェーンにはサイバー攻撃のリスク増。
- 政府が『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)を策定。
- CPSFは既存のISMSやCSFを基に、サイバーとフィジカルの両方のセキュリティ対応。

サイバー・フィジカル・セキュリティ対策フレームワーク

CPSFの目的と適用範囲

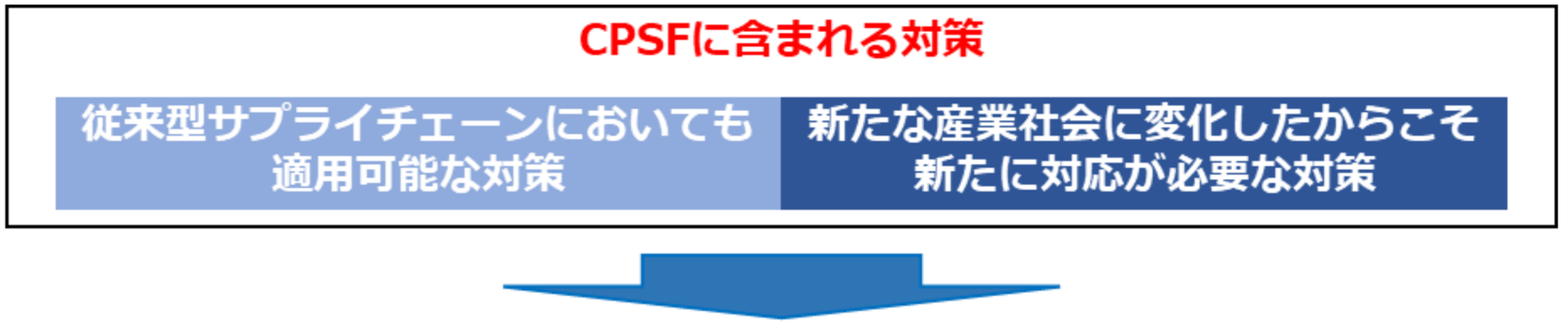
【参照：テキスト7-4-1.】
第7章 - 22

目的

CPSFは新たな産業社会のバリュークリエイションプロセスを理解し、リスクを明確化し、セキュリティ対策を整理すること。

適用範囲

新たな産業社会のバリュークリエイションプロセス全体。



- **新たな産業社会における**バリュークリエイションプロセス全体が適用範囲
- それぞれの組織に応じてセキュリティ対策を選定することが可能

サイバー・フィジカル・セキュリティ対策フレームワーク

3層構造モデル

【参照：テキスト7-4-1.】
第7章 - 23

サイバー空間におけるつながり

[第3層]

自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保

フィジカル空間とサイバー空間のつながり

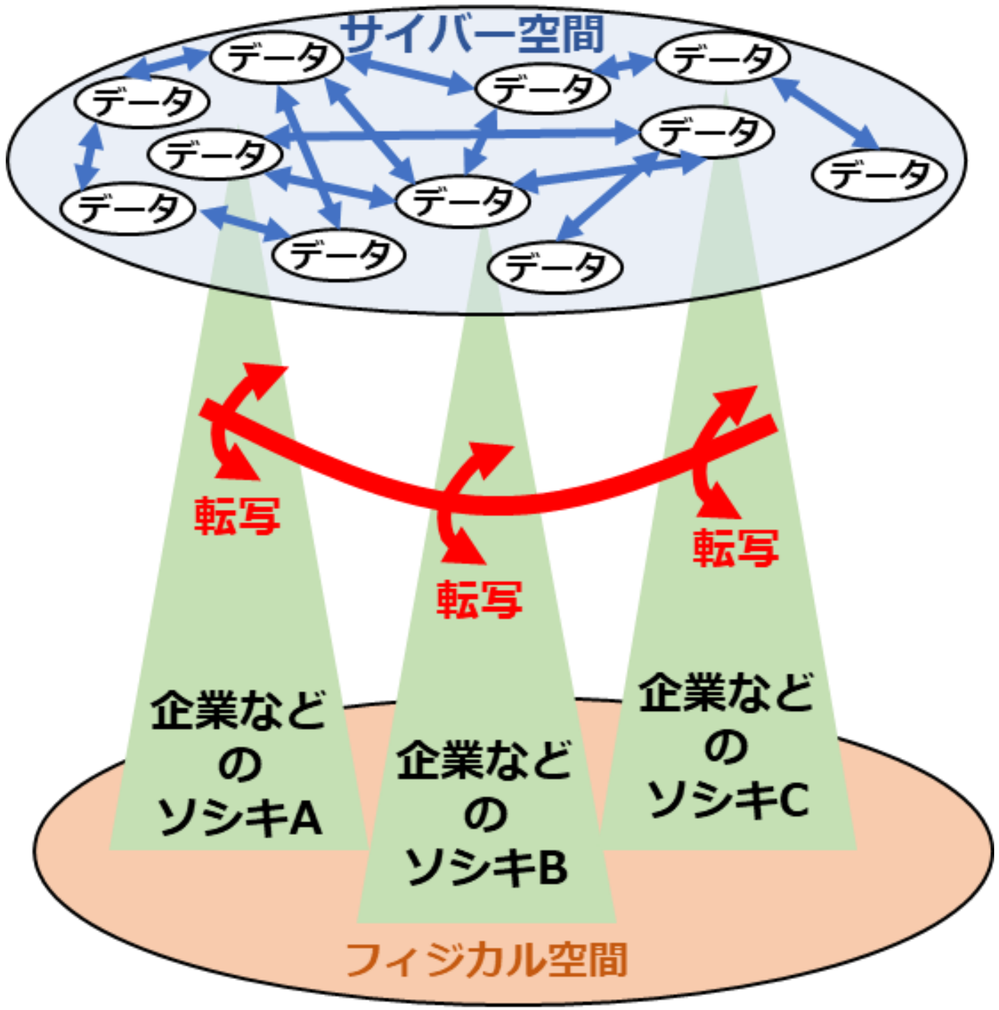
[第2層]

フィジカル空間・サイバー空間を正確に”転写”する機能の信頼性を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラなどの信頼）

企業間のつながり

[第1層]

適切なマネジメントを基盤に各主体の信頼性を確保



サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 25

経営者が認識するべき3原則

原則1	経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップの元で対策を進めることが必要
原則2	サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先など、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
原則3	平時および緊急時のいずれにおいても、効果的なサイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 25

経営の重要10項目（指示1～6）

【サイバーセキュリティリスクの管理体制構築】
- 指示1 サイバーセキュリティリスクの**認識、組織全体での対応方針の策定**
- 指示2 サイバーセキュリティリスク**管理体制の構築**
- 指示3 サイバーセキュリティ対策のための**資源（予算、人材等）確保**

【サイバーセキュリティリスクの特定と対策の実装】
- 指示4 サイバーセキュリティリスクの**把握とリスク対応に関する計画の策定**
- 指示5 サイバーセキュリティリスクに**効果的に対応する仕組みの構築**
- 指示6 PDCAサイクルによるサイバーセキュリティ対策の**継続的改善**

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 25

経営の重要10項目（指示7～10）

【インシデント発生に備えた体制構築】
指示7 インシデント発生時の**緊急対応体制の整備**
指示8 インシデントによる被害に備えた**事業継続・復旧体制の整備**

【サプライチェーンセキュリティ対策の推進】
指示9 ビジネスパートナーや委託先等を含めた**サプライチェーン全体の状況把握及び対策**

【ステークホルダーを含めた関係者とのコミュニケーションの推進】
指示10 サイバーセキュリティに関する**情報の収集、共有及び開示の促進**

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 26

指示1：サイバーセキュリティリスクの認識、組織全体での対応方針の策定

【ポイント】

- サイバーセキュリティリスクを経営者が責任を負うべき経営リスクとして認識し、組織全体としての対応方針（セキュリティポリシー）を策定させる。
- 策定した対応方針を対外的な宣言として公表させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 26

指示2：サイバーセキュリティリスク管理体制の構築

【ポイント】

- サイバーセキュリティリスクの管理に関する各関係者の役割と責任を明確にした上で、リスク管理体制を構築させる。
- サイバーセキュリティリスクの管理体制の構築にあたっては、組織内のガバナンスや内部統制、その他のリスク管理のための体制との整合を取らせる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 26

指示3：サイバーセキュリティ対策のための資源（予算、人材等）確保

【ポイント】

- サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討させ、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組ませる。
- 全ての役職員に自らの業務遂行にあたってセキュリティを意識させ、それぞれのサイバーセキュリティ対策に関するスキル向上のための人材育成施策を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 26

指示4：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

【ポイント】

- 事業に用いるデジタル環境、サービス及び情報を特定させ、それらに対するサイバー攻撃（過失や内部不正を含む）の脅威や影響度から、自組織や自ら提供する製品・サービスにおけるサイバーセキュリティリスクを識別させる。
- サイバー保険の活用や守るべき情報やデジタル基盤の保護に関する専門ベンダへの委託を含めたリスク対応計画を策定させ、対応後の残留リスクを識別させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 26

指示5：サイバーセキュリティリスクに効果的に対応する仕組みの構築

【ポイント】

- サイバーセキュリティリスクに対応するための保護対策として、防御・検知・分析の各機能を実現する仕組みを構築させる。
- 構築した仕組みについて、事業環境やリスクの変化に対応するための見直しを実施させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 27

指示6：PDCAサイクルによるサイバーセキュリティ対策の継続的改善

【ポイント】

- リスクの変化に対応し、組織や事業におけるリスク対応を継続的に改善させるため、サイバーセキュリティリスクの特徴を踏まえた PDCA サイクルを運用させる。
- 経営者は対策の状況を定期的に報告させること等を通じて問題の早期発見に努め、問題の兆候を認識した場合は改善させる。
- 株主やステークホルダーからの信頼を高めるため、改善状況を適切に開示させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 27

指示7：インシデント発生時の緊急対応体制の整備

【ポイント】

- 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT等）を整備させる。
- 被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。
- インシデント発生時の対応について、適宜実践的な演習を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 27

指示8：インシデントによる被害に備えた事業継続・復旧体制の整備

【ポイント】

- インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。
- 制御系も含めた BCP との連携等、組織全体として有効かつ整合のとれた復旧目標計画を定めさせる。
- 業務停止等からの復旧対応について、対象を IT 系・社内・インシデントに限定せず、サプライチェーンも含めた実践的な演習を実施させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 27

指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策

【ポイント】

- サプライチェーン全体にわたって適切なサイバーセキュリティ対策が講じられるよう、国内外の拠点、ビジネスパートナーやシステム管理の運用委託先等を含めた対策状況の把握を行わせる。
- ビジネスパートナー等との契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めるための適切な方策を検討させる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-1.】
第7章 - 27

指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進

【ポイント】

- 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。
- 入手した情報を有効活用するための環境整備をさせる。

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-2.】
第7章 - 28

サイバーセキュリティ経営ガイドラインの読み方（経営者）

役割

- 「3原則」の理解
- 重要10項目について、情報セキュリティ対策の責任者に指示を出す
- リーダーシップの発揮

認識すべきこと

- ERMにサイバー攻撃のリスクを含めること
- サプライチェーン上のリスクを認識すること
- サイバーセキュリティ対策は担当者に丸投げしてはいけない
- サイバーセキュリティ対策は投資と位置付けること

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-2.】
第7章 - 29

サイバーセキュリティ経営ガイドラインの読み方（担当幹部等）

役割

- 重要10項目を理解すること
- 経営者に対して適宜状況報告を行い、経営者が適切な判断を行うために必要な情報を提供すること

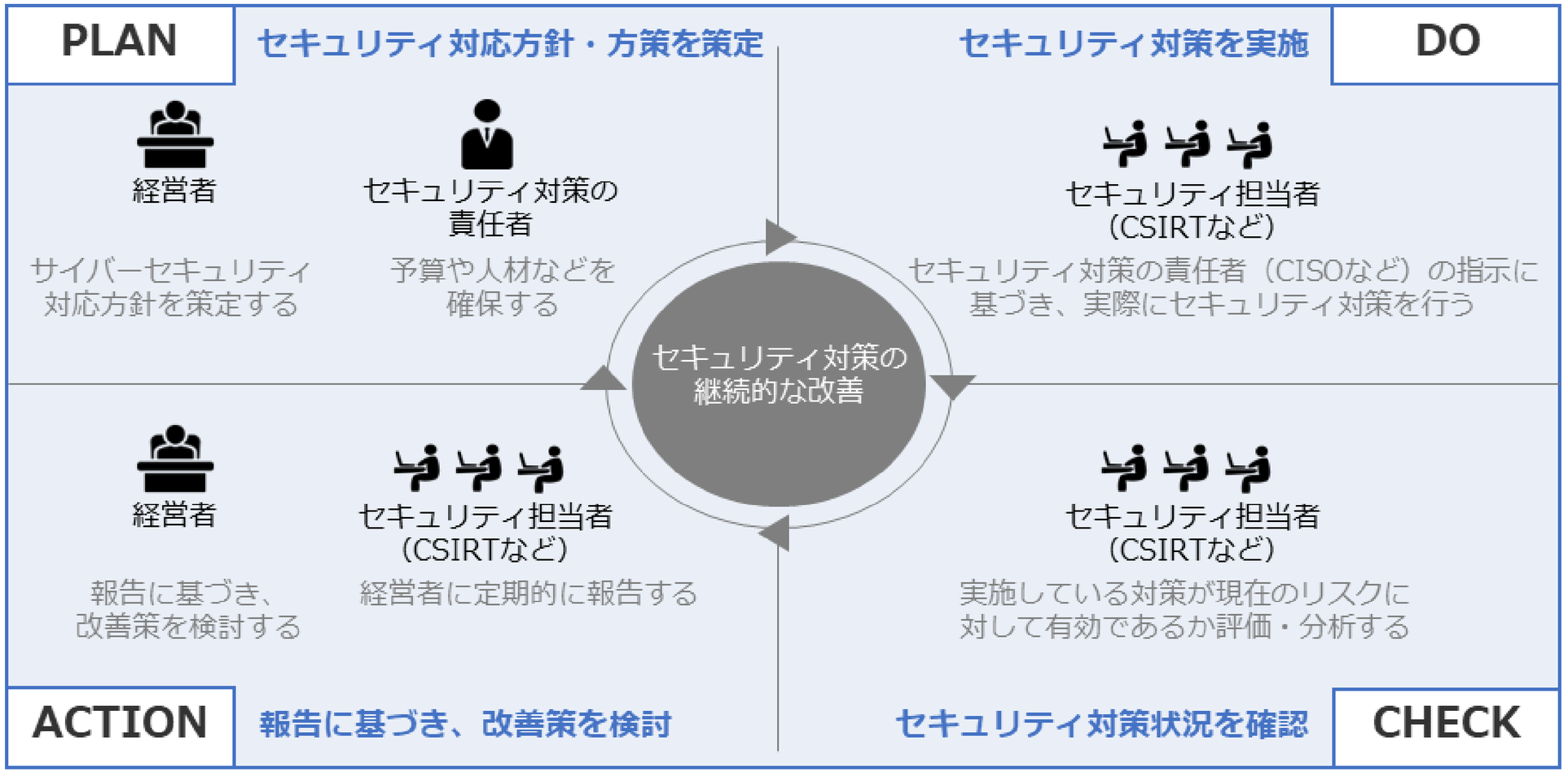
認識すべきこと

- 経営者から指示される内容に関して、より具体的な取組み方を検討し、セキュリティ担当者に対して指示をする必要があること

サイバーセキュリティ経営ガイドライン

【参照：テキスト7-5-3.】
第7章 - 30

サイバーセキュリティ経営ガイドラインの実践の流れ



サイバーセキュリティ経営ガイドラインの全体の流れ
（出典） 経済産業省「サイバーセキュリティ経営ガイドライン Ver3.0」を基に作成

１．セキュリティ対策基準の策定

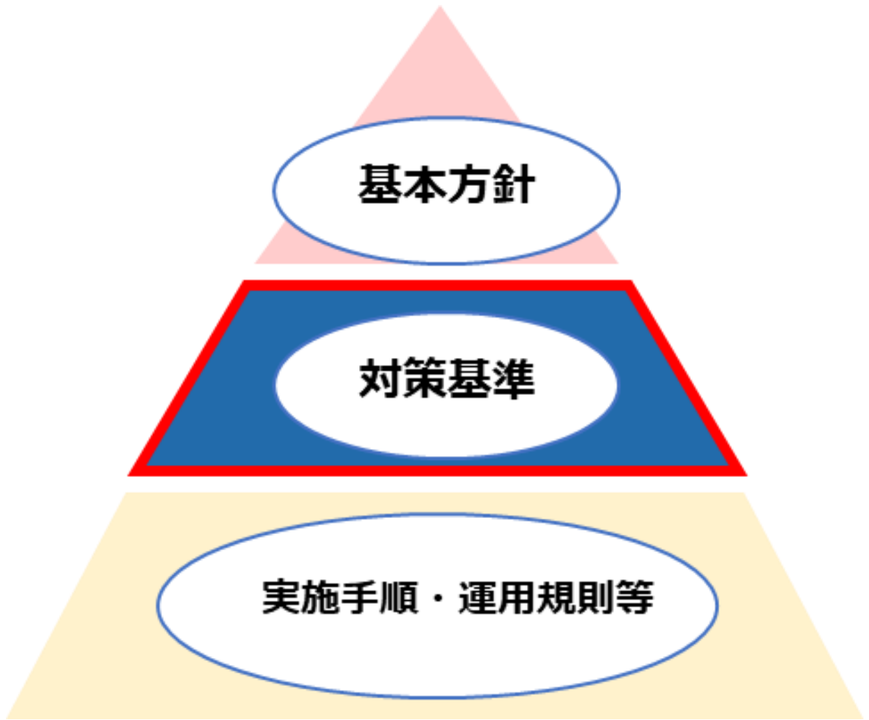
対策基準の策定

対策基準の策定

【参照：テキスト8-1-1.】
第8章 - 02

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”

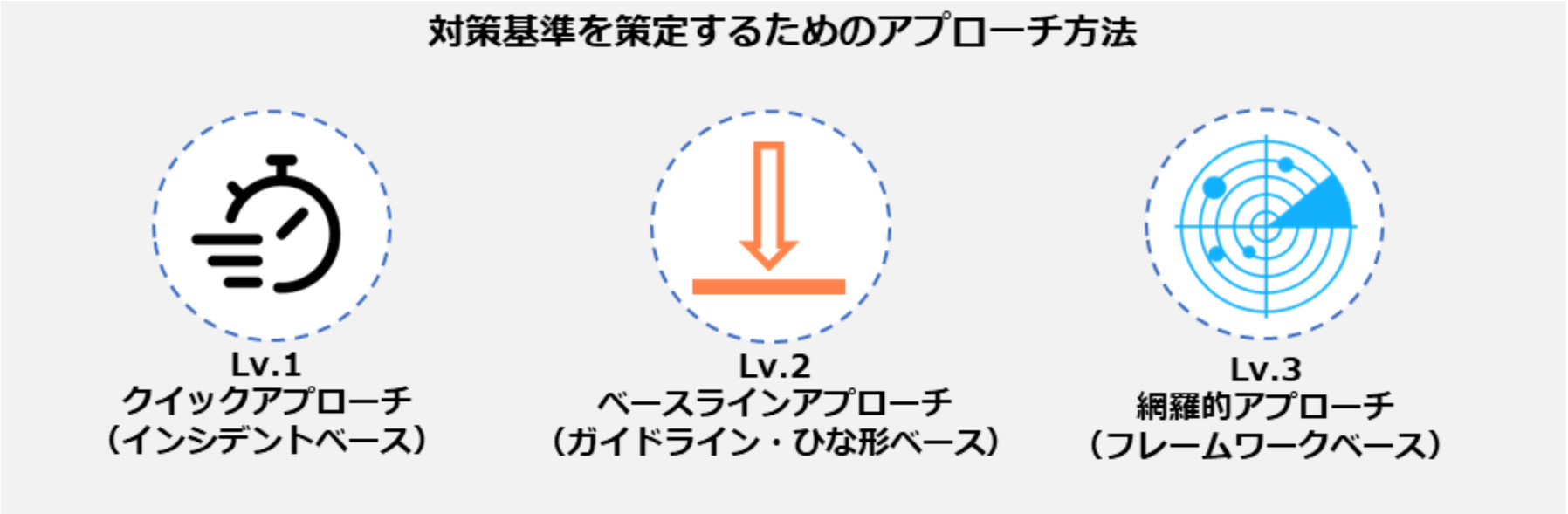
基本方針
情報セキュリティに対する組織の基本方針・宣言を記述する
対策基準
基本方針を実践するための具体的な規則を記述する
実施手順・運用規則等
対象者や用途によって必要な手続きを記述する

対策基準の策定

【参照：テキスト8-1-1.】
第8章 - 02

対策基準のアプローチ方法

- 企業の現状を鑑み、次の段階的なアプローチ方法がある
  - 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【推奨】



対策基準の策定

【参照：テキスト8-1-2.】
第8章 - 03

対策基準のアプローチ概要

アプローチ手法	特徴	想定される適用ケース
Lv.1 クイックアプローチ	• 即時の対応や緊急事態への対処に適したアプローチ手法。 • 様々なインシデント事例内容を参考にし、対策基準を策定。	• 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	• 組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。 • ガイドラインやひな形を参考とし、対策基準を策定。	• 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	• 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などの認証が可能なレベルを目指して、対策基準を策定。	• ISMSのフレームワークに沿った対策基準を策定する場合。

対策基準の策定

【参照：テキスト8-1-2.】
第8章 - 03

メリット・デメリット

アプローチ手法	メリット	デメリット
Lv.1 クイックアプローチ	• 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。 • 進行中の攻撃の拡大や影響を最小限に抑えられる。	• 詳細な分析や検討が不十分な場合がある。 • 短期的な解決策に偏りがちになる。
Lv.2 ベースラインアプローチ	• 組織全体で一貫性を確保できる。 • 最低基準となるセキュリティ対策を講じることができる。	• 追加のセキュリティ対策やリスクに対する適切な対応策を検討することが必要になる。
Lv.3 網羅的アプローチ	• 可能な限り多くの脅威や攻撃手法に対して対策を講じる。 • 予測できない脅威や新たな攻撃手法に対しても準備ができる状態を維持できる。	• 全体的な実施には時間がかかる。

対策基準の策定

【参照：テキスト8-1-2.】
第8章 - 04

Lv.1 クイックアプローチ

【例】ランサムウェアに対する対策基準を作る

記載項目	内容
1．対象とする脅威	ランサムウェアによる情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取等
2．組織的対策	• 組織としてのランサムウェア対応体制の確立 • インシデント対応体制を整備し対応する
3．人的対策	• メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを容易にしない • 提供元が不明なソフトウェアを実行しない • 適切な報告/連絡/相談を行う
4．物理的対策	• 適切なバックアップ運用を行う
5．技術的対策	• 公開サーバーへの不正アクセス対策 • 共有サーバー等へのアクセス権の最小化と管理の強化 • 多要素認証の設定を有効にする • サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う

(出典) IPA「情報セキュリティ10大脅威 2023」を基に作成

対策基準の策定

【参照：テキスト8-1-2.】
第8章 - 05

Lv.2 ベースラインアプローチ

【例】 IPA「情報セキュリティ関連規程」を活用した対策基準

1.情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

1	組織的対策	改訂	20yy.mm.dd
適用範囲	全社・全従業員		

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
システム管理者	社内の情報システムに必要な情報セキュリティ対策の検討・導入を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。

(出典) IPA「情報セキュリティ関連規程（サンプル）」を基に作成

対策基準の策定

【参照：テキスト8-1-2.】
第8章 - 06

Lv.3 網羅的アプローチ

【例】 ISMSフレームワークを活用した対策基準

93種の管理策ごとに対策基準を策定する。

5.組織的管理策	5.24 情報セキュリティインシデント管理の計画および準備
5.1 情報セキュリティのための方針群	5.25 情報セキュリティ事象の評価および決定
5.2 情報セキュリティの役割および責任	5.26 情報セキュリティインシデントへの対応
5.3 職務の分離	5.27 情報セキュリティインシデントからの学習
5.4 経営陣の責任	5.28 証拠の収集
5.5 関係当局との連絡	5.29 事業の中断・阻害時の情報セキュリティ
5.6 専門組織との連絡	5.30 事業継続のためのICTの備え
5.7 脅威インテリジェンス	5.31 法令、規制および契約上の要求事項
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	5.32 知的財産権
5.9 情報およびその他の関連資産の目録	5.33 記録の保護
5.10 情報およびその他の関連資産の利用の許容範囲	5.34 プライバシーおよびPIIの保護
5.11 資産の返却	5.35 情報セキュリティの独立したレビュー
5.12 情報の分類	5.36 情報セキュリティのための方針群、規則および標準の順守
5.13 情報のラベル付け	5.37 操作手順書
5.14 情報転送	6.人的管理策
5.15 アクセス制御	6.1 選考
5.16 識別情報の管理	6.2 雇用条件
5.17 認証情報	6.3 情報セキュリティの意識向上、教育および訓練
5.18 アクセス権	6.4 懲戒手続き
5.19 供給者関係における情報セキュリティ	6.5 雇用の終了又は変更後の責任
5.20 供給者との合意におけるセキュリティの取扱い	6.6 秘密保持契約又は守秘義務契約
5.21 ICTサプライチェーンにおける情報セキュリティの取扱い	6.7 リモートワーク
5.22 供給者のサービス提供の監視およびレビューおよび変更管理	6.8 情報セキュリティ事象の報告
5.23 クラウドサービス利用における情報セキュリティ	

7.物理的管理策	8.10 情報の削除
7.1 物理的セキュリティ境界	8.11 データマスキング
7.2 物理的入退	8.12 データ漏えいの防止
7.3 オフィス、部屋および施設のセキュリティ	8.13 情報のバックアップ
7.4 物理的セキュリティの監視	8.14 情報処理施設の冗長性
7.5 物理的および環境的脅威からの保護	8.15 ログ取得
7.6 セキュリティを保つべき領域での作業	8.16 監視活動
7.7 クリアデスク・クリアスクリーン	8.17 クロックの同期
7.8 装置の設置および保護	8.18 特権的なユーティリティプログラムの使用
7.9 構外にある装置および資産のセキュリティ	8.19 運用システムに関わるソフトウェアの導入
7.10 記憶媒体	8.20 ネットワークのセキュリティ
7.11 サポートユーティリティ	8.21 ネットワークサービスのセキュリティ
7.12 ケーブル配線のセキュリティ	8.22 ネットワークの分離
7.13 装置の保守	8.23 ウェブ・フィルタリング
7.14 装置のセキュリティを保った処分又は再利用	8.24 暗号の使用
8.技術的管理策	8.25 セキュリティに配慮した開発のライフサイクル
8.1 利用者エンドポイント機器	8.26 アプリケーションのセキュリティの要求事項
8.2 特権的アクセス権	8.27 セキュリティに配慮したシステムアーキテクチャおよびシステム構築の原則
8.3 情報へのアクセス制限	8.28 セキュリティに配慮したコーディング
8.4 ソースコードへのアクセス	8.29 開発および受け入れにおけるセキュリティ試験
8.5 セキュリティを保った認証	8.30 外部委託による開発
8.6 容量・能力の管理	8.31 開発環境、試験環境および運用環境の分離
8.7 マルウェアに対する保護	8.32 変更管理
8.8 技術的ぜい弱性の管理	8.33 試験情報
8.9 構成管理	8.34 監査試験中の情報システムの保護

2. 管理策のテーマと属性

管理策の分類と構成

管理策の分類と構成

【参照：テキスト9-1-1.】
第9章 - 02

管理策：ISO/IEC27002

管理策
リスク対応のための対策のこと

ISO/IEC27002
ISO/IEC27001に記載されている要求事項を基に、さらに具体的なISMSの管理策を示した規格のこと。

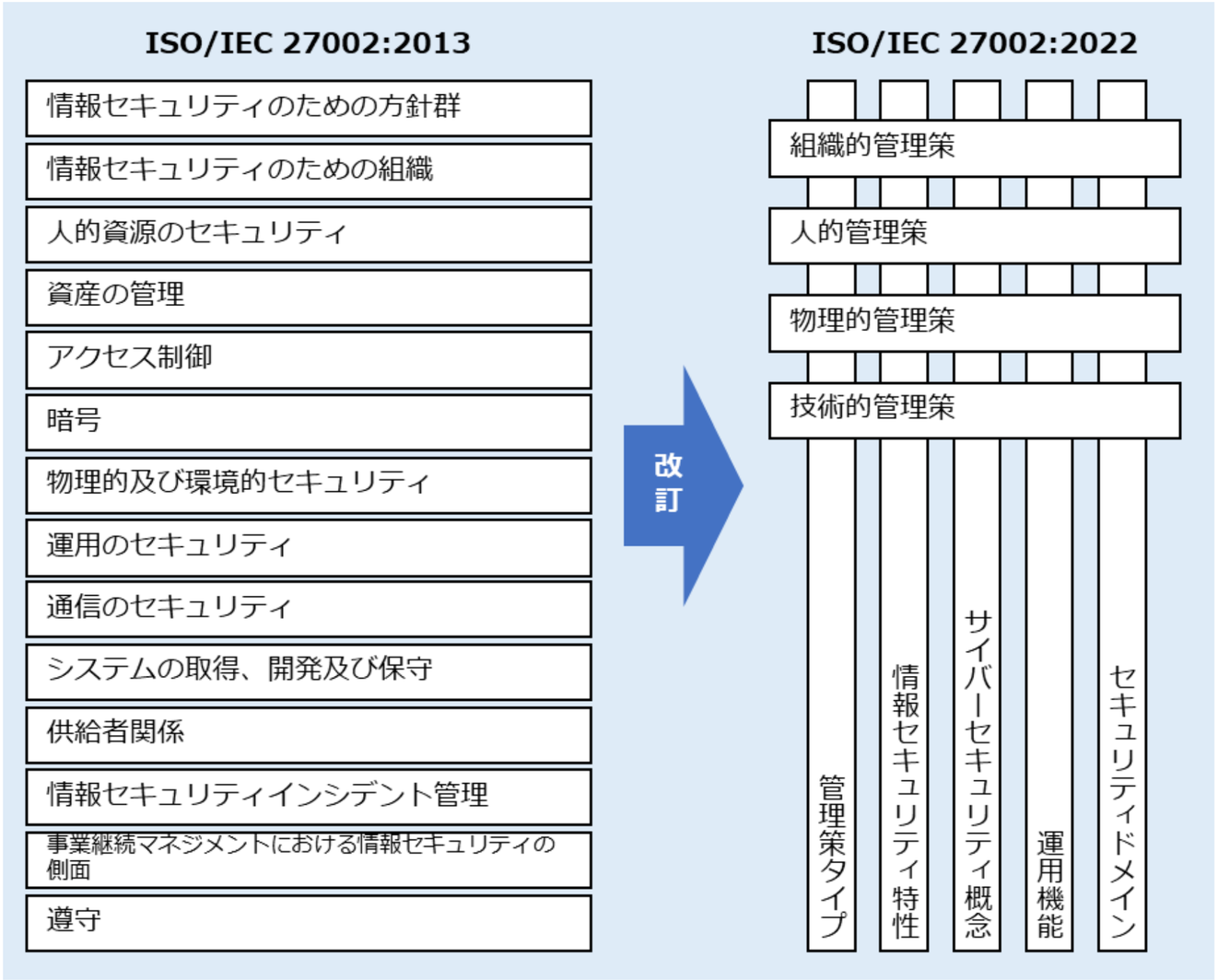
管理策の分類と構成

【参照：テキスト9-1-1.】
第9章 - 02

ISMS：2022年版

2013年版からの改定内容

- 管理策の項目数と章立てが変更され、テーマごとにカテゴリ分けされた
- 新たに属性の概念が導入された



管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 03

テーマと属性

- ISO/IEC 27002の箇条5～8では、管理策が4つの分類（組織的・人的・物理的・技術的）に分けられ、これをテーマと呼ぶ。
- 各管理策に属性が付与し、より細かく見ることができる。

管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 03

属性について

他の組織や団体が発行するガイドラインなどの考え方を取り入れているものもある

管理策の属性	属性値	関連するガイドライン等
管理策タイプ	予防、検知、是正	ー
情報セキュリティ特性	機密性、完全性、可用性	ISO/IEC 27001
サイバーセキュリティ概念	識別、防御、検知、対応、復旧	サイバーセキュリティフレームワーク
運用機能	ガバナンス、資産管理、情報保護、人的資源のセキュリティ、物理的セキュリティ、システムおよびネットワークセキュリティ、アプリケーションのセキュリティ、セキュリティを保った構成、識別情報およびアクセスの管理、脅威および脆弱性の管理、継続、供給者関係のセキュリティ、法および遵守、情報セキュリティ事象管理、情報セキュリティ保証	ISO/IEC 27002:2013
セキュリティドメイン	ガバナンスおよびエコシステム、保護、防御、対応力	ー

管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 04

各テーマの管理策例示（組織的）

【組織的管理策】5.2 情報セキュリティの役割及び責任

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
#予防	#機密性 #完全性 #可用性	#識別	#ガバナンス	#ガバナンス及びエコシステム #対応力

管理策	情報セキュリティの役割及び責任を、組織の要求に従って定め、割り当てることが望ましい。
目的	組織内における情報セキュリティの実施、運用及び管理のために、定義され、承認され、理解される構造を確立するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 04

各テーマの管理策例示（人的）

【人的管理策】6.8 情報セキュリティ事象の報告

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
#検知	#機密性 #完全性 #可用性	#検知	#情報セキュリティ事象管理	#防御

管理策	組織は、要員が発見した又は疑いを持った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するための仕組みを設けることが望ましい。
目的	要員が、特定可能な情報セキュリティ事象を時機を失せず、一貫性をもって効果的に報告することを支援するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 05

各テーマの管理策例示（物理的）

【物理的管理策】7.4 物理的セキュリティの監視

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
#予防 #検知	#機密性 #完全性 #可用性	#防御 #検知	#物理的セキュリティ	#保護 #防御

管理策	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することが望ましい。
目的	認可されていない物理的アクセスを検知し、抑止するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

管理策の分類と構成

【参照：テキスト9-1-2.】
第9章 - 05

各テーマの管理策例示（技術的）

【技術的管理策】8.16 監視活動

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
#検知 #是正	#機密性 #完全性 #可用性	#検知 #対応	#情報セキュリティ事象管理	#防御

管理策	情報セキュリティインシデントの可能性がある事象を評価するために、ネットワーク、システム及びアプリケーションについて異常な行動・動作がないか監視し、適切な処置を講じることが望ましい。
目的	異常な行動・動作及び潜在する情報セキュリティインシデントを検出するため。

（出典）MSQA「ISO/IEC 27002:2022 対応　情報セキュリティ管理策実践ガイド」を基に作成

3. 脅威、脆弱性、リスクの定義と関係性

用語の定義および関係性と識別方法

用語の定義および関係性と識別方法

【参照：テキスト10-1-1.】
第10章 - 02

リスクマネジメントの理解に必要な用語の定義

用語	意味
リスク	目的に対する不確かさの影響
脅威	システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因
脆弱性	一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点
管理策	リスクを修正する対策
保護要求事項	明示されている、通常暗黙のうちに了解されている又は義務として要求されている、ニーズ又は期待
資産	企業や組織などで保有している情報全般のこと。顧客情報や販売情報などの情報自体に加えて、ファイルやデータベースといったデータ、CD-ROMやUSB メモリなどのメディア、そして紙の資料も情報資産に含まれる

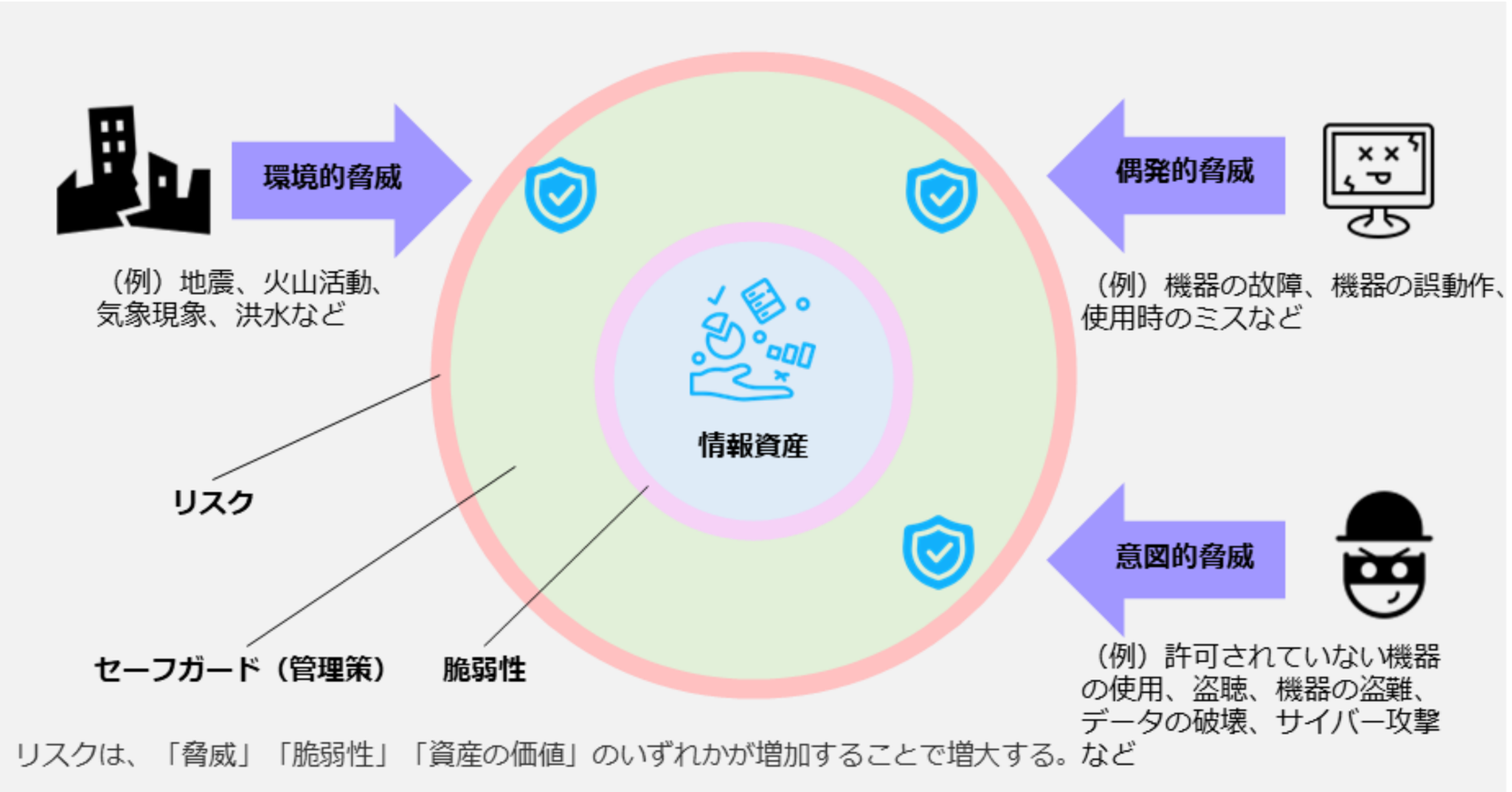
（出典）総務省「安心してインターネットを使うために 国民のためのサイバーセキュリティサイト 用語辞典」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-1.】
第10章 - 02

脅威、脆弱性、情報資産、セーフガード、リスクの関係

- 図にすると以下のようになる



脅威、脆弱性、情報資産、セーフガード、リスクの関係図

用語の定義および関係性と識別方法

【参照：テキスト10-1-1.】
第10章 - 03

【例】業務用ノートPCのリスクマネジメント

- ノートPCに対して、各要素について検討する

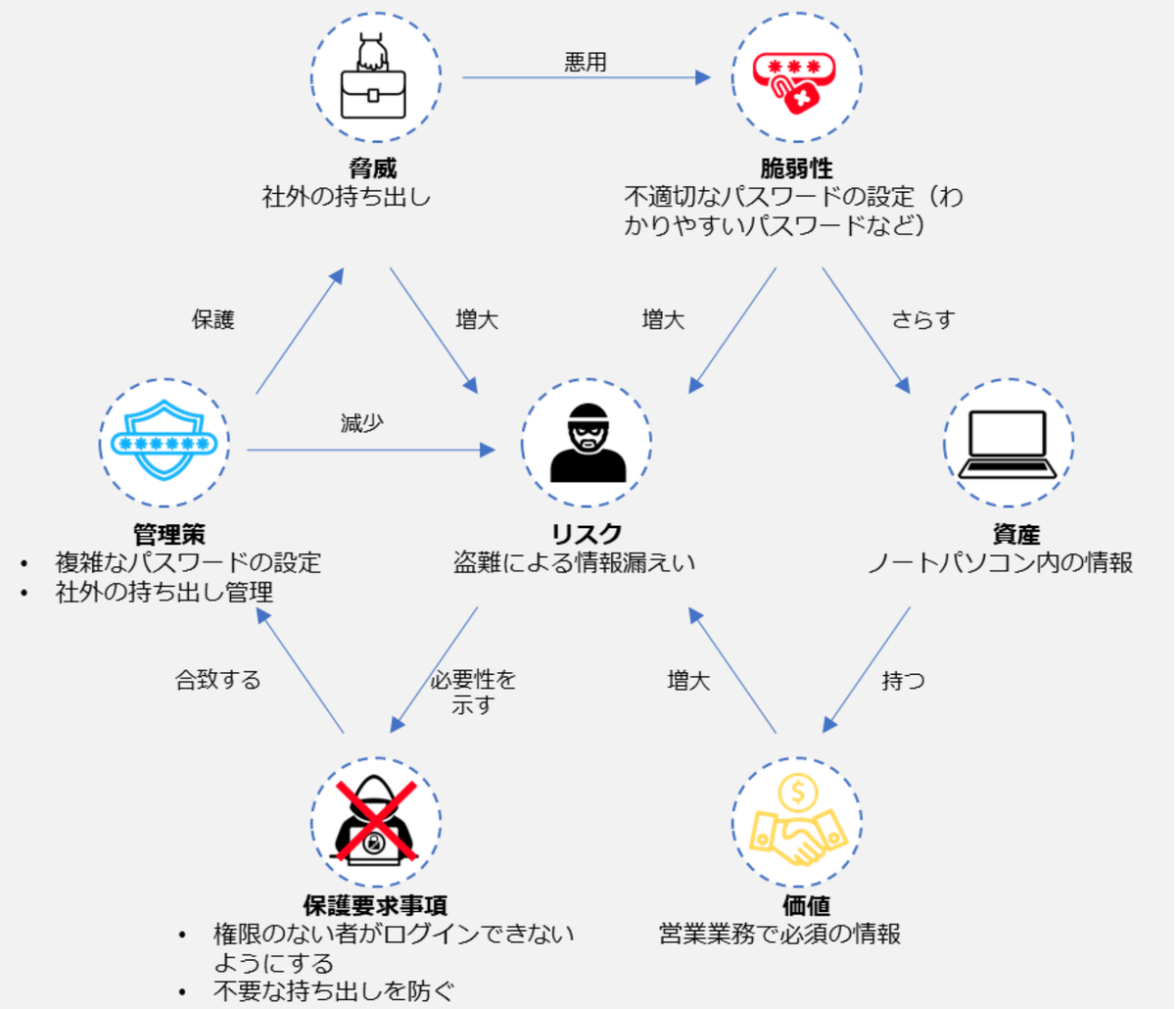
要素	内容
資産	ノートPC内の情報（データ）
価値	営業の業務で必須の情報
脅威	社外への持ち出し
リスク	盗難による情報漏えい
脆弱性	不適切なパスワードの設定（わかりやすい設定など）
保護要求事項	• 権限のないものがログインできないようにする • 不要な持ち出しを防ぐ
管理策	• 複雑なパスワードの設定（8.5 セキュリティを保った認証） • 社外の持ち出し管理（7.9 構外にある装置及び資産のセキュリティ（構外にある資産）

用語の定義および関係性と識別方法

【参照：テキスト10-1-1.】
第10章 - 03

【例】業務用ノートPCのリスクマネジメント

- 関係性は次の通り



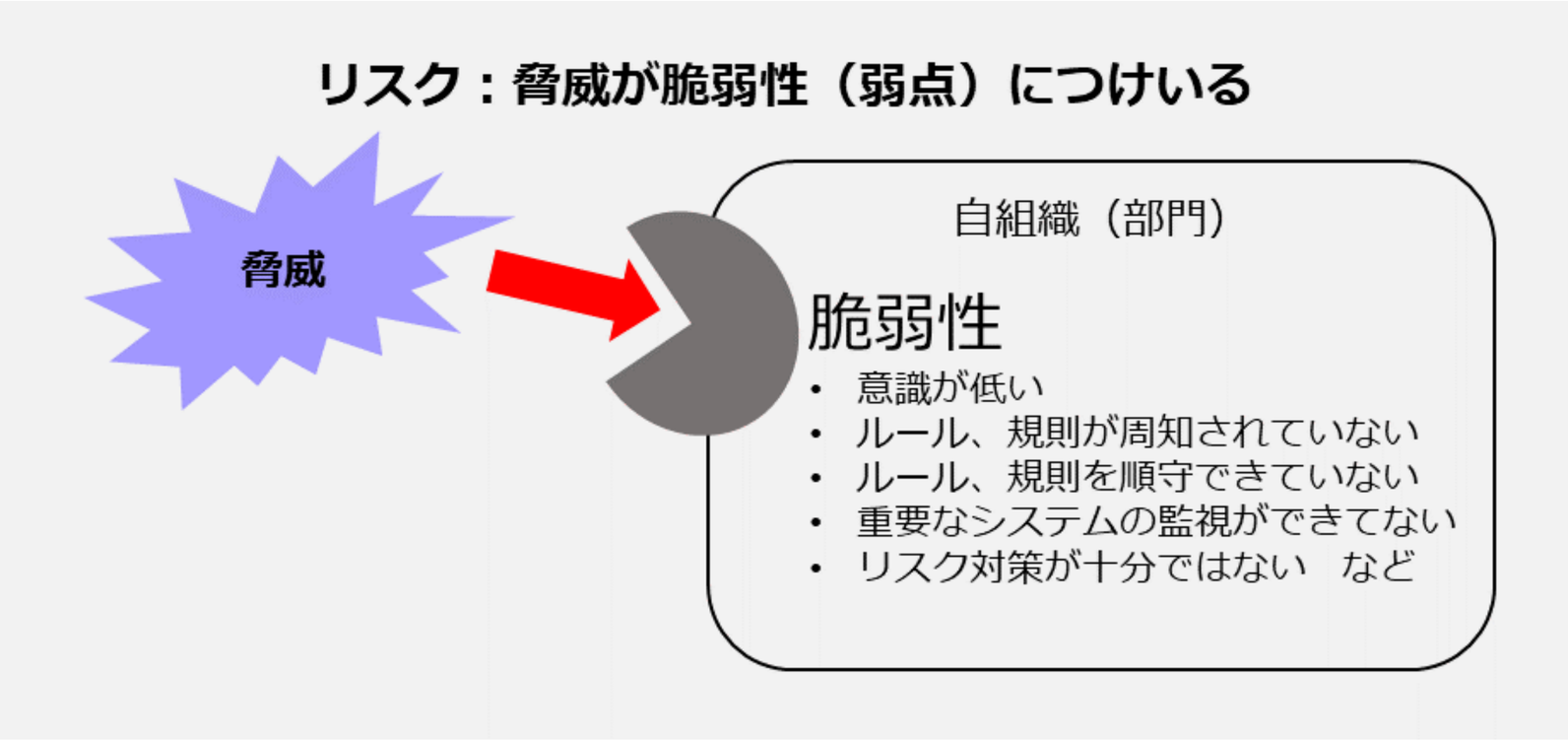
脆弱性、リスクの関係の事例

用語の定義および関係性と識別方法

【参照：テキスト10-1-2.】
第10章 - 04

脅威の識別

- 脅威は「脆弱性」につけいり顕在化することで事故を起こす。



脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-2.】
第10章 - 05

脅威の種類

- 脅威を区別することで、セキュリティ対策を整理しやすくなる

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)		被害：建物倒壊や火災による業務停止 対策：地震発生の可能性が低い場所を選択する、 災害からの回復対策を重視する
人為的脅威	意図的脅威 （Deliberate ➡ D）	被害：内部者による企業秘密の漏洩 対策：漏洩者を罰し、場合により損害賠償請求を行う 規程の明示と教育は抑止的対策の実施 漏洩の早期検知
	偶発的脅威 （Accidental ➡ A）	被害：入力ミスなどが原因の損害 対策：入力ミス防止の技術対策 2回入力 値の範囲制限 チェックデジットやチェックサムの設定

脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-2.】
第10章 - 05

脅威の洗い出し

- 会社の資産に対し、脅威の識別を実施する
- 意図的脅威は、次の観点から判断する
  - 攻撃の動機や攻撃に必要なスキル
  - 利用可能なリソース
  - 資産の特性や魅力
  - 資産の脆弱性
- 偶発的脅威は次の観点から判断する
  - 人為的なミス
  - 誤動作

脅威の分類と、被害例と対策
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-2.】
第10章 - 04

脅威の洗い出し

- 脅威を区別することで、セキュリティ対策を整理しやすくなる

類型	脅威	原因
物理的損傷	火災、水害、汚染、大事故、機器や媒体の破壊、粉塵、腐食、凍結	A, D, E
自然現象	気候、地震、火山活動、気象現象、洪水	E
重要なサービスの喪失	空調や給水システムの故障/電気通信機器の故障	A, D
	電力供給の停止	A, D, E
情報を危うくすること	遠隔スパイ行為、盗聴、媒体や文章の盗難、機器の盗難、再利用又は廃棄した媒体からの復元、ハードウェアの改ざん、位置検知	D
	漏洩・信頼できない情報源からのデータ・ソフトウェアの改ざん	A, D
技術的な故障	機器の故障、機器の誤動作、ソフトウェアの誤作動	A
	情報システムの飽和、情報システムの保守に関する違反	A, D
許可されていない行為	許可されていない機器の使用、ソフトウェアの不正コピー、データの破壊、データの違法な処理	D
	海賊版又は（不正）コピーソフトウェアの使用	A, D

脅威の一覧表の例
（出典）「ISO/IEC 27005」を基に作成

A：偶発的脅威（Accidental）
D：意図的脅威（Deliberate）
E：環境的脅威（Environmental）

用語の定義および関係性と識別方法

【参照：テキスト10-1-3.】
第10章 - 06

脆弱性の識別

- 脆弱性を減らすためには適切な管理策の実施が必要
- 脆弱性は管理策の欠如を意味する
  - 例：
    脆弱性：アクセス権の誤った割り当て
    管理策：アクセス権の適切な設定
- 脆弱性は資産の性質から考えると識別しやすくなる
  - 例：クラウドサービス
    特性：インターネットがあればどこでも利用可能
    脆弱性：インターネットからの不正アクセス

用語の定義および関係性と識別方法

【参照：テキスト10-1-3.】
第10章 - 06

脆弱性の識別例

類型	脆弱性	脅威の例
ハードウェア	記憶媒体の不十分な保守/不適当な設置	システムの保守に関する違反
	定期的な交換計画の欠如	機器や媒体の破壊
	湿気、ホコリ、汚れに対する影響の受けやすさ	粉塵（ダスト）、腐食、凍結
	有効な構成変更管理の欠如	使用時のミス
	電圧の変化に対する影響の受けやすさ	電力供給の停止
	温度変化に対する影響の受けやすさ	気象現象
	保護されない保管	媒体や文書の盗難
	廃棄時の注意の欠如	媒体や文書の盗難
	管理されないコピー作成	媒体や文書の盗難

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-3.】
第10章 - 06

脆弱性の識別例

類型	脆弱性	脅威の例
ソフトウェア	離席時にログアウトしない	権限の濫用
	適切に削除されていない記憶媒体の処理または再利用	権限の濫用
	監査証跡の欠如	権限の濫用
	アクセス権の誤った割り当て	権限の濫用
	複雑なユーザーインタフェース	使用時のミス
	文書化の欠如	使用時のミス
	ユーザの認識及び認証メカニズムの欠如	権限の詐称
	不十分なパスワード管理	権限の詐称
	不要なサービスが実行可能	データの違法な処理
	開発者のための不明確又は不完全な仕様書	ソフトウェアの誤作動
	効率的な変更管理の欠如	ソフトウェアの誤作動
	管理されていないソフトウェアのダウンロード及び使用	ソフトウェアの改ざん
	バックアップコピーの欠如	ソフトウェアの改ざん

脆弱性の識別例
（出典）「ISO/IEC 27005」を基に作成

用語の定義および関係性と識別方法

【参照：テキスト10-1-3.】
第10章 - 06

脆弱性を識別する際に参考になる情報

- ISO/IEC 27001:2022の附属書A「管理目的及び管理策」
- ISO/IEC 27002:2022の管理策
- 情報セキュリティ管理基準　など

１．リスクマネジメント

リスクマネジメント：概要

リスクマネジメント：リスクアセスメント

リスクマネジメント：リスク対応

リスクマネジメント：概要

【参照：テキスト11-1-1.】
第11章 - 02

リスクマネジメントプロセス（ISO31000）

リスクマネジメントとは

存在する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したり低減したりするプロセス全体のこと

ISO31000では

原則

枠組み

プロセス

リスクマネジメント：概要

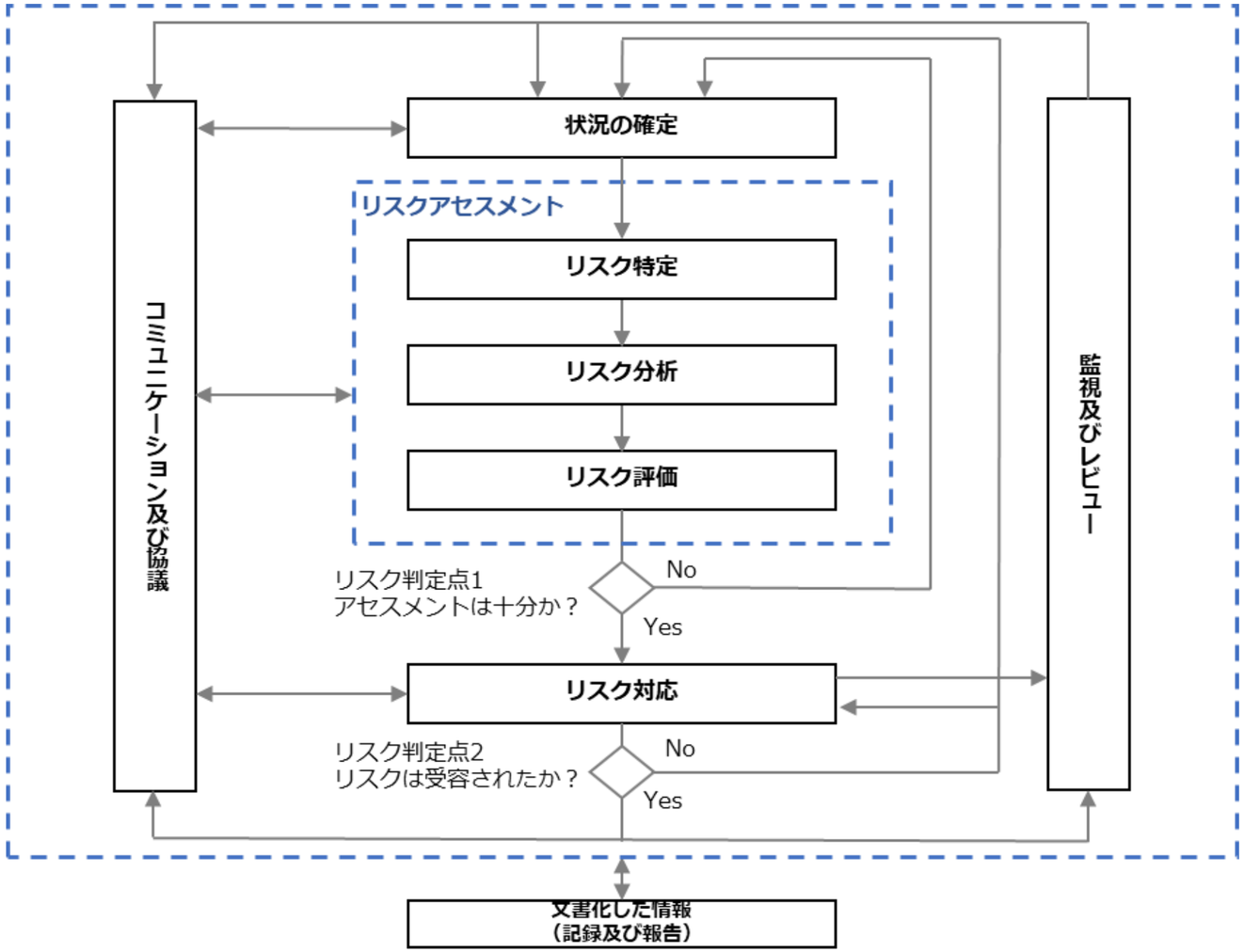
【参照：テキスト11-1-1.】
第11章 - 02

リスクマネジメントの3要素

要素	概要
原則	リスクマネジメントを実施する際に、組織が取り組むべき事項。 「価値の創出および保護」を中心に、次の８つの要素で構成されている。 「統合」「体系化及び包括」「組織への適合」「包含」「動的」 「利用可能な最善の情報」「人的及び文化的要因」「継続的改善」
枠組み	リスクマネジメントを組織全体に定着させるための仕組み。 「リーダーシップおよびコミットメント」を中心に、次の５つの要素で構成されている。 「統合」「設計」「実施」「評価」「改善」
プロセス	リスクマネジメントに取り組む上で実施すべき一連の活動。 次の６つの要素で構成されている。 「コミュニケーション及び協議」「適用範囲、組織の状況及び基準」 「リスクアセスメント」「リスク対応」「モニタリング及びレビュー」 「記録作成及び報告」

リスクマネジメント：概要
情報セキュリティリスクマネジメント（ISO/IEC27005）

【参照：テキスト11-1-2.】
第11章 - 03

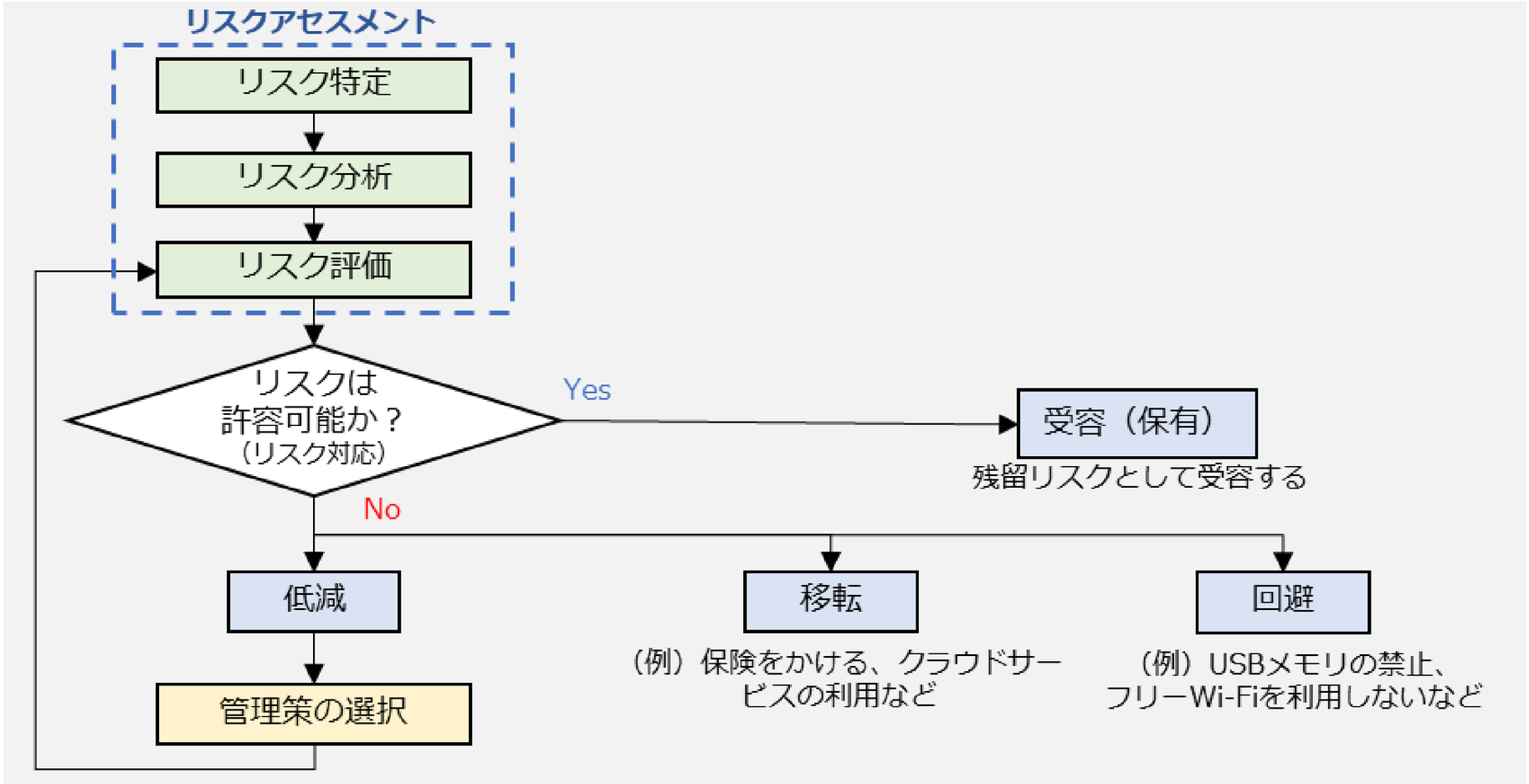


情報セキュリティマネジメントプロセスの概要
（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスクマネジメント：概要

【参照：テキスト11-1-2.】
第11章 - 04

情報セキュリティリスクマネジメント（ISO/IEC27005）

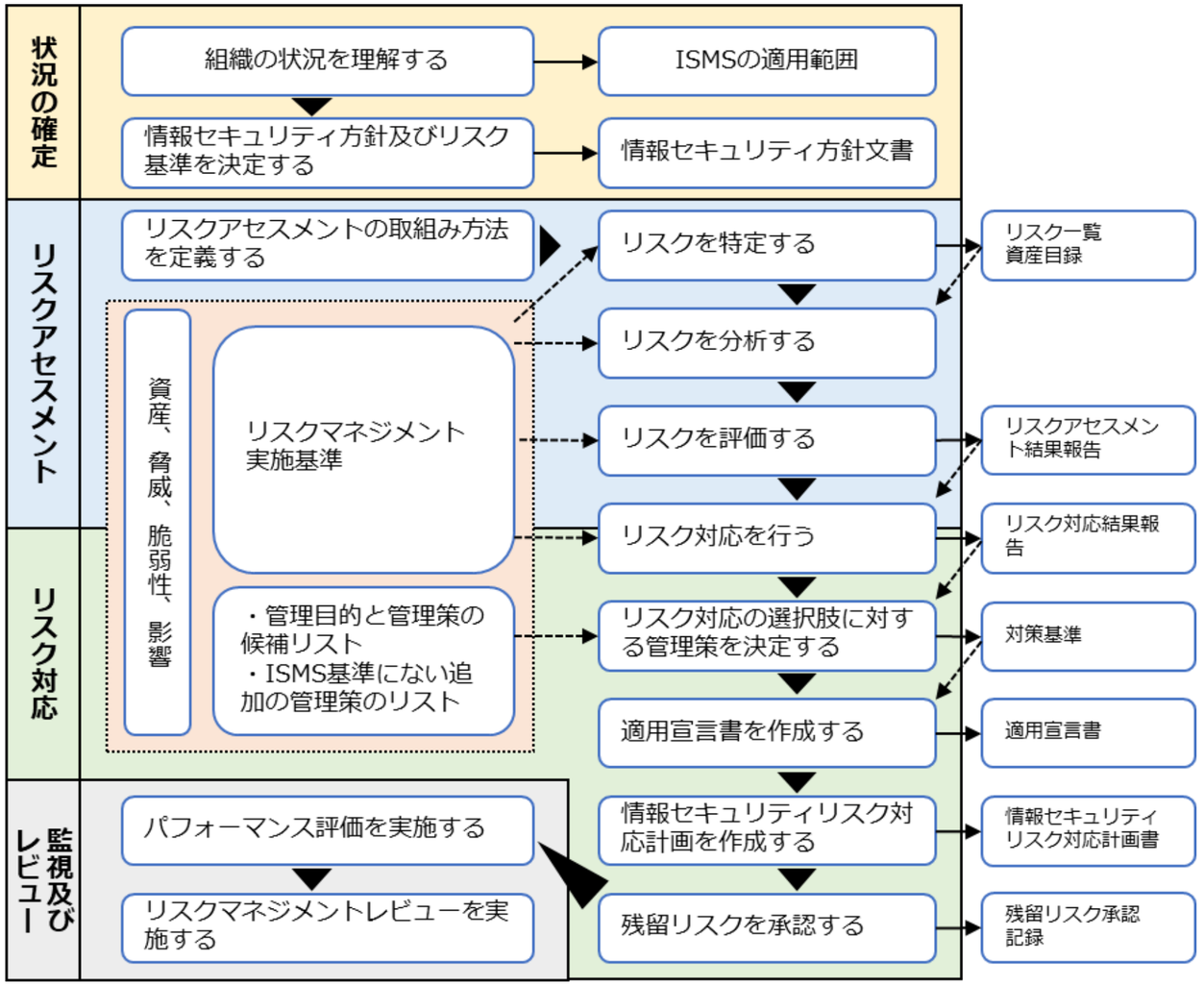


リスクマネジメント全体の流れと、リスク対応の選択プロセス

リスクマネジメント：概要

【参照：テキスト11-1-3.】
第11章 - 05

ISO/IEC 27001におけるリスクマネジメント手順



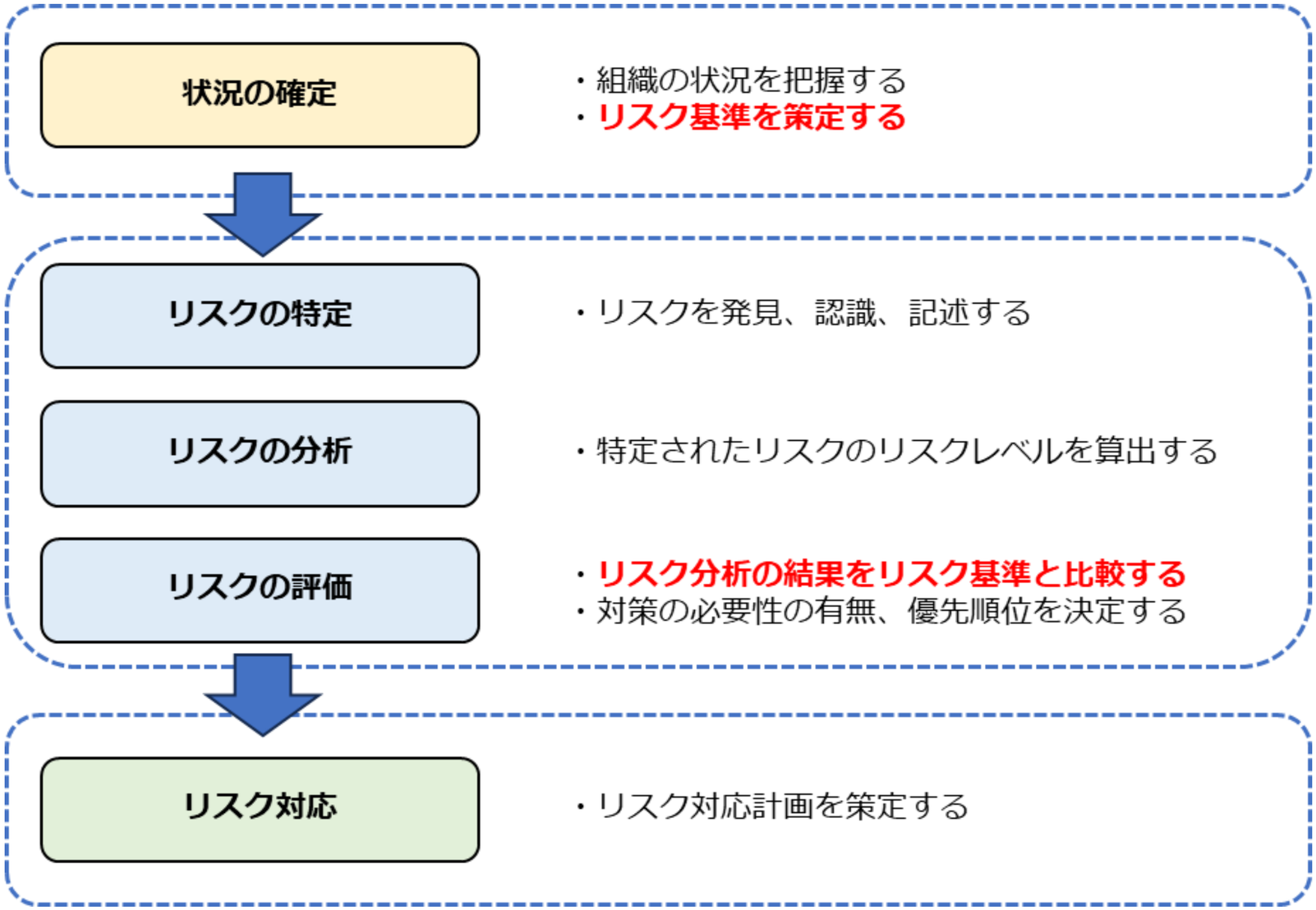
ISMSにおけるリスクアセスメントおよびリスク対応に関する作業の概要

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-1.】
第11章 - 06

リスク基準の確立

必要なリスク基準



リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 07

リスク特定

アプローチ手法と特徴

アプローチ手法	概要
資産ベースのアプローチ	• 資産、脅威及び脆弱性の検査を通じてリスクを特定しアセスメントを行う。 • 資産は、その種類及び優先度に従って主要資産及び支援資産として特定できる。 • 脅威は、資産の脆弱性につけ込み、対応する情報の機密性、完全性または可用性を侵害する。 • 資産のリストを作成することが望ましい。
事象ベースのアプローチ	• 事象及び結果の評価を通じてリスクを特定し、アセスメントを行う。 • 事象及び結果は、トップマネジメントから見た懸念、リスク所有者及び組織の状況を決定する際に特定された要求事項によって発見できる。

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 07

リスク特定

アプローチ手法のメリット・デメリット

アプローチ手法	メリット	デメリット
資産ベースのアプローチ	• 資産、脅威及び脆弱性のすべての有効な組合せをISMSの適用範囲で列挙することができれば、理論上はすべてのリスクが特定される。	• 情報資産が増えたときに、資産のリストの行数が多くなる。 • 同様のリスクを繰り返し記載したりしなければならない場合がある。
事象ベースのアプローチ	• 詳細なレベルで資産を特定することに多大な時間を費やすことなく、高いレベルまたは戦略的なシナリオを確立することができる。	• 網羅性において、資産ベースのアプローチに劣る。

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 07

リスク特定

リスク所有者の特定

- 特定されたリスクに対し、リスク所有者を関連付ける。
- リスク所有者は、トップマネジメント、セキュリティ委員会、プロセス所有者、機能所有者、部門マネージャーおよび資産所有者など、リスクマネジメントに権限を持つ人とする（通常、組織内で一定の権限を持つ人が選ばれる）。

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 08

リスク特定（資産ベースのアプローチ）

アプローチ手法

情報資産の洗い出し

↓

機密性・完全性・可用性が損なわれた場合の影響度を評価

↓

影響度の評価をもとに重要度を算定

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 08

リスク特定（資産ベースのアプローチ）

情報資産の洗い出し（例）

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	事務所PC
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部長	人事部	書類
経理	給与システムデータ	税務署提出用 源泉徴収票	給与計算担当	経理部長	人事部	事務所PC
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	経理部長	総務部	書類
経理	発行済請求書控え	当社発行の請求書の控え（過去3年分）	総務部	経理部長	総務部	書類
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部長	営業部	可搬電子媒体
営業	受注伝票	受注伝票（過去10年分）	営業部	営業部長	営業部	社内サーバ
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部長	営業部	書類

資産目録の例
（出典）IPA 「リスク分析シート」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 09

リスク特定（資産ベースのアプローチ）

資産目録作成の効率化

- 情報資産を、「主要／事業資産」と「支援資産」のカテゴリに分類する

資産種別	概要
主要／事業資産	「主要/事業資産」とは、「組織にとって価値のある情報又はプロセス」のことです。主要資産は、「事業プロセス及び事業活動」と「情報」の2つに分けられます。
支援資産	「支援資産」とは、「1つ以上の事業資産の基礎となる情報システムの構成要素」のことです。

（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
機密性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）
		守秘義務の対象や限定提供データとして指定されている 漏えいすると取引先や顧客に大きな影響がある	• 取引先から秘密として提供された情報 • 取引先の製品・サービスに関わる非公開情報
		自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため） 漏えいすると自社に深刻な影響がある	• 自社の独自技術・ノウハウ • 取引先リスト • 特許出願前の発明情報
	2	漏えいすると事業に大きな影響がある	• 見積書、仕入価格など顧客（取引先）との商取引に関する情報
	1	漏えいしても事業にほとんど影響はない	• 自社製品カタログ • ホームページ掲載情報

（情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「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」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
完全性	3	法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている	• 個人情報（個人情報保護法で定義） • 特定個人情報（マイナンバーを含む個人情報）
		改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある	• 取引先から処理を委託された会計情報 • 取引先の口座情報 • 顧客から製造を委託された設計図
	2	改ざんされると事業に大きな影響がある	• 自社の会計情報 • 受発注・決済・契約情報 • ホームページ掲載情報
	1	改ざんされても事業にほとんど影響はない	• 廃版製品カタログデータ

（情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「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」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 10

リスク特定（資産ベースのアプローチ）

機密性・完全性・可用性が損なわれた場合の影響度を評価

評価値		評価基準	該当する情報の例
可用性	3	利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある	• 顧客に提供しているECサイト • 顧客に提供しているクラウドサービス
	2	利用できなくなると事業に大きな影響がある	• 製品の設計図 • 商品・サービスに関するコンテンツ（インターネット向け事業の場合）
	1	利用できなくなっても事業にほとんど影響はない	• 廃版製品カタログ

情報資産の機密性・完全性・可用性に基づく重要度の定義
（出典）IPA 「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」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 11

リスク特定（資産ベースのアプローチ）

影響度の評価をもとに重要度を算定

重要度	情報資産の価値・事故の影響の大きさ
3	事故が起きると、 「 法的責任を問われる」 「 取引先、顧客、個人に大きな影響がある」 「 事業に深刻な影響を及ぼす」 など、企業の存続を左右しかねない
2	事故が企業の事業に重大な影響を及ぼす
1	事故が発生しても事業にほとんど影響はない

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 11

リスク特定（資産ベースのアプローチ）

重要度の判断例

要素	情報資産の価値・事故の影響の大きさ	評価値
機密性	公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない	1
完全性	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられたりすると顧客や閲覧者に被害が発生し、信用を失う	3
可用性	サーバの障害などでアクセスできなくなると、来店客が減少し、売上も減少する	3

完全性と可用性の評価値3が最大値なので、重要度は評価値：3

重要度の判断例
（出典）IPA 「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」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 12

リスク特定（事象ベースのアプローチ）

アプローチ手法

① リスクの特定	業務プロセスや取扱っている重要な資産に対して、業務上起きたら困ること（リスク）もしくは、過去に発生して業務に影響を及ぼしたことを記載します。 例） 「ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ」
② リスク所有者の特定	①で特定されたリスクの所有者を記載します。

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-2.】
第11章 - 12

リスク特定（事象ベースのアプローチ）

リスク特定の例

リスク	評価値			重要度	リスク所有者
ネットワーク障害により、リモートによる会議が中断もしくは実施できなくなり、取引先や顧客に影響を及ぼす恐れ	機密性	情報が漏えいする類の事象ではない	1	3	○○○○
	完全性	ネットワーク障害の原因がサイバー攻撃やマルウェアの場合、情報が被害を受ける可能性がある事象である	3		
	可用性	ネットワークが利用できなくなり、自社や取引先、顧客に大きな影響をおよぼす事象である	3		

事象ベースのアプローチによるリスク特定の例
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

リスク分析の例

「リスクレベル」＝「重要度」×「被害発生可能性」

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性とは

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する （いつ発生してもおかしくない）
2	特定の状況で脅威が発生する （年に数回程度）
1	通常の状況で脅威が発生することはない （通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない （ほぼ無防備）
2	部分的に対策を実施している （一部対策を実施）
1	必要な対策をすべて実施している （対策を実施）

「起こりやすさ」と「つけ込みやすさ」の換算表で算出する

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性の換算表

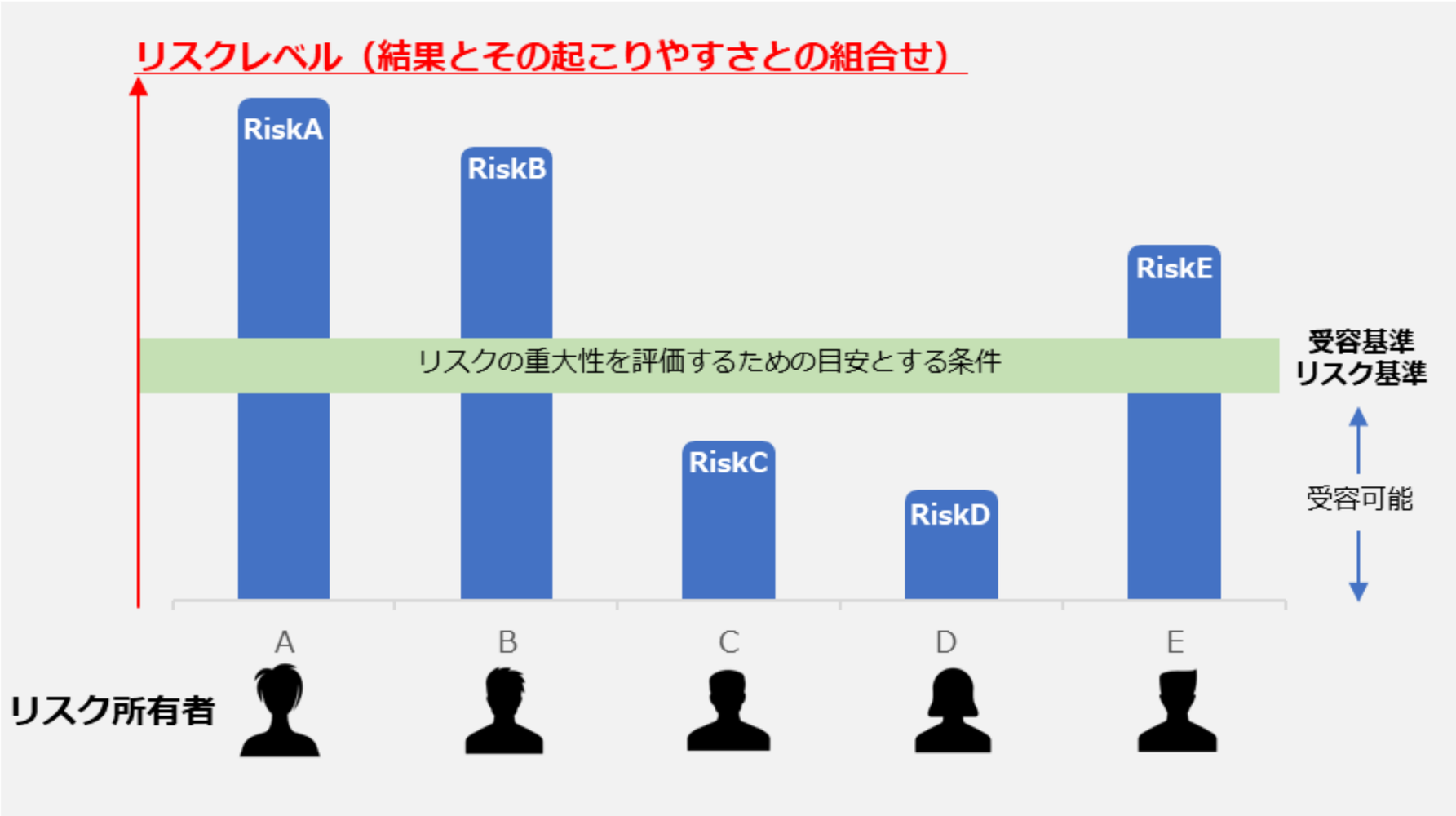
被害発生可能性の換算表		付け込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-4.】
第11章 - 14

リスクの評価

リスク評価



リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-4.】
第11章 - 15

リスクの評価

リスク評価（例）

リスクレベル評価値		被害発生可能性		
		3	2	1
重要度	3	9	6	3
	2	6	4	2
	1	3	2	1

リスク評価の概要図
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 16

対応策の検討

リスク対応プロセス

1. 適切な情報セキュリティリスク対応の選択肢の選定
2. 情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定
3. 決定した管理策とISO/IEC27001:2022附属書Aの管理策との比較
4. 適用宣言書の作成
5. 情報セキュリティリスク対応計画
6. リスク所有者による承認
7. 残留している情報セキュリティリスクの受容

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 16

対応策の検討

１．適切な情報セキュリティリスク対応の選択肢の選定

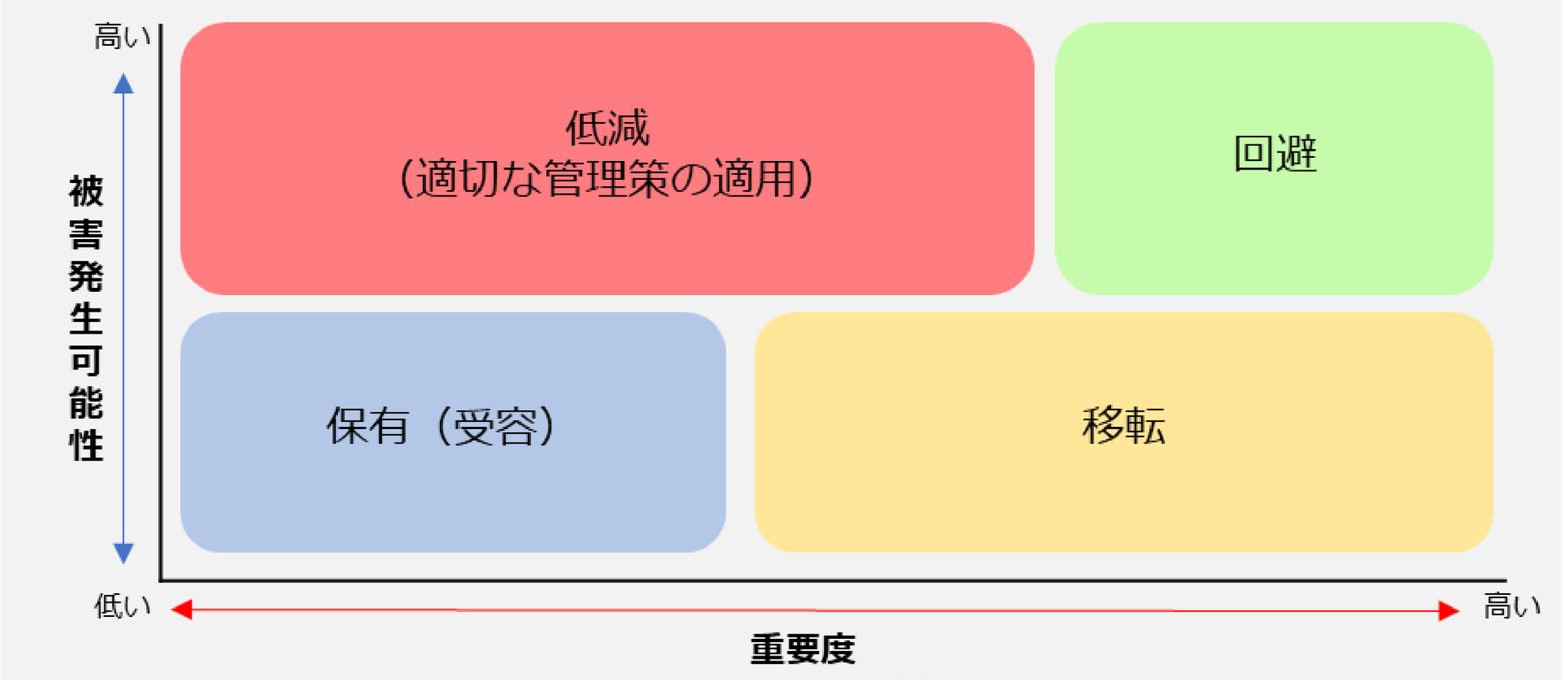
選択肢	対応内容
リスク回避	リスクが発生する可能性のある環境を排除するなど、リスクそのものをなくそうとすることです。たとえば、個人情報を受け取らないようにしたり、その業務自体をやめたりするといった方法です。
リスク低減	セキュリティ対策（管理策）を採用することによって、リスクの発生確率を低くしたり、リスクが顕在化したときの影響の大きさを小さくすることです。「軽減」「修正」と呼ばれることもあります。
リスク移転	リスクを他者に移して、自分たちの責任範囲外にしたり、リスクが顕在化したときの損失を他者に引き受けさせることです。たとえばクラウドのサーバを利用することによって、サーバが破壊されたり盗難されたりするリスクを移転することができます。「共有」と呼ばれることもあります。
リスク受容（保有）	対策を行わずにリスクを受け入れるということです。被害は大きいが発生可能性がほとんどない場合や、発生しても被害がほぼない場合が該当します。

リスクマネジメント：リスクの対応

【参照：テキスト11-2-4.】
第11章 - 15

対応策の検討

リスク対応の選択肢の選定方法



情報セキュリティリスクの考え方
（出典）JNSA.”2-4 リスクアセスメントとリスク対応”. https://www.jnsa.org/ikusei/01/02-04.html,（参照 2023-09-21）

リスクマネジメント：リスクの対応

【参照：テキスト11-2-4.】
第11章 - 15

対応策の検討

リスク受容基準（例）

リスクレベル	リスク評価	記述
低	そのままで受容可能	それ以上の活動なしにリスクを受容可能
中	管理下で受容可能	リスクマネジメントの観点からフォローアップを実施し、中長期にわたる継続的改善の枠組みにおいて活動を設定することが望ましい
高	受容できない	リスクを低減するための対策を短期間で行うことが絶対に望ましい。そうでない場合、活動の全部又は一部を拒否することが望ましい

（出典）ISO/IEC「ISO/IEC 27005:2022」を基に作成

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 16

対応策の検討

２．情報セキュリティリスク対応の選択肢の実施に必要なすべての管理策の決定

　ISO/IEC 27001:2022の附属書A、ISO/IEC 27017などの管理策集から、リスクの回避、低減、移転、受容（保有）の中から選択したリスク対応に必要な全ての管理策を決定します。

３．決定した管理策とISO/IEC27001:2022附属書Aの管理策との比較

　必要な全ての管理策を、ISO/IEC 27001:2022附属書Aに挙げられている管理策と比較します。

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 16

対応策の検討

４．適用宣言書の作成
　必要な全ての管理策と、その理由及び実施状況を文書化します。

５．情報セキュリティリスク対応計画
　組織がリスクに対応する必要性を含んだリスク対応計画を作成します。

6．リスク所有者による承認
　リスク所有者は、リスク対応計画を承認します。

7．残留している情報セキュリティリスクの受容
　リスク所有者は、残留リスクが受容可能かどうかを判断し、決定します。

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 17

対応策の検討

リスク対応プロセス（例）

項目	内容
リスクの内容	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う
リスク対応	リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）
対策例	対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する 対応する管理策：5.15アクセス制御
対策基準の策定	技術的対策 • 公開サーバへの不正アクセス対策 • 公開サーバへのアクセス権の最小化と管理の強化 • 多要素認証の設定の有効化 • WAFの導入

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性とは

起こりやすさ（脅威）	
3	通常の状況で脅威が発生する （いつ発生してもおかしくない）
2	特定の状況で脅威が発生する （年に数回程度）
1	通常の状況で脅威が発生することはない （通常発生しない）

つけ込みやすさ（脆弱性）	
3	対策を実施していない （ほぼ無防備）
2	部分的に対策を実施している （一部対策を実施）
1	必要な対策をすべて実施している （対策を実施）

「起こりやすさ」と「つけ込みやすさ」の換算表で算出する

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

被害発生可能性の換算表

被害発生可能性の換算表		付け込みやすさ（脆弱性）		
		3	2	1
起こりやすさ（脅威）	3	3	2	1
	2	2	1	1
	1	1	1	1

リスクマネジメント：リスクアセスメント

【参照：テキスト11-2-3.】
第11章 - 13

リスクの分析

リスク分析の例

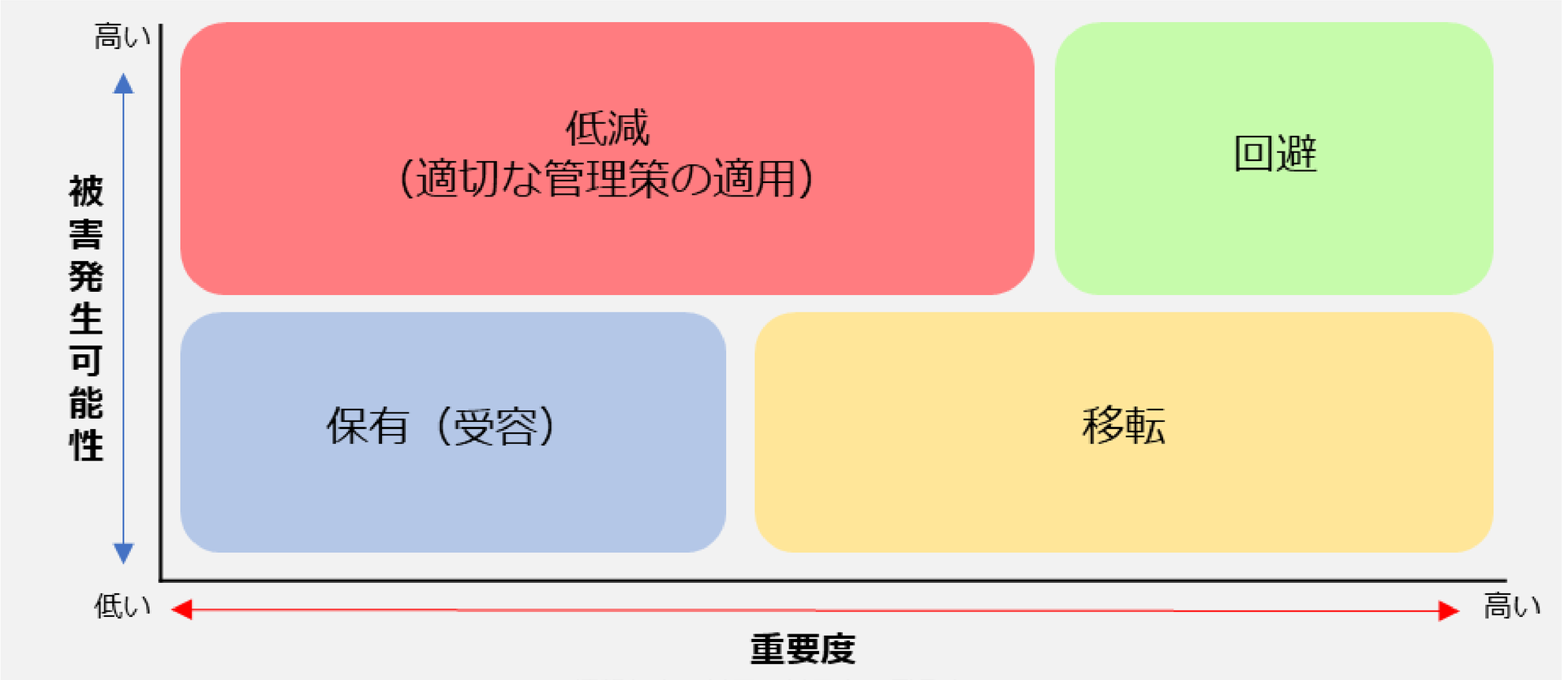
「リスクレベル」＝「重要度」×「被害発生可能性」

リスクマネジメント：リスクの対応

【参照：テキスト11-2-4.】
第11章 - 15

対応策の検討

リスク対応の選択肢の選定方法



情報セキュリティリスクの考え方
（出典）JNSA.”2-4 リスクアセスメントとリスク対応”. https://www.jnsa.org/ikusei/01/02-04.html,（参照 2023-09-21）

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 17

対応策の検討

リスク対応プロセス（例）

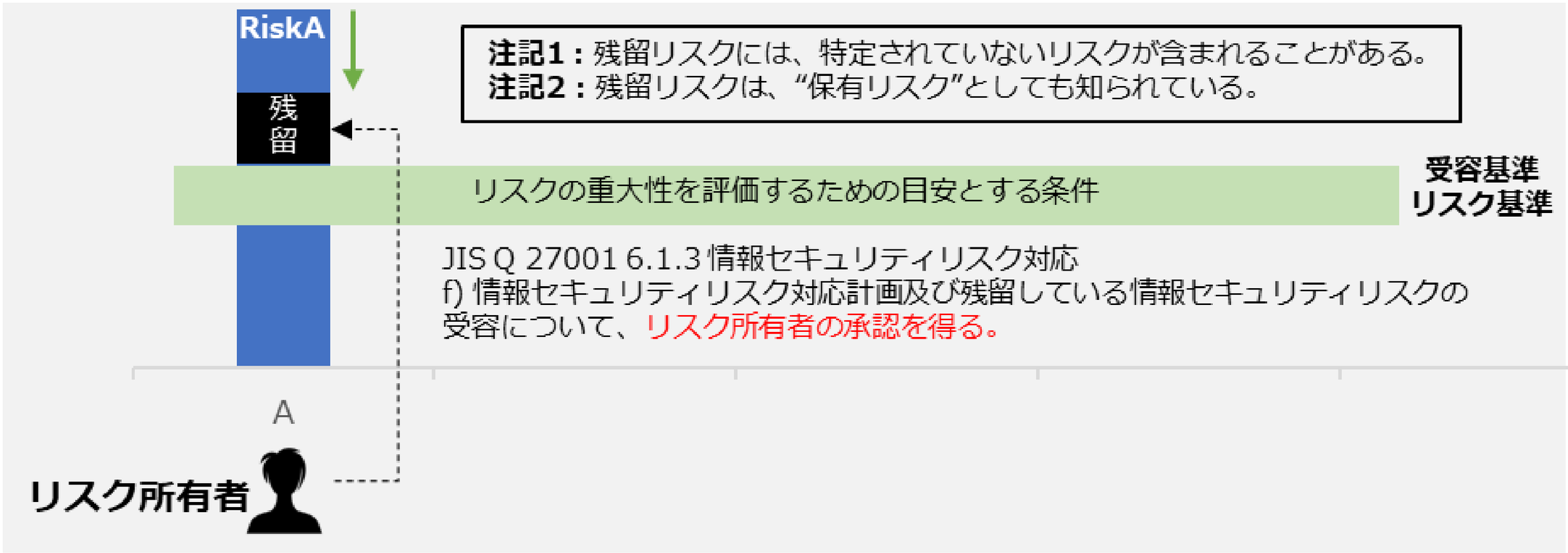
項目	内容
リスクの内容	不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う
リスク対応	リスク評価の結果をもとにリスク対応を決定する（今回は例として「リスクを低減する」方法を選択）
対策例	対策例：不正アクセスが発生する可能性を低減させるために、アクセス権限を最小化したり、パスワードを複雑にしたり、多要素認証を実施したりするなど、認証の強化を行い、不正アクセスが発生する可能性を低減する 対応する管理策：5.15アクセス制御
対策基準の策定	技術的対策 • 公開サーバへの不正アクセス対策 • 公開サーバへのアクセス権の最小化と管理の強化 • 多要素認証の設定の有効化 • WAFの導入

リスクマネジメント：リスクの対応

【参照：テキスト11-3-1.】
第11章 - 17

対応策の検討

残留リスク



残留リスクの概要
（出典）MSQA「ISMS推進マニュアル活用ガイドブック 2022年 1.0版」を基に作成

１．具体的手順の作成

【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】 セキュリティインシデント事例を参考とした実施手順

【Lv.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

クイックアプローチ・ベースラインアプローチ

【参照：テキスト12-1-1.】
第12章 - 02

アプローチ手法概略

【LV.1クイックアプローチ】

即時の対応や緊急事態への対処に適したアプローチ手法。
様々なインシデント事例内容を参考にし、対策基準を策定。

【LV.2ベースラインアプローチ】

組織全体での一貫性を確保し、セキュリティの最低基準を満たすことを目指すアプローチ手法。
ガイドラインやひな形を参考とし、対策基準を策定。

セキュリティインシデント事例を参考とした実施手順

LV1.クイックアプローチの実施手順

【参照：テキスト12-2-1.】
第12章 - 03

インシデント事例

事例：内部不正による情報漏えいの疑い（卸売業・小売業、従業員数6~20名以下）

被害内容

元従業員が退職前に大量にファイルをダウンロードしました。また、同従業員が使用していたPCの履歴が消去され、専門家でも復旧できない状態になっていました。

機密情報の持ち出しをした確定的な証拠が得られなかったため、結果的には被害届を提出しませんでした。しかし、この判断をするまでに2年かかりました。その間、弁護士に情報提供するために、多くの作業が必要になりました。たとえば、経営者と総務担当は、情報漏えいしたと疑われる膨大なログを確認し、どれが機密情報に該当するかチェックする作業を強いられました。トラブル発生時は、人件費だけでなく、心的負担も大きくかかりました。

被害発生の原因

社外からの脅威の対策としてウイルス対策ソフトウェアや電子メールへの対応、アクセス制限などは進めていたが、社内から発生する脅威の対策は不十分であったこと。

セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト12-2-1.】
第12章 - 03

リスク特定

- 対象となる資産情報の洗い出し
- 機密性、完全性、可用性の評価
- 重要度の算出

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3

セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト12-2-1.】
第12章 - 04

リスク分析

- 重要度と被害発生可能性から、リスクレベルを算出

「リスクレベル」＝「重要度」×「被害発生可能性」

業務分類	情報資産名称	備考	利用者範囲	リスク所有者	管理部署	媒体・保存先	機密性	完全性	可用性	重要度	被害発生可能性	リスクレベル
人事	社員名簿	社員基本情報	人事部	人事部長	人事部	人事担当者のPC	3	3	2	3	3	9
経理	当社宛請求書	過去3年分	経理部	経理部長	経理部	経理担当者のPC	3	3	2	3	2	6
営業	顧客リスト	得意先	営業部	営業部長	営業部	営業担当者のPC	3	3	3	3	2	6

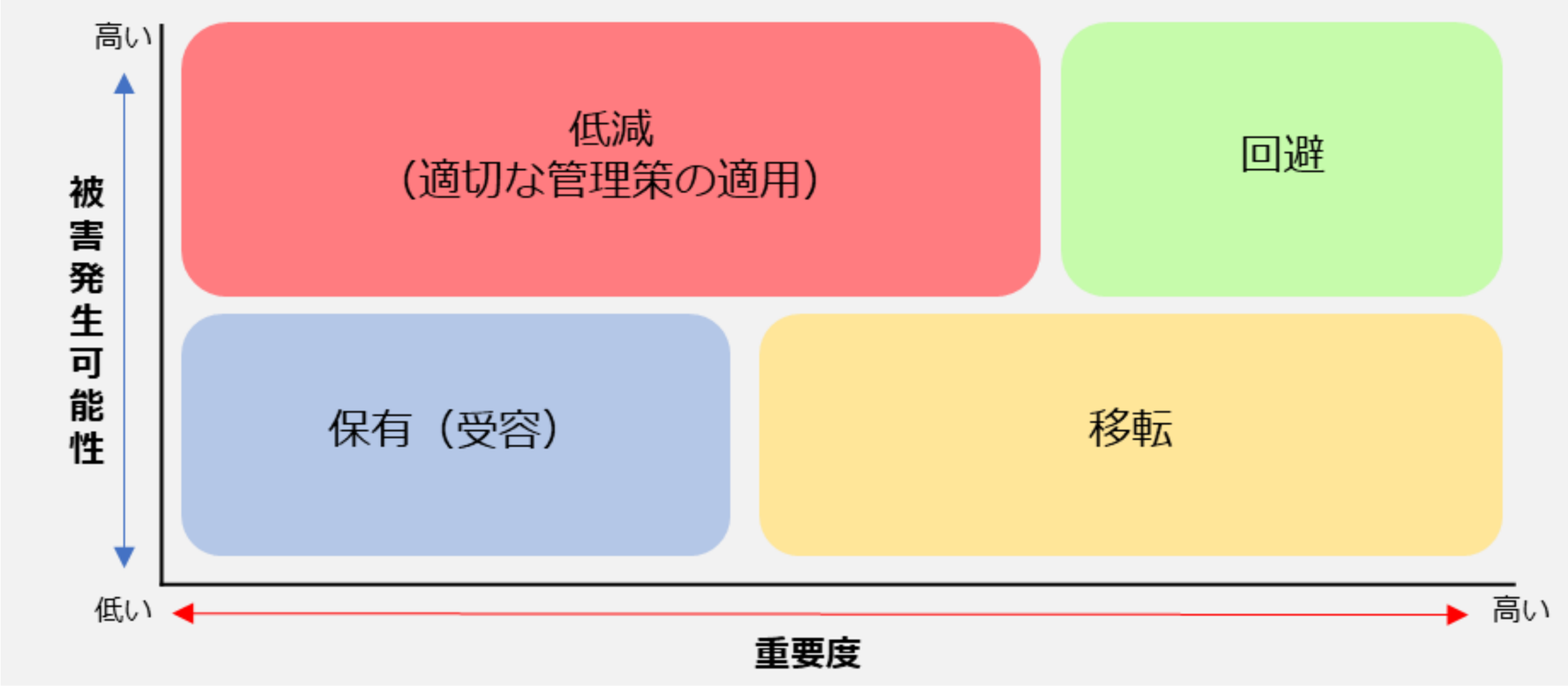
セキュリティインシデント事例を参考とした実施手順

リスクアセスメントの実施

【参照：テキスト12-2-1.】
第12章 - 04

リスク評価

- リスク対応を検討する



セキュリティインシデント事例を参考とした実施手順

対策基準の策定

【参照：テキスト12-2-1.】
第12章 - 04

事例を基にした対策基準

- 社内の機密情報に関する社内規定の策定
- 重要情報の管理、保護
- 物理的管理の実施
- 従業員向け研修の実施

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：テキスト12-2-1.】
第12章 - 05

機密情報に関する社内規定の策定

（例）従業員の責務

従業員は以下を遵守する

- 従業員は、当社が営業秘密として管理する情報およびその複製物の一切を許可されていない組織、人に提供してはならない。
- 従業員は、当社の情報セキュリティ方針および関連規程を遵守する。違反時の懲戒については、就業規則に準じる。
- 従業員は、在職中に交付された業務に関連する資料、個人情報、顧客・取引先から当社が交付を受けた資料またはそれらの複製物の一切を退職時に返還する。
- 従業員は、在職中に知り得た当社の営業秘密または業務遂行上知り得た技術的機密を利用して、競合的あるいは競業的行為を行ってはならない。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：テキスト12-2-1.】
第12章 - 05

重要情報の管理、保護

（例）利用者アカウントの管理

利用者の認証に用いるアカウントが不要になる場合、システム管理者は、当該アカウントの削除または無効化を、当該アカウントが不要になった日の翌日までに実施する。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：テキスト12-2-1.】
第12章 - 05

物理的管理の実施

（例）情報資産の社外持ち出し管理

情報資産を社外に持ち出す場合には、以下を実施する。

- 社外秘の場合は所属部門長の許可を得る。
- 極秘の場合は代表取締役の許可を得る。
- ノートパソコンのハードディスクに保存して持ち出す場合は、ハードディスク/フォルダー/データを暗号化する。
- スマホ、タブレットに保存して持ち出す場合は、セキュリティロックを設定する。
- USBメモリなどの小型電子媒体は、大きなタグをつける/ストラップで体やカバンに固定する/落としてもすぐに分かるように鈴をつける。
- 屋外でネットワークへ接続して極秘または社外秘の情報資産を送受信する場合は、暗号化する。
- 携行中は常に監視可能な距離を保つ。

セキュリティインシデント事例を参考とした実施手順

実施手順の作成

【参照：テキスト12-2-1.】
第12章 - 05

重要情報の管理、保護

（例）情報セキュリティ教育

教育責任者は、以下の点を考慮し、情報セキュリティに関する教育計画を年度単位で立案する。

対象者：全従業員

テーマ：以下は必須とする。

- 情報セキュリティ関連規程の説明（入社時、就業時）
- 最新の脅威に対する注意喚起（随時）
- 関連法令の理解（関連法令の公布・施行時）
- 個人情報の取扱いに関する留意事項
- コンプライアンス教育

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

【参照：テキスト12-3-1.】
第12章 - 06

参考にするガイドラインの例

- IPA「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」
- NISC「インターネットの安全・安心ハンドブックVer.5.0」
- 総務省「テレワークセキュリティガイドライン第5版」
- IPA「中小企業のためのクラウドサービス安全利用の手引き」
- IPA「情報セキュリティ関連規程」

ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

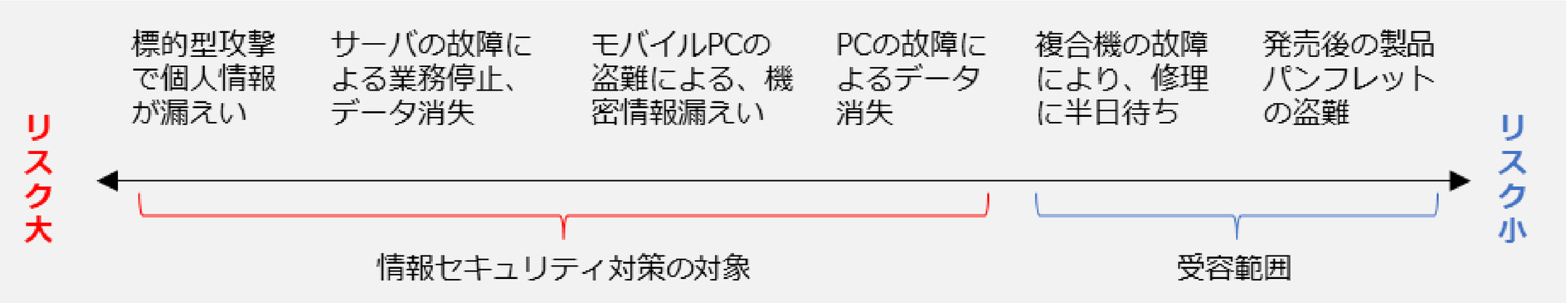
【参照：テキスト12-3-1.】
第12章 - 12

リスクアセスメントの実施

- リスク特定
- リスク分析
- リスク評価

対策決定のヒント

- リスクの受容も視野に入れてリスク評価を実施する



ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

【参照：テキスト12-3-1.】
第12章 - 13

規程の作成

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
ファイルサーバ	ユーザーファイル	アプリケーションバックアップ機能	NASサーバ
Webサーバ	ホームページ	同期ツール	NASサーバ
会計システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウドバックアップサービス

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

＜保管＞

- NASサーバ：施錠つきサーバラックに収納

ガイドラインを参考とした実施手順

情報セキュリティ関連規程（IPA）の活用

【参照：テキスト12-3-1.】
第12章 - 13

規程の作成

3	情報資産管理	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

バックアップ

バックアップ取得対象

システム管理者は、以下の機器で処理するデータのバックアップを定期的に取得する。

機器名	対象	方法	保管先
DBサーバ	取引先に関するデータ	アプリケーションバックアップ機能	自社サーバ
Webサーバ	ホームページ	同期ツール	自社サーバ
発注管理システム	アプリケーションデータ	アプリケーションバックアップ機能	クラウド上のサーバ

バックアップ媒体の取扱い

バックアップに利用した機器および媒体の取扱いは以下に従う。

＜保管＞

- 自社サーバ：ハウジングサービスを利用し、サービス事業者の施設内に保管する

1．ISMSの要求事項と構築

【LV.3網羅的アプローチ】の概要

【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

網羅的アプローチ

【参照：テキスト13-1-1.】
第13章 - 02

アプローチ手法概略

【LV.3網羅的アプローチ】

網羅的な対策を講じることを目指すアプローチ手法。
ISMSなどの認証が可能なレベルを目指して、対策基準を策定。

網羅的アプローチ実施の留意点

- ドキュメントの整備は手段であり目的ではない
- ISMSマネジメントプロセスの導入により、PDCAを実施していくことが重要

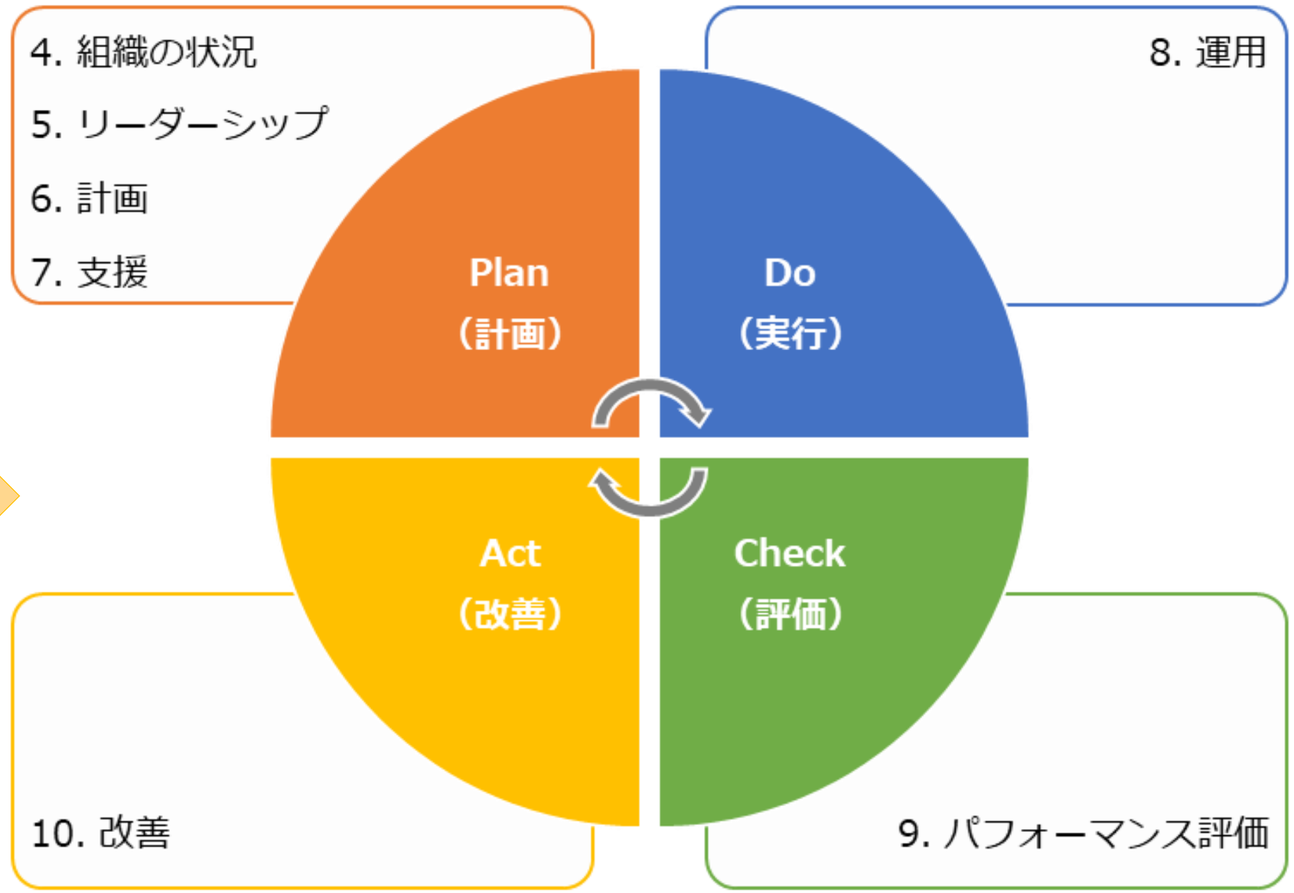
ISMSの概要

【参照：テキスト13-2-1.】
第13章 - 03

ISMSの確立、運用、監視

要求事項

1. 適用範囲
2. 引用規格
3. 用語および定義
4. 組織の状況
5. リーダーシップ
6. 計画
7. 支援
8. 運用
9. パフォーマンス評価
10. 改善

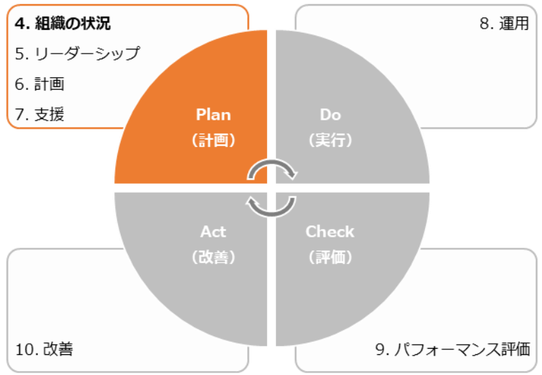


ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 04

概要

4. 組織の状況	作成ドキュメント（例）
4.1 組織及びその状況の理解 ISMSを構築することで解決したい課題（組織の目的に関連する内部課題、外部課題）を明確にします。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解 ISMSに関係する利害関係者（顧客、従業員、取引先など個人や組織）と、利害関係者から要求される情報セキュリティに関係する要求事項を明確にします。	• 利害関係者のニーズ及び期待
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 決定された外部課題・内部課題、利害関係者の要求事項と、業務内容や他の組織との情報のやり取り、ネットワーク構成などを考慮し、ISMSの適用範囲を合理的に決定します。	• ISMS適用範囲 • レイアウト図 • ネットワーク図
4.4 情報セキュリティマネジメントシステム 決定したISMSの適用範囲を対象に、PDCAサイクルに基づくISMSを構築・運用します。	ー



ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 05

4.1 組織及びその状況の理解

作成するドキュメント　外部および内部の課題

外部の課題

課題	リスク	機会
個人情報、機密情報の保護（ウイルス感染、情報漏えい、新たな脅威への対応）	情報セキュリティ事故の発生 →信用低下	情報の活用

内部の課題

課題	リスク	機会
ISMSに関する理解の促進	理解不足による情報セキュリティ事故	体勢強化
情報(紙、電子データ)の適切な取扱い	紛失、訪問先などで置忘れ →信頼喪失	信頼向上
ノウハウ、お客様より預かる機密情報などの保護	機密情報の漏えい、ノウハウの流出	ビジネス機会の拡大

ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 06

4.2 利害関係者のニーズ及び期待の理解

作成するドキュメント　利害関係者のニーズ及び期待

利害関係者	情報セキュリティに関する要求事項	リスク	機会
取引先	適切な情報の取扱い	不適切な取扱いで信頼低下 →案件減少	適切な対応で信頼向上 →受注の維持/増加
	法令遵守	未遵守による信頼低下 →案件減少	遵守による信頼向上 →受注の維持/増加
株主	セキュリティインシデントの未然防止	セキュリティインシデントの発生 →ブランドイメージの低下	セキュリティインシデントの発生数減少 →ブランドイメージの向上
従業者	情報セキュリティに関する教育	機密情報/ノウハウの流出	組織の価値向上
	必要な情報へのアクセス	機密情報/ノウハウの流出	効果的・効率的な業務 →競争力アップ
	個人情報の保護	不適切な情報の取扱い →信頼低下	従業者から信頼向上 →人材の確保
国・自治体	法令・その他規範の遵守	セキュリティインシデント発生時の不適切な対応 →社会的信頼の低下	社会的信頼の向上

ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 – 07, 08

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

作成するドキュメント　ISMS適用範囲
レイアウト図
ネットワーク図

適用範囲を組織の一部としたときの考慮ポイント

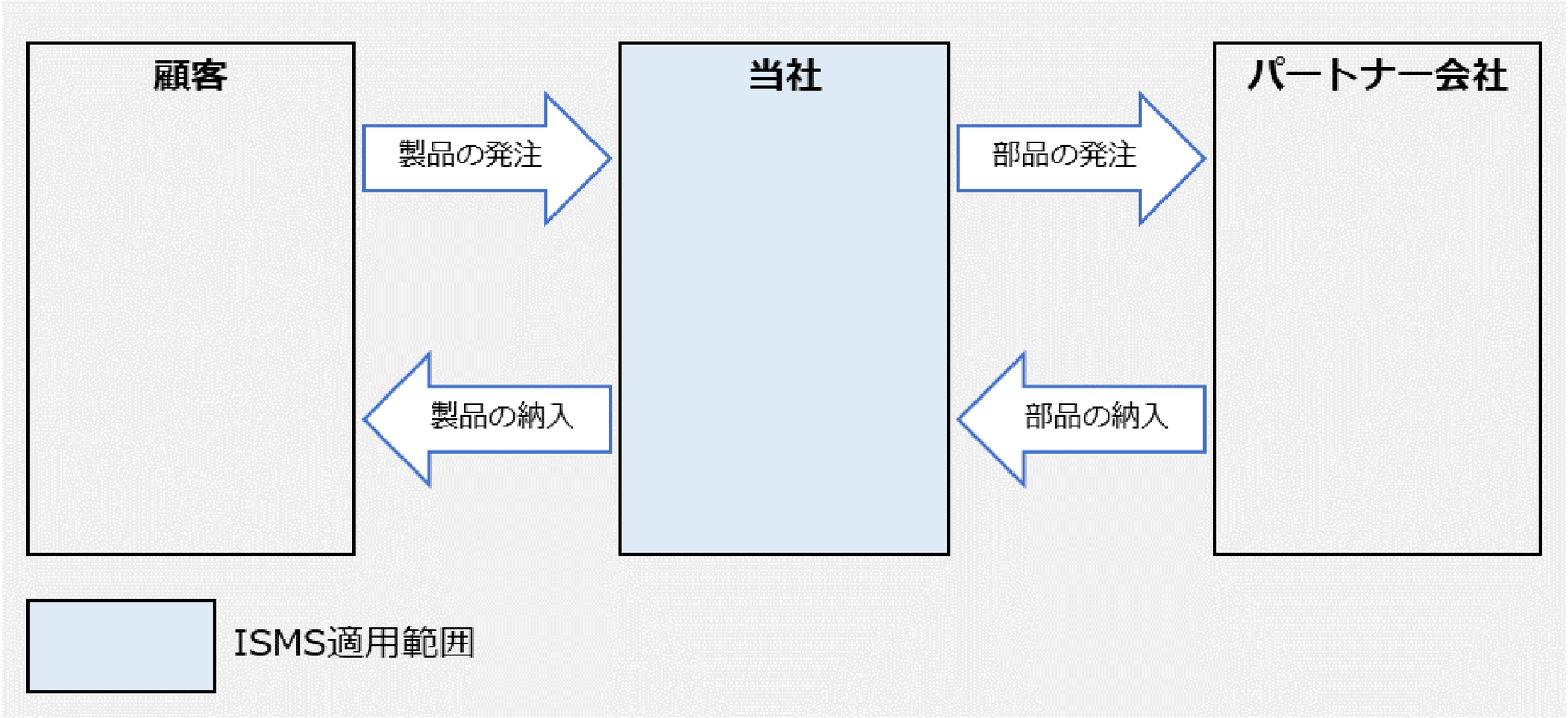
- 人的、組織的境界
- 物理的境界
- 技術的境界
- 資産的境界
- 事業的境界

ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 07

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

適用範囲の記載例



ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 09

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

レイアウト図

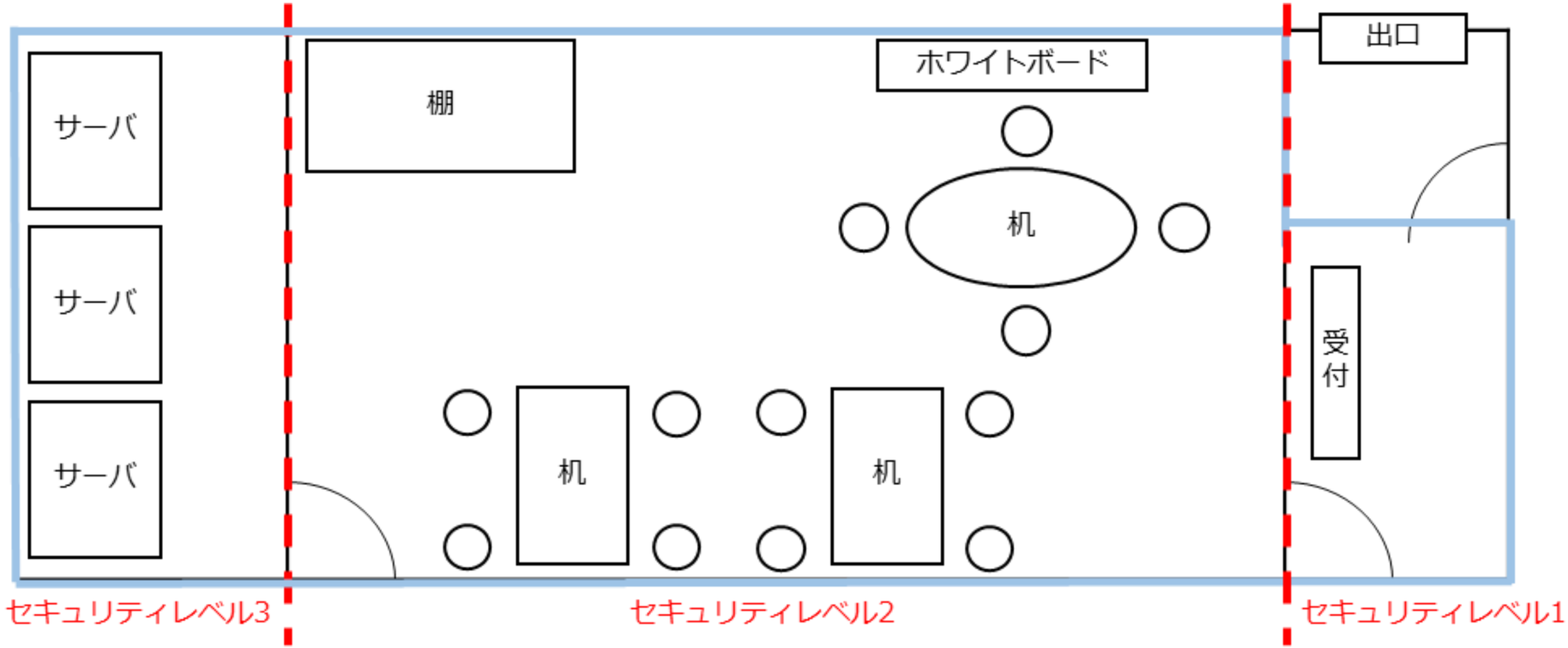


図55. 適用範囲の例（物理的境界）

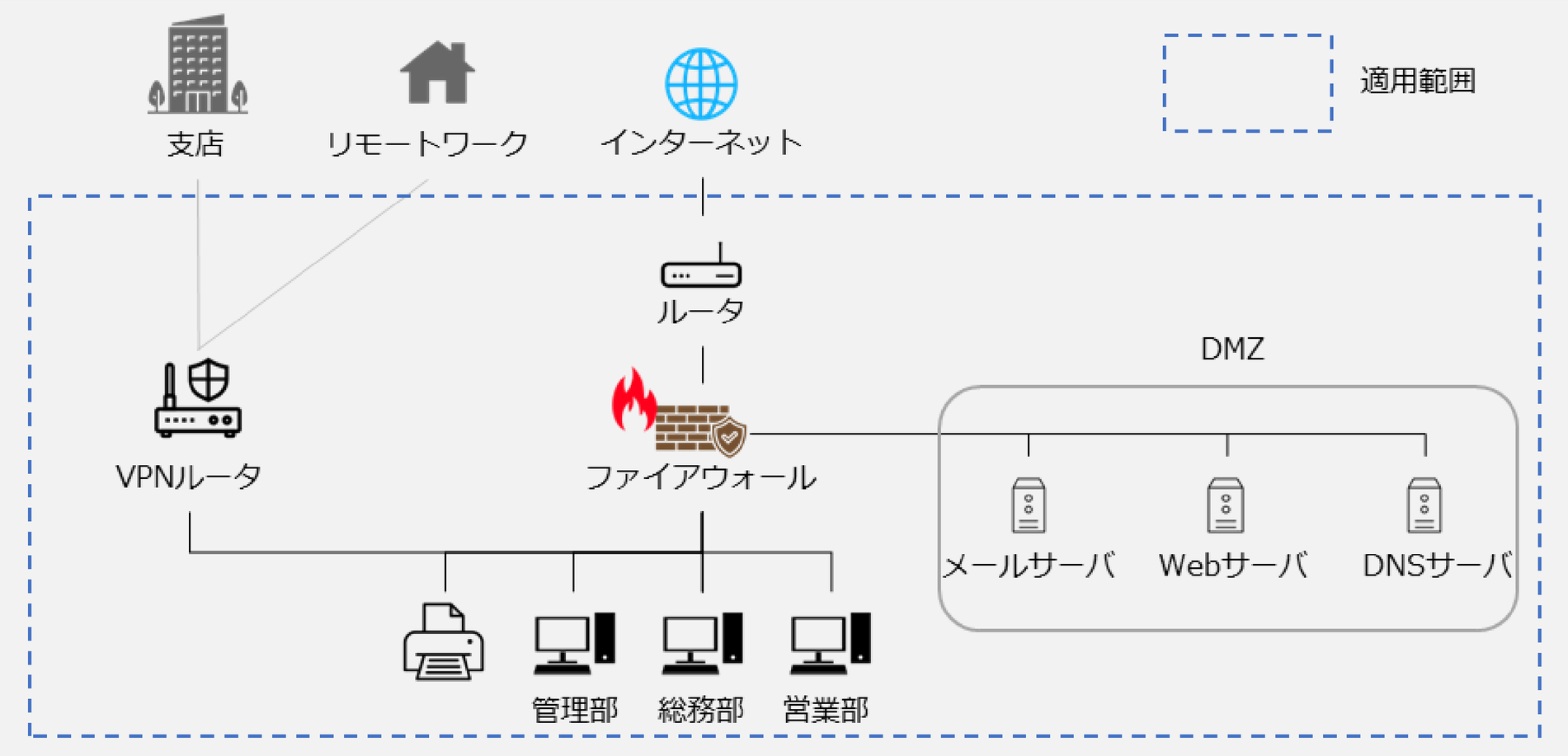
セキュリティレベル1：従業員を含め、外来者は入室可
セキュリティレベル2：対象従業員のみ入室可（対象者以外は入退室管理が必要）
セキュリティレベル3：限られた人員のみ入室可（飲食禁止）

ISMS：4. 組織の状況

【参照：テキスト13-2-2】
第13章 - 09

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

ネットワーク図

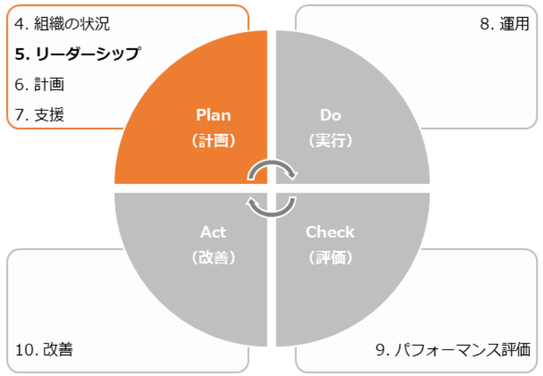


ISMS：5. リーダーシップ

【参照：テキスト13-2-3】
第13章 - 10

概要

5. リーダーシップ	作成ドキュメント（例）
5.1 リーダーシップ及びコミットメント トップマネジメントが責任を持って実行しなければならない事項が記載されています。	ー
5.2 方針 トップマネジメントが、ISMSの目的や方向性、実施する内容について文書化し、「情報セキュリティ方針」を作成することを要求しています。	• 情報セキュリティ方針
5.3 組織の役割、責任及び権限 トップマネジメントは、ISMSを運用するために必要な役割や責任、権限を各要員に割り当て、どの要員がどのような役割や責任、権限を持っているかが分かる文書を作成することを要求しています。	• ISMSの運用組織図 • 責任者または部門の名称と役割を明記した文書



ISMS：5. リーダーシップ

【参照：テキスト13-2-3】
第13章 - 10

5.1 リーダーシップ及びコミットメント

トップマネジメントが行う事項（要求事項）

- 情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にする
- 組織のプロセスへのISMS要求事項の統合を確実にする
- ISMSに必要な資源が利用可能であることを確実にする
- 有効な情報セキュリティマネジメントおよびISMS要求事項への適合の重要性を伝達する
- ISMSがその意図した成果を達成することを確実にする
- ISMSの有効性に寄与するよう人々を指揮し、支援する
- 継続的改善を促進する
- その他の関連する管理層がその責任の領域においてリーダーシップを実証するよう、管理層の役割を支援する

ISMS：5. リーダーシップ

【参照：テキスト13-2-3】
第13章 - 12

5.2 方針

作成するドキュメント　情報セキュリティ方針

a) 自社の経営理念に基づいた事業の目的や、情報セキュリティの必要性などを記載します。また、業務に関わる情報資産と、保護すべき理由などを記載します。

b) 情報セキュリティに関する目標を記載します。

情報セキュリティ方針（例）

【第X版】
【日付】
【社名】
【代表取締役社長　名前】

私たち【社名】は、【提供するサービス名】の提供を通じて、お客様、社員とその家族などすべてのステークホルダーの期待に応え、社会に貢献することを使命と考えています。

当社の事業活動において、お客様からお預かりする個人情報を含む多くの情報資産を活用しており、すべてのステークホルダーの期待に応えるためには、これらの情報資産を保護することは、経営上の最重要課題であると認識しています。

よって、私たちは、情報セキュリティ基本方針を策定し、本基本方針に基づいて、ISMSを構築・運用し、当社を取り巻く環境の変化を踏まえ、継続的改善に全社を挙げて取組むことをここに宣言します。

さらに、当社は、以下のセキュリティ目的を設定し、この目的を達成するための諸施策を確実に実施します。
✓　お客様との契約および法的または規制要求事項を尊重し遵守する。
✓　情報セキュリティ事故を未然に防止する。
✓　万一情報セキュリティ事故が発生した場合、影響を最小限にする。

以上

c) 自社の業務の特徴や課題を記載します。

d) ISMSに関する取組みを定期的に見直し、改善していく内容を記載します。

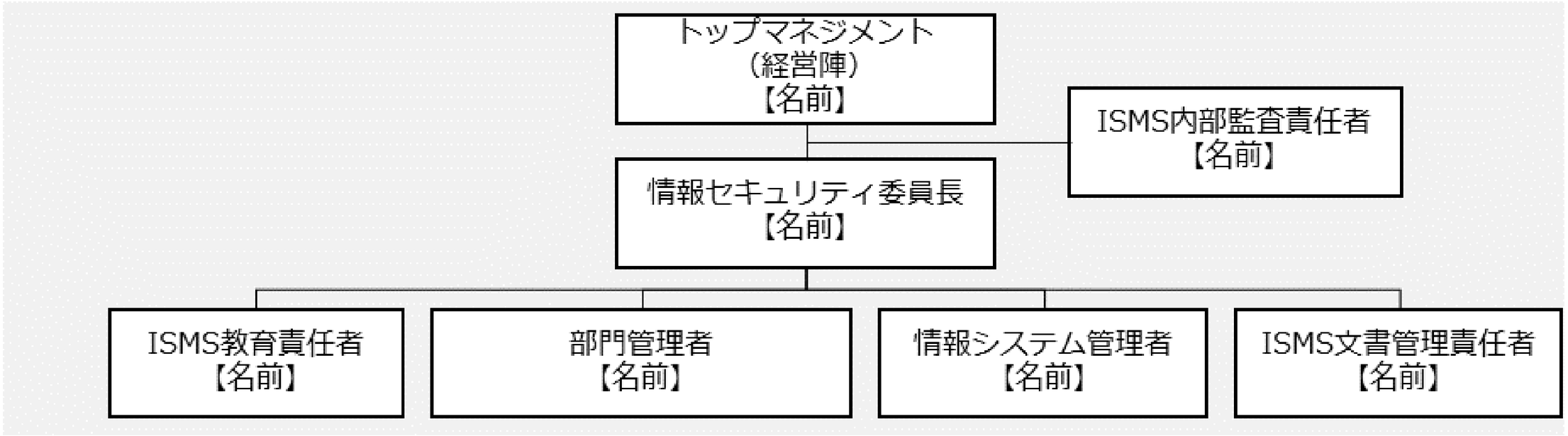
ISMS：5. リーダーシップ

【参照：テキスト13-2-3】
第13章 - 13

5.3 組織の役割、責任および権限

作成するドキュメント　ISMS運用組織図
責任者または部門の名称と役割を明記した文書

ISMS運用組織図



ISMS：5. リーダーシップ

【参照：テキスト13-2-3】
第13章 - 13

5.3 組織の役割、責任および権限

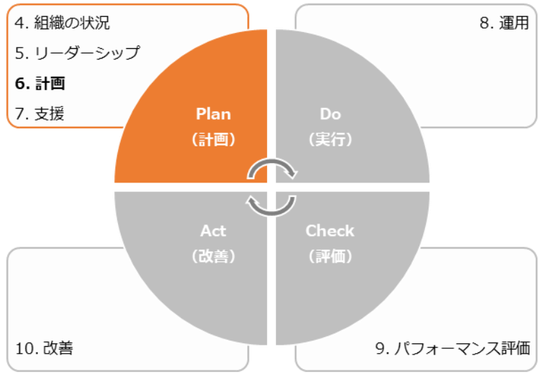
責任者または部門の名称と役割を明記した文書

名称	役割
情報セキュリティ委員長	ISMSの実施、運用について統括する
ISMS内部監査責任者	ISMSとその実施状況に関わる監査を統括する
ISMS教育責任者	ISMSに関する教育計画の立案と実施を行う
部門管理者(情報セキュリティ委員)	ISMSの部門代表者として、部門を管理する
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規程・規則に従い、ISMSを維持するための安全管理対策を実施する
ISMS文書管理責任者	ISMSに関する文書と記録などの維持・管理を行う

ISMS：6. 計画

概要

【参照：テキスト13-2-4】
第13章 - 14



6. 計画	作成ドキュメント（例）
6.1 リスク及び機会に対処する活動 ① **一般** 特定した内外部の課題と、利害関係者のニーズおよび期待を考慮して、リスク・機会（期待する状況や結果）を決定し、対処するための活動を明確にすることを要求しています。 ② **情報セキュリティリスクアセスメント** 組織や企業の資産に対する、情報セキュリティリスクアセスメントプロセスの確立を要求しています。 ③ **情報セキュリティリスク対応** 情報セキュリティリスク対応の手順を確立することを要求しています。	• 資産目録（情報資産管理台帳） • リスクアセスメント結果報告書 • 適用宣言書 • リスク対応計画
6.2 情報セキュリティ目的及びそれを達成するための計画策定 情報セキュリティ目的を確立し、達成するための計画を策定することを要求しています。	• ISMS有効性評価表
6.3 変更の計画策定 ISMSの変更が必要なときは、計画的な変更を要求しています。	ー

ISMS：6. 計画

【参照：テキスト13-2-4】
第13章 - 14

6.1 リスク及び機会に対処する活動

作成するドキュメント　資産目録（情報資産管理台帳）
リスクアセスメント結果報告書

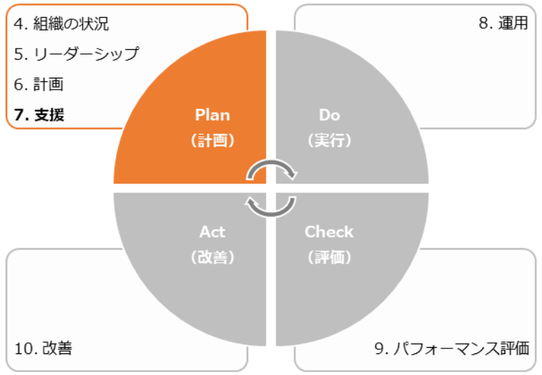
リスクアセスメント結果報告

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	

ISMS：7. 支援

概要

【参照：テキスト13-2-5】
第13章 - 25



7. 支援	作成ドキュメント（例）
7.1 資源 ISMSに必要な資源（人、物、金、情報）を決定し、提供します。	―
7.2 力量 ISMS適用範囲の要員に求められる力量（知識、技能など）を定義し、要員が力量を備えているか評価を行います。力量評価の結果、力量が不足している場合は、力量を身につけるための教育を計画し、実施します。教育の実施後、力量を取得・維持できたか確認テストを行います。最後に、実施した教育内容を記録として保持します。	• 力量確認表 • 教育計画書 • 理解度確認テスト • 教育実施記録
7.3 認識 ISMS適用範囲のすべての要員に、以下の内容を認識させる必要があります。 ・情報セキュリティ方針 ・情報セキュリティパフォーマンスの向上によるメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策 ・ISMSによって割り当てられた責任を果たさなかった際の影響	―
7.4 コミュニケーション ISMSを運用するにあたり、必要な意思疎通ができるプロセスを確立する必要があります。	―
7.5 文書化した情報 ISMSに必要な文書化した情報の作成、更新、管理についての要求事項が記載されています。	―

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 26

7.1 資源

資源	具体例
人	• ISMSを構築・運用するために必要となる要員 • ISMSの推進体制の確立 • 必要に応じた外部の専門家　など
物	• 情報を処理するための機器（サーバ、ネットワーク機器など） • コミュニケーション手段（パソコン、スマホなど） • 活動に必要な施設　など
金	• 人、物の資源を確保するための予算 • 要員の教育費用 • ISMSの維持費　など
情報	• 文書化した情報 • ISMSのPDCAサイクルを回すために有用な情報 • 情報セキュリティに関する最新情報　など

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 27

7.2 力量

作成するドキュメント

力量確認表
教育計画書
理解度確認テスト
教育実施記録

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 28

7.2 力量

力量確認表

役　割	部門管理者
氏　名	○○ ○○

任命基準	A	B	C
区分	任命可	改善確認後任命可※	任命不可 再任命

A：項目のすべてが"3"以上。
B：項目の"2"以下について改善の予定がある。
C：項目の"2"以下について改善の予定がない。

※改善確認までは暫定的に任命し、改善確認後に正式任命とする

	必要条件	評価	改善予定日	改善内容	改善後評価	改善確認日
1	情報セキュリティ基本方針および社内の規程、基準などに精通していること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
2	ISMSに関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
3	情報セキュリティ全般に関する知識があること	2	20XX/-/-	ISMS構築作業を通して獲得	3	20XX/-/-
4	公正な判断ができること	5				

評価基準	内容
5	十分な力量がある。指導・教育ができる
4	力量がある。支援なしに対応ができる
3	力量がある。他の支援により対応ができる
2	改善の余地がある
1	改善が必要

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 28

7.2 力量

教育計画書

教育目的	ISO27001認証取得のため
教育対象者	全従業者
教育方法	方法：eラーニングによる自己学習、確認テスト。 委員会より、受講対象者に受講案内のメールを送付。 受講者は、案内にあるURLからeラーニングのシステムにアクセスし、受講(テキストのダウンロード)／確認テストを行う。
教育内容	ISMSに対する意識向上 ・　当社の方針や手順について（情報セキュリティ基本方針など） ・　ISMSの有効性に対する自らの貢献 ・　ISMS要求に適合しないことの意味 ・　当社のルールの遵守
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
教育の有効性評価	情報セキュリティハンドブックを用いて教育を実施。 教育終了後、アンケート／確認テストを実施し記録に残す。 確認テストは、合格点は100点以上とする。 確認テストは、合格点に達するまで繰り返す。

ISMS：7. 支援

7.2 力量

【参照：テキスト13-2-5】
第13章 - 29

理解度確認テスト

次の【　　】に入る言葉として最も適したものを選びなさい（各10点）

設問			答え
①【　　】とは、ISMSを構築・運用するための国際規格である。			C
A. ISO9001	B.ISO14001	C.ISO27001	
② 情報セキュリティという言葉は、一般的に、情報の【　　】、完全性、可用性を維持改善することと定義されている。			C
A. 信頼性	B.整合性	C.機密性	
③ 2023年度の当社の情報セキュリティ目標は、【　　】である。			A
A.ISMS教育受講／合格　100%(全従業者)	B.予防処置の発行件数を四半期に1件以上	C.セキュリティインシデント発生件数／2件以内	
④【　　】とは、企業や個人の情報を盗みとるため、特定の相手（企業組織や社員）をメールなどの手段で狙う攻撃のことです。			A
A. 標的型攻撃	B. ウイルス型攻撃	C. サイバー攻撃	
⑤ ④【　　】メールの特徴はどれか。			B
A. 支払う必要がない料金を振り込ませるために、債権回収会社などを装い無差別に送信される。	B. 件名や本文に、組織の担当者の業務に関係する内容が記述されている。	C. 偽のホームページにアクセスさせるために、金融機関などを装い無差別に送信される。	

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 30

7.2 力量

教育実施記録

教育の名称	ISMS教育（基本方針、目標、ルール）
実施期間	20XX年-月-日(-)～20XX年-月-日(-)
実施方法	eラーニング
使用テキスト	情報セキュリティハンドブック
教育の概要	情報セキュリティハンドブックなどによるISMSに対する意識向上 ・当社の方針や手順について（情報セキュリティ基本方針など） ・ISMSの有効性に対する自らの貢献 ・ISMS要求に適合しないことの意味 ・当社のルールの遵守 学習後にテスト実施
受講対象者・部門	上記教育実施期間において在籍する全従業者
参加者	別紙：「教育受講者一覧」を参照
備考	特になし

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 31

7.3 認識

理解するべき内容

- 情報セキュリティ方針
- 情報セキュリティパフォーマンスの向上によるメリットや、自身の業務とISMSの関係、実施すべきセキュリティ対策の具体的な内容
- ISMSによって割り当てられた責任を果たさなかった場合の組織に与える影響

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 32

7.4 コミュニケーション

コミュニケーション手順

内容	実施時期	対象者	実施者	方法
情報セキュリティ方針の伝達	随時	利害関係者	トップマネジメント（ISMS事務局）	外部 ・当社HPに公表 内部 ・ISMS定期教育にて ・当社HPに公表 ・社内掲示
各見直し結果の伝達	見直後、1週間以内	従業者	ISMS事務局	承認後、ISMS事務局より通達
セキュリティ調査結果の報告	依頼入手時	お客様	ISMS事務局	・お客様より調査票などを入手した場合、主管部門にて回答を作成 ・ISMS事務局責任者が確認の上、お客様に提出
セキュリティインシデントの伝達	発見時	ISMS事務局	発見者	「情報セキュリティ手順書：セキュリティインシデント対応フロー」の通り
	適時	トップマネジメント	ISMS事務局	同上
	適時	関係当局	ISMS事務局	同上

ISMS：7. 支援

【参照：テキスト13-2-5】
第13章 - 33

7.5 文書化した情報

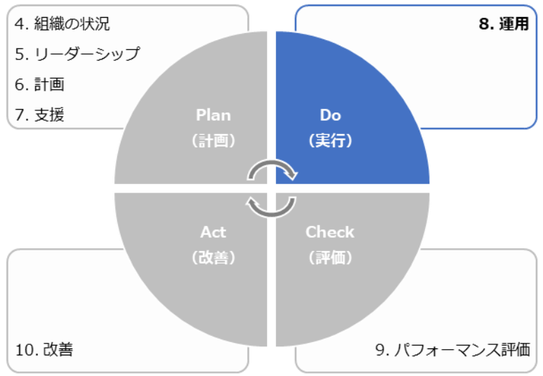
文書化した情報の一覧

文書化した情報	作成する項番
ISMSの適用範囲	「4. 組織の状況」で作成
情報セキュリティ方針	「5. リーダーシップ」で作成
リスクアセスメントプロセスに関わる文書化された情報	「6. 計画」で作成
リスク対応プロセスに関わる文書化された情報	
情報セキュリティ目的に関わる文書化された情報	
力量の証拠	「7. 支援」で作成
組織が決めた文書化された情報	
ISMSのプロセス実施に関わる文書化された情報	「8. 運用」で作成
リスクアセスメントの結果	
リスク対応の結果	
監視・測定の結果	「9. パフォーマンス評価」で作成
監査プログラムの実施、結果に関わる文書化された情報	
マネジメントレビューの結果	
不適合の内容と処置、処置の結果	「10. 改善」で作成

ISMS：8. 運用

概要

【参照：テキスト13-2-6】
第13章 - 34



8. 運用	作成ドキュメント（例）
8.1 運用の計画及び管理 「6. 計画」で計画した活動や、要求事項を満たすための活動の実施状況を管理するための一覧表を作成します。	• ISMS年間計画表
8.2 情報セキュリティリスクアセスメント 「6. 計画」で定めたリスクアセスメントのプロセスを実施し、結果を文書化します。	• 情報セキュリティリスクアセスメント結果報告書
8.3 情報セキュリティリスク対応 「6. 計画」で定めた情報セキュリティリスク対応計画を実施し、結果を文書化します。	• 情報セキュリティリスク対応計画

ISMS：8. 運用

【参照：テキスト13-2-6】
第13章 - 34

8.1 運用の計画及び管理

作成するドキュメント　ISMS年間計画表

年間計画表

No	実施事項		文書名	スケジュール							
				2023年5月				2023年6月			
				8	15	22	29	5	12	19	26
6.1	「リスク及び機会に対処する活動」の検討	外部および内部の課題に対する活動の検討	外部および内部の課題								
		リスクアセスメントの実施	資産目録								
			情報リスクアセスメント結果報告書								
		リスク対応のための計画作成	適用宣言書								
		（アクションプランの作成）	情報セキュリティリスク対応計画								
		管理策(ルール)の検討	情報セキュリティ手順書								
6.2	部門ごとに「情報セキュリティ目的及びそれを達成するための計画」を作成		ISMS有効性評価表								

ISMS：8. 運用

【参照：テキスト13-2-6】
第13章 - 36

8.2 情報セキュリティリスクアセスメント

追記するドキュメント　情報セキュリティリスクアセスメント結果報告書

結果報告書

起こり得る結果	リスク分析(一次評価)			優先順位	リスク対応					
	重要度	被害発生可能性	リスクレベル		保有	低減	回避	移転	管理策	対応
機密情報などが漏えいし顧客に影響、信用喪失	3	2	6	2		●			モバイル機器の利用ルールを整備・強化	済み
機密情報などが漏えいし顧客に影響、信用喪失	2	2	4	3		●			教育訓練	予定
機密情報などが漏えいし顧客に影響、信用喪失	3	3	9	1		●			• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	未定

ISMS：8. 運用

【参照：テキスト13-2-6】
第13章 - 36

8.3 情報セキュリティリスク対応

追記するドキュメント　情報セキュリティリスク対応計画

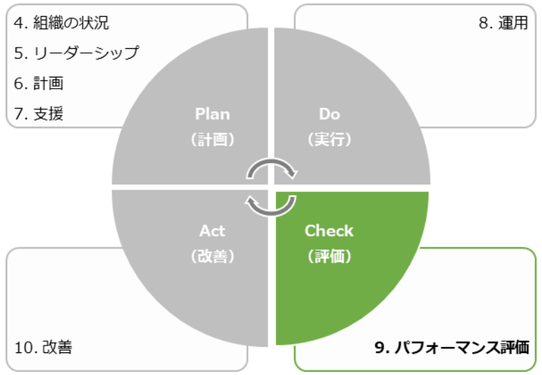
情報セキュリティリスク対応計画

No	管理策	タスク	担当	予定		実績		ステータス
				開始	終了	開始	終了	
1	モバイル機器の利用ルールを整備・強化	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
2	教育訓練	• ルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-	20XX/-/-	終了
3	• 情報の分類定義 • 分類ごとの情報の取扱いルール • ラベリング	• 情報の分類定義 • 分類ごとの取扱いルール検討 • 関係者に周知	委員長	20XX/-/-	20XX/-/-	20XX/-/-		着手

ISMS：9. パフォーマンス評価

概要

【参照：テキスト13-2-7】
第13章 - 37



パフォーマンス評価	作成ドキュメント（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の有効性を評価します。	• 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、あらかじめ定めた間隔で監査を実施します。	• 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の有効性を評価します。	• マネジメントレビュー報告書

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 38

9.1 監査、測定、分析及び評価

作成するドキュメント　ISMS有効性評価表

有効性評価表

【計画】

情報セキュリティ目的：・お客様との契約および法的または規制要求事項を尊重し遵守する
・情報セキュリティ事故を未然に防止する
・情報セキュリティ上の脅威から情報資産を保護する
・当社ISMSの意味を理解した活動の開始

評価指標：　ISMS教育受講／合格　100%(全従業者)
【備考】
取組みの初年度であるため、全従業者が活動に関与、さらには、活動を理解し、全社のセキュリティ目的の達成に向けた活動開始ができたことを確認する。

情報セキュリティ目的達成のための計画

実施事項	必要な資源	責任者	達成期限	評価方法
教育による活動の意味の理解	適用範囲の従業者がISMS教育を受講	ISMS事務局長	20XX年00月	受講者数および合格者数をカウントし、評価する

【評価】　　**評価日：【20XX/00/00】**

情報セキュリティ目的達成に関する評価結果　　**凡例　○：有効　×：有効ではない**

結果	備考
○	全従業員eラーニングでのテストを100点にて合格。有効性があるものと判断する。

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 39

9.2 内部監査

作成するドキュメント　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

内部監査とは

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 40

9.2 内部監査

内部監査チェックリスト

監査項目	チェック事項	確認結果・文書類
4. 組織の状況		
4.1 組織及びその状況の理解	組織は、組織の目的に関連し、かつ、そのISMSの意図した成果を達成する組織の能力に影響を与える、外部および内部の課題を決定しているか。	• 外部および内部の課題
4.2 利害関係者のニーズ及び期待の理解	次の事項を決定したか。 a) ISMSに関連する利害関係者 b) その利害関係者の、情報セキュリティに関連する要求事項	• 外部および内部の課題
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	ISMSの適用範囲は、文書化されているか。	• ISMSマニュアル • ISMS適用範囲 • レイアウト図 • ネットワーク図
5. リーダーシップ		
5.1 リーダージップ及びコミットメント	トップマネジメントは、 a） 情報セキュリティ方針および情報セキュリティ目的を確立し、それらが組織の戦略的な方向性と両立することを確実にしているか。	• 情報セキュリティ方針 • 質問で確認
5.2 方針	情報セキュリティ方針は、 e) 文書化した情報として利用可能であるか。	• 情報セキュリティ方針

事前に作成する部分　　**監査時に記載する部分**

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 41

9.2 内部監査

内部監査計画書

監査概要	
監査名称	ISO27001認証取得に関する内部監査
監査目的	ISO/IEC27001:2022認証取得に向けた当社ISMSの整備、運用状況を確認
監査テーマ	・管理策の運用状況、および有効性の確認 ・第一段階審査の指摘に対する改善状況の確認
監査方法	被監査部門に対するヒアリング、文書化された情報の閲覧、およびオフィスの視察
監査基準	JISQ27001:2022（ISO/IEC27001:2022)の要求事項、当社ISMSマニュアル、および情報セキュリティ手順書

詳細監査計画				
No	被監査部門名	監査人	応対者	日時
1	情報システム部	○○　○○	△△　△△	20XX/-/- 00:00
2	管理部	○○　○○	△△　△△	20XX/-/- 00:00
3	営業部	○○　○○	△△　△△	20XX/-/- 00:00
4	総務部	○○　○○	△△　△△	20XX/-/- 00:00

内部監査結果報告（予定）	
報告予定日	20XX年○月
報告手段	報告会の開催

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 42

9.2 内部監査

内部監査結果報告書

監査総評

ISMSの整備状況を確認
当組織でのISMSは、ISO27001:2022規格に基づく体制構築（文書化）をほぼ完了し、要求事項に対する重大な不適合は検出されなかった。全体として適切な有効な仕組みにより運用を開始したと判断できる。
また社員の周知に関しては、ISMS教育の実施などにより体制や方針などの周知を行っていた。

不適合・観察事項
一部ではあるが、対応が十分でない事項があったため○件を軽微な不適合、○件を観察事項とした。重大な不適合は、検出されなかった。

【軽微な不適合】

No	規格	内容
1	5.2 方針	規格では「情報セキュリティ方針は、次の事項を満たさなければならない。g) 必要に応じて、利害関係者が入手可能である。」としている。しかし、「情報セキュリティ方針」について、お客様などの利害関係者が入手可能であることを確認できなかった。

【観察事項】

No	規格	内容
1	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	ISMSマニュアルとネットワーク図で適用範囲の表現が同じであることの確認が難しい状況でした。ISMSマニュアルでは、ルータまで。ネットワーク図では、ONUまで。
2	7.3 認識	実施中のISMS教育の終了をお願いします。

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 43

9.3 マネジメントレビュー

作成するドキュメント　マネジメントレビュー報告書

マネジメントレビューとは

ISMS：9. パフォーマンス評価

【参照：テキスト13-2-7】
第13章 - 43

9.3 マネジメントレビュー

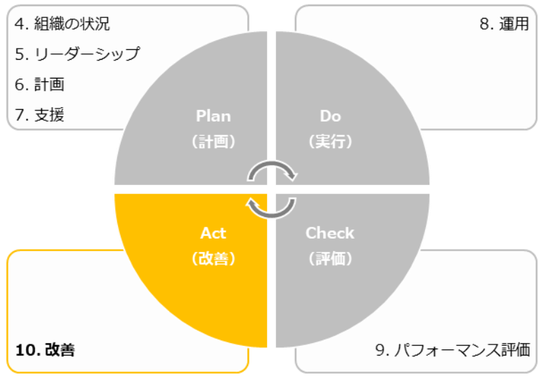
含める項目

インプットに含める必要がある事項
1. 前回までの指示事項に対する処置の進捗や結果 トップマネジメントから前回指示された改善活動の進捗状況や結果を記載します。初回の場合は記載しません。
2. ISMSに関連する外部および内部の課題の変化 事業の変化、法規制の改正など、昨年と比べた外部および内部の課題の変化について記載します。
3. ISMSに関連する利害関係者のニーズおよび期待の変化 「顧客や取引先、従業員、株主など利害関係者からの情報セキュリティに関する要求」の変化について記載します。
4. 情報セキュリティパフォーマンスの実績報告 以下の内容について、報告します。 • 不適合および是正処置 不適合に対する是正処置の実施状況を報告します。 • 監視および測定の結果 情報セキュリティパフォーマンスや、ISMSの有効性についての監視、測定結果を報告します。 • 監査結果 内部監査の結果を報告します。 • 情報セキュリティ目的の達成 情報セキュリティ目的の達成数や未達成数など、情報セキュリティ目的の達成状況を報告します。
5. 利害関係者からのフィードバック 利害関係者から、情報セキュリティに関する要望などについて、対応した結果を報告します。
6. リスクアセスメントの結果およびリスク対応計画の状況 リスクアセスメントにより、新しく特定したリスクや、リスク対応計画の進捗状況を報告します。
7. 継続的改善の機会 トップマネジメントに改善策を提案します。
アウトプットに含める必要がある事項
1. 継続的改善の機会 改善すべき内容について指示を記載します。
2. ISMSのあらゆる変更の必要性 ISMSに関して、次年度以降変更すべき内容について指示を記載します。

ISMS：10. 改善

概要

【参照：テキスト13-2-8】
第13章 - 45



10. 改善	作成ドキュメント（例）
10.1 継続的改善 ISMSのPDCAサイクル（「4. 組織の状況」から「10. 改善」までの活動）を継続して実施し、情報セキュリティパフォーマンスを向上させるために必要となる改善を行っていきます。具体的には、情報セキュリティ方針や情報セキュリティ目的の計画、リスクアセスメントやリスク対応をもとに決定した管理策の実施を継続して行い、改善していきます。	―
10.2 不適合及び是正処置 不適合が発生した際に是正処置を実施します。不適合とは、ISMSの要求事項を満たしていないことです。具体的には、管理策の不備や未実施、セキュリティインシデントの発生などのことです。	• 是正要求書兼回答書

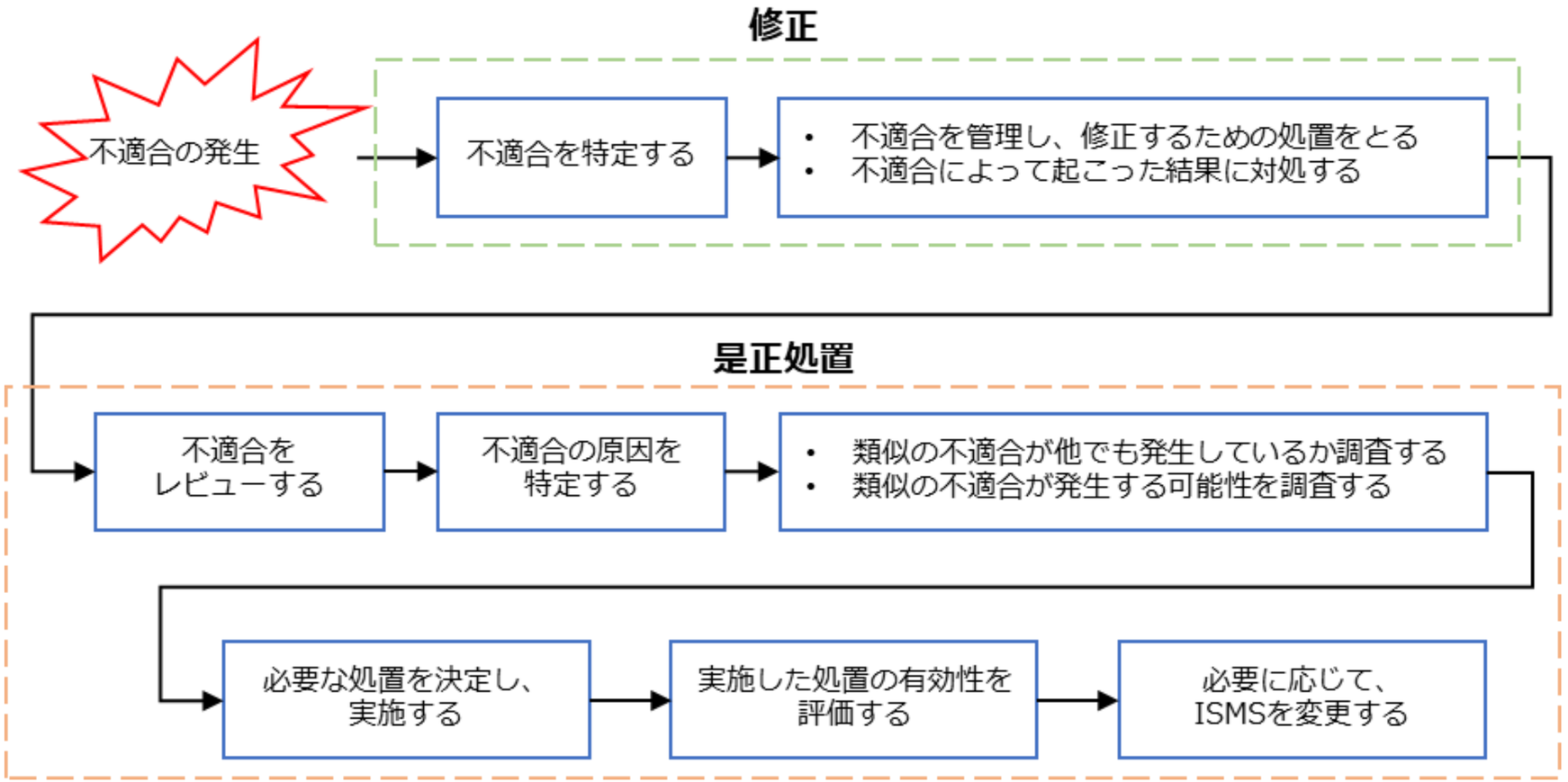
ISMS：10. 改善

【参照：テキスト13-2-8】
第13章 - 46

10.1 不適合及び是正処置

作成するドキュメント　是正要求書兼回答書

プロセス



ISMS：10. 改善

【参照：テキスト13-2-8】
第13章 - 47

10.1 不適合及び是正処置

是正要求書兼回答書

整理番号	00-00	対象部門	○○○○部門	発効日	20XX 年 - 月 - 日

入力情報	分類	監査	■	内部監査における指摘事項													
			□	外部機関が実施した監査における指摘事項（機関名：　　）													
			監査年月日		年		月		日	監査者							
			指摘のランク	観察事項						要求事項項番	7.2 力量						
		監査以外	□	セキュリティインシデントの関連した改善事項													
			□	外部の利害関係者からのニーズに基づく改善事項													
			□	内部において提案された改善事項													
			□	その他（　　）													
	内容		一部情報セキュリティ委員会担当者が仮任命のため、今後本任命を行っていく。												承認	作成	
処置計画	修正		力量の確認。任命力量確認表の更新。														
			実施予定日		年		月		日								
	評価		類似の不適合の有無	無	発生する可能性	無											
		原因	対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。														
			原因を除去するための計画の必要性	有	※有の場合原因除去の計画を記載												
	原因除去		対応の認識はあり、あくまでも観察事項としての取扱いのため、原因などはなし。												承認	作成	
			実施予定日		年		月		日								
実施報告	内容		上記の通り、「ISMS年間計画表」を修正し、運用チェックリストによる点検を実施した。												承認	作成	
			実施完了日		年		月		日								
処置確認	確認		「ISMS年間計画表」の修正、運用チェックリストによる点検記録を確認した。												承認	作成	
			確認日		年		月		日								
	有効性		セキュリティ手順の実行、および技術的遵守について、点検漏れのリスクが低減された。														
			評価日		年		月		日	フォロー監査の要・不要							

１．組織的管理策

組織的管理策を参考とした対策基準・実施手順の策定

組織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14-1-1.】
第14章 - 02

対策基準の策定

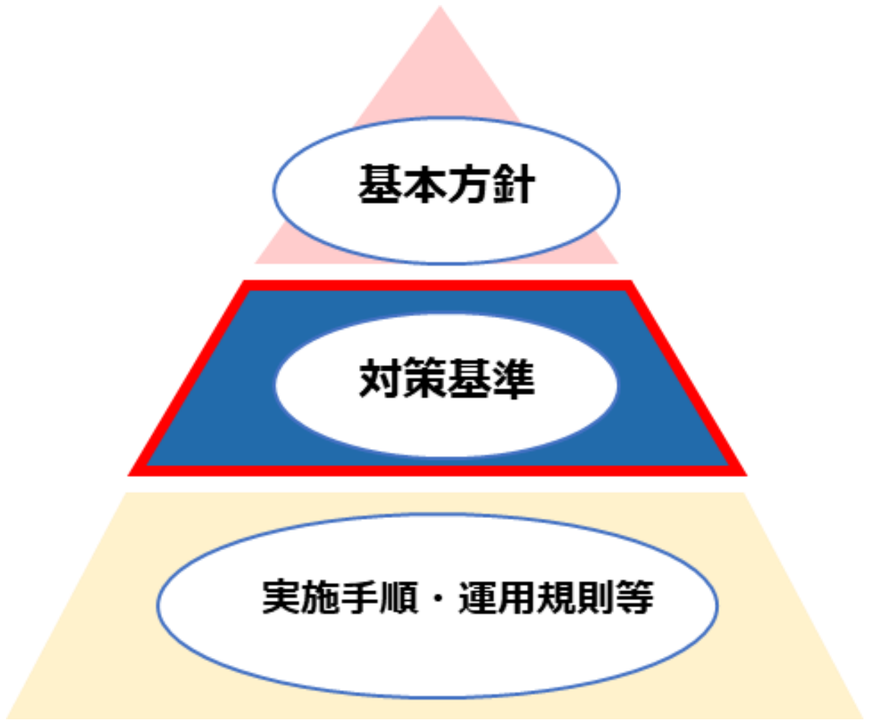
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

組織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

組織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14-1-1.】
第14章 - 04

対策基準（例）

対策基準（例）
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。 **5.2 情報セキュリティの役割及び責任** 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。 **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。

組織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14-1-1.】
第14章 - 04

対策基準（例）

対策基準（例）
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。 **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。 **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による協会・団体との連絡体制を確立し維持しなければならない。 **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。

組織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14-1-1.】
第14章 - 05

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

組織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14-1-1.】
第14章 - 05

対策基準（例）

対策基準（例）

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。

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。

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。

組織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14-1-1.】
第14章 - 05

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

組織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14-1-1.】
第14章 - 06

対策基準（例）

対策基準（例）
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。 **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** 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。 **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。

組織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14-1-1.】
第14章 - 06

対策基準（例）

対策基準（例）
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。 **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。 **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。

組織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14-1-1.】
第14章 - 06

対策基準（例）

対策基準（例）
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。 **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。 **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。 **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。

組織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14-1-1.】
第14章 - 07

対策基準（例）

対策基準（例）
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。
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。
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。
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。
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。

組織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14-1-1.】
第14章 - 07

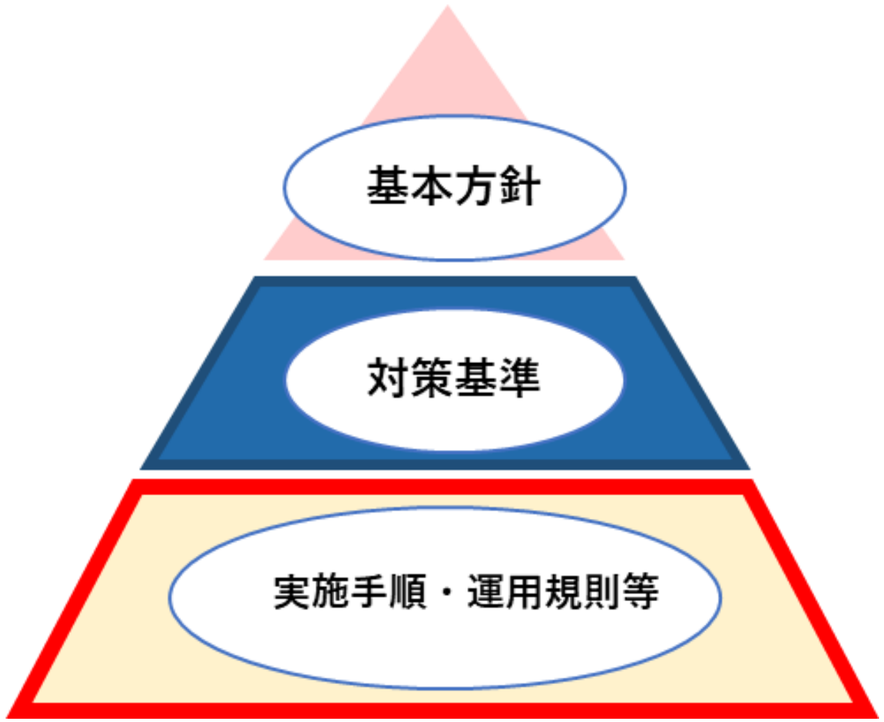
対策基準（例）

対策基準（例）
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。 **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みについて、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。 **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、規則および標準を遵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。 **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。

組織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

組織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14-1-2.】
第14章 - 08

5.1 情報セキュリティのための方針群

実施手順（例）

情報セキュリティ委員会は、「情報セキュリティ方針」などの情報セキュリティに関する方針を定義し、トップマネジメント（経営層）の承認を得る。また、情報セキュリティ委員会は、情報セキュリティに関する方針を適用範囲内の全従業者に公表する。また、「情報セキュリティ方針」は外部関係者にも公表する。

情報セキュリティ委員会は、「情報セキュリティ方針」以外の情報セキュリティのための方針群を、本手順において定める。方針群には以下を含める。

a. モバイル機器の方針
b. テレワーキング
c. アクセス制御方針
d. 暗号による管理策の利用方針
e. クリアデスク・クリアスクリーン
f. 情報転送の方針（および手順）
g. セキュリティに配慮した開発のための方針
h. 供給者関係のための情報セキュリティの方針

組織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14-1-2.】第14章 - 09

5.2 情報セキュリティの役割及び責任

実施手順（例）

トップマネジメント（経営層）は、情報セキュリティに関連する役割を持つ情報セキュリティ委員会、内部監査責任者に対して、以下の責任および権限を割り当てる。また、トップマネジメント（経営層）は、これらの役割、責任および権限を従業者に伝達する。情報セキュリティの運用に際し、トップマネジメント（経営層）は、情報セキュリティ委員会の設置および運営を実施する。

情報セキュリティ委員会の役割は以下の通り。

a. リスク対応計画の策定
b. 情報セキュリティ実行体制の構築
c. 選択された管理策の実施
d. 教育・訓練
e. 運用の管理
f. 経営資源の管理
g. 情報セキュリティ事象・セキュリティインシデントの管理
h. 関連当局との連絡（警察・審査機関・コンサル会社・取引先・委託先など）

組織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14-1-2.】第14章 - 09

5.2 情報セキュリティの役割及び責任

実施手順（例）

情報セキュリティ委員会の責任および権限は以下の通り。

役割	責任および権限
情報セキュリティ委員会責任者	管理策の実施・運用について統括する。 管理策の成果をトップマネジメント（経営層）に報告する。
教育責任者	管理策に関する教育計画の立案と実施を行う。
部門管理者（運用委員）	情報セキュリティの部門代表者として、部門を管理する。
情報システム管理者	情報システム部門の管理者で、情報システム管理に関する規定・規則に従い、情報セキュリティを維持するための安全管理対策を実施する。
文書管理責任者	管理策に関する文書や記録などの維持・管理を行う。

内部監査責任者の責任および権限は以下の通り。
内部監査責任者は、管理策とその実施状況に関わる監査を統括する責任と権限を有する。

組織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14-1-2.】
第14章 - 10

5.3 職務の分離

実施手順（例）
a. 当組織は、申請者または作業者と、承認者を分離するように組織設計する。 b. 従業員の制約により兼任せざるを得ない場合、別部門などによる監視を行うことを条件に、兼任できる。

5.4 経営陣の責任

実施手順（例）
トップマネジメント（経営層）はすべての従業者に対し、情報セキュリティ方針、各実施手順、並びにその他情報セキュリティに関する要求事項の遵守を求める。

組織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14-1-2.】

5.5 関係当局との連絡

実施手順（例）

情報セキュリティ委員会は、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。

関係当局	連絡手段	URL	主目的
【IPA】コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口	ウイルス発見・感染の届出 virus@ipa.go.jp 不正アクセスの届出 crack@pa.go.jp	https://www.ipa.go.jp/security/todokede/crack-virus/about.html	ウイルス感染や、不正アクセスによる被害を報告するため。
【IPA】情報セキュリティ安心相談窓口	TEL:03-5978-7509（受付時間10:00～12:00、13:30～17:00 土日祝日・年末年始は除く）anshin@ipa.go.jp	https://www.ipa.go.jp/security/anshin/about.html	ウイルス感染や不正アクセスに関する技術的な内容の相談に対して、アドバイスをもらうため。
【警視庁】サイバー犯罪相談窓口	TEL:03-5805-1731 受付時間：午前8時30分から午後5時15分まで（平日のみ）	https://www.keishicho.metro.tokyo.lg.jp/sodan/madoguchi/sogo.html	サイバー犯罪被害について相談するため。
【個人情報保護委員会】個人情報・マイナンバーの漏えい報告	Webフォームで報告	https://www.ppc.go.jp/personalinfo/legal/leakAction/	個人情報、マイナンバーの漏えいに対処するため。
【JPCERT/CC】インシデント対応依頼	Webフォームまたは、以下のメールアドレスに報告 info@jpcert.or.jp	https://www.jpcert.or.jp/form/	セキュリティインシデント対応を支援してもらうため。

組織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14-1-2.】
第14章 - 11

5.6 専門組織との連絡

実施手順（例）

情報セキュリティ委員会は、専門組織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。

専門組織	情報の入手方法	URL	主目的
【IPA】重要なセキュリティ情報	Webページを閲覧	https://www.ipa.go.jp/security/security-alert/2023/index.html	危険性が高いセキュリティ上の問題と対策に関する最新情報を収集するため。
【IPA】ランサムウェア対策特設ページ	Webページを閲覧	https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html	ランサムウェア対策に関する最新情報を収集するため。
【個人情報保護委員会】注意情報一覧	Webページを閲覧	https://www.ppc.go.jp/news/careful_information/?category=39	セキュリティ・個人情報・マイナンバーに関する、注意事項を把握するため。
【JPCERT/CC】注意喚起	Webページを閲覧	https://www.jpcert.or.jp/at/2023.html	脆弱性に関する最新情報を収集するため。

組織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14-1-2.】第14章 - 11

5.7 脅威インテリジェンス

実施手順（例）

1. 既存または新たな脅威に関する情報を、次に示す専門機関から収集する。
   ・IPA
   ・JVN（Japan Vulnerability Notes）
   ・JPCERT/CC
   ・ISAC（Information Sharing and Analysis Center）
   ・個人情報保護委員会
   収集する情報は、以下のようなものとする。
   ・変化する脅威の状況に関する情報（例：攻撃者や攻撃の種類）
   ・攻撃の方法、使用されるツールや技術に関する情報
   ・特定の攻撃に関する詳細な情報
2. 収集した情報を分析する。
   脅威が、自組織にどのような影響を及ぼすか把握するために、収集した情報をもとにリスクアセスメントを実施する。
3. リスク低減の処置を実施する。
   リスクアセスメントの結果をもとに、ファイアウォール・侵入検知システム・マルウェア対策ソリューションなど、技術的に予防、検知を行うための管理策を採用する。

組織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14-1-2.】第14章 - 12

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

実施手順（例）

a. プロジェクト管理者は、プロジェクトにおける必要な管理策を特定する。
b. プロジェクトにおける必要な管理策は、プロジェクト終了後も考慮する。
c. プロジェクト管理者は、情報セキュリティ責任者を任命する。
d. 情報システム管理者は、業務用情報システムの導入・改善にあたっては、必要に応じて情報セキュリティ上の要求事項を、要件定義書や提案依頼書などにより文書化する。
文書には下記から必要な事項を含める。
・情報システムの設置場所（環境・障害からの対策を含む）に関する事項
・無停電電源装置などのサポートユーティリティに関する事項
・保守契約に関する事項
・システムの冗長化に関する事項
・通信、データの安全対策に関する事項
・受け入れテストに関する事項
・アクセス権限に関する事項

組織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14-1-2.】
第14章 - 12

5.9 情報及びその他の関連資産の目録

実施手順（例）
a. 情報セキュリティ委員会は「資産目録」を作成し、当組織における重要な資産を識別する。また「資産目録」を「年間計画表」に従い、最低年1回見直す。 b. 情報セキュリティ委員会は「資産目録」において特定した資産に対し、同目録上に管理責任者（リスク所有者）を記載することで管理責任を明確にする。

組織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14-1-2.】
第14章 – 13, 14

5.10 情報及びその他の関連資産の利用の許容範囲

実施手順（例）
情報の区分ごとの取扱いルールを以下に示す。 情報の区分は「5.12 情報の分類」で、ラベル表示については「5.13 情報のラベル付け」で定める。 分類についてはセミナーテキスト参照

5.11 資産の返却

実施手順（例）
情報セキュリティ委員会は、退職者が発生した際に、以下の対応を部門長に要求し、実施されたことを確認する。 a. 名刺、社員証、IDカードなどの返却 b. 会社が支給したノートPCや携帯電話などの返却 c. 紙で保管する書類の返却、または廃棄

組織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14-1-2.】第14章 – 14

5.12 情報の分類

実施手順（例）

情報は一般・社外秘・関係者外秘で分類する。
情報セキュリティ委員会は、情報の分類を最低年1回見直す。

分類	内容
一般	下記以外
社外秘	関係者外秘以外の機密事項であり、当組織の従業者に対してのみ開示が許されるもの。（取引先に開示する必要があるものは除く。）または情報セキュリティに関わる規定・手順書類。
関係者外秘	情報が外に漏れることによって、当組織が重大な損失もしくは不利益を受けるような恐れのある機密事項であり、職務上の限られた関係者のみに開示を許すもの。関係者が明示的に定められていない場合、関係者とは、情報を直接配布された者を指す。

組織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14-1-2.】
第14章 – 14

5.13 情報のラベル付け

実施手順（例）

従業員は、取扱う情報が一般・社外秘・関係者外秘の区分のうち、どれに該当するか認識できる必要がある。
書類の分類を容易に認識できない場合は、以下のいずれかの方法により適切なラベル付けを行う。

a. 分類をシールなどの色により識別する。
b. ファイルなどに分類を記入（またはスタンプ）することで識別する。
c. 分類ごとに収納場所を分ける。

組織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14-1-2.】第14章 – 15

5.14 情報伝送

実施手順（例）
a. 重要な情報を外部に送信する場合は、セキュアなファイル共有サービスを利用する。やむを得ずファイル共有サービスが利用できない場合は、受信者と合意したうえで、メールに添付して送信する。 b. 重要な情報を外部にFAXにて送信する場合は、入力した番号と、名刺や送り状を照合し、間違えがないことを確認してからスタートボタンを押す。また頻繁に送信する送り先は短縮ダイヤルに登録する。 c. 認可されていない者に聞かれる可能性がある場所で、重要な情報を口頭で伝えることは禁じる。 d. 重要な情報を外部に郵送する場合は、配達記録郵便や宅配便など配達記録が残る手段をとる。 e. 重要な情報を格納した媒体は、手渡しを原則とし、やむを得ず郵送する場合は、十分な梱包により媒体を保護する。 f. 個人情報の授受記録 ・紙や記憶媒体による個人情報の受け渡しに際しては、送付票や受領証などで受け渡しの完了を確認する。 ・電子メールにより個人情報の受け渡しを行う際には、送信済みメールおよび、受領確認の返信メールのいずれかまたは両方を受け渡し記録とする。 g. 電子メールの利用 ・電子メールは会社所定のソフトを使用し、その利用は業務上必要な場合に限定する。 ・社外メーリングリストへの参加は、原則禁止とする。 ・重要な情報（社外秘以上）はメール本文に記載して送信せず、aに従う。 h. 情報転送に関する合意 ・情報の転送先との間で、情報転送の手段について、あらかじめ合意を得る。 ・重要な情報を外部にメール添付またはFAXにて送信する場合は、必要に応じて送信予告、到着確認の電話を掛ける。 ・宅配便業者を利用する場合は、会社が指定する業者を利用する。 i. 電子的メッセージ通信 ・当組織のWebサイトに入力する情報の通信は、SSL/TLSにより行う。 ・電子データによる個人情報をインターネット経由で送受信する際は、SSL/TLSなどの暗号化対策やパスワード設定などの措置を講じる。

組織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14-1-2.】第14章 – 16

5.15 アクセス制御

実施手順（例）
a. 業務に必要な者のみが情報にアクセスできるようにし、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。 b. 社内LANは、情報システム管理者の承認を得た従業員、装置に限り接続する。 c. 社内の情報システムへの外部からのアクセスは、ファイアウォールなどによって通信を制限する。 d. 外部から社内のサーバに接続する場合、VPN接続を使用する。 e. 無線LANは物理的・論理的な認証、通信の暗号化などを施したうえで利用する。 f. サーバ室へ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。 g. サーバ室は、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。

5.16 識別情報の管理

実施手順（例）
a. 情報システムの利用者登録および登録削除は、当該利用者の属する部門長が申請し、情報システム管理者の承認を得る。 b. 利用者登録は業務上必要な範囲で従業者に付与する。

組織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14-1-2.】第14章 – 17

5.17 認証情報

実施手順（例）
a. 情報システム管理者は、利用者に仮パスワードを発行する場合、利用者本人のみが知ることができる方法で通知する必要がある。 b. 情報システム管理者は、利用者に対し、仮パスワードを直ちに変更することを要求し、通知する。 c. 秘密認証情報の利用 ・利用者は、英数字と記号を混在した10文字以上のパスワードを設定し、アルファベットには大小文字の両方を含める必要がある。 ・他人に容易に推測されるようなわかりやすいパスワードの使用を禁じる。 ・他のサービスと重複するパスワードの利用を禁じる。 ・各システムにおける管理者IDのパスワードは、情報システム管理者において厳重に管理する必要がある。 ・利用者および情報システム管理者は、パスワードの代替もしくは補完のために、指紋などの生体認証、専用のアプリやメールなどを利用するワンタイムパスワードによる認証、PINコード・機器認証などを利用するパスキーによる認証方式を採用する。 d. パスワード管理システム ・パスワードの入力は対話式とする。 ・パスワード入力時に画面に表示させないようにする。

組織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14-1-2.】
第14章 – 17

5.18 アクセス権

実施手順（例）
a. 利用者のアクセス権は、重要情報に対しては必要最小限の者がアクセスするという原則のもとに、情報システム管理者が検討し、設定を行う。 b. 情報システム管理者は、定期的（最低年1回）および必要時にアクセス権限の棚卸および見直しを行う。 c. 退職者が発生した際は、業務に支障がないよう調整し、速やかに該当アカウントを削除する必要がある。申請は、当該従業員が最後に所属した部門の長がアクセス権限の削除を申請し、情報システム管理者、またはその指名する従業員が削除する。 d. 他部署への移動が生じた際は、aの手順に従い削除する。また、新規のアクセス権限は移動先部門の長が申請し、同様の手順に従い登録する。

組織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14-1-2.】
第14章 – 18

5.19 供給者関係における情報セキュリティ

実施手順（例）
a. 当組織における供給者には、以下がある。 ・ISP、電話サービス、IT機器などのサービス提供者 ・情報システムの開発・保守における外部委託先 ・会計、税務、法律などの専門サービス提供者 ・清掃業者、廃棄業者 ・クラウドサービス b. 情報セキュリティ委員会は、部外者・外部組織によるオフィスエリアや情報システムへのアクセスを許可する際に生じる可能性があるリスクを考慮し、情報セキュリティ上の要求事項を明確にする。

5.20 供給者との合意における情報セキュリティの取り扱い

実施手順（例）
a. 提供されるサービスの利用は、次の手順に従い行う。 1.「委託先審査票」による評価・選定を行う。 2. 情報セキュリティ要求事項を考慮し、次の事項を含む契約を締結する。 ・機密保持契約などの情報の取扱いに関する契約 ・使用許諾に関する取り決め、コードの所有権および知的所有権（開発の場合） ・実施される作業場所および入退室管理 ・外部委託先が不履行となった場合の預託契約に関する取り決め 3. 情報セキュリティ委員会は、「5.19供給者関係における情報セキュリティ」において検討したリスクを考慮し、必要に応じて第三者との間で契約を締結する。 b. クラウドサービスを介して重要資産を取扱う際は、利用者は多要素認証を有効にしてセキュリティを強化する必要がある。

組織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14-1-2.】
第14章 – 19

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

実施手順（例）
a. ICT製品・サービスの供給者との契約には、必要に応じて再委託に関する事項を盛り込む。 b. クラウドサービスの利用にあたっては、クラウドサービス提供者の事業継続性、および以下のサービスに関する情報セキュリティ事項を考慮のうえ、クラウドサービスを選定する。 ・サービスの導入実績、信頼性 ・利用者サポート機能 ・利用終了後のデータの扱い ・サービスの可用性 ・暗号化など、通信経路の安全対策

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

実施手順（例）
a. 情報セキュリティ委員会は、サービスの供給者に対して、あらかじめ定められた頻度（最低年1回）において契約の履行状況ならびに「委託先審査票」による遵守状況の確認を行う。 b. サービスの供給者との間で契約内容やサービスレベルに変更があった場合、変更点を受け入れることができるか否かを検証し、契約内容の見直しを実施する。

組織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14-1-2.】
第14章 – 20

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

実施手順（例）
クラウドサービスを導入する際、以下の評価表をもとにクラウドサービスを評価し、自社のセキュリティ要件事項を満たしているか確認する。 詳細はテキスト参照

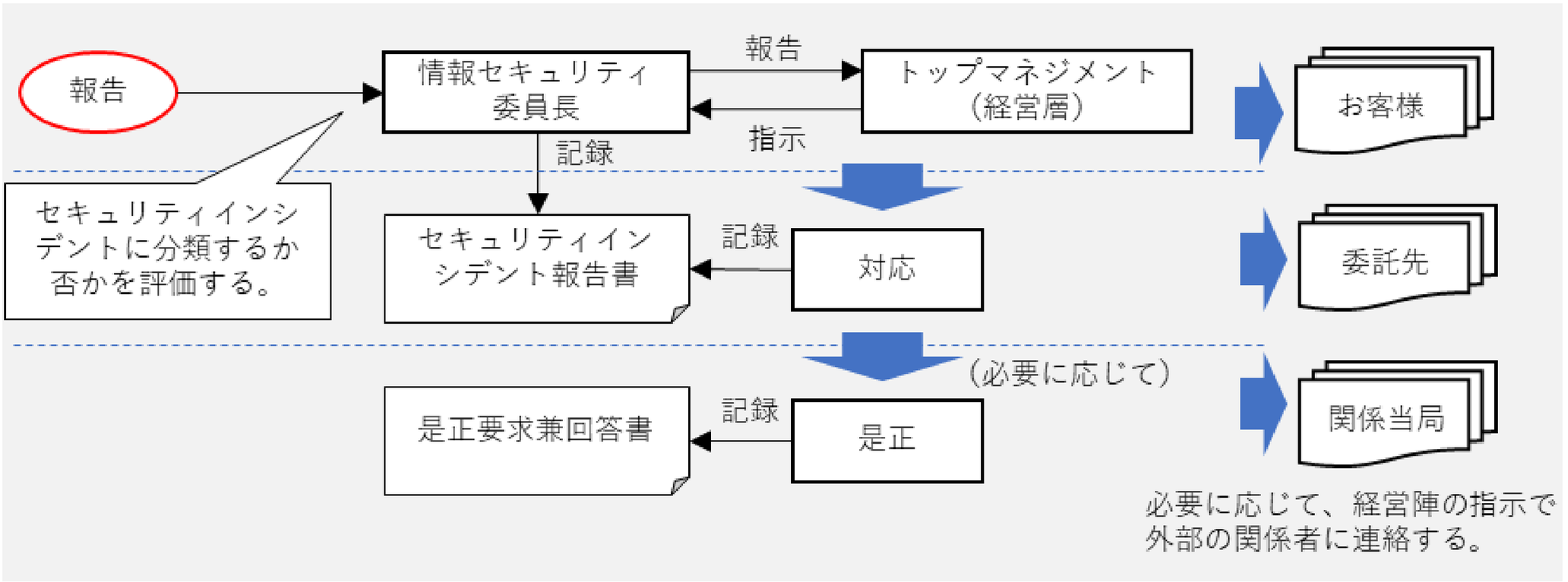
組織的管理策を参考とした対策基準・実施手順の策定

【参照：テキスト14-1-2.】
第14章 – 21

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

実施手順（例）

セキュリティインシデントへの対応は、以下の手順で行う。
管理層の責任のもと、以下の手順を関係者に伝達する。



組織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14-1-2.】
第14章 – 21

5.25 情報セキュリティ事象の評価及び決定

実施手順（例）

a. セキュリティの弱点、脅威に気付いた場合もしくは疑いを持った場合は、情報セキュリティ委員会に報告する。この際、自己で解決することよりも報告を優先させる。

b. 情報セキュリティ事象の評価は、以下の表に従い、部門管理者（情報セキュリティ委員会メンバー）が行う。
・大、中の項目に該当する情報セキュリティ事象は、セキュリティインシデントとして分類する。
・項目の大、中、小の順に優先順位を付ける。

項目	小	中	大
分類	ヒヤリハット・事象	インシデント	インシデント
最終的に被害が及ぶ範囲	現状、事件・事故の発生には及ばない。（将来、被害が発生する可能性がある。）	社員または社内	顧客・取引先
連絡先	情報セキュリティ委員長	情報セキュリティ委員長	情報セキュリティ委員長 トップマネジメント（経営層） 外部関係者

組織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14-1-2.】
第14章 – 22, 23

5.26 情報セキュリティインシデントへの対応

実施手順（例）
セキュリティインシデントへの対応手順は以下の表に従う。 詳細はテキスト参照

5.27 情報セキュリティインシデントからの学習

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティインシデントを管理・分析し、問題があれば、計画を立ててトップマネジメント（経営層）へ提議する。計画には、解決に向けての処置方法・費用・実施予定日・責任者を明確にする。 b. 将来のセキュリティインシデントの起こりやすさや影響を減らすため、情報セキュリティ委員会は、セキュリティインシデントから得られた知識を活かして「6.3 情報セキュリティの意識向上、教育及び訓練」を強化・改善する。

組織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14-1-2.】第14章 – 23

5.28 証拠の収集

実施手順（例）
情報セキュリティ委員会は、情報システムの事故が特定の個人、または組織に起因するもので、事後処置が法的処置に及ぶ可能性のある場合には、必要な証拠の収集、保全に努める。

組織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14-1-2.】
第14章 – 24

5.29 事業の中断・阻害時の情報セキュリティ

実施手順（例）

a. 資産のリスク分析
「資産目録（情報資産管理台帳）」で特定した情報資産のうち、可用性の評価値が3の重要資産を情報セキュリティ継続のリスク分析対象とする。
※可用性の評価値は、「11-2-2. リスク特定」で記載している方法で算出する。

b. aにおいて登録した資産に対して、以下のリスクについて考慮する。
・地震・火災・洪水などの自然災害
・人的なミス
・システム障害
・健康上の問題

c. bのリスクが生じた際に影響を受ける業務プロセスを特定し、リスクが発生した場合のシナリオを作成する。

d. リスクが生じた場合の影響度と、リスクが発生する可能性について検討し、検討結果に基づき優先順位を決定する。

e. dにおいて、優先順位が高いと判断したものに対して「事業継続計画書」を作成し、トップマネジメント（経営層）の承認を得る。
「事業継続計画書」には以下の内容を含む。
・実行開始条件（リスクシナリオの発生）
・非常時手順（発生時の連絡手順）
・回復手順（復旧のための手順）
・回復目標（目標時間を必要に応じて決定）
・再開手順（回復後のリハーサル手順）
・試験のスケジュール
・教育（教育が必要な場合はその計画）

f. 策定した計画および手続について試験を実施し、試験の結果、必要があると判断した場合は計画を更新する。試験は以下のいずれかの方法、またはその組み合わせにより行う。
・机上試験
・模擬試験
・技術的回復試験
・代替施設における回復試験
・供給者施設およびサービスの試験

g. 情報セキュリティ委員会は、事業継続に関する試験を最低年1回、継続的に実施する。

組織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14-1-2.】
第14章 – 25

5.30 事業継続のためのICTの備え

実施手順（例）
a. ビジネスインパクト分析（不測のインシデントによって業務やシステムが停止した場合、会社の事業にどのような影響があるかを分析すること）を行い、事業継続が困難な状況を特定する。 b. 事業が中断・停止になった際の対応手順を策定し、文書化する。 c. 策定した対応手順が有効であることを確実にするため、あらかじめ定めた間隔（年1回以上）で試験を実施し検証する。

組織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14-1-2.】
第14章 – 26

5.31 法令・規制及び契約上の要求事項

実施手順（例）

a. 情報セキュリティ委員会は、当組織が遵守すべき法令、規制、および契約上の要求事項を識別し、「情報セキュリティに関する法令規制一覧表」に記載する。「情報セキュリティに関する法令規制一覧表」は最低年1回見直す。
b. 情報セキュリティ委員会は、当組織の従業者が「情報セキュリティに関する法令規制一覧表」を、必要に応じていつでも参照できる状態にする。
c. 特定した要求事項を満たすために、必要に応じて教育などのテーマとする。
d. 暗号化した装置を輸出する場合、または海外に持ち出す場合、該当する法規制について調査を行い、必要であれば対応を行う。

情報セキュリティに関連する法律（例）	概要
特定電子メールの送信の適正化等に関する法律	利用者の同意を得ずに広告、宣伝または勧誘などを目的とした電子メールの送信を禁止している。
電子署名及び認証業務に関する法律	「本人による一定の条件を満たす電子署名」がなされた文書は、本人の手書署名・押印がある文書と同様、真正に成立したものと推定されることが定められている。
著作権法	プログラムやマニュアル、ホームページなどは、著作権の対象であり、無断での複製は、著作権法の侵害になる。
不正アクセス禁止法	不正アクセス行為や、不正アクセス行為につながる識別符号（ID、パスワード）の不正取得・保管行為、不正アクセス行為を助長する行為などを禁止している。
刑法	無断でデータを改ざん・破壊する行為や、虚偽の金融機関を名乗ったサイトや電子メールを使い、金銭をだまし取るような行為などは、刑法に違反する。

組織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14-1-2.】
第14章 – 27

5.32 知的財産権

実施手順（例）
a. 知的財産権を保護するためのルールを策定し、組織内で教育・啓発活動を行う。 b. 知的財産権を侵害する行為を禁止する。 c. 知的財産権を侵害する行為が発生した場合には、速やかに是正措置を講じる。 d. ソフトウェアなどの使用許諾計画を遵守する。 e. 情報システム管理者は、パッケージソフトのライセンス管理を適切に行う。

組織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14-1-2.】
第14章 – 28

5.33 記録の保護

実施手順（例）
当組織における記録は、関連する法令に基づき次表の保存期間にわたり、消失、破壊、改ざん、不正なアクセス、流失などがないように適切に保存する。 詳細はテキスト参照

5.34 プライバシー及びPIIの保護

実施手順（例）
個人情報は、「5.10 情報およびその他の関連資産の利用の許容範囲」の取扱いルールに従い、厳重に取扱う。

組織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14-1-2.】
第14章 – 29

5.35 情報セキュリティの独立したレビュー

実施手順（例）
a. 年に1度、内部監査により独立したレビューを行う。 b. 以下に例示する、情報セキュリティに影響のある変化が生じた場合も、内部監査により独立したレビューを行う。 ・事業の追加/変更、業務手順の大幅な変更 ・住所変更、拠点の新設 ・情報セキュリティに関する主たる担当者の変更 ・関係する法令・規制、または契約の大幅な変更

5.36 情報セキュリティのための方針群、規制及び標準の順守

実施手順（例）
a. 情報セキュリティ委員会は、セキュリティに関する手順や実施標準が正しく実施されていることを確実にするため、「運用チェックリスト」にて、定期的（3ヶ月ごと）に点検を行う。 b. 情報セキュリティ委員会（入退管理責任者）は、入退記録が適切にとられているかどうかを月に1度確認する。また、入退管理が有効かつ適切に実施されていることを定期的に確認し、不備が発見された場合は速やかに是正の処置をとる必要がある。 c. 情報システム管理者は、技術的な遵守事項が正しく実施されていることを確実にするため、上記のa、bに従い点検する。

組織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14-1-2.】
第14章 – 29

5.37 操作手順書

実施手順（例）
情報処理設備の正確、かつ、セキュリティを保った運用を確実にするために、次の事項を明記した手順書を文書化し、必要に応じて利用者が参照できるようにする。 a. システムが故障した場合の再起動および回復の手順 b. 記憶媒体の取扱い手順 c. バックアップの取得手順 d. 保守手順 e. 容量、能力、パフォーマンスおよびセキュリティなどの監視手順

2. 人的管理策

人的管理策を参考とした対策基準・実施手順の策定

人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14-1-1.】
第14章 – 02

対策基準の策定

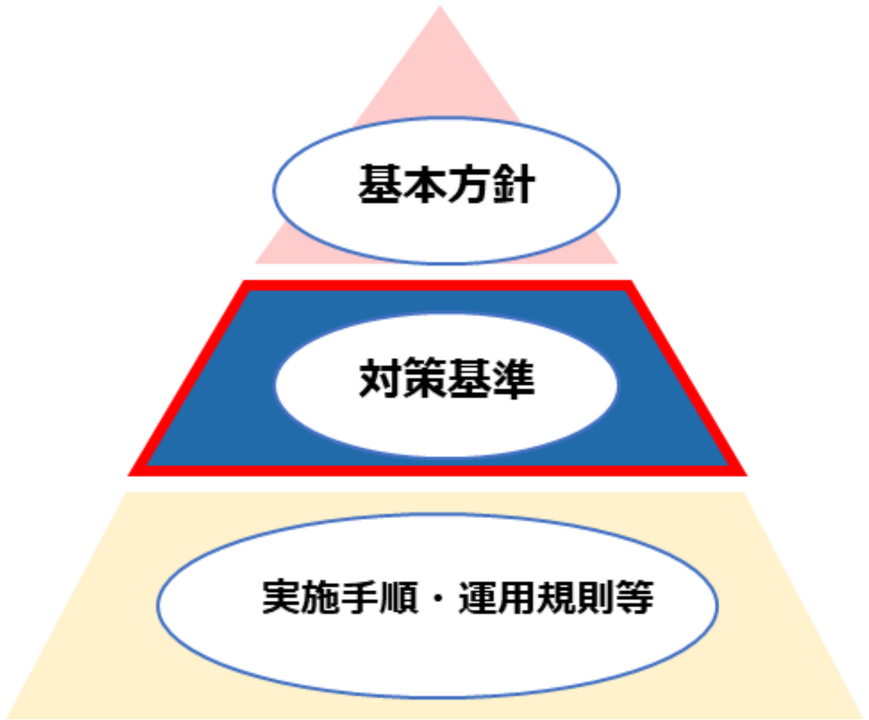
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

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

【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

人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15-1-1.】
第15章 – 03

対策基準（例）

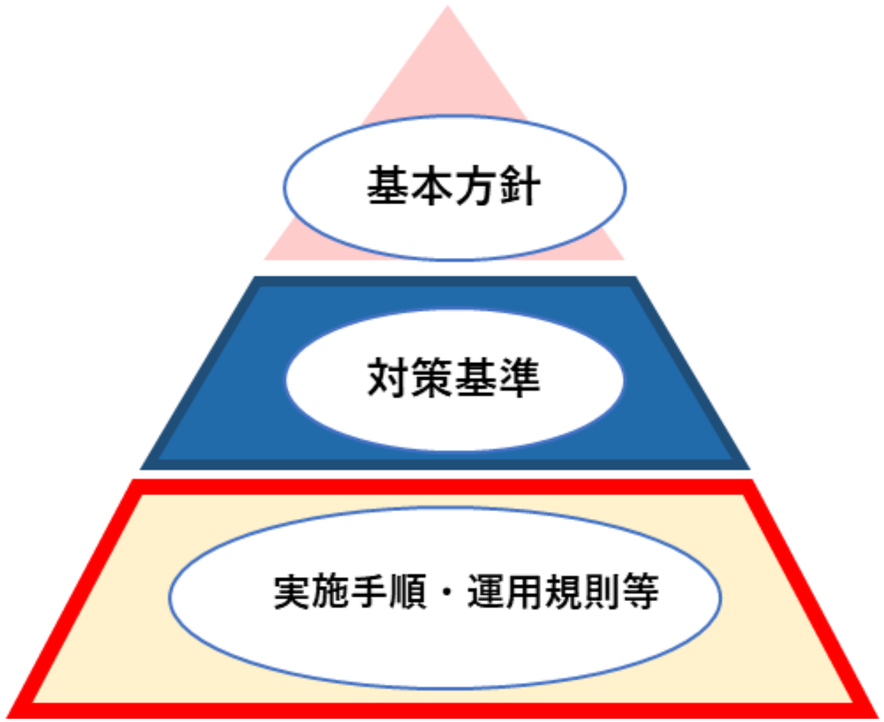
対策基準（例）
6.1 選考 従業員や契約相手を選定する際、個人情報の保護や雇用に関する法令を考慮して経歴などを確認しなければならない。
6.2 雇用条件 雇用契約書には、情報セキュリティに関する要員および組織の責任を記載しなければならない。
6.3 情報セキュリティの意識向上、教育及び訓練 従業員に対し、情報セキュリティに関する教育および訓練を実施しなければならない。
6.4 懲戒手続 情報セキュリティ方針に違反した場合の懲戒手続を、正式に定めなければならない。
6.5 雇用の終了又は変更後の責任 雇用の終了または変更の後も引き続き有効な情報セキュリティの責任や義務を、明確にしなければならない。
6.6 秘密保持契約又は守秘義務契約 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。
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。
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。

人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

人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15-1-2.】
第15章 – 04

6.1 選考

実施手順（例）
従業者の募集・採用プロセスは以下の点を考慮のうえ行う。 a. 取得した履歴書、スキルシートなどから業務上の要求事項への適合を判断し、選考を行う。 b. 採用時の面接などにおける態度や言葉遣いなどから倫理観を判断し、選考を行う。 c. 役員や管理職の採用に関しては、過去の信用情報など、より詳細な調査を行う場合があるが、この際は本人の同意を得たうえで行う。

6.2 雇用条件

実施手順（例）
情報セキュリティに関する責任を理解し、情報セキュリティ方針を守ることを従業員に誓約させるため、雇用契約書に、情報セキュリティに関する事項を盛り込み、誓約書に署名を求める。

人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15-1-2.】
第15章 – 05

6.3 情報セキュリティの意識向上、教育及び訓練

実施手順（例）

a. すべての従業者は、職務に関連する方針および手順についての適切な、意識向上のための教育および訓練を受ける必要がある。
b. 当組織では従業者が次の事項に関して認識を持てるよう教育・訓練を実施する。
・情報セキュリティ方針
・情報セキュリティパフォーマンスの向上によって得られる便益を含む、情報セキュリティに対する自らの貢献
・ISO/IEC 27001の要求事項に適合しないことの意味
c. 教育計画は情報セキュリティ委員会が作成し、トップマネジメント（経営層）が承認する。
d. 当組織の主な教育を以下に示す。（以下の教育は「教育実施記録」に残す。）
・新任部門管理者（運用委員）
新任の情報セキュリティ委員会メンバーに実施する。
・入社時・社内異動者の教育（適時）
新入社員、中間採用者に対して、入社時にセキュリティ教育を実施する。
・定期教育（「年間計画表」に基づく）
年に最低1回、適用範囲内の従業者に対して、情報セキュリティの理解、再確認と改善、向上のための教育を実施する。
・再教育
セキュリティ違反者および情報セキュリティに関する低理解度の従業者に対して、再教育を実施し、違反の再発防止に努める。
・実施した教育の有効性評価
上記の教育実施後理解度調査などを実施し、実施した教育の有効性の評価を行う。

人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15-1-2.】
第15章 – 06

6.4 懲戒手続

実施手順（例）
従業者が故意または過失により情報を漏えいした場合、または情報セキュリティ上の遵守事項に違反した場合は、罰則の対象とする。

6.5 雇用の終了又は変更後の責任

実施手順（例）
情報セキュリティの観点から、雇用の終了または変更後も従業員が守るべき義務や責任（たとえば守秘義務）について定め、雇用時の誓約書に盛り込むと同時に、雇用の終了または変更時に再確認する。

6.6 秘密保持契約又は守秘義務契約

実施手順（例）
a. 当組織の従業者は、当組織との間で機密情報に関する秘密保持の契約を締結する。なお、同契約には原契約の終了後も一定期間、秘密保持の義務が課せられる旨の条項を含める。 b. 当組織との委託先との間で、必要に応じて秘密保持の契約を締結する。 c. 情報セキュリティ委員会は、年に一度、情報セキュリティ要求事項に照らして、秘密保持の契約書の妥当性を検証する。

人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15-1-2.】
第15章 – 07

6.7 リモートワーク

実施手順（例）
a. リモートワークは、情報セキュリティ委員長の承認を得たものに限って行える。 b. リモートワークにて使用するPCは、会社から貸与したPCとし、家族などの同居人と共有することは禁じる。 c. リモートワークにて使用するPCは、アンチウイルスソフトを導入し、「8.7 マルウェアに対する保護」に準じた設定を行う。 d. リモートワークにて使用するPCに、ファイル交換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。 e. 社内ネットワークへはVPNにて接続する。

6.8 情報セキュリティ事象への報告

実施手順（例）
情報セキュリティ事象は、「5.25 情報セキュリティ事象の評価及び決定」に従って報告し、評価を行う。

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

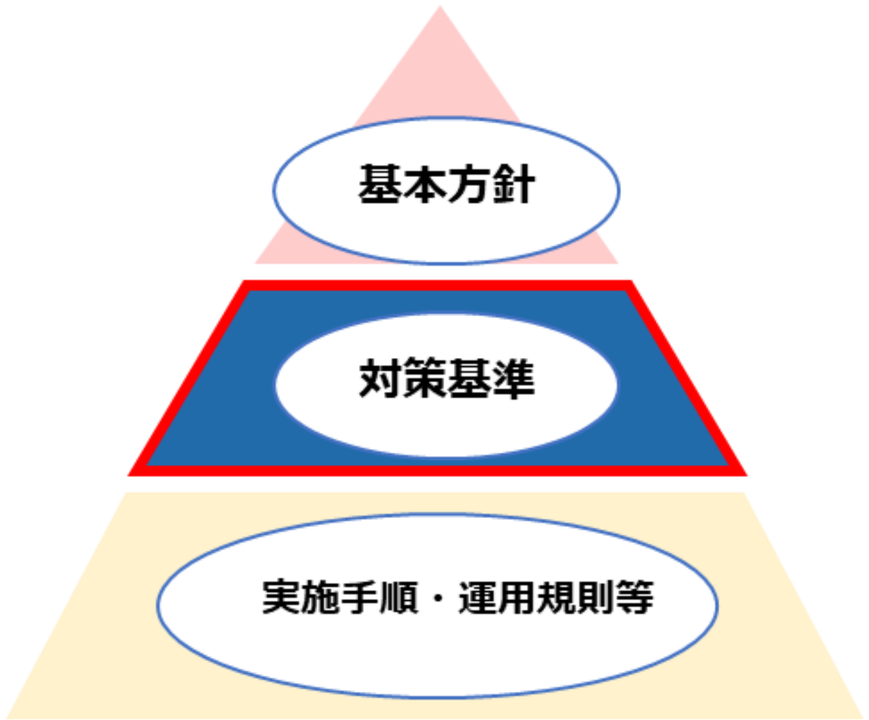
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

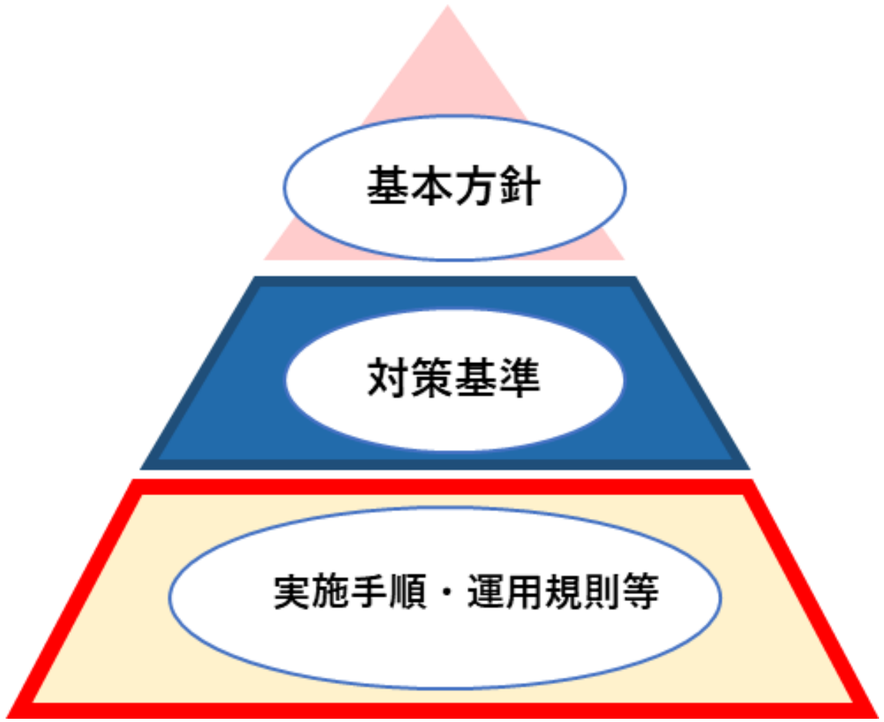
対策基準（例）

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などが入った力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

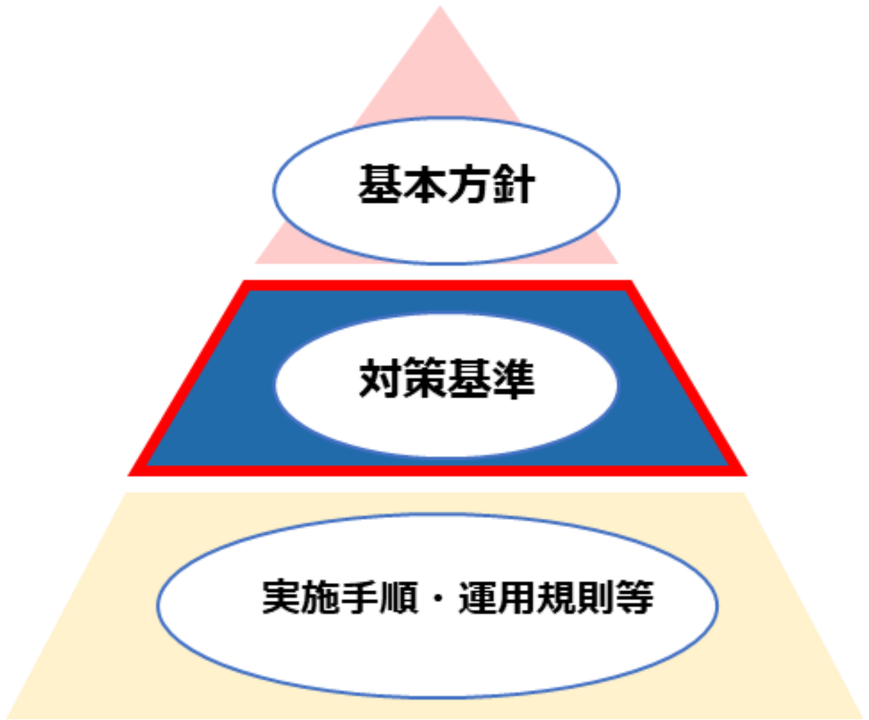
ISO/IEC 27001:2022附属書Aの管理策		
カテゴリ	項目数（合計93）	概要
組織的管理策	37	組織として取組む必要のある管理策。たとえば、情報セキュリティ方針、情報セキュリティの役割と責任、情報の分類などが含まれます。
人的管理策	8	従業員に関して取組む必要のある管理策。従業員の採用、情報セキュリティの意識向上、情報セキュリティ教育と訓練などが含まれます。
物理的管理策	14	情報システムのハードウェアや建物、設備に関する管理策。たとえば、オフィス、部屋および施設のセキュリティ、施設の物理的セキュリティ監視、装置の保守などが含まれます。
技術的管理策	34	技術面での管理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

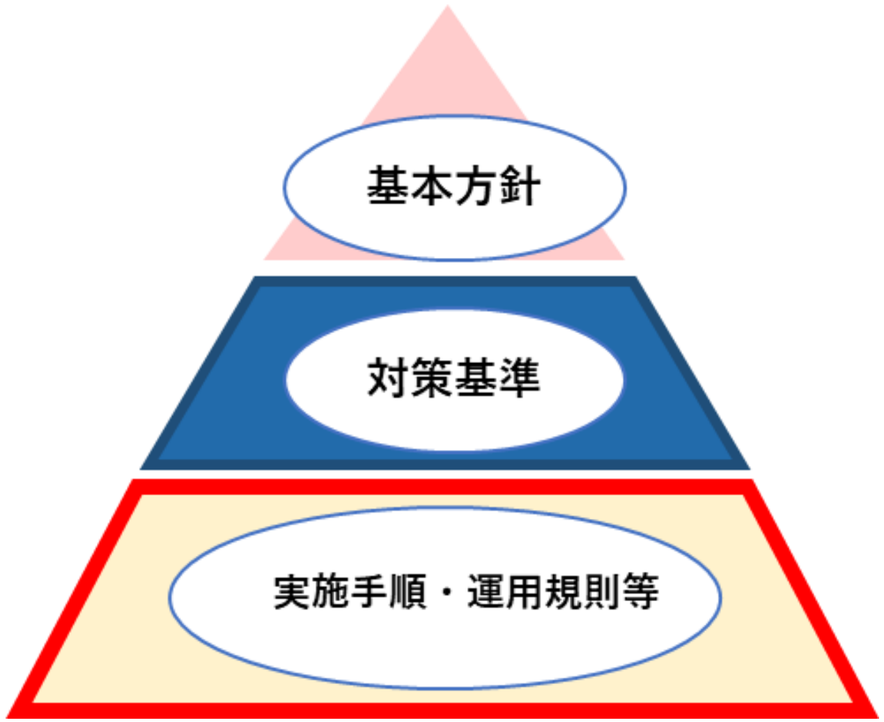
対策基準（例）
8.31 開発環境、試験環境及び運用環境の分離 開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。 **8.32 変更管理** 情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。 **8.33 試験情報** テスト用情報は、適切に選定、保護、管理しなければならない。 **8.34 監査試験中の情報システムの保護** 運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。

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

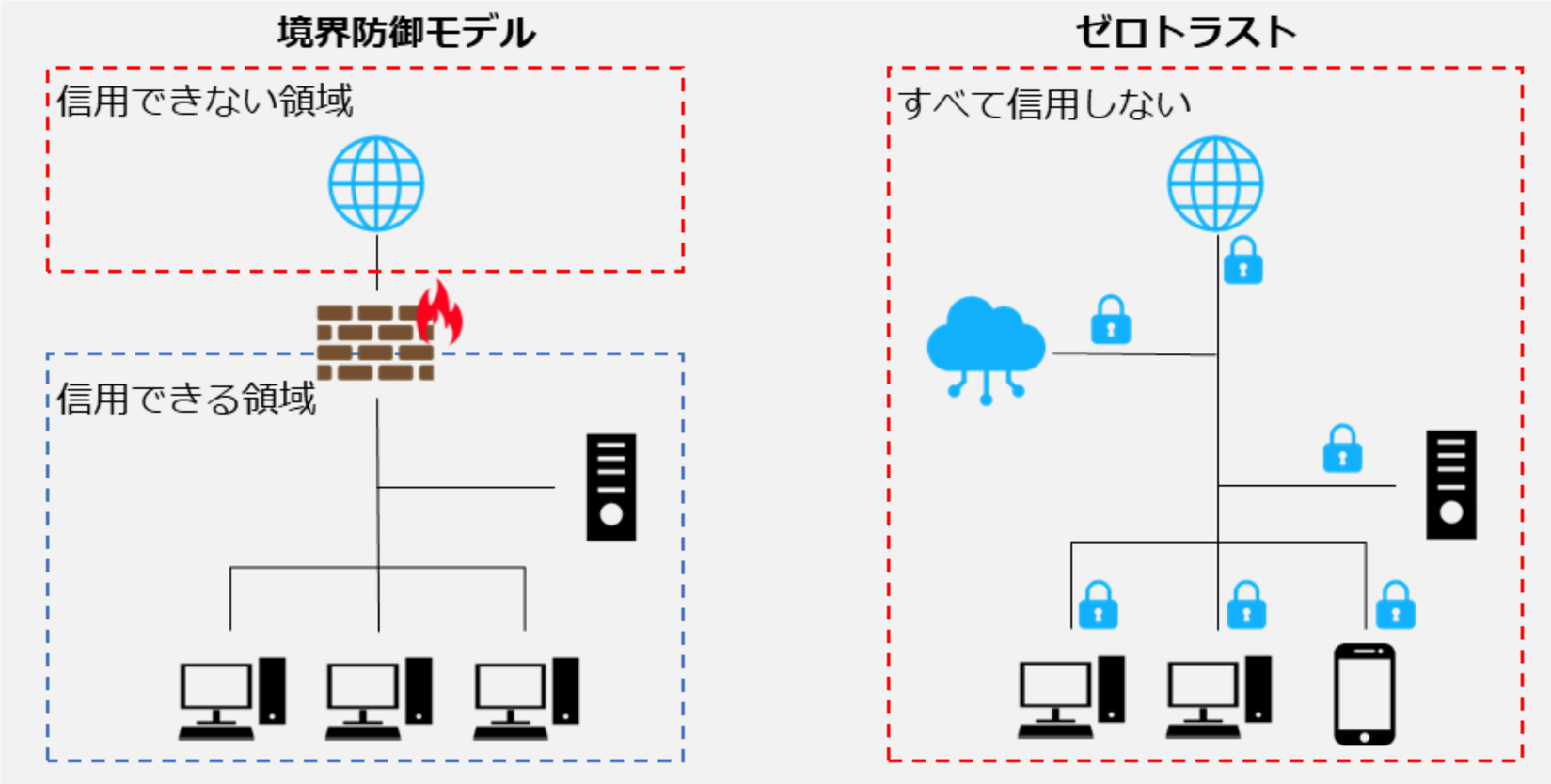
実施手順（例）	選択すべき管理策（例）
セキュリティ運用準備 • セキュリティ運用体制の確立 • 下記項目に対応したセキュリティ運用手順の整備 ➢ 平時の運用 ✓ 構成管理、変更管理 ✓ セキュリティ製品のアラート、システムログなどを活用したセキュリティ監視、検知 ✓ 脅威情報収集、自システムへの影響分析 ✓ CVSSなどに基づくリスクに応じた脆弱性対応 ✓ 定期的な脆弱性診断の実施 ➢ 有事の運用 ✓ インシデント対応 • 有事を想定したセキュリティ運用訓練の実施	• 5.24 情報セキュリティインシデント管理の計画及び準備 • 5.29 事業の中断・阻害時の情報セキュリティ • 8.9 構成管理 • 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

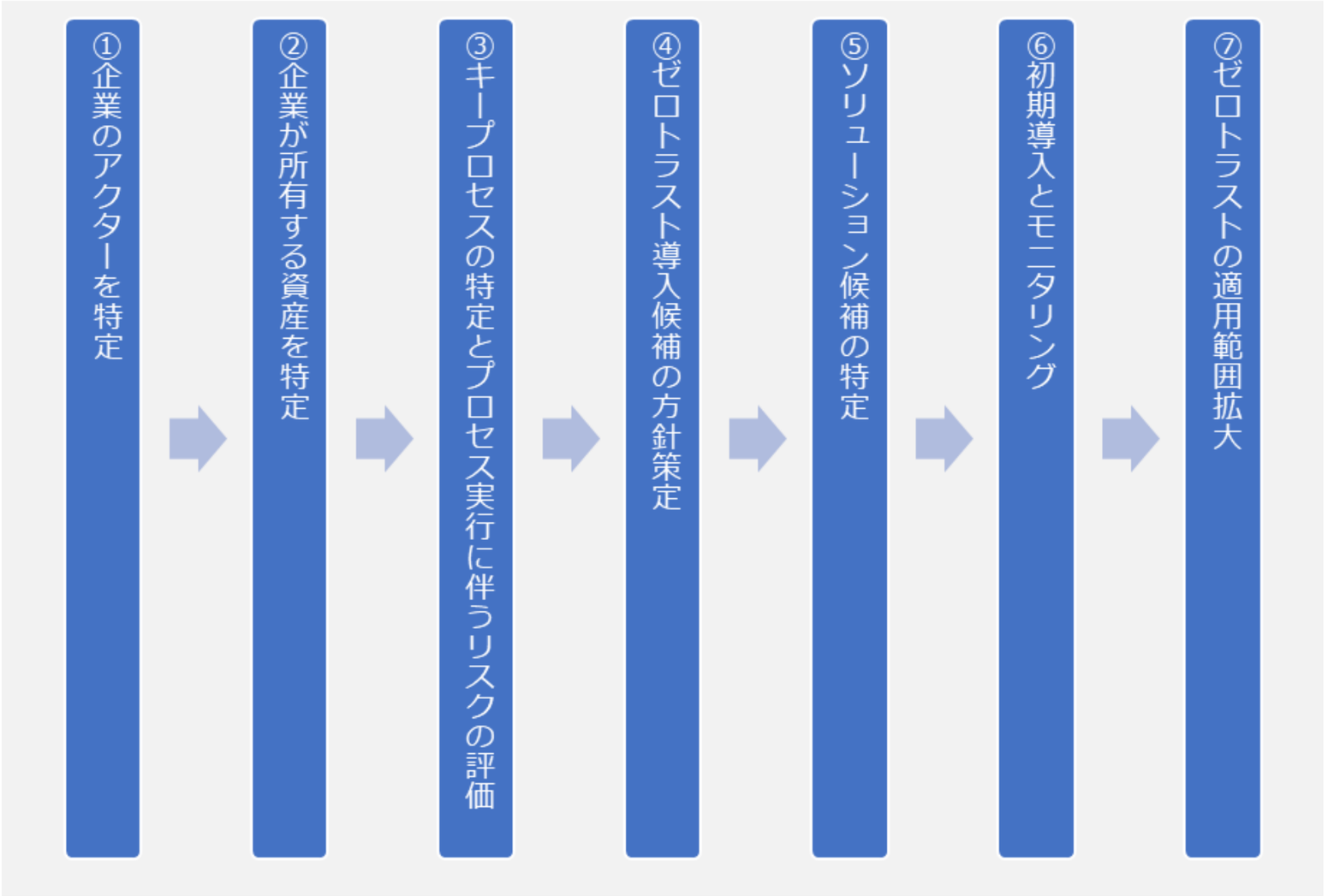
関連する主な管理策
5.9、5.15~5.23、5.29~5.30、8.1~8.3、8.15~8.16、8.21、8.32



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

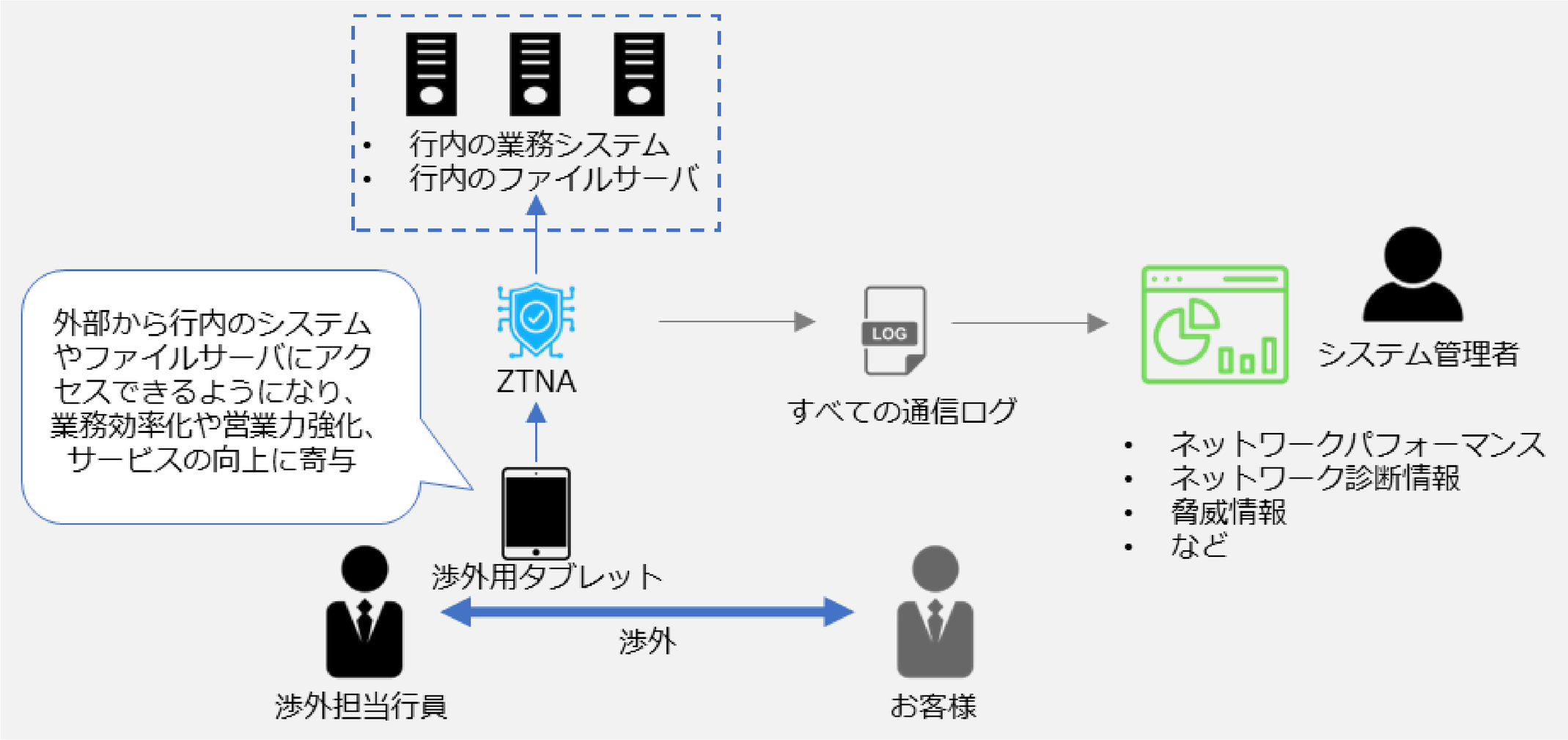
ゼロトラストを実装するための主な技術要素

- 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

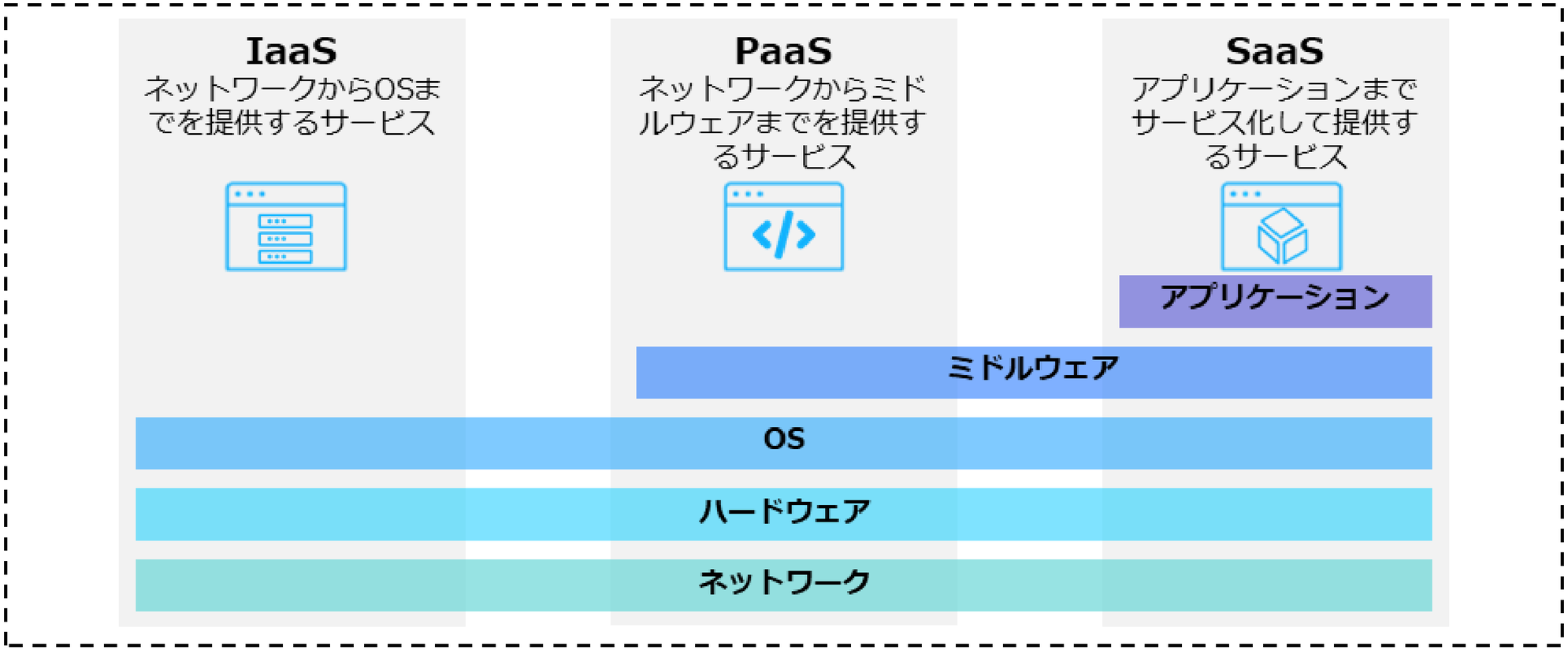


各種テーマごとの対策

【参照：テキスト17-2-3.】
第17章 - 31

ネットワーク制御

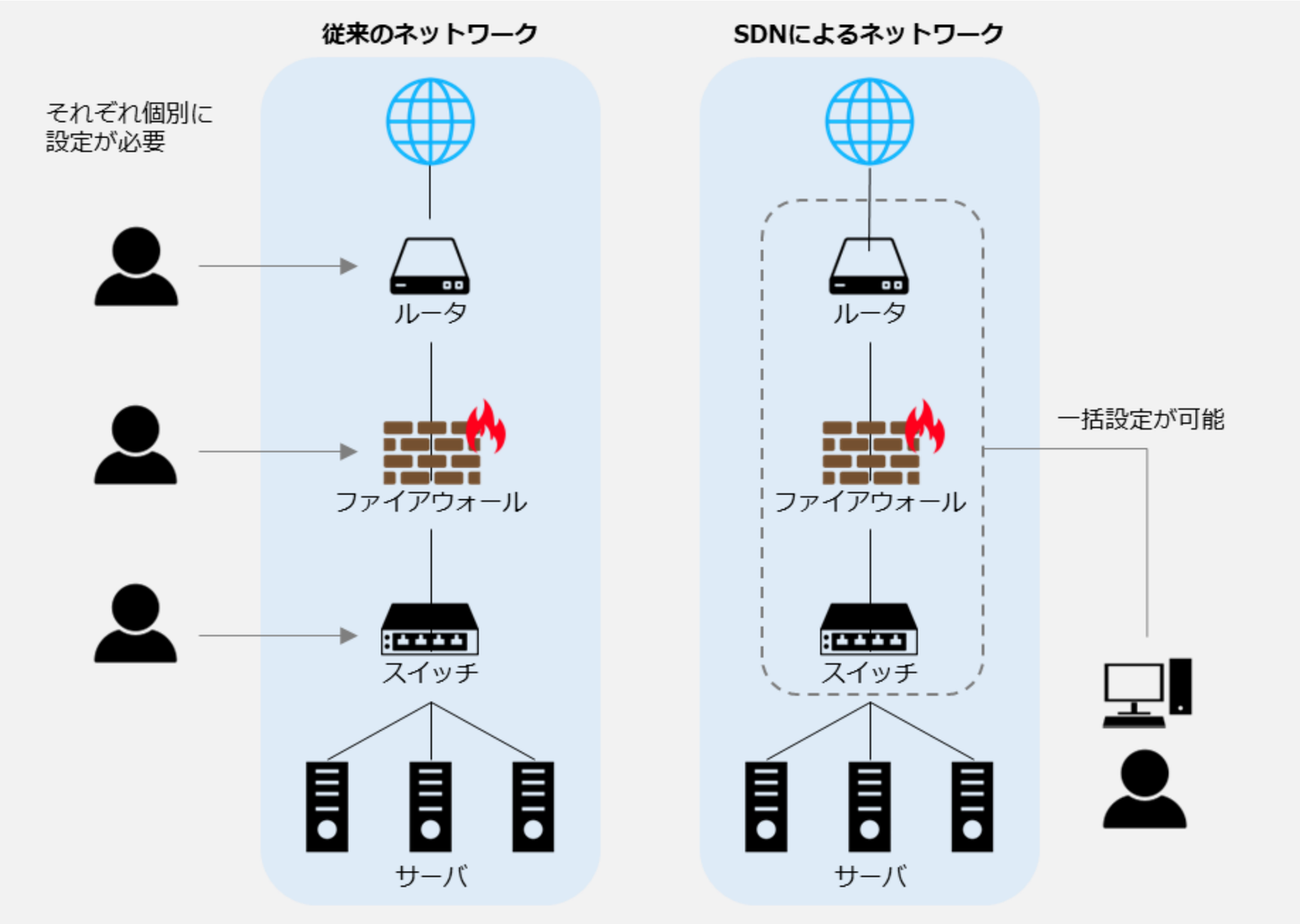
関連する主な管理策
5.23、6.7、8.20~8.24



各種テーマごとの対策

【参照：テキスト17-2-3.】
第17章 - 32

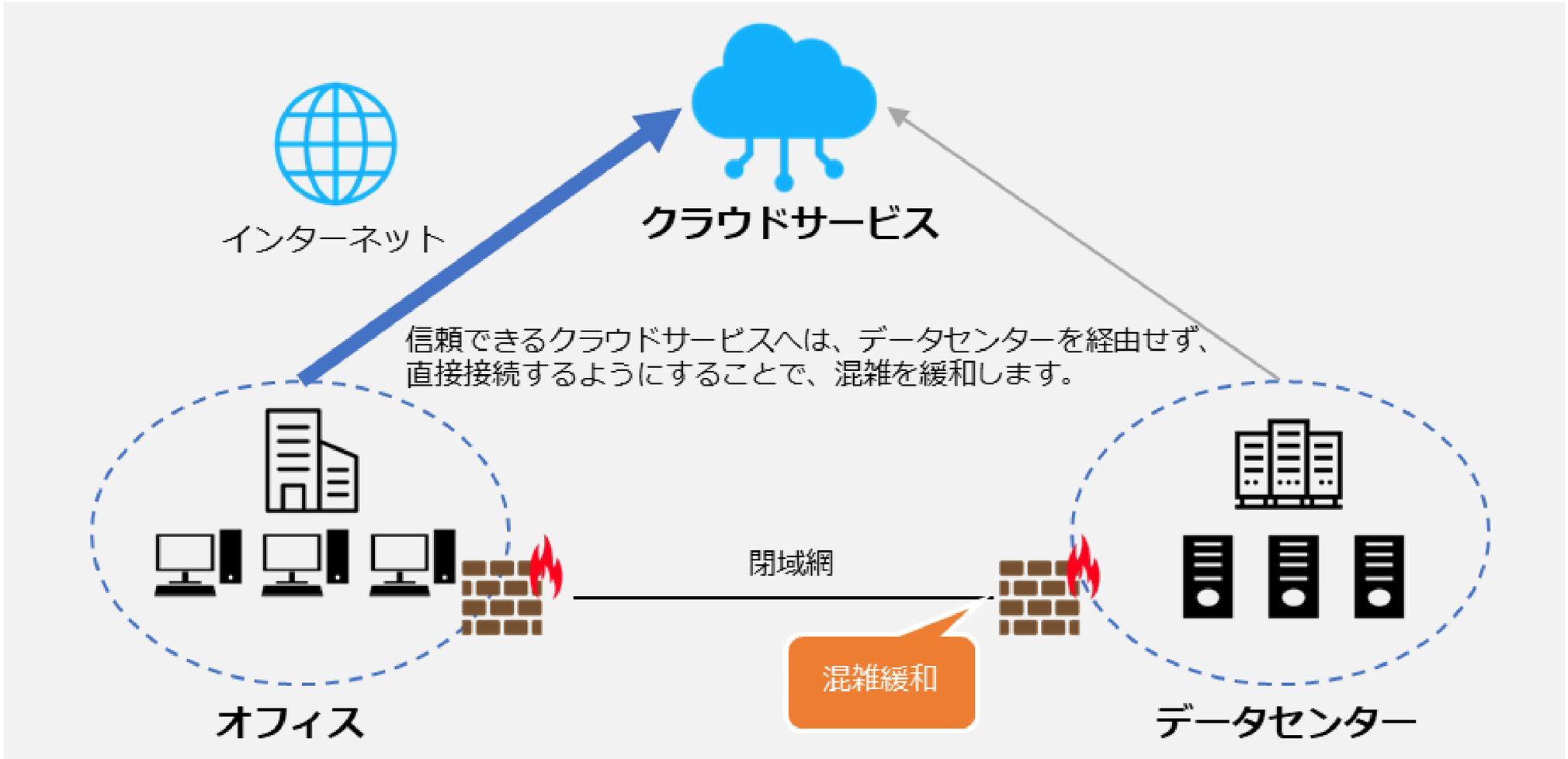
SDN（Software Defined Networking）



各種テーマごとの対策

【参照：テキスト17-2-3.】
第17章 - 33

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

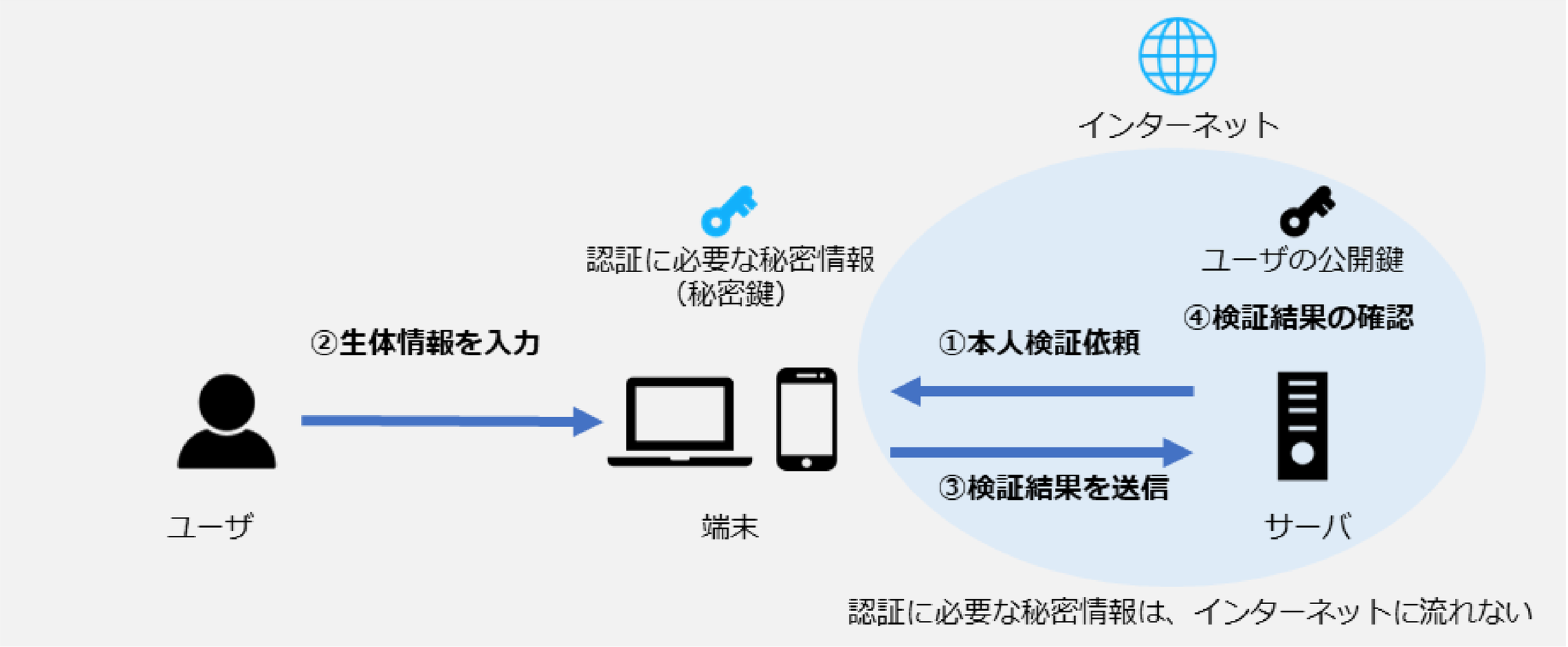
セキュリティ統制を確立するための技術

- 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
インシデント発生時の対応

【参照：テキスト17-2-2.】
第17章 – 38

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

【参照：テキスト17-2-2.】
第17章 – 40

インシデント対応手順例2

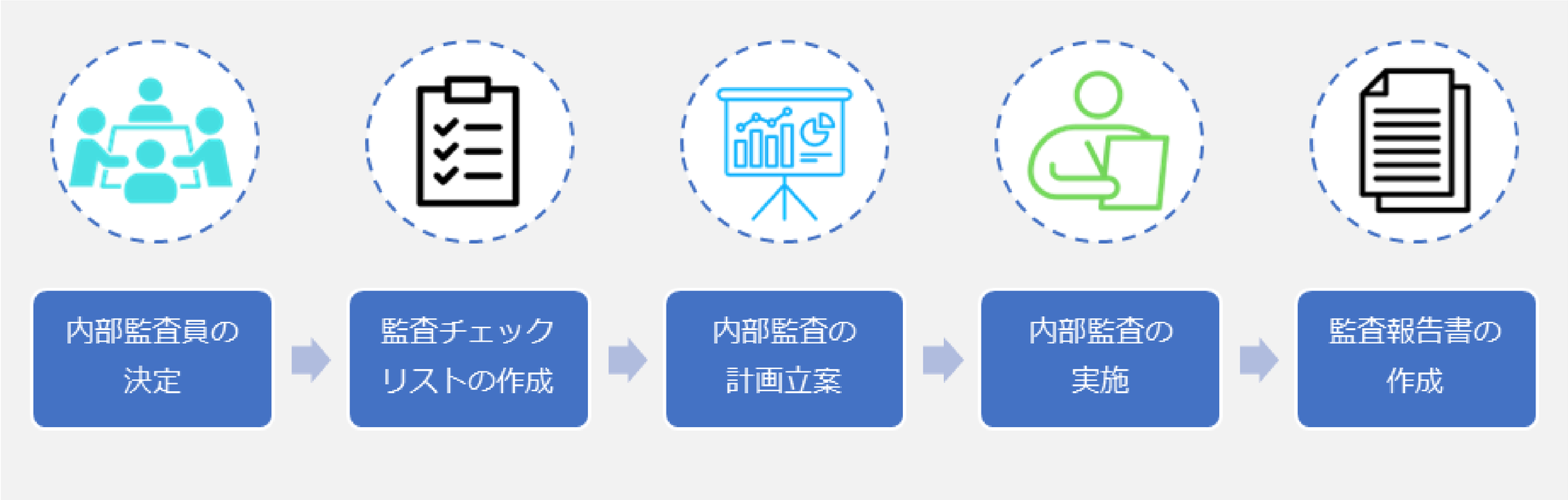
実施手順（例）
2. 発生したインシデントに関する対象物の決定
対象物に対する情報収集および対象物の絞り込み ✓ 発生したインシデントに関する対象物の種類および個数を確認します。 ・コンピュータ（タブレット型、ノート型、デスクトップ型、サーバ型） ・ネットワーク機器（ルータ、ファイアウォール、IDS、IPS） ・HDD、SSDなど ✓ 発生したインシデントに関する対象物の状態（いつどこに存在していたかなど）を確認します。 ✓ 発生したインシデントに関する対象物の使い始めと終わり、および使用頻度を確認します。 ✓ 発生したインシデントに関する対象物の使用者、および管理者を確認します。 ✓ 発生し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。

１．総括編

全体概要

各章のポイント

読者に今後行ってほしいこと

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 02

活用のポイント

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

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 03

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して把握し、それらの脅威に対する対策や、実際に被害にあってしま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

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 03

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

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

テキストの活用

【参照：テキスト19-1-1.】
第19章 - 04

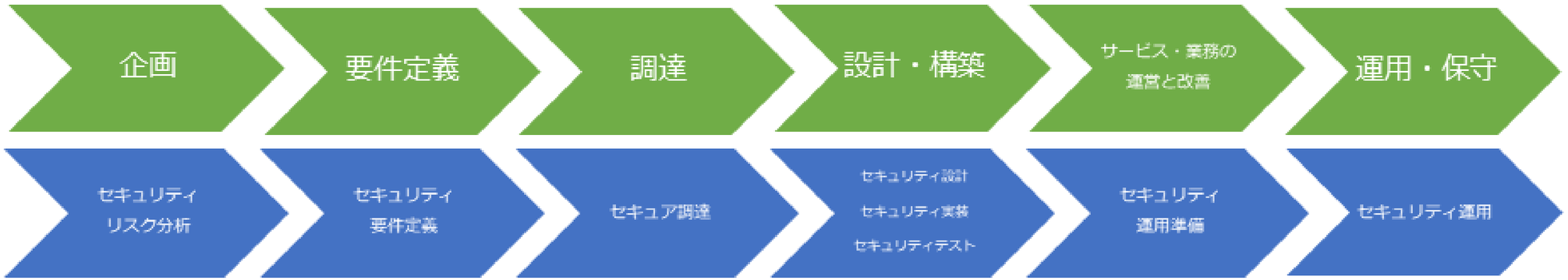
2. 経営者を含めた関係者と共有する

エグゼクティブサマリとしての活用（第19章 総括編）

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

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

4. 具体的なアクションを起こして一歩ずつ実践する



中小企業の情報セキュリティ対策

【参照：テキスト19-1-2.】
第19章 - 05

これまでの振り返り

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。

第1章 デジタル時代の社会とIT情勢

【参照：テキスト19-2-1.】
第19章 - 06

内容

- デジタル時代の社会変革とIT情勢の関係性

主なキーワード

- Society5.0
- DX

全体概要

- 現代社会は技術革新とグローバル化で大きく変わっている。
- 日本政府は、Society5.0という新しい社会モデルを推進。
- Society5.0はデジタル技術を使って社会問題を解決し、生活を向上させることを目指す。
- AIやビッグデータを活用した効率的な社会システムと持続可能な産業構造を構築。
- 企業にはDXを推進し、データとデジタル技術を活用して新たな価値を顧客視点で創出することが期待されている。

第1章 デジタル時代の社会とIT情勢

【参照：テキスト19-2-1.】
第19章 - 06

訴求ポイント

章を通した気づき・学び

- 社会動向の情報収集が企業・組織には重要。
- ビジネス環境の変化への対応のためDX推進が必要。
- デジタル社会に適したビジネスモデル、組織、企業文化への変革が求められる。

認識していただきたい実施概要

- 中小企業はリソースが限られているため、ビジネス環境の変化に対応するためにDXの推進が重要。
- 最新技術に関する知識と精通した人材が要求される。
- データとデジタル技術の安全利用のためにセキュリティ対策が重要。

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

【参照：テキスト19-2-2.】
第19章 - 07

内容

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

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

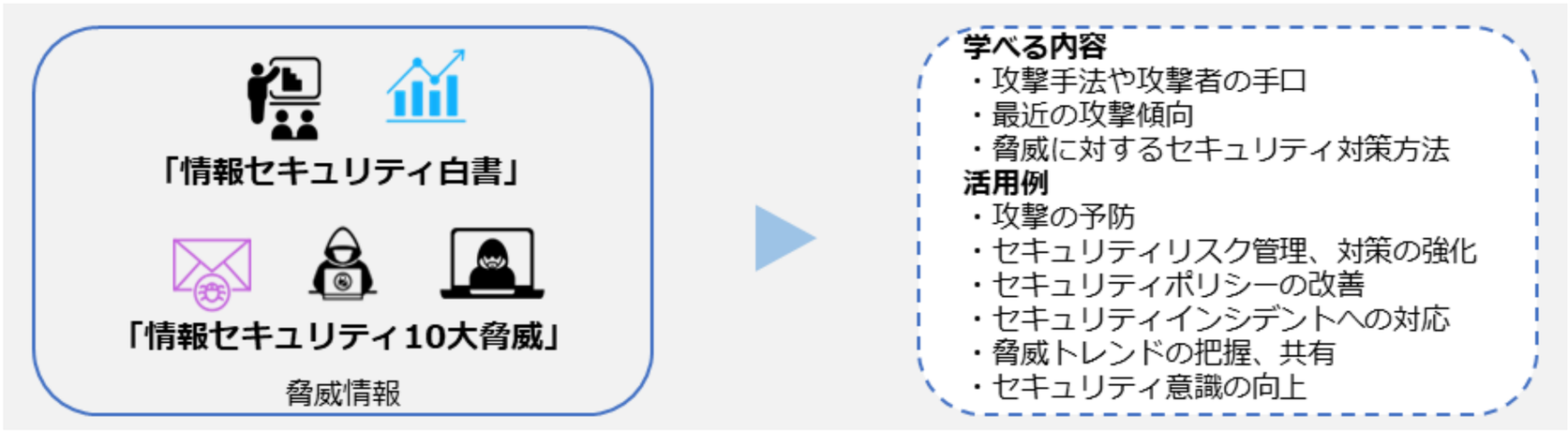
第2章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト19-2-2.】
第19章 - 07

全体概要

- 情報セキュリティ白書と10大脅威、インシデント事例を基に脅威を紹介。
- ランサムウェアとサプライチェーン攻撃が深刻。
- 攻撃は自社業務と取引先の信用に悪影響を与える。
- 攻撃は企業規模に関わらず発生。
- 中小企業もセキュリティ対策が不可欠。

情報セキュリティの概況



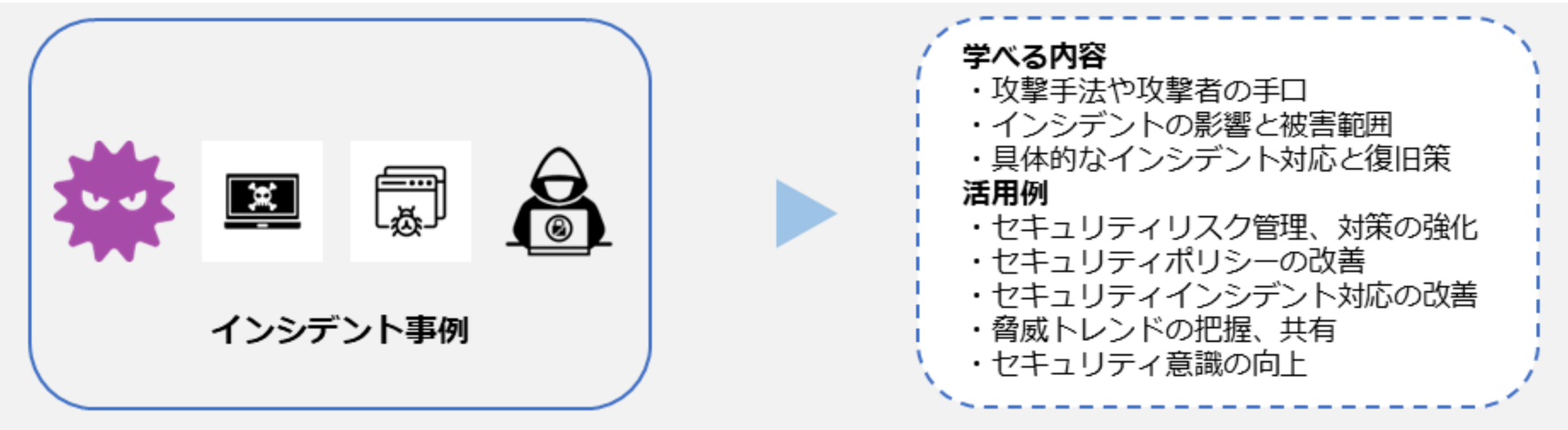
第2章 事例を知る：重大なインシデント発生から課題解決まで

【参照：テキスト19-2-2.】
第19章 - 08

重大インシデント事例から学ぶ課題解決

- 対応策の策定とリスク戦略の改善が必要。
- セキュリティ意識の向上が重要。
- IoTデバイス攻撃、サプライチェーンを介したメール攻撃、テレワークでの情報漏えい、ランサムウェア感染を含むインシデント事例を分析。
- 何が失敗したか、どの攻撃手法が用いられたか、どの脆弱性が標的になったかを理解することが大切。

実際の被害事例から見るケーススタディ



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

訴求ポイント

【参照：テキスト19-2-2.】
第19章 - 08

章を通した気づき・学び

- 最新のセキュリティ脅威と脆弱性を理解する。
- 攻撃傾向を把握し、適切な予防と対策を実施。
- 過去のインシデントを分析し、対応策を強化。

認識していただきたい実施概要

- 脆弱性と脅威情報を最新の状態で把握する。
- セキュリティリスク評価には情報セキュリティ白書や10大脅威の情報が有効。
- 適切な予防策や対策の策定には過去のインシデント事例の分析が役立つ。
- リスク戦略の改善とセキュリティ意識の向上が必要。
- 未来のインシデントに備えるためには、原因とベストプラクティスを理解することが重要。

第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 09

内容

- 導入済と想定するセキュリティ対策機能
- 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
- Security Action（セキュリティ対策自己宣言）
- サイバーセキュリティアプローチ方法

主なキーワード

- UTM
- EDR
- 情報処理技術者試験
- SECURITY ACTION

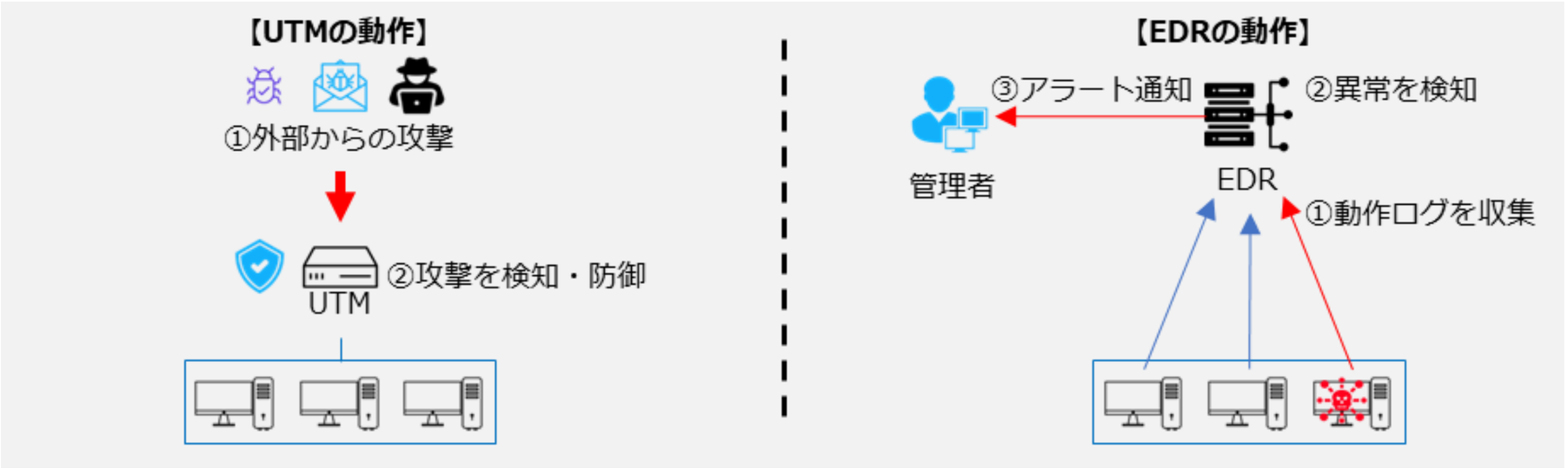
第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 09

全体概要

- UTM、EDR機能とITセキュリティ知識の確認には、情報処理技術者試験が有効。
- 中小企業にはSECURITY ACTIONへの取り組みを推奨。
- サイバーセキュリティの脅威への対処には、3つの段階的アプローチが効果的。

導入済と想定するセキュリティ対策機能



第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 10

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パスポート試験（TP）
- 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）

SECURITY ACTION（セキュリティ対策自己宣言）

- 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

サイバーセキュリティアプローチ方法

- 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

第3章 サイバーセキュリティの基礎知識

【参照：テキスト19-2-3.】
第19章 - 10

訴求ポイント

章を通した気づき・学び

- ITと情報セキュリティの知識習得が重要。
- 社内外のセキュリティ専門家と協力する能力を持つことが必要。
- SECURITY ACTIONに取り組むことで従業員の意識を高め、信頼を向上。

認識していただきたい実施概要

- 情報処理技術者試験がITとセキュリティ知識の習得状況の確認に有効。
- 「SECURITY ACTION」制度は中小企業の情報セキュリティ対策に役立ち、従業員の意識と対外信頼を高める。
- サイバーセキュリティの脅威対処には効果的な3段階アプローチが存在。

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

【参照：テキスト19-2-4.】
第19章 - 11

内容

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

主なキーワード

- 守りのIT投資
- 攻めのIT投資

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

【参照：テキスト19-2-4.】
第19章 - 11

全体概要

- 社会動向に基づくセキュリティ対策とIT活用の重要性を説明。
- 守りのIT投資（業務効率化、コスト削減）と攻めのIT投資（DX）の特徴と違いを紹介。
- デジタル技術の主要な活用方法について説明。
- 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強調。

これからの企業経営で必要な観点：社会の動向

- 社会動向と現実社会とサイバー空間の連携を説明。
- 現代は技術進化と競争激化により、革新的なアイディアと迅速な行動が必要。
- Society5.0が経済発展と社会課題解決のために提唱されている。
- 日本のデジタル化遅れの原因と現状のDX取り組みを米国と比較。

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

【参照：テキスト19-2-4.】
第19章 - 12

守りのIT投資と攻めのIT投資

「守りのIT投資」
（デジタルオプティマイゼーション）
目的：生産性向上

・業務の効率化
・コストの削減

「攻めのIT投資」
（デジタルトランスフォーメーション）
目的：ビジネス継続・競争力強化

・新たなビジネスの展開
・顧客視点で新たな価値の創造

経営投資としてのサイバーセキュリティ対策

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

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

【参照：テキスト19-2-4.】
第19章 - 12

訴求ポイント

章を通した気づき・学び

- Society5.0の提唱のもと、企業はデジタル技術を活用してビジネスモデルを変革。
- 顧客視点で新たな価値を創出するDXの推進には「攻めのIT投資」が重要。
- 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することが大切。

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連携、Society5.0など社会動向の理解が企業経営で重要。
- 「攻め」と「守り」のIT投資を理解し、特に攻めのIT投資への取り組みが必要。
- DX推進とデータ・デジタル技術活用に伴い、サイバーセキュリティ対策が重要。

第5章 デジタル社会の方向性と実現に向けた国の方針【参照：テキスト19-2-5.】第19章 - 13

内容

- 国の基本方針および実施計画の要約
- 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

主なキーワード

- デジタル社会
- DX
- DXの推進
- サプライチェーン

第5章 デジタル社会の方向性と実現に向けた国の方針【参照：テキスト19-2-5.】第19章 - 13

全体概要

- 国のデジタル社会方針や政策、サイバーセキュリティの位置付けについて解説。
- Society5.0を目指すデジタル社会に言及。
- DXに関して、中小企業の優位性について事例を交えて説明。

国の基本方針および実施計画の要約

- IT・セキュリティ関連施策は「経済財政運営と改革の基本方針」に基づく。
- 2023年度の方針には「サプライチェーンの強靭化」と「DXの加速」が含まれる。

第5章 デジタル社会の方向性と実現に向けた国の方針【参照：テキスト19-2-5.】第19章 - 13

国の基本方針および実施計画の要約

- 国の基本方針に従い、IT・セキュリティ関連施策の実施計画が策定。
- 2023年度の方針には「サプライチェーンの強靭化」と「DXの加速」が含まれる。

政府機関が目指す社会の方向性とサイバーセキュリティ課題

- 政府は「経済財政運営と改革の基本方針」に基づく「デジタル社会の実現に向けた重点計画」を策定。
- 重点計画の「産業のデジタル化」部分には「中小企業のDX推進」と「中小企業のデジタル化の支援」が含まれる。

第5章 デジタル社会の方向性と実現に向けた国の方針

【参照：テキスト19-2-5.】
第19章 - 14

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

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な点

- 参考情報が豊富
- 環境が整備されている
- 環境の変化に素早く対応しやすい

第5章 デジタル社会の方向性と実現に向けた国の方針【参照：テキスト19-2-5.】第19章 - 14

訴求ポイント

章を通した気づき・学び

- デジタル活用進展に伴いサイバーセキュリティリスクが増加。
- 企業は自社のIT活用状況を認識する必要がある。
- 必要な知識・スキルを持った人材の育成・確保が重要。

認識していただきたい実施概要

- 国の基本方針と社会実現計画を通じて、IT、デジタル、サイバーセキュリティの方向性・課題を学ぶ。
- 中小企業の優位性を理解し、DXに積極的に取り組むことが組織成長に重要。

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 15

内容

- NISC：サイバーセキュリティ戦略
- 関連法令

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

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 15

全体概要

- NISCの「サイバーセキュリティ戦略」の紹介とDX with Cybersecurityの解説。
- デジタル利用増加に伴いサイバーセキュリティリスクが高まる。
- 企業は自社のIT活用状況を把握し、必要な知識・スキルを持った人材を育成・確保する必要がある。
- 適切なサイバーセキュリティ対策の実施が重要。

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 – 15, 16

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
- 企業経営のためのサイバーセキュリティの考え方
- DX with Cybersecurity
- デジタルスキル標準（DSS）
- プラス・セキュリティ

関連法令

- 個人情報保護法
- GDPR（EU一般データ保護規則）

第6章 サイバーセキュリティ戦略および関連法令

【参照：テキスト19-2-6.】
第19章 - 16

訴求ポイント

章を通した気づき・学び

- 日本政府のサイバーセキュリティ戦略を理解することが重要。
- 関連する知識やスキルの習得が必要。

認識していただきたい実施概要

- 国家レベルでサイバーセキュリティを確保する方針や目標を理解する。
- サイバーセキュリティ対策を経営のための必要な投資と位置付ける。
- DX推進と同時にサイバーセキュリティ対策の重要性を認識し、必要なセキュリティ能力（プラス・セキュリティ）を身につける。
- 個人情報保護法やGDPRを含むサイバーセキュリティ関連法令の遵守と、個人情報の高レベル取扱いの重要性。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 - 17

内容

- セキュリティフレームワークの概要
- 情報セキュリティマネジメントシステム（ISMS）[ISO/IEC27001:2022, 27002:2022]
- NIST サイバーセキュリティフレームワーク（CSF）
- 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）
- サイバーセキュリティ経営ガイドライン

主なキーワード

- セキュリティフレームワーク
- ISMS

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 - 17

全体概要

- セキュリティ対策関連フレームワークの特徴と概要、要素や要件を解説。
- 無計画なセキュリティ対策は複雑化や抜け漏れのリスクを招く。
- 企業はセキュリティフレームワークを用いて、自社に適した対策方針を選択することが重要。

セキュリティフレームワークの概要

- 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

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 17, 18

情報セキュリティマネジメントシステム（ISMS）

- ISMS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。
- セキュリティフレームワークの中で代表的な存在。
- 目標はリスクマネジメントプロセスを通じて情報の機密性、完全性、可用性を維持・改善。
- リスクを適切に管理し、利害関係者に信頼を提供。

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のフレームワーク。
- 防御だけでなく、検知・対応・復旧のインシデント対応を含む。
- 多様な企業に適用可能な汎用性のある要求事項。
- CSFは①コア（対策一覧）、②ティア（成熟度評価基準）、③プロファイル（対策の現状と目標記述）の3要素で構成。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 18

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とCSFを包含する。
- サイバー空間とフィジカル空間の両方のセキュリティ対策に対応したフレームワーク。

サイバーセキュリティ経営ガイドライン

- 経営者向けのサイバーセキュリティ対策指針。
- 経営者が認識すべき事項と、CISOなどの責任者に指示すべき事項を包括的にまとめている。
- 経営者がサイバーセキュリティ対策を実施する際の参考資料。

第7章 セキュリティフレームワーク

【参照：テキスト19-2-7.】
第19章 – 18

訴求ポイント

章を通した気づき・学び

- セキュリティ対策の漏れなく効果的な実施にはセキュリティフレームワークの使用が有効。
- 多様なフレームワークの中から自社の課題や目的に合ったものを選択することが重要。

認識していただきたい実施概要

- フレームワークに沿ってセキュリティ対策を進めることで、効果的な対策実施と信頼向上が可能。
- セキュリティ対策フレームワークは複数存在するが、ISMSを基本枠組みとして使用。
- 必要に応じて、業種や重点領域に特化したフレームワークで補完するのが有効。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

内容

- 対策基準の策定

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

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

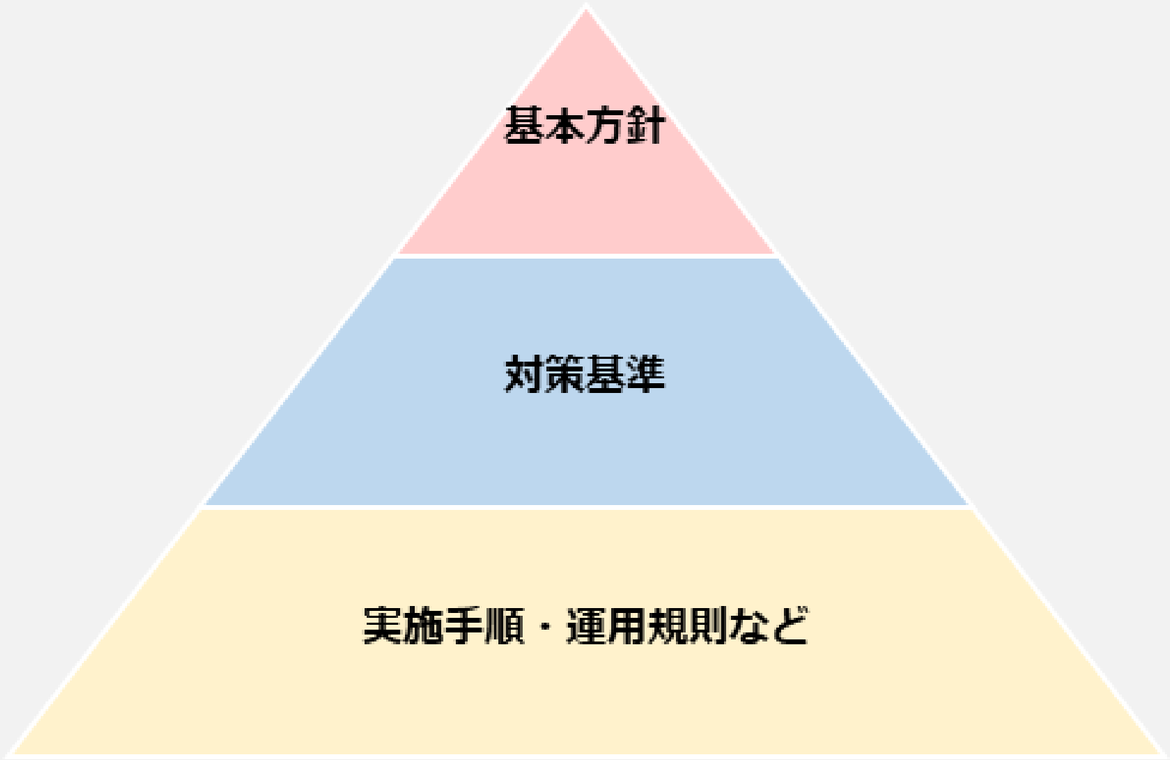
全体概要

- セキュリティポリシー構成（基本方針、対策基準、実施手順・運用規則など）について説明。
- 企業の現状や目標に応じた対策基準策定に3つのアプローチ手法を紹介
  - 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

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 19

対策基準の策定



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・運用規則など
対象者や用途によって必要な手続を記述する。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 20

対策基準策定のアプローチ方法

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。

第8章 セキュリティ対策基準の策定

【参照：テキスト19-2-8.】
第19章 – 20

訴求ポイント

章を通した気づき・学び

- 状況に応じた適切なサイバーセキュリティ対策アプローチを選択することが重要。
- セキュリティ対策実施を内外に示すためには、対策基準の策定が必要。

認識していただきたい実施概要

- 対策基準を外部に公開し、セキュリティ対策の実施と説明責任を果たす。
- 実施手順を策定した対策基準に基づいて作成することが重要。
- 対策基準の策定には、「クイックアプローチ」「ベースラインアプローチ」が可能。
- 網羅的な対策にはISMSを参考にした「網羅的アプローチ」が推奨される。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 21

内容

- 管理策の分類と構成

主なキーワード

- 管理策
- ISO/IEC 27002

全体概要

- ISMSの管理策を示した規格のISO/IEC 27002についての説明。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 21

管理策の分類と構成

- 2013年版では管理策が14分野114項目だったが、2022年版では82項目に統合、新たに11項目が追加され、合計93項目に。
- 2022年版の管理策は「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。
- 「属性（attribute）」という新概念が導入され、管理策のフィルタリング、並び替え、提示が容易に。
- ISMS構築時には、これらの管理策から自社に適したものを選択し、対策基準として採用。

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 22

管理策のテーマと属性

第9章 管理策のテーマと属性

【参照：テキスト19-2-9.】
第19章 – 22

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の管理策から、組織に必要なものを選択することが重要。

認識していただきたい実施概要

- ISMSにおいて、リスク対応の対策として管理策があり、ISO/IEC 27002:2022で93項目が示されている。
- ISO/IEC 27002:2022の管理策には4つのテーマと5つの属性があり、これらを参考に組織に必要なセキュリティ対策を選択することが重要。

第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 23

内容

- 用語の定義および関係性と識別方法

主なキーワード

- リスク
- 脅威
- 脆弱性

全体概要

- 「リスク」、「脆弱性」、「脅威」の定義とそれらの関係性についての理解。
- 「脅威」と「脆弱性」の識別方法についての詳細な説明。

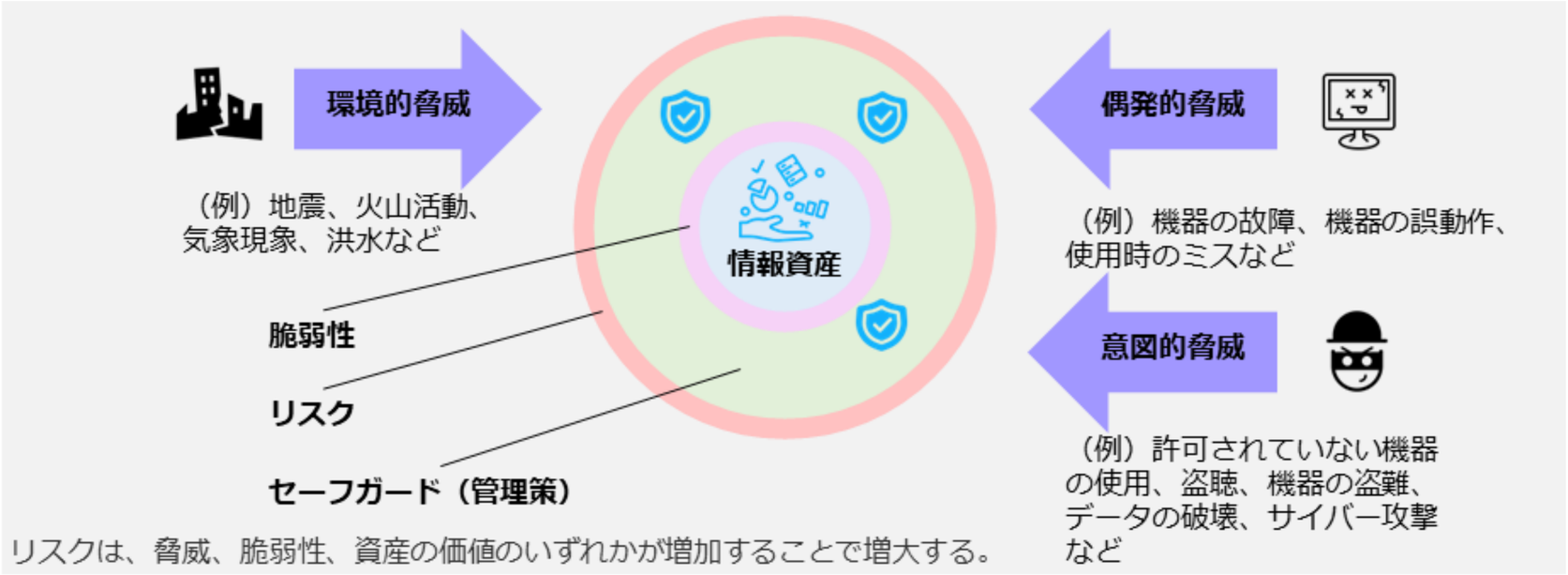
第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 23

用語の定義および関係性と識別方法

- 企業や組織にはセキュリティ上のリスクが存在する。
- これらのリスクを効率的に管理するためにはリスクマネジメントが必要。
- リスクマネジメントを理解するために、「脅威」、「脆弱性」、「リスク」という用語の定義と関係性を説明している。

（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



第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 24

脅威の識別

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になります。
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

- 脆弱性があってもインシデントが発生するわけではないが、脆弱性は脅威を引き起こし、インシデントの発生確率を高める可能性がある。
- 脆弱性を減らすためには適切な管理策が必要であり、脆弱性は管理策の不足を示す。
- 脆弱性を識別することは必要な管理策を特定するのに役立つ。

第10章 脅威、脆弱性、リスクの定義と関係性

【参照：テキスト19-2-10.】
第19章 – 24

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」という用語の定義や関係性を理解することの重要性。
- 「脅威」、「脆弱性」を識別する方法の理解の重要性。

認識していただきたい実施概要

- リスクは「脅威」「脆弱性」「資産の価値」のいずれかが増加することによって増大する。
- 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、保護要求事項を特定し、適切なセーフガードを実施する必要がある。

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 25

内容

- リスクマネジメント：概要
- リスクマネジメント：リスクアセスメント
- リスクマネジメント：リスク対応

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

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 25

全体概要

- リスクマネジメントプロセスにはリスク基準の確立、リスクアセスメント、リスク対応が含まれる。
- リスクマネジメントはセキュリティ対策に必要であるが、顕在化していないリスクを考えるのは難しいことがある。
- リスクマネジメントプロセスの各段階で特定、分析、対応策の検討を円滑に行うための考え方と手法が存在する。

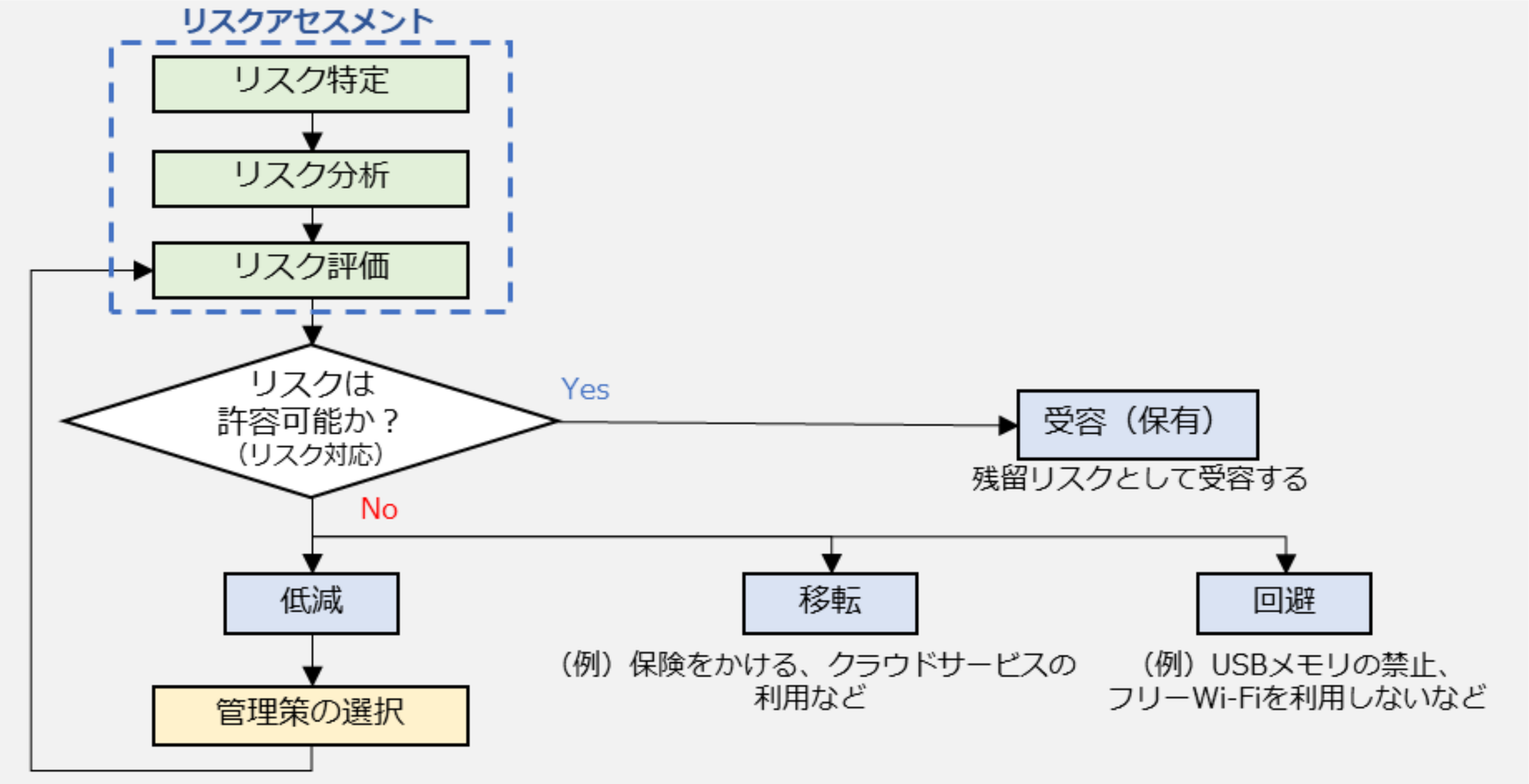
リスクマネジメント：概要

- リスクマネジメントプロセス（ISO 31000）
- 情報セキュリティリスクマネジメント（ISO/IEC 27005）
- ISO/IEC 27001におけるリスクマネジメント手順

第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 26

リスクマネジメント：リスクアセスメント
リスクマネジメント：リスク対応



第11章 リスクマネジメント

【参照：テキスト19-2-11.】
第19章 – 26

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不可欠であるが、潜在的なリスクを考えるのが難しい場合がある。
- リスクマネジメントプロセスの各段階での考え方や手法を使用することで、リスクの特定、分析、対応策の検討を円滑に行うことができる。

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要である。
- 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。
- 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。

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)

【参照：テキスト19-2-12.】
第19章 – 27

内容

- 【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】セキュリティインシデント事例を参考とした実施手順
- 【LV.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

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

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）

【参照：テキスト19-2-12.】
第19章 – 27

全体概要

- クイックアプローチ：実際のセキュリティインシデントの事例に基づいて対策基準や手順を策定するアプローチ。
- ベースラインアプローチ：既存のガイドラインやひな形を参考にして対策基準や手順を策定するアプローチ。
- クイックアプローチは社会的に影響の大きい事案に向いており、ベースラインアプローチは適切な参考元があれば簡易な手順で策定できる。

【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

- セキュリティ対策基準と実施手順の策定は情報漏えいなどのリスク対策に役立つ。
- LV.1 クイックアプローチ：緊急事態に対応するための即時の対策基準と手順を策定するアプローチ。
- LV.2 ベースラインアプローチ：既存のガイドラインを参考にして対策基準と手順を策定するアプローチ。

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）

【参照：テキスト19-2-12.】
第19章 – 28

【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

- 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。

【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

- 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
  - 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必要がある。
  - 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、自社の状況に合わせて検討する必要がある。

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)

【参照：テキスト19-2-12.】
第19章 – 28

訴求ポイント

章を通した気づき・学び

- 緊急性や即効性が必要な場合はクイックアプローチやベースラインアプローチが適している。
- 対策を検討する余裕がある場合、網羅的アプローチが重要である。

認識していただきたい実施概要

- クイックアプローチ：実際のセキュリティインシデントに基づいて発生可能性や被害規模を考慮し、社会的影響の大きいまたは緊急性の高い事象に対策を取りやすいアプローチ。
- ベースラインアプローチ：既存の手法を参考にして自社に適した対策基準や実施手順を簡易に策定できるアプローチ。

第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 29

内容

- 【LV.3 網羅的アプローチ】の概要
- 【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

主なキーワード

- 網羅的アプローチ
- PDCAサイクル

第13章 ISMSの要求事項と構築（LV3. 網羅的アプローチ）

【参照：テキスト19-2-13.】
第19章 – 29

全体概要

- 網羅的アプローチ：ISMSなどのフレームワークを使用して高いセキュリティ対策を策定する方法。時間がかかるが高いセキュリティレベルを確保できる。
- 緊急性や即効性が必要な場合はクイックアプローチやベースラインアプローチが適しているが、余裕がある場合は網羅的アプローチが推奨される。

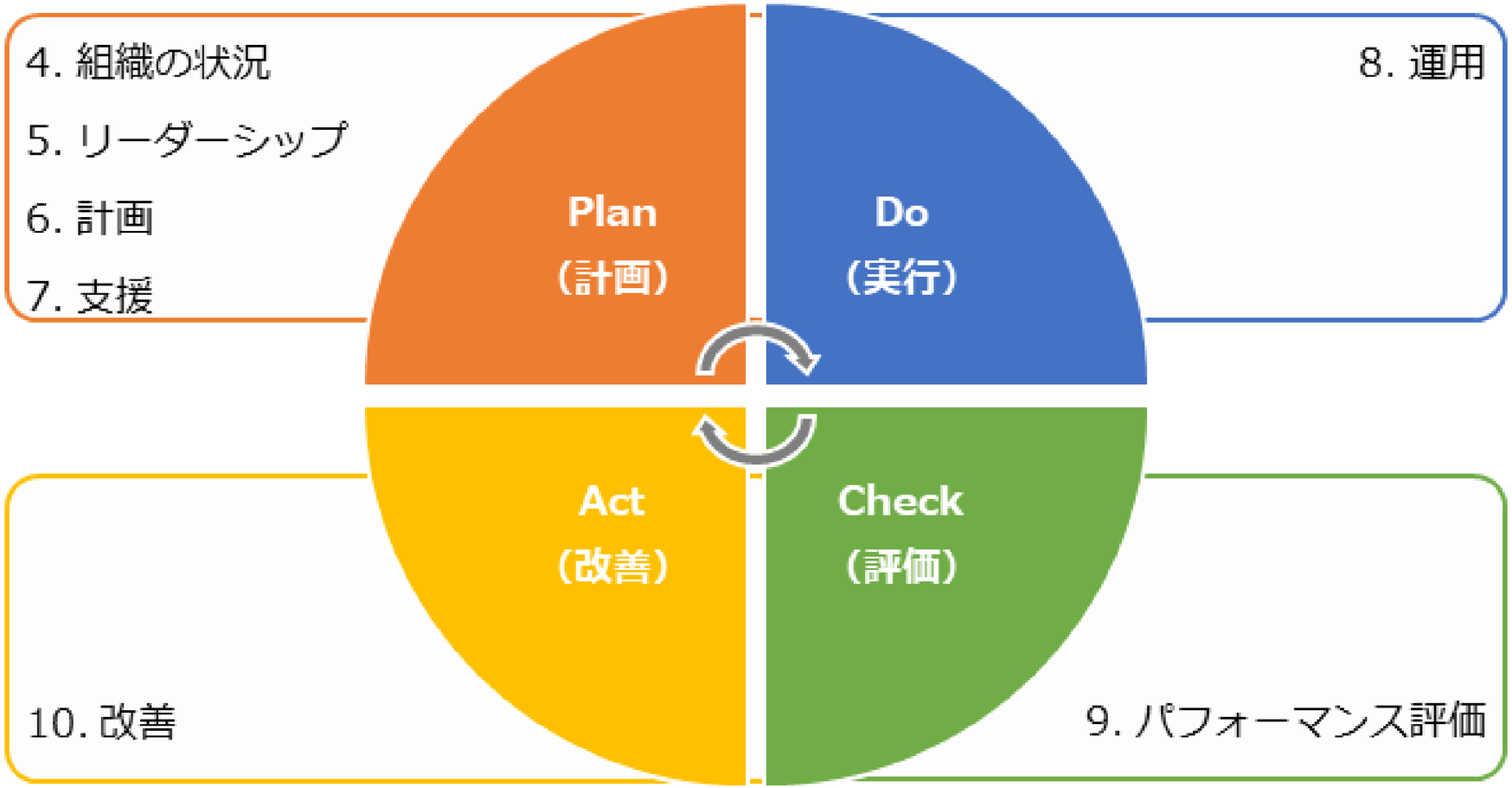
【LV.3 網羅的アプローチ】の概要

- 網羅的アプローチではISMSを使用してセキュリティ対策基準と実施手順を体系的に作成する。
- ISMSに従うため、技術的対策だけでなく運用や監査にも対策を含める。
- 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で、デメリットは時間とコストがかかること。

第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 30

【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



第13章 ISMSの要求事項と構築 (LV3. 網羅的アプローチ)

【参照：テキスト19-2-13.】
第19章 – 30

訴求ポイント

章を通した気づき・学び

- ISMSを使用した網羅的アプローチは、セキュリティ対策だけでなくISMS自体を改善し、自社に適した対策を継続的に検討することができる。

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。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

内容

- 4種類の管理策を参考とした対策基準・実施手順の策定

主なキーワード

- 組織的管理策
- 人的管理策
- 物理的管理策
- 技術的管理策

全体概要

- 対策基準の策定にはISO/IEC 27001:2022附属書Aの合計93項目の管理策を参考にできる。
- それぞれの管理策を参考に、対策基準を策定する手順と実施手順の例について説明。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

4種類の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の管理策（93項目）を参考にして対策基準を策定する。
- リスクアセスメントの結果に基づいて適切な管理策を選択し、それを対策基準とする。
- 対策基準は基本方針と一緒に公開可能なものとして作成する。
- ISMSに基づく管理策を使用して対策基準を策定する際には、ISO/IEC 27001:2022の文献を参照する。

実施手順の策定

- 管理策（対策基準）に基づいてセキュリティ対策の実施手順の例を紹介。
- 実施手順は組織内の文書として作成され、具体的で理解しやすい内容である必要がある。
- ISO/IEC 27002の各管理策の手引きを参考に実施手順の例を紹介。自社に適した実施手順を策定することが重要。

第14～17章 ○○管理策

【参照：テキスト19-2-14～17.】
第19章 – 31～38

訴求ポイント

章を通した気づき・学び

- ISO/IEC 27002を参考にして管理策の対策基準と実施手順を決定することが重要。
- ドキュメントの作成と更新は大切だが、本来の目標は効果的な情報セキュリティ対策を計画し実行することである。

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に基づいて管理策を選択し、対策基準を策定する。
- 対策基準は基本方針と一緒に公開可能なものとして作成する。
- 決定した対策基準に基づいて実施手順を策定する。
- 実施手順は従業員に対してわかりやすく内部文書として作成する。

第18章 セキュリティ対策状況の有効性評価

【参照：テキスト19-2-18.】
第19章 – 39

内容

- 内部監査・外部監査

主なキーワード

- 内部監査
- 外部監査

全体概要

- セキュリティ対策の有効性評価として、内部監査と外部監査が行われる。
- 内部監査は自社で規定した要求事項を満たし、業務がルールに従って実施されているかをチェックする。
- 外部監査は第三者が企業の情報資産を保護する体制や環境が整っているかをチェックする。

第18章 セキュリティ対策状況の有効性評価

【参照：テキスト19-2-18.】
第19章 – 39

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の有効性評価として内部・外部監査を定期的に実施する必要がある。

認識していただきたい実施概要

- 外部監査は第三者視点で情報資産の保護体制をチェックし、顧客や取引先にセキュリティ対策の信頼性を示す役割がある。
- 内部監査はセキュリティのルールや文書の適切性をチェックし、形骸化や目的の喪失を防ぐ役割がある。

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 40

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**

- 各章のポイントの理解
- DX推進の考え方の把握
- セキュリティ対策全容の認識
- 自組織でのセキュリティ対策の実施項目の認識

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。

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 41

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
- 実施手順の実践
  1. 組織体制と役割の決定
  2. 年間を通して実践すべき事項の例示

- 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

実施するための年間計画を作成する

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 43

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
- ISMS推進マニュアル – 活用ガイドブック ISO/IEC 27001:2022対応
- 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」
- ISO/IEC 27002:2022

取組み例

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	－	-	○	－

今後のアクション

【参照：テキスト19-3-1.】
第19章 – 44

継続的な情報収集

- 国の方針、社会の現状と今後の動向
- IT活用事例
- セキュリティインシデント事例

人材育成

- DSSに基づく人材育成
- プラス・セキュリティ人材の育成

中小企業向けサイバーセキュリティ実践ハンドブック セミナースライド

中小企業も安心！セキュリティ対策でDXを加速

2024年4月 Ver.1.0 初版発行

編集・発行　東京都産業労働局商工部経営支援課
新宿区西新宿二丁目8番1号

電話番号　03-5320-4770

セミナースライドの利用について

このセミナースライドは、東京都が著作権を保有しておりますが、利用に際しては、非営利目的、サイバーセキュリティ対策の普及・啓発目的であれば、事前の申請等は必要ありません。
全体を利用されるのであればそのままご利用いただけます。
また、一部分の「引用・参考・参照・転載」であれば、出典元を明記して頂ければご利用いただけます。

中小企業向け
サイバーセキュリティ実践ハンドブック

中小企業も安心！セキュリティ対策でDXを加速

東京都産業労働局