令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

第6回

第7編：ISMSの構築と対策基準の策定と実施手順
その3（第18章～第19章）

第8編：具体的な構築・運用の実践

東京都産業労働局

講師紹介

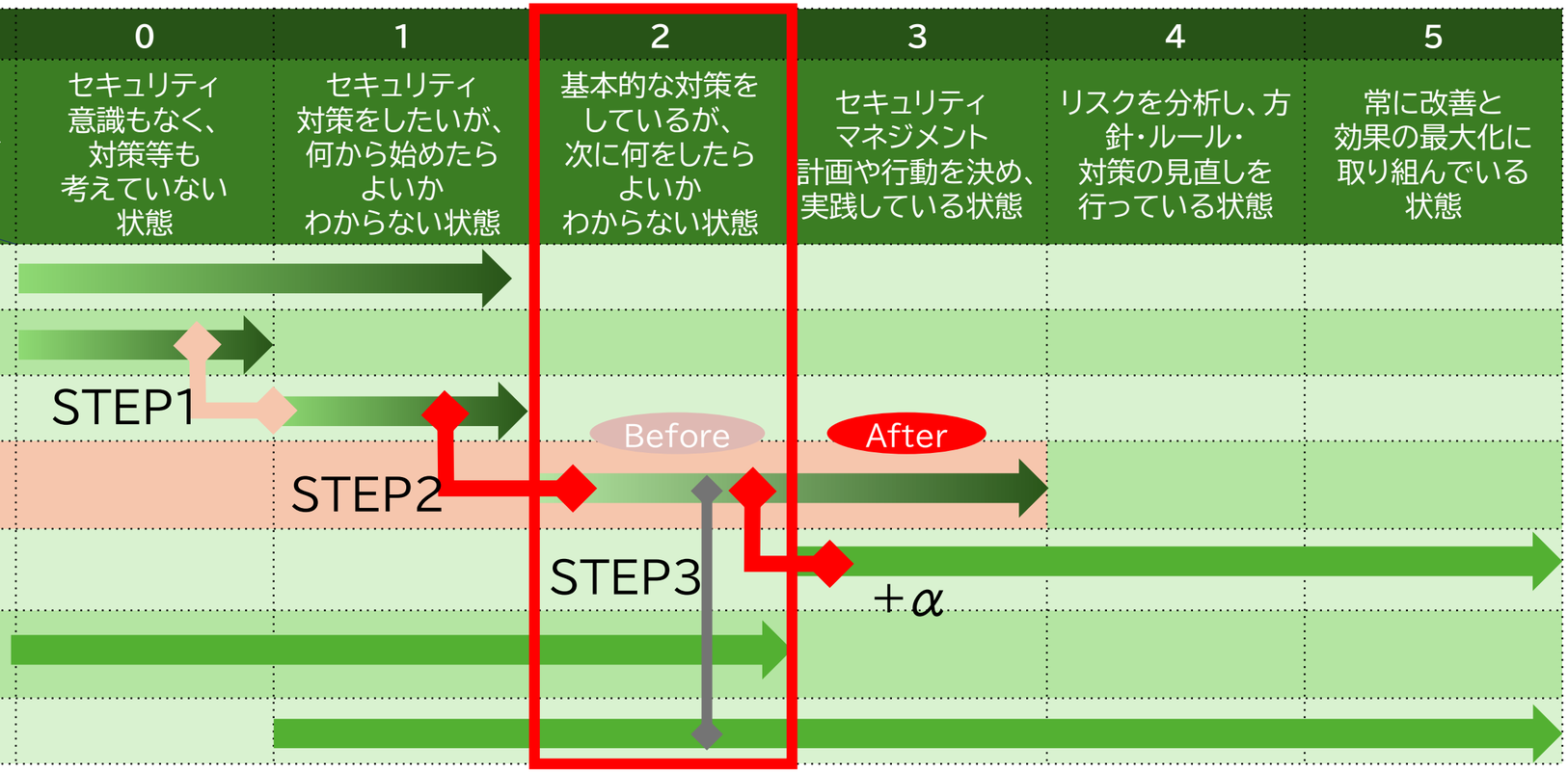
氏名	矢野　泰広（やの　よしひろ）
業務経歴	26年（セキュリティ経験：15年）
専門分野	情報セキュリティ、DX、ICT、クラウド技術、 ネットワーク技術、DB設計・構築、プロジェクト マネジメント、WEBシステム設計・構築、 サーバ設計・構築
保有資格	情報処理安全確保支援士（第004005号） 経済産業省認定 情報処理技術者試験 プロジェクトマネージャ、 情報処理技術者第一種、情報処理技術者第二種 インターネット検定 .com Master ADVANCE★★ 生成AIパスポート 家電製品アドバイザー（AV情報家電・生活家電）
コメント	中小企業を中心にDX、ネットワーク、クラウド技術お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

目的

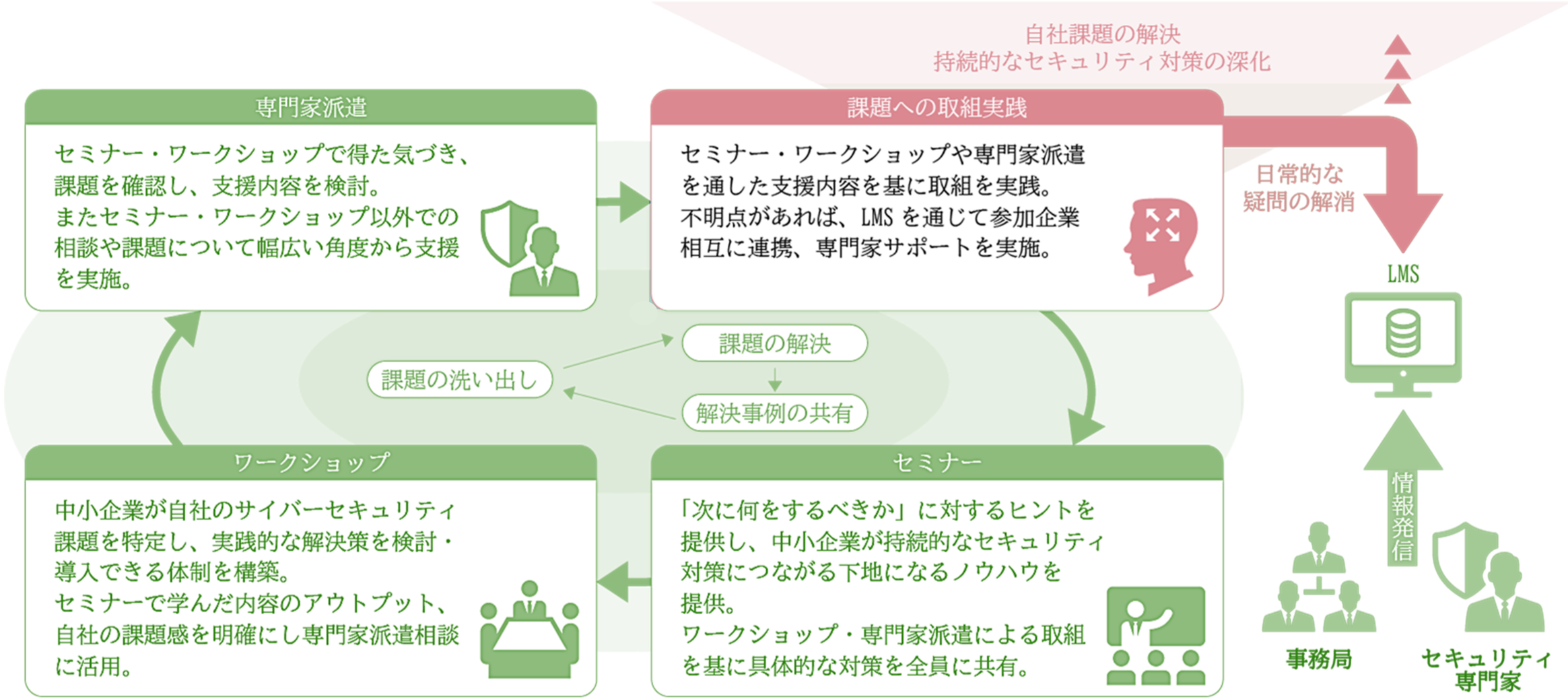
- 継続的なセキュリティ対策の実施を支援する。
- 人材の育成と実践的な課題解決を通じて、サプライチェーン全体のセキュリティ強化を図る。

東京都他事業と本事業の位置づけ

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



支援内容の全体像


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

スケジュール

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

セミナー内容

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

セミナー内容

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

第18章. 技術的対策

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

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.1 利用者エンドポイント機器

利用者エンドポイントデバイスに保存されている情報、処理される情報、または利用者エンドポイントデバイスを介してアクセス可能な情報を保護しなければならない。
【実施手順：テキストP8】

8.2 特権的アクセス権

特権的アクセス権の割り当ておよび利用は、制限し、管理しなければならない。
【実施手順：テキストP9】

8.3 情報へのアクセス制限

情報およびその他の関連資産へのアクセスは、確立されたアクセス制御に関するトピック固有の方針に従って、制限しなければならない。
【実施手順：テキストP9】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.4 ソースコードへのアクセス

ソースコード、開発ツール、ソフトウェアライブラリへの読取りおよび書込みアクセスを、適切に管理しなければならない。
【実施手順：テキストP9】

8.5 セキュリティを保った認証

セキュリティを保った認証技術および手順を、情報へのアクセス制限およびアクセス制御に関するトピック固有の方針に基づいて備えなければならない。
【実施手順：テキストP10】

8.6 容量・能力の管理

現在および予測される容量・能力の要求事項に合わせて、資源の利用を監視し、調整しなければならない。
【実施手順：テキストP10】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.7 マルウェアに対する保護

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

【実施手順：テキストP11】

8.8 技術的脆弱性の管理

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

【実施手順：テキストP11】

8.9 構成管理

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

【実施手順：テキストP12】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.10 情報の削除

情報システム、装置またはその他の記憶媒体に保存している情報は、必要でなくなった時点で削除しなければならない。
【実施手順：テキストP12】

8.11 データマスキング

データマスキングは、適用される法令を考慮して、組織のアクセス制御に関するトピック固有の方針およびその他の関連するトピック固有の方針、並びに事業上の要求事項に従って利用しなければならない。
【実施手順：テキストP12～P13】

8.12 データ漏えいの防止

データ漏えい防止対策を、取扱いに慎重を要する情報を処理、保存、送信するシステム、ネットワークおよびその他の装置に適用しなければならない。
【実施手順：テキストP13】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.13 情報のバックアップ

合意されたバックアップに関するトピック固有の方針に従って、情報、ソフトウェアおよびシステムのバックアップを維持し、定期的に検査しなければならない。
【実施手順：テキストP13】

8.14 情報処理施設の冗長性

情報処理施設・設備は、可用性の要求事項を満たすのに十分な冗長性を持って、導入しなければならない。
【実施手順：テキストP14】

8.15 ログ取得

活動、例外処理、過失、その他の関連する事象を記録したログを取得、保存、保護し、分析しなければならない。
【実施手順：テキストP14】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.16 監視活動

セキュリティインシデントの可能性を評価するために、ネットワーク、システムおよびアプリケーションについて異常な挙動がないか監視し、適切な処置を講じなければならない。
【実施手順：テキストP14～P15】

8.17 クロックの同期

組織が使用する情報処理システムのクロックは、国の原子時計から配信される時刻に基づくクロックと同期させなければならない。
【実施手順：テキストP15】

8.18 特権的なユーティリティプログラムの使用

システムおよびアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は、制限し、厳しく管理しなければならない。
【実施手順：テキストP15】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.19 運用システムに関わるソフトウェアの導入

運用システムへのソフトウェアの導入をセキュリティを保って管理するための手順および対策を実施しなければならない。
【実施手順：テキストP15～P16】

8.20 ネットワークのセキュリティ

システムおよびアプリケーション内の情報を保護するために、ネットワークおよびネットワーク装置のセキュリティを保ち、管理し、制御しなければならない。
【実施手順：テキストP20～P21】

8.21 ネットワークサービスのセキュリティ

ネットワークサービスのセキュリティ機能、サービスレベルおよびサービスの要求事項を特定し、実装し、監視しなければならない。
【実施手順：テキストP21】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.22 ネットワークの分離

情報サービス、利用者および情報システムは、組織のネットワーク上でグループごとに分離しなければならない。
【実施手順：テキストP21】

8.23 ウェブ・フィルタリング

悪意のあるコンテンツにさらされることを減らすために、外部Webサイトへのアクセスを管理しなければならない。
【実施手順：テキストP21】

8.24 暗号の使用

暗号鍵の管理を含む、暗号の効果的な利用のための規則を定め、実施しなければならない。
【実施手順：テキストP22】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.25 セキュリティに配慮した開発のライフサイクル

ソフトウェアおよびシステムのセキュリティに配慮した開発のための規則を確立し、適用しなければならない。
【実施手順：テキストP16】

8.26 アプリケーションのセキュリティの要求事項

アプリケーションを開発または取得する場合、情報セキュリティ要求事項を特定し、規定し、承認しなければならない。
【実施手順：テキストP16～P17】

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

セキュリティに配慮したシステムを構築するための原則を確立、文書化、維持し、すべての情報システムの開発活動に対して適用しなければならない。
【実施手順：テキストP17】

作成する候補となる実施手順書類について

【参照:テキスト18-1、18-2】
P1～P22

8.28 セキュリティに配慮したコーディング

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

【実施手順:テキストP17】

8.29 開発及び受入れにおけるセキュリティ試験

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

【実施手順:テキストP18】

8.30 外部委託による開発

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

【実施手順:テキストP18】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.31 開発環境、試験環境及び運用環境の分離

開発環境、テスト環境および本番環境は、分離してセキュリティを保たなければならない。
【実施手順：テキストP18～P19】

8.32 変更管理

情報処理設備および情報システムの変更は、変更管理手順に従わなければならない。
【実施手順：テキストP19】

8.33 試験情報

テスト用情報は、適切に選定、保護、管理しなければならない。
【実施手順：テキストP19～P20】

作成する候補となる実施手順書類について

【参照：テキスト18-1、18-2】
P1～P22

8.34 監査試験中の情報システムの保護

運用システムのアセスメントを伴う監査におけるテストおよびその他の保証活動を計画し、テスト実施者と適切な管理層との間で合意しなければならない。
【実施手順：テキストP20】

実施手順を適用するセキュリティ概念

【参照:テキスト18-3-1.】
P23～P26

Security by Design

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

導入のメリット

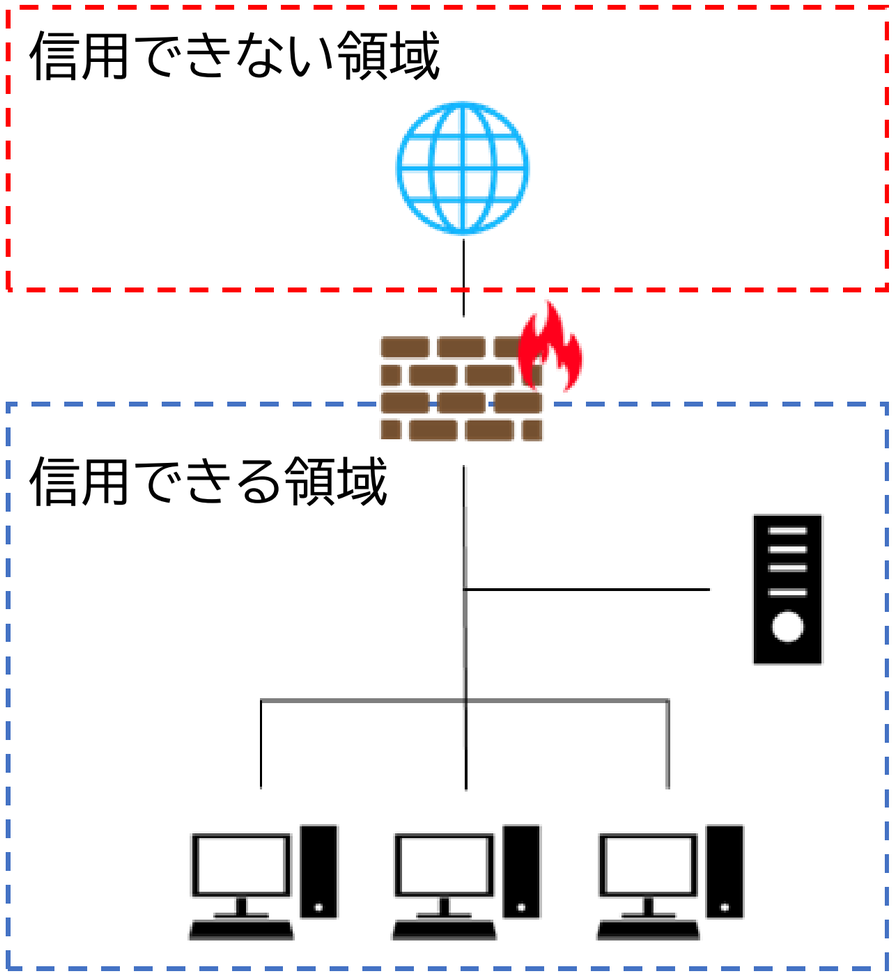
- 手戻りが少なくなり、納期を守れる
- コストを削減できる
- 保守性の高いソフトウェアができる（システムも同様）

ゼロトラスト、境界防御モデル

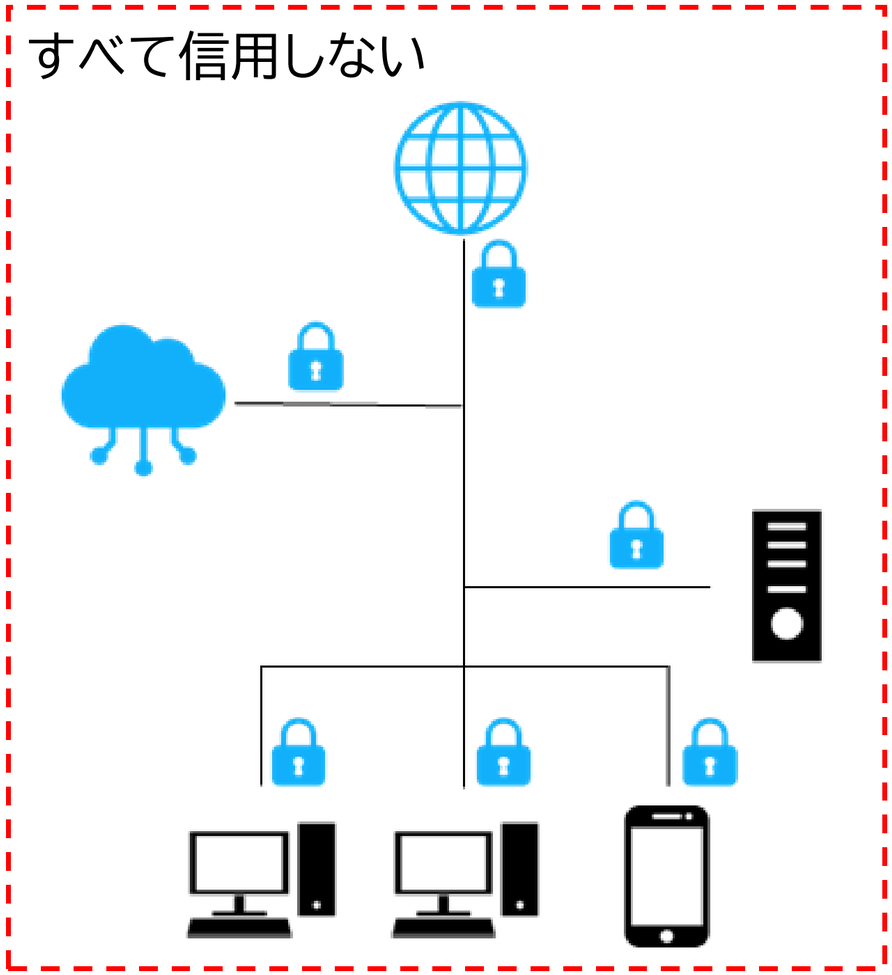
【参照：テキスト18-3-2.】
P27～P33

境界防御モデルとゼロトラストの違い

境界防御モデル



ゼロトラスト



ゼロトラスト導入に向けた進め方

【参照:テキスト18-3-2.】
P27～P33

① 企業のアクターを特定

② 企業が所有する資産を特定

③ キープロセスの特定とプロセス実行に伴うリスクの評価

④ ゼロトラスト導入候補の方針策定

⑤ ソリューション候補の特定

⑥ 初期導入とモニタリング

⑦ ゼロトラストの適用範囲拡大

ゼロトラストを実装するための主な技術要素

【参照：テキスト18-3-2.】
P27～P33

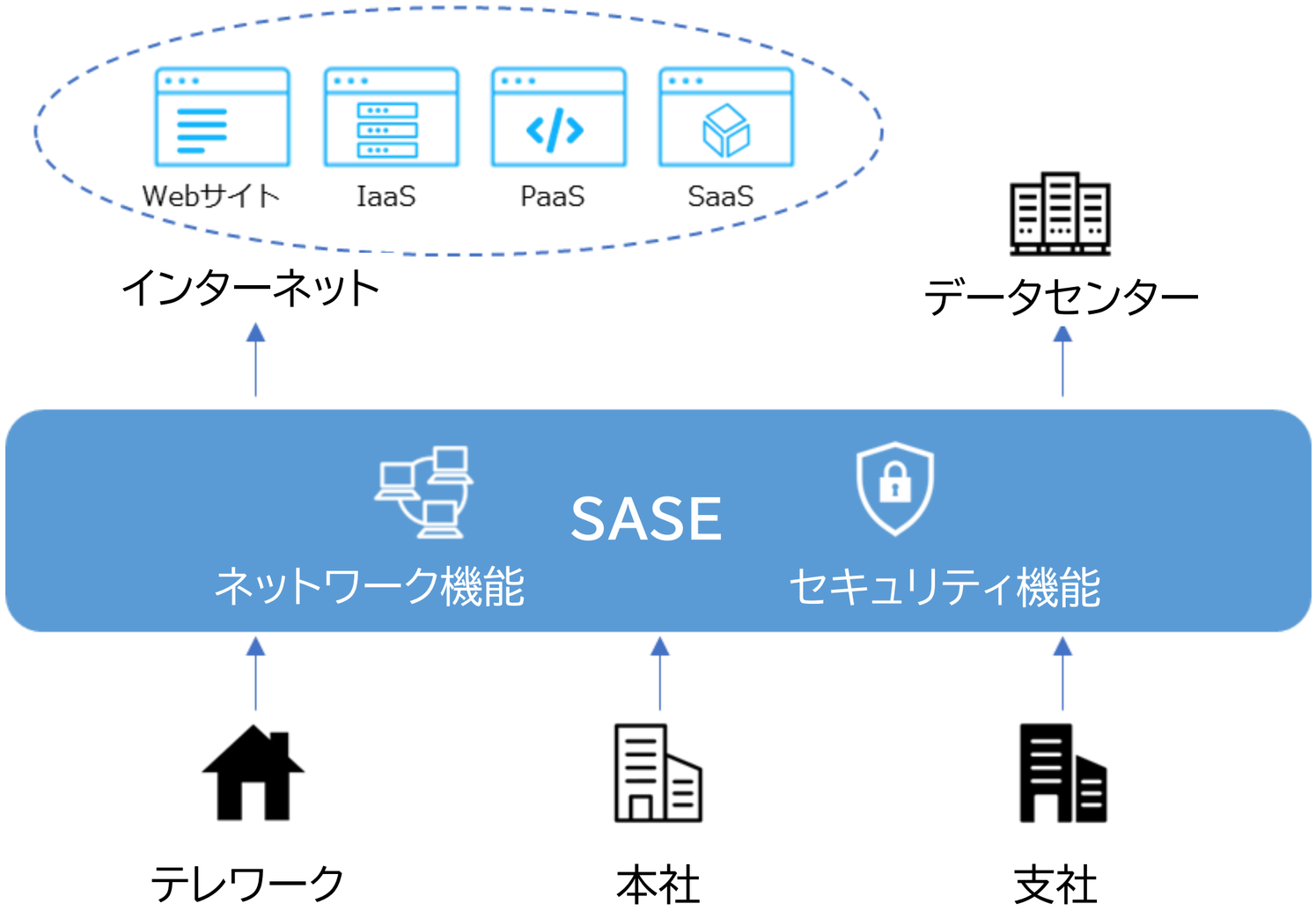
ゼロトラストを実装するために必要な技術要素

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

ゼロトラスト、境界防御モデル

【参照：テキスト18-3-3.】
P33～P35

SASE

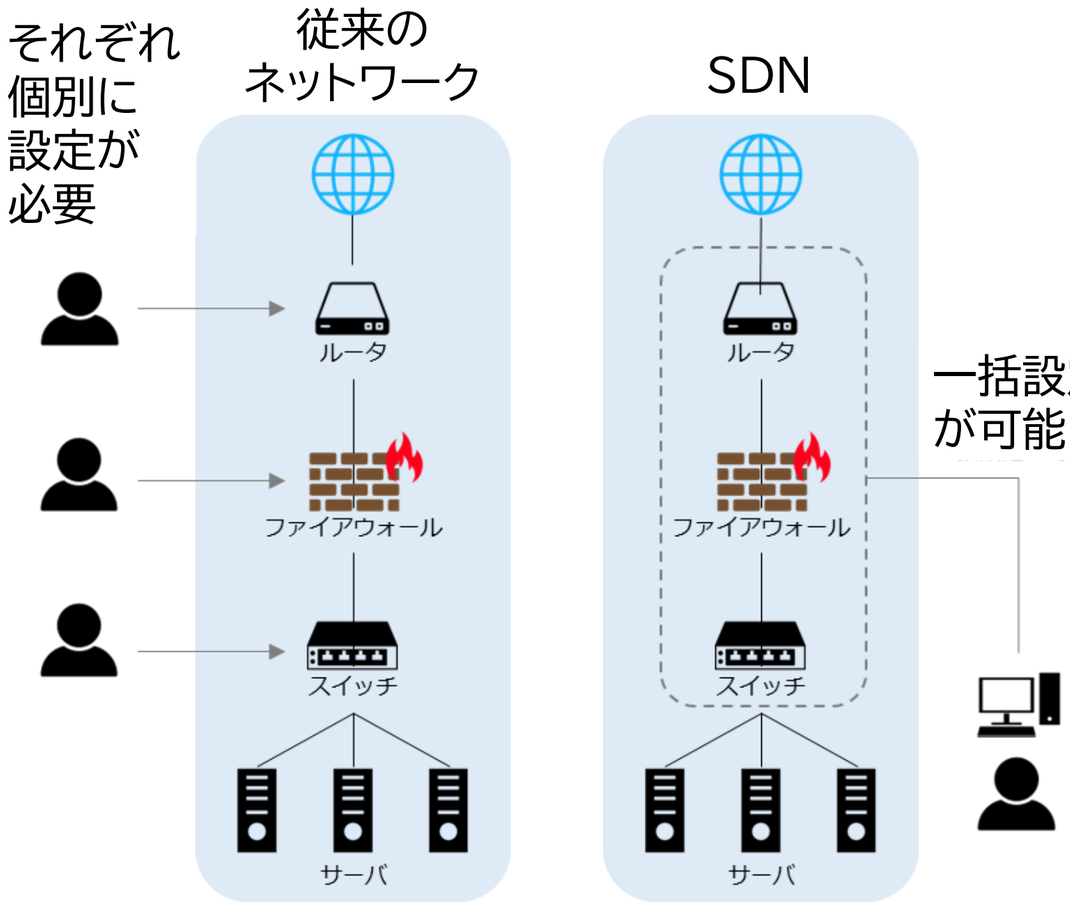


ネットワーク制御

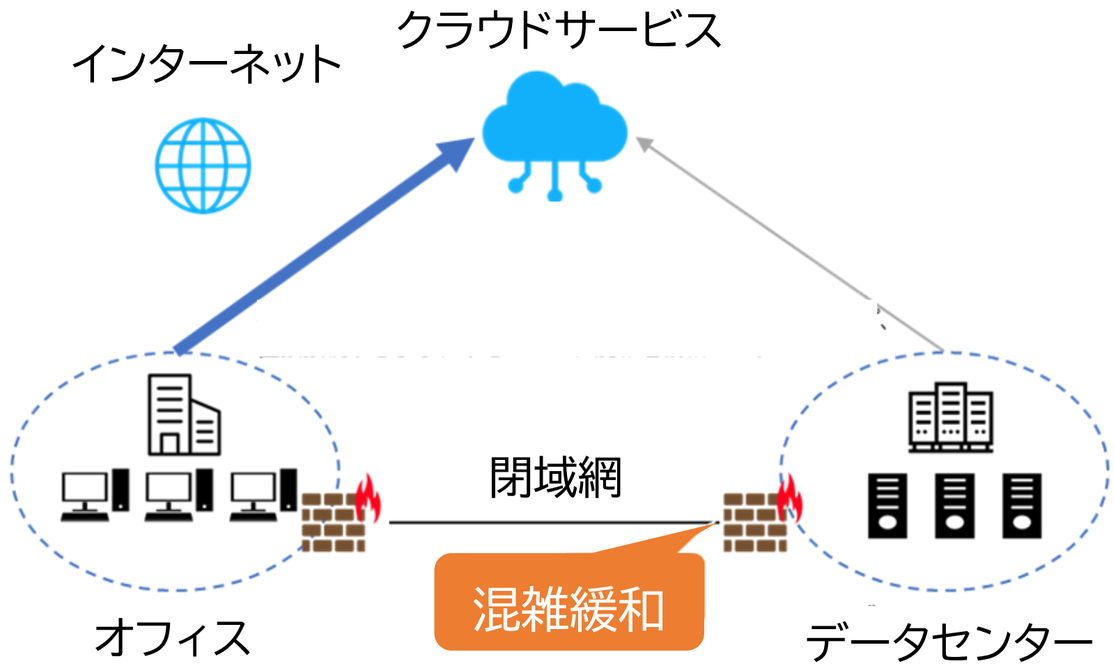
【参照:テキスト18-3-4.】
P36～P39

SDN、SD-WAN

SDN



SD-WAN



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

セキュリティ統制（Security as a Service）

【参照：テキスト18-3-5.】
P39～P44

セキュリティ統制を確立するためのセキュリティ要素

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

インシデント対応

【参照：テキスト18-4.】
P45～P48

インシデント発生時の対応

1. 検知・初動対応
2. 報告・発表
3. 復旧・再発防止

フォレンジックの実施手順例

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

第19章. セキュリティ対策の有効性評価

内部監査

外部監査

内部監査

【参照:テキスト19-1.】
P50

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

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

外部監査

【参照:テキスト19-2.】
P51～P52

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

管理基準・監査基準

- 情報セキュリティ管理基準
  - マネジメント基準
  - 管理策基準

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

第20章. セキュリティ機能の実装と運用

セキュリティ機能の実装と運用

アジャイル開発

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン概要

政府情報システム全般に関するドキュメント

文書番号	タイトル
DS-100	デジタル・ガバメント推進標準ガイドライン
DS-110	デジタル・ガバメント推進標準ガイドライン解説書
DS-120	デジタル・ガバメント推進標準ガイドライン実践ガイドブック
DS-121	アジャイル開発実践ガイドブック
DS-130	標準ガイドライン群用語集

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン概要

セキュリティに関するドキュメント

文書番号	タイトル
DS-200	政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
DS-201	政府情報システムにおけるセキュリティリスク分析ガイドライン ～ベースラインと事業被害の組み合わせアプローチ～
DS-202	CI／CDパイプラインにおけるセキュリティの留意点に関する技術レポート
DS-203	政府情報システムにおけるサイバーセキュリティに係る サプライチェーン・リスクの課題整理及びその対策のグッドプラクティス集
DS-210	ゼロトラストアーキテクチャ適用方針
DS-211	常時リスク診断・対処(CRSA)のエンタープライズアーキテクチャ(EA)

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン概要

セキュリティに関するドキュメント

文書番号	タイトル
DS-212	ゼロトラストアーキテクチャ適用方針における属性ベースアクセス制御に関する技術レポート
DS-220	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
DS-221	政府情報システムにおける脆弱性診断導入ガイドライン
DS-231	セキュリティ統制のカタログ化に関する技術レポート

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン概要

クラウドサービスに関するドキュメント

文書番号	タイトル
DS-310	政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針

データ連携に関するドキュメント

文書番号	タイトル
DS-400	政府相互運用性フレームワーク（GIF）

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン概要

トラストに関するドキュメント7.02

文書番号	タイトル
DS-500	行政手続におけるオンラインによる本人確認の手法に関するガイドライン
DS-531	処分通知等のデジタル化に係る基本的な考え方

その他ドキュメント

文書番号	タイトル
DS-910	安全保障等の機微な情報等に係る政府情報システムの取扱い

セキュリティ機能の実装と運用

【参照:テキスト20-1-1.】
P56～P63

デジタル・ガバメント推進標準ガイドライン

1. プロジェクトの管理
2. 予算および執行
3. サービス・業務企画
4. 要件定義
5. 調達
6. 設計・開発
7. サービス・業務の運営と改善
8. 運用および保守
9. システム監査

プロジェクトの管理

【参照:テキスト20-1-2.】
P63～P70

プロジェクト管理活動の全体の流れ

1. プロジェクトの立ち上げ、初動
2. プロジェクト計画書などの作成
3. プロジェクトのモニタリング
4. プロジェクトの終結

プロジェクトの目標設定におけるポイント

- 顧客が困っていること(受領連絡までの時間)への対応を優先
- 顧客や注文内容の異なりを捉え、個々のニーズへ対応(大量注文)
- 顧客目線で事前、事後の作業も改善(顧客確認)
- 小さく始める。そして、軌道修正しながら最終目標へ到達する
  (段階的なKPI)

プロジェクトの管理

【参照:テキスト20-1-2.】
P63～P70

「KGI」「CSF」「KPI」の定義と関係

- 重要目標達成指標(KGI:Key Goal Indicator)
- 重要成功要因(CSF:Critical Success Factor)
- 重要成果指標(KPI:Key Performance Indicator)

セキュリティ機能を実装・運用するためのポイント

- 多数の事業者間をまたいだシステム障害が発生するリスクへの対応
- 個人情報などの重要情報が漏えいするリスクへの対応

予算および執行

【参照:テキスト20-1-3.】
P70～P78

予算活動の全体の流れ

1. 予算のための稟議(予算要求)の事前準備
2. 見積り依頼
3. 見積りの精査
4. 予算のための稟議(予算要求)に必要な資料の準備
5. 概要要求に向けた調整
6. 予算執行について

セキュリティ機能を実装・運用するためのポイント

- 情報システムを構成する製品のサポート終了に付随する経費の考慮
- 人事異動時の引続き不足を防ぐこと

サービス・業務企画

【参照：テキスト20-1-4.】
P78～P83

サービス・業務企画の全体の流れ

1. サービス・業務企画の開始準備
2. 利用者視点でのニーズ把握
3. 業務の現状把握
4. サービス・業務企画内容の検討
5. 軌道修正
6. 新しい業務要件の定義

セキュリティ機能を実装・運用するためのポイント

- デジタル技術を徹底的に活用する

要件定義

【参照:テキスト20-1-5.】
P83～P91

要件定義の全体の流れ

1. 要件定義の事前準備
2. RFIの実施
3. 要件定義の全体像
4. 機能要件の定義
5. 新しい非機能要件の定義
6. 要件定義終了後の対応

要件定義プロセスにおけるFit＆Gap分析

1. 業務要件の整理
2. パッケージソフトやSaaSの機能確認
3. フィット部分の特定（Fit）
4. ギャップ部分の特定（Gap）
5. コストとリスクの評価

要件定義

【参照:テキスト20-1-5.】
P83～P91

Fit＆Gap分析結果に基づく決定

決定	条件
そのまま導入	フィット部分が大きくカスタマイズ不要な場合
部分的にカスタマイズして導入	小規模なギャップがあり、一部カスタマイズやプロセス変更で対応可能な場合
大幅なカスタマイズまたは導入中止	ギャップが大きく、コストやリスクが許容範囲を超えるような場合

セキュリティ機能を実装・運用するためのポイント

- 非機能要件における、情報セキュリティに関する事項について
- 想定されるリスクの概要と対策について
- 最低限記載すべき情報セキュリティ対策要件

調達

【参照:テキスト20-1-6.】
P91～P95

調達の全体の流れ

1. 調達の事前準備
2. 調達仕様書の作成
3. 調達仕様書以外のドキュメント作成
4. 調達手続きとプロジェクト管理
5. 検収

セキュリティ機能を実装・運用するためのポイント

- 再委託先の情報セキュリティ対策に係る規定を確認すること

設計・開発

【参照:テキスト20-1-7.】
P95～P104

設計・開発の全体の流れ

1. 設計・開発を開始するための事前準備
2. 設計・開発の計画
3. 設計・開発・テストの管理
4. 見落としがちな活動に注意
5. 新業務の運営を円滑に行うための準備

セキュリティ機能を実装・運用するためのポイント

- テスト計画の策定
- テストのレベルと種類
- テストツールの活用

サービス・業務の運営と改善

【参照：テキスト20-1-8.】
P104～P109

サービス・業務の運営と改善の全体の流れ

1. 新しいサービス・業務の事前準備
2. 業務の定着と次の備え
3. 業務の改善

セキュリティ機能を実装・運用するためのポイント

- 業務を外部委託する際の注意
- インシデントの優先度づけ

運用および保守

【参照:テキスト20-1-9.】
P109～P117

運用および保守の全体の流れ

1. 運用・保守を開始するための事前準備
2. 運用・保守の計画
3. 運用・保守の定着と次の備え
4. 運用・保守の改善と業務の引継ぎ

セキュリティ機能を実装・運用するためのポイント

- セキュリティ関連作業を定期的に確実に実施すること
- セキュリティ対策会議の実施
- 情報システムのアカウントの管理

システム監査

【参照:テキスト20-1-10.】
P117～P120

システム監査の全体の流れ

1. システム監査の理解
2. システム監査計画と監査実施計画
3. システム監査の実施
4. 指摘事項を踏まえた改善

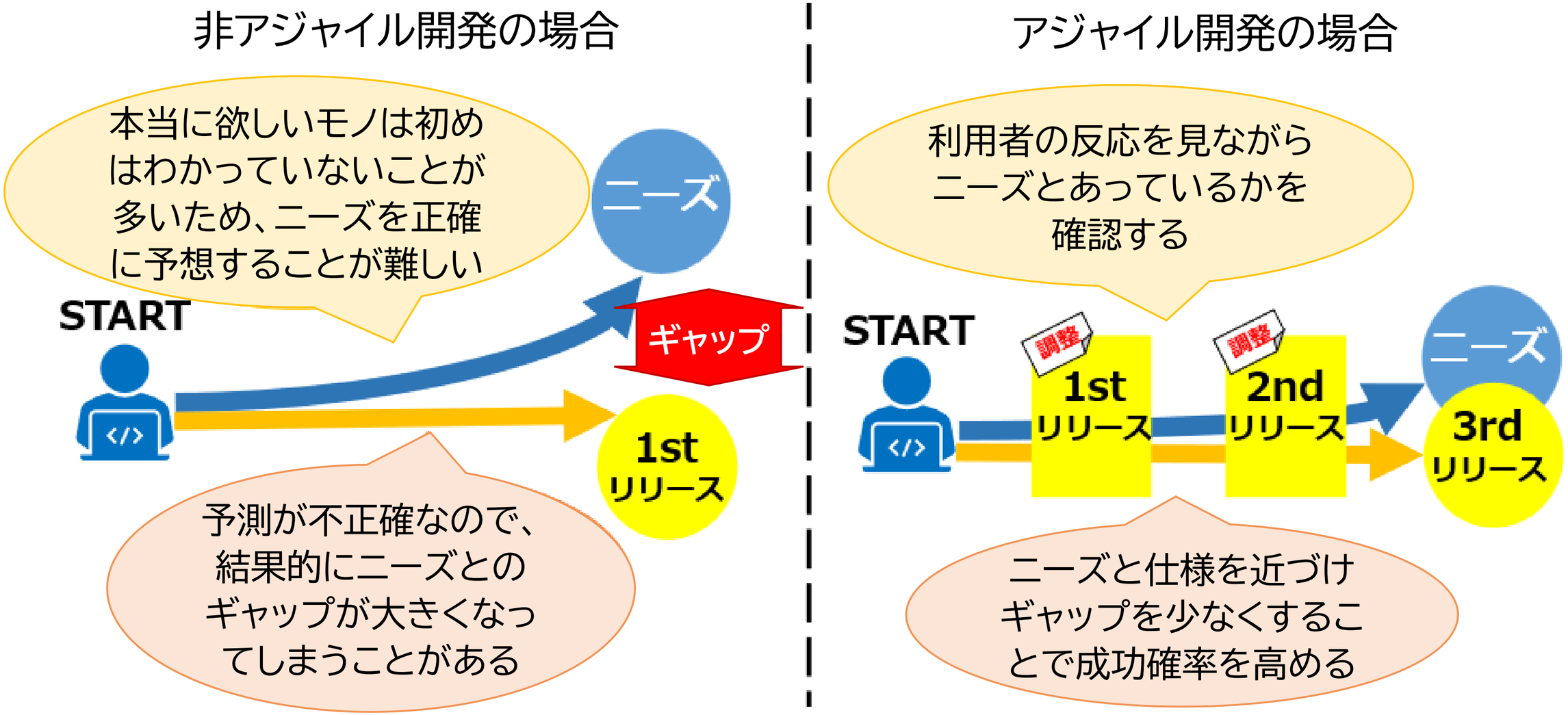
セキュリティ機能を実装・運用するためのポイント

- 情報セキュリティ監査

アジャイル開発

【参照:テキスト20-2-1.】
P121～P122

アジャイル開発の概要

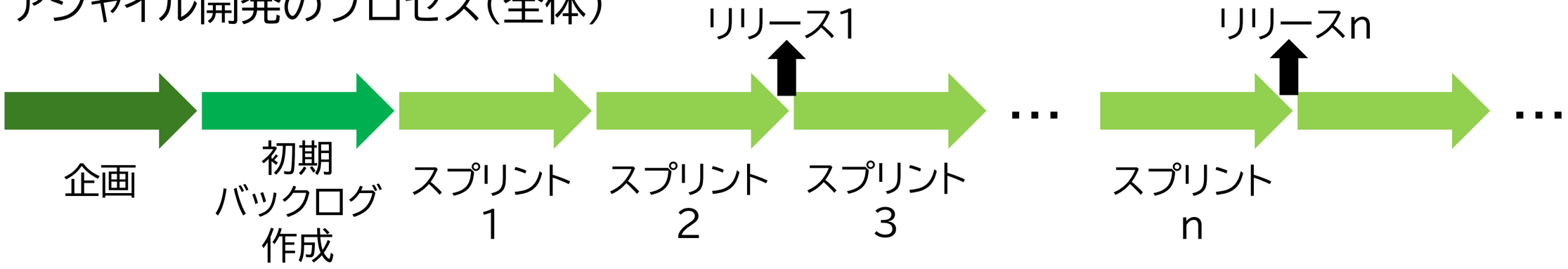


アジャイル開発

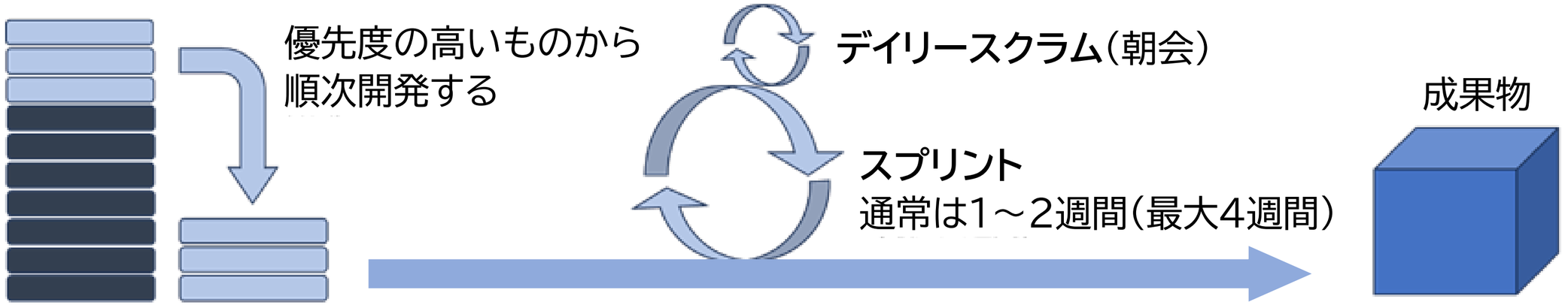
【参照:テキスト20-2-2.】
P122～P124

アジャイル開発の実施ポイント

アジャイル開発のプロセス(全体)



アジャイル開発のプロセス(イテレーション)



令和7年度
中小企業サイバーセキュリティ
実践力強化プログラム

東京都産業労働局