令和6年度
中小企業サイバーセキュリティ
社内体制整備事業

第6回

第8編：具体的な構築・運用の実践【レベル3】

セミナー内容

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

セミナー内容

編	テーマ
第6編	ISMSなどのフレームワークの種類と活用法の紹介
第7編	ISMSの構築と対策基準の策定と実施手順
第8編	具体的な構築・運用の実践
第9編	中小企業が組織として実践するためのスキル・知識と人材育成
第10編	全体総括

セミナー内容

第20章. セキュリティ機能の実装と運用

（IT環境構築・運用実施手順）

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

デジタル・ガバメント推進標準ガイドライン概要

【参照：テキスト20-1-1.】
P3～P4

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

デジタル・ガバメント推進標準ガイドライン概要

【参照：テキスト20-1-1.】
P4～P5

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-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

デジタル・ガバメント推進標準ガイドライン概要

【参照：テキスト20-1-1.】
P5

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

デジタル・ガバメント推進標準ガイドライン概要

【参照：テキスト20-1-1.】
P5～P6

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

デジタル・ガバメント推進標準ガイドライン概要

【参照：テキスト20-1-1.】
P6

トラストに関するドキュメント

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

デジタル・ガバメント推進標準ガイドライン

【参照：テキスト20-1-1.】
P7～P10

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.】
P10～P15

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

「KGI」「CSF」「KPI」の定義と関係

【参照：テキスト20-1-2.】
P16～P17

- 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.】
P17～P26

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.】
P27～P32

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.】
P32～P38

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

Fit＆Gap分析結果に基づく決定

【参照：テキスト20-1-5.】
P38～P40

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	キャップが大きく、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.】
P40～P45

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

設計・開発の全体の流れ

【参照：テキスト20-1-7.】
P45～P54

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

サービス・業務の運営と改善の全体の流れ

【参照：テキスト20-1-8.】
P54～P59

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つけ

運用および保守

運用および保守の全体の流れ

【参照：テキスト20-1-9.】
P59～P67

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

システム監査の全体の流れ

【参照：テキスト20-1-10.】
P67～P71

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

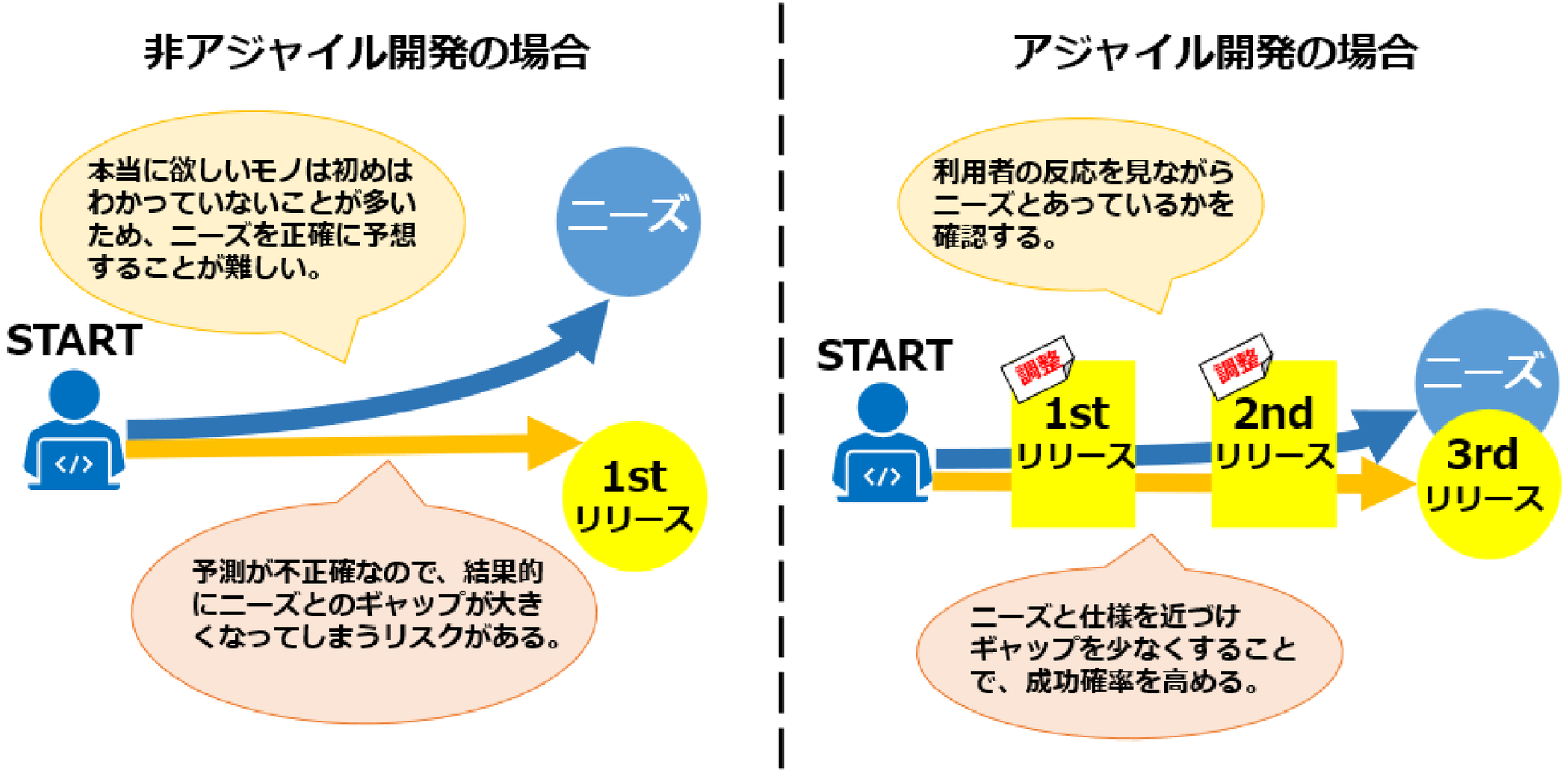
セキュリティ機能を実装・運用するためのポイント

- 情報セキュリティ監査

アジャイル開発

アジャイル開発の概要

【参照：テキスト20-2-1.】
P72～P73

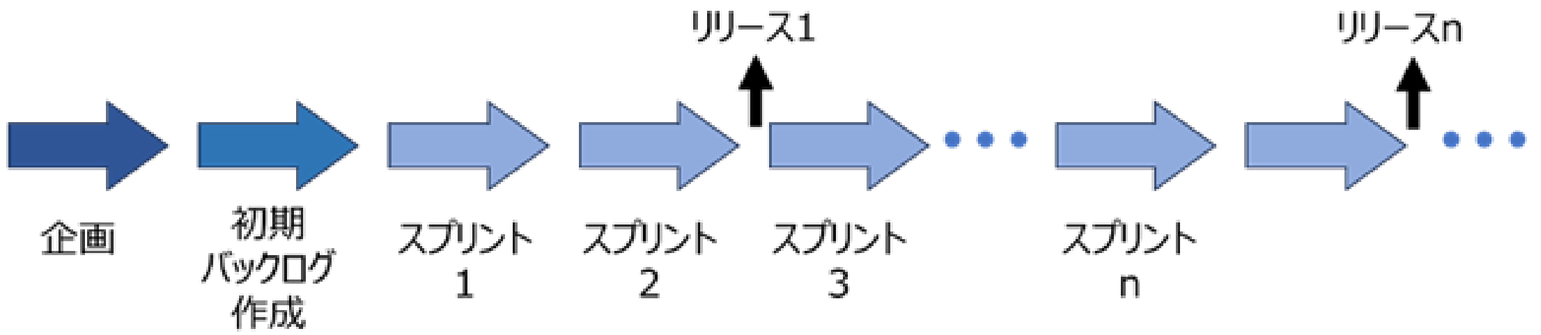


アジャイル開発

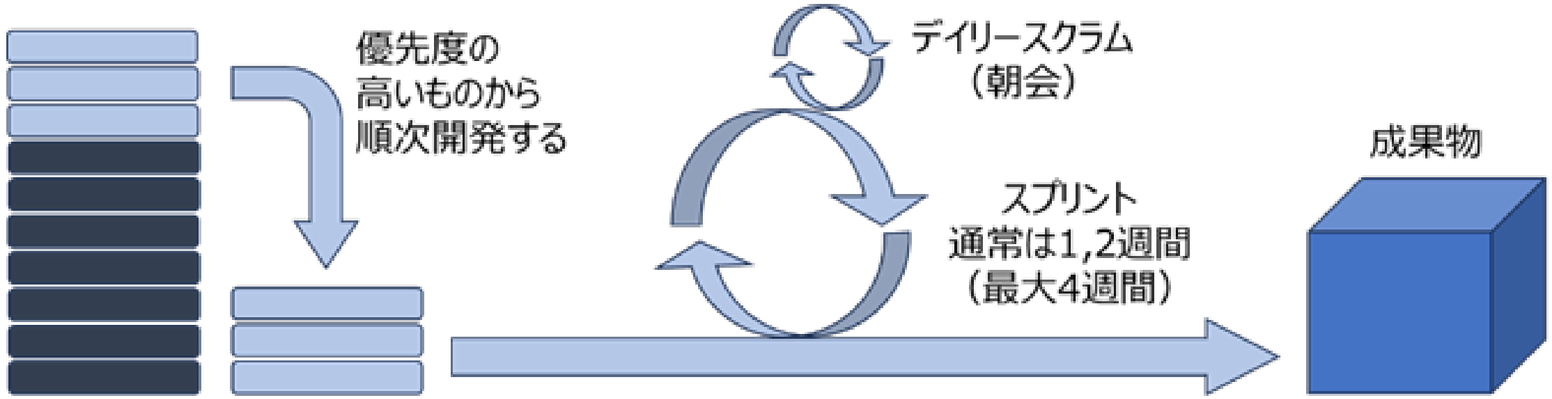
アジャイル開発の実施ポイント

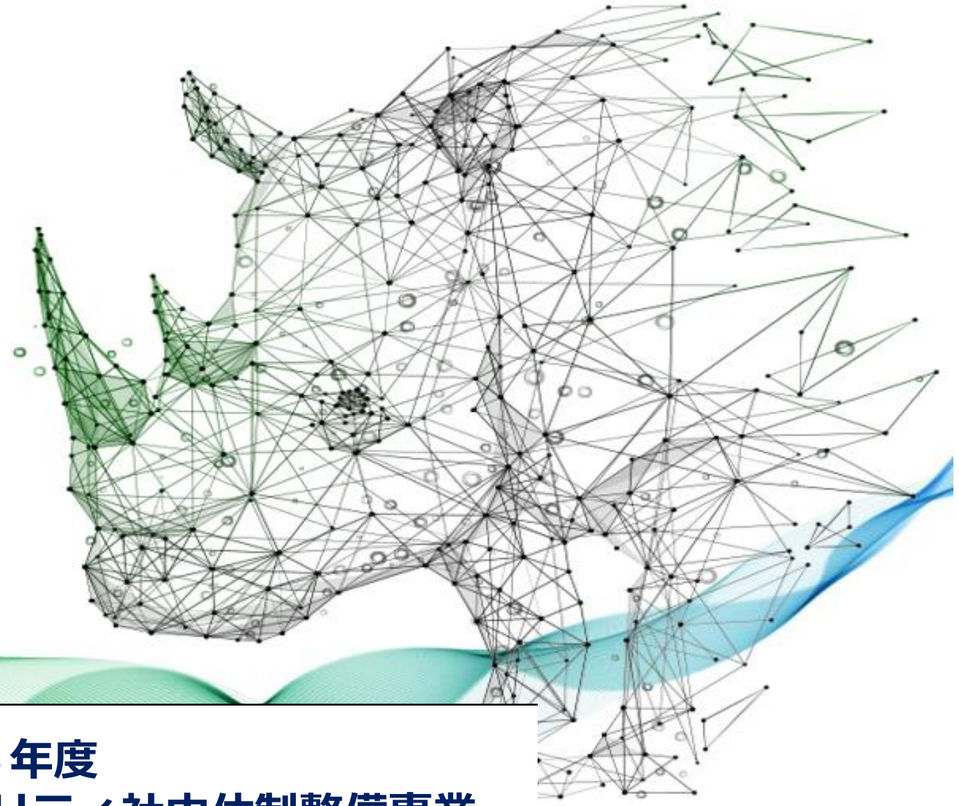
【参照：テキスト20-2-2.】
P73～P75

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６年度
中小企業サイバーセキュリティ社内体制整備事業