HITACHI
Inspire the Next

ソフトウェア品質シンポジウム 2024

セキュリティリスクアセッサー任命制度の導入と効果

トータルセキュリティ品質の向上に向けて

2024/9/12

株式会社 日立製作所 デジタルシステム&サービス統括本部
品質保証統括本部 社会システム品質保証本部
公共システム品質保証部
中村 雄一、増田 耕弐

HITACHI
Inspire the Next

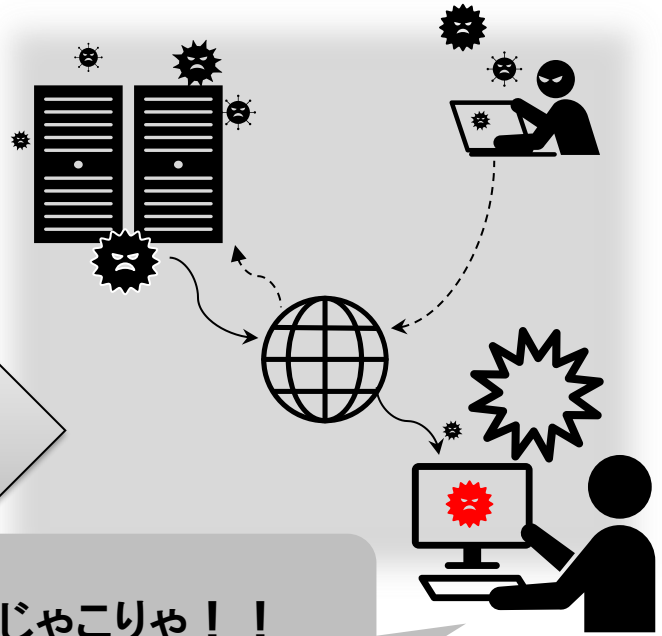
Contents

HITACHI
Inspire the Next

1. イントロダクション

1．1　イントロダクション（問題提起）

レビューはしたけど…



なんじゃこりゃ！！

セキュリティレビューにおける課題

課題①　セキュリティマインドの低さ
課題②　新技術への追従不足
課題③　チェック観点の誤認や対応不足

1．2　イントロダクション（対策方針）

セキュリティリスクアセッサー
任命制度を導入！

アセッサーの目的

アセッサーは、定めたレビューにおいてセキュリティ上必要とした施策に対し、
PMを含む開発メンバーへ指導・助言を行うことを目的にする。
また、アセッサーはプロジェクトに参画していない第三者のメンバーとする。

レビュー対応フェーズ

- ①企画(開発見積)フェーズ
- ②基本設計フェーズ
- ③テスト(脆弱性点検)フェーズ
- ④稼働後の運用フェーズ

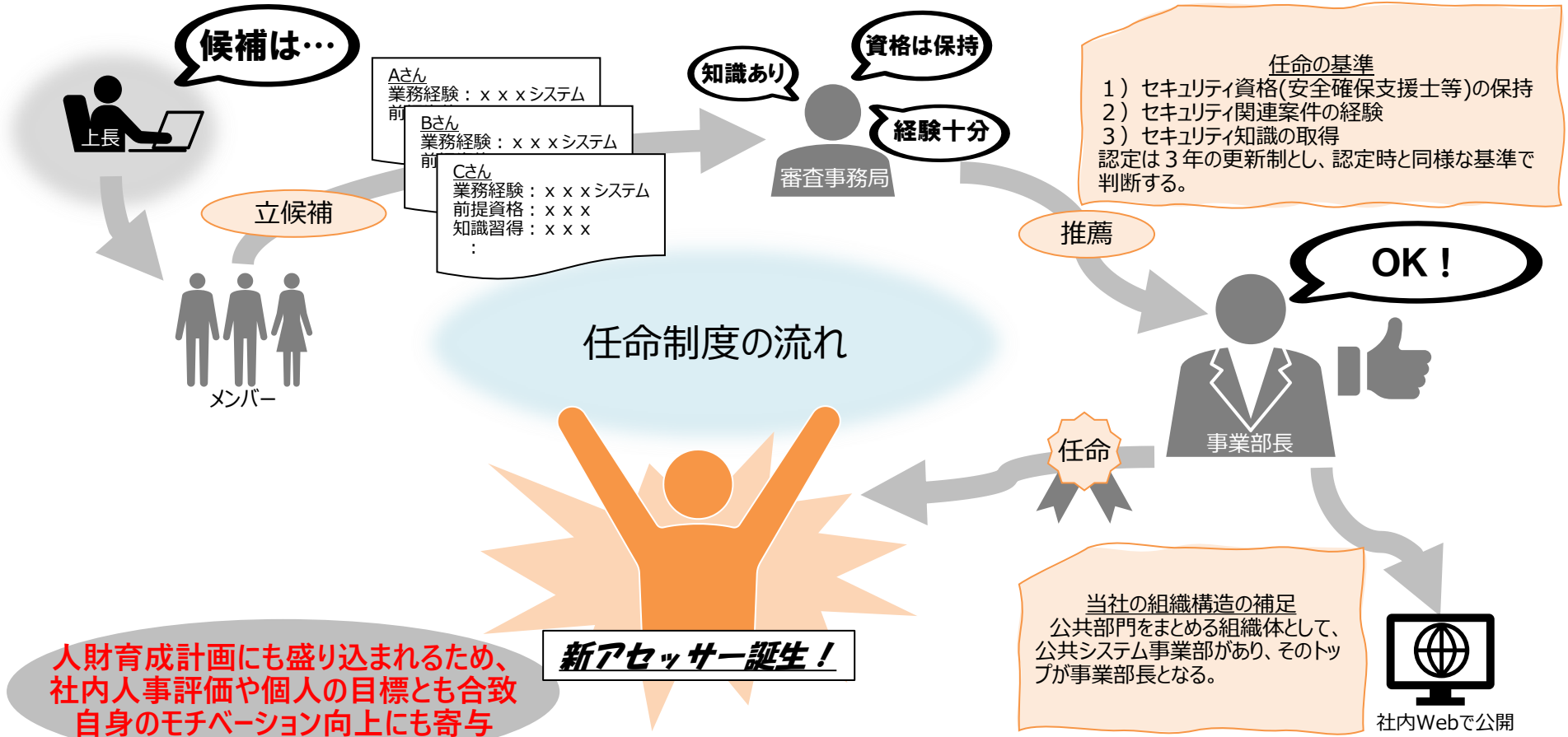
システム開発のポイントとなる
各フェーズでレビューに参画し、
システムの見積から運用までの全体工程で、
トータルセキュリティ品質の向上に
寄与が可能となった！

HITACHI
Inspire the Next

2. 施策概要

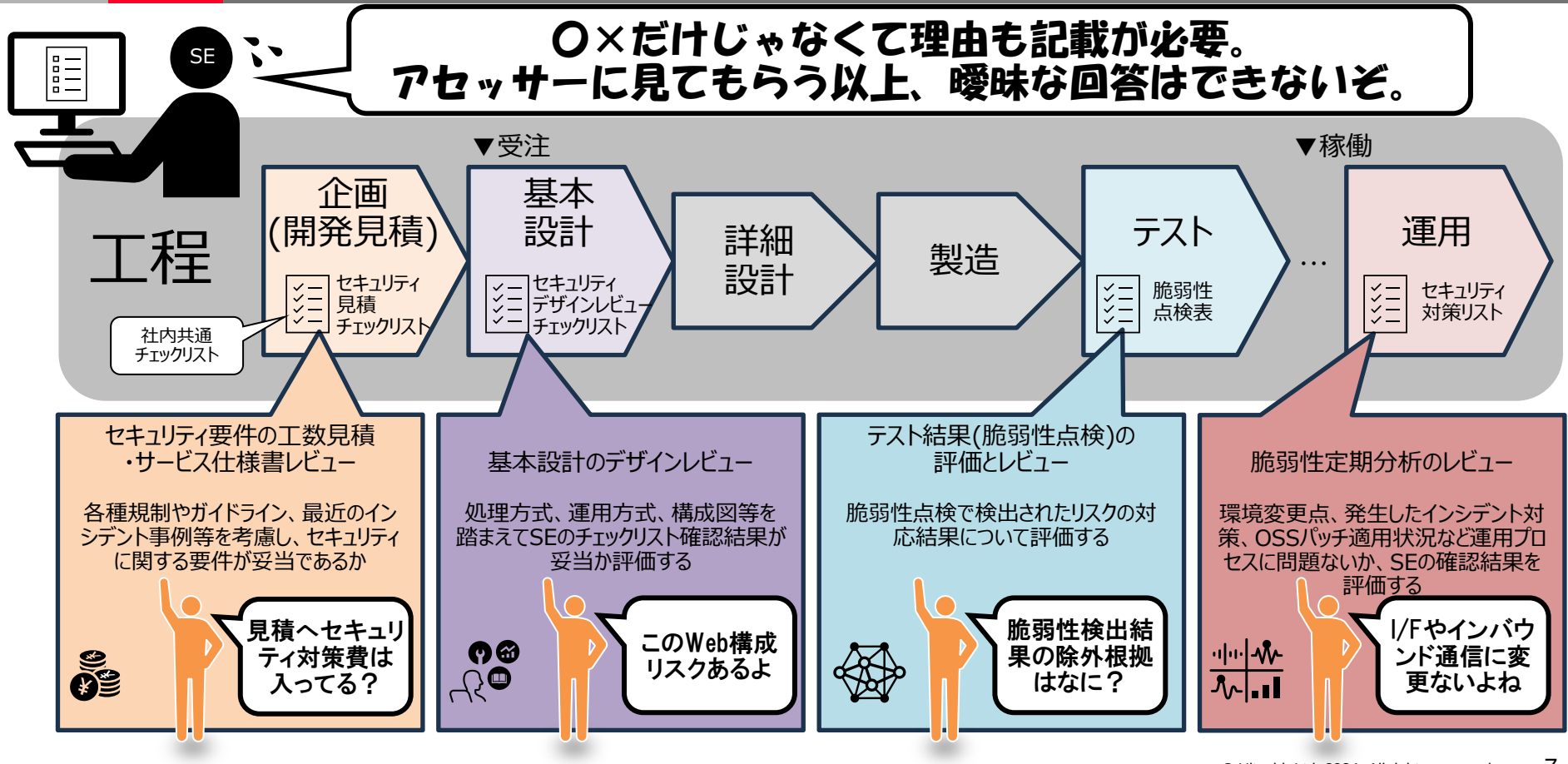
2．1　施策概要（任命制度）

HITACHI
Inspire the Next



2．2　施策概要（役割定義）

HITACHI
Inspire the Next



HITACHI
Inspire the Next

3. 実施結果

3．1　実施結果（レビュー回数）

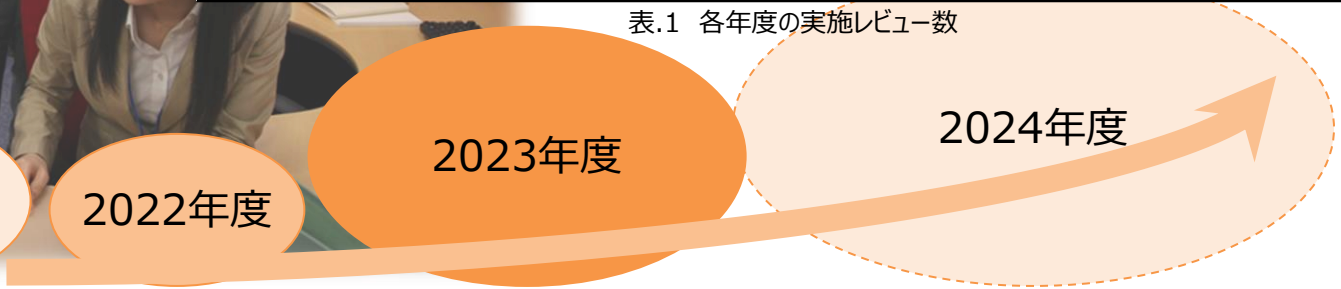
HITACHI
Inspire the Next

具体的な指摘は
次のスライドで紹介

【レビュー対象】
インターネット接続のあるシステムを前提に
・21～22年度は自社システム開発を対象
・23年度は他社システム開発も対象へ拡大

年度	合計	フェーズ			
		企画	設計	テスト	運用
2021年度	100	55	17	15	13
2022年度	88	48	14	8	18
2023年度	171	65	46	29	31

表.1　各年度の実施レビュー数



・対象システムの拡大に伴い、実施レビュー数も増加。
・レビュー未実施だった場合も多くの問題点は従来テストで摘出されるが、見逃したいくつかは残存しセキュリティ脆弱性となってしまう。
・そのままリリースされ、セキュリティインシデントへつながるリスクがあった。そのため、レビュー実施回数の増加は、広く効果ある施策だと分析する。

3．2　実施結果（主な指摘ポイント）

セキュリティ要件定義の見積・サービス仕様書レビュー

・特殊なユーザー認証使用時の対応方針
・外部(インターネット)との通信経路の明確化
・脆弱性点検の実施計画の明記
・開発中に発生するEOL宣言やパッチ対応の費用計上
：

基本設計のデザインレビュー

・社内ネットワークが安全であるとの過信/誤認識によるセキュリティ対策不足の改善
・バックアップ環境の接続元アクセス管理不足
・管理者アカウント/ルートユーザーの制限運用
：

テスト結果(脆弱性点検)の評価とレビュー

・ＷＡＦ(Web Application Firewall)の設定改善
・内部連携するWebAPI用ポートを80番から変更
・脆弱性ツールでの対策内容が設計書へフィードバックされているか不明
：

脆弱性定期分析のレビュー

・ログの保管期間(サイクル間隔)の状況確認
・運用におけるプロジェクトルール等の文書や各種チェックリスト実施の周知や実施結果保持
・構成変更の有無確認
：

HITACHI
Inspire the Next

4. 結論

4. 1　結論（問題解決状況）

HITACHI
Inspire the Next

セキュリティレビューにおける課題

課題①　セキュリティマインドの低さ
課題②　新技術への追従不足
課題③　チェック観点の誤認や対応不足

セキュリティリスクアセッサー任命制度の効果

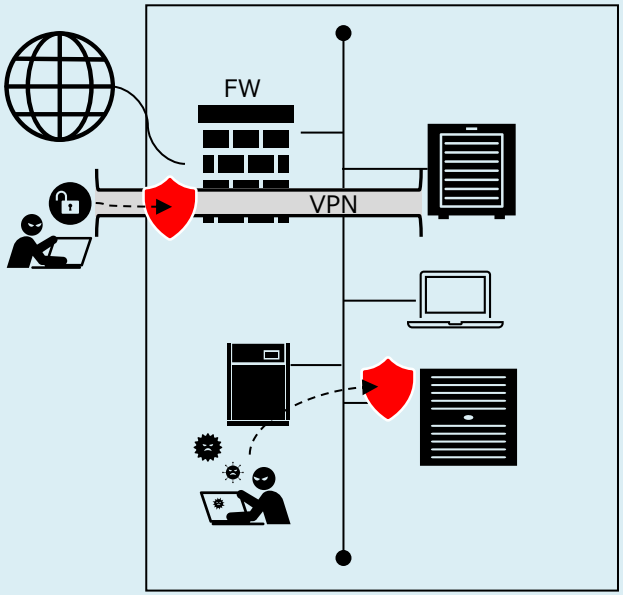
マインド醸成

スキル保持者の確保

育成計画

アセッサーの浸透

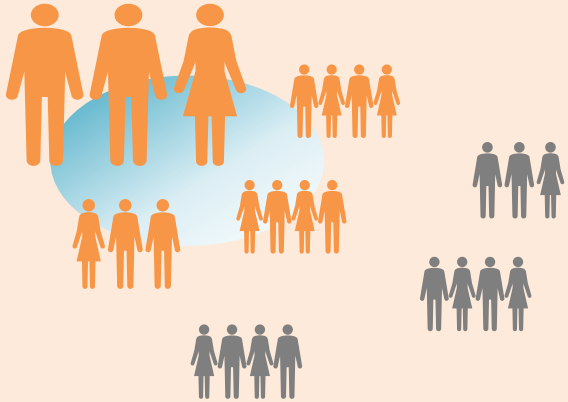
4．2　結論（今後の展開）



ゼロトラストの考えに対応

領域拡大

アセッサーの増員が必要



・アセッサー育成を事業部施策として展開し、トップダウン的に組織として増員していく
・アセッサーの活動をより周知/浸透させ、キャリアプランの一つとなるよう啓発活動を進める

HITACHI
Inspire the Next

END

セキュリティリスクアセッサー任命制度の導入と効果
トータルセキュリティ品質の向上に向けて


Hitachi Social Innovation is
POWERING GOOD