Hardening Designers Conference

NECの実践から考える、AI時代の脆弱性管理

２０２６年7月３日
日本電気株式会社
サイバーセキュリティ技術統括部

NECにおけるセキュア開発・運用の体系

国際的な規格類とNECグループでの独自の知見から、サイバーセキュリティ管理規程、実施基準、マニュアル／ガイドを作成

① 各種情報の集約と体系化

各種外部規格やガイドから必要な要素を
取り込み集約、統一的な枠組みとして体系化

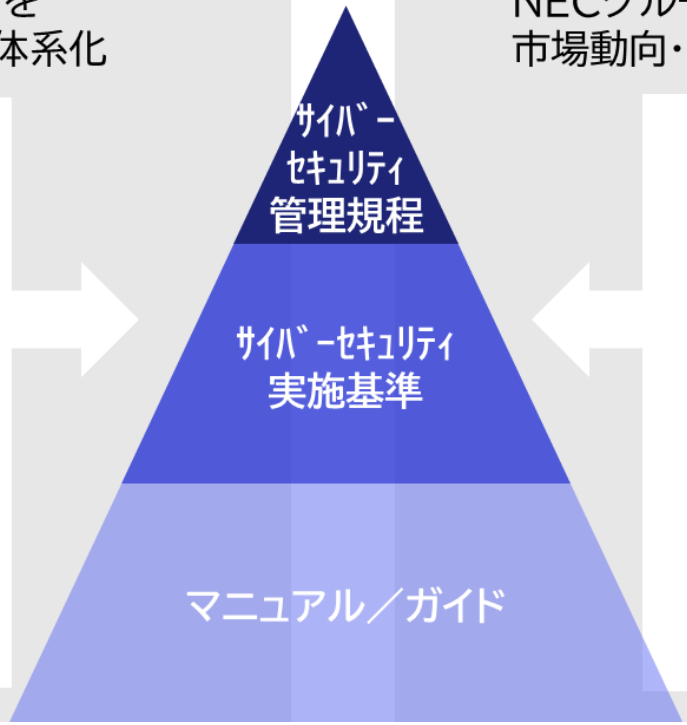
外部規格・ガイド

国際標準規格

ISO/IEC 15408, Common Criteria	PCI DSS
	IEC62443

国内の基準・ガイド	業界団体のガイド
内閣 サイバーセキュリティセンター	IPA
総務省	JPCERT/CC
経済産業省	業界/分野別

海外のガイド	NIST SP800-53



② NECグループでの実践と積み重ね

NECグループ内での長年にわたる活用の中で、
市場動向・事故事例の取り込み等により強化

市場の動向

新たな脆弱性、
サイバー攻撃の対策

セキュリティ
事故の再発防止策

サイバーセキュリティ経営報告書2026 https://jpn.nec.com/sustainability/ja/security/index.html

セキュア開発プロセスの実現

NECでは、20年以上にわたりSecurity By Designの取り組みを実施
システム・製品(サービス)開発全工程にて、経験と実績を活かしたセキュア開発プロセスを実践

事業部門でセキュリティ実装を徹底する仕組みづくり

体制

事業部門にセキュリティ責任者を配置

プロセス

サイバーセキュリティ管理規程
全社員対象に全社規程として厳格化

約400項目のチェックリスト
ISO/IEC15408、NIST SP800-171など
国際標準や業界ガイドライン、最新技術動向を参照

システム化

サイバーセキュリティチェックリスト管理システム
対策状況の一元管理およびモニタリング/是正指示

脆弱性管理システム
システム構成製品の脆弱性情報をタイムリーに配信

脆弱性管理の高度化への取り組み

NECがお客様に提供したシステムに影響する緊急性・優先度の高い脆弱性情報を見極め、対処の早期化により脆弱性起因のセキュリティ事故を防ぐ仕組みを構築

緊急性・優先度の高い脆弱性情報選定

サイバーセキュリティ事業戦略会議(隔週開催)

セキュリティホットトピックス今、注目すべき脆弱性3選

セキュリティ最新情報

注意喚起・通知

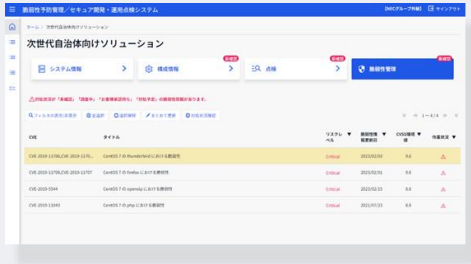
該当システムの絞り込み

セキュリティ責任者向けダッシュボード

各システム担当者(SE)へ調査・対処を指示

脆弱性の詳細確認対処策の把握

脆弱性予防管理システム



システム環境等を考慮したスコアリング・可視化
SEは対処策検討に集中

お客様への対処の必要性の提示

影響有無情報提供

回避策・パッチ適用提案

NECが提供するシステムにおける脆弱性対応の例

お客様との契約内容や脆弱性のトリアージを踏まえて検証を行い、パッチを適用する対応を実施

公的機関
・NVD
・JPCERT/CC　など
脆弱性情報収集

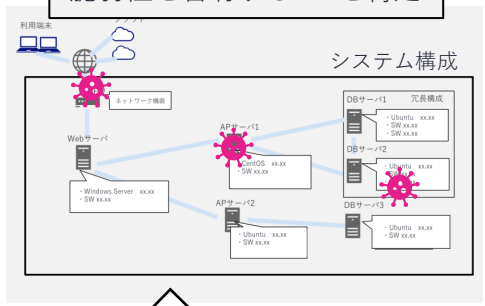
ベンダサイト
・HWベンダー
・SWベンダー　など
脆弱性情報収集

脆弱性予防管理システム

脆弱性情報

脆弱性トリアージとパッチ検証・適用

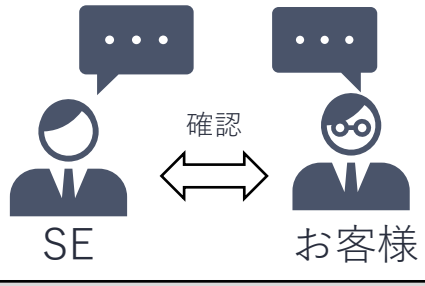
脆弱性を含有するSWを特定



脆弱性をトリアージ

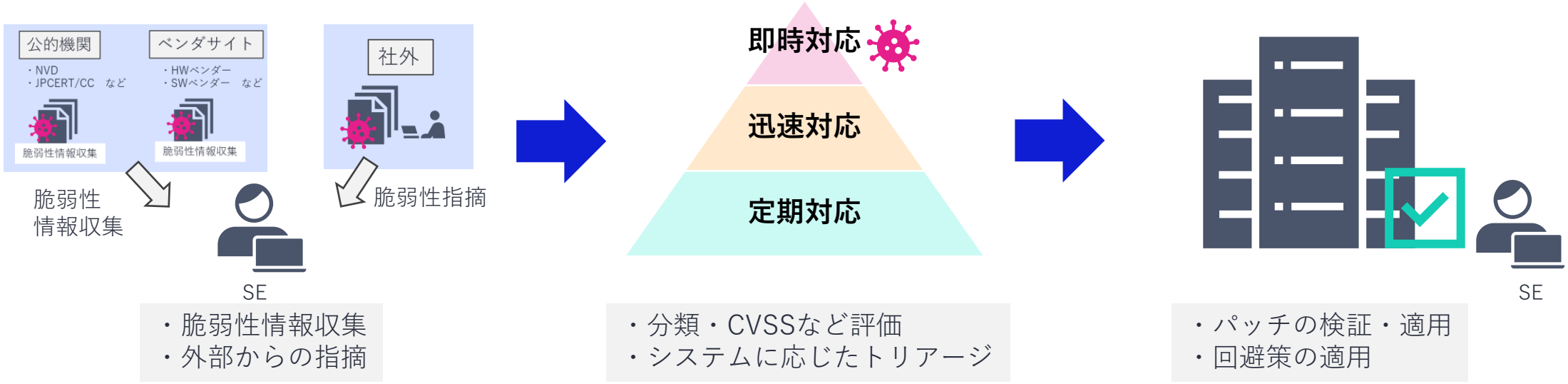
パッチ検証・適用

脆弱性対応方針の整合



AI時代の脆弱性管理における困りごと

AIの到来により、脆弱性はこれまで以上に速く、大量に発見されるようになった
その結果、脆弱性を悪用した攻撃のリスクも高まっている



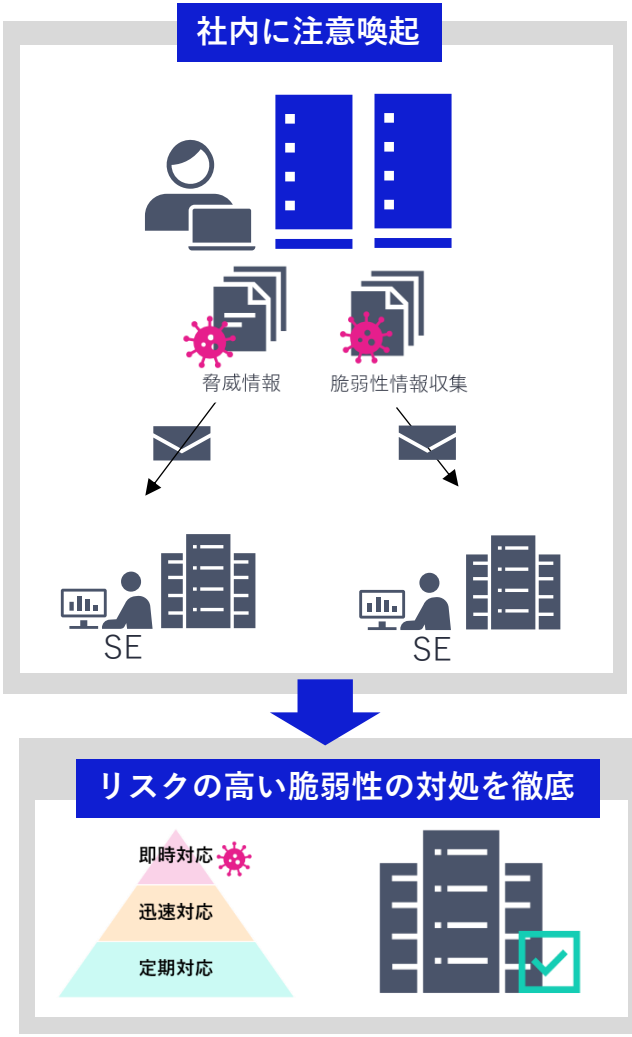
AI

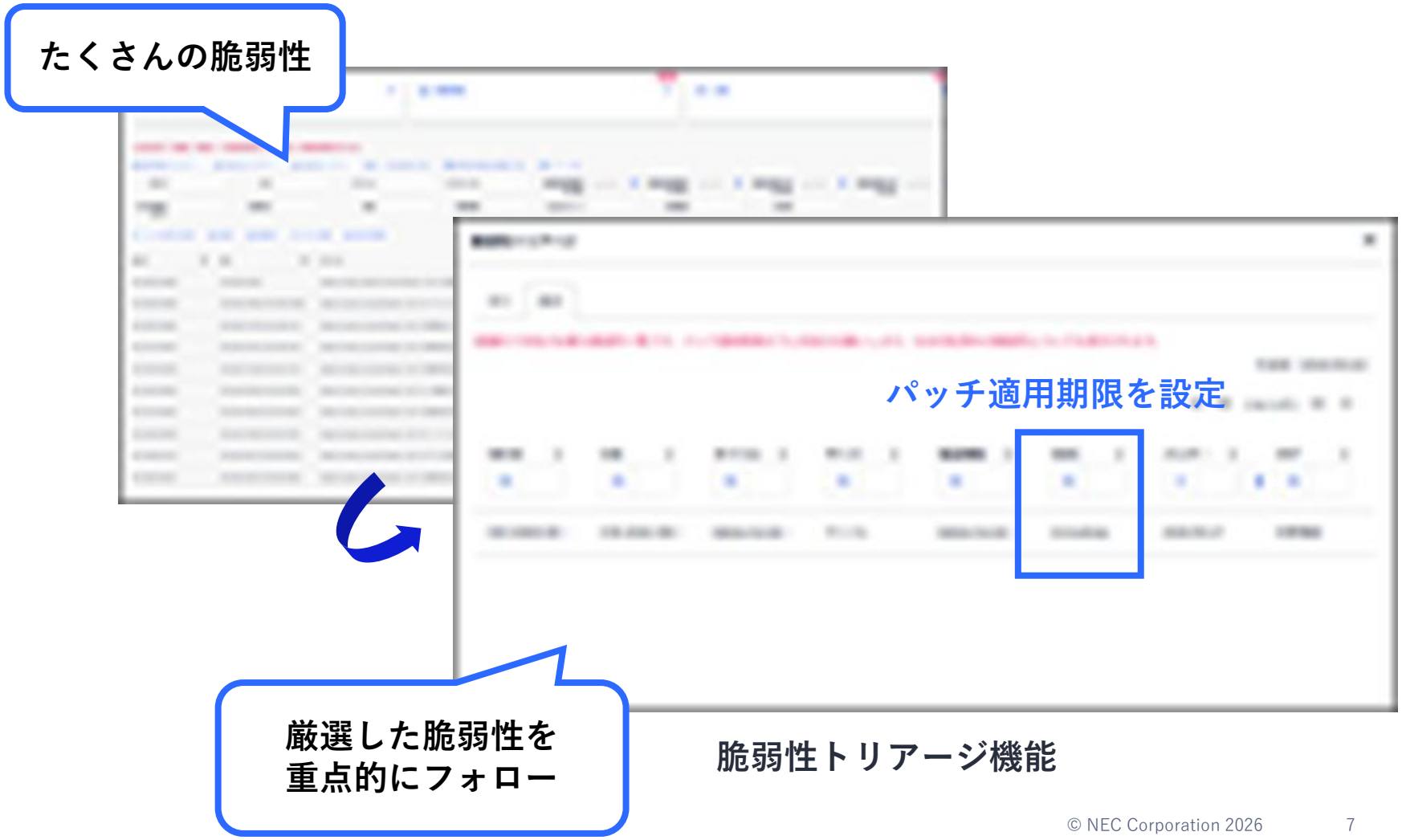
脆弱性発見の速度と網羅性が飛躍的に拡大
・検出される脆弱性が急増し、**人手対応では処理しきれない**状態

対応策としてチャレンジしていることの一部
・NECのインテリジェンスを活かした、**優先的トリアージ・対処徹底**
・SBOMを用いた**網羅的な脆弱性の探索・発見**

NECのインテリジェンスを活かした、優先的トリアージ・対処徹底

脅威情報を集約し、その情報をもとに社内への注意喚起を実施
あわせて、対象となる脆弱性については該当システムを特定し、対処の徹底を図っている

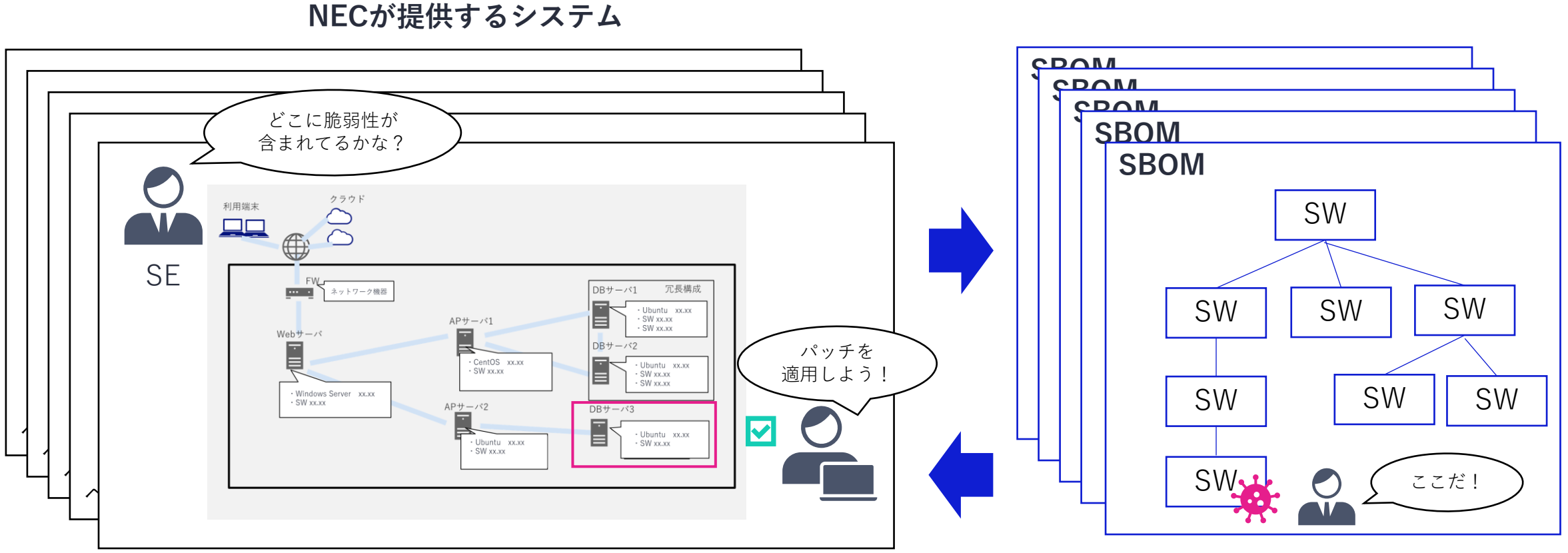




脆弱性トリアージ機能

SBOMを用いた網羅的な脆弱性の探索・発見

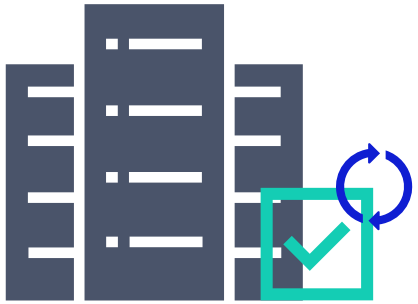
システムで使用するソフトウェアのSBOMを登録し、緊急対応が必要な脆弱性が構成情報のどこに含まれているかを網羅的に特定する



より高度な脆弱性管理へ

これまで紹介した施策に加え、従来から取り組んできた活動を一層徹底することが重要
あわせて、桁違いの変化に対応するため、防御側としてもAIを活用した中長期的な準備が必要

パッチ適用のリードタイムの短縮

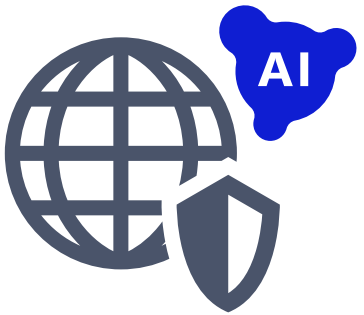


- 社内プロセスのアップデート
- 教育などの意識向上

パッチ適用を前提としたアーキテクチャ

- レガシー環境のクラウドへの移行
- パッチ適用ツールの導入

AIを活用したより高度な脆弱性管理



- 脆弱性の自動検証/自動修復
- 大量の脆弱性情報からのトリアージ

\Orchestrating a brighter world