Interop Tokyo 2026

NEC サプライチェーンセキュリティマネジメント for ネットワーク ご紹介資料

2026年6月

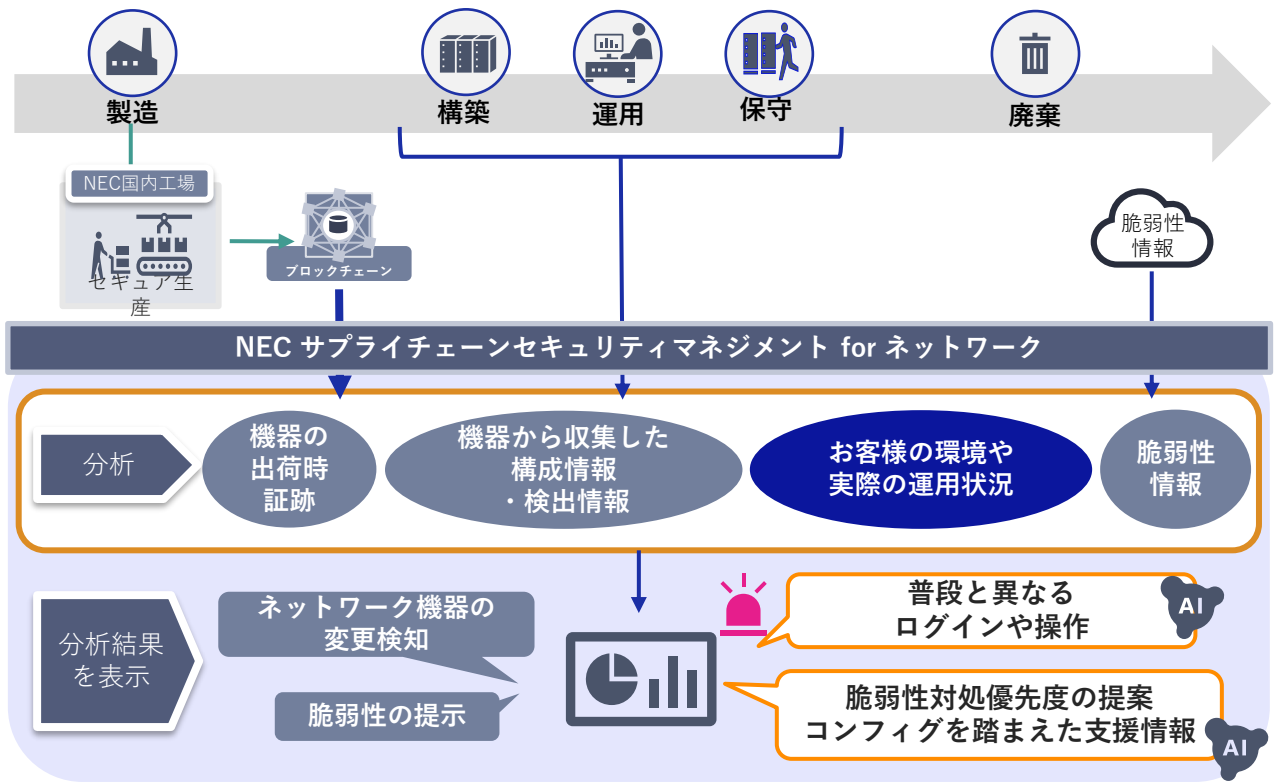
NEC デジタルネットワーク統括部

NEC \Orchestrating a brighter world

「NEC サプライチェーンセキュリティマネジメント for ネットワーク」

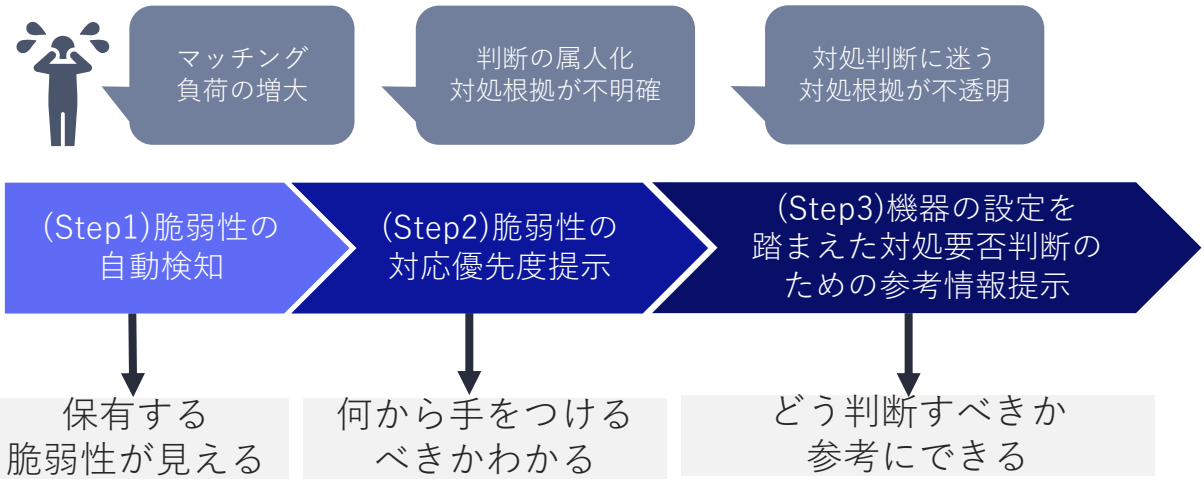
ネットワーク機器の真正性とセキュリティ情報を可視化
脆弱性の優先順位付けやコンフィグなど運用環境を踏まえた一歩先の情報提示でセキュアな機器管理を効率化

■ ご提供イメージ



装置識別名	製品名(ソフトウェア)	バージョン	脆弱性識別子	CVE ID	脆弱性情報	SSVC判定値	AI判定結果	影響度	CVSSスコア	CVSS環境値	CISA掲載	最終更新日時	除外	
FortiGate-60F-1	FortiGate-60F	7.4.5	FG-IR-26-060	CVE-2026-24858	An Authentication Bypass Usin..	至急対応..	対処不要	Critical	9.4	9.4	○	2026-05-12 12..	未	
FortiGate-60F-1	FortiGate-60F	7.4.5	FG-IR-25-647	CVE-2025-59718,C..	An improper verification of cry..	至急対応..	対処不要	Critical	9.1	9.1	○	2026-03-20 12..	未	
Cat9300	Cisco IOS XE Software	17.6.2	cisco-sa-20170629-snmp	CVE-2017-6736,CV..	SNMP Remote Code Execution ..	至急対応..	対処不要	High	8.8	8.4	○	2025-07-30 16..	未	
Cat9300	Cisco IOS XE Software	17.6.2	cisco-sa-snmp-x4LPhte	CVE-2025-20352	Cisco IOS and IOS XE Software ..	至急対応..	対処不要	High	7.7	7.7	○	2025-10-06 18..	未	
Cat9300	Cisco IOS XE Software	17.6.2	cisco-sa-20120328-pai	CVE-2012-0384	Cisco IOS Software Command ..	定期保守..	対処不要	Critical	9	NULL	-	2012-03-28 16..	未	

■ 本製品で実現する脆弱性対応のための3Step



脆弱性管理へのアプローチ

従来の課題

管理のブラックボックス化

- 機器の脆弱性把握や多様な情報の確認が手動では困難
- どれから対処すべきかの判断の属人化
- 対処判断に迷う、確認に時間がかかる

NECのアプローチ

脆弱性の自動検知と対応アシスト

脆弱性の自動検知：
資産に該当する脆弱性や悪用実績などの様々な情報源から自動でマッチング

脆弱性の対応優先度提示：
優先的に対処すべき脆弱性をお客さま環境を踏まえて提示

対応要否判断をアシスト：
生成AIを活用し、機器の設定を踏まえた対処要否の参考情報を提示

導入効果　**機器の脅威発見から対処優先度の仕分けを自動実行、対処方法をAIで提示(※)**

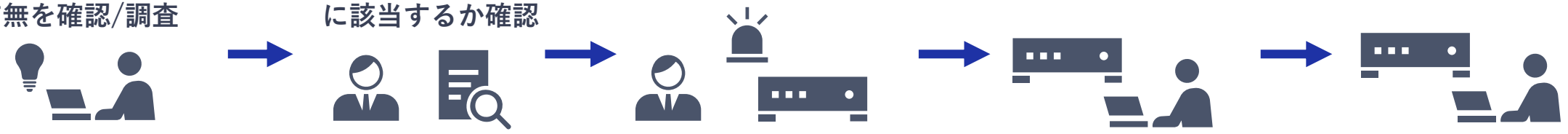
(※)最終的な判断および実施にあたっては、お客さまご自身で十分にご確認ください。

「NEC サプライチェーンセキュリティマネジメント for ネットワーク」脆弱性管理機能

お客様の保有するNW機器の脆弱性を自動で可視化、対処情報(※)を提示することで、セキュアな運用を効率的に行えるようにします。

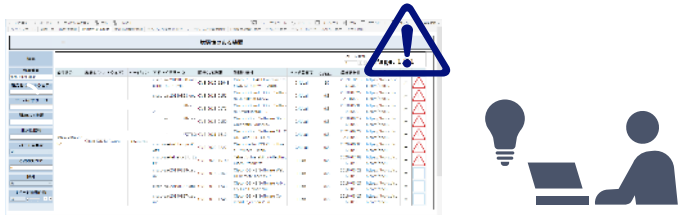
脆弱性情報収集と分析および通知 → 脆弱性対処

①定期的に脆弱性の有無を確認/調査 → ②自社のNW機器に該当するか確認 → ③該当する機器を特定 → ④対策検討 → ⑤対策実施

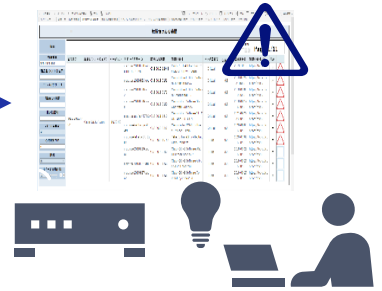


本製品導入による脆弱性対応フロー

①日次でSCSMが脆弱性情報を自動収集し、対象機器抽出、リスクスコア、悪用実績、対処優先度をダッシュボードに通知



②対策要否判断



③対策実施

対象機器への脆弱性 → 悪用実績、環境評価基準による精査 → 対応優先度(SSVC)精査 → コンフィグ＋LLM精査 → 設定変更or パッチ適用

対処すべき脆弱性の絞り込み/精査、対応要否フォロー

(※)最終的な判断および実施にあたっては、お客様ご自身で十分にご確認ください。

脆弱性対処の優先付け(SSVC)

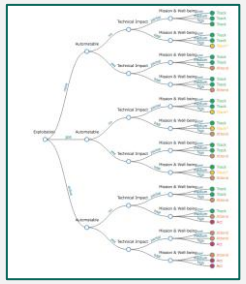
お客さま環境で対処すべき脆弱性を優先度別に自動分類し、
対処タイミングを行動指針として提示

◆ 機能概要

脆弱性情報
- CVSS基本値
- 脆弱性の悪用状況

装置の定義情報
- インターネット露出度
- システムの重要度(環境評価基準)

SSVC計算
入力データが決まれば
優先度のカテゴリは決まる



優先度のカテゴリ(表示)
- 至急対応
- 優先対応
- 定期保守
- 対応保留

SSVC：Stakeholder-Specific Vulnerability Categorization
2019年12月に米カーネギーメロン大学によって提案されたフレームワーク
Decision Treeに判断情報を入力することで対処の行動指針が示される

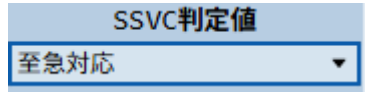
◆ 本機能で判定に用いる情報

- 脆弱性の悪用状況
- インターネット露出度
- CVSS基本値
- システムの重要度(環境評価基準)

◆ 画面イメージ

・行動指針

SSVC判定値で
優先度を確認

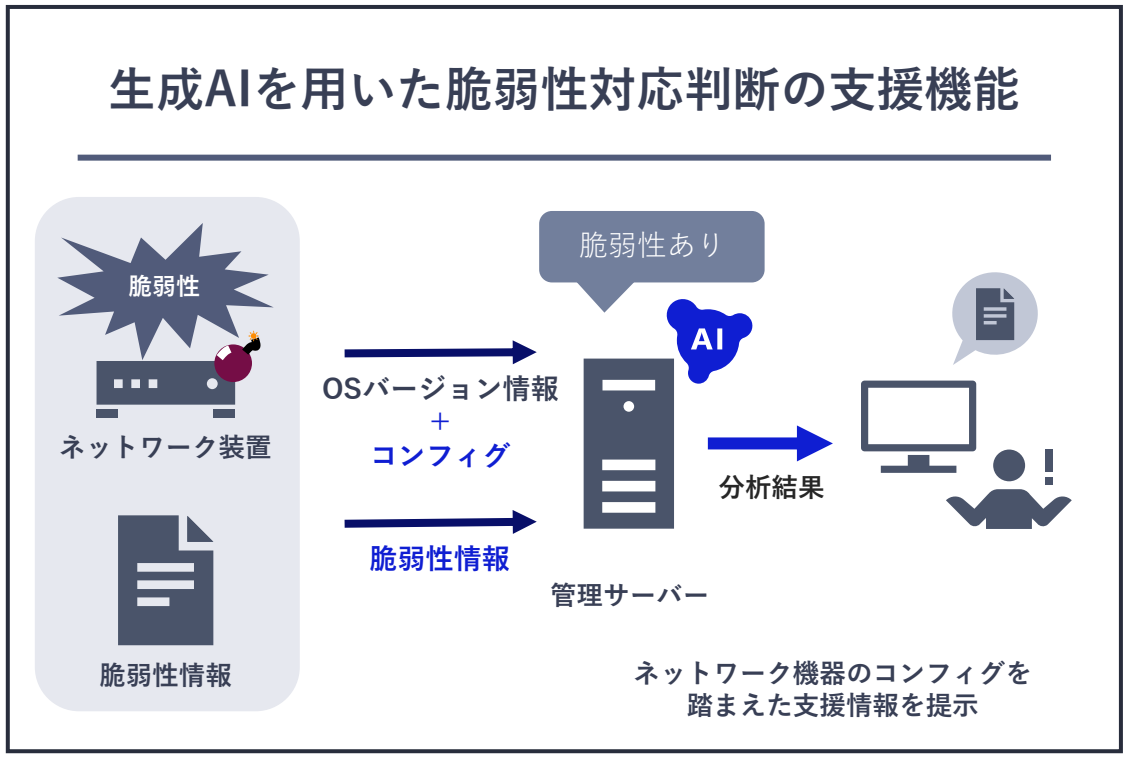


画面左のメニュー操作にて
優先度別の表示変更可能

・判断根拠

至急対応
脆弱性番号(CVE ID):CVE-2023-20198, 悪用実績あり, 外部露出大, 攻撃容易, 技術的影響度全面的, 業務影響度中
脆弱性番号(CVE ID):CVE-2023-20273, 悪用実績あり, 外部露出大, 攻撃困難, 技術的影響度全面的, 業務影響度中

生成AIを用いた脆弱性対応判断の支援機能



◆ 本機能で提示する情報

- 脆弱性の影響を受ける設定があるか
- 対応要否
- 推奨アクション
- 実機データの関連個所
- 攻撃手段
- パッチの有無
- 回避策　　…等

ラインナップ

NEC サプライチェーンセキュリティマネジメント for ネットワーク

提供形態	ソフトウェア版	サービス版
特長	✓ Closed環境にも適用可能	✓ クラウド環境の利用により手軽に始められる
構成イメージ		
ライセンス価格	管理対象機器100台の場合：年額70万円～ ※別途管理サーバー必要 ※必要台数に応じた詳細見積はご相談ください	管理対象機器100台の場合：年額350万円～ ※必要台数に応じた詳細見積はご相談ください
対応製品	ネットワーク機器：Cisco製品（一部除く）、UNIVERGE IXシリーズ、Fortinet　※今後対応製品拡大予定	

機能一覧

提供形態	ソフトウェア版(オンプレミス構成) サービス版(クラウド構成)

＊新規機能はソフトウェア版でも今後対応予定

機器の真正性 ※Ciscoのみ

- ✓ NEC国内工場出荷時の証跡情報を活用
  ※2022年にNECから出荷したCisco製品（Meraki除く）から順次対応開始、2023年６月以降は全数対応
- ✓ 登録機器の真正性を確認

低減されるリスク	不正な改造、すり替え

設定変更

- ✓ HW/コンフィグの変更状況を検出し差分表示

低減されるリスク	改ざん、ヒューマンエラー

イベント

- ✓ イベントを時系列で表示
- ✓ 操作履歴(機器で実行されたコマンドの一覧)を表示

低減されるリスク	改ざん、インシデント発生時のエビデンス不足

脆弱性

- ✓ 管理機器の脆弱性を自動検出
- ✓ リスクの高い脆弱性情報の抽出
- ✓ SSVC(注)フレームワークを用いた脆弱性の対応優先度表示
- ✓ 生成AIを用いた支援情報 New

低減されるリスク	脆弱性放置

(注)SSVC：Stakeholder-Specific Vulnerability Categorization
2019年12月に米カーネギーメロン大学によって提案されたフレームワーク。Decision Treeに判断情報を入力することで意思決定が示される。

ポリシーチェック

- ✓ 設定すべき情報(ポリシー)が遵守されていない機器を検出しアラート発報

低減されるリスク	リスク放置

ログイン

- ✓ ログイン履歴の表示
  (成功/失敗、いつ、誰が)
- ✓ 計画外ログインに対するアラート発報
- ✓ 「普段と異なる」リスクの高いログインを検知

低減されるリスク	改ざん

※低減されるリスクは一例。

製品関連情報のご案内

BluStellar

■ 各種URLのご案内

- 公式HP
  https://jpn.nec.com/scrm/

- プレスリリース（2026年6月4日）New
  https://jpn.nec.com/scrm/press/20260604.html

- お問い合わせ
  NEC サプライチェーンセキュリティマネジメント for ネットワーク
  お問い合わせ窓口
  E-mail：　scrm-ss@dnw.jp.nec.com

■ 試験導入（価値検証）の募集

- 試験的に「NEC サプライチェーンセキュリティマネジメント for ネットワーク」を導入いただき、価値検証を実施させていただけるお客様を募集中です。
  詳細はお問い合わせください。

\Orchestrating a brighter world