NEC \Orchestrating a brighter world

ネットワーク機器のライフサイクル全体を通じた真正性とセキュリティ情報可視化

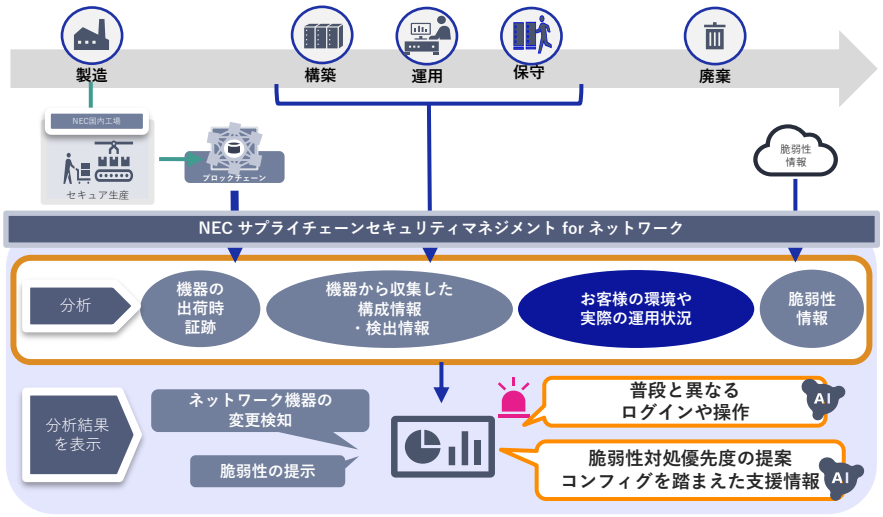
NEC サプライチェーンセキュリティマネジメント for ネットワーク

ネットワーク機器に発生する変更をセキュリティ視点でとらえ、
機器の真正性や管理に必要な情報を分析・可視化するソフトウェア製品

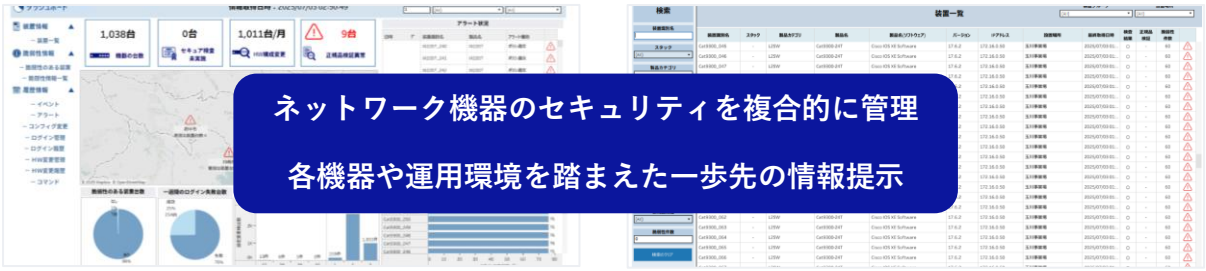
「NEC サプライチェーンセキュリティマネジメント for ネットワーク」とは？

■ ネットワーク機器のシステムライフサイクル上(出荷～運用時）にあるセキュリティリスクを可視化
⇒ **装置の変更が意図したものであるかセキュリティ観点で確認すること**でセキュアな運用を実現！

- ✓ **出荷から運用まで、機器の真正性を検査し続ける**
- ✓ **AI機能で“いつもと違う”リスクに気づく・脆弱性に対するNextアクションがわかる**



➢ 主な機能



ネットワーク機器のセキュリティを複合的に管理

各機器や運用環境を踏まえた一歩先の情報提示

機器の真正性

- ✓NEC国内工場出荷時の証跡情報を活用
  ※2023年6月以降(2022年より順次対応)に
  NECから出荷したCisco製品(Meraki除く)のみ
- ✓登録機器の真正性確認

設定変更

- ✓HW/コンフィグの変更状況を検出・表示
- ✓セキュリティポリシー未遵守の機器を検出

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

**ログデータをもとに運用者の行動を学習・分析
異常なログインや操作を検知しアラートを発報** AI

脆弱性

- ✓SSVC※2フレームワークを用いた対応優先度表示
- ✓生成AIを用いた対応判断のための支援情報提示

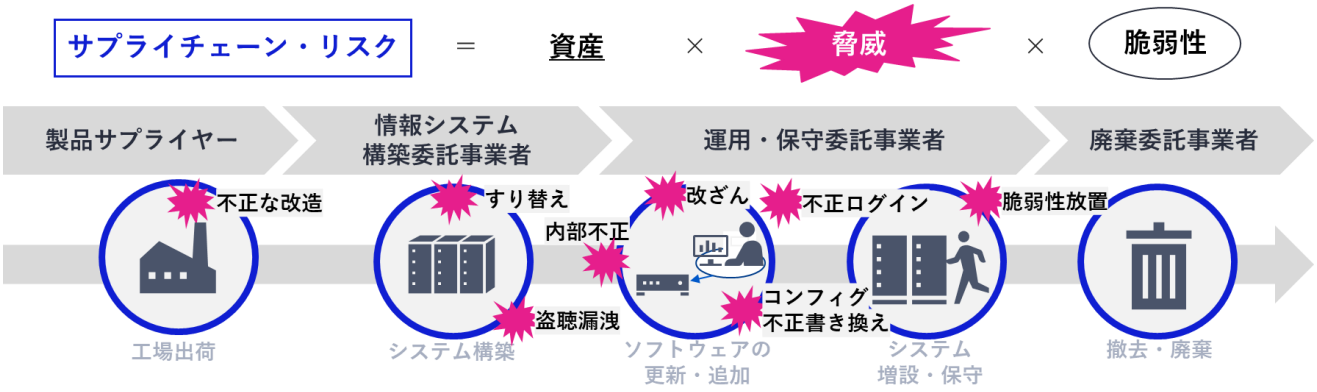
**機器のコンフィグを踏まえた脆弱性対処要否や
Nextアクションなど、対処支援情報を提示** AI

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

経済安全保障上のリスクの高まりやサイバー攻撃の激化・巧妙化に伴い、セキュリティ対応やガバナンスの強化・迅速化が求められています。本製品ではお客さま環境も踏まえた情報分析と可視化を行い、負荷の削減と判断のばらつきを防止。セキュリティの水準を一定に保つ管理に貢献します。

サプライチェーンに潜む製品のセキュリティリスク

■ **製品のライフサイクル全般がリスクの対象です。**
IPA情報セキュリティ10大脅威(※3)へのランクイン、政府統一基準群での記載、
基幹インフラ役務の安定的な提供の確保に関する制度(※4)など、
セキュリティへの関心の高まりとともに、サプライチェーン保護やリスク管理が課題となっています。



システム構成

■ 本製品は下記の構成を選択可能です。詳細はお問い合わせください。

(※1)「政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）」-内閣サイバーセキュリティセンター
https://www.cyber.go.jp/policy/group/general/kijun.html
(※2) SSVC (Stakeholder-Specific Vulnerability Categorization)
(※3)「情報セキュリティ10大脅威 2026」組織部門-情報処理推進機構
https://www.ipa.go.jp/security/10threats/10threats2026.html
(※4)「基幹インフラ役務の安定的な提供の確保に関する制度」-内閣府
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html

NEC　プラットフォーム・テクノロジーサービス事業部門
〒211-8666　神奈川県川崎市中原区下沼部1753 NEC Innovation Park
E-mail: scrm-ss@dnw.jp.nec.com

「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」
製品サイトはこちら
https://jpn.nec.com/scrm/

製品サイトリンク
(QRコード)

2026年6月現在　Ver 6.0