OKI Open up your dreams

インターネットに繋げていなければ安全？
閉域網をリアルタイム監視するネットワークエッジ・セキュリティ

沖電気工業株式会社
技術本部　先行開発センター　モビリティIoT先行開発部
チームマネージャー
八百 健嗣

目次

◆背景

◆OKIの提案
  ◆リアルタイムネットワーク監視

◆監視GUIを用いた異常事象の確認(デモ)

◆利用例

◆今後の展開

ネットワークエッジ領域でのセキュリティ課題

■設定や管理に不備があるIoT機器を経由した内部ネットワークへの侵入事例が登場

■特に十分なセキュリティ対策を適用できないエッジ領域のNW/機器のセキュリティ対策が課題

【セキュリティインシデントの事例】

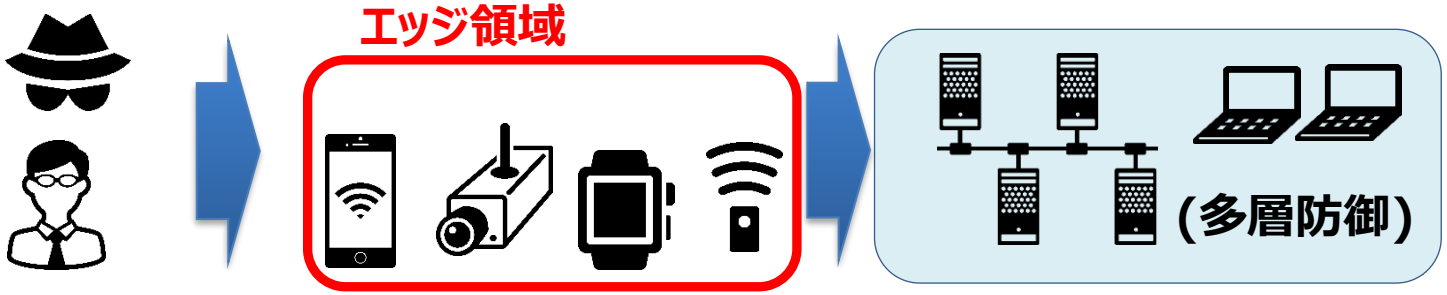
■ **NASAサイバー攻撃で機密データ流出**
侵入口は無許可接続の「Raspberry Pi」(2019)

■ 国内の**公立病院**で**電子カルテ**が暗号化され**閲覧不可**
VPN機器を経由しネットワークに侵入したと想定されている(2021)

【ネットワークエッジ領域のセキュリティ脅威】

従来の汎用的なICT機器とは異なるIoTデバイス

突然、内部ネットワークに「攻撃者」が出現



外部・内部犯行者

様々なデバイスの不正持込み、不正なワイヤレス接続

組織のネットワーク

実際にどんな機器がつながっているのか把握しきれない

セキュリティ対策に不安があるが**どう運用したらよいか**わからない

閉域網※におけるセキュリティインシデント事例

※閉域網：インターネット非接続環境

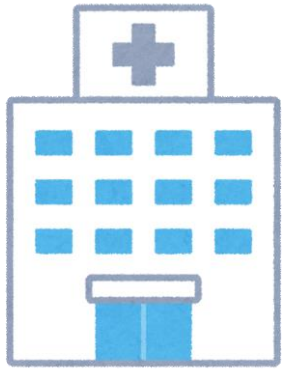
■工場の設備系NWのような閉域網でもサイバー攻撃被害が増加

■一時的なインターネットへの接続やUSBメモリ経由でマルウェアに感染してしまうケース、重要拠点を狙った巧妙な攻撃により不正侵入を許してしまうケースが存在

事例１：某医療機関

Windows端末を
一時的にインターネットに接続
リモートデスクトップ経由でランサムウェアに感染
⇒業務停止に陥ってしまった

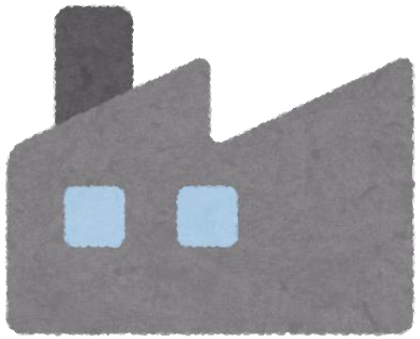
引用：https://www.ccsnet.co.jp/blog/security/021500286.html



事例２：某製造業

インターネット環境で使用する
USBメモリを閉域網に接続し
マルウェアに感染
⇒生産設備の停止に追い込まれた

引用：https://www.ccsnet.co.jp/blog/security/021500286.html



事例３：ウクライナ電力会社

情報系NWのPCを乗っ取り
6か月にわたるモニタリングの後に
閉域網の電力制御システムを遠隔操作
⇒停電を発生させた

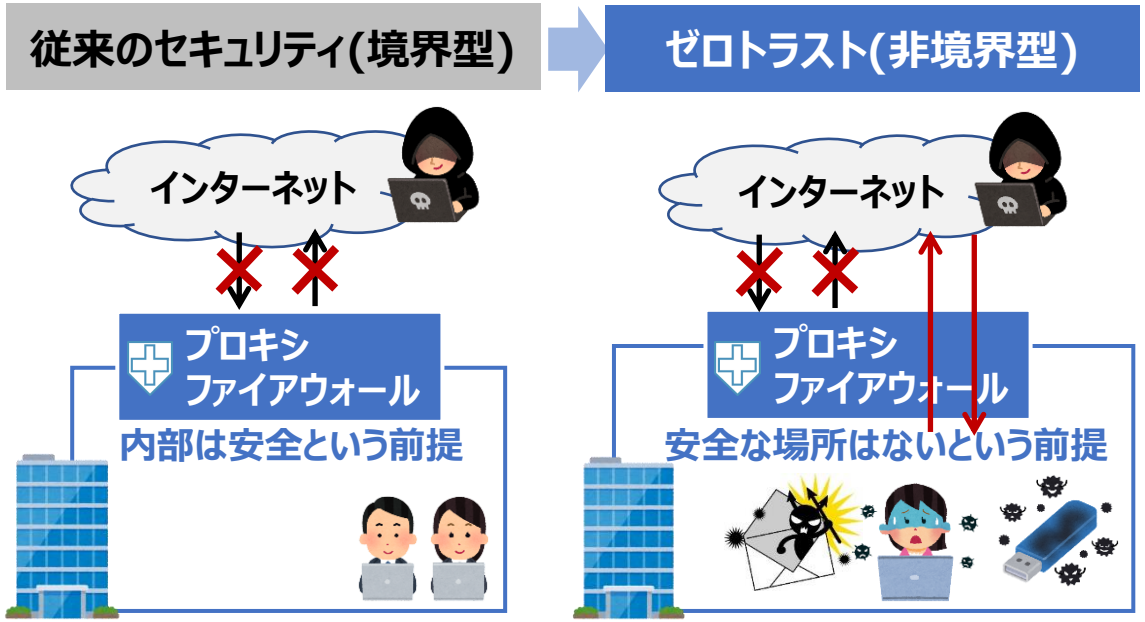
引用：https://xtech.nikkei.com/dm/atcl/column/15/425482/080800285/

サイバーセキュリティに関する動向

■標的型攻撃等によるNW内部の感染により、セキュリティ監視は境界型から非境界型へと拡大

■AI技術の活用等による攻撃検知および対処の自動化・効率化への期待が高い

【セキュリティ監視対象の拡大】

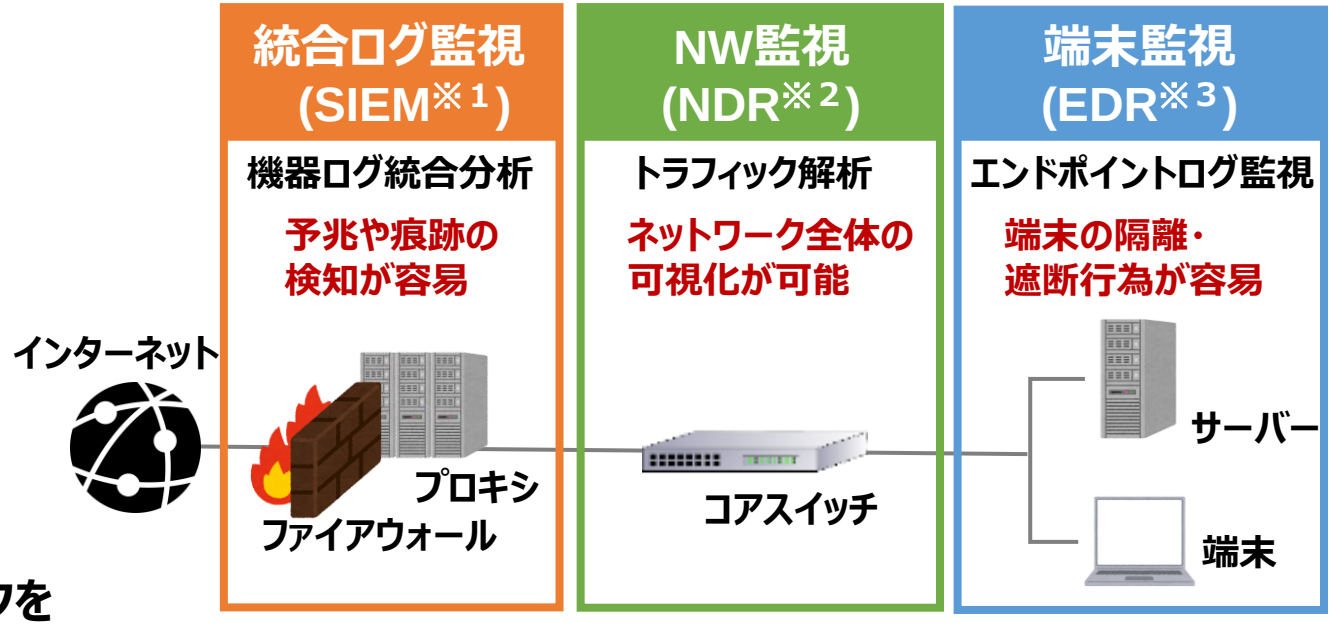


従来は境界となる出入口を重点的に監視していた

今後は端末や内部ネットワークを監視する必要性に迫られている

【セキュリティ対策製品のトレンド】

AI技術も活用し、各ポイントで怪しい挙動を監視



※1 SIEM(:Security Information and Event Management)
※2 NDR(:Network Detection and Response)
※3 EDR(:Endpoint Detection and Response)

OKI Open up your dreams

OKIの提案：リアルタイムネットワーク監視

OKIのリアルタイムネットワーク監視システム

■OKIは、エッジ分析装置をネットワークスイッチにつなぐだけでネットワークエッジ領域の機器を常駐ソフトを搭載することなく監視するシステムを開発

エッジ分析装置に、機器の通信パターンを分析するAI処理機能と脆弱性を検知する機能を搭載し、エッジ領域のNW/機器をリアルタイムで監視することで、不審な通信や脆弱性を持った機器を早期に検知・遮断

システム機能

■監視対象ネットワークに設置することで、そのネットワークにつながる機器と異常を可視化

■１台のエッジ分析装置に各種エンジンと監視GUIが搭載されており、装置単体で動作可能

既に稼働中のNWに対しても後付けでつなぐだけの簡単設置

ネットワークスイッチ

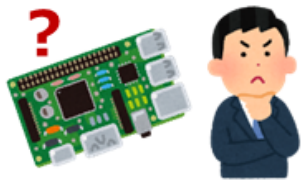
エッジ分析装置

ネットワークスイッチを流れるトラフィックを取得(通信ミラーリング)

トラフィックキャプチャ

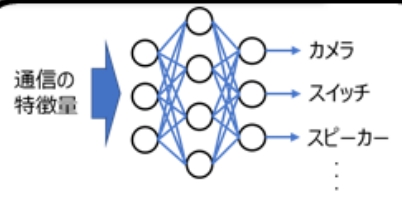
監視NWを流れるトラフィックをキャプチャ

新規端末検知



新たに接続された機器を検知

機器種別判定



ヘッダ情報を特徴量として機械学習で機器種別を判定

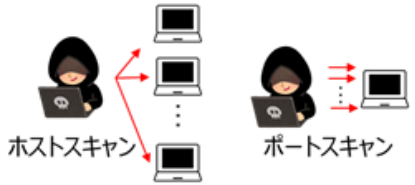
脆弱性スキャン

機器にスキャンをかけ潜在的脆弱性を検知

レア通信検知

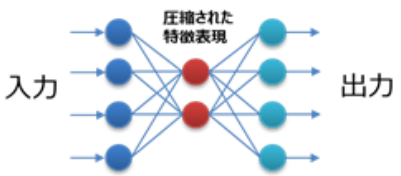
機器が普段と異なる通信先にアクセスしたことを検知

スキャン通信検知



不正侵入後のNW内の探索通信を検知

通信非定常検知



機器の定常通信パターンを学習し外れ値検知

監視GUI

検知状況を確認し、通信先/サービス、通信量等を調査

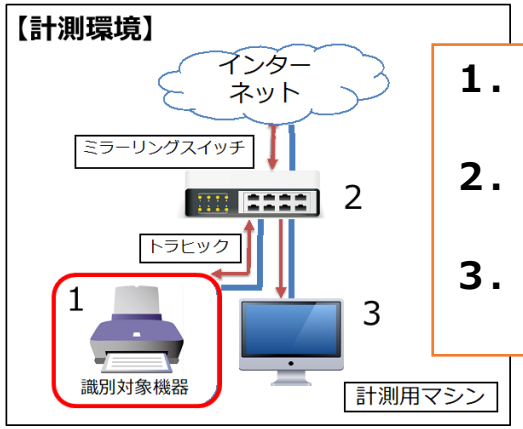
機器種別判定技術（大阪公立大学との共同研究）

■通信トラフィック分析技術
- IP通信機器のトラフィックをパッシブに観測・分析し、通信機器の状態を推定する技術（地の利を活かした長年の共同研究）

■IoTセキュリティ監視への応用：接続機器の種別推定
- IoT機器は通信パターンに規則性があるものが多い
- 通信トラフィック分析によりIoT機器の接続や異常な通信挙動をいち早く検知
  - 管理下にないIoT機器の接続
  - なりすましやマルウェア感染によって引き起こされる異常な通信挙動

■大規模キャンパスネットワークを活用した研究開発
- 大阪公立大学 杉本キャンパスにて取得した、IoT機器を含む多種多様な通信機器のトラフィックデータを学習(計9種別、47機種)
- 2023年1月の実証実験において、**IoT機器の接続を即座に識別**できることを確認（1分経過時点で97.7%の識別精度）

【通信トラフィック分析技術】

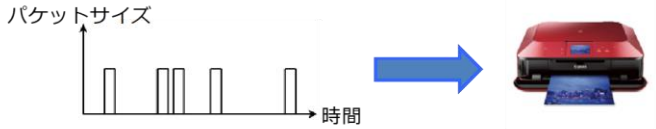


1．分析対象機器をネットワークに接続
2．集約スイッチで通信をミラーリング
3．計測用マシンでミラーリング通信を分析

機器の状態に応じて、そのトラフィックの特徴量に違いが出る

【IoTセキュリティ監視への応用】

データ受信があったときのみ送る → プリンタ

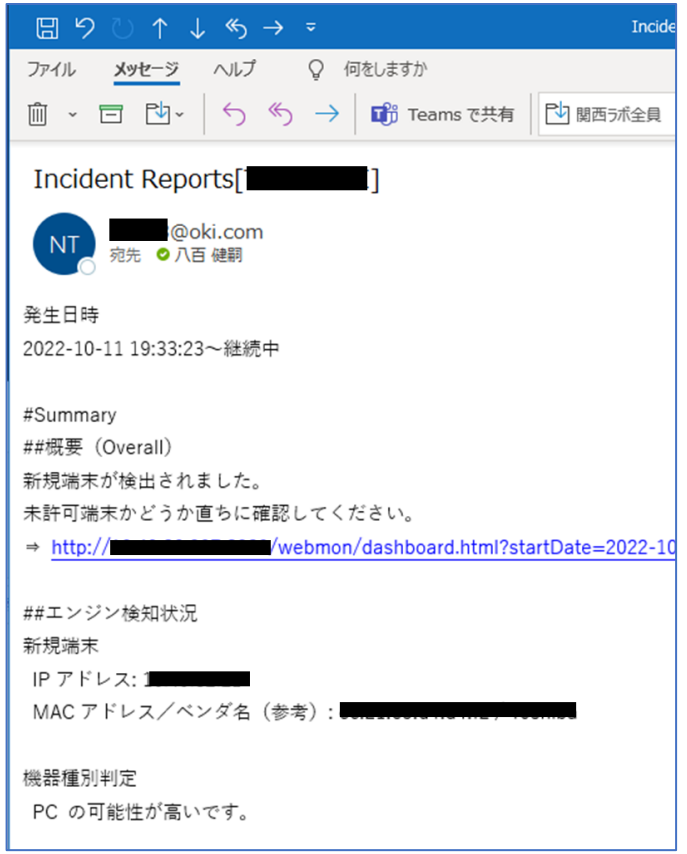


細かく短い間隔で送る → ネットワークカメラ

監視結果の通知と確認

■メイン画面の他に週次レポートやメール通知等、運用監視を支援する基本的な機能を搭載

【メールでのイベント通知】



OKI Open up your dreams

監視GUIを用いた異常事象の確認(デモ)

OKI Open up your dreams

利用例

利用例①　情報NW責任者の皆様　資産を可視化できます！

■自部署のネットワーク接続機器の管理を徹底したいが把握・管理しきれない情報ネットワーク責任者に対して、ネットワーク内に存在する機器や異常を可視化する機能を提供

想定課題

資産を見える化できていない

対策

流れるトラフィック情報からNWに存在する機器を可視化すると共に、確認が必要な機器を通知

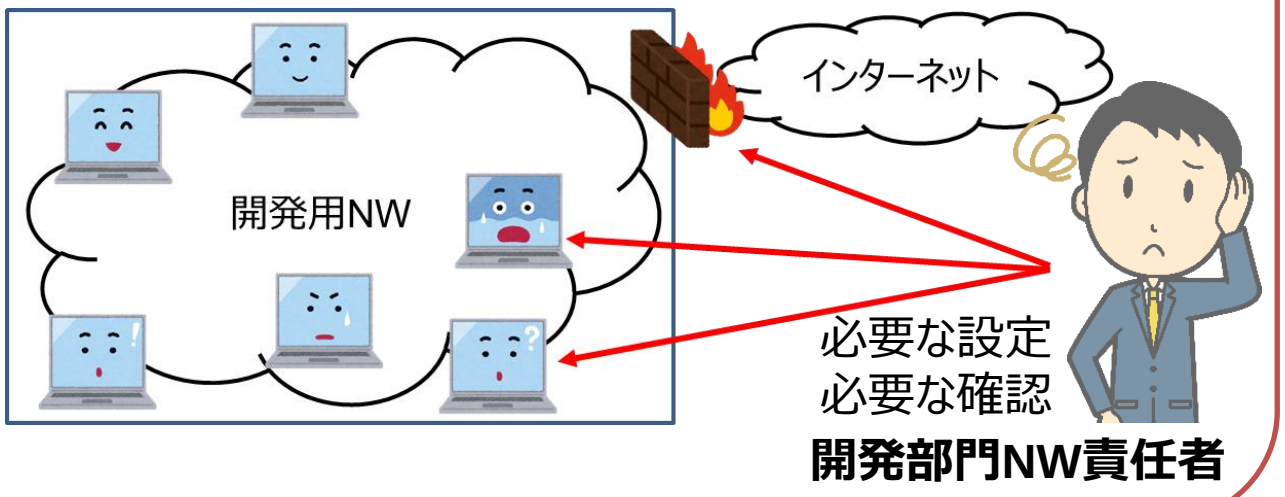
「資産を見える化し、管理者が不明な機器等を特定したい」
「最近ではカメラや小型の組込み機器等の接続も増えており、実際にどんな機器がつながっているか把握しきれていない」
「大規模システムの導入等、ネットワーク管理に手間もコストをかけれない」

利用例②　開発部門NW責任者の皆様　自部門の脆弱性を検査できます！

■実証や開発のために自部門拠点内でネットワークを運用する開発部門ネットワーク責任者に対して、機器の設定やネットワークのアクセス設定に不備がないかを検査する機能を提供

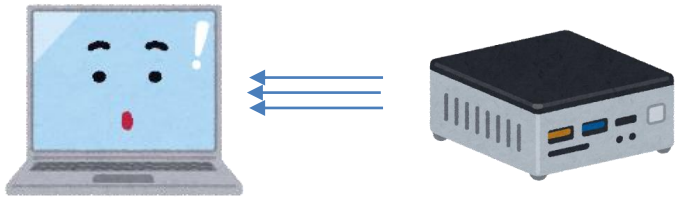
想定課題

脆弱な機器や侵入経路が顕在化していない



対策

ポートスキャン
パスワードチェック



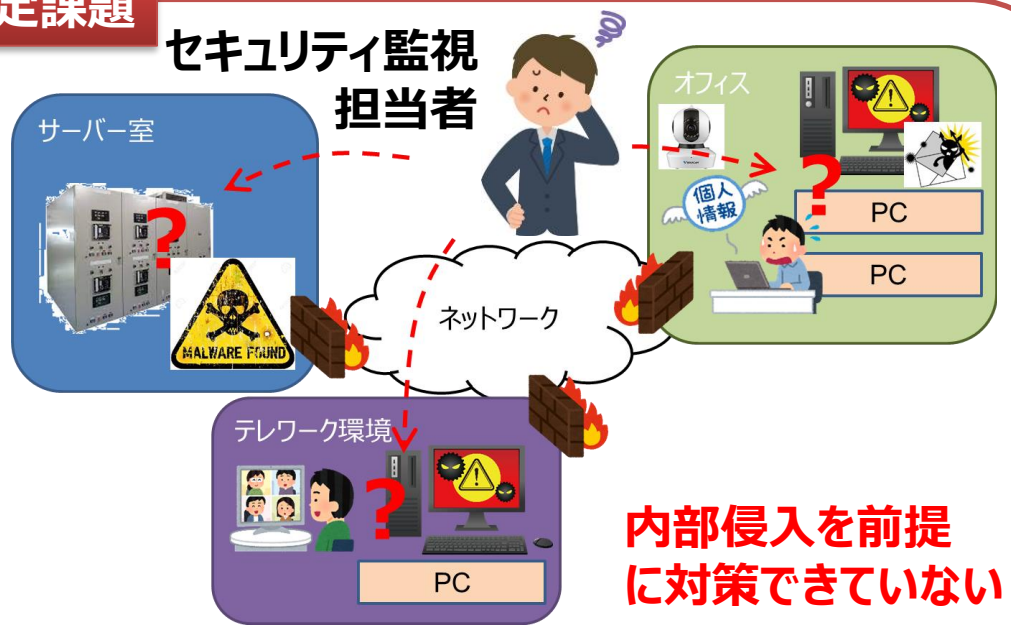
NW内の機器をスキャンし、
不要な空ポートやパスワード設定、
FW設定に不備がないかを検査

「FW設定などセキュリティ対策のための設定がちゃんと機能しているかみえない」
「顕在化していない脆弱な機器や侵入経路がないか気になる」
「セキュリティ対策は必要最低限の範囲/機能のみでできるだけコストを下げたい」

利用例③　セキュリティ監視担当者の皆様　各拠点内部を監視できます！

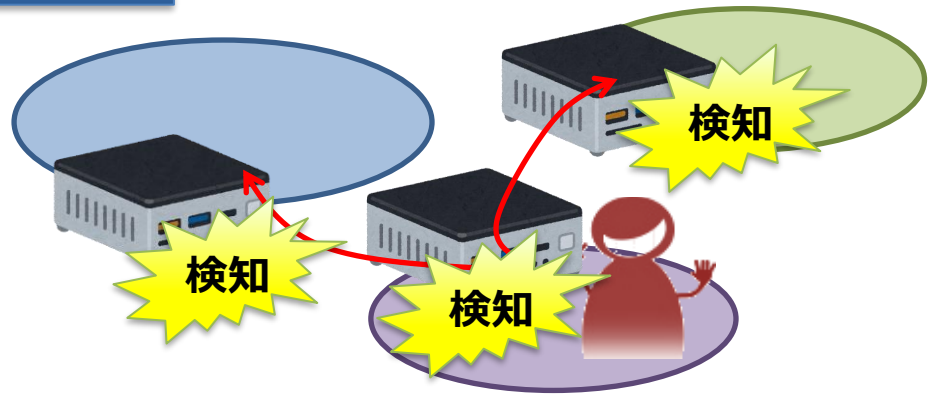
■攻撃の予兆を早期に掴み、セキュリティインシデントの発生を未然に防止したセキュリティ監視担当者に対して、平常時とは異なる怪しいトラフィックを検知する機能を提供

想定課題



内部侵入を前提に対策できていない

対策



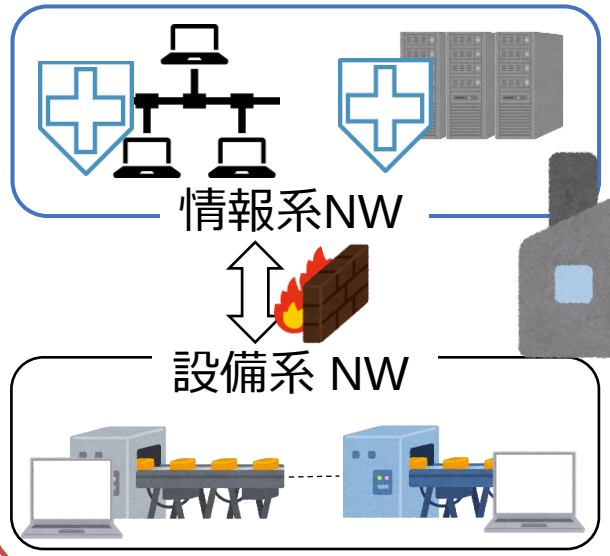
各拠点内部トラフィックを分析し、
偵察等のマルウェア感染活動を検知、
情報漏洩につながる異常なトラフィックを検知

「出入口対策はできているが、内部侵入を前提とした対策が実現できていない」
「高価なセキュリティ対策製品を導入しても、アラート通知が膨大であり、スキル及び工数的に運用を回すことができていない」
「まだ見ぬ脅威に大規模な予算を確保できない」

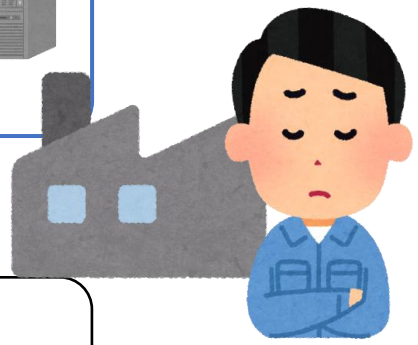
利用例④　工場NW管理責任者の皆様　生産現場を監視できます！

■既設の生産設備やネットワークに影響を与えることなくセキュリティ監視を強化したい工場内ネットワーク管理責任者に対して、管理外機器の接続や通常と異なる通信を検知する機能を提供

想定課題



工場NW管理責任者



設備系NWのセキュリティ対策が不十分

対策

工場内NWへの想定外の機器接続を検知、
生産設備の普段と異なる異常な通信を検知

「情報系NWと設備系NWの境界ではセキュリティ対策しているが、設備系NW内部の通信のセキュリティ対策ができていない」
「セキュリティ対策が十分でない機器があるが、常駐型ソフトの搭載やセキュリティパッチを常に最新の状況に保っておくのは困難」

OKI社内工場のネットワーク監視

■国内２拠点の生産エリアネットワークに監視装置を設置し、接続機器を可視化すると共に異常な通信がないかをリアルタイム監視

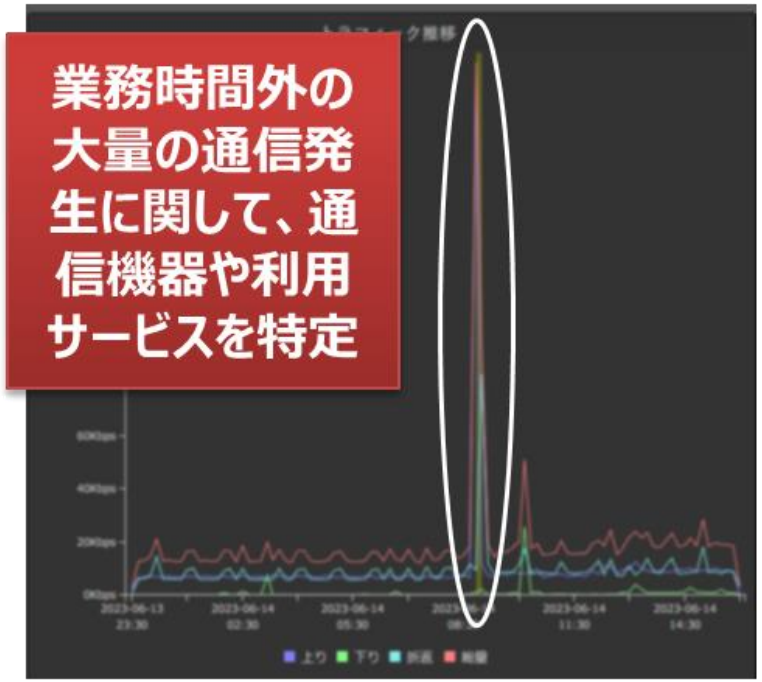
⇒　管理者が把握しきれない**現場レベルでのイベントを通知・警告可能**となった

【生産エリアNWへの接続】

【生産設備(例)】

【新規機器の接続】

【想定外の通信挙動】



OKI Open up your dreams

今後の展開

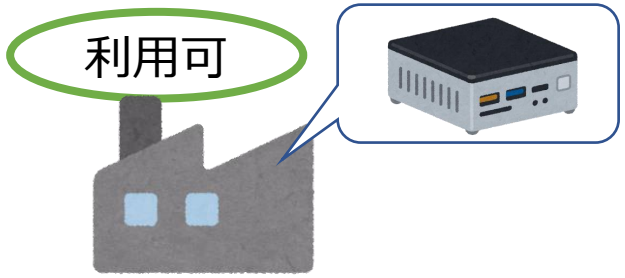
今後の展開

■現在、すでにお客様に提供可能な検証機が準備できており、**実証実験のパートナーを募集中**

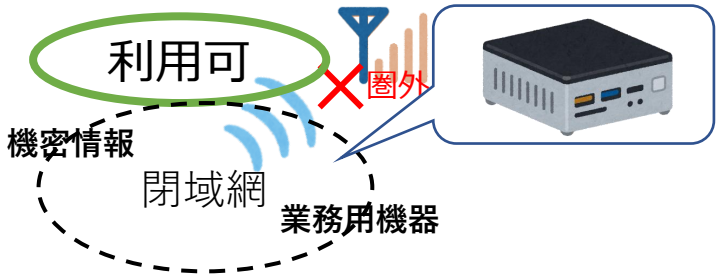
■ネットワークエッジ領域におけるセキュリティ課題に対処すべく、**OKIのリアルタイムネットワーク監視システムを試してみませんか？**

■今後、お客様環境での実証事例を増やし、早期の商品化を目指します。

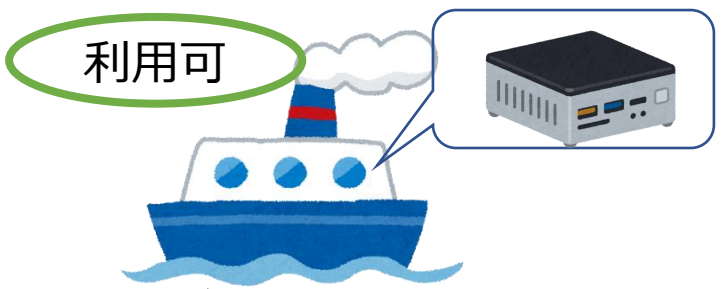
小型かつ単体で動作し、あらゆる拠点に追加整備可能



生産現場(国内拠点・海外拠点)



インターネット非接続NW



その他、船舶や野外拠点のNW


OKI Open up your dreams
ご清聴ありがとうございました
OKIグループフェア in KANSAI 2023
社会の大丈夫をつくっていく。
OKIと共に持続可能な未来へ