OKI Open up your dreams

CIAJトラフィックデータ活用サミット2025

エッジNW監視装置による不正侵入検知

2025年2月28日

沖電気工業株式会社

ネットワークエッジ領域でのセキュリティ課題

OKI
Open up your dreams

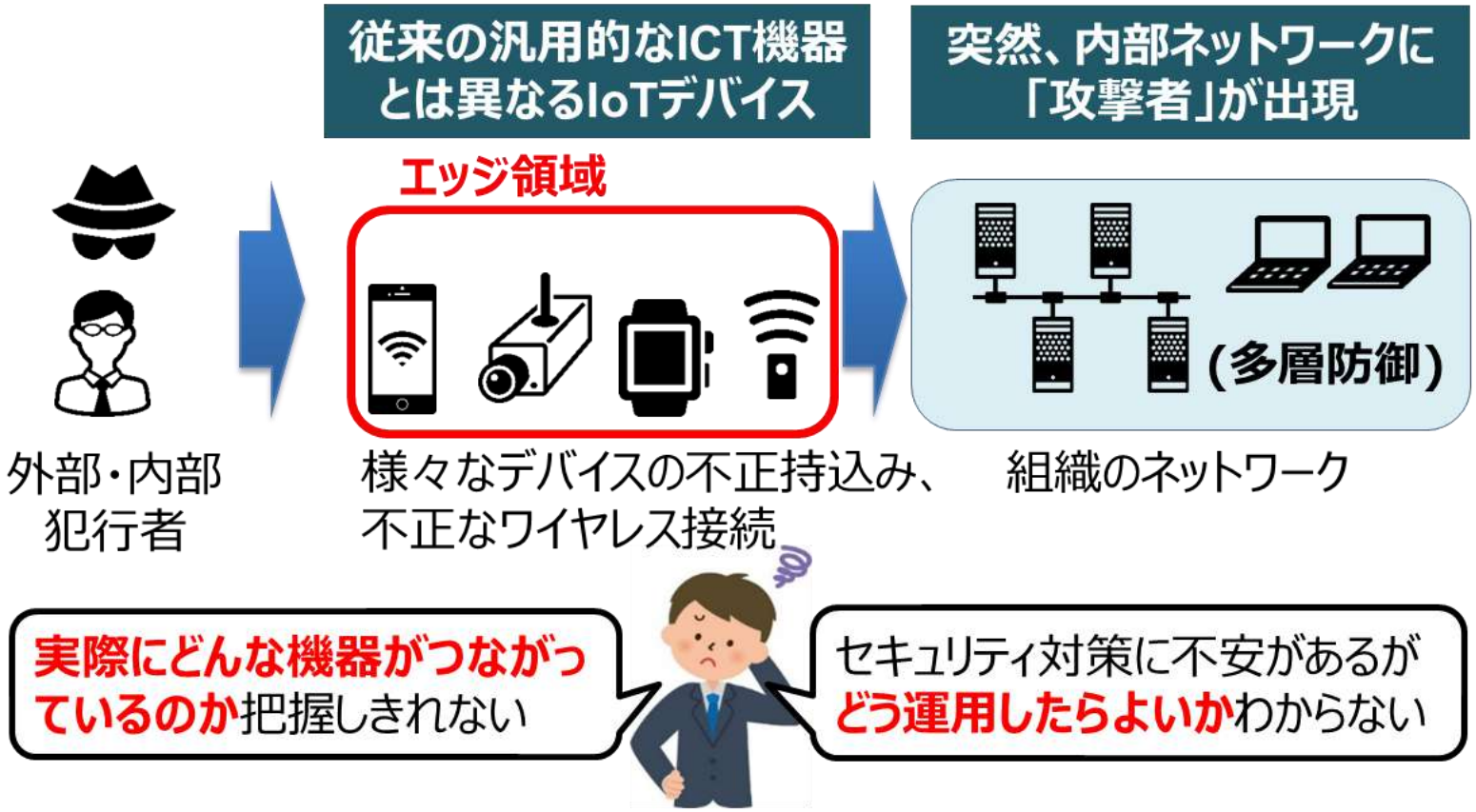
■ 設定や管理に不備があるIoT機器を経由した内部ネットワークへの侵入事例が増加
■ 特に十分なセキュリティ対策を適用できないエッジ領域のNW/機器のセキュリティ対策が課題

【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】

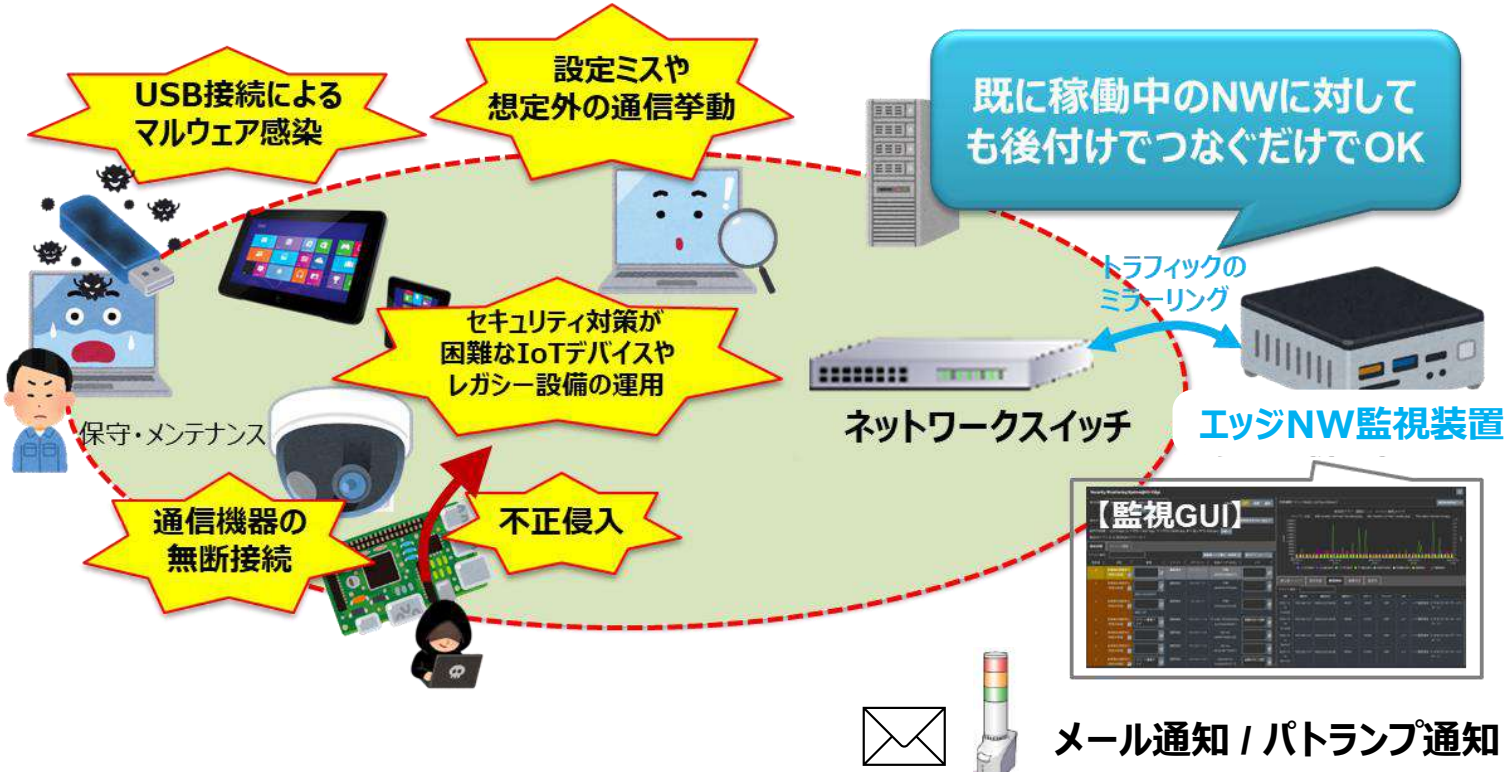


エッジNW監視装置　～コンセプト～

OKI
Open up your dreams

■ 既設のネットワークスイッチに**簡単つなぐだけ**でNWをリアルタイム監視
■ 機器側にソフトを入れるのではなく、**置いておくだけで安心**を提供

既設のネットワークスイッチに簡単つなぐだけで守ります
閉域ネットワークのリスクを洗い出し対処する優秀なネットワーク監視AI



IT機器の可視化	管理者が不明なNW接続機器も通信の実態から確実に把握・管理
未許可機器の隔離	資産管理リストにない未承認機器の接続を自動で遮断し報告
不正侵入検知	通信のリアルタイム分析によりNWへの不正侵入をいち早く検知
脆弱機器の発見	NWへの侵入口となり得る機器の設定不備を発見
通信ログの記録	有事の際、調査のために重要となる通信ログを記録、出力可能

システム機能一覧

OKI
Open up your dreams

■ 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**
■ ベース機能とオプション機能を用意（柔軟にカスタマイズ可能）

★ 本日ご説明

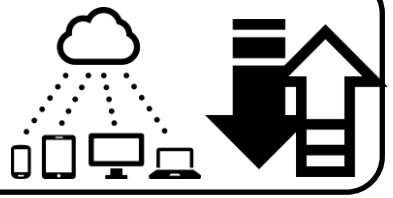
既に稼働中の
NWに対しても
後付けでつなぐ
だけの簡単設置

ネットワークスイッチ

エッジ分析装置

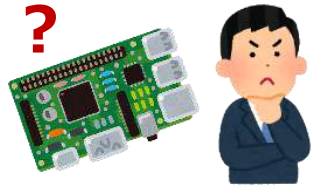
ネットワークスイッチを流れる
トラフィックを監視
(通信ミラーリング)

トラフィックキャプチャ



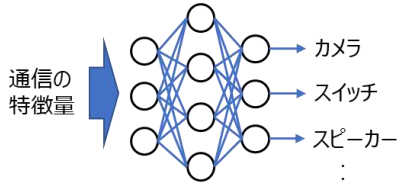
監視NWを流れる
トラフィックをキャプチャ

新規端末検知



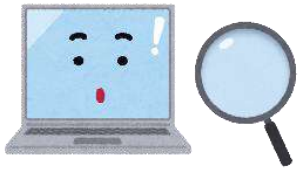
新たに接続された機器
を検知

★ 機器種別判定



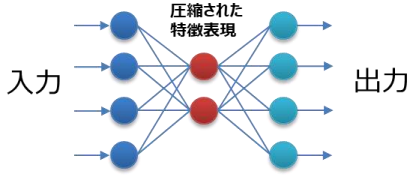
ヘッダ情報を特徴量として
機械学習で機器種別を判定

アクティブスキャン



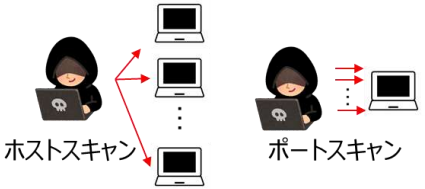
機器にスキャンをかけ
潜在的脆弱性を検知

★ 通信非定常検知



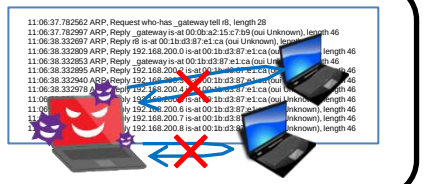
機器の定常通信パターン
を学習し外れ値検知

★ スキャン通信検知



不正侵入後のNW内の
探索通信を検知

通信遮断



異常検知された機器の
通信を妨害し遮断

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　～トラフィックフロー分析技術～

OKI
Open up your dreams

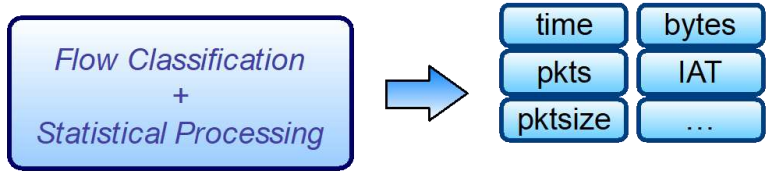
■ IPパケットのペイロードをみることなく、ヘッダー情報のみで、通信機器の種別を推定

- トラフィックフロー分析技術に関する共同研究を実施（**大阪公立大学**）
  - 暗号トラフィックのアプリケーション推定
  - 接続機器の自動識別とネットワーク制御（ネットワークスライシング、分離）

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

観測した通信パケットをフローに分割

フロー単位で統計量を算出

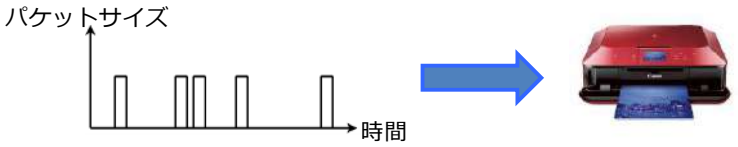


フローとは、セッションのイメージ
送受信IP、ポート番号が同じひとまとまりの通信

- セキュリティ監視への応用：IoT機器の種別判定

IoT機器は通信パターンに規則性があるものが多い
機器種別ごとの通信パターンを学習させて機器を推定

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

通信フロー単位で特徴量を算出し機器種別を判定

【特徴量(例)】

特徴量名	説明
sum_pc	パケット数
sum_pktlen	パケットサイズの合計
max_pktlen	パケットサイズの最大値
min_pktlen	パケットサイズの最小値
mean_pktlen	パケットサイズの平均値
median_pktlen	パケットサイズの中央値
mode_pktlen	パケットサイズの最頻値
stdev_pktlen	パケットサイズの標準偏差
unique_pktlen	パケットサイズの一意な値の数
sum_iat	パケット間隔の合計
max_iat	パケット間隔の最大値
min_iat	パケット間隔の最小値
mean_iat	パケット間隔の平均値
median_iat	パケット間隔の中央値
mode_iat	パケット間隔の最頻値
stdev_iat	パケット間隔の標準偏差
unique_iat	パケット間隔の一意な値の数

キャンパスネットワークを用いた実験(2023年1月)

- 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)

⇒ IoT機器の接続を**97.7%の精度**で識別

・新規機器接続時の付加情報として通知
・IoT機器種別に応じたセキュリティ検査を実施

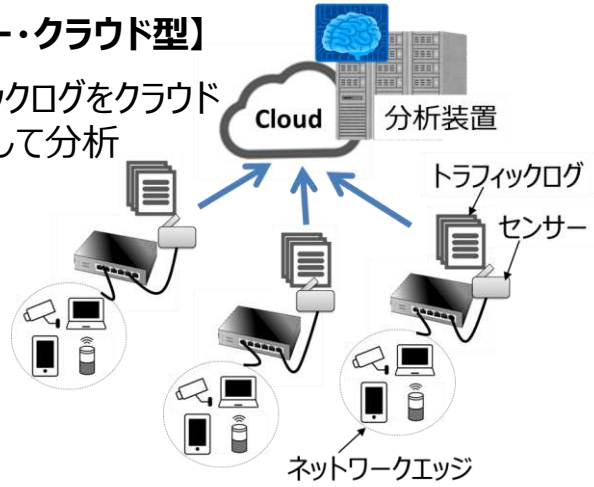
通信非定常検知　～軽量エッジ分析による異常検知～

OKI
Open up your dreams

■ エッジに配備する分析装置でネットワークに閉じて異常検知することで**リアルタイム性**を確保

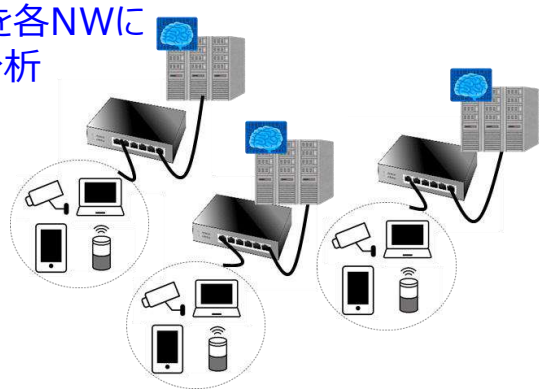
【センサー・クラウド型】

トラフィックログをクラウドに送信して分析



【エッジ分析型】

分析装置を各NWに配備して分析

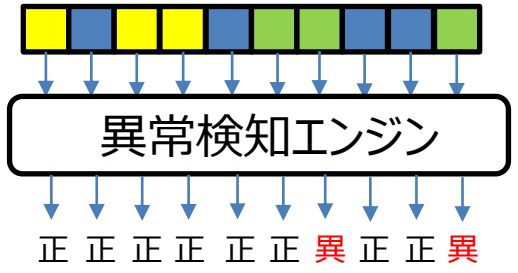


- 各ネットワークに閉じて分析することで**リアルタイム性**の高い異常検知を実現
- 各ネットワークに分析装置を配備することになるため計算資源の限られた装置でも動作可能な**軽量**な方式を検討

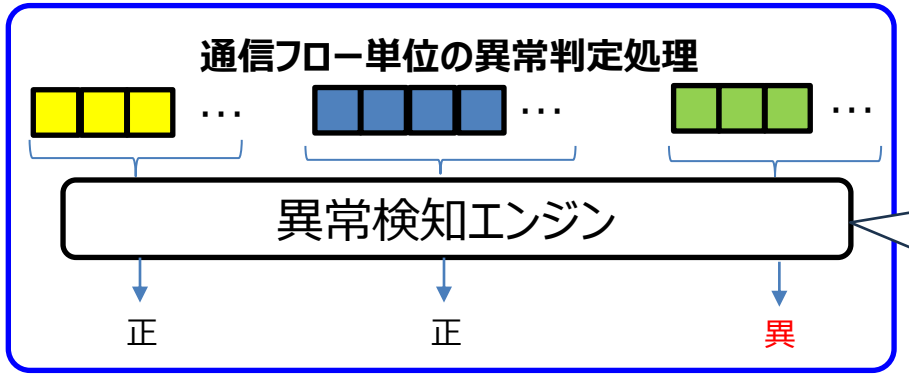
課題：
各パケットに対して異常判定処理が発生

対策：
通信フロー単位で異常判定
先頭数パケットだけを用いることで即座に判定

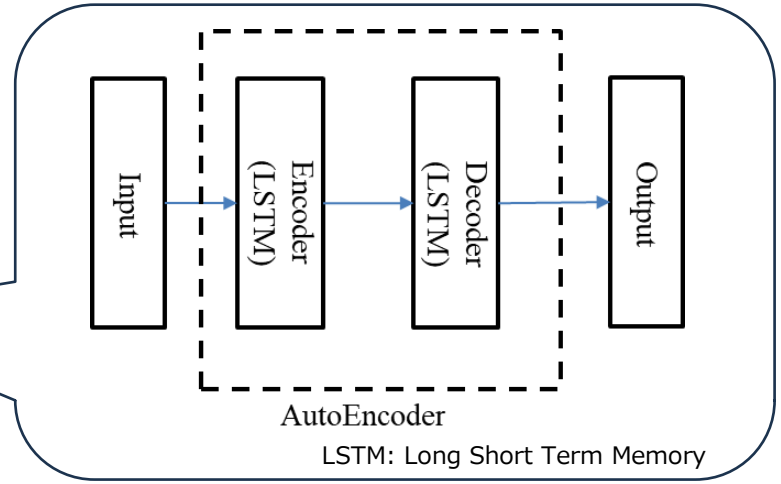
パケット単位の異常判定処理



通信フロー単位の異常判定処理



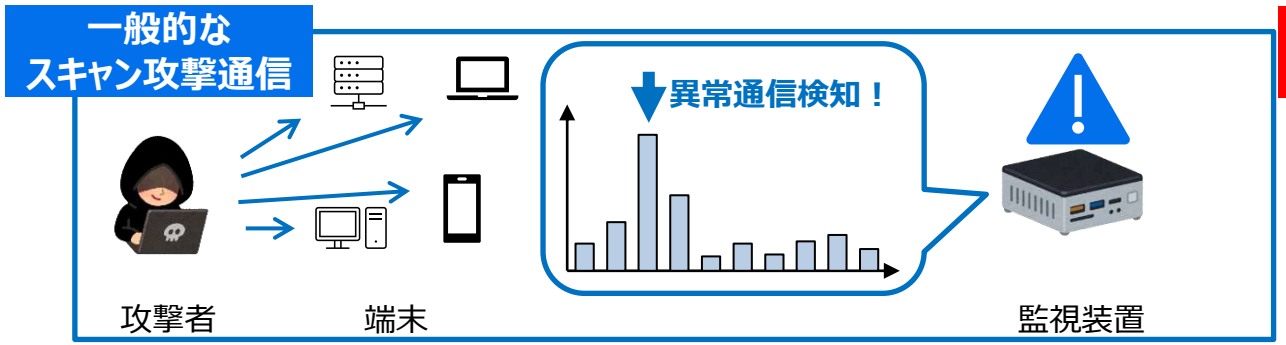
通信フローを特徴量ベクトルに変換(パケット長、到着間隔、…、といったヘッダー情報のみを利用)
正常通信パターンを教師なし学習し、
定常から逸脱する特徴を持つ通信を異常判定

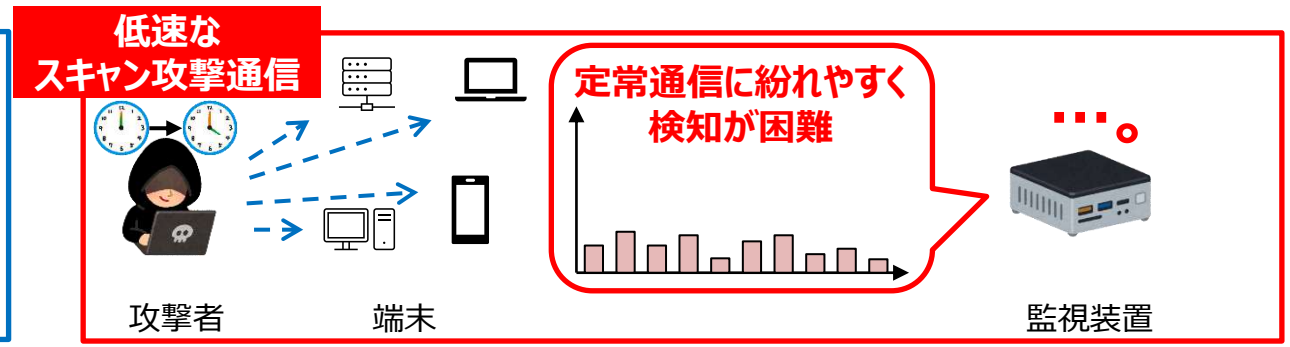


スキャン通信検知　～閉域網での低速なスキャン攻撃通信の検知～

OKI
Open up your dreams

- 機器ごとに**他の機器/ポートへのアクセス履歴**を持ち、閾値超過時に検知
- 時々刻々と変化するネットワークの状態(アクティブ機器数など)に応じた**動的閾値**を利用





【ホストスキャン攻撃通信の検知例】

監視対象ネットワークにおける数日分の通信フローから検知パラメータを算出し、受信した通信フローに対して逐次的に検知処理を実行

検知仮説

・宛先の種類が相対的に多い
- 攻撃に利用されやすいリモートアクセス系ポートへアクセス
- 宛先アドレスやポート番号の変化に規則性あり
- 送信元にとって稀な宛先
- NW全体にとって稀な宛先
…

学習	検知閾値の算出	検知処理
過去数日分の定常通信フローを分析。機器数と宛先IPアドレス数の分布から機器数に対する通信先数の割合を算出。	通信先数の割合と時間毎の機器数から検知閾値を算出。	送信元IPアドレス毎に宛先IPアドレス数を集計。 受信した通信フローに対して動的閾値を用いてスキャン攻撃通信判定。

社内工場での取り組み　～生産エリアNW監視～

OKI
Open up your dreams

■ **国内2工場(沼津工場、本庄工場)の生産エリアネットワークに設置し、ネットワークの可視化と異常通信の監視を実施　⇒　フィードバックを得ながらシステム改良**

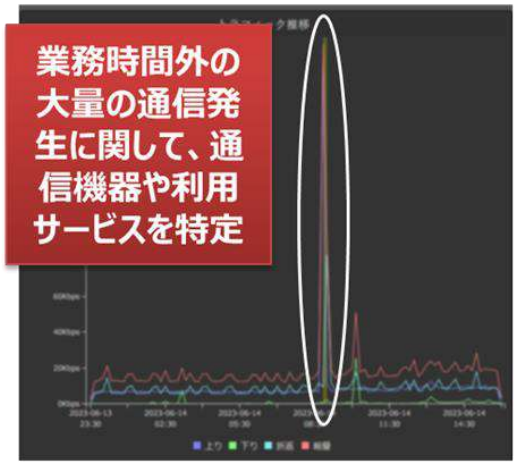
- 沼津工場(2022年2月～)：
  - 本装置を用いて監視運用を回せるかなどのシステム評価を実施
- 本庄工場(2022年8月～)：
  - 新工場の稼働開始に伴い設置
- 通信の可視化とセキュリティ対策強化の要望があり、他工場でも試行検討中

【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】

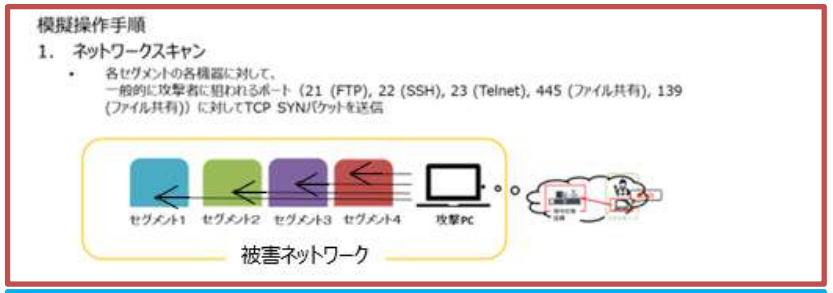


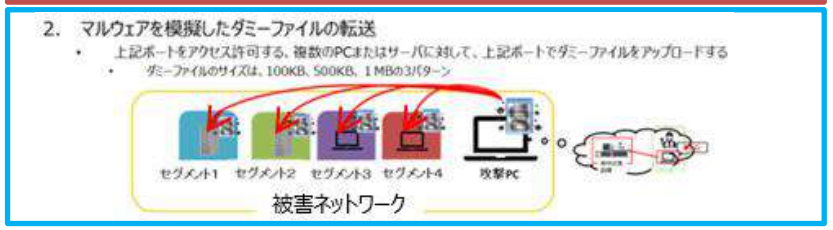
ネットワーク管理者が
詳細に把握できなかった
新規の機器接続や
休日の大量通信を検知

OKI社内工場データを用いた評価

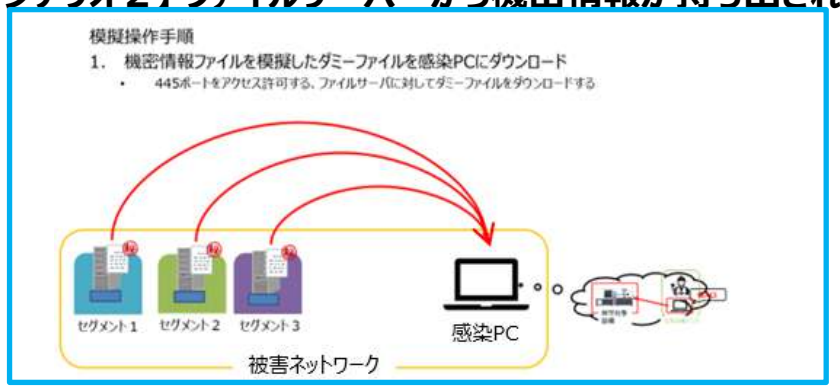
■ 実際に社内工場の**生産エリアNW**で取得したトラフィックデータに、マルウェア感染拡大や機密情報漏洩の通信を**模擬したトラフィック**を紛れ込ませ、検知性能を評価

【シナリオ１】マルウェアが保守対象設備に送り込まれる





【シナリオ２】ファイルサーバーから機密情報が持ち出される



スキャン通信検知：スキャン通信は**すべて検知**、誤検知2件(1機器)

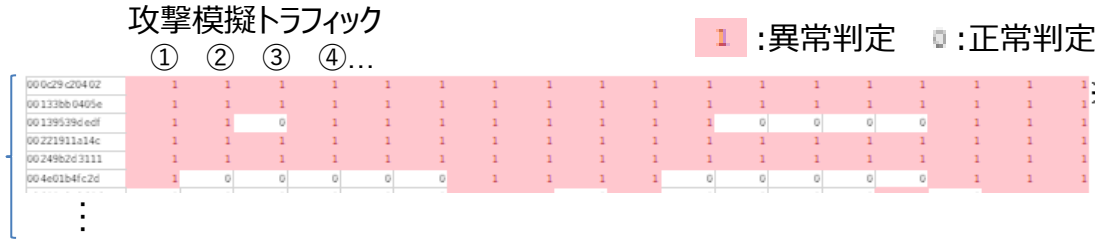
評価期間：5日間(10月13日~17日)
機器数：55台

模擬攻撃通信の発生時間
- 10月13日 5:05:00~5:05:03
- 10月13日 7:05:00~7:06:14
- 10月13日 9:05:00~9:08:13
- 10月13日 11:05:00~11:11:25
- 10月13日 13:05:00~13:26:21

通信非定常検知：機器毎モデルで全模擬通信のうち**82.7%を検知**

もしもNW内の正常機器が突如攻撃模擬通信を発生させたら検知するかを評価

機器
全36台



考察：平常時の運用で似た挙動の通信をしている機器は検知困難。
通信非定常検知エンジン単体に頼るのではなく、宛先のレアさや、時間帯など**複数観点を組み合わせた検知が必要**。

監視結果の通知と確認

OKI
Open up your dreams

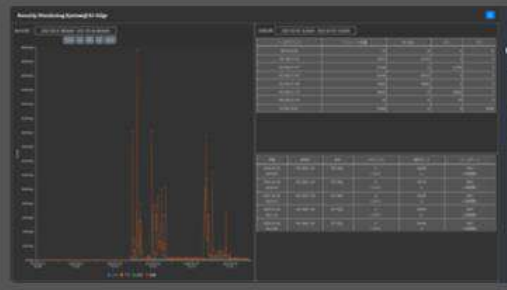
■ メイン画面の他に週次レポートやメール通知等、運用監視を支援する基本機能を標準搭載

Security Monitoring System@AI-Edge

Dashboard

セキュリティ状態を俯瞰します。

機器リストと確認すべき事象を表示



Traffic Amount

トラフィック量を監視します。

通信量が多い機器とサービスを調査

Weekly Report

週次報告書を表示します。

指定期間でのレポートを表示

【メールでのイベント通知】

ファイル　メッセージ　ヘルプ　何をしますか

Teams で共有　関西ラボ全員

Incident Reports[[redacted]]

NT　[redacted]@oki.com
宛先　八百 健嗣

発生日時
2022-10-11 19:33:23～継続中

#Summary
##概要（Overall）
新規端末が検出されました。
未許可端末かどうか直ちに確認してください。
⇒ http://[redacted]/webmon/dashboard.html?startDate=2022-10

##エンジン検知状況
新規端末
IP アドレス: [redacted]
MAC アドレス／ベンダ名（参考）: [redacted]

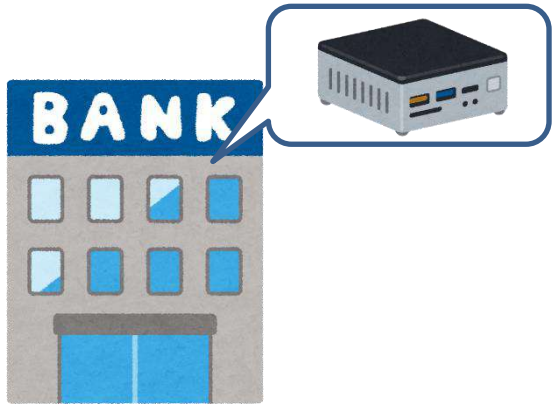
機器種別判定
PC の可能性が高いです。

【パトランプとの連携】

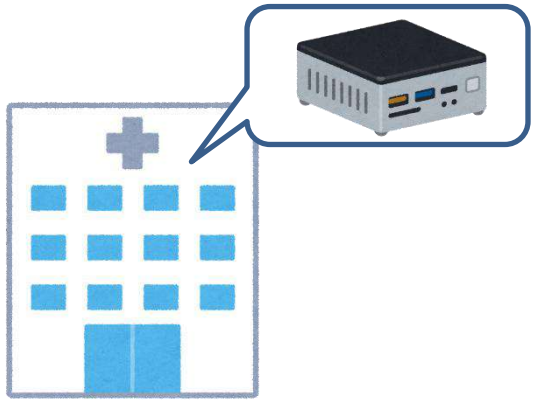
現状と今後の展開

- 各業界でセキュリティガイドラインが発行され、ゼロトラスト的な思考が重要視されている
  - 閉域ネットワークにおいても、機関内システムにアクセスする全ての通信を監視することが重要
- 2025年度の製品化に向けて商品企画中
  - 引き続き実証実験で広くVoCを収集(金融、医療、製造、…)

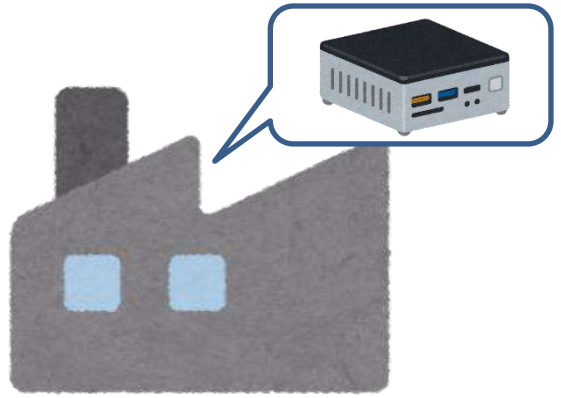
小型かつ単体で動作し、あらゆる拠点に追加整備可能



金融機関



医療現場



生産現場(国内拠点・海外拠点)

実証実験・共創のパートナーも随時募集しております