トラフィックから見るOTセキュリティの世界

2025年2月28日

NTTコミュニケーションズ株式会社

イノベーションセンターテクノロジー部門

加島伸悟

自己紹介

加島 伸悟（かしま しんご）

■ 所属

NTTコミュニケーションズ株式会社（以下、NTT Com）

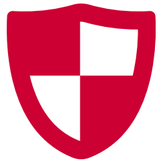
- イノベーションセンター
  - テクノロジー部門 セキュリティグループ責任者
  - セキュリティオペレーション実施責任者
- マネージド＆セキュリティサービス部
  - 国産OT-IDS「OsecT」のプロダクトオーナー

一般社団法人 セキュリティ・キャンプ協議会 理事

■ 略歴

- 広域イーサネットサービスの技術＆商用開発
- フロー監視（xFlow）の技術開発＆国際標準化
  - IETF RFC 7133 Author
- NTTグループ全体のセキュリティガバナンス
  - 東京オリパラに向けた事業インパクトベースのリスクアセスメント
- 制御システムセキュリティの技術開発・サービス開発

セキュリティ用途のトラフィック監視はオワコン？



昨今のサイバーセキュリティの世界では、トラフィック監視だけで対応できるは脅威は限定的

- ✓ 通信の暗号化が当たり前になり、トラフィックの中から正常通信/攻撃通信の見分けをつけることが困難
- ✓ 端末内部の振る舞いの監視まで行わないと何も見えない

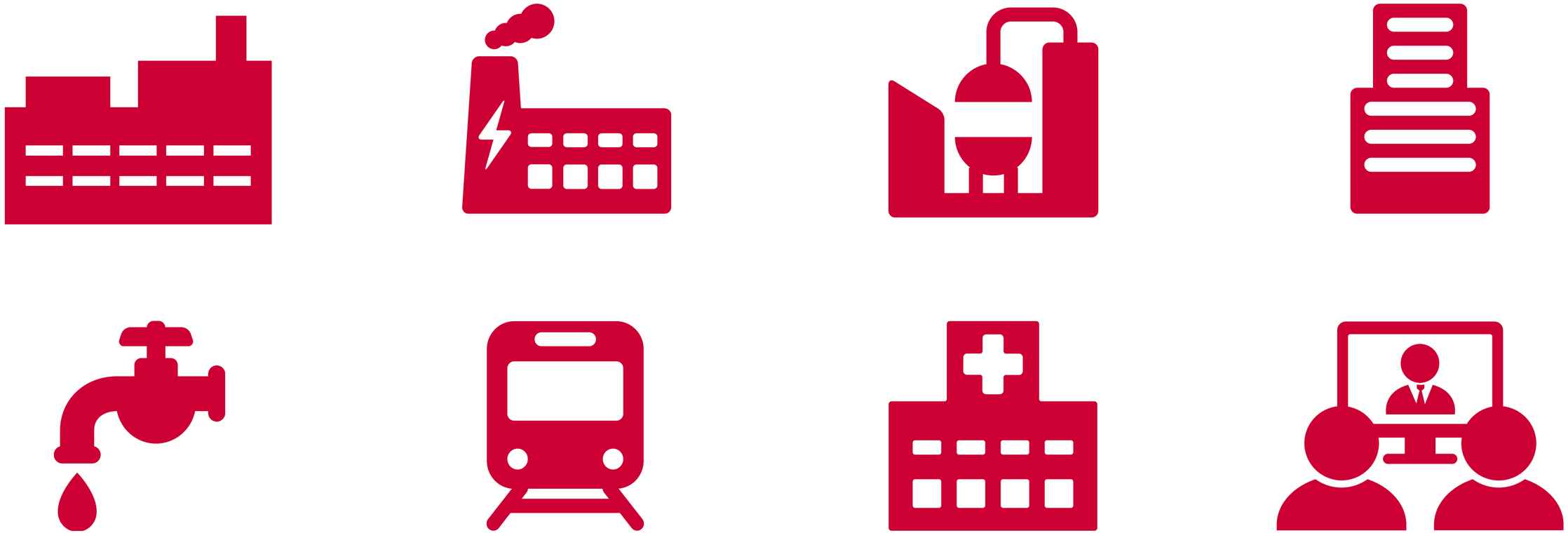
パケットヘッダレベルのトラフィック監視の併用によるセキュリティ運用高度化には価値あり

- ✓ 事後対応における通信フローデータを活用したネットワークフォレンジック

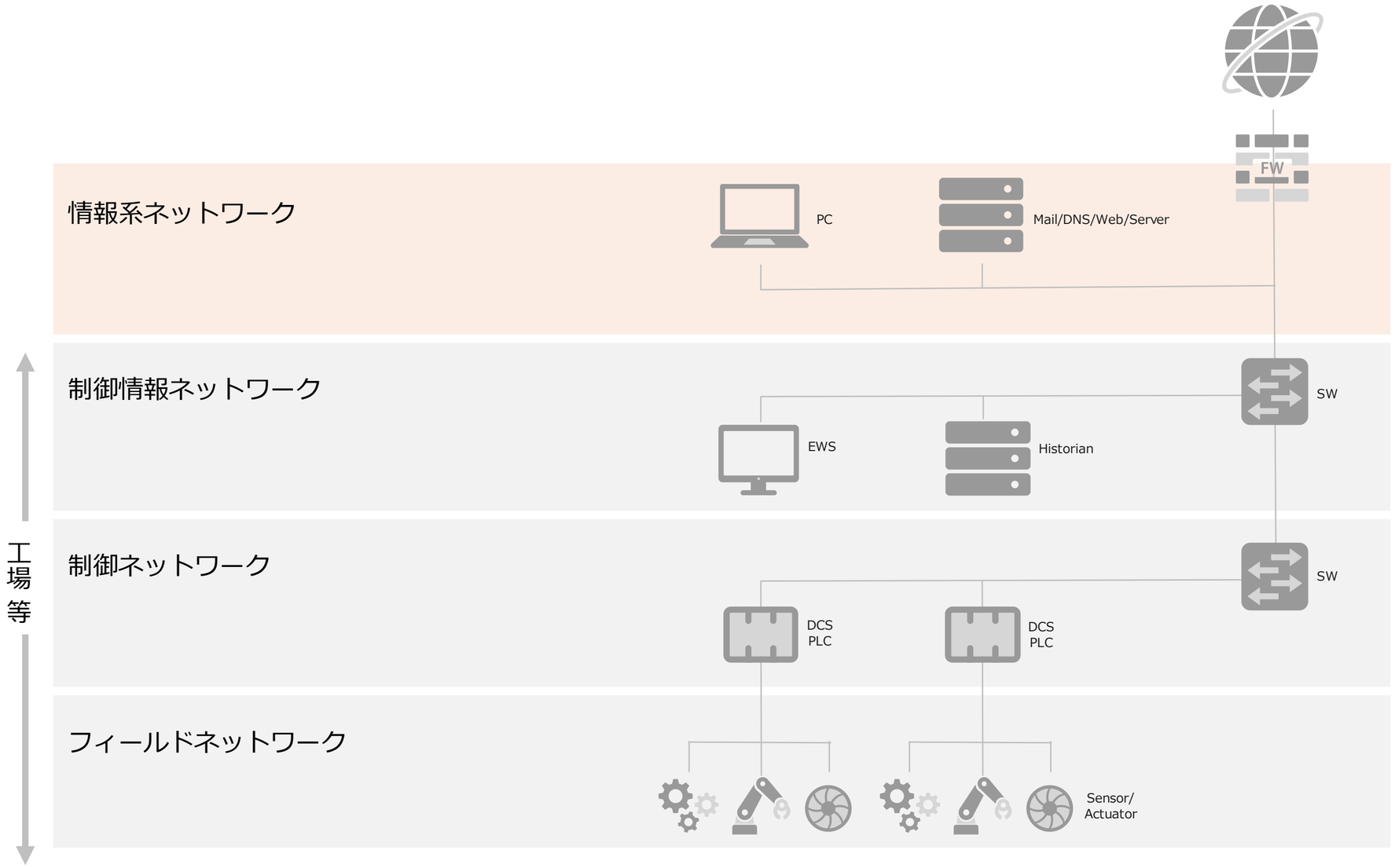
トラフィック監視が主たる対策となりうるOTシステムのセキュリティについてお話しします

Operational Technology (OT) とは

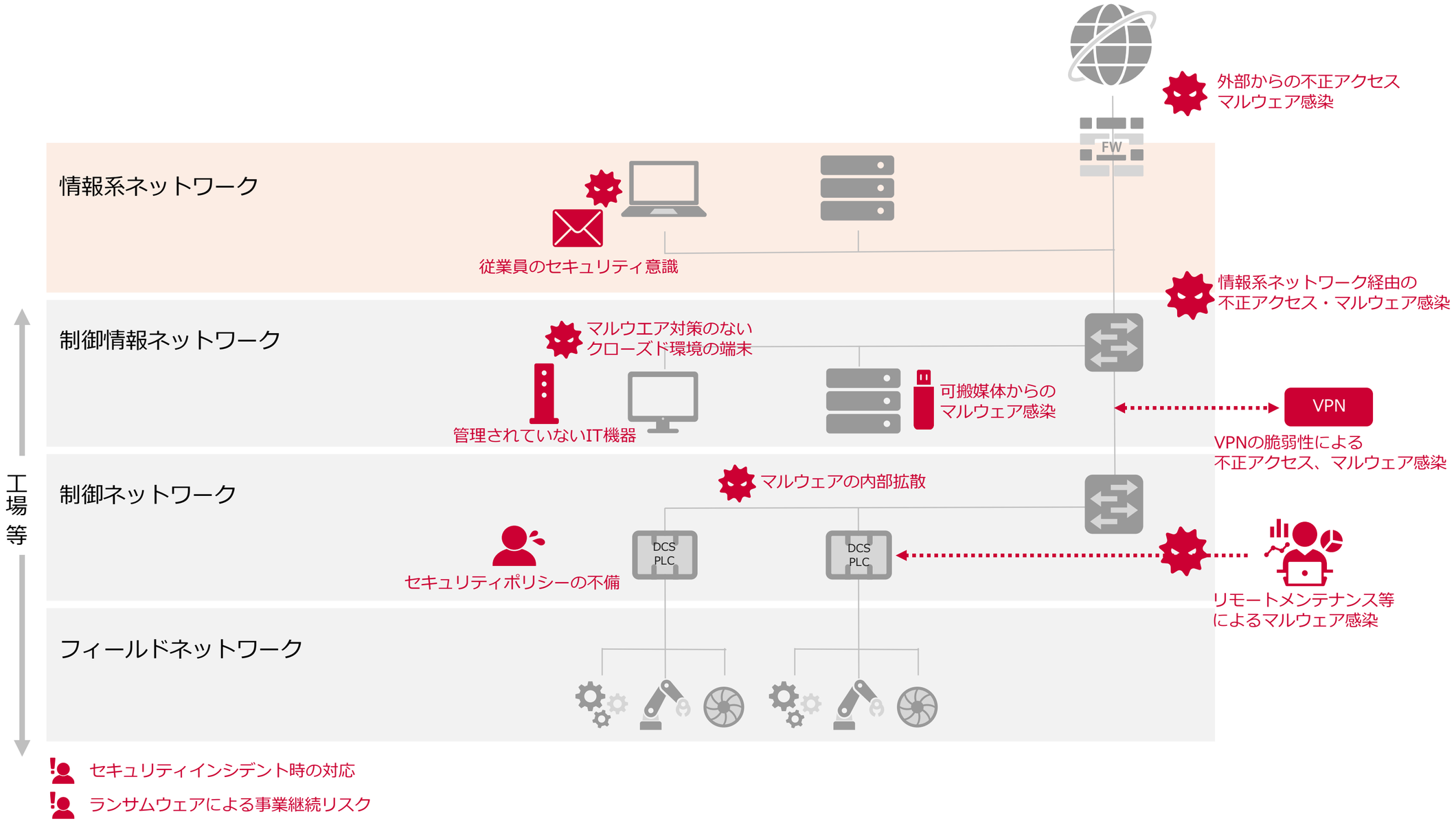
- 製造業、エネルギー、重工業、建物、公共事業、輸送、医療、放送などの産業分野において、設備・システムを最適に動かすための技術
- 情報技術（Information Technology, IT）と対比されることが多い



OTシステム



OTシステムのサイバーリスク俯瞰図



OTシステムとITシステムにおける要件のギャップ

制御システム（OT）	項目	情報システム（IT）
1. 可用性（**A**vailability） 2. 完全性（**I**ntegrity） 3. 機密性（**C**onfidentiality）	セキュリティの優先順位	1. 機密性（**C**onfidentiality） 2. 完全性（**I**ntegrity） 3. 可用性（**A**vailability）
• 健康　（**H**ealth） • 安全　（**S**afety） • 環境　（**E**nvironment）	追加要件	–
• モノ（設備、製品）、サービス（操業）	保護対象	• データ（個人情報等）
• 10～20年+	システム更新サイクル	• 3～5年
• 一般的でない	OS更新・パッチ適用	• オンラインでの定期・随時更新
• 一般的でない	ウイルス対策	• 端末へのアンチウイルス、EDRの導入
• 標準通信プロトコル＋独自通信プロトコル • 平文通信・パスワード等の簡易な認証	通信	• 標準通信プロトコル • 暗号通信・暗号技術による認証有り

制御システム向けセキュリティ製品の要件

安定稼働最優先

セキュリティ対策の導入によりシステムへの影響があってはいけない

既存端末へのランサムウェア対策のソフトウェア（アンチウィルスソフト、EDR等）の導入が難しい

最新の脅威への対応

脅威情報が公開されないためパターンマッチ型の脅威検知が適合しにくい

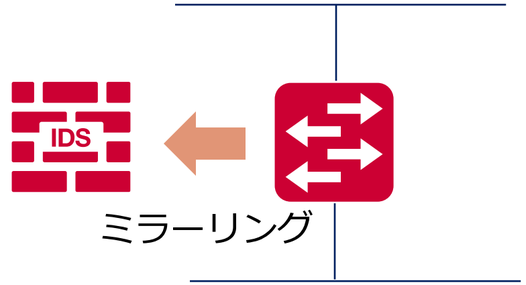
資産管理

機器・端末の状態を把握していない

制御システム向けセキュリティ製品 OT-IDS の特徴

安定稼働最優先

☑ ネットワーク型（端末導入型ではない）
☑ パッシブ型で検知まで
（インライン型での遮断まではしない）



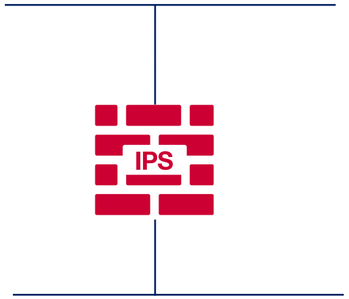
IDS (Intrusion Detection System)
不正侵入検知システム
→ パッシブ型・・・OTへの適用事例が多い

最新の脅威への対応

☑ 学習ベースの脅威検知

資産管理

☑ 充実した可視化機能



IPS (Intrusion Prevention System)
不正侵入防止システム
→ インライン型・・・ITへの適用事例が多い

国産 OT-IDS 「OsecT」

OsecT（オーセクト）は、ISP/Tier1大規模ネットワークにおけるDDoS対策で培った通信フロー解析技術や東京2020オリンピック・パラリンピック競技大会を支えた通信インフラ向けのリスク可視化技術など、NTT研究所の技術を基にNTTコミュニケーションズが製品化したOTシステム向けIDSです。

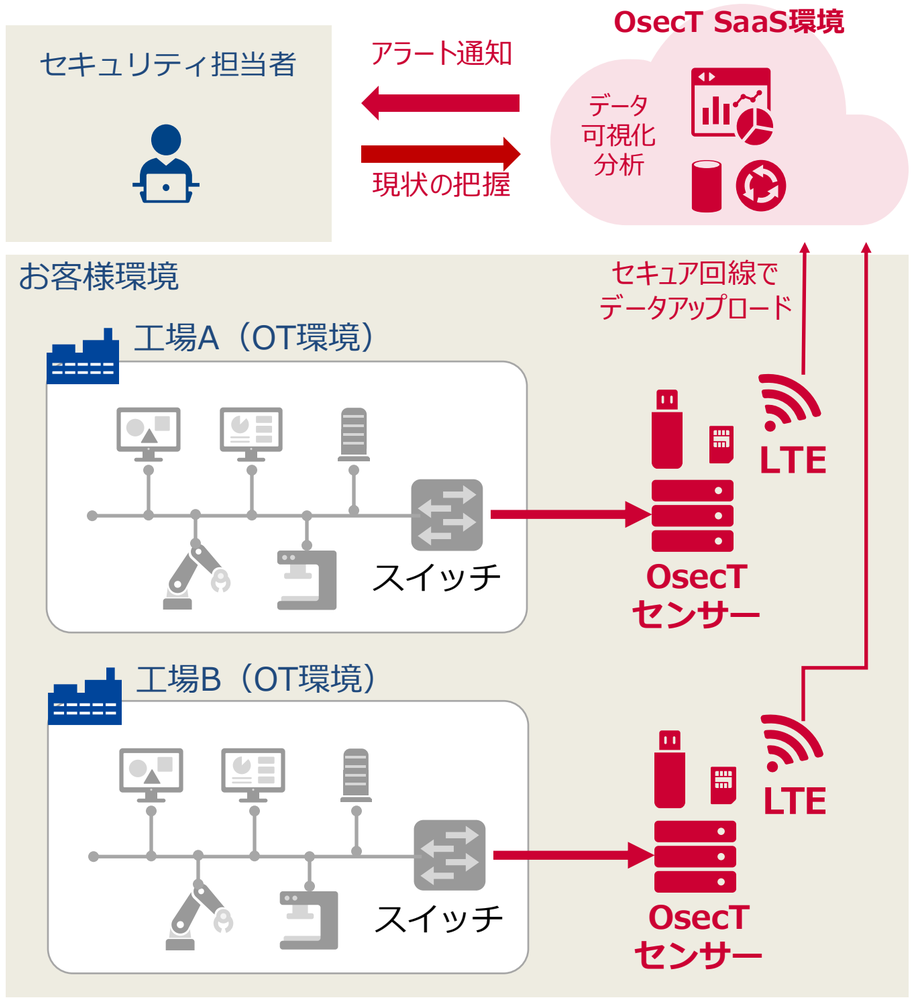
OTネットワーク可視化

さまざまな角度から分析した接続端末や通信をOsecT SaaS環境のポータル画面で確認できます。

サイバー脅威の早期検知

不審な端末や未知の通信などのサイバー脅威を早期に発見し、アラートを通知します。

国産 OT-IDS 「OsecT」の特徴



簡単導入

OsecTセンサーを工場内のスイッチのミラーポートに接続するだけで準備完了。
OsecTセンサーからOsecT SaaS環境へのデータアップロード用の無線通信回線が付属しているため、新たなネットワーク工事は不要です。

セキュリティ管理不要

センサーからSaaSへの通信は当社閉域網を利用するため、 ASM (Attack Surface Management：外部から攻撃を受ける可能性のある対象領域の管理)不要です。

SaaSによる一元管理

セキュリティ監視状況はOsecT SaaS環境のWebポータルで確認できます。遠隔地のセキュリティ担当者が各工場を一元監視することもできます。

低価格

低価格な月額料金でご利用いただけます。
※月額料金には無線通信回線やポータルの利用料も含まれています。

セキュリティサポート

セキュリティ運用サポートサービス付きプランの提供を開始予定（2025年）

おわりに

OTセキュリティ用途のトラフィック監視はオワコンどころか今が旬です

OTネットワークの可視化とサイバー脅威検知ができる製品＝OT-IDS

NTT Comは国産OT-IDS「OsecT」を内製開発、展開中

OsecT