電気通信事業者、セキュリティサービス事業者、およびセキュリティ製品オーナーの視点から、制御システムにおける資産の可視化と常時監視の課題について考える

2024年7月26日

NTTコミュニケーションズ株式会社
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
- マネージド＆セキュリティサービス部　セキュリティサービス部門

■ 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
- NTTグループ全体のセキュリティガバナンス
- 制御システムセキュリティの技術開発・サービス開発

3つの視点から

docomo business | NTT Communications

GIN OCN Nexcenter

電気通信事業者

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

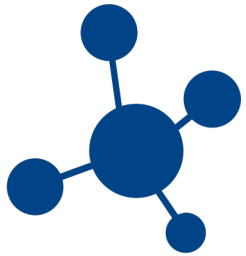
セキュリティサービス事業者

OsecT

セキュリティ製品オーナー

電気通信事業者としてのNTT Com

DDoS攻撃を含むサイバー攻撃からお客様および通信設備を保護するため、バックボーンネットワークのトラフィックを分析（フロー分析）



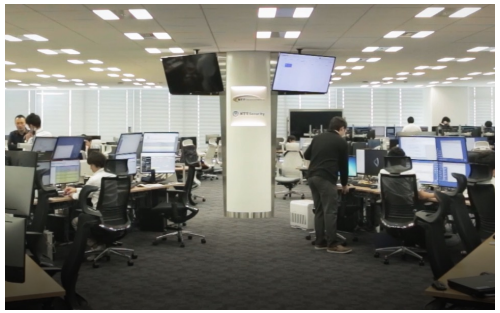
全国の通信設備を保守するための巨大な閉域網を運用

データセンター、通信ビル、オフィスビルのBA（Building Automation）ネットワークを運用

セキュリティサービス事業者としてのNTT Com

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

さまざまな業界の企業や官公庁に対するサイバー攻撃をSOCにていち早く発見・分析し、適切な対処をサポートするマネージドセキュリティサービスを展開



SOCにおける分析の対象は幅広い

- IPS/IDS
- UTM/WAF
- Sandbox
- Firewallログやプロキシログ
- EDR
- Active Directoryのセキュリティログ
- OT-IDS

セキュリティ製品オーナーとしてのNTT Com

OsecT:

- NTT Com社員がセキュリティ製品の海外依存に疑問を感じ、せめてお家芸の製造業（工場）や社会インフラ向けのセキュリティは国産で！との思いから立ち上げたOT-IDS、OTセキュリティサービス
- 詳細は後半で

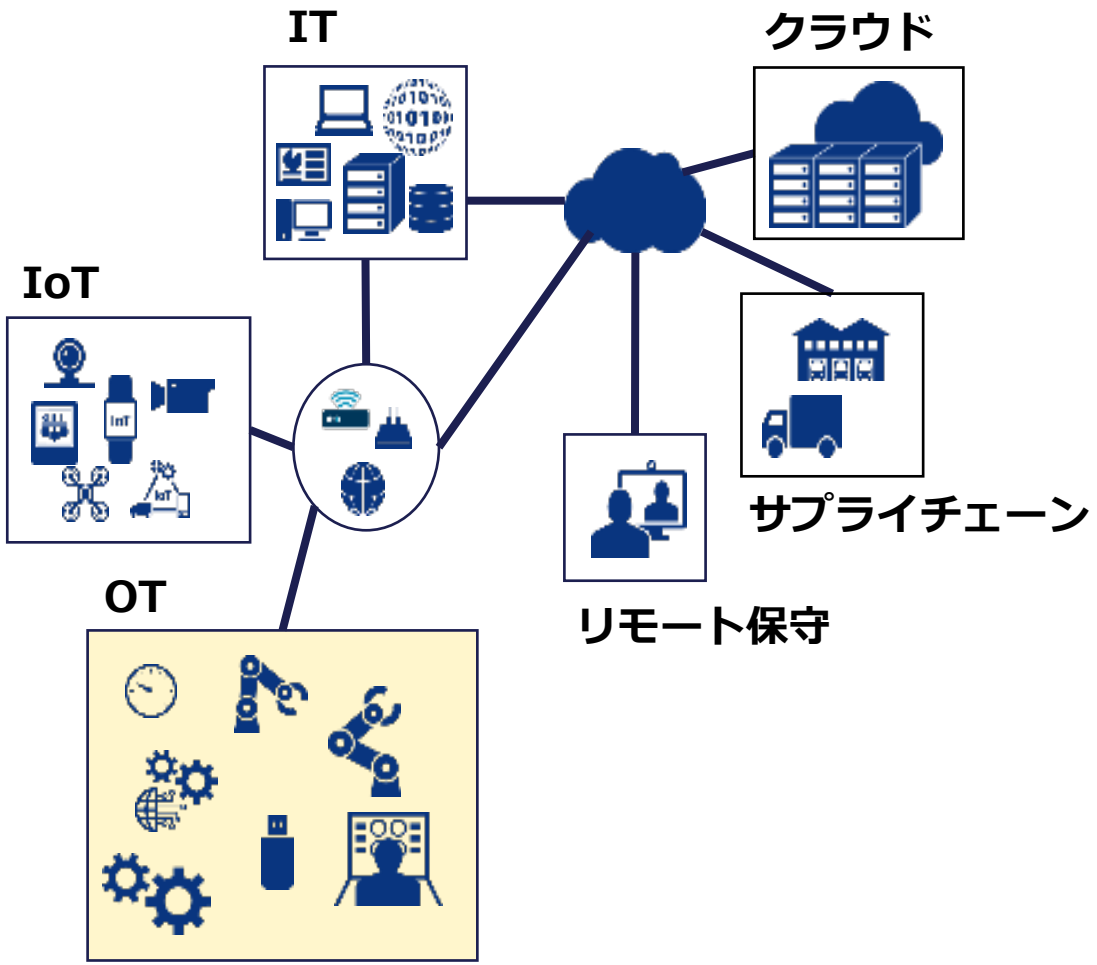
海外セキュリティ製品依存の課題:

- 日本で商用展開されているセキュリティ対策製品は海外依存
  - 「輸入」して展開する「販売店」
  - 付随するサービス（導入・運用等）を提供する
- マーケットサイズに応じた対応となるため、日本固有の要望やトラブルへの対応が不可・遅い
- 技術開発の源泉となるデータへのアクセスが制限される
- 利益率が悪い

後半は NISC 研究開発戦略専門調査会 第10回会合 資料3 国産サイバーセキュリティの現状と課題（鵜飼委員説明資料）から再構築

工場制御システムを取り巻く環境とサイバー攻撃

工場制御システムを取り巻く環境



工場制御システム(OT)は、IoT、情報システム(IT)、クラウド、サプライチェーン等、外部との接続が急増

外部との接続の拡大により、制御システムネットワークはサイバーセキュリティのリスクも増加

サイバーセキュリティの問題は、製造システム、PLC、センサーのダウンタイムまたは不適切な動作を引き起こす可能性が増加

制御システムに影響を与えるサイバー攻撃の現状

- 制御システムへのサイバー攻撃で特徴的なパターンとして以下が挙げられる

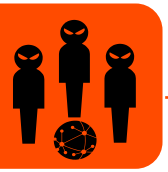
ランサムウェア（RaaS）

✓犯罪グループによる金銭獲得

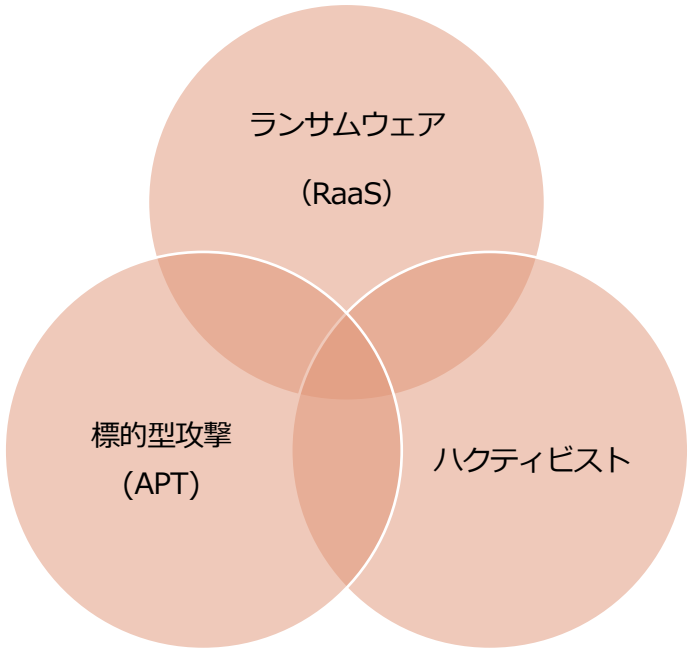
標的型攻撃（APT）

✓軍事的戦略に基づくインフラ破壊

ハクティビスト



✓自らの主張と本気度を広範囲にアピール



※分類上複数に所属することも

製造業への攻撃事例 | ランサムウェア感染

- 制御システムのネットワーク化・デジタル化に伴い、IT環境のみならずOT環境も被害に遭う時代に
- 大手企業だけではなく、サプライチェーン全体が攻撃対象に

半導体工場

WannaCryの亜種に感染し一時生産停止。完全な**復旧に3日間**を要した。最大**190億円**規模の損害
（2018年@台湾）

アルミニウム工場

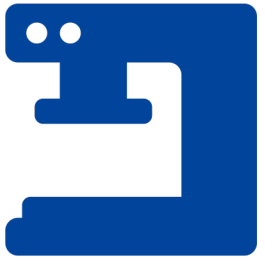
LockerGogaに感染し、一部生産、オフィス業務に影響。プラントは影響拡散防止のためシステムから分離。被害は**最初の1週間で3億円以上**と推定
（2019年@ノルウェー）

自動車メーカ

EKANSまたSNAKEに感染した影響で、自動車工場2拠点の出荷が一時停止。海外にも感染が波及し、**海外9拠点の生産が1~3日間停止**。
（2020年@日本）

自動車メーカの取引先（サプライチェーン）

取引先の子会社1つがリモート接続機器の脆弱性をつかれ感染。調査等のためにシステムを遮断したことにより、**大手自動車生産工場（14工場28ライン）が停止**
（2022年@日本）



制御システムへの攻撃事例 | マルウェア

- **OT特化型のマルウェアも存在**

工場制御システムのセキュリティ課題

制御システムと情報システムにおける要件のギャップ

項目	制御システム（OT）	情報システム（IT）
セキュリティの優先順位	1. 可用性（**A**vailability） 2. 完全性（**I**ntegrity） 3. 機密性（**C**onfidentiality）	1. 機密性（**C**onfidentiality） 2. 完全性（**I**ntegrity） 3. 可用性（**A**vailability）
追加要件	• 健康　（**H**ealth） • 安全　（**S**afety） • 環境　（**E**nvironment）	-
保護対象	• モノ（設備、製品）、サービス（操業）	• データ（個人情報等）
システム更新サイクル	• 10～20年+	• 3～5年
OS更新・パッチ適用	• 一般的でない	• 一般的
ウイルス対策	• 一般的でない	• 一般的
通信	• 標準通信プロトコル • 多数の独自通信プロトコル	• 標準通信プロトコル
セキュリティ機器の特徴	• パッシブ構成、かつ検知まで • 優れた可視化機能	• インライン設置と遮断を許容 • 新しい脅威への常時更新（対応）

工場制御システムのセキュリティ課題

1. レガシーシステム
   もともと設計時にセキュリティを意識しておらず、改修が難しい

2. 資産の可視化
   アセットの状態を把握していない

3. 脆弱性と脅威
   バージョンアップやセキュリティパッチの実施が難しい

4. スキルのある人材の不足
   セキュリティに関するスキルがある人員の確保が難しい

よくあるOTセキュリティソリューション

よくあるOTセキュリティソリューションのアプローチ

STEP1: 現状把握と評価
工場LANの見える化とセキュリティアセスメント

STEP2: 脅威の侵入/拡散防止・検知策の導入
セグメンテーション・アクセス制御とOT-IDS*の導入

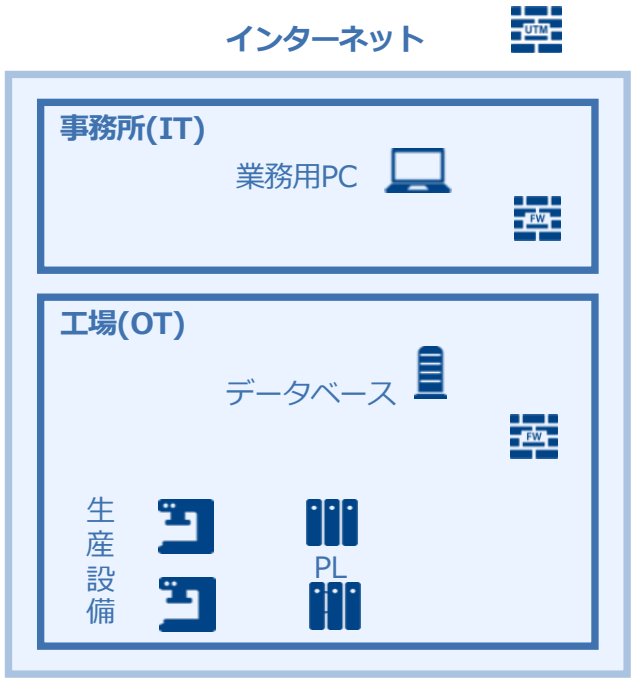
STEP3: 監視体制の構築
外部の専門アナリストよる監視・分析・対処の仕組み（マネージドセキュリティサービス）を導入

* OT-IDS: OT環境向けのIDS。システムの可用性に影響を与えないように、ミラーポートから取得したパケットデータから脅威を検知する機能に加えて、可視化機能を有することが特徴。インライン型は少ない。

STEP1: 現状把握と評価における課題

課題① 生産現場ではトラフィック取得位置の特定とネットワーク機器設定ができない

- ✓ 効果的な監視ができる設置場所の特定
- ✓ ルーター・L2スイッチなどのネットワーク機器設定
- ✓ そもそもネットワーク機器にトラフィック取得機能（ミラーリング機能）がない場合もある



どこに設置すればよいのかわからない。

ネットワーク機器の設定がわからない。

STEP2: 脅威の侵入/拡散防止・検知策の導入における課題

課題② 既存ネットワークの構成変更を伴わない監視を必要とされるケースがある

- ✓ OTネットワークがIT等の別用途のネットワーク分離されていないことが中堅・中小企業中心に見受けられる
- ✓ セキュリティ観点ではIT/OTのネットワーク分離をした上でセキュリティ製品による監視を導入すべきだが、様々な要因で構成変更無しでの監視を要望されるケースが多い
- ✓ しかし、OT-IDSはインターネットトラフィックを監視対象として想定してないため、対応が困難

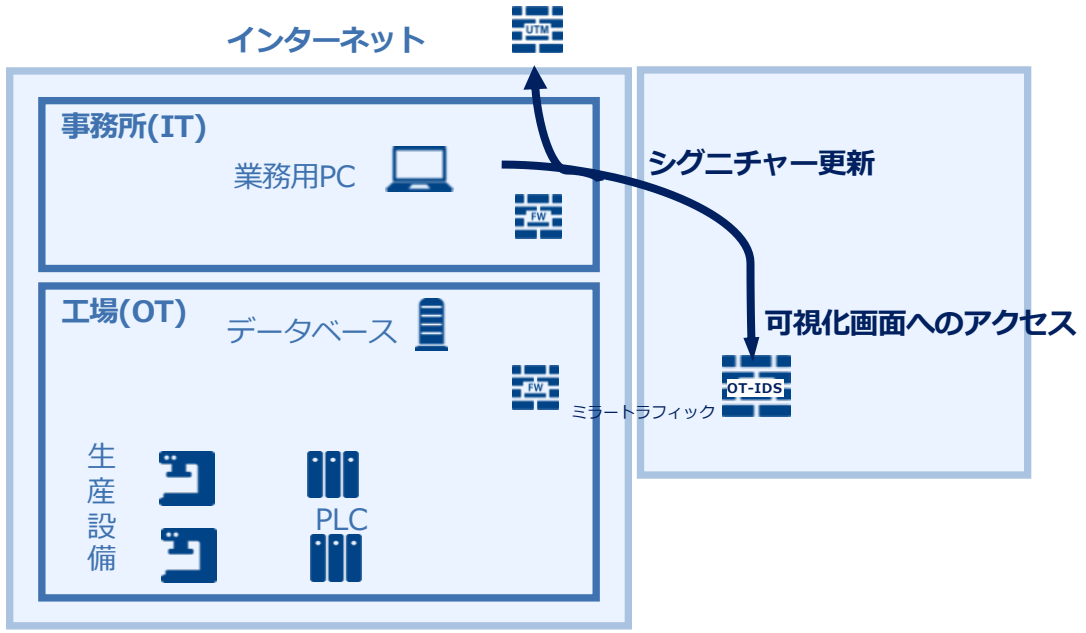
大企業のOTネットワーク：ITと分離されている

中堅・中小企業のOTネットワーク：ITと分離されていない

STEP2: 脅威の侵入/拡散防止・検知策の導入における課題

課題③ OT-IDSの導入コストが高い

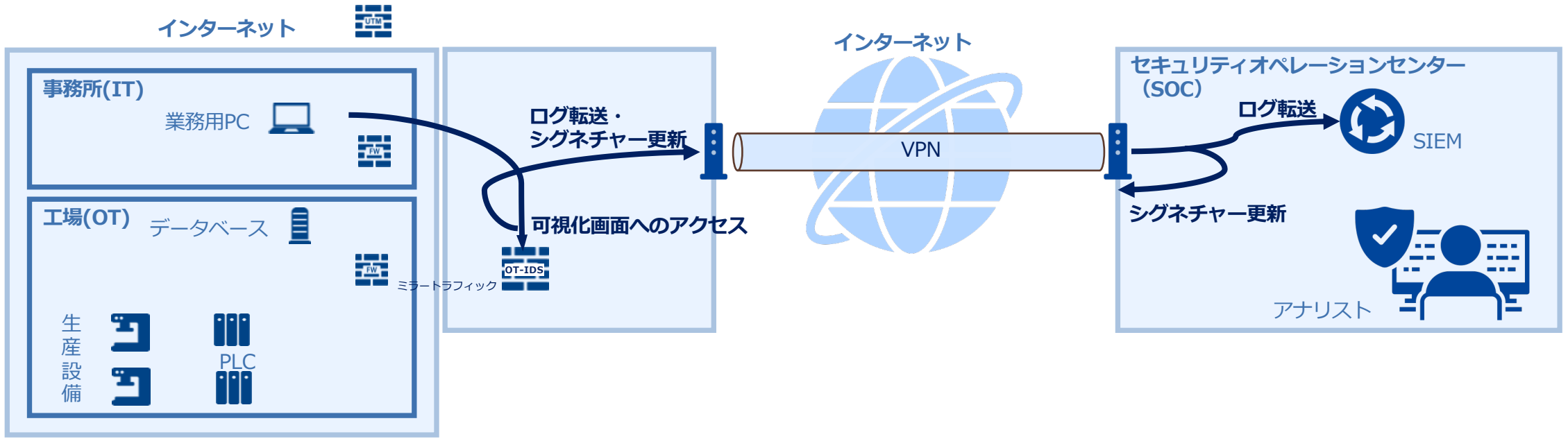
- ✓ 製品コスト: IT-IDSと比較して高額
  - ライセンス費用がアドレス数（≒端末数）に応じた金額となるため、ライセンス費用節約のために、見える化とは逆方向に進みがち
  - OTプロトコル対応が売りだが、FA系でOTプロトコルの中身まで意識した監視をしている現場は皆無に近い（オーバースペック）
- ✓ 構築コスト: 可視化画面へのアクセスやシグネチャー更新ができるようにネットワーク設計が必要



STEP3: 監視体制の構築における課題

課題④ 外部接続時のセキュリティ問題

- ✓ VPN装置のセキュリティ管理が必要
- ✓ 社内からの監視（可視化）と外部SOCからの監視を両立するセキュリティ設計が難しい



STEP3: 監視体制の構築における課題

課題⑤ マネージドセキュリティサービスの必要性

- ✓ OT-IDSは多機能で使いこなすには専門知識が必要であるため、マネージドセキュリティサービスを推奨するケースが多い
- ✓ OT-IDSのアラートは振る舞い検知によるものが多いため、アラートの根本原因までは追及できない
- ✓ 生産現場にはEDR等の深掘り分析できる製品は入っていないため、SOCはIDS製品のアラートを翻訳するだけになってしまうが、そんなSOCにお金を払う価値はあるだろうか？
- ✓ そもそも社外かつリモートのSOCから提供される情報に基づいて生産現場を動かすことができるのか？

STEP1-3共通の課題

課題⑥ 生産現場の協力なしにOTセキュリティは成立しない

- ✓ セキュリティ事故による生産停止の脅威を全面に出してもうまく進まない
- ✓ 生産現場にとっての苦しさ/嬉しさに寄り添った提案が必要

課題の振り返り

既存ソリューションとお客様ニーズは必ずしも適合しておらず、課題が多い

課題① 生産現場ではトラフィック取得位置の特定とネットワーク機器設定ができない

課題② 既存ネットワークの構成変更を伴わない監視を必要とされるケースがある

課題③ OT-IDSの導入コストが高い

課題④ 外部接続時のセキュリティ問題

課題⑤ マネージドセキュリティサービスの必要性

課題⑥ 生産現場の協力なしにOTセキュリティは成立しない

課題解決の概要

NTT Comは電気通信事業者やセキュリティサービス事業者として培ったノウハウを活用して開発した「OsecT」を軸に、パートナーと連携したソリューションを展開中

課題① 生産現場ではトラフィック取得位置の特定とネットワーク機器設定ができない
⇨OsecT導入サポートサービスで解決

課題② 既存ネットワークの構成変更を伴わない監視を必要とされるケースがある
⇨OsecT本体で解決

課題③ OT-IDSの導入コストが高い
⇨OsecT本体で解決

課題④ 外部接続時のセキュリティ問題
⇨OsecT本体で解決

課題⑤ マネージドセキュリティサービスの必要性
⇨OsecT運用サポートサービスで解決

課題⑥ 生産現場の協力なしにOTセキュリティは成立しない　**⇨？**

OsecT（オーセクト）のご紹介

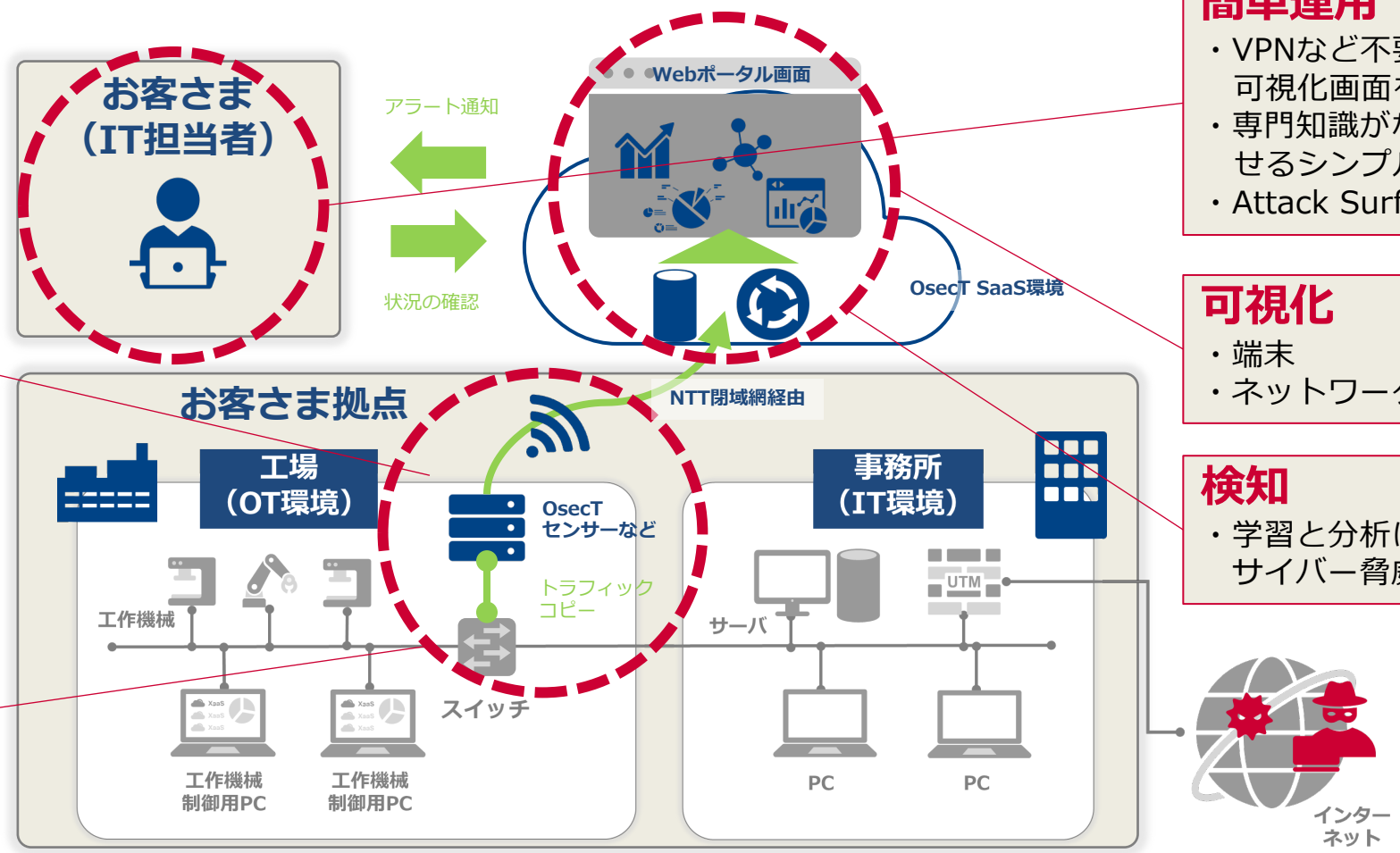
OsecTの概要

生産現場の業務を妨げることなく、制御系システムにおける資産とリスクを可視化し、サイバー脅威・脆弱性を早期に検知することで、工場停止による損失を未然に防ぐことができます。

低価格
・月額費用1桁万円
・PoC等を通じて抽出した真に必要な機能に絞って提供

簡単導入
・センサー機器をスイッチ等のミラーポートに接続するだけ
・OsecTセンサーで取得した情報のアップロードにはNTT閉域モバイル通信を用いるため、ネットワークの設計やVPN機器の設置は不要

制御系システムへの影響なし
・コピーしたトラフィックデータを監視
・既存機器へのソフトウェアのインストール不要



簡単運用
・VPNなど不要でどこからでも可視化画面を参照可能
・専門知識がなくても使いこなせるシンプルな機能/UI設計
・Attack Surface管理不要

可視化
・端末
・ネットワーク

検知
・学習と分析による
サイバー脅威／脆弱性の検知

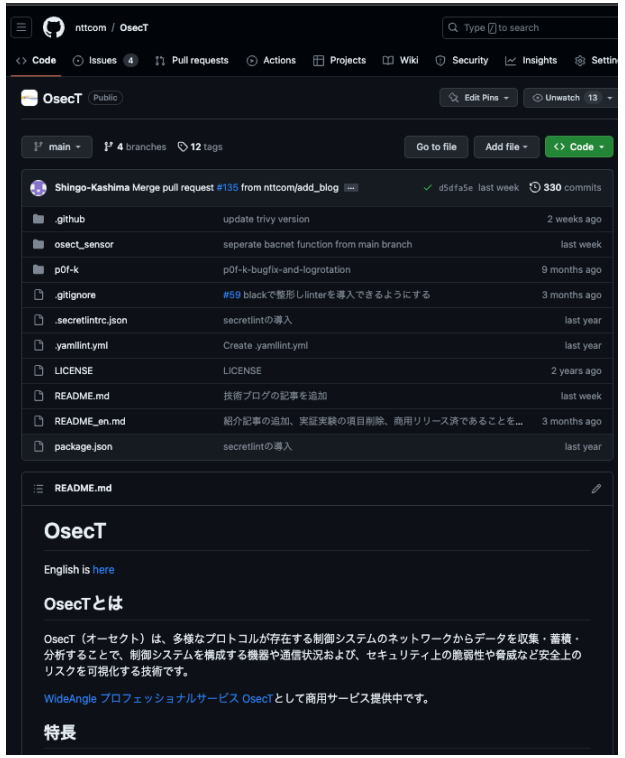
安心してお使いいただくために

安心してお使いいただけるように、以下のような取り組みとネットワーク設計にしています。

- パケット解析機能を有するOsecTセンサーのソースコードを公開*1
  - 見える化・予防/早期発見に**必要最低限の情報のみをSaaS環境に送信**していることを明示

- OsecTセンサー、SaaS環境で利用するソフトウェアは当社による内製開発
  - **日本純正のサービス**として位置づけ

- **Attack Surface Management**は当社にお任せ
  - Web-UIは当社が管理するクラウド上のSaaS環境に一元化
  - OsecTセンサーからSaaS環境へは当社のネットワークサービス*2を組み合わせインターネットを使わずセキュアに閉域接続



*1 https://github.com/nttcom/OsecT
*2 IoT Connect Mobile Type S (閉域網タイプ)及び Flexible InterConnect (FIC)

可視化 -端末-

多角的な端末の可視化、ネットワークマップ、2つ期間のネットワークの構成差分の可視化によって、OTネットワーク環境を視覚的に把握し、資産管理や新たに接続された端末の特定を行うことで、対策強化や有事の際の対応に役立てていただけます。

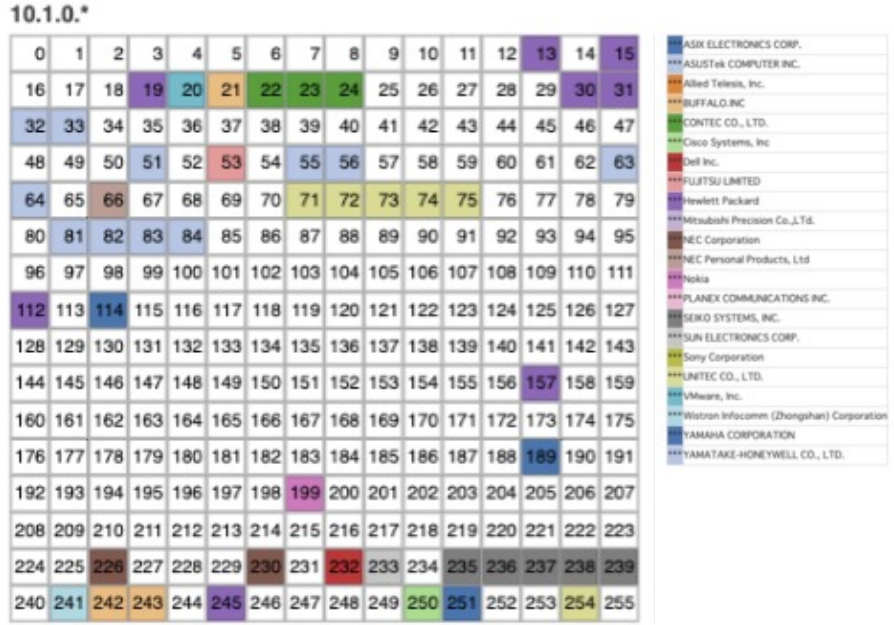
- 自動で端末情報を一覧化
- 端末一覧をCSVファイルで出力し、台帳として利用可能

- 生存端末を16x16のマトリックス形式で可視化
- ベンダ/OS/役割に応じた色分けによって俯瞰した分析が可能

端末一覧

#	IPv4アドレス	IPv6アドレス	MACアドレス	ベンダー	ホスト名	種別・機種	OS	同一サブネット	通信日時（初回）	通信日時（最終）
1	0.0.0.0		00:ff:6c:67:3d:de	Unregistered(00:ff:6c)				mirrored	2024-03-26 15:00:54	2024-03-26 17:43:08
2	0.0.0.0		00:ff:89:ce:a7:fa	Unregistered(00:ff:89)				mirrored	2024-03-28 15:24:48	2024-03-28 15:40:18
3	172.20.10.2 192.168.1.2 0.0.0.0	fe80::4663:b89e:43da:d726 ::	c8:b2:9b:2f:40:77	Intel Corporate	PC4074229		Windows 10	mirrored	2024-03-26 15:59:00	2024-03-26 16:08:23
4	192.168.1.1 169.254.88.181 0.0.0.0	fe80::c833:b868:ccbf:4caf	34:76:c5:cb:c5:6c	I-O DATA DEVICE,INC.	LAPTOP-S2A62IIU		Windows 10/11	mirrored	2024-05-21 14:34:54	2024-05-21 15:03:08
5	192.168.1.1		84:fd:d1:04:69:56	Intel Corporate	LAPTOP-S2A62IIU		Windows 10/11	mirrored	2024-06-11 10:45:00	2024-06-11 12:48:47
6	192.168.1.1 192.168.10.200 0.0.0.0	fe80::b9d2:dc05:6003:3bc9	bc:ec:a0:3f:09:50	COMPAL INFORMATION (KUNSHAN) CO., LTD.	LAPTOP-S2A62IIU		Windows 10/11	mirrored	2024-03-26 15:23:16	2024-03-26 15:26:23
7	192.168.1.98 192.168.1.253 192.168.20.253 192.168.30.253		e8:ed:d6:4f:5f:dc	Fortinet, Inc.				mirrored	2024-04-02 10:11:08	2024-07-16 13:56:57
8	192.168.1.252 0.0.0.0	fe80::c8:f2ff:fecb:dd45 fe80::5480:4fff:fec1:f266 fe80::54fb:c4ff:fe1c:6369 fe80::78cc:81ff:fe40:a290 fe80::a000:26ff:fe28:a53f fe80::ae71:2eff:fea5:d8f8 fe80::fc60:aaff:fe30:a81d ::	ac:71:2e:a5:d8:f8	Fortinet, Inc.	Promotion-AP			mirrored	2024-03-26 14:44:11	2024-06-11 12:49:48
9	192.168.1.254 192.168.10.1 192.168.10.254 192.168.20.1 192.168.20.254 192.168.30.254	::	74:78:a6:14:51:e5	Fortinet, Inc.				mirrored	2024-03-26 14:43:55	2024-07-22 09:59:59
10	192.168.10.1		30:be:3b:db:d6:88	Mitsubishi Electric Corporation				mirrored	2024-07-01 15:45:29	2024-07-22 09:59:41
11	192.168.10.5 192.168.30.2 169.254.25.146 0.0.0.0	fe80::ff99:46f3:f6e9:950 ::	bc:ec:a0:3f:09:51	COMPAL INFORMATION (KUNSHAN) CO., LTD.	Promotion_ATT		Windows 10/11	mirrored	2024-05-21 14:35:29	2024-07-17 17:00:56
12	192.168.18.5		bc:ec:a0:3f:09:50	COMPAL INFORMATION (KUNSHAN) CO., LTD.	Promotion_ATT		Windows 10		2024-03-26 15:23:16	2024-03-26 15:23:36
13	192.168.20.1 192.168.20.2 169.254.89.129 0.0.0.0	fe80::dde4:6585:6a66:4d9c ::	d4:e9:8a:b8:58:49	Intel Corporate	PROMOTION-HMI		Windows 10/11	mirrored	2024-03-26 14:43:57	2024-06-11 12:49:59
14	192.168.20.1	fe80::5f2c:99a1:671e:b726	d8:e2:df:fc:ba:19	Microsoft Corporation	PROMOTION-HMI		Windows 10/11	mirrored	2024-07-01 15:45:27	2024-07-22 09:59:59

端末マトリックス



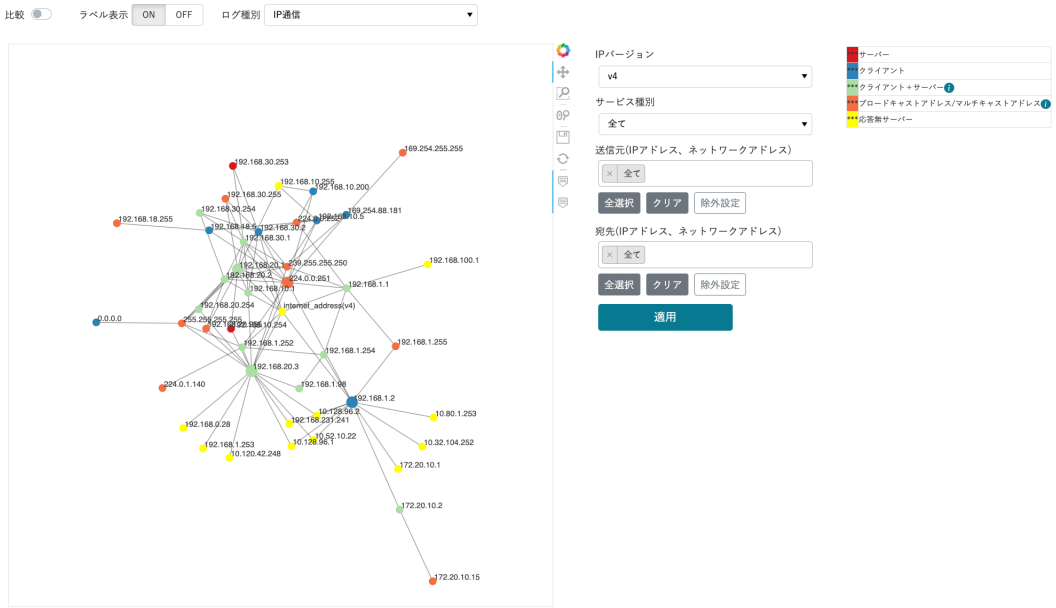
可視化 -端末・ネットワーク-

多角的な端末の可視化、ネットワークマップ、2つ期間のネットワークの構成差分の可視化によって、OTネットワーク環境を視覚的に把握し、資産管理や新たに接続された端末の特定を行うことで、対策強化や有事の際の対応に役立てていただけます。

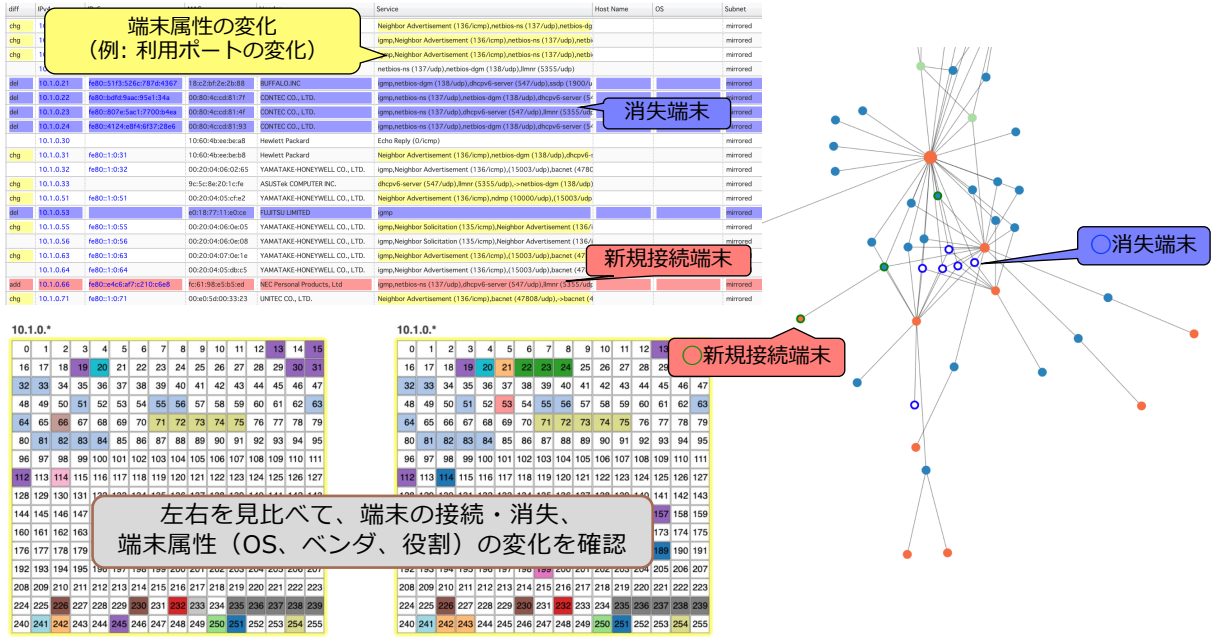
- 端末の通信接続関係をマップ形式で可視化
- 表示データは画像で出力可能

- 2つの期間の端末・ネットワークの構成差分を可視化
- 新たに接続された端末の特定が可能

ネットワークマップ



差分分析



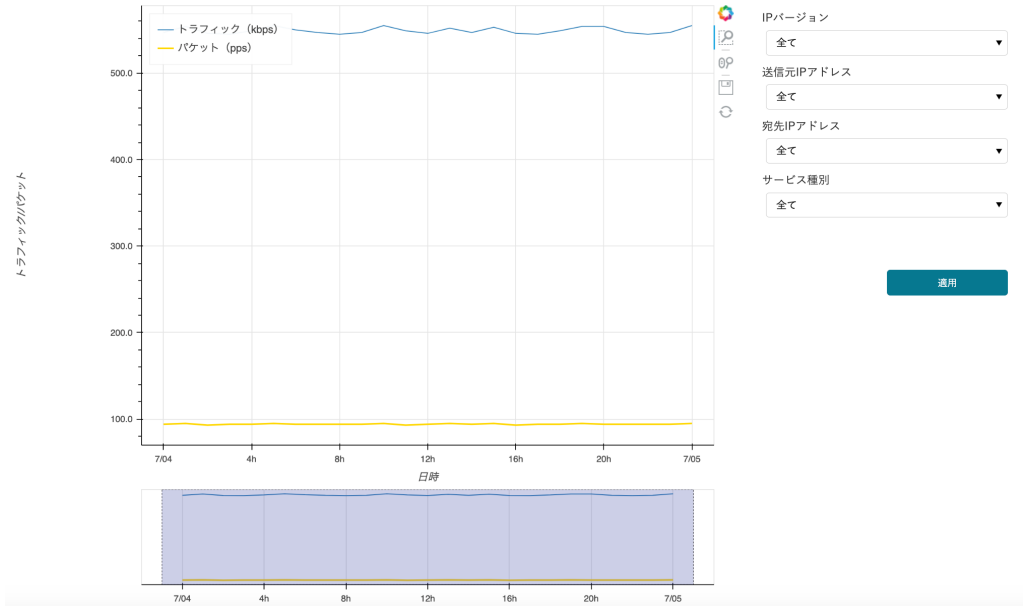
可視化 -ネットワーク-

端末やサービスの利用トラフィック量、接続端末数などの傾向の可視化、ネットワークにおける影響度の高い端末を特定することで、対策強化や有事の際の対応に役立てていただけます。

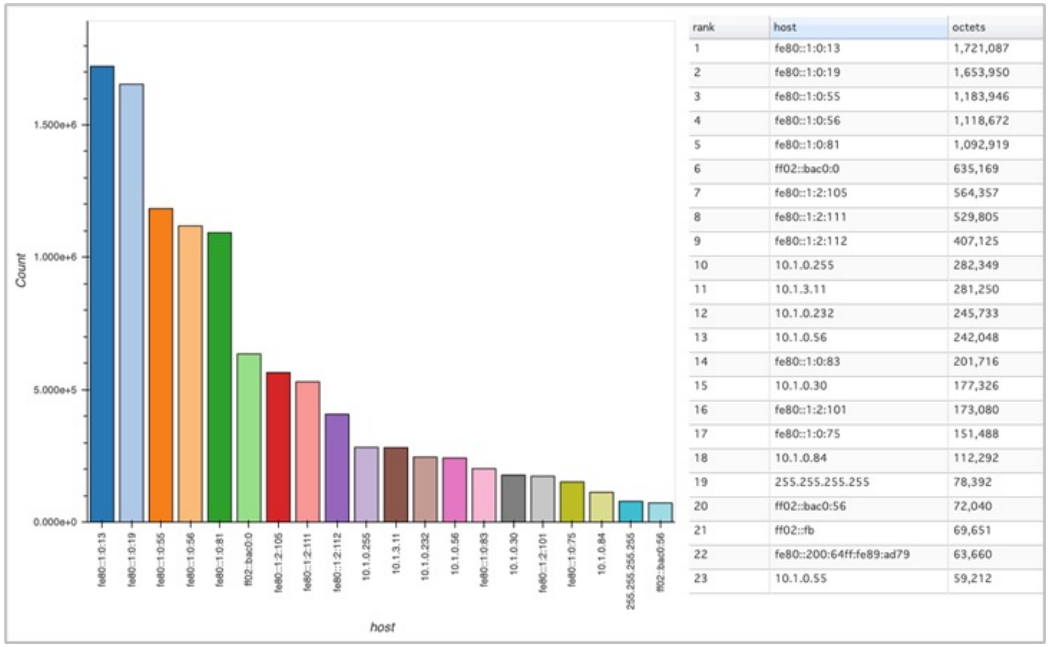
- ネットワークの負荷（使用帯域）を可視化
- ループ等による帯域圧迫を発見

- 接続端末数/トラフィック量が多い端末/サービスを可視化
- OTネットワークの傾向を把握可能

トラフィック



ランキング



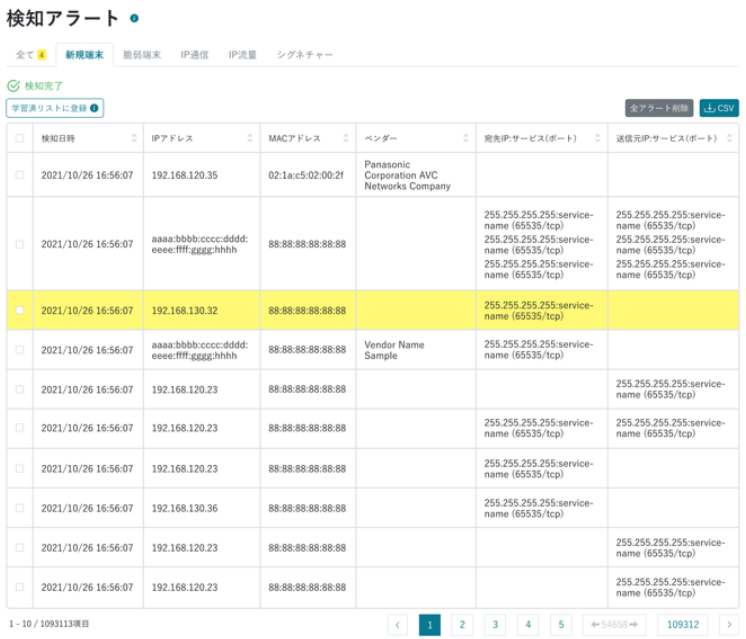
rank	host	octets
1	fe80::1:0:13	1,721,087
2	fe80::1:0:19	1,653,950
3	fe80::1:0:55	1,183,946
4	fe80::1:0:56	1,118,672
5	fe80::1:0:81	1,092,919
6	ff02::bac0:0	635,169
7	fe80::1:2:105	564,357
8	fe80::1:2:111	529,805
9	fe80::1:2:112	407,125
10	10.1.0.255	282,349
11	10.1.3.11	281,250
12	10.1.0.232	245,733
13	10.1.0.56	242,048
14	fe80::1:0:83	201,716
15	10.1.0.30	177,326
16	fe80::1:2:101	173,080
17	fe80::1:0:75	151,488
18	10.1.0.84	112,292
19	255.255.255.255	78,392
20	ff02::bac0:56	72,040
21	ff02::fb	69,651
22	fe80::200:64ff:fe89:ad79	63,660
23	10.1.0.55	59,212

検知 -予防-

新たに接続された端末、未知の通信、サポート切れのOSを使っている端末などを検知・アラート通知することで、お客さまでのリスク対処や予防対応につなげていただけます。

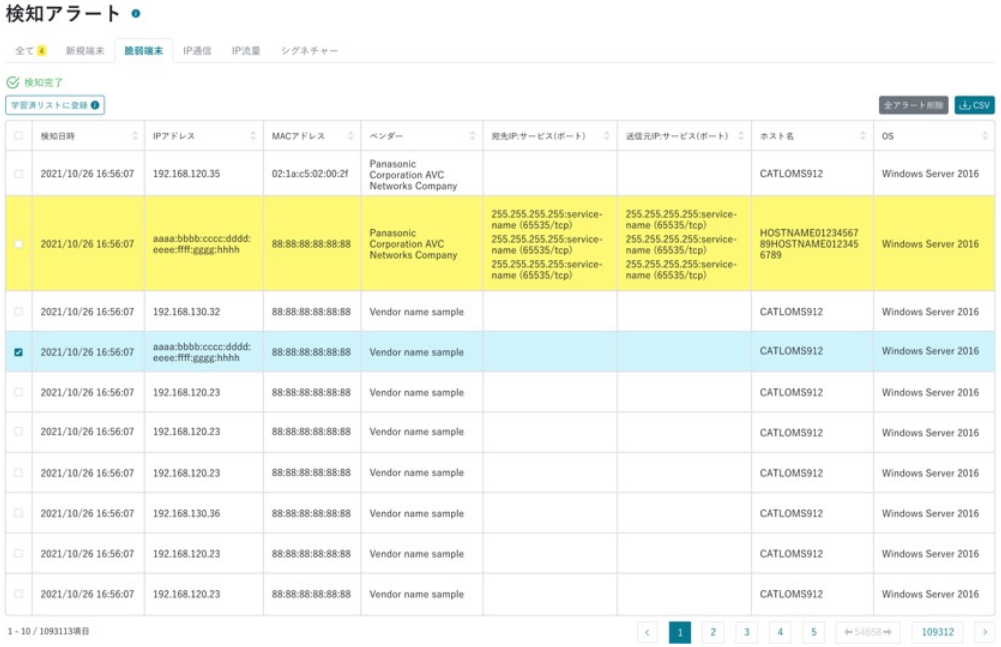
- ネットワーク内の端末アドレスを自動で学習
- 野良端末を見逃さずに早期に発見

新規端末検知



- サポート切れのOSを利用する端末を自動検出
- リスクの高い端末を見逃さず早期に発見

脆弱端末検知

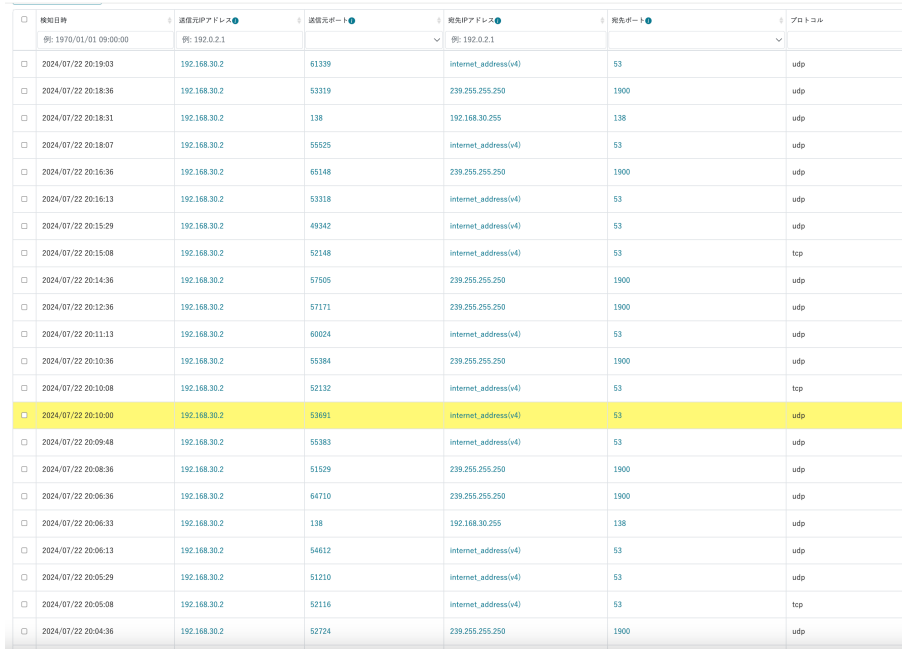


検知 -異常の早期発見-

マルウェア感染等の異常が発生した場合、その挙動（定常業務でなかった通信の発生やトラフィック量の増減など）を検知・アラート通知することで、お客さまでの早期対応・影響の極小化につなげていただけます。

- ネットワーク内の通信情報を自動で学習
- 未知の通信を逃さず早期に発見

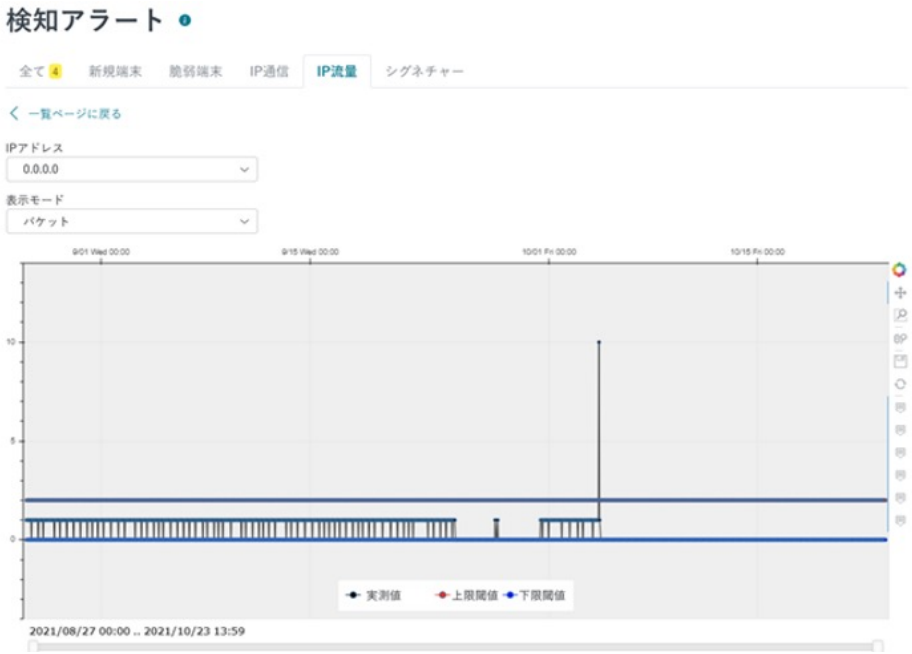
IP通信検知



検知日時	送信元IPアドレス	送信元ポート	宛先IPアドレス	宛先ポート	プロトコル
例: 1970/01/01 09:00:00	例: 192.0.2.1		例: 192.0.2.1		
2024/07/22 20:19:03	192.168.30.2	61339	internet_address(v4)	53	udp
2024/07/22 20:18:36	192.168.30.2	53319	239.255.255.250	1900	udp
2024/07/22 20:18:31	192.168.30.2	138	192.168.30.255	138	udp
2024/07/22 20:18:07	192.168.30.2	55525	internet_address(v4)	53	udp
2024/07/22 20:16:36	192.168.30.2	65148	239.255.255.250	1900	udp
2024/07/22 20:16:13	192.168.30.2	53318	internet_address(v4)	53	udp
2024/07/22 20:15:29	192.168.30.2	49342	internet_address(v4)	53	udp
2024/07/22 20:15:08	192.168.30.2	52148	internet_address(v4)	53	tcp
2024/07/22 20:14:36	192.168.30.2	57505	239.255.255.250	1900	udp
2024/07/22 20:12:36	192.168.30.2	57171	239.255.255.250	1900	udp
2024/07/22 20:11:13	192.168.30.2	60024	internet_address(v4)	53	udp
2024/07/22 20:10:36	192.168.30.2	55384	239.255.255.250	1900	udp
2024/07/22 20:10:08	192.168.30.2	52132	internet_address(v4)	53	tcp
2024/07/22 20:10:00	192.168.30.2	53691	internet_address(v4)	53	udp
2024/07/22 20:09:48	192.168.30.2	55383	internet_address(v4)	53	udp
2024/07/22 20:08:36	192.168.30.2	51529	239.255.255.250	1900	udp
2024/07/22 20:06:36	192.168.30.2	64710	239.255.255.250	1900	udp
2024/07/22 20:06:33	192.168.30.2	138	192.168.30.255	138	udp
2024/07/22 20:06:13	192.168.30.2	54612	internet_address(v4)	53	udp
2024/07/22 20:05:29	192.168.30.2	51210	internet_address(v4)	53	udp
2024/07/22 20:05:08	192.168.30.2	52116	internet_address(v4)	53	tcp
2024/07/22 20:04:36	192.168.30.2	52724	239.255.255.250	1900	udp

- 端末ペア毎に定常業務のトラフィック量を学習
- 時間帯毎の閾値を自動で算出

IP流量検知



検知 -異常の早期発見-

既知のリスクの高い通信パターンに同じマッチした検知・アラートすることで、お客さまでの早期対応・影響の極小化につなげていただけます。

- システムに影響を与えるOTコマンドを検知
- 検知対象のコマンドや端末はカスタマイズ可能

OT振舞検知

検知日時	送信元IPアドレス	送信元ポート	宛先IPアドレス	宛先ポート	プロトコル	OTプロトコル	ファンクション
例: 1970/01/01 09:00:00	例: 192.168.2.0/24		例: 192.168.2.0/24				
2024/07/23 02:54:44	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:54:44	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:50:18	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:50:18	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:45:44	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:45:44	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:41:18	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:41:18	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:36:44	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:36:44	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:32:17	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:32:17	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes
2024/07/23 02:27:44	172.16.134.128	61450	172.16.134.255	61450	udp	cclink_ie_field_basic	cyclicDataReq cyclic
2024/07/23 02:27:44	172.16.134.129	61450	172.16.134.128	61450	udp	cclink_ie_field_basic	cyclicDataRes

- 既知の攻撃パタンにマッチした通信を検知

シグネチャー検知

検知日時	送信元IPアドレス	送信元ポー…	宛先IPアドレス	宛先ポート	プロトコル	シグネチャー	脅威カテゴリ	深刻度
例: 1970/01/01 09:00:00	例: 192.0.2.1		例: 192.0.2.1					
2024/07/23 02:56:26	205.185.216.42	80	10.10.7.101	49737	tcp	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	Misc activity	3
2024/07/23 02:56:16	205.185.216.42	80	10.10.7.101	49737	tcp	ET POLICY PE EXEまたはDLL Windowsファイルのダウンロード HTTP	Potential Corporate Privacy Violation	1
2024/07/23 02:52:54	192.168.1.114	1058	173.194.135.86	80	tcp	ET ポリシー 古い Flash バージョン M1	Potential Corporate Privacy Violation	1
2024/07/23 02:51:59	205.185.216.42	80	10.10.7.101	49737	tcp	ET INFO EXE IsDebuggerPresent (Used in Malware Anti-Debugging)	Misc activity	3
2024/07/23 02:51:50	205.185.216.42	80	10.10.7.101	49737	tcp	ET POLICY PE EXEまたはDLL Windowsファイルのダウンロード HTTP	Potential Corporate Privacy Violation	1
2024/07/23 02:49:13	192.168.1.114	63675	8.8.8.8	53	udp	.cc TLD の ET DNS クエリ	Potentially Bad Traffic	2
2024/07/23 02:49:13	192.168.1.114	54389	8.8.8.8	53	udp	.cc TLD の ET DNS クエリ	Potentially Bad Traffic	2
2024/07/23 02:49:13	209.203.50.200	443	192.168.1.114	1789	tcp	ET MALWARE ABUSE.CH SSL フィンガープリント ブラックリスト 悪意のある SSL 証明書が検出されました (Shylock/URLzone/Gootkit/Zeus Panda C2 の可能性があります)	Domain Observed Used for C2 Detected	1
2024/07/23 02:49:13	192.168.1.114	63674	8.8.8.8	53	udp	.cc TLD の ET DNS クエリ	Potentially Bad Traffic	2
2024/07/23 02:49:13	192.168.1.114	65043	8.8.8.8	53	udp	.cc TLD の ET DNS クエリ	Potentially Bad Traffic	2
2024/07/23 02:49:13	192.168.1.114	49305	8.8.8.8	53	udp	.cc TLD の ET DNS クエリ	Potentially Bad Traffic	2
2024/07/23 02:49:13	177.55.106.46	443	192.168.1.114	2233	tcp	ET MALWARE ABUSE.CH SSL フィンガープリント ブラックリスト 悪意のある SSL 証明書が検出されました (Shylock/URLzone/Gootkit/Zeus Panda C2 の可能性があります)	Domain Observed Used for C2 Detected	1

まとめ

- 制御システムのネットワーク化・デジタル化に伴い、IT環境のみならずOT環境も被害に遭う時代に
- 大手企業だけではなく、サプライチェーン全体が攻撃対象に
- OT環境のセキュリティ対策として、資産の可視化と常時監視が重要だが、既存ソリューションに多くの課題がある
- NTT Comは低価格で簡単導入・運用可能可能な、制御システムの資産とリスクを可視化する国産OT-IDS「OsecT」を提案