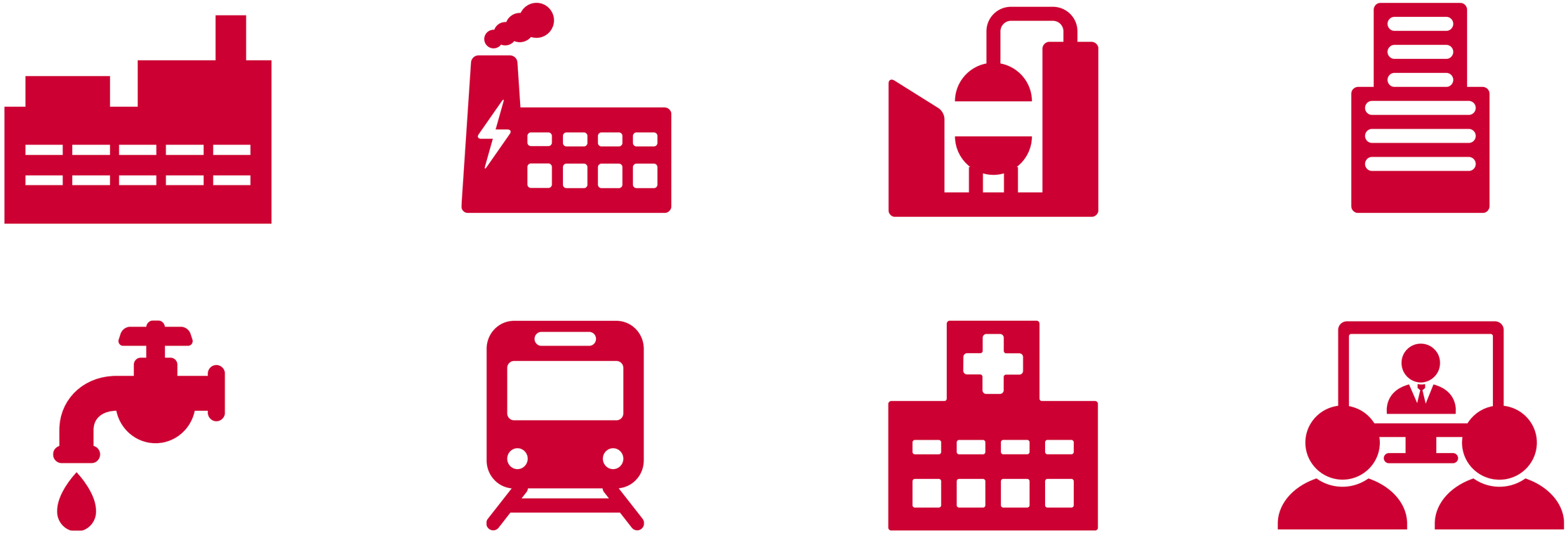
制御システム(OT)向け国産セキュリティ OsecT（オーセクト）のご紹介

2025年6月11日

NTTコミュニケーションズ株式会社

Operational Technology (OT) とは

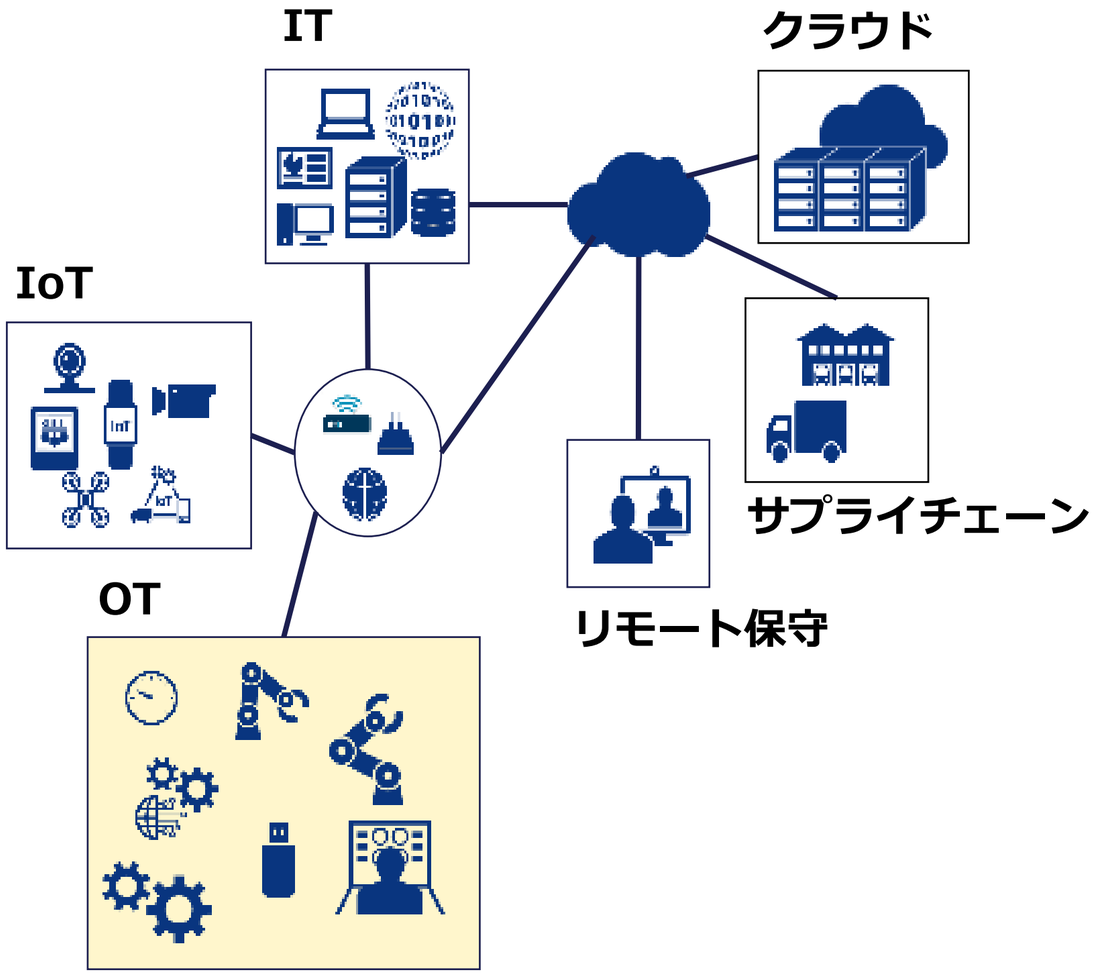
- 製造業、エネルギー、重工業、建物、公共事業、輸送、医療、放送などの産業分野において、設備・システムを最適に動かすための技術
- 情報技術（Information Technology, IT）と対比されることが多い



OTの一例

製造業を取り巻く環境とサイバー攻撃

製造業を取り巻く環境



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

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**

アルミニウム製造（従業員2万人）

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）

自動車製造（グループ従業員20万人）

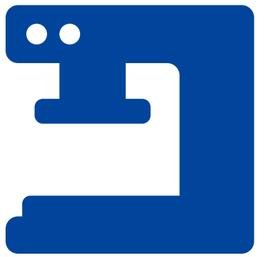
EKANSまたSNAKEに感染した影響で、自動車工場2拠点の出荷が一時停止。海外にも感染が波及し、**海外9拠点の生産が1~3日間停止**。
（2020年@日本 ）

金属製品メーカ（従業員100人）

PCとサーバの合計25台がAvaddonに感染。データ復旧作業や感染経路の調査のため、**業務の完全正常化まで1ヶ月以上**を要した。
（2021年@日本）

自動車部品製造（従業員1500人）

子会社が設置した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、取引先の**大手自動車生産工場（14工場28ライン）が停止**
（2022年@日本）



制御システム向けセキュリティ製品の要件

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

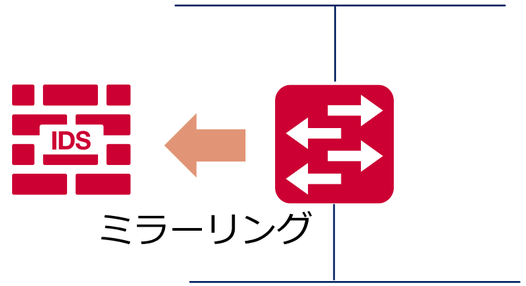
資産管理

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）



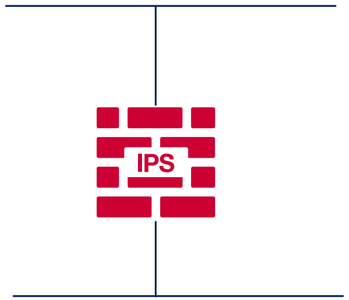
IDS (Intrusion Detection System)
不正侵入検知システム
→ パッシブ型・・・OTへの適用事例が多い

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」

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。

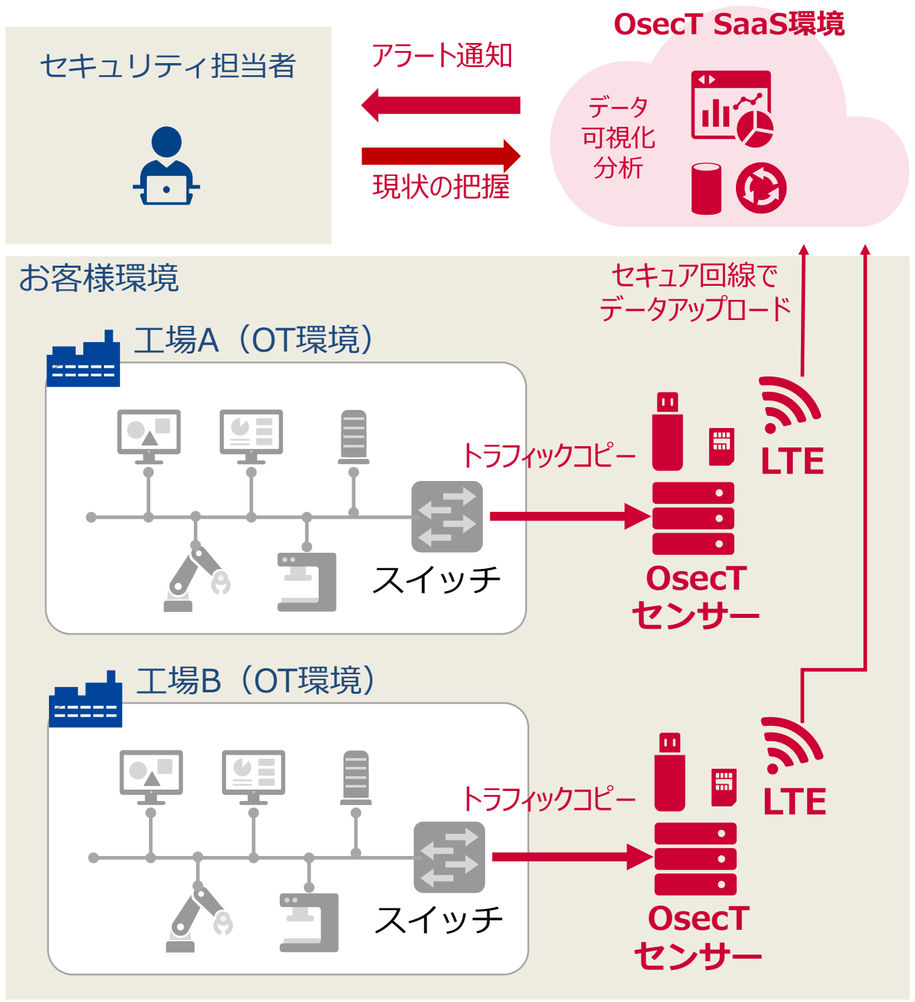
OTネットワーク可視化

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



※SaaS環境を使用しないオンプレミス版OsecTも個別相談にてご提供

可視化と脅威検知

通信の分析で資産、ネットワーク、セキュリティリスクを可視化
不審端末/不審通信などを早期に検知

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

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

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 [NEW]

セキュリティ運用サポートサービス付きプランの提供

資料・お問合せ先一覧

- Interop Tokyo 2025 OsecT/OTセキュリティ展示資料ダウンロードページ
  - Interop Tokyo 2025「NTTコミュニケーションズのOT・生産現場向けセキュリティソリューション」の展示資料などをダウンロード可能です。
- WideAngle OsecT
  - 工場・製造現場のセキュリティ対策サービス OsecT の紹介ページです。
- WideAngle OsecTに関する各種ダウンロード
  - ユーザーガイド、センサー設置手順書、サービス仕様書などがダウンロード可能です。

Interop Tokyo 2025向け資料配布QRコード

https://wa-osect.ntt.com/interop2025/

OsecT 機能紹介

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。

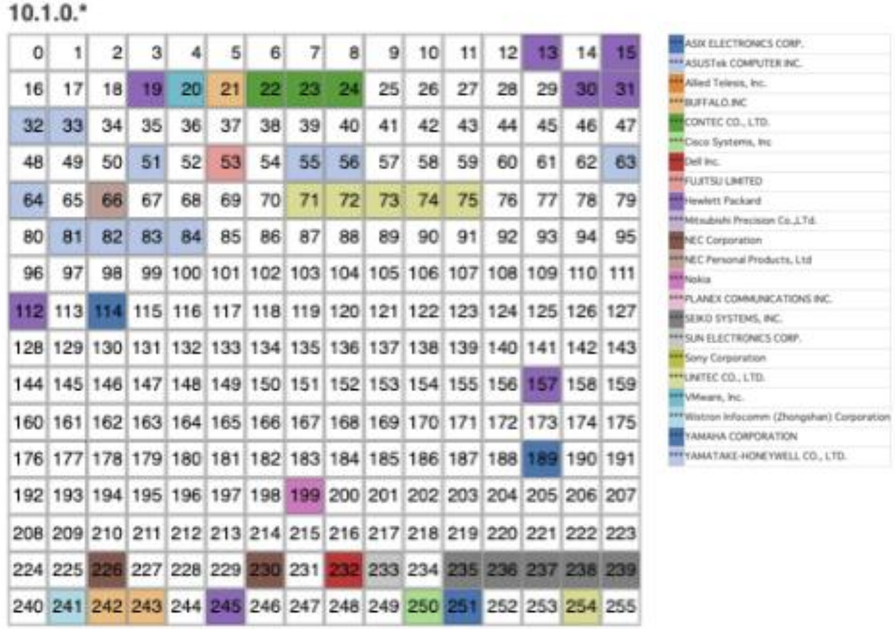
- 自動で端末情報を一覧化
- 端末一覧をCSVファイルで出力し、台帳として利用可能

- 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



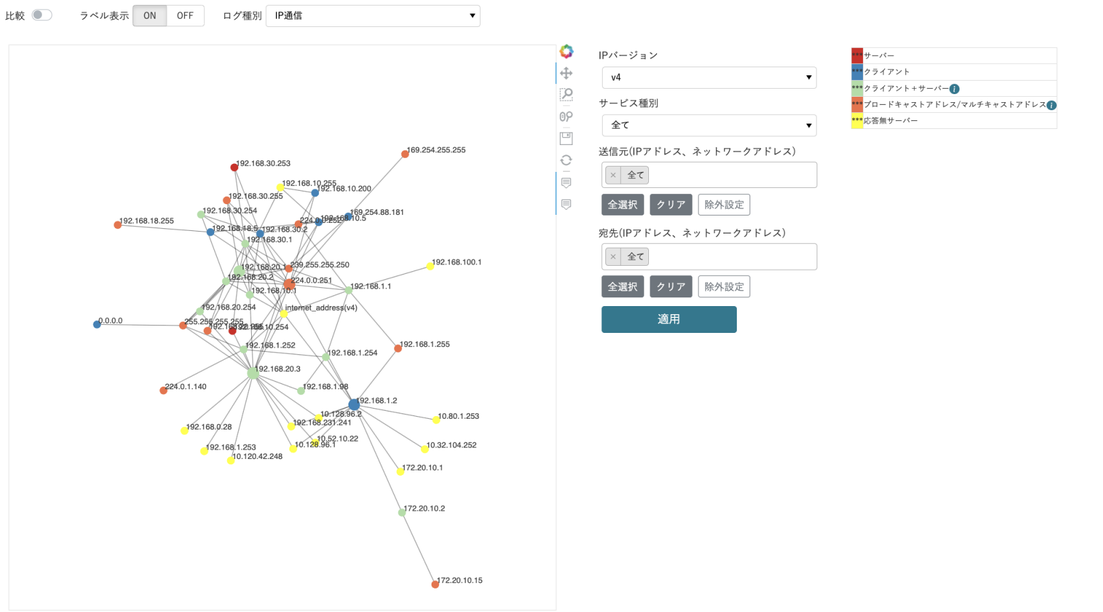
可視化 -端末・ネットワーク-

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。

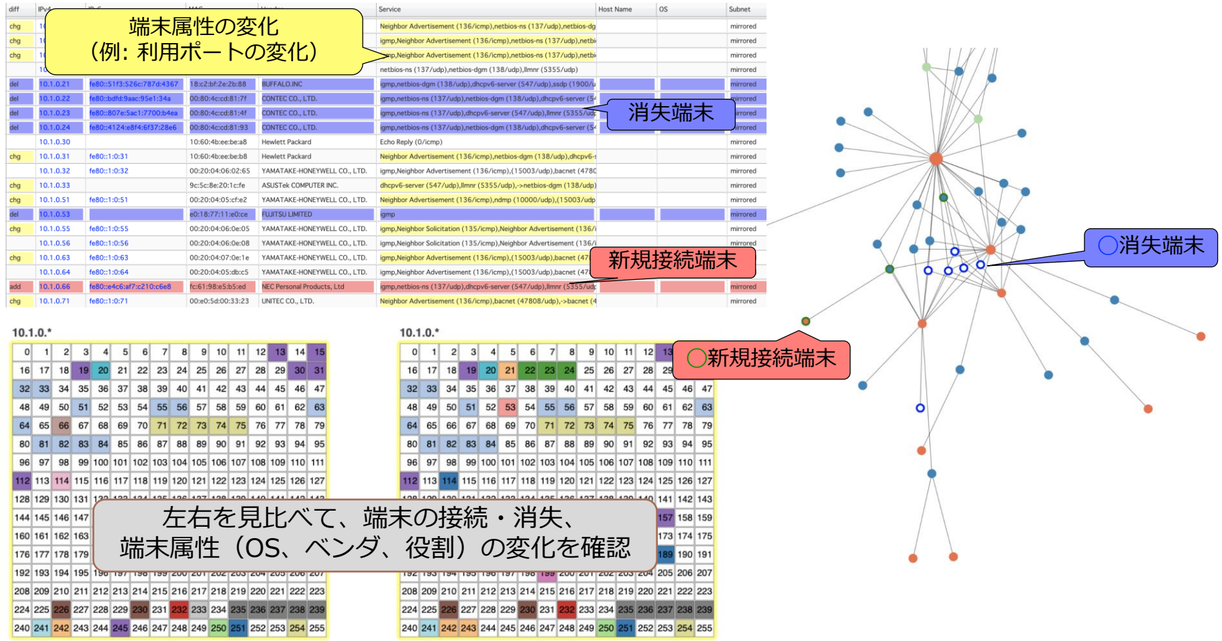
- 端末の通信接続関係をマップ形式で可視化
- 表示データは画像で出力可能

- 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



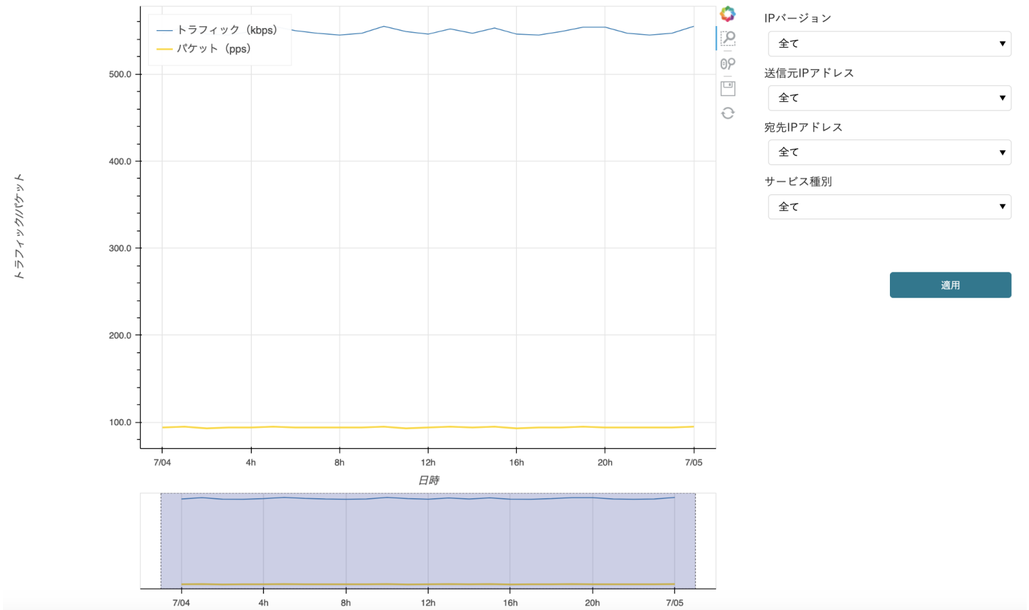
可視化 -ネットワーク-

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。

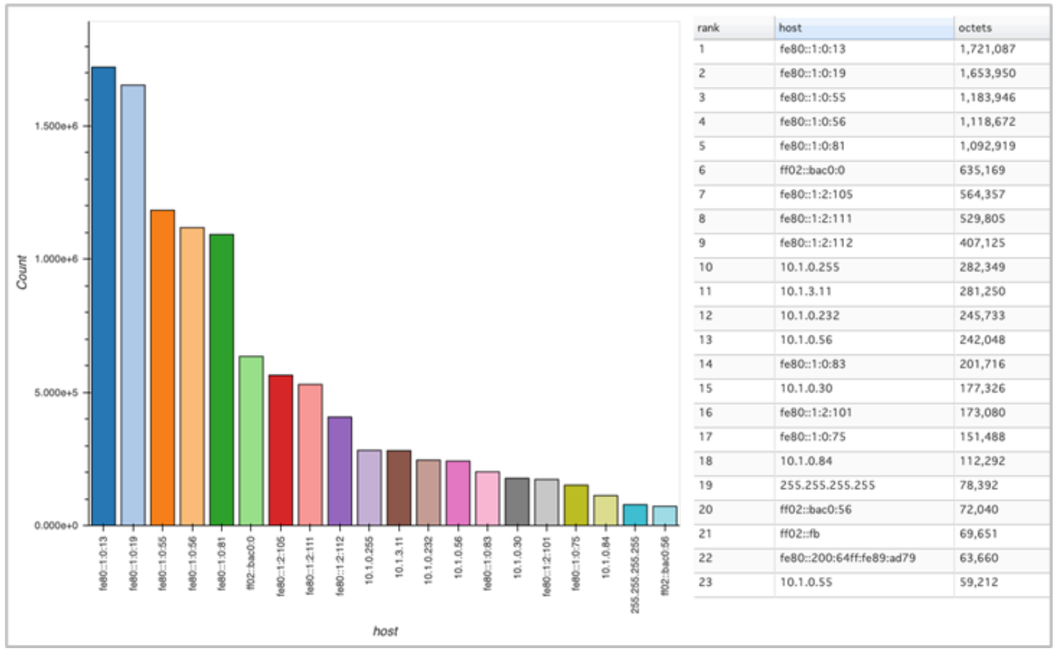
- ネットワークの負荷（使用帯域）を可視化
- ループ等による帯域圧迫を発見

- 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



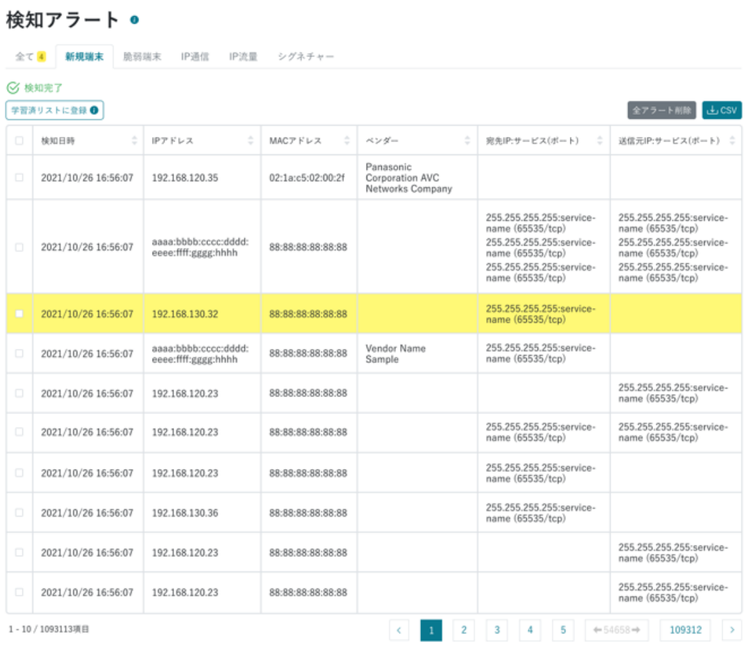
rank	host	octets
1	fe80::1:0:13	1,721,087
2	fe80::1:0:19	1,653,950
3	fe80::1:0:55	1,183,946
4	fe80::1:0:56	1,118,672
5	fe80::1:0:81	1,092,919
6	ff02::bac0:0	635,169
7	fe80::1:2:105	564,357
8	fe80::1:2:111	529,805
9	fe80::1:2:112	407,125
10	10.1.0.255	282,349
11	10.1.3.11	281,250
12	10.1.0.232	245,733
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。

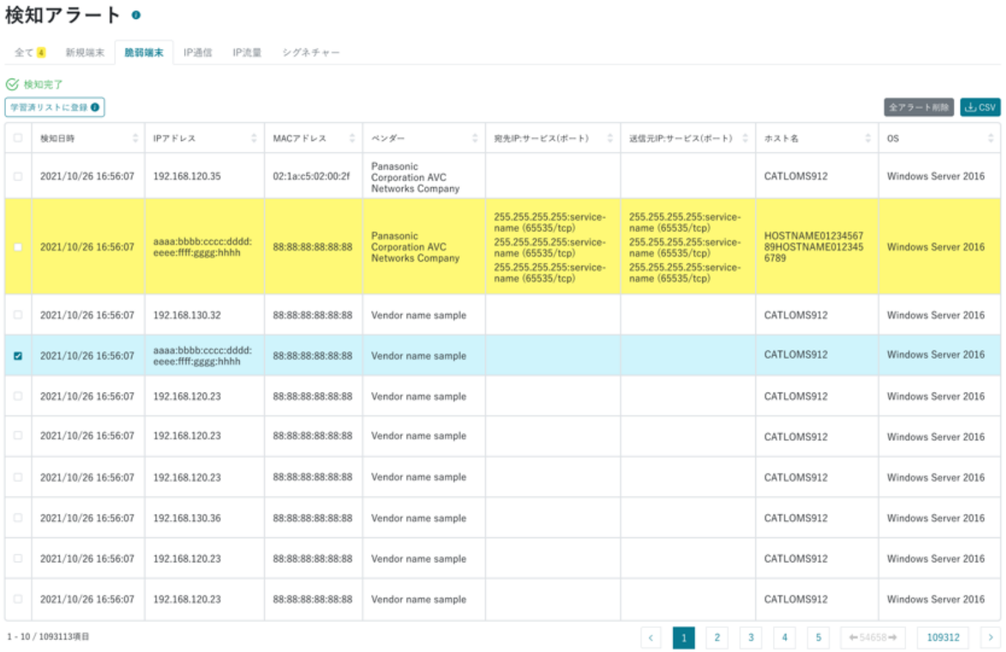
- ネットワーク内の端末アドレスを自動で学習
- 野良端末を見逃さずに早期に発見

接続端末検知



- 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

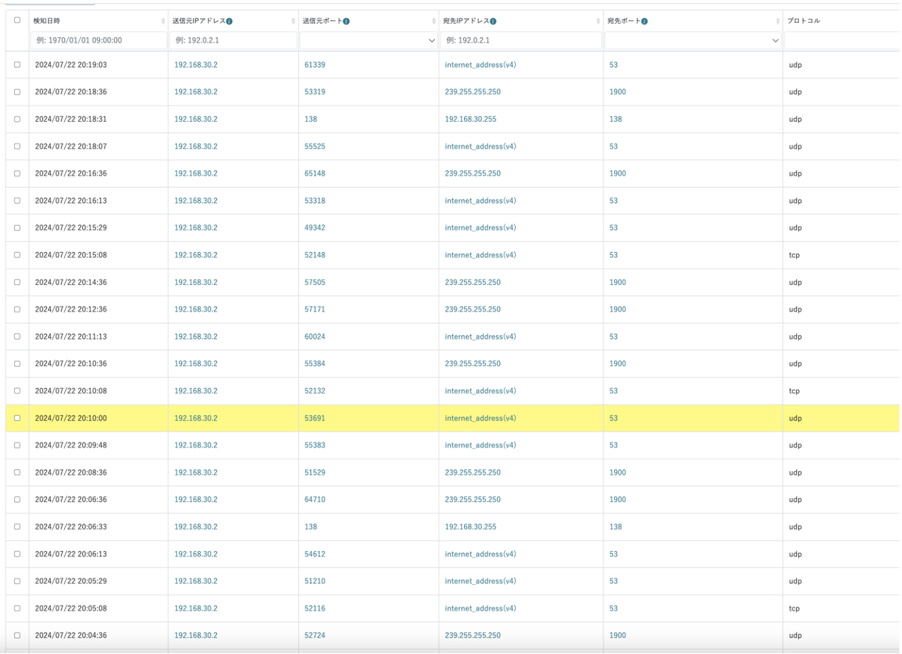


検知 -異常の早期発見-

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

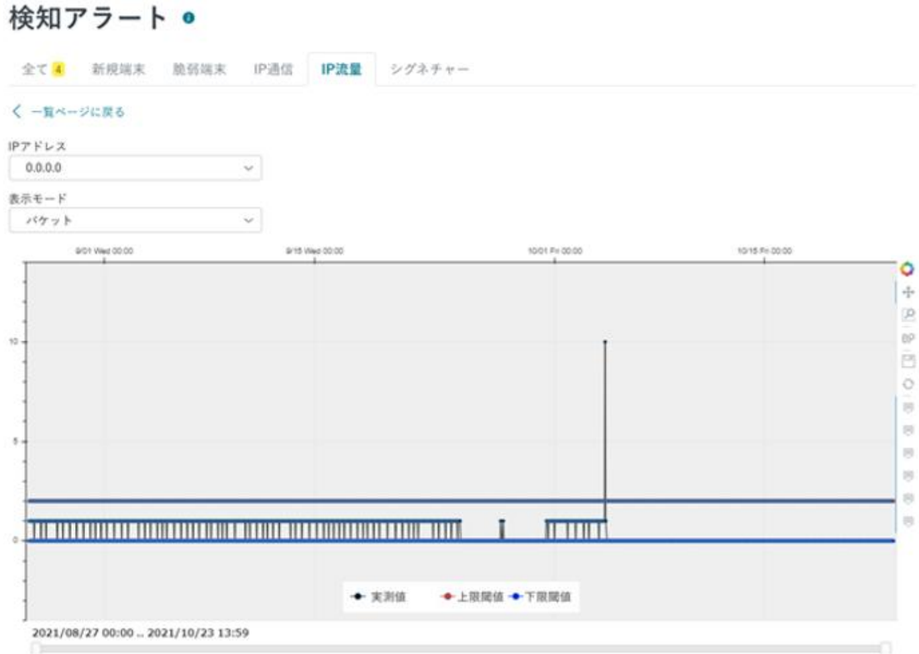
IP通信検知



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

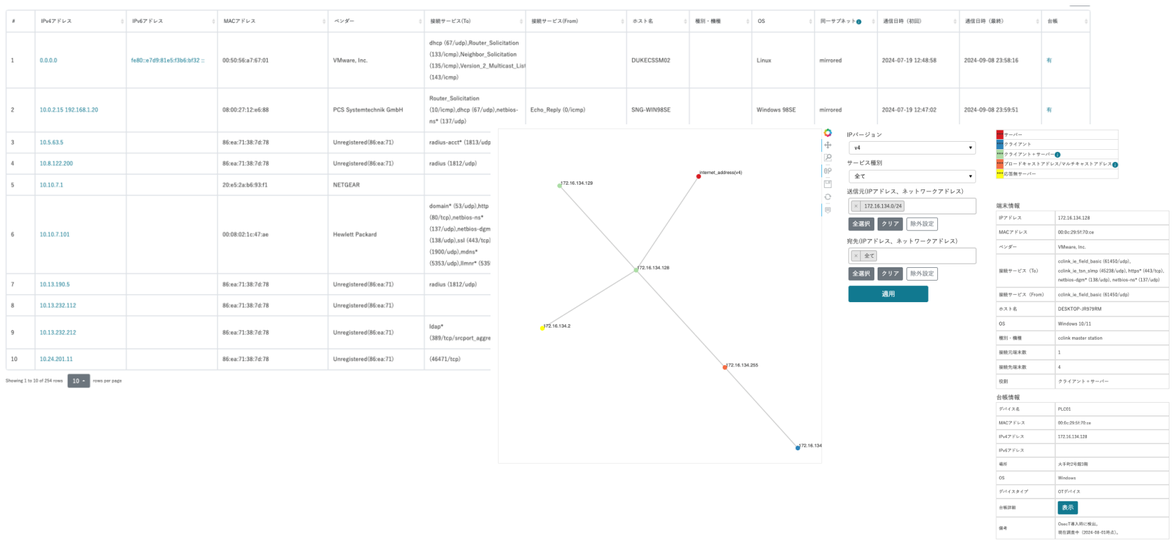
台帳連携 -端末管理やアラート対応の効率化-

既存の資産管理ソフトから台帳データを取り込むことで、OsecTの各種機能と連携し、端末管理や不審端末の検出時の業務の効率化に役立てていただけます。

端末情報を端末一覧やネットワークマップと連携

端末設置場所や設置時期などの情報も併せて表示

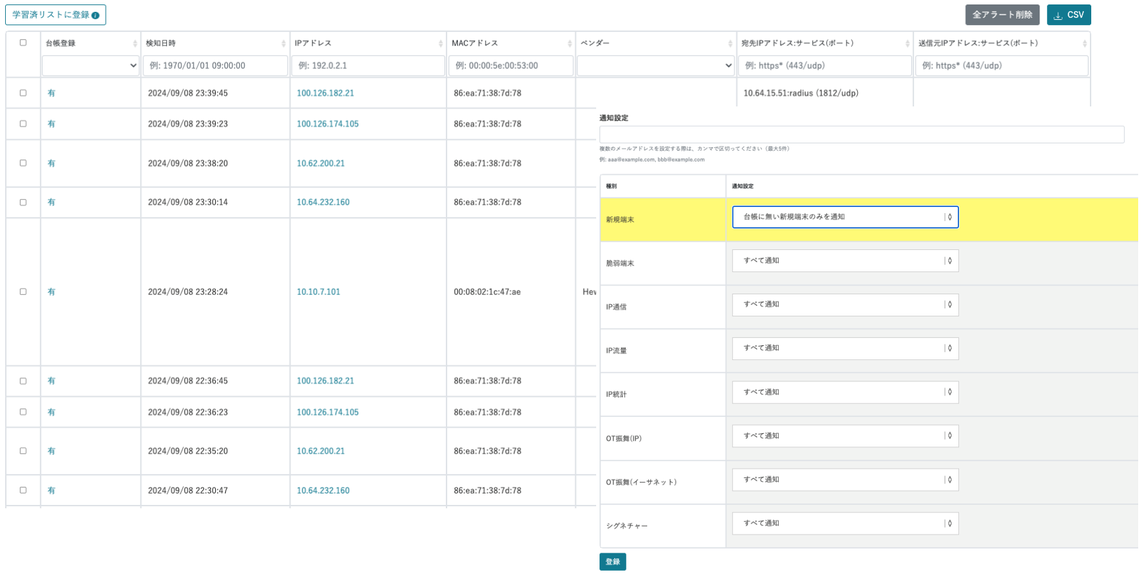
端末一覧/ネットワークマップ機能との連携



台帳情報を接続端末検知機能と連携

アラート画面に台帳有無を表示
端末情報に基づくメール通知の発出条件を設定可能

接続端末検知機能との連携



アセスメント

ボタン一つでネットワークに接続されている資産やリスクの可視化レポートを出力、ポイントを絞ったレポートにより、対策強化や改善の優先順位付けや有事の際の対応に役立てていただけます。

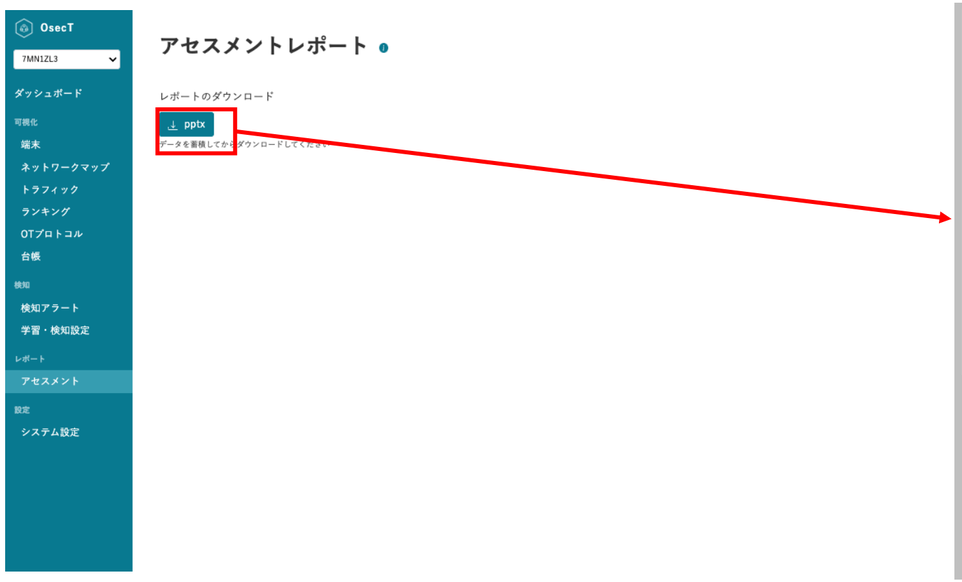
ボタン一つでレポート出力

端末資産やサポート切れのOS端末を一覧化

編集可能なパワーポイント形式で出力

トラフィック量や平文通信、RDP通信なども可視化

アセスメント機能



アセスメントレポートファイル

OsecTからの検知アラートメール例

【OsecT】12件の新着アラートがあります

N noreply@[redacted]
宛先 [redacted]

OsecT の検知アラートの自動メール通知です。

12 件の新着アラートがあります。
（内訳）
OT 振舞(イーサネット): 6 件
接続端末: 3 件
OT 振舞(IP): 2 件
IP 通信: 1 件

アラートの一覧は OsecT 検知アラートページにてご確認いただけます。
https://[redacted]

- 検知日時：2024/12/25 15:19:52
- 検知種別：接続端末
- 詳細：https://[redacted]

- 検知日時：2024/12/25 15:19:55
- 検知種別：接続端末
- 詳細：https://[redacted]

- 検知日時：2024/12/25 15:19:43
- 検知種別：IP 通信
- 詳細：https://[redacted]

- 検知日時：2024/12/25 15:19:45
- 検知種別：OT 振舞(IP)
- 詳細：https://[redacted]