

WideAngle プロフェッショナルサービス OsecT（オーセクト）ユーザーガイド

バージョン 2.90

NTT コミュニケーションズ株式会社
2024 年 3 月 28 日

目次

1. はじめに	4
2. 基本的な使い方	7
2.1. 端末	7
2.2. ネットワークマップ	7
2.3. トラフィック	7
2.4. ランキング	7
2.5. OT プロトコル	7
2.6. 検知アラート	8
2.7. 学習・検知設定	8
2.8. 補足：サービス名の表記について	8
2.9. 補足：制限事項	10
3. 画面左メニュー	11
4. ダッシュボード	12
5. 端末	14
5.1. 一覧（◎：オススメ機能）	14
5.2. 一覧（IP）	17
5.3. 詳細	19
5.4. ベンダーマトリクス（◎：オススメ機能）	21
5.5. OS マトリクス	23
5.6. 役割マトリクス	25
6. ネットワークマップ	27
6.1. 端末（◎：オススメ機能）	27
6.2. サービス	31
7. トラフィック	34
8. ランキング	36
8.1. 端末トラフィック量	36
8.2. 端末接続数	38
8.3. 端末重要度	40
8.4. サービストラフィック量	43
8.5. サービス別端末数	45
8.6. ベンダー別端末数	47
9. OT プロトコル	48
9.1. 一覧（IP）	48
9.2. 一覧（イーサネット）	50

10. 検知アラート	53
10.1. 全て	53
10.2. 新規端末 (◎：オススメ機能)	55
10.3. 脆弱端末 (◎：オススメ機能)	57
10.4. IP 通信	59
10.5. IP 流量	61
10.6. IP 統計	65
10.7. OT 振舞 (IP)	67
10.8. OT 振舞 (イーサネット)	69
10.9. シグネチャー	71
11. 学習・検知設定	73
11.1. 学習・検知ステータス	73
11.2. 学習・検知ステータス (アドバンスモード)	75
11.3. 新規端末	77
11.4. 脆弱端末	80
11.5. IP 通信	82
11.6. IP 流量	86
11.7. IP 統計	90
11.8. OT 振舞 (IP)	93
11.9. OT 振舞 (イーサネット)	97
11.10. シグネチャー	100
11.11. 全般	103
11.12. 全般 (アドバンスモード)	106
12. システム設定	112
12.1. 設定変更	112
12.2. システムログ	116
12.3. センサー管理	118
12.4. ユーザー管理	120
12.5. サービス名管理	128
改訂履歴	131

1. はじめに

本資料では、OsecT の Web 画面の操作方法について説明します。 推奨ブラウザは Google Chrome です。

ログイン手順は以下の通りです。

1. ブラウザーから開通案内に記載された URL へアクセスします。



2. 以下の画面が表示された場合は、弊社提供のログイン情報（ユーザーID とパスワード）を入力して「ログイン」を押下します。

A screenshot of the "ID Federation" login page. It features two input fields: "ユーザーID" (User ID) with the text "@ntt.com" and "パスワード" (Password) with masked characters. Below the password field is a checkbox labeled "ユーザーIDを記憶する" (Remember User ID) and a link "パスワードを変更する" (Change Password) / "パスワードを忘れた" (Forgot Password). A green "ログイン" (Login) button is highlighted with a red rectangle at the bottom right.

3. 以下の画面が表示された場合は、現在のパスワードと新しいパスワードを入力後、「送信」ボタンを押して、パスワード変更を行ってください。

ID Federation

現在のパスワードおよび新しいパスワードを入力してください。

あなたのパスワードは、ログイン前に変更する必要があります。
パスワードを変更して再度お試しください。

現在のパスワード

新しいパスワード

新しいパスワード(確認用)

送信

以下の画面が表示されたらパスワード変更が成功です。「ID Federation サービスに戻る」ボタンを押下してください。

ID Federation

パスワード変更に成功しました。以下のリンクをクリックして処理を継続してください。

ID Federationサービスに戻る

- 以下の画面が表示された場合は、表示されているメールアドレスに届いたメールに記載されているワンタイムパスワードを入力し、「送信」を押下してください。

ID Federation

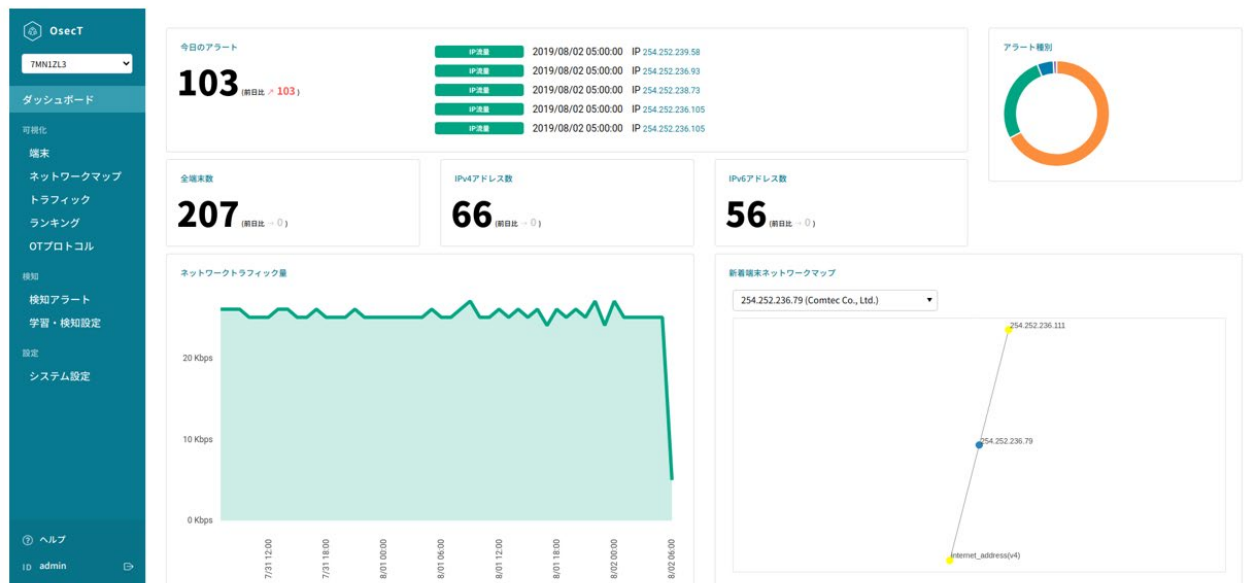
*****@nt*****に届いたワンタイムパスワードを確認してください。

ワンタイムパスワード

もう一度ワンタイムパスワードを送信する

送信

5. OsecT のダッシュボード画面が表示されます。



2. 基本的な使い方

OsecT（オーセクト）では、OsecT センサーが OT（Operational Technology）ネットワークでキャプチャしたパケットデータをリアルタイム（1 分ごと）に通信ログに変換した上でクラウドに送信、クラウドが通信ログをインポート、データ解析することで、OT ネットワークの可視化や、脅威・脆弱性の検知をできます。

カテゴリごとの各画面の機能は以下のとおりです。

2.1. 端末

- OT ネットワークに接続している端末の情報を一覧表示等で確認できます。
- OT ネットワークに接続している端末の情報をサブネットごとのマトリクスで視覚的に確認できます。

2.2. ネットワークマップ

OT ネットワークに接続している端末間の接続関係等をネットワークマップで視覚的に確認できます。

2.3. トラフィック

OT ネットワーク内に流れるトラフィック量を確認できます。

2.4. ランキング

OT ネットワークに関する各種情報をランキング形式で確認できます。

2.5. OT プロトコル

OT プロトコルに関する情報を確認できます。

2.6. 検知アラート

OT ネットワークに関する脅威検知の検知結果を確認できます。

- 新規端末
- 脆弱端末
- IP 通信
- IP 流量
- IP 統計
- OT 振舞 (IP)
- OT 振舞 (イーサネット)
- シグネチャー

2.7. 学習・検知設定

OT ネットワークに関する脅威検知のための学習や検知処理を実行できます。

- 新規端末
- 脆弱端末
- IP 通信
- IP 流量
- IP 統計
- OT 振舞 (IP)
- OT 振舞 (イーサネット)
- シグネチャー

2.8. 補足 : サービス名の表記について

一般的なサービス名は以下のように「サービス名 (宛先ポート番号/トランスポート・プロトコル)」を表示します。

例) http (80/tcp)

サービス名がない場合は宛先ポート番号とトランスポート・プロトコルのみ表示します。

例) (999/udp)

ポート番号に基づくサービス名の場合は、サービス名の後ろに「*（アスタリスク）」が付きます。このサービス名はサービス名管理機能で任意の名称に変更することができます。

例) http* (8080/tcp)

パケットの内容から判定したサービス名の場合は、「*（アスタリスク）」なしとなります。このサービス名はサービス名管理機能で他の名称に変更することはできません。

例) http (80/tcp)

送信元ポート番号が1つで宛先ポート番号が複数存在している場合、サービス名は以下のような表示になり、トランスポート・プロトコルの後に `srcport_aggregated` と表示します。この場合、ポート番号は送信元ポート番号を表示します。

例) svrloc (427/udp/srcport_aggregated) ,
(999/udp/srcport_aggregated)

送信元ポート及び宛先ポート番号の両方が複数存在している場合のサービス名は以下のような表示になり、宛先ポート番号の最小と最大のポート番号をハイフンで区切って表示します。

例) ftp-data (1024-19999/tcp)

また、パケットの内容から判定したサービスでないサービスは名前を「many-high-ports」と表示します。

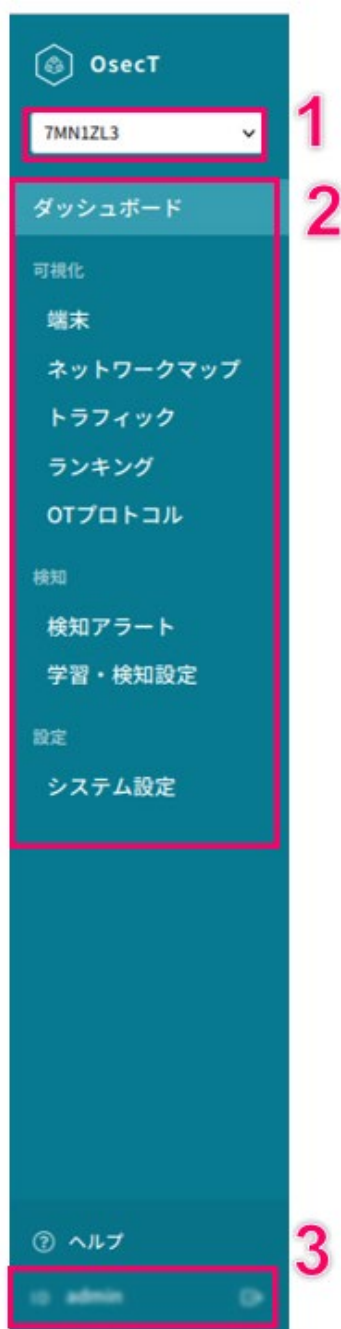
例) many-high-ports (1024-19999/udp)

2.9. 補足：制限事項

ループバックアドレスに対する通信ログは分析対象外となります。

3. 画面左メニュー

全画面では画面左側にメニューが表示されます。 センサーをプルダウン（下図 1）で選択して、表示するセンサーを選択できます。 画面名（下図 2）を押下すると、該当する画面が表示されます。 左メニュー最下部にログインしたユーザーID（下図 3）が表示されます。 ユーザーID には自動的に「@osect」が付与されます。



4. ダッシュボード

OsecT の TOP 画面です。インポートしたデータの各種集計結果を表示する画面です。

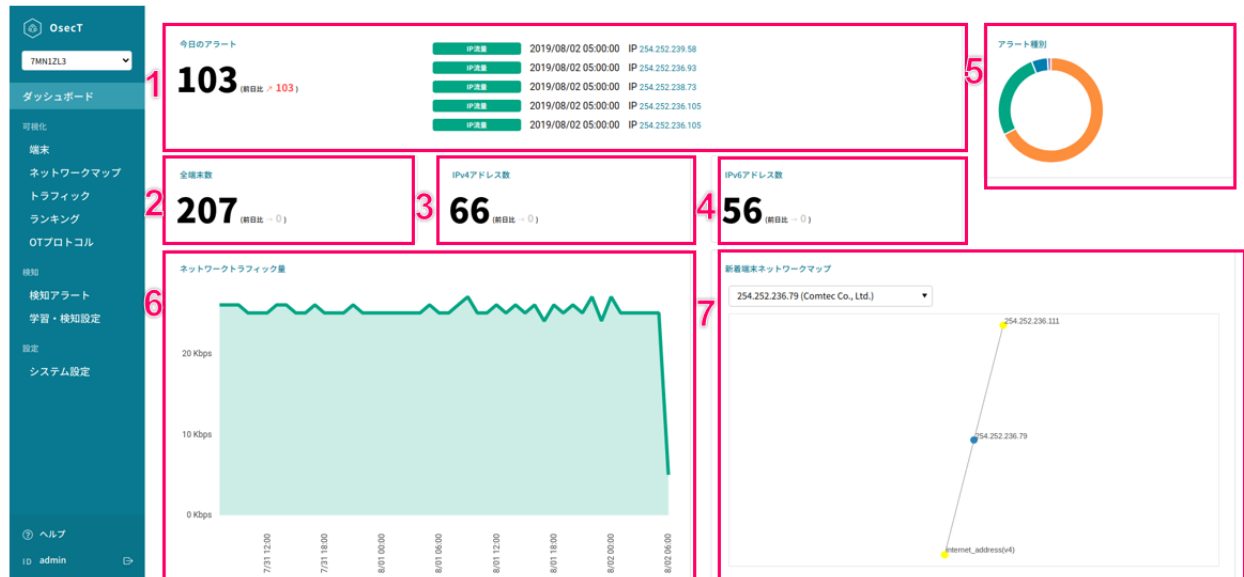


図. ダッシュボード画面

1. 今日のアラート

各検知機能で本日検知されたアラート数を表示します。 前日比は、前日に検知されたアラート数との差分を表示します。 本日検知されたアラート情報を最大 5 件表示します。

2. 全端末数

集計した端末数を表示します。 端末一覧画面で表示する端末数と一致します。 前日比は、前日以前のデータから集計した端末数との差分を表示します。

3. IPv4 アドレス数

集計した IPv4 アドレス数を表示します。 前日比は、前日以前のデータから集計した IPv4 アドレス数との差分を表示します。

4. IPv6 アドレス数

集計した IPv6 アドレス数を表示します。 前日比は、前日以前のデータから集計した IPv6 アドレス数との差分を表示します。

5. アラート種別

本日検知されたアラートを種別単位で集計した割合をグラフで表示します。

- 赤色：シグネチャーで検知された割合
- オレンジ色：IP 通信で検知された割合
- 濃い緑色：IP 流量で検知された割合
- 青色：新規端末で検知された割合
- 紫色：脆弱端末で検知された割合
- 黄色：OT 振舞（IP）で検知された割合
- 緑色：OT 振舞（イーサネット）で検知された割合
- 濃い赤：IP 統計で検知された割合

を表します。

6. ネットワークトラフィック量

トラフィック量を時系列グラフで表示する画面です。トラフィック量は直近 2 日の期間を表示します。

7. 新着端末ネットワークマップ

新規端末機能で検知した端末とその接続先端末をマップ形式で表示します。新規端末の IP アドレス、ベンダーをプルダウンで選択して表示します。

5. 端末

5.1. 一覧（◎：オススメ機能）

端末情報を一覧表示する画面です。 お手持ちの台帳と突合させることで、管理されていない端末がないか確認できます。台帳の自動生成ツールとして利用することもできます。

OsecT

7MN1ZL3

ダッシュボード

可視化

端末

ネットワークマップ

トラフィック

ランキング

OTプロトコル

通知

検知アラート

学習・検知設定

設定

システム設定

ヘルプ

ID admin

端末

期間設定

比較

全センサー

CSV

注

#	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...	通信日時（初...	通信日時（最...
1	10.0.2.2 127.12.34.56		52:54:00:12:35:02	QEMU				mirrored	2024-02-15 13:42:50	2024-02-15 14:59:57
2	10.0.2.15	fe80::375d:6bc0:f831:f	08:00:27:ca:86:cc	PCS Systemtechnik GmbH		Linux 2.2.x-3.x		mirrored	2024-02-15 13:42:50	2024-02-15 14:59:57
3	62.84.236.72 254.252.236.202		00:26:12:e5:b5:ed	Space Exploration Technologies		Windows 7		mirrored	2019-07-29 17:36:02	2019-08-02 06:35:31
4	62.84.236.72 254.252.236.125		00:26:64:11:e0:ce	Core System Japan		Windows 7		mirrored	2019-07-31 07:09:26	2019-07-31 07:12:01
5	62.84.236.72 254.252.236.88		80:34:57:05:c8:96	OT Systems Limited		Windows 7		mirrored	2019-07-29 17:35:55	2019-08-02 06:35:56

図. 一覧画面

1. 比較選択ボタン

期間指定で指定された2つの期間のデータを比較して、差分表示します。差分表示時にはdiff列が表示されます。

端末

2019/07/29 00:00 - 2019/07/30 00:00
[比較 2019/07/30 00:00 - 2019/07/31 20:00]

一覧

一覧 (IP)

詳細

ベンダーマトリクス

OSマトリクス

役割マトリクス

比較

全センサー

CSV

検索

#	diff	IPv4アドレス	IPv6アドレス	MACアドレス	ベンダー	ホスト名	OS	同一サブネット
1	add	62.84.236.72		b0:99:28:af:e1:74	FUJITSU LIMITED			mirrored
2	chg	111.86.229.92,127.12.34.56->127.12.34.56		94:8fee:02:40:c5	Verizon Telematics	hostname_WIN->	Windows Server 2008R2->	mirrored
3	chg	127.12.34.56 254.252.236.89		00:26:64:72:74:ee	Core System Japan		Windows Server 2008R2->	mirrored
4	chg	internet_address(v4)		14:18:77:f3:aa:cf	Dell Inc.		Windows Server 2008R2->	mirrored
5	chg	internet_address(v4)		94:8fee:28:7c:c5	Verizon Telematics		Windows Server 2008R2->	mirrored
6		254.252.22.222	fe80::168:110:110	fc:cf:62:a5:38:5b	IBM Corp	hostname_RD-	Windows Server 2008R2	mirrored
7		254.252.126.60 254.252.236.187	fe80::168:0:75	80:34:57:00:33:66	OT Systems Limited			mirrored
8	del	254.252.172.77		08:4fa9:82:65:c0	Cisco Systems, Inc			mirrored
9	del	254.252.172.78		08:4fa9:bf:f6:e0	Cisco Systems, Inc			mirrored

図. 一覧画面（差分モード）

diff 列の値	説明
add	期間設定にて比較に指定した範囲には存在せず、期間に指定した範囲には存在する端末（行全体の背景色：赤）
del	期間設定にて比較に指定した範囲には存在し、期間に指定した範囲には存在しない端末（行全体の背景色：青）
chg	期間設定にて比較に指定した範囲と期間に指定した範囲で情報に変化があったデータ（変化があったセルの背景色：黄）
なし	変化なし

2. 全センサー

複数のセンサーを利用している場合にすべてのセンサーの情報を表示します。

3. CSV ダウンロードボタン

ボタンを押下すると、一覧に表示されているデータを CSV ファイルとしてダウンロードします。

4. 表示列指定ボタン

チェックを変更することで、一覧に表示する情報を変更することができます。

5. 一覧

カラム名	説明
IPv4 アドレス	端末の IPv4 アドレス。ミラー対象のサブネットと同一サブネットの場合、MAC アドレスをキーに集約して、半角スペース区切りで複数アドレス表示。
IPv6 アドレス	端末の IPv6 アドレス。ミラー対象のサブネットと同一サブネットの場合、MAC アドレスをキーに集約して、半角スペース区切りで複数アドレス表示。
MAC アドレス	端末の MAC アドレス。
ベンダー	MAC ベンダー名を表示。MAC ベンダーが不明の場合は「unknown」と表示。
接続サービス (To)	端末を送信元とする通信のサービス名。L4 プロトコルが TCP, UDP, ICMP の場合は L4 プロトコル名、ポート番号や ICMP Type 値も合わせて括弧書きで表示。それ以外の L4 プロトコルの場合はサービス名の代わり L4 プロトコル名を表示。
接続サービス (From)	端末を宛先とする通信のサービス名。L4 プロトコルが TCP, UDP, ICMP の場合は L4 プロトコル名、ポート番号や ICMP Type 値も合わせて括弧書きで表示。それ以外の L4 プロトコルの場合はサービス名の代わり L4 プロトコル名を表示。
ホスト名	ホスト名を表示。
OS	OS 名の推定結果を表示。
種別・機種	機器種別を表示。
同一サブネット	ミラー対象のサブネットと同一サブネットと判定した場合「mirrored」、そうでない場合は空白を表示。
通信日時（初回）	端末が最初に通信した日時を表示。画面上部で期間指定した場合でも影響を受けない。

通信日時（最終）	端末が最後に通信した日時を表示。画面上部で範囲指定した場合でも影響を受けない。
センサー	端末が検出されたセンサーを表示。

※ 12.3 センサー管理画面でセンサー表示名を変更しても、キャッシュの関係ですぐには端末一覧に反映されません。反映した結果を見たい場合は[設定変更画面](#)で「蓄積中のデータを今すぐ可視化する」を実行してください。

5.2. 一覧（IP）

通信ログの中に現れる IP アドレス・ドメイン名の一覧を表示する画面です。



図. 一覧（IP）画面

1. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決（ARP/ND）	ARP 通信、ND 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

2. 端末種別

値	説明
全て	全ての IP アドレス・ドメイン名を表示
クライアント	通信の送信元であるクライアントとして振る舞う IP アドレスを表示
サーバー	通信の宛先であるサーバーとして振る舞う IP アドレス・ドメイン名を表示（ブロードキャスト・マルチキャストアドレスも含む）
クライアント+サーバー	クライアントとサーバーの両方として振る舞う IP アドレスを表示
応答無サーバー	応答をしていないサーバーの IP アドレス・ドメイン名を表示（ブロードキャスト・マルチキャストアドレスも含む）

3. CSV ダウンロードボタン

ボタンを押下すると、一覧に表示されているデータを CSV ファイルとしてダウンロードします。

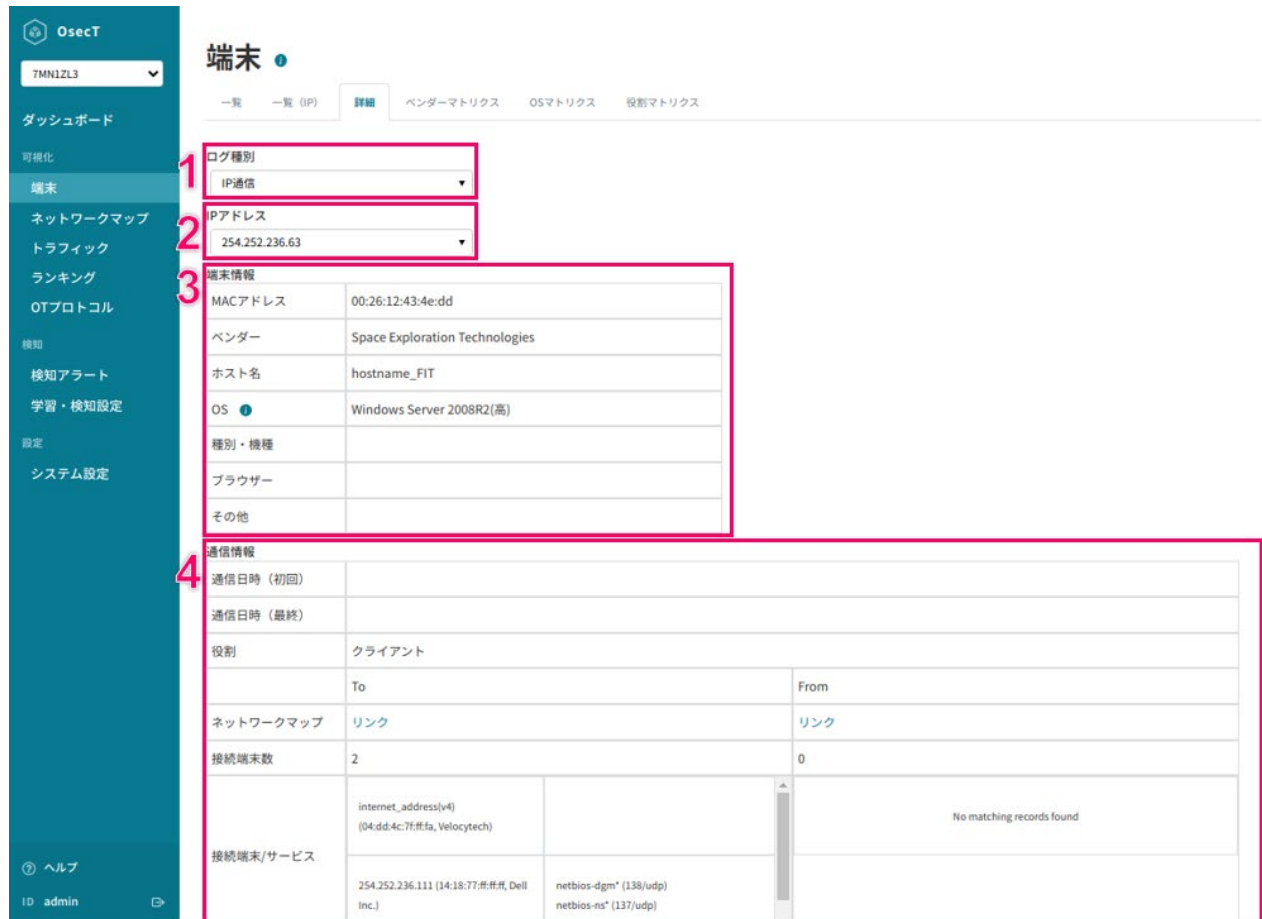
4. IP アドレス一覧

端末種別で選択した条件に一致する IP アドレス・ドメイン名の一覧を表示します。

グローバルアドレスと判定されたものは最後に（global）が付加されます。表示順はプライベート IPv4、プライベート IPv6、グローバル IPv4、グローバル IPv6 ドメイン名の順となります。

5.3. 詳細

選択した端末の情報を表示する画面です。



端末

一覧 一覧 (IP) **詳細** ベンダーマトリクス OSマトリクス 役割マトリクス

ログ種別
IP通信

IPアドレス
254.252.236.63

端末情報	
MACアドレス	00:26:12:43:4e:dd
ベンダー	Space Exploration Technologies
ホスト名	hostname_FIT
OS	Windows Server 2008R2(高)
種別・機種	
ブラウザー	
その他	

通信情報					
通信日時 (初回)					
通信日時 (最終)					
役割	クライアント				
ネットワークマップ	リンク				
接続端末数	2				
接続端末/サービス	<table border="1"> <tr> <td>internet_address(v4) (04:dd:4c:7f:ff:fa, Velocitytech)</td> <td></td> </tr> <tr> <td>254.252.236.111 (14:18:77:ff:ff:ff, Dell Inc.)</td> <td>netbios-dgm* (138/udp) netbios-ns* (137/udp)</td> </tr> </table>	internet_address(v4) (04:dd:4c:7f:ff:fa, Velocitytech)		254.252.236.111 (14:18:77:ff:ff:ff, Dell Inc.)	netbios-dgm* (138/udp) netbios-ns* (137/udp)
internet_address(v4) (04:dd:4c:7f:ff:fa, Velocitytech)					
254.252.236.111 (14:18:77:ff:ff:ff, Dell Inc.)	netbios-dgm* (138/udp) netbios-ns* (137/udp)				

図. 詳細画面

1. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決 (ARP/ND)	ARP 通信、ND 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

2. IP アドレス

通信ログに現れるすべての IP アドレス・ドメイン名を表示します。選択した IP アドレス・ドメイン名を持つ端末の情報が画面に表示されます。

3. 端末情報

IP アドレスで選択した端末の IP アドレスに紐づく端末情報を表示します。（本項目はログ種別が名前解決かつ IP アドレスが送信先の場合は表示されません。）

項目名	説明
MAC アドレス	IP アドレスに紐づく MAC アドレス
ベンダー	IP アドレスに紐づく MAC ベンダー（MAC ベンダー が不明の場合は「unknown」を表示します）
ホスト名	IP アドレスに紐づくホスト名
OS	IP アドレスに紐づく OS 名の推定結果
種別・機種	IP アドレスに紐づく種別・機種
ブラウザ	IP アドレスに紐づくブラウザ
その他	IP アドレスに紐づくその他の端末情報

4. 通信情報

IP アドレスで選択した端末の IP アドレスに紐づく通信情報を表示します。

項目名	説明
通信日時（初回）	IP アドレスに紐づく通信日時（初回）。端末が最初に通信した日時を表示。画面上部で期間指定した場合でも影響を受けない。
通信日時（最終）	IP アドレスに紐づく通信日時（最終）。端末が最後に通信した日時を表示。画面上部で範囲指定した場合でも影響を受けない。
役割	IP アドレスに紐づく役割

ネットワークマップ	IP アドレスに紐づくネットワークマップの端末へのリンク (To & From)
接続端末数	IP アドレスに紐づく接続端末数 (To & From)
接続端末/接続サービス	IP アドレスに紐づく接続端末とサービス (To & From)

5.4. ベンダーマトリクス (◎ : オススメ機能)

端末のベンダー名をサブネットごとのマトリクス形式で表示する画面です。

図. ベンダーマトリクス画面

1. 比較選択ボタン


比較選択ボタンを押下すると、画面上部で指定された 2 つの期間のデータを比較して、差分表示します。差分表示では、画面上部の期間設定にて期間に指定した範囲から比較に指定した範囲に対する差分を表示します。差分表示時には変化があったマトリクスの外枠が黄色になります。

2. サブネット選択リスト

表示したいサブネットを選択できます。決定ボタンを押下することで表示したいサブネットを確定できます。全選択ボタンを押下することで、表示可能なサブネットすべてを選択できます。クリアボタンを押下することで、選択済みのすべてのサブネットを選択からはずすことができます。

3. マトリクス

MAC アドレスからベンダー名を特定し、対応する IP アドレスのマス背景色を塗りつぶします。

 ボタンを押下すると、マトリクスを画像ファイルとして保存できます。

4. 凡例

マトリクスで使用される背景色の凡例と対応するベンダー名を表示します。

5.5. OS マトリクス

端末の OS 名をサブネットごとのマトリクス形式で表示する画面です。

図. OS マトリクス画面

1. 比較選択ボタン


比較選択ボタンを押下すると、画面上部で指定された2つの期間のデータを比較して、差分表示します。差分表示では、画面上部の期間設定にて期間に指定した範囲から比較に指定した範囲に対する差分を表示します。差分表示時には変化があったマトリクスの外枠が黄色になります。

2. サブネット選択リスト

表示したいサブネットを選択できます。決定ボタンを押下することで表示したいサブネットを確定できます。全選択ボタンを押下することで、表示可能なサブネットすべてを選択できます。クリアボタンを押下することで、選択済みのすべてのサブネットを選択から外すことができます。

3. マトリクス

通信ログから OS 名を推定し、対応する IP アドレスのマス背景色を塗りつぶします。

 ボタンを押下すると、マトリクスを画像ファイルとして保存できます。

4. 凡例

マトリクスで使用される背景色の凡例と対応する OS 名を表示します。

5.6. 役割マトリクス

端末の役割をサブネットごとのマトリクスで表示する画面です。

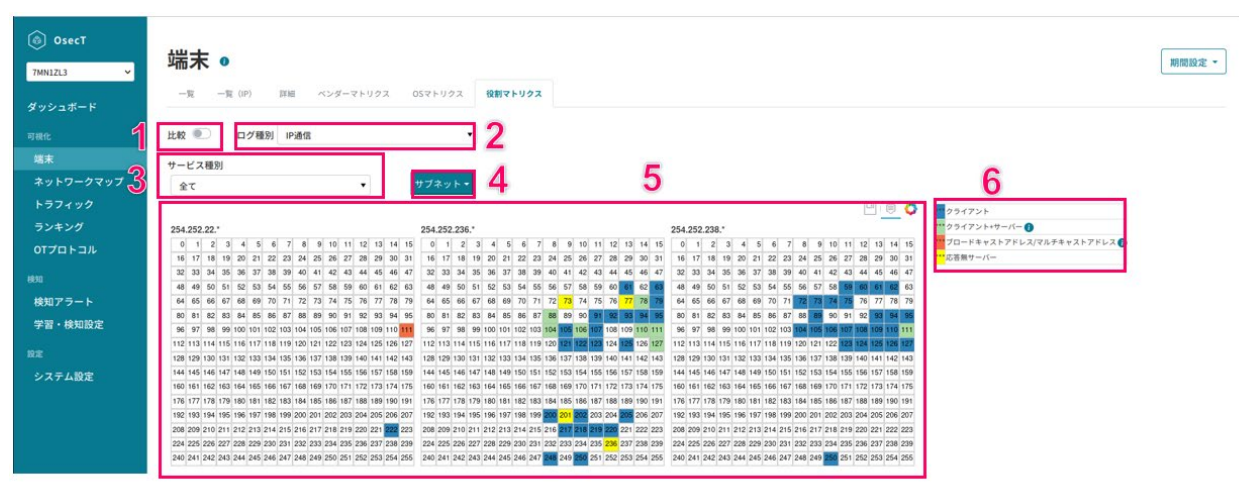


図. 役割マトリクス画面

1. 比較選択ボタン

比較ボタンを押下すると、画面上部で指定された 2 つの期間のデータを比較して、差分表示します。 差分表示では、画面上部の期間設定にて期間に指定した範囲から比較に指定した範囲に対する差分を表示します。差分表示時には変化があったマトリクスの外枠が黄色になります。

2. ログ種別

表示対象とする通信ログ種別を設定します。 以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
ARP (IPv4)	ARP 通信に関する通信ログ

3. サービス種別


サービスの一覧を表示します。選択したサービスによって、データの絞り込みができます。

4. サブネット選択リスト

表示したいサブネットを選択できます。決定ボタンを押下することで表示したいサブネットを確定できます。全選択ボタンを押下することで、表示可能なサブネットすべてを選択できます。クリアボタンを押下することで、選択済みのすべてのサブネットを選択から外すことができます。

5. マトリクス

通信ログの振る舞い分析により端末の役割を推定し、対応する IP アドレスのマス
の背景色を塗りつぶします。

 ボタンを押下すると、マトリクスを画像ファイルとして保存できます。

6. 凡例

マトリクスで使用される背景色の凡例と対応する役割名を表示します。

カテゴリ	説明
クライアント	通信の送信元であるクライアントと判定された端末
サーバー	通信の宛先であるサーバーと判定された端末
クライアント+サーバー	クライアントとサーバー両方の役割を持つと判定された端末
ブロードキャストアドレス/マルチキャストアドレス	ブロードキャストまたはマルチキャストアドレス

6. ネットワークマップ

6.1. 端末（◎：オススメ機能）

端末間の接続状態をマップ形式で表示する画面です。

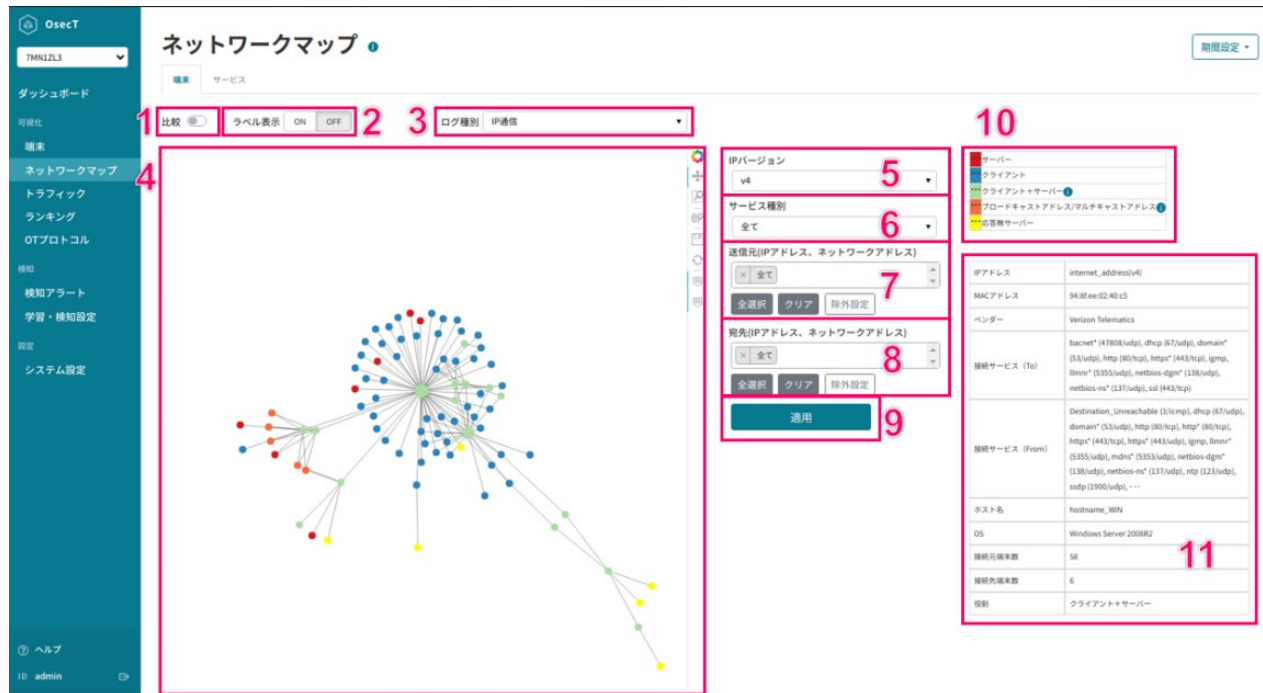


図. 端末画面

1. 比較選択ボタン

左側メニューから遷移した場合は、比較なしのモードで表示されます。 比較選択ボタンを押下すると、画面上部で指定された2つの期間のデータを比較して、差分表示します。 差分表示では、画面上部の期間設定にて期間に指定した範囲から比較に指定した範囲に対する差分を表示します。 差分表示時には変化があったノードの外枠に色をつけます。

外枠の色	説明
緑	比較に指定した範囲には存在せず、期間に指定した範囲には存在するノード

青	比較に指定した範囲には存在し、期間に指定した範囲には存在しないノード。存在しなくなったノードは白塗になります。
なし	変化なし

2. ラベル表示選択ボタン

マップ上のノードにラベル（IP アドレス・ドメイン名）を表示する（ON） / 表示しない（OFF）を選択できます。 ON にした場合、以下のようなマップが表示されます。

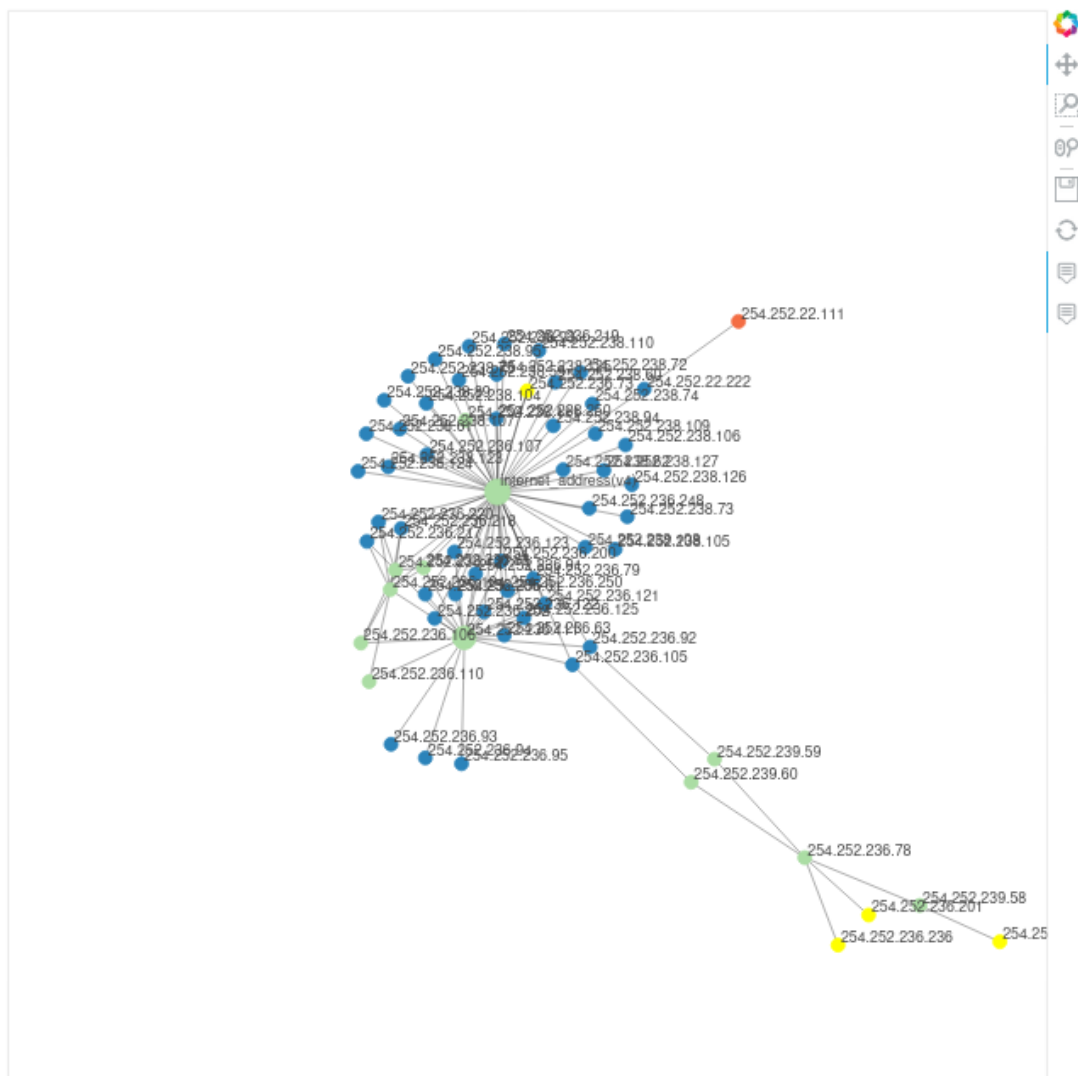


図. ラベル表示 ON 時のマップ

3. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決 (ARP/ND)	ARP 通信、ND 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

4. マップ

ノード (IP アドレス・ドメイン名) 間の接続状態を表示します。役割に応じて、ノードの色が変わります。

5. IP バージョン

選択した IP バージョン (v4/v6) の情報をマップに表示します。

6. サービス種別

選択したサービス種別情報をマップに表示します。

7. 送信元 IP アドレス

表示対象の送信元 IP アドレスやネットワークアドレスと、表示対象外にしたい送信元 IP アドレスやネットワークアドレスを指定できます。

8. 宛先 IP アドレス

表示対象の送信先 IP アドレスやネットワークアドレスと、表示対象外にしたい送信先 IP アドレスやネットワークアドレスを指定できます。

9. 適用ボタン

選択した条件のマップを表示します。

10. 凡例

マップのノード色の凡例と対応する役割名を表示します。

カテゴリ	説明
クライアント	クライアントと判定されたノード

サーバー	サーバーと判定されたノード（無応答サーバー、ブロードキャストアドレス/マルチキャストアドレスを除く）
クライアント+サーバー	クライアントとサーバーの両方の役割を持つと判定されたノード
ブロードキャストアドレス/ マルチキャストアドレス	ブロードキャストアドレスもしくはマルチキャストアドレス
無応答サーバー	サーバーと判定されたノードのうち応答パケットが観測されていないノード

11. 端末の詳細情報

マップ上でノードにマウスオーバーすると表示されます。 ノードの IP アドレス・ドメイン名、MAC アドレス、ベンダー、接続サービス（To）、接続サービス（From）、ホスト名、OS、機種・種別、ブラウザー、接続元端末数、接続先端末数、役割を表形式で表示します。 表示する情報がない場合は、行が表示されません（例：OS 名の推定ができなかった場合は、OS の行は表示されない）。

6.2. サービス

端末とサービス間の関係をマップ形式で表示する画面です。

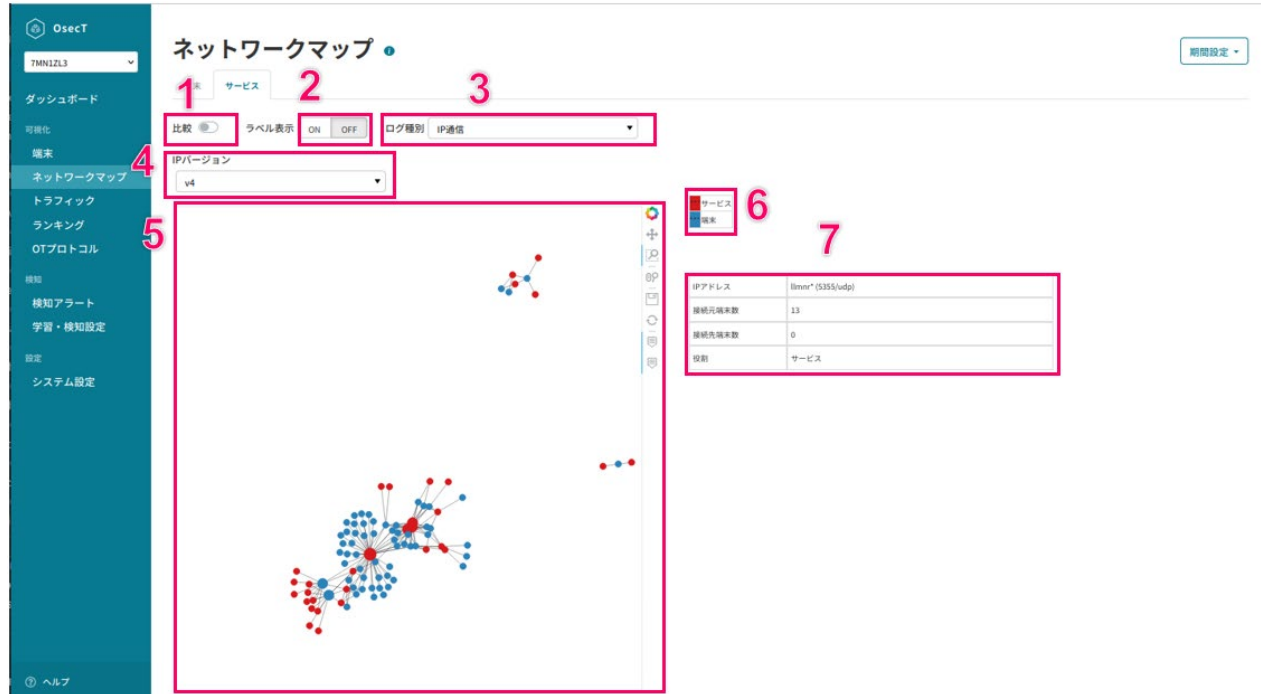


図. サービス画面

1. 比較選択ボタン

比較選択ボタンを押下すると、画面上部で指定された2つの期間のデータを比較して、差分表示します。差分表示では、画面上部の期間設定にて期間に指定した範囲から比較に指定した範囲に対する差分を表示します。差分表示時には変化があったノードの外枠に色をつけます。

外枠の色	説明
緑	比較に指定した範囲には存在せず、期間に指定した範囲には存在するノード
青	比較に指定した範囲には存在し、期間に指定した範囲には存在しないノード。存在しなくなったノードは色が白塗になります。
なし	変化なし

2. ラベル表示選択ボタン

マップ上のノードにラベル（サービス名、IP アドレス・ドメイン名）を表示する（ON）/表示しない（OFF）を選択できます。ON にした場合、以下のようなマップが表示されます。

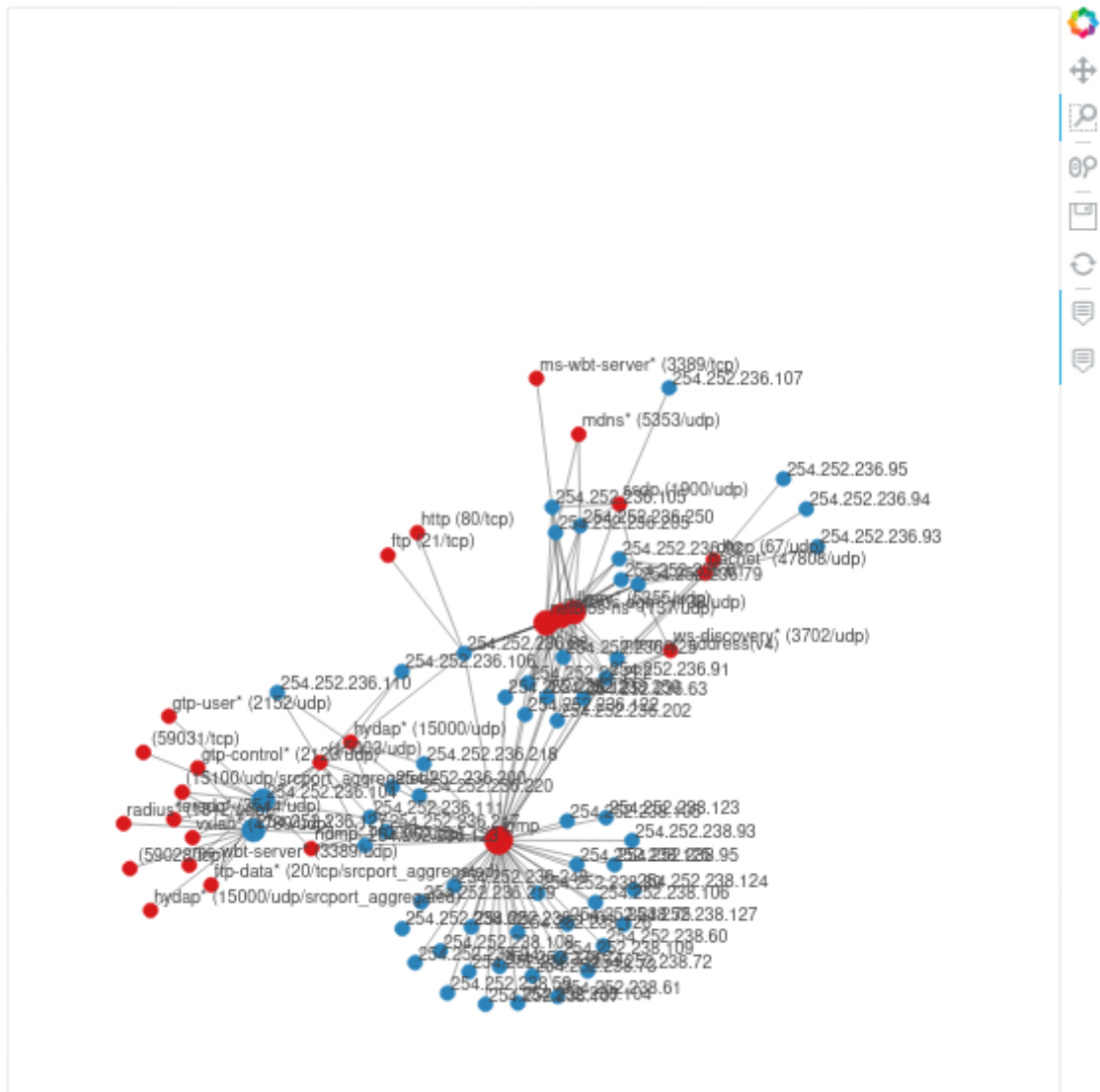


図. ラベル表示 ON 時のマップ

3. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

4. IP バージョン

選択した IP バージョン（v4/v6）の情報をマップに表示します。

5. マップ

ノード（端末またはサービス）の関係を表示します。振る舞いから判定された役割に応じて、ノードの色が変わります。

6. 凡例

マップのノード色の凡例と対応する役割名を表示します。

カテゴリ	説明
サービス	サービスと判定されたノード
端末	端末と判定されたノード

7. 端末の詳細情報

マップ上でノードにマウスオーバーすると表示されます。ノードの IP アドレス、またはサービス名、MAC アドレス、ベンダー、ホスト名、OS、機種・種別、ブラウザ、接続元端末数、接続端末数、役割を表形式で表示します。表示する情報がない場合は、行が表示されません（例：OS 名の推定ができなかった場合は、OS の行は表示されない）。

7. トラフィック

トラフィック量を時系列グラフで表示する画面です。本画面は期間指定したときのみ表示されます。



図. トラフィック画面

1. グラフ

上部：IP 通信ログを 60 分ごと（システム設定値）に集計し、時系列トラフィックグラフを表示します。

下部：上部のグラフに表示する期間を示すグラフを表示します。枠をドラッグすることで上部のグラフに表示する期間を変更できます。

2. IP バージョン

選択した IP バージョン（全て/v4/v6）の情報をグラフに表示します。

3. 送信元 IP アドレス

選択した送信元 IP アドレスの情報をグラフに表示します。

4. 宛先 IP アドレス

選択した宛先 IP アドレスの情報をグラフに表示します。

5. サービス種別

選択したサービス種別の情報をグラフに表示します。

6. 適用ボタン

IP バージョン、送信元 IP アドレス、宛先 IP アドレス、サービス種別で選択した項目を反映したグラフを表示します。

8. ランキング

8.1. 端末トラフィック量

端末ごとのトラフィック量を多い順にグラフ、ランキング表で表示する画面です。想定以上に通信をしている端末がないか確認できます。

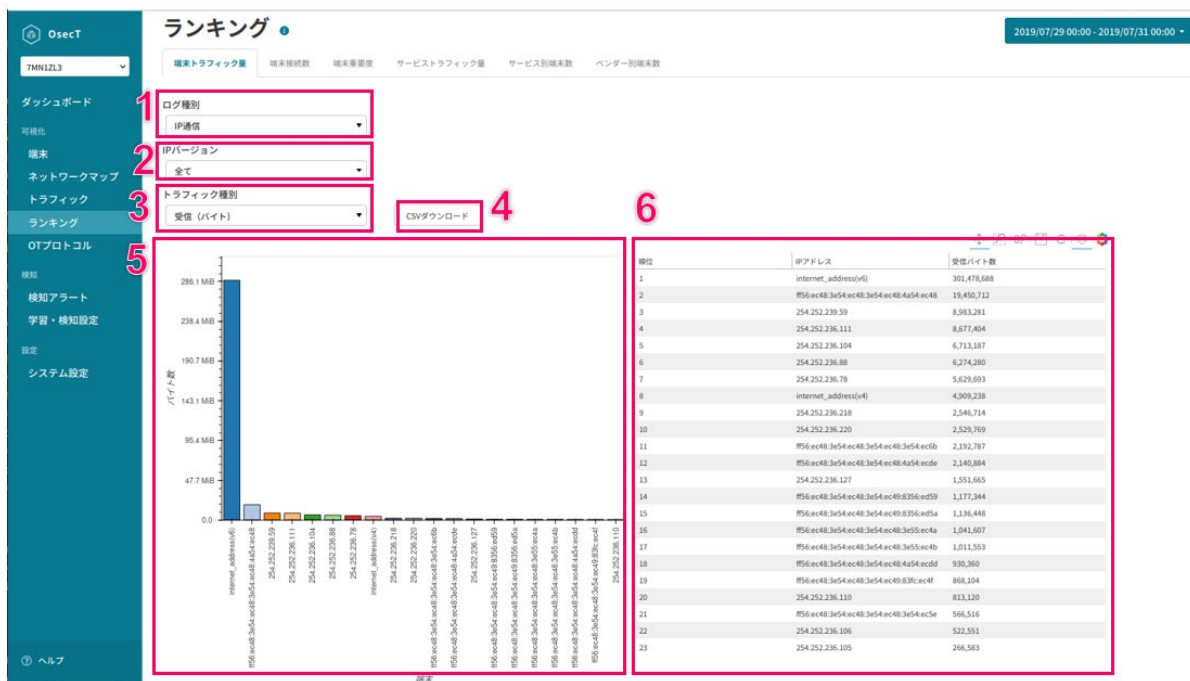


図. 端末トラフィック量画面

1. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決 (ARP/ND)	ARP 通信、ND 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

2. IP バージョン

表示対象とする IP バージョンを設定します。

カテゴリ	説明
すべて	IPv4 アドレス、IPv6 アドレス
v4	IPv4 アドレス
v6	IPv6 アドレス

3. トラフィック種別

グラフ、ランキング表に表示するデータの種別を選択します。

カテゴリ	説明
受信 (バイト)	IP アドレスごとの受信バイト数 (ログ種別が IP 通信のみ)
送信 (バイト)	IP アドレスごとの送信バイト数 (ログ種別が IP 通信のみ)
受信 (パケット)	IP アドレスごとの受信パケット数 (ログ種別が IP 通信のみ)
送信 (パケット)	IP アドレスごとの送信パケット数 (ログ種別が IP 通信のみ)
要求 (パケット)	クライアント IP アドレスごとの要求パケット数 (ログ種別が MAC 解決 (ARP/ND)、名前解決通信の場合のみ)
応答 (パケット)	サーバー IP アドレスもしくはドメイン名ごとの要求パケット数 (ログ種別が MAC 解決 (ARP/ND)、名前解決通信の場合のみ)

4. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

5. グラフ

トラフィック種別で選択した種別の端末ごとのトラフィック量をグラフで表示します。

6. ランキング表

トラフィック種別で選択した種別の端末ごとのトラフィック量をランキング表で表示します。

8.2. 端末接続数

端末ごとの被接続数が多い順にグラフ、ランキング表で表示する画面です。

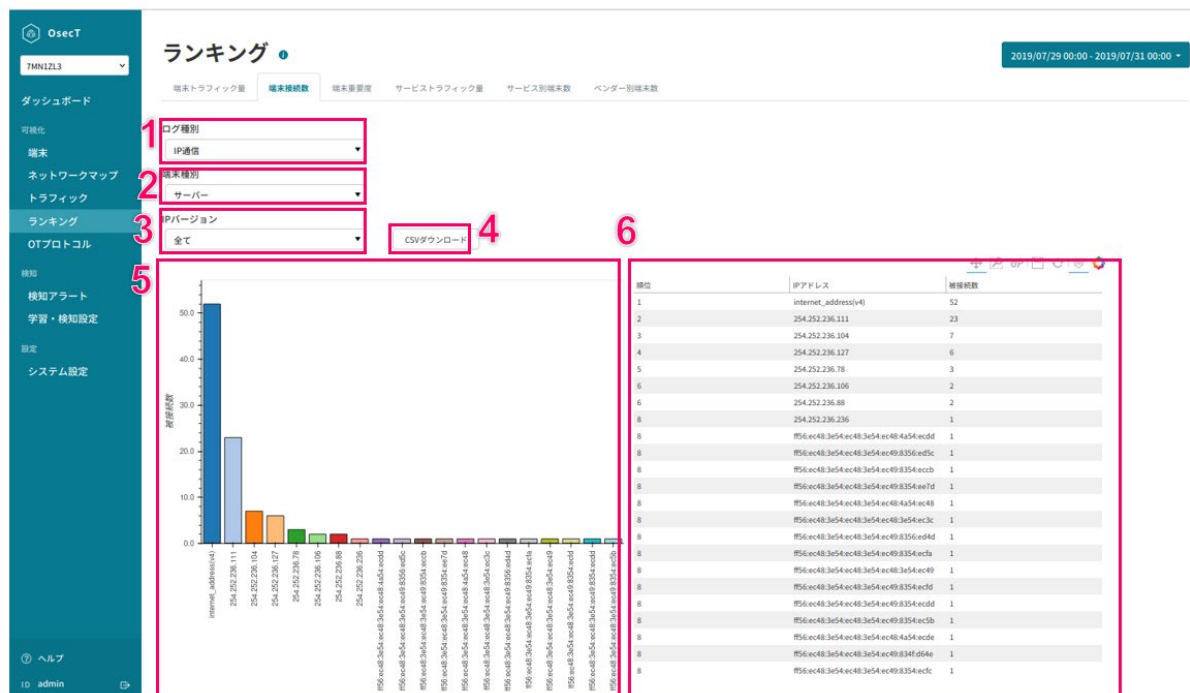


図. 端末接続数画面

1. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決 (ARP/ND)	ARP 通信、ND 通信に関する通信ログ
名前空間	DNS 通信に関する通信ログ

2. 端末種別

グラフ、ランキング表に表示するデータの種別を選択します。

カテゴリ	説明
サーバー	サーバーをクライアントの数の多い順に表示
クライアント	クライアントをサーバーの数の多い順に表示

3. IP バージョン

表示対象とする IP バージョンを設定します。

カテゴリ	説明
すべて	IPv4 アドレス、IPv6 アドレス
v4	IPv4 アドレス
v6	IPv6 アドレス

4. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

5. グラフ

端末種別で選択した種別の端末ごとの被接続数をグラフで表示します。

6. ランキング表

端末種別で選択した種別の端末ごとの被接続数をランキング表で表示します。

8.3. 端末重要度

端末の重要度をグラフ、ランキング表で表示する画面です。

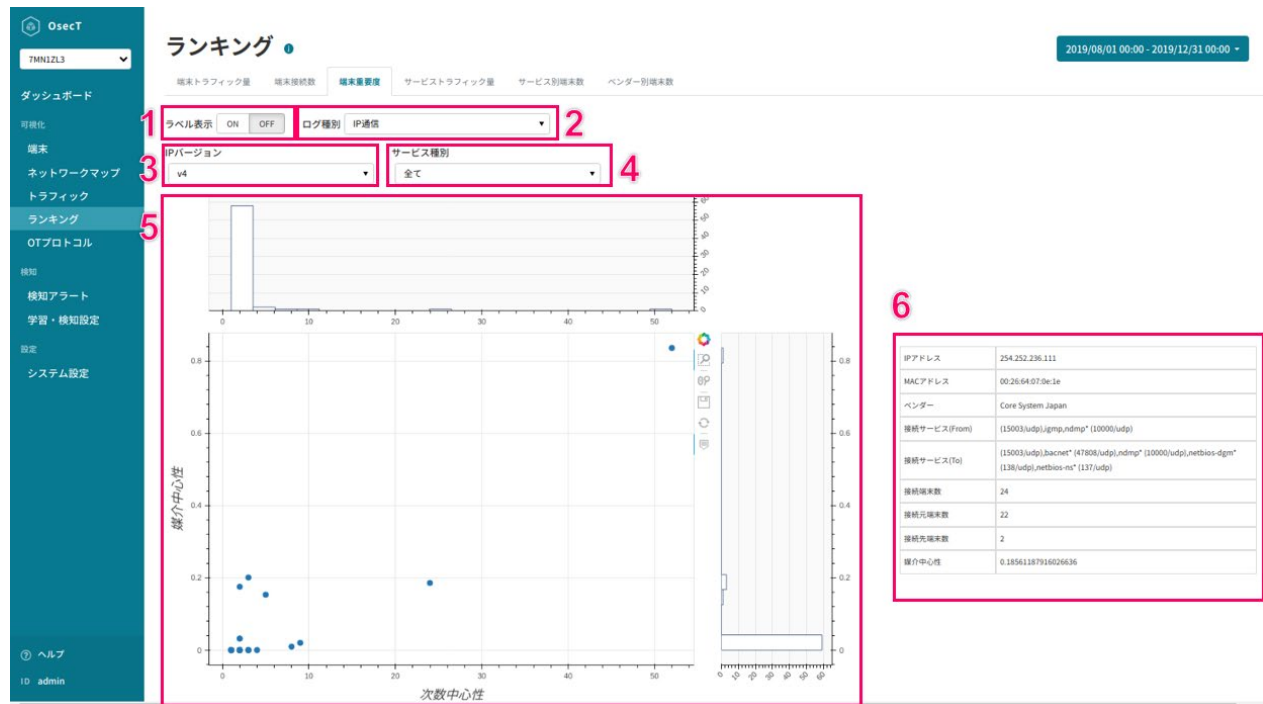


図. 端末重要度画面（1）

1. ラベル表示選択ボタン

マップ上のノードにラベル（IP アドレス・ドメイン名）を表示する（ON）/表示しない（OFF）を選択できます。ON にした場合、以下のようなマップが表示されます。

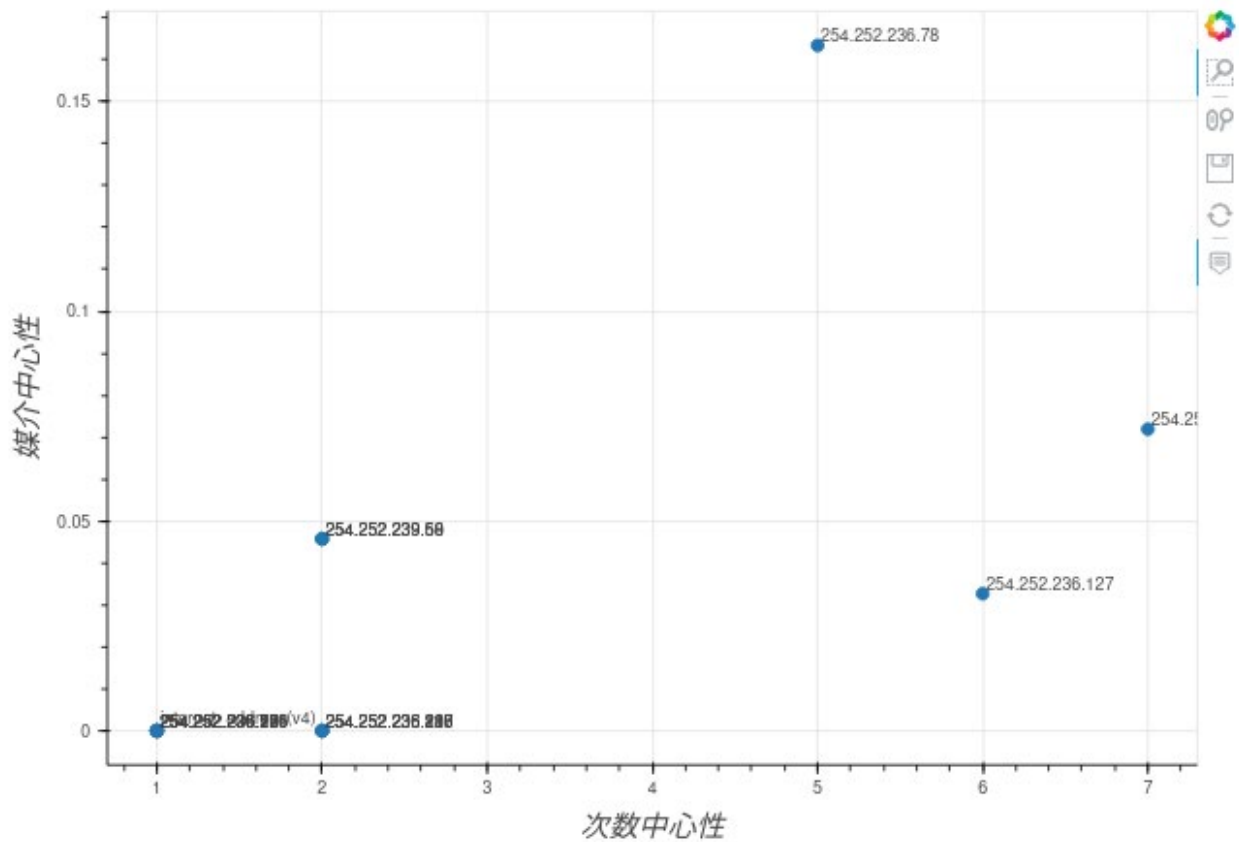


図.ラベル表示 ON 時のマップ（２）

2. ログ種別

表示対象とする通信ログ種別を設定します。以下の通信ログ種別が選択可能です。

カテゴリ	説明
IP 通信	IP 通信に関する通信ログ
MAC 解決 (ARP/ND)	ARP 通信、ND 通信に関する通信ログ
名前解決	DNS 通信に関する通信ログ

3. IP バージョン

選択した IP バージョン（v4/v6）の情報をマップに表示します。

4. サービス種別

選択したサービスの情報をマップに表示します。

5. マップ

ノード（IP アドレス・ドメイン名）の重要度を表示します。

6. 端末の詳細情報

マップ上でノードにマウスオーバーすると表示されます。 ノードの IP アドレス・ドメイン名、MAC アドレス、ベンダー、サービス、ホスト名、OS、種別・機種、ブラウザー、接続端末数、接続元端末数、接続先端末数、媒介中心性を表形式で表示します。 表示する情報がない場合は、行が表示されません（例：OS 名の推定ができなかった場合は、OS の行は表示されない）。

7 CSVダウンロード

8

順位	IPアドレス	重要度	特異度	媒介中心性	次数中心性	接続元端末数	接続先端末数
1	internet_address(v4)	1.303351266290062	0.05265230024855494	0.8358974358974359	1	52	2
2	254.252.236.111	0.48845212589356274	0.2198207227818261	0.1826923076923078	0.453	23	2
3	254.252.236.104	0.15220954980451443	0.1150203691324036	0.019150641025641013	0.151	7	6
4	254.252.236.78	0.14194484812051225	0.053871590301871206	0.12051282051282051	0.075	3	2
5	254.252.236.127	0.1323101800243787	0.10823407799178361	0.009054487179487182	0.132	6	5
6	254.252.236.105	0.10346486273573114	0.062469084385426726	0.09623397435897438	0.038	0	3
7	254.252.236.92	0.103464862735731138	0.06246908438542671	0.09623397435897436	0.038	0	3
8	254.252.239.59	0.07356951395145894	0.05419127296194412	0.07107371794871795	0.019	1	1
8	254.252.239.60	0.07356951395145894	0.05419127296194412	0.07107371794871795	0.019	1	1
10	254.252.236.88	0.057	0.05064734960321484	0	0.057	2	4

図. 端末重要度画面（3）

7. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

8. ランキング表

重要度の大きい順にランキングを表示します。

8.4. サービストラフィック量

サービスごとのトラフィック量を多い順にグラフ、ランキング表で表示する画面です。

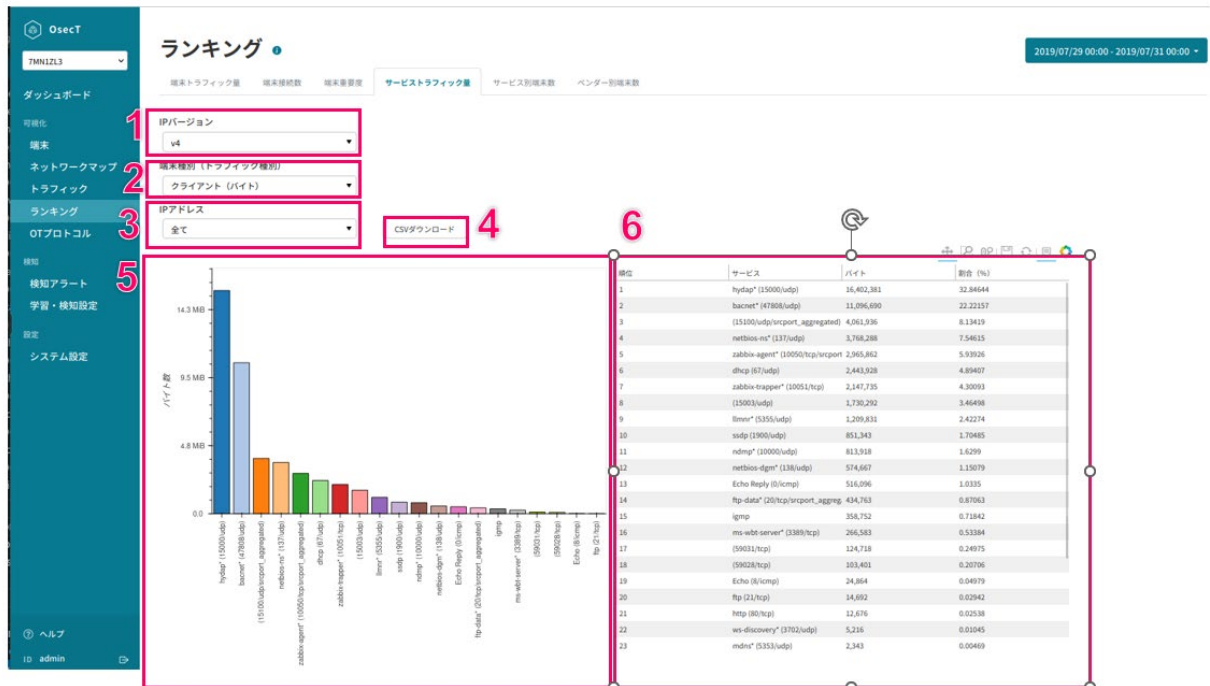


図. サービストラフィック画面

1. IP バージョン

選択した IP バージョン (v4/v6) の情報をマップに表示します。

2. 端末種別 (トラフィック種別)

グラフ、ランキング表に表示するデータの種別を選択します。

カテゴリ	説明
クライアント (バイト)	クライアントのサービスごとに送信バイト数と受信バイト数を合計し多い順に表示
サーバー (バイト)	サーバーのサービスごとに送信バイト数と受信バイト数を合計し多い順に表示
クライアント (パケット)	クライアントのサービスごとに送信パケット数と受信パケット数を合計し多い順に表示

サーバー（パケット）	サーバーのサービスごとに送信パケット数と受信パケット数を合計し多い順に表示
------------	---------------------------------------

3. IP アドレス

選択した IP アドレス・ドメイン名の情報をグラフに表示します。

4. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

5. グラフ

端末種別（トラフィック種別）で選択した種別のサービスごとのトラフィック量をグラフで表示します。

6. ランキング表

端末種別（トラフィック種別）で選択した種別のサービスごとのトラフィック量をランキング表で表示します。

8.5. サービス別端末数

サービスごとの端末数を多い順にグラフ、ランキング表で表示する画面です。

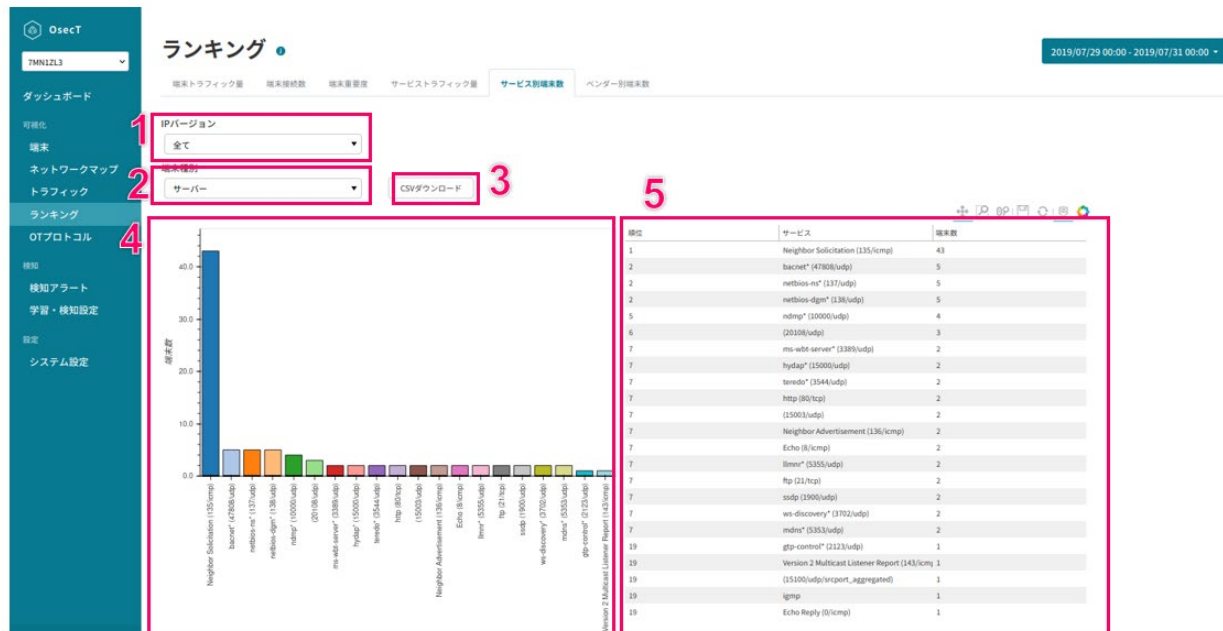


図. サービス別端末数画面

1. IP バージョン

選択した IP バージョン (全て/v4/v6) の情報をグラフ、ランキング表に表示します。

2. 端末種別

カテゴリ	説明
クライアント	サービスをクライアント数の多い順に表示
サーバー	サービスをサーバー数の多い順に表示

3. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

4. グラフ

IP バージョンで選択した IP バージョンのサービスごとの端末数をグラフで表示します。

5. ランキング表

IP バージョンで選択した IP バージョンのサービスごとの端末数をランキング表で表示します。

8.6. ベンダー別端末数

ベンダー名ごとの端末数をランキングで表示する画面です。

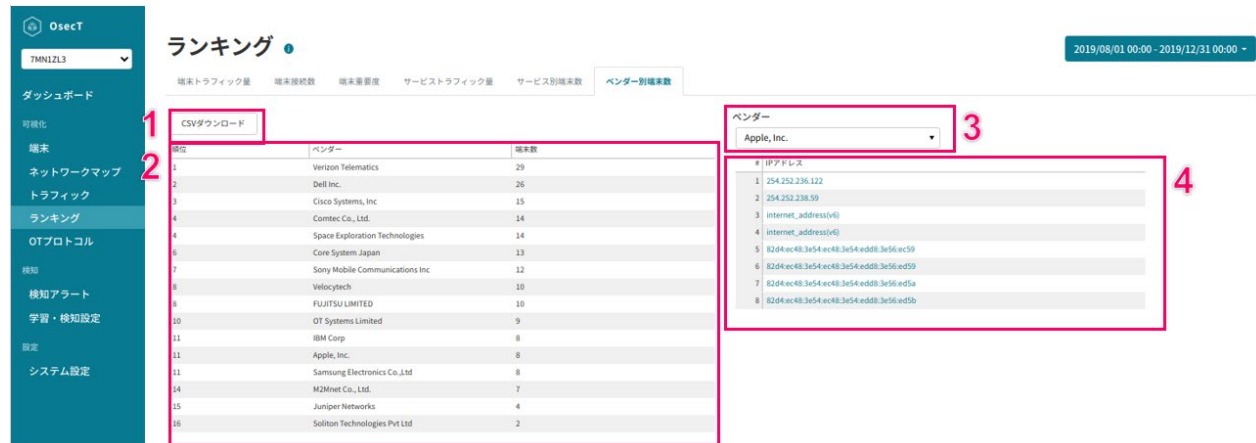


図. ベンダー別端末数画面

1. CSV ダウンロードボタン

ボタンを押下すると、ランキング表に表示されているデータを CSV ファイルとしてダウンロードします。

2. ランキング表

取り込んだデータの MAC アドレスを元にベンダーを推定し、ベンダーごとに端末数をカウントした結果を表示します。 端末数の多い順に表示します。

3. ベンダー

選択したベンダーに対応する端末の IP アドレスを端末一覧に表示します。

4. 端末一覧

ベンダーで選択されたベンダー名と推定された端末の IP アドレスを表示します。

9. OT プロトコル

9.1. 一覧 (IP)

IP 系の OT プロトコル情報を一覧表示する画面です。

#	選択元IPアドレス	宛先IPアドレス	プロトコル	OTプロトコル	ファンクション
1	172.16.134.129	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataRes
2	172.16.134.129	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
3	172.16.134.130	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
4	172.16.134.131	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataRes
5	172.16.134.132	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
6	172.16.134.132	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataRes
7	172.16.134.133	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataRes
8	172.16.134.133	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
9	172.16.134.134	172.16.134.128	udp	cclink_ie_field_basic	未定義
10	172.16.134.135	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic

図. 一覧画面

1. 比較選択ボタン

期間指定で指定された 2 つの期間のデータを比較して、差分表示します。差分表示時には diff 列が表示されます。

#	diff	選択元IPアドレス	宛先IPアドレス	プロトコル	OTプロトコル	ファンクション
1		172.16.134.129	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataRes
2		172.16.134.129	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
3	add	172.16.134.130	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
4	chg	172.16.134.131	172.16.134.128	udp	cclink_ie_field_basic	未定義 → cyclicDataRes
5	add	172.16.134.132	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic
6	del	172.16.134.132	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataReq cyclic
7	del	172.16.134.133	172.16.134.128	udp	cclink_ie_field_basic	cyclicDataReq cyclic
8	del	172.16.134.133	172.16.134.255	udp	cclink_ie_field_basic	cyclicDataReq cyclic

図. 一覧画面（差分モード）

diff 列の値	説明
add	期間設定にて比較に指定した範囲には存在せず、期間に指定した範囲には存在する端末（行全体の背景色：赤）
del	期間設定にて比較に指定した範囲には存在し、期間に指定した範囲には存在しない端末（行全体の背景色：青）
chg	期間設定にて比較に指定した範囲と期間に指定した範囲で情報に変化があったデータ（変化があったセルの背景色：黄）
なし	変化なし

2. CSV ダウンロードボタン

ボタンを押下すると、一覧に表示されているデータを CSV ファイルとしてダウンロードします。

3. 一覧

カラム名	説明
送信元 IP アドレス	送信元となる IPv4 アドレス
宛先 IP アドレス	宛先となる IP アドレス
プロトコル	トランスポート層におけるプロトコル（TCP または UDP）
OT プロトコル	OT 通信におけるプロトコル
ファンクション	使用されたファンクション

4. 一覧データフィルタ

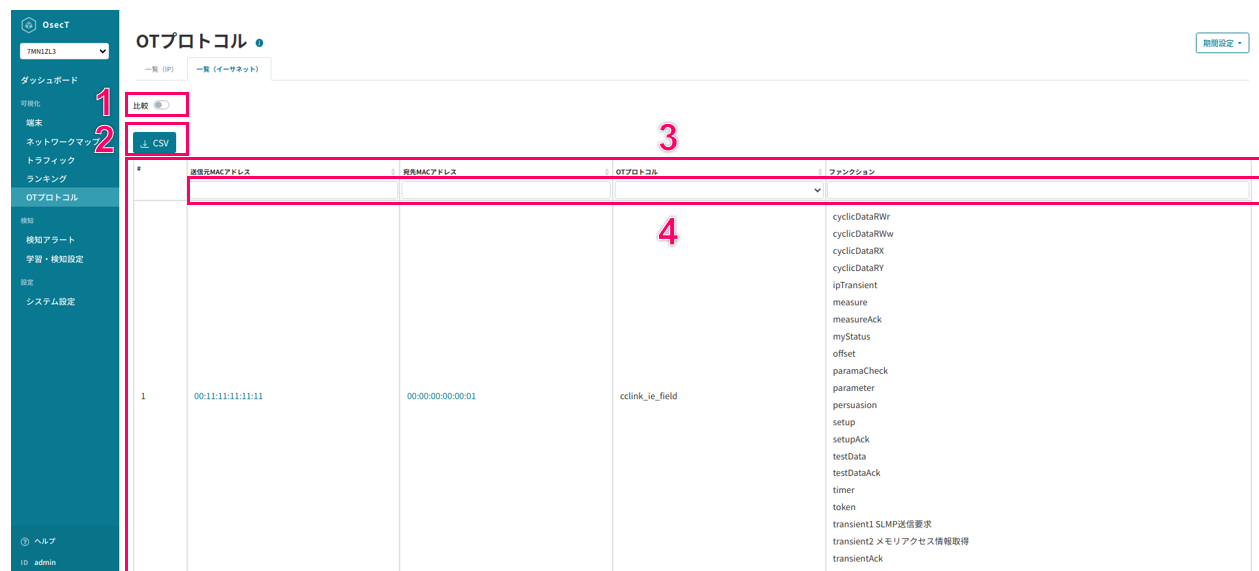
一覧の各列の内容で一覧をフィルタリングできます。

カラム名	説明
diff	選択

送信元 IP アドレス	前方一致、カンマ区切りで複数指定可能
宛先 IP アドレス	前方一致、カンマ区切りで複数指定可能
プロトコル	選択
OT プロトコル	選択
ファンクション	完全一致、カンマ区切りで複数指定可能

9.2. 一覧（イーサネット）

Non-IP 系の OT プロトコル情報を一覧表示する画面です。



The screenshot displays the 'OTプロトコル' (OT Protocol) list interface. The sidebar on the left contains navigation links such as 'ダッシュボード', '可視化', '端末', 'ネットワークマップ', 'トラフィック', 'ランキング', 'OTプロトコル', '検知', '検知アラート', '学習・検知設定', '設定', and 'システム設定'. The main area shows a table with columns for '送信元MACアドレス' (Source MAC Address), '宛先MACアドレス' (Destination MAC Address), 'OTプロトコル' (OT Protocol), and 'ファンクション' (Function). A red box highlights the 'OTプロトコル' column, and a red number '4' points to it. Another red box highlights the '比較' (Compare) and 'CSV' buttons, with red numbers '1' and '2' pointing to them respectively. A red number '3' points to the table header, and a red number '3' points to the 'OTプロトコル' column header.

図. 一覧画面

1. 比較選択ボタン

期間指定で指定された 2 つの期間のデータを比較して、差分表示します。差分表示時には diff 列が表示されます。

OTプロトコル ●

2022/07/20 00:00 - 2022/07/21 23:00
10.41.102.101/22.10.101 - 2022/07/22.23.00

一覧 (IP) 一覧 (イーサネット)

比較 ●

↓ CSV

#	diff	送信元MACアドレス	宛先MACアドレス	OTプロトコル	ファンクション
1	chg	00:11:11:11:11:11	00:00:00:00:00:01	cclink_ie_field	<div> cyclicDataRWr cyclicDataRWw cyclicDataRX cyclicDataRY IpTransient measure measureAck myStatus offset paramaCheck parameter persuasion </div>

図. 一覧画面（差分モード）

diff 列の値	説明
add	期間設定にて比較に指定した範囲には存在せず、期間に指定した範囲には存在する端末（行全体の背景色：赤）
del	期間設定にて比較に指定した範囲には存在し、期間に指定した範囲には存在しない端末（行全体の背景色：青）
chg	期間設定にて比較に指定した範囲と期間に指定した範囲で情報に変化があったデータ（変化があったセルの背景色：黄）
なし	変化なし

2. CSV ダウンロードボタン

ボタンを押下すると、一覧に表示されているデータを CSV ファイルとしてダウンロードします。

3. 一覧

カラム名	説明
送信元 MAC アドレス	送信元となる MAC アドレス
宛先 MAC アドレス	宛先となる MAC アドレス

OT プロトコル	OT 通信におけるプロトコル
ファンクション	使用されたファンクション

4. 一覧データフィルタ

一覧の各列の内容で一覧をフィルタリングできます。

カラム名	説明
diff	選択
送信元 MAC アドレス	前方一致、カンマ区切りで複数指定可能
宛先 MAC アドレス	前方一致、カンマ区切りで複数指定可能
OT プロトコル	選択
ファンクション	完全一致、カンマ区切りで複数指定可能

10. 検知アラート

10.1. 全て

各脅威検知機能で検知された結果を表示する画面です。

検知アラート ●

全て 新規端末 脆弱端末 IP通信 IP誘導 IP統計 OT振舞(IP) OT振舞(イーサネット) シグネチャ

1 絞り込み

2 IP/MACアドレス 送信元 絞り込みなし 宛先 絞り込みなし

3 アラート種別 ☒ 新規端末 ☒ 脆弱端末 ☒ IP通信 ☒ IP誘導 ☒ IP統計 ☒ OT振舞(IP) ☒ OT振舞(イーサネット) ☒ シグネチャ

4 取得期間 ☒ 経過日数指定 7 日分 ☐ 期間指定 YYYY/MM/DD ~ YYYY/MM/DD

5 センサー ☒ 選択中のセンサー ☐ 全センサー

6 リセット 7 適用

8 表示 CSV

新着	検知日時	検知種別	内容	送信元IP/MACアドレス	宛先IP/MACアドレス	検知数	詳細
新着	2024/02/16 11:51:56	新規端末	新規端末 172.17.0.3 が出現	172.17.0.3		1	表示
新着	2024/02/16 11:51:56	新規端末	新規端末 172.17.0.4 が出現	172.17.0.4		1	表示

図. 全て画面

1. 絞り込み

表示する学習結果を絞り込むことができます。

2. IP/MAC アドレス

送信元を指定した場合、送信元 IP または MAC アドレスの絞り込みを設定できます。宛先を指定した場合、宛先 IP または MAC アドレスの絞り込みを設定できます。

3. アラート種別

表示する脅威検知機能の絞り込みを設定できます。

4. 取得期間

表示する結果を取得した期間の絞り込みを設定できます。経過日数指定を指定した場合、現在日時から指定した日付分までに絞り込むことができます。期間指定を指定した場合、指定した期間の範囲内に絞り込むことができます。

5. センサー

検知結果一覧に表示する対象のセンサーを、「選択中のセンサー」または「全センサー」から選択できます。

6. リセットボタン

IP/MAC アドレス・アラート種別・取得期間・センサーで指定した選択をリセットできます。

7. 適用ボタン

IP/MAC アドレス・アラート種別・取得期間・センサーで指定した選択を適用した画面を表示できます。

8. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

9. 検知結果一覧

カラム名	説明
新着	未確認の検知結果の場合、新着と表示
検知日時	検知データの日時
検知種別	検知した脅威検知機能名
内容	検知したアラートの内容
送信元 IP/MAC アドレス	検知データの送信元 IP または MAC アドレス
宛先 IP/MAC アドレス	検知データの宛先 IP または MAC アドレス
検知数	検知データの該当検知数
詳細	表示ボタンを押下すると、対応した脅威検知詳細画面に遷移

10.2. 新規端末（◎：オススメ機能）

新規端末学習済データ（学習期間中に観測された端末情報）にないトラフィックが検知されたアラート情報の一覧画面です。

検知アラート

全て 30

新規端末

学習済端末

IP通信

IP流量

IP統計

OT振舞(IP)

OT振舞(イーサネット)

シグネチャ

検知完了

学習済リストに登録

全アラート削除

CSV

<input type="checkbox"/>	検知日時	IPアドレス	MACアドレス	ベンダー	宛先IPアドレス:サービス(ポート)	送信元IPアドレス:サービス(ポート)
<input type="checkbox"/>	2023/01/17 22:45:28	fe80::20c:29ff:fe04:4a00	00:0c:29:04:4a:00	VMware, Inc.	ff02::2:Router_Solicitation (133/icmp)	
<input type="checkbox"/>	2023/01/17 22:28:51	10.1.0.17	ac:1f:6b:81:07:db	Super Micro Computer, Inc.	10.2.4.6:Destination_Unreachable (3/icmp), domain* (53/udp)	
<input type="checkbox"/>	2023/01/17 22:27:17	10.1.0.16	ac:1f:6b:81:07:db	Super Micro Computer, Inc.	10.2.4.6:Destination_Unreachable (3/icmp), domain* (53/udp)	

図. 新規端末 検知アラート画面

1. ステータス

新規端末検知のステータスが表示されます。

2. 学習済みリストに登録ボタン

学習データに新規端末データを追加登録できます。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止もしくは検知完了の状態で押下することができ、検知のステータスは学習完了になります。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	新規端末を検知した日時
IP アドレス	検知した端末の IP アドレス
MAC アドレス	検知した端末の MAC アドレス

55

© NTT Communications Corporation All Rights Reserved.

ベンダー	検知した端末のベンダー情報
宛先 IP:サービス (ポート)	検知した端末の宛先 IP、サービス、ポート
送信元 IP:サービス (ポート)	検知した端末の送信元 IP、サービス、ポート

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.3. 脆弱端末（◎：オススメ機能）

脆弱端末（サポート切れ OS を利用している端末）が送信する通信を検知したアラート情報の一覧画面です。

検知アラート ●

☐ 全て
 ☒ 検知中
 ☐ IP通信
 ☐ IP接続
 ☐ IP統計
 ☐ OT振舞(IP)
 ☐ OT振舞(イーサネット)
 ☐ シグネチャ

検知日時	IPアドレス	MACアドレス	ベンダー	宛先IPアドレス(サービス(ポート))	送信元IPアドレス(サービス(ポート))	ホスト名	OS
2019/07/30 08:56:52	82d4:ec48:3e54:ec48:3e54	08:4fa9:d1:23:00	Cisco Systems, Inc			hostname_2NZ	Windows 7
2019/07/30 08:56:52	254.252.236.250	90:d8:52:f9:4b:28	Comtec Co., Ltd.	internet_address(v4):ssdp (1900/udp), mdns* (5353/udp), llmnr* (5355/udp) 254.252.236.111:netbios-ns* (137/udp), netbios-dgm* (138/udp)		hostname_2NZ	Windows 7
2019/07/29 23:52:56	82d4:ec48:3e54:ec48:3e54	08:4fa9:d1:23:00	Cisco Systems, Inc			hostname_800	Windows 8.1

図. 脆弱端末 検知アラート画面

1. ステータス

脆弱端末検知のステータスが表示されます。

2. 検知除外リストに登録ボタン

選択したアラートを検知除外リストに追加登録できます。追加登録すると、同じアラートは検知されません。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止の状態では押下すると、検知のステータスが検知処理待ちになります。 検知のステータスが検知完了の状態では押下すると、検知結果を削除し、検知のステータスが検知処理待ちになります。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	脆弱端末を検知した日時
IP アドレス	検知した端末の IP アドレス

MAC アドレス	検知した端末の MAC アドレス
ベンダー	検知した端末のベンダー情報
宛先 IP:サービス (ポート)	検知した端末の宛先 IP、サービス、ポート
送信元 IP:サービス (ポート)	検知した端末の送信元 IP、サービス、ポート
ホスト名	検知した端末のホスト名
OS	検知した端末の OS 情報

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.4. IP 通信

ネットワークホワイトリスト（学習期間中に観測された IP アドレス、プロトコル、ポート番号）にない通信が検知されたアラート情報の一覧画面です。

検知アラート

全て 30 新規検知 1 検知済み 1 IP通信 1 IP流量 1 IP統計 1 OT感測(IP) 1 OT感測(イーサネット) 1 シグネチャ 1

1000件を超える古いアラートは表示されません。

✓ 検知完了 1

学習済みリストに登録 2 5

3 4 全アラート削除 CSV

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
2023/01/19 02:35:53	192.168.2.62	0	225.3.2.1	0	igmp
2023/01/19 02:35:53	169.254.29.212	0	224.0.0.252	0	igmp
2023/01/19 02:34:17	192.168.0.157	5353	224.0.0.251	5353	udp
2023/01/19 02:33:49	192.168.2.52	0	225.0.0.56	0	igmp

図. IP 通信 検知アラート画面

1. ステータス

IP 通信検知のステータスが表示されます。

2. 学習済みリストに登録ボタン

学習データに検知された通信データを追加登録できます。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止もしくは検知完了の状態を押下することができ、検知のステータスは学習完了になります。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	対象のトラフィックを検知した日時
送信元 IP アドレス	検知したトラフィックの送信元 IP アドレス

送信元ポート	検知したトラフィックの送信元ポート番号
宛先 IP アドレス	検知したトラフィックの宛先 IP アドレス
宛先ポート	検知したトラフィックの宛先ポート番号
プロトコル	検知したトラフィックのプロトコル（TCP または UDP）

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.5. IP 流量

学習期間中に測定されたトラフィック流量の上限値、下限値の範囲を超えるトラフィック流量が検知された場合や、機器が無通信の状態となった場合のアラート情報の一覧画面です。

検知アラート

全て 30

新規端末

登録済み

IP 通信

IP 流量

IP 統計

OT 振舞 (IP)

OT 振舞 (イーサネット)

シグネチャ

1

2

3

4

5

検知完了

表示モード

パケット

検知対象から除外

6

全アラート削除

CSV

検知日時	送信元IPアドレス	宛先IPアドレス	検知理由	トラフィック量	上限閾値	下限閾値	操作
2019/07/31 19:00:00	254.252.238.127	internet_address(v4)	upside	6	4	-	詳細
2019/07/31 19:00:00	254.252.238.59	internet_address(v4)	upside	6	4	-	詳細
2019/07/31 19:00:00	254.252.236.105	254.253.236.111	downside	5	-	56	詳細
2019/07/31 19:00:00	254.252.236.121	254.253.236.111	upside	45	20	-	詳細
2019/07/31 18:00:00	254.252.236.92	internet_address(v4)	upside	52	20	-	詳細
2019/07/31 18:00:00	254.252.238.105	internet_address(v4)	upside	5	4	-	詳細

図. IP 流量 検知アラート画面

1. ステータス

IP 流量検知のステータスが表示されます。

2. 表示モード

トラフィック流量の表示モードを選択します。

表示モード	説明
パケット	パケット数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します
バイト	バイト数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します
無通信	無通信となった回数の閾値の推移を折れ線グラフで表示します（1 時間を 10 分間隔で分割して計測したときに 10 分間通信トラフィックがなかった回数）

3. 検知対象から除外ボタン

検知対象から当該アラートを除外するように設定に追加できます。

4. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止もしくは検知完了の状態を押下することができ、検知のステータスは学習完了になります。

5. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

6. 検知結果一覧

(ア) 表示モードにパケット・バイトを選択

カラム名	説明
検知日時	トラフィック流量が閾値を超えて検知された日時
送信元 IP アドレス	検知したトラフィックの送信元 IP アドレス
宛先 IP アドレス	検知したトラフィックの宛先 IP アドレス
検知理由	検知理由 (upside: 上限値を超えた、downside: 下限値を下回った)
トラフィック量	検知したトラフィックのトラフィック流量 (パケット数 / バイト数)
上限閾値	パケット数 / バイト数の上限値
下限閾値	パケット数 / バイト数の下限値
操作	詳細ボタンを押下すると当該のトラフィック流量について、1 時間ごとのパケット数、バイト数、無通信回数の閾値の推移をそれぞれ折れ線グラフで表示する画面に遷移します

(イ) 表示モードに無通信を選択

カラム名	説明
検知日時	トラフィック流量が閾値を超えて検知された日時

送信元 IP アドレス	検知したトラフィックの送信元 IP アドレス
宛先 IP アドレス	検知したトラフィックの宛先 IP アドレス
検知理由	検知理由 (no_comm:無通信回数が上限を超えた)
無通信回数	無通信だった回数
上限閾値	無通信回数の上限値
操作	詳細ボタンを押下すると当該のトラフィック流量について、1時間ごとのパケット数、バイト数、無通信回数の閾値の推移をそれぞれ折れ線グラフで表示する画面に遷移します

7. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

検知アラート

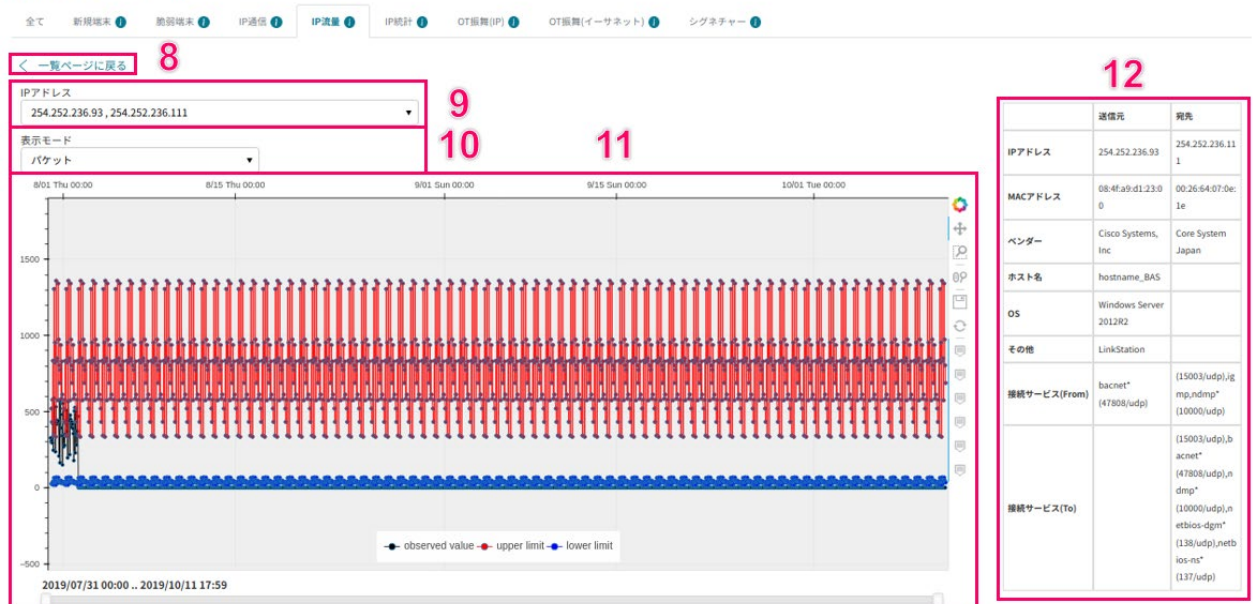


図. IP 流量詳細画面

8. 一覧ページに戻る

トラフィック流量を表示する画面から、遷移前の一覧画面に戻ることができます。

9. IP アドレス

選択された送信元 IP と宛先 IP の組み合わせの上限、下限の閾値の推移を表示します。

10. 表示モード

トラフィック流量の表示モードを選択します。

カラム名	説明
パケット	パケット数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します
バイト	バイト数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します
無通信	無通信となった回数の閾値の推移を折れ線グラフで表示します（1 時間を 10 分間隔で分割して計測したときに 10 分間通信トラフィックがなかった回数）

11. グラフ

IP アドレス・表示モードで選択した条件を適用した推移を折れ線グラフで表示します。

12. 端末の詳細情報

グラフ上でマウスオーバーすると表示されます。送信元/送信先それぞれの、IP アドレス、MAC アドレス、ベンダー、ホスト名、種別・機種、ブラウザー、OS、その他、接続サービス(From)、接続サービス(to) を表形式で表示します。表示する情報がない場合は、行が表示されません（例：OS 名の推定ができなかった場合は、OS の行は表示されない）。

10.6. IP 統計

統計情報を利用して検知された異常に関するアラートの一覧です。

検知アラート

☒ 学習・検知完了

☐ 検知対象から除外

検知日時	IPアドレス	分析種別	統計値種別	実測値	閾値
2019/08/01 22:50:00	254.252.236.123	信頼区間分析	ARP要求送信パケット数	1	0.9999999999
2019/08/01 22:50:00	254.252.236.123	信頼区間分析	ARP要求対象IP数	1	0.9999999999
2019/08/01 22:50:00	254.252.236.123	主成分分析	-	-	-
2019/08/01 22:40:00	254.252.236.123	主成分分析	-	-	-

図. IP 統計 検知アラート画面

1. ステータス

IP 統計のステータスが表示されます。ステータス内容は 11.1 学習・検知ステータスを参照してください。

2. 検知対象から除外ボタン

検知対象から当該アラートを除外する設定を追加登録できます。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	トラフィックを検知した日時
IP アドレス	検知したトラフィックの IP アドレス
分析種別	分析種別（信頼区間分析 / 主成分分析）
統計値種別	信頼区間分析において異常が検知された統計値の種別（主成分分析の場合は空） 種別は以下のとおり ARP 要求対象 IP 数

	ARP 要求送信パケット数 DNS 要求ドメイン数 DNS 要求送信パケット数 MAC アドレス数 送信先 IP 数 送信元ポート数 送信先ポート数 プロトコル番号数 送信パケット数 受信パケット数 送信パケット平均サイズ 受信パケット平均サイズ 送受信パケット数比率（全パケット数で送信パケット数を割った値）
実測値	信頼区間分析の場合の実測値（主成分分析の場合は空）
閾値	信頼区間分析で学習した閾値（主成分分析の場合は空）

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.7. OT 振舞（IP）

IP 上の OT プロトコルにおける特定ファンクションを検知したアラート情報の一覧画面です。

検知アラート



図. OT 振舞（IP） 検知アラート画面

1. ステータス

OT 振舞（IP）検知のステータスが表示されます。

2. 検知除外リストに登録ボタン

選択したアラートを検知除外リストに追加登録できます。追加登録すると、同じアラートは検知されません。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止の状態では押下すると、検知のステータスが検知処理待ちになります。 検知のステータスが検知完了の状態では押下すると、検知結果を削除し、検知のステータスが検知処理待ちになります。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	通信を検知した日時
送信元 IP アドレス	検知した端末の送信元 IP アドレス

送信元ポート	検知した端末の送信元ポート
宛先 IP アドレス	検知した端末の宛先 IP アドレス
宛先ポート	検知した端末の宛先ポート
プロトコル	検知した端末のプロトコル（TCP または UDP）
OT プロトコル	検知した端末の OT プロトコル
ファンクション	検知した端末のファンクション

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.8. OT 振舞（イーサネット）

イーサネット上の OT プロトコルにおける特定ファンクションを検知したアラート情報の一覧画面です。

検知アラート

全て

新規検出

検出済み

IP通信

IP流量

IP統計

OT振舞(IP)

OT振舞(イーサネット)

シグネチャ

✓ 検知完了

検知除外リストに登録

全アラート削除

↓ CSV

<input type="checkbox"/>	検知日時	送信元MACアドレス	宛先MACアドレス	OTプロトコル	ファンクション
<input type="checkbox"/>	2022/12/01 00:02:52	00:11:11:11:11:11	00:00:00:aa:bb:cc	cclink_ie_field	update
<input type="checkbox"/>	2022/12/01 00:02:36	00:11:11:11:11:11	00:00:00:aa:bb:cc	cclink_ie_field	setup
<input type="checkbox"/>	2022/12/01 00:02:32	ab:cd:ef:12:34:56	00:00:00:00:00:02	cclink_ie_control	cyclicDataIn3
<input type="checkbox"/>	2022/12/01 00:02:06	ab:cd:ef:12:34:56	00:00:00:00:00:02	cclink_ie_field	cyclicDataRX cmd02
<input type="checkbox"/>	2022/12/01 00:02:00	ab:cd:ef:12:34:56	00:00:00:00:00:02	cclink_ie_field	update
<input type="checkbox"/>	2022/12/01 00:01:44	ab:cd:ef:12:34:56	00:00:00:00:00:02	cclink_ie_field	setup
<input type="checkbox"/>	2022/12/01 00:01:32	00:11:11:11:11:11	00:00:00:12:34:56	cclink_ie_control	transient2 RUN
<input type="checkbox"/>	2022/12/01 00:01:26	00:11:11:11:11:11	00:00:00:12:34:56	cclink_ie_control	setup

Showing 1 to 8 of 8 rows

図. OT 振舞（イーサネット） 検知アラート画面

1. ステータス

OT 振舞（イーサネット）検知のステータスが表示されます。

2. 検知除外リストに登録ボタン

選択したアラートを検知除外リストに追加登録できます。追加登録すると、同じアラートは検知されません。

3. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。 検知のステータスが検知中止の状態では押下すると、検知のステータスが検知処理待ちになります。 検知のステータスが検知完了の状態では押下すると、検知結果を削除し、検知のステータスが検知処理待ちになります。

4. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

5. 検知結果一覧

カラム名	説明
検知日時	通信を検知した日時
送信元 MAC アドレス	検知した端末の送信元 MAC アドレス
宛先 MAC アドレス	検知した端末の宛先 MAC アドレス
OT プロトコル	検知した端末の OT プロトコル
ファンクション	検知した端末のファンクション

6. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

10.9. シグネチャー

シグネチャーによる検知の一覧画面です。

検知アラート

全て 18 新規検知 0 新規検知 0 IP送信 0 IP受信 0 IP宛先 0 OT宛先(IP) 0 OT宛先(イーサネット) 0 シグネチャー 0

1000件を超える古いアラートは表示されません。

検知除外リストに登録 1

4

2 3

全アラート削除 CSV

<input type="checkbox"/>	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	シグネチャー	脅威カテゴリ	深刻度
<input type="checkbox"/>	2019/08/02 06:28:47	254.252.236.107	1900	163.87.39.105	1900	udp	GPL MISC UPnP の不正なアドバタイズメント	Misc Attack	2
<input type="checkbox"/>	2019/08/02 06:28:47	254.252.236.107	1900	163.87.39.105	1900	udp	GPL MISC UPnP の不正なアドバタイズメント	Misc Attack	2
<input type="checkbox"/>	2019/08/02 06:28:47	254.252.236.107	1900	163.87.39.105	1900	udp	GPL MISC UPnP の不正なアドバタイズメント	Misc Attack	2
<input type="checkbox"/>	2019/08/02 06:28:47	254.252.236.107	1900	163.87.39.105	1900	udp	GPL MISC UPnP の不正なアドバタイズメント	Misc Attack	2
<input type="checkbox"/>	2019/08/02 06:28:47	254.252.236.107	1900	163.87.39.105	1900	udp	GPL MISC UPnP の不正なアドバタイズメント	Misc Attack	2

図. シグネチャー 検知アラート画面

1. 検知除外リストに登録ボタン

検知対象から当該アラートを除外する設定を追加登録できます。

全アラート解除ボタン検知結果をクリアしたい場合に押下します。

2. 全アラート削除ボタン

検知結果をクリアしたい場合に押下します。

3. CSV ボタン

検知結果を CSV ファイルとしてダウンロードできます。

4. 検知結果一覧

カラム名	説明
検知日時	シグネチャーを検知した日時
送信元 IP アドレス	送信元 IP アドレス
送信元ポート番号	送信元ポート番号
宛先 IP アドレス	宛先 IP アドレス
宛先ポート番号	宛先ポート番号

プロトコル	プロトコル（TCP または UDP）
シグネチャー	検知されたシグネチャー
脅威カテゴリ	脅威のカテゴリ
深刻度	脅威の深刻度（1 が最も高く、3 が最も低い）

5. 検知結果フィルタ

検知一覧の各列の内容で一覧をフィルタリングできます。

11. 学習・検知設定

11.1. 学習・検知ステータス

各脅威検知機能の学習・検知ステータスを表示する画面です。

学習・検知設定

1 検知種別	2 ステータス	3 設定データ	4 最大学習期間
新規端末	未学習未検知	学習・検知 未設定	30 日
脆弱端末	未検知	学習・検知 未設定	0 日
IP通信	未学習未検知	学習・検知 未設定	30 日
IP流量	未学習未検知	学習・検知 未設定	21 日
IP統計	未学習未検知	学習・検知 未設定	30 日
OT振舞(IP)	未検知	学習・検知 未設定	0 日
OT振舞(イーサネット)	未検知	学習・検知 未設定	0 日
シグネチャ	検知中	学習・検知 未設定	0 日

図. 学習・検知ステータス画面

1. 検知種別

学習・検知対象の脅威検知機能種別を表示します。

2. ステータス

各脅威検知機能の学習・検知状態を表示します。

ステータス	説明
未学習未検知	初期状態
学習・検知処理待ち	学習・検知開始待ち状態
学習・検知中	学習・検知中状態
学習・検知完了	学習・検知完了状態
学習・検知初期化中	学習・検知初期化中状態
学習・検知失敗	学習・検知が失敗した状態

3. 設定データ

各脅威検知機能の学習・検知それぞれで使用するデータを表示します。使用するデータが設定されていない場合は未設定が表示されます。使用するデータが設定されている場合は設定したデータの期間が表示されます。使用するデータが設定されており、学習・検知モードがリアルタイム検知の場合は検知に開始日時と停止まで継続中のメッセージが表示されます。

4. 最大学習期間

期間指定で指定した期間内で学習する最大期間を表示します。

11.2. 学習・検知ステータス（アドバンスモード）

各脅威検知機能の学習・検知ステータスを表示する画面です。

学習・検知設定

1 検知種別	2 学習・検知モード	3 ステータス	4 設定データ
新規端末	未学習	未学習	学習 未設定 検知 未設定
脆弱端末	検知処理待ち	検知処理待ち	検知 未設定
IP通信	未学習	未学習	学習 未設定 検知 未設定
IP接続	未学習	未学習	学習 未設定 検知 未設定
OT振替(IP)	検知処理待ち	検知処理待ち	検知 未設定
OT振替(イーサネット)	検知処理待ち	検知処理待ち	検知 未設定
シグネチャー	-	検知中	検知 未設定

図. 学習・検知ステータス画面（アドバンスモード）

1. 検知種別

学習・検知対象の脅威検知機能種別を表示します。

2. 学習・検知モード

各脅威検知機能の学習・検知モードを表示します。

※学習・検知モードが未設定の場合、ステータスを表示します。

学習・検知モード	説明
既存データ検知	すでに取り込まれているデータを対象として検知するモード
アップロード学習	登録された学習モデルで学習するモード
リアルタイム検知	リアルタイムに収集するデータを対象として検知するモード

3. ステータス

各脅威検知機能の学習・検知状態を表示します。

ステータス	説明
未学習	初期状態

学習処理待ち	学習開始待ち状態
学習中	学習中状態
学習完了	学習完了状態
学習初期化中	学習初期化中状態
学習失敗	学習が失敗した状態
学習完了待ち	学習完了待ち状態
検知処理待ち	検知開始待ち状態
検知中	検知中状態
検知完了	検知完了状態
検知一時中止	学習を一時停止した状態
検知初期化中	検知初期化中状態
検知失敗	検知が失敗した状態

4. 設定データ

各脅威検知機能の学習・検知それぞれで使用するデータを表示します。使用するデータが設定されていない場合は未設定が表示されます。使用するデータが設定されている場合は設定したデータの期間が表示されます。使用するデータが設定されており、学習・検知モードがリアルタイム検知の場合は検知に開始日時と停止まで継続中のメッセージが表示されます。

11.3. 新規端末

新規端末学習済データ（学習期間中に観測された端末情報）の一覧画面です。



図. 新規端末学習済リスト画面

1. ステータス

新規端末検知のステータスが表示されます。

2. 端末追加ボタン

学習データに新規端末データを追加登録できます。

3. 全アラート削除ボタン

学習結果をクリアしたい場合に押下します。 学習のステータスが学習中止もしくは学習完了の状態で押下でき、学習済みのモデルを削除し、学習のステータスが未学習になります。

4. CSV ボタン

学習済みのモデルを CSV ファイルとしてダウンロードできます。

注意 一覧上で「internet_address (v4)」「internet_address (v6)」と表記されている IP アドレスについて、学習済のモデルとしてダウンロードする際は、それぞれグローバルアドレス集約時の置き換え用ループバックアドレス「127.12.34.56」「::1」に置き換えて出力されます。

5. 学習データ一覧

カラム名	説明
×	「×」をクリックすると、当該学習データを学習済リストから削除します
操作	設定変更ボタンを押下すると、当該学習データを変更できます
IP アドレス	端末の IP アドレス
MAC アドレス	端末の MAC アドレス

6. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。



学習・検知設定

学習・検知ステータス 新規端末 脆弱端末 IP通信 IP流量

< 一覧ページに戻る 7

学習済リスト

IPアドレス 8
例: 192.0.2.1

MACアドレス 9
例: 00:00:5e:00:53:00

追加 10

図. 端末追加画面

7. 一覧ページに戻る

端末追加画面から、新規端末学習済データ一覧画面に戻ることができます。

8. IP アドレス

学習データに追加する端末の IP アドレスを入力できます。

9. MAC アドレス

学習データに追加する端末の MAC アドレスを入力できます。

10. 追加ボタン

追加ボタンを押下することで端末情報を学習データに追加することができます。

11.4. 脆弱端末

脆弱端末（サポート切れ OS を利用している端末）の検知除外リスト一覧です。



図. 脆弱端末検知除外リスト画面

1. ステータス

脆弱端末検知のステータスが表示されます。

2. 端末追加ボタン

検知除外リストに脆弱端末データを追加登録できます。

3. 全検知除外設定削除ボタン

検知除外リストをクリアしたい場合に押下します。

4. CSV ボタン

検知除外リストの一覧を CSV ファイルとしてダウンロードできます。

5. 検知除外端末一覧

カラム名	説明
×	「×」をクリックすると、当該データを検知除外リストから削除します
IP アドレス	IP アドレス
MAC アドレス	MAC アドレス
OS	OS 情報

6. 学習データフィルタ

5. 学習データ一覧の各列の内容で一覧をフィルタリングできます。

学習・検知設定

学習・検知ステータス 新規端末 **脆弱端末** IP通信 IP流量

[← 一覧ページに戻る](#) **7**

検知除外リスト

IPアドレス **8**
例: 192.0.2.1

MACアドレス **9**
例: 00:00:5e:00:53:00

OS **10**
例: Windows Server 2012

追加 **11**

図. 端末追加画面

7. 一覧ページに戻る

端末追加画面から、検知除外リスト一覧画面に戻ることができます。

8. IP アドレス

検知除外リストに追加する端末の IP アドレスを入力できます。

9. MAC アドレス

検知除外リストに追加する端末の MAC アドレスを入力できます。

10. OS

検知除外リストに追加する端末の OS 名を入力できます。

11. 追加ボタン

追加ボタンを押下することで端末情報を検知除外リストに追加することができます。

11.5. IP 通信

ネットワークホワイトリスト（学習期間中に観測された IP アドレス、プロトコル、ポート番号）の一覧画面です。

学習・検知設定

学習・検知ステータス 新規検知 検知結果 IP通信 IP流量 IP統計 OT監視(IP) OT監視(イーサネット) シグネチャ 全般

学習済リスト

1 2 3 4 5 6

学習完了 通信追加 全学習データ削除 CSV

操作	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
X 設定変更	10.0.2.15	*	internet_address(v4)	80	tcp
X 設定変更	10.0.2.15	*	internet_address(v4)	123	udp
X 設定変更	10.0.2.15	*	internet_address(v4)	443	tcp
X 設定変更	10.0.2.15	*	internet_address(v4)	443	udp

図. IP 通信画面学習済リスト画面

1. ステータス

IP 通信検知のステータスが表示されます。

2. 通信追加ボタン

学習データに IP 通信データを追加登録できます。

3. 全学習データ削除ボタン

学習結果をクリアしたい場合に押下します。 学習のステータスが学習中止もしくは学習完了の状態を押下でき、学習済みのモデルを削除し、学習のステータスが未学習になります。

4. CSV ボタン

学習済みのモデルを CSV ファイルとしてダウンロードできます。

注意 一覧上で「internet_address (v4)」「internet_address (v6)」と表記されている IP アドレスについて、学習済のモデルとしてダウンロードする際は、それぞれグローバルアドレス集約時の置き換え用ループバックアドレス「127.12.34.56」「::1」に置き換えて出力されます。

5. 学習データ一覧

カラム名	説明
×	「×」をクリックすると、当該学習データを学習済みリストから削除します
操作	設定変更ボタン押下すると、当該学習データを変更できます
送信元 IP アドレス	送信元 IP アドレス
送信元ポート	送信元ポート番号
宛先 IP アドレス	宛先 IP アドレス
宛先ポート	宛先ポート番号
プロトコル	プロトコル (TCP または UDP)

6. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

学習・検知設定 ①

学習・検知ステータス

新規端末

脆弱端末

IP通信

< 一覧ページに戻る

7

学習済みリスト

送信元IPアドレス

例: 192.0.2.1

8

送信元ポート ①

例: 80

9

宛先IPアドレス

例: 192.0.2.1

10

宛先ポート ①

例: 443

11

プロトコル

例: icmp

12

追加

13

図. 通信追加画面

7. 一覧ページに戻る

端末追加画面から、ネットワークホワイトリスト一覧画面に戻ることができます。

8. 送信元 IP アドレス

学習データに追加する通信の送信元 IP アドレスを入力できます。

9. 送信元ポート

学習データに追加する通信の送信元ポート番号を入力できます。任意のポート番号として「*」を指定することもできます。

10. 宛先 IP アドレス

学習データに追加する通信の宛先 IP アドレスを入力できます。

11. 宛先ポート

学習データに追加する通信の宛先ポート番号を入力できます。任意のポート番号として「*」を指定することもできます。

12. プロトコル

学習データに追加する通信のプロトコル名を入力できます。

13. 追加ボタン

追加ボタンを押下することで通信情報をネットワークホワイトリストに追加することができます。

11.6. IP 流量

IP 流量学習済データ（学習期間中に測定されたトラフィック流量から学習した結果）の送信元・宛先 IP アドレス一覧を表示する画面です。

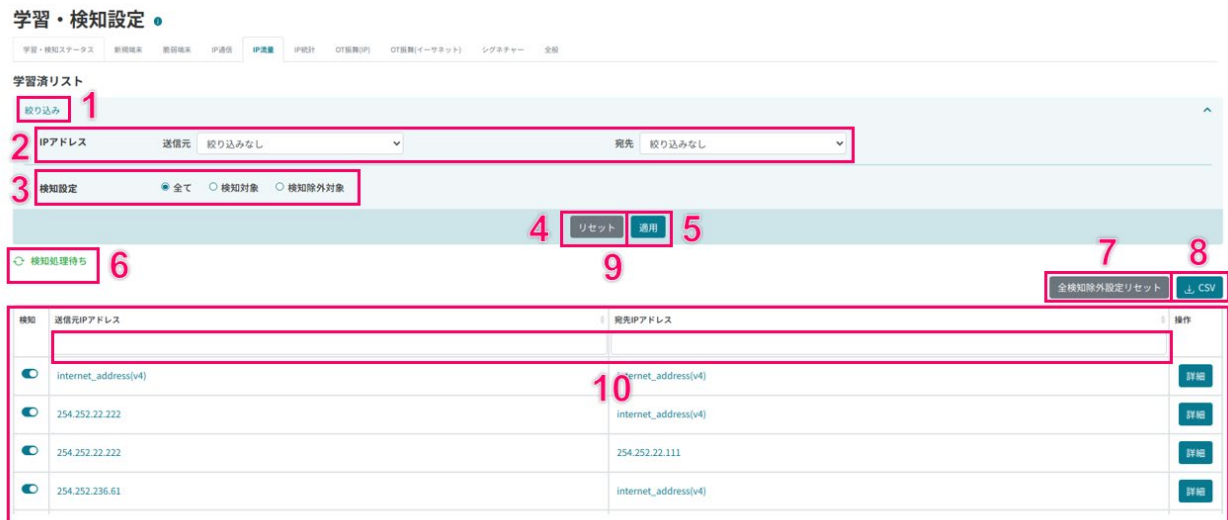


図. IP 流量学習済リスト画面

1. 絞り込み

表示する学習結果を絞り込むことができます。

2. IP アドレス

送信元を指定した場合、送信元 IP アドレスの絞り込みを設定できます。宛先を指定した場合、宛先 IP アドレスの絞り込みを設定できます。

3. 検知設定

検知対象、検知対象外の絞り込みを設定できます。全てを指定した場合、検知対象、検知対象外のいずれも表示できます。

4. リセットボタン

IP アドレス・検知設定で指定した選択をリセットできます。

5. 適用ボタン

IP アドレス・検知設定で指定した選択を適用した画面を表示できます。

6. ステータス

IP 流量検知のステータスが表示されます。

7. 全検知除外設定リセットボタン

全検知除外設定をリセットして全て検知対象としたい場合に押下します。

8. CSV ボタン

学習済みのモデルを CSV ファイルとしてダウンロードできます。

注意 一覧上で「internet_address (v4)」「internet_address (v6)」と表記されている IP アドレスについて、学習済みのモデルとしてダウンロードする際は、それぞれグローバルアドレス集約時の置き換え用ループバックアドレス「127.12.34.56」「::1」に置き換えて出力されます。

9. 学習データ一覧

カラム名	説明
検知	検知の ON/OFF
送信元 IP アドレス	送信元 IP アドレス
宛先 IP アドレス	宛先 IP アドレス
操作	詳細ボタンを押下すると当該の 1 週間分のトラフィック流量について、1 時間ごとのパケット数、バイト数、無通信回数の閾値の推移をそれぞれ折れ線グラフで表示する画面に遷移します

10. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

学習・検知設定



図. IP 流量詳細画面

11. 一覧ページに戻る

トラフィック流量を表示する画面から、遷移前の一覧画面に戻ることができます。

12. IP アドレス

選択された送信元 IP と宛先 IP の組み合わせの上限、下限の閾値の推移を表示します。

13. 表示モード

トラフィック流量の表示モードを選択します。

表示モード	説明
パケット	パケット数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します
バイト	バイト数によるトラフィック流量の上限、下限の閾値の推移を折れ線グラフで表示します

無通信	無通信となった回数の閾値の推移を折れ線グラフで表示します（1 時間を 10 分間隔で分割して計測したときに 10 分間通信トラフィックがなかった回数）
-----	---

14. 検知設定

検知を ON/OFF できます。

15. グラフ

IP アドレス・表示モードで選択した条件を適用した設定を折れ線グラフで表示します。

16. CSV ボタン

学習済みのモデルを CSV ファイルとしてダウンロードできます。

17. 端末の詳細情報

グラフ上でマウスオーバーすると表示されます。送信元/宛先それぞれの、IP アドレス、MAC アドレス、ベンダー、サービス、ホスト名、種別・機種、ブラウザ、OS、その他、を表形式で表示します。表示する情報がない場合は、行が表示されません（例：OS 名の推定ができなかった場合は、OS の行は表示されない）。

11.7. IP 統計

統計情報を利用した異常検知に関する学習済みリストの表示と設定が行えます。

学習・検知設定

学習・検知ステータス 新規検知 検知結果 IP通信 IP流量 **IP統計** OT振舞(P) OT振舞(イーサネット) シグネチャ 全般

端末学習状況リスト

1 2 3 4 5

検知モード	IPアドレス	学習状態 (信頼区間)	学習状態 (主成分)
検知しない 弱 強	254.252.126.60	未学習	学習完了
検知しない 弱 強	254.252.236.61	学習中	学習完了
検知しない 弱 強	254.252.236.63	学習中	学習完了
検知しない 弱 強	254.252.236.79	学習中	学習完了
検知しない 弱 強	254.252.236.88	学習中	学習完了

全検知除外設定リセット

図. IP 統計端末学習状況リスト画面

1. ステータス

IP 統計検知のステータスが表示されます。

2. 検知モード更新ボタン

一覧で設定された検知モードを学習データに設定できます。

3. 全検知除外設定リセットボタン

全端末の検知モードをデフォルト値にリセットしたい場合に押下します。デフォルト値は「弱」です。

4. 学習データ一覧

カラム名	説明
検知モード	検知しない/弱/強 の切り替えを選択 弱の場合は信頼区間分析/主成分分析いずれかで検知された場合にアラート化 強の場合は信頼区間分析/主成分分析の両方で検知された場合にのみアラート化 デフォルトは「弱」
IP アドレス	IP アドレス
学習状態 (信頼区間)	信頼区間分析の学習状態 (未学習/学習完了)

学習状態（主成分）	主成分分析の学習状態（未学習/学習完了）
-----------	----------------------

- 信頼区間分析

IP アドレス単位に要約統計量に対して信頼区間を計算する。

信頼区間は、ポアソン分布か正規分布のいずれかに従うと仮定、単位時間当たりの生起量（ポアソン過程に従う事象）であるものはポアソン分布、その他は正規分布で計算し、信頼水準の値は設定値とする

信頼区間モデルの値が収束したものから学習済みとして検知へ移行する。

- 主成分分析

IP アドレス単位に「全」要約統計量を用いて主成分分析を行う。

一定期間分のデータで学習を行った後に検証期間を設けて、異常が検知されなかった場合に検知へ移行する。

- 分析に使用する要約統計量（端末単位・5分（設定値）毎に計算）

ARP 要求対象 IP 数

ARP 要求送信パケット数

DNS 要求ドメイン数

DNS 要求送信パケット数

MAC アドレス数

送信先 IP 数

送信元ポート数

送信先ポート数

プロトコル番号数

送信パケット数

受信パケット数

送信パケット平均サイズ

受信パケット平均サイズ

送受信パケット数比率（全パケット数で送信パケット数を割った値）

5. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

11.8. OT 振舞（IP）

OT 振舞（IP）（IP 上の OT プロトコルにおける特定ファクションの検知）の検知除外リスト一覧です。



図. OT 振舞（IP） 検知除外リスト画面

1. ステータス

OT 振舞（IP）検知のステータスが表示されます。

2. 通信追加ボタン

OT 振舞（IP）検知しない通信を登録します。

3. 全検知除外設定削除ボタン

OT 振舞（IP）検知しない除外設定をすべて削除します。

4. CSV ボタン

OT 振舞（IP）検知の除外リストをダウンロードできます。

5. 検知除外一覧

カラム名	説明
×	「×」をクリックすると、当該データを検知除外リストから削除します
送信元 IP アドレス	送信元 IP アドレス
宛先 IP アドレス	宛先 IP アドレス
OT プロトコル	検知除外設定された OT プロトコル

	*（アスタリスク）は全ての OT プロトコル
ファンクション	検知除外設定されたファンクション *（アスタリスク）は全てのファンクション

6. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

7. ファンクション選択ボタン

ファンクション毎に OT 振舞（IP）検知の ON/OFF を設定します。

学習・検知設定

[学習・検知ステータス](#)
[新規端末](#)
[脆弱端末](#)
[IP通信](#)
[IP流量](#)
[IP統計](#)
[OT振舞\(IP\)](#)

[< 一覧ページに戻る](#) **8**

検知除外リスト

送信元IPアドレス

9

宛先IPアドレス

10

OTプロトコル

全て ▾

11

ファンクション

全て ▾

12

追加

13

図. 通信追加画面

8. 一覧ページに戻る

追加画面から、OT 振舞（IP）検知除外リスト画面に戻ることができます。

9. 送信元 IP アドレス

検知除外リストに追加する送信元 IP アドレスまたはネットワークアドレスを入力できます。

10. 宛先 IP アドレス

検知除外リストに追加する宛先 IP アドレスまたはネットワークアドレスを入力できます。

11. OT プロトコル

検知除外リストに追加する OT プロトコルを選択できます。

12. ファンクション

検知除外リストに追加するファンクションを選択できます。

13. 追加ボタン

追加ボタンを押下することで通信情報を検知除外リストに追加することができます。

図. 検知対象ファンクション画面

14. 検知除外リストに戻る

検知対象ファンクション画面から、OT 振舞（IP）検知除外リスト画面に戻ることができます。

15. OT プロトコル

ファンクションを表示する OT プロトコルを選択できます。

16. 検知対象ファンクション

検知対象のファンクション毎に検知の ON/OFF を設定できます。

11.9. OT 振舞（イーサネット）

OT 振舞（イーサネット）（イーサネット上の OT プロトコルにおける特定ファクションの検知）の検知除外リスト一覧です。



図. OT 振舞（イーサネット） 検知除外リスト画面

1. ステータス

OT 振舞（イーサネット）検知のステータスが表示されます。

2. 通信追加ボタン

OT 振舞（イーサネット）検知しない通信を登録します。

3. 全検知除外設定削除ボタン

OT 振舞（イーサネット）検知しない除外設定をすべて削除します。

4. CSV ボタン

OT 振舞（イーサネット）検知の除外リストをダウンロードできます。

5. 検知除外一覧

カラム名	説明
×	「×」をクリックすると、当該データを検知除外リストから削除します
送信元 MAC アドレス	送信元 MAC アドレス
宛先 MAC アドレス	宛先 MAC アドレス
OT プロトコル	検知除外設定された OT プロトコル

	*（アスタリスク）は全ての OT プロトコル
ファンクション	検知除外設定されたファンクション *（アスタリスク）は全てのファンクション

6. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

7. ファンクション選択ボタン

ファンクション毎に OT 振舞（イーサネット）検知の ON/OFF を設定します。

学習・検知設定 ①

学習・検知ステータス 新規端末 脆弱端末 IP通信 IP流量

< 一覧ページに戻る 8

検知除外リスト

送信元MACアドレス

例: 00:00:00:00:00:01

9

宛先MACアドレス

例: 00:00:00:00:00:01

10

OTプロトコル

全て ▼

11

ファンクション

全て ▼

12

追加

13

図. 通信追加画面

8. 一覧ページに戻る

追加画面から、OT 振舞（イーサネット）検知除外リスト画面に戻ることができます。

9. 送信元 MAC アドレス

検知除外リストに追加する送信元 MAC アドレスを入力できます。

10. 宛先 MAC アドレス

検知除外リストに追加する宛先 MAC アドレスを入力できます。

11. OT プロトコル

検知除外リストに追加する OT プロトコルを選択できます。

12. ファンクション

検知除外リストに追加するファンクションを選択できます。

13. 追加ボタン

追加ボタンを押下することで通信情報を検知除外リストに追加することができます。

学習・検知設定

学習・検知ステータス 新規端末 脆弱端末 IP通信 IP流量 IP統計 OT振舞(IP) **OT振舞(イーサネット)** シグネチャ 全般

14 < 検知除外リストに戻る

検知対象ファンクション

OTプロトコル cclink_ie_field 15

persuasion	<input type="checkbox"/>	transient1 統計情報取得応答	<input type="checkbox"/>	transient1 SLMP送信要求	<input type="checkbox"/>	paramaCheck	<input type="checkbox"/>
testData	<input type="checkbox"/>	transient1 ノード詳細情報取得要求	<input type="checkbox"/>	transient1 SLMP送信応答	<input type="checkbox"/>	parameter	<input type="checkbox"/>
testDataAck	<input type="checkbox"/>	transient1 ノード詳細情報取得応答	<input type="checkbox"/>	transientAck	<input type="checkbox"/>	measure	<input type="checkbox"/>
setup	<input checked="" type="checkbox"/>	transient1 オプション情報取得要求	<input type="checkbox"/>	transient2 メモリアクセス情報取得	<input type="checkbox"/>	measureAck	<input type="checkbox"/>
setupAck	<input type="checkbox"/>	transient1 オプション情報取得応答	<input type="checkbox"/>	transient2 RUN	<input type="checkbox"/>	offset	<input type="checkbox"/>
token	<input type="checkbox"/>	transient1 通信周期設定要求	<input checked="" type="checkbox"/>	transient2 STOP	<input checked="" type="checkbox"/>	update	<input checked="" type="checkbox"/>
timer	<input type="checkbox"/>	transient1 通信周期設定応答	<input type="checkbox"/>	transient2 メモリ読み出し	<input type="checkbox"/>	cyclicDataRWw	<input type="checkbox"/>
myStatus	<input type="checkbox"/>	transient1 オブジェクト読み出し要求	<input type="checkbox"/>	transient2 メモリ書き込み	<input checked="" type="checkbox"/>	cyclicDataRY	<input type="checkbox"/>
transient1 ノード配信情報要求	<input type="checkbox"/>	transient1 オブジェクト読み出し応答	<input type="checkbox"/>	transient2 メッセージ伝送	<input type="checkbox"/>	cyclicDataRWr	<input type="checkbox"/>
transient1 ノード配信情報応答	<input type="checkbox"/>	transient1 オブジェクト書き込み要求	<input checked="" type="checkbox"/>	transient2 メーカー固有	<input type="checkbox"/>	cyclicDataRX	<input type="checkbox"/>
transient1 統計情報取得要求	<input type="checkbox"/>	transient1 オブジェクト書き込み応答	<input type="checkbox"/>	ipTransient	<input type="checkbox"/>	未定義	<input checked="" type="checkbox"/>

16

図. 検知対象ファンクション画面

14. 検知除外リストに戻る

検知対象ファンクション画面から、OT 振舞（イーサネット）検知除外リスト画面に戻ることができます。

15. OT プロトコル

ファンクションを表示する OT プロトコルを選択できます。

16. 検知対象ファンクション

検知対象のファンクション毎に検知の ON/OFF を設定できます。

11.10. シグネチャー

シグネチャーによる検知除外の一覧画面です。

学習・検知設定

学習・検知ステータス

新検知設定

検知除外

IP通信

IP流量

IP統計

OT振舞(IP)

OT振舞(イーサネット)

シグネチャー

全検

検知除外リスト

シグネチャー追加

全検知除外設定削除

CSV

	送信元IPアドレス	除外タイプ	シグネチャー
X	10.20.1.1	カテゴリ	POLICY
X	10.20.1.2	シグネチャー	ET DNS Hiloti DNS CnC チャネルのインストール成功メッセージ

Showing 1 to 2 of 2 rows

図. シグネチャー検知除外リスト画面

1. シグネチャー追加ボタン

シグネチャー検知しない送信元 IP アドレスとシグネチャーの組を登録します。

2. 全検知除外設定削除ボタン

シグネチャー検知しない除外設定をすべて削除します。

3. CSV ボタン

シグネチャー検知の除外リストを CSV ファイルとしてダウンロードできます。

4. 検知除外一覧

カラム名	説明
------	----

×	「×」をクリックすると、当該データを検知除外リストから削除します
送信元 IP アドレス	送信元 IP アドレス
除外タイプ	カテゴリまたはシグネチャー
シグネチャー	検知除外設定されたシグネチャー

5. 学習データフィルタ

学習データ一覧の各列の内容で一覧をフィルタリングできます。

学習・検知設定

[学習・検知ステータス](#)
[新規端末](#)
[脆弱端末](#)
[IP通信](#)
[IP流量](#)

[一覧ページに戻る](#)

検知除外リスト

IPアドレス

例: 192.0.2.1

☐ カテゴリ
 ☒ シグネチャー

シグネチャー

ET ATTACK_RESPONSE Cisc...

追加

図. シグネチャー追加画面

6. 一覧ページに戻る

追加画面から、シグネチャー検知除外一覧画面に戻ることができます。

7. IP アドレス

シグネチャー検知除外一覧に追加する IP アドレスを入力できます。

8. カテゴリ/シグネチャー選択

除外する対象をカテゴリ単位で指定するかシグネチャー単位で指定するか選択できます。

9. シグネチャー

シグネチャー検知除外一覧に追加するシグネチャー、またはカテゴリを選択できます。

10. 追加ボタン

追加ボタンを押下することでシグネチャー除外情報を一覧に追加することができます。

IT/OT 非分離環境において、IP 流量の学習には 2 日程度かかります。

1. アドバンスモード

アドバンスモードの ON/OFF の切り替えを行うトグルボタンです。

2. 通知設定

設定したメールアドレスに検知を通知できます。 最大 5 件のメールアドレスを設定できます。 複数のメールアドレスを設定する場合は、カンマ (,) で区切ってください。

3. 通知設定詳細

種別ごとにメールで通知する、しないを指定します。シグネチャーのみ通知する深刻度を指定できます。

4. 登録ボタン

通知設定で設定したメールアドレスを登録します。

5. 種別

学習・検知対象の脅威検知機能を選択します。

6. ステータス

各脅威検知機能の学習・検知状態を表示します。

新規端末、IP 通信、IP 流量、IP 統計の種別ステータス

ステータス	説明
未学習未検知	初期状態
学習・検知処理待ち	学習・検知開始待ち状態
学習・検知中	学習・検知中状態
学習・検知完了	学習・検知完了状態
学習・検知初期化中	学習・検知初期化中状態
学習・検知失敗	学習・検知が失敗した状態

脆弱端末、OT 振舞（IP）、OT 振舞（イーサネット）、シグネチャーの種別ステータス

ステータス	説明
未検知	初期状態
検知処理待ち	検知開始待ち状態
検知中	検知中状態
検知完了	検知完了状態
検知中止	検知初期化中状態
学習・検知失敗	検知が失敗した状態

7. アクション

各脅威検知機能の学習処理を制御します。

アクション	説明
開始	検知処理を開始します
初期化	学習・検知内容をすべて削除し初期化します
最大学習期間変更	最大学習期間の値を変更します

8. 期間指定

検知期間を指定します。 開始日時、終了日時を指定した場合、指定した期間を対象とします。 終了日時のみを指定した場合、終了日時以前のデータを対象とします。 開始日時のみを指定した場合、開始日時以降の期間を対象とします。

9. 最大学習期間

期間指定で指定した期間内で学習する最大期間を指定します。

10. 実行ボタン

種別で選択した各脅威検知機能に対し、アクション・期間指定・最大学習期間で設定した項目の内容に応じた学習・検知処理を行います。

11.12. 全般（アドバンスモード）

脅威検知機能を制御する画面です。アドバンスモードは学習期間や検知期間、学習モードを指定するなど、高度な分析を行いたい場合に使用します。

学習・検知設定

学習・検知ステータス 新規端末 脆弱端末 IP通信 IP流量 IP統計 OT振舞(IP) OT振舞(イーサネット) OT通信 シグネチャー 全般

1 アドバンスモード ☒

2 通知設定

複数のメールアドレスを指定する際は、カンマで区切ってください(最大5件)
例: aaa@example.com, bbb@example.com

3

種別	通知設定
新規端末	すべて通知 <input type="checkbox"/>
脆弱端末	すべて通知 <input type="checkbox"/>
IP通信	すべて通知 <input type="checkbox"/>
IP流量	すべて通知 <input type="checkbox"/>

3

IP統計	すべて通知 <input type="checkbox"/>
OT通信	すべて通知 <input type="checkbox"/>
OT振舞(IP)	すべて通知 <input type="checkbox"/>
OT振舞(イーサネット)	すべて通知 <input type="checkbox"/>
シグネチャー	すべて通知 <input type="checkbox"/>

4 登録

学習設定

5

6

7

8

9

<input type="checkbox"/>	学習種別	ステータス	学習モード	アクション	期間指定
<input type="checkbox"/>	新規端末	<input checked="" type="checkbox"/> 未学習	既存データ リアルタイム アップロード ファイル名:	<input type="radio"/> 開始 <input checked="" type="radio"/> 初期化	2019/07/29 17:00 ~ 2019/08/02 07:00
<input type="checkbox"/>	IP通信	<input checked="" type="checkbox"/> 未学習	既存データ リアルタイム アップロード ファイル名:	<input type="radio"/> 開始 <input checked="" type="radio"/> 初期化	2019/07/29 17:00 ~ 2019/08/02 07:00
<input type="checkbox"/>	IP流量	<input checked="" type="checkbox"/> 未学習	既存データ リアルタイム アップロード ファイル名:	<input type="radio"/> 開始 <input checked="" type="radio"/> 初期化	2019/07/29 17:00 ~ 2019/08/02 07:00
<input type="checkbox"/>	OT通信	<input checked="" type="checkbox"/> 未学習	既存データ リアルタイム アップロード ファイル名:	<input type="radio"/> 開始 <input checked="" type="radio"/> 初期化	2019/07/29 17:00 ~ 2019/08/02 07:00

10 11

実行	実行オプション
通常	
検知設定	学習完了後、自動的に検知開始(検知モード: 既存データ) 学習完了後、自動的に検知開始(検知モード: リアルタイム)

図. 全般(アドバンスモード)画面(学習設定)

IT/OT 非分離環境において、IP 流量の学習には 2 日程度かかります。

1. アドバンスモード

アドバンスモードの ON/OFF の切り替えを行うトグルボタンです。

2. 通知設定

設定したメールアドレスに検知を通知できます。最大 5 件のメールアドレスを設定できます。複数のメールアドレスを設定する場合は、カンマ (,) で区切ってください。

3. 通知設定詳細

種別ごとにメールで通知する、しないを指定します。シグネチャーのみ通知する深刻度を指定できます。

4. 登録ボタン

通知設定で設定したメールアドレスを登録します。

5. 学習種別

学習対象の脅威検知機能を選択します。

6. ステータス

各脅威検知機能の学習状態を表示します。

ステータス	説明
未学習	初期状態
学習処理待ち	学習開始待ち状態
学習中	学習中状態
学習完了	学習完了状態
学習中止	学習初期化中状態
学習失敗	学習が失敗した状態

7. 学習モード

各脅威検知機能の学習に使用するデータソースを指定します。

データソース	説明
既存データ	すでに取り込まれているデータを対象として学習する
リアルタイム	すでに取り込まれているデータとリアルタイムに収集するデータを対象として学習する
アップロード	学習済みのモデルを登録する場合に選択する。モデルのフォーマットは CSV ダウンロードボタンで出力される形式のみ

8. アクション

各脅威検知機能の学習処理を制御します。

アクション	説明
開始	学習処理を開始します
初期化	学習結果を中止し初期化します

9. 期間指定

学習期間を指定します。 開始日時、終了日時を指定した場合、指定した期間を対象とします。 終了日時のみを指定した場合、終了日時以前のデータを対象とします。 開始日時のみを指定した場合、開始日時以降の期間を対象とします。

10. 実行ボタン

学習種別で選択した各脅威検知機能に対し、学習モード・アクション・期間指定で設定した項目の内容に応じた学習処理を行います。

11. 実行オプション

学習完了後、自動で検知を開始するためのオプションを設定できます。

実行オプション	説明
通常	学習完了後、自動的に検知開始を行いません
学習完了後、自動的に検知開始 (検知モード：既存データ)	学習完了後、自動的に既存データを対象に検知を行います

学習完了後、自動的に検知開始 (検知モード：リアルタイム)	学習完了後、自動的にリアルタイムに収集するデータを対象に検知を行います
----------------------------------	-------------------------------------

検知設定

12	13	14	15	16
検知種別	ステータス	検知モード	アクション	期間指定
<input type="checkbox"/> 新規端末	学習完了待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> 脆弱端末	検知処理待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> IP通信	学習完了待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> IP流量	学習完了待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> OT振舞(IP)	検知処理待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> OT振舞(イーサネット)	検知処理待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
<input type="checkbox"/> OT通信	学習完了待ち	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00
17 <input type="checkbox"/> シグネチャ	検知中	既存データ リアルタイム	<input type="radio"/> 開始 <input type="radio"/> 一時停止 <input checked="" type="radio"/> 初期化	2019/08/02 07:00 ~ 2019/08/02 07:00

17 実行

図. 全般（アドバンスモード）画面（検知設定）

12. 検知種別

検知対象の脅威検知機能を選択します。

13. ステータス

各脅威検知機能の検知状態を表示します。

ステータス	説明
学習完了待ち	学習完了待ち状態
検知処理待ち	検知開始待ち状態
検知中	検知中状態
検知完了	検知完了状態
検知一時中止	検知を一時停止した状態
検知初期化中	検知を初期化している状態
検知失敗	検知が失敗した状態

14. 検知モード

各脅威検知機能の検知に使用するデータソースを指定します。

検知モード	説明
既存データ	すでに取り込まれているデータを対象として検知する
リアルタイム	すでに取り込まれているデータとリアルタイムに収集するデータを対象として検知する

15. アクション

各脅威検知機能の学習処理を制御します。

アクション	説明
開始	検知処理を開始します
一時停止	検知処理を一時停止します。再度検知を行う場合は、開始を行う必要があります
初期化	検知結果を初期化します

16. 期間指定

検知期間を指定します。 開始日時、終了日時を指定した場合、指定した期間を対象とします。 終了日時のみを指定した場合、終了日時以前のデータを対象とします。 開始日時のみを指定した場合、開始日時以降の期間を対象とします。

17. 実行ボタン

検知種別で選択した各脅威検知機能に対し、検知モード・アクション・期間指定で設定した項目の内容に応じた学習処理を行います。

12. システム設定

12.1. 設定変更

システムに関する設定画面です。



図. 設定変更画面（データベース・サブネット）

1. 蓄積中のデータを今すぐ可視化する

「実行」ボタンを押下すると、蓄積中のデータを今すぐ可視化する処理を開始します。可視化する処理を実行中は再度実行できません。

2. 長期保存用データベースを参照する

長期保存用データベースの参照を ON/OFF できます。ON にすると画面表示に時間を要する可能性があるため、30 日より前のデータを参照する場合に限り、ON にすることを推奨します。

3. 既定サブネット

ミラー対象のサブネットと同一サブネットとして扱うサブネット。システム固定値であり、変更はできません。

4. 追加サブネット

既定サブネットに追加して、同一サブネットとして扱いたいサブネットを設定します。自動更新を ON にすると、可視化データの作成処理時にデータベースに含まれる情報から追加すべきサブネットを自動計算して更新できます。手動入力欄にサブネット情報を入力（カンマ区切りで複数入力できます）後、「登録」ボタンを押下することで、任意のサブネット情報を登録できます。自動更新が ON の場合、手動入力したサブネットは自動計算で算出されたサブネットにマージされた内容で上書き更新されます。（手動入力したサブネットを変更したくない場合は自動更新を OFF にしてください。）

インターネットアドレス可視化 ⓘ

5

個々のグローバルIPアドレスを可視化・検知対象としてデータインポートする
☐

6

可視化対象のグローバルIPアドレスレンジ

登録

複数のグローバルIPアドレスレンジを設定する際は、カンマで区切ってください

7

個々のグローバルドメインを可視化・検知対象としてデータインポートする
☐

8

可視化対象のグローバルドメインのサフィックス

登録

複数のグローバルドメインを設定する際は、カンマで区切ってください

9

システム監視通知設定 ⓘ

登録

複数のメールアドレスを設定する際は、カンマで区切ってください（最大5件）
例: aaa@example.com, bbb@example.com

図. 設定変更画面（アドレス可視化・システム監視通知）

5. 個々のグローバル IP アドレスを可視化・検知対象としてデータインポートする

個々のグローバル IP アドレスを可視化・検知対象としてデータインポートする設定です。インターネット接続環境では OFF に設定することを、閉域環境では ON にすることを推奨します。インターネット接続環境で ON にすると、画面表示の遅延や停止など正常に動作しない可能性があります。

6. 可視化対象のグローバル IP アドレスレンジ

LAN 内でグローバル IP アドレスを利用する環境では、LAN 内で使用しているグローバル IP アドレスを設定してください（レンジ指定可。カンマ区切りで複数入力できます）。「登録」ボタンを押下することで、設定できます。

7. 個々のグローバルドメインを可視化・検知対象としてデータインポートする

個々のドメイン名を可視化対象としてデータインポートする設定です。インターネット接続環境では OFF に設定することを、閉域環境では ON にすることを推奨します。インターネット接続環境で ON にすると、画面表示の遅延や停止など正常に動作しない可能性があります。

8. 可視化対象のグローバルドメインのサフィックス

LAN 内で DNS を利用する環境において、LAN 内で使用しているドメイン名を設定してください（カンマ区切りで複数入力できます）。「登録」ボタンを押下することで、設定できます。

9. システム監視通知設定

システム監視に関する通知メールを送信する宛先メールアドレスを設定（カンマ区切りで最大 5 件まで複数入力できます）して「登録」ボタンを押下することで、設定できます。

10

データ削除（期間指定）
i

期間： ~

11

データ初期化
i

☐ 全ての可視化・検知データを削除する

図. 設定変更画面（データ削除・初期化）

10. データ削除（期間指定）

指定された期間の OsecT のデータを削除します。データ削除を実行後は取り消すことができません。期間を指定して「削除」ボタンを押下して削除します。

11. データ初期化

OsecT の全ての可視化・検知データを削除し、システム設定の設定変更画面にある設定値を初期状態にします。データ削除を実行後は取り消すことができません。

「全ての可視化・検知データを削除する」を選択後、「削除」ボタンを押下して削除します。

12.2. システムログ

アップロードされたデータの確認ができます。



図. システムログ画面

1. データインポート状況

アップロードされたデータの取り込み状況を表示します。

2. データインポート履歴

アップロードされたデータ個別の処理状況を表示します。

カテゴリ	説明
100	インポートされた直近 100 件の情報を表示します。
ALL	インポートされた全件の情報を表示します。

システム設定 ⓘ

[設定変更](#)[システムログ](#)[センサー管理](#)[ユーザー管理](#)[サービス名管理](#)

端末数がシステム上限の1000を大幅に超えたため、データインポートを停止しています。

データインポート状況

complete(Step8/Step8)

図. システムログ画面（データインポート停止中）

端末数がシステム上限の 1000 を大幅に超えた場合、データのインポートを停止します。その場合、システムログ画面に上記のメッセージが表示されます。また、「システム監視通知設定」で設定したメールアドレスにメールが送信されます。

設定変更画面でデータ削除（期間指定）を行い、端末数の削減を行ってください。

12.3. センサー管理

センサーの一覧を表示する画面です。センサー表示名の名称変更、センサー監視 ON/OFF の設定が可能です。

システム設定 ●

設定変更 システムログ センサー管理 ユーザー管理 サービス名管理

操作	センサー表示名	センサーID	データ使用量	センサー監視
名称変更	センサーA	A1B2C3D4	1.1GB / 0.3GB	<input checked="" type="checkbox"/>
名称変更	センサーB	E5F6G7H8	0.9GB / 0.1GB	<input type="checkbox"/>
名称変更	センサーC	I9J0K1L2	1.4GB / 0.4GB	<input checked="" type="checkbox"/>

Showing 1 to 3 of 3 rows

図. センサー管理画面

1. センサー一覧

カラム名	説明
操作	名称変更ボタンを押下するとセンサー表示名を変更できます。
センサー表示名	現在のセンサー表示名です。
センサーID	センサーを一意に識別する ID です。変更はできません。
データ使用量	センサーで利用している SIM の当月のデータ通信量です。 ○ / △の表記の場合は、○が上り使用量、△が下り使用量です。
センサー監視	ON の場合、センサー監視に関する通知メールを設定変更画面で設定されたアドレスに送信します。 OFF の場合、メールは送信されません。

システム設定 ●

設定変更 システムログ センサー管理 ユーザー管理

< 一覧ページに戻る

センサーID
A1B2C3D4

センサー表示名
センサーA 変更

図. センサー表示名変更画面

2. 一覧ページに戻る

センサー表示名変更画面から、遷移前のセンサー一覧画面に戻ることができます。

3. センサーID

センサーを一意に識別する ID です。変更はできません。

4. センサー表示名

センサー表示名の入力欄に任意の名前を入力後、変更ボタンを押下するとセンサー表示名を変更することができます。

※ センサー表示名を変更しても、キャッシュの関係ですぐにはその他の画面（5.1 端末一覧等）には反映されません。反映した結果を見たい場合は[設定変更画面](#)で「蓄積中のデータを今すぐ可視化する」を実行してください。

12.4. ユーザー管理

ユーザーの一覧を表示する画面です。ユーザーの追加・変更・削除が可能です。なお、本機能を利用するには管理者権限が必要です。

システム設定

[設定変更](#)
[システムログ](#)
[センサー管理](#)
[ユーザー管理](#)

ユーザー管理

ユーザー追加

1

2

操作	ユーザーID (メールアドレス)	氏名	管理権限	ステータス
設定変更			管理者	正常
設定変更			一般	正常
設定変更			管理者	正常

Showing 1 to 3 of 3 rows

図. ユーザー管理画面

1. ユーザー追加ボタン

新規ユーザーを追加登録できます。

2. ユーザー一覧

カラム名	説明
操作	設定変更ボタンを押下するとユーザー情報を変更できます。
ユーザーID (メールアドレス)	現在のユーザーID (メールアドレス) です。
氏名	現在のユーザーの氏名です。
管理権限	現在のユーザーの管理権限 (管理者/一般) です。
ステータス	現在のユーザーのステータスです。各状態は「9. ステータス変更」を参照してください。

システム設定 ⓘ

設定変更 システムログ センサー管理 ユーザー管理

3 < 一覧ページに戻る

4 ユーザーID (メールアドレス)
例: yamada@example.com
氏
例: 山田
名
例: 太郎
権限
一般

5 追加

図. ユーザー追加画面

3. 一覧ページに戻る

ユーザー追加画面から、遷移前のユーザー一覧画面に戻ることができます。

4. ユーザー情報入力欄

登録するユーザーのユーザーID（メールアドレス）、氏、名、権限（一般または管理者）を入力・設定します。

5. 追加ボタン

「追加」ボタンを押下することで、ユーザー情報を登録することができます。

システム設定 ①

[設定変更](#)
[システムログ](#)
[センサー管理](#)
[ユーザー管理](#)

[← 一覧ページに戻る](#)
6

ユーザーID（メールアドレス）

変更

7

氏 名

変更

8

ステータス

正常

▼

変更

9

権限

管理者

▼

変更

10

パスワードリセット

再設定用のメールを送信します

実行

11

☐ このユーザーを削除します。

削除

12

図. ユーザー情報変更画面

6. 一覧ページに戻る

ユーザー情報変更画面から、遷移前のユーザー一覧画面に戻ることができます。

7. ユーザーID（メールアドレス）変更

ユーザーのユーザーID（メールアドレス）を変更し、「変更」ボタンを押下することで、ユーザーID（メールアドレス）を変更することができます。

8. 氏名変更

ユーザーの氏、名を変更し、「変更」ボタンを押下することで、氏名を変更することができます。

9. ステータス変更

ユーザーのステータス変更し、「変更」ボタンを押下することで、ステータスを変更することができます。

ステータスは以下の 4 つから選択します。

- ① 正常
- ② ロック（一定期間利用なし）
- ③ ロック（手動）
- ④ ロック（パスワード誤り回数オーバー）

10. 権限変更

ユーザーの権限を変更し、「変更」ボタンを押下することで、権限を変更することができます。

権限は以下の 2 つから選択します。

- ① 一般
- ② 管理者

11. パスワードリセット

「実行」ボタンを押下することで、パスワード再設定用のメールをユーザーに送信することができます。

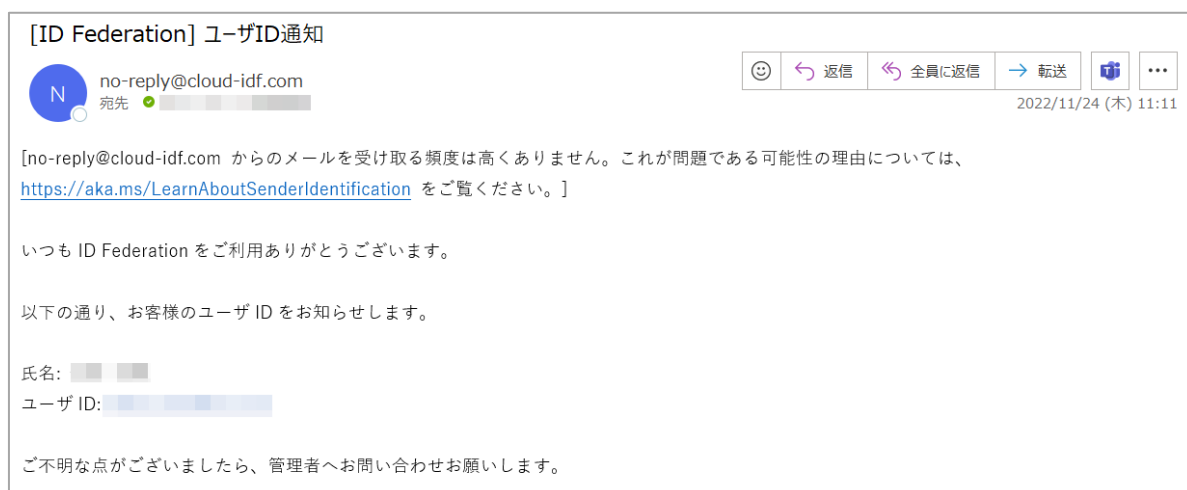
12. ユーザー削除

チェックボックスにチェックを入れると、「削除」ボタンが有効になります。「削除」ボタンを押下することで、ユーザーを削除することができます。

【アカウントを追加した場合】

ユーザーには以下の件名のメールが届きます。

- ① [ID Federation] ユーザ ID 通知



② [ID Federation] パスワード初期設定のご案内



- ②のメールに記載されたパスワード初期設定用の URL にアクセスします。
- ①のメールに記載されたユーザーID と新しいパスワードを入力して、「パスワード設定」ボタンを押下します。

ID Federation

パスワードを設定します。

ユーザーID

@ntt.com

新しいパスワード

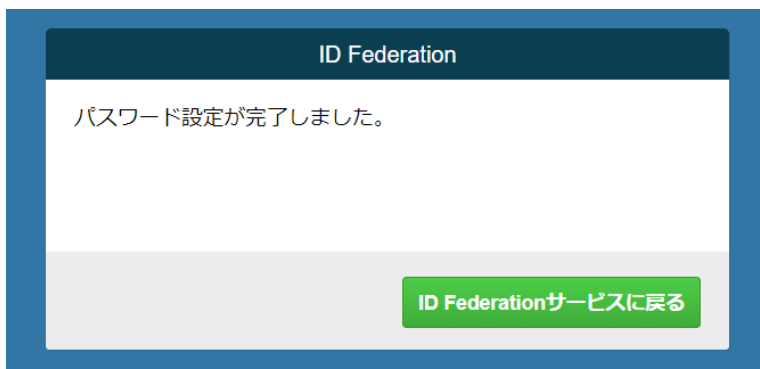
.....

新しいパスワード（確認）

.....

パスワード設定

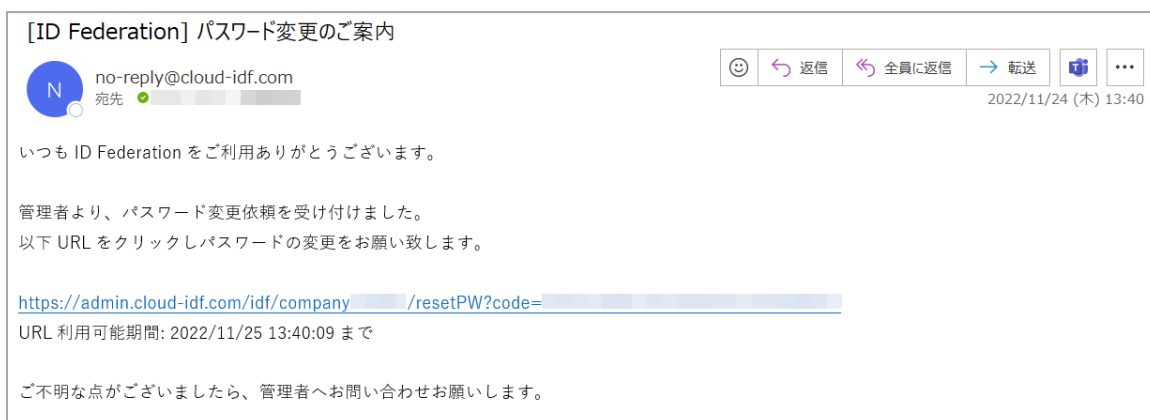
3. パスワードの設定が完了し、OsecT にログインが可能となります。



【管理者がパスワードをリセットした場合】

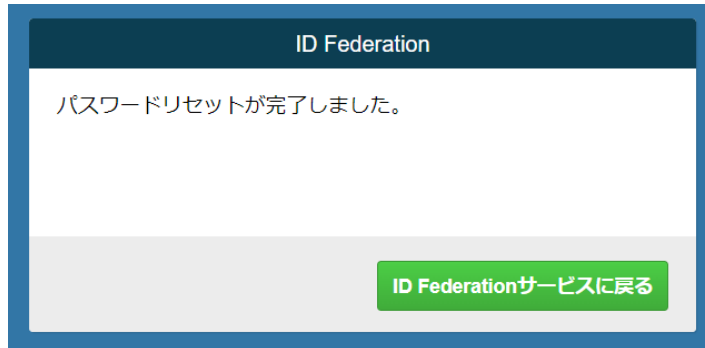
ユーザーには以下の件名のメールが届きます。

① [ID Federation] パスワード変更のご案内



- ①のメールに記載されたパスワード変更用の URL にアクセスします。
- ユーザーID とパスワードを入力して、「パスワードリセット」ボタンを押下します。

3. パスワードリセットが完了しました。



12.5. サービス名管理

TCP、UDP のサービス名の一覧を表示する画面です。

TCP、UDP のポート番号に任意のサービス名を設定することが可能です。

システム設定 ●

設定変更 システムログ センサー管理 ユーザー管理 サービス名管理

1 絞り込み

2 ポート番号 絞り込みなし

3 ポート番号 (範囲検索) 1 ~ 3

4 サービス名 (部分一致検索) 例) http

5 リセット 6 適用

操作	ポート番号	TCP	UDP
名称変更	1	tcpmux	tcpmux
名称変更	2	compressnet	compressnet
名称変更	3	compressnet	compressnet

図. サービス名管理画面

1. 絞り込み

表示するサービス名を絞り込むことができます。

2. ポート番号

プルダウンで選択したポート番号の範囲で絞り込みを設定できます。

3. ポート番号 (範囲検索)

任意の範囲のポート番号で絞り込みを設定できます。

4. サービス名 (部分一致検索)

ポート番号についているサービス名で絞り込みを設定できます。

サービス名の一部だけを指定することもできます。

5. リセットボタン

ポート番号、ポート番号 (範囲検索)、サービス名 (部分一致検索) で指定した選択をリセットできます。

6. 適用ボタン

ポート番号、ポート番号（範囲検索）、サービス名（部分一致検索）で指定した選択を適用した画面を表示できます。

7. サービス名一覧

コラム名	説明
操作	名称変更ボタンを押下するとサービス名を変更できます。
ポート番号	ポート番号です。
TCP	TCP プロトコル用のサービス名です
UDP	UDP プロトコル用のサービス名です。



システム設定 ⓘ

設定変更 システムログ センサー管理 ユーザー管理 **サービス名管理**

8 < 一覧ページに戻る

9 ポート番号 2

10 TCP compressnet
UDP compressnet

11 変更

図. サービス名変更画面

8. 一覧ページに戻る

サービス名変更画面から、遷移前のサービス名一覧画面に戻ることができます。

9. ポート番号

ポート番号を表示します。（変更はできません。）

10. サービス名入力欄

TCP 用、UDP 用のサービスを入力・設定します。

11. 変更ボタン

「変更」ボタンを押下することで、サービス名を変更することができます。

改訂履歴

バージョン	主な変更	日付
1.00	新規作成	2022 年 4 月 25 日
1.10	1. ログイン方法の詳細を追加。 2.8 サービス名の表記について 追加。 5.1 一覧にセンサー表示名に関する注意書きを追加。 12.3 センサー管理 を追加。 0 ユーザー管理 を追加。	2022 年 12 月 1 日
2.00	Web ポータル画面変更に伴う各種図の変更 可視化機能に OT プロトコルを追加 検知機能に IP 統計・OT 振舞（IP, イーサネット）を追加 学習・検知設定の簡素化 システム設定にインターネットアドレス可視化・データ削除（期間指定）・センサー監視を追加	2023 年 6 月 23 日
2.50	Web ポータル画面変更に伴う各種図の変更 「5.1. 一覧」端末一覧に追加された表示列指定ボタンの説明を追加 「5.3. 詳細」端末詳細における接続端末と接続サービスの一体化に合わせて説明を修正 「6.1. 端末」ネットワークマップのフィルター機能拡充に合わせて説明を追加 「11.10. シグネチャー」シグネチャー検知の検知除外リストへの追加方法の変更に合わせて説明を修正 「11.11. 全般」学習・検知設定に追加された通知設定詳細の説明を追加 「11.11. 全般」学習・検知中止と学習・検知初期化の一体化に合わせて説明を修正 「11.12. 全般（アドバンスモード）」学習・検知設定に追加された通知設定詳細の説明を追加	2023 年 10 月 10 日
2.90	シグネチャー日本語化に伴う各種図の変更 各脅威検知機能の学習結果一覧に検索機能を追加したことに伴う変更 インデント調整、列幅調整、誤表記修正（文字足らず、フォント調整、改行足らず）（全体） 目次ページの更新および各章番号の修正（全体）	2024 年 3 月 28 日

	<p>〇〇セレクトボックスと記載あるものは、セレクトボックスと いう文言を統一して削除（全体）</p> <p>図の差し替え</p> <p>6.1. 端末（◎：オススメ機能）</p> <p>11.8. OT 振舞（IP）</p> <p>15. CSV ボタンと 16. グラフの番号が逆になっていたので、 文章入れ替え修正</p> <p>11.6. IP 流量</p>	
--	---	--