# WideAngle

# OsecT（オーセクト）ユーザーガイド

バージョン 4.40

NTT ドコモビジネス株式会社

2026 年 9 月 30 日

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

目次


**1. はじめに ..... 5**

**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. 台帳 ..... 8

2.7. 物理構成 ..... 8

2.8. 脆弱性 ..... 8

2.9. 検知アラート ..... 8

2.10. 学習・検知設定 ..... 8

2.11. アセスメント ..... 9

2.12. 補足：サービス名の表記について ..... 9

2.13. 補足：制限事項 ..... 10

**3. 画面左メニュー ..... 11**

**4. タブ ..... 12**

**5. 期間設定 ..... 13**

**6. ダッシュボード ..... 14**

**7. 端末 ..... 16**

7.1. 一覧（◎：オススメ機能） ..... 16

7.2. 一覧（IP） ..... 19

7.3. 詳細 ..... 21

7.4. ベンダーマトリクス（◎：オススメ機能） ..... 24

7.5. OS マトリクス ..... 26

7.6. 役割マトリクス ..... 28

**8. ネットワークマップ ..... 30**

8.1. 端末（◎：オススメ機能） ..... 30

8.2. サービス ..... 37

**9. トラフィック ..... 41**

**10. ランキング ..... 43**

10.1. 端末トラフィック量 ..... 43

10.2. 端末接続数 ..... 45

10.3. 端末重要度 ..... 47

10.4. サービストラフィック量 ..... 50




© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

10.5. サービス別端末数 ..... 52
10.6. ベンダー別端末数 ..... 54
**11. OT プロトコル ..... 55**
11.1. 一覧（IP） ..... 55
11.2. 一覧（イーサネット） ..... 57
**12. 台帳 ..... 60**
12.1. 一覧 ..... 60
12.2. 詳細 ..... 66
12.3. 補足：可視化や検知機能との連携に関して ..... 67
**13. 物理構成 ..... 68**
**14. 脆弱性 ..... 71**
**15. 検知アラート ..... 75**
15.1. 全て ..... 75
15.2. 接続端末（◎：オススメ機能） ..... 77
15.3. 脆弱端末（◎：オススメ機能） ..... 79
15.4. IP 通信 ..... 81
15.5. IP 流量 ..... 83
15.6. IP 統計 ..... 87
15.7. OT 振舞（IP） ..... 89
15.8. OT 振舞（イーサネット） ..... 91
15.9. シグネチャー ..... 93
15.10. ビルトイン ..... 96
**16. 学習・検知設定 ..... 98**
16.1. 学習・検知ステータス ..... 98
16.2. 学習・検知ステータス（アドバンスモード） ..... 100
16.3. 接続端末 ..... 102
16.4. 脆弱端末 ..... 105
16.5. IP 通信 ..... 108
16.6. IP 流量 ..... 112
16.7. IP 統計 ..... 116
16.8. OT 振舞（IP） ..... 119
16.9. OT 振舞（イーサネット） ..... 123
16.10. シグネチャー ..... 127
16.11. ビルトイン ..... 132
16.12. 全般 ..... 134
16.13. 全般（アドバンスモード） ..... 138



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

16.14. 連携 ..... 144
16.14.1. AMF-SEC ..... 144
16.14.2. 信号灯 ..... 145
16.14.3. SIEM ..... 148
**17. アセスメント ..... 150**
**18. システム設定 ..... 152**
18.1. 設定変更 ..... 152
18.2. システムログ ..... 157
18.3. センサー/ポート管理 ..... 159
18.4. ユーザー管理 ..... 161
18.5. サービス名管理 ..... 166
18.5.1. L4 プロトコル ..... 166
18.5.2. L2 プロトコル ..... 168



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 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。 推奨ブラウザーは Google Chrome です。

ログイン手順は以下のとおりです。

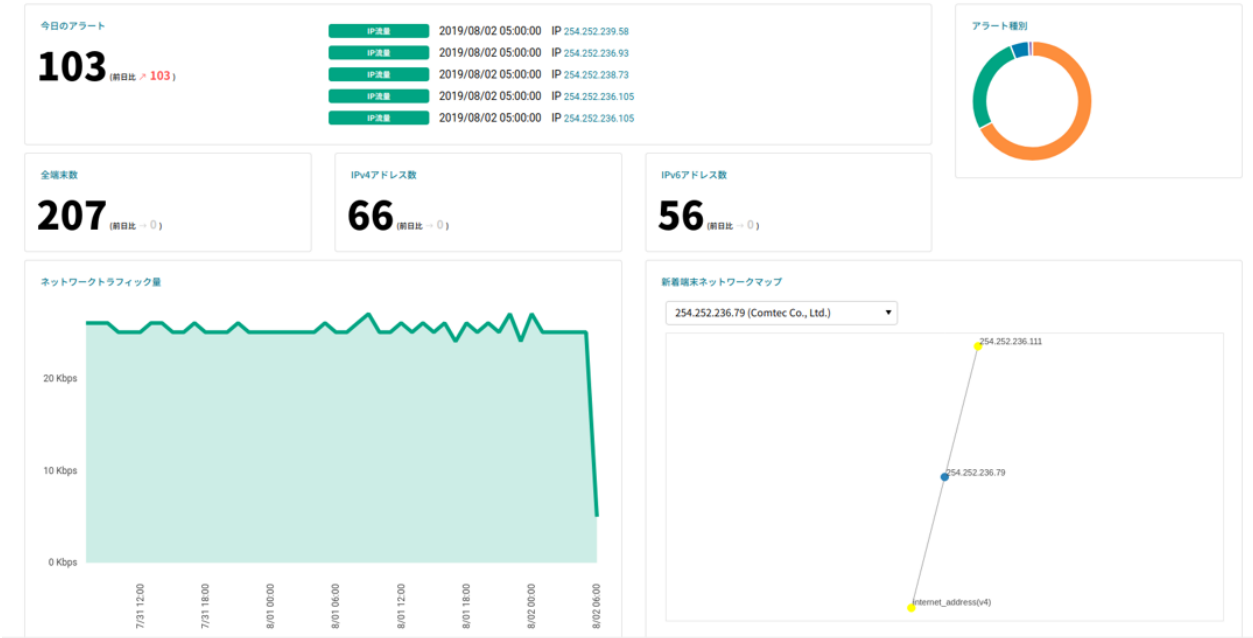
1. ブラウザーから開通案内に記載された URL へアクセスします。

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。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. 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、「認証」を押下してください。

4. OsecT のダッシュボード画面が表示されます。






© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 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・脆弱性の検知ができます。

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 2.6. 台帳

台帳の登録や確認、編集、削除、ダウンロードができます。登録した台帳は、接続端末の検知や可視化機能と連携できます。

## 2.7. 物理構成

OsecT ポーラーの出力ファイルをインポートすることで、機器間の物理接続マップおよび機器詳細情報を確認できます。

## 2.8. 脆弱性

パッシブ監視で収集した通信情報や OsecT スキャナーの出力ファイルをインポートすることで、機器の脆弱性情報を確認できます。

## 2.9. 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。

- 接続端末
- 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
- ビルトイン

## 2.10. 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。

- 接続端末



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

- 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
- ビルトイン

## 2.11. アセスメント

アセスメントレポートを pptx 形式でダウンロードできます。また、分析結果の全件 CSV データとアセスメントレポートの一括ダウンロードも可能です。

## 2.12. 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）



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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）

## 2.13. 補足：制限事項

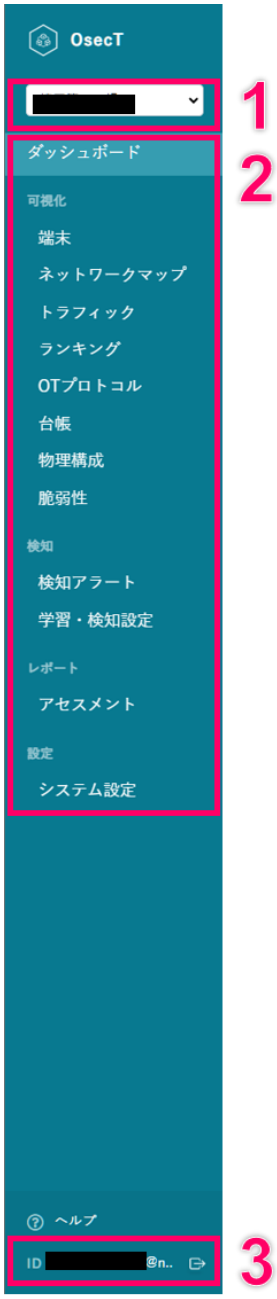
ループバックアドレスに対する通信ログは分析対象外となります。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 3. 画面左メニュー

全ての画面で左側にメニューが表示されます。 下図 1 のプルダウンにより、表示するセンサー/ポートを選択できます。 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ているユーザーID（下図 3）が表示されます。






© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 4. タブ

左メニューを押下すると、一部の画面で、画面上部にタブが表示されます。画面名に対応する各タブ（下図１）を押下すると、該当する画面が表示されます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 5. 期間設定

可視化画面の右上に期間設定メニューが表示されます。期間（下図１）を指定して適用（下図２）を押下すると、指定した期間のデータで可視化することができます。また、デフォルトの可視化期間よりも前のデータを可視化したい場合にも、本機能をご利用ください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 6. 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。

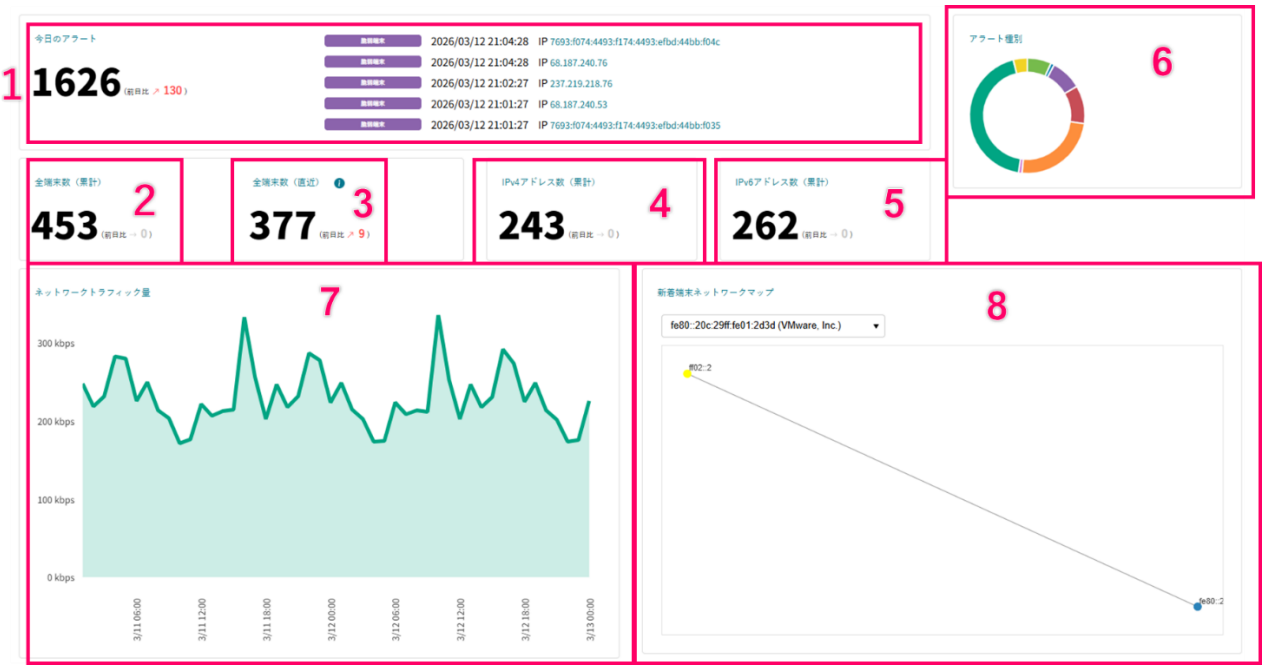



図. ダッシュボード画面

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。今日のアラートを押下すると検知アラート画面が表示されます。

2. 全端末数（累計）

   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。全端末数を押下すると端末一覧画面が表示されます。

3. 全端末数（直近）

   直近 2 時間の通信有無に基づき算出しています。接続端末検知（消滅端末検知オプション含む）が OFF の場合は表示されません。

4. IPv4 アドレス数（累計）



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。IPv4 アドレス数を押下すると端末一覧（IP）画面が表示されます。

5. IPv6 アドレス数（累計）

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。IPv6 アドレス数を押下すると端末一覧（IP）画面が表示されます。

6. 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：接続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。アラート種別を押下すると検知アラート画面が表示されます。

7. 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。ネットワークトラフィック量を押下するとトラフィック画面が表示されます。

8. 新着端末ネットワークマップ

接続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。 接続端末の 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。新着端末ネットワークマップを押下するとネットワークマップ画面が表示されます。

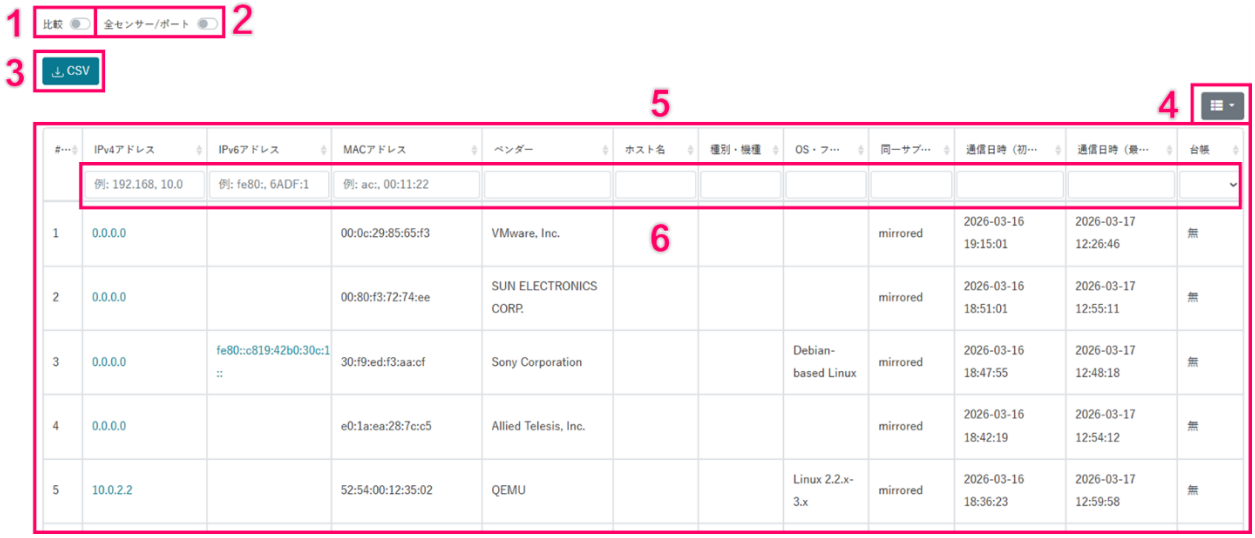


© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 7. 端末

## 7.1. 一覧（◎：オススメ機能）

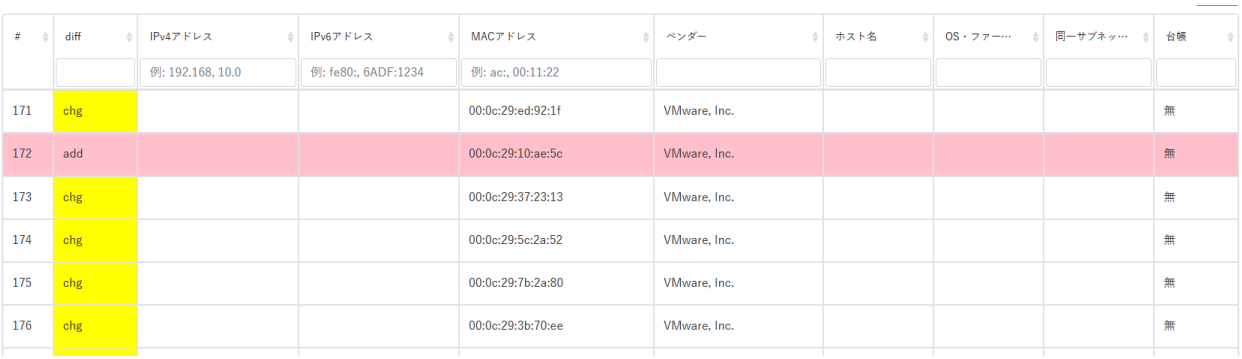
端末情報を一覧表示する画面です。 お手持ちの台帳と突合させることで、管理されていない端末がないか確認できます。台帳の自動生成ツールとして利用することもできます。




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。




図．一覧画面（差分モード）



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| 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/ポート

複数のセンサー/ポートを利用している場合にすべてのセンサー/ポート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。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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「Unregistered」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。L2 プロトコルの場合は辞書をベースに L2 プロトコル名を表示。辞書に存在しない場合は EtherType 等の値を表示。 |
| 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。L2 プロトコルの場合は辞書をベースに L2 プロトコル名を表示。辞書に存在しない場合は EtherType 等の値を表示。 |
| 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/ポート | 端末が検出されたセンサー/ポートを表示。 |
| 台帳 | 端末が台帳に存在する場合は台帳へのリンク付きで「有」、存在しない場合は「無」を表示。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

※ 18.3 センサー/ポート管理画面でセンサー/ポート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 14.11 設定変更の「1. 蓄積積中のデータを今すぐ可視化する」を実行してください。

※ 端末と台帳の紐づけに関しては、「12.3 補足：可視化や検知機能との連携に関して」をご確認ください。

6. 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。

## 7.2. 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。

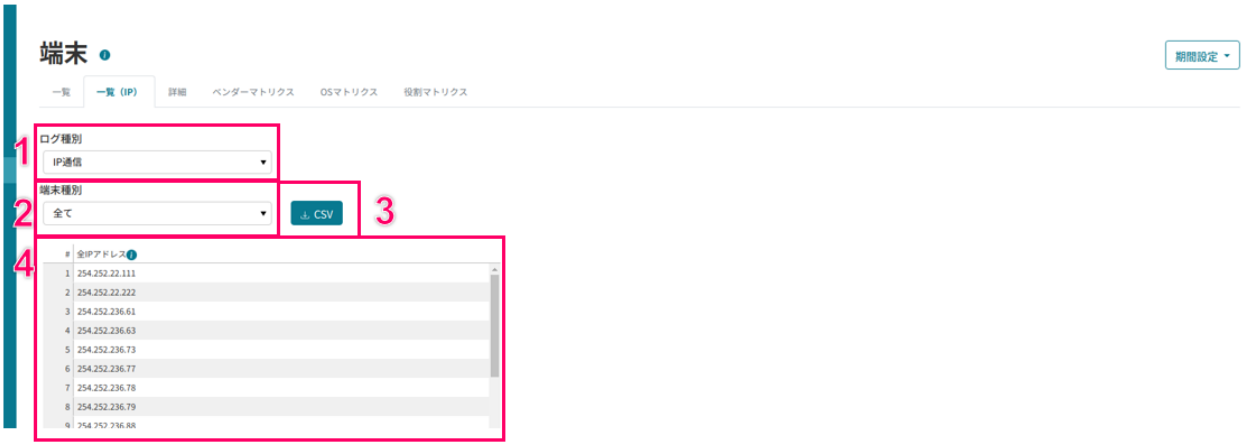



図. 一覧（IP）画面

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

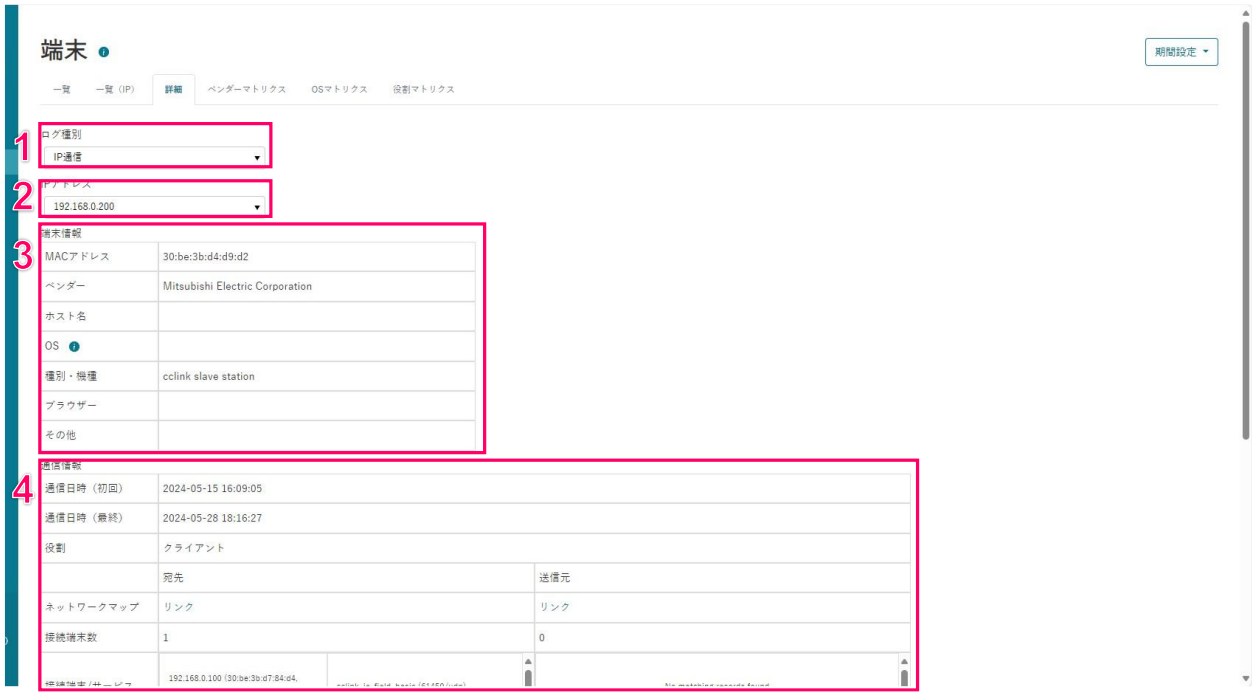
   グローバルアドレスと判定されたものは最後に（global）が付加されます。 表示順はプライベート IPv4、プライベート IPv6、グローバル IPv4、グローバル IPv6 のドメイン名の順となります。



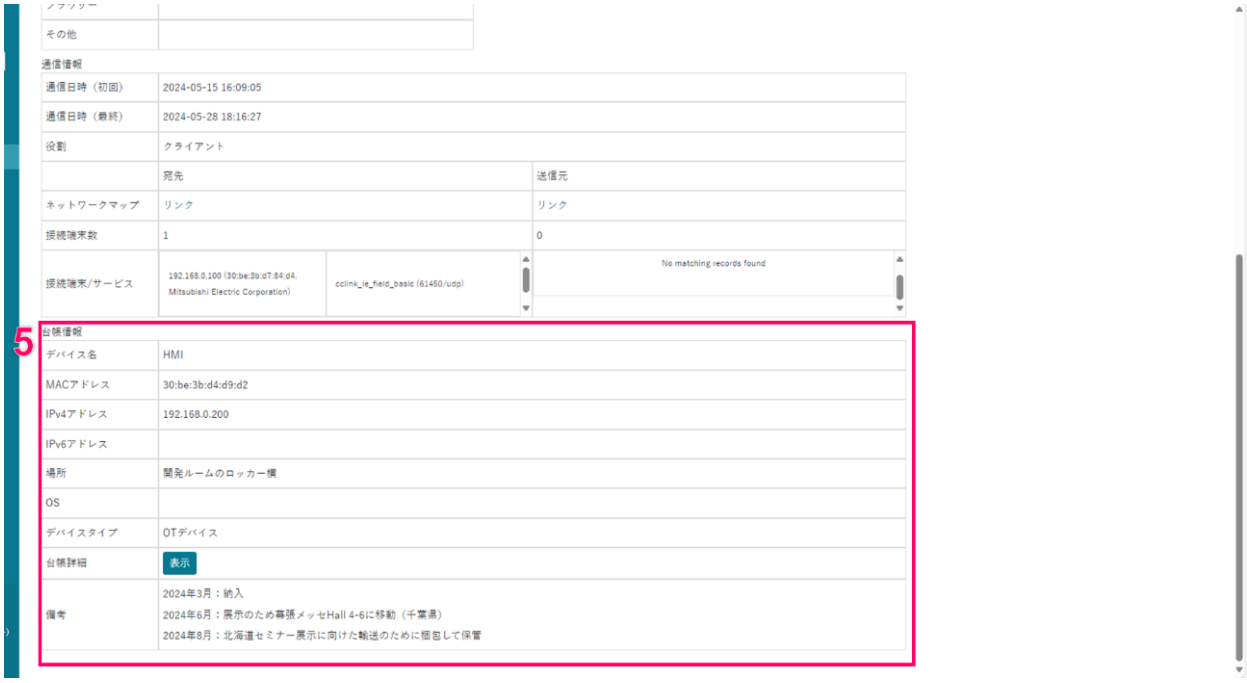
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 7.3. 詳細

選択した端末の情報を表示する画面です。




図．詳細画面（上部）




図．詳細画面（下部）



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 |
| ブラウザー | IP アドレスに紐づくブラウザー |
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| 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. 台帳情報

IP アドレスで選択した端末に紐づく台帳情報を表示します。「台帳詳細」行の「表示」ボタンをクリックすることでより詳細な台帳情報を確認できます。表示される台帳のカラムは「デバイス名」、「MAC アドレス」、「IPv4 アドレス」、「IPv6 アドレス」、「場所」、「OS」、「デバイスタイプ」、「台帳詳細」と「備考」です。各カラムの内容は、本ユーザーガイドの 12.1 一覧の項目をご確認ください。

台帳情報の登録がない IP アドレスの場合、本情報は表示されません。

なお、端末と台帳の紐づけに関しては、「12.3 補足：可視化や検知機能との連携に関して」をご確認ください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 7.4. 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。

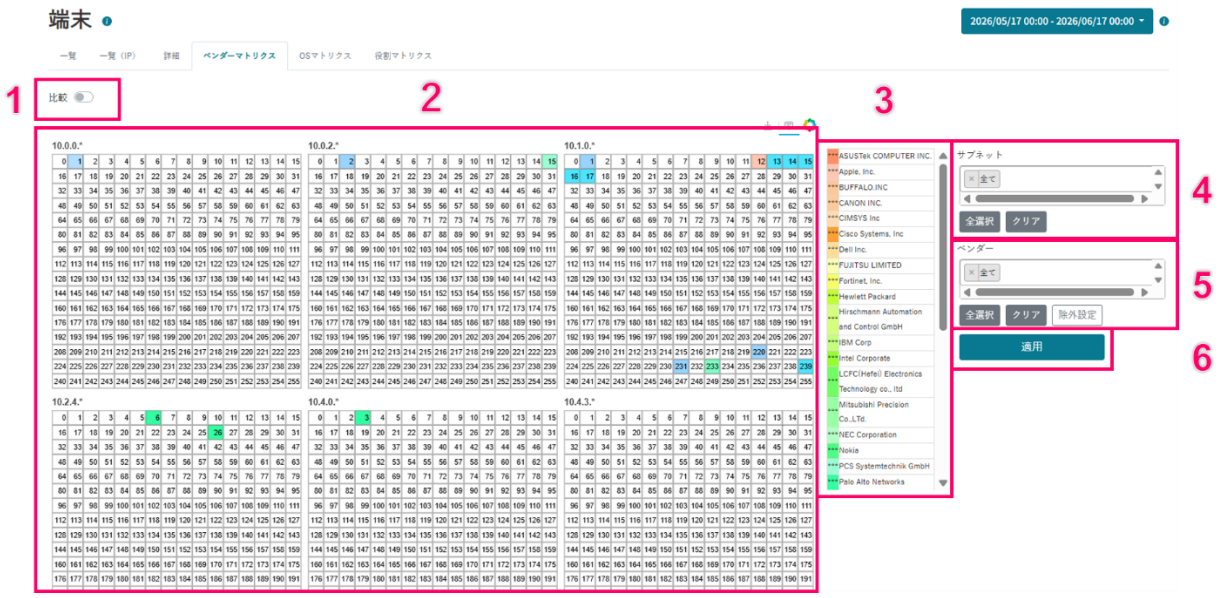



図. ベンダーマトリクス画面

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. 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。

3. 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。

4. サブネット選択リスト



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

表示したいサブネットを選択できます。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。

5. ベンダー選択リスト

   表示したいベンダーを選択できます。全選択ボタンを押下することで、表示可能なベンダー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。また、除外設定をすることで、設定したベンダーを非表示にできます。

6. 適用ボタン

   選択した条件のマトリクスを表示します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 7.5. 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。

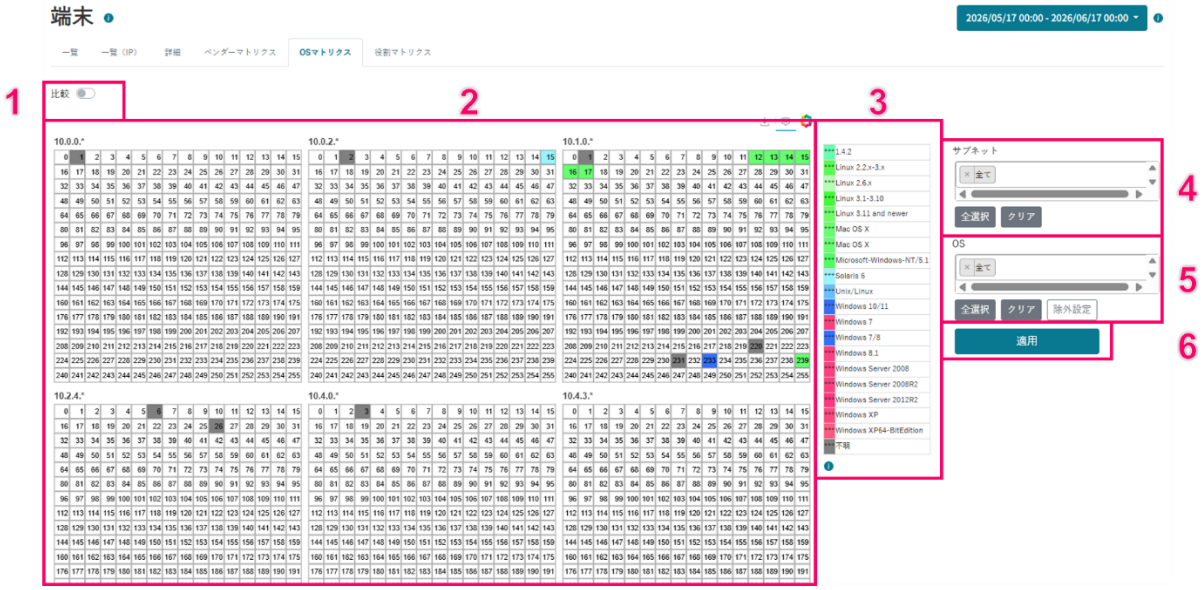



図. OS マトリクス画面

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. 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。

3. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。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. OS 選択リスト

   表示したい OS を選択できます。全選択ボタンを押下することで、表示可能な OS 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 OS を選択から外すことができます。また、除外設定をすることで、設定した OS を非表示にできます。

6. 適用ボタン

   選択した条件のマトリクスを表示します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 7.6. 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。

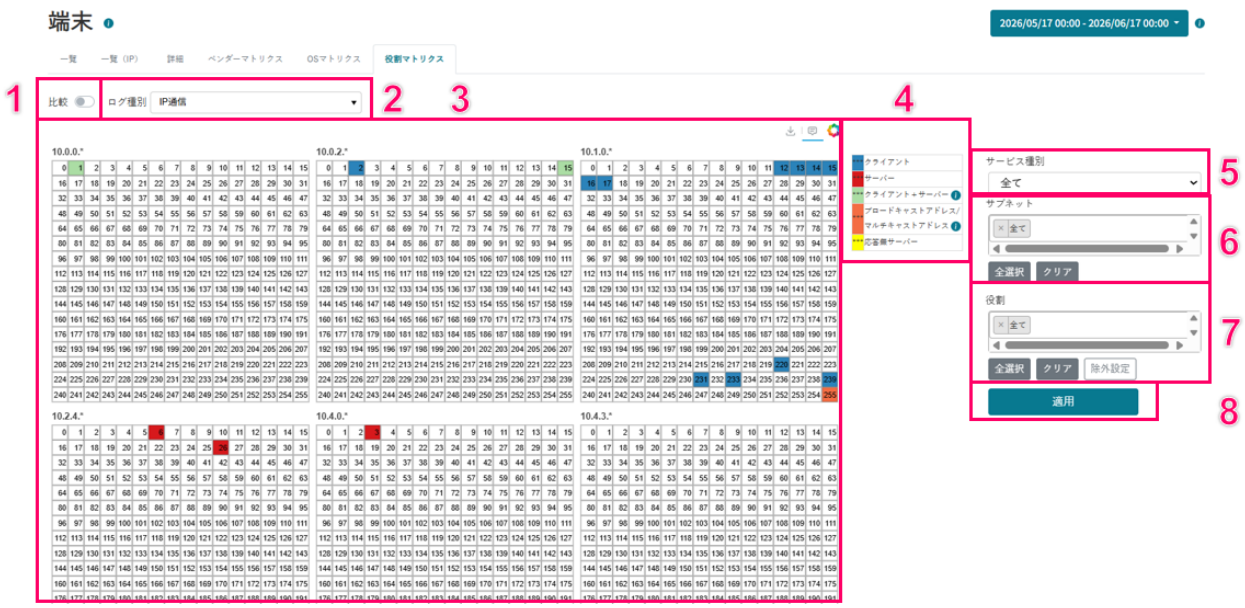



図. 役割マトリクス画面

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. マトリクス



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

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 |

5. 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。

6. 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。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。

7. 役割選択リスト

表示したいサブネットを選択できます。全選択ボタンを押下することで、表示可能な役割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役割を選択から外すことができます。また、除外設定をすることで、設定した役割を非表示にすることができます。

8. 適用ボタン

選択した条件のマトリックスを表示します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 8. ネットワークマップ

## 8.1. 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。

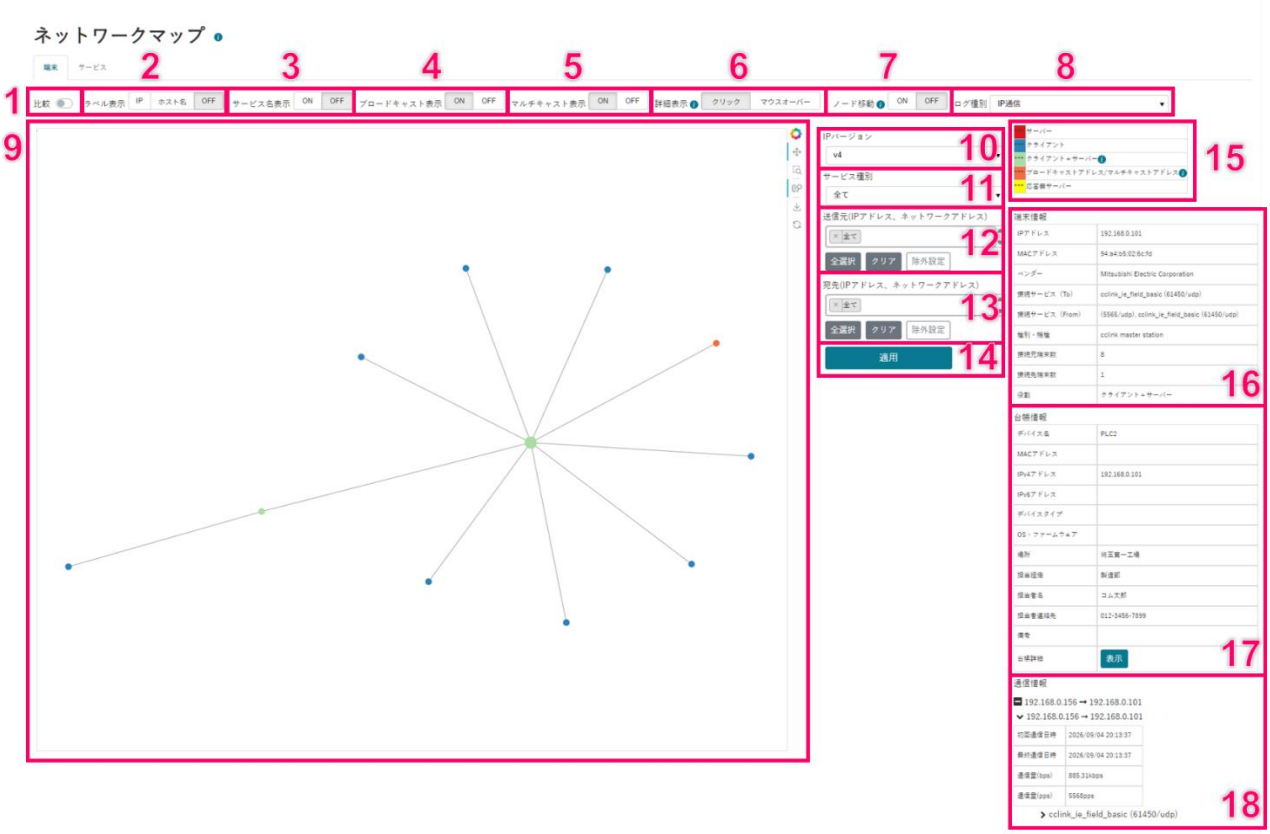



図. 端末画面

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

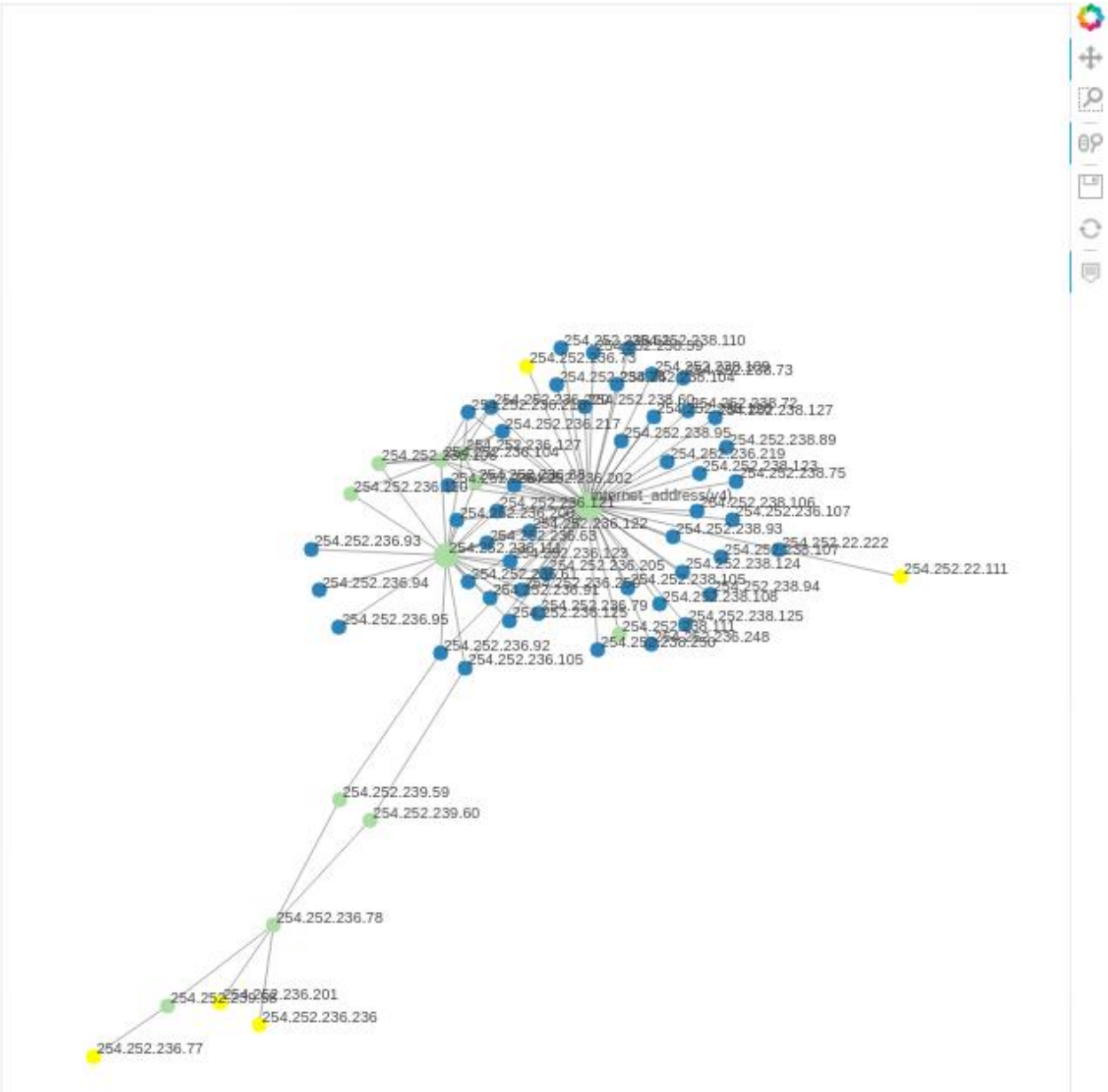
| 外枠の色 | 説明 |
|---|---|
| 緑 | 比較に指定した範囲には存在せず、期間に指定した範囲には存在するノード |
| 青 | 比較に指定した範囲には存在し、期間に指定した範囲には存在しないノード。存在しなくなったノードは白塗になります。 |
| なし | 変化なし |

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、ホスト名）を表示するラベルを選択できます。 ON にした場合、以下のようなマップが表示されます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.




図．ラベル表示 ON 時のマップ



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. サービス名表示選択ボタン

マップ上のリンクにサービス名とトラフィック量を表示する（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。

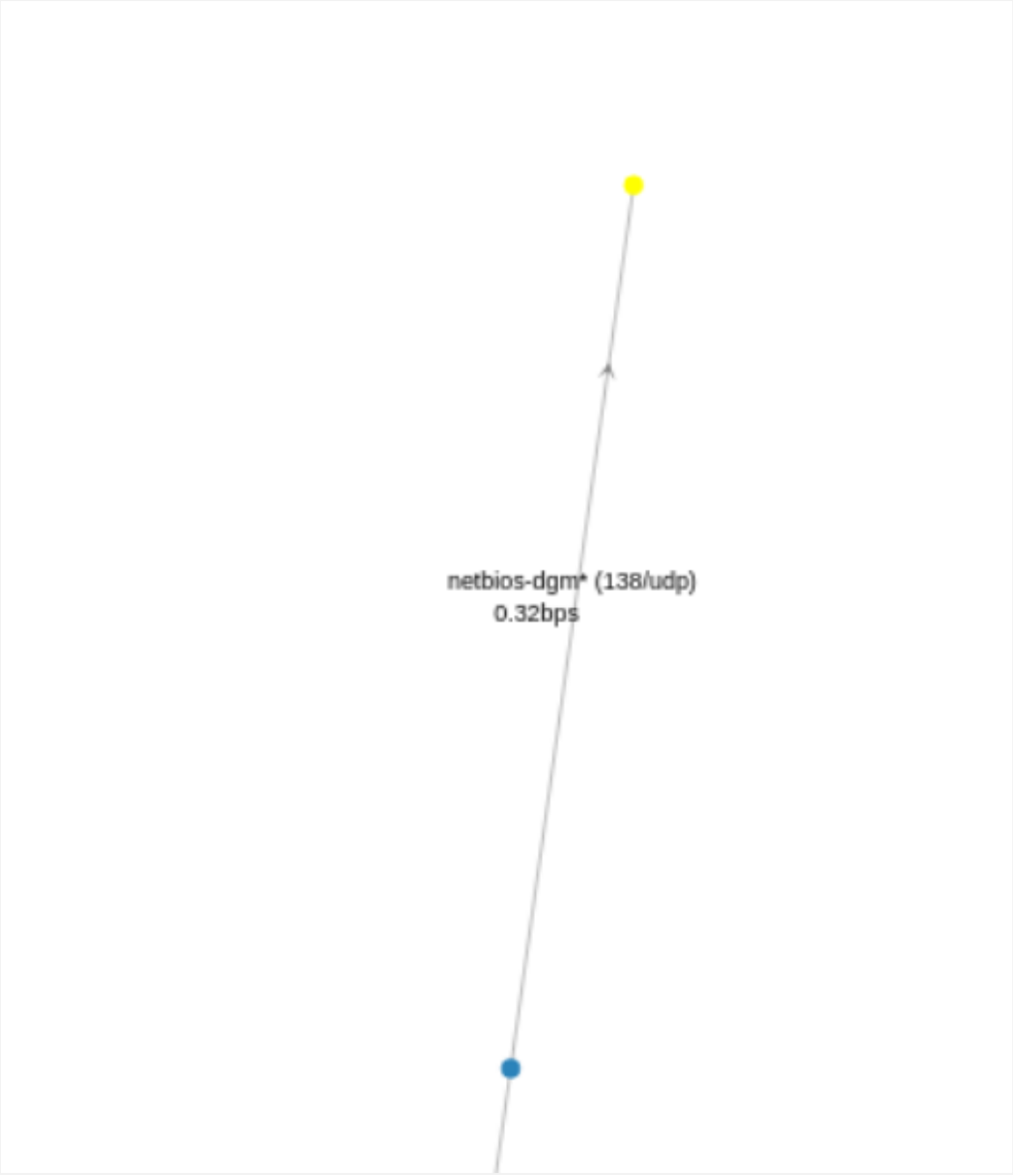



図. サービス名表示 ON 時のマップ

4. ブロードキャスト表示選択ボタン

マップ上に、ブロードキャストアドレスのノードを表示する（ON）/表示しない（OFF）を選択できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. マルチキャスト表示選択ボタン

マップ上に、マルチキャストアドレスのノードを表示する（ON）/表示しない（OFF）を選択できます。

6. 詳細表示

詳細情報(１３、１４、１５の情報)の表示する操作を切り替えます。クリックの場合はクリック、マウスオーバーの場合はマウスオーバーで詳細情報が表示されます。

7. ノード移動

ON にするとマップのノードを移動できます。移動する場合は対象のノードをクリックした後に任意の場所にドラッグアンドドロップしてください。

8. 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 |

9. 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。

10. 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。

11. 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。

12. 送信元 IP アドレス



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

13. 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。

14. 適用ボタン

選択した条件のマップを表示します。

15. 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。バージョン 4.2 以前はフィルタ適用後に表示されるノードを対象に役割を再計算していましたが、バージョン 4.3 以降はフィルタ適用後もネットワーク全体で計算した役割を維持するようになりました。

| **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 |

16. 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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

（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）。

17. 台帳情報

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。マウスオーバーしたノードに紐づく台帳情報を表示します。「台帳詳細」行の「表示」ボタンをクリックすることでより詳細な台帳情報を確認することが出来ます。表示されるカラムは「デバイス名」、「MAC アドレス」、「IPv4 アドレス」、「IPv6 アドレス」、「場所」、「OS」、「デバイスタイプ」、「台帳詳細」と「備考」です。各カラムの内容は、本ユーザーガイドの 12.1 一覧の項目をご確認ください。

なお、端末と台帳の紐づけに関しては、「12.3 補足：可視化や検知機能との連携に関して」をご確認ください。

18. 通信情報

マップ上でリンクにマウスオーバーすると表示されます。リンクの両端のノード間の通信における初回通信日時、最終通信日時、通信バイト数(bps)、通信パケット数(pps)を表形式で表示します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 8.2. 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。

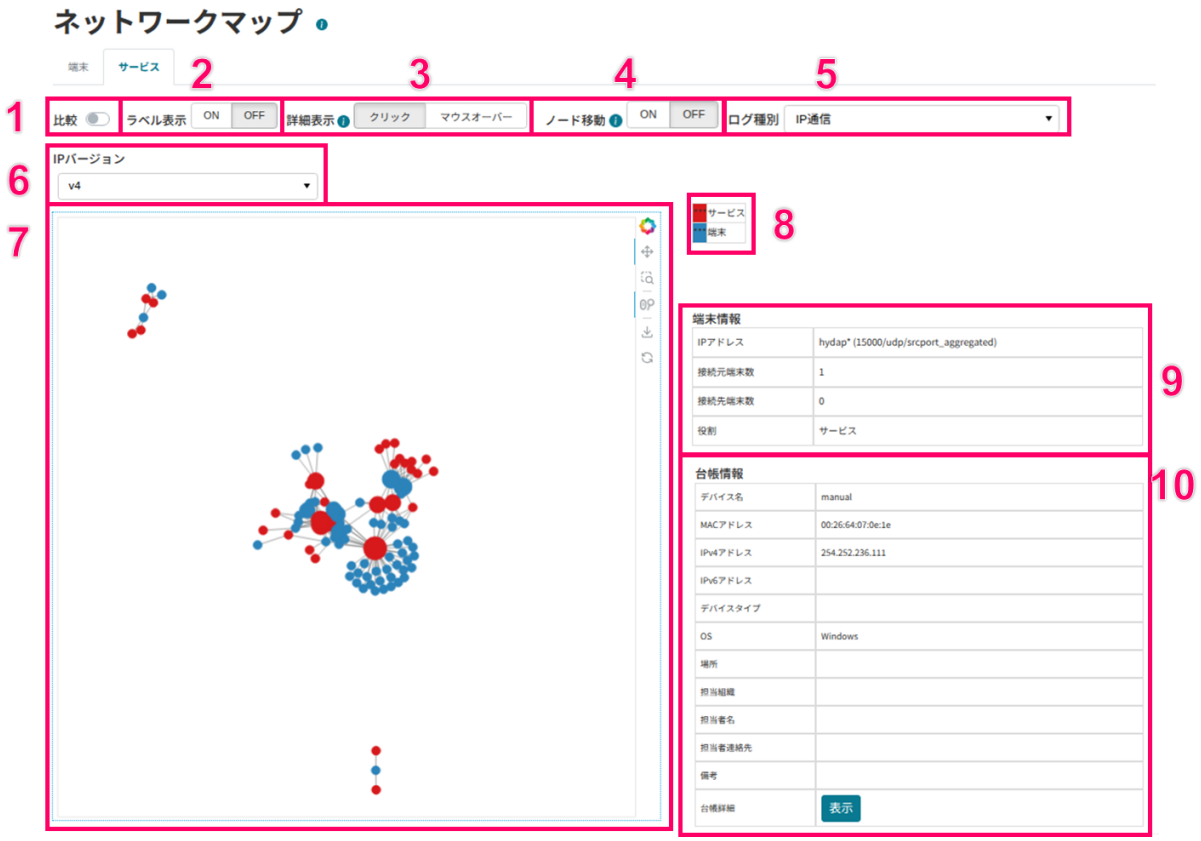



図. サービス画面

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。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。

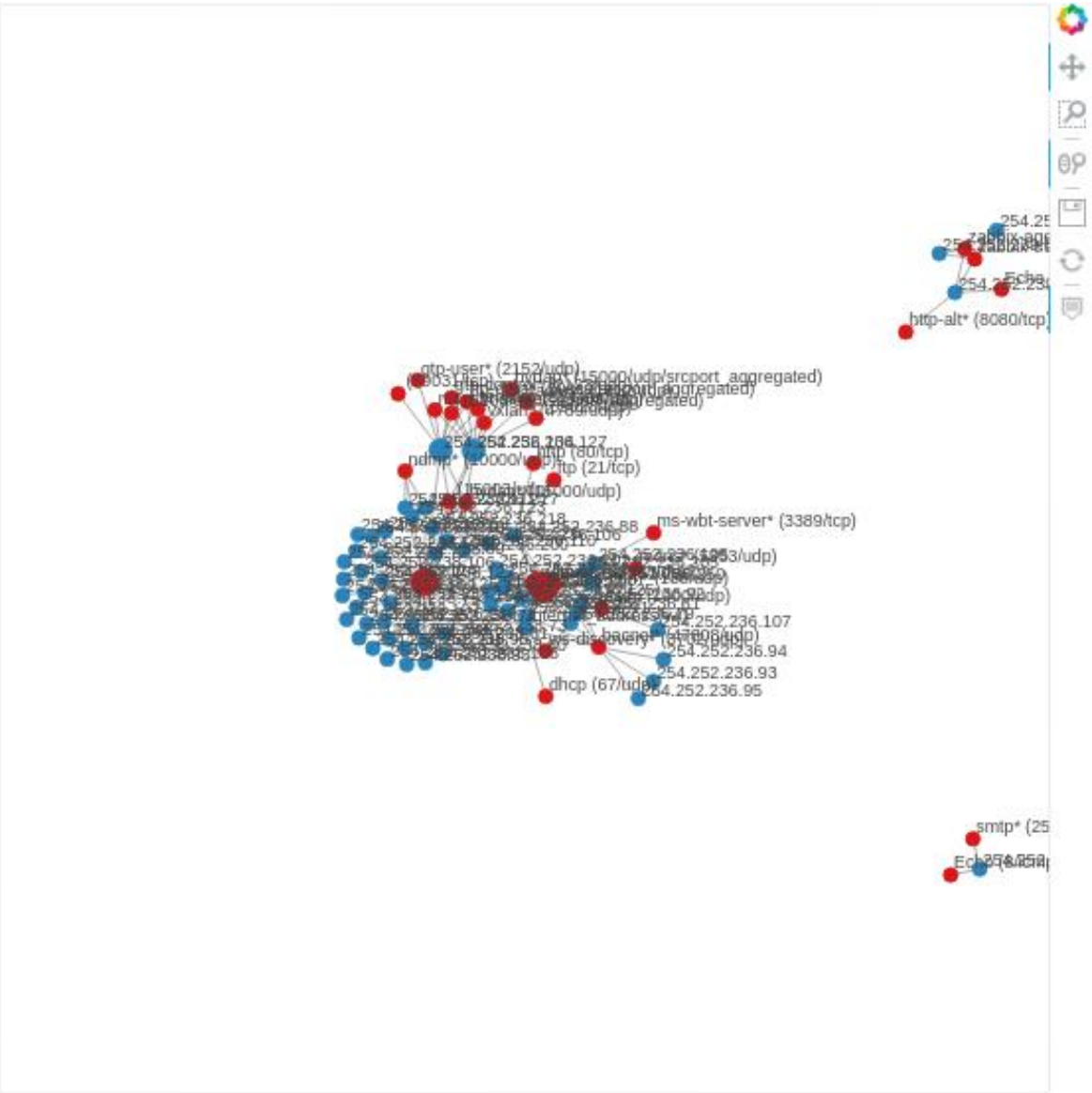



図. ラベル表示 ON 時のマップ

3. 詳細表示



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

詳細情報(9 の情報)の表示する操作を切り替えます。クリックの場合はクリック、マウスオーバーの場合はマウスオーバーで詳細情報が表示されます。

4. ノード移動

ON にするとマップのノードを移動できます。移動する場合は対象のノードをクリックした後に任意の場所にドラッグアンドドロップしてください。

5. 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 |

6. 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。

7. 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。

8. 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 |

9. 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、ブラウザー、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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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. 台帳情報

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。マウスオーバーしたノードに紐づく台帳情報を表示します。「台帳詳細」行の「表示」ボタンをクリックすることでより詳細な台帳情報を確認することが出来ます。表示されるカラムは「デバイス名」、「MAC アドレス」、「IPv4 アドレス」、「IPv6 アドレス」、「場所」、「OS」、「デバイスタイプ」、「台帳詳細」と「備考」です。各カラムの内容は、本ユーザーガイドの 12.1 一覧の項目をご確認ください。

なお、端末と台帳の紐づけに関しては、「12.3 補足：可視化や検知機能との連携に関して」をご確認ください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 9. 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. CSV ダウンロードボタン

   ボタンを押下すると、画面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。フィルタを適用した場合は、ダウンロードされる情報もフィルタ適用時のものとなります。

2. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. 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。

4. 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。

5. 送信元(IP アドレス、ネットワークアドレス)

   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。ネットワークアドレスを指定することも可能です。

6. 宛先(IP アドレス、ネットワークアドレス)

   選択した宛先 IP アドレスの情報をグラフに表示します。ネットワークアドレスを指定することも可能です。

7. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 10.　ランキング

## 10.1.　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。

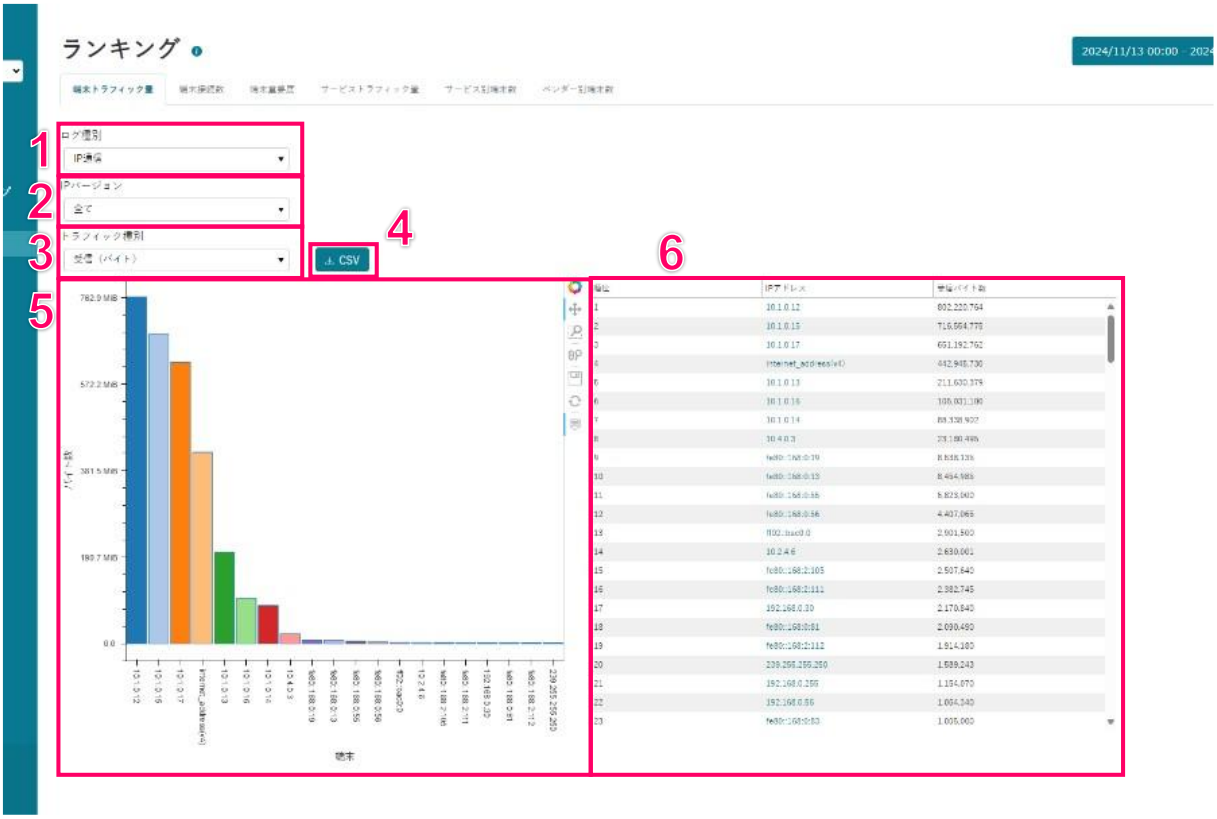



図. 端末トラフィック量画面

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



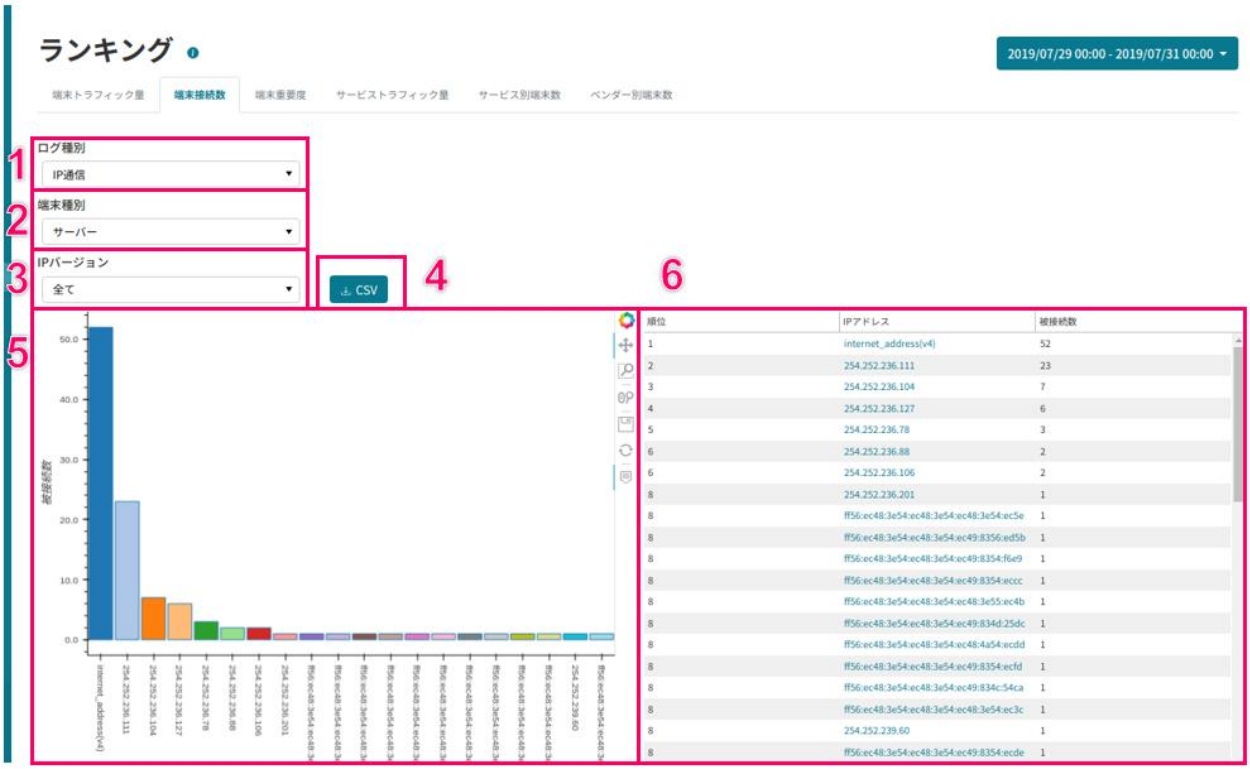
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

## 10.2.　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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 10.3. 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。

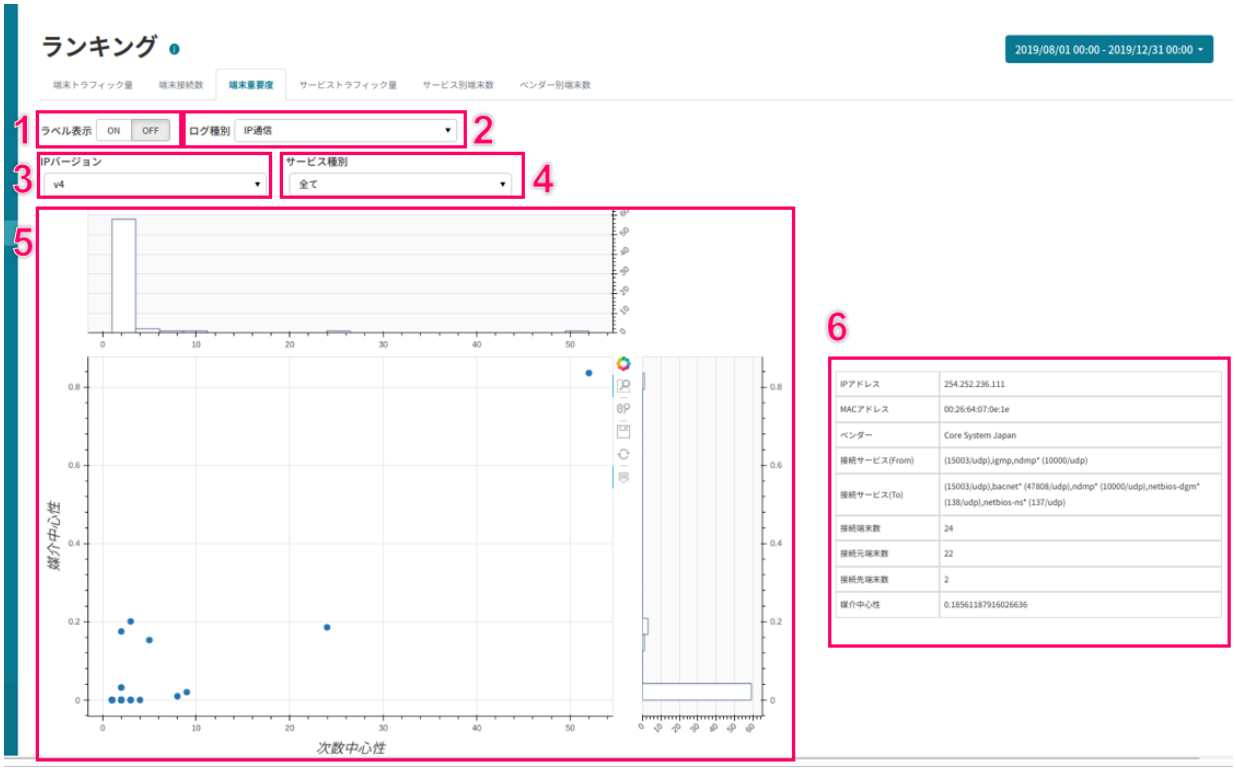



図. 端末重要度画面（１）

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

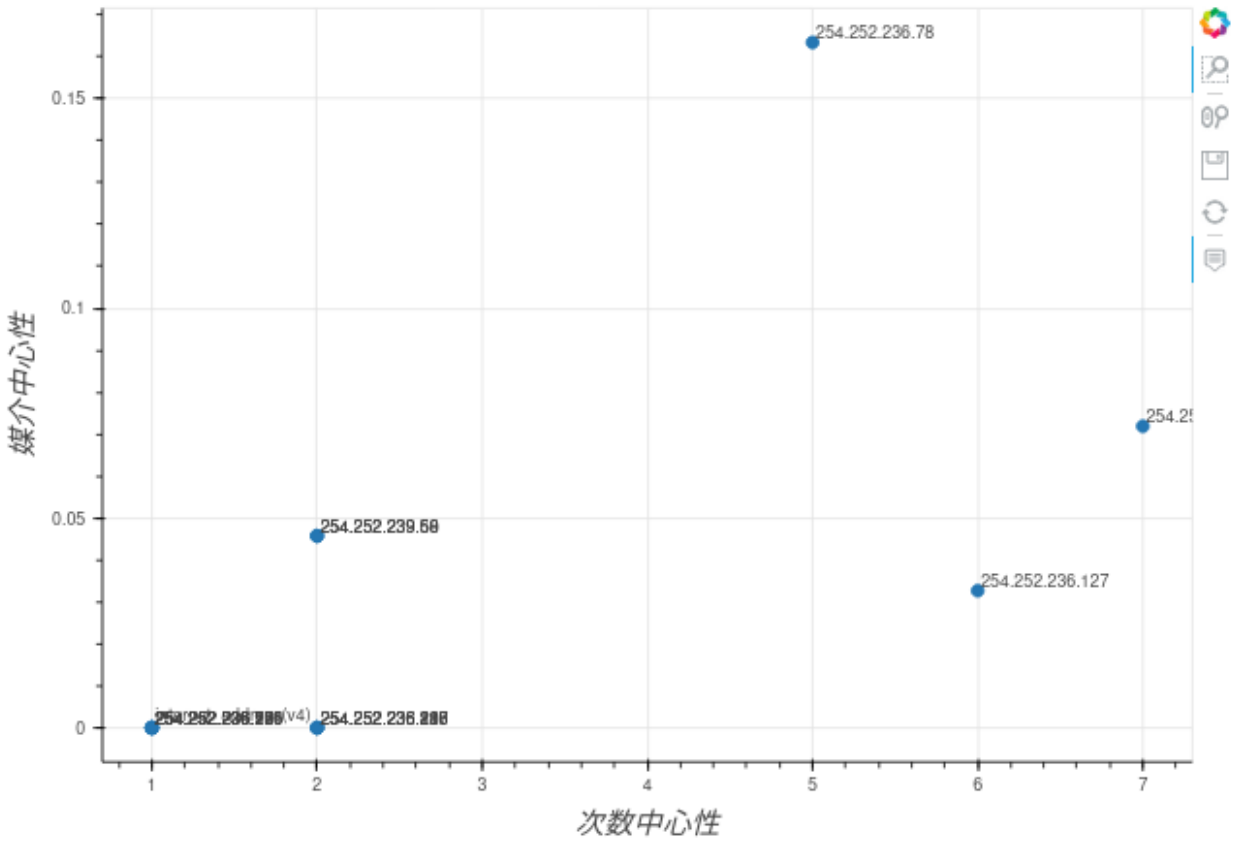



図.ラベル表示 ON 時のマップ（２）

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。



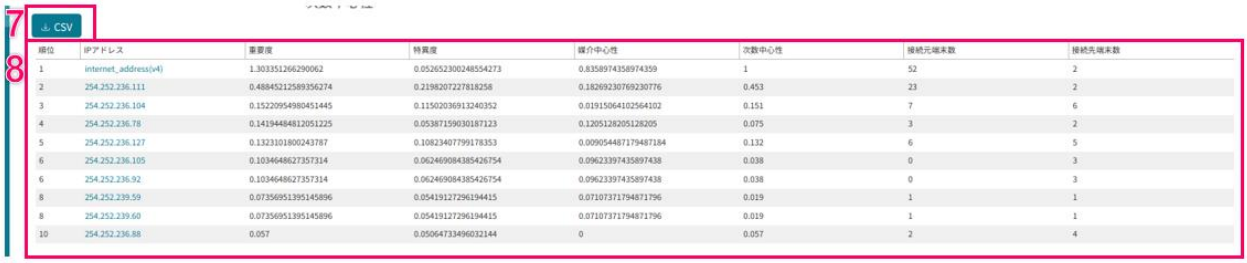
© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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）。




| 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 | 0.052652300248554273 | 0.835897435897435 9 | 1 | 52 | 2 |
| 2 | 254.252.236.111 | 0.48845212589356274 | 0.2198207227818258 | 0.18269230769230776 | 0.453 | 23 | 2 |
| 3 | 254.252.236.104 | 0.15220954980451445 | 0.11502036913240352 | 0.01915064102564102 | 0.151 | 7 | 6 |
| 4 | 254.252.236.78 | 0.14194484812051225 | 0.05387159030187123 | 0.1205128205128205 | 0.075 | 3 | 2 |
| 5 | 254.252.236.127 | 0.1323101800243787 | 0.10823407799178353 | 0.009054487179487184 | 0.132 | 6 | 5 |
| 6 | 254.252.236.105 | 0.1034648627357314 | 0.06246908438542 6754 | 0.09623397435897438 | 0.038 | 0 | 3 |
| 6 | 254.252.236.92 | 0.1034648627357314 | 0.06246908438542 6754 | 0.09623397435897438 | 0.038 | 0 | 3 |
| 8 | 254.252.239.59 | 0.07356951395145896 | 0.05419127296194415 | 0.07107371794871796 | 0.019 | 1 | 1 |
| 8 | 254.252.239.60 | 0.07356951395145896 | 0.05419127296194415 | 0.07107371794871796 | 0.019 | 1 | 1 |
| 10 | 254.252.236.88 | 0.057 | 0.0506473349603214 4 | 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 10.4. 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。

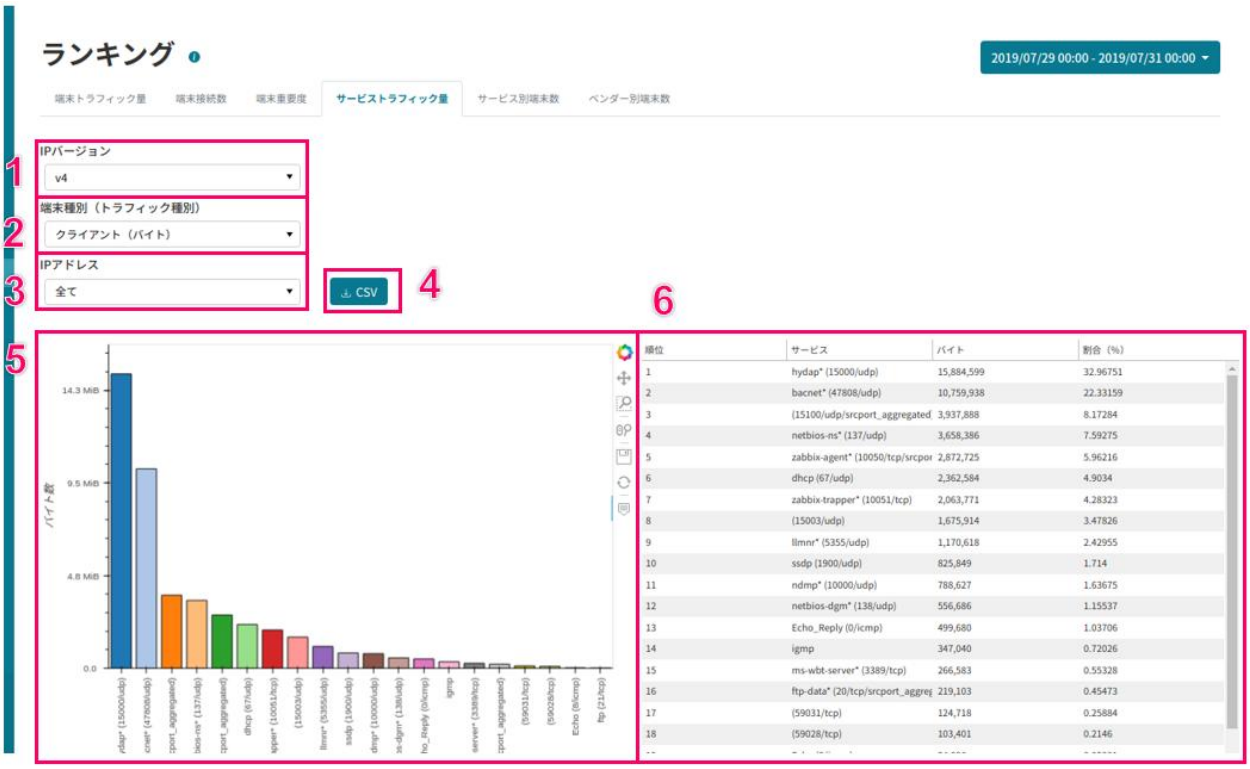



図. サービストラフィック画面

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 10.5. 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。

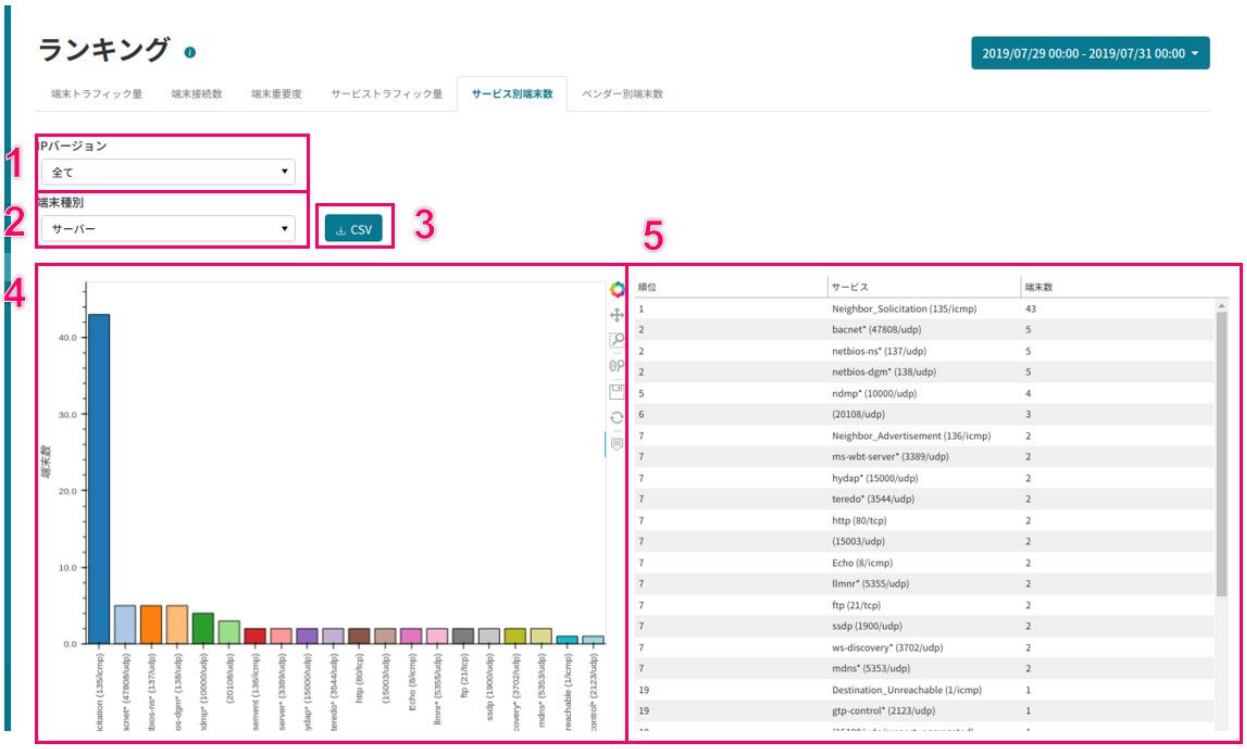



図. サービス別端末数画面

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 10.6. 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。

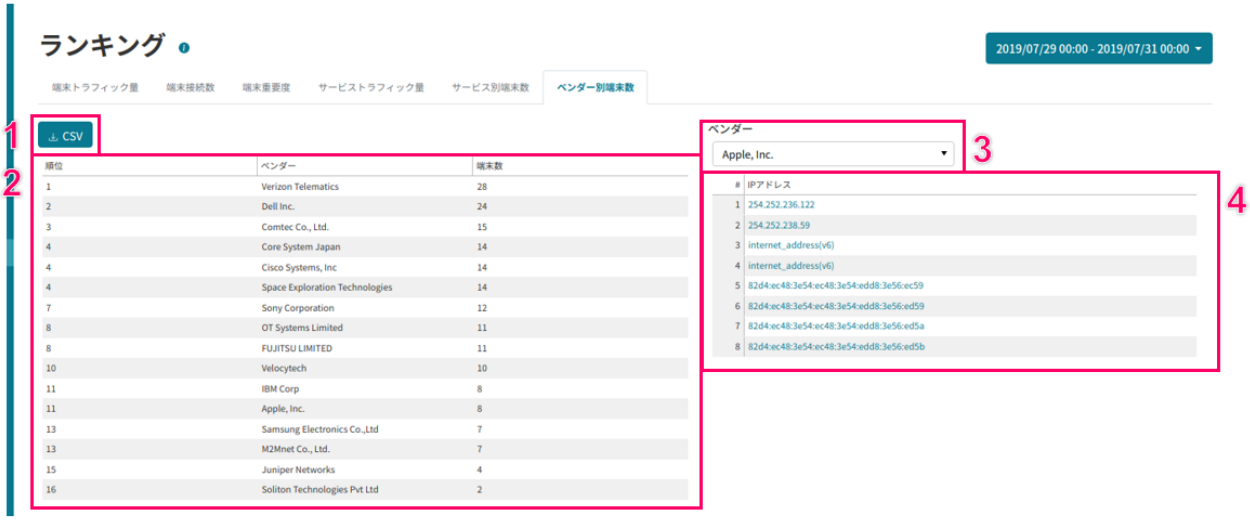



図. ベンダー別端末数画面

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 11. OTプロトコル

## 11.1. 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。

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。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 IP 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 |
| 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。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 |

## 11.2. 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。

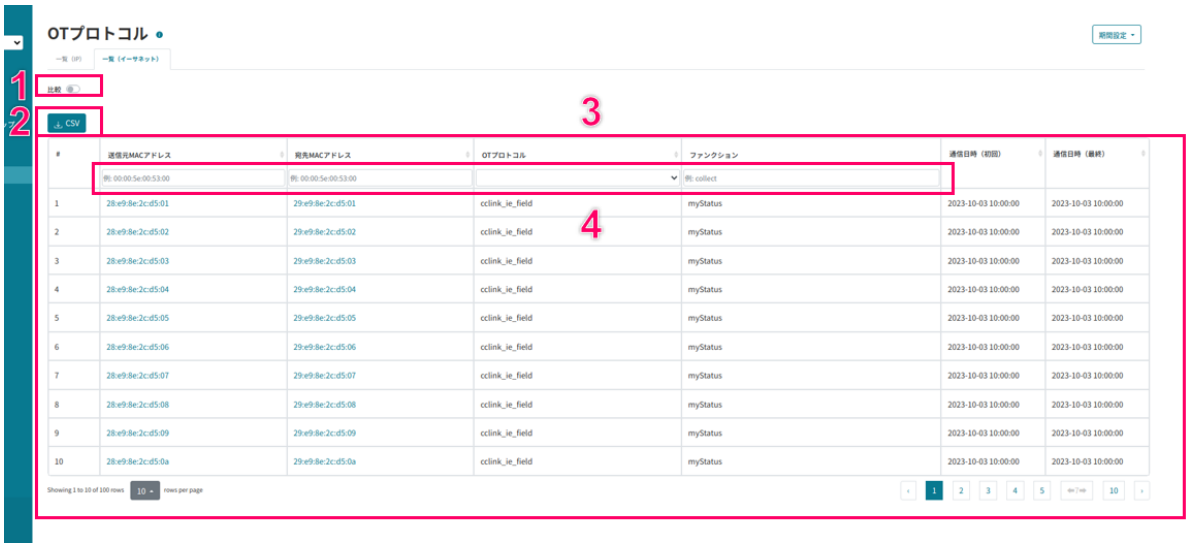


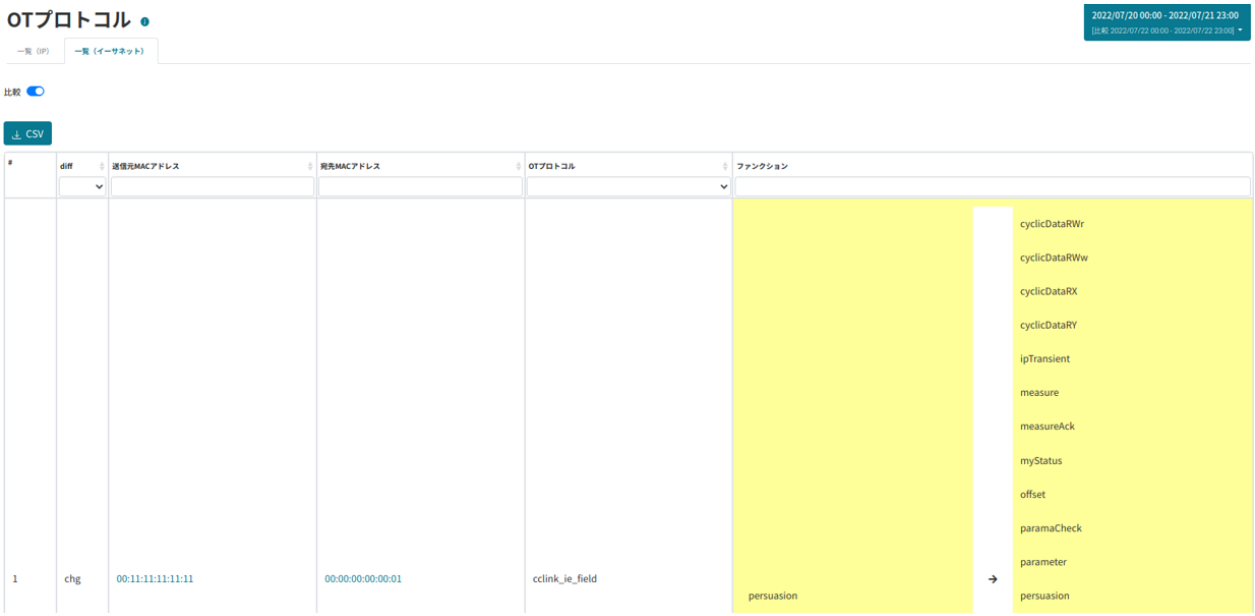

図. 一覧画面

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.




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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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 |
| 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。 |

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 12. 台帳

台帳画面のデータは、お客さまが手動でご登録いただいたデータが表示されます。台帳登録時を除いて、台帳のデータが自動で設定や更新されることはありません。なお、台帳はセンサー/ポート毎に独立して存在します。
登録いただいた台帳データは可視化機能やアラート機能と連携されます。

## 12.1. 一覧

台帳の登録や確認、編集、ダウンロードができます。登録した台帳は、接続端末の検知や可視化機能と連携できます。表示モードと編集モードの２つの状態が存在します。

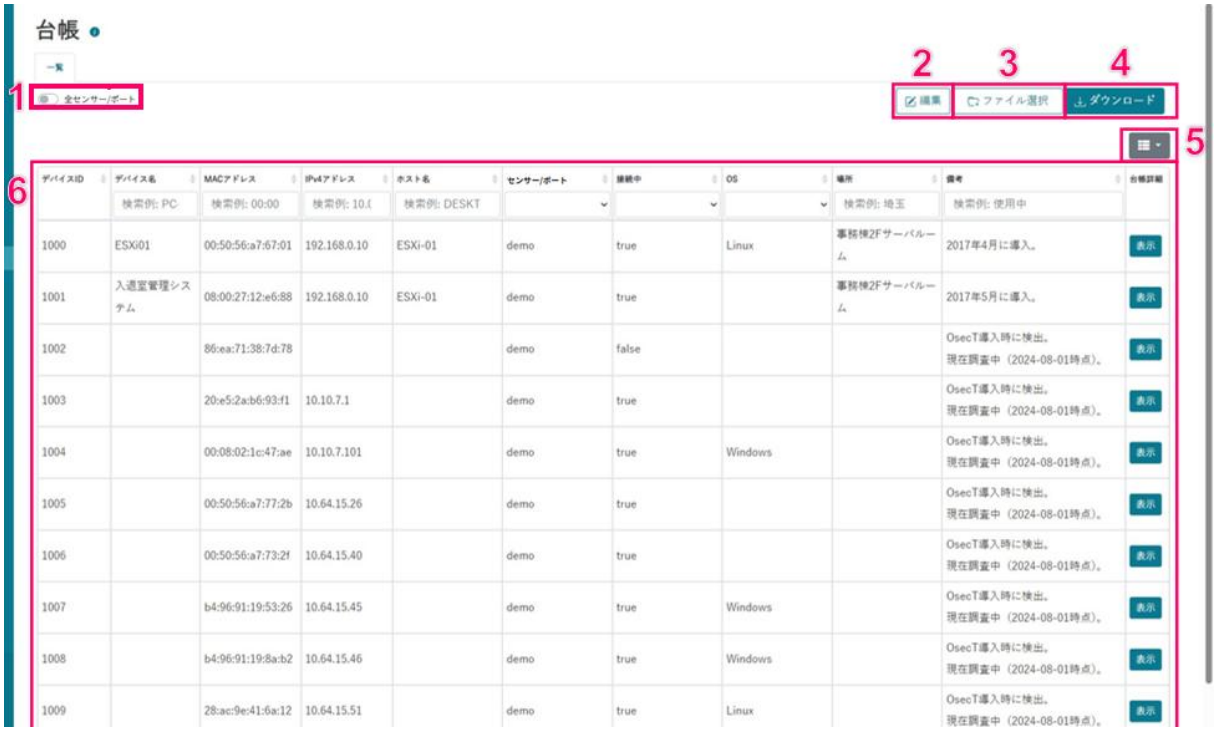



図. 台帳一覧画面（表示モード）

1. 全センサー/ポートボタン
   全センサー/ポートの台帳をまとめて表示できます。
2. 編集ボタン
   台帳の編集を行えます（デバイス ID や自動設定される項目を除く）。編集ボタンを押下すると、下記画像のように画面が変化し、編集モードに移行します。2.1 の一括削



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

除ボタンを押下すると、表示されている台帳をすべて削除します。1 の全センサー/ポートボタン有効時は、全センサー/ポートの台帳が削除される点にご留意ください。編集後、2.2 の保存ボタンを押下すると編集内容を保存できます。2.3 のキャンセルボタンを押下すると、編集内容を破棄し、表示モードに戻ります。2.4 のリセットボタンを押下すると、編集内容の破棄のみを行い引き続き編集を行えます。

なお、3 のファイル選択ボタンを押下し、ファイルを選択すると編集内容が破棄される点にご留意ください。

図. 台帳一覧画面（編集モード）

3. ファイル選択ボタン

台帳を CSV ファイル形式でアップロードすることで登録できます。ファイルを選択すると、下記画像のようにボタンが変化します。保存ボタンを押下することで、台帳を登録できます。登録を中止したい場合は、画面を閉じる、もしくは、キャンセルボタンを押下してください。

図. ファイル選択後に表示されるボタン

お手持ちの台帳がない場合は、端末一覧画面でダウンロードした CSV ファイルをアップロードすることもできます。なお、アップロードするファイルのエンコーディングは BOM 付きの UTF-8 形式である必要があります。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

台帳を CSV ファイル形式でアップロードする際に設定可能な項目は下記のとおりです。

| カラム名 | 説明 |
|---|---|
| デバイス ID | システム上でデバイスを識別するための ID、センサー/ポート毎に一意で、半角英数字と 3 つの半角記号（「-」、「_」、「.」）のみ利用可、最大 255 文字、自動設定有、省略可 |
| デバイス名 | 任意の文字列、最大 255 文字、省略可 |
| MAC アドレス | 他機能と連携する際の紐づけに利用、書式確認有、条件付きで省略可（※1） |
| IPv4 アドレス | 他機能と連携する際の紐づけに利用、書式確認有、条件付きで省略可（※1） |
| IPv4 プレフィックス長 | 半角数字、最小値-1、最大値 32、省略可 |
| IPv4 アドレス割当方法 ID | 「static」、「dhcp」、「apipa」、「none」、「unknown」のみ設定可能、省略可 |
| IPv4 アドレス割当方法 | 「手動」、「DHCPv4」、「APIPA」、「IP 割り当てなし」、「不明」のみ設定可能、省略可 |
| IPv6 アドレス | 他機能と連携する際の紐づけに利用、書式確認有、条件付きで省略可（※1） |
| IPv6 プレフィックス長 | 半角数字、最小値-1、最大値 128、省略可 |
| IPv6 アドレス割当方法 | 「static」、「dhcp」、「slaac」、「none」、「unknown」のみ設定可能、省略可 |
| IPv6 アドレス割当方法 | 「手動」、「DHCPv6」、「SLAAC」、「IP 割り当てなし」、「不明」のみ設定可能、省略可 |
| 優先 DNS サーバー | 任意の文字列、最大 255 文字、省略可 |
| 代替 DNS サーバー | 任意の文字列、最大 255 文字、省略可 |
| ホスト名 | 任意の文字列、最大 255 文字、省略可 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| ラベル ID | 登録先センサー/ポートに対応するラベル ID、自動設定有、省略可 |
| センサー/ポート | 登録先センサー/ポート表示名、自動設定有、省略可 |
| セグメント名 | 任意の文字列、最大 255 文字、省略可 |
| 接続中 | ネットワークに接続している場合「true」に設定、接続端末の検知に利用、自動設定有（設定値：「true」） |
| ベンダー | 任意の文字列、最大 255 文字、省略可 |
| モデル番号 | 任意の文字列、最大 255 文字、省略可 |
| シリアル番号 | 任意の文字列、最大 255 文字、省略可 |
| デバイスタイプ ID | 「nw」、「ot」、「it」、「other」のみ設定可能、省略可 |
| デバイスタイプ | 「ネットワークデバイス」、「OT デバイス」、「IT デバイス」、「その他」のみ設定可能、省略可 |
| デバイスタイプ詳細 ID | デバイスタイプに対応するより詳細なデバイスタイプ、省略可 |
| デバイスタイプ詳細 | デバイスタイプに対応するより詳細なデバイスタイプ、省略可 |
| OS ID | 「win」、「linux」、「unix」、「mac」、「android」、「ios」、「rtos」、「other」のみ設定可能、省略可 |
| OS | 任意の文字列、最大 255 文字、省略可 |
| SBOM URL | URL、最大 512 文字、省略可 |
| 場所 | 任意の文字列、最大 255 文字、省略可 |
| 作成者 | 常時自動設定（入力しても反映されない）、省略可 |
| 更新者 | 常時自動設定（入力しても反映されない）、省略可 |
| 作成日時 | 常時自動設定（入力しても反映されない）、省略可 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 更新日時 | 常時自動設定（入力しても反映されない）、省略可 |
| 担当組織 | 任意の文字列、最大 255 文字、省略可 |
| 担当者名 | 任意の文字列、最大 255 文字、省略可 |
| 担当者連絡先<br>備考 | 任意の文字列、最大 255 文字、省略可<br>最大 1024 文字、改行可、省略可 |

※1：各行ごとに、MAC アドレス、IPv4 アドレス、IPv6 アドレスのいずれか 1 列以上の値を設定する必要があります。また、MAC アドレス、IPv4 アドレス、IPv6 アドレスの組み合わせは、センサー/ポートごとに一意である必要があります。

各デバイスタイプに対して設定可能なデバイスタイプ詳細は下記のとおりです。なお、括弧尾内はそれぞれに対応するデバイスタイプ ID とデバイスタイプ詳細 ID です。

| **デバイスタイプ** | **デバイスタイプ詳細** |
|---|---|
| ネットワークデバイス（nw） | ルーター（rt）<br>スイッチングハブ（l2sw）<br>アクセスポイント（ap）<br>その他（other） |
| OT デバイス（ot） | PLC/シーケンサ（plc）<br>その他（other） |
| IT デバイス（it） | PC（pc）<br>スマートフォン（smart_phone）<br>プリンター（printer）<br>NAS（nas）<br>その他（other） |
| その他（other） | USB 型 LAN アダプター（usb_nic）<br>その他（other） |

4. ダウンロードボタン



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

台帳を CSV ファイル形式でダウンロードできます。ダウンロードしたファイルは、ファイル選択ボタンからアップロードすることもできます。

5. 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できます。

6. 一覧

   登録した台帳の確認や絞り込みができます。

| **カラム名** | **説明** |
|---|---|
| デバイス ID | 登録した値、もしくは自動設定された値 |
| デバイス名 | 登録した値 |
| MAC アドレス | 登録した値 |
| IPv4 アドレス | 登録した値、ネットワークアドレスを用いた絞り込みが可能（例：192.0.2.0/24） |
| IPv4 プレフィックス長 | 登録した値、-1 の場合は空白を表示 |
| IPv4 アドレス割当方法 | 登録した値 |
| IPv6 アドレス | 登録した値、ネットワークアドレスを用いた絞り込みが可能（例：2001:db8::/32） |
| IPv6 プレフィックス長 | 登録した値、-1 の場合は空白を表示 |
| IPv6 アドレス割当方法 | 登録した値 |
| 優先 DNS サーバー | 登録した値 |
| 代替 DNS サーバー | 登録した値 |
| ホスト名 | 登録した値 |
| センサー/ポート | 登録した値、もしくは自動設定された値 |
| セグメント名 | 登録した値 |
| 接続中 | 登録した値、もしくは自動設定された値 |
| ベンダー | 登録した値 |
| モデル番号 | 登録した値 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| シリアル番号 | 登録した値 |
| デバイスタイプ | 登録した値 |
| デバイスタイプ詳細 | 登録した値 |
| OS | 登録した値 |
| SBOM URL | 登録した値、ハイパーリンク |
| 場所 | 登録した値 |
| 更新者 | 台帳をアップロードしたお客さまのユーザーID |
| 更新日時 | 台帳の登録日時 |
| 備考 | 登録した値、最大表示文字数 300 文字、最大表示行数 3 行 |
| 担当組織 | 登録した値 |
| 担当者名 | 登録した値 |
| 担当者連絡先 | 登録した値 |
| 台帳詳細 | 台帳詳細を確認するためのボタン |

## 12.2. 詳細

表示される項目は、一覧と同じです。一覧では最大 3 行のみ表示される備考を、全て確認できます。また、編集も可能です。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. 台帳詳細画面（表示モード）

1. 編集ボタン

   台帳の編集を行うことが出来ます（デバイス ID や自動設定される項目を除く）。編集ボタンを押下すると、編集できます。

2. 詳細

   登録した台帳情報を確認できます。

## 12.3. 補足：可視化や検知機能との連携に関して

可視化機能や検知機能との連携時には、MAC アドレスと IPv4 アドレス、IPv6 アドレスを利用して端末と台帳の紐づけを行います。この際、端末に対して複数の台帳が紐づけられる可能性があります。

なお、検知機能との連携時には端末と台帳の紐づけは誤判定によるアラートの不送出を防ぐために可視化機能との連携時よりも厳密な紐づけ処理を行い、更に接続中である端末のみ紐づけます。そのため、各可視化画面では台帳情報が表示されるにもかかわらず、アラート画面では台帳情報が表示されないことがあります。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 13. 物理構成

OsecT ポーラーの出力ファイルをインポートすることで、機器間の物理接続マップおよび機器やリンクの詳細情報を確認できます。本画面の情報は、SNMP ポーリングによりネットワーク機器等から収集した情報に基づき生成されます。
※本機能をご利用されたい場合は、個別にお問い合わせください。

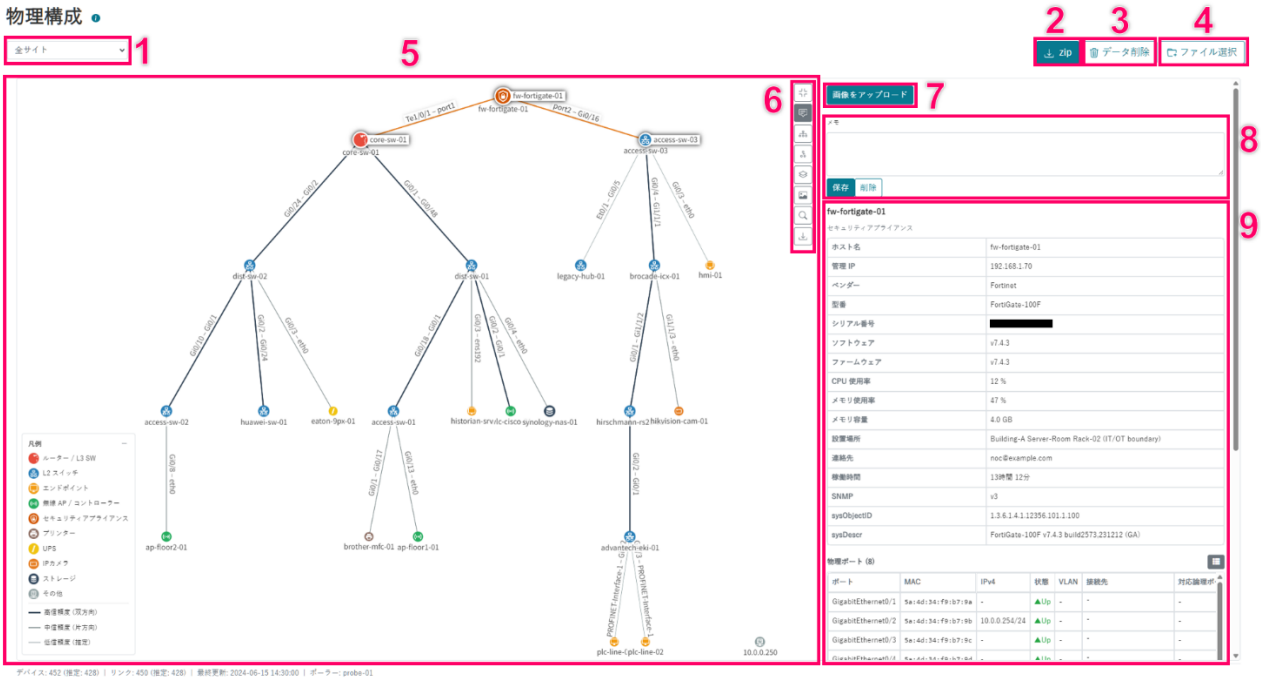



図. 物理構成画面

1. サイト切り替え
   OsecT ポーラーの出力ファイル内のサイトの単位で表示情報を切り替えできます。
   全サイトを選択した場合は、全サイトのデータを統合表示します。
2. ZIP ボタン
   ボタンを押下することで、8 に表示される機器やリンクに関する詳細情報データ CSV で構成される ZIP 形式ファイルをダウンロードできます。
3. データ削除ボタン



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

インポートされた OsecT ポーラーの出力ファイルデータを削除します。アップロードした画像ファイルや登録したメモは削除されません。物理構成に関する全てのデータを削除したい場合は、システム設定画面から削除してください。

4. ファイル選択ボタン

   OsecT ポーラーの出力ファイルをインポートできます。ファイルを選択すると、ボタンが変化し、保存ボタンを押下することで、選択したファイルが取り込まれます。登録を中止したい場合は、画面を閉じる、もしくは、キャンセルボタンを押下してください。

5. 物理マップ

   機器間の物理的な接続状態をマップ表示します。役割に応じて、ノードの色が変わります。

6. マップメニュー

   - ズームリセット

     マップのズームを初期状態にリセットします。

   - ポートラベル表示

     リンクの傍に両端の物理ポートのラベル情報を表示します。

   - MAC FDB 端末表示

     MAC フォワーディングデータベース情報に基づき、各機器のポートの先に存在すると推測される機器をマップ上に表示します。実際には、物理的にワンホップでの接続関係にない可能性があります。

   - 集約ノードを展開

     MAC フォワーディングデータベース情報に基づく推定機器など、1 つの物理ポートの先に複数の物理機器情報が紐づく状況の場合、デフォルトではそれらの機器を 1 つのノードとして集約して図示します。本ボタンを ON にすることで、これらを 1 機器ずつマップ上に図示できます。

   - レイアウト

     現在のレイアウトの保存・復元・削除ができます（最大 10 個）。ノードの位置をドラッグで移動して調整した後のレイアウトの保存に利用できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

- 背景

  任意の画像をインポートし、マップ領域の背景として設定できます。

- 検索

  検索に入力したキーワードを含むノードやリンクをハイライト表示できます。

- PNG エクスポート

  マップを PNG 形式で保存できます。

7. 画像をアップロードボタン

   機器の写真などをアップロードできます。

8. メモ

   機器に関するテキスト情報などを記載できます。

9. 機器/リンク詳細情報

   ノードやリンクを押下することで、標準 MIB やベンダー個別 MIB で取得した機器、ポート、リンクの詳細情報を表示できます。値が取得できていない項目は非表示になります。

   表示される情報には、次のようなものが含まれます。

   - 機器情報：ホスト名、管理 IP、ベンダー、型番、シリアル番号、ハードウェアリビジョン、ソフトウェア/ファームウェア、リソース情報（CPU 使用率、メモリ使用率など）、設置場所、連絡先、稼働時間、sysObjectID、sysDescr
   - 物理ポート情報：インタフェース毎のポート名、ifDescr、ifAlias、MAC、IPv4、IPv6、リンク状態、速度、VLAN（Tagged / Native）、PoE、接続先、対応論理ポート
   - 論理ポート情報：ポート名、ifDescr、ifAlias、種別、IPv4、IPv6、状態、VLAN、対応物理/論理ポート
   - VLAN 情報：VLAN ID や名前
   - IP アドレス情報：インタフェースに割り当てられた IPv4/IPv6 アドレス
   - ストレージ：ストレージ情報
   - 無線 LAN 情報：無線 AP の WLAN 情報、AP ラジオ別接続数、AP に接続された無線クライアント情報、ワイヤレスコントローラの管理する AP 情報



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 14. 脆弱性

パッシブ監視で収集した通信情報や OsecT スキャナーの出力ファイルをインポートすることで、機器のベンダー、モデル、バージョンと公開脆弱性情報を突合し、その機器に該当し得る脆弱性（CVE）を一覧で確認できます。

※OsecT スキャナーをご利用されたい場合は、個別にお問い合わせください。

図. 脆弱性画面

1. ジョブファイルダウンロードボタン

   選択中のセンサー/ポートについて、期間設定で指定された期間の通信ログから OT プロトコルの通信を行っている機器を抽出し、OsecT スキャナー用のジョブファイル（JSON 形式）をダウンロードできます。対象となる機器が存在しない場合は、その旨を表示し、ファイルは出力されません。

2. CSV ボタン

   一覧に表示されている突合結果を CSV ファイルとしてダウンロードできます。既定で非表示の列も含めて出力し、画面の表示上限（5,000 件）を超える場合も全件が対象となります。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. 通信ログから突合ボタン

選択中のセンサー/ポートについて、期間設定で指定された期間の通信ログ（パッシブ解析）から機器情報を取得し、公開脆弱性情報と突合します。OsecT スキャナーの出力ファイルの取り込みなしで利用できます。

ただし、通信ログ（パッシブ解析）から機器の識別情報を取得できるのは、一部のプロトコルの通信に限られます。

本ボタンによる突合結果は、最新の 1 回分のみ保持され、実行するたびに以前の結果と置き換わります（スキャン結果のアップロードによる突合結果は削除されません）。

4. スキャン結果を選択ボタン／スキャン結果アップロードボタン

OsecT スキャナーの出力ファイル（JSON 形式）を選択します。複数のファイルを同時に選択できます。ファイルを選択すると「スキャン結果アップロード」ボタンが表示され、押下することで、選択したファイルが取り込まれ、公開脆弱性情報と突合されます。

なお、ファイル内のセンサー/ポート ID が選択中のセンサー/ポートと異なる場合、そのファイルは取り込まれません。

5. データ削除ボタン

取り込んだ機器情報と突合結果をすべて削除します。取り込み済みのデータが存在する場合のみ表示されます。

6. 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。

7. 一覧

1 行が「機器 × 部品 × CVE」の突合結果を表します。同じ IP アドレスの機器でも、応答した OT プロトコルが異なる場合は別の部品として表示されることがあります。

| カラム名 | 説明 |
|---|---|
| IP アドレス | 機器の IP アドレス。 |
| MAC アドレス | 機器の MAC アドレス。 |
| ベンダー | 機器のベンダー名。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| モデル | 機器のモデル名（型番） |
| バージョン | 機器のファームウェアなどのバージョン |
| CVE | 該当し得る脆弱性の CVE 番号。紐づく脆弱性情報が見つからなかった場合は空欄 |
| 深刻度 | CVSS の深刻度（CRITICAL、HIGH、MEDIUM、LOW） |
| 信頼度 | その機器が脆弱性の影響を受けるかの確からしさ（高、中、低、不明）。詳細は「補足：信頼度について」を参照 |
| 機器情報取得日時 | 機器情報を取得した日時 |
| OT プロトコル ※1 | 機器情報の取得に使用した OT プロトコル |
| 部品種別 ※1 | 判定した部品の種別 |
| アドバイザリ ID ※1 | 判定の根拠としたアドバイザリの ID。 |
| 取り込み日時 ※1 | 機器情報を OsecT へ取り込んだ日時 |
| センサー/ポート ID ※1 | 機器情報を取得したセンサー/ポートの ID |

※1 既定では非表示です。表示列指定ボタンから表示できます。

8. 一覧フィルタ

一覧の各列の内容で一覧をフィルタリングできます。IP アドレスと MAC アドレスは、カンマ区切りで複数指定でき、それぞれ前方一致で判定します。

9. 詳細表示

一覧の各行の左端を押下すると、その脆弱性の詳細情報を表示します。表示される情報は以下のとおりです。

| **項目** | **説明** |
|---|---|
| 概要 | 脆弱性の概要 |
| 脆弱性の名称 | アドバイザリに記載された脆弱性の名称 |
| アドバイザリ | 判定の根拠としたアドバイザリの ID とタイトル |
| 発行元 | アドバイザリの発行元と公開日 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| CVSS | CVSS のスコアとバージョン |
| CWE | 脆弱性の種類（CWE） |
| 対処 | 対処方法。「ベンダの修正」「緩和策」「回避策」「修正なし」「修正予定なし」の区分とともに表示 |
| 出典 | 判定に使用したアドバイザリ |
| 概要 | 脆弱性の概要 |
| 脆弱性の名称 | アドバイザリに記載された脆弱性の名称 |
| アドバイザリ | 判定の根拠としたアドバイザリの ID とタイトル |
| 発行元 | アドバイザリの発行元と公開日 |
| CVSS | CVSS のスコアとバージョン |
| CWE | 脆弱性の種類（CWE） |

概要と対処は日本語に翻訳して表示し、あわせて原文を併記します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 15. 検知アラート

## 15.1. 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。上部のタブから脅威検知ごとの検知結果画面を表示することもできます。

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. センサー/ポート

   検知結果一覧に表示する対象のセンサー/ポートを、「選択中のセンサー/ポート」または「全センサー/ポート」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/ポート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/ポート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（最終） | 最後に検知された日時 |
| 検知日時（初回） | 最初に検知された日時 |
| 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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.2. 接続端末（◎：オススメ機能）

接続端末学習済データ（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。また、消滅端末検知オプションを有効化することで、未学習端末の出現アラート後、一定時間通信しなかった端末を消滅としてアラート表示します。

図. 接続端末 検知アラート画面

1. ステータス

   接続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

   学習データに接続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** |
|---|---|
| 台帳登録 | 端末が台帳に存在する場合は台帳へのリンク付きで「有」、存在しない場合は「無」を表示 |
| 検知日時 | 接続端末を検知した日時 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 検知種別 | 検知した種別（出現または消滅） |
| 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 |

※　端末と台帳の紐づけに関しては「12.3 補足：可視化や検知機能との連携に関して」をご確認ください。

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.3. 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。

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.4. 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。

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 | 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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.5. 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。

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） |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

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（流量上振れ: 上限値を超えた、流量下振れ: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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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（流量停止: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。

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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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）。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.6. 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。

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。

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）<br>種別は以下のとおり<br>ARP 要求対象 IP 数 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| | ARP 要求送信パケット数<br>DNS 要求ドメイン数<br>DNS 要求送信パケット数<br>MAC アドレス数<br>送信先 IP 数<br>送信元ポート数<br>送信先ポート数<br>プロトコル番号数<br>送信パケット数<br>受信パケット数<br>送信パケット平均サイズ<br>受信パケット平均サイズ<br>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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.7. 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（学習画面の検知対象ファンクションで設定）を検知したアラート情報の一覧画面です。

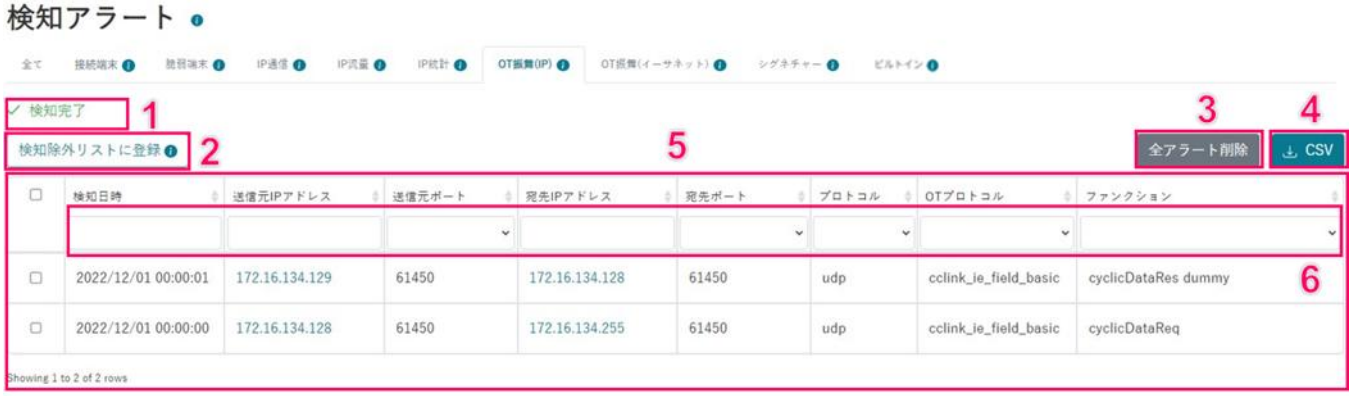



図. OT 振舞（IP） 検知アラート画面

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.8. 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（学習画面の検知対象ファンクションで設定）を検知したアラート情報の一覧画面です。

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.9. シグネチャー

シグネチャーによる検知の一覧画面です。

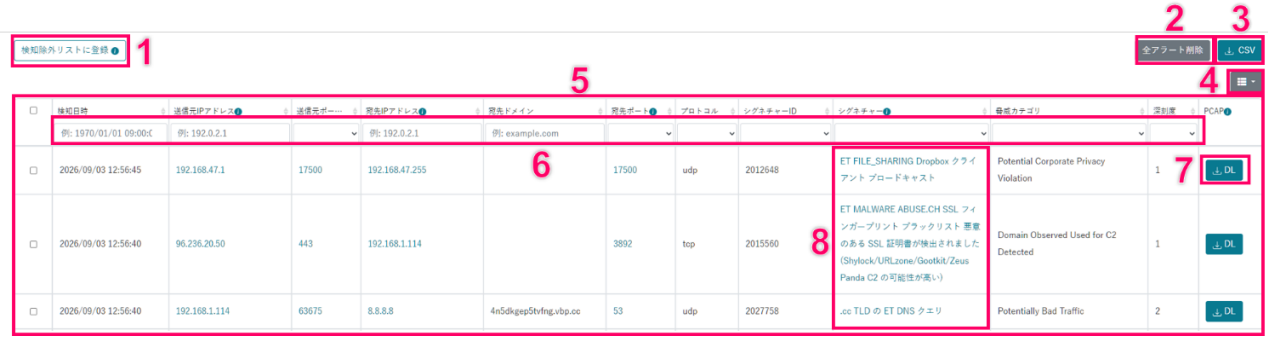



図. シグネチャー 検知アラート画面

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。

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. 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できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. 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 |
| 宛先ドメイン | 宛先ドメイン名 |
| 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ID | 検知されたシグネチャーの ID |
| 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） |

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。

7. DL ボタン

シグネチャー検知された際のトラフィックの情報を pcap ファイルとしてダウンロードできます。「DL」ボタンを押下すると、「DL 準備中」にボタンが変化します。5 分程度お待ち頂き、ボタンが「DL 可能」に変化した後に押下頂くことで、pcap ファイルをダウンロードできます。また、センサーに当該アラートに関する pcap ファイルが存在しない場合は、ボタンが「取得失敗」に変化します。pcap ファイルはセンサー内に最大 14 日間、最大 5GB まで蓄積されます。

DL ボタンを頻繁に押下した場合、pcap 取得のための通信により、月間の通信量を超過し、帯域制限がかかることで、センサーから Web ポータルへのログ送信が不能になる可能性があるため、注意してご利用ください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

なお、1 つの pcap には複数のアラートに関するパケットが記録されるため、あるアラートの「DL」ボタンを押下した際に、連動して別のアラートの「DL」ボタンも「DL 準備中」に変化する場合があります。

8. シグネチャー解説ページへのリンク

シグネチャー列の文字部分のリンクを押下することで、下記のようなシグネチャー解説画面を表示できます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 15.10. ビルトイン

ビルトインによる検知の一覧画面です。

図. ビルトイン 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。

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. 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できます。

5. 検知結果一覧

| **カラム名** | **説明** |
|---|---|
| 検知日時 | 検知した日時 |
| 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 |
| 脅威カテゴリ | 脅威のカテゴリ（ARPSPOOF 等） |
| 検知内容 | 検知した内容の概要 |
| 補足 | 検知した内容の補足 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 16.　学習・検知設定

## 16.1.　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。

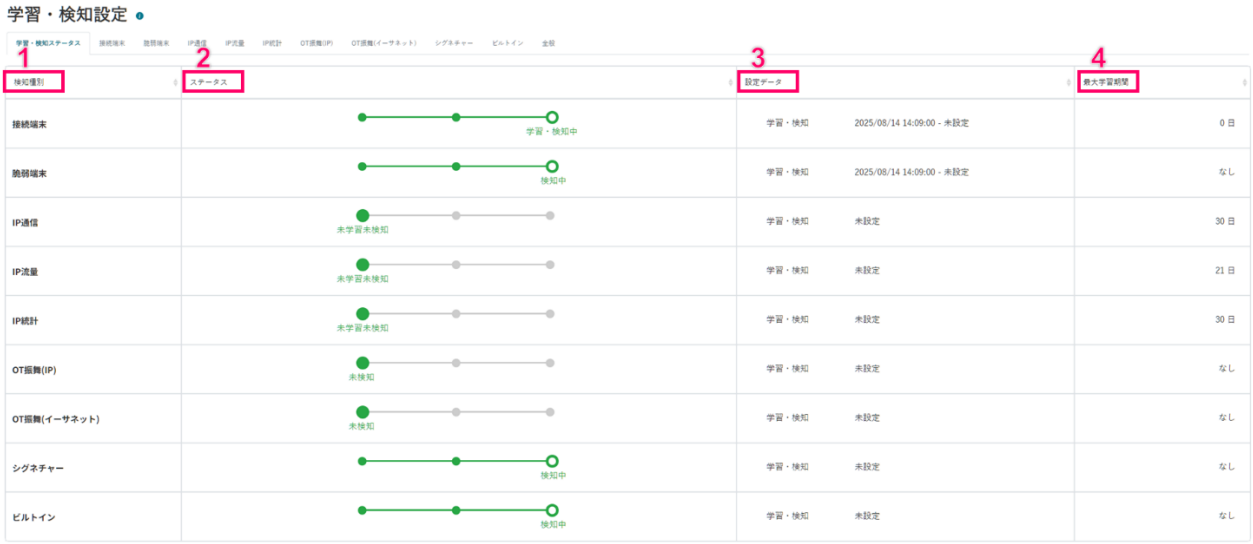



図. 学習・検知ステータス画面

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.2. 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。

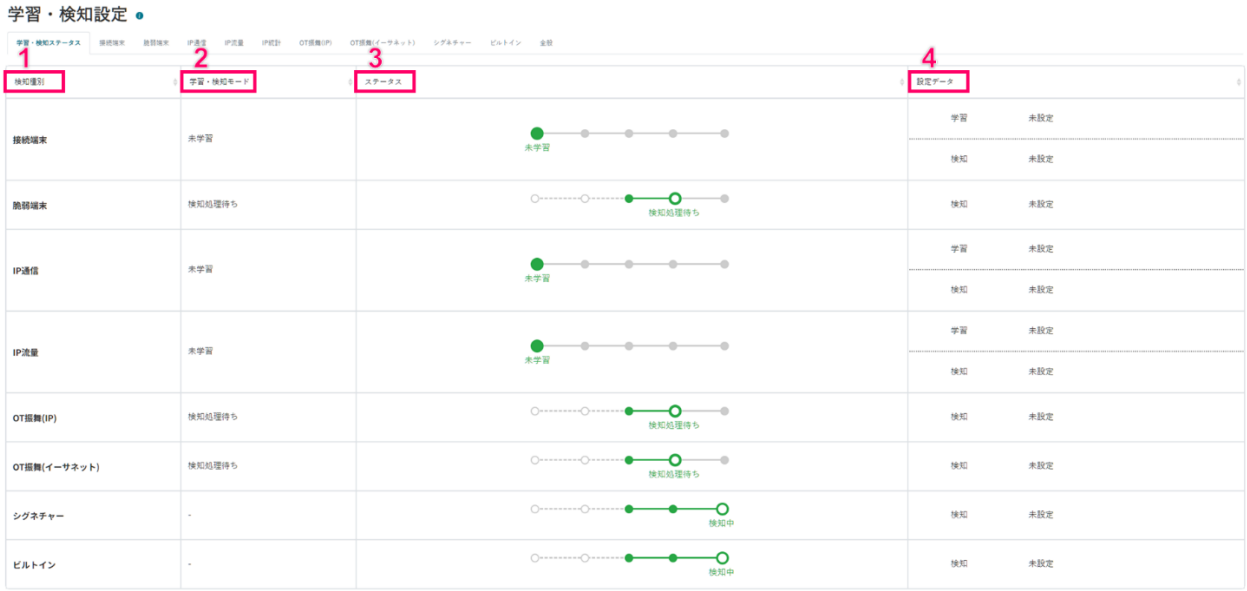



図. 学習・検知ステータス画面（アドバンスモード）

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** |
|---|---|



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.3. 接続端末

接続端末学習済データ（学習期間中に観測された端末情報）の一覧画面です。

図. 接続端末学習済リスト画面

1. ステータス

   接続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

   端末追加画面を表示し、学習データに接続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 |
|---|---|



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| × | 「×」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 |
| 消滅検知 | 消滅端末検知機能が有効の場合のみ表示されます。端末毎に消滅検知の対象とするかのオン/オフができます |
| 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。

学習データに接続端末データを追加登録する画面です。

図. 端末追加画面

7. 一覧ページに戻る

端末追加画面から、接続端末学習済データ一覧画面に戻ることができます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。IP アドレスを*、MAC アドレスのみを入力して登録することで、MAC アドレスのみに基づき出現・消滅の判定が実施されます。

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.4. 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

   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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

検知除外リストに脆弱端末データを追加登録できます。

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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.5. 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。

図. IP 通信学習済リスト画面

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 |
|---|---|



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| × | 「×」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。

学習データに IP 通信データを追加登録できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. 通信追加画面

7. 一覧ページに戻る

   通信追加画面から、ネットワークホワイトリスト一覧画面（IP 通信学習済リスト画面）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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.6. 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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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. 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。

16. 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。

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、ブラウザー、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）。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.7. 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。

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<br>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<br>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<br>デフォルトは「弱」 |
| IP アドレス | IP アドレス |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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）



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.8. 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ンクションの検知）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. 通信追加ボタンステータス

   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<br>＊（アスタリスク）は全ての OT プロトコル |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| ファンクション | 検知除外設定されたファンクション<br>＊（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

   検知対象ファンクション画面を表示し、ファンクション毎に OT 振舞（IP）検知の ON/OFF を設定します。

OT 振舞（IP）検知しない通信を登録します。

図. 通信追加画面



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.9. 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ンクションの検知）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<br>＊（アスタリスク）は全ての OT プロトコル |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| ファンクション | 検知除外設定されたファンクション<br>＊（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

   検知対象ファンクション画面を表示し、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。

OT 振舞（イーサネット）検知しない通信を登録します。

図．通信追加画面



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

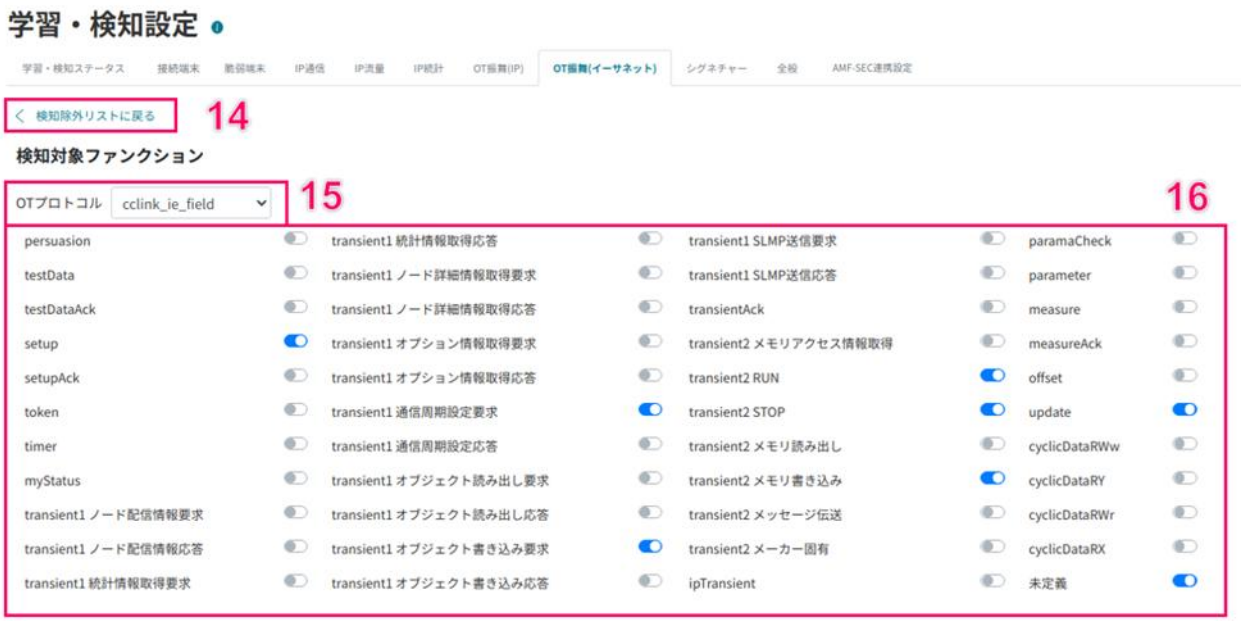



図. 検知対象ファンクション画面

14. 検知除外リストに戻る



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.10. シグネチャー

シグネチャーにおける検知除外の一覧、カスタムシグネチャー設定画面です。

図. シグネチャー検知除外リスト・カスタムシグネチャー画面

1. シグネチャー追加ボタン

   検知除外リスト追加画面に遷移し、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できます。

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. フィルタ



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

テーブルの各列の内容で一覧をフィルタリングできます。

6. カスタムシグネチャー編集ボタン

カスタムシグネチャー編集画面に遷移し、カスタムルールを登録できます。

検知除外リスト追加画面では、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できます。

図. 検知除外リスト追加画面

1. 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。

2. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

3. 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。
4. 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。
5. 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。

カスタムシグネチャー編集画面では、シグネチャー検知に用いるカスタムルールを登録できます。

図. カスタムシグネチャー編集画面（全センサー/ポート共通ルール設定・確認画面）

1. センサー/ポート選択
   「全センサー/ポート共通」、「個別のセンサー/ポート」を選択することで、全センサー/ポート共通で設定するルールを編集・確認する画面と、個別のセンサー/ポートのみに設定するルールを編集・確認する画面の切り替えができます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

2. カスタムシグネチャールール入力欄

   カスタムシグネチャールールを入力できます。ルールは Suricata ルール形式かつ、「action」は「alert」で、「sid」を必ず含む形で、1 ルールを 1 行に記述してください。なお、「sid」は標準のルールセットに設定されたものを含めてユニークである必要があります。カスタムシグネチャールールでは、「1000000-1999999」のローカル利用のために予約された範囲の値を割り当てて頂くことを推奨します。

3. 保存ボタン

   カスタムシグネチャールール入力欄に入力したルールを保存できます。保存後、5-10 分程度で、対象のセンサー/ポートにカスタムルールが反映されます。各センサーへのカスタムルール反映状況は、後述の個別センサー/ポートルール設定・確認画面で確認できます。

4. クリアボタン

   カスタムシグネチャールール入力欄に入力したルールを削除します。クリア後、5-10 分程度で、対象のセンサー/ポートからカスタムルールが除去されます。

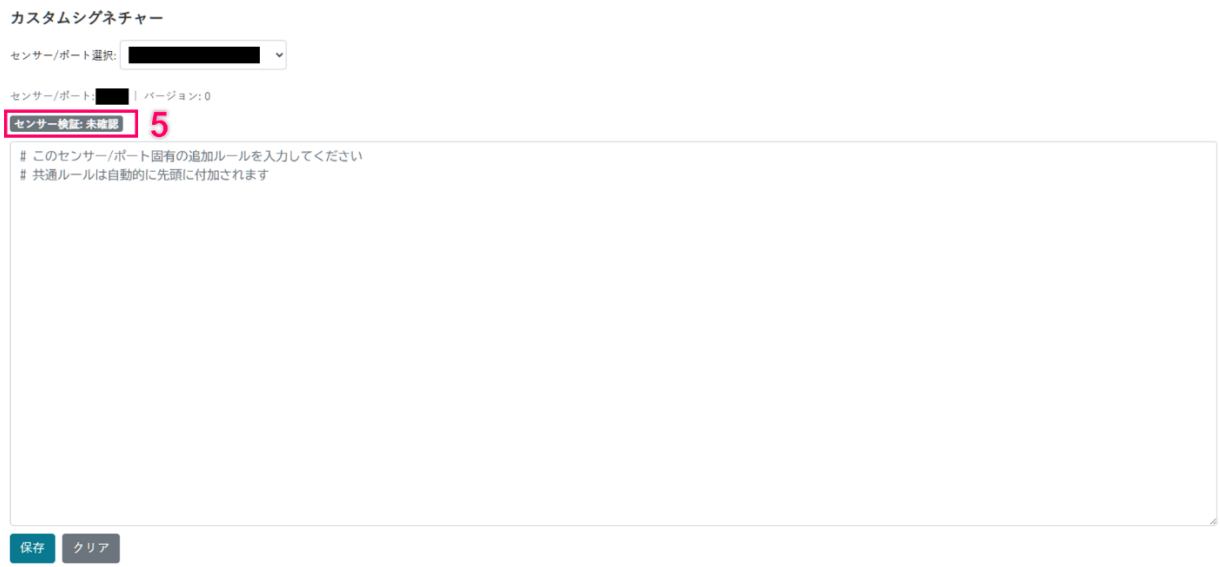



図. カスタムシグネチャー編集画面（個別センサー/ポートルール設定・確認画面）

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. カスタムルールが正常に適用された場合のセンサー検証ステータス表示

5. センサー検証ステータス

個別センサー/ポートルール設定・確認画面において、当該センサー/ポートへのカスタムルール設定状況を確認できます。

- 未確認：当該センサー/ポートにカスタムルールが設定されていない状況です。
- OK：当該センサー/ポートにカスタムルールが正常に設定されている状況です。また、右側にカスタムルールが適用された時刻が表示されます。
- エラー：当該センサー/ポートへのカスタムルール設定がエラーになっている状況です



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.11. ビルトイン

ビルトインによる検知除外の一覧画面です。

図. ビルトイン検知除外リスト画面

1. 除外対象追加ボタン

   検知除外リスト追加画面に遷移し、ビルトイン検知しない送信元 IP アドレスと脅威カテゴリの組を登録できます。

2. 全検知除外設定削除ボタン

   除外設定をすべて削除します。

3. CSV ボタン

   ビルトイン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 |
| 脅威カテゴリ | 検知除外設定された脅威カテゴリ |

5. フィルタ

   テーブルの各列の内容で一覧をフィルタリングできます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

検知除外リスト追加画面では、ビルトイン検知しない送信元 IP アドレスと脅威カテゴリの組を登録できます。

図. 検知除外リスト追加画面

6. 一覧ページに戻る
   追加画面から、ビルトイン検知除外リスト画面に戻ることができます。
7. 送信元 IP アドレス
   ビルトイン検知除外対象に追加する送信元 IP アドレスを入力できます。
8. 脅威カテゴリ
   ビルトイン検知除外対象に追加する脅威カテゴリを選択できます。
9. 追加ボタン
   追加ボタンを押下することでビルトイン検知除外対象をリストに追加することができます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.12. 全般

脅威検知機能を簡易に制御する画面です。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. 全般画面

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. 適用範囲

   現在のセンサー/ポートのみに設定を適用するか、全センサー/ポートに設定を適用するかの選択ができます。本メニューは複数のセンサー/ポートが存在する場合のみ表示されます。適用範囲の切り替えによる、全センサー/ポートへの一括設定に対応している項目は、アドバンスモードの切り替え、学習・検知設定になります。なお、通知設定は、適用範囲の選択に関わらず、全センサー/ポート共通の設定項目になります。

2. 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。

3. 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。また、各メールアドレスに通知する言語およびタイムゾーンを設定できます。「連絡先を追加」を押下することで、最大 5 件のメールアドレスを設定できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

4. 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。また、接続端末のみ「台帳に無い接続端末のみ通知」を選択できます。

5. 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。

6. 種別

学習・検知対象の脅威検知機能を選択します。

7. 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。

接続端末、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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 | 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 |

9. 消滅端末検知

消滅端末検知機能を有効化、無効化できます。

10. 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。

11. 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。

12. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.13. 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。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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. 適用範囲

   現在のセンサー/ポートのみに設定を適用するか、全センサー/ポートに設定を適用するかの選択ができます。本メニューは複数のセンサー/ポートが存在する場合のみ表示されます。適用範囲の切り替えによる、全センサー/ポートへの一括設定に対応している項目は、アドバンスモードの切り替え、学習設定、検知設定になります。なお、通知設定は、適用範囲の選択に関わらず、全センサー/ポート共通の設定項目になります。

2. 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。

3. 通知設定

   設定したメールアドレスに検知アラートを通知できます。また、各メールアドレスに通知する言語およびタイムゾーンを設定できます。「連絡先を追加」を押下することで、最大 5 件のメールアドレスを設定できます。

4. 通知設定詳細



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。また、接続端末のみ「台帳に無い接続端末のみ通知」を選択できます。

5. 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。

6. 学習種別

学習対象の脅威検知機能を選択します。

7. 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 |

8. 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 |

9. アクション



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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 |

10. 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。

11. 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。

12. 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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. 全般（アドバンスモード）画面（検知設定）

13. 検知種別

検知対象の脅威検知機能を選択します。

14. 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 |

15. 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 |
|---|---|



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | |
|---|---|
| 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 |

16. 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 |

17. 消滅端末検知

消滅端末検知機能を有効化、無効化できます。

18. 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。

19. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 16.14. 連携

OsecT と他製品/機能との連携設定に関する画面です。

画面上部の連携タブにカーソルを合わせることで、各連携製品/機能の設定ページへ遷移するためのメニューが表示されます。

図. 連携タブにカーソルを合わせた際の表示メニュー

### 16.14.1. AMF-SEC

アライドテレシス社 AMF-SEC との連携機能に関する設定のための画面です。本機能により、OsecT で特定の脅威を検知した場合に、メールを通じて AMF-SEC に通知することで、当該アラートに含まれる送信元 IP アドレスまたは MAC アドレスを用いた通信の自動遮断（対処の自動化）を行えます。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. AMF-SEC 画面

1. 通知設定

   AMF-SEC 機能との連携に用いるメールアドレスを登録できます。また、各メールアドレスに通知する言語を設定できます。「連絡先を追加」を押下することで、最大 5 件のメールアドレスを設定できます。

2. 検知種別設定

   AMF-SEC 連携による自動対処の対象にしたい検知種別を選択できます。接続端末とシグネチャーを登録できます。シグネチャーは、シグネチャー種別から選択できます。

3. 登録

   登録ボタンをクリックすることで、通知設定と検知種別設定の変更点を保存できます。

### 16.14.2. 信号灯

パトライト社の信号灯との連携設定に関する画面です。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

OsecT で特定の脅威を検知した場合に、信号灯を光らせることができます。

※本機能をご利用されたい場合は、個別にお問い合わせください。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図．信号灯通知設定画面

1．通知間隔設定

信号灯への通知頻度を制御し、頻繁な通知を防ぐための機能です。前回通知から設定時間が経過後かつ新しい未通知アラートが存在する場合に、信号灯に通知されます。デフォルト値である 0 分に設定すると即時通知となります。こちらは全センサー/ポート共通の設定です。

2．通知種別点灯色

検知種別毎に、点灯させる信号灯の色を設定できます。通知しない、赤、黄、緑、青、白から選択できます。複数のアラートが同時に検知された場合は、各アラート



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

の設定に基づき、信号灯の（複数の）色が同時に点灯します。こちらはセンサー/ポート毎の設定です。

3. 登録
   登録ボタンを押下することで、通知間隔設定と検知種別点灯色の変更点を登録できます。
4. テスト点灯
   パトライトを全色点灯させて、OsecT とパトライト間の接続を確認できます。

また、信号灯機能がオンになっている場合、検知アラート「全て」画面において CSV ダウンロードボタンの左に「信号灯消灯」ボタンが出現します。本ボタンを押下することで、信号灯本体の物理的なクリアボタンだけでなく、Web ポータルから信号灯を消灯できます。

### 16.14.3. SIEM

WideAngle SIEM&MDR との連携設定に関する画面です。OsecT で取得した通信ログや検知アラートを WideAngle SIEM&MDR に集約して活用いただけます。
※本機能をご利用されたい場合は、個別にお問い合わせください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. SIEM 連携設定画面

1. SIEM 連携用認証トークン

   WideAngle SIEM&MDR 側で発行した連携のためのトークン（UUIDv4 形式）を設定できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 17. アセスメント

画面左メニューのレポート ＞ アセスメントで表示される画面で、パワーポイント(.pptx)形式のアセスメントレポートをダウンロードできます。 また、分析結果の全件CSV データとアセスメントレポートの一括ダウンロードができます。
レポートの種類は 2 種、選択中のセンサー/ポートについてのレポートおよび全てのセンサー/ポートに対してのレポートとなっております。種別のそれぞれに対して、分析結果の CSV データ一括ダウンロードもございます。
また、画面上部の期間設定にて期間を指定した場合、当該期間のみを対象としたレポートとなります。

図. アセスメント画面

1. アセスメントレポートのみのダウンロード「pptx」ボタン
   選択中のセンサー/ポートに関するパワーポイント(.pptx)形式のアセスメントレポートをダウンロードできます。レポートには以下のような項目が含まれます。これら以外の項目や詳細はレポートをダウンロードしてご確認ください。
   - 概要（集計期間、端末数、センサー/ポート名など）
   - 検出された資産の一覧
   - サポート切れの OS が搭載されている端末



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

- サービストラフィック量 トップ 10 グラフ IPv4
- サービストラフィック量 トップ 10 グラフ IPv6
- サービストラフィック量 表 IPv4
- サービストラフィック量 表 IPv6

2. 分析結果の全件 CSV データとアセスメントレポートの一括ダウンロード「zip」ボタン

   分析結果の全件 CSV データとアセスメントレポートの一括ダウンロードができます。項目については、ダウンロードした pptx ファイルのスライド上に案内がございますのでそちらをご参照ください。分析の結果、0 件の項目は csv ファイルが生成されない点にご注意ください。

3. 全センサー/ポート版アセスメントレポートのみのダウンロード「pptx」ボタン

   全てのセンサー/ポートに関するパワーポイント(.pptx)形式のアセスメントレポートをダウンロードできます。レポートの項目は 1 と基本同じです。項目ごと、センサー/ポートごとの端末数をまとめた表が追加されます。詳細はレポートをダウンロードしてご確認ください。

4. 全センサー/ポート版アセスメントレポートのみのダウンロード「pptx」ボタン

   全てのセンサー/ポートに関する分析結果の全件 CSV データとアセスメントレポートの一括ダウンロードができます。項目については、ダウンロードした pptx ファイルのスライド上に案内がございますのでそちらをご参照ください。分析の結果、0 件の項目は csv ファイルが生成されない点にご注意ください。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

# 18. システム設定

## 18.1. 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. 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。

3. 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



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。）

図. 設定変更画面（インターネットアドレス可視化、監視対象外ネットワーク設定、システム監視通知設定）

4. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

5. 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。

6. 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。

7. 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。

8. 監視対象/監視対象外ネットワーク設定

監視対象としたいネットワークアドレスや IP アドレスを設定することで、そちらの設定範囲外を「(unmonitored_address)」に集約して表示します。また、監視対象から除外したいネットワークアドレスや IP アドレスを設定することでそちらの設定範囲内を「(unmonitored_address)」に集約して表示します。監視対象外のネットワークや IP アドレスのみを含む検知アラートは画面表示・通知されません。

監視対象と監視対象外のどちらか一方のみの設定と、両方を同時に設定する 3 パターンに対応しており、同時に設定した場合は、監視対象に含まれ、監視対象外に含まれない IP アドレスレンジのみが監視対象となります。

なお、「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」が OFF の場合で監視対象設定と競合する場合、グローバル IP アドレスは「(internet_address)」への置き換えが優先されます。「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」が ON の場合または可視化対象のグローバル IP アドレスレンジが設定されている場合で、監視対象設定と競合する場合は、監視対象設定側にも可視化したいグローバル IP アドレスレンジを設定



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

してください。設定しない場合は、「(unmonitored_address)」に集約されて表示されます。

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して「適用」ボタンを押下することで、設定できます。「通知言語」「通知タイムゾーン」を変更することができます。複数のメールアドレスを登録したい場合は、「連絡先を追加」をクリックしてください(最大 5 件まで)

図. 設定変更画面（言語切り替え設定、データ削除、データ初期化）

10. 言語切り替え設定



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

表示したい言語を切り替えることができます。表示したい言語を選択し、「変更」ボタンを押下して変更します。

11. タイムゾーン設定

表示に用いるタイムゾーンを選択できます。何も設定しない場合は自動検出されたタイムゾーンで表示します。「変更」ボタンを押下して変更します。

12. ストレージ使用量

現在のストレージの使用量を確認することができます。

13. 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。

14. データ初期化

OsecT の全ての可視化・検知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。「全ての可視化・検知データを削除する」のみを選択して「削除」ボタンを押下した場合は、全ての可視化データ、検知アラート、学習データが削除されます（サブネット設定の自動更新が ON の場合はサブネット設定も削除）。また、「全ての可視化・検知データを削除する」および「システム設定を削除する」を選択して「削除」ボタンを押下した場合は、システム設定の設定変更画面にある各種設定値（データベース設定、インターネットアドレス可視化設定、システム監視通知設定、サブネット設定）も削除されます。なお、システム設定のみを削除することはできません。「物理構成関連データを削除する」を選択して「削除」ボタンを押下することで、物理構成画面からアップロードしたデータ、画像、編集したメモ欄などを含む、すべての物理構成関連データが一括削除されます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 18.2. 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。

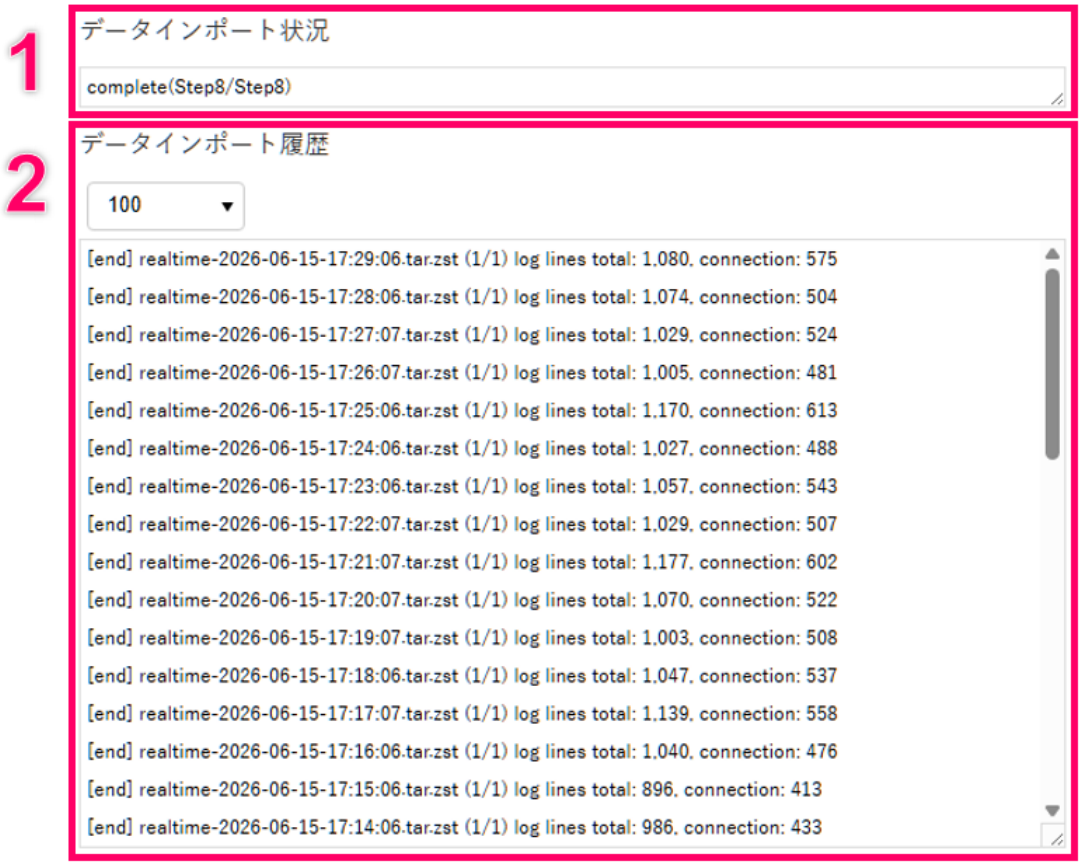



図. システムログ画面

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。log lines total はインポートされたログの総行数、connection はインポートされたログに含まれるコネクション数を表します。

| 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。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。
設定変更画面からデータ削除（期間指定）を行うなどで、端末数を削減することで、データのインポートが再開します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 18.3. センサー/ポート管理

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

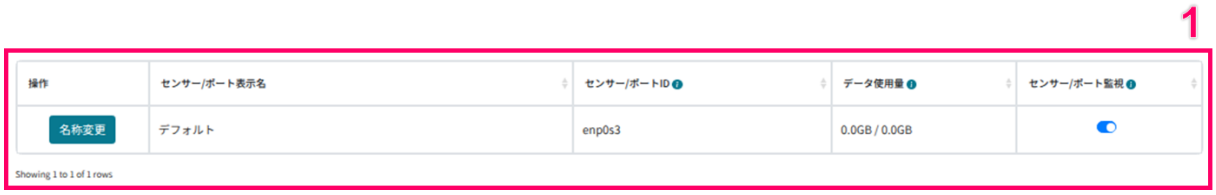
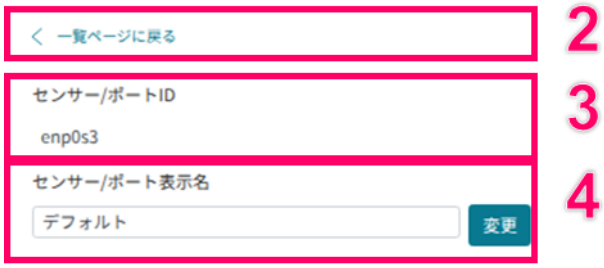



図. センサー/ポート管理画面

1. センサー/ポート一覧

| 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/ポート表示名を変更できます。 |
| センサー/ポート表示名 | 現在のセンサー/ポート表示名です。 |
| センサー/ポート ID | センサー/ポートを一意に識別する ID です。変更はできません。 |
| データ使用量 | センサー/ポートで利用している SIM の当月のデータ通信量です。<br>○ / △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/ポート監視 | ON の場合、センサー/ポート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。<br>OFF の場合、メールは送信されません。 |






© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

図. センサー/ポート表示名変更画面

2. 一覧ページに戻る
   センサー/ポート表示名変更画面から、遷移前のセンサー/ポート一覧画面に戻ることができます。
3. センサー/ポート ID
   センサー/ポートを一意に識別する ID です。変更はできません。
4. センサー/ポート表示名
   センサー/ポート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/ポート表示名を変更することができます。

センサー/ポート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（例：7.1.一覧 など）には反映されません。反映した結果を見たい場合は 14.1 設定変更で「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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 18.4. 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。

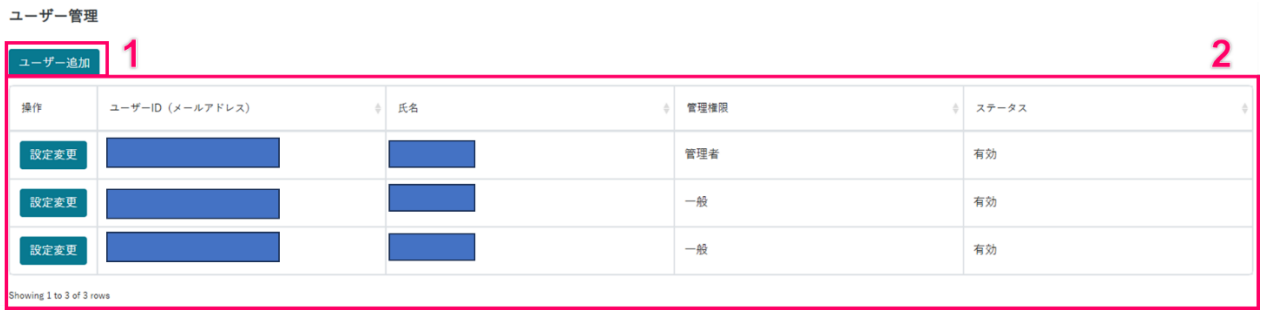



図. ユーザー管理画面

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。 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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. 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。

8. 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

9. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

【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。

[OsecT]パスワード登録のお願い

【OsecT】パスワード登録のお願い

N noreply@trustlogin.com
宛先 [redacted]

docomo business RINK IDaaS をご利用いただきありがとうございます。

·osect の管理者により docomo business RINK IDaaS にユーザー登録が行われました。

docomo business RINK IDaaS は ID 管理、アクセス管理、シングルサインオンの機能を提供する
クラウドサービスです。

以下 URL より、本サービスのパスワードと秘密の質問をご登録ください。

▼パスワード登録 URL
https://portal.trustlogin.com/users/password/auth?create_password_token=[redacted]

登録情報の確認用として、本メールは大切に保管いただきますようお願いいたします。

▼アカウント情報

1. 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。
2. パスワード、秘密の質問、秘密の答えを入力し「ログインパスワード作成」ボタンを押下します。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 18.5. サービス名管理

TCP、UDP、L2 プロトコルのサービス名を管理する画面です。

### 18.5.1. L4 プロトコル

TCP、UDP のポート番号に任意のサービス名を設定できます。

図. サービス名管理画面（プロトコル種別が L4 プロトコルの場合）

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. プロトコル種別

   L4 プロトコルを選択することで TCP、UDP のポート番号に対応するサービス名を設定できます。

3. 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。

4. 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。

5. 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。

6. リセットボタン



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

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。

7. 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。

8. サービス名一覧

| カラム名 | 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。 |

図. サービス名変更画面（プロトコル種別が L4 プロトコルの場合）

9. 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。

10. ポート番号

ポート番号を表示します。（変更はできません。）

11. 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。

12. 変更ボタン

「変更」ボタンを押下することで、サービス名を変更できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

### 18.5.2. L2 プロトコル

L2 プロトコルに任意のサービス名を設定できます。

図．サービス名管理画面（プロトコル種別が L2 プロトコルの場合）

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. プロトコル種別

   L2 プロトコルを選択することで L2 プロトコルに対応するサービス名を設定できます。

3. 種別

   プルダウンで選択した Ethernet フレームの形式で絞り込みを設定できます。

4. キー（部分一致検索）

   EtherType など L2 プロトコルの識別情報で絞り込みを設定できます。キーは全て 16 進数です。

5. 表示名（部分一致検索）

   L2 プロトコルについているサービス名で絞り込みを設定できます。

6. 参照元

   参照している L2 プロトコル辞書で絞り込みを設定できます。

   デフォルトの表示名が設定されているサービスは「システム辞書」を選択することで絞り込みを設定できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

ユーザーが表示名を変更したサービスは「ユーザー定義」を選択することで絞り込みを設定できます。

L2 プロトコル辞書になく、ユーザーによる表示名変更も行われていないプロトコルは「なし」を選択することで絞り込みを設定できます。

7. リセットボタン

プロトコル種別、種別、キー（部分一致検索）、表示名（部分一致検索）、参照元で指定した選択をリセットできます。

8. 適用ボタン

プロトコル種別、種別、キー（部分一致検索）、表示名（部分一致検索）、参照元で指定した選択を適用した画面を表示できます。

9. サービス名一覧

| カラム名 | 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。 |
| 種別 | Ethernet フレームの形式です。 |
| キー | L2 プロトコルを識別するための情報です。 |
| 表示名 | サービス名です。 |
| 参照元 | サービス名の参照元です。 |

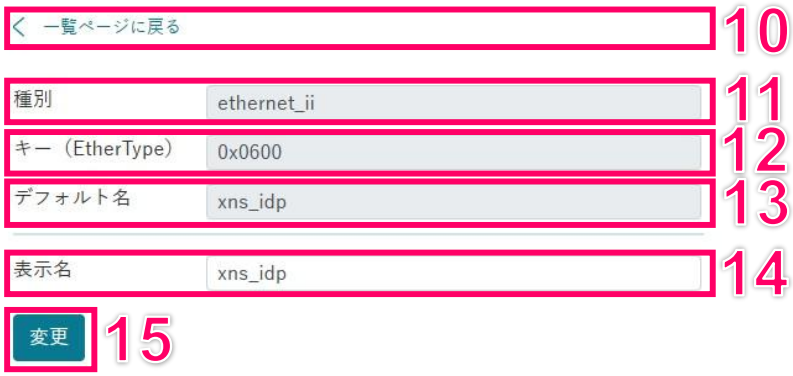



図. サービス名変更画面（プロトコル種別が L2 プロトコルの場合）

10. 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。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

11. 種別

Ethernet フレームを表示します。（変更はできません。）

12. キー

L2 プロトコルを識別するための情報です。（変更は出来ません。）

13. デフォルト名

デフォルトのサービス名です。（変更は出来ません。）

14. 表示名

サービス名を入力・設定します。

15. 変更ボタン

「変更」ボタンを押下することで、サービス名を変更できます。



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

## 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。<br>2.12 サービス名の表記について 追加。<br>7.1 一覧にセンサー表示名に関する注意書きを追加。<br>18.3 センサー管理 を追加。<br>16.4 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<br>可視化機能に OT プロトコルを追加<br>検知機能に IP 統計・OT 振舞（IP, イーサネット）を追加<br>学習・検知設定の簡素化<br>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<br>「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<br>「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<br>「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<br>「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<br>「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<br>「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<br>「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<br>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<br>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）<br>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 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | | |
|---|---|---|
| | ○○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）<br>図の差し替え<br>　6.1.端末（◎：オススメ機能）<br>　11.8. OT 振舞（IP）<br>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<br>　11.6. IP 流量 | |
| 3.00 | データ連携機能の追加に伴う説明の変更と図の差し替え<br>「10. 台帳」の説明を追記 | 2024 年 9 月 5 日 |
| 3.10 | メニュー変更に伴う図の修正<br>画面デザイン変更に伴う図の修正<br>トラフィック画面のネットワークアドレス検索機能追加に伴う説明の修正<br>台帳に編集・一括削除の説明を追加<br>検知機能の新規端末→接続端末の名称変更に伴う説明の修正<br>学習・検知設定に AMF-SEC 連携の追加<br>アセスメントの追加<br>システム設定に監視対象外ネットワーク設定の説明を追加 | 2024 年 12 月 25 日 |
| 3.20 | 「タブ」および「期間設定」に関する説明を追加<br>ネットワークマップに、リンク上へのサービス名表示と通信情報表示機能の説明を追加<br>トラフィックに、CSV ダウンロード機能の説明を追加<br>システム設定に、言語切り替え設定を追加<br>システム設定の「長期保存用データベースを参照する」設定を削除。（期間設定にて同等の機能を利用可） | 2025 年 3 月 28 日 |
| 4.03 | 「8. ネットワークマップ」<br>　ラベル表示選択ボタンに、ホスト名をノード傍に表示する機能を追加<br>　詳細表示ボタンとして、ノードやリンクの詳細情報を表示する際の操作切り替え機能を追加<br>　ノード移動ボタンを追加<br>ビルトイン検知機能追加に伴い、「13. 検知アラート>13.10. ビルトイン」、「14.学習・検知設定>14.11. ビルトイン」の説明を追加<br>「15. アセスメント」に、全センサーのレポートをマージして出力するボタンの説明を追加 | 2025 年 10 月 31 日 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | | |
|---|---|---|
| | 「16.1.設定変更」に、ストレージ使用量表示機能の説明を追加 | |
| 4.10 | センサー→センサー/ポートへの表記変更に伴う修正<br>「14. 学習・検知設定」に「14.14. 連携」を追加 | 2026 年 1 月 16 日 |
| 4.20 | 「1. はじめに」ログイン手順を新認証システム向けに修正<br>「6. ダッシュボード」全端末数（直近）の説明を追加<br>「7.1. 一覧」フィルタの説明を追加<br>「13.2. 接続端末」消滅端末検知オプションの説明を追加<br>「13.9. シグネチャー」シグネチャー解説ページの説明を追加<br>「14.3. 接続端末」消滅検知列の説明を追加<br>「14.12. 全般」消滅端末検知トグルの説明を追加<br>「14.13. 全般（アドバンスモード）」消滅端末検知トグルの説明を追加<br>「14.14.2. 信号灯」パトライト社の信号灯との連携機能の説明を追加<br>「16.4. ユーザー管理」新認証システム向けに修正 | 2026 年 3 月 23 日 |
| 4.30 | 「2.7. 物理構成」を追加<br>「3. 画面左メニュー」 図を最新化<br>「7.4. ベンダーマトリクス」、「7.5. OS マトリクス」、「7.6. 役割マトリクス」に、フィルタ機能（リスト）の説明を追加<br>「8.11. 端末」 フィルタ適用前後の役割に関する計算方法の変更点の説明を追加<br>「13. 物理構成」を追加<br>「15.10. シグネチャー」 カスタムシグネチャー設定機能の説明を追加<br>「15.12. 全般」、「15.13. 全般（アドバンスモード）」に、適用範囲と宛先メールアドレスごとの言語設定の説明を追加<br>「15.14.1. AMF-SEC」 宛先メールアドレスごとの言語設定の説明を追加<br>「15.14.3. SIEM」を追加<br>「17.1 設定変更」宛先メールアドレスごとの言語設定と物理構成関連データ削除の説明を追加<br>「17.2. システムログ」 コネクション数の説明を追加 | 2026 年 6 月 30 日 |
| 4.40 | 「2.8. 脆弱性」を追加<br>「3. 画面左メニュー」 図を最新化 | 2026 年 9 月 30 日 |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

| | | |
|---|---|---|
| | 「7. 端末 7.1. 一覧」 接続サービスの説明に L2 プロトコルの場合を追加<br>「8. ネットワークマップ 8.1. 端末」 ブロードキャスト表示選択ボタン・マルチキャスト表示選択ボタンの説明を追加<br>「13. 物理構成」 ノード種別の追加に伴う図の修正、背景画像登録機能・機器/リンク詳細情報の説明を修正<br>「14. 脆弱性」を追加<br>「15.9. シグネチャー」 DL ボタンの説明を追加<br>「16.3. 接続端末」 MAC アドレスのみでの検知設定の説明を追加<br>「16.12. 全般」、「16.13. 全般（アドバンスモード）」 通知設定にタイムゾーンの説明を追加<br>「18.1 設定変更」 監視対象/監視対象外ネットワーク設定の説明を追加、タイムゾーン設定の説明を追加<br>「18.4. ユーザー管理」 ステータス変更機能廃止に伴う修正<br>「18.5. サービス名管理」 L2 プロトコルに関するサービス名変更機能の追加に伴い、「18.5.1. L4 プロトコル」、「18.5.2. L2 プロトコル」への構成変更・説明追加 | |



© NTT DOCOMO BUSINESS, Inc. All Rights Reserved.