「ギガらくVPN」「ギガらくスイッチ」ダッシュボードのご利用ガイド

・ダッシュボードとは？
お客様の店舗やオフィスの通信ご利用状況を収集し、一覧表示したものです。マーケティングやIT管理にご活用ください。

事前準備

1-1. ダッシュボードのパスワード設定
1-2. ダッシュボードの日本語表記設定

利用方法

2. 基本画面構成
3. ネットワーク全体
4. セキュリティ＆SD-WAN
5. スイッチ
6. ワイヤレス

高度な利用

7. トラフィック分析
8. 故障診断
9. 無線診断
10. イベントログ

1-1. ダッシュボードのパスワード設定（1/3）

- まずはじめに連絡先確認メールの承認を実施します。
  ※承認完了後にパスワード設定用メールが送付されますので、忘れずに実施ください。

1．ご利用開始日前に、設定申込書に記載いただいたお客様メールアドレス宛てに以下のメールが届きます。本文中のURL(https://から始まる文字列)をクリックします。

差出人：ネットワーク機器サポートセンタ <gigaraku-sdx-support@east.ntt.co.jp>
件名：【重要】ＮＴＴ東日本ネットワーク機器サポートセンタからの連絡先の確認

こちらは、ＮＴＴ東日本ギガらくVPN・ギガらくスイッチのネットワーク機器サポートセンタです。
この度は、弊社サービスにご契約いただき、誠にありがとうございます。
当ネットワーク機器サポートセンタでは、ギガらくVPNおよびギガらくスイッチに関する電話サポートに加え、重要なご連絡を本メールアドレス宛にお送りさせていただきます。
以下のURLをクリックし、メールアドレスの承認処理をお願い致します。

https://amw.ntt-east.co.jp/fasthelp5/EmailApproval.html?key=T...

...

2．URLをクリックすると、下図の様なメッセージが表示されます。
記載内容を確認し、誤りがなければ**「承認」**ボタンをクリックしてください。

メールアドレス承認
aaa@bbb.com

今後サポートのご連絡先アドレスが上記で宜しければ
承認ボタンを押してください。

承認

以上で連絡先確認メールの承認は終了です。

1-1. ダッシュボードのパスワード設定 (2/3)

- ダッシュボードを利用するためのパスワードを設定します

1. 利用開始日の前日（土日祝日を除く）までに、差出人「Cisco Meraki」より、以下のメールが届きます。
本文内の「Choose your password here」をクリックします。

⚠ **メールは、タイトル・本文ともに英語の文章です。**
迷惑メールと思わず、必ず確認、クリックをしてください。

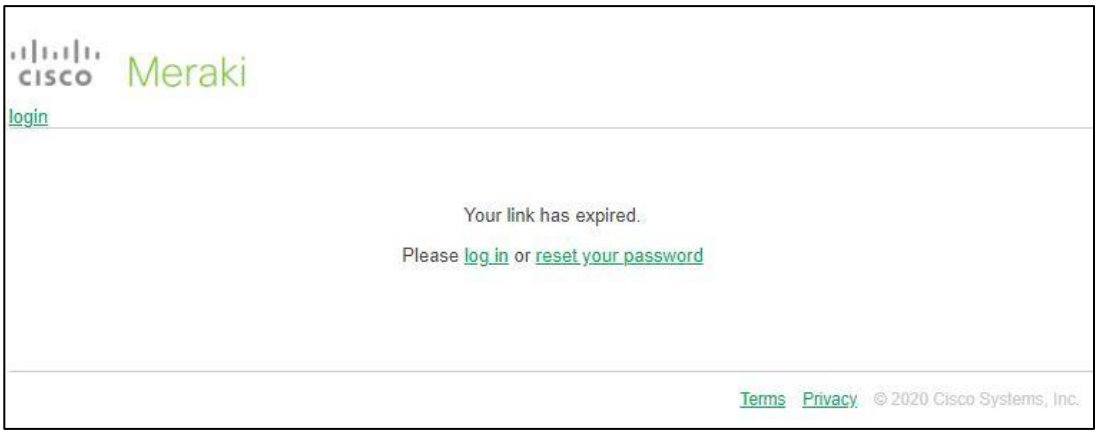
差出人：Cisco Meraki - No Reply noreply@meraki.com
件名：Welcome to Cisco Meraki

Hi ○○! You have been signed up for a Cisco Meraki account with administrator privileges to a network in the organization "Gigaraku Promotion." Your login email is

xxxx.xxxx@xxxx.co.jp.
Choose your password here.

Thanks,
Cisco Mereki

? Cisco Meraki とは…
ギガらくＶＰＮ装置およびダッシュボードサービスの提供会社です

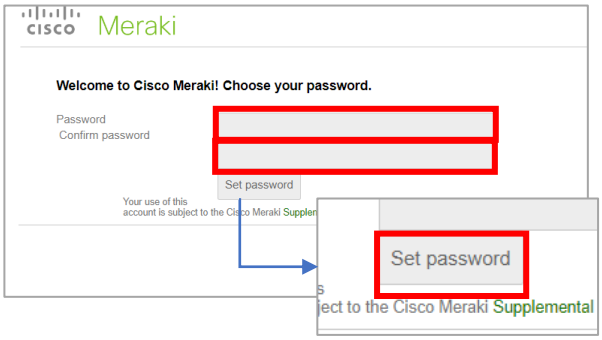


※Choose your password here をクリック後、上記のような画面が表示される場合、
下記サポートセンタまでご連絡願います。

ネットワーク機器サポートセンタ (年中無休 9：00-21:00)
TEL：0120-051-003　　MAIL：gigaraku-sdx-support@east.ntt.co.jp

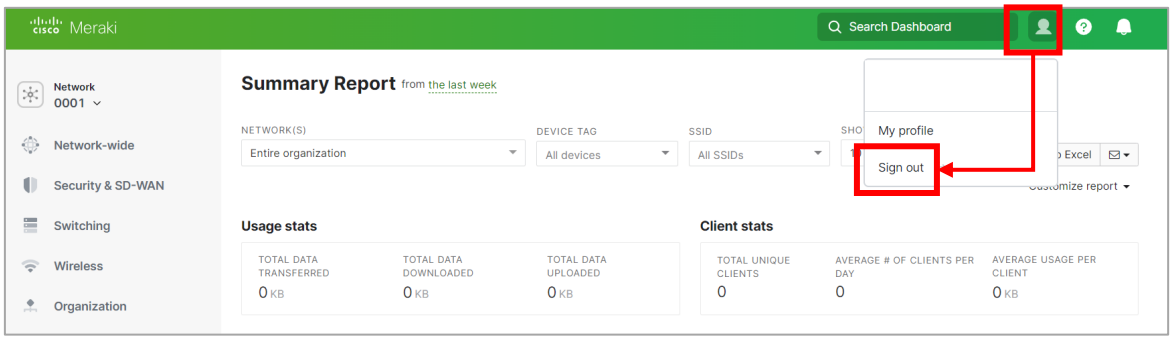
1-1. ダッシュボードのパスワード設定 (3/3)

2. パスワード設定画面が表示されるので、任意のパスワードを入力します。
パスワード入力後、「Set password」ボタンをクリックします。

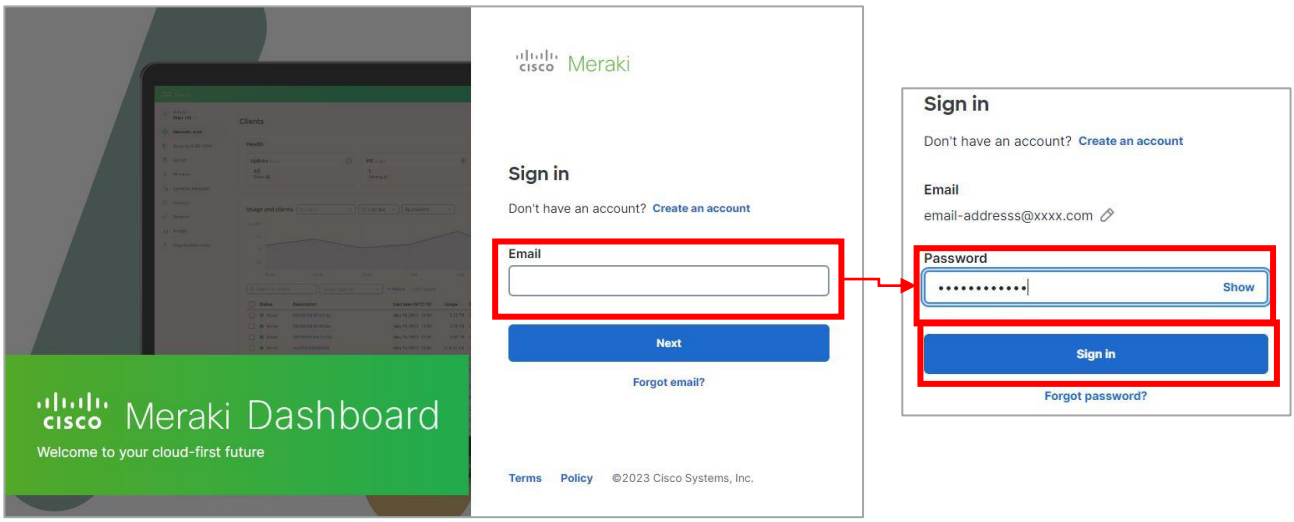


※パスワードは大文字、
小文字、数字、および記号のうち3種類以上を使用し、
8文字以上とする必要があります。

3. 画面右上の アイコンをクリック後、「sign out」をクリックするとログアウトします。



4. 以下のログイン画面が表示されたことを確認し、Email欄にダッシュボードアカウント登録したメールアドレスを入力後、「Next」をクリック。Password欄にお客様が設定したパスワード入力後に「Sign in」をクリックし、ダッシュボードにアクセスできるか確認します。



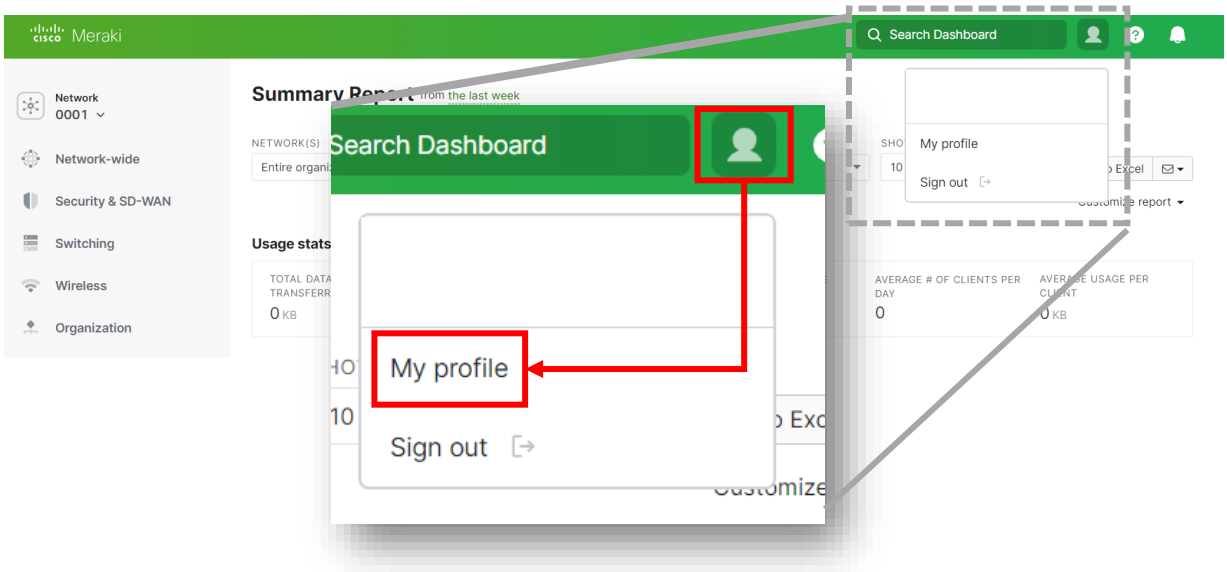
5. 次回以降、ブラウザから次のURL(https://dashboard.meraki.com)にアクセスいただくことで上記のログイン画面が表示されます。
※ログイン画面をお気に入り登録しておくことをお薦めいたします。

これで事前準備は完了です！

1-2. ダッシュボードの日本語表記設定

- ダッシュボードはデフォルトでは英語表記ですが、日本語表記に変更します。
  これ以降のページは日本語で説明します。

1. ダッシュボードにログインし、画面右上の  アイコンをクリックします。
2. 次に「My profile」をクリックします。



3. 「Dashboard Language」の「Preferred language」横のリストをクリックし、「日本語」を選択、「Save」をしていただくことでダッシュボードが日本語化されます。

これでダッシュボードの日本語化設定は完了です！

利用方法

利用方法

2. 基本画面構成
3. ネットワーク全体
4. セキュリティ&SD-WAN
5. スイッチ
6. ワイヤレス

機器が正常に稼動しているか、通信が正常に行えているかを確認するための基本的な確認方法を記載します。

また、サポートセンターでも支援していますので、サポートセンターまでお問い合わせいただければ、オペレータにて稼動状態を確認することも可能です。

なお、お客様のアカウントは読み取り専用のアカウントとなります。設定については設定値を確認することはできますが、設定を変更することはできません。設定変更が必要な場合はサポートセンターまでご相談ください。

2-1. 基本画面構成

- ダッシュボードの基本画面は二つのエリアから構成されています。

1. 左メニューから（ ① ）から閲覧したい項目のカテゴリを選択、クリックすることで、右側の詳細表示エリア（ ② ）に各情報が表示されます。
2. カテゴリをマウスでポイントするとさらに細かいカテゴリが表示されます。

各カテゴリの詳細はそれぞれのページを参照ください。

カテゴリ	内容	参照ページ
ネットワーク全体	拠点(ネットワーク)に関する情報の表示	p7 ～ p11
セキュリティ＆SD-WAN	**VPN装置**に関する情報の表示	p12 ～ p17
スイッチ	**スイッチ**に関する情報の表示	p18 ～ p21
ワイヤレス	**Wi-Fi**に関する情報の表示	p22 ～ p24

3-1. ネットワーク全体

- ネットワーク全体で確認できる主な情報を確認する

➢ 「ネットワーク全体」にカーソルを合わせると、以下画像のように「監視」、「設定」メニューが表示されます。「監視」は主に通信量など統計情報の閲覧、「設定」は各設定の閲覧が可能です。

ネットワーク状況の確認をする際、主に以下のカテゴリから確認を行います。

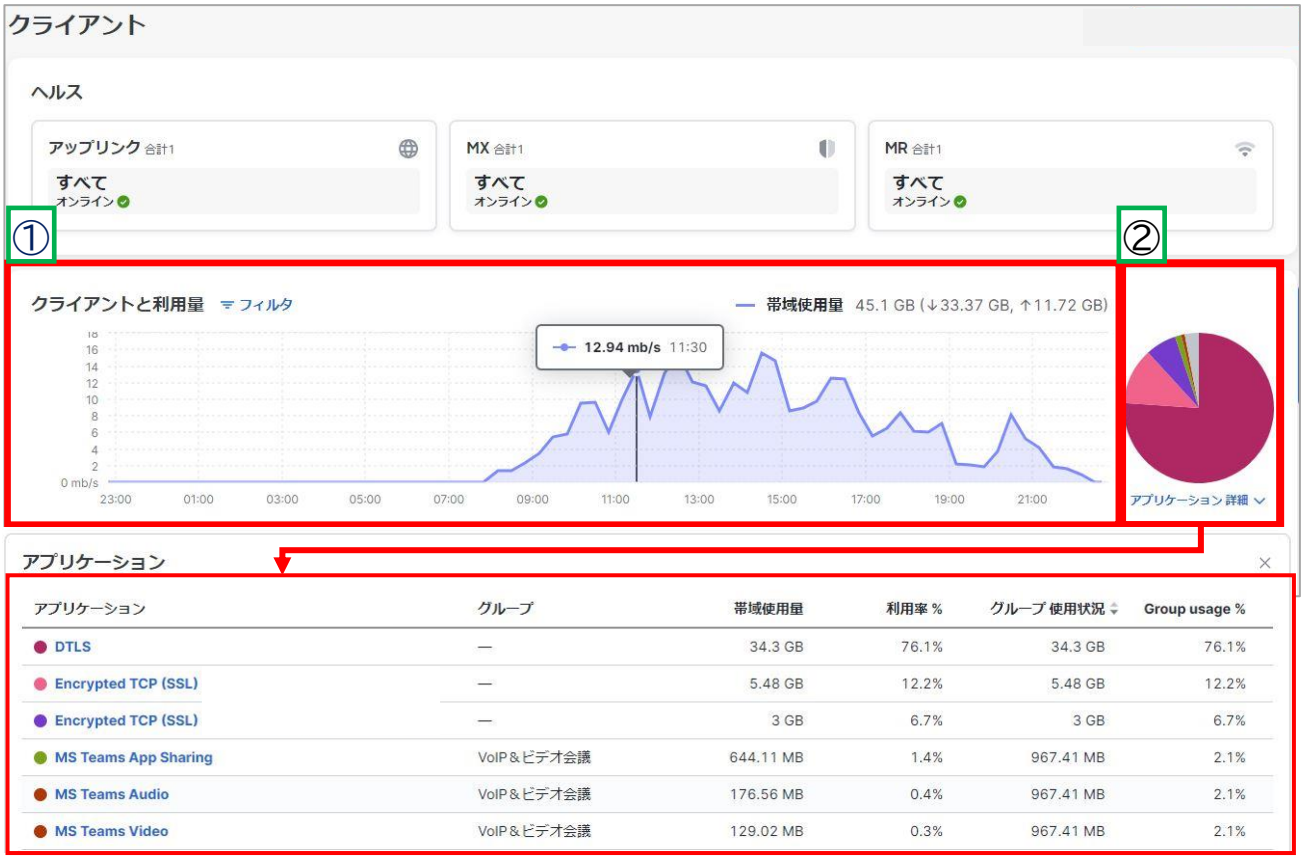
カテゴリ	内容
クライアント	• ネットワーク接続したクライアントに関する情報 • クライアントのIPアドレスやMACアドレス • クライアントの通信量やアプリケーション別通信量
トラフィック分析	• ネットワーク全体のクライアント接続数や通信量
トポロジー(※)	• ネットワーク機器の接続状況の可視化 ※ギガらくスイッチを導入いただいた場合に表示されます。
イベントログ	• ネットワーク機器で発生したイベントの表示
サマリーレポート	• ネットワークの稼働レポートを表示

3-2. ネットワーク全体　－クライアント－

- クライアントの通信利用量や通信の内訳を確認する。

① 時間帯ごとのネットワーク利用量が確認できます。「▼フィルタ」で表示期間や抽出対象を変更することが可能です。日々の通信量の確認や「ネットワークが遅い」と感じた場合に通常より多くの通信が発生していないか等、ネットワークの状況を確認する際にご活用いただけます。

② 通信の内訳が表示されます。円グラフの下部「アプリケーション詳細」をクリックすることで、どのアプリケーションの通信が多く発生しているか詳細が確認でき、通信内容の分析をサポートします。



アプリケーション	グループ	帯域使用量	利用率 %	グループ使用状況	Group usage %
DTLS	—	34.3 GB	76.1%	34.3 GB	76.1%
Encrypted TCP (SSL)	—	5.48 GB	12.2%	5.48 GB	12.2%
Encrypted TCP (SSL)	—	3 GB	6.7%	3 GB	6.7%
MS Teams App Sharing	VoIP＆ビデオ会議	644.11 MB	1.4%	967.41 MB	2.1%
MS Teams Audio	VoIP＆ビデオ会議	176.56 MB	0.4%	967.41 MB	2.1%
MS Teams Video	VoIP＆ビデオ会議	129.02 MB	0.3%	967.41 MB	2.1%

- ネットワークに接続しているクライアント（パソコンやモバイル）情報を確認する

③ ネットワークに接続している端末の一覧が表示されます。
状態（オンライン状況と接続形式）、説明（クライアント名）、帯域使用量（通信量）、端末のOS、MACアドレス、IPアドレスなど一覧で確認できます。端末数が多い場合、検索機能で対象を絞ることも可能です。

無線端末：ワイヤレス
有線端末：有線
リモートアクセス端末：クライアントVPN
左のアイコンは緑がオンライン、灰がオフラインを示します。

3-3. ネットワーク全体　–トポロジー–

- 機器の構成（どの様につないであるか）を確認する
  ※トポロジー表示はギガらくスイッチが必要になります。

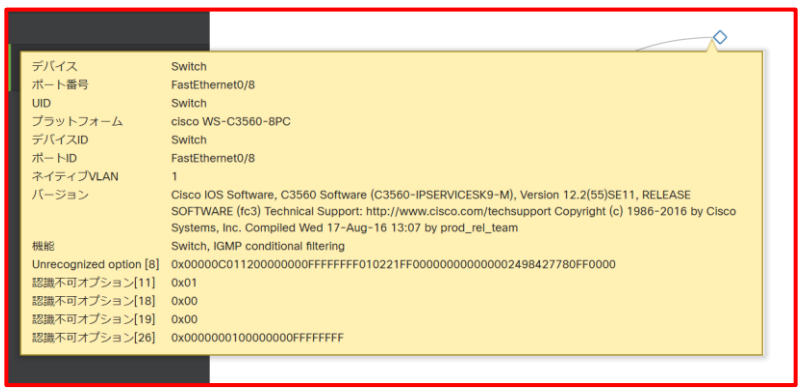
➢ トポロジーでは拠点に設置しているネットワーク機器の接続構成を確認できます。
遠隔地で機器が故障した場合やネットワーク機器を誤ったポートに接続していないか等の確認などに便利です。

機器間の線をポイントするとどのポートに接続しているか確認できます。

凡例

VPN装置：
スイッチ：
Wi-Fi装置：
その他機器：

CDP/LLDP対応機器をポイントすると機器の情報を確認することができます。



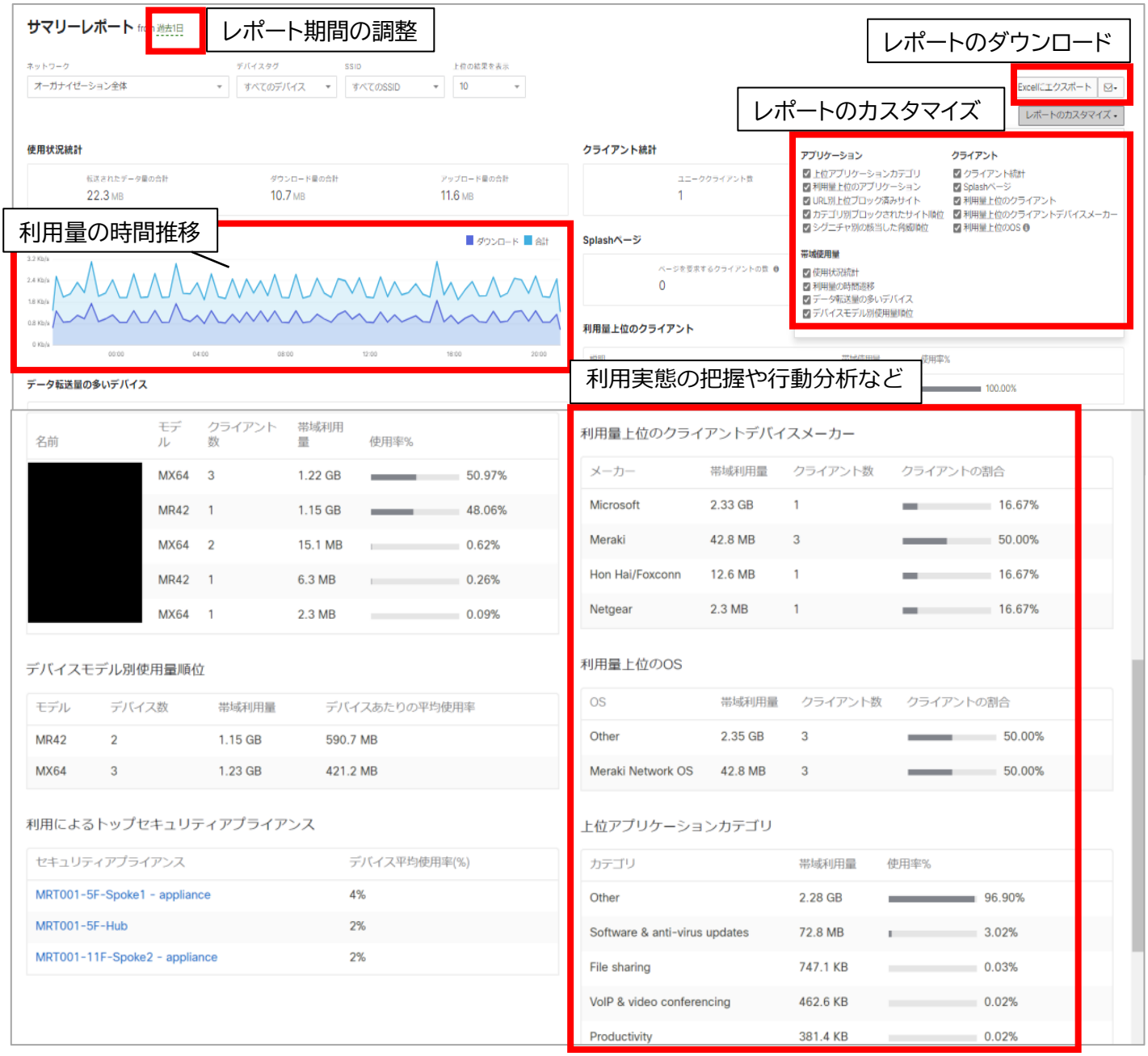
3-4. ネットワーク全体　－サマリーレポート－

- ネットワークの各通信レポートを表示・ダウンロードする。

➢ サマリーレポートでは、指定期間に発生した通信量やクライアント数の統計や通信量が多かったクライアントTOP3等、ランキング形式で確認ができます。

➢ 表示しているレポートはExcelファイルでダウンロードすることが可能です。

➢ 不要な項目は「レポートのカスタマイズ」で非表示にすることも可能です。



4-1. セキュリティ&SD-WAN

- VPN装置の各情報を確認する。

➢ 「セキュリティ&SD-WAN」メニューではVPN装置のステータスやVPNの状況、機器の設定状況が確認できます。

➢ 主に以下の「監視」項目でVPNの状態が確認できます。

カテゴリ	内容
アプライアンス	• VPN装置のステータスの確認 • VPN装置の通信量の確認 • グローバルIPアドレスの確認 • DHCP機能のIPアドレス割り当て状況を確認する
VPNの状況(※)	• 各拠点とのVPN通信量の確認 • 拠点間VPNのVPN接続状況の確認 ※拠点間VPN機能を利用している場合に表示されるメニューです。
ルートテーブル	・VPN機器のルートテーブルを表示します。

4-2. セキュリティ&SD-WAN －アプライアンス－

- VPN装置の稼動状態を確認する
- VPN装置の通信量を確認する

① VPN装置名 横の●は、現在のステータスを表します。

緑：オンライン 赤：オフライン 橙：オンラインだが機器に何らかの問題が発生している

② VPN装置のポート状態が表示されます。VPN機器のポートに他の機器が接続されたことを検知している場合は緑色で表示されます。

③ 指定期間内でVPN装置のステータス推移が表示されます。（過去1か月間まで確認可）
緑：オンライン 赤：オフライン 橙：オンラインだが機器に何らかの問題が発生していたことを示します。(※)

④ VPN装置の通信量が表示されます。

(※) 機器のオンライン状況はネットワーク機器が管理クラウドと通信できているかで機器状態を判断しております。そのため、インターネットには接続できているが、管理クラウドとの通信に問題が発生した場合（クラウドサーバーの障害、システムメンテナンス、回線障害など）、ネットワーク機器が正常に稼動していても、異常と表示されることがあります。

4-2. セキュリティ&SD-WAN －機器のステータスー

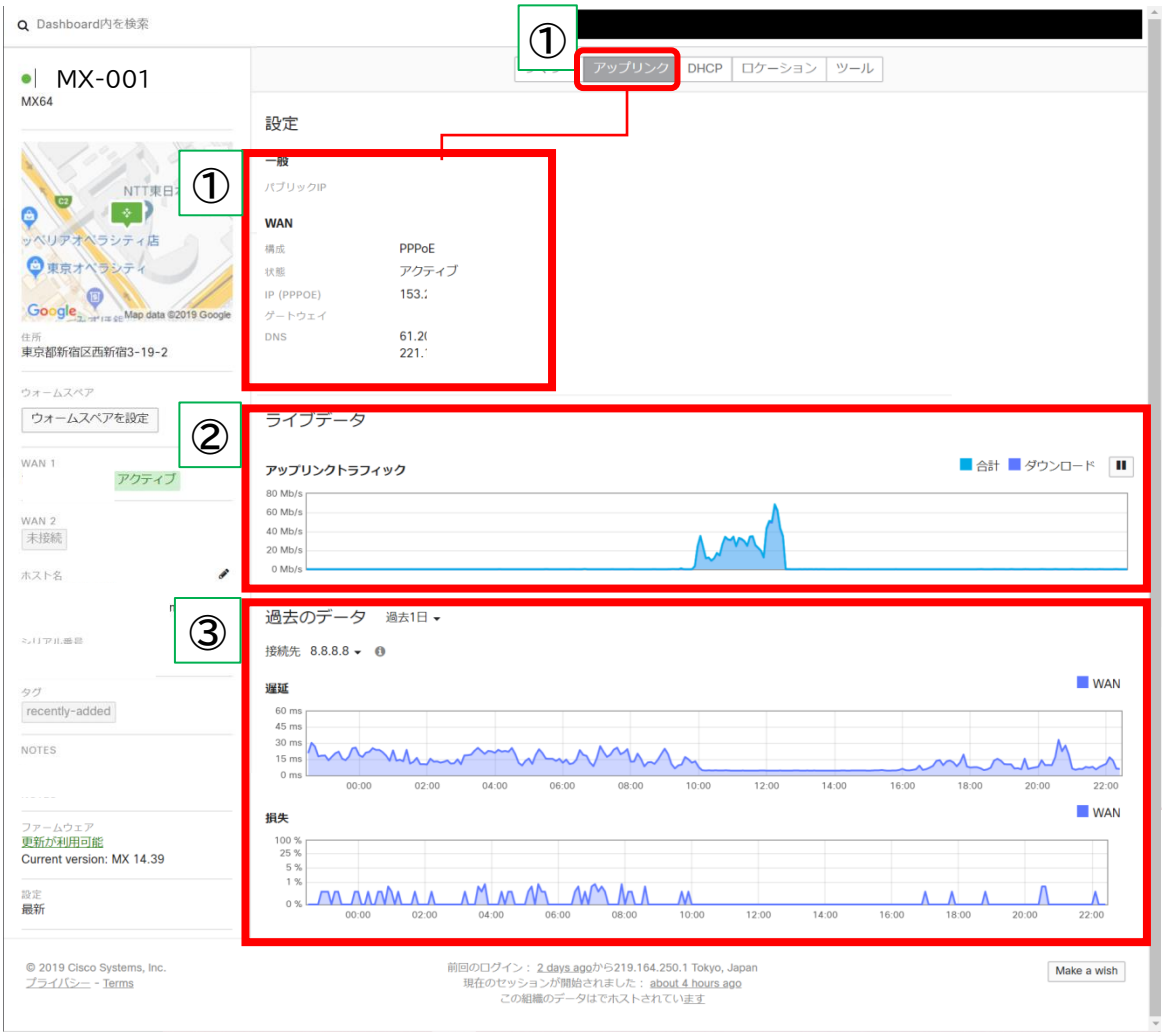
- インターネット回線の接続状態を確認する

① 画面上部の「アップリンク」からWANの設定状態やWAN側のIPアドレス等が確認できます。

② アップリンクを通るトラフィックがリアルタイムに表示されます。

③ WANポートに流れる通信の状態が表示されます。過去〇〇の▼ボタンをクリックすると、表示期間や対象を変更できます。

遅延や損失率※が高い状態が断続的に続く場合、利用回線の混雑や機器スペック以上のトラフィック発生等、何らかの障害が疑われます（一時的なトラフィックの上昇はこの限りではありません。）



4-2. セキュリティ&SD-WAN －機器のステータスー

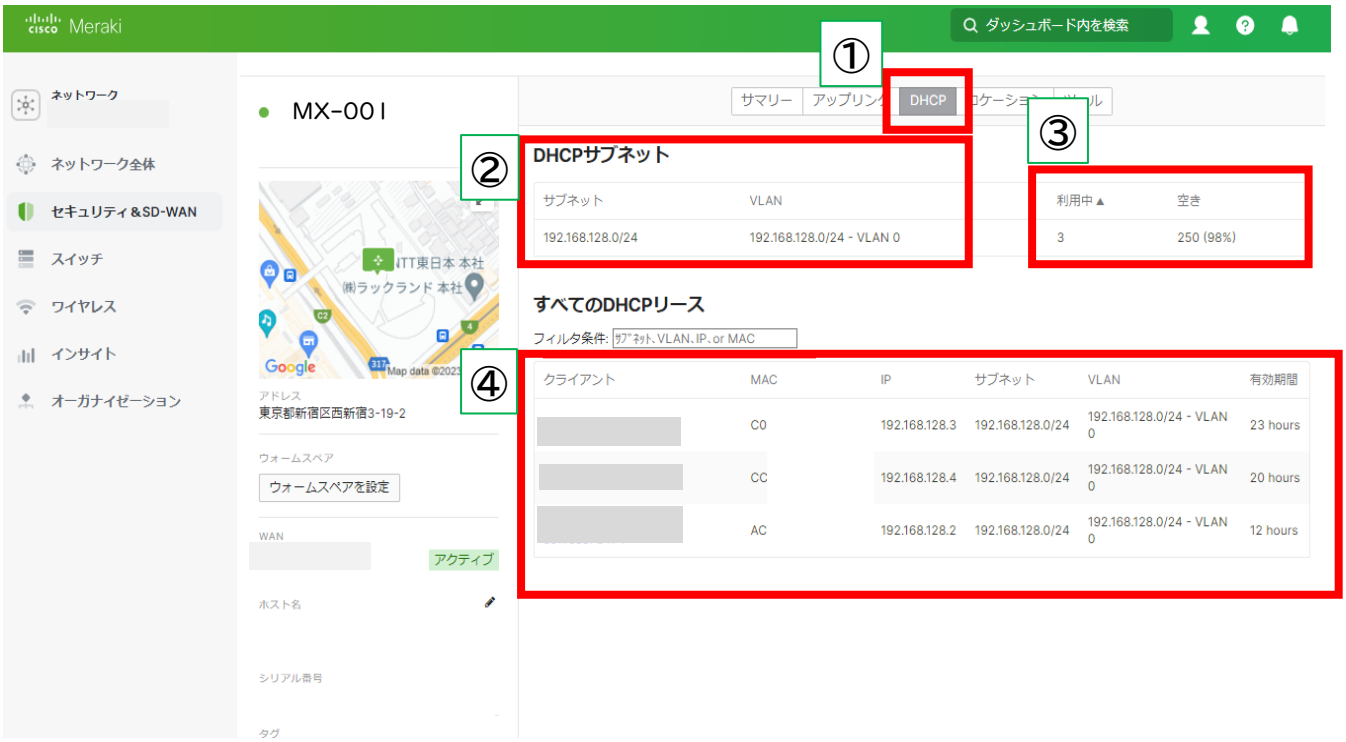
- DHCP機能で割り当てているIPアドレスのリース状況を確認する

① 画面上部の「DHCP」をクリックするとDHCPの情報が確認できます。

② 現在DHCPで払出しているサブネット、レンジの情報が表示されます。

③ リースしているIPアドレス数、空きアドレス数が表示されます。
IPアドレスが枯渇していないかの確認や、DHCP払出数の検討などにご利用いただけます。

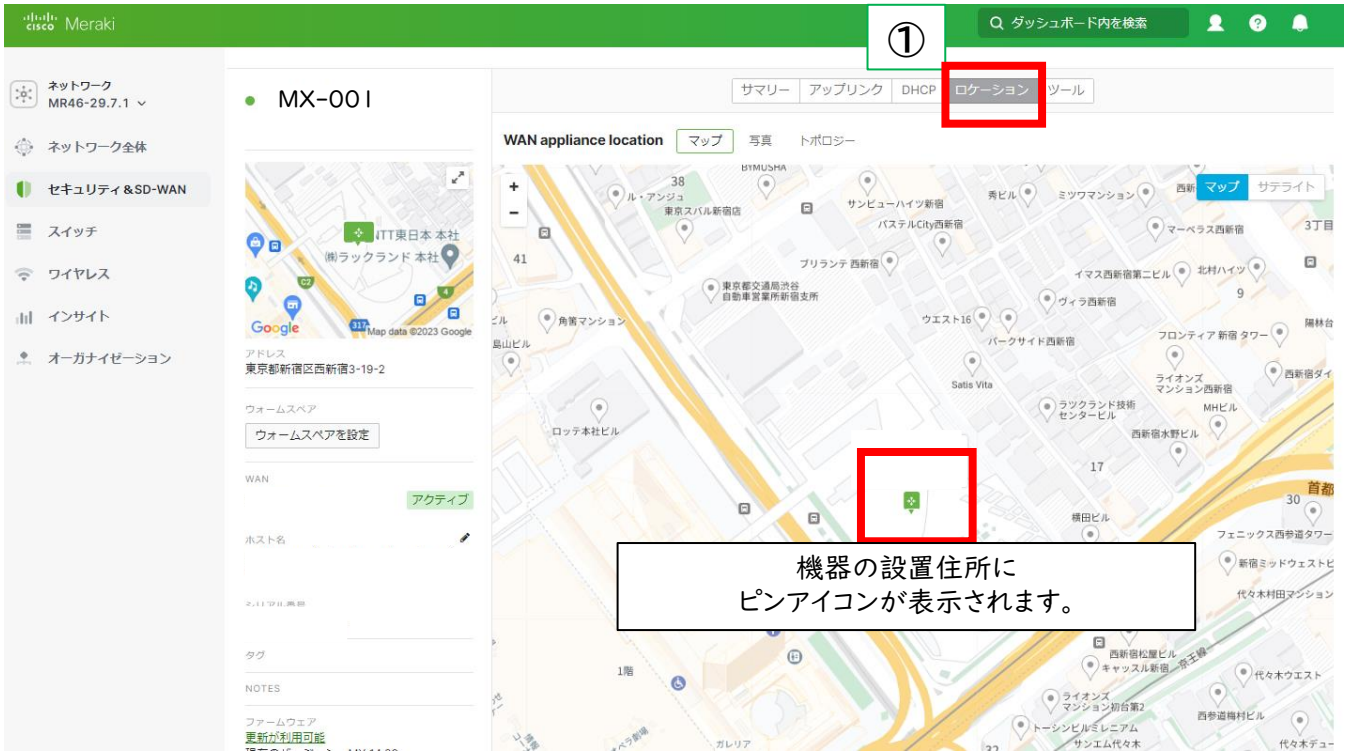
④ IPアドレスを割り当てたパソコンの詳細情報が表示されます。
フィルタ条件にキーワードを入力することで対象を絞り込むことができます。



4-2. セキュリティ&SD-WAN －機器のステータスー

- 機器の設置場所の確認

① 画面上部の「ロケーション」をクリックすると、マップ上でVPN機器の設置場所を確認できます。

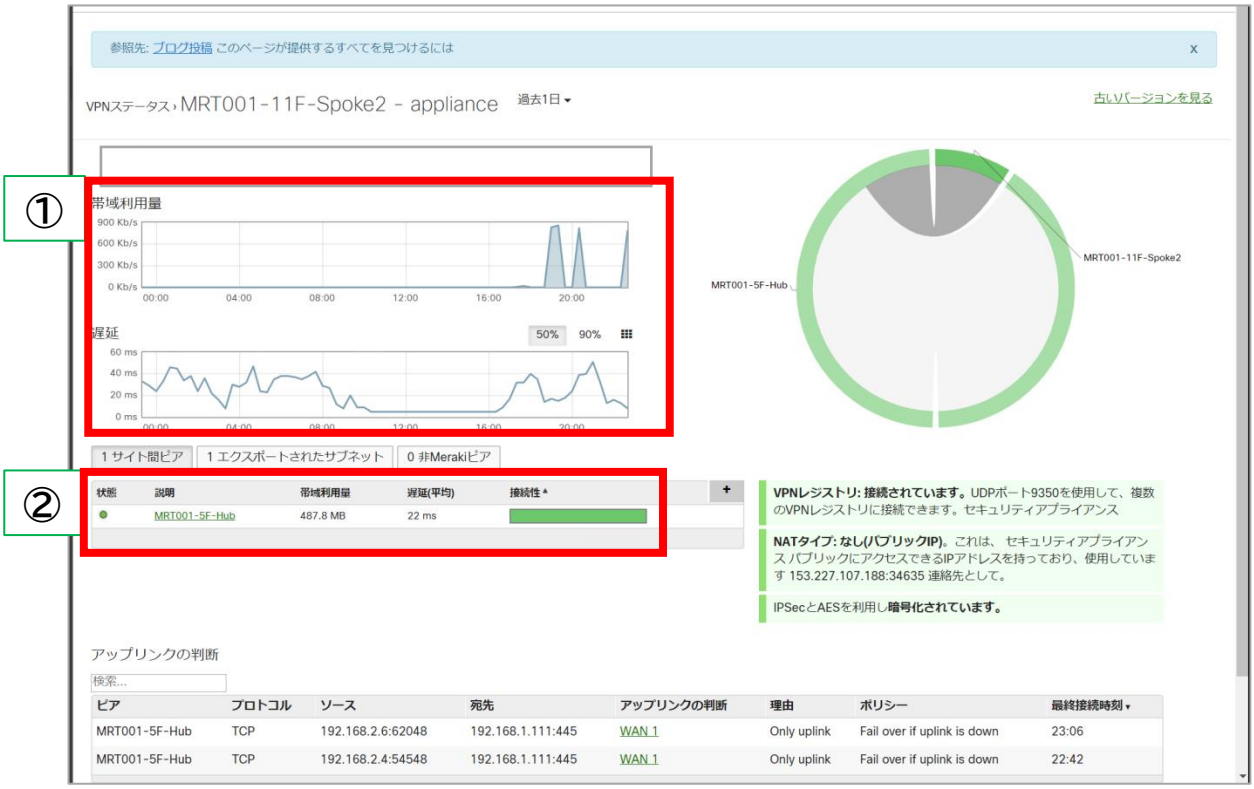


4-3. セキュリティ&SD-WAN －VPNの状況－

- 各拠点とのVPN通信量を確認する
- 接続先の拠点が稼動しているか確認する

① サイト間VPNの帯域利用量、遅延が表示されます。
帯域利用量や遅延時間が高い状態が続く場合、回線契約の見直しや帯域制御などの対応が必要な場合があります。

② サイト間VPNで接続されている拠点のVPN装置の稼動状態が表示されます。
正常は緑色。異常が発生すると赤色、または黄色になります。(※)



(※) 機器のオンライン状況はネットワーク機器が管理クラウドと通信できているかで機器状態を判断しております。そのため、インターネットには接続できているが、管理クラウドとの通信に問題が発生した場合（クラウドサーバーの障害、システムメンテナンス、回線障害など）、ネットワーク機器が正常に稼動していても、異常と表示されることがあります。

5-1. スイッチ

- スイッチ装置のステータスや通信状況を確認する

➢ 「スイッチ」メニューではスイッチ装置のステータスや各ポートの状況、通信状況や各種設定状況が確認できます。

➢ 主に以下の「監視」項目でVPNの状態が確認できます。

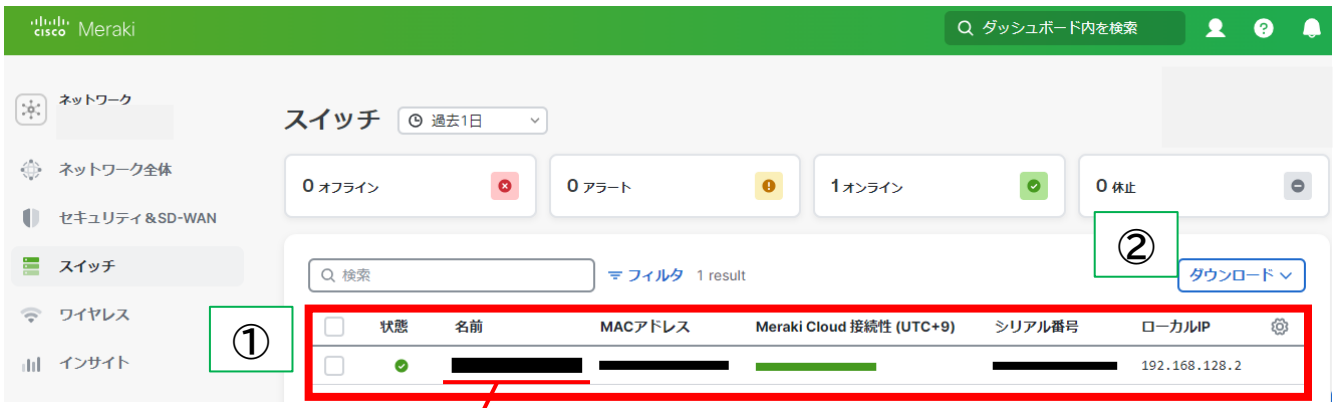
カテゴリ	内容
スイッチ	• スイッチ装置のステータス確認 • 各スイッチ装置の状態、通信状況 • 各ポートの状態、接続機器を確認する • 通信診断ツールで通信不調の原因を調査する
スイッチポート	• 各スイッチポートの設定・ステータス確認

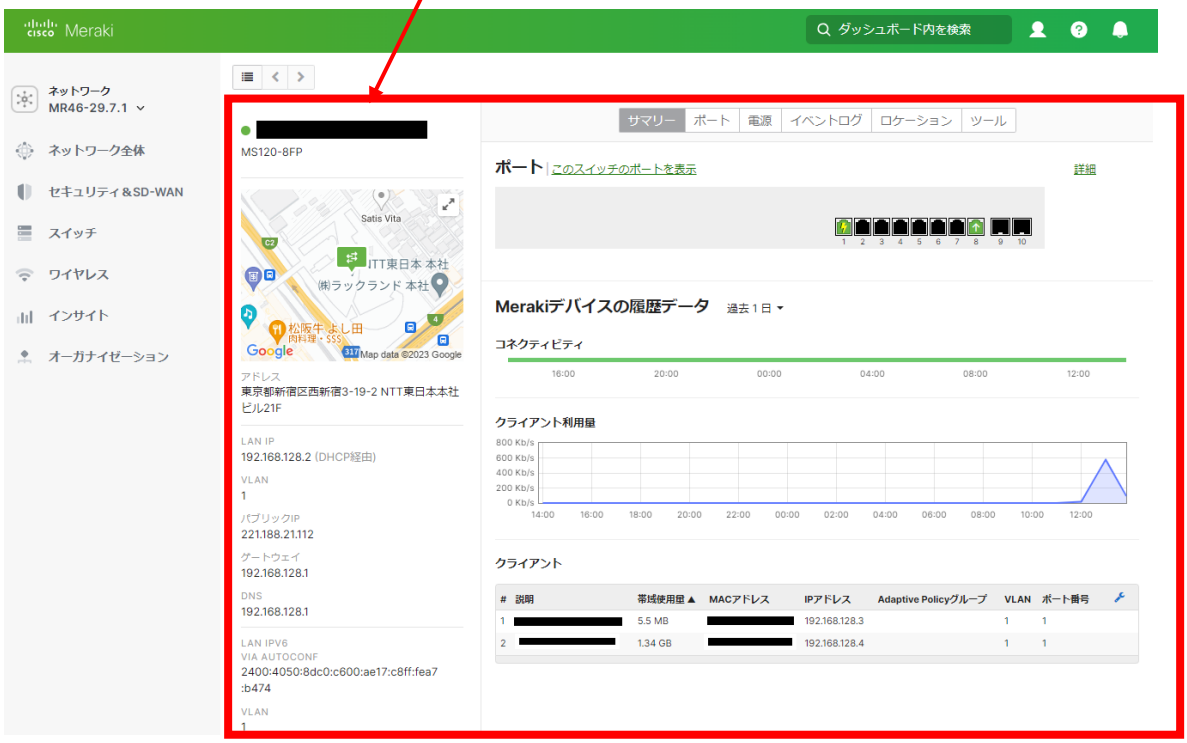
5-2. スイッチ　－スイッチー

- スイッチ装置の稼動状態を確認する

① ネットワークに登録されている各スイッチ装置のステータスが表示されます。
各スイッチの名前をクリックするとスイッチの詳細情報を確認できます。
※詳細画面で確認できる内容は次頁を参照ください。

② 一覧画面はcsvでダウンロードすることも可能です。





5-2. スイッチ　－スイッチー

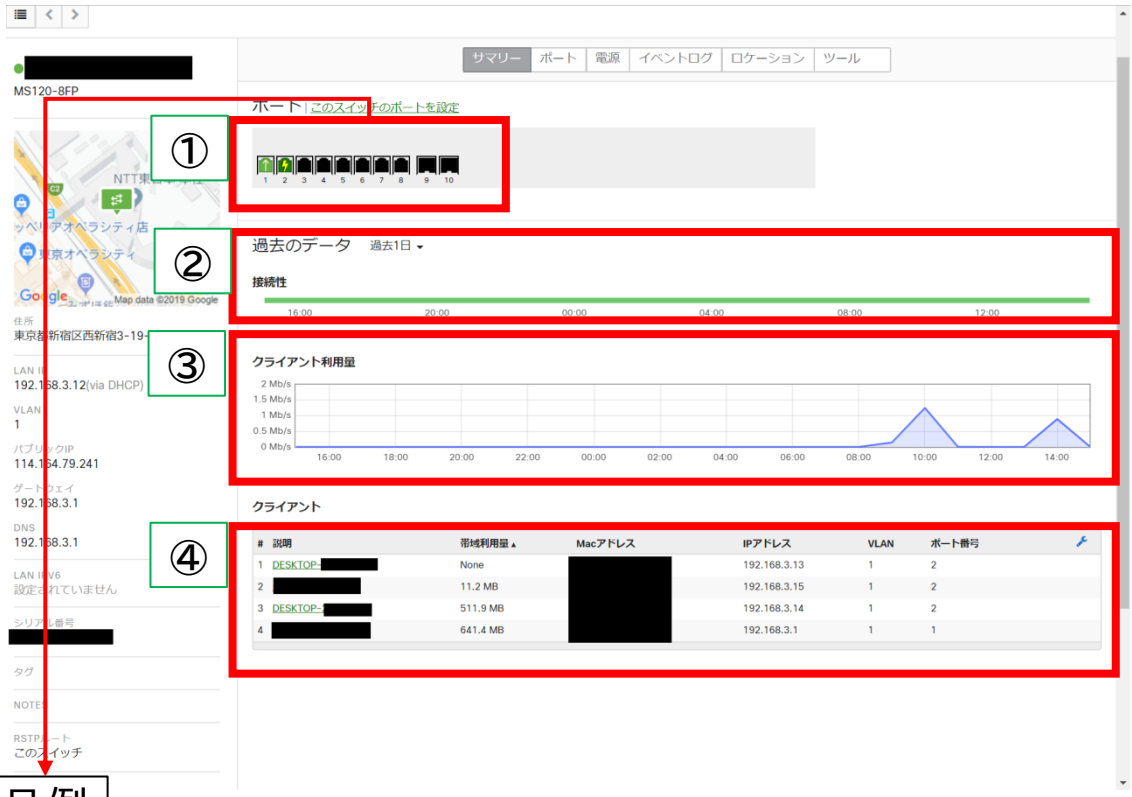
- 各スイッチ装置の状態、通信を確認する

① 各ポートの状態を確認できます。

② スイッチの稼動状態が表示されます。▼ボタンで表示期間や対象を変更できます。
緑色は正常。異常があった場合、その期間が赤色、またはオレンジになります。(※)

③ このスイッチの通信量を確認できます。

④ このスイッチに接続している機器やパソコン、スマートフォンを確認できます。



凡例

停止：
起動：
アップリンク：
PoE給電：
ブロックポート：
（STP、LACP）

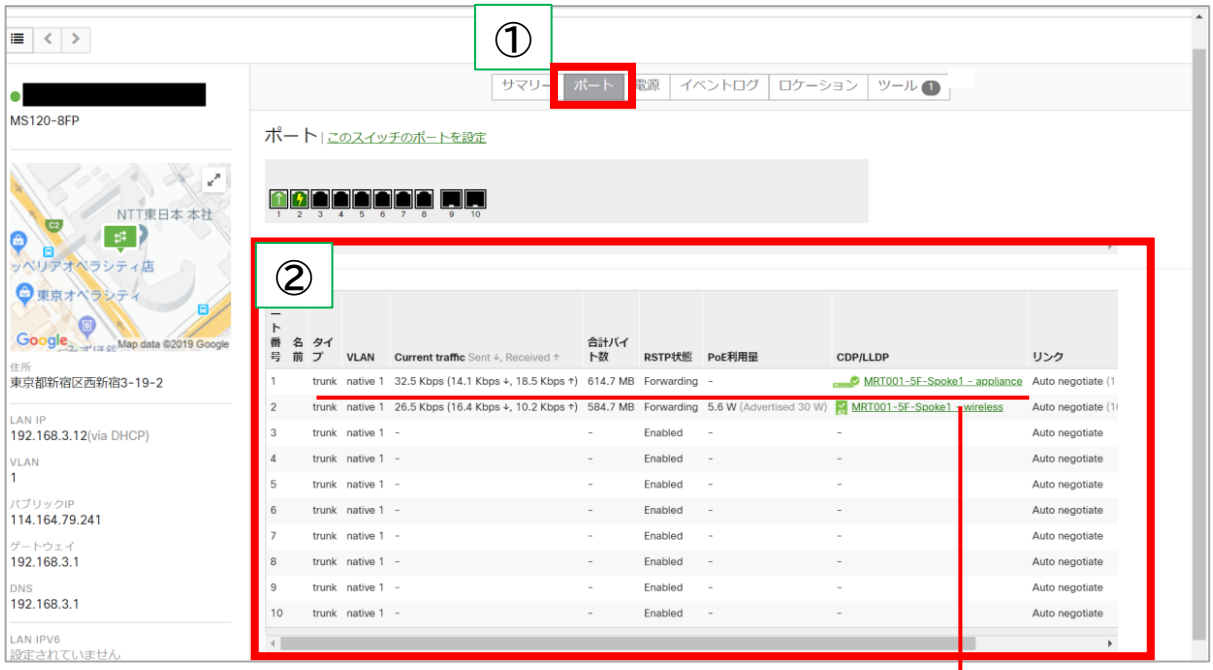
(※) 機器のオンライン状況はネットワーク機器が管理クラウドと通信できているかで機器状態を判断しております。そのため、インターネットには接続できているが、管理クラウドとの通信に問題が発生した場合（クラウドサーバーの障害、システムメンテナンス、回線障害など）、ネットワーク機器が正常に稼動していても、異常と表示されることがあります。

5-2. スイッチ　－スイッチー

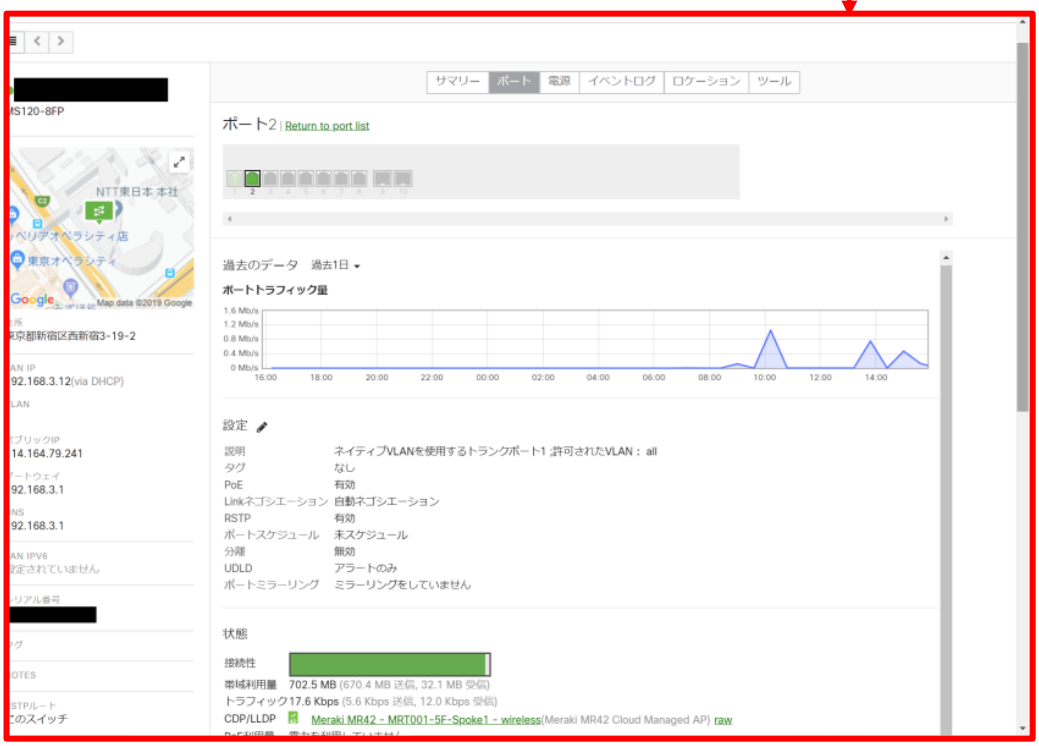
- 各ポートの状態、接続機器を確認する

① 上部の「ポート」をクリックすると各ポートの詳細画面になります。

② 各ポートの状態、接続機器を確認できます。



③ 各ポートをクリックするとさらに詳細情報が確認できます。



6-1. ワイヤレス

- 各アクセスポイントの機器状態を確認する

➢ 「ワイヤレス」メニューではアクセスポイントのステータスやWi-Fiの通信状況、各種設定状況が確認できます。

➢ 主に以下の「監視」項目でアクセスポイントに関する情報が確認できます。

カテゴリ	内容
概要	• 無線環境における品質評価の確認 （接続性、パフォーマンス、ネットワークサービス）
アクセスポイント	• 各アクセスポイントのステータスの確認
ロケーション分析	• Wi-Fiで検出したパソコンやスマートフォンを分析する
RFスペクトル	• アクセスポイント周辺の電波環境を測定
ヘルス	• 接続性に関するログを確認することができます。

➢ メニューから「ワイヤレス」にカーソルを合わせ「アクセスポイント」をクリックすると、各アクセスポイントの状態を一覧で確認することができます。

アクセスポイント毎のステータスを一覧で確認ができます。
●:オンライン(正常)、●:オフライン、●:アラート(警告)

6-1. ワイヤレス －概要－（1/3）

- ワイヤレス環境の品質を確認する

➢ 「ワイヤレス」-「概要」では、アクセスポイントにクライアントが接続する際の接続性や通信のパフォーマンスを観点にスコア表示され、問題が起きていないか確認することができます。

主に以下のような情報が表示されます。

カテゴリ	概要
接続ヘルス	接続失敗したクライアント数、SSIDに接続するまでにかかった時間、平均ローミング時間が確認でき、接続失敗率を基にスコア表示します。
パフォーマンスヘルス	遅延やパケットロス、シグナル品質（SNR）を基にパフォーマンススコアを表示します。
ネットワークサービスヘルス	クライアントがSSIDに接続した際、インターネット通信を行うために必要なネットワークサービスとの接続に成功しているかを成功率として表示し、スコアを表示します。

■ 「接続ヘルス」の表示例

表示	失敗率
悪い	80%－100%
低い	60%－80%
平均的	40%－60%
良い	20%－40%
非常に良い	0%－20%

スコアが平均的未満の場合、接続性に関して何らかの問題が発生している可能性があります。

更にどのクライアントで失敗が頻発しているのか確認したい場合∨をクリックすると、より細かい情報が確認可能です。

6-1. ワイヤレス －概要－（2/2）

- ワイヤレス環境の品質を確認する

■「パフォーマンスヘルス」の表示例

パフォーマンスヘルスでは遅延やパケットロスの発生状況、シグナル品質（SNR）を確認することができます。遅延やパケットロスが多く発生していたり、シグナル品質が著しく低い場合、電波干渉が発生している、アクセスポイントとクライアントまでの距離が遠い、遮蔽物がある等無線環境に何らかの問題が発生している可能性があります。

シグナル品質（SNR）は電波の品質を示し、指定している時間帯での平均値を表示します。無線環境が混雑している、周辺の無線機器等との電波干渉が著しい場合、値が低くなり、逆に環境が良好の場合、値が高くなります。

表示	シグナル品質（>27db）
悪い	80%－100%
平均未満	60%－80%
平均的	40%－60%
良い	20%－40%
非常に良い	0%－20%

スコアが平均より低い場合、問題を抱えているクライアントが多いことを示します。

更にどのクライアントで問題が起きているのか確認したい場合、∨をクリックすると、より細かい情報が確認可能です。

■「ネットワークサービスヘルス」の表示例

ネットワークサービスヘルスではRADIUS認証(※)、DHCPやDNSへの問い合わせの成功率に関するスコアを確認することができます。RADIUS認証の失敗やDHCPから有効なIPアドレスを取得できなかった等、問題が発生している場合にスコアが低くなります。

表示	失敗率
悪い	80%－100%
低い	60%－80%
平均的	40%－60%
良い	20%－40%
非常に良い	0%－20%

※無線クライアントがRADIUS認証を利用していない場合は「なし」と表示されます。

6-2. ワイヤレス　－ロケーション分析－

- アクセスポイント周辺の無線デバイス（スマートフォン等）を滞在率で分析

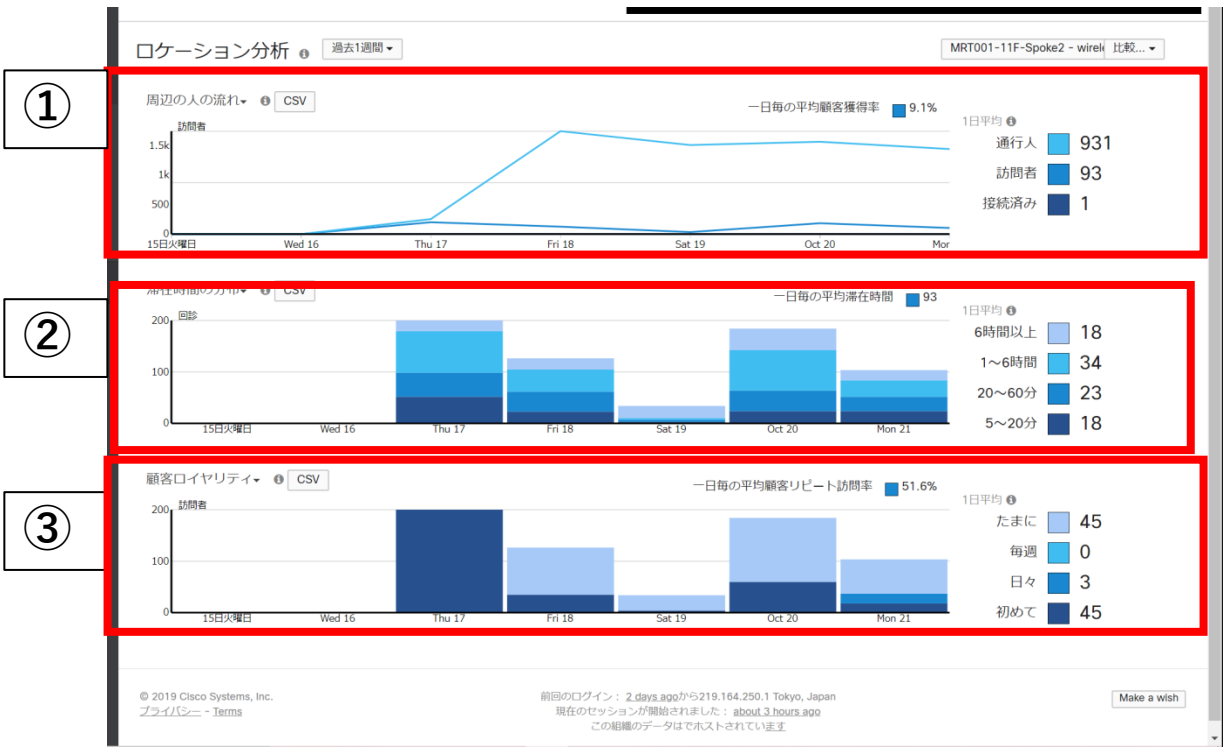
ロケーション分析では、アクセスポイントの周辺のスマートフォンなどの無線デバイスの状況を検知し、そのデバイスが通り過ぎただけなのか、一時的に滞在していたのか等、来訪者の傾向を分析することができます。メニューから「ワイヤレス」－「ロケーション分析」から確認できます。

① 周辺の人の流れ：店舗への訪問者（APの電波環境下に入った人数、Wi-Fiに接続した人数）を確認できます。
曜日毎の混雑状況を見ることで、勤務体制やメニューの検討を行ったり、キャンペーンの来客効果確認など、様々なマーケティング利用が可能です。

通行人：AP電波環境下に5分未満滞在した人数
訪問者：AP電波環境下に5分以上滞在した人数
接続済み：Wi-Fiに接続した人数

② 滞在時間の分析：店舗のAP電波環境下に入った人の滞在時間を確認できます。
滞在時間を延ばす、回転率を上げる施策の効果検証等のマーケティング利用が可能です。

③ 顧客ロイヤリティ：店舗のAPの電波環境下に入った人の訪問頻度を確認できます。
リピート客の割合把握（曜日毎のリピート客把握）や新規顧客増を狙ったキャンペーン効果等のマーケティング利用が可能です。



高度な利用

高度な利用

分析や診断など、より高度な利用方法を記載いたします。
これらの利用はある程度ネットワークの知識に精通されている方を対象としています。

また、これらの分析や診断についてもサポートセンターで支援していますので、記載されている内容が「難しい」と感じる方はサポートセンターまでお問い合わせください。

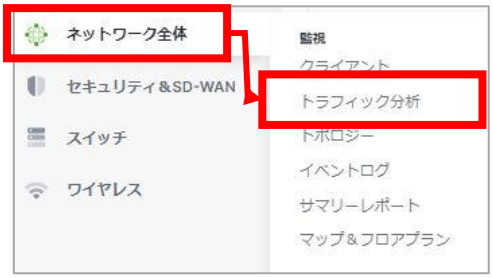
7.トラフィック分析

- 時系列でクライアントの接続数や通信量を確認

トラフィック分析では、クライアントの接続数や平均通信量を時系列で確認することができます。

通信の遅延などを感じた際に、クライアントの通常より多く接続されていなかったか、通信が突発的に増加していないか等の問題分析や、ネットワークの利用状況の分析等に活用いただけます。

トラフィック分析は、メニュー「ネットワーク全体」-「トラフィック分析」から確認できます。



	カテゴリ	概要
①	**クライアントカウント**	クライアント接続数と時系列でのグラフ表示 利用状況の傾向分析や意図しない時間帯に端末がアクセスしていないか等の確認。
②	**帯域使用量**	発生したトラフィック量の総計と時系列グラフ表示 通信が多く発生する時間帯、慢性的に通信が多く発生していないか等の分析に。
③	**トラフィック詳細**	発生したトラフィックの内訳の表示 どのような通信が多く発生しているのかの確認や意図していないアプリケーション通信がないか等の確認、またファイアウォールの設計の際どのアプリケーションを制限するかの検討に役立ちます。

8-1. 故障診断　ツールの場所

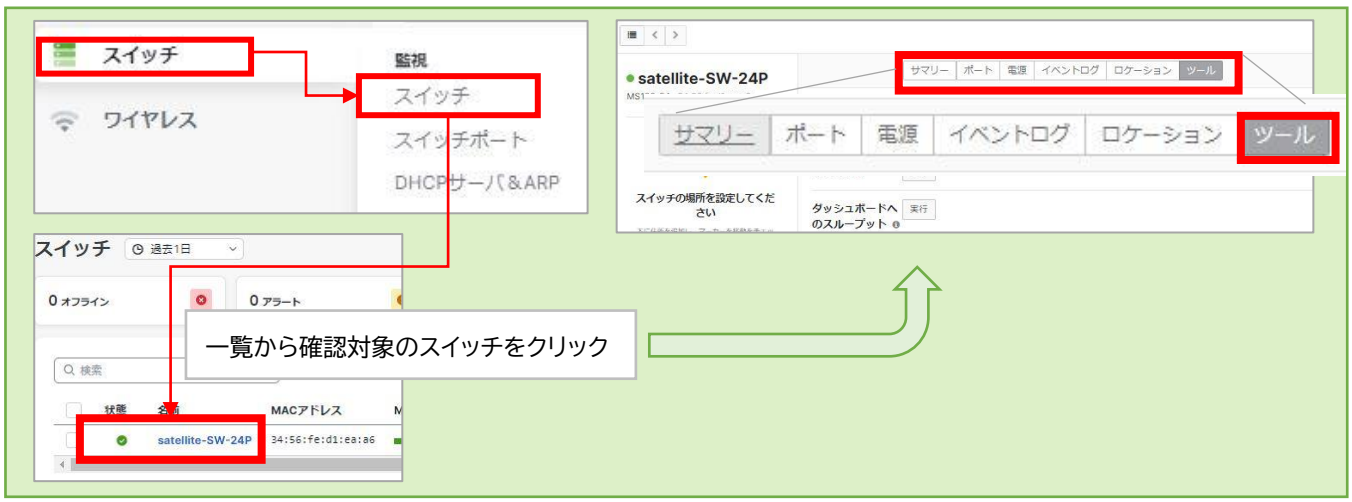
- 通信診断ツールで通信不調の原因を調査する

各機器（VPN装置・スイッチ・アクセスポイント）ではダッシュボードから疎通確認（Ping）等、各種診断に役立つツールが利用可能できます。各診断ツールは各機器のデバイス情報画面の「ツール」からご利用ください。

■VPN装置の場合

■アクセスポイントの場合

■スイッチの場合

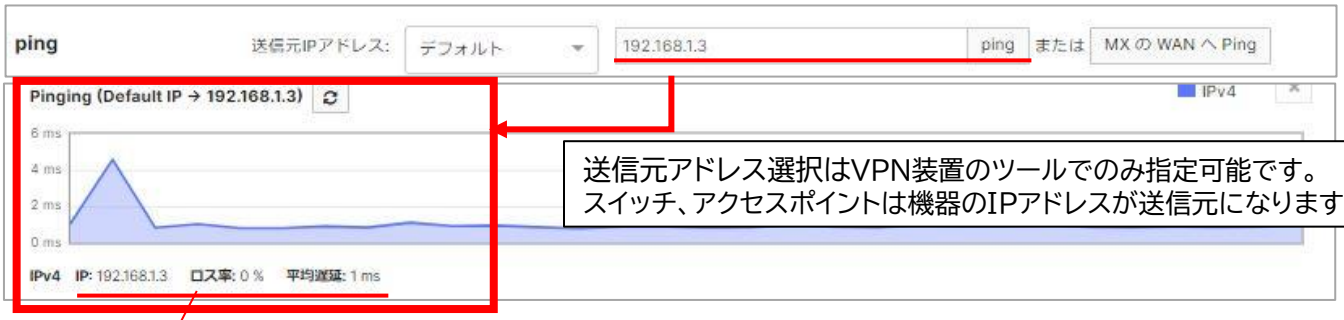


8-1. 故障診断 （各機種共通）

- 通信診断ツールで通信不調の原因を調査する

➢ Ping（疎通確認）（ネットワーク機器から指定IPアドレスへの疎通確認）

アドレス入力欄に宛先のドメイン名、またはIPアドレスを入力し、Pingボタンをクリックすると
Pingの応答結果が表示されます。
ロス率が100%の場合、宛先まで到達できない、宛先がダウンしている、または到達はしているが
ファイアウォール等でブロックされているなどが考えられます。 ネットワークに問題がない場合、
宛先のファイアウォール設定やアンチウイルスソフト等でブロックされていないか確認してください。

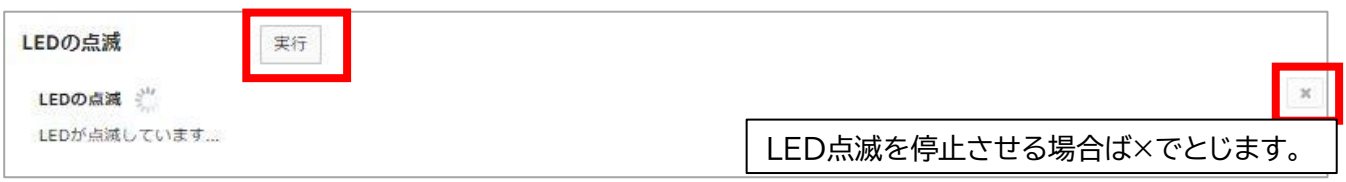


送信元アドレス選択はVPN装置のツールでのみ指定可能です。
スイッチ、アクセスポイントは機器のIPアドレスが送信元になります。

損失率、平均遅延が大きい場合、通信経路の混雑や干渉他何らかの問題が疑われます。
※宛先側の設定によって、正常に接続できている場合でも損失率100%となる場合がございます。

➢ **LEDの点滅**

ネットワーク機器本体のLEDを高速点滅させます。設置されているデバイスがダッシュボード上の
どの装置か判別が困難な場合、本体のLEDを意図的に点滅させ、視認することで確認ができます。
特にアクセスポイントなど天井や壁に設置されている場合に有用です。



LED点滅を停止させる場合は×でとじます。

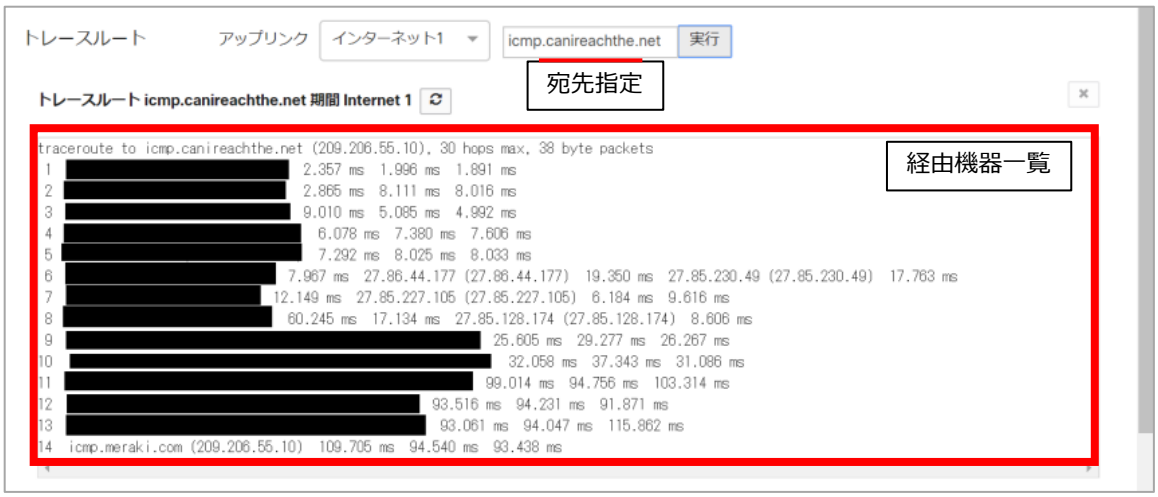
➢ **ダッシュボードへのスループット測定**

ネットワーク機器～管理クラウド間のスループットを測定します。
対象ネットワーク機器から先の経路で速度が遅くなっていないか調査する際に有用です。

8-1. 故障診断 （経路診断）

- 通信診断ツールで通信不調の原因を調査する

➢ トレースルート 宛先までの経路を確認できます。（VPN装置、アクセスポイントで利用可能）
宛先を入力してから実行ボタンをクリックしてください。宛先までに経由する機器のIPアドレスが表示されます。結果が表示されるまでは数分かかる場合もございます。



➢ MTR:宛先までの経路を確認できます。（VPN装置、スイッチで利用可能）
トレースルートとほぼ同じことが確認できます。トレースルートに失敗する場合、MTRを実行すると確認できる場合があります。

8-2. 故障診断 －スイッチ－

- 各ポートに接続されたケーブル故障診断、ポート再起動、MACアドレスの調査

➢ ケーブルの故障診断 （スイッチのみ）

指定したポートに接続されているケーブルの診断を行うことができます。

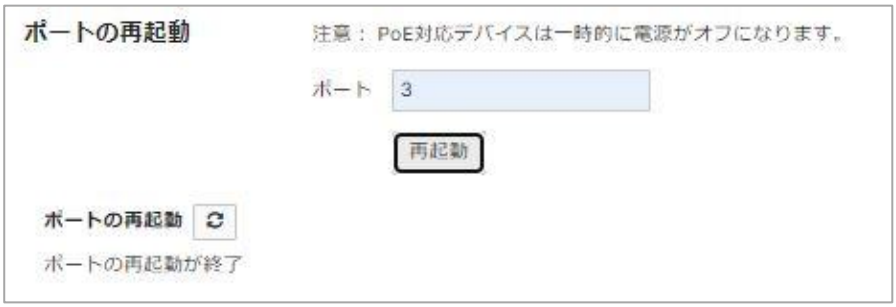
※故障診断を実行すると、通信が中断される可能性がございます。
アップリンク（ルーターと接続しているポート）に対しては故障診断を行うことができません。

➢ ポートの再起動 （スイッチのみ）

指定したポートの再起動を行うことができます。

指定ポートに接続されたPoE給電デバイス等（アクセスポイントやカメラ）を意図的に再起動したい場合にも有用です。（PoE給電対応モデルご利用時）

※ポート再起動中は、対象とポートで一時的に通信断が発生します。



➢ MAC転送テーブル

スイッチに接続されている機器のMACアドレスを表示します。

8-2. 故障診断　－スイッチー

- スイッチに接続されたクライアントのスリープ解除 Wake on LAN

➢ クライアントのスリープ解除

スリープ中の機器を遠隔で起動させることができます。起動させたい機器のMACアドレス、VLAN IDを指定します。（スイッチに接続されていない機器を起動させることはできません。）

また、遠隔起動できる機器は「Wake On LAN」という技術に対応した機器で該当機能が有効となっている必要があります。

9-1. 無線診断 －RFスペクトルー (1/3)

- アクセスポイント周辺のチャネル利用率を確認する

➢ 「RFスペクトル」では、アクセスポイント周辺の電波状況やチャネル使用率の確認が可能です。
Wi-Fiが頻繁に切れるといった事象や電波状態が悪いと感じられる際、問題の要因として周辺の無線機器からの電波干渉や無線接続機器が多い等の原因が考えられます。
RFスペクトルでは、アクセスポイント周辺の無線状況を確認し、チャネルが混雑していないか等、問題の原因調査に役立てることが可能です。

➢ 「RFスペクトル」はメニューの「ワイヤレス」－「RFスペクトル」から確認ができます。

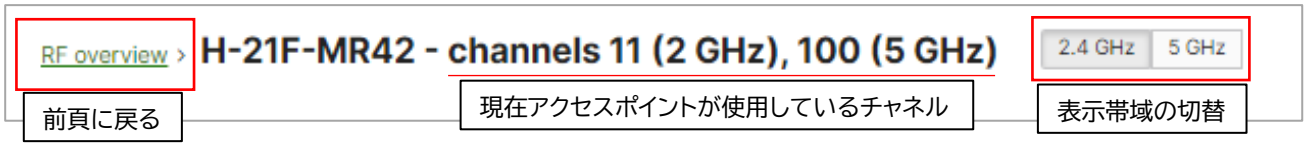
① アクセスポイント一覧が表示され、アクセスポイントが使用しているチャネル、2.4GHz/5GHzの平均チャネル使用率が表示されます。特定のアクセスポイントをクリックすると詳細表示されます。

項目名	内容
名前	APの名称
使用チャネル	アクセスポイントが現在使用しているチャネル
平均チャネル使用率（2.4GHz）（5GHz）	帯域毎に過去80秒間の平均チャネル使用率を表示 Very low　:チャネルが空いています。 Very high　: チャネルが混雑しています。

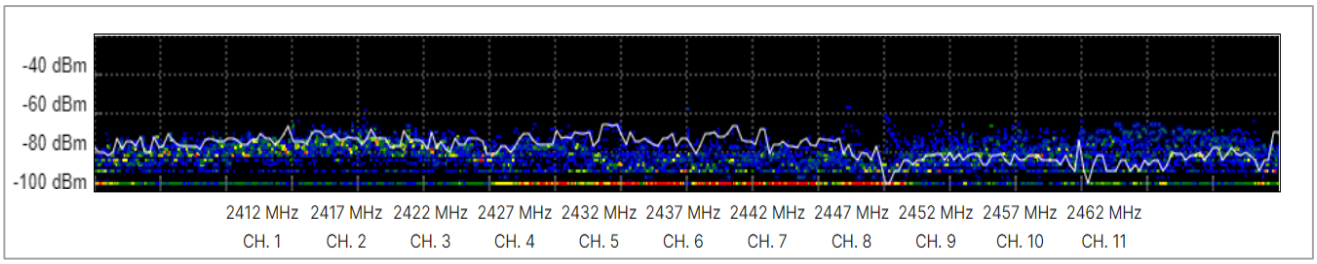
9-1. 無線診断 －RFスペクトルー (2/3)

- アクセスポイント周辺のチャネル利用率を確認する

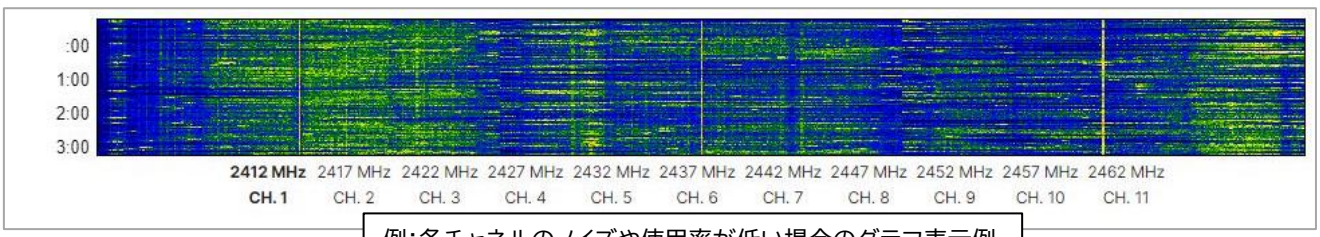
➢ アクセスポイント毎の詳細画面では各チャネルごとの使用率、周辺の機器が送波しているSSID名や信号強度、使用しているチャネルを確認することができます。



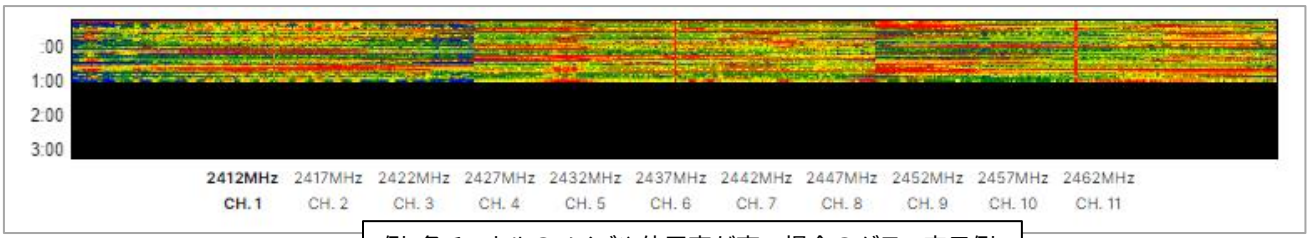
➢ 各チャネルの使用率のスナップショットが表示されます。
白い線が現在の読取値で描画され、測定毎に更新されます（測定値がその点に一致するにつれ、グラフ上の点は青から赤に移動します)。値(dBm）は低いほど優れています。



➢ 下段のグラフは経時的な各測定値が表示され、時間経過とともに下に流れていきます。
青はノイズが低いことを示し、黄～赤はノイズが高く、電波干渉が起きやすい状態を示します。
ノイズや使用率が顕著に高い場合、通信遅延やパケットロスが発生する可能性が高くなります。



例:各チャネルのノイズや使用率が低い場合のグラフ表示例

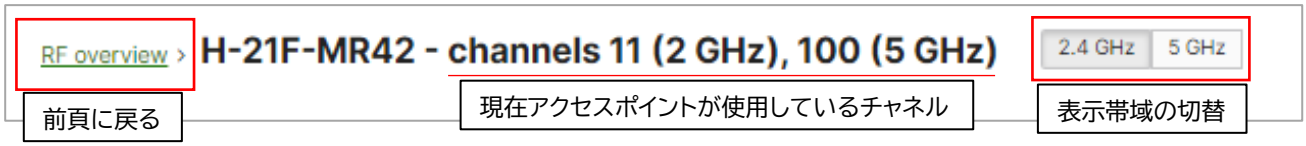


例:各チャネルのノイズや使用率が高い場合のグラフ表示例

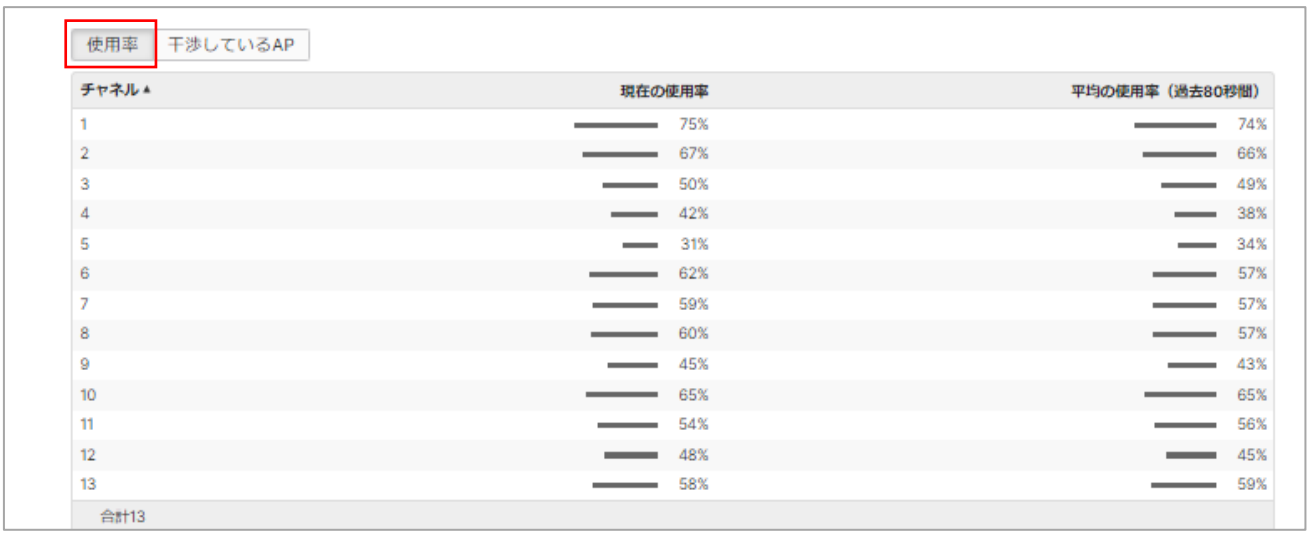
9-1. 無線診断 －RFスペクトルー (3/3)

- アクセスポイント周辺のチャネル利用率を確認する

➢ アクセスポイント毎の詳細画面では各チャネルごとの使用率、周辺の機器が送波しているSSID名や信号強度、使用しているチャネルを確認することができます。



➢ 前頁のグラフ下部の表では「使用率」「干渉しているAP」が確認可能で、「使用率」では、表示している帯域に応じた各チャネルの使用率状況と平均使用率が表示されます。



チャネル	現在の使用率	平均の使用率（過去80秒間）
1	75%	74%
2	67%	66%
3	50%	49%
4	42%	38%
5	31%	34%
6	62%	57%
7	59%	57%
8	60%	57%
9	45%	43%
10	65%	65%
11	54%	56%
12	48%	45%
13	58%	59%
合計13		

➢ 「干渉しているAP」では、選択したチャネル上で検出されたワイヤレスネットワークとその情報をリストします。dBmが高いほど (例: -40 は -60 よりも高い)、信号が強いことを示します。
自身が使用しているチャネルと近傍のAP（アクセスポイント）とチャネルがかぶっていないか、近い位置に併設して設置されているアクセスポイントがいないか等の確認に利用いただけます。

BSSID	SSID	dBm	Channel	Mode	On LAN
00:	W	-40	12	802.11g (WPA)	not seen
08:	at	-40	6	802.11ac (WPA2)	not seen
80:	at	-42	1	802.11ac (WPA2)	not seen
a4:	rt	-42	6	802.11n (WPA2)	not seen
84:	9	-50	10	802.11ac (WPA2)	not seen
cc:	fu	-50	3	802.11n (WPA2)	not seen
74:	B	-50	8	802.11n (WPA2)	not seen

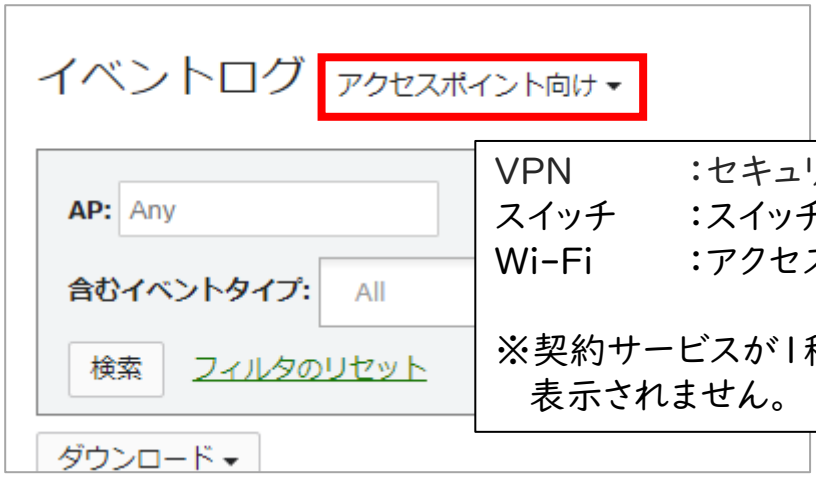
10-1. イベントログを確認する

・イベントログでは端末の接続、サービス機器に関する様々なログを
確認することができます。
・通信状況の確認の参考としてお使いください。

イベントログの確認方法

➢ 「ネットワーク全体」-「イベントログ」を選択します。

➢ イベントログの種別で確認したいカテゴリに切り替えます。



VPN　　：セキュリティアプライアンス向け
スイッチ　：スイッチ向け
Wi-Fi　　：アクセスポイント向け

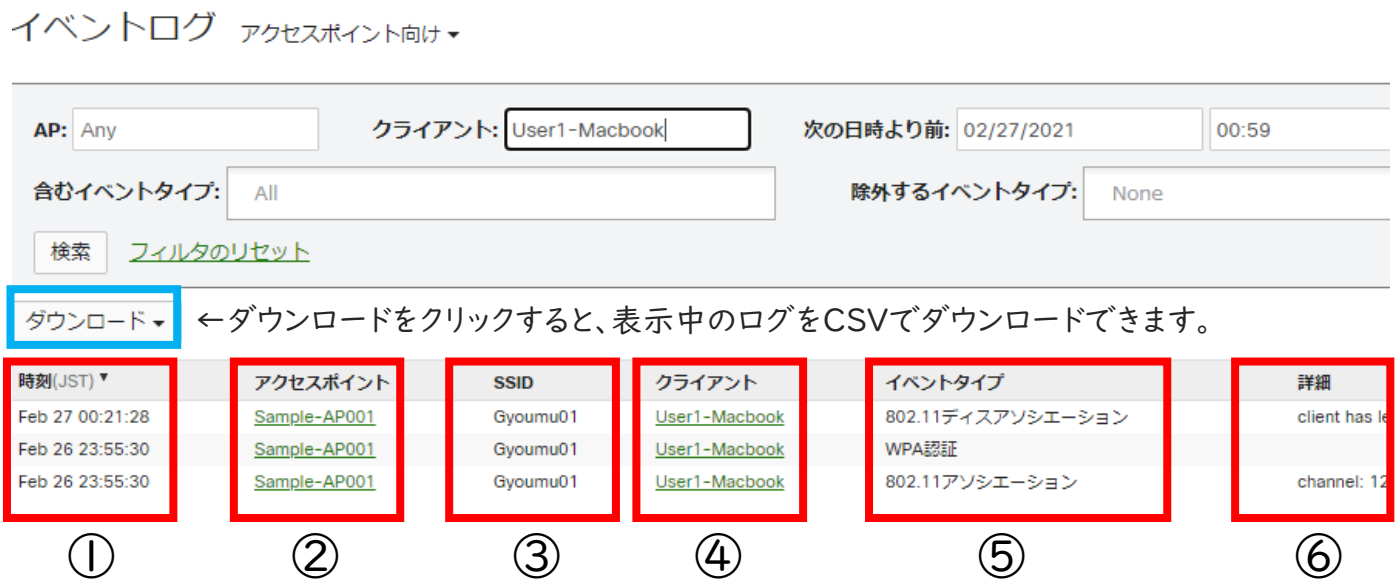
※契約サービスが1種の場合はカテゴリ選択は
表示されません。

→次ページへ続く

10-1. イベントログを確認する

ログフィールドで確認できる項目

➢ ログフィールドに出力されたイベントログで以下の項目を確認いただけます。



各列に表示される内容

	区分	内容
①	時刻	(いつ)イベントが発生した時刻。
②	アクセスポイント※	(どのAPで)イベントが発生したアクセスポイント名。 アクセスポイント名をクリックすると詳細なアクセスポイント情報が確認できます。
③	SSID※	(どのSSIDで)イベントが発生したSSID名。
④	クライアント	(誰が)対象のクライアント名。 クライアント名をクリックすると詳細なクライアント情報が確認できます。
⑤	イベントタイプ	発生したイベントタイプ。
⑥	詳細	発生イベントの詳細。

※ アクセスポイント向け表示時のみ

10-2. イベントログを確認する –VPN向け-

主要なイベントタイプのご紹介

本項ではイベントログ（セキュリティアプライアンス（VPN））で確認できる
主要な内容を一部紹介します。

■ DHCPリース/リリースを確認する

	イベントタイプ	詳細
①	DHCPリース	ip: 192.168.xxx.xxx がリースされたことを示します。 More >> をクリックするとより詳細な情報が確認できます。 Router / subnet /dns / duration(リース期限/秒) Server ip/ server_mac 情報
②	DHCPリリース	DHCPがリリースされたことを示します。
③	DHCPの問題	(Extra: no_offers_received) DHCPサーバからの応答がない、アドレス取得できなかった場合に表示されます。

■ リモートアクセスの接続状況を確認する

	イベントタイプ	詳細
①	VPNクライアントが接続しました	Local_ip：割り当てられたIPアドレス User_id: ログイン時に使用したID Remote_ip：接続元のIPアドレス リモートアクセスが成功した際に表示されます。
②	VPNクライアントが切断しました	Local_ip：割り当てられていたIPアドレス User_id: ログイン時に使用したID Remote_ip：接続元のIPアドレス リモートアクセスを切断した際に表示されます。
③	クライアントアドレスプールが空です。	接続してきたリモートアクセスクライアントに割り当てるIPアドレスが枯渇しています。

10-2. イベントログを確認する –VPN向け-

■ リモートアクセスの接続状況を確認する（前項の続き）

	イベントタイプ	詳細
④	Meraki以外/ クライアントVPNネゴシエーション	msg: invalided DH group 19. msg: invalided DH group 20. クライアントVPN接続エラー 789 主な原因 ・クライアントで設定した事前共有キーが誤っている ・UDP500・4500等ファイアウォールでブロックされている ・（Windows時） IKEやAuthIPIPsecサービスが無効になっている。
⑤	Meraki以外/ クライアントVPNネゴシエーション	msg: not matched ISAKMP-SA established xxxxxx[4500]-xxxxx[4500]xxx クライアントVPN接続エラー 691 主な原因 ・ログインIDやパスワードが間違っている ・許可されていないユーザのアクセス
⑥	ログが表示されていない場合	関連するイベントログが表示されない場合、VPN装置に通信が到達していないため、ログが表示されていないと思われます。（上位ルータや、クライアントの接続先情報に誤りがないかご確認ください。）

■ IPアドレスが重複している

	イベントタイプ	詳細
①	クライアントIPの重複	クライアントIPが重複していることを検知した際に表示されます。

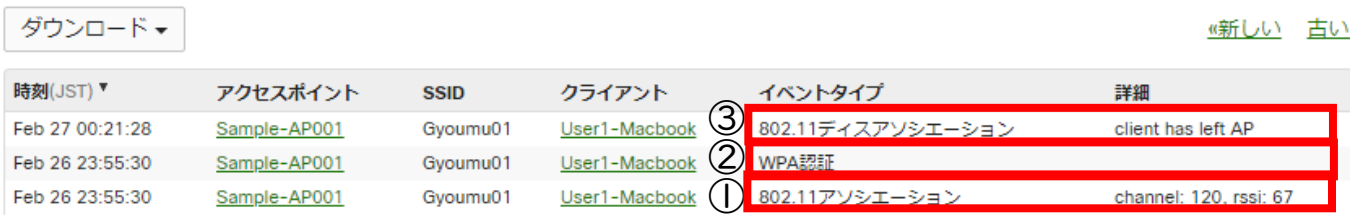
VPNイベントログの主な使用方法は以上となります。

10-3. イベントログを確認する - アクセスポイント向け -

主要なイベントタイプのご紹介

本項ではイベントログで確認できる主要な内容を一部紹介します。

■ Wi-Fiクライアントが対象SSIDに接続/認証成功/切断したことを確認する



	イベントタイプ	詳細
①	802.11アソシエーション	(Channel xxx, rssi yy) SSIDへアクセスした際のチャネル(Channel)、クライアント信号強度(RSSI)を示します。
②	WPA認証	正しい事前共有キー(PSK)が入力されたことを示します。
③	802.11ディスアソシエーション	(Client has left AP) クライアントがAPから離れたことを示します。 クライアントの電源断や休止モードの際にも表示されることがあります。 (previous authentication expired) クライアントの事前共有器キー(PSK)を誤入力や正しく認証解除が行われずにクライアントがSSIDから切断した(された)ことを示します。 (Client association expired) クライアントが非アクティブな為、関連付けを解除しました ※5分間無応答の場合、関連付けを解除します (unknown reason) クライアントがAPからの通信を突然停止した場合や電波干渉が発生し、クライアントとAPが不安定な状態で通信できなくなった場合などに表示されます。

10-3. イベントログを確認する - アクセスポイント向け -

■ DFSが発生していないか、イベントログで確認する場合

5GHz帯では「気象レーダー」や「航空機レーダー」も利用しており、それらのレーダーに影響を与えないよう、検知、動的に回避する機能を「DFS」といいます。
「DFS」発生時は他のチャネルへ切り替えが発生する為、一時的にデータ通信できなくなります。その為、5GHz帯の通信が時折切れてしまう場合はイベントログで「DFS」が発生していないか確認し、発生頻度によってはレーダー影響のない帯域(W52帯)へチャネルを変更する等の検討が必要となります。

1. 含むイベントタイプ入力欄をクリックし「DFS event detected」を選択します。
2. 「検索」をクリックします。
3. 該当するログが表示されます。

	イベントタイプ	詳細
①	DFSイベントを検出しました	channel xxx (DFS検知時に使用していたチャネル) radio 1 (該当のアンテナ 1は5GHzのアンテナという意味)

ワイヤレスイベントログの主な使用方法は以上となります。