

「ギガらくルーター Type-C」 「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. アシユアランス
5. セキュリティ&SD-WAN
6. スイッチ
7. ワイヤレス

高度な利用

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

- 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。
本文に表示されている承認処理用URL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東日本ギガらくルーター・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、ギガらくルーター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。

[承認処理用URL\(例 https://~~~\)](https://~~~)

...

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@ccc.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。

- 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

- 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「Create password」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

Hello,

You have been signed up for a Cisco Meraki account with administrator privileges for 1 network in the organization "xxxxxxxx xxxxxxxxx." Your login email is xxxx.xxxx@xxxx.co.jp.


[Create password](#)

Thanks,
Cisco Meraki

? Cisco Meraki とは…

ギガらくルーターType-C装置、ギガらくスイッチおよびダッシュボードサービスの提供会社です

Welcome to Cisco Meraki!
Enter new password

 You have an invalid token.

Password

[Show](#)

Must be 8 characters or more

Confirm password

[Show](#)

[Return to sign in](#)

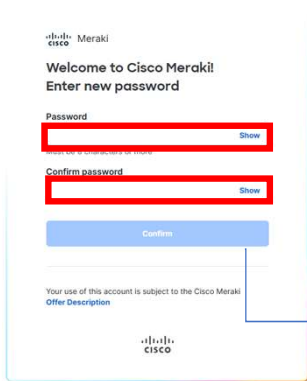
[Reset password](#)

※メール受信後24時間以内にCreate Passwordからリンク先でパスワード設定を行わないと上記画面が表示されてPassword、Confirm password欄へ入力できなくなります。
この画面でReturn to sign inをクリックするとダッシュボードログイン画面へ遷移します がパスワード設定が完了していないためログインができません。

上記画面が表示された場合は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

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、「Confirm」ボタンをクリックします。



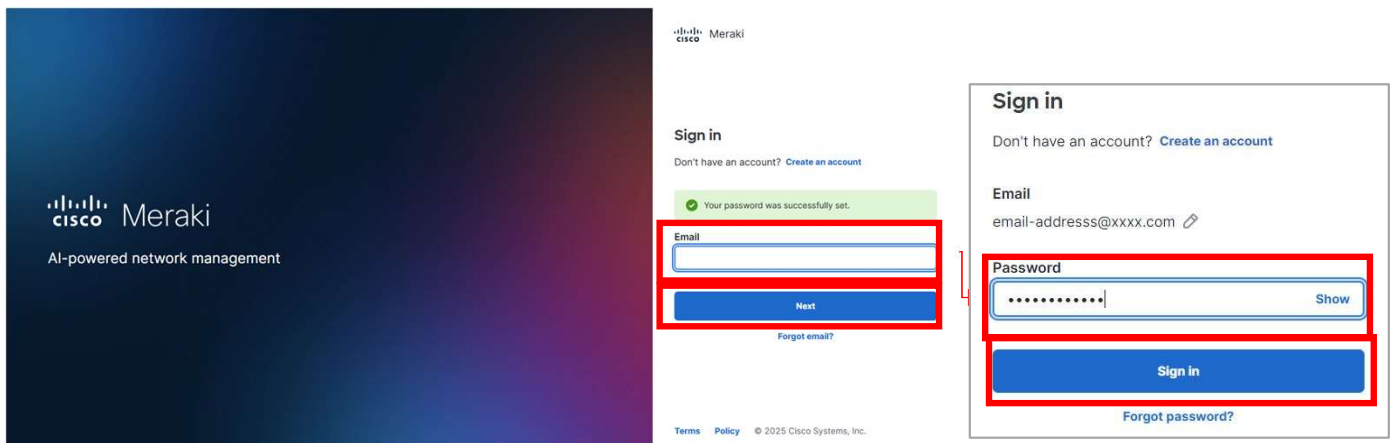
- ※パスワードは以下のうち3種類以上を
組み合わせて8文字以上の入力が必要
- 半角英字(大文字)
 - 半角英字(小文字)
 - 半角数字
 - 記号(- _ . @ # \$)



3. 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。


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。

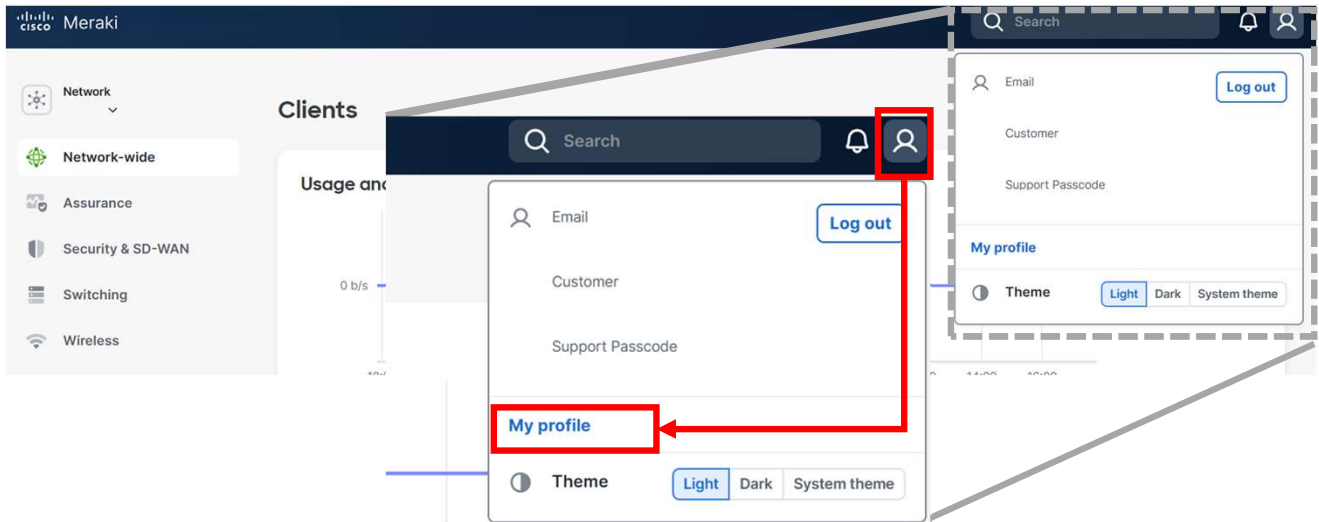
※ログイン画面をお気に入り登録しておくことをお勧めいたします。



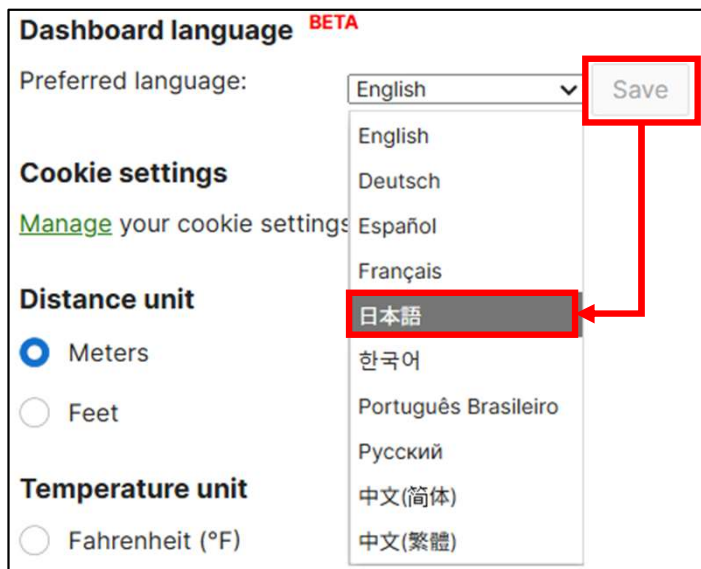
これで事前準備は完了です！

- 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。

- 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。
- 次に「My profile」をクリックします。



- Dashboard LanguageのPreferred languageから「日本語」を選択し、「Save」をクリックすることで、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. アシユアランス
5. セキュリティ&SD-WAN
6. スイッチ
7. 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。

- 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。



- 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。
- 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 ~ p10
アシュアランス	パフォーマンス、監視情報の表示	p11 ~ p17
セキュリティ&SD-WAN	ルーター装置に関する情報の表示	P18 ~ p24
スイッチ	スイッチに関する情報の表示	p25 ~ p28
ワイヤレス	Wi-Fiに関する情報の表示	p29 ~ p32

- 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。

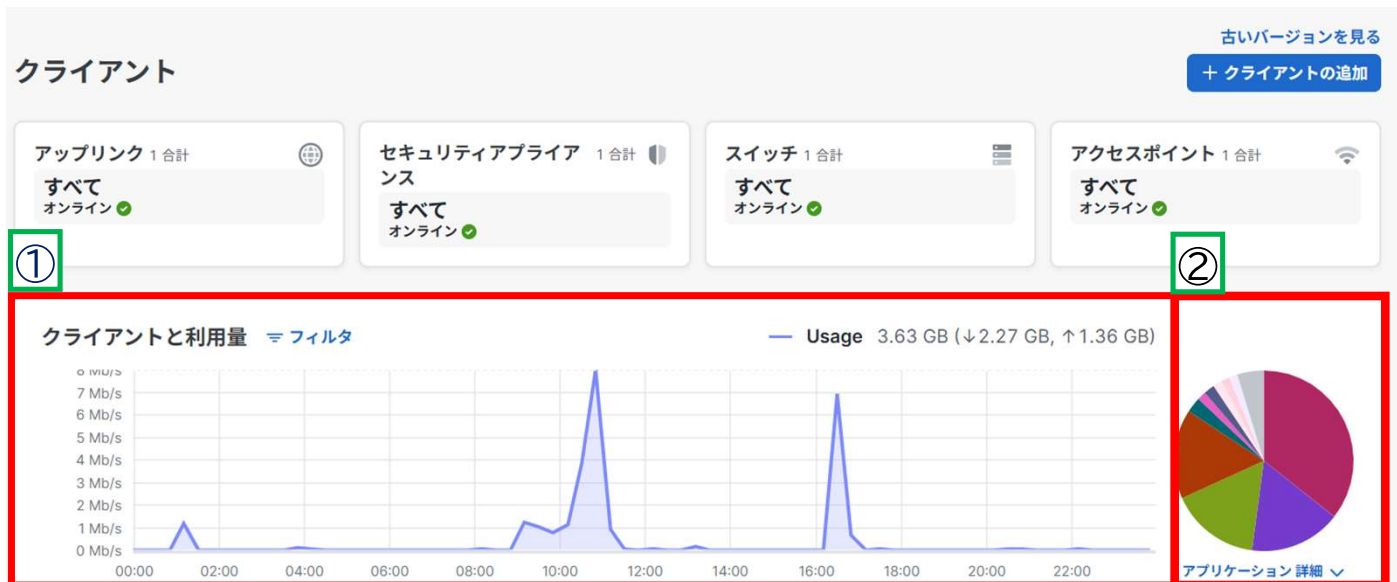


ネットワーク状況の確認をする際、主に以下のカテゴリから確認を行います。

カテゴリ	内容
クライアント	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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(※)	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • ネットワークの稼働レポートを表示

・ 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

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 %
Windows file sharing - 192.168.20.10	ファイル共有	2.15 GB	35.6%	2.15 GB	35.6%
Windowsファイル共有	ファイル共有	411 KB	0.1%	2.15 GB	35.6%
Microsoft SkyDrive	ファイル共有	2 KB	0.1%	2.15 GB	35.6%
UDP - 165.225.111.190	—	1017.36 MB	16.5%	1017.36 MB	16.5%
DTLS	—	993.82 MB	16.1%	993.82 MB	16.1%
Zscaler	セキュリティ	990.72 MB	16.0%	990.75 MB	16.0%
DigiCert	セキュリティ	34 KB	0.1%	990.75 MB	16.0%

・ 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。

状態	説明	接続先	IPv4アドレス	MACアドレス	帯域使用量	デバイスタイプ, OS	最終確認日時 (UTC+9)
Wireless		AP-001		Bc:2f	887 KB	その他	Nov 20 2025 21:50
Wireless		AP-001		04:e	471 KB	Intel	Nov 21 2025 08:26
Wireless		AP-001		ca:b	46 KB	その他	Nov 20 2025 22:48
Wireless		AP-001		c8:c	2.53 MB	Intel	Nov 20 2025 16:43
Wireless		AP-001		c8:c	582.32 MB	Intel	Nov 21 2025 10:35
Wireless		AP-001		ca:8	4 KB	その他	Nov 21 2025 13:38
Wireless		AP-001		4c:f	3.23 MB	Apple	Nov 21 2025 10:28
Wired					GB	HP	Nov 21 2025 14:21
Wireless					4 MB	Intel	Nov 21 2025 14:21

無線端末 : Wireless
 有線端末 : Wired
 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。

• 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。



トポロジー

L2-リンク層 L3-ネットワーク層

展開 ▾ 折りたたむ ▾ ⓘ 検索... 3 オンライン

すべてのデバイスにラベル付け



ポート: ↔ 1
速度: 1 Gbps
クライアント:
13

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

- ルーター装置:
- スイッチ:
- Wi-Fi装置:
- その他機器:

The screenshot shows the configuration page for a Meraki switch. The device name is 'OH-001'. The port is 'GigabitEthernet0/1'. The platform is 'cisco WS-C2960CG-8TC-L'. The address is '10.0.0.10'. The version is 'Cisco IOS Software, C2960C Software (C2960c405ex-UNIVERSALK9-M), Version 15.0(2)SE8, RELEASE SOFTWARE (fc1) Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2015 by Cisco Systems, Inc. Compiled Thu 14-May-15 03:25 by prod_rel_team'. Capabilities include 'Switch, IGMP conditional filtering'. There are several unrecognized options listed at the bottom.

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。

・ 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。

- グラフの表示期間は変更が可能です。
(過去1日/過去1週間/過去1か月間/カスタム期間が選択できます。)
- 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。

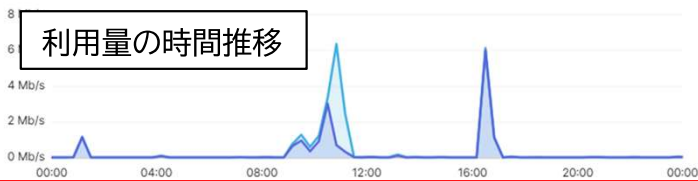
サマリーレポート from **過去1日** レポート期間の調整

ネットワーク: 0001 - appliance | デバイスタグ: すべてのデバイス | SSID: すべてのSSID

使用状況統計

転送されたデータ量の合計	ダウンロード量の合計	アップロード量の合計
3.77 GB	2.30 GB	1.47 GB

利用量の時間推移



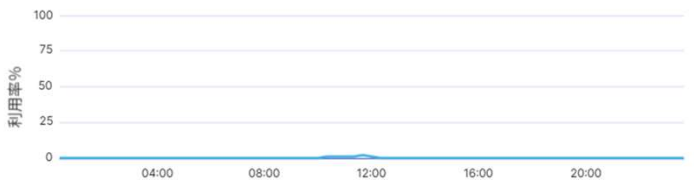
データ転送量の多いデバイス

名前	モデル	クライアント数	帯域使用量	使用率%
RT-001	MX67	10	3.77 GB	100.00%

デバイスモデル別使用量順位

モデル	デバイス数	帯域使用量	デバイスあたりの平均使用率
MX67	1	3.77 GB	3.77 GB

デバイス使用率



レポートのダウンロード

Excelにエクスポート

レポートのカスタマイズ

- クライアント
- 上位アプリケーションカテゴリ
 - 利用量上位のアプリケーション
 - URL別上位ブロック済みサイト
 - カテゴリ別ブロックされたサイト順位
 - シングニチャ別の該当した脅威順位
- アップリンク
- アップリンク
- クライアント
- クライアント統計
 - Splashページ
 - 利用量上位のクライアント
 - 利用量上位のクライアントデバイスメーカー
 - 利用量上位のOS
- 帯域使用量
- 使用状況統計
 - 利用量の時間推移
 - データ転送量の多いデバイス
 - デバイスモデル別使用量順位

説明	帯域使用量	使用率%
	2.44 GB	64.75%
	1.17 GB	31.01%
	101.3 MB	2.62%
	35.5 MB	0.92%
	22.3 MB	0.58%
	2.5 MB	0.07%
	1.8 MB	0.05%

利用実態の把握や行動分析など

利用量上位のクライアントデバイスメーカー

メーカー	帯域使用量	クライアント数	クライアントの割合
HP	2.44 GB	1	10.00%
Intel	1.17 GB	3	30.00%
Meraki	136.8 MB	2	20.00%
CHONGQING FUGUI...	22.3 MB	1	10.00%
Other	1.8 MB	3	30.00%

利用量上位のOS

- アシユアランスで確認できる主な情報を確認する

- 「アシユアランス」メニューではクライアントやネットワークデバイスの接続状況、時系列別のアラート情報が確認できます。

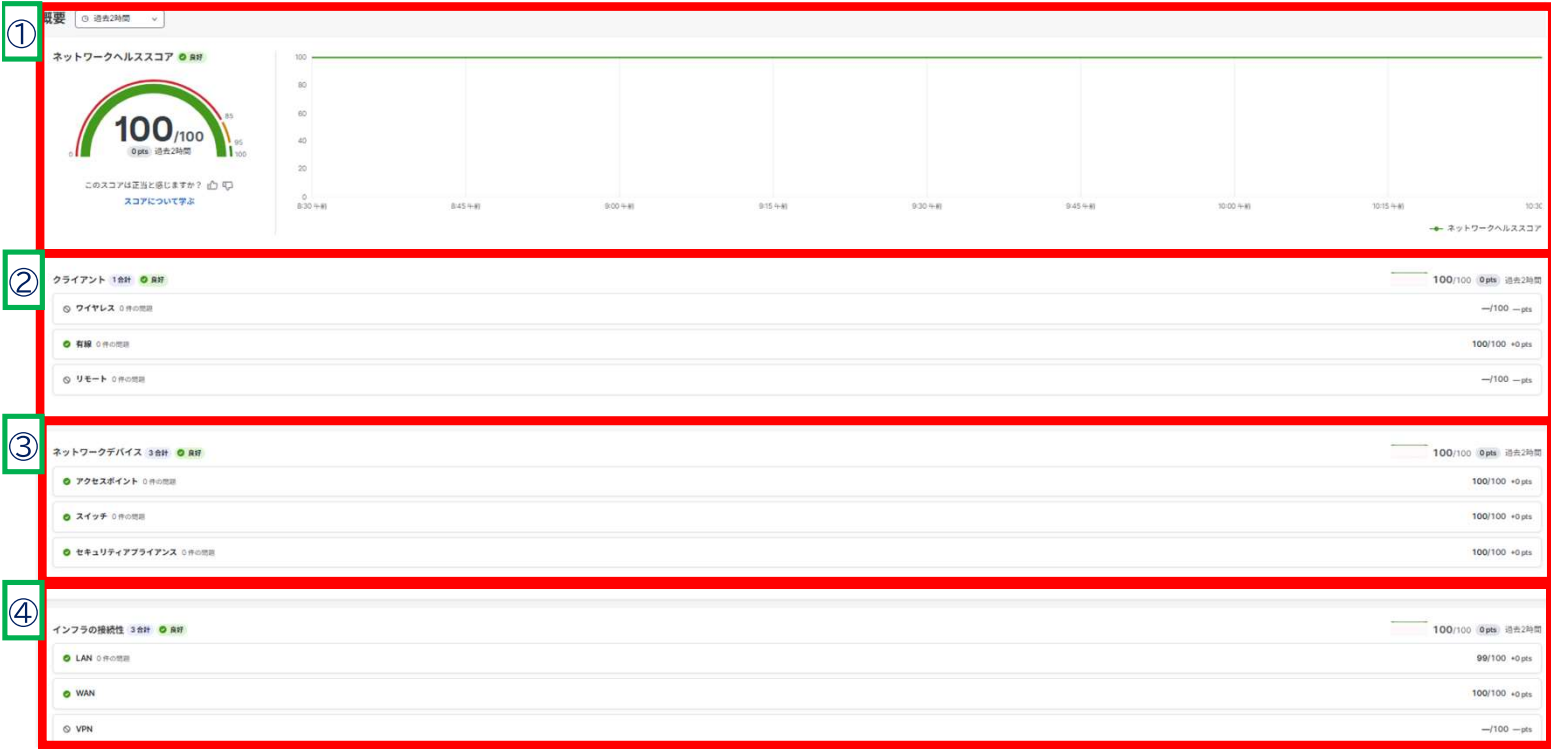


- 各ネットワークデバイスやクライアントの接続状況の確認をする際、主に以下のカテゴリから確認を行います。

カテゴリ	内容
概要	<ul style="list-style-type: none"> 接続別に影響を受けたクライアント数と原因に関する情報 ネットワークデバイス毎の状態に関する情報 ネットワーク全体のリンク状況やパフォーマンスに関する情報
アラート	<ul style="list-style-type: none"> ネットワーク全体の障害状況や発生件数に関する情報
クライアント(※)	<ul style="list-style-type: none"> 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 <p>※ネットワーク全体のクライアント情報と同様となります。 詳細手順はp8をご参照ください。</p>
イベントログ(※)	<ul style="list-style-type: none"> 端末の接続、サービス機器に関するログを確認 <p>※高度な利用の10.イベントログ同様となります。 詳細手順はp42をご参照ください。</p>

- ネットワーク全体接続の健全性を確認する。

- 「アシユアランス」-「概要」では、クライアント接続状況、ネットワークデバイスの稼働状況からネットワーク全体の健全性を観点にスコア表示されます。
- 主に以下のような情報が表示されます。



	カテゴリ	概要
①	ネットワークヘルススコア	ネットワーク全体のネットワーク接続の健全性を確認することができ、クライアント、ネットワークデバイス、インフラの接続失敗を基に総合的なスコアを表示します。
②	クライアント	クライアントの接続タイプ(無線・有線・リモート)の健全性を確認することができ、クライアント接続失敗を基にスコア表示します。
③	ネットワークデバイス	ネットワークデバイスのステータス確認をすることができ、各デバイス(ルーター・スイッチ・アクセスポイント)のエラー・警告、クラウド接続失敗を基にスコアを表示します。
④	インフラの接続性	LAN/WAN、VPN疎通の健全性を確認することができ、リンク不良やLAN/WAN障害を基にスコアを表示します。

- ネットワーク全体の接続ステータスを確認する。

■ ネットワークヘルススコアの表示例

概要 過去2時間 確認したい期間を指定します。(過去2時間、過去1日、過去1週間、カスタム(開始終了日時の指定が可能))

ネットワークヘルススコア 良好

このスコアは正当と感じますか? 👍 👎
スコアについて学ぶ

Nov 25 2025 20:45 JST - Nov 25 2025 22:45 JST
99/100 良好
クライアント 97/100
デバイス 100/100
インフラの接続性 100/100

Nov 25 2025 22:00 JST
100/100 良好
クライアント 100/100
デバイス 100/100
インフラの接続性 100/100

カーソルを合わせたときの表示例

確認したい日時にカーソルを合わせることでその時点のネットワークヘルススコアを確認可能です。グラフは指定した日時の総合スコアを表示します。

指定した期間の総合評価されたネットワークヘルススコアを確認可能です。

表示	スコアの状態
良好	95-100
ほどよい	85-94
不良	0-84

ネットワークヘルススコア ほどよい

Nov 19 2025 12:00 JST - Nov 19 2025 17:00 JST
87/100 ほどよい
クライアント 62/100
デバイス 93/100
インフラの接続性 87/100

ネットワークヘルススコア 不良

Nov 19 2025 14:00 JST - Nov 19 2025 16:00 JST
75/100 不良
クライアント 53/100
デバイス 94/100
インフラの接続性 79/100

カーソルを合わせることでクライアント、デバイス、インフラの接続性毎のヘルススコアを確認することができます。状況を確認したい場合、画面下部へスクロールして詳細を確認することが可能です。

詳細は各確認手順をご参照ください。
クライアント……………P.14
デバイス……………P.15
インフラの接続性… P.16


- ネットワーク全体の各ステータスを確認する。

■ ネットワーク全体の各ステータスでの表示例

- クライアント・ネットワークデバイス・インフラの接続性単位の各ステータス表示が確認できます。
- 各デバイス・クライアント種別や健全性が確認できます。
各カテゴリをクリックすると問題の詳細画面を確認することが可能です。

(参考) ネットワークデバイスの表示例

ネットワークデバイス 3 合計 ▲ ほどよい



94/100 - pts current period

2 ✖ **アクセスポイント** 2 件の問題 80/100 -20 pts

1 Access point impacted

▲ **スイッチ** 1 件の問題 89/100 -11 pts

1 Switch impacted

● **セキュリティアプライアンス** 1 件の問題 100/100 - pts

1 WAN appliance impacted

ネットワークデバイスのステータス表示

- ...デバイスが正常
- ▲ ...デバイスが軽度な影響や注意が必要な警告レベルの問題が発生
- ✖ ...デバイスが影響を受けるような重大な問題が発生

1 指定期間に対象となった数

2

3 合計

▲ ほどよい



94/100 - pts current period

✖	アクセスポイント 2 件の問題	80/100	-20 pts
	1 Access point impacted		
▲	スイッチ 1 件の問題	89/100	-11 pts
	1 Switch impacted		
●	セキュリティアプライアンス 1 件の問題	100/100	- pts
	1 WAN appliance impacted		

- ネットワークデバイスのステータス表示
- ...デバイスが正常
 - ▲ ...デバイスが軽度な影響や注意が必要な警告レベルの問題が発生
 - ✖ ...デバイスが影響を受けるような重大な問題が発生

- アラート状態の確認をする。

- 「アシユアランス」-「アラート」では、時系列別に発生しているアクティブなアラートや解決済みのアラートを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。

アラート 1 過去1週間

① 時系列毎のアラート発生件数

② アクティブ 解除 解決済み

アラートタイプ デバイスタイプ デバイスタグ 1 マッチング結果

更新 Less than 1 minute ago

1 クリティカル 0 警告 0 情報提供

発生中のアラート

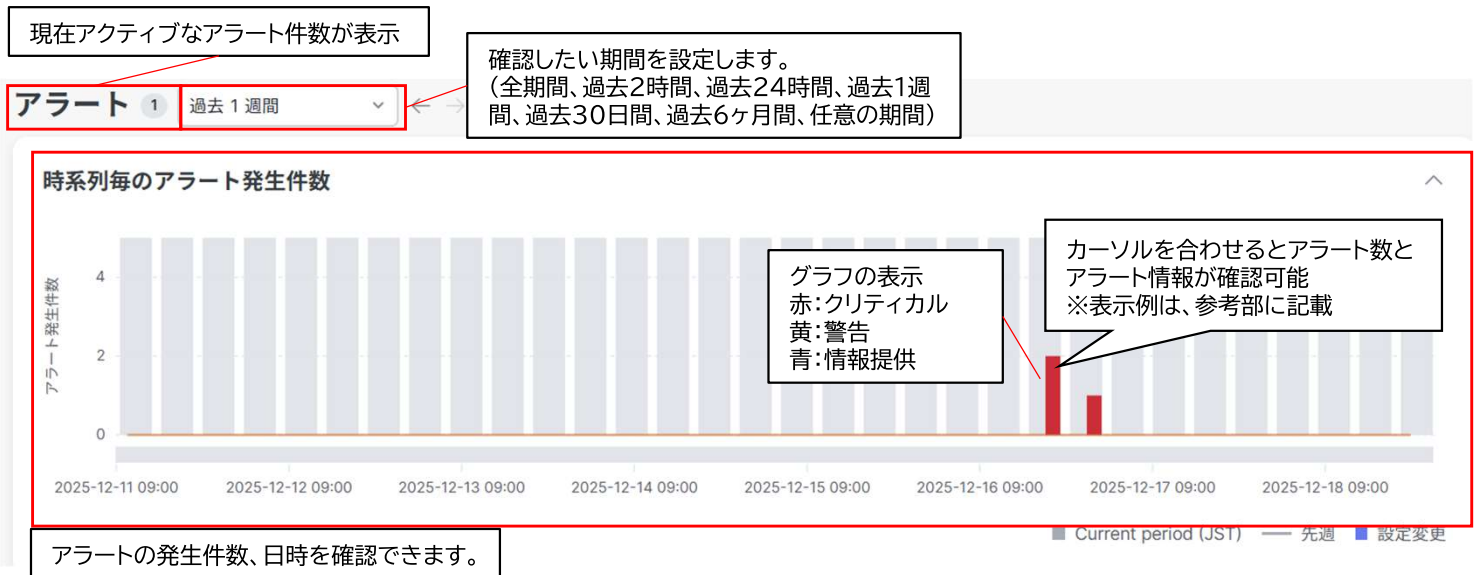
深さ	アラートタイプ	アラート数	デバイスの種類	ネットワーク数	最終発報日時	カテゴリ
+	クラウドに到達不能なデバイス	1	MS	1	12月 19 17:45 JST	コネクティビティ

①アラート発生日時・件数を確認できます。

②アクティブなアラートや解決済みのアラート詳細を確認することが可能です。

- アラート件数や発生日時を確認する。

➤ アラート日時・件数の表示画面で以下のような情報が表示されます。



(参考) オフラインデバイスがある場合のアラート例



- アラート情報の詳細を確認する。

➤ アクティブなアラート画面では以下のような情報が表示されます。

アラート状態の選択

アラートタイプ ▼ デバイスタイプ ▼ デバイスタグ ▼ 1 マッチング結果 42 minutes ago 時点

各アラートの深刻度と発生件数が表示

発生中のアラート

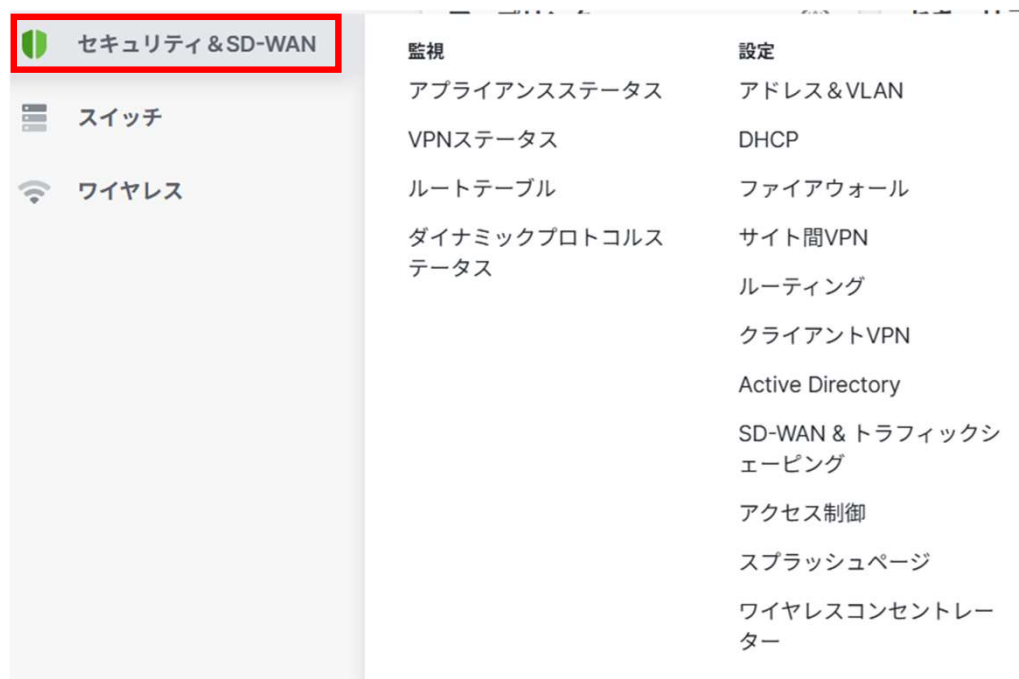
深刻度	アラートタイプ	アラート数	デバイスの種類	ネットワーク数	最終発報日時	カテゴリ
赤	クラウドに到達不能なデバイス	1	MR	1	12月 16 22:15 JST	コネクティビティ

① ② ③ ④ ⑤ ⑥ ⑦

	区分	内容
①	深刻度	アラートの重要度 赤:クリティカル 黄:警告 青:情報提供
②	アラートタイプ	アラートの種別 青文字をクリックすることでどのネットワークで発生したかを確認できます。
③	アラート数	選択した期間内でアラートタイプが発生した件数
④	デバイスの種類	アラートが発生したデバイスの種類
⑤	ネットワーク数	同じアラートが発生したネットワーク数
⑥	最終発報日時	アラートが最後に発生した日時
⑦	カテゴリ	アラートの分類

- ルーター装置の各情報を確認する。

- 「セキュリティ&SD-WAN」メニューではルーター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
アプライアンスステータス	<ul style="list-style-type: none"> • ルーター装置のステータスの確認 • ルーター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ステータス(※)	<ul style="list-style-type: none"> • 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 <p>※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。</p>
ルートテーブル	<ul style="list-style-type: none"> • ルーター装置のルートテーブルを表示します。

- ルーター装置の稼動状態を確認する
- ルーター装置の通信量を確認する

① ルーター装置名 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 ルーター装置のポート状態が表示されます。ルーター装置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 指定期間内でルーター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 ルーター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。

・ 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。）

The screenshot displays the Meraki dashboard for device RT-001 (MX67). It is divided into three main sections:

- ① Settings (設定):** A red box highlights the 'アップリンク' (Upstream) tab and the 'WAN' configuration table. The table shows:

タイプ	IPv4	IPv6
構成	PPPoE	自動 (ステートレス)
状態	アクティブ	未接続
IPアドレス		
ゲートウェイ		
DNS		
- ② Live Data (ライブデータ):** A red box highlights the 'アップリンクトラフィック' (Upstream Traffic) graph, which shows real-time traffic volume in MB/h for both upload and download.
- ③ Historical Data (Merakiデバイスの履歴データ):** A red box highlights the 'Merakiデバイスの履歴データ' (Meraki Device History Data) section for the last 24 hours. It includes two graphs: '遅延' (Latency) in ms and '損失率' (Loss Rate) in %, both showing WAN-specific data.

• 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。

RT-001
MX67

サマリー ア **①** DHCP IPv6プレフィックス ロケーション ツール

② DHCPサブネット

サブネット	VLAN	③ 利用中 ▲	空き
192.168.10.0/24	192.168.10.0/24 - VLAN 10	0	253 (100%)
192.168.128.0/24	192.168.128.0/24 - VLAN 1	8	245 (96%)

④ すべてのDHCPリース

フィルタ条件: サブネット, VLAN, IP, or MAC

クライアント	MAC	IP	サブネット	VLAN	有効期間
	F8:9	192.168.128.3	192.168.128.0/24	192.168.128.0/24 - VLAN 1	23 hours
	2C:3	192.168.128.4	192.168.128.0/24	192.168.128.0/24 - VLAN 1	23 hours
	8E:2	192.168.128.16	192.168.128.0/24	192.168.128.0/24 - VLAN 1	19 hours
	CA:B	192.168.128.10	192.168.128.0/24	192.168.128.0/24 - VLAN 1	14 hours

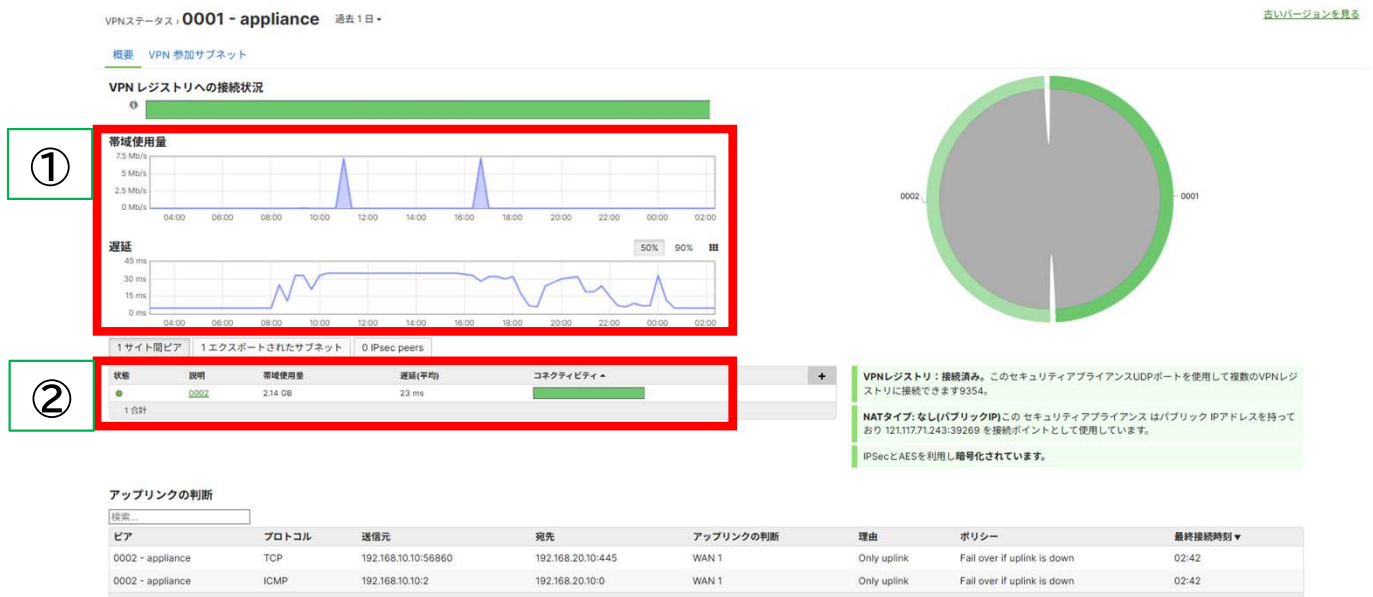
• 機器の設置場所の確認

① 画面上部の「ロケーション」をクリックすると、マップ上でルーター装置の設置場所を確認できます。



- 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ルーター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。

• 機器の設置場所の確認

- ① 画面上部の「VPN参加サブネット」をクリックするとルーター装置の参加しているネットワーク情報が確認できます

VPNステータス: **0001 - appliance** 過去1日

概要 **VPN 参加サブネット**

①

VPN 参加サブネット

ネットワーク、VLAN名、サブイ

ネットワーク ▲	VLAN名	VLAN ID	サブネット
0001 - appliance	VLANID 10	10	192.168.10.0/24
0002 - appliance	VLANID 20	20	192.168.20.0/24

結果: 2

• 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。

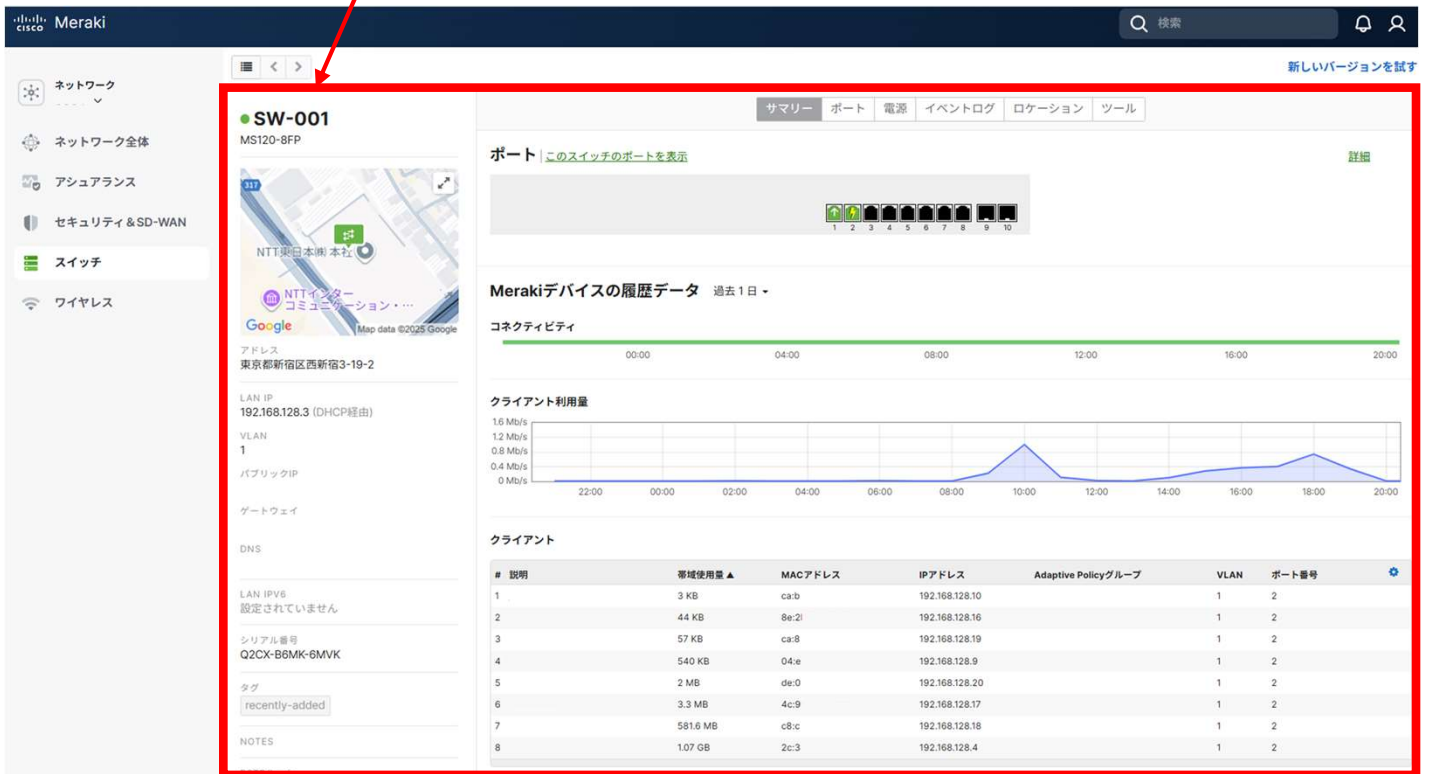


- 主に以下の「監視」項目でスイッチの状態が確認できます。

カテゴリ	内容
スイッチ	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 各スイッチポートの設定・ステータス確認

・ 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。



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。

SW-001
MS10-8FP

サマリー ポート 電源 イベントログ ロケーション ツール

ポート | このスイッチのポートを表示

Merakiデバイスの履歴データ 過去1日

クライアント利用量

クライアント

#	説明	帯域使用量 ▲	MACアドレス	IPアドレス	Adaptive Policyグループ	VLAN	ポート番号
1		3 KB	ca:b	192.168.128.10		1	2
2		44 KB	8e:2f	192.168.128.16		1	2
3		57 KB	ca:8	192.168.128.19		1	2
4		540 KB	04:e	192.168.128.9		1	2
5		2 MB	de:0	192.168.128.20		1	2
6		3.3 MB	4c:9	192.168.128.17		1	2
7		581.6 MB	c8:c	192.168.128.18		1	2
8		1.07 GB	2c:3	192.168.128.4		1	2

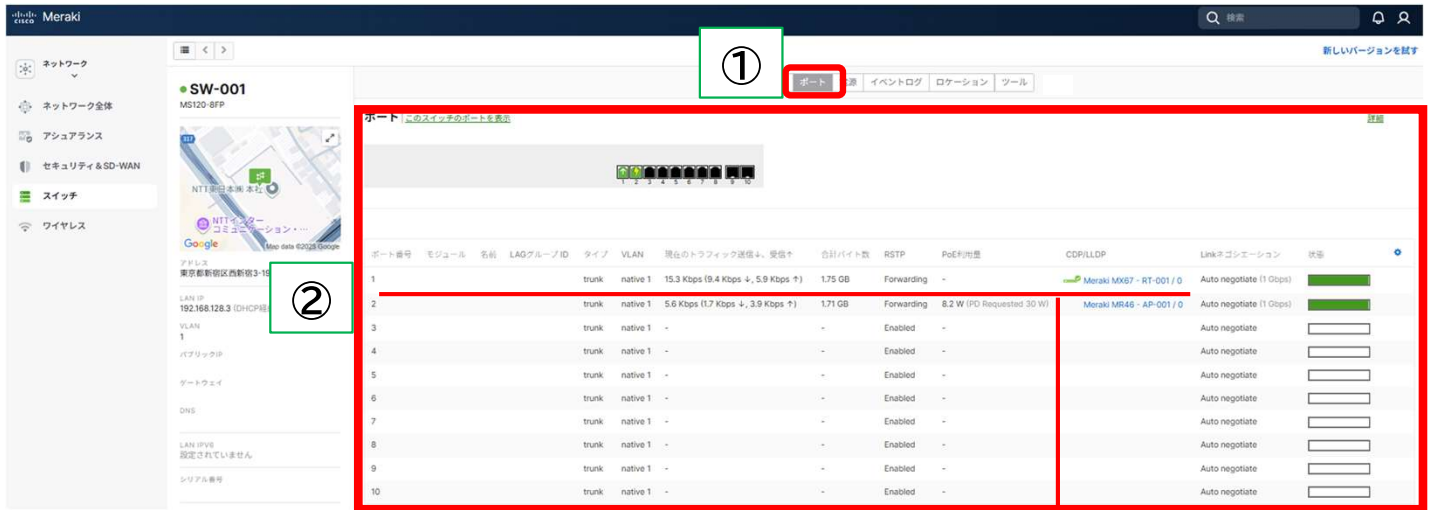
凡例

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

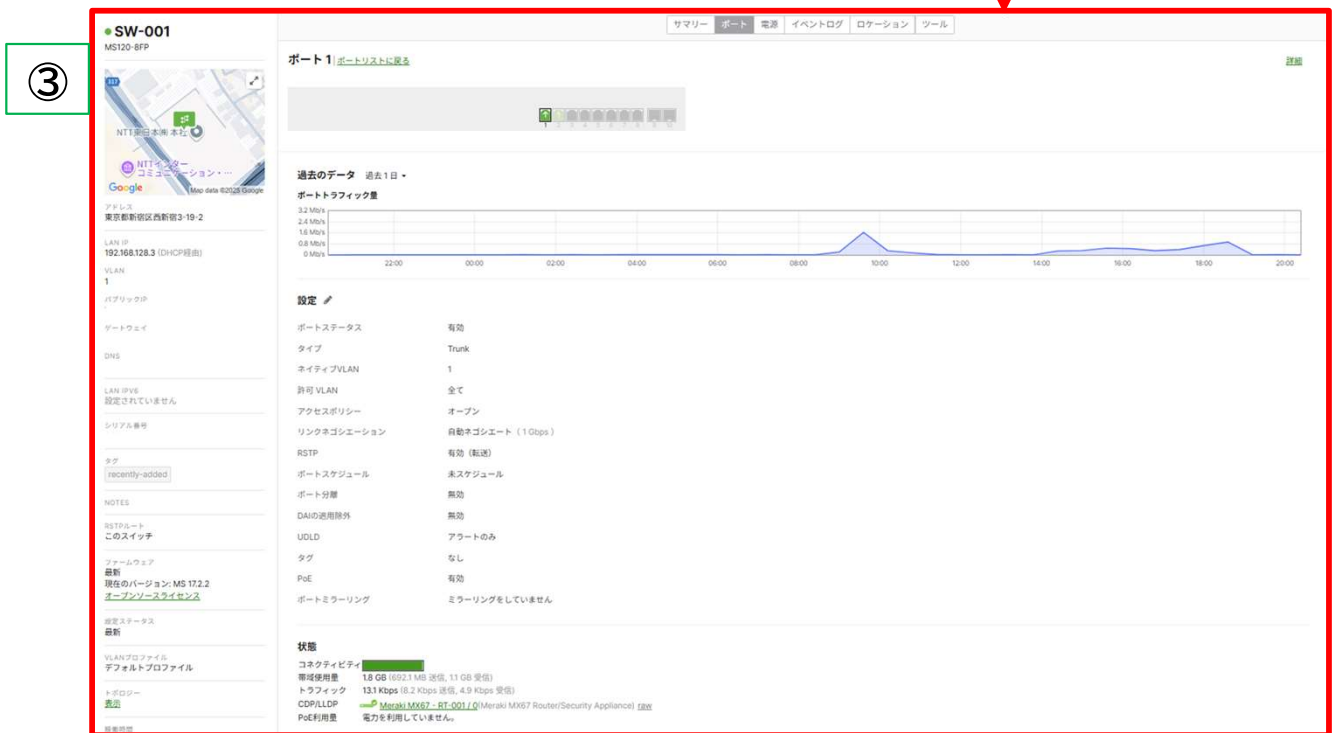
(※) 機器のオンライン状況はネットワーク機器が管理クラウドと通信できているかで機器状態を判断しております。そのため、インターネットには接続できているが、管理クラウドとの通信に問題が発生した場合(クラウドサーバーの障害、システムメンテナンス、回線障害など)、ネットワーク機器が正常に稼動していても、異常と表示されることがあります。

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。



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
ロケーションアナリティクス	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スペクトラム	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。

ワイヤレス

監視 **アクセスポイント** ✓

設定 SSID
Air Marshal アクセス制御
ロケーションアナリティクス ファイアーウォール&トラ
ス

一覧 ヘルス マップ 接続ログ タイムライン

アクセスポイントが1台、オフラインになっている場合は「1オフライン」と表示されます。正常時はオンラインにカウントされます。

0 オフライン 0 アラート 1 オンライン 0 リピーター

検索 フィルタ 1 result ダウンロード

名前	MACアドレス	シリアル番号	状態	ローカルIP	Meraki Cloud 接続性 (UTC+9)
AP-001	2c:3		●	192.168.128.4	

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)

1ページあたりの行数 100 < 1 >

・ 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

確認したい期間を指定します。
(過去2時間、過去1日、過去1週間)

ワイヤレス概要 過去2時間

接続ヘルス ①

非常に良い

接続失敗したクライアント 4/29 変化なし

接続までの時間 0.77 s -2.16 s
期待値 < 5秒

平均ローミング時間 0.47 s -0.76 s
期待値 < 3秒

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%

指定した期間内で発生した接続の失敗数/成功数を表示

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Vをクリックすると、より細かい情報が確認可能です。

・ 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。

パフォーマンスヘルス ⓘ



遅延
なし

パケットロス

3% ↗ 1%

期待値 3% ~ 5%

シグナル品質 (SNR)

39 dB 変化なし

期待値 > 27 dB

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、V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。

ネットワークサービスヘルス ⓘ



RADIUS 成功率
なし

DHCP 成功率

100% 変化なし

DNS 成功率

100% ↗ 7%

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。

・ 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

ロケーションアナリティクスでは、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」-「ロケーションアナリティクス」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。

ロケーション分析 過去1週間 0001 - wireless



高度な利用

高度な利用

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

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。

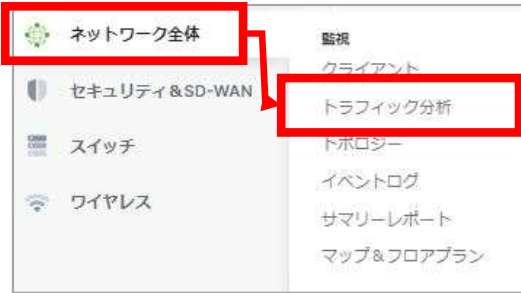
また、これらの分析や診断についてもサポートセンターで支援していますので、記載されている内容が「難しい」と感じる方はサポートセンターまでお問い合わせください。

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。

期間を指定します。
(過去2時間、1日、1週間、30日間)

トラフィック分析 アクセスポイント: 過去1日 全てのSSID上

① クライアントカウント 一意なクライアント: 約6台

② 帯域使用量 1.18 GB (↓ 964.3 MB, ↑ 239.1 MB)

③

アプリケーション	宛先	プロトコル	ポート番号	使用率%	帯域使用量	送信済み	受信済み	フロー	アクティブ時間	クライアント数
DTLS	-	-	-	84.6%	1018.2 MB	209.6 MB	808.6 MB	3	2.5 hours	2
Encrypted TCP (SSL)	-	TCP	443	7.4%	88.7 MB	16.1 MB	72.6 MB	789	2.2 hours	1
Statistical Peer-To-Peer	-	-	-	4.1%	49.8 MB	6.2 MB	43.5 MB	2	52 minutes	1
Unknown	-	-	-	3.4%	40.5 MB	6.1 MB	34.4 MB	148	1.4 hours	2
Microsoft Services	-	-	-	0.3%	3.2 MB	890 KB	2.3 MB	127	16 minutes	4
Statistical Conference Audio	-	-	-	0.1%	1.7 MB	211 KB	1.5 MB	1	10 minutes	1
Microsoft Windows Update Service	-	-	-	0.1%	1.3 MB	23 KB	1.3 MB	3	60 seconds	1
7 合計										

*総ネットワークトラフィックの0.1%未満の宛先への通信は除外されます

[レポートをCSV形式でダウンロードする](#)

アプリケーションをクリックすると、どんなアプリケーション七日の説明とどのクライアントが使用していたのか詳細情報が確認できます。

● 通信診断ツールで通信不調の原因を調査する

各機器（ルーター装置・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。

■ ルーター装置の場合

The screenshot shows the router configuration interface. On the left, the 'セキュリティ & SD-WAN' menu is highlighted. Under the '監視' (Monitoring) section, 'アプライアンスステータス' (Appliance Status) is selected. On the right, the 'RT-001' device page is shown, with the 'ツール' (Tools) tab highlighted in the top navigation bar.

■ アクセスポイントの場合

The screenshot shows the access point management interface. On the left, the 'ワイヤレス' (Wireless) menu is highlighted, and 'アクセスポイント' (Access Point) is selected under '監視'. On the right, the 'AP-001' device page is shown, with the 'ツール' (Tools) tab highlighted. Below, a table lists access points, with 'AP-001' selected. A callout box says '一覧から確認対象のアクセスポイントをクリック' (Click the access point to be checked from the list).

■ スイッチの場合

The screenshot shows the switch configuration interface. On the left, the 'スイッチ' (Switch) menu is highlighted, and 'スイッチ' (Switch) is selected under '監視'. On the right, the 'SW-001' device page is shown, with the 'ツール' (Tools) tab highlighted. Below, a table lists switches, with 'SW-001' selected. A callout box says '一覧から確認対象のスイッチをクリック' (Click the switch to be checked from the list).

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ルーター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効です。

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効です。

213.5 Mbps

• 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。（ルーター装置、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。

トレースルート icmp.canireachthe.net 期間 Internet 1

宛先指定

```

traceroute to icmp.canireachthe.net (209.206.55.10), 30 hops max, 38 byte packets
 1  [redacted] 2.357 ms 1.996 ms 1.891 ms
 2  [redacted] 2.865 ms 8.111 ms 8.016 ms
 3  [redacted] 9.010 ms 5.085 ms 4.992 ms
 4  [redacted] 6.078 ms 7.380 ms 7.606 ms
 5  [redacted] 7.292 ms 8.025 ms 8.033 ms
 6  [redacted] 7.967 ms 27.86.44.177 (27.86.44.177) 19.350 ms 27.85.230.49 (27.85.230.49) 17.763 ms
 7  [redacted] 12.149 ms 27.85.227.105 (27.85.227.105) 6.184 ms 9.616 ms
 8  [redacted] 60.245 ms 17.134 ms 27.85.128.174 (27.85.128.174) 8.606 ms
 9  [redacted] 26.605 ms 29.277 ms 26.267 ms
10  [redacted] 32.058 ms 37.343 ms 31.086 ms
11  [redacted] 99.014 ms 94.756 ms 103.314 ms
12  [redacted] 93.516 ms 94.231 ms 91.871 ms
13  [redacted] 93.061 ms 94.047 ms 115.962 ms
14 icmp.meraki.com (209.206.55.10) 109.705 ms 94.540 ms 93.438 ms
    
```

経由機器一覧

- MTR:宛先までの経路を確認できます。（ルーター装置、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。

MTR icmp.canireachthe.net サイクル数: 1 インタフェース: インターネット1

宛先指定

ホスト	損失%	Snt	最終	平均	問題無	RTT
1. [redacted]	0	1	4.1	4.1	4.1	4.1
2. [redacted]	0	1	2.2	2.2	2.2	2.2
3. [redacted]	0	1	4.5	4.5	4.5	4.5
4. [redacted]	0	1	4.1	4.1	4.1	4.1
5. [redacted]	0	1	3.7	3.7	3.7	3.7
6. [redacted]	0	1	5.5	5.5	5.5	5.5
7. [redacted]	0	1	9.1	9.1	9.1	9.1
8. [redacted]	0	1	4.6	4.6	4.6	4.6
9. [redacted]	0	1	3.9	3.9	3.9	3.9
10. [redacted]	0	1	12.6	12.6	12.6	12.6
11. [redacted]	0	1	92.0	92.0	92.0	92.0
12. [redacted]	0	1	92.1	92.1	92.1	92.1
13. [redacted]	0	1	91.1	91.1	91.1	91.1
14. [redacted]	0	1	96.4	96.4	96.4	96.4

経由機器一覧

- 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あります。

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。

ケーブルテスト 警告：本テストによってこのポートのトラフィックが中断される可能性があります。

3 ケーブルテストの実行

ポートに接続されたケーブルのテスト3 ✕

ポート番号	Linkネゴシエーション	長さ	状態	ヘア1	ヘア2	ヘア3	ヘア4
3	10Gdx	57.75 m	OK	ok	ok	ok	ok

- 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。

ポートの再起動 注意： PoE対応デバイスは一時的に電源がオフになります。

ポート 3

再起動

ポートの再起動 ✕

ポートの再起動が終了

- 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。

MAC転送テーブル 実行

MAC転送テーブル ✕

フィルタ条件:

MACアドレス数: 4

MAC	ポート番号	VLAN
98:18:88:0d:27:70	1	222
e0:cb:bc:89:d4:0d	3	1
a4:2a:95:1d:bc:a1	1	222
98:18:88:0d:27:70	1	1

- スイッチに接続されたクライアントの遠隔起動 Wake on LAN

➤ クライアントの遠隔起動

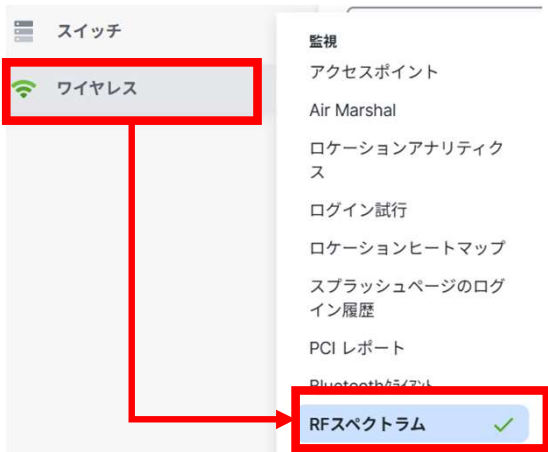
スリープ中の機器を遠隔で起動させることができます。起動させたい機器のMACアドレス、VLAN IDを指定します。(スイッチに接続されていない機器を起動させることはできません。)

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。

クライアントのスリープ解除	このツールでは、クライアントのスリープを解除するためのWake On LAN信号を送信します。ターゲットクライアントでもWake On LANを有効にしている必要があります。			
MAC:	<input type="text" value="eg. 00:11:22:33:44:55"/>	VLAN:	<input type="text" value="eg. 123"/>	<input type="button" value="送信"/>
クライアントの遠隔起動	このツールでは、クライアントのスリープを解除するためのWake On LAN信号を送信します。ターゲットクライアントでもWake On LANを有効にしている必要があります。			
MAC:	<input type="text" value="eg. 00:11:22:33:44:55"/>	VLAN:	<input type="text" value="eg. 123"/>	<input type="button" value="送信"/>

• アクセスポイント周辺のチャンネル利用率を確認する

- 「RFスペクトラム」では、アクセスポイント周辺の電波状況やチャン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、チャン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スペクトラム」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ンネル、2.4GHz/5GHzの平均チャン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。



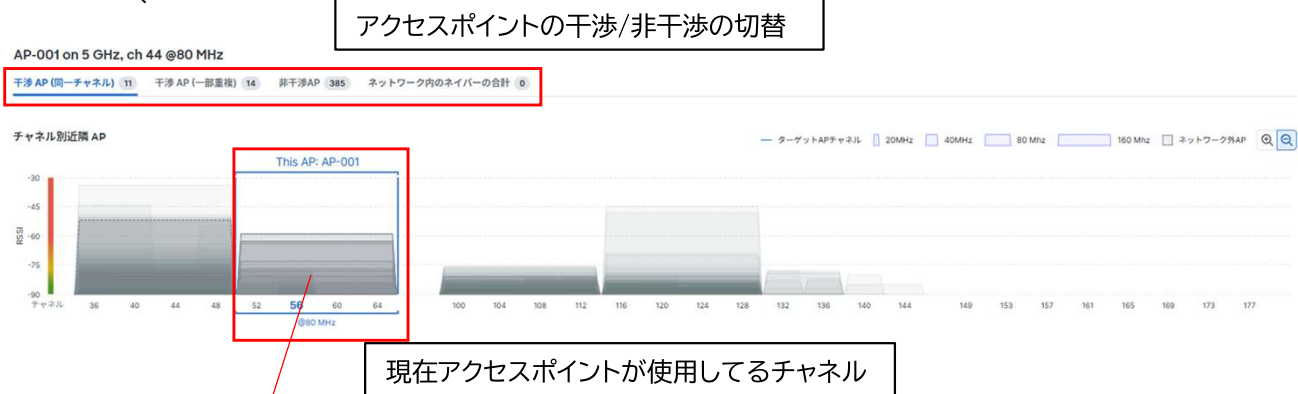
項目名	内容
名前	APの名称
使用チャンネル	アクセスポイントが現在使用しているチャンネルと範囲
平均チャンネル使用率 (2.4GHz)(5GHz)(6GHz)	帯域毎に過去80秒間の平均チャンネル使用率とパケットロス率を表示 ・チャンネル使用率(水色+グレーがチャンネル全体の使用率) 水色:自身のAPチャンネル使用率 グレー:近隣ネットワークのチャンネル使用率 ・パケットロス 赤:15%超、黄:5%以上15%未満、緑:5%未満

• アクセスポイント周辺のチャン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ンネルごとの使用率、周辺の機器が送波しているSSID名や信号強度、使用しているチャンネルを確認することができます。



➤ 各チャンネルの使用率の棒グラフが表示されます。
 青枠が現在のAPが動作しているチャンネル番号、チャンネル幅が測定毎に更新されます。
 グレーのグラフはネットワーク外のAPのチャンネル使用率が表示されます。
 (濃いグレー程ネットワーク外のAPの数が多いことを示しています)。
 値RSSI(dBm)は低いほど優れています。



カーソルを合わせるネットワーク外のアクセスポイントごとのチャンネル毎の干渉レベルが確認できます。

低干渉	
Ch	128
RSSI	- 87 dBm
SSID	

Moderate Interference	
Ch	116
RSSI	- 47 dBm
SSID	

高干渉	
Ch	120
RSSI	- 45 dBm
SSID	

• 周辺のネットワーク外アクセスポイントの利用チャンネルを干渉状況を確認する

➤ アクセスポイント毎の詳細画面では各チャンネルごとの使用率、周辺の機器が送波しているSSID名や信号強度、使用しているチャン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ネットワーク外のアクセスポイントが利用している利用チャンネル、干渉レベル、dBmの値が確認可能です。

#	干渉	AP ネイバー	RSSI (dBm)	Ch	Ch使用率	アクティブクライアント数	送信出力 (dBm)	SSID
1	● 同-ch	42:9	-59	64 (80 MHz)	—%	0		
2	● 同-ch	38:9	-59	64 (80 MHz)	—%	0		
3	● 同-ch	00:2	-63	52 (80 MHz)	—%	0		
4	● 同-ch	00:2	-65	52 (80 MHz)	—%	0		
5	● 同-ch	00:2	-65	52 (80 MHz)	—%	0		
6	● 同-ch	48:e:	-73	64 (80 MHz)	—%	0		
7	● 同-ch	0e:1	-77	56 (80 MHz)	—%	0		
8	● 同-ch	08:1	-78	56 (80 MHz)	—%	0		
9	● 同-ch	e4:e	-83	56 (80 MHz)	—%	0		
10	● 同-ch	ec:6	-83	64 (80 MHz)	—%	0		
11	● 同-ch	34:3	-85	64 (80 MHz)	—%	0		

- ・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。

イベントログ アクセスポイント▼

AP: Any

表示するイベントタイプを指定:

検索 [フィルタのリセット](#)

ダウンロード▼ [AIで要約する](#)

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

Catalystスイッチ:Catalystスイッチ向け
(Catalystスイッチは提供していない機器となります)

※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

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。

イベントログ アクセスポイント

AP: Any クライアント: User1-Macbook 次の日時より前: 11/19/2025 17:00

表示するイベントタイプを指定: All 除外するイベントタイプを指定: None

検索 [フィルタのリセット](#)

←ダウンロードをクリックすると、表示中のログをCSVでダウンロードできます。

ダウンロード [AIで要約する](#)

時刻(JST)	アクセスポイント	SSID	クライアント	カテゴリ	イベントタイプ	詳細
Nov 19 16:58:12	AP-001	0000Gigaraku	User1-Macbook	802.11	802.11ディスアソシエーション	client has left AP
Nov 19 16:57:46	AP-001	0000Gigaraku	User1-Macbook	WPA	WPA認証	radio: 1, vap: 1, client_mac: 6A
Nov 19 16:57:46	AP-001	0000Gigaraku	User1-Macbook	802.11	802.11アソシエーション	channel: 44, rssi: 27

① ② ③ ④ ⑤ ⑥ ⑦

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	カテゴリ	イベントタイプをグループ化した情報。
⑥	イベントタイプ	発生したイベントタイプ。
⑦	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

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。

■ 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: invalidated DH group 19. msg: invalidated 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AuthIPsec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]- xxxxxx[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、Type-Cルーター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。(上位他社ルーターや、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。

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

ダウンロード ▾	AI で要約する					
時刻(JST) ▾	アクセスポイント	SSID	クライアント	カテゴリ	イベントタイプ	詳細
Nov 19 16:58:12	AP-001	0000Gigaraku	User1-Macbook	802.11 ③	802.11ディスアソシエーション	client has left AP
Nov 19 16:57:46	AP-001	0000Gigaraku	User1-Macbook	WPA ②	WPA認証	radio: 1, vap: 1, client_mac: 6A:
Nov 19 16:57:46	AP-001	0000Gigaraku	User1-Macbook	802.11 ①	802.11アソシエーション	channel: 44, rssi: 27

	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ンネル(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。

■ 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」発生時は他のチャン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)へチャンネルを変更する等の検討が必要となります。

イベントログ アクセスポイント▼

AP: Any クライアント: すべて 次の日時より前: 11/11/2025 20:10 (JST)

表示するイベントタイプを指定: DFS event detected x 除外するイベントタイプを指定: None

検索 フィルタのリセット

ダウンロード▼ AIで要約する [Newer](#) [Older](#)

時刻(JST)▼	アクセスポイント	SSID	クライアント	カテゴリ	イベントタイプ	詳細
Nov 11 19:29:26	AP-001			DFS	DFSイベントを検出しました	band: 5, channel: 64, radio: 1
Nov 11 11:14:45	AP-001			DFS	DFSイベントを検出しました	band: 5, channel: 56, radio: 1

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ンネル) 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。