

Cisco Meraki セキュリティアプライアンス

MX84 / MX100 / MX250 / MX450

つなぎかたガイド

== STEP 1 ==

同梱物を確認しよう

== STEP 2 ==

接続して、電源を入れよう

== STEP 3 ==

アカウントを作り、Webページにアクセスしよう

== STEP 4 ==

基本設定を行おう

== STEP 5 ==

ファイアウォールの設定を行おう

== TIPS ==

Cisco Meraki MXがクラウドとうまく接続できないとき



STEP 1

同梱物を確認しよう

Cisco Meraki MX のパッケージには、次のものが同梱されています。
不足などないか、確認しましょう。

MX84/MX100/MX250/MX450の同梱物

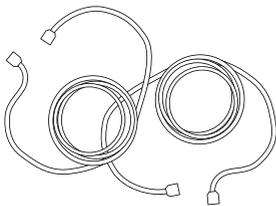
- ① Cisco Meraki MX セキュリティアプライアンス本体 1 台
- ② LAN ケーブル(カテゴリ6) 2 本
- ③ 電源ケーブル 1 本(MX250/MX450は2本)[※]
- ④ ラックマウント用ケージナット、ネジ(MX84/MX100/MX250/MX450)

※MXパッケージ購入時に電源ケーブルも別途購入いただく必要がございます。

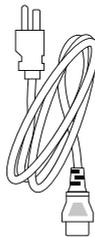
1



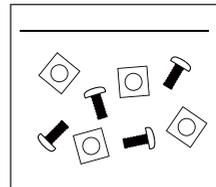
2



3



4



STEP 2

接続して、電源を入れよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

①

Cisco Meraki MX に電源ケーブルを接続し、起動させます。

※MX84、MX100、MX250、MX450 は電源コード差し込みだけで起動します。



②

LAN ケーブルを用いて、Cisco Meraki MX 設定用パソコン(ノート PC など)と、Cisco Meraki MX の Management ポートを接続します。

カチッと音がするまで差し込みます。

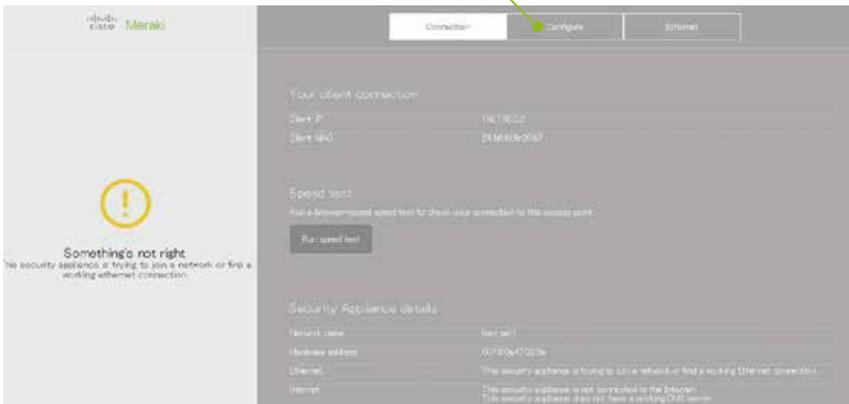


③

パソコン上のWeb ブラウザを起動し、アドレス欄に「<http://setup.meraki.com>」と入力して、Cisco Meraki MX へアクセスします。

④

アクセスすると以下の画面が表示されるので、**Configure** をクリックします。



STEP 2

接続して、電源を入れよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

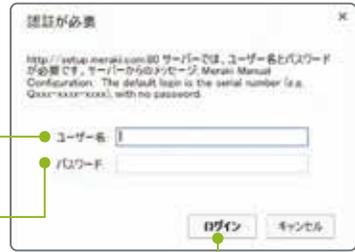
⑤

右の認証プロンプト画面が表示されます。

【ユーザー名】欄にCisco Meraki MXのシリアル番号(「Qxxx-xxxx-xxxx」形式)を入力します。

【パスワード】は入力不要です。

【ユーザー名】欄を入力したら、【ログイン】ボタンをクリックします。

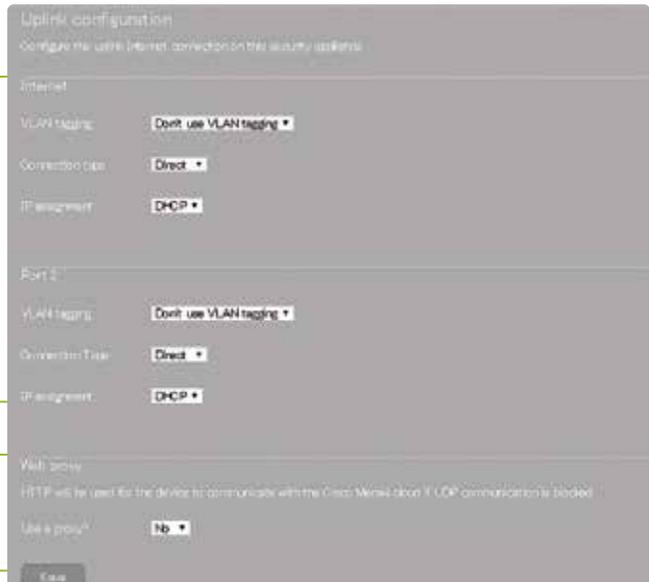


⑥

【Uplink Configuration】の各項目を設定します。

A

B



STEP 2

接続して、電源を入れよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

A 【Internet】、【Port 2】の設定

【VLAN tagging】

VLAN タグを入れる場合は
【Use VLAN tagging】を選択し、
【VLAN ID】を入力します。



【Connection type】

【PPPoE】または
それ以外（【Direct】）を選択します。



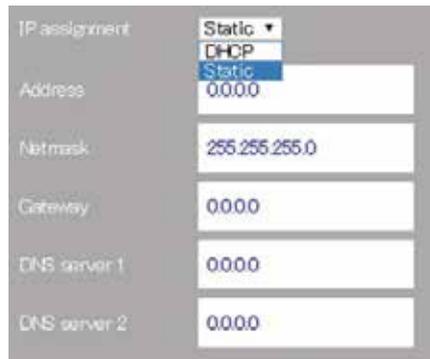
【Connection Type】が【PPPoE】の場合

- ▶ 【Authentication】: 認証の有無
- ▶ 【Use authentication】の場合
 【Username】(ID)
 【Password】
 【IP assignment】
 【Static】または【Dynamic】



【Connection Type】が【Direct】の場合

- ▶ 【IP assignment】:
 【DHCP】または、【Static】(静的)
- ▶ 【Static】の場合以下を設定します:
 【Address】: IP アドレス
 【Netmask】
 【Gateway】
 【DNS server1】
 【DNS server2】(任意)



STEP 2

接続して、電源を入れよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

B 【Web proxy】の設定 (オプション)

※Web プロキシを使わないとインターネットにアクセスできない環境の場合、こちらの設定をします。この設定により、Cisco Meraki MX とMeraki クラウドの通信が可能となります。

【Use a proxy?】

使用する場合は【Yes】を選択し、以下も確認します。

【Hostname or IP】(プロキシサーバーのホスト名またはIP アドレス)

【Port】(プロキシサーバーのポート)

【Authentication】(プロキシサーバーの認証の有無)

➤ 【Use authentication】(認証有)を選択した場合は以下も設定します：

【Username】

【Password】

Web proxy

HTTP will be used for the device to communicate with the Cisco Meraki cloud if UDP communication is blocked

Use a proxy? Yes ▾

Hostname or IP 0.0.0.0

Port Port #

Authentication Use authentication ▾

Username Username

Password Password

STEP 2

接続して、電源を入れよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

⑦

Cisco Meraki MX のInternet ポートとブロードバンドモデム (CATV モデム、ONU など) のLAN ポートなどをLANケーブルを用いて接続します。

カチッと音がするまで差し込みます。



⑧

Cisco Meraki MX のPower ランプが【Ready】状態になるまで待ちます。

MX84/MX100/MX250/MX450
橙⇒(電源ON、クラウドに未接続)
様々な色に交互に点灯⇒(クラウドに接続中)
白⇒(クラウド接続済み【Ready】)



STEP 3

アカウントを作り、Web ページにアクセスしよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

- ①
パソコンを起動します。
- ②
Web ブラウザを起動し、アドレス欄に次のURL を入力して、ページにアクセスします。
https://account.meraki.com/secure/login/dashboard_login

- ③
アクセスすると右の画面が表示されるので、
【Create an account】 をクリックします。

Dashboard Login

Email

Password

Stay logged in

[Forgot my password](#) [Create an account](#)

- ④
アカウントを作成します。

メールアドレスを入力します。

自分の名前を入力します。(アルファベット)

ログインするときに必要な
パスワードを入力します。

上記と同じパスワードを入力します。

自分の会社名を入力します。

Create a new Meraki Dashboard account

Email Available

Full Name

Password

Confirm password

Company

Address

Region is

Enter the words above:
Get another CAPTCHA
110

上に画像で表示されている数字を入力します。

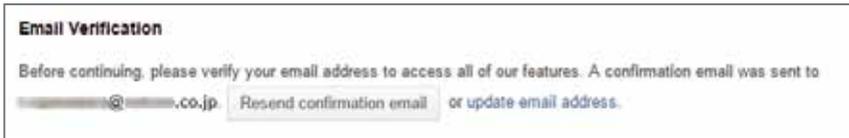
すべて入力できたら、クリックします。

STEP 3

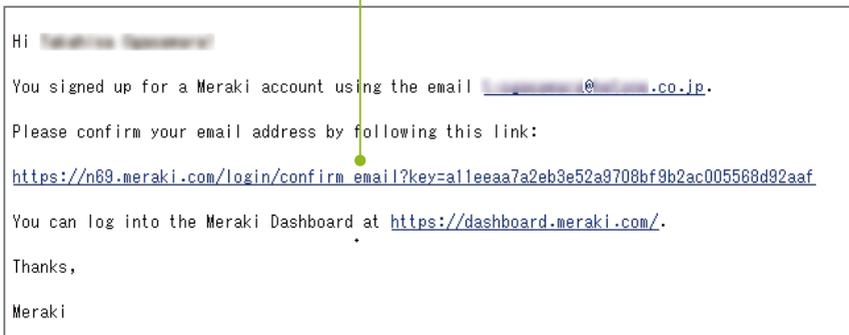
アカウントを作り、Web ページにアクセスしよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

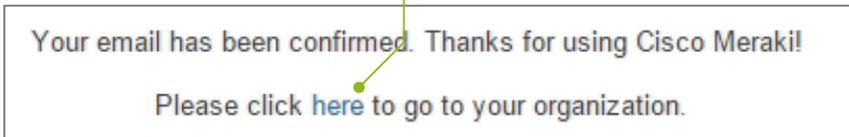
- ⑤
クリックすると以下の画面になります。
先ほど登録したメールアドレスにメールが送られているので、メールを確認しましょう。



- ⑥
送られてきたメールに記されている URL をクリックします。



- ⑦
クリックすると以下の画面に移ります。[here] をクリックします。



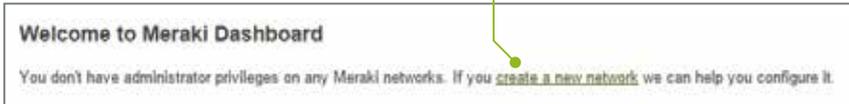
STEP 3

アカウントを作り、Web ページにアクセスしよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

⑧

以下の画面が表示されるので、**[create a new network]** をクリックします。



⑨

続いて、以下のページが表示されます。必要な項目を入力しましょう。

任意のネットワークの名前を入力します。

Security appliance を選択します。

登録する機器のシリアル番号を入力します。

シリアル番号を入力後、クリックします。

The screenshot shows the "Create network" form. It includes a "Name" field with "Meraki switch" entered. Under "Network type", "Security appliance" is selected. The "Devices" section has a "Search devices" field and a "Claim" button. A "Create network" button is at the bottom. Green callout boxes with pointers indicate where to enter the network name, select the network type, and enter device serial numbers.

STEP 3

アカウントを作り、Web ページにアクセスしよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

⑩

シリアル番号を入力後、**[Claim]** ボタンをクリックすると対象機器が追加されます。追加されたことを確認したら、**[Create network]** ボタンをクリックします。

Organization

Help

Create network

Name:

Network type:

- Wireless
- Security appliance
- Switch
- Combined hardware
- MDM
- VM concentrator

Devices: Add devices from your organization's inventory or add them using their serial/order number.
If multiple security appliances are selected, a separate network will be created for each. The networks will be given the name specified above with a number appended, e.g. "New network - 1", "New network - 2", "New network - 3".

<input checked="" type="checkbox"/>	MAC address	Serial number	Model	Claimed on	Order number	Country
<input checked="" type="checkbox"/>	00:10:5a:3a:3a:3a	0000000000000000	MX64V	5/16/2015 3:17 PM		JP

ライセンスを登録します。お手元にライセンスキー（12ケタ）をご用意ください。

①

Organization>License Infoをクリック



②

Add another licenseをクリック



STEP 3

アカウントを作り、Web ページにアクセスしよう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

③

Operation [License more device]の選択

※「Renew my Dashboard license」は
ライセンス更新時に利用します。



④

License key xxxx xxxx xxxx (12ケタ)の入力

⑤

Add Licenseのクリック

⑥

License History にライセンスが登録されます



※上記はMRシリーズのライセンス登録例。

⑪

画面左側 **【Security appliance】** を
クリックし、**【Monitor】**のところにある
【Appliance status】 をクリックします。



⑫

先ほど入力したシリアル番号に紐
づいている機器のStatusが緑に
なっており、Status欄にプロバイ
ダから払い出されたIPアドレス情
報などが表示されていることを確
認します。



※赤の場合は数分後、ブラウザの更新マークを押し、緑になることを確認します。

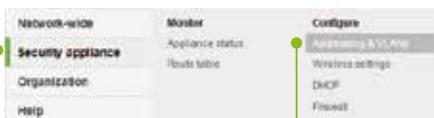
STEP 4

基本設定を行おう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

①

画面左側 **【Security appliance】** をクリックし、**【Configure】** のところにある **【Addressing & VLANs】** をクリックします。

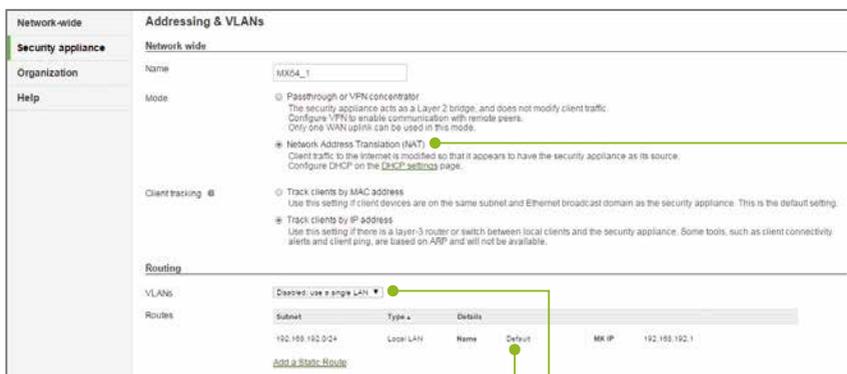


②

【Network wide】 の **【Mode】** で、**【Network Address Translation (NAT)】** が選択されていることを確認します。

→Cisco Meraki MX 自身からクライアント端末へDHCPを払い出す設定です。

※Cisco Meraki MX 上位にDHCP サーバーなどが配置されている場合は、**【Passthrough or VPN concentrator】**を選択し、Cisco Meraki MX のDHCP サーバー機能を有効にせず、パススルーモードで動作させることも可能です。



1 個以上 **【Subnet】** が割り振られていることを確認してください。
※当該行をクリックして **【Subnet】**、**【MX IP】** を任意のセグメント/アドレスに変更することが可能です。

【Disable: use a single LAN】 で OK です。
※複数のVLANを設定したい場合は、**【enable】** を選択してください。

設定変更した場合は、画面一番下の **【Save Changes】** ボタンをクリックして変更を反映してください。
これで、最低限の設定は完了です。
通常のルータとして使用可能となります。



STEP 4

基本設定を行おう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

③

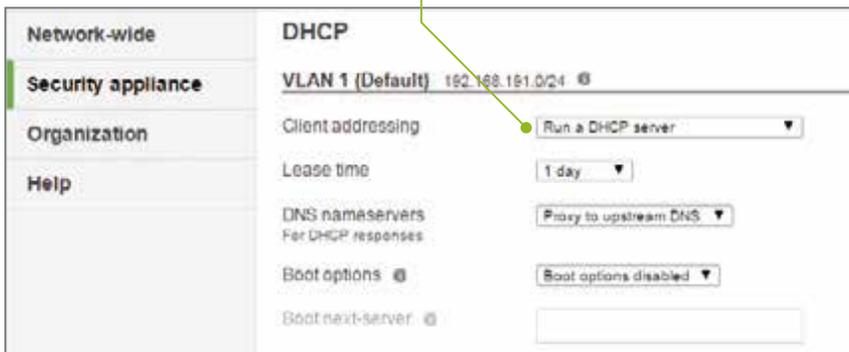
DHCP は初期設定で有効になっています。

画面左側 **【Security appliance】** をクリックし、**【Configure】**のところにある **【DHCP】** をクリックします。



④

【Client addressing】 に **【Run a DHCP server】** が設定されていることを確認してください。



⑤

クラウド上 (Web 画面) からの設定保存後、手元のCisco Meraki MX へ設定が反映されるまで1～2分ほどかかる場合があります。(クラウドとの接続断の際は反映されないのをご注意ください)

【Security appliance】 → **【Monitor】** → **【Appliance status】**画面で **【Configuration Status】**が **【Up to date】**になっていれば Web GUIで設定保存した項目はすべてCisco Meraki MX へ反映されています。



STEP 5

ファイアウォールの設定を行おう

実際にパソコンで表示される画面は、予告なく変更されることがあります。

①

画面左側【Security appliance】をクリックし、【Configure】 のところにある【Firewall】をクリックします。

②

Firewall の設定を行います。

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Hits	Actions
1	Deny	TCP	192.168.2.0/24	443	Any	443		0	Deny
2	Deny	TCP	192.168.2.0/24	Any	Any	443		0	Deny
	Allow	Any	Any	Any	Any	Any	Default rule	0	Allow

ICMP Ping

インターネット側からの Ping への応答可否を設定します。入力可能値は【None】、【Any】(すべて)、または応答するアドレス / アドレス範囲 (22.1.218.254.0/24 など) です。

Web local status & configuration

インターネット側から Cisco Meraki MX のローカル管理ページへのアクセス制御を設定します。設定値は ICMP Ping と同様です。

SNMP (SNMP 設定時のみ)

インターネット側からの SNMP ポーリングに対する応答可否を設定します。設定値は ICMP Ping と同様です。

通常のネットワーク機器と同様の方法で、Layer3 の Firewall rule (ACL) を追加します。

【Add a rule】をクリックすると、デフォルト設定である【Allow Any Any...】の上に行を挿入します。

【Cellular failover rules】は設定不要です。
(設定しても当該インターフェースがないため、適用されません)

制限するカテゴリ、サービス名をドロップダウンリストから選択します。特定の国への通信制限も可能です。

#	Policy	Application	Deny	Actions
1	Deny	No deny		Deny
2	Deny	Deny every		Deny

クリックして Layer7 の Firewall rule を追加します。

それぞれの項目の【Add ...】をクリックして、【Port forwarding】、【1:1 NAT】、【1:Many NAT】(PAT)、【Bourour forwarding】(VLAN 間) の設定を適宜実施してください。

#	Policy	Application	Deny	Actions
1	Deny	No deny		Deny
2	Deny	Deny every		Deny

最後に【Save Changes】をクリックして設定を保存します。

Cisco Meraki MXがクラウドとうまく接続できないとき

実際にパソコンで表示される画面は、予告なく変更されることがあります。

- ①
画面左側【Security appliance】をクリックし、【Monitor】のところにある【Appliance status】をクリックします。

Cisco Meraki MX がMeraki クラウドと接続できているか確認してください。ステータスアイコンが緑以外の場合は、何らかの通信障害により、Cisco Meraki MX がMeraki クラウドと接続できていません。



- ②
確認ポイント

- (1) ▶ ローカル管理画面上のインターネット接続設定
- (2) ▶ Firewall Info で提示されているポートの設定

- ③
確認方法

- (1) ▶ ローカル管理画面上のインターネット接続設定

ローカル管理画面に接続し、設定内容を再確認します。

「http://setup.meraki.com」と入力してCisco Meraki MX へアクセスし、

【Configure】をクリックします。

プロバイダなどから提示された情報（ID、パスワードなど）と比較し、項目が正しく設定されているか再確認してください。

※項目の詳細は4～5ページを参照ください。



Cisco Meraki MXがクラウドとうまく接続できないとき

実際にパソコンで表示される画面は、予告なく変更されることがあります。

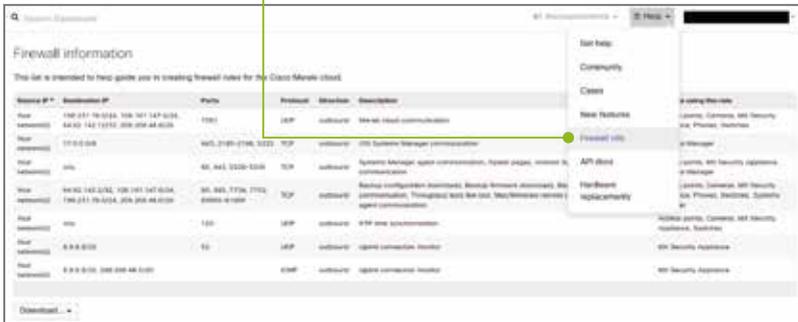
④

Firewall info で提示されているポートの設定

(2) ▶ Firewall info で提示されているポートの設定

もしCisco Meraki MX の外側に別製品のファイアウォールやスイッチ、ルータなどが設置してあり、通信を制御している場合は、以下のとおりCisco Meraki MX がMeraki クラウドとの通信に必要なポートを閉じていないか確認してください。

画面左側【Help】の **Firewall info** をクリックします。



Outbound のみの表記となっていますが、上位の機器がステータフルなアクセスリスト制限設定が不可の場合は、Inbound も指定の IP、ポートを開く必要があります。



ネットワークパートナーズ株式会社
www.netone-pa.co.jp

本 社

〒100-7026 東京都千代田区丸の内2-7-2 JPタワー
TEL 03-6256-0700(代表)

西日本営業部

〒532-0003 大阪府大阪市淀川区宮原3-5-36 新大阪トラストタワー
TEL 06-6105-0356(代表)



[Facebook] <https://www.facebook.com/NetOnePartners>

>>> 島崎久子の耳寄り情報局 動画配信中 …… <http://www.netone-pa.co.jp/videos/>

>>> NOPエンジニア blog 公開中 …… <https://www.netone-pa.co.jp/blog/>

記載内容は予告なく変更することがありますのでご了承ください。
掲載している商品名、システム名、名称は、各社の商標、または登録商標です。