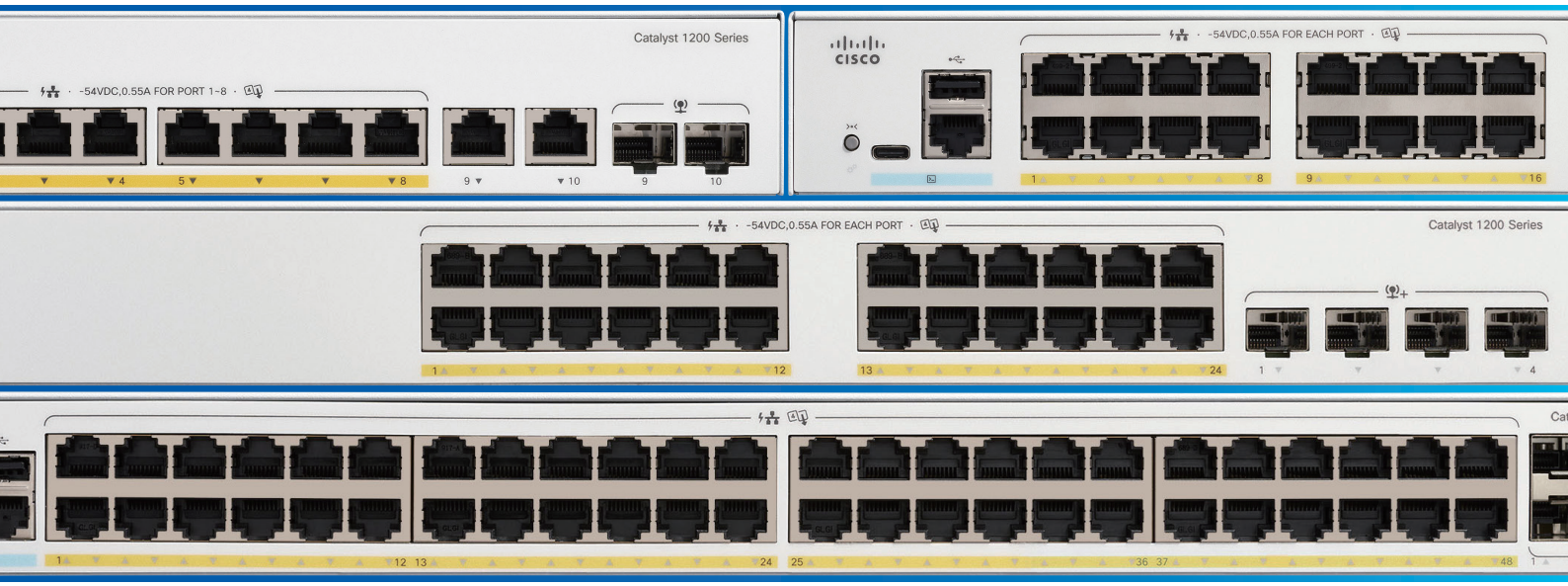
Cisco Catalyst 1200 シリーズ スマートスイッチ



――かんたんセットアップガイド――

Web インターフェイス基本編

本ガイドでは、スマートスイッチの接続から内蔵の Web インターフェイスによる初期セットアップまでを解説します。

1 スイッチをネットワークに接続する P04
2 Web インターフェイスにアクセスする P05
3 設定ウィザードを使用する P13

2024 年 1 月版

はじめに

Cisco Catalyst 1200 シリーズ スマートスイッチは、シスコならではのパフォーマンスと信頼性、セキュリティ、および中小企業のネットワークに必要十分な機能を兼ね備えたネットワーク基盤を、シンプルに構築および運用管理できるネットワークスイッチです。

- **パフォーマンス**

  全モデルが 1 ギガビットイーサネット（1GE）に対応、一部のモデルは 10 ギガビットイーサネット（10GE）にも対応しています。さらに PoE 給電対応モデルは全モデルが 1 ポートあたり 30 W の給電が可能な PoE+（802.3at）に対応、Wi-Fi 6 アクセスポイントなど最新のネットワーク機器のすっきり配線が可能です。

- **信頼性**

  国内外で数々の導入実績を誇る、安心と信頼のシスコ製品。万が一の障害時も、Web インターフェイスや Cisco Business Mobile アプリによるモニタリングで迅速に対応できます。

- **セキュリティ**

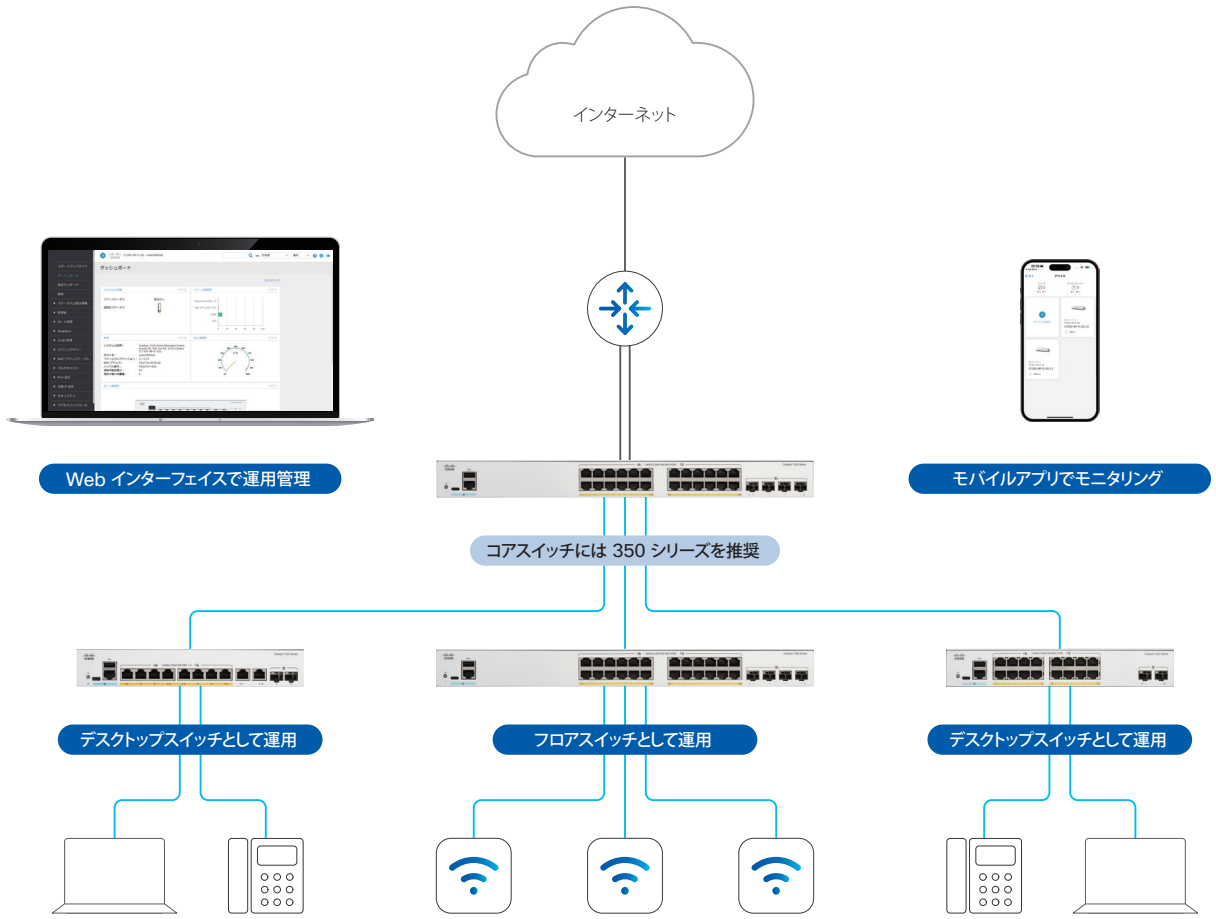
  ACL（アクセスコントロールリスト）など、ビジネスに必要不可欠なセキュリティを Web インターフェイスで簡単に設定できます。

- **中小企業のネットワークに必要不可欠な機能**

  レイヤ 3 スタティック（静的）ルーティングや VLAN など、中小企業のネットワーク構築に必要十分な機能を Web インターフェイスで簡単に設定できます。

- **シンプルに構築および運用管理**

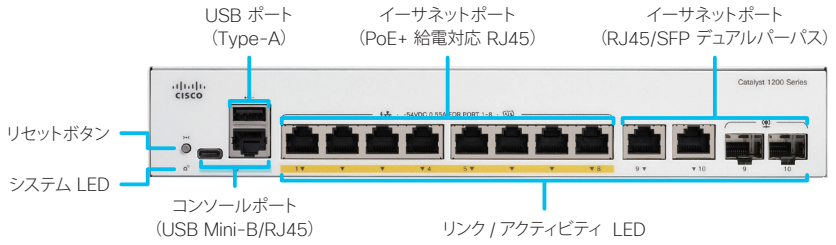
  つなぐだけで使用を開始できる、プラグアンドプレイスイッチとしても導入可能。Web インターフェイスでは、設定ウィザードによる簡単設定ときめ細やかな個別設定の両方をサポートします。さらに Cisco Business Mobile アプリを利用すれば、複数の Cisco Catalyst 1200/1300 シリーズ スイッチおよび Cisco Business 製品の簡易設定とモニタリングが可能です。



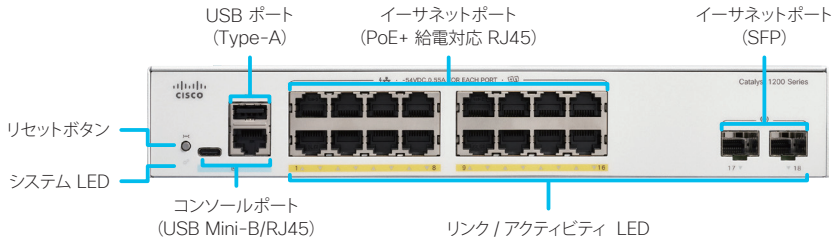
スマートスイッチの前面パネル

スマートスイッチの前面パネルには、ネットワーク機器や端末を接続するイーサネットポート、CLI（コマンドライン インターフェイス）でスマートスイッチを設定管理する場合に使用するコンソールポート、ファームウェアなど各種ファイルのストレージとして USB メモリを接続できる USB ポート、スイッチの状態を表示する LED、スイッチを再起動または工場出荷状態に戻す場合に使用するリセットボタンが配置されています。

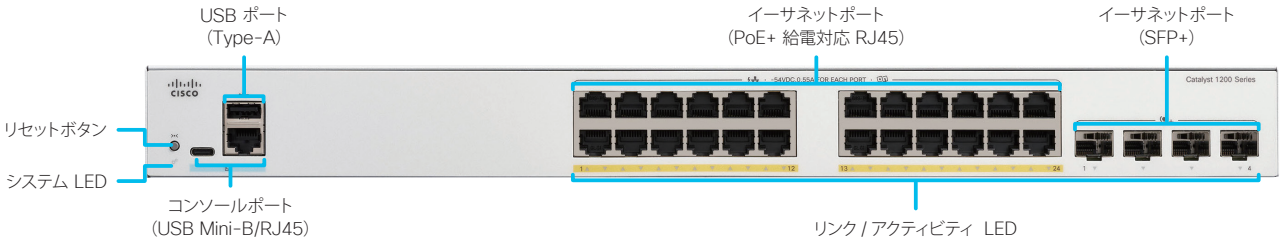
8 ポートモデル例（C1200-8P-E-2G）



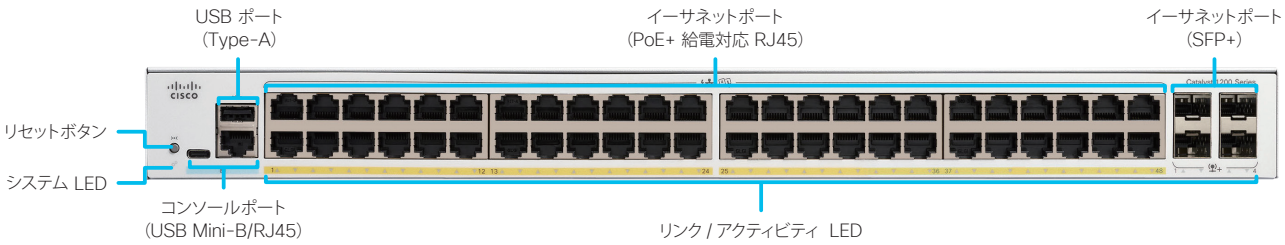
16 ポートモデル例（C1200-16FP-2G）



24 ポートモデル例（C1200-24FP-4X）



48 ポートモデル例（C1200-48P-4X）



LED 状態表示

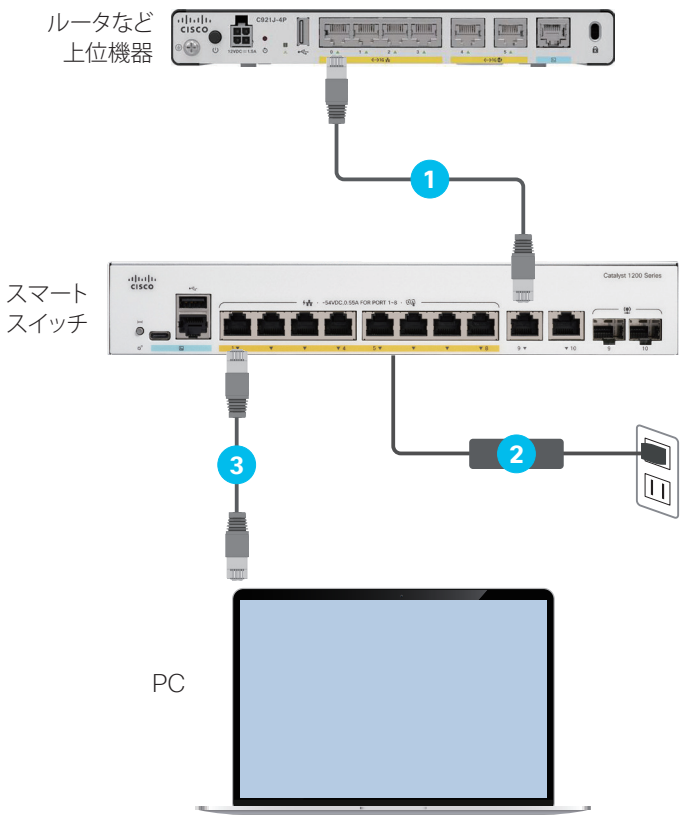
	システム LED	リンク / アクティビティ LED
緑色で点灯	IP アドレス取得済み	接続した機器 / 端末とリンクを確立
緑色で点滅	起動中、セルフテスト中、IP アドレス取得中	接続した機器 / 端末と通信中
オレンジ色で点滅	障害発生中	
消灯	電源 OFF	機器 / 端末と未接続、またはリンクを未確立

1 スイッチをネットワークに接続する

スマートスイッチをネットワークおよび電源に接続します。さらに、スマートスイッチ内蔵の Web インターフェイスにアクセスするために、必要に応じて PC を接続します。

注意

スマートスイッチをネットワーク（ルータなど上位機器）に接続するためのイーサネットケーブル、または SFP/SFP+ モジュールと光ファイバケーブルの組み合わせが必要です。
また、PC をスマートスイッチに接続するためのイーサネットケーブルも必要です。ただし、静的 IP アドレスの割り当てや MAC アドレスによる接続制限などがないシンプルなネットワーク構成の場合、Wi-Fi を含むネットワークに接続済みの PC から Web インターフェイスにアクセスすることができるため、PC をスマートスイッチに直接接続する必要はありません。



1 スマートスイッチをネットワークに接続

スマートスイッチは、イーサネットケーブル（LAN ケーブル、UTP ケーブル）、または SFP モジュールと光ファイバケーブルの組み合わせによる接続をサポートします。
通常は、スマートスイッチの RJ45 ポートとルータなど上位機器の RJ45 ポートをイーサネットケーブルを使用して接続します。
スマートスイッチでは PoE 非対応ポートの使用を推奨します。上位機器で使用すべきポートの詳細は、お使いの機器のマニュアルを参照してください。

2 スマートスイッチを電源に接続

付属の電源アダプタと電源ケーブルの組み合わせ、または付属の電源ケーブルを使用して接続します。
電源に接続したら、スマートスイッチ前面のシステム LED が緑色で点滅します。

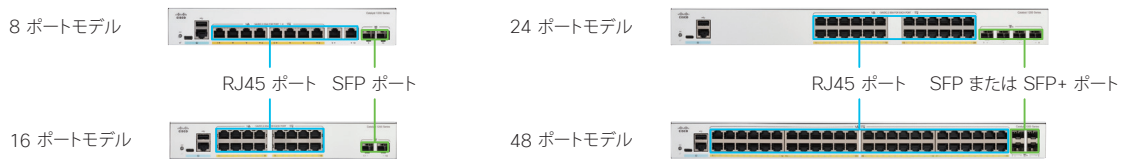
3 （必要に応じて）PC をスマートスイッチに接続

必要に応じて、PC の RJ45 ポートとスマートスイッチの RJ45 ポートをイーサネットケーブルを使用して接続します。

MEMO

スマートスイッチの前面には、2 種類のイーサネットポートがあります。[*1]

- **RJ45 ポート**：一般的なイーサネットケーブル（LAN ケーブル、UTP ケーブル）を接続
- **SFP または SFP+ ポート（モジュールスロット）**：SFP モジュールまたは SFP+ モジュールを装着

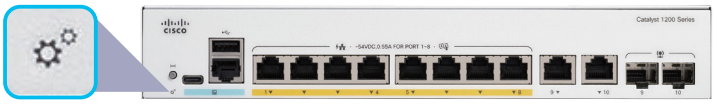


*1　8 ポートモデルの 9 番ポートおよび 10 番ポートは、RJ45 ポートと SFP ポートを組み合わせたデュアルパーパスポートです。RJ45 ポートと SFP ポートのどちらか一方だけを使用できます（同時使用不可）。

2 Web インターフェイスにアクセスする

スマートスイッチをネットワークに接続したら、PC のブラウザで内蔵の Web インターフェイスにアクセスします。前面のシステム LED の状態に応じて、アクセス方法（ブラウザのアドレスバーに入力する IP アドレス）が異なります。

- 2-1 Web インターフェイスにアクセスする（LED が緑色で点灯）
- 2-2 Web インターフェイスにアクセスする（LED が緑色で点滅）
- 2-3 Web インターフェイスにログインする



MEMO

2023 年 12 月現在、次のブラウザ（バージョン）による Web インターフェイスへのアクセスをサポートします。

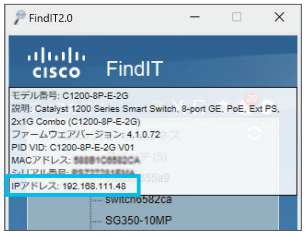
- Apple Safari（バージョン 14 以降）
- Google Chrome（バージョン 85 または 86 以降）
- Microsoft Edge
- Mozilla Firefox（バージョン 81 または 82 以降）

2-1 Web インターフェイスにアクセスする（LED が緑色で点灯）

スマートスイッチのシステム LED が緑色で点灯している場合は、ネットワークへの接続が完了しています。ルータなど上位機器（DHCP サーバー）がスマートスイッチに割り当てた IP アドレスを確認し、Web インターフェイスにアクセスします。マネージドスイッチに直接接続した PC だけでなく、Wi-Fi を含むネットワークに接続済みの PC からもアクセスすることができます。

IP アドレス確認例：シスコ ルータ

IP アドレス確認例：Meraki ダッシュボード



IP アドレス確認例：FindIT ネットワーク検出ユーティリティ

1 スマートスイッチの IP アドレスを確認

ルータなど上位機器（DHCP サーバー）がスマートスイッチに割り当てた IP アドレスを確認します。詳細は、お使いの機器のマニュアルを参照してください。

2 ブラウザのアドレスバーにスマートスイッチの IP アドレスを入力

ブラウザを起動して、1で確認した IP アドレスをアドレスバーに入力します。

3 ログイン画面を確認

Web インターフェイスのログイン画面が表示されたら、「**2-3 Web インターフェイスにログインする**」に進みます。

注意

ブラウザのセキュリティ設定などによって、Web インターフェイスのログイン画面ではなく、次の例のようなエラー画面や警告画面が表示される場合があります。

- Apple Safari：接続はプライベートではありません
- Google Chrome：この接続ではプライバシーが保護されません
- Microsoft Edge：接続がプライベートではありません
- Mozilla Firefox：警告：潜在的なセキュリティリスクあり

ログイン画面を表示するためには、それぞれのブラウザで次の手順を実行します。

- Apple Safari：［**詳細を表示**］＞［**この Web サイトを閲覧**］＞［**Web サイトを閲覧**］の順にクリック
- Google Chrome：［**詳細設定**］＞［***nnn.nnn.nnn.nnn* にアクセスする（安全ではありません）**］の順にクリック
- Microsoft Edge：［**詳細設定**］＞［***nnn.nnn.nnn.nnn* に進む（安全ではありません）**］の順にクリック
- Mozilla Firefox：［**詳細へ進む**］＞［**危険性を承知で続行**］の順にクリック

2-2 Web インターフェイスにアクセスする（LED が緑色で点滅）

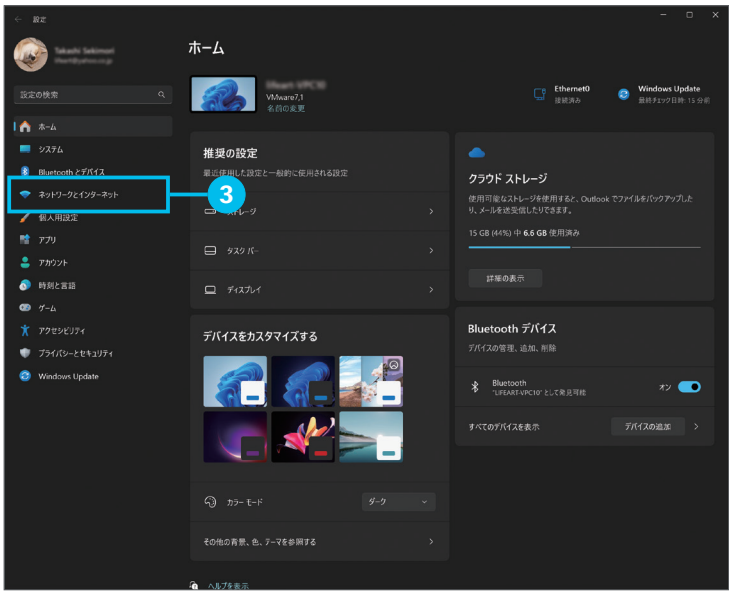
スマートスイッチのシステム LED が緑色で点滅している場合は、ネットワークへの接続が完了していません。IP アドレスの設定など、ネットワークに合わせてスマートスイッチを設定する必要があります。スマートスイッチに直接接続できるように PC のネットワーク設定を変更し、Web インターフェイスにアクセスします。

注意

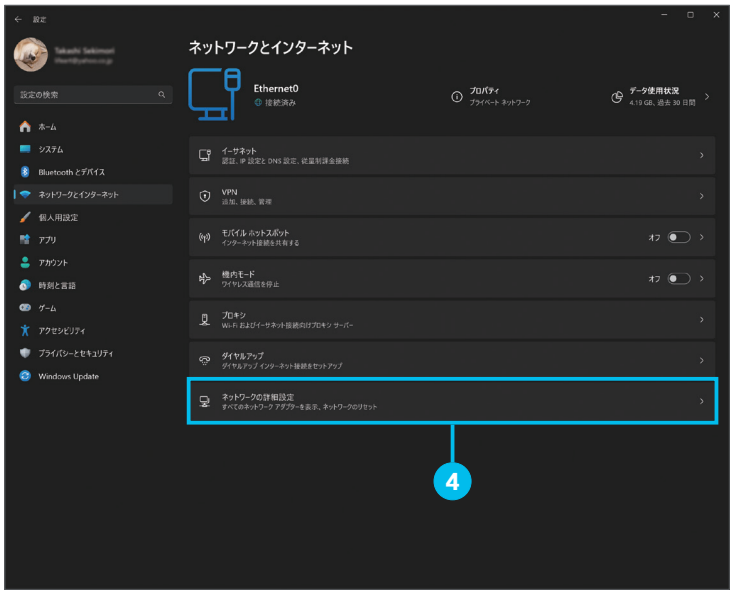
ネットワークへの接続が完了していない（IP アドレスが割り当てられていない）場合、スマートスイッチは工場出荷時のデフォルト IP アドレス「192.168.1.254」で動作します。スマートスイッチは DHCP サーバー機能をサポートしないため、スマートスイッチに直接接続している PC のネットワーク設定（IP アドレス）を「192.168.1.2」～「192.168.1.253」の範囲で設定する必要があります。本ガイドでは、Windows 11 バージョン 23H2 のネットワーク設定変更例を解説します。

1 ［**スタート**］メニューを右クリック

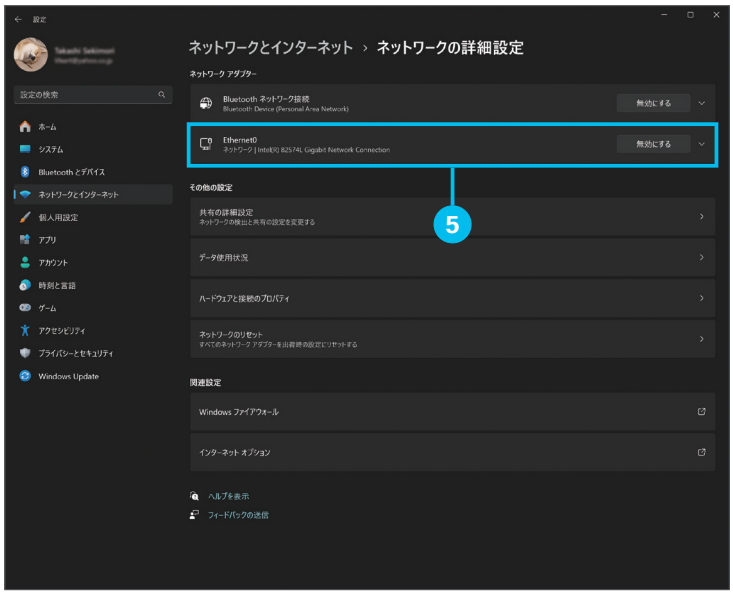
2 ［**設定**］をクリック



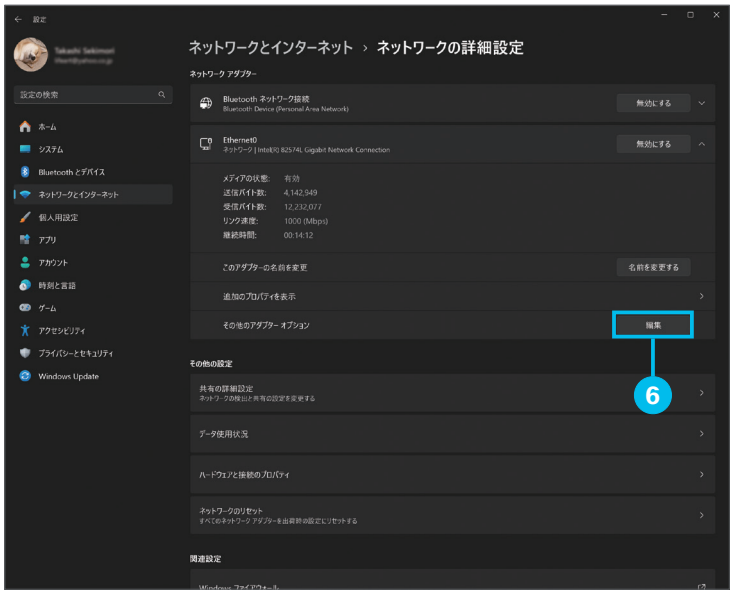
3 ［**ネットワークとインターネット**］をクリック



4 ［ネットワークの詳細設定］をクリック



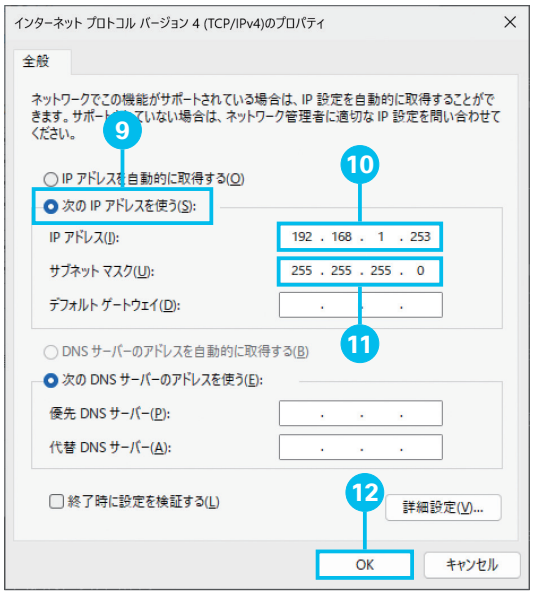
5 スマートスイッチへの接続に使用している
ネットワークアダプタをクリック



6 ［その他のアダプター オプション］の［編集］
をクリック

7 ［インターネット プロトコル バージョン 4 (TCP/IPv4)］をクリックして選択

8 ［プロパティ］をクリック



9 ［次の IP アドレスを使う］をクリック

10 ［IP アドレス］に「192.168.1.2」から「192.168.1.253」の範囲で任意の IP アドレスを入力

11 ［サブネット マスク］に「255.255.255.0」を入力

12 ［OK］をクリック

13 ［OK］をクリック

ネットワーク設定の変更が完了しました。

14 ブラウザのアドレスバーにスマートスイッチの IP アドレス「**192.168.1.254**」を入力

15 ログイン画面を確認

Web インターフェイスのログイン画面が表示されたら、「**2-3 Web インターフェイスにログインする**」に進みます。

注意

ブラウザのセキュリティ設定などによって、Web インターフェイスのログイン画面ではなく、次の例のようなエラー画面や警告画面が表示される場合があります。

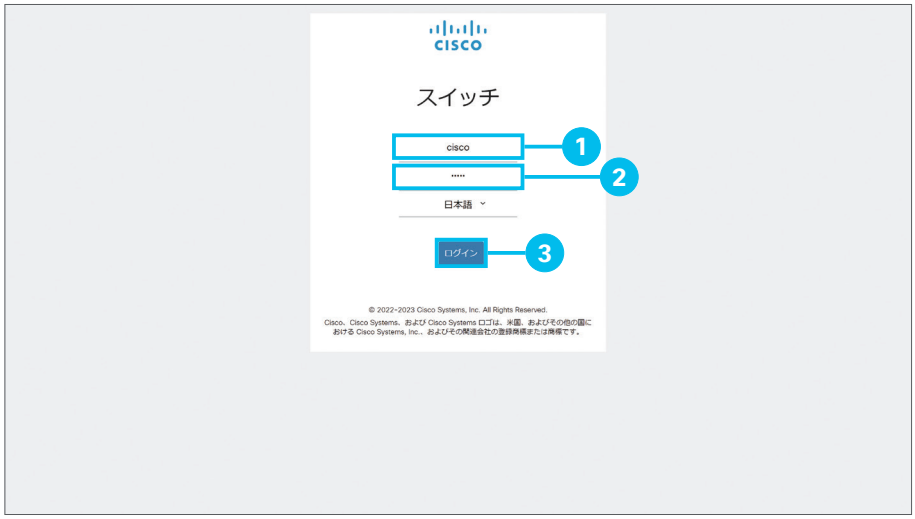
- Apple Safari：接続はプライベートではありません
- Google Chrome：この接続ではプライバシーが保護されません
- Microsoft Edge：接続がプライベートではありません
- Mozilla Firefox：警告：潜在的なセキュリティリスクあり

ログイン画面を表示するためには、それぞれのブラウザで次の手順を実行します。

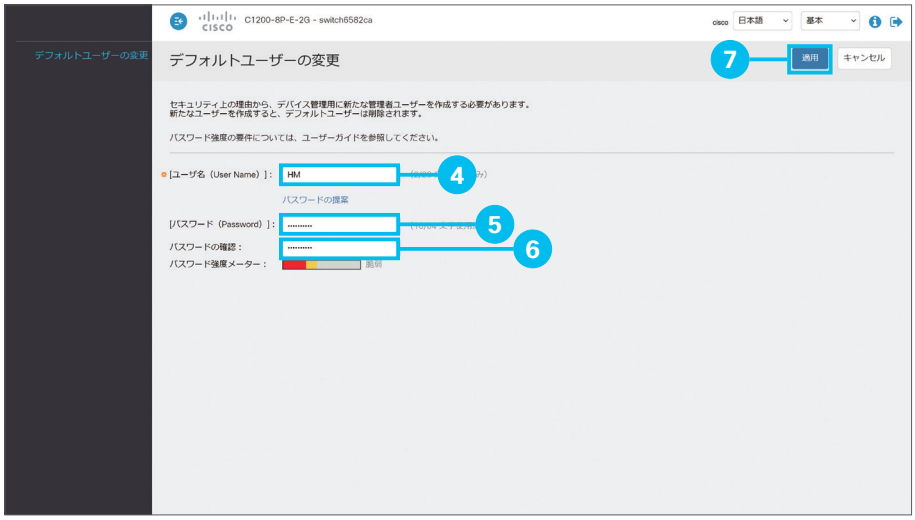
- Apple Safari：［**詳細を表示**］＞［**この Web サイトを閲覧**］＞［**Web サイトを閲覧**］の順にクリック
- Google Chrome：［**詳細設定**］＞［***nnn.nnn.nnn.nnn* にアクセスする（安全ではありません）**］の順にクリック
- Microsoft Edge：［**詳細設定**］＞［***nnn.nnn.nnn.nnn* に進む（安全ではありません）**］の順にクリック
- Mozilla Firefox：［**詳細へ進む**］＞［**危険性を承知で続行**］の順にクリック

2-3 Web インターフェイスにログインする

スマートスイッチの Web インターフェイスにアクセスしたら、デフォルトのユーザー名「cisco」とパスワード「cisco」を使ってログインします。初回ログイン時はデフォルトのユーザーアカウントを作成する必要があります。

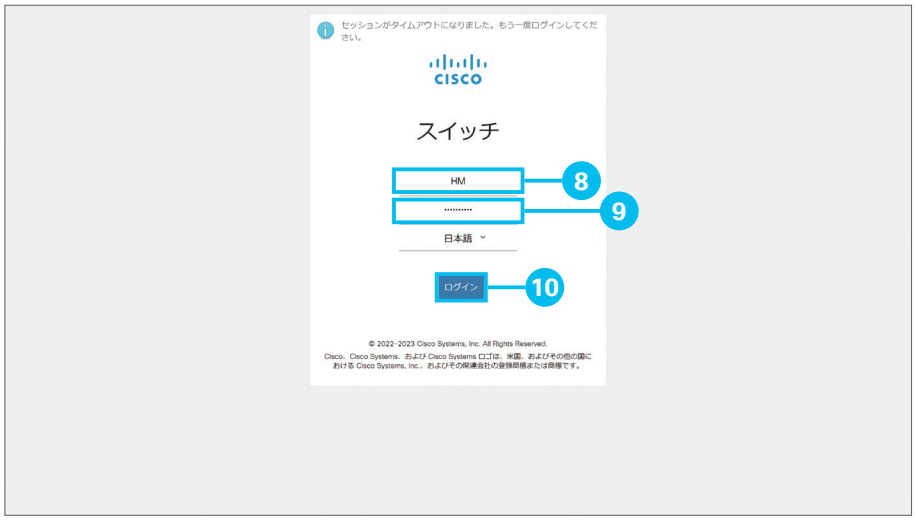


1. ［User Name］に「cisco」を入力
2. ［Password］に「cisco」を入力
3. ［**ログイン**］をクリック



4. ［**ユーザー名**］に任意の名前を入力
5. ［**パスワード**］に任意のパスワードを入力
6. ［**パスワードの確認**］に❺で入力したパスワードを入力
7. ［**適用**］をクリック

ユーザーアカウントの作成が完了しました。Web インターフェイスに再ログインします。



8 ［User Name］に5で入力したユーザー名を入力

9 ［Password］に6で入力したパスワードを入力

10 ［**ログイン**］をクリック

11 アイコンをクリック

スマートスイッチが起動時に読み込むスタートアップ設定ファイルに、作成したユーザーアカウント情報を保存します。

注意

保存せずにスマートスイッチを再起動すると、1からの手順をやり直す必要があります。

3 設定ウィザードを使用する

Web インターフェイスの「**設定ウィザード**」を使用して、スマートスイッチを初期設定します。次の 3 種類のウィザードを使用可能です。

- **3-1 開始ウィザードを使用する**：スマートスイッチの IP アドレス設定など、初期セットアップを実行できます。
- **3-2 VLAN 設定ウィザードを使用する**：部署別や目的別に LAN を分割する、VLAN（仮想 LAN）を設定できます。
- **3-3 ACL 設定ウィザードを使用する**：端末の MAC アドレスや IP アドレスに基づいてスイッチポートへの接続を許可またはブロックするなど、ACL（アクセスコントロールリスト）を設定できます。

設定ウィザードの使用は任意です。各ウィザードで設定可能な機能は、すべて個別に設定可能です。

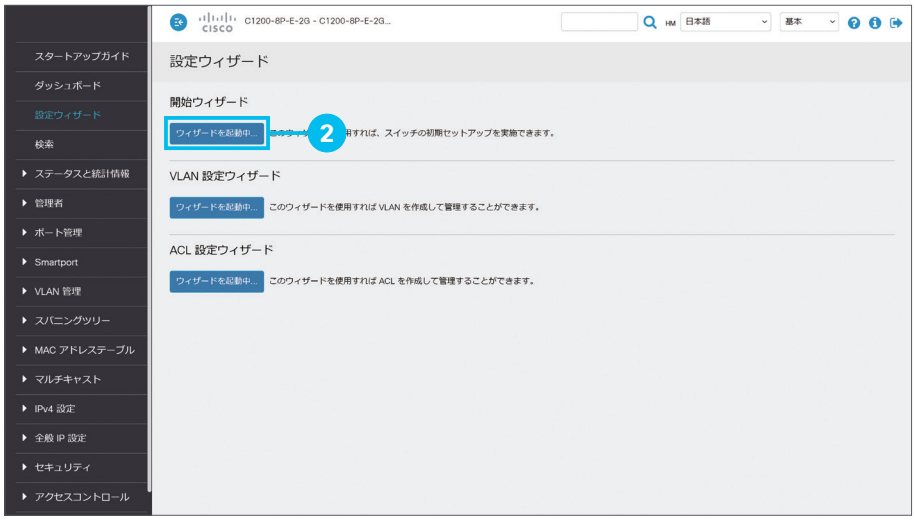
注意

設定内容をスマートスイッチの再起動後も保持したい場合は、ユーザー名の横で点滅して表示される アイコンをクリックして、スマートスイッチが起動時に読み込むスタートアップ設定ファイルに設定内容を保存します。

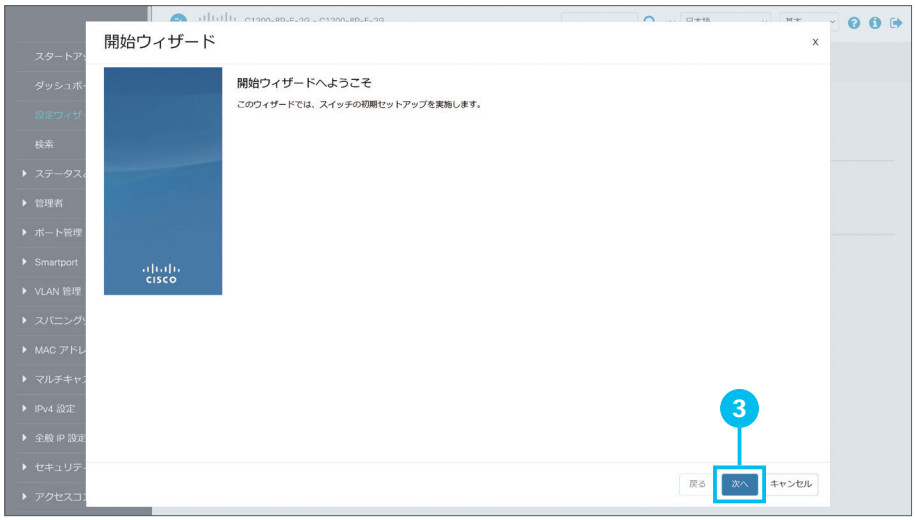
3-1 開始ウィザードを使用する

「**開始ウィザード**」によって、スマートスイッチの IP アドレス設定など、初期セットアップを簡単に実行できます。本ガイドでは例として、ホスト名（スマートスイッチの名前）、静的 IP アドレス、および時刻（SNTP サーバー）を設定します。

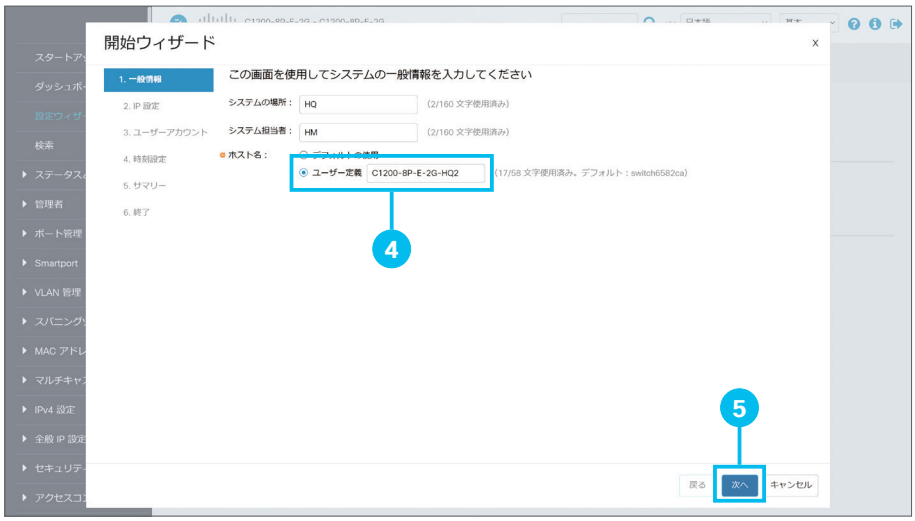
1 ［**設定ウィザード**］をクリック



2 ［**開始ウィザード**］の［**ウィザードを起動中 ...**］をクリック



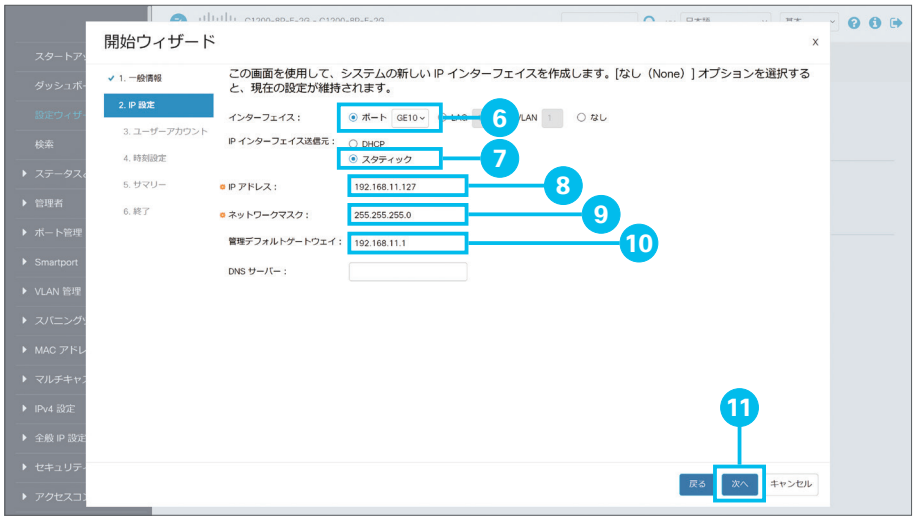
3 ［**次へ**］をクリック



4 ［**ホスト名**］の［**ユーザー定義**］をクリックして選択し、任意のホスト名（スマートスイッチの名前）を入力

［**ホスト名**］のデフォルトは、「**switch*xxxxxx***」です（*xxxxxx* はスマートスイッチの MAC アドレス末尾）。Cisco Business Mobile アプリなどの管理ツールで複数のネットワーク機器を管理する場合に備えて、わかりやすいホスト名に変更することを推奨します。
本ガイドでは例として、「C1200-8P-E-2G-HQ2」を設定します。

5 ［**次へ**］をクリック



注意

「2-1 Web インターフェイスにアクセスする（LED が緑色で点灯）」のようにスマートスイッチのネットワーク接続が完了している場合は通常、上位機器と接続中のポートを選択して設定を変更する必要はありません。
❻で上位機器と接続中のポートを選択して設定を変更すると、⓯の設定適用後に接続断などの予期せぬエラーが発生する可能性があります。

❻ ［**インターフェイス**］の［**ポート**］をクリックして選択し、ドロップダウンリストで設定したいポートを選択

❼ ［**IP インターフェイス送信元**］の［**スタティック**］をクリックして選択

❽ ［**IP アドレス**］に任意の IP アドレスを入力

本ガイドでは例として、10 番ポート（［GE10］）に「192.168.11.127」を設定します。

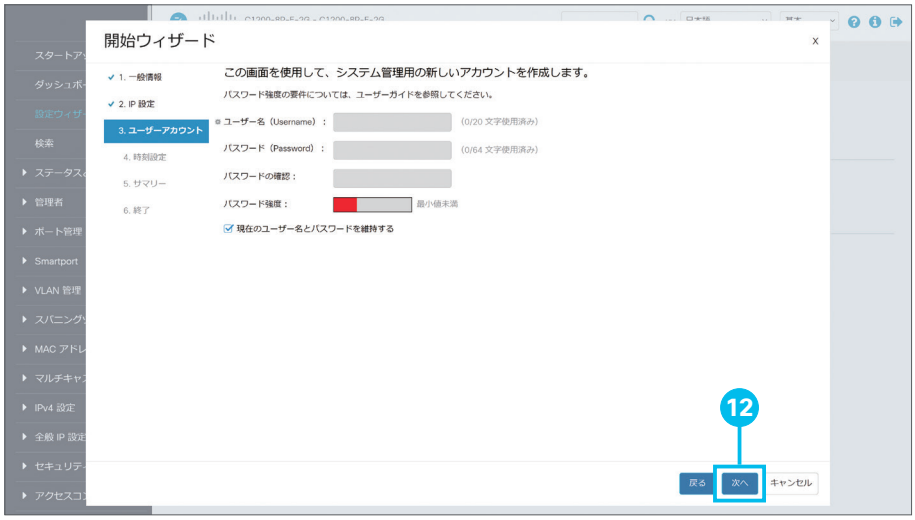
❾ ［**ネットワークマスク**］に任意のサブネットマスクを入力

本ガイドでは例として、「255.255.255.0」を設定します。

❿ ［**管理デフォルトゲートウェイ**］にデフォルトゲートウェイの IP アドレスを入力

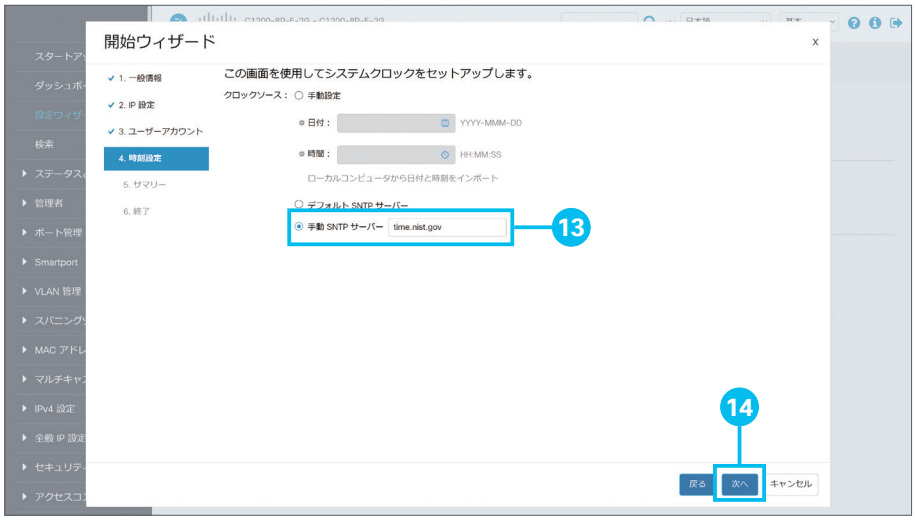
本ガイドでは例として、ルータの LAN 側 IP アドレス「192.168.11.1」を設定します。

⓫ ［**次へ**］をクリック



⓬ ［**次へ**］をクリック

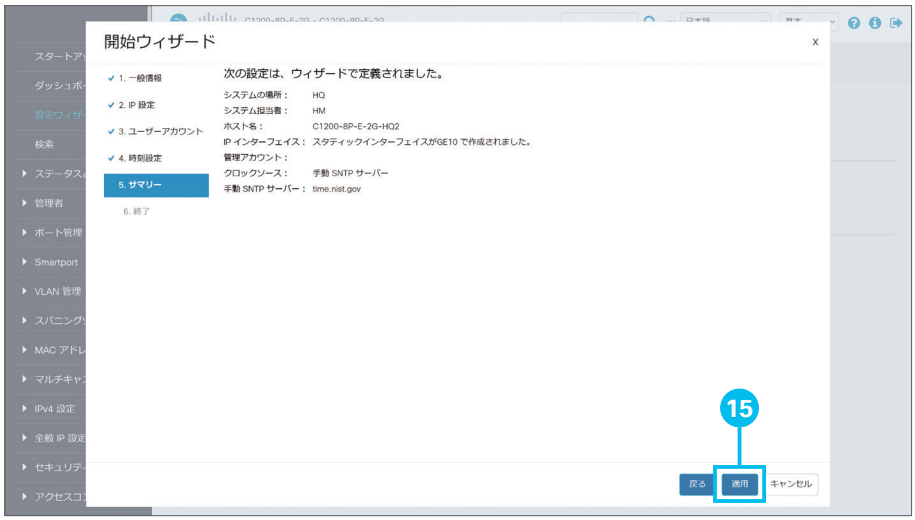
初回ログイン時に作成したデフォルトのユーザーアカウントとは別のユーザーアカウントを作成することもできます。



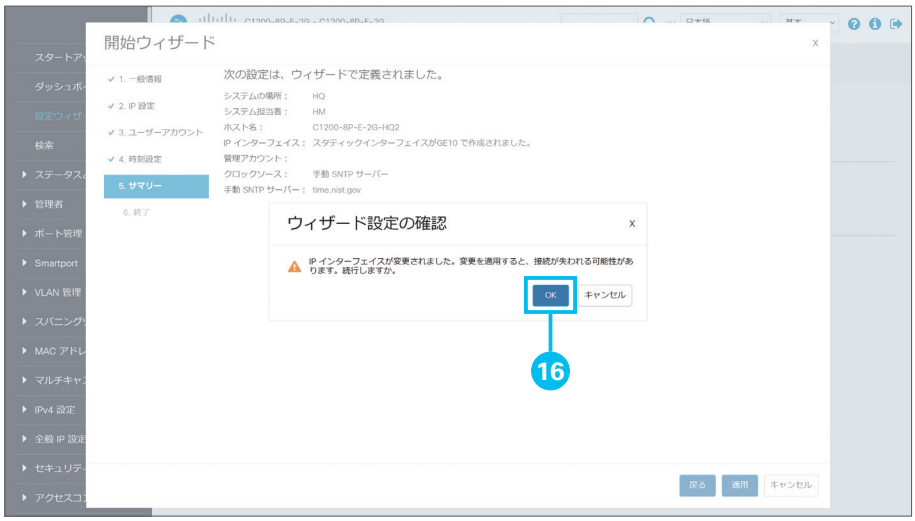
13 ［**手動 SNTP サーバー**］をクリックして選択し、IP アドレスまたは名前を入力

本ガイドでは例として、SNTP サーバー「**time.nist.gov**」を設定します。

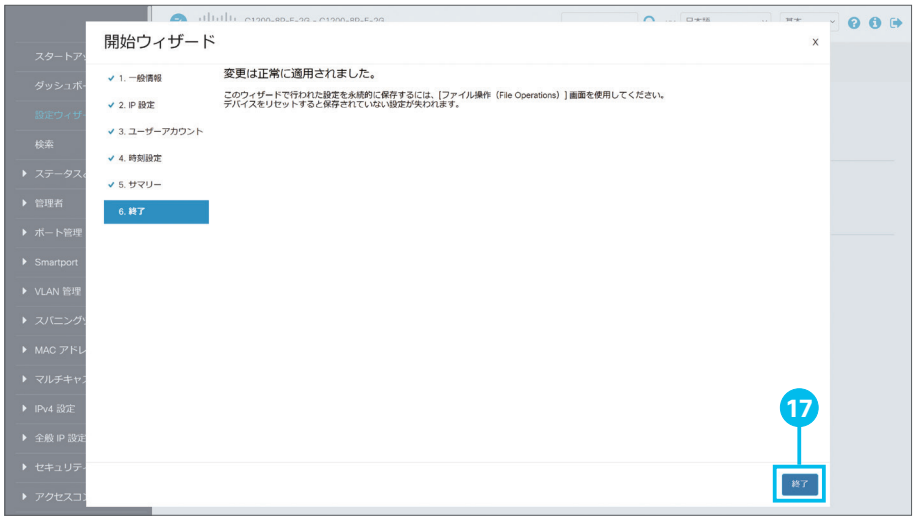
14 ［**次へ**］をクリック



15 ［**適用**］をクリック



16 ［**OK**］をクリック



17 ［終了］をクリック

注意

「2-2 Web インターフェイスにアクセスする（LED が緑色で点滅）」の手順で PC のネットワーク設定を変更した場合は、Web インターフェイスに再アクセスする前にネットワーク設定を元に戻す必要があります。

3-2 VLAN 設定ウィザードを使用する

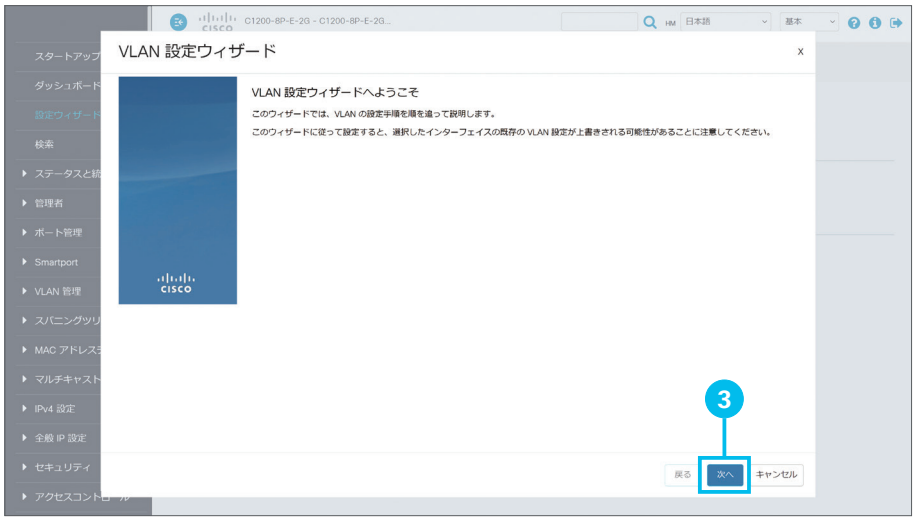
「**VLAN 設定ウィザード**」によって、部署別や目的別に LAN を分割する「**VLAN（仮想 LAN）**」を簡単に設定できます。本ガイドでは例として、営業部用の VLAN と経理部用の VLAN を設定します。

1 ［設定ウィザード］をクリック

MEMO

VLAN（Virtual Local Area Network；仮想 LAN）によって LAN を分割することで、VLAN 間の通信を制限して通信量を削減すると同時にセキュリティを確保することができます。たとえば、営業部の仮想 LAN で発生するブロードキャスト通信（全端末宛の通信）は経理部の仮想 LAN に所属する端末宛には発生しないため、通信量を削減できます。また、営業部の端末から経理部の端末にはデフォルトではアクセスできないため、セキュリティを確保できます（VLAN 間の通信可否はルータやレイヤ 3 スイッチで制御します）。
さらに VLAN には、ネットワーク機器の場所や配線など物理的な構成に制約されずに、柔軟にネットワークを構成できるというメリットがあります。たとえば、複数のスイッチをまたいで同じ営業部 VLAN や経理部 VLAN を設定できるだけでなく、営業部 VLAN から経理部 VLAN へとスイッチポートの設定を簡単に変更できるなど、席替えやレイアウト変更、あるいは部署の異動にも、スムーズに対応できます。

2 ［**VLAN 設定ウィザード**］の［**ウィザードを起動中 ...**］をクリック

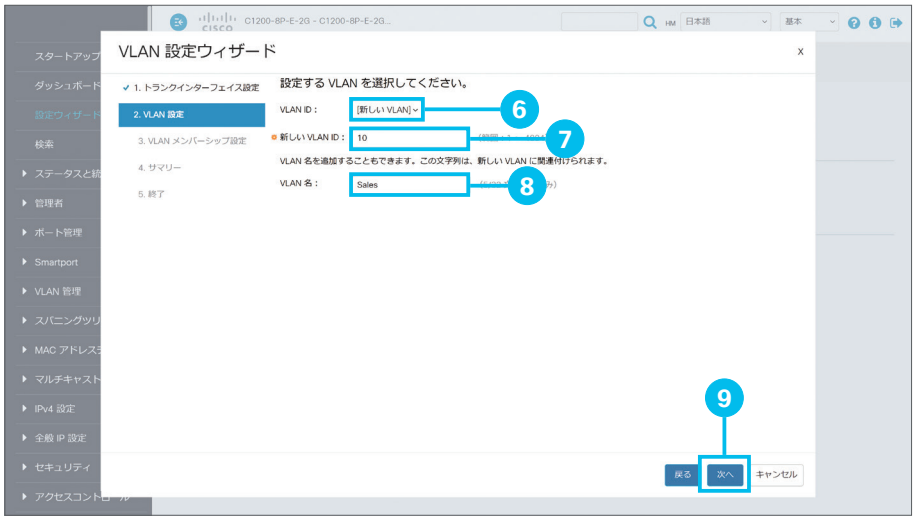


3 ［**次へ**］をクリック

4 「**トランクインターフェイス**」をクリックして選択

トランクインターフェイスには通常、ルータやスイッチ、Wi-Fi アクセスポイントなど、他の VLAN 対応ネットワーク機器と接続するポートを選択します。
本ガイドでは例として、9 番ポートと 10 番ポートを選択します。
選択したポートは黄色でマークされます。

5 ［**次へ**］をクリック



6 ［VLAN ID］ドロップダウンリストで［新しい VLAN］が選択されていることを確認

7 ［新しい VLAN ID］に任意の VLAN ID を入力

2 ～ 4094 の範囲で入力します。
本ガイドでは例として、営業部 VLAN として運用中の VLAN ID「10」を入力します。

8 （必要に応じて）［VLAN 名］に VLAN 名を入力

管理しやすい名前を付けることを推奨します。
本ガイドでは例として、「Sales」を入力します。

9 ［次へ］をクリック

10 ［次へ］をクリック

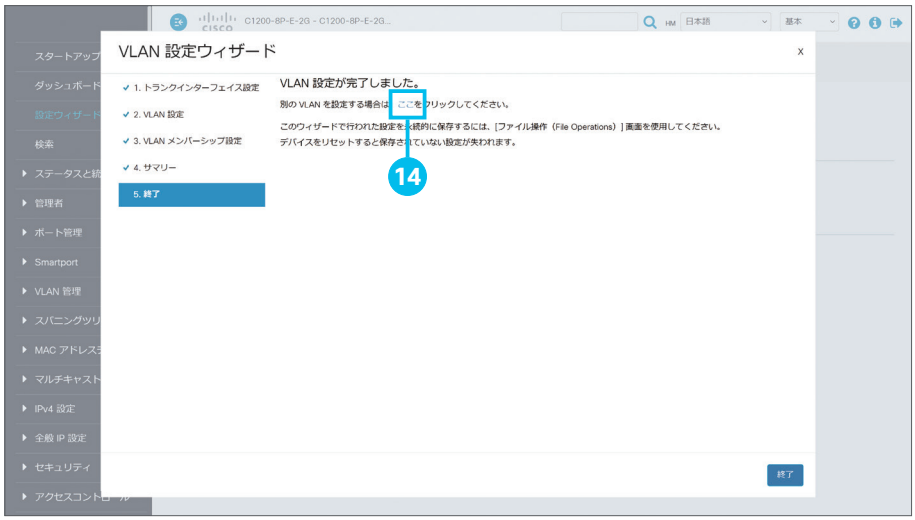
Web インターフェイスへのアクセスなど、管理用通信に使用される「ネイティブ VLAN」（デフォルトでは VLAN ID 1）を変更したい場合に選択します。

11 ［アクセスインターフェイス］をクリックして選択

アクセスインターフェイスには通常、設定中の VLAN に所属する端末が接続するポートを選択します。
本ガイドでは例として、営業部のユーザー（端末）が接続する 5 番ポートと 6 番ポートを選択します。
選択したポートは黄色でマークされます。

12 ［次へ］をクリック

13 ［**適用**］をクリック



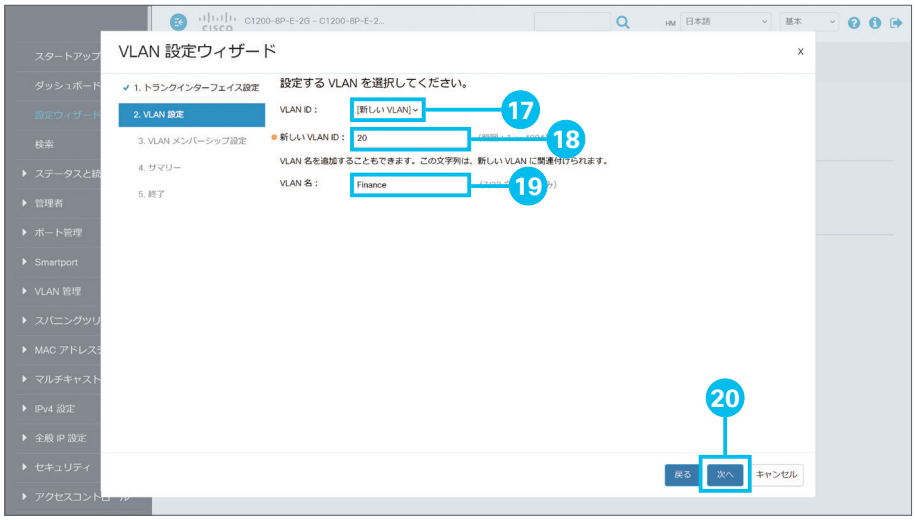
14 ［**ここ**］をクリック

営業部 VLAN の設定が完了しました。続けて、経理部 VLAN を設定します。

15 「**トランクインターフェイス**」が選択されていることを確認

デフォルトでは、❹で選択したスイッチポートが選択された状態で表示されます。

16 ［**次へ**］をクリック



17 ［**VLAN ID**］ドロップダウンリストで［**新しい VLAN**］が選択されていることを確認

18 ［**新しい VLAN ID**］に任意の VLAN ID を入力

本ガイドでは例として、経理部 VLAN として運用中の VLAN ID「**20**」を入力します。

19 （必要に応じて）［**VLAN 名**］に VLAN 名を入力

本ガイドでは例として、「**Finance**」を入力します。

20 ［**次へ**］をクリック

21 ［**次へ**］をクリック

22 ［**アクセスインターフェイス**］をクリックして選択

本ガイドでは例として、経理部のユーザー（端末）が接続する 7 番ポートと 8 番ポートを選択します。

23 ［**次へ**］をクリック

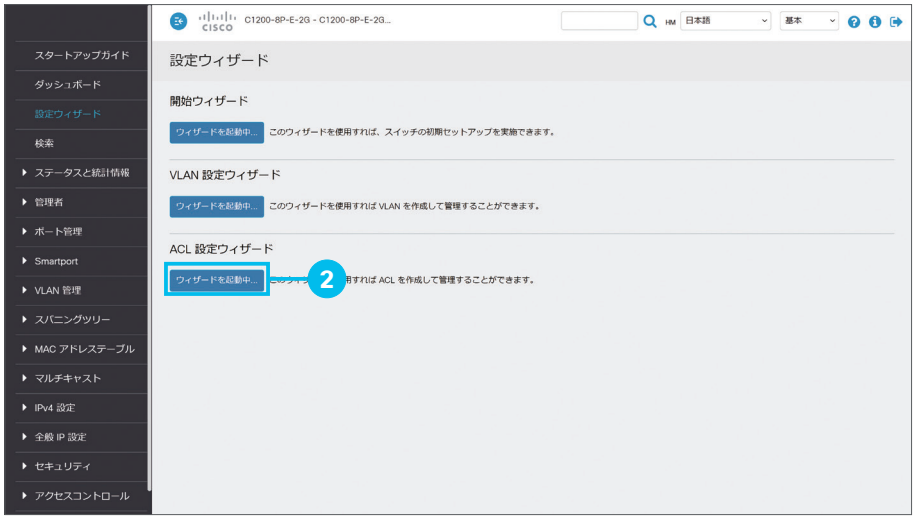
24 ［適用］をクリック

25 ［終了］をクリック

3-3 ACL 設定ウィザードを使用する

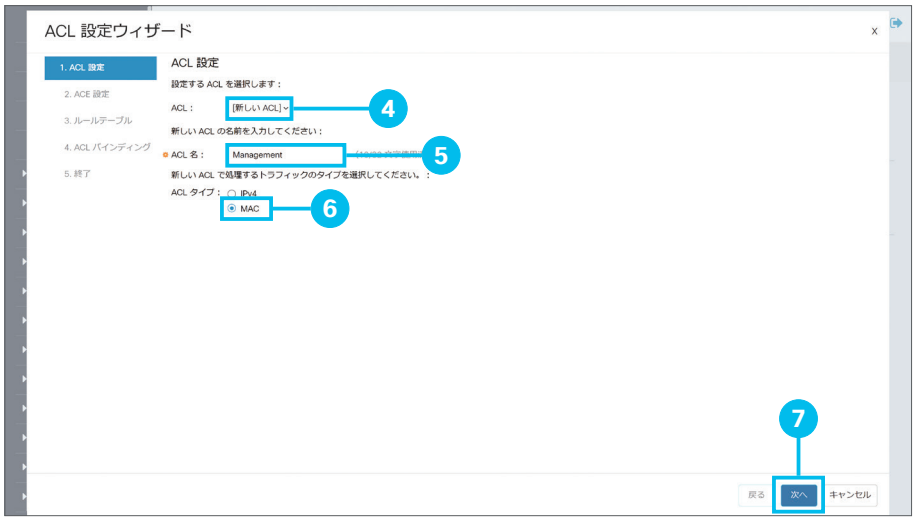
「**ACL 設定ウィザード**」によって、端末の MAC アドレスや IP アドレスに基づいてスイッチポートへの接続を許可またはブロックする「**ACL（アクセスコントロールリスト）**」を設定できます。
本ガイドでは例として、1 番ポートに特定の端末だけがアクセスできるように設定します。

1 ［**設定ウィザード**］をクリック



2 ［**ACL 設定ウィザード**］の［**ウィザードを起動中 ...**］をクリック

3 ［次へ］をクリック



4 ［ACL］ドロップダウンリストで［新しい ACL］が選択されていることを確認

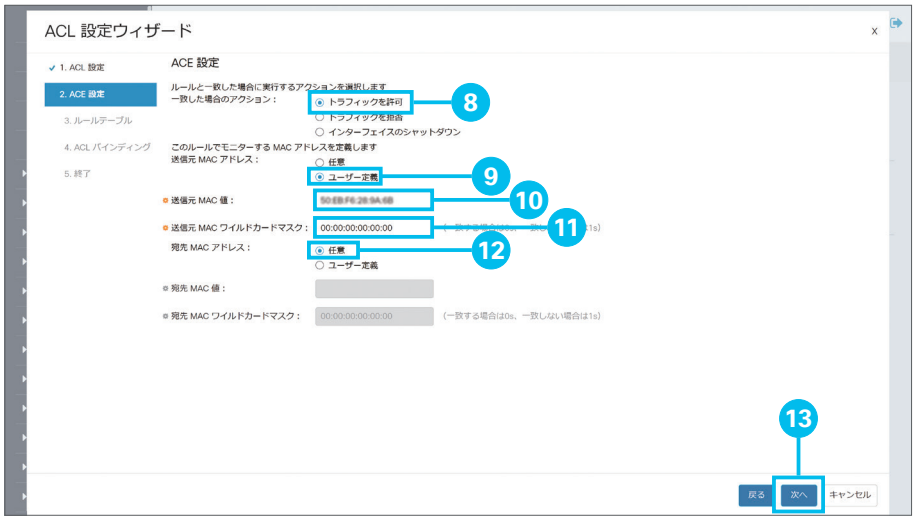
5 ［ACL 名］に任意の ACL 名を入力

管理しやすい名前を付けることを推奨します。本ガイドでは例として、「Management」を入力します。

6 ［ACL タイプ］の［MAC］をクリックして選択

本ガイドでは例として、［MAC］を選択します。IP アドレスに基づいて設定する場合は［IPv4］を選択します。

7 ［次へ］をクリック



8 ［**一致した場合のアクション**］の［**トラフィックを許可**］をクリックして選択

9 ［**送信元 MAC アドレス**］の［**ユーザー定義**］をクリックして選択

10 ［**送信元 MAC 値**］に任意の MAC アドレスを入力

11 ［**送信元 MAC ワイルドカードマスク**］が「00:00:00:00:00:00」であることを確認

12 ［**宛先 MAC アドレス**］の［**任意**］が選択されていることを確認

本ガイドでは例として、特定の端末（送信元）だけがどの端末（宛先）にもアクセスできるように許可するルールを作成します。
特定の端末（サーバーなど）だけにアクセスできるように許可したい場合は、［**宛先 MAC 値**］にその端末の MAC アドレスを入力します。
「**ワイルドカードマスク**」によって、条件に当てはまる複数の MAC アドレスを対象にすることができます。たとえば、［**送信元 MAC 値**］に「90:2b:34:de:11:4a」、［**送信元 MAC ワイルドカードマスク**］に「00:00:00:11:11:11」を入力した場合、「90:2b:34」で始まる MAC アドレスすべてを対象にすることができます。

13 ［**次へ**］をクリック

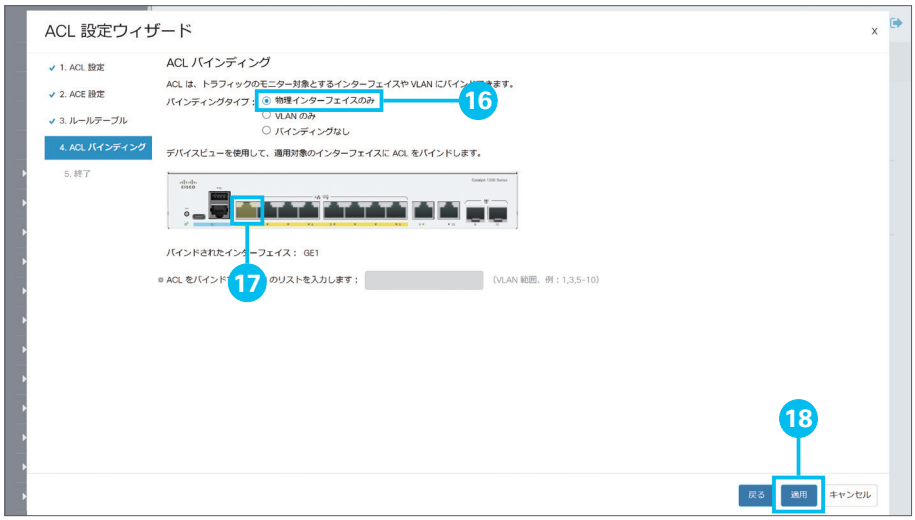
14 ［**OK**］をクリック

MEMO

［**送信元 MAC 値**］と［**宛先 MAC 値**］の「**ワイルドカードマスク**」は、「0」が「**当該バイトに該当する**」、「1」が「**当該バイトをマスクする**」意味になります。MAC アドレスの前半 6 バイトは、たとえばネットワーク インターフェイスカードなど、ネットワーク機器のベンダーを表します。そこで、同じモデルの PC を多数運用しているネットワーク環境では、後半 6 バイトをマスクすることで（00:00:00:11:11:11）、そのモデルの PC をすべて対象にすることができます。たとえば、シスコのネットワーク機器は「00:1B:67」などで始まる MAC アドレスを割り当てられています。

15 ［**次へ**］をクリック

ルールを追加する場合は ＋ アイコンをクリックして、❽～⓭の手順をくり返します。



16 ［**バインディングタイプ**］の［**物理インターフェイスのみ**］が選択されていることを確認

17 物理インターフェイスをクリックして選択

本ガイドでは例として、1 番ポートを選択します。選択したポートは黄色でマークされます。

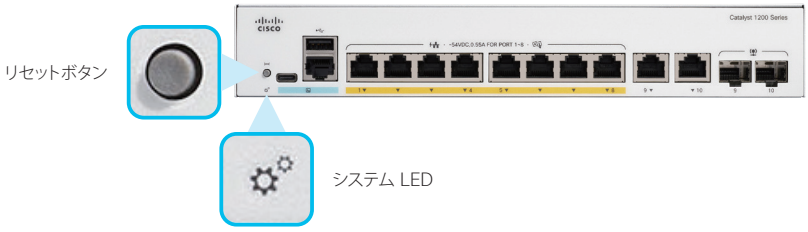
18 ［**適用**］をクリック

19 ［**終了**］をクリック

リセットボタンとシステム LED の挙動について

スイッチの稼動中にリセットボタンを長押しすると、次の条件でスイッチをリブート（再起動）または初期設定へリセット（工場出荷状態に初期化）することができます。

- リセットボタンを 6 ～ 10 秒間の長押しでシステム LED が緑色で点滅（**低速**）、点滅中にボタンを放すと**再起動**
- リセットボタンを 16 ～ 20 秒間の長押しでシステム LED が緑色で点滅（**高速**）、点滅中にボタンを放すと**工場出荷状態に初期化**



製品サポートページ

www.cisco.com/c/ja_jp/support/switches/catalyst-1200-series-switches/series.html

シスコ コミュニティ

community.cisco.com/t5/japan/ct-p/japanese-community

シスコ お問い合わせ窓口

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して ｜ サービスに関して ｜ 各種キャンペーンに関して ｜ お見積依頼 ｜ 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

©2024 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における商標登録または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。（1502R）この資料の記載内容は 2024 年 1 月現在のものです。この資料に記載された仕様は予告なく変更する場合があります。

シスコシステムズ合同会社
〒 107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
cisco.com/jp

2409-2401-000-TO