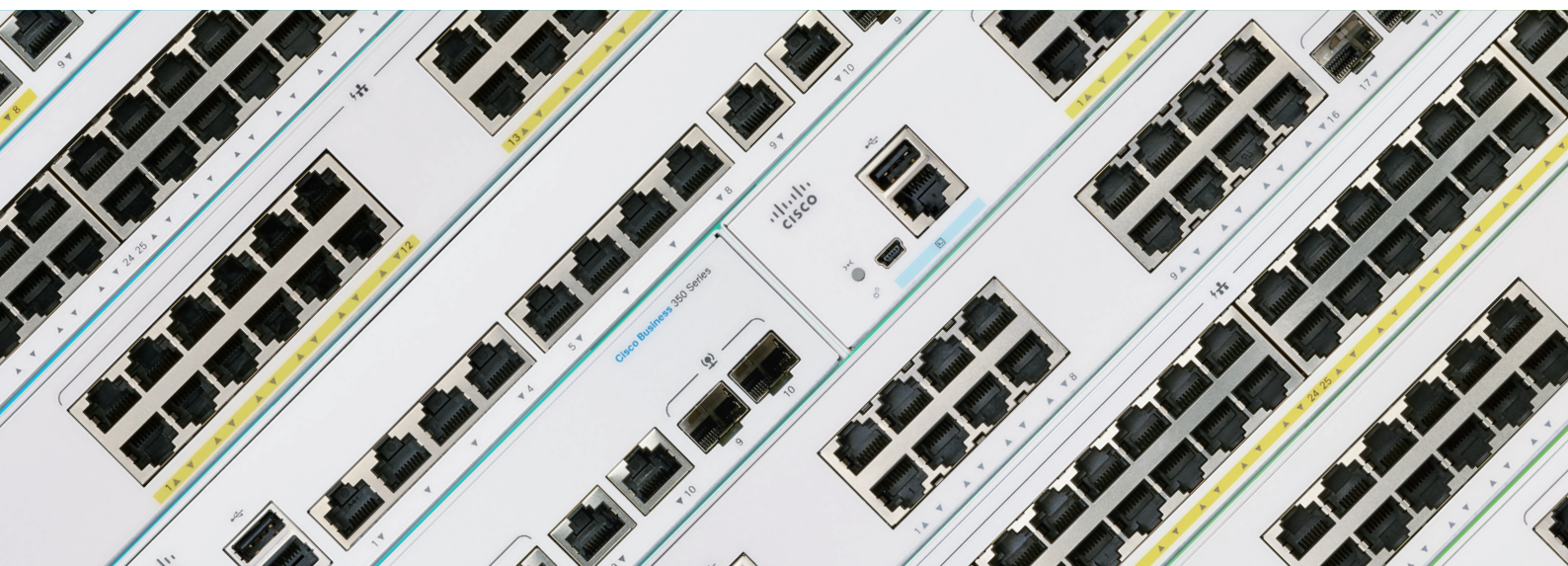




Cisco Business 350 シリーズ マネージドスイッチ



——かんたんセットアップガイド——

本ガイドの手順で Cisco Business 350 シリーズ マネージドスイッチをかんたんにセットアップできます

- | | | |
|---|---------------------|-----|
| 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 | P11 |
| 4 | スイッチポートを設定する | P24 |
| 5 | レイヤ 3 機能を設定する | P33 |
| 6 | ダッシュボードをカスタマイズする | P51 |
| 7 | ファームウェアを更新する | P57 |

はじめに

Cisco Business 350 シリーズ マネージドスイッチは、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な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) 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。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への給電をサポート。

● 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。万が一の障害にも Web インターフェイスやモバイルアプリによるモニタリングで迅速に対応可能 (モバイルアプリは近日リリース予定)。

● セキュリティ

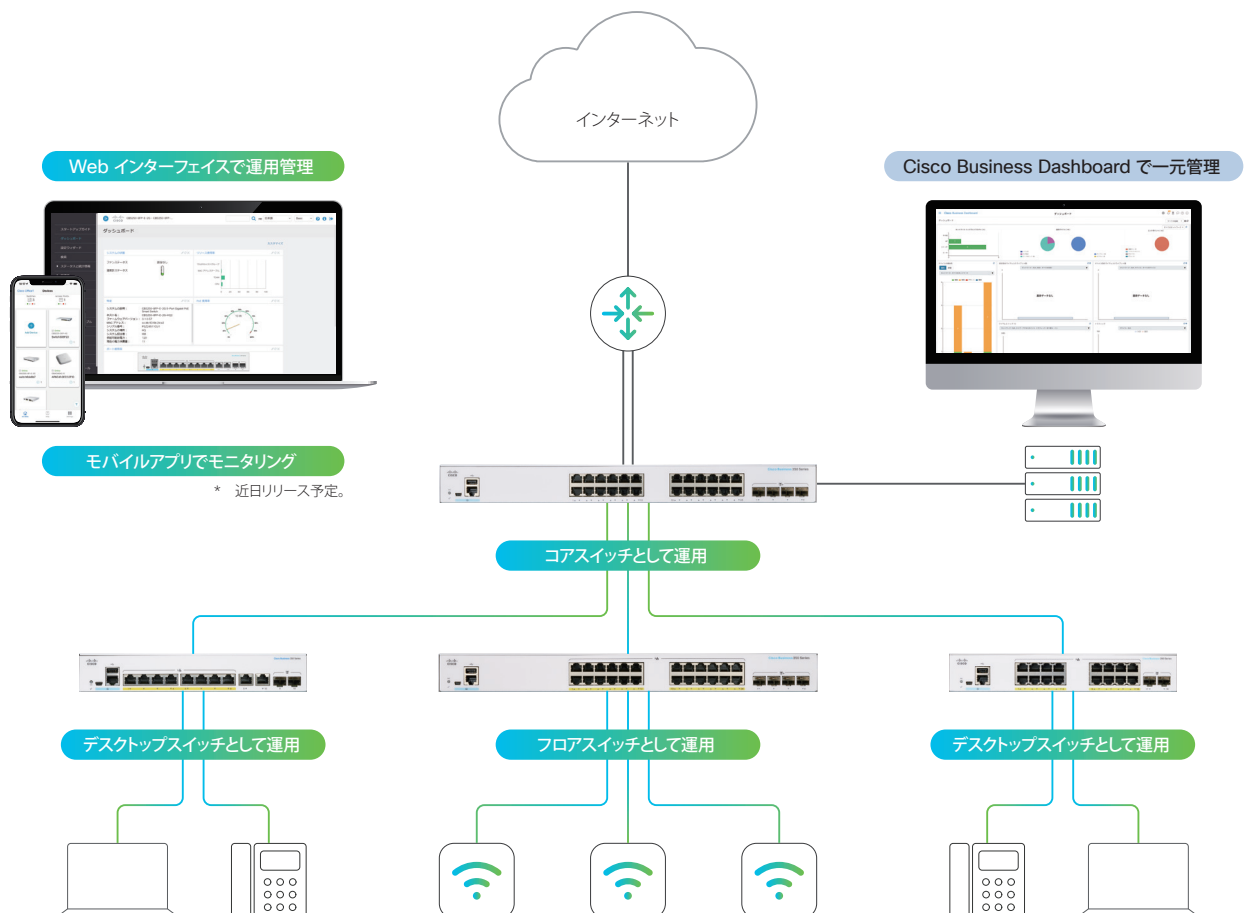
ACL (アクセスコントロールリスト) など、ビジネスに必要な不可欠なセキュリティを Web インターフェイスで簡単設定可能。

● 中小企業のネットワークに必要な不可欠な機能

レイヤ 3 ダイナミック (動的) 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な十分な機能を Web インターフェイスで簡単設定可能。

● シンプルに構築および運用管理

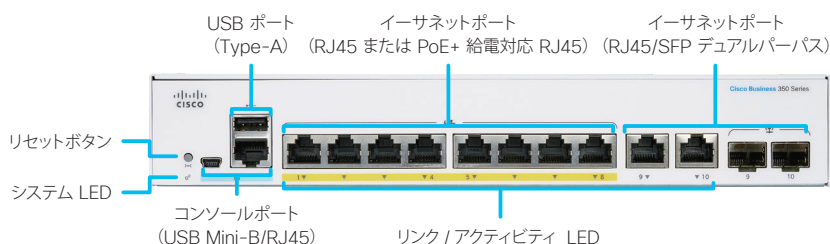
つなぐだけで使用を開始できる、プラグアンドプレイスイッチとしても導入可能。Web インターフェイスでは、設定ウィザードによる簡単設定ときめ細やかな個別設定をサポート。VMware などのハイパーバイザや AWS で実行できる Cisco Business Dashboard Manager を導入すれば、複数拠点の Cisco Business 製品を無料で 25 台まで一元管理可能。



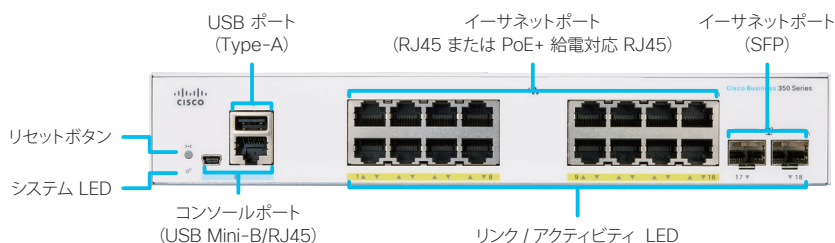
マネージドスイッチの前面パネル

マネージド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）でマネージド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。

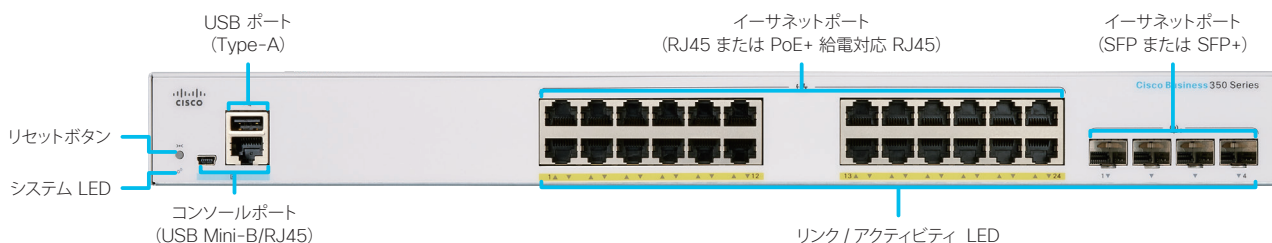
8 ポートモデル



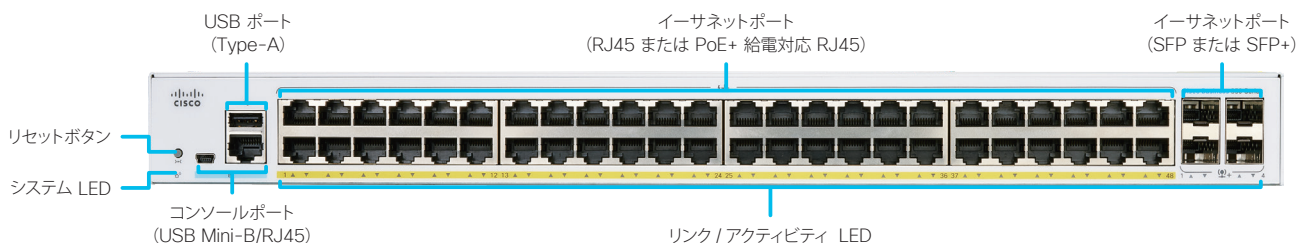
16 ポートモデル



24 ポートモデル



48 ポートモデル



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

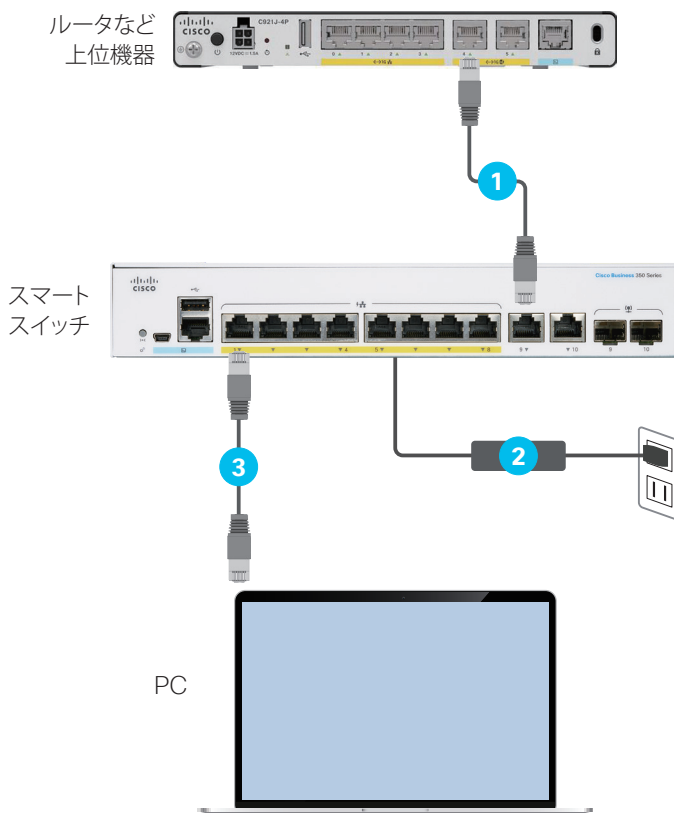
スイッチをネットワークに接続する

マネージド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、マネージドスイッチ内蔵の 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

マネージド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 をマネージド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、スタティック（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 をマネージドスイッチに直接接続する必要はありません。



1 マネージドスイッチをネットワークに接続

マネージドスイッチは、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、マネージドスイッチの 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。マネージドスイッチでは PoE 非対応ポートの使用を推奨します。上位機器で使用する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 マネージド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、本体前面の LED が点灯または点滅します。

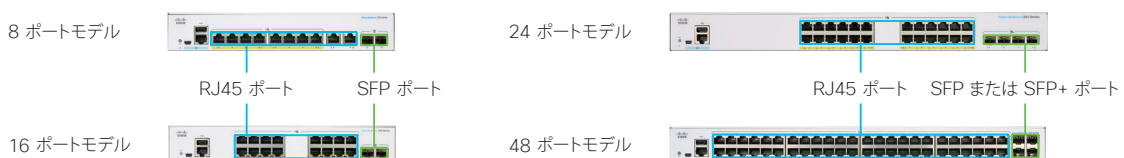
3 （必要に応じて）PC をマネージドスイッチに接続

必要に応じて、PC の RJ45 ポートとマネージドスイッチの 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。

TIP MEMO

マネージド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

マネージド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



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）

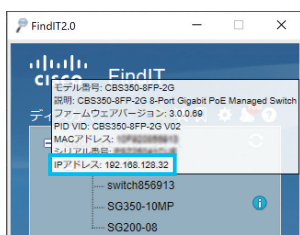
マネージドスイッチのシステム LED が緑色で**点灯**している場合は、**ネットワークへの接続が完了**しています。ルータなど上位機器（DHCP サーバ）がマネージドスイッチに割り当てた **IP アドレスを確認**し、Web インターフェイスにアクセスします。マネージドスイッチに直接接続した PC だけでなく、Wi-Fi を含むネットワークに接続済みの PC からアクセスすることができます。

switch6b2da3	192.168.1.115	Dynamic
--------------	---------------	---------

IP アドレス確認例：シスコ ルータ

switch6b2da3	8月 30 16:01	192.168.128.26
--------------	-------------	----------------

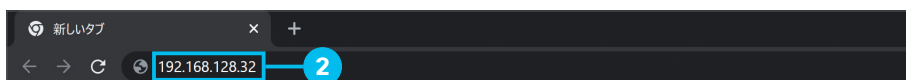
IP アドレス確認例：Meraki ダッシュボード



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 マネージドスイッチの IP アドレスを確認

ルータなど上位機器（DHCP サーバ）がマネージド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マネージドスイッチの 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。

TIP MEMO

2021 年 9 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）



3 ログイン画面を確認

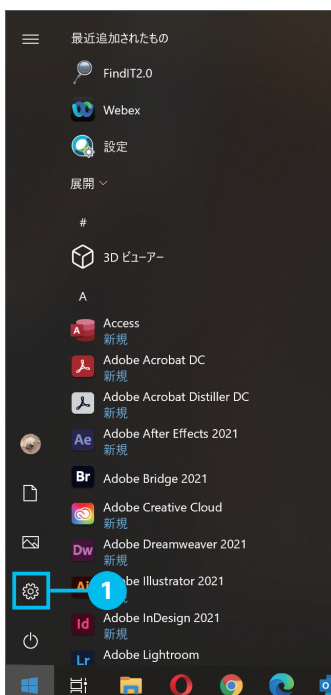
Web インターフェイスのログイン画面が表示されたら、「2-3 Web インターフェイスにログインする」に進みます。

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)

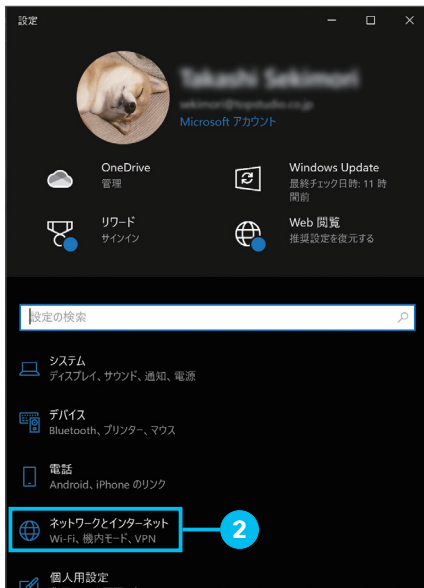
マネージドスイッチのシステム LED が緑色で点滅している場合は、ネットワークへの接続が完了していません。スタティック IP アドレスの割り当てなど、ネットワークに合わせてマネージドスイッチを設定する必要があります。マネージドスイッチに直接接続できるように PC のネットワーク設定を変更し、Web インターフェイスにアクセスします。

注意

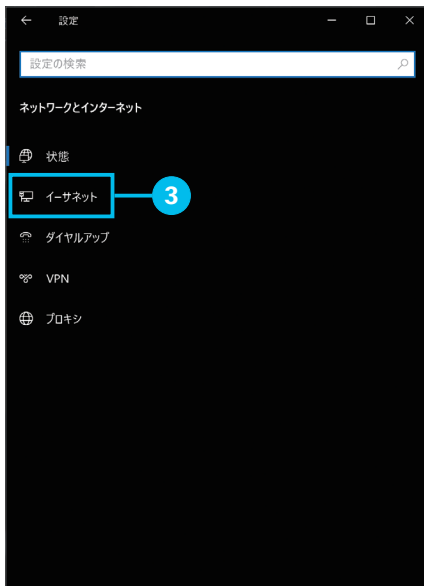
ネットワークへの接続が完了していない (IP アドレスが割り当てられていない) 場合、マネージドスイッチは工場出荷時のデフォルト IP アドレス「192.168.1.254」で動作します。工場出荷時のマネージドスイッチは DHCP サーバ機能をサポートしないため、マネージドスイッチに直接接続する PC のネットワーク設定 (IP アドレス) を「192.168.1.2」～「192.168.1.253」の範囲で設定する必要があります。本ガイドでは、[Windows 10 のネットワーク設定変更例](#)を解説します。



1 [スタート] メニューの [設定] をクリック



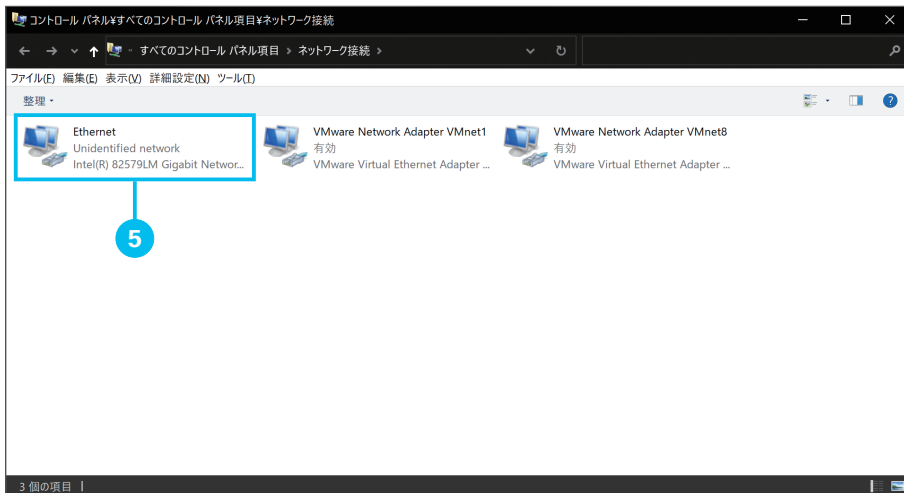
2 [ネットワークとインターネット] をクリック



3 [イーサネット] をクリック



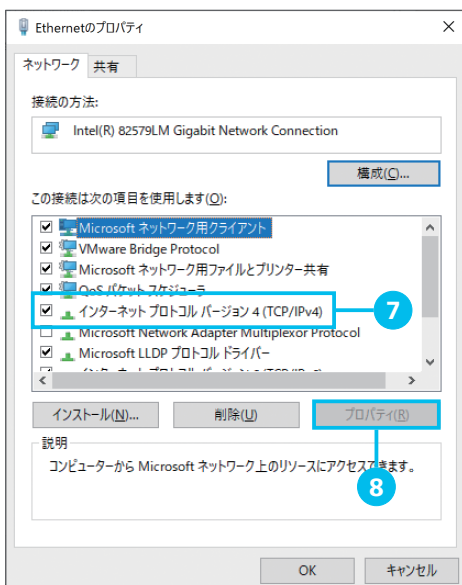
4 [アダプターのオプションを変更する] をクリック



5 マネージド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

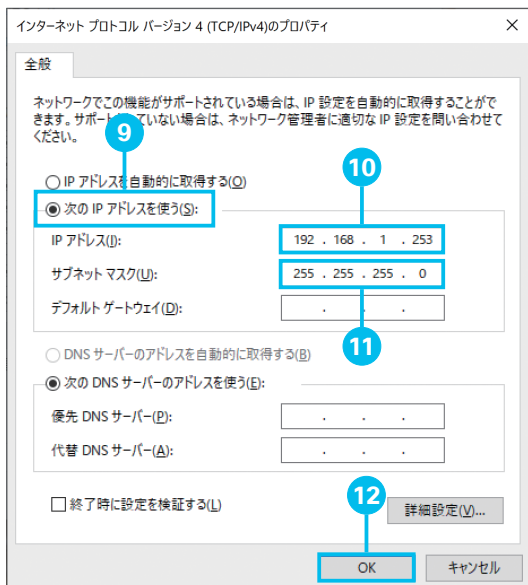


6 [プロパティ] をクリック



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
- ネットワーク設定の変更が完了しました。



- 13 ブラウザのアドレスバーにマネージドスイッチの IP アドレス「192.168.1.254」を入力



- 14 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。

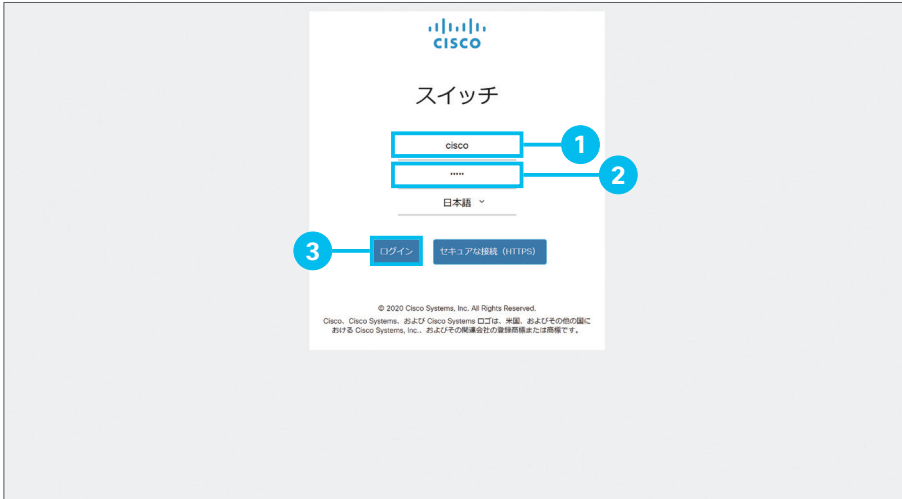
TIP MEMO

2021 年 9 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）
- Microsoft Edge
- Google Chrome（バージョン 85 または 86 以降）
- Mozilla Firefox（バージョン 81 または 82 以降）

2-3 Web インターフェイスにログインする

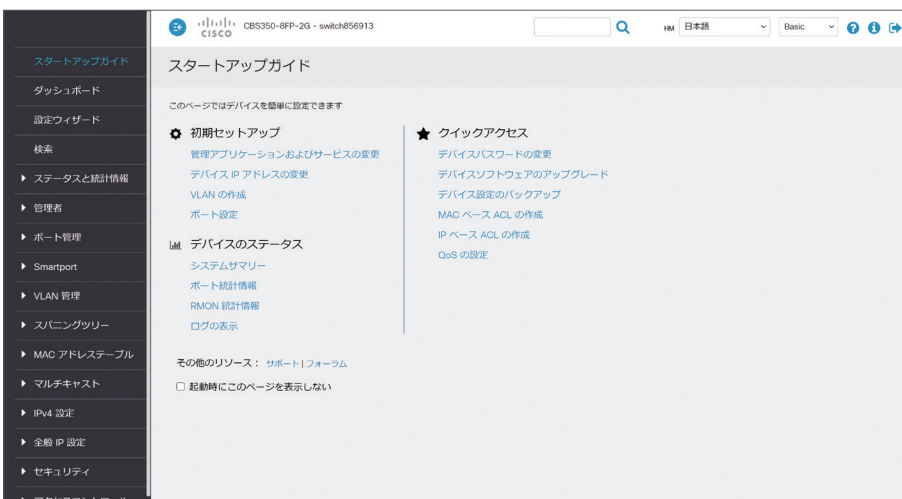
マネージドスイッチの Web インターフェイスにアクセスしたら、デフォルトのユーザ名「**cisco**」とパスワードを「**cisco**」を使ってログインします。初回ログイン時はユーザ名とパスワードを設定する必要があります。



- 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5で入力したパスワードを入力
- 7 [適用] をクリック



- 14 [スタートアップガイド] 画面を確認

Web インターフェイスへのログインが完了しました。

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、マネージド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** : マネージドスイッチの 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

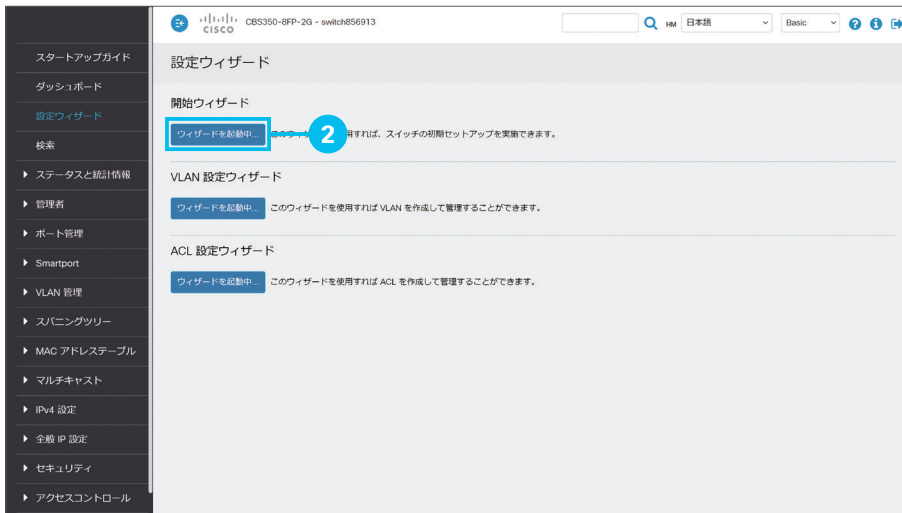
設定内容をマネージドスイッチの再起動後も保持したい場合は、ユーザ名の横で点滅して表示される [保存] アイコンをクリックして、マネージドスイッチが起動時に読み込むスタートアップ設定ファイルにも設定内容を反映します。

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、マネージドスイッチの 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（マネージドスイッチの名前）、スタティック IP アドレス、および時刻（SNTP サーバ）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



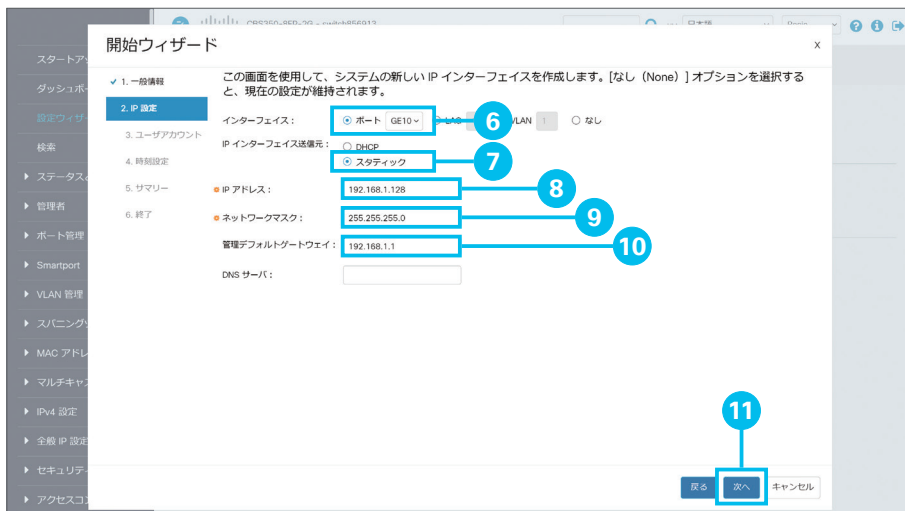
3 [次へ] をクリック



4 [ホスト名] の [ユーザ定義] をクリックして選択し、任意のホスト名（マネージドスイッチの名前）を入力

[ホスト名] のデフォルトは、「switchxxxxxx」です（xxxxxx はマネージドスイッチの MAC アドレス末尾）。Cisco Business Dashboard 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、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、「CBS350-8P-2G-HQ1」を設定します。

5 [次へ] をクリック



6 [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

7 [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

8 [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「192.168.1.128」を設定します。

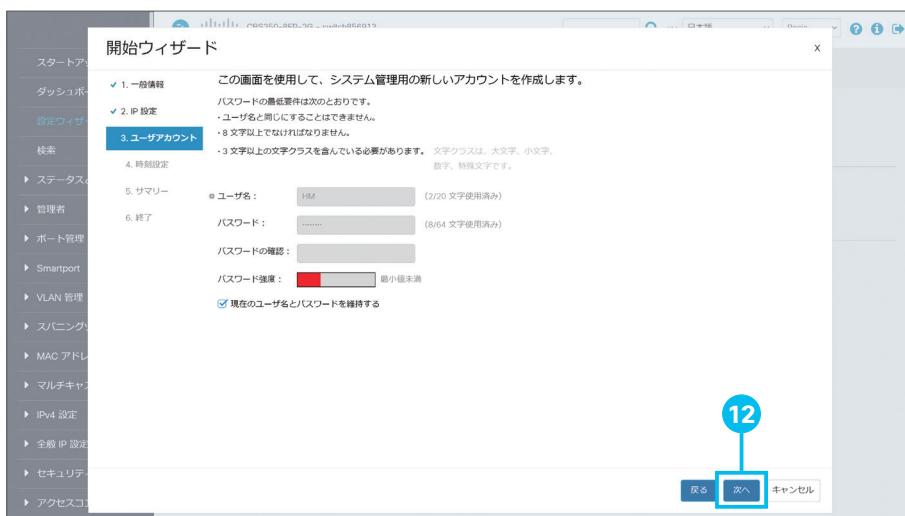
9 [ネットワークマスク] に任意のサブネットマスクを入力

本ガイドでは例として、「255.255.255.0」を設定します。

10 [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

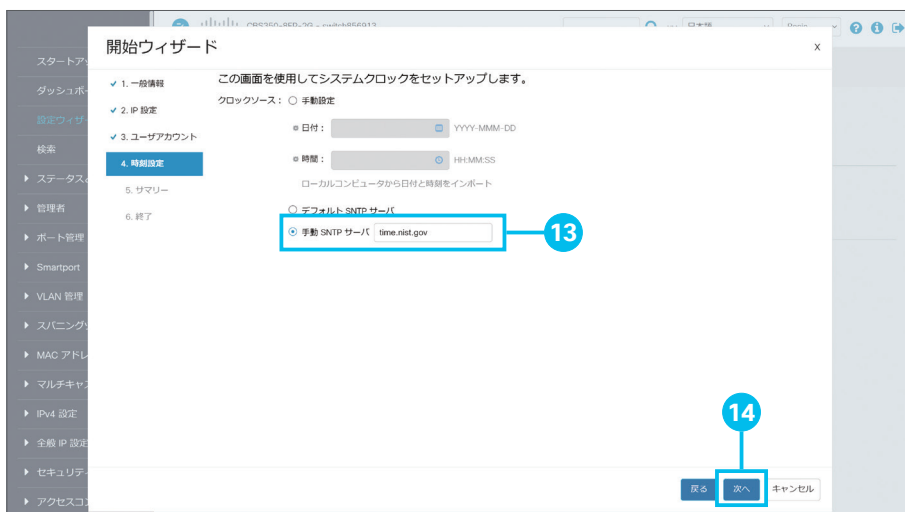
本ガイドでは例として、ルータの LAN 側 IP アドレス「192.168.1.1」を設定します。

11 [次へ] をクリック



12 [次へ] をクリック

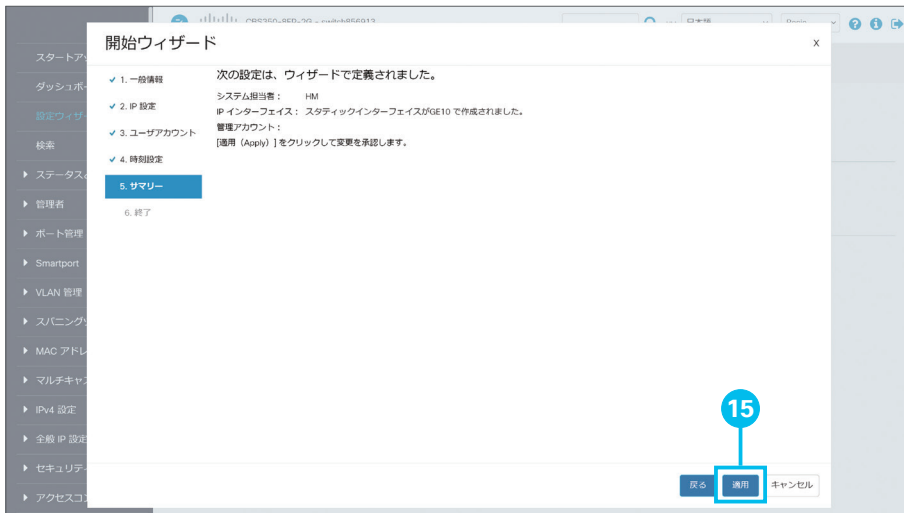
初回ログイン時に設定したユーザ名とパスワードを変更することもできます。



13 [手動 SNTP サーバ] 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「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

6で上位機器との接続に使用中のポートを選択した場合など、設定変更によって接続が遮断されて「変更は正常に適用されました。」メッセージが表示されないことがあります。その他の設定作業を続行したい場合は、変更した設定（マネージドスイッチのスタティック IP アドレスなど）に従って、Web インターフェイスに再アクセスします。

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



2 「VLAN 設定ウィザード」の「ウィザードを起動中...」をクリック

TIP 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。



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、上位機器など他の 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、「1-1 スイッチをネットワークに接続する」①で使用した 9 番ポートと、予備として 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 (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、4で選択したスイッチポート
が選択された状態が表示されます。

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（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



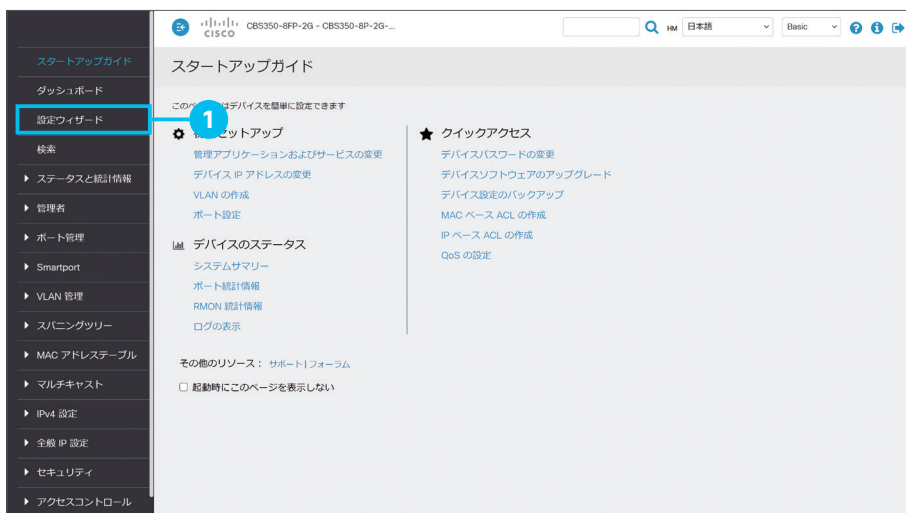
24 [適用] をクリック



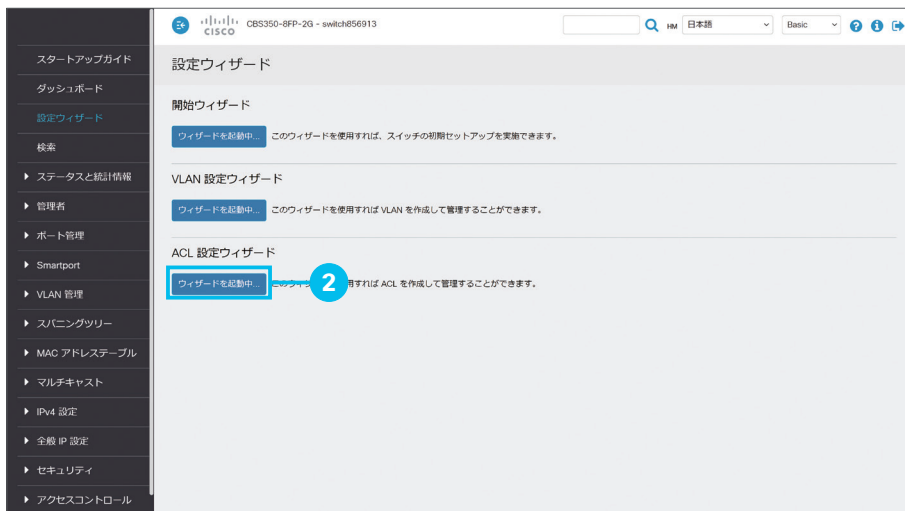
25 「終了」をクリック

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など、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。



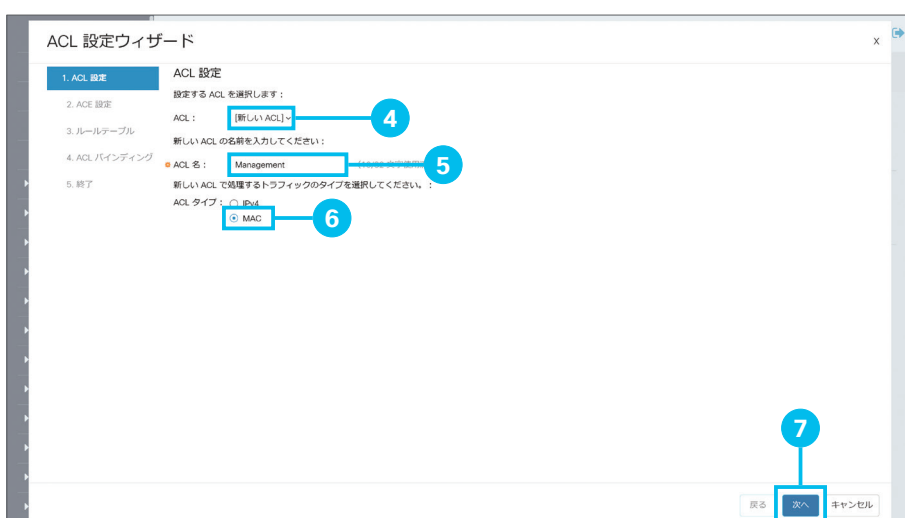
1 「設定ウィザード」をクリック



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



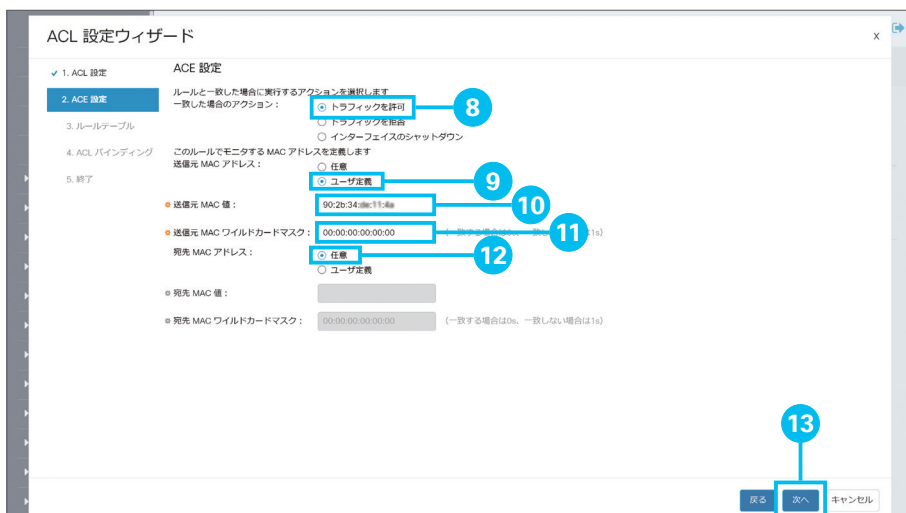
4 [ACL] ドロップダウンリストで [新しい ACL] が選択されていることを確認

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

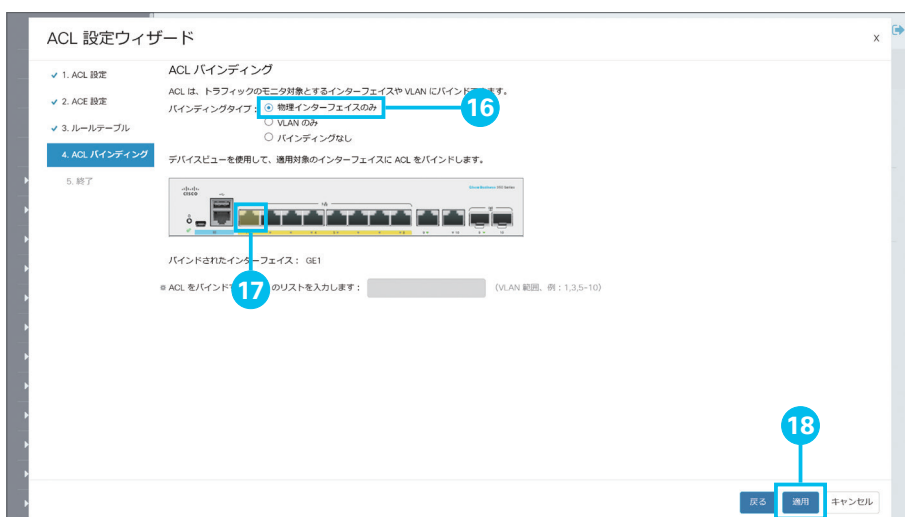
TIP MEMO

[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、6~10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

4

スイッチポートを設定する

Web インターフェイスでは、設定ウィザードで設定可能な機能を含む基本的な機能から、IPv6 設定を含む高度な機能まで、きめ細やかな設定が可能です。本ガイドではまず、使用頻度が高いスイッチポート関連機能に絞って設定例を紹介します。

- 4-1 スwitchポートを設定する
- 4-2 ループバック検出を設定する
- 4-3 Auto Smartport を設定する

注意

設定内容をマネージドスイッチの再起動後も保持したい場合は、ユーザ名の横で点滅して表示される [保存] アイコンをクリックして、マネージド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も設定内容を反映します。

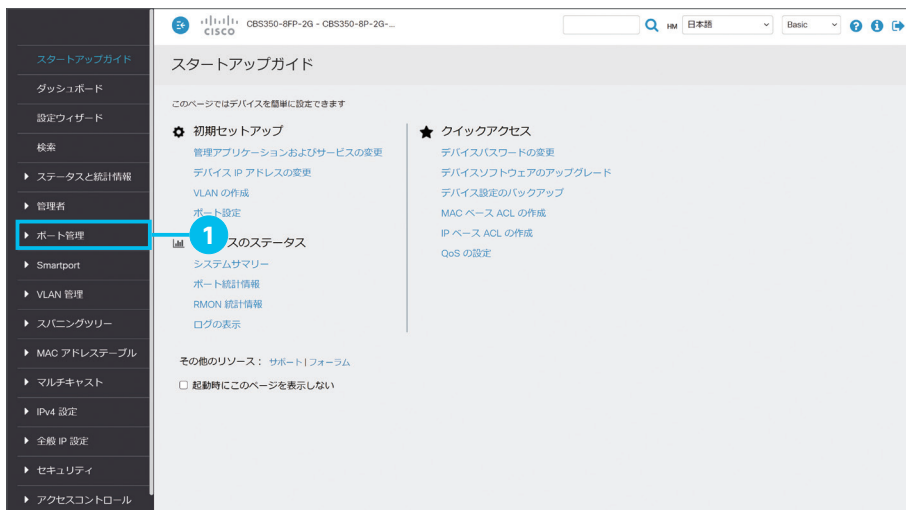
TIP MEMO

Web インターフェイスには「Basic」と「Advanced」の2つの表示モードがあります。IPv6 設定など高度な機能は、Advanced モードで表示することができます。表示モードは Web インターフェイス右上のドロップダウンリストで切り替え可能です。

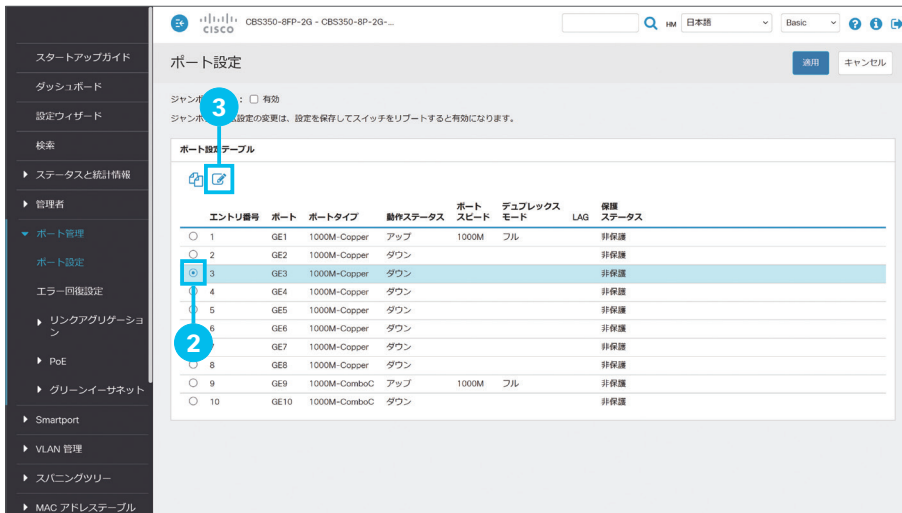


4-1 スwitchポートを設定する

Web インターフェイスでは、スイッチポートの通信速度や通信モードなどを個別に設定することができます。デフォルトでは自動ネゴシエーションによって、接続する端末やケーブルに応じて通信速度や通信モードが自動的に設定されますが、ネゴシエーションに失敗して設定が一致しない場合などには、手動で設定する必要があります。本ガイドでは例として、3番ポートの通信速度を 100M (ファストイーサネット)、通信モードをハーフ (半二重) に設定 (固定) し、さらに 3番ポートの設定を 4番ポートにコピーします。

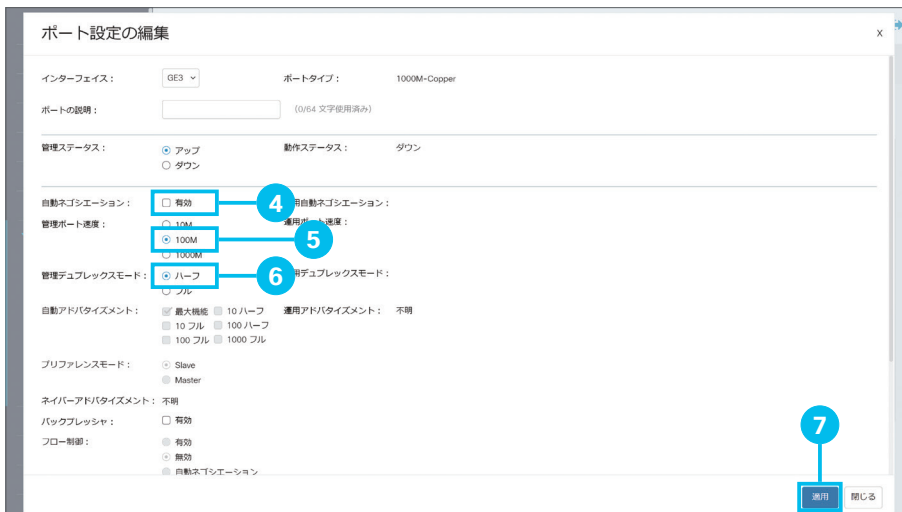


1 [ポート管理] をクリック



2 [エントリ番号] 列 [3] のラジオボタンをクリックして 3 番ポートを選択

3 編集 [] アイコンをクリック



4 [自動ネゴシエーション] の [有効] をクリックして選択を解除

5 [管理ポート速度] の [100M] をクリックして選択

6 [管理デュプレックスモード] の [ハーフ] をクリックして選択

7 [適用] をクリック

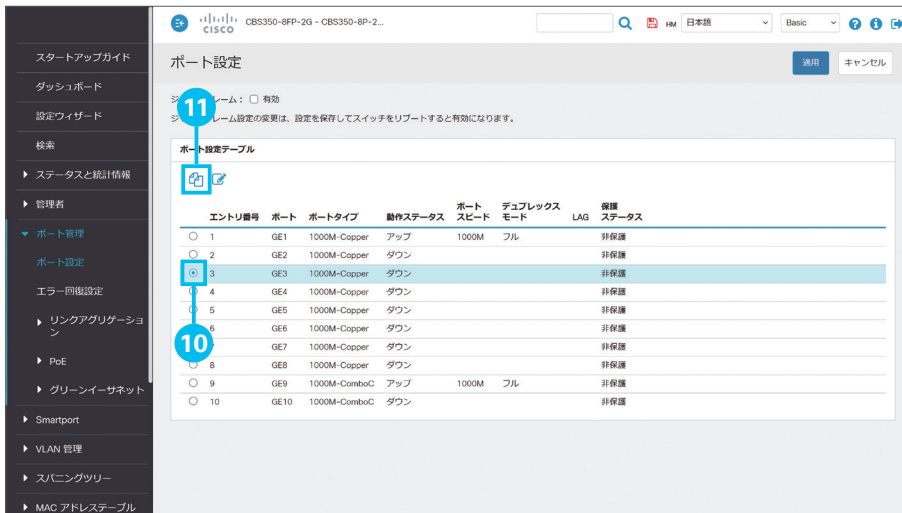


8 [成功] メッセージが表示されたことを確認

9 [閉じる] をクリック

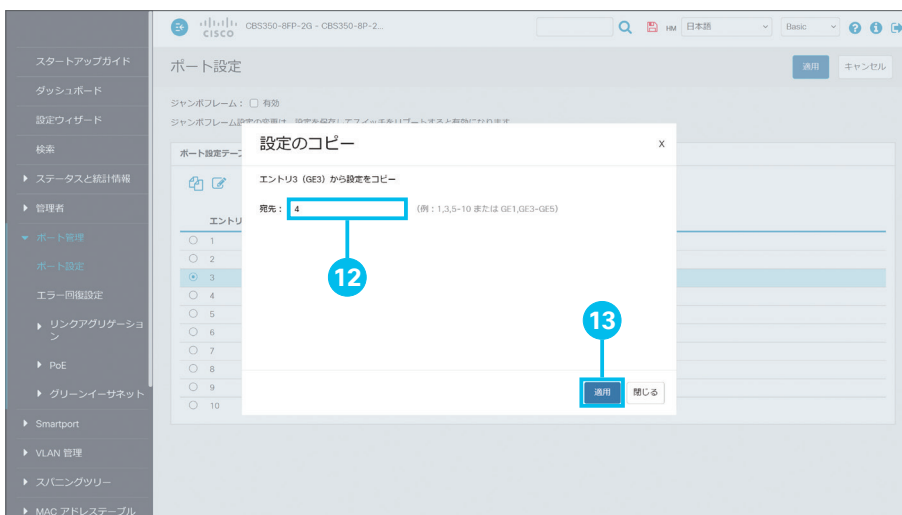
3 番ポートの通信速度と通信モードの設定が完了しました。

続けて、3 番ポートの設定を 4 番ポートにコピーします。



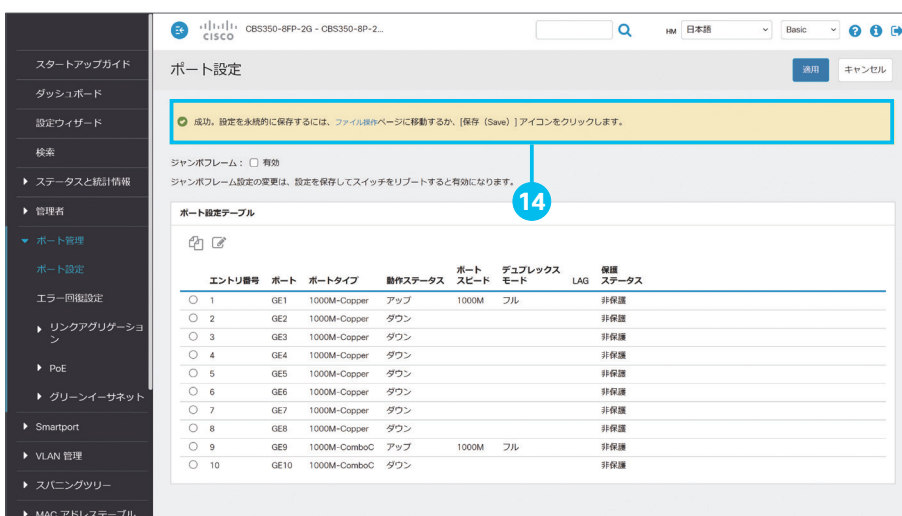
10 [エントリ番号] 列 [3] のラジオボタンをクリックして 3 番ポートを選択

11 編集 [] アイコンをクリック



12 [宛先] に「4」を入力

13 [適用] をクリック



14 [成功] メッセージが表示されたことを確認

4-2 ループバック検出を設定する

複数のスイッチを運用している環境では、スイッチの誤接続などによってブロードキャスト通信（すべての端末宛の通信）やマルチキャスト通信（複数の端末宛の通信）がくり返し転送されて（ループ）、ネットワークのパフォーマンスが低下したり、停止したりすることがあります。マネージドスイッチでは、特定のスイッチポートでループの発生を検出すると、そのポートおよびループを遮断する**ループバック検出**を設定できます。本ガイドでは例として、10番ポートでループバック検出を設定します。

TIP MEMO

ループバック検出を設定したスイッチポートでは、定期的に**ループプロトコル/パケット**を送信します。そのポートで同じパケットを受信すると（ループバック）、ループが発生したと判定してポートおよびループを遮断し、ネットワークパフォーマンスの低下を未然に防止します。

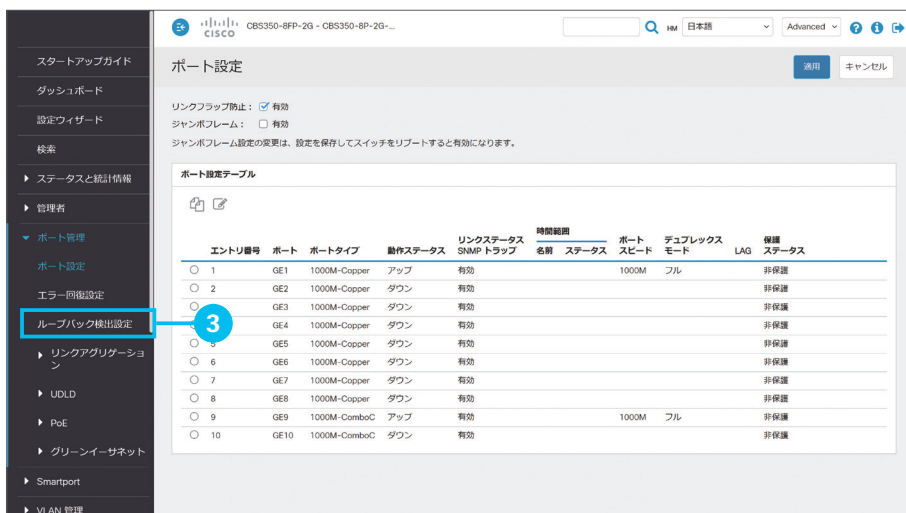


- 1 表示モードのドロップダウンリストで [Advanced] を選択

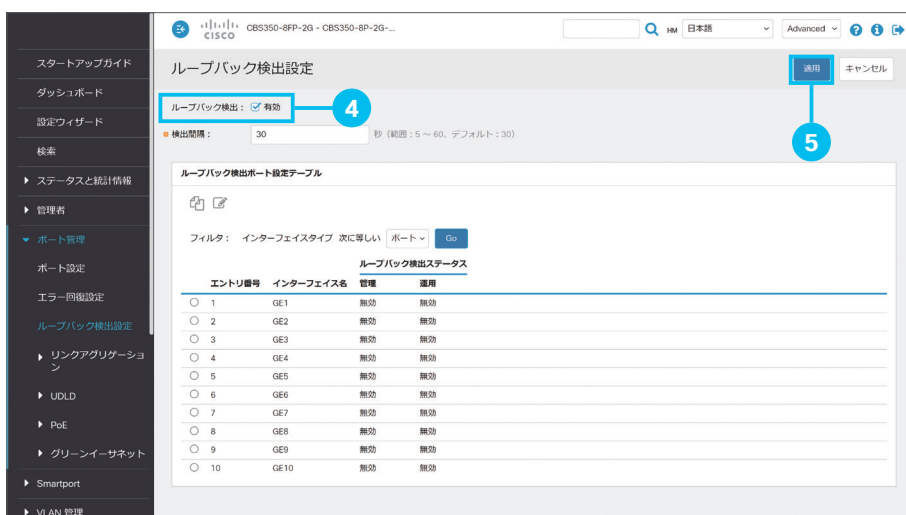
ループバック検出は Basic モードでは表示されないため、Advanced モードに切り替えます。



- 2 [ポート管理] をクリック



3 [ループバック検出設定] をクリック



4 [ループバック検出] の [有効] チェックボックスをクリックして選択

必要に応じて、[検出間隔] に任意の値 (秒) を入力することで、ループプロトコルパケットの送信間隔をデフォルトの 30 秒から変更することができます。

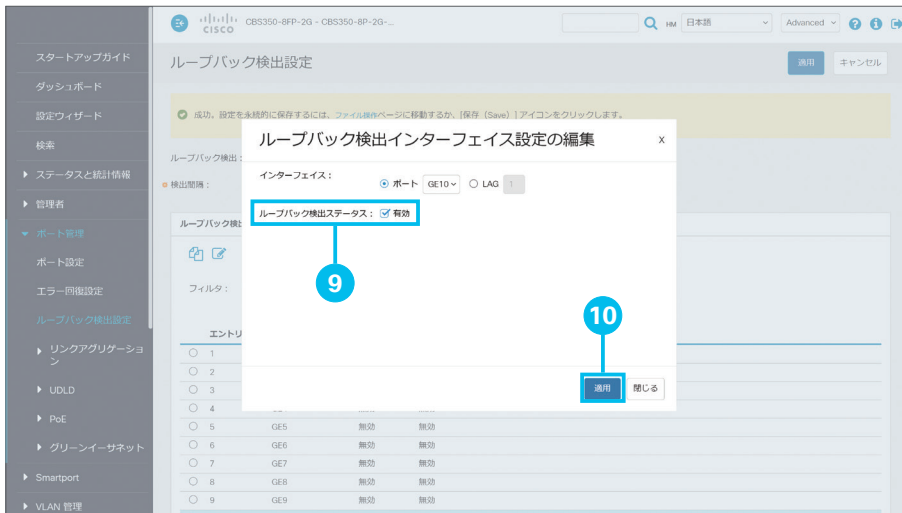
5 [適用] をクリック



6 [成功] メッセージが表示されたことを確認

7 [エントリ番号] 列 [10] のラジオボタンをクリックして 10 番ポートを選択

8 編集 [編集] アイコンをクリック



9 [ループバック検出ステータス] の [有効] チェックボックスをクリックして選択

10 [適用] をクリック



11 [成功] メッセージが表示されたことを確認

12 [閉じる] をクリック

4-3 Auto Smartport を設定する

マネージドスイッチは、接続するネットワーク機器や端末に応じて最適な設定をスイッチポートに適用できる「Smartport」をサポートします。スイッチやワイヤレスアクセスポイント、ルータなどのネットワーク機器、デスクトップ PC やサーバ、IP フォンや IP カメラなどの端末、さらにホストやゲストなどの用途向けに、事前に最適化された設定 (Smartport マクロ)を選択して適用できます。

さらにマネージドスイッチは、接続するネットワーク機器や端末に応じて Smartport マクロを自動的に適用できる「Auto Smartport」をサポートします。たとえば、あるスイッチポートにワイヤレスアクセスポイントを接続すると、そのスイッチポートにワイヤレスアクセスポイント用の Smartport マクロを自動的に適用することができます。本ガイドでは例として、Auto Smartport を有効化し、ワイヤレスアクセスポイントの接続による Smartport マクロの自動適用を確認します。

TIP MEMO

Auto Smartport は Basic モードでも有効化できますが、本ガイドでは Smartport マクロの適用状況を確認するために Advanced モードに切り替えます。Auto Smartport で検出するネットワーク機器の種類を変更する場合や Smartport マクロを編集する場合も、Advanced モードに切り替える必要があります。



1 表示モードのドロップダウンリストで [Advanced] を選択



2 [Smartport] をクリック



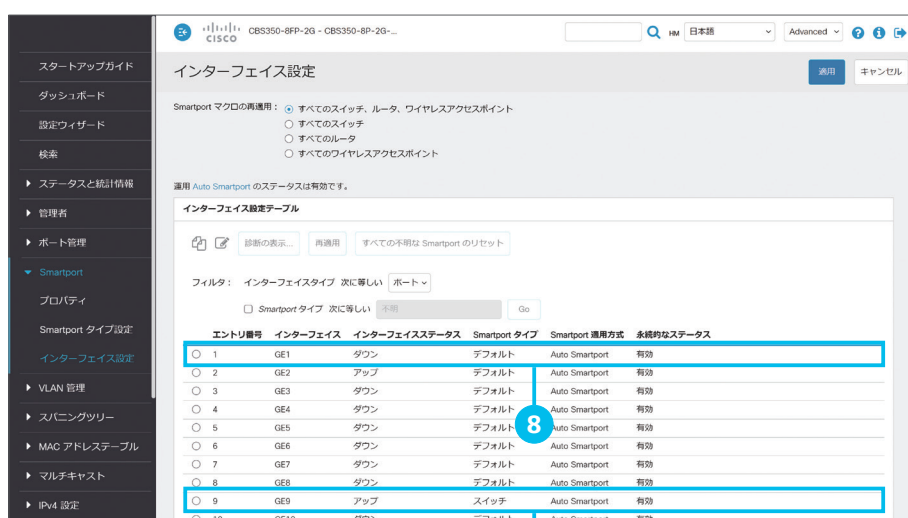
3 [管理 Auto Smartport] の [有効] ラジオボタンをクリックして選択

4 [適用] をクリック



5 [成功] メッセージが表示されたことを確認

6 [インターフェイス設定] をクリック



7 (例として) [エントリ番号] 列 [9] 行の [Smartport タイプ] 列が [スイッチ] であることを確認

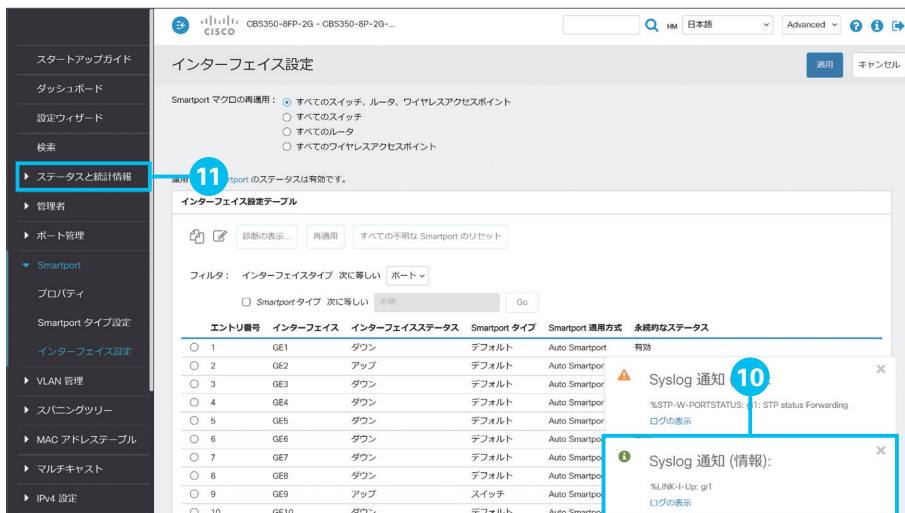
本ガイドでは 9 番ポートにスイッチを接続しているため、Auto Smartport によってスイッチの Smartport マクロ (Smartport タイプ) が適用されたことを確認できます。

8 (例として) [エントリ番号] 列 [1] 行の [Smartport タイプ] 列が [デフォルト] であることを確認

一方、本ガイドでは、この時点で 1 番ポートには何も接続していないため、Smartport マクロが適用されていない [デフォルト] であることを確認できます。

9 1 番ポートにワイヤレスアクセスポイントを接続

本ガイドでは例として、1 番ポートにワイヤレスアクセスポイントを接続して、Smartport マクロが自動的に適用されるかどうか確認します。

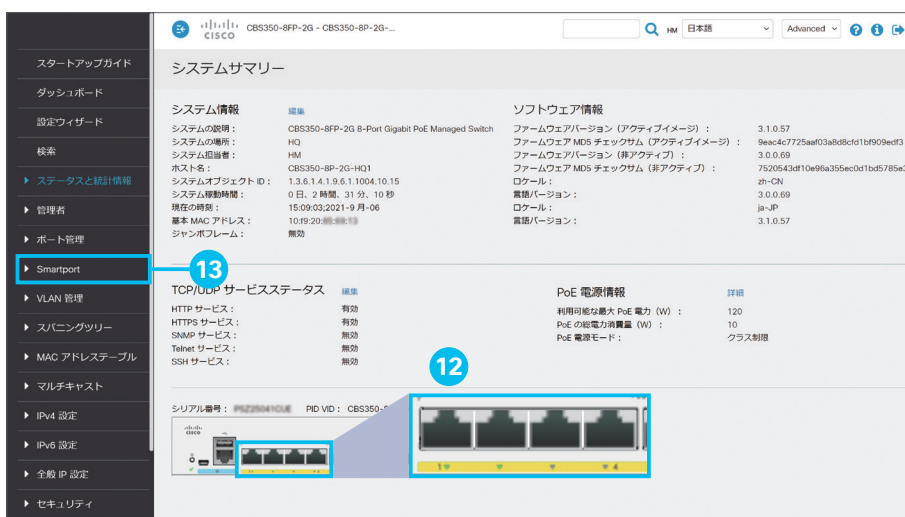


10 「Syslog 通知 (情報)」ポップアップウィンドウを確認

1 番ポートにワイヤレスアクセスポイントを接続すると、ポップアップウィンドウで 1 番ポートのインターフェイスステータスが「アップ」になったことが表示されます。

11 「ステータスと統計情報」をクリック

念のため、「ステータスと統計情報」で 1 番ポートの状態を確認します。



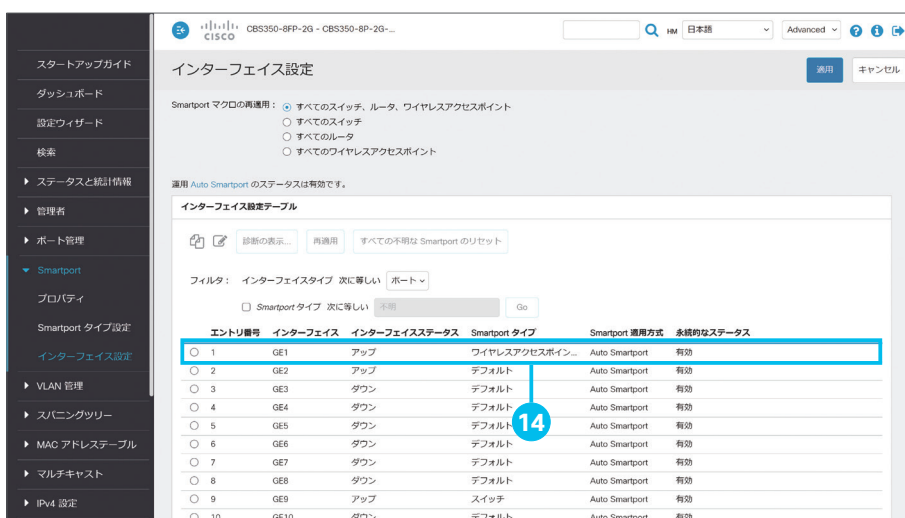
12 1 番ポートの LED が緑色であることを確認

「ステータスと統計情報」の「システムサマリー」では、マネージドスイッチの前面パネルイメージを確認できます。

1 番ポートの LED に相当する部分が緑色で表示されていれば、ワイヤレスアクセスポイントの接続が完了しています（実際のマネージドスイッチの LED は緑色で点滅します）。

13 [Smartport] をクリック

「Smartport」の「インターフェイス設定」に戻ります。

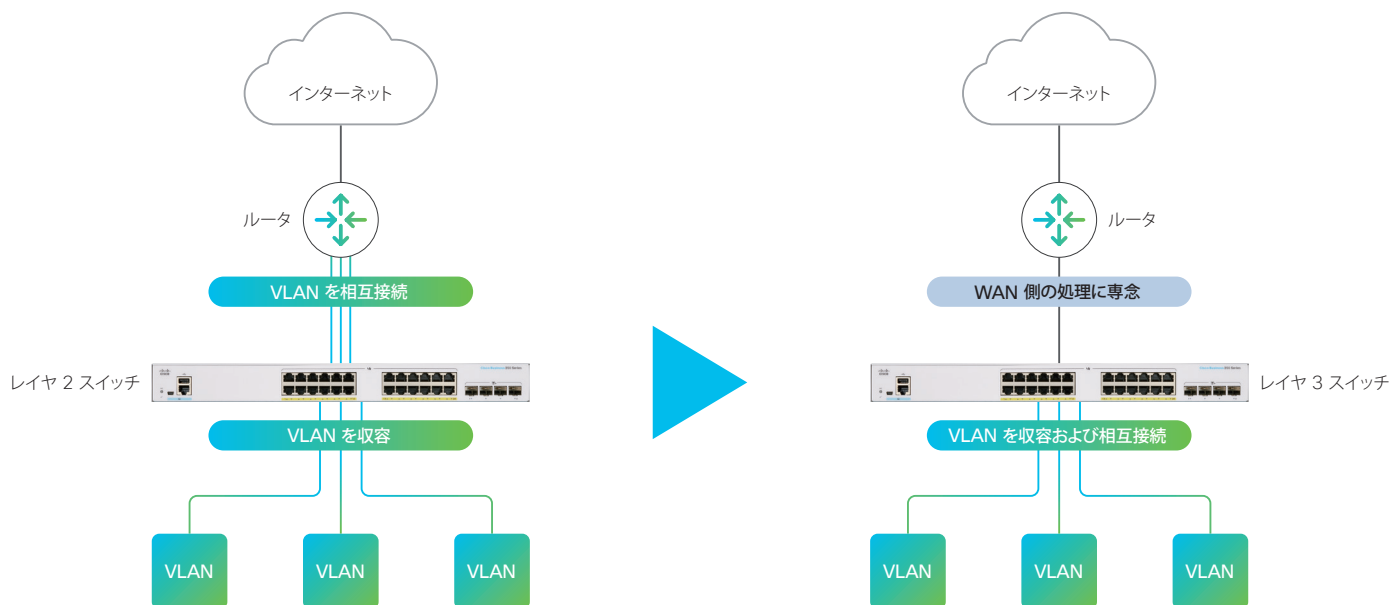


14 [エントリ番号] 列 [1] 行の [Smartport タイプ] 列が [ワイヤレスアクセスポイント] であることを確認

Auto Smartport によってワイヤレスアクセスポイントの Smartport マクロが適用されたことを確認できます。

5 レイヤ 3 機能を設定する

マネージドスイッチは、ダイナミック（動的）ルーティングや DHCP サーバなど、豊富なレイヤ 3 機能をサポートするレイヤ 3 スイッチでもあります。VLAN の相互接続など、ルータの役割をマネージドスイッチに担当させることで、ルータの負荷を軽減することができます。



本ガイドでは、VLAN の相互接続、VLAN とルータの相互接続（VLAN からインターネットに接続）など、使用頻度が高いレイヤ 3 機能に絞って設定例を紹介します。

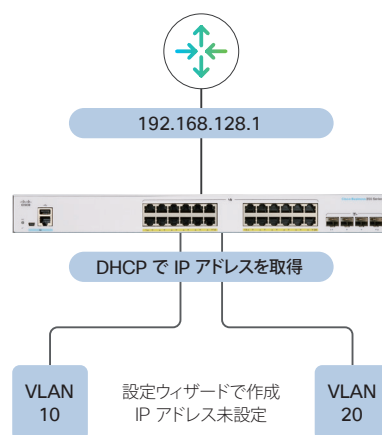
- 5-1 VLAN に IP アドレスを割り当てる（VLAN を相互接続する）
- 5-2 ホストに IP アドレスを自動的に割り当てる（DHCP サーバを設定する）
- 5-3 VLAN とルータを相互接続する（VLAN からインターネットを利用する）
- 5-4 ダイナミックルーティングを設定する（RIPv2 を設定する）

⚠ 注意

本ガイドの設定例は、次のネットワーク構成を前提に紹介します。

- ルータの（LAN 側）IP アドレスは 192.168.128.1、ルータが DHCP サーバとして機能
- マネージドスイッチのネイティブ VLAN の IP アドレスはルータから DHCP で取得（プラグアンドプレイ）
- マネージドスイッチの設定ウィザードで VLAN を新規作成済み、VLAN の IP アドレスは未設定

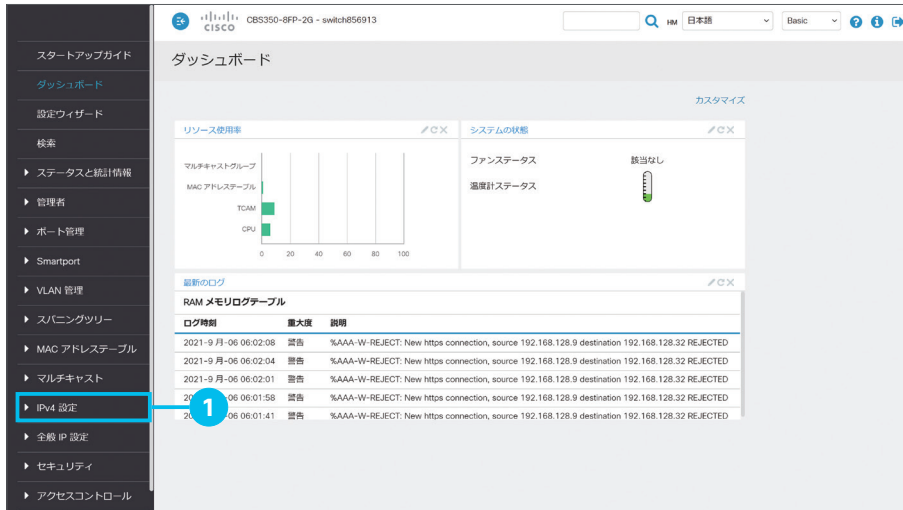
一部の設定例では、ルータの設定を変更する必要があります（詳細は、お使いの機器のマニュアルを参照してください）。また、マネージドスイッチは Advanced モードで設定します。



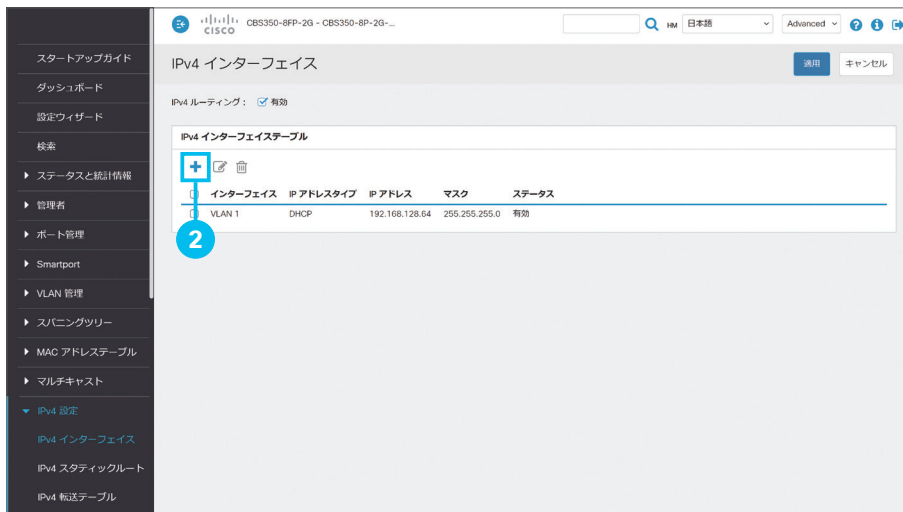
5-1

VLAN に IP アドレスを割り当てる (VLAN を相互接続する)

VLAN に IP アドレスを割り当てると、マネージドスイッチが VLAN を自動的に相互接続します。本ガイドでは例として、「3-2 VLAN 設定ウィザードを使用する」で作成した VLAN に スタティック IP アドレス を割り当てます。



1 [IPv4 設定] をクリック



2 [+] アイコンをクリック

デフォルトでは、ネイティブ VLAN に IP アドレスが割り当てられていることを確認できます。
[+] アイコンをクリックして、「3-2 VLAN 設定ウィザードを使用する」で作成した VLAN に IP アドレスを割り当てます。



- 3 [インターフェイス] の [VLAN] ドロップダウンリストで設定したい VLAN ID を選択

本ガイドでは例として、「3-2 VLAN 設定ウィザードを使用する」で作成した VLAN 10 を選択します。

- 4 [IP アドレスタイプ] で [スタティック IP アドレス] をクリックして選択

本ガイドでは「7-2 ホストに IP アドレスを自動的に割り当てる (DHCP サーバを設定する)」で DHCP サーバを有効化するため、スタティック IP アドレスを設定します。

- 5 [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、「192.168.10.1」を入力します。

- 6 [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」を入力します。

- 7 [適用] をクリック



- 8 [成功] メッセージが表示されたことを確認

続けて、「3-2 VLAN 設定ウィザードを使用する」で作成した VLAN 20 を設定します。

- 9 [インターフェイス] の [VLAN] ドロップダウンリストで設定したい VLAN ID を選択

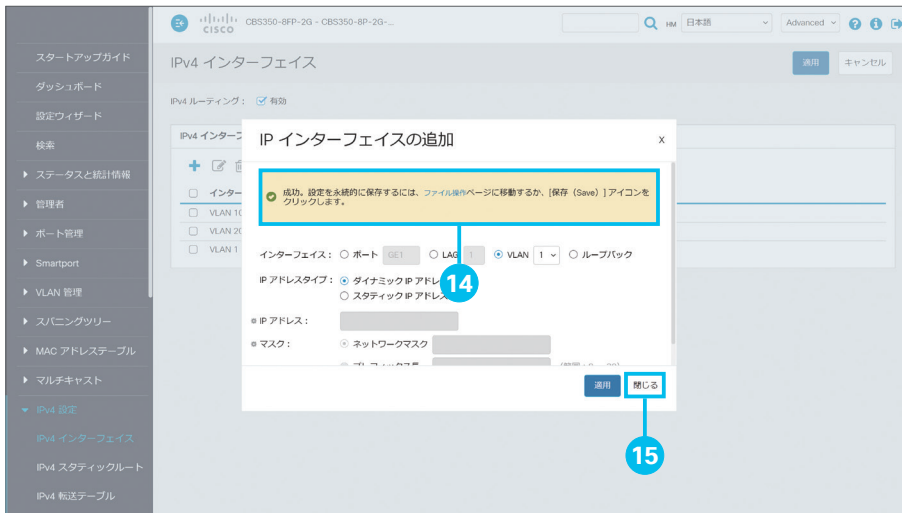
- 10 [IP アドレスタイプ] で [スタティック IP アドレス] をクリックして選択

- 11 [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、「192.168.20.1」を入力します。

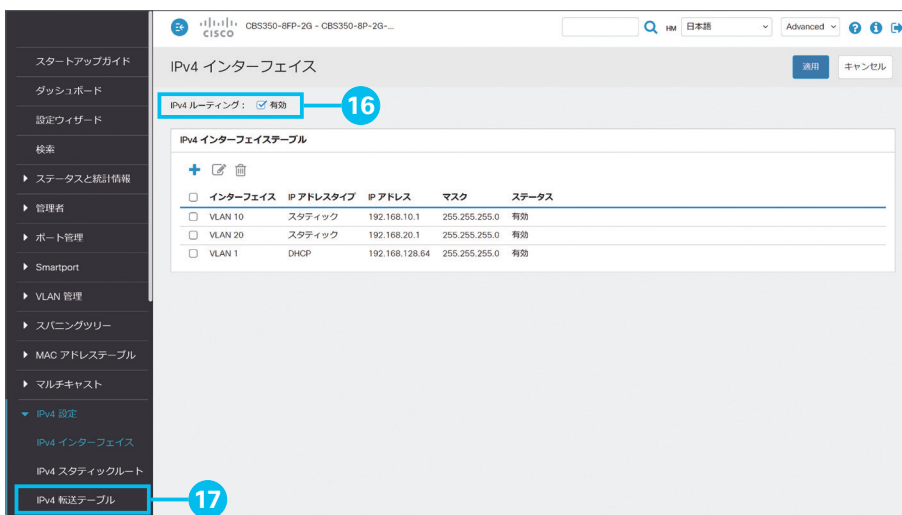
- 12 [ネットワークマスク] に任意のサブネットマスクを入力

- 13 [適用] をクリック



14 [成功] メッセージが表示されたことを確認

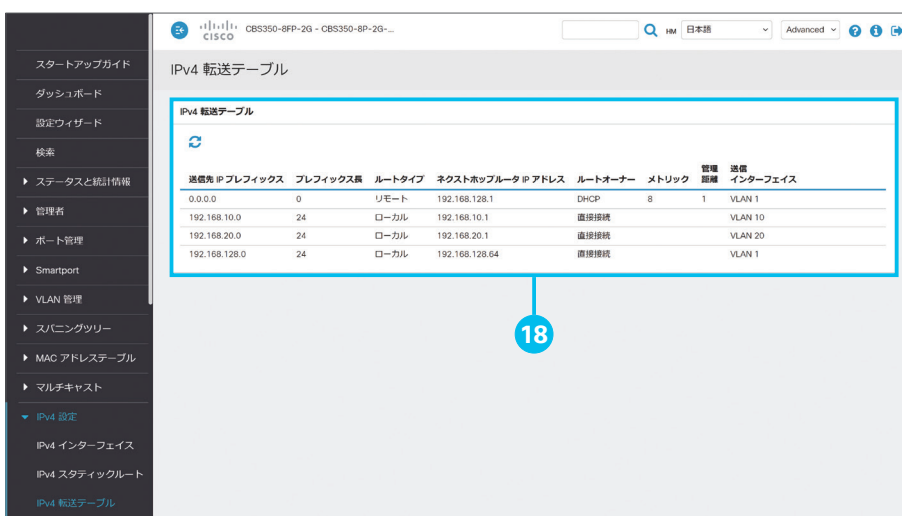
15 [閉じる] をクリック



16 [IPv4 ルーティング] の [有効] が選択されていることを確認

デフォルトでは IPv4 ルーティングが有効化されているため、VLAN に IP アドレスを割り当てると、その VLAN への転送ルートが自動的に設定されます。

17 [IPv4 転送テーブル] をクリック



18 [IPv4 転送テーブル] を確認

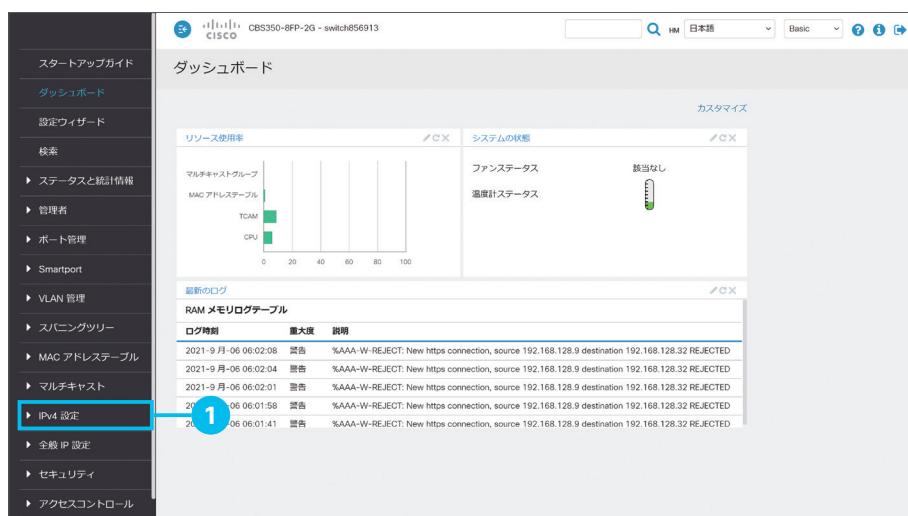
各 VLAN の転送ルートが設定されて、相互に接続可能になったことを確認できます。たとえば、[送信先 IP プレフィックス]/[プレフィックス長] が「192.168.10.0/24」のネットワークは VLAN 10 を表します。VLAN 10 宛の通信は、「ローカル」すなわちマネージドスイッチ内部の [ネクストホップルータ IP アドレス] である「192.168.10.1」(VLAN 10 のゲートウェイ) に転送されることがわかります。

5-2 ホストに IP アドレスを自動的に割り当てる (DHCP サーバを設定する)

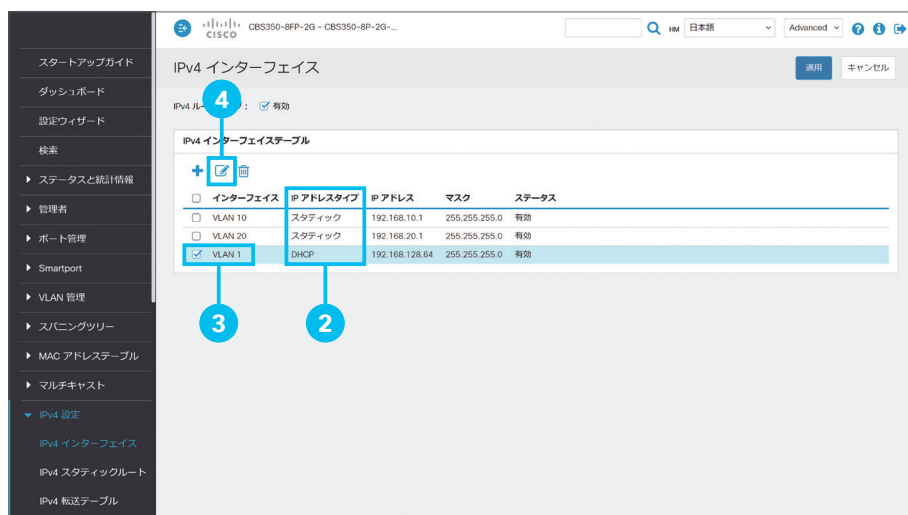
マネージドスイッチは、PC などマネージドスイッチに直接接続するホストに IP アドレスを自動的に割り当てる、DHCP サーバ機能をサポートします。ただし、マネージドスイッチのポートや VLAN など何らかのインターフェイスが、外部の DHCP サーバから IP アドレスを取得する DHCP クライアントとして動作している場合は、マネージドスイッチの DHCP サーバ機能を有効化できません。本ガイドでは例として、DHCP クライアントとして動作しているネイティブ VLAN にスタティック IP アドレスを設定し、そのうえで各 VLAN 接続用に DHCP サーバを設定します。

注意

本ガイドの設定例で前提とするネットワーク構成のように、ルータなど外部の DHCP サーバからマネージドスイッチ (ネイティブ VLAN) の IP アドレスを取得している場合は、マネージドスイッチにスタティック IP アドレスを設定する前に、外部の DHCP サーバでマネージドスイッチに割り当てる IP アドレスを固定する必要があります。詳細は、お使いの機器のマニュアルを参照してください。



1 [IPv4 設定] をクリック



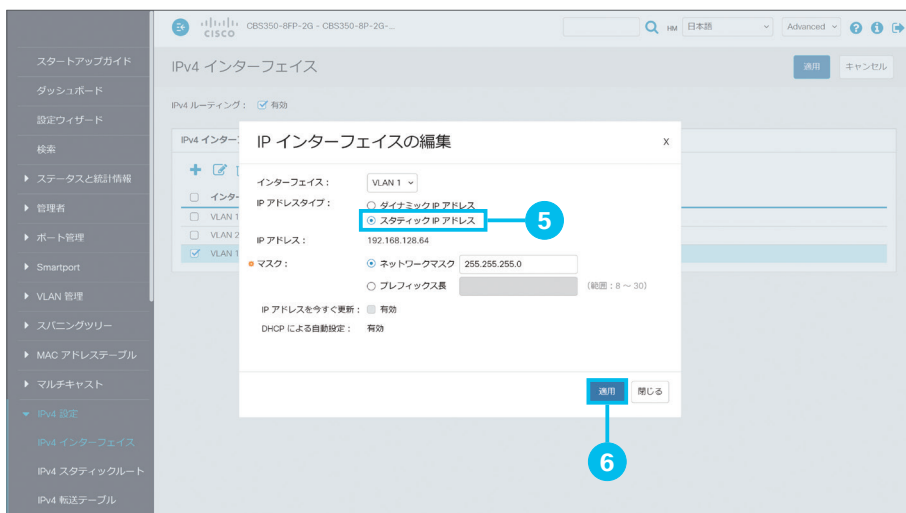
2 各インターフェイスの [IP アドレスタイプ] 列を確認

[IP アドレスタイプ] が「DHCP」であるインターフェイスが存在する場合、DHCP サーバを有効化できません。

3 [IP アドレスタイプ] が「DHCP」であるインターフェイスのチェックボックスをクリックして選択

本ガイドでは例として、プラグアンドプレイで DHCP クライアントとして動作するように設定された、ネイティブ VLAN である [VLAN 1] のチェックボックスをクリックして選択します。

4 編集 [編集] アイコンをクリック



5 [IP アドレスタイプ] で [スタティック IP アドレス] をクリックして選択

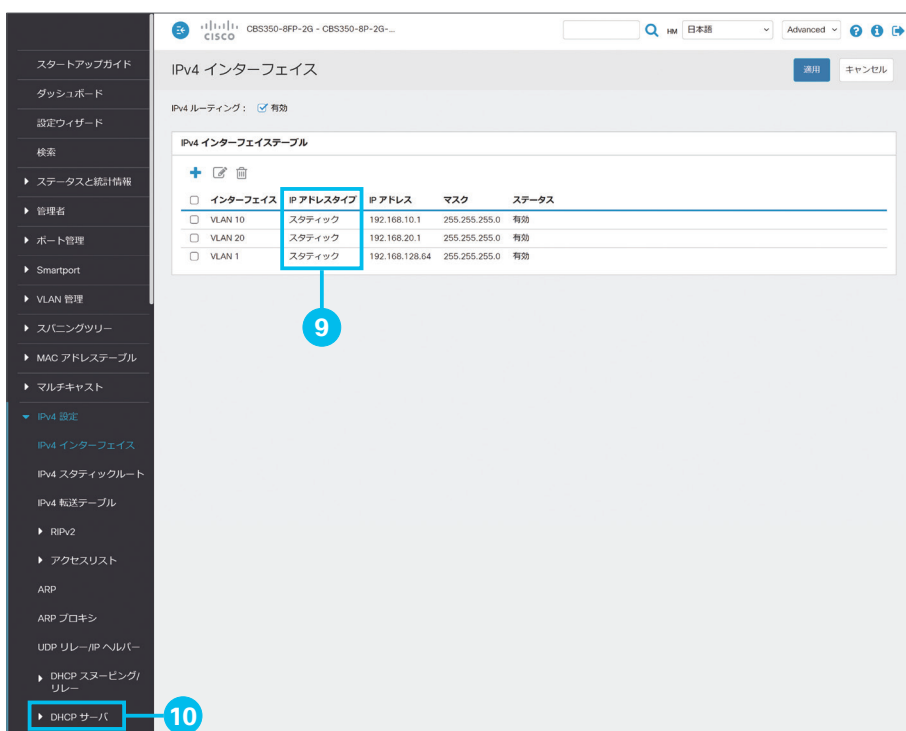
[スタティック IP アドレス] をクリックして選択すると、外部の DHCP サーバから割り当てられた IP アドレスがスタティック IP アドレスとして設定されます。

6 [適用] をクリック



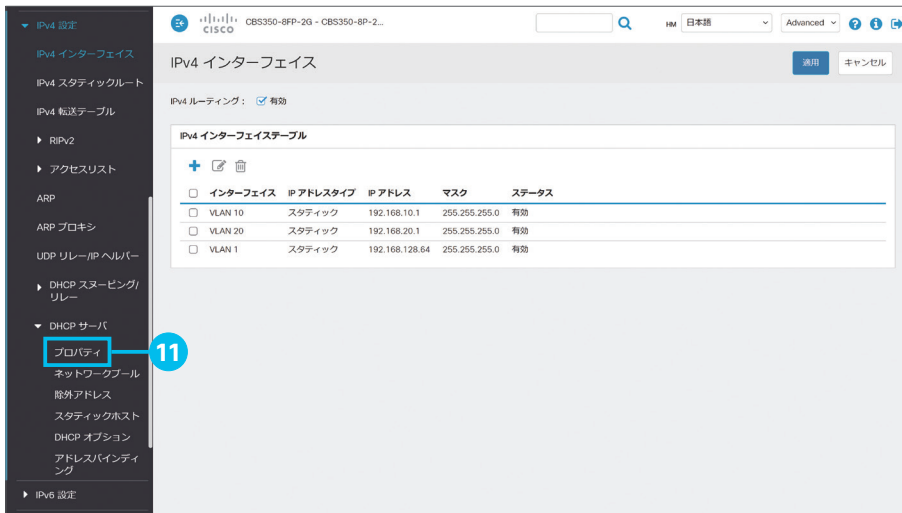
7 [成功] メッセージが表示されたことを確認

8 [閉じる] をクリック

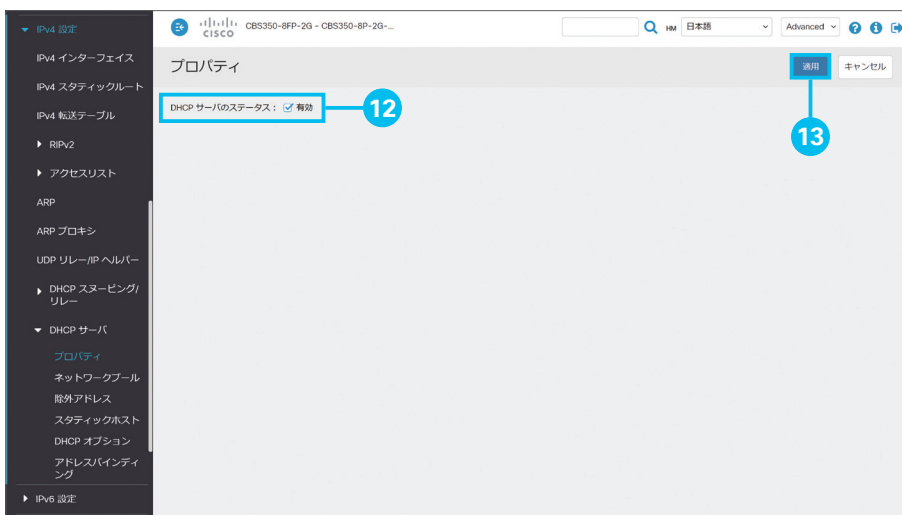


9 各インターフェイスの [IP アドレスタイプ] 列が「スタティック」であることを確認

10 [DHCP サーバ] をクリック



11 [プロパティ] をクリック



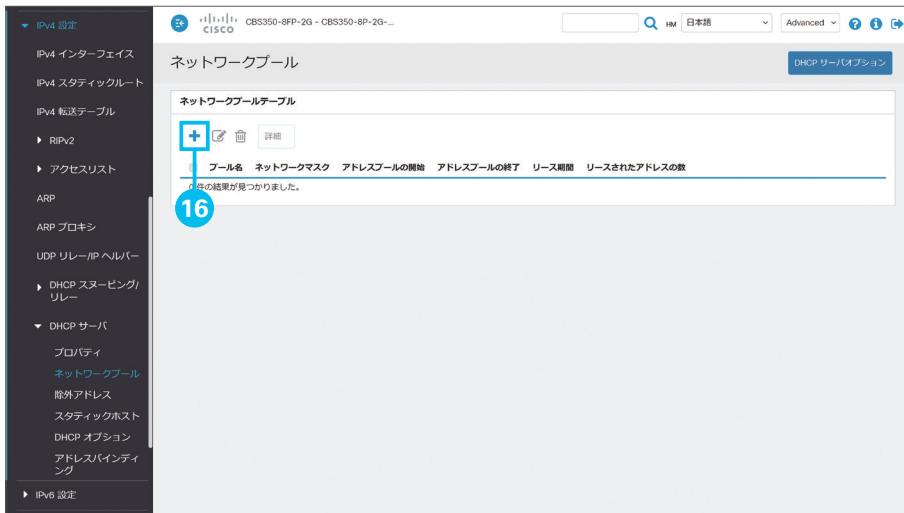
12 [DHCP サーバのステータス] の [有効] チェックボックスをクリックして選択

13 [適用] をクリック



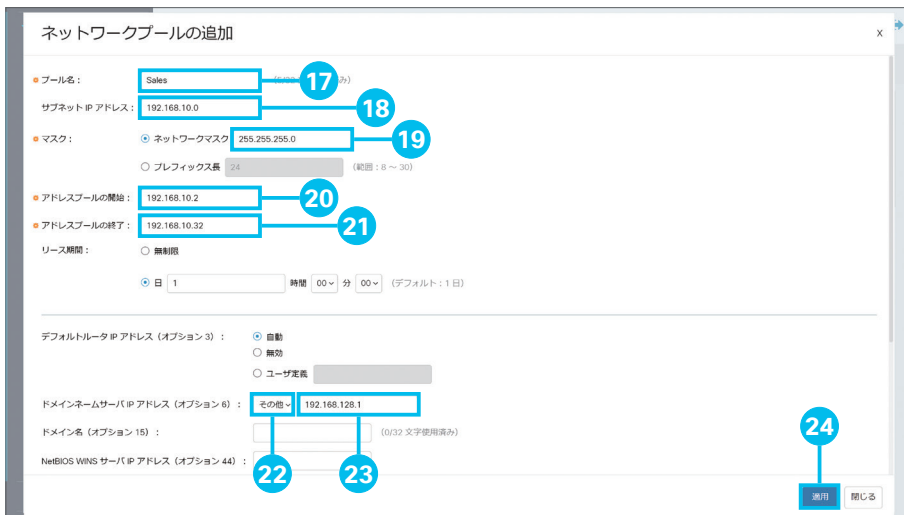
14 [成功] メッセージが表示されたことを確認

15 [ネットワークプール] をクリック



16 [+] アイコンをクリック

まず、VLAN 10 用のネットワークプールを作成します。



17 [プール名] に任意の名前を入力

本ガイドでは例として、VLAN 10 の名前である「Sales」を入力します。

18 [サブネット IP アドレス]に任意のサブネット IP アドレスを入力

本ガイドでは例として、VLAN 10 のサブネットである「192.168.10.0」を入力します。

19 [ネットワークマスク] に任意のネットワークマスクを入力

本ガイドでは例として、「255.255.255.0」を入力します。

20 [アドレスプールの開始] に任意の IP アドレスを入力

21 [アドレスプールの終了] に任意の IP アドレスを入力

[アドレスプールの開始] に入力した IP アドレスから [アドレスプールの終了] に入力した IP アドレスの範囲で、接続するホストに IP アドレスを自動的に割り当てます。

22 [ドメインネームサーバ IP アドレス (オプション 6)] のドロップダウンリストで [その他] を選択

23 [ドメインネームサーバ IP アドレス (オプション 6)] に DNS サーバの IP アドレスを入力

本ガイドでは例として、ルータの IP アドレスである「192.168.128.1」を入力します。

24 [適用] をクリック

ネットワークプールの追加

成功。設定を永続的に保存するには、ファイル操作ページに移動するか、[保存 (Save)] アイコンをクリックします。

● プール名: Finance (26)

● サブネット IP アドレス: 192.168.20.0 (27)

● マスク: ネットワークマスク 255.255.255.0 (28) プレフィックス長 24 (範囲: 8 ~ 30)

● アドレスプールの開始: 192.168.20.2 (29)

● アドレスプールの終了: 192.168.20.32 (30)

リース期間: 無制限 日 1 時間 00 分 00 (デフォルト: 1 日)

デフォルトルータ IP アドレス (オプション 3): 自動 ユーザ定義 (32)

ドメインネームサーバ IP アドレス (オプション 6): その他 192.168.128.1 (31)

適用 閉じる (33)

25 [成功] メッセージが表示されたことを確認

続けて、VLAN 20 用のネットワークプールを作成します。

26 [プール名] に任意の名前を入力

本ガイドでは例として、VLAN 20 の名前である「Finance」を入力します。

27 [サブネット IP アドレス]に任意のサブネット IP アドレスを入力

本ガイドでは例として、VLAN 20 のサブネットである「192.168.20.0」を入力します。

28 [ネットワークマスク] に任意のネットワークマスクを入力

29 [アドレスプールの開始] に任意の IP アドレスを入力

30 [アドレスプールの終了] に任意の IP アドレスを入力

31 [ドメインネームサーバ IP アドレス (オプション 6)] のドロップダウンリストで [その他] を選択

32 [ドメインネームサーバ IP アドレス (オプション 6)] に DNS サーバの IP アドレスを入力

本ガイドでは例として、ルータの IP アドレスである「192.168.128.1」を入力します。

33 [適用] をクリック

ネットワークプールの追加

成功。設定を永続的に保存するには、ファイル操作ページに移動するか、[保存 (Save)] アイコンをクリックします。

● プール名: (0/32 文字使用済み)

● サブネット IP アドレス:

● マスク: ネットワークマスク プレフィックス長 (範囲: 8 ~ 30)

● アドレスプールの開始:

● アドレスプールの終了:

リース期間: 無制限 日 1 時間 00 分 00 (デフォルト: 1 日)

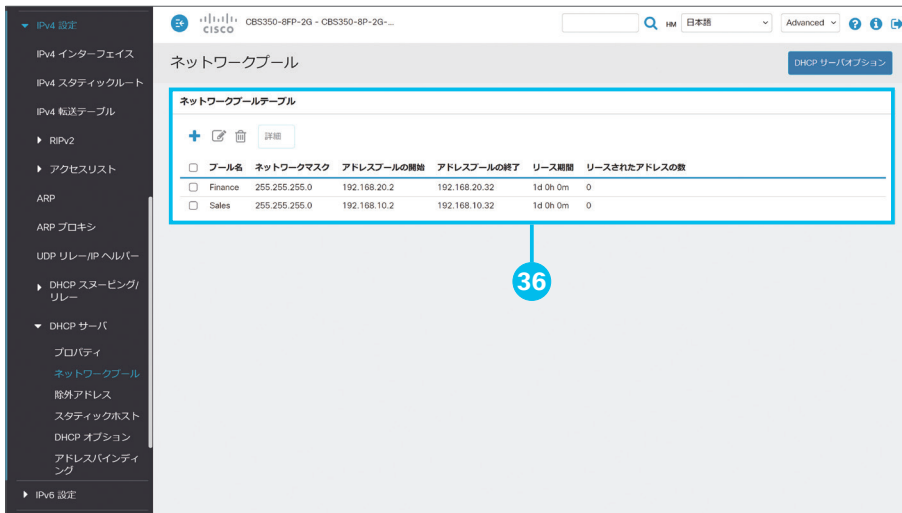
デフォルトルータ IP アドレス (オプション 3): 自動 無効 ユーザ定義

ドメインネームサーバ IP アドレス (オプション 6): なし

適用 閉じる (35)

34 [成功] メッセージが表示されたことを確認

35 [閉じる] をクリック



36 [ネットワークポリシー]を確認

VLAN 10 および VLAN 20 に接続するホストに IP アドレスが自動的に割り当てられるようになりました。

5-3 VLAN とルータを相互接続する (VLAN からインターネットを利用する)

「5-1 VLAN に IP アドレスを割り当てる (VLAN を相互接続する)」の設定によって、たとえば VLAN 10 に接続した PC から VLAN 20 に接続したプリンタを利用したり、VLAN 20 に接続した PC から VLAN 10 に接続したサーバを利用したりすることができるようになりました。

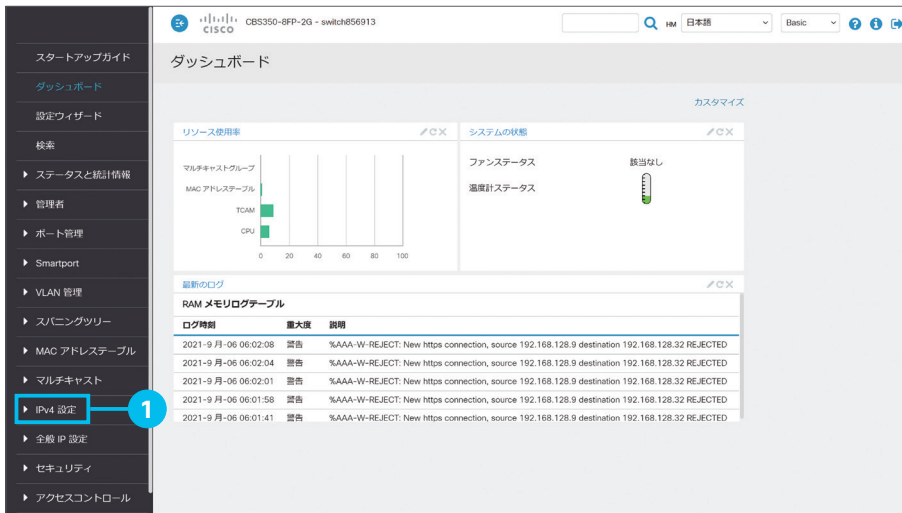
しかし、VLAN 10 および VLAN 20 に接続した PC などホストからインターネットを利用することは、まだできません。VLAN 10 および VLAN 20 とルータを相互接続するための転送ルートが設定されていないためです。VLAN とルータを相互接続して VLAN からインターネットを利用できるようにするためには、次の 2 つの転送ルートを設定する必要があります。

- マネージドスイッチ側：VLAN からインターネットに向かう通信をルータに転送する
- ルータ側：インターネットから VLAN に向かう通信をマネージドスイッチに転送する

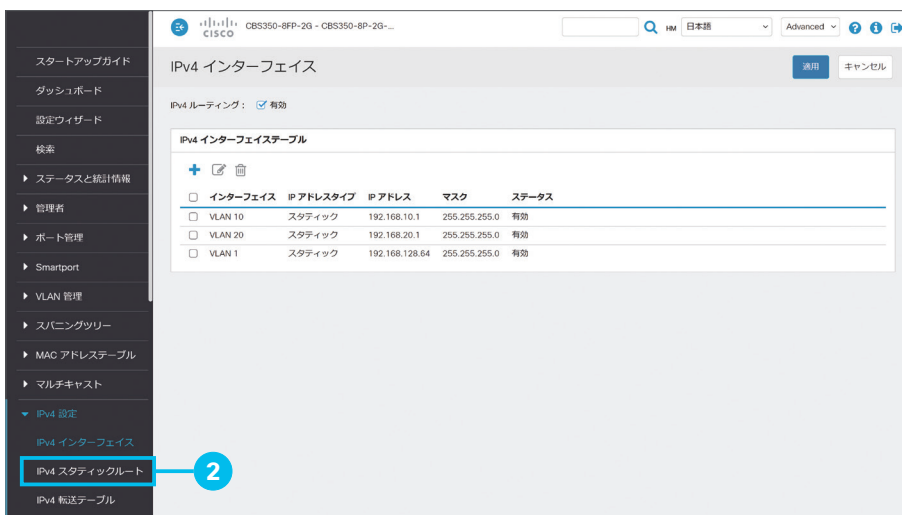
本ガイドでは例として、VLAN からインターネットに向かう通信をルータに転送する、マネージドスイッチ側の スタティックルート を設定します。

注意

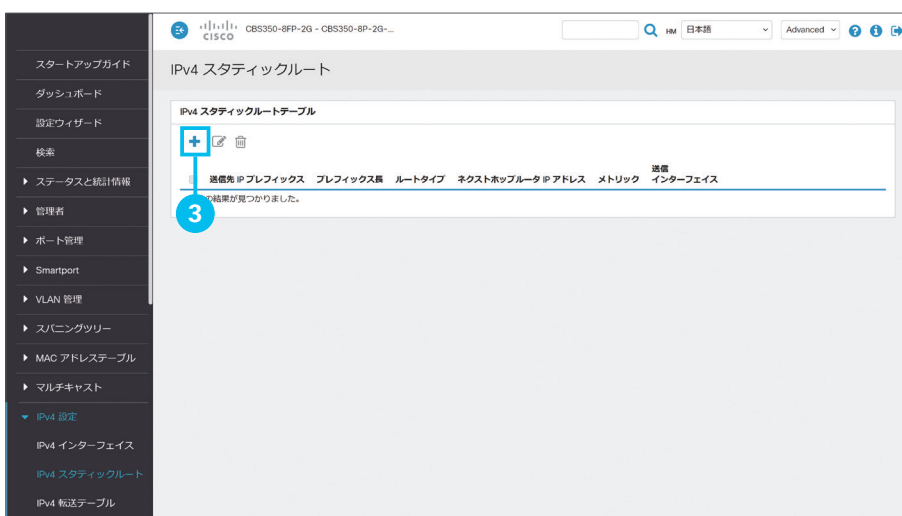
インターネットから VLAN に向かう通信をマネージドスイッチに転送する、ルータ側のスタティックルートを設定する必要もあります。本ガイドでは一例として、Cisco Meraki MX の設定画面例を紹介しますが、手順は省略します。詳細は、お使いの機器のマニュアルを参照してください。



1 [IPv4 設定] をクリック

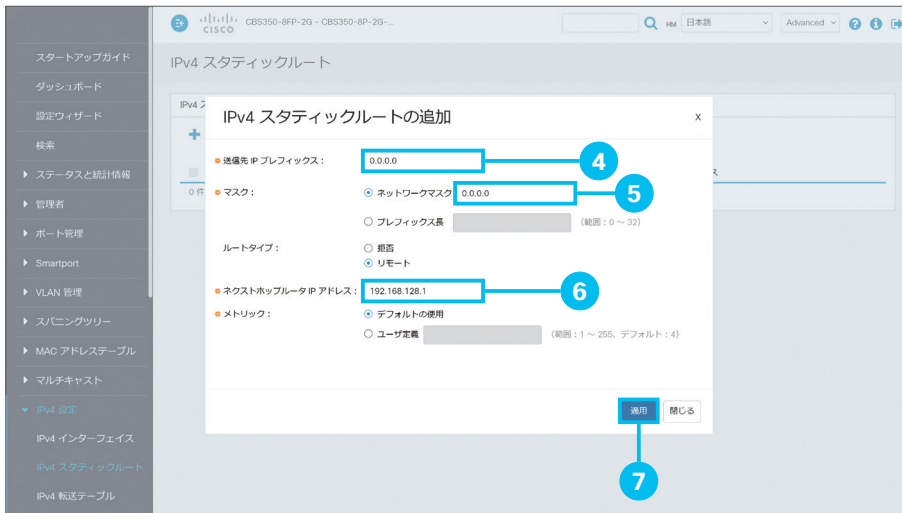


2 [IPv4 スタティックルート] をクリック



3 [+ アイコン] をクリック

まず、VLAN 10 用のネットワークプールを作成します。



4 [送信先 IP プレフィックス] に「0.0.0.0」を入力

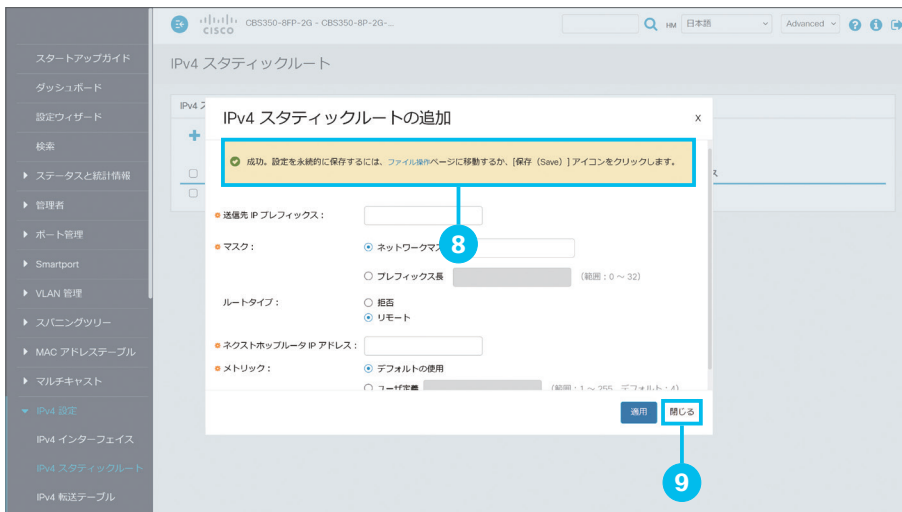
「0.0.0.0」は「任意の IP アドレス」を表します。

5 [ネットワークマスク] に「0.0.0.0」を入力

6 [ネクストホップルータ 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、ルータの IP アドレスである「192.168.128.1」を入力します。

7 [適用] をクリック



8 [成功] メッセージが表示されたことを確認

9 [閉じる] をクリック

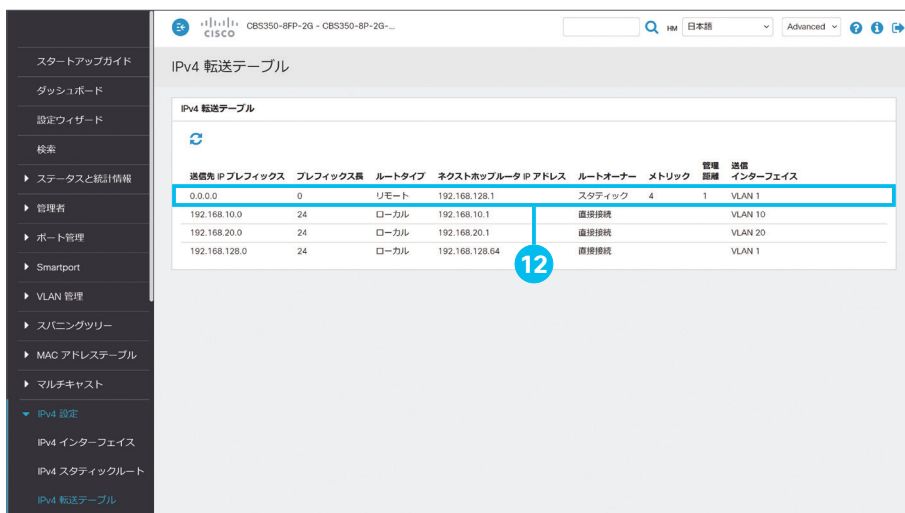


10 [IPv4 スタティックルートテーブル] を確認

[送信先 IP プレフィックス] / [プレフィックス長] が「0.0.0.0/0」宛の通信は、「リモート」すなわちマネージドスイッチ外部の [ネクストホップルータ IP アドレス] である 192.168.128.1 (ルータのゲートウェイ) に転送されることがわかります。

この特殊な表記「0.0.0.0/0」は任意の宛先を表すため、0.0.0.0/0 宛の転送ルートを「デフォルトルート」と呼びます。

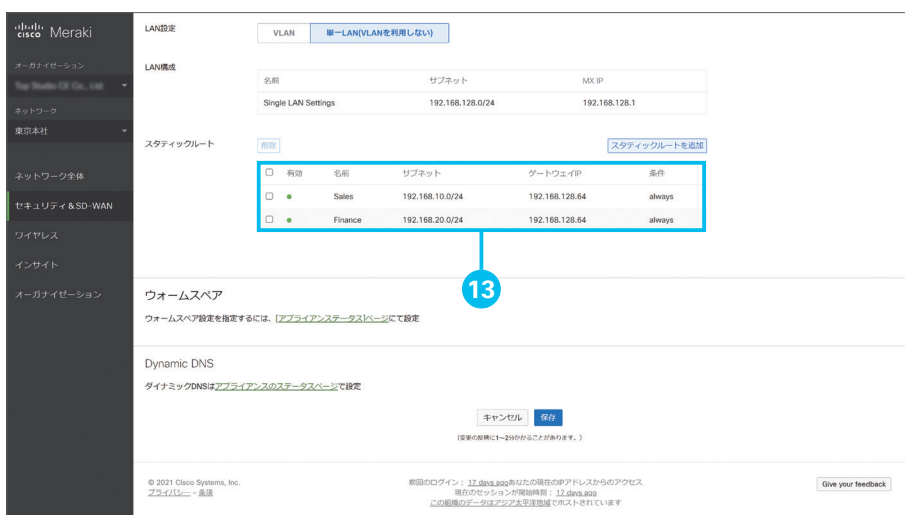
11 [IPv4 転送テーブル] をクリック



12 [IPv4 転送テーブル] を確認

各 VLAN の転送ルートとは別にデフォルトルートが設定されたことを確認できます。各 VLAN に向かう通信を除く任意の通信、たとえばインターネットに向かう通信は、このデフォルトルートに従って 192.168.128.1、すなわちルータに転送されます。

マネージドスイッチ側の設定は完了しました。ルータ側の設定画面例を紹介します。



13 ルータ側のスタティックルートを設定

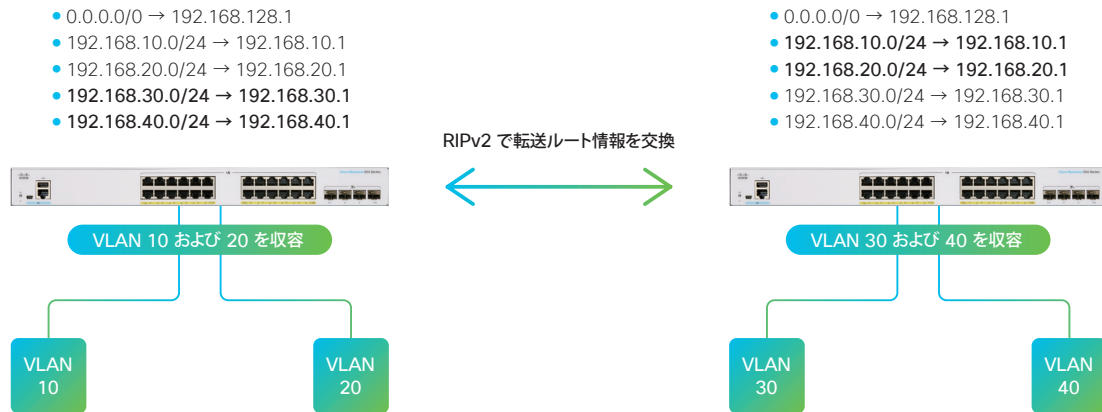
Cisco Meraki MX のスタティックルート設定画面例です。

2 つのスタティックルートが存在し、[サブネット] すなわち VLAN 10 (192.168.10.0/24) および VLAN 20 (192.168.20.0/24) 宛の通信が [ゲートウェイ IP] すなわちマネージドスイッチ (192.168.128.64) に転送されることがわかります。

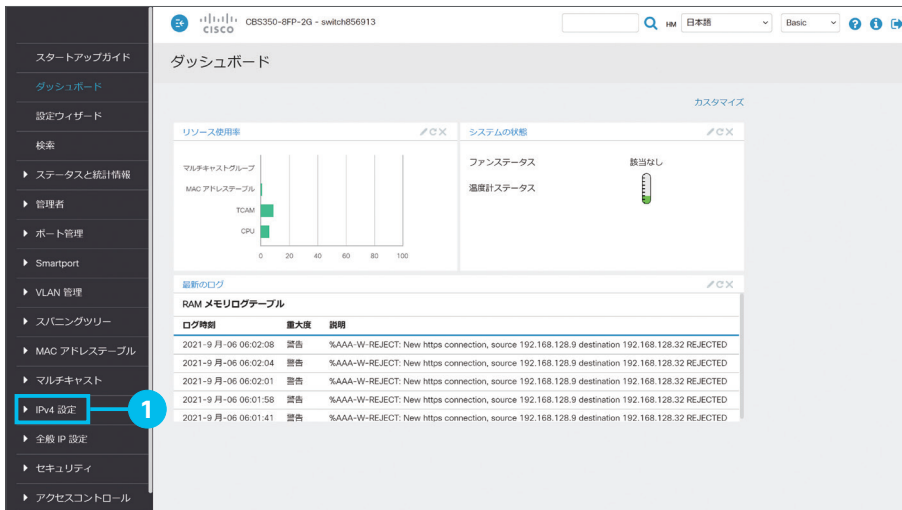
5-4

ダイナミックルーティングを設定する (RIPv2 を設定する)

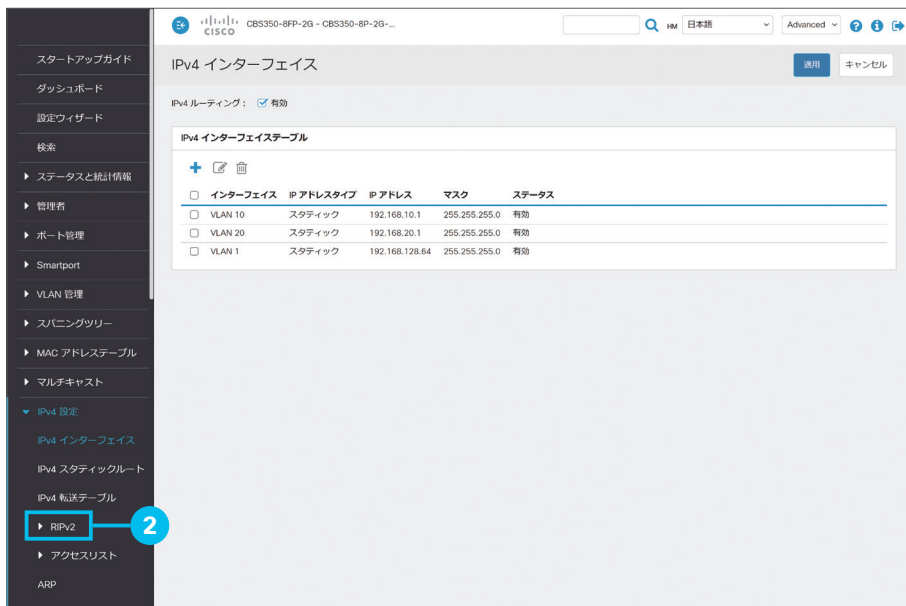
マネージドスイッチは、ダイナミックルーティング プロトコルである RIPv2 (Routing Information Protocol version 2) をサポートします。 RIPv2 によって、複数のマネージドスイッチ間で転送ルート情報を自動的に交換することができるため、常に最適な転送テーブルを使用できます。たとえば、あるマネージドスイッチで VLAN を新規作成したことで追加された転送ルート情報は、別のマネージドスイッチの転送テーブルに自動的に反映されるため、面倒な手動設定の必要がなくなります。



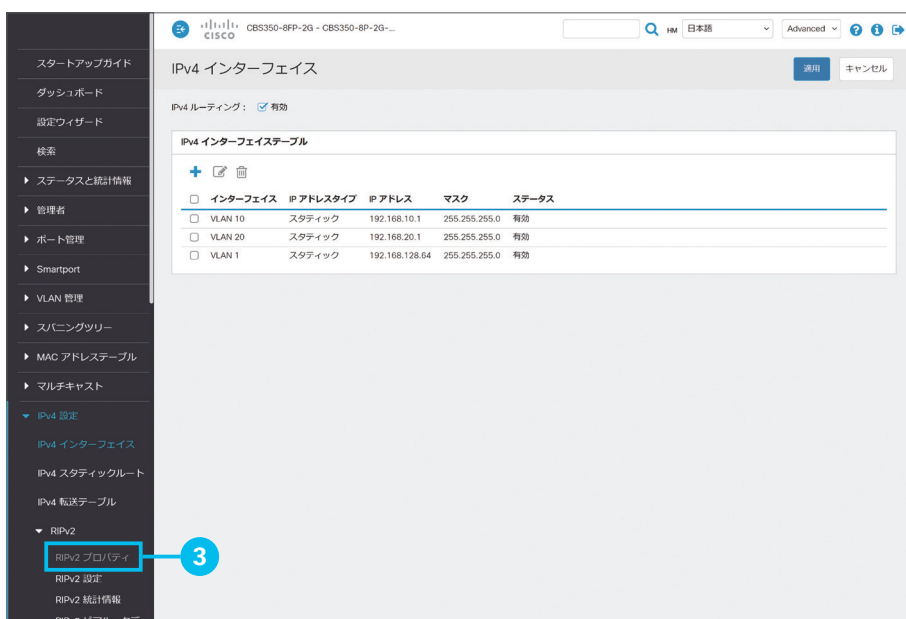
本ガイドでは例として、RIPv2 を有効化して、VLAN 10 および VLAN 20 の転送ルート情報を他のマネージドスイッチに送信できるようにします。



1 [IPv4 設定] をクリック



2 [RIPv2] をクリック



3 [RIPv2 プロパティ] をクリック



4 [RIP] の [有効] をクリックして選択

5 [適用] をクリック

「5-3 VLAN とルータを相互接続する(VLAN からインターネットを利用する)」で設定したデフォルトルート情報を他のマネージドスイッチに送信する場合は、「デフォルトルート アドバタイズメント」の [有効] をクリックして選択します。



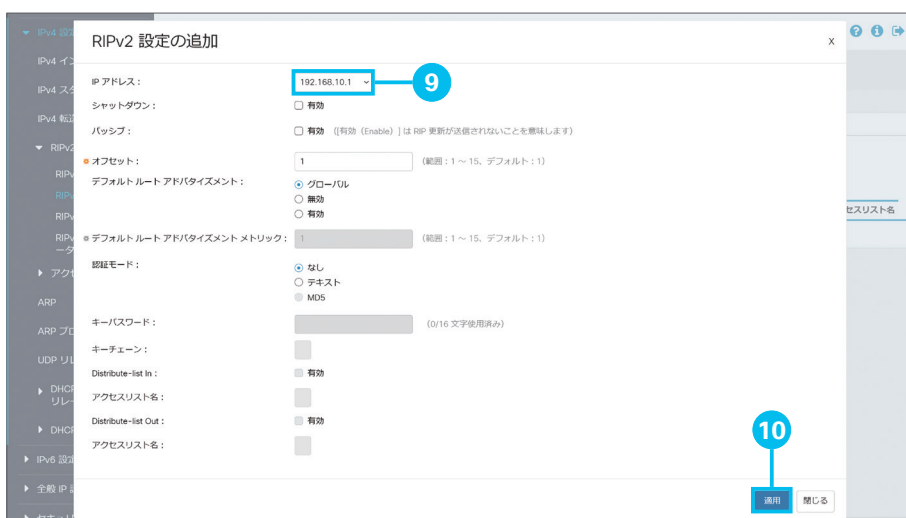
6 [成功] メッセージを確認

RIPv2 を有効化すると、他のマネージドスイッチから転送ルート情報を受信できるようになります。

7 [RIPv2 設定] をクリック



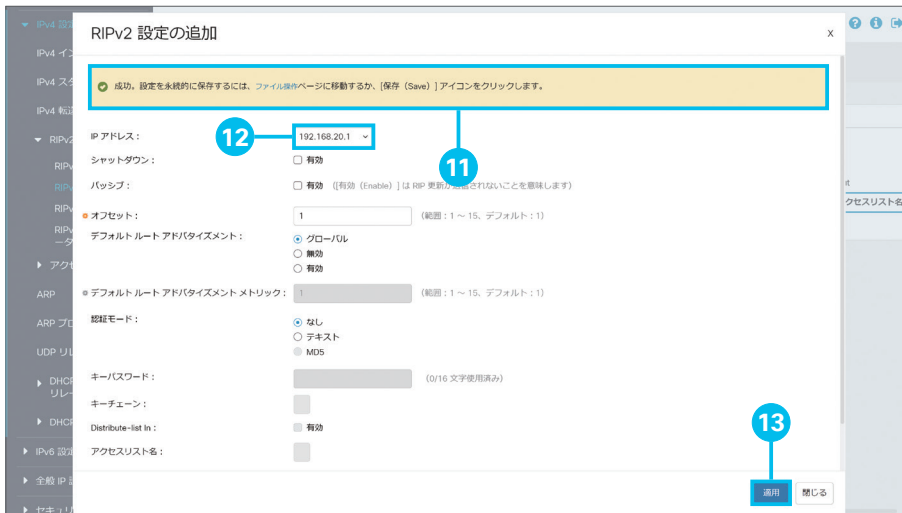
8 [+] アイコンをクリック



9 [IP アドレス] ドロップダウンリストで、RIPv2 を有効化したい VLAN の IP アドレスを選択

本ガイドでは例として、VLAN 10 の IP アドレスである「192.168.10.1」を選択します。

10 [適用] をクリック

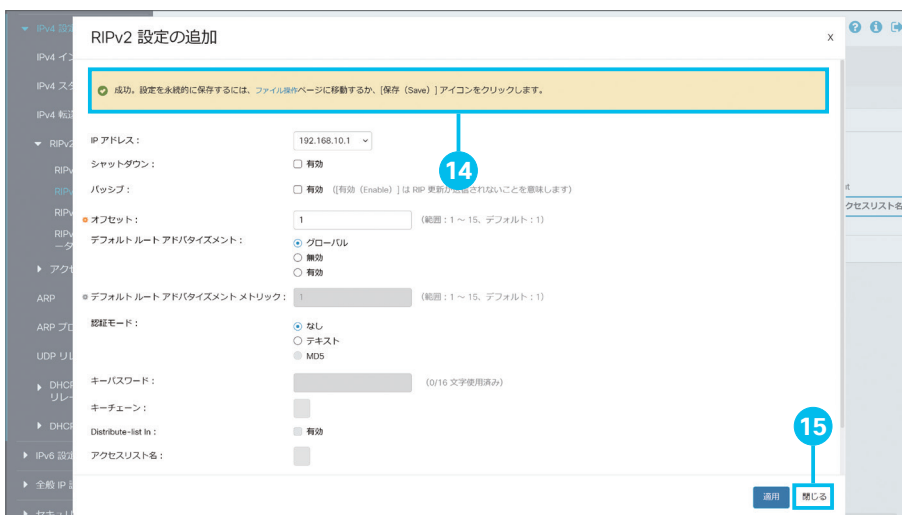


11 [成功] メッセージを確認

12 [IP アドレス] ドロップダウンリストで、RIPv2 を有効化したい VLAN の IP アドレスを選択

本ガイドでは例として、VLAN 20 の IP アドレスである「192.168.20.1」を選択します。

13 [適用] をクリック



14 [成功] メッセージを確認

15 [閉じる] をクリック



16 [RIP 設定テーブル] を確認

VLAN 10 の IP アドレスと VLAN 20 の IP アドレスが追加されたことがわかります。

17 [RIP 統計情報] をクリック

RIPv2 統計情報

RIP 統計情報テーブル

すべてのインターフェイスカウンタの...

IP インターフェイス	不正なパケットを受信しました	不正なルートを受信しました	更新が送信されました
192.168.10.1	0	0	2
192.168.20.1	0	0	1
192.168.128.64	0	0	0

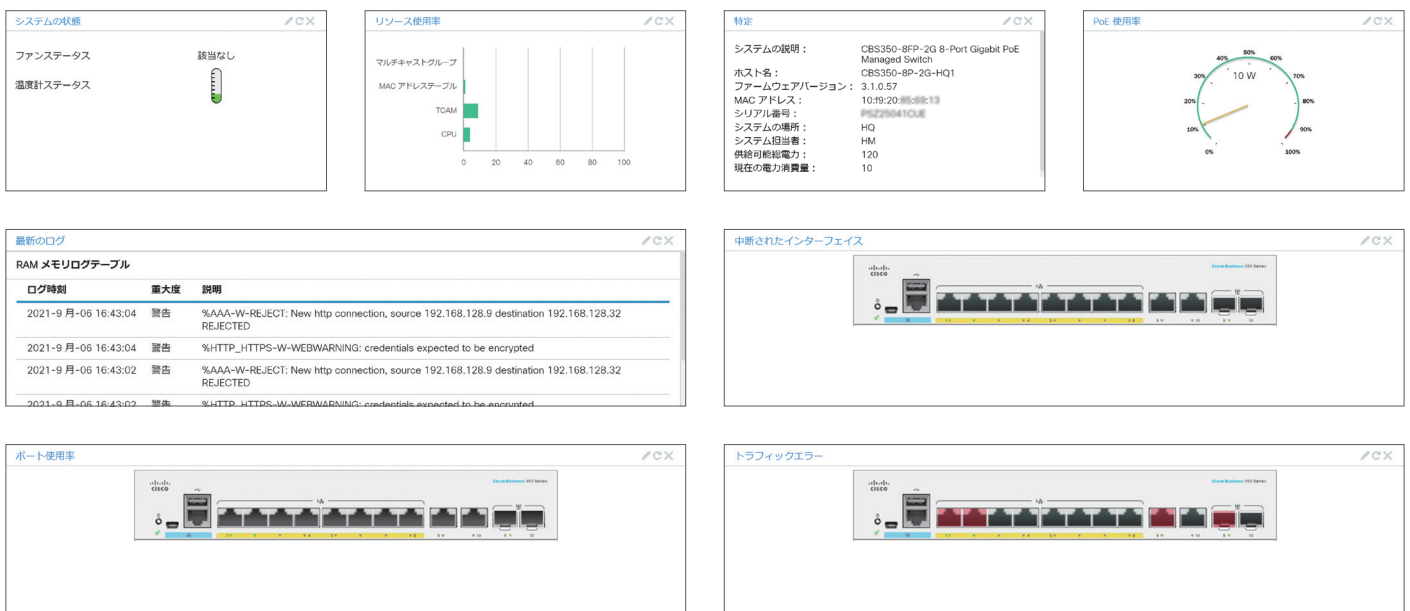
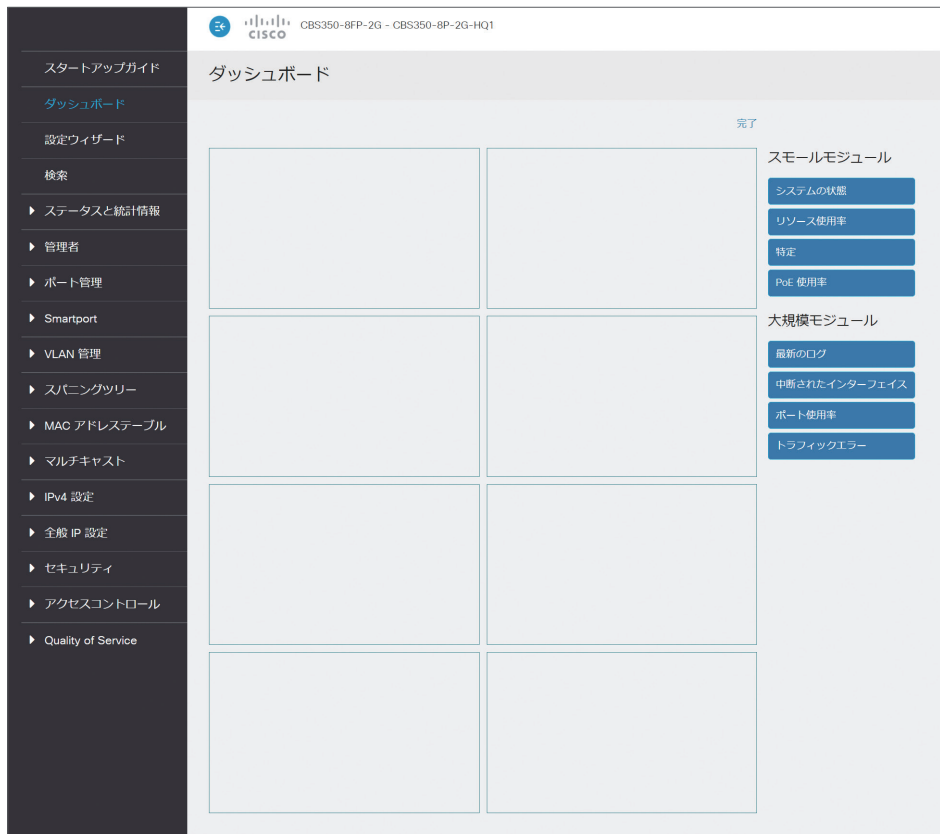
18 [RIP 統計情報テーブル] を確認

VLAN 10 と VLAN 20 の転送ルートの送信が開始されたことがわかります。

6

ダッシュボードをカスタマイズする

Web インターフェイスでは、マネージドスイッチの運用（モニタリング）に役立つ「ダッシュボード」を利用できます。2 × 4 のグリッドに、大小それぞれ 4 種類のモジュールを配置できます。本ガイドでは例として、ダッシュボードにモジュールを追加して並べ替えます。

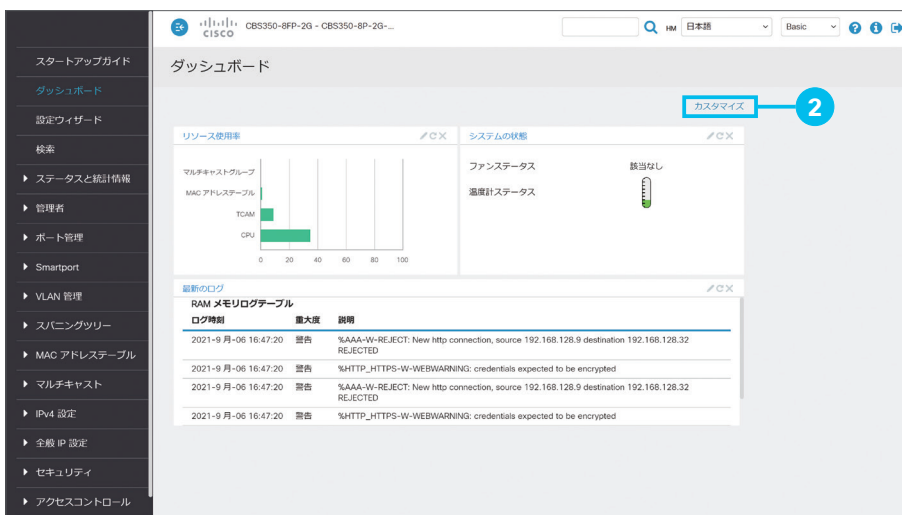




1 [ダッシュボード] をクリック

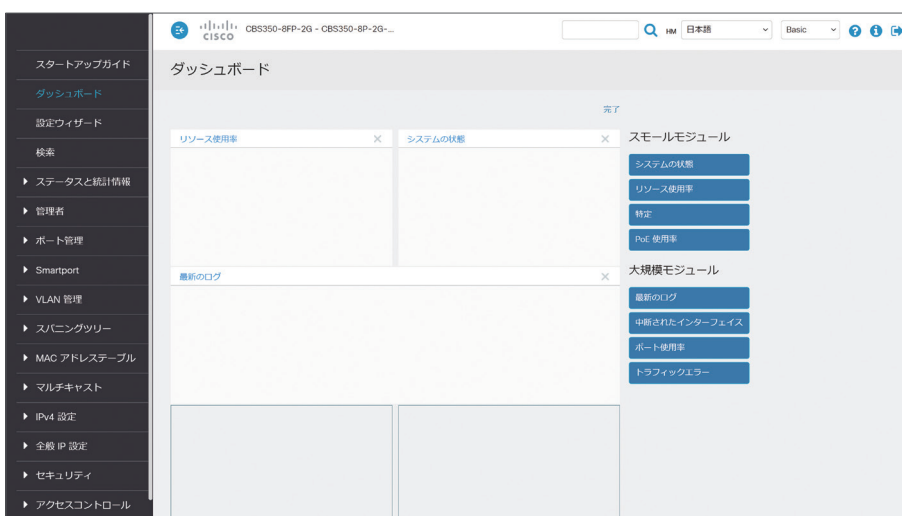
TIP MEMO

デフォルトではログイン時に「スタートアップガイド」が表示されますが、「その他のリソース」の「起動時にこのページを表示しない」チェックボックスをクリックして選択すると、次回ログイン時からはダッシュボードが表示されます。



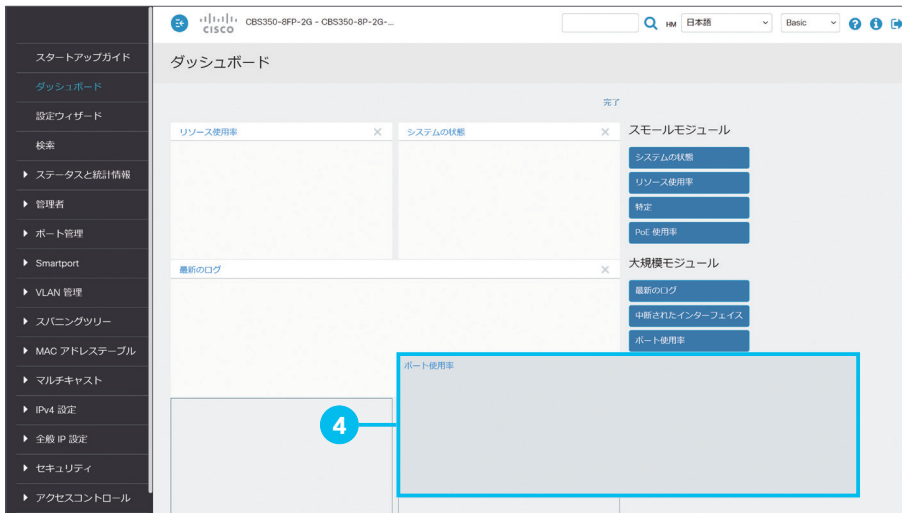
2 [カスタマイズ] をクリック

デフォルトでは「リソース使用率」「システムの状態」「最新のログ」の3種類のモジュールが表示されます。

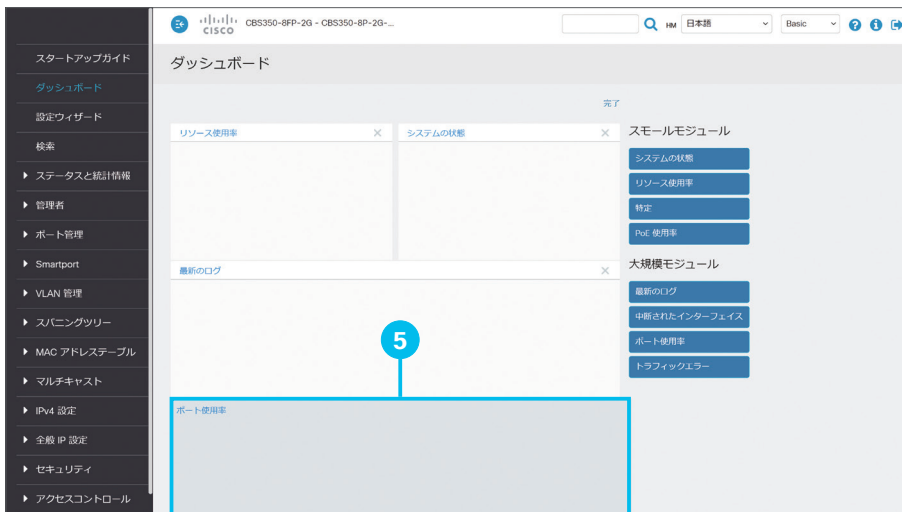


3 カスタマイズ画面を確認

「スモールモジュール」と「大規模モジュール」を2×4のグリッドにドラッグ & ドロップすると、モジュールを追加できます。また、グリッドに配置された不要なモジュールは、[X] アイコンをクリックして削除できます。本ガイドでは例として、「ポート使用率」モジュールを「最新のログ」モジュールの下のグリッドに追加します。



4 [大規模モジュール] の [ポート使用率] モジュールをクリックしてドラッグ

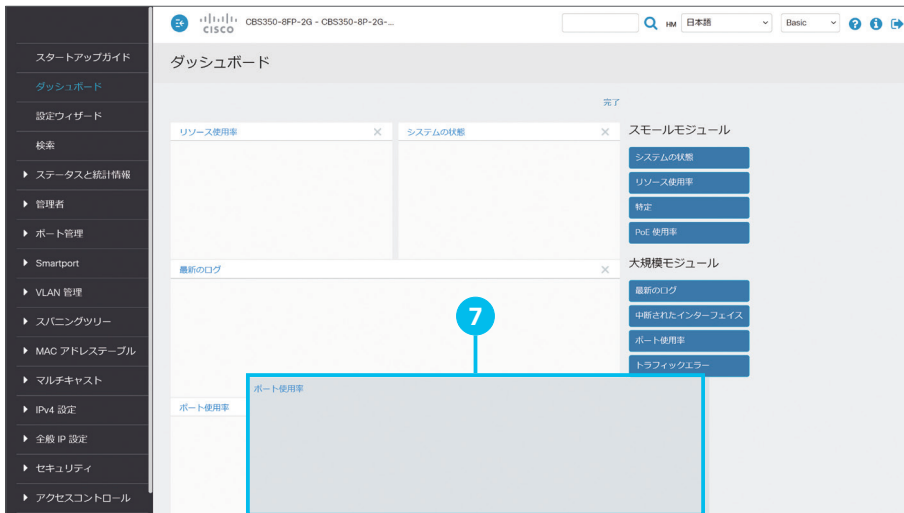


5 [最新のログ] モジュールの下のグリッドに [ポート使用率] モジュールをドロップ



6 [ポート使用率] モジュールの配置を確認

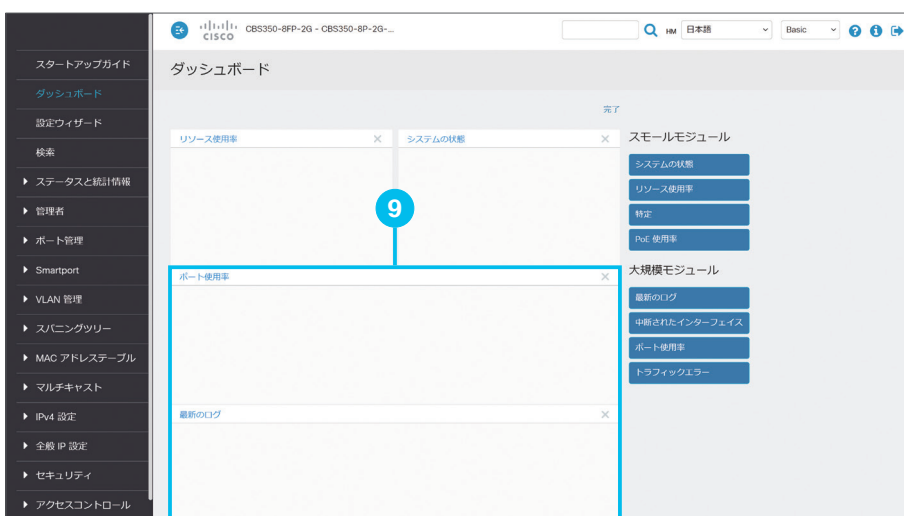
また、グリッドに配置されたモジュールどうしを、ドラッグ & ドロップで入れ替えることもできます。本ガイドでは例として、[最新のログ] モジュールと [ポート使用率] モジュールを入れ替えます。



7 「ポート使用率」モジュールをクリックしてドラッグ

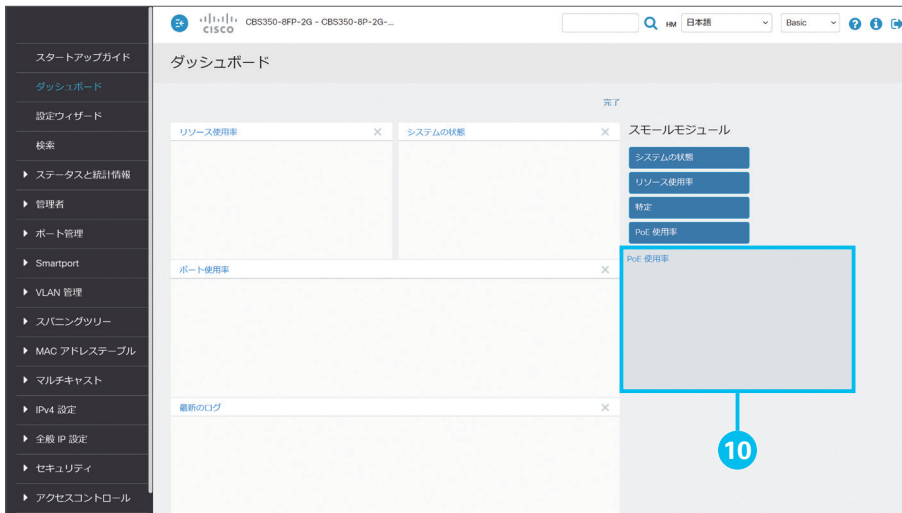


8 「最新のログ」モジュールに「ポート使用率」モジュールをドロップ



9 「最新のログ」モジュールと「ポート使用率」モジュールが入れ替わったことを確認

さらに、グリッドに配置されたモジュールを、まだグリッドに配置されていないモジュールで置き換えることもできます。本ガイドでは例として、「システムの状態」モジュールを「PoE 使用率」モジュールで置き換えます。



10 [PoE 使用率] モジュールをクリックしてドラッグ



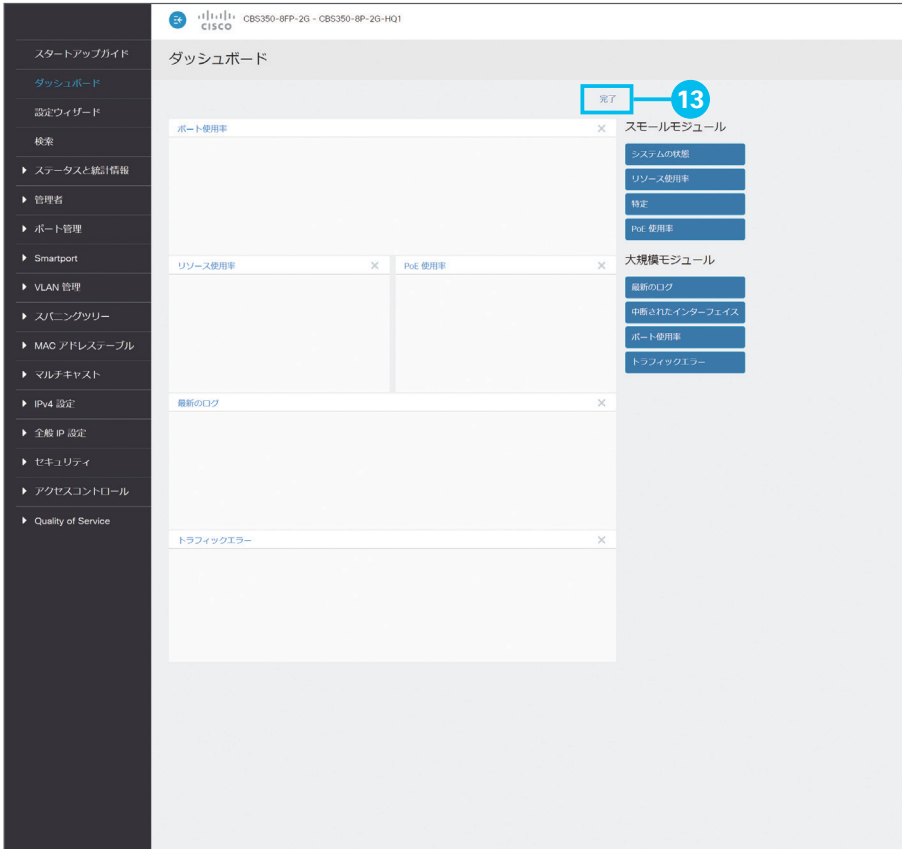
11 [システムの状態] モジュールに [PoE 使用率] モジュールをドロップ



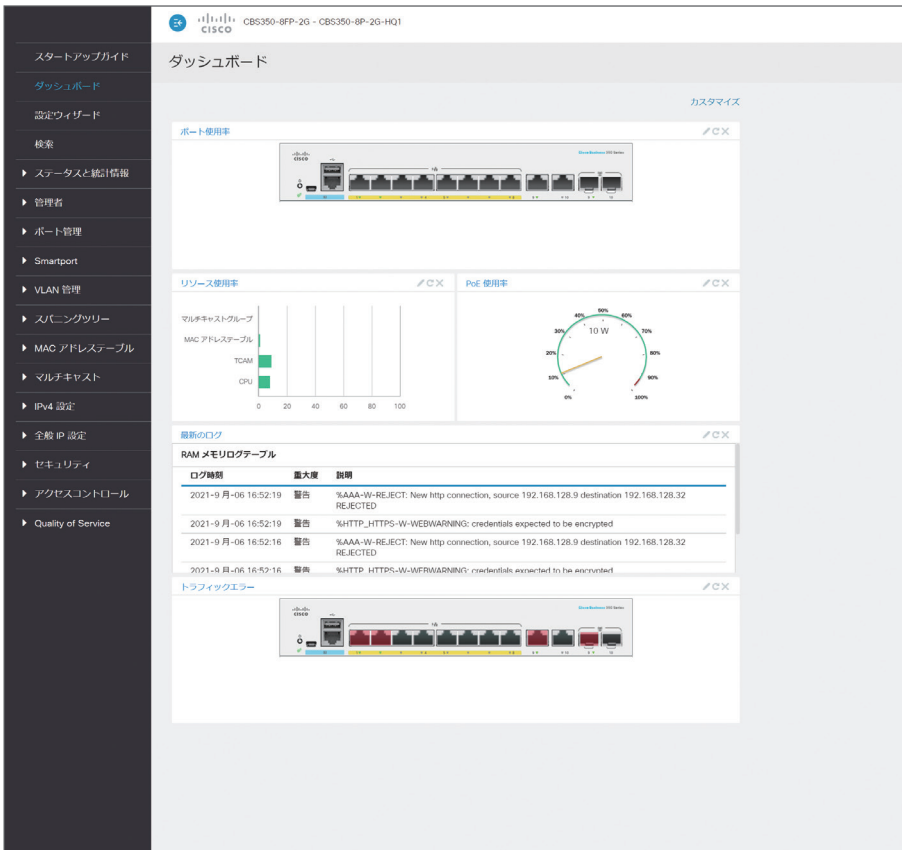
12 [システムの状態] モジュールが [PoE 使用率] モジュールに置き変わったことを確認

ここまでの手順をくり返して、ダッシュボードに配置するモジュール、表示する順序をカスタマイズします。

13 [完了] をクリック



14 配置を確認



7 ファームウェアを更新する

Web インターフェイスでは、マネージドスイッチの動作と機能を制御する**ファームウェア**を更新（アップグレード）することができます。ファームウェアを更新することで、新機能の追加、パフォーマンスの最適化、セキュリティの強化など、さまざまなメリットを享受できます。最新のファームウェアイメージ、および最新のファームウェアで Web インターフェイスを日本語化する言語ファイルは、Cisco.com からダウンロードできます。

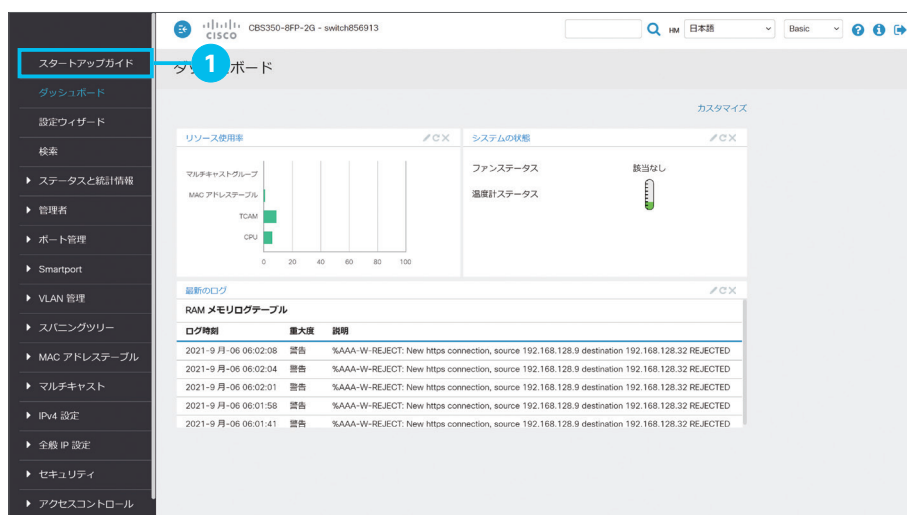
7-1 ファームウェアイメージと言語ファイルをダウンロードする

7-2 ファームウェアを更新する

7-3 言語ファイルを更新する

7-1 ファームウェアイメージと言語ファイルをダウンロードする

最新のファームウェアイメージおよび言語ファイルは、Cisco.com からダウンロードできます。本ガイドでは例として、Web インターフェイスから Cisco.com にアクセスしてダウンロードします。

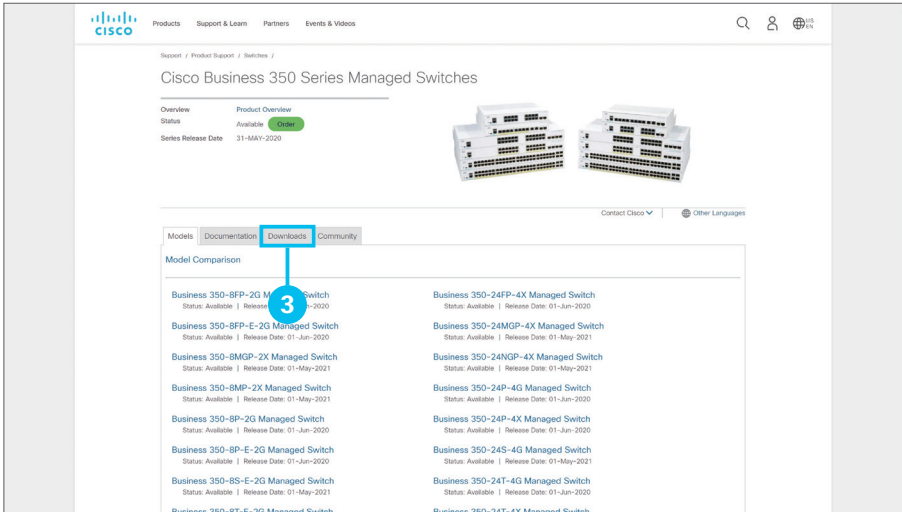


1 [スタートアップガイド] をクリック

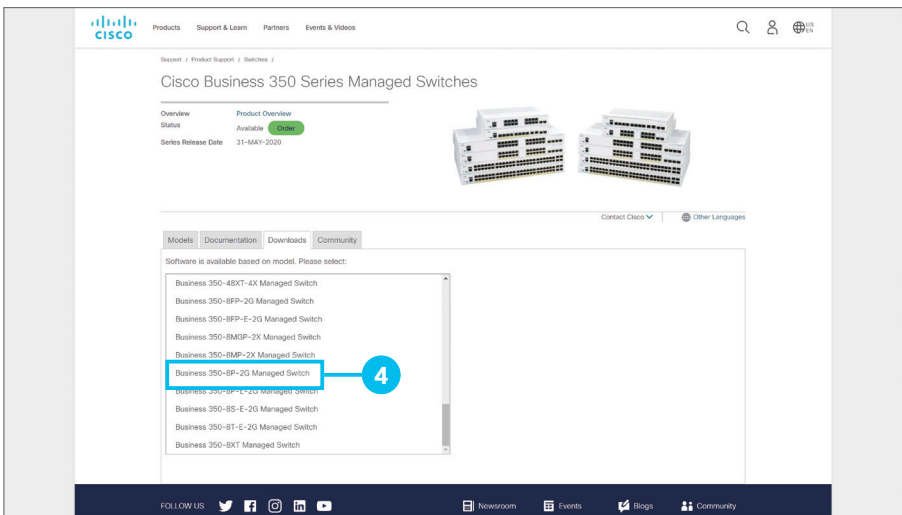


2 [その他のリソース] の [サポート] をクリック

ブラウザの新しいタブで Cisco.com のサポートページが開きます。

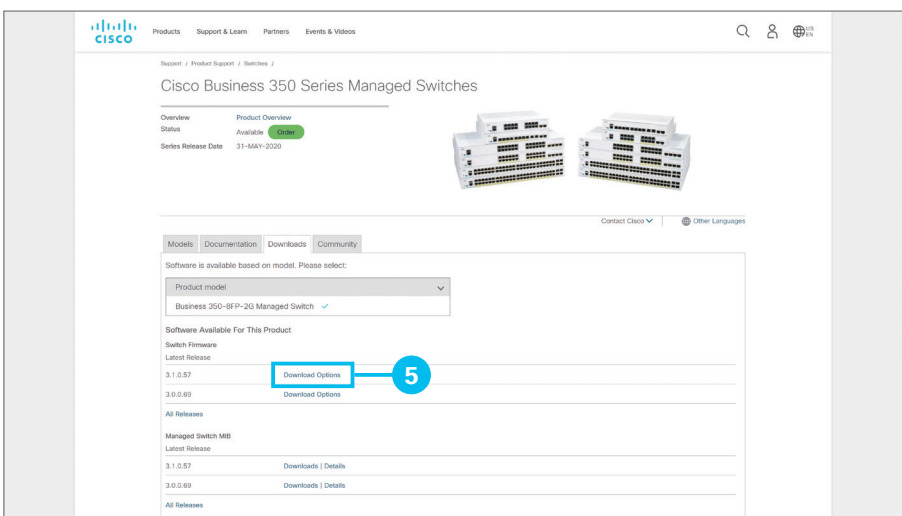


3 [Downloads] タブをクリック



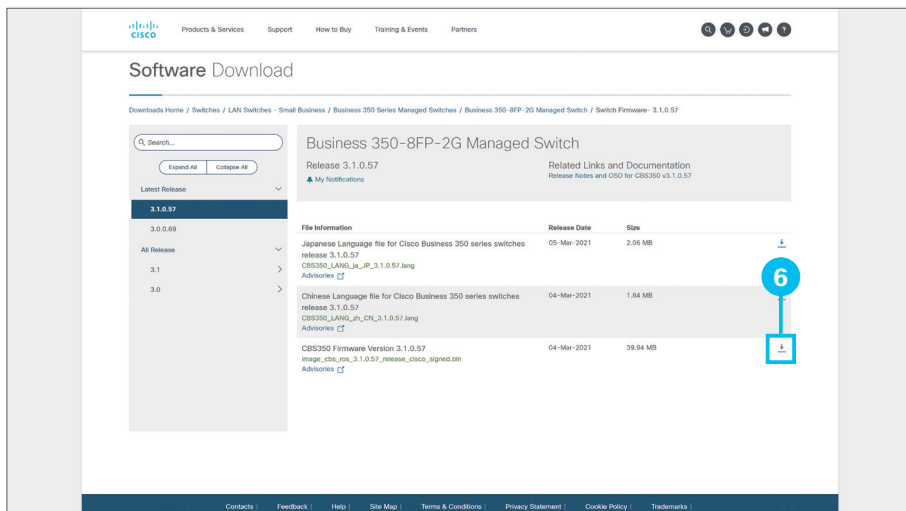
4 [Product Model] リストでモデル名をクリック

マネージドスイッチのモデル名をクリックします。本ガイドでは例として、[Business 250-8P-E-2G Smart Switch] をクリックします。

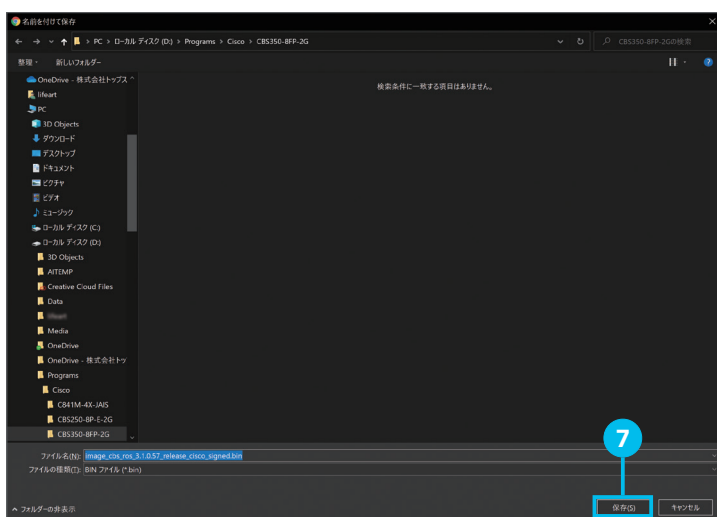


5 [Smart Switch Firmware] で、ダウンロードしたいリリースの横に表示されている [Download Options] をクリック

本ガイドでは例として、「3.1.0.57」リリースをダウンロードします。

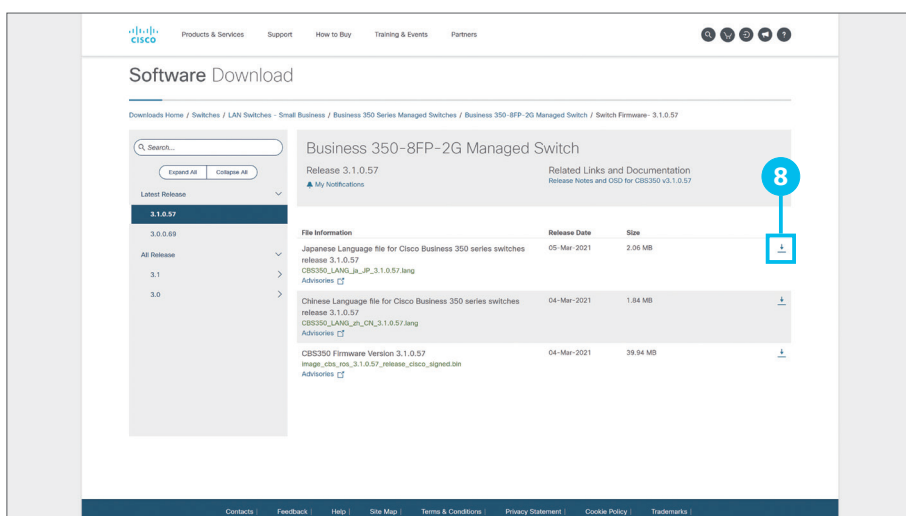


6 [Firmware image...] のダウンロード
[↓] アイコンをクリック

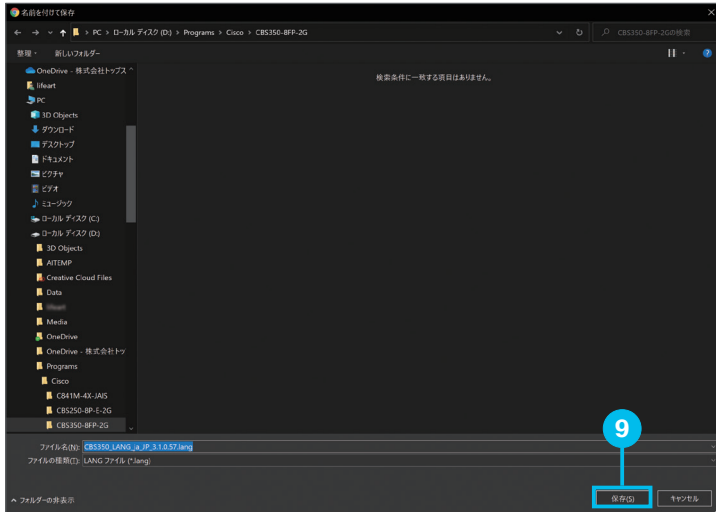


7 ファームウェアイメージを任意の場所に保存

ファームウェアイメージをダウンロードしたら、
続けて言語ファイルをダウンロードします。



8 [JapaneseLanguage file...] のダウンロード
[↓] アイコンをクリック

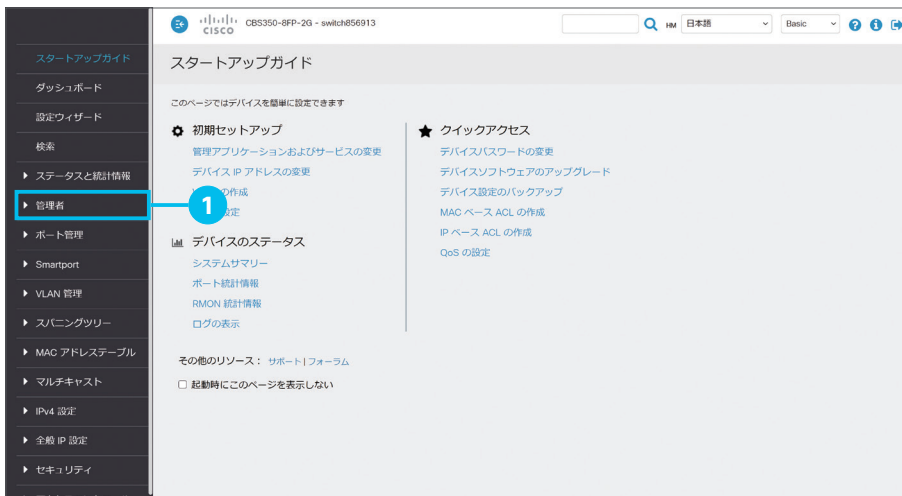


9 言語ファイルを任意の場所に保存

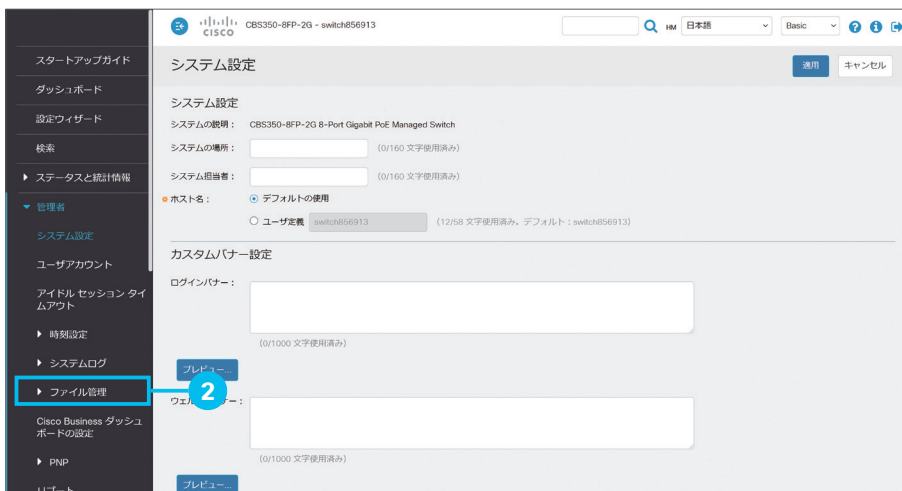
ファームウェアイメージおよび言語ファイルをダウンロードしたら、Web インターフェイスに戻ります。

7-2 ファームウェアを更新する

まず、ファームウェアを更新し、次に言語ファイルを更新します。



1 「管理者」をクリック



2 「ファイル管理」をクリック



3 [ファームウェア操作] をクリック



4 [操作タイプ] で [ファームウェアの更新] が選択されていることを確認

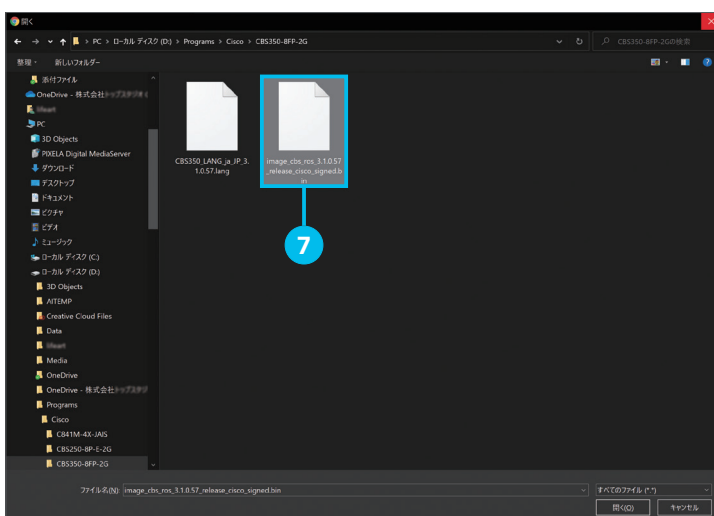
5 [コピー方式] で [HTTP/HTTPS] が選択されていることを確認

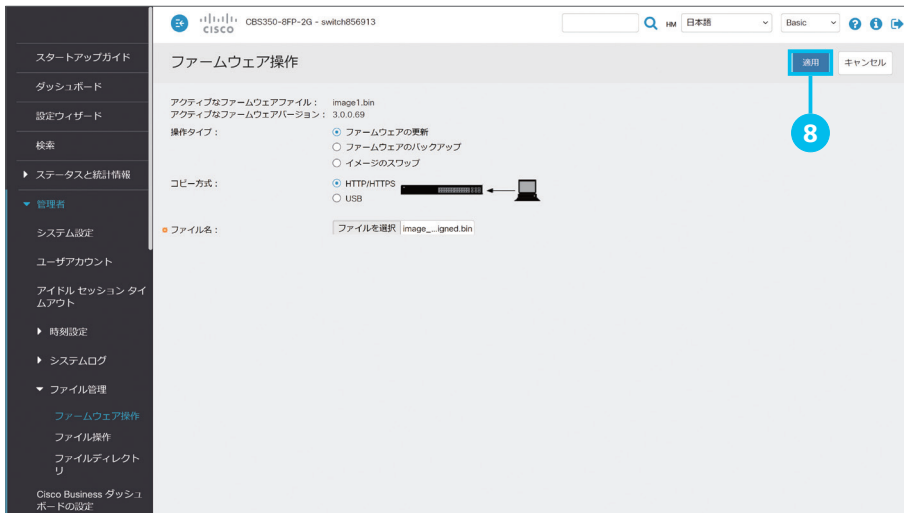
「6-1 ファームウェアイメージと言語ファイルをダウンロードする」でダウンロードしたファームウェアイメージを USB ドライブに保存し、マネージドスイッチの USB ポートに接続すれば、USB ドライブからファームウェアイメージをコピーすることもできます。本ガイドでは Web インターフェイスを使用している PC からコピーするため、[HTTP/HTTPS] を選択します。

6 [ファイルを選択] をクリック

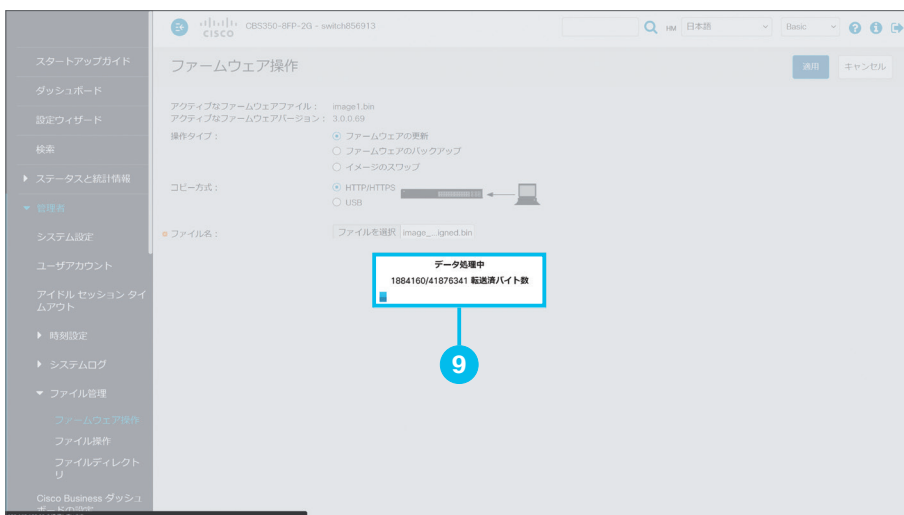
7 ファームウェアイメージを選択

「6-1 ファームウェアイメージと言語ファイルをダウンロードする」7でダウンロードしたファームウェアイメージを選択します。





8 [適用] をクリック



9 データ処理を待機



10 [成功。] メッセージを確認

ファームウェアイメージのコピーが完了しました。ファームウェアの更新を完了するため、マネージャドスイッチを再起動（リポート）します。

11 [リポート] をクリック



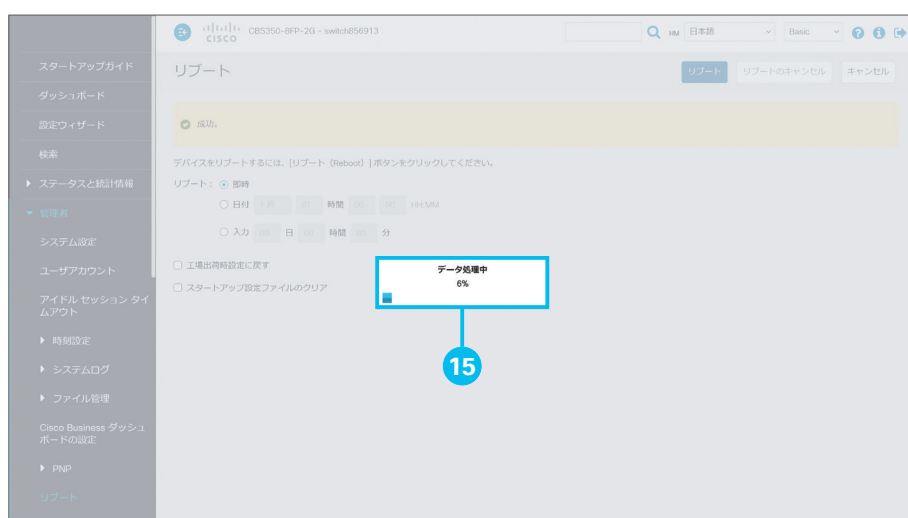
12 [リポート] で [即時] が選択されていることを確認

再起動する日時を選択することもできます。

13 [リポート] をクリック



14 [OK] をクリック



15 データ処理を待機

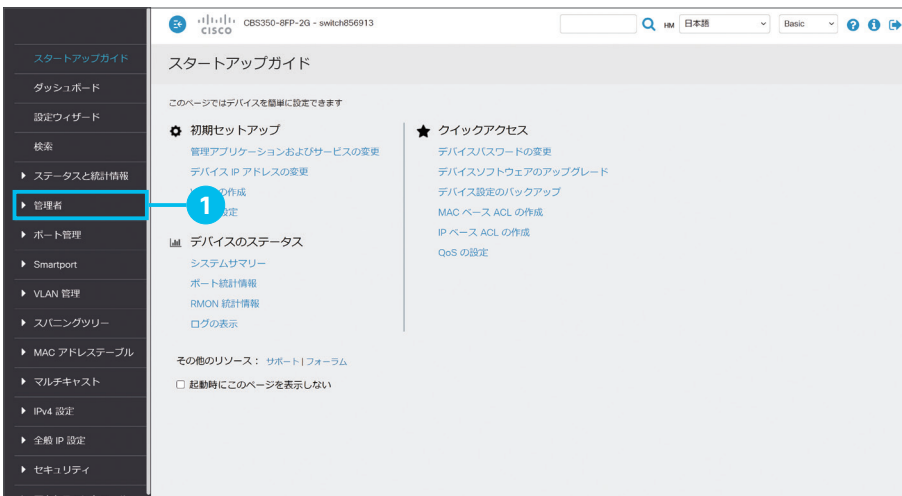


16 ログイン画面を確認

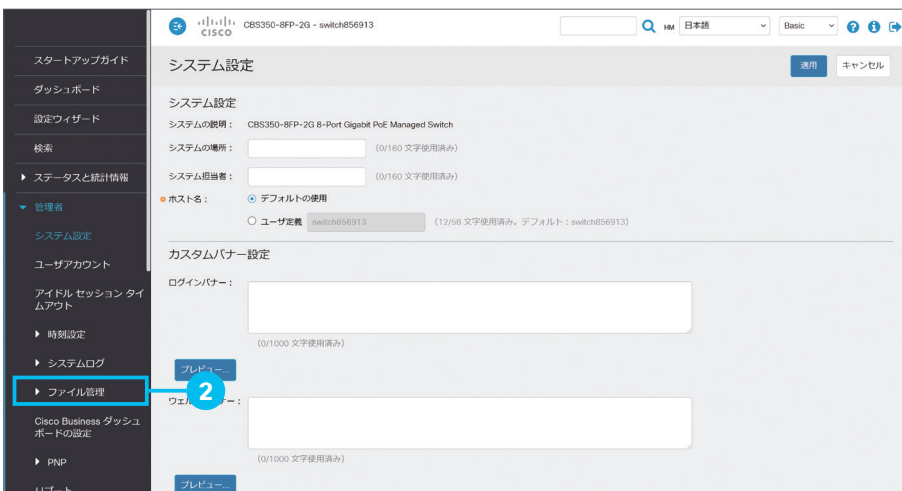
マネージドスイッチが再起動すると、Web インターフェイスのログイン画面が表示されます。続けて、言語ファイルを更新します。Web インターフェイスに再ログインします。

7-3 言語ファイルを更新する

ファームウェアの更新が完了したら、言語ファイルを更新します。



1 「管理者」をクリック



2 「ファイル管理」をクリック



3 [ファイル操作] をクリック

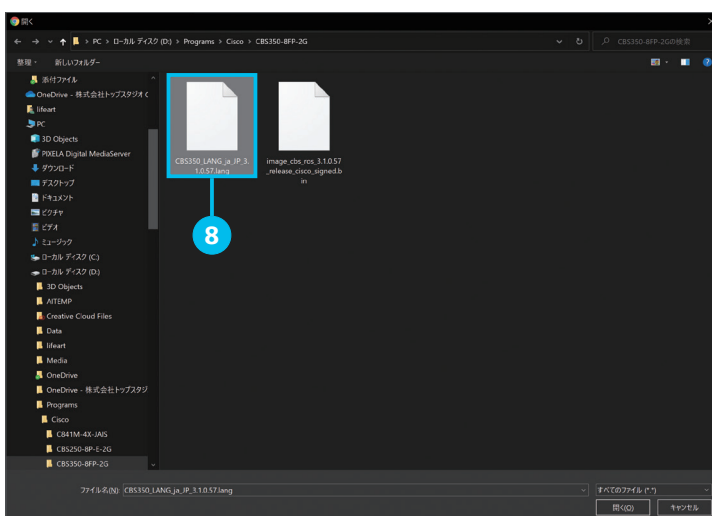


4 [操作タイプ] で [ファイルの更新] が選択されていることを確認

5 [宛先ファイルタイプ] で [言語ファイル] をクリックして選択

6 [コピー方式] で [HTTP/HTTPS] が選択されていることを確認

7 [ファイルを選択] をクリック



8 言語ファイルを選択

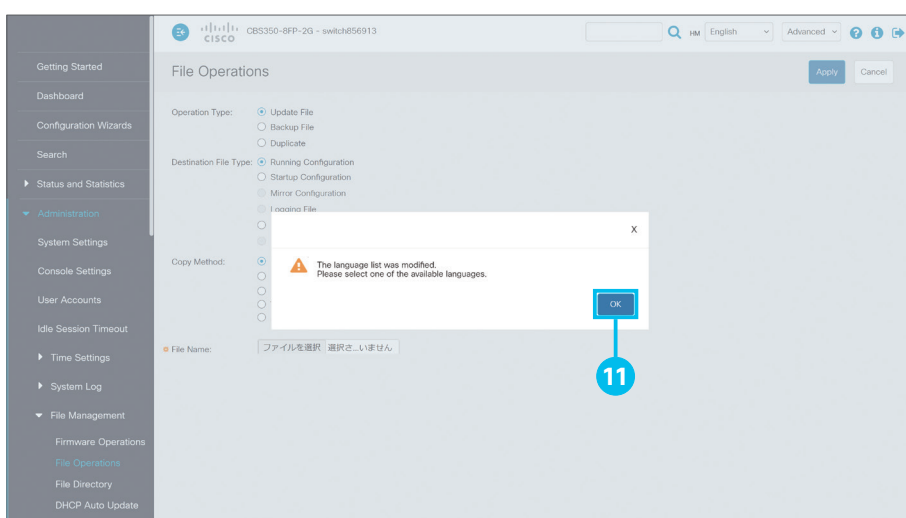
「6-1 ファームウェアイメージと言語ファイルをダウンロードする」⑨でダウンロードした言語ファイルを選択します。



9 [適用] をクリック

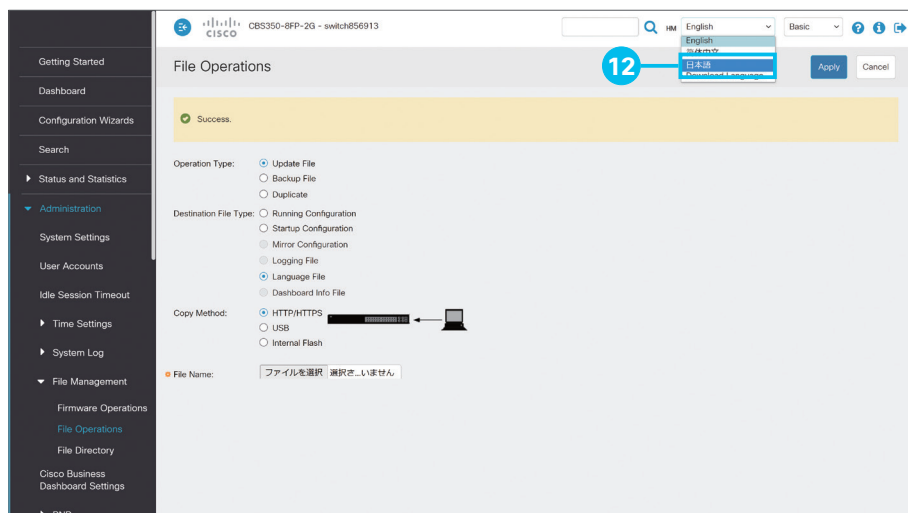


10 データ処理を待機



11 [OK] をクリック

言語ファイルのコピーが完了すると、Web インターフェイスが英語で表示されます。



12 言語のドロップダウンリストで [日本語] を選択



13 日本語表示を確認

お役立ちリンク集

Cisco Business 350 シリーズ マネージドスイッチ Web サイト

 www.cisco.com/c/ja_jp/products/switches/business-350-series-managed-switches/index.html

スモールビジネス向けネットワーク関連資料

 www.cisco.com/c/ja_jp/solutions/small-business/resource-center/networking.html

シスコ サポートコミュニティ

 www.cisco.com/c/ja_jp/solutions/small-business/resource-center/networking.html

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



©2021 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 2021 年 9 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