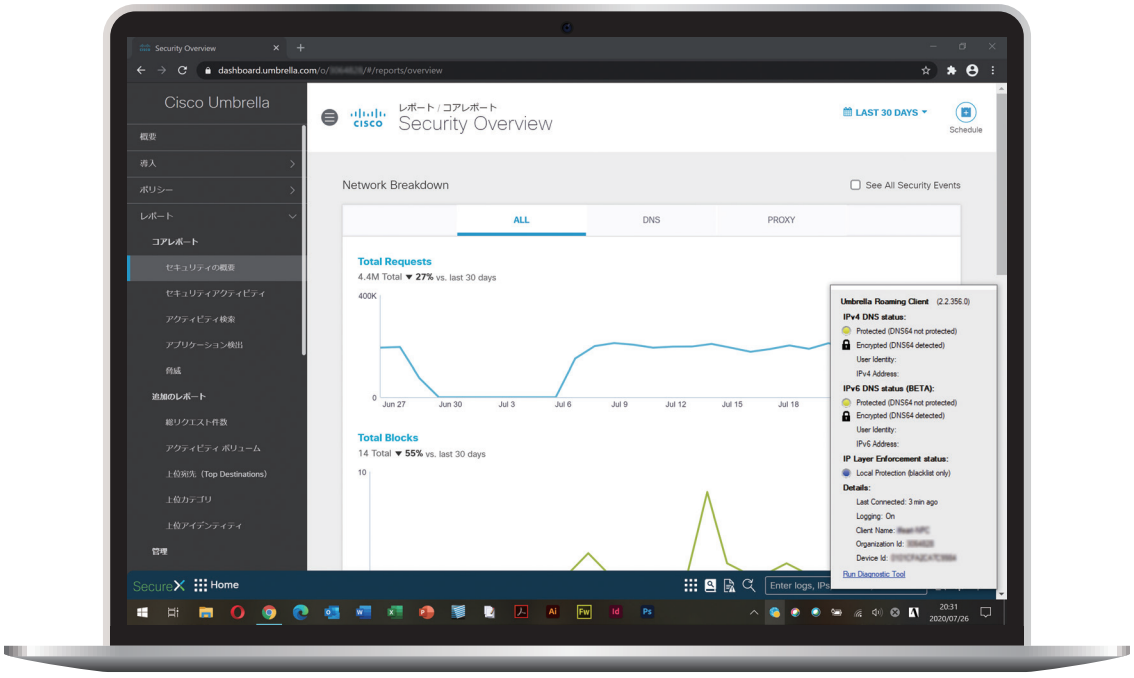
Cisco Umbrella ローミングクライアント

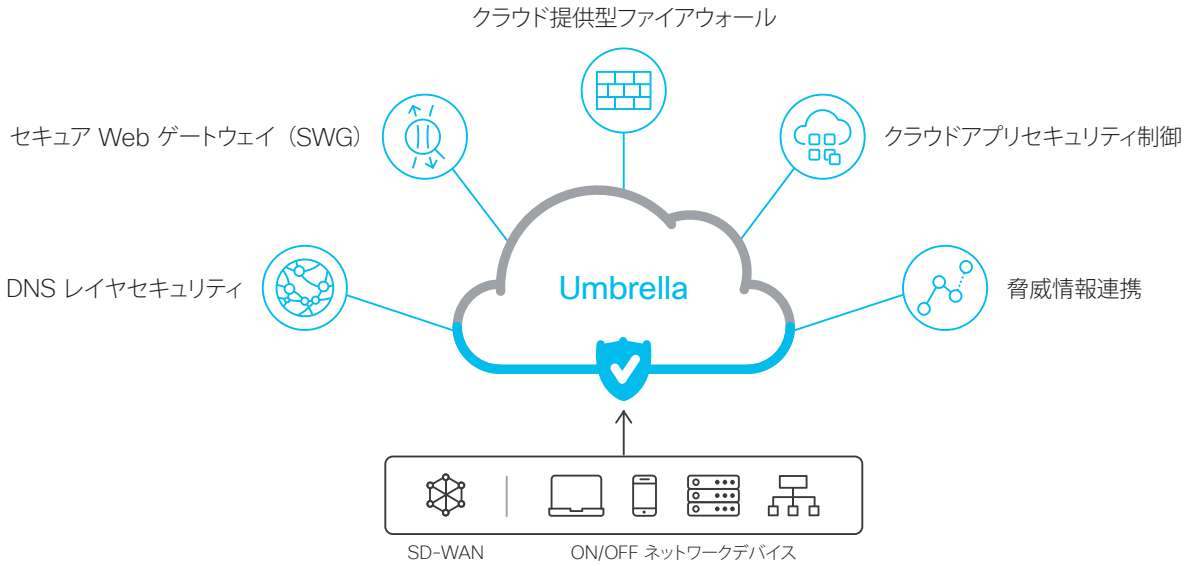
――かんたんセットアップガイド――



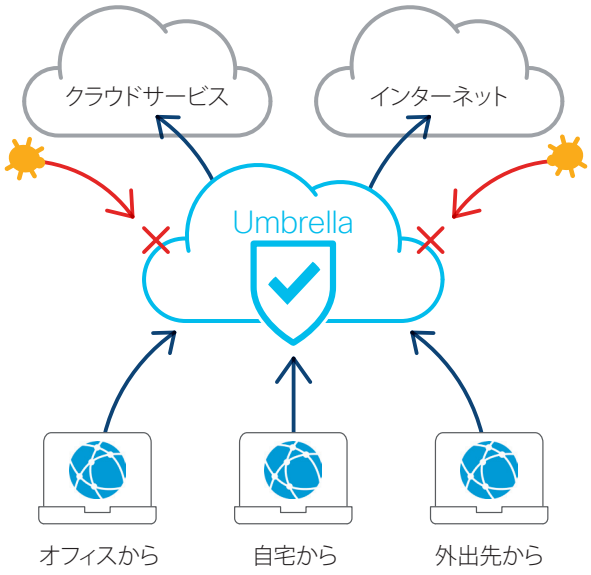
本ガイドの手順で Cisco Umbrella ローミングクライアントをかんたんにセットアップできます

はじめに

Cisco Umbrella は、インターネット上の脅威を防御するための最前線として機能する「**セキュア インターネットゲートウェイ**」［Secure Internet Gateway（SIG）］です。DNS レイヤのセキュリティをベースに、セキュア Web ゲートウェイ（SWG）、クラウド提供型ファイアウォール、クラウドアプリセキュリティ制御、サンドボックスなどの脅威情報連携も含めた、幅広いセキュリティサービスを提供します。本社、拠点などの場所、移動中、VPN の ON/OFF を問わず、あらゆるユーザ、そしてデバイスを保護できる、最も簡単かつ迅速に導入可能なクラウドセキュリティです。



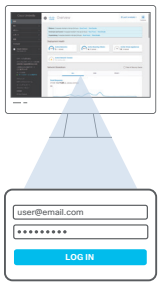
Cisco Umbrella ローミングクライアントは、Windows または Mac コンピュータで動作する軽量な DNS クライアントソフトウェアです。Cisco Umbrella ローミングクライアントをインストールすれば、オフィスや自宅、外出先など、場所を問わず Cisco Umbrella で保護されるため、どこからでも安全にインターネットやクラウドサービスを利用できるようになります。



本ガイドでは、Cisco Umbrella ローミングクライアントのインストール方法など、Cisco Umbrella のご契約後、お使いのコンピュータですぐに活用するためのセットアップ方法を紹介します。

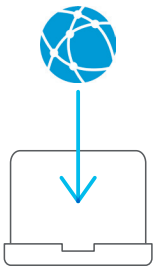
セットアップの流れ

1 ダッシュボードにログイン



2 インストーラをダウンロード

3 クライアントをインストール



4 ポリシーを設定

対応 OS（ローミングクライアント）

Cisco Umbrella ローミングクライアントは、次の OS で動作します。

- Windows 10（.NET 4.5 が必要）
- Windows 8 および 8.1（64 ビット、.NET 4.5 が必要）
- Windows 7 SP1 (32 および 64 ビット、.NET 3.5 が必要）
- macOS 10.11 以上

また、競合や問題の発生を回避するために、オンラインドキュメント『**Cisco Umbrella ユーザガイド**』の「**前提条件**」もご覧ください。

WEB docs.umbrella.com/deployment-umbrella/docs/ 前提条件

対応ブラウザ（ダッシュボード）

Cisco Umbrella ダッシュボードには、次のブラウザの最新バージョンでアクセスしてください（Microsoft Internet Explorer を除き、原則として最新の 2 バージョンをサポートします）。

- Apple Safari
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer
- Mozilla Firefox

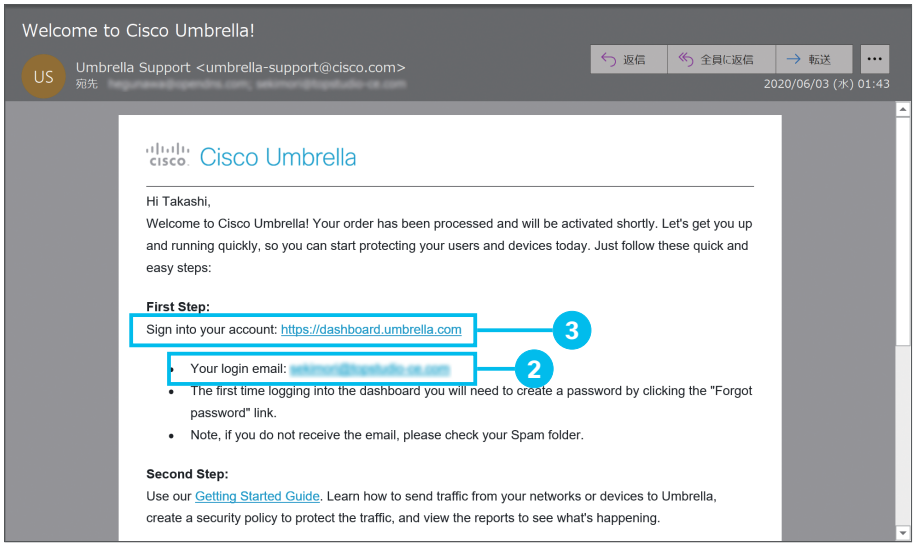
注意

本ガイドは、2020 年 8 月時点の Cisco Umbrella ダッシュボードを Windows 10 および Google Chrome の画面例で解説しています。Cisco Umbrella のアップデートやパッケージ、OS およびブラウザの種類やバージョンによって、画面や手順が異なる場合があります。

1 ダッシュボードにログインする

Cisco Umbrella は、直感的に使えるブラウザベースの管理画面「**Cisco Umbrella ダッシュボード**」で設定管理します。
ご契約後、お客様の Cisco Umbrella アカウントが開設されたことを通知する、シスコからのメールを受信します。メール本文に記載されているリンクからパスワードを設定し、Cisco Umbrella ダッシュボードにログインします。

1 送信者［**Umbrella Support**］からの件名［**Welcome to Cisco Umbrella!**］メールを開封



2 ［**Your login email**］に記載されているメールアドレスを確認

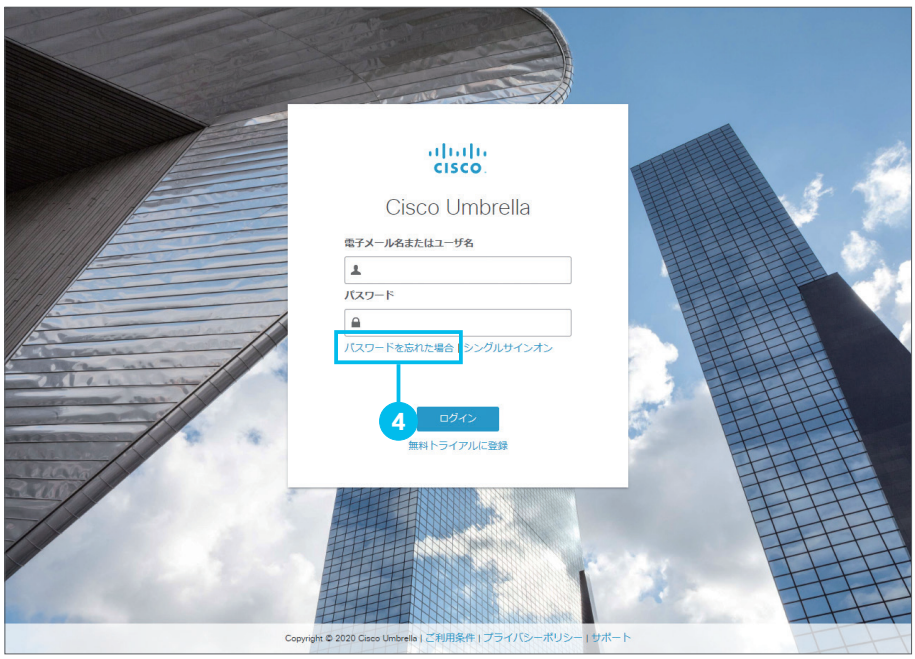
契約時に指定した管理者用メールアドレスが記載されていることを確認します。

3 ［**Sign into your account**］に記載されているリンクをクリック

または次の URL をクリックして、ダッシュボードにアクセスします。

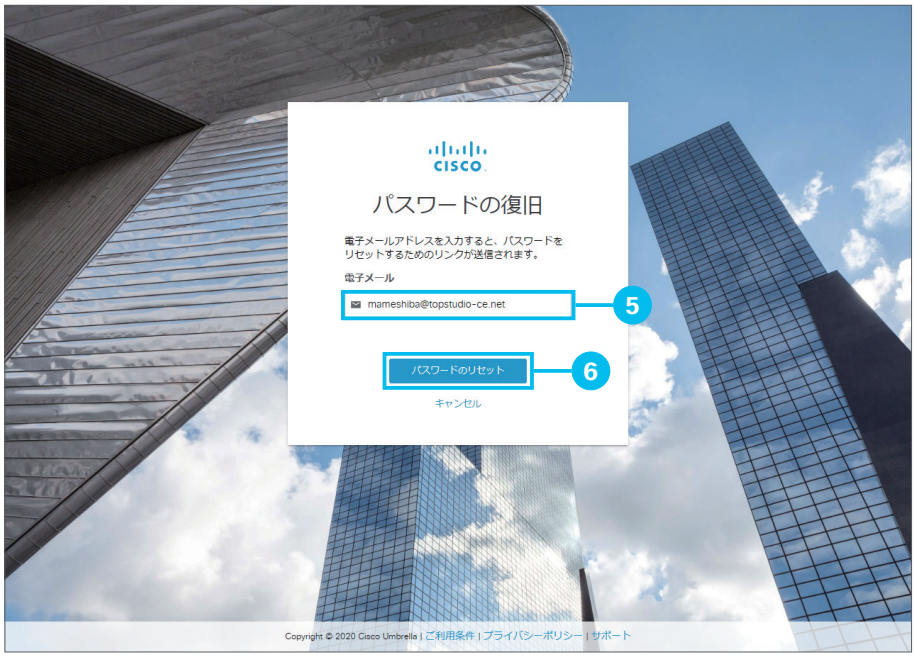
WEB dashboard.umbrella.com

ブラウザにダッシュボードのログインページが表示されます。



4 ［**パスワードを忘れた場合**］をクリック

パスワードの設定（復旧）ページが表示されます。



5 ［**電子メール**］に❷で確認した管理者用メールアドレスを入力

6 ［**パスワードのリセット**］をクリック

❷で入力したメールアドレスに電子メールが送信されました。メーラーに移動します。

7 送信者［Umbrella Support］からの件名［Cisco Umbrella パスワードのリセット］メールを開封

8 メール本文に記載されているリンクをクリック

ブラウザにパスワードの設定（復旧）ページが表示されます。

9 ［**電子メール**］に2で確認した管理者用メールアドレスを入力

10 ［**パスワード**］に任意のパスワードを入力

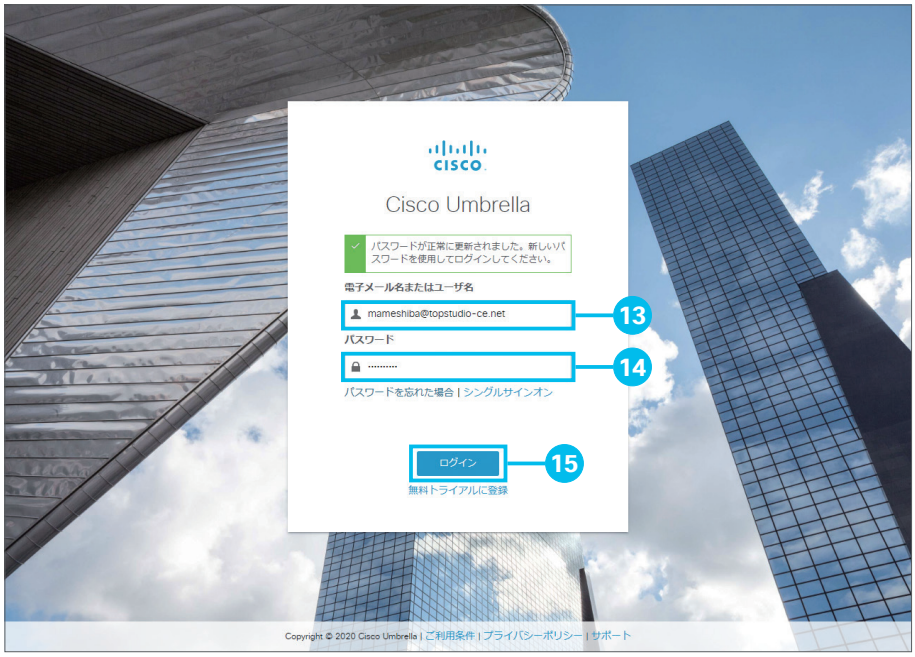
11 ［**パスワードの確認**］に10で入力したパスワードを再度入力

12 ［**パスワードのリセット**］をクリック

パスワードの設定が完了すると、ログインページが表示されます。

注意

パスワードは、英大文字、英小文字、数字、および記号（! や @ など）を、それぞれ 1 文字以上含む、8 ～ 256 文字の長さで設定する必要があります。予測しやすい単語や名前、メールアドレスは含めないでください。



13 ［**電子メール**］に2で確認した管理者用メールアドレスを入力

14 ［**パスワード**］に任意のパスワードを入力

15 ［**ログイン**］をクリック

ログインが完了すると、ダッシュボードが表示されます。
続けて、ダッシュボードから Cisco Umbrella ローミングクライアントのインストーラをダウンロードします。

MEMO

以降は次の URL から、管理者用メールアドレスと設定したパスワードでダッシュボードにログインできます。

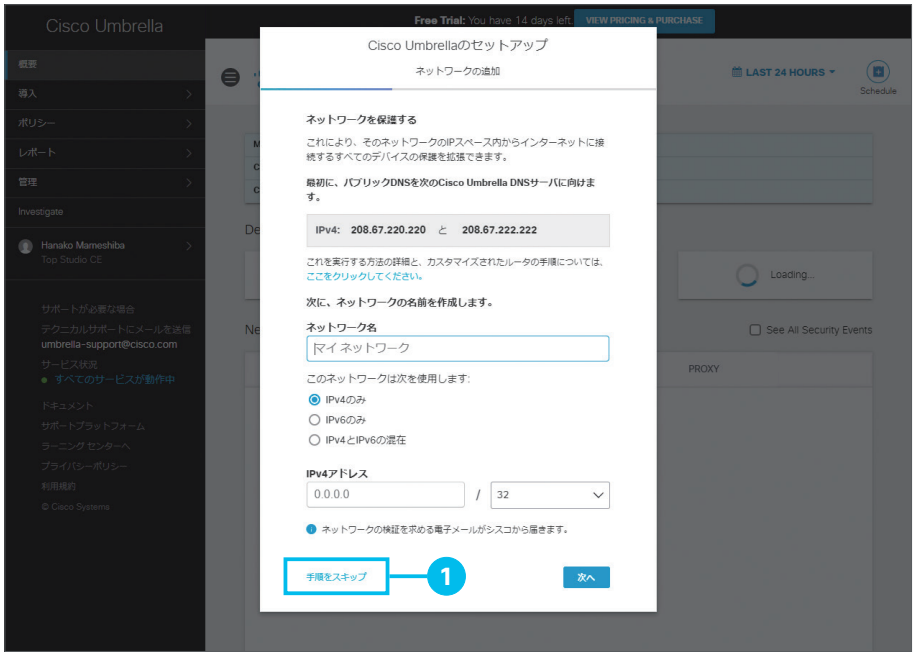
WEB dashboard.umbrella.com

2 インストーラをダウンロードする

Cisco Umbrella ダッシュボードから、Cisco Umbrella ローミングクライアントの**インストーラ**をダウンロードします。
インストーラは、初回ログイン時のみ表示される「**Cisco Umbrella のセットアップ**」ウィザードから、または常時表示される「**導入**」メニューからダウンロードできます。

2-1 セットアップウィザードからインストーラをダウンロードする

Cisco Umbrella ダッシュボードへの初回ログイン時のみ、「**Cisco Umbrella のセットアップ**」ウィザードが表示されます。ウィザードでは、Cisco Umbrella ローミングクライアントのインストールによる**ローミングコンピュータの追加**（インストーラのダウンロード）だけでなく、DHCP サーバやルータ、ファイアウォール向けの**ネットワークの追加**もサポートしますが、**本ガイドでは省略します**。「**1　ダッシュボードにログインする**」の手順で、初回ログインが完了した状態から説明します。



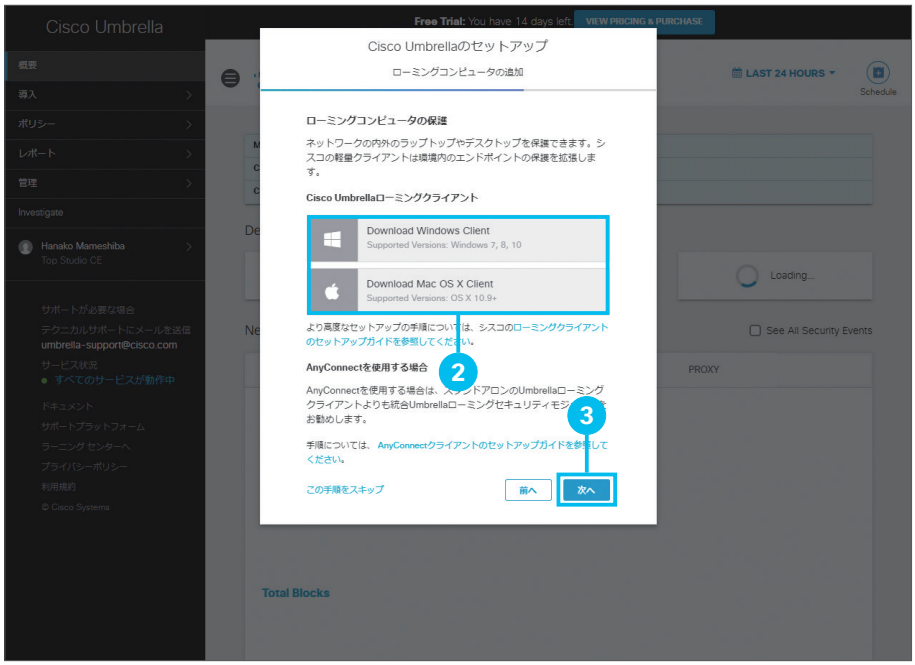
1 ［**手順をスキップ**］をクリック

ウィザードではまず、「**ネットワークの追加**」画面が表示されますが、本ガイドでは省略します。

MEMO

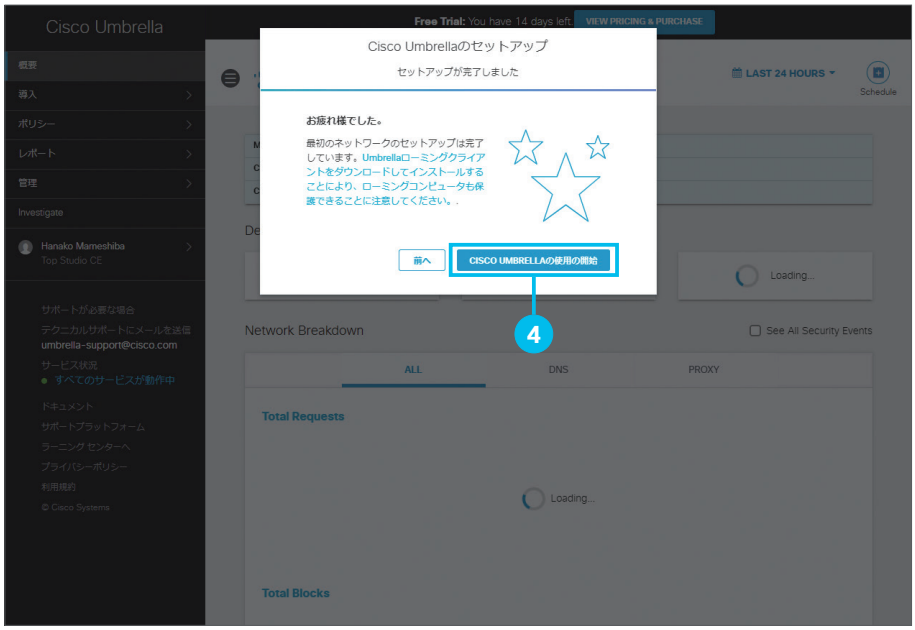
「**ネットワークの追加**」画面では、DHCP サーバやルータ、ファイアウォールの設定管理ツールで DNS 設定を変更するなど、各種設定が必要になります。くわしくは、オンラインドキュメント『**Cisco Umbrella ユーザガイド**』の「**DNS の接続先を Cisco Umbrella に設定する**」および「**アイデンティティの追加とネットワークの保護**」をご覧ください。

WEB docs.umbrella.com/deployment-umbrella/docs/cisco-umbrella- へようこそ -1



2 Windows 用インストーラは［**Download Windows Client**］、macOS 用インストーラは［**Download macOS Client**］をクリックして、インストーラを任意の場所に保存

3 ［**次へ**］をクリック



4 ［**CISCO UMBRELLA の使用の開始**］をクリック

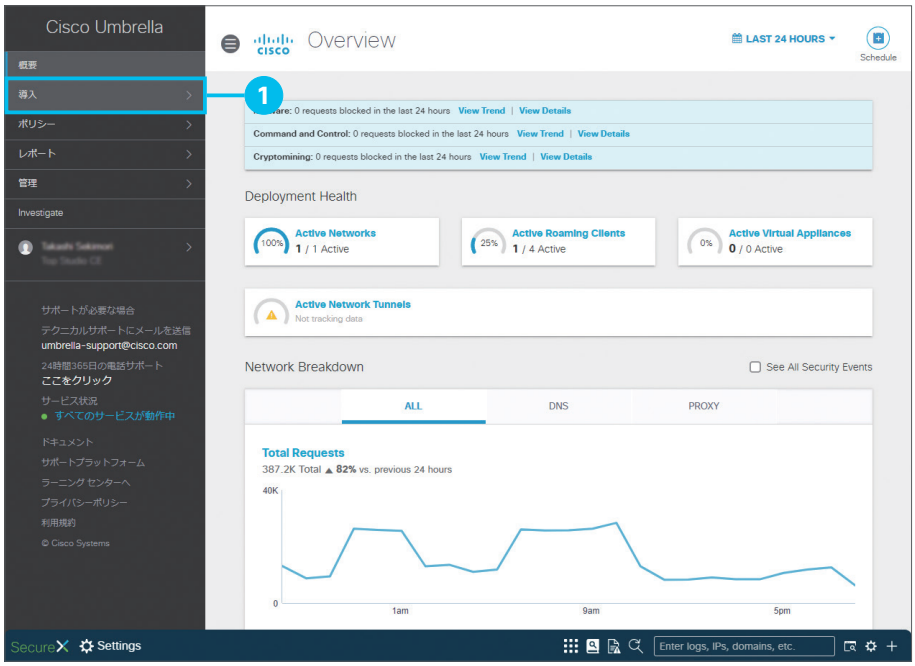
インストーラのダウンロードが完了しました。続けて、Cisco Umbrella で保護したいコンピュータに Cisco Umbrella ローミングクライアントをインストールします。「**3　ローミングクライアントをインストールする**」をご覧ください。または、「**2-2　導入メニューからインストーラをダウンロードする**」で、ダッシュボードに常時表示される「**導入**」メニューからのダウンロード方法も確認してください。

注意

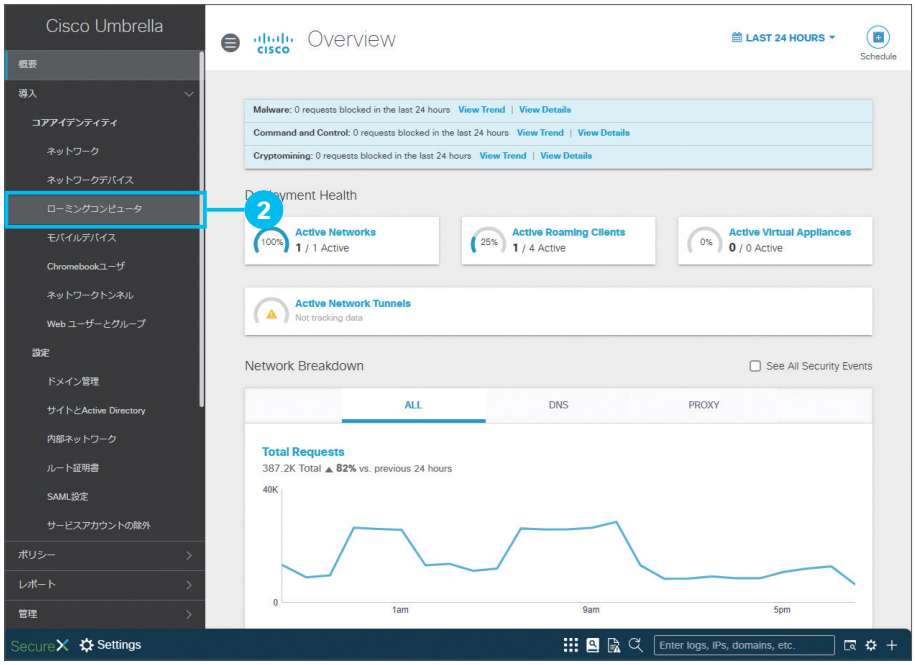
ダウンロードしたインストーラは、お客様の組織専用です（組織に固有の情報を含んでいます）。外部には配布しないでください。

2-2 導入メニューからインストーラをダウンロードする

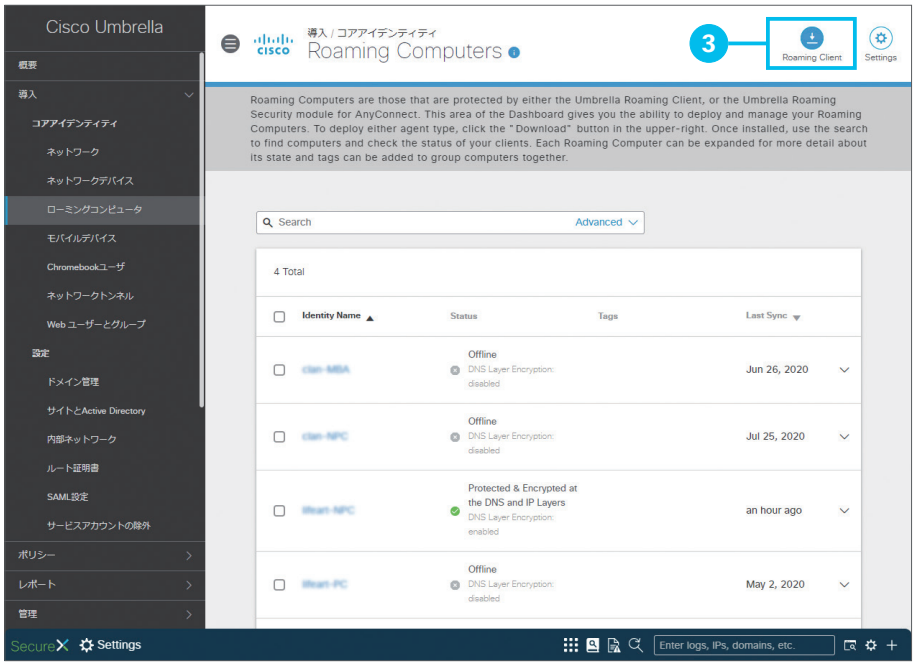
続けて、Cisco Umbrella ダッシュボードに常時表示される「導入」メニューからのダウンロード方法を説明します。



1 ［導入］をクリック

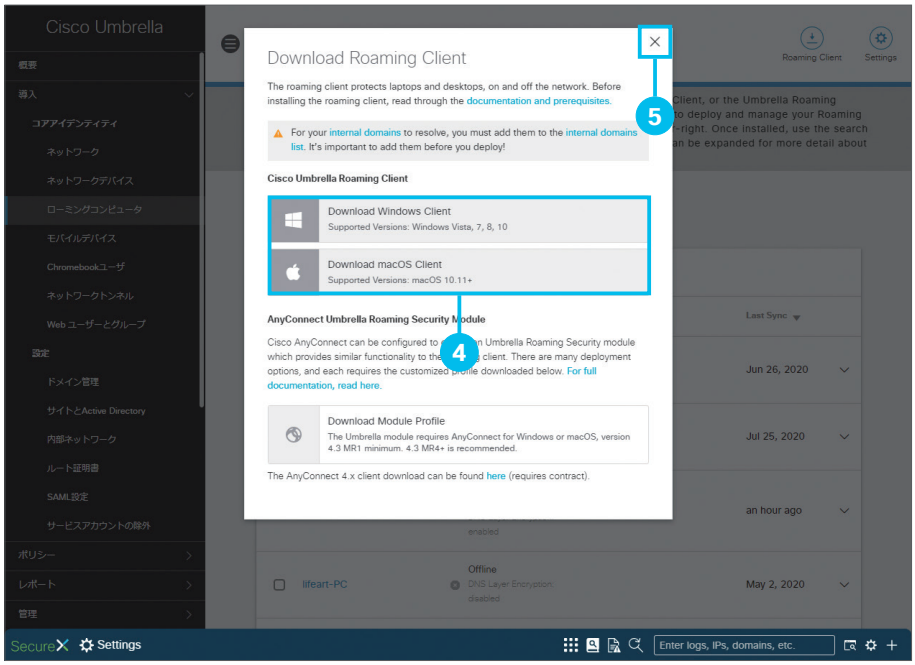


2 ［ローミングコンピュータ］をクリック



3 ［Roaming Client］をクリック

［Download Roaming Client］ポップアップウィンドウが開きます。



4 Windows 用インストーラは［**Download Windows Client**］、macOS 用インストーラは［**Download macOS Client**］をクリックして、インストーラを任意の場所に保存

5 ［×］をクリック

インストーラのダウンロードが完了しました。続けて、Cisco Umbrella で保護したいコンピュータに Cisco Umbrella ローミングクライアントをインストールします。

注意

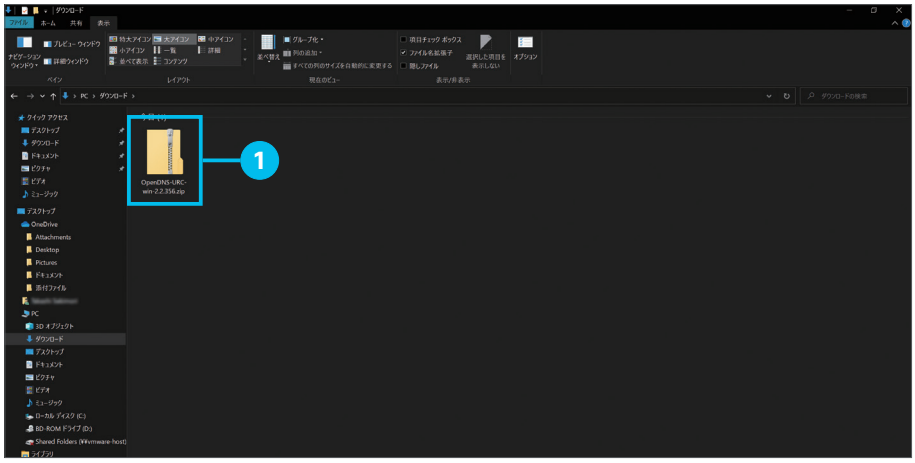
ダウンロードしたインストーラは、お客様の組織専用です（組織に固有の情報を含んでいます）。外部には配布しないでください。
また、インストーラを配布する前に、OS 標準の機能やユーティリティなどでインストーラの圧縮ファイルを解凍できるかどうか確認することを推奨します。

3 ローミングクライアントをインストールする

Cisco Umbrella で保護したいコンピュータに Cisco Umbrella ローミングクライアントをインストールし、テスト URL にアクセスして実際の動作を確認します。

3-1 ローミングクライアントをインストールする

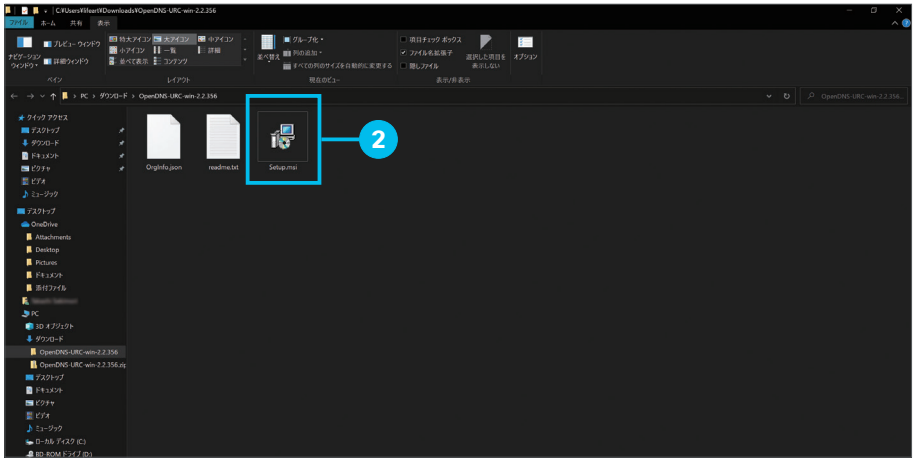
Cisco Umbrella で保護したいコンピュータでインストーラを解凍および実行し、Cisco Umbrella ローミングクライアントをインストールします。本ガイドでは、Windows 10 の画面例で手順を説明します。



1 インストーラ（圧縮ファイル）を解凍

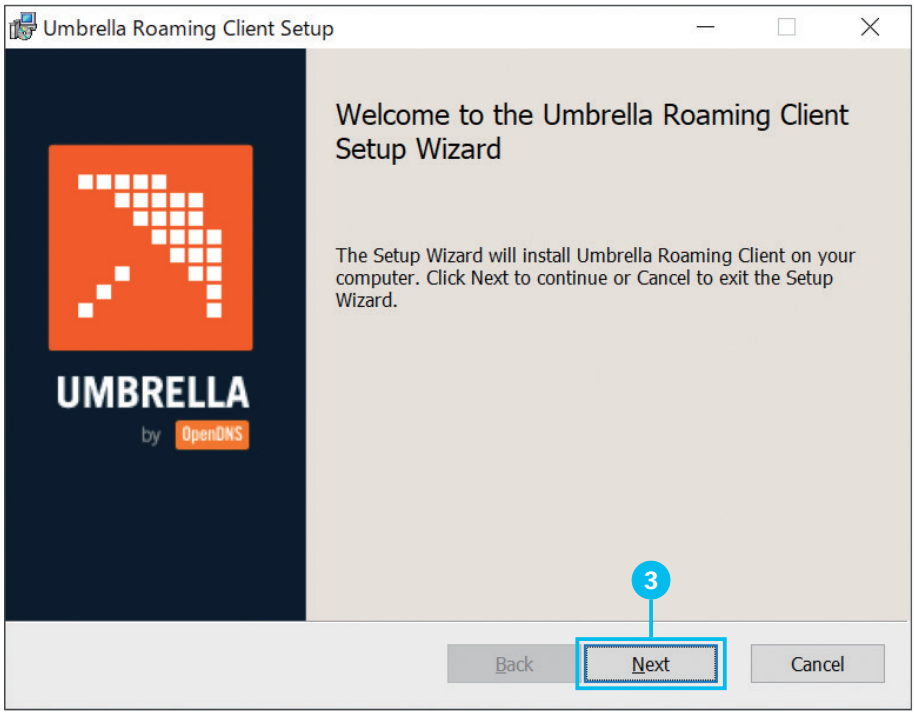
「**2-1　セットアップウィザードからインストーラをダウンロードする**」**2**または「**2-2　導入メニューからインストーラをダウンロードする**」**4**でインストーラを保存した場所（フォルダ）を開いて、インストーラの圧縮ファイルを解凍（展開）します。ファイル名は、[OpenDNS-URC-win-x.x.xxx]（拡張子なし表示）または［OpenDNS-URC-win-x.x.xxx.zip］（拡張子あり表示）です。

> **TIP MEMO**
>
> 特定のソフトウェアで圧縮ファイルを解凍できない場合は、OS 標準の機能やユーティリティなど、別のソフトウェアで解凍してください。

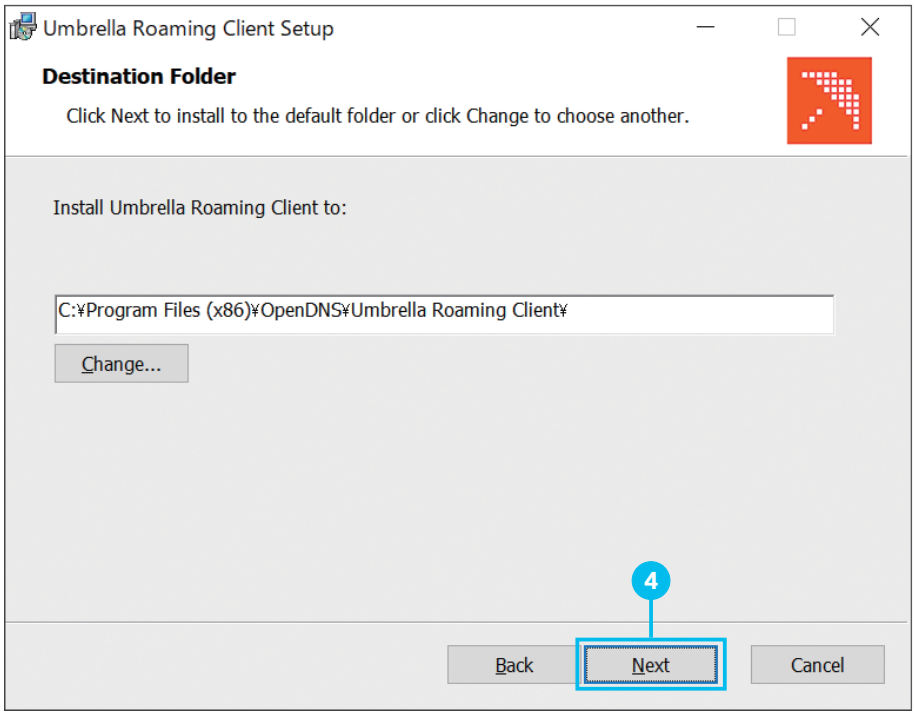


2 インストーラを実行

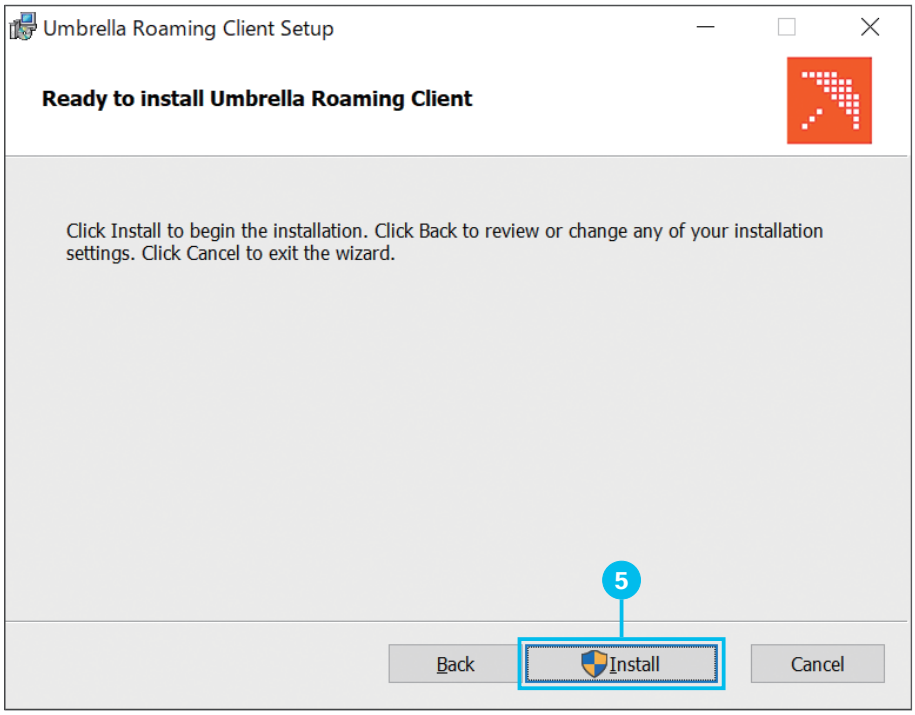
解凍したインストーラを実行します。ファイル名は、[Setup]（拡張子なし表示）または［Setup.msi］（拡張子あり表示）です。セットアップウィザードが起動します。



3 ［Next］をクリックし



4 ［Next］をクリック

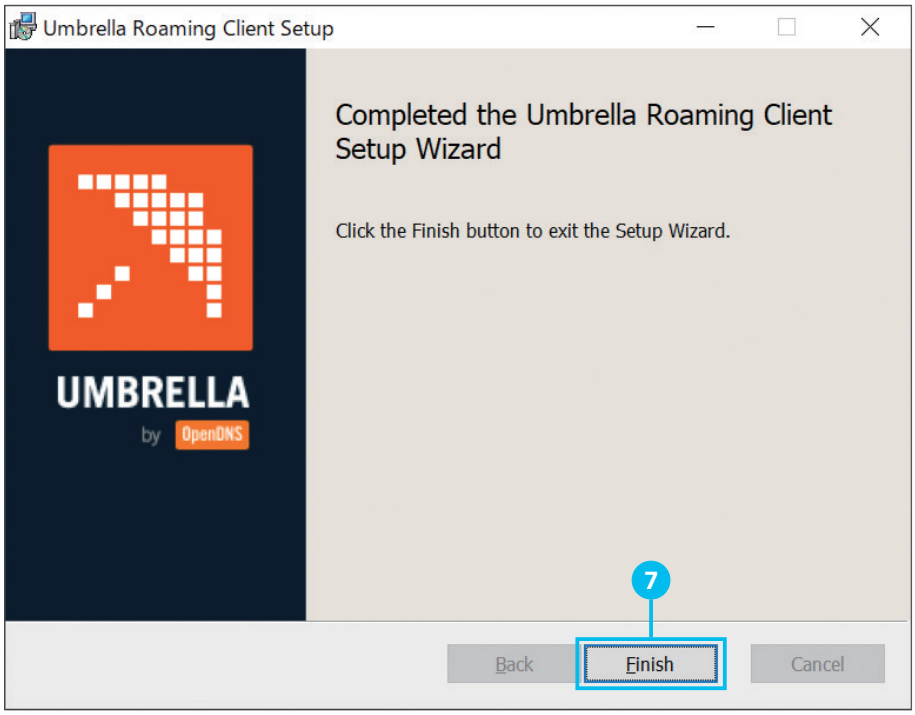


5 ［Install］をクリック

［**ユーザー アカウント制御**］ダイアログボックスが開きます。

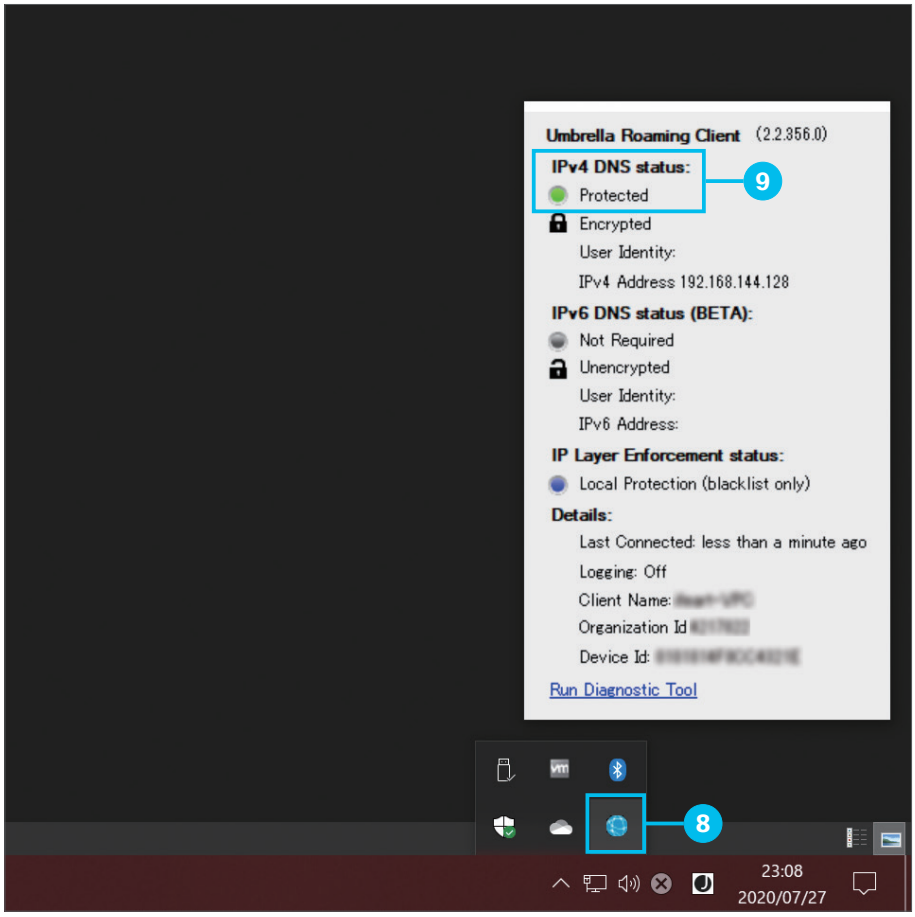
6 ［**はい**］をクリック

インストールが開始します。



7 ［Finish］をクリック

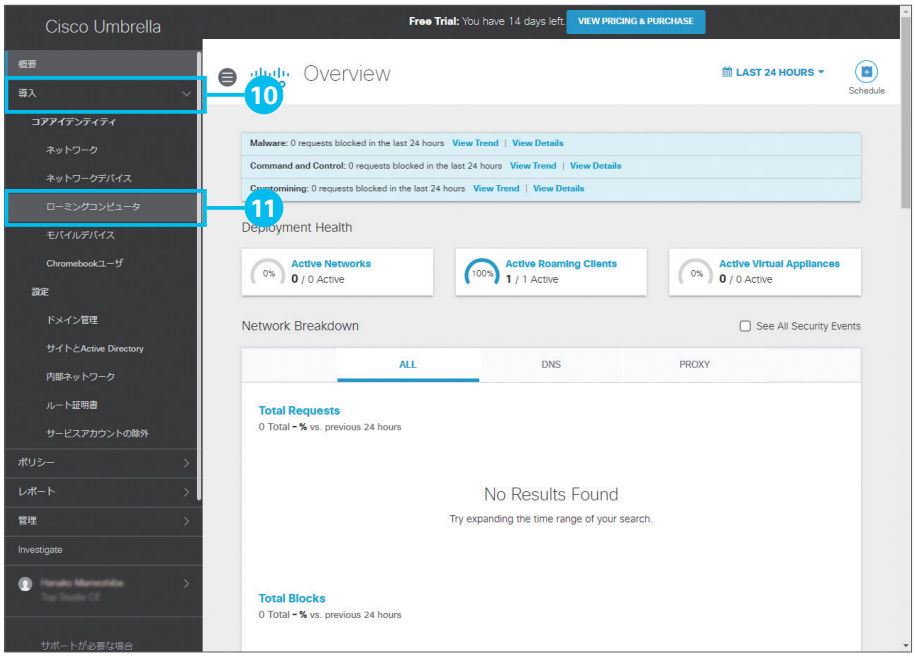
インストールが完了しました。Windows のタスクトレイに表示されているローミングクライアントのトレイアイコンで状態を確認します。



8 タスクトレイの［ ］アイコンをクリック

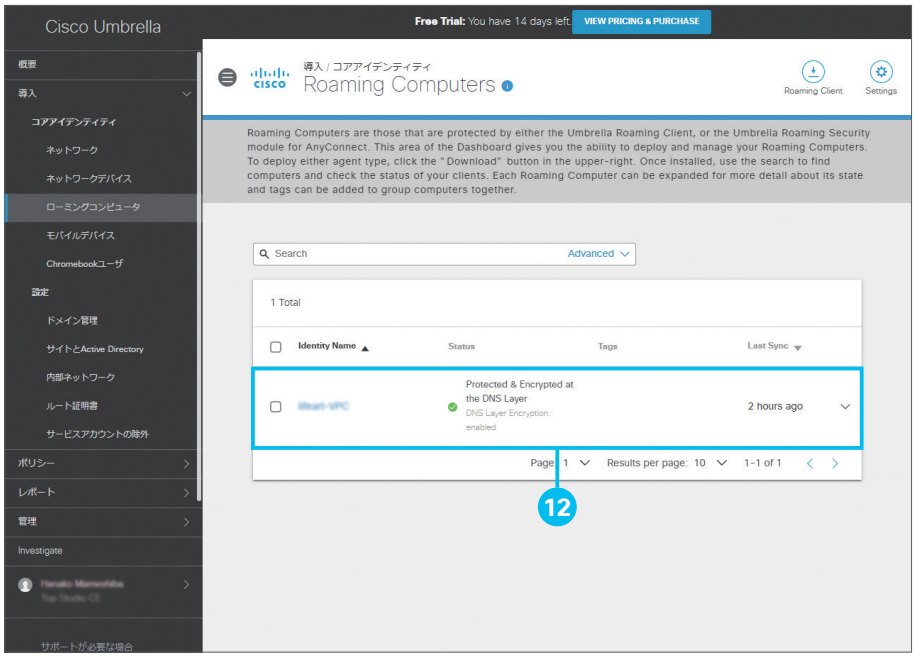
9 ［IPv4 DNS status］が［Protected］であることを確認

［IPv4 DNS status］が［Protected］の場合、ローミングクライアントは正常に動作しています。また、ローミングクライアントをインストールしたコンピュータの名前が、ダッシュボードに**ローミングコンピュータ**として追加されています。ダッシュボードにアクセスして追加を確認します。



10 ［導入］をクリック

11 ［ローミングコンピュータ］をクリック



12 コンピュータの追加を確認

ローミングクライアントをインストールしたコンピュータ名が、ステータス情報などとともにリスト表示されます。

3-2 ローミングクライアントをテストする

Cisco Umbrella ローミングクライアントをインストールしたコンピュータでテスト URL にアクセスして、正常に動作しているかどうか確認します。

1 ブラウザのアドレスバーに［**https://malware.opendns.com**］を入力

または次の URL をクリックして、テスト URL にアクセスします。

WEB https://malware.opendns.com

2 「ブロックページ」が表示されることを確認

ローミングクライアントが正常に動作している場合は、「**ブロックページ**」（［**このサイトはセキュリティに対する脅威があるためブロックされました**］メッセージ）が表示されます。

MEMO

シスコ コミュニティの「**Umbrella: 動作確認用 URL の紹介**」もご覧ください。

WEB community.cisco.com/t5/ セキュリティ - ドキュメント /umbrella- 動作確認用 -url- の紹介 /ta-p/3215326

注意

ブロックページの表示や SSL 復号を有効化したインテリジェントプロキシなど、Cisco Umbrella の HTTPS 通信関連機能を利用している場合、「**セキュリティ証明書**」に関する警告メッセージが表示されることがあります。たとえば、本来は❷のようなブロックページが表示されるべきタイミングで、右のような警告メッセージが表示されます（Google Chrome の例）。

この問題を解決するためには、シスコの「**ルート証明書**」をブラウザにインストールする必要があります。くわしくは、「**付録:シスコの「ルート証明書」をブラウザにインストールする**」をご覧ください。

4 ポリシーを設定する

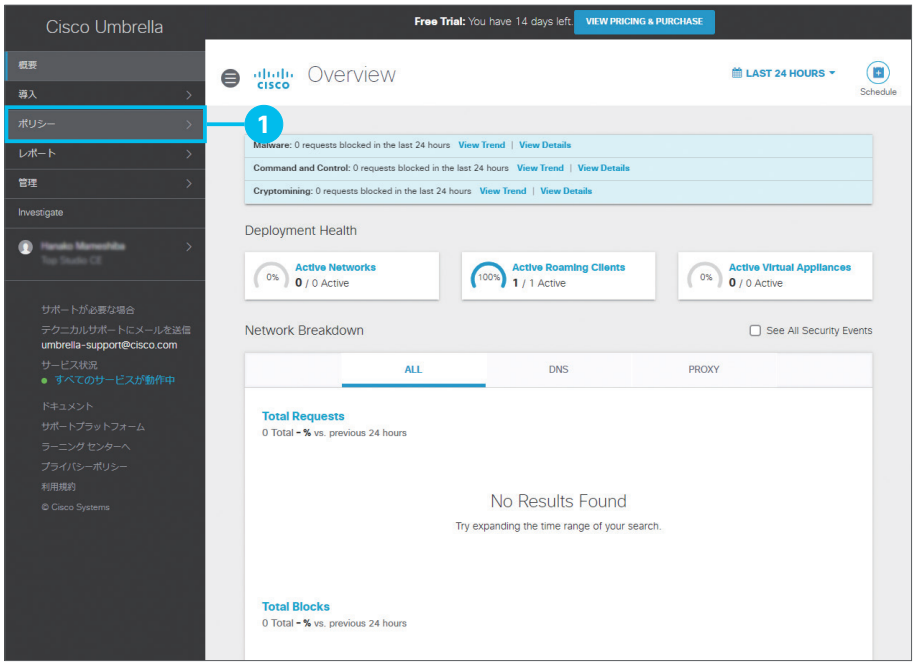
ポリシーとは、「**どのコンピュータにどんなセキュリティ設定を適用するか**」を定義した、ルールのようなものです。
Cisco Umbrella では、会社支給のコンピュータ用、社員の私物コンピュータ用など、適用対象に応じて柔軟にポリシーを設定できます。たとえば、次のような設定が可能です。

- 「DNS レイヤのセキュリティを適用したい」「コンテンツフィルタリングを適用したい」などの目的に応じた設定
- 「マルウェアをブロック」「フィッシング攻撃をブロック」「クリプトマイニングをブロック」など、セキュリティカテゴリに応じた設定
- ブロックしたいコンテンツを含む Web サイトを「高い」「中程度」「低い」のカテゴリグループで選択、または個別のカテゴリで選択するなど、コンテンツカテゴリに応じたフィルタリング設定

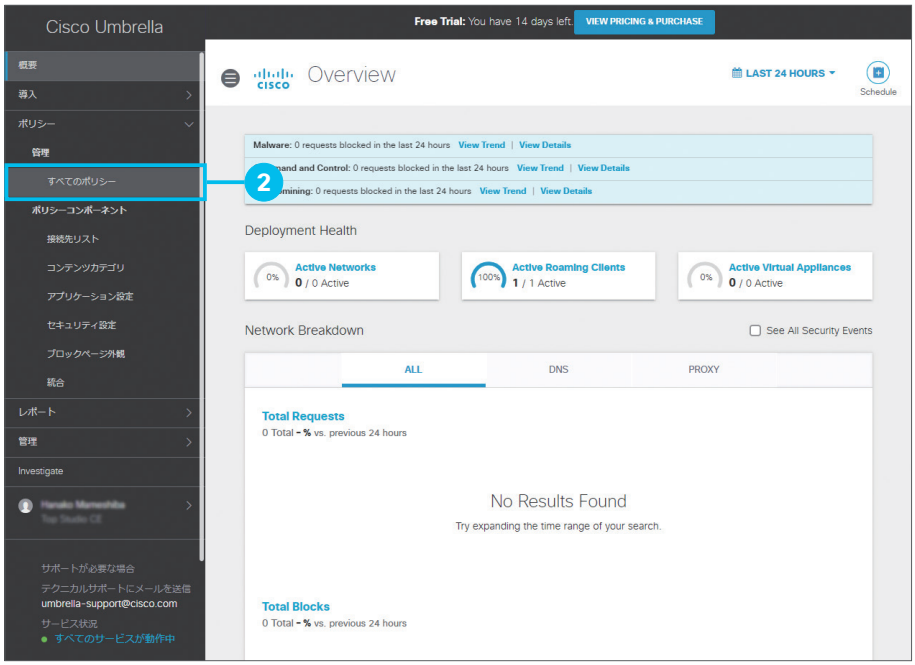
Cisco Umbrella ローミングクライアントをインストールしたコンピュータには、デフォルトでは（文字どおりの）「**Default Policy**」が適用されます。このポリシーの初期設定では、マルウェア、コマンド & コントロールのコールバック、フィッシング攻撃をブロックします。
Default Policy を編集することで、たとえばクリプトマイニングもブロックする、コンテンツフィルタリングも適用するなどの追加設定も可能です。しかし、Default Policy はすべてのコンピュータに適用されるため、たとえば会社支給のコンピュータ用と社員の私物コンピュータ用で異なるポリシーを適用したい場合には、新しくポリシーを追加する必要があります。
本ガイドでは一例として、社員の私物コンピュータ用にプライバシーに配慮したロギング設定で、ポリシーを追加する手順を紹介します（Default Policy を編集する場合も参考にしてください）。

4-1 ポリシーを追加する

Cisco Umbrella ダッシュボードにログインして、新しくポリシーを追加します。



1 ［**ポリシー**］をクリック



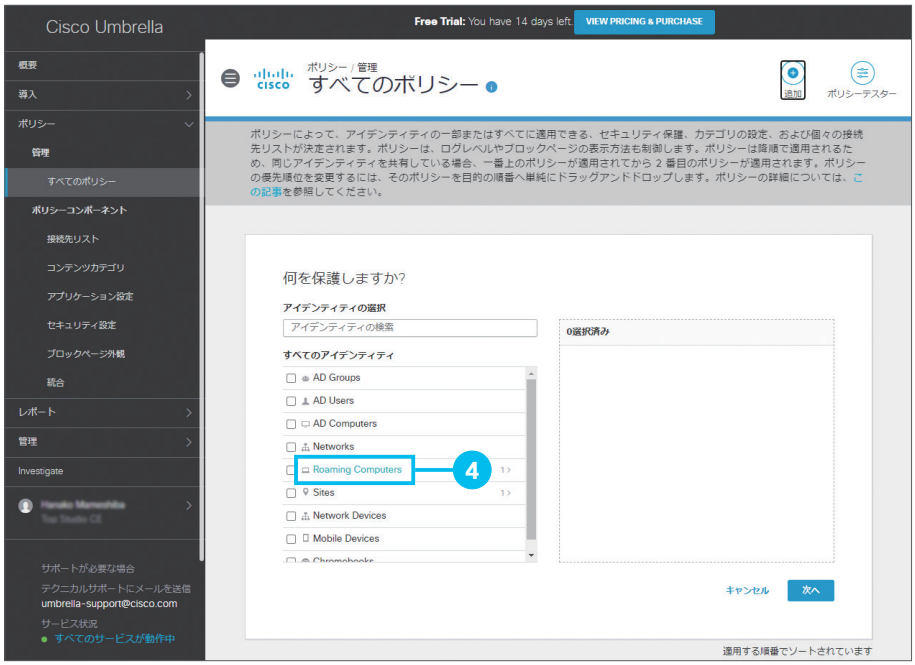
2 ［**すべてのポリシー**］をクリック

セキュア インターネットゲートウェイ（SIG）Essentials パッケージでは、［**DNS ポリシー**］をクリックします。

3 ［**追加**］をクリック

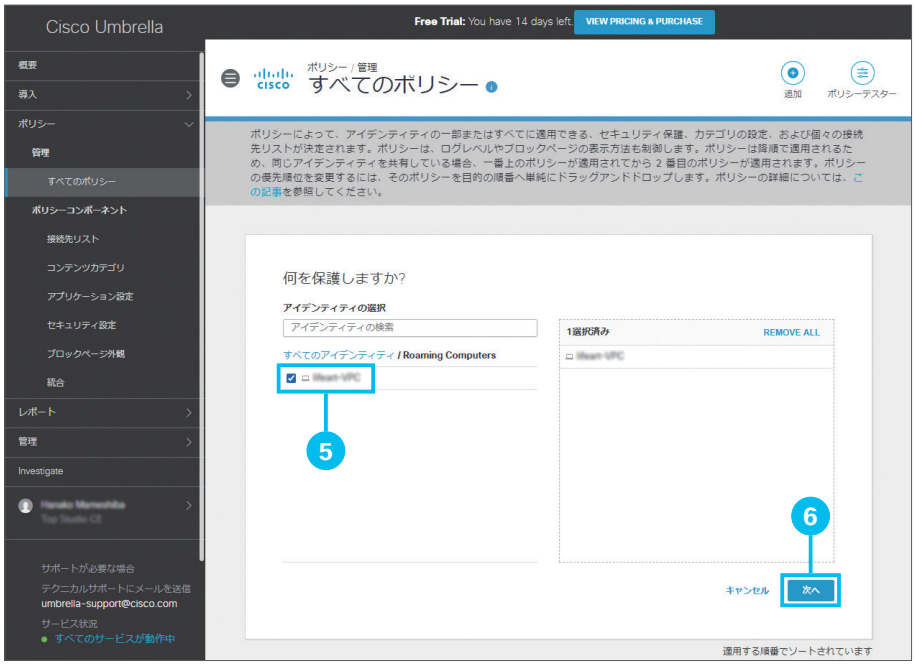
注意

パッケージによって、設定項目や表示画面が異なります。本ガイドでは主として、DNS セキュリティ Advantage パッケージに相当する無料トライアルの画面例を使用しています。



4 ［Roaming Computers］をクリック

［Roaming Computers］文字列をクリックします。



5 ポリシーを適用したいコンピュータ名のチェックボックスをクリックして選択

6 ［次へ］をクリック

MEMO

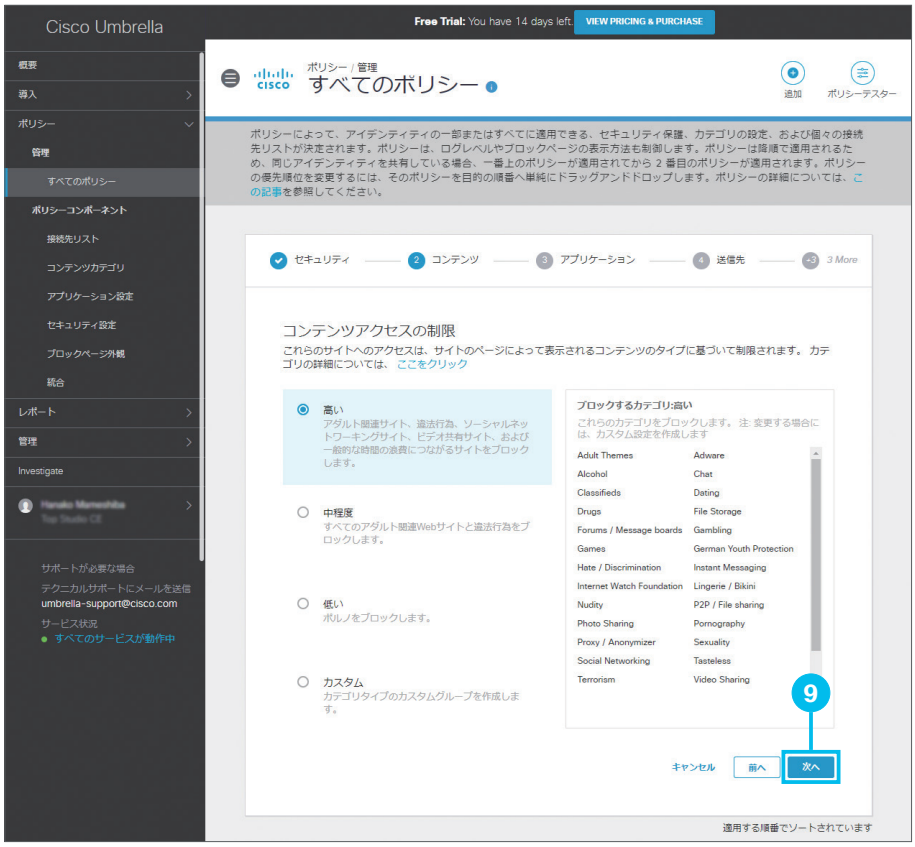
❹で［Roaming Computers］チェックボックスをクリックすると、すべてのローミングコンピュータがポリシーの適用対象になります。本ガイドで紹介している設定例のように、特定のローミングコンピュータ（社員の私物コンピュータ）用にポリシーを追加する場合は、［Roaming Computers］文字列をクリックして、❺のようにポリシーを適用したいコンピュータを個別に選択します。

7 ［**次へ**］をクリック

以降の設定項目（ポリシーコンポーネント）を選択できます。デフォルトでは設定可能なすべての項目が選択されています。

8 ［**次へ**］をクリック

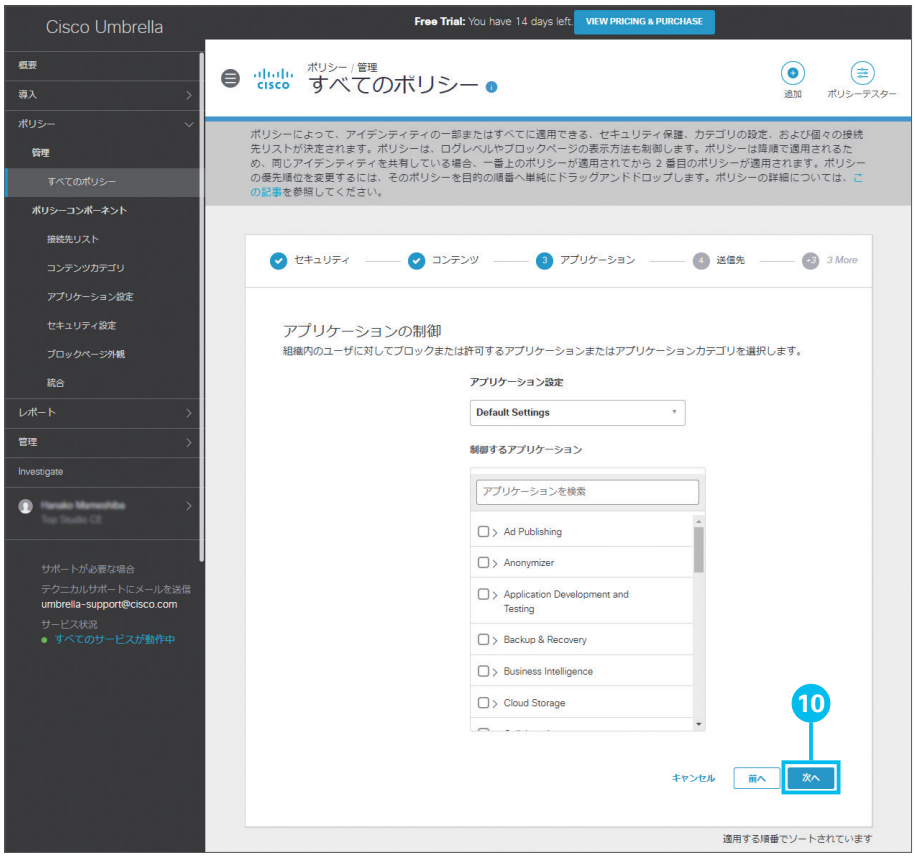
［**ブロックするカテゴリ**］の［**編集**］をクリックすると、DNS レイヤのセキュリティでブロックするセキュリティカテゴリを選択できます。デフォルトでは、［**マルウェア**］、［**コマンド & コントロールのコールバック**］、［**フィッシング攻撃**］が選択されています。



9 ［**次へ**］をクリック

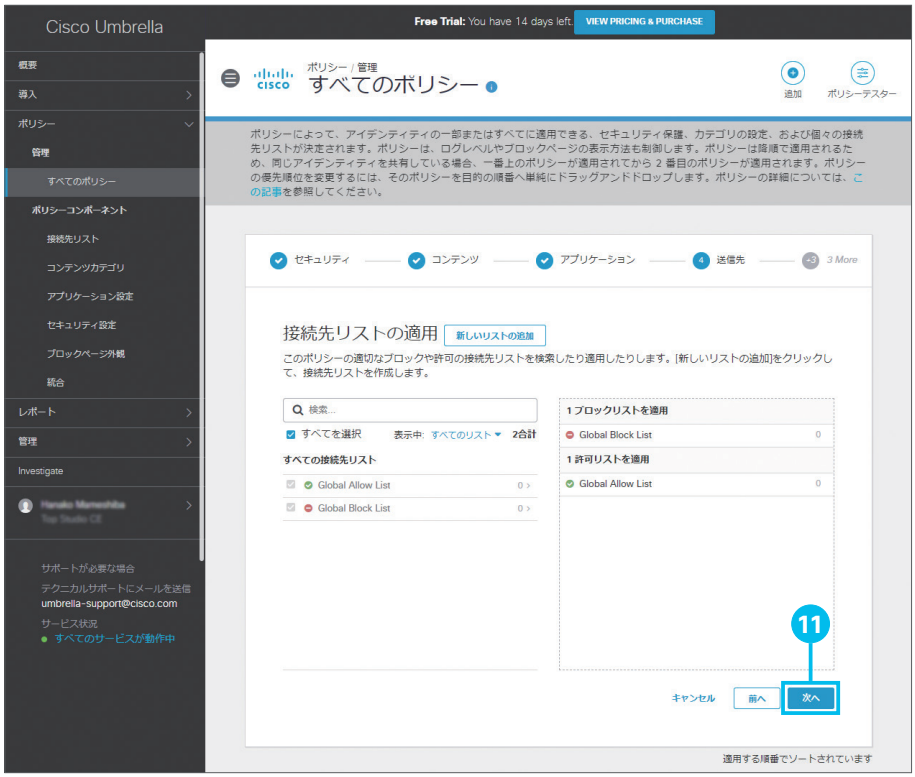
ブロックしたいコンテンツを含む Web サイトを［**高い**］［**中程度**］［**低い**］のカテゴリグループ別、または［**カスタム**］で個別のカテゴリ別に選択できます。デフォルトでは［**高い**］が選択されています。

本ガイドで紹介している設定例のように、社員の私物コンピュータ用にプライバシーに配慮したい場合は、［**低い**］や［**カスタム**］を選択、または**7**で［**コンテンツアクセスの制限**］を選択しないことを推奨します。



10 ［**次へ**］をクリック

ブロックしたいアプリケーションをカテゴリ別または個別に選択できます。



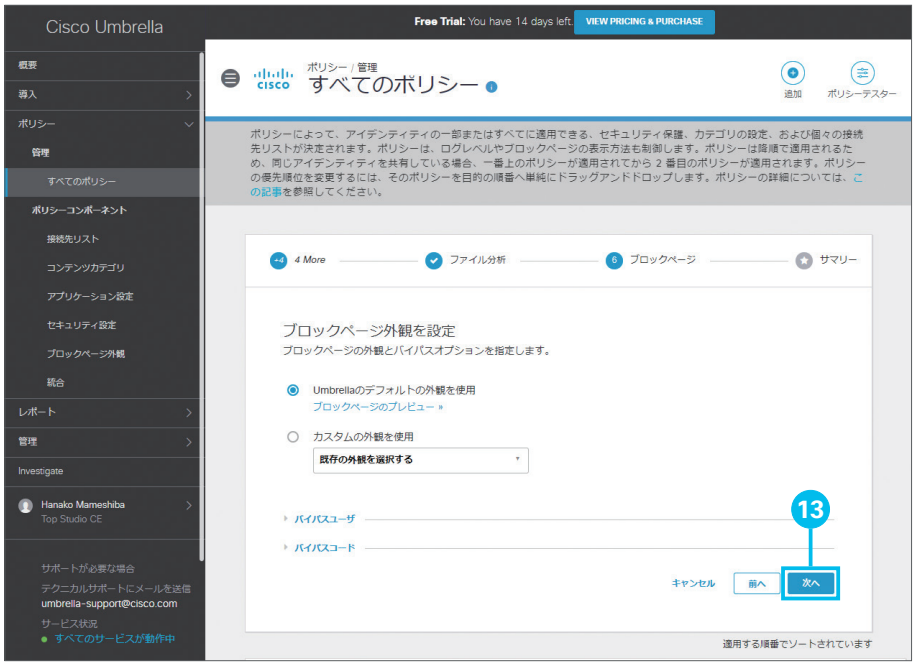
11 ［**次へ**］をクリック

ブロックまたは許可したいドメインや URL を含む接続先リストを選択および追加できます。デフォルトでは［**Global Block List**］によるブロックリスト、［**Global Allow List**］による許可リストが選択されています。

> **MEMO**
>
> ［**Global Block List**］および［**Global Allow List**］は、すべてのポリシー設定に適用されます。この 2 つの接続先リストは［**ポリシー**］メニューの［**接続先リスト**］で編集できます。

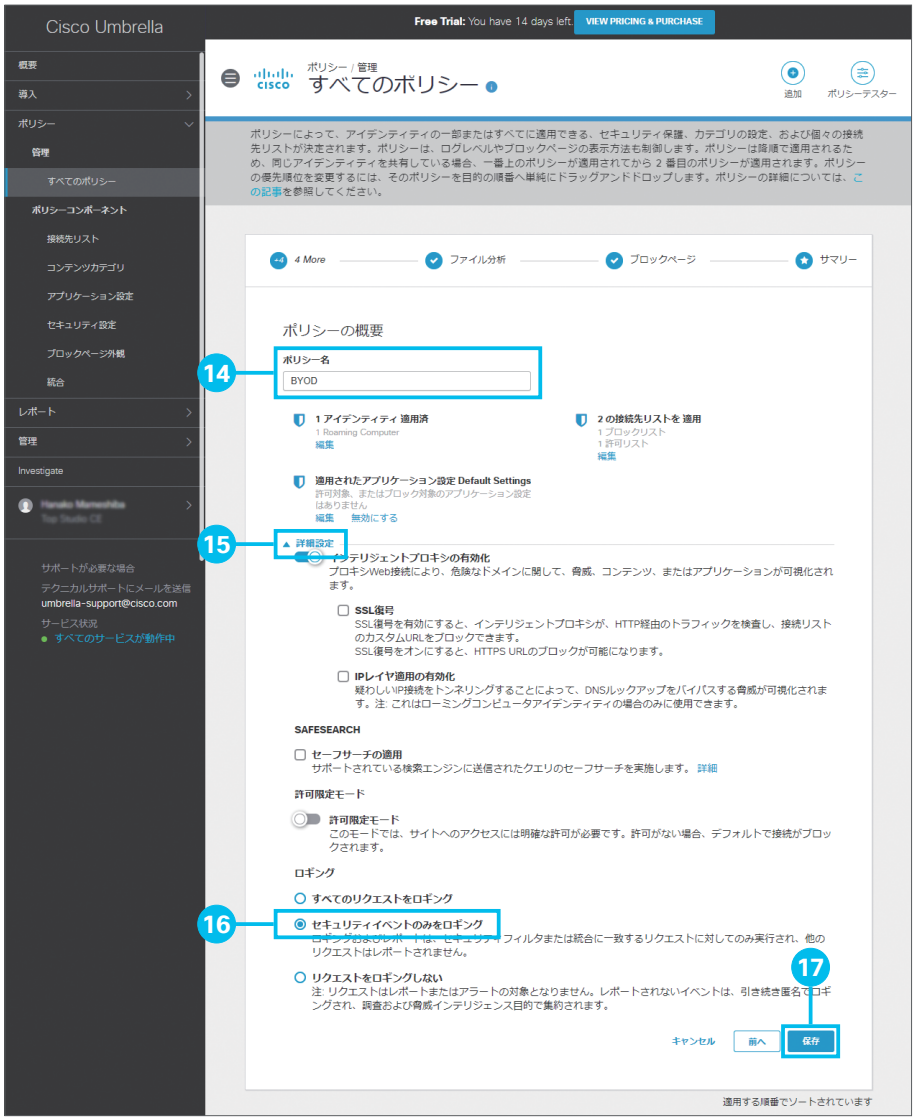
12 ［**次へ**］をクリック

ファイルを分析して、マルウェアなど悪意のあるファイルをブロックできます。
DNS セキュリティ Essentials パッケージでは表示されない（利用できない）設定項目です。DNS セキュリティ Advantage およびセキュアインターネットゲートウェイ（SIG）Essentials パッケージでは、デフォルトでオンになっています。



13 ［**次へ**］をクリック

ブロックするように設定した Web サイトにユーザがアクセスすると表示される「**ブロックページ**」の外観を設定できます。



14 ［**ポリシー名**］に任意の名前を入力

15 ［**詳細設定**］をクリック

16 ［**セキュリティイベントのみをロギング**］をクリックして選択

デフォルトでは［**すべてのリクエストをロギング**］が選択されています。本ガイドで紹介している設定例のように、社員の私物コンピュータ用にプライバシーに配慮したい場合は、［**セキュリティイベントのみをロギング**］を選択します。［**すべてのリクエストをロギング**］を選択した場合は、社員のプライベート利用も含めた全リクエスト（接続先）がロギング（記録）されますが、［**セキュリティイベントのみをロギング**］を選択した場合は、ポリシー設定に基づいてブロックされたリクエストなど、セキュリティに関連するリクエストのみロギングされます。

17 ［**保存**］をクリック

18 ポリシーの追加を確認

⓮で入力したポリシー名が表示されていることを確認します。ポリシーは適用する順番に表示されます。

MEMO

Default Policy 以外に複数のポリシーを運用している環境では、ポリシーをドラッグ & ドロップすることで、ポリシーが適用される順番を調整できます。

4-2 ポリシーをテストする

最後に、新しく追加したポリシーが正常に適用されているかどうか確認します。

1 ［**ポリシーテスター**］をクリック

2 ［**アイデンティティ**］検索ボックスにポリシーをテストしたいコンピュータ名を入力し、表示された検索候補から該当するコンピュータ名をクリックして選択

本ガイドの設定例では、「**4-1　ポリシーを追加する**」5で選択したコンピュータ名を検索します。

3 ［**接続先**］に任意の URL を入力

4 ［**テストの実行**］を入力

5 ［**適用されたポリシー**］を確認

本ガイドの設定例では、「**4-1　ポリシーを追加する**」14で入力したポリシー名が表示されていることを確認します。

以上で、Cisco Umbrella ローミングクライアントのセットアップは完了しました。

TIP MEMO

Default Policy 以外に複数のポリシーを運用している環境で、意図しないテスト結果が表示される場合は、1の［**すべてのポリシー**］画面でポリシーが適用される順番を調整してください。

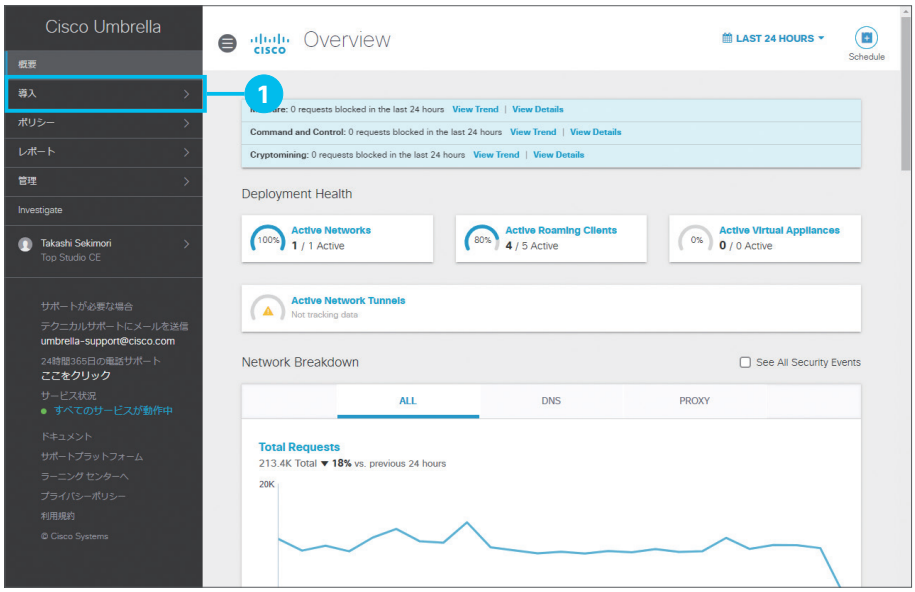
付録：シスコの「ルート証明書」をブラウザにインストールする

ブロックページの表示や SSL 復号を有効化したインテリジェントプロキシなど、Cisco Umbrella の HTTPS 通信関連機能を利用している場合、「**セキュリティ証明書**」に関する警告メッセージが表示されることがあります。たとえば、本来はブロックページが表示されるべきタイミングで、右のような警告メッセージが表示されます（Google Chrome の画面例）。

この問題を解決するためには、シスコの「**ルート証明書**」をブラウザにインストールする必要があります。これによって、警告メッセージが表示される問題を解決できるだけでなく、ファイル検査などの HTTPS 通信関連機能でブロック可能なトラフィックが増加するなど、セキュリティ効果の向上も期待できます。

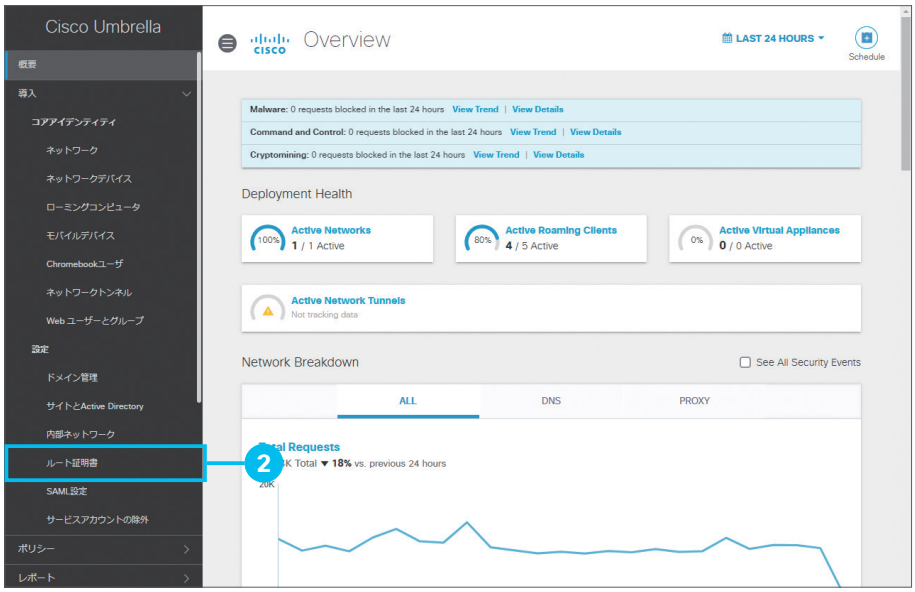
本ガイドでは、各ユーザが Google Chrome に手動でルート証明書をインストールする画面例を紹介します。その他のブラウザ、および、大規模ネットワークの管理者が Active Directory のグループポリシーを利用して、全ユーザの任意のブラウザに自動でインストールする場合など、その他のインストールオプションに関しては、オンラインドキュメント『**Cisco Umbrella ユーザガイド**』の「**Cisco 証明書のインポート**」をご覧ください。

docs.umbrella.com/deployment-umbrella/docs/cisco- 証明書のインポート

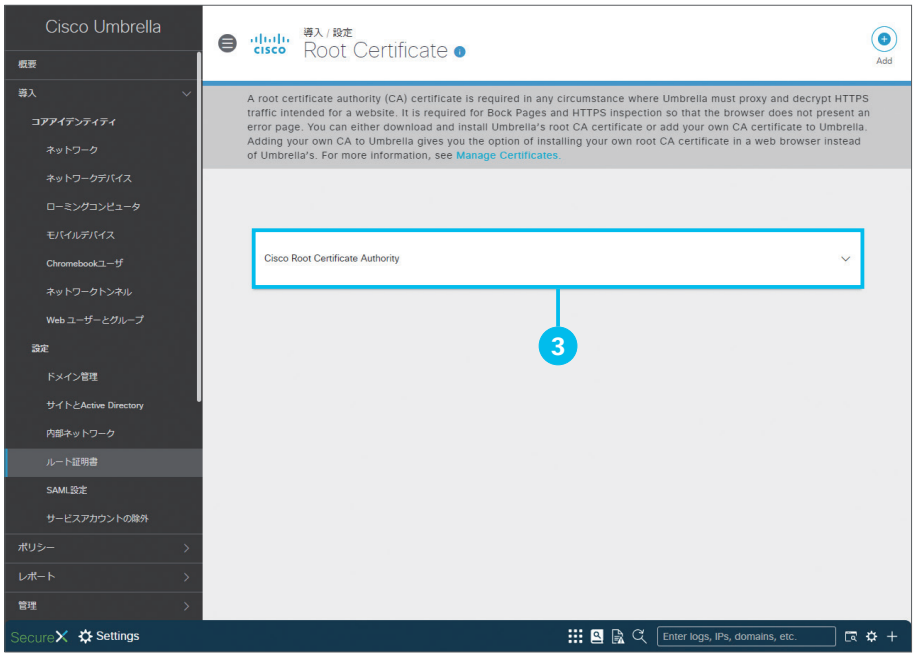


1 ［**導入**］をクリック

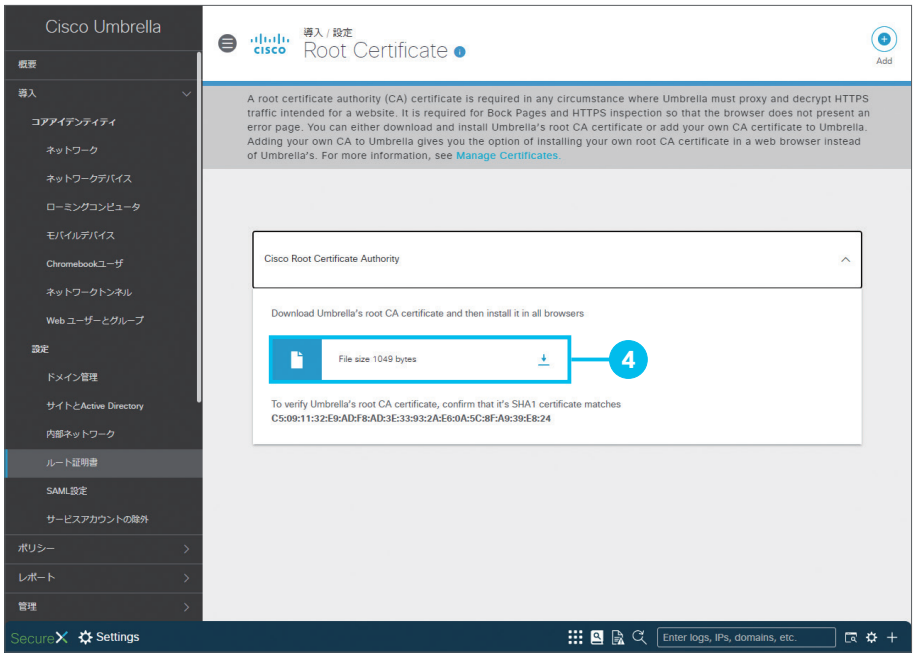
Umbrella ダッシュボードにアクセスして、［**導入**］をクリックします。



2 ［**ルート証明書**］をクリック



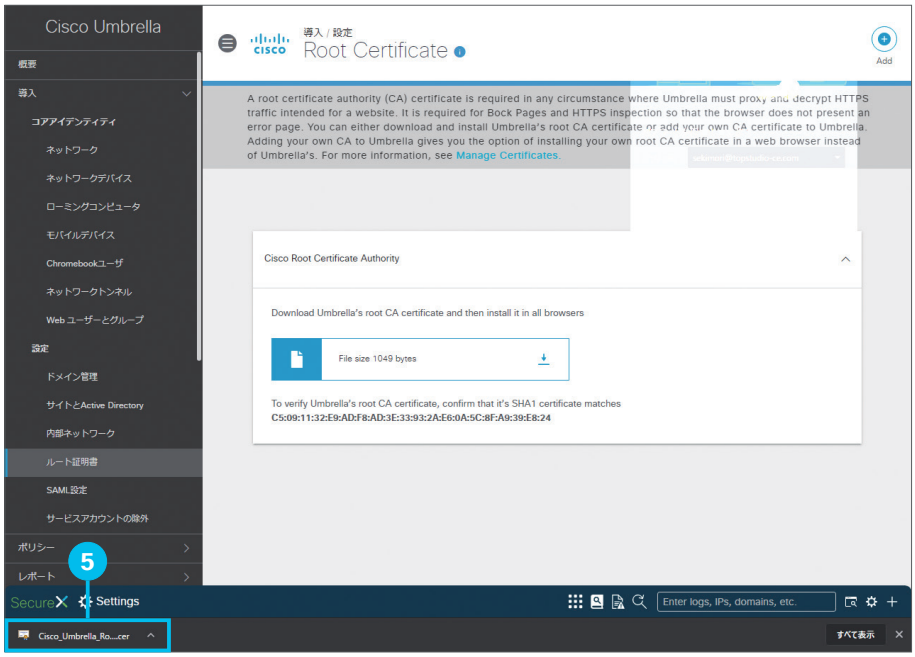
3 ［Cisco Root Certificate Authority］をクリック



4 ［ ］アイコンをクリック

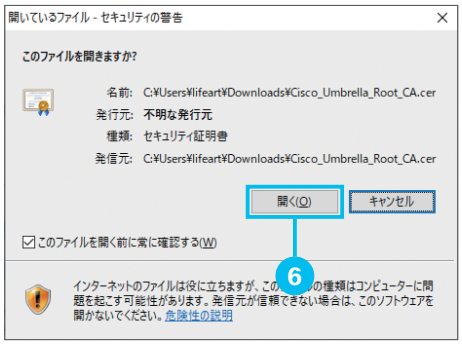
ルート証明書をダウンロードします。

> **MEMO**
>
> 「**この種類のファイルはコンピュータに損害を与える可能性があります。Cisco_Umbrella_Root_CA.cer のダウンロードを続けますか?**」などの警告メッセージが表示されることがありますが、［**保存**］をクリックして続行してください。

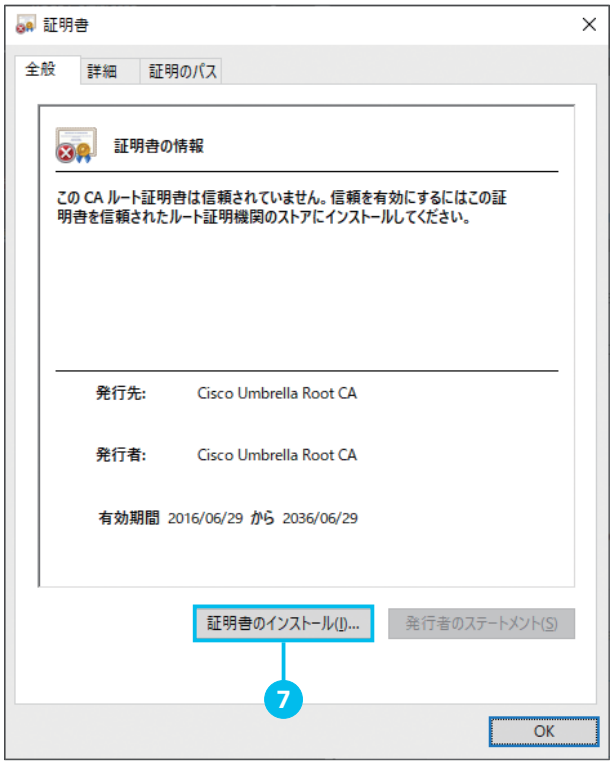


5 ルート証明書をクリック

ダウンロードしたルート証明書（Cisco_Umbrella_Root_CA.cer）をクリックして開きます。「**セキュリティの警告**」ダイアログボックスが表示されます。



6 ［**開く**］をクリック

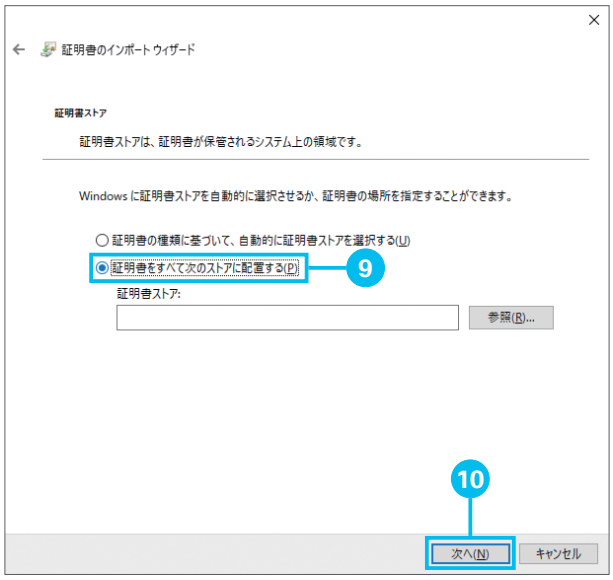


7 ［**証明書のインストール**］をクリック

「**証明書のインポート ウィザード**」が表示されます。

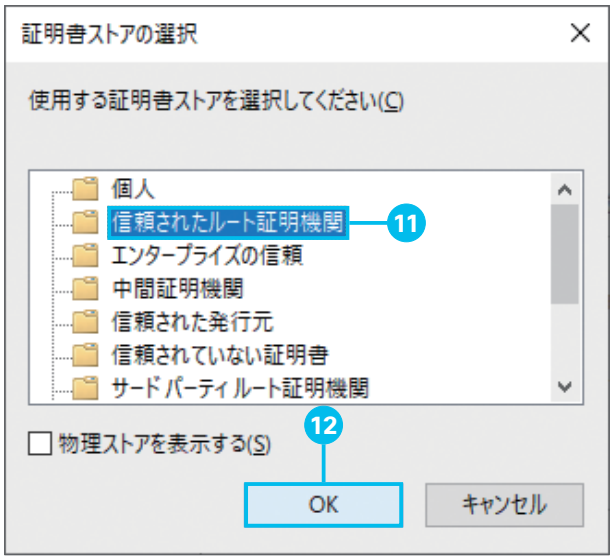
8 ［**次へ**］をクリック

デフォルトでは［**現在のユーザ**］が選択されています。必要に応じて［**ローカル コンピューター**］を選択してください。



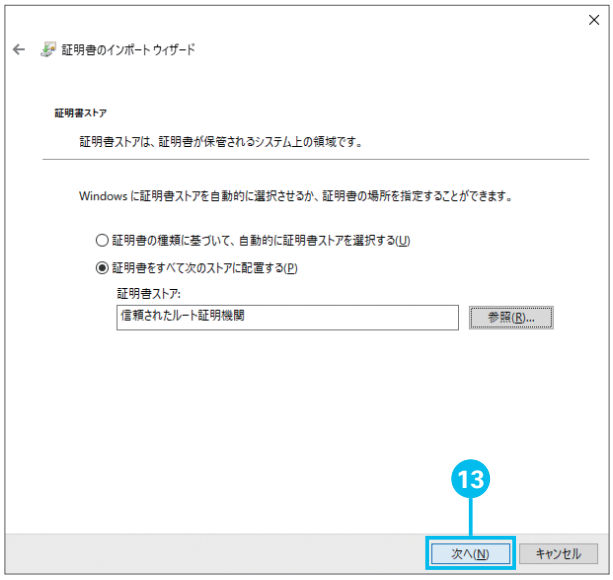
9 ［**証明書をすべて次のストアに配置する**］をクリック

10 ［**参照**］をクリック

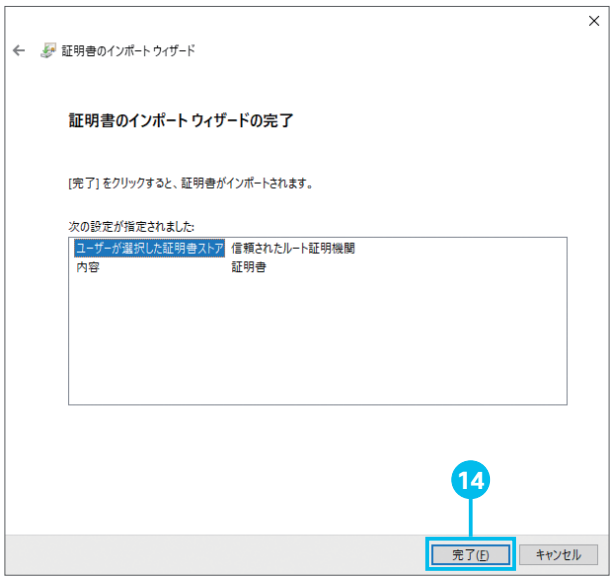


11 ［**信頼されたルート証明機関**］をクリック

12 ［**OK**］をクリック

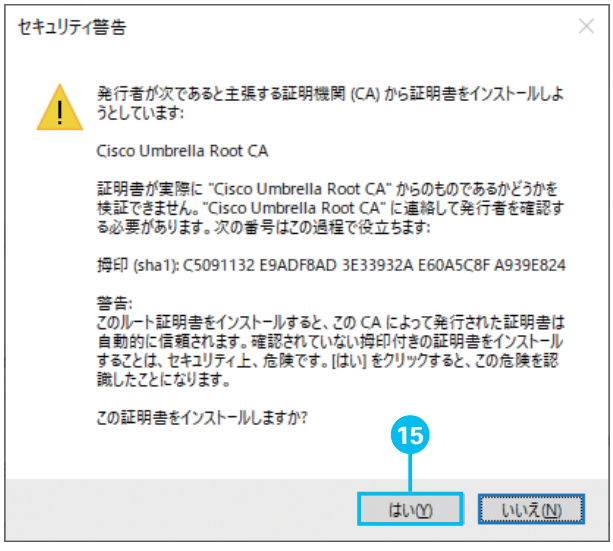


13 ［**次へ**］をクリック

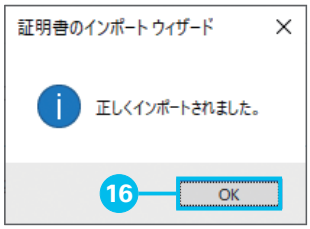


14 ［**完了**］をクリック

「**セキュリティ警告**」ダイアログボックスが表示されます。

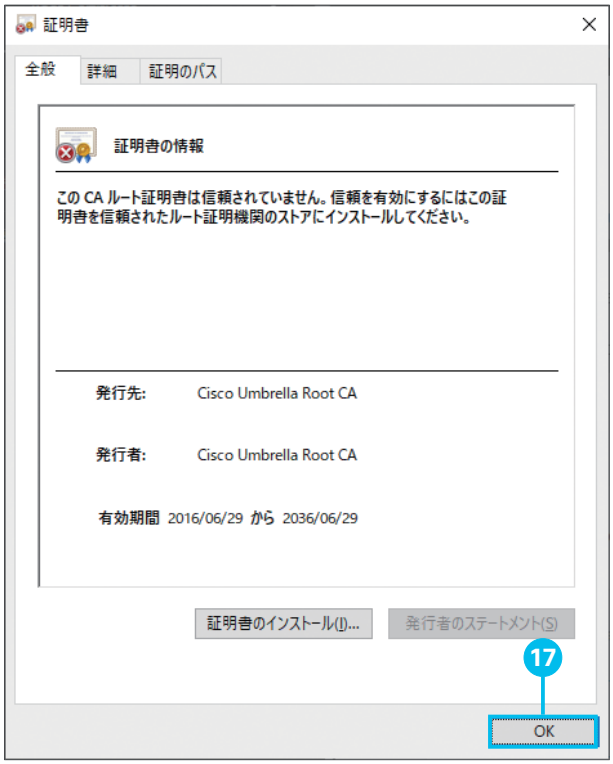


15 ［**はい**］をクリック



16 ［OK］をクリック

［**正しくインポートされました**］メッセージを確認したら、［OK］をクリックします。



17 ［OK］をクリック

以上で、ルート証明書のインストールが完了しました。

シスコ コンタクトセンター

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 10:00-12:00, 13:00-17:00
0120-092-255

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

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
http://www.cisco.com/jp

2174-2009-000-TO