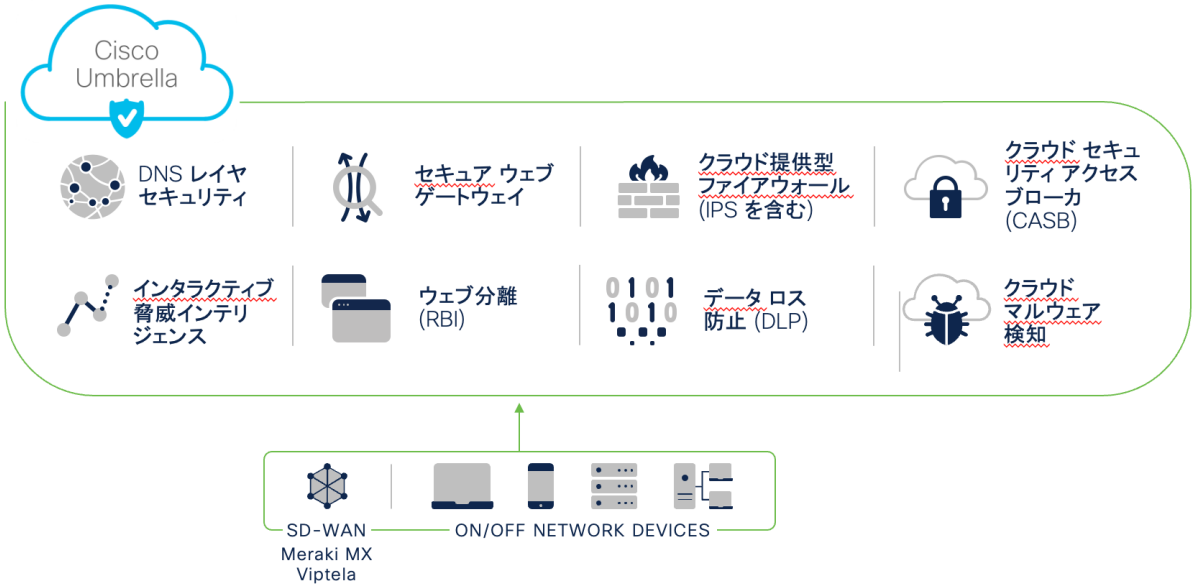
Cisco Umbrella SIG
ローミングコンピュータ

かんたんセットアップガイド

2024年6月

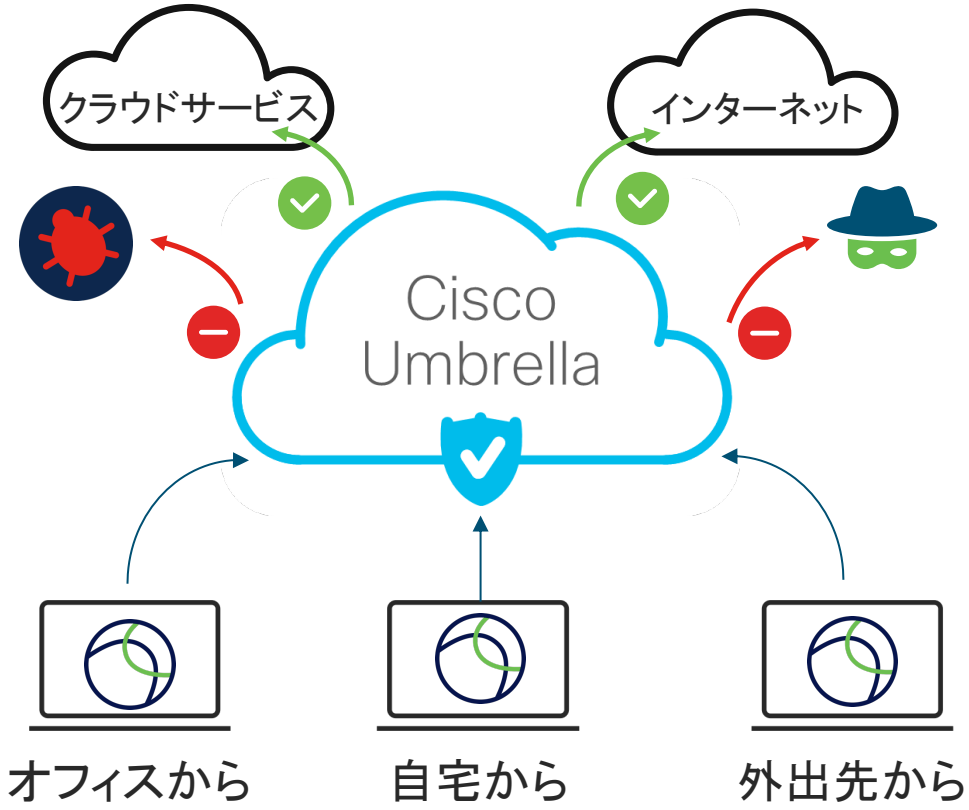
はじめに

- **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。



はじめに

- **Cisco Umbrella** をご契約のお客様は、お使いのコンピュータで **Cisco Secure Client (旧AnyConnect)クライアントをインストール**および **Umbrella モジュールを有効化**することで、DNS レイヤ セキュリティおよびセキュア Web ゲートウェイによって、オフィスや自宅、外出先など、場所を問わず、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。



対応OS(Cisco Secure Client:Umbrellaモジュール)

- Cisco Secure Client(旧AnyConnect):Umbrellaローミングセキュリティモジュール(以下 Umbrellaモジュールという。)は次のOS※で動作します。
  - バージョン5.1.0以降
    - Windows 10 (64ビット,86ビット)
    - Windows 11 (64ビット、ARM版64 ビット)
  - macOS 11.x以上

※最新の対応OS一覧は以下オンラインドキュメントをご覧ください。

利用システム要件
https://docs.umbrella.com/deployment-umbrella/docs/prerequisites-5#system

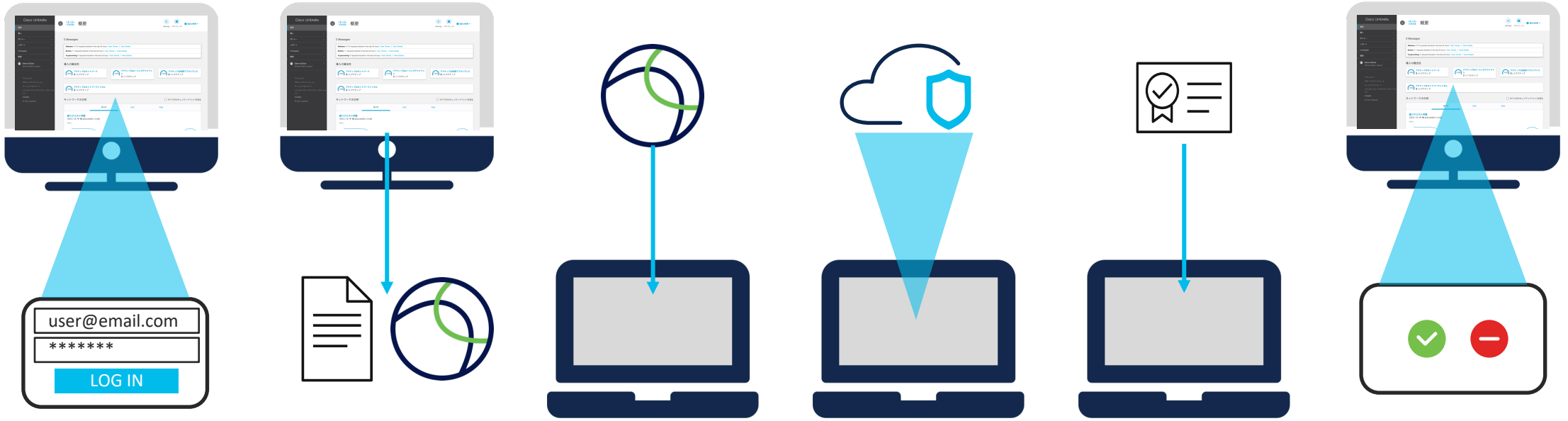
対応ブラウザ(ダッシュボード)

- 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（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
  - Mozilla Firefox

注意
本ガイドは、2024年6月時点のCisco Umbrellaダッシュボード及びCisco Secure Clientを、Windows11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やブラウザ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。

セットアップの流れ

1. ダッシュボードにログイン
2. プロファイルとインストーラをダウンロード
3. Cisco Secure Clientをインストール
4. Umbrellaモジュールを有効化
5. ルート証明書をインストール
6. ポリシーを設定



目次

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

1.ダッシュボードにログインする

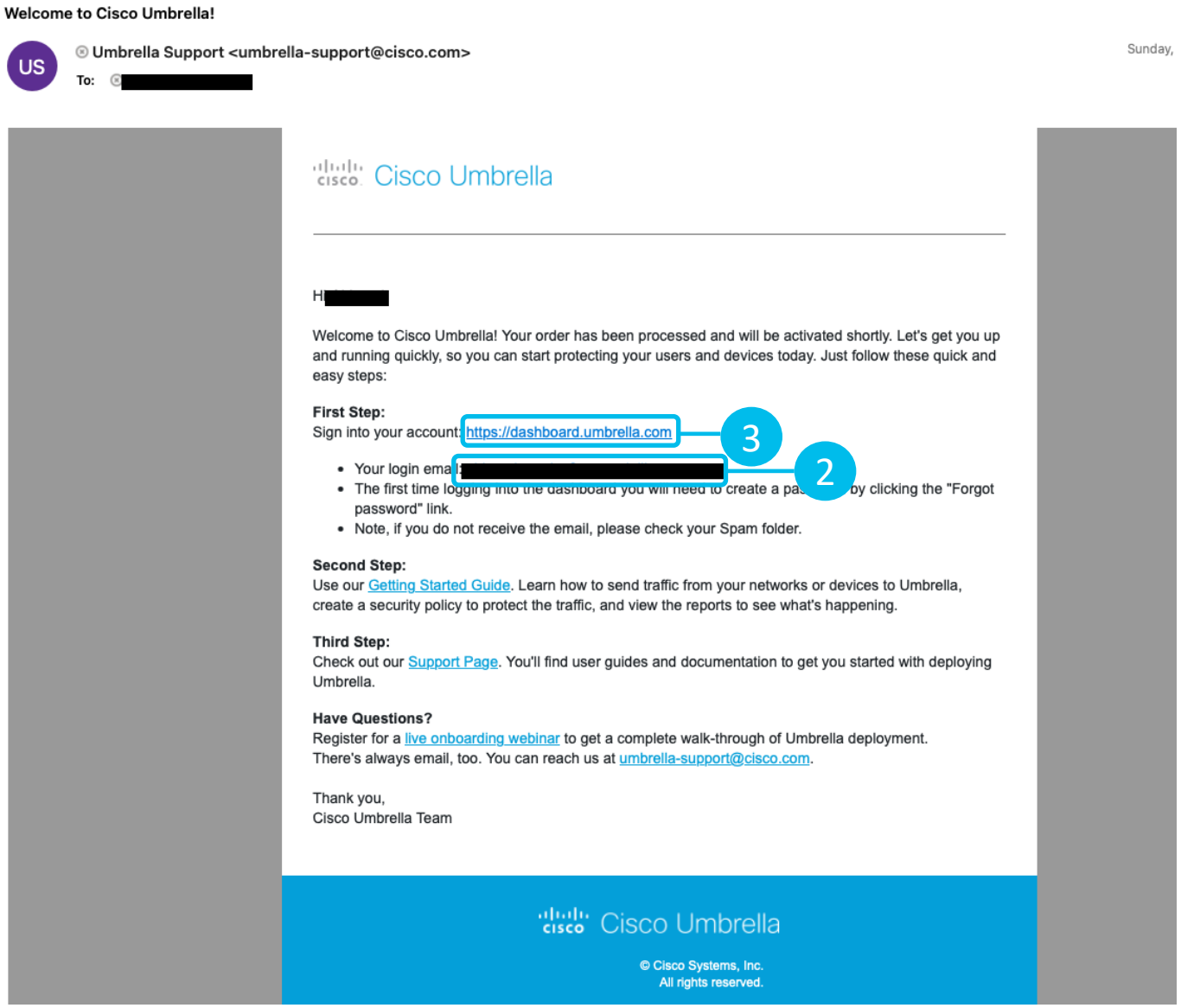
1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

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「**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 Cisco Umbrella Teamからの件名 [**Welcome to Cisco Umbrella!**]メールを開封

1. ダッシュボードにログインする



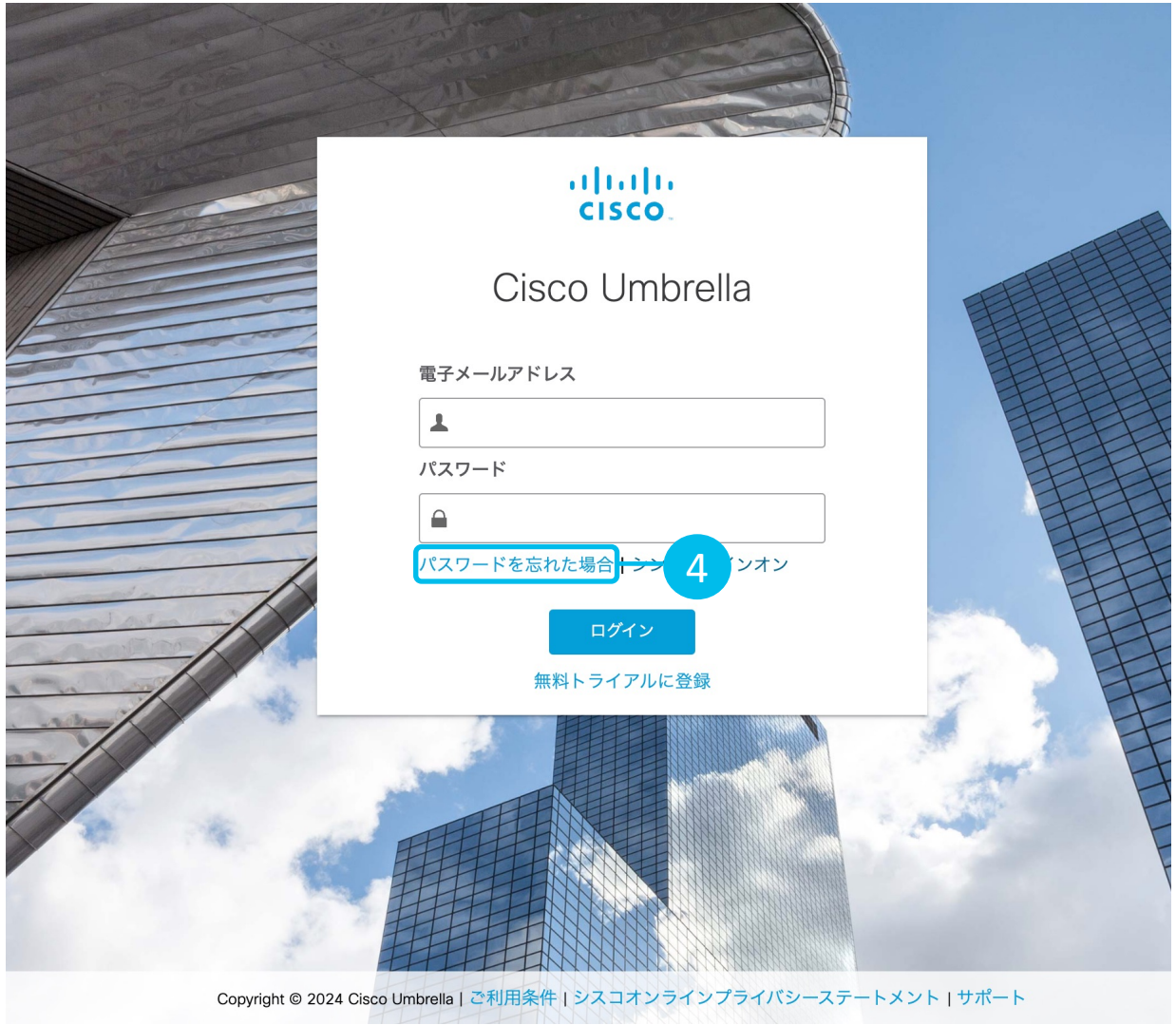
2 **[Your login email]に記載されているメールアドレスを確認**

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]②記載されているリンクをクリック**

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。

1. ダッシュボードにログインする



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。

1. ダッシュボードにログインする

5 [**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

6 [**パスワードのリセット**]をクリック

⑤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。

1. ダッシュボードにログインする

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。

1. ダッシュボードにログインする

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。

1. ダッシュボードにログインする

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、Cisco Secure Clientのプロファイルと、インストーラをダウンロードします。

2.プロファイルとインストーラをダウンロードする

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

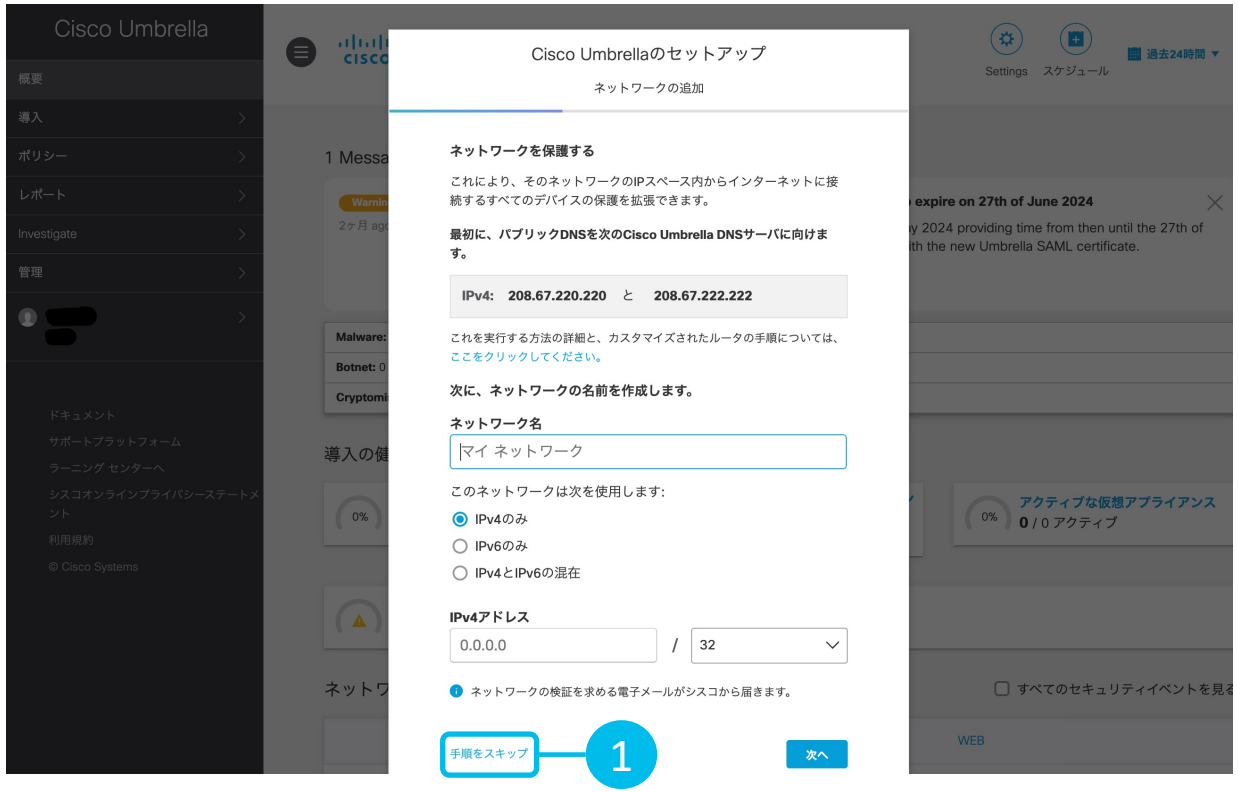
2. プロファイルとインストーラをダウンロードする

- Cisco Umbrella ダッシュボードから2点ダウンロードします。
  - Cisco Secure Client(Umbrellaモジュール)のプロファイル
  - Cisco Secure Clientのインストーラ

注意
Cisco UmbrellaではUmbrellaモジュールのみ利用します。Cisco Secure FirewallやCisco Meraki MX等に対してリモートアクセスVPNを利用するためVPNモジュールを利用する場合、別途Cisco Secure Clientライセンスが必要となります。

2. プロファイルとインストーラをダウンロードする

- 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。2 回目以降のログイン時は、④からご覧ください。

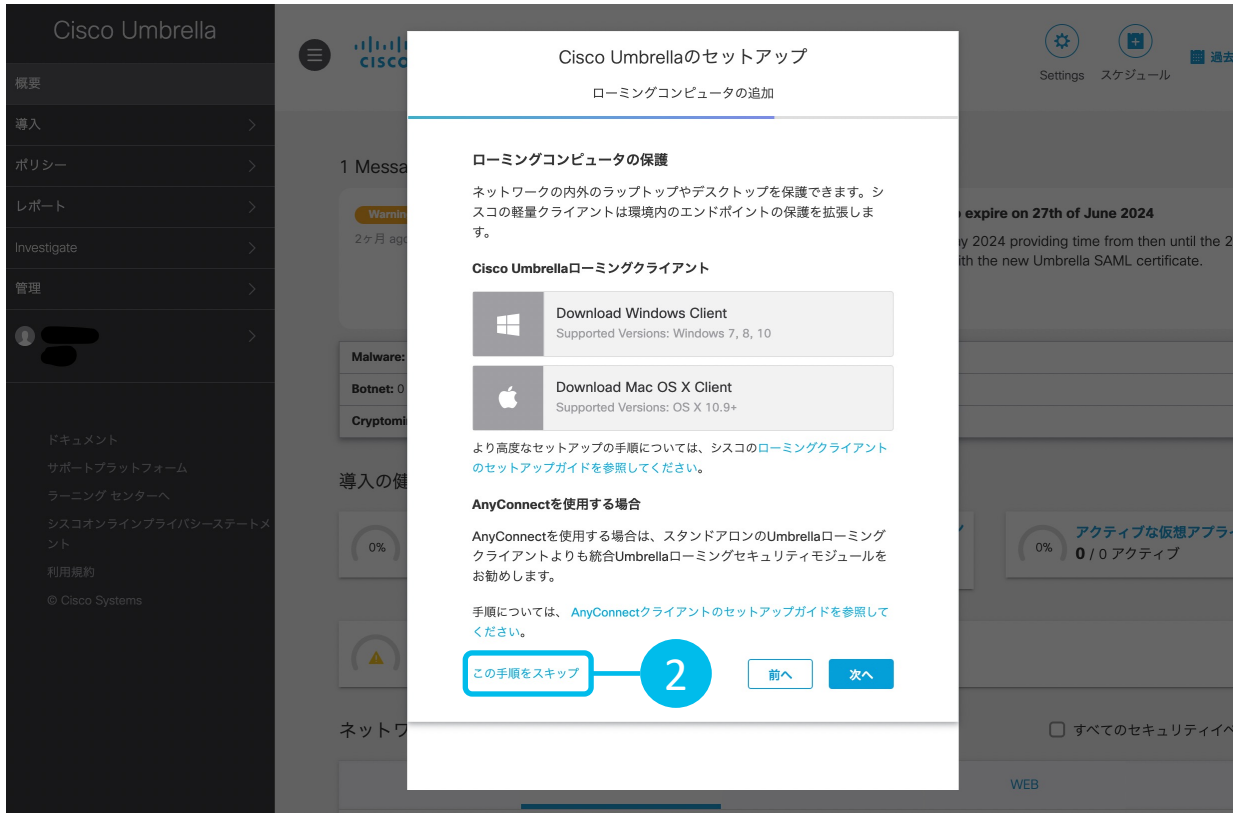


1 [手順をスキップ]をクリック

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。

※「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。
詳細はオンラインドキュメントを参照ください。
https://docs.umbrella.com/umbrella-user-guide/docs/register-a-fixed-network

2. プロファイルとインストーラをダウンロードする



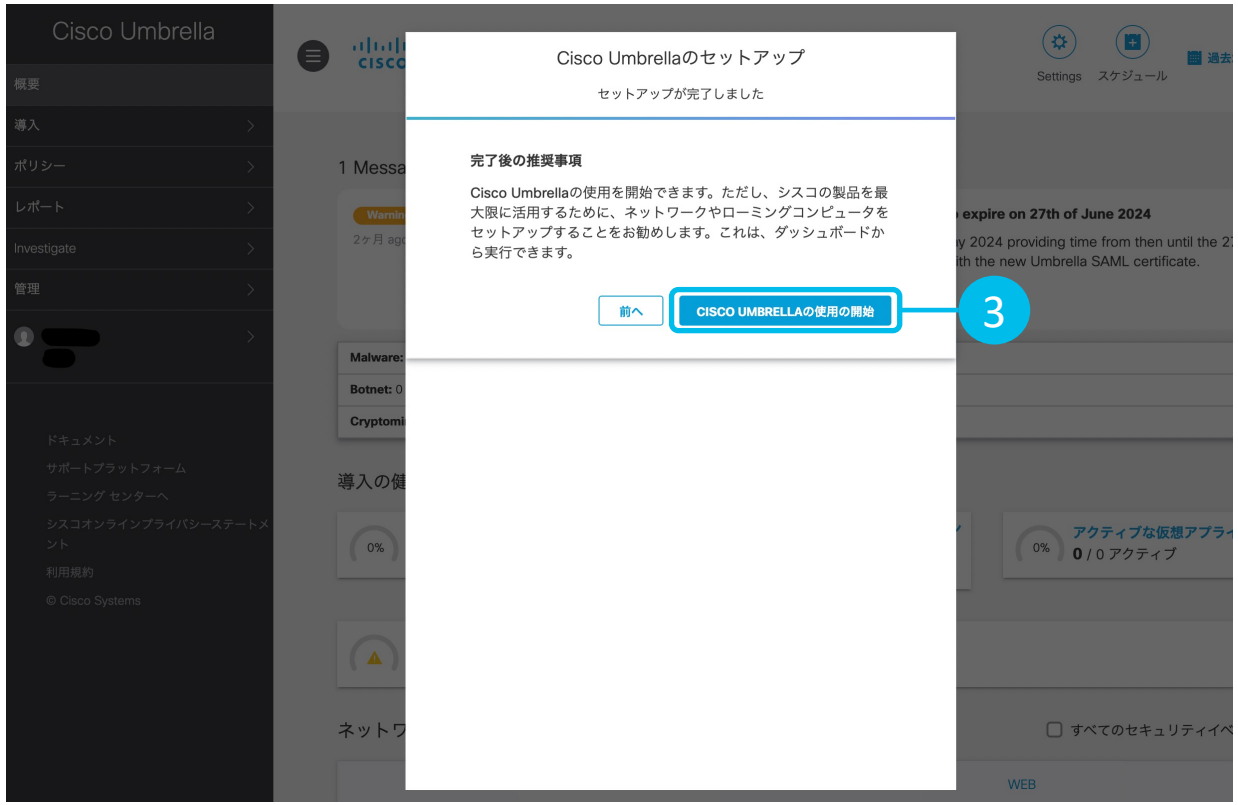
2 [手順をスキップ]をクリック

さらに「ローミングコンピュータの追加」画面が表示されますが、本ガイドでは省略します。

注意

「Cisco Umbrellaローミングクライアント」はDNSレイヤセキュリティを提供するソフトウェアです。(2025年4月 サポート終了予定)
Cisco Secure Client(Umbrellaモジュール)と異なりますのでご注意ください。Umbrellaローミングクライアントの機能は全てCisco Secure Clientでご利用いただけます。

2. プロファイルとインストーラをダウンロードする



3 **[CISCO UMBRELLAの使用に開始]をクリック**

ウィザードが閉じて、ダッシュボードの概要が表示されます。

2. プロファイルとインストーラをダウンロードする

4 [導入]をクリック

2. プロファイルとインストーラをダウンロードする

5 [ローミングコンピュータ]をクリック

2. プロファイルとインストーラをダウンロードする

6 **[ローミングクライアント]をクリック**

[Cisco Secure Clientダウンロード]
ポップアップウィンドウが開きます。

目次に戻る

2. プロファイルとインストーラをダウンロードする

7 Cisco Secure Clientのインストーラをダウンロード

- [**展開前パッケージ**]を選択します。
- 利用OSに応じて一つ選択
  -Windows(x86/x64)
  -Windows(Arm)
  -macOS

注意

Cisco Umbrellaローミングクライアント」はサポート終了予定となるため、Cisco Secure Client利用推奨です。

8 [**モジュールのプロファイルをダウンロード**]をクリックし、プロファイルをダウンロード及び任意の場所に保存

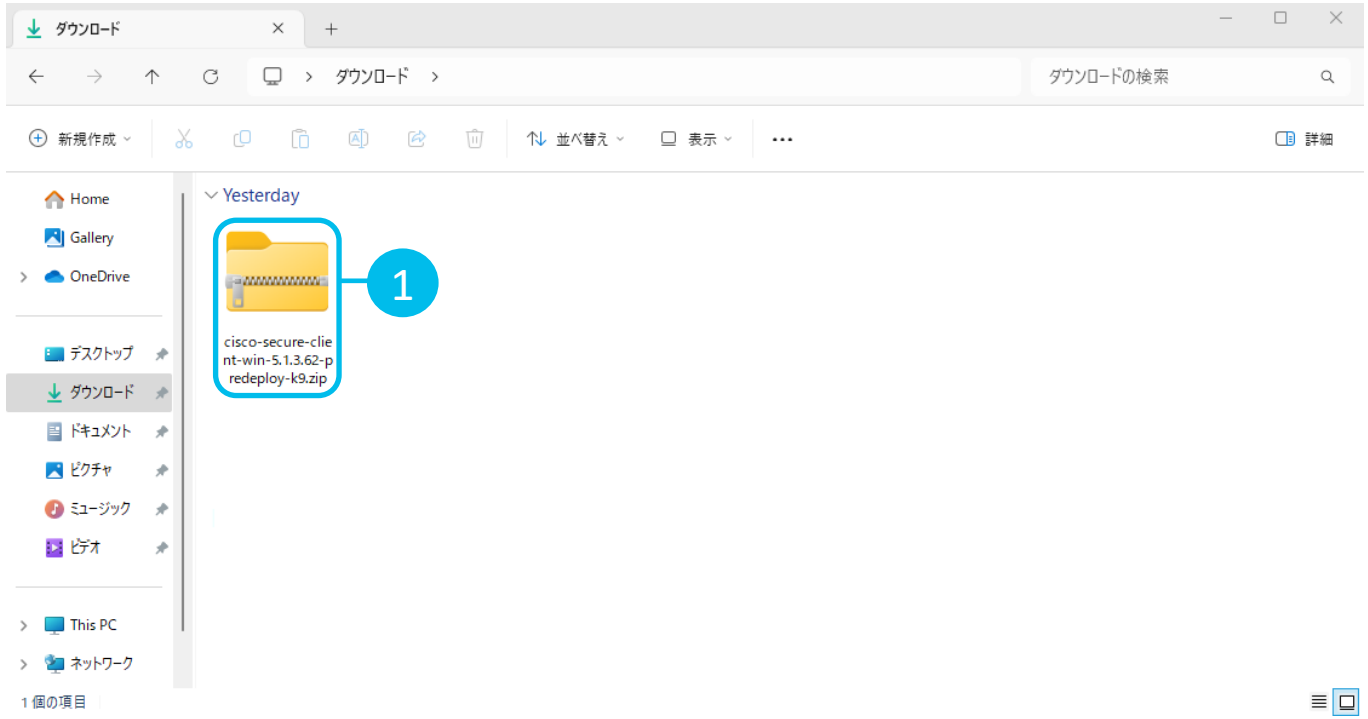
Cisco Secure Client(Umbrellaモジュール)のプロファイルをダウンロードし、任意の場所に保存します。

3.Cisco Secure Client をインストール

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

3. Cisco Secure Clientをインストール

- Cisco Umbrella で保護したいコンピュータにて、インストーラを解凍および実行し、Cisco Secure Clientをインストールします。本ガイドではWindow 11の画面例で手順を説明します。

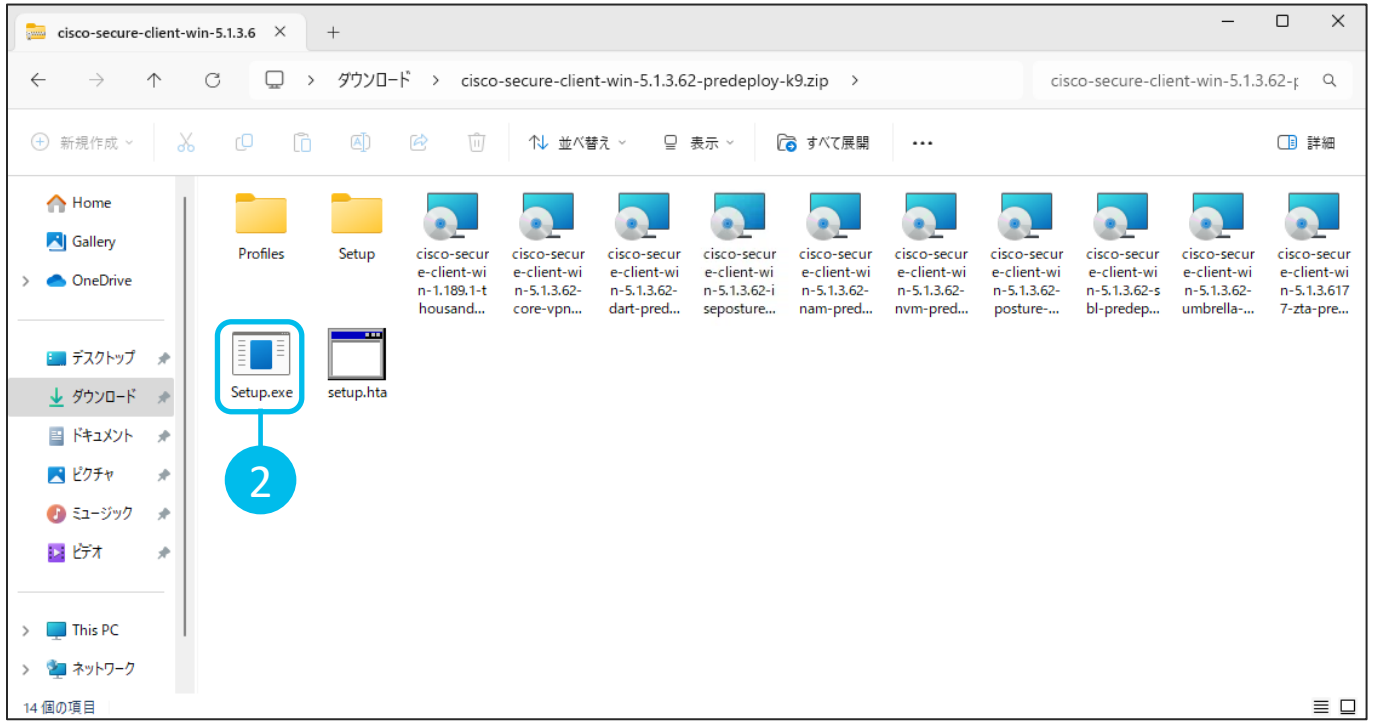


1 インストーラ(圧縮ファイル)を解凍

2-⑦ でダウンロードした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、[**cisco-secure-client-win-5.x.x.xxxx-predeploy-k9**](拡張子なし表示)または[**cisco-secure-client-win-5.x.x.xxxx-predeploy-k9.zip**](拡張子あり表示)です。

※特定のソフトウェアで圧縮ファイルを回答できない場合は、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回答してください。

3. Cisco Secure Clientをインストール



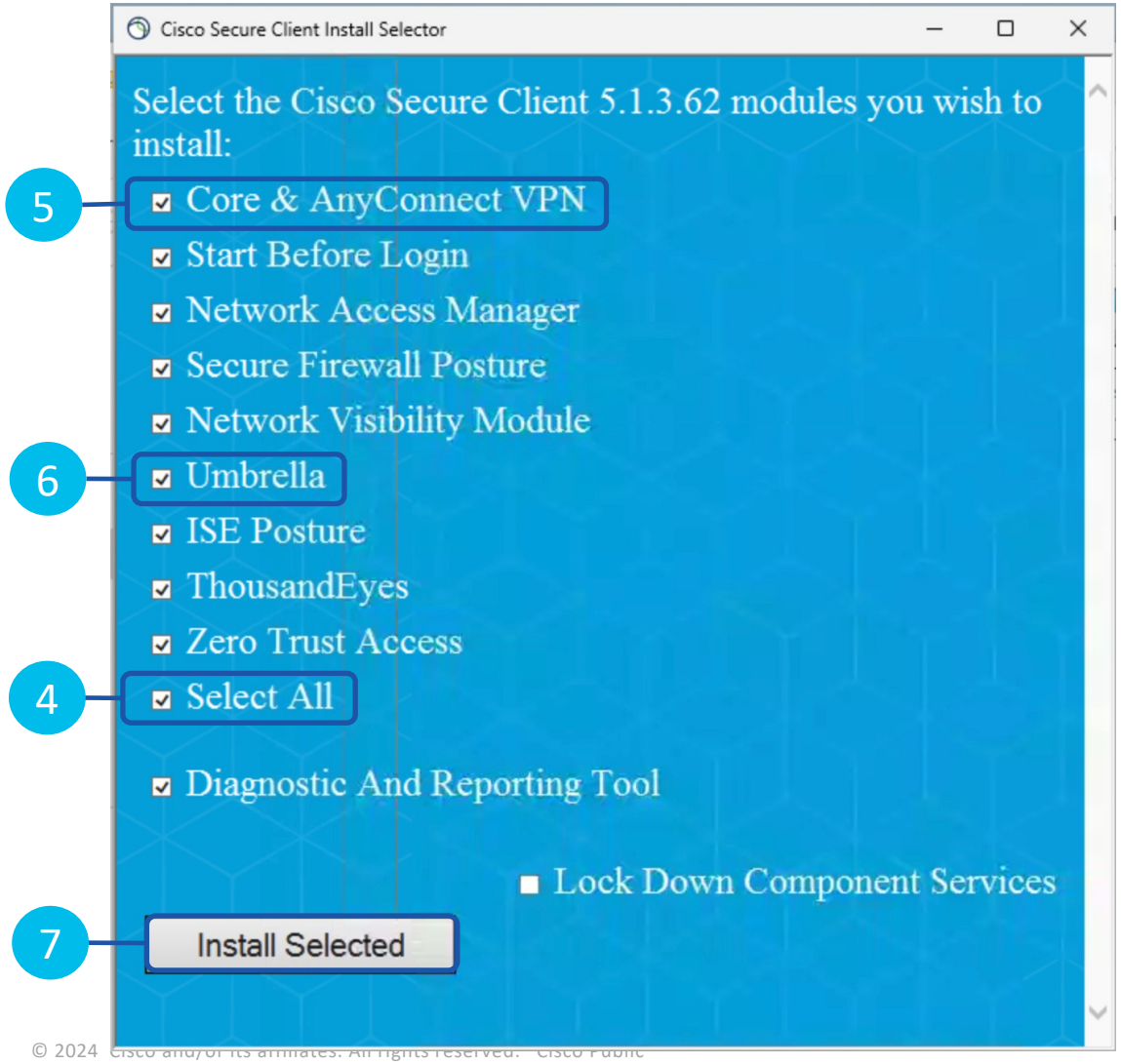
2 インストーラを実行

回答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.exe**](拡張子あり表示)です。[**ユーザアカウント制御**]ダイアログボックスが表示されます。

3 [はい]をクリック

[**はい**]をクリックし、インストーラを実行します。

3. Cisco Secure Clientをインストール



4 **[Select All]をクリックし選択解除**

デフォルトではすべてのインストールオプション(モジュール)が選択されています。[**Select All**]をクリックし、選択を**解除**します。

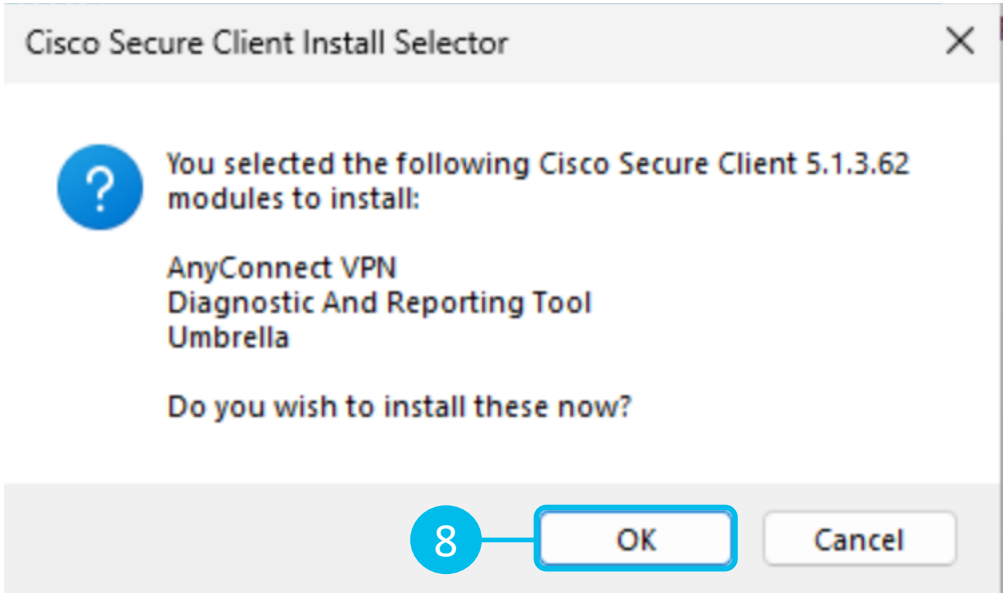
5 **[Core & AnyConnect VPN]をクリック**

6 **[Umbrella]をクリック**

Umbrellaでコンピュータを保護するために必要となる[**Core& AnyConnect VPN**]を選択します。その他のインストールオプションは必要に応じて選択します。

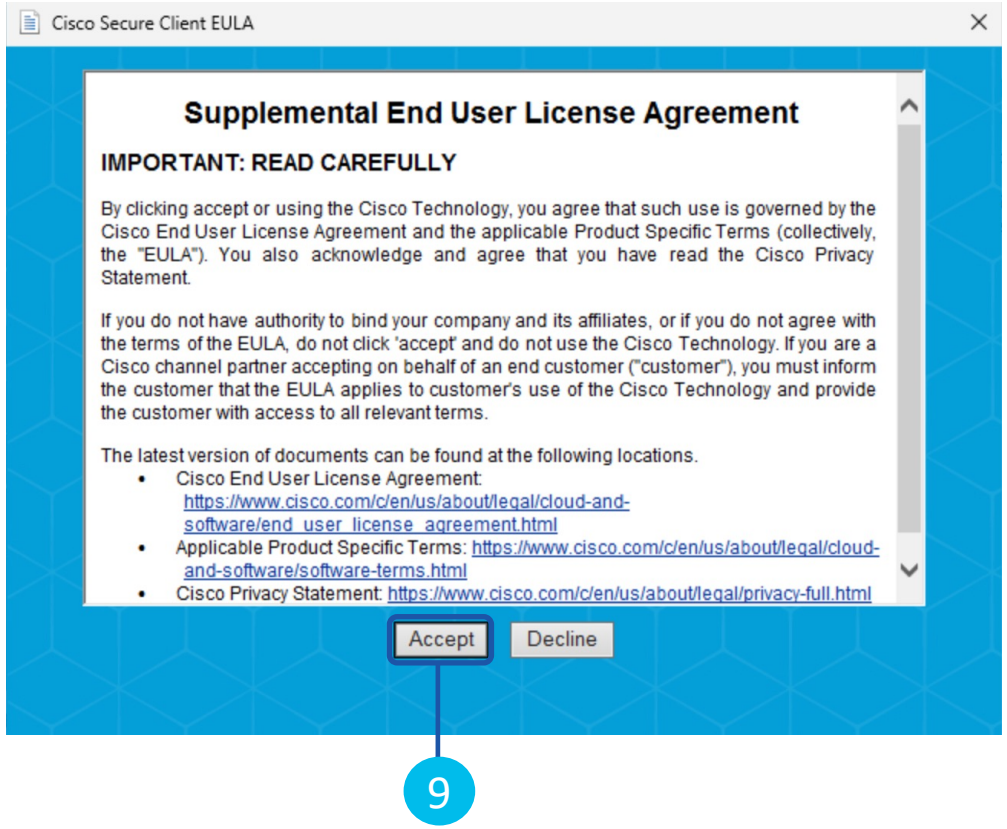
7 **[Install Selected]をクリック。**

3. Cisco Secure Clientをインストール



8 [OK]をクリック

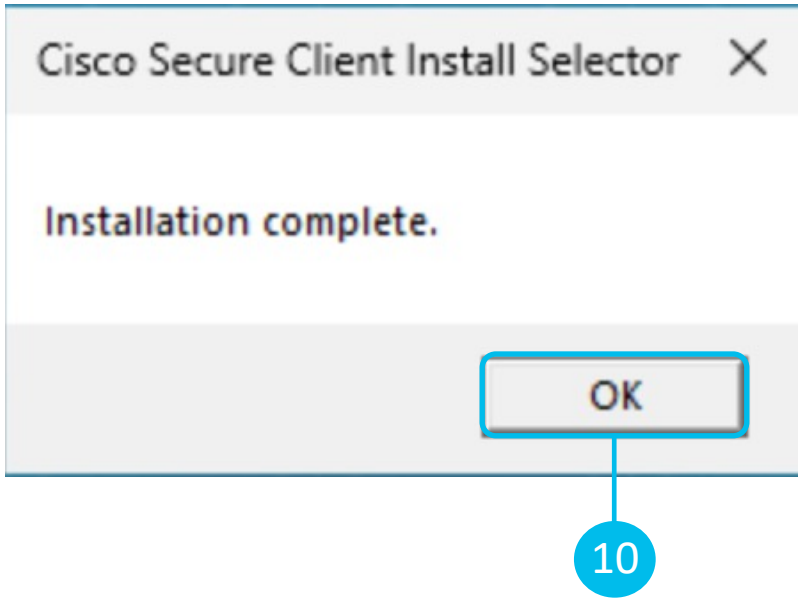
3. Cisco Secure Clientをインストール



9 [Accept]をクリック

[Accept]をクリックと、ダウンロードを開始します。

3. Cisco Secure Clientをインストール



10 [**OK**]をクリック

[**Accept**]をクリックと、ダウンロードを開始します。Cisco Secure Clientのインストールが完了しました。
続けて、Cisco Secure Clientに組み込まれたUmbrellaモジュールを有効化します。

4.Umbrellaモジュールを有効化する

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

4. Umbrellaモジュールを有効化する

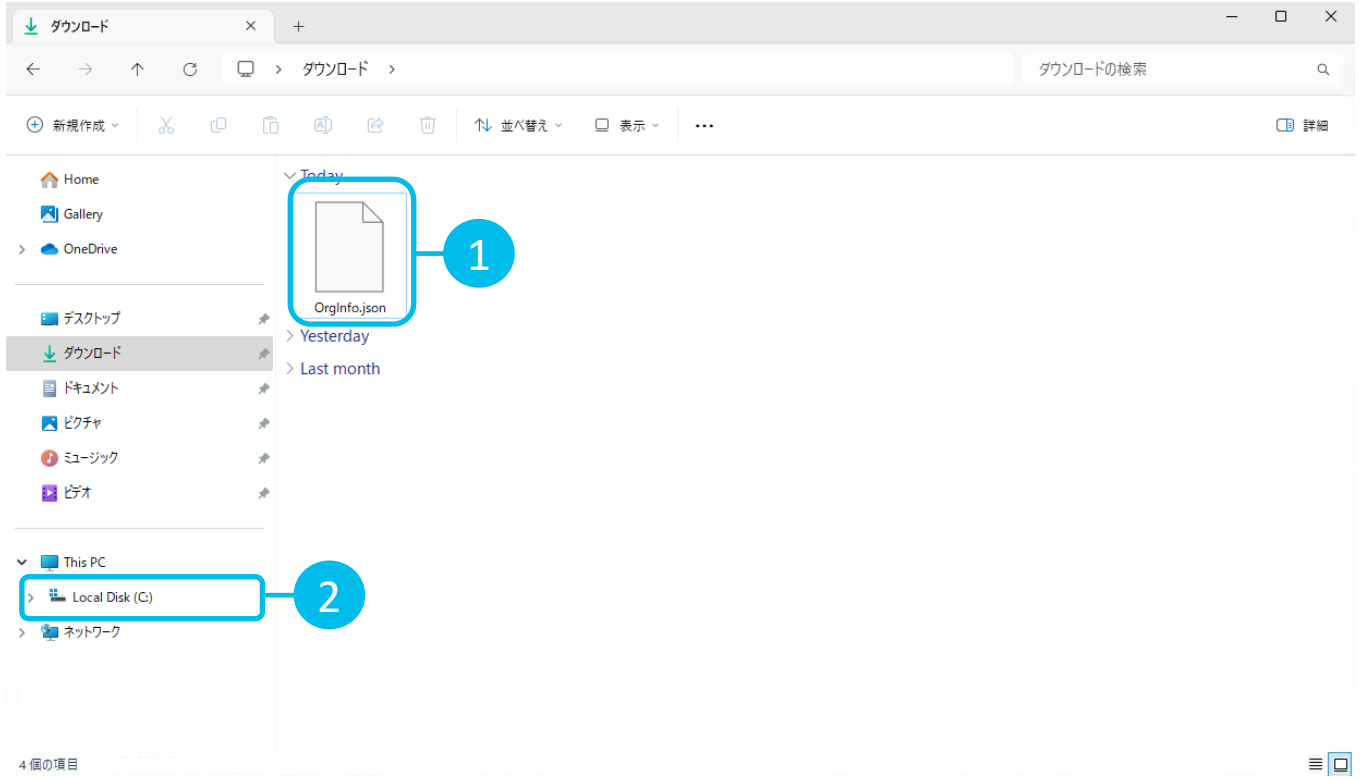
- Cisco Secure Clientに組み込まれたUmbrellaモジュールを有効化し、コンピュータの保護を開始します。
  - ステップ1:Umbrellaモジュールを有効化
  - ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化

4. Umbrellaモジュールを有効化する
ステップ1:Umbrellaモジュールを有効化

- [**2-⑧ モジュールのプロファイルをダウンロード**」でダウンロードしたプロファイルを次のフォルダに配置し、Umbrellaモジュールを有効化します。
  - Windows: C:\ProgramData\Cisco\Cisco Secure Client\Umbrella
  - macOS: /opt/cisco/secureclient/Umbrella/

本ガイドはWindows 11の画面例で手順を説明します。

4. Umbrellaモジュールを有効化する
ステップ1:Umbrellaモジュールを有効化



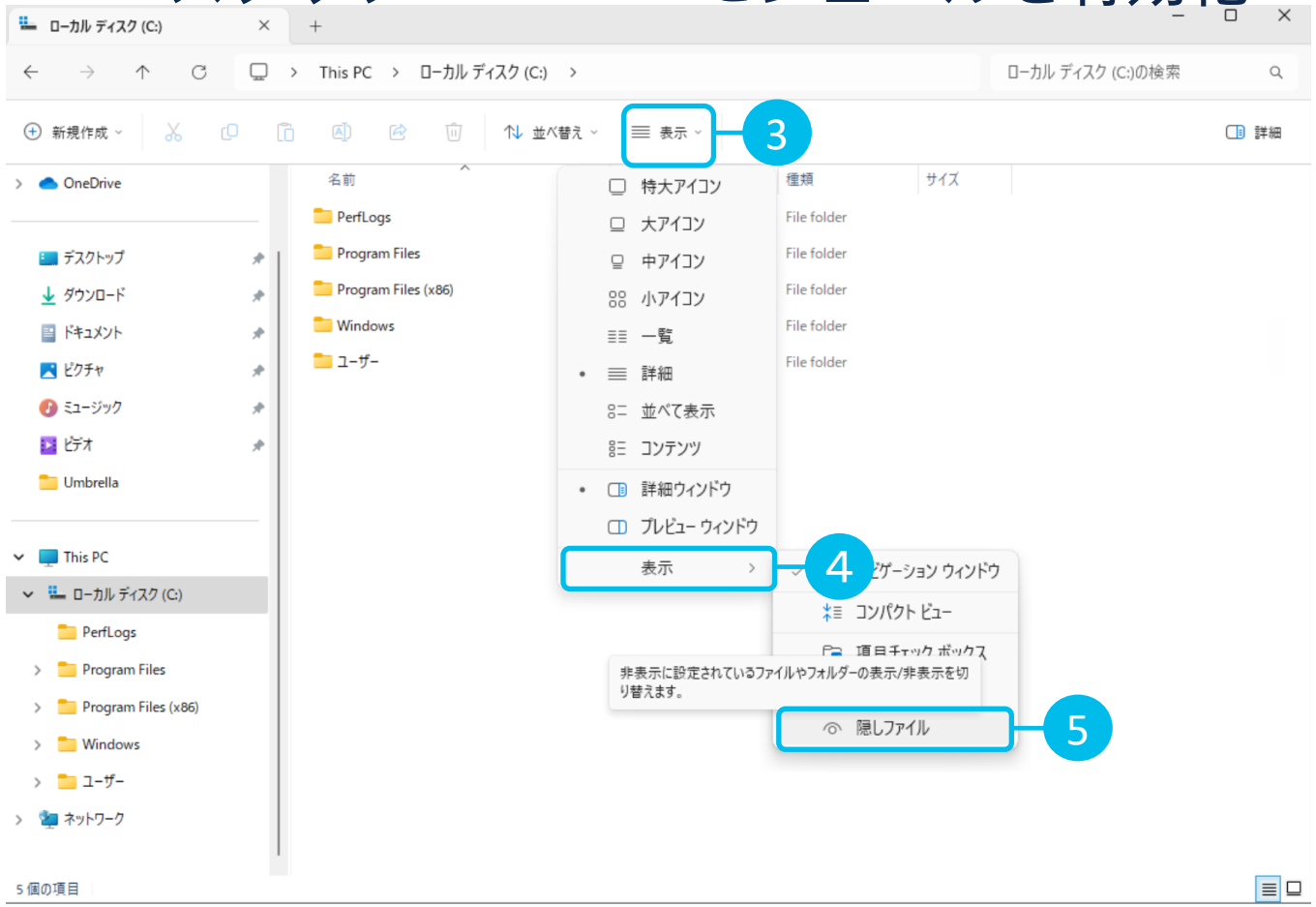
1 プロファイルをコピー

[2–⑧ **モジュールのプロファイルをダウンロード**]でプロファイルを保存した場所(フォルダ)を開き、プロファイルをコピーします。
ファイル名は、[**OrgInfo**](拡張子なし表示)または[**OrgInfo.json**](拡張子あり表示)です。

2 [**ローカルディスク(C:)**]をクリック

4. Umbrellaモジュールを有効化する

ステップ1:Umbrellaモジュールを有効化



3 (必要に応じて)[**表示**]タブをクリック

[**ProgramData**]フォルダが表示されない場合は、隠しファイルを表示する設定に変更します。

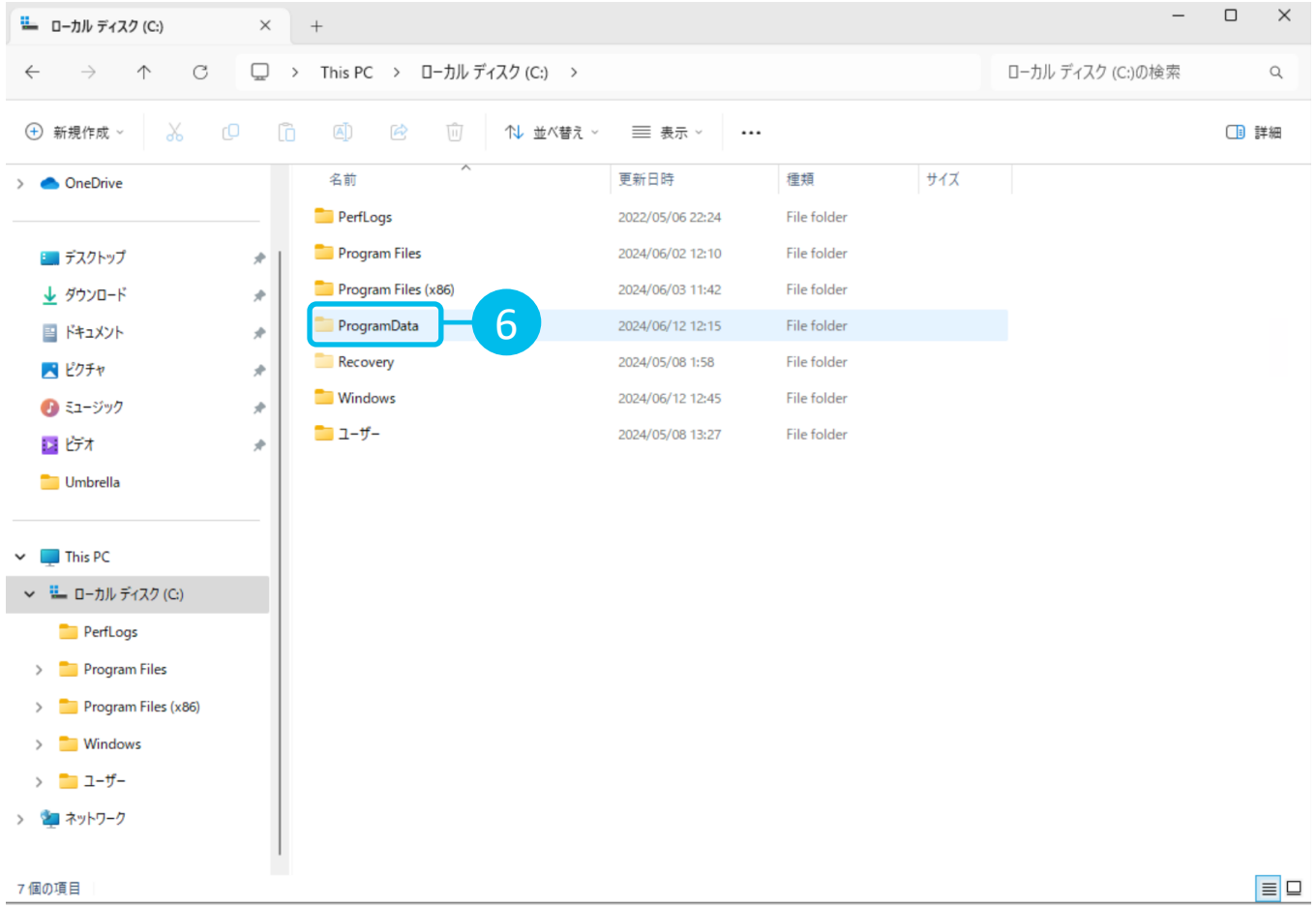
4 (必要に応じて)[**表示**] をクリック

5 (必要に応じて)[**隠しファイル**]をクリック

[**隠しファイル**]をクリックして、隠しファイルを表示する設定に変更します。[**ProgramData**]や、その他のフォルダやファイルが表示されます。

4. Umbrellaモジュールを有効化する

ステップ1:Umbrellaモジュールを有効化

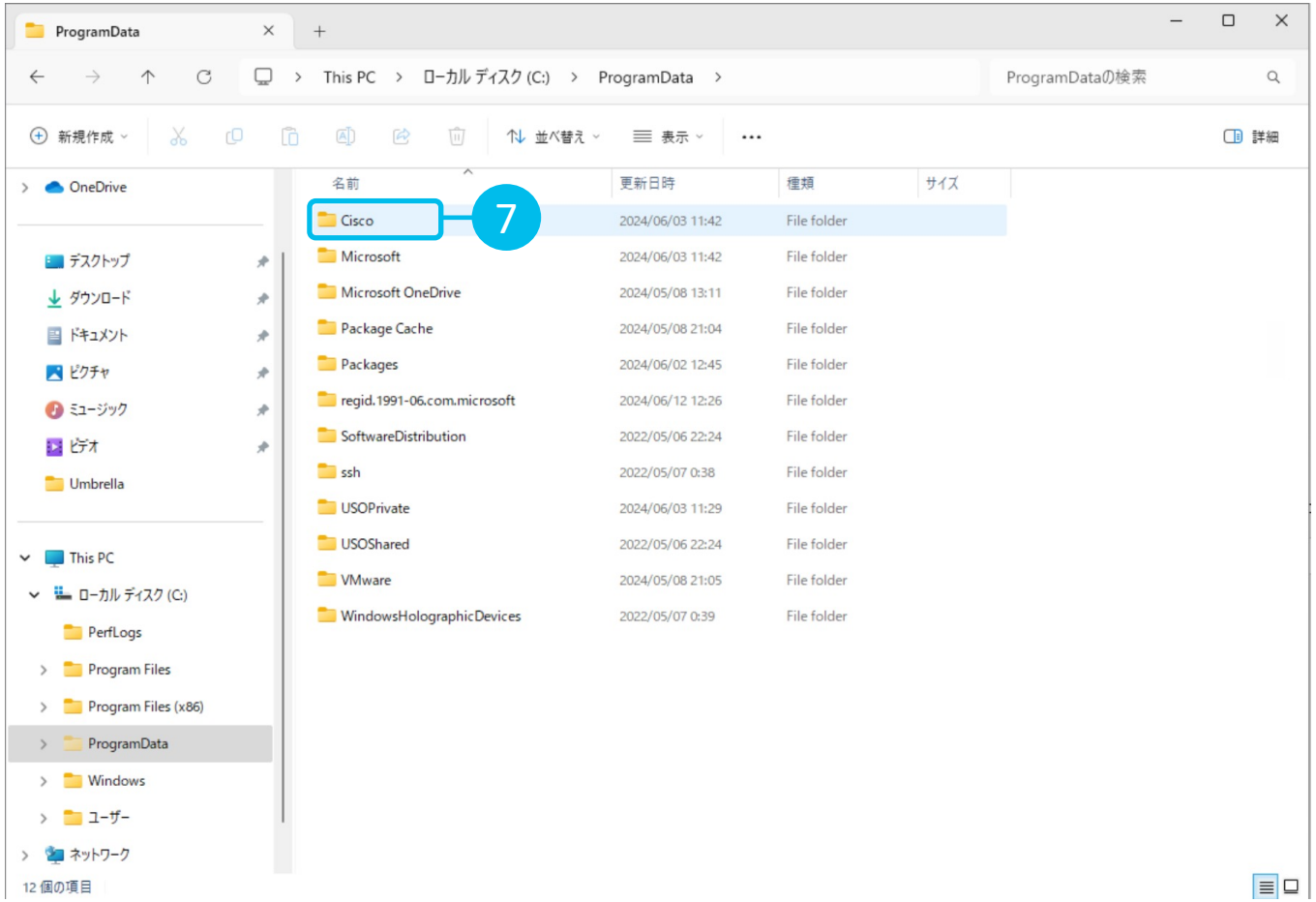


6 **[ProgramData]フォルダをクリック**

[ProgramData]フォルダをクリックして開きます。同様に、目的の**[Umbrella]**フォルダまで各フォルダを開いていきます。

4. Umbrellaモジュールを有効化する

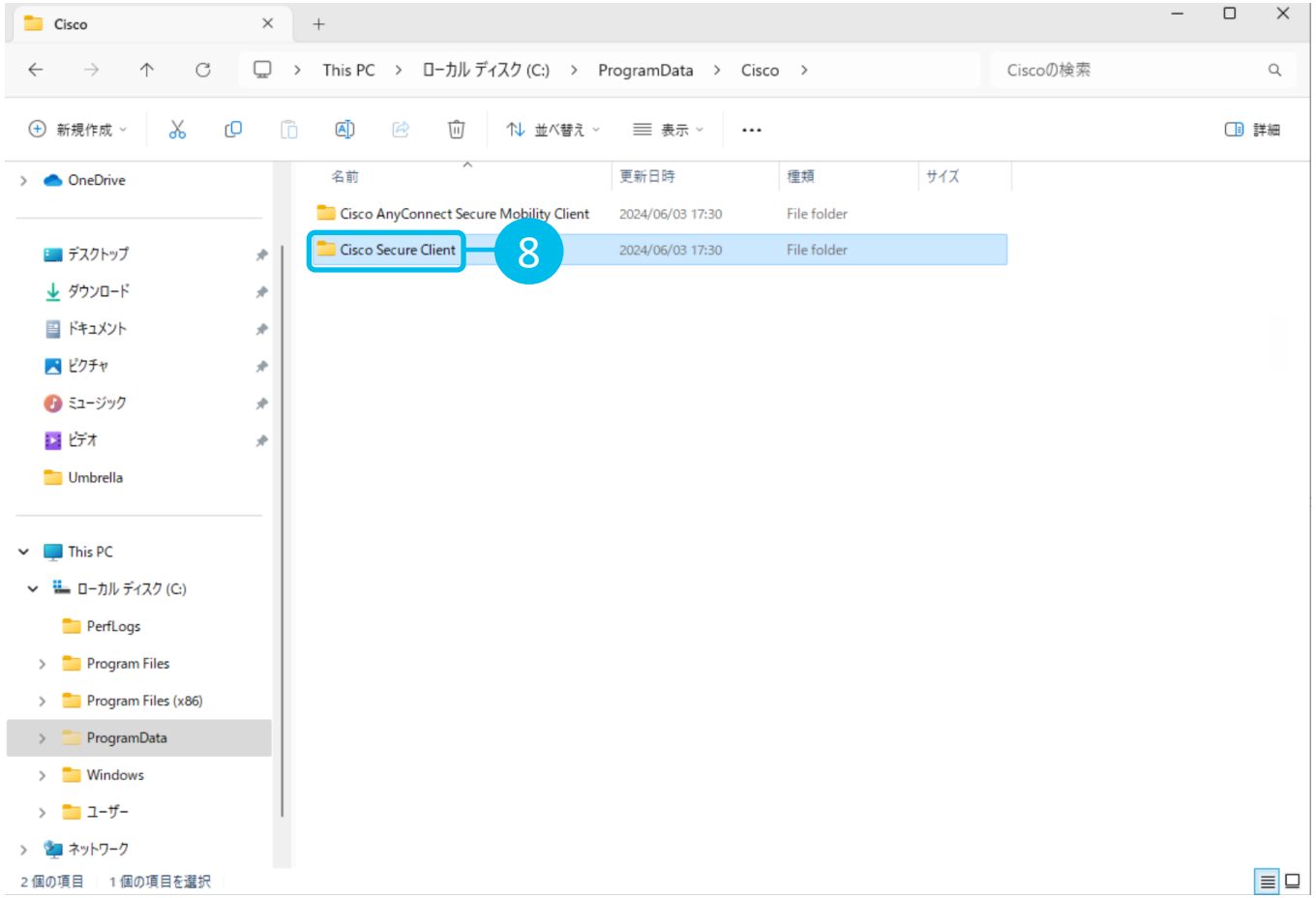
ステップ1:Umbrellaモジュールを有効化



7 [Cisco]フォルダをクリック

4. Umbrellaモジュールを有効化する

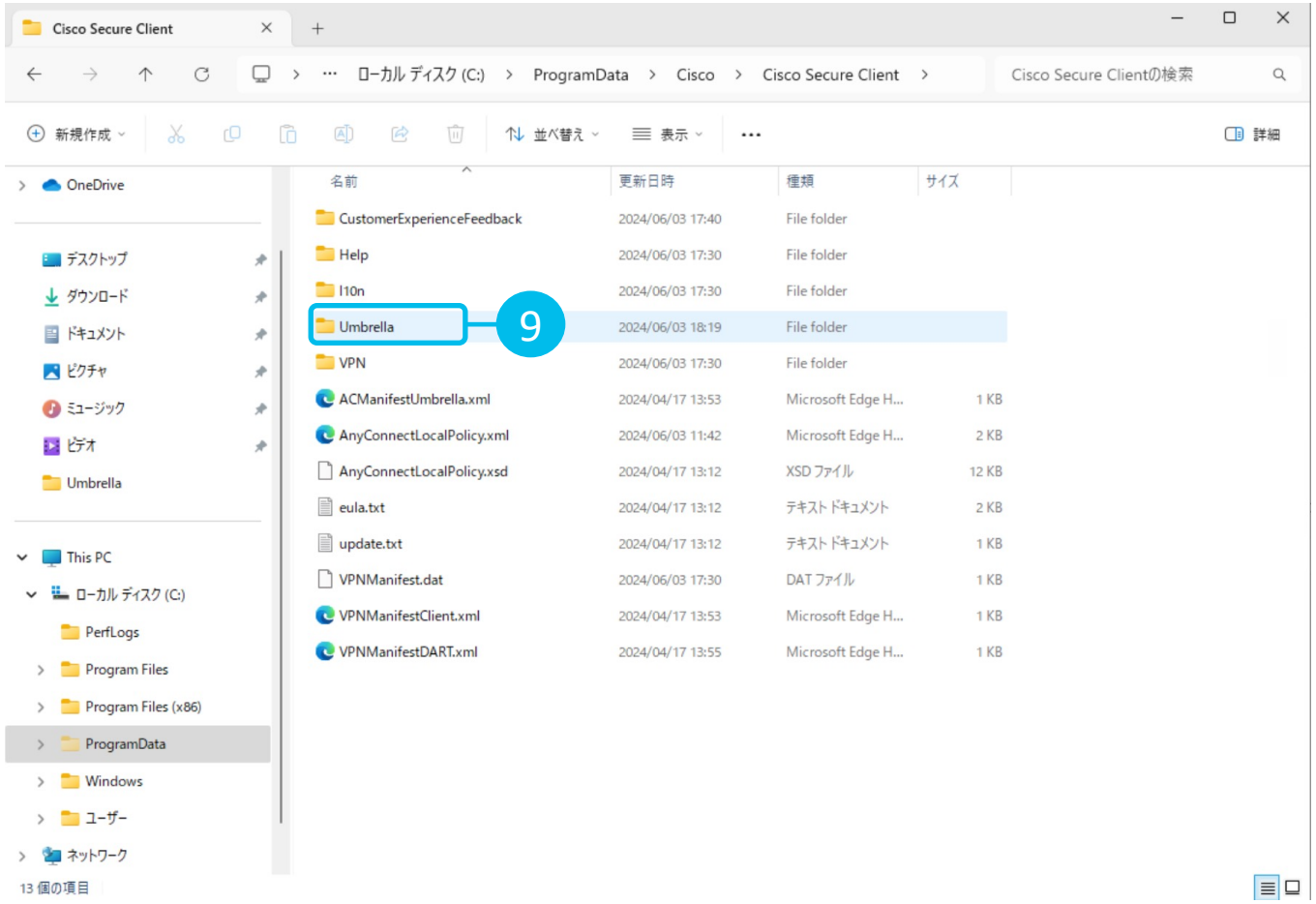
ステップ1:Umbrellaモジュールを有効化



8 [Cisco Secure Client]フォルダをクリック

4. Umbrellaモジュールを有効化する

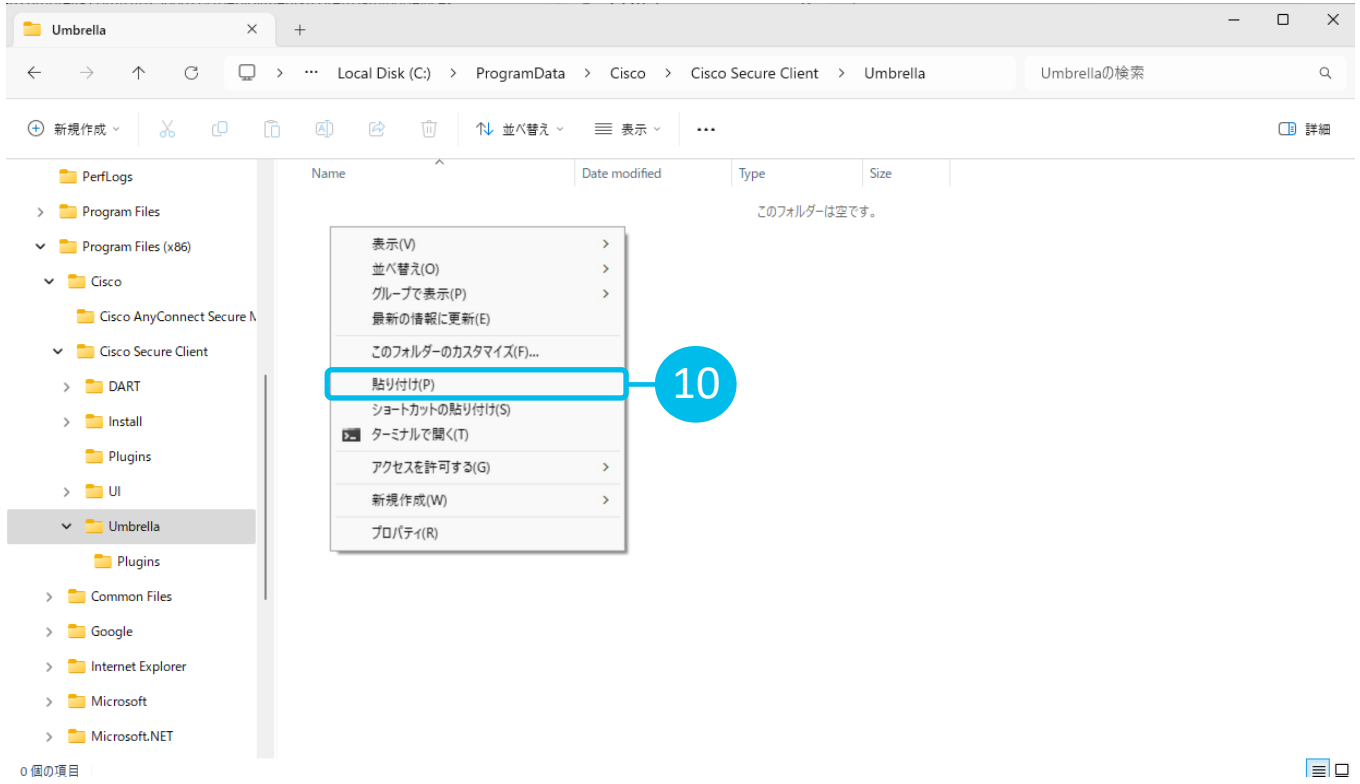
ステップ1:Umbrellaモジュールを有効化



9 [Umbrella]フォルダをクリック

4. Umbrellaモジュールを有効化する

ステップ1:Umbrellaモジュールを有効化



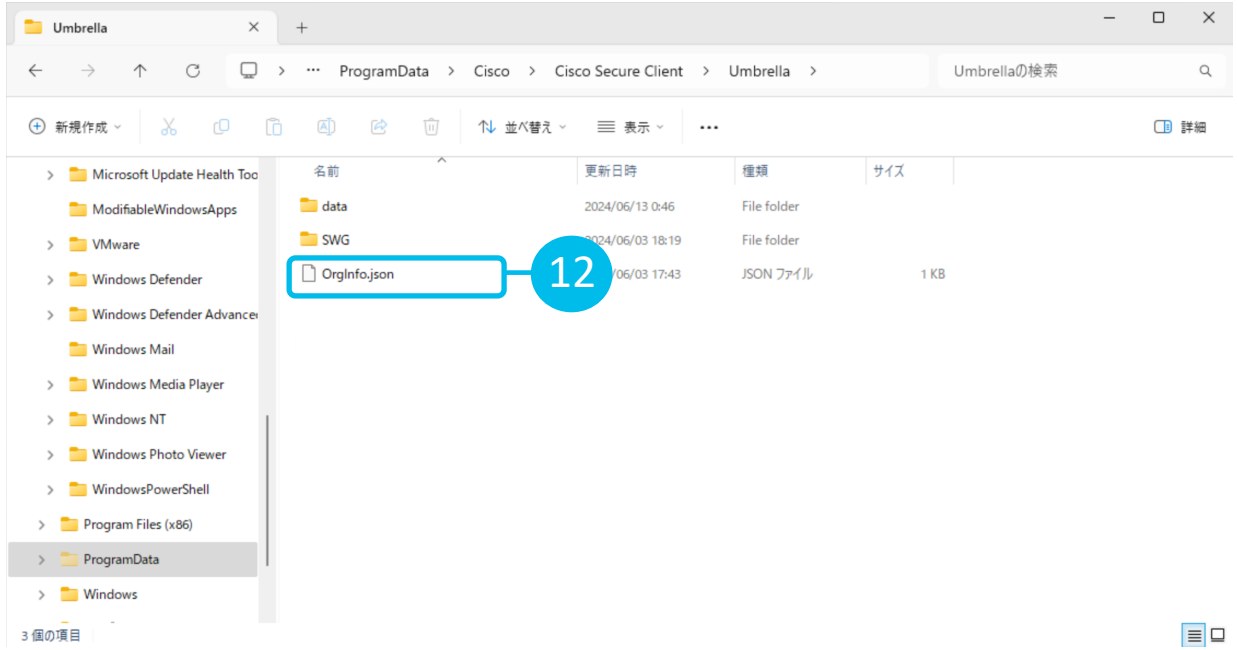
10 4-①でコピーしたプロファイルをペースト

[**Umbrella**]フォルダにプロファイルをペースト(貼り付ける)すると、[**対象のフォルダーへのアクセスは拒否されました**]ダイアログボックスが表示されます。

4. Umbrellaモジュールを有効化する

ステップ1:Umbrellaモジュールを有効化

11 [**続行**]をクリック

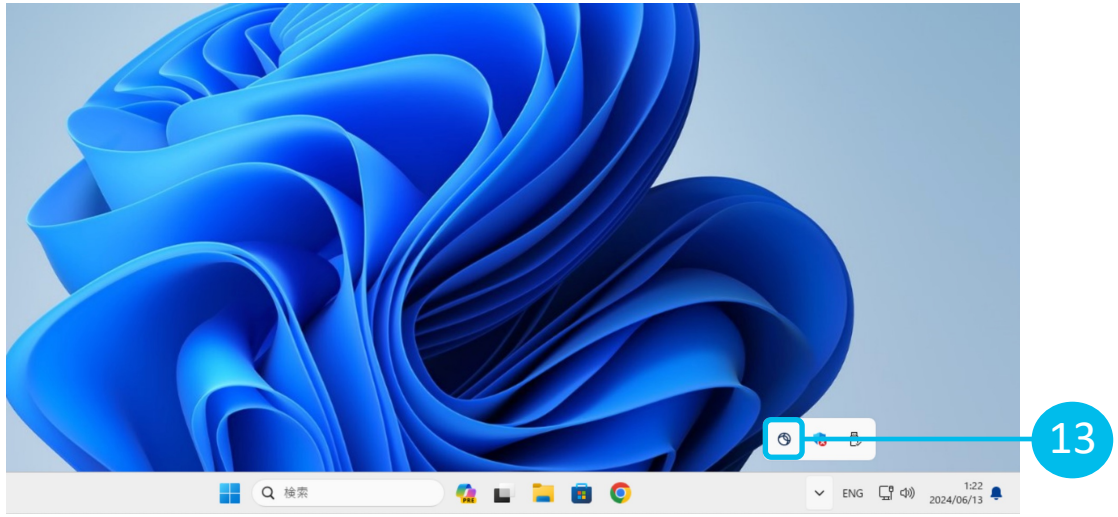


12 プロファイルの配置を確認

[**Umbrella**]フォルダにプロファイルが配置されました。配置が完了すると、自動的に[**data**]フォルダおよび[**SWG**]フォルダが作成されます。

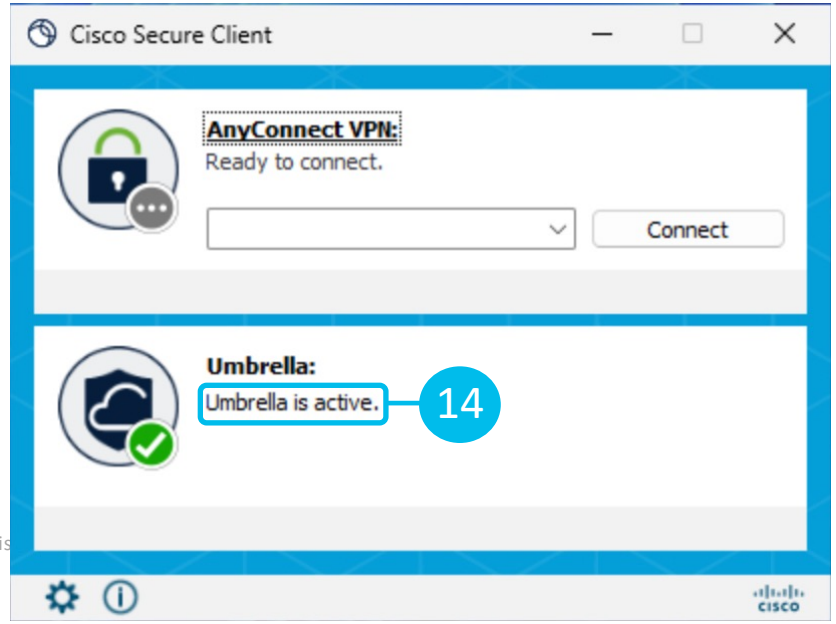
4. Umbrellaモジュールを有効化する

ステップ1:Umbrellaモジュールを有効化



13 タスクトレイのCisco Secure Client[ ]アイコンをクリック

Cisco Secure Clientで、Umbrellaモジュールが有効化されたことを確認します。



14 [**Umbrella is active.**]メッセージを確認

[**Umbrella is active.**]メッセージを確認したら、Umbrellaモジュールの有効化は完了です。

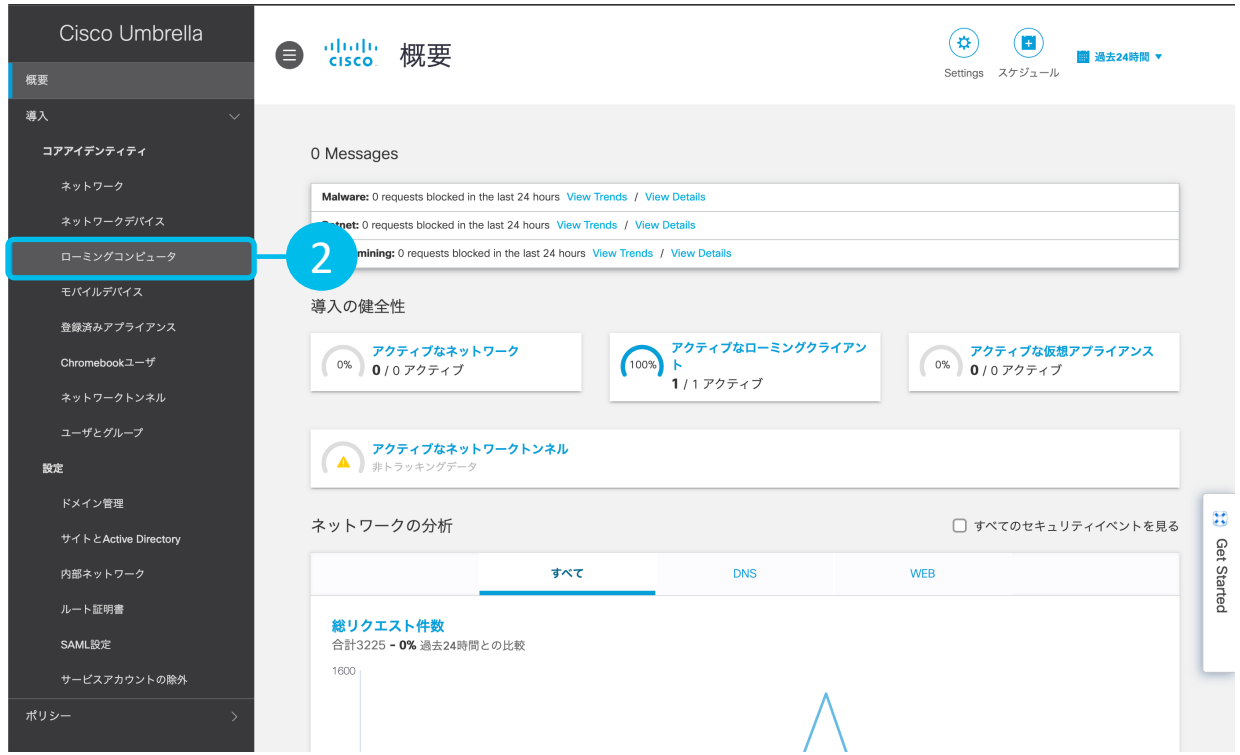
続いて、UmbrellaセキュリティWebゲートウェイ機能を有効化します。

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化

1 [導入] をクリック

ダッシュボードをクリックし、[導入]をクリックします。

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化

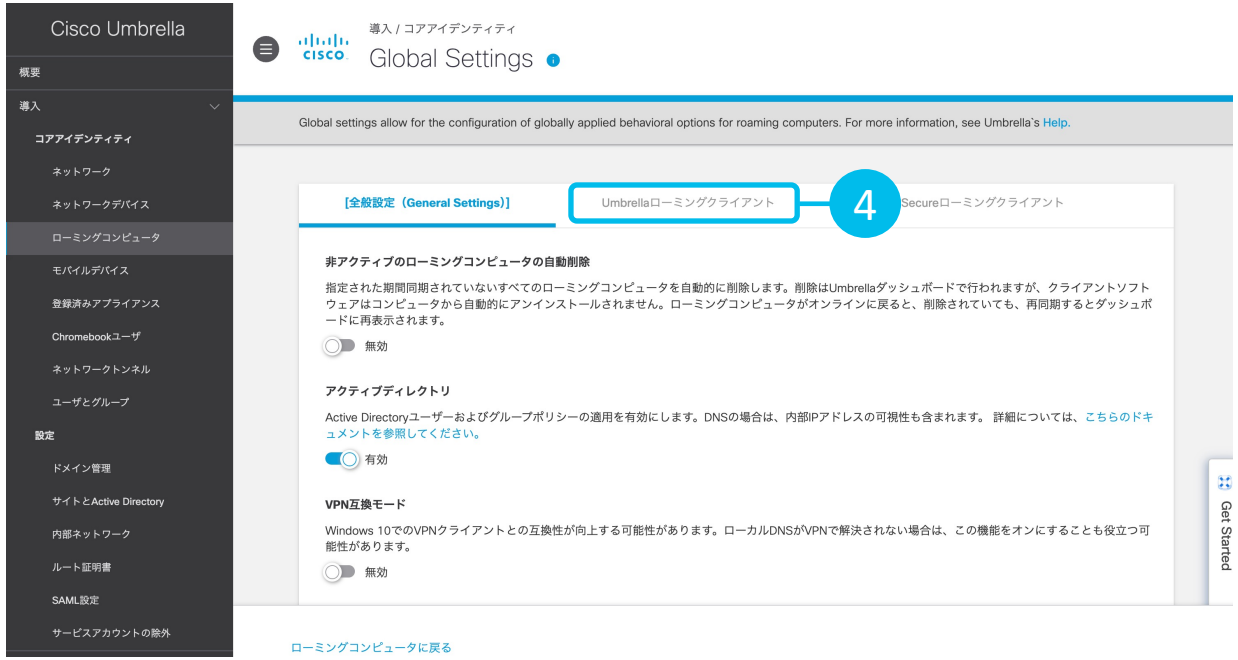


2 [ローミングコンピュータ] をクリック

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化

3 [設定] をクリック

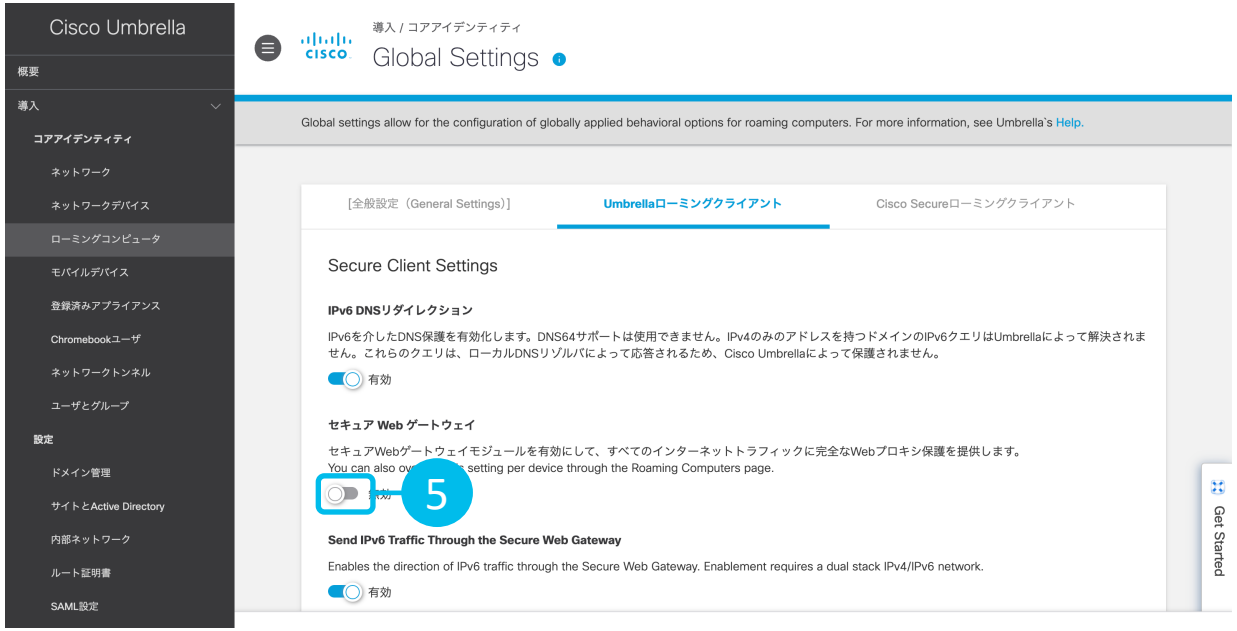
4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化



4 [Umbrellaローミングクライアント] をクリック

注意
言語設定が英語の場合、「Client Settings」を選択してください。

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化

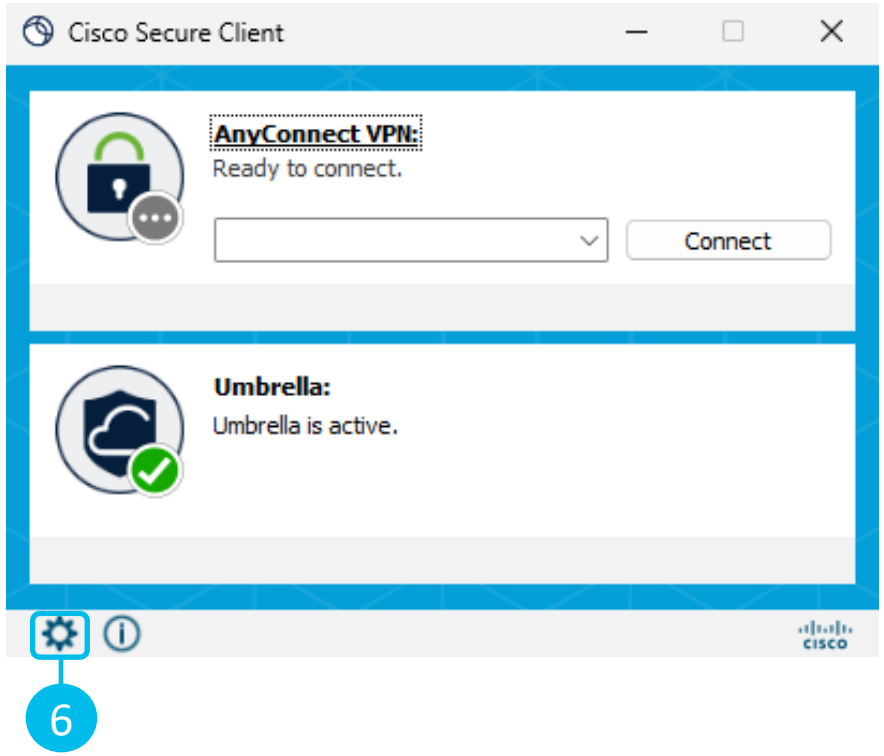


5 **[セキュアWebゲートウェイ] スイッチをクリックしオンにする**

注意

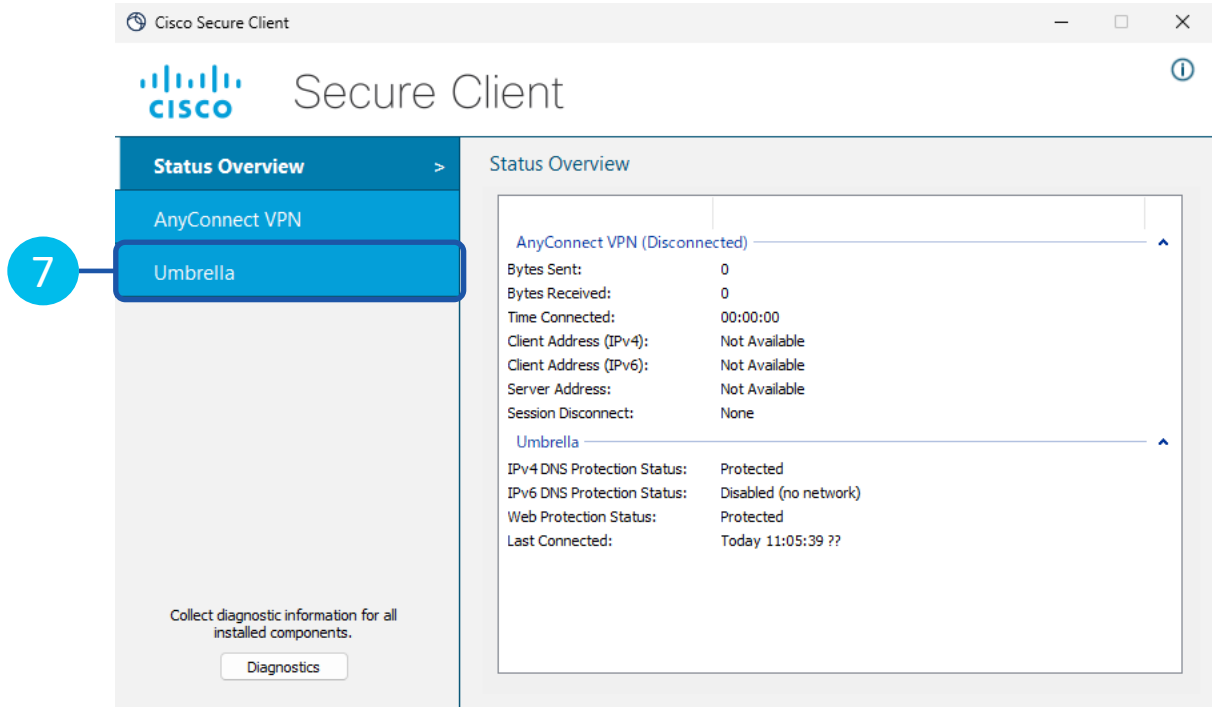
Global Settingsにおける設定変更の反映は、最大**60分**かかる場合があります。

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化



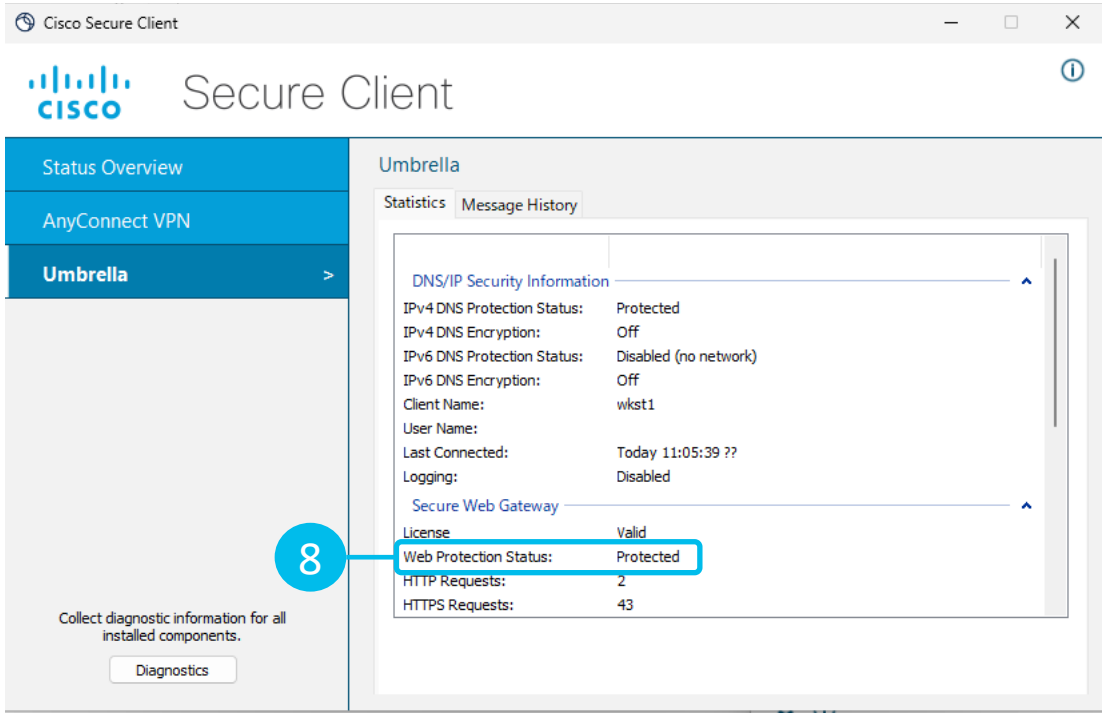
6 詳細ウィンドウ[⚙]アイコンをクリック

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化



7 [**Umbrella**]をクリック

4. Umbrellaモジュールを有効化する
ステップ2:Umbrella セキュアWebゲートウェイ機能を有効化



8

[Web Protection Status]が[Protected]であることを確認

[Secure Web Gateway]項目に表示される**[Web Protection Status]**が**[Protected]**であることを確認したら、Umbrella セキュアWeb ゲートウェイ機能の有効化は完了です。

続いて、ルート証明書をインストールします。

5.ルート証明書をインストールする

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

5. ルート証明書をインストールする

- Cisco UmbrellaがWebサイト向けのHTTPSトラフィックをプロキシし複合する必要がある場合では、ルート証明書が必要となります。
- 本ガイドでは、Google Chrome やMicrosoft Edge等で使用するWindows の証明書ストアに、シスコUmbrellaの「**ルート証明書**」を手動※でインストールする画面例を紹介します。

※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は、オンラインドキュメントを参照ください。
https://docs.umbrella.com/umbrella-user-guide/docs/install-the-cisco-umbrella-root-certificate#automatically-install-the-cisco-umbrella-root-certificate-for-an-active-directory-network

5. ルート証明書をインストールする

1 [導入]をクリック

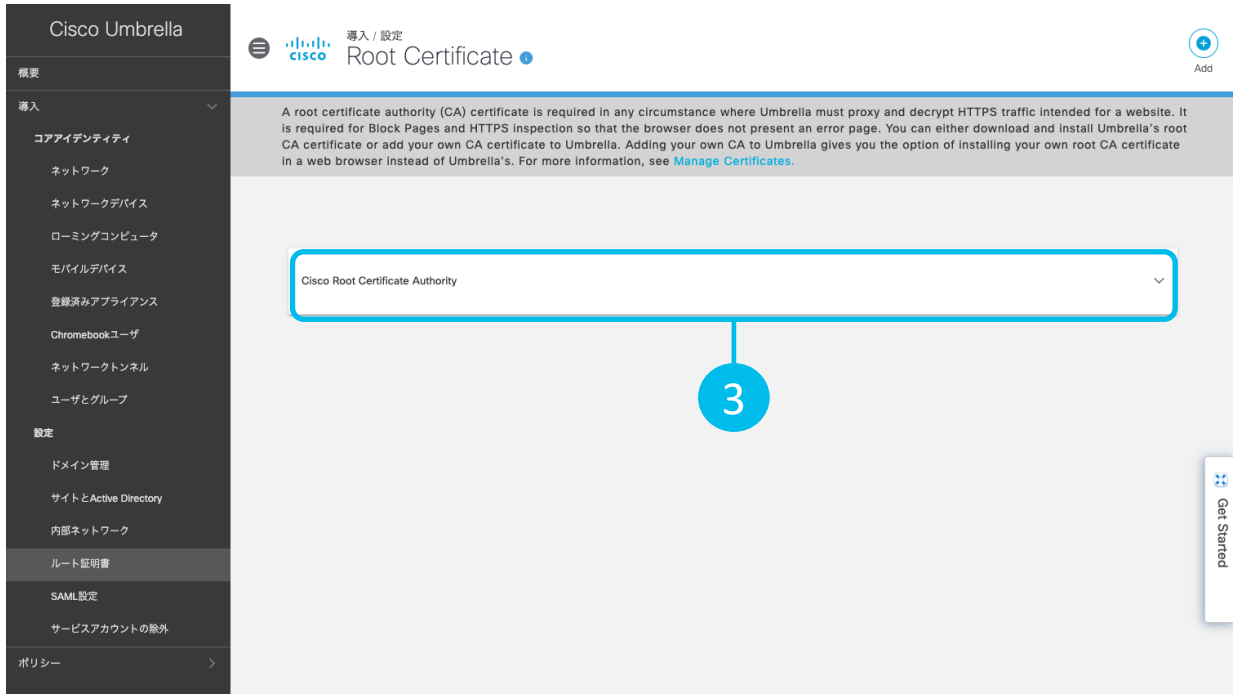
ダッシュボードにアクセスし、[導入]をクリック

目次に戻る

5. ルート証明書をインストールする

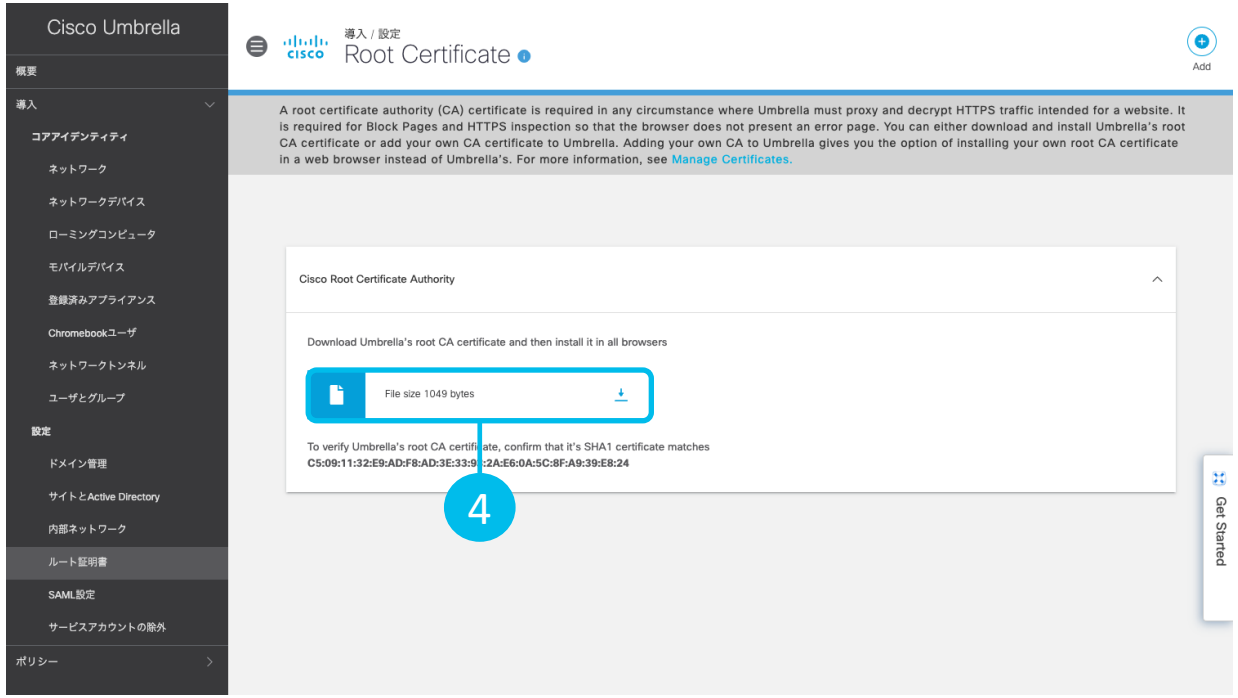
2 [ルート証明書]をクリック

5. ルート証明書をインストールする



3 **[Cisco Root Certificate Authority]** をクリック

5. ルート証明書をインストールする

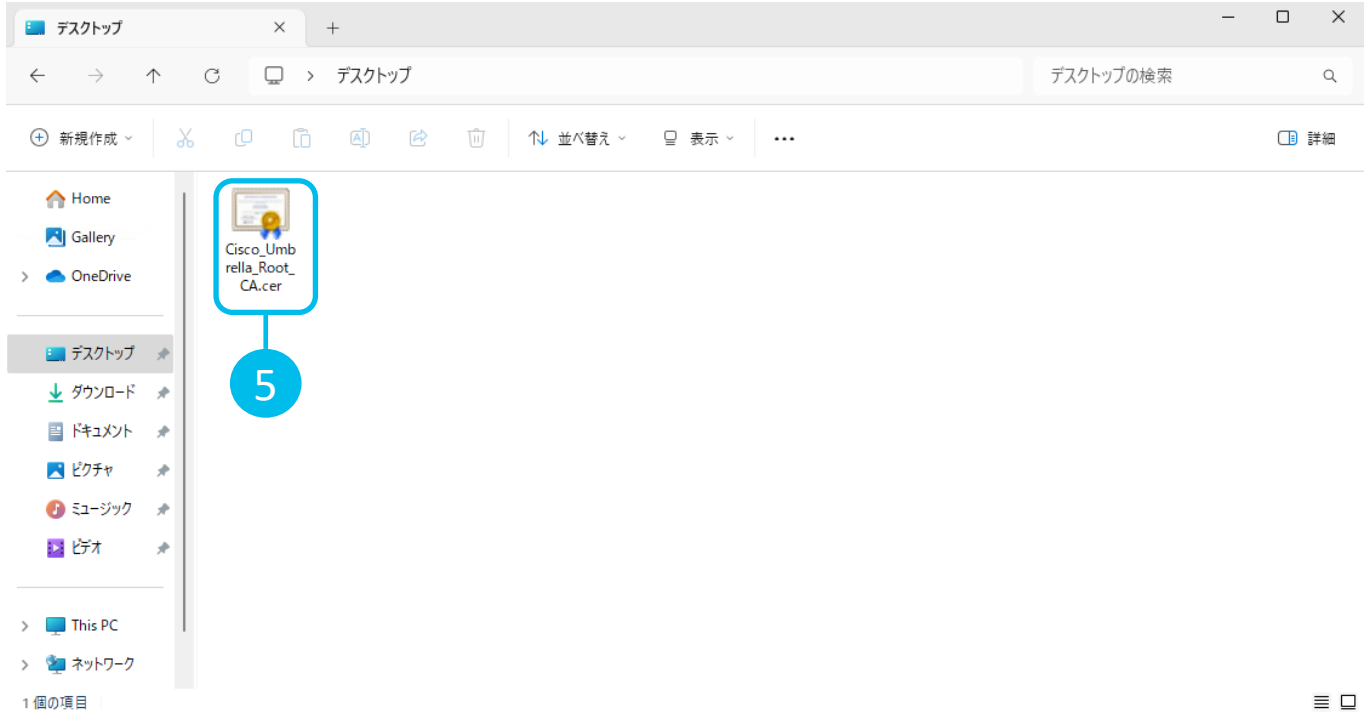


4 [ ]アイコンをクリックし、ルート証明書をダウンロード及び任意の場所に保存

「Cisco_Umbrella_Root_CA.cerはデバイスに問題を起こす可能性があります。このまま保存しますか?」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]**をクリックし続行してください。

目次に戻る

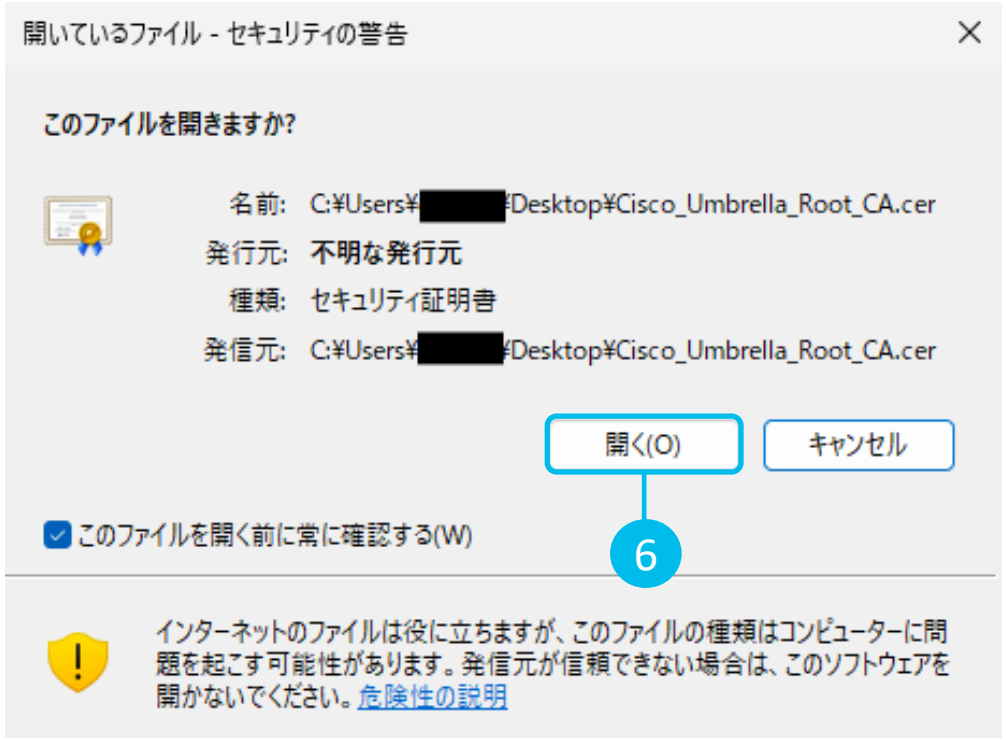
5. ルート証明書をインストールする



5 ルート証明書をクリック

5-④でルート証明書を保存した場所(フォルダ)を開き、ルート証明書をクリックします。ファイル名は、[**Cisco Umbrella_Root_CA**](拡張子なし表示)または[**Cisco_Umbrella_root_CA.cer**](拡張子あり表示)です。
[**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。

5. ルート証明書をインストールする



6 [開く]をクリック

5. ルート証明書をインストールする

7 [証明書のインストール]をクリック

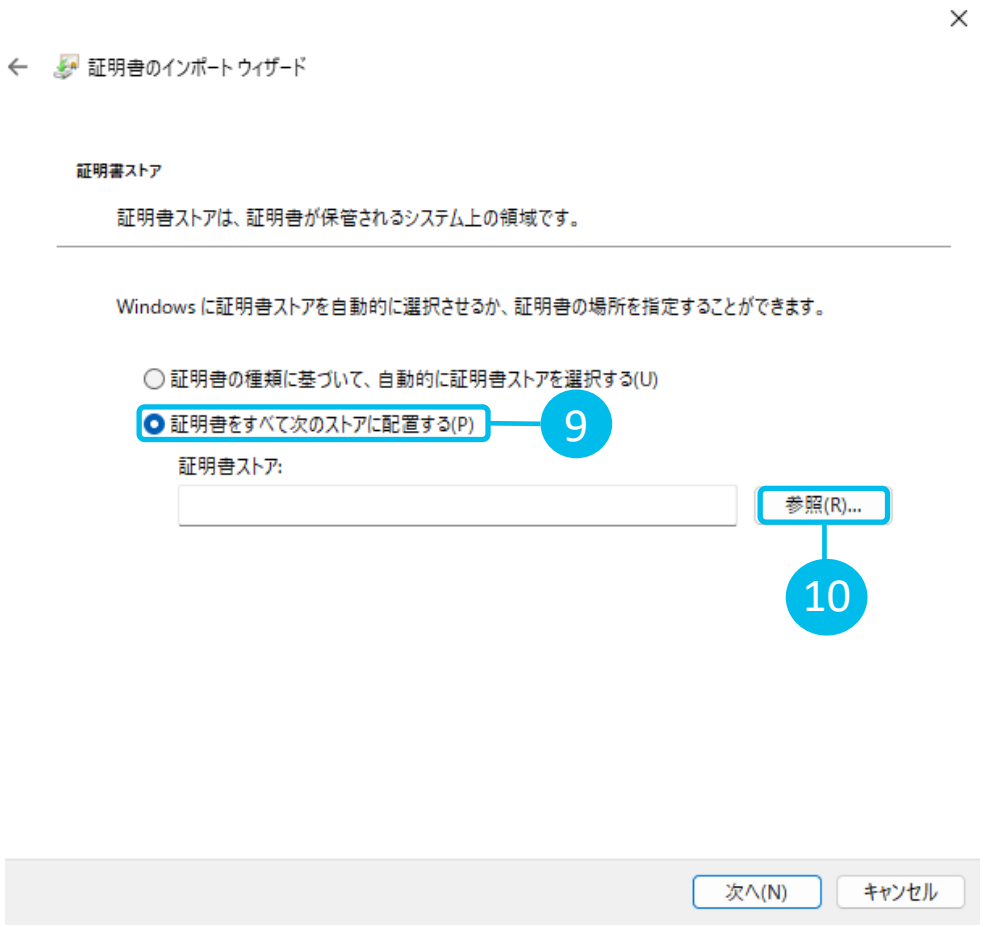
[証明書のインポート ウィザード]が表示されます。

5. ルート証明書をインストールする

8 [次へ]をクリック

デフォルトでは[**現在のユーザー**]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。

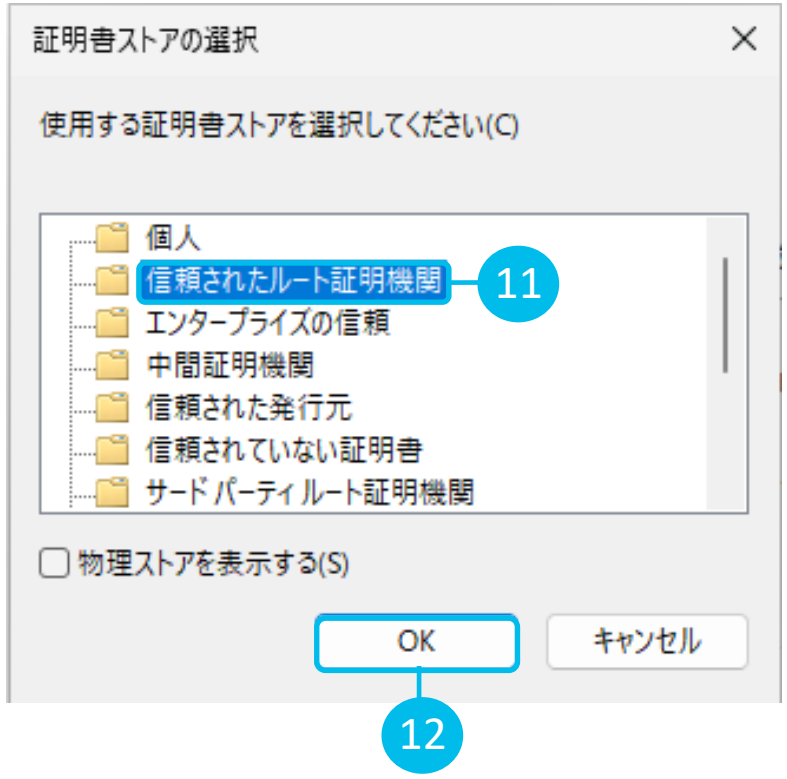
5. ルート証明書をインストールする



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

5. ルート証明書をインストールする



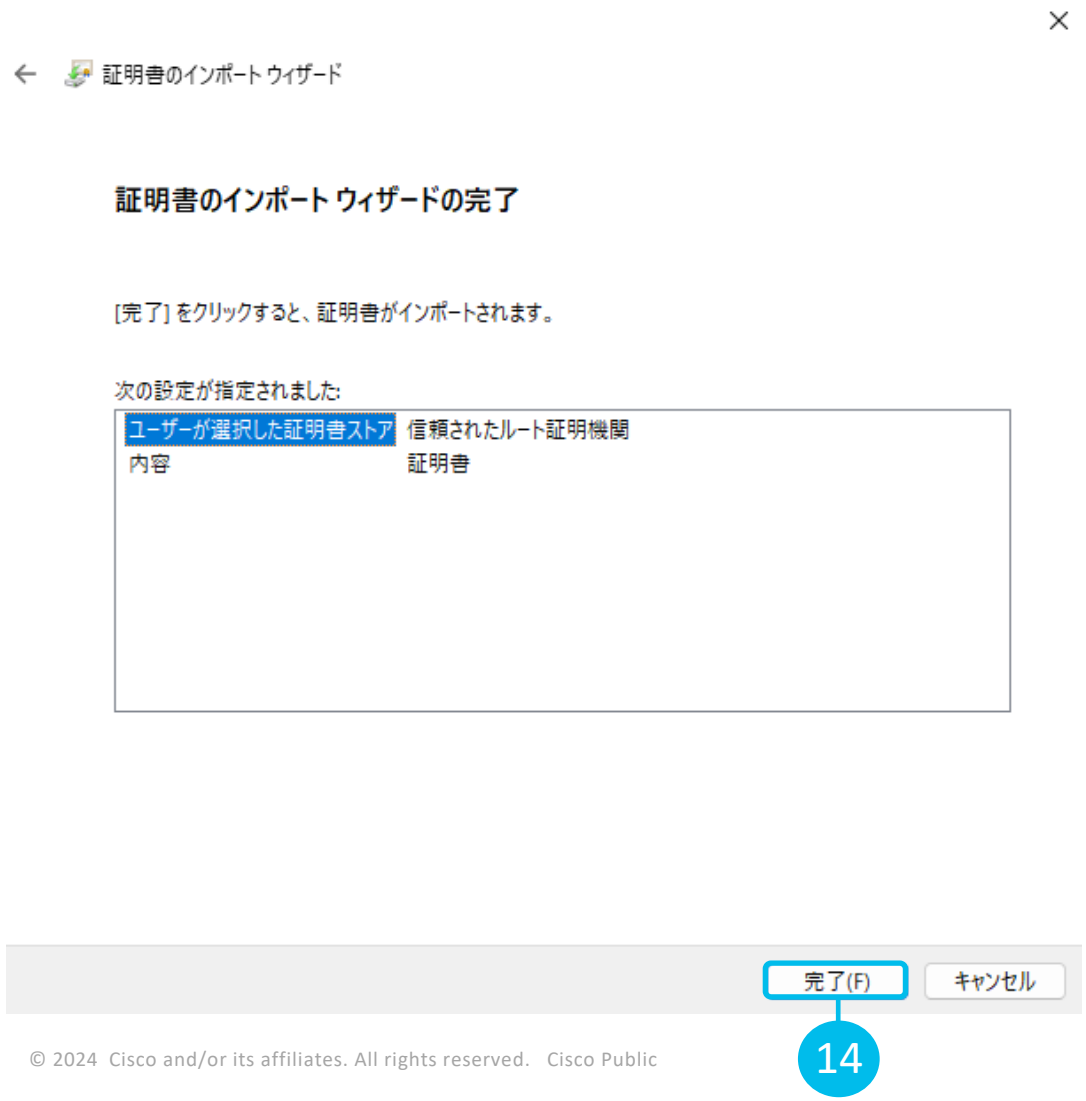
11 [信頼されたルート証明機関]をクリック

12 [OK]をクリック

5. ルート証明書をインストールする

13 [次へ]をクリック

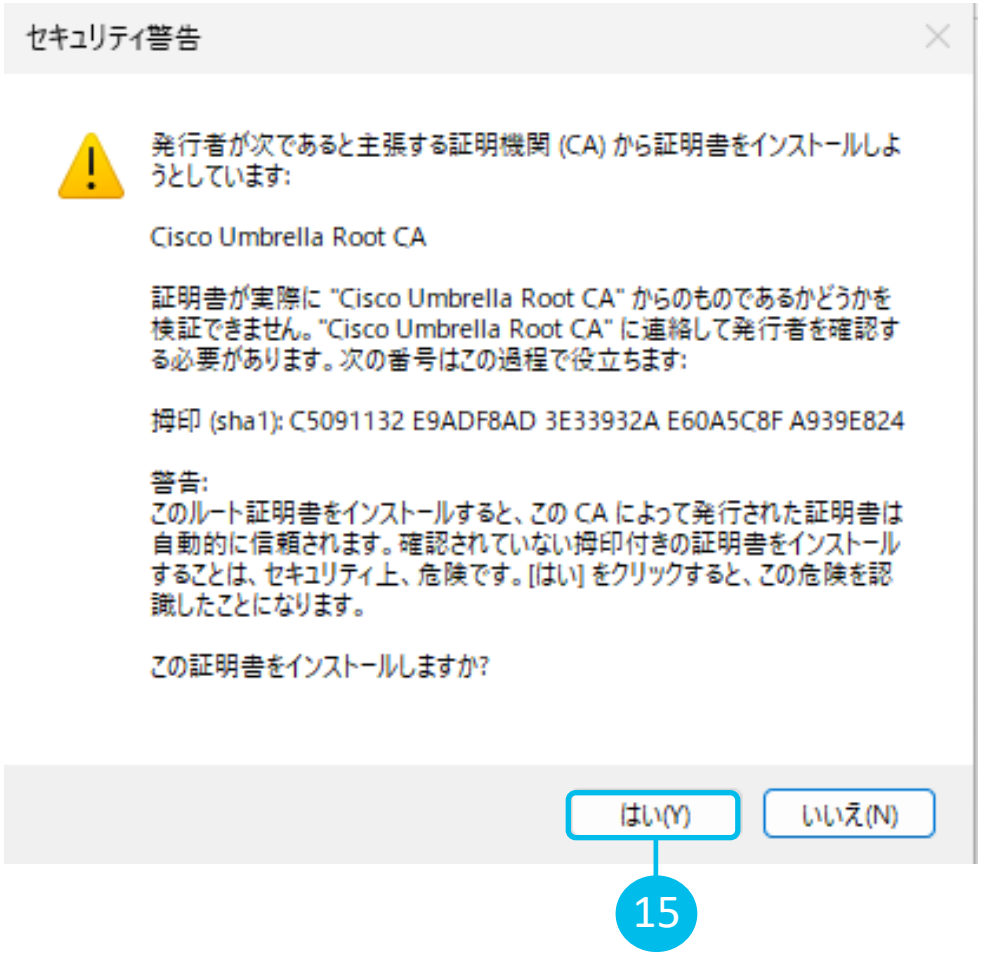
5. ルート証明書をインストールする



14 [完了]をクリック

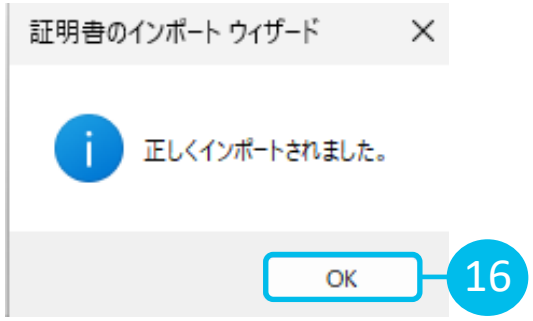
[セキュリティ警告]のダイアログボックスが表示されます。

5. ルート証明書をインストールする



15 [はい]をクリック

5. ルート証明書をインストールする



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

ルート証明書のインストールが完了しました。

5. ルート証明書をインストールする

- **Cisco Secure Client**のインストール、**Umbrella**モジュールの有効化およびルート証明書のインストールが完了したら、次のURLをクリックし、テストサイト※にアクセスしてください。https://malware.opendns.com
  - 正常に動作している場合は、以下のような「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。

※その他の動作確認サイトは、オンラインドキュメントを参照ください。
https://docs.umbrella.com/umbrella-user-guide/docs/test-your-destinations

6.ポリシーを設定する

1. ダッシュボードにログインする P7
2. プロファイルとインストーラをダウンロードする P15
3. Cisco Secure Clientをインストールする P24
4. Umbrellaモジュールを有効にする P31
   - Umbrellaモジュールを有効化
   - Umbrella セキュアWebゲートウェイ機能を有効化
5. ルート証明書をインストールする P51
6. ポリシーを設定する P68
   - DNSポリシー
   - Webポリシー

6. 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設定**ができます。たとえば、次のような設定が可能です。
  - 「マルウェアをブロック」「フィッシング攻撃をブロック」など、**脅威のカテゴリに応じた設定**
  - 「業務に関係がないWebコンテンツをブロック」「有害なWebコンテンツをブロック」など、**Webコンテンツのカテゴリに応じた設定**（コンテンツフィルタリング）

6. ポリシーを設定する

- Cisco Umbrella セキュラインターネットゲートウェイ(SIG)パッケージでは、このようなポリシーを次の**2段階で適用**することができます。
  - **DNSポリシー**:「umbrella.cisco.com」のような**ドメインベース**
  - **Webポリシー**: 「umbrella.cisco.com/products」のような**URLベース**

  たとえば、DNSポリシーによって「umbrella.cisco.com」へのアクセス要求が許可されても、Webポリシーによって「umbrella.cisco.com/products」へのアクセス要求はブロックされるような、きめ細やかな設定が可能になります。

6. ポリシーを設定する

- Cisco Secure Clientをインストール及びUmbrellaモジュールを有効化したコンピュータ(ローミングコンピュータ)には、**デフォルト**では(文字どおりの)「**Default Policy**」および「**Default Web Policy**」が適用されます。これらのポリシーの**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、フィッシング攻撃などをブロックします。
  - デフォルトポリシーを編集することで、たとえば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。
  - デフォルトポリシーはすべてのローミングコンピュータに適用されるため、端末ごとにポリシーを分けたい場合、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でプライバシーに配慮したポリシーとして、セキュリティに関係があるアクセス要求のみ記録およびレポートする設定で、ポリシーを追加する手順を紹介します。

6. ポリシーを設定する
DNSポリシー

- Cisco Umbrellaダッシュボードにアクセスし、**DNSポリシー**を追加します。

1

1 [ポリシー]をクリック

6. ポリシーを設定する
DNSポリシー

2 [DNSポリシー]をクリック

6. ポリシーを設定する
DNSポリシー

3 [追加]をクリック

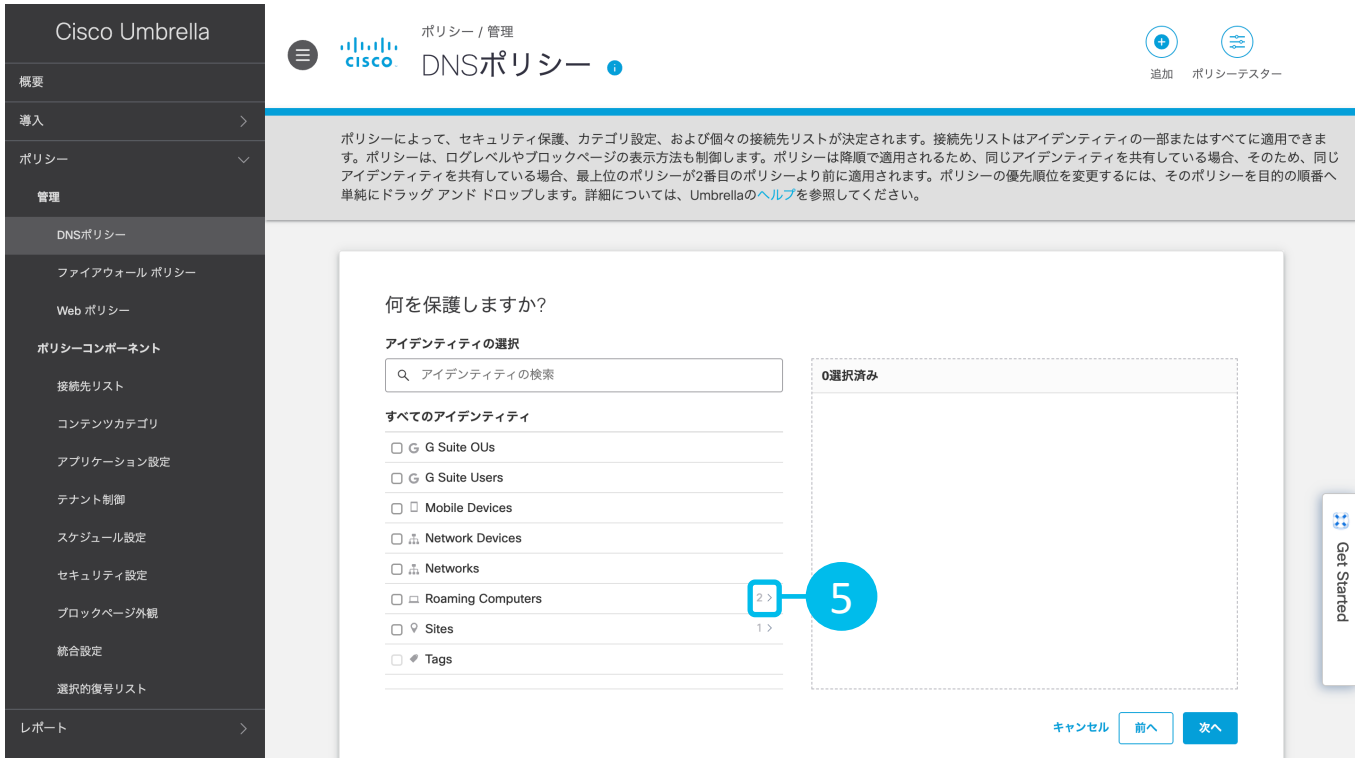
※**Default Policy**は、その他のルールセットに適用されないIDに適用するポリシーとなります。管理外・想定していないようなデバイス/ユーザがインターネットにアクセスしようとした場合に強制するポリシーとなります。そのため**Default Policy**は最も制限の厳しいルールセットとし、**Default Policy**からボトムアップ方式のルールセットの構築することが推奨です。詳細はオンラインドキュメントを参照ください。
https://docs.umbrella.com/umbrella-user-guide/docs/best-practices-for-dns-policies

6. ポリシーを設定する
DNSポリシー

4 [次へ]をクリック

設定するポリシーの要素(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保護対象が選択されています。

6. ポリシーを設定する
DNSポリシー



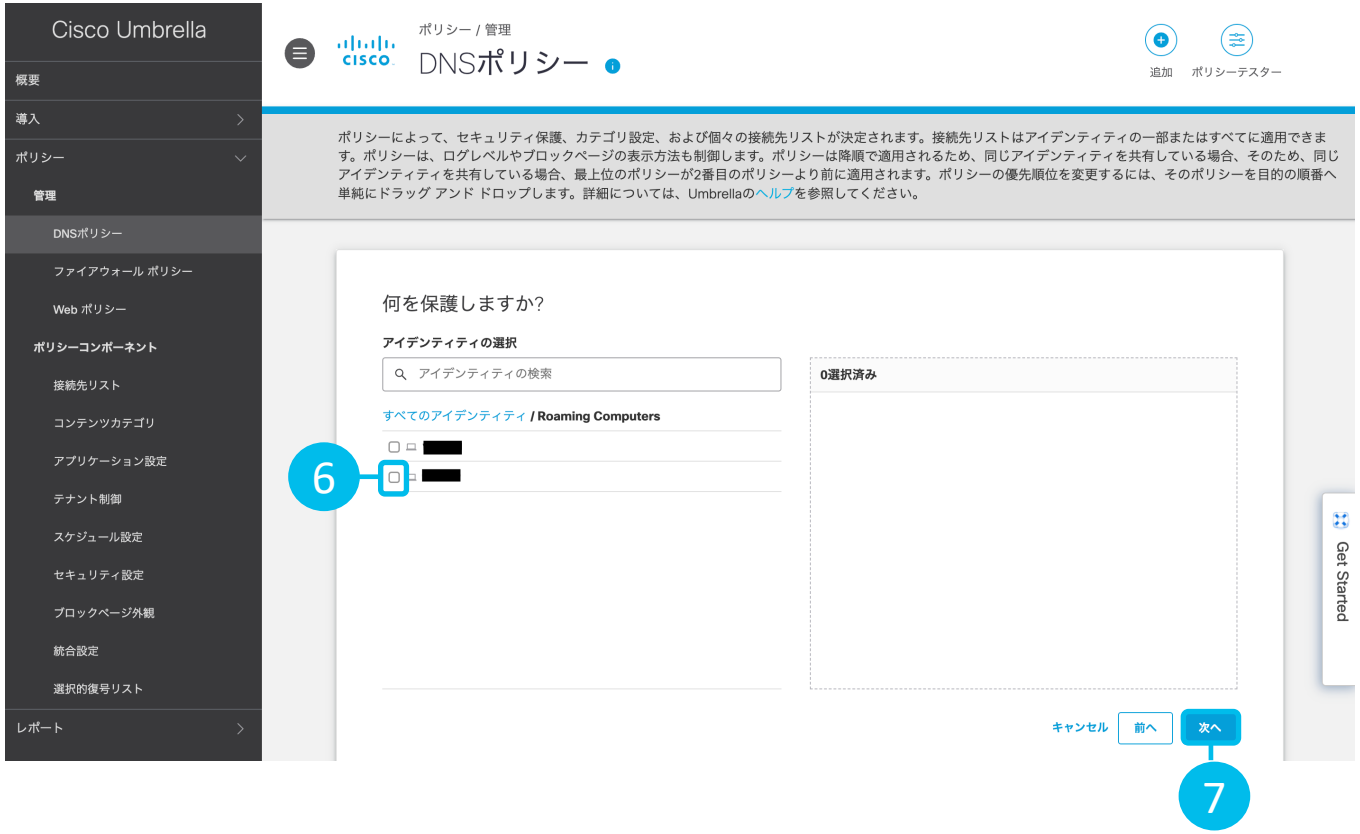
5 **[Roaming Computers]をクリック**

[**Roaming Computers**] [›]をクリック※します。

※[**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。

本ガイドでは、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)をポリシー適用対象とするため、[**Roaming Computers**]文字列をクリックし、6-⑥で該当するローミングコンピュータを選択します。

6. ポリシーを設定する
DNSポリシー



6 ポリシーを適用するローミングコンピュータ名のチェックボックスをクリックし選択

7 [次へ]をクリック

6. ポリシーを設定する
DNSポリシー

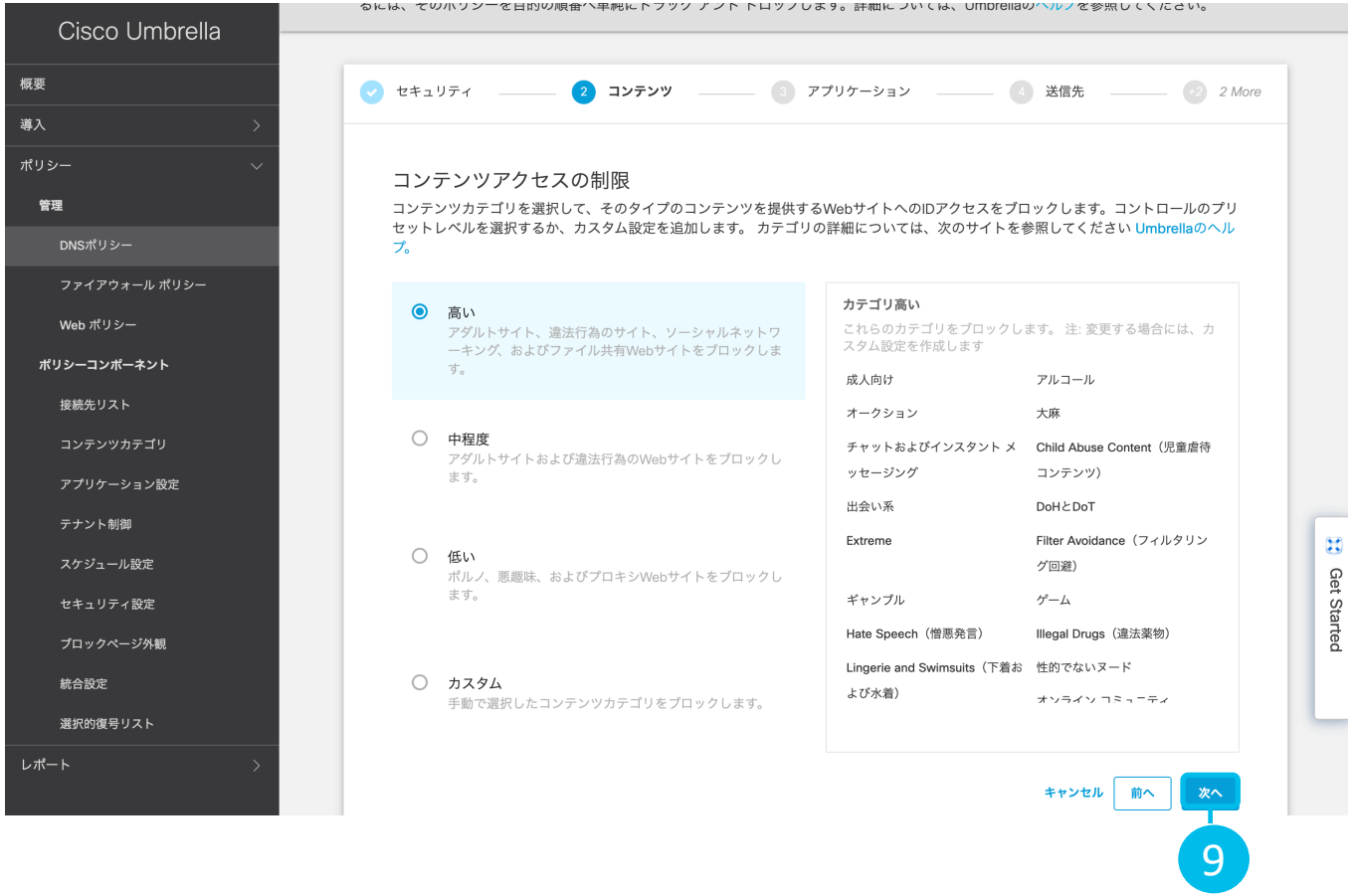
8 [次へ]をクリック

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**」をブロックする[**Default Settings**]が選択されています([**Default Settings**]を編集した場合、その設定内容が[ブロックするカテゴリ]に表示されます)。

独自のセキュリティ設定を選択または作成※したり、[**ブロックするカテゴリ**]の[**編集**]で既存のセキュリティ設定を編集したりすることもできます。

※セキュリティ設定は、[**ポリシー**]メニューの[**セキュリティ設定**]でも追加および編集できます。

6. ポリシーを設定する
DNSポリシー



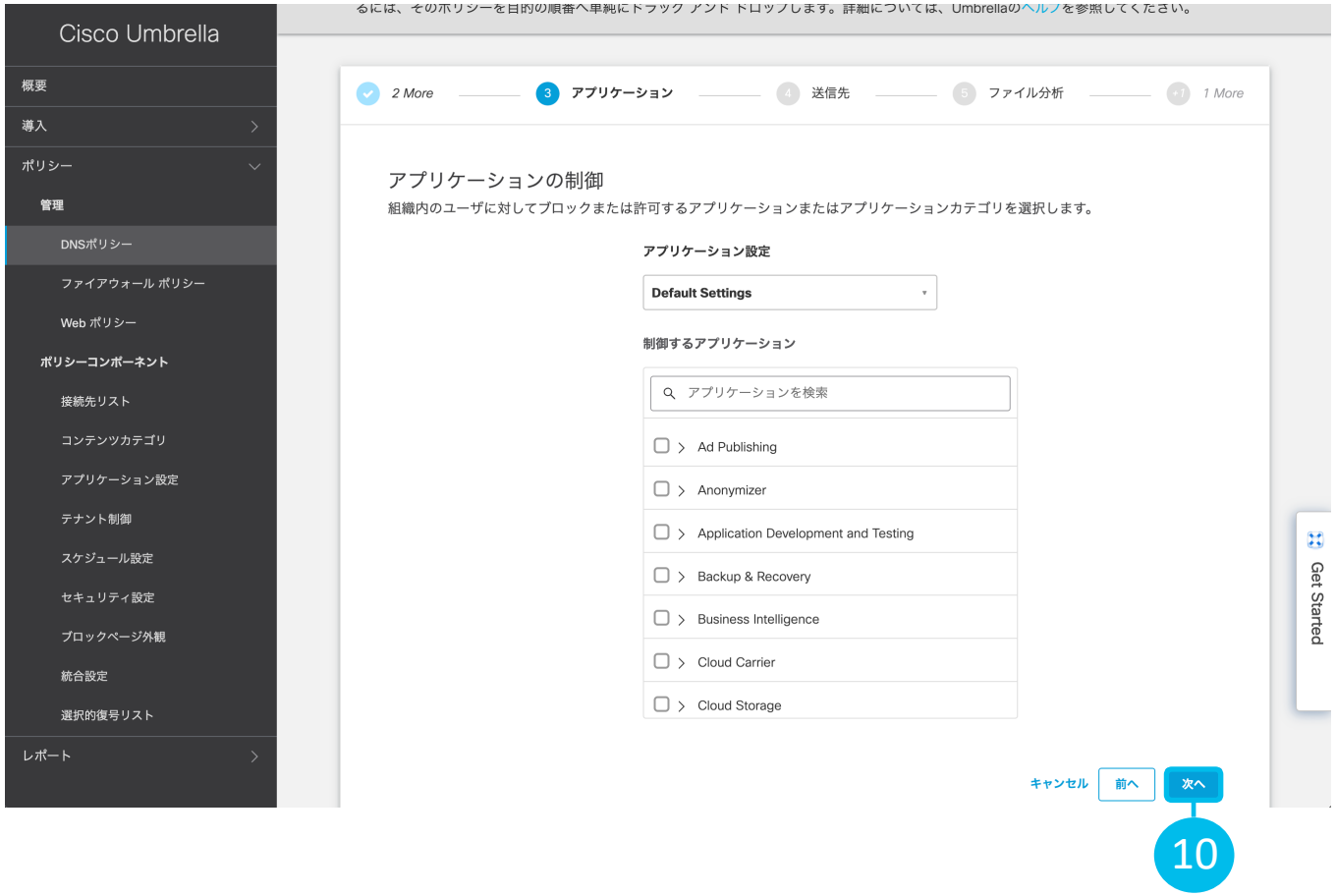
9 [次へ]をクリック

デフォルトでは、業務に関係がないコンテンツカテゴリや有害なコンテンツカテゴリの多くが含まれる[**高い**]が選択されています。

[**中程度**]や[**低い**]を選択したり、[**カスタム**]で独自のコンテンツカテゴリ設定を選択または作成※したり、[**ブロックするカテゴリ**]で既存のコンテンツカテゴリ設定を編集したりすることもできます。

※コンテンツカテゴリ設定は、[**ポリシー**]メニューの[**コンテンツカテゴリ**]でも追加および編集できます。

6. ポリシーを設定する
DNSポリシー



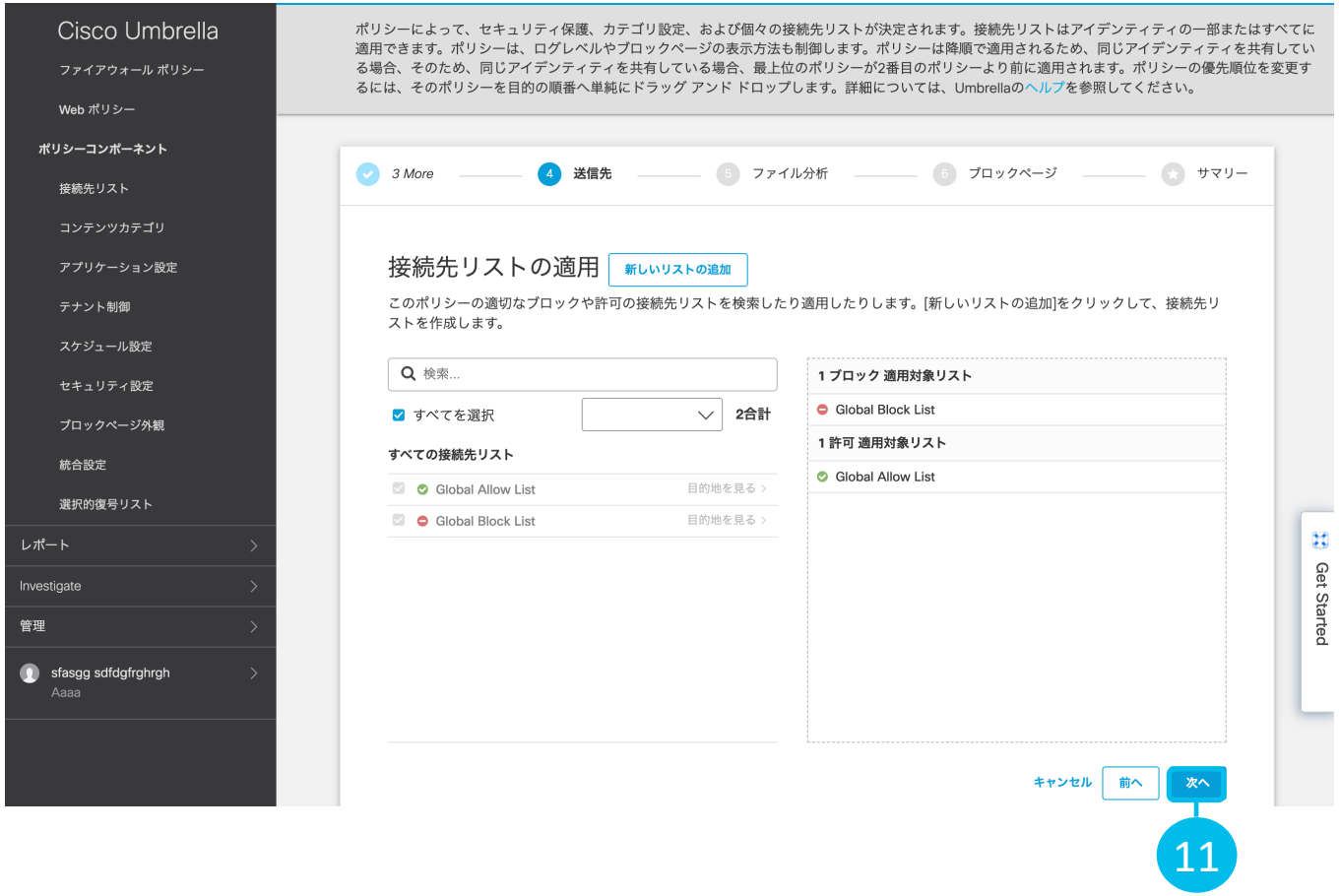
10 [次へ]をクリック

デフォルトでは、制御するアプリケーションが設定されていない[**Default Settings**]が選択されています([**Default Settings**]を編集した場合は、その設定内容が[**制御するアプリケーション**]に表示されます)。

独自のアプリケーション設定を選択または作成※したり、[**制御するアプリケーション**]でアプリケーションをカテゴリ別にブロック、個別に許可またはブロックなど、既存のアプリケーション設定を編集したりすることもできます。

※アプリケーション設定は、[**ポリシー**]メニューの[**アプリケーション設定**]でも追加および編集できます。

6. ポリシーを設定する
DNSポリシー



11 [次へ]をクリック

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。

独自の接続先リストを選択または作成※したり、既存の接続先リストを編集したりすることもできます。

※接続先リストは、[**ポリシー**]メニューの[**接続先リスト**]でも追加および編集できます。

6. ポリシーを設定する
DNSポリシー

12 **[次へ]をクリック**

デフォルトでは**オン**になっています。
ファイルを分析し、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。

6. ポリシーを設定する
DNSポリシー

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。

6. ポリシーを設定する
DNSポリシー

14 [**ポリシー名**]に任意の名前を入力

デフォルトでは[**新しいポリシー**]となっています。

15 [**インテリジェントプロキシの有効化**]をクリックし、**オフ**にする

デフォルトでは**オン**になっています。

「[6.ポリシーを設定する(Webポリシー)]」にて設定するWebポリシー(SWG)を同じアイデンティティに適用する場合、Webポリシーで予期せぬ動作を起こす場合があるため、本機能をオフにすることが推奨です。

16 [**セキュリティイベントのみをロギング**]をクリック

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。

本ガイドでは、社員の私物コンピュータ用にプライバシーに配慮したポリシーとして、[**セキュリティイベントのみをロギング**]を選択します。

17 [**保存**]をクリック

6. ポリシーを設定する
DNSポリシー

18 ポリシーの追加を確認

6-⑭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。ポリシーは適用する順番※に表示されます。

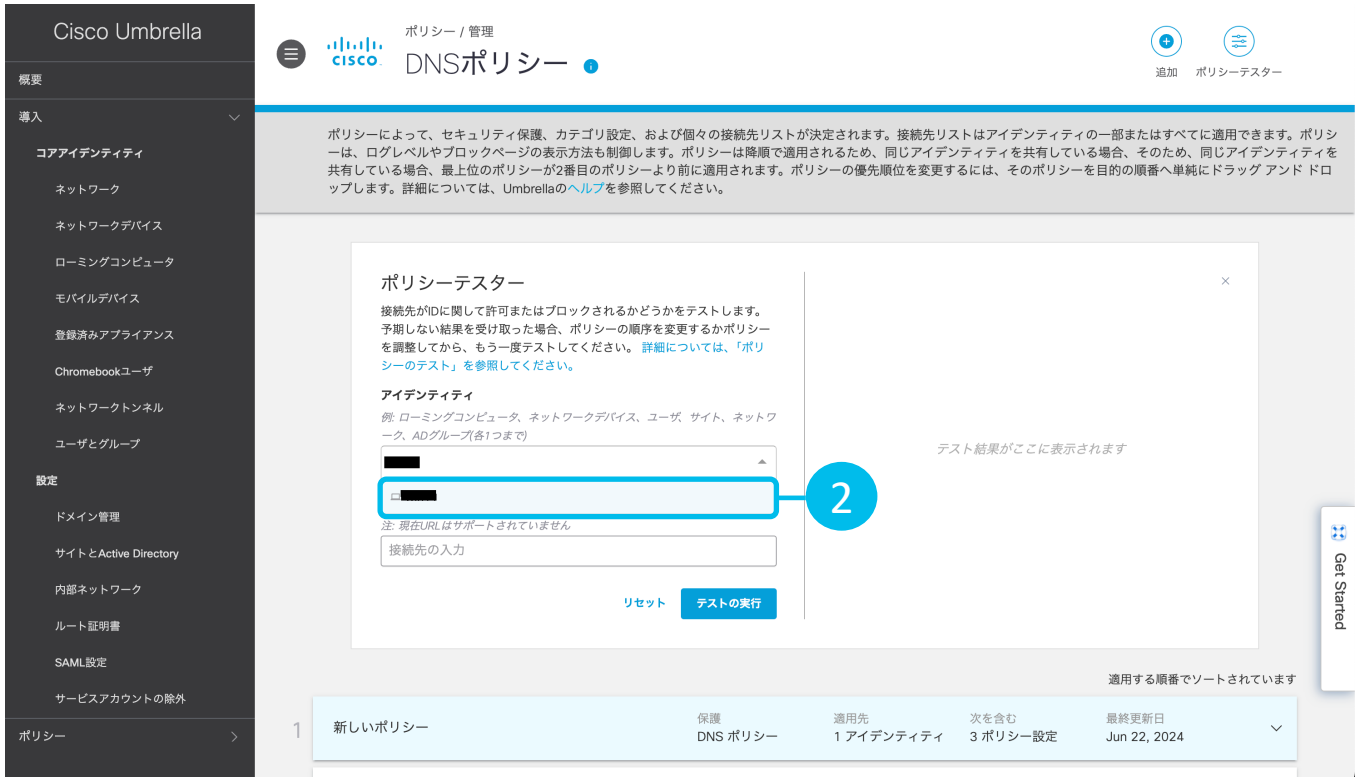
※「**Default Policy**」以外に複数のポリシーを運用している環境では、ポリシーをドラッグ&ドロップすることで、ポリシーが適用される順番を調整できます。
全てのアイデンティティに適用される[**Default Policy**]は順番の変更はできません。

6. ポリシーを設定する
DNSポリシーテスター

- 新しく追加したDNSポリシーが正常に適用されるか確認します。

1 [ポリシーテスター]をクリック

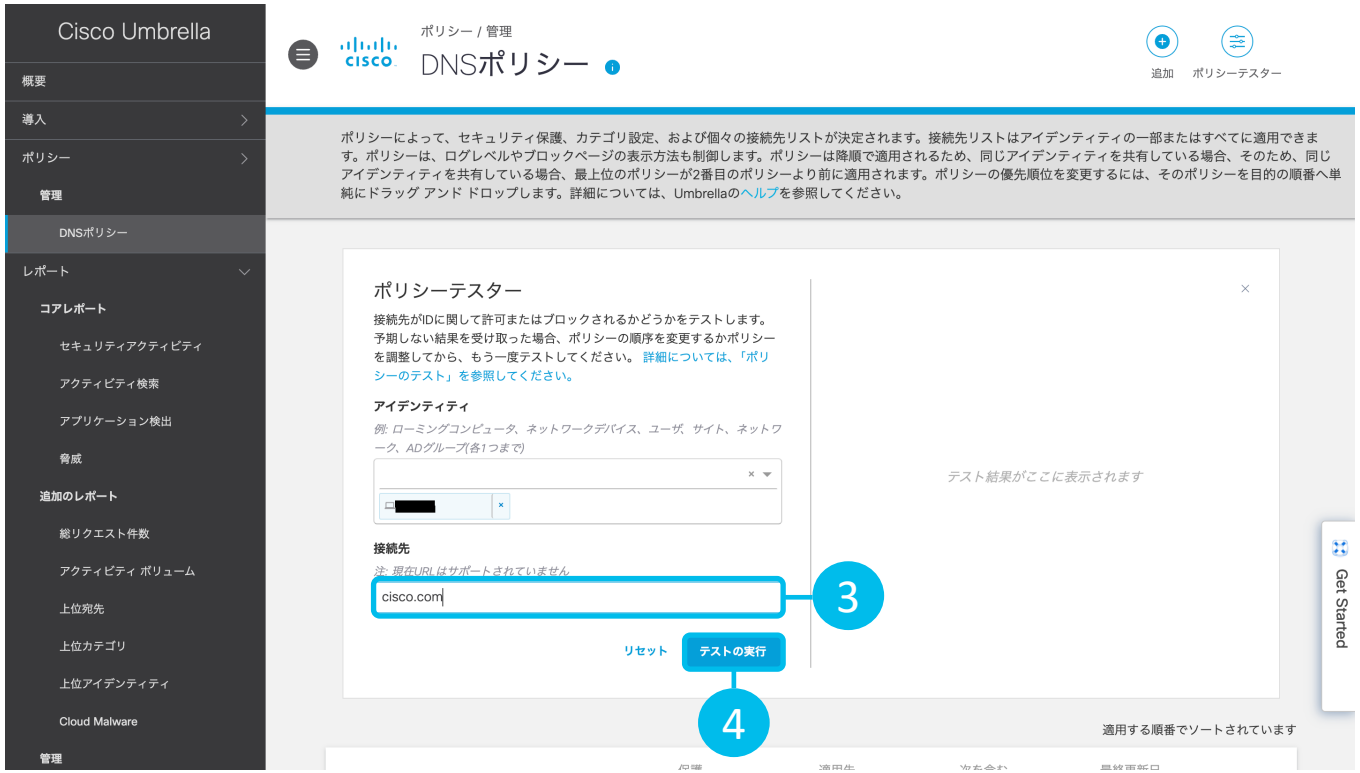
6. ポリシーを設定する
DNSポリシーテスター



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ローミング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ローミングコンピュータ名をクリックし選択

本ガイドの設定例では、「**6.ポリシーを設定する(DNSポリシー)⑥**」で選択したコンピュータ名を検索します。

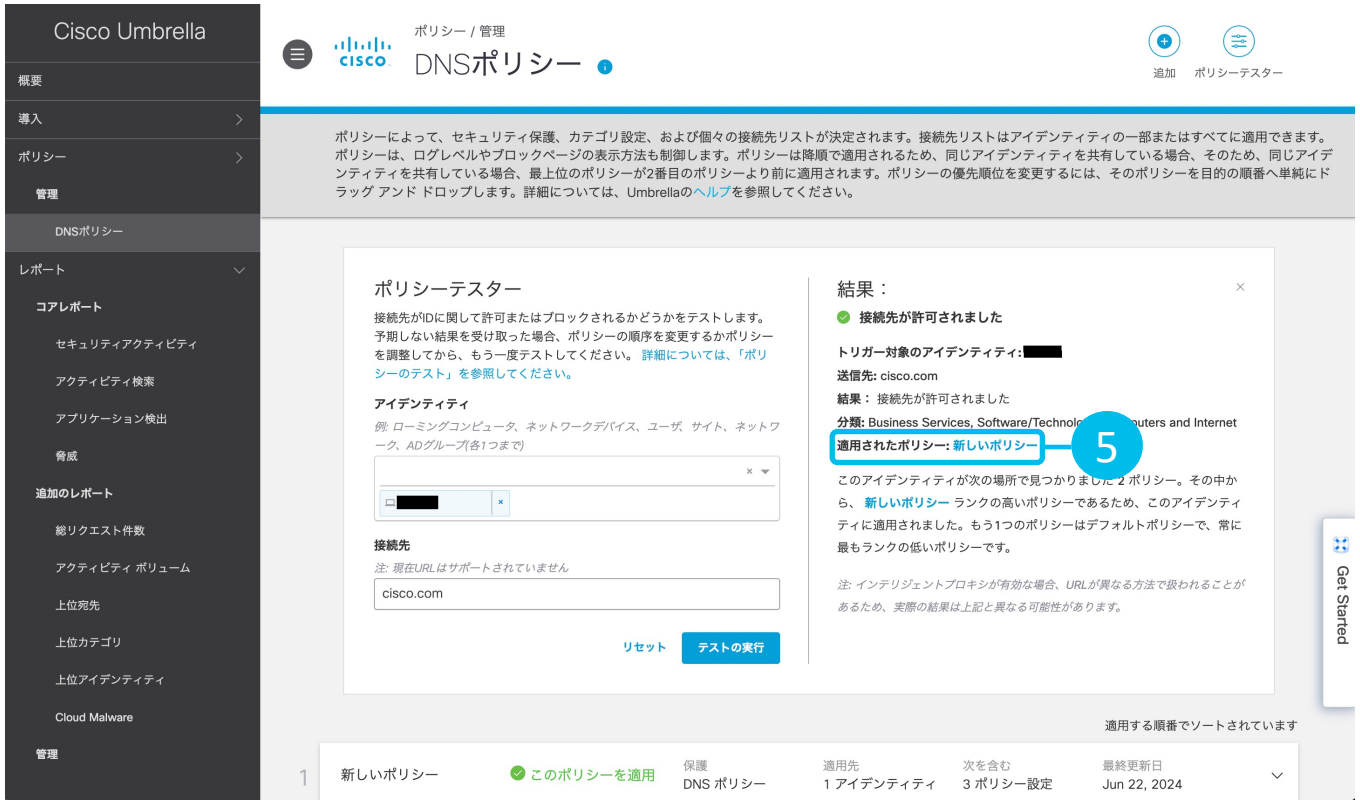
6. ポリシーを設定する
DNSポリシーテスター



3 [接続先]に任意のドメインを入力

4 [テストの実行]を入力

6. ポリシーを設定する
DNSポリシーテスター



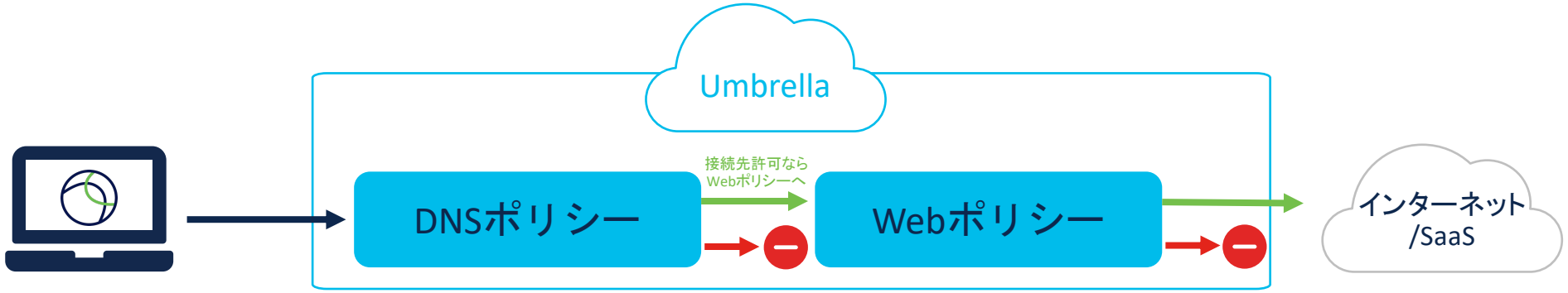
5 [適用されたポリシー]を確認

本ガイドの設定例では、「**6.ポリシーを設定する(DNSポリシー)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。

※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、ポリシーの一覧画像でポリシーをドラッグ&ドロップし、適用される順番を調整可能です。

6. ポリシーを設定する
Webポリシー

- 最後に、**フルプロキシ機能**(SWG)を提供する**Webポリシー**を設定します。
  - ポリシーの適用順序として、DNSポリシー > Webポリシーの順番で当たります。



- Webポリシーはルールセット及びそのルールで構成されています。
  - ステップ1:[**ルールセット**]の追加
    - ルールを適用する保護対象(アイデンティティ)や保護オプションを決定
  - ステップ2:[**ルールセットルール**]を追加
    - 個々の保護対象および接続先のルールアクション(許可、警告、ブロック、隔離※)を決定

※隔離アクションは、SIGパッケージの追加オプションであるリモートブラウザ分離(RBI)機能となります。
https://docs.umbrella.com/umbrella-user-guide/docs/manage-remote-browser-isolation

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

1 [ポリシー]をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

2 [Webポリシー]をクリック

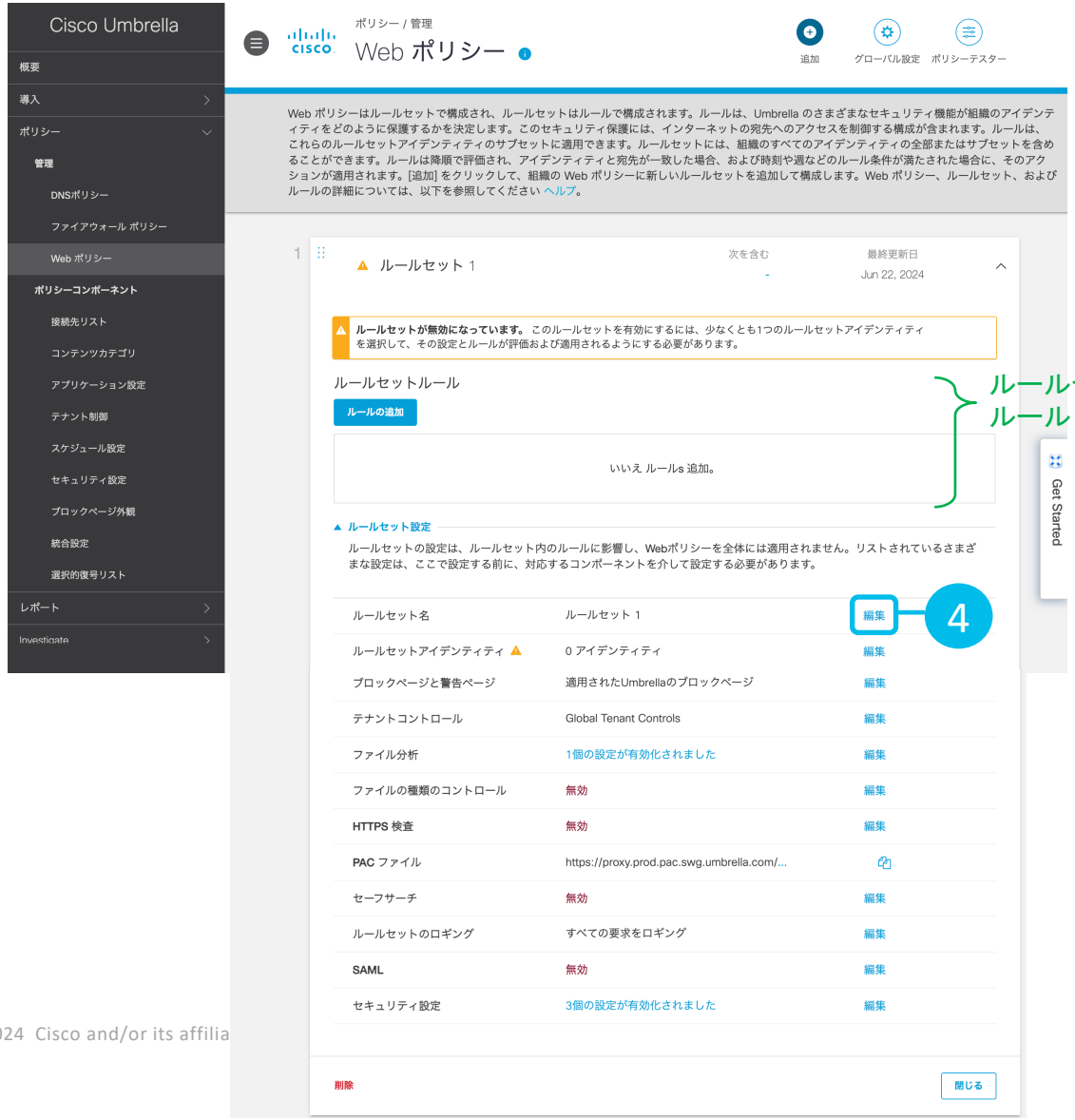
6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

3 [追加]をクリック

※**Default Policy**は、その他のルールセットに適用されないIDに適用するポリシーとなります。管理外・想定していないようなデバイス/ユーザがインターネットにアクセスしようとした場合に強制するポリシーとなります。そのため**Default Policy**は最も制限の厳しいルールセットとし、**Default Policy**からボトムアップ方式のルールセットの構築することが推奨です。詳細はオンラインドキュメントを参照ください。
https://docs.umbrella.com/umbrella-user-guide/docs/best-practices-for-web-policy

6. ポリシーを設定する

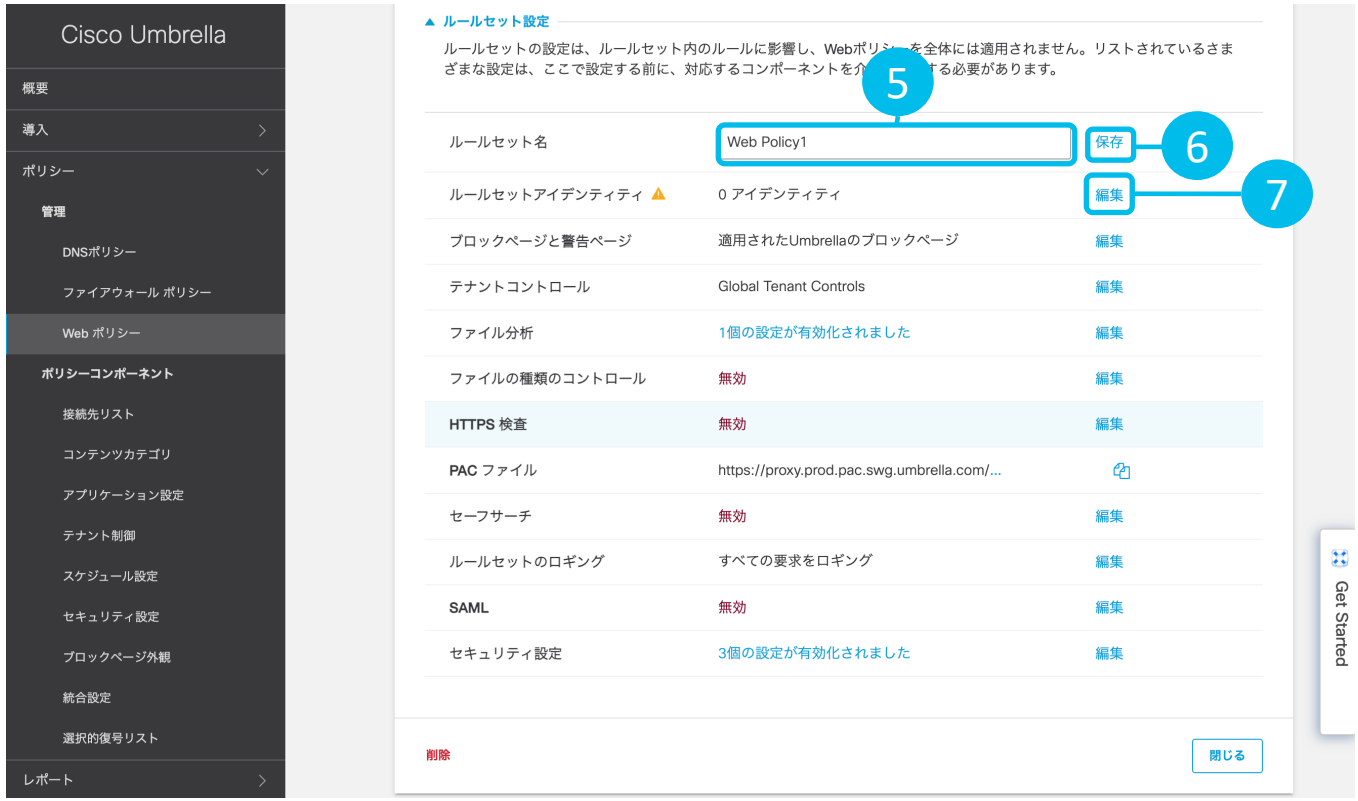
Webポリシー ステップ1:ルールセットの追加



4 **[ルールセット名]の[編集]をクリック**

デフォルトでは**[ルールセット1]**となっています。

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加



5 [**ルールセット名**]に任意の名前を入力

デフォルトでは[**ルールセット1**]となっています。

6 [**保存**]をクリック

7 [**ルールセットアイデンティティ**]の[**編集**]をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

8 **[Roaming Computers]をクリック**

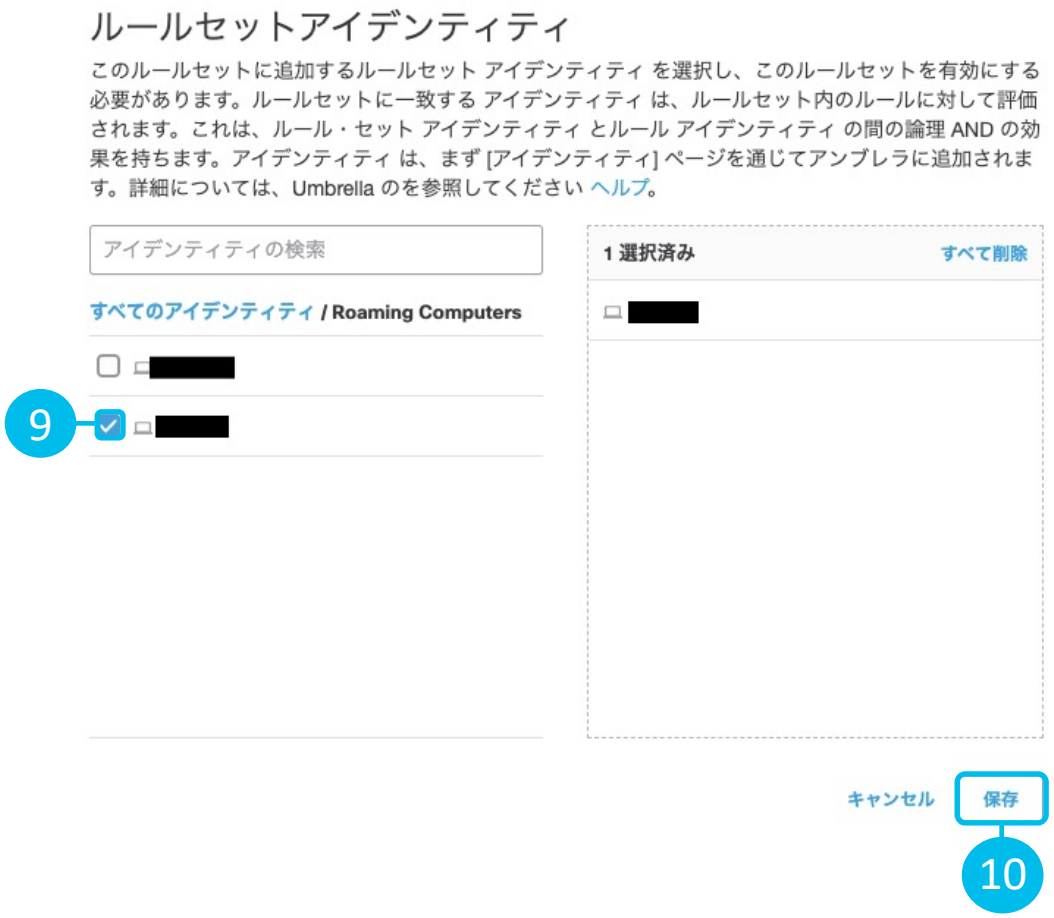
[Roaming Computers] [›]をクリック※します。

※[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。

本ガイドでは、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)をポリシー適用対象とするため、[Roaming Computers]文字列をクリックし、「6.ポリシーを設定する(Webポリシー)⑨」で該当するローミングコンピュータを選択します。

6. ポリシーを設定する

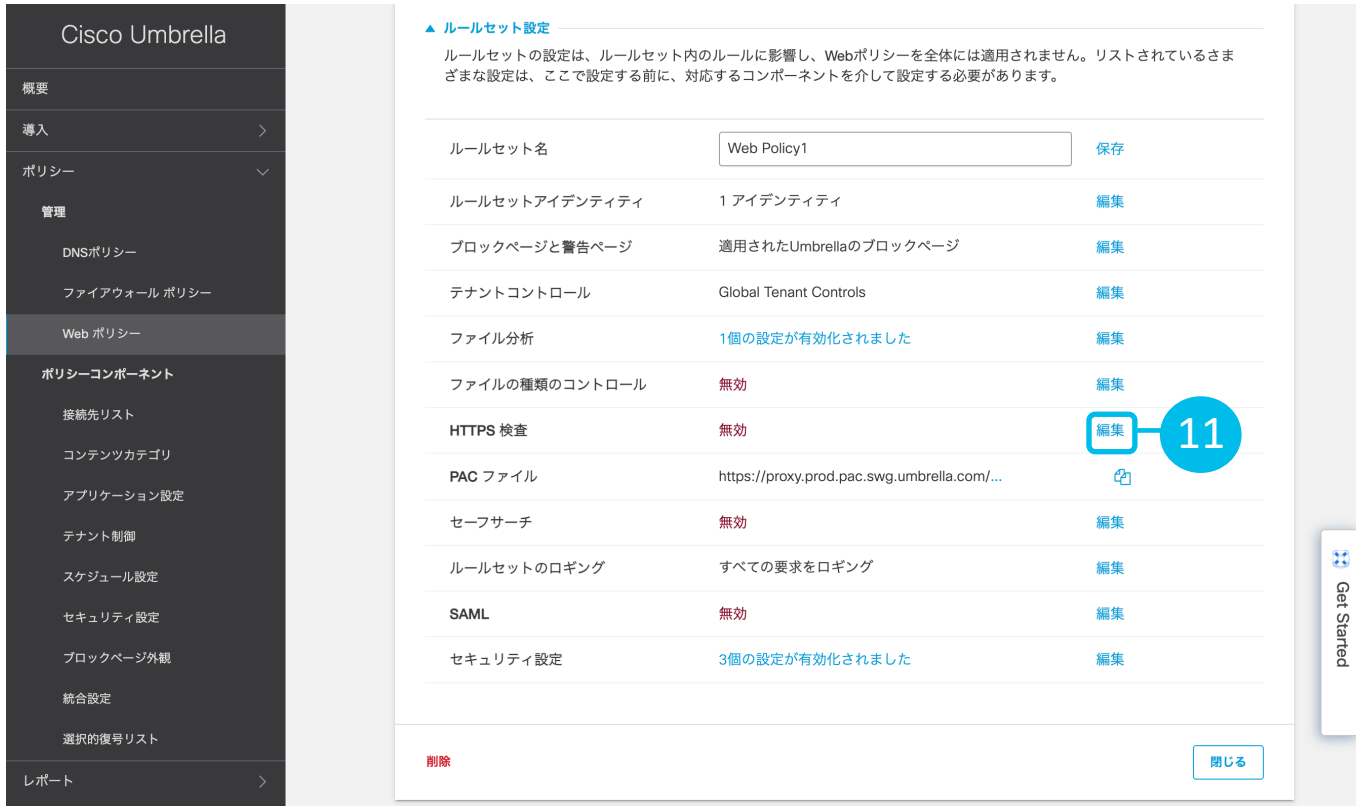
Webポリシー ステップ1:ルールセットの追加



9 ポリシーを適用するローミングコンピュータ名のチェックボックスをクリックし選択

10 [保存]をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加



11 [HTTPS検査]の[編集]をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

12 **[HTTPSトラフィック検査の有効化]をクリック**

デフォルトでは、すべてのHTTPS通信を検査します(特定のHTTPS通信を検査から除外する**[ドメインを追加し、HTTPSトラフィック検査対象から除外するカテゴリを選択します]**で**「選択的復号リスト」**が選択されていません。)

検査から除外するコンテンツカテゴリやアプリケーション、ドメインのリスト※を選択または作成したり、既存リストを編集が可能です。

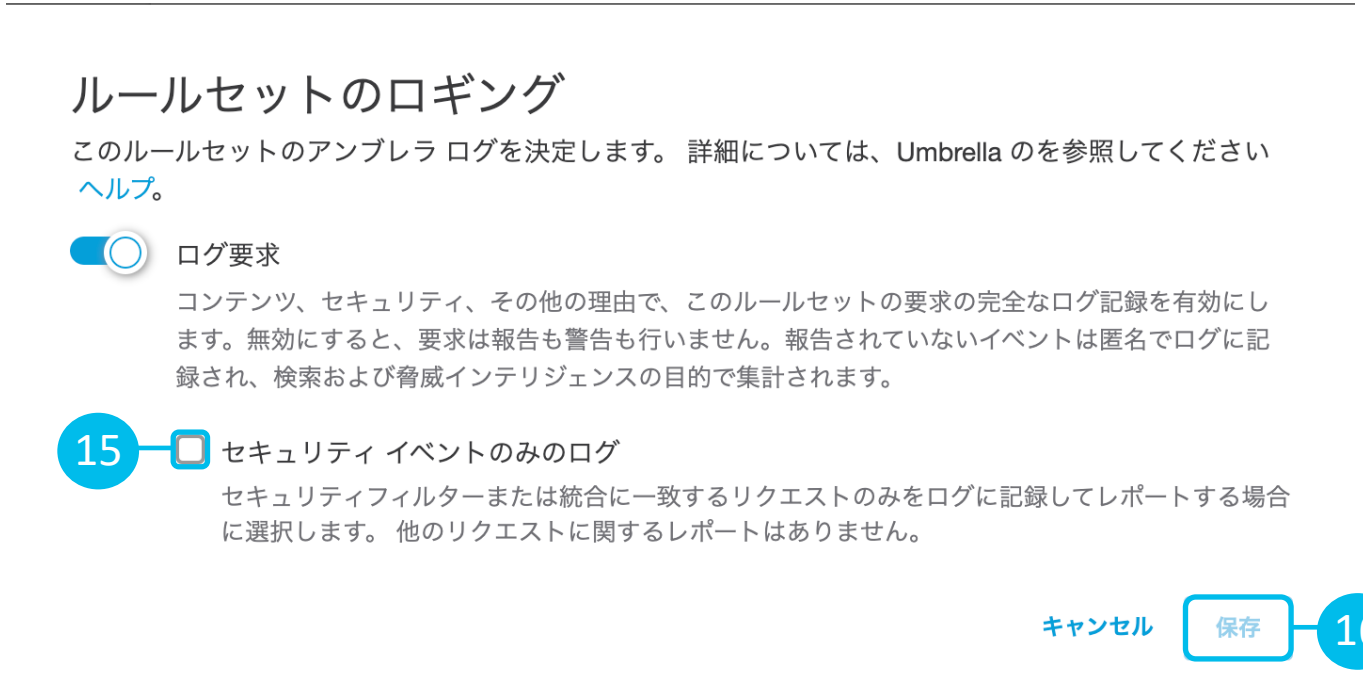
13 **[保存]をクリック**

※検査から除外するコンテンツカテゴリやアプリケーション、ドメインを定義する選択的復号リストは、**[ポリシー]**メニューの**[選択式復号リスト]**でも追加および編集できます。

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

14 [ルールセットのロギング]の[編集]をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加



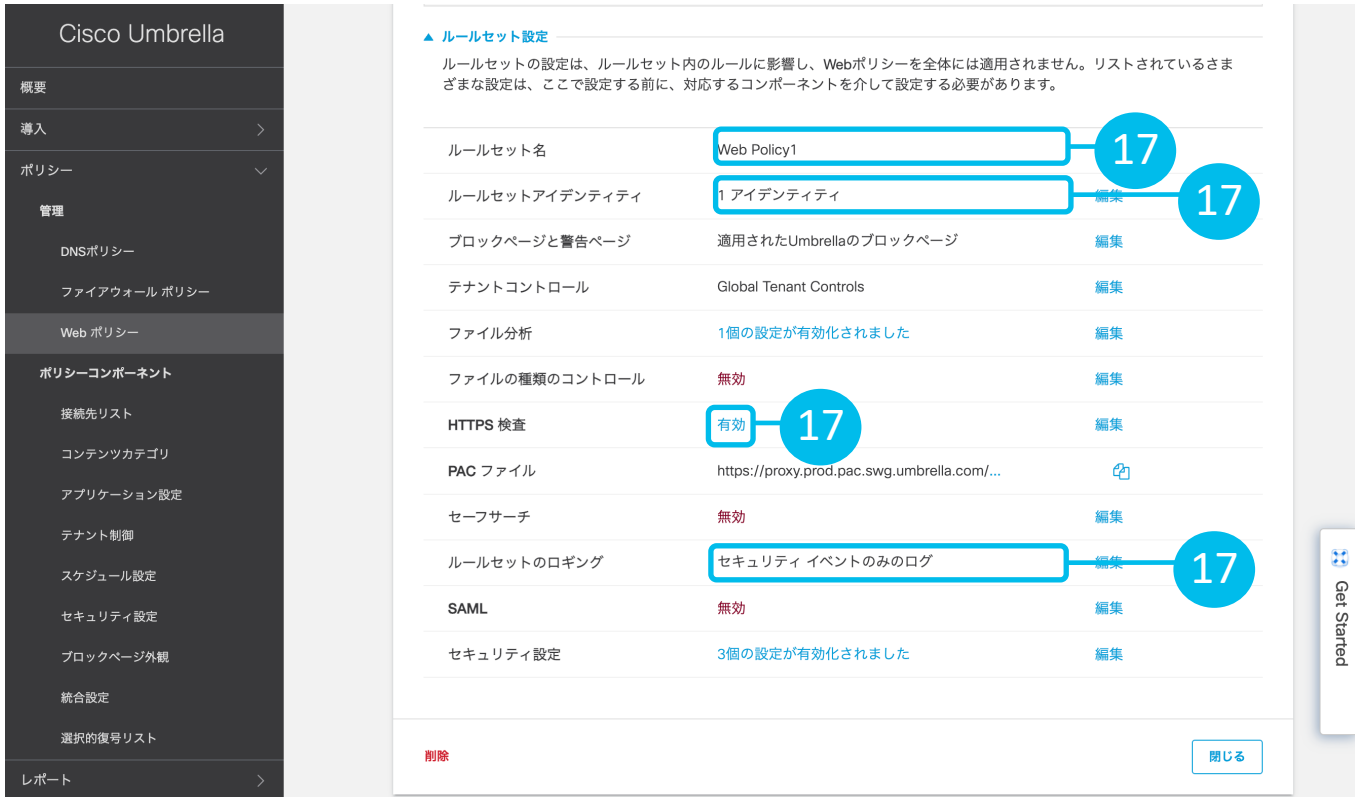
15 **[セキュリティ イベントのみのログ]**にチェック

デフォルトでは[**すべての要求をロギング**] が選択されています。

本ガイドでは、社員の私物コンピュータ用にプライバシーに配慮したポリシーとして、[**セキュリティ イベントのみのログ**]を選択します。

16 **[保存]**をクリック

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加



17 **[ルールセット名]、[ルールセットアイデンティティ]、[HTTPS検査],[ルールセットのロギング]がそれぞれ設定変更されていることを確認**

6. ポリシーを設定する
Webポリシー ステップ1:ルールセットの追加

18 ポリシーの追加を確認

⑤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。

※「**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。
全てのアイデンティティに適用される[**Default Policy**]は順番の変更はできません。

続いて、ルールセットルールを設定します。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

- ルールセットルールでは、個々のアイデンティティとそのアイデンティがアクセスしようとする送信先に対して、許可、警告、ブロック、隔離などのルールアクションを設定します。

1 **[ルールの追加]をクリック**

本ガイドでは、ルールセット「**Web Policy1**」のルールセットルールを設定します。

注意

ステップ1で設定した**ルールセット**は、設定したアイデンティティ毎に適用される一方、ステップ2で設定する**ルールセットルール**は、設定したアイデンティティおよびその送信先に基づき適用されます。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

2 [ルール名]に任意の名前を入力

デフォルトでは[新しいルール1]となっています。

3 [ルールアクション]の[⌄]をクリック

デフォルトではルールアクション[ブロック]となっています。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

4 [ブロック]をクリック

※本ガイドでは、サンプルルールとして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)およびその送信先としてSNS「Instagram」に対して「**ルールアクション：ブロック**」とする [**Rule1**]を作成します。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

5 [アイデンティティ]の[アイデンティティを追加する]をクリック

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

6 **[ルールセット アイデンティティの継承]** をクリックし、**オン**にする

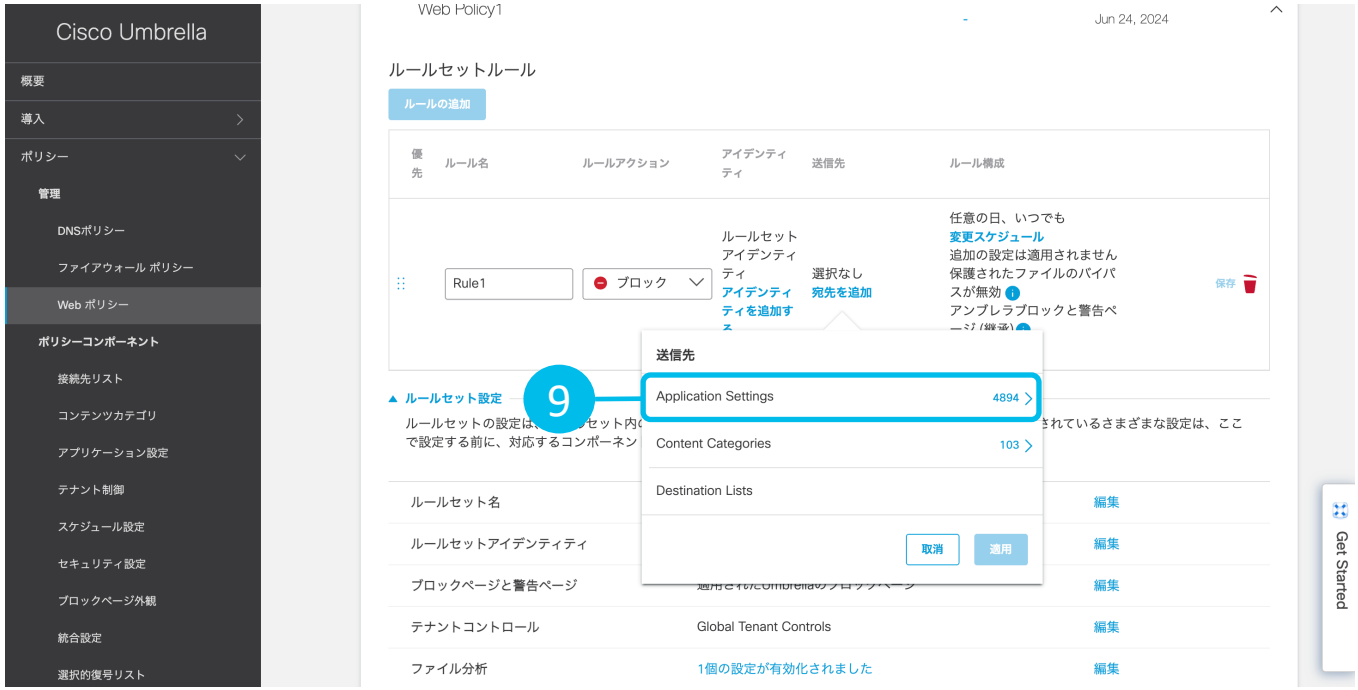
デフォルトでは**オフ**となっています。
[ルールセット アイデンティティの継承]を有効化した場合、ステップ1で設定した**ルールセット**のアイデンティティが適用(継承)され、その他のアイデンティティは選択できなくなります。

7 **[適用]** をクリック

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

8 [送信先]の[宛先を追加]をクリック

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加



9 [送信先]の[Application Settings]をクリック

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

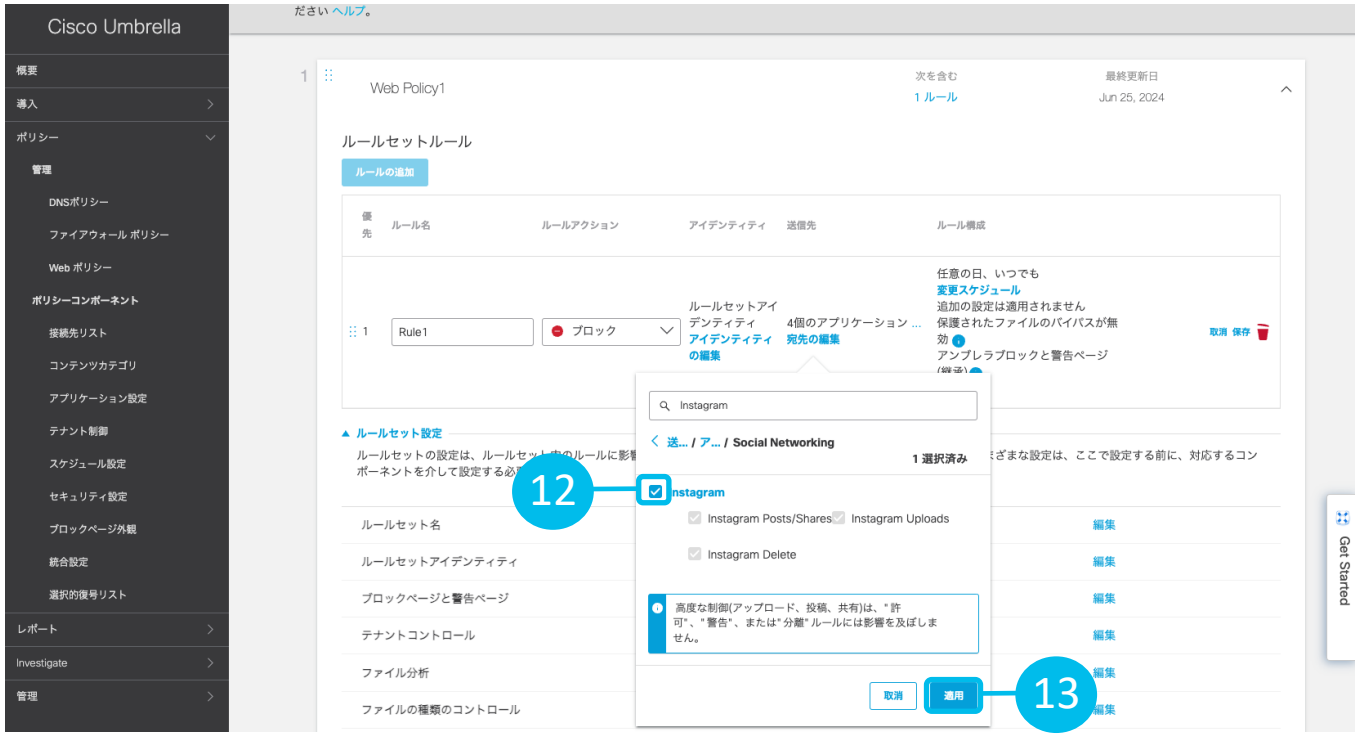
10 [Instagram]と検索

11 ヒットした「**Social Networking(Instagram)**」の[›]をクリック

※アプリケーション設定は、[**ポリシー**]メニューの[**アプリケーション設定**]で予め設定および編集ができます。

独自のアプリケーション設定を選択または作成したり、[制御するアプリケーション]でアプリケーションをカテゴリ別に風呂奥、個別に許可またはブロックなど、既存のアプリケーション設定を編集できます。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加



12 [Instagram]をクリック※

13 [適用]をクリック

※[Instagram Posts/Shares]を選択した場合、**高度な制御機能**としてInstagramでの**投稿**や**共有**のみがルールアクションの影響(ブロックや隔離など)があります。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

14 [保存]をクリック

注意
ルールセットルールを[**保存**]だけではルールは適用されません。
必ず[**ルールの有効化**]手順が必要となります。

6. ポリシーを設定する
Webポリシー ステップ2:ルールセットルールの追加

15 […]をクリック

16 [**ルールの有効化**]をクリックし、オンにする

デフォルトでは**オフ**となっています。

17 [**更新**]をクリック

6. ポリシーを設定する
Webポリシーテスター

- 新しく追加したWebポリシーが正常に適用されるか確認します。

1 [ポリシーテスター]をクリック

6. ポリシーを設定する
Webポリシーテスター

2 [プライマリアイデンティティ]検索ボックスにポリシーをテストしたいローミング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ローミングコンピュータ名をクリックし選択

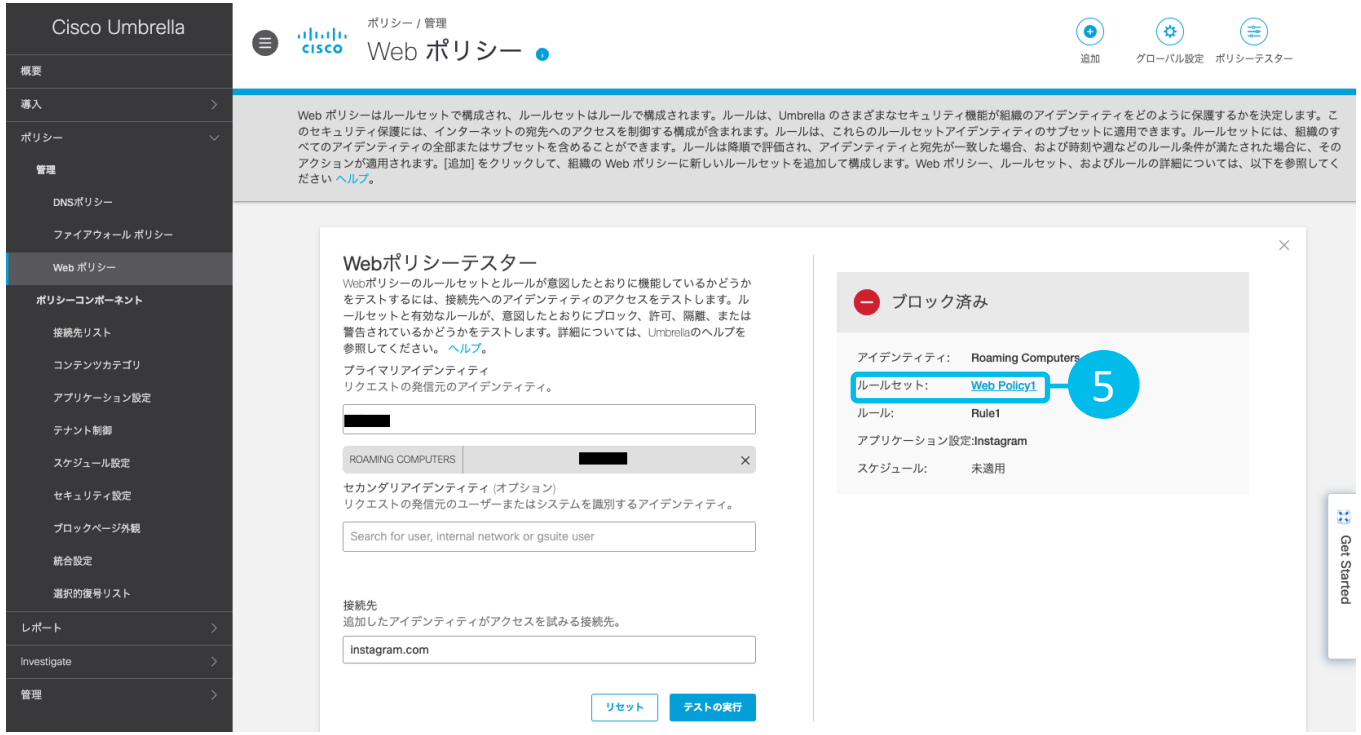
本ガイドの設定例では、「**6.ポリシーを設定する(Webポリシー)⑨**」で選択したコンピュータ名を検索します。

6. ポリシーを設定する
Webポリシーテスター

3 [**接続先**]に任意のドメイン、URL、IPv4またはCIDRを入力

4 [**テストの実行**]を入力

6. ポリシーを設定する
Webポリシーテスター



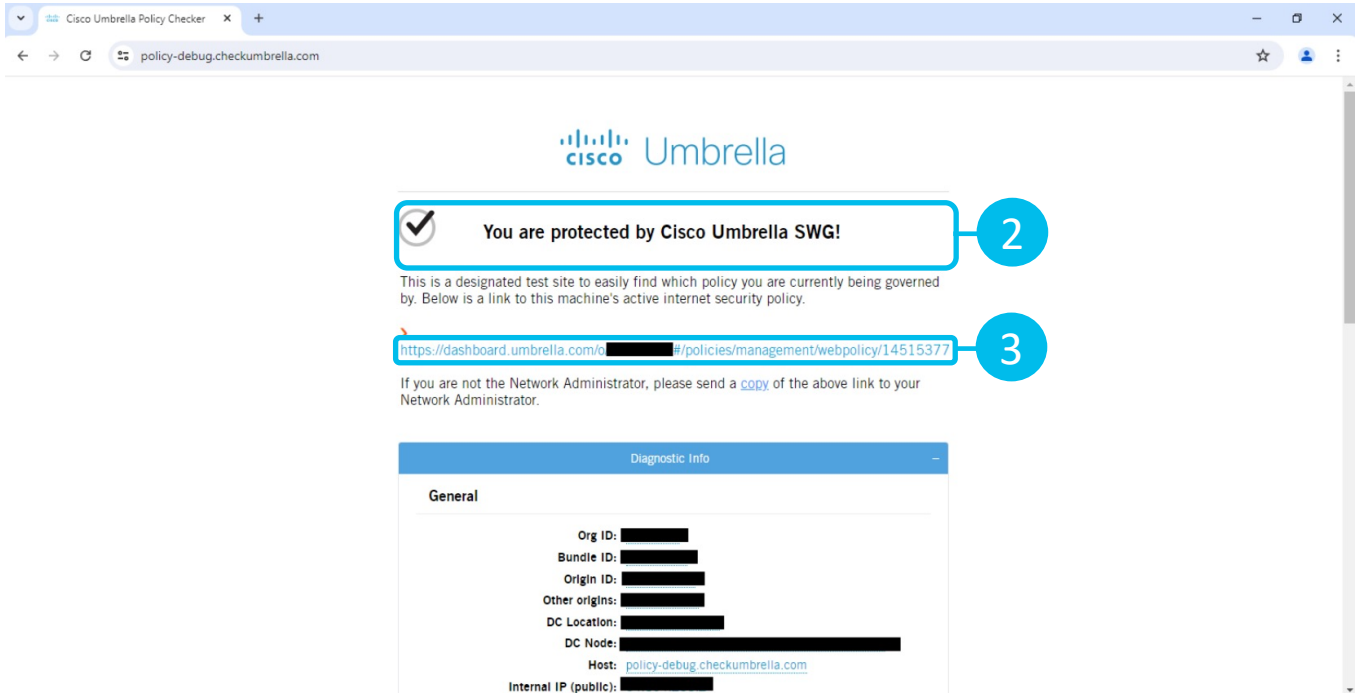
5 [適用されたポリシー]を確認

本ガイドの設定例では、「**6.ポリシーを設定する(Webポリシー)⑤**」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。

※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、ポリシーの一覧画像でポリシーをドラッグ&ドロップし、適用される順番を調整可能です。

6. ポリシーを設定する
Webポリシーテストサイト

- 最後に、新たに設定したWebポリシーが正常に適用されるか**ブラウザ(本ガイドではGoogle Chrome)**上で確認します。



1 ブラウザのアドレスバーに[**policy-debag.checkumbrella.com**]を入力

2 [**You are protected by Cisco Umbrella SWG!**]メッセージが表示されることを確認

Cisco Secure Client Umbrellaモジュールが正常に動作している場合は、「**You are protected by Cisco Umbrella SWG!**」メッセージが表示されます。

3 リンクをクリック

リンクをクリックし、ダッシュボードにアクセスします。

6. ポリシーを設定する
Webポリシーテストサイト

4 「6.ポリシーを設定する(Webポリシー)」で作成したポリシーの編集画面が表示されることを確認

ダッシュボードにアクセスすると、現在適用されているWebポリシーの編集画面が表示されます。

本設定ガイドでは、「**6.ポリシーを設定する(Webポリシー)**」で作成したポリシーの編集画面が表示されることを確認します。

6. ポリシーを設定する
Webポリシーテストサイト

5 ブラウザのアドレスバーに[**Instagram.com**]を入力

6 Cisco Umbrella**のブロックページ**が表示されていることを確認

本ガイドで作成したWebポリシー「**Rule1**」では、接続先「**Instagram**」に対して**ブロック**するポリシーを作成・適用されたためです。

以上で、Cisco Umbrella SIGローミングコンピュータのセットアップは完了となります。

The bridge to possible

参考情報

- Cisco Umbrella SIGユーザガイド

https://docs.umbrella.com/umbrella-user-guide/docs/getting-started

- Cisco Secure Clientクイックスタートガイド

https://docs.umbrella.com/umbrella-user-guide/docs/secure-client-quick-start-guide

- DNSポリシーのベストプラクティス

https://docs.umbrella.com/umbrella-user-guide/docs/best-practices-for-dns-policies

- Webポリシーとルールセットのベストプラクティス

https://docs.umbrella.com/umbrella-user-guide/docs/best-practices-for-web-policy

- 接続先のテスト

https://docs.umbrella.com/umbrella-user-guide/docs/test-your-destinations