



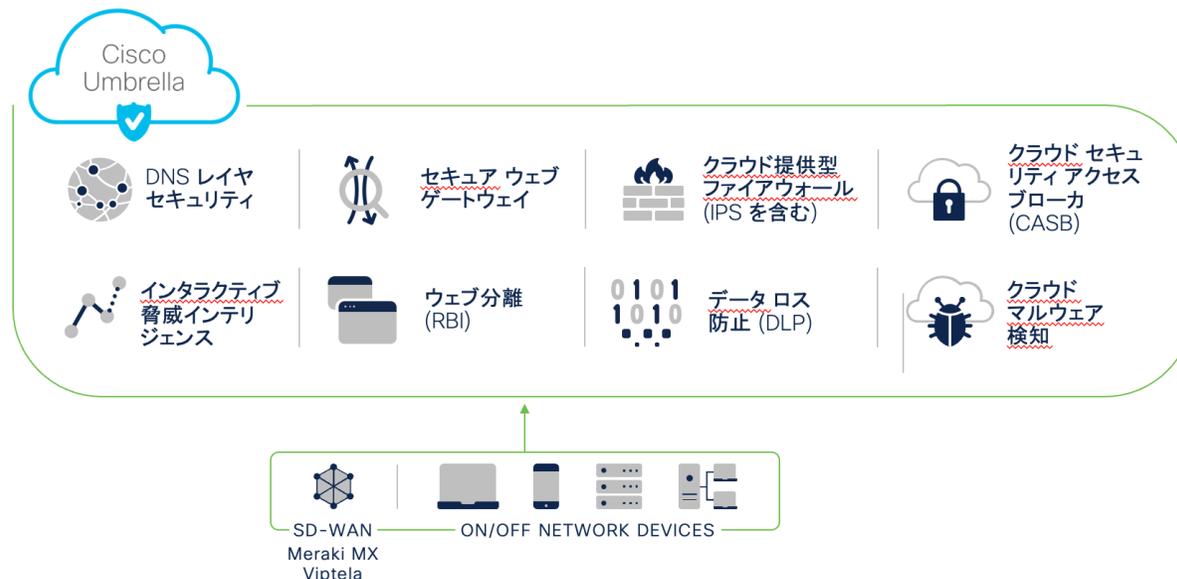
Cisco Umbrella SIG ローミングコンピュータ

かんたんセットアップガイド

2024年6月

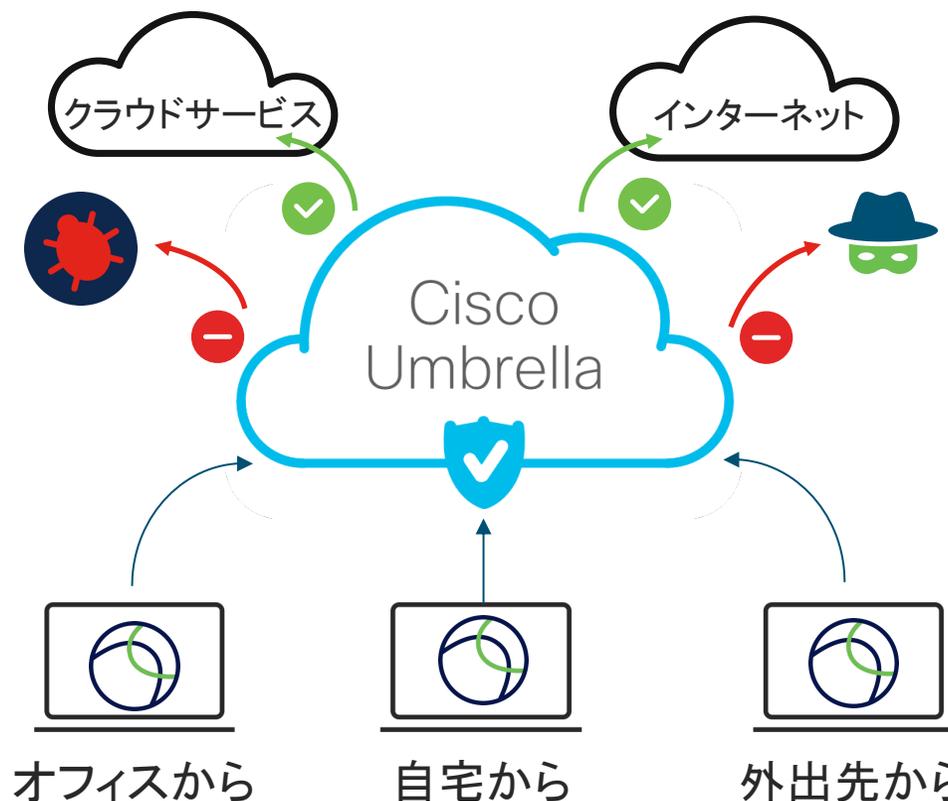
はじめに

- 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>

3

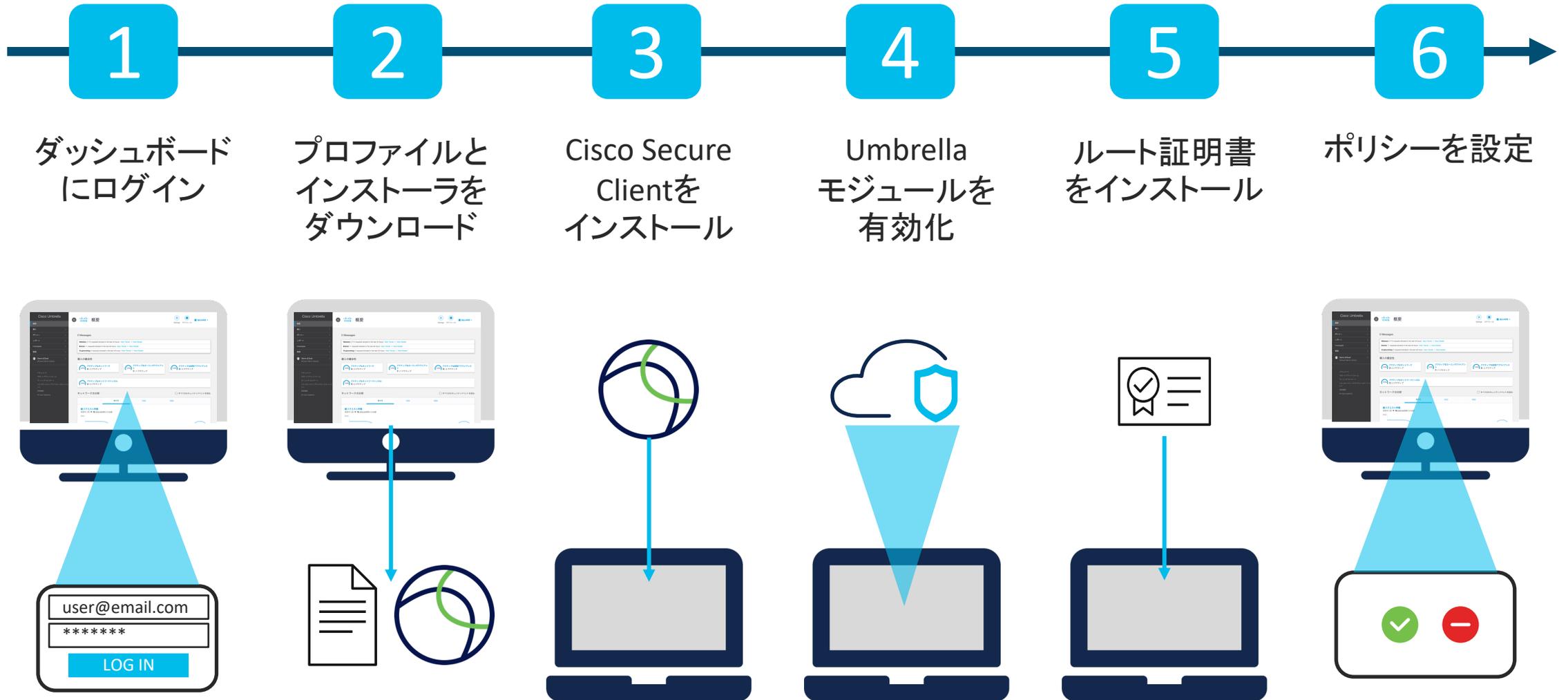
対応ブラウザ(ダッシュボード)

- 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



目次

1. [ダッシュボードにログインする](#) P7
2. [プロフィー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。

Welcome to Cisco Umbrella!



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

Welcome to Cisco Umbrella!

US Umbrella Support <umbrella-support@cisco.com>
To: C [REDACTED]

Sunday,

 Cisco Umbrella

H [REDACTED]

Welcome to Cisco Umbrella! Your order has been processed and will be activated shortly. Let's get you up and running quickly, so you can start protecting your users and devices today. Just follow these quick and easy steps:

First Step:

Sign into your account: <https://dashboard.umbrella.com>

- Your login email is [REDACTED]
- The first time logging into the dashboard you will need to create a password by clicking the "Forgot password" link.
- Note, if you do not receive the email, please check your Spam folder.

Second Step:

Use our [Getting Started Guide](#). Learn how to send traffic from your networks or devices to Umbrella, create a security policy to protect the traffic, and view the reports to see what's happening.

Third Step:

Check out our [Support Page](#). You'll find user guides and documentation to get you started with deploying Umbrella.

Have Questions?

Register for a [live onboarding webinar](#) to get a complete walk-through of Umbrella deployment. There's always email, too. You can reach us at umbrella-support@cisco.com.

Thank you,
Cisco Umbrella Team

 Cisco Umbrella

© Cisco Systems, Inc.
All rights reserved.

2

[Your login email]に記載されているメールアドレスを確認

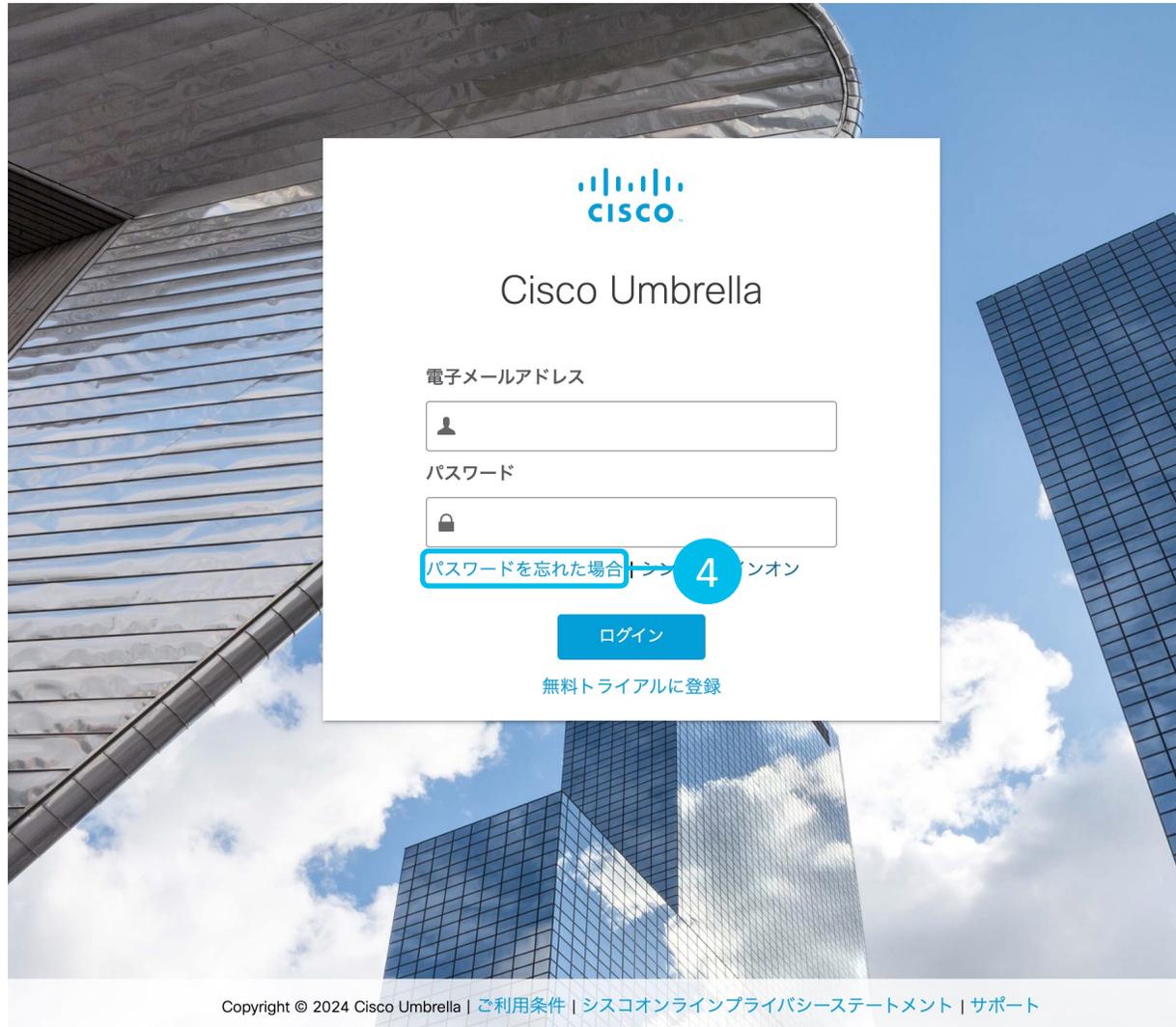
契約時に指定した管理者用メールアドレスが記載されていることを確認します。

3

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

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

Cisco Umbrella パスワードのリセット

Cisco Umbrella パスワードのリセット



umbrella-support@cisco.com <umbrella-support@cisco.com>

To: [Redacted]



Today at 18:20



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



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

The screenshot shows the Cisco password reset interface. At the top is the Cisco logo and the title 'パスワードの復旧'. Below the title is a paragraph explaining the process: '電子メールアドレスと新しいパスワードを入力してください。パスワードがリセットされると、他のコンピュータ上の既存のセッションからログアウトされます。' There are three input fields: '電子メール' (with a callout 9), 'パスワード' (with a callout 10), and 'パスワードの確認' (with a callout 11). Below these fields is a list of password requirements: 'パスワードは: 8~256文字である必要があります', '大文字と小文字を少なくとも1文字ずつ含めます', 'また、少なくとも1つの数字と1つの特殊文字(*, \$, πなど)が含まれている必要があります', and 'ユーザ名の一部を含めることはできません'. At the bottom are two buttons: 'パスワードのリセット' (with a callout 12) and 'キャンセル'.

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

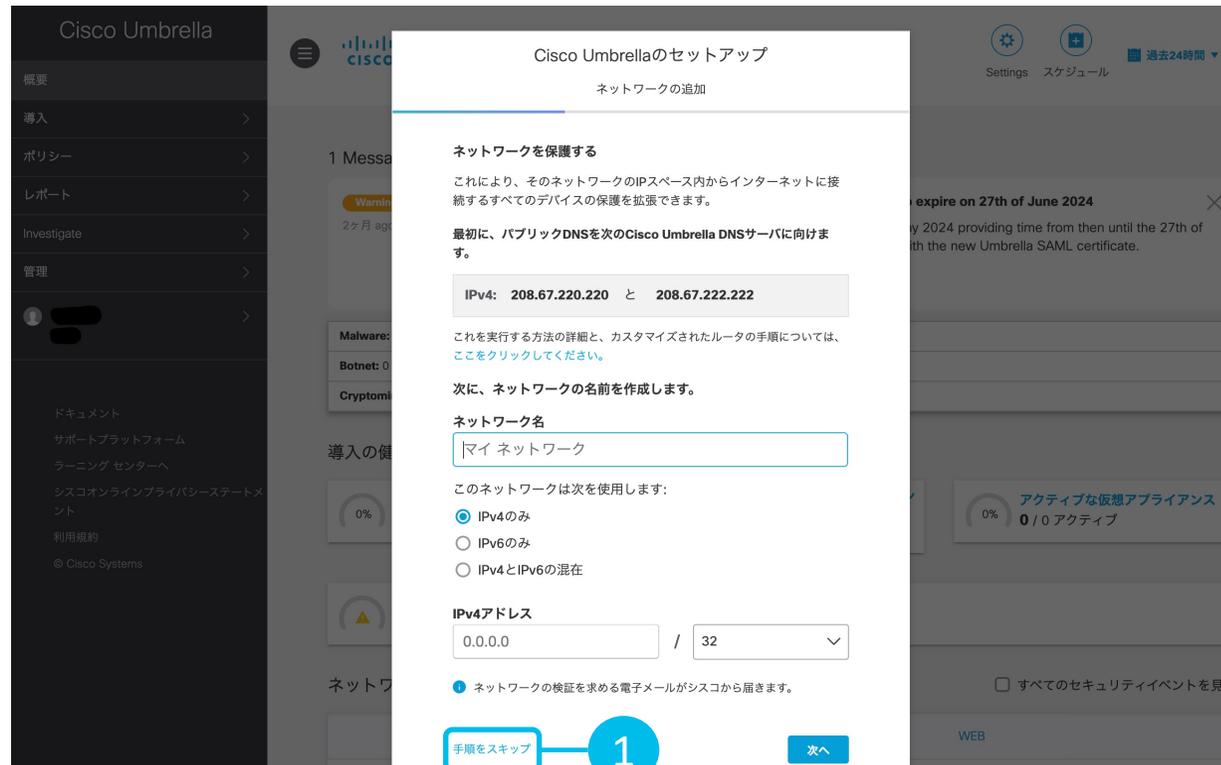
- Cisco Umbrella ダッシュボードから2点ダウンロードします。
 - Cisco Secure Client(Umbrellaモジュール)のプロファイル
 - Cisco Secure Clientのインストーラ

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

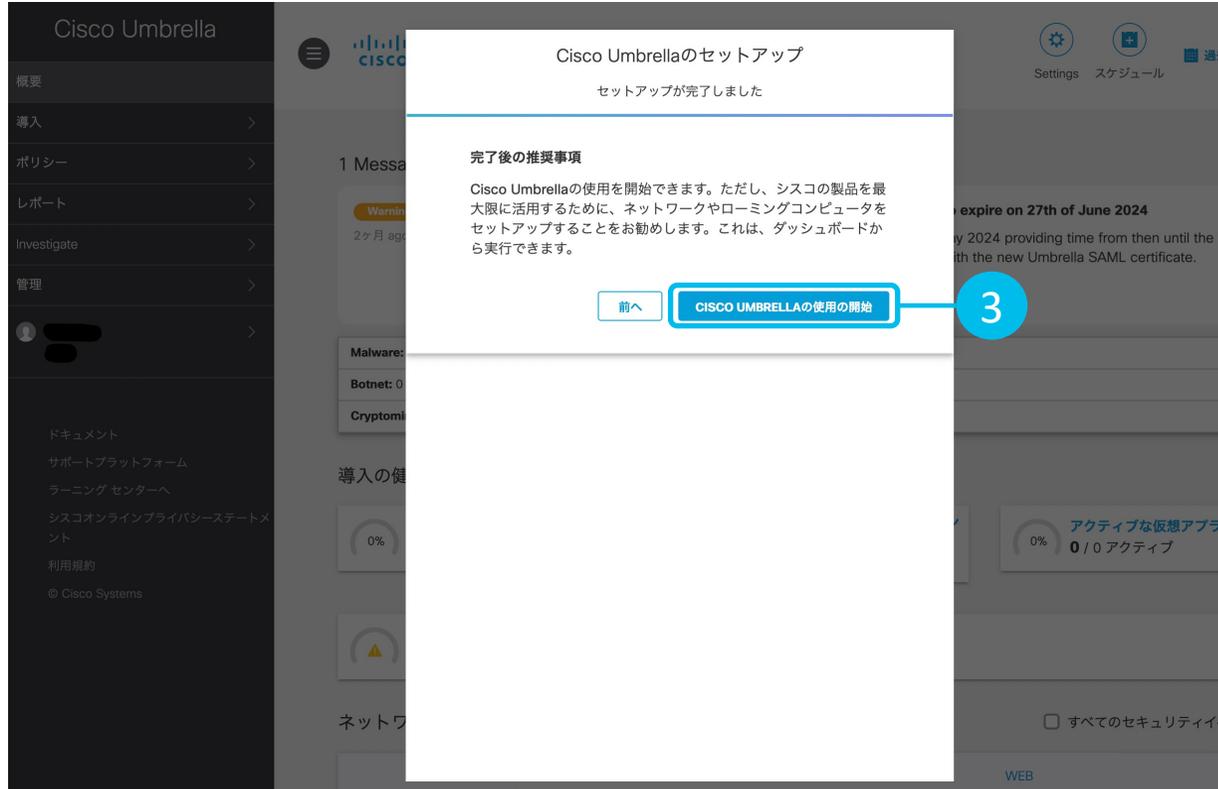
[手順をスキップ]をクリック

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の使用を開始]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

The screenshot shows the Cisco Umbrella dashboard. On the left sidebar, the '導入' (Import) menu item is highlighted with a blue circle and the number 4. The main content area shows a summary of security events for the last 24 hours, including Malware, Botnet, and Cryptomining blocks. Below this, there are three cards for '導入の健全性' (Import Health): 'アクティブなネットワーク' (Active Networks), 'アクティブなローミングクライアント' (Active Roaming Clients), and 'アクティブな仮想アプライアンス' (Active Virtual Appliances), all showing 0/0 active. A fourth card for 'アクティブなネットワークトンネル' (Active Network Tunnels) shows a warning icon and '非トラッキングデータ' (Non-tracking data). At the bottom, there is a 'ネットワークの分析' (Network Analysis) section with a table showing zero results for total requests, blocked requests, and security blocks.

すべて	DNS	WEB
総リクエスト件数 合計0 - 0% 過去24時間との比較	総ブロック 合計0 - 0% 過去24時間との比較	セキュリティブロック 合計0 - 0% 過去24時間との比較
検索結果がありません	検索結果がありません	検索結果がありません

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

Cisco Umbrella 概要

0 Messages

Malware: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Botnet: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Roaming: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

導入の健全性

0% アクティブなネットワーク 0 / 0 アクティブ

0% アクティブなローミングクライアント 0 / 0 アクティブ

0% アクティブな仮想アプライアンス 0 / 0 アクティブ

0% アクティブなネットワークトンネル 非トラッキングデータ

ネットワークの分析 すべてのセキュリティイベントを見る

すべて	DNS	WEB
総リクエスト件数 合計0 - 0% 過去24時間との比較	総ブロック 合計0 - 0% 過去24時間との比較	セキュリティブロック 合計0 - 0% 過去24時間との比較

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

Cisco Umbrella

導入 / コアアイデンティティ

ローミングコンピュータ

6 ローミングクライアント 設定

ローミングコンピュータとは、UmbrellaローミングクライアントまたはCisco Secure Client Umbrellaモジュール(旧AnyConnect)によって保護されるコンピュータを指します。ダッシュボードのこの領域では、管理者は右上のダウンロードボタンを使用してクライアントを展開し、下のローミングコンピュータを管理することができます。

ローミングコンピュータがまだ展開されていません。

それでは始めましょうAnyConnect向けのUmbrellaローミングクライアントまたはUmbrellaローミングセキュリティモジュールをダウンロードするには、右上隅にある[ダウンロード]アイコンをクリックします。

Get Started

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。

2. プロファイルとインストーラをダウンロードする

Cisco Secure Clientのダウンロード

Cisco Secure Clientは、ネットワーク内外のラップトップやデスクトップを保護します。前提条件などの詳細については、Cisco Umbrellaのヘルプを参照してください。

▲ 内部ドメインを解決するには、展開する前にinternal domainsを追加する必要があります。

Cisco Secure Client (推奨)

ステップ1. Cisco Secure Clientの最新バージョンをダウンロードします

展開前パッケージ:
[Windows \(x86/x64\)](#) | [Windows \(Arm\)](#) | [macOS](#)

ヘッドエンド展開パッケージ:
[Windows \(x86/x64\)](#) | [Windows \(Arm\)](#) | [macOS](#)

注: Cisco Secure Clientの以前のバージョンは、Software Centralからダウンロードできません。

ステップ2. Cisco Umbrellaのローミングセキュリティ モジュール プロファイルをダウンロードします

Cisco Secure Clientは、DNSとWebセキュリティの両方を提供するCisco Umbrella ローミングセキュリティ モジュールを有効化するように設定できます。インストーラはモジュールプロファイルと組み合わせる必要があります。詳細については、Cisco Umbrellaのヘルプを参照してください。

モジュールのプロファイルをダウンロード
Umbrellaモジュールには、WindowsまたはmacOS用のCisco Secure Clientが必要で、最新のリリースをお勧めします。

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

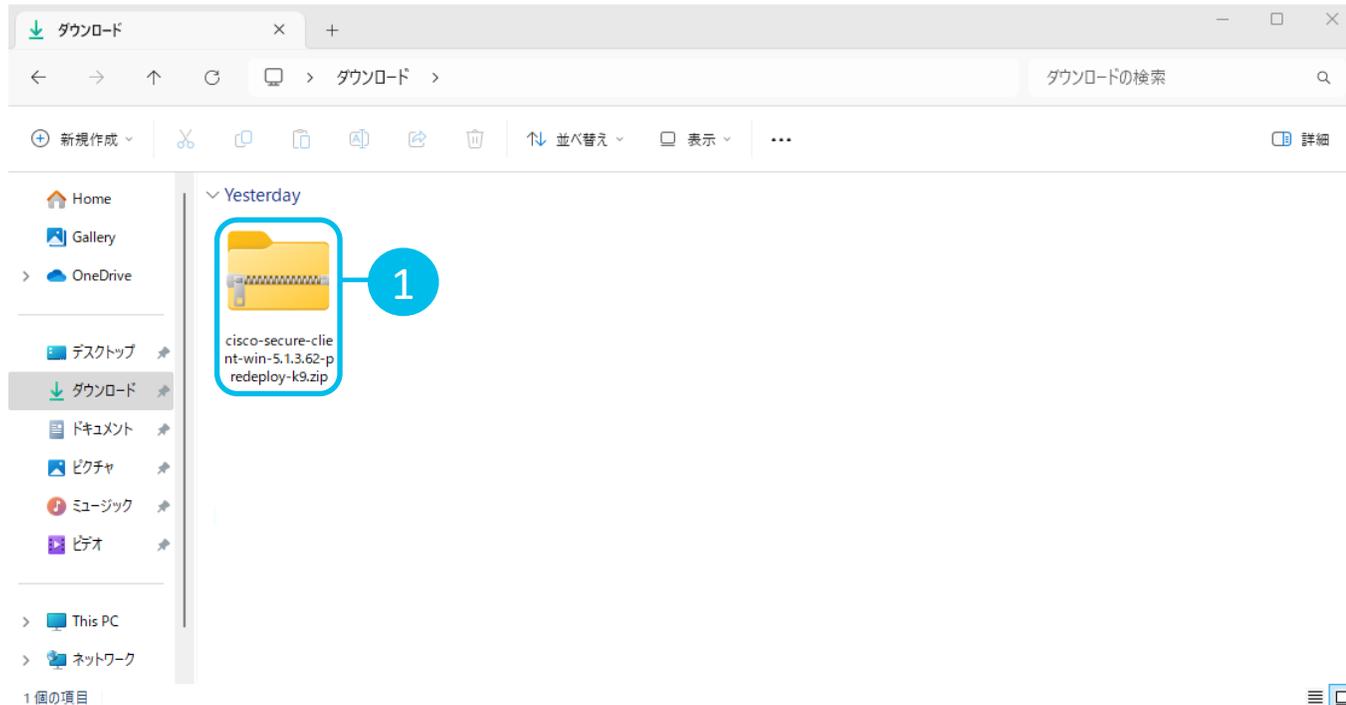
Cisco Secure Client(Umbrellaモジュール)のプロファイルをダウンロードし、任意の場所に保存します。

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。

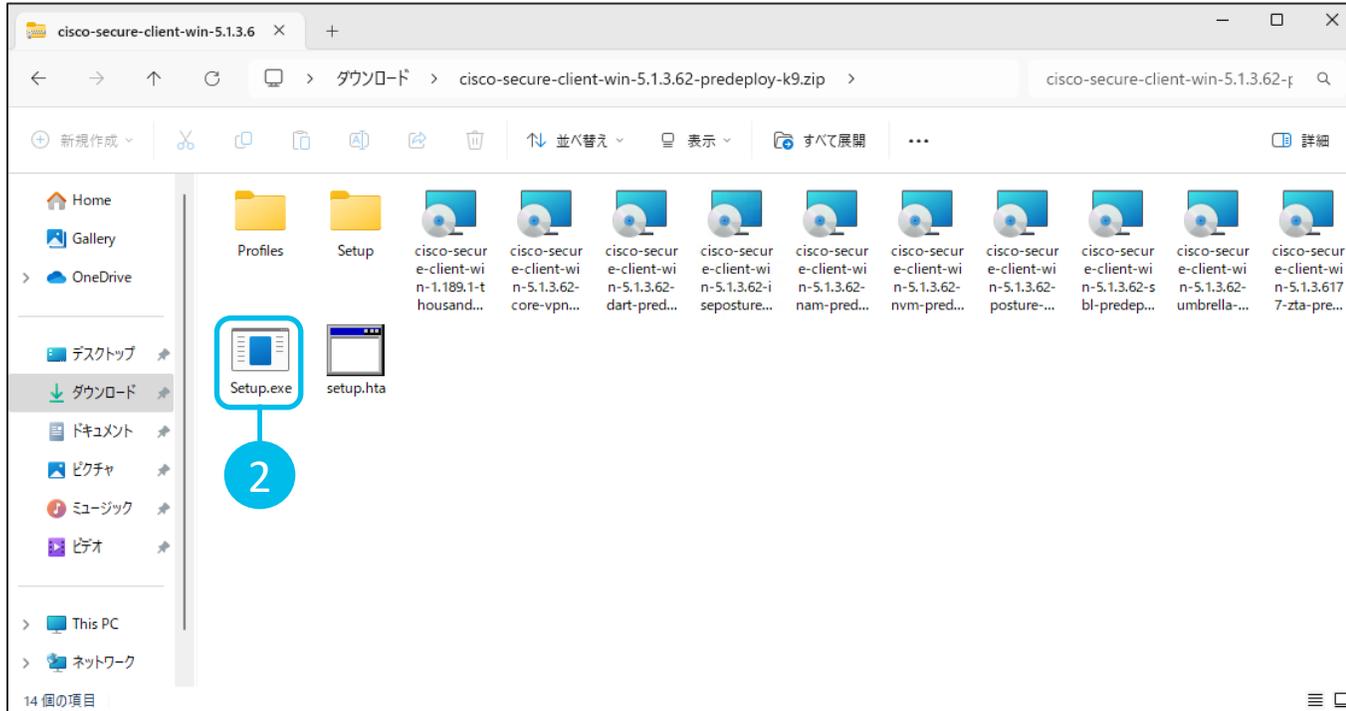


- 1 インストーラ(圧縮ファイル)を解凍
2-⑦ でダウンロードしたインストーラを保存した場所(フォルダ)を開いて、インストーラの圧縮ファイルを解凍※(展開)します。ファイル名は、[**cisco-secure-client-win-5.x.x.xxxx-predeploy-k9**] (拡張子なし表示)または[**cisco-secure-client-win-5.x.x.xxxx-predeploy-k9.zip**] (拡張子あり表示)です。



※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。[ユーザーアカウント制御]ダイアログボックスが表示されます。

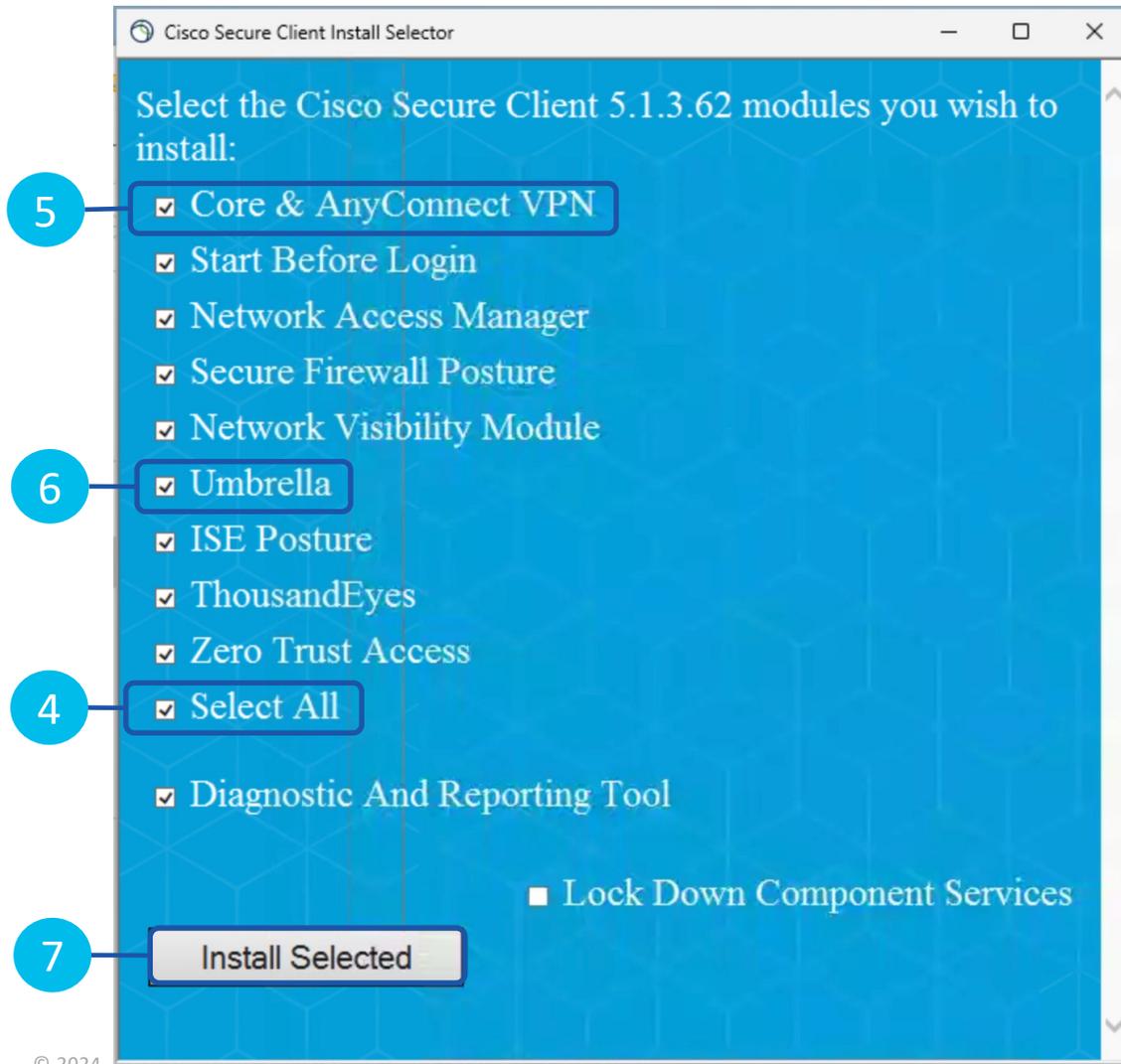


3

[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



5

 Core & AnyConnect VPN Start Before Login Network Access Manager Secure Firewall Posture Network Visibility Module

6

 Umbrella ISE Posture ThousandEyes Zero Trust Access

4

 Select All Diagnostic And Reporting Tool Lock Down Component Services

7

Install Selected

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

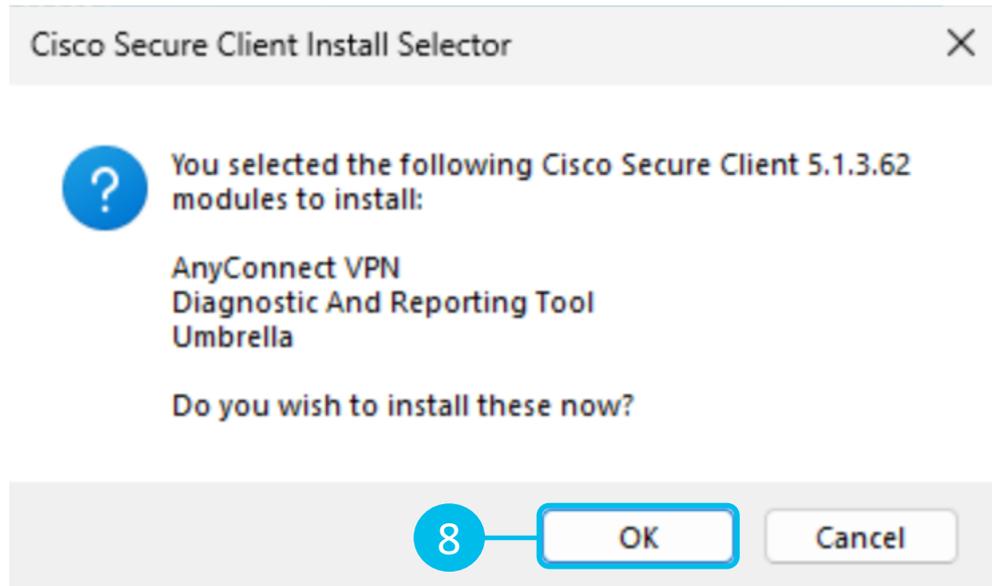
[Umbrella]をクリック

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。

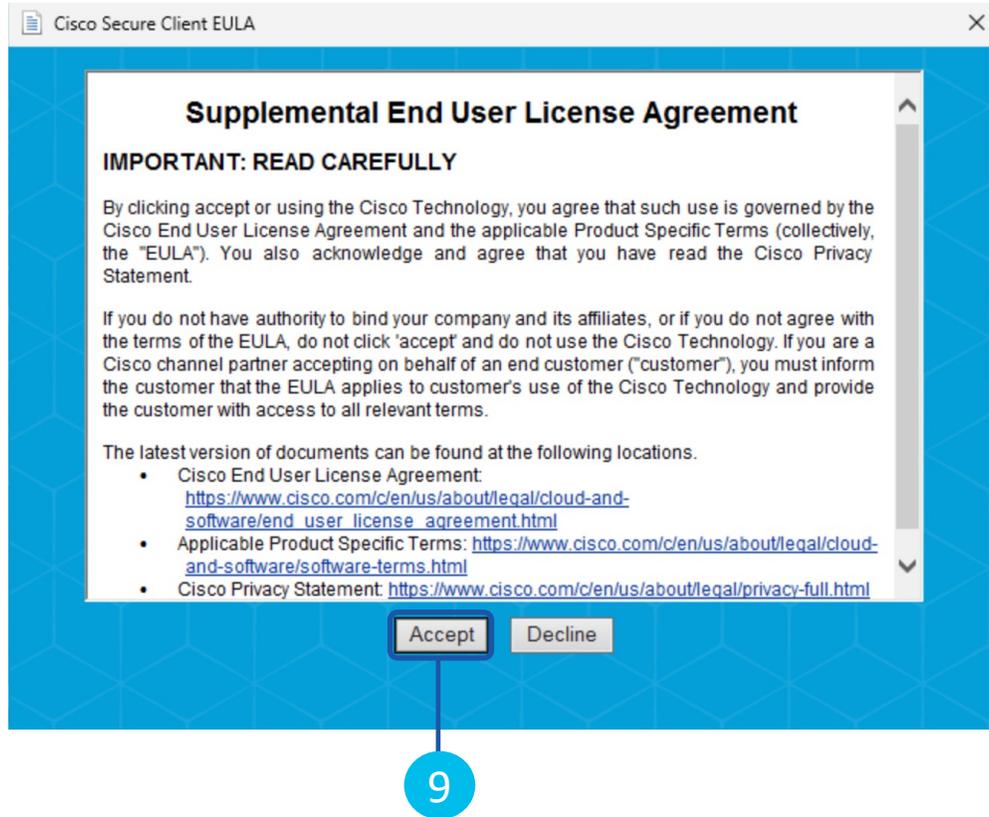
7

[Install Selected]をクリック。

3. Cisco Secure Clientをインストール



3. Cisco Secure Clientをインストール

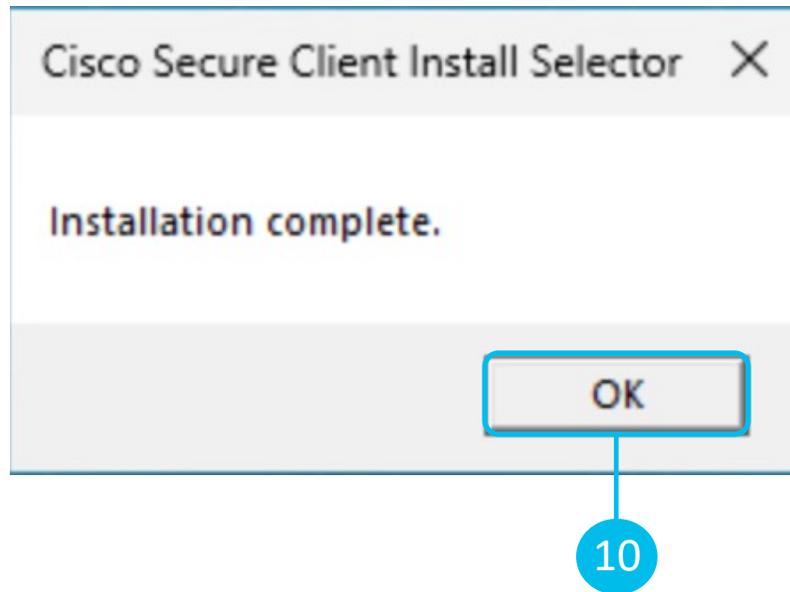


9

[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

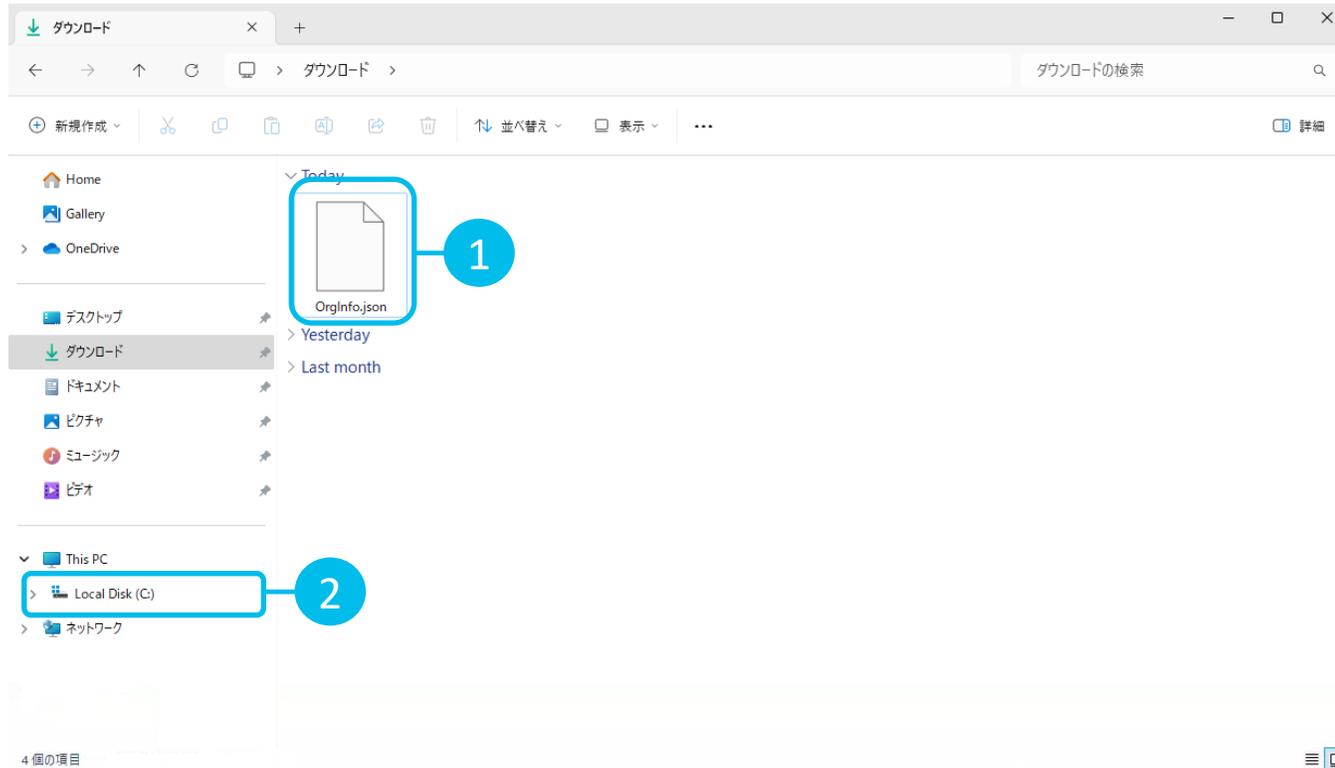
ステップ1: Umbrellaモジュールを有効化

- [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

プロフィールをコピー

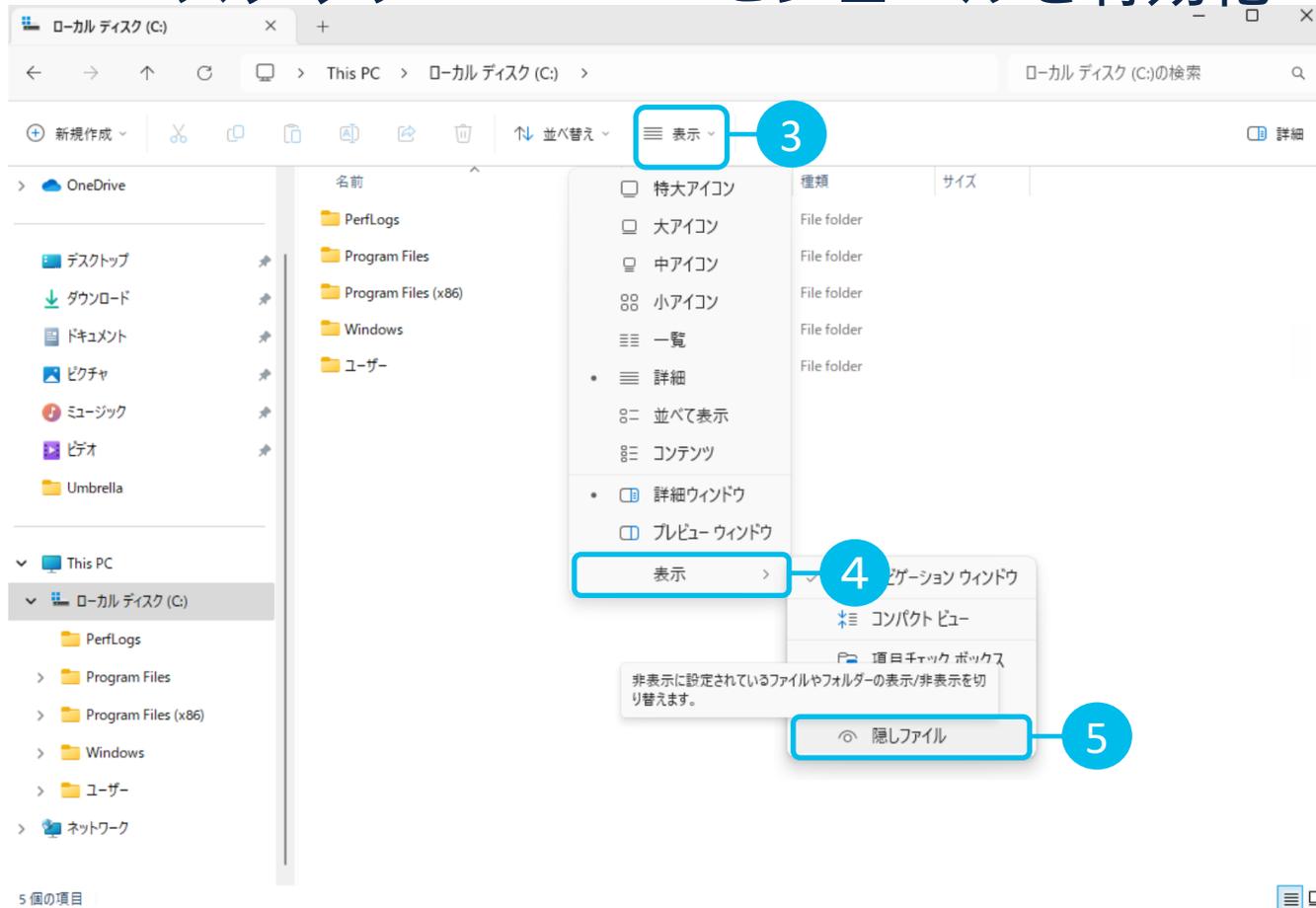
[2-⑧ モジュールのプロファイルをダウンロード]でプロフィールを保存した場所(フォルダ)を開き、プロフィールをコピーします。ファイル名は、[OrgInfo](拡張子なし表示)または[OrgInfo.json](拡張子あり表示)です。

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。

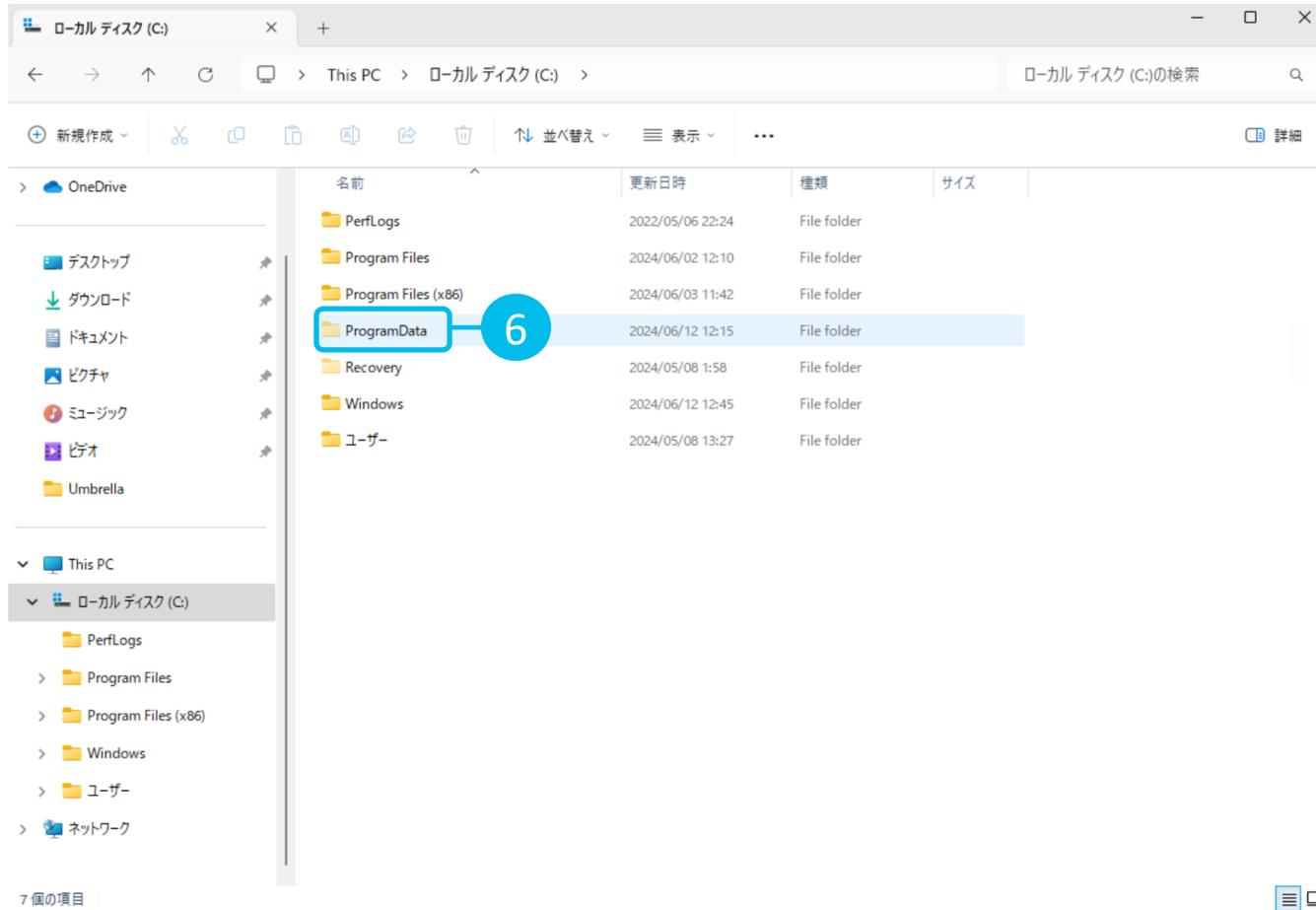
4 (必要に応じて)[表示] をクリック

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

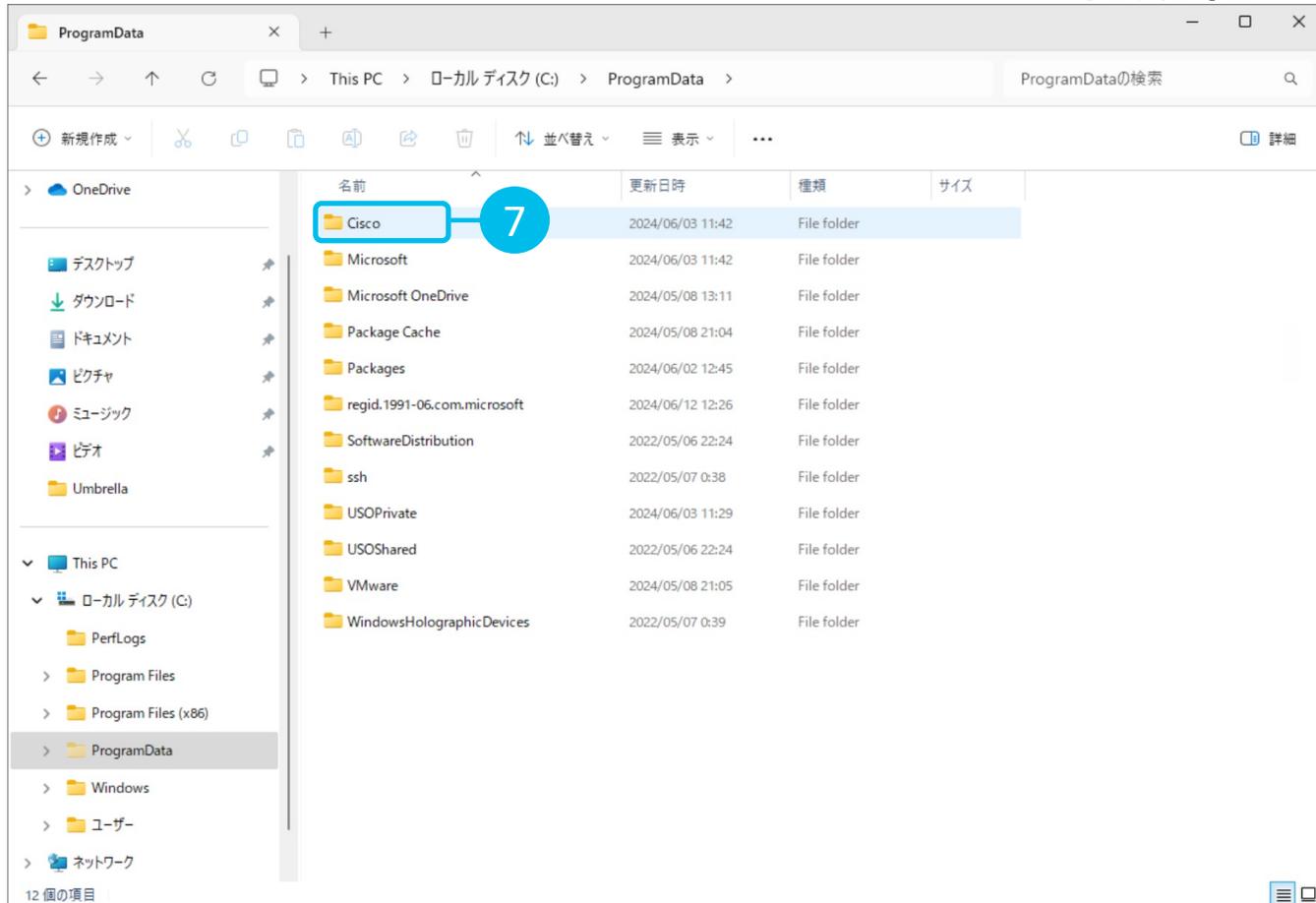


6 [ProgramData]フォルダをクリック

[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

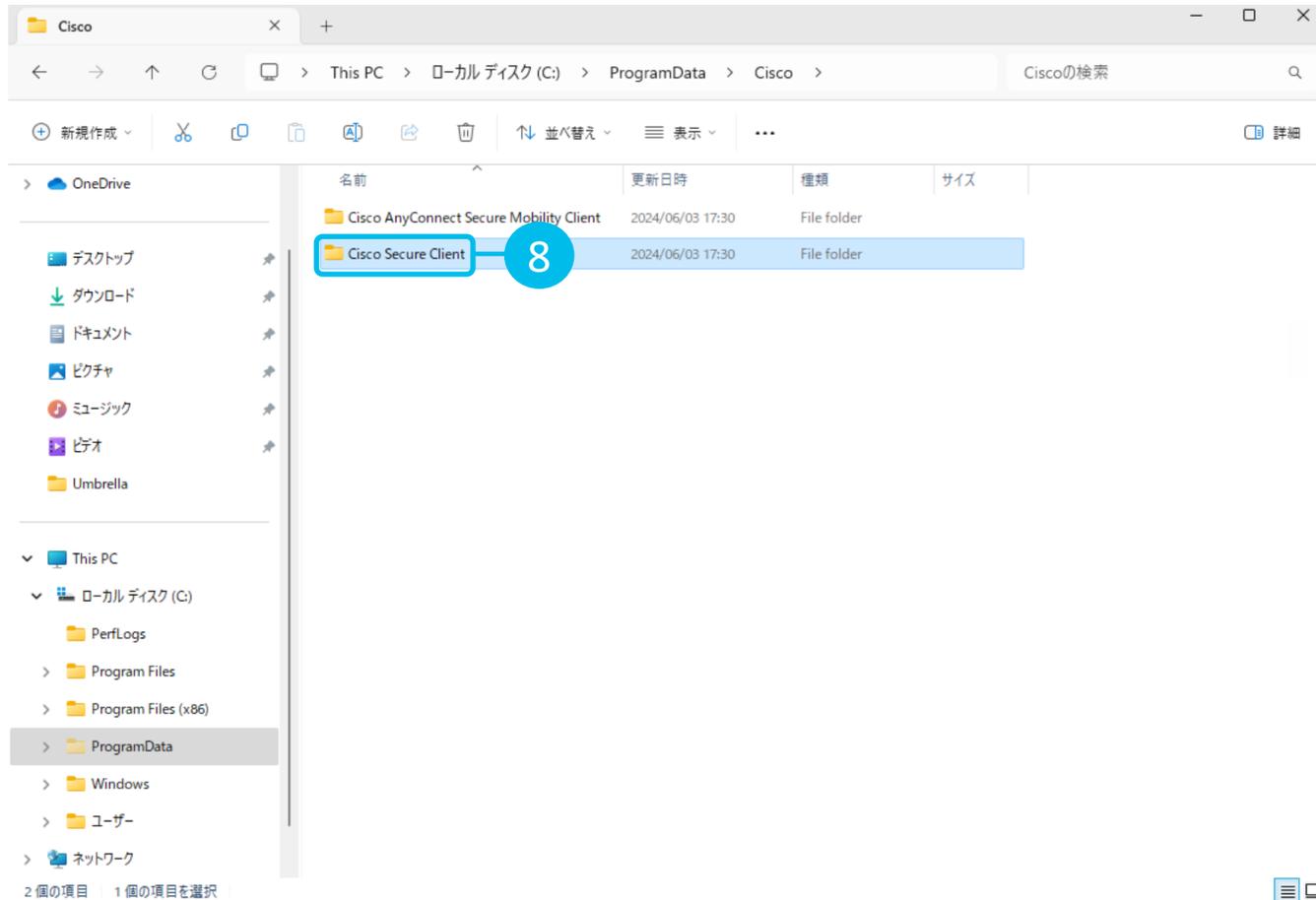
ステップ1:Umbrellaモジュールを有効化



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

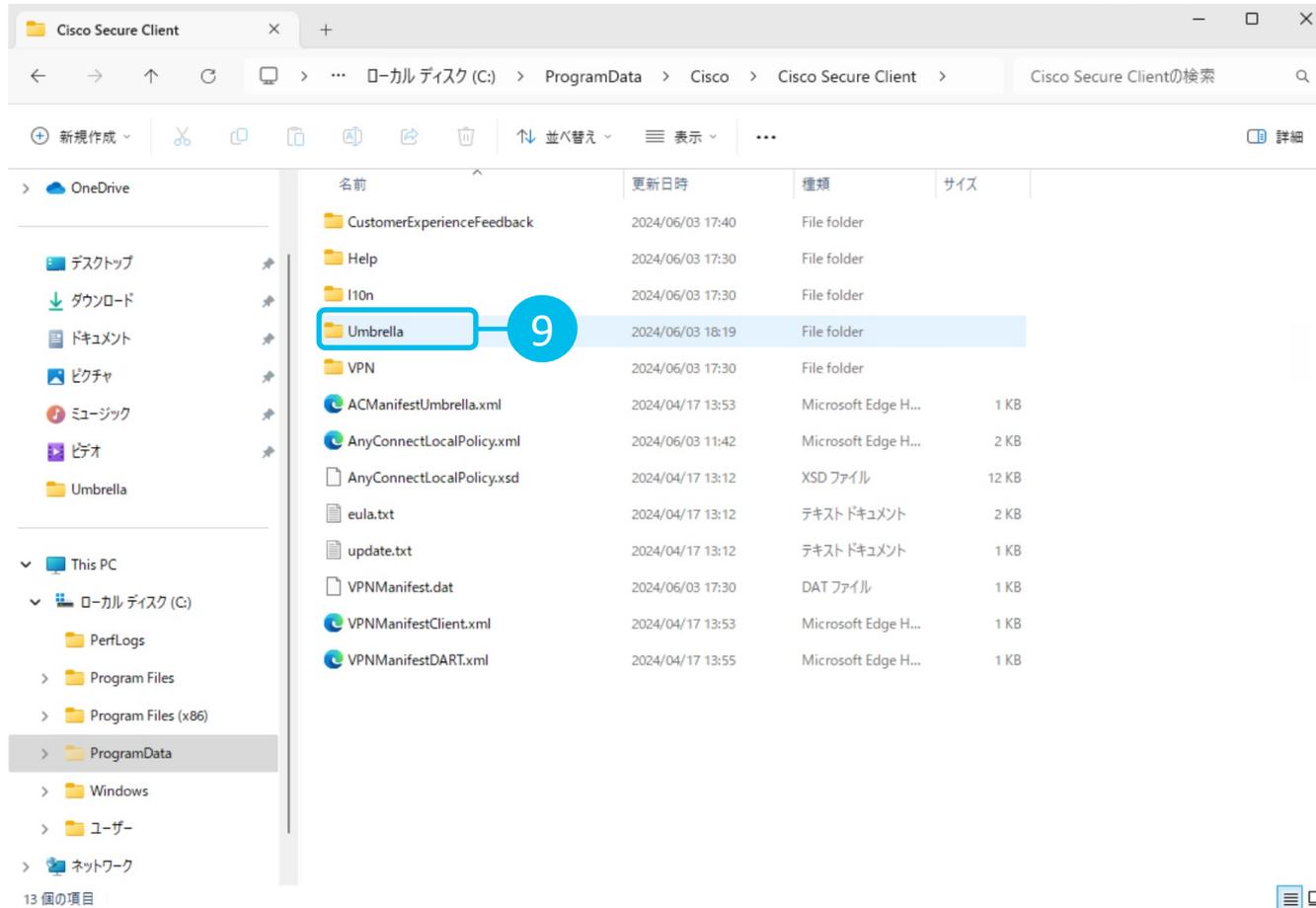


8

[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

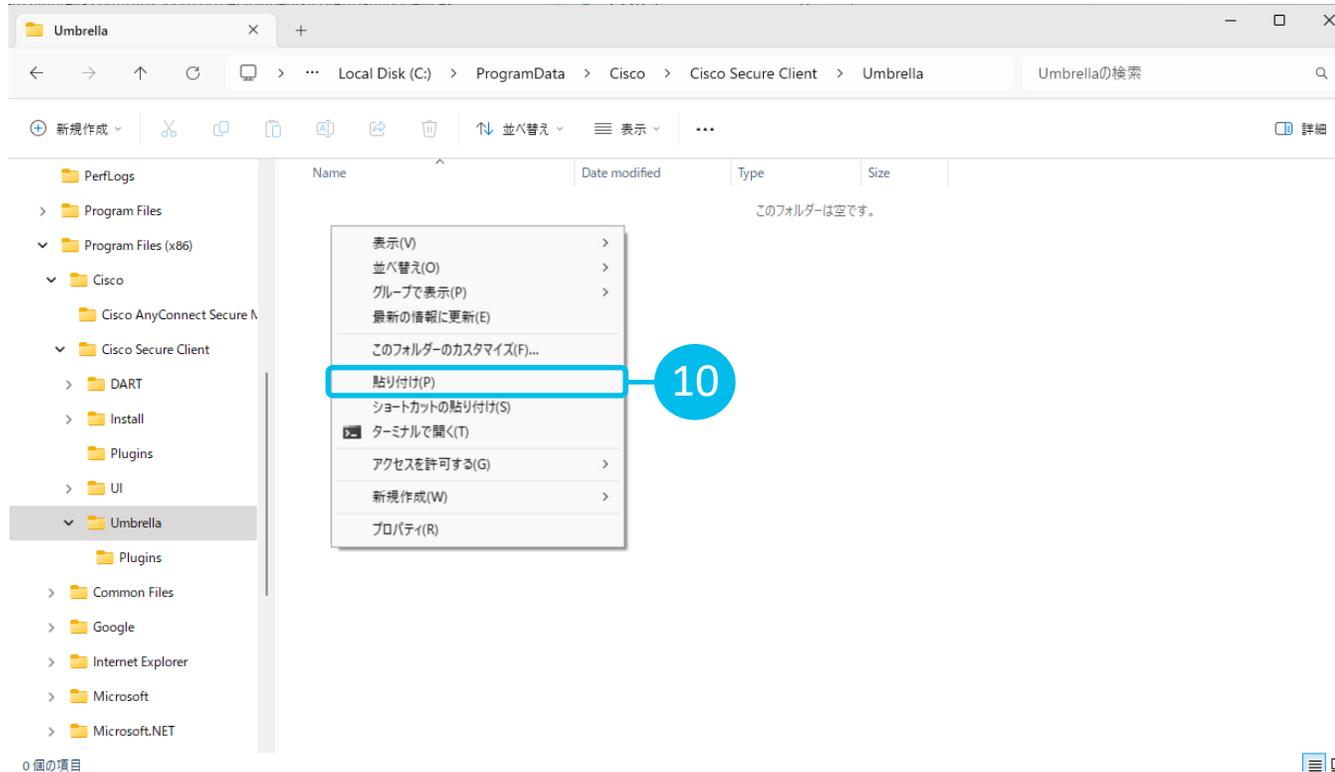


9

[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

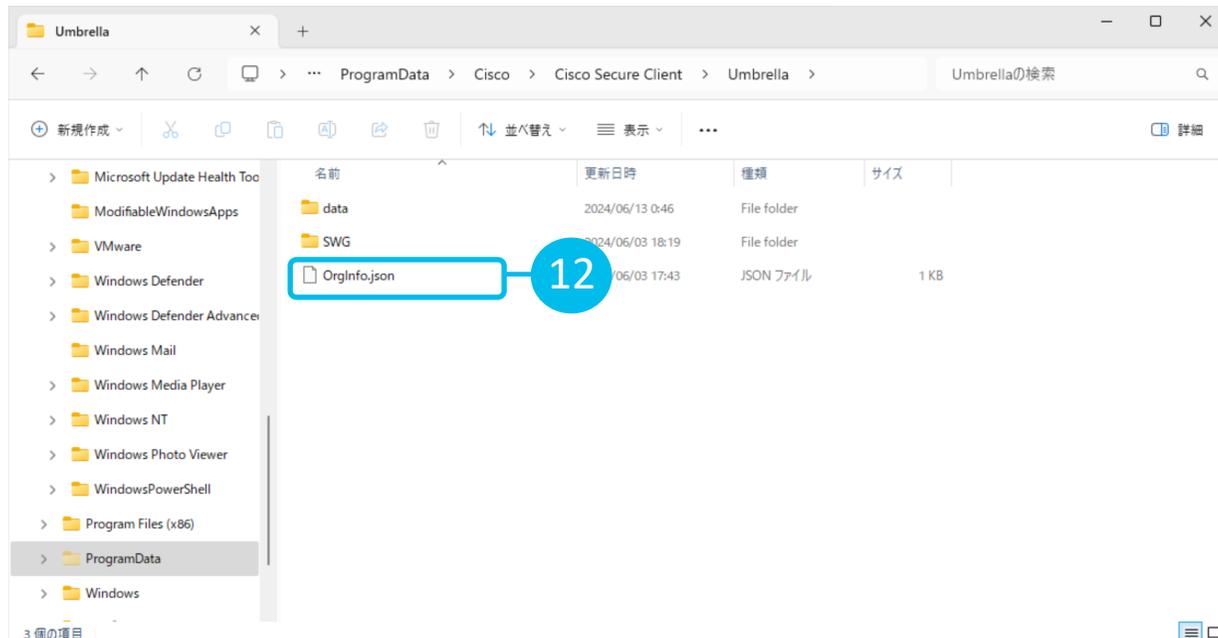
[Umbrella]フォルダにプロファイルをペースト(貼り付ける)すると、[対象のフォルダへのアクセスは拒否されました]ダイアログボックスが表示されます。

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

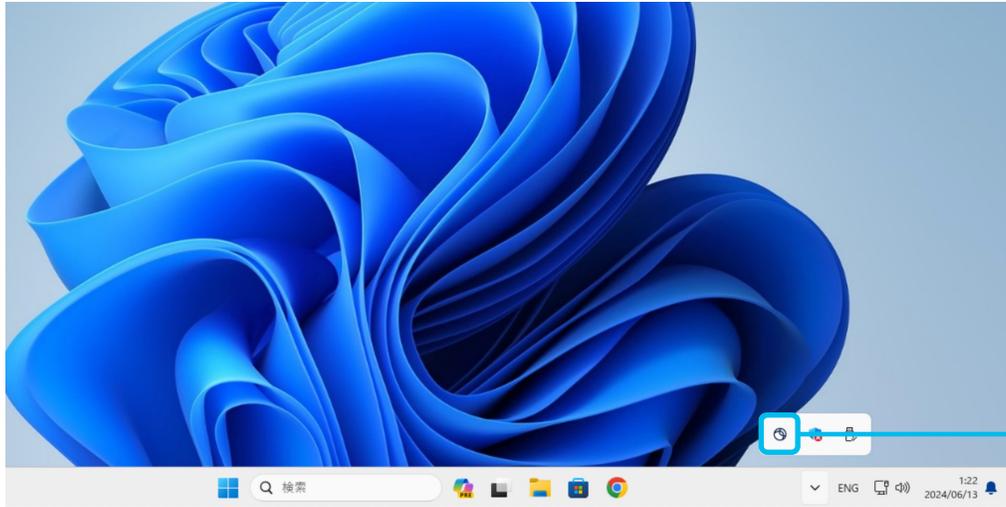


12 プロファイルの配置を確認

[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

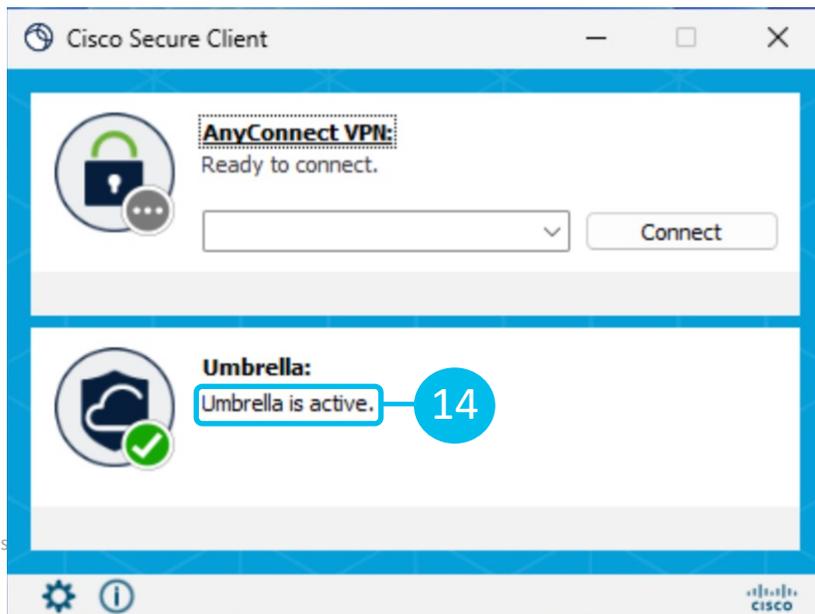


13

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。

13



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

The screenshot shows the Cisco Umbrella dashboard. On the left sidebar, the '導入' (Import) menu item is highlighted with a red circle and the number '1'. The main content area shows a summary of security events, including Malware, Botnet, and Cryptomining blocks. Below this, there are three cards for '導入の健全性' (Import Health): 'アクティブなネットワーク' (0/0 Active), 'アクティブなローミングクライアント' (1/1 Active), and 'アクティブな仮想アプライアンス' (0/0 Active). A warning card for 'アクティブなネットワークトンネル' (非トラッキングデータ) is also visible. At the bottom, there is a 'ネットワークの分析' (Network Analysis) section with a 'すべて' (All) tab selected, showing a total request count of 3225 with a 0% change over the last 24 hours.

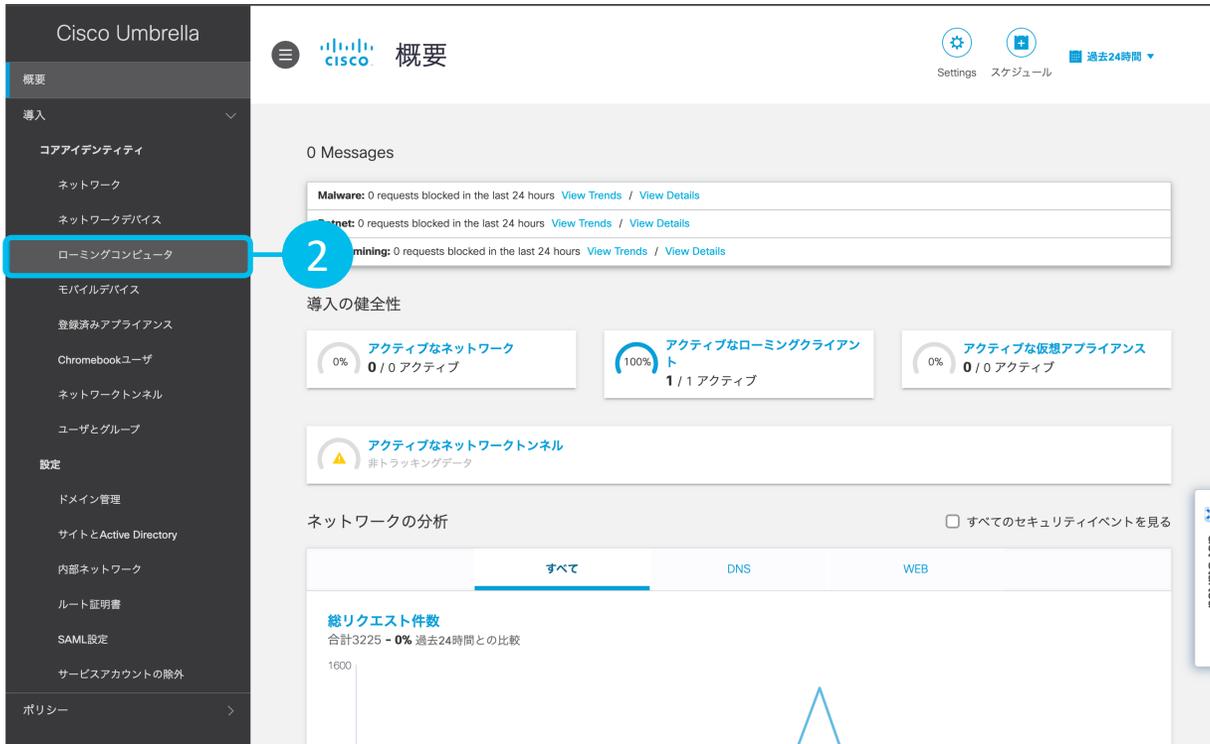
1

[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



The screenshot shows the Cisco Umbrella console interface. On the left, a dark sidebar contains a list of modules. The 'ローミングコンピュータ' (Roaming Computer) module is highlighted with a blue box. A blue circle with the number '2' is overlaid on this item. The main content area shows a summary of security events, including a '0 Messages' section and a '導入の健全性' (Import Health) section with three status cards: 'アクティブなネットワーク' (0/0 Active), 'アクティブなローミングクライアント' (1/1 Active), and 'アクティブな仮想アプライアンス' (0/0 Active). Below this is a 'ネットワークの分析' (Network Analysis) section with a '総リクエスト件数' (Total Request Count) of 3225 and a comparison to the previous 24 hours.

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

Cisco Umbrella

導入 / コアアイデンティティ

ローミングクライアント 設定

ローミングコンピュータ

ローミングコンピュータとは、UmbrellaローミングクライアントまたはCisco Secure Client Umbrellaモジュール(旧AnyConnect)によって保護されるコンピュータを指します。ダッシュボードのこの領域では、管理者は右上のダウンロードボタンを使用してクライアントを展開し、下のローミングコンピュータを管理することができます。

検索

1合計

ID名 ▲	ステータス	タグ	SWG 設定のオーバーライド	前回の同期 ▼
●	オフライン DNSレイヤ暗号化:無効		グローバル設定	5時間前 ▼

ページ: 1 ▼ 各ページの結果数 10 ▼ 1-1/ < >

Get Started

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

Cisco Umbrella

導入 / コアアイデンティティ
Global Settings

Global settings allow for the configuration of globally applied behavioral options for roaming computers. For more information, see Umbrella's [Help](#).

[全般設定 (General Settings)] Umbrellaローミングクライアント 4 Secureローミングクライアント

非アクティブのローミングコンピュータの自動削除
指定された期間同期されていないすべてのローミングコンピュータを自動的に削除します。削除はUmbrellaダッシュボードで行われますが、クライアントソフトウェアはコンピュータから自動的にアンインストールされません。ローミングコンピュータがオンラインに戻ると、削除されていても、再同期するとダッシュボードに再表示されます。
 無効

アクティブディレクトリ
Active Directoryユーザーおよびグループポリシーの適用を有効にします。DNSの場合は、内部IPアドレスの可視性も含まれます。詳細については、[こちらのドキュメントを参照してください](#)。
 有効

VPN互換モード
Windows 10でのVPNクライアントとの互換性が向上する可能性があります。ローカルDNSがVPNで解決されない場合は、この機能をオンにすることも役立つ可能性があります。
 無効

Get Started

[ローミングコンピュータに戻る](#)

4

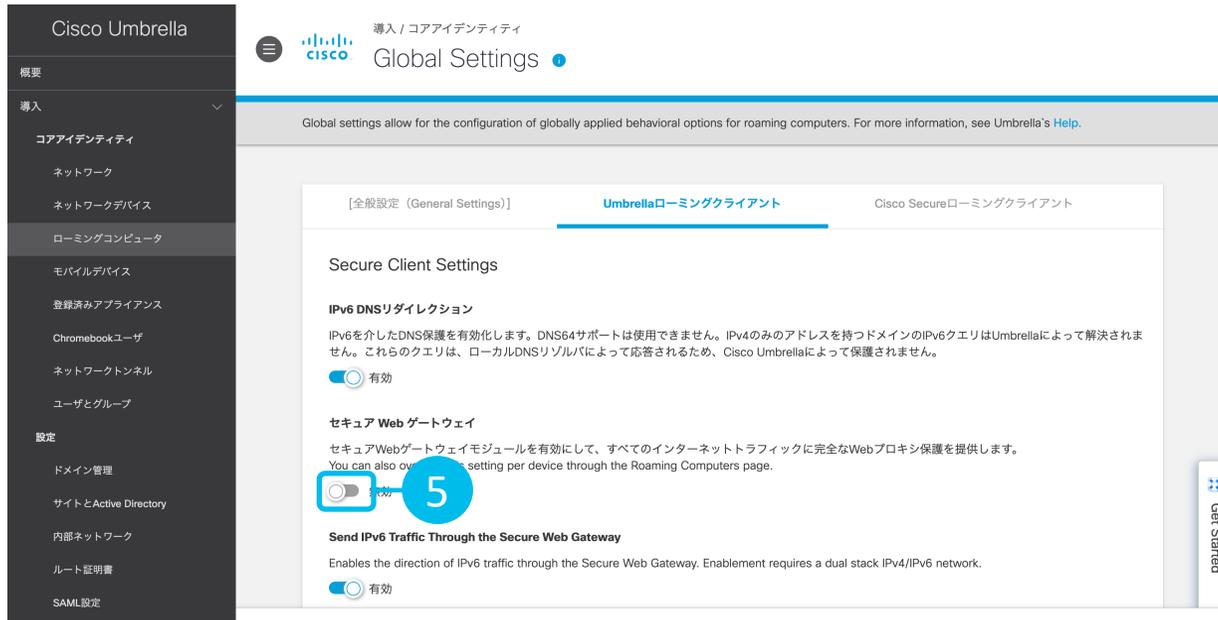
[Umbrellaローミングクライアント] をクリック

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

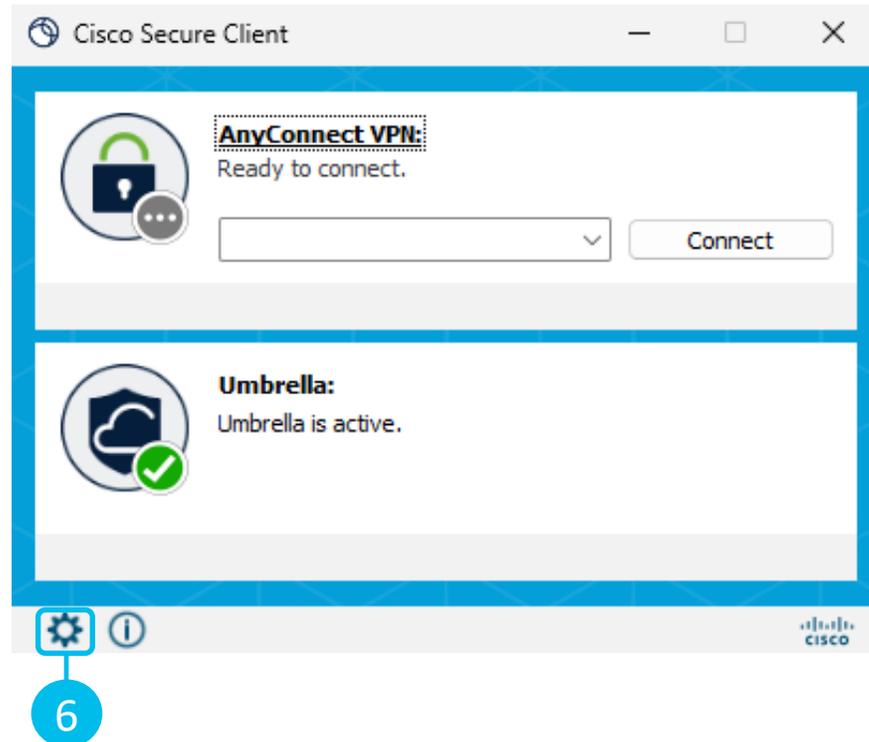
[セキュアWebゲートウェイ] スイッチをクリックしオンにする

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

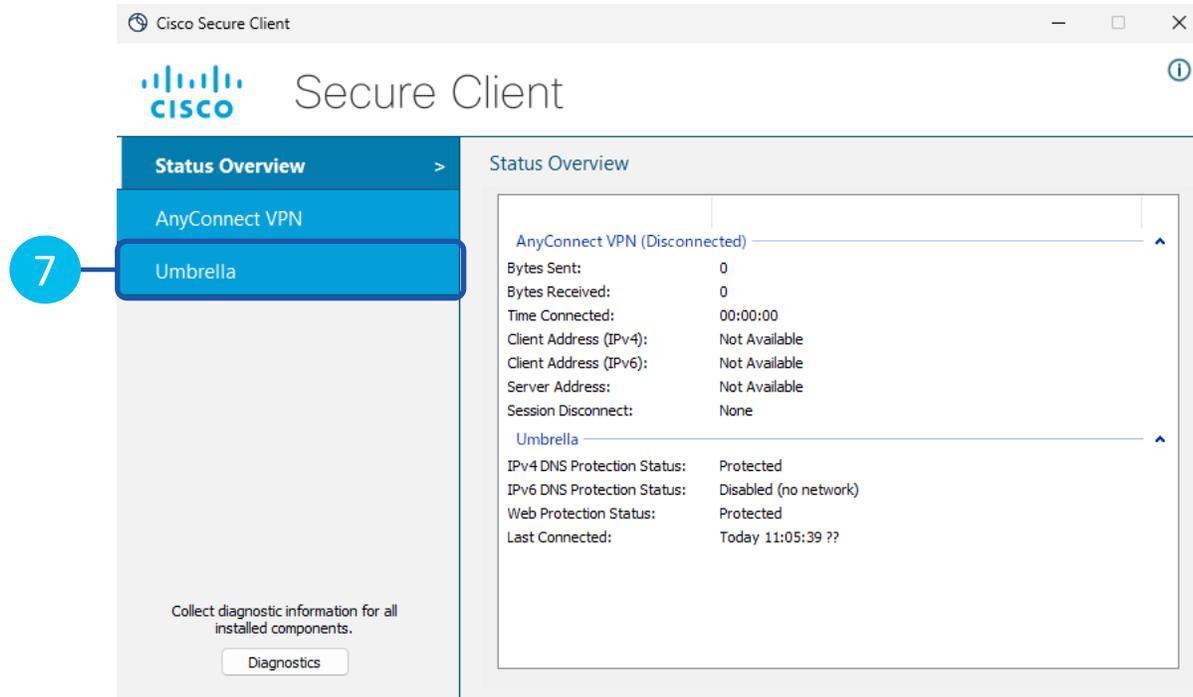


6

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

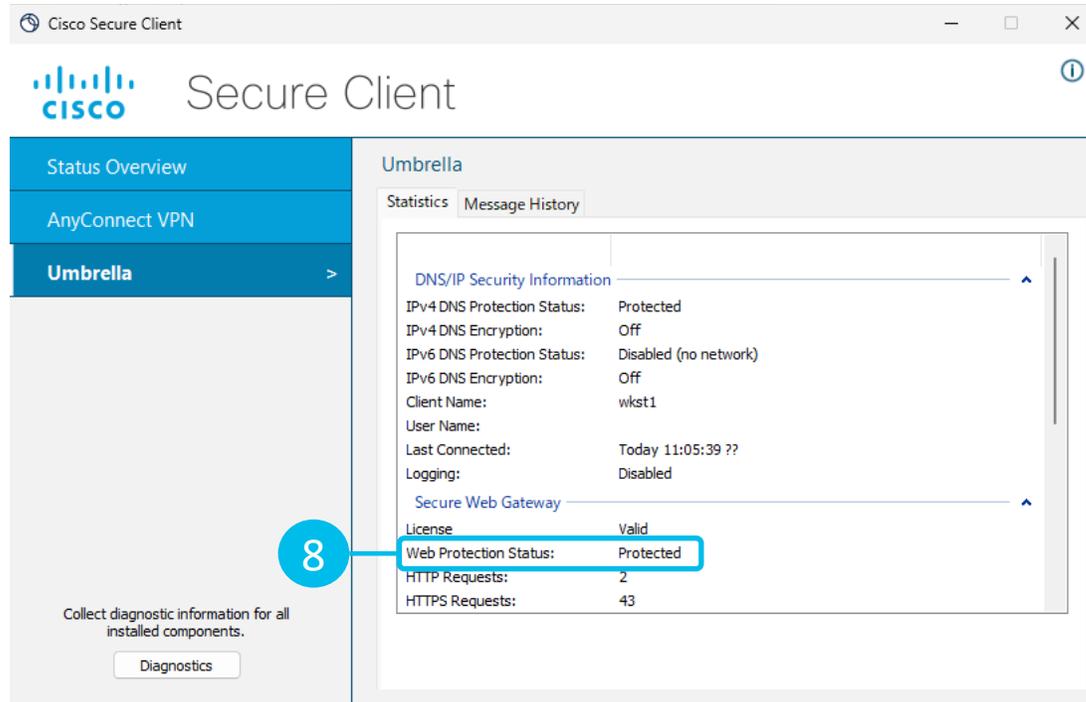


7

[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

The screenshot shows the Cisco Umbrella dashboard. On the left sidebar, the 'Import' button is highlighted with a red circle and the number '1'. The main dashboard area shows a summary of network health and analytics. The 'Import' button is located in the top-left corner of the main content area, next to the 'Messages' section.

1

Cisco Umbrella

概要

導入

ポリシー

レポート

Investigate

管理

0 Messages

導入の健全性

0% アクティブなネットワーク
0 / 0 アクティブ

100% アクティブなローミングクライアント
1 / 1 アクティブ

0% アクティブな仮想アプリ
0 / 0 アクティブ

アクティブなネットワークトンネル
非トラッキングデータ

ネットワークの分析

すべて DNS WEB

総リクエスト件数
合計1641 ▲ 47% 過去24時間との比較

総ブロック
合計0 - 0% 過去24時間との比較

セキュリティブロック
合計0 - 0% 過去24時間との比較

検索結果がありません
検索の時間範囲を拡大してみてください。

検索結果がありません
検索の時間範囲を拡大してみてください。

ファイアウォールの内訳

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

5. ルート証明書をインストールする

The screenshot shows the Cisco Umbrella dashboard. On the left sidebar, the 'ルート証明書' (Route Certificates) menu item is highlighted with a blue circle and the number '2'. The main dashboard area displays various metrics and charts, including '導入の健全性' (Import Health) and 'ネットワークの分析' (Network Analysis).

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

Cisco Umbrella

導入 / 設定 Root Certificate

A root certificate authority (CA) certificate is required in any circumstance where Umbrella must proxy and decrypt HTTPS traffic intended for a website. It is required for Block Pages and HTTPS inspection so that the browser does not present an error page. You can either download and install Umbrella's root CA certificate or add your own CA certificate to Umbrella. Adding your own CA to Umbrella gives you the option of installing your own root CA certificate in a web browser instead of Umbrella's. For more information, see [Manage Certificates](#).

Cisco Root Certificate Authority

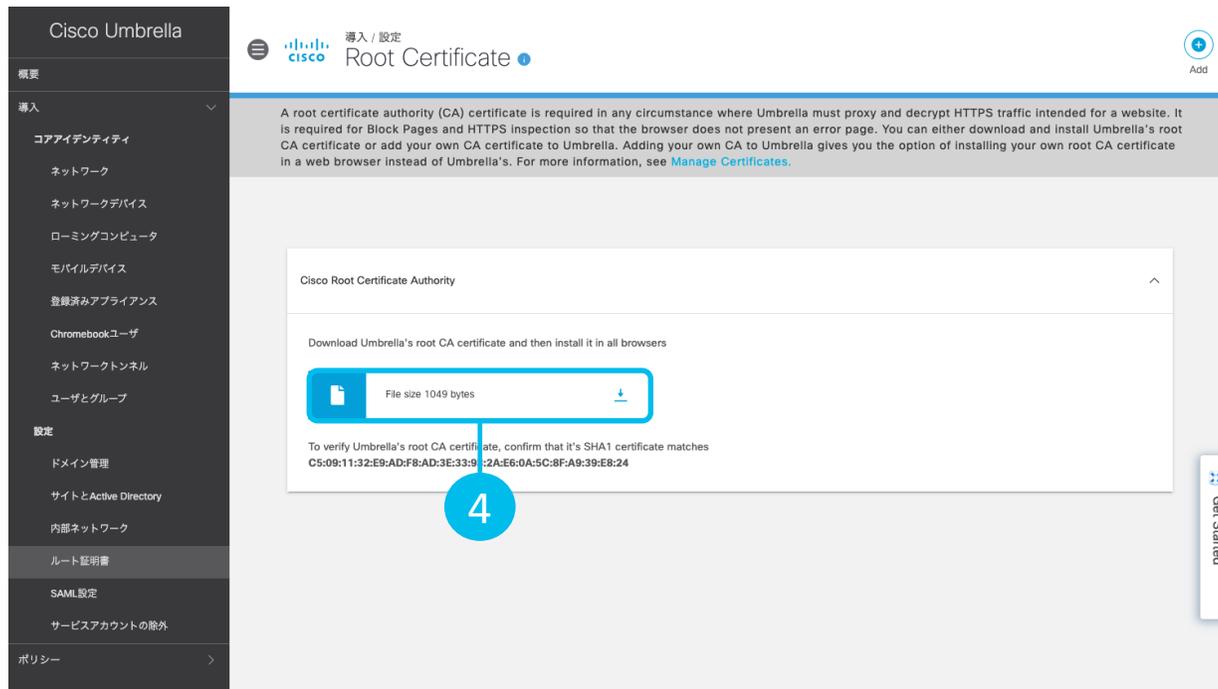
3

Get Started

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



The screenshot shows the Cisco Umbrella management console. The left sidebar contains navigation options like '概要', '導入', '設定', and 'ポリシー'. The main content area is titled 'Root Certificate' and includes an 'Add' button. A text block explains the need for a root certificate authority (CA) certificate. Below this, a 'Cisco Root Certificate Authority' section provides instructions to download and install the certificate. A download button is highlighted with a blue circle and the number '4'. Below the button, a SHA1 certificate match verification string is displayed.

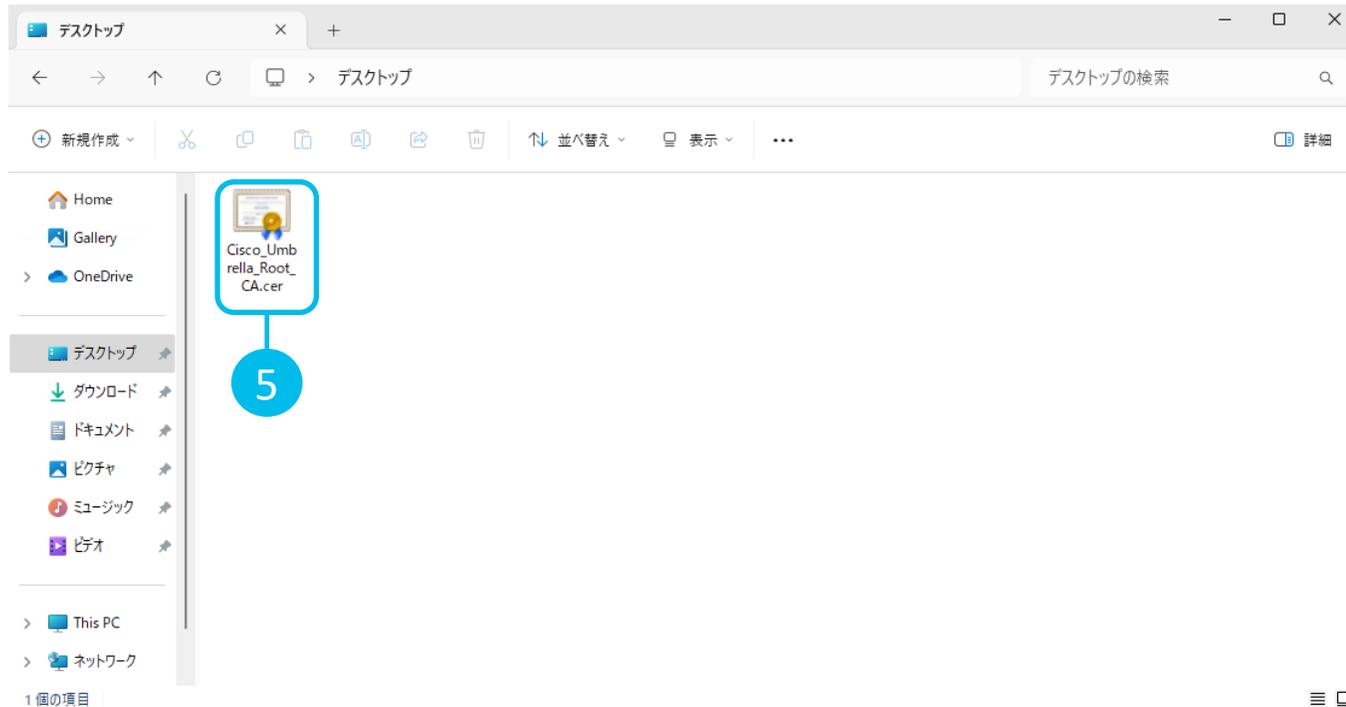
4

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。

5. ルート証明書をインストールする

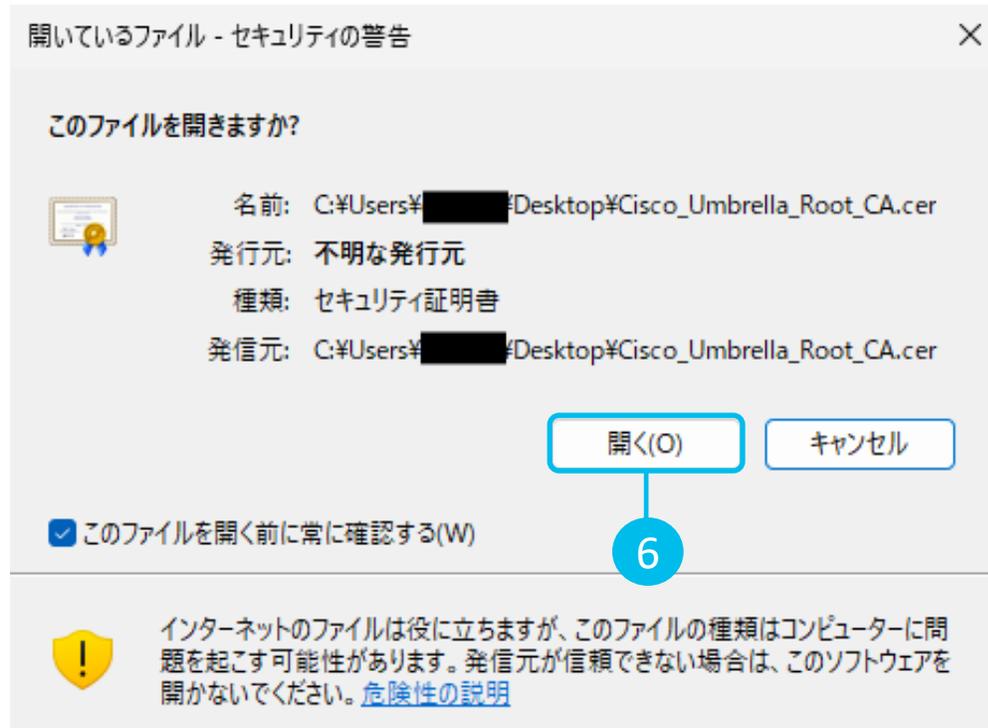


5 ルート証明書をクリック

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

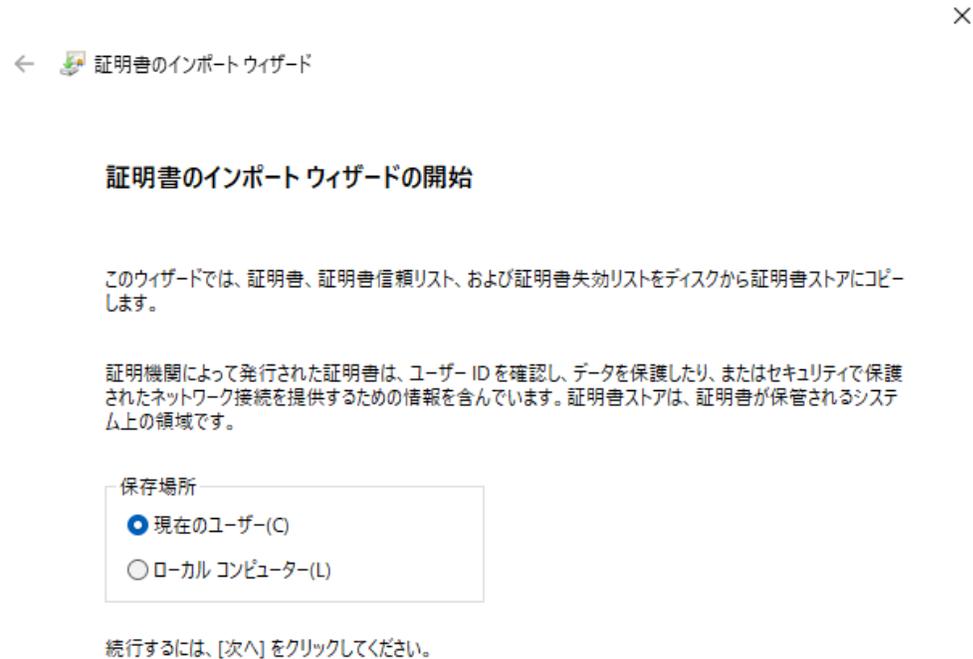
5. ルート証明書をインストールする



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

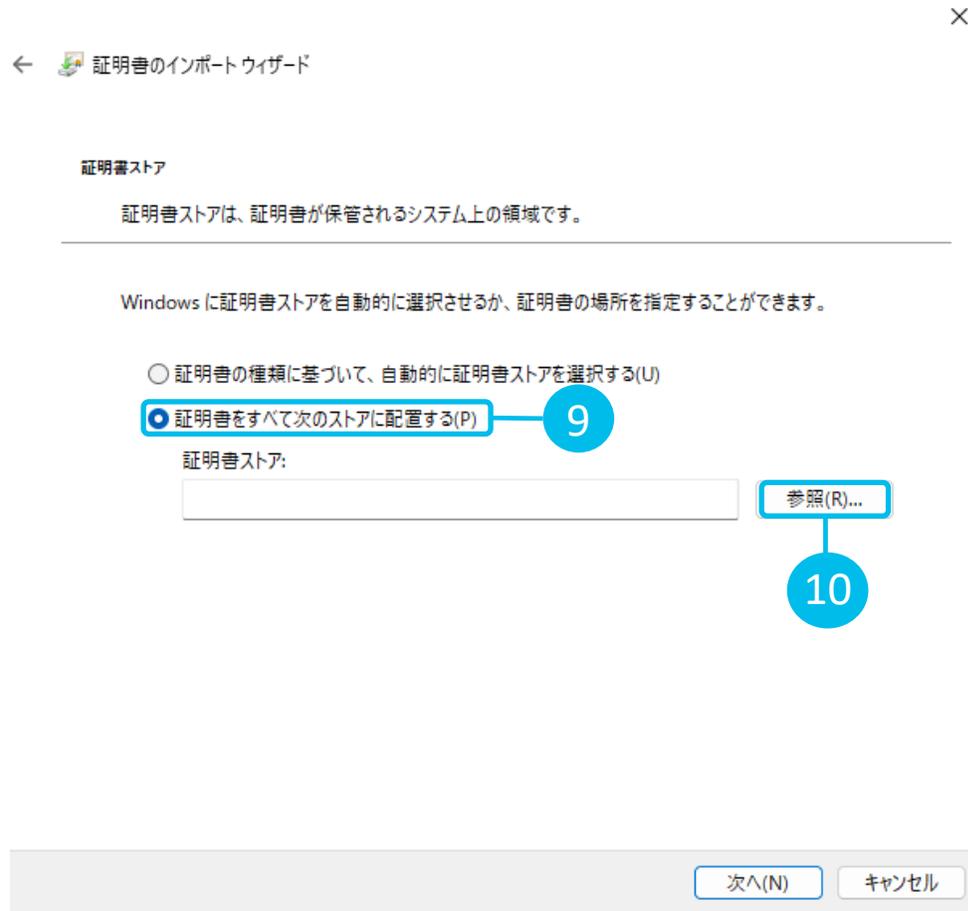


8

[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



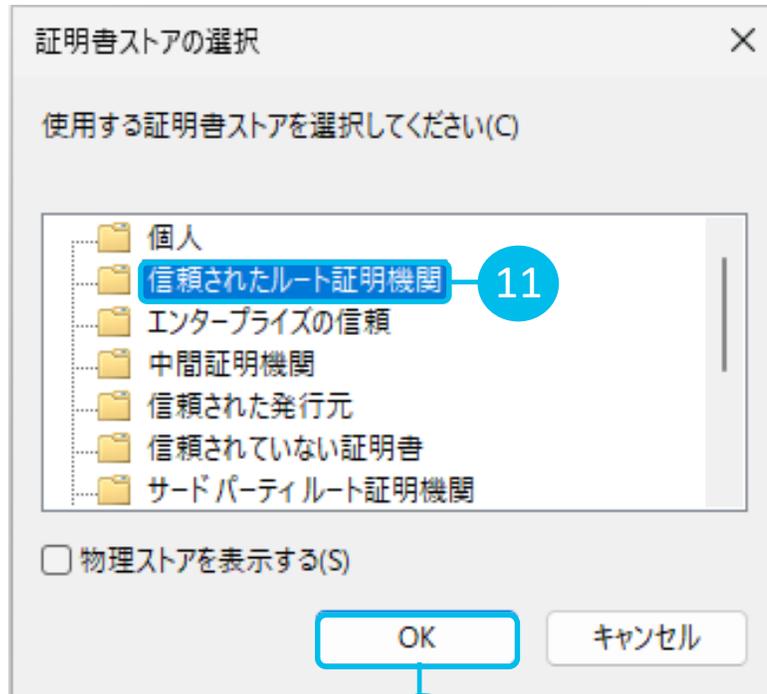
9

[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

13

5. ルート証明書をインストールする

×

←  証明書のインポートウィザード

証明書のインポートウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア 内容	信頼されたルート証明機関 証明書

14 [完了]をクリック

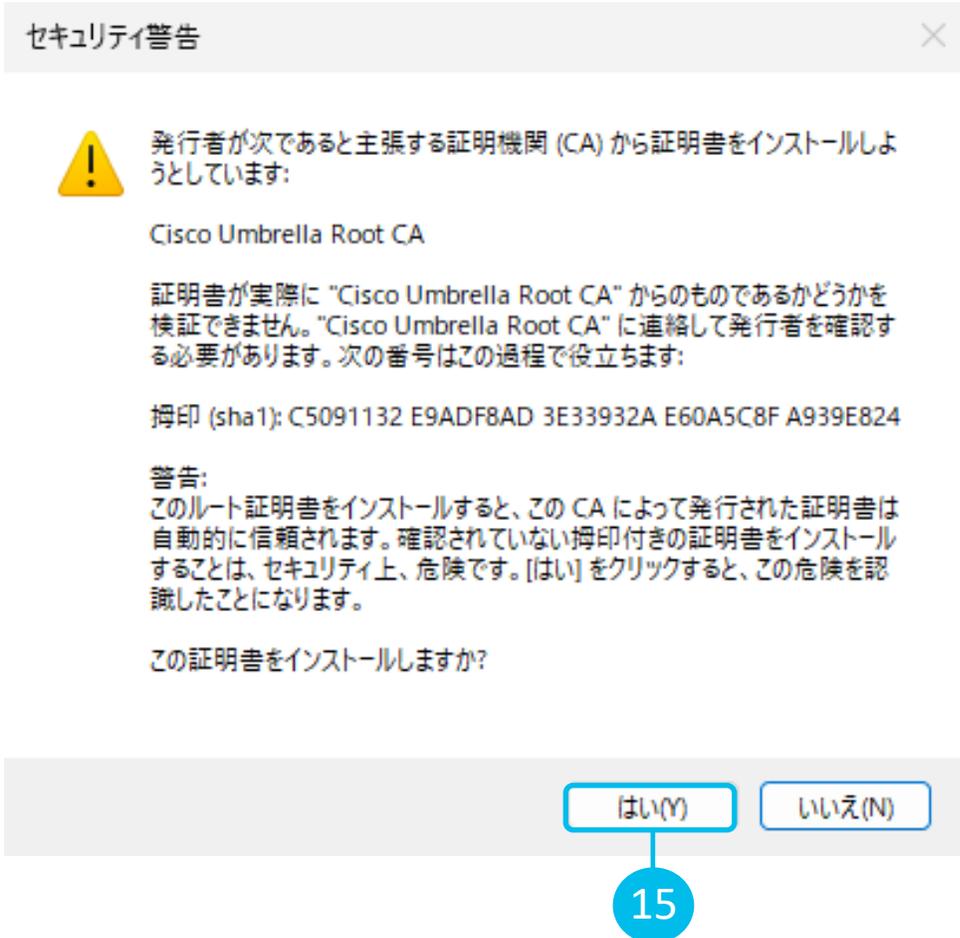
[セキュリティ警告]のダイアログボックスが表示されます。

完了(F)

キャンセル

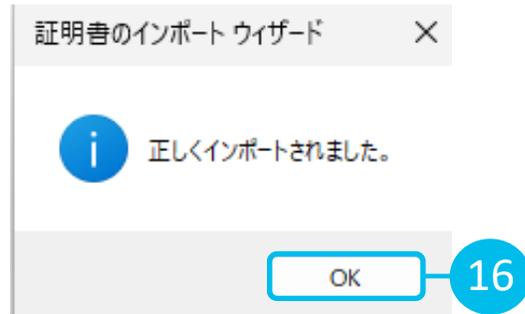
14

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。

The screenshot shows the Cisco Umbrella dashboard interface. On the left, a dark sidebar contains a menu with the following items: 概要 (Overview), 導入 (Onboarding), **ポリシー (Policies)** (highlighted with a red box and a red circle containing the number 1), レポート (Reports), Investigate, 管理 (Management), and a user profile icon. The main content area is titled '概要' (Overview) and displays various security metrics and network analysis tools. A 'Get Started' button is visible on the right side of the dashboard.

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

Cisco Umbrella

概要

導入

ポリシー

管理

2 DNSポリシー

ファイアウォール ポリシー

Web ポリシー

ポリシーコンポーネント

接続先リスト

コンテンツカテゴリ

アプリケーション設定

テナント制御

スケジュール設定

セキュリティ設定

ブロックページ外観

統合設定

選択的復号リスト

レポート

概要

0 Messages

Malware: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Botnet: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

Cryptomining: 0 requests blocked in the last 24 hours [View Trends](#) / [View Details](#)

導入の健全性

0% アクティブなネットワーク
0 / 0 アクティブ

100% アクティブなローミングクライアント
1 / 1 アクティブ

0% アクティブな仮想アプライアンス
0 / 0 アクティブ

アクティブなネットワークトンネル
非トラッキングデータ

ネットワークの分析 すべてのセキュリティイベントを見る

すべて	DNS	WEB
総リクエスト件数 合計2266 ▲ 103% 過去24時間との比較	総ブロック 合計0 - 0% 過去24時間との比較	セキュリティブロック 合計0 - 0% 過去24時間との比較

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 ポリシーテスター

概要

導入 >

ポリシー >

管理

DNSポリシー

ファイアウォール ポリシー

Web ポリシー

ポリシーコンポーネント

接続先リスト

コンテンツカテゴリ

アプリケーション設定

テナント制御

スケジュール設定

セキュリティ設定

ブロックページ外観

統合設定

選択的復号リスト

レポート >

ポリシー / 管理

DNSポリシー

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

適用する順番でソートされています

	保護	適用先	次を含む	最終更新日	
1	DNS ポリシー	すべてのアイデンテ...	3 ポリシー設定	May 29, 2024	✖

Get Started

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

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

保護する方法を選択してください。
アクセス制御のタイプまたはブロックする脅威のタイプを選択します。選択に基づいて、ポリシーで使用可能な機能、レポートの可視性レベルが決定されます。また、選択内容はUmbrella導入環境と一致する必要があります。詳細については、[ここをクリックしてください](#)。

保護対象を選択します。

- アクセスコントロール**
さまざまなカテゴリに基づくブロックング、ピンポイントでのブロックや許可接続先リストでアクセスを制限します。
- コンテンツカテゴリのブロックング**
コンテンツカテゴリに基づいて接続先へのアクセスをブロックします。
- 接続先リストの適用**
リストを作成または変更して、接続先を明示的にブロックまたは許可します。注: グローバルブロックおよびグローバル許可接続先リストは、デフォルトで適用されます。
- アプリケーション制御**
アプリケーションへのアクセスを個別に、またはグループごとにブロックまたは許可します。
- 脅威の阻止**
さまざまなウイルス対策エンジンおよび脅威インテリジェンスを使用して、ネットワークとエンドポイントを保護します。
- セキュリティカテゴリのブロックング**
マルウェア、コマンド&コントロール、フィッシングなどをホストしている場合に、ドメインがブロックされることを確認します。
- ファイル分析**
シグネチャ、ヒューリスティックおよびファイルレピュテーション(Cisco Advanced Malware Protection)により有効化)を使用して、マルウェアに関してファイルを検査します。

▶ **詳細設定**

キャンセル 次へ

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

Cisco Umbrella

ポリシー / 管理
DNSポリシー

概要
導入
ポリシー
管理

DNSポリシー
ファイアウォール ポリシー
Web ポリシー
ポリシーコンポーネント
接続先リスト
コンテンツカテゴリ
アプリケーション設定
テナント制御
スケジュール設定
セキュリティ設定
ブロックページ外観
統合設定
選択的復号リスト
レポート

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できません。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

何を保護しますか?

アイデンティティの選択

アイデンティティの検索

0選択済み

すべてのアイデンティティ

- G Suite OUs
- G Suite Users
- Mobile Devices
- Network Devices
- Networks
- Roaming Computers
- Sites
- Tags

キャンセル 前へ 次へ

Get Started

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

Cisco Umbrella

ポリシー / 管理
DNSポリシー

概要
導入
ポリシー
管理

DNSポリシー
ファイアウォール ポリシー
Web ポリシー
ポリシーコンポーネント
接続先リスト
コンテンツカテゴリ
アプリケーション設定
テナント制御
スケジュール設定
セキュリティ設定
ブロックページ外観
統合設定
選択的復号リスト
レポート

何を保護しますか?

アイデンティティの選択

アイデンティティの検索

0選択済み

すべてのアイデンティティ / Roaming Computers

6

7

キャンセル 前へ 次へ

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



セキュリティ設定

セキュリティ設定を選択または作成することにより、このポリシーを使用するアイデンティティが保護されていることを確認します。[Edit Setting]をクリックして既存の設定を変更するか、ドロップダウンメニューから[Add New Setting]を選択します。

[設定]を選択します

Default Settings

ブロックするカテゴリ

編集

- マルウェア
悪意のあるソフトウェア、ドライブバイダウンロード/エキスプロイト、モバイル脅威をホストしているWeb サイトと他のサーバ。
- 新しく発見されたドメイン
ごく最近アクティブになったドメイン。これらは新手法の攻撃で頻繁に使用されます。
- コマンド&コントロールのコールバック
侵害されたデバイスと攻撃者のインフラストラクチャとの通信を防止します。
- フィッシング攻撃
ユーザをだまして個人情報や金融情報を送信させることを目的とする不正なWebサイト。
- ダイナミックDNS
ダイナミックDNSコンテンツをホストしているサイトをブロックします。
- 損害が発生する可能性があるドメイン
不審な動作を示し、攻撃の一端を担う可能性のあるドメイン。
- DNS トンネリング VPN
ユーザがDNSプロトコルを介したトンネリングによってトラフィックを隠すことを可能にするVPNサービス。これらは、アクセスとデータ転送に関する企業のポリシーを回避するために使用される場合があります。
- クリプトマイニング
クリプトマイニングにより、組織は、マイニングプールとWebマイナーへのクリプトマイナーのアクセスを制御できます。

キャンセル

前へ

次へ

8

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

Cisco Umbrella

概要
導入
ポリシー
管理

DNSポリシー
ファイアウォール ポリシー
Web ポリシー
ポリシーコンポーネント
接続先リスト
コンテンツカテゴリ
アプリケーション設定
テナント制御
スケジュール設定
セキュリティ設定
ブロックページ外観
統合設定
選択的復号リスト
レポート

コンテンツアクセスの制限

コンテンツカテゴリを選択して、そのタイプのコンテンツを提供するWebサイトへのIDアクセスをブロックします。コントロールのプリセットレベルを選択するか、カスタム設定を追加します。カテゴリの詳細については、次のサイトを参照してください [Umbrellaのヘルプ](#)。

高い
アダルトサイト、違法行為のサイト、ソーシャルネットワーク、およびファイル共有Webサイトをブロックします。

中程度
アダルトサイトおよび違法行為のWebサイトをブロックします。

低い
ポルノ、悪趣味、およびプロキシWebサイトをブロックします。

カスタム
手動で選択したコンテンツカテゴリをブロックします。

カテゴリ高い
これらのカテゴリをブロックします。注: 変更する場合には、カスタム設定を作成します

成人向け	アルコール
オークション	大麻
チャットおよびインスタントメッセージング	Child Abuse Content (児童虐待コンテンツ)
出会い系	DoHとDoT
Extreme	Filter Avoidance (フィルタリング回避)
ギャンブル	ゲーム
Hate Speech (憎悪発言)	Illegal Drugs (違法薬物)
Lingerie and Swimsuits (下着および水着)	性的でないヌード オンライン コミュニティ

キャンセル 前へ 次へ

9

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

The screenshot shows the Cisco Umbrella console interface. On the left is a navigation sidebar with categories like '概要', '導入', 'ポリシー', and '管理'. The 'DNSポリシー' option is selected. The main content area displays a configuration wizard for 'アプリケーションの制御' (Application Control). The wizard has five steps: 1. 2 More, 2. アプリケーション (highlighted), 3. 送信先, 4. ファイル分析, 5. 1 More. The 'アプリケーション' step includes a 'Default Settings' dropdown menu and a list of application categories to control, such as Ad Publishing, Anonymizer, Application Development and Testing, Backup & Recovery, Business Intelligence, Cloud Carrier, and Cloud Storage. At the bottom of the wizard are 'キャンセル', '前へ', and '次へ' buttons. A blue circle with the number '10' is overlaid on the '次へ' button.

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

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

3 More 4 送信先 5 ファイル分析 6 ブロックページ サマリー

接続先リストの適用 [新しいリストの追加](#)

このポリシーの適切なブロックや許可の接続先リストを検索したり適用したりします。[新しいリストの追加]をクリックして、接続先リストを作成します。

検索...

すべてを選択 2合計

すべての接続先リスト

- Global Allow List 目的地を見る >
- Global Block List 目的地を見る >

1 ブロック 適用対象リスト

- Global Block List

1 許可 適用対象リスト

- Global Allow List

キャンセル 前へ 次へ

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。

11

6. ポリシーを設定する

DNSポリシー

3 More 送信先 5 ファイル分析 6 ブロックページ サマリー

ファイル分析

静的分析と動的分析の組み合わせを使用して、悪意のある動作のファイルを検査する方法があり、ファイルの評価と高度なヒューリスティックに加えられています。

ファイル検査
シグネチャ、ヒューリスティックおよびファイルレピュテーション(Cisco Advanced Malware Protectionにより有効化)を使用して、マルウェアに関してファイルを検査します。

キャンセル 前へ **次へ**

適用する順番で **12** います

1	Default Policy	保護	適用先	次を含む	最終更新日
		DNS ポリシー	すべてのアイデンテ...	3 ポリシー設定	May 29, 2024

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

3 More 送信先 ファイル分析 **6** ブロックページ サマリー

ブロックページ外観を設定
ブロックページの外観とバイパスオプションを指定します。

Umbrellaのデフォルトの外観を使用
ブロックページのプレビュー

カスタムの外観を使用
既存の外観を選択する

▶ バイパスユーザ
▶ バイパスコード

キャンセル 前へ **次へ**

適用する順番で **13** 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サイトにユーザー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

15

ています。[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ベート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

Cisco Umbrella

ポリシー / 管理

DNSポリシー

追加 ポリシースター

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

適用する順番でソートされています

	保護	適用先	次を含む	最終更新日
1	DNS ポリシー	1 アイデンティティ	3 ポリシー設定	6月 22, 2024
2	DNS ポリシー	適用先 全てのアイデンティ...	3 ポリシー設定	5月 29, 2024

Get Started

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。

Cisco Umbrella

ポリシー / 管理

DNSポリシー

追加 ポリシーテスター 1

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

適用する順番でソートされています

	新しいポリシー	保護 DNS ポリシー	適用先 1 アイデンティティ	次を含む 3 ポリシー設定	最終更新日 6月 22, 2024	▼
1						
2	Default Policy	保護 DNS ポリシー	適用先 すべてのアイデンティ...	次を含む 3 ポリシー設定	最終更新日 5月 29, 2024	▼

Get Started

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

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

ポリシーテスター

接続先がIDに関して許可またはブロックされるかどうかをテストします。予期しない結果を受け取った場合、ポリシーの順序を変更するかポリシーを調整してから、もう一度テストしてください。詳細については、「ポリシーのテスト」を参照してください。

アイデンティティ

例: ローミングコンピュータ、ネットワークデバイス、ユーザ、サイト、ネットワーク、ADグループ(各1つまで)

接続先を入力

リセット テストの実行

テスト結果がここに表示されます

適用する順番でソートされています

1	新しいポリシー	保護	適用先	次を含む	最終更新日
		DNS ポリシー	1 アイデンティティ	3 ポリシー設定	Jun 22, 2024

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

Cisco Umbrella

ポリシー / 管理

DNSポリシー

追加 ポリシーテスター

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

ポリシーテスター

接続先がIDに関して許可またはブロックされるかどうかをテストします。予期しない結果を受け取った場合、ポリシーの順序を変更するポリシーを調整してから、もう一度テストしてください。詳細については、「ポリシーのテスト」を参照してください。

アイデンティティ

例: ローミングコンピュータ、ネットワークデバイス、ユーザ、サイト、ネットワーク、ADグループ(各1つまで)

接続先

注: 現在のURLはサポートされていません

cisco.com

リセット テストの実行

テスト結果がここに表示されます

適用する順番でソートされています

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

Cisco Umbrella

ポリシー / 管理

DNSポリシー

追加 ポリシーテスター

ポリシーによって、セキュリティ保護、カテゴリ設定、および個々の接続先リストが決定されます。接続先リストはアイデンティティの一部またはすべてに適用できます。ポリシーは、ログレベルやブロックページの表示方法も制御します。ポリシーは降順で適用されるため、同じアイデンティティを共有している場合、そのため、同じアイデンティティを共有している場合、最上位のポリシーが2番目のポリシーより前に適用されます。ポリシーの優先順位を変更するには、そのポリシーを目的の順番へ単純にドラッグアンドドロップします。詳細については、Umbrellaのヘルプを参照してください。

ポリシーテスター

接続先がDに許可またはブロックされるかどうかをテストします。予期しない結果を受け取った場合、ポリシーの順序を変更するかポリシーを調整してから、もう一度テストしてください。詳細については、「ポリシーのテスト」を参照してください。

アイデンティティ

例: ローミングコンピュータ、ネットワークデバイス、ユーザ、サイト、ネットワーク、ADグループ(各1つまで)

接続先

注: 現在URLはサポートされていません

注: インテリジェントプロキシが有効な場合、URLが異なる方法で扱われることがあるため、実際の結果は上記と異なる可能性があります。

結果:

接続先が許可されました

トリガー対象のアイデンティティ: [redacted]

送信先: cisco.com

結果: 接続先が許可されました

分類: Business Services, Software/Technology, Computers and Internet

適用されたポリシー: 新しいポリシー

このアイデンティティが次の場所で見つかりました 2 ポリシー。その中から、新しいポリシー ランクの高いポリシーであるため、このアイデンティティに適用されました。もう1つのポリシーはデフォルトポリシーで、常に最もランクの低いポリシーです。

適用する順番でソートされています

適用する順番でソートされています	新しいポリシー	このポリシーを適用	保護	DNS ポリシー	適用先	次を含む	最終更新日
1	新しいポリシー	このポリシーを適用	保護	DNS ポリシー	1 アイデンティティ	3 ポリシー設定	Jun 22, 2024

5

[適用されたポリシー]を確認

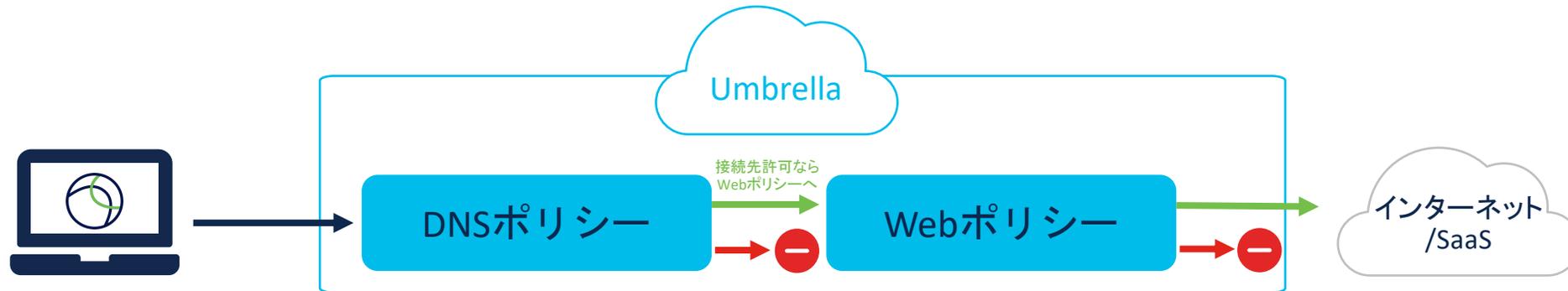
本ガイドの設定例では、「6.ポリシーを設定する(DNSポリシー)¹⁴」で入力したポリシー名が表示されていることを確認※します。

※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

The screenshot shows the Cisco Umbrella dashboard. On the left sidebar, the 'ポリシー' (Policies) menu item is highlighted with a blue box and a red circle containing the number '1'. The main content area displays various security metrics and network analysis tools. At the top right, there are icons for 'Settings' and 'スケジュール' (Schedule), along with a dropdown menu for '過去24時間' (Last 24 hours). The dashboard includes sections for '0 Messages', '導入の健全性' (Import Health), and 'ネットワークの分析' (Network Analysis). The '導入の健全性' section shows three metrics: 'アクティブなネットワーク' (0/0 Active), 'アクティブなローミングクライアント' (1/1 Active), and 'アクティブな仮想アプライアンス' (0/0 Active). The 'ネットワークの分析' section has tabs for 'すべて' (All), 'DNS', and 'WEB', with the 'すべて' tab selected. Below the tabs, there are three cards: '総リクエスト件数' (Total Requests: 2266, +103% vs 24h), '総ブロック' (Total Blocks: 0, -0% vs 24h), and 'セキュリティブロック' (Security Blocks: 0, -0% vs 24h). A 'Get Started' button is visible on the right side of the dashboard.

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

The screenshot shows the Cisco Umbrella management interface. On the left, a dark sidebar contains a menu with the following items: 概要, 導入, ポリシー, 管理, DNSポリシー, ファイアウォール ポリシー, Web ポリシー (highlighted with a blue box and a '2' in a blue circle), ポリシーコンポーネント, 接続先リスト, コンテンツカテゴリ, アプリケーション設定, テナント制御, スケジュール設定, セキュリティ設定, ブロックページ外観, 統合設定, 選択的復号リスト, レポート. The main content area shows a summary of blocked requests for Malware, Botnet, and Cryptomining, all at 0. Below this is a '導入の健全性' (Import Health) section with three cards: 'アクティブなネットワーク' (0/0 active), 'アクティブなローミングクライアント' (1/1 active), and 'アクティブな仮想アプライアンス' (0/0 active). A 'ネットワークの分析' (Network Analysis) section is partially visible at the bottom.

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

	次を含む	最終更新日
1 Default Web Policy	-	Jun 22, 2024

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは隣順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

ルールセットが無効になっています。このルールセットを有効にするには、少なくとも1つのルールセットアイデンティティを選択して、その設定とルールが評価および適用されるようにする必要があります。

ルールセットルール

ルールの追加

いいえ ルールを 追加。

ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	ルールセット 1	編集
ルールセットアイデンティティ ▲	0 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集
HTTPS 検査	無効	編集
PAC ファイル	https://proxy.prod.pac.swg.umbrella.com/...	編集
セーフサーチ	無効	編集
ルールセットのロギング	すべての要求をロギング	編集
SAML	無効	編集
セキュリティ設定	3個の設定が有効化されました	編集

ルールセット
ルール

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。

ルールセット

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

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを紹介する必要があります。

ルールセット名	Web Policy1	保存
ルールセットアイデンティティ ⚠	0 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集
HTTPS 検査	無効	編集
PAC ファイル	https://proxy.prod.pac.swg.umbrella.com/...	🔗
セーフサーチ	無効	編集
ルールセットのロギング	すべての要求をロギング	編集
SAML	無効	編集
セキュリティ設定	3個の設定が有効化されました	編集

削除 閉じる

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

ルールセットアイデンティティ

このルールセットに追加するルールセット アイデンティティ を選択し、このルールセットを有効にする必要があります。ルールセットに一致する アイデンティティ は、ルールセット内のルールに対して評価されます。これは、ルール・セット アイデンティティ とルール アイデンティティ の間の論理 AND の効果を持ちます。アイデンティティ は、まず [アイデンティティ] ページを通じてアンブレラに追加されず。詳細については、Umbrella のを参照してください [ヘルプ](#)。

すべてのアイデンティティ

- Chromebooks
- G Suite OUs
- G Suite Users
- Tunnels
- Networks
- Roaming Computers **8**
- Internal Networks (All Tunnels)

0 選択済み

[キャンセル](#) [保存](#)

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

ルールセットアイデンティティ

このルールセットに追加するルールセット アイデンティティ を選択し、このルールセットを有効にする必要があります。ルールセットに一致する アイデンティティ は、ルールセット内のルールに対して評価されます。これは、ルール・セット アイデンティティ とルール アイデンティティ の間の論理 AND の効果を持ちます。アイデンティティ は、まず [アイデンティティ] ページを通じてアンブレラに追加されます。詳細については、Umbrella のを参照してください [ヘルプ](#)。

すべてのアイデンティティ / Roaming Computers

 [redacted]

9

 [redacted]

1 選択済み

[すべて削除](#)

 [redacted]

[キャンセル](#)

[保存](#)

10

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

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	Web Policy1	保存
ルールセットアイデンティティ	1 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集
HTTPS 検査	無効	編集
PAC ファイル	https://proxy.prod.pac.swg.umbrella.com/...	🔗
セーフサーチ	無効	編集
ルールセットのロギング	すべての要求をロギング	編集
SAML	無効	編集
セキュリティ設定	3個の設定が有効化されました	編集

削除 閉じる

11

[HTTPS検査]の[編集]をクリック

Get Started

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

HTTPS 検査

このルールセットの HTTPS トラフィックを Umbrella で処理する方法を選択します。詳細については、Umbrella のを参照してください [ヘルプ](#)。

12

HTTPSトラフィック検査の有効化

HTTPSトラフィックが代行受信および復号され、セキュリティとルールセットがURLレイヤで適用され、URLパスが可視化されます。デフォルトでは、HTTPSインスペクションがすべてのHTTPSトラフィックの復号を試みます。HTTPSインスペクションをバイパスするには、選択的復号リストを追加します。

HTTPS 経由でブロック ページを表示する

この機能は、ブロックされたトラフィックを完全に検査するわけではありませんが、ブロックがドメインレベルで決定された後、トラフィックを検査して HTTPS 経由でブロック ページ ブロック ページを表示します。Umbrella ルート CA の展開またはカスタム CA の展開は、ブロックページへのブラウザリダイレクトを実行するために引き続き必要です。

HTTPSトラフィック検査の無効化

HTTPS トラフィックは傍受されません。ドメインレイヤのセキュリティとルールセットの適用は引き続き適用されます。ドメインレイヤーの可視性のみが可能です。

キャンセル

保存

13**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

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	Web Policy1	編集
ルールセットアイデンティティ	1 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集
HTTPS 検査	有効	編集
PAC ファイル	https://proxy.prod.pac.swg.umbrella.com/...	🔗
セーフサーチ	無効	編集
ルールセットのロギング	すべての要求をロギング	編集 14
SAML	無効	編集
セキュリティ設定	3個の設定が有効化されました	編集

削除 閉じる

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

ルールセットのロギング

このルールセットのアンブレラ ログを決定します。詳細については、Umbrella のを参照してください [ヘルプ](#)。

ログ要求

コンテンツ、セキュリティ、その他の理由で、このルールセットの要求の完全なログ記録を有効にします。無効にすると、要求は報告も警告も行いません。報告されていないイベントは匿名でログに記録され、検索および脅威インテリジェンスの目的で集計されます。

15 セキュリティ イベントのみのログ

セキュリティフィルターまたは統合に一致するリクエストのみをログに記録してレポートする場合に選択します。他のリクエストに関するレポートはありません。

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。

キャンセル

保存

16

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

ルールセット名	Web Policy1	編集
ルールセットアイデンティティ	1 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類別のコントロール	無効	編集
HTTPS 検査	有効	編集
PAC ファイル	https://proxy.prod.pac.swg.umbrella.com/...	🔗
セーフサーチ	無効	編集
ルールセットのロギング	セキュリティ イベントのみのログ	編集
SAML	無効	編集
セキュリティ設定	3個の設定が有効化されました	編集

削除 閉じる

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

番号	名前	ルール数	最終更新日
1	Web Policy1	1 ルール	Jun 25, 2024
2	Default Web Policy	-	Jun 22, 2024

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。

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
	新しいルール 1	ブロック	選択なし アイデンティティを追加する	選択なし 宛先を追加	任意の日、いつでも 変更スケジュール 追加の設定は適用されません 保護されたファイルのバイパスが無効 ① アンプレラブロックと警告ページ (継承) ② 編集

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

Cisco Umbrella

ポリシー / 管理

Web ポリシー

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
	新しいルール1	ブロック	選択なし アイデンティティを追加する	選択なし 宛先を追加	任意の日、いつでも 変更スケジュール 保護されたファイルのパスが無効 アンブレラブロックと警告 ページ (継承) 編集

2

3

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

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

The screenshot shows the Cisco Umbrella management console. On the left is a navigation menu with 'Web ポリシー' selected. The main area is titled 'Web Policy1' and 'ルールセットルール'. A table lists rule sets with columns for priority, name, action, identity, destination, and configuration. A 'Rule1' entry is highlighted with a blue box. A modal window is open over 'Rule1', showing a dropdown menu with 'ブロック' selected. A blue circle with the number '4' is overlaid on the 'ブロック' option. The modal also displays a '許可 - 実施されたセキュリティ' (Allow - Applied Security) section with a warning icon and a '警告' (Warning) section with a warning icon. A '保存' (Save) button is visible in the top right of the modal.

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

Web Policy1 次を含む 最終更新日 Jun 24, 2024

ルールセットルール

ルールの追加

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
...	Rule1		選択なし アイデンティティを追加する	選択なし 宛先を追加	任意の日、いつでも 変更スケジュール 追加の設定は適用されません 保護されたファイルのバイパスが無効 アンブレラブロックと警告ページ (継承) 編集

5

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	Web Policy1	編集
ルールセットアイデンティティ	1 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
コメント	1行のコメントが有効化されています	編集

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

Cisco Umbrella

ポリシー / 管理

Web ポリシー

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

1 Web Policy1 次を含む 最終更新日 Jun 24, 2024

ルールセットルール

ルールの追加

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
...	Rule1	ブロック	ルールセット アイデンティティ	宛先を追加	任意の日、いつでも 変更スケジュール 追加の設定は適用されません 保護されたファイルのバイパスが無効 アンプレラブロックと警告ページ (継承) 編集

Get Started

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

The screenshot shows the Cisco Umbrella Web Policy configuration page. On the left is a navigation menu with 'Web ポリシー' selected. The main area is titled 'Web Policy1' and 'ルールセットルール'. A 'ルールの追加' button is visible. A table lists rules, with 'Rule1' selected. A dialog box titled '送信先' (Destination) is open, showing a list of options: 'Application Settings' (4894), 'Content Categories' (103), and 'Destination Lists'. A blue circle with the number '9' highlights the 'Application Settings' option. Below the table, there are sections for 'ルールセット設定' (Rule Set Settings) and 'ルールセットアイデンティティ' (Rule Set Identity).

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

The screenshot displays the Cisco Umbrella Web Policy configuration page. The main area shows a table for 'ルールセットルール' (Rule Set Rules) with columns: 優先 (Priority), ルール名 (Rule Name), ルールアクション (Rule Action), アイデンティティ (Identity), 送信先 (Destination), and ルール構成 (Rule Details). A modal window titled 'ルールの追加' (Add Rule) is open, showing a search for 'Instagram' under the 'Social Networking (Instagram)' category. A red 'X' icon is visible in the modal. The number '10' is overlaid on the search input, and '11' is overlaid on the right arrow of the search results.

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

The screenshot shows the Cisco Umbrella management interface. On the left is a navigation menu with options like '概要', '導入', 'ポリシー', '管理', 'DNSポリシー', 'ファイアウォール ポリシー', 'Web ポリシー', 'ポリシーコンポーネント', '接続先リスト', 'コンテンツカテゴリ', 'アプリケーション設定', 'テナント制御', 'スケジュール設定', 'セキュリティ設定', 'ブロックページ外観', '統合設定', '選択的復号リスト', 'レポート', 'Investigate', and '管理'. The main area displays 'Web Policy1' with '1 ルール' and a '最終更新日' of 'Jun 25, 2024'. Below this is a table for 'ルールセットルール' with columns for '優先', 'ルール名', 'ルールアクション', 'アイデンティティ', '送信先', and 'ルール構成'. A modal window titled 'ルールセット設定' is open, showing a search for 'Instagram' and a list of results including 'Instagram', 'Instagram Posts/Shares', 'Instagram Uploads', and 'Instagram Delete'. A blue circle with the number '12' points to the 'Instagram' rule set. Another blue circle with the number '13' points to the '適用' (Apply) button at the bottom of the modal.

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

1 Web Policy1 次を含む 1 ルール 最終更新日 Jun 25, 2024

ルールセットルール

ルールの追加

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
1	Rule1	ブロック	ルールセットアイデンティティ 4個のアプリケーション... アイデンティティ 宛先の編集 の編集		任意の日、いつでも 変更スケジュール 追加の設定は適用されません 保護されたファイルのバイパスが無効 アンブレラブロックと警告ページ (継承) 編集

▲ **ルールセット設定**

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	Web Policy1	編集
---------	-------------	----

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や選などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
1	Rule1	ブロック	ルールセットアイデンティティ	4個のアプリケーション...	任意の日、いつでも追加の設定は適用されません。保護されたファイルのバイパスが無効。アンプレラブロックと警告ページ (継承)

▲ ルールセット設定
ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

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

ルールの編集

ルールの有効化



16

ルールの削除

ルールステータスの更新

このルールのステータスを更新してもよろしいですか？

キャンセル

更新

17

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。

Web ポリシー / 管理
Web ポリシー

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

	次を含む	最終更新日
1 Web Policy1	1 ルール	Jun 25, 2024
2 Default Web Policy	-	Jun 22, 2024

Get Started

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

Webポリシーテスター

Webポリシーのルールセットとルールが意図したとおり機能しているかどうかをテストするには、接続先へのアイデンティティのアクセスをテストします。ルールセットと有効なルールが、意図したとおりプロック、許可、隔離、または警告されているかどうかをテストします。詳細については、Umbrellaのヘルプを参照してください。 [ヘルプ](#)。

プライマリアイデンティティ
リクエストの発信元のアイデンティティ。

2

ROAMING COMPUTERS

リクエストの発信元のユーザーまたはシステムを識別するアイデンティティ。

接続先

アクションの結果

アイデンティティ:
ルールセット:
ルール:

Get Started

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

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは階層で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

Webポリシーテスター

Webポリシーのルールセットとルールが意図したとおりに機能しているかどうかをテストするには、接続先へのアイデンティティのアクセスをテストします。ルールセットと有効なルールが、意図したとおりにブロック、許可、隔離、または警告されているかどうかをテストします。詳細については、Umbrella のヘルプを参照してください。 [ヘルプ](#)。

プライマリアイデンティティ
リクエストの発信元のアイデンティティ。

セカンダリアイデンティティ (オプション)
リクエストの発信元のユーザーまたはシステムを識別するアイデンティティ。

Search for user, internal network or gsuite user

接続先
追加したアイデンティティがアクセスを試みる接続先。

Instagram.com

リセット テストの実行

アクションの結果

アイデンティティ:
ルールセット:
ルール:

Get Started

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

Web ポリシー / 管理

Web ポリシー

Web ポリシーはルールセットで構成され、ルールセットはルールで構成されます。ルールは、Umbrella のさまざまなセキュリティ機能が組織のアイデンティティをどのように保護するかを決定します。このセキュリティ保護には、インターネットの宛先へのアクセスを制御する構成が含まれます。ルールは、これらのルールセットアイデンティティのサブセットに適用できます。ルールセットには、組織のすべてのアイデンティティの全部またはサブセットを含めることができます。ルールは降順で評価され、アイデンティティと宛先が一致した場合、および時刻や週などのルール条件が満たされた場合に、そのアクションが適用されます。[追加] をクリックして、組織の Web ポリシーに新しいルールセットを追加して構成します。Web ポリシー、ルールセット、およびルールの詳細については、以下を参照してください [ヘルプ](#)。

Webポリシーテスター

Webポリシーのルールセットとルールが意図したとおり機能しているかどうかをテストするには、接続先へのアイデンティティのアクセスをテストします。ルールセットと有効なルールが、意図したとおりブロック、許可、隔離、または警告されているかどうかをテストします。詳細については、Umbrellaのヘルプを参照してください。 [ヘルプ](#)。

プライマリアイデンティティ
リクエストの発信元のアイデンティティ。

ROAMING COMPUTERS

セカンダリアイデンティティ (オプション)
リクエストの発信元のユーザーまたはシステムを識別するアイデンティティ。

Search for user, internal network or gsuite user

接続先
追加したアイデンティティがアクセスを試みる接続先。

instagram.com

リセット テストの実行

ブロック済み

アイデンティティ: Roaming Computers

ルールセット: **Web Policy1** 5

ルール: Rule1

アプリケーション設定: Instagram

スケジュール: 未適用

5

[適用されたポリシー]を確認

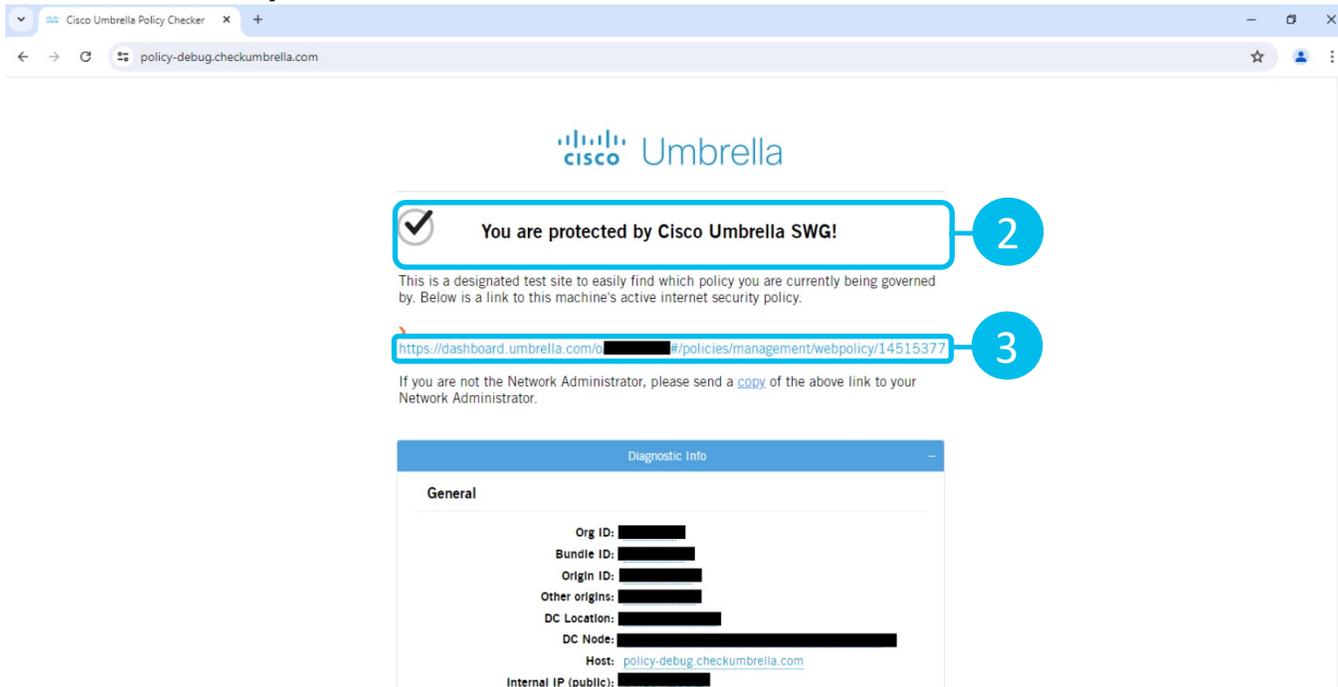
本ガイドの設定例では、「6.ポリシーを設定する(Webポリシー)⑤」で入力したポリシー名が表示されていることを確認※します。

※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-debug.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

Web Policy1 次を含む 1 ルール 最終更新日 Jun 25, 2024

ルールセットルール

ルールの追加

優先	ルール名	ルールアクション	アイデンティティ	送信先	ルール構成
1	Rule1	ブロック	ルールセットアイデンティティ	4個のアプリケーション	任意の日、いつでも追加の設定は適用されません 保護されたファイルのバイパスが無効 アンブレラブロックと警告ページ(継承)

▲ ルールセット設定

ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

ルールセット名	Web Policy1	編集
ルールセットアイデンティティ	2 アイデンティティ	編集
ブロックページと警告ページ	適用されたUmbrellaのブロックページ	編集
テナントコントロール	Global Tenant Controls	編集
ファイル分析	1個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集

4

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

← → ↻ block.opendns.com/swg?server=swg-nginx-proxy-https-8b0970e633d1.signinix.syd&cv=eyJhbGciOiAiSF1MTiILCAia2lkjogJjE1NjM1NTk3OTYifQ.eyJidHlwZSI6IiIiLCiCAib3JnljogOD... ☆



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>