

セキュリティおまかせプラン どこでもプライム ご利用マニュアル (Ver 1.7)

2025年12月
西日本電信電話株式会社

改定履歴

| No | Date | 主な変更内容 | Ver |
|----|------------|---|-----|
| 1 | 2025/03/31 | 初版 | 1.0 |
| 2 | 2025/04/25 | 6. コンソールへのログイン手順 <管理者アカウント 初回ログイン> 7-2. インターネットが使えない | 1.1 |
| 3 | 2025/05/09 | 3. ソフトウェアの対応OS、バージョン、システム要件 | 1.2 |
| 4 | 2025/05/13 | 7-1-1. 特定のサイトが見られない① 7-1-2. 特定のサイトが見られない② 7-10. 広告のページを開けるようにしたい | 1.3 |
| 5 | 2025/7/11 | 9-12. デバイス制御方法 11. 契約番号の確認方法 | 1.4 |
| 6 | 2025/8/1 | 4-3. インストール手順 <ダウンロードしたインストーラの実行> 4-4. インストール手順 <ソフトウェアの起動／ステータス確認> 5. ソフトウェアのアンインストール手順 | 1.5 |
| 7 | 2025/10/27 | 3. ソフトウェアの対応OS、バージョン、システム要件① 3. ソフトウェアの対応OS、バージョン、システム要件② 4-4. インストール手順 <ソフトウェアの起動／ステータス確認> 10. elganaの設定手順 (elganaとは) | 1.6 |
| 8 | 2025/12/04 | 12. ログ取得および送付手順 | 1.7 |

| | |
|------------------------------------|------------------|
| 1. 提供サービス概要 | P4 |
| 2. 事前準備 | P5 |
| 3. ソフトウェアの対応OS、バージョン、システム要件 | P6 ~ P7 |
| 4. ソフトウェアのインストール手順 | P8 ~ P44 |
| 5. ソフトウェアのアンインストール手順 | P45 ~ P57 |
| 6. セキュアインターネットゲートウェイ コンソールへのログイン手順 | P58 ~ P65 |
| 7. セキュアインターネットゲートウェイ機能を設定変更する | P66 ~ P140 |
| 8. セキュアエンドポイント コンソールへのログイン手順 | P141 ~ P151 |
| 9. セキュアエンドポイント機能を設定変更する | P152 ~ P209 |
| 10. elgana連携の設定手順 | P210 ~ P214 |
| 11. どこでもプライム契約IDの確認手順 | P215 ~ P217 |
| 12. ログ取得および送付手順 | P218 ~ P246 |

1. 提供サービス概要

1 セキュアインターネットゲートウェイ (Cisco Umbrella SIG Essentials) ^{※1}



クラウド上のゲートウェイがお客さまの異常通信の監視・遮断をし、オフィス内外を問わないセキュリティ対策を実現。複数の拠点や個人が私物として所有しているパソコンを業務に使う場合にも効果を発揮します。



2 セキュアエンドポイント (Cisco Secure Endpoint Essentials) ^{※2}



ウイルスの侵害を受ける前に、脅威を阻止するEPP機能と、例え未知の脅威に感染したときでもEDRの機能でインシデントを可視化することで、お客さまの端末を脅威から守ります。

※EPP: Endpoint Protection Platformの略 EDR: Endpoint Detection and Responseの略



3 ビジネスチャット elgana®



企業や組織内での円滑なコミュニケーションや情報共有を目的として設計された、ビジネス向けチャット・コラボレーションツール。リモートワークやハイブリッドワーク環境にもピッタリのサービスです。



elgana

※1 以降、セキュアインターネットゲートウェイ もしくは Umbrellaと記載

※2 以降、セキュアエンドポイント もしくは Secure Endpointと記載

ウイルス対策ソフトやMDMソフトが入っている場合、本サービスで提供するセキュリティソフトのインストールが行えない場合があるため、事前にアンインストールをお願い致します

<Windows 10 の場合>

「スタート」⇒「コントロールパネル」⇒「プログラムと機能」⇒「プログラムのアンインストール」

<Windows 11 の場合>

「スタート」⇒「コントロールパネル」⇒「プログラム」⇒「プログラムのアンインストール」

<Macの場合>

- ・App Store からインストールしたアプリを削除するには、まず Launchpad を開きます。
⇒ LaunchPad を起動後、どれか一つアプリを長押しします。
⇒ アプリの左上に × マークが表示されます。
⇒ 削除したいアプリの × マークをクリックします。
- ・App Store 以外からインストールしたアプリの場合、アンインストールプログラムが用意されている場合は、対象のプログラムをクリックしてアンインストールを実施。

★詳しくは各ソフトウェアのマニュアルをご参照ください。

3. ソフトウェアの対応OS、バージョン、システム要件①

本サービスで提供するソフトウェアの対応OS、バージョン、システム要件については下記をご参照ください

<対象ソフトウェア>

- セキュアインターネットゲートウェイ (Cisco Umbrella SIG Essentials)
- セキュアエンドポイント (Cisco Secure Endpoint Essentials)

| | Windows | Mac |
|--------|--|--|
| 対応OS | Windows 10 (※)、11 ※Microsoft 社によるWindows 10 の公式サポート終了 (2025年10月14日)に伴い、Windows10 は動作保証の対象外となります。 Windows 10の拡張セキュリティ Updates (ESU)が適用されている端末は、引き続き動作保証対象となります。 | macOS 14、15、26 |
| 対応デバイス | Windows デバイスは、トラステッド プラットフォーム モジュールバージョン 2.0 を含むシステムで実行されている必要があります。 また、本サービス仕様上、x64アーキテクチャ互換のチップである必要があります。 ※ARM版はサポート対象外となります。 | macOS デバイスは、Apple T1 チップを搭載した Touch Bar (2016 および 2017) 搭載の MacBook Pro コンピュータなどの Secure Enclave を含むシステムで実行されている必要があります。 Apple T2 Security チップを搭載した Intel ベースの Mac コンピュータ、または Apple シリコンを搭載した Mac コンピュータ また、本サービス仕様上、X64アーキテクチャ互換のチップである必要があります。 ※ARM版はサポート対象外となります。 |

上記表は、2025年10月時点の情報です。最新情報は以下のURLをご確認ください。

[セキュアインターネットゲートウェイ](#) ※「Umbrella Roaming Security」の欄をご確認ください。

[セキュアエンドポイント \(Windows OS\)](#)

[セキュアエンドポイント \(mac OS\)](#)

3. ソフトウェアの対応OS、バージョン、システム要件②

本サービスで提供するソフトウェアの対応OS、バージョン、システム要件については下記をご参照ください

<対象ソフトウェア>

- セキュアインターネットゲートウェイ (Cisco Umbrella SIG Essentials)
- セキュアエンドポイント (Cisco Secure Endpoint Essentials)

| | Windows | Mac |
|----------|---|--|
| 最小システム要件 | 2GB RAM 2GB のハード ディスク空き領域 ※Windows のシステム要件は考慮していません | 2GB RAM 2GBのハード ディスク空き領域 ※Mac のシステム要件は考慮していません |

※Cisco Secure Endpoint ユーザガイド (システム要件) 参照

※Windowsのシステム要件参照

※Macのシステム要件参照

4. ソフトウェアのインストール手順

WindowsOSの場合

| 手順概要 | | 備考 | 時間目安 |
|------|---------------------------------------|--|-------|
| 1 | 開通メールからelganaマイページへログイン | <開通メールの送信元メールアドレス> dokopura-kaian@west.ntt.co.jp <開通メールの件名> 【NTT西日本セキュリティおまかせプラン】どこでもプライムのご案内 | 20分／台 |
| 2 | elganaマイページからWindowsOS用のインストーラをダウンロード | ZIP形式の圧縮ファイル | |
| 3 | ダウンロードしたインストーラの実行（解凍後／2ファイル） | ・WindowsOS用実行ファイル ・ルート証明書実行ファイル | |
| 4 | ソフトウェアの起動／設定／ステータス確認 | ・セキュアインターネットゲートウェイ（Cisco Umbrella） ・セキュアエンドポイント（Cisco Secure Endpoint） | |

MacOSの場合

| 手順概要 | | 備考 | 作業時間目安 |
|------|-----------------------------------|--|--------|
| 1 | 開通メールからelganaマイページへログイン | <開通メールの送信元メールアドレス> dokopura-kaian@west.ntt.co.jp <開通メールの件名> 【NTT西日本セキュリティおまかせプラン】どこでもプライムのご案内 | 20分／台 |
| 2 | elganaマイページからMacOS用のインストーラをダウンロード | ZIP形式の圧縮ファイル | |
| 3 | ダウンロードしたインストーラの実行（解凍後／3ファイル） | ・MacOS用実行ファイル ・CSEコネクタモジュール実行ファイル ・ルート証明書実行ファイル | |
| 4 | ソフトウェアの起動／設定／ステータス確認 | ・セキュアインターネットゲートウェイ（Cisco Umbrella） ・セキュアエンドポイント（Cisco Secure Endpoint） | |

4-1. 開通メールからelganaマイページへログイン

4-1. インストール手順 <elganaマイページへのログイン-1>

- ①事前に送付させていただいている「開通メール」を確認
- ②端末設定ツール欄に記載の右記URLをクリック (<https://connect-contract.elgana.jp/connectMyPage>)

| 項目 | 情報 |
|------|--|
| TO | (申込書にご記載いただいたメールアドレス) |
| BCC | 〇〇〇 |
| From | dokopura-kaian@west.ntt.co.jp |
| 件名 | NTT西日本セキュリティおまかせプラン】どこでもプライムのご案内 (契約ID XXXXXX) ※配信専用※ |
| 本文 | <p>セキュリティおまかせプラン どこでもプライムご契約者様 (契約ID XXXXXX)</p> <p>この度は NTT西日本 セキュリティおまかせプラン どこでもプライムへのお申込みありがとうございます。 どこでもプライムの契約ID数や端末設定ツールのダウンロードURLなどの情報を送付いたします。 ご契約総ID数 : ●●ID</p> <p>尚、サービスが有効になるのは、ご利用開始予定日のYYYY年MM月DD日からとなっております。 ご利用開始前にインストールされた場合、さかのぼっての課金対象となりますのでご注意ください。</p> <p>ご利用開始日になりましたら次のURLから端末設定ツールをダウンロードいただき、 手順書に従って、クライアントソフトのインストールを実施ください。</p> <p>◆端末設定ツール（インストーラーおよびルート証明書） https://connect-contract.elgana.jp/connectMyPage アカウント名：（申込書にご記載いただいたメールアドレス） 初期パスワード：（開通センタで設定するパスワード）</p> <p>※複数端末にインストールされる場合、上記からダウンロードした端末設定ツールを端末に展開ください。 ※ご契約総ID数を超えて端末にインストールされた場合、追加請求が発生する場合ございます。 ※インストーラの取り扱いには十分ご注意ください。</p> <p>◆インストールの手順書等掲載先 https://office-support.ntt-west.co.jp/security_dokodemo_prime/</p> <p>~~~</p> <p>【elganaに関するお問い合わせ】 elgana カスタマーサポートセンター TEL : 0120-000-559 MAIL : elgana-pj-help-m1@west.ntt.co.jp 受付時間：9：30～17：30（土日祝、年末年始（12/29～1/3）を除く）</p> <p>【セキュリティおまかせプラン サポートサイト】 サービスの使い方や、設定方法、よくあるご質問などを掲載しております。ご活用ください。 https://office-support.ntt-west.co.jp/security_dokodemo_prime/</p> |

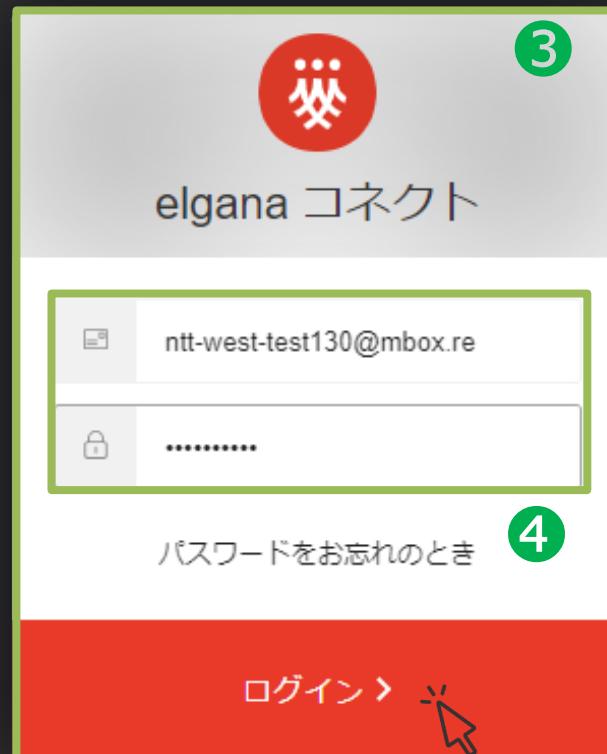
①開通メールイメージ

②端末設定ツール入手用のURL及びログイン情報

4-1. インストール手順 <エルガナマイページへのログイン-2>

③elganaコネクトのログイン画面へ遷移

④開通メールに記載の「ログインID」「パスワード」を入力し、「ログイン」を選択



4-2. インストーラーのダウンロード

4-2. インストール手順概要 <elganaマイページからインストーラダウンロード>

The screenshot shows the elgana Connect My Page interface. At the top, there is a navigation bar with the elgana logo, a search bar, and links for "よくあるご質問" (FAQ) and "ログアウト". Below the navigation bar, the page title "マイページ" is displayed. A message encourages users to "「サービス一覧へ進む」からサービスをお申し込みください". A red button labeled "サービス一覧へ進む" (Go to Service List) is visible. The main content area is divided into three sections: "お客様情報" (Customer Information), "サービス契約内容" (Service Contract Details), and "ワークスペース情報" (Workspace Information). The "サービス契約内容" section is currently active. It displays a workspace ID "ntt-west-test110". Below this, a message states "上記ワークスペースIDで契約中のサービス" (Services contracted under the above workspace ID). A red callout box highlights the "セキュリティおまかせプランどこでもプライベート" (Security Omaease Plan Private Anywhere) button. At the bottom, there are fields for "elgana 利用開始日" (Start Date) and "elgana 利用完了日" (End Date), both showing "未インストール/インストール済み" (Not Installed/Installed). To the right, a green button labeled "Windows用" (For Windows) is highlighted with a red arrow pointing from the text "対象OSのインストーラを選択しダウンロード" (Select the installer for the target OS and download).

elgana コネクト

よくあるご質問

ログアウト

マイページ

「サービス一覧へ進む」からサービスをお申し込みください

サービス一覧へ進む

お客様情報

サービス契約内容

ワークスペース情報

ワークスペースID
ntt-west-test110

上記ワークスペースIDで契約中のサービス

セキュリティおまかせプランどこでもプライベート

elgana 利用開始日
未インストール/インストール済み

elgana 利用完了日

Windows用

Mac 用

対象OSのインストーラを選択しダウンロード

4-3. ダウンロードしたインストーラーの実行_Windows

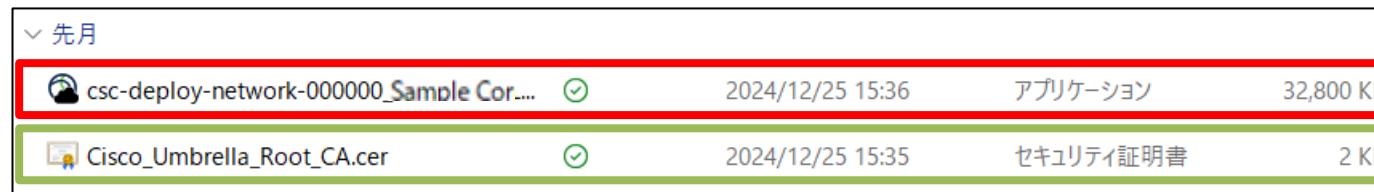
4-3. インストール手順 <ダウンロードしたインストーラの実行-1>

elganaマイページから初期セットアップファイル一式をダウンロードし、該当するOS用のパッケージに含まれるファイルをすべて実行する
(下記はWindowsの場合)



展開後のファイル構成によって、インストールの動作が異なります。以下をご確認ください。

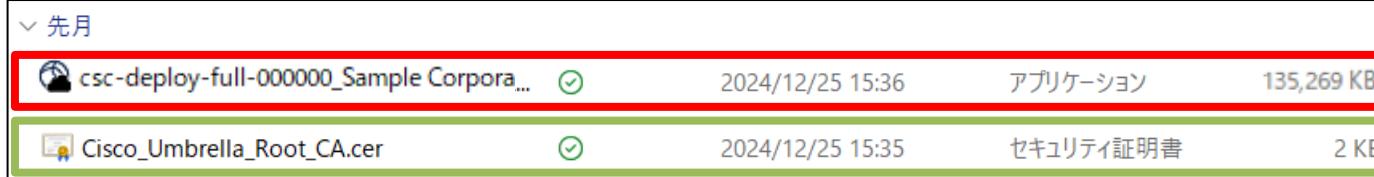
①以下画面が表示される方 (赤枠内のファイルが「csc-deploy-network-000000_Sample Corporation.exe」となっている)



👉 ダブルクリックで実行後、ポップアップ画面に従いインストール

👉 ダブルクリックで実行後、ポップアップ画面に従い証明書をインポート

②以下画面が表示される方 (赤枠内のファイルが「csc-deploy-full-000000_Sample Corporation.exe」となっている)



👉 ダブルクリックで実行後、ポップアップ画面に従いインストール

👉 ダブルクリックで実行後、ポップアップ画面に従い証明書をインポート

👉 具体的なインストール手順は次ページ以降を参照

4-3. インストール手順 <ダウンロードしたインストーラの実行-2>

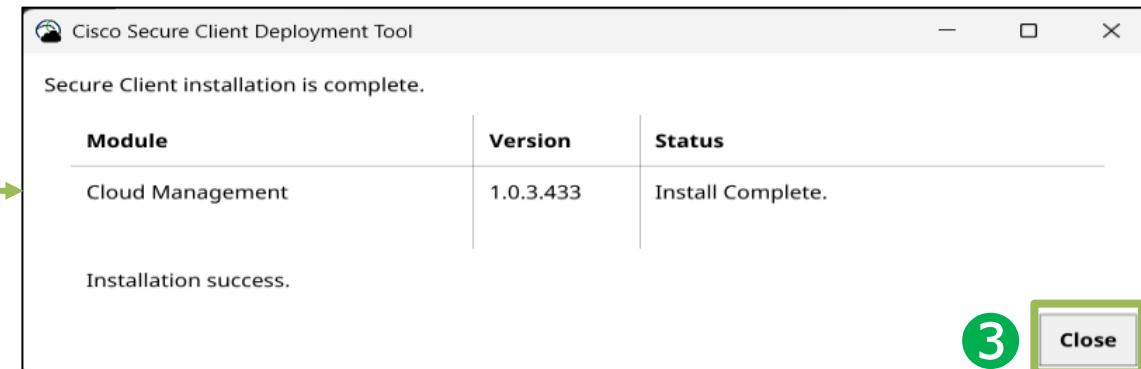
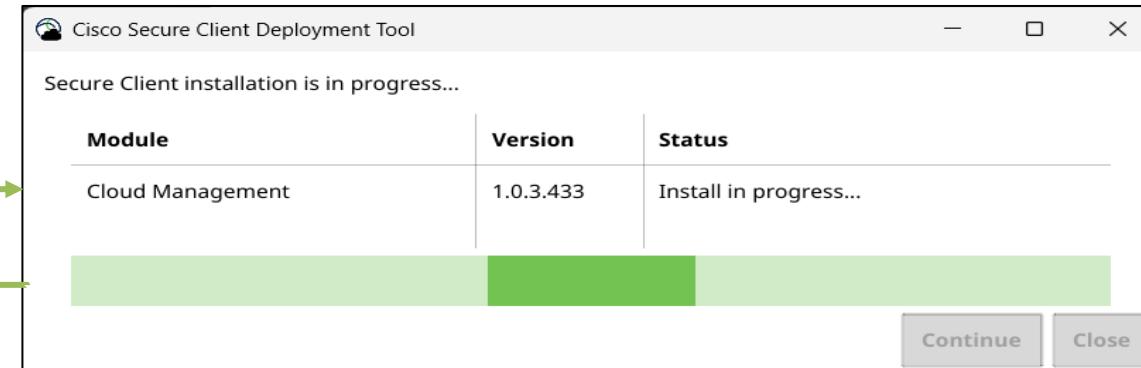
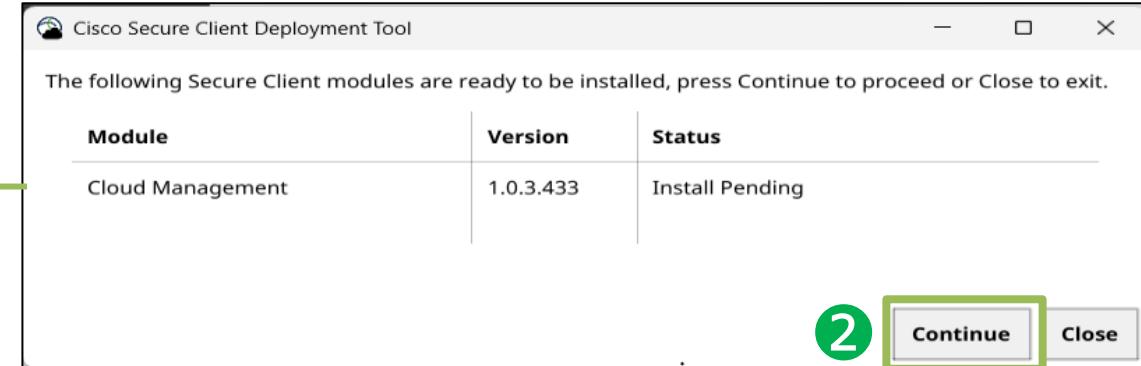
①以下画面になっている方（ファイルが「csc-deploy-network-000000_Sample Corporation.exe」となっている）

👉 対象のネットワークインストーラを実行
(csc-deploy-network-[契約ID]_[会社名].exeの実行)



※契約IDは開通メールをご参考ください

👉 「Continue」を選択
1分程度でインストールが完了するので「close」でウィザードを終了

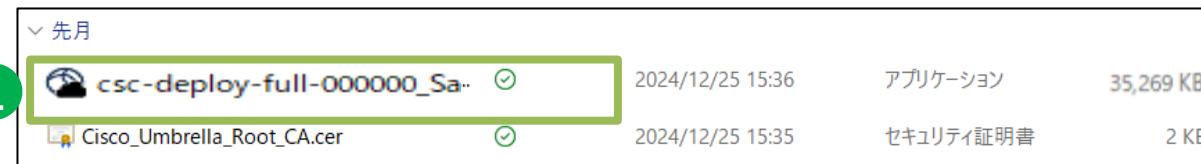


1分程度待つ

4-3. インストール手順 <ダウンロードしたインストーラの実行-3>

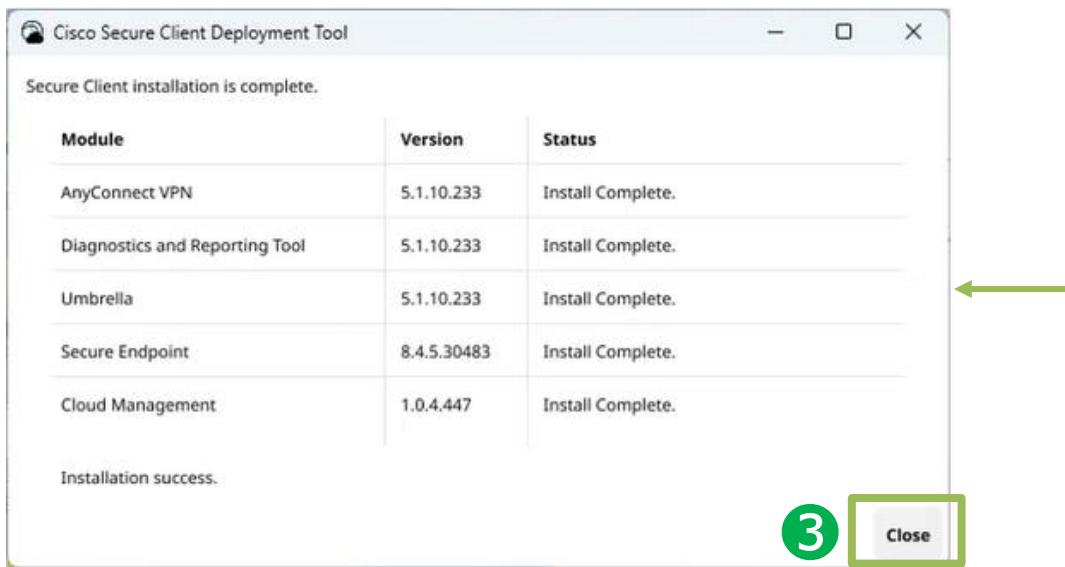
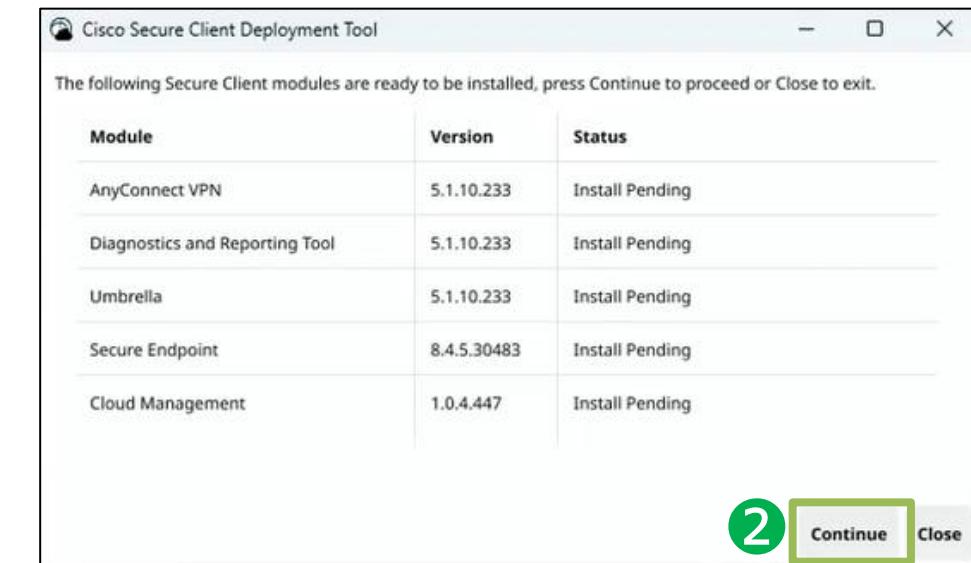
②以下画面になっている方（ファイルが「csc-deploy-full-000000_Sample Corporation.exe」となっている）

👉 対象のネットワークインストーラを実行
(csc-deploy-full-[契約ID]_[会社名].exeの実行)



※契約IDは開通メールをご参考ください

👉 「Continue」を選択
1分程度でインストールが完了するので「close」でウィザードを終了



1分程度待つ



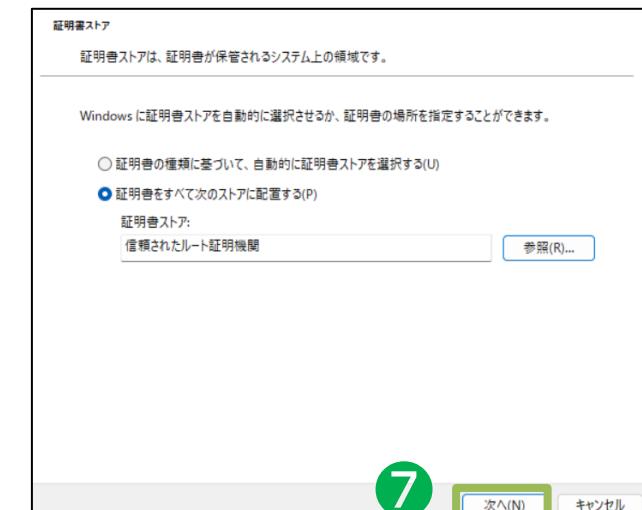
4-3. インストール手順 <ダウンロードしたインストーラの実行-4>

ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-1

「証明書のインストール」を選択

「現在のユーザー」を選択した状態で次へ進む

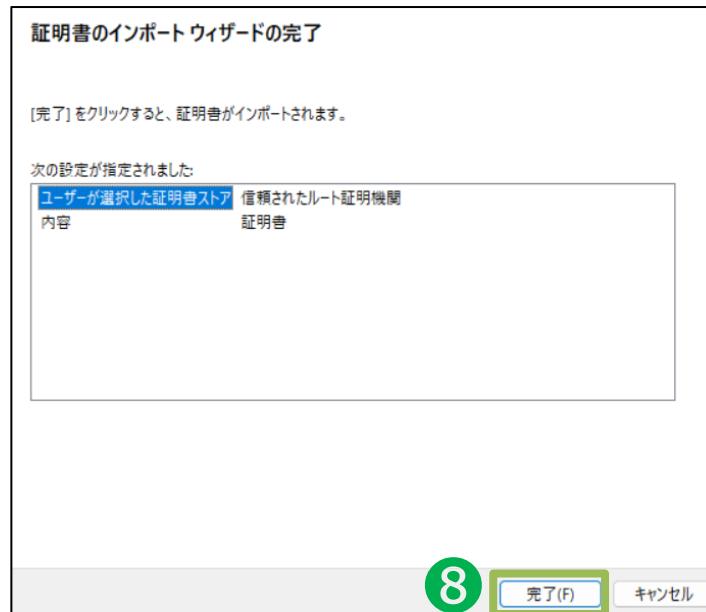
「証明書をすべて次のストアに配置する」を選択した状態で参照から
「信頼されたルート証明機関」を指定して次へ進む



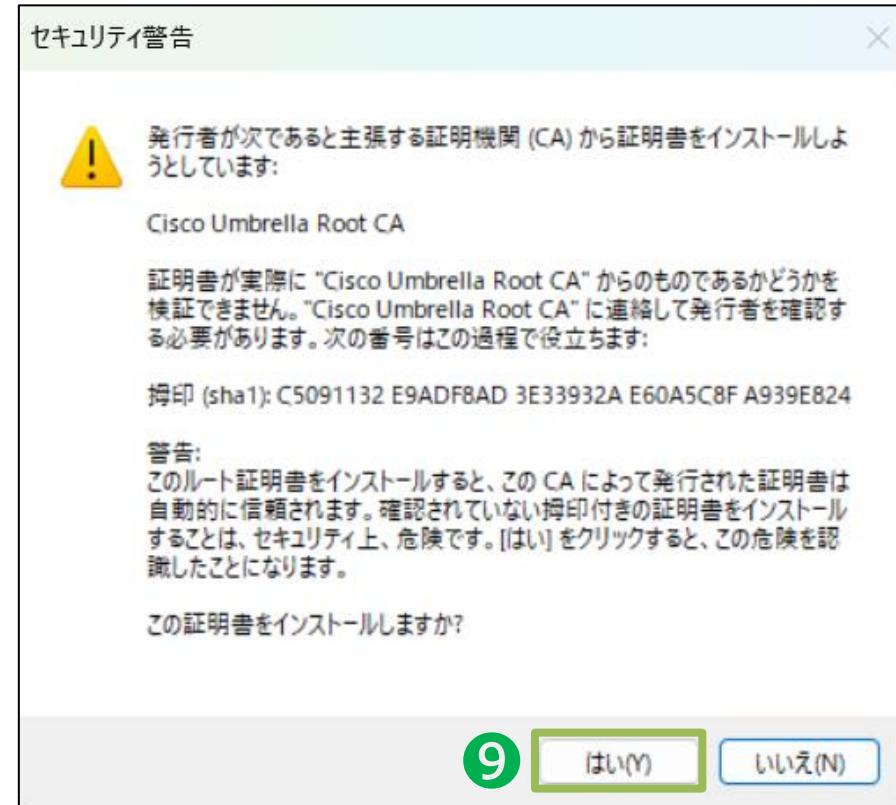
4-3. インストール手順 <ダウンロードしたインストーラの実行-5>

ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-2

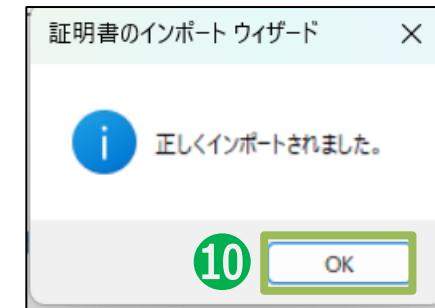
「完了」を選択してインポートを開始



セキュリティ警告がポップアップした場合は「はい」を選択



インポート完了

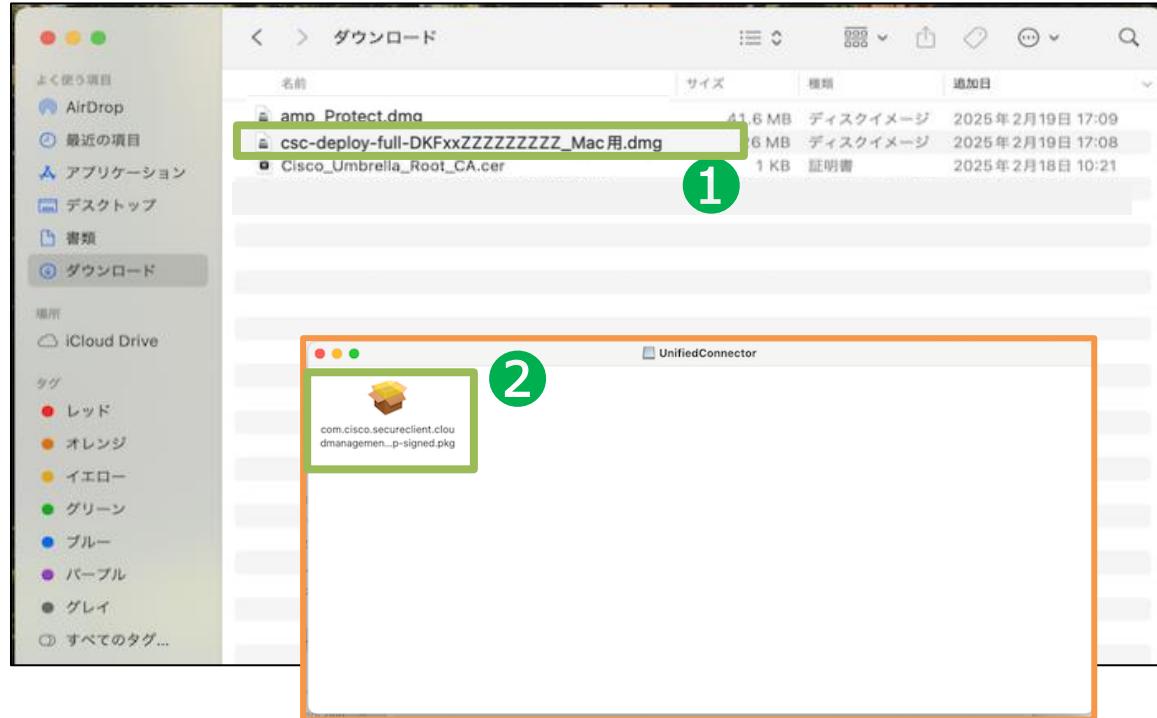


4-3. ダウンロードしたインストーラーの実行_Mac

4-3. インストール手順 <ダウンロードしたインストーラの実行-1>

👉 対象のインストーラ（※）を実行

※インストーラによって、インストール手順が異なります。
ページ下部をご参照ください。



👉 「続ける」を選択



対象のインストーラについて

※契約IDは開通メールをご参照ください

①以下画面が表示される方 （赤枠内のインストーラが「csc-deploy-network-[契約ID]_[会社名]_Mac用.dmg」となっている方）



②以下画面が表示される方 （赤枠内のインストーラが「csc-deploy-full-[契約ID]_[会社名]_Mac用.dmg」となっている方）



4-3. インストール手順 <ダウンロードしたインストーラの実行-2>

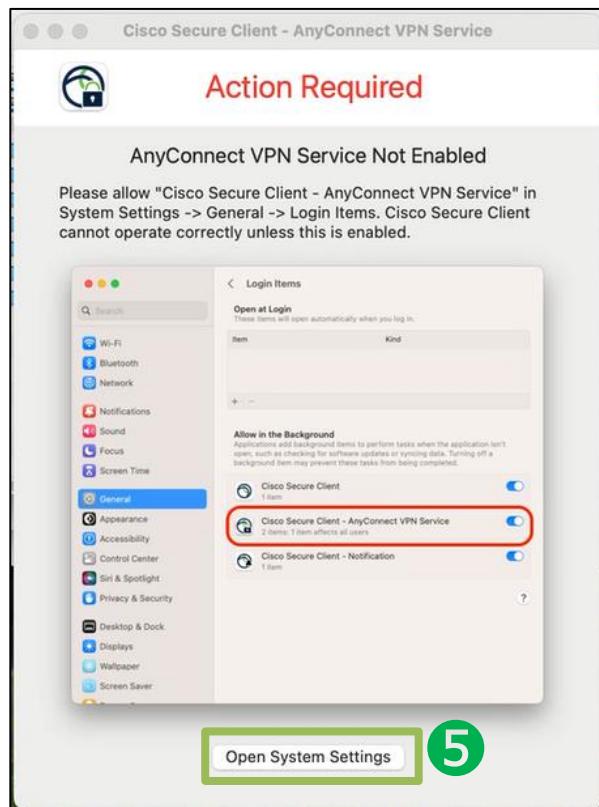
👉 「インストール」を選択



4-3. インストール手順 <ダウンロードしたインストーラの実行-3>

※こちらのページ（手順⑤～⑦）は、
インストーラが②「csc-deploy-full-[契約ID]_[会社名]_Mac用.dmg」となっている方のみ、必要な手順です※

「Open System Settings」をクリック



「Cisco Secure Client – AnyConnect VPN Service」を有効にする（※）



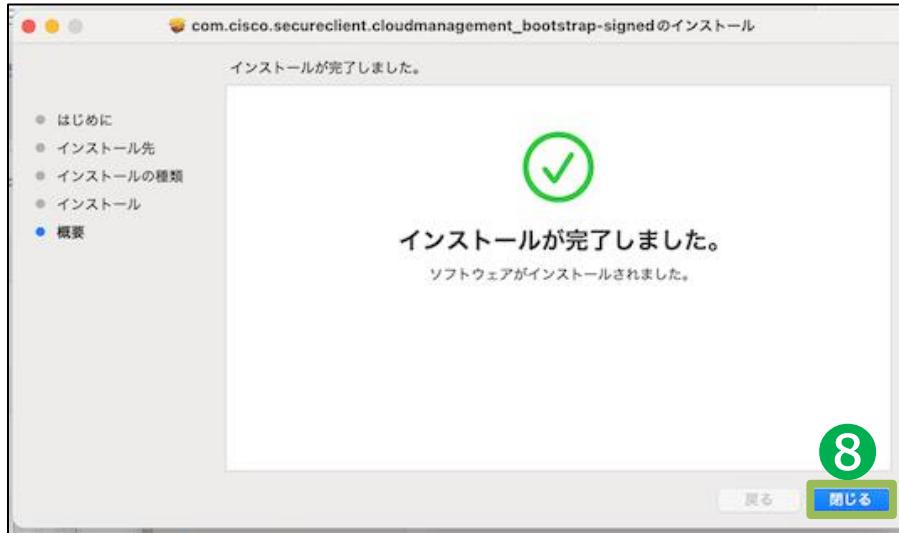
パスワードを入力し、「設定を変更」をクリック



※自動で有効になっている場合もありますので、その場合は画面左上の「×」で画面を閉じてください。

4-3. インストール手順 <ダウンロードしたインストーラの実行-4>

「閉じる」を選択



「ゴミ箱に入れる」を選択



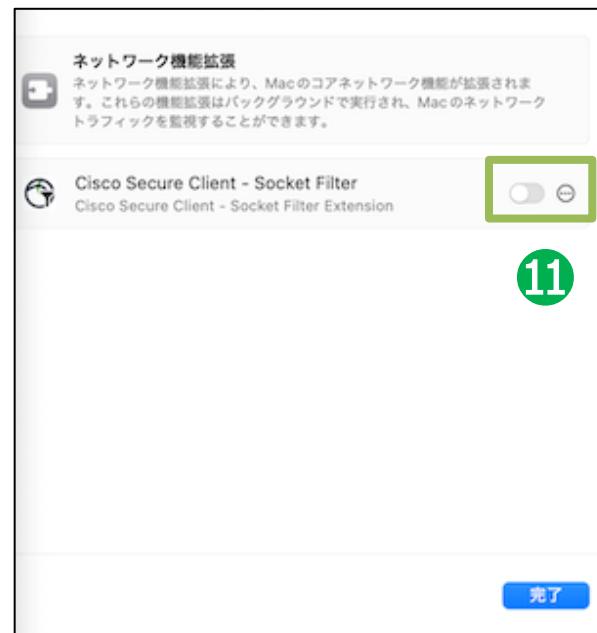
※以降の手順では、
端末によりポップアップの表示される順番が前後する可能性があります。
表示されたポップアップに従ってアプリの初期設定を実施してください。

4-3. インストール手順 <ダウンロードしたインストーラの実行-5>

「システム設定を開く」を選択



「Cisco Secure Client - Socket Filter」を有効化



「許可」を選択

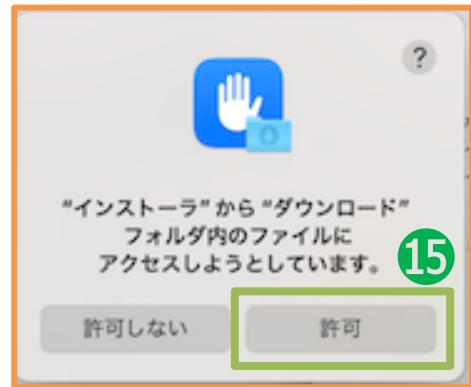


「解散」を選択し、「完了」で設定画面を閉じる

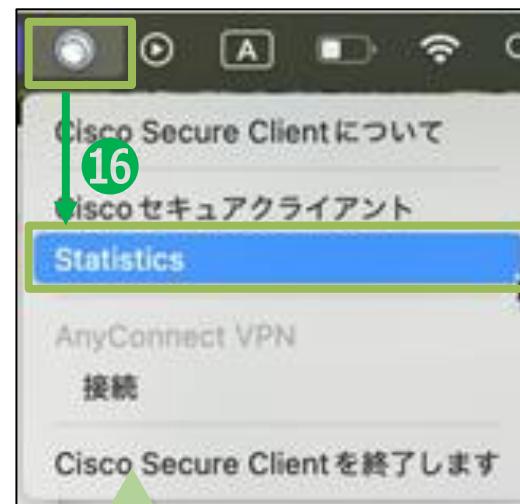


4-3. インストール手順 <ダウンロードしたインストーラの実行-6>

👉 「許可」を選択



👉 「Statistics」を選択



Cisco Secure Clientが自動で起動しない場合は
「Finder」>「アプリケーション」>
「Cisco」フォルダ>「Cisco Secure Client」を実行する

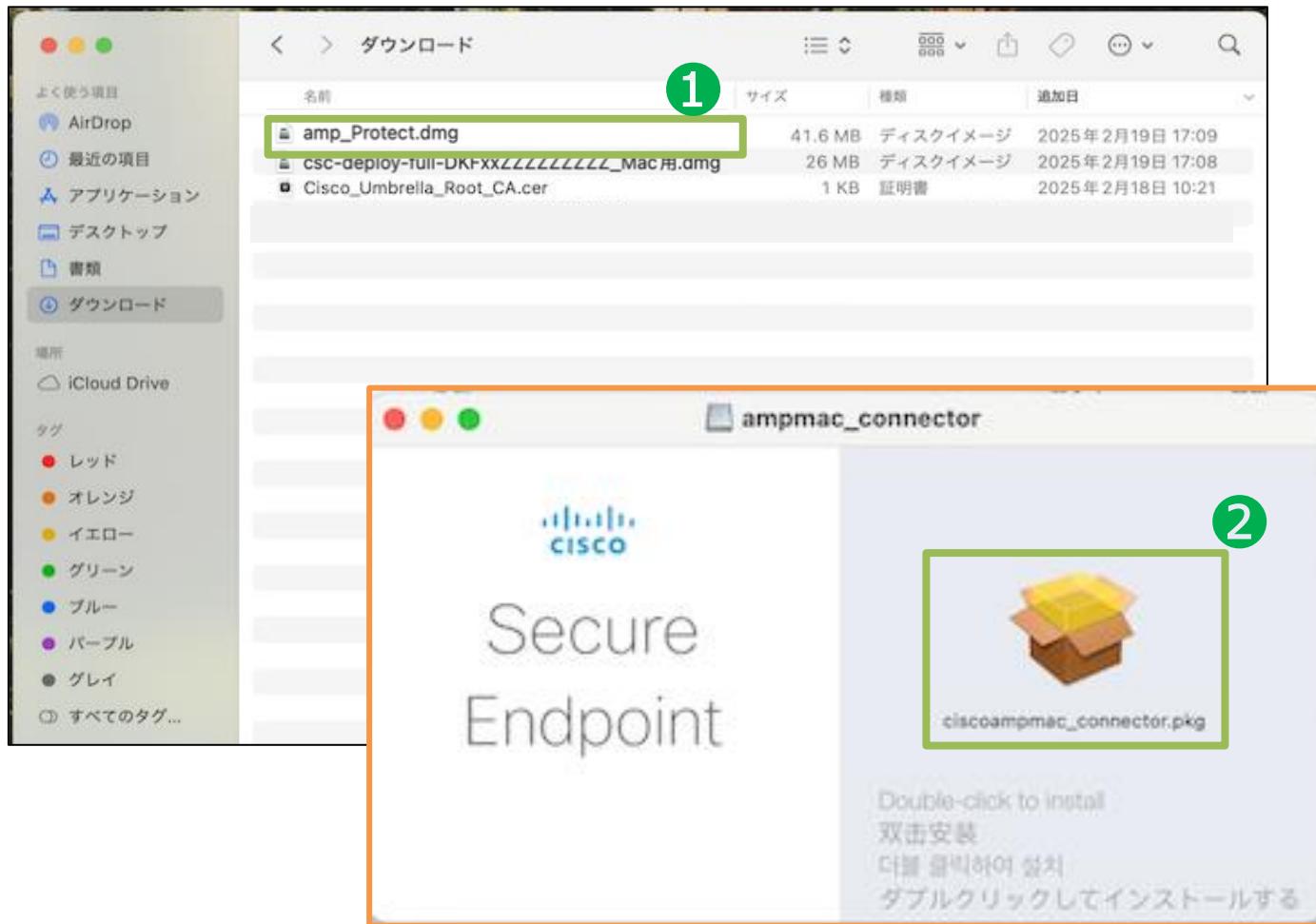
👉 Umbrellaの「IPv4 DNS保護のステータス」が「保護されています」、
「Web保護ステータス」が「保護されています」であることを確認



4-3. インストール手順 <ダウンロードしたインストーラの実行-7>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-1

👉 「amp_Protect.dmg」を選択し、開いたPKGファイルをダブルクリック



👉 「続ける」を選択



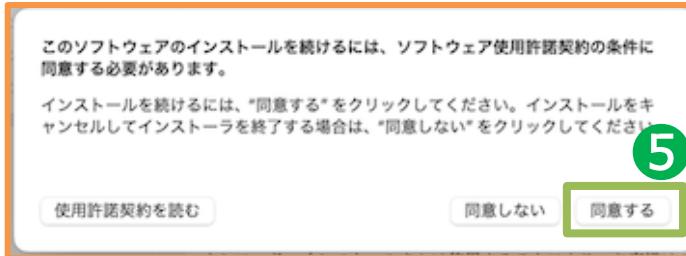
4-3. インストール手順 <ダウンロードしたインストーラの実行-8>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-2

👉 「続ける」を選択



👉 「同意する」を選択



👉 「続ける」を選択



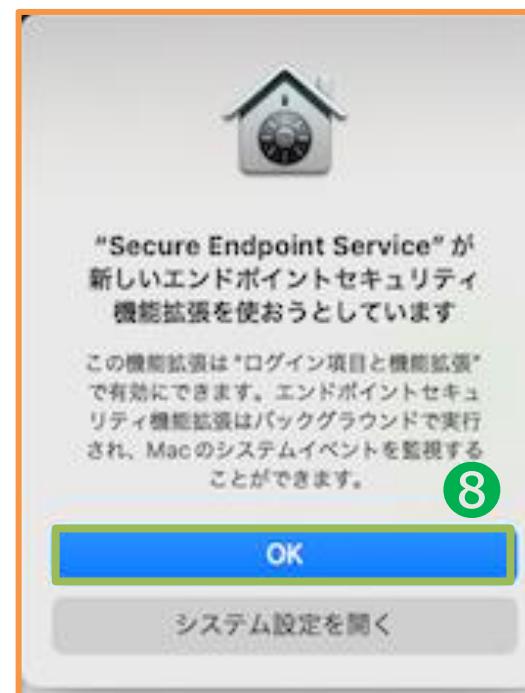
4-3. インストール手順 <ダウンロードしたインストーラの実行-9>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-3

👉 「インストール」を選択



👉 「OK」を選択



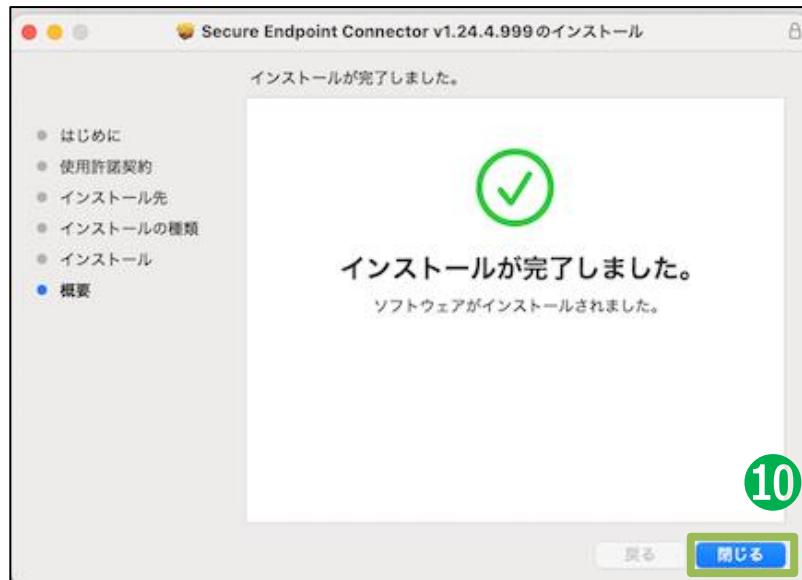
👉 「OK」を選択



4-3. インストール手順 <ダウンロードしたインストーラの実行-10>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-4

👉 「閉じる」を選択



👉 「ゴミ箱に入れる」を選択



👉 画面右上にある「」マークを選択し、「システム機能拡張を許可」を選択



4-3. インストール手順 <ダウンロードしたインストーラの実行-11>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-5

「セキュアエンドポイント機能拡張」の「*i*」を選択



「Secure Endpointサービス」を有効化



「完了」を選択



4-3. インストール手順 <ダウンロードしたインストーラの実行-12>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-6

👉 「ネットワーク機能拡張」の「 ⓘ 」を選択



👉 「Secure Endpointサービス」を有効化



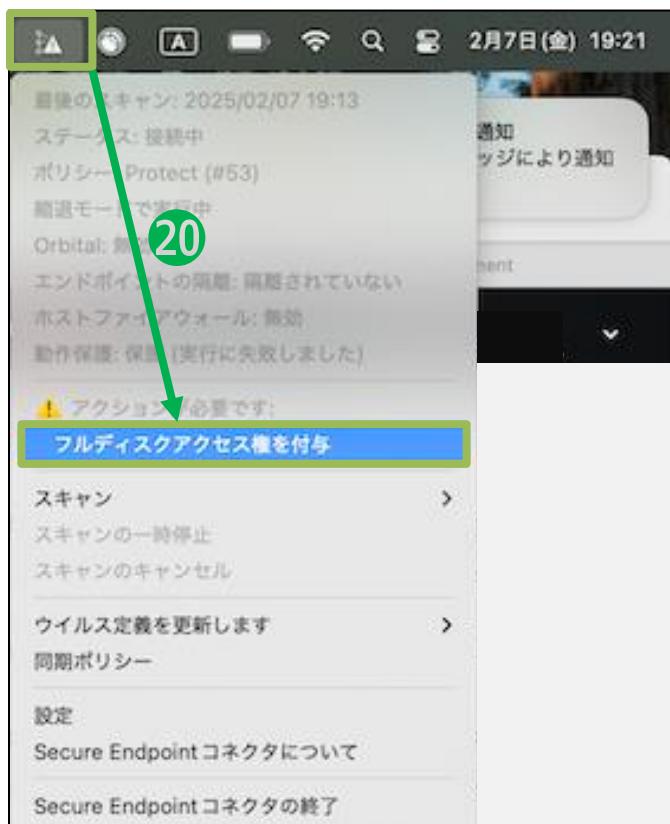
👉 「完了」を選択



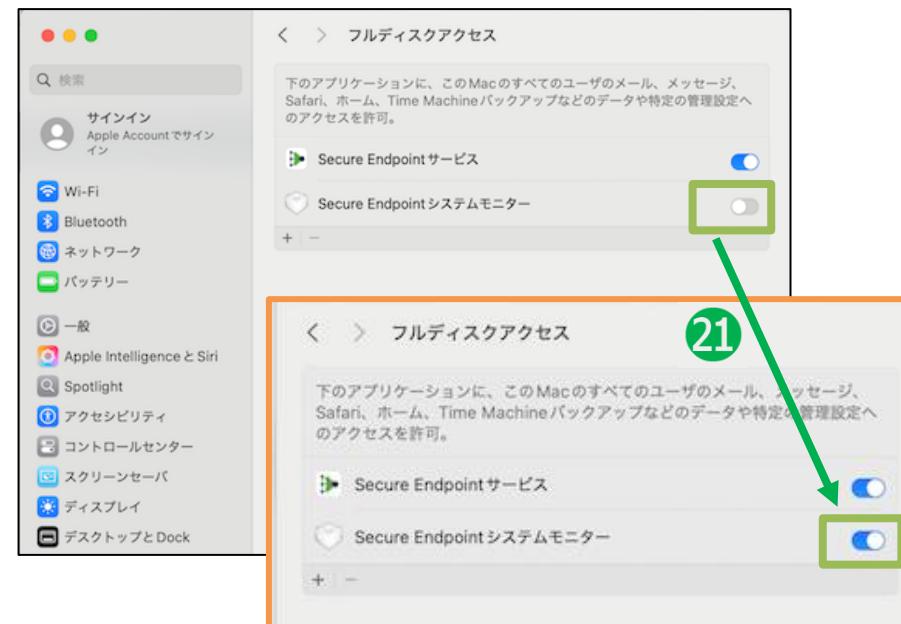
4-3. インストール手順 <ダウンロードしたインストーラの実行-13>

CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-7

画面右上にある「」マークを選択し、「フルディスクアクセス権を付与」を選択



「Secure Endpointシステムモニター」を有効化



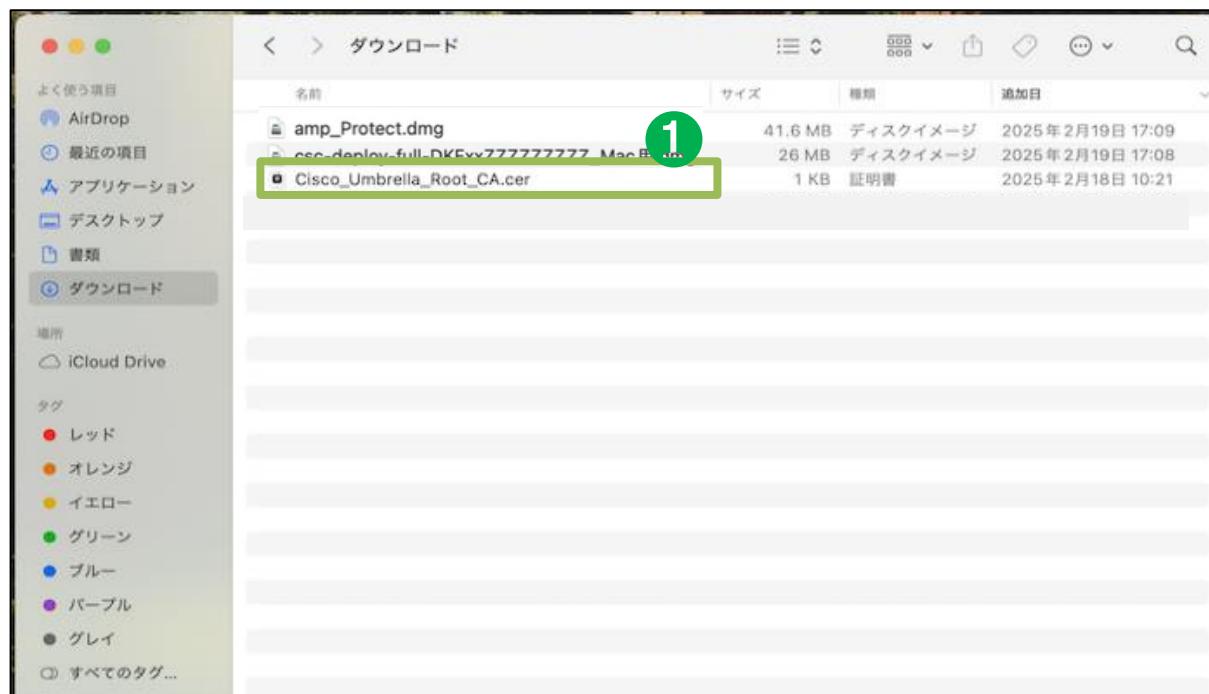
追加アクション要求「」がなくなっていることを確認



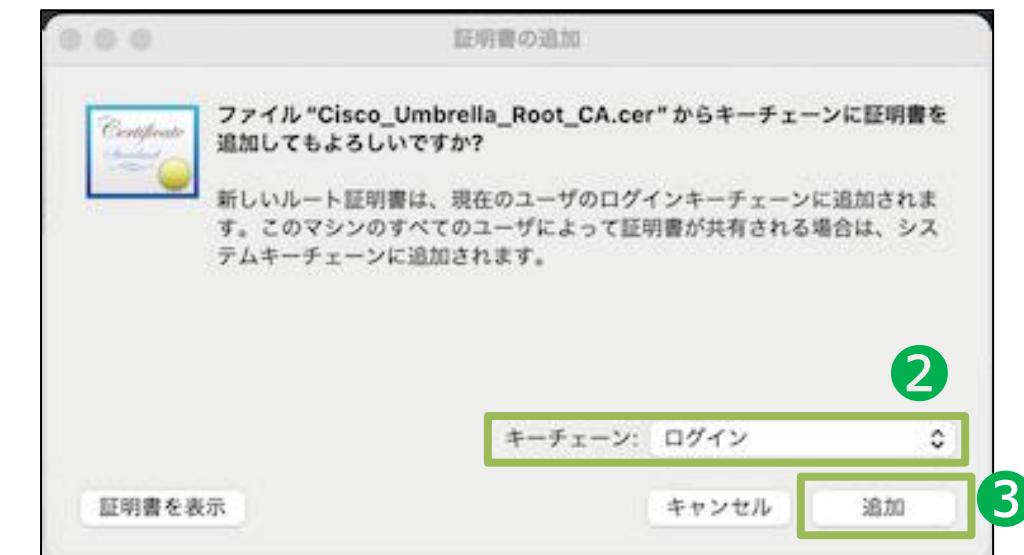
4-3. インストール手順 <ダウンロードしたインストーラの実行-14>

ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-1

👉 「Cisco_Umbrella_Root_CA.cer」をダブルクリックで実行



👉 キーチェーンに「ログイン」を選択し、「追加」を選択



4-3. インストール手順 <ダウンロードしたインストーラの実行-15>

ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-2

👉 証明書が信頼されていないことを確認し、
インポートした「Cisco Umbrella Root CA」をダブルクリック
(既に信頼済みであればルート証明書のインポートは完了)

👉 「信頼」のプルダウンを開く

The screenshot shows the 'Keychain Access' application window. A green callout box points to the 'Cisco Umbrella Root CA' entry in the list, with the text: 「Cisco Umbrella Root CA」が見当たらなければ、「自分の証明書」にないか確認。 A green circle labeled '5' highlights the certificate entry. Another green circle labeled '6' highlights the status message: このルート証明書は信頼されていません (This root certificate is not trusted). A large orange arrow points from the left panel to the right panel.

The right panel shows the detailed view of the 'Cisco Umbrella Root CA' certificate. A green circle labeled '7' highlights the 'Trust' dropdown menu. A red error message at the top states: このルート証明書は信頼されていません (This root certificate is not trusted). The certificate details include:

- サブジェクト名: Cisco Umbrella Root CA
- 組織: Cisco
- 有効期限: 2036年6月29日 日曜日 0時37分53秒 日本標準時
- 発行者名: Cisco
- シリアル番号: 58678097385
- バージョン: 3
- 署名アルゴリズム: RSA暗号化を使用
- パラメータ: なし
- 有効になる日付: 2016年6月29日
- 無効になる日付: 2036年6月29日

Below the certificate details, there is a section for 'SSL (Secure Sockets Layer)' settings, all of which are set to '値が指定されていません' (Value is not specified). There is also a '詳細な情報' (Detailed Information) section at the bottom.

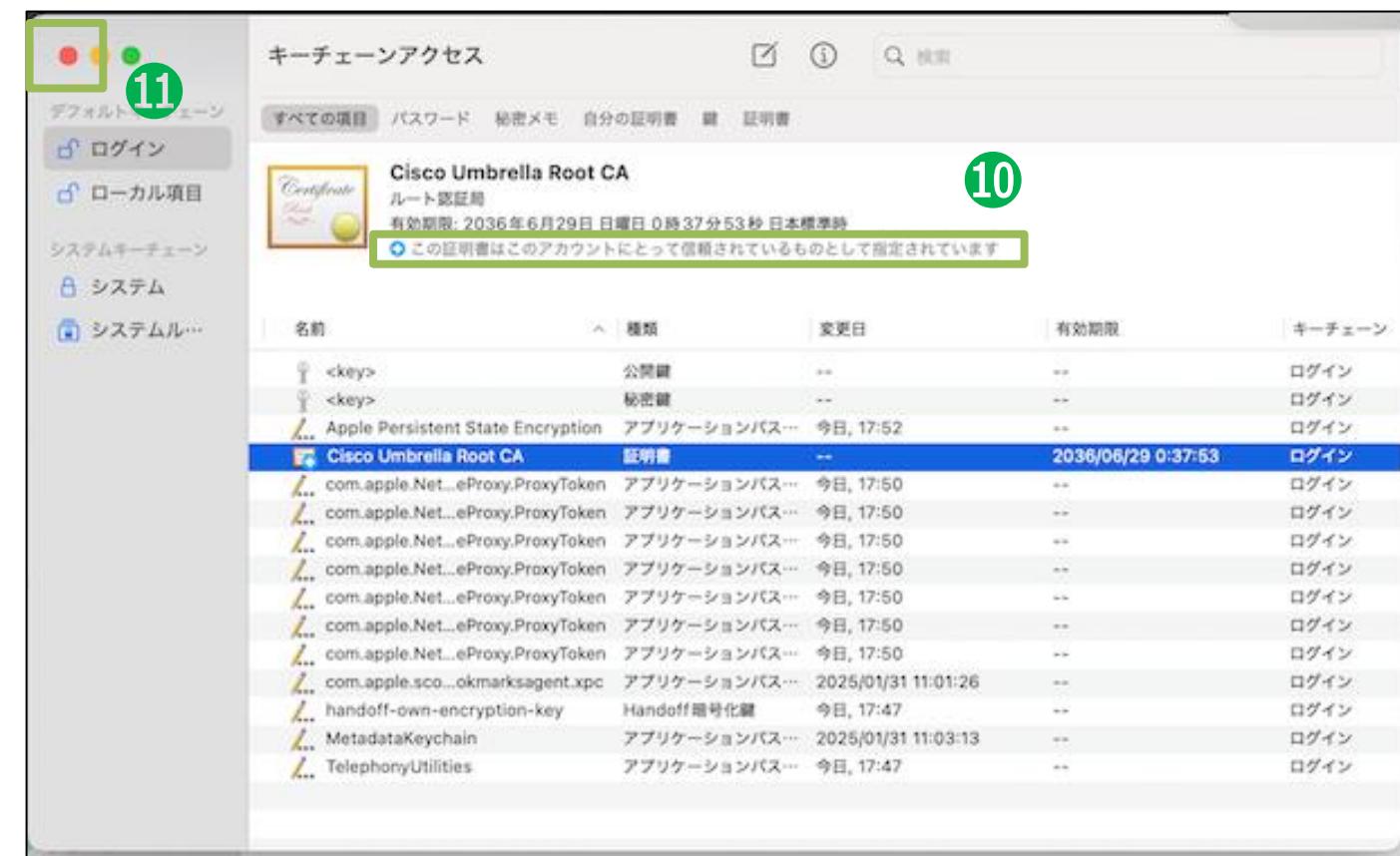
4-3. インストール手順 <ダウンロードしたインストーラの実行-16>

ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-3

👉 「この証明書を使用するとき」を「常に信頼」に変更



👉 信頼されているものとして指定されていることを確認し、画面を閉じる



4-4. ソフトウェアの起動／ステータス確認_Windows

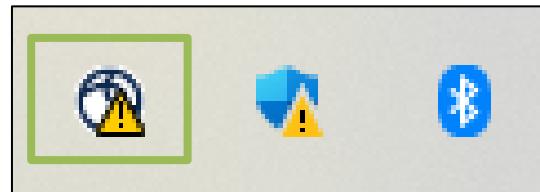
4-4. インストール手順 <ソフトウェアの起動／ステータス確認-1>

- ①インストールの完了後、「Ciscoセキュアクライアント」のアイコンが初期設定中となる（5分程度待機）
- ②初期選定が完了後、「Ciscoセキュアクライアント」のアイコンをクリック
- ③Ciscoセキュアクライアントのホーム画面に遷移
- ④「設定／歯車アイコン」をクリックし詳細ステータス確認に遷移

①初期設定中



または



5分程度
待機

②初期設定完了



👉 初期設定完了状態でクリック

※クラウドサーバとの通信状況により、アイコンが表示されるまでに5～10分程度かかる場合があります。

③セキュアクライアントホーム画面



👉 ④各アプリの詳細は次ページ

4-4. インストール手順 <ソフトウェアの起動／ステータス確認-2>

⑤「Secure Endpoint」を選択し、「エージェント※」のステータスが「接続中」であることを確認

※エージェント：ソフトウェアエージェント。ここではSecureEndpoint等のクライアントに常駐するソフトウェアを意味します。

⑥「Umbrella」を選択し、「DNS/IPセキュリティ情報」のステータスが「保護されています」、暗号化が「オン」であることを確認 「セキュアWebゲートウェイ」のライセンスが「有効」、Web保護ステータスが「保護されています」であることを確認

⑤Secure Endpointステータス情報



⑥Umbrellaステータス情報



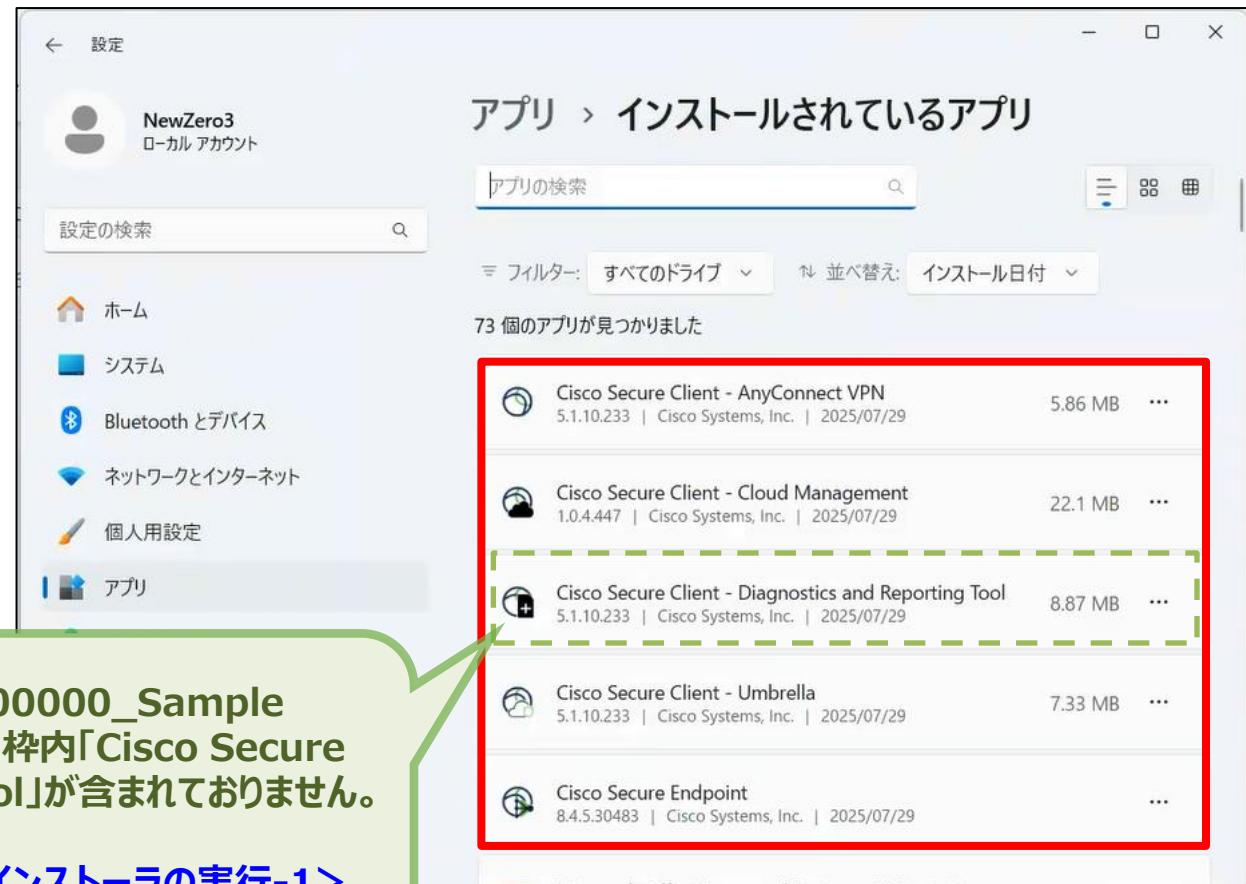
4-4. インストール手順 <ソフトウェアの起動／ステータス確認-3>

- ⑦「 スタートメニュー」から 設定をクリックしWindowsの設定から「アプリ」をクリック
⑧インストールされているアプリに以下「赤枠内」のアプリがインストールされていることを確認（※）

⑦アプリ画面の起動

「 スタートメニュー」から 設定をクリックし
Windowsの設定から「アプリ」をクリック

⑧インストールされているアプリの確認



※インストーラが①「csc-deploy-network-000000_Sample Corporation.exe」となっている方は、 枠内「Cisco Secure Client – Diagnostics and Reporting Tool」が含まれておりません。

参照：[4-3. インストール手順 <ダウンロードしたインストーラの実行-1>](#)

4-4. ソフトウェアの起動／ステータス確認_Mac

4-4. インストール手順 <ソフトウェアの起動／ステータス確認-1>

- ①インストール時の初期設定が完了後、画面右上の「Ciscoセキュアクライアント」アイコンが初期設定中となる
- ②「Ciscoセキュアクライアント」のアイコンを選択
- ③「Ciscoセキュアクライアント」を選択
- ④Umbrellaのステータスがアクティブとなっていることを確認

①初期設
定中



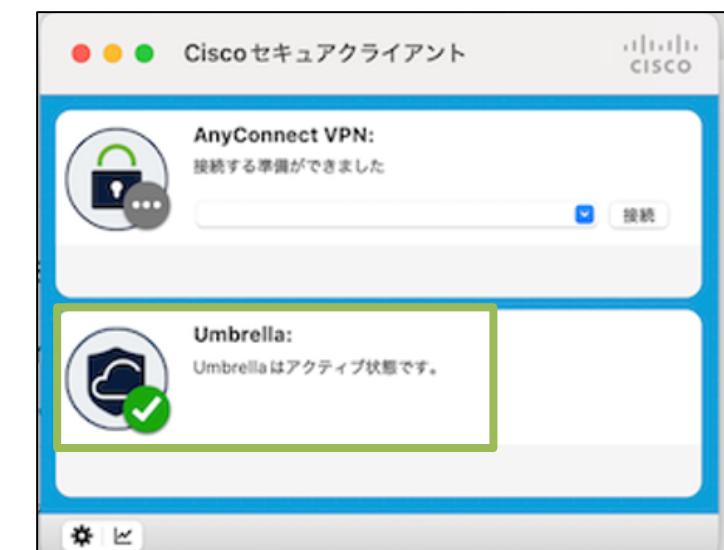
②初期設定
完了



③セキュアクライアントホーム画面を表示



④セキュアクライアントホーム画面



インストール設定後
自動遷移

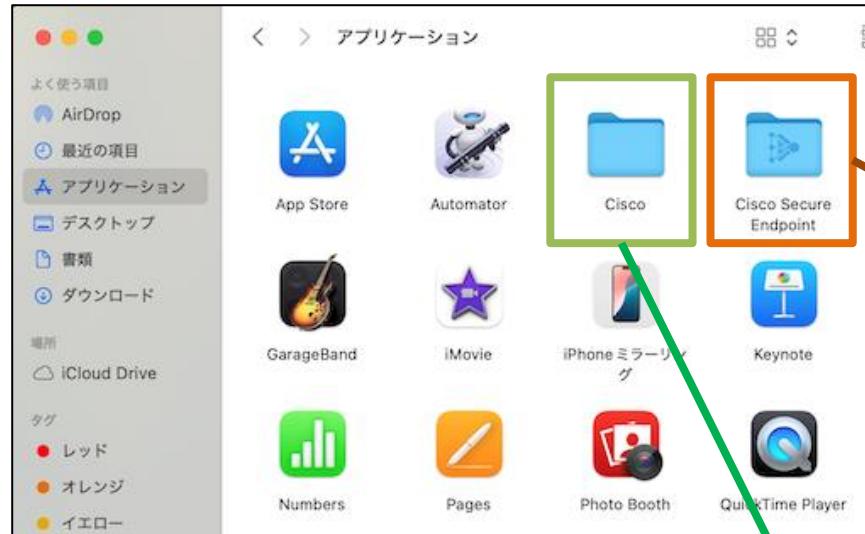
4-4. インストール手順 <ソフトウェアの起動／ステータス確認-2>

- ⑤インストール時の初期設定が完了後、画面右上の「Ciscoセキュアエンドポイント」アイコンが初期設定完了となる
- ⑥「Ciscoセキュアエンドポイント」のアイコンを選択
- ⑦ステータスが「接続中」となっていることを確認



4-4. インストール手順 <ソフトウェアの起動／ステータス確認-3>

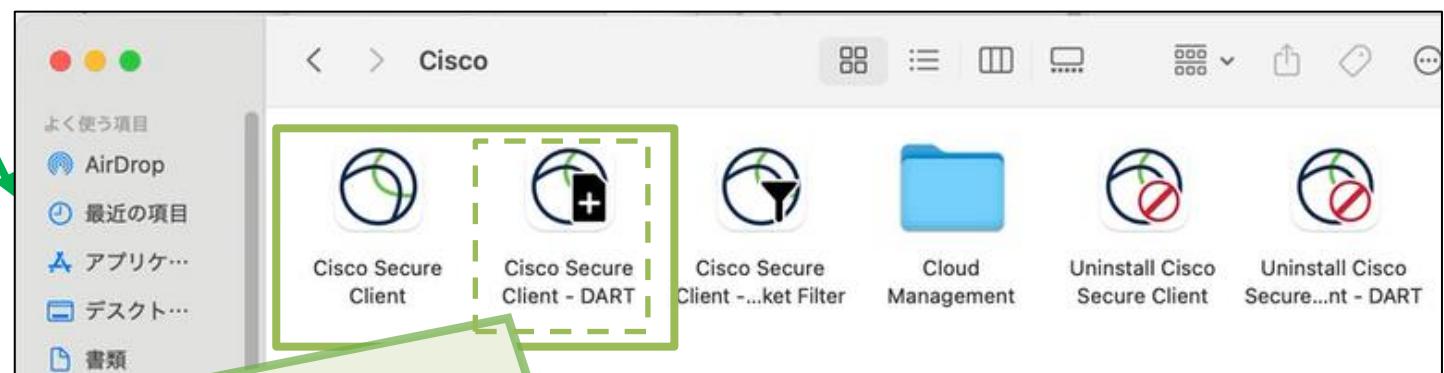
⑧Finderから「Cisco」、「Cisco Secure Endpoint」フォルダを開き、「Secure Endpoint コネクタ」、「Secure Endpointサービス」、「Cisco Secure Client」、「Cisco Secure Client-DART（※）」がインストールされていることを確認



⑧Cisco Secure Endpoint



⑧Cisco Secure Client(Umbrella)



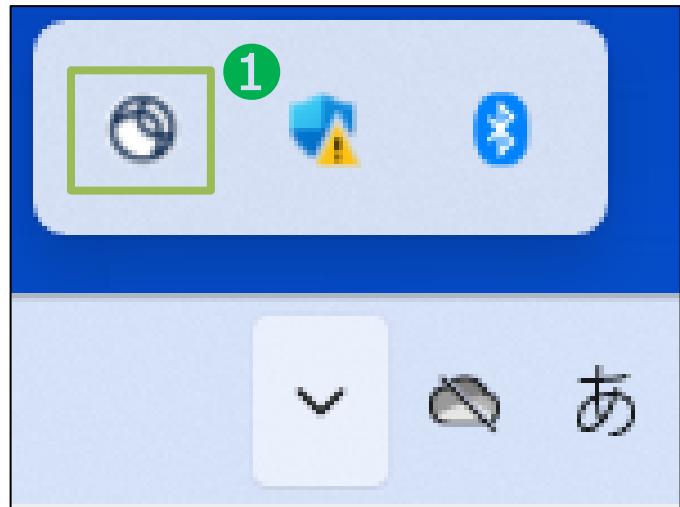
※インストーラが①「csc-deploy-network-[契約ID]_[会社名]_Mac用.dmg」となっている方は、「Cisco Secure Client – DART」が含まれておりません。
参照：4-3. インストール手順 <ダウンロードしたインストーラの実行-1>

5. ソフトウェアのアンインストール手順_Windows

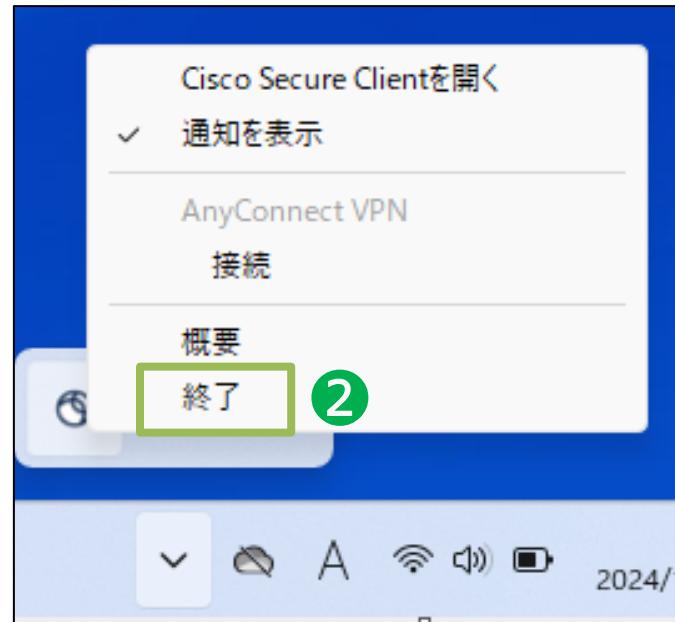
5. アンインストール手順<Cisco Secure Clientの停止-1>

実行中のCisco Secure Clientを停止させてください。

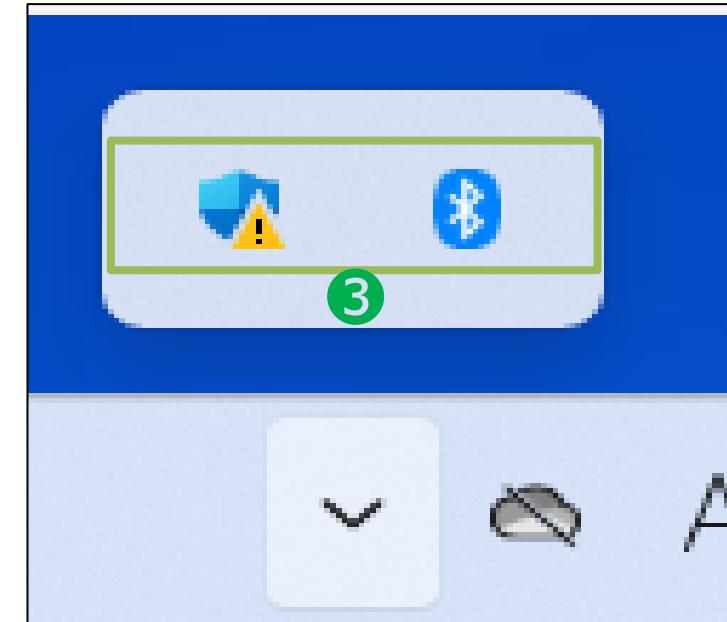
タスクバーから「Cisco Secure Client」を右クリック



「Cisco Secure Client」を終了させる



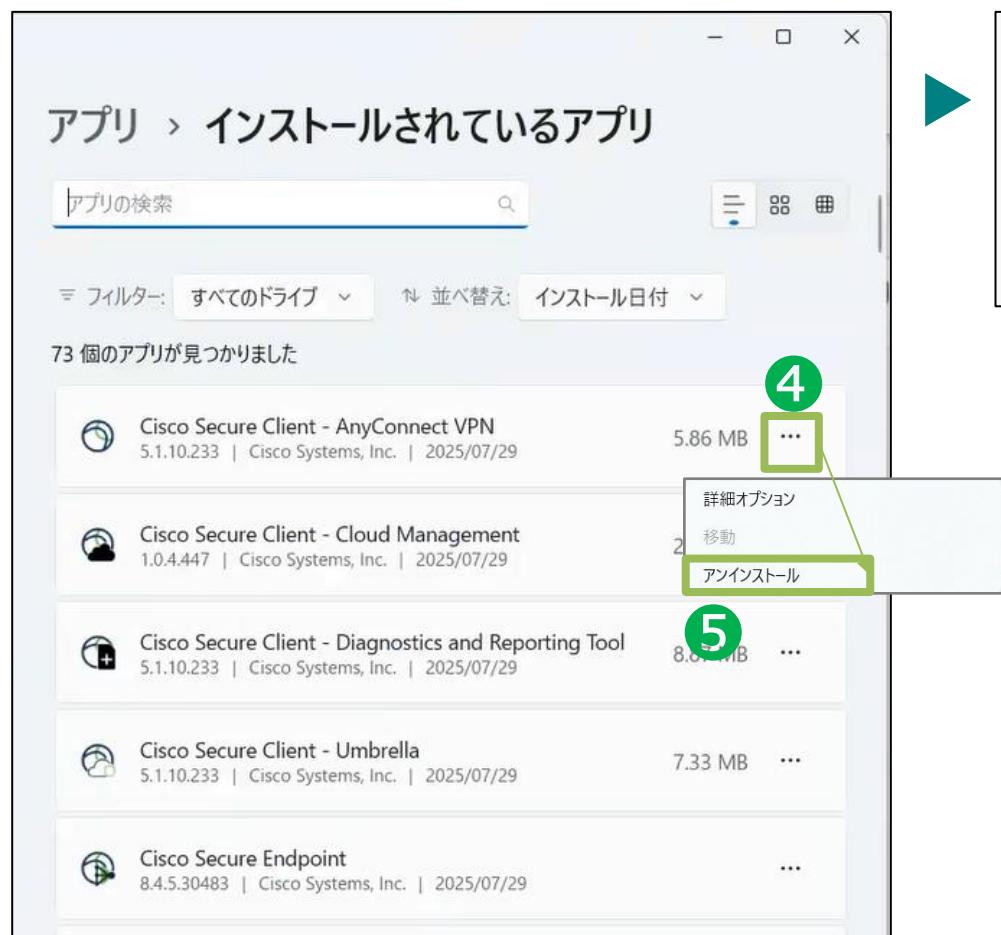
タスクバーから「Cisco Secure Client」が消えていることを確認する



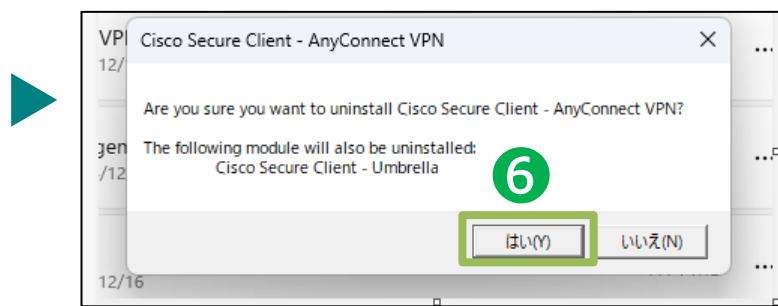
5. アンインストール手順 <ソフトウェアのアンインストール-1>

手順に従ってソフトウェアをアンインストールしてください。

「Windows」→「設定」→「アプリ」→「インストールされているアプリ」を開き、「Cisco Secure Client – AnyConnect VPN」をアンインストール



依存関係にあるUmbrellaも削除するか聞かれるので「はい」を選択



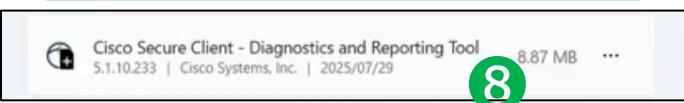
同様の手順で「Cisco Secure Client – Cloud Management」をアンインストール



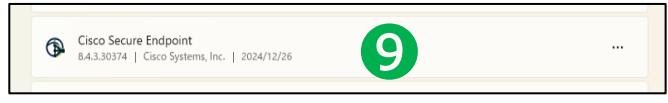
5. アンインストール手順 <ソフトウェアのアンインストール-2>

続けてソフトウェアをアンインストールしてください。

「Cisco Secure Client – Diagnostics and Reporting Tool」をアンインストール（※）



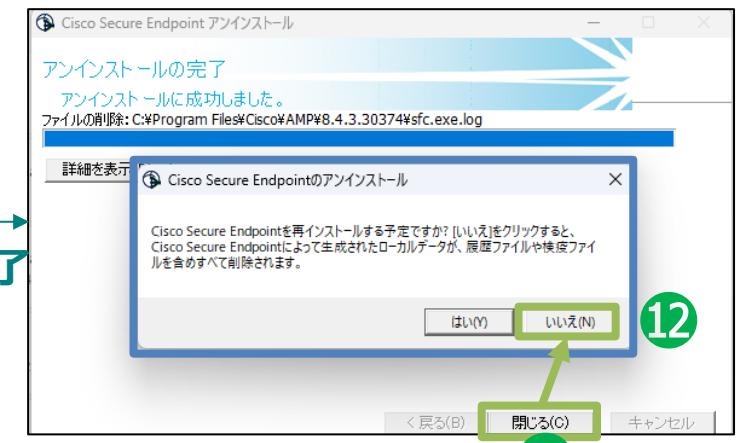
「Cisco Secure Endpoint」を
アンインストール



「次へ」でアンインストールを開始し、「閉じる」を選択すると、
再インストール時用のキャッシュを残すか聞かれるので
「いいえ」を選択



1分程度で
アンインストールが完了



※インストーラが、
①「csc-deploy-network-
000000_Sample Corporation.exe」となっ
ている場合、上記アプリはございません。

参照：[4-3. インストール手順 <ダウンロードしたイ
ンストーラの実行-1>](#)

5. ソフトウェアのアンインストール手順_Mac

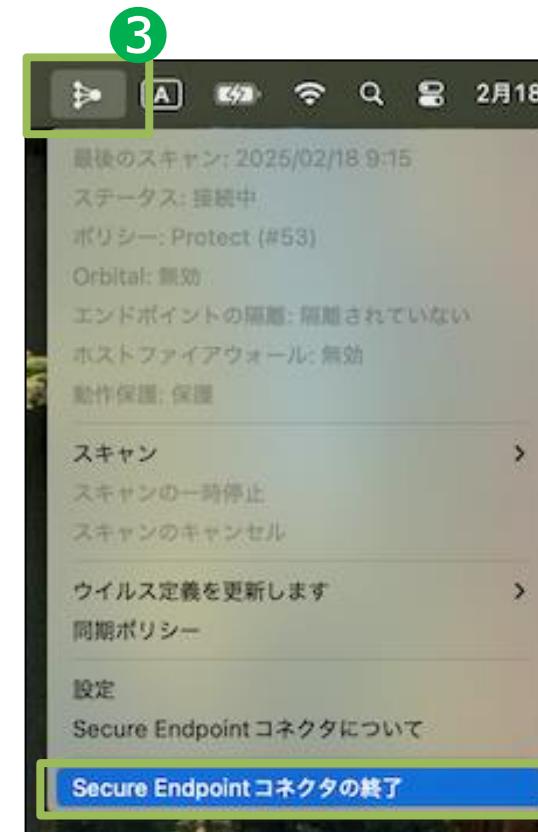
5. アンインストール手順 <Ciscoアプリケーションの停止>

実行中のCiscoアプリケーションを停止させてください。

画面右上の「Cisco Secure Client」をクリックし、終了させる



画面右上の「Secure Endpointコネクタ」をクリックし、終了させる



画面右上のアイコンが消えていることを確認する



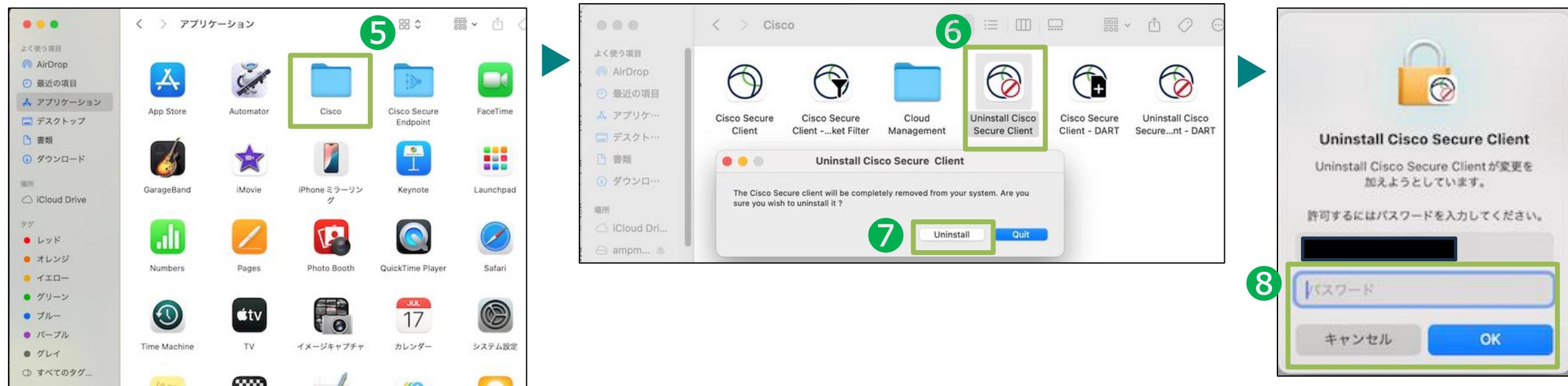
5. アンインストール手順 <ソフトウェアのアンインストール-1>

手順に従ってソフトウェアをアンインストールしてください。

Finder[] から「Cisco」フォルダを開く

「Uninstall Cisco Secure Client」を
ダブルクリックし、「Uninstall」を選択

パスワードを入力し、
「OK」を選択



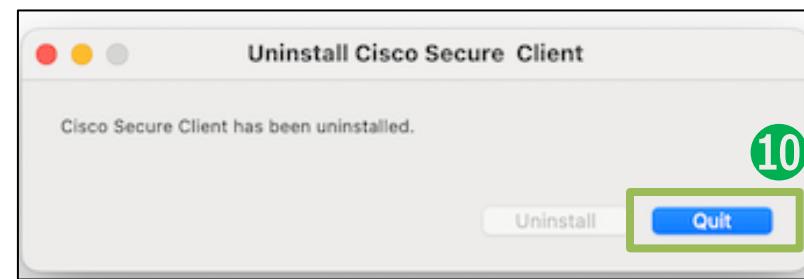
5. アンインストール手順 <ソフトウェアのアンインストール-2>

手順に従ってソフトウェアをアンインストールしてください。

続けてパスワードを入力し
「OK」を選択

「Quit」を選択して閉じる

「Uninstall Cisco Secure…nt - DART」を
ダブルクリックし、「Uninstall」を選択（※）



※インストーラが、
①「csc-deploy-network-[契約ID]_[会社名]_Mac用.dmg」の場合、上記アプリはございません。

参照：[4-3. インストール手順 <ダウンロードしたインストーラの実行-1>](#)

5. アンインストール手順 <ソフトウェアのアンインストール-3>

手順に従ってソフトウェアをアンインストールしてください。

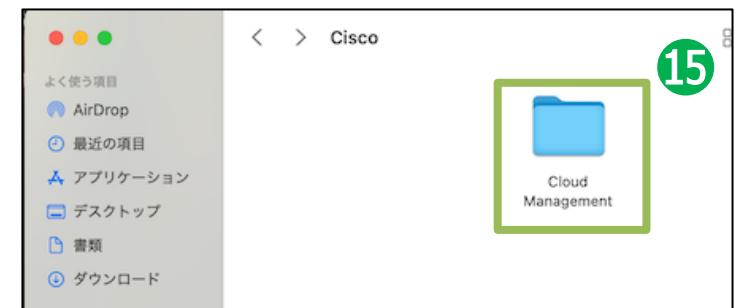
続けてパスワードを入力し
「OK」を選択



「Quit」を選択して閉じる



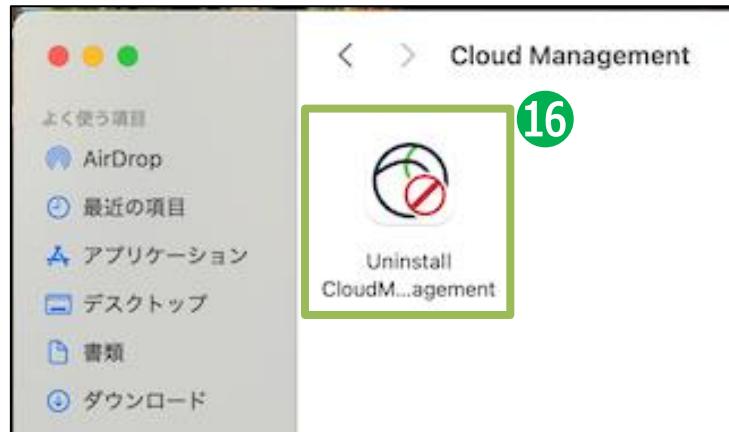
Ciscoフォルダに残った
「Cloud Management」フォルダを開く



5. アンインストール手順 <ソフトウェアのアンインストール-4>

手順に従ってソフトウェアをアンインストールしてください。

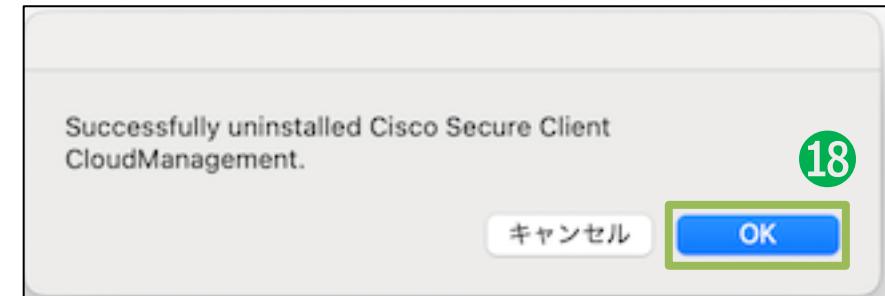
「Uninstall CloudManagement」をダブルクリック



パスワードを入力し、「OK」を選択



「OK」を選択



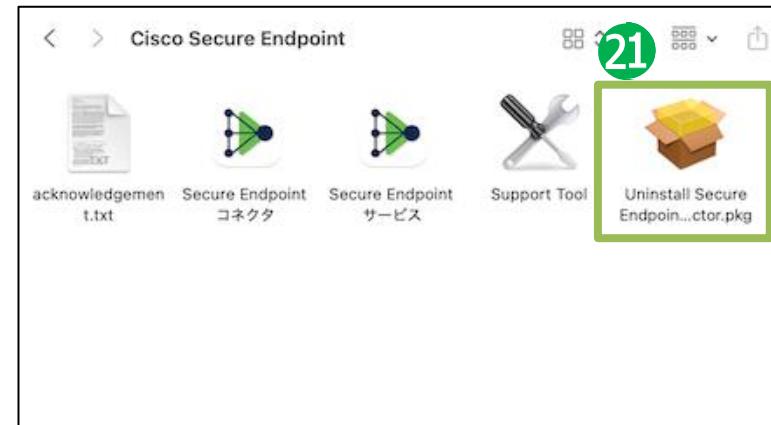
5. アンインストール手順 <ソフトウェアのアンインストール-5>

手順に従ってソフトウェアをアンインストールしてください。

アプリケーションフォルダに戻り、「Cisco Secure Endpoint」フォルダを開く



「Uninstall Secure Endpoint Connector.pkg」をダブルクリック



「続ける」を選択



5. アンインストール手順 <ソフトウェアのアンインストール-6>

手順に従ってソフトウェアをアンインストールしてください。

「インストール」を選択
(アンインストール用のアプリケーションをインストールします)



パスワードを入力し、
「ソフトウェアをインストール」を選択



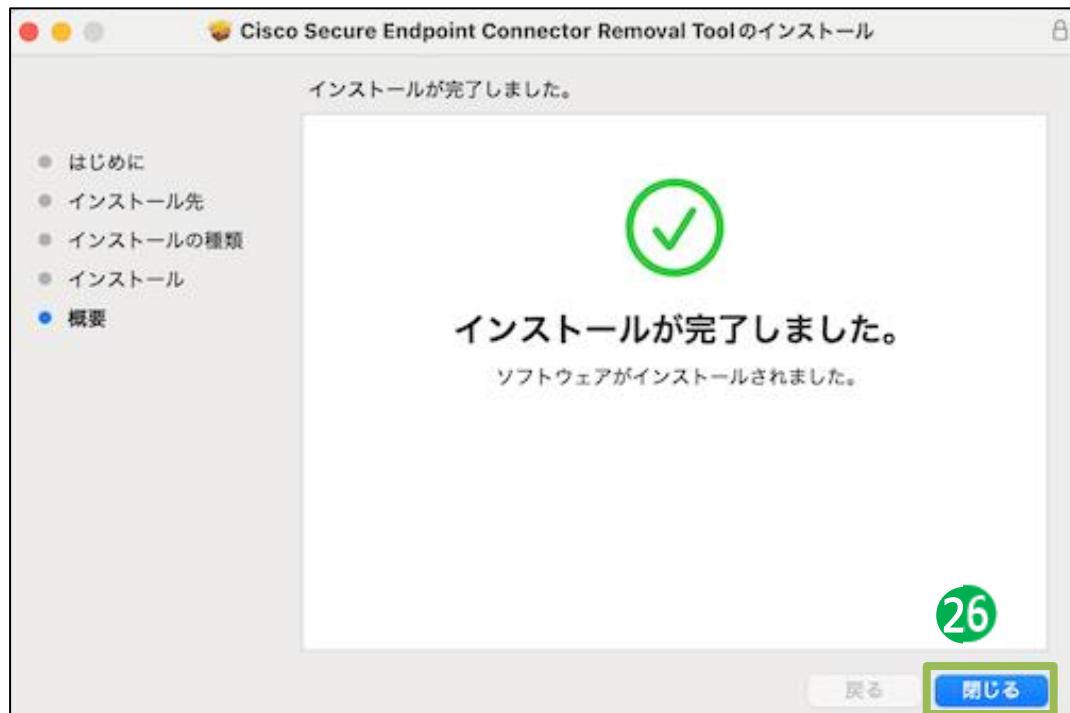
続けて、パスワードを入力し、
「OK」を選択



5. アンインストール手順 <ソフトウェアのアンインストール-7>

手順に従ってソフトウェアをアンインストールしてください。

「閉じる」を選択



アプリケーションフォルダに戻り、
不要な「Cisco」フォルダを削除

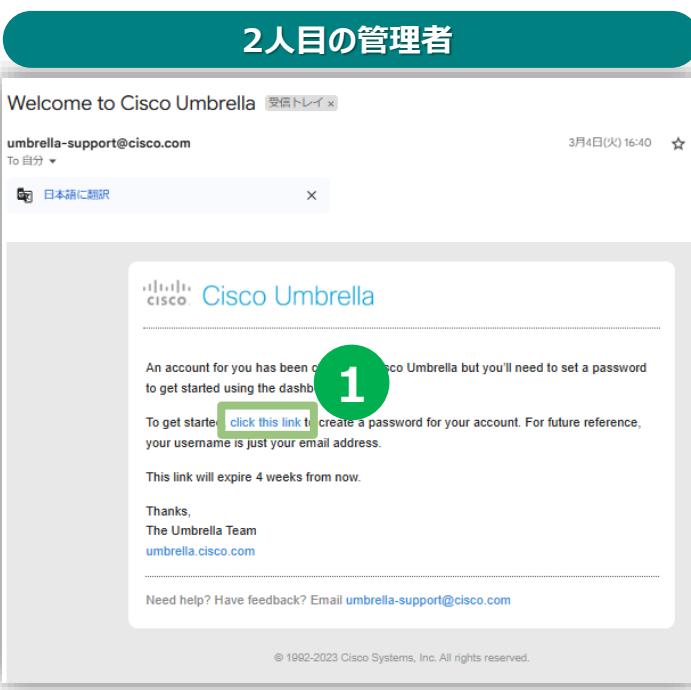
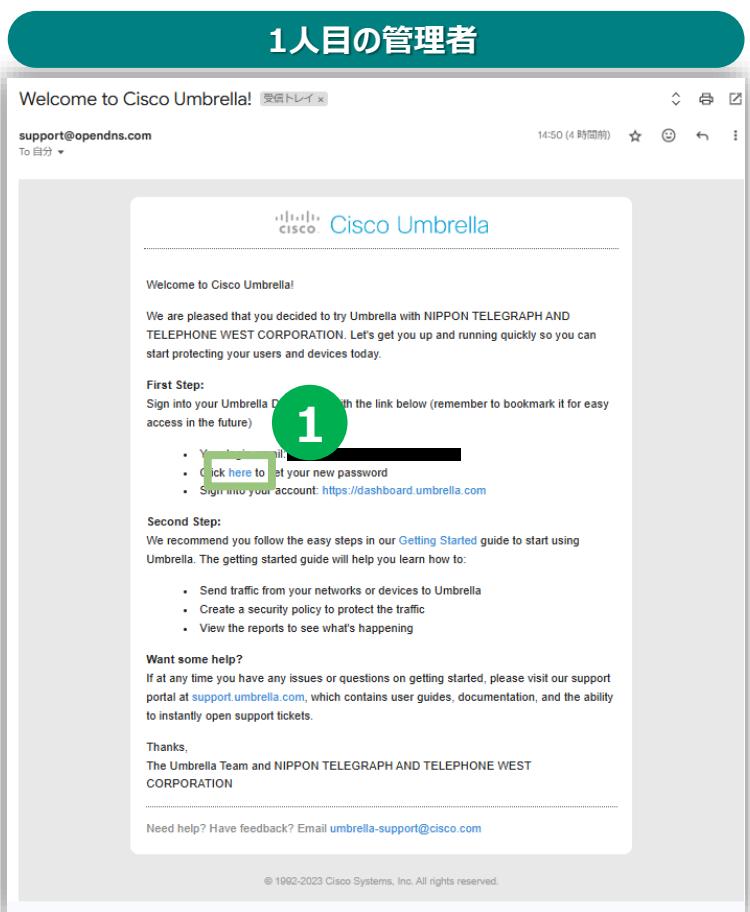


6. セキュアインターネットゲートウェイ コンソールへのログイン手順 < Cisco Umbrella SIG Essentials >

6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

管理者向けのインビテーションメールを受信してから管理コンソール ログインまでの手順を記載します。

- ① 1人目の管理者は受信した電子メールから枠内の[here]をクリック
2人目の管理者は受信した電子メールから枠内の [click this link]をクリック
- ② [氏名]、[電子メール^{※1}]、[パスワード^{※2}]を入力
※1電子メールには申込書に記載したメールアドレスを記載ください ※2設定するパスワードには条件があります（図の②下部をご参照ください）
- ③ [パスワードのリセット]をクリック



CISCO

ようこそ!

下記に情報を入力します。パスワードが設定されると、Umbrellaダッシュボードにログインできます。

名

姓

電子メール

パスワード

パスワードの確認

パスワードは次のとおりです。

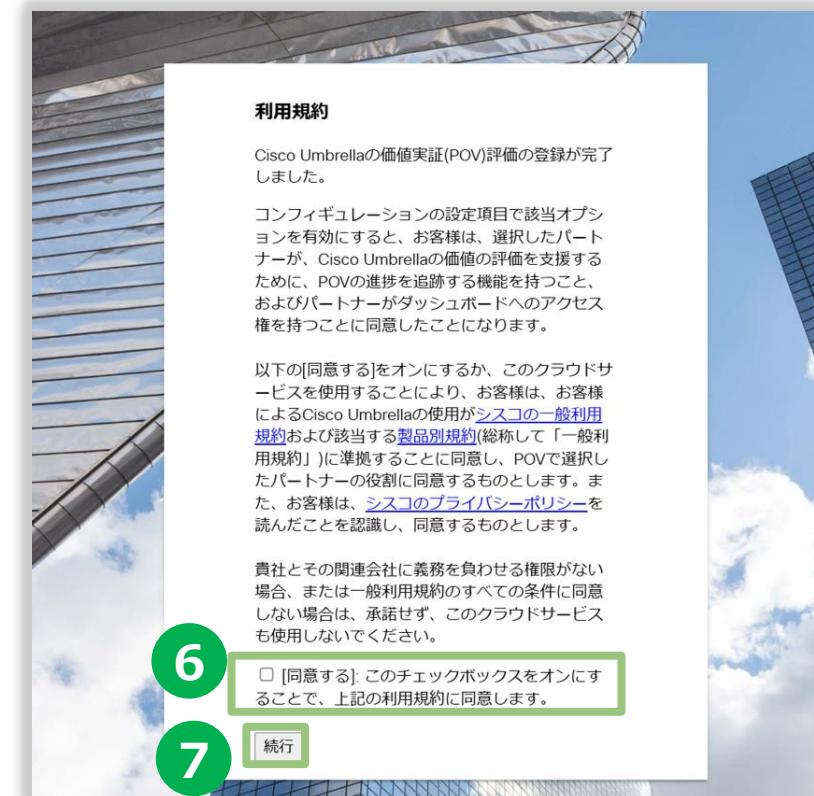
- 8~256文字である必要があります
- 大文字と小文字を少なくとも1文字ずつ含めます
- また、少なくとも1つの数字と1つの特殊文字(*、\$、!など)が含まれている必要があります
- ユーザ名の一部を含めることはできません

3 [パスワードのリセット](#)

キャンセル

6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ④ 前手順で入力した[電子メールアドレス]と[パスワード]を入力
- ⑤ [ログイン]をクリック
- ⑥ [同意する]のチェックボックスをクリック
- ⑦ [続行]をクリック



6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ⑧ [手順をスキップ]をクリック
- ⑨ [この手順をスキップ]をクリック
- ⑩ [CISCO UMBRELLAの使用の開始]をクリック



6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

⑪ ログインに成功するとUmbrellaのトップ画面が表示されます。

The screenshot shows the Cisco Umbrella dashboard interface. On the left, there is a dark sidebar with navigation links: '概要' (Overview), '導入' (Introduction), 'ポリシー' (Policy), 'レポート' (Report), 'Investigate' (Investigate), '管理' (Management), 'ドキュメント' (Documents), 'サポートプラットフォーム' (Support Platform), 'ラーニングセンターへ' (Go to Learning Center), 'シスコオンラインプライバシーステートメント' (Cisco Online Privacy Statement), and '利用規約' (Terms of Use). A user profile icon is also present.

The main content area is titled '概要' (Overview) and displays the following information:

- 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 (Deployment Health):

- アクティブなネットワーク: 0% (0 / 1 アクティブ)
- アクティブなローミングクライアント: 0% (0 / 0 アクティブ)
- アクティブな仮想アプライアンス: 0% (0 / 0 アクティブ)
- アクティブなネットワークトンネル: 0% (非トラッキングデータ)

ネットワークの分析 (Network Analysis):

- すべて (selected)
- DNS
- WEB

総リクエスト件数 (Total Requests): 合計0 - 0% 過去24時間との比較 (Comparison).

検索結果がありません (No search results). 検索の時間範囲を拡大してみてください。

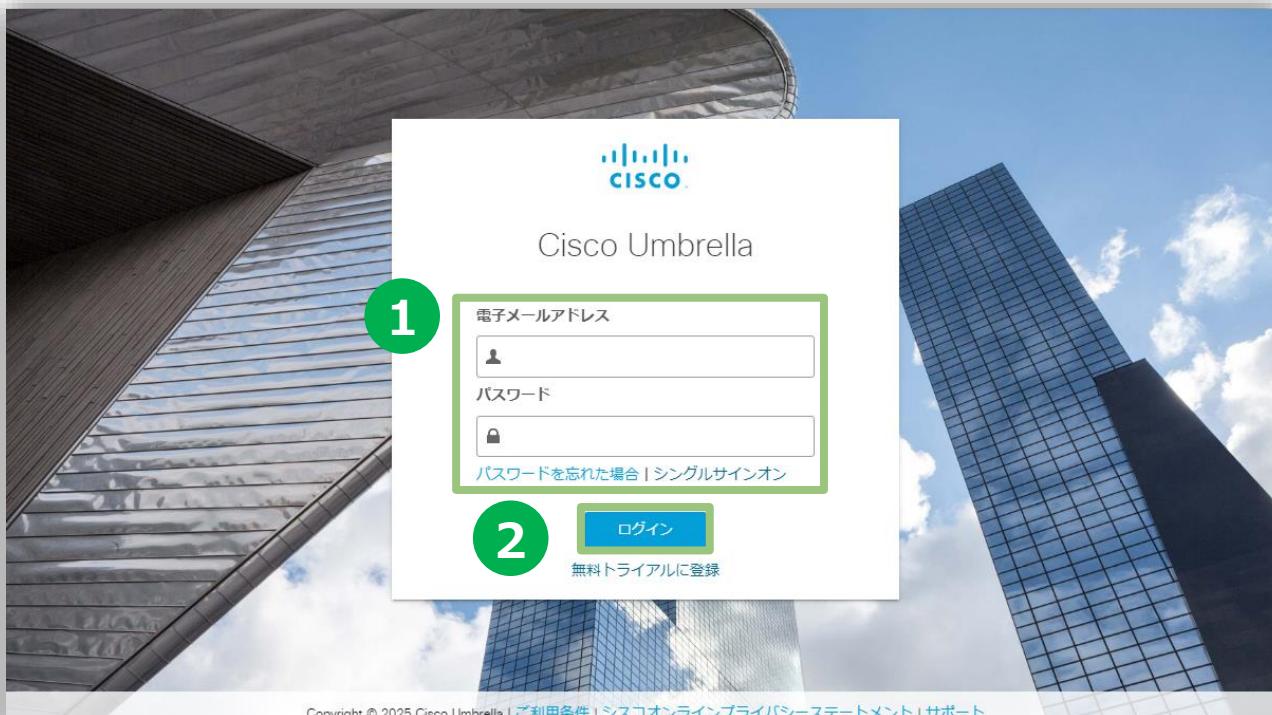
A 'Get Started' button is located on the right side of the dashboard.

6. コンソールへのログイン手順 <システムログイン>

各ユーザテナントへのCisco Umbrellaへのログイン方法を示します

- ① ログインID(電子メールアドレス)/パスワードを入力
- ② [ログイン]をクリック⇒ログイン後、トップ画面が表示されます。

<アクセスURL <https://login.umbrella.com>>



Umbrella ログイン画面

The image shows the Cisco Umbrella dashboard. At the top, there's a navigation bar with '概要' (Overview), 'Settings', 'スケジュール' (Schedule), and a '過去24時間' (Past 24 hours) button. The main area is titled '概要' (Overview) and displays '0 Messages'. It includes sections for 'Malware', 'Botnet', 'Cryptomining', and device status for 'WIN-TCBOOQ9KFE: is in a state of error' and 'Umbrella-VA1: is in a state of error'. Below this is a section for '導入の健全性' (Deployment Health) showing network status: 'アクティブなネットワーク' (Active Network) at 17% (1/6 active), 'アクティブなローミングクライアント' (Active Roaming Client) at 0% (0/0 active), and 'アクティブな仮想アプライアンス' (Active Virtual Appliance) at 0% (0/2 active). At the bottom, there's a 'ネットワークの分析' (Network Analysis) section with tabs for 'すべて' (All), 'DNS', and 'WEB'.

ログイン トップ画面

6. コンソールへのログイン手順 <ダッシュボード説明>

概要ページ（ダッシュボード）では全カテゴリの統計情報を見やすい形で表示します。
Cisco Umbrellaへログイン、または左メニューの[概要]をクリックするとダッシュボード(概要)画面が表示されます。

The screenshot displays the Cisco Umbrella Dashboard interface. On the left, a sidebar menu includes '導入' (Introduction), 'ポリシー' (Policy), 'レポート' (Report), 'Investigate', '管理' (Management), and a user profile section for 'Test Accoun NOP west Takashi Kato' under 'NOP-LAB'. The main dashboard area has a title '概要' (Overview) with a 'Cisco' logo. It features several sections: '0 Messages' with links to 'Malware', 'Botnet', 'Cryptomining', and error logs for 'WIN-TCBOQ09KFE' and 'Umbrella-VA2/VA1'; '導入の健全性' (Deployment Health) with four status cards: 'アクティブなネットワーク' (17%, 1/6 active), 'アクティブなローミングクライアント' (0%, 0/0 active), 'アクティブな仮想アプライアンス' (0%, 0/2 active), and 'アクティブなネットワークトンネル' (33%, 2/6 active); 'ネットワークの分析' (Network Analysis) with tabs for 'すべて' (All), 'DNS', and 'WEB', and a checkbox for 'すべてのセキュリティイベントを見る' (View all security events); and a 'Get Started' button on the right.

6. コンソールへのログイン手順 <ダッシュボード説明>

Cisco Umbrellaのダッシュボードの主な機能とその内容について示します。

[Messages]

コンソールからのメッセージ情報を表示

[導入の健全性]

アクティブ アイデンティティ／トータル アイデンティティ情報を表示

※アイデンティティとはUmbrellaへの接続元デバイスを指します

[ネットワークの分析]

DNSクエリ／Webトラフィックの統計情報や各ブロックカテゴリの統計情報を表示

[ファイアウォールの内訳]

ファイアウォールで処理した統計情報を表示

[IPSの分類]

IPSイベントの統計情報を表示

[セキュリティカテゴリ]

各ブロックカテゴリの統計情報を表示

[アプリケーションの検出と制御]

利用アプリケーションおよび制御イベントの統計情報を表示

[セキュリティリクエスト]

DNS／WEBで接続の多い統計情報を 宛先／アイデンティティ／イベントタイプ の視点から表示

[ファイルレトロスペクティブ]

レトロスペクティブにより（過去に遡り）悪意あるものと判断されたファイルを表示

7. セキュアインターネットゲートウェイ機能を設定変更する < Cisco Umbrella SIG Essentials >

7. セキュアインターネットゲートウェイ機能を設定変更する（設定変更例一覧）

弊社推奨設定でサービスをご利用開始いただいておりますが、ご利用環境やセキュリティポリシーに応じて、設定の変更をお願いいたします。

トラブル対応による設定変更例

- 1-1. 特定のサイトが見られない①
- 1-2. 特定のサイトが見られない②
- 2. インターネットが使えない
- 3. 導入後、通信速度が遅くなった
- 4. 「セキュリティ証明書に問題があります」と表示される
- 5. 共有フォルダにアクセスできない
- 6. ベンダーのリモートツールが動かない
- 7. 新しいパソコンでメールの送受信ができない
- 8. 500番台のエラーメッセージが表示される

ご利用環境等に応じた設定変更例

- 9. DNSポリシーを変更したい
- 10. 広告のページを開けるようにしたい
- 11. 怪しいサイトがUmbrellaの検知をすり抜けている
- 12. Umbrellaの許可リスト・ブロックリストを設定したい
- 13. CASB^{*}の設定方法を知りたい
- 14. CASB^{*}の機能を利用して組織が利用しているクラウドサービスの状況を確認したい
- 15. CASB^{*}の機能を利用して会社が契約しているテナントにのみアクセスさせたい
- 16. Umbrellaでユーザの利用しているアプリの可視化をし、特定アプリをブロックしたい
- 17. 内部ドメインを参照したい

※ Cloud Access Security Broker。SaaSアプリケーションの利用状況を可視化。リスクを評価してブロックを行ったり、会社契約のテナントを区別してアクセスすることも可能。

Cisco Umbrella がサイトの安全性を確認できない場合、その通信を遮断する場合があります。表示を行うためには管理コンソールで、対象のサイトへの通信を許可する設定を行う必要があります。サイトに問題がないと判断できる場合のみ、下記手順で許可設定をお願いします。

許可／ブロックリスト設定方法

- ①左側のメニューより「ポリシー」－「ポリシーコンポーネント」－「接続先リスト」をクリックし、接続先リスト管理画面にて実施します。

The screenshot shows the Cisco Umbrella management interface. On the left, a vertical navigation menu is displayed with several sections highlighted by red boxes:

- 概要 (Overview)
- 導入 (Import)
- ポリシー (Policy)**
- 管理 (Management)
- DNSポリシー (DNS Policy)
- ファイアウォールポリシー (Firewall Policy)
- Webポリシー (Web Policy)
- ポリシーコンポーネント (Policy Component)**
- IPS SIGニチャリスト (IPS Signature List)
- 接続先リスト (Connection List)**
- コンテンツカテゴリ (Content Category)
- アプリケーション設定 (Application Settings)
- テナント制御 (Tenant Control)
- スケジュール設定 (Schedule Settings)
- セキュリティ設定 (Security Settings)
- ブロックページ外観 (Block Page Appearance)
- 統合 (Integration)
- 選択的署名リスト (Selective Signature List)
- レポート (Report)
- Investigate
- 管理 (Management)

The main content area is titled "ポリシー / ポリシーコンポーネント" and "接続先リスト" (Connection List). It includes a descriptive text about using connection lists to block or allow domains. Below this is a search bar and two tables:

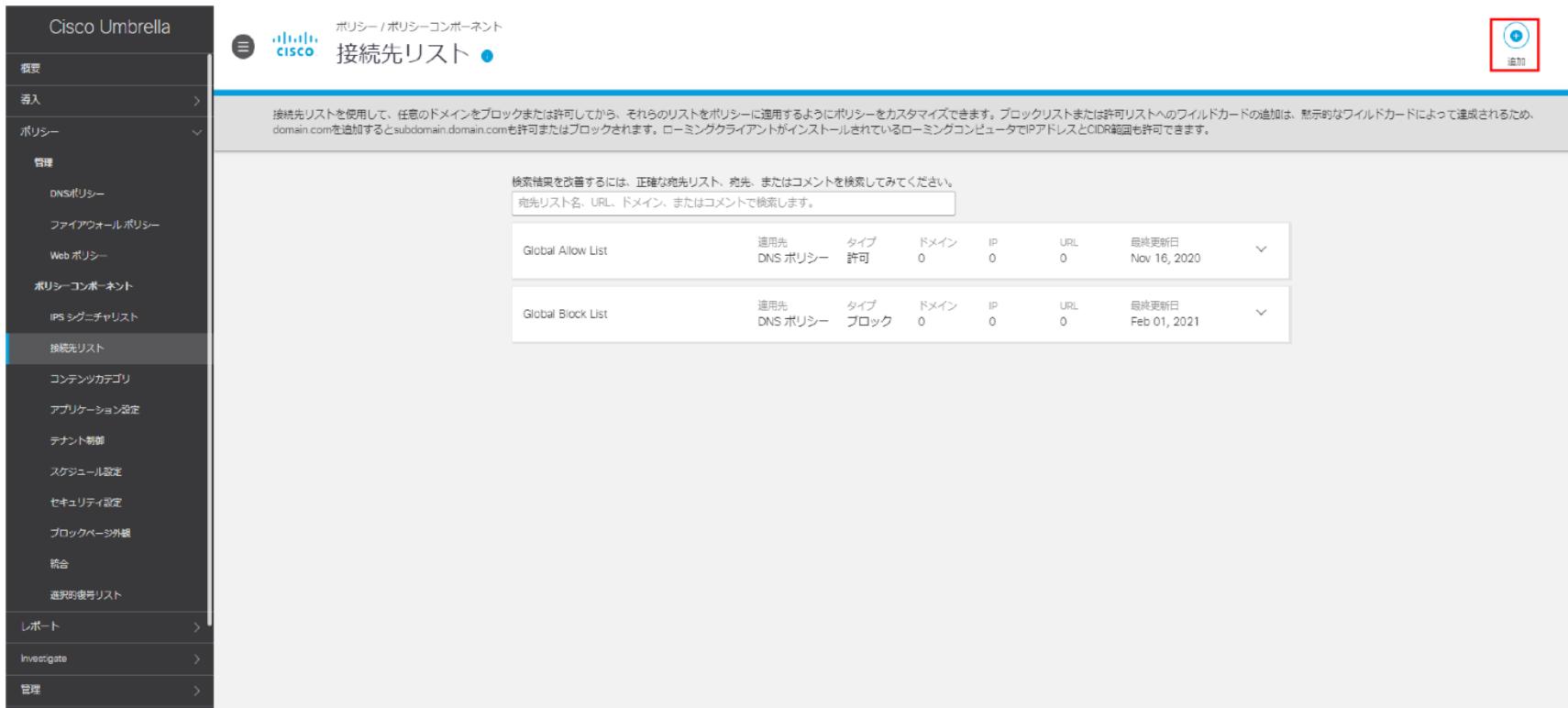
| 接続先リスト名 | 適用先 | タイプ | ドメイン | IP | URL | 最終更新日 |
|-------------------|----------|-----|------|----|-----|--------------|
| Global Allow List | DNS ポリシー | 許可 | 0 | 0 | 0 | Nov 16, 2020 |

| 接続先リスト名 | 適用先 | タイプ | ドメイン | IP | URL | 最終更新日 |
|-------------------|----------|------|------|----|-----|--------------|
| Global Block List | DNS ポリシー | ブロック | 0 | 0 | 0 | Feb 01, 2021 |

A "追加" (Add) button is located in the top right corner of the main content area.

許可／ブロックリスト設定方法（つづき）

②画面右上の「追加」をクリックします。



The screenshot shows the Cisco Umbrella web interface. On the left, there's a sidebar with various navigation options like '検索', '導入', 'ポリシー', '管理', etc. The main content area is titled '接続先リスト' and contains a message about using connection peer lists to block or allow domains. Below this is a search bar and two tables: 'Global Allow List' and 'Global Block List'. The 'Add' button in the top right corner is highlighted with a red box.

| 接続先リスト名 | 適用先 | タイプ | ドメイン | IP | URL | 最終更新日 |
|-------------------|----------|------|------|----|-----|--------------|
| Global Allow List | DNS ポリシー | 許可 | 0 | 0 | 0 | Nov 16, 2020 |
| Global Block List | DNS ポリシー | ブロック | 0 | 0 | 0 | Feb 01, 2021 |

許可／ブロックリスト設定方法（つづき）

- ③「リスト名」に新しい接続先リストを設定します。
同じリスト名を複数登録できるため、混乱を避けるためにも一意のリスト名を設定します。

The screenshot shows the Cisco Umbrella web interface. On the left, a dark sidebar menu lists various policy components: Overview, Import, Policies (with DNS, Firewall, Web), Policy Components (with Connection Target List selected), Content Categories, Application Settings, Tenant Control, Schedules, Security Settings, Block Page View, Global Settings, Selected Block Lists, Reports, and Investigate.

The main content area is titled "ポリシー / ポリーコンポーネント" (Policy / Policy Component) and "接続先リスト" (Connection Target List). It includes a descriptive text about connection target lists and a search bar. A large central form is titled "新しい接続先リスト" (New Connection Target List). The "リスト名" (List Name) field contains "テストDNSポリシー" (Test DNS Policy), which is highlighted with a red rectangle. The "送信先リストタイプ" (Recipient List Type) dropdown is set to "Select...". Below it, the question "このリストに含まれている接続先は:" (The connections in this list are:) has two radio buttons: "ブロック" (Block) and "許可" (Allow), with "Block" selected. The "目的地" (Destination) section contains a text input field with "ドメインまたは URL" (Domain or URL) and a "追加" (Add) button. Below this is a message stating "このリストに接続先が追加されていません" (No connections have been added to this list). At the bottom, there are pagination controls ("Page: 1", "Results per page: 10", "1-0 of 0") and buttons for "キャンセル" (Cancel) and "保存" (Save).

許可／ブロックリスト設定方法（つづき）

- ④「この 接続先リスト 次に適用されます」で
DNSポリシーを作成する場合：DNSポリシーを選択し、⑤に進む。
Webポリシーを作成する場合：Webポリシーを選択し、⑥に進む。

The screenshot shows the Cisco Umbrella web interface. On the left, a dark sidebar menu lists various policy components: Overview, Import, Policy (selected), Management (DNS Policy, Firewall Policy, Web Policy), Policy Components (Connections), Content Categories, Application Settings, Tenant Filtering, Scheduling, Security Settings, Block Page Overview, Integration Settings, and Selectional Whitelist. Below these are Reports and Investigate sections.

The main content area is titled "Policy / Policy Component" and "Connections List". It contains a descriptive text about connection lists and their purpose. A search bar at the top allows filtering by "Recipient List Name" or "Search".

A central form is titled "New Connection List" and includes fields for "List Name" (set to "Test DNS Policy") and "Recipient List Type" (set to "DNS Policy", which is highlighted with a red box). Below this, it says "This list contains the following connections: Block (radio button selected) or Allow (radio button unselected)."

The "Destination" section contains a field for "Domain or URL" (set to "Domain or URL") and a "Count" field showing "0 total". Below this, a note says "No connections have been added to this list." At the bottom, pagination controls show "Page: 1" and "Results per page: 10".

At the bottom right of the main panel are "Cancel" and "Save" buttons. To the right of the main panel, there is a vertical sidebar with a "Get Started" button and a Cisco logo.

許可／ブロックリスト設定方法（つづき）

⑤ DNSポリシーを作成する場合

「このリストに含まれている接続先は」で以下の通り選択する。

- 接続拒否リストを作成する場合：ブロック（見せたくないサイトを見られないようにする場合は、こちらを選択）
接続許可リストを作成する場合：許可（見れないサイトを見られるようにする場合は、こちらを選択）

The screenshot shows the Cisco Umbrella web interface with the following details:

- Sidebar Navigation:** Includes links for Overview, Import, Policies, Management, DNS Policy, Firewall Policy, Web Policy, Policy Components, Connection List (highlighted), Content Categories, Application Settings, Tenant Control, Schedule Settings, Security Settings, Blockpage Exempt, Global Settings, and Selected Blocklist.
- Header:** Shows the Cisco logo and the title "Policy / Policy Component" followed by "Connection List".
- Information Panel:** Describes what a connection list is: "A connection list is a list of destinations that are controlled by Umbrella policies using Internet destination rules." It notes that lists are policy-specific and must be added to the policy before being added to Umbrella.
- Form Fields:**
 - "Recipient List Name": "新しい接続先リスト"
 - "Recipient List Type": "DNS Policy" (selected)
 - "This list contains the following connections (radio button group):
 - Block (selected)
 - Allow
 - "Destination": "Domain or URL": "ドメインまたは URL" (empty)
 - "Buttons at the bottom right: "Cancel" and "Save"
- Footer:** Includes "Page: 1" and "Results per page: 10" with navigation arrows, and a "Get Started" button.

許可／ブロックリスト設定方法（つづき）

【DNSポリシー用に宛先を追加する場合の画面】

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 >

Investigate >

ポリシー / ポリシーコンポーネント

接続先リスト 1

宛先リストは、これらのリストされた宛先へのアイデンティティアクセスを制御するために Umbrella ポリシーで使用されるインターネット宛先のリストです。宛先リストのタイプに応じて、これらの宛先はドメイン、URL、または CIDR になります。宛先リストはポリシータイプ(DNS または Web)に固有であり、ポリシーに追加する前に Umbrella に追加する必要があります。

送信先リスト名 検索

新しい接続先リスト

リスト名 テストWEBポリシー

送信先リストタイプ DNSポリシー

このリストに含まれている接続先は:
 ブロック 許可

目的地 ドメインまたは URL

このリストに接続先が追加されていません

接続先が見つかりませんでした

Page: 1 Results per page: 10 1-0 of 0 < >

追 削除

キャンセル 保存

許可／ブロックリスト設定方法（つづき）

⑥Webポリシーを作成する場合：

対象の宛先を赤枠に設定し、右側の「追」ボタンをクリックします。
設定できる値は、以下の通りです。

| No | 適用先 | 種別 | 設定できる値 | | |
|----|----------|---------|--------|------|-------------|
| | | | ドメイン | URL | IPv4またはCIDR |
| 1 | DNS ポリシー | 接続拒否リスト | 利用可 | 利用不可 | 利用不可 |
| 2 | | 接続許可リスト | 利用可 | 利用不可 | 利用可 |
| 3 | Webポリシー | - | 利用可 | 利用可 | 利用可 |

【Webポリシー用に宛先を追加する場合の画面】

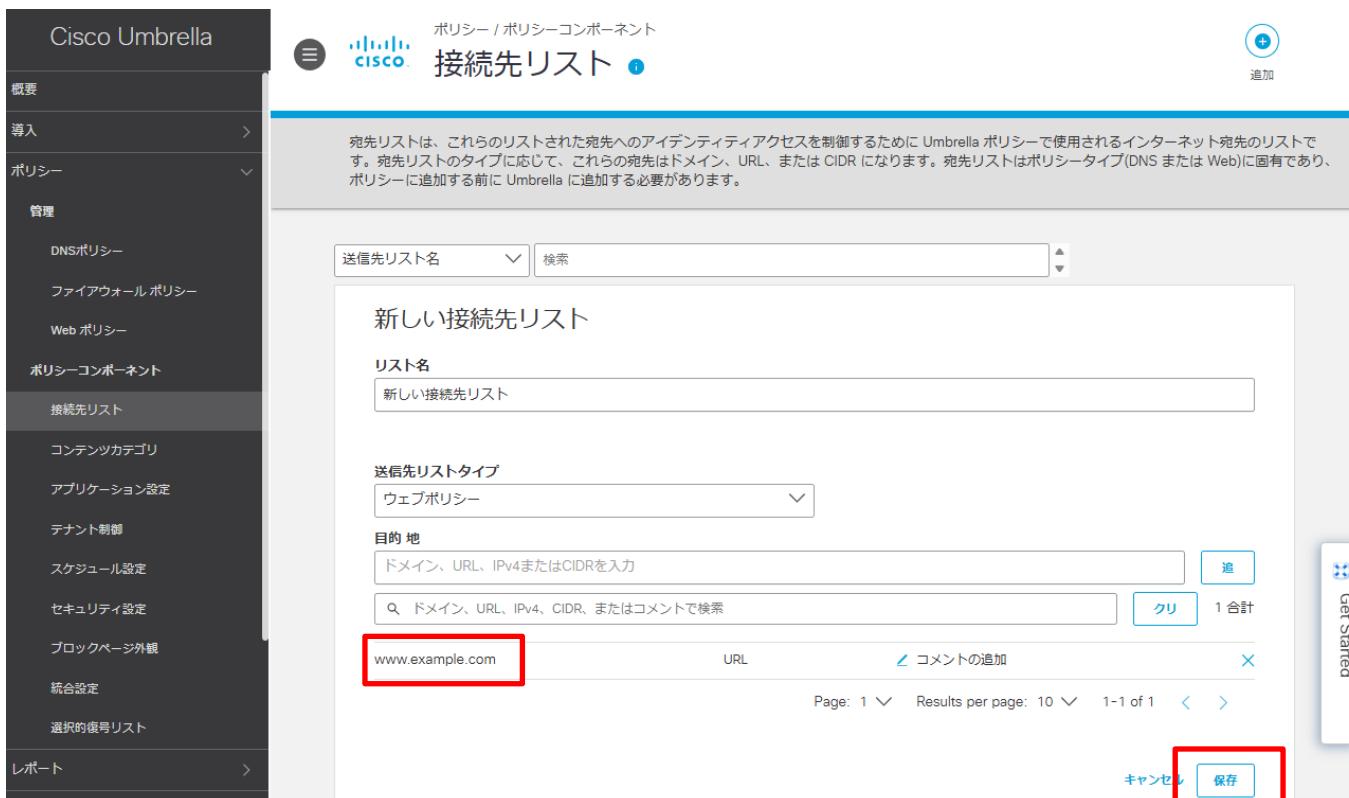
The screenshot shows the Cisco Umbrella web interface with the following details:

- Left Sidebar:** Shows navigation options like Overview, Import, Policies (selected), DNS Policy, Firewall Policy, Web Policy (selected), Policy Component, Connection Destination List, Content Category, Application Settings, Tenant Control, Scheduling, Security Settings, Block Pages, Overall Settings, and Advanced Lists.
- Top Bar:** Displays the Cisco logo and the title "Cisco Umbrella" followed by "Policy / Policy Component" and "Connection Destination List".
- Main Content Area:**
 - Section Header:** "新しい接続先リスト" (New Connection Destination List).
 - Form Fields:**
 - "リスト名" (List Name): "テストWEBポリシー" (Test Web Policy).
 - "送信先リストタイプ" (Recipient List Type): "ウェブポリシー" (Web Policy).
 - "目的地" (Destination): A text input field containing "www.example.com".
 - Buttons:** A red box highlights the "追加" (Add) button located to the right of the destination input field.
 - Message:** Below the input fields, there is a message: "このリストに接続先が追加されていません" (There are no connection destinations added to this list).
 - Pagination:** At the bottom, it says "Page: 1 Results per page: 10 1-0 of 0" with navigation arrows.
 - Bottom Buttons:** "キャンセル" (Cancel) and "保存" (Save).

許可／ブロックリスト設定方法（つづき）

- ⑦追加した宛先が、表示されていることを確認し、「保存」をクリックします。
宛先が複数ある場合は、⑥の作業を繰り返します。

注) 1つの接続先リストに追加可能な宛先は5,000件となっていますが、パフォーマンスの観点から100件以下に抑えることを推奨します。



許可/ブロックリスト設定方法（つづき）

⑧作成した接続先リストが表示されていることを確認します。

| 接続先リスト名 | 適用先 | タイプ | ドメイン | IP | URL | 最終更新日 |
|------------|---------|-----|------|----|-----|--------------|
| テストWEBポリシー | Webポリシー | - | 2 | 0 | 0 | Oct 05, 2022 |

注) Webポリシーの接続先リストヘドメインを登録する際、以下エラーが出る場合はUmbrellaにて必要な宛先となるため、リストへ登録できません。

| リスト名 | 適用先 | タイプ | ドメイン | IP | URL | 最終更新日 |
|---------------|---------|-----|------|----|-----|--------------|
| テストWebブラックリスト | Webポリシー | - | 2 | 0 | 0 | Sep 01, 2022 |

許可／ブロックリスト設定方法（つづき）

⑨作成したDNSポリシーを適用します。

左側のメニューより「ポリシー」－「DNSポリシー」－「Default Policy」をクリックします。

The screenshot shows the Cisco Umbrella web interface. On the left, a dark sidebar menu lists various policy types: Overview, Import, Policies (highlighted with a red box), Management, Firewall Policy, Web Policy, Policy Component, Connection List, Content Category, Application Settings, Tenant Control, Schedule, Security, Blockpage Appearance, Integration, and Advanced Filtering. The main content area is titled "Policy / Management" and "DNS Policy". It contains a descriptive text about how policies affect security, categories, and connection lists. Below this is a table with one row, "Default Policy", highlighted with a red box. The table columns are: 次を含む (Contains Next), 3 Policy Settings, and 最終更新日 (Last Updated) May 12, 2025. A "Get Started" button is visible in the bottom right corner.

許可/ブロックリスト設定方法（つづき）

⑩接続先リスト適用の「編集」をクリックします。

The screenshot shows the Cisco Umbrella web interface. On the left, a dark sidebar menu lists various policy types: Overview, Import, Policies (selected), Management (DNS Policy, Firewall Policy, Web Policy), Policy Components (Connection List, Content Category, Application Settings, Tenant Control, Scheduling, Security Settings, Block Page Overrides, Integration Settings, Selectional Backups), Reports, Investigate, and Management. The main content area is titled 'Policy / Management' and 'DNS Policy'. It displays a note about how policies determine security protection, category settings, and connection lists. Below this is a table titled 'Default Policy' with columns for 'Policy Name' (Default Policy), 'Next Action' (Contains), 'Setting' (3 Policies Set), and 'Last Updated' (May 12, 2025). The table lists several policy rules:

- すべてのアイデンティティに適用 (All identities apply)
- 適用されたセキュリティ設定: NTT West Settings (Applied security settings: NTT West Settings)
コマンド&コントロールのコールバック、マルウェア、フィッシング攻撃、5以上がブロックされます。
いいえ 統合 等しい enabled に設定します。
編集 無効にする
- 適用されたコンテンツ設定 NTT West Settings (Applied content settings: NTT West Settings)
アルコール、出会い系、ギャンブル、13以上がブロックされます。
編集 無効にする
- 適用されたアプリケーション設定がありません (No application settings applied)
- ファイル分析 無効 (File analysis disabled)
インテリジェントプロキシが必要です
ファイル検査 無効
- 適用されたカスタムブロックページ (Applied custom block page: NTT West Settings)
編集

At the bottom, there's a 'Detailed Settings' section for 'NTT West Settings' with a 'USE CUSTOM SETTINGS' button and a note about intelligent proxy functionality.

許可／ブロックリスト設定方法（つづき）

- ⑪作成した「テストDNSポリシー」を「チェック」—ブロック適用対象リストに「テストDNSポリシー」が反映—「設定して戻る」をクリック

The screenshot shows the Cisco Umbrella interface for managing DNS Policies. On the left, a sidebar lists various policy types: Summary, Import, Policy (selected), Firewall Policy, Web Policy, Policy Component, Connection List, Content Category, Application Settings, Tenant Control, Scheduling, Security Settings, Block Page Appearance, Integration Settings, and Selectional Backups. The main panel displays the 'Default Policy' settings. At the top right, it says '適用する順番でソートされています' (Sorted by priority). Below that, the 'Default Policy' details are shown: '次を含む' (Contains next), '3 ポリシー設定' (3 Policy Settings), and '最終更新日' (Last updated) on 'May 12, 2025'. Under '接続先リストの適用' (Apply connection list), there is a button '新しいリストの追加' (Add new list). A search bar '宛先リスト名で検索' (Search by recipient list name) is present. A checkbox 'すべてを選択' (Select all) is checked. A dropdown menu 'すべてのリスト' (All lists) is open, showing '3合計' (3 total). In the 'すべての接続先リスト' (All connection lists) section, a checkbox for 'テストDNSポリシー' (Test DNS Policy) is checked and highlighted with a red box. In the '2 ブロック 適用対象リスト' (2 Block Apply target list) section, a checkbox for 'テストDNSポリシー' (Test DNS Policy) is also checked and highlighted with a red box. In the '1 許可 適用対象リスト' (1 Allow Apply target list) section, a checkbox for 'Global Allow List' is checked. At the bottom right, there are 'キャンセル' (Cancel) and '設定して戻る' (Save and return) buttons, with the latter also highlighted with a red box.

許可/ブロックリスト設定方法（つづき）

⑫接続先リスト適用に追加したポリシーが反映されていることを確認し「保存」をクリック

The screenshot shows the Cisco Umbrella web interface under the 'DNS Policy' section. On the left sidebar, 'Connections' is selected under the 'Management' category. In the main content area, the 'Connections' tab is active, displaying a table with one row:

| Default Policy | 次を含む 3 ポリシー設定 | 最終更新日 May 12, 2025 |
|---|---|-----------------------|
| ポリシー名 Default Policy | | |
| すべてのアイデンティティに適用 | | |
| 適用されたセキュリティ設定: NTT West Settings <small>コマンド&コントロールのコードバック、マルウェア、フィッシング攻撃、5以上 がブロックされます</small> | 3 接続先リスト 適用 <small>1 許可リスト 編集</small> | |
| 適用されたコンテンツ設定 NTT West Settings <small>アルコール、出会い系、ギャンブル、13 以上 がブロックされます</small> | | |
| 適用されたアプリケーション設定がありません <small>有効</small> | | |
| 詳細設定 | | |
| <small>NTT West Settings USE CUSTOM SETTINGS</small> | | |
| インテリジェントプロキシの有効化 <small>プロキシWeb接続により、危険なメインに関して、脅威、コンテンツ、またはアプリケーションが可視化されます。</small> | | |

A red box highlights the '3 接続先リスト 適用' (Apply connection list) status in the 'Connections' section. At the bottom right of the page, there are 'Cancel' and 'Save' buttons, with 'Save' being highlighted by a red box.

許可／ブロックリスト設定方法（つづき）

⑬作成したWebポリシーを適用します。

左側のメニューより「ポリシー」→「Webポリシー」→「Default Web Policy」をクリックします。

The screenshot shows the Cisco Umbrella web interface. On the left, a sidebar menu lists various policy components: Overview, Import, Policy (highlighted with a red box), Management, DNS Policy, Firewall Policy, and Web Policy (also highlighted with a red box). The main content area is titled 'Policy / Management' and 'Web Policy'. It contains a detailed description of what a Web Policy is, mentioning rule sets and rule conditions. Below this, a table displays a single entry: 'Default Web Policy'. The table columns include a thumbnail icon, the policy name, a 'Next' button, and an 'Updated' date ('May 09, 2025'). A red box highlights this row. At the bottom right of the main area, there is a 'Get Started' button.

許可/ブロックリスト設定方法（つづき）

⑯接続先リスト適用の「ルールの追加」をクリックします。

The screenshot shows the Cisco Umbrella management interface for a 'Web Policy'. The left sidebar lists various policy types: DNS Policy, Firewall Policy, Web Policy (selected), Policy Components, Connection List, Content Categories, Application Settings, Tenant Control, Schedule, Security Settings, Block Page Appearance, and Integration. The main content area displays the 'Default Web Policy' with one rule named 'Default Rule' which blocks traffic. A red box highlights the 'Add Rule' button. Below the table, there's a section titled 'Rule Set Configuration' with settings for the rule set name, identity type, and tenant controls.

| 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 | Default Rule | ● ブロック | ルールセットアイデンティティ | 適用されたカテゴリリスト ... 任意の日、いつでも 保護されたファイルのバイパスが有効 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 | Default Web Policy | 編集 |
| ルールセットアイデンティティ | すべてのアイデンティティ | 編集 |
| ブロックページと警告ページ | NTT West Settings | 編集 |
| テナントコントロール | Global Tenant Controls | 編集 |

許可/ブロックリスト設定方法（つづき）

⑯例えはルール名「ホワイトリスト」、ルールアクション「許可」のルールを追加する場合

The screenshot shows the Cisco Umbrella management interface under the 'Web Policy' section. The left sidebar lists various policy categories like DNS, Firewall, and Web. The main area displays the 'Default Web Policy' with one existing rule named '新しいルール 1' (New Rule 1) which blocks traffic from specific identities. A new rule is being added with the name 'ホワイトリスト' (White List) and the action '許可' (Allow), which adds identities to the whitelist. The interface includes tabs for 'ルールの追加' (Add Rule) and 'ルールセット名' (Rule Set Name). Buttons for '変更スケジュール' (Change Schedule) and '保存' (Save) are also visible.

許可／ブロックリスト設定方法（つづき）

⑯アイデンティティの「ルールセットアイデンティティの継承」を選択し、「適用」をクリック

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

Investigate

管理

ポリシー / 管理

Web ポリシー 1

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削除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。ルールは順序で評価され、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](#)。

Default Web Policy

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 |
|--------------|------|----------------|---------------------------------|--------|
| ホワイトリスト | 許可 | セキュリティの上書き | ルールセットアイデンティティ アイデンティティを追加する | 1 選択済み |
| Default Rule | ブロック | ルールセットアイデンティティ | | 1 選択済み |

▲ 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。りります。

ルールセット名

Default Web Policy

ルールセットアイデンティティの継承

適用

セキュアインターネットゲートウェイ

許可／ブロックリスト設定方法（つづき）

⑯送信先の「Destination Lists」を選択し、「>」をクリック

The screenshot shows the Cisco Umbrella web policy configuration interface. The left sidebar includes sections for Overview, Import, Policies (selected), Management, DNS Policies, Firewall Policies, Web Policies (selected), Policy Components, Connection Lists, Content Categories, Application Settings, and Destination Lists. The main panel displays the 'Default Web Policy' with one rule: 'Default Rule' (Action: Block). The 'Rule Set Definition' section shows a table with columns: Priority, Rule Name, Rule Action, Identity Type, Destination, and Rule Configuration. The 'Identity Type' dropdown is set to 'Allow'. The 'Destination' dropdown is set to 'Select none' and has an option 'Add destination' highlighted with a red box. Below the table, there are sections for Application Settings (6034 items) and Content Categories (104 items). A note at the bottom states: '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ポリシーに適用されます。' (Rule set settings affect rules within the rule set and apply to the Web policy). A 'Get Started' button is visible on the right.

許可／ブロックリスト設定方法（つづき）

⑯送信先／宛先リストで作成した「テストWEBポリシー」を選択し、「適用」をクリック

The screenshot shows the Cisco Umbrella management interface. On the left, the navigation menu is visible with 'Web ポリシー' selected. The main content area shows the 'Default Web Policy' with one rule. A modal window is overlaid on the rule, specifically on the 'ルールセット設定' (Rule Set Configuration) section. In this modal, the 'ルールセット' dropdown is set to 'ホワイトリスト' and the 'アクション' (Action) is '許可' (Allow). The 'ルールセットアイデンティティ' (Rule Set Identity) dropdown shows '1個の接続先リスト ...' (One connection list ...) and '宛先を追加' (Add recipient). Below this, there's a search bar for '送信先' (Recipient) and a link to '送信先 / 宛先リスト' (Recipient / Recipient List). At the bottom of the modal, the '選択済み' (Selected) section shows '1 テストWEBポリシー' (1 Test WEB Policy) with a checked checkbox. The '適用' (Apply) button is highlighted with a red box. The overall interface is in Japanese.

許可／ブロックリスト設定方法（つづき）

⑯「保存」をクリック、「^」をクリック

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 >

Investigate >

管理 >

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](#)。

Default Web Policy

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 |
|--------------|------|----------------|------------------|--------------------------------|---------------------|
| ホワイトリスト | 許可 | ルールセットアイデンティティ | 1個の接続先リスト ... | 任意の日、いつでも 変更スケジュール | セキュリティの上書き |
| Default Rule | ブロック | ルールセットアイデンティティ | 適用されたカテゴリリスト ... | 任意の日、いつでも 保護されたファイルのバイパスが有効 | 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

Default Web Policy

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

Default Web Policy

編集

許可／ブロックリスト設定方法（つづき）

②改めて「Default Web Policy」をクリックします。

The screenshot shows the Cisco Umbrella web policy management interface. On the left, a sidebar menu lists various policy types: DNS Policy, Firewall Policy, and Web Policy (which is currently selected and highlighted in blue). The main content area is titled 'Web ポリシー' (Web Policy) and contains a detailed description of what a Web Policy is. Below this, a table displays a single entry: 'Default Web Policy'. This entry has a red border around it, indicating it is the selected item. The table includes columns for the policy name ('Default Web Policy'), a 'Next' button ('次を含む'), and the last update date ('最終更新日' - May 09, 2025). A 'Get Started' button is located in the bottom right corner of the main content area.

許可／ブロックリスト設定方法（つづき）

② 作成したホワイトリストの「…」をクリック、「ルールの有効化」をオン

Cisco Umbrella

ポリシー / 管理

Web ポリシー

Default Web Policy

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 | ホワイトリスト | 許可 | ルールセットアイデンティティ | 1個の接続先リスト ... | 任意の日、いつでも 保護されたファイルのバイパスが有効 |
| 2 | ブロックルール | ブロック | ルールセットアイデンティティ | 適用されたカテゴリリスト ... | 任意の日、いつでも 保護されたファイルのバイパスが有効 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

ルールセット名: Default Web Policy

ルールセットアイデンティティ: サマリのアイデンティティ

ブロックページと警告ページ: NTT West Settings

テナントコントロール: 無効

ファイル分析: 2個の設定が有効化されました

ファイルの種類のコントロール: 無効

HTTPS 検査: 有効

ルールセットのロギング: すべての要求をロギング

セーフサーチ: 無効

Get Started

ルールの編集

ルールの有効化 (Switch On)

ルールの削除

ルールの無効化 (Switch Off)

許可/ブロックリスト設定方法（つづき）

②ルールステータスの「更新」をクリック

The screenshot shows the Cisco Umbrella web policy configuration interface. On the left, the navigation menu includes 'Web ポリシー' (selected), 'Default Web Policy', and various settings like 'ルールセット名' (Default Web Policy), 'ブロックページと警告ページ' (NTT West Settings), and 'HTTPS 検査'. In the center, a modal dialog titled 'ルールステータスの更新' (Update Rule Status) asks 'このルールのステータスを更新してもよろしいですか?' (Do you want to update the rule status?). The '更新' (Update) button is highlighted with a red box. Below the dialog, the 'Default Web Policy' table lists two rules: 'ホワイトリスト' (Allow) and 'ブロックルール' (Block). On the right, there are tabs for 'ルールの編集' (Edit Rule) and 'ルールの削除' (Delete Rule), with the 'ルールの有効化' (Enable Rule) switch turned off.

Cisco Umbrella ではHTTPS通信の復号を行う際、通信を中継して内容をチェックするために独自のSSL/TLS証明書を使用します。

しかし、一部のサイトでは証明書の厳格な検証を行い、独自の証明書による復号を拒否することがあります。

例えば、銀行や政府機関のサイトは特に厳格な証明書管理をしているため、HTTPS復号を試みるとアクセスできなくなることや、一部のウェブサイトは、中間者攻撃（Man-in-the-Middle攻撃）を防ぐため、HTTPS復号を行う環境からのアクセスをブロックすることがあります。

アクセスを行うためには管理コンソールで、対象サイトへのHTTPS通信の復号除外設定を行う必要があります。

サイトに問題がないと判断できる場合のみ、下記手順でHTTPS通信の復号除外設定をお願いします。

HTTPS通信の復号除外設定方法

- 左側のメニューより「ポリシー」 – 「選択的複合リスト」 – 「Default Web Selective Decryption List」をクリックします。

The screenshot shows the Cisco Umbrella management interface. On the left, a dark sidebar menu lists various policy components like DNS, Firewall, and Web policies, along with security and reporting features. A red box highlights the '選択的復号リスト' (Selective Decryption List) option under the 'ポリシー' (Policy) section. The main content area has a light gray header 'ポリシー / ポリシーコンポーネント' and '選択的復号リスト'. Below it is a detailed description of the list's purpose. A table titled 'Default Web Selective Decryption List' is displayed, showing one entry: 'Webポリシー' (Web Policy) with 3 categories, 0 applications, and 0 domains, last updated on 'Apr 09, 2025'. A red box surrounds this table. In the bottom right corner of the main window, there is a small vertical panel with the text 'Get Started'.

| Default Web Selective Decryption List | 適用先 | カテゴリ | アプリケーション | ドメイン | 最終更新日 |
|---------------------------------------|-----|------|----------|--------------|-------|
| Webポリシー | 3 | 0 | 0 | Apr 09, 2025 | |

HTTPS通信の復号除外設定方法（つづき）

②画面右の「追加」をクリックします。

The screenshot shows the Cisco Umbrella web interface with the following details:

- Sidebar Navigation:** Includes links like '概要', '導入', 'ポリシー', '管理' (DNS Policy, Firewall Policy, Web Policy), 'ポリシーコンポーネント' (Connections, Content Categories, Applications, Tenants, Schedules, Security, Blocklist, Integration), and '選択的復号リスト' (selected).
- Header:** 'Cisco Umbrella' logo, 'ポリシー / ポリシーコンポーネント' (Policy / Policy Component), and '選択的復号リスト' (Selective Decryption List) with a count of 1.
- Main Content:** A table titled 'Default Web Selective Decryption List' showing statistics: 適用先 'Webポリシー' (Web Policy), カテゴリ '3', アプリケーション '0', ドメイン '0', and date 'Apr 09, 2025'. Below the table are three lists:
 - リスト名:** Default Web Selective Decryption List
 - 3 選択されたカテゴリ:** Health and Medicine, Finance, Government and Law. The '追加' (Add) button is highlighted with a red box.
 - 0 選択したアプリケーション:** (empty)
 - 0 ドメイン:** (empty)
- Buttons:** 'キャンセル' (Cancel) and '保存' (Save) at the bottom right.
- Right Sidebar:** 'Get Started' button.

HTTPS通信の復号除外設定方法（つづき）

③復号除外する「ドメイン」を記載し「追加」をクリックします。

The screenshot shows the Cisco Umbrella web interface with the following details:

- Sidebar Navigation:** Includes links for Overview, Import, Policies, Management, DNS Policy, Firewall Policy, Web Policy, Policy Components, Connection Lists, Content Categories, Application Settings, Tenant Control, Schedules, Security Settings, Blockpage Appearance, Integration, Selective Decryption Lists, Reports, Investigate, and Manage.
- Current View:** The "Selective Decryption Lists" page under the "Management" section.
- Table Header:** Default Web Selective Decryption List, with columns: 適用先 (Policy), カテゴリ (Category), アプリケーション (Application), ドメイン (Domain), and Last Updated (Apr 09, 2025).
- Form Fields:**
 - リスト名 (List Name):** Default Web Selective Decryption List.
 - 選択されたカテゴリ (Selected Categories):** Health and Medicine, Finance, Government and Law. The "Finance" category is highlighted with a red box.
 - 選択したアプリケーション (Selected Applications):** An empty list.
 - ドメイン (Domains):** example.com. The "example.com" entry is highlighted with a red box.
- Buttons:** キャンセル (Cancel) and 保存 (Save).
- Right Sidebar:** Get Started button.

HTTPS通信の復号除外設定方法（つづき）

④復号除外する「ドメイン」が追加されていることを確認し「保存」をクリックします。

The screenshot shows the Cisco Umbrella web interface with the following details:

- Sidebar Navigation:** Includes links for Overview, Import, Policies, Management (DNS Policy, Firewall Policy, Web Policy), Policy Components (Policy Lists, Peering Lists, Content Categories, Applications, Tenants, Schedules, Security, Block Pages, Global Settings), and Selective Decryption Lists.
- Current View:** The "Selective Decryption List" page under the "Management" section.
- Page Title:** ポリシー / ポリシー・コンポーネント 選択的復号リスト
- Table Headers:** Default Web Selective Decryption List, 運用先 (Web Policy), カテゴリ (Category), アプリケーション (Application), ドメイン (Domain), and Date (Apr 09, 2025).
- Form Fields:** リスト名 (List Name) set to "Default Web Selective Decryption List".
- Category Selection:** 3 選択されたカテゴリ (3 selected categories): Health and Medicine, Finance, Government and Law.
- Application Selection:** 0 選択したアプリケーション (0 selected applications): "いいえ 選択したアプリケーション" (No selected applications).
- Domain Selection:** 1 ドメイン (1 domain): example.com.
- Buttons:** キャンセル and 保存 (Save) button, with the 保存 button highlighted by a red box.
- Right Sidebar:** Get Started link.

HTTPS通信の復号除外設定方法（つづき）

⑤復号除外する「ドメイン」が追加されていることを確認します。

The screenshot shows the Cisco Umbrella web interface. The left sidebar has a dark theme with white text. The main area is titled 'ポリシー / ポリーコンポーネント' (Policy / Policy Component) and '選択的復号リスト' (Selective Decryption List). A sub-section title 'Default Web Selective Decryption List' is visible. The table below shows the following data:

| 適用先 | カテゴリ | アプリケーション | ドメイン | 最終更新日 |
|---------|------|----------|------|--------------|
| Webポリシー | 3 | 0 | 1 | Apr 26, 2025 |

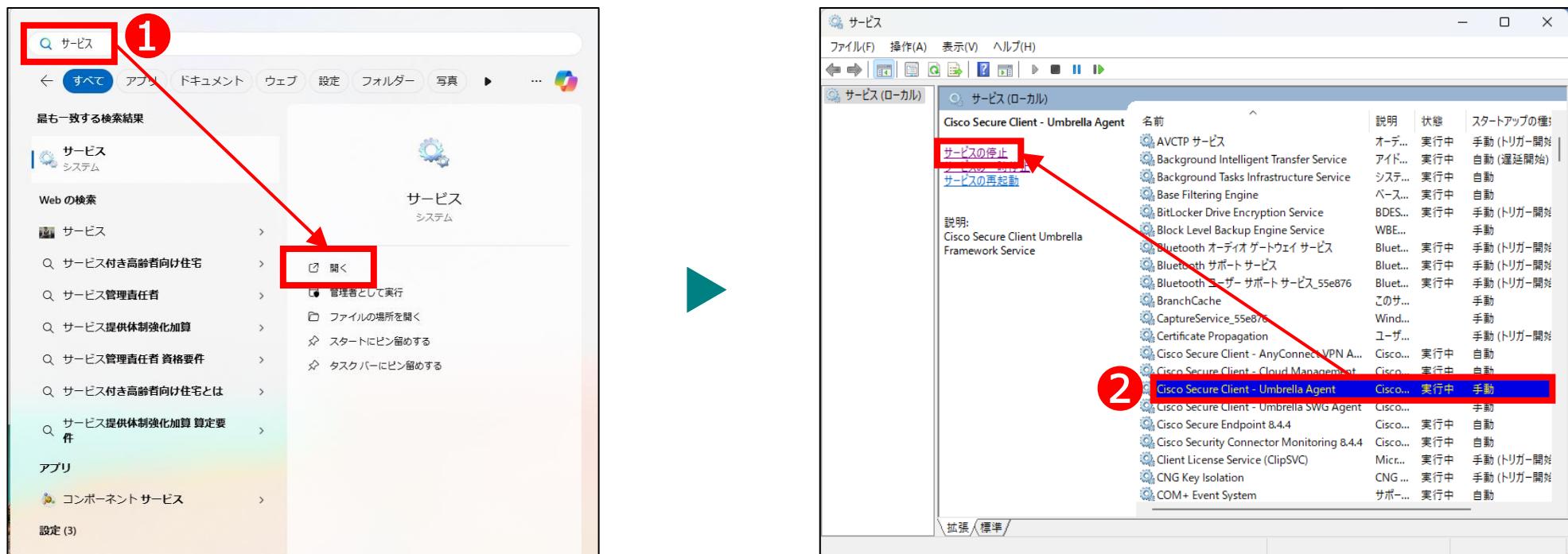
A red box highlights the 'ドメイン' column value '1'. The right side of the interface features a 'Get Started' button.

まずCisco Umbrella が要因でインターネットができるないのかをご確認いただくため、Cisco Umbrellaを無効化し、インターネット接続ができるかをお試しください。
※Cisco Umbrellaを無効にしてもインターネットに接続できない場合はCisco Umbrella 要因ではございません。
Cisco Umbrella 要因であった場合は、お電話にてサポートセンターお問合せください。

本サービスのセキュリティソフトを無効にする方法

◆ WindowsOSの場合

- ① Windowsキーを押下し、[サービス]を検索して[開く]を押下します。
- ② [Cisco Secure Client - Umbrella Agent]を選択し、[サービスの停止]を押下します。
※サービス停止後、再起動をするとCisco Umbrellaが有効な状態に戻ります。



Cisco Umbrella を無効にし、速度遅延がおさまるかご確認ください。

※Cisco Umbrellaを無効にしても速度遅延がおさまらない場合はCisco Umbrella要因ではありませんので、お客様にてその他のご利用環境をお調べいただくか、回線状態をお調べください。

Cisco Umbrella を無効にする方法

p92を参照ください。

「セキュリティ証明書に問題があります」と表示される場合、いくつかの要因が考えられます。下記手順をご確認、お試しください。
下記手順にて解決できない場合は、お電話にてサポートセンターにお問合せください。

要因① 利用端末の日付が電子証明書の有効期限と合っていない

コンピュータ（パソコン）で設定されている日付にずれがないかご確認ください。

要因② 電子証明書の有効期限切れ

電子証明書の有効期限が切れている場合は、再度新たに電子証明書のインストールを行う必要があります。

電子証明書の設定方法（次項を参照ください）

電子証明書の設定方法（つづき）

Cisco Umbrellaのログイン画面より、ダッシュボードにログインします。



①「導入」をクリックします。

A screenshot of the Cisco Umbrella dashboard. On the left is a sidebar menu with the following items: "概要" (Overview), "導入" (Import) [highlighted with a blue circle and the number 1], "ポリシー" (Policy), "レポート" (Report), "Investigate", "管理" (Management), and a user icon. The main content area is titled "概要" (Overview). It shows "0 Messages" and "導入の健全性" (Import Health) with four status boxes: "アクティブなネットワーク" (Active Network) 0/0, "アクティブなローミングクライアント" (Active Roaming Client) 1/1, "アクティブな仮想アプライアンス" (Active Virtual Appliance) 0/0, and "アクティブなネットワーク" (Active Network) 0/0. Below this is a section titled "ネットワークの分析" (Network Analysis) with a chart showing "総リクエスト件数" (Total Requests) over time. The chart shows a sharp peak around 1 PM. To the right of the chart are two search results sections: "検索結果がありません" (No results found) and another "検索結果がありません" (No results found).

電子証明書の設定方法（つづき）

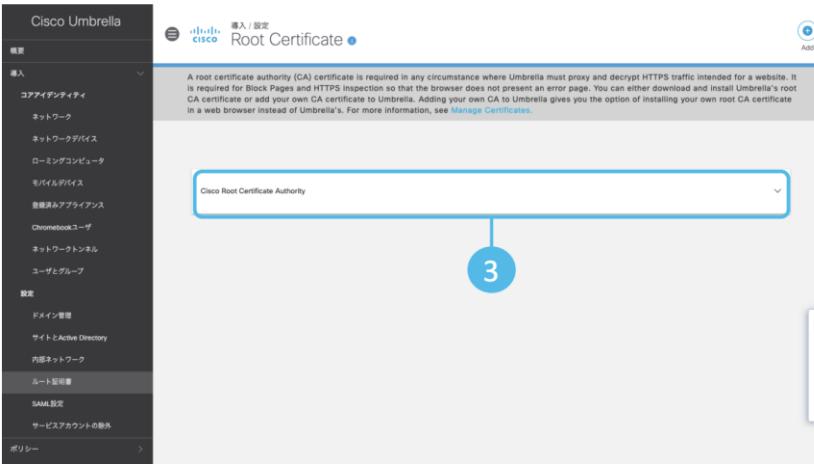
②「ルート証明書」をクリックします。



The screenshot shows the Cisco Umbrella dashboard. On the left, a sidebar menu lists various categories: Core Identity, Import, Network, Network Devices, Roaming Computer, Mobile Device, Logging Analytics, Chromebook User, Network Tunnel, User Groups, and Settings. Under Settings, the 'Route Certificate' option is highlighted with a blue circle containing the number '2'. The main dashboard area is titled '概要' (Overview) and displays '0 Messages'. It includes sections for 'Import Integrity' (Active Network 0/0, Active Roaming Line 1/1, Active Virtual Appliance 0/0, Active Tunnel 0/0), 'Network Analysis' (Total Requests 1641, Total Block 0%, Security Block 0%), and search results for 'File Watcher' (No results). A 'Get Started' button is located on the right.

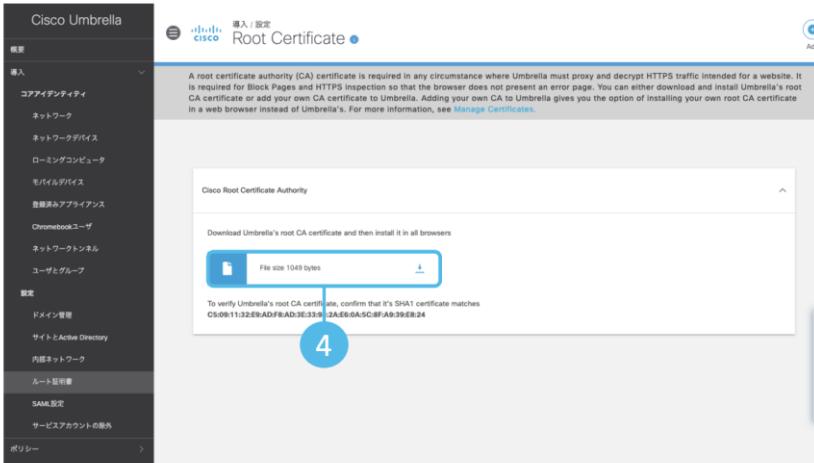
電子証明書の設定方法（つづき）

- ③「Cisco Root Certificate Authority」をクリックします



- 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します。

「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、「保存」をクリックし 続行してください。

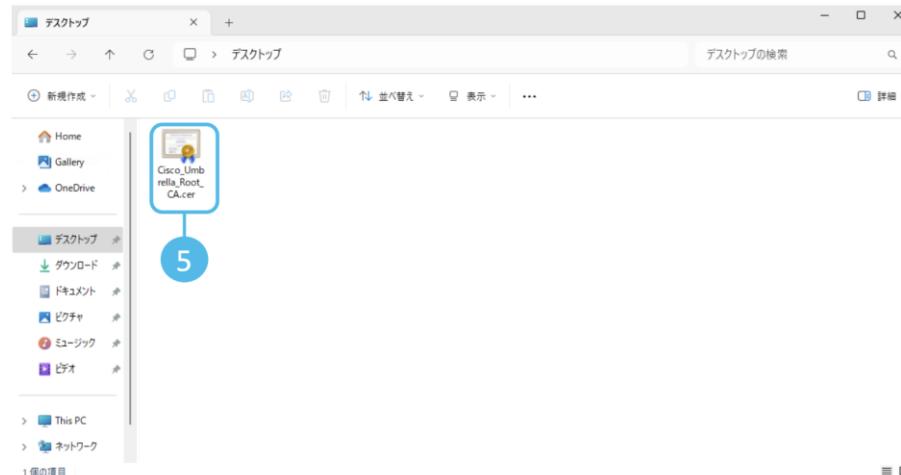


電子証明書の設定方法（つづき）

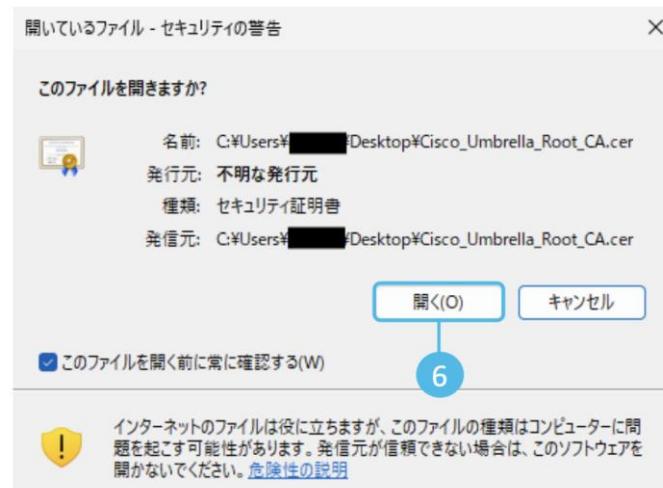
⑤④で保存した場所（フォルダ）を開き、ルート証明書をクリックします。

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。



⑥「開く」をクリックします。



電子証明書の設定方法（つづき）

⑦[証明書のインストール]をクリックします。



⑧[証明書のインポート ウィザード]が表示されます。「次へ」をクリックします。

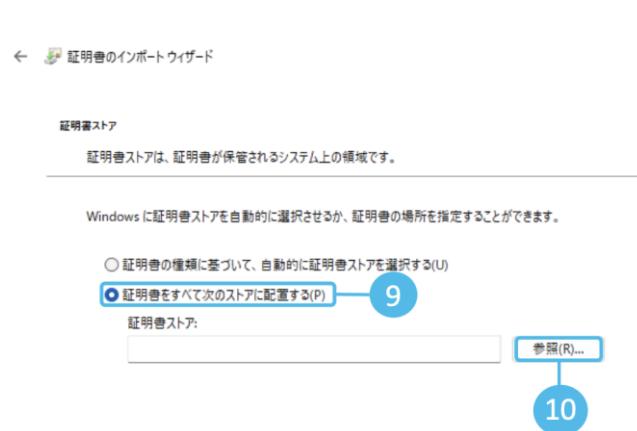
デフォルトでは[現在のユーザー]が選択されています。必要に応じて [ローカルコンピューター] を選択してください。



電子証明書の設定方法（つづき）

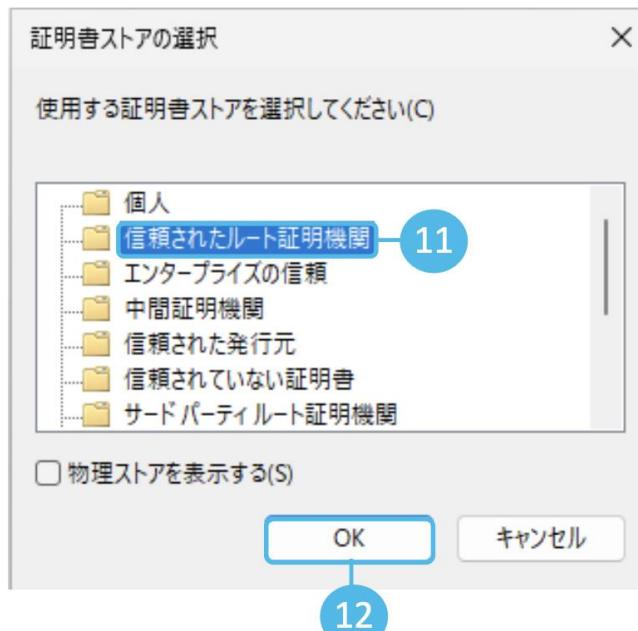
⑨「証明書をすべて次のストアに配置する」をクリックします。

⑩「参照」をクリックします。



⑪「信頼されたルート証明機関」をクリックします。

⑫ 「OK」をクリックします。

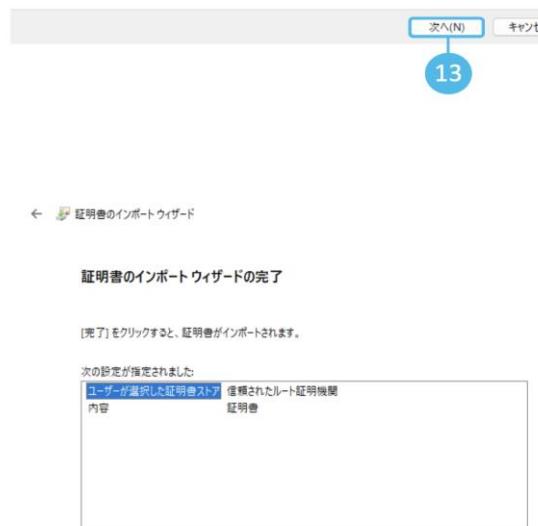


電子証明書の設定方法（つづき）

- ⑬ 「証明書をすべて次のストアに配置する」にチェックが入っていることを確認し、「次へ」をクリックします。



- ⑭ 「完了」をクリックします。

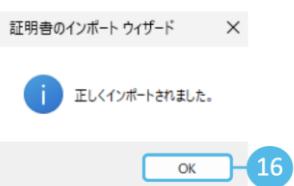


電子証明書の設定方法（つづき）

- ⑯ [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。「はい(Y)」をクリックします。



- ⑰ [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。



- ⑱ 「OK」をクリックします。



まずCisco Umbrella 要因で共有フォルダにアクセスができないのかをご確認いただくため、Cisco Umbrella を無効にし、共有フォルダにアクセスができるかをお試しください。

※Cisco Umbrella を無効にしても共有フォルダにアクセスができない場合はCisco Umbrella 要因ではございません。
Cisco Umbrella 要因であった場合は、サポートセンターにお電話にてお問合せください。

Cisco Umbrella を無効にする方法

p92を参照ください。

まずCisco Umbrella 要因でツールが動かないかをご確認いただくため、以下の手順をお試しください。
下記手順にて解決できない場合には、サポートセンターに電話にてお問い合わせください。

①Cisco Umbrella を無効にする方法

p92を参照ください。

②Cisco Umbrellaの許可／ブロックリスト設定方法

ベンダーのリモートツール接続時のURLを許可登録し、ツールが動くか確認します。

p64-86を参照ください。

③Cisco UmbrellaのHTTP通信の復号除外設定方法

ベンダーのリモートツール接続時のドメインをHTTPS通信の復号除外設定し、ツールが動くか確認します。

p87-91を参照ください。

まずCisco Umbrella 要因でメールの送受信ができないかをご確認いただくため、以下の手順をお試しください。
下記手順にて解決できない場合には、サポートセンターに電話にてお問い合わせください。

①Cisco Umbrella を無効にする

Umbrellaを無効にして、メールの送受信ができるか確認します。
無効にする手順は、p92を参照ください。

②証明書の問題

証明書に問題がないか確認します。
証明書の設定手順は、p94-102を参照ください。

Webブラウザに表示される場合のある500番台のエラーメッセージ（代表的なもの）をご紹介します。

Intelligent Proxyを有効にした場合、通常「白」と判定されるドメインの中で、「危険性が疑われるが、その確証がないドメイン」または「正常な通信の中に危険性が高い通信が紛れ込む可能性のあるドメイン」を「グレー」と判定し、Umbrella クラウド上の Intelligent Proxy サーバーの IP アドレスを返します。

515 Upstream Certificate Untrusted

このエラー メッセージは、Intelligent Proxy サーバーが実際の Web サーバーに対して HTTPS リクエストを送った際、Web サーバーから返ってきたサーバー証明書の内容が信頼できない (Untrusted) 場合に表示されます。

サーバー証明書が信頼できない理由は多岐にわたり、証明書の有効期限が切れている、自己署名証明書（いわゆるオレオレ証明書）を使っている、サーバー証明書に上位の証明書が含まれていないなどが考えられます。

このエラー メッセージが表示された場合、まずは Web サーバーの管理者にサーバー証明書の状況について確認してください。



515 Upstream Certificate Untrusted

This site uses an untrusted SSL security certificate. The certificate is not trusted because the issuer certificate is unknown or invalid and this website could pose a threat. There is no way to verify if the site is legitimate and attackers might be using this site to steal your information (for example, passwords, messages, or credit cards). If you continue seeing this error, please contact your Administrator.

This page is served by Umbrella Cloud Security Gateway. Server: mps-237dbd9c99ea.sigenv1.nrt

Thu, 13 Jun 2019 00:51:27 GMT

517 Upstream Certificate Revoked

このエラー メッセージは、Intelligent Proxy サーバーが実際の Web サーバーに対して HTTPS リクエストを送った際、Web サーバーから返ってきたサーバー証明書のステータスが失効している (Revoked) 場合に表示されます。

このエラー メッセージが表示された場合、まずは Web サーバーの管理者にサーバー証明書の状況について確認してください。



0403修正

✖ 517 Upstream Certificate Revoked

The SSL security certificate presented by this site has been revoked by the certificate authority. This means attackers might be trying to steal your information (for example, passwords, messages, or credit cards). If you continue seeing this error, please contact your Administrator.

This page is served by Umbrella Cloud Security Gateway. Server: mps-1556a1994fc3.sigenv1.sin

Fri, 15 Jan 2021 12:27:39 GMT

502 Bad Gateway

前項のエラー コード 515 は Intelligent Proxy 特有のものですが、一般的な HTTP レスポンスのステータス コード 500 番台 (サーバー エラー) が表示される場合があります。

502 Bad Gateway の場合、Intelligent Proxy サーバーが実際の Web サーバーにアクセスしようとしたが、ネットワークの途中にあるゲートウェイに問題がある、IP アドレスが不正な内容であるなどの理由により、通信できなかったことを示します。



✖ 502 Bad Gateway

An upstream server error has occurred. If you believe you are seeing this message in error, please contact your network administrator.

This page is served by Umbrella Cloud Security Gateway.

Server: swg-nginx-proxy-https-a6f0606f2756.signginx.sin

Fri, 07 Apr 2023 00:45:22 GMT

「7-1.特定のサイトが見られない」より高度な設定として、DNSポリシーを変更することができます。

EMOTETなどのランサムウェア対策についてはDNSポリシーを利用しています。

Cisco UmbrellaのDNSポリシーは、企業や組織がインターネットアクセスを制御し、セキュリティを強化するために設定できるルールのことを指します。

これにより、不正なサイトや不要なカテゴリのサイトへのアクセスをブロックしたり、特定のユーザーやグループに異なる制限を適用したりすることが可能になります。

ただし本ポリシーを変更することでセキュリティリスクが高まる場合もあるため、変更に際しては十分ご注意ください。

<Cisco UmbrellaのDNSポリシーの主な機能>

1.コンテンツフィルタリング

- ・アダルト、ギャンブル、SNS、ストリーミングなどのカテゴリ別にWebアクセスを制御
- ・カスタムリストを作成し、特定のドメインを許可またはブロック

2.セキュリティ対策（脅威インテリジェンス）

- ・マルウェア、フィッシング、ランサムウェアに関連するドメインへのアクセスをブロック
- ・Cisco Talosの脅威インテリジェンスを活用し、最新の脅威を自動で防御

3.ポリシーの適用範囲の設定

- ・ユーザー、グループ、ネットワーク、デバイスごとに異なるポリシーを適用可能
- ・AD（Active Directory）やIDプロバイダーと連携し、特定のユーザー向けの制御も可能

4.セーフサーチ＆アプリケーション制御

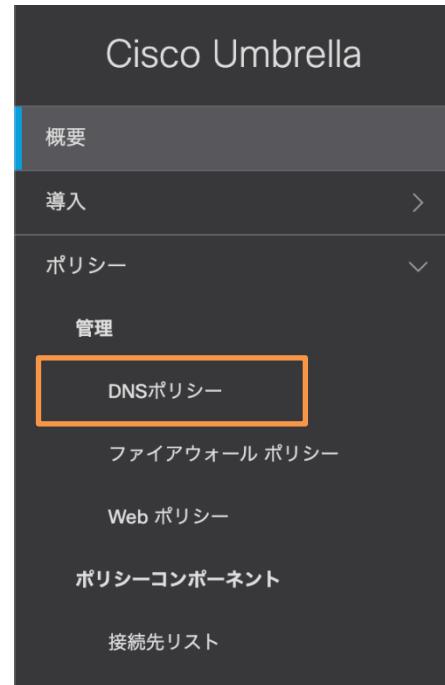
- ・GoogleやBingのセーフサーチを強制適用し、不適切な検索結果をフィルタリング
- ・DropboxやGoogle Driveなどのクラウドアプリの使用を制限

5.カスタムブロックページの設定

- ・ポリシーでブロックされた際に表示するページをカスタマイズ可能
- ・ユーザーに警告を出し、適切なアクセス制御を促す

DNSポリシーの作成・管理方法

- ①Cisco Umbrellaの管理コンソールにログイン
- ②ポリシー > DNSポリシー に移動



- ③新しいポリシーを作成します
(または既存のポリシーを編集します)

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も前に適用されます。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。ヘルプを参照してください。

DNSポリシーの作成・管理方法

④保護対象を選択します

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導入環境と一致している必要があります。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キング、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キング
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キング
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ビューション(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

次へ

DNSポリシーの作成・管理方法

⑤保護するアイデンティティ（ネットワーク、ユーザー、デバイスなど）を選択します

何を保護しますか？

アイデンティティの選択

Q アイデンティティの選択

すべてのアイデンティティ

AD Computers

AD Groups

AD Users

Chromebooks

G Suite OUs

G Suite Users

Mobile Devices

Network Devices

Networks

0選択済み

キャンセル

前へ

次へ

DNSポリシーの作成・管理方法

⑥セキュリティ設定を適用（マルウェア、フィッシングブロックなど）します

The screenshot shows the 'Security Settings' configuration page. At the top, there is a navigation bar with five tabs: 1. Security (highlighted), 2. Content, 3. Applications, 4. Recipients, and 5. 2 More. Below the tabs, the title 'Security Settings' is displayed with a sub-instruction: 'Select or create settings to apply to this policy. Click [Edit Setting] to change existing settings or use the dropdown menu to add new ones.' A 'Default Settings' dropdown menu is open, showing the 'Edit' button. The main area lists various threat categories with their descriptions:

- マルウェア: Malicious software, drive-by download, exploit, and mobile malware host sites.
- 新しく発見されたドメイン: Recently discovered domains used by novice attackers.
- コマンド&コントロールのコールバック: Command & Control communication between compromised devices and attackers.
- フィッシング攻撃: Phishing attacks targeting user information or financial data.
- ダイナミックDNS: Dynamic DNS content hosts.
- 損害が発生する可能性があるドメイン: Domains with potential damage, characterized by unusual behavior.
- DNS トンネリング VPN: DNS tunneling used to hide traffic for VPN services.
- クリプトマイニング: Cryptomining activity.

At the bottom right, there are buttons for 'Cancel', 'Previous', and 'Next'.

DNSポリシーの作成・管理方法

⑦コンテンツアクセスの制限を設定します

The screenshot shows the 'Content' tab of a DNS policy configuration interface. The top navigation bar includes tabs for Security (selected), Content (selected), Applications, Recipients, and More. The Content tab displays a list of content categories to be blocked:

- 高い**: Includes adult, illegal activity, peer-to-peer, and file sharing websites.
- 中程度**: Includes adult and illegal activity websites.
- 低い**: Includes pornographic, tasteless, and proxy websites.
- カスタム**: Allows manual selection of content categories to block.

To the right, a detailed list of specific content categories is shown:

| カテゴリ | 説明 |
|----------------------------------|--|
| 成人向け | アルコール |
| オーケーション | 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 | 暗号化されたDNS |
| 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 | Online Storage and Backup (オンライン ストレージおよびバックアップ) |

At the bottom right are buttons for 'キャンセル' (Cancel), '前へ' (Previous), and '次へ' (Next).

DNSポリシーの作成・管理方法

⑧アプリケーションの制御を設定します

2 More ━━━━ 3 アプリケーション ━━━━ 4 送信先 ━━━━ 5 ファイル分析 ━━━━ +1 1 More

アプリケーションの制御

組織内のユーザに対してブロックまたは許可するアプリケーションまたはアプリケーションカテゴリを選択します。

アプリケーション設定

Default Settings ▾

制御するアプリケーション

Q アプリケーションを検索

- > Ad Publishing
- > Anonymizer
- > Application Development and Testing
- > Backup & Recovery
- > Business Intelligence
- > Cloud Carrier
- > Cloud Storage

キャンセル 前へ 次へ

DNSポリシーの作成・管理方法

⑨接続先リストの適用を設定します

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。

以降順に、「送信先」「ファイル分析」「ブロックページ」の設定を行います

最後に「サマリー」にて設定した内容を確認し、「保存」します。

The screenshot shows the 'DNS Policy Creation and Management' wizard at step 4: Destination settings. The 'Destination List Application' section is highlighted with a blue border. It contains a search bar, a 'Select All' checkbox, and a dropdown menu showing 'All Lists' and '2 items'. Below this, there are two sections: 'All Destination List' and '1 Block Application Target List' (which is currently empty). The '1 Allow Application Target List' section shows 'Global Allow List' selected. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

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。

宛先リスト名で検索

すべてを選択

すべてのリスト **すべてのリスト** 2合計

すべての接続先リスト

Global Allow List

Global Block List

目的地を見る >

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

Cisco Umbrellaのダッシュボードにログインし、広告ページへのアクセスを許可します。

広告ページのアクセス許可設定方法

Cisco Umbrellaのログイン画面より、ダッシュボードにログインします。

- ①ポリシー > ポリシーコンポーネント > コンテンツカテゴリへ移動します
- ②Default Settingsタブを選択後、カテゴリ中の「広告」を選択解除し、設定を保存します

(※以下はコンテンツカテゴリとして「成人向け」「アルコール」は選択し、「広告」は選択解除する場合の設定例となります)

The screenshot shows two parts of the Cisco Umbrella web interface. On the left is a sidebar menu with options like 'Policy', 'Content Category', and 'Default Settings'. The 'Content Category' option is highlighted with a red box. On the right is a detailed view of 'Content Category' settings under a 'Policy Component' section. It includes a search bar, a 'Default Settings' tab (also highlighted with a red box), and a list of categories. Under 'Category' settings, 'Adult' (成人向け) and 'Alcohol' (アルコール) are checked, while 'Advertising' (広告) is unchecked.

| Category | Status |
|---------------------------|--------------------------|
| Adult (成人向け) | Selected (checked) |
| Advertising (広告) | Not Selected (unchecked) |
| Alcohol (アルコール) | Selected (checked) |
| Animals and Pets (動物とペット) | Not Selected (unchecked) |
| Arts (芸術) | Not Selected (unchecked) |

広告ページのアクセス許可設定方法（つづき）

- ③作成したコンテンツカテゴリを適用します。
左側のメニューより「ポリシー」→「DNSポリシー」→「Default Policy」をクリックします。

The screenshot shows the Cisco Umbrella web interface. On the left, a dark sidebar menu lists various policy types: Overview, Import, Policies (highlighted with a red box), Management, Firewall Policy, Web Policy, Policy Component, Connection List, Content Category, Application Settings, Tenant Control, Scheduling, Security, Blockpage Appearance, and Integration. Under Policies, the DNS Policy option is also highlighted with a red box. The main content area is titled "Policy / Management" and "DNS Policy". It contains a descriptive text about how policies affect security, categories, and connection lists. Below this is a table with one row, "Default Policy", highlighted with a red box. The table columns include "次を含む" (Contains next), "3 Policy Settings", and "最終更新日" (Last Updated) set to "May 12, 2025". A "Get Started" button is visible at the bottom right.

広告ページのアクセス許可設定方法（つづき）

④適用されたコンテンツ設定の「編集」をクリックします。

The screenshot shows the Cisco Umbrella web interface. On the left, a sidebar menu under 'Management' includes 'DNS Policy'. The main panel is titled 'DNS Policy' and displays a table of policies. The first policy listed is 'Default Policy'. In the 'Content Settings' section of this policy, there is a red box around the 'Edit' button next to the 'Edit' link for the 'Content Settings NTT West Settings' row.

| ポリシー名 | 次を含む | 最終更新日 |
|----------------|----------|--------------|
| Default Policy | 3 ポリシー設定 | May 12, 2025 |

Default Policy

ポリシー名: Default Policy

すべてのアイデンティティに適用

適用されたセキュリティ設定: NTT West Settings

適用されたコンテンツ設定 NTT West Settings

適用されたアプリケーション設定がありません

詳細設定

NTT West Settings USE CUSTOM SETTINGS

インテリジェントプロキシの有効化

広告ページのアクセス許可設定方法（つづき）

⑤作成したコンテンツカテゴリ「Default Settings」を選択し「設定して戻る」をクリック

The screenshot shows the Cisco Umbrella interface under the 'DNS Policy' section. On the left sidebar, 'Default Settings' is highlighted. The main panel displays the 'Default Policy' configuration. A red box highlights the 'Default Settings' dropdown in the 'Custom Settings' section. Another red box highlights the 'Set and Return' button at the bottom right of the page.

Default Policy

コンテンツアクセスの制限

そのタイプのコンテンツを提供するウェブサイトへのアクセスをブロックするコンテンツカテゴリを選択してください。プリセットの制御レベルを選択するか、カスタム設定を追加してください。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
「適度」オプションでブロックされるコンテンツに加えて、アダルト、違法活動、ソーシャルネットワーキング、ファイル共有ウェブサイトをブロックします。

○ 中程度
「低」オプションでブロックされるコンテンツに加えて、アダルトサイトと違法活動の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。

カスタム設定

Default Settings

カテゴリ

すべてを選択

成人向け

アルコール

芸術

オークション

大麻

Cheating and Plagiarism (不正および盗用)

コンピュータセキュリティ

総会、会議、および見本市

出会い系

飲食

ダイナミックIPアドレスおよびレジデンシャルIPアドレス

広告

動物とペット

占星術

ビジネスと産業

チャットおよびインスタントメッセージング

クラウドヒーディング

コンピュータおよびインターネット

暗号通貨

デジタルはがき

DIYプロジェクト

教育

脱毛システム

キャンセル 設定して戻る

広告ページのアクセス許可設定方法（つづき）

- ⑥適用されたコンテンツ設定にポリシーが反映されていることを確認し「保存」をクリック

The screenshot shows the Cisco Umbrella web interface under the 'DNS Policy' section. The left sidebar includes options like 'Overview', 'Import', 'Policy' (selected), 'Management', 'DNS Policy' (selected), 'Firewall Policy', 'Web Policy', 'Policy Components', 'Connection List', 'Content Category', 'Application Settings', 'Threat Detection', 'Schedule Settings', 'Security Settings', 'Blockpage Overview', 'Integration Settings', 'Selected Keyword List', 'Reports', 'Investigate', and 'Management'. The main content area is titled 'DNS Policy' and contains a note about policy application. It lists the 'Default Policy' with the following details:

| 次を含む | 最終更新日 |
|----------|--------------|
| 3 ポリシー設定 | May 12, 2025 |

The policy settings include:

- ポリシーネーム:** Default Policy
- すべてのアイデンティティに適用:** Enabled
- 適用されたセキュリティ設定: NTT West Settings:** Includes Command & Control Blocking, Malware, Phishing, and more.
- 適用されたコンテンツ設定 Default Settings:** Includes URL Filtering and Content Blocking.
- 接続先リスト 適用:** Includes 1 Blocklist and 1 Whitelist.
- ファイル分析 無効:** Intelligent proxying is required.
- 適用されたカスタムブロックページ:** NTT West Settings.

A red box highlights the 'URL Filtering' section under 'Content Settings'. At the bottom, there are 'Cancel' and 'Save' buttons, with 'Save' being highlighted by a red box.

例えば覚えのない入金を促すなど不審なサイトへの接続をUmbrellaでも防げない場合があります。
Cisco Umbrellaにて特定のサイトへのアクセスをブロックするには、下記の手順にしたがって操作してください。

Cisco Umbrellaの許可／ブロックリスト設定方法

p64-86を参照ください。

Cisco Umbrellaにて特定のサイトへのアクセスを許可もしくはブロックするには、下記の手順にしたがって操作してください。

Cisco Umbrellaの許可／ブロックリスト設定方法

p64-86を参照ください。

Umbrella には CASB (Cloud Access Security Broker) に関する機能がいくつか導入されています。CASB は一般的に「組織のユーザーがクラウド サービスを安全にアクセスするための仲介役 (ブローカー) の役割を果たす機能やサービス」のことです。

CASBの設定方法

Umbrella Dashboardからポリシ → ポリシーコンポーネント → アプリケーション設定をクリックし、設定したいポリシーをクリックします。

The screenshot shows the 'Application Settings' section of the Cisco Umbrella Policy Management interface. At the top, there's a header with the Cisco logo and the text 'Policy / Policy Component' and 'Application Settings'. A blue circular button labeled 'Add' is visible. Below the header, a message states: '[Application settings] を使用すると、サポートされているアプリケーションで特別な権限を適用できます。' (Using [Application settings], you can apply special permissions to supported applications.)

| Policy Name | Applies To | Last Updated |
|-------------------|------------|--------------|
| Cisco Test Policy | Web Policy | Feb 25, 2025 |
| Default Settings | DNS Policy | Feb 18, 2025 |

特定のクラウドサービスへのアクセスを全面的に禁止したい場合は、DNSポリシーを選択します。
閲覧は許可するが投稿はさせたくない場合は、「Webポリシー」に該当するポリシーを選択します。

注意：すべてのクラウドサービスが設定できるわけはございません。

CASBの設定方法（つづき）

以下の例ではクラウドストレージ全般を選択し、登録されているストレージにアクセスできない（ブロック）設定になっています。

The screenshot shows a list of applications under the 'Cloud Storage' category. Each application has a checkbox and a 'Block' button next to it. All checkboxes are checked, indicating they are blocked.

| Application | Action |
|-------------------------|--------|
| Expedient Cloud Storage | Block |
| 115Tech | Block |
| 123RF | Block |
| 1fichier | Block |
| 23 Photo Sharing | Block |
| 3BB Broadband Cludbox | Block |
| 4shared | Block |
| 4Svnc | Block |

より詳細な設定方法は以下マニュアルを確認ください。

<https://docs.umbrella.com/umbrella-user-guide/docs/add-an-application-setting>

<https://docs.umbrella.com/umbrella-user-guide/docs/add-a-web-application-setting>

Umbrella には CASB (Cloud Access Security Broker) に関する機能がいくつか導入されています。CASB は一般的に「組織のユーザーがクラウド サービスを安全にアクセスするための仲介役 (プローカー) の役割を果たす機能やサービス」のことです。

クラウドサービスの利用状況を確認する方法

Umbrellaダッシュボードから レポート > コアレポート > アプリケーション検出 を選択します。

The screenshot shows the Cisco Umbrella Core Report Application Discovery interface. At the top, there are navigation links: '報告/コアレポート' (Report/Core Report) and 'PDF のダウンロード' (Download PDF). Below these are three cards representing flagged application categories:

- Generative AI**: Shows a red flag icon and the number 2. Description: '未確認のアプリケーションです' (Unverified application). Detail: 'Generative AI apps have the potential for generating misleading or fraudulent content and copyright or intellectual property infringements.' A '詳細' (Details) link is at the bottom.
- P2P**: Shows a red flag icon and the number 1. Description: '未確認のアプリケーションです' (Unverified application). Detail: 'P2Pアプリケーションは、それによって、ウイルスやマルウェアに感染したファイルが送信される可能性があるため、高いリスクになります。' A '詳細' (Details) link is at the bottom.
- ゲーム**: Shows an orange flag icon and the number 1. Description: '未確認のアプリケーションです' (Unverified application). Detail: 'オンラインゲームは、生産性を失う可能性があるだけでなく、リスクにもなります。多くの企業の環境では、これらのアプリケーションの使用は推奨されません。' A '詳細' (Details) link is at the bottom.

各カテゴリなどの説明についてはUmbrella マニュアルを参照してください。

<https://docs.umbrella.com/deployment-umbrella/docs/app-discovery>

テナント制御とは、管理者によって指定されたクラウドサービスの契約テナント（環境）のみにアクセスできるよう制御する機能です。

例えば、会社貸与のパソコンから会社で契約しているMicrosoft 365環境へのみ接続を許し、個人契約のMicrosoft 365に接続させないなど制御することができるようになります。

Umbrella では現在 Microsoft 365, Google G Suite (Google Workspace), Slack, Dropbox に対応しています。

- ①Umbrellaダッシュボードにログインし、左枠 ポリシー → ポリシーコンポーネント → テナント制御をクリックします。



- ②「Global Tenant Controls」をクリックします。

Cisco Umbrella の「Global Tenant Controls」画面。画面の上部には「ポリシー / ポリシーコンポーネント」と「テナントコントロール」があります。下部にはテナント制御に関する説明文があり、「テナント制御を使用すると、Software as a Service (SaaS) のクラウド内のアプリケーションへのアイデンティティアクセスを制御できます。設定して Web ポリシールールセットに追加すると、アイデンティティアクセスは組織で承認されたりソースのみに制限されます。その結果、共有ドメインで実行されているクラウド内のリソースにアクセスするときに、組織は保護され、安全になります。開始するには、[追加 (Add)] をクリックします。詳細については、Umbrella の ヘルプ を参照してください。」

| Global Tenant Controls | Microsoft 365 0 テナント | G Suite 0 ドメイン | Slack 0 ワークスペース | Dropbox 0 Teams | 変更日 May 12, 2025 |
|--|-------------------------|-------------------|--------------------|--------------------|---------------------|
| <input type="button" value="Search..."/> | | | | | |

②例えば、Example 社には Microsoft 365 の契約しているテナントがあり、a.example.com というテナントのみアクセスを許可したい場合の例を示します。Microsoft 365 の「テナントドメイン/ID」に a.example.com を入力し、追加ボタンをクリックします。

| Global Tenant Controls | Microsoft 365 0 テナント | G Suite 0 ドメイン | Slack 0 ワークスペース | Dropbox 0 Teams | 変更日 Feb 26, 2025 |
|------------------------|-------------------------|-------------------|--------------------|--------------------|---------------------|
|------------------------|-------------------------|-------------------|--------------------|--------------------|---------------------|

設定名
Global Tenant Controls

Microsoft 365 アプリケーションおよびサービスへのアクセスを許可するアカウントのタイプを選択します。

テナント
アクセスを承認するクラウドアプリケーションまたはスイートを選択します。

Microsoft 365
OneDrive、Word、PowerPoint、Excel、Outlookなど

Slack
エンタープライズ向けSlack

Dropbox
Dropbox for Enterprise

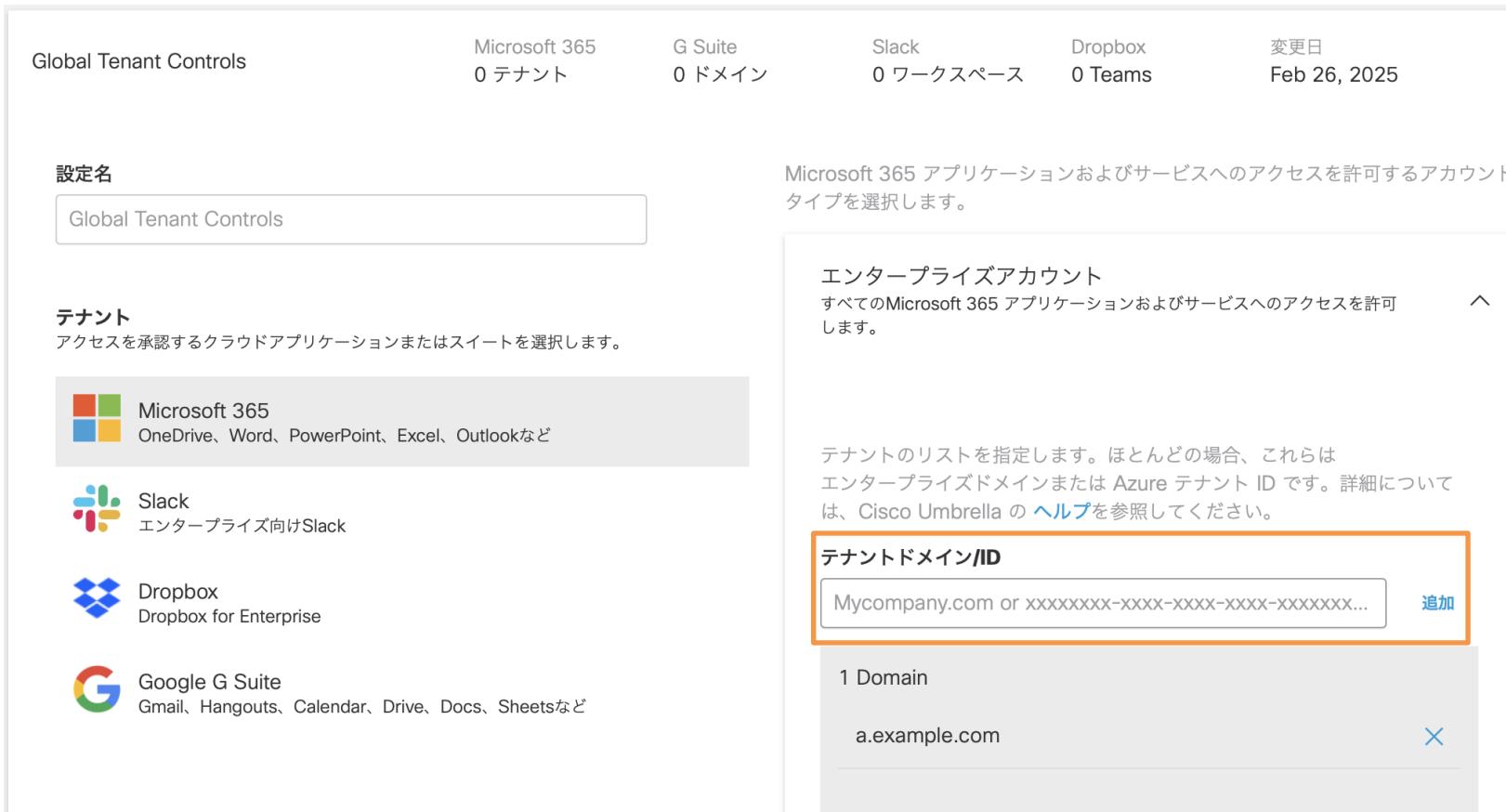
Google G Suite
Gmail、Hangouts、Calendar、Drive、Docs、Sheetsなど

エンタープライズアカウント
すべてのMicrosoft 365 アプリケーションおよびサービスへのアクセスを許可します。
▲

テナントのリストを指定します。ほとんどの場合、これらはエンタープライズドメインまたは Azure テナント ID です。詳細については、Cisco Umbrella の [ヘルプ](#)を参照してください。

テナントドメイン/ID
Mycompany.com or xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx...
追加

1 Domain
a.example.com X



③画面下部に個人アカウントにて「個人用Microsoft 365アカウントのアクセスをブロックする」をクリックしレバーをオンの状態にします。



④画面下部の保存ボタンをクリックします。

以上で設定は終了です。



Cisco Umbrellaでは、DNSやWebポリシーのログから、Webアプリやクラウドサービスの利用状況を可視化し、通信を制御することができます。

- ①Umbrella Dashboardのトップ画面（概要）の下部に表示される「アプリケーションの検出と制御」から、「すべて表示」をクリックします。
(左メニューの レポート > コアレポート > アプリケーション検出 からもアクセスできます)

The screenshot shows the Cisco Umbrella Dashboard under the 'Overview' tab. On the left, a sidebar lists various menu items. In the center, there's a large section titled 'Application Detection and Control (Past 90 Days)' which displays the following data:

- 114 detected cloud applications
- 1 risky cloud application

A button labeled 'View All' is highlighted with an orange box at the bottom right of this section. To the right, there are two panels: 'Flags Set for Categories' and 'Flags Set for Applications'. The bottom right corner of the dashboard has a 'Dashboard' button.

Left sidebar (Menu Items):

- 概要 (highlighted with an orange box)
- 導入
- コアアイデンティティ
- ネットワーク
- ネットワークデバイス
- ローミングコンピュータ
- モバイルデバイス
- 登録済みアプリアンス
- Chromebookユーザー
- ネットワークトンネル
- ユーザとグループ
- 設定
- ドメイン管理
- サイトとActive Directory

Bottom right corner (Buttons):

- すべて表示 (highlighted with an orange box)
- ダッシュボードの表示

②「アプリケーション検出」画面から、検出されたWebアプリケーションやクラウドサービスが一覧で確認できます。リスクのあるアプリケーションは判定が「Very High」、「High」として表示されます。

Reporting / Core Reports
Cisco App Discovery

Back to Dashboard

FILTERS Search by application or vendor

Filter by Identity

Label Select All

- Unreviewed (114)
- Approved (0)
- Not Approved (0)
- Under Audit (0)

Controllable Apps

- All Controllable Apps
- Advanced Controls

Risk Select All

- Very High
- High
- Medium
- Low
- Very Low

Category Select All

- Ad Publishing
- Application Development and Testing
- Business Intelligence
- Cloud Storage
- Collaboration
- Compute
- Content Delivery Network

114 Total Applications

| Application | Risk Score | Identities | DNS Requests | Total Web Traffic | Label | Control this app |
|---|------------|------------|--------------|--|------------|------------------|
| Protected Media Security | High | 1 | -- | 669.2 KB total traffic 621.3 ... 47.9 KB | Unreviewed | Control this app |
| OneTrust Security | Medium | 4 | 8 | 157.9 KB total traffic 66.4 KB 91.5 KB | Unreviewed | Control this app |
| walkme Digital Adoption Platform Business Intelligence | Medium | 3 | 234 | 4.6 MB total traffic 4.4 MB 192.0 ... | Unreviewed | Control this app |
| Intercom Customer Relationship Manage... | Medium | 4 | 37 | 120.7 KB total traffic 79.8 KB 40.9 KB | Unreviewed | Control this app |
| Qualtrics Website and App Feed... Business Intelligence | Medium | 6 | 131 | 3.9 MB total traffic 3.5 MB 380.5 ... | Unreviewed | Control this app |

Download CSV

③対象のアプリケーションをクリックすると、リスクが高い理由に加えて、いつ、どの端末が、これくらいアクセスしたのかを確認することができます。

The screenshot shows the Umbrella application dashboard with the following details:

Application Details:

- Name:** Protected Media
- Category:** Security
- Vendor:** Protected Media
- DNS Requests:** Total: -- Blocked: --
- First Detected (UTC):** Feb 17, 2025
- Last Detected (UTC):** Feb 17, 2025

Risk Details:

- Weighted Risk:** High
- Business Risk:** High
- Usage Risk:** Medium
- Vendor Compliance:** Not Found

How We Calculate Risk (Help us improve): App Discovery's Composite Risk Score (CRS) for cloud services combines three elements to calculate a standardized measure of the risk for a cloud service: Business Risk, Usage Risk and Vendor Compliance.

Business Risk Factors:

- Typical use of the service (personal or organizational).
- The Talos Security Intelligence Web Reputation score for the service.
- Financial viability of the app vendor.
- Type of data stored by the app.

Usage Risk Factors:

- Volume; how much data flows to and from the service.
- Users; how many of your users depend on or use the service.

Vendor Compliance Factors:

- Security controls in place.
- Certifications earned.

Identity Details:

| Identities | DNS Requests | Blocked DNS Requests | Web Traffic | Blocked Web Traffic | First Detected | Last Detected |
|------------|--------------|----------------------|-------------|---------------------|----------------|---------------|
| AAA | -- | -- | 669.2 KB | -- | Feb 17, 2025 | Feb 17, 2025 |

Page Navigation: ページ: 1 / 各ページの結果数 50 / 1-1/1 < >

Labels:

- リスク判定理由 (Reason for Risk Judgment) - Points to the Business Risk section.
- 端末の確認 (Device Confirmation) - Points to the Identity table.

④アプリケーションに対して、許可やブロックの評価が完了した後は、それに応じたラベルを付与できます。

評価に基づいて
ラベルを付与

Unreviewed (selected)

Approved

Not Approved

Under Audit

Control this app

通信拒否設定

⑤実際にDNSポリシーやWebポリシーによって、通信を許可、拒否することができます。
(DNSはドメイン単位、WebはURL単位)

Control Protected Media

To control an application, select an application list and an action.
For more information, see Umbrella's [Help](#).

DNS Application Settings Web Application Settings

3 Total, 1 Selected

| Application Settings | Applied in Policies | Action |
|---|--|--------------------------------------|
| <input checked="" type="checkbox"/> XYZ | Not applied. Add to a DNS Policy . | <input type="button" value="Block"/> |
| <input type="checkbox"/> ABCD | Not applied. Add to a DNS Policy . | <input type="button" value="Block"/> |
| <input type="checkbox"/> LMNOP | Not applied. Add to a DNS Policy . | <input type="button" value="Block"/> |

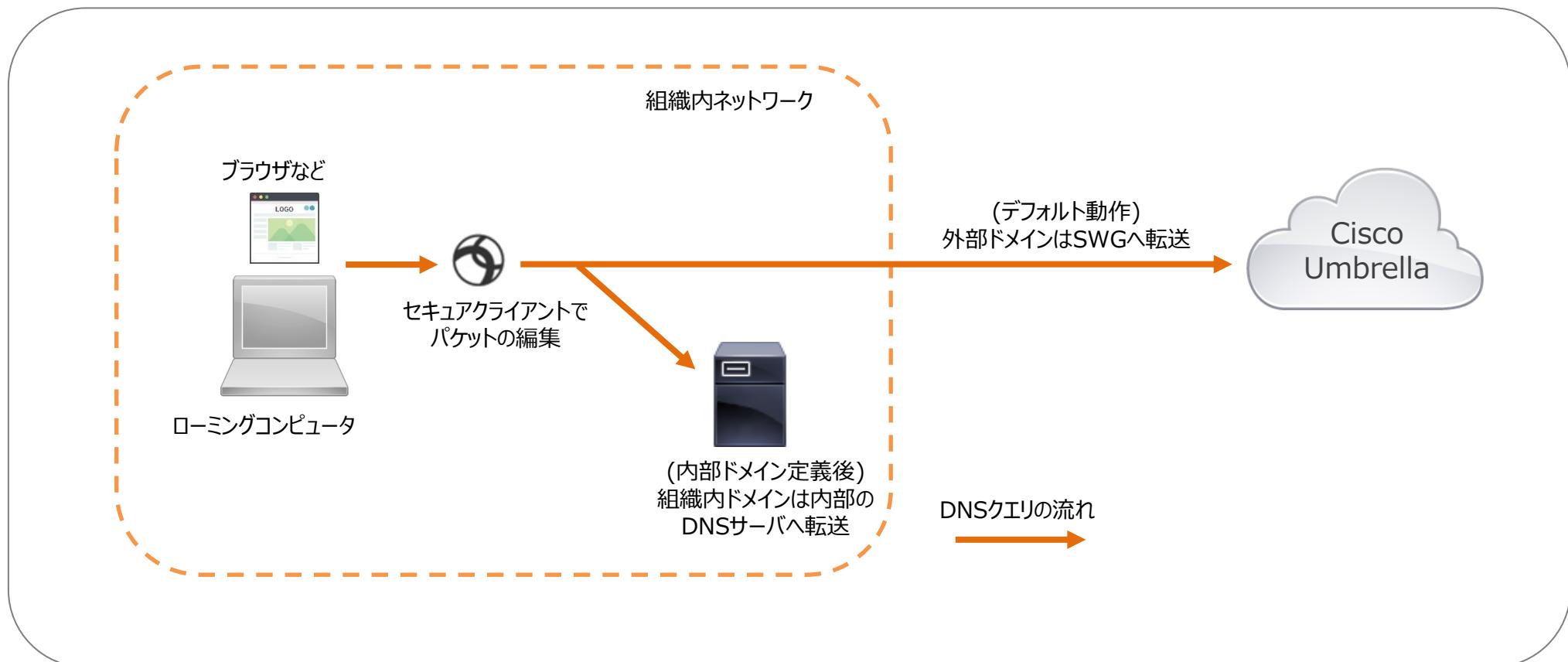
CANCEL SAVE

ポリシーごとにアクションを定義可能

デフォルト動作では、Cisco Umbrella はユーザー PC 上で生成された 全てのDNS クエリを Umbrella に転送し、そのクエリを検査/ブロックすることでセキュリティ機能を提供しています。

しかし、組織内のサーバに対する名前解決までもが組織外にある Umbrella によって行われますので、組織内のコンテンツにアクセスできなくなる問題が発生します。これに対応できるようにUmbrella Dashboard の「内部ドメイン」という設定で組織内のドメインを定義できるようになり、PC 上で生成された DNS クエリーのうち、組織内のドメインの DNS クエリだけを Umbrella に転送しないようにすることができます。

以下にデフォルト動作のDNSクエリの流れ、内部ドメインを定義した際のDNSクエリの流れを示します。



ドメインの追加画面「導入 → ドメイン管理 → 追加」では Umbrella に直接ルーティングしないトラフィックの内部ドメインリストを作成します。リスト化したドメインはUmbrellaではなく、組織内ネットワークに属するDNSサーバ等で名前解決をします。

①例として、「example.com」ドメインを追加した際の動作を以下に示します。

「example.com」を追加した場合、「www.example.com」や「ftp.example.com」といったとすべてのサブドメインが内部ドメインとして処理されます。また、「.local」ドメインの場合は、事前に内部ドメインリストに登録されているため設定不要です。

②「適用先」では内部ドメインの適用先を選択できます。

「サイト」は「導入 > 設定 > サイトとActive Directoryで定義したサイト」を、「デバイス」はローミングコンピュータに該当します。

適用例として、「サイト」に適用し、「デバイス」には適用しない場合、サイトからのトラフィックのみがローカルリゾルバを使用する動作となります。

新しいバイパスドメインまたはサーバの追加

ドメインを追加すると、そのドメインのすべてのサブドメインが設定を引き継ぎます。
'example.com'が内部ドメインリストにある場合、
'www.example.com'は内部ドメインとしても処理されます。

ドメインタイプ
 内部ドメイン 外部ドメインおよびIP

1

ドメイン
example.com

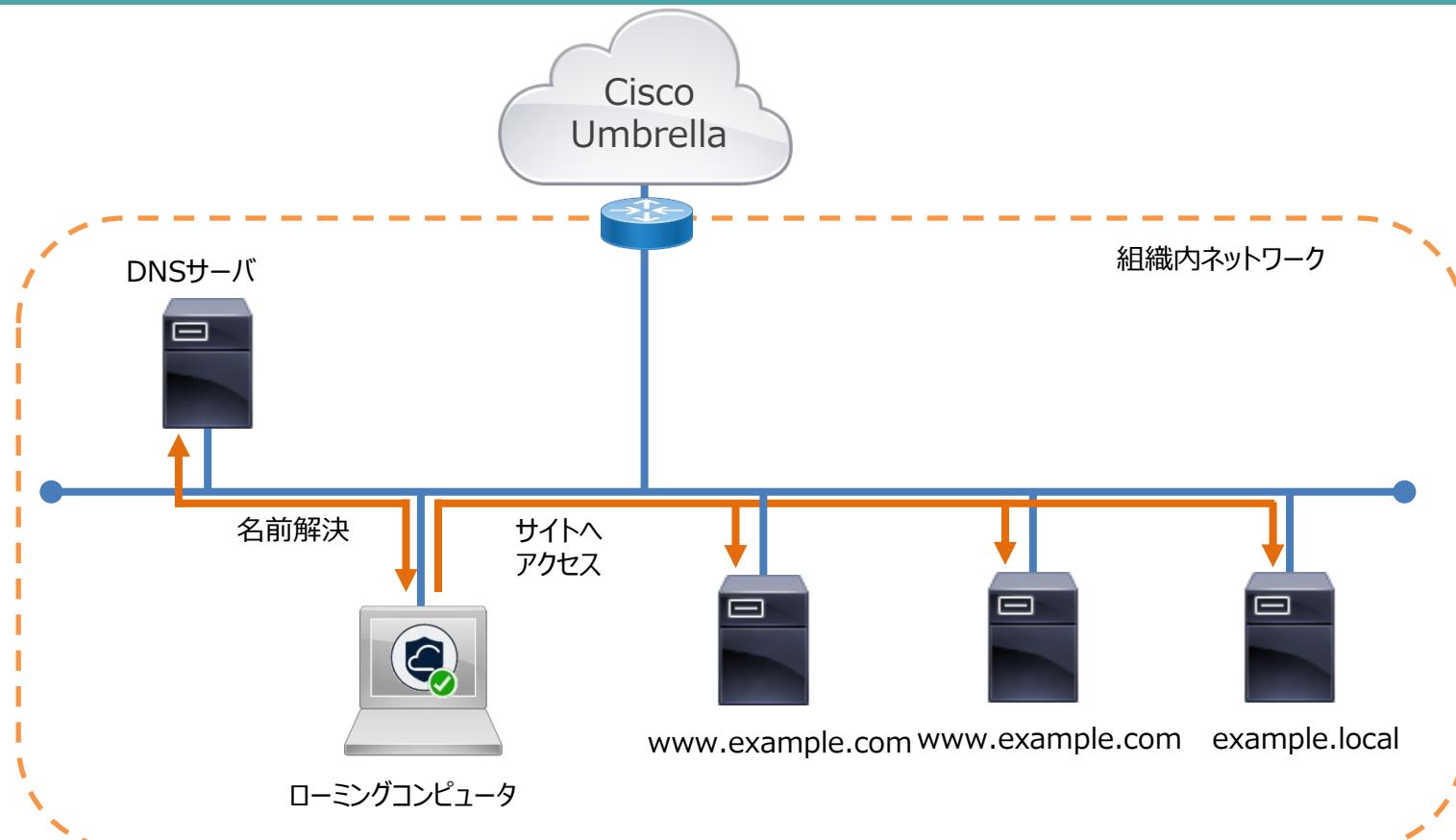
説明

2

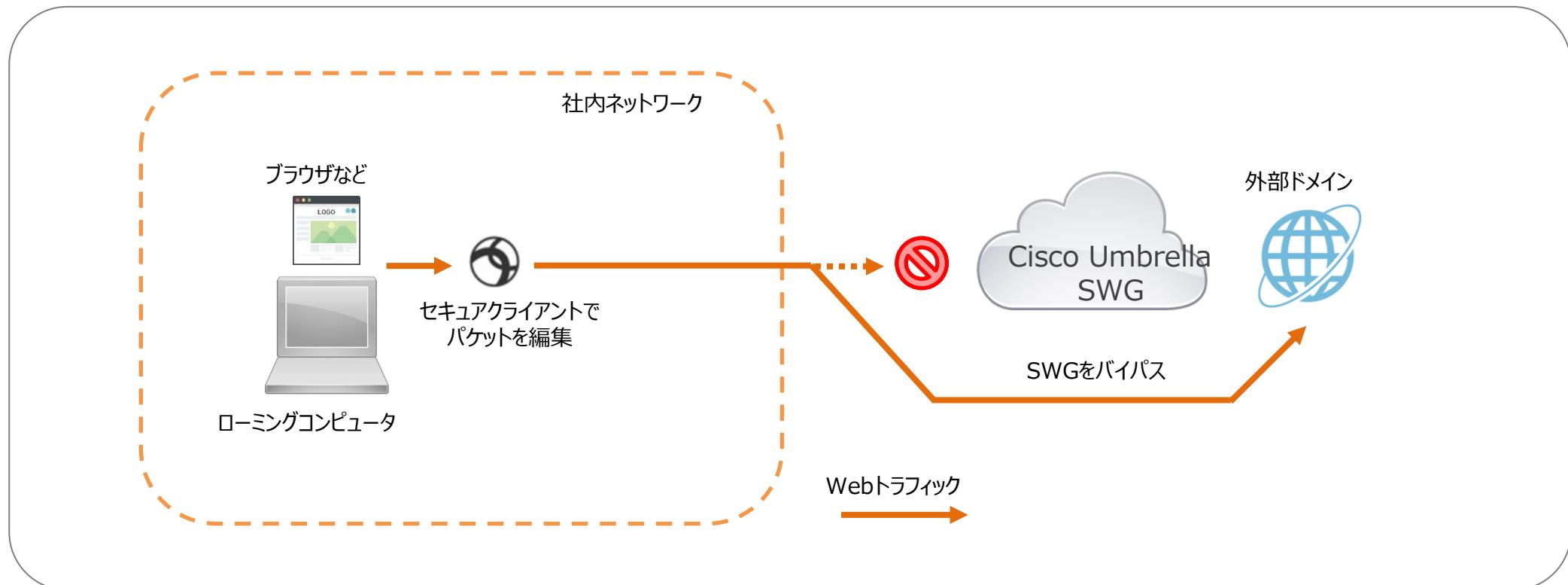
適用先
すべてのサイト ✕ すべてのデバイス ✕ ▾

キャンセル 保存

ドメインの追加画面



Umbrellaでは、クラウド側に SWG (Secure Web Gateway) という HTTP/HTTPS のフルプロキシサーバを提供しています。しかし、プロキシを介した場合、Web通信が正常に行われないサイトや、送信元IPアドレスによるアクセス制限を適用しているサイト等へアクセスする際、組織外の一部のドメイン宛ての通信をUmbrella から除外したい場合があります。これに対応できるようにUmbrella Dashboard の「外部ドメイン」設定で組織外のドメインを定義し、SWGを経由せず、ローミングコンピュータから直接対象の外部ドメインへ通信を行うことが可能になります。以下に外部ドメインを定義した際のWebトラフィックの動作イメージを示します。

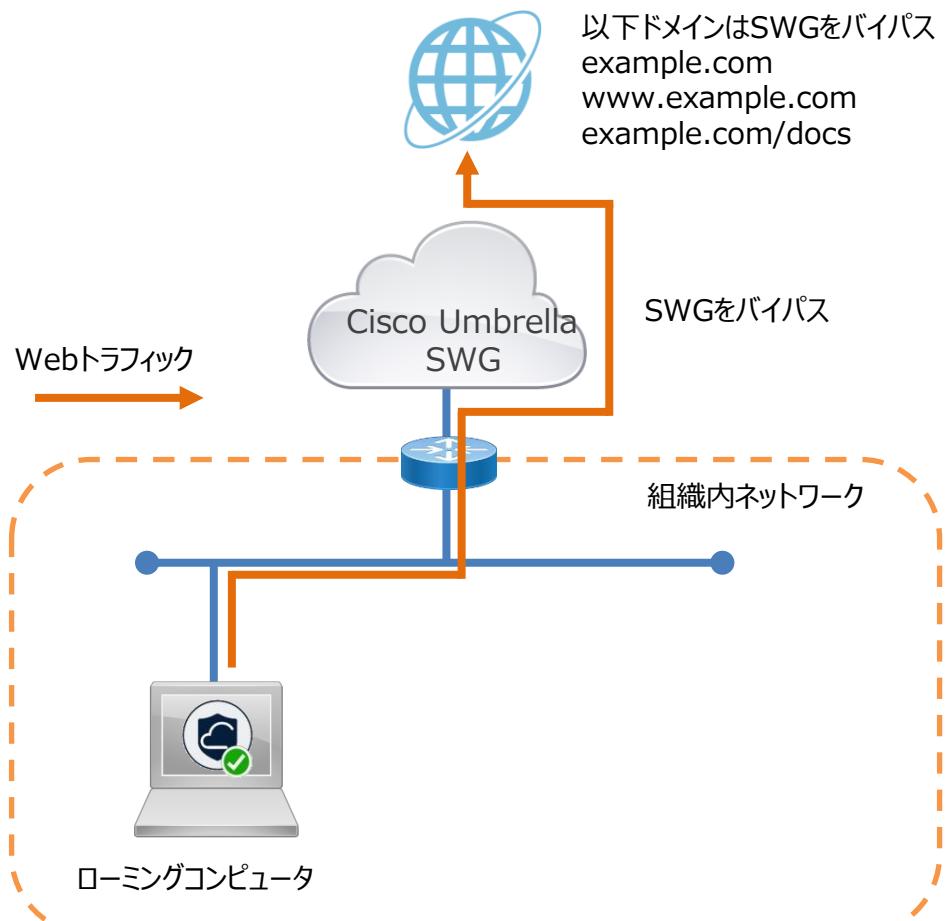


ドメインの追加画面「導入 → ドメイン管理 → 追加」にて、SWGを経由しない外部ドメインのリストを作成します。

①「ドメインタイプ」では「外部ドメインおよびIP」を選択し、②「エンティティ」にはSWGを経由せずに直接通信を行いたいWebサイトの「ドメイン、IPまたはCIDR」を入力します。以下に「エンティティ」に「example.com」を設定した際のWebトラフィックの動作イメージを示します。

また、以下表に記した通り、ドメインリストに追加するとすべてのドメインには、左側と右側に暗黙のワイルドカードが適用され、表に示したドメインが外部ドメインとして処理されます。ただし、Umbrellaのドメインリストはアスタリスク(*)をサポートしていません。そのため、アスタリスク(*)を使用して、ドメインの一部をワイルドカードとして登録することはできません。

| エンティティ | 暗黙のワイルドカード |
|----------------|--------------------|
| example.com | *.example.com/* |
| com | *.com/* |
| www.domain.com | *.www.domain.com/* |



ドメインの追加画面

8. セキュアエンドポイント コンソールへのログイン手順 < Cisco Secure Endpoint Essentials >

8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

受信したインビテーションメール等からCisco Secure Endpoint管理コンソールへログインするまでの手順を示します。

- ① 1人目の管理者は開通メール記載の右記URLをクリック (<https://sign-on.security.cisco.com/signin/register>)
2人目の管理者は受信した電子メールから枠内の [here] をクリック
- ② [Email^{*1}]、[First name]、[Last name]、[Country]、[Password^{*2}]を入力し、規約の同意にチェック
※¹Emailには申込書に記載したメールアドレスを記入ください ※²設定するパスワードには条件があります (図の②右部をご参照ください)
- ③ [Sign up]をクリック

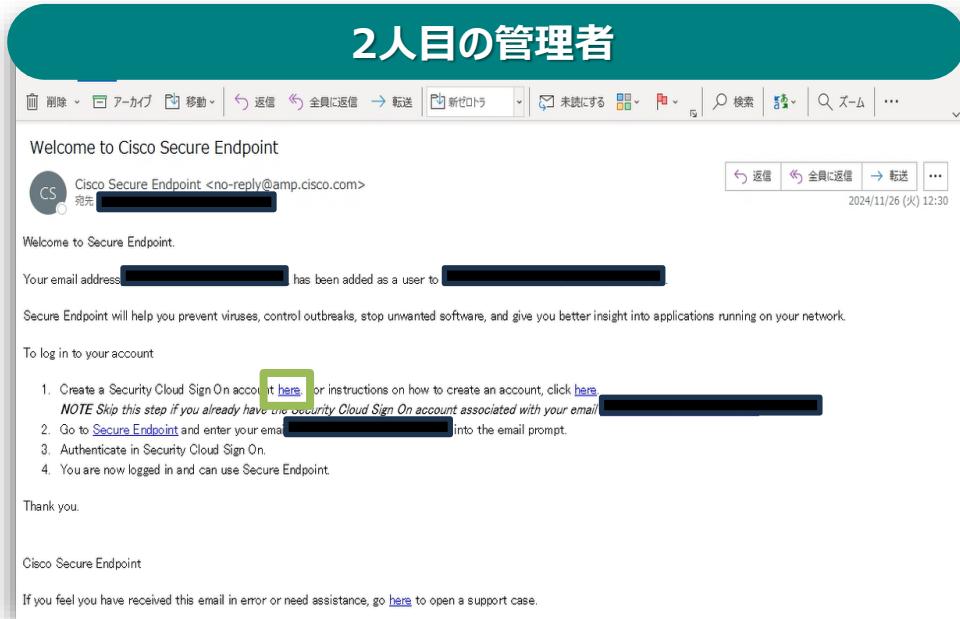
1人目の管理者

1

<https://sign-on.security.cisco.com/signin/register>

2人目の管理者

1



Account Sign Up

2

Provide following information to create enterprise account.
[Back to login page](#)

Email *

First name *

Last name *

Country *

Password *

Confirm Password *

I agree to the [General Terms](#) and [Privacy statement](#).

3

Sign up

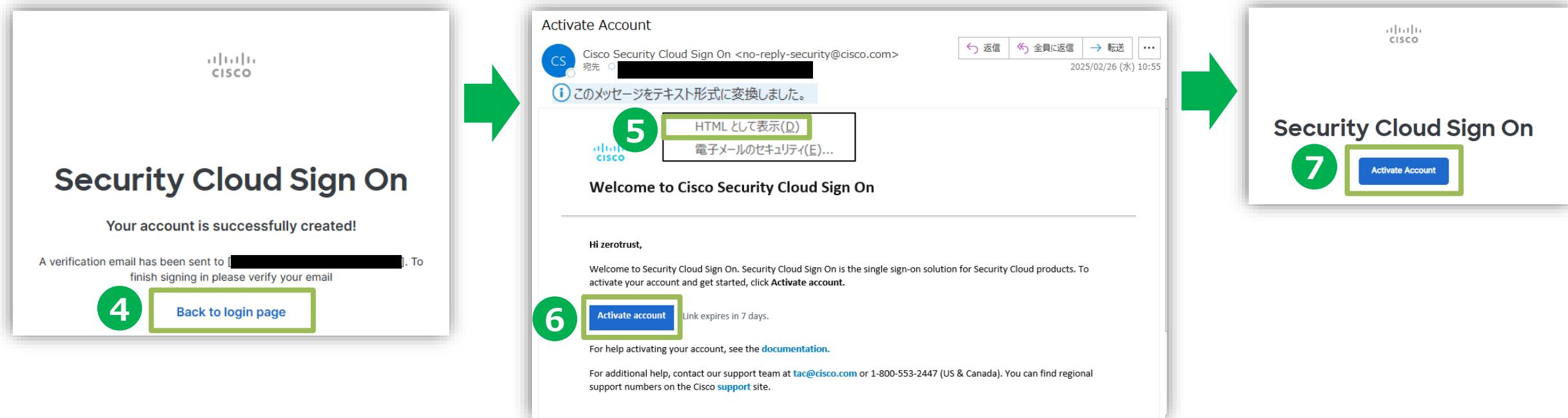
Cancel

Password Requirements

- ✓ 最低8文字
- ✓ 最低1文字の数字を含む
- ✓ 最低1文字の記号を含む
- ✓ 最低1文字の小文字を含む
- ✓ 最低1文字の大文字を含む
- ✓ 'ユーザー名'の一部を含まない
- ✓ 'First name'を含まない
- ✓ 'Last name'を含まない

8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ④ [Back to login page]をクリックし、ブラウザを閉じます。
- ⑤ 受信した電子メール[件名：Activate Account]を開き、[このメッセージをテキスト形式に変換しました]をクリックしてHTMLとして表示させます。
- ⑥ [Activate account]をクリック
- ⑦ [Activate Account]をクリック



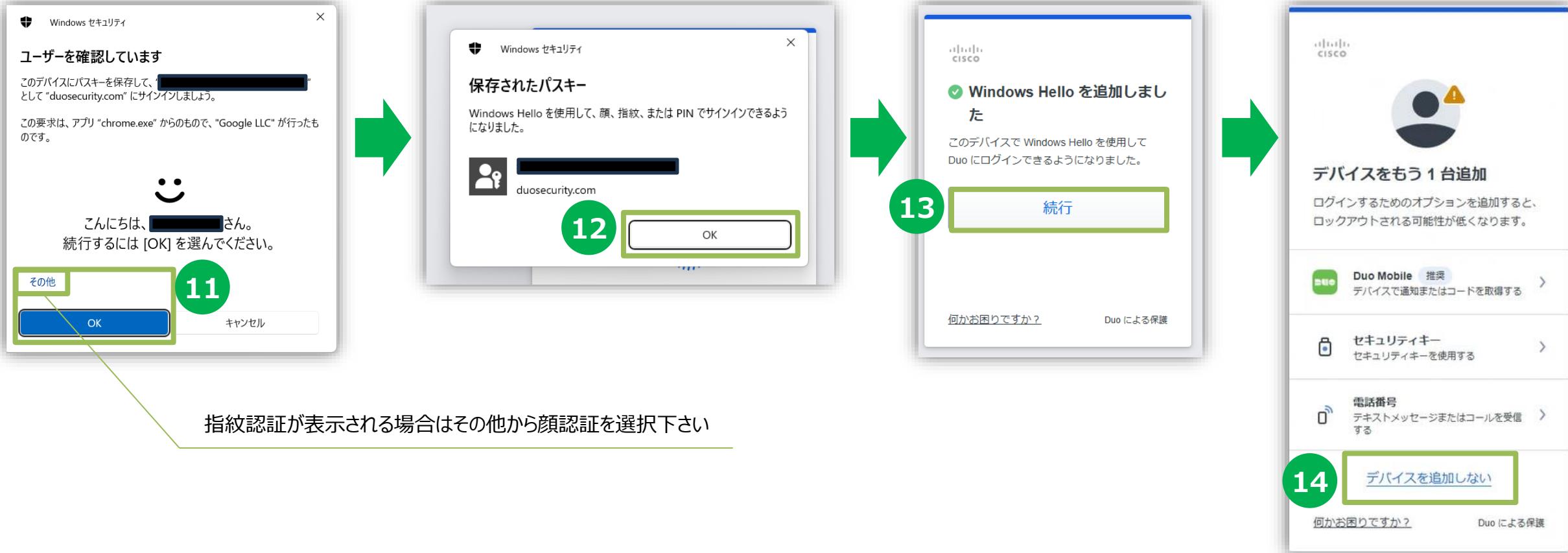
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ⑧ [始める]をクリック
⑨ [Windows Hello]をクリック ※二段階認証を設定してください。マニュアル上では[Windows Hello]を使用し顔認証を設定しています。
⑩ [続行]をクリック



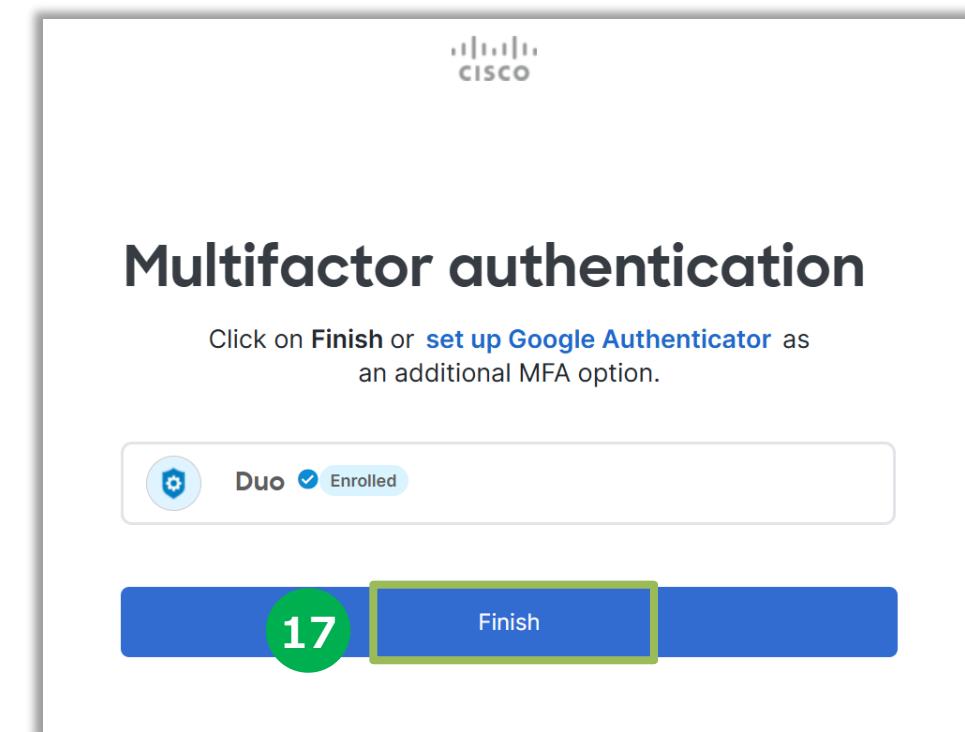
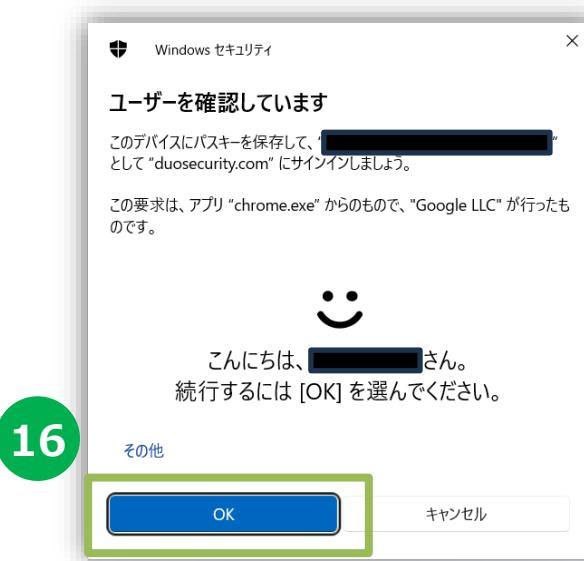
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ⑪ 顔認証が成功したら[OK]をクリック（指紋認証が表示される場合は[その他]から顔認証を選択下さい）
- ⑫ [OK]をクリック
- ⑬ [続行]をクリック
- ⑭ [デバイスを追加しない]をクリック ※認証方法は後からでも追加・変更が可能です。



8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ⑯ [Duoでログイン]をクリック
- ⑰ 顔認証が成功したら[OK]をクリック
- ⑱ [Finish]をクリック



8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

⑯ 初回ログインではCiscoサービスのポータルサイトが立ち上がります。

⑰ ブラウザを開き直し、改めてCisco Secure Endpoint管理コンソールのURLを開きます。

Cisco Secure Endpoint管理コンソール : <https://console.apjc.amp.cisco.com>

18

Welcome back, [REDACTED]

Secure Client Management
Use these links to access Secure Client Management. You may bookmark these regional URLs for future direct access.
North America Europe APJC

Applications (39 Products)

Global Region 7 Products

Cisco Cloudlock Cisco Meraki Cisco Umbrella
Launch → Launch → Launch →
Duo Secure Access Secure Malware Analytics (India)
Launch → Launch → Launch →
Secure Workload
Launch →

North America Region 11 Products
Europe Region 9 Products
APJC Region 12 Products

19

ダッシュボード
DMY020000031_ダミー会社2-31

はじめに
オンラインヘルプの表示

Secure Endpointコネクタの導入
Windowsコネクタのセットアップ
Macコネクタのセットアップ
Linuxコネクタのセットアップ

アウトブレイク制御
デモデータ
デモデータを使用して、実際にマルウェアに感染した状態から再生したデータをコンソールに入力することができます。デモデータを有効になると、コンピューターとイベントがSecure Endpointコンソールに追加され、マルウェアが検出されたときの各表示(グッシュボード、ファイルトラッキング、デバイスマラウェア)、脅威の痕跡、検出結果とイベントの動作を見ることができます。デモデータは実際に使用中のSecure Endpoint環境からのデータと差がありませんが、データの品質の良さにはシビア(重大度)が高いため、表示によっては実際のイベントが見えなくなる場合があります。

アドミン
デモデータの有効化

Cisco XDR
またはSecure Client
詳しくはこち
Cloud Managementへの統合

Q Search

Upbita ここをクリックしてPDFを表示します
Secure Endpointの動作確認エンジン、エンドコードされたPowerShellを実行するWMIPRIVEサービス(wmpvive.exe)を検出すると、 WannaMine攻撃は停止されます。エンコードされたコマンドが攻撃結果には必要ですが、動作確認エンジンプロセスを終了して、悪意のあるアクションが以上実行されないようにします。

CozyDuke ここをクリックしてPDFを表示します
悪用されたDLL挟み(パス)まで検出トレースし、アップストリームCnCへの通信をブロックし、エンドポイントNOCを削除してさらなる攻撃を防ぎます。

Upatre ここをクリックしてPDFを表示します
スピアフィッシング攻撃の帮助から終了までの軌跡を表示します。

PlugX ここをクリックしてPDFを表示します
マルウェア攻撃をトレースし、エンドポイントNOCを使用してさらなる攻撃を封じ込む方法を学習します。

Cryptowall ここをクリックしてPDFを表示します
Secure Endpointが複数のURLを検出します。Secure Malware Analyticsでサンドボックスを使用してマルウェアを検出する方法を確認します。

低抵抗の実行可能ファイル ここをクリックしてPDFを表示します
自動抵抗サンドボックス機能を使用すると、未知のマルウェアを検出し、レトロスペクティブイベントを使用してマルウェアを封じ込めることができます。

8. コンソールへのログイン手順 <システムログイン>

Cisco Secure Endpoint管理コンソールへログインするまでの手順を示します。

- ① 以下のURLへアクセス

<https://console.apjc.amp.cisco.com>

- ② Email欄に[メールアドレス]を入力し、[Continue]をクリック

- ③ [パスワード]を入力し、[Log in]をクリック

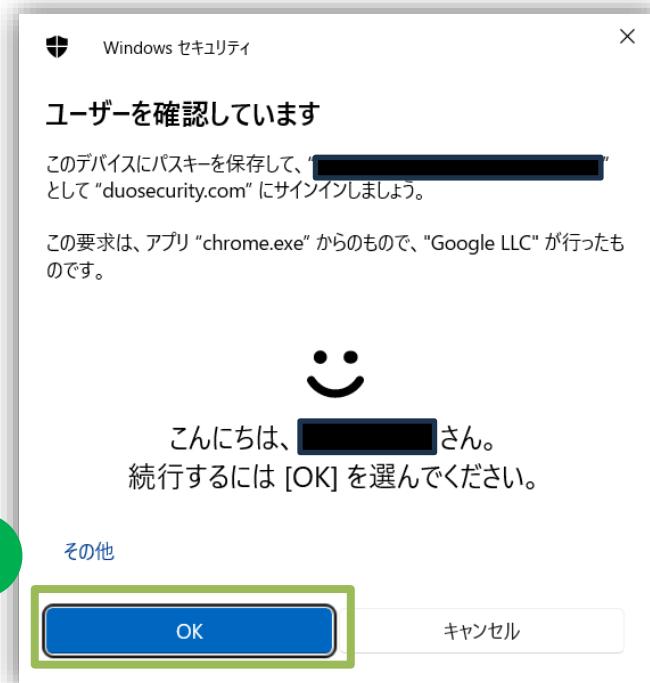
The screenshot shows a browser window titled "Security Cloud Sign On - サインイン". The URL in the address bar is "https://console.apjc.amp.cisco.com". The main content area displays the "Security Cloud Sign On" logo and a large green callout box labeled "1" containing the URL. Below the logo, there is a "Email" input field with a placeholder and a blue "Continue" button. At the bottom, there is a link "Don't have an account? [Sign up now](#)".

The screenshot shows the same "Security Cloud Sign On" page after step 1. A large green arrow points from the previous screen to this one. The "Email" input field is highlighted with a green border and labeled "2". The "Continue" button is also highlighted with a green border.

The screenshot shows the final step of the login process. The "Email" input field is filled with a redacted email address and has a green border. The "Password" input field contains redacted text and has a green border. To the right of the password field is a "Show" link. Below the fields are "Forgot password" and "Log in" buttons. The "Log in" button is highlighted with a green border and labeled "3".

8. コンソールへのログイン手順 <システムログイン>

- ④ 設定した2段階認証を実施 ※以下はWindows Helloで顔認証を実施しています。
- ⑤ 認証が成功し、Cisco Secure Endpointの管理コンソール画面が表示されることを確認



A screenshot of the Cisco Secure Endpoint management console. The title bar says "Secure Endpoint". A green circle with the number "5" is in the top-left corner of the dashboard area. The dashboard features a sidebar with links like "ダッシュボード", "受信トレイ", "概要", "イベント", "分析", "アウトブレイク制御", and "管理". The main content area shows a message "としてログインしています" above the "ダッシュボード" section. On the right side, there are sections for "Cisco XDR", "デモコンピュータ" (with examples like WMIPRVSE and CozyDuke), "Upatre", "PlugX", "CryptoWal", and "低抵散度の実行可能ファイル". Each section includes a link to a PDF for more details.

8. コンソールへのログイン手順 <ダッシュボード説明>

ログイン後最初に開くページです。

社内のマルウェア感染状況を一覧で確認することが可能です

The dashboard displays the following key information:

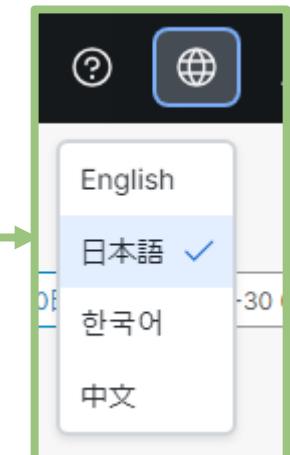
- Overall Threat Level:** 76.9% 優先されている
- Threat Status:** 受信トレイのステータス (30個が要注意, 0個が進行中, 0個が解決済み)
- Isolation:** 隔離された検出 (1/39)
- Vulnerability:** 脆弱性 (シビアティ(重大度)の高い脆弱性, リスクスコアが高いコンピュータ)
- Secure Malware Analytics:** 自動分析の送信, 遊戏的な脅威検出
- Statistics:** 39 コンピュータ, 29.4K スキャンされたファイル, 3.31K ログに記録されたネットワーク接続
- Quick Start:** Windowsコネクタのセットアップ, Macコネクタのセットアップ, Linuxコネクタのセットアップ
- Event Timeline:** 重大侵害の観測対象 (12月 31, 1月 1-29)
- Event Types:** 侵害イベントタイプ (検出された脅威, 実行されたマルウェア)

ヘルプ、およびヘルプ目次、リリースノート、サポートへの問い合わせリンク



不明な点はこちらに説明が記載しております。

<言語設定>



8. コンソールへのログイン手順 <管理メニュー>

各操作項目の概要を以下に記載します



| メニュー項目 | 説明 |
|-----------|---|
| ダッシュボード | ヒートマップ、脆弱なソフトウェア、Secure Malware Analytics／遡及的脅威検出、等 |
| 受信トレイ | 侵害の兆候(IoC)が見られるエンドポイントの優先順位付けされたビュー |
| 概要 | 管理対象エンドポイントの正常性に関する概要 |
| イベント | すべてのイベントのテーブルビュー |
| 分析 | 脅威イベントを多様な角度から分析した内容を確認することが可能 |
| アウトブレイク制御 | ブロックリスト、許可リスト、隔離、および多数の自動アクションを制御 |
| 管理 | ポリシー、グループなどエージェントの挙動に関する設定をする項目 |
| アドミン | ユーザーアカウントの設定、監査ログやデータ等のシステムの管理項目 |

9. セキュアエンドポイント機能を設定変更する < Cisco Secure Endpoint Essentials >

9. セキュアエンドポイント機能を設定変更する（設定変更例一覧）

弊社推奨設定でサービスをご利用開始いただいておりますが、ご利用環境やセキュリティポリシーに応じて、設定の変更をお願いいたします。

トラブル対応による設定変更例

1. ウィルスに感染したかもしれない
2. 自分の名前で勝手にメールが送られている

ご利用環境等に応じた設定変更例

3. セキュアエンドポイントをインストールしたい
4. パソコンを買い替えたのでセキュリティを入れなおしたい
5. パソコンを廃棄するのでセキュリティソフトを消したい
6. 検知エンジンの動作モードを確認・変更したい
7. アインインストール時にパスワードロックしたい
8. 検知したマルウェアが実際に危険なファイルであるかを確認したい
9. ファイル隔離が過検知であったので解除したい
10. 隔離されたファイルを復元したい
11. パソコンの動作が重くなったように感じる
12. デバイス制御方法

「ウィルスに感染したかもしれない」と感じられる場合、Cisco Secure Endpoint管理コンソールで以下の作業を実行してください。

1. 該当端末をネットワークから切断する

感染が疑われる端末は、LANケーブルを抜いたり無線接続のスイッチを切り、すぐにネットワークへの接続を切断してください。
情報漏えいや他のパソコン・端末等へのウイルス拡散・感染といった被害を防ぐことにつながります。

2. Secure Endpointでの手動隔離の実施

同じネットワークで別の端末(パソコン等)をご利用の場合、全てのパソコンで実施してください。

- ①Secure Endpointのダッシュボードを開きます。
- ②[管理] をクリックし、
- ③「コンピュータ」を選択します。



2. Secure Endpointでの手動隔離の実施（つづき）

④感染が疑われるコンピュータを選択し、「隔離の開始」のクリックします。

The screenshot shows the 'Protect' group details for 'Demo1'. A purple circle labeled '4' highlights the 'Isolation Start' button in the bottom navigation bar, which is highlighted with a red box. The navigation bar also includes 'Scan...', 'Diagnose...', 'Move to Group...', 'Uninstall Connect...', and 'Delete' buttons.

⑤任意でコメントを記載し、「開始」をクリックします。



2. Secure Endpointでの手動隔離の実施（つづき）

⑥隔離を停止したい場合、対象のコンピュータを選択し、「隔離の停止」のクリックします。

グループ「Protect」内のDemo_AMP

▶ 隔離

| | | | |
|---------------|--|------------------------|---------|
| ホスト名 | Demo_AMP | グループ | Protect |
| オペレーティング システム | Windows 10 (ビルド 19044.1466) | ポリシー | Protect |
| コネクタバージョン | 8.4.4.30419 ダウンロードURLを表示する | 内部IP | 1 |
| インストール日 | 2025-02- | 外部IP | 5 |
| コネクタのGUID | 07ff74c3- 33d | 最新の確認日時 | 2 |
| プロセッサID | 6a50b8d1 | BP署名バージョン | な |
| BP署名の最終更新 | なし | Cisco Secure Client ID | なし |

イベント デバイストラジェクトリ 診断 変更の表示

6 隔離の停止 スキャン... 診断 グループへの移動... コネクタのアンインストール 削除

⑦任意でコメントを記載し、「開始」をクリックします。



参考

下記の症状がみられる場合、パソコンがウィルスに感染している場合があります。

1. デスクトップに怪しい広告が表示される
2. 急に別のサイトが表示される
3. ブラウザーを開いた時、トップページが変わっている
4. ネット速度が遅く、頻繁に通信が切れる
5. お気に入りやツールバーなど、見覚えのないものが登録されている
6. 画面上に課金を要求するメッセージが表示される
7. 見覚えのない宛先からメールが届く
8. 相手に自分を騙るメールが届いている
9. パソコンが急に再起動する
10. パソコンの動作が極端に重くなった
11. アプリケーションが急に落ちる
12. 画面がフリーズする

※9～12はパソコン本体のトラブルでも発生する場合があります。

主な感染経路

インターネットサイトからの感染

Webブラウザー(インターネットを表示するソフト)の脆弱性を利用した感染方法が増加してきており、ホームページを閲覧するだけでウィルスに感染する場合があります。

電子メールの添付ファイル

電子メールの添付されているファイルを実行してしまうと、ウィルスに感染することがあります。感染してしまった場合、本人情報や取引先の情報が流失していくまい、本人に成りましたメールが多数送信されるケースが発生してしまい、被害が増加しています。不明な送信元だけでなく、送信元が社内や取引先の相手でも注意が必要です。

電子メールのHTMLスクリプト

電子メールの形式がHTMLメールの場合、ウィルスを送信されてしまうことがあります。HTMLメールはホームページ同じ仕組みでウィルスを侵入させておくことができます。ご利用のメールソフトで、HTMLメールのスクリプトを自動的に実行する設定となっている場合、電子メールを表示しただけでウィルスに感染する場合があります。

マクロプログラムの実行

マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染するタイプのウィルスがあります。マクロウィルスに感染したファイルを開いてしまうと、ウィルスが実行されて、自己増殖などの活動が開始されます。

USBメモリからの感染

多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウィルスがあります。

Cisco Secure Endpoint 管理コンソールにアクセスし、ネットワークからの切り離しと同じ環境にあるすべての端末をSecure Endpointでフルスキャンを実施して、ウイルス等に感染していないかを確認ください。

下記対応を実施しても、事象がおさまらない場合にはお電話でサポートセンターにお問い合わせください。

対応方法

- ①対象のパソコンのSecure Endpointエージェントで、「フルスキャン」を実行します。
- ②スキャンが完了し、ウイルス等が検出された場合にはポップアップで表示されます。サポートセンターに連絡してください。



下記手順に従って、対象のソフトウェアをインストールしてください。

① Secure Endpoint をインストールする方法

p8-41を参照ください。

下記手順に従って、対象のソフトウェアをインストールしてください。
なお、廃棄する古いコンピュータ（パソコン）から、対象のソフトウェアを削除してください。

① Secure Endpoint をインストールする方法

p8-41を参照ください。

下記手順に従って、対象のソフトウェアをインストールしてください。
なお、廃棄する古いコンピュータ（パソコン）から、対象のソフトウェアを削除してください。

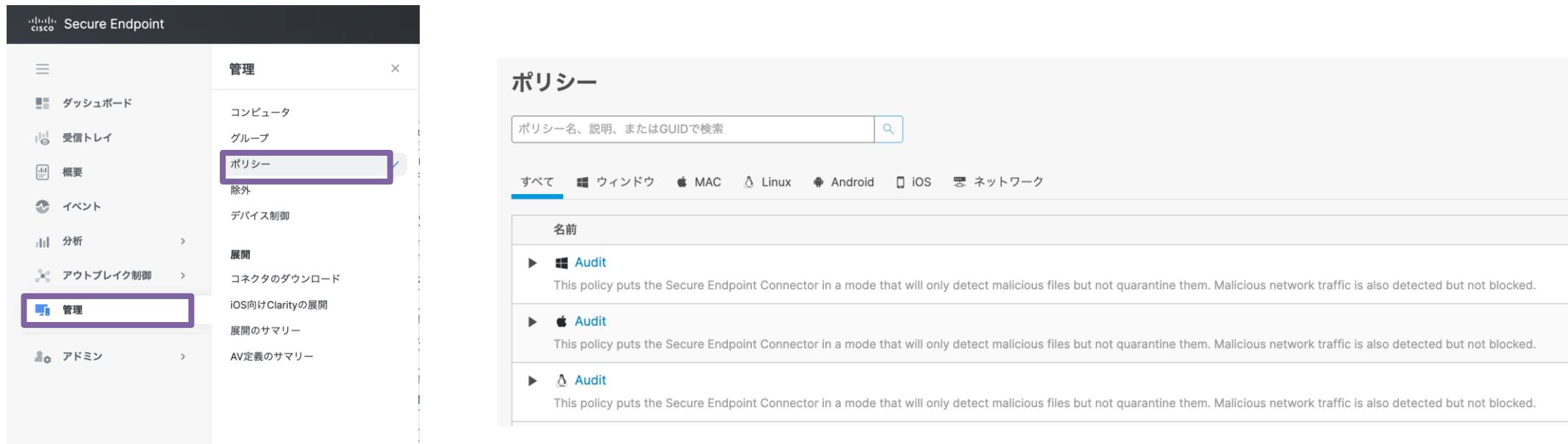
① Secure Endpoint をアンインストールする方法

p42-53を参照ください。

Cisco Secure Endpointでは、検知エンジンごとに動作モードを確認し、変更できます。

検知エンジンのポリシー確認

- ①「管理」→「ポリシー」を選択します。ポリシー一覧から該当のポリシーを選択します。



The screenshot shows the Cisco Secure Endpoint management interface. On the left, the navigation menu is visible with various options like Dashboard, Inbox, Summary, Events, Analysis, Outbreak Control, Management, and Admin. The 'Management' option is selected and highlighted with a purple box. Under 'Management', the 'Policy' option is also highlighted with a purple box. The main content area is titled 'Policy' and displays a search bar and a list of policies. The list includes three entries, each preceded by a small icon representing the operating system:

- ▶ **Audit**
This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but not blocked.
- ▶ **Audit**
This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but not blocked.
- ▶ **Audit**
This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but not blocked.

②それぞれ動作モードを変更できます。各項目で、「検疫」「ブロック」「監査」「無効」がありますが、一部動作の仕組み上選択できないモードがあります。
(例:「ファイル」では検疫・監査のみ)

← ポリシー
ポリシーの編集
Windows

名前 Audit

説明 This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network traffic is also detected but

モードとエンジン

除外 19個の除外セット

プロキシ

アウトブレイク制御

デバイス制御

製品の更新

詳細設定

判定モード

これらの設定で、疑わしいファイルとネットワークアクティビティにSecure Endpointが応答する方法が制御されます。 [Show policy guidance](#)

ファイル ①

検疫 (選択済) 監査

悪意のあるファイルを報告しますが、他のアクションは実行しません。

ネットワーク ①

ブロック 監査 無効

悪意のあるネットワーク接続を報告しますが、他のアクションは実行しません。

悪意のあるアクティビティからの保護 ①

検疫 ブロック 監査 無効

ランサムウェアのようなプロセスを報告しますが、他のアクションは実行しません。

システムプロセス保護 ①

保護 監査 無効

重要なオペレーティングシステムプロセスの悪意のある改ざんの可能性を報告しますが、他のアクションは実行しません。

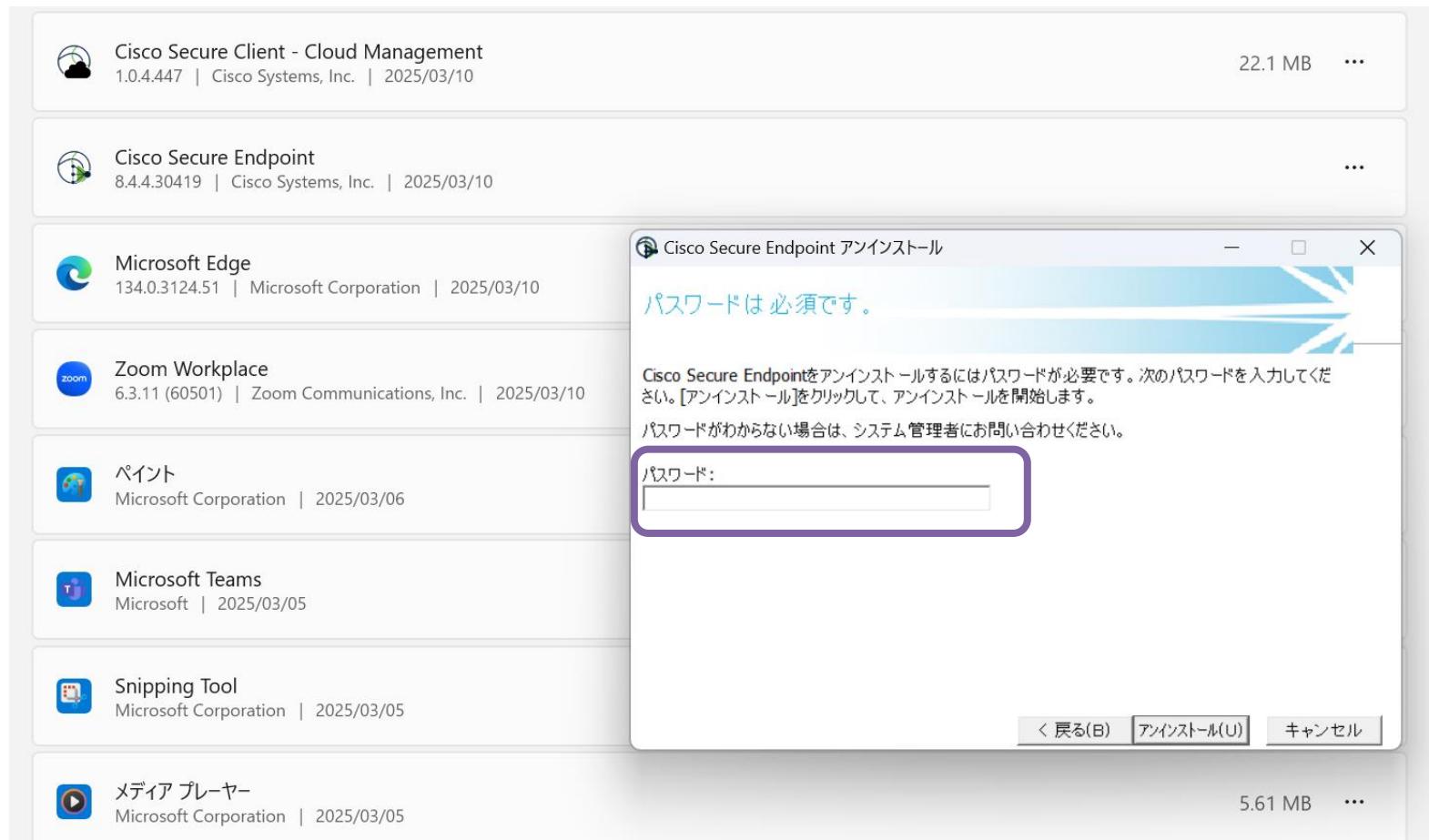
スクリプト保護 ①

検疫 監査 無効

悪意のあるスクリプトが実行された場合に報告しますが、他のアクションは実行しません。

Cisco Secure Endpoint (Windows) にはポリシーでアンインストール時にパスワード入力を必須とし、エンドユーザによってアンインストールできないように制限を設けることが可能です。

コネクタ保護の有効化を実施すると、以下のようにアンインストール時にパスワードの入力画面が表示されます。
具体的な設定手順は次項を参照ください。



アインインストール時のパスワードロック方法

①Secure Endpoint管理コンソールを開き、ログインします。

Secure Endpoint管理コンソール：<https://console.apjc.amp.cisco.com>

The screenshot shows the Cisco Secure Endpoint management console interface. A purple circle with the number '1' is overlaid on the top-left corner of the browser window. The main dashboard includes a sidebar with navigation links like 'ダッシュボード', '受信トレイ', '概要', 'イベント', '分析', 'アウトブレイク制御', '管理', and 'アドミン'. The central area displays the 'ダッシュボード' (Dashboard) with sections for 'はじめに' (Getting Started), 'Secure Endpointコネクタの導入' (Introduction to Secure Endpoint Connectors), and 'デモデータ' (Demo Data). On the right side, there is a 'Cisco XDR' integration banner and several cards with PDF links for various threat types: 'WMIPRVSEがエンコードされたPowerShellを起動しました', 'CozyDuke', 'Upatre', 'PlugX', 'CryptoWall', and '抵抗度の実行可能ファイル'.

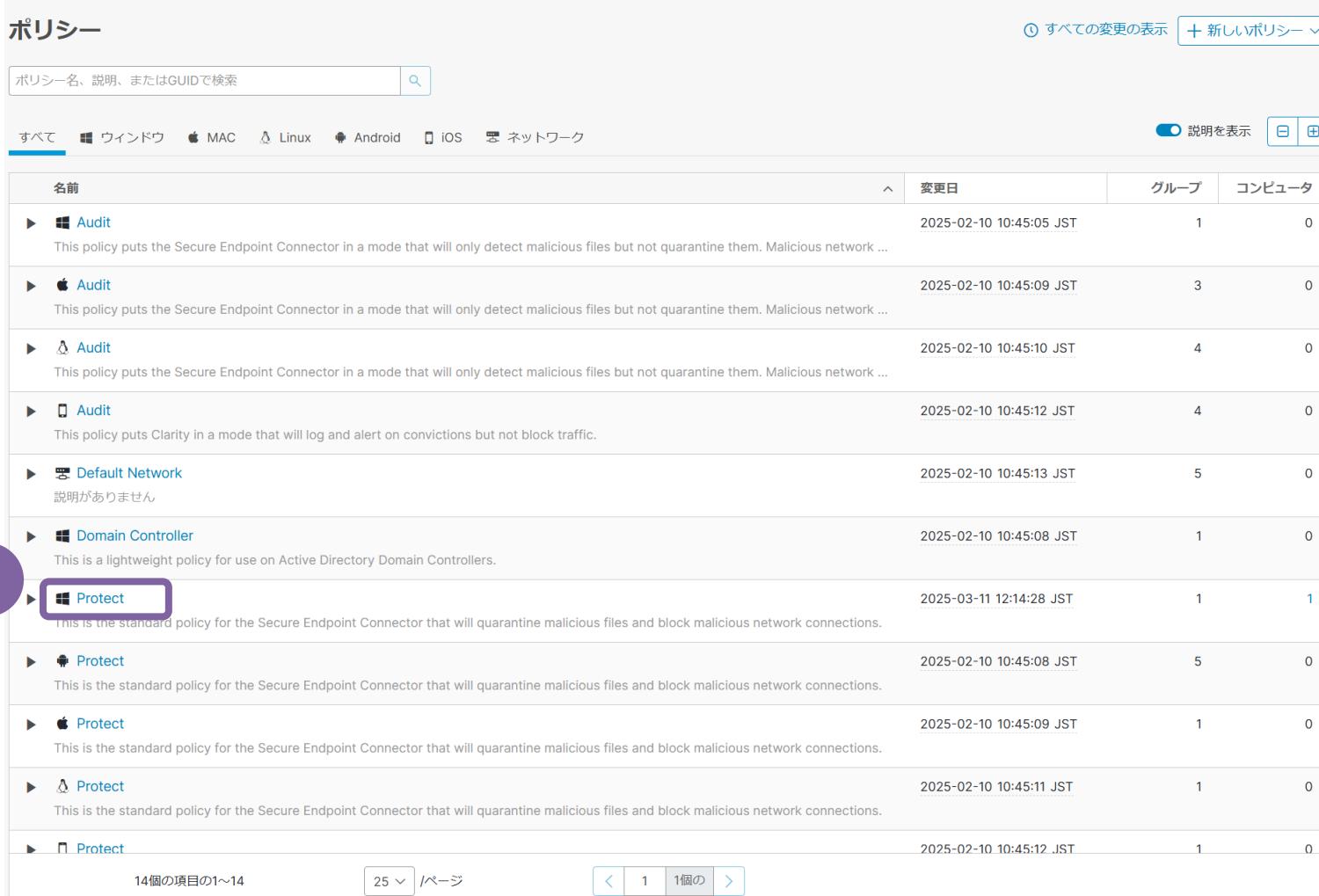
アインインストール時のパスワードロック方法（続き）

- ②左メニュー内から「管理」をクリックします。
- ③「ポリシー」をクリックします。

The screenshot shows the Cisco Secure Endpoint web interface. The top navigation bar includes the Cisco logo, the title 'Secure Endpoint', a search bar, and a user icon. The left sidebar has a three-dot menu, followed by several sections: 'ダッシュボード', '受信トレイ' (with a circled '2'), '概要' (with a circled '3'), 'イベント', '分析', 'アウトブレイク制御' (with a circled '2'), and '管理'. The '管理' section is currently selected and expanded, showing sub-options: 'コンピュータ', 'グループ', 'ポリシー' (which is highlighted with a purple rectangle and circled '3'), '除外', 'デバイス制御', 'ホストファイアウォール', '展開' (expanded to show 'コネクタのダウンロード', 'iOS向けClarityの展開', '展開のサマリー', and 'AV定義のサマリー'), and 'アドミン'. The main content area displays '受信トレイのステータス' (0個が要注意, 0が進行中, 0個が解決済み), '隔離された検出' (0/1), and a 'Protect' button.

アインインストール時のパスワードロック方法（続き）

- ④対象 Secure Endpoint が所属するグループが使用しているポリシーの名前をクリックします。
ここでは例として、「Protect」のポリシーを修正をするものとして説明を続けます。



ポリシー

① すべての変更の表示 + 新しいポリシー ▾

ポリシー名、説明、またはGUIDで検索

すべて ウィンドウ MAC Linux Android iOS ネットワーク

説明を表示

| 名前 | 変更日 | グループ | コンピュータ |
|-------------------|-------------------------|------|--------|
| Audit | 2025-02-10 10:45:05 JST | 1 | 0 |
| Audit | 2025-02-10 10:45:09 JST | 3 | 0 |
| Audit | 2025-02-10 10:45:10 JST | 4 | 0 |
| Audit | 2025-02-10 10:45:12 JST | 4 | 0 |
| Default Network | 2025-02-10 10:45:13 JST | 5 | 0 |
| Domain Controller | 2025-02-10 10:45:08 JST | 1 | 0 |
| Protect | 2025-03-11 12:14:28 JST | 1 | 1 |
| Protect | 2025-02-10 10:45:08 JST | 5 | 0 |
| Protect | 2025-02-10 10:45:09 JST | 1 | 0 |
| Protect | 2025-02-10 10:45:11 JST | 1 | 0 |
| Protect | 2025-02-10 10:45:12 JST | 1 | 0 |

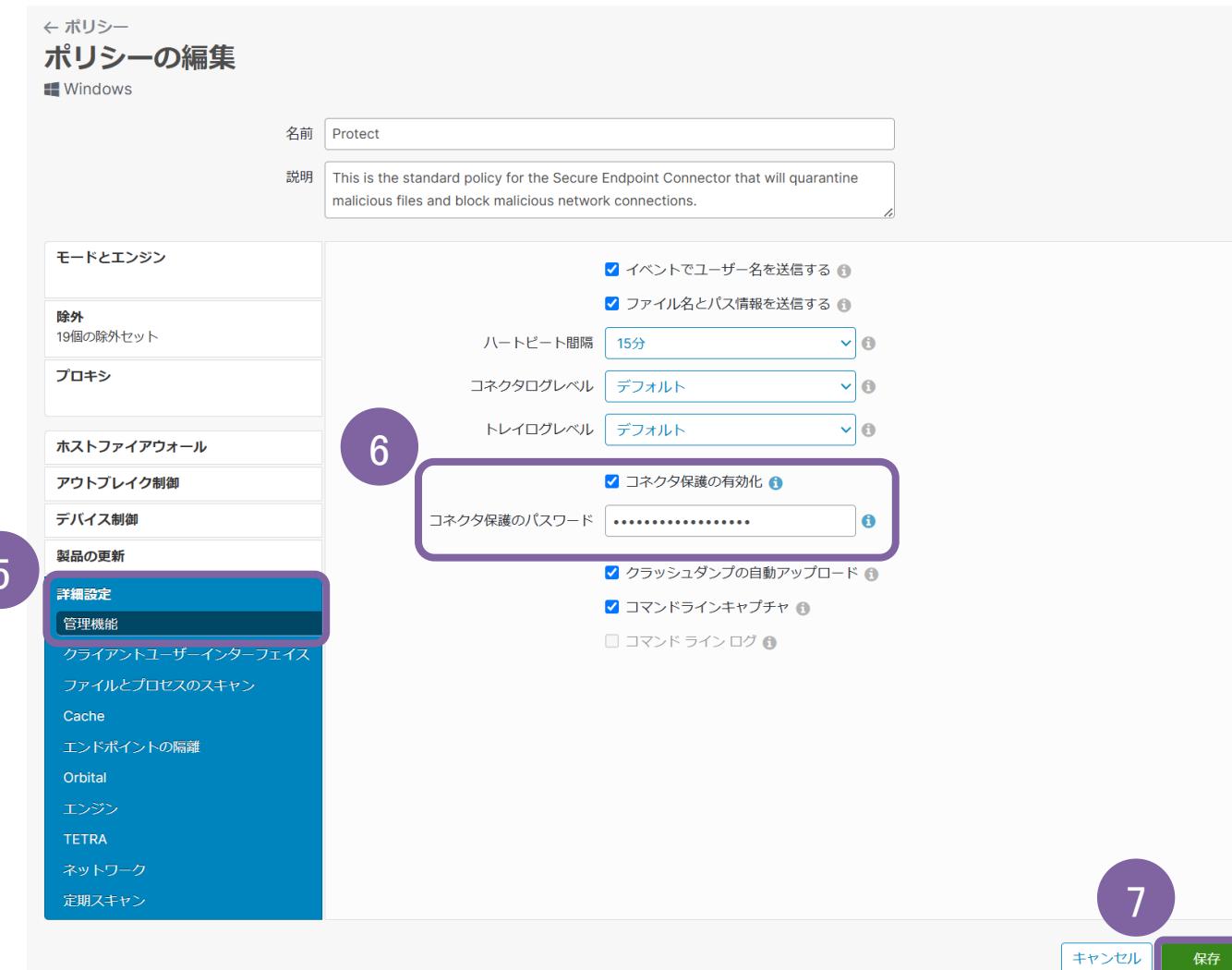
14個の項目の1~14 25 ページ < 1 1個の >

アインインストール時のパスワードロック方法（続き）

⑤「詳細設定」→「管理機能」をクリックします。

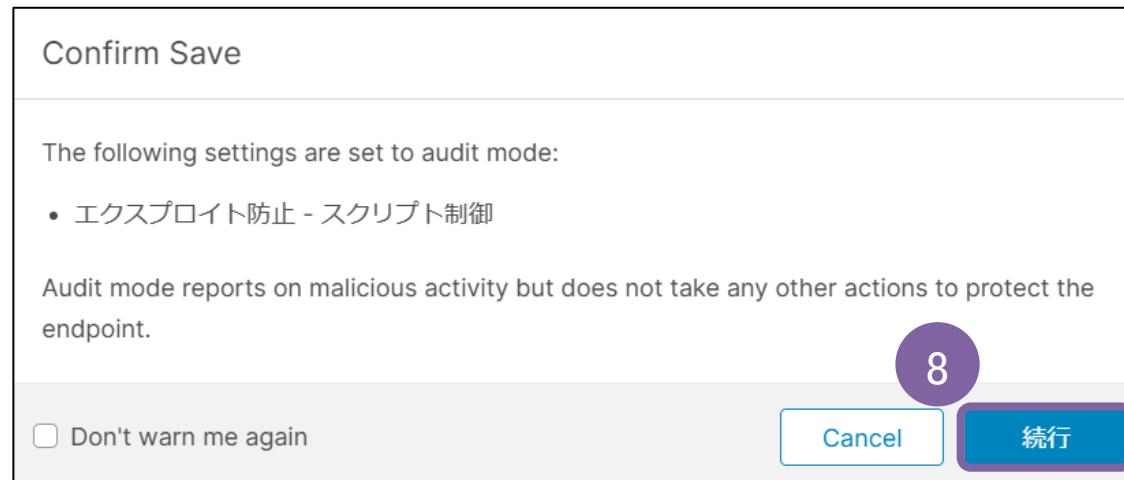
⑥「コネクタ保護の有効化」にチェックを入れて、「コネクタ保護のパスワード」にアインストール時に入力必須なパスワードを設定します。

⑦「保存」をクリック



アインインストール時のパスワードロック方法（続き）

⑧確認画面が表示されたら「続行」をクリックし、設定を完了します。



Cisco Secure Endpoint では、ファイルのハッシュ値 (SHA256) 毎に、ファイルを Malicious/Unknown/Clean と判定しています。しかしながら、お客様が正規の方法で取得して、マルウェアでないと考えられるファイルが Cisco Secure Endpoint で誤検知として Malicious 判定されているケース (False Positive) は稀にございます。

また、逆に、デバイストラジェクトリ上怪しい動作をしているファイルが Clean/Unknown と判定され、マルウェアを逃してしまうケース (False Negative) も考えられ、こちらもお客様にて判断が難しい場合がございます。そういう場合に、「本当に Malware であるか？」を判断するための材料として、Cisco Secure Endpoint 管理コンソールに備わっている Sandbox 機能 (ファイル分析) を使った分析が非常に有用です。

ファイル分析の利用方法

ファイル分析 は、Sandbox 上の小さな端末上で実際に、検体を実行し、その挙動を観察、レポート化さらに、発生した挙動の危険度/信頼度に応じて点数化をするため、お客様が Malware であるかを判断するために非常に有効なツールです。ファイル分析 の最も基本的な使用方法はCisco Secure Endpoint 管理コンソール上からの直接ファイルアップロードになります。以下手順を説明いたします。

- ①Cisco Secure Endpoint 管理コンソールにて分析> ファイル分析 ヘアクセスし、ファイルの送信 ヘアクセスし、ファイルの送信 をクリックします。



ファイル分析の利用方法（つづき）

②ファイルの送信 で対象となるファイルを選択し、実行する OS の Image を選択し、Upload を実行します。

ファイル分析のための送信 ×

分析のためにファイルをサーバーに送信しようとしています。分析が完了すると、電子メールで通知されます。ファイルアップロードの上限は20 MBです

サポートされているファイルタイプ:
.EXE、.DLL、.JAR、.SWF、.PDF、.RTF、.DOC(X)、.XLS(X)、.PPT(X)、.ZIP、.VBN、.SEP

利用可能な送信: 200 1日あたりの送信, 200 残り

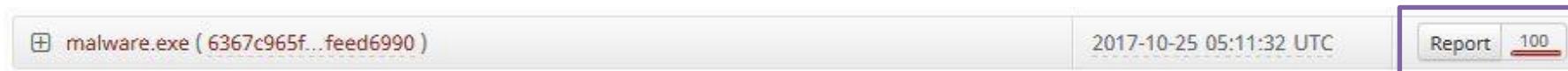
送信するファイル: 参照

分析用のVMイメージ:

キャンセル ▲ アップロード

ファイル分析の利用方法（つづき）

③分析の状況は、分析 > ファイル分析 で確認可能です。分析が完了するまで Pending と表示されておりますが、一定時間（5分程度）が経過すると、Report と点数が以下の通り、表示されます。



④Report をクリックすると、実行結果の詳細となるレポートが表示されます。

こちらの例では、TOR のノードに対して DNS の名前解決を実行していることから、高い確度で Malware であると判定していることが確認できます。

Behavioral Indicators

Potential TOR Connection

A DNS request was made for a potential TOR node. The Onion Router (TOR) is a web anonymity service. TOR uses a series of routing nodes to tunnel or wrap traffic to hide its origins or destination. Malware often uses TOR to hinder tracking and takedown of their command and control communications.

Severity: 100 Confidence: 100

Categories
Tags

network
network, dns, routing, obfuscation

Query ID

Query Data

3

zsn5qrgtgu4lmpg.tor2web.org

2

zsn5qrgtgu4lmpg.tor2web.org

ファイル分析の利用方法（つづき）

⑤具体的な表示されている内容として、Severity が危険度であり、Confidential は、この イベントが信頼出来る挙動であるかの度合いとなります。Confidentiality が低い挙動 (Behavioral Indicators) は不確かな情報であるということになります。

Sandbox で検体を実行した結果、観察できた様々な挙動に対して、Severity と Confidential を掛け合わせたものの最大値を100で割ったものを点数として表示させており、この例では危険度 100 に対して信頼度も 100 なので、100点(最高点)という意味になり、ほぼ マルウェアで間違いない、という判断をすることが出来ます。

隔離された/疑わしいファイルを ファイル分析 へ送る方法

Secure Endpointによって、端末上でマルウェアのファイルが隔離されてしまった場合、隔離されたファイルは無効化された状態で保存されているため、端末からファイルを取得して、Cisco Secure Endpoint管理コンソール からアップロードするには不可能となります（厳密に言えば一旦リストアすれば可能ですが、それでは再び悪影響が出ます）。また、仮にマルウェアの情報源となつたサーバ等から検体を取得できたとしても、マルウェアを直接、業務端末にダウンロードすることは危険が伴い、組織のセキュリティポリシー上好ましくない場合がございます。

その場合、端末からのファイルの収集 (Remote File Fetch)機能を使って端末からリモートでファイルを取得し、それをファイル分析にアップロードする方法が有用です。本項では、分析およびイベント、デバイストラジェクトリからの、検体のリモートでの取得、および、Sandbox へ自動送信を行う方法を説明いたします。

- ①イベントより、Malicious なファイルとして端末から隔離された イベント の詳細情報を表示し、分析 のボタンがあることを確認します。

▼ Demo_AMP_Threat_Auditがekjrngrker.exeをW32.File.MalParentとして検出しました

| ファイルの検出 | 検出 | W32.File.MalParent |
|---------|--------------------|--|
| コネクタの詳細 | MITRE ATT&CK | 戦術 TA0002: Execution TA0011: Command and Control TA0042: Res |
| コメント | | 技術 T1105: Ingress Tool Transfer T1204: User Execution T1204.003: |
| | フィンガープリント(SHA-256) | b1380fd9...df523967 |
| | ファイル名 | ekjrngrker.exe |
| | ファイルパス | C:\ekjrngrker.exe |
| | ファイルサイズ | 3.82 MB |
| | 親 | 使用可能な親SHA/ファイル名がありません。 |

分析

隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

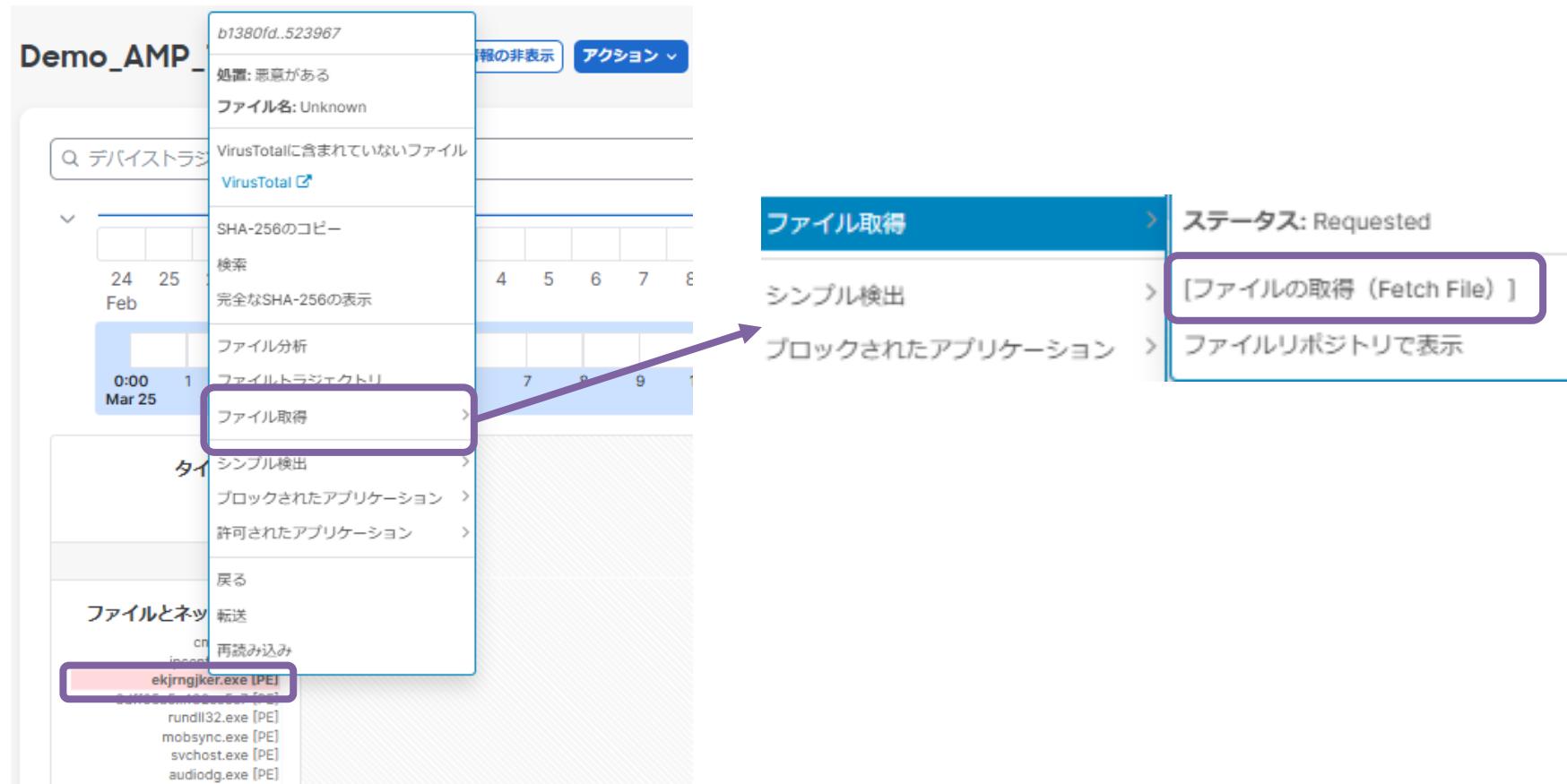
②分析 をクリックし、ファイル分析のための情報（どの端末からファイルを取得するのか、どの種類の OS で実行するのか）を入力して、取得して分析のために送信 をクリックします。



これにより、ファイルは自動的に端末から収集され、最終的に、ファイル分析 にアップロードされ、Sandbox による分析結果を確認することが可能です。
端末からのファイルの収集 (Remote File Fetch) と、Sandbox での実行時間のため、少々時間がかかります。特に、端末がネットワークに接続していないタイミングでは対象のファイルが取得出来ない場合がございます。

隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

③また、隔離されてはいなくても、疑わしいファイルが デバイストラジェクトリ 上にある場合に、直接管理者が取得することを避けたい場合は、デバイストラジェクトリ上から ファイルの取得 にて クラウド ハップロードすることが可能です。デバイストラジェクトリ の該当ファイルもしくは ハッシュ値を右クリックして ファイルの取得 (Fetch File) を実行します。



隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

- ④ 取得したファイルはファイル分析に自動で送信されないため、一定時間経過後に、分析 -> ファイルリポジトリで該当ファイルがアップロードされたことを確認し、分析をクリックすれば、Sandboxで分析することが可能です。

The screenshot shows the 'File Repository' interface. At the top, there are search and filter options. Below that, a table lists files with columns for Status, Requester, Date, and Actions. One specific file entry is highlighted:

| ファイル | ステータス | リクエスト作成者 | 日付 | アクション |
|--|-------|--------------|-------------------------|-------|
| 3372c1edab46837f1e973164fa2d726c5c5e17bcb888828ccd7c4dfcc234a370 | 要求済み | 自動化されているア... | 2025-03-25 19:36:55 JST | |

At the bottom right of the table, there are three buttons: 'Analysis' (highlighted with a purple oval), 'Download', and 'Delete'.

最後に重要な点ですが、ファイル分析自体は、二段階認証を設定する必要はありませんが、端末からのファイルの収集(Remote File Fetch)を実行するためには、二段階認証を有効にする必要がありますので、あらかじめご設定ください。

実行頻度の低い実行ファイルを自動的にファイル分析へ送る方法

Cisco Secure Endpoint では、低拡散度 と呼ばれる機能があり、ある組織の中であまり実行されていないファイルは Malware の疑いがあるという考え方のもと、組織中 (Business) の一つの端末でしか実行されていないファイルをリストアップし、必要に応じて、ファイル分析へ送付させることができます。拡散度 は デフォルト設定では、該当ファイルがリストアップされるだけであり、ファイル分析 に送付させるためには、設定が必要となります。

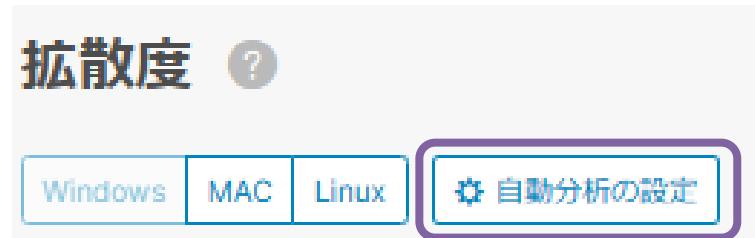
- ①分析 > 拡散度 にアクセスすると、組織の中で1つの端末でしか実行されていないファイルがリストアップされて表示されます。

The screenshot shows the 'Diffusion' (拡散度) page in the Cisco Secure Endpoint interface. At the top, there are tabs for Windows, MAC, and Linux, and a 'Automatic analysis settings' button. Below the tabs is a search bar with placeholder text '検索' (Search). The main area displays a table of detected files:

| ファイル名 | 実行環境 | 操作 | 最終更新日時 |
|---------------------|---|----|-------------------------|
| 25791113...deddb603 | Demo_Command_Line_Arguments_Meterpreter | 分析 | 2025-03-25 19:21:06 JST |
| eba241a9...35feb63a | Demo_Command_Line_Arguments_Meterpreter | 分析 | 2025-03-25 19:21:03 JST |
| 30ffb0cc...f1981e0c | Demo_Command_Line_Arguments_Meterpreter | 分析 | 2025-03-25 19:21:03 JST |
| f396dcd3...d5ec7f30 | Demo_Command_Line_Arguments_Meterpreter | 分析 | 2025-03-25 19:21:03 JST |
| 0cc2c9c2...9e86e32b | Demo_Command_Line_Arguments_Meterpreter | 分析 | 2025-03-25 19:20:52 JST |

実行頻度の低い実行ファイルを自動的にファイル分析へ送る方法（つづき）

②手動で、各ファイルの分析をクリックすると、イベントの画面と同じようにSandboxへアップロードすることができます。今回は、自動的に送付する設定を行いますので、拡散度のページ上部にある自動分析の設定を設定します。



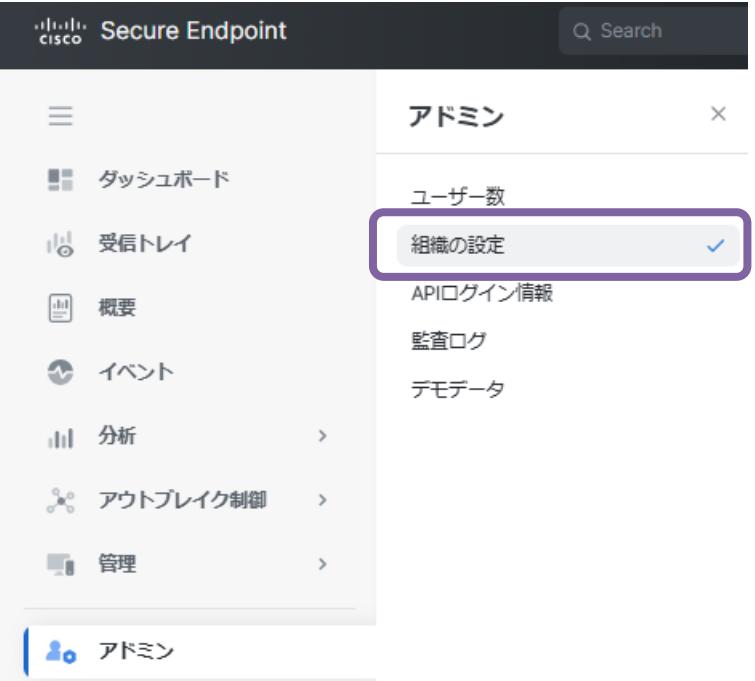
③自動分析の対象となる端末が所属する グループを指定し、
適用をクリックすれば、実行頻度の低いファイルを自動的に
Sandbox 分析にかけることが可能です。



実行頻度の低い実行ファイルを自動的にファイル分析へ送る方法（つづき）

こちらの機能の注意点としては2点あります。

- 1日に実行可能な ファイル分析 の合計カウント数に追加されることになりますため、数多くファイルが アップロードされる環境では注意が必要です。
- 先ほどと同様、拡散度 からの 自動分析も、端末からのファイルの収集 (Remote File Fetch)を実行するため、二段階認証を有効にする必要があります。有効になっていない場合は、分析 ボタンと 自動分析 ボタンがグレーアウトされて実行できませんので、設定する場合は、事前に設定をお願いします。



The image shows two screenshots illustrating the configuration of file analysis settings.

Screenshot 1: Cisco Secure Endpoint - Organization Settings

This screenshot shows the Cisco Secure Endpoint dashboard with the "Organization" tab selected. A purple box highlights the "Organization Settings" dropdown menu, which is currently set to "User count". Other options in the menu include "API login information", "Audit log", and "Demodata".

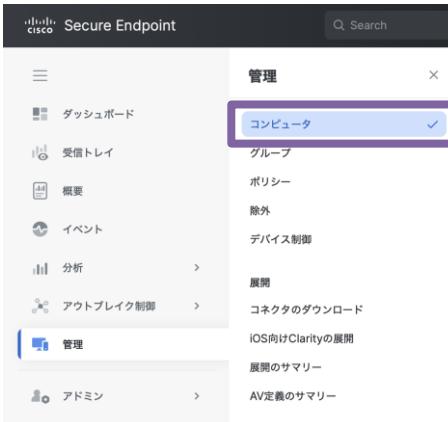
Screenshot 2: Secure Malware Analytics API

This screenshot shows the "Secure Malware Analytics API" configuration page. It displays the current API key and a progress bar for daily file uploads. The progress bar shows 80% (160 / 200) completed. A purple box highlights the message "Available transfers: 200 per day, 200 left" and the "Windows 7 x64" VM selection dropdown. A green button at the bottom right is labeled "Update transfer settings".

業務上必要なファイル・アプリケーションが検知・隔離されてしまい、業務に影響が出た場合、取り急ぎの対処として、対象の実行ファイルをSecure Endpointの検査対象から除外するように、許可リスト(ホワイトリスト)へ登録いただく方法がございます。

1. すでに業務上必要なファイル・アプリケーションが検知・隔離されてしまった場合

- ①意図しないファイル隔離が発生した端末を探します。管理 > コンピュータ を選択したのち、対象の端末を探してください。



- ②端末情報を展開すると、デバイストラジェクトリというリンクが表示されるので、それをクリックします。

The screenshot shows the detailed information for a specific endpoint named 'Demo_SFEicar' belonging to the 'Audit' group. The table contains the following data:

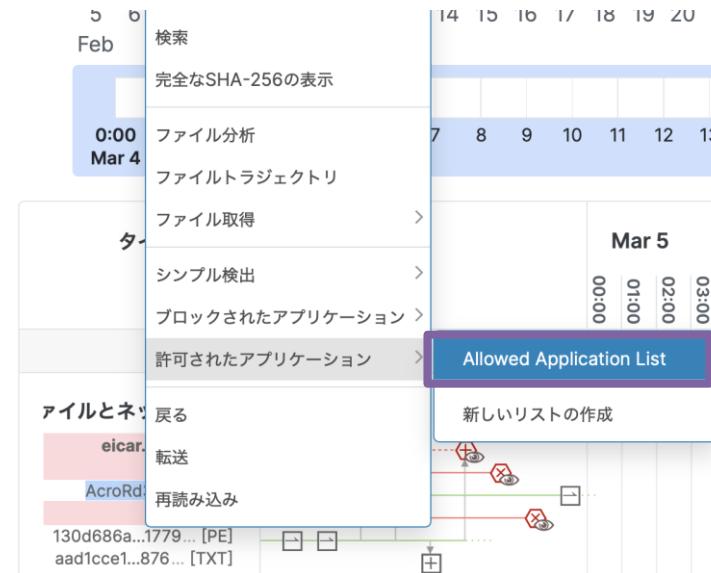
| ホスト名 | Demo_SFEicar | グループ | Audit |
|---------------|--|------------------------|-------------------------|
| オペレーティング システム | Windows 10 (ビルト 19043.1266) | ポリシー | Audit |
| コネクタバージョン | 8.4.4.30419 ↓ ダウンロードURLを表示する | 内部IP | 63.85.183.224 |
| インストール日 | 2025-02-03 00:37:39 UTC | 外部IP | 222.176.197.7 |
| コネクタのGUID | 36b6891b-e248-4462-8dc8-7f2eff09f190 | 最新の確認日時 | 2025-03-05 00:37:39 UTC |
| プロセッサID | 51034db9726ae8f | BP署名バージョン | なし |
| BP署名の最終更新 | なし | Cisco Secure Client ID | なし |

At the bottom of the table, there are several buttons: 「イベント」, 「デバイストラジェクトリ」 (which is highlighted with a purple box), 「診断」, and 「変更の表示」. Below the table is a row of smaller buttons: 「スキャン...」, 「診断...」, 「グループへの移動...」, 「コネクタのアンインストール」, and 「削除」.

1. すでに業務上必要なファイル・アプリケーションが検知・隔離されてしまった場合（つづき）

③該当端末でのトラジェクトリ情報が表示されたら、許可されたアプリケーションに登録したいファイルを右クリックします。

※本ドキュメントの例では、AcroRd32exeを対象のファイルと想定して記述します。



④サブメニューが表示されたらAllowed Application List を選択します。レ点が表示されていれば許可リスト（ホワイトリスト）への登録が完了です。



2. まだ検知・隔離が発生しておらず、事前に許可リスト(ホワイトリスト)に登録したい場合

①Cisco Secure Endpoint管理コンソールにログインし、アウトブレイク制御 > 許可されたアプリケーションを選択してください。

作成されている許可されたアプリケーション（以下の例ではAllowed Application List）が表示されますので、編集ボタンを押すと、画面右側に追加のウィンドウが表示されます。

The screenshot shows the Cisco Secure Endpoint management interface. On the left, there's a sidebar with icons for Dashboard, Inbox, Summary, Events, Analysis, and Outbreak Control. The Outbreak Control icon is selected. The main area has a title 'アウトブレイク制御' (Outbreak Control) with sub-options like 'カスタム検出' (Custom Detection), 'Simple', 'Advanced', and 'Android'. Below that is another section titled 'アプリケーション制御' (Application Control) with 'プロックされたアプリケーション' (Blocked Applications) and '許可されたアプリケーション' (Allowed Applications). A purple box highlights the 'Allowed Applications' tab, which is checked. At the bottom right of this panel is a blue '作成' (Create) button.

Allowed Application List
0個のファイル Masashi Ikuse • 2025-02-17 06:29:20 UTCによって作成されました
ポリシーで使用されている: Audit, Audit, Audit, Domain Controller, Protect, Protect, Protect, Server, Triage, Triage
グループで使用されている: Audit, docopura, Domain Controller, Protect, Server, Triage

変更の表示 **編集** **削除...**

②まだ検知・隔離が発生しておらず、事前に許可リスト(ホワイトリスト)に登録したい場合

②ここに、任意のファイル(もしくはファイルハッシュ値)を追加していくことができます。

Allowed Application List

更新名

SHA-256の追加 ファイルのアップロード

SHA-256のセットのアップロード

リストに追加するファイルをアップロードします(上限は20 MB)

ファイル 選択されているファイルなし 参照

注

▲ アップロード

含まれているファイル

このリストにファイルが追加されていません



③許可リスト登録後、登録されているファイル数が増加しているのが確認できます。以上で対象ファイルの許可リストへの登録は完了です。

作成

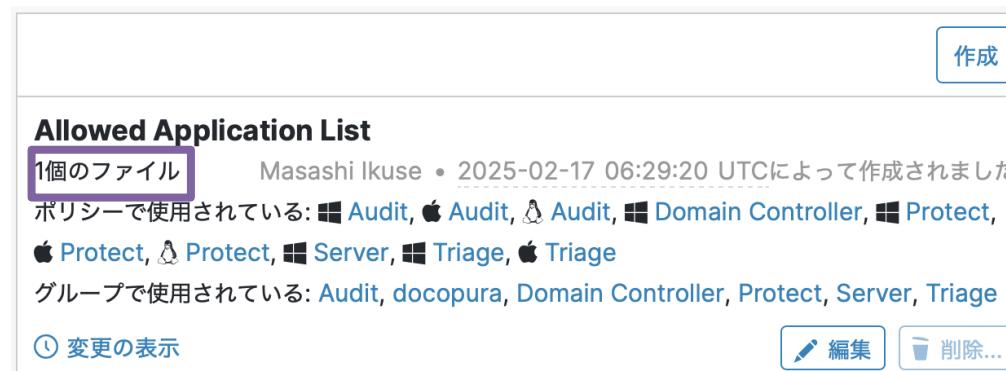
Allowed Application List

1個のファイル Masashi Ikuse • 2025-02-17 06:29:20 UTCによって作成されました

ポリシーで使用されている: Audit, Audit, Audit, Domain Controller, Protect, Protect, Protect, Protect, Server, Triage, Triage

グループで使用されている: Audit, docopura, Domain Controller, Protect, Server, Triage

① 変更の表示 編集 削除...



業務上必要なファイル・アプリケーションが検知・隔離されてしまい、業務に影響が出たトラブルに直面された場合の取り急ぎの対処として、対象の実行ファイルを復元する方法がございます。

隔離されたファイルの復元方法

- ①Cisco Secure Endpoint管理コンソールにログイン後、以下の画面にて隔離されたイベントを探します。
※イベント のタブより、フィルタ > イベントタイプ 「隔離された脅威」でフィルタします

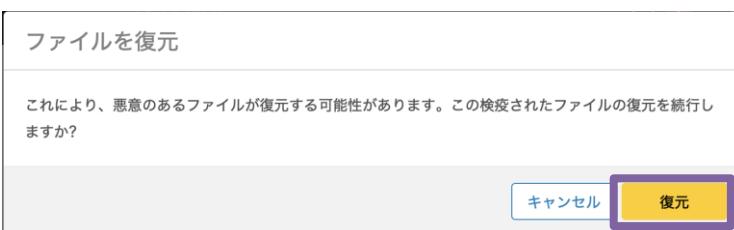
The screenshot shows the 'Events' page of the Cisco Secure Endpoint management console. A filter dialog is open, titled '▼ フィルタ: (新規) ?'. The 'Event Type' dropdown is set to '隔離された脅威' (Quarantine Threat). Other filter options include '潜在的なランサムウェア' (Potential Ransomware), '隔離ステータス' (Quarantine Status), and '隔離の失敗' (Quarantine Failure). Below these, a list of event details is shown for three entries: 'Demo_Qak', 'Demo_Qak', and 'Demo_Upa'. Each entry has a small icon and a list of event types: '隔離された項目が復元されました' (Item quarantined was restored), '隔離の復元に失敗しました' (Restore failed), '隔離の復元が要求されました' (Restore requested), and '隔離リクエストの配信に失敗しました' (Delivery of quarantine request failed).

隔離されたファイルの復元方法（つづき）

②該当の隔離ファイルをクリックし、「ファイルを復元」のボタンをクリックします。



③警告画面が表示されますので確認の上、「復元」のボタンをクリックします。



④対象の端末にて、隔離されたファイルが復元されたことが確認できれば完了です。

ファイルの復元に失敗するようであれば、まずは以下の点をご確認ください。

- ・ 対象の端末が正常に起動していること
- ・ 対象の端末にてSecure Endpointが正常に動作していること

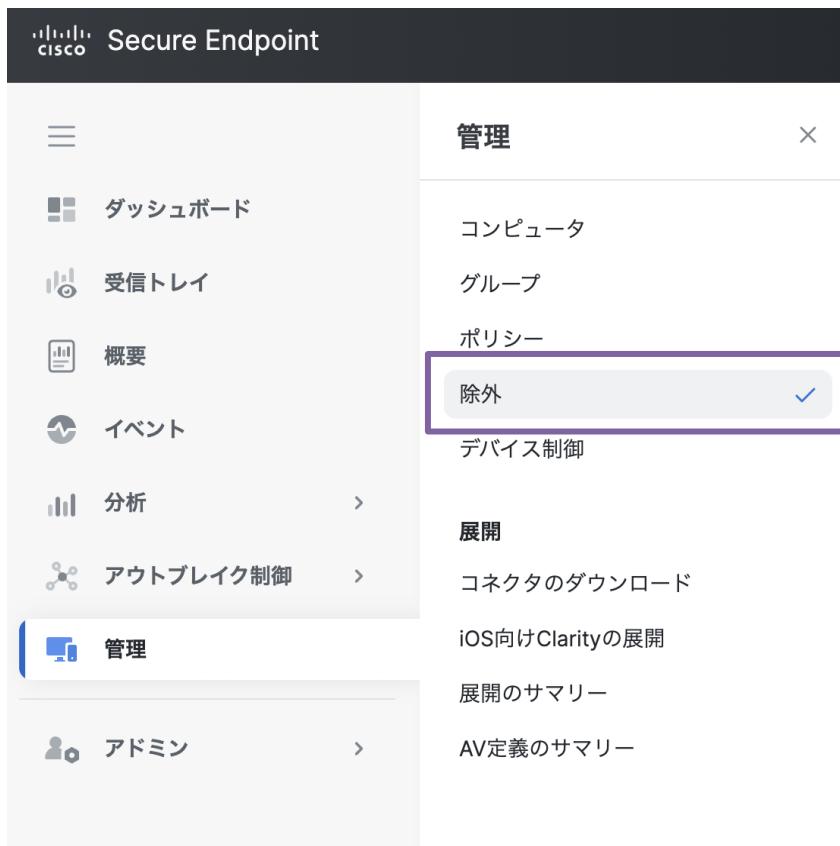
上記に問題がなければ、サポート窓口にお問い合わせください。

以下の理由により、PCの動作が重くなったように感じる場合があります。

- ・ ファイルが大量に存在するようなディレクトリをスキャンしてしまい、端末のリソース(CPU/メモリ等)が大量に消費されている
- ・ 他社アンチウィルス製品との競合が発生してしまっている

対処方法

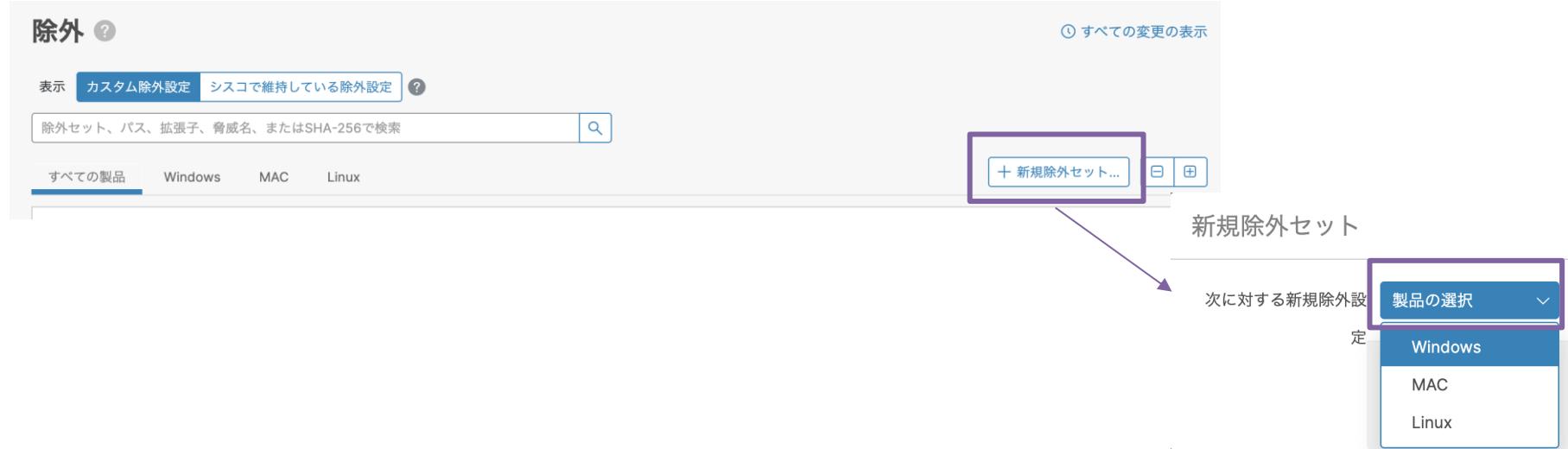
①Cisco Secure Endpoint管理コンソールにログインし、管理 > 除外を選択してください。



対処方法（つづき）

②除外の一覧が表示されますので、以下の手順で「新規の除外セット」を作成します。

「+新規除外セット...」をクリックします。「製品の選択」から対象のOSを選択します。(本ガイドでは例としてWindowsを選択)

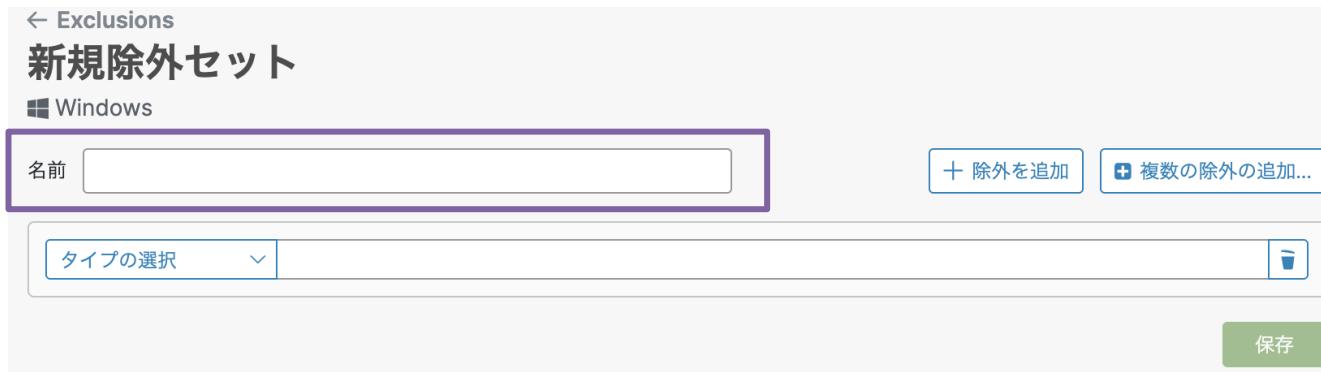


③作成をクリックします



対処方法（つづき）

④任意の名前を入力します。



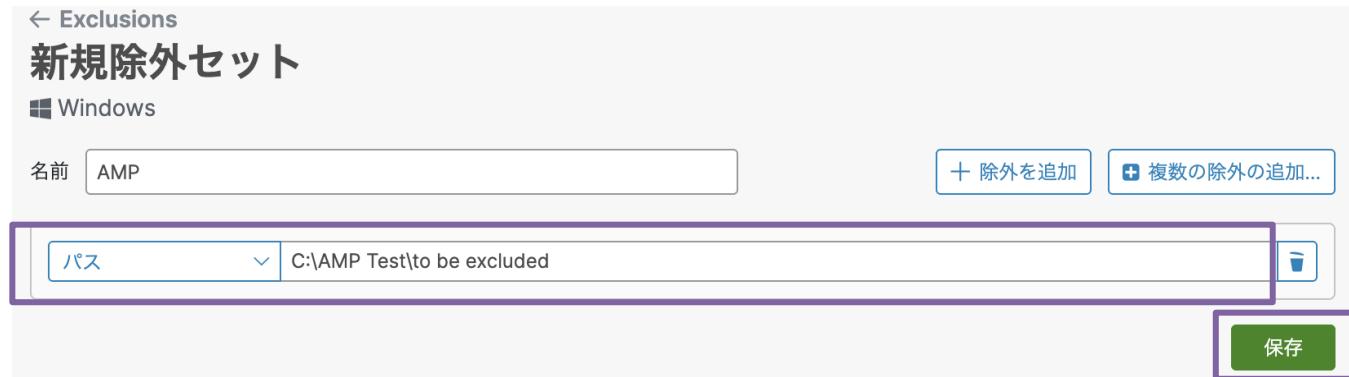
⑤「タイプの選択」から「パス」を選択します。

※例として「C:\¥AMP Test\to be excluded」という「パス」を除外する設定を追加してみます。

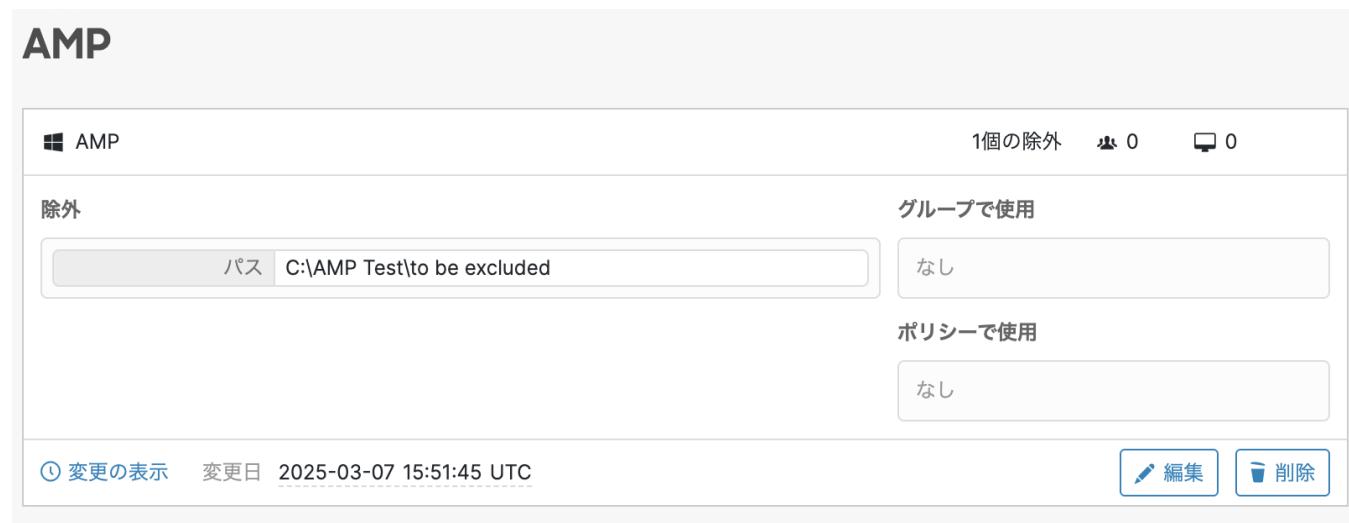


対処方法（つづき）

⑥パスの項目に"C:\AMP Test\to be excluded"を入力し、保存します。

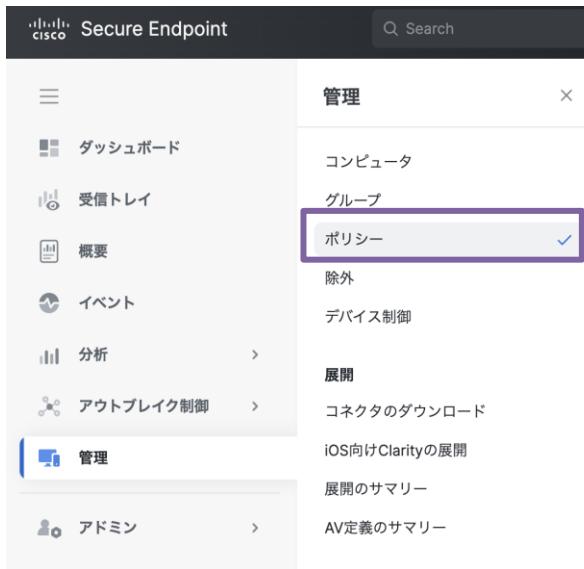


⑦作成したパスが表示されます。



対処方法（つづき）

⑧次に、管理 > ポリシー を選択します。



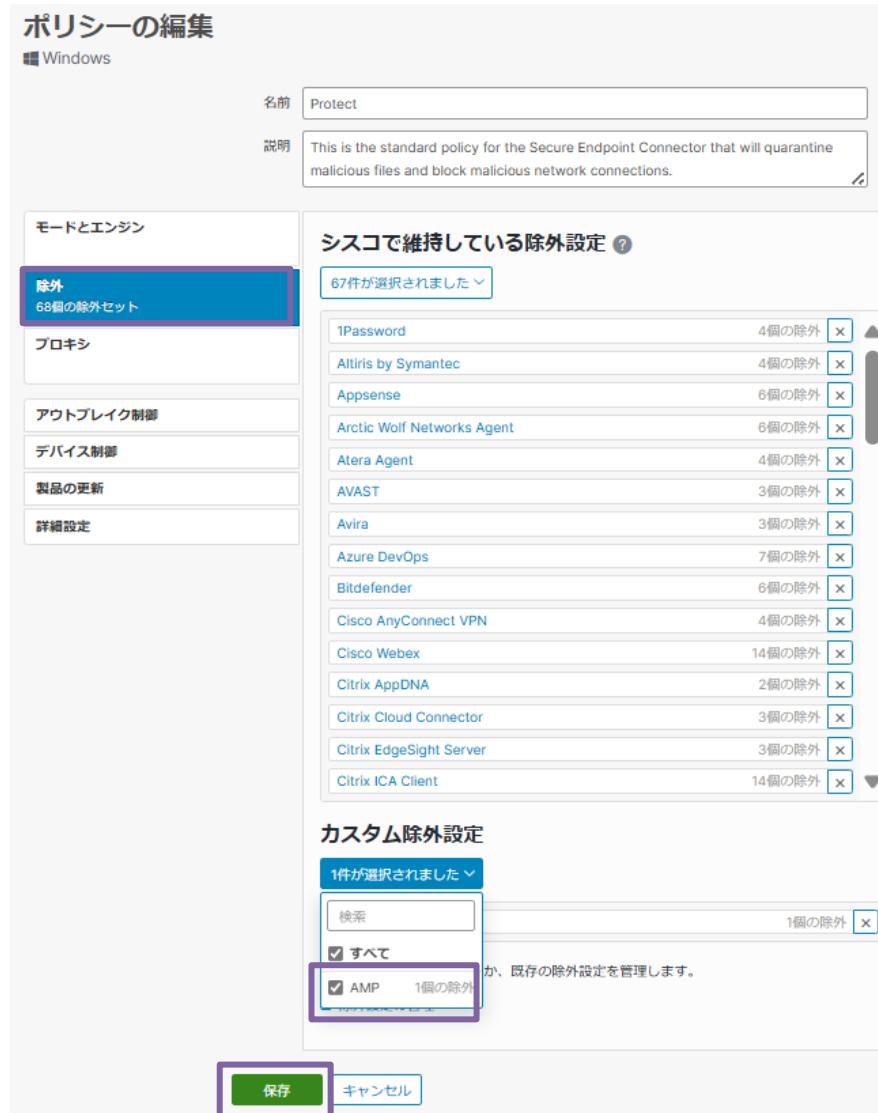
⑨該当の端末に適用されているポリシーを選択します。

※例としてWindowsOSで利用中のポリシー「Protect」で除外設定を追加してみます。

A screenshot of the 'Policy' list page. At the top, there's a search bar and buttons for 'すべて' (All), 'Windows' (selected), 'MAC', 'Linux', 'Android', 'iOS', and 'Network'. There are also buttons for '説明表示' (Show description) and '新規ポリシー' (New policy). The main table lists policies with columns for Name, Change Date, Group, and Computer count. The 'Protect' policy is highlighted with a purple box. The table data is as follows:

対処方法（つづき）

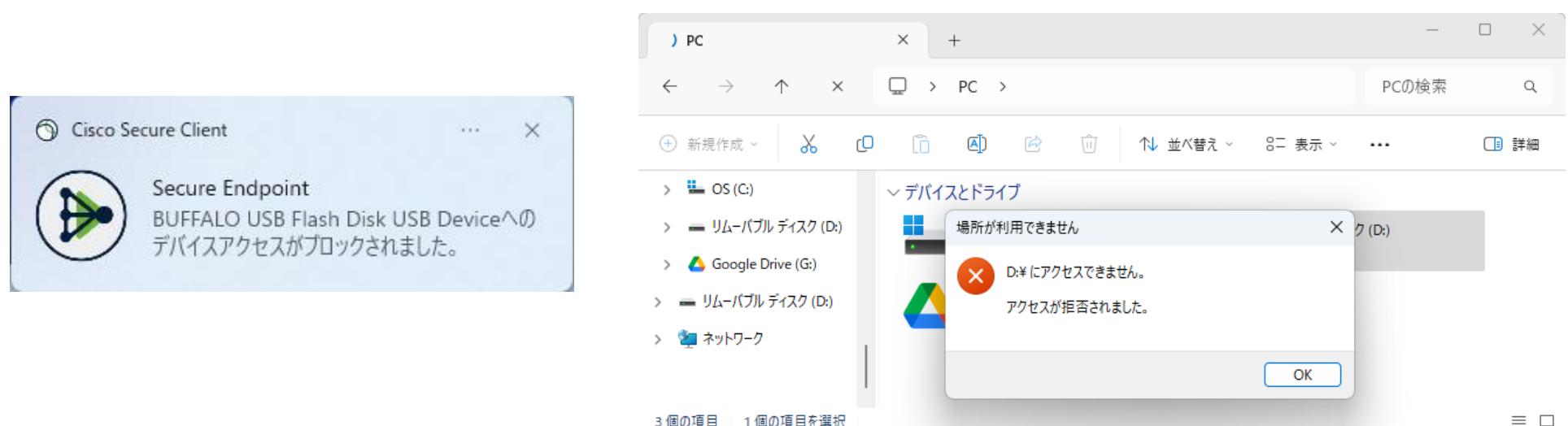
⑩「除外」をクリックし、「カスタム除外設定」のドロップダウンから、作成した除外名を選択して保存します。



Cisco Secure Endpoint (Windows) では、ポリシーで組織内の USB デバイス (Windows ポータブルデバイス (WPD) を含む) の使用状況を表示して制御することができます。

デバイス制御の設定をすると、デバイスを繋いだ際に以下エラーが出るようになります。

※エラー通知をするかどうかは、手順⑧の「エンドポイントユーザに通知」で選択いただけます。
具体的な設定手順は次項を参照ください。



デバイス制御方法

①Secure Endpoint管理コンソールを開き、ログインします。

Secure Endpoint管理コンソール：<https://console.apjc.amp.cisco.com>

The screenshot shows the Cisco Secure Endpoint management console. The left sidebar contains navigation links: ダッシュボード, 受信トレイ, 概要, イベント, 分析, アウトブレイク制御, 管理, and アドミン. The main area is divided into several sections:

- 最新のイベント**: A table showing recent events:

| Event Type | Description | Date |
|-------------------------------|--|-------------------------|
| Scan Completed, No Detections | A scan has completed without detecting anything malicious. | 2025-07-01 06:38:34 UTC |
| Scan Started | An agent has started scanning. | 2025-07-01 06:36:53 UTC |
| Component Download Failure | Component download failed | 2025-07-01 06:14:24 UTC |
| Component Download Failure | Component download failed | 2025-07-01 06:14:18 UTC |
| Component Download Failure | Component download failed | 2025-07-01 06:14:18 UTC |
- 最近のコンピュータ**: A table showing recent computers:

| OS | バージョン | ホスト名 | グループ |
|--------------------|------------------------|--------------------------|---------|
| Windows 11, SP 0.0 | 8.4.5.30483 | ODS-NewZero1 | Protect |
| Windows 11, SP 0.0 | 8.4.4.30419-DEPRECATED | ODS-NewZero2 | Protect |
| macOS 15.5.0 | 1.26.0.1010 | ODS-NewZero5のMacBook Air | Protect |
| 2 | 1 | 0 | 0 |
- 最近の監査ログ**: A table showing audit logs:

| User | Log Type | Log Details | Date |
|--|-----------|------------------------------|-------------------------|
| dokopura_mssp13@west.ntt.co.jp | sso_login | User | 2025-07-02 07:37:12 UTC |
| dokopura_mssp12@west.ntt.co.jp | sso_login | User | 2025-07-02 05:23:18 UTC |
| ODS-NewZero1 | create | Computer | 2025-07-01 02:14:15 UTC |
| a82f10dc-ddcd-44d4-83bb-edb47a884d84-posaas-hook | update | Webhook::WebhookSubscription | 2025-06-28 10:55:45 UTC |
| 605c29be-3f78-43b3-878d-b1ea7879f2e0-posaas-hook | update | Webhook::WebhookSubscription | 2025-06-28 03:41:07 UTC |
- 最近のアウトブレイク制御リスト**: A table showing detection lists:

| リスト名 | 説明 | 最終更新日 | 操作 |
|------------------------------|------------------------------|-------------------------|-------|
| Simple Custom Detection List | Simple Custom Detection List | 2025-02-10 01:35:15 UTC | すべて表示 |
| TEST | TEST | 2025-06-06 07:30:34 UTC | すべて表示 |
- 最近のポリシー**: A table showing policies:

| 名前 | 最終更新日 |
|-----------------|-------------------------|
| Protect | 2025-06-11 01:55:02 UTC |
| Default Network | 2025-02-10 01:35:18 UTC |
| Protect | 2025-02-10 01:35:18 UTC |
| Audit | 2025-02-10 01:35:17 UTC |
| Protect | 2025-02-10 01:35:17 UTC |
- アプリケーション**: A section stating "アプリケーションが見つかりません" (No applications found).
- ライセンス情報**: A section for license information.

デバイス制御方法（続き）

- ②左メニュー内から「管理」をクリックします。
- ③「デバイス制御」をクリックします。

The screenshot shows the Cisco Secure Endpoint management interface. A purple circle labeled '2' highlights the 'Management' button in the left sidebar. Another purple circle labeled '3' highlights the 'Device Control' button in the expanded 'Management' menu.

The main area displays several sections:

- Recent Computers**: Shows a list of recent computer activity. One entry is visible: "as completed without detecting anything malicious. 2025-07-01 06:38:34 UTC".
- Recent Outbreak Control List**: Shows a list of recent outbreak control lists. One entry is visible: "Simple Custom Detection List 2025-02-10 01:35:15 UTC".
- Applications**: Shows a message: "Applicationが見つかりません" (No applications found).
- Recent Outbreak Control**: Shows a list of recent outbreak control entries. Several entries are listed, such as "13@west.ntt.co.jp 2025-07-03 00:33:30 UTC" and "13@west.ntt.co.jp 2025-07-02 09:56:11 UTC".
- Recent Computer Scan**: Shows a list of recent computer scan logs. Several entries are listed, such as "as completed without detecting anything malicious. 2025-07-01 06:38:34 UTC" and "it has started scanning. 2025-07-01 06:36:53 UTC".
- Recent Outbreak Failed**: Shows a list of recent outbreak failed logs. Several entries are listed, such as "outbreak download failed 2025-07-01 06:14:24 UTC" and "outbreak download failed 2025-07-01 06:14:18 UTC".

デバイス制御方法（続き）

④デバイス制御ページが表示されますので、「+新規設定」をクリックします。

The screenshot shows the 'Device Control' section of the Cisco Secure Endpoint interface. On the left, there's a sidebar with navigation links: Dashboard, Inbound Tray, Summary, Events, Analysis, Outbreak Control, Management (which is selected), and Admin. The main area has a search bar and a table listing a single policy named 'test_20250509'. The table columns include Name, Setting Type, Permissions, Rules, Policy, Computer, Group, and Last Updated. A purple circle with the number '4' is overlaid on the '+ New Setting' button in the top right corner of the main content area.

| 名前 | 設定タイプ | 権限 | ルール | ポリシー | コンピュータ | グループ | 最終更新日 |
|---------------|-------------|------|-----|------|--------|------|---|
| test_20250509 | USB大容量ストレージ | ブロック | 1 | 1 | 2 | 1 | 2025-05-09 07:54:06 UTC 更新者: どこプラ管理 NTT西日本 |

デバイス制御方法（続き）

- ⑤「名前」に任意のものを入力します。
- ⑥「説明（任意）」は必要に応じて入力します。
- ⑦「設定タイプの選択」のプルダウンで、設定したいものをクリックします。
※ここでは例として、「USB大容量ストレージ」を選択します。



デバイス制御方法（続き）

⑧「基本ルール」で設定したいものにチェックを入れます。

※ここでは例として、「ブロック」、エンドポイントユーザに通知では「常に保存」を選択します。

※Windows ポータブルデバイス（WPD）の場合、実行制御は現在サポートされておりません。

⑨「保存」をクリックします。



【デバイス制御の権限】

権限を使用して、コネクタが接続された USB大容量ストレージデバイスとエンドポイントとの対話を許可する方法を制御します。

| 権限 | 説明 |
|-----------------|--|
| ブロック (Block) | いかなる方法でも、デバイスへのアクセスをエンドポイントに許可しません。 |
| 読み取り専用 | デバイスからのファイルの読み取りのみをエンドポイントに許可します。ユーザーは引き続き、デバイスからエンドポイントにファイルを手動でコピーし、書き込みまたは実行できることに注意してください。 |
| 読み取りと書き込みのみ | デバイスでのファイルの読み取りと書き込みをエンドポイントに許可します。ユーザーは引き続き、デバイスからエンドポイントにファイルを手動でコピーして実行できることに注意してください。 |
| 読み取り、書き込み、および実行 | デバイスへのフルアクセスをエンドポイントに許可します。このバージョンは、現在実行をサポートしていないため、WPDでは使用できません。 |

※前頁手順⑦プルダウンで「Windows ポータブルデバイス（WPD）」を選択した場合、
以下のように「読み取り、書き込み、および実行」がグレーアウトされ、選択できません。



デバイス制御方法（続き）

⑩「設定が作成されました。」という文字が表示され、ルールの新規作成が完了しました。

10

The screenshot shows the Cisco Secure Endpoint web interface. The top navigation bar includes the Cisco logo, 'Secure Endpoint', a search bar, and various icons. A purple callout box labeled '10' points to the top-left corner of the interface. The main content area has a dark header with the title 'USB利用の制御' and a green success message box containing the text '設定が作成されました。'. Below this, a table lists a single rule: 'すべてのUSB大容量ストレージ' (All USB storage devices) with condition '1' and action 'ブロック' (Block). The bottom of the page displays footer information and a feedback link.

Secure Endpoint

検索

設定が作成されました。

最終更新日： 2025-07-03 02:21:27 UTC 更新者: どこプラ管理 NTT西日本

USB利用の制御 編集

USB無効化の設定

0個のポリシー | ポリシーへの割り当て | 0 | 0

キャンセル 保存

+ ルールの追加 (Add Rule)

| ルール(1/1000) | 条件 | 許可 | エンドポイントユーザに通知 | 最終更新日 |
|-----------------|----|------|---------------|---|
| すべてのUSB大容量ストレージ | 1 | ブロック | 常に保存 | 2025-07-03 02:21:27 UTC 更新者: どこプラ管理 NTT西日本 |

147.161.194.252からの約1時間時間前の最後のログイン
現在のセッションは1分未満時間前に開始されました

この組織のデータは日本でホストされています

© 2025 Cisco Systems, Inc.
サービス契約

フィードバックをお送りください

200

デバイス制御方法（続き）

- ⑪左メニュー内から「管理」をクリックします。
- ⑫「ポリシー」をクリックします。

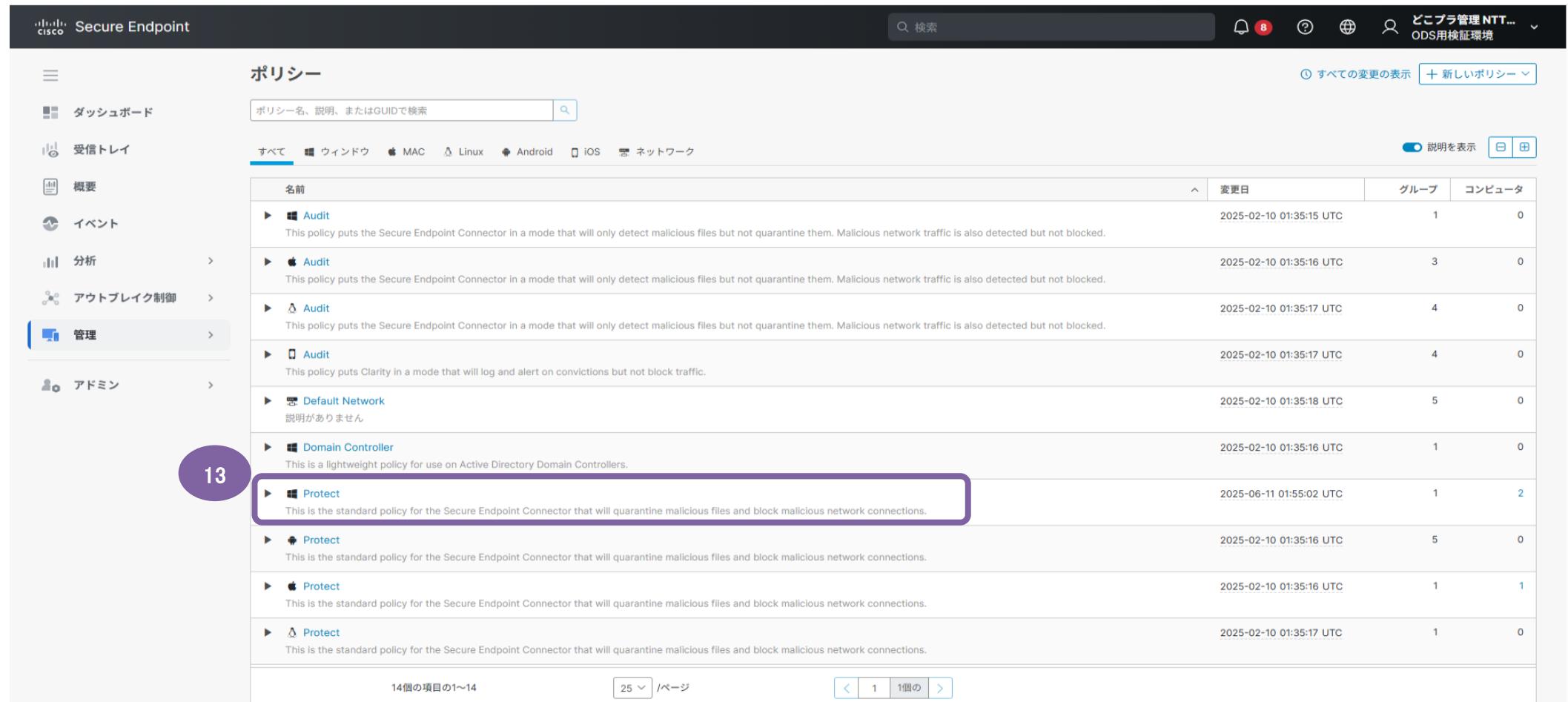
The screenshot shows the Cisco Secure Endpoint management interface. On the left, a sidebar menu is open with several options: ダッシュボード, 受信トレイ, 概要, イベント, 分析, アウトブレイク制御, 管理 (highlighted with a purple box and labeled 11), and アドミン. A secondary menu under '管理' is also open, listing: コンピュータ, グループ, ポリシー (highlighted with a purple box and labeled 12), 除外, and デバイス制御. The main content area displays several sections: 'Recent Computers' (listing three Windows 11 and one macOS 15.5.0 host), 'Recent Outbreak Control Lists' (listing two entries: 'Simple Custom Detection List' and 'TEST'), and an empty 'Applications' section. At the bottom left, there is a URL: <https://console.apjc.amp.cisco.com/policies>.

デバイス制御方法（続き）

⑬対象 Secure Endpoint が所属するグループが使用しているポリシーの名前をクリックします。

ここでは例として、「Protect」のポリシーを修正をするものとして説明を続けます。

※デバイス制御はWindowsのみ設定が可能です。



The screenshot shows the Cisco Secure Endpoint web interface under the 'Policy' tab. On the left, a sidebar lists navigation options: Dashboard, Inbox, Overview, Events, Analysis, Outbreak Control, Management (which is selected), and Admin. A purple circle with the number '13' is placed over the 'Management' link. The main content area displays a table of policies. The 'Protect' policy is highlighted with a purple box and selected, as indicated by the purple border around its row. The table columns include Name, Last Modified, Group, and Computer. The 'Protect' policy was last modified on June 11, 2025, at 01:55:02 UTC, and is associated with 1 group and 2 computers.

| 名前 | 変更日 | グループ | コンピュータ |
|-------------------|-------------------------|------|--------|
| Audit | 2025-02-10 01:35:15 UTC | 1 | 0 |
| Audit | 2025-02-10 01:35:16 UTC | 3 | 0 |
| Audit | 2025-02-10 01:35:17 UTC | 4 | 0 |
| Audit | 2025-02-10 01:35:17 UTC | 4 | 0 |
| Default Network | 2025-02-10 01:35:18 UTC | 5 | 0 |
| Domain Controller | 2025-02-10 01:35:16 UTC | 1 | 0 |
| Protect | 2025-06-11 01:55:02 UTC | 1 | 2 |
| Protect | 2025-02-10 01:35:16 UTC | 5 | 0 |
| Protect | 2025-02-10 01:35:16 UTC | 1 | 1 |
| Protect | 2025-02-10 01:35:17 UTC | 1 | 0 |

デバイス制御方法（続き）

⑭ポリシーの編集画面が開きます。

14

The screenshot shows the Cisco Secure Endpoint web interface. The left sidebar has a purple header '14' and navigation items: ダッシュボード, 受信トレイ, 概要, イベント, 分析, アウトブレイク制御, 管理 (selected), and アドミン. The main area title is 'ポリシーの編集' under 'Windows'. It shows a policy named 'Protect' with the following details:

- 名前:** Protect
- 説明:** This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.

The 'モードとエンジン' section lists '除外' (69個の除外セット) and 'プロキシ'.

The '判定モード' section contains several tabs:

- ファイル**: 検疫 (selected), 監査, 無効. Description: 悪意のあるファイルを削除して報告します.
- ネットワーク**: ブロック (selected), 監査, 無効. Description: 悪意のあるネットワーク接続をブロックして報告します.
- アクティビティからの保護**: 検疫, ブロック, 監査, 無効. Description: 悪意のあるアクティビティからの保護 (ランサムウェアのようなプロセスを終了し、その実行可能ファイルを削除して報告します).
- システムプロセス保護**: 保護 (selected), 監査, 無効. Description: 重要なオペレーティングシステムプロセスの悪意のある改ざんをブロックし、アクティビティを報告します.
- スクリプト保護**: 検疫, 監査, 無効. Description: 悪意のあるスクリプトが実行された場合は、停止、削除して、報告します.
- エクスプロイトの防止**: ブロック (selected), 監査, 無効. Description: 一部のプロセスに対するバイナリコードインジェクション攻撃を報告しますが、他のアクションは実行しません.

At the bottom, there's a link to 'エクスプロイト防止 - スクリプト制御'.

Page footer: https://console.apjc.amp.cisco.com/dashboard

デバイス制御方法（続き）

⑯「デバイス制御」をクリックします。

The screenshot shows the Cisco Secure Endpoint interface. On the left, there's a navigation sidebar with icons for Dashboard, Inbox, Summary, Events, Analysis, Outbreak Control, Management, and Admin. A purple circle with the number 15 highlights the 'Management' section. The main area is titled 'Policy Editor' and shows a 'Protect' policy being edited. The 'Device Control' tab is selected. The interface includes sections for USB storage devices and Windows portable devices, each with a configuration dropdown set to 'なし' (None). The top right corner shows a notification badge with the number 7.

Secure Endpoint

検索

7

どこプラ管理 NTT...
ODS用検証環境

ポリシーの編集

Windows

名前: Protect

説明: This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.

モードとエンジン

除外: 69個の除外セット

プロキシ

USB大容量ストレージ

Configuration: なし

Windowsポータブルデバイス

Configuration: なし

新しい設定を作成するか、既存の設定を管理します。

デバイス制御設定の管理

15

デバイス制御方法（続き）

⑯USB大容量ストレージの「Configuration」で手順⑩で作成したルールを選択します。

The screenshot shows the 'Secure Endpoint' interface with the title 'ポリシーの編集' (Policy Edit) and 'Windows' selected. A purple circle labeled '16' highlights the 'USB大容量ストレージ' (USB Storage Device) section under 'デバイス制御' (Device Control). The 'Configuration' dropdown is set to 'test_20250509'. In the table, there is one rule named 'USB利用の制御' (Control of USB usage), which is checked and set to 'ブロック' (Block). The table also includes columns for '件数' (Count), '許可' (Allow), and 'エンドポイント通知' (Endpoint Notification). Below this, the 'Windowsポータブルデバイス' (Windows Portable Device) section is shown with a configuration dropdown set to 'なし' (None).

デバイス制御方法（続き）

（Windowsポータブルデバイスの設定も行う場合）

- ⑯ Windowsポータブルデバイスの「Configuration」で設定したいルールを選択します。

The screenshot shows the Cisco Secure Endpoint web interface. On the left, there's a navigation sidebar with options like Dashboard, Inbox, Summary, Events, Analysis, Outbreak Control, Management, and Admin. The 'Management' section is currently selected. In the main content area, the user is editing a policy named 'Protect'. The 'Device Control' section is open, specifically the 'USB Large Capacity Storage' tab. It shows a table with one rule: 'すべてのUSB大容量ストレージ' (All USB large capacity storage) is blocked ('ブロック') and always saved ('常に保存'). Below this, the 'Windows Portable Device' section is visible, showing configuration options for 'なし' (None) and 'Windows Portable Device Control' (which is selected). A purple circle with the number '17' is overlaid on the bottom-left corner of the screenshot.

デバイス制御方法（続き）

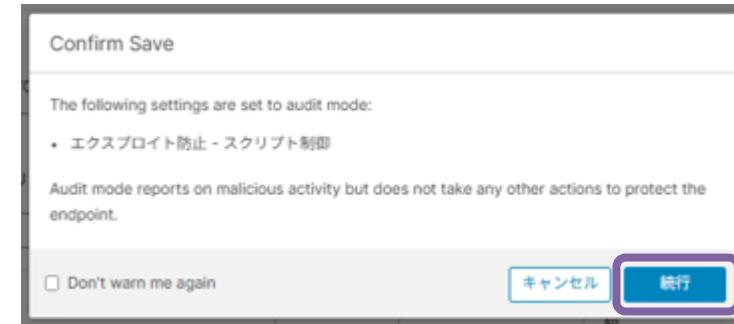
⑯「保存」をクリックします。

The screenshot shows the Cisco Secure Endpoint web interface. The left sidebar includes links for Dashboard, Inbound Mailbox, Summary, Events, Analysis, Outbreak Control, Management, and Admin. The Management link is currently selected. The main content area displays two sections: 'USB大容量ストレージ' (USB Storage) and 'Windowsポータブルデバイス' (Windows Portable Device). Both sections show a table with one row, indicating a rule that blocks access to all USB storage devices. The 'USB大容量ストレージ' section has a configuration dropdown set to 'USB利用の制御' and a '設定の管理' (Manage Settings) button. The 'Windowsポータブルデバイス' section also has a configuration dropdown set to 'Windowsポータブルデバイスの制御' and a '設定の管理' button. At the bottom, there is a note about creating new settings or managing existing ones, and a link to 'デバイス制御設定の管理' (Manage Device Control Settings). A purple circle with the number '18' is overlaid on the bottom left, and a green '保存' (Save) button is highlighted with a red border at the bottom center.

デバイス制御方法（続き）

⑯以下のポップアップが表示されますので、「続行」をクリックします。

※「監査モードでは悪意のある活動を報告しますが、エンドポイントを保護するためのその他の措置は一切行いません。」という確認です。



デバイス制御方法（続き）

②以下画面が表示されますので、これにて設定完了です。

The screenshot shows the Cisco Secure Endpoint management interface. A purple circle with the number '20' is overlaid on the top center of the screen. A blue notification bar at the top right displays the message "ポリシー"Protect"が正常に更新されました。" (Policy "Protect" was successfully updated). The main area is titled "ポリシー" (Policy) and lists various policies with details like name, type, and last modified date. The "Audit" policy is listed twice, and the "Protect" policy is listed four times.

| 名前 | 変更日 | グループ | コンピュータ |
|-----------------------|-------------------------|------|--------|
| ▶ Audit | 2025-02-10 01:35:15 UTC | 1 | 0 |
| ▶ Apple Audit | 2025-02-10 01:35:16 UTC | 3 | 0 |
| ▶ ⚙️ Audit | 2025-02-10 01:35:17 UTC | 4 | 0 |
| ▶ 📁 Audit | 2025-02-10 01:35:17 UTC | 4 | 0 |
| ▶ 🌐 Default Network | 2025-02-10 01:35:18 UTC | 5 | 0 |
| ▶ 🏢 Domain Controller | 2025-02-10 01:35:18 UTC | 1 | 0 |
| ▶ 🛡️ Protect | 2025-07-03 02:48:42 UTC | 1 | 2 |
| ▶ 🍏 Protect | 2025-02-10 01:35:16 UTC | 5 | 0 |
| ▶ 🍏 Protect | 2025-02-10 01:35:16 UTC | 1 | 1 |
| ▶ ⚙️ Protect | 2025-02-10 01:35:17 UTC | 1 | 0 |
| ▶ 📁 Protect | 2025-02-10 01:35:18 UTC | 1 | 0 |

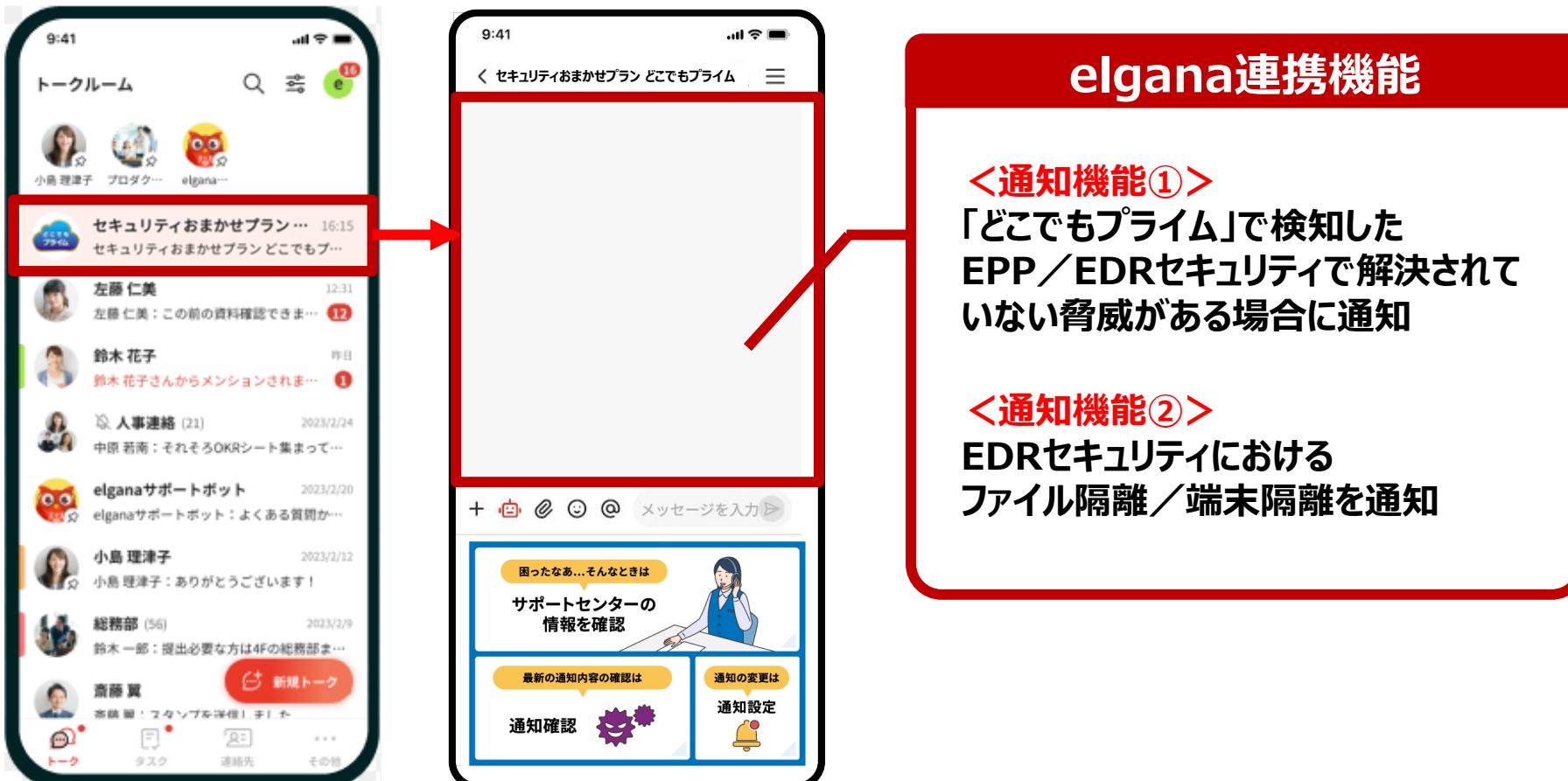
10. elgana連携の設定手順

10. elganaの設定手順 (elganaとは)

elgana（エルガナ）は、どなたでも簡単に使えるビジネスチャットです。

ご紹介HPはこちら ► <https://business.ntt-west.co.jp/service/assist/elgana/>

ビジネスチャットとしてのご利用に加え、このたびお申込みいただいた「セキュリティおまかせプラン どこでもプライム」との連携機能をご利用いただけます。利用手順は、次頁以降をご参照ください。



10. elganaの設定手順（elganaサービス管理サイトでユーザー登録）

STEP1

「elganaサービスご利用開始のお知らせ」に記載されている以下サービス管理サイトへログイン
サービス管理サイトのURLはこちら ►<https://ncs.nttcom.biz/cms/>

- ① 「ユーザー登録」をお願いいたします。
- ② 「登録可能なユーザー数」は「契約ユーザー数」が上限となります。

The screenshot shows the 'User' section of the elgana service management site. A green box labeled '2' highlights the '契約ユーザー数' (Contracted User Count) field, which displays '10'. A blue box labeled '1' highlights the 'ユーザー登録' (User Registration) button. The interface includes a search bar, sorting options for '氏名' (Name), '組織1' (Organization 1), '組織2' (Organization 2), 'アカウント状況' (Account Status), '更新日' (Last Update Date), and 'トータル数制限' (Total Number Limit). Below the search bar, there are two user entries, each with a status of '利用中' (In Use) and a last update date of '2024/12/10'.

10. elganaの設定手順（登録したユーザーでelganaにログイン）

STEP2

elganaサービス管理サイトで登録いただいた各ユーザーでの画面設定となります。

以下の設定を行うことで、「どこでもプライム」で検知したEPP／EDRセキュリティで解決されていない脅威がある場合の通知等を受け取ることが可能です。情報セキュリティ担当、管理者など設定したいユーザにおいて実施ください。

①ログインいただいた画面で「連絡先」を選択

②「検索」をクリックしてください。

③「セキュリティおまかせプラン どこでもプライム」を選択し、吹き出しマーク  をクリックいただくことで、トーカルームが作成されます。

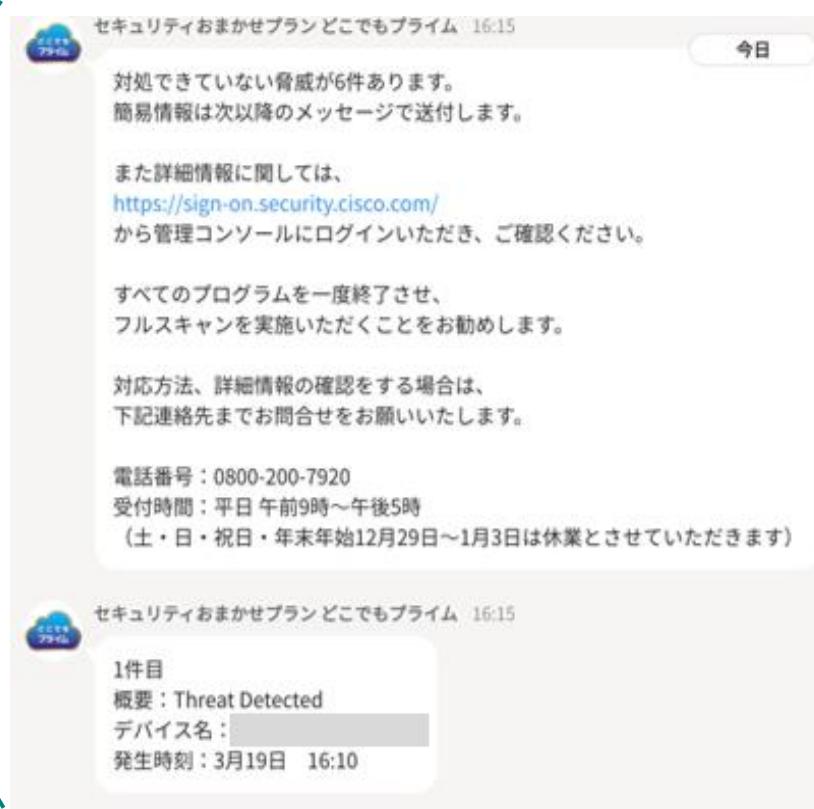


10. elganaの設定手順 (elgana通知開始)

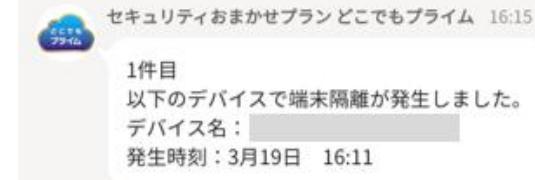
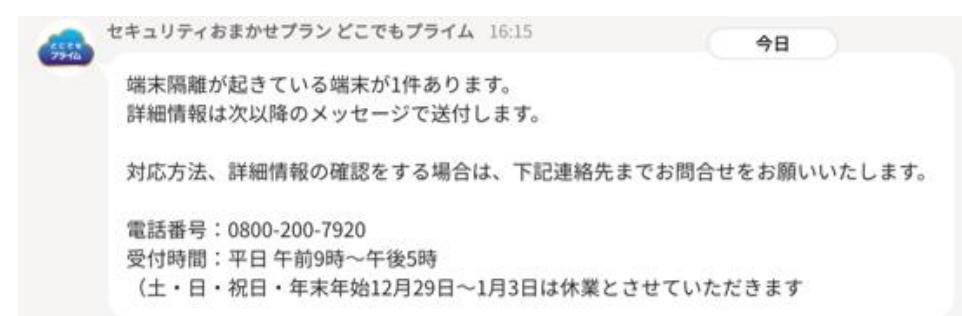
STEP3

以上で設定は完了となり、「どこでもプライム」で検知した内容に基づき通知されます。
もしくは、以下の「通知確認」をクリックすることで、最新の通知内容をご確認をいただくことが可能です。
通知確認のみならず、内部のコミュニケーションとしてもご利用ください。

解決されていない脅威がある場合の通知



端末隔離・解除の通知



11. どこでもプライム契約IDの確認手順

11. どこでもプライム契約IDの確認手順（開通案内メールの場合）

開通メール「【NTT西日本セキュリティおまかせプラン】どこでもプライムのご案内」に記載されている
「契約ID」で確認いただけます。▶送信元：dokopura-kaian@west.ntt.co.jp
件名とメール本文に記載されています。



11. どこでもプライム契約IDの確認手順（Ciscoコンソールの場合）

■Cisco Umbrellaシステムのコンソールでご確認いただく場合

[Cisco Umbrella管理コンソールへのログイン手順](#) を参考にログインいただき、赤枠内に表示されている契約IDをご確認ください。

The screenshot shows the Cisco Umbrella management console interface. On the left, there is a sidebar with navigation links: 概要, 導入, ポリシー, レポート, Investigate, 管理, and a user profile section with the email address DKF@DKO.co.jp. A red arrow points from this user profile to a red box highlighting the text "DKFまたはDKO + 数字10桁". The main dashboard area has tabs for すべて, DNS, and WEB. It displays sections for 0 Messages, Malware, Botnet, Cryptomining, and Network Health. The Network Health section includes four cards: アクティブなネットワーク (0% active), アクティブなローミングクライアント (55% active), アクティブな仮想プライアンス (0% active), and アクティブなネットワークトンネル (yellow warning icon). A "Get Started" button is visible on the right.

12. ログ取得および送付手順

12. ログ取得および送付手順

セキュアインターネットゲートウェイ（Cisco Umbrella）、セキュアエンドポイント（Cisco Secure Endpoint）を導入後、不具合等が発生した際、弊社サポート担当から各種ログ（※）の取得を依頼する場合がございます。

次頁以降で、対象となるログごとに、Windows環境およびMac環境での取得手順を説明いたします。

| ログの種類 | 説明 | 使用ツール | 説明ページ |
|-------------|---|---------------|----------------------------------|
| DARTログ | セキュアインターネットゲートウェイ（Cisco Umbrella）に関する問題を調査するための診断ログを指します。 | DART | DARTログの取得手順 |
| サポート診断ツールログ | セキュアエンドポイント（Cisco Secure Endpoint）に関する問題を調査するためのログを指します。 | サポート診断ツール | サポート診断ツールログの取得手順 |
| HARファイル | セキュアインターネットゲートウェイ（Cisco Umbrella）のWeb通信問題を調査するためのファイルを指します。 | 各種ブラウザの開発者ツール | HARファイルの取得手順 |

参考：Cisco社サイト

[DARTログ取得手順](#) (Windows)

[DARTログ取得手順](#) (Mac)

[サポート診断ツールログ取得手順](#) (Windows)

[サポート診断ツールログ取得手順](#) (Mac)

12-1. DARTログの取得手順_Windows

12-1. DARTログの取得手順_Windows 1/4

不具合事象の再現後、以下手順に従ってDARTログを取得してください。

タスクバーから「Cisco Secure Client」アプリをクリック

「⊕」マークをクリックし、詳細画面を開く

「診断」をクリックし、DARTアプリを起動する



12-1. DARTログの取得手順_Windows 2/4

ウィザードに従い、ログを取得します。

「次へ」をクリック



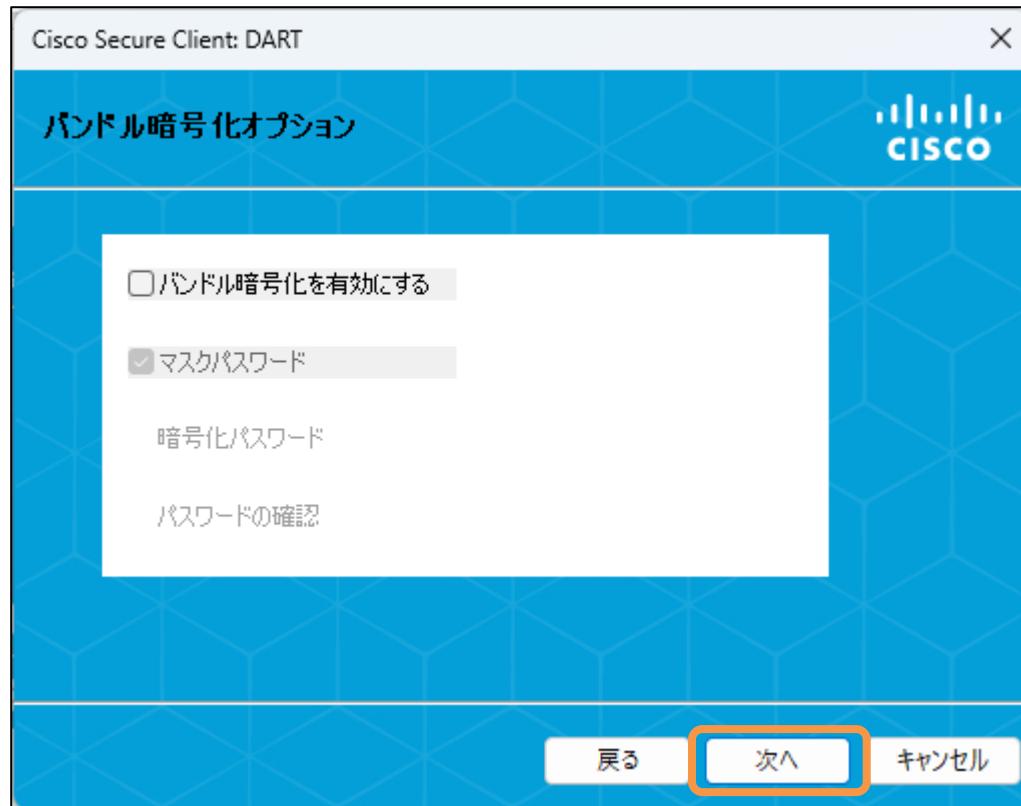
「デフォルト-バンドルはデスクトップに保存されます」を選択し、「次へ」をクリック



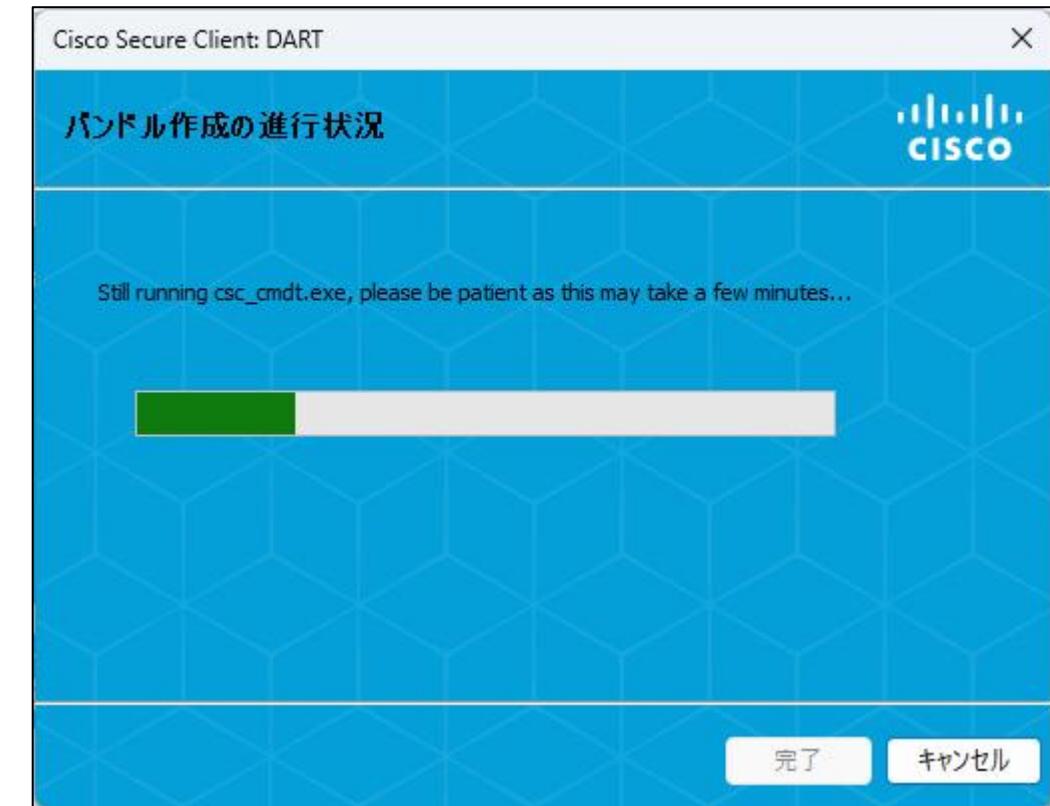
12-1. DARTログの取得手順_Windows 3/4

ウィザードに従い、ログを取得します。

「次へ」をクリック



3分程度お待ちください



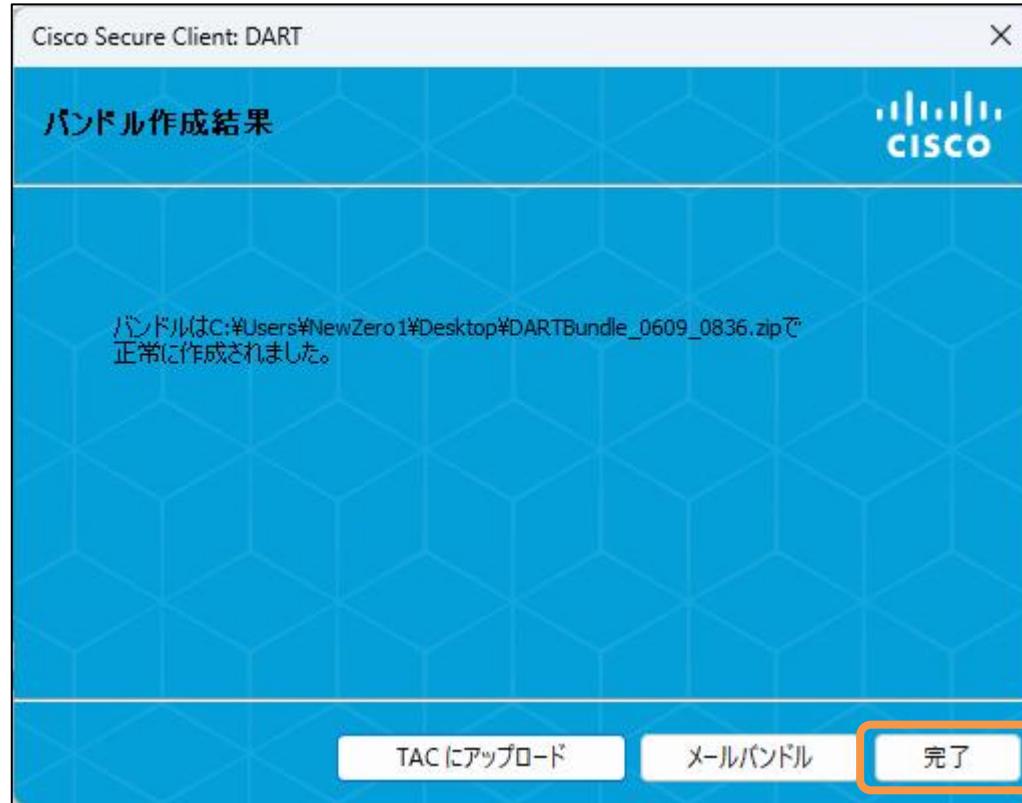
12-1. DARTログの取得手順_Windows 4/4

以下画像「完了」までの処理が終わると、デスクトップにログファイル「DARTBundle_(日付)_(時刻).zip」が生成されます。

生成されたDARTログファイルの送付手順については、[\[12-4. ログの送付方法\]](#)をご参照ください。

「完了」をクリック

デスクトップにログファイル
「DARTBundle_(日付)_(時刻).zip」が
生成される

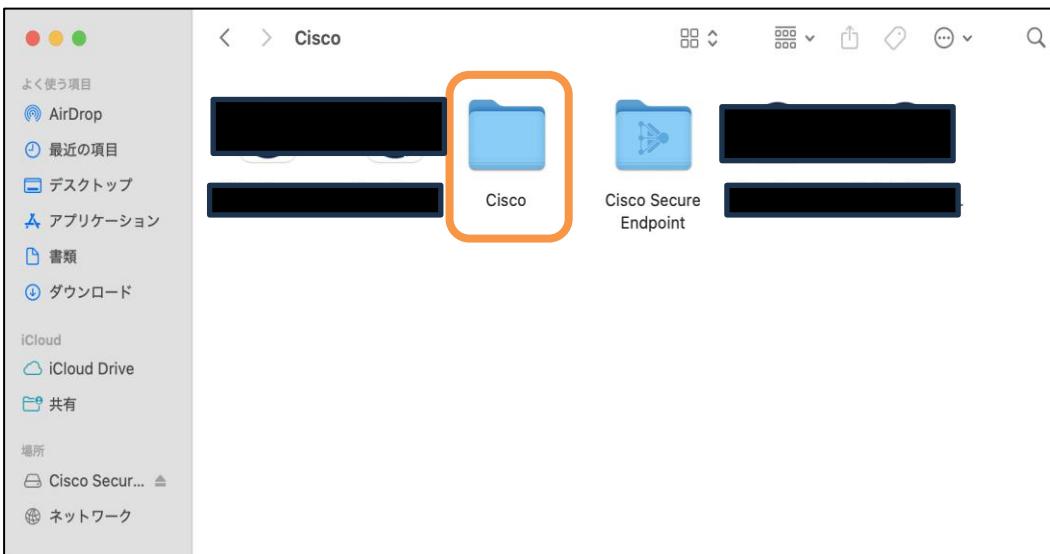


12-1. DARTログの取得手順_Mac

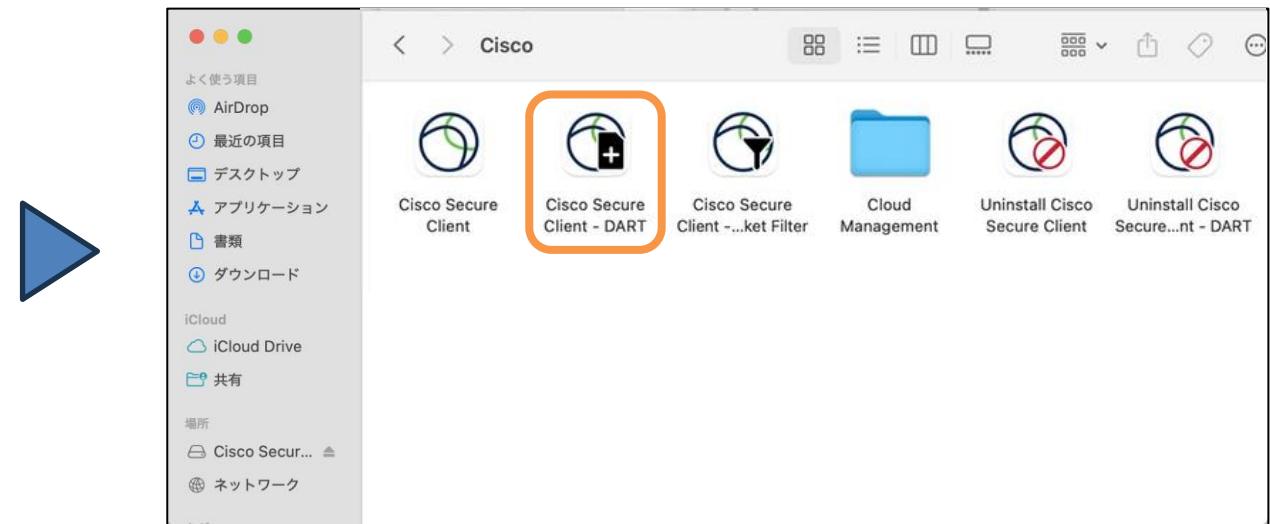
12-1. DARTログの取得手順_Mac 1/3

不具合事象の再現後、以下手順に従ってDARTログを取得してください。

アプリケーションフォルダの「Cisco」
をダブルクリック



「Cisco Secure Client - DART」をダブルクリック



12-1. DARTログの取得手順_Mac 2/3

手順に従ってDARTログを取得してください。

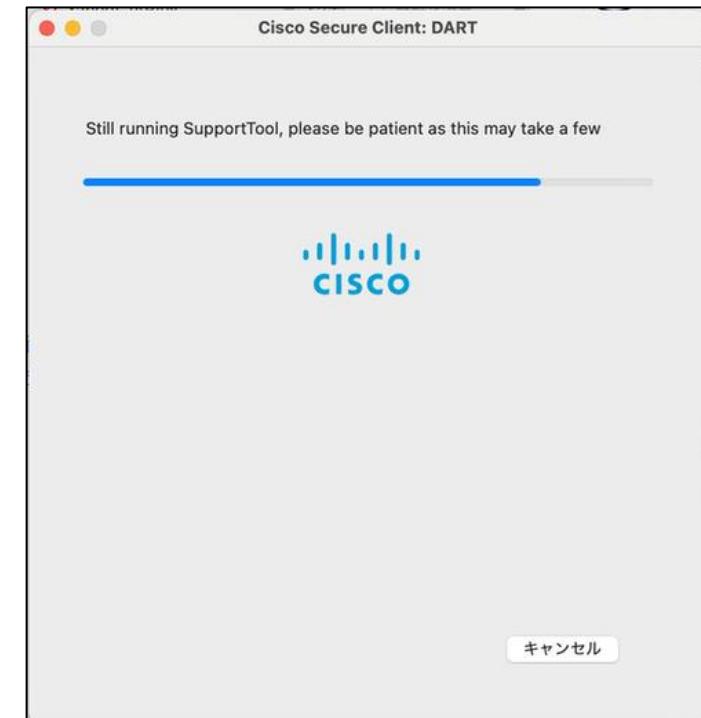
「追加のログオプション」の枠内2つに□を入れて、
「実行」をクリック



パスワードを入力し、「OK」をクリック



3分程度お待ちください



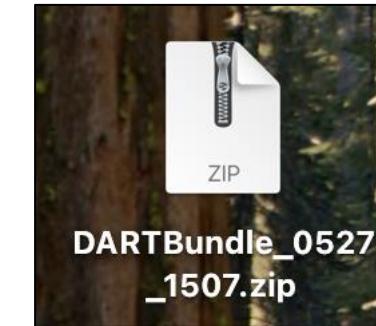
12-1. DARTログの取得手順_Mac 3/3

以下画像「完了」までの処理が終わると、デスクトップにログファイル「DARTBundle_(日付)_(時刻).zip」が生成されます。

生成されたDARTログファイルの送付手順については、[「12-4. ログの送付方法」](#)をご参照ください。

「完了」をクリック

デスクトップにログファイル
「DARTBundle_(日付)_(時刻).zip」が
生成される



12-2. サポート診断ツールログの取得手順_Windows

12-2. サポート診断ツールログの取得手順_Windows

不具合事象の再現後、以下手順に従い、ログを取得してください。

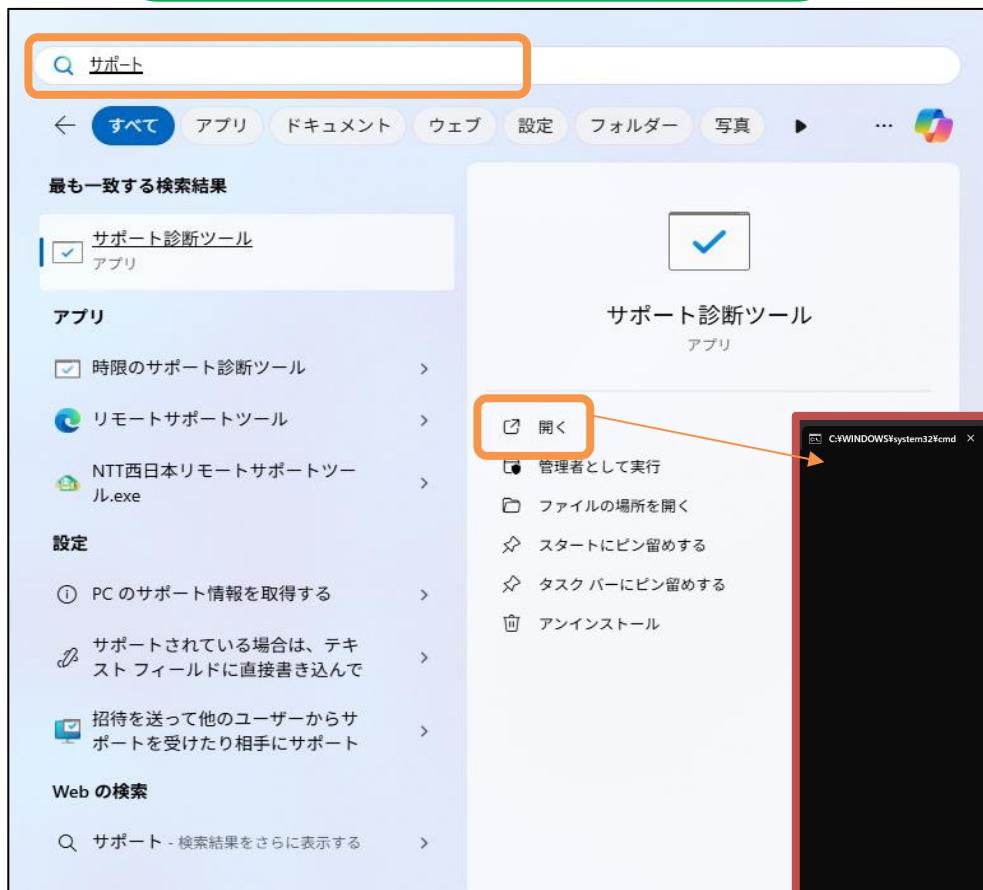
※サポートセンターから依頼があった場合は、事前に「デバッグロギング有効化」の手順に従って設定を行ってください。

設定完了後、本ページの作業を実施いただきますようお願いいたします。

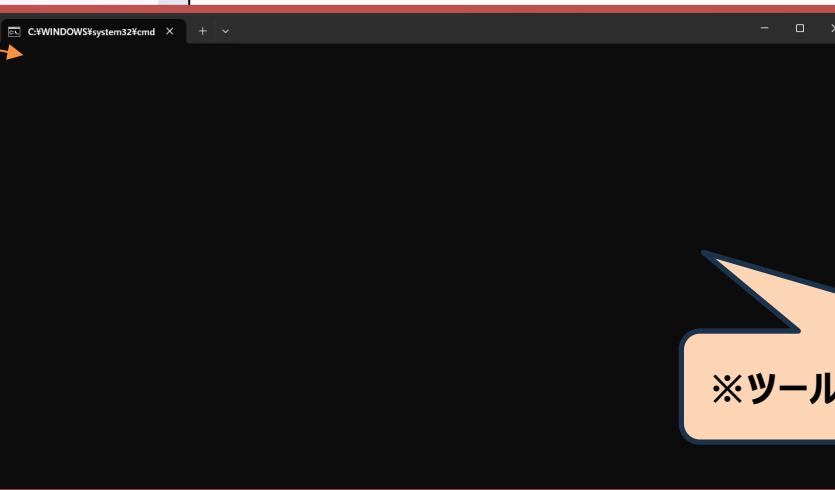
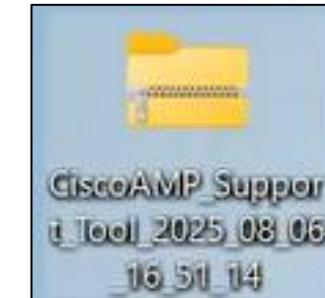
なお、「デバッグロギング」は、詳細なログを取得するための設定です。

生成されたサポート診断ツールログファイルの送付手順については、[「12-4. ログの送付方法」](#)をご参照ください。

「Windows」で「サポート診断ツール」を検索。「開く」をクリックし実行する。



デスクトップにログファイルが「CiscoAMP_Support_Tool_(西暦)(月)(日)(時)(分)(秒).zip」が生成される。



※ツール実行中はこの画面が表示されます

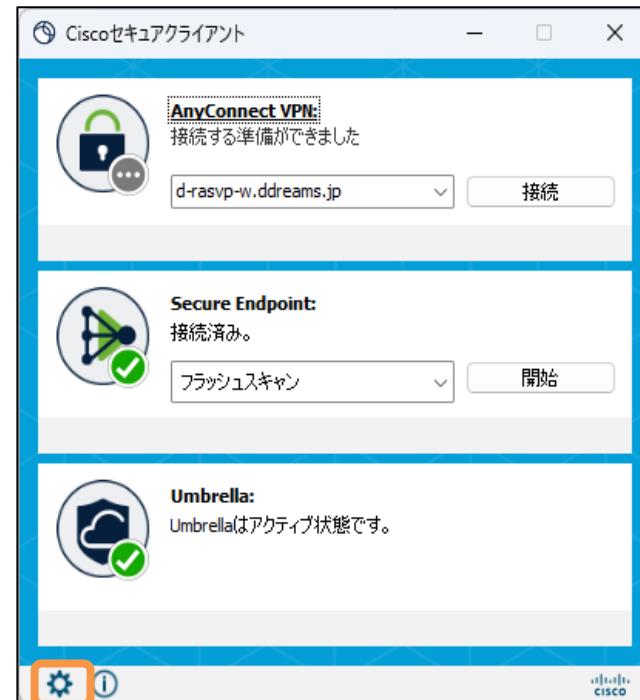
前頁のログ取得前(不具合事象の再現前)に、
以下手順に従い、デバッグロギングを有効にしてください。

※ログ取得完了後、デバッグロギングを無効化することを忘れないようご注意ください。

タスクバーから「Cisco Secure Client」アプリをクリック



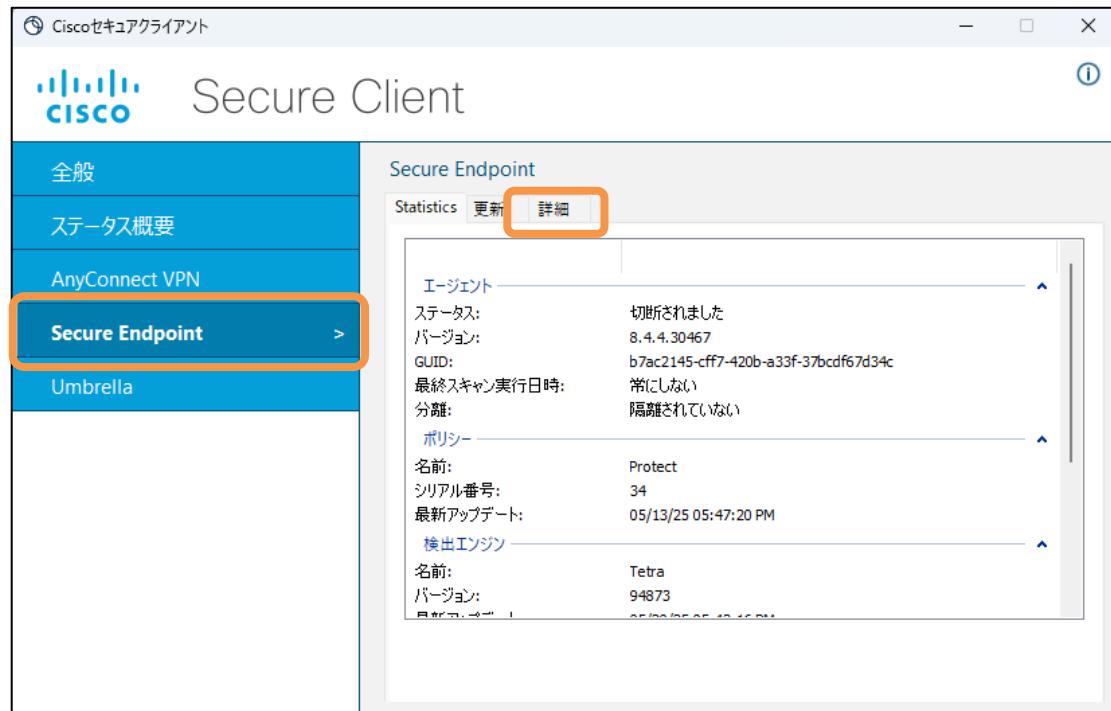
「⚙️」マークをクリックし、詳細画面を開く



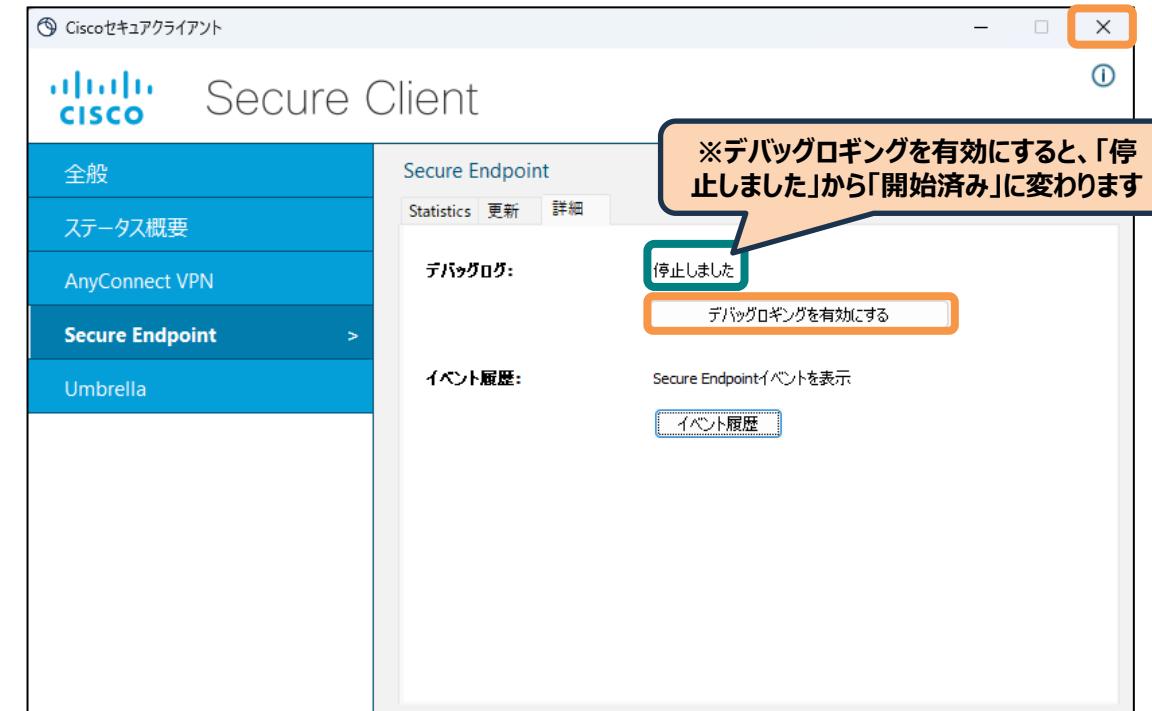
以下手順に従い、デバッグロギングを有効にしてください。

※ログ取得完了後、デバッグロギングを無効化することを忘れないようご注意ください。

「Secure Endpoint」をクリックし、「詳細」を開く



「デバッグロギングを有効にする」をクリックし、
「×」で画面を閉じる



ログ取得後、デバッグロギングを無効化します。

「デバッグロギングを無効にする」をクリックし、
「×」で画面を閉じる



12-2. サポート診断ツールログの取得手順_Mac

12-2. サポート診断ツールログの取得手順_Mac 1/2

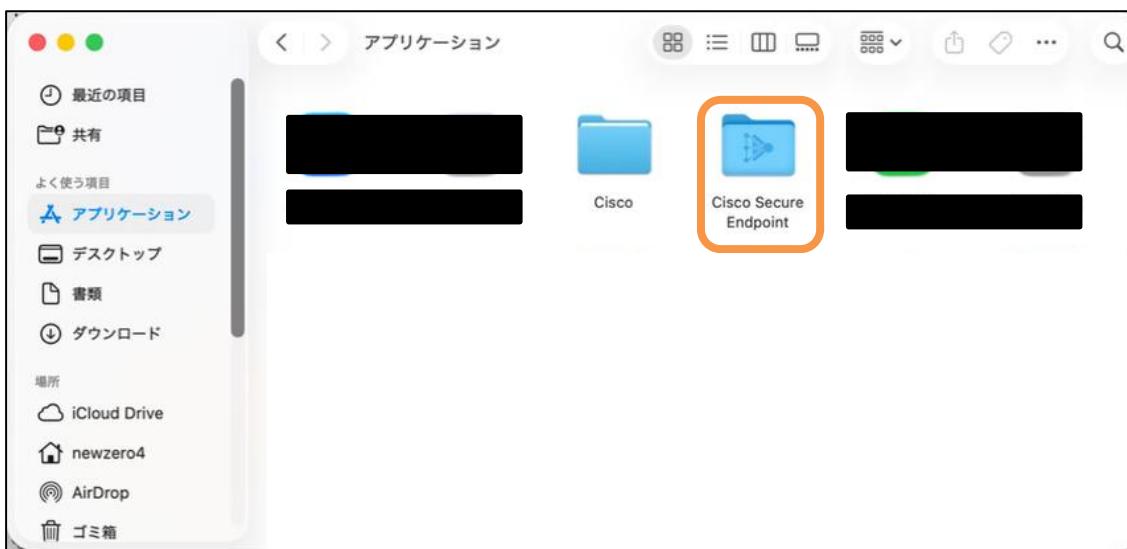
不具合事象の再現後、以下手順に従ってサポート診断ツールログを取得してください。

※サポートセンターから依頼があった場合は、事前に<デバッグモード有効化>の手順に従って設定を行ってください。

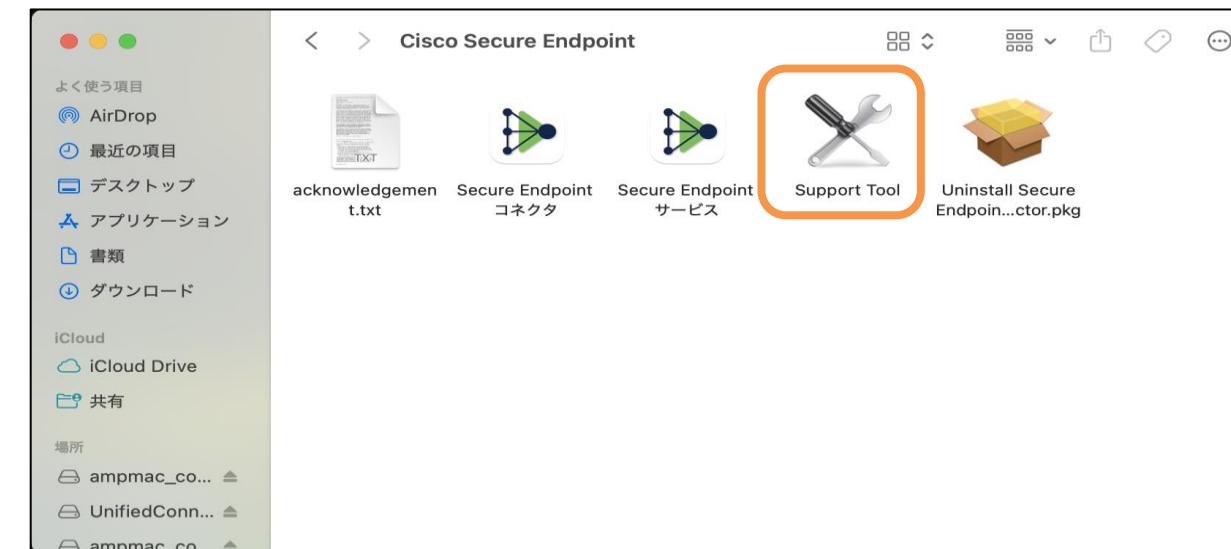
設定完了後、本ページの作業を実施いただきますようお願いいたします。

なお、「デバッグモード」は、詳細なログを取得するための設定です。

アプリケーションフォルダの「Cisco Secure Endpoint」をダブルクリック



「Support Tool」をダブルクリック



12-2. サポート診断ツールログの取得手順_Mac 2/2

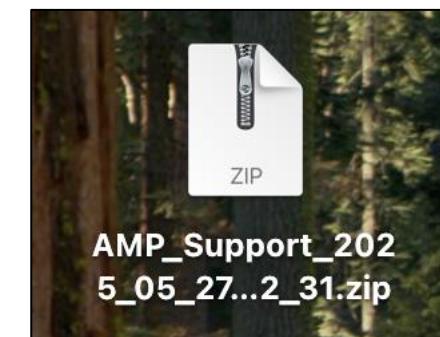
デスクトップにログファイル「AMP_Support_(西暦)_(月)_(日)_(時)_(分)_(秒).zip」が生成されます。

生成されたサポート診断ツールログファイルの送付については、[「12-4. ログの送付方法」](#)をご参照ください。

パスワードを入力し、「OK」をクリック



デスクトップにログファイル
「AMP_Support_(西暦)_(月)_(日)_(時)_(分)_(秒).zip」が生成される



前頁のログ取得前(不具合事象の再現前)に、

コンソール画面に入り、以下手順でデバッグモードを有効にしてください。

※ログ取得完了後、デバッグモードを無効化することを忘れないようご注意ください。

参考URL : [Debugログ取得方法](#)

「管理」→「ポリシー」の順でクリックし、ポリシー画面に移動する

The screenshot shows the Cisco Secure Endpoint management interface. On the left sidebar, under the '管理' (Management) section, the 'ポリシー' (Policy) item is highlighted with a blue box. In the main content area, there are several cards: '最近のコンピュータ' (Recent Computers) showing a list of OS versions and host names, '最近のアウトブレイク制御リスト' (Recent Outbreak Control Lists) showing a file list and detection list, and 'アプリケーション' (Applications) which displays a message stating 'アプリケーションが見つかりません' (No applications found). The URL at the bottom of the page is <https://console.apjc.amp.cisco.com/policies>.

以下手順でデバッグモードを有効にしてください。

「MAC」→「Protect」をクリック

The screenshot shows the Cisco Secure Endpoint web interface. On the left, there's a sidebar with navigation links: ダッシュボード, 受信トレイ, 概要, イベント, 分析, アウトブレイク制御, 管理 (which is selected), and アドミン. The main area is titled "ポリシー" and has a sub-header "新しいバージョンをお試しください". It includes a search bar and a filter section with tabs for "すべて", "ウィンドウ", "MAC" (which is highlighted with an orange box), "Linux", "Android", "iOS", and "ネットワーク". Below this is a table of policies:

| 名前 | 変更日 | グループ | コンピュータ |
|---------|-------------------------|------|--------|
| Audit | 2025-02-10 01:35:16 UTC | 3 | 0 |
| Protect | 2025-02-10 01:35:16 UTC | 1 | 2 |
| Triage | 2025-02-10 01:35:17 UTC | 1 | 0 |

At the bottom of the page, there are footer messages: "147.161.195.27からの22分時間前の最後のログイン 現在のセッションは22分時間前に開始されました", "この組織のデータはJapanでホストされています", "© 2025 Cisco Systems, Inc. サービス契約", and a blue button "フィードバックをお送りください".

以下手順でデバッグモードを有効にしてください。

詳細設定の「管理機能」をクリックし、コネクタログレベルが「デフォルト」となっているので、プルダウンで「デバッグ」に変更し、「保存」をクリック

The screenshot shows the 'Secure Endpoint' interface with the 'Protect' policy selected. The left sidebar shows navigation categories like Dashboard, Inbox, Overview, Events, Analysis, Outbreak Control, Management, and Admin. Under Admin, the 'Management Functions' option is highlighted with a blue box. In the main content area, the 'Policy Editor' shows the 'Protect' policy with its name and description. The 'Mode and Engine' section includes options like 'Exclude' and 'Proxy'. The 'Advanced Settings' section contains various checkboxes and dropdowns. The 'Connector Log Level' dropdown is set to 'Default' and is highlighted with an orange box. The 'Save' button at the bottom left is also highlighted with an orange box.

(参考) サポート診断ツールログの取得手順_Mac <デバッグモード有効化> 4/5

端末にPolicyが反映されるまで待ちます。

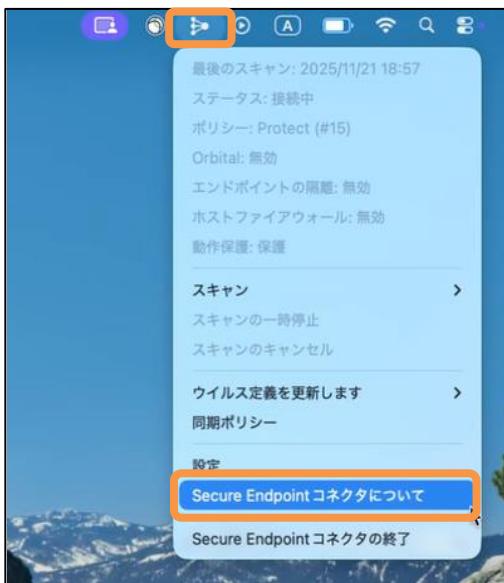
通常は、変更後すぐに反映されますが、以下手順で同期状態を確認後、[サポート診断ツールログの取得](#)をお願いいたします。

※ログ取得完了後、デバッグモードを無効化することを忘れないようご注意ください。

▶ をクリックし、「Secure Endpoint コネクタについて」を選択する

「ポリシー」を選択する

最終更新日時が最新になっているか確認
(同画面の「同期」ボタンをクリックすると、手動でポリシーの同期も可能です)



以下手順でデバッグモードを無効化してください。

詳細設定の「管理機能」をクリックし、コネクタログレベルが「デバッグ」となっているので、プルダウンで「デフォルト」に変更し、「保存」をクリック

The screenshot shows the Cisco Secure Endpoint web interface. On the left, a sidebar menu includes 'Secure Endpoint' (selected), 'ダッシュボード', '受信トレイ', '概要', 'イベント', '分析', 'アウトブレイク制御', '管理' (selected), and 'アドミン'. Under '管理', '詳細設定' is expanded, and '管理機能' is selected. The main content area shows the 'ポリシーの編集: Protect' screen for a 'MAC' policy. The 'Name' field is 'Protect' and the 'Description' is 'This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.' In the 'Mode and Engine' section, the 'Connector Log Level' dropdown is set to 'Debug' (highlighted with an orange box). Below it, the 'Log Level' dropdown is set to 'Default'. Other settings include sending event user names, file names, and path information every 15 minutes. The 'Save' button at the bottom left is also highlighted with an orange box.

12-3. HARファイルの取得手順

12-3. HARファイルの取得手順

以下手順に従ってHARファイルを取得してください。

詳細な手順については、Cisco社のサイト（下記URL）をご参照ください。

※HARファイルの取得手順については、OS（Windows、Mac）による差分はございません。

URL: <https://community.cisco.com/t5/-/ta-p/4459253>

【HARファイルの取得手順】

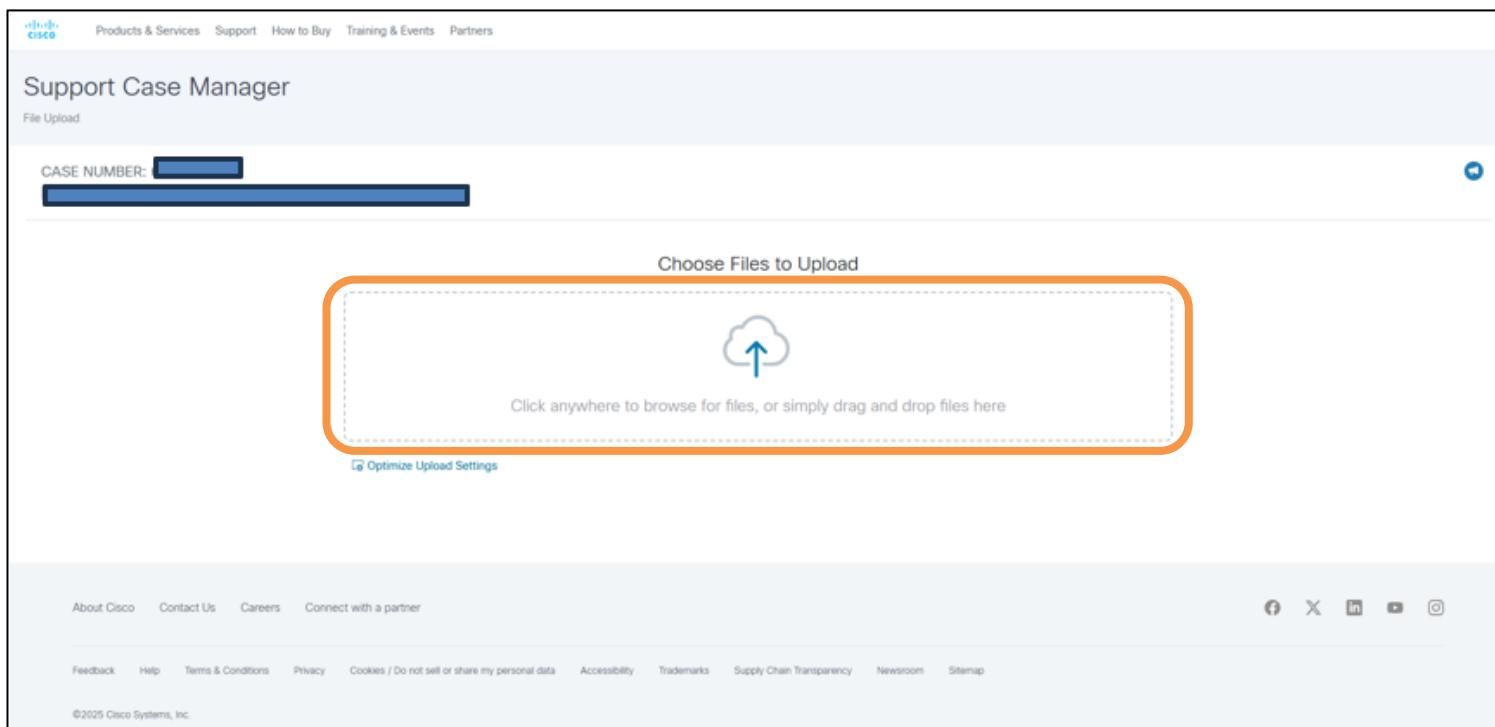
- ①該当端末でGoogle Chrome/Microsoft edgeを開きます。
- ②デベロッパーツール(開発者ツール)を開きます。
- ③[Network]タブを開き、[Preserve log]と[Disable cache]にチェックを入れます。
- ④レコーディングが開始されていることを確認します。
- ⑤「ネットワークログのクリア」アイコンをクリックし、ログを一旦削除します。
- ⑥表示できないサイトのURLを開きます。
- ⑦エラー画面が表示されたら右上のダウンロードボタンからファイルを出力します。

12-4. ログの送付方法

12-4. ログの送付方法 1/2

サポートセンターより、ログアップロード用URLを共有いたしますので、
以下手順で、取得したログファイルをアップロードしてください。

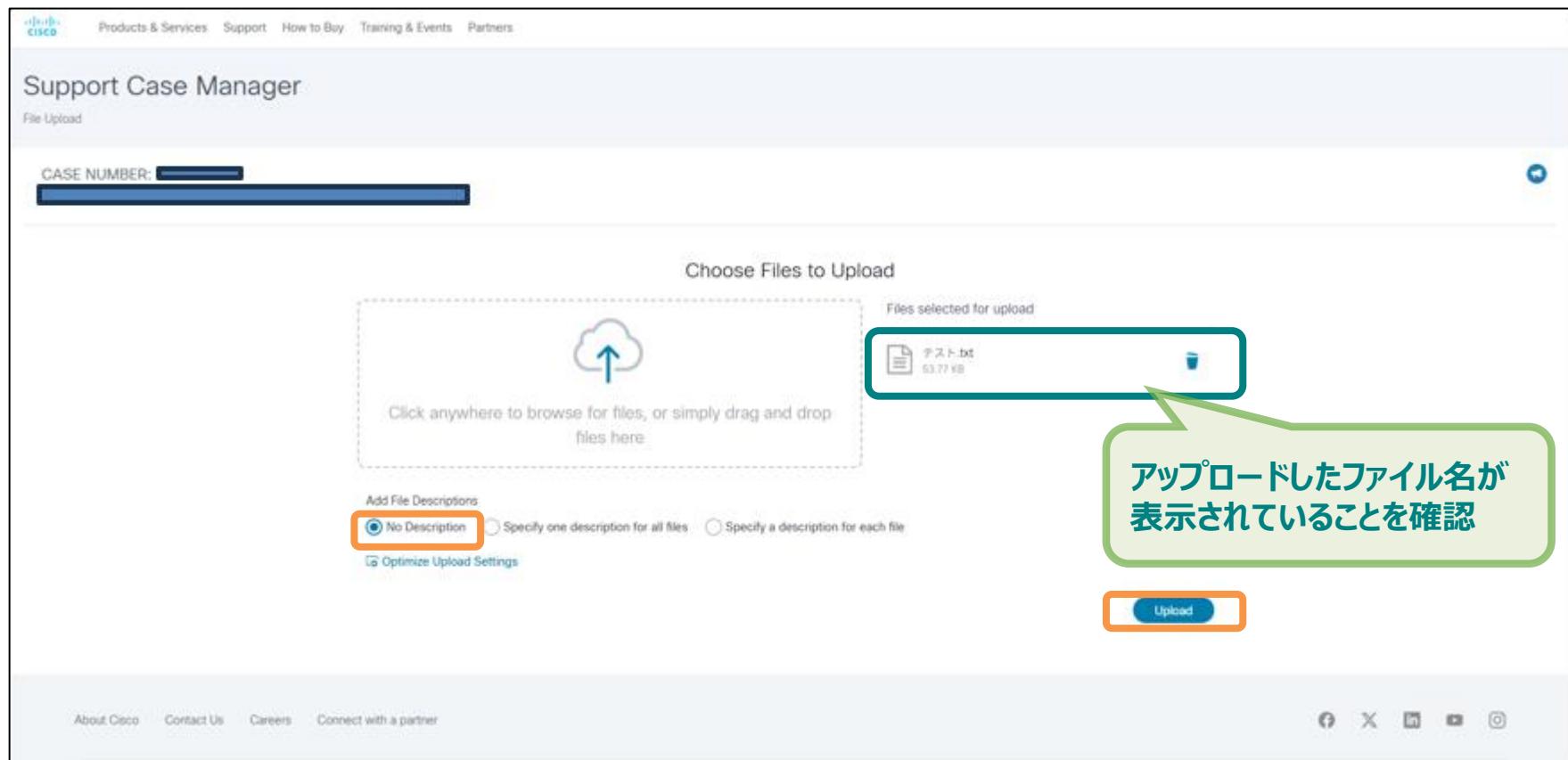
取得したログファイルを  のマークがある枠内にドラッグアンドドロップしてください。
(もしくは、枠内をクリック→ファイル選択→「開く」クリックでもアップロード可能です)



12-4. ログの送付方法 2/2

以下手順に従ってログのアップロードを完了させてください。

「No Description」を選択し、「Upload」をクリックしてください。



アップロードしたファイル名が
表示されていることを確認