

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

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。



※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

2. 事前準備

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	<div><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><div><div>◆ 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)</div><div>② 端末設定ツール入手用のURL及びログイン情報</div></div><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がございます。 ※インストーラの取り扱いには十分ご注意ください。</p><div><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>【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-ml@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></div></div>

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

3

elgana コネクト

ntt-west-test130@mbox.re

パスワードをお忘れのとき

4

ログイン >

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 displays the 'elgana コネクト' (elgana Connect) website's 'マイページ' (My Page) section. At the top, there's a navigation bar with the elgana logo and a 'よくあるご質問' (Frequently Asked Questions) link. Below this, a 'ログアウト' (Logout) button is visible. The main heading is 'マイページ' (My Page), followed by a sub-heading '「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' (Please apply for services from 'Go to Service List'). A prominent red button labeled 'サービス一覧へ進む' (Go to Service List) is centered. Below this, there are two tabs: 'お客様情報' (Customer Information) and 'サービス契約内容' (Service Contract Details), with the latter being the active tab. Under the 'サービス契約内容' tab, the section is titled 'ワークスペース情報' (Workspace Information). It contains a 'ワークスペースID' (Workspace ID) field with the value '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 with the above Workspace ID). A red button labeled 'セキュリティおまかせプランどこでもプライム' (Security Trust Plan Anywhere Prime) is positioned above a table. The table has two rows: 'elgana 利用開始日' (elgana Start Date) and 'elgana 利用完了日' (elgana Completion Date). To the right of the table, the text '未インストール/インストール済み' (Not installed/Installed) is displayed. Further right, there are two buttons: 'Windows用' (For Windows) and 'Mac用' (For Mac). A red line points from the 'Windows用' button to 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 it).

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ム

elgana 利用開始日	未インストール/インストール済み	<div>Windows用</div> <div>Mac用</div>
elgana 利用完了日		

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)

▼ 先月				
	csc-deploy-network-000000_Sample Cor...	2024/12/25 15:36	アプリケーション	32,800 KB
	Cisco_Umbrella_Root_CA.cer	2024/12/25 15:35	セキュリティ証明書	2 KB

👉 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)

▼ 先月				
	csc-deploy-full-000000_Sample Corpora...	2024/12/25 15:36	アプリケーション	135,269 KB
	Cisco_Umbrella_Root_CA.cer	2024/12/25 15:35	セキュリティ証明書	2 KB

👉 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）

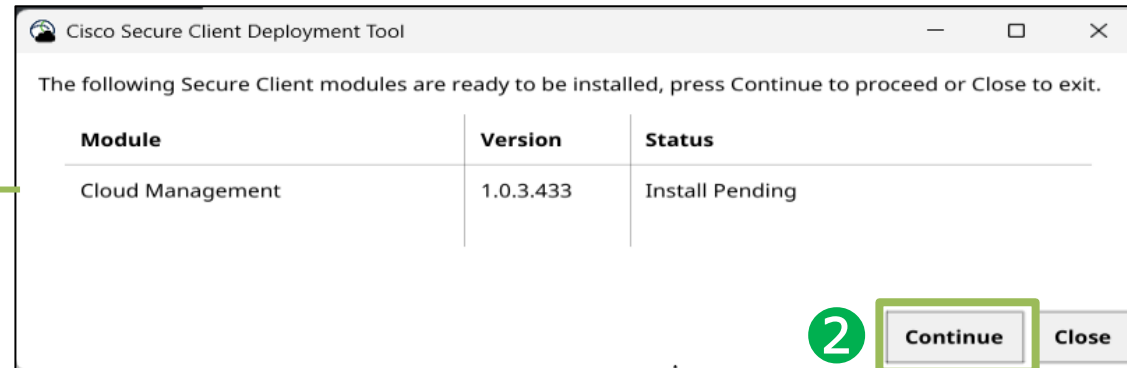
👉 対象のネットワークインストーラを実行
(csc-deploy-network-[契約ID]_[会社名].exeの実行)

1

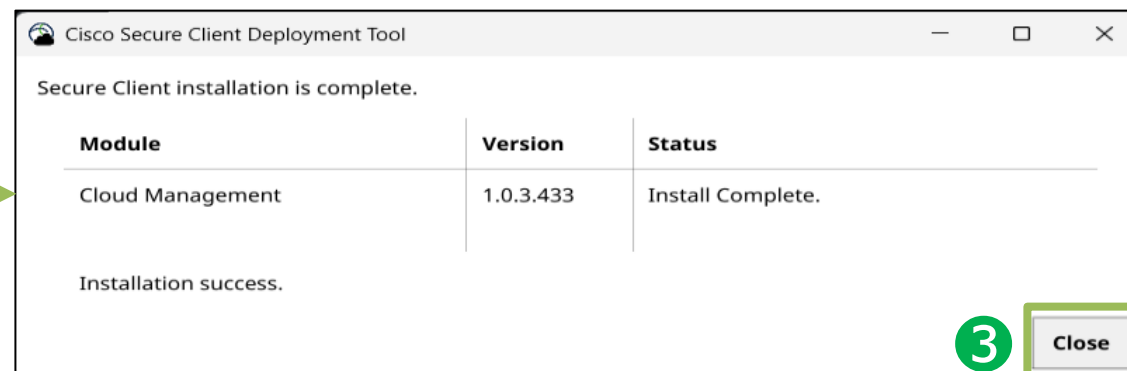
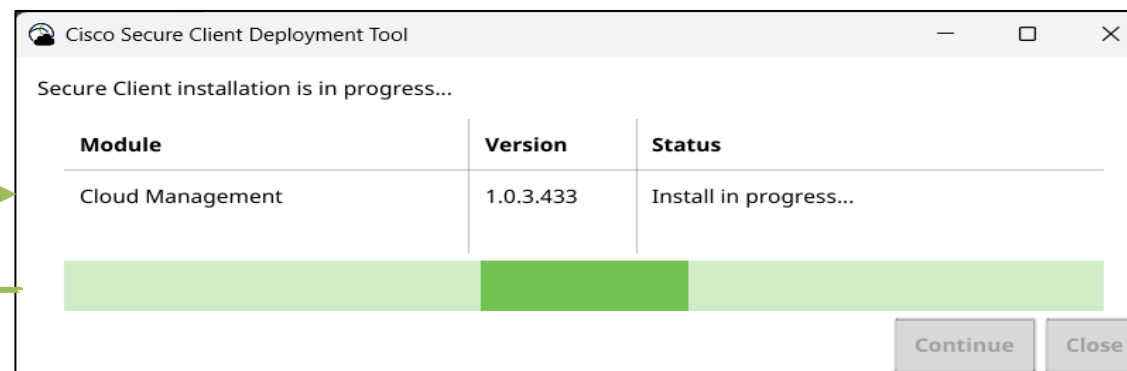
▼ 先月				
	csc-deploy-network-000000_Sample Cor...	2024/12/25 15:36	アプリケーション	32,800 KB
	Cisco_Umbrella_Root_CA.cer	2024/12/25 15:35	セキュリティ証明書	2 KB

※契約IDは開通メールをご参照ください

👉 「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）

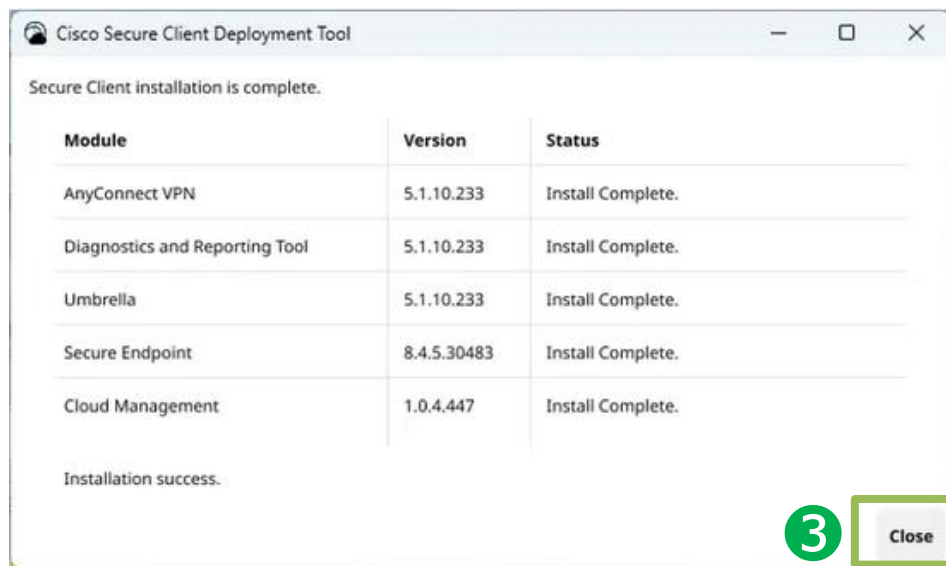
👉 対象のネットワークインストーラを実行
（csc-deploy-full-[契約ID]_[会社名].exeの実行）

👉 「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

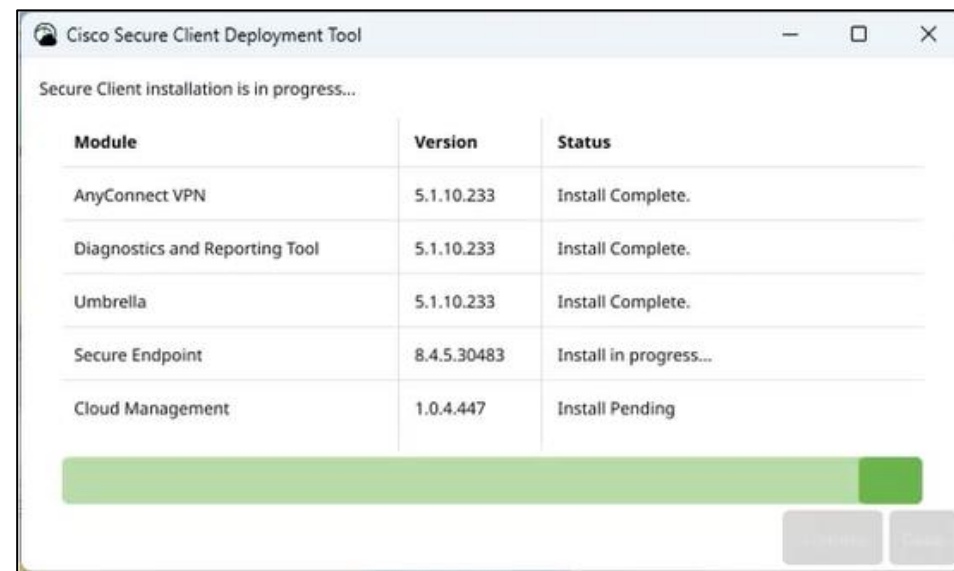
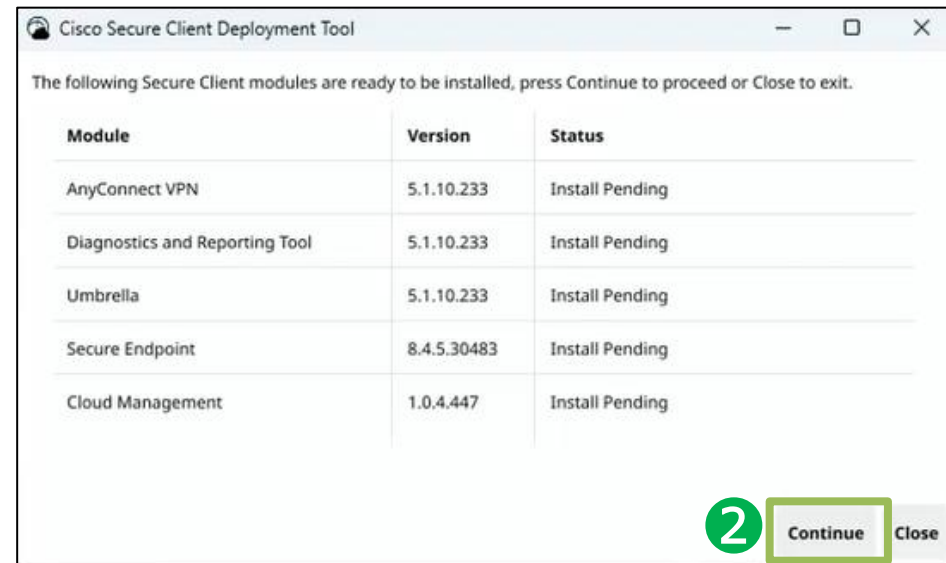
1

▼ 先月				
 csc-deploy-full-000000_Sa..	2024/12/25 15:36	アプリケーション	35,269 KB	✓
 Cisco_Umbrella_Root_CA.cer	2024/12/25 15:35	セキュリティ証明書	2 KB	✓

※契約IDは開通メールをご参照ください



1分程度待つ



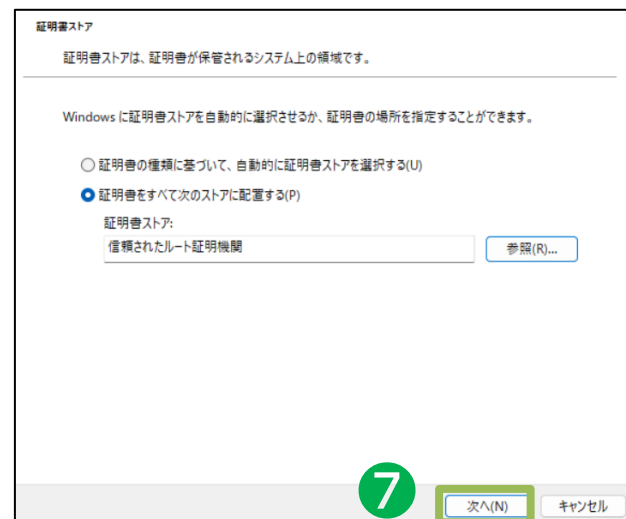
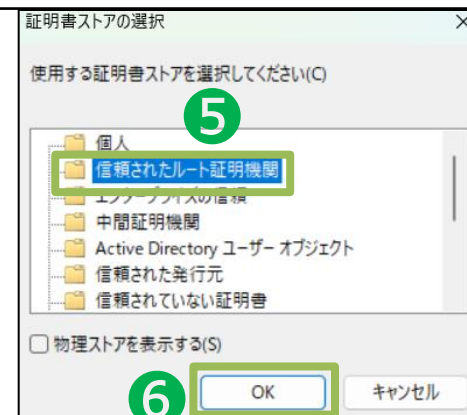
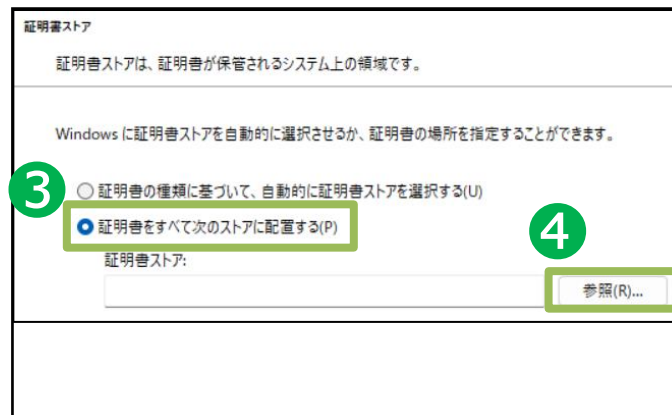
4-3. インストール手順 <ダウンロードしたインストーラの実行-4>

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

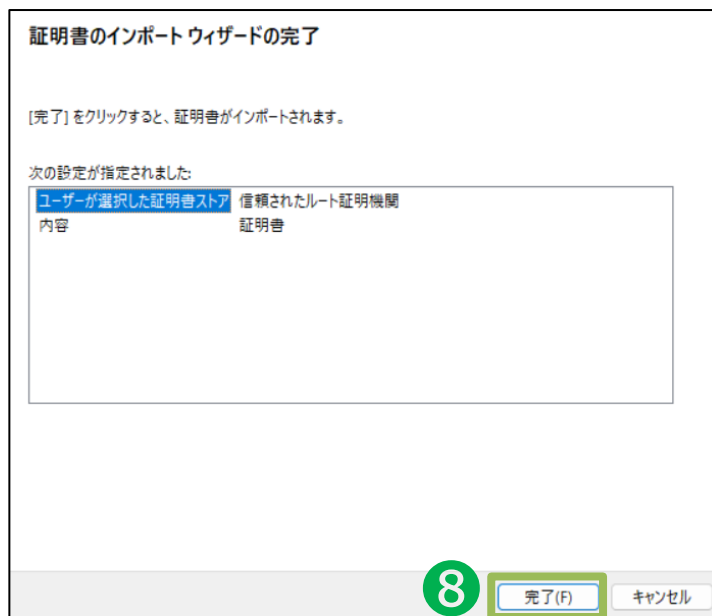
👉 「証明書をすべて次のストアに配置する」を選択した状態で参照から「信頼されたルート証明機関」を指定して次へ進む



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

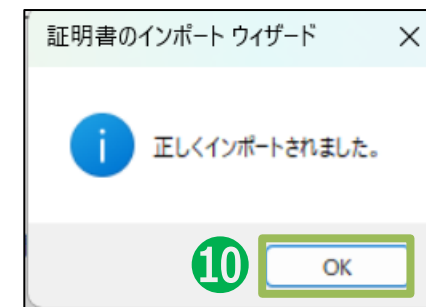
👉 「完了」を選択してインポートを開始



👉 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



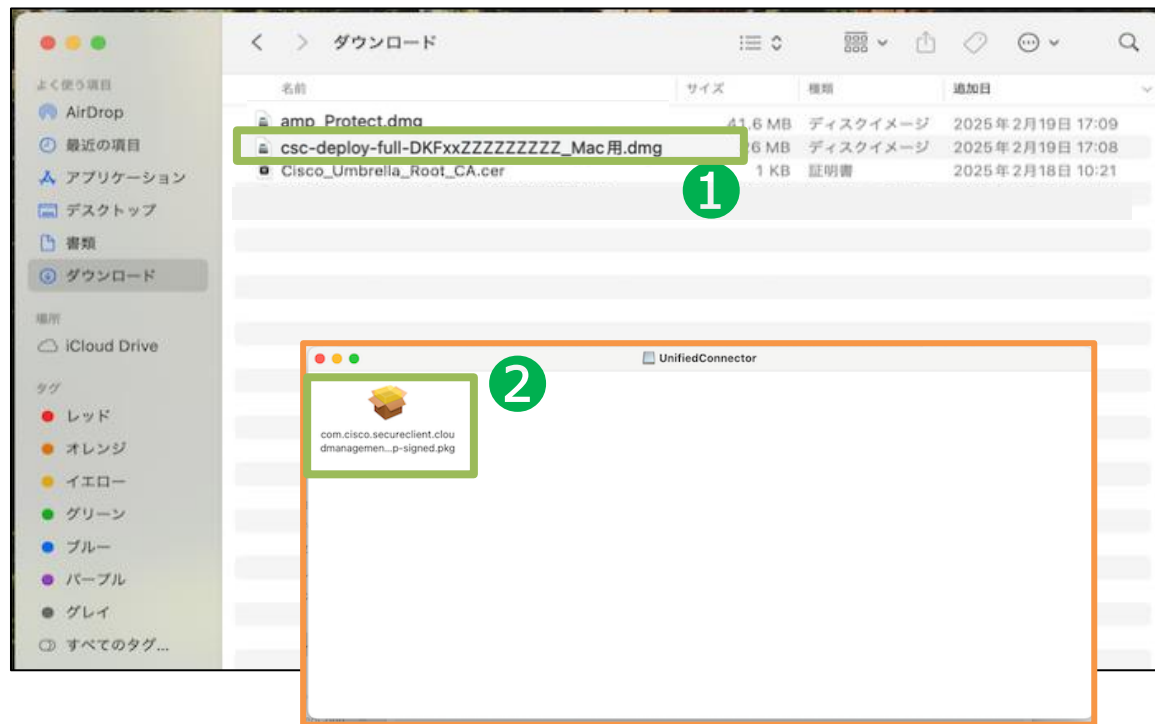
👉 インポート完了



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）

名前	サイズ	種類	追加日
amp_Protect.dmg	41.6 MB	ディスクイメージ	2025年2月19日 17:09
csc-deploy-network-DKFxxZZZZZZZZ_Mac.dmg	2 MB	ディスクイメージ	2025年2月19日 17:08
Cisco_Umbrella_Root_CA.cer	1 KB	証明書	2025年2月18日 10:21

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）

名前	サイズ	種類	追加日
amp_Protect.dmg	41.6 MB	ディスクイメージ	2025年2月19日 17:09
csc-deploy-full-DKFxxZZZZZZZZ_Mac用.dmg	2 MB	ディスクイメージ	2025年2月19日 17:08
Cisco_Umbrella_Root_CA.cer	1 KB	証明書	2025年2月18日 10:21

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>

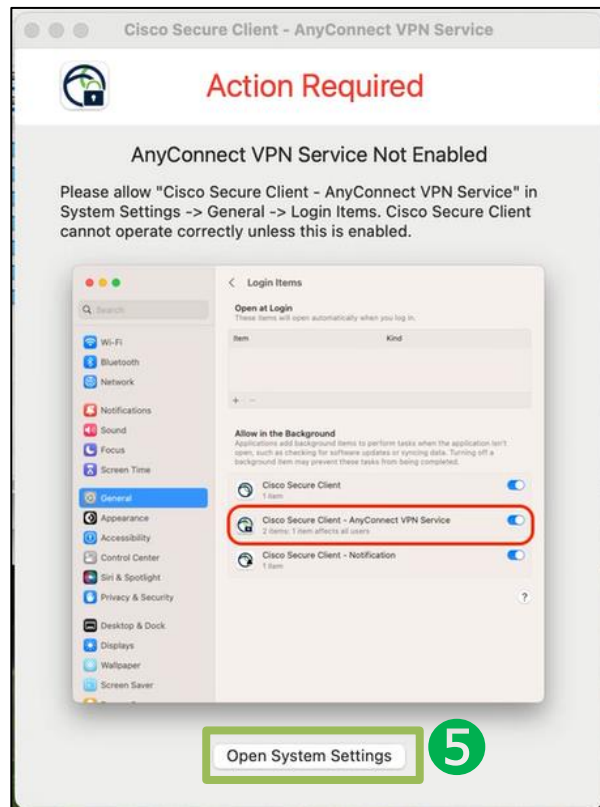
👉 「インストール」を選択



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（※）



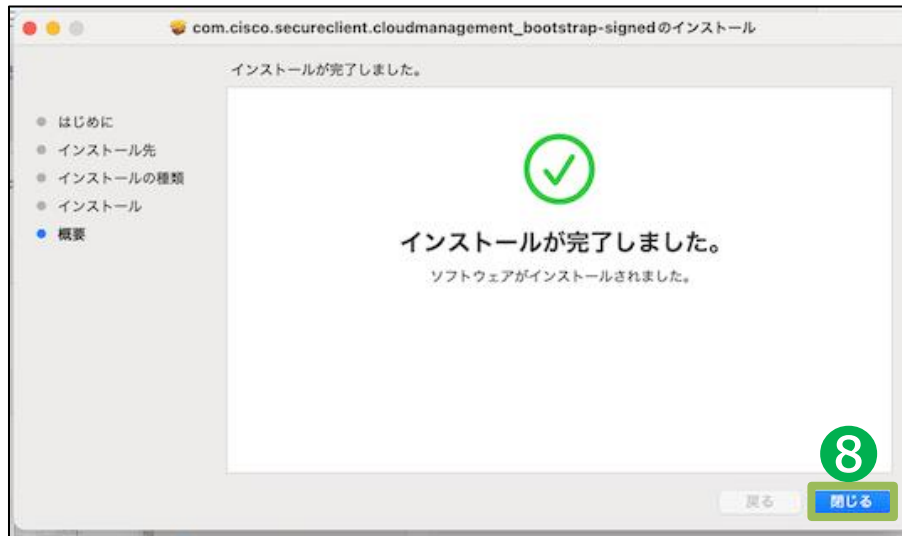
※自動で有効になっている場合もありますので、その場合は画面左上の「×」で画面を閉じてください。

👉 パスワードを入力し、「設定を変更」をクリック



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



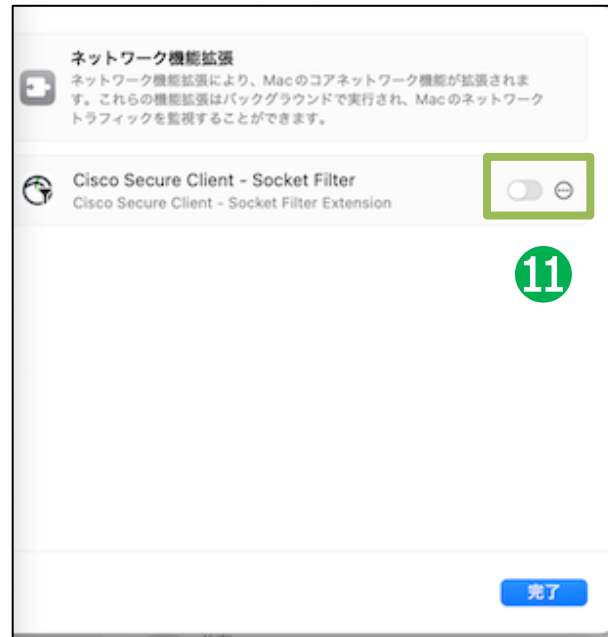
※以降の手順では、
端末によりポップアップの表示される順番が前後する可能性があります。
表示されたポップアップに従ってアプリの初期設定を実施してください。

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

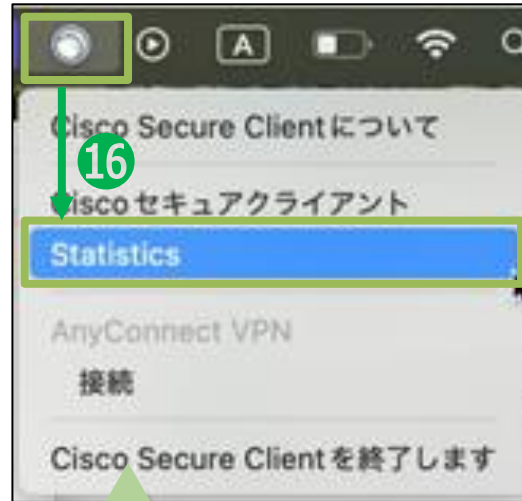


4-3. インストール手順 <ダウンロードしたインストーラの実行-6>

👉 「許可」を選択

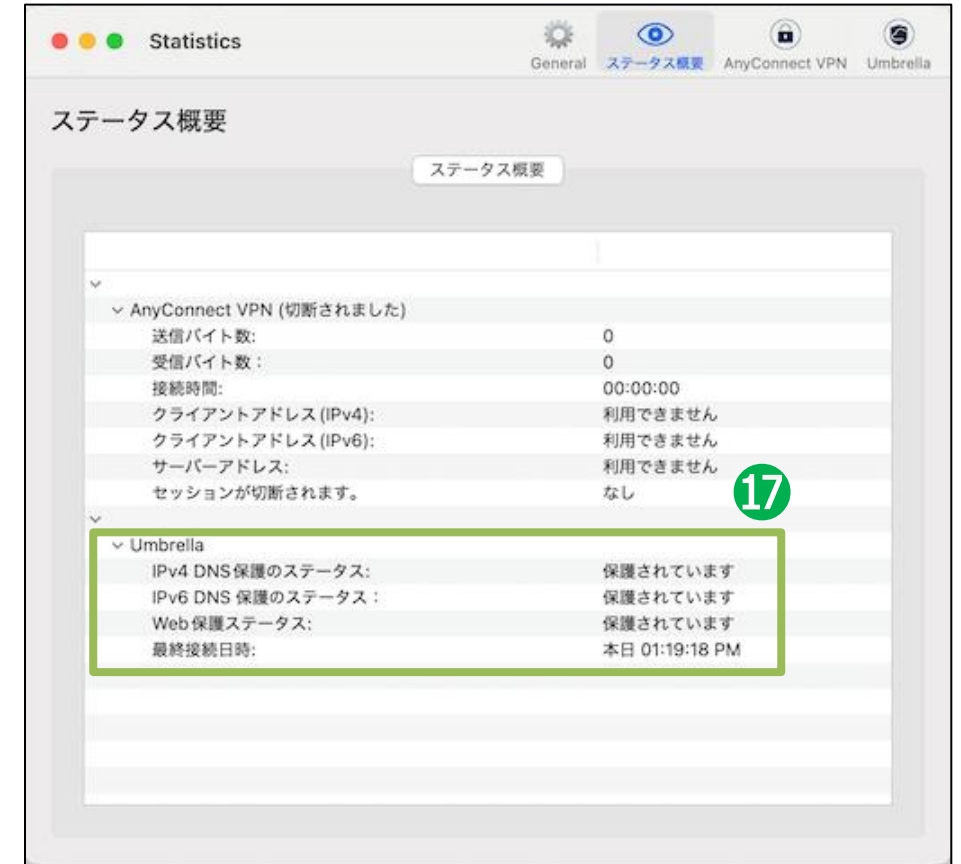


👉 「Statistics」を選択



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

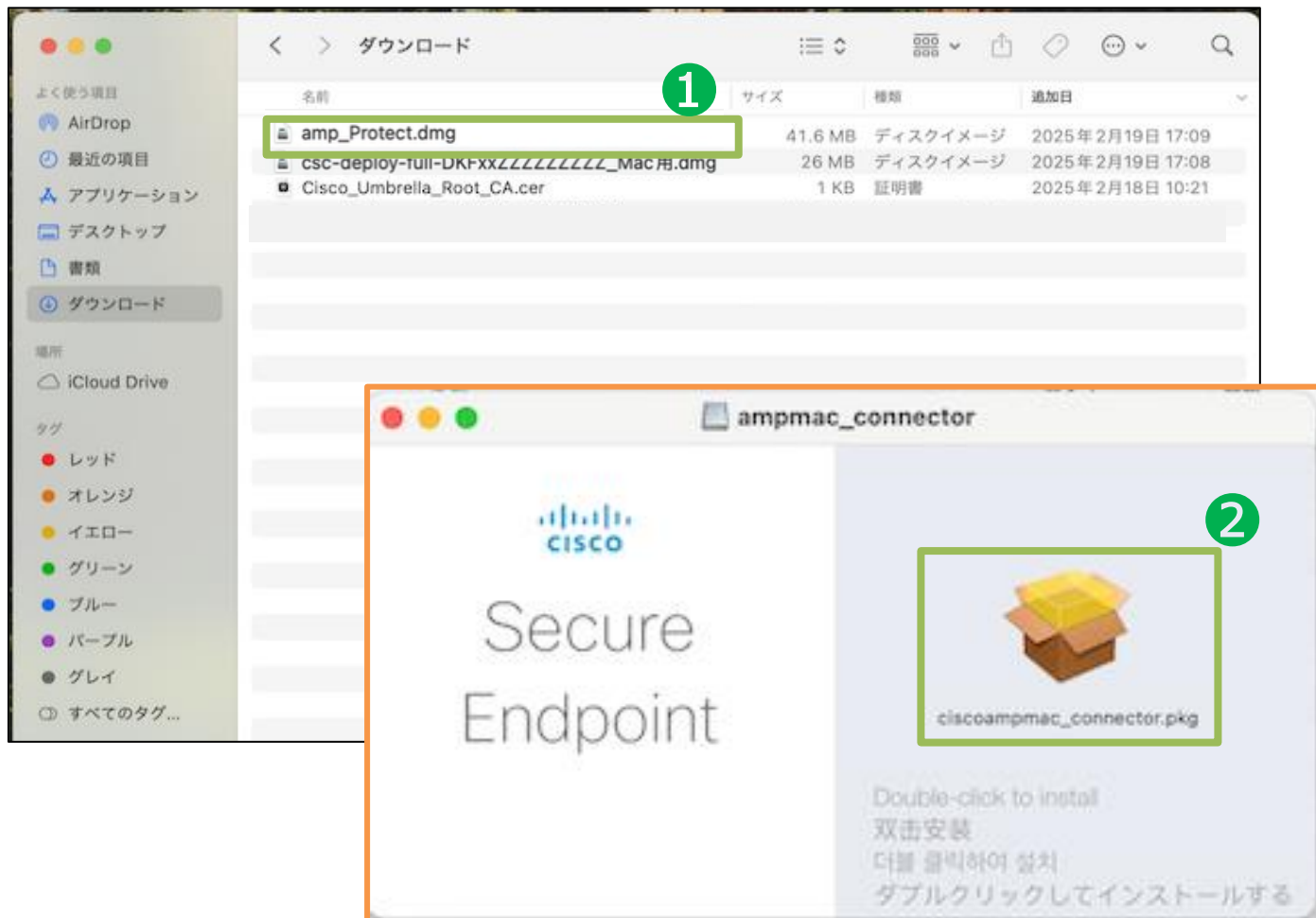
👉 Umbrellaの「IPv4DNS保護のステータス」が「保護されています」、
「Web保護ステータス」が「保護されています」であることを確認



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



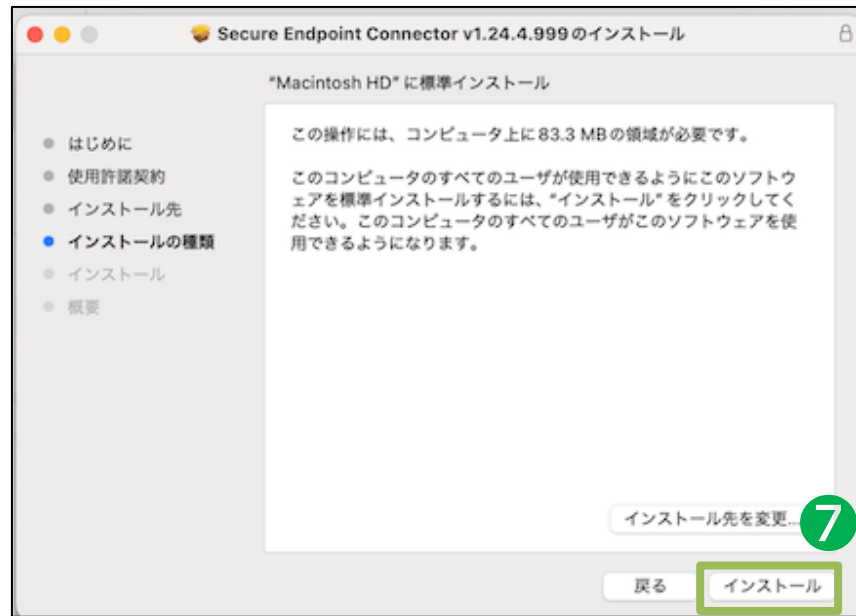
👉 「続ける」を選択



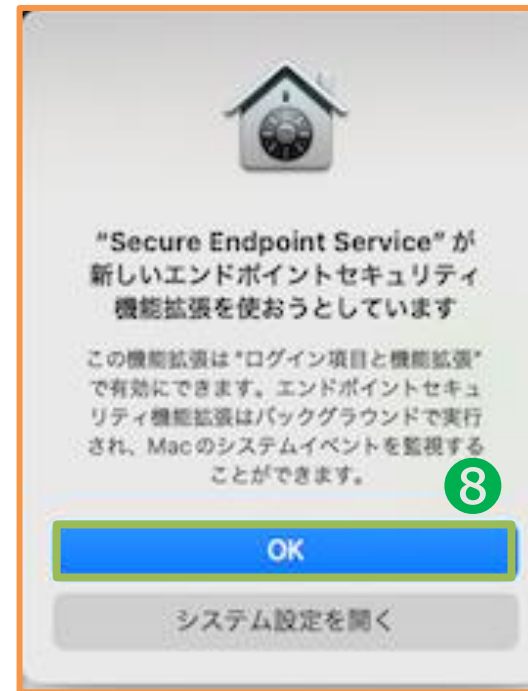
4-3. インストール手順 <ダウンロードしたインストーラの実行-9>

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

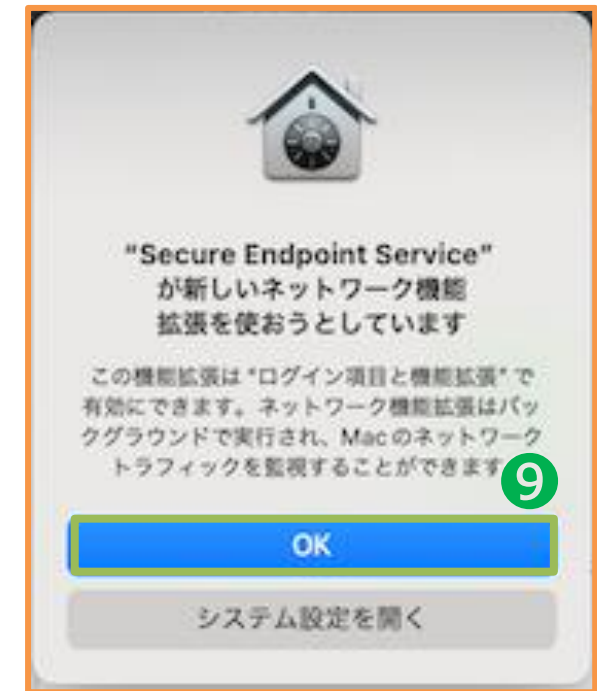
👉 「インストール」を選択



👉 「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「 ⓘ 」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



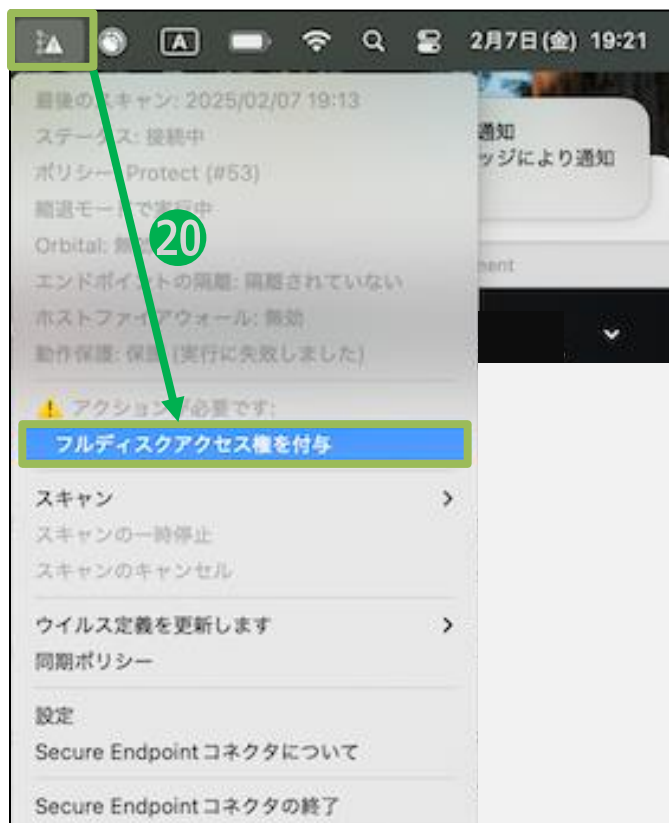
👉 「完了」を選択



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



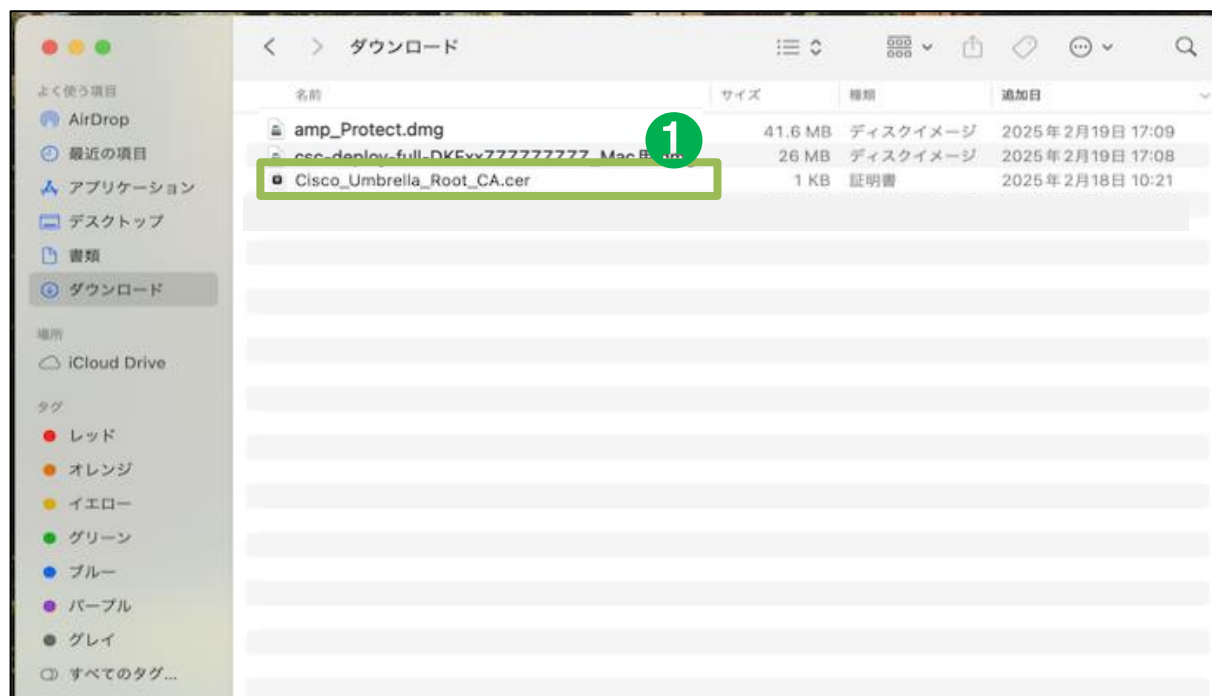
👉 追加アクション要求「」がなくなっていることを確認



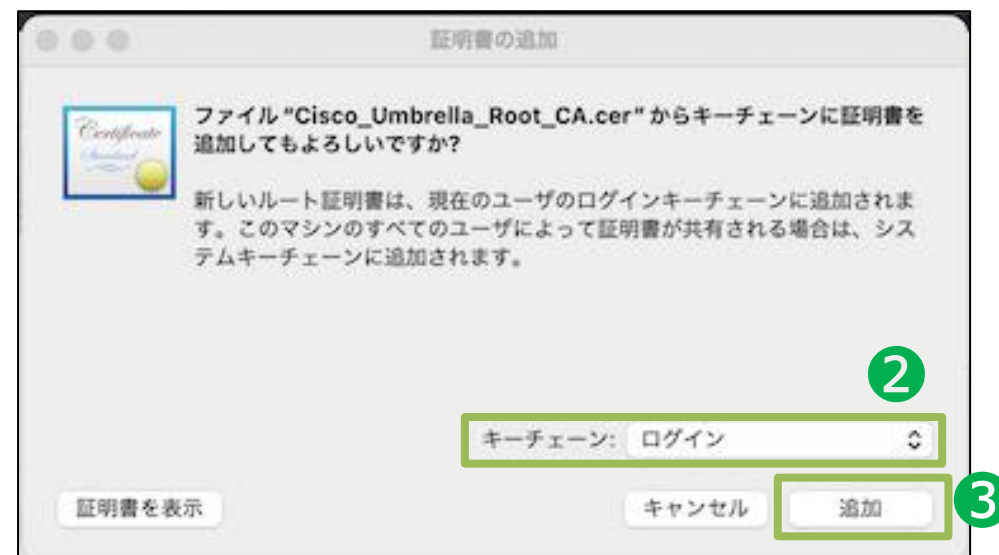
4-3. インストール手順＜ダウンロードしたインストーラの実行-14＞

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

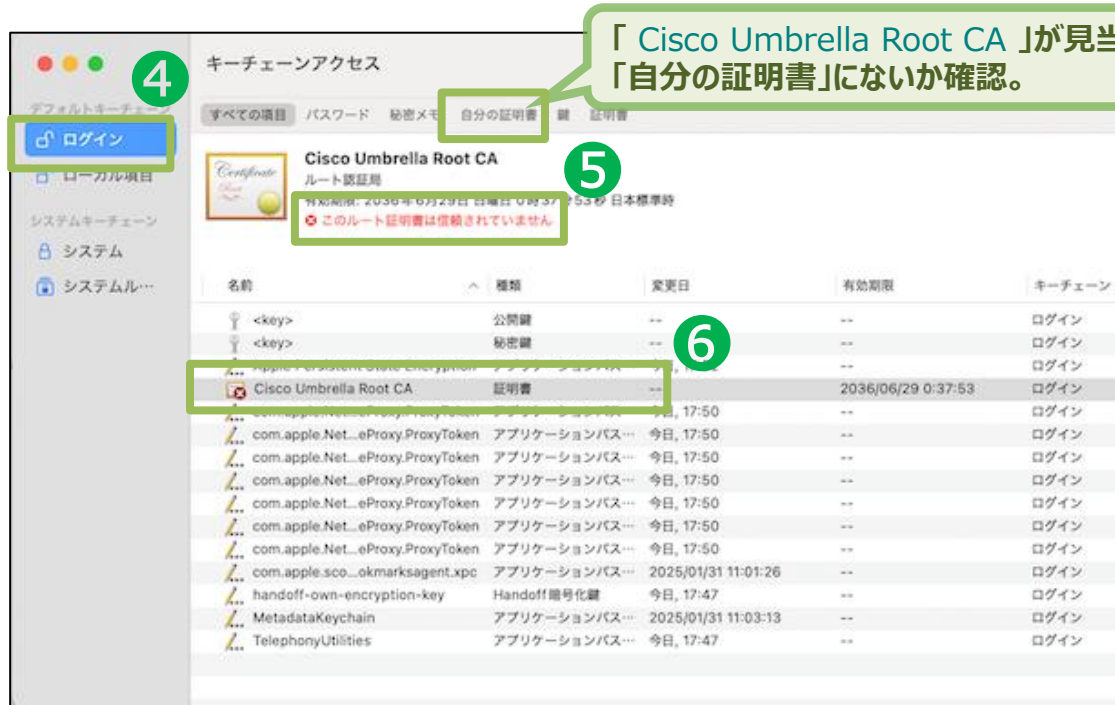


4-3. インストール手順 <ダウンロードしたインストーラの実行-15>

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

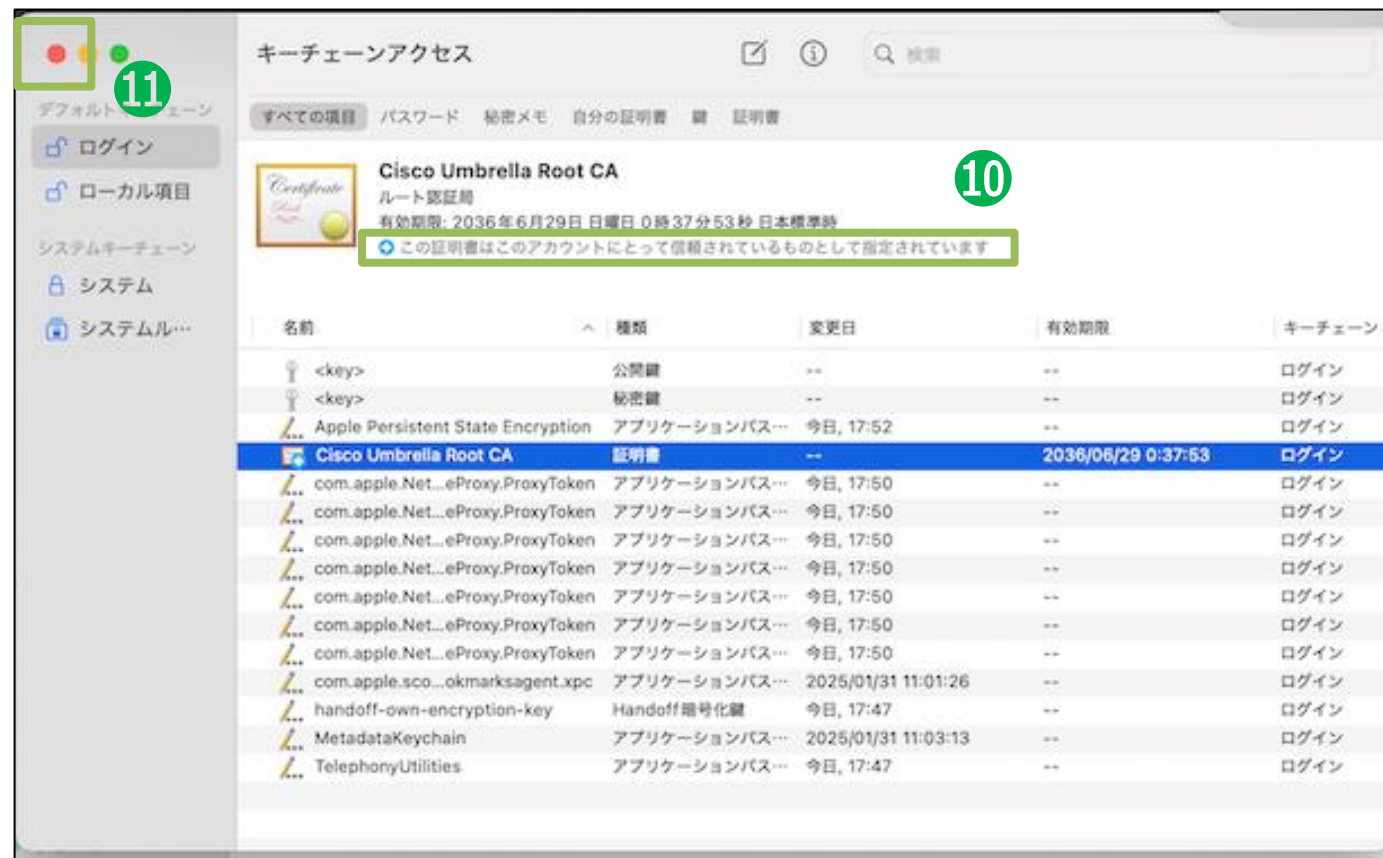


4-3. インストール手順 <ダウンロードしたインストーラの実行-16>

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

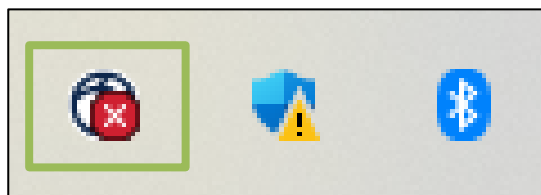


4-4. ソフトウェアの起動／ステータス確認_Windows

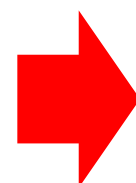
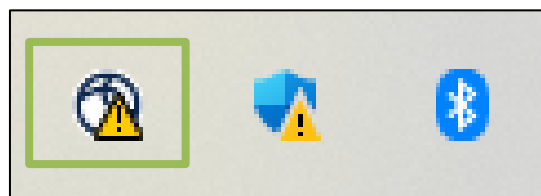
4-4. インストール手順＜ソフトウェアの起動／ステータス確認-1＞

- 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

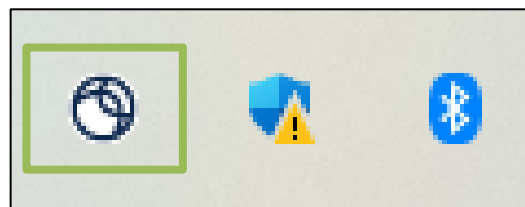


または



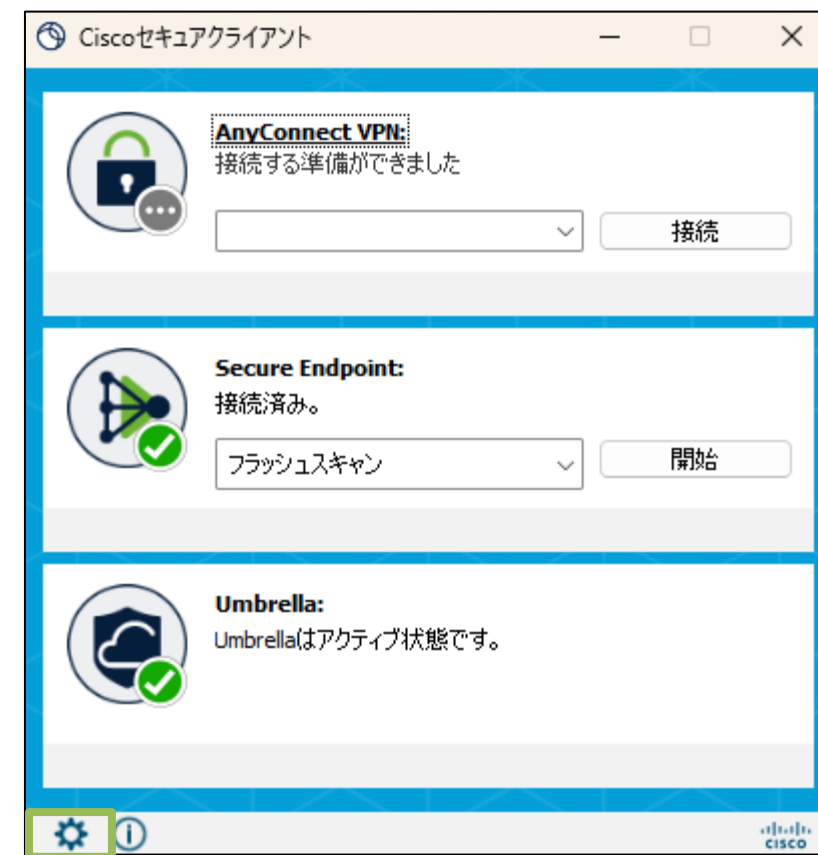
5分程度
待機

② 初期設定完了



👉 初期設定完了状態でクリック

③ セキュアクライアントホーム画面



※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。

👉 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



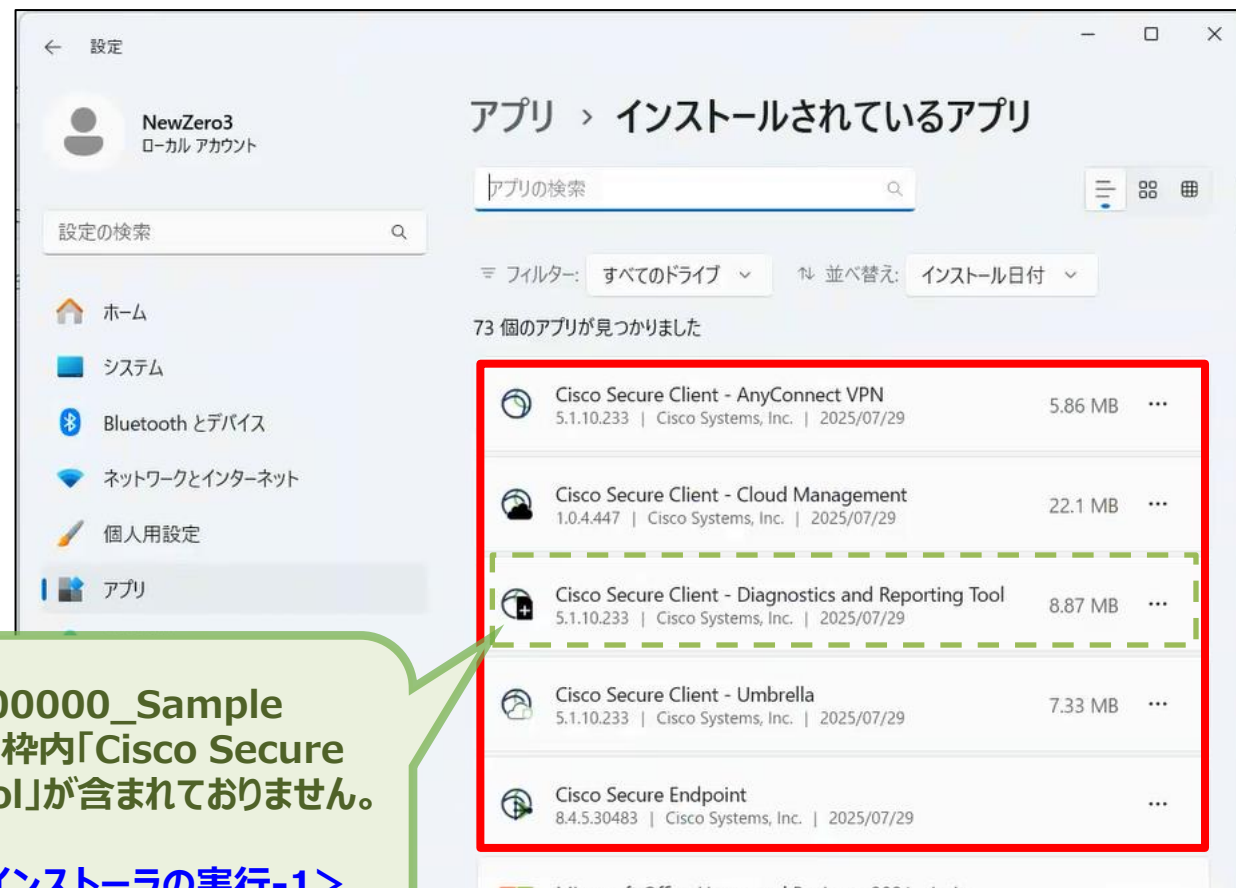
4-4. インストール手順＜ソフトウェアの起動／ステータス確認-3＞

- 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

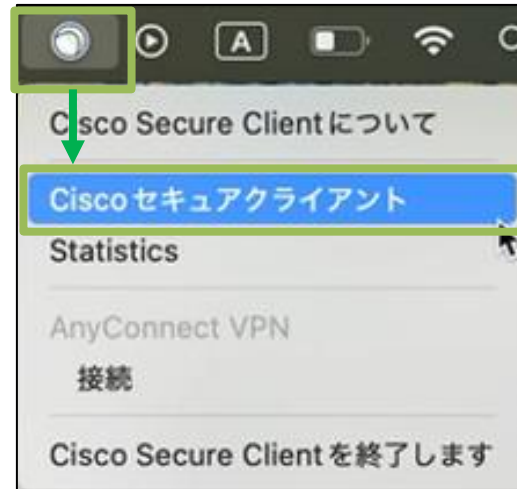


②初期設定完了



インストール設定後
自動遷移

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



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

⑤初期設
定中



⑥初期設定
完了



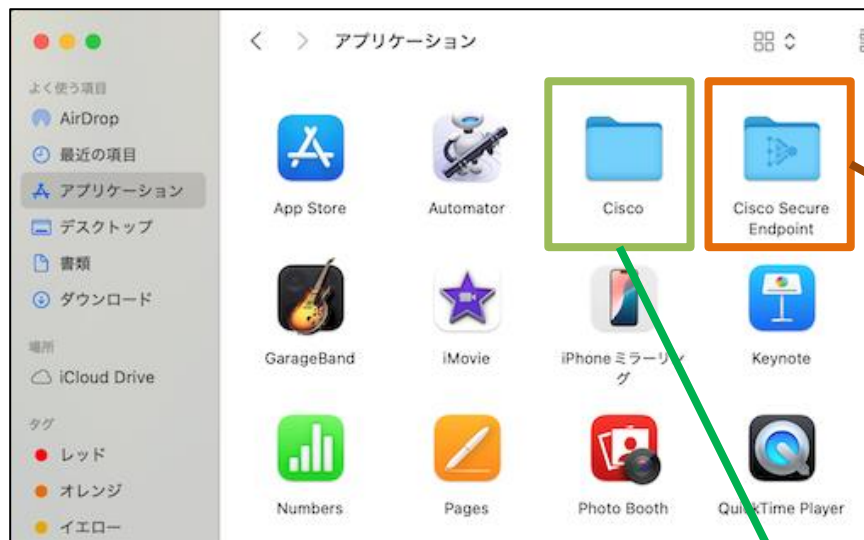
⑦セキュアエンドポイント
ステータス



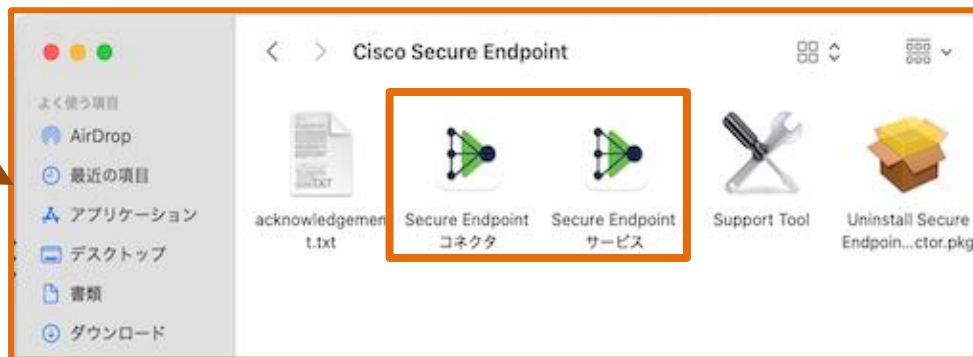
インストール設定後
自動遷移

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-3>

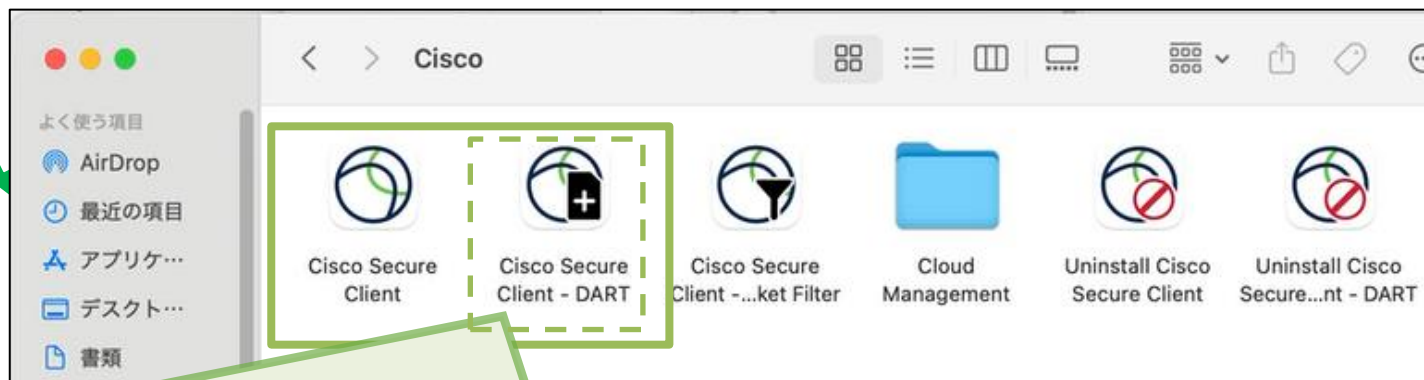
⑧Finderから「Cisco」、「Cisco Secure Endpoint」フォルダを開き、「Secure Endpoint コネクタ」、「Secure Endpointサービス」、「Cisco Secure Client」、「Cisco Secure Client-DART（※）」がインストールされていることを確認



👉 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。

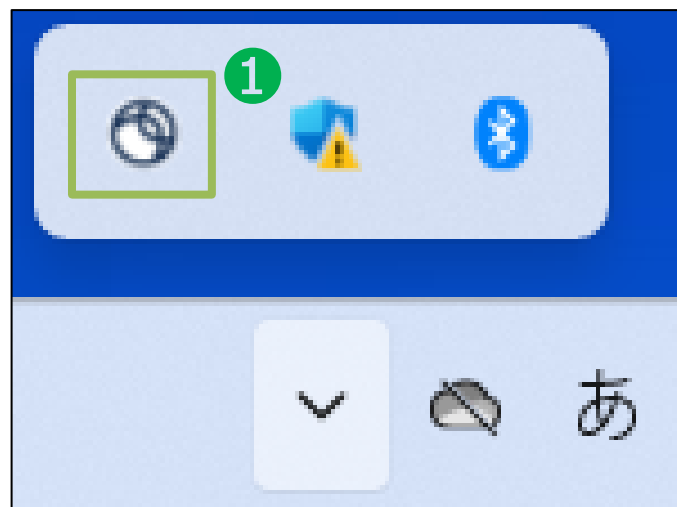
参照：4-3. インストール手順<ダウンロードしたインストーラの実行-1>

5. ソフトウェアのアンインストール手順_Windows

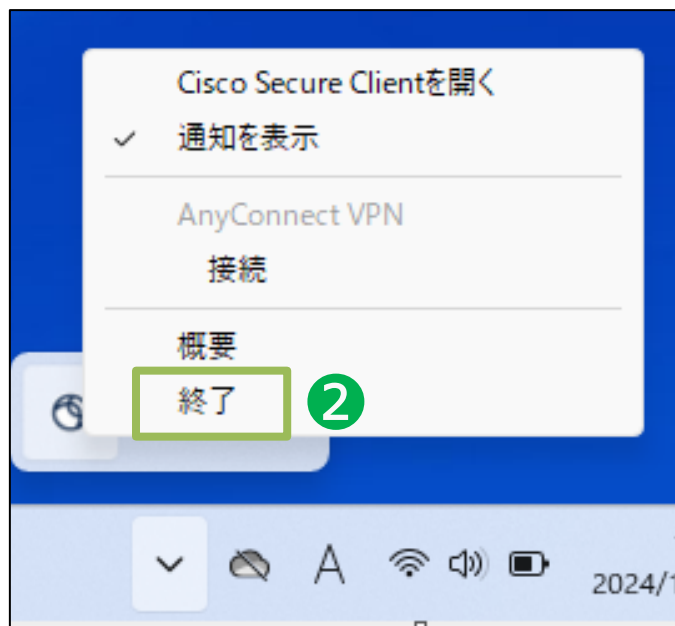
5. アンインストール手順 <Cisco Secure Clientの停止-1>

実行中のCisco Secure Clientを停止させてください。

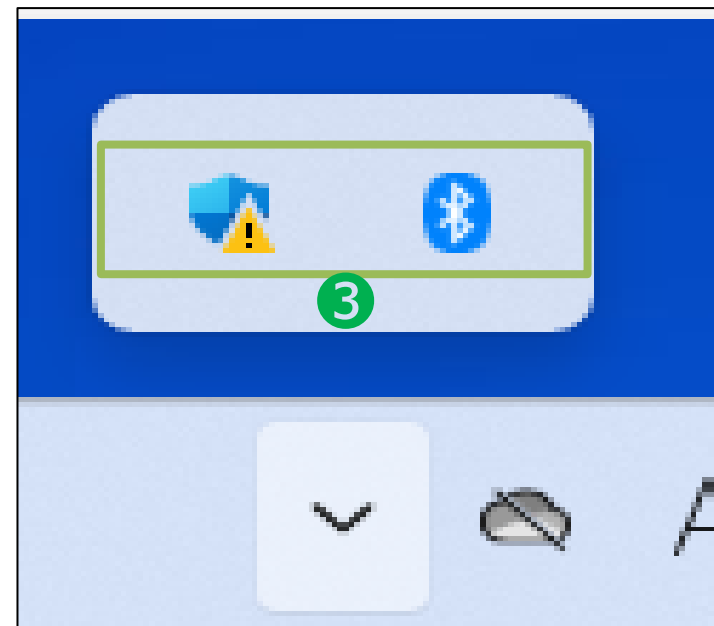
タスクバーから「Cisco Secure Client」を右クリック



「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



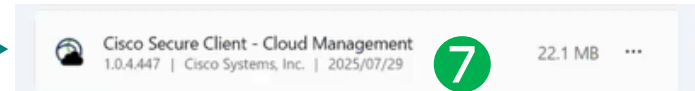
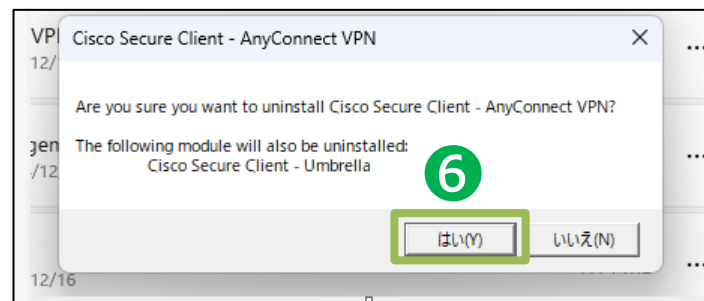
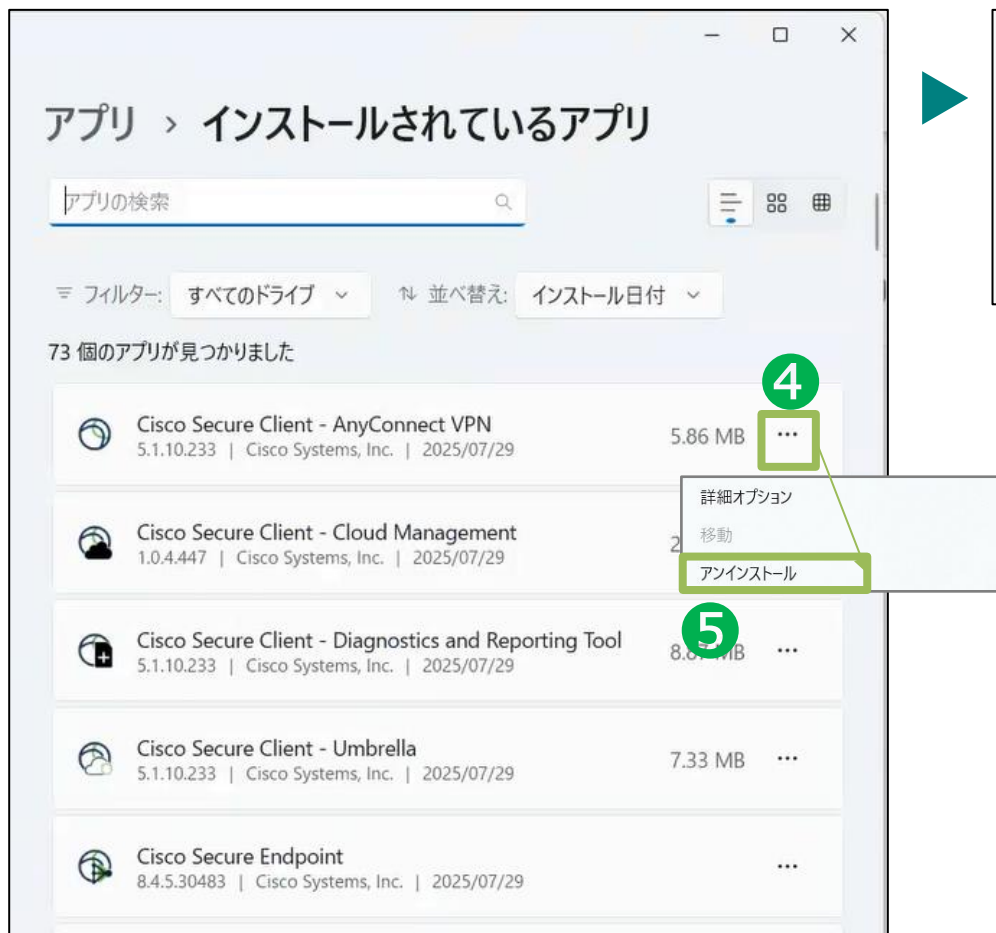
5. アンインストール手順 <ソフトウェアのアンインストール-1>

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

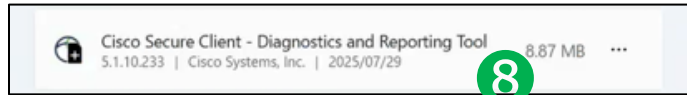
同様の手順で「Cisco Secure Client – Cloud Management」をアンインストール



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。

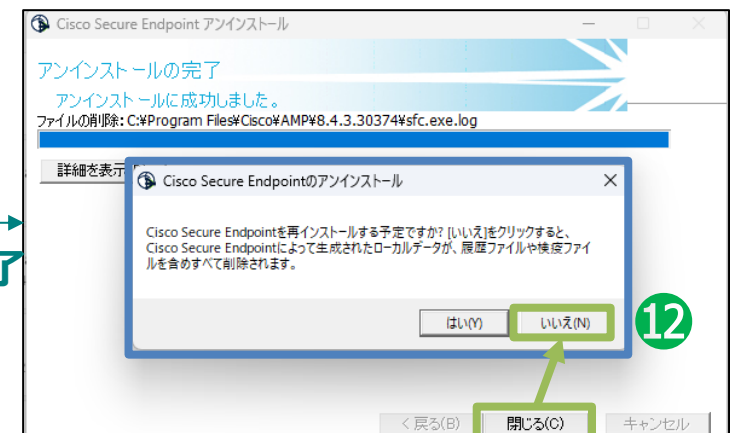
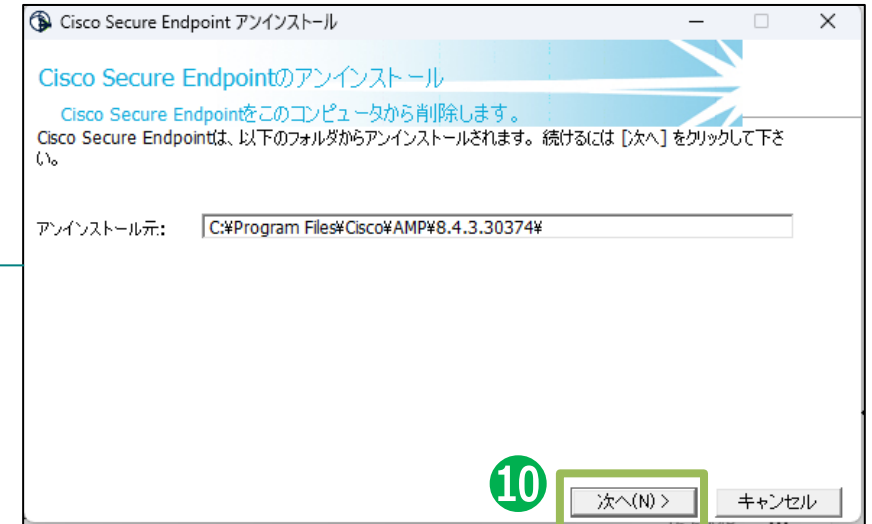
「Cisco Secure Client – Diagnostics and Reporting Tool」をアンインストール (※)



「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。

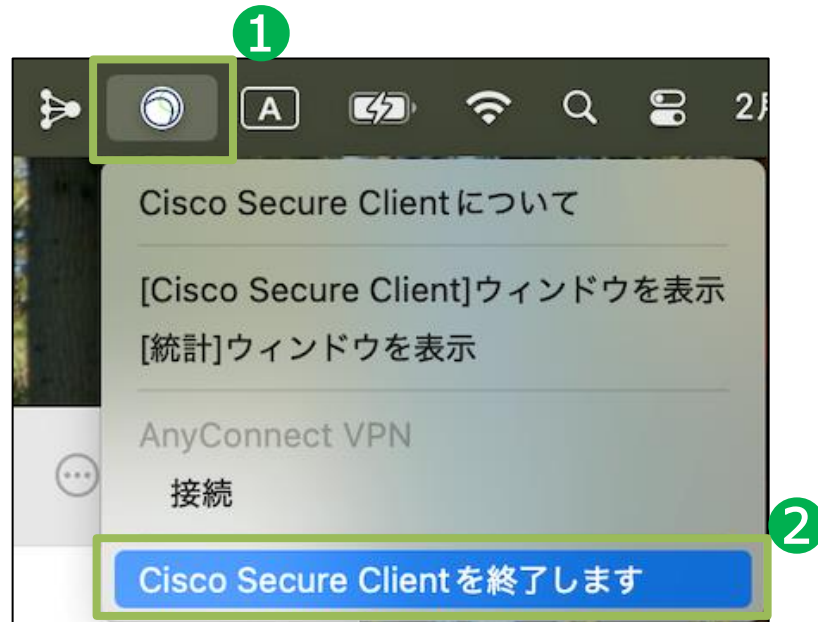
参照 : [4-3. インストール手順 <ダウンロードしたインストーラの実行-1>](#)

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。

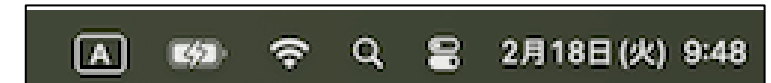
画面右上の「Cisco Secure Client」を
クリックし、終了させる



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



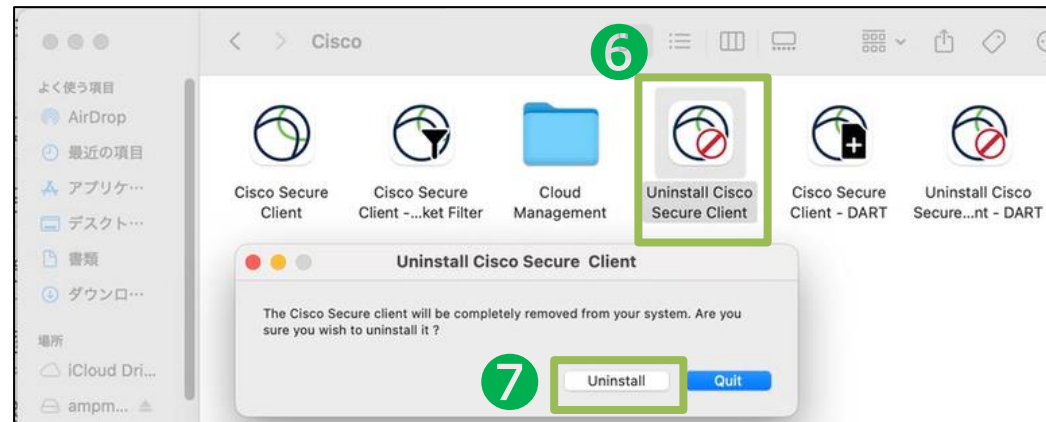
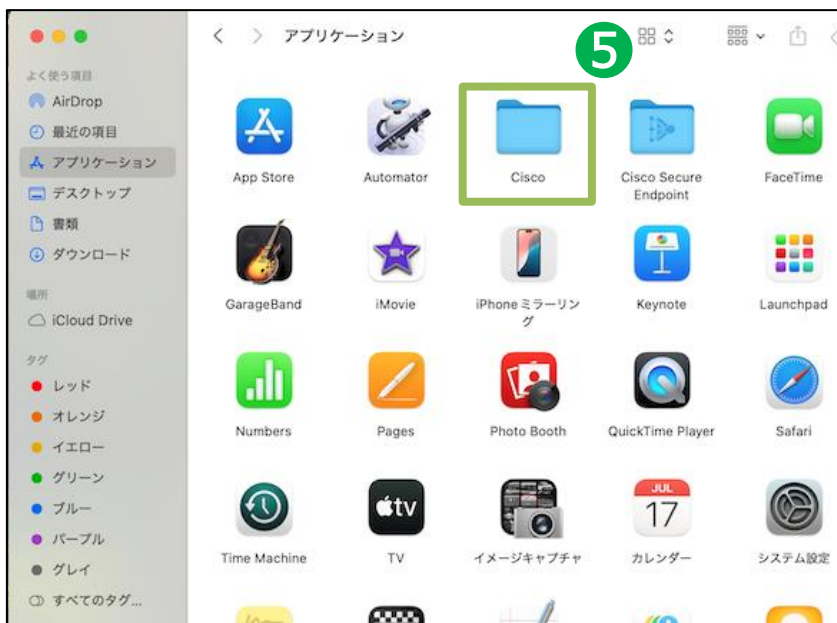
5. アンインストール手順 <ソフトウェアのアンインストール-1>

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



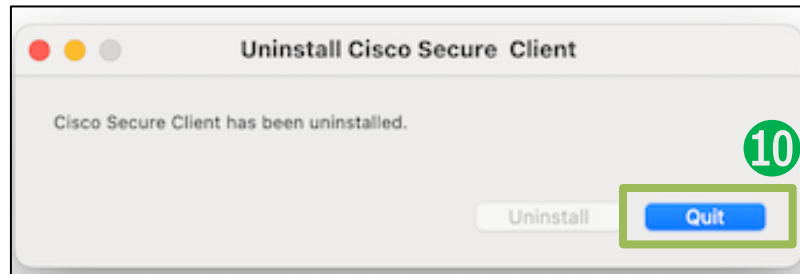
5. アンインストール手順 <ソフトウェアのアンインストール-2>

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>](#)

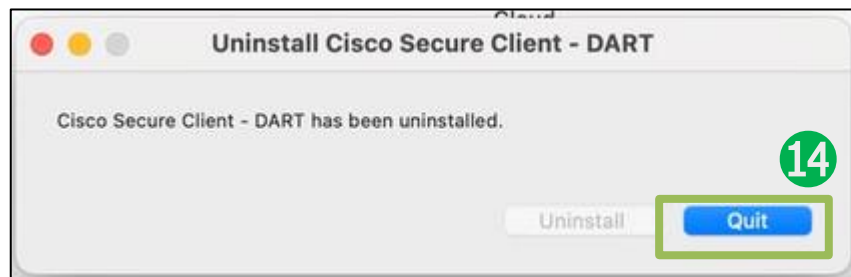
5. アンインストール手順 <ソフトウェアのアンインストール-3>

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。

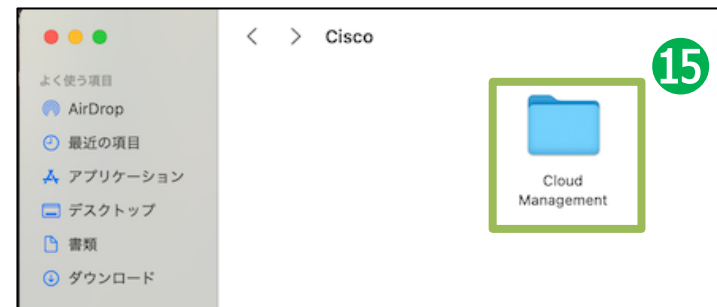
続けてパスワードを入力し
「OK」を選択



「Quit」を選択して閉じる



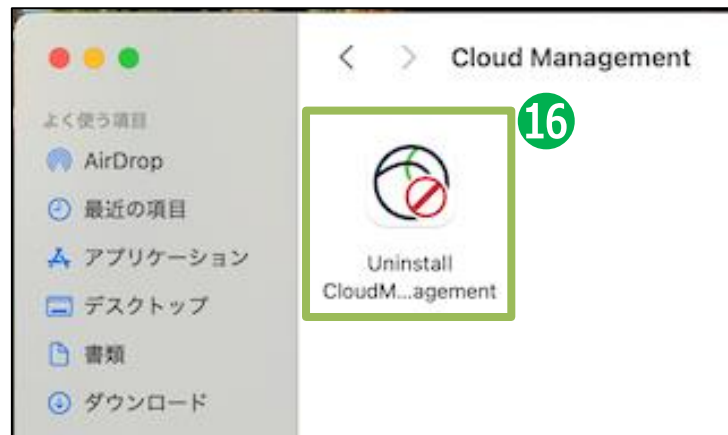
Ciscoフォルダに残った
「Cloud Management」フォルダを開く



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。

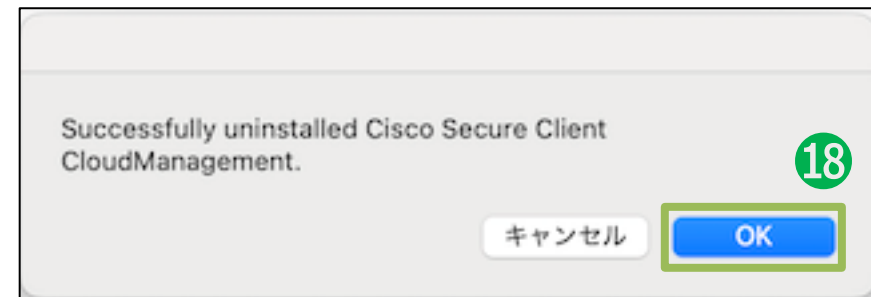
「Uninstall CloudManagement」を
ダブルクリック



パスワードを入力し、
「OK」を選択



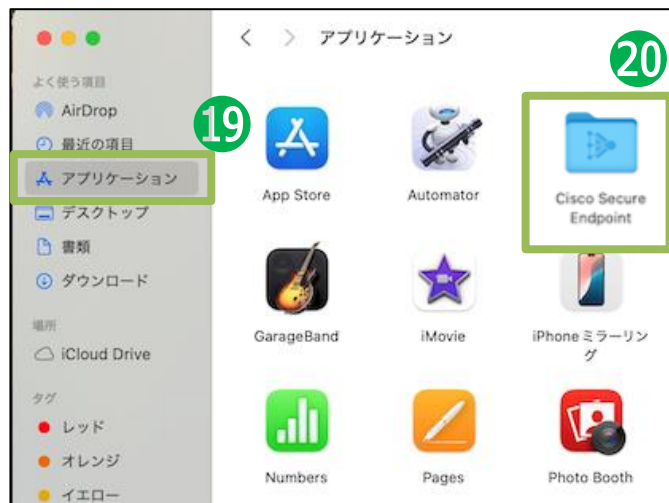
「OK」を選択



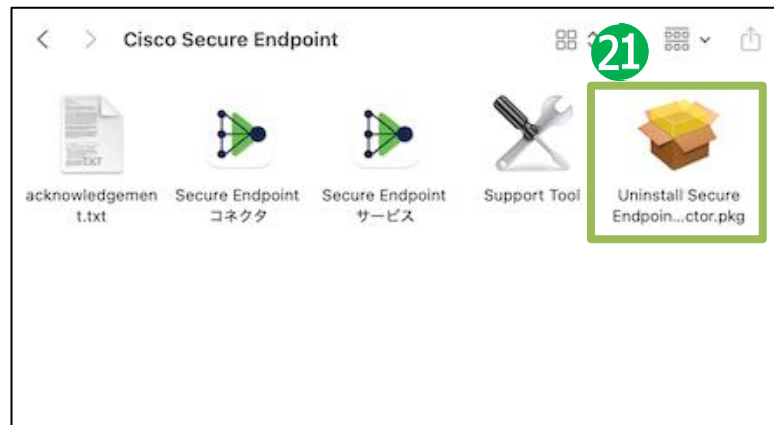
5. アンインストール手順 <ソフトウェアのアンインストール-5>

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



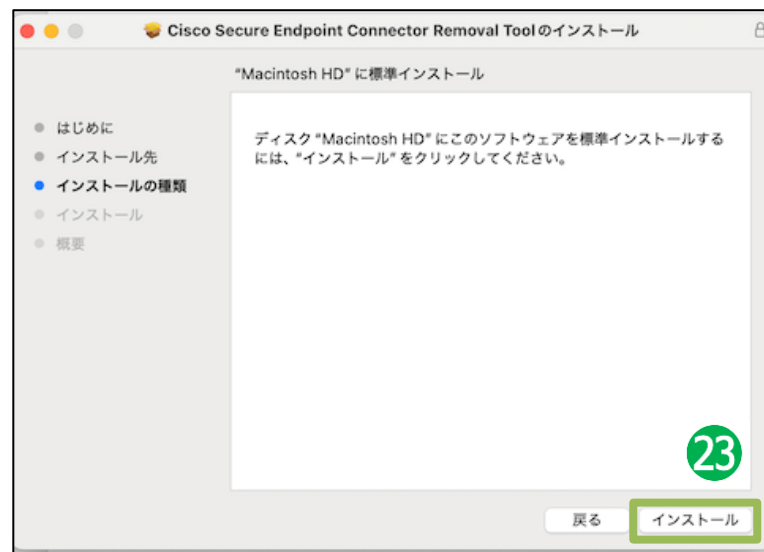
「続ける」を選択



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



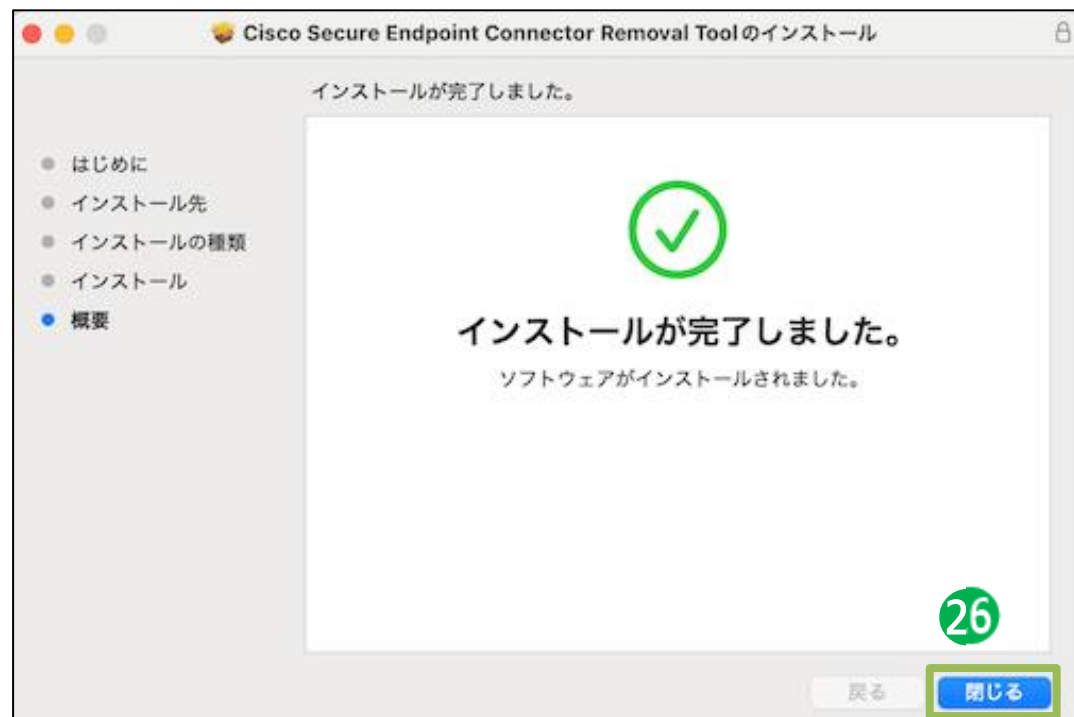
続けて、パスワードを入力し、
「OK」を選択



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>

管理者向けのインベ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。

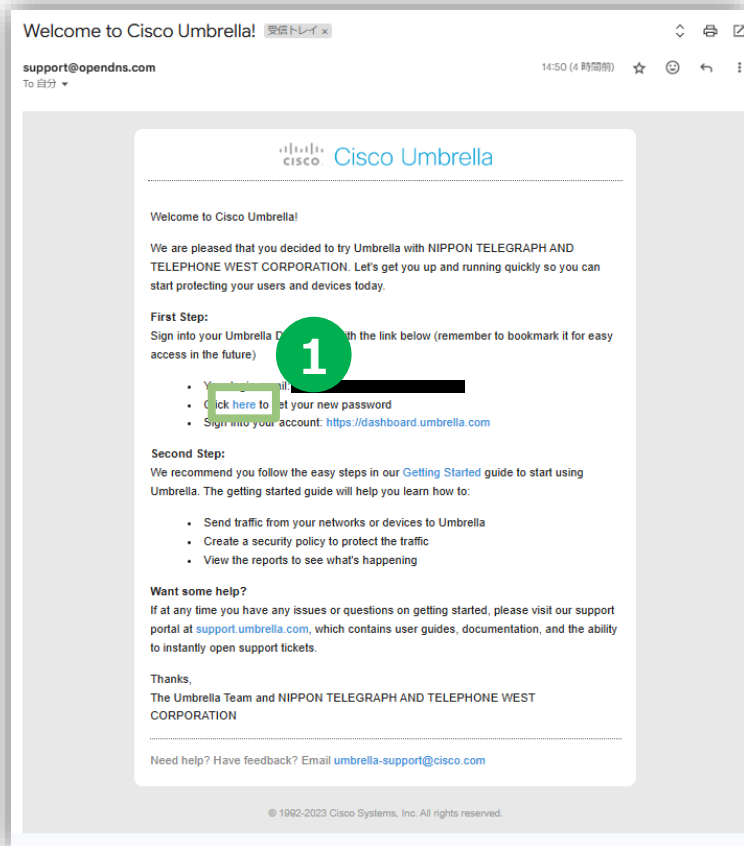
- ① 1人目の管理者は受信した電子メールから枠内の[here]をクリック
2人目の管理者は受信した電子メールから枠内の [click this link]をクリック

- ② [氏名]、[電子メール※¹]、[パスワード※²]を入力

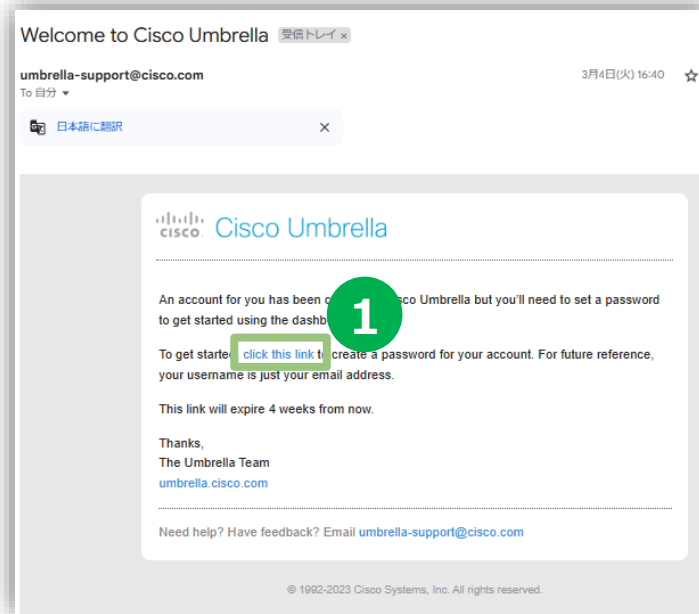
※¹電子メールには申込書に記載したメールアドレスを記載ください ※²設定するパスワードには条件があります（図の② 下部をご参照ください）

- ③ [パスワードのリセット]をクリック

1人目の管理者



2人目の管理者



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
- ユーザー名の一部を含めることはできません

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>

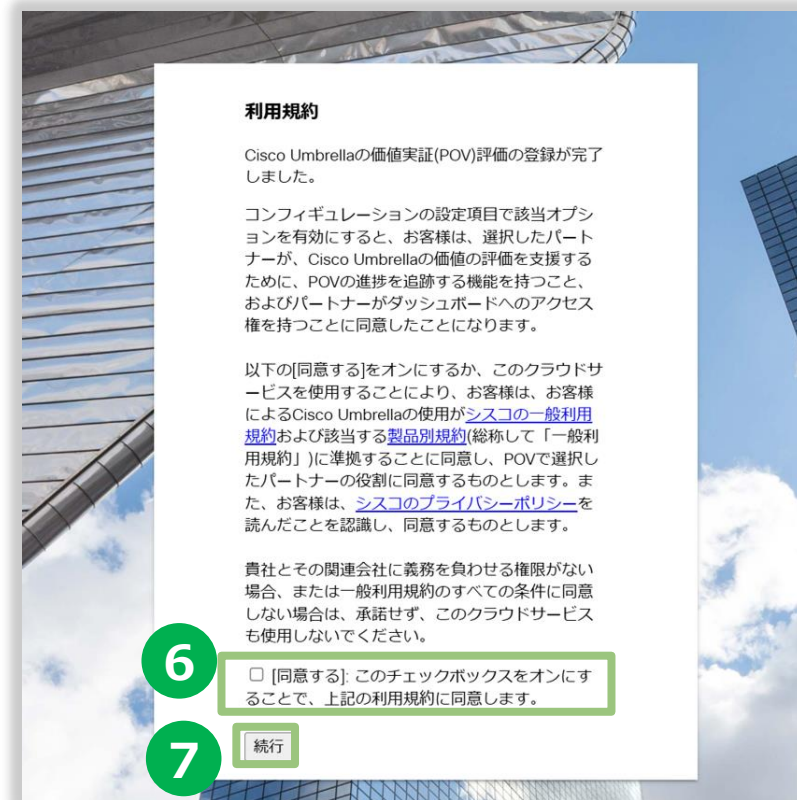
- ④ 前手順で入力した[電子メールアドレス]と[パスワード]を入力
- ⑤ [ログイン]をクリック
- ⑥ [同意する]のチェックボックスをクリック
- ⑦ [続行]をクリック



The login screen for Cisco Umbrella. At the top is the Cisco logo and the text "Cisco Umbrella". Below this is a green checkmark icon and a message: "パスワードが正常に更新されました。新しいパスワードを使用してログインしてください。" (Your password has been successfully updated. Please use your new password to log in). There are two input fields: "電子メールアドレス" (Email address) with a person icon and "パスワード" (Password) with a lock icon. Below the password field is a link: "パスワードを忘れた場合 | シングルサインオン" (Forgot your password? | Single sign-on). At the bottom is a blue "ログイン" (Login) button. A green circle with the number "4" is next to the input fields, and a green circle with the number "5" is next to the login button.

4

5



The Terms of Use screen for Cisco Umbrella. At the top is the title "利用規約" (Terms of Use). Below this is a paragraph: "Cisco Umbrellaの価値実証(POV)評価の登録が完了しました。" (Your registration for the Cisco Umbrella Value Proposition (POV) evaluation is complete). Another paragraph follows: "コンフィギュレーションの設定項目で該当オプションを有効にすると、お客様は、選択したパートナーが、Cisco Umbrellaの価値の評価を支援するために、POVの進捗を追跡する機能を持つこと、およびパートナーがダッシュボードへのアクセス権を持つことに同意したことになります。" (When you enable the corresponding option in the configuration settings, you agree that the selected partner will be able to track the progress of the POV to support the evaluation of the value of Cisco Umbrella, and that the partner will have access to the dashboard). Below this is a paragraph: "以下の[同意する]をオンにするか、このクラウドサービスを使用することにより、お客様は、お客様によるCisco Umbrellaの使用がシスコの一般利用規約および該当する製品別規約(総称して「一般利用規約」)に準拠することに同意し、POVで選択したパートナーの役割に同意するものとします。また、お客様は、シスコのプライバシーポリシーを読んだことを認識し、同意するものとします。" (By turning on the following [I agree] or by using this cloud service, you agree that your use of Cisco Umbrella complies with Cisco's General Terms of Use and applicable product-specific terms (collectively, "General Terms of Use"), and you agree to the role of the partner selected in the POV. You also acknowledge and agree that you have read and understand Cisco's Privacy Policy). At the bottom is a checkbox: "[同意する]: このチェックボックスをオンにすることで、上記の利用規約に同意します。" (I agree: By turning on this checkbox, I agree to the above terms of use). Below the checkbox is a "続行" (Continue) button. A green circle with the number "6" is next to the checkbox, and a green circle with the number "7" is next to the continue button.

6

7

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

Cisco Umbrellaのセットアップ

ネットワークの追加

ネットワークを保護する

これにより、そのネットワークのIPスペース内からインターネットに接続するすべてのデバイスの保護を拡張できます。

最初に、パブリックDNSを次のCisco Umbrella DNSサーバに向けてます。

IPv4: 208.67.220.220 と 208.67.222.222

これを実行する方法の詳細と、カスタマイズされたルータの手順については、[ここをクリックしてください。](#)

次に、ネットワークの名前を作成します。

ネットワーク名

マイ ネットワーク

このネットワークは次を使用します:

☒ IPv4のみ

☐ IPv6のみ

☐ IPv4とIPv6の混在

IPv4アドレス

0.0.0.0 / 32

⑧ ネットワークの検証を求める電子メールがシスコから届きます。

手順をスキップ 8 次へ



Cisco Umbrellaのセットアップ

ローミングコンピュータの追加

ローミングコンピュータの保護

ネットワークの内外のラップトップやデスクトップを保護できます。シスコの軽量クライアントは環境内のエンドポイントの保護を拡張します。

Cisco Umbrellaローミングクライアント

 Download Windows Client
Supported Versions: Windows 7, 8, 10

 Download Mac OS X Client
Supported Versions: OS X 10.9+

より高度なセットアップの手順については、シスコの[ローミングクライアントのセットアップガイド](#)を参照してください。

AnyConnectを使用する場合

AnyConnectを使用する場合は、スタンドアロンのUmbrellaローミングクライアントよりも統合Umbrellaローミングセキュリティモジュールをお勧めします。

手順については、[AnyConnectクライアントのセットアップガイド](#)を参照してください。

9 この手順をスキップ 前へ 次へ



Cisco Umbrellaのセットアップ

セットアップが完了しました

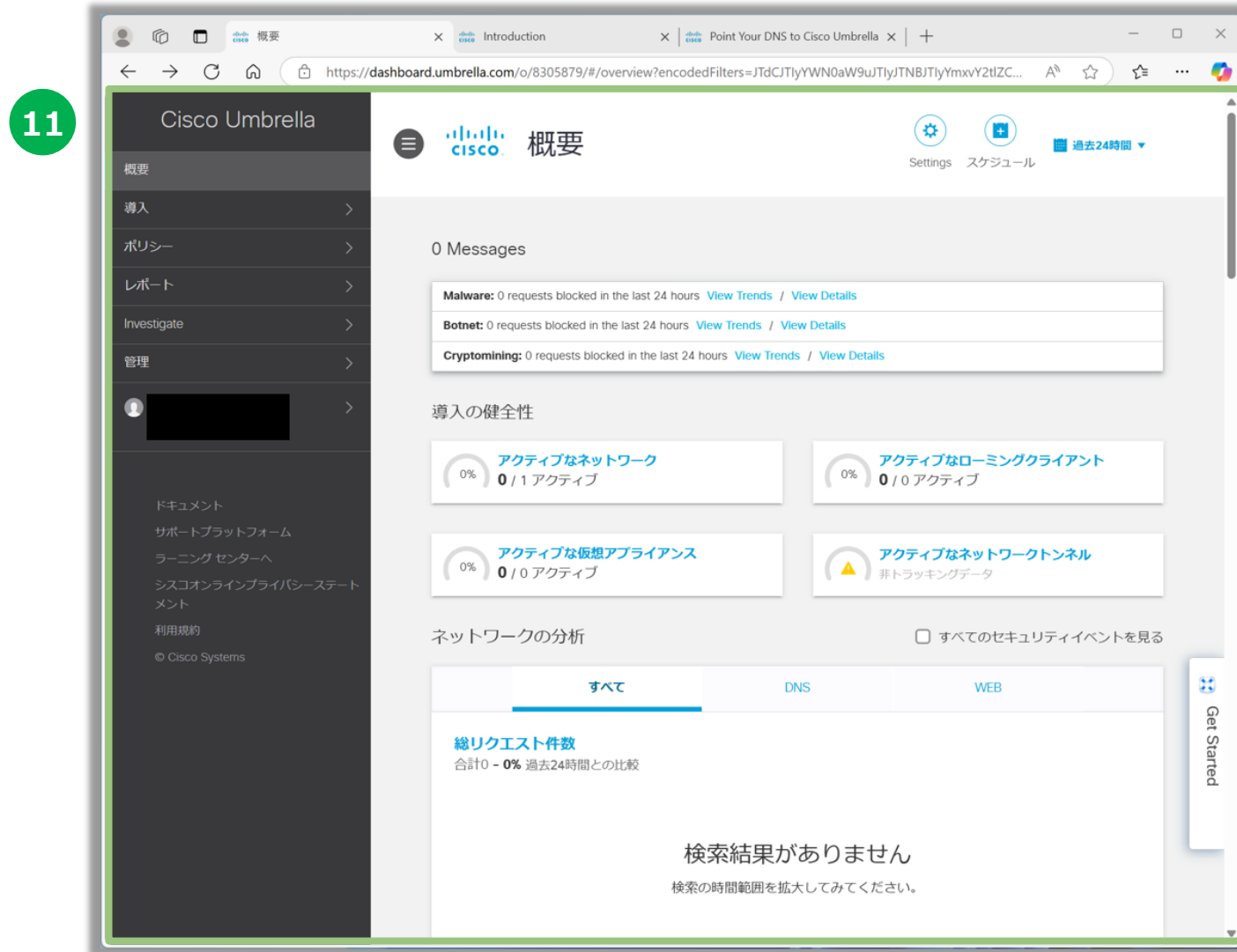
完了後の推奨事項

Cisco Umbrellaの使用を開始できます。ただし、シスコの製品を最大限に活用するために、ネットワークやローミングコンピュータをセットアップすることをお勧めします。これは、ダッシュボードから実行できます。

10 前へ CISCO UMBRELLAの使用の開始

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。

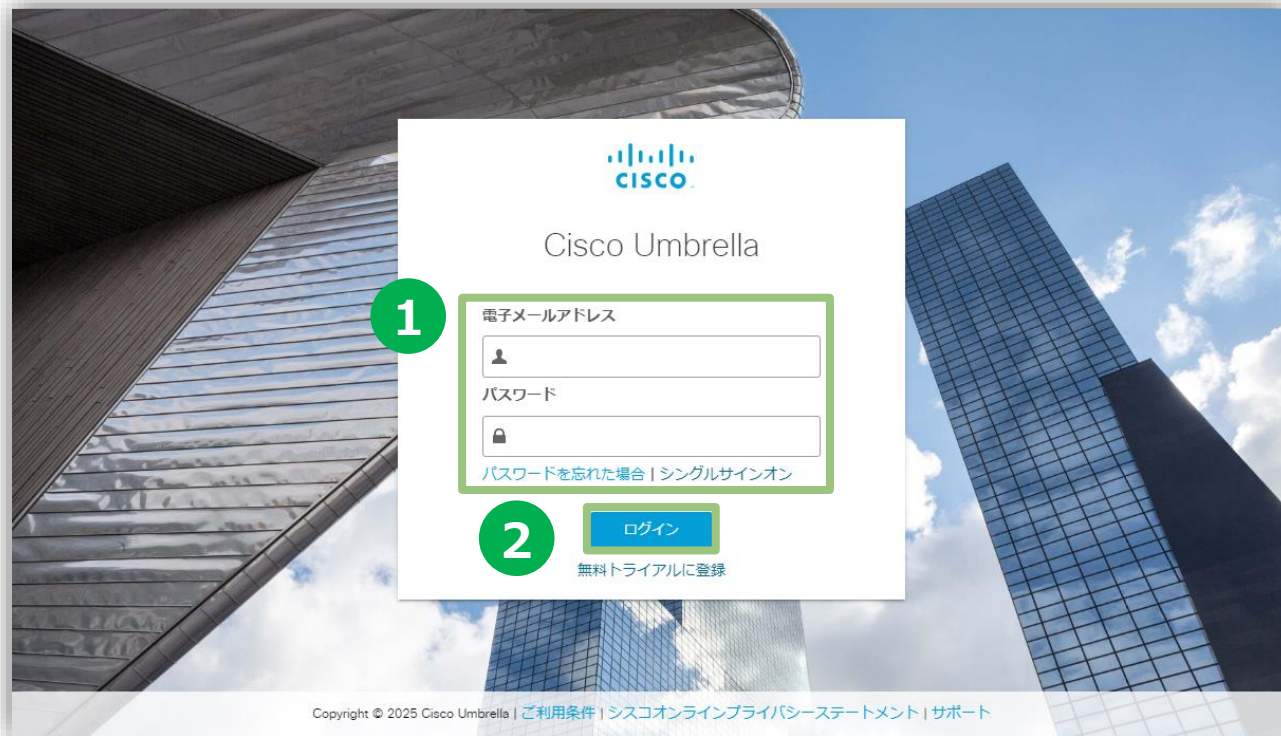


6. コンソールへのログイン手順 <システムログイン>

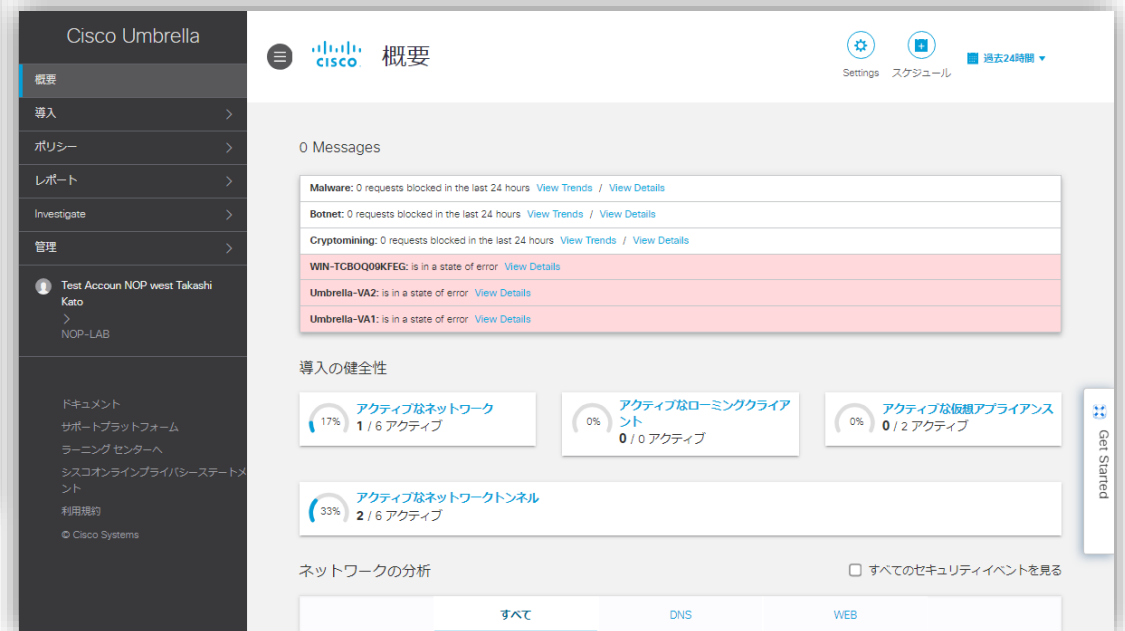
各ユーザテナントへのCisco Umbrellaへのログイン方法を示します

- 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



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 shows the Cisco Umbrella dashboard interface. On the left is a dark sidebar with the 'Cisco Umbrella' logo and a menu. The '概要' (Overview) menu item is highlighted. The main content area has a top bar with the Cisco logo, the title '概要', and links for 'Settings' and 'スケジュール' (Schedule). A dropdown menu shows '過去24時間' (Last 24 hours). Below this, a section titled '0 Messages' contains a list of security alerts: 'Malware: 0 requests blocked in the last 24 hours', 'Botnet: 0 requests blocked in the last 24 hours', 'Cryptomining: 0 requests blocked in the last 24 hours', and three error messages for 'WIN-TCBOQ09KFEG', 'Umbrella-VA2', and 'Umbrella-VA1'. The '導入の健全性' (Onboarding Health) section features four cards: 'アクティブなネットワーク' (17% active, 1/6 total), 'アクティブなローミングクライアント' (0% active, 0/0 total), 'アクティブな仮想アプライアンス' (0% active, 0/2 total), and 'アクティブなネットワークトンネル' (33% active, 2/6 total). At the bottom, the 'ネットワークの分析' (Network Analysis) section has 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 filter bar with 'すべて' (All), 'DNS', and 'WEB' tabs.

Cisco Umbrella

概要

Settings スケジュール 過去24時間

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](#)

WIN-TCBOQ09KFEG: is in a state of error [View Details](#)

Umbrella-VA2: is in a state of error [View Details](#)

Umbrella-VA1: is in a state of error [View Details](#)

導入の健全性

17% アクティブなネットワーク 1 / 6 アクティブ

0% アクティブなローミングクライアント 0 / 0 アクティブ

0% アクティブな仮想アプライアンス 0 / 2 アクティブ

33% アクティブなネットワークトンネル 2 / 6 アクティブ

ネットワークの分析 ☐ すべてのセキュリティイベントを見る

すべて DNS WEB

Get Started

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

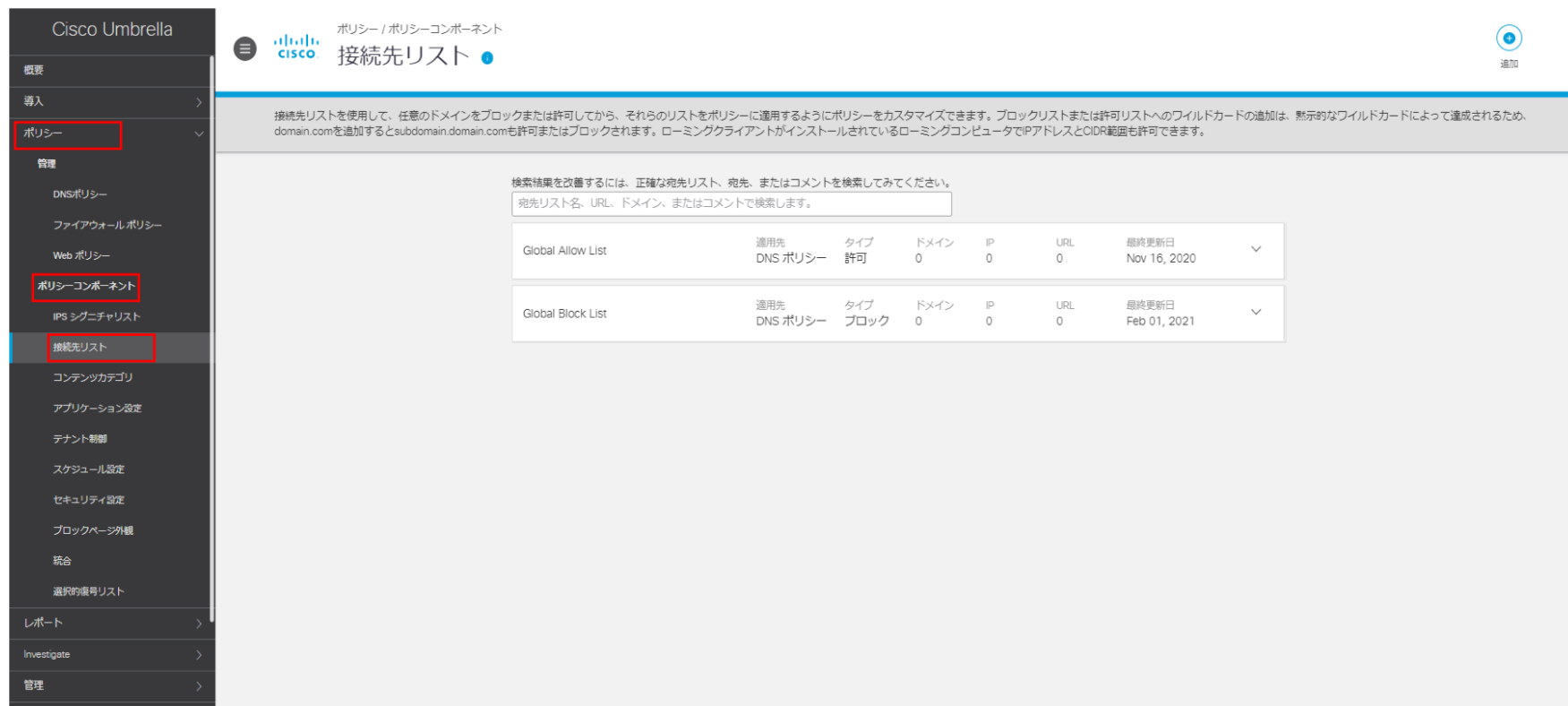
9. DNSポリシーを変更したい
10. 広告のページを開けるようにしたい
11. 怪しいサイトがUmbrellaの検知をすり抜けている
12. Umbrellaの許可リスト・ブロックリストを設定したい
13. CASB※の設定方法を知りたい
14. CASB※の機能を利用して組織が利用しているクラウドサービスの状況を確認したい
15. CASB※の機能を利用して会社が契約しているテナントにのみアクセスさせたい
16. Umbrellaでユーザの利用しているアプリの可視化をし、特定アプリをブロックしたい
17. 内部ドメインを参照したい

※ 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。



Cisco Umbrella

ポリシー / ポリシーコンポーネント

接続先リスト

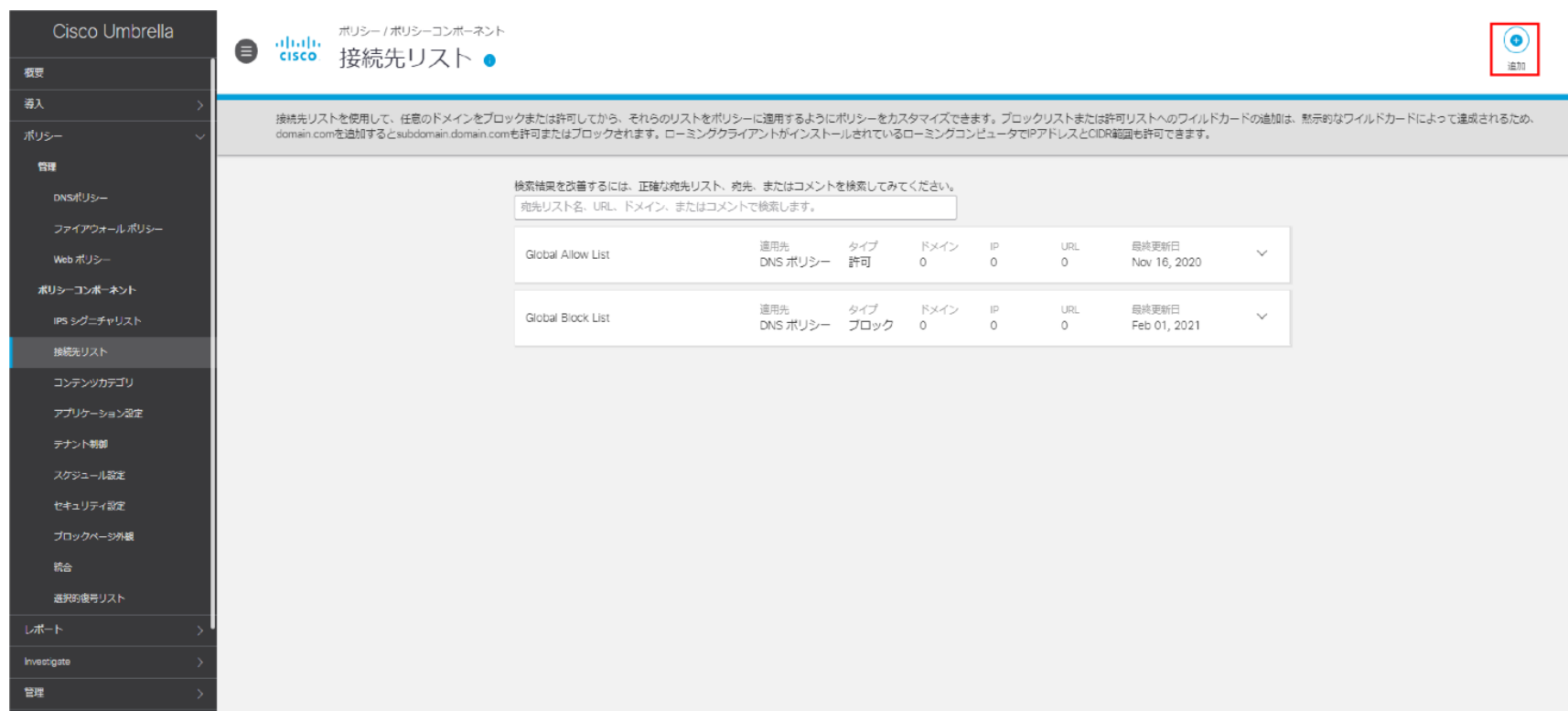
接続先リストを使用して、任意のドメインをブロックまたは許可してから、それらのリストをポリシーに適用するようにポリシーをカスタマイズできます。ブロックリストまたは許可リストへのワイルドカードの追加は、黙示的なワイルドカードによって達成されるため、domain.comを追加するとsubdomain.domain.comも許可またはブロックされます。ローミングクライアントがインストールされているローミングコンピュータでIPアドレスとCIDR範囲も許可できます。

検索結果を改善するには、正確な宛先リスト、宛先、またはコメントを検索してみてください。
宛先リスト名、URL、ドメイン、またはコメントで検索します。

Global Allow List	適用先 DNS ポリシー	タイプ 許可	ドメイン 0	IP 0	URL 0	最終更新日 Nov 16, 2020	▼
Global Block List	適用先 DNS ポリシー	タイプ ブロック	ドメイン 0	IP 0	URL 0	最終更新日 Feb 01, 2021	▼

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 interface for managing policies. The left sidebar contains navigation options like '概要' (Overview), '導入' (Import), 'ポリシー' (Policy), '管理' (Manage), '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 Components), 'IPS シグニチャリスト' (IPS Signature List), '接続先リスト' (Connect 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), and '選択的番号リスト' (Selective Number List). The main content area is titled 'ポリシー / ポリシーコンポーネント' (Policy / Policy Components) and '接続先リスト' (Connect List). It includes a search bar and a table of lists.

検索結果を改善するには、正確な宛先リスト、宛先、またはコメントを検索してみてください。
宛先リスト名、URL、ドメイン、またはコメントで検索します。

	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 is a dark sidebar with navigation links: 概要, 導入, ポリシー, 管理 (with sub-links for DNS, Firewall, and Web), ポリシーコンポーネント, 接続先リスト (highlighted), コンテンツカテゴリ, アプリケーション設定, デナント制御, 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, and Investigate. 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'. It includes a search bar and a section for '新しい接続先リスト'. In this section, the 'リスト名' (List Name) field contains 'テストDNSポリシー' and is highlighted with a red rectangle. Below it, the '送信先リストタイプ' (Destination List Type) is set to 'Select...'. There are radio buttons for 'ブロック' (selected) and '許可' (allowed). The '目的地' (Destination) field is empty. At the bottom, it says 'このリストに接続先が追加されていません' (No destinations added to this list) and '0 合計' (0 total). Pagination controls show 'Page: 1', 'Results per page: 10', and '1-0 of 0'. 'キャンセル' (Cancel) and '保存' (Save) buttons are at the bottom right.

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 is a dark sidebar with navigation links: 概要, 導入, ポリシー, 管理 (with sub-links for DNS, Firewall, and Web policies), ポリシーコンポーネント, 接続先リスト (highlighted), 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, and Investigate. The main header area includes the Cisco logo, the title 'ポリシー / ポリシーコンポーネント', and a sub-header '接続先リスト'. A blue '+ 追加' button is in the top right. Below the header is a grey informational box about connection lists. The main content area is titled '新しい接続先リスト' and contains a form with the following fields: '送信先リスト名' (set to 'テストDNSポリシー'), '送信先リストタイプ' (a dropdown menu with 'DNSポリシー' selected, highlighted by a red rectangle), and radio buttons for 'ブロック' (selected) and '許可'. Below these is a '目的 地' field with the placeholder 'ドメインまたは URL' and a '追' button. At the bottom of the form, it says 'このリストに接続先が追加されていません' and '0 合計'. A footer bar shows 'Page: 1', 'Results per page: 10', and '1-0 of 0'. At the very bottom right are 'キャンセル' and '保存' buttons.

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. On the left is a navigation menu with options like '概要', '導入', 'ポリシー', '管理', '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', and 'Investigate'. The main 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'. A blue banner explains that connection lists are used to control access to destinations. Below this is a form to create a '新しい接続先リスト' (New Connection List). The form includes a '送信先リスト名' (Destination List Name) field, a '送信先リストタイプ' (Destination List Type) dropdown set to 'DNSポリシー', and a section 'このリストに含まれている接続先は:' (Connections included in this list) with radio buttons for 'ブロック' (Block) and '許可' (Allow). The 'ブロック' option is selected. Below this is a '目的地' (Destination) field with the placeholder 'ドメインまたは URL' and a '追' (Add) button. The status indicates 'このリストに接続先が追加されていません' (No destinations added to this list) and '0 合計' (0 total). At the bottom, there are 'キャンセル' (Cancel) and '保存' (Save) buttons. A 'Get Started' button is visible on the right side of the interface.

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

ポリシー / ポリシーコンポーネント

接続先リスト

追加

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 ポリシーで使用す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

キャンセル 保存

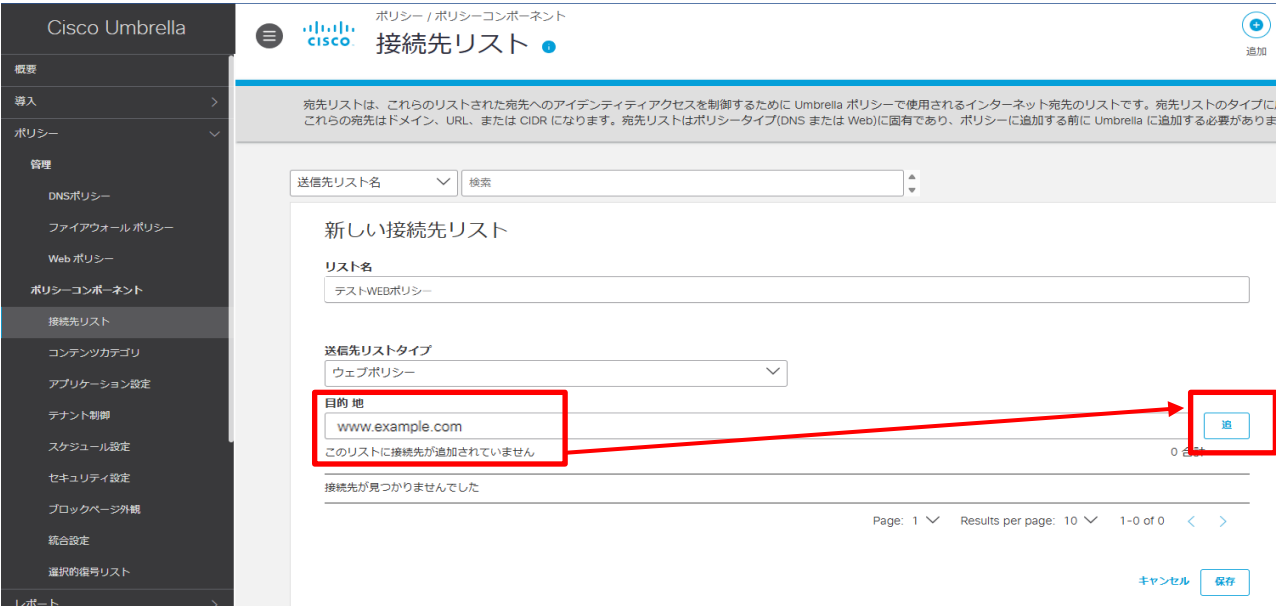
Get Started

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：
対象の宛先を赤字に設定し、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】



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。

The screenshot shows the Cisco Umbrella web interface for managing policies. The left sidebar contains navigation links: 概要, 導入, ポリシー, 管理 (with sub-links for DNS, Firewall, and Web), ポリシーコンポーネント (with sub-links for Destination List, Content Categories, Application Settings, Tenant Control, Scheduling, Security Settings, Block Page External View, Integration Settings, and Selective Whitelist), and レポート. 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'. It includes a description of destination lists and a form to '新しい接続先リスト' (New Destination List). The form fields are: 'リスト名' (List Name) with the value '新しい接続先リスト', '送信先リストタイプ' (Destination List Type) set to 'ウェブポリシー' (Web Policy), and '目的地' (Destination) with the value 'ドメイン、URL、IPv4またはCIDRを入力'. Below these is a search bar with the text 'www.example.com' highlighted by a red box. At the bottom right, the '保存' (Save) button is highlighted by a red box. The interface also shows pagination information: 'Page: 1', 'Results per page: 10', and '1-1 of 1'.

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。



注) Webポリシーの接続先リストへ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。



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。

Cisco Umbrella

ポリシー / 管理

DNSポリシー

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

適用する順番でソートされています

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

Get Started

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。

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

DNSポリシー

追加 ポリシーデスター

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

適用する順番でソートされています

1

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
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](#)

2 接続先リスト 適用
1 ブロックリスト
1 許可リスト
[編集](#)

ファイル分析 無効
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
NTT West Settings
[編集](#)

適用されたコンテンツ設定 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
有効

▲ 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
プロキシWeb接続により、危険なドメインに関して、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。

78

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

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

Cisco Umbrella

ポリシー / 管理

DNSポリシー

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

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

適用する順番でソートされています

1	Default Policy	次を含む 3 ポリシー設定	最終更新日 May 12, 2025
<p>ポリシー名 Default Policy</p> <ul style="list-style-type: none">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 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 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 有効3 接続先リスト 適用 2 ブロックリスト 1 許可リスト 編集ファイル分析 無効 インテリジェントプロキシが必要で ファイル検査 無効適用されたカスタムブロックページ NTT West Settings 編集 <p>詳細設定</p> <p>NTT West Settings USE CUSTOM SETTINGS</p> インテリジェントプロキシの有効化 プロキシWeb接続により、危険なドメインに関して、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。			

キャンセル [保存](#)

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。



許可／ブロックリスト設定方法（つづき）

⑭接続先リスト適用の「ルールの追加」をクリックします。



⑮例えばルール名「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



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



許可／ブロックリスト設定方法（つづき）

⑰送信先の「Destination Lists」を選択し「>」をクリック



許可／ブロックリスト設定方法（つづき）

⑱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 console. On the left, the 'Web ポリシー' (Web Policy) section is active in the sidebar. The main content area shows the 'Default Web Policy' configuration page. A modal dialog is open, displaying a list of destinations. The destination 'テストWEBポリシー' (Test Web Policy) is selected, and the '適用' (Apply) button is highlighted. The background shows the 'Default Web Policy' configuration table with columns for '優先' (Priority), 'ルール名' (Rule Name), 'ルールアクション' (Rule Action), 'アイデンティティ' (Identity), '送信先' (Destination), and 'ルール構成' (Rule Configuration).

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 保護されたファイルのバイパスが有効
1	Default Rule	ブロック			...

許可／ブロックリスト設定方法（つづき）

⑱「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

追加

グローバル設定

ポリシーテスター

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

1

Default Web Policy

次を含む
1 ルール

最終更新日
May 13, 2025

^

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 アイデンティティを追加する	1個の接続先リスト ... 宛先を追加	任意の日、いつでも 変更スケジュール 保護されたファイルのバイパスが有効
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
...

許可／ブロックリスト設定方法（つづき）

⑳改めて「Default Web Policy」をクリックします。



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

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

dokopura_msap12@west.ntt.co.jp

ODS用検証環境

Need Help?

Service Status

All services are operational

ドキュメント

サポートプラットフォーム

ラーニング センターへ

シスコオンラインプライバースタート

ポリシー / 管理

Web ポリシー

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

1

Default Web Policy

次を含む

2 ルール

最終更新日

Jun 09, 2025

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)

ルールの編集

ルールの有効化

ルールの削除

▲ ルールセット設定

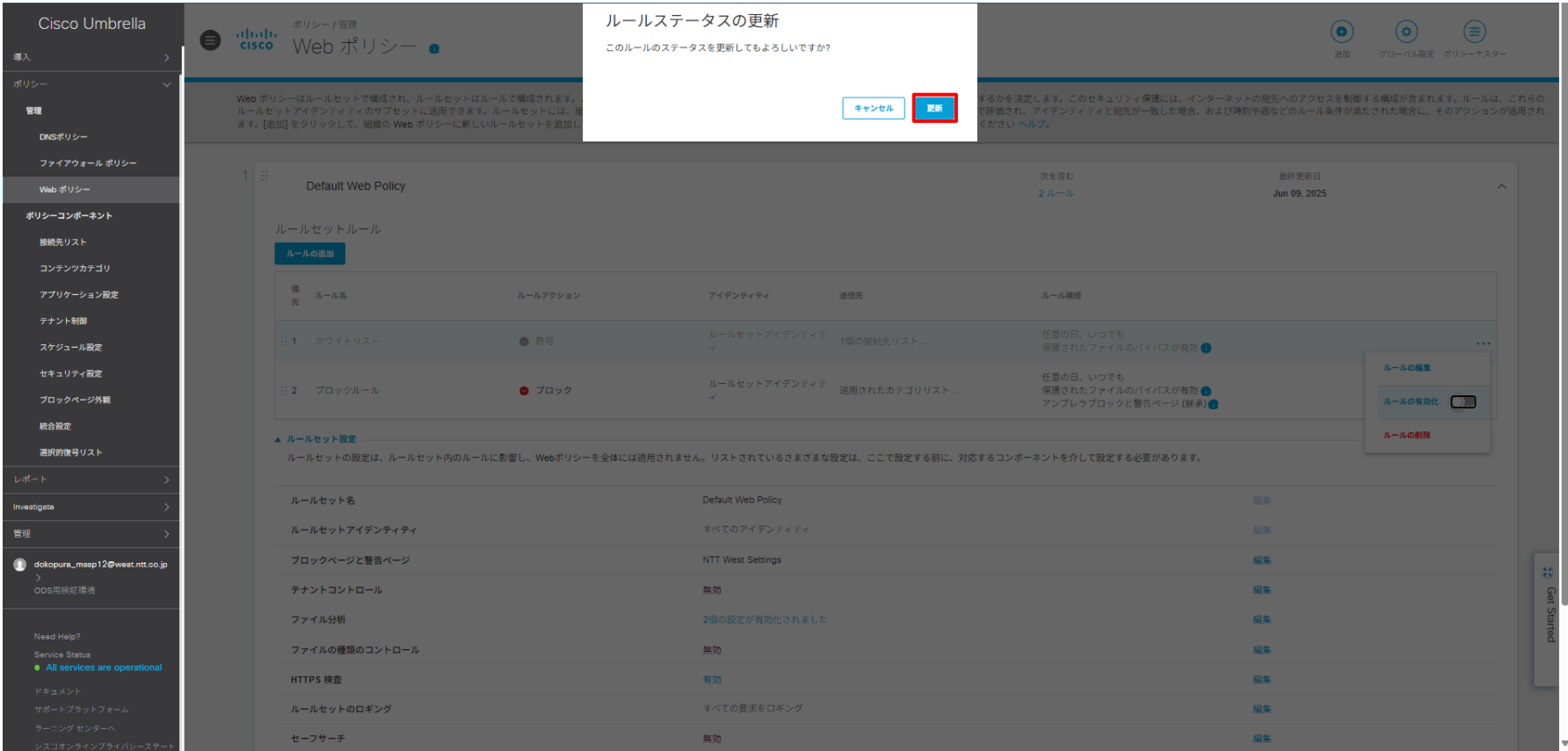
ルールセットの設定は、ルールセット内のルールに影響し、Webポリシーを全体には適用されません。リストされているさまざまな設定は、ここで設定する前に、対応するコンポーネントを介して設定する必要があります。

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	無効	編集
ファイル分析	2個の設定が有効化されました	編集
ファイルの種類のコントロール	無効	編集
HTTPS 検査	有効	編集
ルールセットのロギング	すべての要求をロギング	編集
セーフサーチ	無効	編集

Get Started

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



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

①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 is a dark sidebar menu with various options. The 'Policy' (ポリシー) section is expanded, and 'Selective Decryption List' (選択的復号リスト) is highlighted. The main content area shows the 'Default Web Selective Decryption List' table. The table has columns for 'Policy' (ポリシー), 'Category' (カテゴリ), 'Application' (アプリケーション), 'Domain' (ドメイン), and 'Last Updated' (最終更新). The 'Default Web Selective Decryption List' is highlighted with a red box.

ポリシー	カテゴリ	アプリケーション	ドメイン	最終更新
Default Web Selective Decryption List	Webポリシー	3	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 displays the Cisco Umbrella interface for configuring a 'Default Web Selective Decryption List'. The left sidebar shows the navigation menu with 'ポリシー' (Policies) selected. The main content area shows the 'Default Web Selective Decryption List' configuration page. The page includes a header with the Cisco logo and the title '選択的復号リスト' (Selective Decryption List). Below the header, there is a description of the selective decryption list and its purpose. The main configuration area is divided into three columns: 'リスト名' (List Name), '適用先' (Target), and 'カテゴリ' (Category). The '適用先' column shows 'Webポリシー' (Web Policy) with a count of 3. The 'カテゴリ' column shows 0 selected categories. The 'アプリケーション' (Application) column shows 0 selected applications. The 'ドメイン' (Domain) column shows 0 domains. The 'ドメイン' column has a red box around the '追加' (Add) button. The 'リスト名' column shows a text input field with the value 'Default Web Selective Decryption List'. Below the input field, there are three columns for selecting categories, applications, and domains. The 'カテゴリ' column shows 3 selected categories: 'Health and Medicine', 'Finance', and 'Government and Law'. The 'アプリケーション' column shows 0 selected applications. The 'ドメイン' column shows 0 domains. The 'ドメイン' column has a red box around the '追加' (Add) button. At the bottom right, there are 'キャンセル' (Cancel) and '保存' (Save) buttons.

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 displays the Cisco Umbrella Policy Manager interface. The sidebar on the left contains navigation links: 概要, 導入, ポリシー, 管理, DNSポリシー, ファイアウォール ポリシー, Web ポリシー, ポリシーコンポーネント, 接続先リスト, コンテンツカテゴリ, アプリケーション設定, テナント制御, スケジュール設定, セキュリティ設定, ブロックページ外観, 統合設定, 選択的復号リスト, レポート, Investigate, and 管理. The main content area is titled 'ポリシー / ポリシーコンポーネント' and '選択的復号リスト'. It shows a 'Default Web Selective Decryption List' with a table containing columns for '適用先' (Webポリシー), 'カテゴリ' (3), 'アプリケーション' (0), and 'ドメイン' (0). A modal window is open for adding domains, with 'example.com' entered in the 'Domains' field and the '追加' button highlighted.

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。

Cisco Umbrella

ポリシー / ポリシーコンポーネント
選択的復号リスト

選択的復号リストでは、HTTPSトラフィック検査の対象から除外するHTTPSトラフィックを定義します。選択的復号リストには、任意の数のコンテンツカテゴリやドメインを指定できます。選択的復号リストに一致するHTTPSトラフィックは検査されませんが、ドメイン層のセキュリティとポリシーは引き続き適用され、ドメイン層のみ可視化できます。

Default Web Selective Decryption List

適用先: Webポリシー | カテゴリ: 3 | アプリケーション: 0 | ドメイン: 0 | Apr 09, 2025

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

0 選択したアプリケーション

いいえ 選択したアプリケーション

1 ドメイン

example.com

キャンセル 保存

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。

Cisco Umbrella

ポリシー / ポリシーコンポーネント

選択的復号リスト

選択的復号リストでは、HTTPSトラフィック検査の対象から除外するHTTPSトラフィックを定義します。選択的復号リストには、任意の数のコンテンツカテゴリやドメインを指定できます。選択的復号リストに一致するHTTPSトラフィックは検査されませんが、ドメイン層のセキュリティとポリシーは引き続き適用され、ドメイン層のみ可視化できます。

Default Web Selective Decryption List	適用先 Webポリシー	カテゴリ 3	アプリケーション 0	ドメイン 1	Apr 26, 2025	▼
---------------------------------------	----------------	-----------	---------------	-----------	--------------	---

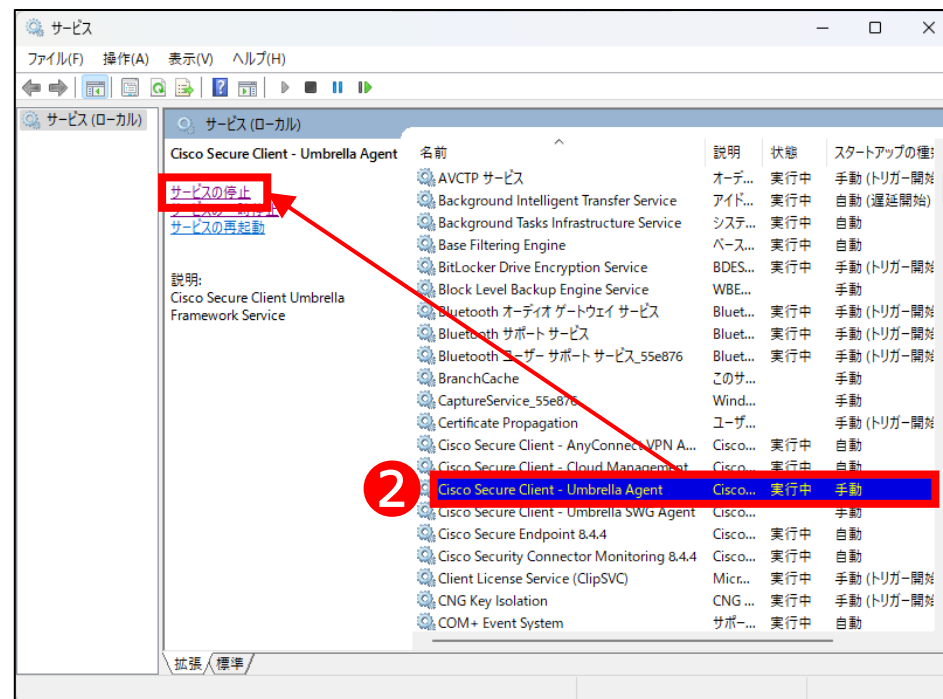
Get Started

まずCisco Umbrella が要因でインターネットができてい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。



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。

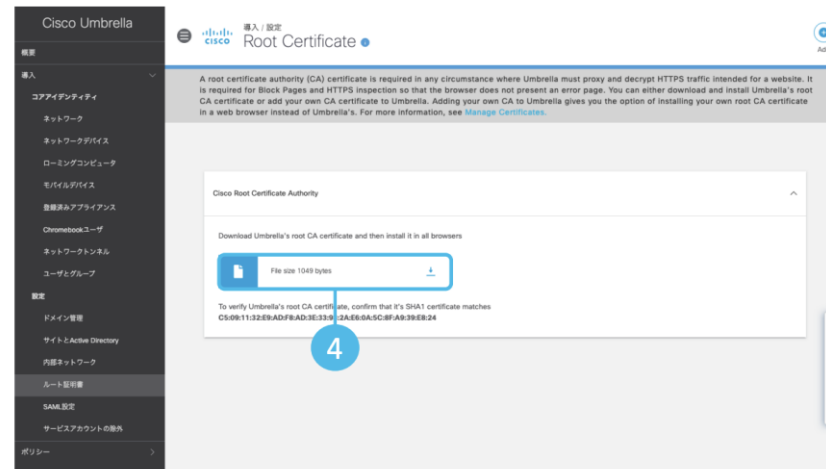
The screenshot displays the Cisco Umbrella management interface. On the left, a dark sidebar contains a menu with the following items: 概要 (Overview), 導入 (Import), コアアイデンティティ (Core Identity), ネットワーク (Network), ネットワークデバイス (Network Devices), ローミングコンピュータ (Roaming Computers), モバイルデバイス (Mobile Devices), 登録済みアプライアンス (Registered Appliances), Chromebook ユーザー (Chromebook Users), ネットワークトンネル (Network Tunnel), ユーザーとグループ (Users and Groups), 設定 (Settings), ドメイン管理 (Domain Management), サイトとActive Directory (Sites and Active Directory), 内部ネットワーク (Internal Network), **ルート証明書** (Root Certificate), SAML設定 (SAML Settings), サービスアカウントの除外 (Service Account Exclusion), and ポリシー (Policy). A blue circle with the number '2' is positioned next to the 'ルート証明書' item, indicating it is the next step. The main content area shows a '概要' (Overview) page with various status cards and a 'ネットワークの分析' (Network Analysis) section. The 'ネットワークの分析' section includes a line graph for '総リクエスト件数' (Total Request Count) and two empty search result boxes for '総ブロック' (Total Blocks) and 'セキュリティブロック' (Security Blocks). The '総リクエスト件数' graph shows a peak around 1 PM. The '総ブロック' and 'セキュリティブロック' boxes both display '検索結果がありません' (No search results found) and suggest expanding the search time range.

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が、[保存]をクリック
し 続行してください。



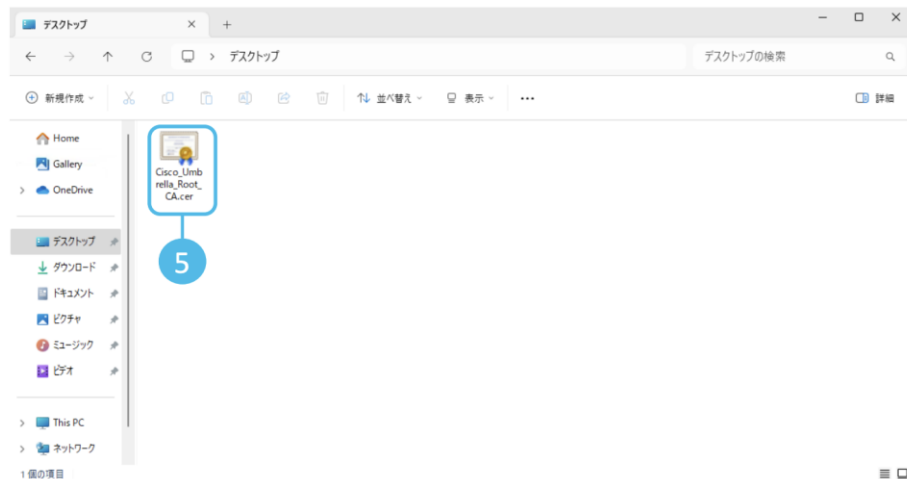
電子証明書の設定方法（つづき）

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。

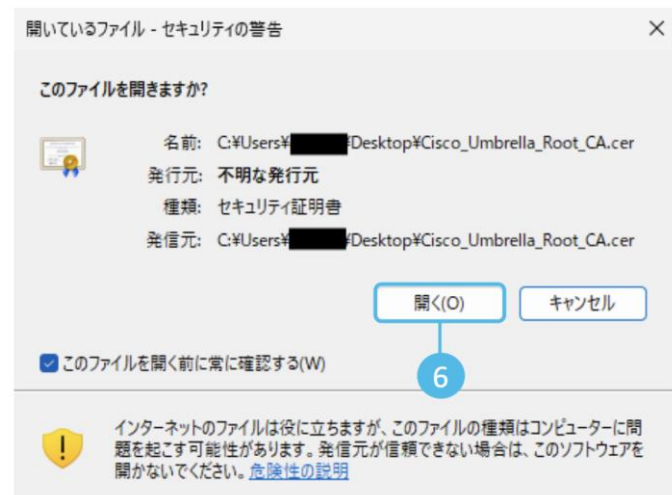
ファイル名は、[Cisco Umbrella_Root_CA](拡張子なし表示)または

[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。



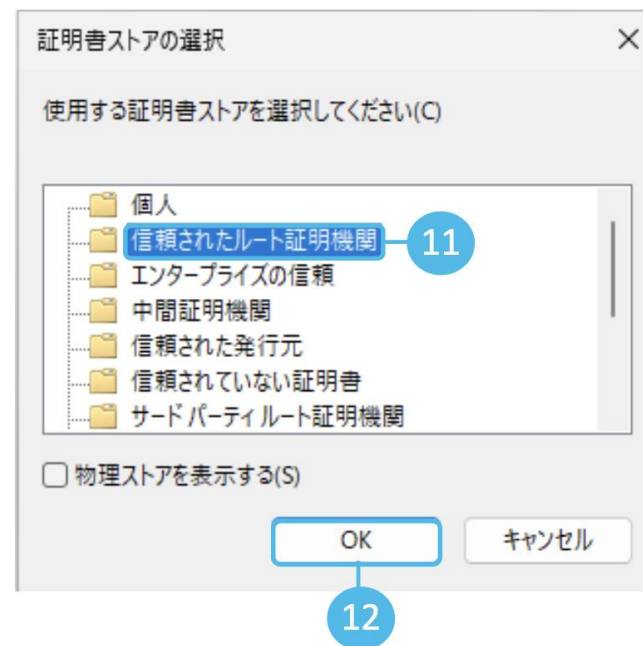
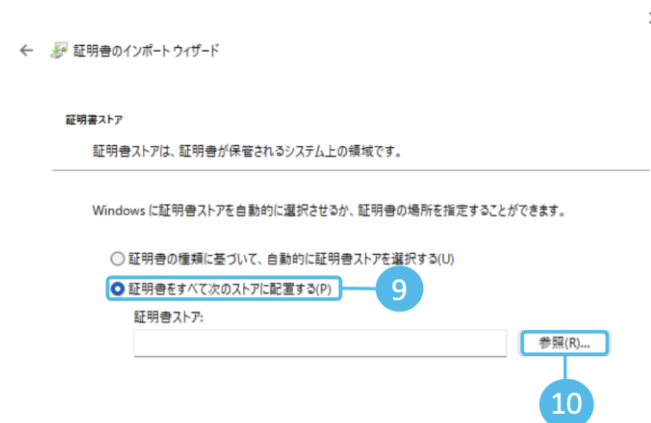
電子証明書の設定方法（つづき）

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。

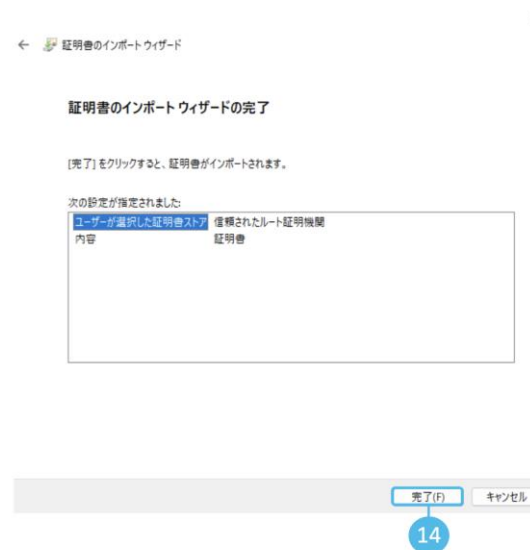


電子証明書の設定方法（つづき）

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。

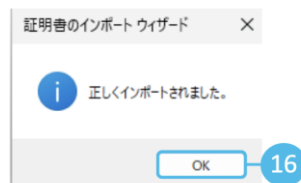


電子証明書の設定方法（つづき）

⑮ [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。



⑯ [正しくインポートされました。]メッセージを確認したら、「OK」をクリックします。



⑰ 「OK」をクリックします。



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てください。
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を無効しにて、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。



502 Bad Gateway

前項のエラー コード 515 は Intelligent Proxy 特有のもですが、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。



「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ーリスクが高まる場合もあるため、変更の際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

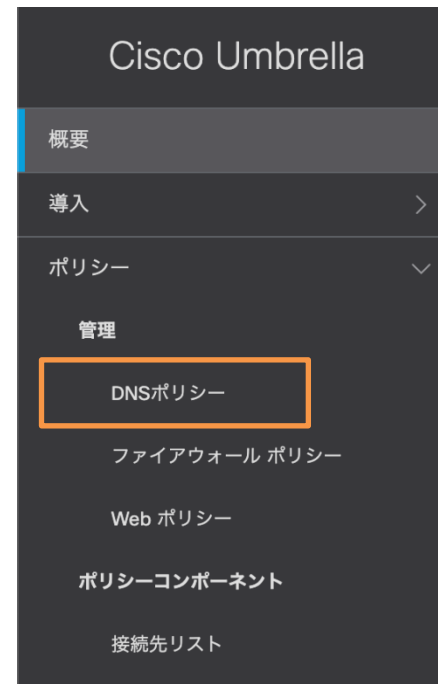
- GoogleやBingのセーフサーチを強制適用し、不適切な検索結果をフィルタリング
- DropboxやGoogle Driveなどのクラウドアプリの使用を制限

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ピュテーション(Cisco Advanced Malware Protectionにより有効化)を使用して、マルウェアに関してファイルを検査します。

[キャンセル](#)[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

🔍 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

1セキュリティ

2コンテンツ

3アプリケーション

4送信先

2 More

セキュリティ 設定

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

[設定]を選択します

Default Settings

ブロックするカテゴリ

編集

マルウェア

悪意のあるソフトウェア、ドライブバイダウンロード/エクスプロイト、モバイル脅威をホストしているWeb サイトと他のサーバ。

新しく発見されたドメイン

ごく最近アクティブになったドメイン。これらは新手の攻撃で頻繁に使用されます。

コマンド&コントロールのコールバック

侵害されたデバイスと攻撃者のインフラストラクチャとの通信を防止します。

フィッシング攻撃

ユーザをだまして個人情報や金融情報を送信させることを目的とする不正なWebサイト。

ダイナミックDNS

ダイナミックDNSコンテンツをホストしているサイトをブロックします。

損害が発生する可能性があるドメイン

不審な動作を示し、攻撃の一端を担う可能性のあるドメイン。

DNS トンネリング VPN

ユーザがDNSプロトコルを介したトンネリングによってトラフィックを隠すことを可能にするVPNサービス。これらは、アクセスとデータ転送に関する企業のポリシーを回避するために使用される場合があります。

クリプトマイニング

クリプトマイニングにより、組織は、マイニングプールとWebマイナーへのクリプトマイナーのアクセスを制御できます。

キャンセル

前へ

次へ

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

✓ セキュリティ

2 コンテンツ

3 アプリケーション

4 送信先

+2 2 More

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クワーキング、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。

カテゴリ高い

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

成人向け	アルコール
オークション	大麻
チャットおよびインスタント メッセージング	Child Abuse Content (児童虐待コンテンツ)
出会い系	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)

キャンセル

前へ

次へ

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 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

<input type="checkbox"/>	> Ad Publishing
<input type="checkbox"/>	> Anonymizer
<input type="checkbox"/>	> Application Development and Testing
<input type="checkbox"/>	> Backup & Recovery
<input type="checkbox"/>	> Business Intelligence
<input type="checkbox"/>	> Cloud Carrier
<input type="checkbox"/>	> 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。

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。

Q 宛先リスト名で検索

すべてを選択

すべてのリスト

2合計

すべての接続先リスト

☒

Global Allow List

目的地を見る

☒

Global Block List

目的地を見る

1 ブロック 適用対象リスト

☒

Global Block List

1 許可 適用対象リスト

☒

Global Allow List

キャンセル

前へ

次へ

119

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)



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。

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

選択的番号リスト

レポート

Investigate

管理

ポリシー / 管理

DNSポリシー

追加 ポリシーテスター

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

適用する順番でソートされています

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

Get Started

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。

Cisco Umbrella

ポリシー / 管理

DNSポリシー

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

適用する順番でソートされています

1	Default Policy	次を含む 3 ポリシー設定	最終更新日 May 12, 2025	↑
<p>ポリシー名 Default Policy</p> <div><div><p>すべてのアイデンティティに適用</p><p>適用されたセキュリティ設定: 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</p><p>適用されたコンテンツ設定: NTT West Settings マルウェア、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</p><p>適用されたアプリケーション設定がありません 有効</p></div><div><p>2 接続先リスト 適用 1 ブロックリスト 1 許可リスト 編集</p><p>ファイル分析 無効 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</p><p>適用されたカスタムブロックページ NTT West Settings 編集</p></div></div> <p>▲ 詳細設定</p> <p>NTT West Settings USE CUSTOM SETTINGS</p> <p>インテリジェントプロキシの有効化 プロキシWeb接続により、危険なドメインに関して、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。</p>				

Get Started

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」を選択ー「設定して戻る」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

1 Default Policy

次を含む
3 ポリシー設定

最終更新日
May 12, 2025

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

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

クラウドとデータセンター

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

暗号化されたDNS

すべてを選択

キャンセル

設定して戻る

Get Started

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 displays the Cisco Umbrella management interface for DNS policies. The left-hand navigation pane includes sections for Overview, Import, Policies, Management, Policy Components, Connection Lists, Content Categories, Application Settings, Tenant Control, Scheduling, Security Settings, Block Page Appearance, Integration Settings, and Selective Forwarding Lists. The 'Policies' section is expanded, showing 'DNS Policy' as the active item. The main panel shows the 'Default Policy' configuration page. A header note explains that policies determine security, category, and connection lists, and that they are applied in order of priority. The configuration area lists several settings: 'すべてのアイデンティティに適用' (Apply to all identities), '適用されたセキュリティ設定: NTT West Settings' (Applied security settings), '適用されたコンテンツ設定: Default Settings' (Applied content settings), '適用されたアプリケーション設定がありません' (No applied application settings), '2 接続先リスト 適用' (2 Connection lists applied), 'ファイル分析 無効' (File analysis disabled), and '適用されたカスタムブロックページ' (Applied custom block page). The '適用されたコンテンツ設定: Default Settings' section is highlighted with a red box, showing the text 'アダルト および 成人向け がブロックされます。' (Adult and adult-oriented content is blocked). At the bottom right, the '保存' (Save) button is highlighted with 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」のことを指します。

CASBの設定方法

Umbrella Dashboardからポリシー → 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。

ポリシー / ポリシーコンポーネント

アプリケーション設定

[アプリケーションの設定]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。

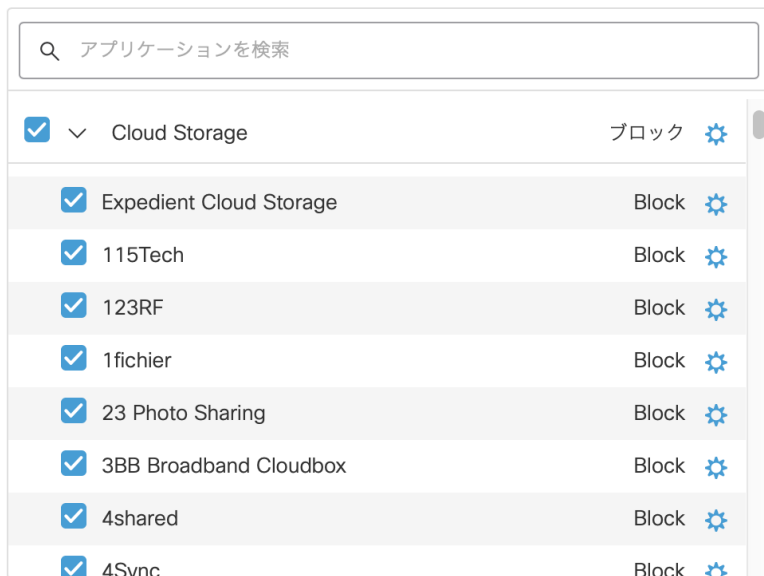
Cisco Test Policy	に適用されます Webポリシー	最終更新日 Feb 25, 2025	▼
Default Settings	に適用されます DNSポリシー	最終更新日 Feb 18, 2025	▼

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ではありません。

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。



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 (ブローカー) の役割を果たす機能やサービス」のことを指します。

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。



組織の利用実態の中で特にリスクが高いものについてはフラグがつけられて表示されます。



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>

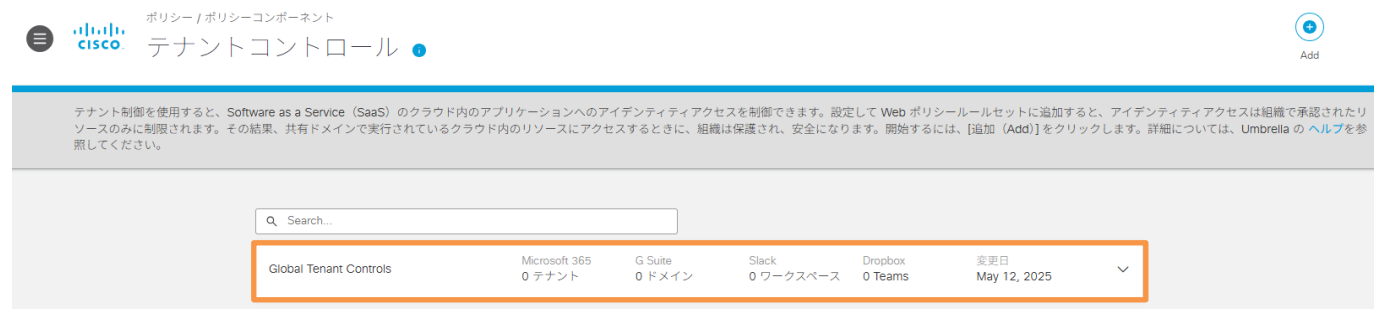
テナント制御とは、管理者によって指定されたクラウドサービスの契約テナント（環境）のみにアクセスできるよう制御する機能です。
例えば、会社貸与のパソコンから会社で契約しているMicrosoft 365環境へのみ接続を許し、個人契約のMicrosoft 365に接続させないなど制御することができます。

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。




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

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

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。

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-xxxxxxx... [追加](#)

1 Domain

a.example.com [×](#)

131

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。

キャンセル

保存

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 からアクセスできます）

The screenshot displays the Cisco Umbrella dashboard. On the left is a dark sidebar menu with the 'Cisco Umbrella' logo at the top. The '概要' (Overview) menu item is highlighted with an orange box. Below it are sections for '導入' (Onboarding) and '設定' (Settings). The main content area has a top bar with the Cisco logo, a hamburger menu, and the title '概要'. To the right of the title are links for 'Settings' and 'スケジュール' (Schedule), and a dropdown for '過去24時間' (Last 24 hours). Below the title bar, there's a '0 Messages' section with three rows of blocked requests: 'Malware: 0 requests blocked in the last 24 hours', 'Botnet: 0 requests blocked in the last 24 hours', and 'Cryptomining: 0 requests blocked in the last 24 hours'. Each row has links for 'View Trends' and 'View Details'. Below this is a yellow warning box with a triangle icon, stating: 'For Customers with Cisco-managed S3 buckets enabled, please rotate your Cisco-managed Amazon S3 bucket key. After this time, your logs will continue to be sent to your S3 bucket but you won't be able to access them. To ensure you can access your information, read the knowledge base article here.' Below the warning is a 'LOG MANAGEMENT' link. The '導入の健全性' (Onboarding Health) section contains three circular progress indicators, all at 0%: 'アクティブなネットワーク' (0 / 0 アクティブ), 'アクティブなローミングクライアント' (0 / 0 アクティブ), and 'アクティブなデバイス' (0 / 0 アクティブ). Below this is the 'ネットワークの分析' (Network Analysis) section. The 'アプリケーションの検出と制御(過去90日間)' (Applications Detected and Controlled (Last 90 Days)) section is highlighted with an orange box. It contains two cards: '114 検出されたクラウドアプリケーション' (114 Detected Cloud Applications) and '1 リスクのあるクラウドアプリケーション' (1 Risky Cloud Applications). Below these cards is a 'すべて表示' (Show All) button, which is highlighted with an orange box. To the right of the 'すべて表示' button is a 'ダッシュボードの表示' (Dashboard View) button. Further right is a 'フラグが設定されているカテゴリ' (Categorized by Flagged) section with a list of categories: 'クラウドストレージ' (0 確認 4 合計アプリケーション数), 'ソーシャルネットワーキング' (0 確認 2 合計アプリケーション数), 'コラボレーション' (0 確認 1 合計アプリケーション数), and 'メディア' (0 確認 2 合計アプリケーション数). To the right of this list is a 'フラグが設定されている' (Flagged) section with a '検索結果' (Search Results) section showing '検索の時間' (Search Time).

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
App Discovery

Download CSV

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	
<input type="checkbox"/> Protected Media Security	High	1	--	669.2 KB total traffic 621.3 ... 47.9 KB	Unreviewed	Control this app
<input type="checkbox"/> OneTrust Security	Medium	4	8	157.9 KB total traffic 66.4 KB 91.5 KB	Unreviewed	Control this app
<input type="checkbox"/> Digital Adoption Platform Business Intelligence	Medium	3	234	4.6 MB total traffic 4.4 MB 192.0 ...	Unreviewed	Control this app
<input type="checkbox"/> Intercom Customer Relationship Manage...	Medium	4	37	120.7 KB total traffic 79.8 KB 40.9 KB	Unreviewed	Control this app
<input type="checkbox"/> Qualtrics Website and App Feed... Business Intelligence	Medium	6	131	3.9 MB total traffic 3.5 MB 380.5 ...	Unreviewed	Control this app

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。

Back to Dashboard / Apps

Application

Protected Media

Provides an anti fraud solution that enables users to detect and block bots to protect brands.

Risk Score

High

Control this app

Unreviewed

Details

App URL

<https://www.protected.media/>

Identities

1

Traffic

Total: 669.2 KB
Blocked: --

First Detected (UTC)

Feb 17, 2025

Category

Security

Vendor

Protected Media

DNS Requests

Total: --
Blocked: --

Last Detected (UTC)

Feb 17, 2025

Risk Details

Identities (1)

Attributes (38)

How We Calculate Risk (Help us improve)

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

Weighted Risk

High

Business Risk

High

Usage Risk

Medium

Vendor Compliance

Not Found

Business Risk

Factors:
1. Typical use of the service (personal or organizational).
2. The Talos Security Intelligence Web Reputation score for the service.
3. Financial viability of the app vendor.
4. Type of data stored by the app.
[Show details](#)

Usage Risk

Factors:
1. Volume; how much data flows to and from the service.
2. Users; how many of your users depend on or use the service.
[Show details](#)

Vendor Compliance

Factors:
1. Security controls
2. Certifications earned
[Show details](#)

Risk Details

Identities (1)

Attributes (38)

Search by identity

MMM DD YYYY

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

ページ: 1

各ページの結果数 50

1-1/1

リスク判定理由

端末の確認

135

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

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 .	Block
<input type="checkbox"/> ABCD	Not applied. Add to a DNS Policy .	
<input type="checkbox"/> LMNOP	Not applied. Add to a DNS Policy .	

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可能です。

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。

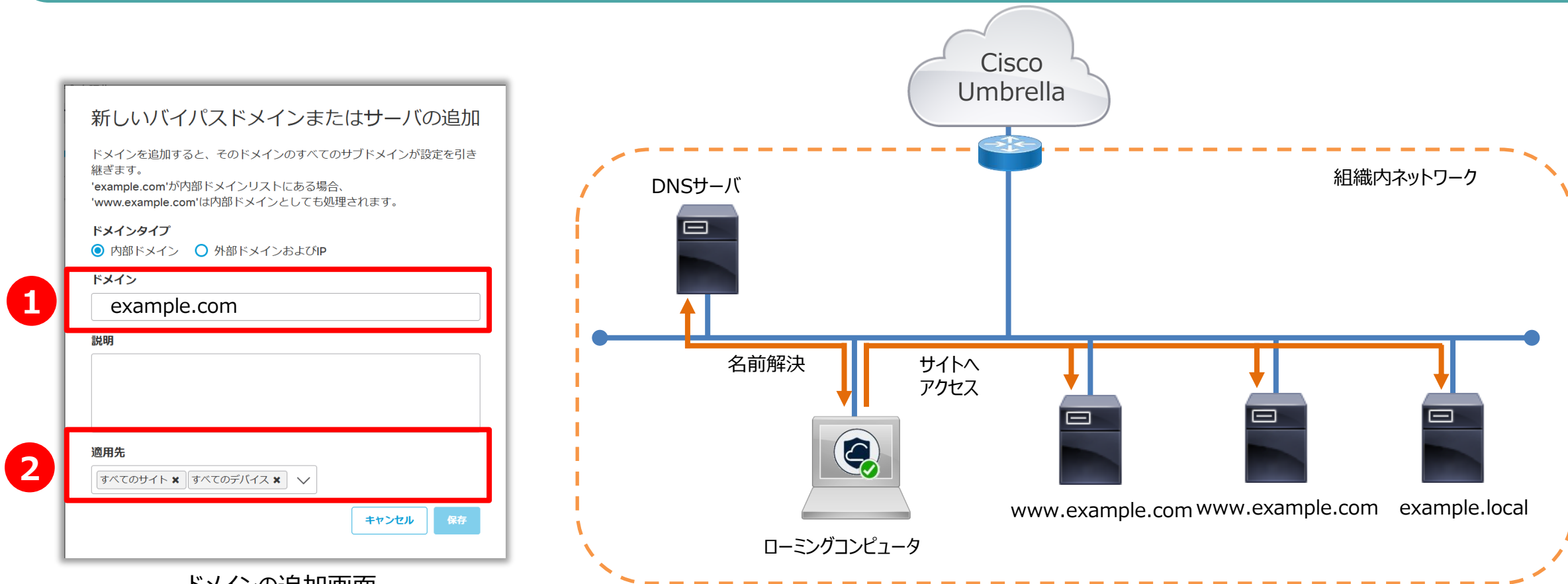
①例として、「example.com」ドメインを追加した際の動作を以下に示します。

「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。

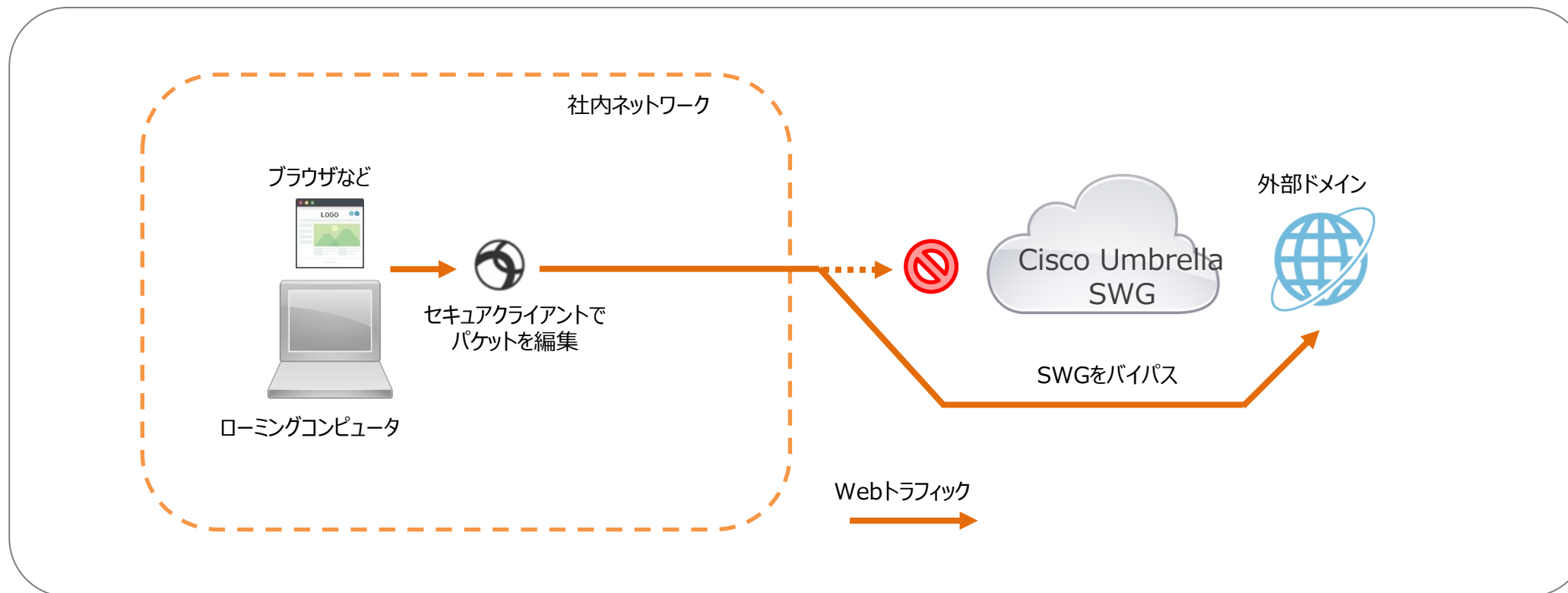
②「適用先」では内部ドメインの適用先を選択できます。

「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。



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/*

1

2

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

エンティティ

説明

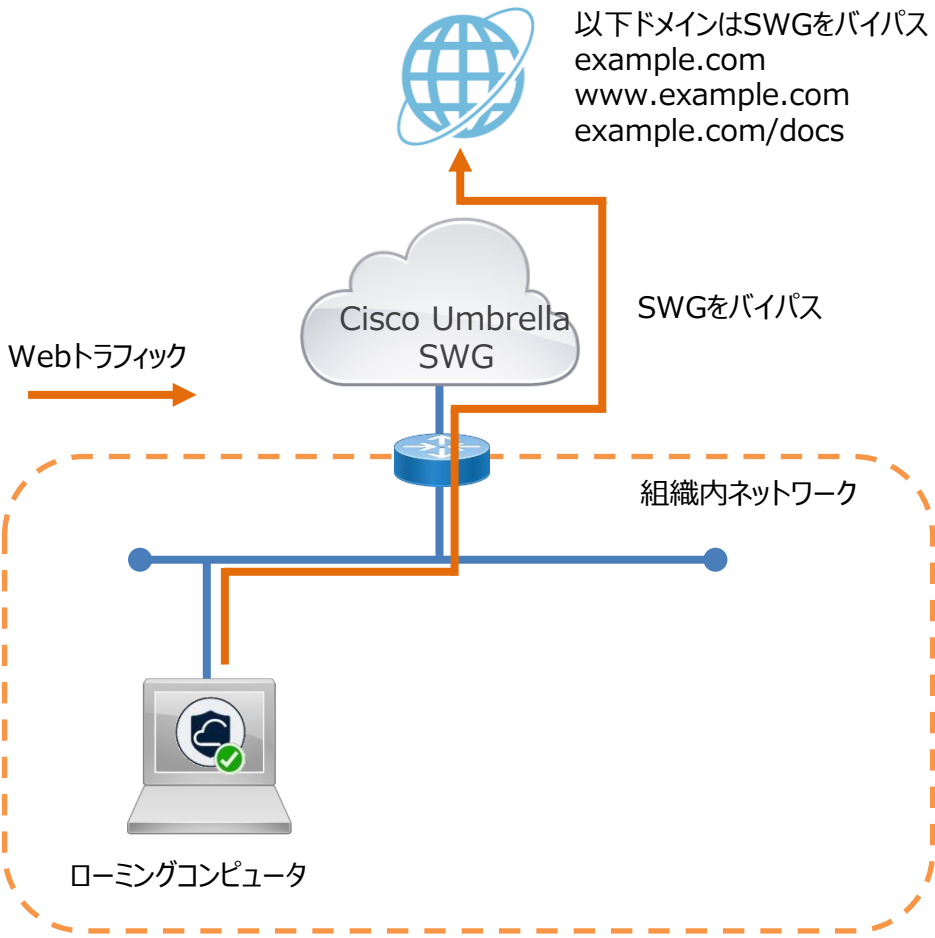
適用先

ドメイン: ホスト対象のPAC, AnyConnect, appliesTo.chromebook
IP: AnyConnect, appliesTo.chromebook

キャンセル

保存

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
- ① [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

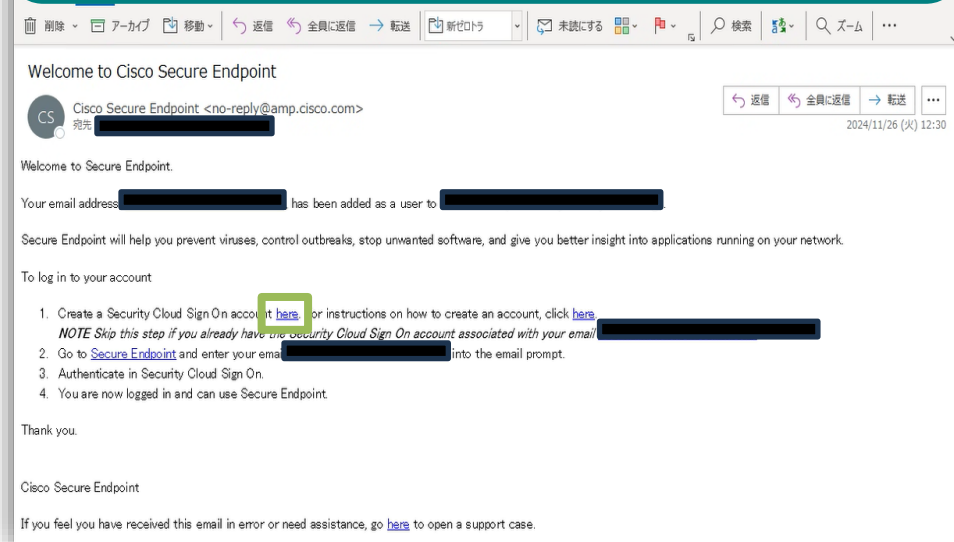
1人目の管理者

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 *

Japan

Password *

..... Show

Confirm Password *

..... Show

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

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

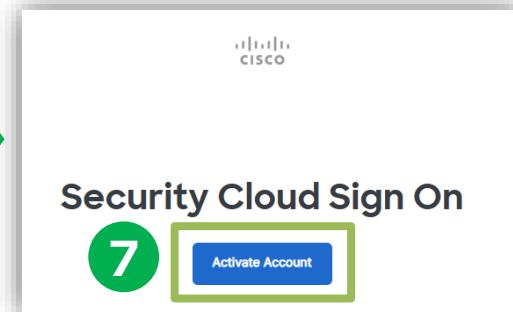
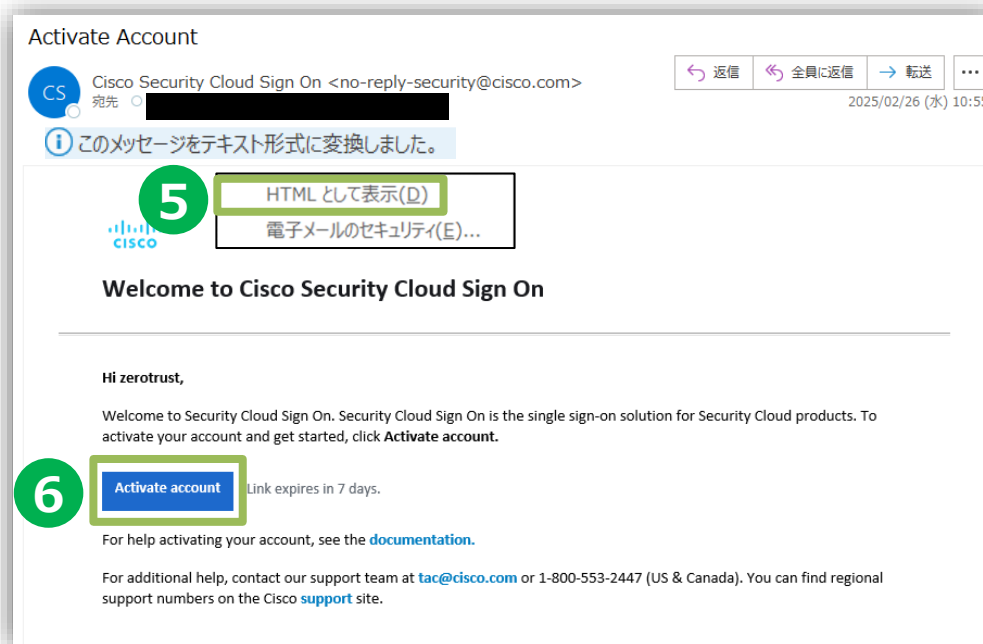
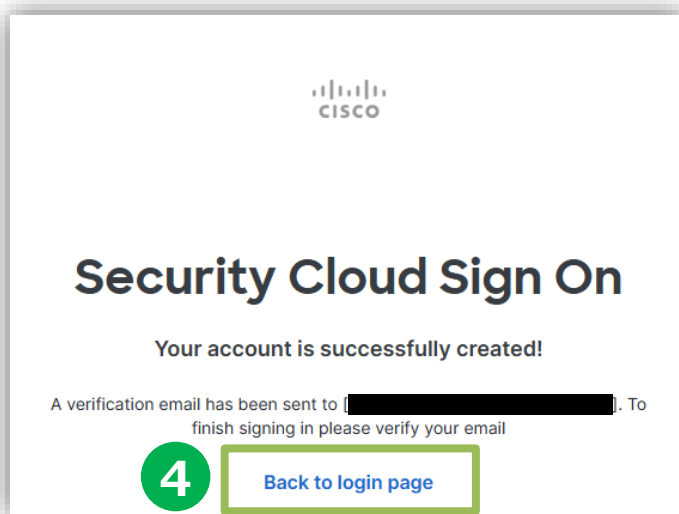
3

Sign up

Cancel

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



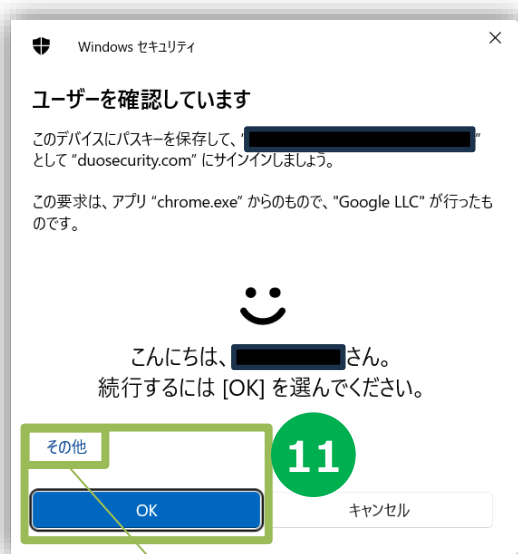
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- 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

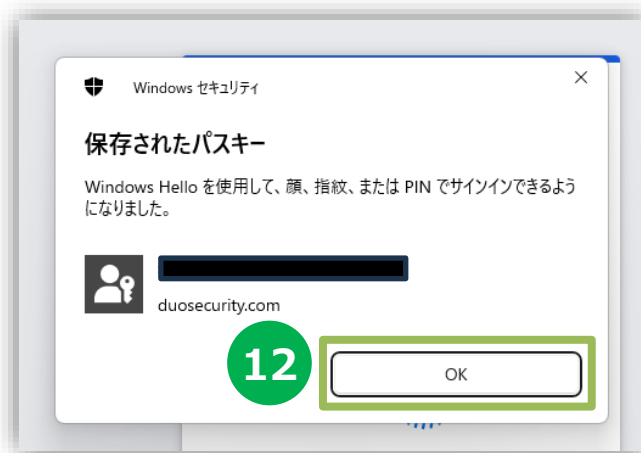


8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- 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。

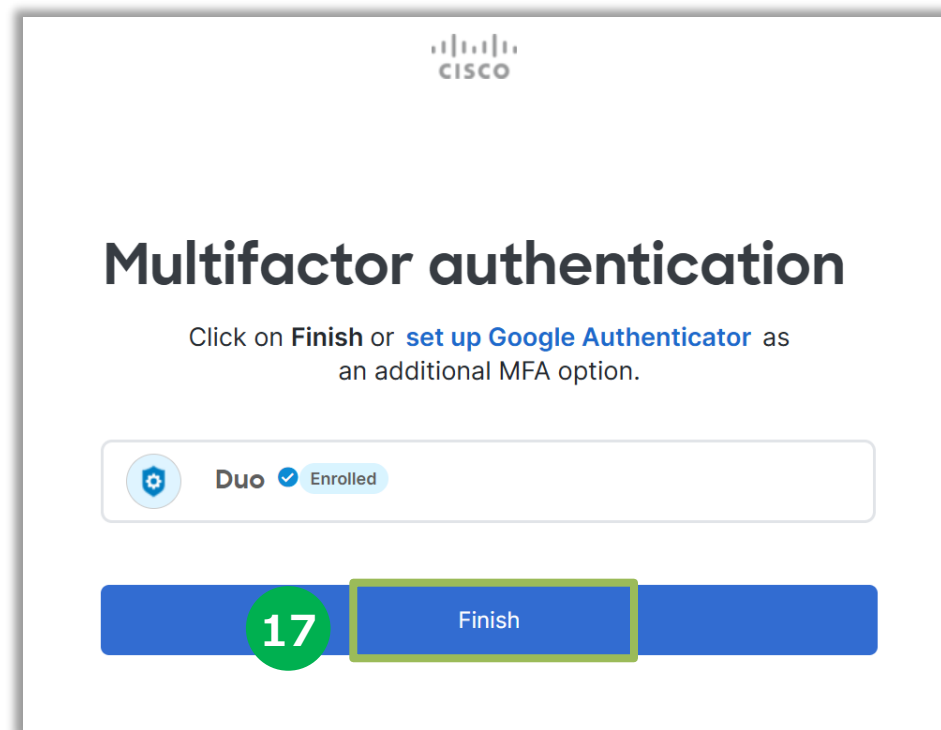
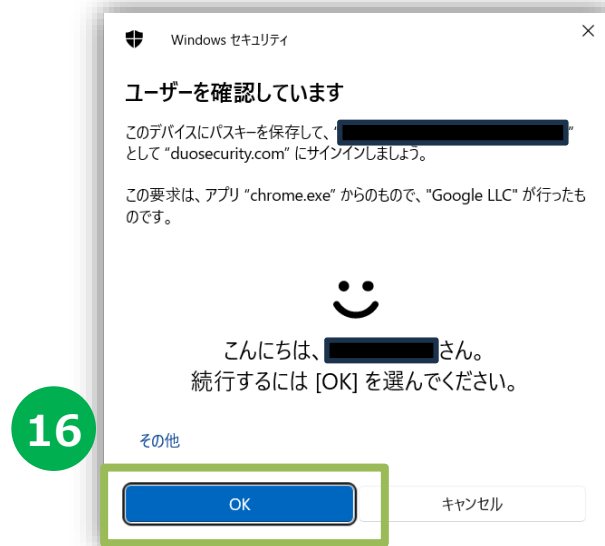


指紋認証が表示される場合はその他から顔認証を選択下さい



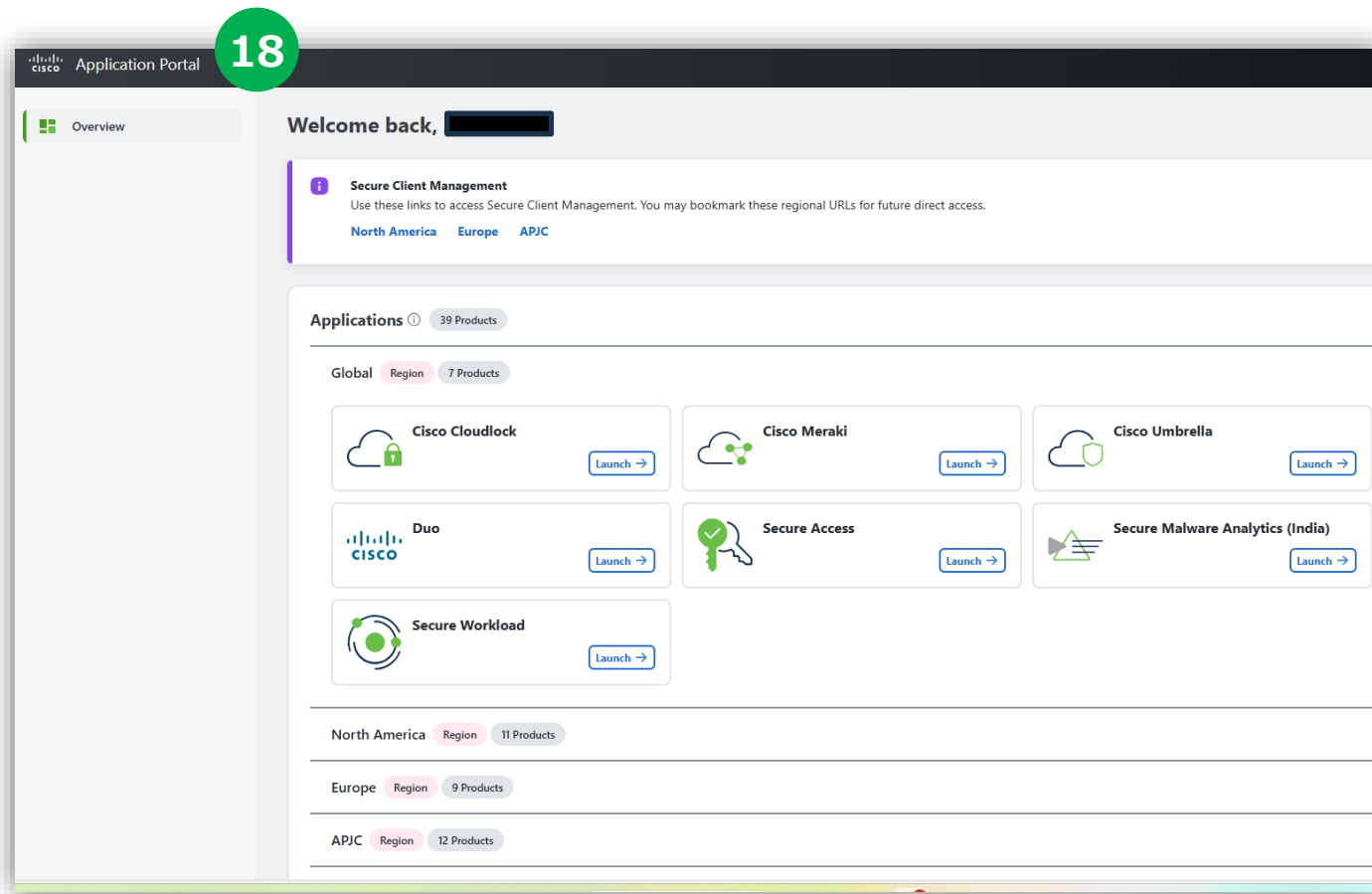
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

- ⑮ [Duoでログイン]をクリック
- ⑯ 顔認証が成功したら[OK]をクリック
- ⑰ [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>

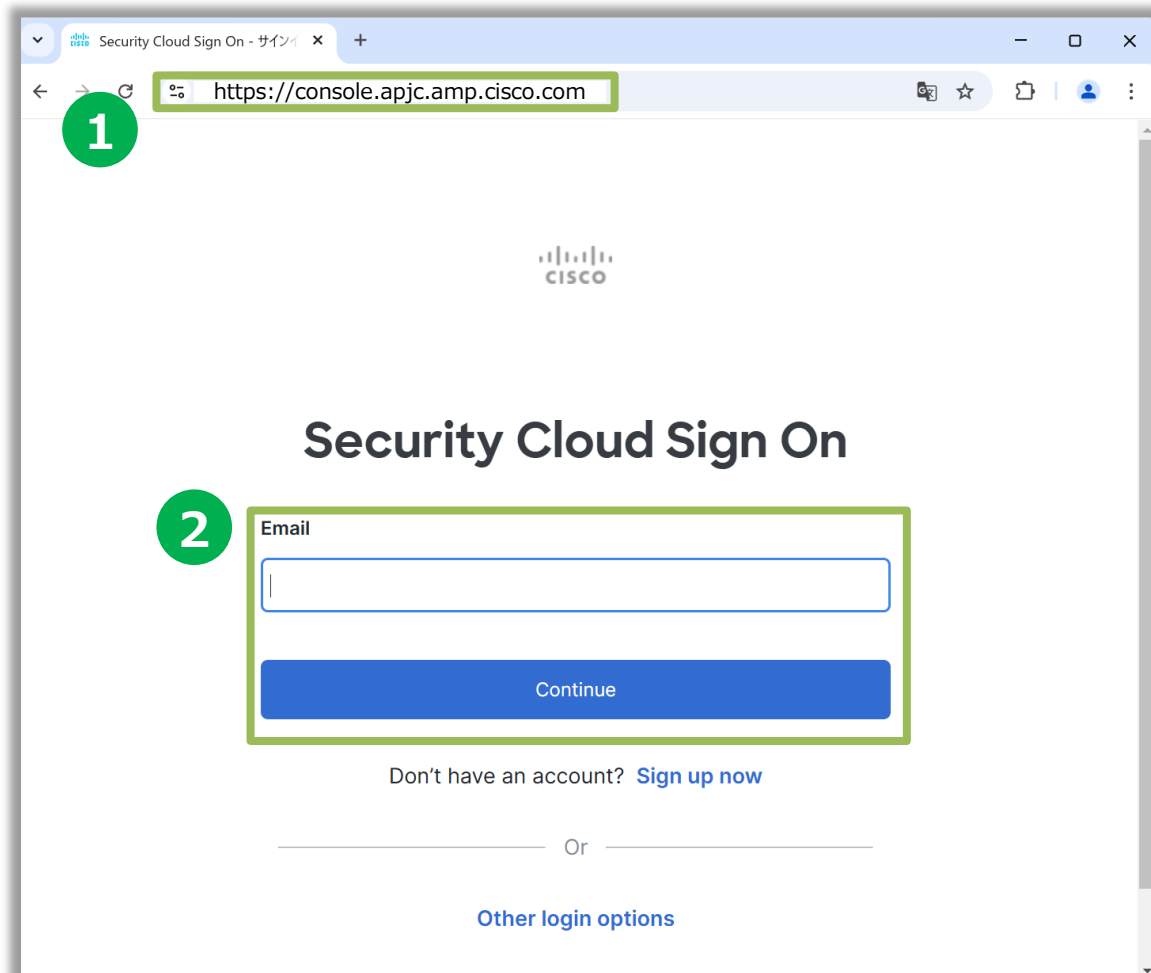
- ⑮ 初回ログインではCiscoサービスのポータルサイトが立ち上がります。
- ⑯ ブラウザを開き直し、改めてCisco Secure Endpoint管理コンソールのURLを開きます。
Cisco Secure Endpoint管理コンソール : <https://console.apjc.amp.cisco.com>



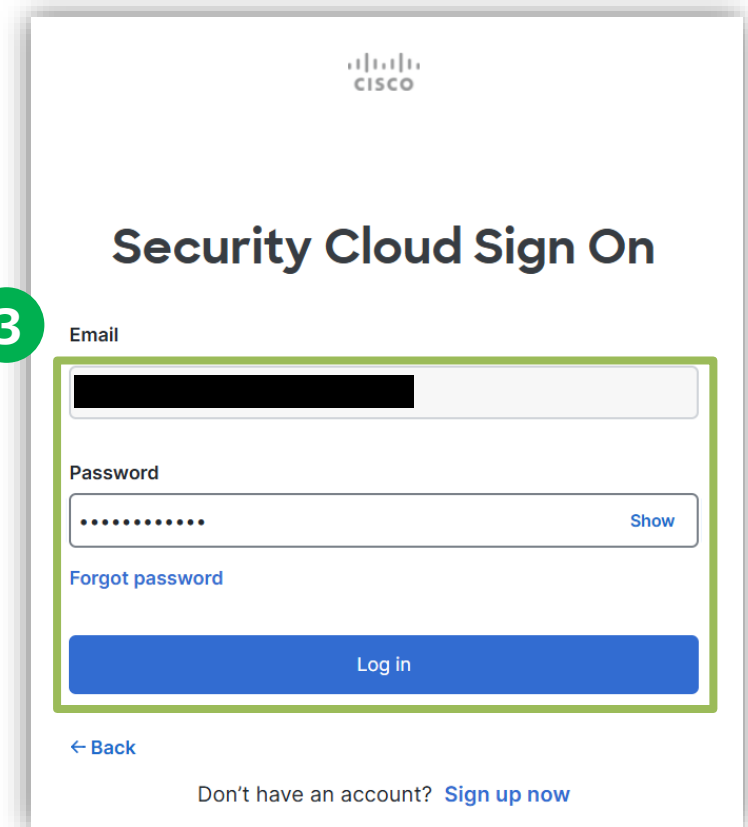
8. コンソールへのログイン手順 <システムログイン>

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



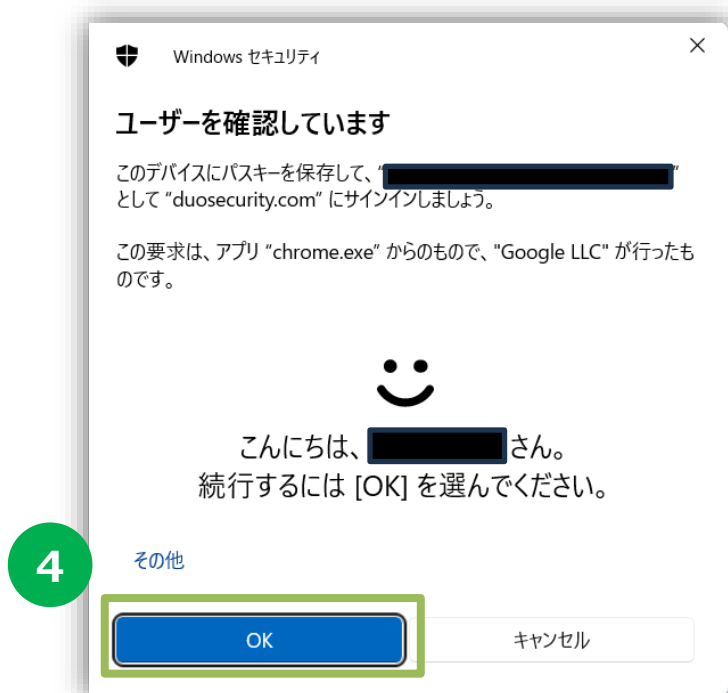
The screenshot shows a web browser window with the URL <https://console.apjc.amp.cisco.com> in the address bar. The page title is "Security Cloud Sign On". A green circle with the number "1" is next to the address bar. Below the title, there is a green circle with the number "2" next to the "Email" input field. The input field is empty, and the "Continue" button is visible below it. At the bottom, there is a link "Don't have an account? Sign up now" and "Other login options".



The screenshot shows the "Security Cloud Sign On" page. A green circle with the number "3" is next to the "Email" input field. The input field contains a blacked-out email address. Below it is the "Password" input field, which contains a masked password (dots). A "Show" button is next to the password field. Below the password field is a link "Forgot password". At the bottom, there is a "Log in" button. At the very bottom, there is a link "Don't have an account? Sign up now".

8. コンソールへのログイン手順 <システムログイン>

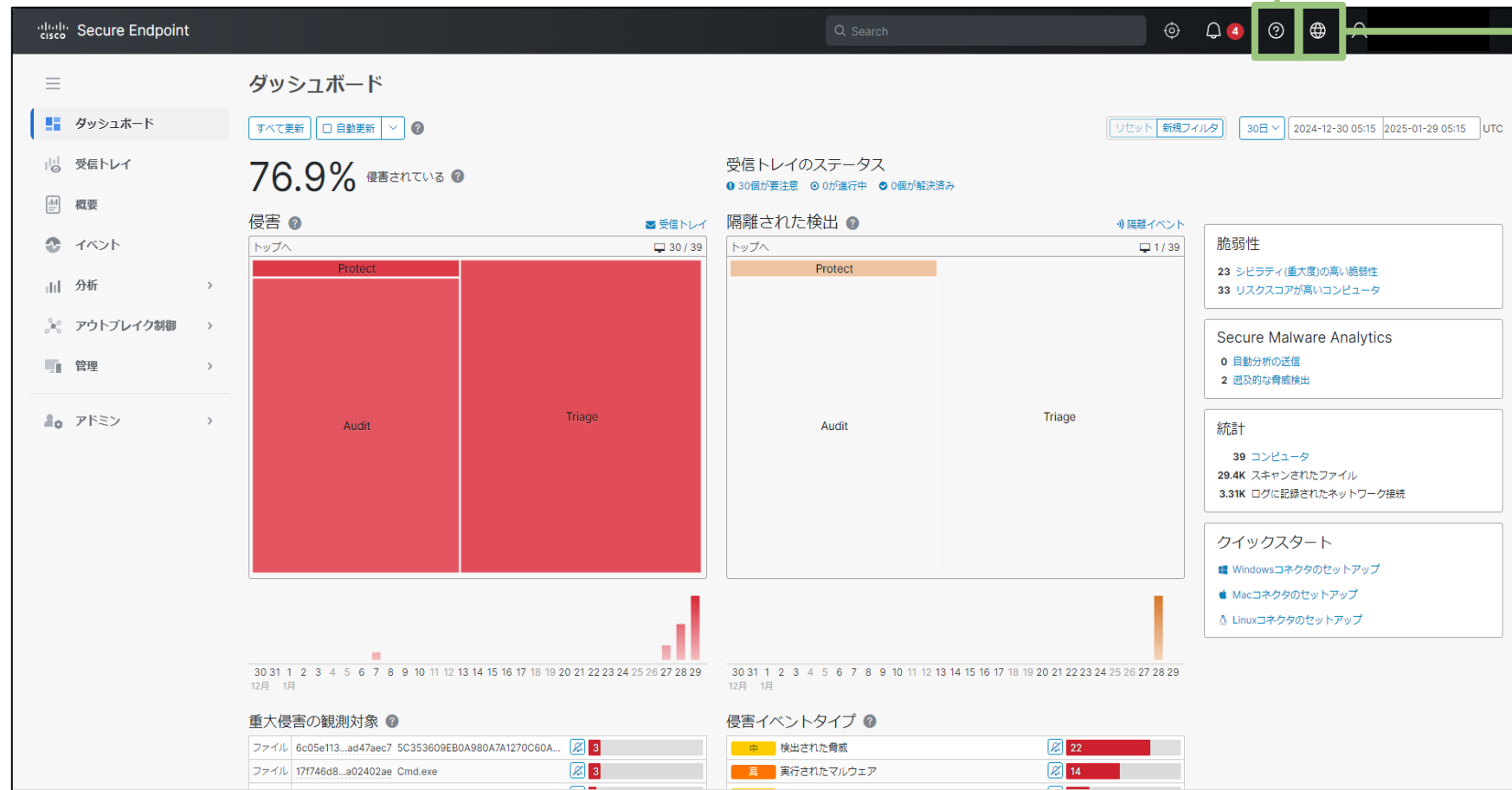
- ④ 設定した2段階認証を実施 ※以下はWindows Helloで顔認証を実施しています。
- ⑤ 認証が成功し、Cisco Secure Endpointの管理コンソール画面が表示されることを確認



8. コンソールへのログイン手順 <ダッシュボード説明>

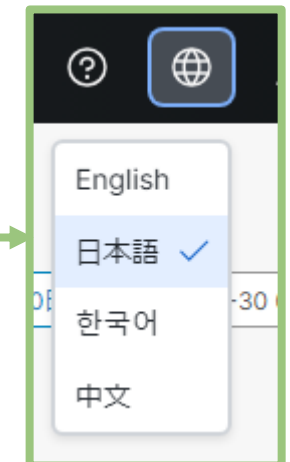
ログイン後最初に開くページです。
社内のマルウェア感染状況を一覧で確認することが可能です

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



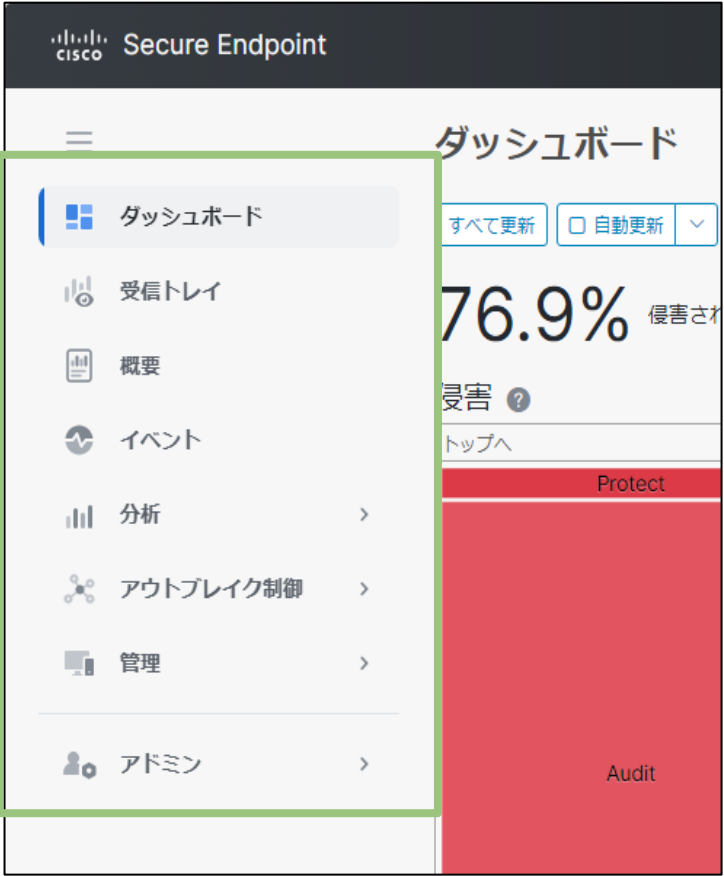
不明な点はこちらに説明が
記載されております。

<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	ユーザアカウントの設定、監査ログやデモ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・端末等へのウィルス拡散・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」をクリックします。

グループ「Protect」内のODS-NewZero3 Demo1

ホスト名	ODS-NewZero3	Demo1	グループ	Protect
オペレーティング システム	Windows 11, SP 0.0 (ビルド)			Protect
コネクタバージョン	8.4.3.30374			172.16.1.4
インストール日	2025-02-20 03:05:46 UTC			217.178.126.230
コネクタのGUID	996f2b9d-ed64-436c-b34c		時	2025-02-20 03:49:47 UTC
プロセッサID	bfebfbff000906a4		ション	71384
BP署名の最終更新	2025-02-20 03:08:06 UTC		ン	TETRA 64ビット (日次パッチ)
定義の最終更新日時	2025-02-20 03:07:57 UTC			tetra-defs.apjc.amp.cisco.c
Cisco Secure Client ID	5244cca4-c21e-436f-b361			

イベント デバイストラジェクトリ 診断 変更の表示

4 隔離の開始 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

⑤任意でコメントを記載し、「開始」をクリックします。

エンドポイントの隔離

プロキシを通過するトラフィックは許可されます。

コメント

5

キャンセル 開始

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」をクリックします。



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、パソコンがウイ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(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まい、本人に成りす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ることができます。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

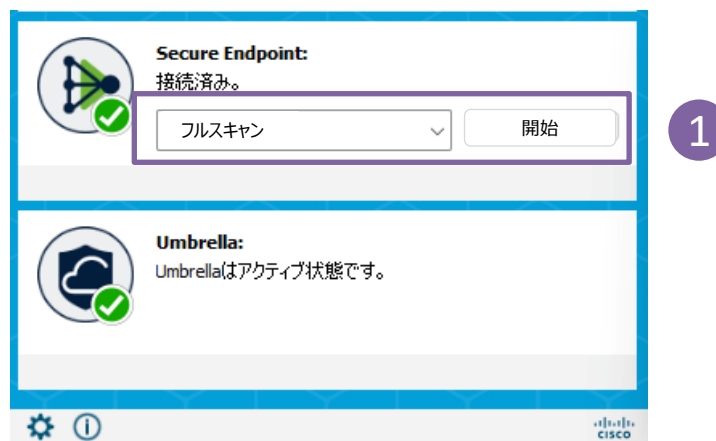
多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウィルスがあります。

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。

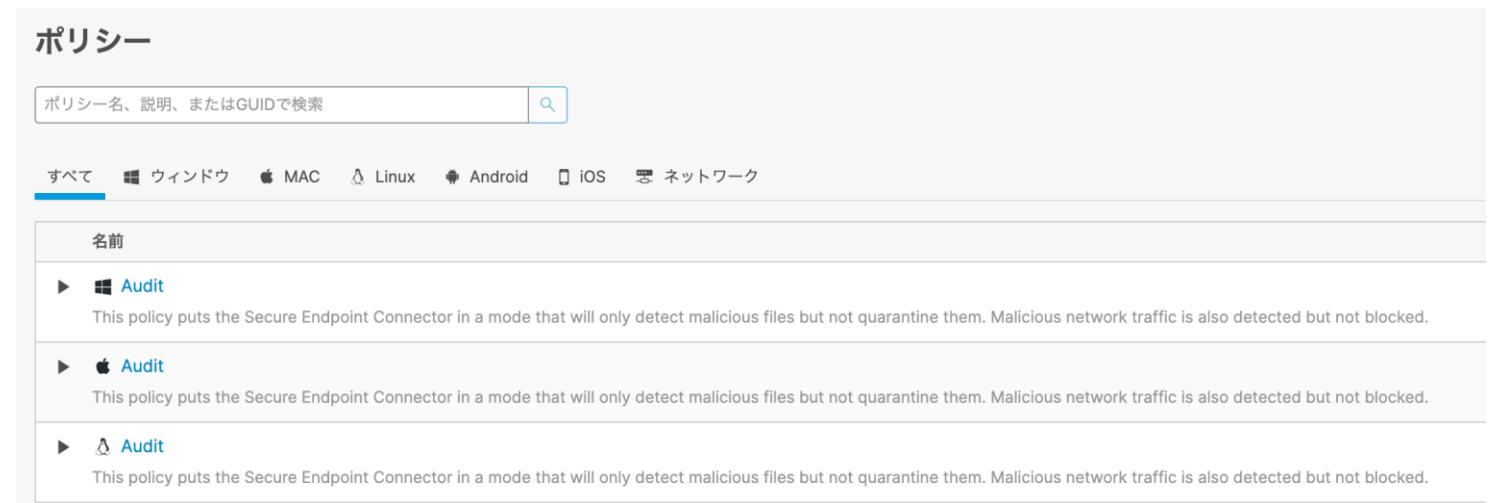
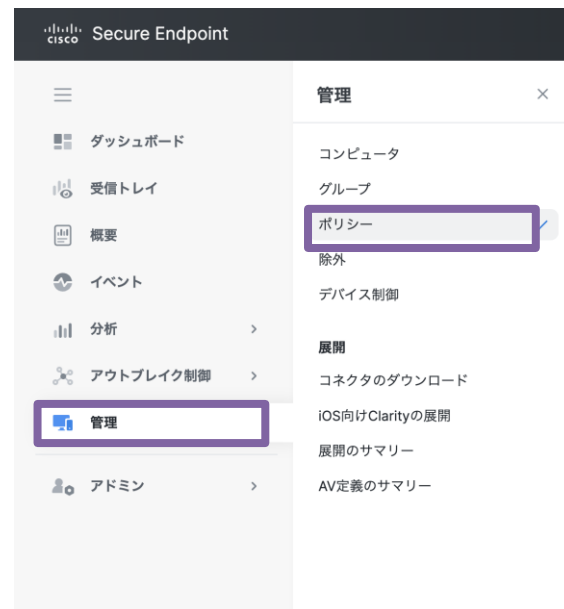
① Secure Endpoint をアンインストールする方法

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。



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

ブロキシ

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 ⓘ

検疫監査

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 ⓘ

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 ⓘ

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 ⓘ

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。

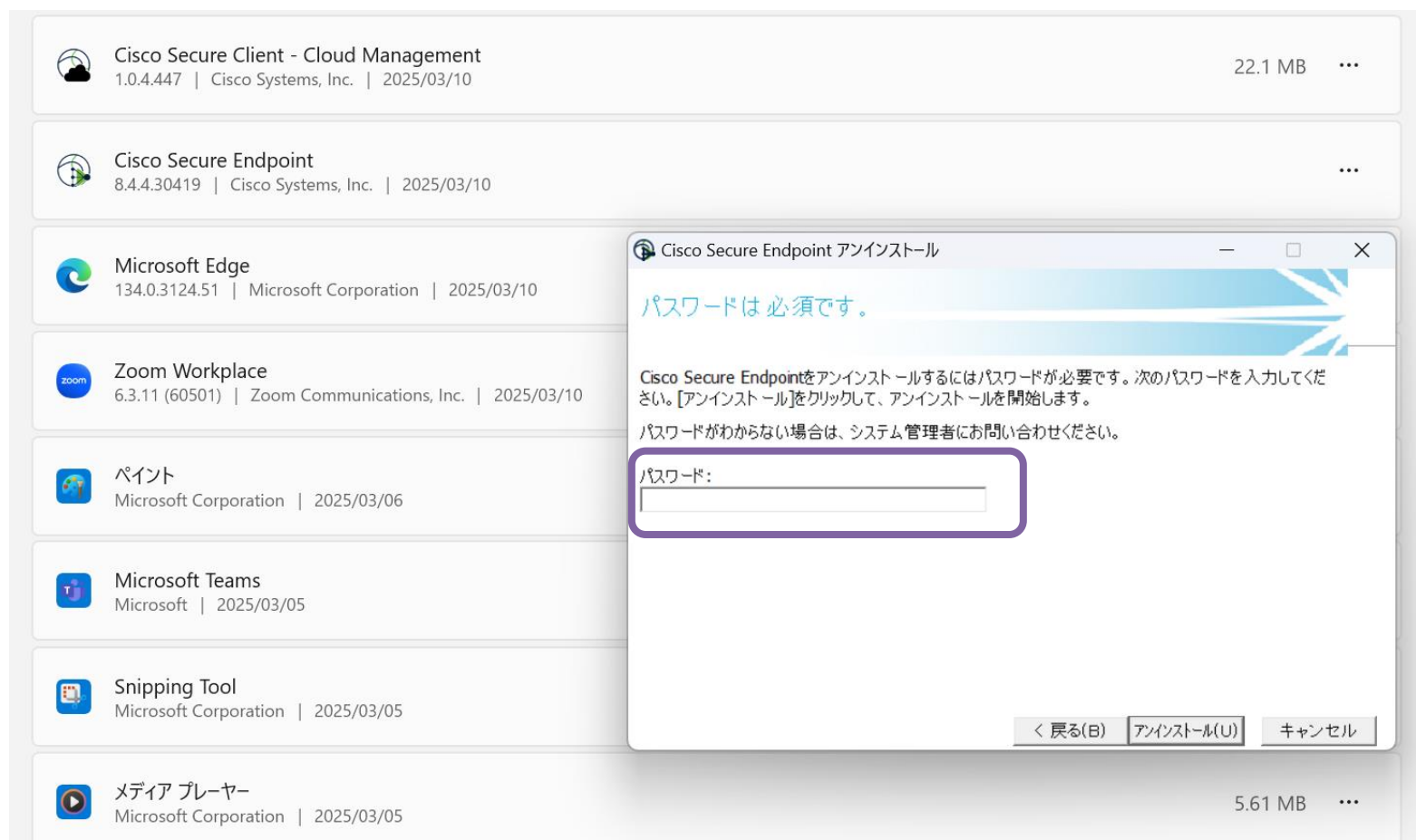
スクリプト保護 ⓘ

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。

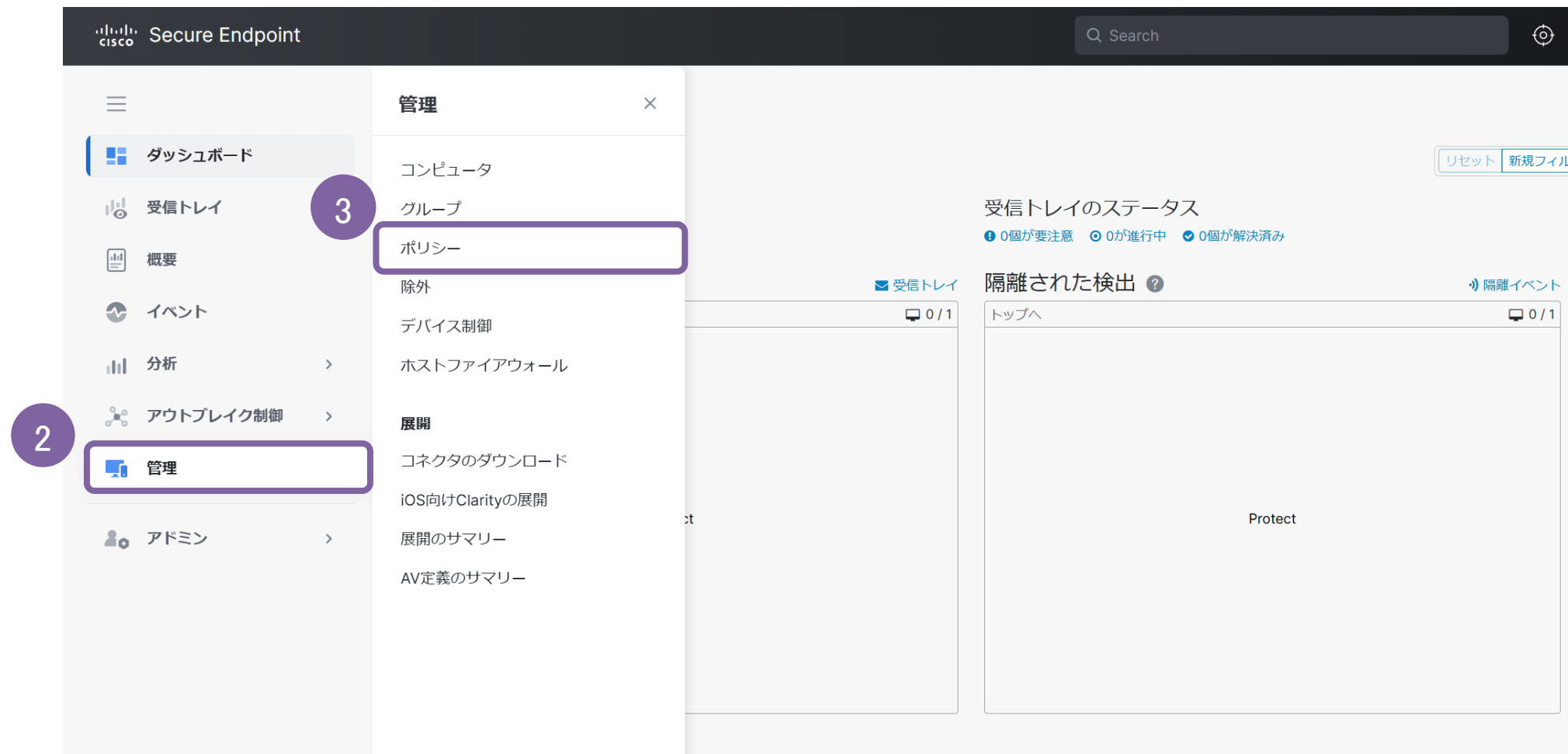


①Secure Endpoint管理コンソールを開き、ログインします。
Secure Endpoint管理コンソール : <https://console.apjc.amp.cisco.com>



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。



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
<div>▶ Audit</div> <div>This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network ...</div>	2025-02-10 10:45:05 JST	1	0
<div>▶ Audit</div> <div>This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network ...</div>	2025-02-10 10:45:09 JST	3	0
<div>▶ Audit</div> <div>This policy puts the Secure Endpoint Connector in a mode that will only detect malicious files but not quarantine them. Malicious network ...</div>	2025-02-10 10:45:10 JST	4	0
<div>▶ Audit</div> <div>This policy puts Clarity in a mode that will log and alert on convictions but not block traffic.</div>	2025-02-10 10:45:12 JST	4	0
<div>▶ Default Network</div> <div>説明がありません</div>	2025-02-10 10:45:13 JST	5	0
<div>▶ Domain Controller</div> <div>This is a lightweight policy for use on Active Directory Domain Controllers.</div>	2025-02-10 10:45:08 JST	1	0
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-03-11 12:14:28 JST	1	1
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 10:45:08 JST	5	0
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 10:45:09 JST	1	0
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 10:45:11 JST	1	0
<div>▶ Protect</div>	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

← ポリシー
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
19個の除外セット

プロキシ

ホストファイアウォール

アウトブレイク制御

デバイス制御

製品の更新

5 詳細設定
管理機能
クライアントユーザーインターフェイス
ファイルとプロセスのスキャン
Cache
エンドポイントの隔離
Orbital
エンジン
TETRA
ネットワーク
定期スキャン

6

☒ イベントでユーザー名を送信する ⓘ

☒ ファイル名とパス情報を送信する ⓘ

ハートビート間隔 15分 ⓘ

コネクタログレベル デフォルト ⓘ

トレイログレベル デフォルト ⓘ

☒ コネクタ保護の有効化 ⓘ

コネクタ保護のパスワード ⓘ

☒ クラッシュダンプの自動アップロード ⓘ

☒ コマンドラインキャプチャ ⓘ

☐ コマンドライン ログ ⓘ

7

キャンセル 保存

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。

Confirm Save

The following settings are set to audit mode:

- エクスプロイト防止 - スクリプト制御

Audit mode reports on malicious activity but does not take any other actions to protect the endpoint.

☐ Don't warn me again

8

Cancel

続行

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ject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。そういった場合に、「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効です。

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是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 へアクセスし、ファイルの送信 へアクセスし、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: malware.exe

参照

分析用のVMイメージ

Windows 7 ×64

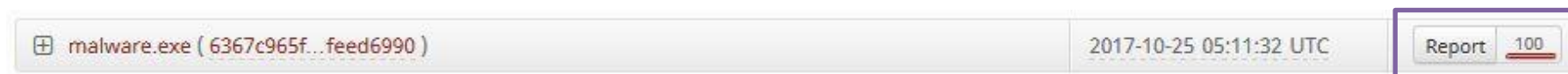
▼

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

Severity: 100 Confidence: 100

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.

Categories Tags

network
network, dns, routing, obfuscation

Query ID

Query Data

3

zsn5qrgt5u4tmgp.tor2web.org

2

zsn5qrgt5u4tmgp.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がない、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の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っ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効です。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ekjrngjker.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 技術 T1105: Ingress Tool Transfer T1204: User Execution T1204.003:
コメント	フィンガープリント(SHA-256)	b1380fd9...df523967
	ファイル名	ekjrngjker.exe
	ファイルパス	C:\ekjrngjker.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。

×

ファイルの取得元コンピュータの選択

ファイル名 Unknown

SHA-256 b1380fd9...df523967

コンピュータを選択します Demo_AMP_Threat_Audit - (ファ

分析用のVMイメージ Windows 7 x64

警告: 分析されたファイルには、組織内のすべてのユーザーが[ファイル分析]ページからアクセスできます。

閉じる 取得して分析のために送信

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 へア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 > ファイルの取得（Fetch File） を実行します。

The screenshot shows the 'Demo AMP' interface. On the left, a sidebar menu is open, and the 'ファイル取得' (File Acquisition) option is highlighted with a purple box. An arrow points from this option to a detailed view on the right. This view shows the 'ファイル取得' (File Acquisition) section with a status of 'ステータス: Requested'. Below this, there are three options: 'シンプル検出' (Simple Detection), 'ブロックされたアプリケーション' (Blocked Application), and '許可されたアプリケーション' (Allowed Application). The 'シンプル検出' option is highlighted with a purple box, and an arrow points to a sub-menu where '[ファイルの取得 (Fetch File)]' is selected, also highlighted with a purple box. The bottom of the interface shows a list of files in the 'ファイルとネットワーク' (Files and Network) section, with 'ekjrnjker.exe [PE]' highlighted in a purple box.

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。

ファイルリポジトリ コネクタ診断機能の概要 すべての変更の表示

検索 タイプ グループ

All Available Requested Being Processed Failed Rejected

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	<input type="button" value="目"/> <input type="button" value="目"/>
元のファイル名:				
フィンガープリント(SHA-256)	3372c1ed...c234a370			
ファイルサイズ	284 KB			
コンピュータ	Demo_TeslaCrypt			
<input type="button" value="① 変更の表示"/>				<input type="button" value="分析"/> <input type="button" value="ダウンロード"/> <input type="button" value="削除"/>

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

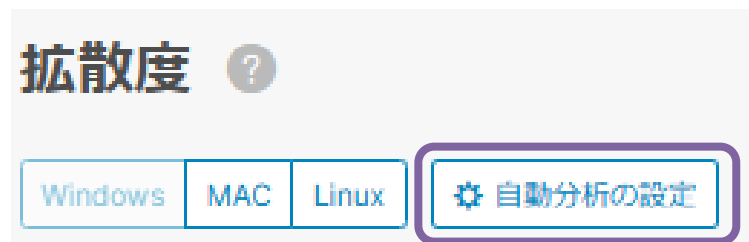
Cisco Secure Endpoint では、低拡散度 と呼ばれる機能があり、ある組織の中であまり実行されていないファイルは Malware の疑いがあるという考えのもと、組織中 (Business) の一つの端末でしか実行されていないファイルをリストアップし、必要に応じて、ファイル分析へ送付させることが可能です。拡散度 は デフォルト設定では、該当ファイルがリストアップされるだけであり、ファイル分析 に送付させるためには、設定が必要となります。

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。

拡散度 ?				
Windows		MAC	Linux	自動分析の設定
▶	25791113...deddb603 は Demo_Command_Line_Arguments_Meterpreterでの...	分析	 	2025-03-25 19:21:06 JST
▶	eba241a9...35feb63a は Demo_Command_Line_Arguments_Meterpreterでの...	分析	 	2025-03-25 19:21:03 JST
▶	30ffb0cc...f1981e0c は Demo_Command_Line_Arguments_Meterpreterでのみ...	分析	 	2025-03-25 19:21:03 JST
▶	f396dcd3...d5ec7f30 は Demo_Command_Line_Arguments_Meterpreterでの...	分析	 	2025-03-25 19:21:03 JST
▶	0cc2c9c2...9e86e32b は Demo_Command_Line_Arguments_Meterpreterでの...	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可能です。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。



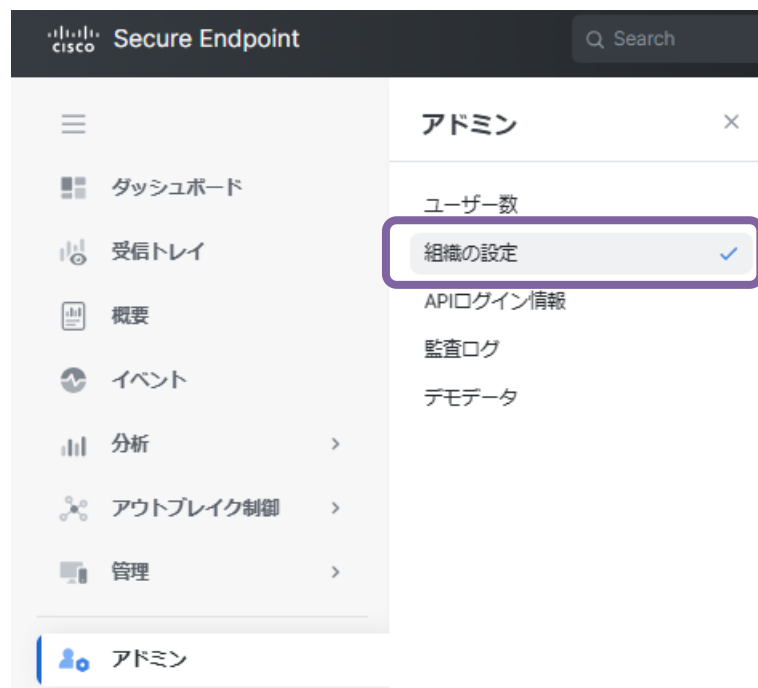
③自動分析の対象となる端末が所属する グループ を指定し、適用 をクリックすれば、実行頻度の低いファイルを自動的に Sandbox 分析にかけることが可能です。



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。

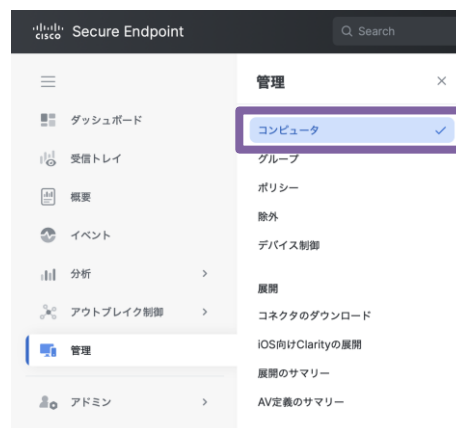
- 1日に実行可能な ファイル分析 の合計カウント数に追加されることとなりますため、数多くファイルが アップロードされる環境では注意が必要です。
- 先ほどと同様、拡散度 からの 自動分析も、端末からのファイルの収集 (Remote File Fetch)を実行するため、二段階認証を有効にする必要があります。有効になっていない場合は、分析 ボタンと 自動分析 ボタンがグレーアウトされて実行できませんので、設定する場合は、事前に設定をお願いします。



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紹介します。

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。

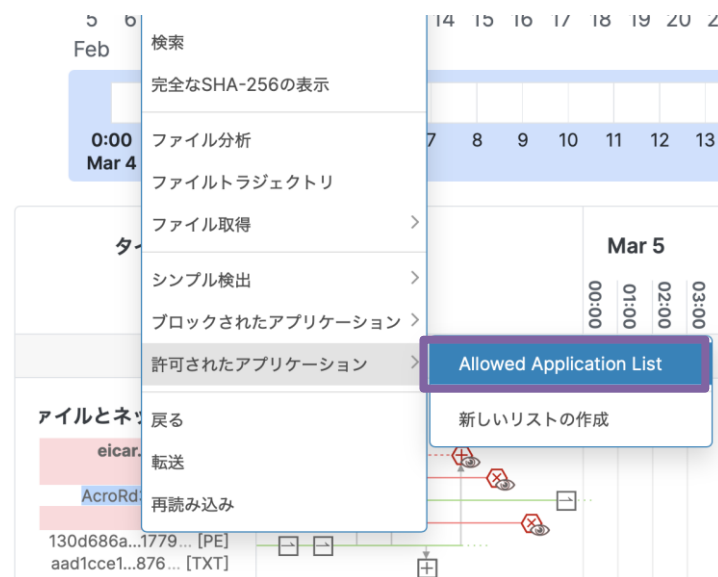


②端末情報を展開すると、デバイストラジェクトリというリンクが表示されるので、それをクリックします。

▼ グループ「Audit」内のDemo_SFEicar			
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 (ビルド 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
イベント デバイストラジェクトリ 診断 変更の表示			
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			

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。

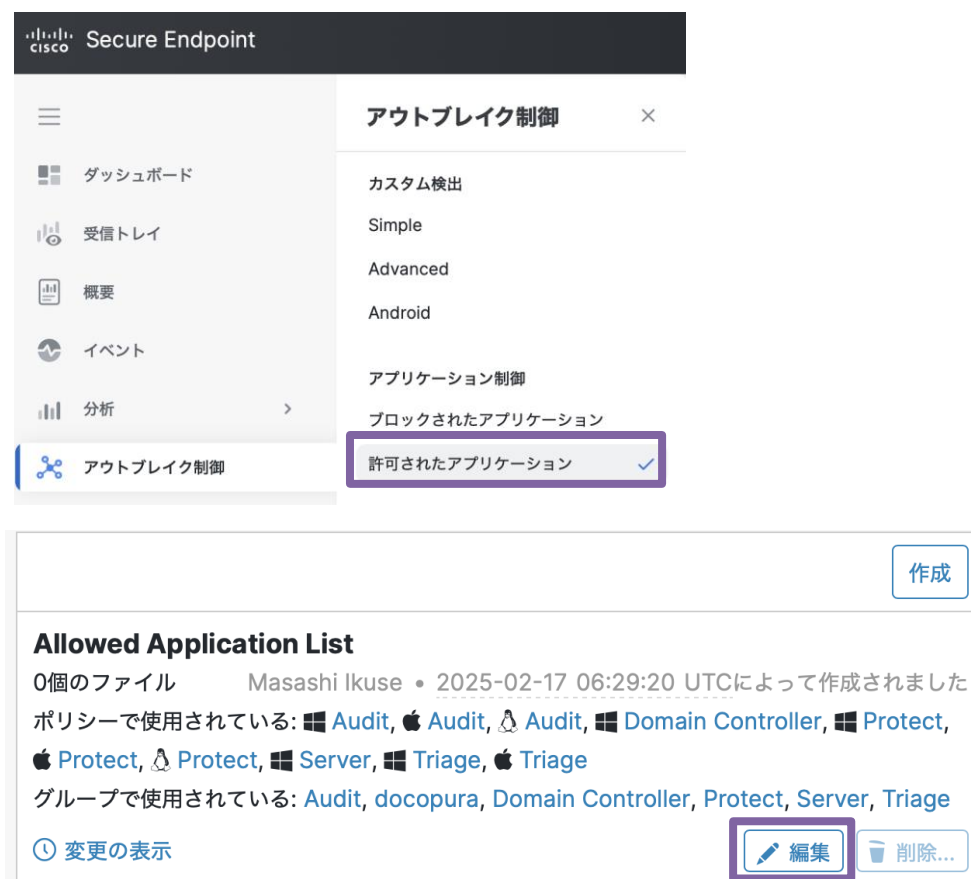


- ④サブメニューが表示されたらAllowed Application List を選択します。レ点が表示されていれば許可リスト（ホワイトリスト）への登録が完了です。



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。



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, 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...

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紹介します。

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

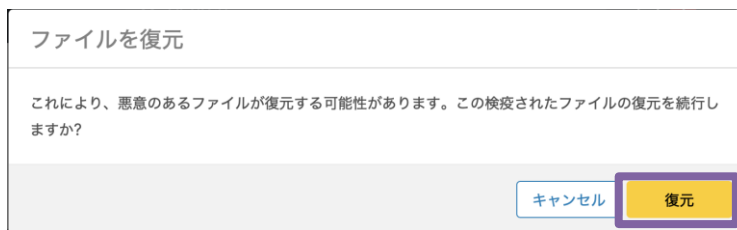


隔離されたファイルの復元方法（つづき）

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

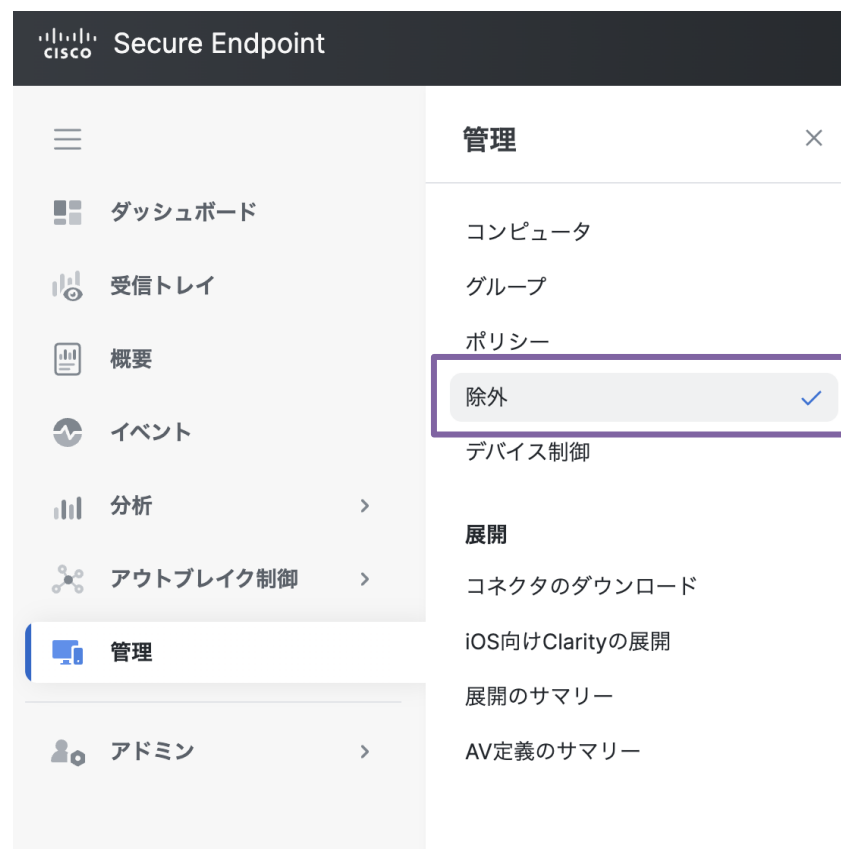
上記に問題がなければ、サポート窓口にお問い合わせください。

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
- 他社アンチウイルス製品との競合が発生してしまっている

対処方法

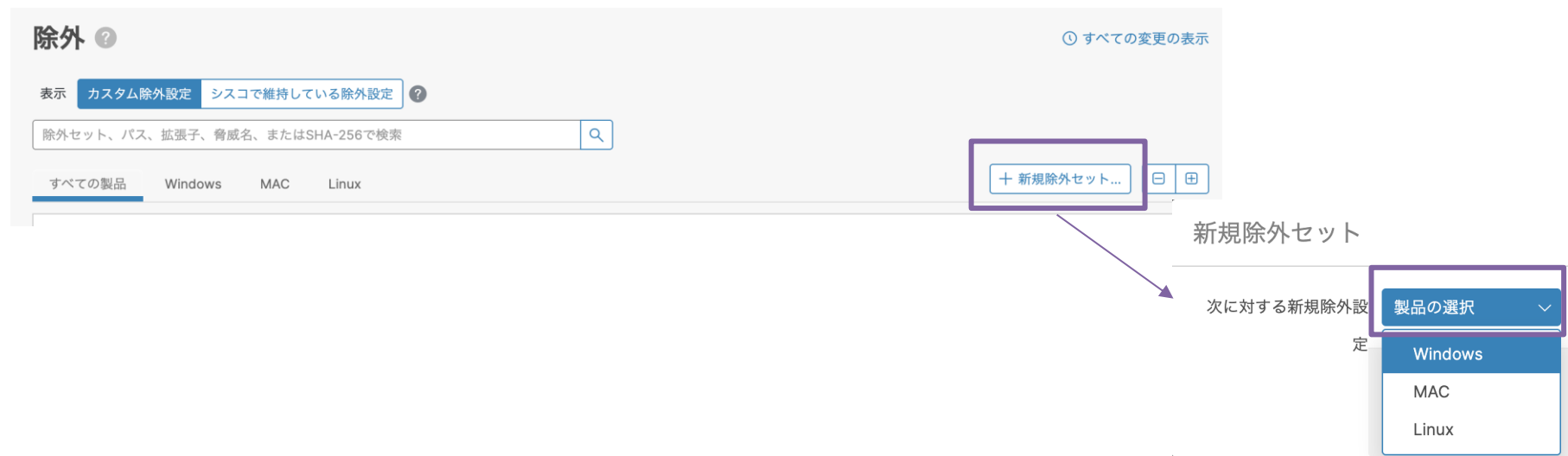
①Cisco Secure Endpoint管理コンソールにログインし、管理 > 除外を選択してください。



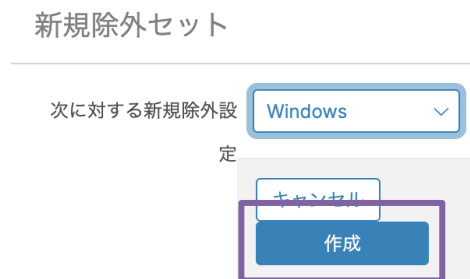
対処方法（つづき）

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)

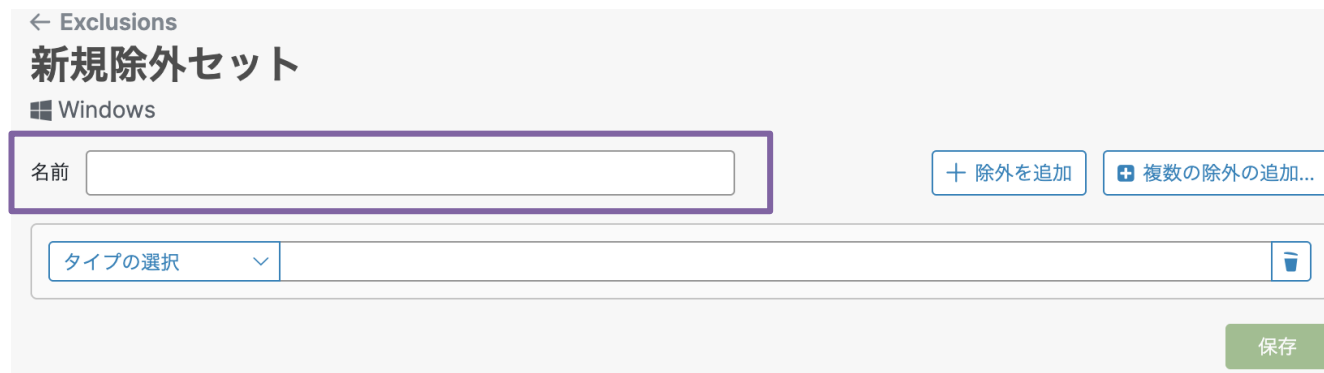


③作成をクリックします



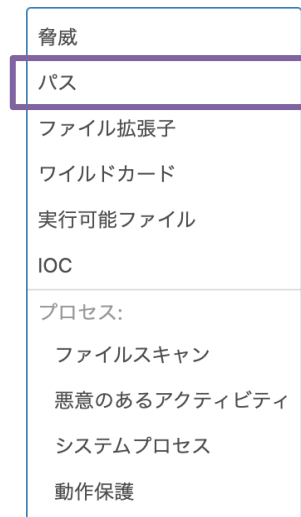
対処方法（つづき）

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。

← Exclusions
新規除外セット
Windows

名前 AMP

+ 除外を追加 + 複数の除外の追加...

パス C:\AMP Test\to be excluded

保存

⑦作成したパスが表示されます。

AMP

AMP 1個の除外 0 0

除外

パス C:\AMP Test\to be excluded

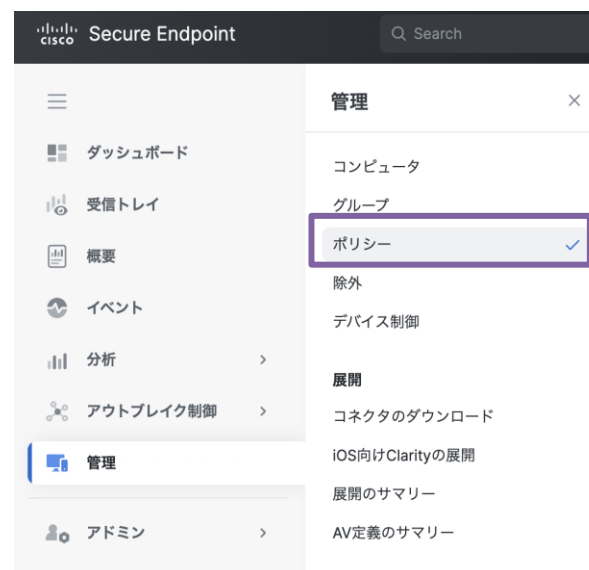
グループで使用
なし

ポリシーで使用
なし

① 変更の表示 変更日 2025-03-07 15:51:45 UTC 編集 削除

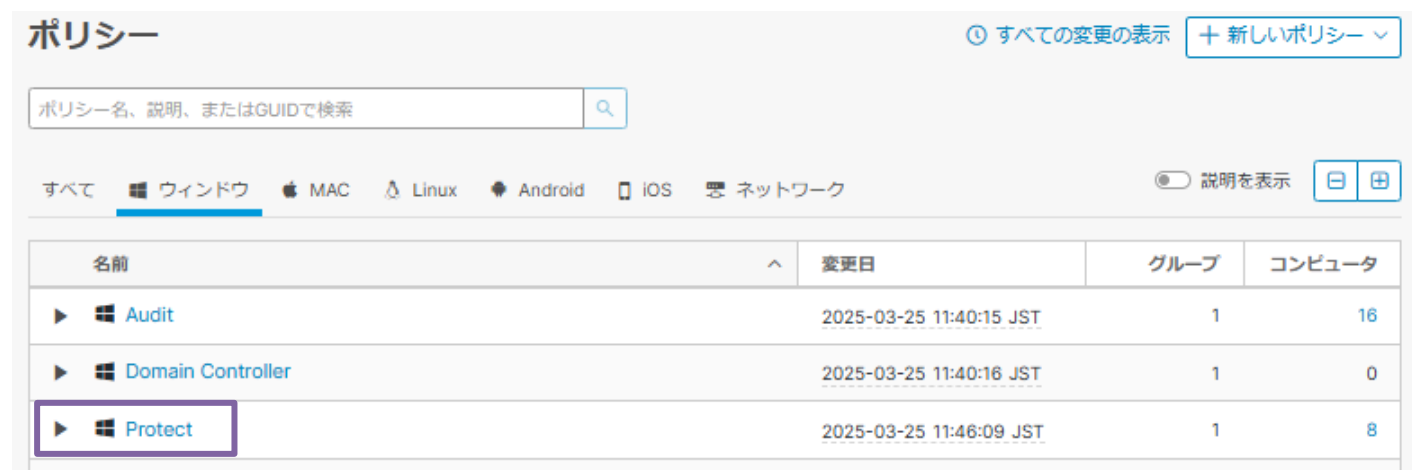
対処方法（つづき）

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。



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。

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** 68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

シスコで維持している除外設定 67件が選択されました

1Password	4個の除外	X
Altiris by Symantec	4個の除外	X
Appsense	6個の除外	X
Arctic Wolf Networks Agent	6個の除外	X
Atera Agent	4個の除外	X
AVAST	3個の除外	X
Avira	3個の除外	X
Azure DevOps	7個の除外	X
Bitdefender	6個の除外	X
Cisco AnyConnect VPN	4個の除外	X
Cisco Webex	14個の除外	X
Citrix AppDNA	2個の除外	X
Citrix Cloud Connector	3個の除外	X
Citrix EdgeSight Server	3個の除外	X
Citrix ICA Client	14個の除外	X

カスタム除外設定 1件が選択されました

検索

☒ すべて

☒ AMP 1個の除外

1個の除外 X

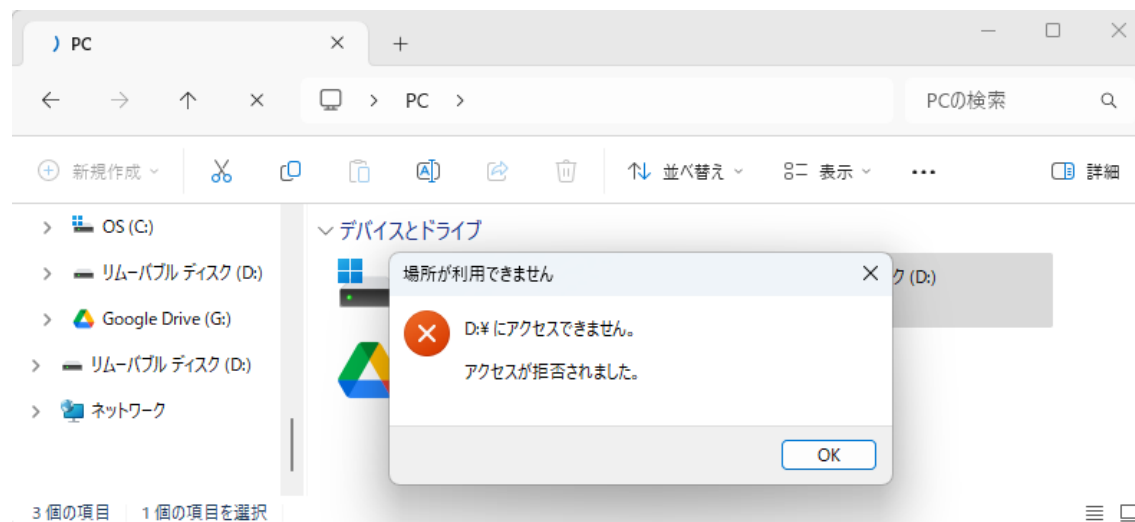
保存 キャンセル

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可能です。

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>

1

Secure Endpoint

検索

8

?

🌐

👤

どこブラ管理 NTT...

ODS用検証環境

☰

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

アドミン

最新のイベント

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

最新のコンピュータ

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

最近の監査ログ

sso_logi	User	dokopura_mssp13@west.ntt.co.jp	2025-07-02 07:37:12 UTC
sso_logi	User	dokopura_mssp12@west.ntt.co.jp	2025-07-02 05:23:18 UTC
create	Computer	ODS-NewZero1	2025-07-01 02:14:15 UTC
update	Webhook::WebhookSubscription	a82f10dc-ddcd-44d4-83bb-edb47a884d84-posaas-hook	2025-06-28 10:55:45 UTC
update	Webhook::WebhookSubscription	605c29be-3f78-43b3-878d-b1ea7879f2e0-posaas-hook	2025-06-28 03:41:07 UTC

最近のポリシー

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

最近のアウトブレイク制御リスト

ファイルリスト	Simple Custom Detection List	2025-02-10 01:35:15 UTC
除外セット	TEST	2025-06-06 07:30:34 UTC

アプリケーション

アプリケーションが見つかりません

ライセンス情報

195

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。

管理

コンピュータ

グループ

ポリシー

除外

デバイス制御

展開

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

AV定義のサマリー

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

アドミン

検索

7

NTT...

ODS用検証環境

すべて表示

as completed without detecting anything malicious. 2025-07-01 06:38:34 UTC

t has started scanning. 2025-07-01 06:36:53 UTC

ent download failed 2025-07-01 06:14:24 UTC

ent download failed 2025-07-01 06:14:18 UTC

ent download failed 2025-07-01 06:14:18 UTC

最近のコンピュータ

すべて表示

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

最近のアウトブレイク制御リスト

すべて表示

ファイルリスト	Simple Custom Detection List	2025-02-10 01:35:15 UTC	すべて表示
除外セット	TEST	2025-06-06 07:30:34 UTC	すべて表示

アプリケーション

アプリケーションが見つかりません

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。

Secure Endpoint

検索

7

?

🌐

👤

どこブラ管理 NTT...

ODS用検証環境

☰

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

アドミン

デバイス制御

名前、説明、最終更新日、GUIDで検索

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 説明がありません	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: どこブラ管理 NTT西日本	<div>✎</div> <div>🗑</div>

1個の項目の1~1

25 / ページ

<

1

1個の

>

+ 新規設定

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

4

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。

新規設定

5 名前
USB利用の制御

6 説明(任意)
USB無効化の設定

7 設定タイプの選択

- USB大容量ストレージ
外部ハードドライブやUSBメモリなど、エンドポイントに接続されているUSBストレージデバイスを管理します。
- Windowsポータブルデバイス
エンドポイントに接続されているスマートフォンやデジタルカメラなど、他のUSBデバイスのストレージ機能を管理します。

キャンセル 保存

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。

8

新規設定

名前

USB利用の制御

説明(任意)

USB無効化の設定

USB大容量ストレージ

基本ルール

次にデフォルト権限を設定します。

ブロック

読み取り専用

読み取りと書き込みのみ

読み取り、書き込み、および実行

エンドポイントユーザに通知: ●

常に保存

常にしない

キャンセル

保存

9

【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。

Windowsポータブルデバイス

基本ルール

次にデフォルト権限を設定します。

ブロック

読み取り専用

読み取りと書き込みのみ

読み取り、書き込み、および実行

エンドポイントユーザに通知: ●

常に保存

常にしない

キャンセル

保存

199

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

Secure Endpoint

検索

7

?

🌐

👤

どこブラ管理 NTT...
ODS用検証環境

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

アドミン

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: どこブラ管理 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

USB大容量ストレージのルール ?

ルール(1/1000)

すべてのUSB大容量ストレージ

条件

許可

エンドポイントユーザに通知

最終更新日

2025-07-03 02:21:27 UTC
更新者: どこブラ管理 NTT西日本

常に保存

✎

キャンセル

保存

+ ルールの追加 (Add Rule)

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

フィードバックを送ってください

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 console interface. On the left, the navigation menu is visible with the '管理' (Management) option highlighted by a red circle and labeled with the number 11. A secondary menu is open, showing 'ポリシー' (Policy) highlighted by a red circle and labeled with the number 12. The main content area displays a list of events and a table of recent computers.

管理

- コンピュータ
- グループ
- ポリシー**
- 除外
- デバイス制御
- 展開
- 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
- AV定義のサマリー

最近のコンピュータ

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

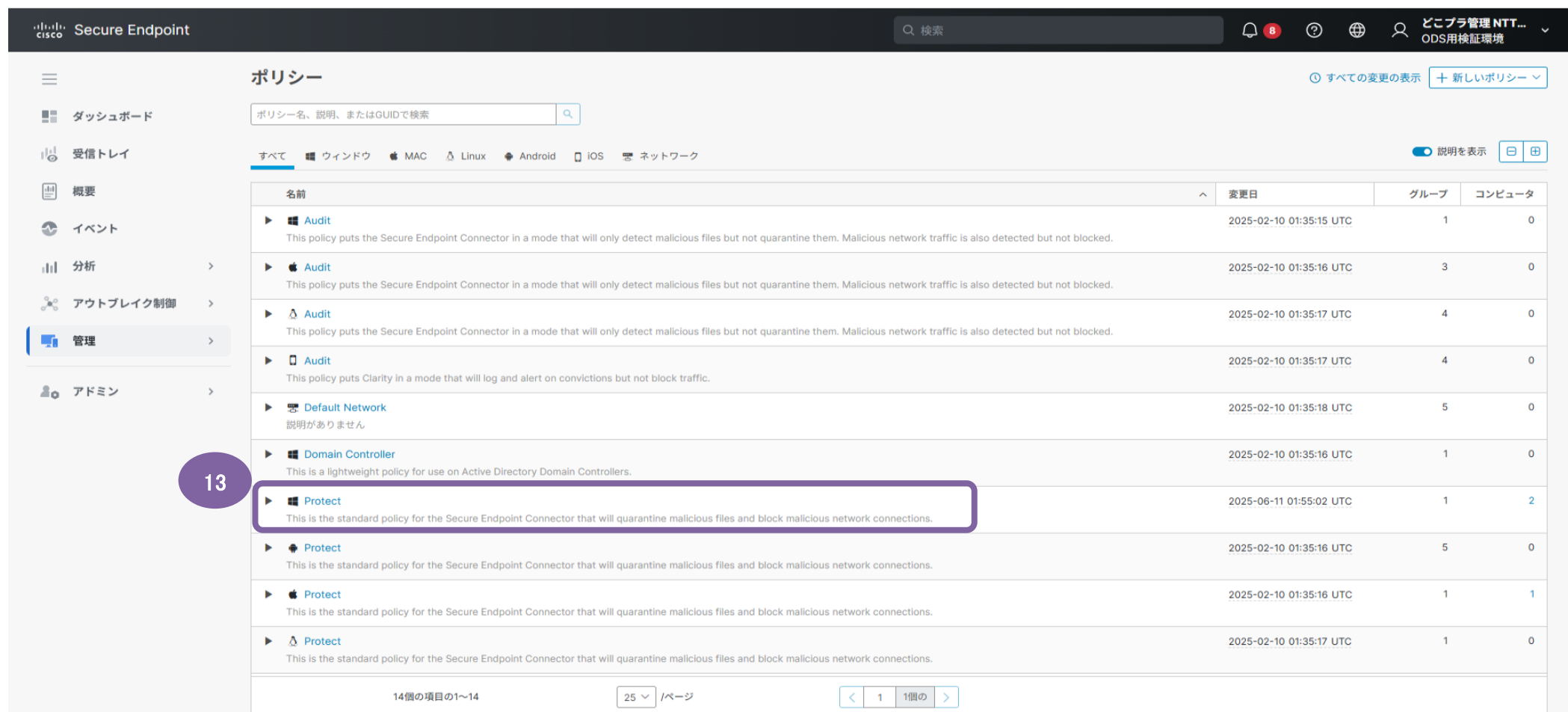
最近のアウトレイク制御リスト

ファイルリスト	Simple Custom Detection List	2025-02-10 01:35:15 UTC	すべて表示
除外セット	TEST	2025-06-06 07:30:34 UTC	すべて表示

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 management interface. The left sidebar contains navigation 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), and アドミン. The main area is titled 'ポリシー' (Policy) and includes a search bar and tabs for different operating systems: ウィンドウ, MAC, Linux, Android, iOS, and ネットワーク. A table lists the policies, with the 'Protect' policy for Windows highlighted. A red circle with the number 13 points to this policy.

名前	変更日	グループ	コンピュータ
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.	2025-02-10 01:35:15 UTC	1	0
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.	2025-02-10 01:35:16 UTC	3	0
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.	2025-02-10 01:35:17 UTC	4	0
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.	2025-02-10 01:35:17 UTC	4	0
Default Network 説明がありません	2025-02-10 01:35:18 UTC	5	0
Domain Controller This is a lightweight policy for use on Active Directory Domain Controllers.	2025-02-10 01:35:16 UTC	1	0
Protect This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.	2025-06-11 01:55:02 UTC	1	2
Protect This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.	2025-02-10 01:35:16 UTC	5	0
Protect This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.	2025-02-10 01:35:16 UTC	1	1
Protect This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.	2025-02-10 01:35:17 UTC	1	0

14個の項目の1~14 25 / ページ < 1 1個の >

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

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

アドミン

← ポリシー

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

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

Show policy guidance

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。

ファイル ①

検疫

監査

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 ①

ブロック

監査

無効

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。

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 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 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は、停止、削除して、報告します。

エクスプロイトの防止 ①

ブロック

監査

無効

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。

エクスプロイト防止 - スクリプト制御 ①

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

203

デバイス制御方法（続き）

⑮「デバイス制御」をクリックします。

The screenshot shows the Cisco Secure Endpoint management console. The top navigation bar includes the Cisco logo, 'Secure Endpoint', a search bar, and user information. The left sidebar contains a menu with items like 'Dashboard', 'Inbox', 'Summary', 'Events', 'Analysis', 'Outbreak Control', 'Management', and 'Admin'. The 'Management' item is expanded, and 'Device Control' is highlighted with a blue bar and a purple circle containing the number 15. The main content area is titled 'Policy Edit' for 'Windows'. It shows the policy name 'Protect' and a description. Below this, there are sections for 'Device Control' and 'Windows Portable Device'. The 'Device Control' section has a description and a 'Configuration' dropdown set to 'None'. The 'Windows Portable Device' section also has a description and a 'Configuration' dropdown set to 'None'. At the bottom, there is a link to 'Manage Device Control Settings'.

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。



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）
⑰ 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。

Secure Endpoint

検索

通知7

ヘルプ

グローバル

ユーザー

どこまで管理 NTT...
ODS用検証環境

メニュー

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

アドミン

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

アウトブレイク制御

デバイス制御

製品の更新

詳細設定

デバイス制御

以下のリストから、ポリシーに割り当てするデバイス制御設定を選択します。

USB大容量ストレージ

外部ハードドライブやUSBメモリなど、エンドポイントに接続されているUSBストレージデバイスを管理します。

Configuration USB利用の制御 設定の管理

ルール	条件	許可	エンドポイントユ- 知
すべてのUSB大容量ストレージ	1	ブロック	常に保存

1個の項目の1~1 25 /ページ < 1 1個の >

Windowsポータブルデバイス

エンドポイントに接続されているスマートフォンやデジタルカメラなど、他のUSBデバイスのストレージ機能を管理します。

Configuration なし

新しい設定を作成する

デバイス制御設定

Windowsポータブルデバイスの制御
Windowsポータブルデバイス無効化の設定

なし
Windowsポータブルデバイスタイプのデバイス制御を無効にしま
す

保存 キャンセル

デバイス制御方法（続き）

⑱「保存」をクリックします。

Secure Endpoint

検索

通知7

ヘルプ

グローバル

ユーザー

どこブラ管理 NTT...
ODS用検証環境

メニュー

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

アドミン

モードとエンジン

除外
69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

説明

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

デバイス制御

以下のリストから、ポリシーに割り当てるデバイス制御設定を選択します。

USB大容量ストレージ

外部ハードドライブやUSBメモリなど、エンドポイントに接続されているUSBストレージデバイスを管理します。

Configuration

USB利用の制御

設定の管理

ルール	条件	許可	エンドポイントユ- 知
すべてのUSB大容量ストレージ	1	ブロック	常に保存

1個の項目の1~125 / ページ<11個の>

Windowsポータブルデバイス

エンドポイントに接続されているスマートフォンやデジタルカメラなど、他のUSBデバイスのストレージ機能を管理します。

Configuration

Windowsポータブルデバイスの制御

設定の管理

ルール	条件	許可	エンドポイントユ- 知
すべてのWindowsポータブルデバイス	1	ブロック	常に保存

1個の項目の1~125 / ページ<11個の>

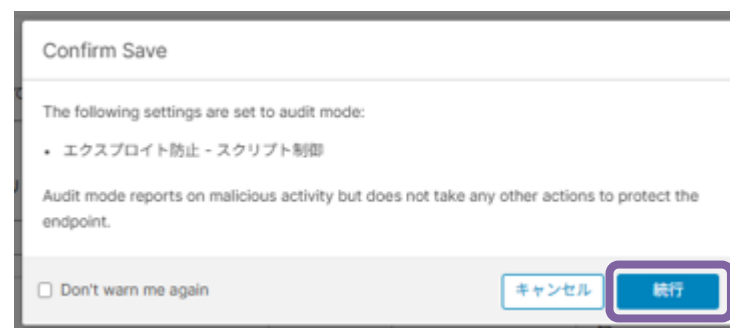
新しい設定を作成するか、既存の設定を管理します。
デバイス制御設定の管理

保存キャンセル

デバイス制御方法（続き）

①9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。



19

デバイス制御方法（続き）

⑳以下画面が表示されますので、これにて設定完了です。

Secure Endpoint

検索

7

?

🌐

👤

どこブラ管理 NTT ...
ODS用検証環境

☰

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

アドミン

20

ポリシー"Protect"が正常に更新されました。

ポリシー

すべての変更を表示

+ 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
<div>▶ Audit</div> <div>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.</div>	2025-02-10 01:35:15 UTC	1	0
<div>▶ Audit</div> <div>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.</div>	2025-02-10 01:35:16 UTC	3	0
<div>▶ Audit</div> <div>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.</div>	2025-02-10 01:35:17 UTC	4	0
<div>▶ Audit</div> <div>This policy puts Clarity in a mode that will log and alert on convictions but not block traffic.</div>	2025-02-10 01:35:17 UTC	4	0
<div>▶ Default Network</div> <div>説明がありません</div>	2025-02-10 01:35:18 UTC	5	0
<div>▶ Domain Controller</div> <div>This is a lightweight policy for use on Active Directory Domain Controllers.</div>	2025-02-10 01:35:16 UTC	1	0
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-07-03 02:48:42 UTC	1	2
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 01:35:16 UTC	5	0
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 01:35:16 UTC	1	1
<div>▶ Protect</div> <div>This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.</div>	2025-02-10 01:35:17 UTC	1	0
<div>▶ Protect</div> <div></div>	2025-02-10 01:35:18 UTC	1	0

14個の項目の1〜14

25 / ページ

< 1 1個の >

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。



elgana連携機能

<通知機能①>

「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に通知

<通知機能②>

EDRセキュリティにおける
ファイル隔離／端末隔離を通知

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 elgana management interface. The top header displays the elgana logo and the text 'elgana. 管理'. The sidebar on the left contains navigation links: 基本 (Basic), ダッシュボード (Dashboard), ユーザー (User), 利用端末 (Usage Terminal), 環境設定 (Environment Settings), サービス連携 (Service Linkage), 詳細 (Details), 契約プラン (Contract Plan), 管理者 (Administrator), メッセージログ (Message Log), ファイル (File), 操作履歴 (Operation History), プランをアップグレード (Upgrade Plan), ご利用ガイド (Usage Guide), カスタマーサポート (Customer Support), and ご利用者ヘルプ (User Help). The main content area is titled 'ユーザー' (User) and shows the number of registered users (2) and the number of contracted users (10). A green box labeled '2' highlights the 'ユーザー' section. A green box labeled '1' highlights the 'ユーザー登録' (User Registration) button. The table below shows a list of users with columns 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 (Update Date), and トーク数制限 (Talk Limit).

氏名	組織1	組織2	アカウント状況	更新日	トーク数制限
[Redacted]			利用中	2024/12/10	
[Redacted]			利用中	2024/12/10	

10. elganaの設定手順（登録したユーザで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、トーク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

セキュリティおまかせプラン どこでもプライム 16:15 今日

対処できていない脅威が6件あります。
簡易情報は次以降のメッセージで送付します。

また詳細情報に関しては、
<https://sign-on.security.cisco.com/>
から管理コンソールにログインいただき、ご確認ください。

すべてのプログラムを一度終了させ、
フルスキャンを実施いただくことをお勧めします。

対応方法、詳細情報の確認をする場合は、
下記連絡先までお問合せをお願いいたします。

電話番号：0800-200-7920
受付時間：平日 午前9時～午後5時
（土・日・祝日・年末年始12月29日～1月3日は休業とさせていただきます）

セキュリティおまかせプラン どこでもプライム 16:15

1件目
概要：Threat Detected
デバイス名：[REDACTED]
発生時刻：3月19日 16:10

端末隔離・解除の通知

セキュリティおまかせプラン どこでもプライム 16:15 今日

端末隔離が起きている端末が1件あります。
詳細情報は次以降のメッセージで送付します。

対応方法、詳細情報の確認をする場合は、下記連絡先までお問合せをお願いいたします。

電話番号：0800-200-7920
受付時間：平日 午前9時～午後5時
（土・日・祝日・年末年始12月29日～1月3日は休業とさせていただきます）

セキュリティおまかせプラン どこでもプライム 16:15

1件目
以下のデバイスで端末隔離が発生しました。
デバイス名：[REDACTED]
発生時刻：3月19日 16:11



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。



DKFまたはDKO + 数字10桁

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 displays the Cisco Umbrella management console. On the left sidebar, the 'DKF' label is highlighted in a red box, with a red arrow pointing to a red-bordered text box that reads 'DKFまたはDKO + 数字10桁'. The main dashboard area shows a summary of blocked requests for Malware, Botnet, and Cryptomining, along with network health metrics.

DKFまたはDKO + 数字10桁

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

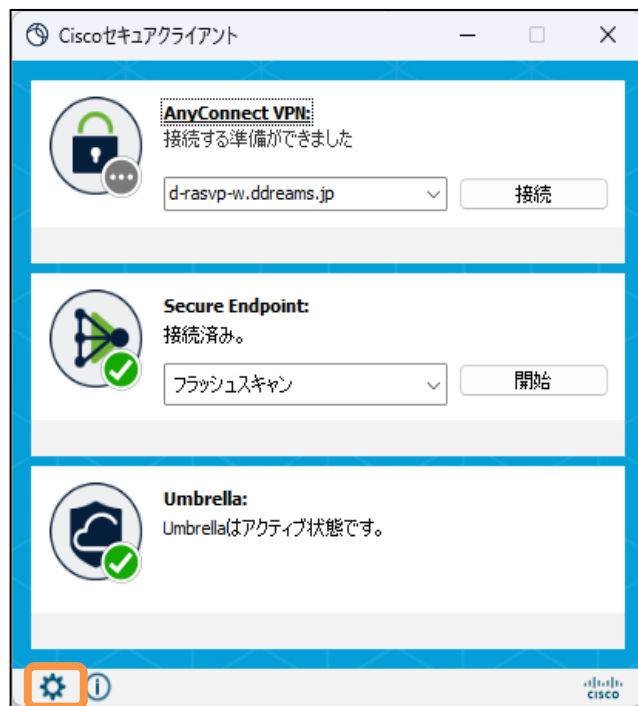
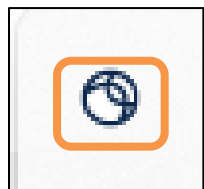
12-1. DARTログの取得手順_Windows 1/4

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

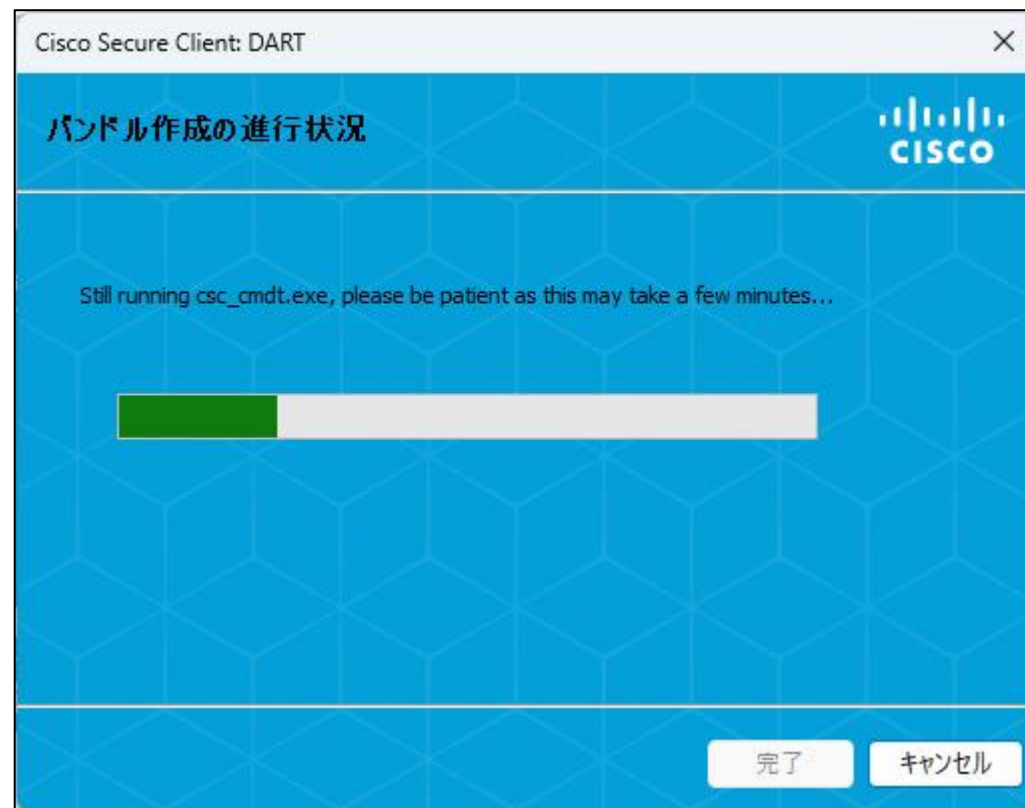
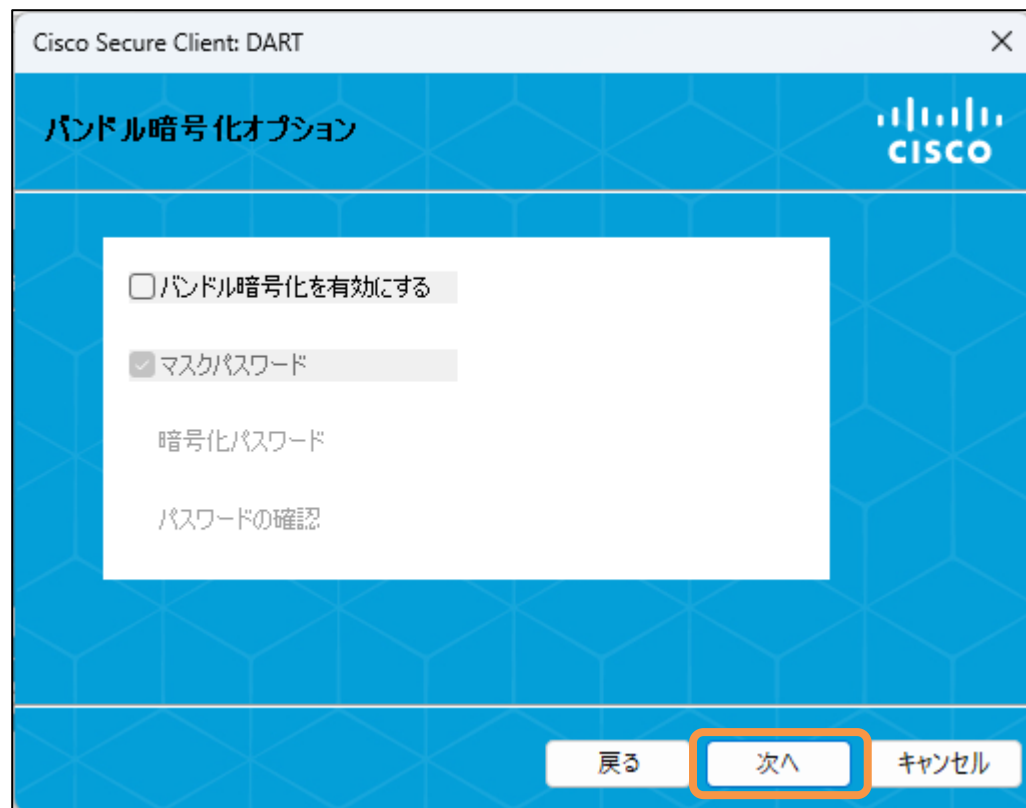


12-1. DARTログの取得手順_Windows 3/4

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

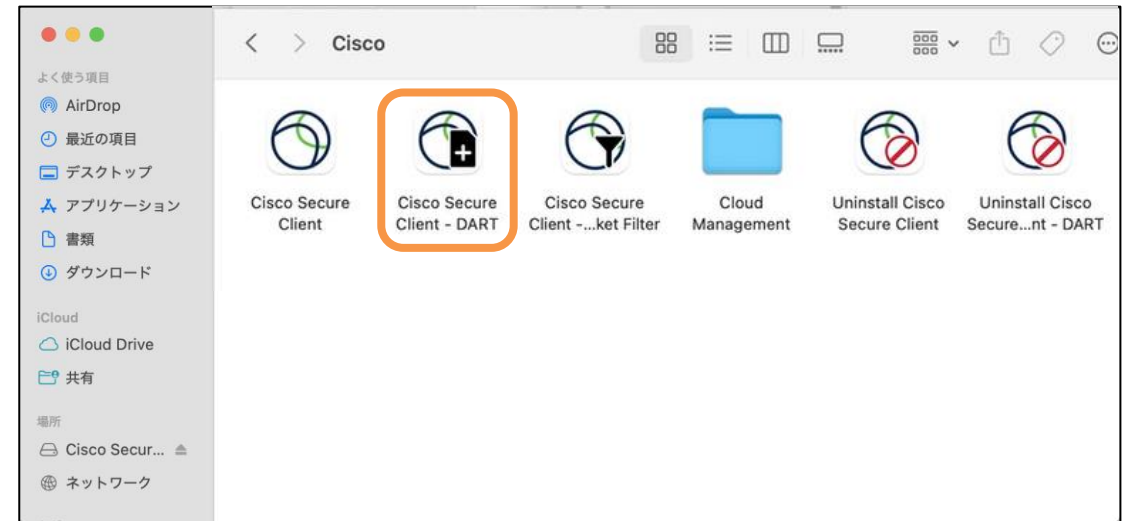
12-1. DARTログの取得手順_Mac 1/3

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



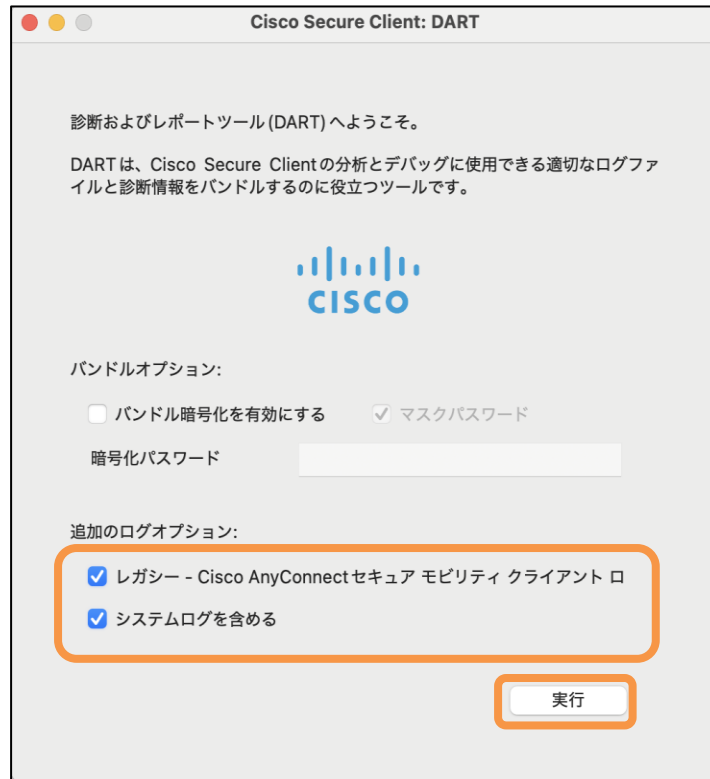
「Cisco Secure Client - DART」をダブルクリック



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

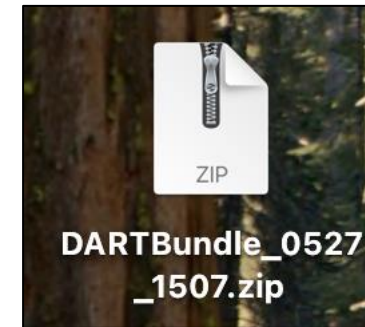
以下画像「完了」までの処理が終わると、デスクトップにログファイル「DARTBundle_(日付)_(時刻).zip」が生成されます。

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。

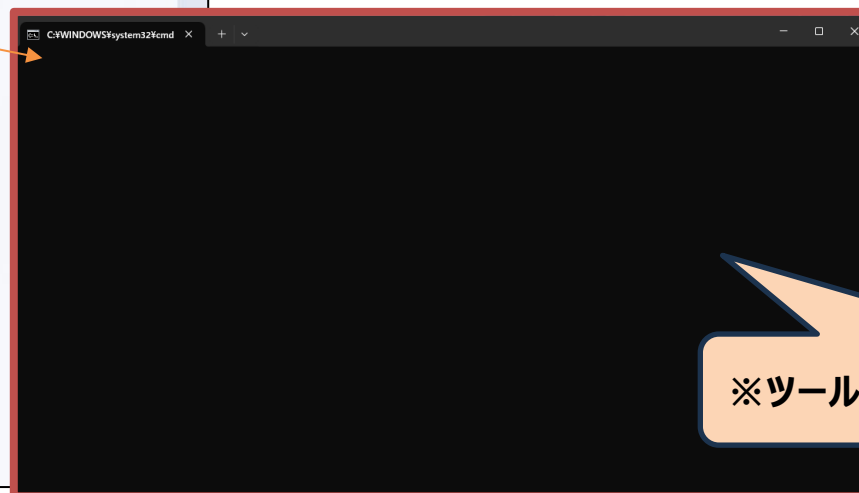
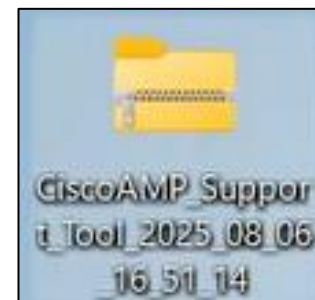
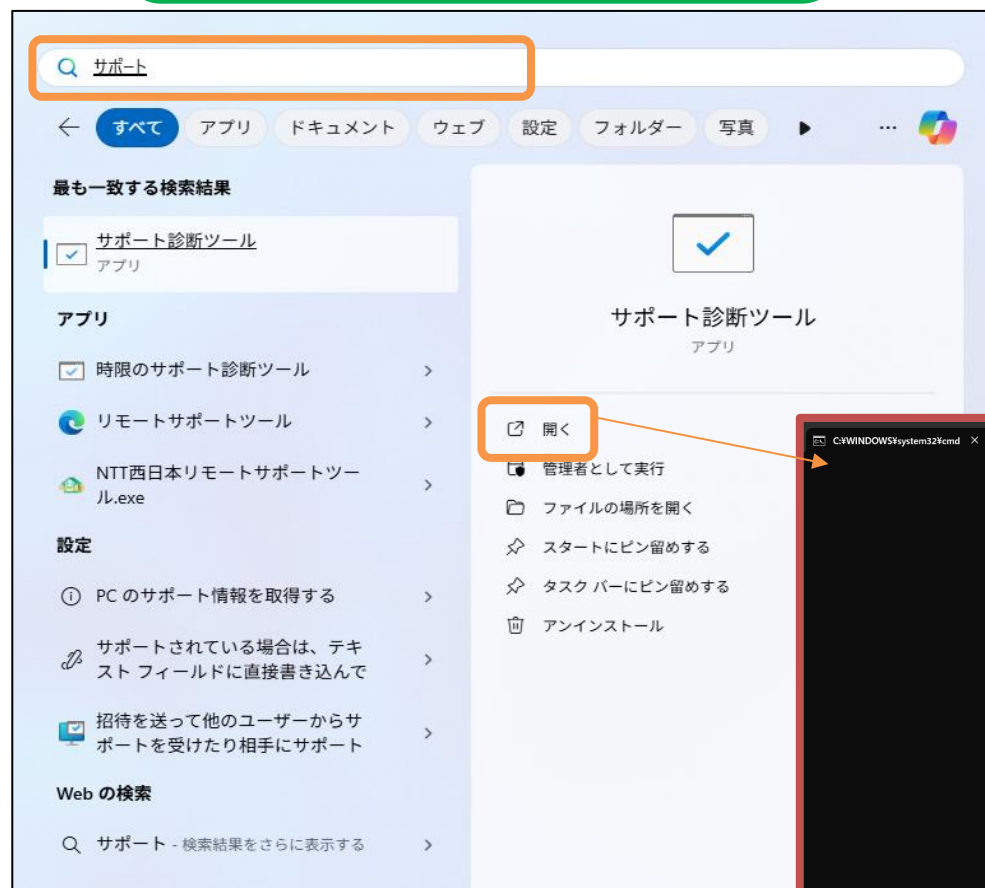
設定完了後、本ページの作業を実施いただきますようお願いいたします。

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。

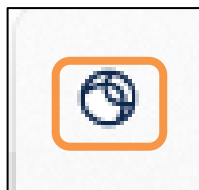


※ツール実行中はこの画面が表示されます

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

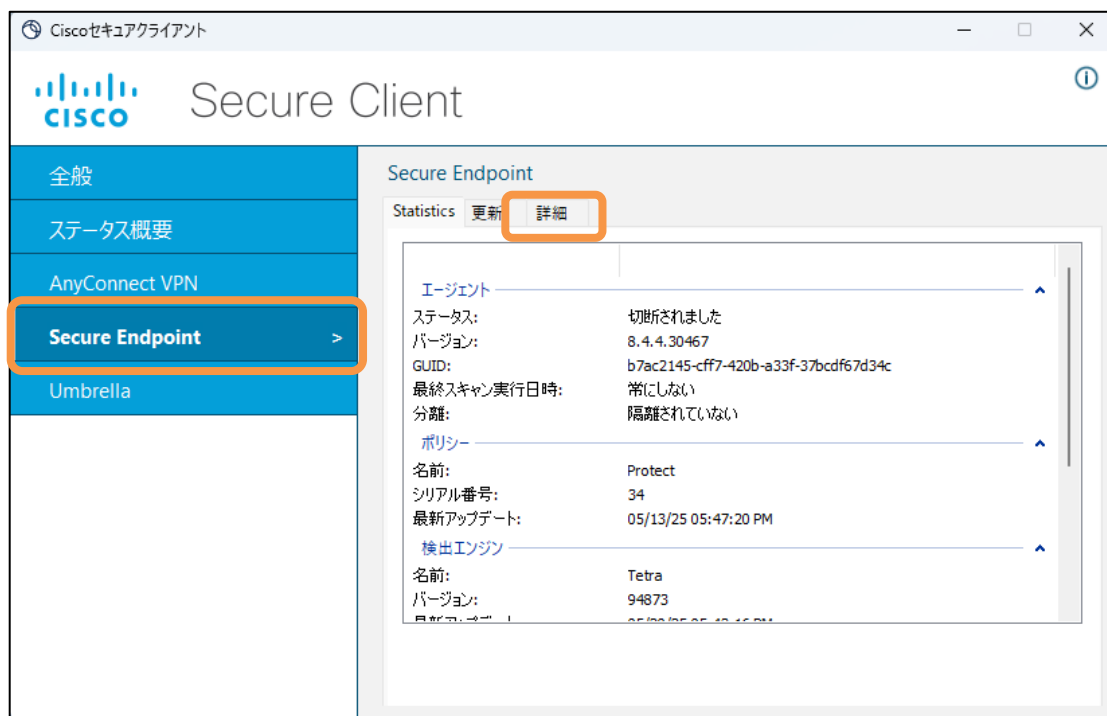


(参考) サポート診断ツールログの取得手順_Windows <デバッグロギング有効> 2/3

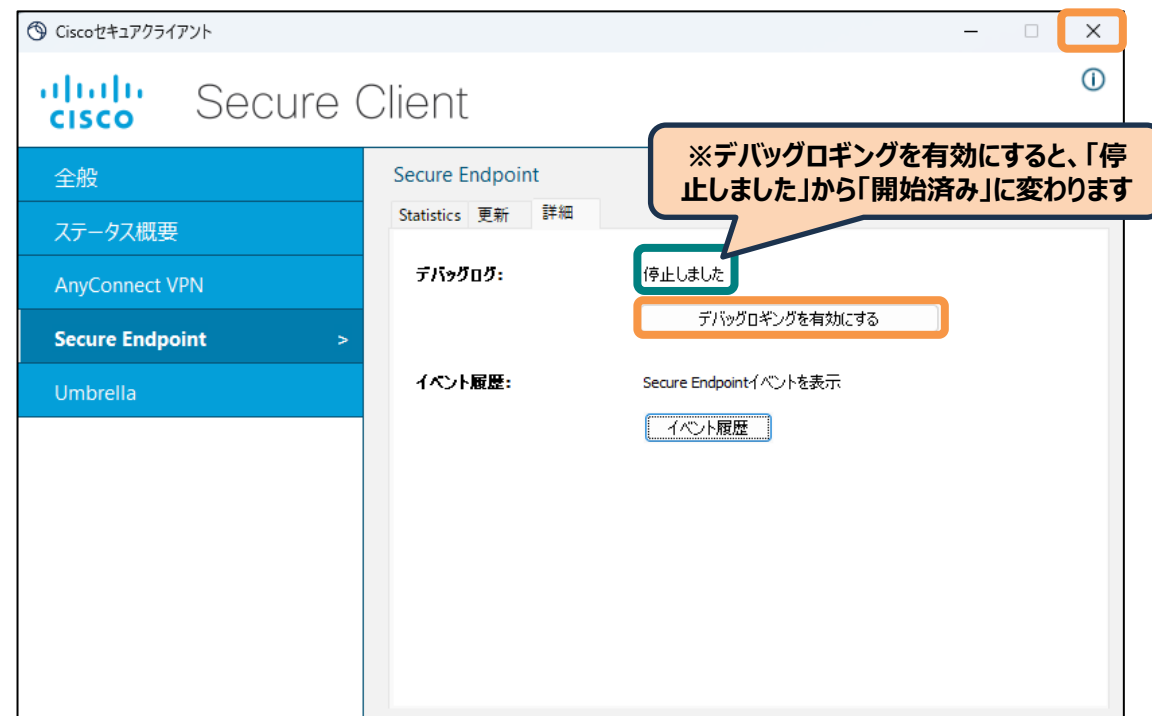
以下手順に従い、デバッグロギングを有効にしてください。

※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

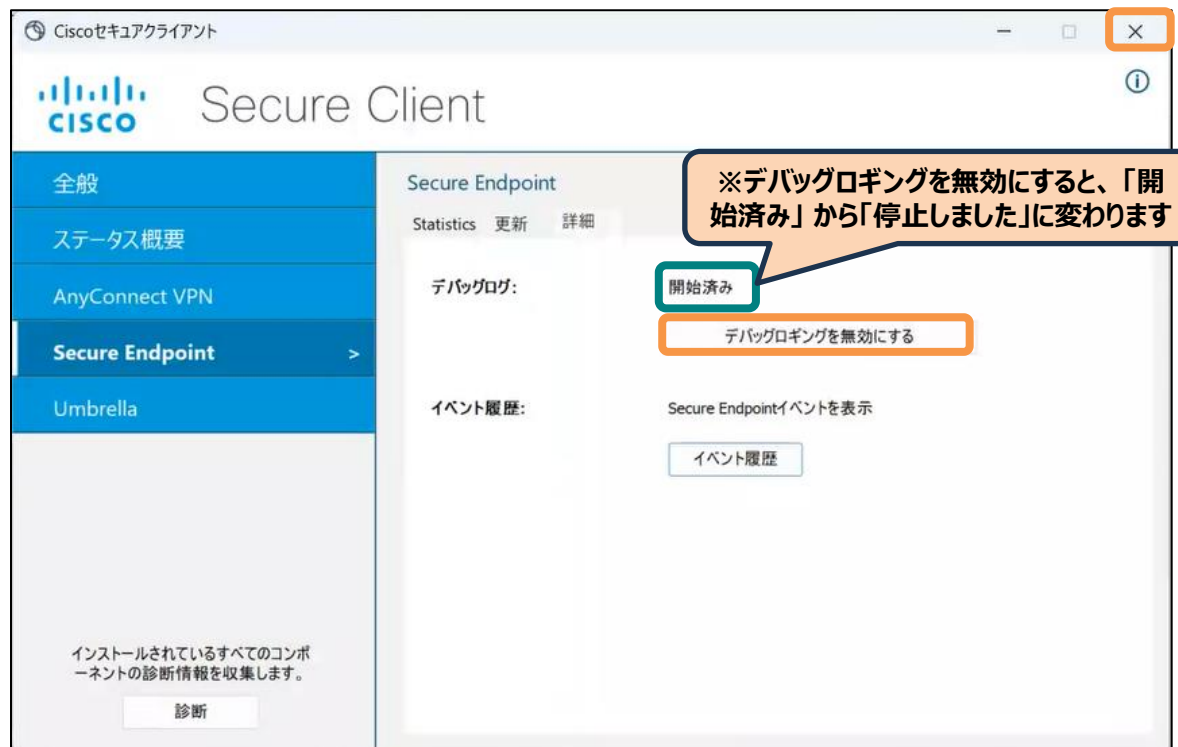


「デバッグロギングを有効にする」をクリックし、「×」で画面を閉じる



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

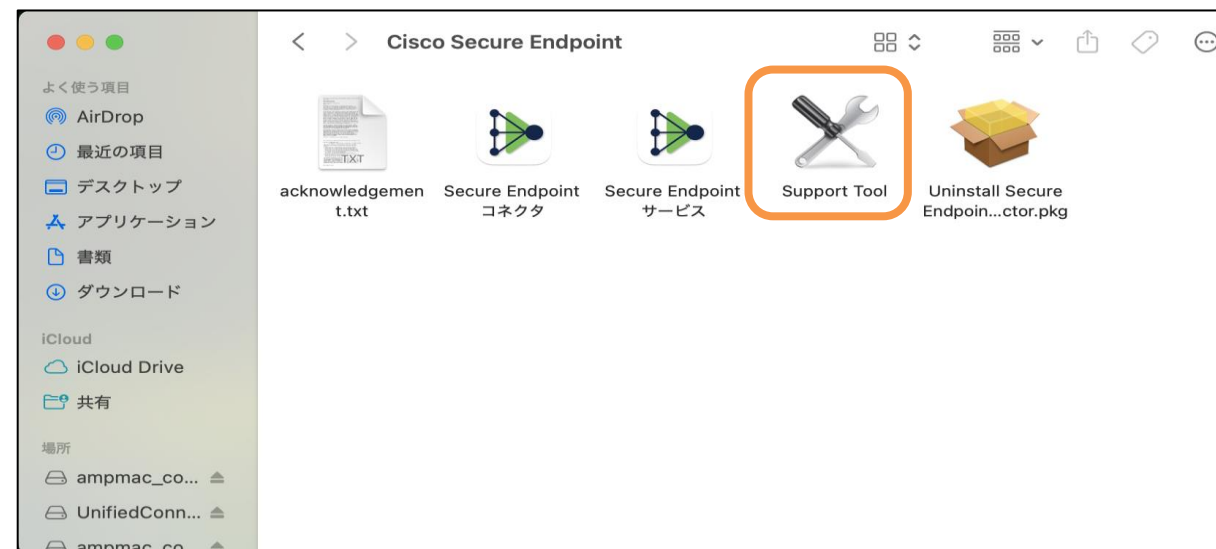
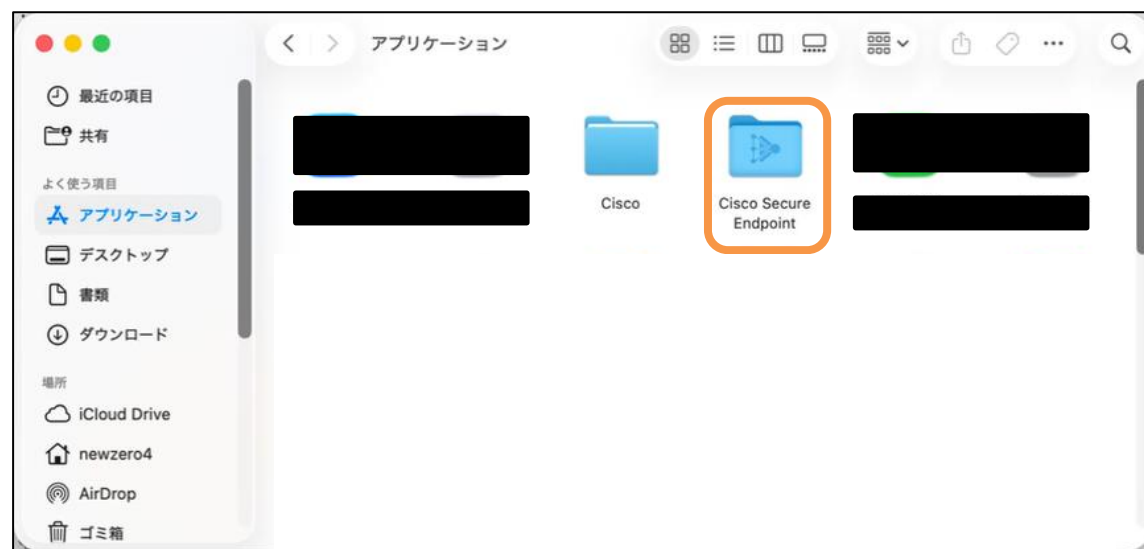
12-2. サポート診断ツールログの取得手順_Mac 1/2

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

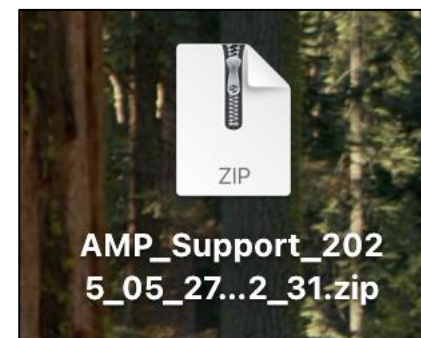
デスクトップにログファイル「AMP_Support_(西暦)_(月)_(日)_(時)_(分)_(秒).zip」が生成されます。

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 console interface. The left sidebar contains a navigation menu with the following 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 (highlighted with an orange box), and アドミン. The '管理' (Management) section is expanded, showing a sub-menu with: 設定インサイト, コンピュータ, グループ, **ポリシー** (highlighted with an orange box), 除外, デバイス制御, 展開, 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. The main content area displays several panels: 'Signature set updated' logs, '最近のコンピュータ' (Recent Computers) table, '最近のアウトブレイク制御リスト' (Recent Outbreak Control List) table, and 'アプリケーション' (Applications) section.

OS	バージョン	ホスト名	グループ
macOS 26.0.1	1.27.0.1046	[REDACTED]	Protect
Windows 11, SP 0.0	8.5.0.30551	[REDACTED]	Protect
Windows 11, SP 0.0	8.4.4.30419-DEPRECATED	[REDACTED]	Protect
macOS 15.5.0	1.26.0.1010	[REDACTED]	Protect

ファイルリスト	Simple Custom Detection List	2025-02-10 01:35:15 UTC	すべて表示
除外セット	TEST	2025-06-06 07:30:34 UTC	すべて表示

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. 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 content area is titled 'ポリシー' (Policy) and includes a search bar and tabs for different operating systems: 'すべて', 'ウィンドウ', 'MAC', 'Linux', 'Android', 'iOS', and 'ネットワーク'. The 'MAC' tab is selected and highlighted with an orange box. Below the tabs, a table lists three policies: 'Audit', 'Protect', and 'Triage'. The 'Protect' policy is highlighted with an orange box. The table columns are '名前' (Name), '変更日' (Modified), 'グループ' (Group), and 'コンピュータ' (Computer). The footer contains login information and a copyright notice for Cisco Systems, Inc.

名前	変更日	グループ	コンピュータ
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.	2025-02-10 01:35:16 UTC	3	0
Protect This is the standard policy for the Secure Endpoint Connector that will quarantine malicious files and block malicious network connections.	2025-02-10 01:35:16 UTC	1	2
Triage This is an aggressive policy that enables the offline engine to scan computers that are suspected or known to be infected with malware.	2025-02-10 01:35:17 UTC	1	0

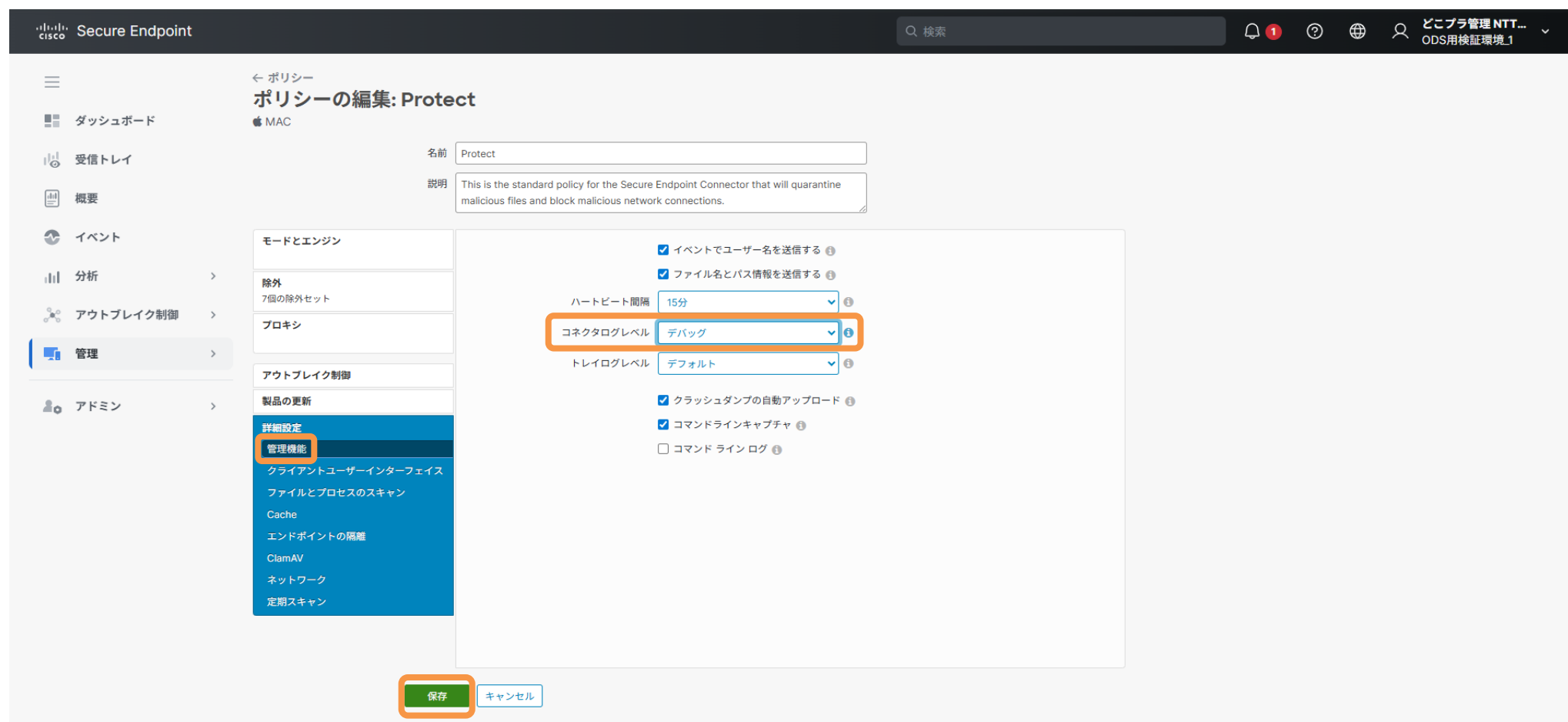
3個の項目の1~3 30 / ページ < 1 1個の >

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
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



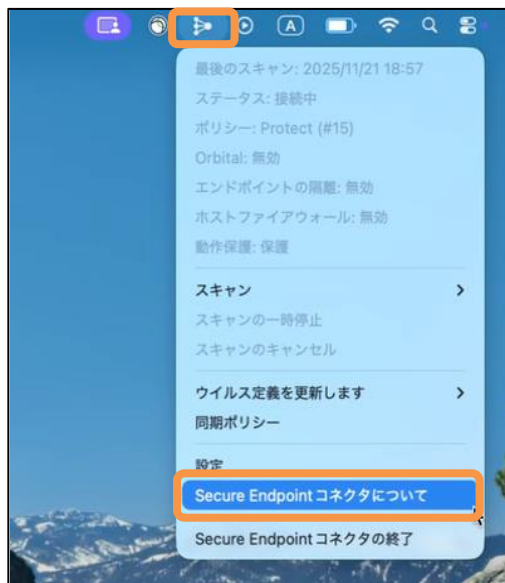
(参考) サポート診断ツールログの取得手順_Mac <デバッグモード有効化> 4/5

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」となっているのを、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. The left sidebar contains a menu with 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, and アドミン. The '管理' (Management) option is selected and highlighted. The main content area is titled 'ポリシーの編集: Protect' and shows the configuration for a policy named 'Protect'. The 'モードとエンジン' (Mode and Engine) section is expanded, showing '除外' (Exclusions) and 'プロキシ' (Proxy) settings. The 'コネクタログレベル' (Connector Log Level) is set to 'デフォルト' (Default). The '保存' (Save) button is highlighted at the bottom.

Cisco Secure Endpoint

検索

どこプラ管理 NTT...
ODS用検証環境_1

← ポリシー
ポリシーの編集: Protect
MAC

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
7個の除外セット

プロキシ

アウトブレイク制御

製品の更新

詳細設定
管理機能
クライアントユーザーインターフェイス
ファイルとプロセスのスキャン
Cache
エンドポイントの隔離
ClamAV
ネットワーク
定期スキャン

イベントでユーザー名を送信する
ファイル名とパス情報を送信する
ハートビート間隔 15分
コネクタログレベル デフォルト
トレイログレベル デフォルト
クラッシュダンプの自動アップロード
コマンドラインキャプチャ
コマンドラインログ

保存 キャンセル

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】

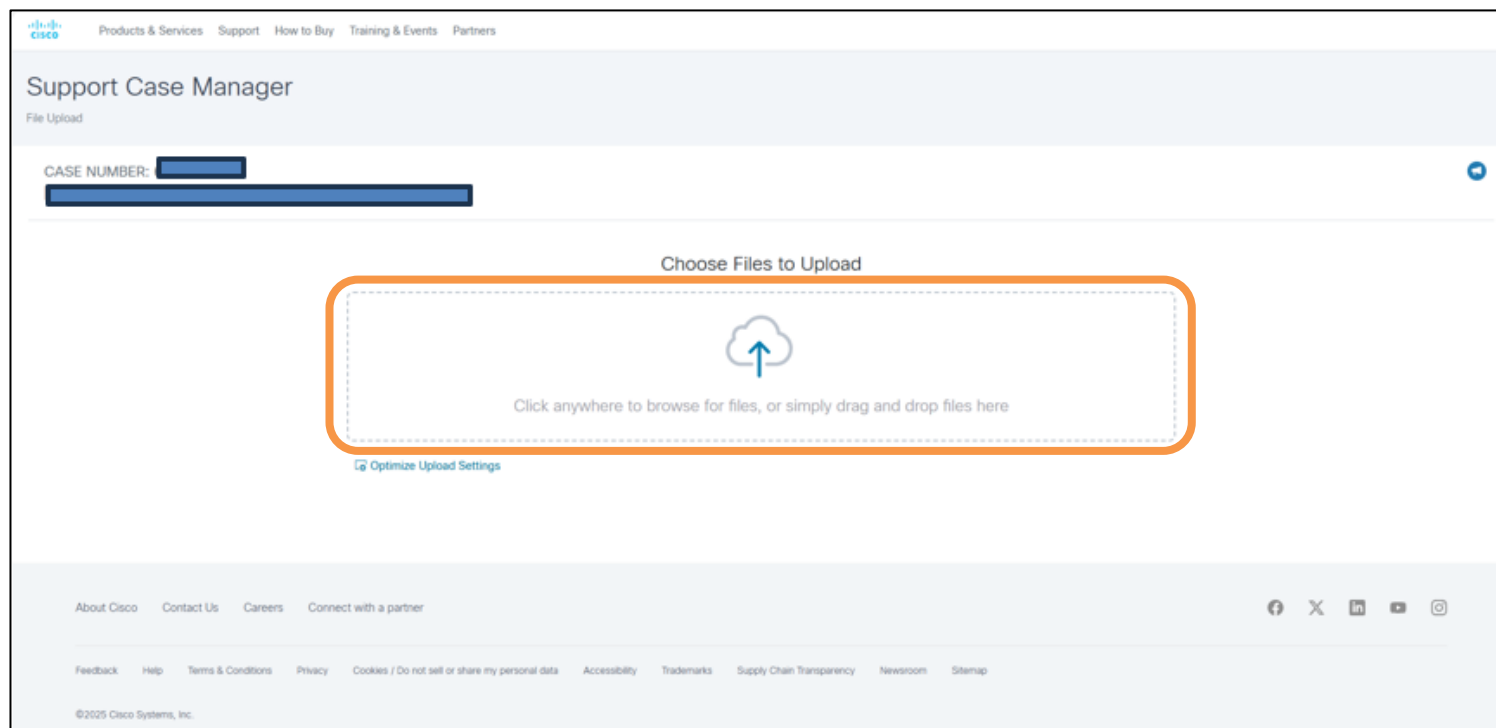
- ①該当端末でGoogle Chrome/Microsoft edgeを開きます。
- ②デベロッパーツール(開発者ツール)を開きます。
- ③[Network]タブを開き、[Preserve log]と[Disable cache]にチェックを入れます。
- ④レコーディングが開始されていることを確認します。
- ⑤「ネットワークログのクリア」アイコンをクリックし、ログを一旦削除します。
- ⑥表示できないサイトのURLを開きます。
- ⑦エラー画面が表示されたら右上のダウンロードボタンからファイルを出力します。

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。

The screenshot shows the Cisco Support Case Manager File Upload page. At the top, there is a navigation bar with links: Products & Services, Support, How to Buy, Training & Events, and Partners. Below this is the 'Support Case Manager' header and 'File Upload' sub-header. A 'CASE NUMBER:' field is visible. The main section is titled 'Choose Files to Upload'. It features a dashed box with a cloud icon and an upward arrow, containing the text 'Click anywhere to browse for files, or simply drag and drop files here'. To the right, a box labeled 'Files selected for upload' contains a file named 'テスト.txt' (53.77 KB). Below the dashed box, there are radio buttons for 'Add File Descriptions': 'No Description' (selected), 'Specify one description for all files', and 'Specify a description for each file'. There is also a link for 'Optimize Upload Settings'. An 'Upload' button is at the bottom right. A green callout bubble points to the file list with the text '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' (Confirm that the uploaded file name is displayed). An orange box highlights the 'No Description' radio button and the 'Upload' button.