

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 1.0)

2025年3月
西日本電信電話株式会社

No	Date	主な変更内容	Ver
1	2025/3/31	初版	1.0
2			
3			
4			
5			
6			
7			
8			
9			

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 P6
4. ソフトウェアのインストール手順 P7 ~ P40
5. ソフトウェアのアンインストール手順 P41 ~ P52
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 P53 ~ P60
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 P61 ~ P112
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 P113 ~ P123
9. セキュアエンドポイント機能を設定変更する P124 ~ P165
10. elgana連携の設定手順 P166 ~ P170

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 セキュアエンドポイントと記載

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

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	macOS 11、12、13、14
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。	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

※上記の表以外のOSはサポート対象外

4. ソフトウェアのインストール手順

WindowsOSの場合

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

MacOSの場合

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

4-1. 開通メールからelganaマイページへログイン

4-1. インストール手順 <elganaマイページへのログイン-1>

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

項目	情報
TO	(申込書にご記載いただいたメールアドレス)
BCC	〇〇〇
From	dokopura-kaian@west.ntt.co.jp
件名	NTT西日本セキュリティおまかせプランどこでもプライムのご案内 (契約ID XXXXXX) ※配信専用※
本文	<p>セキュリティおまかせプラン どこでもプライムご契約者様 (契約ID XXXXXX)</p> <p>この度は NTT西日本 セキュリティおまかせプラン どこでもプライムへのお申込みありがとうございます。 どこでもプライムの契約ID数や端末設定ツールのダウンロードURLなどの情報を送付いたします。 ご契約総ID数：●●ID</p> <p>尚、サービスが有効になるのは、ご利用開始予定日のYYYY年MM月DD日からとなっております。 ご利用開始前にインストールされた場合、さかのぼっての課金対象となりますのでご注意ください。</p> <p>ご利用開始日になりましたら次のURLから端末設定ツールをダウンロードいただき、 手順書に従って、クライアントソフトのインストールを実施ください。</p> <p>◆端末設定ツール (インストーラーおよびルート証明書) https://connect-contract.elgana.jp/connectMyPage アカウント名：(申込書にご記載いただいたメールアドレス) 初期パスワード：(開通センターで設定するパスワード)</p> <p>※複数端末にインストールされる場合、上記からダウンロードした端末設定ツールを端末に展開ください。 ※ご契約総ID数を超過し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> <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>

① 開通メールイメージ

② 端末設定ツール入手用のURL及びログイン情報

4-1. インストール手順 <エルガナマイページへのログイン-2>

③ elganaコネクトのログイン画面へ遷移

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



4-2. インストーラーのダウンロード

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

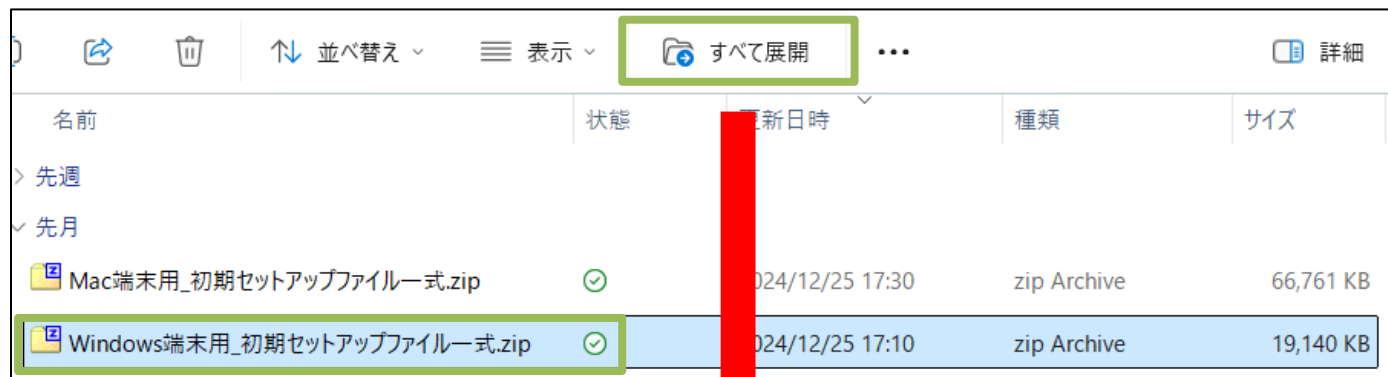
The screenshot shows the elgana Connect user interface. At the top left is the elgana logo and 'elgana コネクト'. At the top right is a link for 'よくあるご質問' and a 'ログアウト' button. The main heading is 'マイページ'. Below it is a message: 「サービス一覧へ進む」からサービスをお申し込みください. A red button labeled 'サービス一覧へ進む' is centered. Below this are two tabs: 'お客様情報' and 'サービス契約内容'. The 'サービス契約内容' tab is active, showing 'ワークスペース情報'. A field for 'ワークスペースID' contains 'ntt-west-test110'. Below this is the text '上記ワークスペースIDで契約中のサービス'. 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' is present. At the bottom left are fields for 'elgana 利用開始日' and 'elgana 利用完了日'. In the center, it says '未インストール/インストール済み'. To the right, there are two buttons: 'Windows用' and 'Mac用'. 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' on the right side of the image.

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)



名前	状態	更新日時	種類	サイズ
> 先週				
> 先月				
Mac端末用_初期セットアップファイル一式.zip	✓	2024/12/25 17:30	zip Archive	66,761 KB
Windows端末用_初期セットアップファイル一式.zip	✓	2024/12/25 17:10	zip Archive	19,140 KB

展開後のファイル構成

名前	状態	更新日時	種類	サイズ
csc-deploy-network-000000_NIPPON TEL...	✓	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

👉 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>

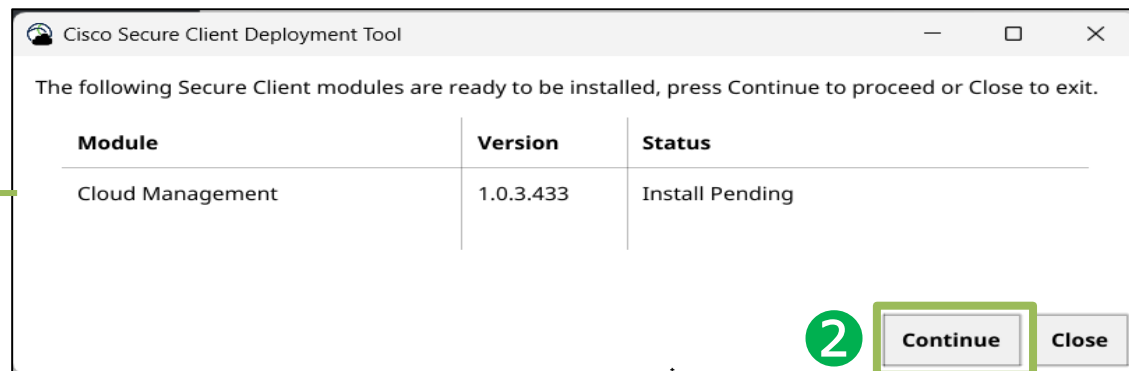
 対象のネットワークインストーラを実行
(csc-deploy-network-[契約ID]_[会社名].exeの実行)

1

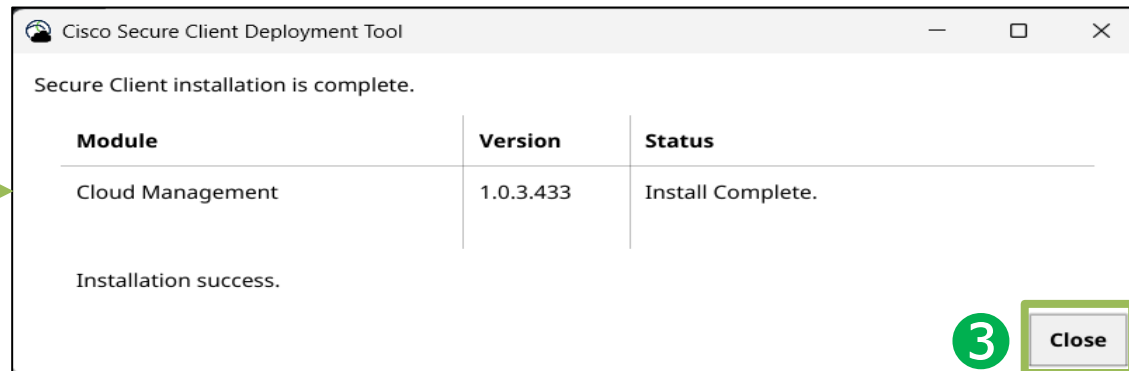
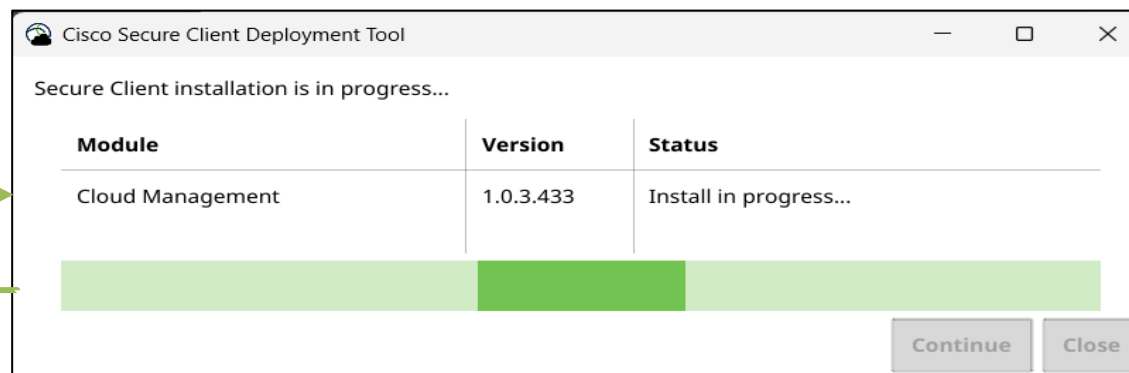
先月				
	csc-deploy-network-000000_NIPPON TEL...	2024/12/25 15:36	アプリケーション	32,800 KB
	Cisco_Umbrella_Root_CA.cer	2024/12/25 15:35	セキュリティ証明書	2 KB

※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



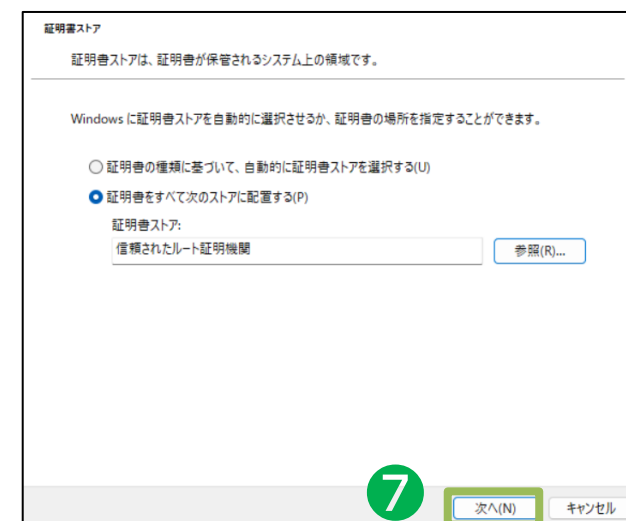
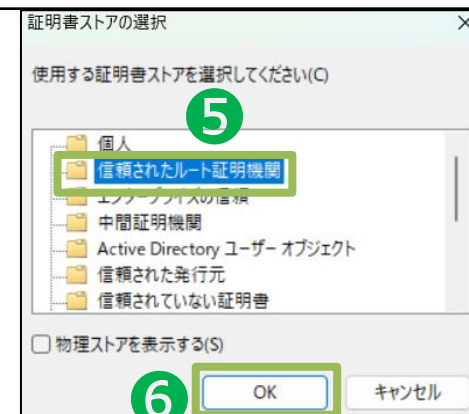
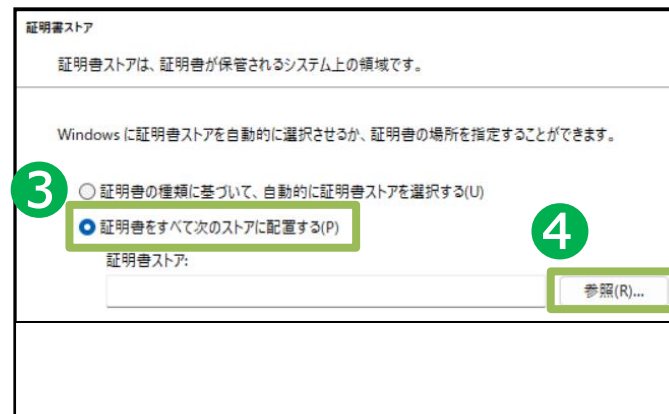
4-3. インストール手順 <ダウンロードしたインストーラの実行-3>

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

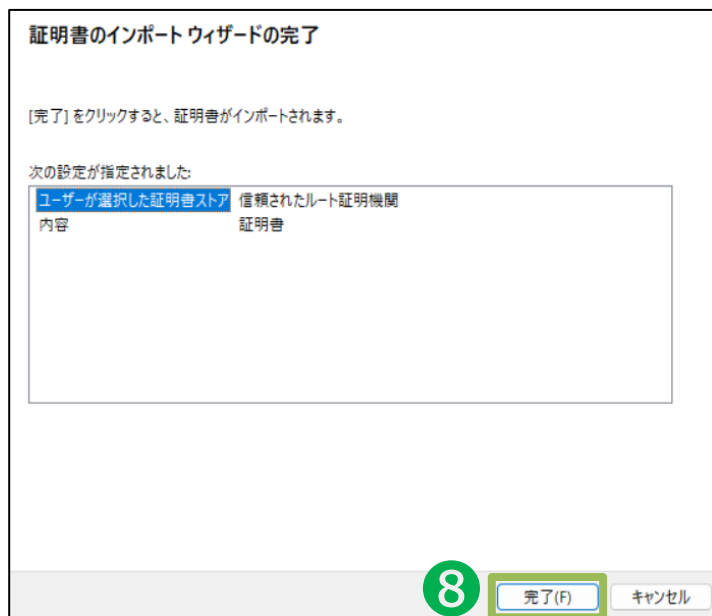
👉 「現在のユーザー」を選択した状態で次へ進む

👉 「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



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

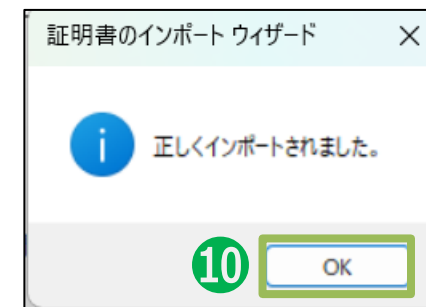
👉 「完了」を選択してインポートを開始



👉 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



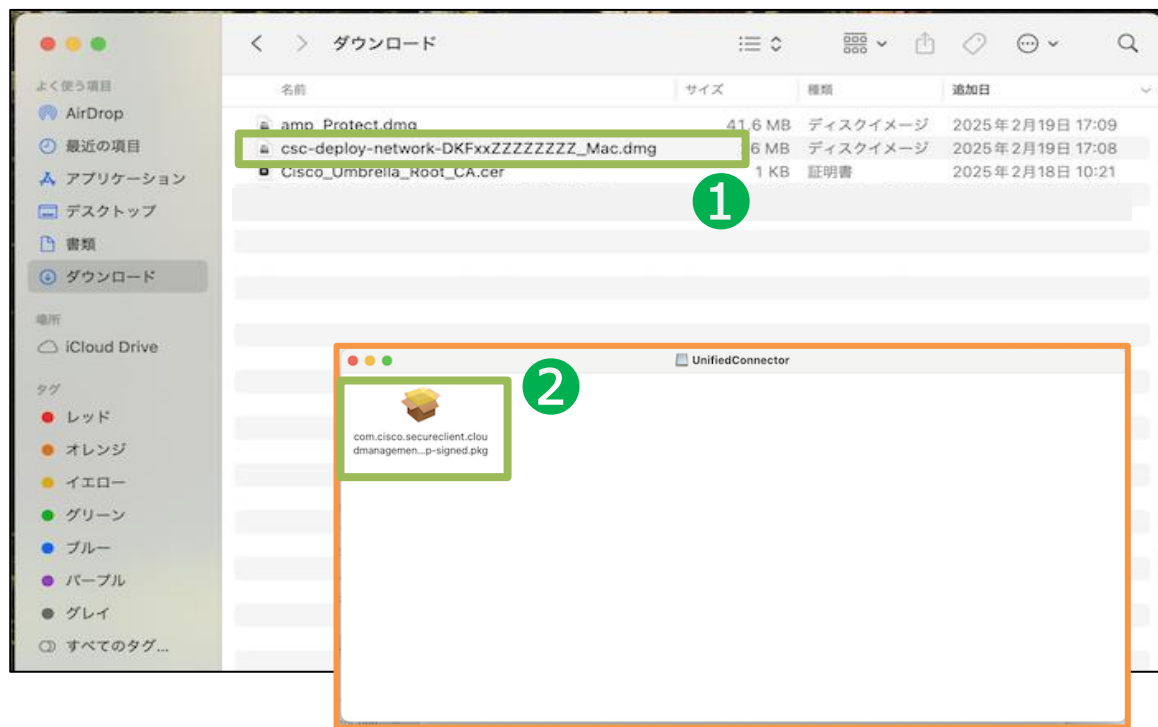
👉 インポート完了



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)



 「続ける」を選択



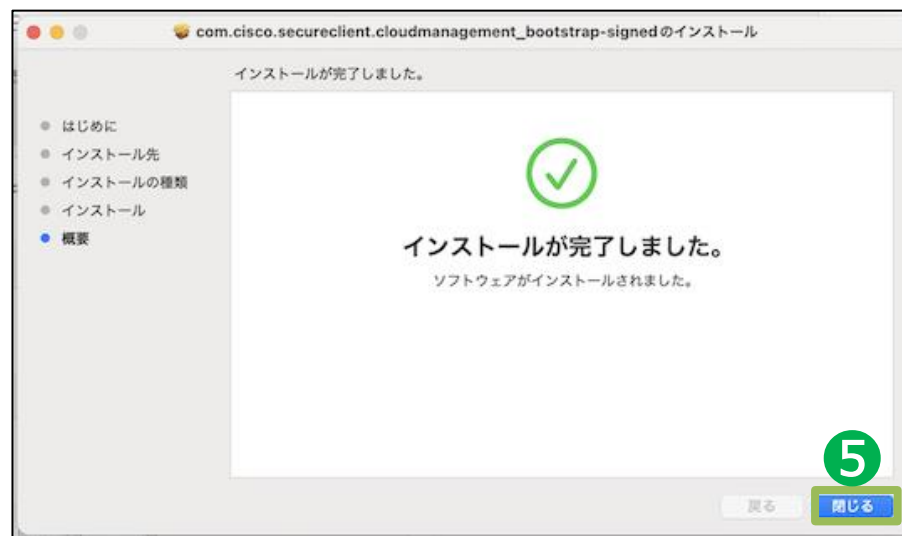
※契約IDは開通メールをご参照ください

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-2>

👉 「インストール」を選択



👉 「閉じる」を選択



👉 「ゴミ箱に入れる」を選択



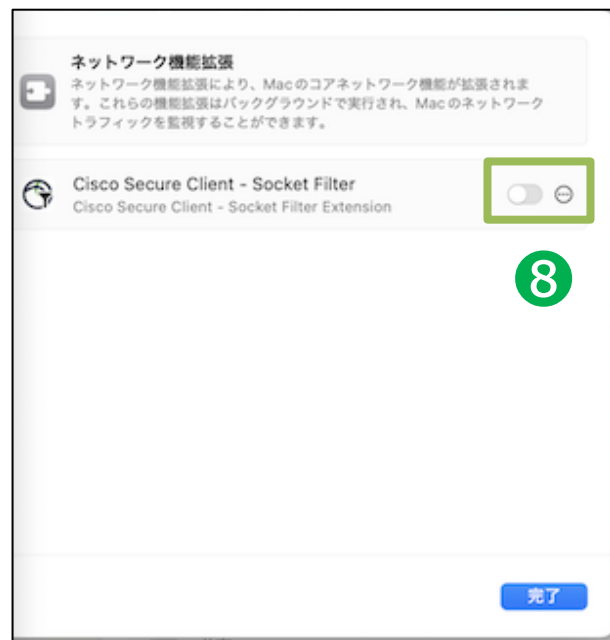
※以降の手順では、
端末によりポップアップの表示される順番が前後する可能性があります。
表示されたポップアップに従ってアプリの初期設定を実施してください。

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-3>

👉 「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

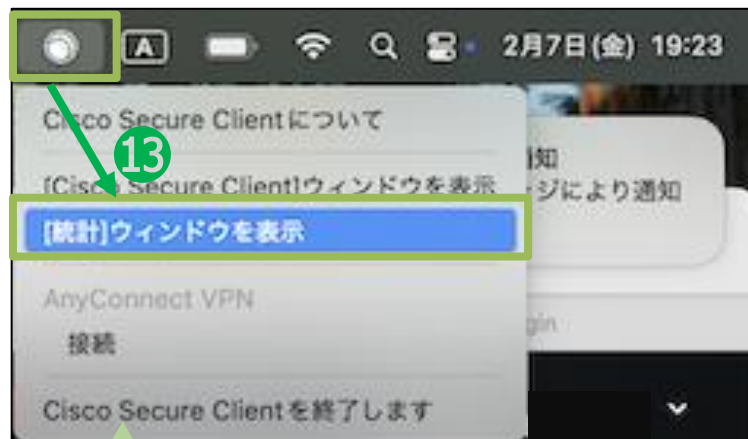


4-3. インストール手順 <ダウンロードしたインストーラの実行-4>

👉 「許可」を選択



👉 「[統計]ウィンドウを表示」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

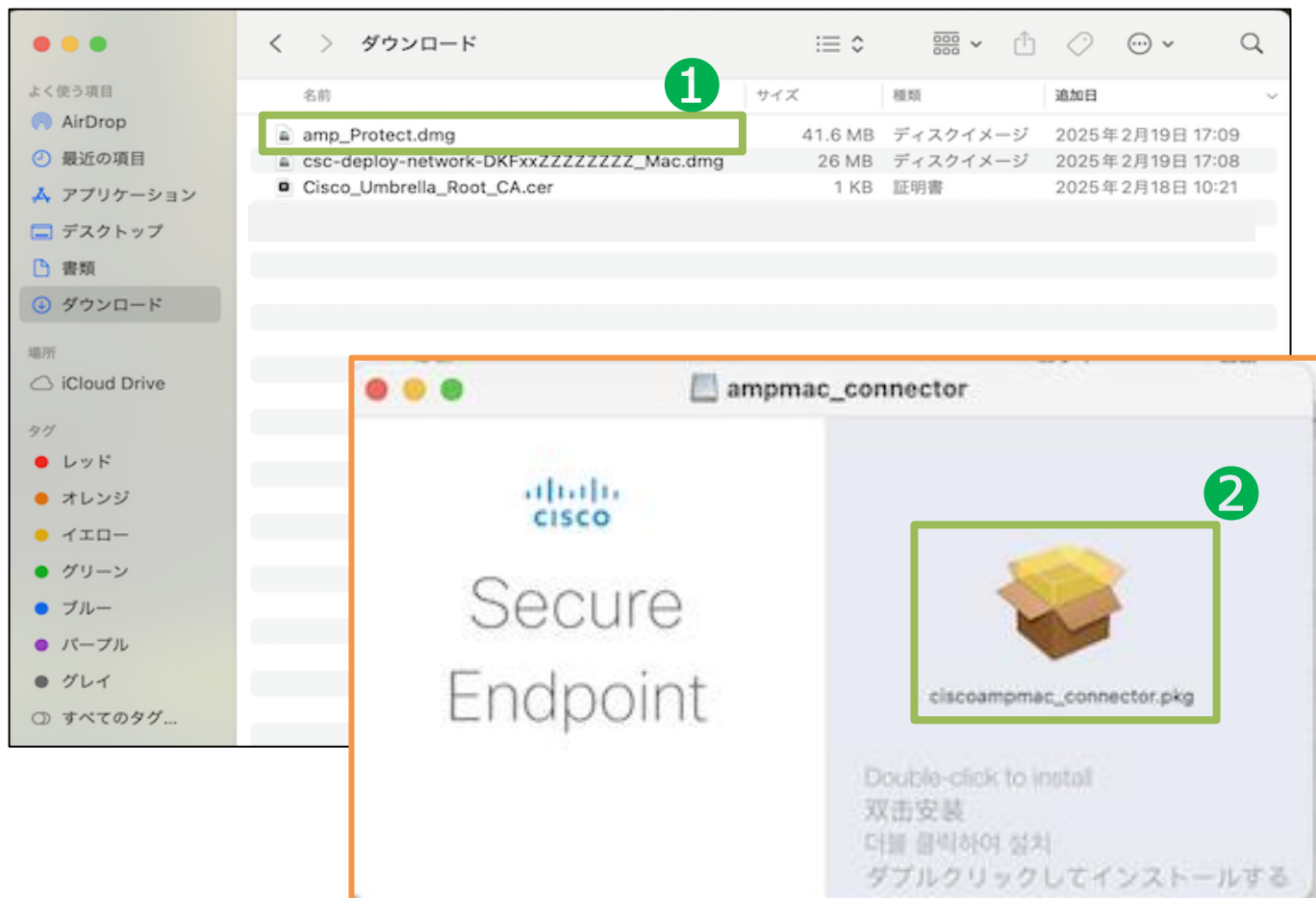
👉 Umbrellaの「IPv4DNS保護のステータス」が「保護されています」、「Web保護ステータス」が「保護されています」であることを確認



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-5>

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-6>

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



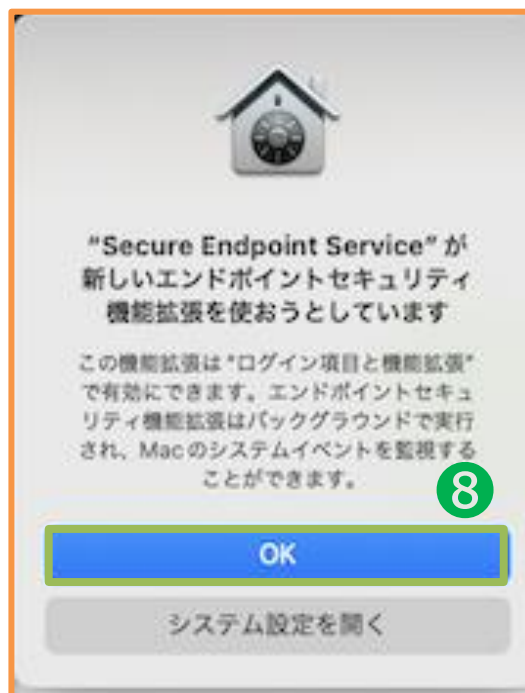
4-3. インストール手順 <ダウンロードしたインストーラの実行-7>

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

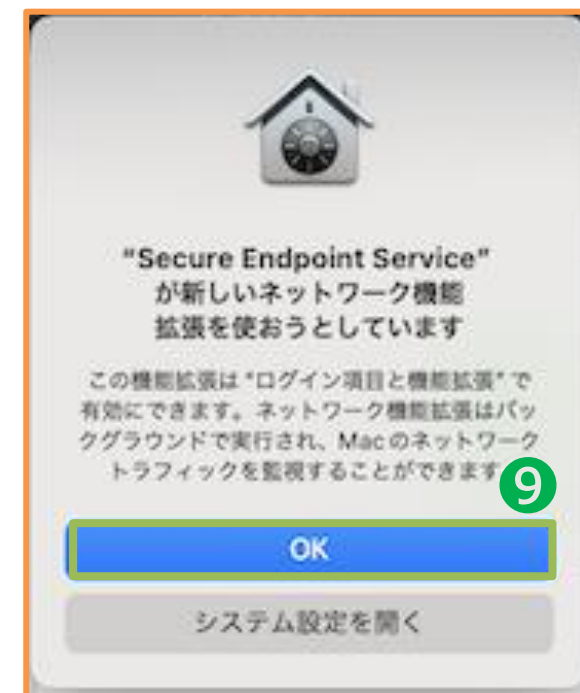
👉 「インストール」を選択



👉 「OK」を選択



👉 「OK」を選択



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



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-10>

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




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



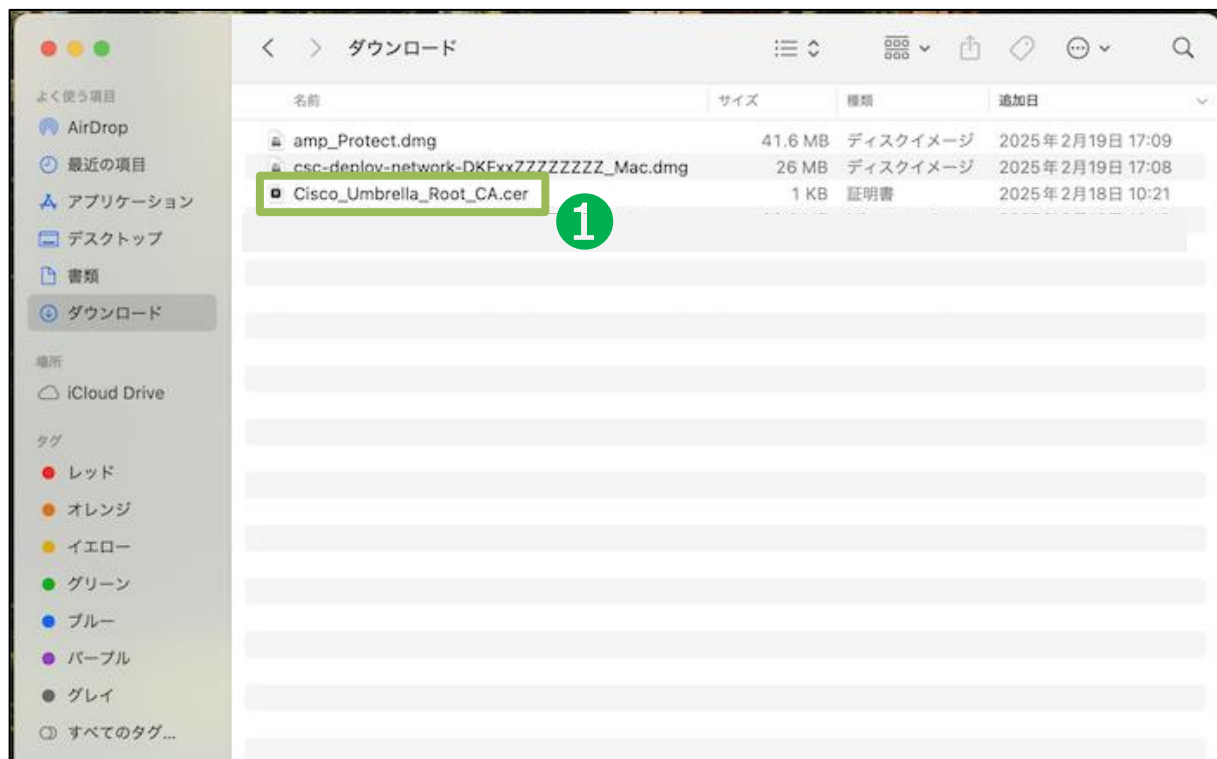
追加アクション要求「」がなくなっていることを確認



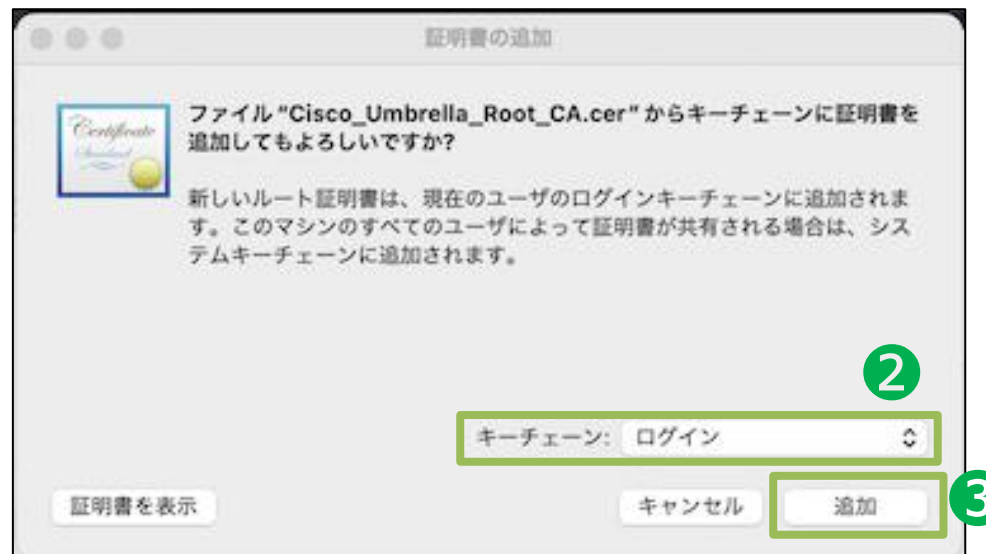
4-3. インストール手順 <ダウンロードしたインストーラの実行-12>

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-13>

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

「Cisco Umbrella Root CA」が見当たらなければ、「自分の証明書」にないか確認。

4 ログイン

5 このルート証明書は信頼されていません

名前	種類	変更日	有効期限	キーチェーン
<key>	公開鍵	--	--	ログイン
<key>	秘密鍵	--	--	ログイン
Cisco Umbrella Root CA	証明書	--	2036/06/29 0:37:53	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.Net...eProxy.ProxyToken	アプリケーションパス...	今日, 17:50	--	ログイン
com.apple.sco...okmarksagent.xpc	アプリケーションパス...	2025/01/31 11:01:26	--	ログイン
handoff-own-encryption-key	Handoff 暗号化鍵	今日, 17:47	--	ログイン
MetadataKeychain	アプリケーションパス...	2025/01/31 11:03:13	--	ログイン
TelephonyUtilities	アプリケーションパス...	今日, 17:47	--	ログイン

7

Cisco Umbrella Root CA
ルート証明書
有効期限: 2036年6月29日 日曜日 0時37分53秒 日本標準時
このルート証明書は信頼されていません

信頼

この証明書を使用するとき: システムデフォルトを使用

SSL (Secure Sockets Layer) 値が指定されていません

安全なメール (S/MIME) 値が指定されていません

拡張認証 (EAP) 値が指定されていません

IP Security (IPsec) 値が指定されていません

コード署名 値が指定されていません

タイムスタンプ 値が指定されていません

X.509基本ポリシー 値が指定されていません

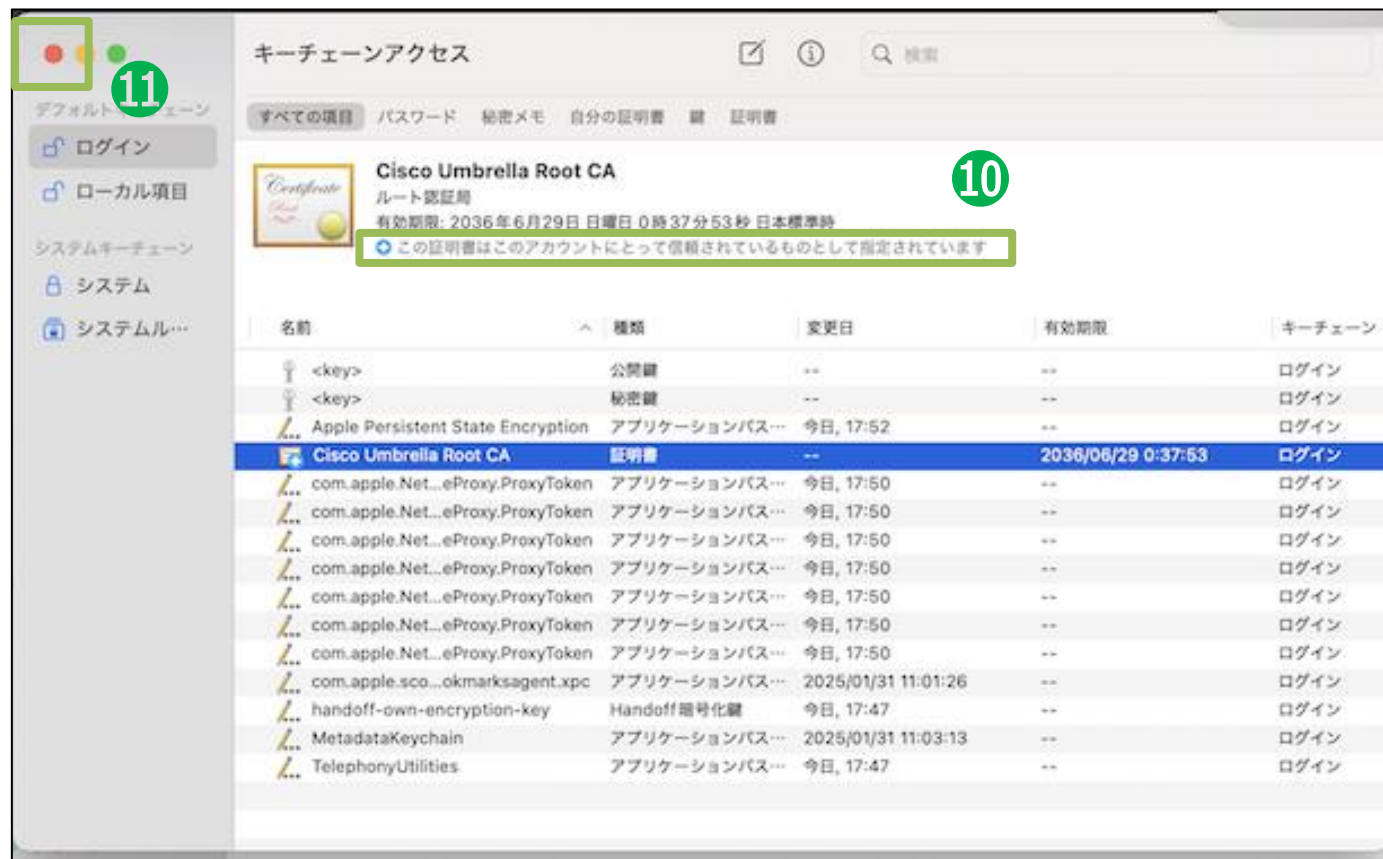
4-3. インストール手順 <ダウンロードしたインストーラの実行-14>

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

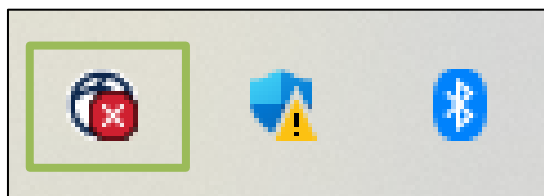


4-4. ソフトウェアの起動／ステータス確認_Windows

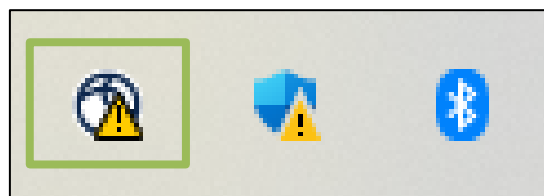
4-4. インストール手順 <ソフトウェアの起動/ステータス確認-1>

- 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

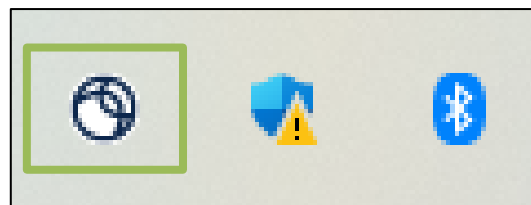
① 初期設定中



または



② 初期設定完了

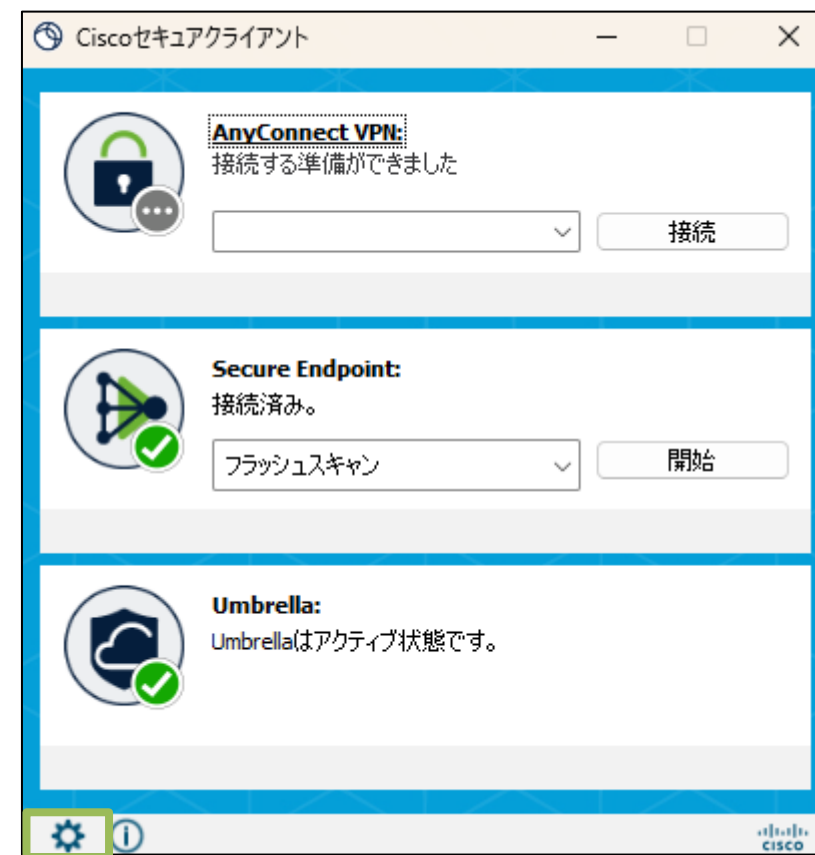


👉 初期設定完了状態でクリック



5分程度
待機

③ セキュアクライアントホーム画面



👉 ④ 各アプリの詳細は次ページ

※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。

4-4. 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

⑤ Secure Endpointステータス情報

The screenshot shows the Cisco Secure Client interface. The left sidebar has a menu with 'Secure Endpoint' selected. The main content area displays the 'Secure Endpoint' status page. A green box highlights the 'エージェント' (Agent) section, where the 'ステータス' (Status) is '接続中' (Connected).

エージェント	
ステータス:	接続中
バージョン:	8.4.3.30374
GUID:	8bf07ce3-9d65-4b73-ba59-e4eca3bed602
最終スキャン実行日時:	02/26/25 12:51:26 PM
分離:	隔離されていない
ポリシー	
名前:	Protect
シリアル番号:	28
最新アップデート:	02/26/25 12:50:33 PM
検出エンジン	
名前:	Tetra
バージョン:	94427

⑥ Umbrellaステータス情報



The screenshot shows the Cisco Secure Client interface. The left sidebar has a menu with 'Umbrella' selected. The main content area displays the 'Umbrella' status page. A green box highlights the 'DNS/IPセキュリティ情報' (DNS/IP Security Information) section, showing 'IPv4 DNS保護のステータス' (IPv4 DNS Protection Status) as '保護されています' (Protected) and 'IPv4 DNS暗号化' (IPv4 DNS Encryption) as 'オン' (On). Another green box highlights the 'セキュア Web ゲートウェイ' (Secure Web Gateway) section, showing 'ライセンス' (License) as '有効' (Valid) and 'Web保護ステータス' (Web Protection Status) as '保護されています' (Protected).

DNS/IPセキュリティ情報	
IPv4 DNS保護のステータス:	保護されています
IPv4 DNS暗号化:	オン
IPv6 DNS保護のステータス:	保護されています
IPv6 DNS暗号化:	オン
クライアント名:	ODS-Newzero1
ユーザー名:	
最終接続日時:	本日 10:12:08 ◆:0
ロギング:	無効
セキュア Web ゲートウェイ	
ライセンス:	有効
Web保護ステータス:	保護されています
HTTPリクエスト:	118
HTTPSリクエスト:	2533

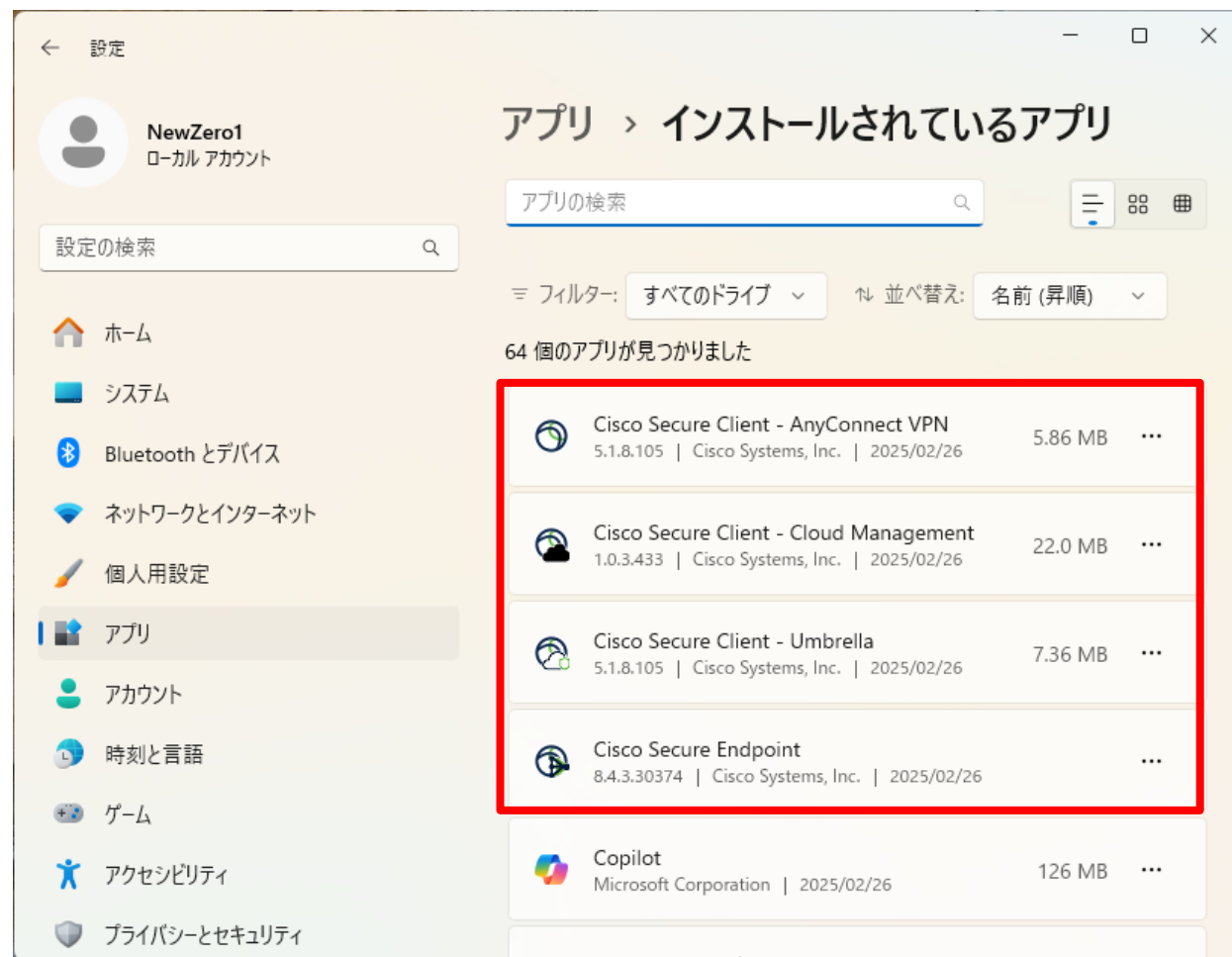
4-4. インストール手順 <ソフトウェアの起動 / ステータス確認-3>

- 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



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 Secure Client]ウィンドウを表示」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

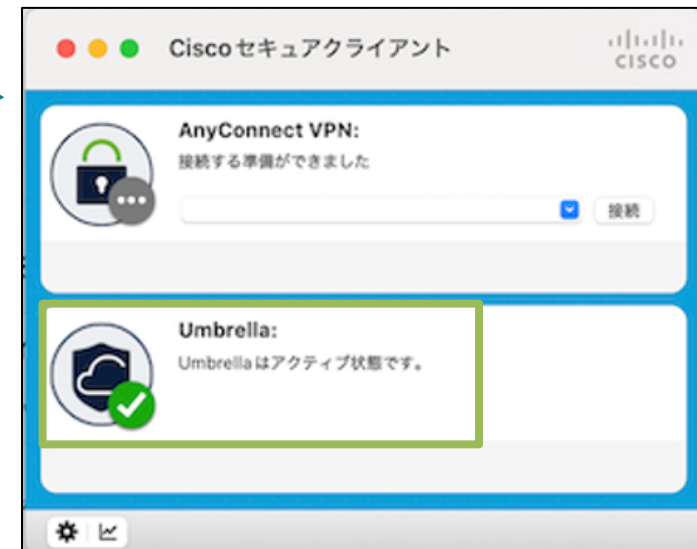


インストール設定後
自動遷移

③セキュアクライアントホーム画面を表示



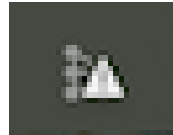
④セキュアクライアントホーム画面



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



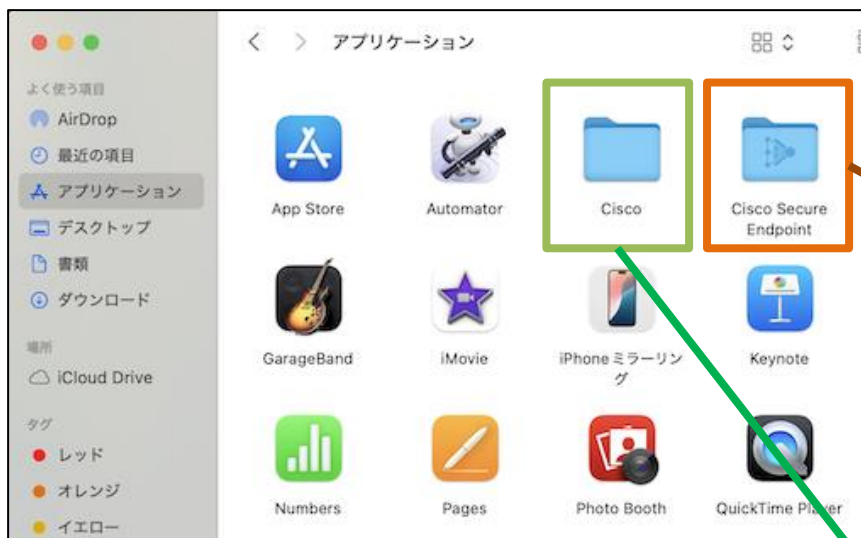
⑦セキュアエンドポイントステータス



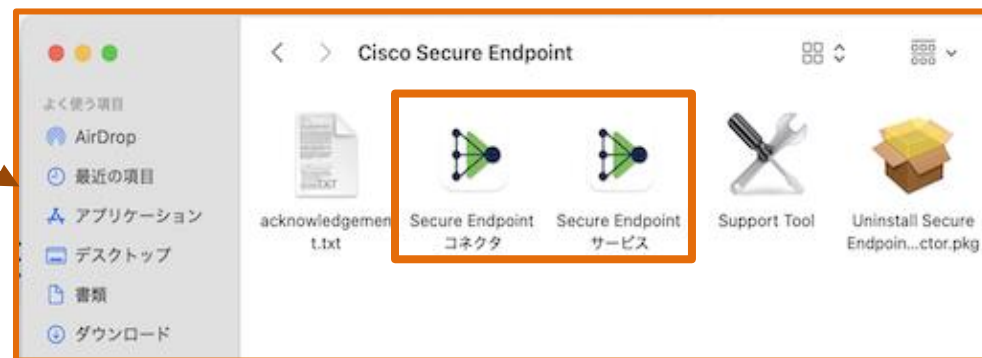
インストール設定後
自動遷移

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>

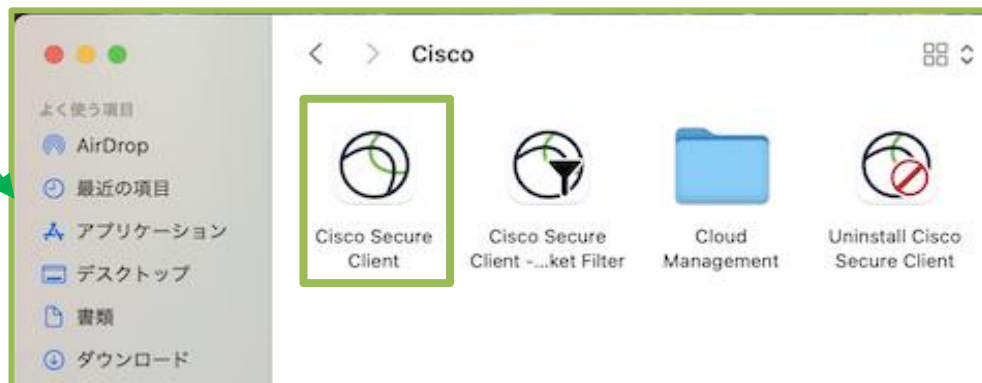
⑧ Finderから「Cisco」、「Cisco Secure Endpoint」フォルダを開き、「Secure Endpoint コネクタ」、「Secure Endpointサービス」、「Cisco Secure Client」がインストールされていることを確認



⑧ Cisco Secure Endpoint



⑧ Cisco Secure Client(Umbrella)

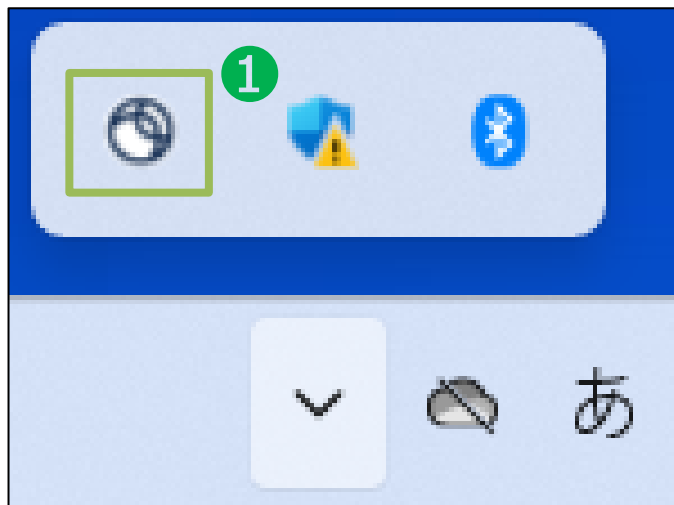


5. ソフトウェアのアンインストール手順_Windows

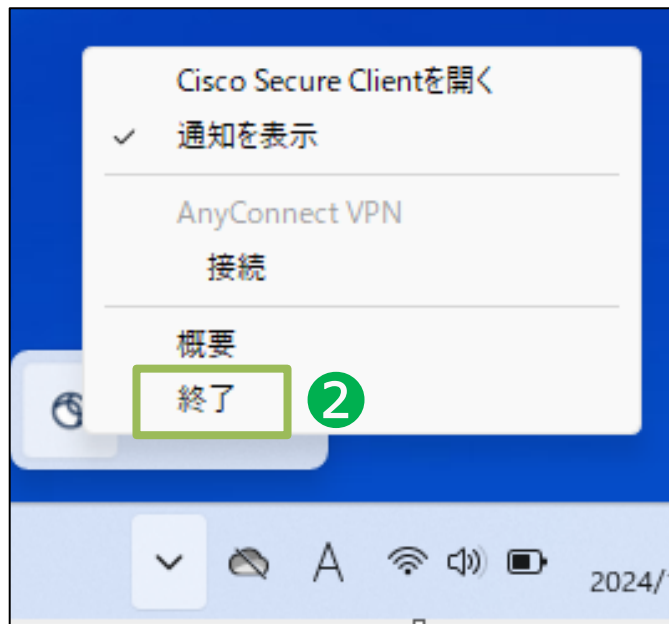
5. アンインストール手順 <Cisco Secure Clientの停止-1>

実行中のCisco Secure Clientを停止させてください。

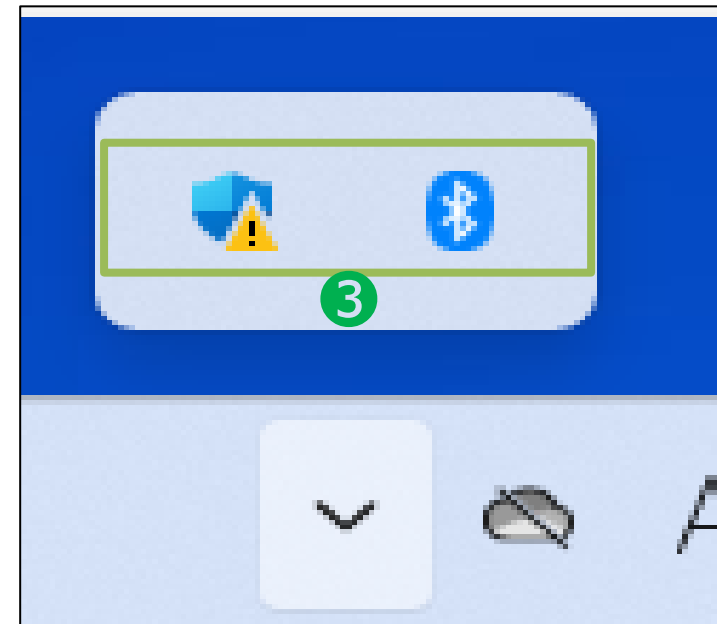
タスクバーから「Cisco Secure Client」を右クリック



「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



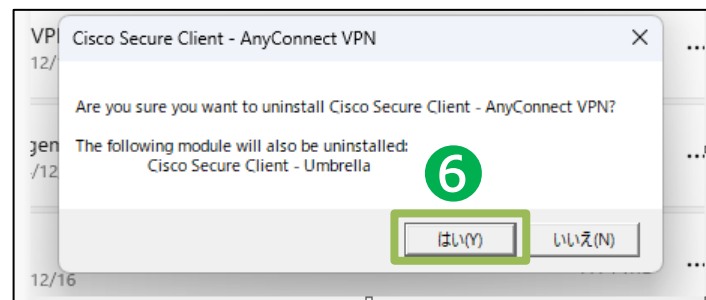
5. アンインストール手順 <ソフトウェアのアンインストール-1>

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も削除するかどうか聞かれるので「はい」を選択



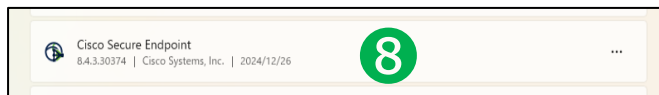
同様の手順で「Cisco Secure Client – Cloud Management」をアンインストール



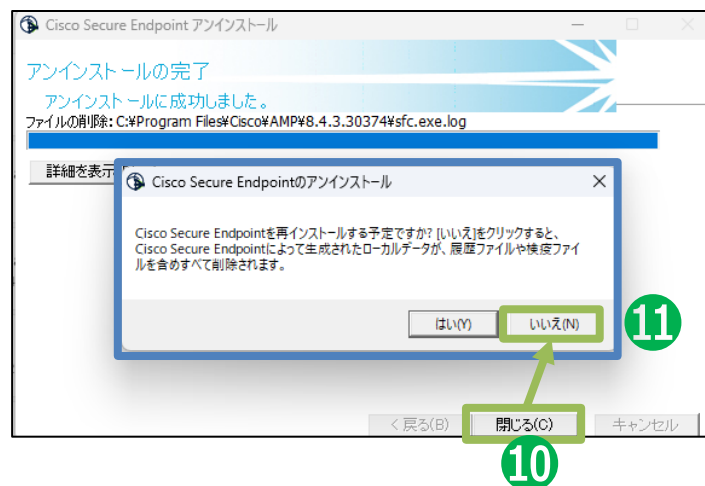
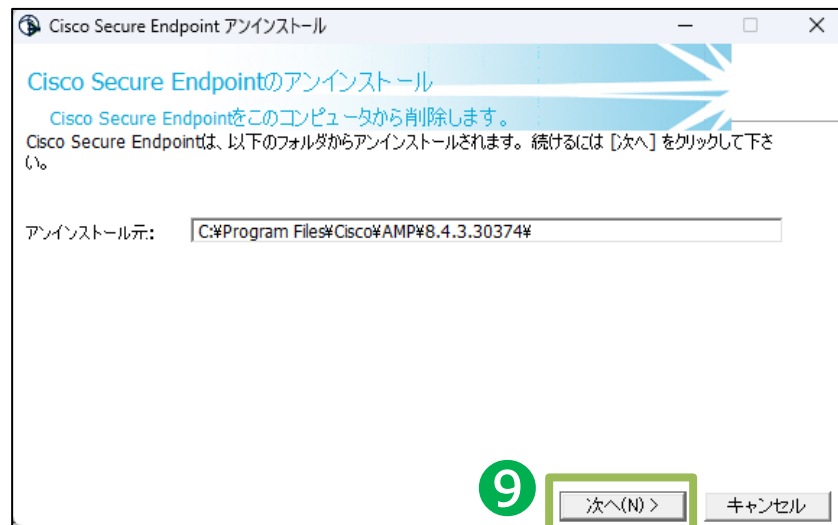
5. アンインストール手順 <ソフトウェアのアンインストール-2>

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 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



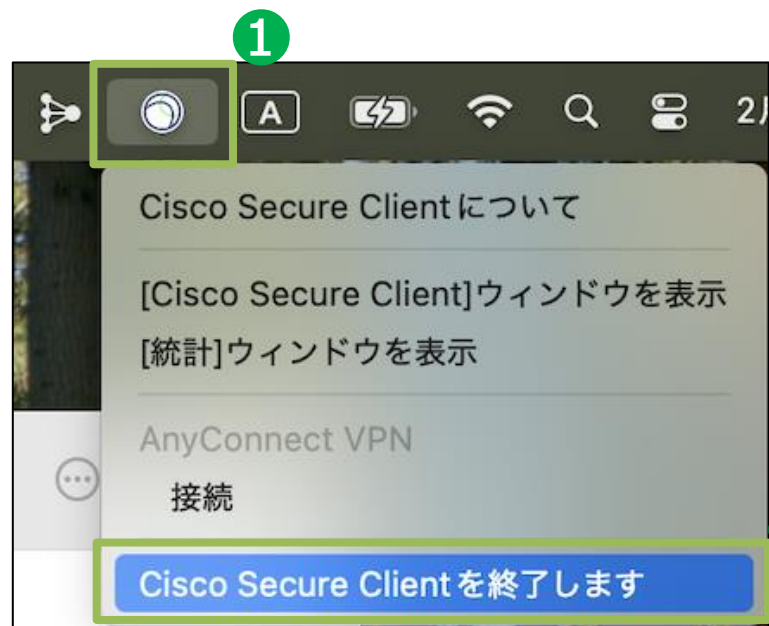
1分程度で
アンインストールが完了

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。

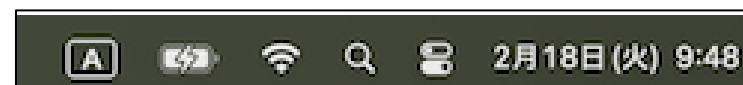
画面右上の「Cisco Secure Client」をクリックし、終了させる



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



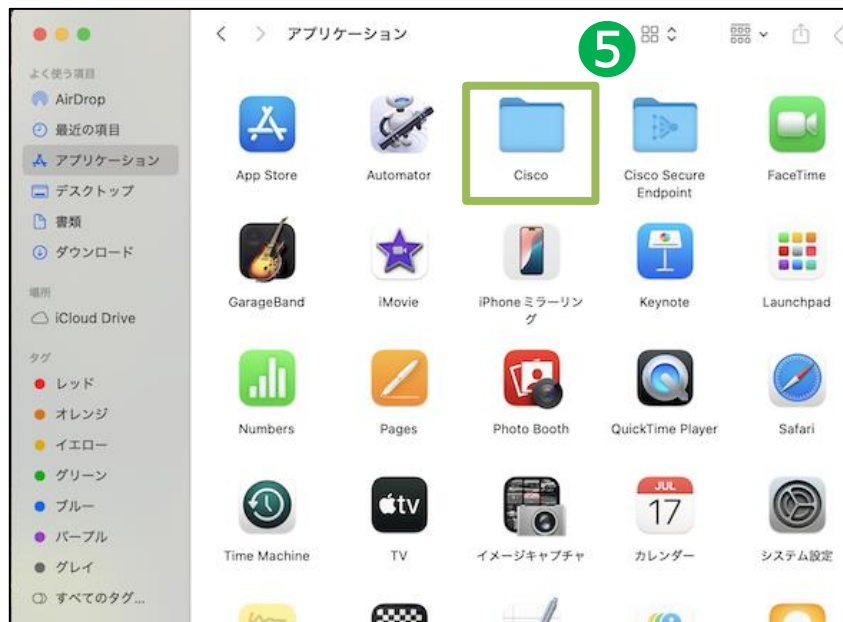
画面右上のアイコンが消えていることを確認する



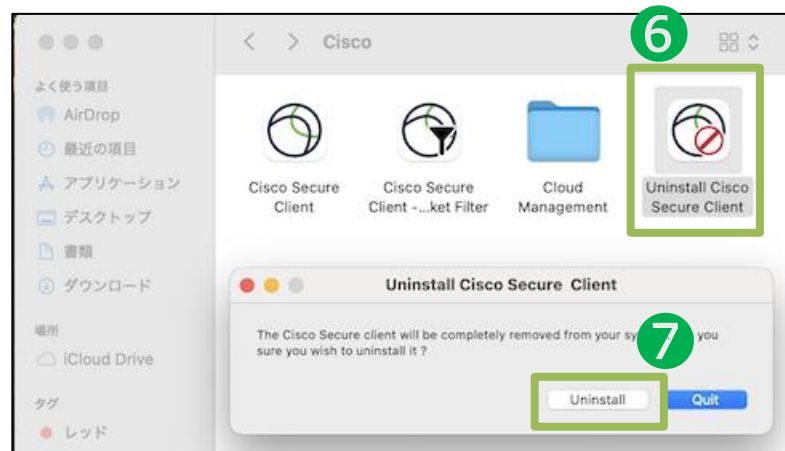
5. アンインストール手順 <ソフトウェアのアンインストール-1>

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



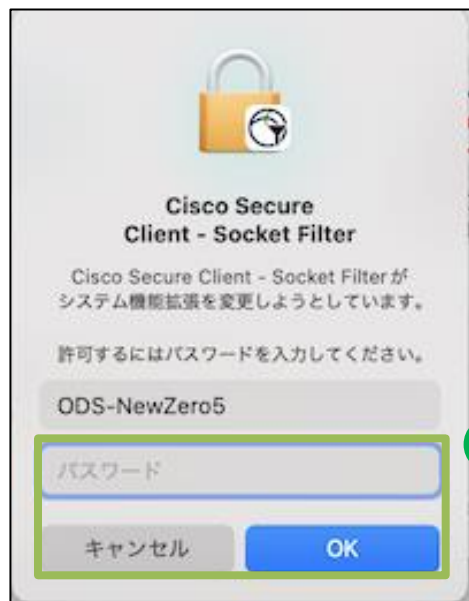
パスワードを入力し、「OK」を選択



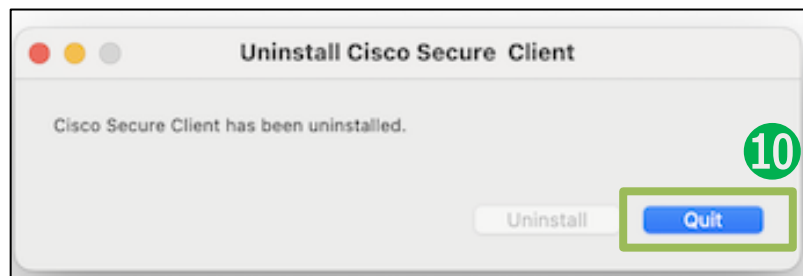
5. アンインストール手順 <ソフトウェアのアンインストール-2>

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。

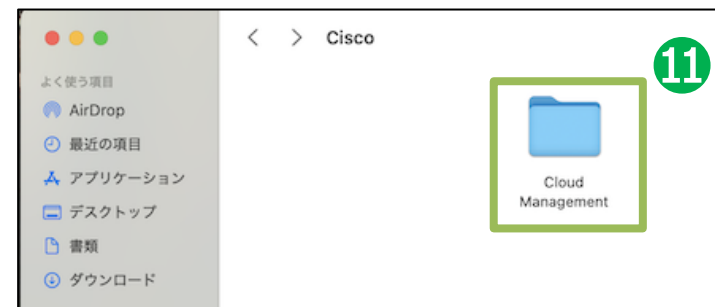
続けてパスワードを入力し
「OK」を選択



「Quit」を選択して閉じる



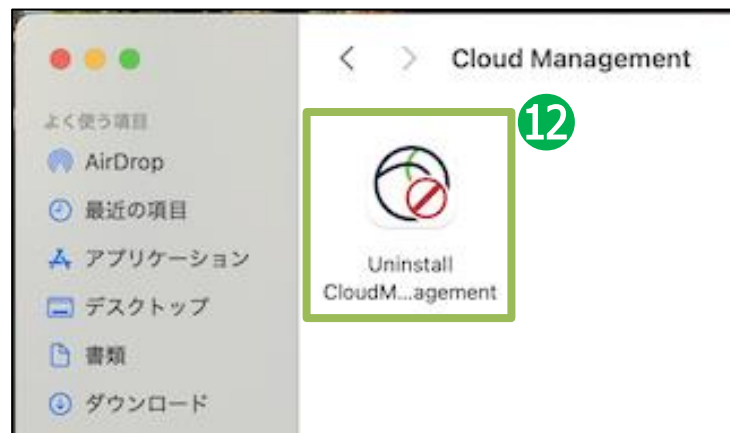
Ciscoフォルダに残った
「Cloud Management」フォルダを開く



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-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。

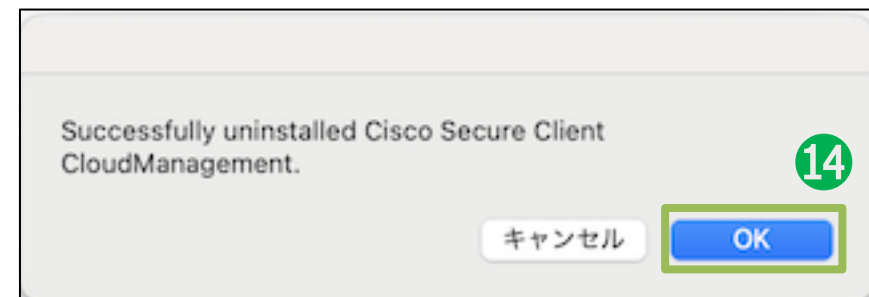
「Uninstall CloudManagement」を
ダブルクリック



パスワードを入力し、
「OK」を選択



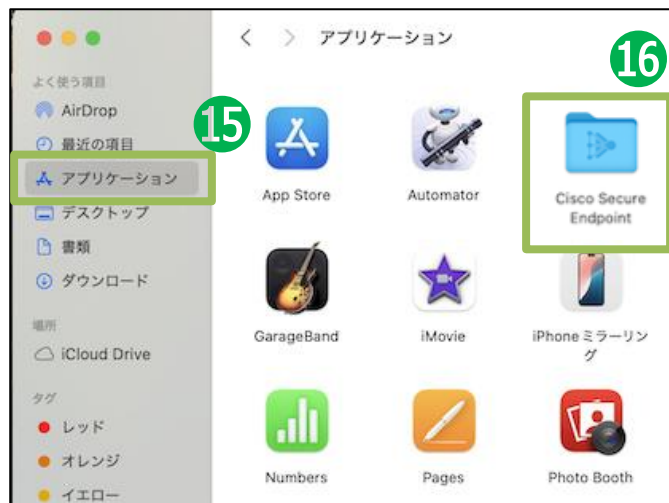
「OK」を選択



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-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。

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-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。

「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



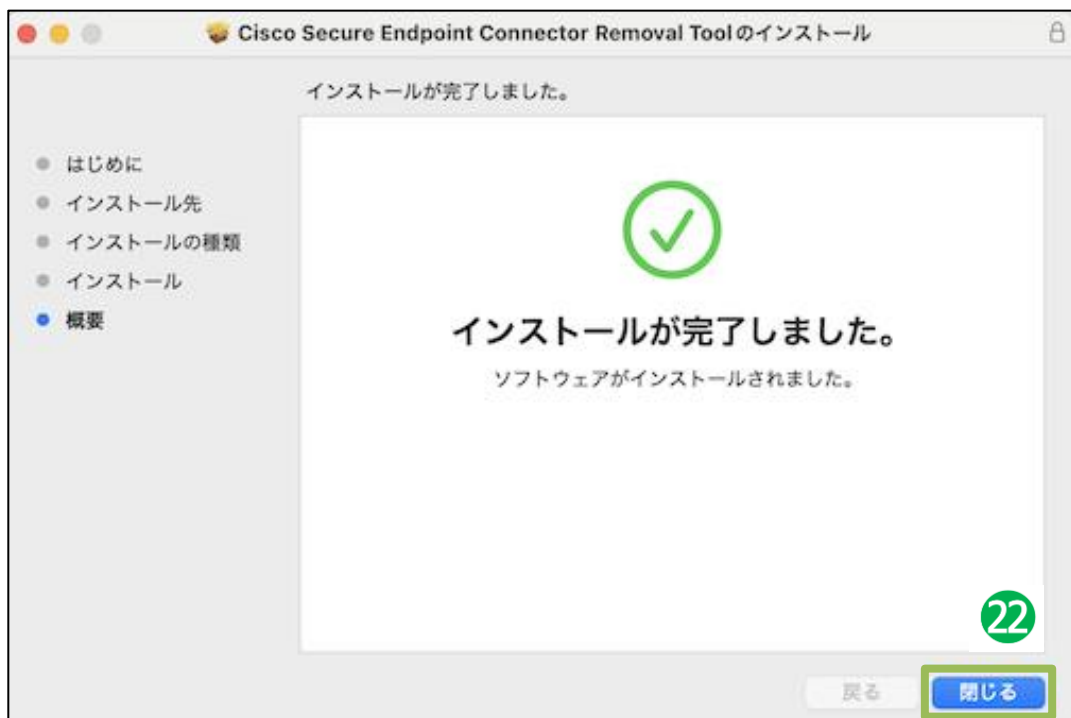
続けて、パスワードを入力し、
「OK」を選択



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-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。

「閉じる」を選択



アプリケーションフォルダに戻り、
不要な「Cisco」フォルダを削除



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

6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

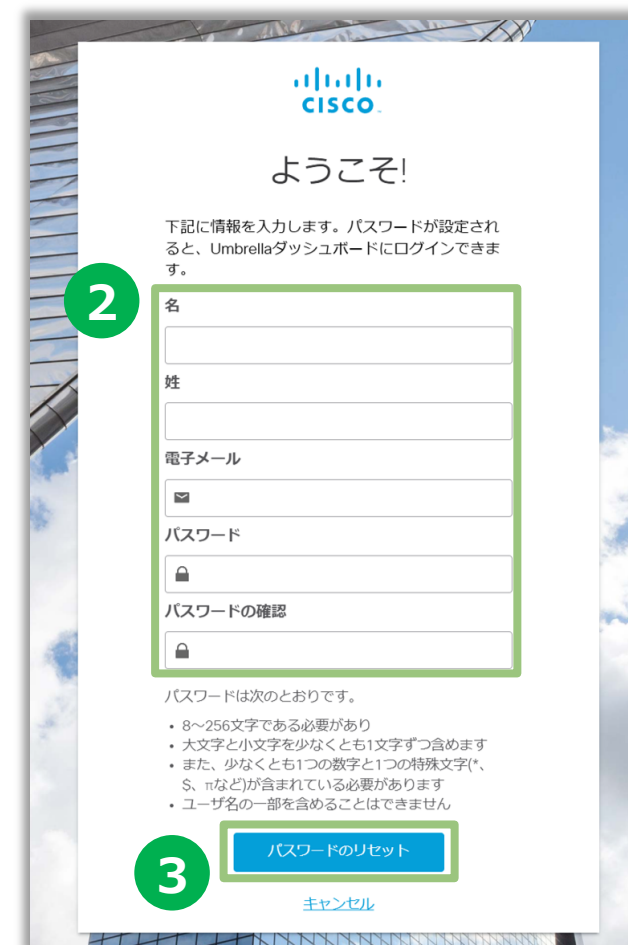
管理者向けのインビテーションメールを受信してから管理コンソール ログインまでの手順を記載します。

① 受信した電子メールから[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



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

CISCO
Cisco Umbrella

✓ 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。

④ 電子メールアドレス

パスワード

パスワードを忘れた場合 | シングルサインオン

⑤ ログイン

無料トライアルに登録



利用規約

Cisco Umbrellaの価値実証(POV)評価の登録が完了しました。

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。

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。

貴社とその関連会社に義務を負わせる権限がない場合、または一般利用規約のすべての条件に同意しない場合は、承諾せず、このクラウドサービスも使用しないでください。

⑥ [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。

⑦ 続行

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 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。

11

The screenshot displays the Cisco Umbrella dashboard in Japanese. The left sidebar contains navigation options: 概要 (Overview), 導入 (Introduction), ポリシー (Policies), レポート (Reports), Investigate, 管理 (Management), and a user profile. The main content area shows 0 Messages, followed by security alerts for Malware, Botnet, and Cryptomining. Below these are four health status cards: アクティブなネットワーク (0/1 Active), アクティブなローミングクライアント (0/0 Active), アクティブな仮想アプライアンス (0/0 Active), and アクティブなネットワークトンネル (0/0 Active). The bottom section is titled ネットワークの分析 (Network Analysis) and shows a search for total requests with a result of 0. A 'Get Started' button is visible on the right side.

6. コンソールへのログイン手順 <システムログイン>

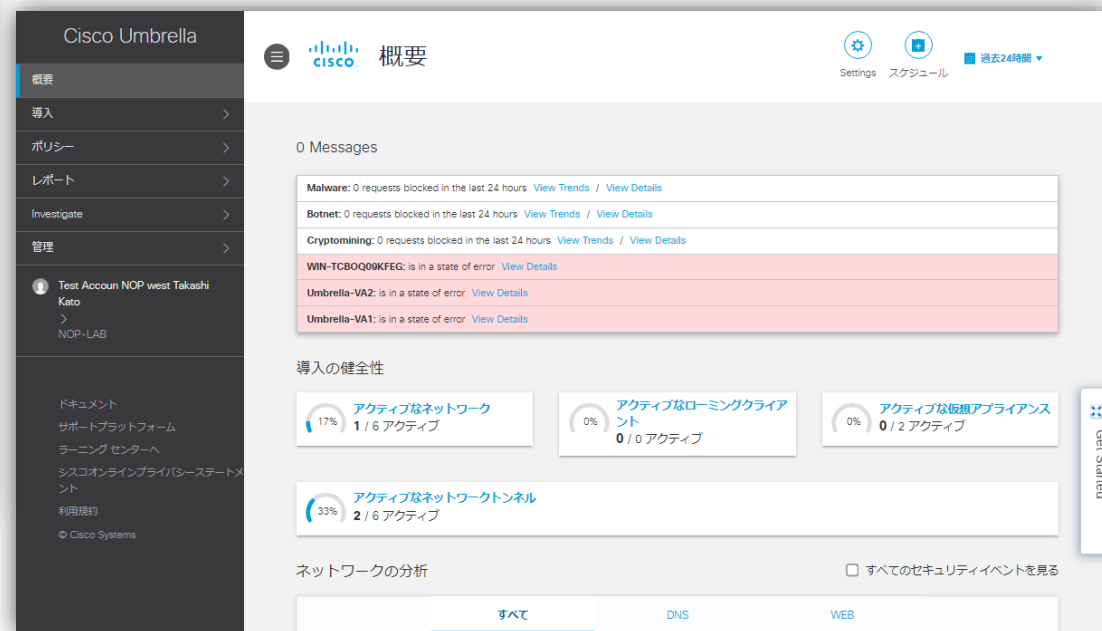
各ユーザテナントへのCisco Umbrellaへのログイン方法を示します

- 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 menu with the following items: 概要 (Summary), 導入 (Import), ポリシー (Policy), レポート (Report), Investigate, 管理 (Management), and a user profile for Test Account NOP west Takashi Kato. The main content area is titled '概要' and shows '0 Messages'. Below this is a list of security events:

- 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](#)

The '導入の健全性' (Import Health) section contains three cards:

- アクティブなネットワーク (Active Networks): 17% progress, 1 / 6 アクティブ
- アクティブなローミングクライアント (Active Roaming Clients): 0% progress, 0 / 0 アクティブ
- アクティブな仮想アプライアンス (Active Virtual Appliances): 0% progress, 0 / 2 アクティブ

Below these is another card for 'アクティブなネットワークトンネル' (Active Network Tunnels) with 33% progress and 2 / 6 アクティブ.

The 'ネットワークの分析' (Network Analysis) section at the bottom 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' options.

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. 特定のサイトが見られない
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フィールドカードの追加は、明示的なフィー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。

名前	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）

②画面右上の「追加」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
接続先リスト

追加

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、明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。

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 displays the Cisco Umbrella management console. On the left is a navigation sidebar with categories 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 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'. A sub-header explains that destination lists are used to control access to internet destinations. Below this is a search bar for '送信先リスト名'. The main form is titled '新しい接続先リスト' and includes a 'リスト名' field with the value 'テストDNSポリシー' (highlighted with a red box), a '送信先リストタイプ' dropdown set to 'Select...', and radio buttons for 'ブロック' (selected) and '許可'. A '目的地' field contains 'ドメインまたは URL'. At the bottom, it shows '0 合計' and a message '接続先が見つかりませんでした'. Navigation controls at the bottom right include '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）

- 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 interface for configuring a connection list. The left sidebar contains navigation options like '概要', '導入', 'ポリシー', '管理', 'DNSポリシー', 'ファイアウォール ポリシー', 'Web ポリシー', 'ポリシーコンポーネント', '接続先リスト', 'コンテンツカテゴリ', 'アプリケーション設定', 'テナント制御', 'スケジュール設定', 'セキュリティ設定', 'ブロックページ外観', '統合設定', '選択的番号リスト', 'レポート', and 'Investigate'. The main content area is titled '接続先リスト' and includes a search bar and a '新しい接続先リスト' form. The form fields are: 'リスト名' (testDNSポリシー), '送信先リストタイプ' (DNSポリシー, highlighted with a red box), 'このリストに含まれている接続先は:' (radio buttons for 'ブロック' and '許可'), '目的 地' (ドメインまたは URL), and a '追' button. At the bottom, there 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 interface for creating a new connection list. The left sidebar contains navigation options like '概要', '導入', 'ポリシー', '管理', 'DNSポリシー', 'ファイアウォール ポリシー', 'Web ポリシー', 'ポリシーコンポーネント', '接続先リスト', 'コンテンツカテゴリ', 'アプリケーション設定', 'テナント制御', 'スケジュール設定', 'セキュリティ設定', 'ブロックページ外観', '統合設定', '選択的復号リスト', 'レポート', 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'. A search bar for '送信先リスト名' is at the top. Below it, a form titled '新しい接続先リスト' has a 'リスト名' field with '新しい接続先リスト' entered. The '送信先リストタイプ' dropdown is set to 'DNSポリシー'. A red box highlights the 'このリストに含まれている接続先は:' section, where the 'ブロック' radio button is selected. The '目的地' field is empty. Below 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'. At the bottom, there 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）

【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 ポリシーで使用されるインターネット宛先のリストです。宛先リストのタイプに応じて、これらの宛先はドメイン、URL、または CIDR になります。宛先リストはポリシータイプ(DNS または Web)に固有であり、ポリシーに追加する前に Umbrella に追加する必要があります。

送信先リスト名

検索

新しい接続先リスト

リスト名

テストWEBポリシー

送信先リストタイプ

DNSポリシー

このリストに含まれている接続先は:

ブロック 許可

目的地

ドメインまたはURL

このリストに接続先が追加されていません

接続先が見つかりませんでした

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

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）

- ⑥ Webポリシーを作成する場合：
対象の宛先を赤枠に設定し、右側の「追」ボタンをクリックします。
設定できる値は、以下の通りです。

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

【Webポリシー用に宛先を追加する場合の画面】

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 ポリシーで使用されるインターネット宛先のリストです。宛先リストのタイプに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: ウェブポリシー

目的地: www.example.com

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

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 Policy Editor interface. The left sidebar contains navigation options: 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. 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". A description states: "宛先リストは、これらのリストされた宛先へのアイデンティティアクセスを制御するために Umbrella ポリシーで使用されるインターネット宛先のリストです。宛先リストのタイプに応じて、これらの宛先はドメイン、URL、または CIDR になります。宛先リストはポリシータイプ (DNS または Web) に固有であり、ポリシーに追加する前に Umbrella に追加する必要があります。" Below this is a form for "新しい接続先リスト" with fields for "リスト名" (新しい接続先リスト), "送信先リストタイプ" (ウェブポリシー), and "目的地" (ドメイン、URL、IPv4またはCIDRを入力). A search bar shows "ドメイン、URL、IPv4、CIDR、またはコメントで検索" and "1 合計". A table below the search bar shows one entry: "www.example.com" (URL) with a "コメントの追加" link. At the bottom right, there are "キャンセル" and "保存" buttons. The "保存" button is highlighted with a red box.

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。

Cisco Umbrella

ポリシーコンポーネント

IPS シグニチャリスト

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

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。

Search...

名前	適用先	タイプ	ドメイン	IP	URL	最終更新日
テストWEBポリシー	Webポリシー	-	2	0	0	Oct 05, 2022

注) Webポリシーの接続先リスト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。

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

テストWebブラックリスト

適用先: Webポリシー

タイプ: -

ドメイン: 2

IP: 0

URL: 0

最終更新日: Sep 01, 2022

リスト名

テストWebブラックリスト

ダウンロード

crl.geotrust.com

追加

アップロード

whitelisted_domain [詳細については、次をクリックしてください] ここをクリックしてください。

検索...

クリ

2 合計

blockweb01.test	DOMAIN	コメントの追加	×
blockweb.test	DOMAIN	コメントの追加	×

Page: 1

Results per page: 10

1-2 of 2

削除

キャンセル

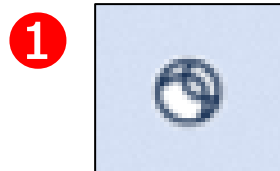
保存

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しいただき。
 ※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

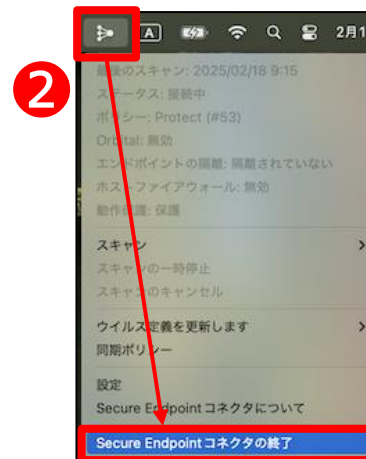
◆WindowsOSの場合

- ① タスクバーから実行中の「Cisco Secure Client」を右クリック
- ② [終了]でタスクを終了します。



◆MacOSの場合

- ① タスクバーから実行中のCisco Secure Endpointを終了します。
- ② タスクバーから実行中の「Secure Endpoint」をクリックし、終了します。



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

p72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。

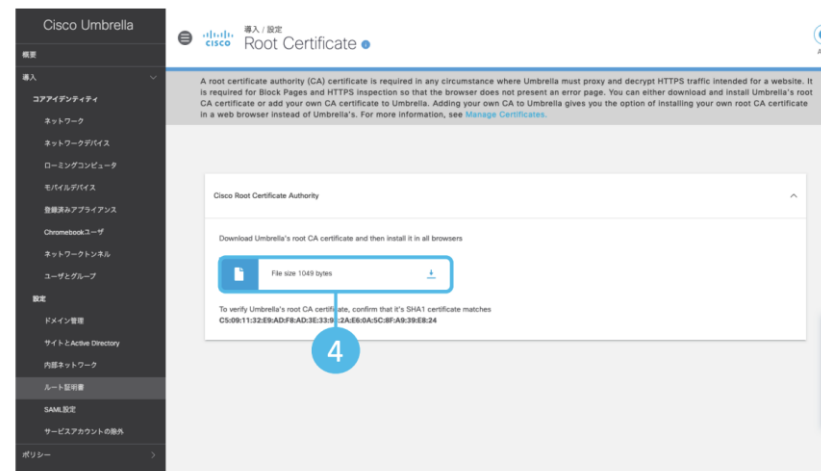
The screenshot displays the Cisco Umbrella management interface. On the left, a dark sidebar contains a menu with the following items: 概要 (Overview), 導入 (Import), コアアイデンティティ (Core Identity), ネットワーク (Network), ネットワークデバイス (Network Devices), ローミングコンピュータ (Roaming Computers), モバイルデバイス (Mobile Devices), 登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 Tunnels), 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 Exclusions), and ポリシー (Policies). A blue circle with the number '2' is positioned next to the 'ルート証明書' item, which is highlighted with a blue border. The main content area shows a '概要' (Overview) page with various status indicators and charts. A 'Get Started' button is visible on the right side of the interface.

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）

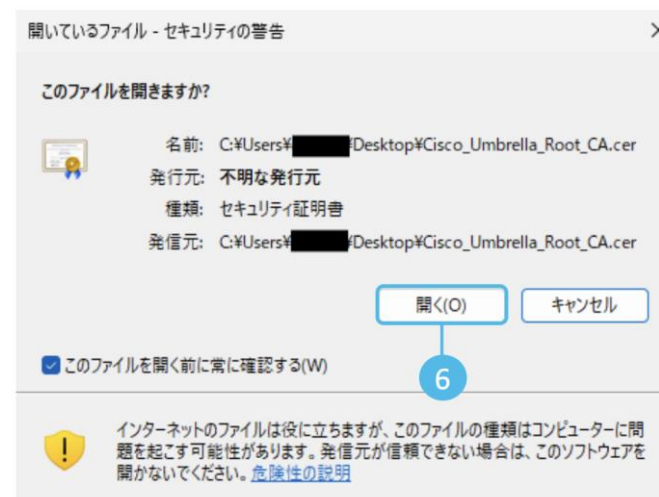
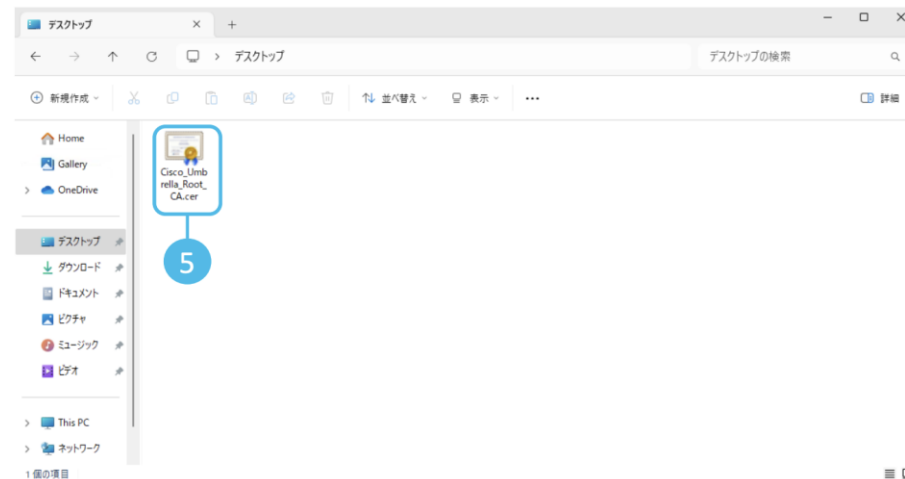
⑤④で保存した場所（フォルダ）を開き、ルート証明書をクリックします。

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。



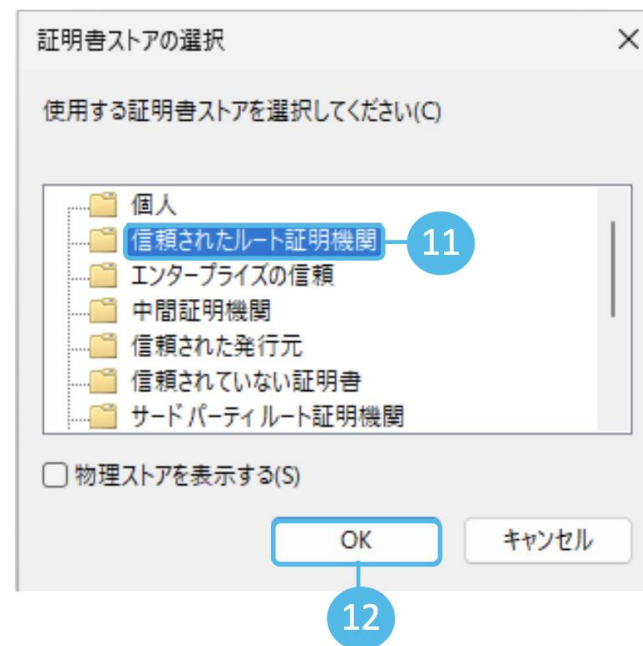
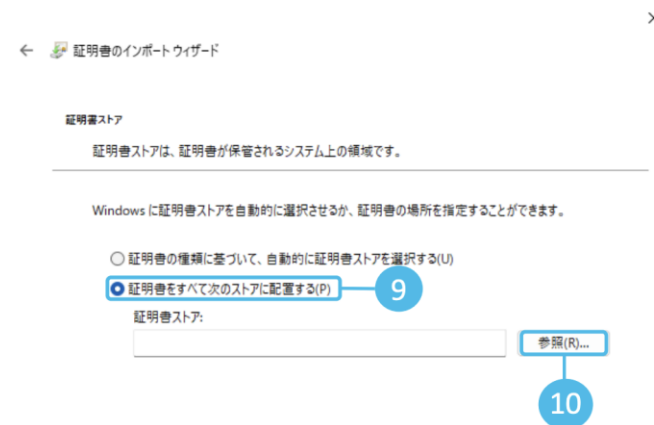
電子証明書の設定方法（つづき）

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。

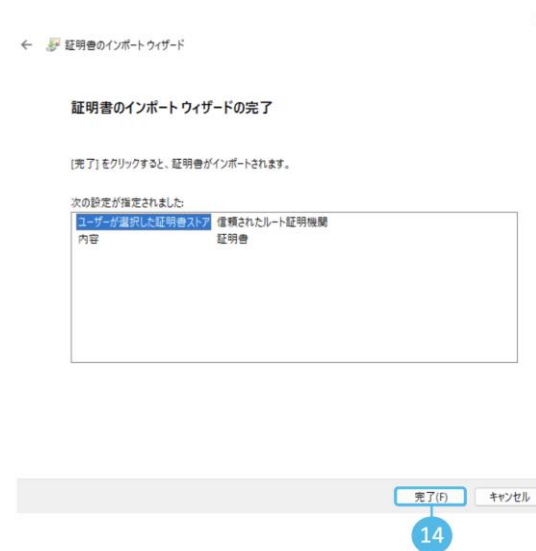


電子証明書の設定方法（つづき）

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。

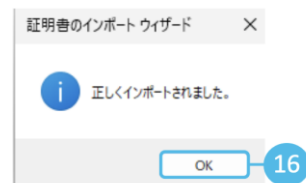


電子証明書の設定方法（つづき）

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

p72を参照ください。

まずCisco Umbrella 要因でツールが動かないかをご確認いただくため、以下の手順をお試してください。
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 を無効にする方法

p72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。

p63-71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、p72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、p74-82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。



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



502 Bad Gateway

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

This page is served by Umbrella Cloud Security Gateway.
Server: swg-nginx-proxy-https-a6f0606f2756.signginx.sin

Fri, 07 Apr 2023 00:45:22 GMT

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

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

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

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

ただし本ポリシーを変更することでセキュリティリスクが高まる場合もあるため、変更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

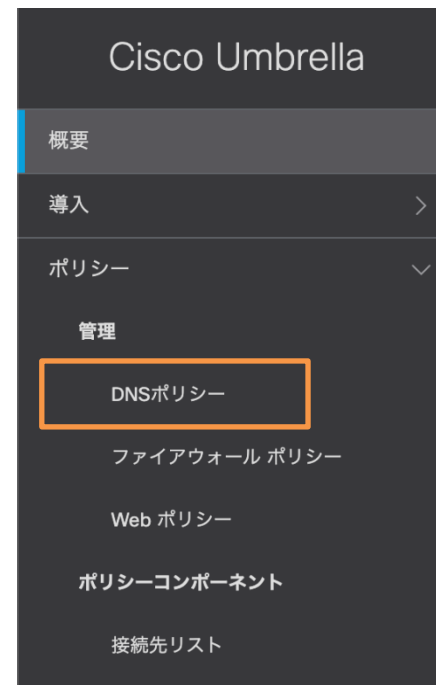
- GoogleやBingのセーフサーチを強制適用し、不適切な検索結果をフィルタリング
- DropboxやGoogle Driveなどのクラウドアプリの使用を制限

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。これらは新手的な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

アプリケーションを検索

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

キャンセル 前へ 次へ

DNSポリシーの作成・管理方法

⑨接続先リストの適用を設定します

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

以降順に、「送信先」「ファイル分析」「ブロックページ」の設定を行います

最後に「サマリー」にて設定した内容を確認し、「保存」します。

3 More 4 送信先 5 ファイル分析 6 ブロックページ 7 サマリー

接続先リストの適用 [新しいリストの追加](#)

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

🔍 宛先リスト名で検索

すべてを選択 すべてのリスト ▼ 2合計

すべての接続先リスト

<input checked="" type="checkbox"/>	🟢 Global Allow List	目的地を見る >
<input checked="" type="checkbox"/>	🔴 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

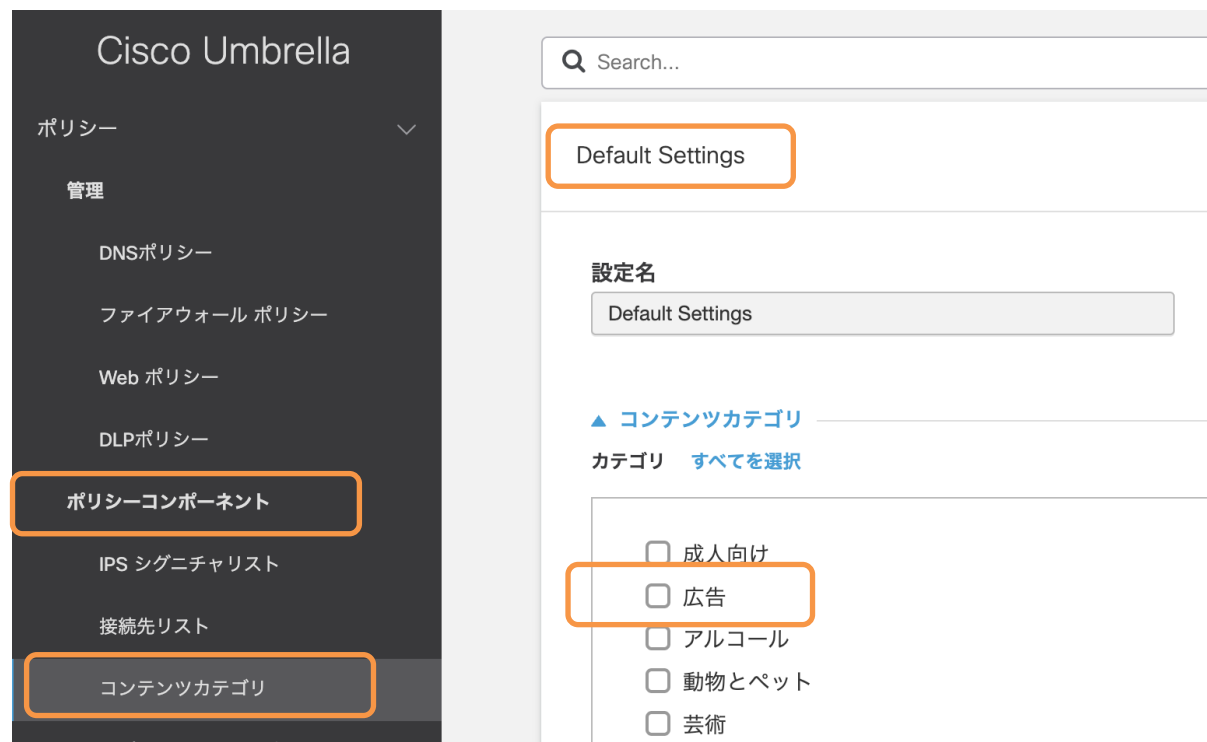
キャンセル [前へ](#) [次へ](#)

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、変更する設定名を選択し、カテゴリ中の“広告”を選択し、設定を保存します



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

p63-71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

p63-71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。

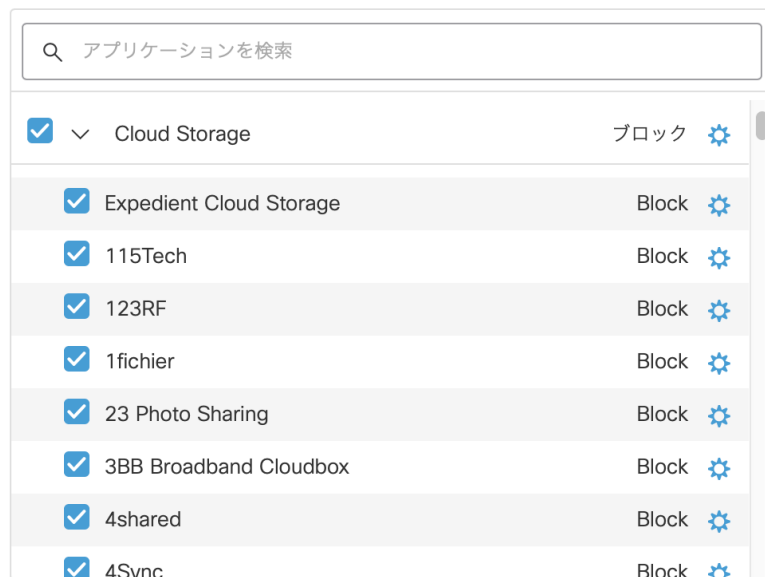
ポリシー名	適用されるポリシー	最終更新日
Cisco Test Policy	に適用されます Webポリシー	最終更新日 Feb 25, 2025
Default Settings	に適用されます DNSポリシー	最終更新日 Feb 18, 2025

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。

フラグが設定されているカテゴリ

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

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>

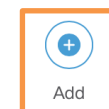
テナント制御とは、管理者によって指定されたクラウドサービスの契約テナント（環境）のみにアクセスできるよう制御する機能です。例えば、会社貸与のパソコンから会社で契約しているMicrosoft 365環境へのみ接続を許し、個人契約のMicrosoft 365に接続させないなど制御することができます。

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右枠に表示されるテナントコントロール画面にて右上のAdd（追加）ボタンをクリックします。



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	G Suite	Slack	Dropbox	変更日
0 テナント	0 ドメイン	0 ワークスペース	0 Teams	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 [×](#)

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 interface. On the left is a dark sidebar menu with 'Cisco Umbrella' at the top and various navigation items like '概要' (Overview), '導入' (Onboarding), and '設定' (Settings). The main content area is titled '概要' (Overview) and includes a '0 Messages' section with alerts for Malware, Botnet, and Cryptomining. Below this is a 'LOG MANAGEMENT' section with a warning message. The '導入の健全性' (Onboarding Health) section shows three progress indicators for 'アクティブなネットワーク' (Active Networks), 'アクティブなローミングクライアント' (Active Roaming Clients), and 'アクティブなDNS' (Active DNS), all at 0%. The 'ネットワークの分析' (Network Analysis) section is partially visible. 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 and contains a 'すべて表示' (Show All) button. To the right, there are sections for 'フラグが設定されているカテゴリ' (Categorized by Flagged) and 'フラグが設定された検索結果' (Flagged Search Results).

Cisco Umbrella

概要

0 Messages

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

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

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

▲ 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](#).

LOG MANAGEMENT

導入の健全性

0% アクティブなネットワーク
0 / 0 アクティブ

0% アクティブなローミングクライアント
0 / 0 アクティブ

0% アクティブなDNS
0 / 0 アクティブ

ネットワークの分析

アプリケーションの検出と制御(過去90日間)

114
検出されたクラウドアプリケーション

1
リスクのあるクラウドアプリケーション

すべて表示

フラグが設定されているカテゴリ

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)

メディア (0 確認 2 合計アプリケーション数)

ダッシュボードの表示

フラグが設定された検索結果

検索結果
検索の時間軸

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。

The screenshot displays the Cisco Umbrella App Discovery interface. The top navigation bar includes the Cisco logo, the text 'Reporting / Core Reports', and 'App Discovery'. A 'Download CSV' button is visible in the top right corner. The main content area features a search bar and a table of applications. The table has columns for Application, Risk Score, Identities, DNS Requests, Total Web Traffic, and Label. The 'Protected Media Security' application is highlighted with a red box, showing a 'High' risk score. Other applications listed include 'OneTrust Security', 'Digital Adoption Platform Business Intelligence', 'Intercom Customer Relationship Manage...', and 'Qualtrics Website and App Feed... Business Intelligence'.

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

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**

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** **Medium**

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** **Not Found**

Factors:

 1. Security controls p
 2. Certifications earn[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

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)

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。

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。

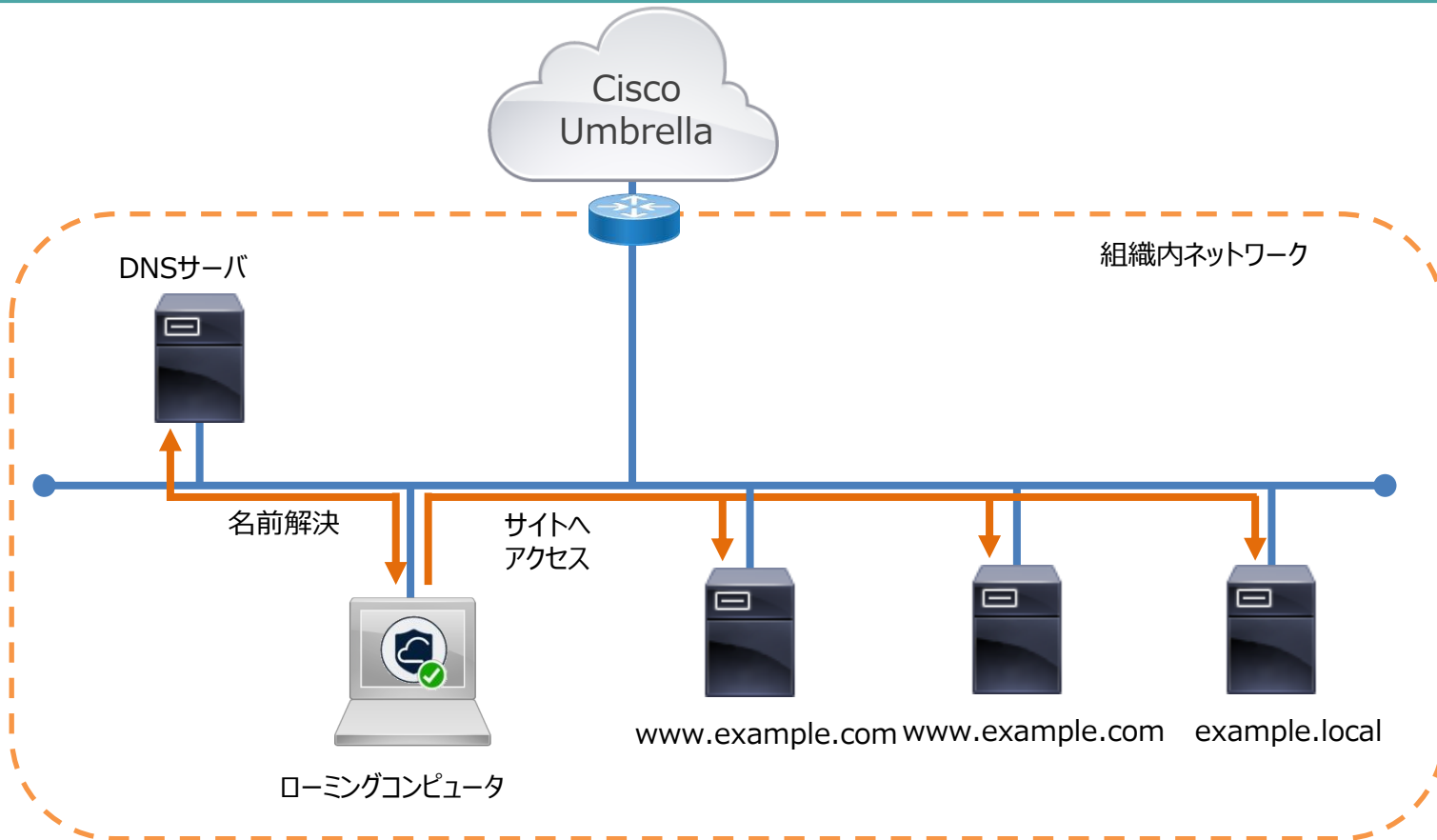
ドメインタイプ
 内部ドメイン 外部ドメインおよびIP

ドメイン

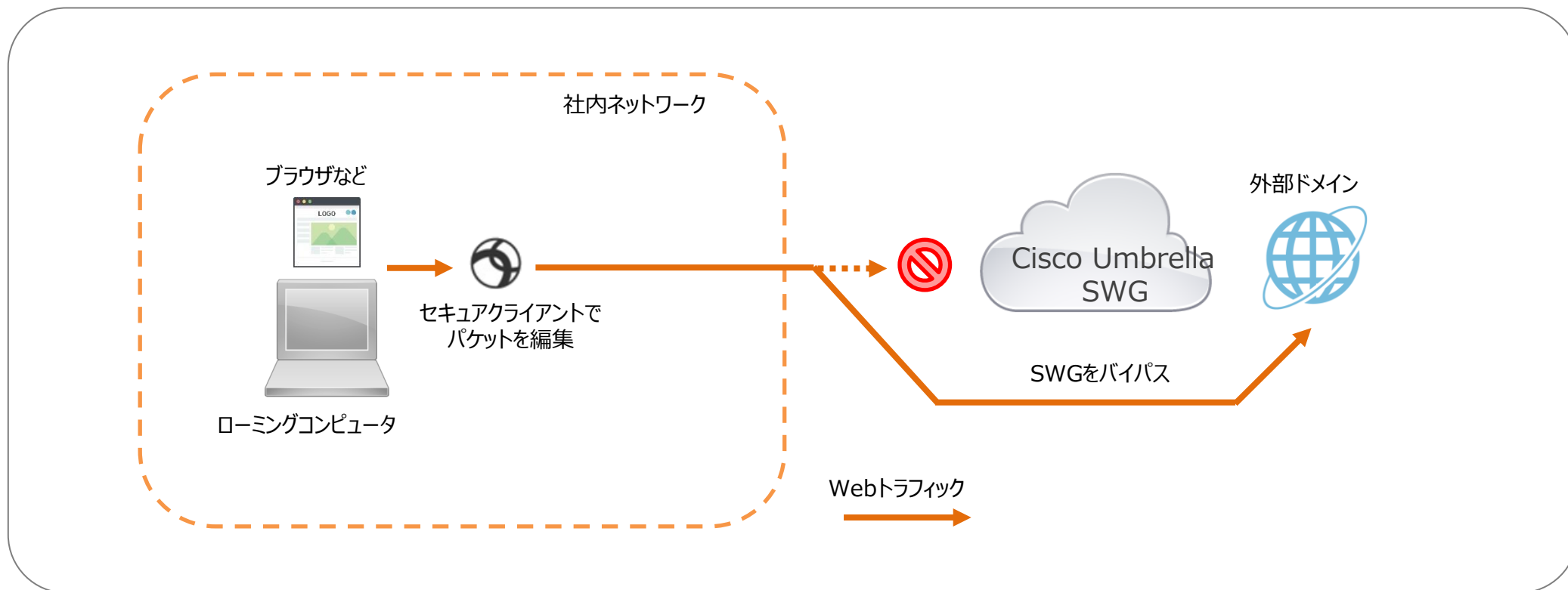
説明

適用先
 ▼

ドメインの追加画面



Umbrellaでは、クラウド側に SWG (Secure Web Gateway) という HTTP/HTTPS のフルプロキシサーバを提供しています。しかし、プロキシを介した場合、Web通信が正常に行われたいサイトや、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/*

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。

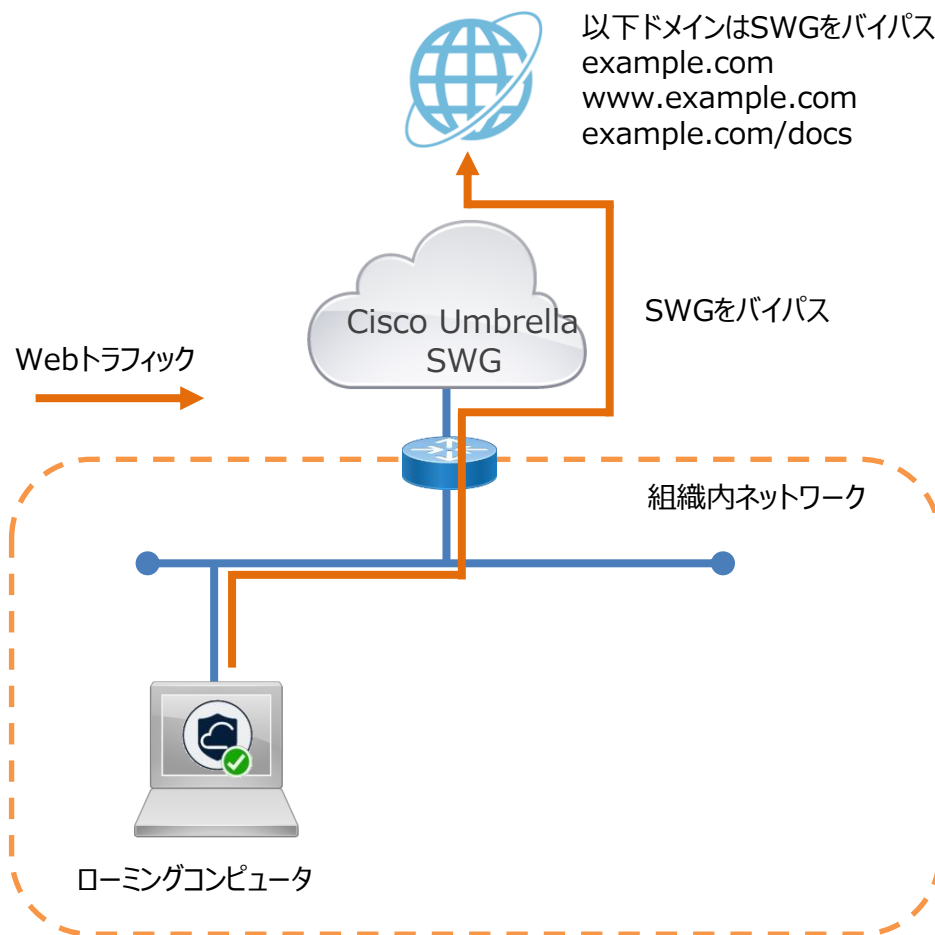
1 **ドメインタイプ**
 内部ドメイン 外部ドメインおよびIP

2 **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

ドメインの追加画面

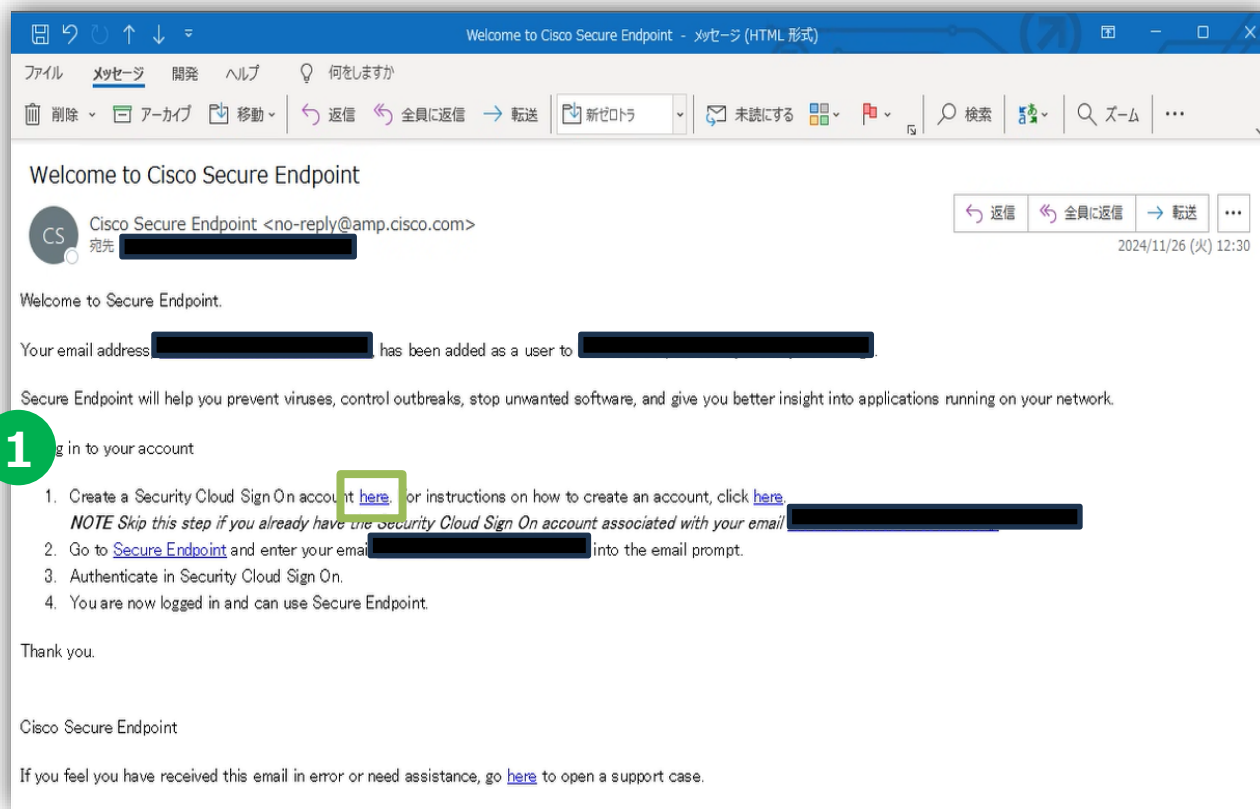


8. セキュアエンドポイント コンソールへのログイン手順 < Cisco Secure Endpoint Essentials >

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 受信した電子メールから枠内の [here] をクリック
- ② [Email^{※1}]、[First name]、[Last name]、[Country]、[Password^{※2}] を入力し、規約の同意にチェック
※1 Email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



The screenshot shows the "Account Sign Up" form. A green circle with the number "2" is placed over the "Provide following information to create enterprise account." text. The form includes the following fields and options:

- Email *
- First name *
- Last name *
- Country * (Dropdown menu showing "Japan")
- Password * (with "Show" link)
- Confirm Password * (with "Show" link)
- I agree to the [General Terms and Privacy statement](#).

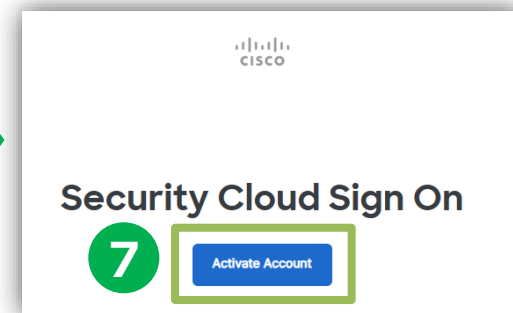
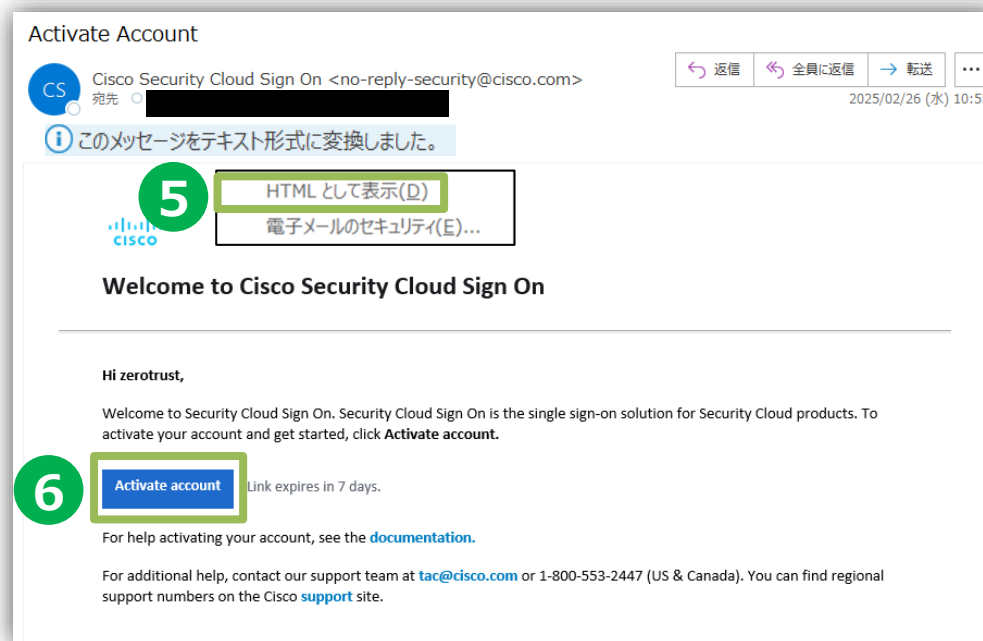
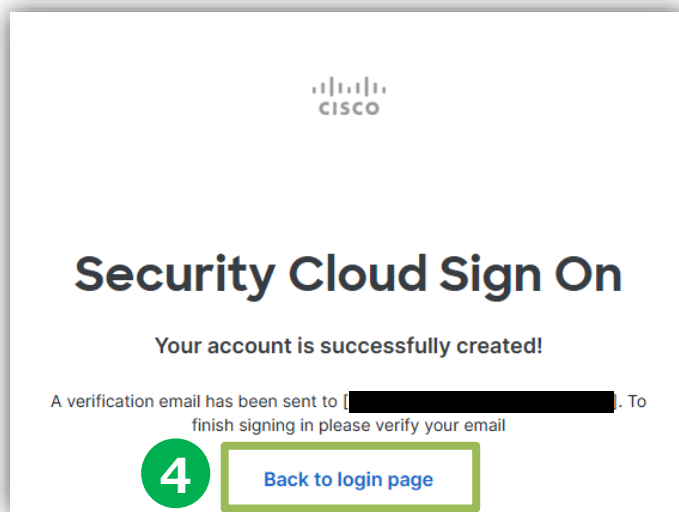
At the bottom, there is a "Sign up" button (highlighted with a green box) and a "Cancel" button. A green circle with the number "3" is placed over the "Sign up" button.

Password Requirements

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

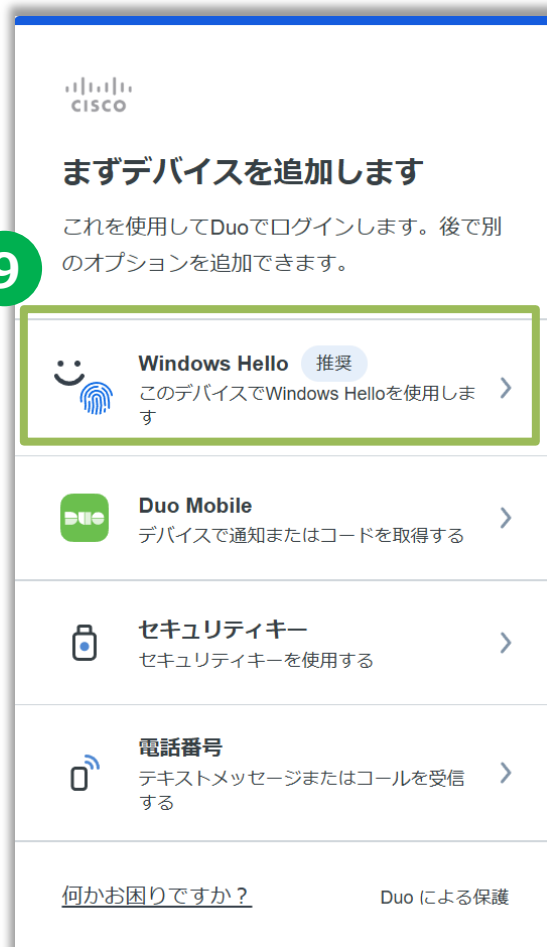
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

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



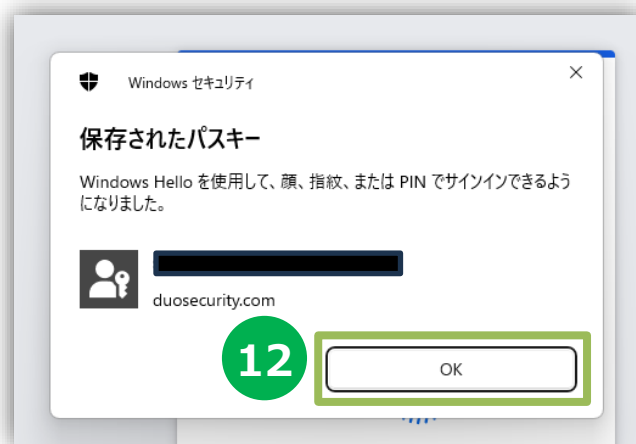
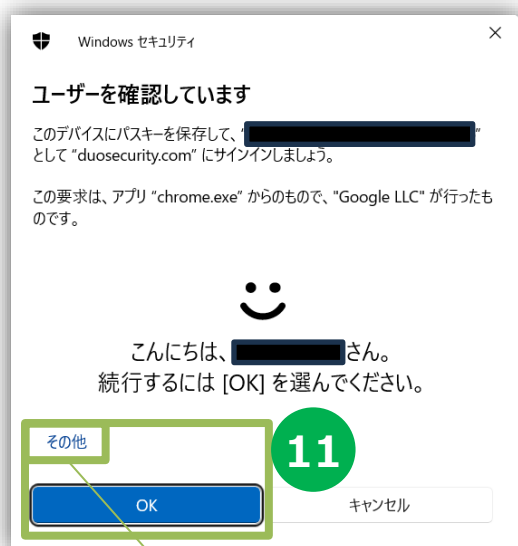
8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

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



8. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

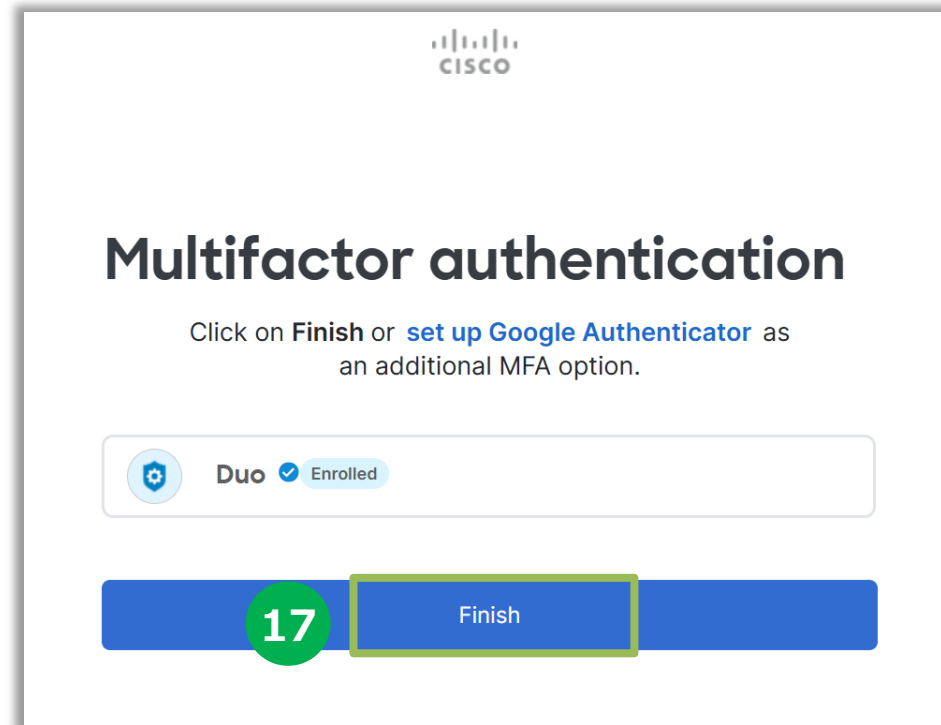
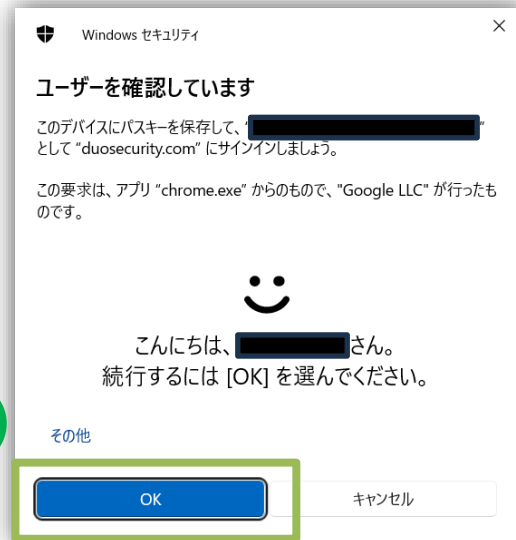
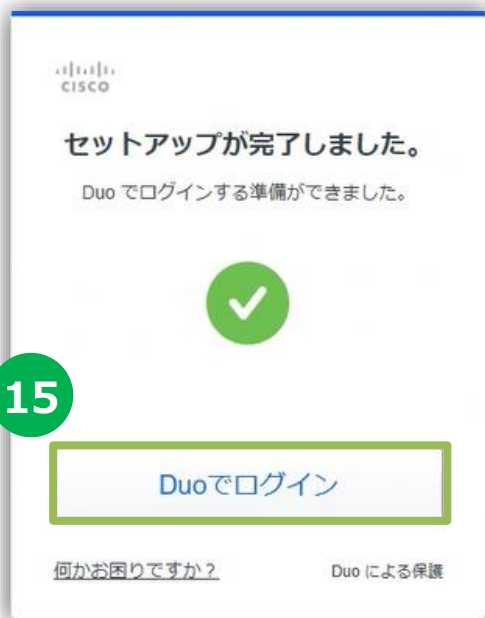
- ⑪ 顔認証が成功したら[OK]をクリック（指紋認証が表示される場合は[その他]から顔認証を選択下さい）
- ⑫ [OK]をクリック
- ⑬ [続行]をクリック
- ⑭ [デバイスを追加しない]をクリック ※認証方法は後からでも追加・変更が可能です。



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>

- 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。
- ブラウザを開き直し、改めてCisco Secure Endpoint管理コンソールのURLを開きます。
Cisco Secure Endpoint管理コンソール : <https://console.apjc.amp.cisco.com>

18

The screenshot shows the Cisco Application Portal interface. At the top, it says 'Application Portal' and 'Welcome back, [redacted]'. Below this, there is a section for 'Secure Client Management' with links for 'North America', 'Europe', and 'APJC'. The main content area is titled 'Applications' and shows a grid of application launch buttons for 'Cisco Cloudlock', 'Cisco Meraki', 'Cisco Umbrella', 'Duo', 'Secure Access', 'Secure Malware Analytics (India)', and 'Secure Workload'. Each button has a 'Launch ->' link. The interface is clean and professional, with a dark header and a light main area.

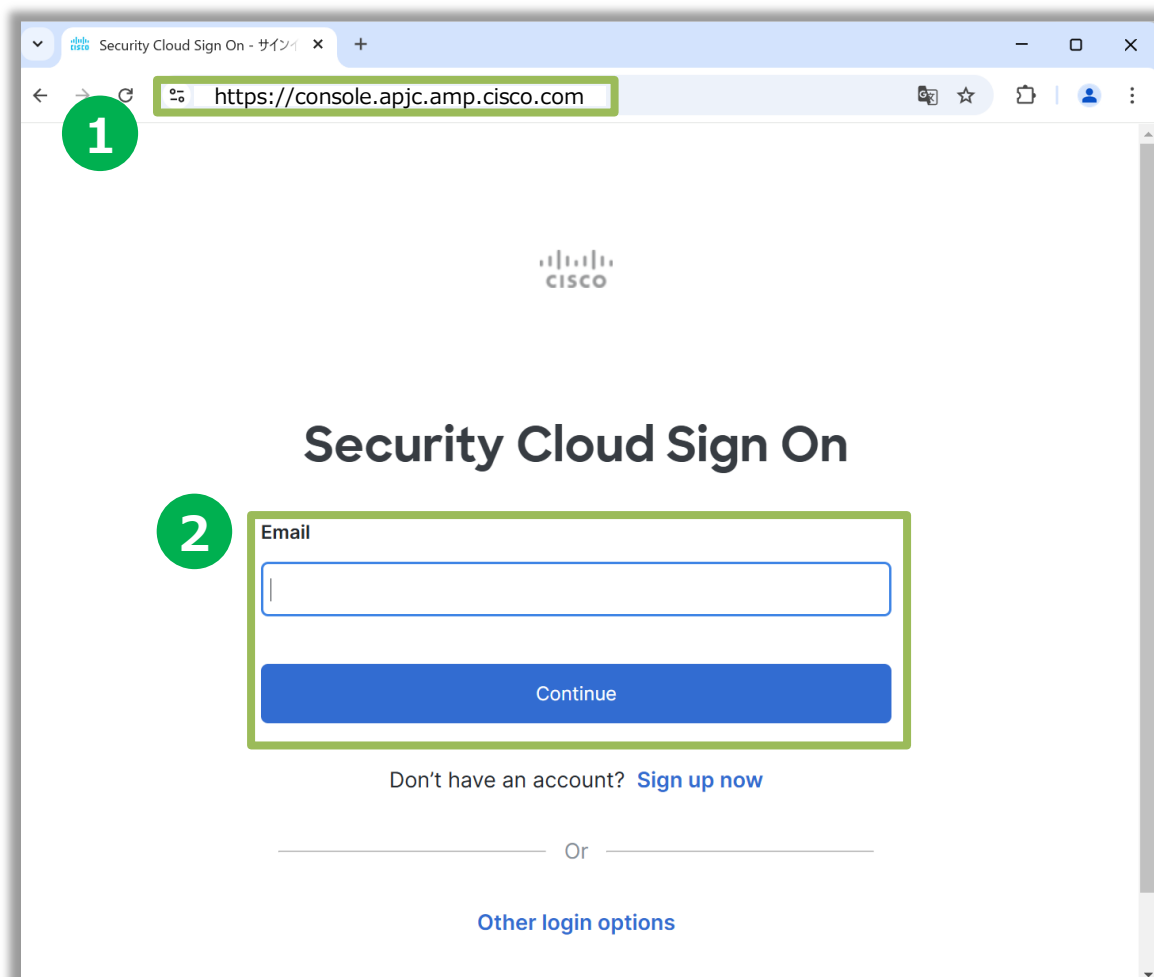
19

The screenshot shows the Cisco Secure Endpoint dashboard in Japanese. The header includes 'Secure Endpoint' and a search bar. The main content area is titled 'ダッシュボード' (Dashboard) and shows a 'はじめに' (Getting Started) section with links for 'Secure Endpointコネクタの導入' (Secure Endpoint Connector Installation) for Windows, Mac, and Linux. There are also sections for 'デモコンピュータ' (Demo Computer) and '低検知度の実行可能ファイル' (Low-detectability executable files). The interface is dark-themed and contains a lot of text and links.

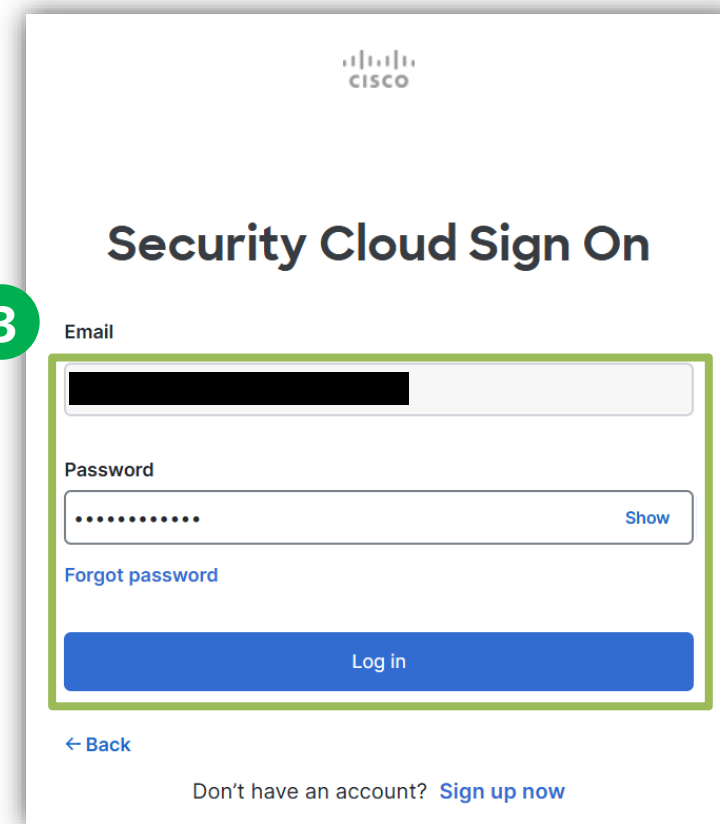
8. コンソールへのログイン手順 <システムログイン>

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



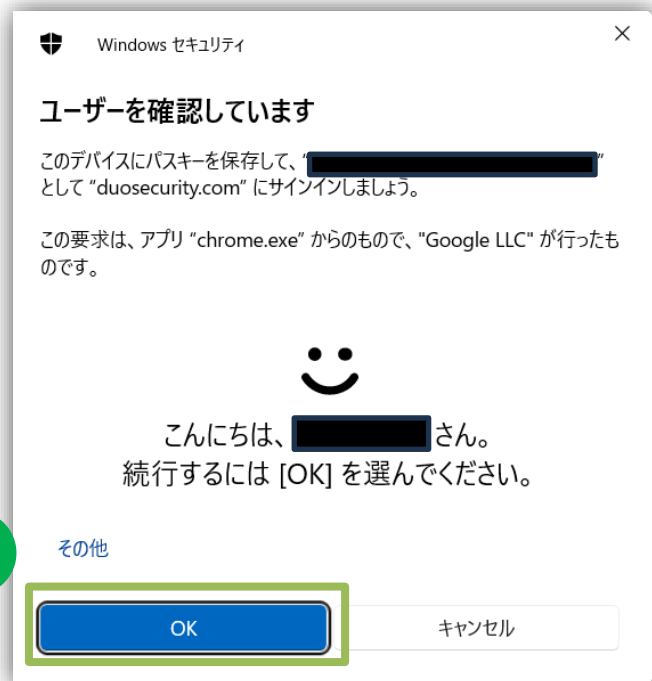
The screenshot shows a web browser window with the URL <https://console.apjc.amp.cisco.com> in the address bar. The page title is "Security Cloud Sign On". A green circle with the number "1" highlights the address bar. Below the title, there is a form with an "Email" label and an empty input field. A green circle with the number "2" highlights this input field. Below the input field is a blue "Continue" button. At the bottom of the page, 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 with the "Email" input field filled with a blacked-out address. A green circle with the number "3" highlights the "Email" label and the input field. Below the "Email" field is a "Password" field with a "Show" button. Below the "Password" field is a "Forgot password" link. At the bottom of the form is a blue "Log in" button. Below the "Log in" button is a "Back" link and a "Don't have an account? Sign up now" link.

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



5

Secure Endpoint

ダッシュボード

はじめに

Secure Endpointコネクタの導入

デモデータ

Cisco XDR
またはSecure Client
Cloud Managementへの統合

デモコンピュータ

CozyDuke

Upatre

PlugX

CryptoWall

低拡散度の実行可能ファイル

The dashboard shows a navigation menu on the left with items like 'ダッシュボード', '受信トレイ', '概要', 'イベント', '分析', 'アウトブレイク制御', '管理', and 'アドミン'. The main content area displays a 'ダッシュボード' (Dashboard) with a 'はじめに' (Getting Started) section, 'Secure Endpointコネクタの導入' (Secure Endpoint Connector Installation) with buttons for Windows, Mac, and Linux, and a 'デモデータ' (Demo Data) section. On the right, there are several informational cards for 'Cisco XDR', 'CozyDuke', 'Upatre', 'PlugX', 'CryptoWall', and '低拡散度の実行可能ファイル'.

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

The screenshot displays the Cisco Secure Endpoint dashboard. The main header shows the Cisco logo and 'Secure Endpoint' text. Below the header, there's a search bar and navigation icons. The dashboard is divided into several sections:

- ダッシュボード (Dashboard):** Shows a large red bar chart for '受信トレイ' (Inbox) with a 76.9% '侵害されている' (Compromised) status. Below it are charts for '重大侵害の観測対象' (Critical Incident Targets) and '侵害イベントタイプ' (Incident Types).
- 受信トレイのステータス (Inbox Status):** Shows 30 items requiring attention, 0 in progress, and 0 resolved.
- 脆弱性 (Vulnerabilities):** Lists 23 high-severity vulnerabilities and 33 high-risk computers.
- Secure Malware Analytics:** Shows 0 automatic analysis submissions and 2 suspicious detections.
- 統計 (Statistics):** Shows 39 computers, 29.4K scanned files, and 3.31K network connections.
- クイックスタート (Quick Start):** Provides links to set up Windows, Mac, and Linux connectors.

This screenshot shows the help menu that appears when the help icon is clicked. It includes the following information:

- ヘルプのインデックス (Help Index)
- ダッシュボード (Dashboard) タブ (Dashboard Tab): Explains that the dashboard shows the top 14 days of detected incidents and provides details on how to filter and refresh data.
- ヘルプ目次 (Help Contents)
- リリースノート (Release Notes)
- サポートへの問い合わせ (Contact Support)

不明な点はこちらに説明が
記載されております。

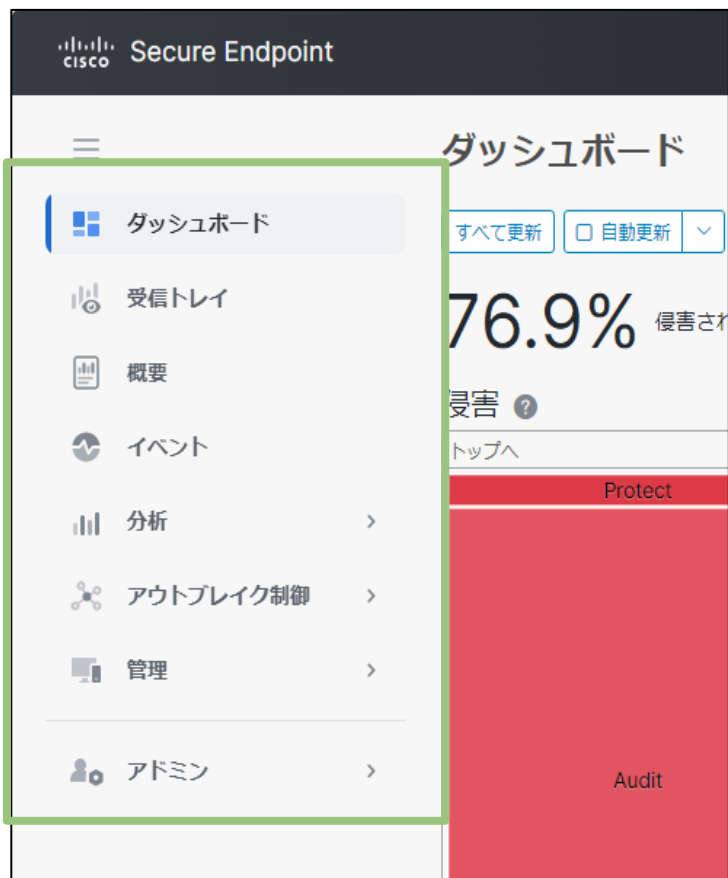
<言語設定>

This screenshot shows the language selection menu. It includes the following options:

- English
- 日本語 (Japanese) - Selected with a checkmark
- 한국어 (Korean)
- 中文 (Chinese)

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

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

1. 該当端末をネットワークから切断する

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

2. Secure Endpointでの手動隔離の実施

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

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



2. Secure Endpointでの手動隔離の実施（つづき）

④感染が疑われるコンピュータを選択し、「隔離の開始」をクリックします。



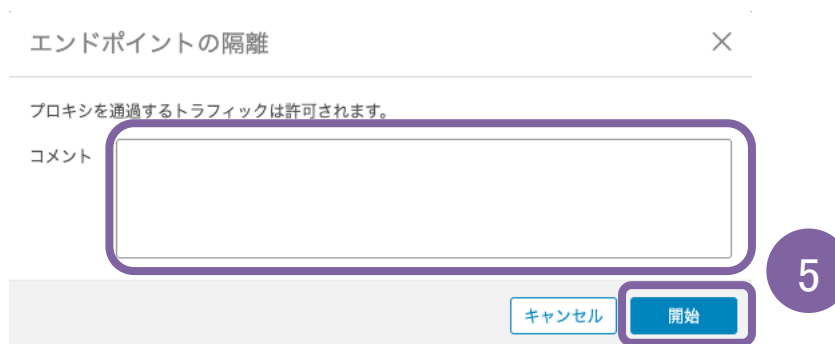
グループ「Protect」内のODS-NewZero3 Demo1 定義は最新です

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
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。

グループ「Protect」内の Demo_AMP

▶ 隔離

ホスト名	Demo_AMP	グループ	Protect
オペレーティング システム	Windows 10 (ビルド 19044.1466)	ポリシー	Protect
コネクタバージョン	8.4.4.30419 ダウンロードURLを表示する	内部IP	1.
インストール日	2025-02-	外部IP	5
コネクタのGUID	07ff74c3-	最新の確認日時	2
プロセッサID	6a50b8d-	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

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

⑦任意でコメントを記載し、「開始」をクリックします。

エンドポイントの隔離

コメント

キャンセル 停止

7

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イ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、ウイ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しまい、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、ウイ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イ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イ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イルスがあります。マクロウイルスに感染したファイルを開いてしまうと、ウイルスが実行されて、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

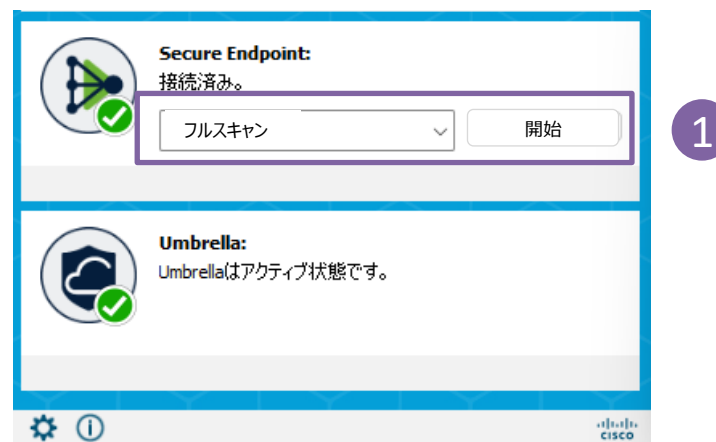
多くのコンピュータでは、USBメモリをコンピュータに差し込んだだけで自動的にプログラムが実行される仕組みが用意されています。この仕組みを悪用して、コンピュータに感染するウイルスがあります。

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

p7-40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

p7-40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。

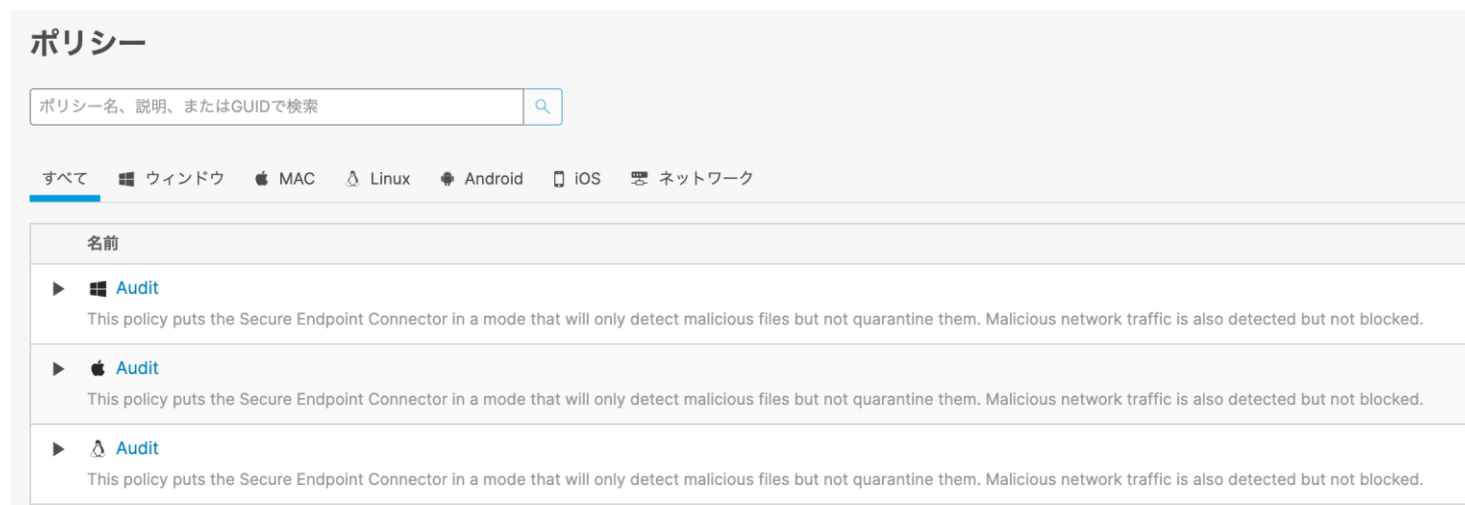
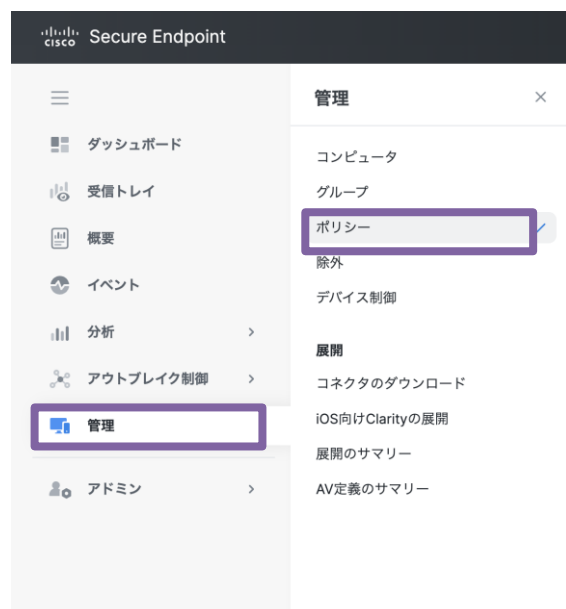
① Secure Endpoint をアンインストールする方法

p41-52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
- プロキシ
- アウトブレイク制御
- デバイス制御
- 製品の更新
- 詳細設定

判定モード

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

ファイル ⓘ

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。

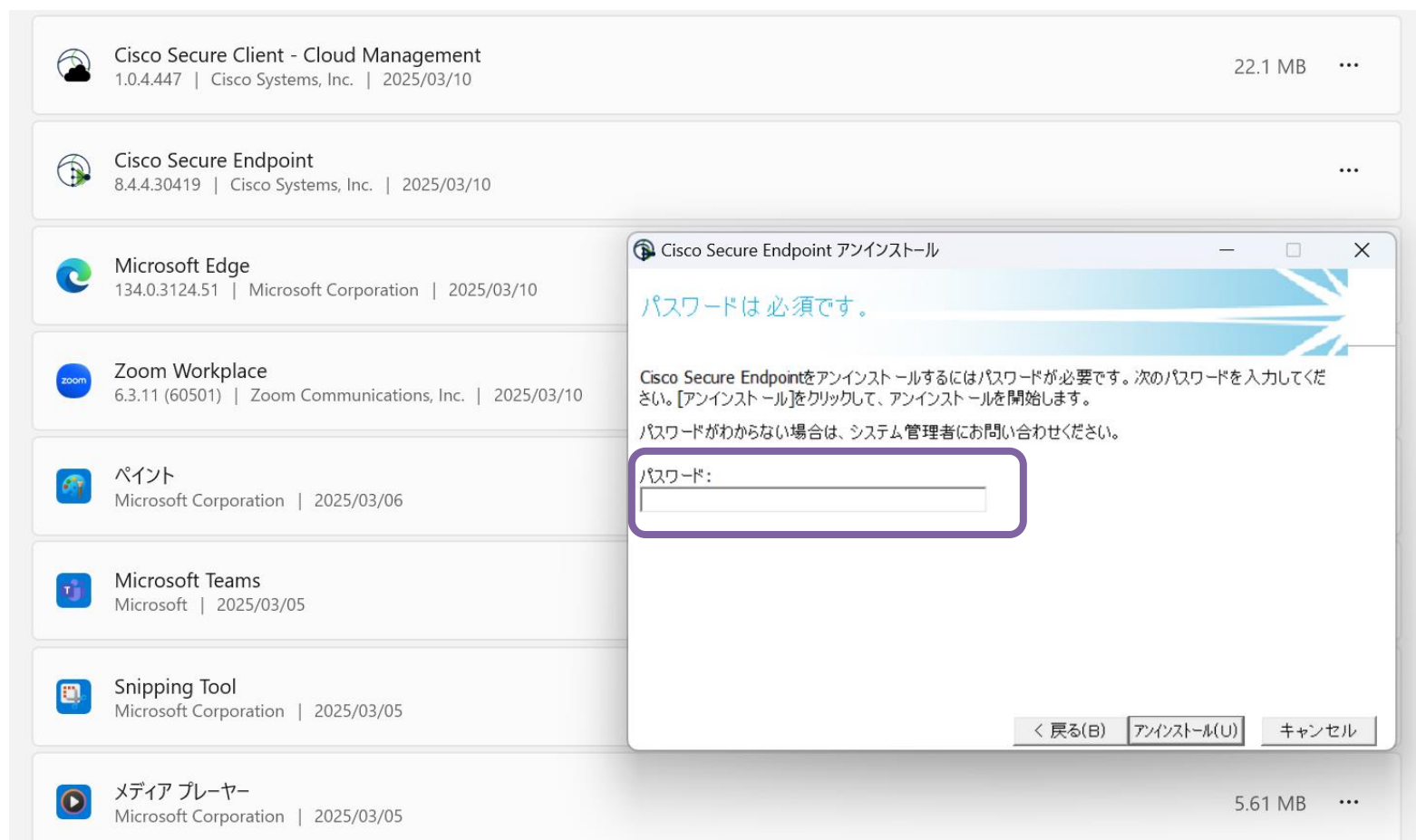
スクリプト保護 ⓘ

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、エンドユーザー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。



インストール時のパスワードロック方法

- ① Secure 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 Cisco Secure Endpoint

ダッシュボード

はじめに
[オンラインヘルプの表示](#)

Secure Endpointコネクタの導入

- [Windowsコネクタのセットアップ](#)
- [Macコネクタのセットアップ](#)
- [Linuxコネクタのセットアップ](#)

デモデータ

デモデータを使用して、実際にマルウェアに感染した状態から再生したデータをコンソールに入力することにより、Cisco Secure Endpointの仕組みを知ることができます。デモデータを有効にすると、コンピュータとイベントがSecure Endpointコンソールに追加され、マルウェアが検出されたときの各表示(ダッシュボード、ファイルトラジェクトリ、デバイストラジェクトリ、脅威の根本原因、検出結果とイベント)の動作を見ることができます。デモデータは実際に使用中のSecure Endpoint環境からのデータと共存させることができますが、デモデータ中のマルウェアにはシビラティ（悪大度）が高いものがあり、表示によっては実際のイベントが見えなくなる場合があります。

[デモデータの有効化](#)

デモコンピュータ

WMIPRVSEがエンコードされたPowerShellを起動しました [ここをクリックしてPDFを表示します](#)

Secure Endpointの動作保護エンジンが、エンコードされたコマンドでPowerShellを実行するWMIプロバイダーサービス(wmiprvse.exe)を検出すると、WannaMine攻撃は停止されます。エンコードされたコマンドが攻撃継続には必要ですが、動作保護エンジンがプロセスを終了して、悪意のあるアクションがそれ以上実行されないようにします。

CozyDuke [ここをクリックしてPDFを表示します](#)

悪用されたDLL検索パスまで検出をトレースし、アップストリームCnCへの通信をブロックし、エンドポイントIOCを展開してさらなる攻撃を封じ込めます。

Upatre [ここをクリックしてPDFを表示します](#)

スパイフィッシング攻撃の開始から終了までの軌跡を表示します。

PlugX [ここをクリックしてPDFを表示します](#)

マルウェア攻撃をトレースし、エンドポイントIOCを使用してさらなる攻撃を封じ込める方法を学習します。

CryptoWall [ここをクリックしてPDFを表示します](#)

Secure Endpointが疑わしいURLを検出します。Secure Malware Analyticsでサンドボックスを使用してランサムウェアを検出する方法を確認します。

低拡散度の実行可能ファイル [ここをクリックしてPDFを表示します](#)

Cisco XDR
またはSecure Client [詳しくはこちら](#) [今すぐ統合](#)
Cloud Managementへの統合

インストール時のパスワードロック方法（続き）

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

The screenshot displays the Cisco Secure Endpoint management interface. On the left, a navigation menu is visible 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, and アドミン. The '管理' (Management) item is highlighted with a purple box and a circled '2'. A secondary menu is open for '管理', listing options such as コンピュータ, グループ, ポリシー, 除外, デバイス制御, ホストファイアウォール, 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 'ポリシー' (Policy) item is highlighted with a purple box and a circled '3'. The main content area shows the '受信トレイのステータス' (Inbox Status) section with indicators for 0 items needing attention, 0 in progress, and 0 resolved. Below this is the '隔離された検出' (Isolated Detection) section, which is currently empty.

アインインストール時のパスワードロック方法（続き）

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

ポリシー

① すべての変更の表示 + 新しいポリシー

ポリシー名、説明、またはGUIDで検索

すべて ウィンドウ MAC Linux Android iOS ネットワーク 説明を表示

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

14個の項目の1~14 25 / ページ 1 1個の

4

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 ⓘ

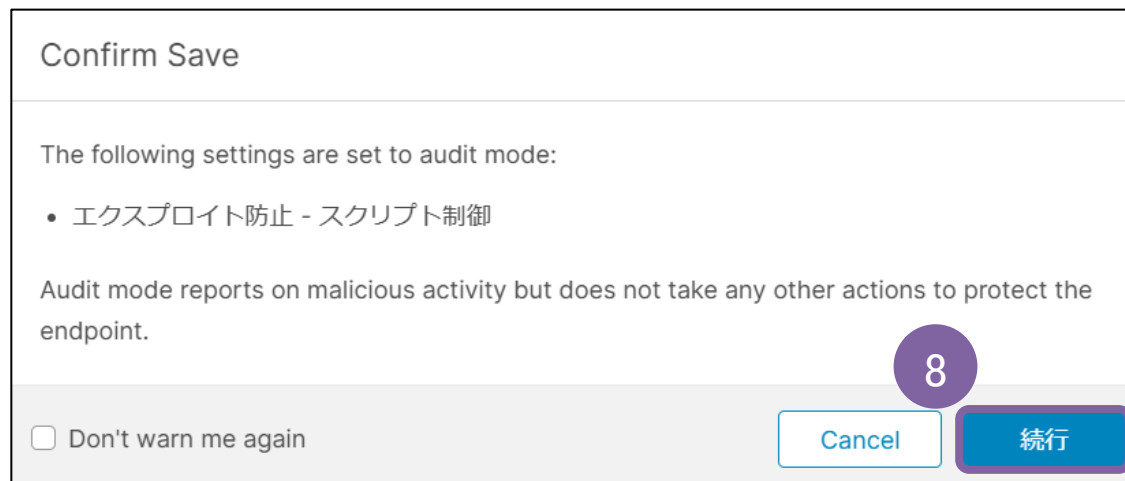
コマンドラインログ ⓘ

⑦

キャンセル 保存

インストール時のパスワードロック方法（続き）

⑧確認画面が表示されたら「続行」をクリックし、設定を完了します。



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

また、逆に、デバイストラジェクトリ上怪しい動作をしているファイルが Clean/Unknown と判定され、マルウェアを逃してしまうケース (False Negative) も考えられ、こちらもお客様にて判断が難しい場合がございます。そういった場合に、「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用です。

ファイル分析の利用方法

ファイル分析 は、Sandbox 上の小さな端末上で実際に、検体を実行し、その挙動を観察、レポート化さらに、発生した挙動の危険度/信頼度に応じて点数化をするため、お客様が Malware であるかを判断するために非常に有効なツールです。ファイル分析 の最も基本的な使用方法是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

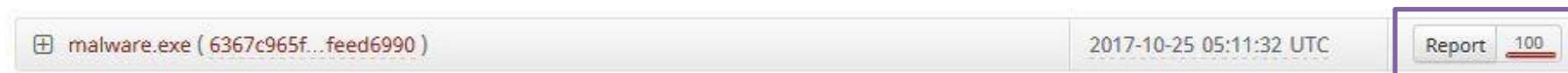
送信するファイル: 参照

分析用のVMイメージ ▼

キャンセル アップロード

ファイル分析の利用方法（つづき）

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



④Report をクリックすると、実行結果の詳細となるレポートが表示されます。こちらの例では、TOR のノードに対して DNS の名前解決を実行していることから、高い確度で Malware であると判定していることが確認できます。

Behavioral Indicators

Potential TOR Connection 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, 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用です。本項では、分析およびイベント、デバイストラジェクトリからの、検体の リモートでの取得、および、Sandbox へ自動送信を行う方法を説明いたします。

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

▼ Demo_AMP_Threat_Auditがekjrnjgkjer.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	ekjrnjgkjer.exe
	ファイルパス	C:\ekjrnjgkjer.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

分析用のVMイメージ

▲ 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。

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 security console interface. On the left, a table lists files in the device registry. The file 'ekjrnjker.exe [PE]' is highlighted with a red box. A context menu is open over this file, with 'ファイル取得' (File Acquisition) highlighted by a purple box. An arrow points from this menu to a detailed view of the 'ファイル取得' (File Acquisition) action on the right. This view shows the status as 'Requested' and lists available actions: 'ファイル取得' (File Acquisition), 'シンプル検出' (Simple Detection), and 'ブロックされたアプリケーション' (Blocked Application). The 'ファイル取得' (File Acquisition) option is highlighted with a purple box.

Demo AMP

b1380fd..523967

処置: 悪意がある

ファイル名: Unknown

VirusTotalに含まれていないファイル

VirusTotal

SHA-256のコピー

検索

完全なSHA-256の表示

ファイル分析

ファイルトラジェクトリ

ファイル取得

シンプル検出

ブロックされたアプリケーション

許可されたアプリケーション

戻る

転送

再読み込み

ekjrnjker.exe [PE]

rundll32.exe [PE]

mobsync.exe [PE]

svchost.exe [PE]

audiodg.exe [PE]

ファイル取得

シンプル検出

ブロックされたアプリケーション

ファイル取得

ステータス: Requested

[ファイルの取得 (Fetch File)]

ファイルリポジトリで表示

隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

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



The screenshot shows the 'ファイルリポジトリ' (File Repository) interface. At the top, there is a search bar with the text 'SHA-256またはファイル名で検索' and a search icon. To the right, there are dropdown menus for 'タイプ' (Type) set to 'すべて' and 'グループ' (Group) set to 'すべてのグループ'. Below these are buttons for 'フィルタのクリア' and 'フィルタを適用'. A navigation bar below the search area includes tabs for 'All', 'Available', 'Requested', 'Being Processed', 'Failed', and 'Rejected'. The main content is a table with columns: 'ファイル', 'ステータス', 'リクエスト作成者', '日付', and 'アクション'. A single file entry is visible with the ID '3372c1edab46837f1e973164fa2d726c5c5e17bcb888828cccd7c4dfcc234a370', status '要求済み', creator '自動化されているア...', and date '2025-03-25 19:36:55 JST'. Below the table, there is a '変更の表示' link and a row of buttons: '分析' (highlighted with a purple box), 'ダウンロード', and '削除'. A detailed view of the file is shown below the table, including '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', and 'コンピュータ: Demo_TeslaCrypt'.

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。

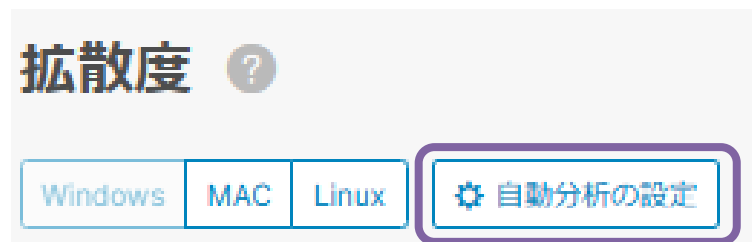
①分析 > 拡散度 にアクセスすると、組織の中で1つの端末でしか実行されていないファイルがリストアップされて表示されます。



拡散度 ?			
OS	File Name	Action	Timestamp
Windows	25791113...deddb603 は Demo_Command_Line_Arguments_Meterpreterでの...	分析	2025-03-25 19:21:06 JST
MAC	eba241a9...35feb63a は Demo_Command_Line_Arguments_Meterpreterでの...	分析	2025-03-25 19:21:03 JST
Linux	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。



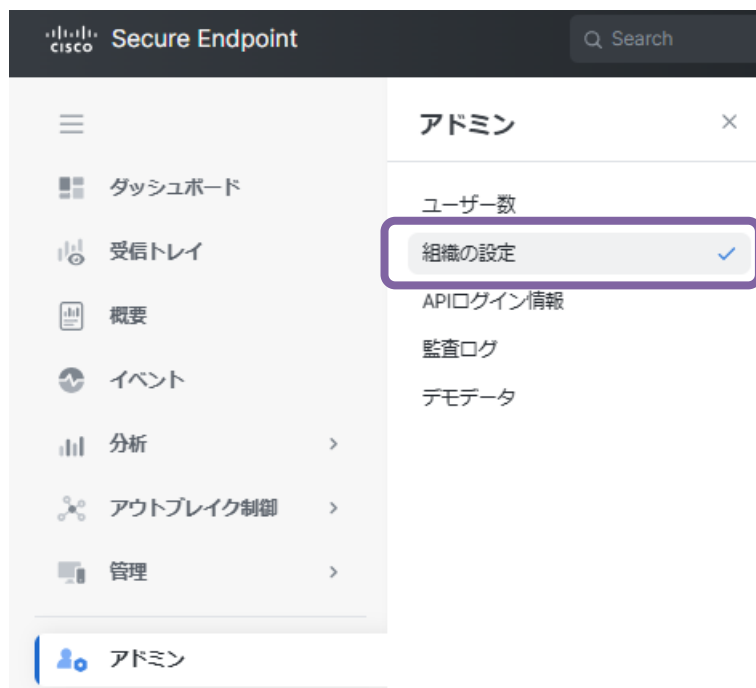
③自動分析の対象となる端末が所属する グループ を指定し、適用 をクリックすれば、実行頻度の低いファイルを自動的にSandbox 分析にかけることが可能です。



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。

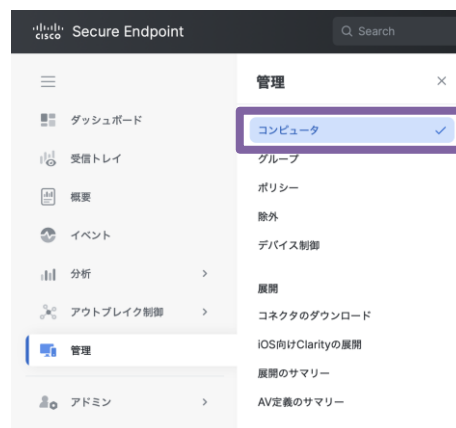
- 1日に実行可能な ファイル分析 の合計カウント数に追加されることとなりますため、数多くファイルが アップロードされる環境では注意が必要です。
- 先ほどと同様、拡散度 からの 自動分析も、端末からのファイルの収集 (Remote File Fetch)を実行するため、二段階認証を有効にする必要があります。有効になっていない場合は、分析 ボタンと 自動分析 ボタンがグレーアウトされて実行できませんので、設定する場合は、事前に設定をお願いします。



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。

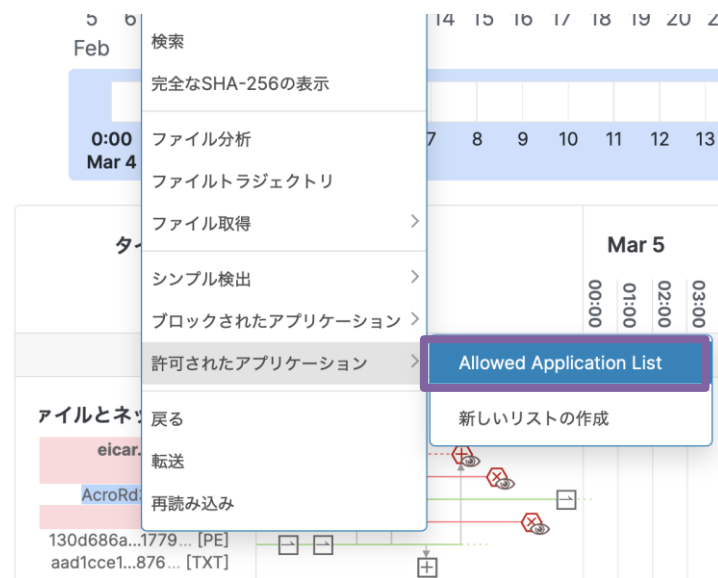
グループ 'Audit' 内の Demo_SFEicar			
ホスト名	Demo_SFEicar	グループ	Audit
オペレーティング システム	Windows 10 (ビルド 19043.1266)	ポリシー	Audit
コネクタバージョン	8.4.4.30419 ダウンロードURLを表示する	内部IP	63.85.183.224
インストール日	2025-02-03 00:37:39 UTC	外部IP	222.176.197.7
コネクタのGUID	36b6891b-e248-4462-8dc8-7f2eff09f190	最新の確認日時	2025-03-05 00:37:39 UTC
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

デバイスストラジェクトリ

検索ボタン: 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。

The screenshot displays the Cisco Secure Endpoint management console interface. The top navigation bar includes the Cisco logo and the text 'Secure Endpoint'. A sidebar on the left contains a menu with items: 'ダッシュボード', '受信トレイ', '概要', 'イベント', '分析', and 'アウトブレイク制御'. The 'アウトブレイク制御' menu item is highlighted, and a sub-menu is open, showing options: 'カスタム検出', 'Simple', 'Advanced', 'Android', 'アプリケーション制御', 'ブロックされたアプリケーション', and '許可されたアプリケーション'. The '許可されたアプリケーション' option is selected and highlighted with a purple box. Below the navigation, a '作成' (Create) button is visible. The main content area shows the 'Allowed Application List' configuration page. It includes the title 'Allowed Application List', the number of files '0個のファイル', the creator 'Masashi Ikuse', and the creation time '2025-02-17 06:29:20 UTC'. Below this, it lists applications used in policies: 'Audit, Audit, Audit, Domain Controller, Protect, Protect, Protect, Server, Triage, Triage' and applications used in groups: 'Audit, docopura, Domain Controller, Protect, Server, Triage'. At the bottom of the configuration area, there are three buttons: '変更の表示' (Show changes), '編集' (Edit), and '削除...' (Delete...). The '編集' button is highlighted with a purple box.

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。

The screenshot shows the 'Allowed Application List' management page. At the top, there is a title bar with 'Allowed Application List' and a '更新名' button. Below this, there are two links: 'SHA-256の追加' and 'ファイルのアップロード', with the latter being underlined. A third link, 'SHA-256のセットのアップロード', is also present. The main area contains the instruction '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)'. Below this is a file selection interface with three buttons: 'ファイル', '選択されているファイルなし', and '参照'. A '注' (Note) field is empty. At the bottom of this section is an 'アップロード' button with an upload icon. The bottom section is titled '含まれているファイル' and states '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。

The screenshot shows the details of an 'Allowed Application List'. At the top right is a '作成' button. The title is 'Allowed Application List'. Below the title, '1個のファイル' is highlighted with a red box. The creator is 'Masashi Ikuse' and the creation time is '2025-02-17 06:29:20 UTC'. The text indicates it was created by a policy. The list of applications is: 'Audit, Audit, Audit, Domain Controller, Protect, Protect, Protect, Server, Triage, Triage'. The groups using it are: 'Audit, docopura, Domain Controller, Protect, Server, Triage'. At the bottom, there are buttons for '変更の表示', '編集', and '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。

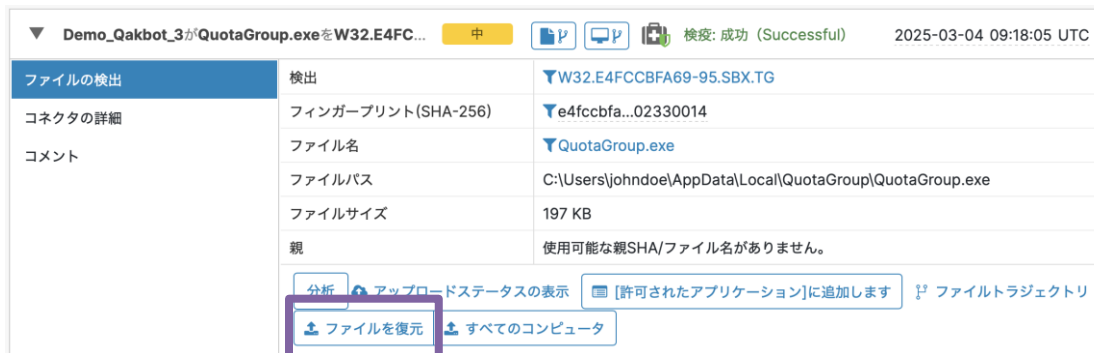
隔離されたファイルの復元方法

- 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

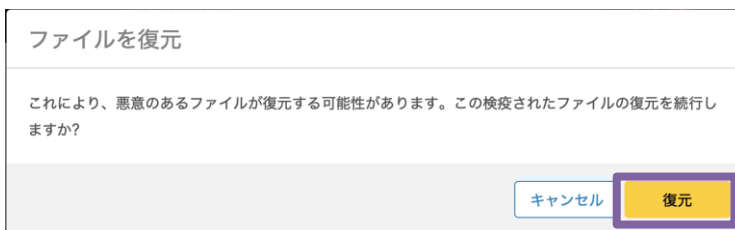


隔離されたファイルの復元方法（つづき）

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

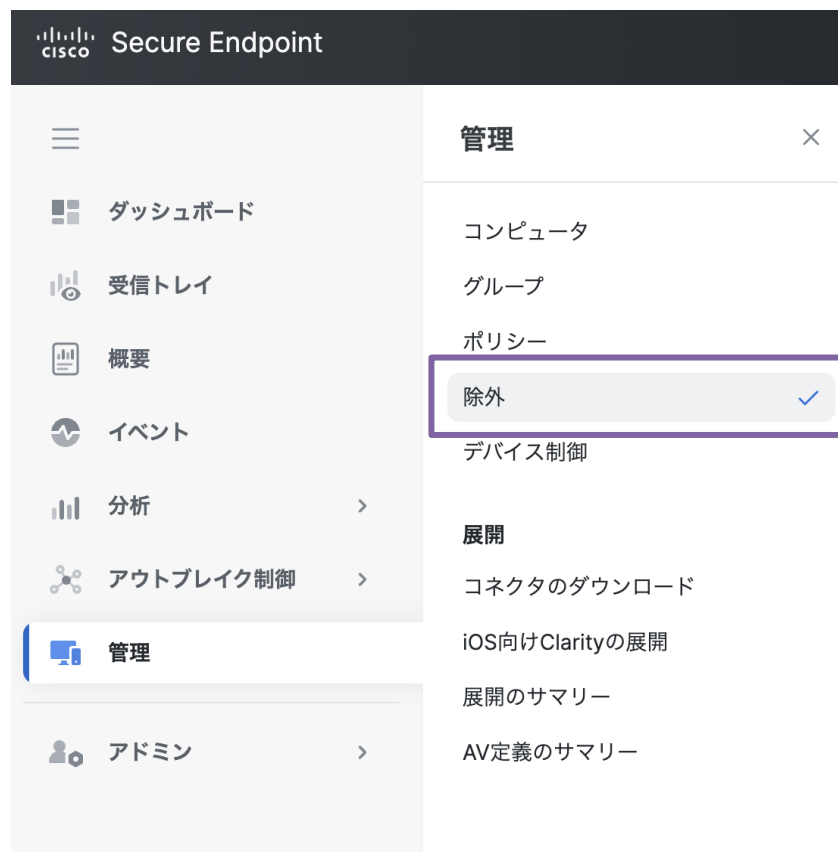
上記に問題がなければ、サポート窓口にお問い合わせください。

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

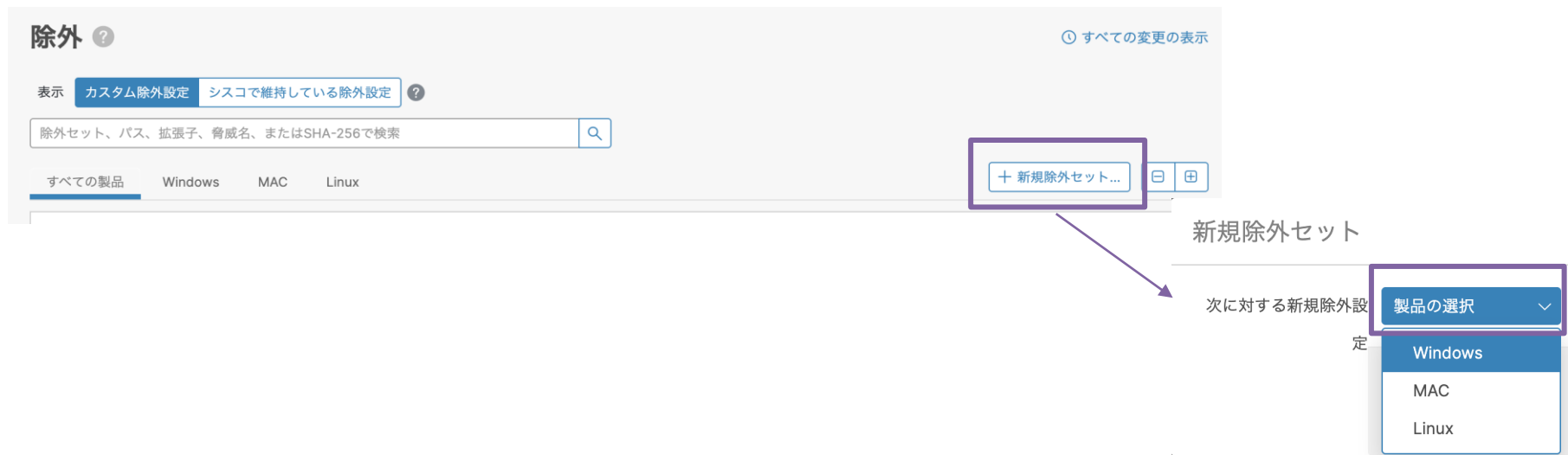
①Cisco Secure Endpoint管理コンソールにログインし、管理 > 除外を選択してください。



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。

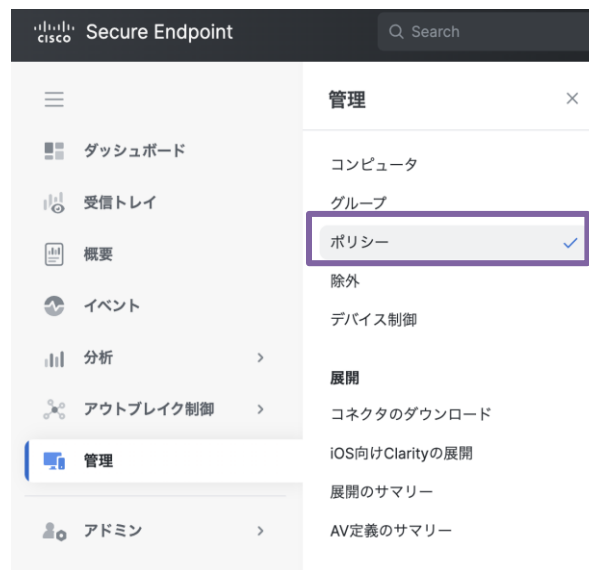
← Exclusions
新規除外セット
Windows
名前 AMP
+ 除外を追加 + 複数の除外の追加...
パス C:\AMP Test\to be excluded
保存

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 グループで使用
パス C:\AMP Test\to be excluded なし
ポリシーで使用
なし
変更の表示 変更日 2025-03-07 15:51:45 UTC 編集 削除

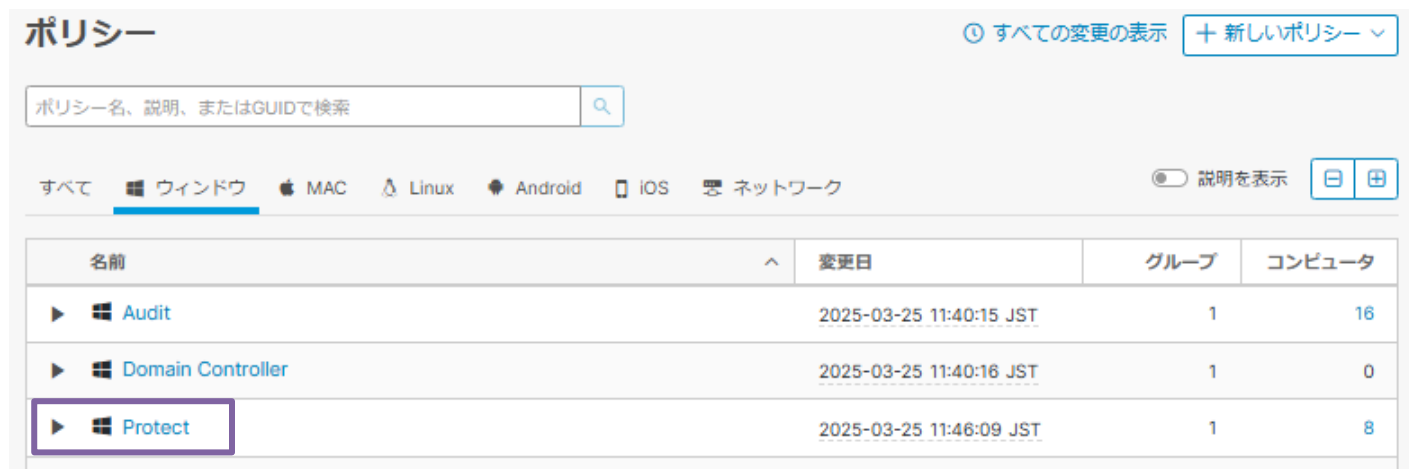
対処方法（つづき）

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

カスタム除外設定 1件が選択されました

検索 AMP 1個の除外

AMP 1個の除外

保存 キャンセル

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://elgana.jp/>

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. 管理' (elgana Management) interface. On the left is a navigation menu with items like 'ダッシュボード', 'ユーザー', '利用端末', '環境設定', 'サービス連携', '詳細', '契約プラン', '管理者', 'メッセージログ', 'ファイル', '操作履歴', 'プランをアップグレード', 'ご利用ガイド', 'カスタマーサポート', and 'ご利用者ヘルプ'. The main content area is titled 'ユーザー' (Users) and features a summary box with '登録ユーザー数' (Registered User Count) at 2 and '契約ユーザー数' (Contracted User Count) at 10, with a '変更' (Change) button. To the right of this box is a 'ユーザー登録' (User Registration) button. Below the summary is a search bar and a table of users. The table has 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). Two users are listed, both with '利用中' (In Use) status and an update date of 2024/12/10.


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。



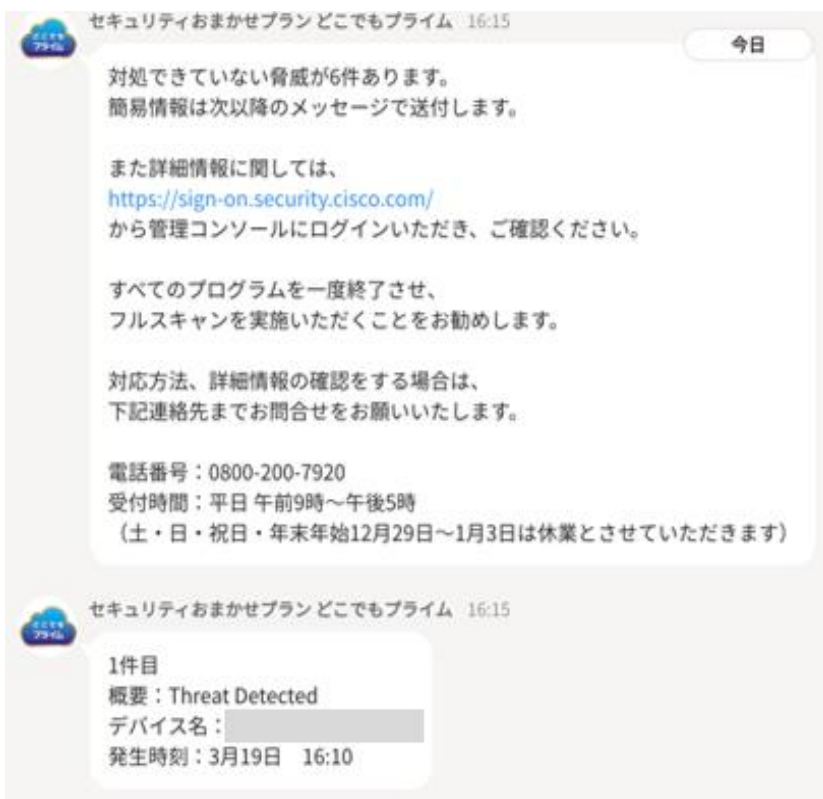
スクリーンショットは、elganaサービス管理サイトの検索画面を示しています。左側のナビゲーションメニューには「お気に入り」、「所属組織」、「検索」、「タスク」、「組織図」、「連絡先」があります。左側の「連絡先」メニュー項目は1で示されています。検索ボックスには「セキュリティおまかせ」と入力されており、検索ボタンは2で示されています。検索結果には「あか た な は ま や ら わ A #」と表示されています。検索結果のリストには「名前/所属先」、「メールアドレス」、「電話番号」の列があります。リストには「セキュリティおまかせ」と「セキュリティおまかせプランどこでもプライム」が表示されています。右側の「セキュリティおまかせ」項目には吹き出しマークがあり、これは3で示されています。

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。

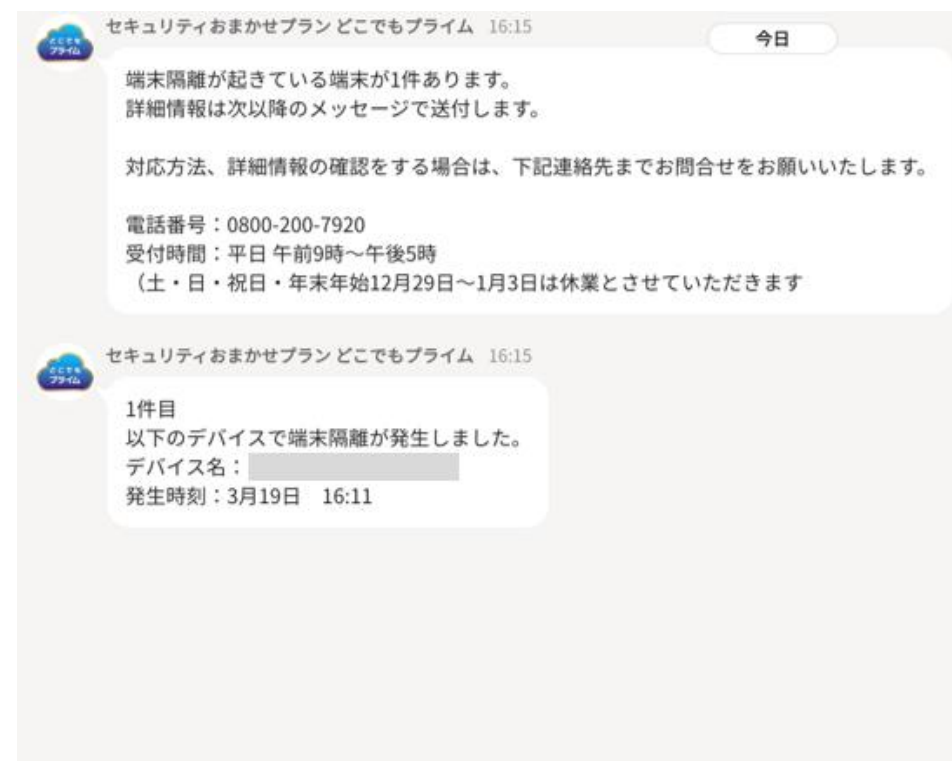
対応方法、詳細情報の確認をする場合は、
下記連絡先までお問合せをお願いいたします。

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

困ったなあ...そんなときは

サポートセンターの
情報を確認



最新の通知内容の確認は

通知確認

通知の変更は

通知設定

