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 1.6）

2025年10月
西日本電信電話株式会社

改定履歴

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

目次

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

セキュリティおまかせプラン どこでもプライム

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

セキュリティおまかせプラン どこでもプライム

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®

セキュリティおまかせプラン どこでもプライム

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

elgana

※1　以降、セキュアインターネットゲートウェイ　もしくは　Umbrellaと記載
※2　以降、セキュアエンドポイント　もしくは　Secure Endpointと記載

2. 事前準備

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

＜Windows 10 の場合＞
「スタート」⇒「コントロールパネル」⇒「プログラムと機能」⇒「プログラムのアンインストール」

＜Windows 11 の場合＞
「スタート」⇒「コントロールパネル」⇒「プログラム」⇒「プログラムのアンインストール」

＜Macの場合＞
・App Store からインストールしたアプリを削除するには、まず Launchpad を 開きます。
⇒ LaunchPad を起動後、どれか一つアプリを長押しします。
⇒ アプリの左上に × マークが表示されます。
⇒ 削除したいアプリの × マーク をクリックします。

・App Store 以外からインストールしたアプリの場合、アンインストールプログラムが 用意されている場合は、対象のプログラムをクリックしてアンインストールを実施。

★詳しくは各ソフトウェアのマニュアルをご参照ください。

3. ソフトウェアの対応OS、バージョン、システム要件①

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

＜対象ソフトウェア＞

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

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

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

セキュアインターネットゲートウェイ　※「Umbrella Roaming Security」の欄をご確認ください。
セキュアエンドポイント（Windows OS）
セキュアエンドポイント（mac OS）

3. ソフトウェアの対応OS、バージョン、システム要件②

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

<対象ソフトウェア>

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

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

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

※Windowsのシステム要件参照

※Macのシステム要件参照

4. ソフトウェアのインストール手順

WindowsOSの場合

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

MacOSの場合

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

4-1. 開通メールからelganaマイページへログイン

4-1. インストール手順＜elganaマイページへのログイン-1＞

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

項目	情報
TO	（申込書にご記載いただいたメールアドレス）
BCC	○○○
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	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）** 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 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えますのでご注意ください。 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。 **◆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たメールアドレス）** **初期パスワード：（開通センタで設定するパスワード）** ※複数端末にインストールされる場合、上記からダウンロードした端末設定ツールを端末に展開ください。 ※ご契約総ID数を超えて端末にインストールされた場合、追加請求が発生する場合がございます。 ※インストーラの取り扱いには十分ご注意ください。 **◆インストールの手順書等掲載先** **https://office-support.ntt-west.co.jp/security_dokodemo_prime/** ～～ ～～ 【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） 【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/

①開通メールイメージ

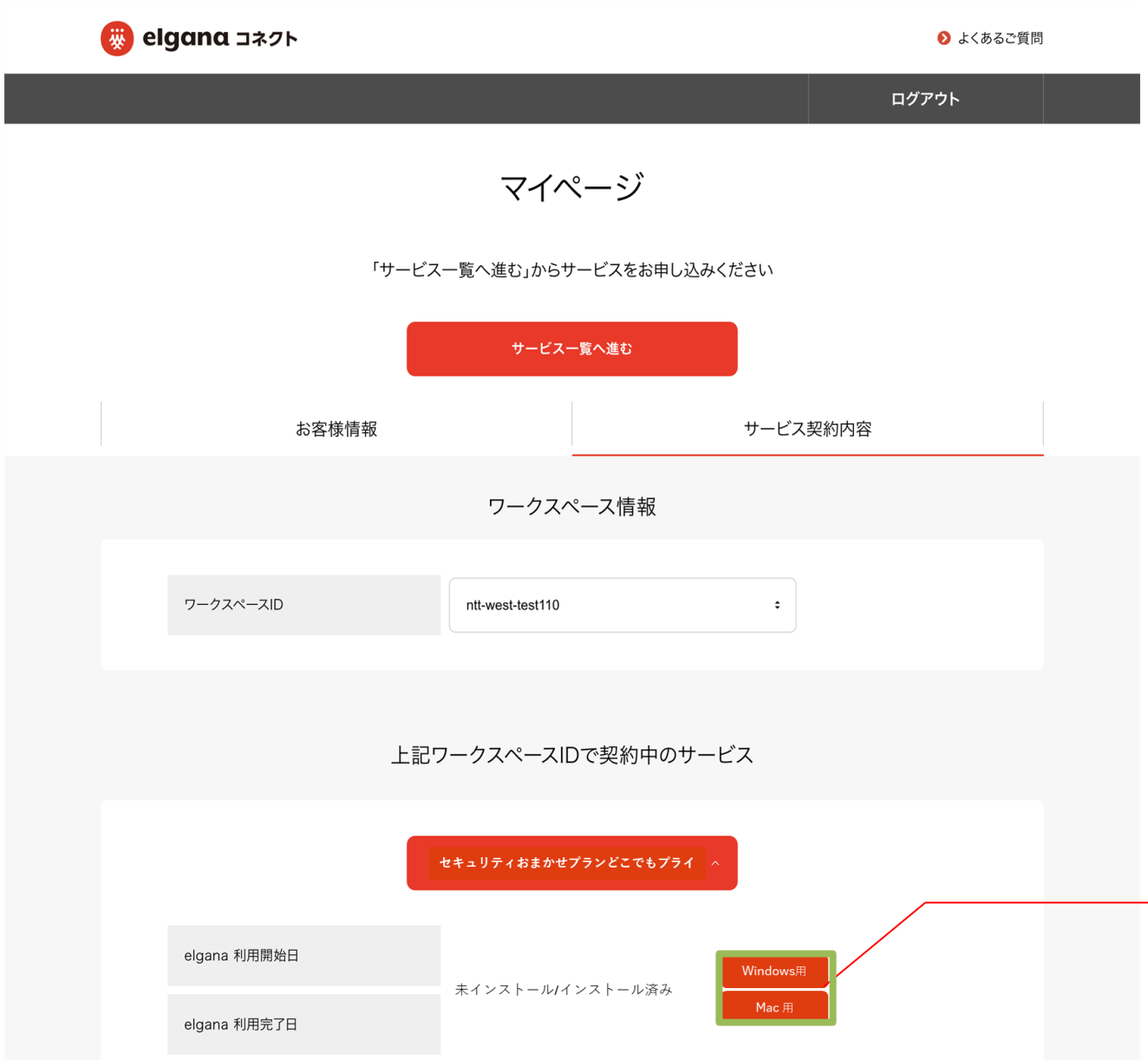
②端末設定ツール入手用のURL及びログイン情報

4-1. インストール手順＜エルガナマイページへのログイン-2＞

③elganaコネクトのログイン画面へ遷移
④開通メールに記載の「ログインID」「パスワード」を入力し、「ログイン」を選択

4-2. インストーラーのダウンロード

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

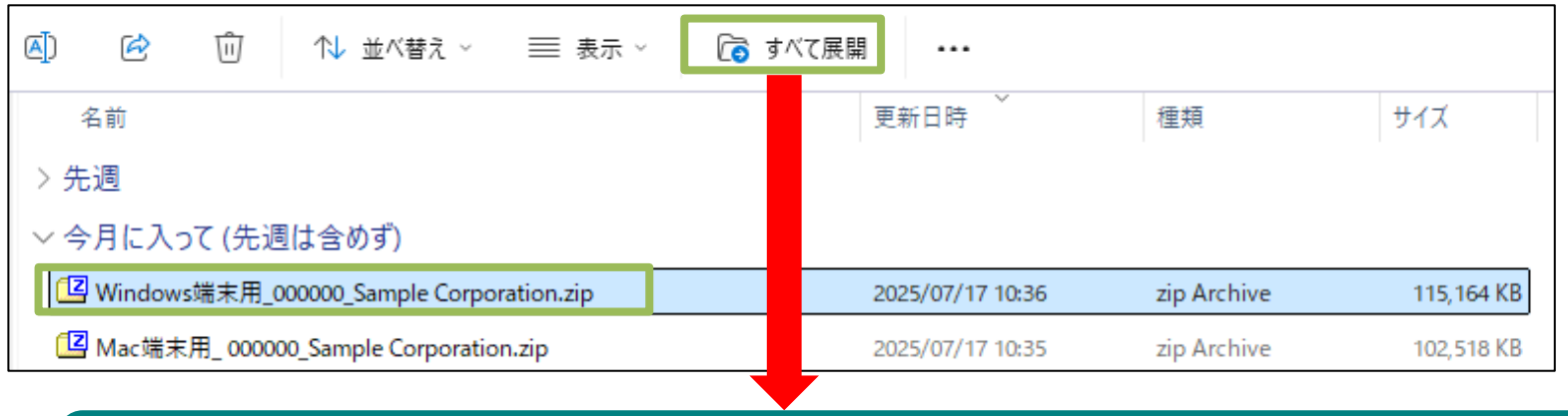


対象OSのインストーラを選択しダウンロード

4-3. ダウンロードしたインストーラーの実行_Windows

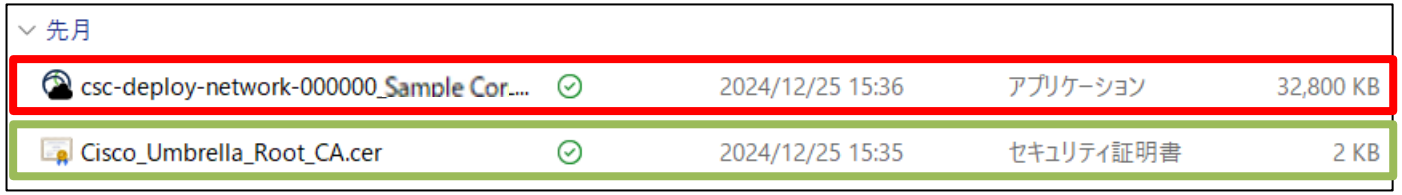
4-3. インストール手順＜ダウンロードしたインストーラの実行-1＞

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



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

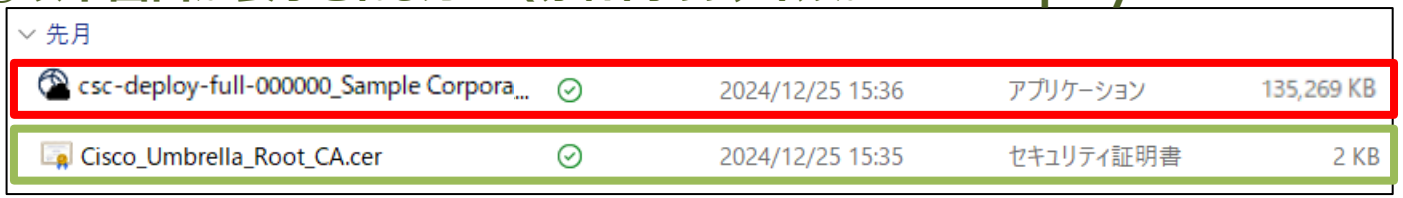
①以下画面が表示される方　（赤枠内のファイルが「csc-deploy-network-000000_Sample Corporation.exe」となっている）



👆 ダブルクリックで実行後、ポップアップ画面に従いインストール

👆 ダブルクリックで実行後、ポップアップ画面に従い証明書をインポート

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



👆 ダブルクリックで実行後、ポップアップ画面に従いインストール

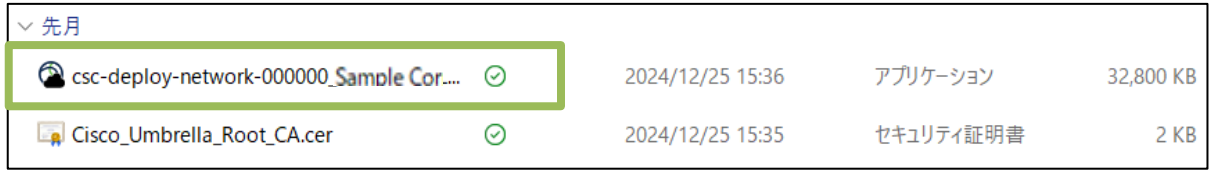
👆 ダブルクリックで実行後、ポップアップ画面に従い証明書をインポート

👆 **具体的なインストール手順は次ページ以降を参照**

4-3. インストール手順 <ダウンロードしたインストーラの実行-2>

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

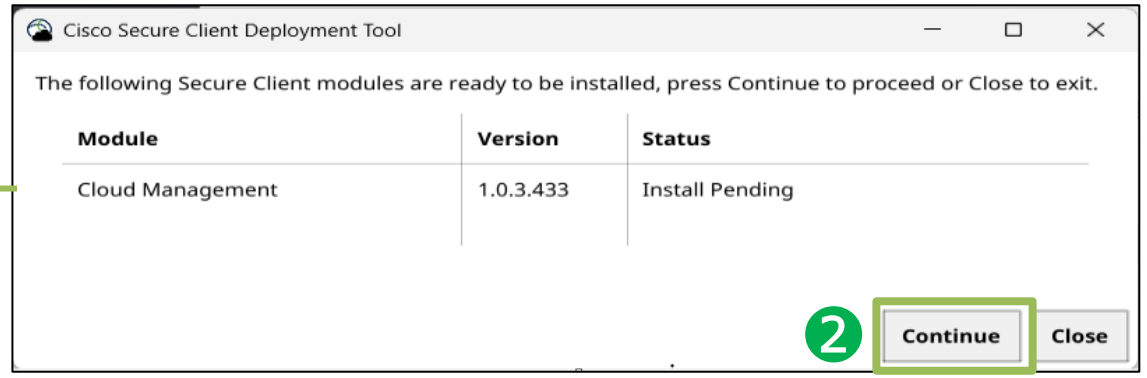
👆 対象のネットワークインストーラを実行
（csc-deploy-network-[契約ID]_[会社名].exeの実行）

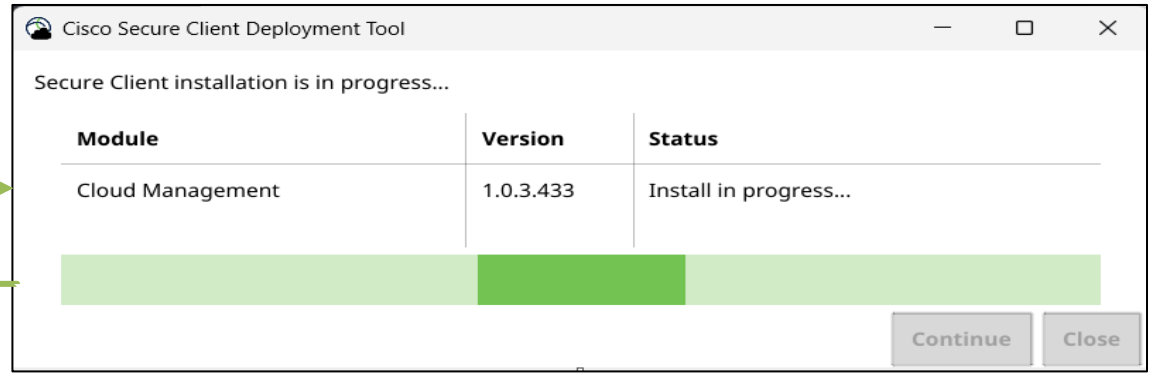


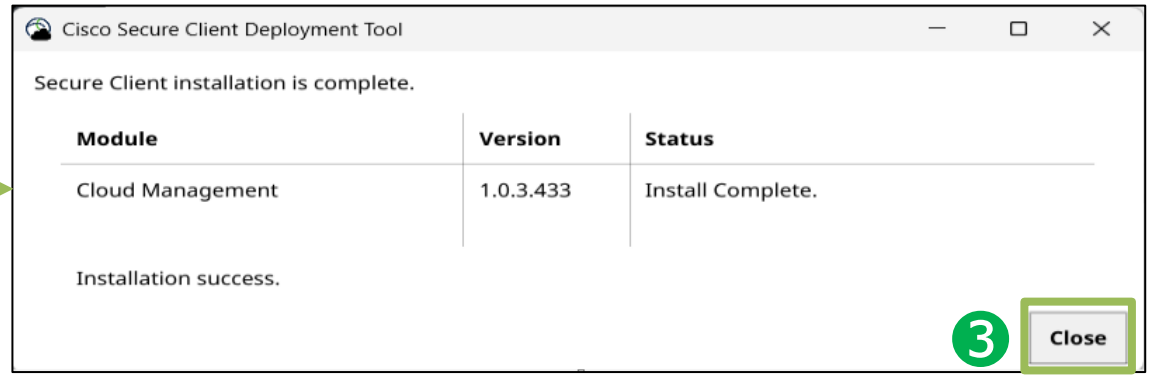
※契約IDは開通メールをご参照ください

1分程度待つ

👆 「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



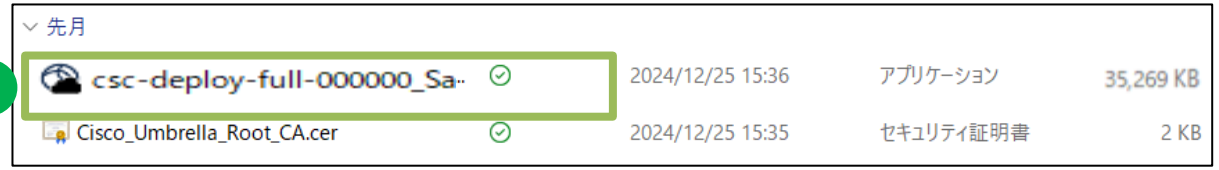




4-3. インストール手順 <ダウンロードしたインストーラの実行-3>

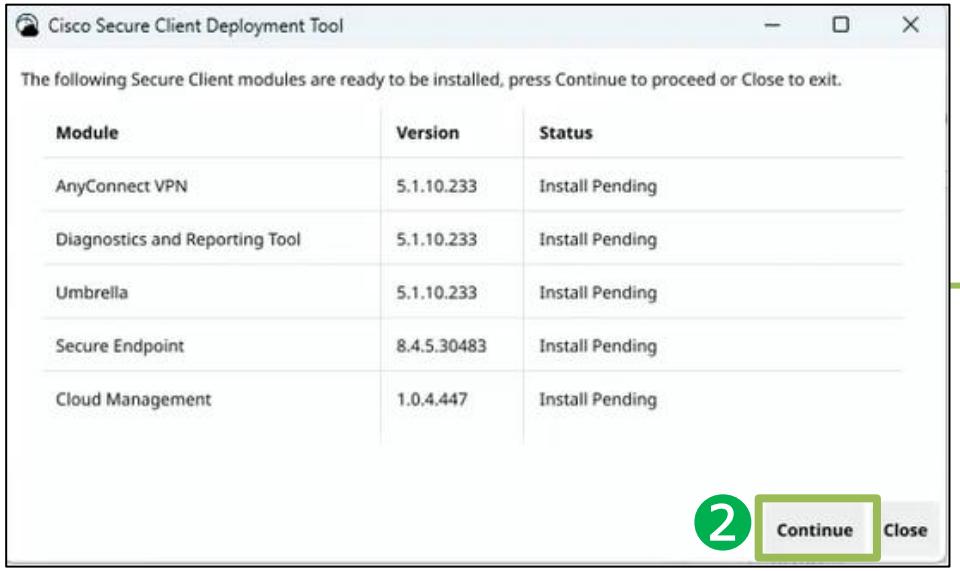
②以下画面になっている方（ファイルが「csc-deploy-full-000000_Sample Corporation.exe」となっている）

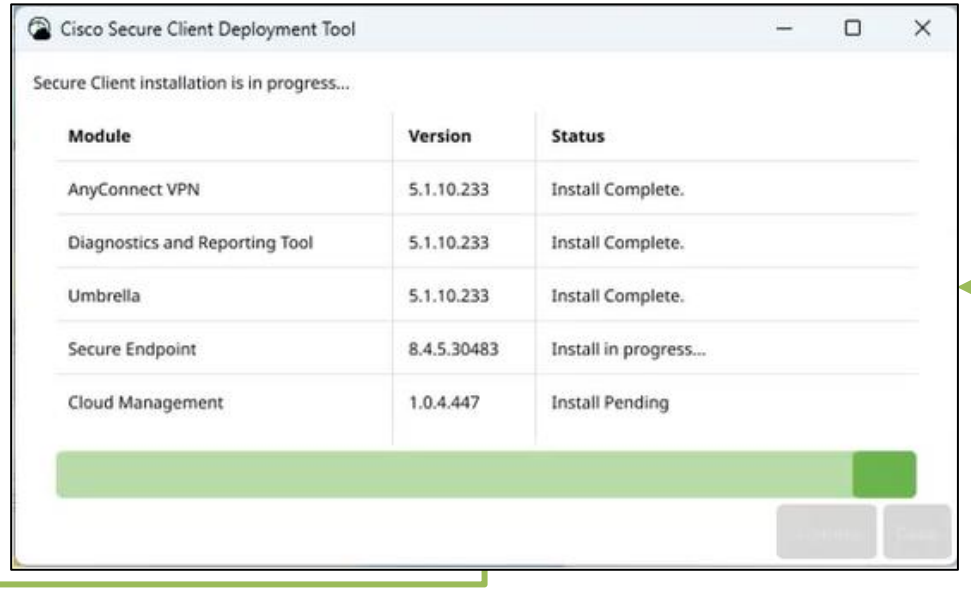
👆 対象のネットワークインストーラを実行
（csc-deploy-full-[契約ID]_[会社名].exeの実行）



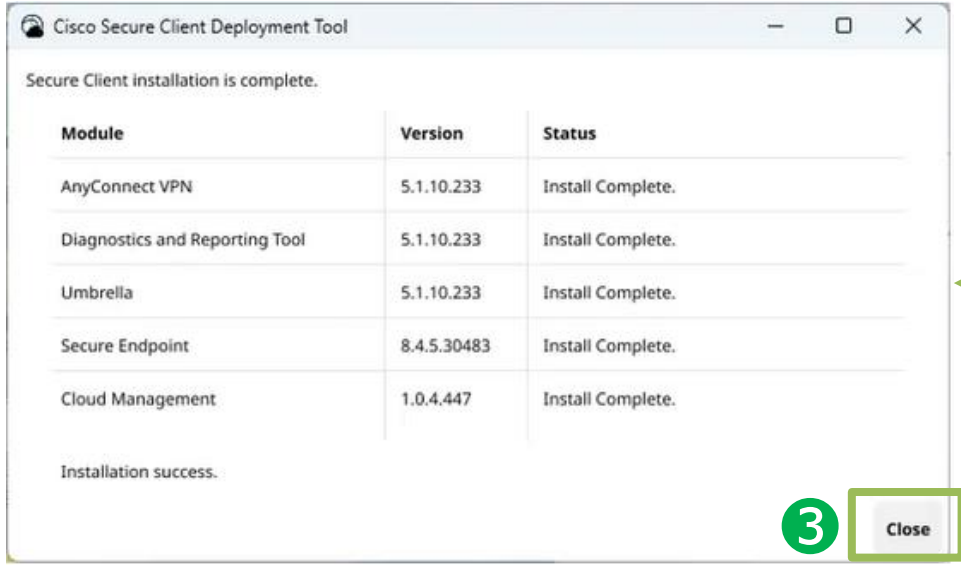
※契約IDは開通メールをご参照ください

👆 「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

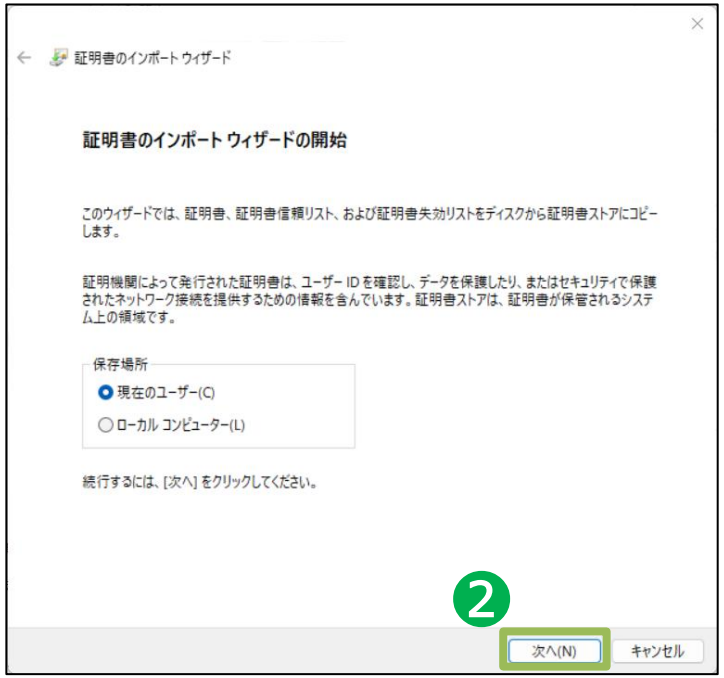


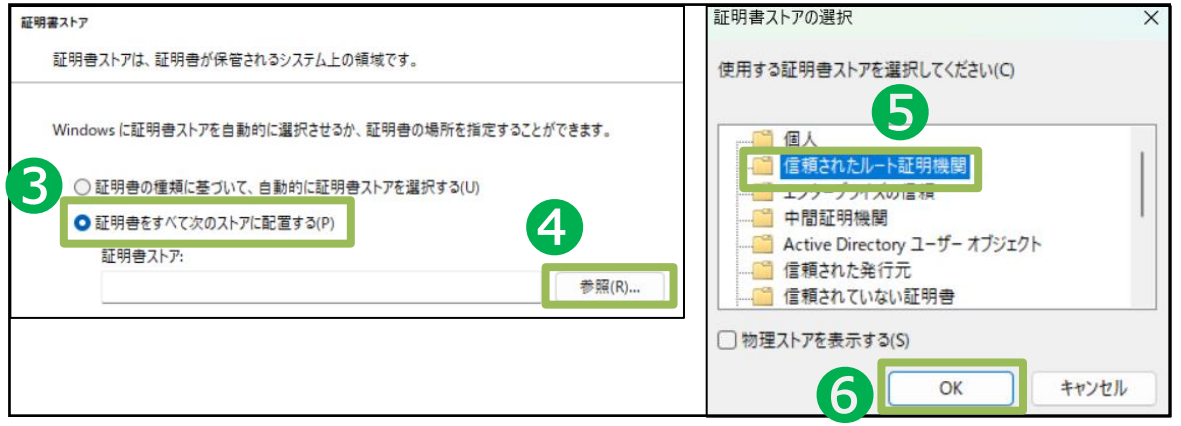
ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-1

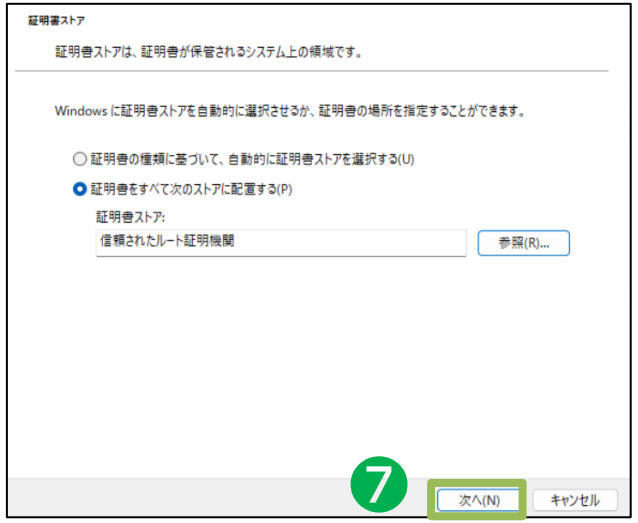
「証明書のインストール」を選択

「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

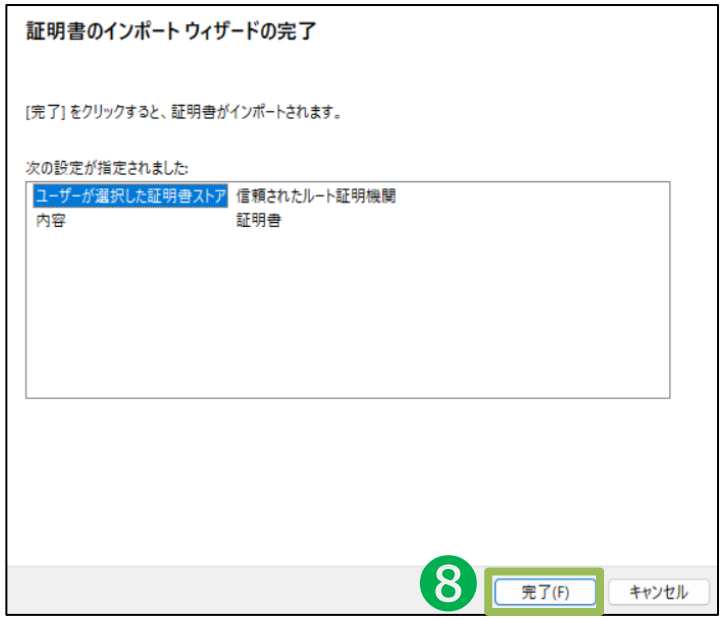






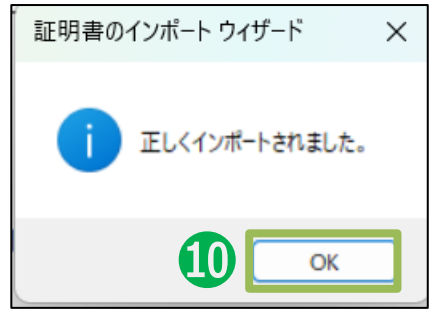
ルート証明書「Cisco_Umbrella_Root_CA.cer」のインポート手順-2

👆「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

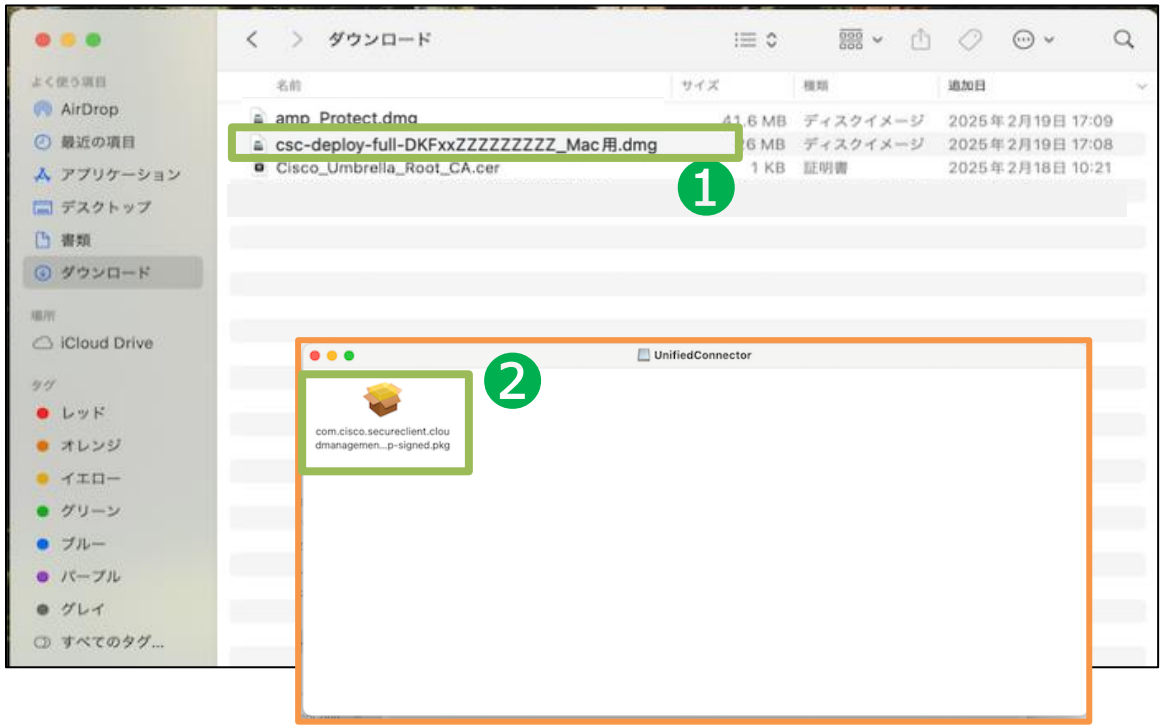
👆インポート完了



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>

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



👆「続ける」を選択

対象のインストーラについて　※契約IDは開通メールをご参照ください

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

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

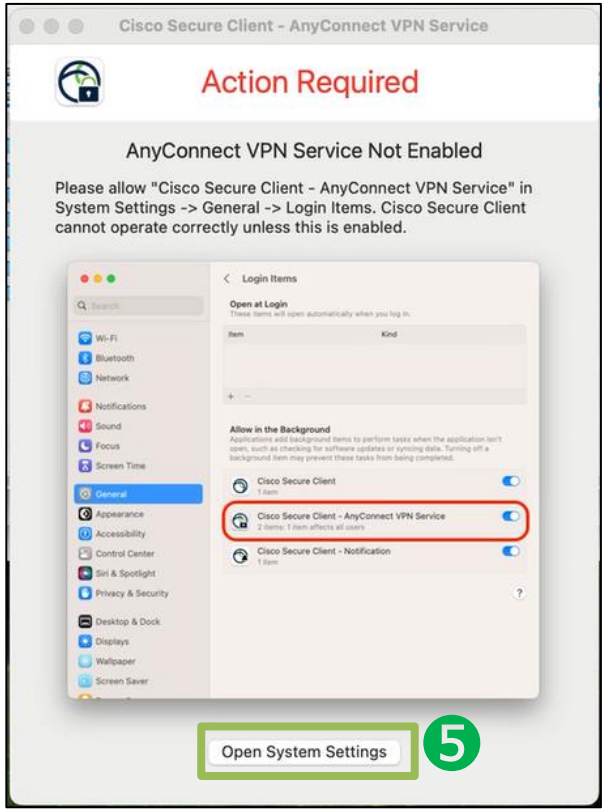
4-3. インストール手順 <ダウンロードしたインストーラの実行-2>

👆「インストール」を選択

4-3. インストール手順 <ダウンロードしたインストーラの実行-3>

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

👆「Open System Settings」をクリック



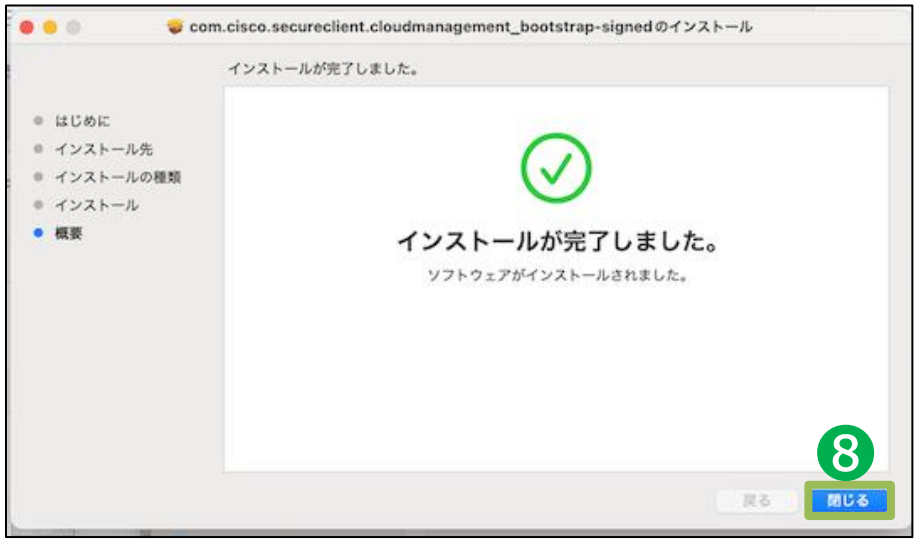
👆「Cisco Secure Client – AnyConnect VPN Service」を有効にする（※）

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

👆パスワードを入力し、「設定を変更」をクリック

4-3. インストール手順 <ダウンロードしたインストーラの実行-4>

👆「閉じる」を選択



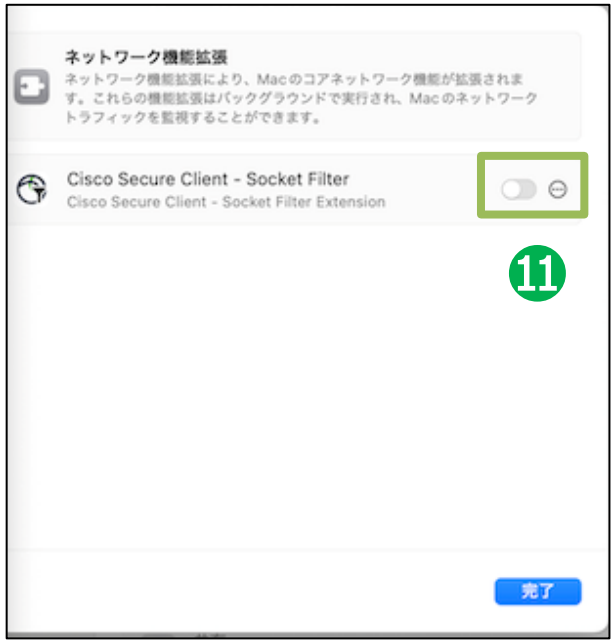
👆「ゴミ箱に入れる」を選択

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

4-3. インストール手順 <ダウンロードしたインストーラの実行-5>

👆「システム設定を開く」を選択

👆「Cisco Secure Client – Socket Filter」を有効化



👆「許可」を選択

👆「解散」を選択し、「完了」で設定画面を閉じる

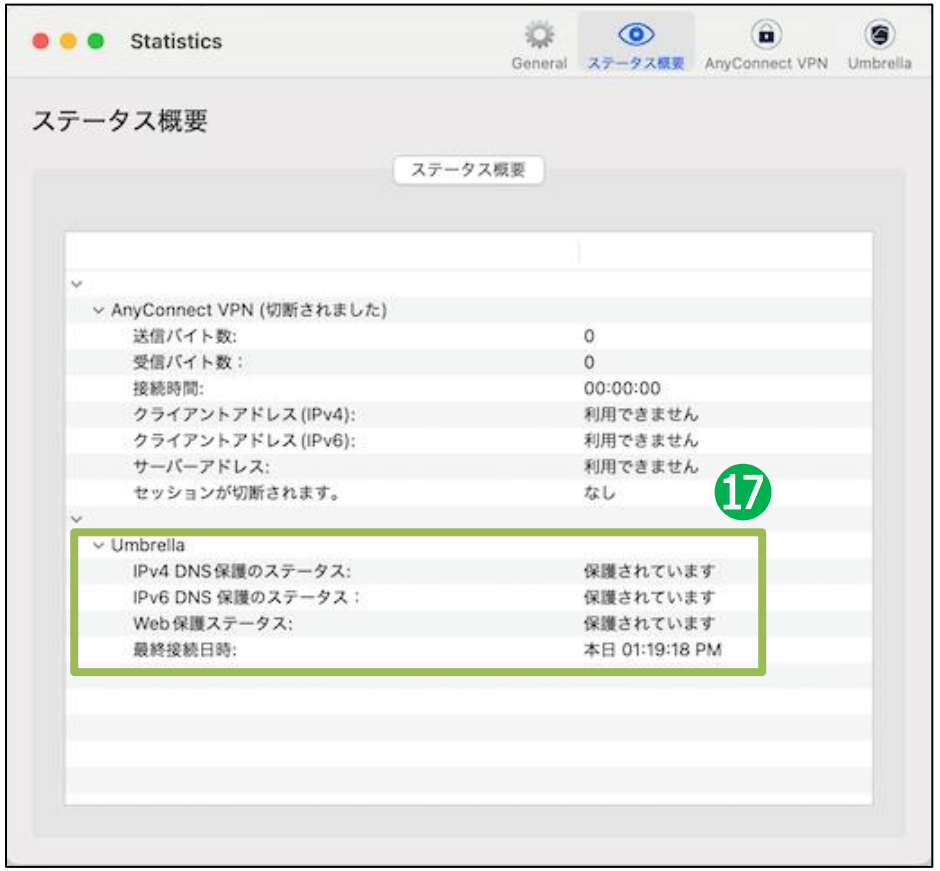
4-3. インストール手順＜ダウンロードしたインストーラの実行-6＞

👆「許可」を選択

👆「Statistics」を選択

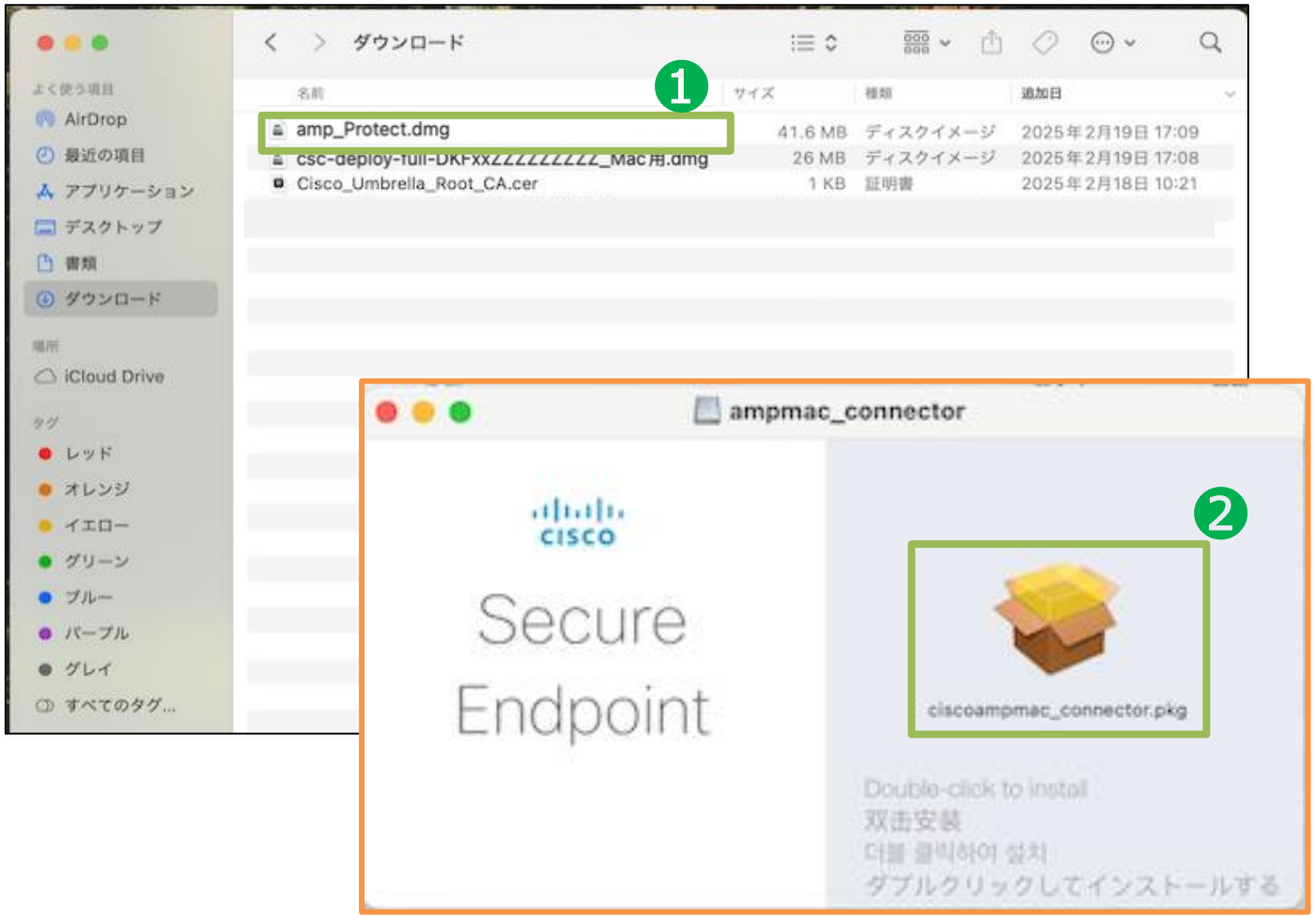
Cisco Secure Clientが自動で起動しない場合は
「Finder」>「アプリケーション」>
「Cisco」フォルダ>「Cisco Secure Client」を実行する

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

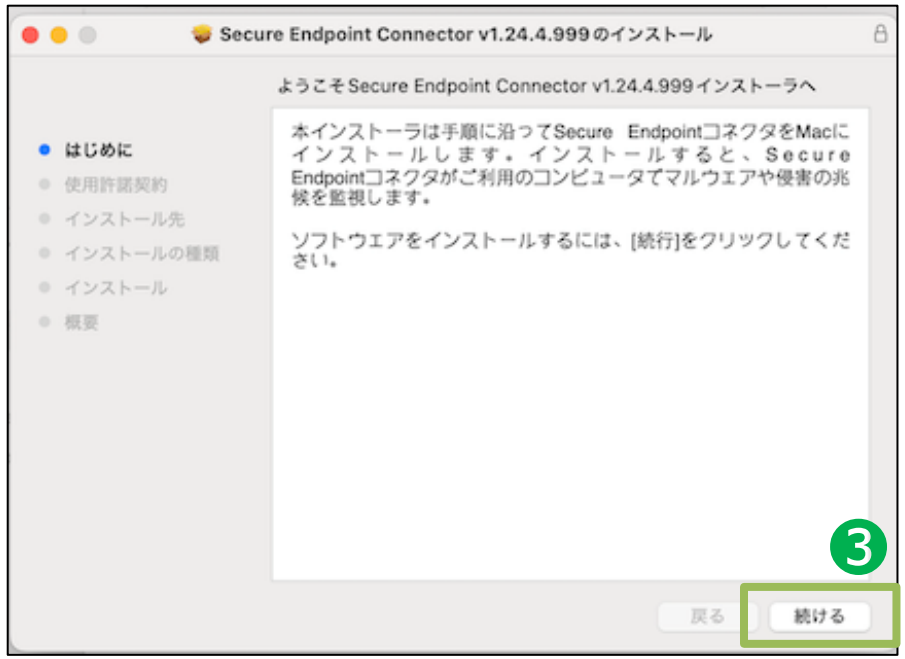


CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-1

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



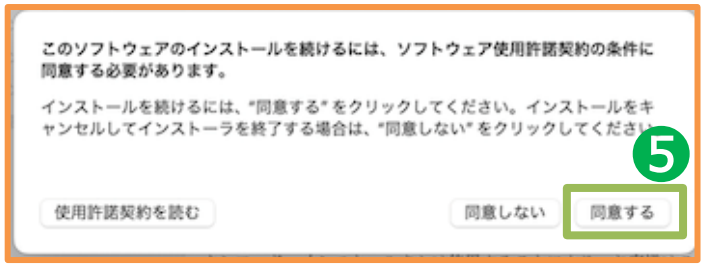
👆「続ける」を選択



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

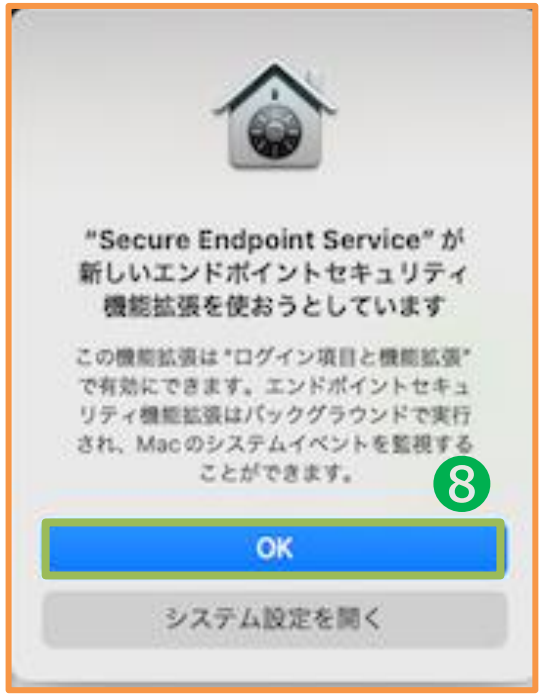


👆「続ける」を選択

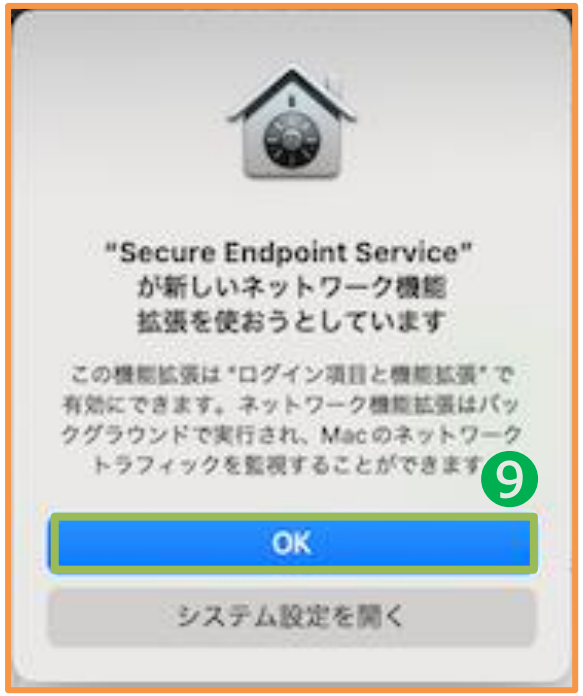
CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-3

👆「インストール」を選択

👆「OK」を選択

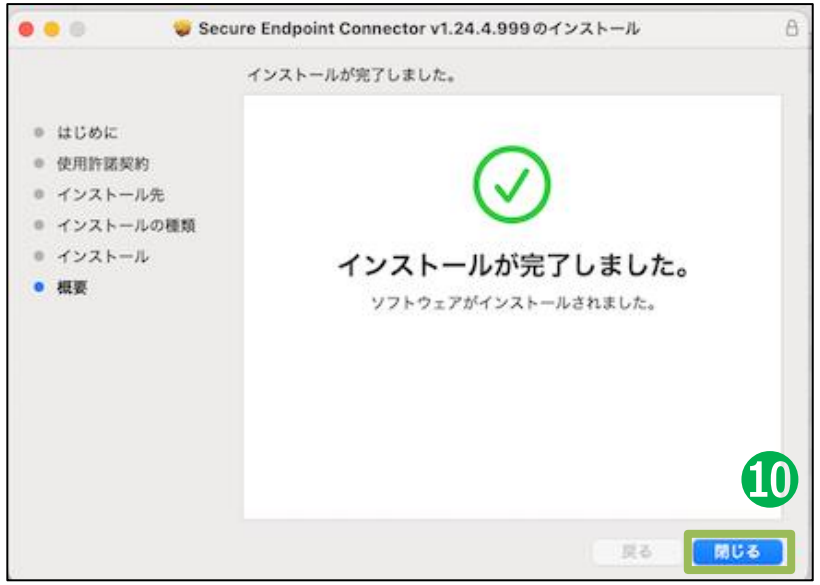


👆「OK」を選択



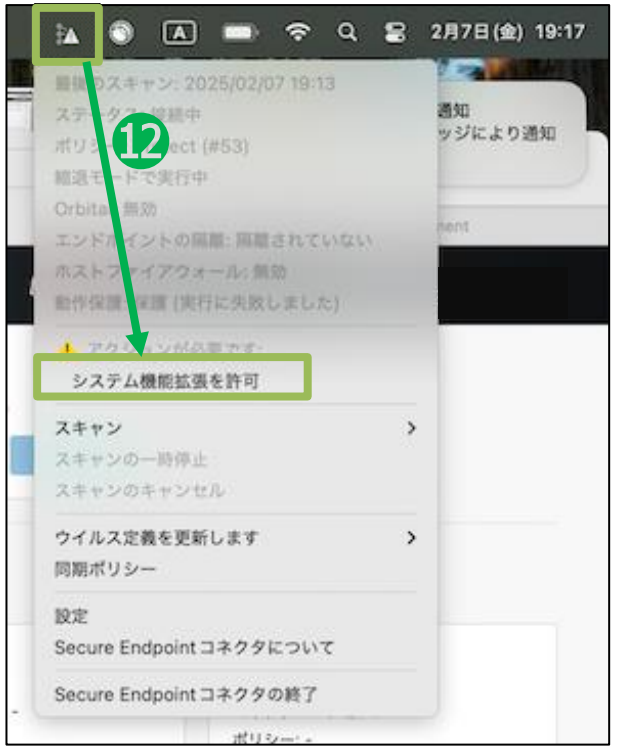
CSEコネクタモジュール「amp_Protect.dmg」のインストール手順-4

👆「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

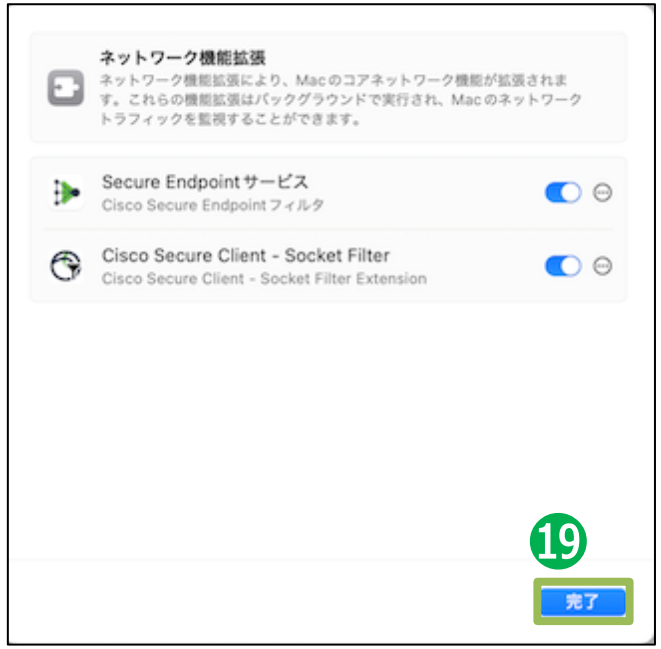
👆「完了」を選択

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

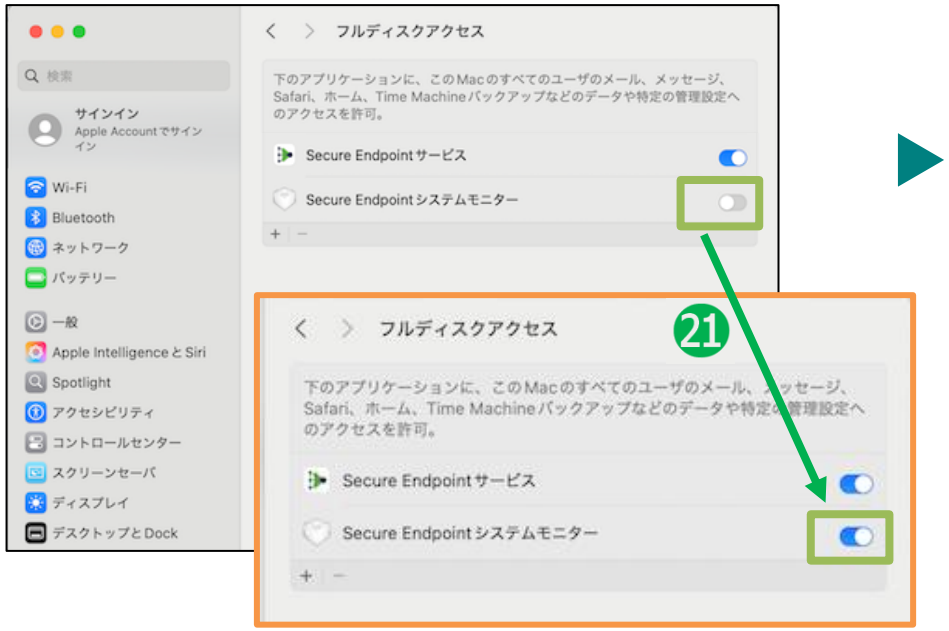
👆「完了」を選択



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

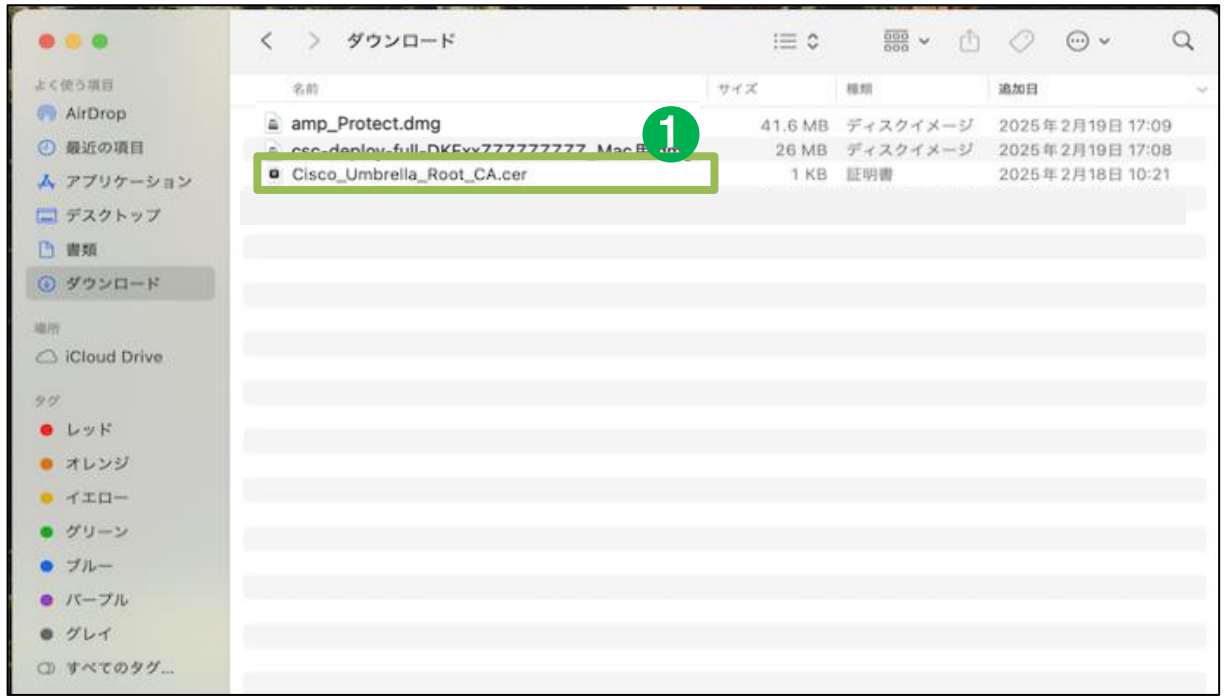
👆「Secure Endpointシステムモニター」を有効化



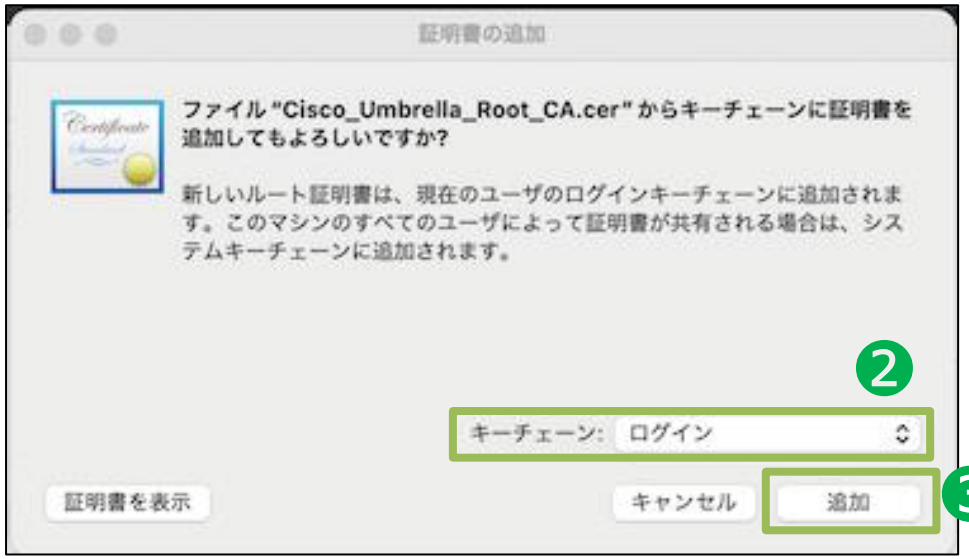
👆追加アクション要求「 」がなくなっていることを確認

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



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

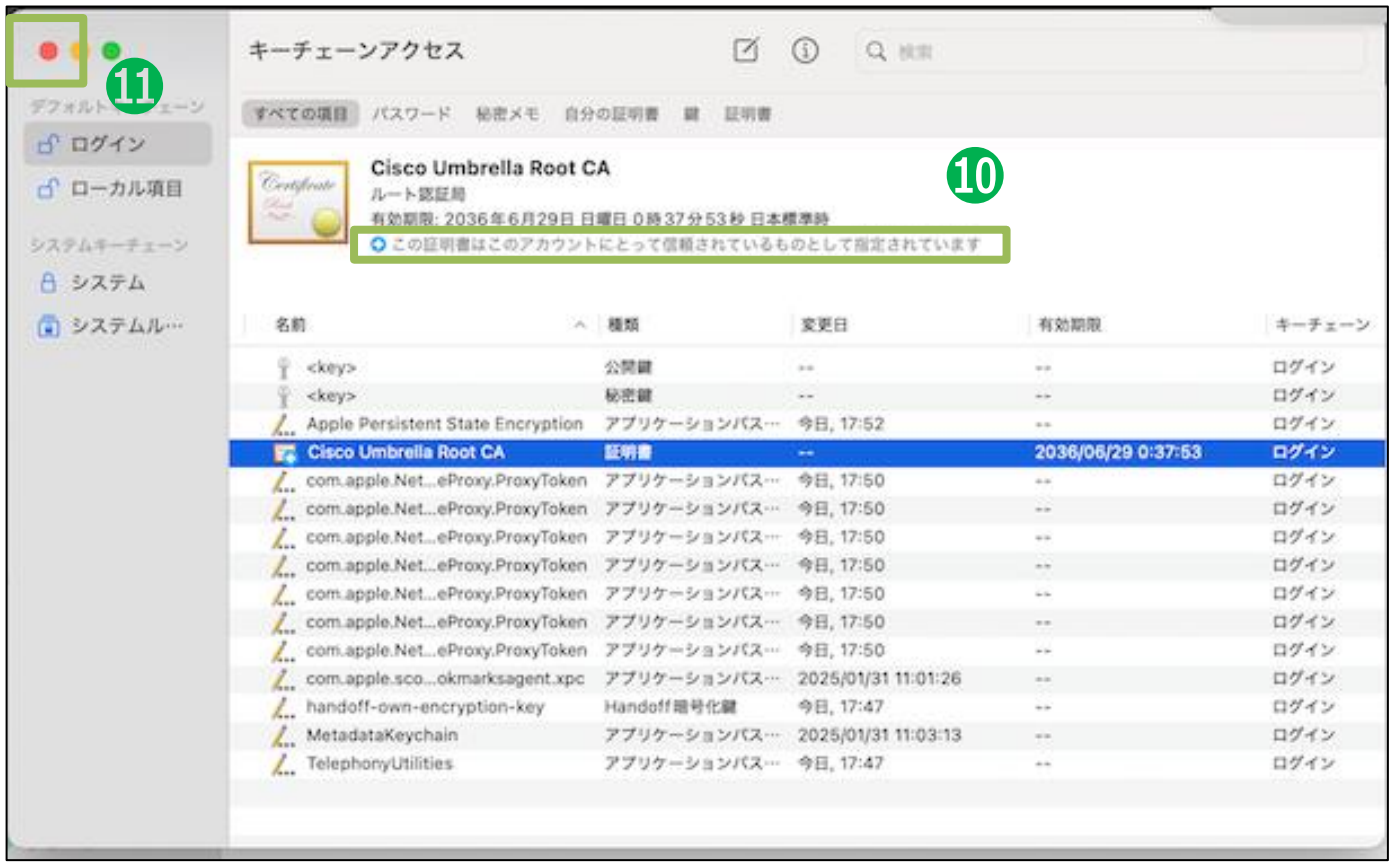
👆証明書が信頼されていないことを確認し、
インポートした「Cisco Umbrella Root CA」をダブルクリック
（既に信頼済みであればルート証明書のインポートは完了）

👆「信頼」のプルダウンを開く

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

👆「この証明書を使用するとき」を「常に信頼」に変更

👆信頼されているものとして指定されていることを確認し、
画面を閉じる

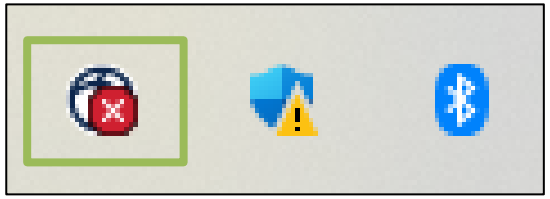


4-4. ソフトウェアの起動／ステータス確認_Windows

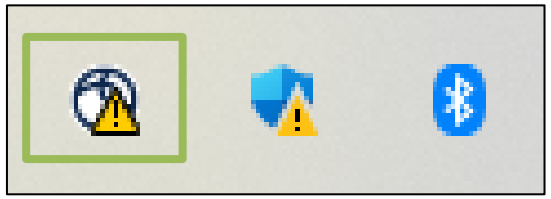
4-4. インストール手順＜ソフトウェアの起動／ステータス確認-1＞

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

①初期設定中

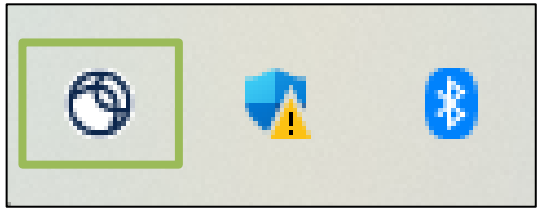


または



5分程度
待機

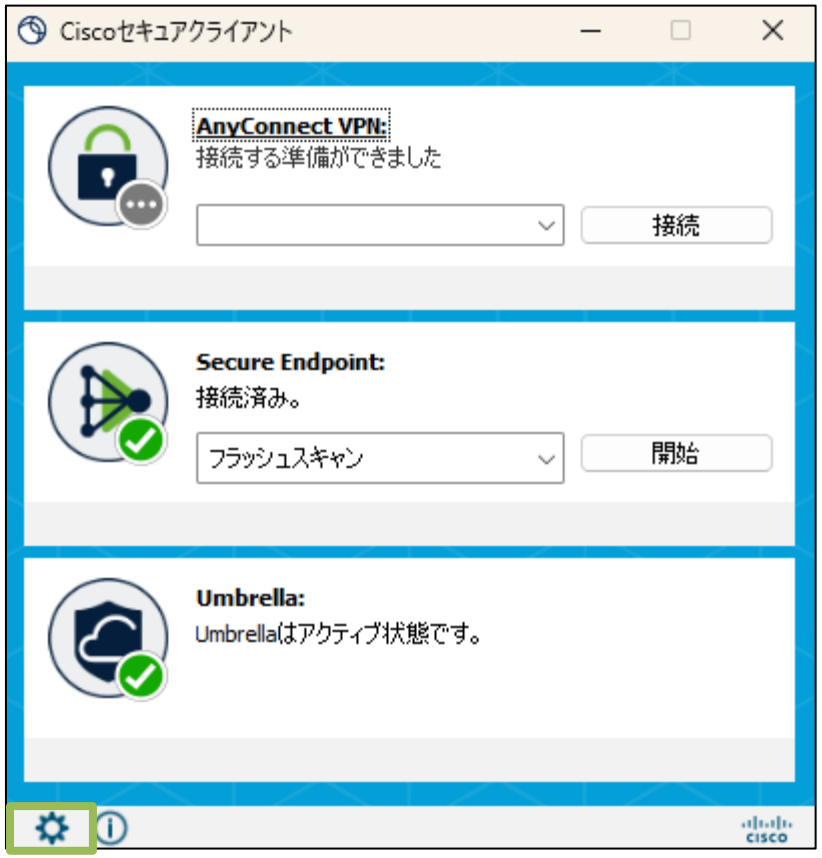
②初期設定完了



👆初期設定完了状態でクリック

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

③セキュアクライアントホーム画面



👆④各アプリの詳細は次ページ

4-4. インストール手順 <ソフトウェアの起動／ステータス確認-2>

⑤「Secure Endpoint」を選択し、「エージェント※」のステータスが「接続中」であることを確認
※エージェント：ソフトウェアエージェント。ここではSecureEndpoint等のクライアントに常駐するソフトウェアを意味します。
⑥「Umbrella」を選択し、「DNS/IPセキュリティ情報」のステータスが「保護されています」、暗号化が「オン」であることを確認
「セキュアWebゲートウェイ」のライセンスが「有効」、Web保護ステータスが「保護されています」であることを確認

⑤Secure Endpointステータス情報

⑥Umbrellaステータス情報

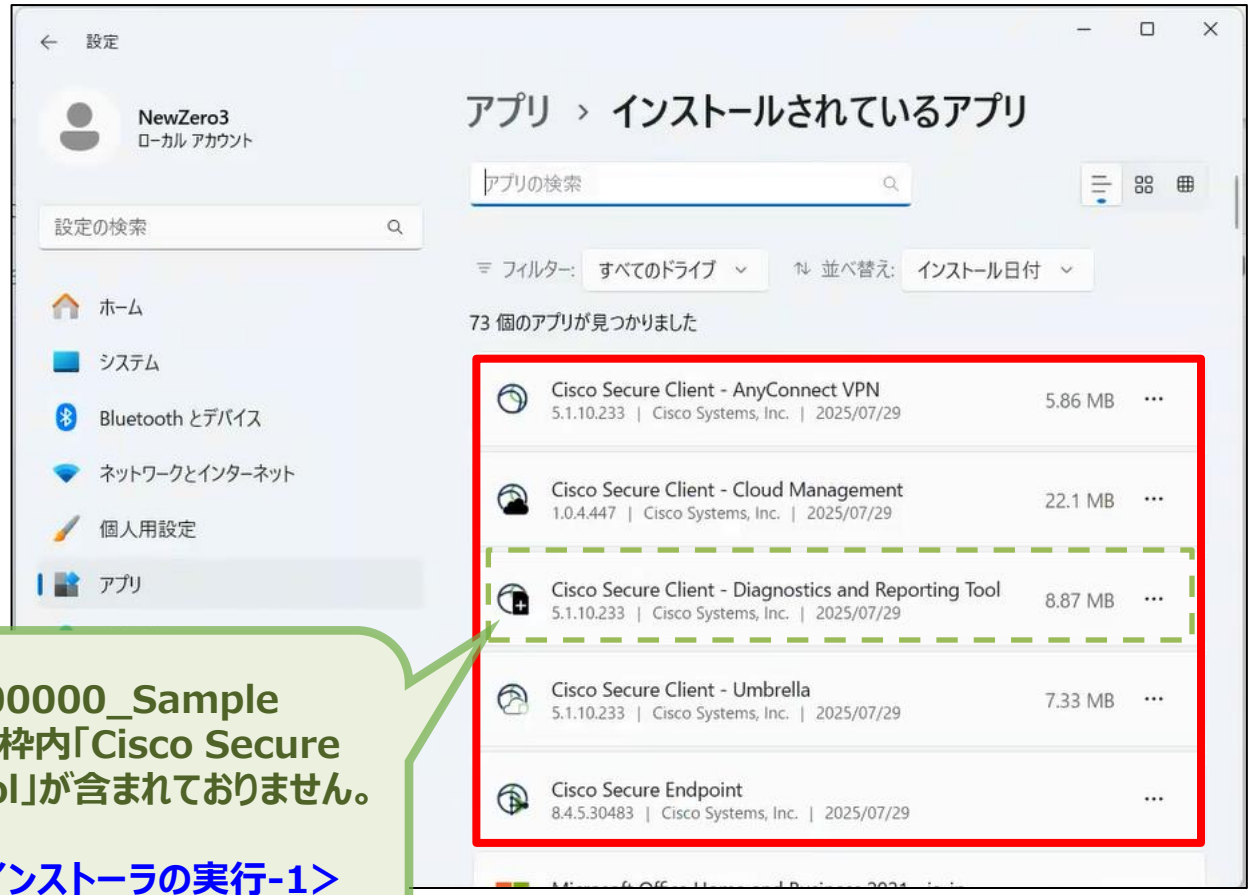
4-4. インストール手順 <ソフトウェアの起動／ステータス確認-3>

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

⑦アプリ画面の起動

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

⑧インストールされているアプリの確認



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

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

4-4. ソフトウェアの起動／ステータス確認_Mac

4-4. インストール手順＜ソフトウェアの起動／ステータス確認-1＞

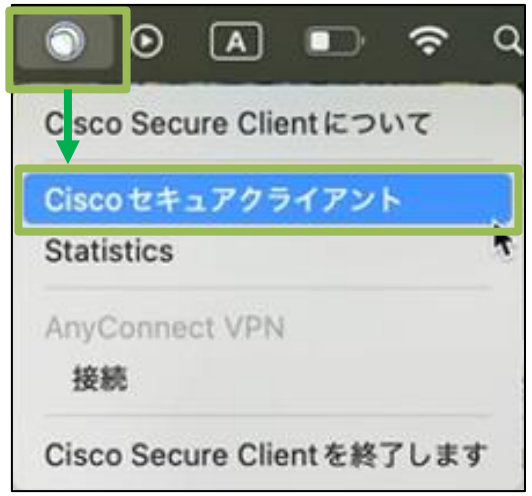
①インストール時の初期設定が完了後、画面右上の「Ciscoセキュアクライアント」アイコンが初期設定中となる
②「Ciscoセキュアクライアント」のアイコンを選択
③「Ciscoセキュアクライアント」を選択
④Umbrellaのステータスがアクティブとなっていることを確認

①初期設定中

②初期設定完了

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

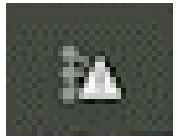


④セキュアクライアントホーム画面

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



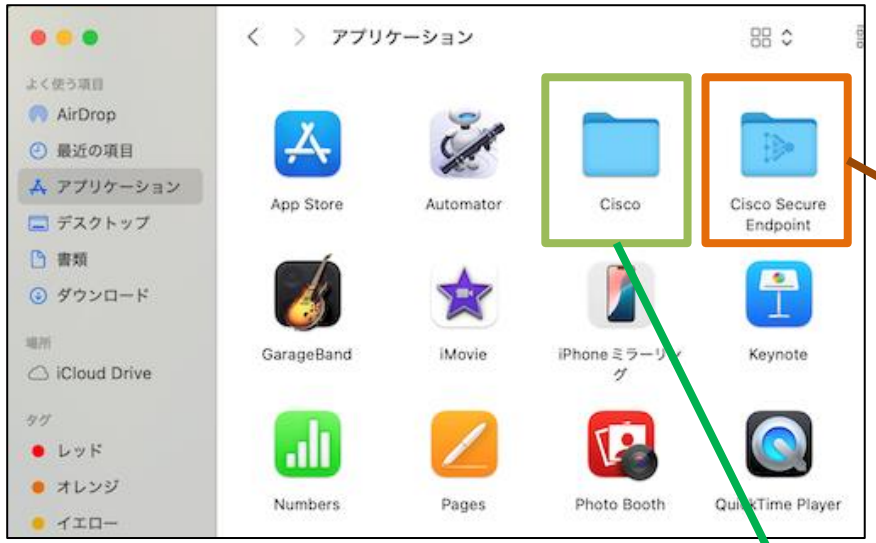
⑥初期設定完了

インストール設定後
自動遷移

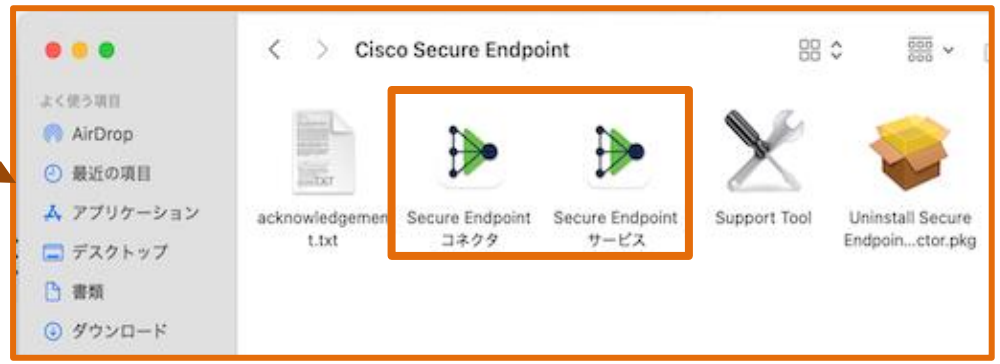
⑦セキュアエンドポイントステータス

4-4. インストール手順 <ソフトウェアの起動／ステータス確認-3>

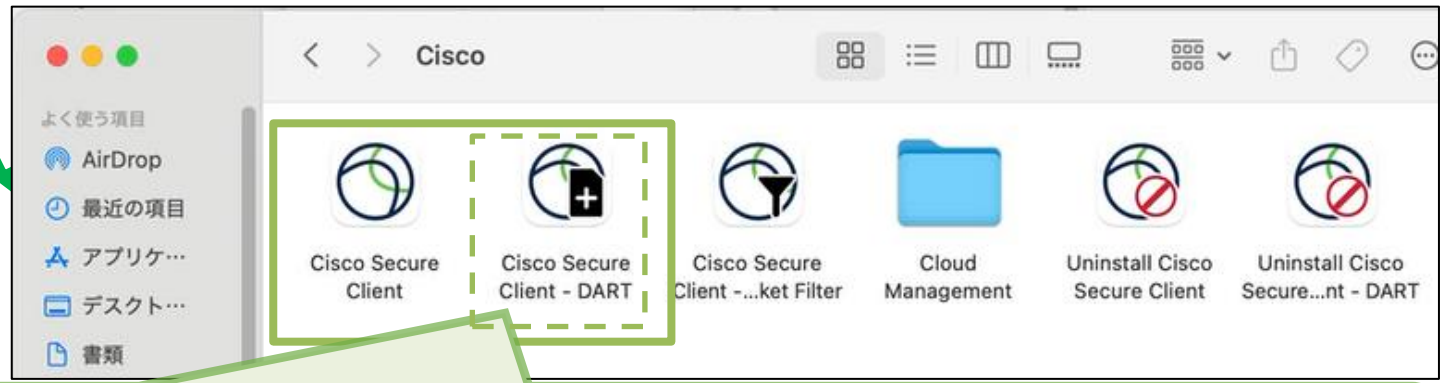
⑧Finderから「Cisco」、「Cisco Secure Endpoint」フォルダを開き、「Secure Endpoint コネクタ」、「Secure Endpointサービス」、「Cisco Secure Client」、「Cisco Secure Client-DART（※）」がインストールされていることを確認



👇⑧Cisco Secure Endpoint



👇⑧Cisco Secure Client(Umbrella)



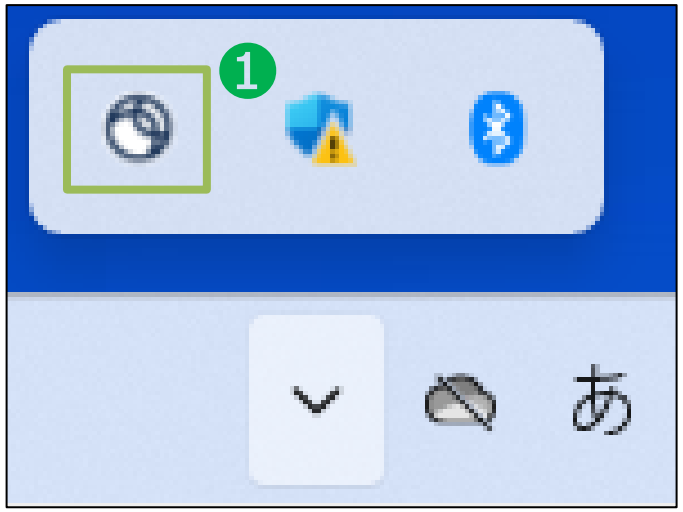
※インストーラが①「csc-deploy-network-[契約ID]_[会社名]_Mac用.dmg」となっている方は、「Cisco Secure Client – DART」が含まれておりません。
参照：4-3. インストール手順 <ダウンロードしたインストーラの実行-1>

5. ソフトウェアのアンインストール手順_Windows

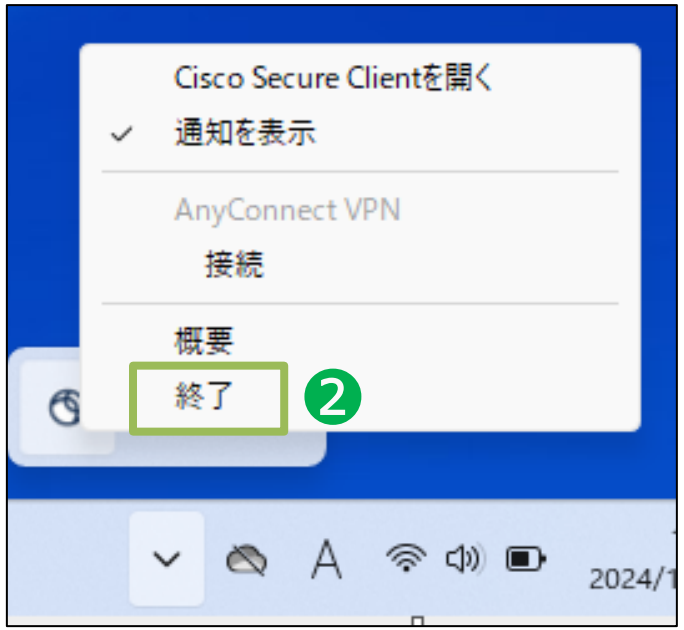
5. アンインストール手順＜Cisco Secure Clientの停止-1＞

実行中のCisco Secure Clientを停止させてください。

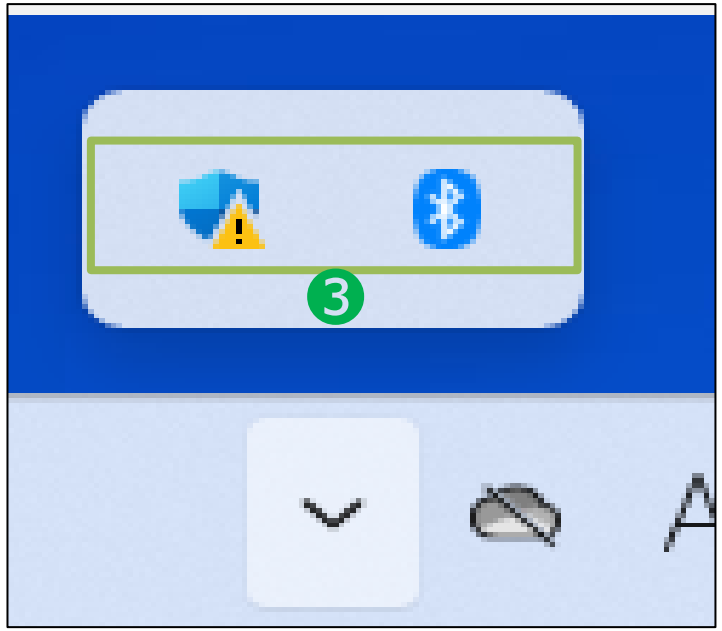
タスクバーから「Cisco Secure Client」を右クリック



「Cisco Secure Client」を終了させる



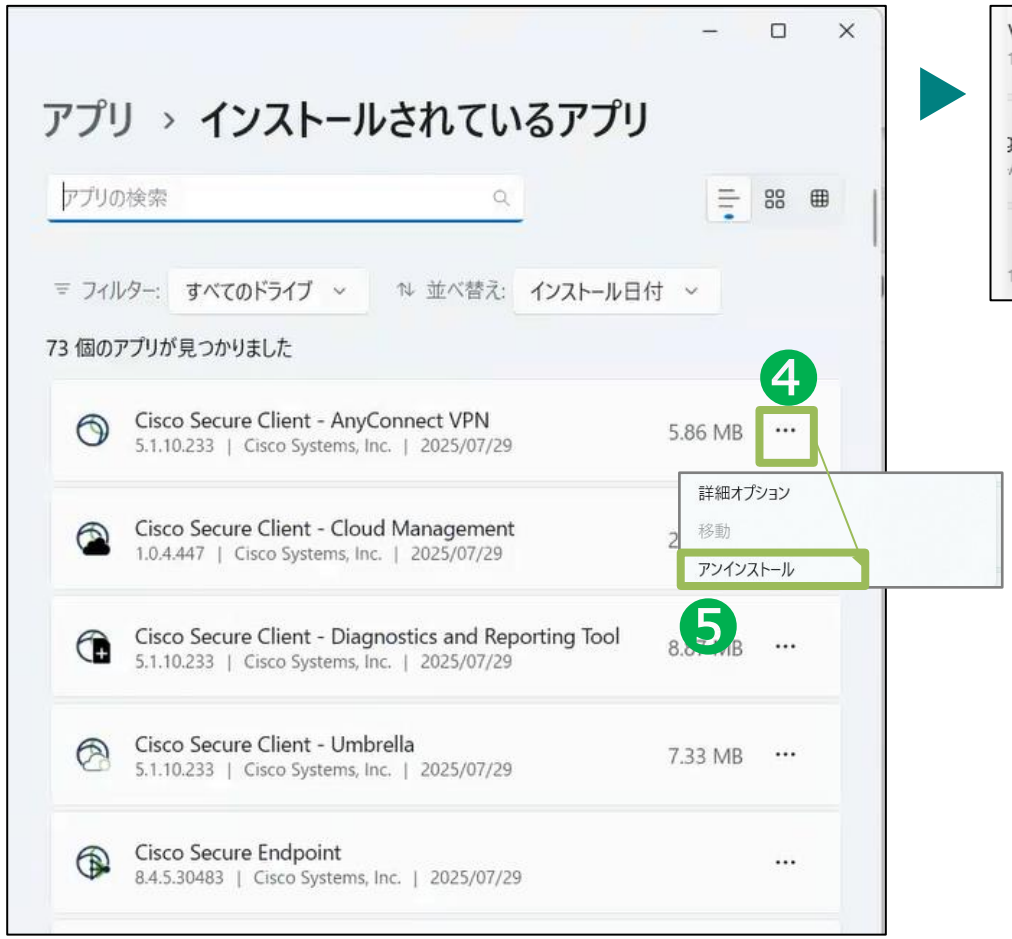
タスクバーから「Cisco Secure Client」が消えていることを確認する



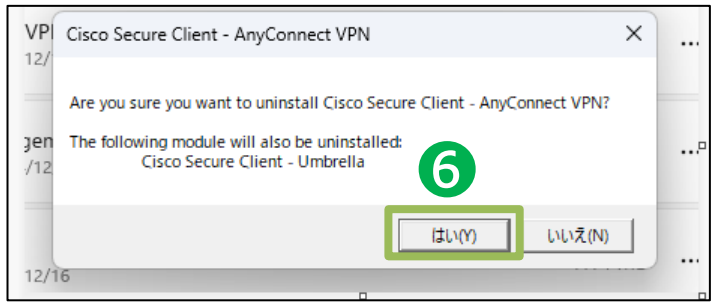
5. アンインストール手順 <ソフトウェアのアンインストール-1>

手順に従ってソフトウェアをアンインストールしてください。

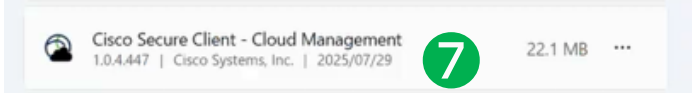
「Windows」→「設定」→「アプリ」→「インストールされているアプリ」を開き、「Cisco Secure Client – AnyConnect VPN」をアンインストール



依存関係にあるUmbrellaも削除するか聞かれるので「はい」を選択



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



5. アンインストール手順 <ソフトウェアのアンインストール-2>

続けてソフトウェアをアンインストールしてください。

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

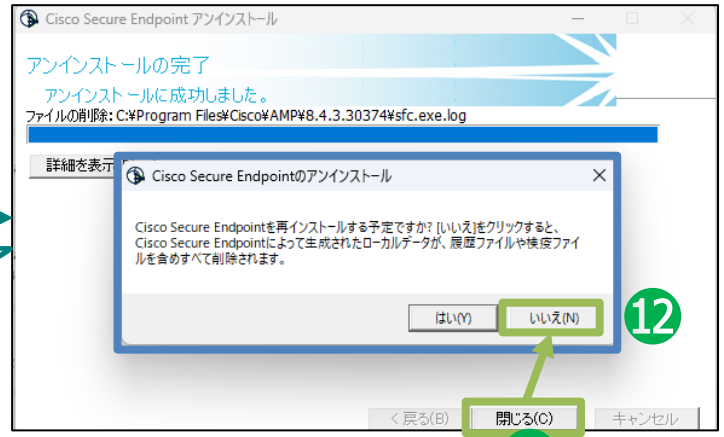
※インストーラが、
①「csc-deploy-network-000000_Sample Corporation.exe」となっている場合、上記アプリはございません。

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

「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

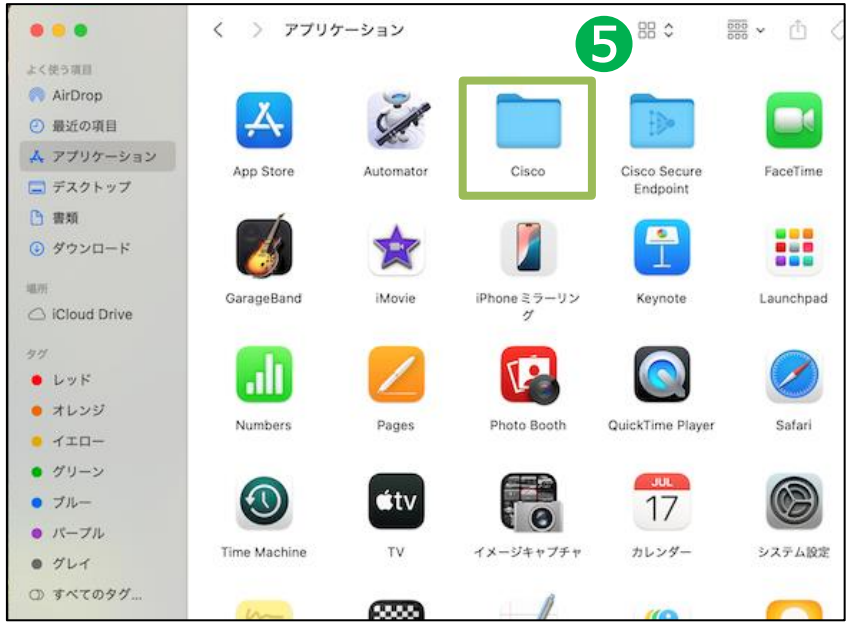
画面右上の
「Secure Endpointコネクタ」を
クリックし、終了させる

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

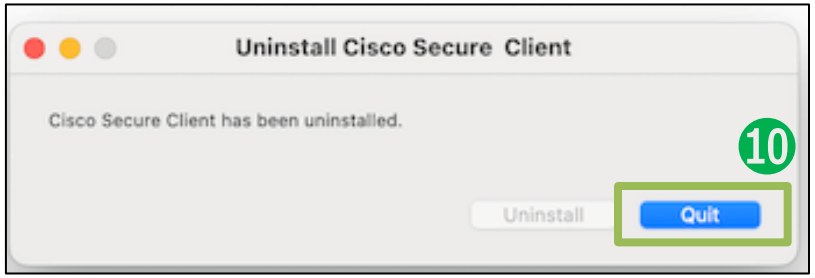
5. アンインストール手順 <ソフトウェアのアンインストール-2>

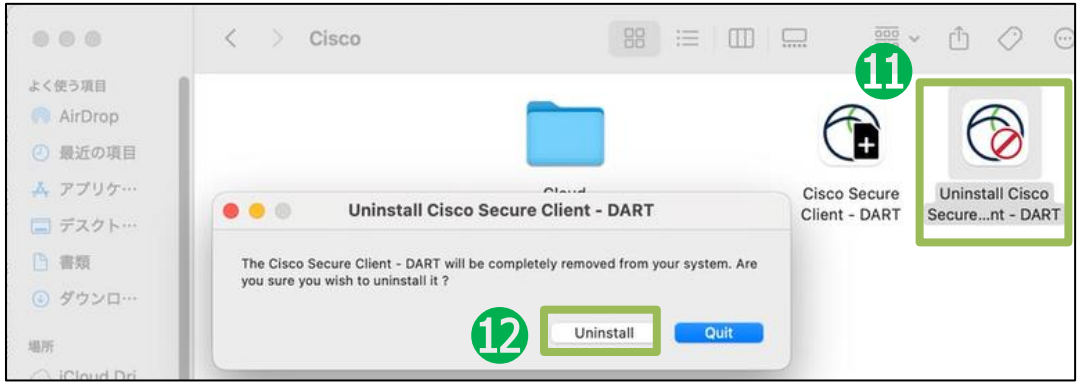
手順に従ってソフトウェアをアンインストールしてください。

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

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





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

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

5. アンインストール手順 <ソフトウェアのアンインストール-3>

手順に従ってソフトウェアをアンインストールしてください。

続けてパスワードを入力し「OK」を選択

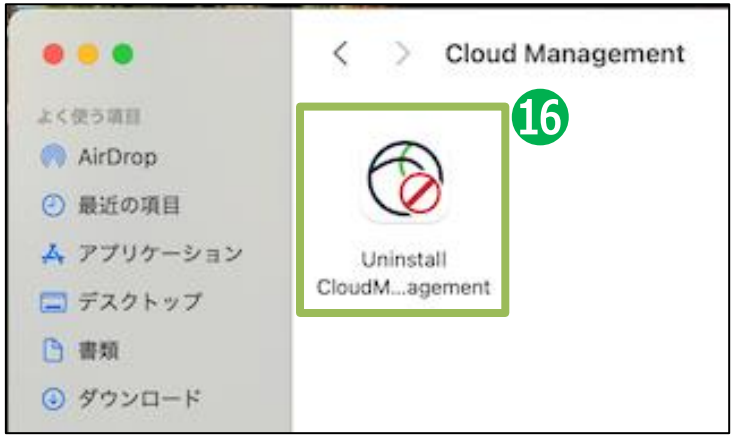
「Quit」を選択して閉じる

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

5. アンインストール手順 <ソフトウェアのアンインストール-4>

手順に従ってソフトウェアをアンインストールしてください。

「Uninstall CloudManagement」をダブルクリック



パスワードを入力し、「OK」を選択

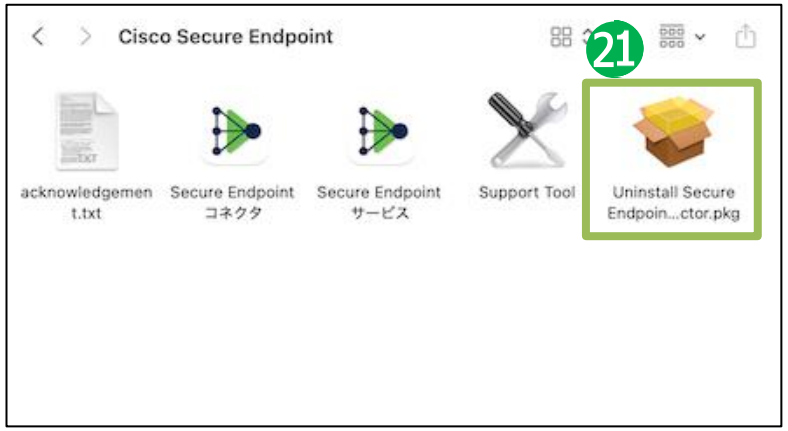
「OK」を選択

5. アンインストール手順 <ソフトウェアのアンインストール-5>

手順に従ってソフトウェアをアンインストールしてください。

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

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

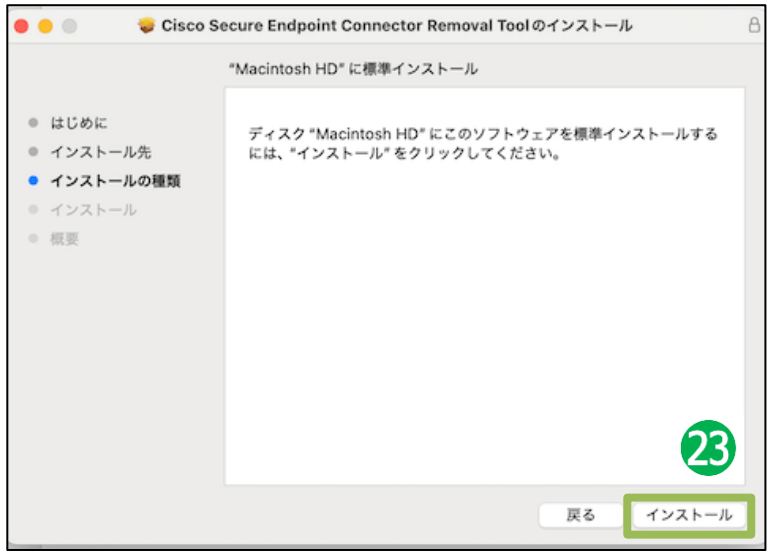


「続ける」を選択

5. アンインストール手順 <ソフトウェアのアンインストール-6>

手順に従ってソフトウェアをアンインストールしてください。

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



パスワードを入力し、
「ソフトウェアをインストール」を選択

24

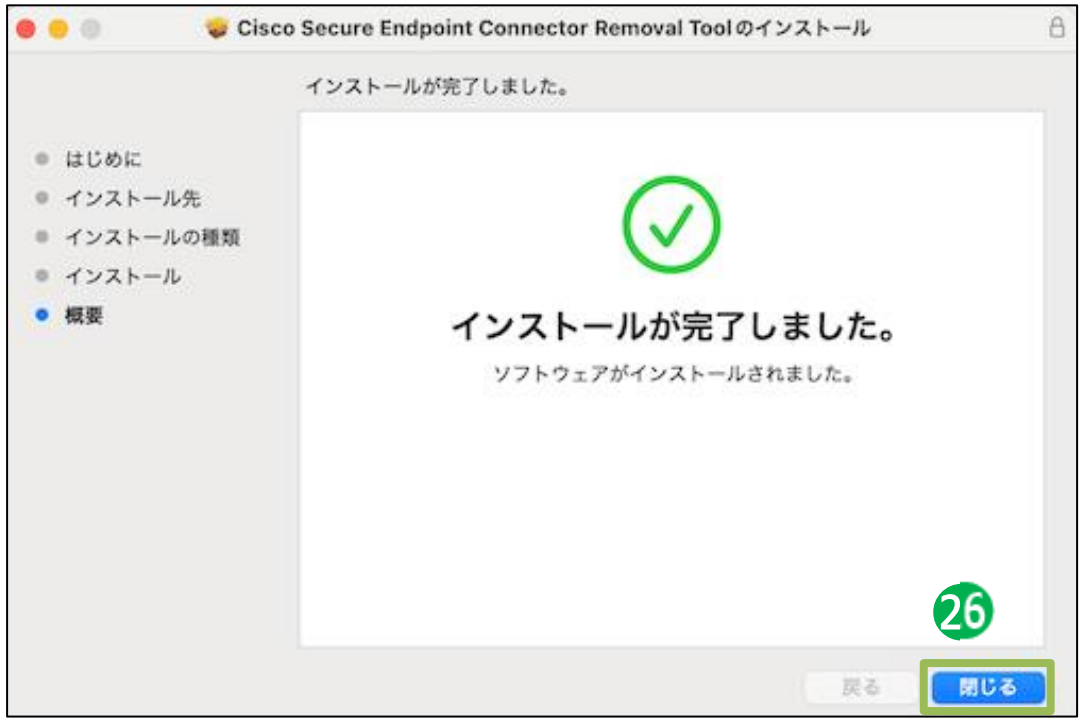
続けて、パスワードを入力し、
「OK」を選択

25

5. アンインストール手順 <ソフトウェアのアンインストール-7>

手順に従ってソフトウェアをアンインストールしてください。

「閉じる」を選択



アプリケーションフォルダに戻り、
不要な「Cisco」フォルダを削除

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

6. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

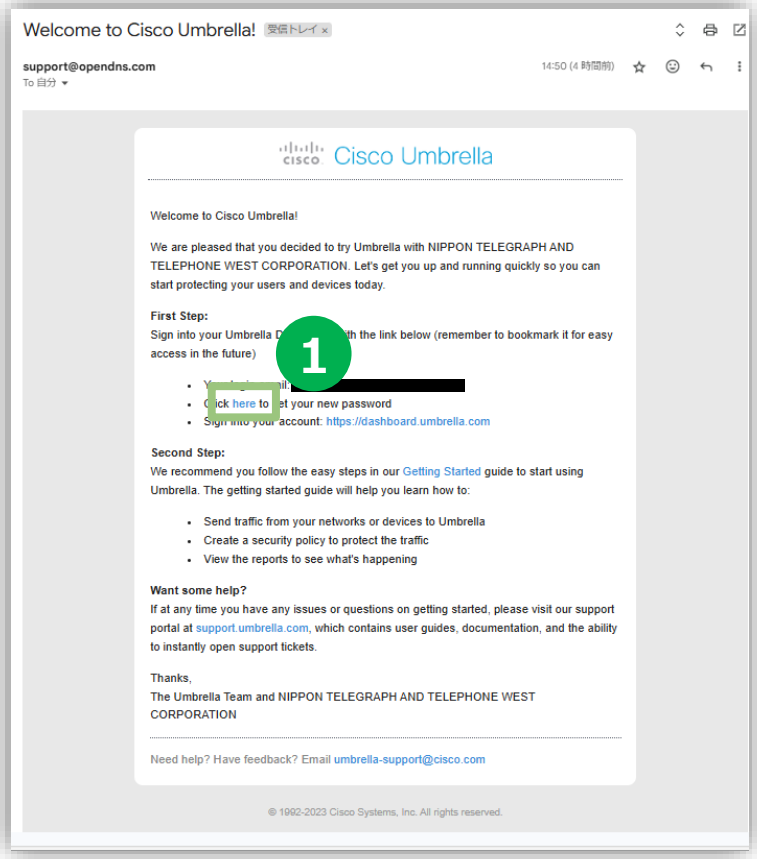
管理者向けのインビテーションメールを受信してから管理コンソール ログインまでの手順を記載します。

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

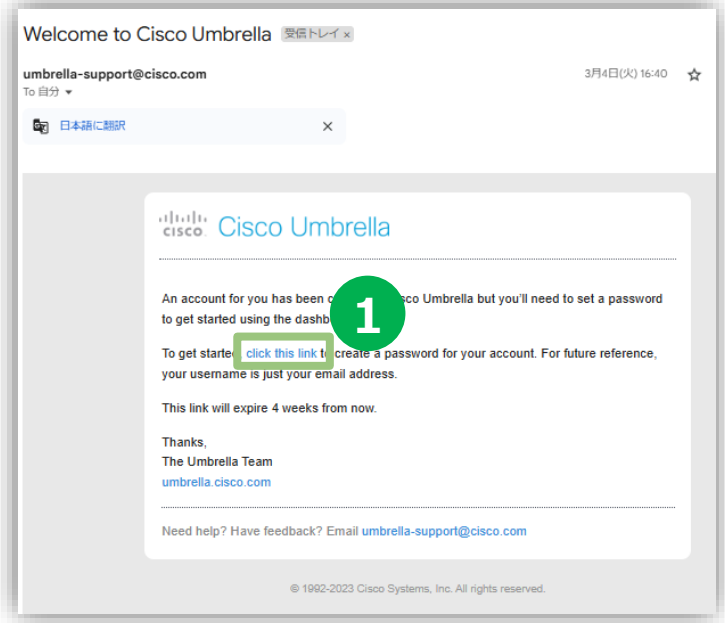
② [氏名]、[電子メール※1]、[パスワード※2]を入力
　※1電子メールには申込書に記載したメールアドレスを記載ください　※2設定するパスワードには条件があります（図の②下部をご参照ください）

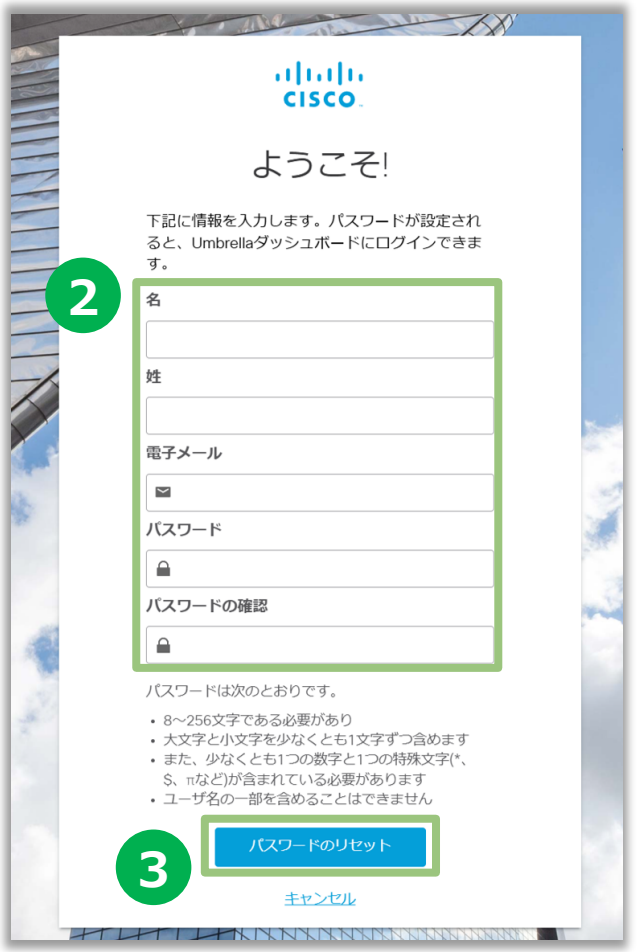
③ [パスワードのリセット]をクリック

1人目の管理者



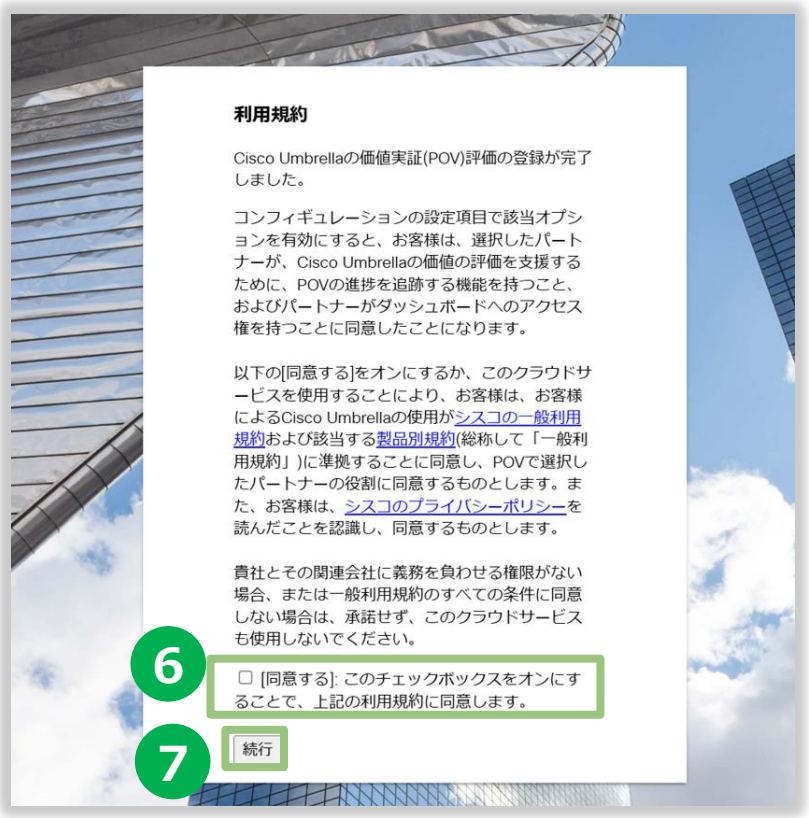
2人目の管理者





6. コンソールへのログイン手順 <管理者アカウント 初回ログイン>

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



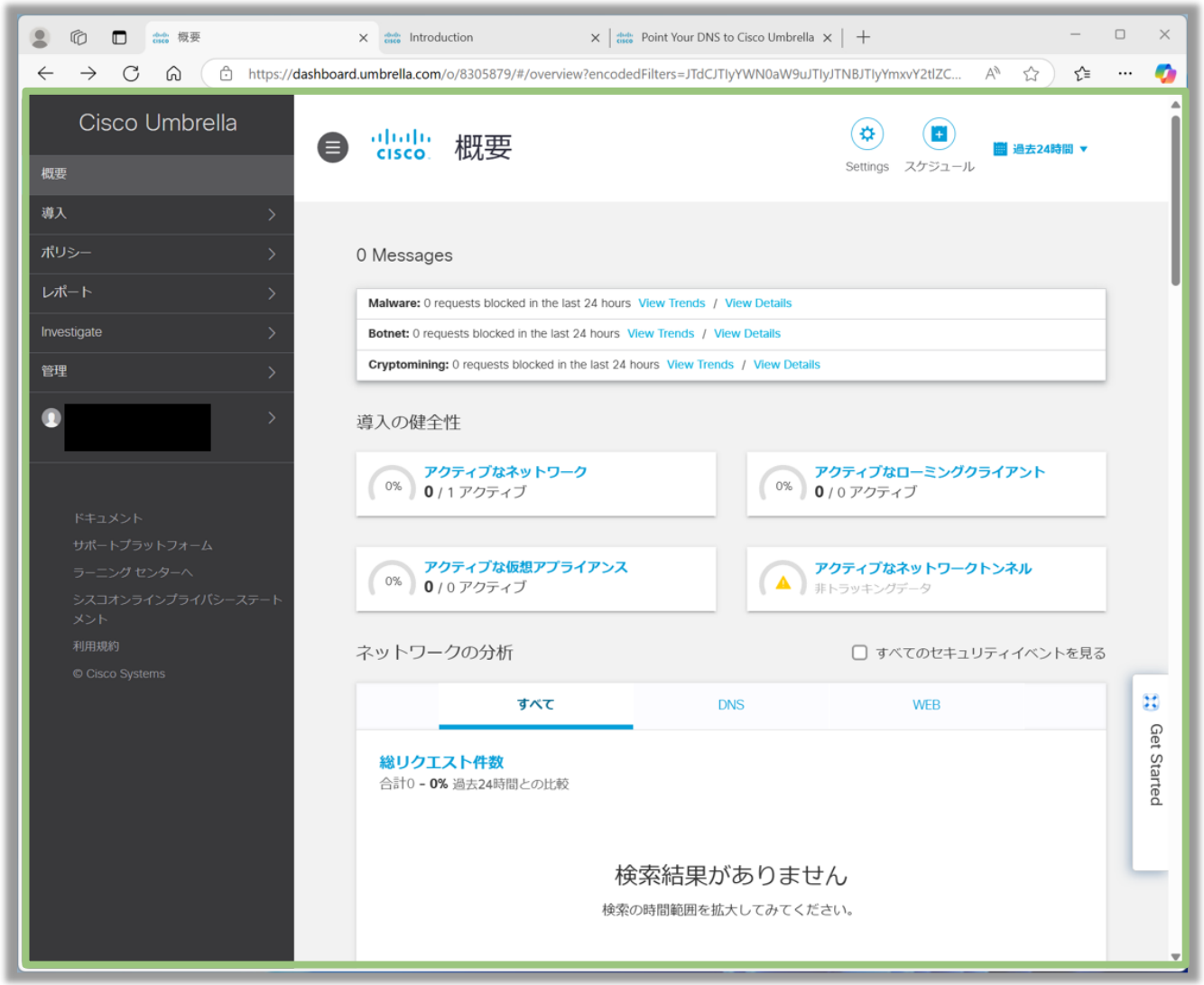
6. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

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

6. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

⑪ ログインに成功するとUmbrellaのトップ画面が表示されます。

11

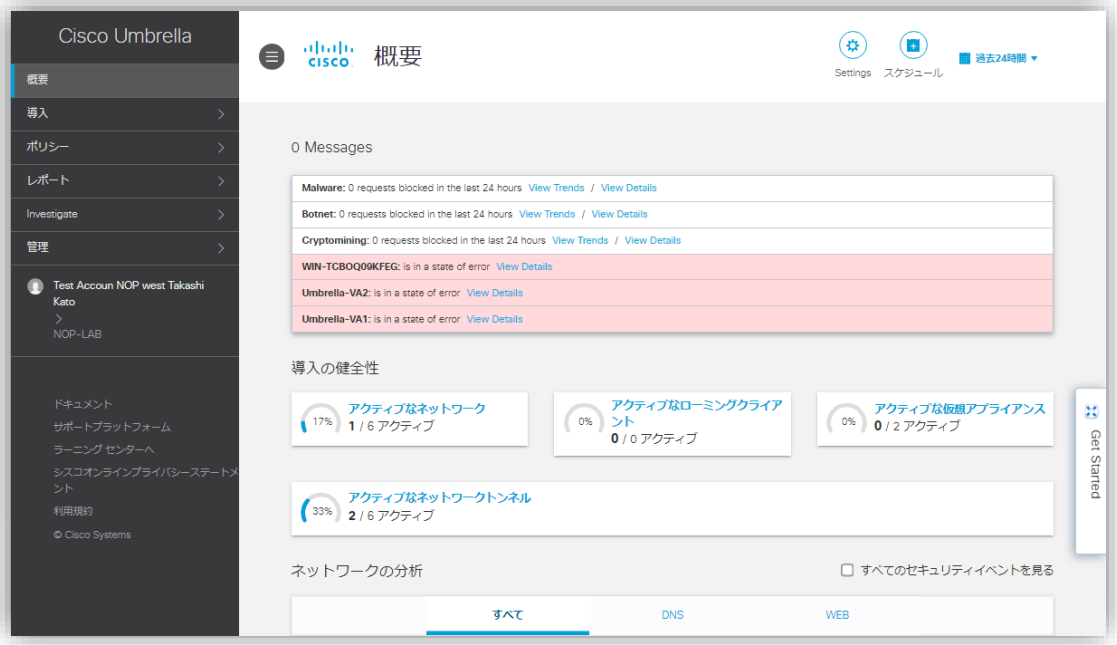


6. コンソールへのログイン手順 <システムログイン>

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/>

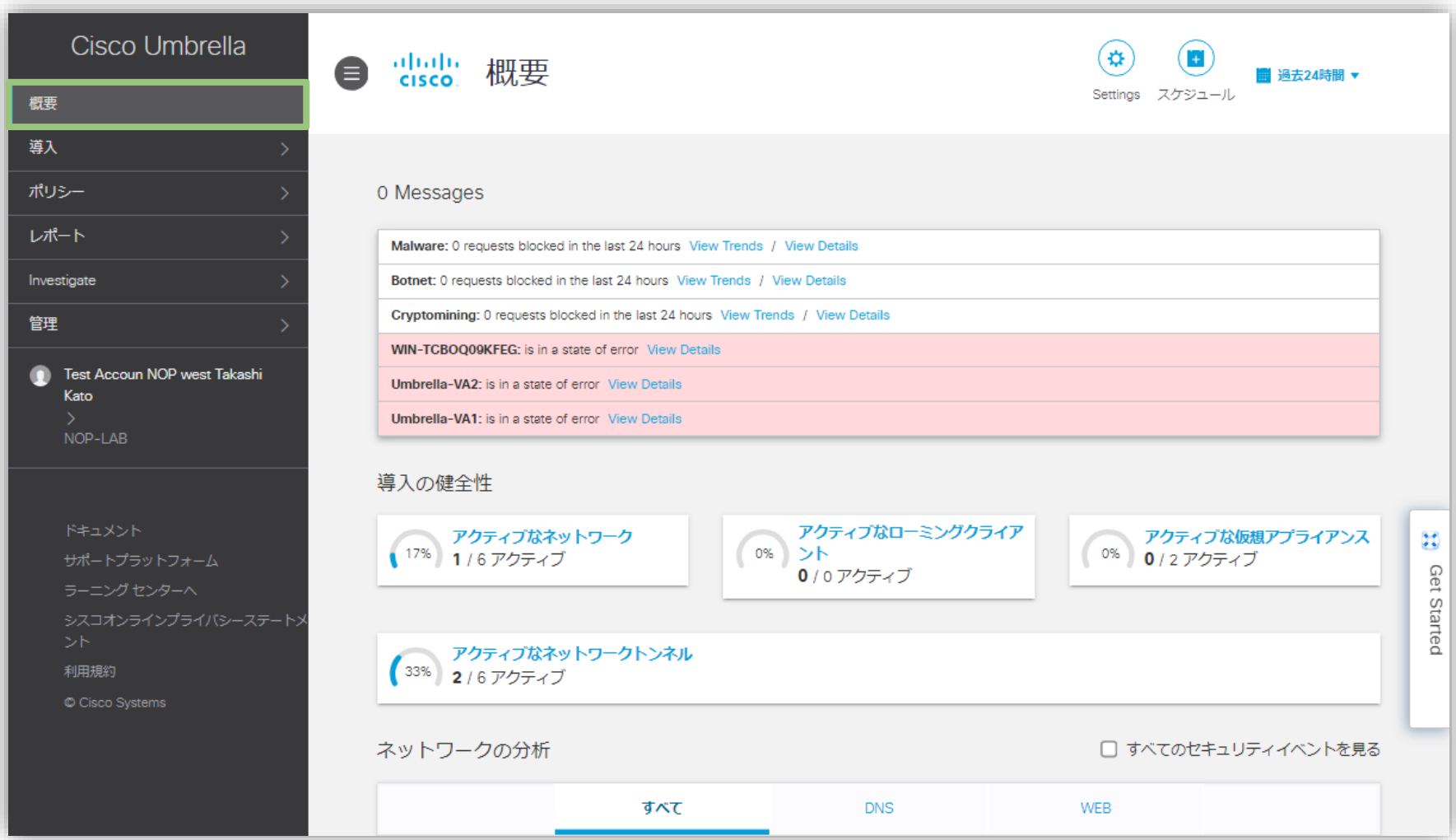
Umbrella ログイン画面



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。



6. コンソールへのログイン手順 <ダッシュボード説明>

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

[Messages] コンソールからのメッセージ情報を表示
[導入の健全性] アクティブ アイデンティティ／トータル アイデンティティ情報を表示 ※アイデンティティとはUmbrellaへの接続元デバイスを指します
[ネットワークの分析] DNSクエリ／Webトラフィックの統計情報や各ブロックカテゴリの統計情報を表示
[ファイアウォールの内訳] ファイアウォールで処理した統計情報を表示
[IPSの分類] IPSイベントの統計情報を表示
[セキュリティカテゴリ] 各ブロックカテゴリの統計情報を表示
[アプリケーションの検出と制御] 利用アプリケーションおよび制御イベントの統計情報を表示
[セキュリティリクエスト] DNS／WEBで接続の多い統計情報を 宛先／アイデンティティ／イベントタイプ の視点から表示
[ファイルレトロスペクティブ] レトロスペクティブにより（過去に遡り）悪意あるものと判断されたファイルを表示

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

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

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

トラブル対応による設定変更例

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

ご利用環境等に応じた設定変更例

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

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

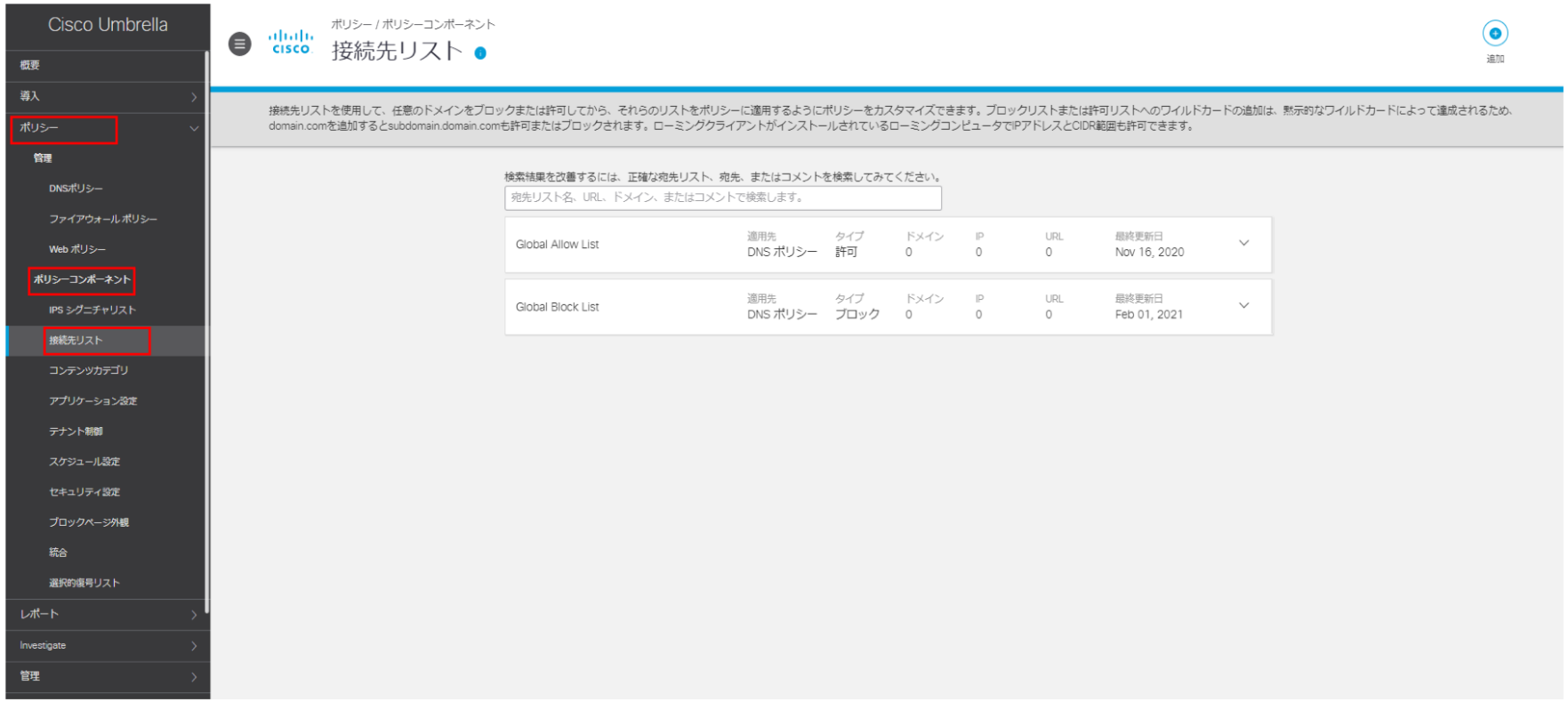
7-1-1. 特定のサイトが見られない① 1/23

セキュアインターネットゲートウェイ

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。

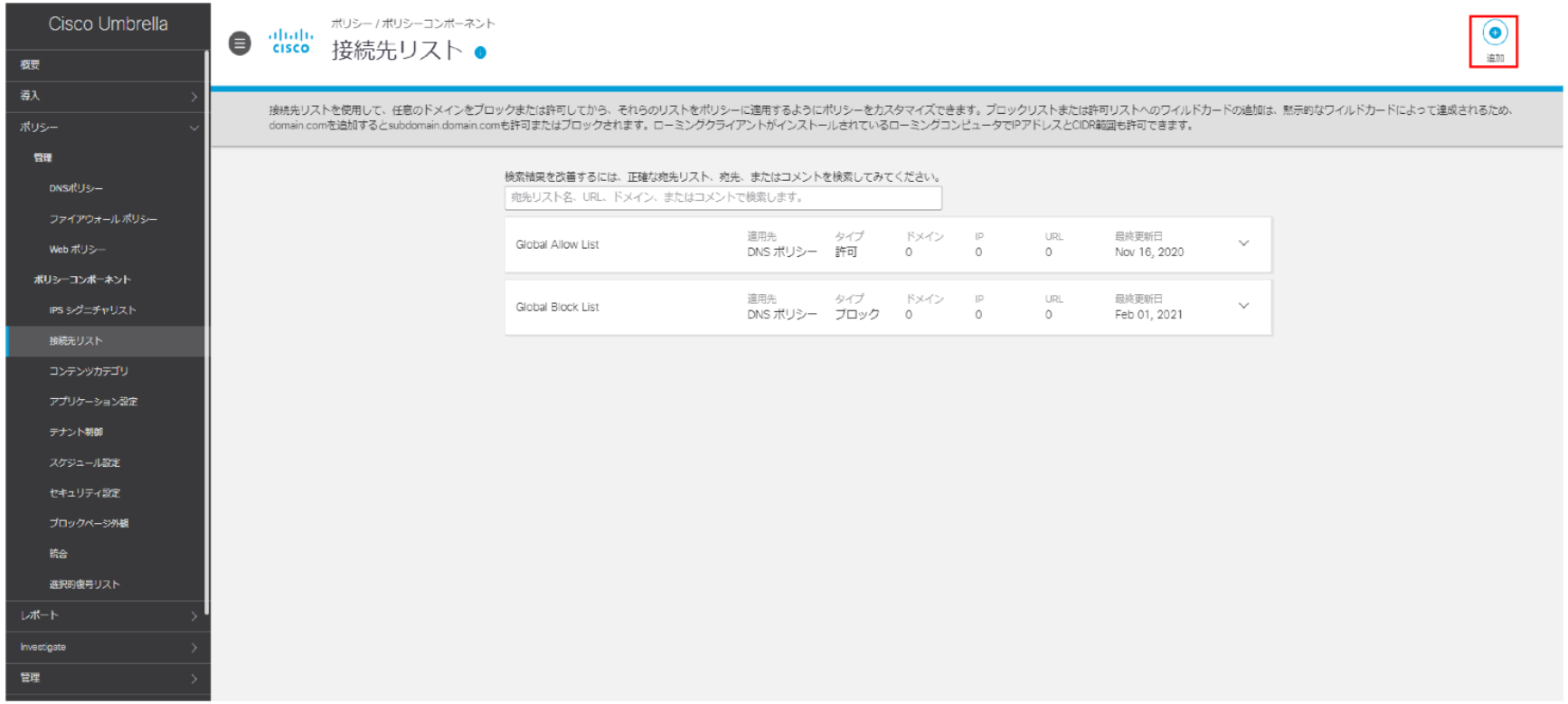
許可／ブロックリスト設定方法

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。



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。



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。

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。

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）

許可／ブロックリスト設定方法（つづき）

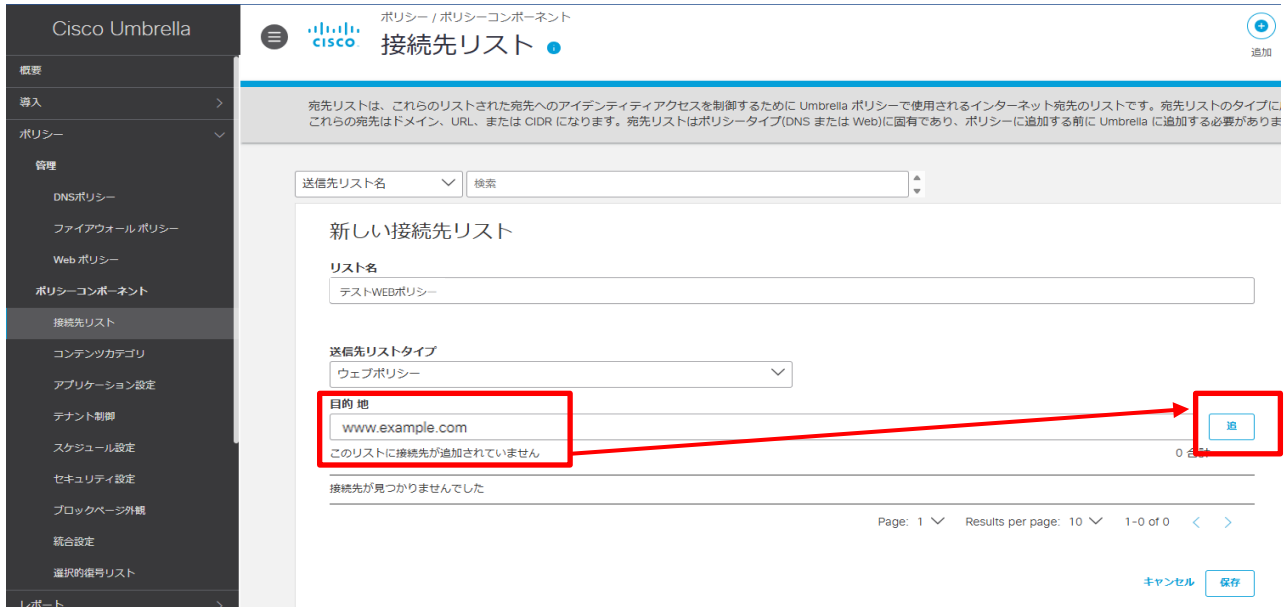
【DNSポリシー用に宛先を追加する場合の画面】

許可／ブロックリスト設定方法（つづき）

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

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

【Webポリシー用に宛先を追加する場合の画面】



許可／ブロックリスト設定方法（つづき）

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

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

許可／ブロックリスト設定方法（つづき）

⑧作成した接続先リストが表示されていることを確認します。

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

許可／ブロックリスト設定方法（つづき）

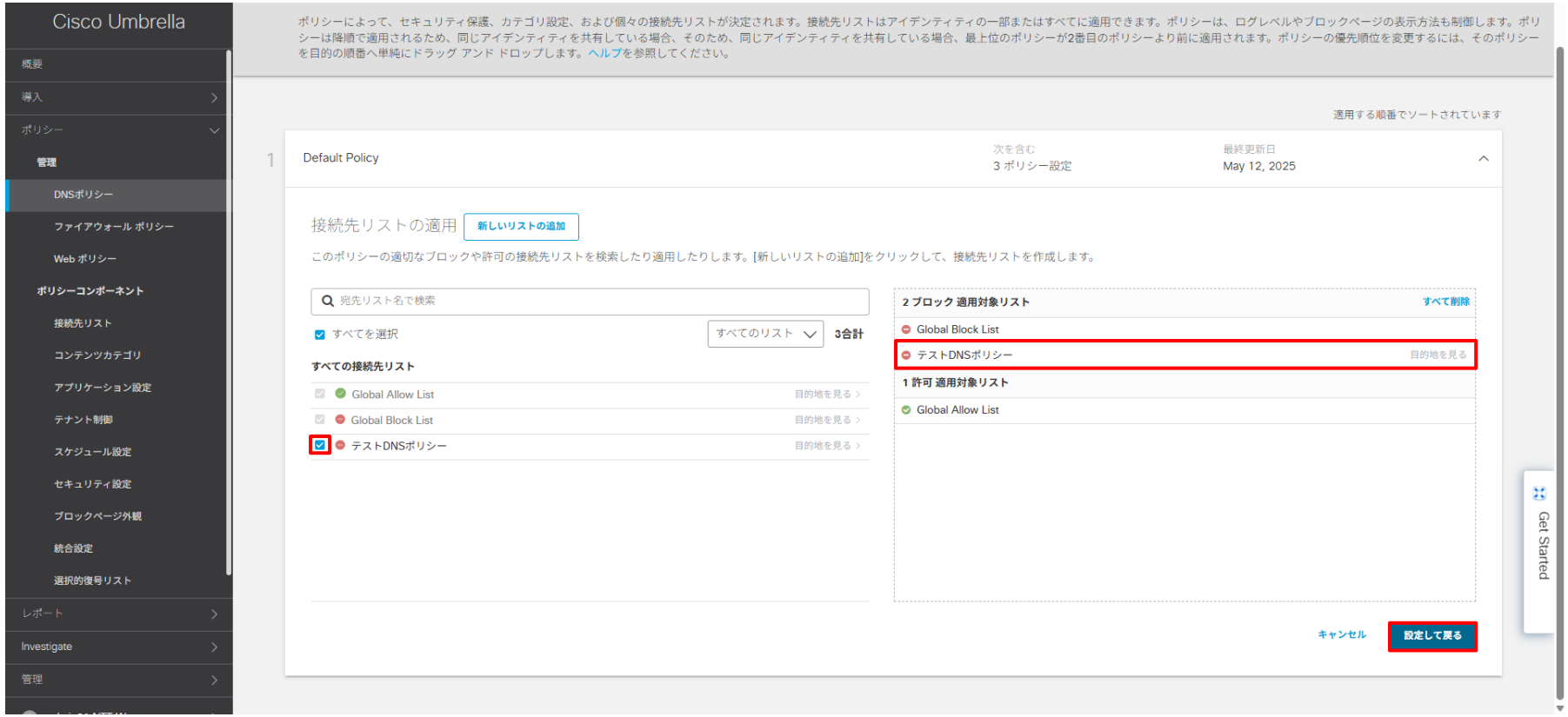
⑨作成したDNSポリシーを適用します。
　左側のメニューより「ポリシー」－「DNSポリシー」－「Default Policy」をクリックしします。

許可／ブロックリスト設定方法（つづき）

⑩接続先リスト適用の「編集」をクリックします。

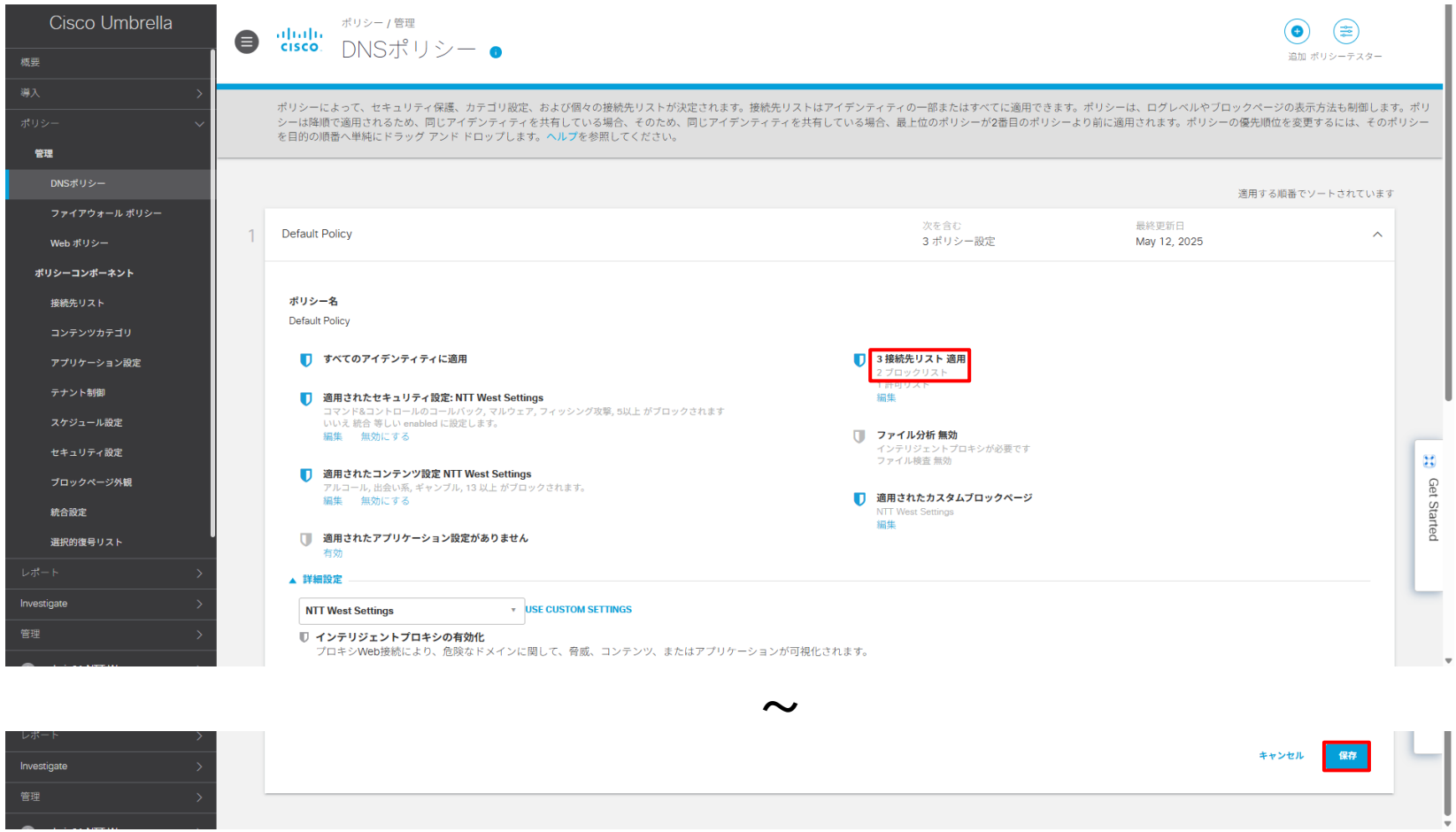
許可／ブロックリスト設定方法（つづき）

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



許可／ブロックリスト設定方法（つづき）

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



許可／ブロックリスト設定方法（つづき）

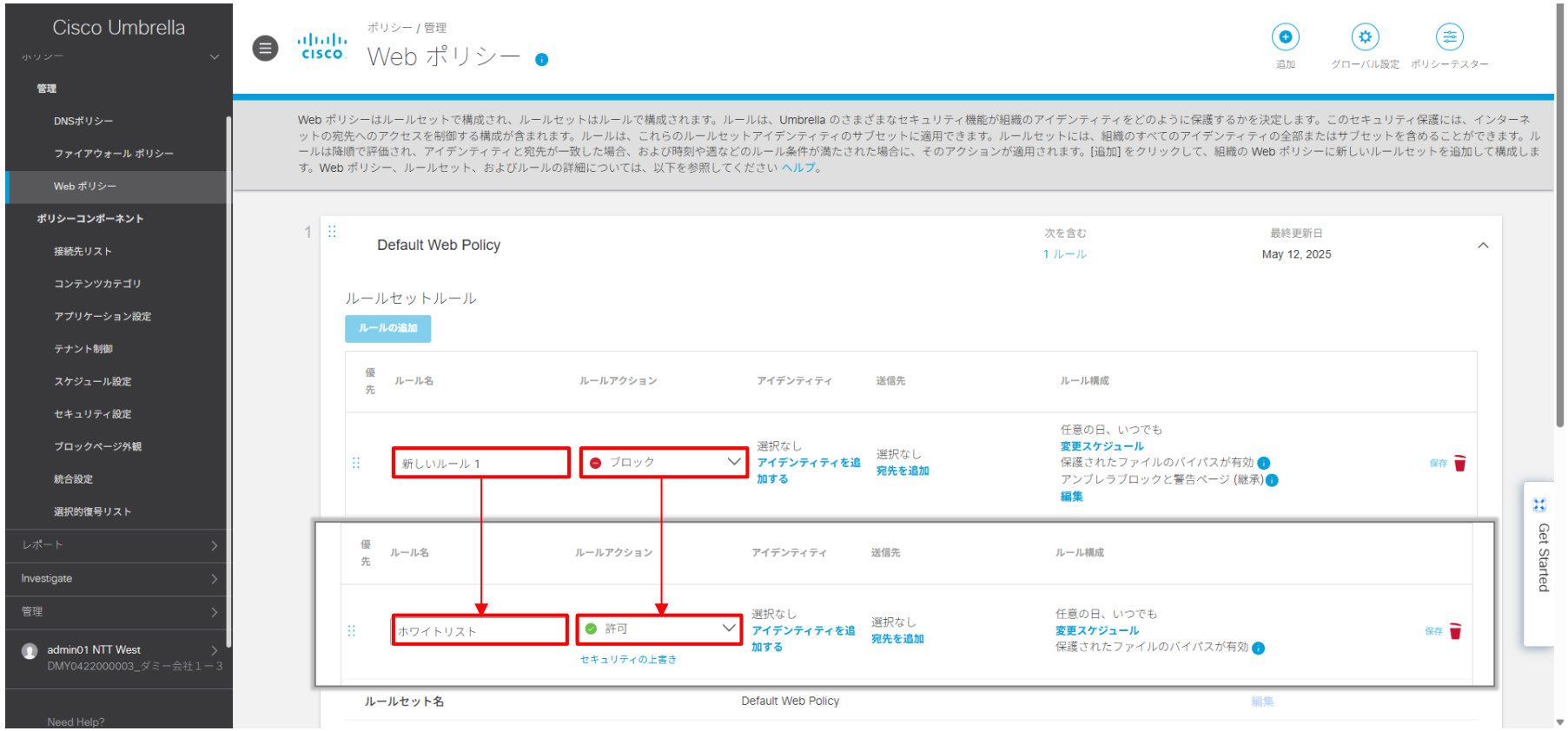
⑬作成したWebポリシーを適用します。
　左側のメニューより「ポリシー」－「Webポリシー」－「Default Web Policy」をクリックしします。

許可／ブロックリスト設定方法（つづき）

⑭接続先リスト適用の「ルールの追加」をクリックします。

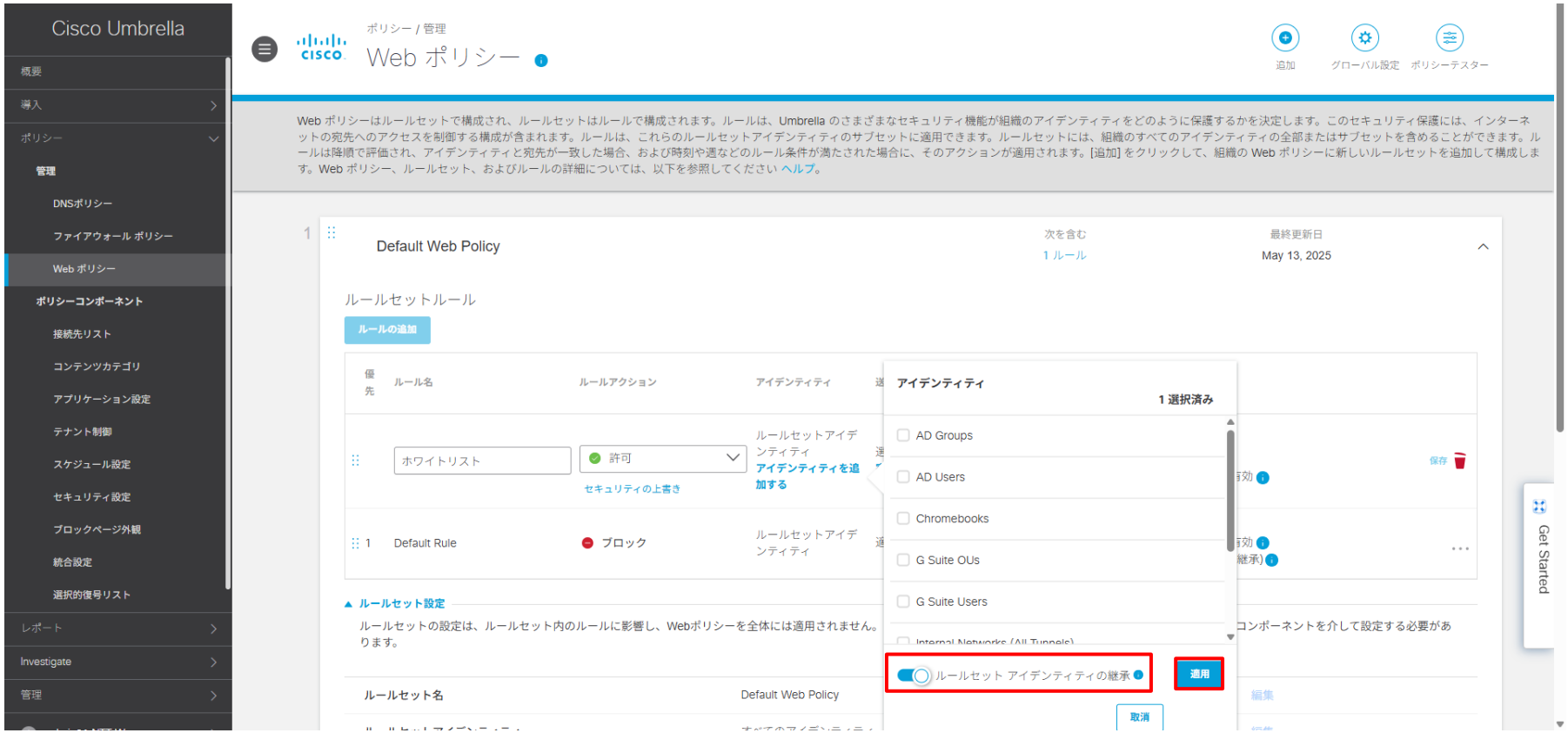
許可／ブロックリスト設定方法（つづき）

⑮例えばルール名「ホワイトリスト」、ルールアクション「許可」のルールを追加する場合



許可／ブロックリスト設定方法（つづき）

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



許可／ブロックリスト設定方法（つづき）

⑰送信先の「Destination Lists」を選択し－「＞」をクリック

許可／ブロックリスト設定方法（つづき）

⑱送信先／宛先リストで作成した「テストWEBポリシー」を選択し「適用」をクリック

許可／ブロックリスト設定方法（つづき）

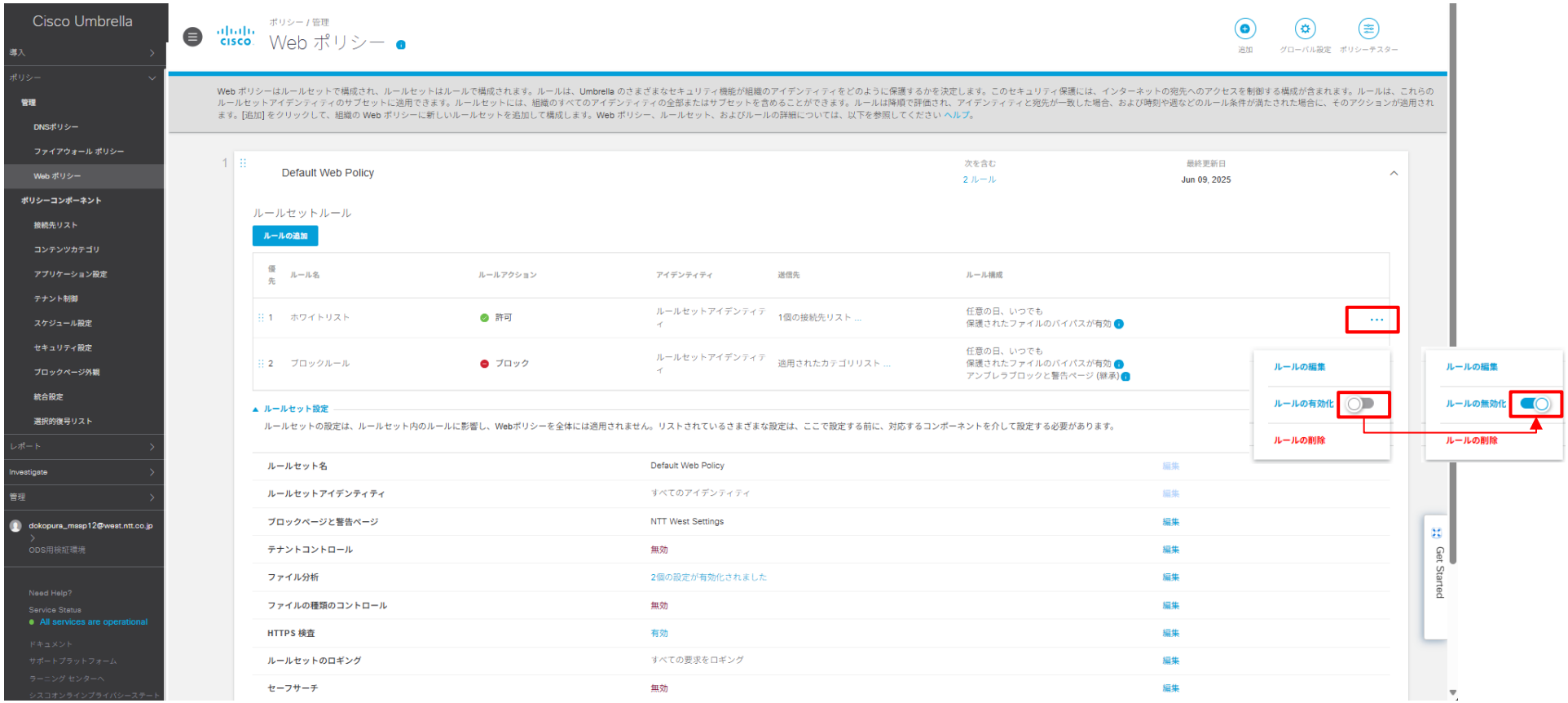
⑲「保存」をクリック→「＾」をクリック

許可／ブロックリスト設定方法（つづき）

⑳改めて「Default Web Policy」をクリックします。

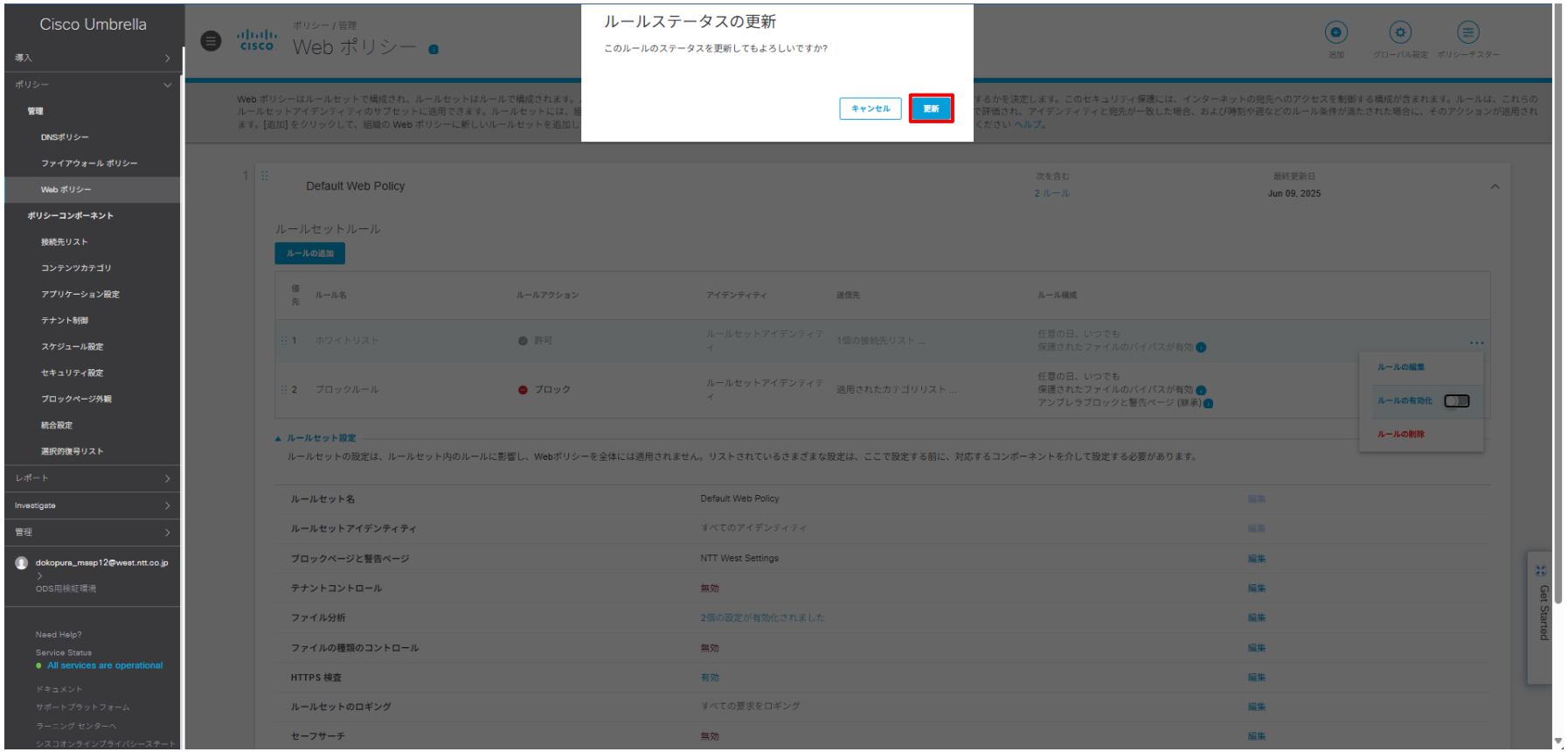
許可／ブロックリスト設定方法（つづき）

㉑作成したホワイトリストの「・・・」をクリック→「ルールの有効化」をオン



許可／ブロックリスト設定方法（つづき）

㉒ルールステータスの「更新」をクリック



7-1-2. 特定のサイトが見られない② 1/5

Cisco Umbrella ではHTTPS通信の復号を行う際、通信を中継して内容をチェックするために独自のSSL/TLS証明書を使用します。
しかし、一部のサイトでは証明書の厳格な検証を行い、独自の証明書による復号を拒否することがあります。
例えば、銀行や政府機関のサイトは特に厳格な証明書管理をしているため、HTTPS復号を試みるとアクセスできなくなることや、一部のウェブサイトは、中間者攻撃（Man-in-the-Middle攻撃）を防ぐため、HTTPS復号を行う環境からのアクセスをブロックすることがあります。

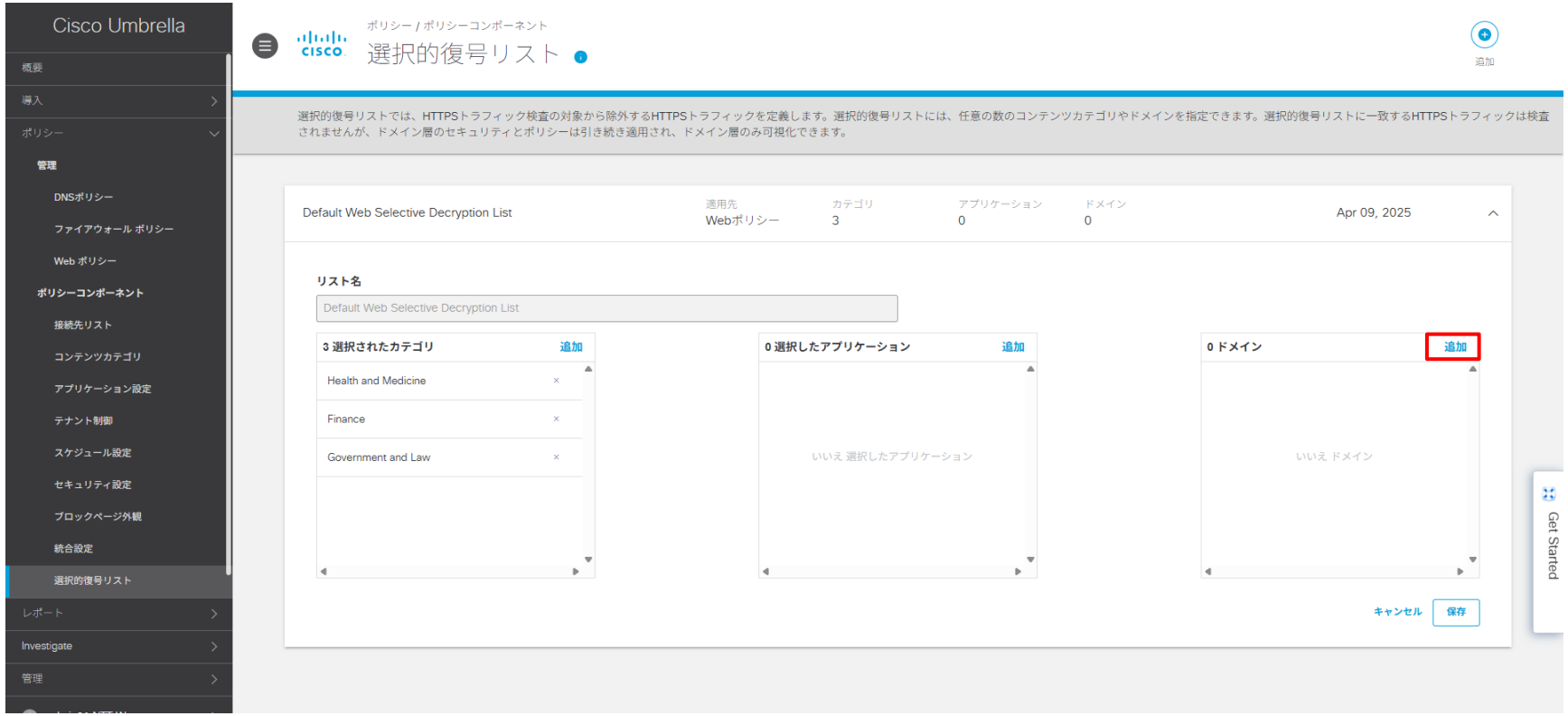
アクセスを行うためには管理コンソールで、対象サイトへのHTTPS通信の復号除外設定を行う必要があります。
サイトに問題がないと判断できる場合のみ、下記手順でHTTPS通信の復号除外設定をお願いします。

HTTPS通信の復号除外設定方法

①左側のメニューより「ポリシー」－「選択的複合リスト」－「Default Web Selective Decryption List」をクリックします。

HTTPS通信の復号除外設定方法（つづき）

②画面右の「追加」をクリックします。



HTTPS通信の復号除外設定方法（つづき）

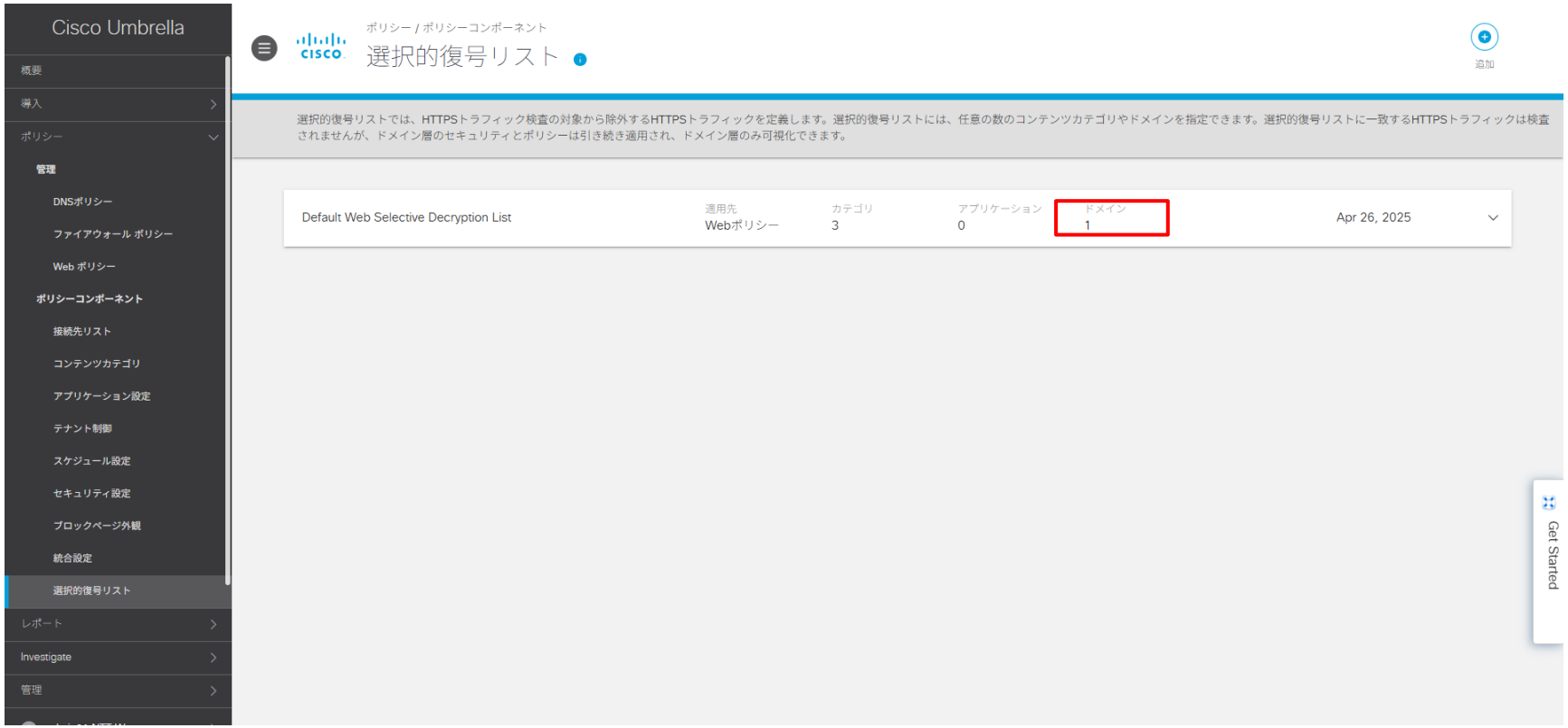
③復号除外する「ドメイン」を記載し「追加」をクリックします。

HTTPS通信の復号除外設定方法（つづき）

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

HTTPS通信の復号除外設定方法（つづき）

⑤復号除外する「ドメイン」が追加されていることを確認します。



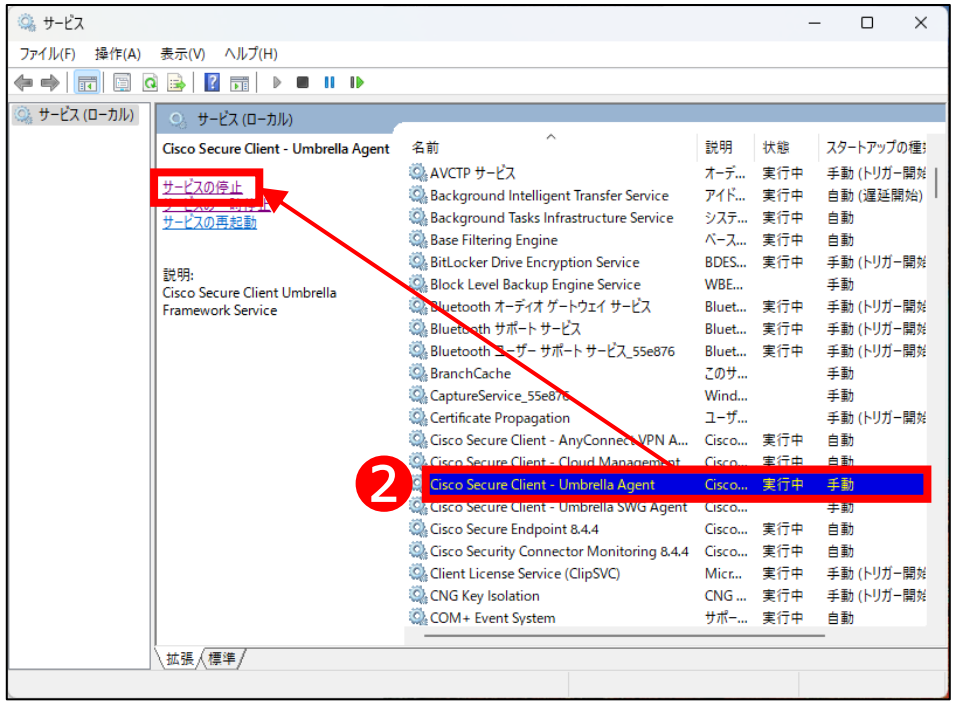
7-2. インターネットが使えない

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ください。
※Cisco Umbrellaを無効にしてもインターネットに接続できない場合はCisco Umbrella 要因ではございません。
Cisco Umbrella 要因であった場合は、お電話にてサポートセンターお問合せください。

本サービスのセキュリティソフトを無効にする方法

◆WindowsOSの場合

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



7-3. 導入後、通信速度が遅くなった

セキュアインターネットゲートウェイ

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

Cisco Umbrella を無効にする方法

p92を参照ください。

7-4.「セキュリティ証明書に問題があります」と表示される 1/9

「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。

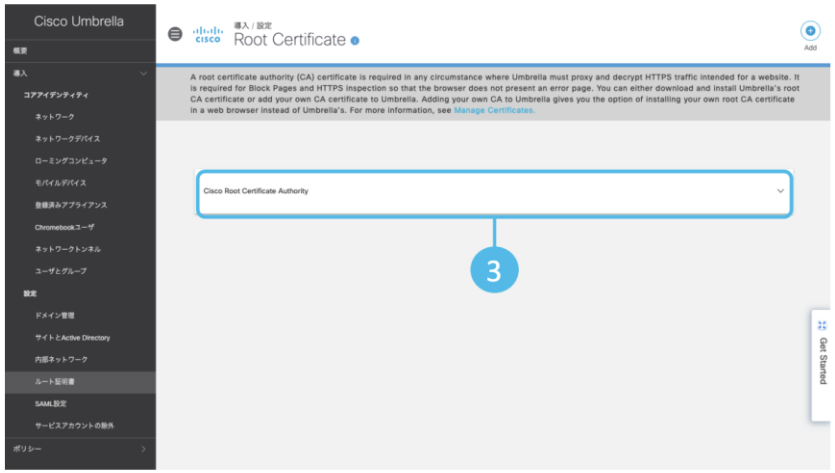
①「導入」をクリックします。

電子証明書の設定方法（つづき）

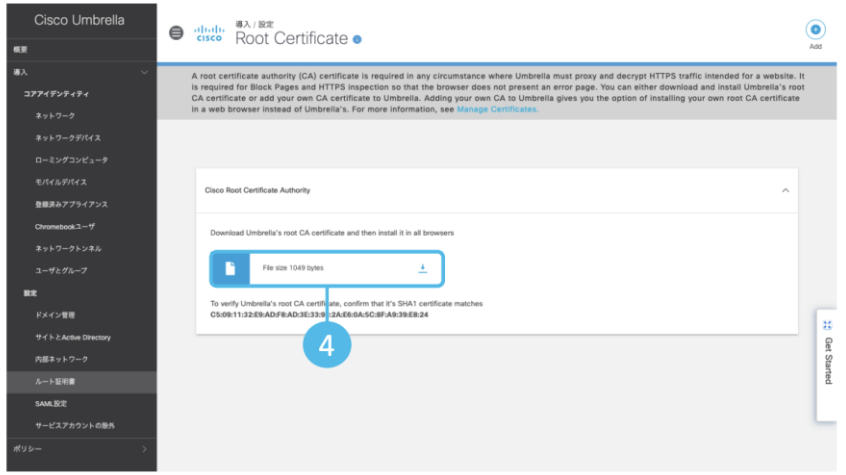
②「ルート証明書」をクリックします。

電子証明書の設定方法（つづき）

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

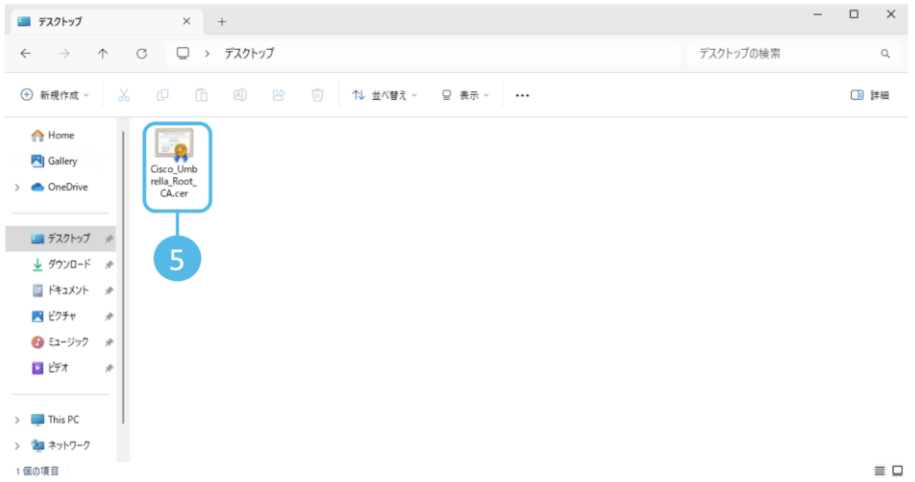


④[↓]アイコンをクリックし、ルート証明書をダウンロード及び任意の場所に保存します。
「Cisco_Umbrella_Root_CA.cerはデバイ スに問題を起こす可能性があります。このま ま保存しますか?」などの警告メッセージが表示されることがありますが、[保存]をクリックし 続行してください。

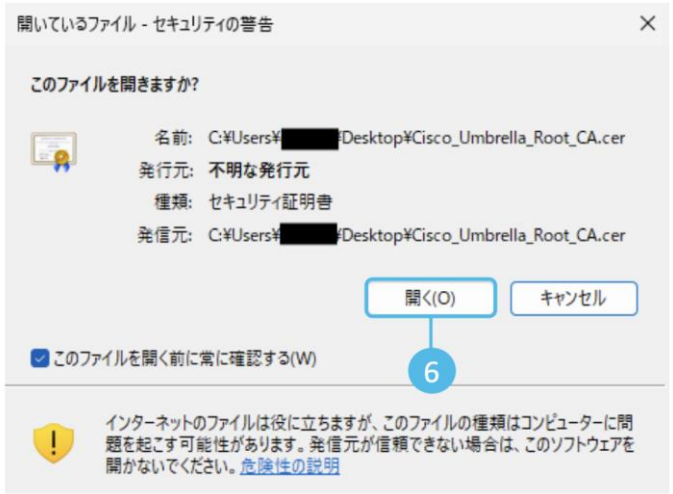


電子証明書の設定方法（つづき）

⑤④で保存した場所（フォルダ）を開き、、ルート証明書をクリックします。
ファイル 名は、[Cisco Umbrella_Root_CA](拡張子なし表示)または
[Cisco_Umbrella_root_CA.cer](拡張子あり 表示)です。
[セキュリティの警告]ダイアログボックスが表示されます。



⑥「開く」をクリックします。



電子証明書の設定方法（つづき）

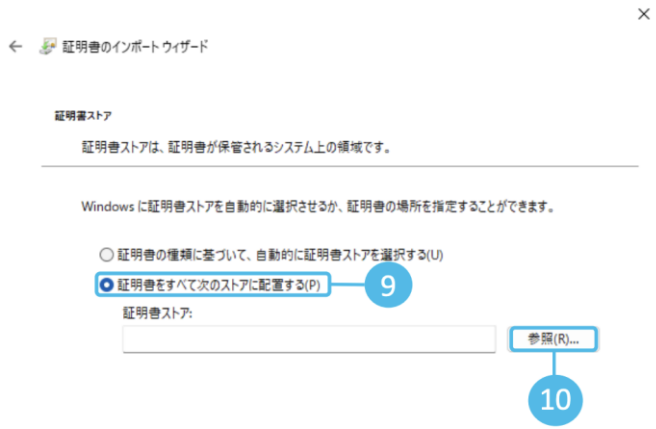
⑦[証明書のインストール]をクリックします。

⑧[証明書のインポート ウィザード]が表示されます。「次へ」をクリックします。
デフォルトでは[現在のユーザー]が選択されています。必要に応じて[ローカルコンピューター] を選択してください。

電子証明書の設定方法（つづき）

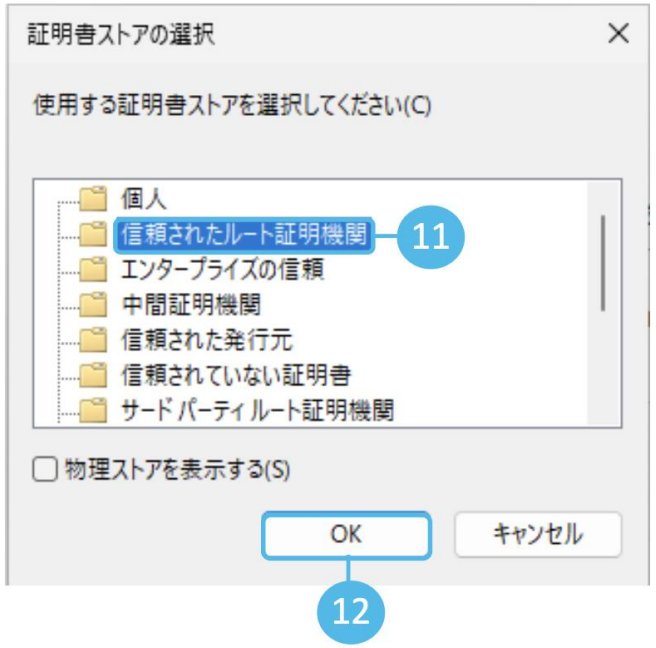
⑨「証明書をすべて次のストアに配置する」をクリックします。

⑩「参照」をクリックします。



⑪「信頼されたルート証明機関」をクリックします。

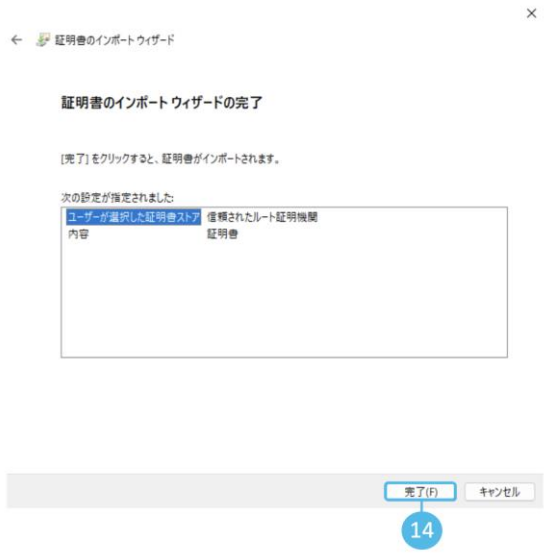
⑫　「OK」をクリックします。



電子証明書の設定方法（つづき）

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

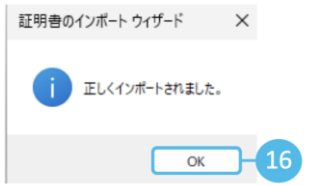
⑭「完了」をクリックします。



電子証明書の設定方法（つづき）

⑮ [セキュリティ警告]のダイアログボックスが表示されます。「はい(Y)」をクリックします。

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



⑰「OK」をクリックします。

7-5. 共有フォルダにアクセスできない

セキュアインターネットゲートウェイ

まずCisco Umbrella 要因で共有フォルダにアクセスができないのかをご確認いただくため、Cisco Umbrella を無効にし、共有フォルダにアクセスができるかをお試しください。
※Cisco Umbrella を無効にしても共有フォルダにアクセスができない場合はCisco Umbrella 要因ではございません。
Cisco Umbrella 要因であった場合は、サポートセンターにお電話にてお問合せください。

Cisco Umbrella を無効にする方法

p92を参照ください。

7-6. ベンダーのリモートツールが動かない

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

①Cisco Umbrella を無効にする方法

p92を参照ください。

②Cisco Umbrellaの許可／ブロックリスト設定方法

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

p64-86を参照ください。

③Cisco UmbrellaのHTTP通信の復号除外設定方法

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

p87-91を参照ください。

7-7. 新しいパソコンでメールの送受信ができない

セキュアインターネットゲートウェイ

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

①Cisco Umbrella を無効にする

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

②証明書の問題

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

7-8. 500番台のエラーメッセージが表示される 1/2

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。

7-8. 500番台のエラーメッセージが表示される 2/2

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

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

7-9. DNSポリシーを変更したい 1/8

「7-1.特定のサイトが見られない」より高度な設定として、DNSポリシーを変更することができます。
EMOTETなどのランサムウェア対策についてはDNSポリシーを利用しています。
Cisco UmbrellaのDNSポリシーは、企業や組織がインターネットアクセスを制御し、セキュリティを強化するために設定できるルールのことを指します。
これにより、不正なサイトや不要なカテゴリのサイトへのアクセスをブロックしたり、特定のユーザーやグループに異なる制限を適用したりすることが可能になります。
ただし本ポリシーを変更することでセキュリティーリスクが高まる場合もあるため、変更に際しては十分ご注意ください。

＜Cisco UmbrellaのDNSポリシーの主な機能＞

1.コンテンツフィルタリング

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

2.セキュリティ対策（脅威インテリジェンス）

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

3.ポリシーの適用範囲の設定

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

4.**セーフサーチ＆アプリケーション制御**

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

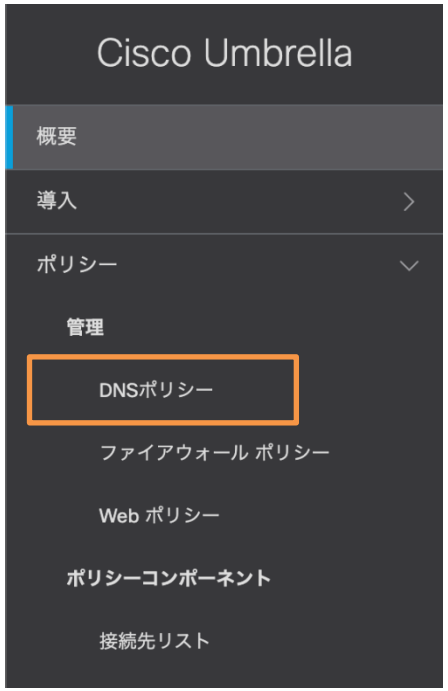
5.**カスタムブロックページの設定**

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

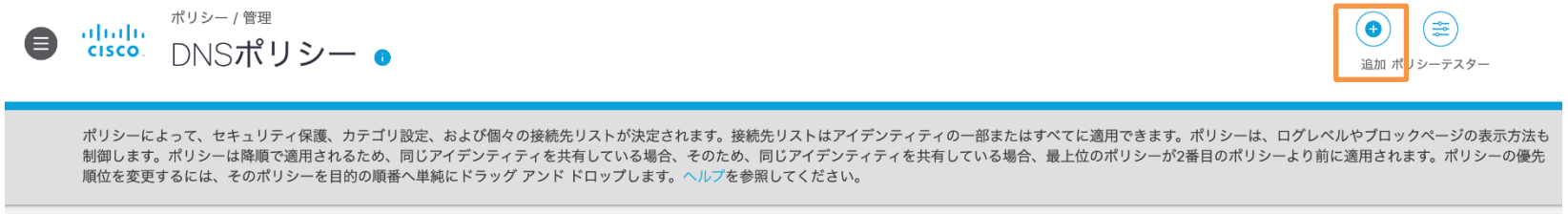
DNSポリシーの作成・管理方法

①Cisco Umbrellaの管理コンソールにログイン

②ポリシー > DNSポリシー に移動



③新しいポリシーを作成します
（または既存のポリシーを編集します）



DNSポリシーの作成・管理方法

④保護対象を選択します

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

DNSポリシーの作成・管理方法

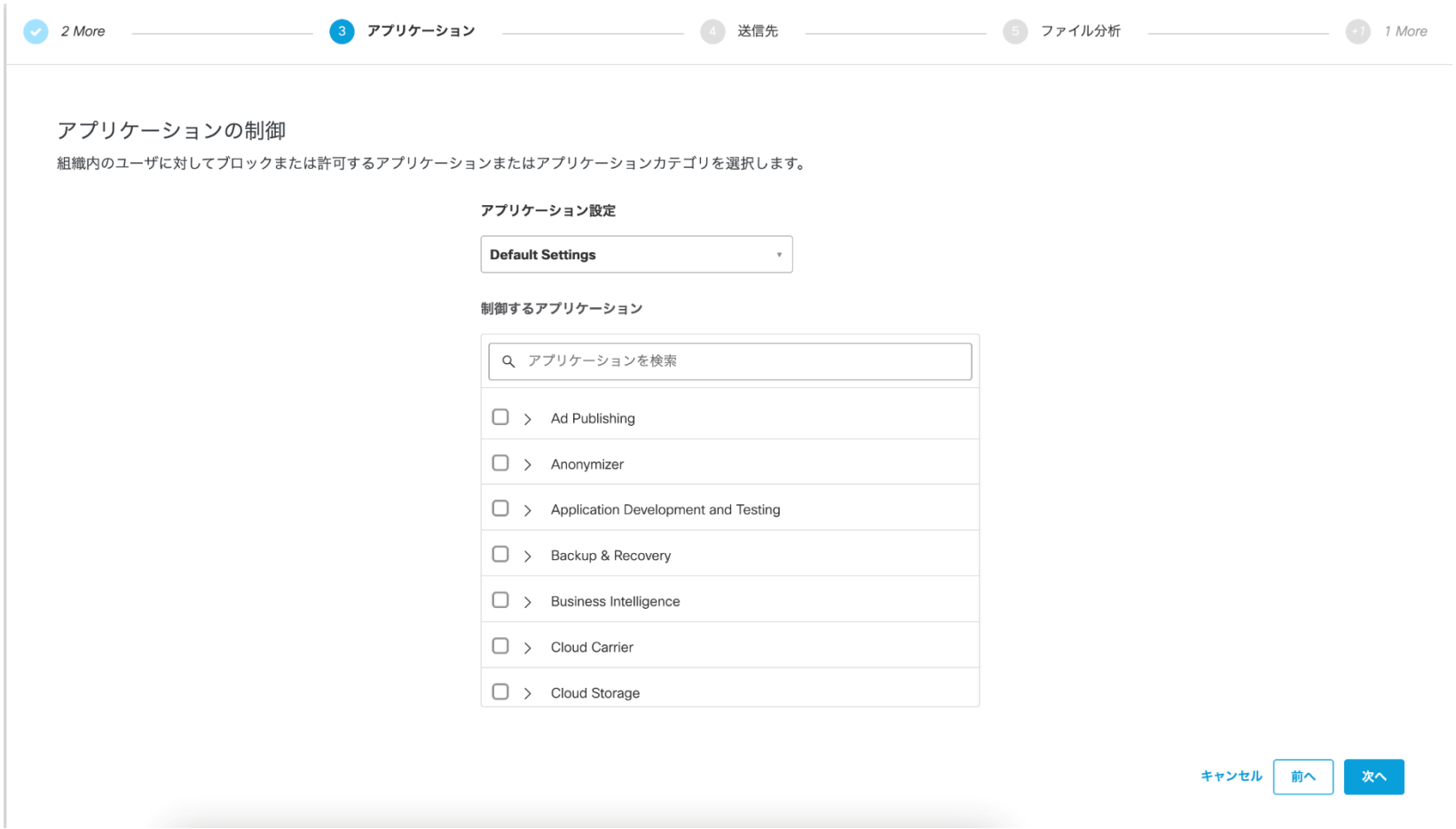
⑥セキュリティ設定を適用（マルウェア、フィッシングブロックなど）します

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

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



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。

7-10. 広告のページを開けるようにしたい 1/5

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

広告ページのアクセス許可設定方法

Cisco Umbrellaのログイン画面より、ダッシュボードにログインします。
①ポリシー > ポリシーコンポーネント > コンテンツカテゴリへ移動します
②Default Settingsタブを選択後、カテゴリ中の「広告」を選択解除し、設定を保存します
（※以下はコンテンツカテゴリとして「成人向け」「アルコール」は選択し、「広告」は選択解除する場合の設定例となります）

広告ページのアクセス許可設定方法（つづき）

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

広告ページのアクセス許可設定方法（つづき）

④適用されたコンテンツ設定の「編集」をクリックします。

広告ページのアクセス許可設定方法（つづき）

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

広告ページのアクセス許可設定方法（つづき）

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

7-11. 怪しいサイトがUmbrellaの検知をすり抜けている

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

Cisco Umbrellaの許可／ブロックリスト設定方法

p64-86を参照ください。

7-12. Umbrellaの許可・ブロックリストを設定したい

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

Cisco Umbrellaの許可／ブロックリスト設定方法

p64-86を参照ください。

7-13. CASBの設定方法を知りたい 1/2

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

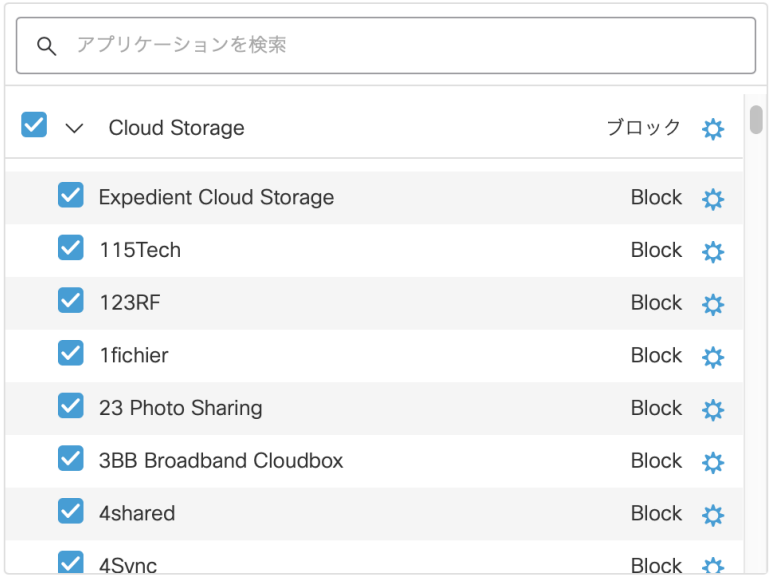
Umbrella Dashboardからポリシ → ポリシーコンポーネンツ → アプリケーション設定をクリックし、設定したいポリシーをクリックします。

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

注意：すべてのクラウドサービスが設定できるわけはございません。

CASBの設定方法（つづき）

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



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

7-14. 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

セキュアインターネットゲートウェイ

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

クラウドサービスの利用状況を確認する方法

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

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

各カテゴリなどの説明についてはUmbrella マニュアルを参照してください。
https://docs.umbrella.com/deployment-umbrella/docs/app-discovery

7-15. 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 1/3

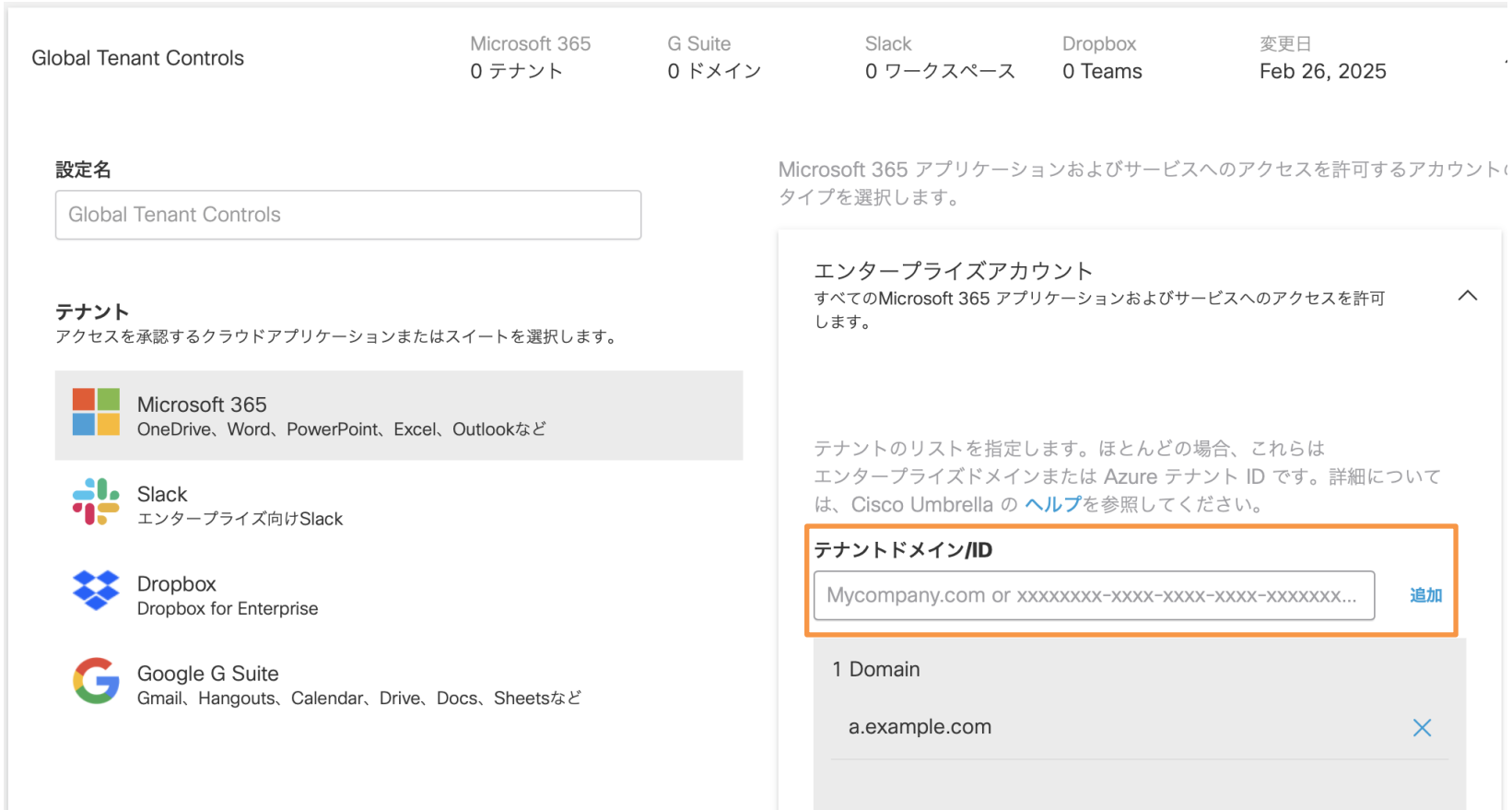
テナント制御とは、管理者によって指定されたクラウドサービスの契約テナント（環境）のみにアクセスできるよう制御する機能です。
例えば、会社貸与のパソコンから会社で契約しているMicrosoft 365環境へのみ接続を許し、個人契約のMicrosoft 365に接続させないなど制御することができるようになります。
Umbrella では現在 Microsoft 365, Google G Suite (Google Workspace), Slack, Dropbox に対応しています。

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

②「Global Tenant Controls」をクリックします。

7-15. 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 2/3

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。



7-15. 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 3/3

セキュアインターネットゲートウェイ

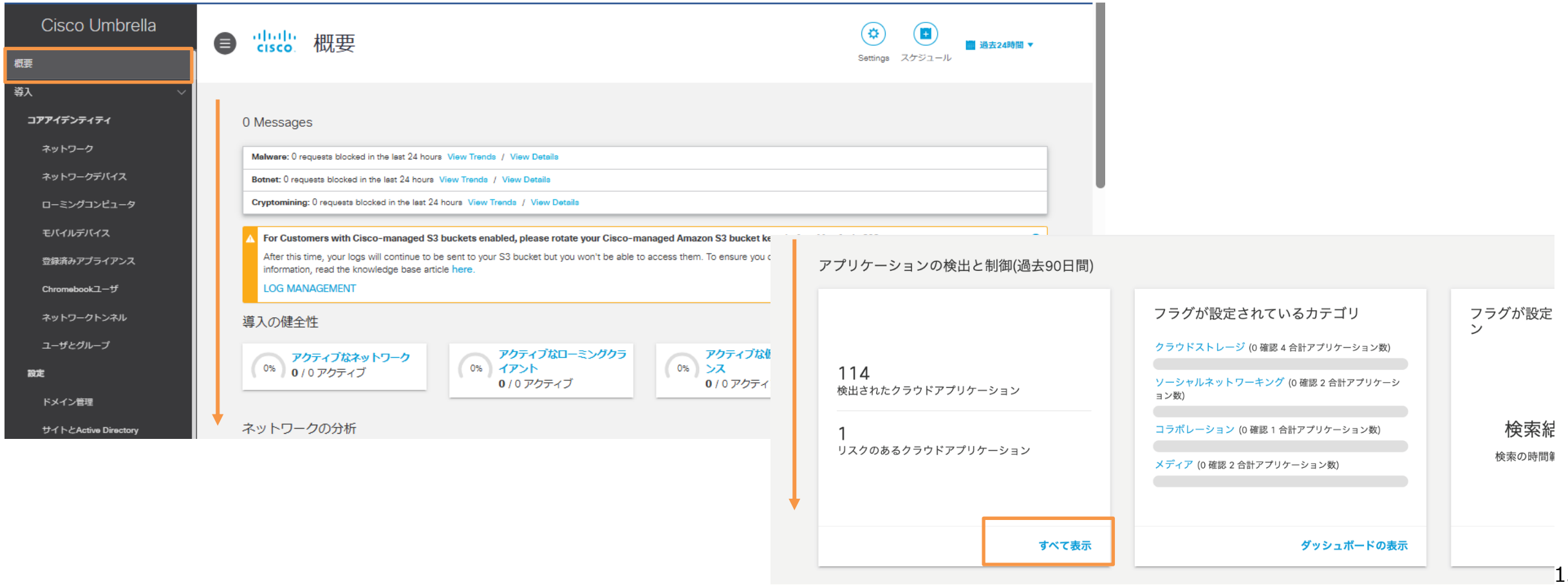
③画面下部に個人アカウントにて「個人用Microsoft 365アカウントのアクセスをブロックする」をクリックしレバーをオンの状態にします。

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。

7-16. 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 1/4

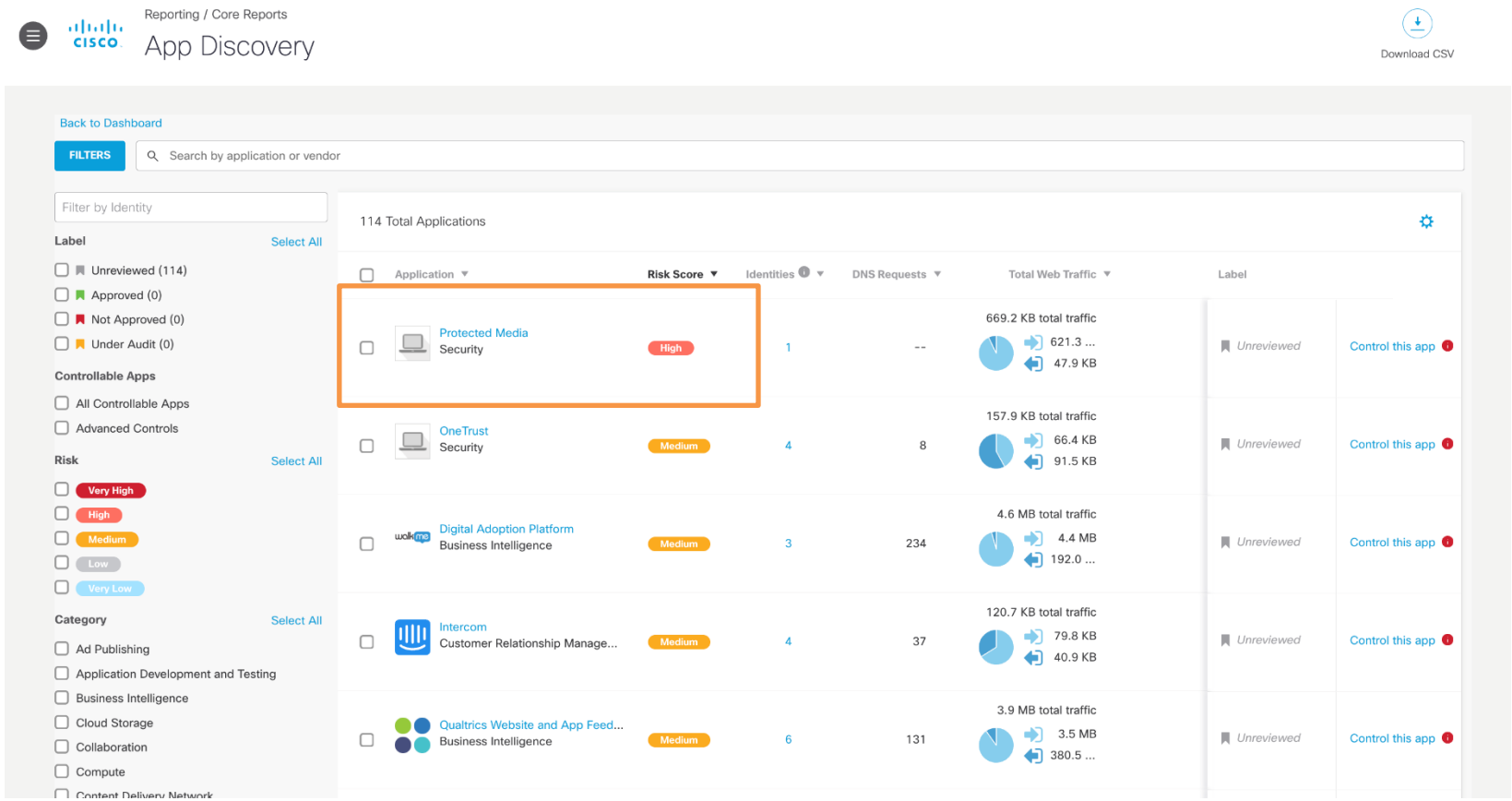
Cisco Umbrellaでは、DNSやWebポリシーのログから、Webアプリやクラウドサービスの利用状況を可視化し、通信を制御することができます。

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



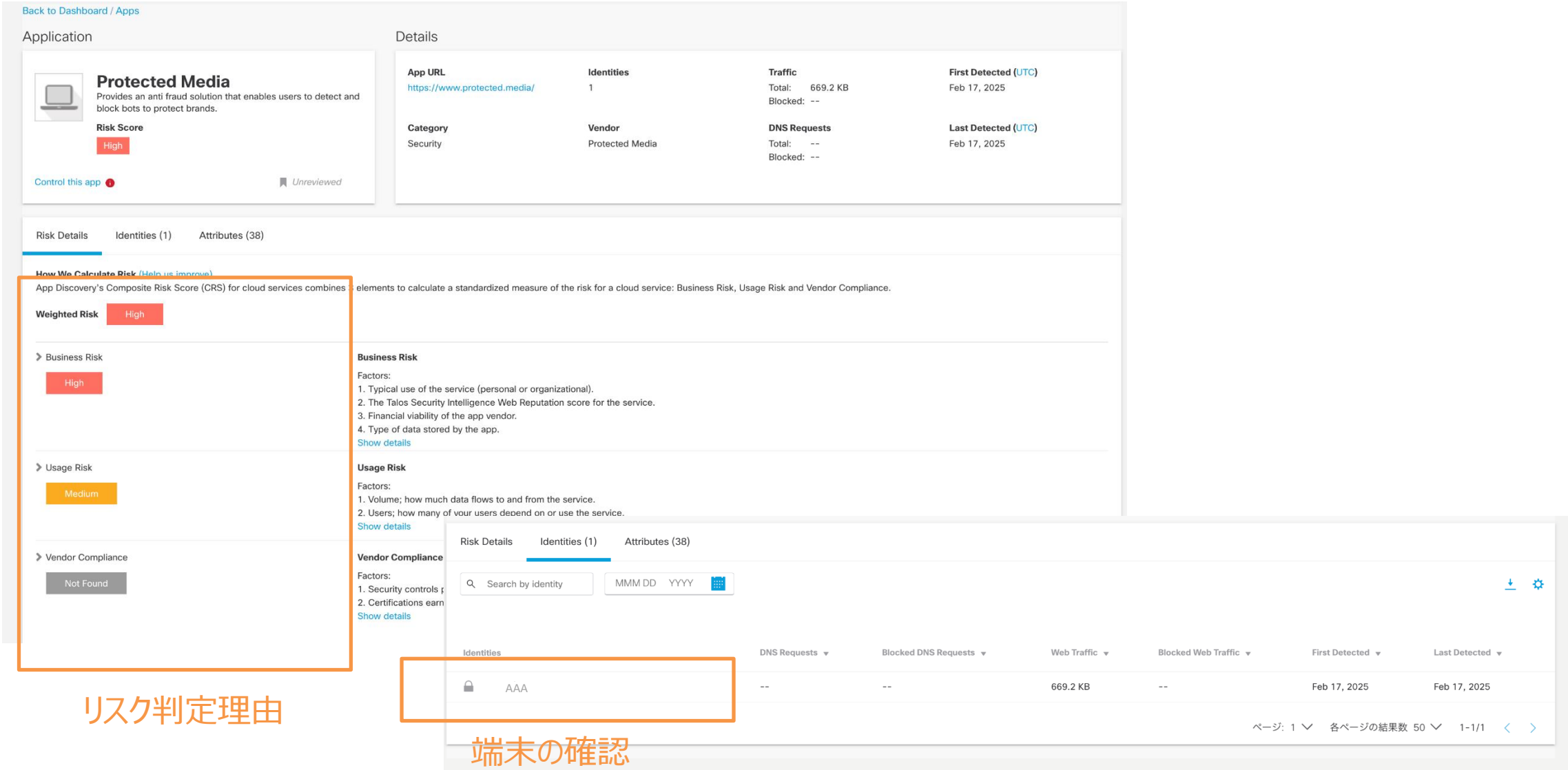
7-16. Umbrellaでユーザの利用しているアプリの可視化をし、特定アプリをブロックしたい 2/4

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。



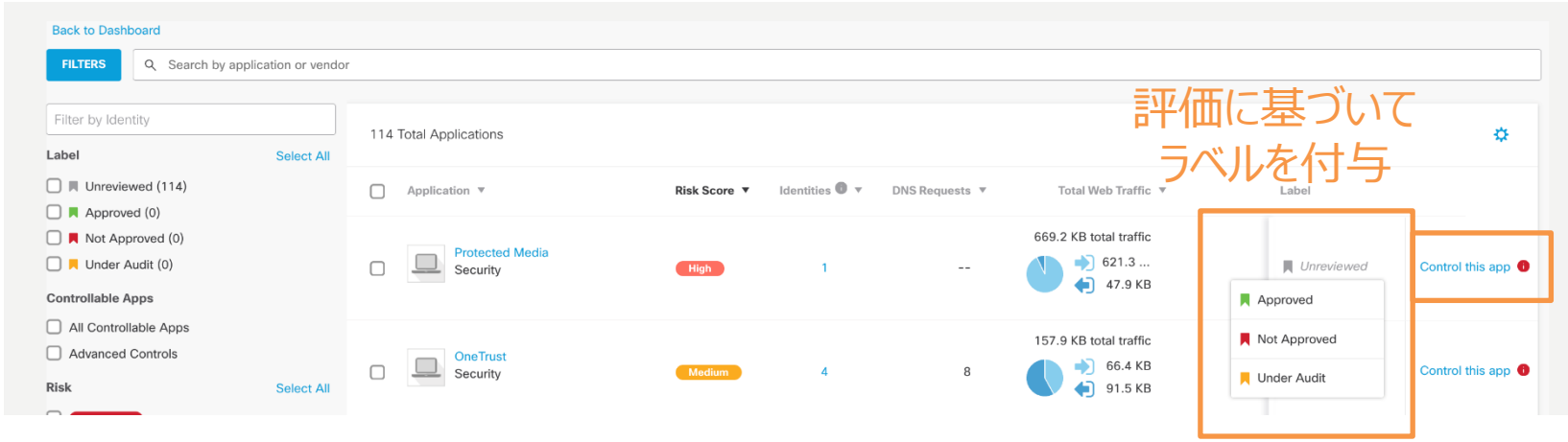
7-16. Umbrellaでユーザの利用しているアプリの可視化をし、特定アプリをブロックしたい 3/4

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。

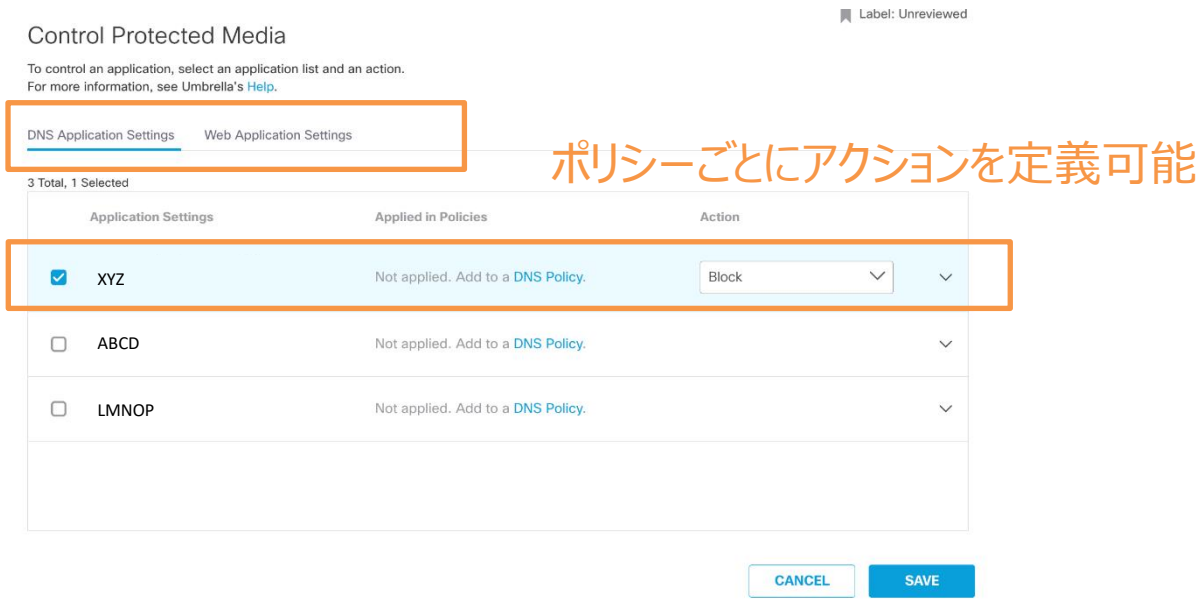


7-16. Umbrellaでユーザの利用しているアプリの可視化をし、特定アプリをブロックしたい 4/4

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。

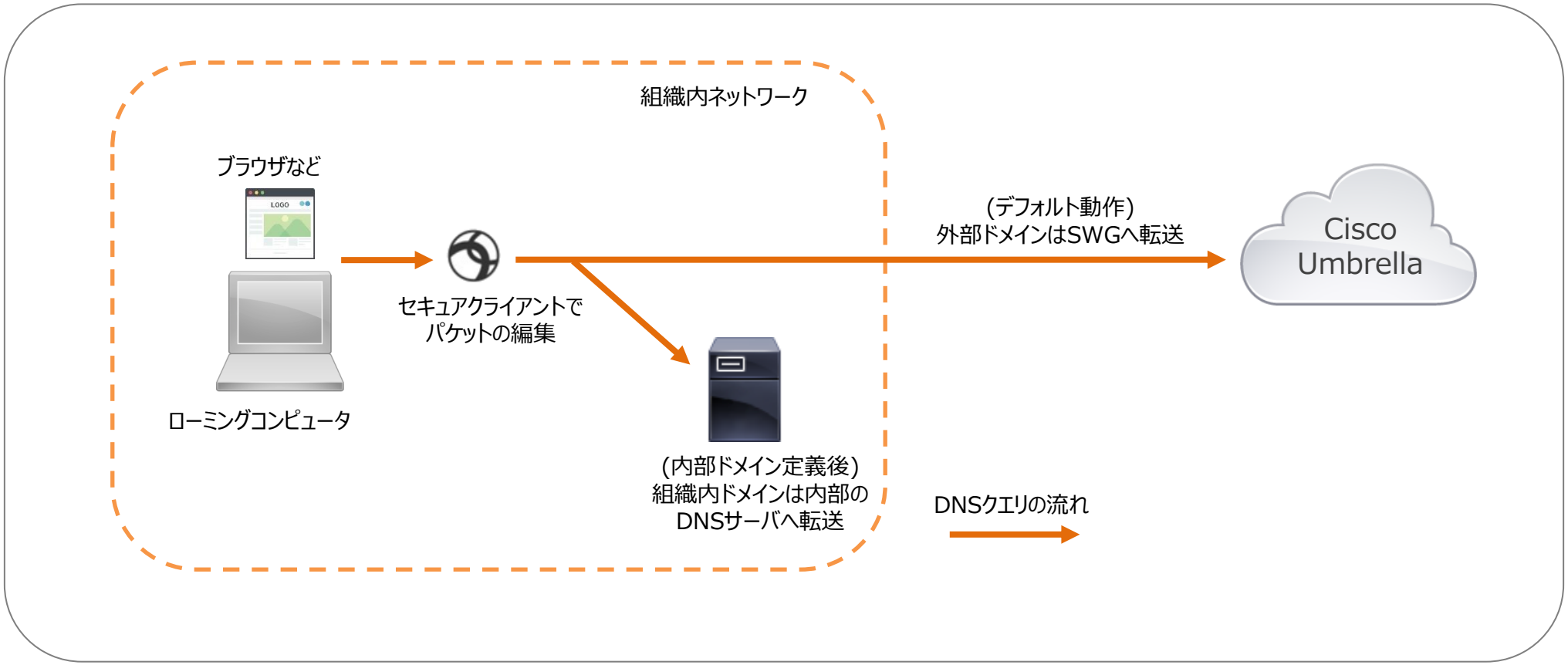


⑤実際にDNSポリシーやWebポリシーによって、通信を許可、拒否することができます。
（DNSはドメイン単位、WebはURL単位）



7-17. ドメイン管理 1/4

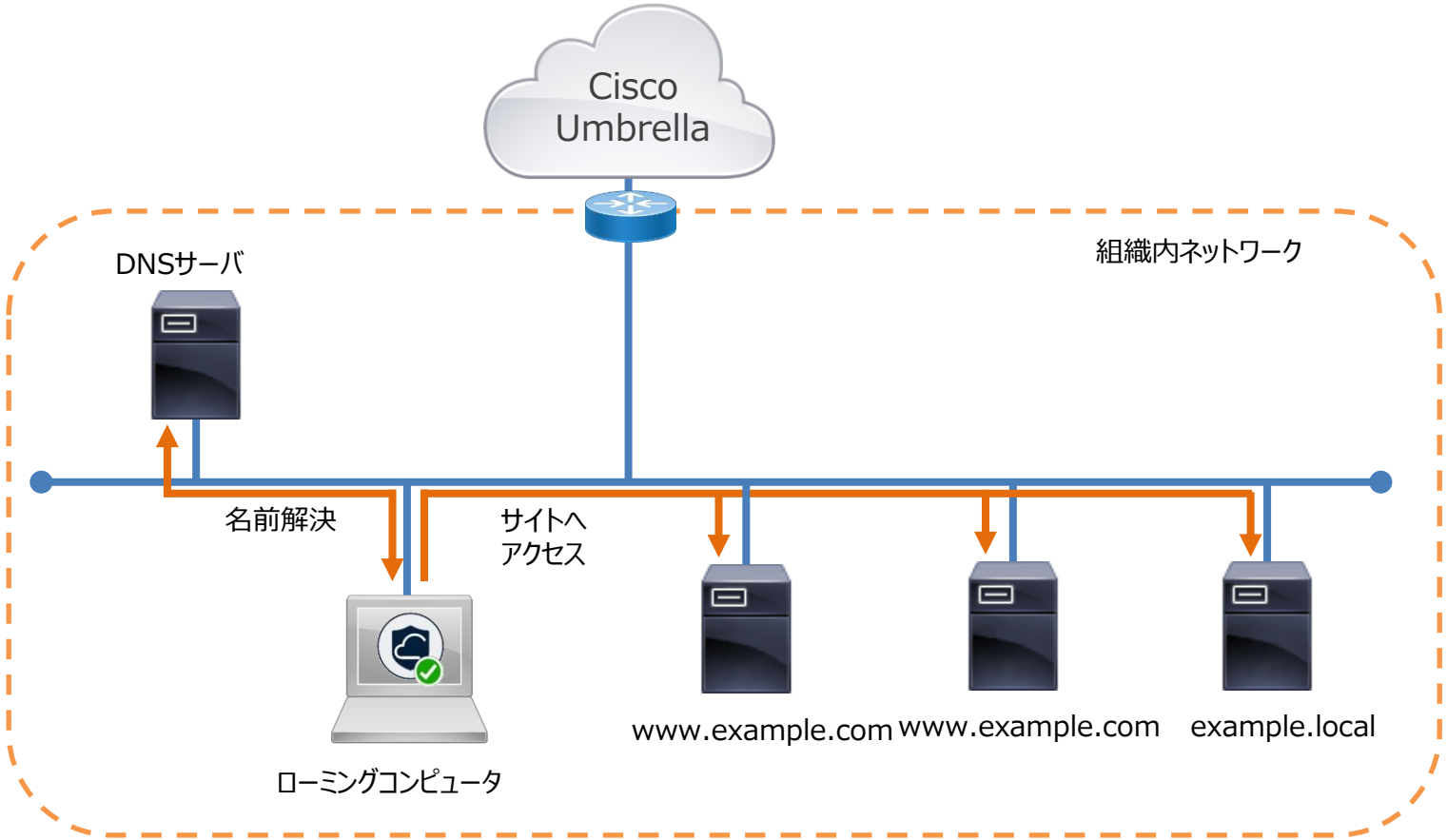
デフォルト動作では、Cisco Umbrella はユーザー PC 上で生成された 全てのDNS クエリを Umbrella に転送し、そのクエリを検査/ブロックすることでセキュリティ機能を提供しています。
しかし、組織内のサーバに対する名前解決までもが組織外にある Umbrella によって行われますので、組織内のコンテンツにアクセスできなくなる問題が発生します。これに対応できるようにUmbrella Dashboard の「内部ドメイン」という設定で組織内のドメインを定義できるようになり、PC 上で生成された DNS クエリーのうち、組織内のドメインの DNS クエリだけを Umbrella 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。



7-17. ドメイン管理 2/4

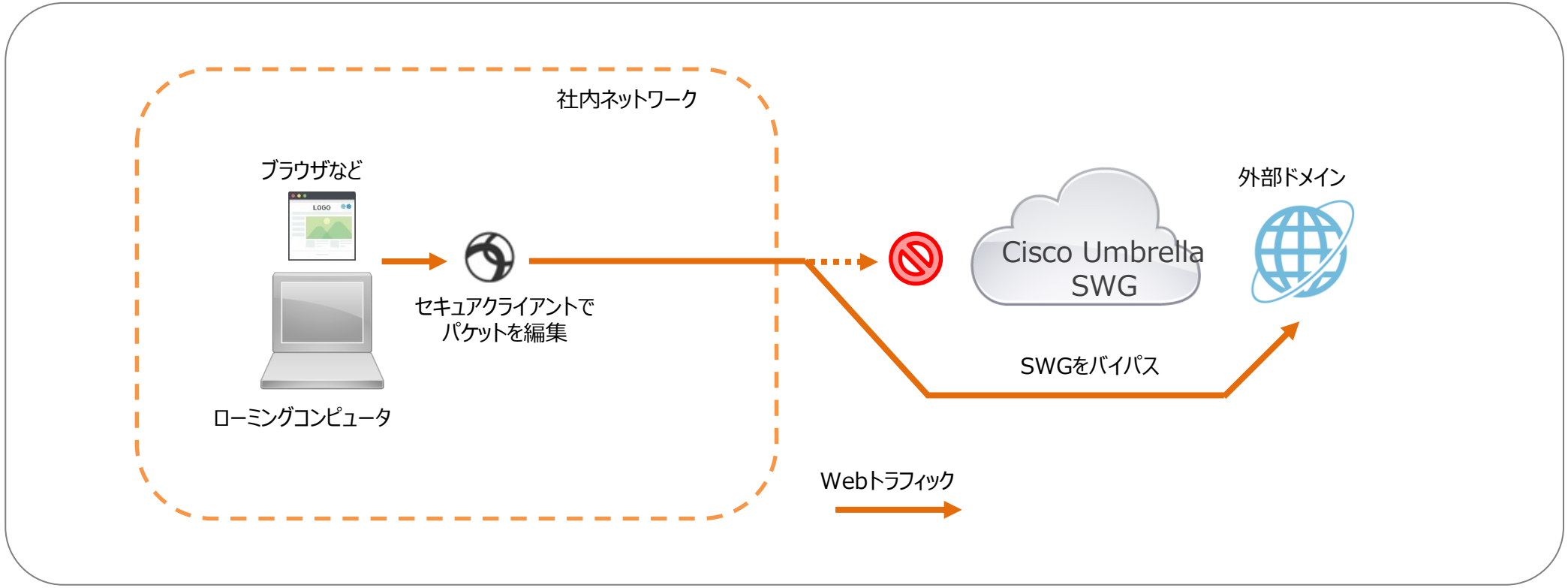
ドメインの追加画面「 導入 → ドメイン管理 → 追加 」では Umbrella に直接ルーティングしないトラヒックの内部ドメインリストを作成します。
リスト化したドメインはUmbrellaではなく、組織内ネットワークに属するDNSサーバ等で名前解決をします。
①例として、「example.com」ドメインを追加した際の動作を以下に示します。
「example.com」を追加した場合、「www.example.com」や「ftp.example.com」といったとすべてのサブドメインが内部ドメインとして処理されます。
また、「.local」ドメインの場合は、事前に内部ドメインリストに登録されているため設定不要です。
②「適用先」では内部ドメインの適用先を選択できます。
「サイト」は「導入 > 設定 > サイトとActive Directoryで定義したサイト」を、「デバイス」はローミングコンピュータに該当します。
適用例として、「サイト」に適用し、「デバイス」には適用しない場合、サイトからのトラフィックのみがローカルリゾルバを使用する動作となります。

ドメインの追加画面



7-17. ドメイン管理 3/4

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

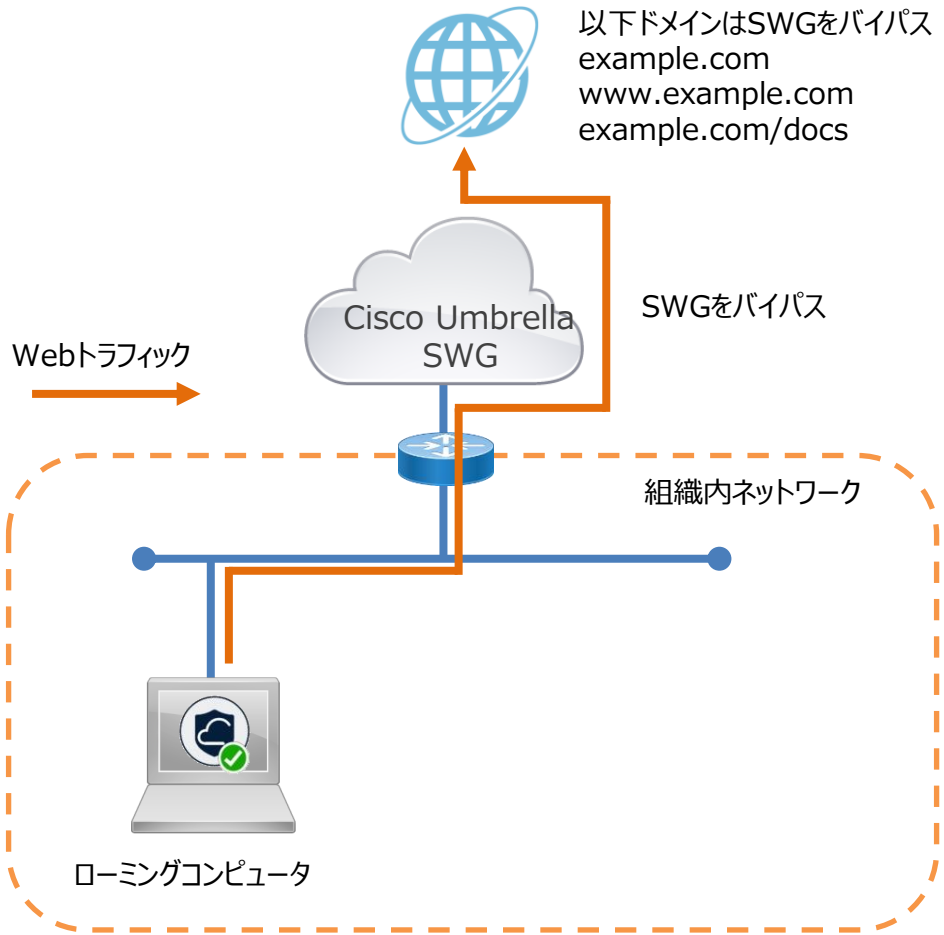


7-17. ドメイン管理 4/4

ドメインの追加画面「 導入 → ドメイン管理 → 追加 」にて、SWGを経由しない外部ドメインのリストを作成します。
①「ドメインタイプ」では「外部ドメインおよびIP」を選択し、②「エンティティ」にはSWGを経由せずに直接通信を行いたいWebサイトの「ドメイン、IPまたはCIDR」を入力します。以下に「エンティティ」に「example.com」を設定した際のWebトラフィックの動作イメージを示します。
また、以下表に記した通り、ドメインリストに追加するとすべてのドメインには、左側と右側に暗黙のワイルドカードが適用され、表に示したドメインが外部ドメインとして処理されます。ただし、Umbrellaのドメインリストはアスタリスク(*)をサポートしていません。そのため、アスタリスク(*)を使用して、ドメインの一部をワイルドカードとして登録することはできません。

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

ドメインの追加画面



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

8. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

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

① 1人目の管理者は開通メール記載の右記URLをクリック（https://sign-on.security.cisco.com/signin/register）
　2人目の管理者は受信した電子メールから枠内の [here]をクリック

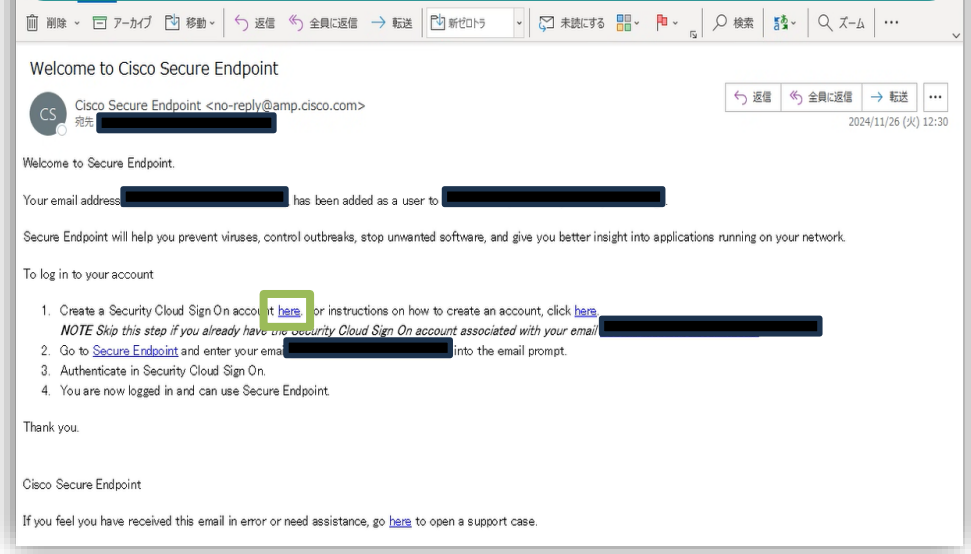
① [Email※1]、[First name]、[Last name]、[Country]、[Password※2]を入力し、規約の同意にチェック
※1Emailには申込書に記載したメールアドレスを記入ください　※2設定するパスワードには条件があります（図の②右部をご参照ください）

③ [Sign up]をクリック

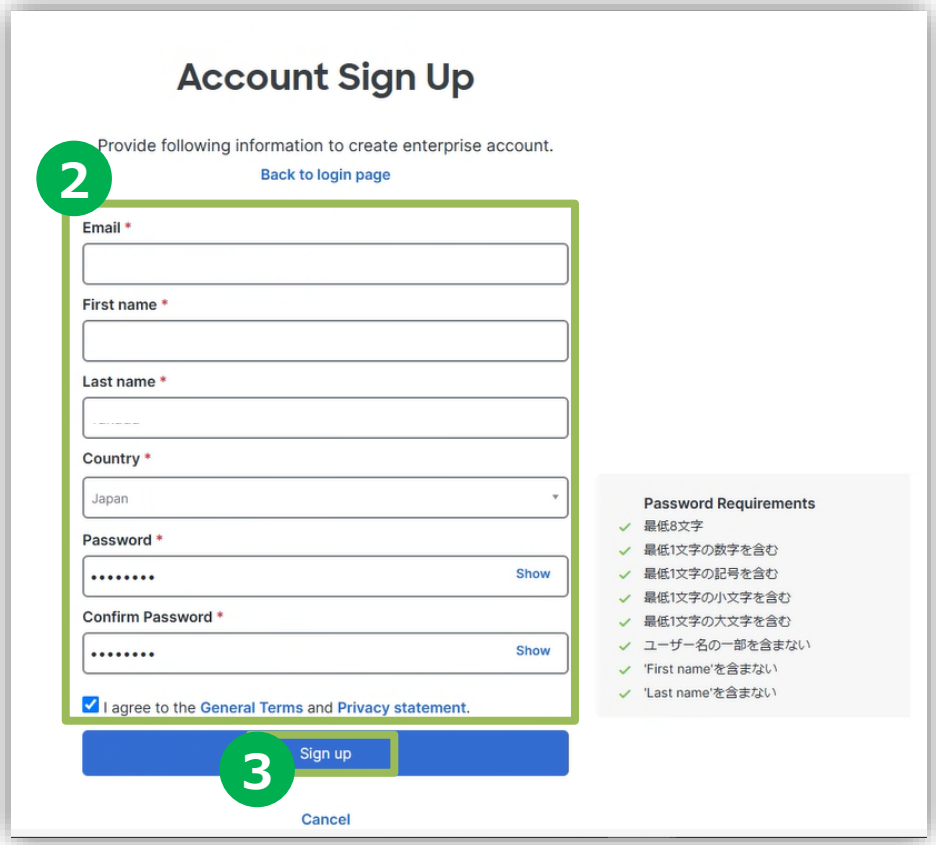
1人目の管理者

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

2人目の管理者

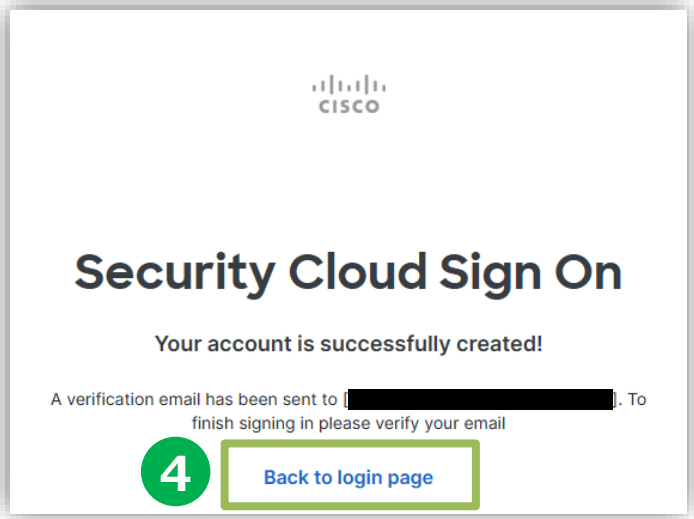


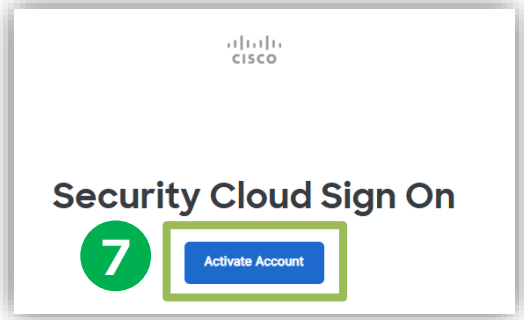
1



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＞

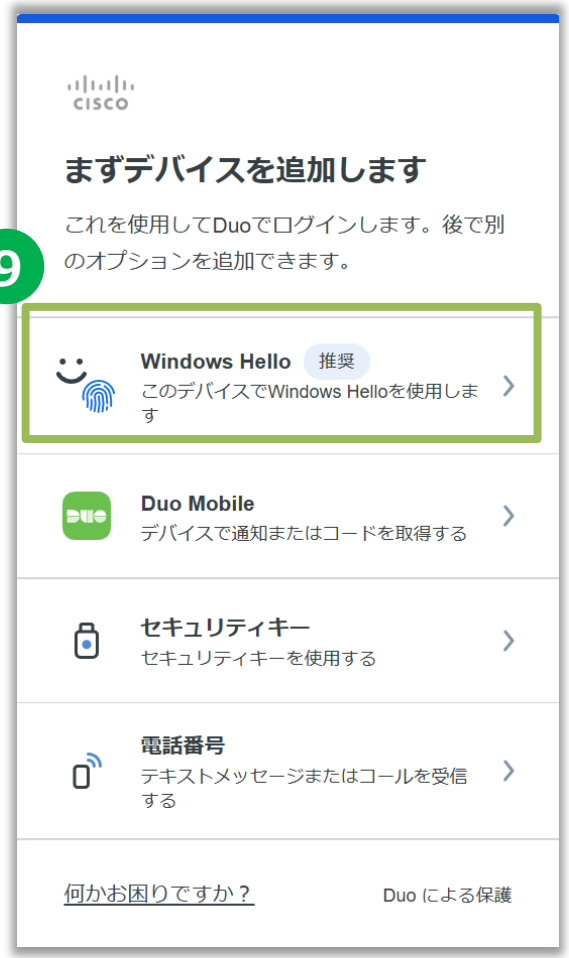
④ [Back to login page]をクリックし、ブラウザを閉じます。
⑤ 受信した電子メール[件名：Activate Account]を開き、
[このメッセージをテキスト形式に変換しました]をクリックしてHTMLとして表示させます。
⑥ [Activate account]をクリック
⑦ [Activate Account]をクリック





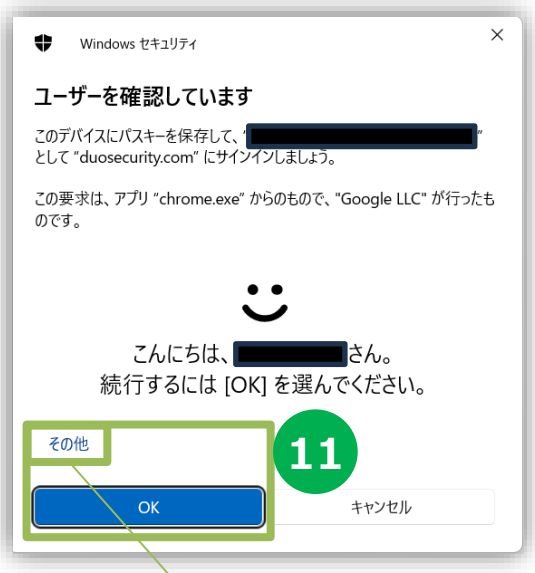
8. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

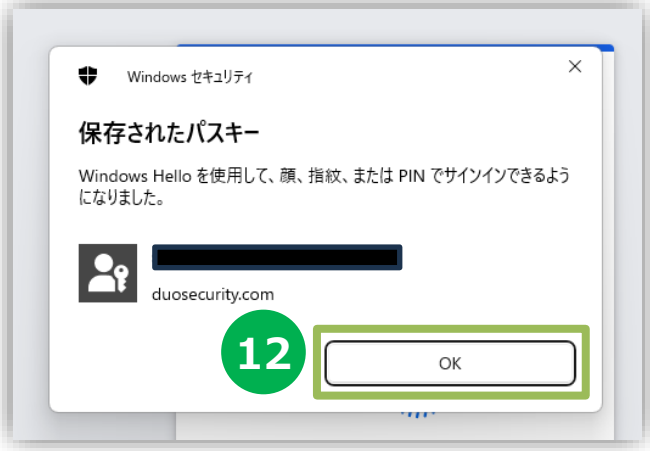
⑧ [始める]をクリック
⑨ [Windows Hello]をクリック　※二段階認証を設定してください。マニュアル上では[Windows Hello]を使用し顔認証を設定しています。
⑩ [続行]をクリック



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。

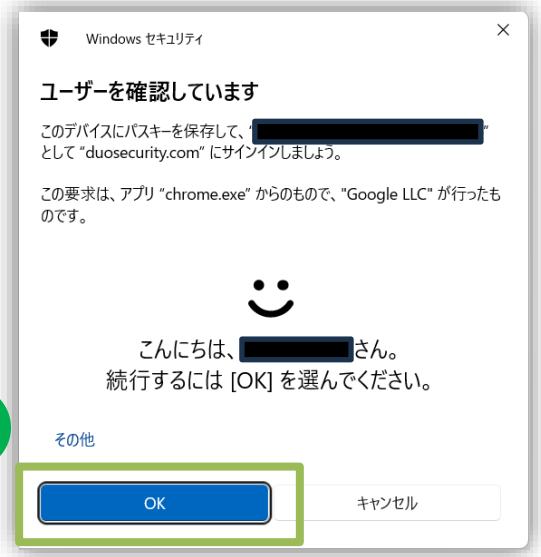


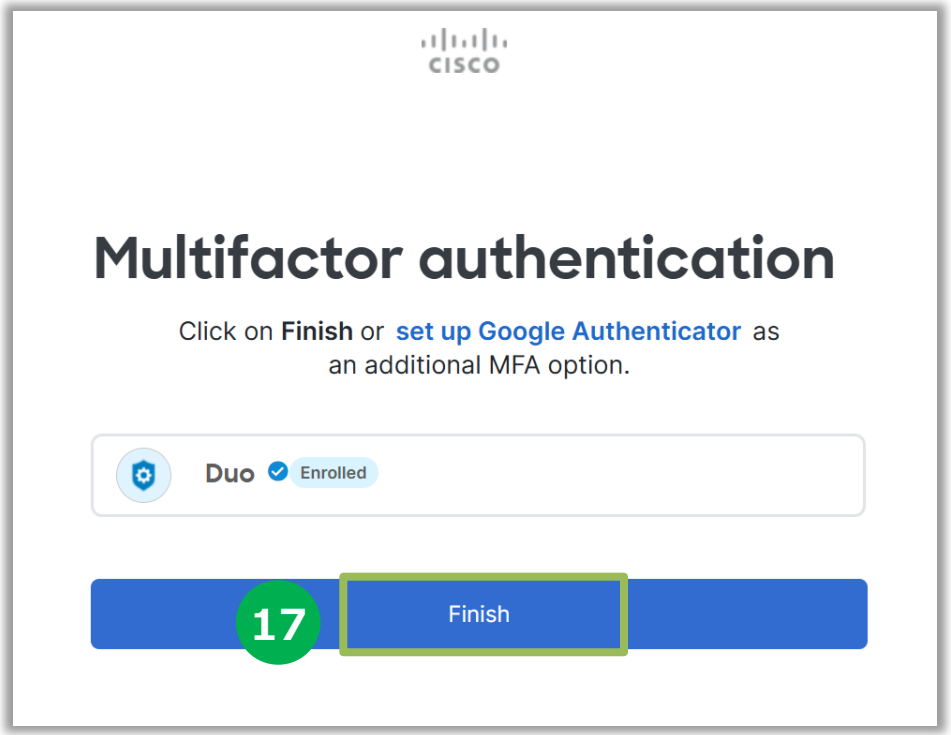


指紋認証が表示される場合はその他から顔認証を選択下さい

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

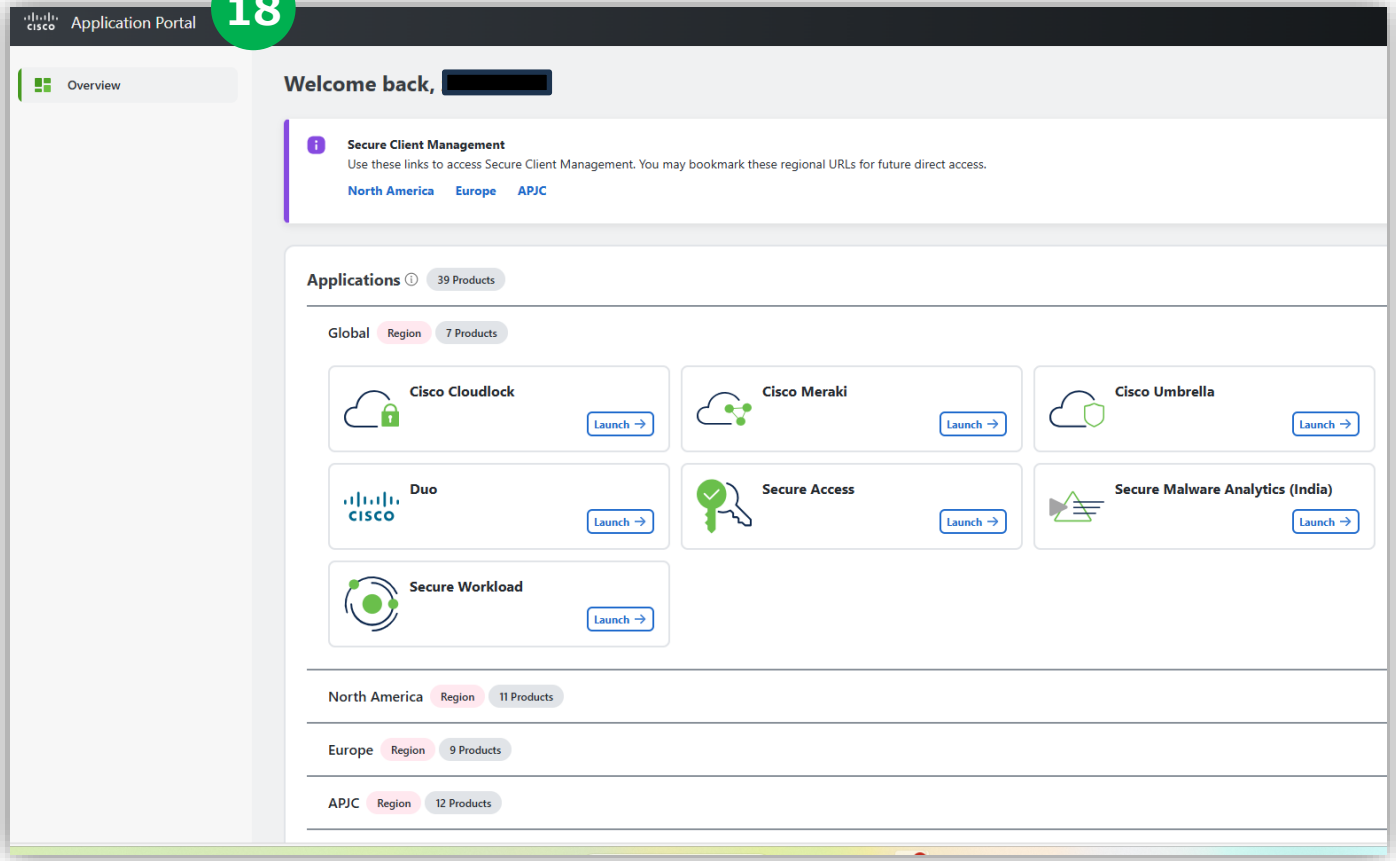




8. コンソールへのログイン手順＜管理者アカウント 初回ログイン＞

⑱ 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。
⑲ 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

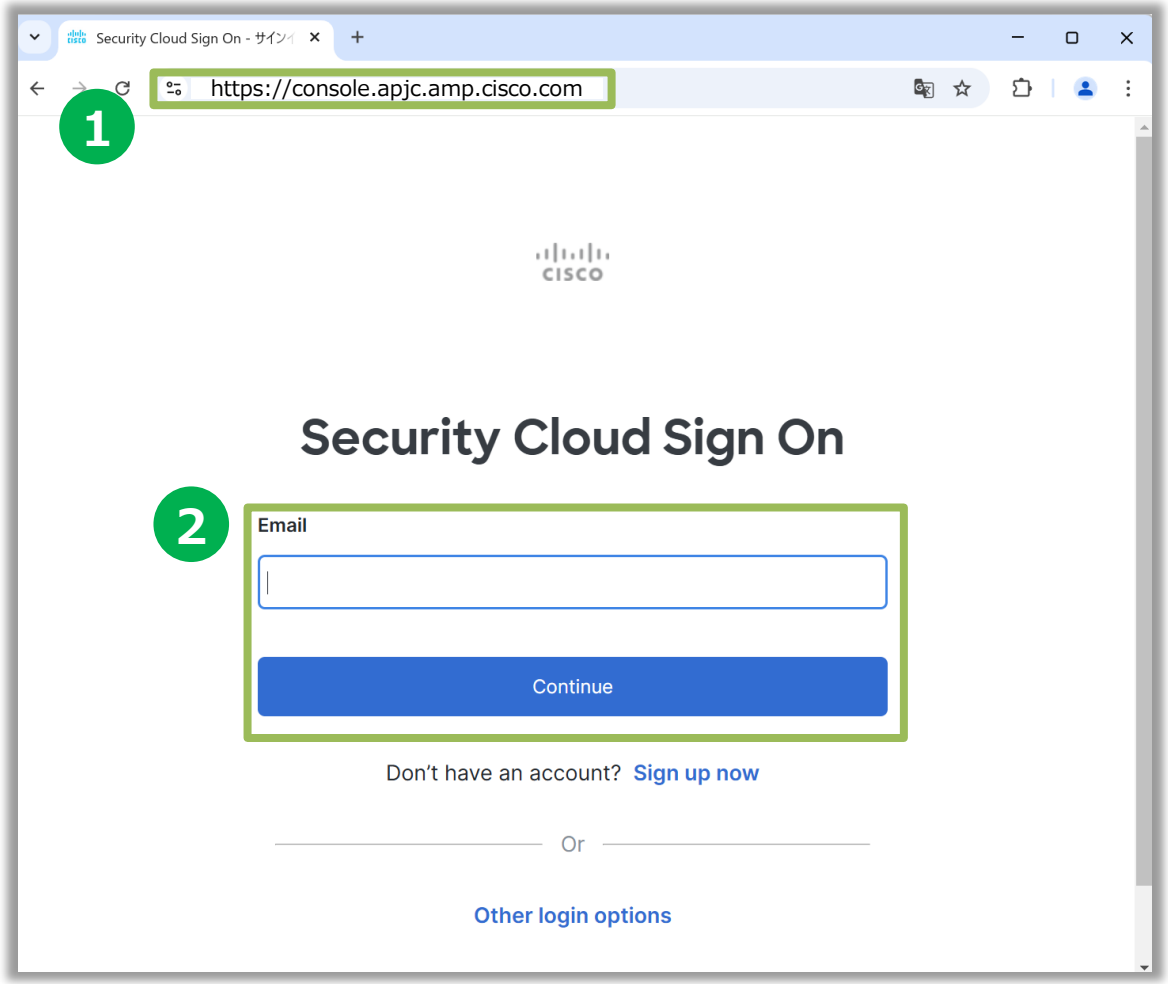
18

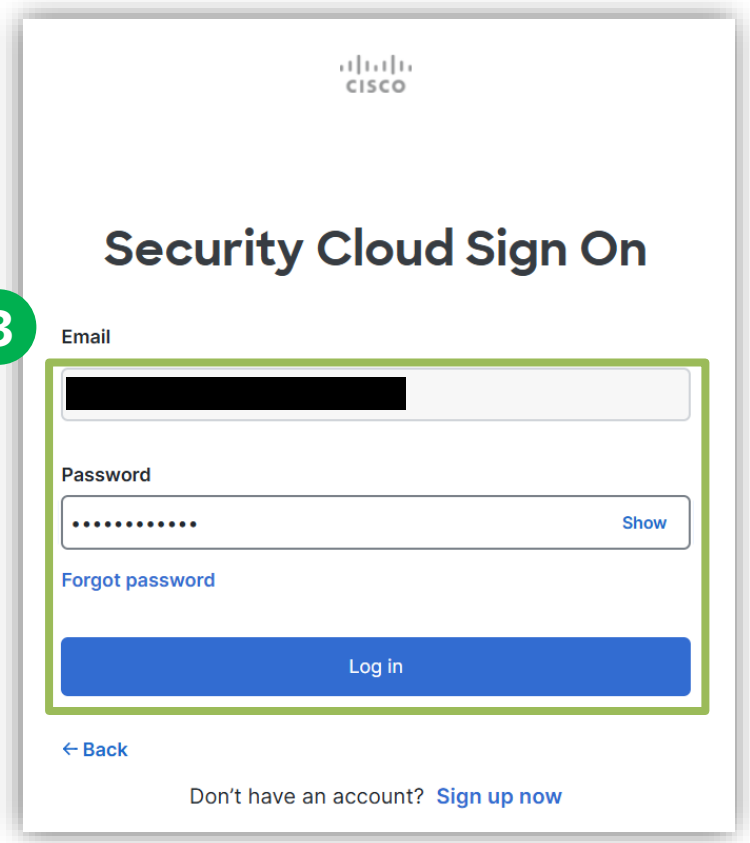


19

8. コンソールへのログイン手順 <システムログイン>

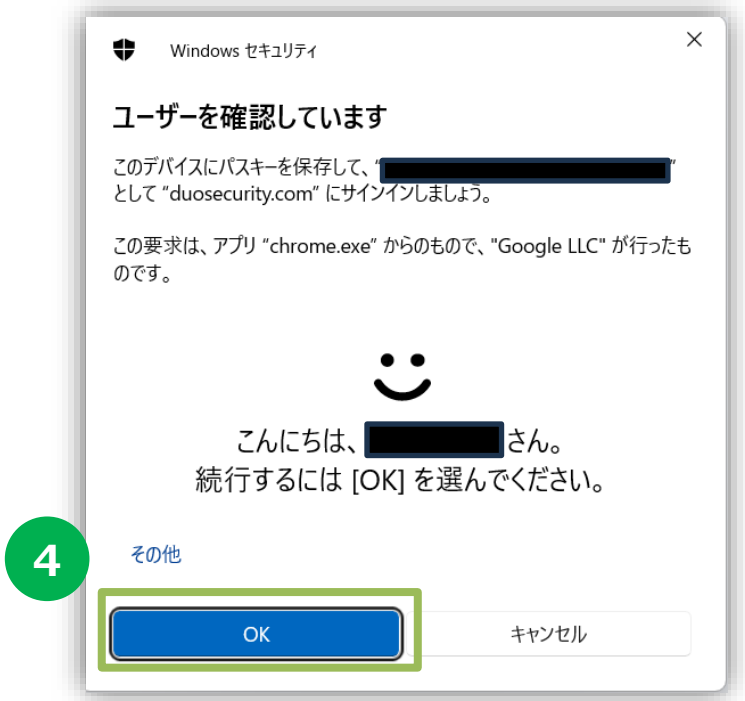
Cisco Secure Endpoint管理コンソールへログインするまでの手順を示します。
① 以下のURLへアクセス
https://console.apjc.amp.cisco.com
② Email欄に[メールアドレス]を入力し、[Continue]をクリック
③ [パスワード]を入力し、[Log in]をクリック





8. コンソールへのログイン手順 <システムログイン>

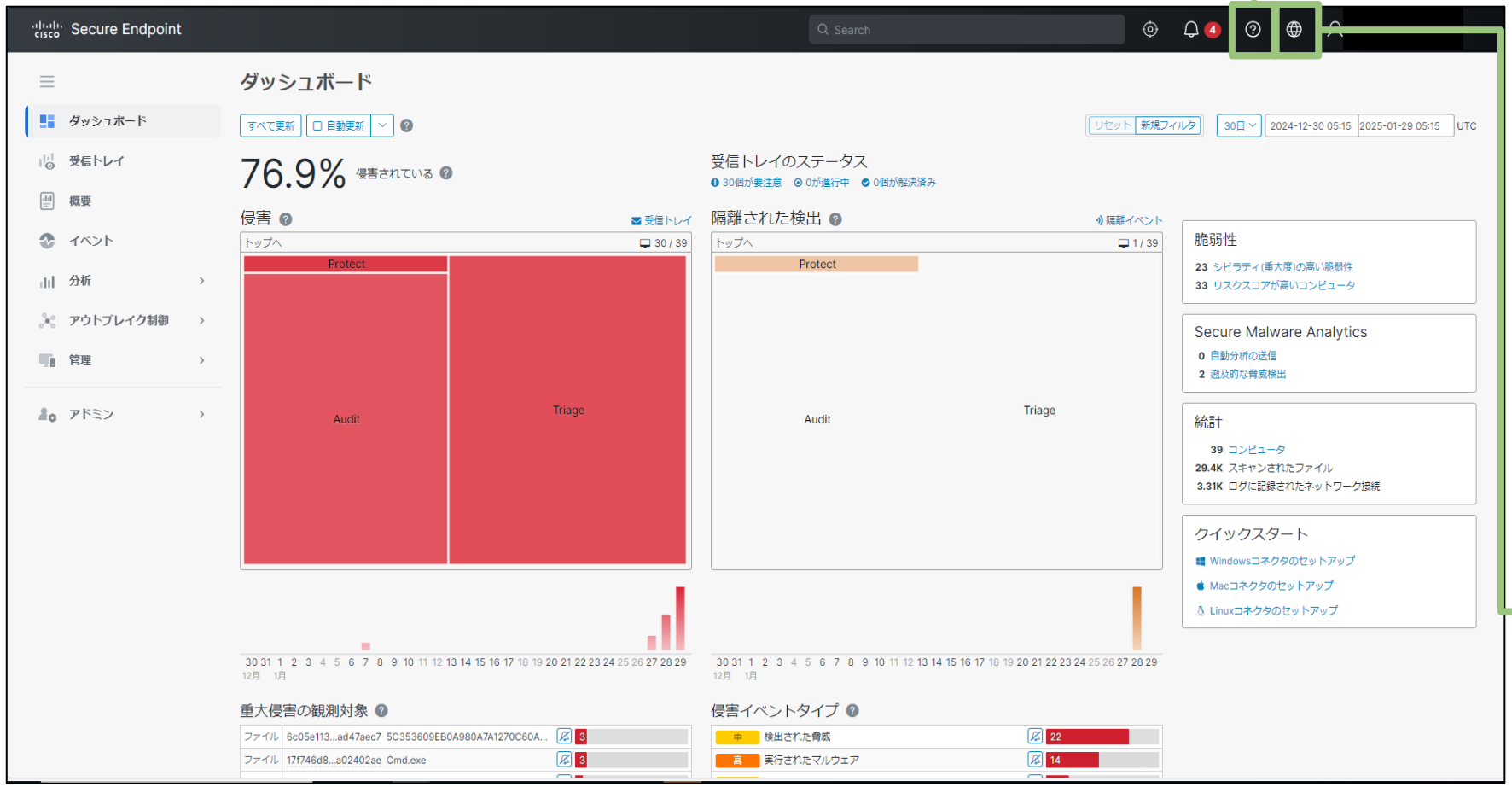
④ 設定した2段階認証を実施 ※以下はWindows Helloで顔認証を実施しています。
⑤ 認証が成功し、Cisco Secure Endpointの管理コンソール画面が表示されることを確認



8. コンソールへのログイン手順 <ダッシュボード説明>

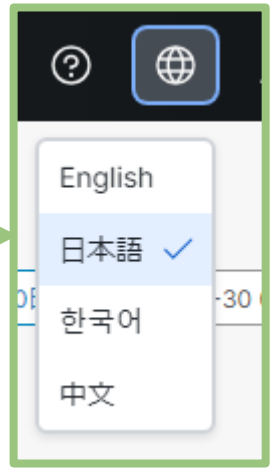
ログイン後最初に開くページです。
社内のマルウェア感染状況を一覧で確認することが可能です

ヘルプ、およびヘルプ目次、リリース
ノート、サポートへの問い合わせリンク



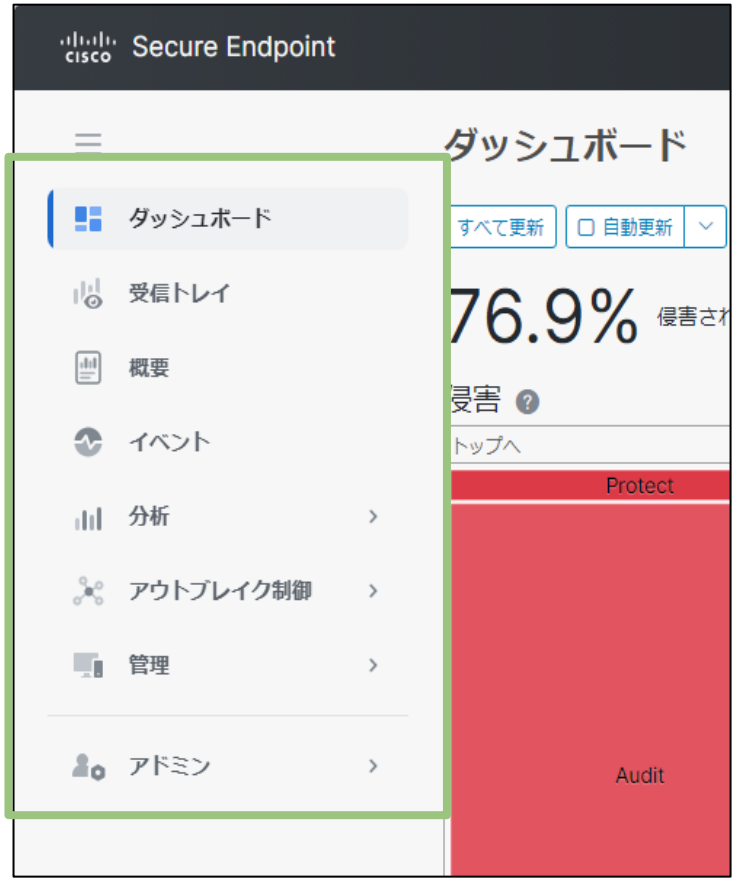
不明な点はこちらに説明が
記載されております。

＜言語設定＞



8. コンソールへのログイン手順＜管理メニュー＞

各操作項目の概要を以下に記載します



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

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

9. セキュアエンドポイント機能を設定変更する（設定変更例一覧）

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

トラブル対応による設定変更例

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

ご利用環境等に応じた設定変更例

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

9-1. ウィルスに感染したかもしれない 1/5

セキュアエンドポイント

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

1. 該当端末をネットワークから切断する

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

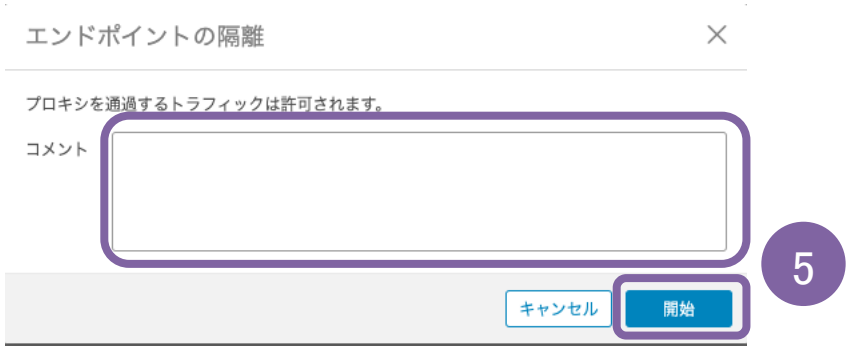
2. Secure Endpointでの手動隔離の実施

同じネットワークで別の端末(パソコン等)をご利用の場合、全てのパソコンで実施してください。
①Secure Endpointのダッシュボードを開きます。
②[管理] をクリックし、
③「コンピュータ」を選択します。

2. Secure Endpointでの手動隔離の実施（つづき）

④感染が疑われるコンピュータを選択し、「隔離の開始」のクリックします。

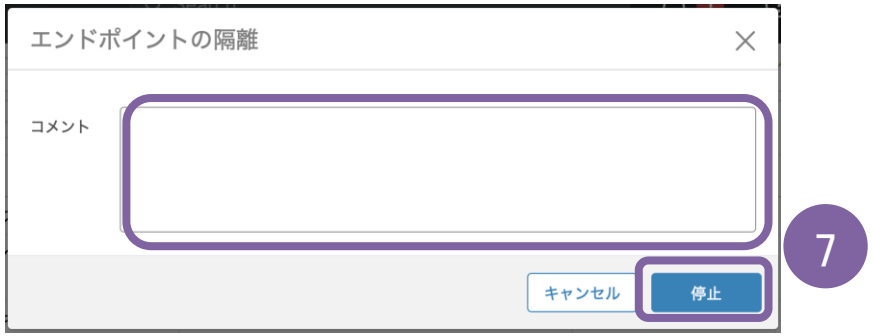
⑤任意でコメントを記載し、「開始」をクリックします。



2. Secure Endpointでの手動隔離の実施（つづき）

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

⑦任意でコメントを記載し、「開始」をクリックします。



参考

下記の症状がみられる場合、パソコンがウイルスに感染している場合があります。

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

※9～12はパソコン本体のトラブルでも発生する場合があります。

主な感染経路

インターネットサイトからの感染

Webブラウザー(インターネットを表示するソフト)の脆弱性を利用した感染方法が増加してきており、ホームページを閲覧するだけでウ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いまい、本人に成りすましたメールが多数送信されるケースが発生してしまい、被害が増加しています。不明な送信元だけでなく、送信元が社内や取引先の相手でも注意が必要です。

電子メールのHTMLスクリプト

電子メールの形式がHTMLメールの場合、ウ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ておくことができます。ご利用のメールソフトで、HTMLメールのスクリプトを自動的に実行する設定となっている場合、電子メールを表示しただけでウ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。

9-2. 自分の名前で勝手にメールが送られている

セキュアエンドポイント

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。

1

9-3. セキュアエンドポイントをインストールしたい

下記手順に従って、対象のソフトウェアをインストールしてください。

① Secure Endpoint をインストールする方法

p8-41を参照ください。

9-4. パソコンを買い替えたのでセキュリティソフトを入れなおしたい

セキュアエンドポイント

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

① Secure Endpoint をインストールする方法

p8-41を参照ください。

9-5. 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

セキュアエンドポイント

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

① Secure Endpoint をアンインストールする方法

p42-53を参照ください。

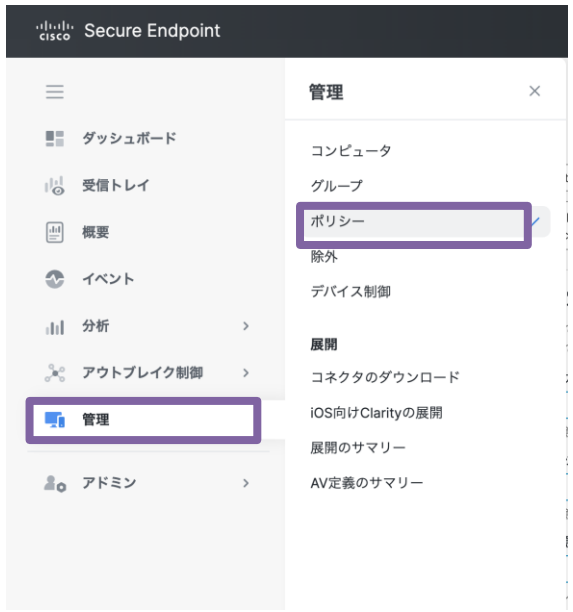
9-6. 検知エンジンの動作モードを確認・変更したい 1/2

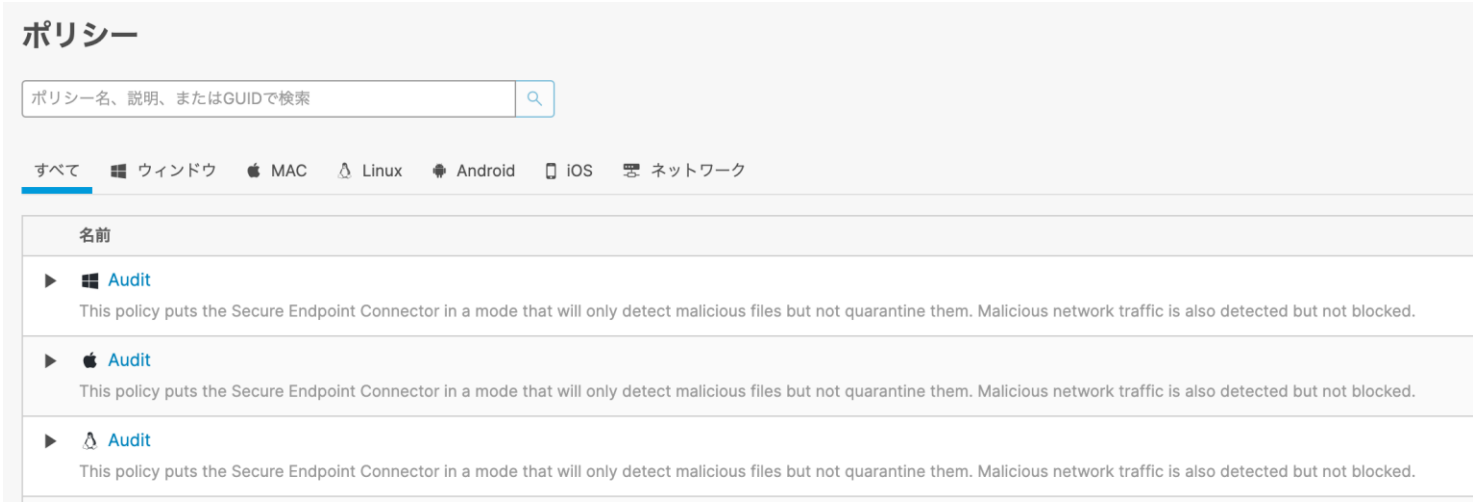
セキュアエンドポイント

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。





9-6. 検知エンジンの動作モードを確認・変更したい 2/2

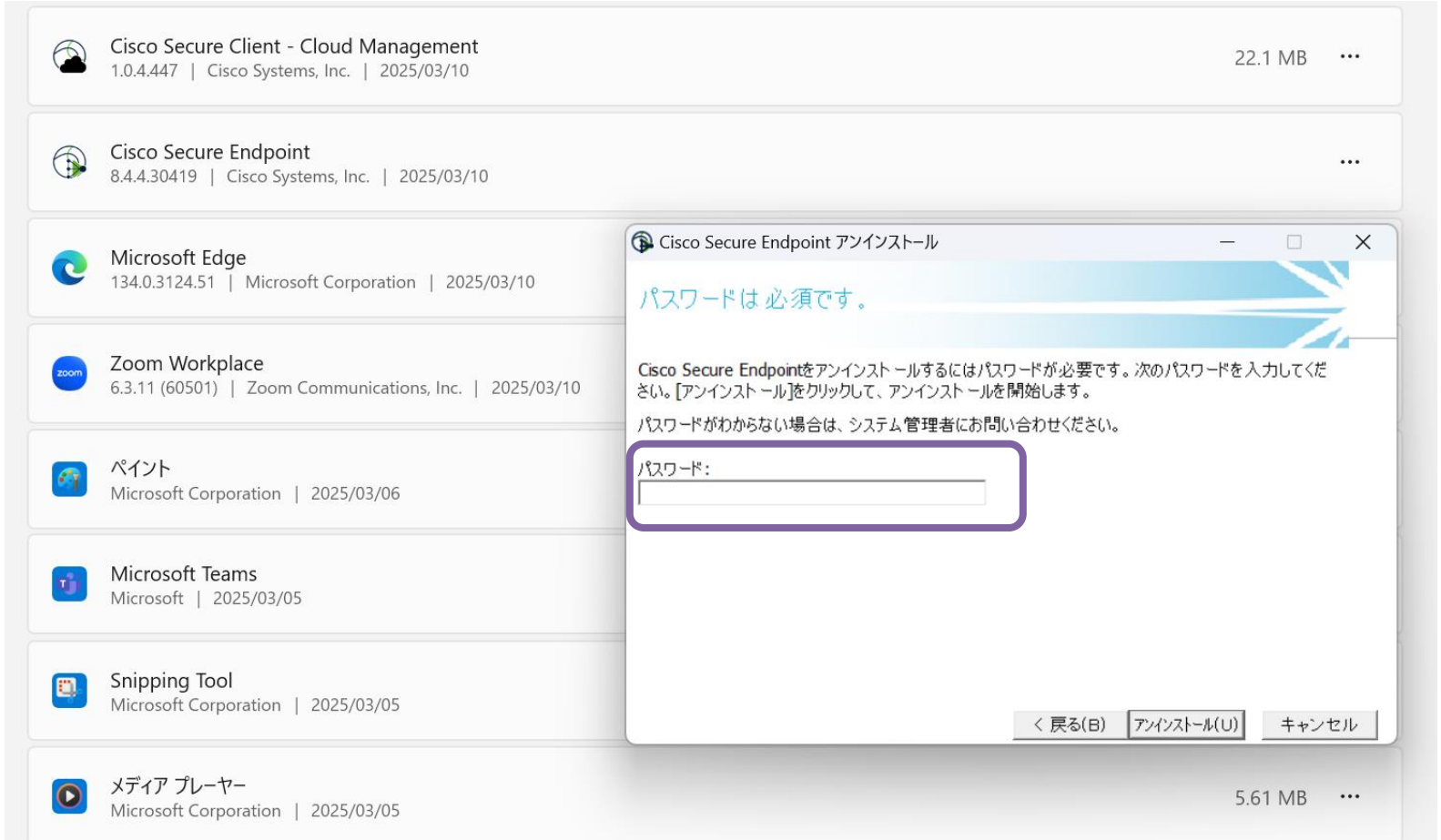
②それぞれ動作モードを変更できます。各項目で、「検疫」「ブロック」「監査」「無効」がありますが、一部動作の仕組み上選択できないモードがあります。
（例：「ファイル」では検疫・監査のみ）

9-7. アインインストール時のパスワードロック方法（コネクタ保護の有効化） 1/6

セキュアエンドポイント

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

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

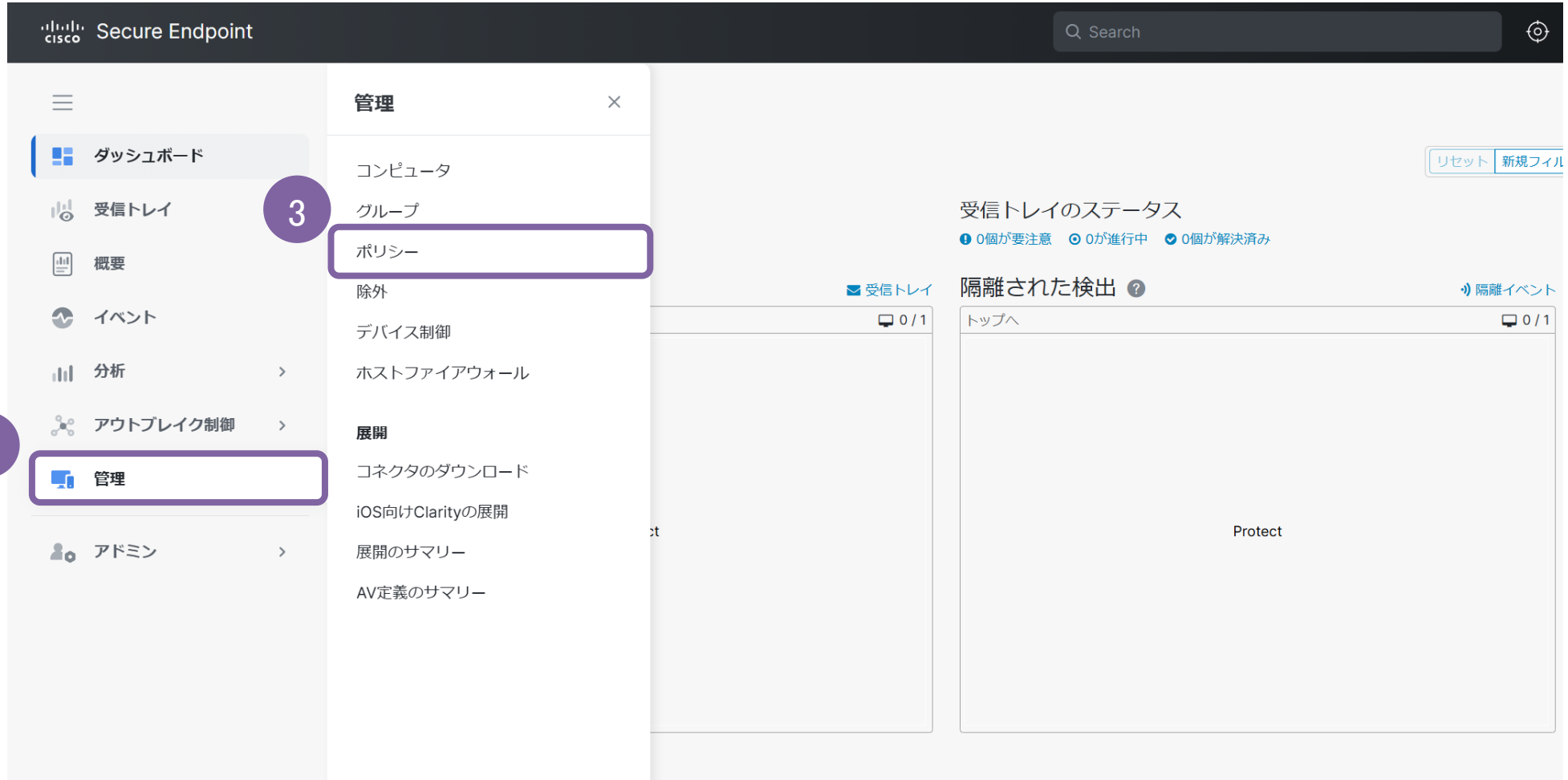


アインインストール時のパスワードロック方法

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

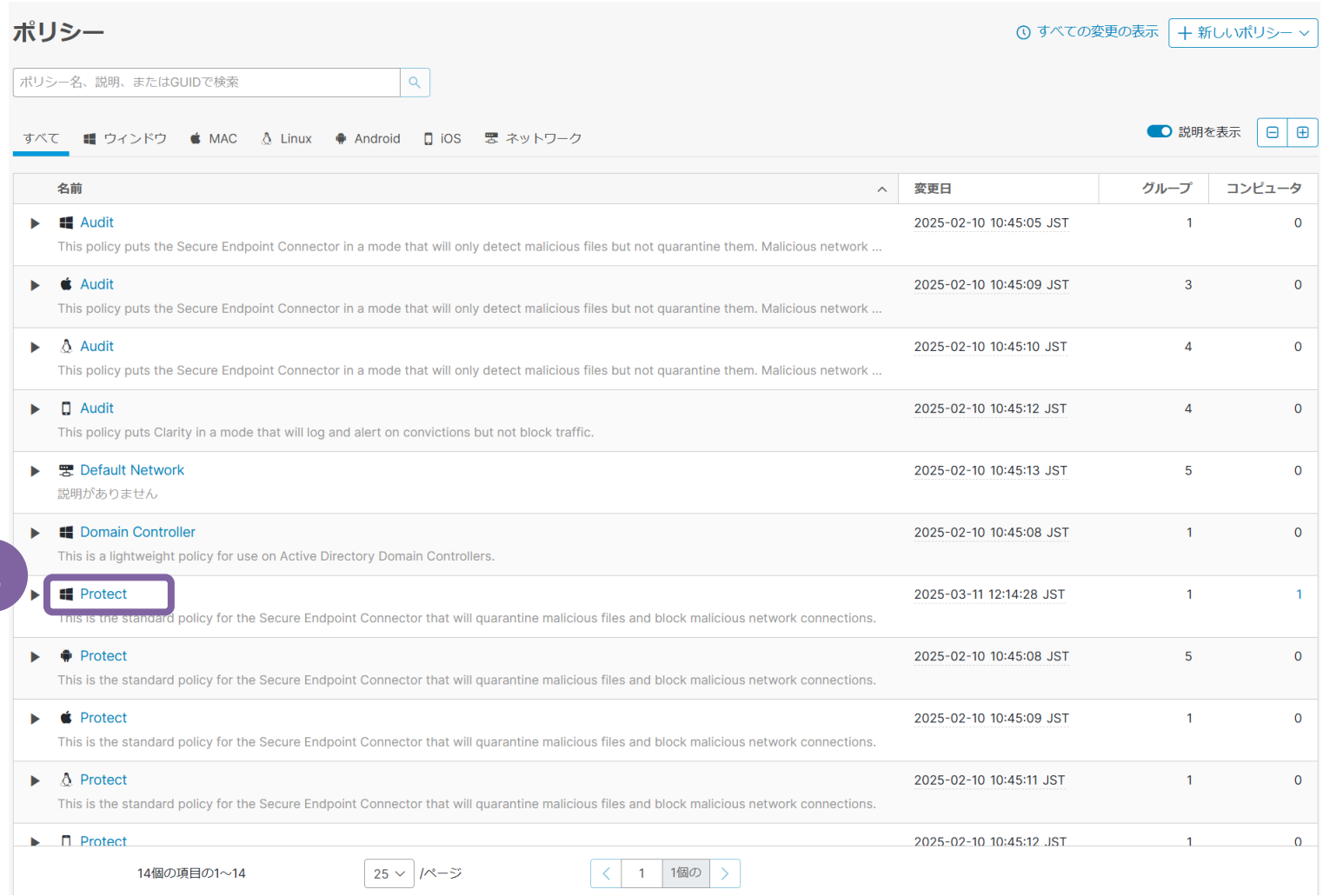
アインインストール時のパスワードロック方法（続き）

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



アインインストール時のパスワードロック方法（続き）

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

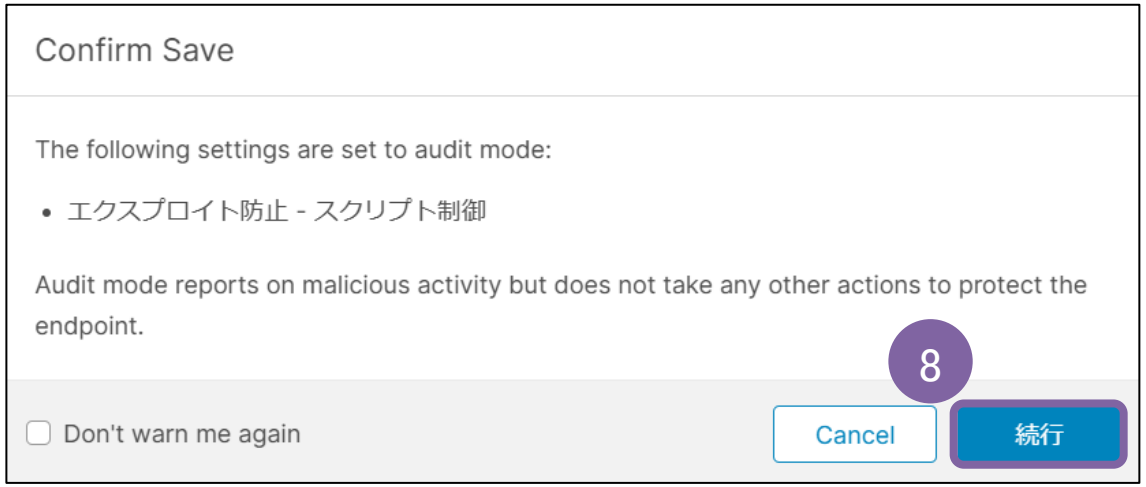


アインインストール時のパスワードロック方法（続き）

⑤「詳細設定」→「管理機能」をクリックします。
⑥「コネクタ保護の有効化」にチェックを入れて、「コネクタ保護のパスワード」にアンインストール時に入力必須なパスワードを設定します。
⑦「保存」をクリック

アインインストール時のパスワードロック方法（続き）

⑧確認画面が表示されたら「続行」をクリックし、設定を完了します。



9-8. 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 1/11

セキュアエンドポイント

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

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

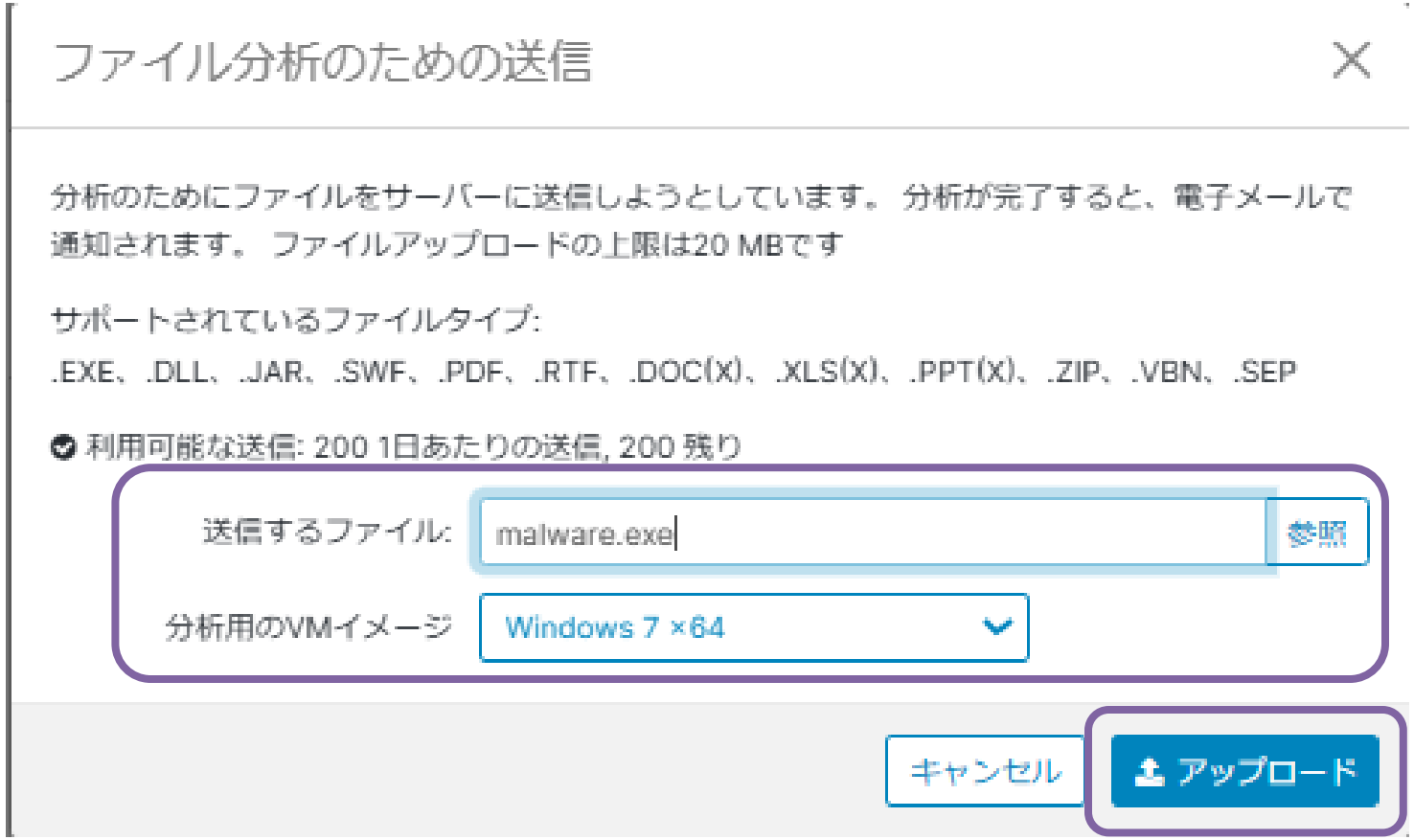
ファイル分析の利用方法

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はCisco Secure Endpoint 管理コンソール上からの直接ファイルアップロードになります。以下手順を説明いたします。

①Cisco Secure Endpoint 管理コンソールにて分析> ファイル分析 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。

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

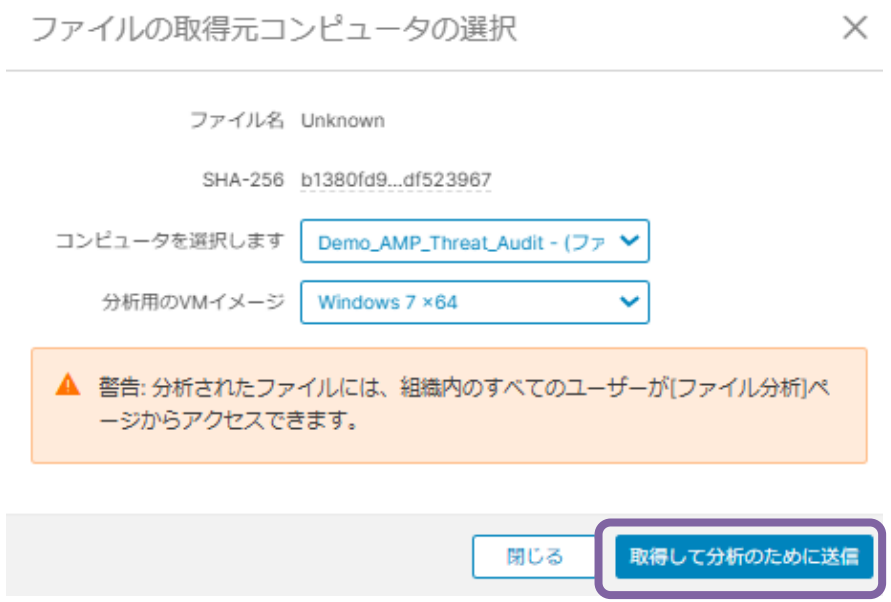
Secure Endpointによって、端末上で マルウェアのファイルが隔離されてしまった場合、隔離されたファイルは無効化された状態で保存されているため、端末からファイルを取得して、Cisco Secure Endpoint管理コンソール からアップロードするのは不可能となります (厳密に言えば一旦リストアすれば可能ですが、それでは再び悪影響が出ます) 。また、仮に マルウェアの情報源となったサーバ等から検体を取得できたとしても、マルウェア を直接、業務端末にダウンロードすることは危険が伴い、組織のセキュリティポリシー上好ましくない場合がございます。

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。

隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

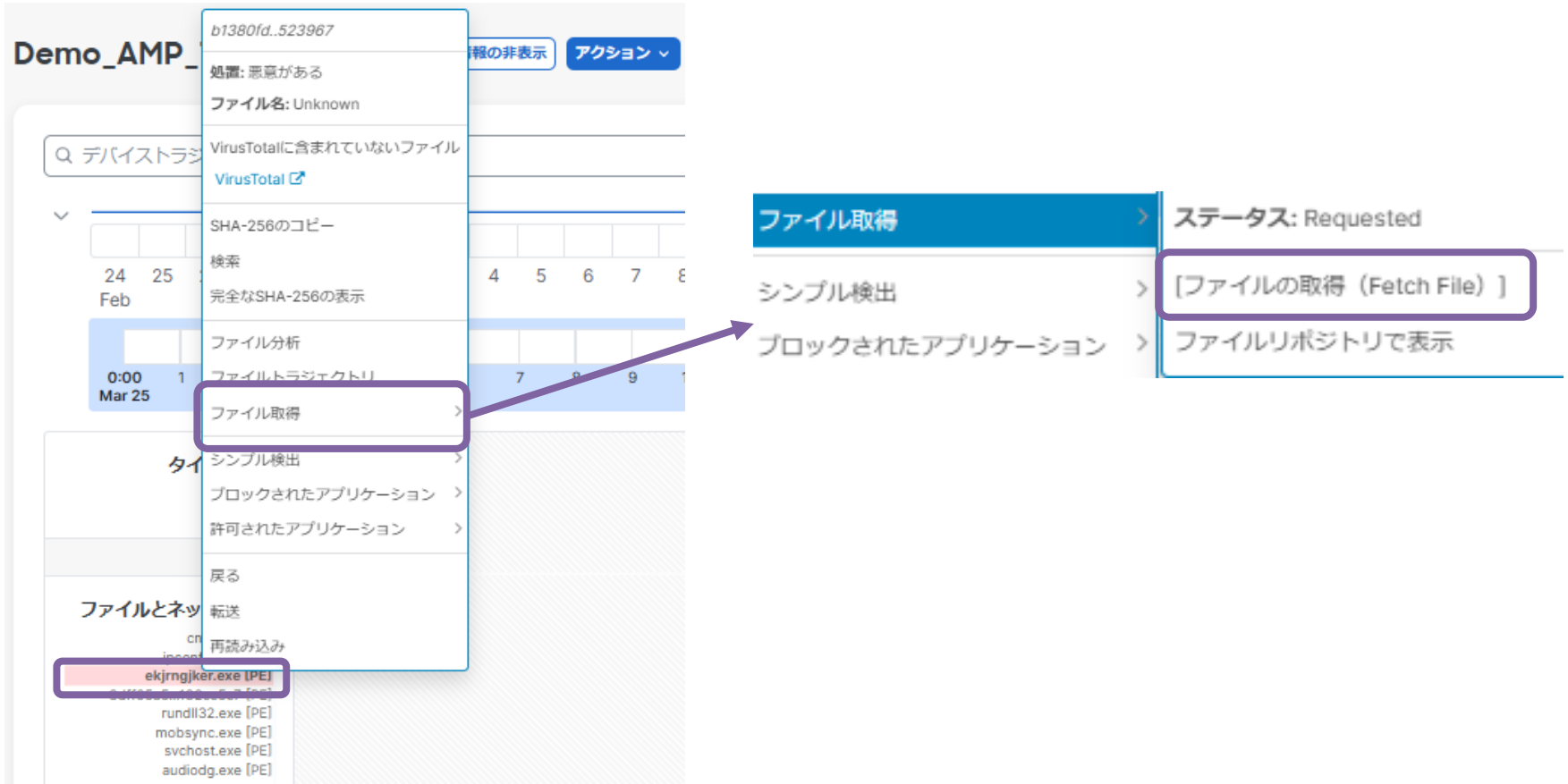
②分析 をクリックし、ファイル分析のための情報 (どの端末からファイルを取得するのか、どの種類の OS で実行するのか) を入力して、取得して分析のために送信 をクリックします。



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

隔離された/疑わしいファイルをファイル分析へ送る方法（つづき）

③また、隔離されてはいなくても、疑わしいファイルが デバイストラジェクトリ 上にある場合に、直接管理者が取得することを避けたい場合は、デバイストラジェクトリ上から ファイルの取得 にて クラウド 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。



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）

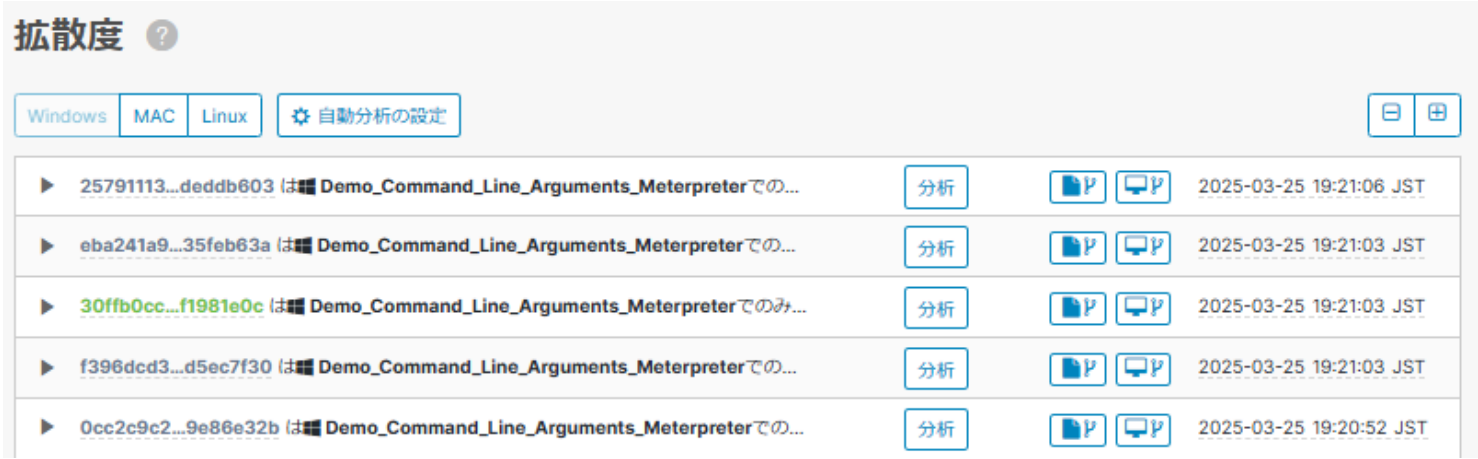
④ 取得したファイルはファイル分析 に自動で送信されないため、一定時間経過後に、分析 -> ファイルリポジトリ で該当ファイルがアップロードされたことを確認し、分析 をクリックすれば、Sandbox で分析することが可能です。

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

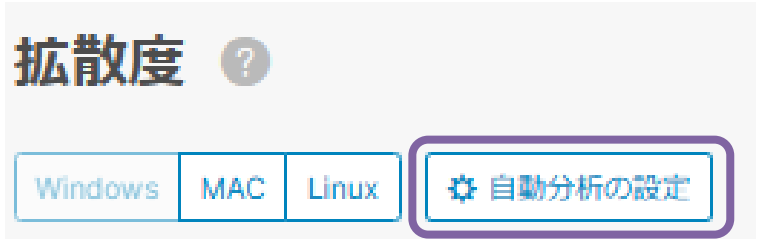
Cisco Secure Endpoint では、低拡散度 と呼ばれる機能があり、ある組織の中であまり実行されていないファイルは Malware の疑いがあるという考えのもと、組織中 (Business) の一つの端末でしか実行されていないファイルをリストアップし、必要に応じて、ファイル分析へ送付させることが可能です。拡散度 は デフォルト設定では、該当ファイルがリストアップされるだけであり、ファイル分析 に送付させるためには、設定が必要となります。

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。



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。

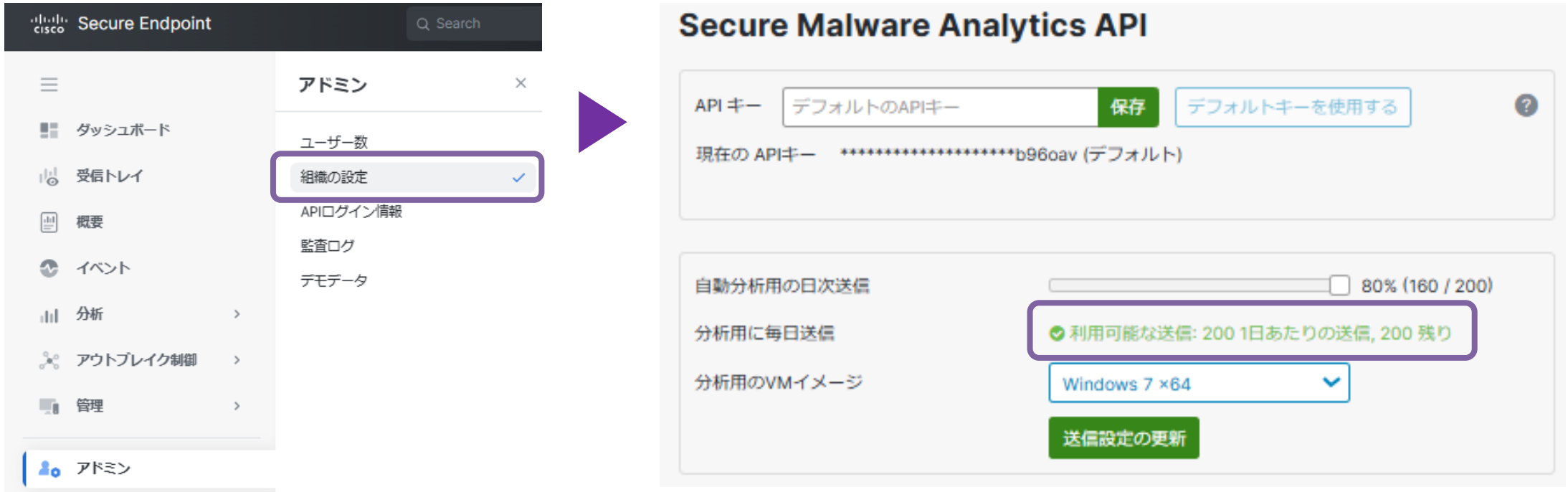


③自動分析の対象となる端末が所属する グループ を指定し、
適用 をクリックすれば、実行頻度の低いファイルを自動的に
Sandbox 分析にかけることが可能です。

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

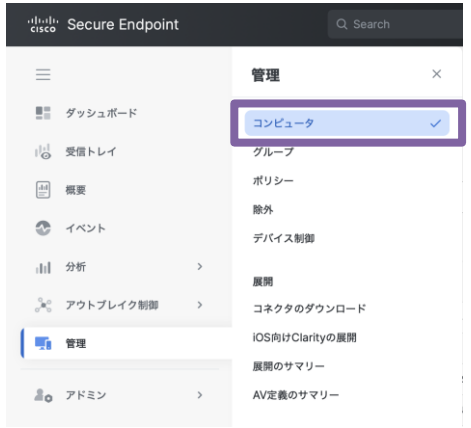


9-9. ファイル隔離が過検知であったので解除したい 1/4

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 Enpointの検査対象から除外するように、許可リスト(ホワイトリスト)へ登録いただく方法がございます。

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

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

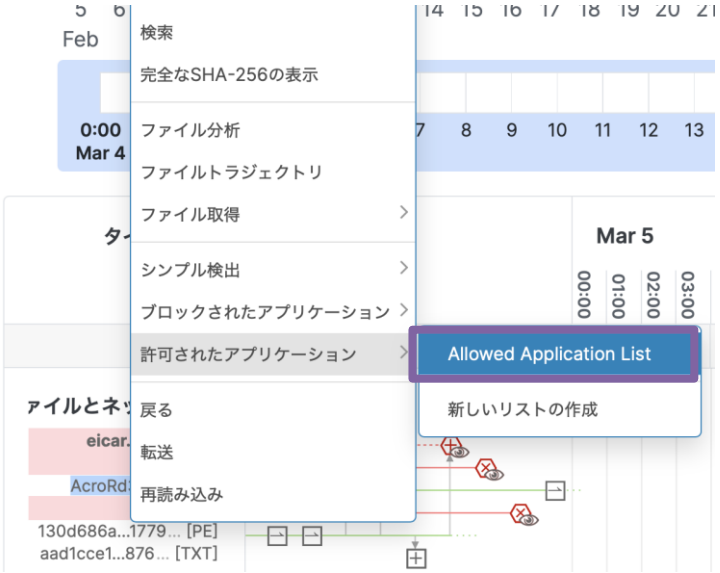


②端末情報を展開すると、デバイストラジェクトリというリンクが表示されるので、それをクリックします。

9-9. ファイル隔離が過検知であったので解除したい 2/4

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。

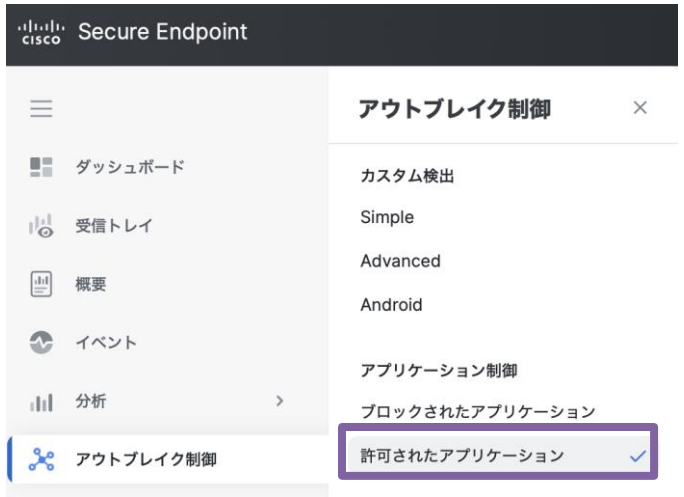


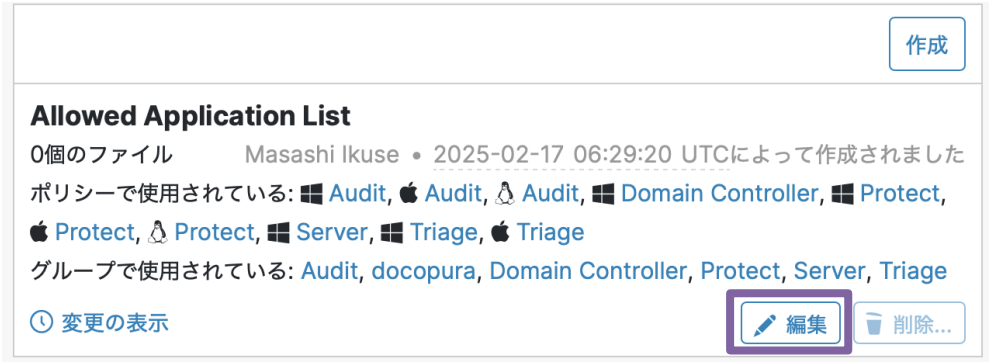
④サブメニューが表示されたらAllowed Application List を選択します。レ点が表示されていれば許可リスト（ホワイトリスト）への登録が完了です。

9-9. ファイル隔離が過検知であったので解除したい 3/4

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 Enpoint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。

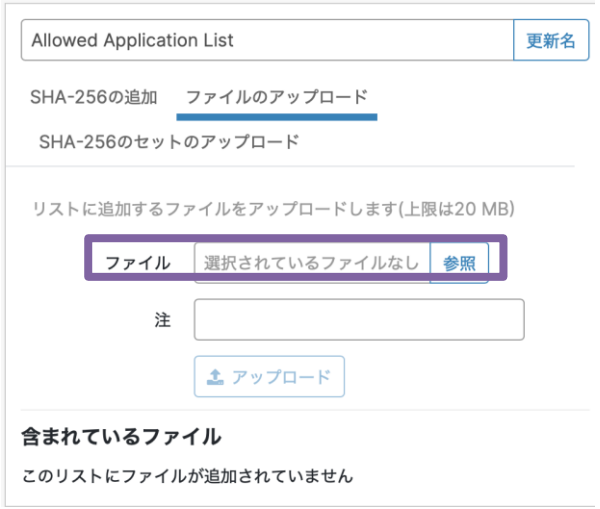




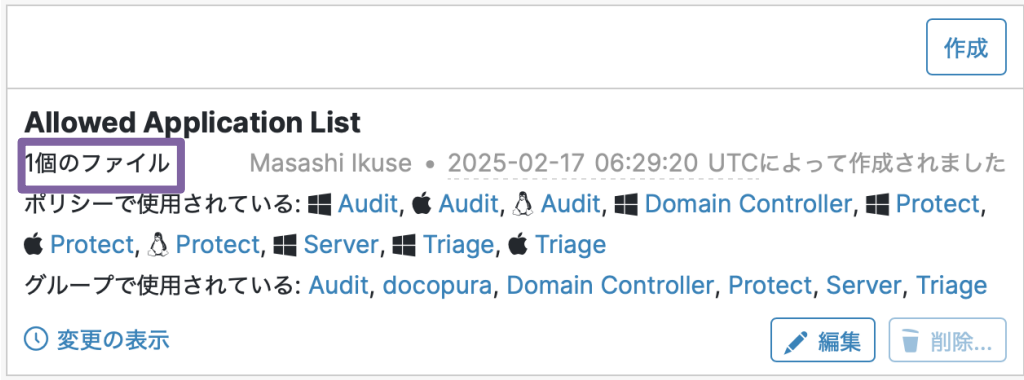
9-9. ファイル隔離が過検知であったので解除したい 4/4

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。



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。



9-10. 隔離されたファイルを復元したい 1/2

セキュアエンドポイント

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

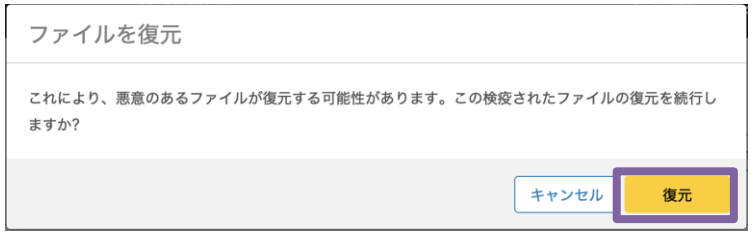
隔離されたファイルの復元方法

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

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 Enpointが正常に動作していること

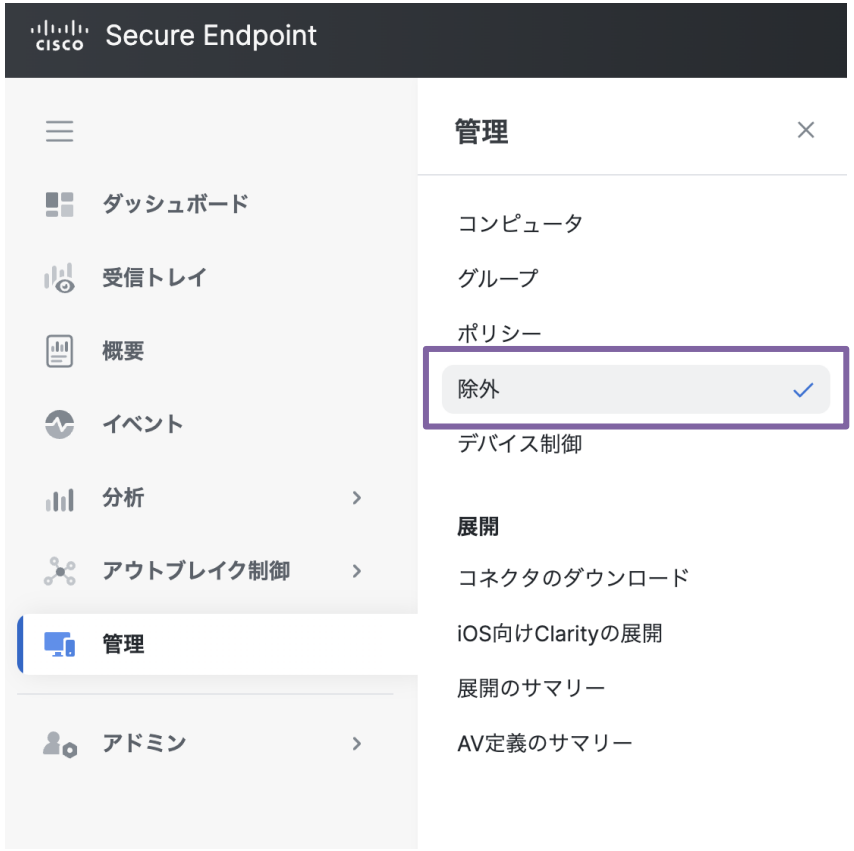
上記に問題がなければ、サポート窓口にお問い合わせください。

9-11. パソコンの動作が重くなったように感じる 1/6

以下の理由により、PCの動作が重くなったように感じる場合があります。
- ファイルが大量に存在するようなディレクトリをスキャンしてしまい、端末のリソース(CPU/メモリ等)が大量に消費されている
- 他社アンチウィルス製品との競合が発生してしまっている

対処方法

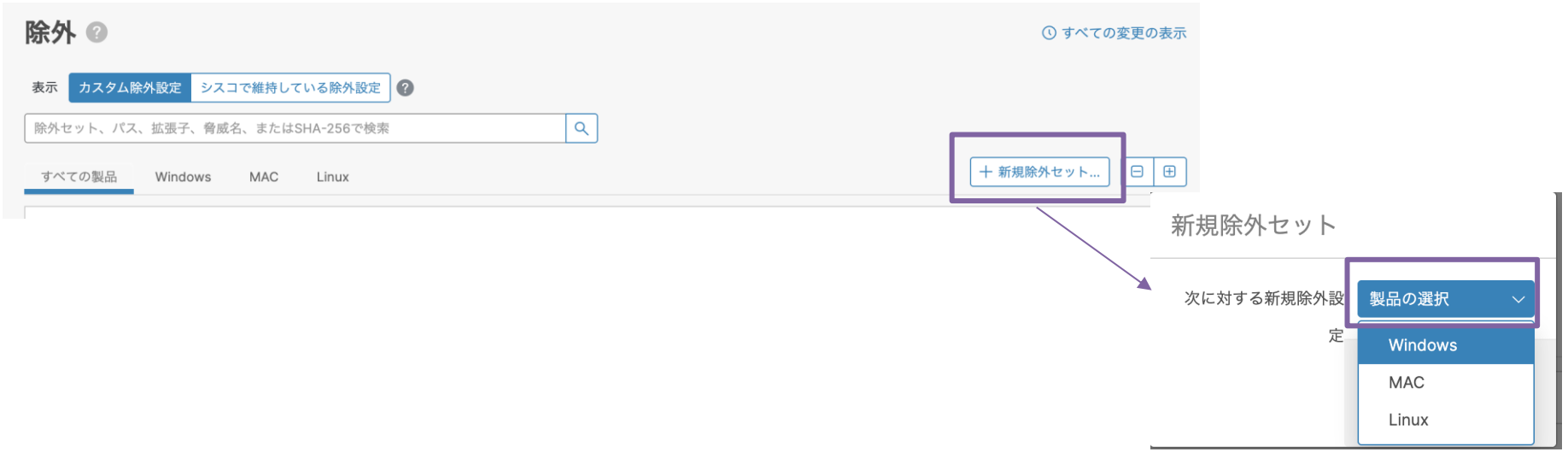
①Cisco Secure Endpoint管理コンソールにログインし、管理 > 除外を選択してください。



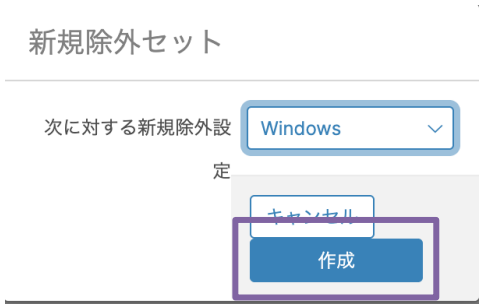
対処方法（つづき）

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

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

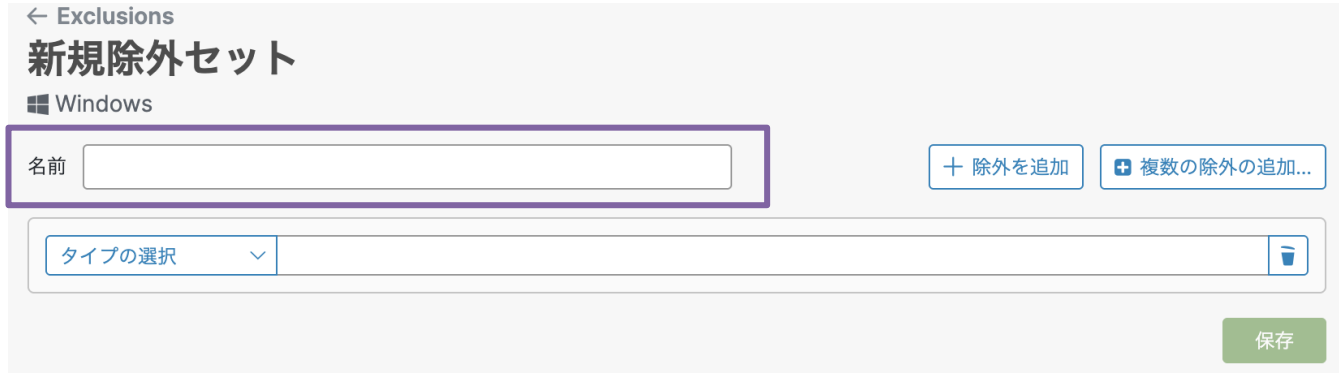


③作成をクリックします



対処方法（つづき）

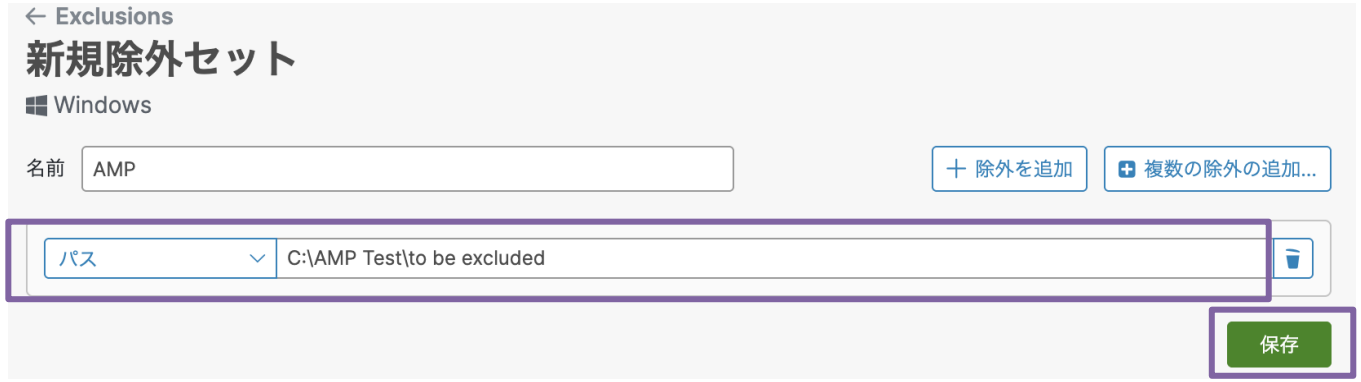
④任意の名前を入力します。



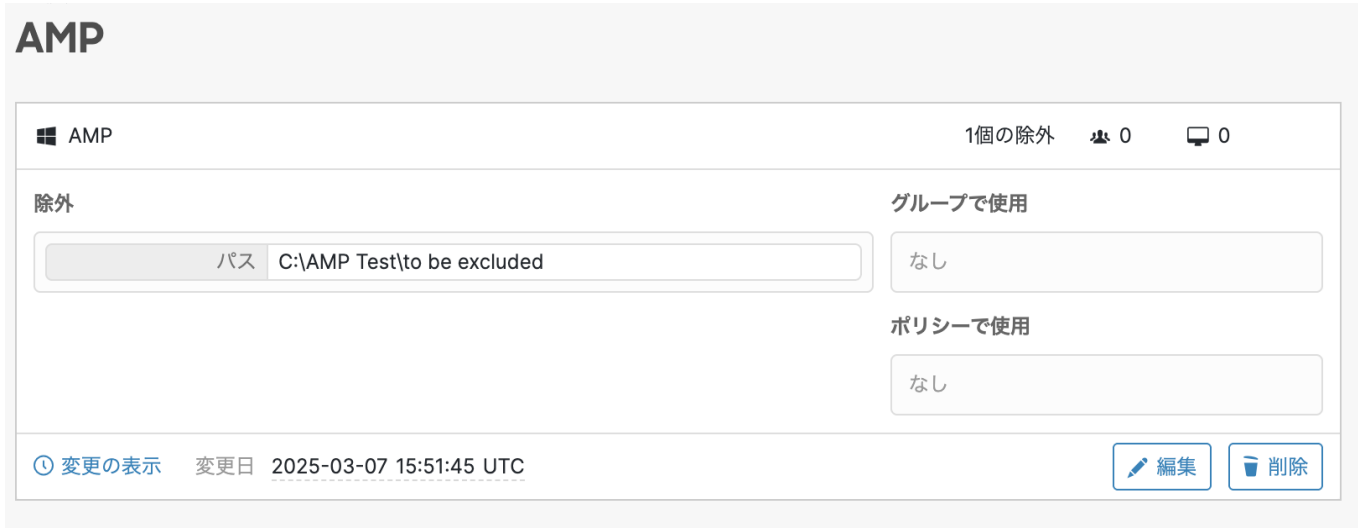
⑤「タイプの選択」から「パス」を選択します。
※例として「C:¥AMP Test¥to be excluded」という「パス」を除外する設定を追加してみます。

対処方法（つづき）

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

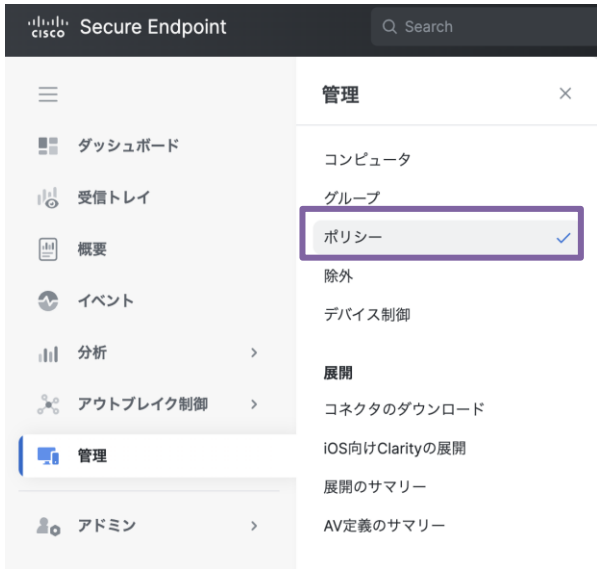


⑦作成したパスが表示されます。

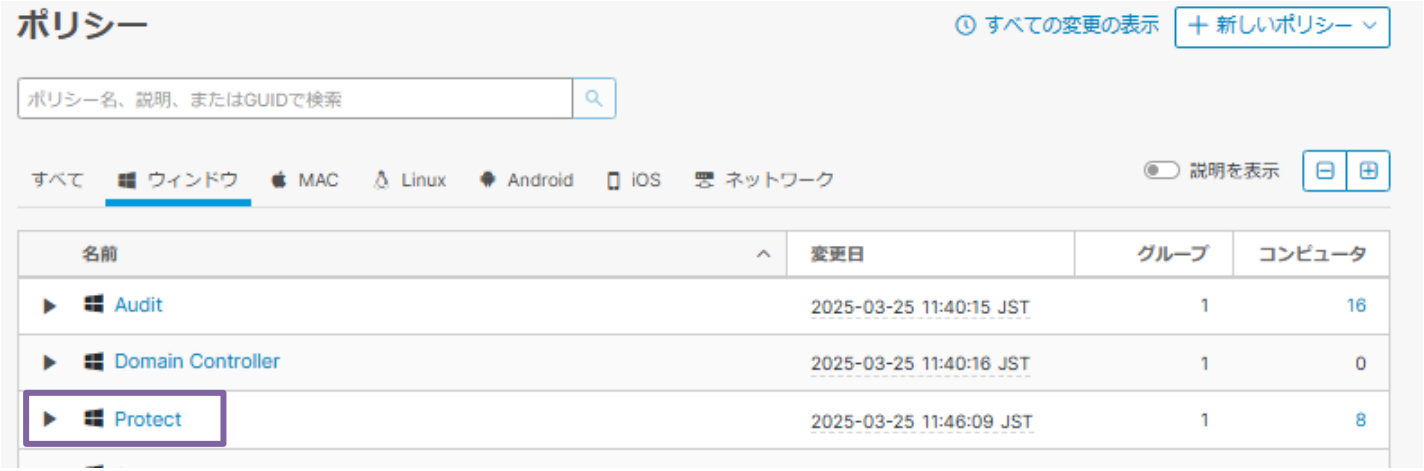


対処方法（つづき）

⑧次に、管理　> ポリシー　を選択します。

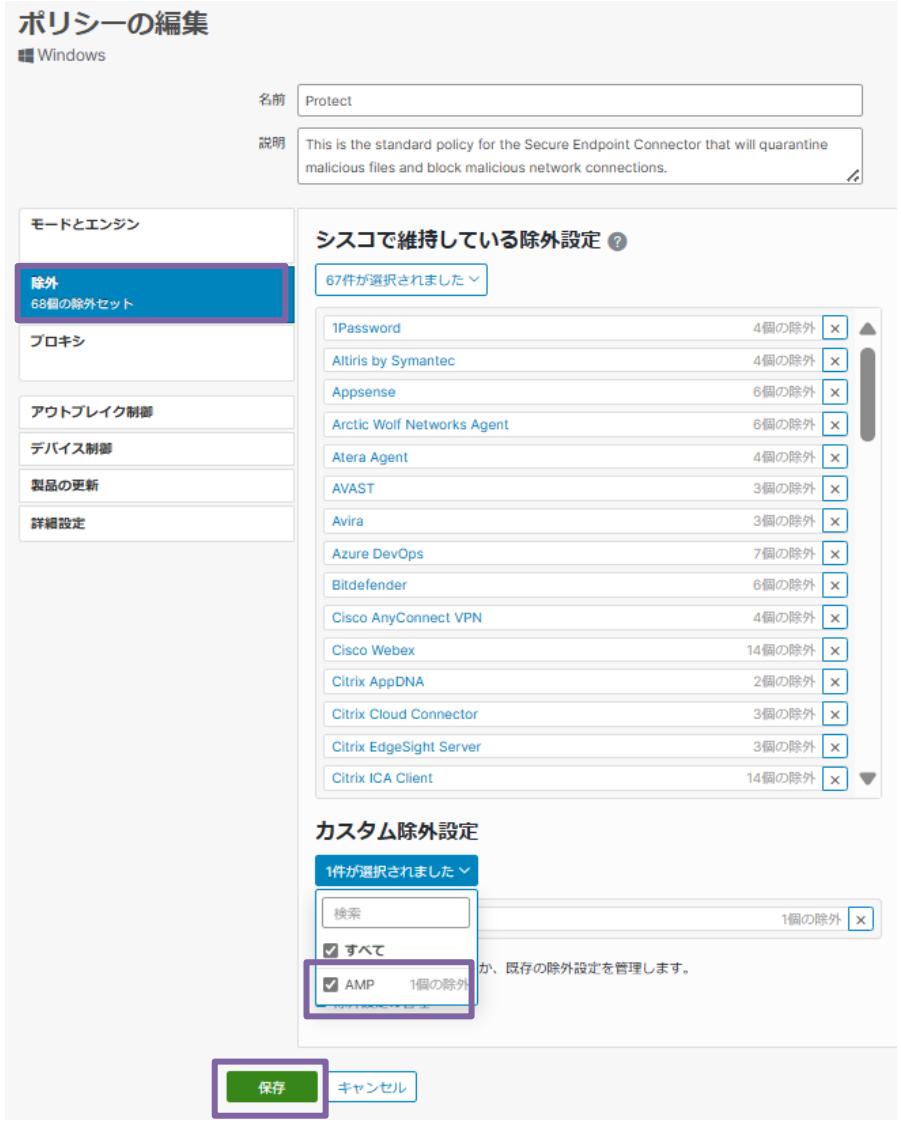


⑨該当の端末に適用されているポリシーを選択します。
※例としてWindowsOSで利用中のポリシー「Protect」で除外設定を追加してみます。



対処方法（つづき）

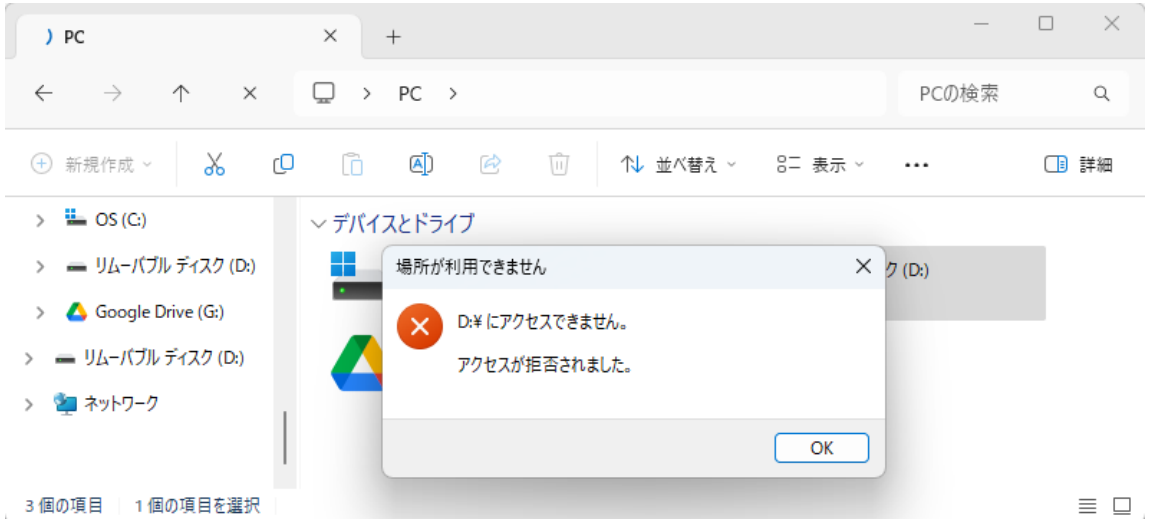
⑩「除外」をクリックし、「カスタム除外設定」のドロップダウンから、作成した除外名を選択して保存します。



9-12. デバイス制御方法 1/16

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

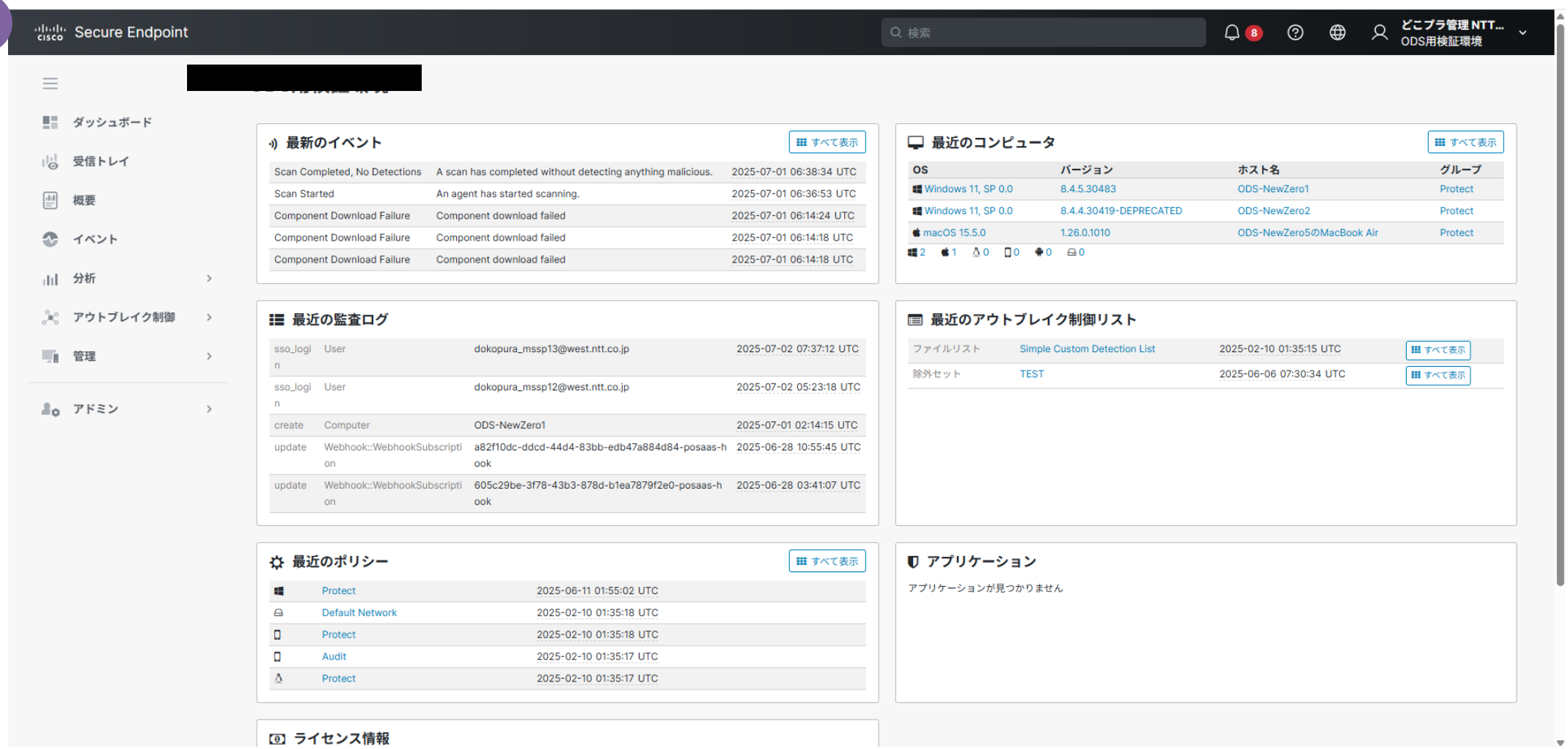
デバイス制御の設定をすると、デバイスを繋いだ際に以下エラーが出るようになります。
※エラー通知をするかどうかは、手順⑧の「エンドポイントユーザに通知」で選択いただけます。
具体的な設定手順は次項を参照ください。



デバイス制御方法

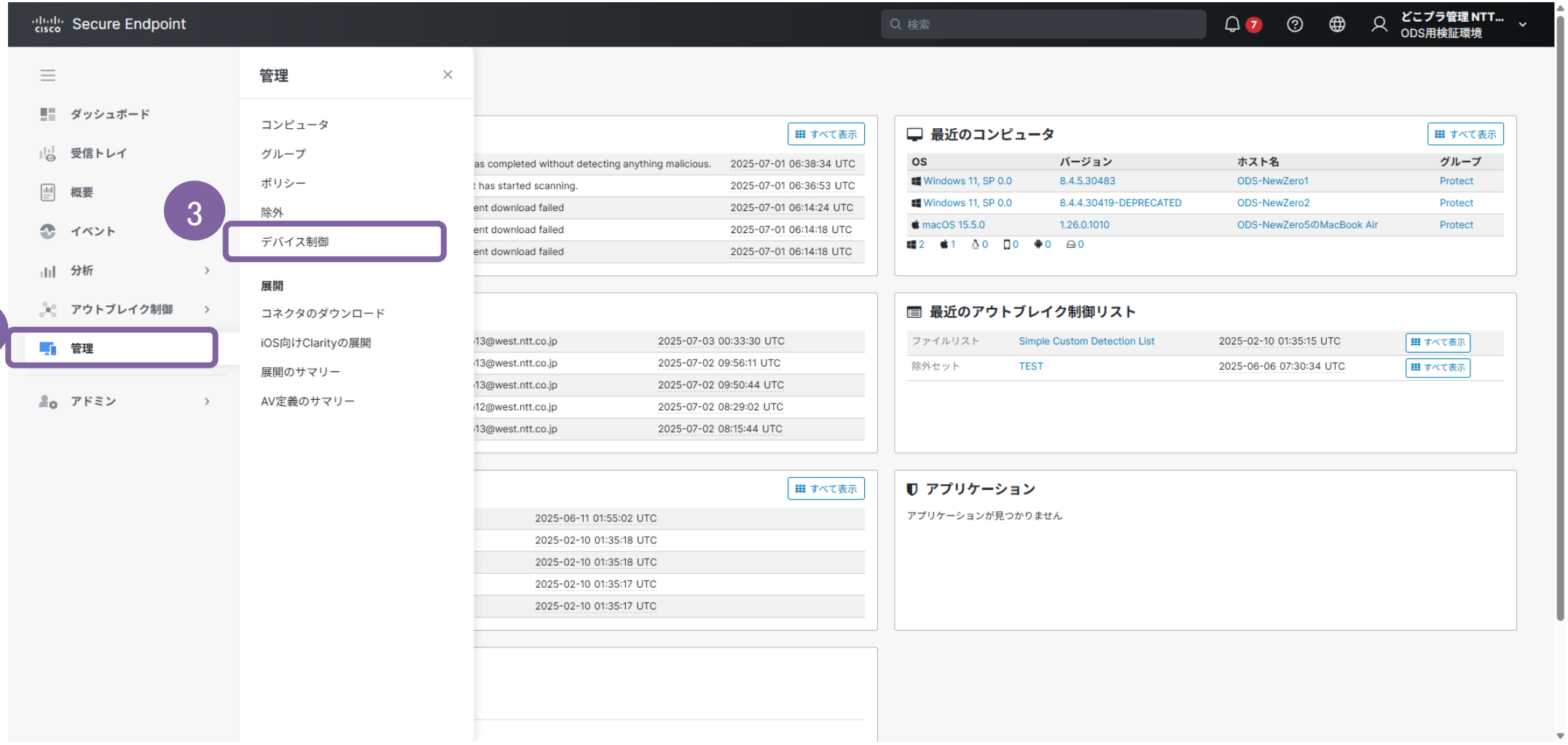
①Secure Endpoint管理コンソールを開き、ログインします。
Secure Endpoint管理コンソール：https://console.apjc.amp.cisco.com

1



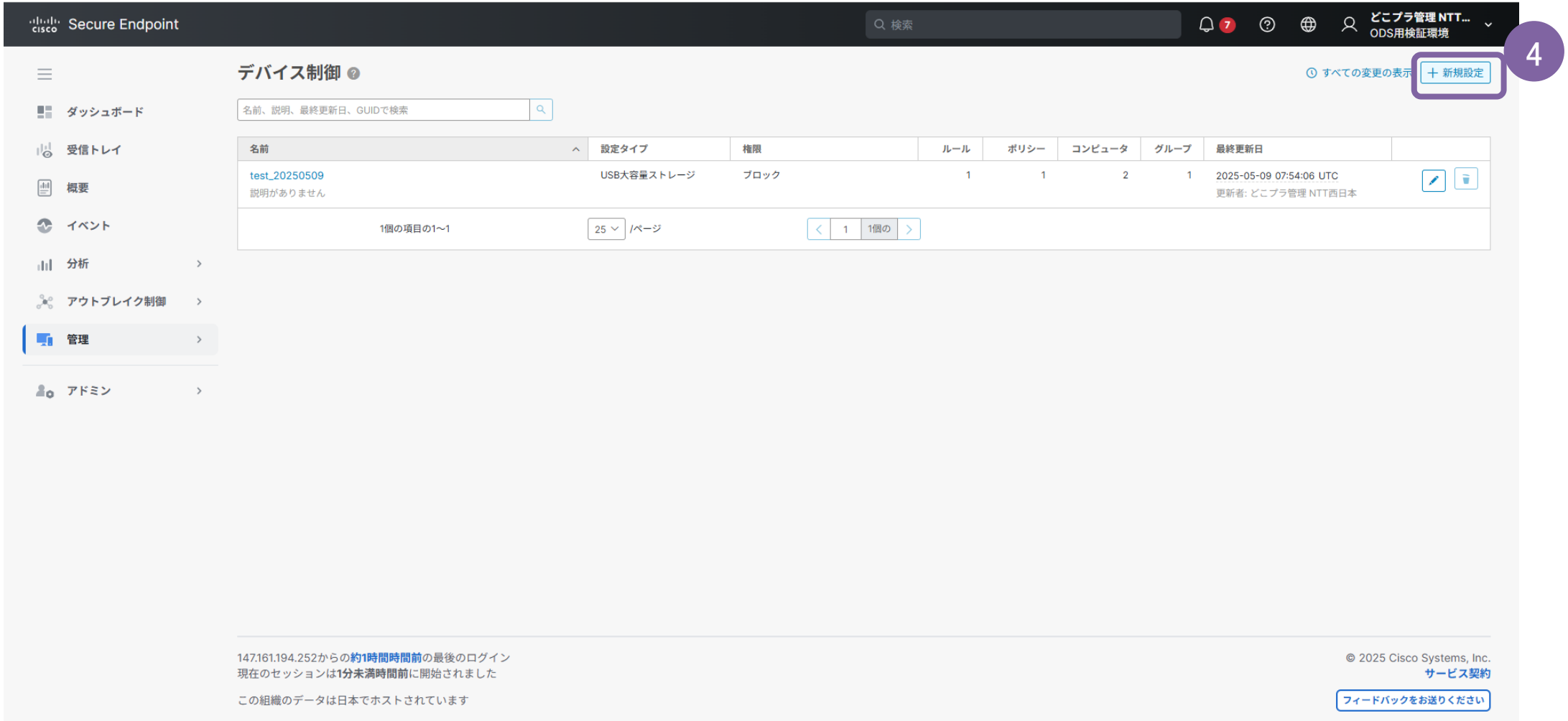
デバイス制御方法（続き）

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



デバイス制御方法（続き）

④デバイス制御ページが表示されますので、「＋新規設定」をクリックします。



デバイス制御方法（続き）

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

デバイス制御方法（続き）

⑧「基本ルール」で設定したいものにチェックを入れます。
※ここでは例として、「ブロック」、エンドポイントユーザに通知では「常に保存」を選択します。
※Windows ポータブルデバイス（WPD） の場合、実行制御は現在サポートされておりません。
⑨「保存」をクリックします。

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

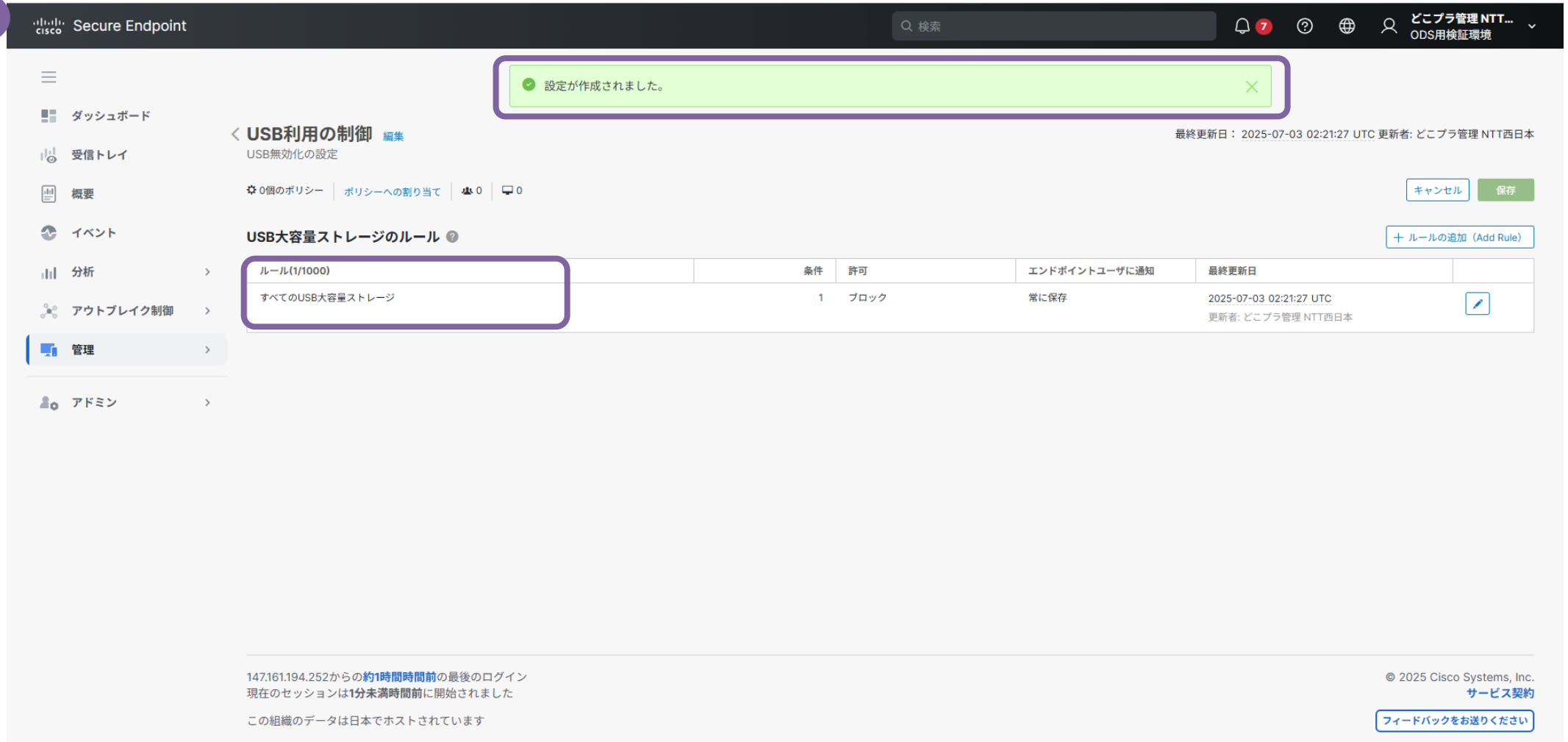
権限	説明
ブロック（Block）	いかなる方法でも、デバイスへのアクセスをエンドポイントに許可しません。
読み取り専用	デバイスからのファイルの読み取りのみをエンドポイントに許可します。ユーザーは引き続き、デバイスからエンドポイントにファイルを手動でコピーし、書き込みまたは実行できることに注意してください。
読み取りと書き込みのみ	デバイスでのファイルの読み取りと書き込みをエンドポイントに許可します。ユーザーは引き続き、デバイスからエンドポイントにファイルを手動でコピーして実行できることに注意してください。
読み取り、書き込み、および実行	デバイスへのフルアクセスをエンドポイントに許可します。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

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

デバイス制御方法（続き）

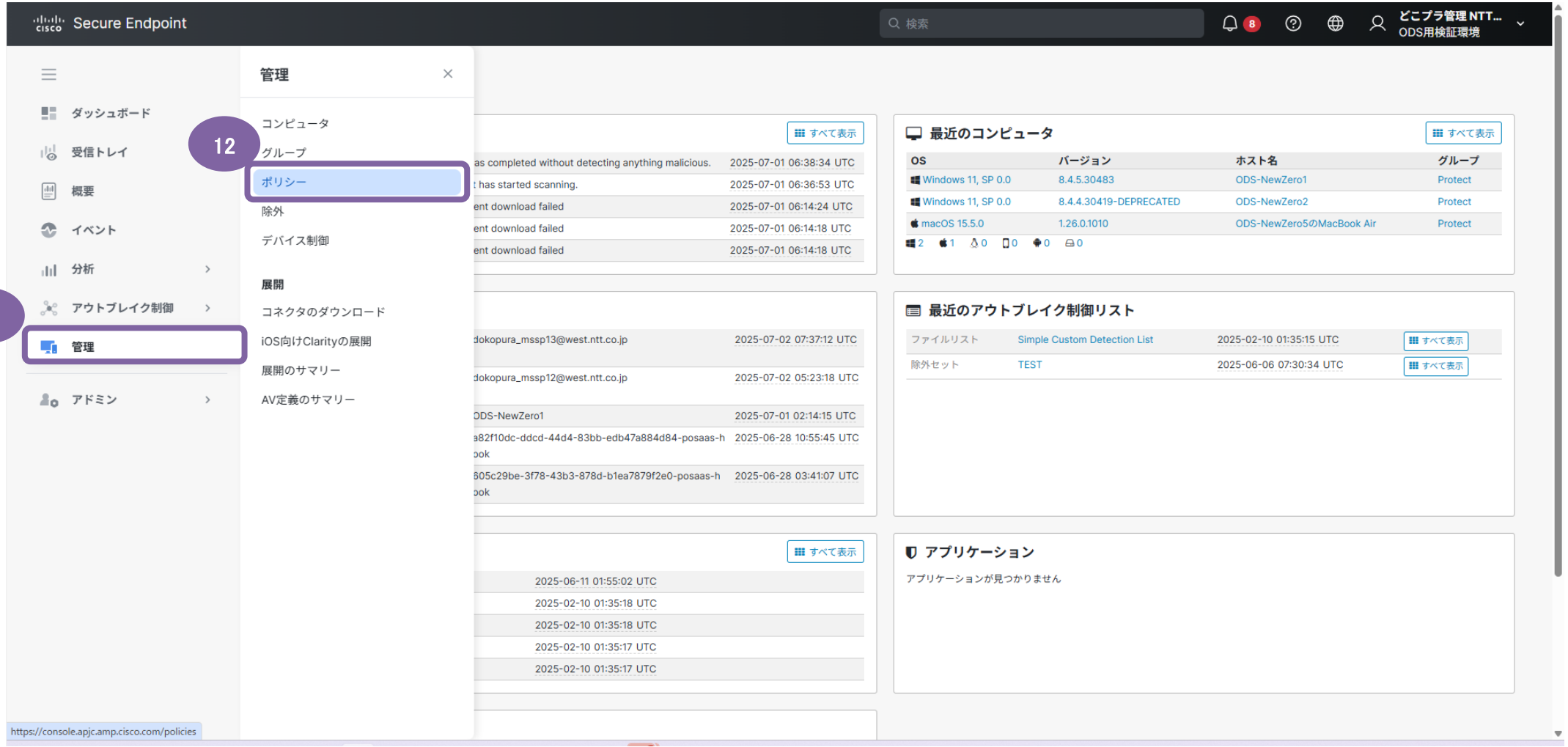
⑩「設定が作成されました。」という文字が表示され、ルールの新規作成が完了しました。

10



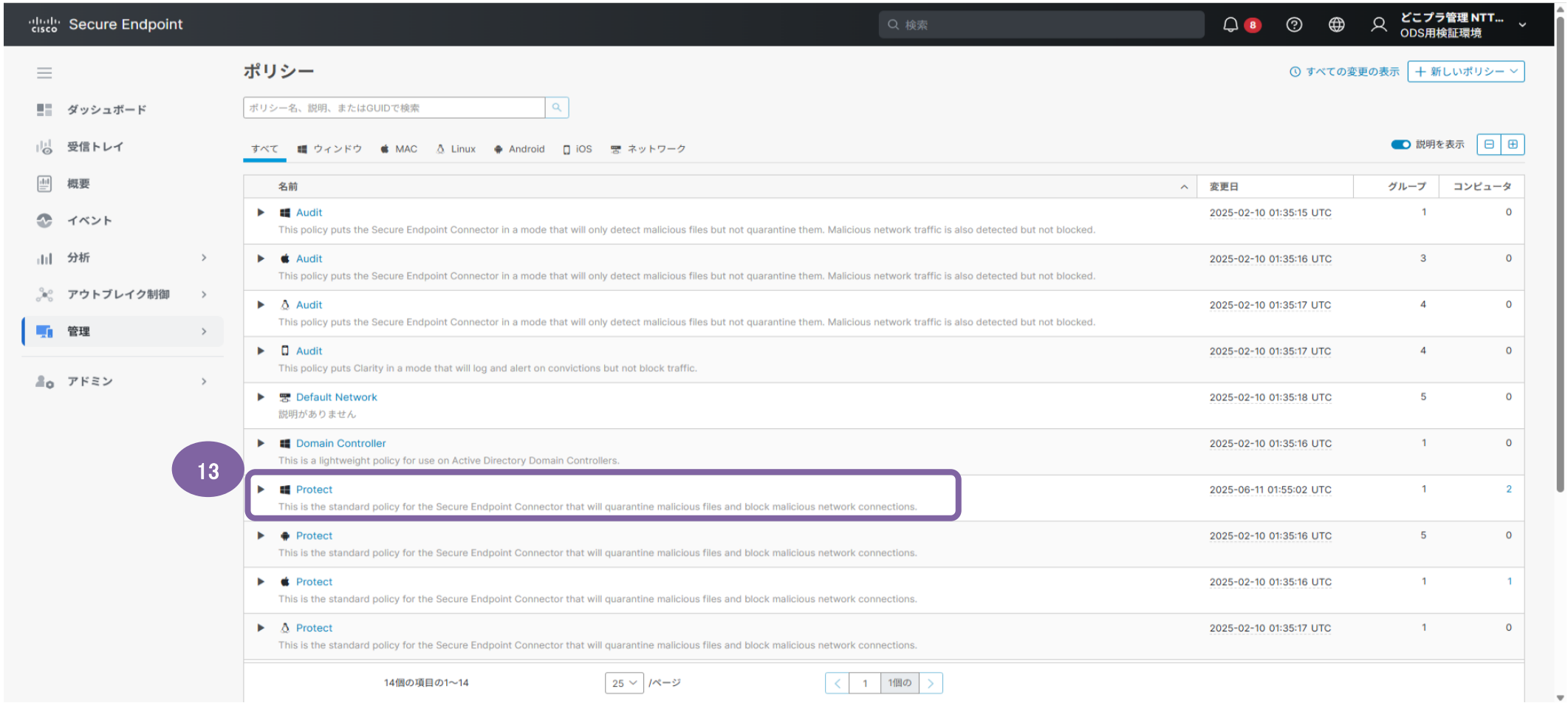
デバイス制御方法（続き）

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



デバイス制御方法（続き）

⑬対象 Secure Endpoint が所属するグループが使用しているポリシーの名前をクリックします。
ここでは例として、「Protect」のポリシーを修正をするものとして説明を続けます。
※デバイス制御はWindowsのみ設定が可能です。



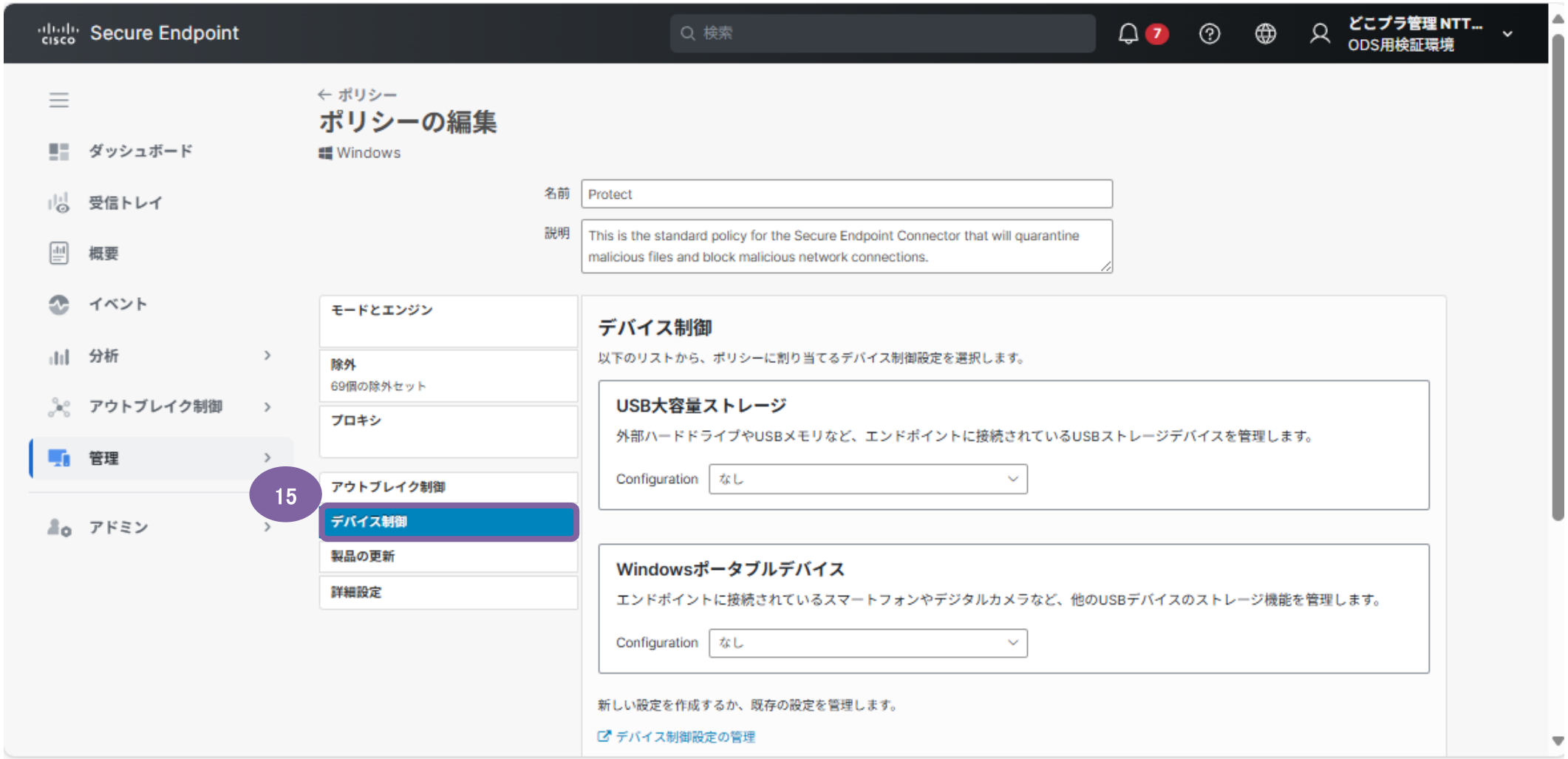
デバイス制御方法（続き）

⑭ポリシーの編集画面が開きます。

14

デバイス制御方法（続き）

⑮「デバイス制御」をクリックします。

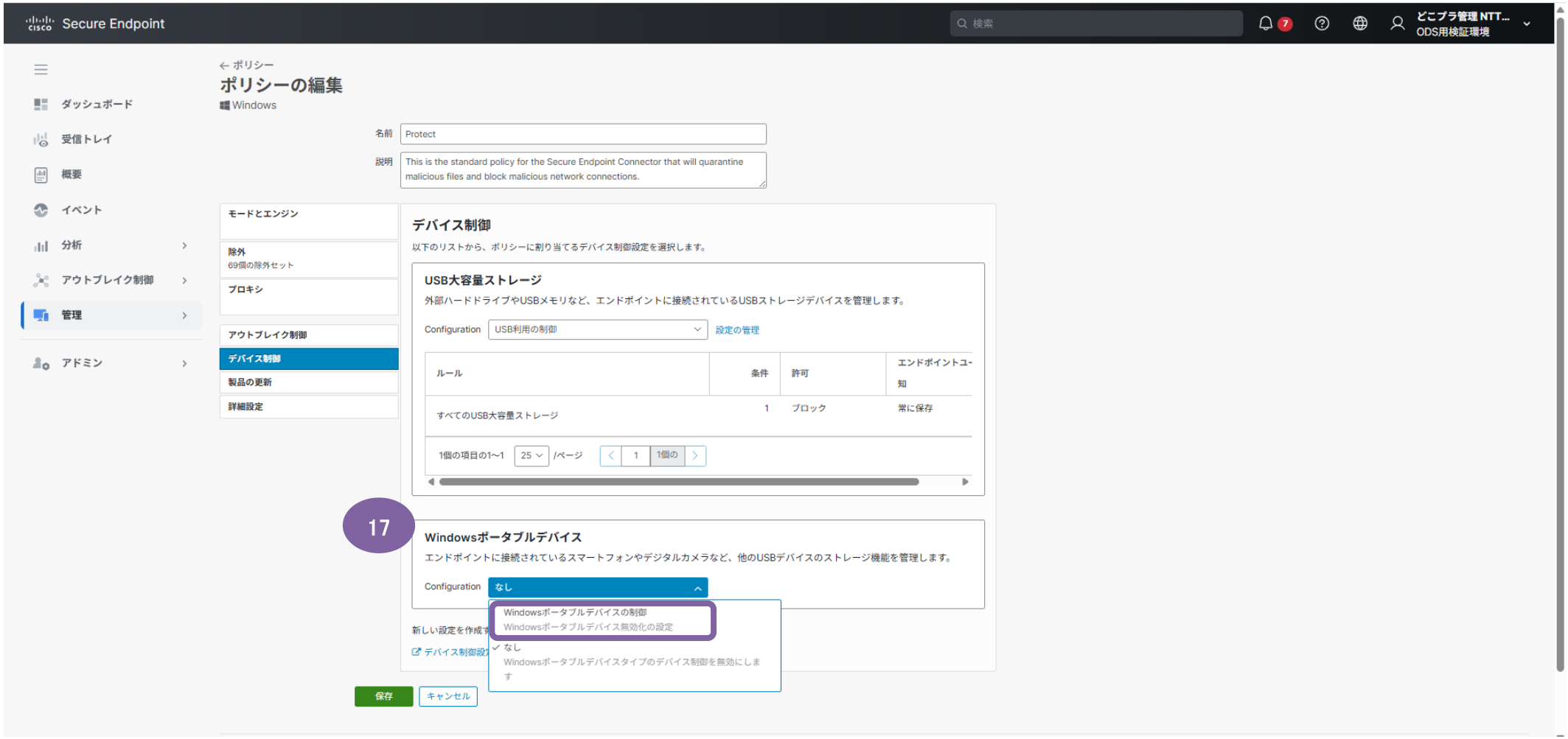


デバイス制御方法（続き）

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

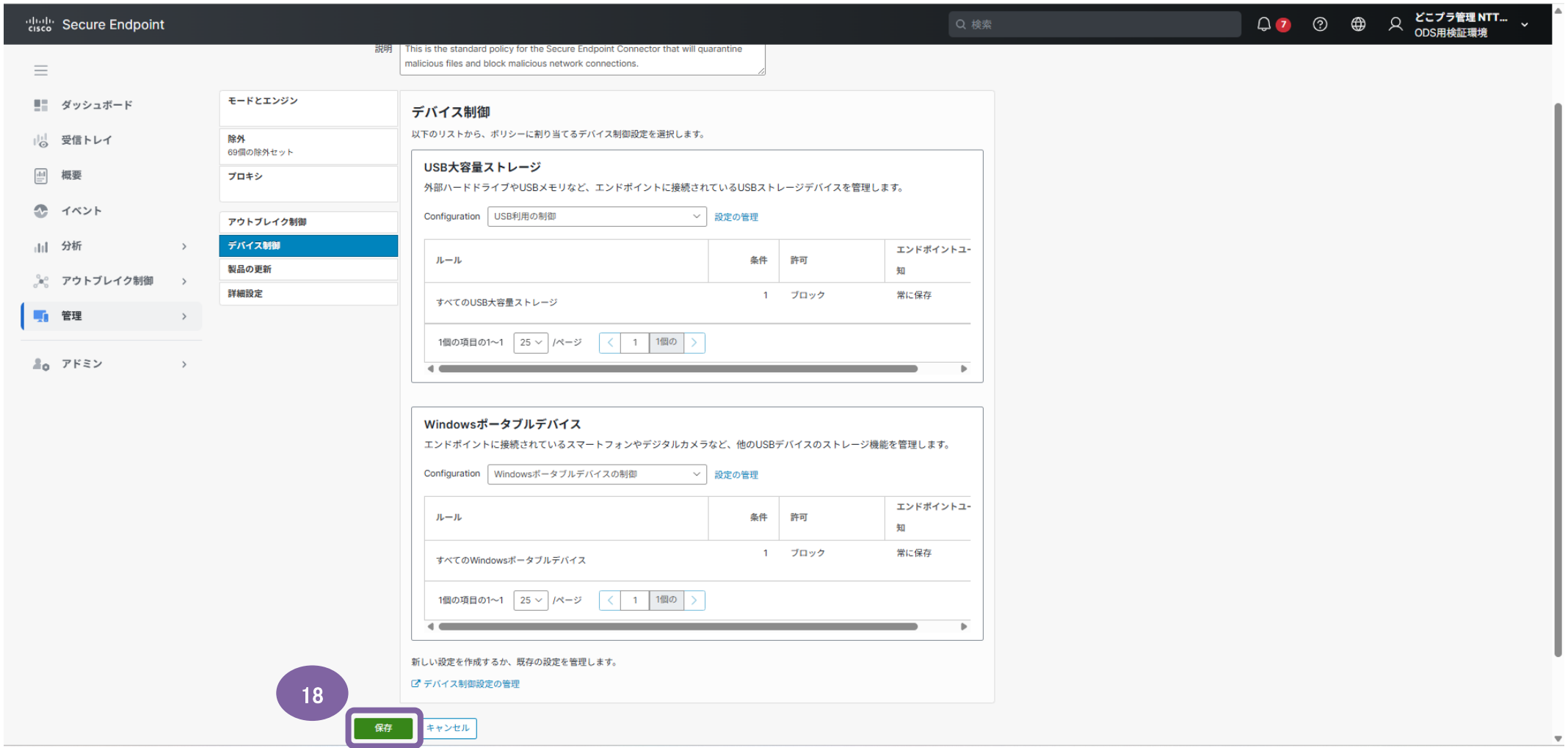
デバイス制御方法（続き）

（Windowsポータブルデバイスの設定も行う場合）
⑰Windowsポータブルデバイスの「Configuration」で設定したいルールを選択します。



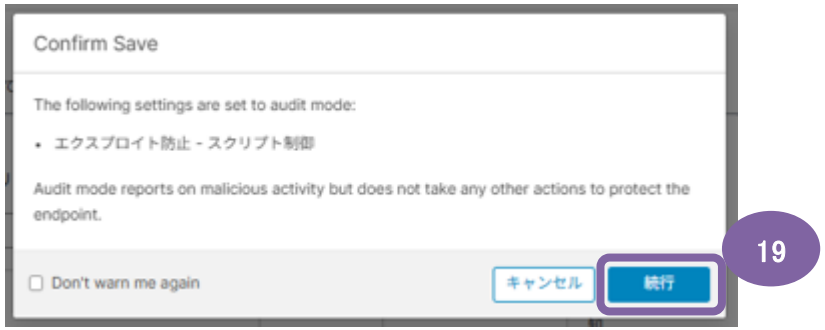
デバイス制御方法（続き）

⑱「保存」をクリックします。



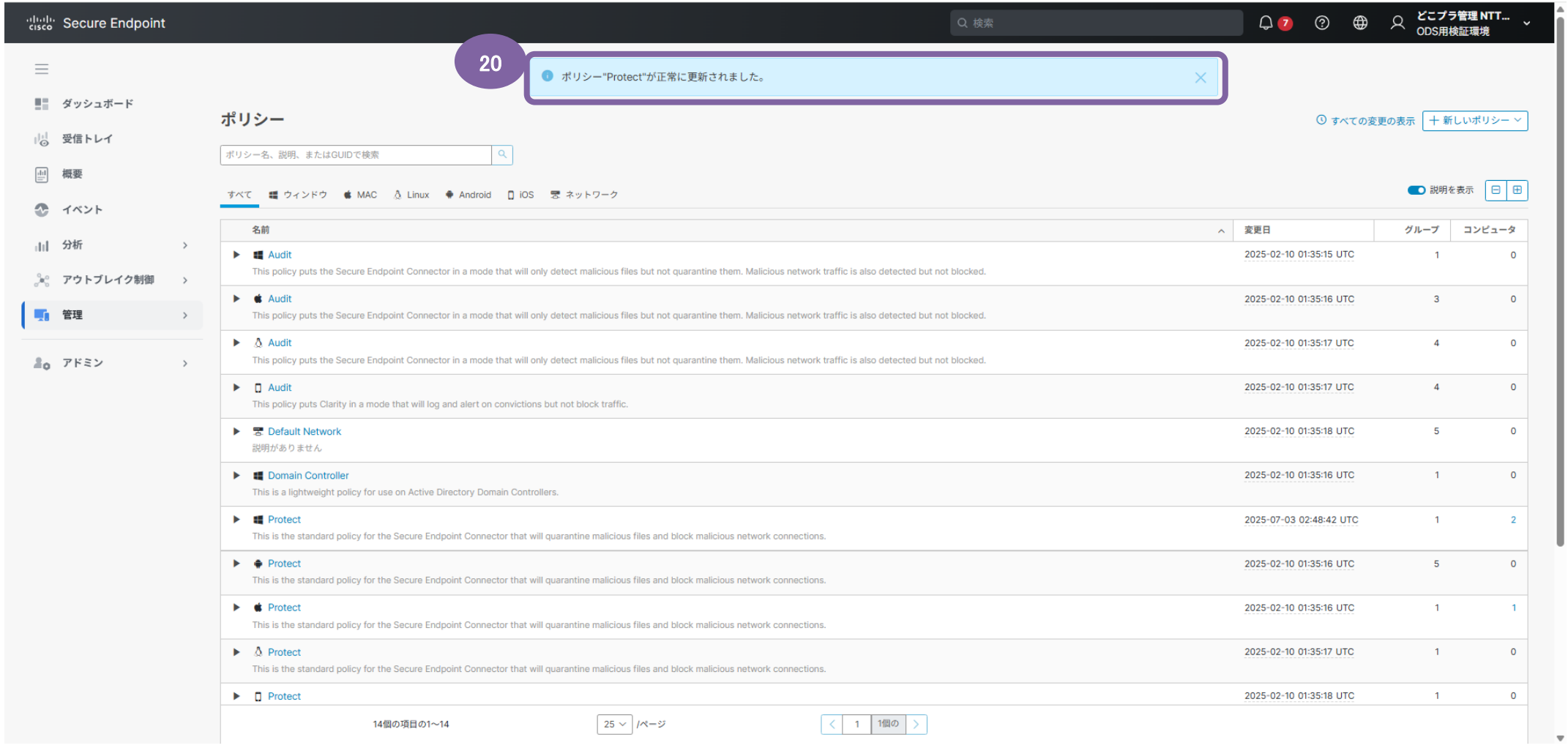
デバイス制御方法（続き）

⑲以下のポップアップが表示されますので、「続行」をクリックします。
※「監査モードでは悪意のある活動を報告しますが、エンドポイントを保護するためのその他の措置は一切行いません。」という確認です。



デバイス制御方法（続き）

⑳以下画面が表示されますので、これにて設定完了です。



10. elgana連携の設定手順

10. elganaの設定手順（elganaとは）

elgana（エルガナ）は、どなたでも簡単に使えるビジネスチャットです。
ご紹介HPはこちら　▶　https://business.ntt-west.co.jp/service/assist/elgana/
ビジネスチャットとしてのご利用に加え、このたびお申込みいただいた**「セキュリティおまかせプラン どこでもプライム」との連携機能**をご利用いただけます。利用手順は、次頁以降をご参照ください。

elgana連携機能

＜通知機能①＞
「どこでもプライム」で検知した
EPP／EDRセキュリティで解決されて
いない脅威がある場合に通知

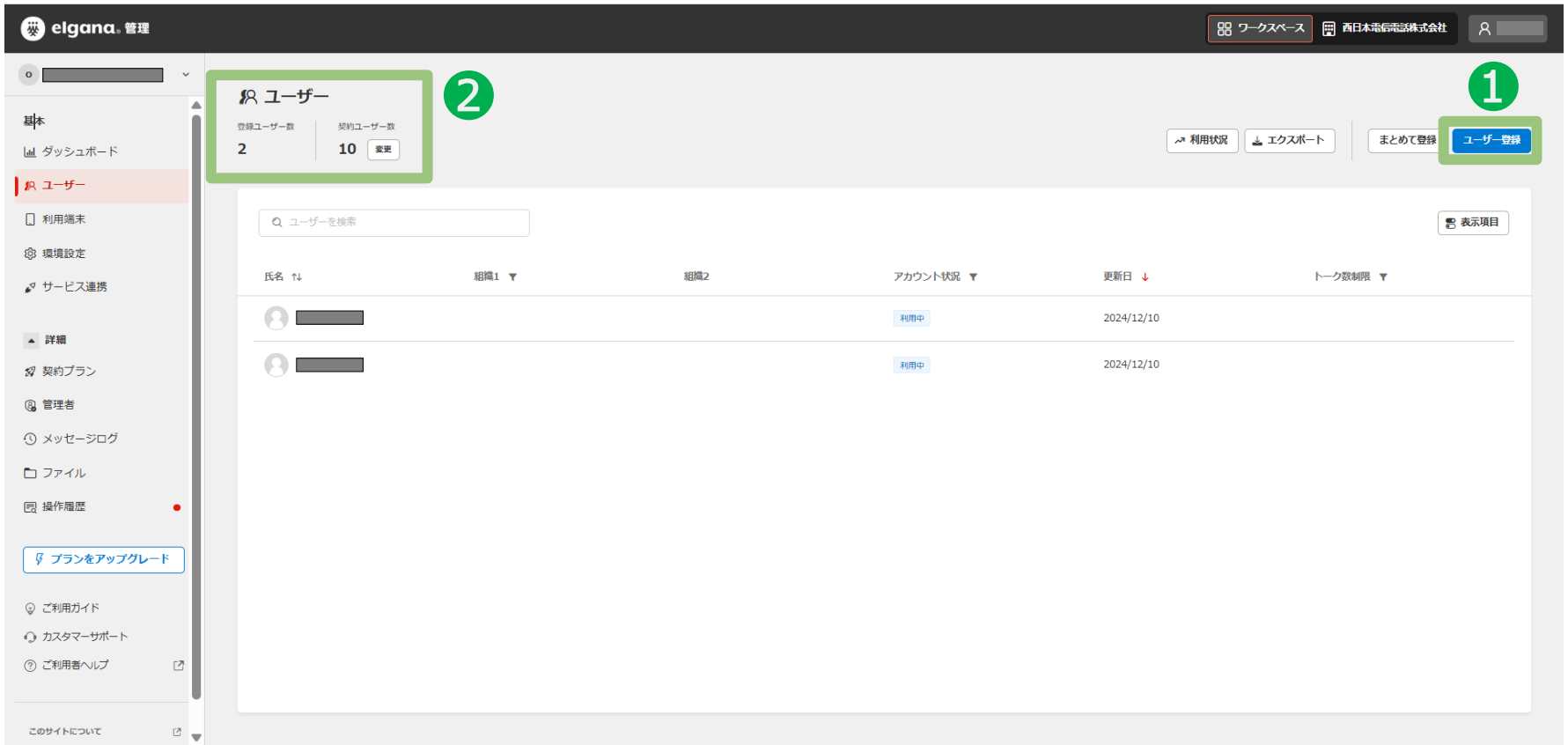
＜通知機能②＞
EDRセキュリティにおける
ファイル隔離／端末隔離を通知

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

STEP1

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

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



10. elganaの設定手順（登録したユーザでelganaにログイン）

STEP2

elganaサービス管理サイトで登録いただいた各ユーザーでの画面設定となります。
以下の設定を行うことで、「どこでもプライム」で検知したEPP／EDRセキュリティで解決されていない脅威がある場合の通知等を受け取ることが可能です。情報セキュリティ担当、管理者など設定したいユーザにおいて実施ください。

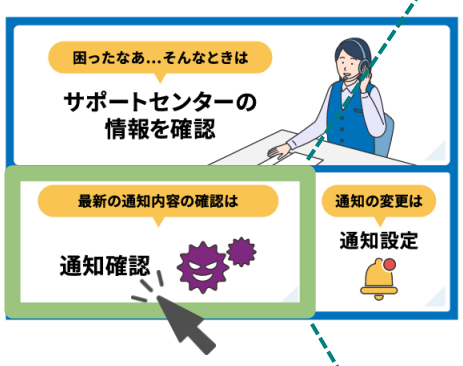
①ログインいただいた画面で「連絡先」を選択
②「検索」をクリックしてください。
③「**セキュリティおまかせプラン どこでもプライム**」を選択し、吹き出しマーク をクリックいただくことで、トークルームが作成されます。

10. elganaの設定手順（elgana通知開始）

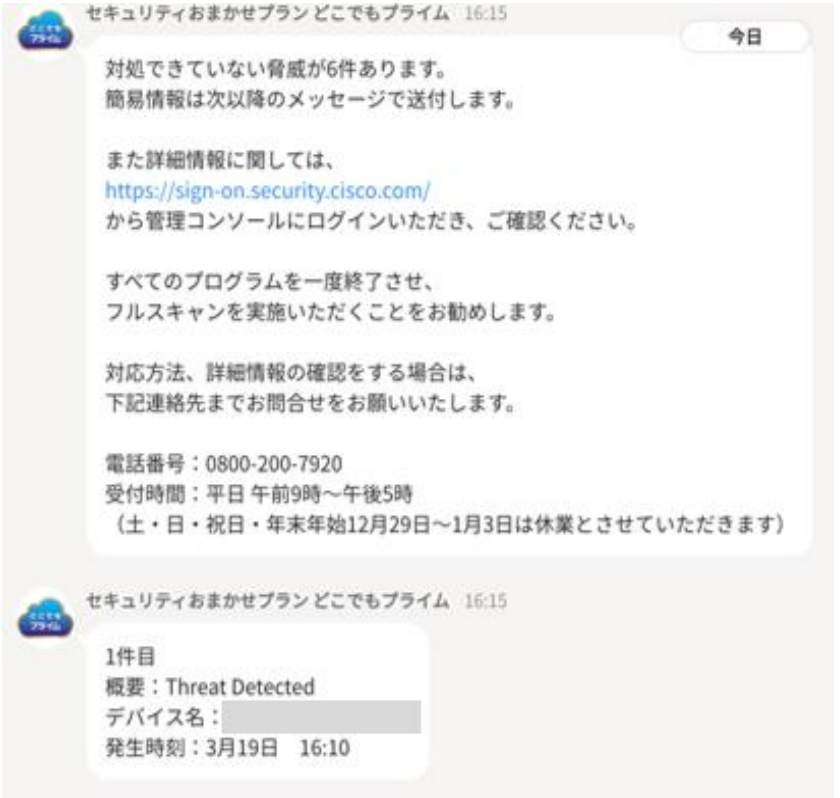
STEP3

以上で設定は完了となり、「どこでもプライム」で検知した内容に基づき通知されます。
もしくは、以下の「通知確認」をクリックすることで、最新の通知内容をご確認をいただくことが可能です。

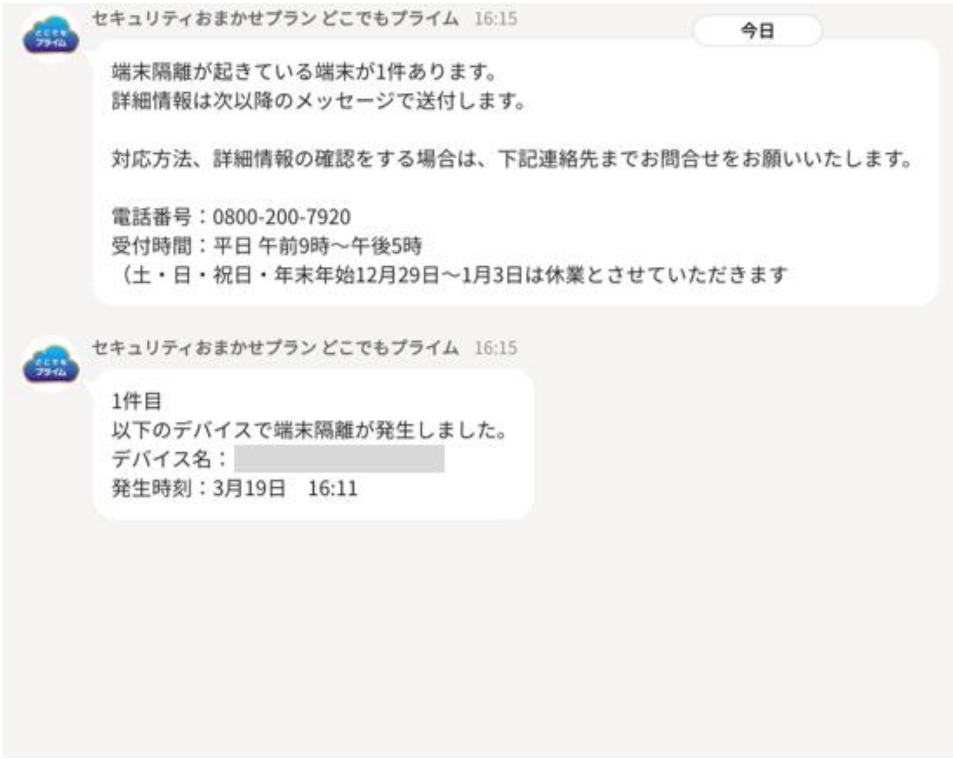
通知確認のみならず、内部のコミュニケーションとしてもご利用ください。



解決されていない脅威がある場合の通知



端末隔離・解除の通知



11. どこでもプライム契約IDの確認手順

11. どこでもプライム契約IDの確認手順（開通案内メールの場合）

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

11. どこでもプライム契約IDの確認手順（Ciscoコンソールの場合）

■Cisco Umbrellaシステムのコンソールでご確認いただく場合

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