# Secure Endpoint ユーザーガイド

最終更新日：2023 年 10 月 19 日

# 目次

# 目次

# 目次

# 目次

# 目次

# 第 1 章

# ダッシュボード

Cisco Secure Endpoint（旧 Cisco Advanced Malware Protection for Endpoints）ダッシュボードには、マルウェアやネットワークの脅威検出に関する更新とともに、環境内にあるデバイスの問題箇所の概要が表示されます。[ダッシュボード（Dashboard）] ページでは、イベントにドリル ダウンしてより詳細な情報を収集することで、潜在的な侵害に対処できます。

## コンソールシステム要件

Cisco Secure Endpoint コンソールにアクセスするには、次のいずれかの Web ブラウザが必要です。

- Microsoft Edge 88 以降
- Mozilla Firefox 81 以降
- Apple Safari 14 以降
- Google Chrome 86 以降

## 組織スイッチャ

組織スイッチャを使用すると、Cisco Secure Endpoint の組織をすばやく切り替えることができます。組織を切り替えるには、各組織のアカウントが必要です。組織スイッチャは、複数の組織のアカウントがある場合にのみ表示されます。現在の組織の名前がリボンに表示されます。

別の組織に切り替えるには、次の手順を実行します。

1. [切り替え（Switch）] ボタンをクリックすると、組織のリストが表示されます。
2. アクセスする組織を選択します。

**重要：**組織スイッチャは、ユーザーが複数の組織に属して組織を切り替えることを可能にする、Cisco Secure Endpoint の優れた機能です。ただし、これに関連して予期しない動作が発生する可能性があります。Cisco XDR、SecureX、または Orbital への初回ログイン時には、ログインしている Cisco Secure Endpoint 組織のセッションが割り当てられます。Cisco Secure Endpoint で組織を切り替えても、Orbital または SecureX では組織は切り替えられません。Cisco XDR、Orbital、または SecureX で組織を切り替えるには、各システムからログアウトしてから再度ログインし、使用する組織を選択する必要があります。

# 脅威のシビラティ（重大度）

脅威のシビラティ（重大度）は、色分けされたタグで表されて 、[ダッシュボード（Dashboard）] タブ、[受信トレイ（Inbox）] タブ、および [イベント（Events）] タブなどのページのインターフェイスに表示され、最も重要なセキュリティ侵害についての迅速な分析が得られます。


脅威のシビラティ（重大度）は、イベントの相対的な数を要約した色分けされたミニバーグラフとして [受信トレイ（Inbox）] タブインターフェイスにも表示されます。グラフの上にマウスカーソルを合わせると、詳細ビューを表示できます。


個々のイベントタイプに割り当てられた脅威の重大度レベルは、シスコの脅威調査チームによって評価され、脅威が相互にどのように組み合わされて出現するかによって変化する場合があります。

# ダッシュボード タブ

[ダッシュボード（Dashboard）] タブには、過去 14 日間に組織で発生した脅威アクティビティが表示されます。また、侵害されたコンピュータの割合や [受信トレイ（Inbox）] タブの各項目のステータスも表示されます。[ダッシュボード（Dashboard）] および [受信トレイ（Inbox）] タブビューの [フィルタ（Filters）] は作成、編集、またはリセットできます。[期間選択（Time Period）] は、[ダッシュボード（Dashboard）] タブのすべてのデータに適用されます。

[すべて更新（Refresh All）] ボタンをクリックして最新のデータをページにロードしたり、[自動更新（Auto-Refresh）] ボタンをクリックして自動的にリロードされるデータの間隔を設定したりできます。データをロードする時間間隔を 5、10、または 15 分から選択します。[自動更新（Auto-Refresh）] がアクティブになっている場合は、そのボタンの上にチェック マークが表示されます。ページの更新を停止するには、チェック マークをクリックしてオフにします。

セキュリティ侵害、検疫済みの検出、および脆弱性に関するヒートマップビューに加えて、次のような情報のサマリーも確認できます。

- 組織の [機能（Features）] に設定している場合、環境内のグローバル脅威アラート。
- 低拡散度の実行ファイルの自動分析を設定している場合、Cisco Secure Malware Analytics（旧 Threat Grid）による自動送信およびレトロスペクティブ脅威検出。
- Cisco Secure Endpoint コネクタによってスキャンされたファイル数とログに記録されたネットワーク接続数に関する統計情報。

> **重要事項：**ネットワーク接続のロギングには、ポリシーでデバイス フロー コリレーションを有効にする必要があります。

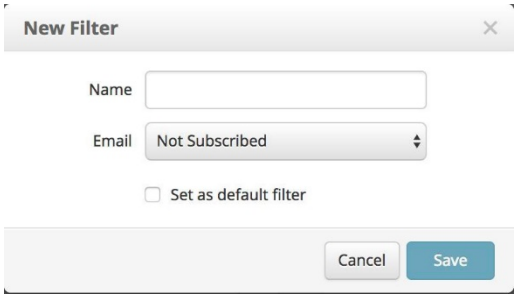
- 各コネクタタイプの [クイックスタート（Quick Start）] 設定へのリンク。

## フィルタ

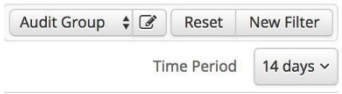
指定したグループ、期間（過去 14 日間、7 日間、1 日、1 時間）、日付/時刻選択、特定の侵害観測対象、侵害イベントタイプでアクティビティをフィルタ処理できます。

これらの各フィルタは、単独でも、組み合わせても、適用できます。侵害観測対象と侵害イベントタイプフィルタは、侵害に関連した情報にのみ適用されます。ここで適用されるページ フィルタはすべて受信トレイにも適用されます。

表示するグループ、観測対象、イベントタイプ、および期間を選択し、[新規フィルタ（New Filter）] をクリックしてカスタムフィルタを作成します。フィルタに名前を付けたり、電子メールのアラートを即時、1 時間ごと、毎日、または毎週受信するかどうか選択したり、[ダッシュボード（Dashboard）] および [受信トレイ（Inbox）] タブのデフォルト ビューとしてフィルタを設定したりすることができます。



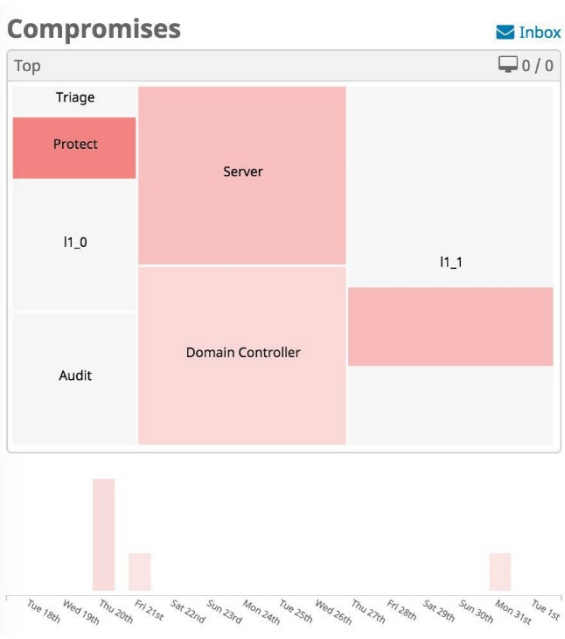

カスタム フィルタを保存した後は、ドロップ ダウンから選択したり、選択したフィルタを編集したり、フィルタが適用されていないデフォルトの状態にビューをリセットしたりすることができます。




選択したフィルタを変更または削除するには、フィルタ名の横にある編集ボタンを使用します。

## セキュリティ侵害

「セキュリティ侵害」とは、Cisco Secure Endpoint で検出され、検疫されていないがユーザーアクションが必要な可能性がある潜在的に悪意のあるアクティビティを指します。セキュリティ侵害は、侵害されたコンピュータが属するグループを示すヒート マップと、過去 14 日間の、1 日ごとまたは 1 時間ごとの侵害数を示す時刻グラフによって表示されます。[受信トレイ（Inbox）] リンクをクリックして、[受信トレイ（Inbox）] にあるセキュリティ侵害を表示し、解決する手順を実行します。




ヒート マップのグループをクリックし、このグループにドリルダウンして、子グループを表示します。また、日付/時刻、侵害観測対象、侵害イベントタイプもドリルダウンできます。ドリルダウンすると、検疫済みの検出および脆弱性ヒートマップなど、[ダッシュボード（Dashboard）] タブにある他の項目の表示も変わります。時刻グラフのバーのいずれかをクリックすると、ダッシュボード表示をフィルタ処理して、選択した侵害が発生した特定の日付を表示できます。これを実行してカスタム期間を選択すると [自動更新（Auto-Refresh）] ボタンがグレー表示され無効になります。[リセット（Reset）] ボタンをクリックするか、またはドロップダウン メニューから期間を選択して [自動更新（Auto-Refresh）] ボタンを再度有効にします。

**重要：**同じコンピュータが何度も侵害された場合は、ある期間に侵害されたコンピュータの数よりもイベント数が多くなる可能性があります。

## 重大侵害の観測対象：

セキュリティ侵害の観測対象とは、指定した期間における侵害に関連するファイル、IP アドレス、または URL です。上位 100 個の重大なセキュリティ侵害の観測対象は、拡散度順にリストされます。

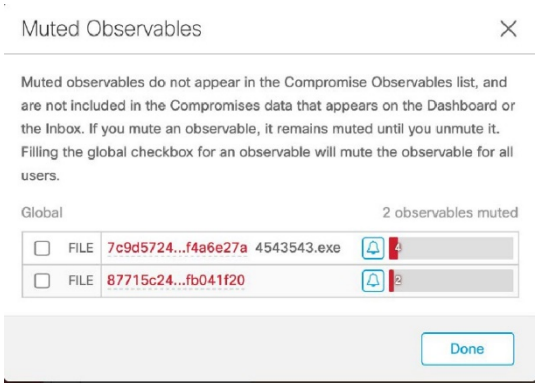

[ダッシュボード（Dashboard）] および [受信トレイ（Inbox）] ビューの侵害関連データを選択した観測対象でフィルタ処理するには、侵害観測対象の 2 番目の列にある最初の（FILE、URL、IP）または最後の列（赤いバー付き）またはファイル名をクリックします。

結果のビューでは、[侵害率（% compromised）]、[侵害数（Compromises）]、[侵害イベントタイプ（Compromise Event Types）] における他の観測対象データはすべて除外されます。

観測対象が選択されているかぎり、その観測対象のみがページに適用されます。[重大侵害の観測対象（Significant Compromise Observables）] ボックスの右上にある青色の [X] をクリックすると、観測対象の選択を解除できます。

ベルのアイコンをクリックして観測対象タイプをミュートし、関連したデータが、ダッシュボードや受信トレイに表示されないようにすることができます。

また、歯車アイコンをクリックして、ミュートした観測対象を管理することもできます。




ベルのアイコンをクリックすると観測対象のミュートを解除できます。グローバルチェックボックスがオンになっていなければ、観測対象をミュートしても、変更対象のユーザーアカウントにしか影響しません。すべてのユーザーアカウントの観測対象をミュートするには、グローバルチェックボックスをオンにします。グローバルチェックボックスをオンにした後に、グローバルにイベントをミュートすることの説明を追加することができます。

ミュートされた観測対象は、[重大侵害の観測対象（Significant Compromise Observables）] リストには表示されません。また、[ダッシュボード（Dashboard）] または [受信トレイ（Inbox）] に表示される侵害関連のデータにも含まれません。観測対象をミュートすると、歯車アイコンを使用してミュートを解除するまでミュート状態が継続します。ミュート状態は、その後 [ダッシュボード（Dashboard）] や [受信トレイ（Inbox）] にアクセスしても引き継がれます。

2 番目の列の観測対象（IP アドレス、URL、またはファイル SHA-256 など）を直接クリックすることで、ポップアップで情報を素早く表示し、一般的に使用される機能にアクセスすることもできます。ポップアップに表示される情報は、選択された観測対象のタイプによって決まります。

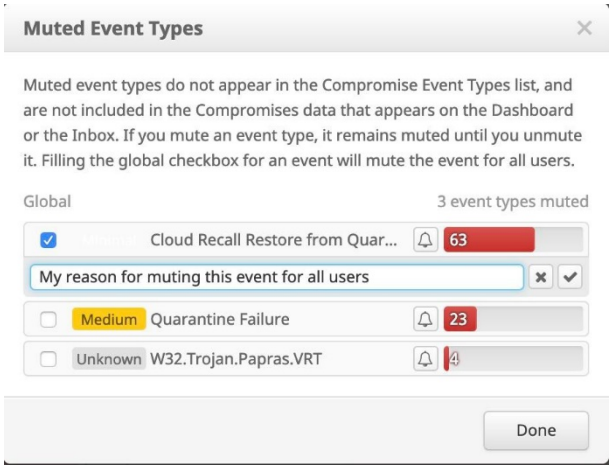
**ヒント：**ポップアップは [ダッシュボード（Dashboard）] タブに限定されていません。コンソールインターフェイス内の任意の場所で観測対象をクリックして、ポップアップを表示できます。

## 侵害イベント タイプ

侵害イベントタイプは、Cisco Secure Endpoint で検出されたイベントで、ファイル、ネットワーク、およびコネクタのアクティビティが含まれます。[侵害イベント タイプ（Compromise Event Types）] 機能は、指定した期間内（1 時間、1 日、7 日間、14 日間など）に検出された各イベント タイプの数を示します。侵害イベント タイプをクリックして侵害に関連したデータをフィルタ処理することで、選択したイベント タイプごとに [ダッシュボード（Dashboard）] に表示できます。

ベルのアイコンをクリックしてイベントタイプをミュートし、ダッシュボードや受信トレイに関連するデータを表示させないようにすることができます。

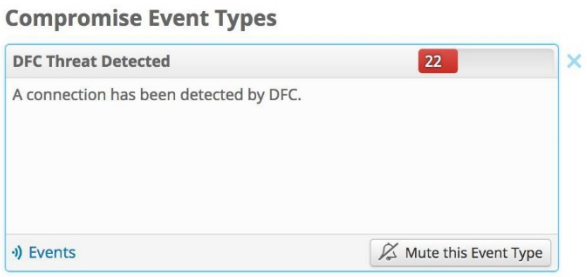

また、歯車アイコンをクリックして、ミュートしたイベントタイプを表示することもできます。




ベルのアイコンをクリックするとイベントタイプのミュートを解除できます。グローバルチェックボックスがオンになっていなければ、イベントをミュートしても、変更対象のユーザーアカウントにしか影響しません。すべてのユーザーアカウントのイベントをミュートするには、グローバルチェックボックスをオンにします。グローバルチェックボックスをオンにした後に、グローバルにイベントをミュートすることの説明を追加することができます。

イベントをミュートすると、そのイベントは [侵害イベント タイプ（Compromise Event Types）] リストには表示されません。また、[ダッシュボード（Dashboard）] または [受信トレイ（Inbox）] に表示される侵害データにも含まれません。イベントをミュートすると、歯車アイコンでミュートを解除するまでミュート状態が継続します。ミュート状態は、その後 [ダッシュボード（Dashboard）] や [受信トレイ（Inbox）] にアクセスしても引き継がれます。

イベント タイプの名前をクリックすれば、検出されたイベント タイプに関する情報を表示できます。ある侵害イベントを選択すると、侵害率、侵害数、侵害観測対象における他のイベントタイプデータは、そのイベントタイプが選択されている間、すべて除外されます。




侵害イベント タイプが選択されている間、ページに反映されるのはそのイベント タイプのみとなります。[侵害イベント タイプ（Compromise Event Types）] ボックスの右上の青い X をクリックすれば、選択したイベント タイプの選択を解除できます。

イベントタイプが侵害の兆候である場合は、IOC の説明が、それに関連する戦術および手法とともに表示されます。[インジケータ（Indicators）] ページのフィルタ処理されたビューを表示するには、[インジケータ（Indicators）] リンクをクリックします。

## 検疫済みの検出

検疫済みの検出は、侵害または悪意の可能性のあるイベントが検出され正常に検疫されているため、注意を払う必要はありません。これらは、悪意のあるアクティビティが検出されたコンピュータのグループを表示するヒート マップから表示されます。また、指定した期間の検疫数を表示する時刻グラフからも表示されます。


ヒート マップ内のグループをクリックして、そのグループにドリル ダウンしたり、子グループを表示したりします。ドリルダウンすると、選択したグループや子グループを表示するために、[ダッシュボード（Dashboard）] タブ（セキュリティ侵害および脆弱性ヒートマップを含む）に表示されるデータがフィルタ処理されます。

時刻グラフのバーをクリックすると、選択した検疫が発生した特定の日付または時刻（14 日から 2 分単位まで）で [ダッシュボード（dashboard）] ビューがフィルタ処理されます。また、[検疫イベント（Quarantine Events）] リンクをクリックすると、すべての検疫を示す [イベント（Events）] タブのフィルタ処理されたビューを表示できます。誤って隔離されたと思われるファイルをそこから復元することができます。

**重要：**ファイルは 30 日間隔離されたままになり、その後は復元できません。

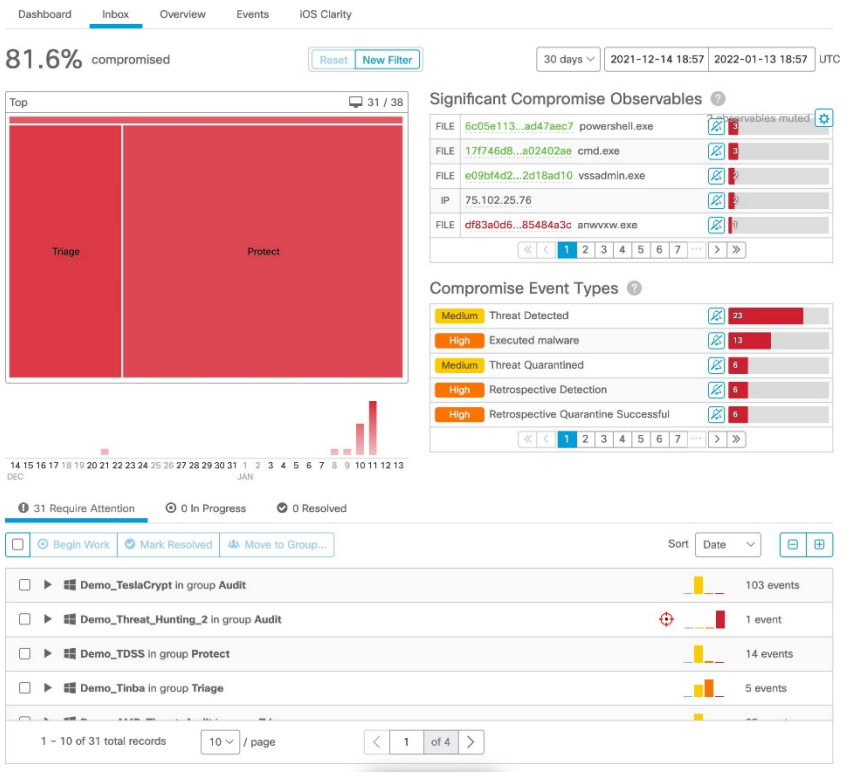
### 脆弱性

[脆弱性（Vulnerabilities）] は、既知の脆弱性が存在するアプリケーションがインストールされているコンピュータを含むグループを示すヒート マップから表示されます。


ヒートマップ内のグループをクリックして、そのグループにドリルダウンしたり、子グループを表示したりします。また、ドリルダウンすると、選択したグループや子グループを表示するために、[ダッシュボード（Dashboard）] タブ（セキュリティ侵害および検疫済みの検出ヒートマップを含む）に表示されるデータがフィルタ処理されます。[脆弱なソフトウェア（Vulnerable Software）] ページに移動するには、[表示（View）] ボタンをクリックします。

## [受信箱（Inbox）] タブ

[受信トレイ（Inbox）] は、組織にある侵害されたコンピュータを確認し、解決に手動の操作が必要な侵害のステータスをトラッキングできるツールです。ヒートマップで [グループ（Groups）] を選択する、棒グラフでセキュリティ侵害があった日を選択する、[重大侵害の観測対象（Significant Compromise Observables）] リストから SHA-256 を選択する、または [侵害イベントタイプ（Compromise Event Types）] リストから選択して、コンピュータをフィルタ処理できます。これらのフィルタは保存してデフォルトビューとして設定できます。注意が必要なコンピュータ、進行中のコンピュータ、解決済みのコンピュータ別に、一致するタブをクリックしてリストをフィルタ処理することもできます。[並べ替え（Sort）] ドロップダウンメニューから選択して、日付または重大度でリストを並べ替えることができます。コンピュータが解決済みとマークされたら、その後 [ダッシュボード（Dashboard）] や [受信トレイ（Inbox）] のデータには表示されません。




**重要：**[受信トレイ（Inbox）] の項目は 30 日間保持されます。30 日を経過すると、ステータスに関係なく、あらゆるセキュリティ侵害が表示できなくなります。

[侵害イベントタイプ（Compromise Event Types）] 機能では、指定した期間内（1 時間、1 日、7 日間、14 日間など）に検出された各イベントタイプの数が表示されます。特定のイベントタイプの通知を受信しない場合は、ベルアイコンをクリックしてイベントタイプをミュートしたり、ミュートイベントがあるときに表示される歯車アイコンをクリックしてイベントタイプのミュートを解除したりできます。

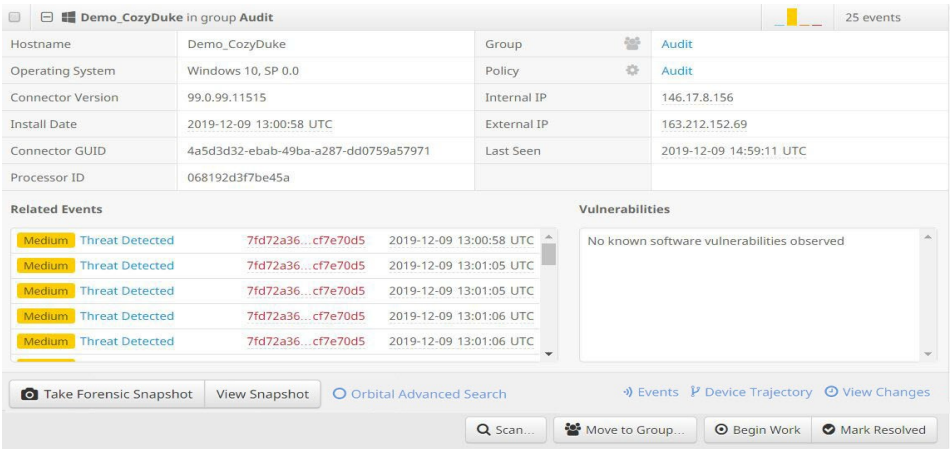
[組織の設定（Organization Settings）] ページからグローバル脅威アラートを有効にしている場合は、組織全体のエージェントレスグローバル脅威アラートの数も表示されます。このリンクをクリックすると、[エージェントレスグローバル脅威アラート（Agentless Global Threat Alerts）] ページにデバイスとインシデントのリストが表示されます。


**重要事項：**受信トレイが [重大侵害の観測対象（Significant Compromise Observables）] でフィルタ処理されている場合、複数のコンピュータに対して [解決済みとしてマーク（Mark Resolved）] をクリックしても、観測対象が複数あるコンピュータは解決済みにはなりません。複数の観測対象が複数の侵害元を示している場合、それぞれのコンピュータを個別に解決する必要があります。

1 つ以上のコンピュータを選択し、対策を開始したり、解決済みとしてマークしたり、別のグループに移動したりできます。また、[進行中（In Progress）] ステータスのコンピュータを複数選択し、[重点（Focus）] ボタンをクリックして、リスト内で該当するコンピュータのみを表示することもできます。[すべて表示（Show All）] をクリックすると、完全なリストが再び表示されます。

コンピュータが侵害されている可能性があり、解決済みとしてもマークされていないにもかかわらず、侵害されたのが 2 週間よりも前のため、[受信トレイ（Inbox）] に表示されなくなる場合があります。そのコンピュータが再度侵害されると、[受信トレイ（Inbox）] のコンピュータの横にアイコンが表示され、前の侵害がまだ解決済みとしてマークされずに残っていることが示されます。[デバイストラジェクトリ（Device Trajectory）] や [イベント（Events）] をチェックして、該当コネクタで以前の侵害イベントが検出されていて、解決されたことを確認する必要があります。

侵害されたコンピュータのエントリを展開し、そのコンピュータの基本情報、侵害に関連するイベントのリスト、およびそのコンピュータで検出された脆弱なソフトウェアを表示します。また、該当コンピュータに対して、フルスキャンやフラッシュスキャンの実行、別グループへのコンピュータの移動、診断の開始、コンピュータのデバイストラジェクトリの表示、侵害を解決済みとしてマークするなどの各種アクションを実行できます（「コンピュータの管理：コネクタの診断」を参照）。コンピュータを新しいグループに移動すると、そのコンピュータに関連付けられたの侵害データは、新しいグループのデータに表示されます。




関連イベントの名前をクリックすると、そのイベントにフォーカスしたコンピュータのデバイストラジェクトリが起動されます。関連イベントの SHA-256 をクリックすると、その SHA-256 を含む侵害イベントもある、組織内のコンピュータがすべて表示されます。

コンピュータを侵害する範囲を特定し、インシデントを解決するには、次の操作を実行します。

- 特定のコンピュータに対してフィルタ処理された [イベント（Events）] タブ を開く
- コンピュータのデバイストラジェクトリを起動する
- [変更の表示（View Changes）] をクリックして、そのコンピュータの監査ログを表示する
- ファイルスキャンまたはエンドポイント IOC スキャナを起動する

セキュリティ侵害されたコンピュータのステータスを追跡、および管理するためには、[作業開始（Begin Work）] をクリックして、選択したコンピュータの侵害の解決を開始します。作業が始まったら、コンピュータのステータスが [進行中（In Progress）] に変わります。作業が完了したら、[解決済みとしてマーク（Mark Resolved）] をクリックできます。

Cisco Secure Endpoint を使用してインシデントを解決する方法の詳細については、「Cisco Secure Endpoint デモデータストーリー」を参照してください。

# [概要（Overview）] タブ

[概要（Overview）] タブには、環境のステータスが表示され、Cisco Secure Endpoint 展開における最近の脅威と悪意のあるアクティビティが強調表示されます。各セクションの見出しをクリックして、コンソール内の関連するページに直接移動し、状況を調査して解決することができます。

- [受信トレイ（Inbox）] タブへのセキュリティ侵害のリンク

- コンピュータへのコンピュータのリンク
- AV 定義の概要への AV 定義ステータスのリンク
- [ダッシュボード（Dashboard）] タブへの脅威のリンク（検出された脅威によってフィルタ処理済み）
- [ダッシュボード（Dashboard）] タブへのネットワークの脅威のリンク（検出されたデバイス フロー コリレーション脅威、グローバル脅威アラート、および iOS ネットワーク検出によってフィルタ処理済み）
- 脆弱なソフトウェアへの脆弱性のリンク
- ファイル分析へのファイル分析のリンク

各セクションの青い項目をクリックすることでも、コンソールの該当するページに直接移動できます。


積み上げ棒グラフの上にマウスカーソルを合わせると、データの詳細ビューを表示できます。


ページの右上隅にある [グループ（Groups）] ドロップダウンメニューから選択して、表示されるデータをフィルタリングすることもできます。[すべて更新（Refresh All）] ボタンをクリックして最新のデータをページにロードしたり、[自動更新（Auto-Refresh）] ボタンをクリックして自動的にリロードされるデータの間隔を設定したりできます。ボタンに付いているドロップダウンメニューをクリックして、データをロードする時間間隔を 5、10、または 15 分から選択します。[自動更新（Auto-Refresh）] がアクティブになっている場合は、そのボタンの上にチェック マークが表示されます。ページの更新を停止するには、チェック マークをクリックしてオフにします。

**重要：**ミュートされたイベントがある場合に表示される歯車ボタンをクリックすると、[概要（Overview）] タブの [侵害（Compromise）] セクションに、ミュートされたイベントタイプが表示されます。

# [イベント（Events）] タブ

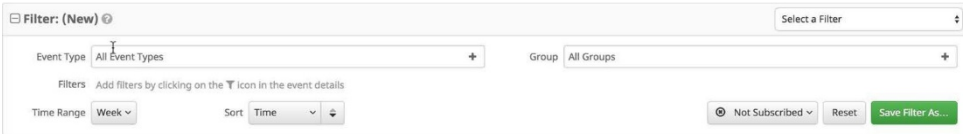
[イベント（Events）] タブには、Cisco Secure Endpoint 展開における最近のイベントが最初に表示されます。[ダッシュボード（Dashboard）] タブで脅威、IP アドレス、またはコンピュータ名をクリックして [イベント（Events）] タブに移動すると、別のフィルタ処理されたビューが表示されます。

## フィルタとサブスクリプション

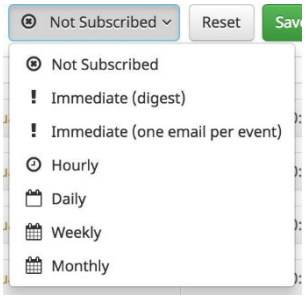
[フィルタ（Filters）] は、[イベント（Events）] タブの最上部に表示されます。右側にあるドロップダウンから過去に保存されたフィルタを選択することも、既存のイベントからイベント タイプ、グループ、特定のフィルタを追加することもできます。フィルタ基準を削除するには、削除する項目の横にある [x] をクリックします。また、[イベント（Events）] リストは、ドロップダウンリストの条件に基づいて昇順または降順にソートできます。すべてのフィルタ基準を削除するには [リセット（Reset）] ボタンをクリックします。現在のフィルタ処理されたビューを保存するには [名前を付けてフィルタを保存（Save Filter As）] ボタンをクリックします。

**重要：**[期間範囲（Time Range）] フィルタは、導入されているコネクタが 10,000 未満の場合、デフォルトで 1 週間に設定されます。導入されているコネクタが 10,000 以上の場合は、1 日に設定されます。

保存済みフィルタを表示中に、フィルタを更新し、[新規保存（Save New）] をクリックして変更内容を新しいフィルタとして保存したり、[更新（Update）] をクリックして既存のフィルタを上書きしたりできます。




フィルタ ビューをサブスクライブするには、[サブスクライブなし（Not Subscribed）] ボタンをクリックして、サブスクリプション タイミング オプション付きのメニューを表示します。イベントは、即時、毎時、毎日、毎週、または毎月の通知でサブスクライブできます。イベントごとに 1 つの電子メールで即時にアラートを受け取るオプションや、約 5 分間のイベントをまとめた 1 通の電子メールを受信するオプションがあります。




通知頻度を選択したら、[更新（Update）] をクリックして設定を保存します。フィルタ ビューの通知を受け取る必要がなくなった場合、通知の頻度を [サブスクライブなし（Not Subscribed）] に切り替えて、[更新（Update）] をクリックします。

## [SHA-256 File Info] コンテキスト メニュー

Cisco Secure Endpoint コンソールで [SHA-256] をクリックすると、追加情報を確認したり、いくつかのアクションを実行したりできるコンテキストメニューが表示されます。コンテキスト メニューには、SHA-256 の現在の分類だけでなく、それに関連付けられた特定のファイル名も表示されます。また、VirusTotal でファイルを検出したベンダー数も確認できます。VirusTotal のファイルに使用されている最も長い共通名も表示されます。

**重要事項：**Casebook が有効になっている場合、[SHA-256ファイル情報（SHA-256 File Info）] コンテキストメニューはピボットメニューに変わります。

完全な SHA-256 値をコピーまたは表示したり、その SHA-256 の検索を実行して組織内で検出された他の場所を確認したりできます。また、SHA-256 に対してファイルトラジェクトリを起動したり、それをファイル分析のために送信したりできます。

[アウトブレイクコントロール（Outbreak Control）] サブメニューを使用すると、SHA-256 をアウトブレイク コントロール リストのいずれかにすばやく追加することもできます。ここでは、SHA-256 を新規または既存の簡易リスト、ブロックリスト、または許可リストに追加するためのオプションを使用できます。

[Cisco Threat Responseで調査（Investigate in Cisco Threat Response）] を使用すると、Cisco Threat Response でファイル、URL、IP アドレスのリストを確認できます。

**重要：**特権のないユーザーはコンテキスト メニュー上のすべての項目にアクセスできません。

## イベントリスト

イベントリストには、検出したコンピュータの名前、検出の名前、最近実行されたアクション、およびイベントの日付と時刻が表示されます。イベントに関連付けられたコマンド ラインの引数があった場合、それも合わせて表示されます。イベントをクリックすると、検出に関する詳細情報、コネクタの情報、およびイベントに関するコメントが表示されます。詳細ビューでは、情報アイコンを使用してコンテキスト メニューにアクセスできます。コンピュータエントリ用のコンテキストメニューを使用すると、そのコンピュータのデバイストラジェクトリを起動したり、[コンピュータの管理（Computer Management）] ページを開いたりできます。ファイルエントリ用のコンテキストメニューは [SHA-256ファイル情報（SHA-256 File Info）] コンテキストメニューと同じです。ファイルを取得して、ファイル分析に送信するには、[分析（Analyze）] ボタンをクリックします。ファイルを取得するには、ファイルリポジトリを有効にする必要があります。あるファイルが検疫されると、そのファイルを、特定のコンピュータ、または、そのファイルを検疫したすべてのコンピュータのどちらに復元するか選択できます。ファイルは 30 日間隔離されたままになり、その後は復元できません。

**重要：**[分析（Analyze）] ボタンを使用できない場合は、ファイルがすでに送信済みであるか、ファイルリポジトリが有効になっていないか、または現在のユーザーが管理者ではない可能性があります。

フィールドが一致するエントリでリストビューをフィルタ処理するには、フィルタアイコン付きのエントリをクリックします。また、[CSVにエクスポート（Export to CSV）] ボタンを使用すると、イベントを CSV ファイルで要求できます。CSV ファイルが生成されると、その CSV ファイルを含むアーカイブファイルをダウンロードするためのリンクを含む電子メールを受信します。Splunk などのアプリケーションで API を使用して、多数のイベントのイベントストリームを作成することもできます。

**重要：**以前に要求した CSV ファイルがまだ生成されている間に [CSVにエクスポート（Export to CSV）] ボタンをもう一度クリックすると、要求をキャンセルして再開するオプションが表示されます。

**重要事項：**エクスポートされた CSV ファイルの日時は、タイムゾーンの設定に関係なくすべて UTC 表示です。

**重要事項：**脅威名の説明については、AMP 命名規則を参照してください。

### 動作保護イベント

動作保護エンジンによって生成されるイベントには、追加情報が含まれます。検出に関連するインジケータはすべて、[戦術（Tactics）] フィールドと [手法（Techniques）] フィールドに一覧表示されます。イベントの残りの部分は 3 つのセクションで構成されます。

#### オブザーバブル（Observables）

イベントに関連するすべてのファイル、ホスト、および IP アドレスが一覧表示されます。観察されたファイルを分析のためにファイルリポジトリにアップロードする要求を開始できます。該当する場合は、ファイルトラジェクトリとデバイストラジェクトリへのリンクも表示されます。

#### 観察されたアクティビティ

ここでは、検出された攻撃の一部であったすべてのアクティビティの概要が提供されます。これには、インシデント対応分析の一部として使用できる、検出に関するファイル、プロセス、レジストリ、およびネットワークイベントが含まれます。

#### 操作

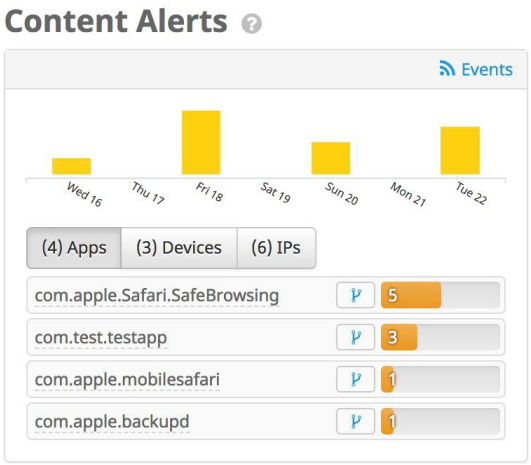
イベントのコンポーネントに対してコネクタによって実行されるアクション（存在する場合）とアクションの結果が一覧表示されます。アクションには、ファイルの隔離、プロセスの終了、分析のためのファイルのアップロードが含まれます。動作保護が保護モードの場合にのみ、アクションが実行されます。

## [iOS Clarity] タブ

[ダッシュボード（Dashboard）] に移動して、[iOS Clarity] タブを選択します。Meraki SM やその他の Mobile Device Manager（MDM）にすでにリンクを設定している場合、このタブには、アクティビティのサマリー、管理対象 iOS デバイスで最近監視されたアプリケーションのリスト、および 7 日以上報告がないデバイスのリストが表示されます。

## コンテンツアラート

**コンテンツアラート**には、過去 7 日間に確認された悪意のあるサイトとブロックされたサイトの概要が表示されます。コンテンツアラートは、デバイスで [判定モード（Conviction Modes）] が [監査（Audit）]、[ブロック（Block）]、または [アクティブブロック（Active Block）] に設定されている場合に生成されます。[イベント（Events）] リンクをクリックして、[イベント（Events）] タブのフィルタ処理されたビューを表示し、これらのイベントのみを確認できます。



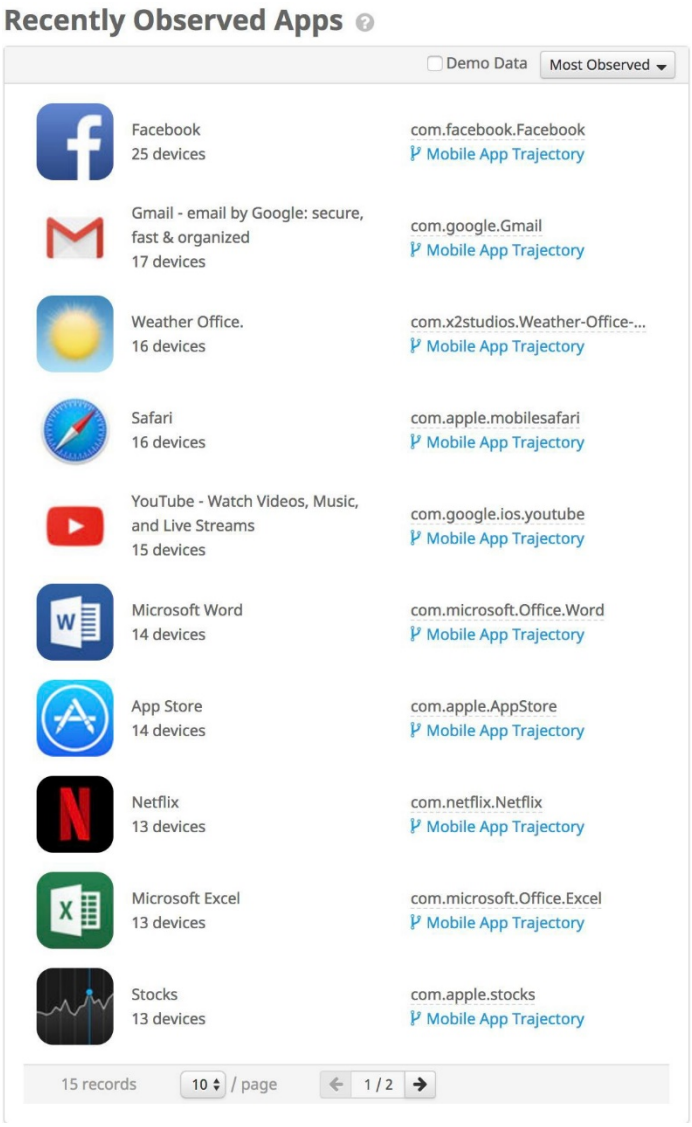

[アプリケーション（Apps）] タブには、悪意のある IP や IP ブロックリストにあるアドレスに接続していることが確認されたデバイス上の上位 5 つのアプリケーションと、各アプリケーションが過去 7 日間に接続を試みた回数が表示されます。アプリケーションの名前をクリックして、アプリケーションの名前、パブリッシャとその他のオプション（そのアプリケーションのモバイル アプリ トラジェクトリへのリンクなど）を示すコンテキストメニューを表示できます。

[デバイス（Devices）] タブには、悪意のある IP や IP ブロックリスト にあるアドレスへの接続を試みた上位 5 つのデバイスと、各デバイスが過去 7 日間に接続を試みた回数が表示されます。また、そのデバイスの [イベント（Events）] タブのフィルタ処理されたビューとデバイストラジェクトリを表示するためのアイコンもあります。

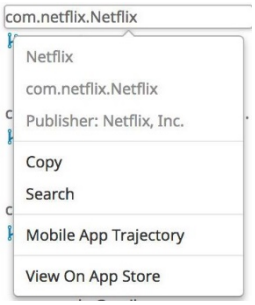
[IP（IPs）] タブには、デバイスが過去 7 日間に接続を試みた上位 5 つの悪意のある IP アドレスまたはブロックされた IP アドレスが表示されます。IP アドレスをクリックして詳細情報（[ウイルス全体（Virus Total）] の結果など）を表示したり、Cisco Threat Response でファイルを調査したりすることができます。

## 最近確認されたアプリケーション

[最近確認されたアプリケーション（Recently Observed App）] リストには、アプリケーションの名前、確認されたデバイスの数、バンドル ID、モバイル アプリ トラジェクトリにアプリケーションを表示するためのリンクが表示されます。組織から得られた**実際のデータ**と**デモデータ**の間でビューを切り替えることもできます。




バンドル ID をクリックして、アプリ名、パッケージ名、および発行元の名前を表示するメニューを有効にします。また、パッケージ名をコピーしたり、一致アクティビティがある他のアプリケーションの Cisco Secure Endpoint データを検索したりできます。このメニューは、Cisco Secure Endpoint コンソールに表示されている任意のバンドル ID をクリックして表示できます。




## 未表示のデバイス

[未表示のデバイス（Unseen Device）] には、7 日以上報告がない iOS デバイスが表示されます。10 台を超えるデバイスがリストに含まれている場合、それらのデバイスはグループ別に集約されます。グループ名をクリックして、7 日以上報告がないデバイスのリストが表示される [コンピュータ（Computers）] ページのフィルタ 処理されたビューを確認します。

# 第 2 章

# 感染管理

Cisco Secure Endpoint は、アウトブレイクコントロールと呼ばれる、ニーズに合わせてカスタマイズ可能な多様なリストを提供します。主要なリストには、シンプルカスタム検出、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、高度なカスタム検出、IP ブロック/許可リストなどがあります。これらのリストについて以降の項で説明します。

## カスタム検出：簡易

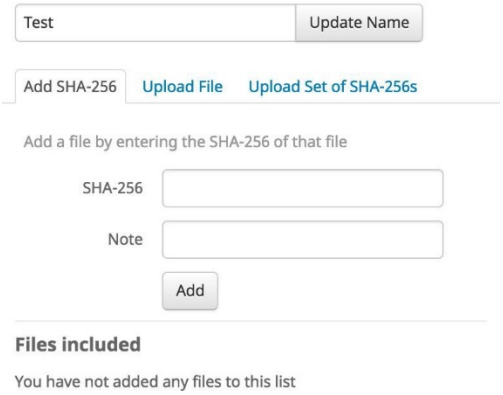
シンプルカスタム検出リストはブロックリストに似ています。このリストは検出して検疫するファイルです。シンプル カスタム検出リスト内のエントリは、以降のファイルを検疫するだけでなく、レトロスペクティブ検出により、サービスが検出した組織内のエンドポイント上でファイルのインスタンスも検疫します。

簡易カスタム検出リストを作成するには、[アウトブレイク制御（Outbreak Control）] > [簡易（Simple）] に移動します。[作成（Create）] をクリックして新しいシンプルカスタム検出を作成し、名前を入力して、[保存（Save）] をクリックします。

シンプルカスタム検出を保存してから [編集（Edit）] をクリックすると、リストに値を追加する 3 種類の方法が表示されます。

単一の SHA-256 を追加して、ファイルに関する注釈を作成できます。ファイル（最大 20MB）をアップロードでき、そのファイルから SHA-256 を取得して、メモを追加できます。SHA-256 のセットもアップロードできます。SHA-256 のセットをアップロードする際は、1 行に 1 つの SHA-256 が指定された単一のテキストファイルに収める必要

があります。右下にある [含まれているファイル（Files included）] リンクをクリックすると、SHA-256 とメモを確認できます。不要な SHA-256 を追加した場合は、[削除（Remove）] をクリックできます。リストの名前を編集して、[名前の更新（Update Name）] をクリックすることによって、名前を変更することもできます。




シンプルカスタム検出を追加する場合、ポリシーの [キャッシュ（Cache）] タブで指定されているキャッシングの対象になることに注意してください。ファイルがキャッシュされる時間のデフォルトの長さは、ファイルの属性によって次のように異なります。

- クリーン ファイル：7 日間
- 不明なファイル：1 時間
- 悪意のあるファイル：1 時間

シンプル カスタム検知リストにファイルが追加された場合、検知が有効になるのはキャッシュ時間が過ぎた後です。たとえば、不明なファイルがキャッシュされてから 5 分後にそのファイルのシンプル カスタム検出を追加した場合は、その時点から 55 分後まで検出は有効になりません。

**重要事項：**シスコのグローバル許可リストに登録されているファイルや、まだ失効していない証明書で署名されているファイルを追加することはできません。誤って分類または署名されているファイルが見つかり、署名者を取り消したい場合は、サポートに連絡してください。

[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、シンプルカスタム検出エントリのみ表示されます。シンプルカスタム検出リストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、その検出リストのレコードのみ表示されます。

# カスタム検出：高度

高度なカスタム検出は、従来型のウイルス対策シグニチャに類似していますが、ユーザーにより作成される点が異なります。これらのシグネチャは、ファイルのさまざまな側面を検査し、異なるシグネチャの形式を使用できます。使用可能なシグニチャ形式の一部を以下に示します。

- MD5 シグニチャ
- MD5、PE セクションベースのシグニチャ
- ファイル本文ベースのシグニチャ
- 拡張シグニチャ形式（オフセット、ワイルドカード、正規表現）
- 論理的シグニチャ
- アイコン シグニチャ

シグニチャ形式の詳細については、https://docs.clamav.net/manual/Signatures.html で確認できます。これらのシグニチャは、エンドポイントにダウンロードされるファイルにコンパイルされます。

高度なカスタム検出を作成するには、[アウトブレイクコントロール（Outbreak Control）] > [高度（Advanced）] に移動します。[シグニチャセットの作成（Create Signature Set）] をクリックして、新しい高度なカスタム検出セットを作成し、それに名前を付けて、[作成（Create）] をクリックします。

高度なカスタム検出セットを作成してから [編集（Edit）] をクリックすると、[署名の追加（Add Signature）] リンクが表示されます。署名の名前を入力後、[作成（Create）] をクリックします。

すべての署名が一覧表示されたら、[署名セットからデータベースを構築（Build a Database from Signature Set）] を選択します。誤って不要なシグニチャを追加した場合は、[削除（Remove）] をクリックすることによって、それを削除できます

**重要：**シグニチャを追加または削除する場合は、必ず、[署名セットからデータベースを構築（Build a Database from Signature Set）] をクリックする必要があります。

ファイルの高度なカスタム検出を作成する場合は、それが 1 時間のキャッシングの対象になることに注意してください。高度なカスタム検出セットにファイルが追加された場合、検出が有効になるのはキャッシュ時間が過ぎた後です。たとえば、不明なファイルがキャッシュされてから 5 分後に高度なカスタム検出を追加した場合は、その時点から 55 分後まで検出は有効になりません。

**重要：**高度なカスタム検出は、不明な分類のファイルのみで動作します。

[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、高度なカスタム検出エントリのみ表示されます。1 つのリストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、その検出リストのレコードのみ表示されます。

## カスタム検出 - Android

Android カスタム検出リストは、デバイス ユーザーが望ましくないアプリケーションに関する警告を受け取り、手動でそのアプリケーションをアンインストールする必要があることを除いて、簡易カスタム検出リストと同様です。新しい悪意のあるアプリケーション、または、ユーザーにインストールを許可しないアプリケーションを Android カスタム検出リストに追加できます。

Android カスタム検出リストを作成するには、[アウトブレイク制御（Outbreak Control）] > [Android] に移動します。[作成（Create）] をクリックして新しい Android カスタム検出を作成し、名前を入力して、[保存（Save）] をクリックします。

カスタム検出を保存したら、[編集（Edit）] をクリックし、APK ファイルをアップロードすることでアプリケーションを追加できます。リストにアプリケーションを追加したら、[保存（Save）] をクリックします。

[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、Android カスタム検出エントリのみ表示されます。1 つの Android カスタム検出リストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、その検出リストのレコードのみ表示されます。

## 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

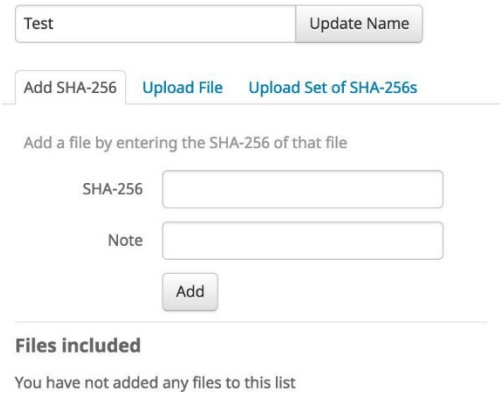
ブロックされたアプリケーションリストには、ユーザーに実行を許可しないものの、検疫もしないファイルが含まれます。このリストは、そのファイルがマルウェアや無許可のアプリケーションであると断定できない場合、または脆弱性があるアプリケーションの実行をパッチがリリースされるまで禁止する場合に使用できます。

**重要：**任意の SHA-256 値をブロックされたアプリケーションリストに追加できますが、開くことができないのは実行可能なタイプのファイルのみです。

ブロックされたアプリケーションリストを作成するには、[アウトブレイクコントロール（Outbreak Control）] > [ブロックされたアプリケーション（Blocked Applications）] に移動します。[作成（Create）] をクリックして新しいブロックされたアプリケーションリストを作成し、名前を入力して、[保存（Save）] をクリックします。

ブロックされたアプリケーションリストを保存してから [編集（Edit）] をクリックすると、そのリストに値を追加する 3 種類の方法が表示されます。

単一の SHA-256 を追加して、ファイルに関する注釈を作成できます。ファイル（最大 20 MB）をアップロードし、そのファイルから SHA-256 を取得して注釈を追加することも、一連の SHA-256 をアップロードすることもできます。一連の SHA-256 をアップロードする場合、1 行ごとに SHA-256 が 1 つ存在するテキスト ファイルの形式になっている必要があります。右下にある [含まれているファイル（Files included）] リンクをクリックすると、SHA-256 とメモを確認できます。不要な SHA-256 を誤って追加した場合は、[削除（Remove）] をクリックします。リストの名前を編集して、[名前の更新（Update Name）] をクリックすることによって、名前を変更することもできます。




ファイルをブロックされたアプリケーションリストに追加する場合は、それがキャッシュの対象になることに注意してください。ファイルがローカルキャッシュ内に存在せず、ポリシーで [実行開始モード（On Execute Mode）] が [パッシブ（Passive）] に設定されている場合は、ブロックされたアプリケーションリストにファイルを追加した後で初めてファイルが実行されたときに、ファイルの実行が許可される可能性があります。ポリシーで [オンエグゼキュートモード（On Execute Mode）] を [アクティブ（Active）] に設定すると、この問題を避けることができます。

ファイルがローカル キャッシュ内に存在する場合、アプリケーション ブロッキングが有効になるのはキャッシュ時間が過ぎた後です。ファイルがキャッシュされる時間の長さは、ファイルの属性と、ポリシーの [キャッシュ（Cache）] タブで指定された時間の長さによって異なります。デフォルト値は次のとおりです。

- クリーン ファイル：7 日間
- 不明なファイル：1 時間
- 悪意のあるファイル：1 時間

ファイルがブロックされたアプリケーションリストに追加された場合、検出が有効になるのはキャッシュ時間が過ぎた後です。たとえば、不明なファイルがキャッシュされてから 5 分後にそのファイルをリストに追加した場合は、その時点から 55 分後まで検出が有効になりません。

[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、ブロックされたアプリケーションのエントリのみ表示されます。1 つのブロックされたアプリケーションリストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、そのブロックされたリストのレコードのみ表示されます。

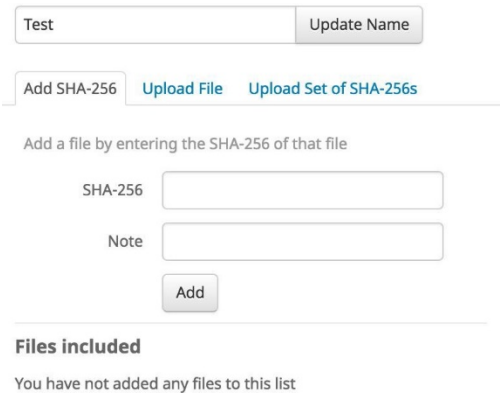
## アプリケーション制御：許可されたアプリケーション

許可されたアプリケーションリストは、全面的に信用できるファイル用です。使用例としては、全社で使用している汎用エンジンや、標準イメージによって検出されたカスタムアプリケーションなどが挙げられます。

許可されたアプリケーションリストを作成するには、[アウトブレイクコントロール（Outbreak Control）] > [許可されたアプリケーション（Allowed Applications）] に移動します。次に、[作成（Create）] をクリックして新しい許可されたアプリケーションリストを作成し、名前を入力して、[保存（Save）] をクリックします。

許可されたアプリケーションリストを保存してから [編集（Edit）] をクリックすると、そのリストに値を追加する 3 種類の方法が表示されます。

単一の SHA-256 を追加して、ファイルに関する注釈を作成できます。ファイル（最大 20 MB）をアップロードし、そのファイルから SHA-256 を取得して注釈を追加することも、一連の SHA-256 をアップロードすることもできます。SHA-256 のセットをアップロードする際は、1 行に 1 つの SHA-256 が指定された単一のテキストファイルに収める必要があります。SHA-256 とメモは、右下の [含まれているファイル（Files included）] リンクをクリックすると確認できます。不要な SHA-256 を追加した場合は、[削除（Remove）] をクリックします。リストの名前を編集して、[名前の更新（Update Name）] をクリックすることによって、名前を変更することもできます。




[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、許可されたアプリケーションリストのエントリのみ表示されます。1 つの許可されたアプリケーションリストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、その許可されたリストのレコードのみ表示されます。

# ネットワーク：IP ブロック/許可リスト

IP ブロックリストと IP 許可リストは、カスタム IP アドレス検出を定義するためのデバイス フロー コリレーションで使用します。リストを作成したら、Cisco Intelligence Feed と一緒に使用するか、単独で使用するようにポリシーで定義できます。

リストは、個別の IP アドレス、CIDR ブロック、または IP アドレスとポートの組み合わせを使用して定義できます。リストを送信すると、バックエンドで冗長なアドレスが付加されます。

たとえば、リストに次のエントリを追加した場合:

```
192.168.1.0/23
192.168.1.15
192.168.1.135
192.168.1.200
```

リストは、次の最終結果で処理されます。

```
192.168.1.0/23
```

ただし、ポートも含める場合は結果が異なります。

```
192.168.1.0/23
192.168.1.15:80
192.168.1.135
192.168.1.200
```

リストは、次の最終結果で処理されます。

```
192.168.1.0/23
192.168.1.15:80
```

IP アドレスに関係なく、ポートをブロックリストまたは許可リストに追加するには、以下のように、2 つのエントリを該当リストに追加します。XX はブロックするポート番号を表します。

```
0.0.0.1/1:XX
128.0.0.1/1:XX
```

**重要：**アップロードする IP リストは、含まれる行数が 100,000 以下で、サイズが 2 MB 以下にする必要があります。現在は、IPv4 アドレスしかサポートされていません。

[すべての変更を表示（View All Changes）] リンクをクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、 IP ブロックリストと許可リストのエントリのみ表示されます。1 つの IP リストの横にある [変更の表示（View Changes）] をクリックすると、フィルタ処理されたすべてのレコードを含む監査ログが表示され、その IP リストのレコードのみ表示されます。

## IP ブロックリスト

IP ブロックリストを使用すると、ユーザーのコンピュータのいずれかが接続するたびに検出される IP アドレスを指定できます。単一の IP アドレスを追加することも、CIDR ブロック全体を追加することも、あるいは IP アドレスとポート番号の両方を指定することもできます。コンピュータがリスト内の IP アドレスに接続したときに実行されるアクションは、ポリシーの [ネットワーク（Network）] セクションで指定した内容によって異なります。

## IP 許可リスト

IP 許可リストを使用すると、検出されない IP アドレスを指定できます。IP 許可リスト内のエントリは、IP ブロックリストだけでなく、Cisco Intelligence Feed に対しても優先されます。単一の IP アドレスを追加することも、CIDR ブロック全体を追加することも、あるいは IP アドレスとポート番号の両方を指定することもできます。

## IP 隔離許可リスト

IP 隔離許可リストを使用すると、エンドポイントを隔離するときに Cisco Secure Endpoint Windows および Mac コネクタでブロックされない IP アドレスを指定できます。これにより、エンドポイントはアクティブなエンドポイント隔離セッション中にネットワーク内の信頼されている場所と通信し、さらなる調査を行うことができます。このリストには、最大 200 個の IPv4 アドレスを追加できます。IP 隔離許可リストはポート番号をサポートしていません。

**重要：**デフォルトでは許可リストにすべての Cisco Secure Endpoint Cloud アドレスが含まれているため、コネクタで、ポリシーの更新の受信、クラウドルックアップの実行、および隔離ステータスの更新ができます。

## IP ブロックリストと IP 許可リストの作成

IP リストを作成するには、[アウトブレイクコントロール（Outbreak Control）] > [IPブロック/許可リスト（IP Block & Allow Lists）] に移動して、[IPリストの作成...（Create IP List...）] をクリックします。これにより、[新しいIPリスト（New IP List）] ページが表示されます。新しいリストの名前と説明を入力し、[リストタイプ（List Type）] ドロップダウンリストから [許可（Allow）]、[ブロック（Block）]、または [隔離許可（Isolation Allow）] を選択します。行ごとに 1 つの IP アドレスまたは CIDR ブロックを入力できます。[行の追加（Add Row）] をクリックして、単一の行を追加できます。[複数行の追加（Add Multiple Rows）] をクリックして、複数の IP アドレスと CIDR ブロックをすばやく追加することもできます。次のダイアログに IP アドレスと CIDR ブロックのリストを入力または貼り付けてから、[行の追加（Add Rows）] をクリックします。

また、改行文字で区切られた IP アドレスと CIDR ブロックを含む CSV ファイルをアップロードすることもできます。ファイルをアップロードするには、[アップロード...（Upload...）] をクリックし、[参照（Browse）] をクリックして CSV ファイルを選択し、[アップロード（Upload）] をクリックします。

## IP ブロックリストと IP 許可リストの編集

IP リストを編集するには、[アウトブレイクコントロール（Outbreak Control）] > [IPブロック/許可リスト（IP Block & Allow Lists）] に移動します。編集する IP リストの横にある [+] をクリックして、ビューを展開します。[編集（Edit）] をクリックします。リストに含まれている項目が 500 未満の場合には、デフォルトのリストエディタが表示され、行を編集、追加、削除できます。リストに 500 以上の項目がある場合には、長いリストエディタが表示されます。このリストエディタでは、大きなリストを簡単に参照および編集できますが、ライブ入力検証は実行できません。

完了したら、[保存（Save）] をクリックします。長いリストエディタを使用している場合には、[エラーの発生しているIP/CIDRブロック（IPs / CIDR Blocks with Errors）] リストに無効な項目が表示されます。これを使用して、リストを再保存する前に項目を編集できます。

**重要：**[変更を元に戻す（Revert Changes）] をクリックすると、いつでも IP リストを編集前の状態に戻せます。

### ブロックリストと許可リストのエクスポートと置換

IP アドレスと CIDR ブロックのリストを含む CSV ファイルをダウンロードして、オフラインで作業することもできます。リストをダウンロードするには、ダウンロードする IP リストのビューを展開してから、[エクスポート（Export）] をクリックします。

既存のリストをアップロードして置き換えるには、アップロードする IP リストのビューを展開してから、[置換...（Replace...）] をクリックします。[参照（Browse）] をクリックして、リストを含むファイルを選択し、[置換（Replace）] をクリックします。

# 第 3 章

# デバイス制御

デバイス制御を使用すると、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できます。また、可視性を利用してエンドポイントに接続されているデバイスを確認できます。たとえば、デバイストラジェクトリでセキュリティ侵害を調査する際、デバイスのブロックといったデバイス制御イベントを確認できます。このようなイベントをフィルタリングしてページ内で見やすくすることも可能です。

詳細な制御により、承認された USB デバイス以外が環境で使用されないようにするルールを作成できます。組織には USB デバイスの管理方法に関する独自の設定があるため、Cisco Secure Endpoint では、さまざまな設定や使用例に対応できる詳細なルールを提供しています。

たとえば、一般的なポリシー（読み取り/書き込み/実行のブロックなど）を定義すると同時に、デバイスプロパティに基づいて特定のタイプのデバイスを許可する詳細なルールを作成することができます。ルールは必要な実施順序に合わせて並べ替えることができます。また、ルールはポリシーに割り当てられるため、管理のしやすさ（ポリシー間でルールセットを共有）と詳細な制御（ポリシーおよびグループごとに異なるルールセットを使用）のバランスをとることができます。

新しいデバイス制御設定を作成できるのは管理者だけです。非特権ユーザーは、アクセス制御で権限を付与された設定を管理でき、設定内のルールの追加、更新、削除、および並べ替えや、アクセス可能なポリシーへの設定の追加が可能です。

**重要：**デバイス制御は Cisco Secure Endpoint Windows コネクタ 8.1.3 以降で使用でき、8.2.1 以降では WPD がサポートされます。

# デバイス制御の設定とルール

デバイス制御ルールは設定の一部です。デバイス制御の設定はポリシーに追加され、そのポリシーを使用するグループ内のエンドポイントによって処理されます。

デバイス設定の監査モードはありません。デバイス制御の設定は、接続されている USB 大容量ストレージデバイスおよび WPD のみを収集し、デバイスへのアクセスを制限しないように作成できます。読み取り、書き込み、および実行の基本ルールを含む設定を作成します。すべての USB 大容量ストレージデバイスおよび WPD が許可され、イベントが [イベント（Events）] ページと [デバイストラジェクトリ（Device Trajectory）] に表示されます。

**重要：**実行は現在サポートされていないため、WPD の読み取り、書き込み、および実行のオプションはありません。

## デバイス制御設定の作成

新しいデバイス制御設定を作成できるのは管理者だけです。

1. [管理（Management）] -> [デバイス制御（Device Control）] に移動します。
2. [新規設定（New Configuration）] をクリックします。
3. 設定に対して一意の名前を入力します。
4. 設定の説明を入力します（任意）。
5. USB 大容量ストレージまたは Windows ポータブルデバイスを選択します。
6. 基本ルールの権限を選択します。各権限の説明については、「デバイス制御の権限」を参照してください。
7. デバイス制御ルールがトリガーされたときに、エンドポイントに通知を表示するかどうかを選択します。

   **重要事項：**Cisco Secure Endpoint Windows コネクタ 8.1.3 の場合、エンドポイントに通知を表示するには、ポリシーでクライアント ユーザー インターフェイスの [エンジン通知（Engine Notifications）] を有効にする必要があります。これは、バージョン 8.1.5 以降では必要ありません。

8. [保存（Save）] をクリックします。

ルールを指定しない設定は、その設定タイプの全デバイスに影響を与えます。詳細な制御のためのルールを設定に追加すると、特定の USB 大容量ストレージデバイスを許可またはブロックすることができます。たとえば、すべての USB 大容量ストレージデバイスをブロックし、特定のベンダーのデバイスへの読み取りおよび書き込みアクセスを許可するような設定を作成できます。

## 設定へのルールの追加

1 つの設定に最大 1000 のルールを追加できます。ルールを作成するには、次の識別子の少なくとも 1 つが必要です。

識別子

| 基準 | 説明 |
|---|---|
| ベンダー名 | メーカー名ともいいます。 |
| Vendor ID | USB 委員会によってベンダーに割り当てられる 4 桁のコード。<br>一般的な使用例：複数のエンドポイントで、特定のベンダーからのデバイスをブロックまたは許可します。 |
| 製品名 | わかりやすい名前またはデバイス名とも呼ばれます。 |
| 製品 ID | ベンダーによって特定の製品に割り当てられる 4 桁のコード。<br>一般的な使用例：複数のエンドポイントで、あるモデルやタイプのデバイスに対してデバイスをブロックまたは許可します。 |
| インスタンス ID | ベンダー ID と製品 ID で構成される一意の識別子。<br>一般的な使用例：特定のエンドポイント（エンドポイント間ではなく）のコンテキストで、特定のデバイスをブロックまたは許可します。 |
| デバイスID | ベンダー ID と製品 ID を含むインスタンス ID の最初の部分。<br>一般的な使用例：複数のエンドポイントで特定の USB デバイスをブロックまたは許可します。 |

**重要：**シリアル番号は USB メーカーの任意のフィールドであり、信頼性が低いため、基準として使用されません。

[デバイス制御（Device Control）] ページ、イベントリストのデバイス制御イベント、またはデバイストラジェクトリのデバイス制御イベントから設定にルールを追加できます。

設定のルールを作成するには、次の操作を実行します。

1. 設定の名前、または [アクション（Actions）] の下の [設定の編集（Edit Configuration）] ボタンをクリックします。
2. [ルールの追加（Add Rule）] をクリックします。
3. ルールの説明を入力します（任意）。
4. ルールをトリガーするために、条件のいずれかを満たす必要があるか、またはすべてを満たす必要があるかを選択します。[いずれか（Any）] は論理 OR に相当し、[すべて（All）] は論理 AND に相当します。

5. [値（Value）] フィールドに使用する識別子を選択します。
6. ルールの演算子を選択します。
7. ルールの条件をさらに追加するには、[条件の追加（Add Condition）] をクリックします。それ以外の場合は、ステップ 8 に進みます。
8. ルールの権限を選択します。各権限の説明については、「デバイス制御の権限」を参照してください。
9. デバイス制御ルールがトリガーされたときに、エンドポイントに通知を表示するかどうかを選択します。

> **重要事項：**Cisco Secure Endpoint Windows コネクタ 8.1.3 の場合、エンドポイントに通知を表示するには、ポリシーでクライアント ユーザー インターフェイスの [エンジン通知（Engine Notifications）] を有効にする必要があります。これは、バージョン 8.1.5 以降では必要ありません。

10. [保存（Save）] をクリックします。

## デバイス制御の権限

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

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

### ポリシーへの設定の追加

設定がエンドポイントによって処理されるようにするには、設定をポリシーに割り当てる必要があります。次の 2 つの方法のいずれかで、設定をポリシーに追加できます。

1. [管理（Management）] > [ポリシー（Policies）] の順に移動します。目的のポリシーを編集し、[デバイス制御（Device Control）] タブに移動します。プルダウンから設定を選択し、ポリシーを保存します。
2. [デバイス管理（Device Management）] ページから、ポリシーに追加する設定を選択します。[ポリシーに割り当て（Assign to Policies）] をクリックし、設定を割り当てる 1 つ以上のポリシーを選択します。

**重要：**1 つのポリシーに複数の設定を割り当てられますが、設定タイプごとに 1 つのみです。

## 既知の問題と制限事項

- デバイス制御の対象は現在、USB 大容量ストレージデバイスと USB を介して接続された Windows ポータブルデバイスに制限されています。
- 特定の条件下では、コネクタをアップグレード/アンインストールするときに、デバイス制御の再起動が必要になる場合があります。デバイス制御がエンドポイントで少なくとも 1 回有効になっている場合、これによりデバイス制御ドライバがエンドポイントにインストールされ、次のシナリオの 1 つ以上が発生します。
  - （アップグレード）バージョン 8.2.1 へのアップグレード時に既存の外部デバイスが存在する場合、再起動しないと WPD サポートが想定どおりに機能しない可能性があります。
  - （アンインストール）エンドポイントに現在接続されている外部デバイスからドライバをクリーンに接続解除できない場合。
- デバイス制御機能が有効になっている場合、エンドポイントに現在接続されている USB 大容量ストレージデバイスは、デバイスが再接続されるか、エンドポイントが再起動されるまで管理できない場合があります。
- USB 大容量ストレージデバイスがすでにエンドポイントに接続されており、そのデバイスに影響を与える新しいルール（たとえば、書き込みアクセスをブロックするルールを追加する）が展開された場合、そのデバイスでアクション（デバイスで新しいファイルを作成する）が許可されているように見えることがありますが、デバイスのプラグを抜いて再度プラグを差し込むと、アクションが完了しなかったことがユーザーに表示されます。
- スロットリングの制限により、後続の挿入イベントがスキップされる場合があります。

- 書き込み権限がブロックされたエンドポイントに USB 大容量ストレージデバイスがすでに接続されていて、デバイスへの書き込み権限を許可する新しいルールが展開された場合、またはデバイス制御機能がポリシーで無効になった場合、USB デバイスに NTFS ファイルシステムがあると、書き込み権限はデバイスが再接続されるまで引き続きブロックされます。
- バージョン 8.1.7 を実行しているエンドポイントに接続されている一部の Android デバイスは、バージョン 8.2.1 へのアップグレード後に Windows のデバイスマネージャに表示されない場合があります。このデバイス用に作成されたデバイス制御ルールが、想定どおりに機能しない可能性があります。この問題を解決するには、デバイスを取り外して再度接続する必要があります。
- デバイス制御機能は、HyperV 仮想マシンでの動作に制限がある場合があります。
- iTunes などの外部アプリケーションは、デバイス制御ルールによってブロックされるデバイスを引き続き管理できます。

# 第 4 章

# 除外事項

除外設定は、Cisco Secure Endpoint コネクタでスキャンまたは判定しないディレクトリ、ファイル拡張子、または脅威名のリストです。[管理（Management）] > [除外（Exclusions）] に移動し、除外設定の一覧を表示します。除外では、頻繁に書き込まれる大きなファイル（データベースなど）を含むディレクトリを除外することで、他のセキュリティ製品との競合を解消したり、パフォーマンス低下を軽減したりできます。Cisco Secure Endpoint コネクタによる単一ファイルの検疫（誤検出など）を停止する場合は、アプリケーション制御：許可されたアプリケーションを使用します。

**警告：**除外リストに追加されたディレクトリ内のファイルは、アプリケーション ブロッキング、シンプル カスタム検出、または高度なカスタム検出のリストの対象になりません。

除外設定の作成の詳細については、「Secure Endpoint の除外対象のベストプラクティス」を参照してください。

## ウイルス対策製品の互換性の構成

コネクタとアンチウイルスまたはその他のセキュリティソフトウェア間での競合を避けるには、コネクタがアンチウイルスソフトウェアのディレクトリをスキャンせず、かつアンチウイルスソフトウェアがコネクタのディレクトリをスキャンしないように除外項目を作成する必要があります。悪意のあるファイル、または検疫済みのファイルに伴う問題であるとコネクタで判断された文字列がウイルス対策署名に含まれている場合、問題になる可能性があります。

詳細については、「除外を使用したウイルス対策の互換性」を参照してください。

# カスタム除外設定

[カスタム除外設定（Custom Exclusions）] ボタンをクリックして、組織で作成された除外設定を表示または編集したり、新しい除外設定を作成したりします。各行には、オペレーティングシステム、除外設定名、除外対象数、除外設定を使用するグループの数、除外設定を使用するコンピュータの数が表示されます。検索バーを使用して、名前、パス、拡張子、脅威名、または SHA-256 で除外セットを検索できます。それぞれのタブをクリックして、オペレーティングシステム別にリストをフィルタ処理することもできます。[すべての変更を表示（View All Changes）] をクリックすると、監査ログのフィルタ処理されたリストが表示され、除外設定のすべての変更が表示されます。

除外設定をクリックすると、設定の詳細が展開されます。このビューで [変更の表示（View Changes）] をクリックして、その除外設定に加えた変更を確認できます。

**重要：**付与されているアクセス許可に応じて、特定のグループやポリシーを表示できないことがあります。

ここから除外設定を編集または削除することもできます。

**重要：**ポリシーで使用されていない除外設定のみを削除できます。1 つ以上のポリシーで除外設定が使用されている場合、[削除（Delete）] ボタンはグレー表示（無効）となります。

カスタム除外設定を作成するには、[新規除外設定（New Exclusion Set）] をクリックします。Cisco Secure Endpoint Windows、Cisco Secure Endpoint Mac、または Cisco Secure Endpoint Linux のコネクタを除外するかを選択できるダイアログが表示されます。[作成（Create）] をクリックします。

新しい除外設定には、デフォルトの除外対象が事前に設定されています。指定のフィールドに新しい除外設定の名前を入力します。

空のドロップダウンメニューをクリックして、追加する除外タイプを選択します（「除外タイプ」を参照）。

除外タイプを選択したら、パス、脅威名、ファイル拡張子、プロセス、またはファイル名、拡張子、パスに対するワイルドカードを入力します。設定に除外対象を追加する場合は、[除外対象の追加（Add Exclusion）] をクリックします。完了した場合は [保存（Save）] をクリックします。[変更を元に戻す（Revert Changes）] をクリックすると、いつでも最後に保存した除外設定のバージョンに戻せます。

[複数の除外対象を追加...（Add Multiple Exclusions...）] をクリックすると、一度に複数の除外対象を追加することもできます。次のダイアログに除外対象のリストを入力するか、貼り付けて、完了したら [除外対象の追加（Add Exclusions）] をクリックします。除外タイプは自動的に検出され（可能な場合）、除外設定に追加されます。検出されない除外対象は、除外タイプがブランクの状態で設定に追加されます。除外タイプがブランクのものについては、ドロップダウンメニューから手動で選択する必要があります。

**重要：**ワイルドカードを使用して複数の除外対象を追加できます。

保存すると、確認のために除外設定が表示されます。表示されたら、[編集（Edit）] をクリックして設定をさらに変更し、[変更の表示（View Changes）] をクリックして除外設定に対する変更を確認したり、[削除（Delete）] をクリックして設定を削除したりできます。クリックして、除外設定に割り当てられている任意のグループまたはポリシーに移動することもできます。

## 除外タイプ

脅威名、ファイルへのパス、ファイル拡張子、プロセス、または実行可能ファイル名に基づいて除外項目を作成できます。ワイルドカード除外は、除外対象にワイルドカード文字を含めることが可能な、パスまたはファイル拡張子による除外です。

### 脅威除外

**脅威**除外を使用すると、検疫対象から特定の脅威名を除外できます。脅威除外は、指定するイベントが誤検出の結果であることが確かである場合にみ使用してください。使用する場合は、イベントの正確な脅威名を指定してください。このタイプの除外を使用すると、指定した脅威名の検出が真陽性の場合でも、検出および隔離されなくなり、イベントも生成されません。

### パス除外

通常、アプリケーションの競合にはディレクトリの除外を伴うため、**パス**除外が最も頻繁に使用されます。除外パスは絶対パスまたは CSIDL を使用して指定できます。たとえば、プログラム ファイル ディレクトリ内でウイルス対策アプリケーションを除外する場合は、次のような除外パスを入力します。

```
C:\Program Files\MyAntivirusAppDirectory
```

**重要：**パス内の「スペース」文字をエスケープする必要はありません。英語以外の一部言語では、パスの区切り記号に異なる文字が使用されている場合があります。コネクタの除外設定で使用できる有効なパス区切り記号は「\」に限られます。

組織内にある一部のコンピュータの Program Files ディレクトリが別のドライブやパス上に存在する場合は、代わりに KNOWNFOLDERID を使用できます。前述の除外パスは次のようになります。

```
FOLDERID_ProgramFiles\MyAntivirusAppDirectory
```

**重要：**パス除外は、指定されたディレクトリ内のすべてのファイルとサブディレクトリを Cisco Secure Endpoint コネクタがスキャンするのを阻止します。

Windows 上でパスによる除外を追加する場合は、KNOWNFOLDERID（https://learn.microsoft.com/en-us/windows/win32/shell/knownfolderid）を使用することを強く推奨します。これらは、すべてのシステム上でパスが同じでない場合の Windows コンピュータ上の変数です。

**重要事項：**KNOWNFOLDERID は、Cisco Secure Endpoint Windows コネクタ 8.1.7 以降でサポートされています。8.1.7 より前のバージョンのコネクタでは CSIDL（http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx）の値が使用されます」バージョン 8.1.7 では CSIDL の除外が認識されますが、8.1.7 より前のバージョンのコネクタでは KNOWNFOLDERID の除外が認識されません。

**重要：**KNOWNFOLDERID の値では大文字と小文字が区別されます。たとえば、FolderID_programfiles ではなく FOLDERID_ProgramFiles を使用する必要があります。

## ファイル拡張子除外

拡張子除外を使用すれば、特定の拡張子が付いたファイルを除外できます。たとえば、次の除外を作成することによって、すべての Microsoft Access データベース ファイルを除外できます。

```
MDB
```

## ワイルドカード除外

ワイルドカード除外は、パス（CSIDL パスを含む）または拡張子でアスタリスク文字をワイルドカードとして使用できる点を除いて、パス除外や拡張子除外と同じです。たとえば、Mac 上の仮想マシンをスキャンから除外するには、次のパス除外を入力できます。

```
/Users/johndoe/Documents/Virtual Machines/
```

ただし、この除外は 1 人のユーザーに対してしか機能しないため、代わりにパス内のユーザー名をアスタリスクに置き換え、すべてのユーザーのこのディレクトリを除外するワイルドカード除外を作成します。

```
/Users/*/Documents/Virtual Machines/
```

Windows のワイルドカード除外については、[すべてのドライブ文字に適用（Apply to all drive letters）] も選択できます。これにより、マウントされているすべてのドライブに除外が適用されます。

## Windows プロセス除外

Cisco Secure Endpoint Windows コネクタのプロセス除外を使用すると、実行中のプロセスを通常のファイルスキャン（Cisco Secure Endpoint Windows コネクタのバージョン 5.1.1 以降）、システムプロセス保護、悪意のあるアクティビティからの保護、または動作保護から除外できます。

プロセスを除外するには、プロセスの実行ファイルへのフル パス、プロセスの実行ファイルの SHA-256 値、またはその両方を指定します。システムコンテキストフォルダには、直接パスを入力するか、KNOWNFOLDERID（https://learn.microsoft.com/en-us/windows/win32/shell/knownfolderid）の値を使用できます。プロセスの除外でパスと SHA-256 の両方を指定する場合、除外対象プロセスは両方の条件に適合する必要があります。

**重要事項：**KNOWNFOLDERID は、Cisco Secure Endpoint Windows コネクタ 8.1.7 以降でサポートされています。8.1.7 より前のバージョンのコネクタでは CSIDL（http://msdn.microsoft.com/en-us/library/windows/desktop/bb762494(v=vs.85).aspx）の値が使用されます。バージョン 8.1.7 では CSIDL の除外が認識されますが、8.1.7 より前のバージョンのコネクタでは KNOWNFOLDERID の除外が認識されません。

**重要事項：**使用するポリシーで設定されている [最大スキャンファイルサイズ（Maximum Scan File Size）] よりもプロセスのファイルサイズが大きい場合、プロセスの SHA-256 は計算されず、除外は機能しません。スキャン ファイルの最大サイズを超えるファイルには、プロセス除外でパスを指定します。

コネクタバージョン 7.5.3 以降では、プロセス実行パスに関してワイルドカード除外を指定してプロセスを除外できます。ワイルドカードを使用して、1 つのディレクトリに含まれる任意の数の文字を表すことができます。必要な除外対象を指定するために必要な最小限の文字数に対応するワイルドカードのみを使用してください。ワイルドカードをディレクトリ内の文字と一緒に使用して、除外をさらに絞り込むこともできます。

二重ワイルドカードを使用して、パス内のサブフォルダを除外することもできます。これは、プロセス除外の最後にのみ使用できます。

次のワイルドカードがサポートされています。

- パス内の * 文字は、その次に指定された文字にのみ一致します。
- パスの最後にある * 文字は、その次に指定された文字に一致しますが、サブディレクトリでは一致しません。
- パスの最後にある ** は、すべてのサブディレクトリに一致します。パスの途中で ** を使用することはできません。

除外されたプロセスによって作成された子プロセスは、デフォルトでは除外されません。たとえば、MS Word のプロセス除外を作成した場合、デフォルトでは、Word によって作成された追加のプロセスはすべて引き続きスキャンされ、このアプリケーションのネットワークトラフィックとともにデバイストラジェクトリに表示されます。これは、トラジェクトリで毎回 MS Word の起動を表示する必要はないが、悪意のある Word ドキュメントによってコマンド シェルなどの別のアプリケーションが起動されていないことを確認する場合に便利です。ただし、子プロセスをスキャンしたり、子プロセスのネットワークトラフィックとともにデバイストラジェクトリに表示したりしない場合は、[子プロセスに適用（Apply for child processes）] チェックボックスをオンにできます。

## エクスプロイト防止の実行ファイルの除外

実行ファイルの除外は、エクスプロイト防止が有効になっているコネクタにのみ適用されます。実行ファイルの除外を使用すると、エクスプロイト防止による保護から特定の実行ファイルを除外できます。より優れたセキュリティ態勢を維持するため、実行ファイルをエクスプロイト防止から除外するのは、問題やパフォーマンスの低下が発生した場合のみとしてください。

保護されたプロセスのリストを確認し、アプリケーション除外フィールドに実行ファイルの名前を指定することによって保護から除外できます。実行ファイルの除外は、`name.exe` の形式の実行ファイル名と正確に一致する必要があります。ワイルドカードは使用できません。

**重要：**エクスプロイト防止から除外した実行ファイルは、除外がコネクタに適用された後に再起動する必要があります。

## IOC の除外

IOC の除外では、クラウド侵害の兆候を除外できます。これは、署名されていない可能性のあるカスタムアプリケーションまたは内部アプリケーションがあり、特定の IOC が頻繁にトリガーされる場合に役立ちます。

除外タイプのプルダウンから IOC を選択し、除外する IOC の名前を選択します。部分的な文字列でもリストを検索できます。

**重要：**重大度が高い IOC を除外すると可視性が失われるため、組織がリスクにさらされる可能性があります。これらの IOC は、誤検出が多数発生した場合にのみ除外するようにしてください。

## Linux および Mac プロセス除外

Cisco Secure Endpoint Linux および Cisco Secure Endpoint Mac コネクタのプロセス除外を使用すると、通常のファイルスキャンと動作保護（Cisco Secure Endpoint Linux コネクタ 1.22.0 以降）から実行中のプロセスを除外できます。

実行可能なプロセスへの完全な（絶対）パスとプロセスのユーザー名を指定することにより、プロセスを除外できます。プロセスの除外でパスとユーザーの両方を指定する場合、除外対象プロセスは両方の条件に適合する必要があります。ユーザーフィールドを空白のままにすると、除外は指定したプログラムを実行しているすべてのプロセスに適用されます。

コネクタバージョン 1.15.2 以降では、プロセス実行パスに関してワイルドカード除外を指定してプロセスを除外できます。ワイルドカードを使用して、1 つのディレクトリに含まれる任意の数の文字を表すことができます。たとえば、すべてのバージョンの Java をスキャンから除外するには、次のパス除外を入力します。

```
/Library/Java/JavaVirtualMachines/*/Contents/Home/bin/java
```

必要な除外対象を指定するために必要な最小限の文字数に対応するワイルドカードのみを使用してください。ワイルドカードをディレクトリ内の文字と一緒に使用して、除外をさらに絞り込むこともできます。たとえば、特定のバージョンの Java のみをスキャンから除外するには、次のパス除外を入力します。

```
/Library/Java/JavaVirtualMachines/jdk1.7.*.jdk/Contents/Home/bin/java
```

除外されたプロセスによって作成された子プロセスは、デフォルトでは除外されません。たとえば、Java のプロセス除外を作成した場合、デフォルトでは、Java によって作成された追加のプロセスはすべて引き続きスキャンされ、このプロセスで生成されたネットワークトラフィックとともにデバイストラジェクトリに表示されます。これは、トラジェクトリで毎回 Java の起動を表示する必要はないものの、悪意のある Java アプリケーションによってシェルなどの別のアプリケーションが起動されていないかどうか確認する場合に便利です。ただし、子プロセスをスキャンしたり、子プロセスのネットワークトラフィックとともにデバイストラジェクトリに表示したりしない場合は、[子プロセスに適用（Apply for child processes）] チェックボックスをオンにできます。

詳細については、「macOS および Linux でのプロセス除外」を参照してください。

## シスコで維持している除外設定

シスコで維持している除外設定は、シスコにより作成および維持されており、Cisco Secure Endpoint コネクタとウイルス対策、セキュリティ、または他のソフトウェアとの互換性が向上します。除外設定のリストを表示するには、[シスコで維持している除外設定（Cisco-Maintained Exclusions）] ボタンをクリックします。これらの除外設定は削除も変更もできず、アプリケーションごとに除外されているファイルとディレクトリを確認するために提示されています。これらの除外設定は、時間の経過に伴い改善されて更新される可能性もあり、新しいバージョンのアプリケーションに対して新しい除外設定が追加される可能性もあります。いずれかの除外設定が更新されると、その除外設定を使用しているすべてのポリシーも更新され、新しい除外設定がコネクタにプッシュされます。

各行には、オペレーティングシステム、除外設定名、除外対象数、除外設定を使用するグループの数、除外設定を使用するコンピュータの数が表示されます。検索バーを使用して、名前、パス、拡張子、脅威名、または SHA-256 で除外セットを検索できます。それぞれのタブをクリックして、オペレーティングシステム別にリストをフィルタ処理することもできます。

## 除外を使用したウイルス対策の互換性

コネクタとウイルス対策またはその他のセキュリティソフトウェア間での競合を避けるには、コネクタがウイルス対策ソフトウェアのディレクトリをスキャンせず、かつウイルス対策ソフトウェアがコネクタのディレクトリをスキャンしないように除外項目を作

成する必要があります。悪意のあるファイル、または検疫済みのファイルに伴う問題であるとコネクタで判断された文字列がウイルス対策署名に含まれている場合、問題になる可能性があります。適切なシスコで維持している除外設定をポリシー に追加するか、独自のカスタム除外設定を作成できます。

除外設定の作成の詳細については、「Secure Endpoint の除外対象のベストプラクティス」を参照してください。

## ウイルス対策ソフトウェア向けの除外設定

コネクタでウイルス対策製品の除外を作成する以外にも、エンドポイントで実行されるウイルス対策製品でコネクタの除外を作成する必要があります。ファイル、ディレクトリ、およびプロセスをスキャン対象から除外する手順については、アンチウイルスソフトウェアのドキュメントを参照してください。

各種ウイルス対策ソフトウェアでコネクタの除外を作成する方法の詳細については、Cisco Secure Endpoint の「トラブルシューティング テクニカルノーツ」を参照してください。

### Secure Endpoint Windows コネクタ

ウイルス対策製品で、以下のディレクトリと、その中に含まれるファイル、ディレクトリ、および実行可能ファイルを除外する必要があります。

- C:\Program Files\Cisco\AMP\

**重要：**これはデフォルトのインストールディレクトリです。カスタム インストール ディレクトリを指定した場合は、そのディレクトリを除外する必要があります。

除外対象の実行可能ファイルへのフルパスを必要とするウイルス対策製品の場合は、C:\Program Files\Cisco\AMP\[connector version]\ ディレクトリ内のすべてのバイナリファイルを除外する必要があります。

次に例を示します。

- C:\Program Files\Cisco\AMP\[connector version]\ConnectivityTool.exe
- C:\Program Files\Cisco\AMP\[connector version]\creport.exe
- C:\Program Files\Cisco\AMP\[connector version]\ipsupporttool.exe
- C:\Program Files\Cisco\AMP\[connector version]\iptray.exe
- C:\Program Files\Cisco\AMP\[connector version]\sfc.exe
- C:\Program Files\Cisco\AMP\[connector version]\uninstall.exe
- C:\Program Files\Cisco\AMP\[connector version]\updater.exe
- C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclam.exe

- C:\Program Files\Cisco\AMP\clamav\[clam version]\freshclamwrap.exe

ここで、[connector version] には最近インストールしたコネクタのバージョン番号を入力し、[clam version] には ClamAV エンジンの最新バージョンを指定します。

また、次のコネクタ UI ログファイルを除外する必要が生じる場合もあります。

- C:\ProgramData\Cisco\AMP\IPTray.log

## Secure Endpoint Mac コネクタ

Secure Endpoint Mac コネクタとの互換性を確保するため、ウイルス対策製品で以下のディレクトリとその中に含まれるファイル、ディレクトリ、および実行可能ファイルを除外する必要があります。

- /Library/Application Support/Cisco/AMP for Endpoints Connector
- /opt/cisco/amp

## Secure Endpoint Linux コネクタ

Secure Endpoint Linux コネクタとの互換性を確保するため、ウイルス対策製品で以下のディレクトリとその中に含まれるファイル、ディレクトリ、および実行可能ファイルを除外する必要があります。

- /opt/cisco/amp

ウイルス対策製品に実行可能ファイルへのフルパスが必要な場合は、次を含む /opt/cisco/amp/bin/ 内のすべてのバイナリファイルを除外する必要があります。

- /opt/cisco/amp/bin/ampdaemon
- /opt/cisco/amp/bin/ampupdater
- /opt/cisco/amp/bin/ampscansvc（バージョン 1.9.0 以降）
- /opt/cisco/amp/bin/ampcli
- /opt/cisco/amp/bin/ampmon
- /opt/cisco/amp/bin/ampsupport
- /opt/cisco/amp/bin/ampsigncheck

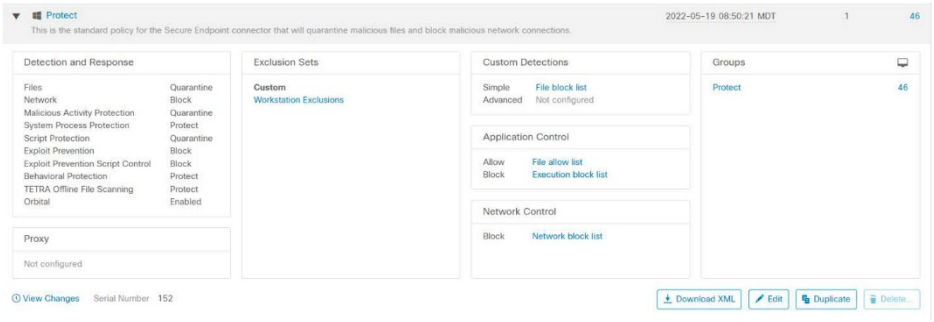
# 第 5 章

# ポリシー

アウトブレイクコントロールと除外のセットを他の設定と組み合わせてポリシーを作成します。このポリシーは、コネクタの動作と特定の設定に影響を与えます。ポリシーは、グループを介してコンピュータに適用されます。

## ポリシーの概要

ポリシー名の横にある矢印をクリックして設定の展開ビューと折りたたみビューを切り替えます。または、リストの右上にある [すべて展開（Expand All）] ボタンと [すべて縮小（Collapse All）] ボタン を使用すると、そのページのすべてのポリシーについて同じように展開ビューと折りたたみビューを切り替えることができます。



[表示の変更（View Changes）] を使用すると、監査ログのフィルタ処理されたビューが表示され、特定のポリシーに対するすべての変更が表示されます。また、ページの上部にある [すべての変更を表示（View All Changes）] を使用すると、すべてのポリシーに対する変更を表示できます。

既存のポリシーを変更するには [編集（Edit）] またはポリシー名をクリックします。また、同じ設定を使用して新しいポリシーを作成する場合は、[重複（Duplicate）] をクリックします。

[XMLのダウンロード（Download XML）] ボタンを使用して、コネクタに関する特定のポリシーを含む XML ファイルをダウンロードできます。コネクタインストーラには、デフォルトでポリシーが含まれているため、特定のトラブルシューティング シナリオではそのポリシーだけを使用する必要があります。

**重要：**重複した除外は、ダウンロードした XML ファイルから削除されます。

新しいポリシーを作成するには、[新しいポリシー...（New Policy...）] をクリックします。次に、以下に対するポリシーを作成するかどうかを選択します。

- Cisco Secure Endpoint Windows
- Cisco Secure Endpoint Android
- Cisco Secure Endpoint Mac
- Cisco Secure Endpoint Linux
- Secure Endpoint iOS

# Cisco Secure Endpoint Windows コネクタのポリシー

ここでは、Cisco Secure Endpoint Windows コネクタに使用可能なポリシーのオプションについて説明します。

## Windows コネクタ：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しいポリシーを保存する前に完了させる必要がある一連の設定ページの最初のページが表示されます。設定を入力して [次へ（Next）] をクリックし、ページを進めます。これらのページの設定については以下で説明します。

**重要：**これらのページで設定を完了するまでは、新しいポリシーの [アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] ページにはアクセスできません。

## 名前（Name）と説明（Description）

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

## モードとエンジン

このページには、判定モードと検出エンジンに関する設定が含まれています。各エンジンの詳細については、「Windows コネクタサポートツール」を参照してください。[ワークステーション設定の適用（Apply Workstation Settings）] または [サーバー設定の適用（Apply Server Settings）] をクリックすると、ポリシー内のすべての判定モードをワークステーションやサーバーの推奨設定にすばやく設定できます。

### 判定モード

判定モードでは、疑わしいファイル、ネットワークアクティビティ、プロセスに対するコネクタの対応方法を指定します。ファイルを [監査（Audit ）] に設定すると、Cisco Secure Endpoint コネクタによるファイルの検疫が停止します。この設定は、Cisco Secure Endpoint コネクタのバージョン 3.1.0 以降にのみ適用されます。

**重要事項：**[ファイル判定モード（File Conviction Mode）] が [監査（Audit）] に設定されている場合は、エンドポイント上の悪意のあるファイルがアクセス可能なままになり、実行が許可されます。アプリケーション ブロッキング リストも適用されません。この設定は、独自のソフトウェアを使用したテストにのみ使用してください。

Malicious Activity Protection（MAP） エンジンは、プロセスの実行時に悪意のあるアクションを特定することで、エンドポイントをランサムウェア攻撃から保護し、データの暗号化を防ぎます。[監査（Audit）] モードの場合、イベントがログに記録されますが、検出されたプロセスに関する処理は行われません。[検疫（Quarantine）] モードでは、検出されたプロセスが検疫されます。[ブロック（Block）] モードの場合、プロセスの実行が停止されます。エンジンを [ネットワークドライブのモニター（Monitor Network Drives）] に設定することもできます。

システムプロセス保護は、他のプロセスによるメモリインジェクション攻撃によって重要な Windows システムプロセスが侵害されるのを防ぎます。[保護（Protect）] モードの場合、重要な Windows システムプロセスに対する攻撃がブロックされます。

[検疫（Quarantine）] モードの場合、スクリプト保護は、悪意のあるスクリプトファイルの実行をブロックします。[監査（Audit）] モードでは、悪意のあるスクリプトが実行されたときにイベントが作成されますが、スクリプトの実行はブロックされません。

エクスプロイト防止エンジンは、未修正ソフトウェアの脆弱性をターゲットとするマルウェアやゼロデイ攻撃で一般的に使用されるメモリインジェクション攻撃からエンドポイントを保護します。[監査（Audit）] モードは、コネクタのバージョン 7.3.1 以降で使用できます。7.3.1 より前のバージョンのコネクタでは、[監査（Audit）] モードは [ブロック（Block）] モードと同様に扱われます。

**重要事項：**[エクスプロイトの防止（Exploit Prevention）] を無効にした場合は、保護されたプロセスのいずれかを再起動する必要があります。保護されたプロセスのリストについては、「保護されたプロセス」を参照してください。

スクリプト制御は、特定の DLL が一部のアプリケーションやその子プロセスによってロードされるのを防ぎます。[ブロック（Block）] モードでは、プロセスまたはその子プロセスのいずれかが特定の DLL をロードしようとすると、エンジンによってプロセスが強制終了されます。[監査（Audit）] モードでは、アクティビティが検出されたときにイベントが作成されますが、プロセスは強制終了されません。

動作保護は、[保護（Protect）] モードにおいて悪意のあるアクティビティに関するアラートを表示、ファイルを検疫、およびプロセスを終了することで、一連の動作署名と一致する悪意のあるアクティビティを阻止します。[監査（Audit）] モードでは、一致するアクティビティが検出されたときにイベントが作成されますが、アクションは実行されません。

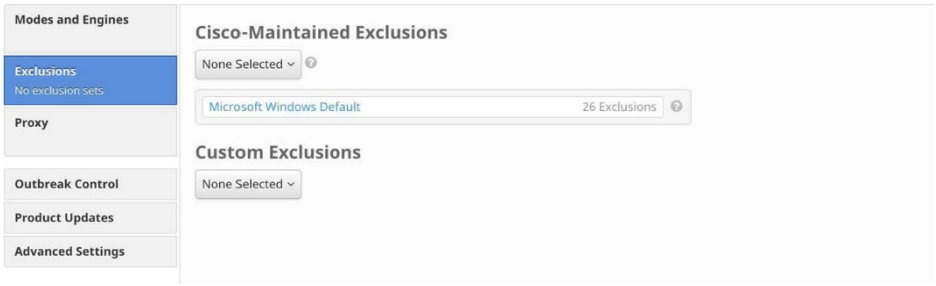
### 検出エンジン

追加の検出エンジンを有効にすると、Cisco Cloud に接続して各ファイルにクエリを実行することなく、マルウェアからエンドポイントを保護できます。

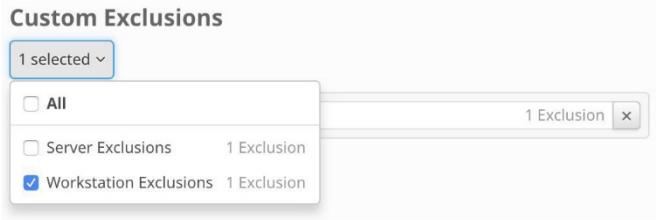
TETRA は、ウイルス対策製品に全面的に代わるものであり、別のウイルス対策エンジンがインストールされている場合は絶対に有効にしないでください。また、TETRA は、定義更新をダウンロードするときに大量の帯域幅を消費する可能性があるため、大規模環境で有効にする場合は注意が必要です。[詳細設定（Advanced Settings）] > [TETRA] では、TETRA の他の設定を使用できます。

## 除外事項

ここで、除外設定を選択してポリシーに適用できます。すべての新しい Windows ポリシーには、Windows オペレーティングシステムの特定のコンポーネントに関するシスコで維持されている除外設定が含まれています。この一連の除外設定は削除できません。ポリシーグループに存在するアプリケーションに応じて、ポリシーに追加するその他のシスコで維持している除外設定を選択し、ユーザーのカスタム除外設定をポリシーに追加できます。

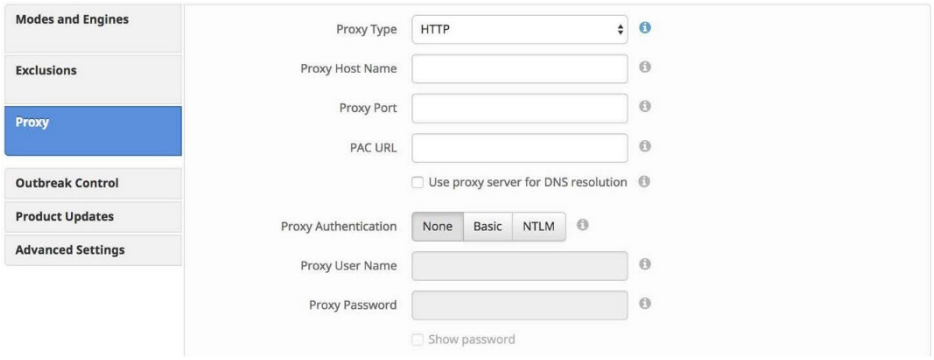


シスコで維持されている除外設定またはカスタム除外設定のいずれかのドロップダウンメニューをクリックし、チェックボックスをオンにして除外設定を選択します。詳細については、「除外事項」を参照してください。




## プロキシ

このページでプロキシ設定を実行します。




[プロキシタイプ（Proxy Type）] は、接続しているプロキシのタイプです。コネクタは、**http_proxy**、**socks4**、**socks4a**、**socks5**、および **socks5_hostname** をサポートします。

[プロキシホスト名（Proxy Host Name）] は、プロキシサーバーの名前または IP アドレスです。サポートされているのは IPv4 アドレスだけです。

[プロキシポート（Proxy Port）] は、プロキシサーバーで使用されるポートです。

[PAC URL] を使用すると、コネクタがプロキシ自動設定（PAC）ファイルを取得する場所を指定できます。

**重要：**URL はポリシー経由で定義した場合に HTTP または HTTPS を指定する必要があり、.pac 拡張子付きの ECMAScript ベースの PAC ファイルだけがサポートされます。PAC ファイルが Web サーバー上でホストされている場合は、適切な MIME タイプ（application/x-javascript-config）を指定する必要があります。

[DNS解決にプロキシサーバーを使用（Use Proxy Server for DNS Resolution）] を使用すると（Windows のみ）、すべてのコネクタ DNS クエリをプロキシサーバー上で実行するかどうかを指定できます。

[プロキシ認証（Proxy Authentication）] は、プロキシサーバーで使用される認証のタイプです。**基本**認証と **NTLM** 認証がサポートされています。

[プロキシユーザー名（Proxy User Name）] は、認証されたプロキシに使用されます。これは、接続時に使用するユーザー名です。

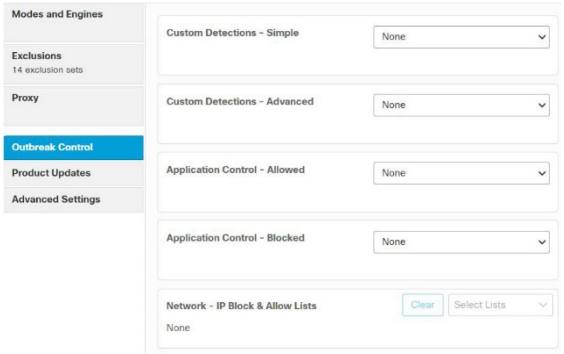
**重要：**プロキシ認証タイプとして NTLM を選択した場合は、このフィールドを domain\username の形式にする必要があります。

[プロキシパスワード（Proxy Password）] は、認証されたプロキシに使用されます。これは、プロキシ ユーザー名と一緒に使用するパスワードです。

## Windows コネクタ：その他のポリシー設定

必須の設定ページへの入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] にアクセスできるようになります。以降の項で設定について説明します。

### アウトブレイク コントロール

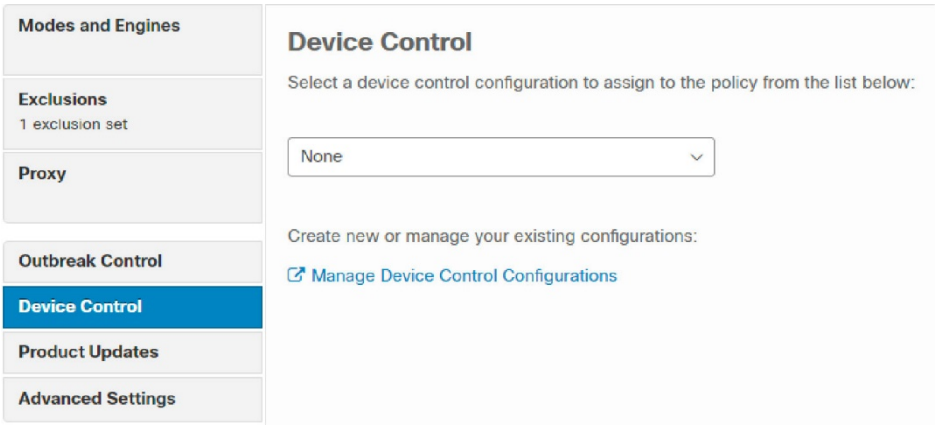



このページでは、ポリシーに割り当てるリストを選択します。各リストの作成の詳細については、「カスタム検出：簡易」、「カスタム検出：高度」、「アプリケーション制御：許可されたアプリケーション」、「アプリケーション制御：ブロックされたアプリケーション」、および「ネットワーク：IP ブロック/許可リスト」を参照してください。すべてのコネクタですべてのリストタイプがサポートされているわけではありません。

**重要事項：**ネットワーク：IPブロック/許可リストは、[詳細設定（Advanced Settings）] の [ネットワーク（Network）] タブで [デバイスフローコリレーション（Device Flow Correlation）] が有効になっている場合にのみ機能します。

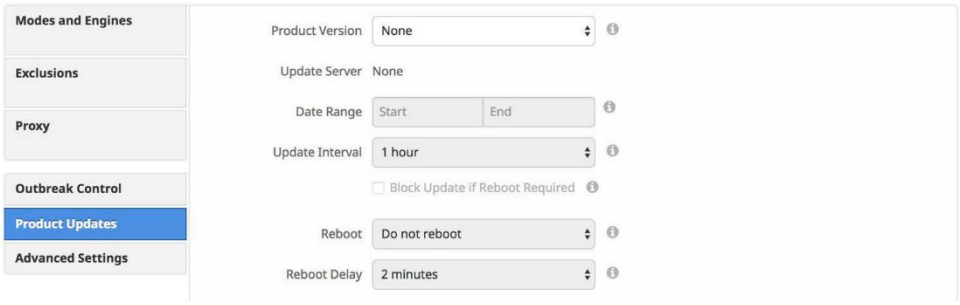
使用可能な IP 許可リストまたはブロックリストがある場合は、[リストの選択（Select Lists）] をクリックするとポリシーに追加するリストを選択できます。ドロップダウンメニューで、追加するすべてのリストのチェックボックスをオンにします。単一のポリシーに複数の IP リストを追加できますが、IP 許可リストエントリが IP ブロックリストエントリをオーバーライドします。

## Windows コネクタ：デバイス制御




ポリシーに任意のデバイス制御設定を追加します。プルダウンから設定を選択して追加します。ポリシーごとに 1 つの設定のみを追加できます。

## Windows コネクタ：製品の更新




製品の更新が利用可能な場合は、ポリシー単位でエンドポイントの更新の有無を選択できます。表示するバージョンを示すエントリが [製品バージョン（Product Version）] ドロップダウンメニューに表示されます。そのエントリが [更新サーバー（Update Server）] に読み込まれるため、ファイルの抽出元を確認できます。また、そのポリシーを使用するグループ内にあり、更新後に再起動が必要なコネクタの数を示す情報も表示されます。Orbital を有効にしており、[スケジュールの更新（Update Schedule）] で [コネクタ搭載（With Connector）] を選択している場合にのみ、Orbital の更新オプションが表示されます。

次に、[日付範囲（Date Range）] を選択することで、更新の実行が許可される時間枠を定義できます。[日付範囲（Date Range）] で、[開始（Start）] をクリックして、開始時間帯の日付と時刻を選択し、[終了（End）] をクリックして終了時間帯の日付と時刻を選択します。また、[今月（This Month）] を選択して現在の日から現在の月の月末までの日付範囲を設定するか、[今後 7 日間（Next 7 Days）] を選択して範囲を今後 7 日間に設定するか、[今後 30 日間（Next 30 Days）] を選択して範囲を今後 30 日間に設定することもできます。[更新間隔（Update Interval）] を使用すると、コネクタが新製品の更新（Orbital の更新を含む）をチェックする間隔を指定できます。これは、ネットワーク トラフィックを削減するために 30 分 ~ 24 時間の間に設定する必要があります。

[日付範囲（Date Range）] に設定された時刻の間にコネクタがホームをコールしてポリシーを取得した場合、製品の更新が取得されます。コネクタはハートビート間隔に応じた間隔でホームをコールするため、更新期間をこの間隔に従って計画することをお勧めします。そうすることで、更新期間で指定された間隔を、ハートビート間隔より長くできます。

Cisco Secure Endpoint Windows コネクタのバージョン 4.3 以降に更新する場合は、別の再起動オプションが表示されます。バージョン 4.3 の時点では、一部の更新はリブートして反映させる必要がないものもあります。

更新後に再起動が必要な場合は、[再起動が必要な場合は更新をブロック（Block Update if Reboot Required）] をオンにして、コネクタの更新を阻止します。これは、サーバーや高可用性コンピュータでリブートが必要な場合に更新を手動で実行した方がよい場合に便利です。必要に応じて、多少のダウンタイムが許容される期間に新しい更新期間を設定できます。特定の更新のリブート要件については、この記事を参照してください。

**重要事項：**Cisco Secure Endpoint Windows コネクタ 7.x.x 以降では、7.x.x から任意の新しいバージョンへのコネクタのアップグレードを完了するための再起動は必要ありません。ほとんどのアップグレードでは再起動は必要ありませんが、再起動が必要な場合もあります。再起動が必要な状況のリストについては、『Secure Endpoint Windows Connector Update Reboot Requirements』を参照してください。

[再起動（Reboot）] には、[再起動しない（Do not reboot）]、ユーザーから [再起動を要求する（Ask for reboot）]、または [後で再起動を強制する...（Force reboot after...）]（[再起動の遅延（Reboot Delay）] を選択可能）などのオプションが表示されます。

**重要事項：**更新に「再起動が必要（Reboot required）」と表示されている場合、コンピュータが再起動されるまでコネクタサービスは停止します。このような更新の後にコンピュータが脆弱にならないようにするには、[再起動が必要な場合は更新をブロック（Block Update if Reboot Required）] をオンにします。
更新に「再起動を推奨（Reboot suggested）」と表示されている場合、コネクタサービスは更新後も引き続き実行されますが、更新の新機能はコンピュータが再起動されるまで使用できません。

Windows 8 以降では、[高速スタートアップ（Fast Startup）] モードまたはハイバネーションが有効になっている場合は、Windows のシャットダウンオプションを使用せずに、更新の完了後にコンピュータを再起動する必要があります。再起動することで、コネクタのドライバを更新する最終手順を適切に完了できます。

## Windows コネクタ：詳細設定

### 管理機能

[イベント内のユーザー名を送信（Send User Name in Events）] では、プロセスを実行、コピー、または移動した実際のユーザー名（既知の場合）が送信されます。これは、マルウェアを観察している人物を追跡するのに役立ちます。この機能が有効になっていない場合は、ユーザーとして実行、コピー、または移動したマルウェアには「u」が、管理者として実行、コピー、または移動したマルウェアには「a」が表示されます。

[ファイル名とパス情報を送信（Send Filename and Path Info）] では、ファイル名とパス情報が Cisco Secure Endpoint に送信されるため、[イベント（Events）] タブ、[デバイストラジェクト（Device Trajectory）]、および [ファイルトラジェクトリ（File Trajectory）] で確認できます。この設定をオフにすると、この情報の送信が停止されます。

[ハートビート間隔（Heartbeat Interval）] は、コネクタがホームをコールして、レトロスペクティブ機能または管理者によって復元するファイル、取得するポリシー、実行するタスク（製品の更新やスキャンなど）の有無を確認するための間隔です。

[コネクタログレベル（Connector Log Level）] と [トレイログレベル（Tray Log Level）] を使用すると、デフォルトのログレベルとデバッグ（詳細）ログレベルを選択できます。デフォルト レベルは、トラブルシューティング中にサポートからデバッグが要求されないかぎり、設定しておく必要があります。

**警告：**[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合、ログファイルでさらに 550MB のドライブ容量が使用される可能性があります。

[コネクタ保護の有効化（Enable Connector Protection）] を使用すると、コネクタをアンインストールしたり、サービスを停止したりする場合にパスワードを要求できます。

**重要：**展開済みのコネクタを含むポリシーで [コネクタ保護（Connector Protection）] を有効にした場合は、コンピュータを再起動するか、コネクタサービスを停止してから再起動して、設定を有効にする必要があります。

[コネクタ保護パスワード（Connector Protection Password）] は、コネクタサービスを停止またはアンインストールするために [コネクタ保護（Connector Protection）] に指定するパスワードです。

**重要：**パスワードに特殊文字を含める場合は、エンドポイントのコマンドプロンプトまたは PowerShell でパスワードを入力するときに、その文字をエスケープする必要があります。

[クラッシュダンプの自動アップロード（Automated Crash Dump Uploads）] を選択すると、分析のためにコネクタのクラッシュダンプファイルをシスコに自動的にアップロードするかどうかを選択できます。

[コマンドラインキャプチャ（Command Line Capture）]（Cisco Secure Endpoint Windows コネクタ 5.0 以降）を選択すると、ファイルの実行中に使用するコマンドライン引数（ユーザー名、ファイル名、パスワードなど）をコネクタがキャプチャして、情報が Cisco Secure Endpoint に送信されます。この情報は、管理者がシングルサインオン（Security Cloud Sign-On など）を使用しているか、二要素認証が有効になっている限り、デバイストラジェクトリに表示されます。

**重要事項：**[コマンドラインのキャプチャ（Command Line Capture）] により、非常に長いコマンドライン引数が切り捨てられる場合があります。問題がある場合は、サポートにお問い合わせください。

[コマンドラインキャプチャ（Command Line Capture）] が有効になっており、[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合は、エンドポイントで [コマンドラインロギング（Command Line Logging）] を使用して、キャプチャされたコマンドライン引数をローカルのコネクタログファイルに記録できます。

## クライアント ユーザー インターフェイス

[クライアント ユーザー インターフェイスを開始（Start Client User Interface）] を使用すると、コネクタ ユーザー インターフェイスを完全に非表示にするかどうかを指定できます。このオプションをオフにすると、コネクタはサービスとして実行されますが、ユーザー インターフェイス コンポーネントは実行されません。

**重要：**この設定を変更した場合、コネクタを再起動するまで、変更は有効になりません。

[クラウド通知（Cloud Notifications）] は、コネクタがクラウドとの接続に成功したときに Windows システムトレイに表示されるバルーンポップアップです。この通知には、クラウドに登録されたユーザー数と検出数が表示されます。

[エンジン通知（Engine Notifications）] には、さまざまなコネクタエンジンによって生成された通知が表示されます。次のようなものがあります。

- クラウドルックアップ
- TETRA
- 悪意のあるアクティビティからの保護

- システム プロセス保護
- エクスプロイトの防止
- デバイス フロー相関
- エンドポイント IOC のカタログ化

[除外事項を非表示にする（Hide Exclusions）] を選択すると、設定された除外事項がコネクタ ユーザー インターフェイスに表示されません（Cisco Secure Endpoint Windows コネクタのバージョン 5.1.3 以降で使用可能）。

[TETRA定義の更新をユーザーに許可（Allow User to Update TETRA Definitions）] を選択すると、TETRA 定義をオンデマンドで更新するためのボタンが Cisco Secure Endpoint Windows コネクタ UI 上で有効になります（Cisco Secure Endpoint Windows コネクタのバージョン 7.2.11 以降で使用可能）。

## ファイルとプロセスのスキャン

[ファイルのコピーおよび移動時のモニタリング（Monitor File Copies and Moves）] は、コピーまたは移動されたファイルにコネクタがリアルタイム保護を提供するための機能です。

[プロセス実行のモニタリング（Monitor Process Execution）] は、実行されたファイルにコネクタがリアルタイム保護を提供するための機能です。

[詳細な履歴（Verbose History）]（Windows 5.1.9 以降のみ）は、Cisco Secure Endpoint Windows コネクタによる history.db ファイルへ詳細な履歴情報の書き込みを制御します。

[オンエグゼキュートモード（On Execute Mode）] は、2 種類のモード（[アクティブ（Active）] と [パッシブ（Passive）]）で実行できます。[アクティブ（Active）] モードでは、ファイルおよびスクリプトに悪意があるかどうかが判断されるまで、またはタイムアウトになるまで、それらの実行がブロックされます。[パッシブ（Passive）] モードでは、ファイルおよびスクリプトは実行を許可されると同時に、検査され、悪意があるかどうかが判断されます。

**警告：**アクティブ モードはより優れた保護を提供しますが、パフォーマンスの問題を引き起こす可能性があります。エンドポイントにすでにウイルス対策製品がインストールされている場合は、これを [パッシブ（Passive）] のままにすることをお勧めします。

[最大スキャンファイルサイズ（Maximum Scan File Size）] では、コネクタによってスキャンされるファイルのサイズを制限します。しきい値設定より大きなファイルはスキャンされません。

[最大アーカイブ スキャン ファイル サイズ（Maximum Archive Scan File Size）] では、コネクタによってスキャンされるアーカイブファイルのサイズを制限します。しきい値設定より大きなアーカイブ ファイルはスキャンされません。

## キャッシュ

SHA-256 値は、クラウド検索トラフィックを削減するためにキャッシュされます。値がキャッシュされる時間は、その SHA-256 に対して最後のクラウド検索が実行されたファイルの分類によって異なります。ファイルがキャッシュされている間、コネクタは常に、その分類を最後にクラウド検索が実行されたときの分類と見なします。たとえば、SHA-256 がアプリケーション ブロッキング リストに含まれており、TTL が 3,600 秒の場合、管理者がそのアプリケーションをアプリケーション ブロッキング リストから削除しても、次の 1 時間はコネクタによってアプリケーションの実行がブロックされます。

[悪意のあるキャッシュTTL（Malicious Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に悪意のある分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[クリーンキャッシュTTL（Clean Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前にクリーンな分類のファイルがキャッシュされる時間です。デフォルト値は 1 週間です。

[不明なキャッシュTTL（Unknown Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に不明な分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[アプリケーションブロッキングTTL（Application Blocking TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に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リストにあるファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

**重要：**コネクタによって過去に観察されたアプリケーション ブロッキング リストに「クリーン（Clean）」分類の SHA-256 を追加する場合は、コネクタを停止して、アプリケーションの実行をブロックするコンピュータのインストールディレクトリから cache.db ファイルを削除する必要があります。削除しないと、アプリケーションの実行をブロックする前に、クリーンファイルの TTL 期限が切れ、別のクラウド検索がコネクタによって実行されるまで待機する必要があります。

## エンドポイントの隔離

エンドポイントの隔離を使用すると、Windows コンピュータでの着信および発信ネットワークアクティビティをブロックし、データ漏洩やマルウェアの拡散などの脅威を防ぐことができます。

[DNSの許可（Allow DNS）] により、エンドポイントが隔離されている間に DNS ルックアップを実行できます。エンドポイントのネットワーク設定で構成された DNS サーバーのアドレスは、コネクタによって許可リストに自動的に追加されます。この設定をオフにする場合は、DNS サーバーのアドレスを手動で許可リストに追加する必要があります。

[DHCPの許可（Allow DHCP）] により、エンドポイントが UDP ポート 67 および 68 でトラフィックを送受信できるようになるため、DHCP リースを取得または更新できます。静的 IP アドレスを使用する場合は、これを安全にオフにできます。この設定をオフにする場合は、DHCP サーバーのアドレスを手動で許可リストに追加する必要があります。

特定のプロキシを構成する必要がある上級ユーザーには、[プロキシでの使用を許可（Allow use with proxy）] が与えられます。この機能は、より汎用的なインターネットプロキシとは異なる内部通信や、セキュリティで保護された通信を管理するプロキシがある場合に便利です。ただし、バージョンが 7.5.1 より前のコネクタでは、プロキシを使用する場合、そのプロキシを介して Cisco Secure Endpoint Cloud インフラストラクチャでトラフィックを送受信できることを確認する必要があります。

**重要事項：**[プロキシでの使用を許可（Allow use with proxy）] がオンになっている隔離エンドポイントは、プロキシが IP 隔離許可リストに含まれている場合、プロキシを介してネットワークトラフィックを送受信できます。ほとんどの場合、これは隔離の影響を無効にし、エンドポイントは公開されたままになります。IP 隔離許可リストでプロキシが指定されていない場合、エンドポイントはバージョンが 7.5.1 より前のコネクタの Cisco Secure Endpoint Cloud とは通信できません。その場合は、エンドポイントのコマンドラインから Windows 隔離セッションを停止のみ可能です。コネクタバージョン 7.5.1 以降は、隔離時にプロキシの背後からシスコクラウドと通信する機能を保持しています。プロキシを有効にして隔離を展開する前に、慎重なネットワークテストを行う必要があります。

隔離セッション中にコネクタが使用する [IP許可リスト（IP Allow Lists）] を指定できます。[リストの選択（Select Lists）] プルダウンを使用して、このポリシーで使用する IP 隔離許可リストを指定します。

## Orbital

**重要：**Orbital は、Cisco Secure Endpoint Advantage または上位のパッケージを使用している場合に利用できます。

Orbital を使用すると、Orbital の展開場所に関係なくエンドポイントをクエリして詳細情報を取得できます。Orbital の使用の詳細については、Orbital のマニュアル（https://orbital.amp.cisco.com/help/）を参照してください。

ポリシーで Orbital を有効にするには、[Orbital Advanced Searchを有効にする（Enable Orbital Advanced Search）] チェックボックスをオンにして、[保存（Save）] をクリックします。

Orbital は、Windows 10 1709 以降および Windows Server 2012、2012 R2、2016 以降のバージョンで、以前にこの機能を有効にしていないすべてのコンピュータにインストールされます。インストールが正常に完了すると、コネクタから Cisco Secure Endpoint コンソールにイベントが送信されます。Orbital のインストール間隔は、

Windows コネクタ：製品の更新の [更新間隔（Update Interval）] の設定と同じです（デフォルト値：1 時間）。

[スケジュールの更新（Update Schedule）] では、新しいバージョンが利用可能になるたびに Orbital を自動的に更新するか、Windows コネクタ：製品の更新で更新をスケジュールするかを定義できます。

コネクタのバージョン 7.4.5 以降では、管理者権限を持つアカウントを使用し、コネクタのインストールディレクトリから次のコマンドを使用して Orbital を強制的に更新できます。

```
sfc.exe -forceOrbitalUpdate
```

このコマンドにより、失敗したキャッシュ済みバージョンがすべて削除され、現在のバージョンが再試行されます。

**重要：**Orbital は、エンドポイントが分離されている間は有効にできません。

**重要：**ポリシーに関して Orbital を無効にすると、サービスは無効になりますが、Orbital はエンドポイントからアンインストールされません。再度有効にすると、サービスが再起動されます。

## エンジン

[ネットワークドライブのモニター（Monitor Network Drives）] を使用すると、ネットワークドライブに影響を与えるローカルコンピュータからの悪意のあるアクティビティを検出するように Malicious Activity Protection エンジンを設定できます。この設定により、VPN を介してネットワークドライブをモニターするときに速度が低下する可能性があることに注意してください。VPN を介して定期的にネットワークドライブにアクセスするユーザーを、この設定を無効にしたポリシーを使用するグループに入れることを検討してください。この設定は、Cisco Secure Endpoint Windows コネクタのバージョン 6.3.1 以降にのみ適用されます。

**重要：**Malicious Activity Protection エンジンがネットワークドライブ上でアクティビティを検出した場合、ローカルプロセスをブロックして隔離することはできますが、ネットワークドライブからファイルを隔離することはできません。

[スクリプトの制御（Script Control）] により、スクリプト保護動作が設定されます。デフォルトでは、[スクリプトの制御（Script Control）] の設定は、[モードとエンジン（Modes and Engines）] タブの [エクスプロイト防止（Exploit Prevention）] と同じ設定に関連付けられます。ブロック、監査、および無効化の設定を使用して、[スクリプトの制御（Script Control）] の動作と [エクスプロイト防止（Exploit Prevention）] の動作を別にすることができます。

**重要：**この機能を使用するには、[エクスプロイト防止（Exploit Prevention）] を有効にする必要があります。これらの設定は、Cisco Secure Endpoint Windows コネクタ 7.3.5 以降にのみ適用されます。以前のバージョンでは、エクスプロイト防止と同じ設定が使用されます。

ETHOS と SPERO の両方が汎用エンジンと見なされています。そのため、ETHOS または SPERO ハッシュの誤検出傾向をユーザーが制御できます。

**ETHOS** は、シスコファイルグループ化エンジンです。これを使用すると、ファイルのファミリをまとめてグループ化できるため、マルウェアのバリアントが確認されたら、ETHOS ハッシュが悪意があるとしてマーキングされ、マルウェアのファミリ全体が即座に検出されます。

ETHOS はリソースを大量に消費する可能性があるため、バージョン 6.2.1 以降の Cisco Secure Endpoint Windows コネクタではスキャンするファイルは最大 5MB に制限されています。ETHOS で**オンコピー/オンムーブ**スキャンが実行されている場合、コネクタはコピーまたは移動が完了してから、ファイルの ETHOS を計算するために別のスレッドをキューに入れられるため、速度の低下を緩和できます。

[ETHOSハッシュあたりの検出しきい値（Detection Threshold per ETHOS Hash）] は、単一の ETHOS ハッシュが単一の SHA を不明な分類と判定できる最大回数を意味します。デフォルトは 10 です。これは ETHOS が 24 時間の間に 10 回確認した SHA-256 を、コミュニティ全体で有害と判断しないことを意味します。検出しきい値に到達しても、検出が誤検出とは考えられず、特定の SHA の判定を継続したい状況が発生した場合は、その SHA をカスタム検出：簡易またはカスタム検出：高度リストに追加する必要があります。

**SPERO** は、シスコのマシンベースの学習システムです。SPERO フィンガープリントと呼ぶ、何百ものファイルの特徴を利用します。これがクラウドに送信され、SPERO ツリーによってファイルに悪意があるかどうかが判断されます。

[SPEROツリーあたりの検出しきい値（Detection Threshold per SPERO Tree）] は、単一の SPERO ツリーが単一の SHA を不明な分類と判定できる最大回数を意味します。デフォルトは 10 です。これは SPERO が 24 時間の間に 10 回確認した SHA-256 を、コミュニティ全体で有害と判断しないことを意味します。検出しきい値に到達しても、検出が誤検出とは考えられず、特定の SHA の判定を継続したい状況が発生した場合は、その SHA をカスタム検出：簡易またはカスタム検出：高度リストに追加する必要があります。

[ステップアップの有効化（Step-Up Enabled）] は、「大量感染」と判断された場合に追加の SPERO ツリーをオンにするための機能です。これらの SPERO ツリーでは、誤検出傾向が強くなりますが、マルウェアの検出率は高くなります。「大量感染」の判断はステップアップしきい値に基づきます。

[ステップアップしきい値（Step-Up Threshold）] は、コネクタが「大量感染」しているかどうかの判断に使用されます。デフォルトは 5 で、SHA 一対一検出が 30 秒の間に 5 回発生すると、「大量感染」と見なされ、追加の SPERO ツリーが次の 30 秒間有効になること意味します。

動作保護が有効になっている場合、[Windowsのイベントトレースの有効化（Enable Event Tracing for Windows）] により、エンドポイントにおける悪意のあるアクティビティの検出が向上します。設定がアクティブになっている場合、Cisco Secure Endpoint Windows コネクタにより各エンドポイントの Windows 監査ポリシーに次の変更が加えられます。

- ユーザーアカウント管理成功の監査 - 有効
- ログオン成功の監査 - 有効
- ログオン失敗の監査 - 有効
- セキュリティシステム拡張成功の監査 - 有効
- その他のオブジェクト アクセス イベント成功の監査 - 有効

継続的なモニタリングを実現するために、コネクタによってこれらの設定がすべてのハートビート間隔に適用されます。

この設定は、Windows 10 または Windows Server 2019 以降で実行されている Cisco Secure Endpoint Windows コネクタ 7.3.5 以降にのみ適用されます。

**重要：**イベントトレースを無効にする場合は、各エンドポイントで Windows 監査ポリシーの設定をリセットする必要があります。

## TETRA

TETRA を使用すると、オフライン スキャンやルートキット スキャンなどの従来型ウイルス対策製品によるスキャンを実行できます。これは、シグニチャ ベースであり、ローカル コンピュータ上のディスク領域をより多く消費します。TETRA は、1 時間ごとに更新されたシグニチャをチェックして、新しいシグニチャが利用可能になるとダウンロードします。この主な欠点は他のウイルス対策製品との互換性であり、他のウイルス対策製品がコンピュータ上にインストールされている場合は絶対に有効にしないでください。このポリシー設定オプションは、このタブか、または [モードとエンジン（Modes and Engines）] タブで TETRA が選択されている場合にのみ使用できます。

[アーカイブのスキャン（Scan Archives）] では、コネクタが圧縮ファイルを開いて、ファイルの内容をスキャンするかどうかを決定します。デフォルトの制限は、50 MB を超える圧縮されたファイルはスキャンしないことです。

[圧縮ファイルのスキャン（Scan Packed）] では、コネクタが圧縮ファイルを開いて、ファイルの内容をスキャンするかどうかを決定します。

[ファイルのディープスキャン（Deep Scan Files）] では、コネクタが製品のインストールファイルおよび CHM ファイルの内容をスキャンするかどうかを決定します。

[拡張された脅威タイプの検出（Detect Expanded Threat Types）] は、悪意を持って使用されることがあるアーカイブ爆弾とアプリケーションを検出します。

[自動署名更新（Automatic Signature Updates）] を使用すると、コネクタがその TETRA 署名を自動的に更新できます。TETRA シグニチャ更新は、大量の帯域幅を消費する可能性があるため、大規模環境で自動シグニチャ更新を有効にする場合は注意が必要です。

[コンテンツの更新間隔（Content Update Interval）] では、署名などの新しい TETRA コンテンツがコネクタでチェックされる頻度を指定できます。更新間隔が長いほど、TETRA 更新によるネットワーク トラフィックが減少するのに対して、更新間隔が短いほど、大量の帯域幅が消費される可能性があり、大規模展開にはお勧めできません。[コンピュータの管理（Computer Management）] ページで、コンピュータの TETRA 定義のバージョンと更新ステータスを確認できます。

**ローカルの Cisco Secure Endpoint 更新サーバー** は、TETRA 定義を取得するためにコネクタの Cisco Secure Endpoint 更新サーバーを設定している場合にのみ有効にする必要があります。[Cisco Secure Endpoint更新サーバーの設定（Secure Endpoint Update Server Configuration）] リンクをクリックして、サーバーをダウンロードします。Cisco Secure Endpoint 更新サーバーの場合、Cisco Cloud からコンテンツを初めてダウンロードする際に 1 時間以上かかることがあります。

**重要：** Cisco Secure Endpoint Windows コネクタ 5.1.13 以降でのみローカルの Cisco Secure Endpoint 更新サーバーを使用できます。

**Cisco Secure Endpoint 更新サーバー**の設定では、ローカルの Cisco Secure Endpoint 更新サーバーのホスト名または IP アドレスを指定する必要があります。このフィールドには、HTTP:// または HTTPS:// を含めないでください。

[TETRA定義の更新にHTTPSを使用する（Use HTTPS for TETRA Definition Updates）] にはローカルの Cisco Secure Endpoint 更新サーバーが必要です。自己ホストモードで動作している Cisco Secure Endpoint 更新サーバーは、ポート 80 で HTTP プロトコルのみサポートできます。HTTPS プロトコルが必要な場合には、Apache、Nginx などの HTTPS が有効な Web サーバーを、有効な SSL 証明書とともに使用する必要があります。

## ネットワーク

[ネットワーク（Network）] タブには、デバイス フロー コリレーション設定など、コネクタのネットワークフロー機能に関する設定が含まれています。

[デバイスフローコリレーションの有効化（Enable Device Flow Correlation）] を使用すると、ネットワークアクティビティをモニターして、悪意のあるホストへの接続が検出されたときにコネクタが実行するアクションを決定できます。

[検出アクション（Detection Action）] を使用すると、コネクタに悪意のあるホストへのネットワーク接続をブロックさせるか、接続を単純に記録させるかを選択できます。

[終了して検疫（Terminate and quarantine）] を使用すると、プロセスが不明な分類のファイルから発生した場合に、コネクタが悪意のあるホストへの接続の親プロセスを停止できます。このオプションは、検出アクションとして [ブロッキング（Blocking）] を選択したのみ使用できます。

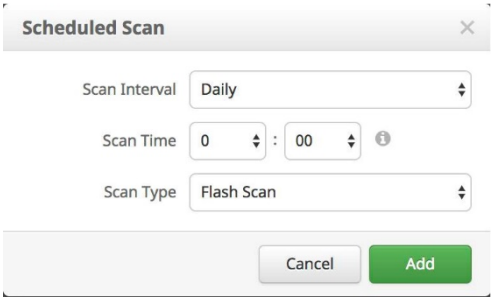
**警告：** この機能を有効にする前に、環境内で許可するアプリケーション、特に自前のソフトウェアやカスタムソフトウェアが許可リストに追加されていることを確認します。

[ブロックリストのデータソース（Blocked List Data Source）] を選択すると、コネクタが使用する IP ブロックリストを選択できます。[カスタム（Custom）] を選択すると、ポリシーに追加した IP ブロックリストのみコネクタで使用されます。悪意のあるサイトを定義するために、コネクタに Cisco Intelligence Feed だけを使用させる場合は、[シスコ（Cisco）] を選択します。Cisco Intelligence Feed は、Talos によって評価が低いと判断された IP アドレスを表示します。このリスト内のすべての IP アドレスが 24 時間ごとにフラッシュされます。Talos がアドレスに関連した不正な動作を続けて観察した場合は、それがリストに追加されます。[カスタムとシスコ（Custom and Cisco）] オプションを使用すると、ポリシーに追加した IP ブロックリストと Cisco Intelligence Feed の両方を使用できます。

## 定期スキャン

ファイルは、コピー、移動、および実行時に確認されるため、コネクタの処理に対して定期スキャンを実行する必要ありません。ファイルは、レトロスペクティブ機能を使用して 7 日後に再度確認されます。これにより、会社は、スケジュールされたスキャンの必要性を排除して、エネルギー フットプリントを削減できます。ただし、会社によっては、ポリシーのために定期スキャンが必要な場合があります。そのため、このスキャンは必要に応じてポリシー経由で有効にできるようになっています。

[スケジュール（Schedule）] の下にある [+新規（+New）] をクリックすると、スキャン間隔、スキャン時間、およびスキャンタイプを選択できるオーバーレイが表示されます。




[スキャン間隔（Scan Interval）] では、実行頻度を設定できます。オプションは [毎週（Weekly）] または [毎月（Monthly）] です。

[スキャン時間（Scan Time）] では、スキャンの開始時刻を設定できます。

[スキャンタイプ（Scan Type）] では、スキャンのタイプを設定できます。[フラッシュ（Flash）] スキャンでは、実行中のプロセスとプロセスで使用されているファイルとレジストリエントリがスキャンされます。[フル（Full）] スキャンでは、実行中のプロセス、レジストリエントリ、およびディスク上のすべてのファイルがスキャンされます。このスキャンは、大量のリソースを必要とするため、定期的に実行しないようにしてください。[カスタム（Custom）] スキャンでは、指定した特定のパスがスキャンされます。

### ID の永続化

**重要事項：**このポリシー設定はサポートによって有効になっている場合のみ使用可能です。この機能が必要な場合は、サポートに連絡して有効にしてください。

[IDの永続化（Identity Persistence）] を使用すると、仮想環境内で、またはコンピュータが再イメージ化されたときに、イベントログの整合性を維持できます。新しい仮想セッションが開始されるたびに、またはコンピュータが再イメージ化されるたびに新しいイベントログが作成されないように、コネクタを MAC アドレスまたはホスト名にバインドできます。以下のように、複数のポリシー全体または組織全体の単位でこの設定を適用することもできます。

- [なし（None）]：コネクタログは、いかなる環境下でも新しいコネクタのインストール環境に同期されません。
- [組織全体でMACアドレスを使用（By MAC Address across Oranization）]：新しいコネクタは、同じ MAC アドレスを持つ最新のコネクタを探して、[IDの同期（Identity Synchronization）] が [なし（None）] 以外の値に設定されている組織のすべてのポリシー全体で同期します。
- [ポリシー全体でMACアドレスを使用（By MAC Address across Policy）]：新しいコネクタは、同じ MAC アドレスを持つ最新のコネクタを探して同じポリシー内で同期します。
- [組織全体でホスト名を使用（By Host name across Oranization）]：新しいコネクタは、同じホスト名を持つ最新のコネクタを探して、[IDの同期（Identity Synchronization）] が [なし（None）] 以外の値に設定されている組織のすべてのポリシー全体で同期します。
- [ポリシー全体でホスト名を使用（By Host name across Policy）]：新しいコネクタは、同じホスト名を持つ最新のコネクタを探して同じポリシー内で同期します。

**重要：**複製された仮想マシンが、複製元のグループ以外のデフォルトグループに配置される場合があります。その場合は、Cisco Secure Endpoint コンソールで仮想マシンを正しいグループに移動します。

## Cisco Secure Endpoint Mac コネクタのポリシー

ここでは、Cisco Secure Endpoint Mac コネクタに使用可能なポリシーのオプションについて説明します。

## Mac コネクタ：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しいポリシーを保存する前に完了させる必要がある一連の設定ページの最初のページが表示されます。設定を入力して [次へ（Next）] をクリックし、ページを進めます。これらのページの設定については以下で説明します。

**重要：**これらのページで設定を完了するまでは、新しいポリシーの [アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] ページにはアクセスできません。

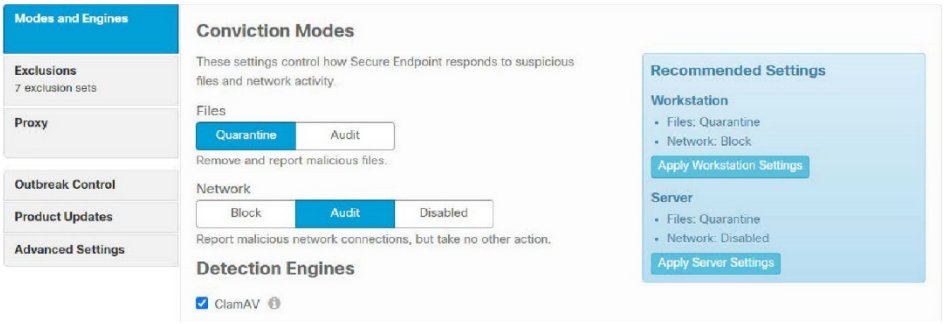
ここでは、Cisco Secure Endpoint Mac コネクタに使用可能なポリシーのオプションについて説明します。

### 名前（Name）と説明（Description）

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

### モードとエンジン

このページには、判定モードと検出エンジンに関する設定が含まれています。




#### 判定モード

判定モードでは、疑わしいファイルやネットワークアクティビティ対するコネクタの対応方法を指定します。ファイルを [監査（Audit ）] に設定すると、Cisco Secure Endpoint コネクタによるファイルの検疫が停止します。この設定は、Cisco Secure Endpoint コネクタのバージョン 3.1.0 以降にのみ適用されます。

**警告：**[ファイル判定モード（File Conviction Mode）] が [監査（Audit）] に設定されている場合は、エンドポイント上の悪意のあるファイルがアクセス可能なままになり、実行が許可されます。アプリケーション ブロッキング リストも適用されません。この設定は、独自のソフトウェアを使用したテストにのみ使用してください。

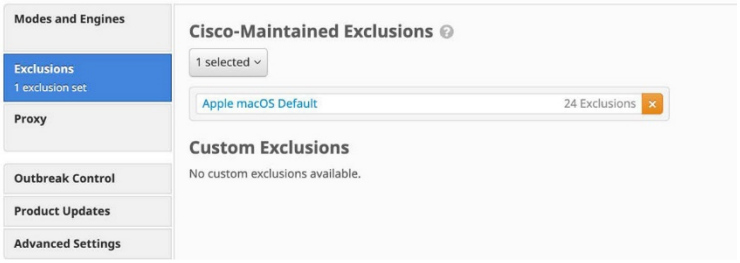
### 検出エンジン

Windows、Mac、および Linux のコネクタには、Cisco Cloud に接続して各ファイルにクエリを実行することなく、マルウェアからエンドポイントを保護するためのオフライン検出エンジン（Windows の場合は TETRA、Mac および Linux の場合は ClamAV）を有効にするオプションが用意されています。

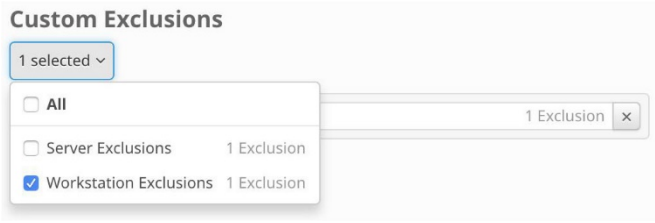
**ClamAV** は、ウイルス対策製品に全面的に代わるものであり、別のウイルス対策エンジンがインストールされている場合は絶対に有効にしないでください。また、ClamAV は、定義更新をダウンロードするときに大量の帯域幅を消費する可能性があるため、大規模環境で有効にする場合は注意が必要です。[詳細設定（Advanced Settings）] では、より多くの ClamAV 設定を使用できます。

## 除外事項

ここで、除外設定を選択してポリシーに適用できます。すべての新しい Mac ポリシーには、MacOS の特定のコンポーネントに関するシスコで維持されている除外設定が含まれています。この除外設定は削除できません。ポリシーグループに存在するアプリケーションに応じて、ポリシーに追加するその他のシスコで維持している除外設定を選択し、ユーザーのカスタム除外設定をポリシーに追加できます。

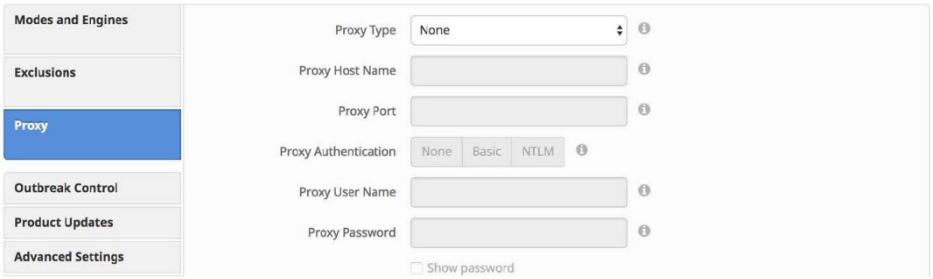



シスコで維持されている除外設定またはカスタム除外設定のいずれかのドロップダウンメニューをクリックし、チェックボックスをオンにして除外設定を選択します。詳細については、「除外事項」を参照してください。



### プロキシ

このページでプロキシ設定を実行します。




[プロキシタイプ（Proxy Type）] は、接続しているプロキシのタイプです。コネクタは、**http_proxy**、**socks4**、**socks4a**、**socks5**、**socks5_hostname**、および **mac_system_pac** をサポートします。

**重要事項：**mac_system_pac プロキシタイプには、コネクタバージョン 1.22.0 以降が必要です。コネクタでは、macOS ネットワークシステム設定の自動プロキシ設定 URL を使用してプロキシが設定されます。この URL が指定されていない限り、プロキシは使用されません。詳細については、Cisco Secure Endpoint Mac プロキシ自動設定（PAC）セットアップガイド [英語] を参照してください。

[プロキシホスト名（Proxy Host Name）] は、プロキシサーバーの名前または IP アドレスです。サポートされているのは IPv4 アドレスだけです。

[プロキシポート（Proxy Port）] は、プロキシサーバーで使用されるポートです。

[プロキシ認証（Proxy Authentication）] は、プロキシサーバーで使用される認証のタイプです。基本認証と NTLM 認証がサポートされています。

[プロキシユーザー名（Proxy User Name）] は、認証されたプロキシに使用されます。これは、接続時に使用するユーザー名です。

**重要：**プロキシ認証タイプとして NTLM を選択した場合は、このフィールドを domain\username の形式にする必要があります。

[プロキシパスワード（Proxy Password）] は、認証されたプロキシに使用されます。これは、プロキシ ユーザー名と一緒に使用するパスワードです。

## Mac コネクタ：その他のポリシー設定

必須の設定ページへの入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] にアクセスできるようになります。以降の項で設定について説明します。

**重要：**Cisco Defense Center が Cisco Secure Endpoint と統合されている場合は、ネットワークポリシータイプを使用できます。ネットワーク ポリシーには、次の一部の設定が含まれています。Cisco Defense Center と Cisco Secure Endpoint の統合の詳細については、Cisco Defense Center のマニュアルを参照してください。

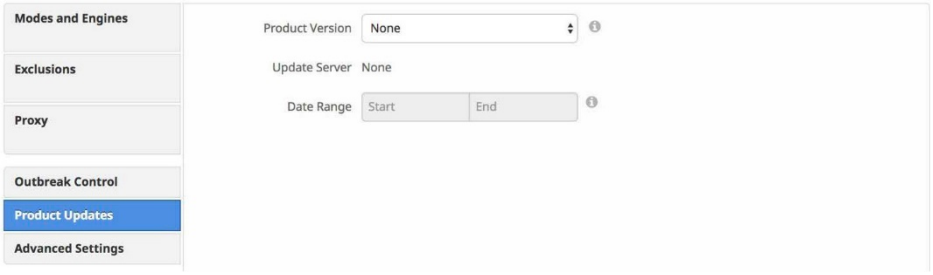
## Mac コネクタ：アウトブレイクコントロール

このページでは、ポリシーに割り当てるリストを選択します。各リストの作成の詳細については、「カスタム検出：簡易」、「カスタム検出：高度」、「アプリケーション制御：許可されたアプリケーション」、「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」、および「ネットワーク：IP ブロック/許可リスト」を参照してください。すべてのコネクタですべてのリストタイプがサポートされているわけではありません。

**重要事項：**ネットワーク：IPブロック/許可リストは、[詳細設定（Advanced Settings）] の [ネットワーク（Network）] タブで [デバイス フロー コリレーション（Device Flow Correlation）] が有効になっている場合にのみ機能します。

使用可能な IP ブロックリストまたは許可リストがある場合は、[リストの選択（Select Lists）] をクリックするとポリシーに追加するリストを選択できます。ドロップダウンメニューで、追加するすべてのリストのチェックボックスをオンにします。単一のポリシーに複数の IP リストを追加できますが、IP 許可リストエントリが IP ブロックリストエントリをオーバーライドします。

## Mac コネクタ：製品の更新

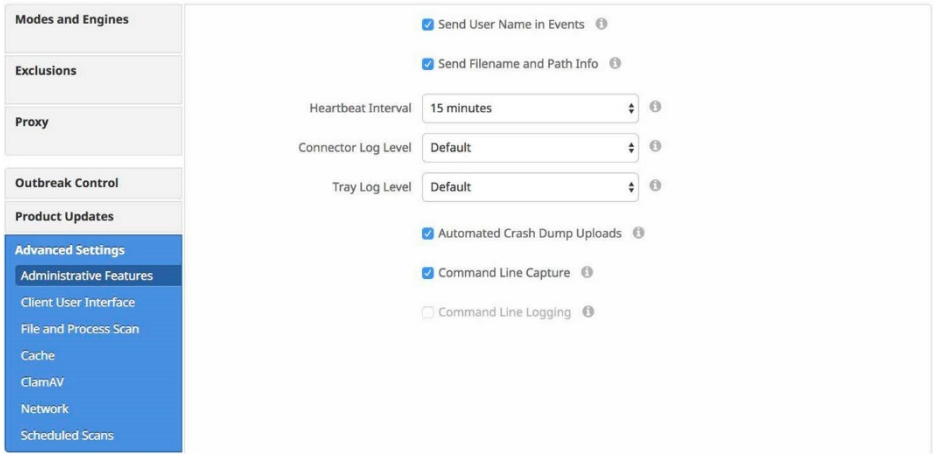



製品の更新が利用可能な場合は、ポリシー単位でエンドポイントの更新の有無を選択できます。表示するバージョンを示すエントリが [製品バージョン（Product Version）] ドロップダウンメニューに表示されます。そのエントリが [更新サーバー（Update Server）] に読み込まれるため、ファイルの抽出元を確認できます。z87 を有効にしており、[スケジュールの更新（Update Schedule）] で [コネクタ搭載（With Connector）] を選択している場合にのみ、Orbital の更新オプションが表示されます。

次に、[日付範囲（Date Range）] を選択することで、更新の実行が許可される時間枠を定義できます。[日付範囲（Date Range）] で、[開始（Start）] をクリックして、開始時間帯の日付と時刻を選択し、[終了（End）] をクリックして終了時間帯の日付と時刻を選択します。また、[今月（This Month）] を選択して現在の日から現在の月の月末までの日付範囲を設定するか、[今後 7 日間（Next 7 Days）] を選択して範囲を今後 7 日間に設定するか、[今後 30 日間（Next 30 Days）] を選択して範囲を今後 30 日間に設定することもできます。[日付範囲（Date Range）] に設定された時刻の間にコネクタがホームをコールしてポリシーを取得した場合、製品の更新が取得されます。コネクタはハートビート間隔に応じた間隔でホームをコールするため、更新期間をこの間隔に従って計画することをお勧めします。そうすることで、更新期間で指定された間隔を、ハートビート間隔より長くできます。

# Mac コネクタ：詳細設定

## 管理機能




[イベント内のユーザー名を送信（Send User Name in Events）] では、プロセスを実行、コピー、または移動した実際のユーザー名（既知の場合）が送信されます。これは、マルウェアを観察している人物を追跡するのに役立ちます。この機能が有効になっていない場合は、ユーザーとして実行、コピー、または移動したマルウェアには「u」が、管理者として実行、コピー、または移動したマルウェアには「a」が表示されます。

[ファイル名とパス情報を送信（Send Filename and Path Info）] では、ファイル名とパス情報が Cisco Secure Endpoint に送信されるため、[イベント（Events）] タブ、[デバイストラジェクト（Device Trajectory）]、および [ファイルトラジェクトリ（File Trajectory）] で確認できます。この設定をオフにすると、この情報の送信が停止されます。

[ハートビート間隔（Heartbeat Interval）] は、コネクタがホームをコールして、レトロスペクティブ機能または管理者によって復元するファイル、取得するポリシー、実行するタスク（製品の更新やスキャンなど）の有無を確認するための間隔です。

[コネクタログレベル（Connector Log Level）] と [トレイログレベル（Tray Log Level）] を使用すると、デフォルトのログレベルとデバッグ（詳細）ログレベルを選択できます。デフォルト レベルは、トラブルシューティング中にサポートからデバッグが要求されないかぎり、設定しておく必要があります。

**警告：**[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合、ログファイルでさらに 550MB のドライブ容量が使用される可能性があります。

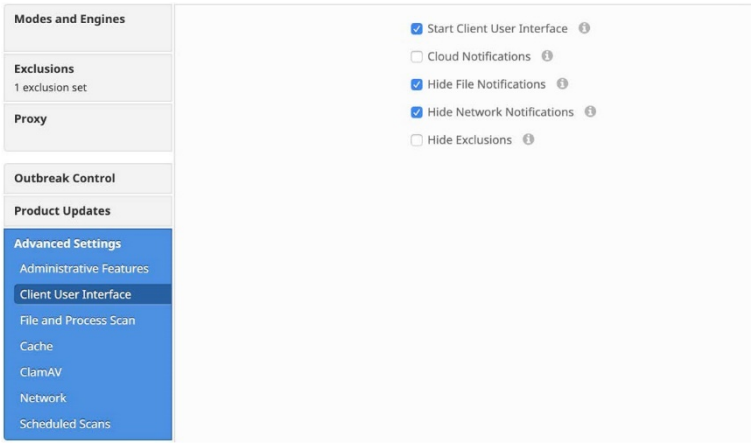
[クラッシュダンプの自動アップロード（Automated Crash Dump Uploads）] を選択すると、分析のためにコネクタのクラッシュダンプファイルをシスコに自動的にアップロードするかどうかを選択できます。

[コマンドラインキャプチャ（Command Line Capture）]（Cisco Secure Endpoint Mac 1.5.0 以降）を選択すると、ファイルの実行中に使用するコマンドライン引数（ユーザー名、ファイル名、パスワードなど）をコネクタがキャプチャして、情報が Cisco Secure Endpoint に送信されます。この情報は、管理者がシングルサインオン（Security Cloud Sign-On など）を使用しているか、二要素認証が有効になっている限り、デバイストラジェクトリに表示されます。

**重要：**コマンド ライン キャプチャを使用するには、 macOS 10.12 以降がインストールされている必要があります。

[コマンドラインキャプチャ（Command Line Capture）] が有効になっており、[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合は、エンドポイントで [コマンドラインロギング（Command Line Logging）] を使用して、キャプチャされたコマンドライン引数をローカルのコネクタログファイルに記録できます。

## クライアント ユーザー インターフェイス




[クライアント ユーザー インターフェイスを開始（Start Client User Interface）] を使用すると、コネクタ ユーザー インターフェイスを完全に非表示にするかどうかを指定できます。

**重要：**この設定を変更した場合、コネクタを再起動するまで、変更は有効になりません。

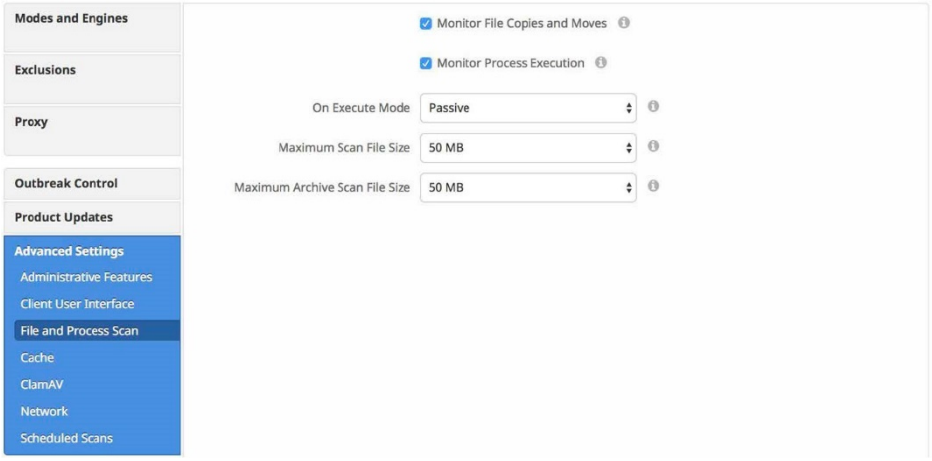
[クラウド通知（Cloud Notifications）] は、コネクタがクラウドとの接続に成功したときにメニューバーから表示されるバルーンポップアップです。この通知には、クラウドに登録されたユーザー数と検出数が表示されます。

[ファイル通知を非表示にする（Hide File Notifications）] を選択すると、悪意のあるファイルがコネクタによって判定または検疫された場合に通知がユーザーに表示されません。

[ネットワーク通知を非表示にする（Hide Network Notifications）] を選択すると、悪意のあるネットワーク接続がコネクタによって検出またはブロックされた場合に通知がユーザーに表示されません。

[除外事項を非表示にする（Hide Exclusions）] を選択すると、設定された除外事項がコネクタ ユーザー インターフェイスに表示されません。

## ファイルとプロセスのスキャン




[ファイルのコピーおよび移動時のモニタリング（Monitor File Copies and Moves）] は、コピーまたは移動されたファイルにコネクタがリアルタイム保護を提供するための機能です。

[プロセス実行のモニタリング（Monitor Process Execution）] は、実行されたファイルにコネクタがリアルタイム保護を提供するための機能です。

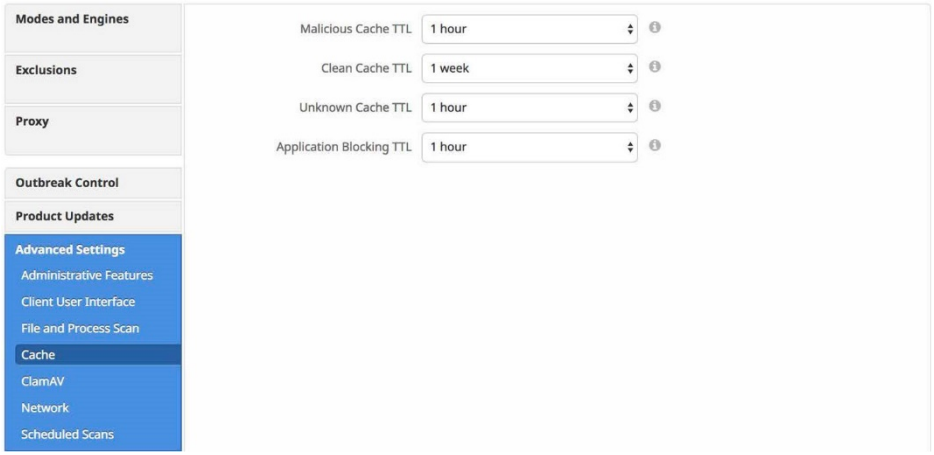
[オンエグゼキュートモード（On Execute Mode）] は、2 種類のモード（[アクティブ（Active）] と [パッシブ（Passive）]）で実行できます。[アクティブ（Active）] モードでは、ファイルが有害かどうか、またはタイムアウトに到達したかどうかが判断されるまで実行がブロックされます。パッシブ モードでは、ファイルが実行を許可されると同時に、検査され、有害かどうかが判断されます。

**警告：**アクティブ モードはより優れた保護を提供しますが、パフォーマンスの問題を引き起こす可能性があります。エンドポイントにすでにウイルス対策製品がインストールされている場合は、これを [パッシブ（Passive）] のままにすることをお勧めします。

[最大スキャンファイルサイズ（Maximum Scan File Size）] では、コネクタによってスキャンされるファイルのサイズを制限します。しきい値設定より大きなファイルはスキャンされません。

[最大アーカイブ スキャン ファイル サイズ（Maximum Archive Scan File Size）] では、コネクタによってスキャンされるアーカイブファイルのサイズを制限します。しきい値設定より大きなアーカイブ ファイルはスキャンされません。

## キャッシュ




SHA-256 値は、クラウド検索トラフィックを削減するためにキャッシュされます。値がキャッシュされる時間は、その SHA-256 に対して最後のクラウド検索が実行されたファイルの分類によって異なります。ファイルがキャッシュされている間、コネクタは常に、その分類を最後にクラウド検索が実行されたときの分類と見なします。たとえば、SHA-256 がアプリケーション ブロッキング リストに含まれており、TTL が 3,600 秒の場合、管理者がそのアプリケーションをアプリケーション ブロッキング リストから削除しても、次の 1 時間はコネクタによってアプリケーションの実行がブロックされます。

[悪意のあるキャッシュTTL（Malicious Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に悪意のある分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[クリーンキャッシュTTL（Clean Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前にクリーンな分類のファイルがキャッシュされる時間です。デフォルト値は 1 週間です。

[不明なキャッシュTTL（Unknown Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に不明な分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[アプリケーション ブロッキングTTL（Application Blocking TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に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リストにあるファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

**重要：**コネクタによって過去に観察されたアプリケーション ブロッキング リストに「クリーン（Clean）」分類の SHA-256 を追加する場合は、コネクタを停止して、アプリケーションの実行をブロックするコンピュータのインストールディレクトリから cache.db ファイルを削除する必要があります。削除しないと、アプリケーションの実行をブロックする前に、クリーンファイルの TTL 期限が切れ、別のクラウド検索がコネクタによって実行されるまで待機する必要があります。

## エンドポイントの隔離

エンドポイントの隔離を使用すると、Mac コンピュータでの着信および発信ネットワークアクティビティをブロックし、データ漏洩やマルウェアの拡散などの脅威を防ぐことができます。

[DNSの許可（Allow DNS）] により、エンドポイントが隔離されている間に DNS ルックアップを実行できます。エンドポイントのネットワーク設定で構成された DNS サーバーのアドレスは、コネクタによって許可リストに自動的に追加されます。この設定をオフにする場合は、DNS サーバーのアドレスを手動で許可リストに追加する必要があります。

[DHCPの許可（Allow DHCP）] により、エンドポイントが UDP ポート 67 および 68 でトラフィックを送受信できるようになるため、DHCP リースを取得または更新できます。静的 IP アドレスを使用する場合は、これを安全にオフにできます。この設定をオフにする場合は、DHCP サーバーのアドレスを手動で許可リストに追加する必要があります。

隔離セッション中にコネクタが使用する [IP許可リスト（IP Allow Lists）] を指定できます。[リストの選択（Select Lists）] プルダウンを使用して、このポリシーで使用する IP 隔離許可リストを指定します。

## Orbital

**重要：**Orbital は、Cisco Secure Endpoint Advantage または上位のパッケージを使用している場合に利用できます。

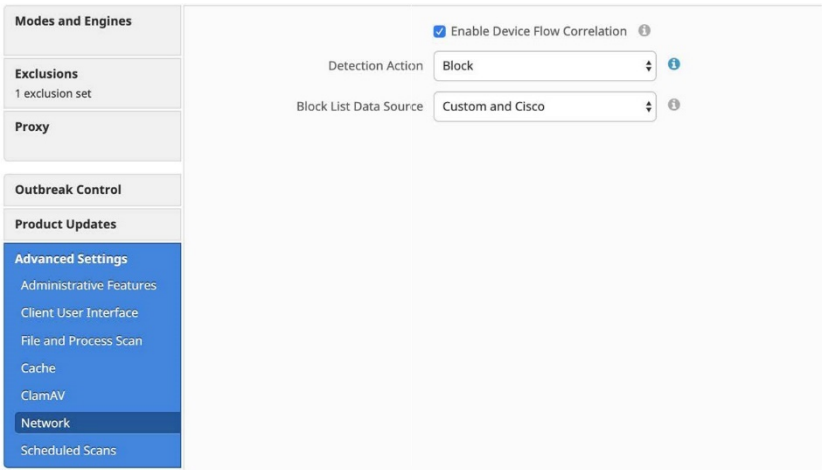
Orbital を使用すると、Orbital の展開場所に関係なくエンドポイントをクエリして詳細情報を取得できます。Orbital の使用の詳細については、Orbital のマニュアル（https://orbital.amp.cisco.com/help/）を参照してください。

ポリシーで Orbital を有効にするには、[Orbital Advanced Searchを有効にする（Enable Orbital Advanced Search）] チェックボックスをオンにして、[保存（Save）] をクリックします。

Orbital は、Intel プロセッサを搭載した macOS 10.15 以降で動作するコンピュータ、または Apple シリコンを搭載した macOS 12 以降で動作するコンピュータにインストールされます。Orbital は、Apple シリコンでは Cisco Secure Endpoint Mac コネクタバージョン 1.20 以降でサポートされ、Orbital Node 1.21 以降が必要です。インストールが正常に完了すると、コネクタから Cisco Secure Endpoint コンソールにイベントが送信されます。[スケジュールの更新（Update Schedule）] では、新しいバージョンが利用可能になるたびに Orbital を自動的に更新するか、Mac コネクタ：製品の更新で更新をスケジュールするかを定義できます。

**重要：**ポリシーに関して Orbital を無効にすると、サービスは停止されて無効になりますが、Orbital はエンドポイントからアンインストールされません。再度有効にすると、サービスが再起動され、Orbital の更新が再度有効になります。

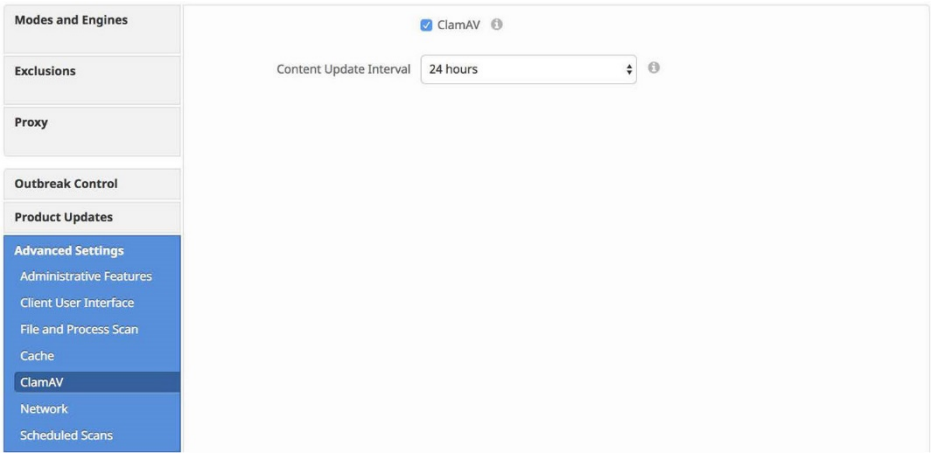
## ClamAV




完全なウイルス対策製品として、ClamAV を使用するとオフラインのスキャンを実行できます。これは、シグニチャ ベースであり、ローカル コンピュータ上のディスク領域をより多く消費します。これは、デフォルトで 24 時間ごとに更新されたシグニチャをチェックして、新しいシグニチャが利用可能になるとダウンロードします。この主な欠点は他のウイルス対策製品との互換性であり、他のウイルス対策製品がコンピュータ上にインストールされている場合は有効にしないでください。

[コンテンツの更新間隔（Content Update Interval）] では、署名などの新しい ClamAV コンテンツがコネクタでチェックされる頻度を指定できます。更新間隔が長いほど、ClamAV 更新によるネットワーク トラフィックが減少します。逆に更新間隔が短いほど、大量の帯域幅が消費される可能性があり、大規模展開にはお勧めできません。[コンピュータの管理（Computer Management）] ページで、コンピュータの ClamAV 定義のバージョンと更新ステータスを確認できます。

## ネットワーク



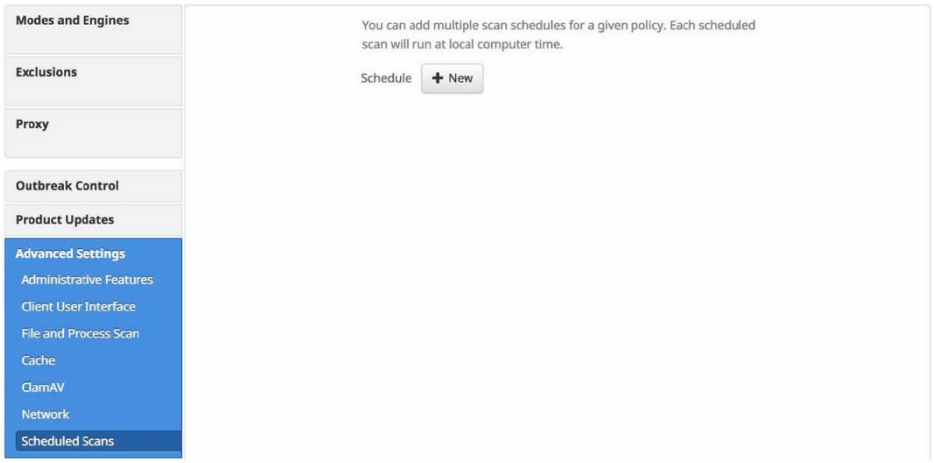
[ネットワーク（Network）] タブには、デバイス フロー コリレーション設定など、コネクタのネットワークフロー機能に関する設定が含まれています。

[デバイス フロー コリレーションの有効化（Enable Device Flow Correlation）] を使用すると、ネットワークアクティビティをモニターして、悪意のあるホストへの接続が検出されたときにコネクタが実行するアクションを決定できます。

[検出アクション（Detection Action）] を使用すると、コネクタに悪意のあるホストへのネットワーク接続をブロックさせるか、接続を単純に記録させるかを選択できます。

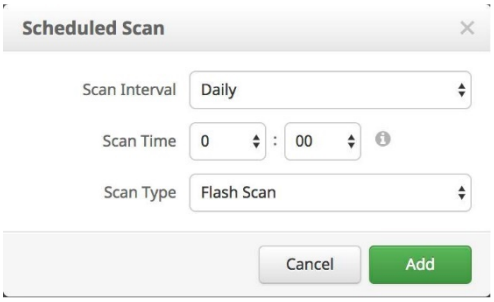
[ブロックリストのデータソース（Blocked List Data Source）] を選択すると、コネクタが使用する IP ブロックリストを選択できます。[カスタム（Custom）] を選択すると、ポリシーに追加した IP ブロックリストのみコネクタで使用されます。悪意のあるサイトを定義するために、コネクタに Cisco Intelligence Feed だけを使用させる場合は、[シスコ（Cisco）] を選択します。Cisco Intelligence Feed は、Talos によって評価が低いと判断された IP アドレスを表示します。このリスト内のすべての IP アドレスが 24 時間ごとにフラッシュされます。Talos がアドレスに関連した不正な動作を続けて観察した場合は、それがリストに追加されます。[カスタムとシスコ（Custom and Cisco）] オプションを使用すると、ポリシーに追加した IP ブロックリストと Cisco Intelligence Feed の両方を使用できます。

## 定期スキャン




ファイルは、コピー、移動、および実行時に確認されるため、コネクタの処理に対して定期スキャンを実行する必要ありません。ファイルは、レトロスペクティブ機能を使用して 7 日後に再度確認されます。これにより、会社は、スケジュールされたスキャンの必要性を排除して、エネルギー フットプリントを削減できます。ただし、会社によっては、ポリシーのために定期スキャンが必要な場合があります。そのため、このスキャンは必要に応じてポリシー経由で有効にできるようになっています。

[スケジュール（Schedule）] の下にある [+新規（+New）] をクリックすると、スキャン間隔、スキャン時間、およびスキャンタイプを選択できるオーバーレイが表示されます。




[スキャン間隔（Scan Interval）] では、実行頻度を設定できます。オプションは [毎週（Weekly）] または [毎月（Monthly）] です。

[スキャン時間（Scan Time）] では、スキャンの開始時刻を設定できます。

[スキャンタイプ（Scan Type）] では、スキャンのタイプを設定できます。[フラッシュ（Flash）] スキャンでは、実行中のプロセスとプロセスで使用されているファイルとレジストリエントリがスキャンされます。[フル（Full）] スキャンでは、実行中のプロセス、レジストリエントリ、およびディスク上のすべてのファイルがスキャンされます。このスキャンは、大量のリソースを必要とするため、定期的に実行しないようにしてください。[カスタム（Custom）] スキャンでは、指定した特定のパスがスキャンされます。

# Cisco Secure Endpoint Linux コネクタのポリシー

ここでは、Cisco Secure Endpoint Linux コネクタに使用可能なポリシーのオプションについて説明します。

## Linux コネクタ：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しいポリシーを保存する前に完了させる必要がある一連の設定ページの最初のページが表示されます。設定を入力して [次へ（Next）] をクリックし、ページを進めます。これらのページの設定については以下で説明します。

**重要：**これらのページで設定を完了するまでは、新しいポリシーの [アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] ページにはアクセスできません。

ここでは、Cisco Secure Endpoint Linux コネクタに使用可能なポリシーのオプションについて説明します。

## 名前と説明

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

## モードとエンジン

このページには、判定モードと検出エンジンに関する設定が含まれています。

### 判定モード

判定モードでは、疑わしいファイルやネットワークアクティビティ対するコネクタの対応方法を指定します。ファイルを [監査（Audit ）] に設定すると、Cisco Secure Endpoint コネクタによるファイルの検疫が停止します。この設定は、Cisco Secure Endpoint コネクタのバージョン 3.1.0 以降にのみ適用されます。

**警告：**[ファイル判定モード（File Conviction Mode）] が [監査（Audit）] に設定されている場合は、エンドポイント上の悪意のあるファイルがアクセス可能なままになり、実行が許可されます。アプリケーション ブロッキング リストも適用されません。この設定は、独自のソフトウェアを使用したテストにのみ使用してください。

動作保護は、[保護（Protect）] モードにおいて悪意のあるアクティビティに関するアラートを表示、ファイルを検疫、およびプロセスを終了することで、一連の動作署名と一致する悪意のあるアクティビティを阻止します。[監査（Audit）] モードでは、一致するアクティビティが検出されたときにイベントが作成されますが、アクションは実行されません。

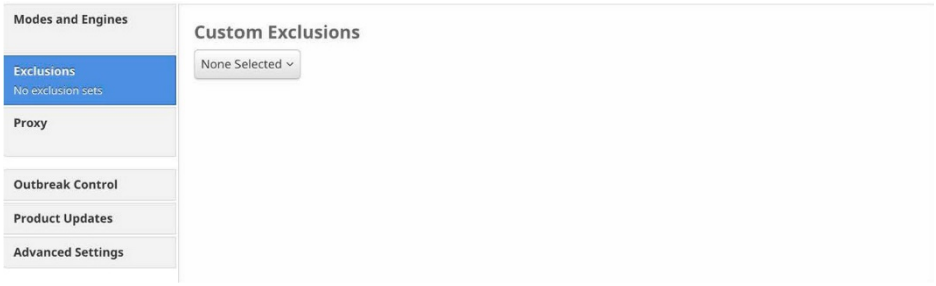
### 検出エンジン

Windows、Mac、および Linux のコネクタには、Cisco Cloud に接続して各ファイルにクエリを実行することなく、マルウェアからエンドポイントを保護するためのオフライン検出エンジン（Windows の場合は TETRA、Mac および Linux の場合は ClamAV）を有効にするオプションが用意されています。

**ClamAV** は、ウイルス対策製品に全面的に代わるものであり、別のウイルス対策エンジンがインストールされている場合は絶対に有効にしないでください。また、ClamAV は、定義更新をダウンロードするときに大量の帯域幅を消費する可能性があるため、大規模環境で有効にする場合は注意が必要です。[詳細設定（Advanced Settings）] では、より多くの ClamAV 設定を使用できます。

## 除外事項

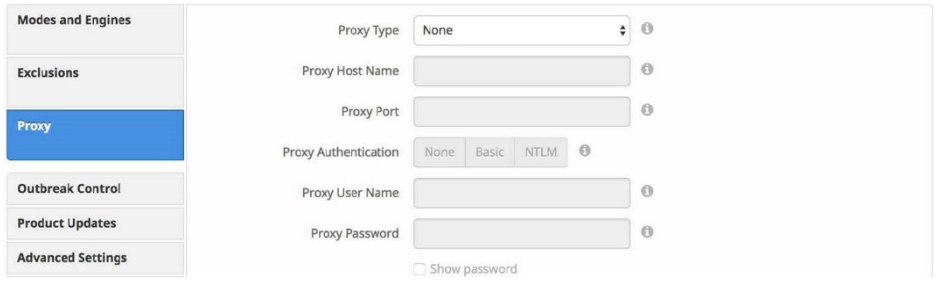
ここで、除外設定を選択してポリシーに適用できます。




ドロップダウンメニューをクリックし、チェックボックスをオンにしてカスタム除外設定を選択します。詳細については、「除外事項」を参照してください。


## プロキシ

このページでプロキシ設定を実行します。




[プロキシタイプ（Proxy Type）] は、接続しているプロキシのタイプです。コネクタは、**http_proxy**、**socks4**、**socks4a**、**socks5**、および **socks5_hostname** をサポートします。

[プロキシホスト名（Proxy Host Name）] は、プロキシサーバーの名前または IP アドレスです。サポートされているのは IPv4 アドレスだけです。

[プロキシポート（Proxy Port）] は、プロキシサーバーで使用されるポートです。

[プロキシ認証（Proxy Authentication）] は、プロキシサーバーで使用される認証のタイプです。**基本**認証と **NTLM** 認証がサポートされています。

[プロキシユーザー名（Proxy User Name）] は、認証されたプロキシに使用されます。これは、接続時に使用するユーザー名です。

**重要：**プロキシ認証タイプとして NTLM を選択した場合は、このフィールドを domain\username の形式にする必要があります。

[プロキシパスワード（Proxy Password）] は、認証されたプロキシに使用されます。これは、プロキシ ユーザー名と一緒に使用するパスワードです。

## Linux コネクタ：その他のポリシー設定

必須の設定ページへの入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページ、[製品の更新（Product Updates）] ページ、および [詳細設定（Advanced Settings）] にアクセスできるようになります。以降の項で設定について説明します。

**重要：**Cisco Defense Center が Cisco Secure Endpoint と統合されている場合は、ネットワークポリシータイプを使用できます。ネットワーク ポリシーには、次の一部の設定が含まれています。Cisco Defense Center と Cisco Secure Endpoint の統合の詳細については、Cisco Defense Center のマニュアルを参照してください。

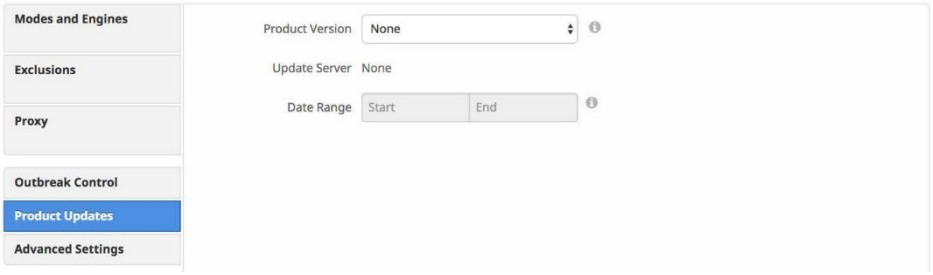
## Linux コネクタ：アウトブレイクコントロール

このページでは、ポリシーに割り当てるリストを選択します。各リストの作成の詳細については、「カスタム検出：簡易」、「カスタム検出：高度」、「アプリケーション制御：許可されたアプリケーション」、「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」、および「ネットワーク：IP ブロック/許可リスト」を参照してください。すべてのコネクタですべてのリストタイプがサポートされているわけではありません。

**重要事項：**ネットワーク：IPブロック/許可リストは、[詳細設定（Advanced Settings）] の [ネットワーク（Network）] タブで [デバイス フロー コリレーション（Device Flow Correlation）] が有効になっている場合にのみ機能します。

使用可能な IP 許可リストまたはブロックリストがある場合は、[リストの選択（Select Lists）] をクリックするとポリシーに追加するリストを選択できます。ドロップダウンメニューで、追加するすべてのリストのチェックボックスをオンにします。単一のポリシーに複数の IP リストを追加できますが、IP 許可リストが IP ブロックリストエントリをオーバーライドします。

## Linux コネクタ：製品の更新



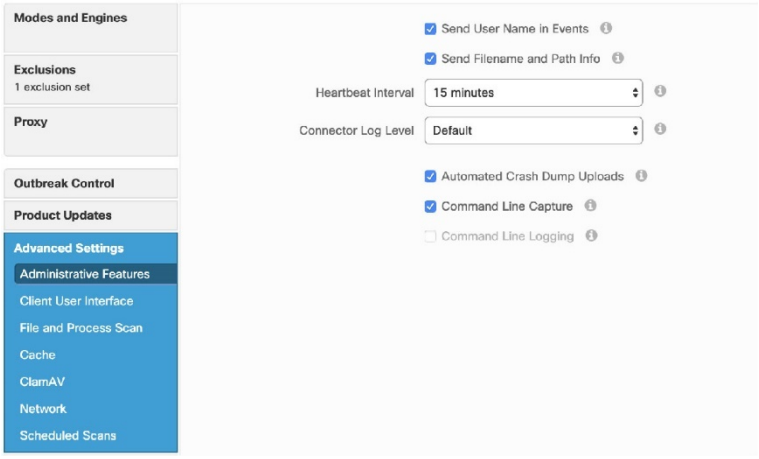

製品の更新が利用可能な場合は、ポリシー単位でエンドポイントの更新の有無を選択できます。表示するバージョンを示すエントリが [製品バージョン（Product Version）] ドロップダウンメニューに表示されます。そのエントリが [更新サーバー（Update Server）] に読み込まれるため、ファイルの抽出元を確認できます。Orbital を有効にしており、[スケジュールの更新（Update Schedule）] で [コネクタ搭載（With Connector）] を選択している場合にのみ、Orbital の更新オプションが表示されます。一部の更新プログラムを正しくインストールするには、リブートが必要です。特定の更新のリブート要件については、この記事を参照してください。

次に、[日付範囲（Date Range）] を選択することで、更新の実行が許可される時間枠を定義できます。[日付範囲（Date Range）] で、[開始（Start）] をクリックして、開始時間帯の日付と時刻を選択し、[終了（End）] をクリックして終了時間帯の日付と時刻を選択します。また、[今月（This Month）] を選択して現在の日から現在の月の月末までの日付範囲を設定するか、[今後 7 日間（Next 7 Days）] を選択して範囲を今後 7 日間に設定するか、[今後 30 日間（Next 30 Days）] を選択して範囲を今後 30 日間に設定することもできます。

[日付範囲（Date Range）] に設定された時刻の間にコネクタがホームをコールしてポリシーを取得した場合、製品の更新が取得されます。コネクタはハートビート間隔に応じた間隔でホームをコールするため、更新期間をこの間隔に従って計画することをお勧めします。そうすることで、更新期間で指定された間隔を、ハートビート間隔より長くできます。

# Linux コネクタ：詳細設定

## 管理機能




[イベント内のユーザー名を送信（Send User Name in Events）] では、プロセスを実行、コピー、または移動した実際のユーザー名（既知の場合）が送信されます。これは、マルウェアを観察している人物を追跡するのに役立ちます。この機能が有効になっていない場合は、ユーザーとして実行、コピー、または移動したマルウェアには「u」が、管理者として実行、コピー、または移動したマルウェアには「a」が表示されます。

[ファイル名とパス情報を送信（Send Filename and Path Info）] では、ファイル名とパス情報が Cisco Secure Endpoint に送信されるため、[イベント（Events）] タブ、[デバイストラジェクト（Device Trajectory）]、および [ファイルトラジェクトリ（File Trajectory）] で確認できます。この設定をオフにすると、この情報の送信が停止されます。

[ハートビート間隔（Heartbeat Interval）] は、コネクタがホームをコールして、レトロスペクティブ機能または管理者によって復元するファイル、取得するポリシー、実行するタスク（製品の更新やスキャンなど）の有無を確認するための間隔です。

[コネクタログレベル（Connector Log Level）] を使用すると、デフォルトのログレベルとデバッグ（詳細）ログレベルを選択できます。デフォルト レベルは、トラブルシューティング中にサポートからデバッグが要求されないかぎり、設定しておく必要があります。

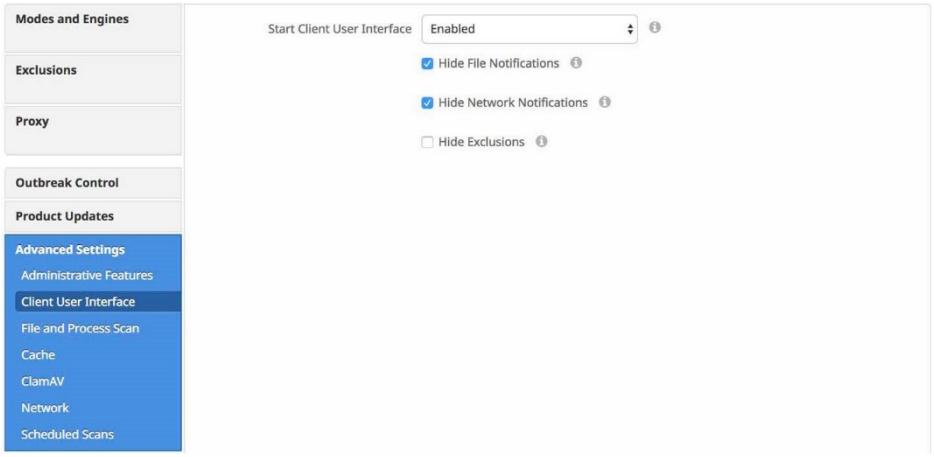
**警告：**[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合、ログファイルでさらに 550MB のドライブ容量が使用される可能性があります。

[クラッシュダンプの自動アップロード（Automated Crash Dump Uploads）] を選択すると、分析のためにコネクタのクラッシュダンプファイルをシスコに自動的にアップロードするかどうかを選択できます。

[コマンドラインキャプチャ（Command Line Capture）]（Cisco Secure Endpoint Linux コネクタ 1.5.0 以降）を選択すると、ファイルの実行中に使用するコマンドライン引数（ユーザー名、ファイル名、パスワードなど）をコネクタがキャプチャして、情報が Cisco Secure Endpoint に送信されます。この情報は、管理者がシングルサインオン（Security Cloud Sign-On など）を使用しているか、二要素認証が有効になっている限り、デバイストラジェクトリに表示されます。

[コマンドラインキャプチャ（Command Line Capture）] が有効になっており、[コネクタログレベル（Connector Log Level）] が [デバッグ（Debug）] に設定されている場合は、エンドポイントで [コマンドラインロギング（Command Line Logging）] を使用して、キャプチャされたコマンドライン引数をローカルのコネクタログファイルに記録できます。

## クライアント ユーザー インターフェイス




[クライアント ユーザー インターフェイスを開始（Start Client User Interface）] を使用すると、コネクタ ユーザー インターフェイスを完全に非表示にするかどうかを指定できます。[無効（Disabled）] を選択すると、コネクタはサービスとして実行されますが、ユーザー インターフェイス コンポーネントは実行されません。[コマンドラインのみ（Command Line Only）] と [特権コマンドラインのみ（Privileged Command Line Only）] を選択すると、コネクタはインターフェイス コンポーネントなしにサービスとして実行されますが、端末を経由したユーザーアクセスは許可されます。

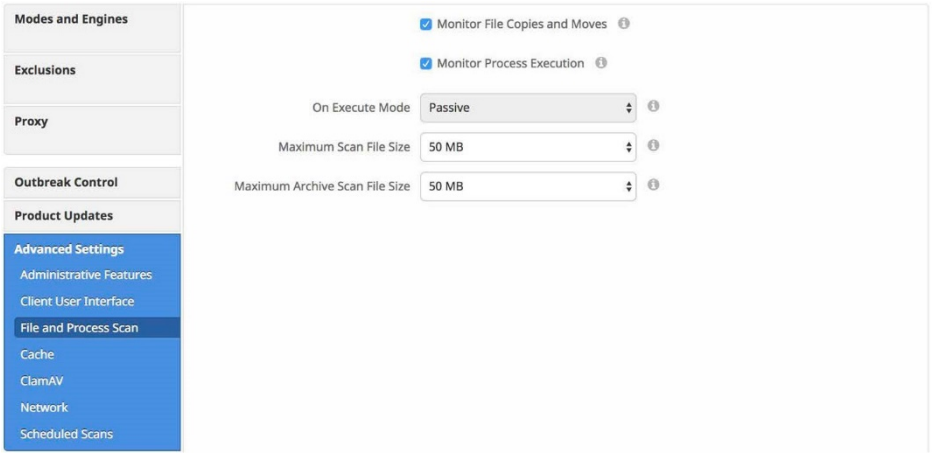
**重要：**この設定を変更した場合、コネクタを再起動するまで、変更は有効になりません。

[ファイル通知を非表示にする（Hide File Notifications）] を選択すると、悪意のあるファイルがコネクタによって判定または検疫された場合に通知がユーザーに表示されません。

[ネットワーク通知を非表示にする（Hide Network Notifications）] を選択すると、悪意のあるネットワーク接続がコネクタによって検出またはブロックされた場合に通知がユーザーに表示されません。

[除外事項を非表示にする（Hide Exclusions）] を選択すると、設定された除外事項がコネクタ ユーザー インターフェイスに表示されません。

## ファイルとプロセスのスキャン




[ファイルのコピーおよび移動時のモニタリング（Monitor File Copies and Moves）] は、コピーまたは移動されたファイルにコネクタがリアルタイム保護を提供するための機能です。

[プロセス実行のモニタリング（Monitor Process Execution）] は、実行されたファイルにコネクタがリアルタイム保護を提供するための機能です。

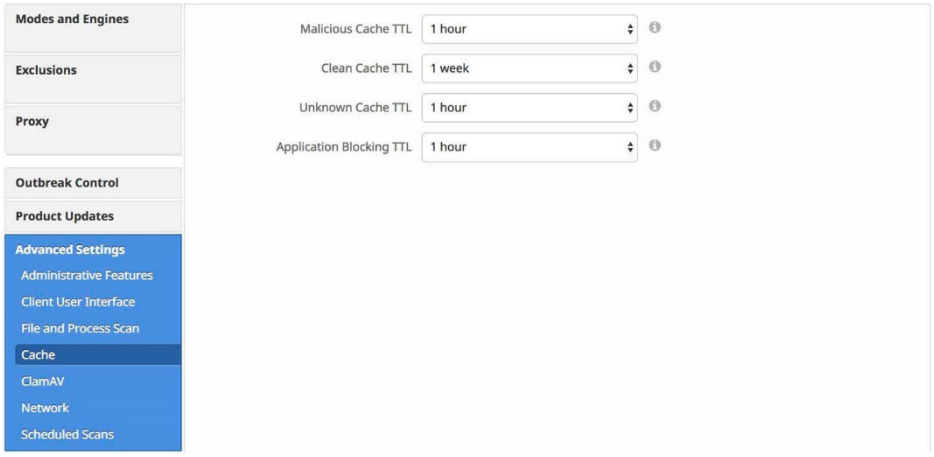
[オンエグゼキュートモード（On Execute Mode）] は、2 種類のモード（[アクティブ（Active）] と [パッシブ（Passive）]）で実行できます。[アクティブ（Active）] モードでは、ファイルが有害かどうか、またはタイムアウトに到達したかどうかが判断されるまで実行がブロックされます。パッシブ モードでは、ファイルが実行を許可されると同時に、検査され、有害かどうかが判断されます。

警告：アクティブ モードはより優れた保護を提供しますが、パフォーマンスの問題を引き起こす可能性があります。エンドポイントにすでにウイルス対策製品がインストールされている場合は、これを [パッシブ（Passive）] のままにすることをお勧めします。

[最大スキャンファイルサイズ（Maximum Scan File Size）] では、コネクタによってスキャンされるファイルのサイズを制限します。しきい値設定より大きなファイルはスキャンされません。

[最大アーカイブ スキャン ファイル サイズ（Maximum Archive Scan File Size）] では、コネクタによってスキャンされるアーカイブファイルのサイズを制限します。しきい値設定より大きなアーカイブ ファイルはスキャンされません。

## キャッシュ




SHA-256 値は、クラウド検索トラフィックを削減するためにキャッシュされます。値がキャッシュされる時間は、その SHA-256 に対して最後のクラウド検索が実行されたファイルの分類によって異なります。ファイルがキャッシュされている間、コネクタは常に、その分類を最後にクラウド検索が実行されたときの分類と見なします。たとえば、SHA-256 がアプリケーション ブロッキング リストに含まれており、TTL が 3,600 秒の場合、管理者がそのアプリケーションをアプリケーション ブロッキング リストから削除しても、次の 1 時間はコネクタによってアプリケーションの実行がブロックされます。

[悪意のあるキャッシュTTL（Malicious Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に悪意のある分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[クリーンキャッシュTTL（Clean Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前にクリーンな分類のファイルがキャッシュされる時間です。デフォルト値は 1 週間です。

[不明なキャッシュTTL（Unknown Cache TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に不明な分類のファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

[アプリケーション ブロッキングTTL（Application Blocking TTL）] は、コネクタで SHA-256 値が確認されたときに、別のクラウドルックアップが実行される前に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リストにあるファイルがキャッシュされる時間です。デフォルト値は 1 時間です。

**重要：**コネクタによって過去に観察されたアプリケーション ブロッキング リストに「クリーン（Clean）」分類の SHA-256 を追加する場合は、コネクタを停止して、アプリケーションの実行をブロックするコンピュータのインストールディレクトリから cache.db ファイルを削除する必要があります。削除しないと、アプリケーションの実行をブロックする前に、クリーンファイルの TTL 期限が切れ、別のクラウド検索がコネクタによって実行されるまで待機する必要があります。

## Orbital

**重要：**Orbital は、Cisco Secure Endpoint Advantage または上位のパッケージを使用している場合に利用できます。

Orbital を使用すると、Orbital の展開場所に関係なくエンドポイントをクエリして詳細情報を取得できます。Orbital の使用の詳細については、Orbital のマニュアル（https://orbital.amp.cisco.com/help/）を参照してください。

ポリシーで Orbital を有効にするには、[Orbital Advanced Searchを有効にする（Enable Orbital Advanced Search）] チェックボックスをオンにして、[保存（Save）] をクリックします。

インストールが正常に完了すると、コネクタから Cisco Secure Endpoint コンソールにイベントが送信されます。[スケジュールの更新（Update Schedule）] では、新しいバージョンが利用可能になるたびに Orbital を自動的に更新するか、Linux コネクタ：製品の更新で更新をスケジュールするかを定義できます。

ポリシーに関して Orbital を無効にすると、サービスは停止されて無効になりますが、Orbital はエンドポイントからアンインストールされません。再度有効にすると、サービスが再起動され、Orbital の更新が再度有効になります。

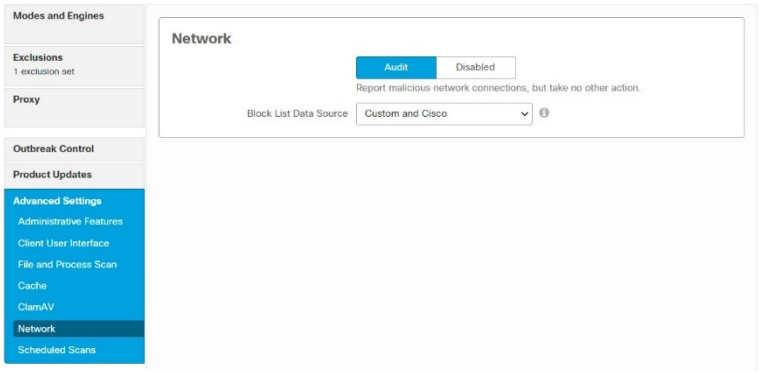
## ClamAV

完全なウイルス対策製品として、ClamAV を使用するとオフラインのスキャンを実行できます。これは、シグニチャ ベースであり、ローカル コンピュータ上のディスク領域をより多く消費します。これは、デフォルトで 24 時間ごとに更新されたシグニチャをチェックして、新しいシグニチャが利用可能になるとダウンロードします。この主な欠点は他のウイルス対策製品との互換性であり、他のウイルス対策製品がコンピュータ上にインストールされている場合は有効にしないでください。

ClamAV 定義には、Linux、macOS、および Windows に影響するマルウェアを検出するためのシグニチャがデフォルトで含まれています。[AV定義（AV definitions）] 設定を使用して、一連の ClamAV 定義をすべてダウンロードするか、または Linux マルウェアの署名のみを含む定義の小規模なサブセットをダウンロードするかを選択します。スキャンする予定のファイルのタイプなど、環境に最も適した定義を選択します。詳細については、『Secure Endpoint: ClamAV Virus Definition Options in Linux』を参照してください。

[コンテンツの更新間隔（Content Update Interval）] では、署名などの新しい ClamAV コンテンツがコネクタでチェックされる頻度を指定できます。更新間隔が長いほど、ClamAV 更新によるネットワーク トラフィックが減少します。逆に更新間隔が短いほど、大量の帯域幅が消費される可能性があり、大規模展開にはお勧めできません。[コンピュータの管理（Computer Management）] ページで、コンピュータの ClamAV 定義のバージョンと更新ステータスを確認できます。

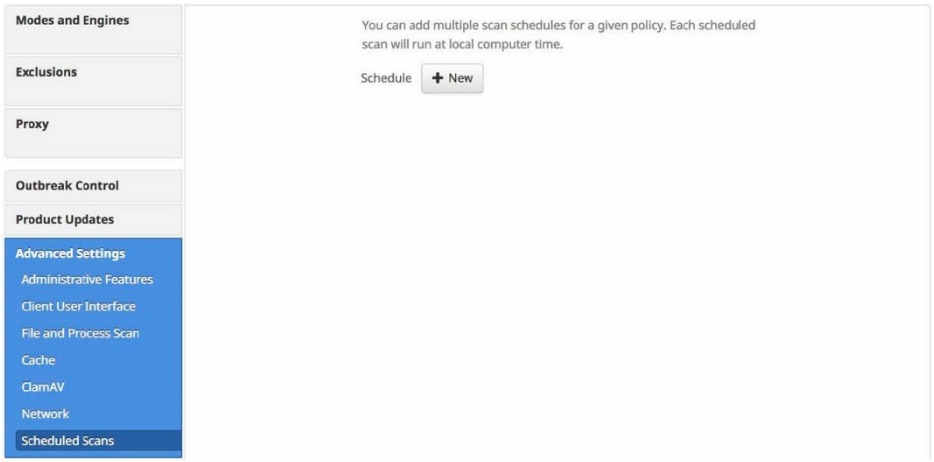
## ネットワーク




[ネットワーク（Network）] タブには、デバイス フロー コリレーション設定など、コネクタのネットワークフロー機能に関する設定が含まれています。[デバイス フロー コリレーションの無効化（Disable Device Flow Correlation）] を選択するか、または [監査（Audit）] を選択してネットワーク接続をログに記録できます。

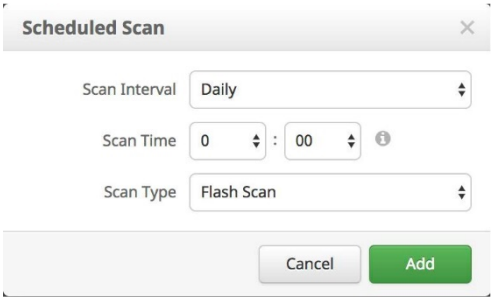
[ブロックリストのデータソース（Blocked List Data Source）] を選択すると、コネクタが使用する IP ブロックリストを選択できます。[カスタム（Custom）] を選択すると、ポリシーに追加した IP ブロックリストのみコネクタで使用されます。悪意のあるサイトを定義するために、コネクタに Cisco Intelligence Feed だけを使用させる場合は、[シスコ（Cisco）] を選択します。Cisco Intelligence Feed は、Talos によって評価が低いと判断された IP アドレスを表示します。このリスト内のすべての IP アドレスが 24 時間ごとにフラッシュされます。Talos がアドレスに関連した不正な動作を続けて観察した場合は、それがリストに追加されます。[カスタムとシスコ（Custom and Cisco）] オプションを使用すると、ポリシーに追加した IP ブロックリストと Cisco Intelligence Feed の両方を使用できます。

## 定期スキャン



ファイルは、コピー、移動、および実行時に確認されるため、コネクタの処理に対して定期スキャンを実行する必要ありません。ファイルは、レトロスペクティブ機能を使用して 7 日後に再度確認されます。これにより、会社は、スケジュールされたスキャンの必要性を排除して、エネルギー フットプリントを削減できます。ただし、会社によっては、ポリシーのために定期スキャンが必要な場合があります。そのため、このスキャンは必要に応じてポリシー経由で有効にできるようになっています。

[スケジュール（Schedule）] の下にある [+新規（+New）] をクリックすると、スキャン間隔、スキャン時間、およびスキャンタイプを選択できるオーバーレイが表示されます。




[スキャン間隔（Scan Interval）] では、実行頻度を設定できます。オプションは [毎週（Weekly）] または [毎月（Monthly）] です。

[スキャン時間（Scan Time）] では、スキャンの開始時刻を設定できます。

[スキャンタイプ（Scan Type）] では、スキャンのタイプを設定できます。[フラッシュ（Flash）] スキャンでは、実行中のプロセスとプロセスで使用されているファイルとレジストリエントリがスキャンされます。[フル（Full）] スキャンでは、実行中のプロセス、レジストリエントリ、およびディスク上のすべてのファイルがスキャンされます。このスキャンは、大量のリソースを必要とするため、定期的に実行しないようにしてください。[カスタム（Custom）] スキャンでは、指定した特定のパスがスキャンされます。

# Cisco Secure Endpoint Android コネクタのポリシー

ここでは、Cisco Secure Endpoint Android コネクタに使用可能なポリシーのオプションについて説明します。

## Android コネクタ：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しい Cisco Secure Endpoint Android ポリシーが表示されます。これらのページの設定については以下で説明します。Cisco Secure Endpoint Android コネクタのポリシーには、デバイスの特性に基づくいくつかのオプションが含まれています。

### 名前（Name）と説明（Description）

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

## Android コネクタ：その他のポリシー設定

[名前（Name）] と [説明（Description）] の入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページと [詳細設定（Advanced Settings）] にアクセスできるようになります。以降の項で設定について説明します。

### 感染管理


カスタム検出：Android リストタイプについては、このマニュアルの「アウトブレイクコントロール」の項を参照してください。

### 詳細設定（Advanced Settings）


[ハートビート間隔（Heartbeat Interval）] は、コネクタがホームを呼び出して、取得するポリシー、新しいカスタム検出、または実行するタスク（製品の更新など）の有無を確認するための間隔です。

# ネットワークポリシー

ネットワークポリシーは、Cisco Defense Center が Cisco Secure Endpoint と統合されている場合に [アプリケーション（Applications）] の下に表示されます。Cisco Defense Center と Cisco Secure Endpoint の統合の詳細については、Cisco Defense Center のマニュアルを参照してください。

## ネットワークポリシー：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しい Cisco Secure Endpoint ネットワークポリシーが表示されます。これらのページの設定については以下で説明します。Cisco Secure Endpoint ネットワークのポリシーには、デバイスの特性に基づくいくつかのオプションが含まれています。

#### 名前と説明

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

### ネットワークポリシー：その他のポリシー設定

[名前（Name）] と [説明（Description）] の入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページにアクセスできるようになります。次の項で設定について説明します。

#### 感染管理

カスタム検出については、このユーザーガイドの「アウトブレイクコントロール」の項を参照してください。許可リストについては、「アプリケーション制御：許可されたアプリケーション」の項を参照してください。

## Cisco Secure Endpoint iOS Connector のポリシー

ここでは、Cisco Secure Endpoint iOS Connector with Clarity に使用可能なポリシーのオプションについて説明します。

### iOS コネクタ：必要なポリシー設定

[新しいポリシー（New Policy）] をクリックすると、新しい Cisco Secure Endpoint iOS ポリシーが表示されます。これらのページの設定については以下で説明します。Cisco Secure Endpoint iOS Connector のポリシーには、デバイスの特性に基づいたいくつかのオプションが含まれています。コネクタの設定の多くは、Mobile Device Manager（MDM）を介して処理されます。

#### 名前（Name）と説明（Description）

[名前（Name）] ボックスでは、ポリシーの識別に使用可能な名前を作成できます。オプションの [説明（Description）] ボックスにポリシーに関する詳細を追加できます。

### モードとエンジン

このページには、ネットワーク判定モードに関する設定が含まれています。


#### 判定モード

判定モードでは、不審なネットワークアクティビティに対する Cisco Secure Endpoint iOS Connector の Clarity モジュールの対応方法を指定します。使用可能なモードは次の 3 つです。

- [アクティブブロック（Active Block）] では、接続を許可する前に、トラフィックの宛先が悪意のあるアドレスやブロックリストにあるアドレスでないことがチェックされます。これにより最高レベルのセキュリティが提供されますが、ネットワーク接続ごとにレイテンシも発生します。

  **重要：**アクティブブロックモードの接続でも、デバイスがシスコのクラウドに到達して宛先アドレスの判定結果を確認できない場合は、最終的に接続が許可されます。

- [ブロック（Block）] では、ネットワーク接続が許可されますが、同時に宛先が悪意のあるアドレスやブロックリストにあるアドレスであるかチェックされます。初期接続は許可されますが、悪意のあるサイトやブロックリストにあるサイトへのその後の接続はすべてブロックされます。
- [監査（Audit）] では、すべての接続が許可されますが、悪意のあるサイトやブロックリストにあるサイトへの接続はログに記録されます。

## iOS コネクタ：その他のポリシー設定

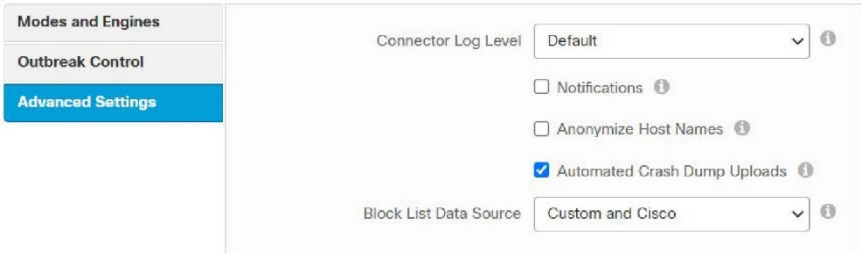
必須の設定ページへの入力が完了すると、[アウトブレイクコントロール（Outbreak Control）] ページと [詳細設定（Advanced Settings）] ページにアクセスできます。次の項で設定について説明します。

### 感染管理

使用可能な IP 許可リストまたはブロックリストがある場合は、[リストの選択（Select Lists）] をクリックするとポリシーに追加するリストを選択できます。ドロップダウン

メニューで、追加するすべてのリストのチェックボックスをオンにします。単一のポリシーに複数の IP リストを追加できますが、IP 許可リストエントリが IP ブロックリストエントリをオーバーライドします。これらのリストの作成方法の詳細については、「ネットワーク：IP ブロック/許可リスト」を参照してください。

## 詳細設定




[コネクタログレベル（Connector Log Level）] を使用すると、デフォルトのログレベルとデバッグ（詳細）ログレベルを選択できます。現時点では、デフォルト ログのみ使用できます。

[通知（Notifications）] は、悪意のある接続やその他のイベントに関する通知をエンドユーザーのデバイスで表示します。

[ホスト名の匿名化（Anonymize Host Names）] を選択すると、匿名化した名前がデバイスに割り当てられ、Cisco Cloud に送信される個人情報がすべて削除されます。

[クラッシュダンプの自動アップロード（Automated Crash Dump Uploads）] を選択すると、分析のためにコネクタのクラッシュダンプファイルをシスコに自動的にアップロードするかどうかを選択できます。

[ブロックリストのデータソース（Blocked List Data Source）] を選択すると、コネクタが使用する IP ブロックリストを選択できます。[カスタム（Custom）] を選択すると、ポリシーに追加した IP ブロックリストのみコネクタで使用されます。悪意のあるサイトを定義するために、コネクタに Cisco Intelligence Feed だけを使用させる場合は、[シスコ（Cisco）] を選択します。Cisco Intelligence Feed は、Talos によって評価が低いと判断された IP アドレスを表示します。このリスト内のすべての IP アドレスが 24 時間ごとにフラッシュされます。Talos がアドレスに関連した不正な動作を続けて観察した場合は、それがリストに追加されます。[カスタムとシスコ（Custom and Cisco）] オプションを使用すると、ポリシーに追加した IP ブロックリストと Cisco Intelligence Feed の両方を使用できます。

# 第 6 章

# グループ

グループを使用すれば、組織内のコンピュータをその機能や場所（または管理者によって定義された他の基準）に従って管理できます。新しいグループを作成するには、[グループを作成（Create Group）] をクリックします。既存のグループを編集したり、削除したりすることもできます。[すべての変更を表示（View All Changes）] を使用して監査ログのフィルタ処理されたビューを表示し、グループに加えられたすべての変更を表示するか、特定のグループで [変更の表示（View Changes）] をクリックして、そのグループに加えられた変更のみを表示します。

## グループの設定

ここでは、グループを作成し、設定するための手順を説明します。新しいグループの作成と、既存のグループの編集は、同じ手順で行います。

### 名前と説明

グループの名前と説明はその識別にのみ使用されます。グループの多くは、地理的位置、事業単位、ユーザー グループなどを反映することができます。グループはそれぞれに適用されるポリシーに基づいて定義する必要があります。

## [親グループ（Parent Group）] メニュー

[親グループ（Parent Group）] メニューを使用すると、作成しているグループの親グループを設定できます。これが特定の Cisco Secure Endpoint 展開で作成された最初のグループである場合、使用可能な唯一のオプションは親グループなし（空白のエントリ）または [デフォルトグループ（Default Group）] です。

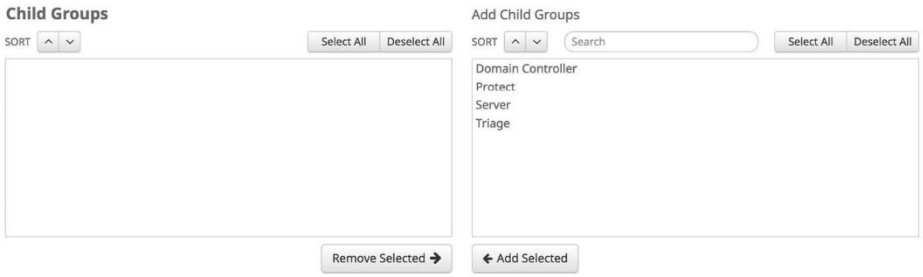
## [ポリシー（Policy）] メニュー

[ポリシー（Policy）] メニューを使用すると、作成しているグループに適用されるポリシーを指定できます。親グループが選択されていない場合、デフォルトポリシーが新しいグループに適用されます。親グループが選択されている場合、新しいグループは親のポリシーを継承します。

**重要：**親グループが後で変更された場合は、そのグループが新しい親グループのポリシーを継承します。親グループが削除された場合は、すべての子グループがデフォルトグループに移動され、そのポリシーを継承します。

## 子グループ

個々のグループ、複数のグループ、またはすべてのグループを選択し、子グループとして追加または削除できます。




**重要：**親からのポリシーを継承する子グループを削除する場合、そのグループのポリシーは、グループを新しい親グループに割り当てるまで、組織のデフォルトポリシーに戻ります。

## コンピュータの追加と移動

コンピュータを新規グループに割り当てるには、[保存（Save）] をクリックし、[管理（Management）] > [コンピュータ（Computers）] に移動してコンピュータを追加または移動します。詳細については、「コンピュータの管理」を参照してください。

**重要事項：**Cisco Secure Endpoint コンソールからは新しいグループに iOS デバイスを移動できません。単一のデバイスを移動するには、Meraki ダッシュボードを使用して、リンクされたグループがあるプロファイルにデバイスを再度タグ付けする必要があります。デバイスを新しいプロファイルに再度展開することもできます。その他の MDM で Cisco Secure Endpoint iOS Connector をアンインストールし、新しいグループのために再度インストールする必要があります。

# 第 7 章

# コネクタの導入

ポリシーを作成してグループに割り当てたら、コネクタを組織内のコンピュータとデバイスに展開できます。[管理（Management）] > [コネクタのダウンロード（Download Connector ）] に移動して、コネクタを Windows、Mac、Linux、または Android に展開します。Cisco Secure Endpoint iOS Connector を展開するには、[管理（Management）] > [Clarity for iOSの展開（Deploy Clarity for iOS）] に移動します。

## コネクタのダウンロード

[コネクタのダウンロード（Download Connector）] ページでは、各コネクタタイプのインストーラパッケージをダウンロードしたり、グループを選択した後にダウンロードできる URL をコピーしたりできます。インストーラ パッケージはネットワーク共有に配置することも、管理ソフトウェアを介して配布することもできます。ダウンロード URL をリモート ユーザーに電子メールで送信して、リモート ユーザーが自分でダウンロードしてインストールできるようにすると便利な場合があります。

### Secure Endpoint Windows コネクタ

Cisco Secure Endpoint Windows コネクタを展開するには、最初にドロップダウンメニューからグループを選択します。選択したポリシーでの指定に従い、または組織のデフォルトとしてダウンロードされるコネクタのバージョンを確認でき、ダウンロードしているコネクタのバージョンに更新する必要があるグループ内のコネクタを確認できます。最新バージョンのコネクタに更新した場合に再起動が必要となるコンピュータの台数も表示されます。

インストールプロセス中にコネクタでフラッシュスキャンを実行するかどうかを選択します。フラッシュ スキャンは、メモリ内で実行中のプロセスをチェックします。スキャンはインストールごとに実行する必要があります。

デフォルトでは、再頒布可能なインストーラがダウンロードされます。これは、32 ビットと 64 ビットの両インストーラを含む 46 MB のファイルです。複数のコンピュータにコネクタをインストールするには、このファイルをネットワーク共有先に保存するか、System Center Configuration Manager などのツールを使用してグループ内のすべてのコンピュータにプッシュします。インストーラには、インストール用の設定ファイルとして使用される policy.xml ファイルが含まれます。

**重要：**Microsoft System Center Configuration Manager（SCCM）を使用してコネクタを Windows XP コンピュータに導入する場合は、追加の手順を実行する必要があります。Cisco Secure Endpoint Windows コネクタインストーラを右クリックして、コンテキストメニューから [プロパティ（Properties）] を選択します。[環境（Environment）] タブで、[ユーザーがこのプログラムとやり取りできるようにする（Allow users to interact with this program）] ボックスをオンにして、[OK] をクリックします。

Cisco Secure Endpoint Windows コネクタをインストールするための小さなブートストラッパファイル（900 KB 以下）もダウンロードできます。この実行ファイルにより、適切なバージョンの Cisco Secure Endpoint Windows コネクタがダウンロードされてインストールされます。ブートストラッパはメイン インストーラから取得する必要があるため、プロキシを通じた場合は機能しません。その場合は再配布可能インストーラを使用する必要があります。

**重要：**Windows XP および Windows Server 2003 の場合、接続を考慮して Cisco Secure Endpoint Windows コネクタを cisco.com のアドレスに移行しているとブートストラッパは機能しません。これらのオペレーティング システムのバージョンの再頒布可能なインストーラをダウンロードする必要があります。

## Secure Client

Cisco XDR または SecureX との統合を有効にしている場合は、Cisco Secure Client のフルインストーラをダウンロードできます。Secure Client を使用すると、1 つのパッケージから Cisco Secure Endpoint Windows コネクタと Secure Client VPN を展開できます。Cisco XDR または SecureX でまだ設定されていないグループを選択した場合、Secure Client のインストーラには、デフォルトのクラウド管理の設定を含む Cisco Secure Endpoint コネクタのみ含まれます。後で、Cisco XDR または SecureX コンソールに移動して、追加の設定を行い、AnyConnect VPN モジュールを追加できます。Secure Client の設定の詳細については、https://docs.xdr.security.cisco.com/Content/Client-Management/client- management.htm または https://securex.us.security.cisco.com/help/insights/topic/secure-client を参照してください。

## Cisco Secure Endpoint Mac コネクタ

Cisco Secure Endpoint Mac コネクタを展開するには、最初にドロップダウンメニューからグループを選択し、インストールプロセス中にコネクタでフラッシュスキャンを実行するかどうかを選択します。フラッシュ スキャンは、現在メモリ内で実行中のプロセスをチェックします。インストールごとに実行する必要があります。

次に PKG または DMG ファイルをダウンロードして、Cisco Secure Endpoint Mac コネクタをインストールするか、ダウンロードリンクをコピーします。インストーラはネットワーク共有に配置できます。ファイルには、インストール用の設定ファイルとして使用される policy.xml ファイルも含まれています。

## Cisco Secure Endpoint Linux コネクタ

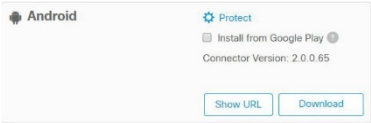
Cisco Secure Endpoint Linux コネクタを展開するには、最初にドロップダウンメニューからグループを選択し、インストールプロセス中にコネクタでフラッシュスキャンを実行するかどうかを選択します。フラッシュ スキャンは、現在メモリ内で実行中のプロセスをチェックします。インストールごとに実行する必要があります。

[ディストリビューション（Distribution）] プルダウンを使用して、使用しているディストリビューションに適したコネクタのバージョンを選択します。サポートされているディストリビューションについては、『Cisco Secure Endpoint Linux Connector OS Compatibility』を参照してください。

次に rpm または deb ファイルをダウンロードして、Cisco Secure Endpoint Linux コネクタをインストールするか、ダウンロードリンクをコピーします。インストーラはネットワーク共有に配置できます。ファイルには、インストール用の設定ファイルとして使用される policy.xml ファイルが含まれています。ダウンロード ページにリンクされた GPG Public Key をコピー、またはダウンロードする必要があります。これは、ポリシーによる Linux コネクタ：製品の更新に必要です。

## Cisco Secure Endpoint Android コネクタ

Cisco Secure Endpoint Android コネクタは、Cisco Secure Endpoint コンソールからアプリケーションをダウンロードするか、アプリケーションのダウンロードリンクを電子メールで送信するか、または Google Play ストアを使用して展開できます。




[コネクタのダウンロード（Download Connector）] ページでグループを選択します。[URLを表示（Show URL）] をクリックして、ユーザーに電子メールで送信できる APK へのリンクをコピーするか、[ダウンロード（Download）] をクリックして APK をダウンロードし、Mobile Device Manager（MDM）を介して配布できます。

ユーザー自身がアプリケーションをダウンロードしてインストールする場合は、[Google Playからのインストール（Install from Google Play）] をオンにします。[アクティベーションURLの表示（Show Activation URL）] をクリックして、ユーザーに電子メールで送信されるアクティベーションリンクを表示します。このリンクは、EMM API を使用し管理対象の設定を介して展開する場合、`amp_provisioning_url` 値にも使用されます。ポリシーを受信してコネクタを有効にするには、Cisco Secure Endpoint Android コネクタがインストールされているデバイスからアクティベーションリンクをクリックする必要があります。Google Play を介してアプリをインストールしたユーザーは、Google Play ストアアプリの**アプリ自動更新**設定に応じてコネクタの更新を受信します。

**重要：**ユーザーがデバイスのアクティベーションリンクをクリックせずに Google Play からインストールした場合、Cisco Secure Endpoint Android コネクタのポリシーはなく、デバイスは保護されません。

## 管理対象の設定

任意の Mobile Device Manager（MDM）または Enterprise Mobility Manager（EMM）を介して管理対象の設定で Cisco Secure Endpoint Android コネクタを展開することもできます。

管理対象設定スキーマはアプリケーション内に組み込まれており、Google EMM API を使用して取得できます。

### コネクタのブートストラップ

コネクタをブートストラップするには、EMM を使用して、[コネクタのダウンロード（Download Connector）] ページにあるアクティベーション URL を `amp_provisioning_url` の文字列として指定する必要があります。この値が存在する場合、コネクタは、追加のクラウド接続のために指定されたポリシーを Cisco Cloud から取得します。EMM API を介して値を指定しない場合は、他の方法でプロビジョニング URL をユーザーに提供することもできます。

### デバイス名のプロビジョニング

コネクタのデバイス名を `amp_device_name` の文字列として指定してプロビジョニングすることもできます。この文字列は 3 ～ 63 文字で指定する必要があり、Cisco Secure Endpoint コンソールに表示されるデバイスの名前になります。このフィールドはオプションです。指定しない場合、ユーザーは登録時にデバイス名を入力するように求められます。

# Clarity for iOS の展開

Cisco Secure Endpoint iOS Connector と Clarity の展開手順は、使用している Mobile Device Manager（MDM）によって異なります。Cisco Secure Endpoint iOS Connector を展開する前に、MDM の統合を設定する必要があります。

## Meraki を介した展開

[管理（Management）] > [Clarity for iOS の展開（Deploy Clarity for iOS）] に移動して、Meraki の導入環境に変更を加えます。Cisco Secure Endpoint グループを Meraki SM プロファイルに適用できます。各プロファイルには 1 つのグループとその関連付けられているポリシーのみ適用できます。

1. 適用する Cisco Secure Endpoint の [グループ（Group）] を選択するか、または Meraki SM を更新します。
2. Meraki SM から適用先の [組織（Organization）] を選択します。
3. 組織内の [ネットワーク（Network）] を選択します。
4. Clarity を適用する 1 つ以上の [プロファイル（Profiles）] を選択します。プロファイルの作成の詳細については、構成プロファイル [英語] を参照してください。

> **重要：** 1 台の iOS デバイスに複数のプロファイルを展開できますが、Clarity が適用されている複数のプロファイルを展開しようとするとエラーが発生し、2 番目のプロファイルは適用されません。Clarity だけが適用されている 2 番目のプロファイルは、Cisco Umbrella だけが適用されている既存プロファイルがあるデバイスには問題なく展開できます。

5. [更新（Update）] をクリックして展開します。

Cisco Secure Endpoint iOS Connector を展開したら、Cisco Meraki ダッシュボードを使用し、Apple の Volume Purchase Program（VPP）とシステムマネージャの使用 [英語] の手順に従いアプリをデバイスに展開する必要があります。

通知を設定する場合、次の手順に従います。

1. [システムマネージャ（System Manager）] > [設定（Settings）] に移動します。
2. [プロファイルを追加（Add Profile）] をクリックします。
3. [デバイスプロファイル（デフォルト）（Device profile (default)）] を選択し、[続行（Continue）] をクリックします。
4. プロファイルの名前と説明を入力します。
5. 適切な [対象範囲（Target Scope）] および [デバイスタグ（Device Tags）] を選択します。
6. [設定の追加（Add Settings）] をクリックします。

7. 検索バーで「Notification」を検索します。
8. [iOSアプリの通知（iOS App Notifications）] をクリックします。
9. [アプリ（App）] ドロップダウンメニューで、[Cisco Security Connector（com.cisco.ciscosecurity.app）] を選択します。

   チェックボックスをすべてオンにして、[アラートタイプ（Alert type）] に [バナー（Banner）] を選択します。
10. [保存（Save）] をクリックします。

## Workspace ONE を介した展開

Workspace ONE から展開するには、まず Cisco Secure Endpoint コンソールから Mobileconfig ファイルをダウンロードする必要があります。

1. [管理（Management）] > [Clarity for iOS の展開（Deploy Clarity for iOS）] に移動します。
2. iOS ポリシーに事前に割り当てている Cisco Secure Endpoint の[グループ（Group）] を選択します。
3. [クリップボードにコピー（Copy to Clipboard）] をクリックします。

**重要事項：**ドメインを Cisco Cloud への送信対象から除外するには、「Clarity ドメインの除外」のステップ 2 と 3 で Workspace ONE について確認してから続行してください。

この段階で、Workspace ONE ダッシュボードから Mobileconfig ファイルを追加する必要があります。

1. [デバイス（Devices）] > [プロファイルとリソース（Profiles & Resources）] > [プロファイル（Profiles）] に移動します。
2. [追加（Add）] > [プロファイルの追加（Add Profile）] をクリックします。
3. [iOS] をクリックします。
4. [全般（General）] の下で以下の手順を実行します。
   - [名前（Name）] と [説明（Description）] を割り当てます。
   - [展開（Deployment）] を [管理型（Managed）] に設定します。
   - [割り当てタイプ（Assignment Type）] を [自動（Auto）] に設定します。
   - [削除の許可（Allow Removal）] を [常時（Always）] に設定します。
   - 以前作成したグループを [割り当てグループ（Assigned Groups）] に追加します。
5. クリップボードの内容を [カスタム設定（Custom Settings）] テキスト ボックスに貼り付けます。
6. [通知（Notifications）] をクリックします。
7. [設定（Configure）] をクリックします。

8. [アプリの選択（Select App）] をクリックします。
9. [アプリの選択（Select App）] フィールドで、[Cisco Security Connector（com.cisco.ciscosecurity.app）] を選択します。
10. チェックボックスをすべてオンにして、[解除時のアラートスタイル（Alert Style when unlocked）] に [バナー（Banner）] を選択します。
11. [保存（Save）] をクリックします。
12. [保存してパブリッシュ（Save & Publish）] をクリックします。
13. [デバイス割り当ての表示（View Device Assignment）] の下に、[グループ（Group）] に含まれているデバイスが表示されます。
14. [パブリッシュ（Publish）] をクリックします。

**重要：**通知を設定しない場合は、手順 6 ~ 11 をスキップします。

## MobileIron を介した展開

MobileIron から展開するには、まず Cisco Secure Endpoint コンソールから Mobileconfig ファイルをダウンロードする必要があります。

1. [管理（Management）] > [Clarity for iOS の展開（Deploy Clarity for iOS）] に移動します。
2. iOS ポリシーに事前に割り当てている Cisco Secure Endpoint の[グループ（Group）] を選択します。
3. [MobileIronプロファイルのダウンロード（Download MobileIron Profile）] をクリックします。

**重要事項：**ドメインを Cisco Cloud への送信対象から除外するには、「Clarity ドメインの除外」のステップ 2 と 3 で MobileIron について確認してから続行してください。

この段階で、MobileIron ダッシュボードから Mobileconfig ファイルを追加する必要があります。

1. [ポリシーと構成（Policies & Configs）] > [構成（Configurations）] に移動します。
2. [新規追加（Add New）] > [iOS と OS X（iOS and OS X）] > [構成プロファイル（Configuration Profile）] をクリックします。
   - 構成プロファイルに [名前（Name）] と [説明（Description）] を割り当てます。
   - [参照（Browse）] をクリックして、Cisco Secure Endpoint コンソールからダウンロードした Mobileconfig ファイルに移動します。
   - [保存（Save）] をクリックします。
3. 作成したばかりの構成プロファイルを選択します。

4. [アクション（Actions）] > [ラベルに適用（Apply to Labels）] をクリックします。
   - 事前に作成したラベルを選択します。
   - [適用（Apply）] をクリックします。
5. ダイアログで [OK] をクリックします。

通知を設定する場合、次の手順に従います。

1. [ポリシーと構成（Policies & Configs）] > [構成（Configurations）] に移動します。
2. [新規追加（Add New）] > [iOS と OS X（iOS and OS X）] > [構成プロファイル（Configuration Profile）] をクリックします。
   - 構成プロファイルに [名前（Name）] と [説明（Description）] を割り当てます。
   - [追加+（Add+）] をクリックします。
   - [バンドル識別子（Bundle Identifier）] で [Cisco Security Connector（com.cisco.ciscosecurity.app）] を選択します。
   - チェックボックスをすべてオンにして、[アラートタイプ（Alert Type）] に [バナー（Banner）] を選択します。
   - [保存（Save）] をクリックします。

### 他の MDM を介した展開

1. [管理（Management）] > [Clarity for iOS の展開（Deploy Clarity for iOS）] に移動します。
2. iOS ポリシーに事前に割り当てている Cisco Secure Endpoint の**[グループ（Group）]** を選択します。[プロファイルのダウンロード（Download Profile）] をクリックします。

これで、MDM のコンソールから MDM に Mobileconfig ファイルをアップロードして、導入を完了することができます。

## 設置概要

[展開の概要（Deployment Summary）] ページには、コネクタの成功したインストールと失敗したインストールのほかに、現在進行中のインストールも表示されます。

コンピュータの名前、IP アドレス、MAC アドレス、およびインストール試行日時に加えて、オペレーティングシステムとコネクタのバージョンを確認できます。完全に失敗した可能性があるインストールとその原因が表示される場合もあれば、インストール開始後のクラウドとの通信が表示されない場合もあります。

# コンピュータの管理

コネクタを展開すると、[コンピュータ（Computers）] 画面にインストール対象のエンドポイントが表示されます。[コンピュータ（Computers）] 画面には、[管理（Management）] > [コンピュータ（Computers）] からアクセスできます。コンピュータのリストには、コネクタがインストールされているすべてのエンドポイントが表示されます。ページの上部には、AV やコネクタの更新が必要なコンピュータの数、障害が発生して注意が必要なコンピュータの数など、コンピュータに関するいくつかの重要な指標のサマリーが表示されます。[すべての変更を表示（View All Changes）] を使用すると、監査ログのフィルタ処理されたビューが表示され、コンピュータに加えたすべての変更が表示されます。リストにフィルタを適用することも、ページを移動してより多くのコンピュータを表示することもできます。チェックボックスからすべてのコンピュータを選択するか、特定のコンピュータを選択して、選択したコンピュータを別のグループや新規グループに移動・削除できます。コネクタの GUID、ホスト名、オペレーティングシステム、コネクタのバージョン、グループ、コネクタのインストール日、前回の検出日、定義の更新ステータスを含むコンピュータのリストのダウンロードリンクが記載された電子メールを受信するには、コンピュータを 1 つ以上選択して、[CSVにエクスポート（Export to CSV）] をクリックします。

**重要事項：**エクスポートされた CSV ファイルの日時は、タイムゾーンの設定に関係なくすべて UTC 表示です。

特定のコンピュータの詳細を展開するには、リストでそのコンピュータをクリックします。現在のページですべてのコンピュータに関する詳細を展開したり、折りたたんだりするには、[+] または [-] ボタンをクリックします。詳細画面からは、コンピュータが属している [グループ（Groups）] を変更したり、コンピュータに適用されている [ポリシー（Policies）] やその他の関連情報を確認したりできます。また、Orbital クエリを起動したり、フォレンジック スナップショットを取得したりできます。リモートアンインストールを使用すると、個々のエンドポイントからコネクタをアンインストールできます。

[前回の検出時間（Last Seen Time）] は約 15 分間隔で更新されます。このリストからコンピュータを削除したり、リスト内のコンピュータにフラグを設定したり、フラグを解除したりすることもできます。[変更の表示（View Changes）] を使用すると、監査ログのフィルタ処理されたビューが表示され、特定のコンピュータに加えたすべての変更が表示されます。

**重要：**前回の検出時間をクリックすると詳細が表示されます。時間を ISO-8601 形式の日付および UNIX 形式のタイムスタンプでクリップボードにコピーするオプション、およびタイムゾーンを変更するためのリンクを示すポップアップも合わせて表示されます。

**重要：**コンピュータを削除しても、[コンピュータ管理（Computer Management）] ページのリストから削除されるだけです。コンピュータからコネクタをアンインストールしない限り、削除したコンピュータによって生成されたイベントが表示され続け、利用可能なライセンスが 1 つ使用されたままとなります。

[スキャン（Scan）] をクリックするとダイアログが表示され、ファイルスキャンまたは IOC スキャンを選択して、フルスキャンまたはフラッシュスキャンを実行できます。

**警告：**エンドポイント IOC のフル スキャンは時間がかかるうえ、大量のリソースが消費されます。大量のファイルが存在するエンドポイントでフル スキャンを実行すると数日かかる場合があります。フル スキャンは、夜間や週末などの営業時間外にのみスケジュール設定してください。コネクタで初めてフルスキャンを実行する際には、システムがカタログ化されるため、通常のフルスキャンよりも時間がかかります。

## Kenna リスクスコア

Kenna リスクスコアは、0 ~ 100 のスケールで表されます。技術的な重大度と、実際の攻撃者が実際に脆弱性をどのように利用しているかを調べることで、脆弱性のリスクを定量化します。このスコアを計算する際には、脆弱性の兵器化を予測する予測モデリング、記録されたエクスプロイトまたはエクスプロイトキットの可用性、ほぼリアルタイムのエクスプロイトの存在など、さまざまな脆弱性および脅威の変数が考慮されます。

Cisco Secure Endpoint 内の脆弱性を評価およびスコアリングするために、Kenna Inference は、環境で実行されているソフトウェア（つまり、OS ベンダー、名前、バージョンなど）を NIST の National Vulnerability Database（NVD）およびその他のナレッジベースにマッピングして、関連する CVE を特定します。Kenna の主要な脆弱性管理プラットフォームの基礎となる同じデータサイエンスベースのアルゴリズムと脆弱性インテリジェンスを使用して、これらの CVE ごとに一意の Kenna リスクスコアが計算されます。Kenna リスクスコアが 33 以上の CVE は、検証のために分析されます。

コンピュータのリストを Kenna リスクスコアでフィルタリングし、スコアの昇順または降順でリストを並べ替えることができます。

リスクスコアをクリックすると、コンピュータに関連付けられている CVE のリストが表示されます。各 CVE には次が含まれます。

- Kenna リスクスコア
- 共通脆弱性評価システム（CVSS）2 スコア
- CVE の説明
- 脆弱性の影響を受けるプロパティ

脆弱性に対する修正が存在する場合、[利用可能な修正（Fix Available）] ボタンにより、修正へのリンクのリストが表示されます。

**重要：**Windows 10 IoT Enterprise で動作しているコンピュータは、現時点ではサポートされていません。

## フィルタの保存と管理

後で使用するために、フィルタを保存しておき、すばやく呼び出すことができます。フィルタを保存するには、フィルタパラメータを選択してから、[適用して保存（Apply and Save）] をクリックします。表示される [フィルタの保存（Save Filter）] ダイアログボックスでフィルタの名前を入力して、[保存（Save）] をクリックします。

保存されているフィルタは、[コンピュータ（Computers）] ページのドロップダウンリストから選択することによって適用できます。[更新（Update）] をクリックして、現在のフィルタへの変更を保存します。

フィルタのインターフェイスの左上にあるフィルタの名前をクリックして、現在のフィルタの名前を変更できます。[削除（Delete）] をクリックすることで、フィルタを削除することもできます。

## コンピュータの管理：コネクタの診断

[受信トレイ（Inbox）] タブ、デバイストラジェクトリ、または [コンピュータの管理（Computer Management）] ページの展開されたコンピュータの詳細ビューで、[診断...（Diagnose...）] ボタンをクリックすると、コンピュータの診断をリモートでトリガーできます。この機能はコネクタが正しく動作していないと判断した場合に使用でき、診断ファイルをサポートチケットに添付したり、独自の分析を実行したりできます。

この機能を使用して診断をリモートで収集するために、コンピュータに必要なコネクタの最小バージョンは以下のとおりです。

- Windows：6.2.1
- Mac：1.9.0
- Linux：1.9.0
- iOS：1.2.0

**重要：**診断は以前のバージョンのコネクタから引き続きローカルで収集できます。

これにより、ファイルリポジトリからダウンロードして表示できるデバッグログを含む診断ファイルが生成されます。

**重要事項：**この機能はファイルリポジトリにアクセスする必要があるため、コネクタの診断をトリガーする場合は、アカウントで二要素認証が有効になっており、ファイルリポジトリからファイルを取得する権限がある必要があります（「ユーザーは、[マイアカウント（My Account）] をクリックすることで、このページで自分のアカウント設定にアクセスできます」を参照）。）

デバッグセッションの長さは、ドロップダウンメニューから選択できます。また、診断オプションも選択できます。

**重要：**使用可能なオプションは、デバイスのオペレーティングシステムによって異なります。

Windows コンピュータの [履歴データ（Historical Data）] チェックボックスをオンにすると、要求前に存在していたログファイルが収集されます。Linux および Mac コンピュータでこのオプションを有効にすると、デバッグセッション中のログローテーションを防止できます。

Windows コンピュータの [カーネルログ（Kernel Log）] チェックボックスをオンにすると、カーネルドライバから生成された追加のログファイルが収集されます。Linux および Mac コンピュータでは、このオプションを有効にすると、カーネルモジュールの詳細なログが有効になります。

[キャッシュデータベースを含める（Include cache database）] チェックボックスをオンにすると、iOS デバイスが Web サービス要求からデータを収集します。

[Umbrellaのログを含める（Include Umbrella Logs）] チェックボックスをオンにすると、iOS デバイスがすべての Umbrella コンポーネントのログを収集します。

目的のオプションを選択したら、[作成（Create）] をクリックします。お知らせを電子メールで受信することを選択した場合（「ユーザー」を参照）、診断ファイルがファイルリポジトリからダウンロード可能になった時点で電子メールが届きます。

**重要：**診断ファイルの生成には最大 24 時間かかります。

診断ファイルにアクセスするには、[診断（Diagnostics）] をクリックし、コネクタの診断でフィルタ処理されている [ファイルリポジトリ（File Repository）] ページに直接移動します。

## コンピュータの管理：Cisco Secure Endpoint iOS Connector

詳細を表示するには、iOS デバイスの名前をクリックします。

詳細情報からクリックして、コネクタと関連付けられているすべての [イベント（Events）]、[デバイストラジェクトリ（Device Trajectory）]、およびそのデバイスの [監査ログ（Audit Log）] を確認できます。デバイスを削除することもできます。iOS デバイスは Cisco Secure Endpoint コンソールを使用して移動できないため、[移動（Move）] ボタンは無効化されています。単一のデバイスを移動するには、Meraki ダッシュボードを使用して、リンクされたグループがあるプロファイルにデバイスを再度タグ付けする必要があります。デバイスを新しいプロファイルに再度展開することもできます。

[変更の表示（View Changes）] を使用すると、監査ログのフィルタ処理されたビューが表示され、特定のコンピュータに加えたすべての変更が表示されます。[イベント（Events）] リンクをクリックして、選択したコンピュータのフィルタ処理された [イベント（Events）] タブビューを開くこともできます。

**重要事項：**Cisco Secure Endpoint コンソールからは新しいグループに iOS デバイスを移動できません。単一のデバイスを移動するには、Meraki ダッシュボードを使用して、リンクされたグループがあるプロファイルにデバイスを再度タグ付けする必要があります。デバイスを新しいプロファイルに再度展開することもできます。その他の MDM で Cisco Secure Endpoint iOS をアンインストールし、新しいグループのために再度インストールする必要があります。

# 第 8 章

# SECURE ENDPOINT WINDOWS コネクタ

グループ、ポリシー、および展開戦略を定義したら、Cisco Secure Endpoint Windows コネクタをエンドポイントにインストールできます。ここでは、手動インストールプロセスを確認しながら、コネクタ ユーザー インターフェイスの主な機能について説明します。コネクタの機能については、「コネクタのエンジンと機能」を参照してください。

## Windows システム要件

以下は、デスクトップコンピュータおよびサーバー用の Cisco Secure Endpoint Windows コネクタの最小システム要件です。Cisco Secure Endpoint Windows コネクタは、x86 プロセッサのオペレーティングシステムの 64 ビットバージョンをサポートしています。特定のコネクタ機能を有効にする場合に、追加のディスク容量が必要になることがあります。これらは Cisco Secure Endpoint Windows コネクタの要件であり、Windows のシステム要件は考慮していません。

- 2 GB のメモリ
- 650 MB の使用可能なハード ディスク領域：クラウド専用モード
- 1 GB のハードディスク空き領域（TETRA）
- CPU の推奨事項については、Microsoft の推奨要件を参照してください。

オペレーティングシステムの互換性については、Cisco Secure Endpoint Windows コネクタ OS の互換性 [英語] を参照してください。

# 互換性のない Windows ソフトウェアおよび構成

Secure Endpoint Windows コネクタは現在、次のソフトウェアとの互換性がありません。

- Check Point の ZoneAlarm
- Carbon Black（コネクタバージョン 6.3.5 以前とのみ互換性なし）
- Res Software AppGuard

Cisco Secure Endpoint Windows コネクタは現在、次のプロキシ設定をサポートしていません。

- Websense NTLM クレデンシャル キャッシュ。Secure Endpoint で現在サポートされている回避策は、Websense の NTLM クレデンシャルキャッシングを無効にするか、コネクタで認証例外を使用したプロキシ認証のバイパスを許可するかのどちらかです。
- HTTPS コンテンツ インスペクション。現在サポートされている回避策は、HTTPS コンテンツインスペクションを無効にするか、コネクタに対する除外項目を設定するかのどちらかです。
- Kerberos/GSSAPI 認証。現在サポートされている回避策は、基本認証と NTLM 認証のどちらかを使用することです。

Malicious Activity Protection エンジンは、Hyper-V クラスタと互換性がありません。

Cisco Secure Endpoint Windows コネクタは、Windows 10 IoT Enterprise では次の設定をサポートしていません。

- HORM および UWF はサポートされていません。
- Kenna リスクスコアは使用できません。

コネクタ UI から起動されたルートキットスキャンは、デスクトップまたはファイル仮想化ソフトウェアと互換性がありません。

# Windows コネクタファイアウォールの例外

Cisco Secure Endpoint Windows コネクタを適切に動作させるためのファイアウォールの例外については、「コネクタファイアウォールの例外」を参照してください。

# Windows プロキシ自動検出

コネクタは、複数のメカニズムを使用して匿名プロキシサーバーをサポートできます。特定のプロキシサーバーやプロキシ自動設定（PAC）ファイルへのパスはポリシーで定義することも、Windows レジストリからエンドポイントプロキシ設定をコネクタが検出することもできます。

コネクタは、エンドポイントのプロキシ設定を自動的に検出するように設定できます。コネクタは、プロキシ設定情報を検出すると、Cisco Secure Endpoint 管理サーバーに接続にして、プロキシサーバーの設定が正しいことを確認しようとします。

コネクタは、ポリシーで指定されているプロキシ設定を最初に使用します。Cisco Secure Endpoint 管理サーバーとの接続を確立できない場合、コネクタは、エンドポイント上の Windows レジストリからプロキシ設定を取得しようとします。コネクタは、ユーザー単位の設定ではなく、システム全体の設定からのみ設定を取得しようとします。

Windows レジストリからプロキシ設定を取得できない場合、コネクタはプロキシ自動設定（PAC）ファイルを検索します。この動作は、ポリシー設定で指定することも、または Web プロキシ自動検出プロトコル（WPAD）を使用して決定することもできます。PAC ファイルの場所がポリシーで指定されている場合は、http または https で始まる必要があります。サポートされている PAC ファイルは ECMAScript ベースのみであり、..pac ファイル拡張子を付ける必要があることに注意してください。PAC ファイルが Web サーバー上でホストされている場合は、適切な MIME タイプ（application/x-javascript-config）を指定する必要があります。コネクタの通信はすべて暗号化されるため、HTTPS プロキシはサポートされません。コネクタのバージョン 3.0.6 では、SOCKS プロキシ設定は PAC ファイルを使用して指定できません。

クラウドルックアップに一定回数失敗すると、コネクタはプロキシ設定の再検出を試みるため、ラップトップがエンタープライズ ネットワークの外部にある場合に、ネットワークプロキシ設定が変更されてもコネクタの接続が確保されます。

# Windows インストーラ

インストーラは、インタラクティブモードで、または一連のコマンドラインパラメータを使用して実行できます。

**重要：**環境内で他のセキュリティ製品を実行している場合、Cisco Secure Endpoint コネクタのインストーラが脅威として検出される可能性があります。コネクタを正常にインストールするには、他のセキュリティ製品で許可リストに追加するか、対象から除外してから再度実行してください。

## Windows インタラクティブ インストーラ

ブートストラッパを使用してインストールする場合（ダウンロードしたファイルとして、または電子メール経由で）、管理者が Windows インストーラのコマンドラインスイッチを使用してサイレントインストールを実行し、オプションを指定していない限り、エンドポイントでの対話操作が必要になります。

Windows User Access Control（UAC）が有効になっている場合はプロンプトが表示されるので、[はい（Yes）] を選択して続行する必要があります。

ブートストラッパを使用してインストールする場合は、この時点で、ダウンロードマネージャがインストーラパッケージの適切なバージョンを取得します。再配布可能インストーラが使用されている場合は、この手順が省略されます。

1. インストール場所のダイアログが表示されます。ほとんどの場合、デフォルトの場所が最適な選択肢です。コネクタのエンドユーザーライセンス契約およびプライバシーポリシーへのリンクも表示されます。[インストール（Install）] をクリックして続行します。
2. インストールが完了したら、[次へ（Next）] をクリックして次に進みます。
3. チェックボックスをオンのままにすると、デスクトップにコネクタのアイコンが作成されます。[閉じる（Close）] ボタンをクリックしてインストールを終了します。

   インストール時にフラッシュスキャンを実行するオプションが選択されていた場合は、スキャンが実行されます。コネクタに適用されたポリシーで [クラウド通知（Cloud Notifications）] が選択されている場合、Cisco Cloud に接続されていることが Windows のシステムトレイアイコンに示されます。
4. スキャンが完了したら、[閉じる（Close）] をクリックしてすべてのインストール手順を終了します。これで、コネクタがエンドポイント上で実行されます。

## Windows インストーラのコマンドラインスイッチ

独自の展開ソフトウェアを使用している管理者は、コマンド ライン スイッチを使用して展開を自動化できます。使用可能なスイッチのリストを以下に示します。

- /R：5.1.13 以降の全バージョンのコネクタでは、最初にこのスイッチを使用する必要があります。
- /S：インストーラをサイレント モードに切り替える場合に使用します。

  **重要事項：**これは、最初のパラメータ（または /R の直後のパラメータ）として指定する必要があります。
- /desktopicon 0：コネクタ用のデスクトップアイコンが作成されません。
- /desktopicon 1：コネクタ用のデスクトップアイコンが作成されます。
- /startmenu 0：[Start Menu] ショートカットが作成されません。
- /startmenu 1：スタート メニューのショートカットが作成されます。
- /contextmenu 0：右クリックのコンテキスト メニューから [即時スキャン（Scan Now）] が無効になります。
- /contextmenu 1：右クリックのコンテキスト メニューから [即時スキャン（Scan Now）] が有効になります。
- /remove 0：コネクタはアンインストールされますが、後で再インストールできるようにファイルは残されます。

- /remove 1：コネクタがアンインストールされ、すべての関連ファイルが削除されます。
- /uninstallpassword（コネクタの保護パスワード）：ポリシーで [コネクタ保護（Connector Protection）] を有効にした場合にコネクタをアンインストールできます。このスイッチと共に [コネクタ保護（Connector Protection）] のパスワードを提供する必要があります。
- /skipdfc 1：デバイス フロー コリレーション ドライバのインストールをスキップします。

**重要事項：**このフラグを使用してインストールされたコネクタは、[モードとエンジン（Modes and Engines）] > [ネットワーク（Network）] が [無効（Disabled）] に設定されているポリシーを使用するグループに含める必要があります。

- /skiptetra 1：TETRA ドライバのインストールをスキップします。

**重要事項：**このフラグを使用してインストールされたコネクタは、[モードとエンジン（Modes and Engines）] > [TETRA] がオフに設定されているポリシーを使用するグループに含める必要があります。

- /D=[PATH]：インストール先ディレクトリを指定するために使用します。たとえば、/D=C:\tmp は C:\tmp にインストールします。

**重要事項：**これは、最後のパラメータとして指定する必要があります。

- /overridepolicy 1：以前のコネクタのインストール環境にインストールする場合に、既存の policy.xml ファイルを置き換えます。
- /overridepolicy 0：以前のコネクタのインストール環境にインストールする場合に、既存の policy.xml ファイルを置き換えません。

**重要事項：**あるグループから別のグループにコンピュータを移動するのに /overridepolicy スイッチを使用しないでください。代わりに、Cisco Secure Endpoint コンソールを使用してください。詳細については、「コンピュータの追加と移動」を参照してください。
異なるグループにコンピュータがあり、ポリシー設定をオーバーライドせずにすべてのコンピュータを新しいコネクタのバージョンにアップグレードする必要がある場合は、デフォルト以外の値「/overridepolicy 0」を指定して /overridepolicy を使用します。

- /temppath：コネクタのインストール時に作成される一時ファイルのパスを指定します。たとえば、/temppath C:\somepath\temporaryfolder のように指定します。このスイッチは、Secure Endpoint Windows コネクタ 5.0 以降でのみ使用できます。

  **重要：**コネクタの登録と起動をスキップする以下のスイッチは、展開可能なゴールデンイメージとして Windows のオペレーティングイメージを作成するときに使用します。

- /goldenimage 1：インストール時のコネクタの初期登録と起動をスキップします。
- /goldenimage 0：インストール時のコネクタの初期登録と起動をスキップしません。

**重要：**Cisco Secure Endpoint Windows コネクタバージョン 6.3.1 以降では、一重引用符（'）を含むパス引数（/temppath、/D switches など）を含むインストーラスイッチを使用している場合、パス全体を二重引用符（"）で囲む必要があります。そうしないと、インストーラによって引数が誤って解析され、予期しない場所にコネクタがインストールされます。

どのスイッチも指定せずにコマンド ライン インストーラを実行することと、/desktopicon 0 /startmenu 1 /contextmenu 1 /skipdfc 0 /skiptetra 0 /overridepolicy 1 は等価です。

Secure Endpoint Windows コネクタ 5.1.3 以降には、5.1.1 より前のバージョンから 5.1.3 以降にアップグレードする場合に、インストールディレクトリを「Sourcefire」から「Cisco」に移行することをオプトイン（またはオプトアウト）できるコマンドラインスイッチがあります。その方法を次に示します。

- /renameinstalldir 1 は、インストールディレクトリを Sourcefire から Cisco に変更します。
- /renameinstalldir 0 は、インストールディレクトリを変更しません。

  **重要事項：**デフォルトでは、/renameinstalldir 1 が使用されます。

Secure Endpoint Windows コネクタ 6.0.5 以降には、Microsoft Security Advisory 3033929 の確認をスキップするためのコマンドラインスイッチがあります。

- /skipexprevprereqcheck 1：Microsoft Windows KB3033929 の確認をスキップします。
- /skipexprevprereqcheck 0：Microsoft Windows KB3033929 を確認します（デフォルト）。

**重要事項：**このスイッチを使用しても、この KB、または Windows 7 および Windows Server 2008 R2 の SHA-2 コード署名サポートを有効にする Windows の更新がインストールされていない場合は、Cisco Cloud への接続に問題が発生します。

Secure Endpoint Windows コネクタ 6.0.7 以降は、Windows セキュリティ更新プログラム KB 4072699 の受信に必要なレジストリキーを設定するためのコマンドラインスイッチを備えています。

- /kb4072699 1：レジストリ キーの値を設定します。
- /kb4072699 0：レジストリ キーの値を設定しません（デフォルト）。

**重要事項：**レジストリ キーの値は、このコマンド ライン スイッチを使用してのみ設定できます。このスイッチを使用するか、あるいは手動でこのキーを設定しない場合、パッチは受信されません。『Cisco Secure Endpoint Compatibility with Windows Security Update KB4056892』で互換性のあるバージョンの一覧を参照してください。

Cisco Secure Endpoint Windows コネクタ 7.0.5 以降では、後続のバージョンへのアップグレードを完了するための再起動は必要ありません。ただし、これが予期せず発生する場合があるため、インストーラでは、アップグレードを続行して完了する（ただし再起動が必要）か、アップグレードを中断してすべてを以前の状態/バージョンにロールバックするかを選択できます。

- /overrideupgradefailure 0：アップグレードで再起動しないと続行できない問題が発生した場合、すべての変更がロールバックされ、アップグレード失敗イベントが送信されます。
- /overrideupgradefailure 1：アップグレードで再起動しないと続行できない問題が発生した場合、アップグレードは続行されます。アップグレードを完了するには再起動が必要です。

## Windows インストーラ終了コード

インストーラの終了コードと説明については、このテクニカルノートを参照してください。

## Cisco Security モニタリングサービス

バージョン 6.3.1 未満の Cisco Secure Endpoint Windows コネクタでは、TETRA エンジンが有効で定義が最新の場合、Windows Security Center（WSC）への登録はコネクタによって実行されます。正常に登録されると、Windows Defender が無効になり、Secure Endpoint がアクティブなウイルスおよび脅威保護プロバイダーとして指定されます。

Cisco Secure Endpoint Windows コネクタ 6.3.1 以降では、Cisco Security モニタリングサービスによって WSC への登録が実行されます。アンチマルウェア保護プロセスライト（AM-PPL）サービスとして、WSC と通信し、TETRA のステータスに従って Windows Defender を有効化または無効化できるようになります。

**重要：**Windows Server バージョン 2016 以降では、Windows Defender を自動的に無効化できません。これらのオペレーティングシステムで TETRA を実行する場合は、Windows Defender を手動で無効にする必要があります。

# Windows コネクタ ユーザー インターフェイス

コネクタをインストールしたら、デスクトップショートカットをダブルクリックするか、Windows のスタートメニューで Cisco Secure Client エントリをクリックか、Windows のトレイから起動することでコネクタにアクセスできます。

ユーザーインターフェイスは、エンドポイントで最大 8 人の同時ユーザーをサポートします（コネクタバージョン 8.1.3 以降）。9 人目の同時ユーザーがクライアント ユーザー インターフェイスを開こうとすると、起動はしますが無効と表示されます。コネクタは引き続き実行され、すべてのユーザーに保護が提供されます。

コネクタのメイン画面で、スキャンの起動やコネクタの設定の表示を選択できます。ネットワークへの接続状況やサービスの停止状況、最後のスキャン実行日時、およびコネクタに現在適用されているポリシーを示すコネクタのステータスも表示されます。これらのエントリは、コネクタの問題の診断に役立つことがあります。このログファイルは `%Program Files%\Cisco\AMP\[version number]\sfc.exe.log` にあります。

## スキャン

プルダウンからスキャンタイプを選択し、[開始（Start）] をクリックすると、スキャンが開始されます。

使用可能なスキャン オプションは次のとおりです。

[フラッシュスキャン（Flash Scan）]：システム レジストリと実行中のプロセスをスキャンして、悪意のあるファイルの兆候を検索します。このスキャンはクラウドベースのため、ネットワーク接続が必要です。フラッシュ スキャンは実行が比較的高速です。

[カスタムスキャン（Custom Scan）]：スキャンする特定のファイルやディレクトリを定義できます。[カスタムスキャン（Custom Scan）] を選択すると、スキャン対象を指定するためのダイアログが開きます。

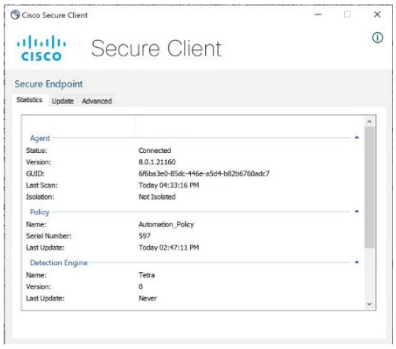
[フルスキャン（Full Scan）]：接続されたすべてのストレージデバイス（USB デバイスなど）を含む、コンピュータ全体をスキャンします。このスキャンは、時間がかかり、大量のリソースが消費されるため、コネクタの初回インストール時のみ実行してください。

[ルートキットスキャン（Rootkit Scan）]：コンピュータをスキャンしてインストールされたルートキットの兆候を検索します。ルートキット スキャンを実行するには [ポリシー（Policy）] で TETRA を有効にする必要があります。有効にしなかった場合は、[ルートキットスキャン（Rootkit Scan）] ボタンが非表示になります。

**重要：**ルートキットスキャンは、デスクトップまたはファイル仮想化ソフトウェアと互換性がありません。

## 設定

歯車アイコンをクリックすると、[統計（Statistics）]、[更新（Update）]、および [詳細（Advanced）] タブに分かれた設定画面が表示されます。[診断（Diagnostics）] ボタンは、コネクタに関する問題のトラブルシューティングの一環として、サポートから要請があった場合にのみ使用してください。




[統計（Statistics）] タブには、ポリシー名/シリアル番号、TETRA エンジン情報、プロキシ設定といったコネクタに関する情報が表示されます。これは、トラブルシューティングやサポートセッションに役立ちます。

[更新（Update）] タブでは、ポリシー、ソフトウェア、および検出エンジンのシグネチャの更新を確認したり、それらをインストールすることができます。

[詳細（Advanced）] タブでは、デバッグロギングを開始し、イベント履歴を確認することができます。デバッグロギングは、システムリソースを消費する可能性があるため、コネクタに関する問題のトラブルシューティングの一環として、サポートから要請があった場合にのみ使用してください。[イベント履歴（Event History）] ボタンをクリックすると、Windows のイベントビューアが起動し、コネクタによって生成された情報イベントとエラーイベントが表示されます。これには、マルウェア検出イベントおよび検疫イベントが含まれます。

**重要：** Secure Client がインストールされている場合は、AnyConnect VPN モジュールに関する情報も [設定（Settings）] に表示されます。

## Windows コネクタ コマンド ライン インターフェイス

コネクタの機能は、コマンド ライン インターフェイスからも使用および管理できます。実行ファイルは `<install path>\<version>\sfc.exe` にあります。インストールパスはインストール中に指定したパスで、バージョンはコネクタのバージョン番号です。たとえば、コネクタのバージョン 8.0.1 のデフォルトパスは次のようになります。

```
%Program Files%\Cisco\AMP\8.0.1.21160\sfc.exe
```

**重要：**コマンド ライン インターフェイスを使用する場合は、フルパスを指定する必要があります。

便利なコマンドは次のとおりです。

- `sfc.exe -s`：コネクタサービスを起動します。
- `sfc.exe -k <password>` ：コネクタサービスを停止します。<password> はコネクタ保護のパスワードです。
- `sfc.exe -l start`：ローカルデバッグロギングを開始します。デバッグロギングは、サービスを再起動したりコンピュータを再起動すると停止します。
- `sfc.exe -l stop`：ローカルデバッグロギングを停止します。
- `sfc.exe -forceUpdate`：製品と定義の更新を確認します。

**重要：**コネクタの CLI コマンドを実行するには、管理者権限が必要です。

# Windows コネクタサポートツール

Cisco Secure Endpoint Windows コネクタには、コネクタの問題のトラブルシューティングに役立つツールが含まれています。

## Windows サポート向け診断ツール

サポート向け診断ツールは、Windows のスタートメニューの [Cisco AMP for Endpointsコネクタ（Cisco AMP for Endpoints Connector）] フォルダにあります。サポート向け診断を実行すると、スナップショットが作成され、CiscoAMP_Support_Tool_[datetime].zip としてデスクトップに保存されます。ここで、[datetime] はツールの実行日時です。このツールは、シスコサポートから依頼された場合のみ実行する必要があります。

## Windows 時間指定診断ツール

時間指定診断ツールは、Windows のスタートメニューの [Cisco AMP for Endpointsコネクタ（Cisco AMP for Endpoints Connector）] フォルダにあります。時間指定診断を実行すると、30 分間のアクティビティがログに記録され、CiscoAMP_Support_Tool_[datetime].zip としてデスクトップに保存されます。ここで、[datetime] はツールの実行日時です。このツールは、シスコサポートから依頼された場合のみ実行する必要があります。

## Windows 接続テストツール

いずれかのコネクタから Cisco Cloud へのアクセスに問題が発生している場合は、接続テストツールを使用してトラブルシューティングを支援できます。接続テストツールは、Cisco Secure Endpoint Windows コネクタのバージョン 5.1.1 以降で使用できます。

[管理者として実行（Run as administrator）] を使用してコマンドプロンプトを開き、ツールのインストールフォルダに移動します。ツールは、次の場所にあります。

```
%ProgramFiles%\Cisco\AMP\[Version]\ConnectivityTool.exe
```

ここで、[version] はコネクタのバージョン番号（5.1.1 など）です。/? スイッチを指定してこのツールを実行すると、コマンド ライン スイッチとその機能いついてのリストが表示されます。

以下のスイッチがあります。

| | |
|---|---|
| /D | クラッシュ ダンプ テスト ファイルを Cisco Cloud にアップロードします。 |
| /F [policynum] | ポリシーをダウンロードします。[policynum] に値を指定すると、ポリシー番号が有効であれば、ツールによってこのポリシーがダウンロードされます。スイッチとポリシー番号の間にはスペースを含める必要があります。 |
| /H | HTTP アップロードテストを実行して、ファイルレジストリに対する通信を検証します。 |
| /I | イベントを受け取るサーバーで接続テストを実行します。 |
| /HC | 登録サーバーで接続テストを実行します。 |
| /UH | 更新サーバーで接続テストを実行します。ポリシーを介して更新が設定されている場合にのみ機能します。 |
| /R | リモートファイル取得サーバーで接続テストを実行します。 |
| /O | Orbital サーバーで接続テストを実行します。組織で Orbital が有効になっている場合にのみ使用できます。 |
| /BPD | 動作保護サーバーテストと XML 接続テストを実行します。 |
| /BPU | 動作保護アップロードテストを実行します。 |

スイッチを指定しないでツールを実行すると、すべてのスイッチが有効になった状態で実行されます。ツールを実行するたびに、ログ ファイルが ConnectivityTool.exe.log というファイル名で同じディレクトリに作成されます。

## Windows コネクタのアンインストール

ライセンスを再利用するには、コネクタをアンインストールして、別のエンドポイントで使用できるようにする必要があります。エンドポイントからコネクタをアンインストールするには、次の手順を実行します。

1. [コントロールパネル（Control Panel）] に移動します。
2. [プログラム（Programs）] で、[プログラムのアンインストール（Uninstall a program）] を選択します。
3. プログラムリストで [Cisco Secure Endpoint] を選択し、[アンインストールと変更（Uninstall/Change）] をクリックします。
4. ダイアログボックスで [アンインストール（Uninstall）] ボタンをクリックして、アプリケーションを削除します。
5. コネクタをアンインストールするためのパスワード要件がポリシーで設定されている場合は、入力するように求められます。
6. アンインストール プロセスが完了したら、[閉じる（Close）] ボタンをクリックします。

最後に、すべてのコネクタの履歴と検疫ファイルの削除を確認するプロンプトが表示されます。アンインストールプロセスを完了するには、プロンプトが表示されたときにコンピュータを再起動します。コネクタバージョン 7.0.5 以降をアンインストールする際には、ほとんどの場合、コンピュータを再起動する必要はありません。

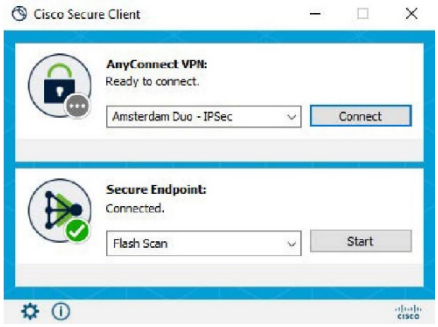
**重要：**Windows 8 以降では、[高速スタートアップ（Fast Startup）] モードが有効になっており、再起動を要求するプロンプトが表示される場合、アンインストールが完了したら Windows のシャットダウンオプションを使用せずにコンピュータを再起動する必要があります。再起動することで、コネクタのドライバを削除する最終クリーンナップ手順を正常に終了できます。

## Cisco Secure Client

Cisco Secure Client を使用すると、クラウド管理モジュールによって管理される単一のパッケージとして Cisco Secure Endpoint Windows コネクタおよび Secure Client VPN をエンドポイントに展開できます。

Secure Client を使用するには、 Cisco XDR または SecureX との統合を有効にする必要があります。統合がアクティブ化されると、Cisco Secure Endpoint コンソールの [コネクタのダウンロード（Download Connector）] ページ、あるいは Cisco XDR または SecureX コンソールから Secure Client の完全なインストーラをダウンロードできます。Secure Client の追加の設定と AnyConnect VPN モジュールの追加の詳細については、https://docs.xdr.security.cisco.com/Content/Client-Management/client- management.htm または https://securex.us.security.cisco.com/help/insights/topic/secure-client を参照してください。

**重要事項：**Cisco XDR または SecureX で Secure Client を有効にすると、Cisco Secure Endpoint 組織で読み取り/書き込み API ログイン情報が作成されるため、インストールトークンを作成できます。




Secure Client のユーザーインターフェイスは、AnyConnect VPN モジュールの設定が追加された Windows コネクタ ユーザー インターフェイスと同じです。

ユーザーインターフェイスの Cisco Secure Endpoint 部分は、エンドポイントで最大 8 人の同時ユーザーをサポートします（コネクタバージョン 8.1.3 以降）。9 人目の同時ユーザーがクライアント ユーザー インターフェイスを開こうとすると、起動はしますが無効と表示されます。コネクタは引き続き実行され、すべてのユーザーに保護が提供されます。他の Secure Client モジュールのユーザーインターフェイスは、現在、同時ユーザーをサポートしていません。

## Secure Client インストーラのコマンドラインスイッチ

独自の展開ソフトウェアを使用している管理者は、コマンド ライン スイッチを使用して展開を自動化できます。使用可能なスイッチのリストを以下に示します。

- -c または --cleanup：終了時の一時ディレクトリの削除を有効にします。インストールが成功した場合でも一時ディレクトリを保持するには、-c=false を使用します。デフォルトは -c=true です。
- -d または --debug：デバッグ出力を有効にします。
- -la：実行するインストールアクションのリストを表示します。
- -ls：埋め込みファイルのリストを表示します。
- -lsjson：埋め込みファイルのリストを表示します（JSON 出力）。
- -q または --quiet：インストーラをサイレントで実行します。このオプションは、無効の（または古い）ディスプレイドライバを搭載しているコンピュータに Secure Client をインストールする場合にも使用する必要があります。
- -v または --verbose：詳細出力を有効にします。

# 第 9 章

# Cisco Secure Endpoint Mac コネクタ

グループ、ポリシー、および展開戦略を定義したら、コネクタをエンドポイントにインストールできます。ここでは、手動インストールプロセスを確認しながら、コネクタユーザー インターフェイスの主な機能について説明します。コネクタの機能については、「コネクタのエンジンと機能」を参照してください。

## MacOS システム要件

Secure Endpoint Mac コネクタの最小システム要件は次のとおりです。これらは Cisco Secure Endpoint Mac コネクタの要件であり、Mac のシステム要件は考慮していません。

- 1 GB のメモリ
- 1 GB のハード ディスク空き領域

オペレーティングシステムの互換性については、Cisco Secure Endpoint Mac コネクタ OS の互換性 [英語] を参照してください。

## 互換性のない macOS ソフトウェアおよび構成

Secure Endpoint Mac コネクタは現在、次のプロキシ設定をサポートしていません。

- Websense NTLM クレデンシャルキャッシュ：Secure Endpoint で現在サポートされている回避策は、Websense で NTLM クレデンシャルキャッシュを無効にするか、コネクタに認証除外を使用したプロキシ認証の省略を許可することです。

- HTTPS コンテンツインスペクション：現在サポートされている回避策は、HTTPS コンテンツインスペクションを無効にするか、コネクタ用の除外をセットアップすることです。
- Kerberos/GSSAPI 認証：現在サポートされている回避策は、基本認証と NTLM 認証のどちらかを使用することです。

## Mac コネクタファイアウォールの例外

Cisco Secure Endpoint Mac コネクタを適切に動作させるためのファイアウォールの例外については、「コネクタファイアウォールの例外」を参照してください。

## Mac コネクタプロキシ自動検出

コネクタは、複数のメカニズムを使用して匿名プロキシサーバーをサポートできます。特定のプロキシサーバーをポリシーで定義することも、プロキシ自動設定（PAC）ファイルで定義されたエンドポイントプロキシ設定をコネクタが検出することもできます。PAC ファイルの場所（URL）は、macOS ネットワークアダプタ設定で指定されています。

ポリシーでプロキシタイプが自動プロキシ設定に指定され、有効な PAC ファイルへの URL を使用してエンドポイントで自動プロキシ設定が有効になっている場合、コネクタは、それらのエンドポイントプロキシ設定を自動的に検出できます。コネクタは、プロキシ設定情報を検出すると、Cisco Secure Endpoint 管理サーバーに接続にして、プロキシサーバーの設定が正しいことを確認しようとします。コネクタは、ユーザー単位の設定ではなく、システム全体の設定からのみ設定を取得しようとします。

サポートされている PAC ファイルは ECMAScript ベースのみであり、..pac ファイル拡張子を付ける必要があることに注意してください。PAC ファイルが Web サーバー上でホストされている場合は、適切な MIME タイプ（application/xjavascript-config）を指定する必要があります。コネクタのすべての通信はすでに暗号化されているため、HTTPS プロキシはサポートされていません。

30 分ごとに、またはクラウドルックアップが一定回数失敗すると、コネクタはプロキシ設定の再検出を試みるため、ラップトップがエンタープライズ ネットワークの外部にある場合に、ネットワークプロキシ設定が変更されてもコネクタの接続が確保されます。

詳細については、Cisco Secure Endpoint Mac プロキシ自動設定（PAC）セットアップガイド [英語] を参照してください。

## Cisco Secure Endpoint Mac コネクタのインストール

Cisco Secure Endpoint Mac コネクタは、次の 2 つの形式で配布されます。

- macOS インストールパッケージ（.pkg）
- Apple のディスクイメージ（.dmg）

- .pkg ファイルとして配布される Mac コネクタをインストールするには、ファイルをダブルクリックしてインストールプロセスを開始します。
- .dmg ファイルとして配布される Mac コネクタをインストールするには、ファイルをダブルクリックしてディスクイメージを開き、画面の指示に従います。

インストーラ コマンドを使用してターミナルから pkg ファイルをインストールすることもできます。詳細については、ターミナルから「`man installer`」と入力してください。

ソフトウェア ライセンス契約書を読んで、[続行（Continue）] をクリックします。[同意（Agree）] をクリックして契約書の条件に同意します。次に、ソフトウェア インストールの宛先ドライブを選択します。コネクタには、約 40 MB の空きディスク領域と署名ファイル用の約 50 MB が必要です。[続行（Continue）] をクリックして進みます。

インストールの場所を確認したら、[インストール（Install）] をクリックして開始します。先に進むためのパスワードの入力が要求されます。[終了（Finish）] をクリックして Cisco Secure Endpoint Mac コネクタのインストールを完了します。

**重要事項：**コネクタバージョン 1.10.0 以降、ファイルスキャン操作は非特権プロセスを使用して実行されます。コネクタのインストール中、`cisco-amp-scan-svc` という名前のユーザーとグループがシステムに作成されます。ユーザーまたはグループが既に存在していても設定が異なっている場合は、インストーラは、それらを削除後、必要な設定で再作成します。ユーザーおよびグループが必要な設定で作成できなかった場合、インストーラは失敗します。

**ヒント：**失敗したコネクタのインストールの詳細については、`/var/log/install.log` を確認してください。

**重要：**環境内で他のセキュリティ製品を実行している場合、Cisco Secure Endpoint コネクタのインストーラが脅威として検出される可能性があります。コネクタを正常にインストールするには、他のセキュリティ製品で許可リストに追加するか、対象から除外してから再度実行してください。

## 自動化による Cisco Secure Endpoint Mac コネクタのインストール

スクリプトまたはその他の自動化を使用してコネクタをインストールするには、次の手順のようなワークフローを使用します。

1. Cisco Secure Endpoint コンソールから amp_<groupname>.dmg をダウンロードします。
2. amp_<groupname>.dmg をエンドポイントにプッシュします。

3. .dmg ファイルをマウントします。
   ```
   $ hdiutil attach amp_<groupname>.dmg
   ```
4. Apple 社認証済みの Mac コネクタパッケージファイルを実行します。
   ```
   $ sudo installer -pkg /Volumes/ampmac_connector/
   amp_<groupname>.pkg -target /
   ```
5. .dmg ファイルのマウントを解除します。
   ```
   $ hdiutil detach /Volumes/amp_<groupname>
   ```

# Cisco Secure Endpoint Mac コネクタのインストール後にユーザー承認を付与する

Mac コネクタが正しく動作するには、次のユーザー承認が必要です。

- システム拡張機能（macOS 10.13 以降）
- フルディスクアクセス権（macOS 10.14 以降）

## システム拡張機能の承認

macOS 10.13 では、アプリケーションがシステム拡張機能を実行する前にユーザーの同意が必要になるという変更が導入されました。コネクタは、システム拡張機能を使用してファイルシステムとネットワークアクティビティを監視します。コネクタが起動し、承認が付与されていない場合、シスコが署名したシステム拡張機能がブロックされていることを示すメッセージが表示されます。画面の指示に従い、[システム設定（System Preferences）] の [セキュリティとプライバシー（Security and Privacy）] を開き、拡張機能を許可します。Cisco Secure Endpoint Mac コネクタ 1.14.0 では、macOS 10.15 以降で承認が必要な 2 つの新しいシステム拡張機能が追加されました。

### MDM を使用したシステム拡張の許可

システム機能拡張は、展開と管理のためのモバイルデバイス管理（MDM）プロファイルでカーネル拡張ポリシーペイロードを使用して自動的に承認できます。これにより、エンドユーザーはアクションをとる必要がなくなります。Cisco Secure Endpoint Mac コネクタ 1.14.0 以降の場合は、macOS 11（Big Sur）、macOS 10.15（Catalina）、および macOS10.14（Mojave）における Cisco Secure Endpoint Mac コネクタのアドバイザリ [英語] を参照してください。

**重要：**ユーザーは、デバイス登録プログラム（DEP）に含まれていない macOS 10.13.4 以降を実行している Mac で MDM プロファイルを受け入れる必要があります。

## フルディスクアクセス権の付与

macOS 10.14 では、アプリケーションが連絡先、カレンダー、写真、メール、メッセージなどのユーザーファイルにアクセスする前にユーザーの同意が必要になるという変更が導入されました。コネクタが macOS 10.14 以降上の該当ファイルにアクセスしてスキャンするには、フルディスクアクセス権が許可されている必要があります。

**Cisco Secure Endpoint Mac コネクタ 1.16.0 ~ 1.16.2 の場合**

1. [システム設定（System Preferences）] を起動します。
2. [セキュリティとプライバシー（Security and Privacy）] をクリックします。
3. [ロック（Lock）] をクリックして、変更を加えます。
4. macOS 10.14 では、左側のペインから [フルディスクアクセス権（Full Disk Access）] を選択し、次のいずれかを実行して「AMP for Endpoints Service」を追加します。
   - [+] ボタンをクリックし、ファイル選択ダイアログボックスで [/Applications/Cisco AMP for Endpoints/ AMP for Endpoints Service] を選択します。
   - Finder から [/Applications/Cisco AMP for Endpoints/AMP for Endpoints Service.app] を右側のペインにドラッグします。

   macOS 10.15 以降 では、左側のペインから [フルディスクアクセス権（Full Disk Access）] を選択します。実行中の Mac コネクタのバージョンに応じて、Mac コネクタのフルディスクアクセス権用の異なるプログラムが表示されます。リストに次の項目が表示されているかどうかを確認します。
   - ampdaemon
   - AMP for Endpoints サービス
   - AMP Security Extension

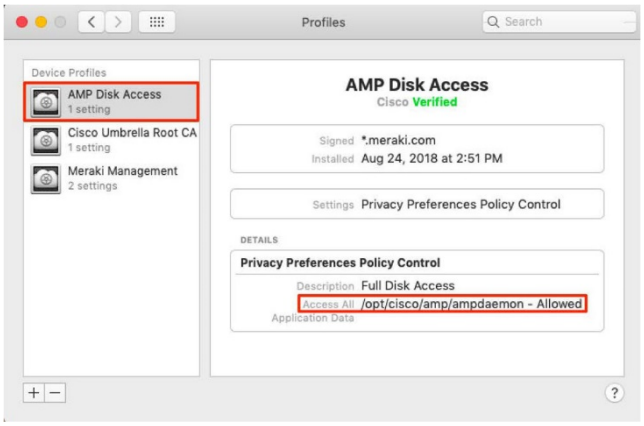
**Cisco Secure Endpoint Mac コネクタ 1.18.0 以降の場合**

1. [システム設定（System Preferences）] を起動します。
2. [セキュリティとプライバシー（Security and Privacy）] をクリックします。
3. [ロック（Lock）] をクリックして、変更を加えます。
4. 左側のペインから [フルディスクアクセス権（Full Disk Access）] を選択します。実行中の Mac コネクタのバージョンに応じて、Mac コネクタのフルディスクアクセス権用の異なるプログラムが表示されます。リストに次の項目が表示されているかどうかを確認します。
   - ampdaemon
   - Cisco Secure Endpoint サービス
   - Cisco Secure Endpoint ファイルモニター

### MDM を使用したフルディスクアクセス権の付与

展開および管理にモバイルデバイス管理（MDM）ソリューション（Cisco Meraki など）を使用しているお客様の場合は、MDM プロファイルの Privacy Preferences Policy Control Payload を使用してフルディスクアクセス権が付与されます。これにより、エンドユーザーはアクションをとる必要がなくなります。Cisco Secure Endpoint Mac コネクタ 1.14.0 以降の場合は、macOS 11（Big Sur）、macOS 10.15 （Catalina）、および macOS10.14（Mojave）における Cisco Secure Endpoint Mac コネクタのアドバイザリ [英語] を参照してください。

**重要：**ユーザーは、デバイス登録プログラム（DEP）に含まれていない macOS 10.13.4 以降を実行している Mac で MDM プロファイルを受け入れる必要があります。




Cisco Secure Endpoint の詳細は次のとおりです。

- 名称：Cisco Systems, Inc.（TDNYQP7VRK）
- チームの識別子：TDNYQP7VRK

Cisco Secure Endpoint Mac コネクタ 1.9.0 以降、保護パスへのアクセスが許可されていないエンドポイントから Cisco Secure Endpoint コンソールに表示されるイベントが送信されます。このイベントタイプを生成しているデバイスを確認することで、劣化状態で動作している可能性があるコネクタを判断できます。

## Cisco Secure Endpoint Mac コネクタの使用方法

Mac のメニューバーのアイコンの外観で、Mac コネクタのステータスを判断できます。

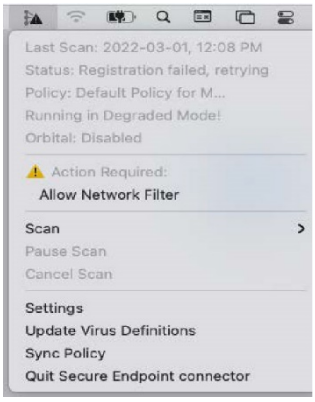
動作中：コネクタは Cisco Cloud に接続されていて、システムは保護されています。

アラート：コネクタにエラーが発生し、正しく動作していません。保護が無効になっているため、アクションが必要です。

オフライン：コネクタは Cisco Cloud から切断されています。保護はオフラインエンジンに限定されます。

スキャン中：スキャンが進行中です。

アイコンをクリックするとメニュレットが表示され、最後のスキャンの実行日時、現在のステータス、コネクタが使用しているポリシーなどの情報が表示されます。メニューレットからスキャンを開始、一時停止、およびキャンセルすることもできます。

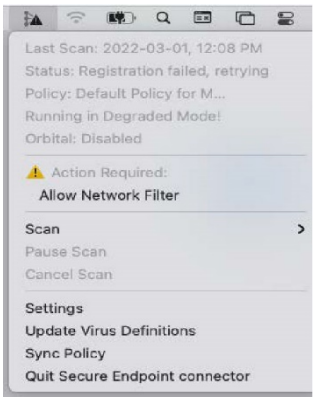



メニュレットには実行する必要があるアクションやコネクタのエラーも表示されます。

**重要事項：**Cisco Secure Endpoint Mac コネクタでは、グラフィカル ユーザー インターフェイスに加えてコマンド ライン インターフェイスがエンドポイントで使用されます。コネクタのコマンド ライン インターフェイスは `/opt/cisco/amp/ampcli` にあります。インタラクティブ モードで実行するか、または 1 つのコマンドを実行して終了できます。`./ampcli --help` を使用して、使用可能なオプションやコマンドの完全なリストを確認します。

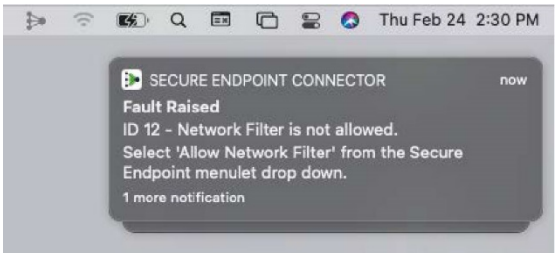
## 必要な処理

メニューバーのコネクタアイコンは、コネクタが作動状態に戻る上でアクションが必要な場合に点滅します。メニュレットで必要なアクションをクリックすると、アクションを実行するプロセスが画面に表示されます。




## Mac コネクタのエラー

コネクタの正常な動作に影響を与える状態が検出されると、コネクタから障害発生イベントが通知されることがあります。同様に、障害解消イベントは、その状況がもはや存在しないことを示しています。詳細については、この Cisco Secure Endpoint テクニカルノートを参照してください。




## 設定

[設定（Settings）] インターフェイスを使用すると、個別のユーザーが、特定のコネクタに適用されるポリシーの全側面をポリシー管理者がどのように設定しているのか確認できます。管理されたインストール環境では、設定内のすべてのエントリが読み取り専用であり、情報提供または診断の目的でのみ提供されます。

## 同期ポリシー

同期ポリシーは、コネクタで最新バージョンのポリシーが実行されているかチェックします。そうでない場合は、最新バージョンをダウンロードします。

### Mail.app

マルウェアを含む電子メールメッセージは、ローカルメールデータベースの破損を防ぐために Cisco Secure Endpoint Mac コネクタによって検疫されません。それでも、電子メール メッセージはスキャンされ、マルウェアに関する検出イベントが生成されるため、管理者は、悪意のある電子メールをメール サーバーから直接除外できますが、検疫失敗イベントも表示されます。Mail.app が自動的に添付ファイルをダウンロードするように設定されている場合は、すべての悪意のある添付ファイルが想定どおりに検疫されます。

### Mac コネクタの [無効（Disabled）] ステータス

コネクタのステータスが [無効（Disabled）] の場合は、サポートに連絡してください。

## Mac コネクタのアンイストール

Cisco Secure Endpoint Mac コネクタをアンインストールするには、インストールフォルダの [アプリケーション（Applications）] > [Cisco Secure Endpoint] に移動して、**Uninstall Secure Endpoint Connector.pkg** ファイルをダブルクリックします。アプリケーションをアンインストールするには、ウィザードの手順に従います。Orbital が有効になっている場合は、アンインストールプロセスの一部として自動的に削除されます。

アンインストーラでは `cisco-amp-scan-svc` ユーザーおよびグループは削除されないため、次の 2 つのコマンドを実行してユーザーおよびグループを削除します。

```
sudo dscl .-delete /Users/cisco-amp-scan-svc
sudo dscl . -delete /Groups/cisco-amp-scan-svc
```

何らかの理由でアンインストーラが正常に機能しない場合は、 Cisco Secure Endpoint Mac コネクタを手動で削除する必要があります。手動でのアンインストールについては、この TechZone の記事を参照してください。

# 第 10 章

# Cisco Secure Endpoint Linux コネクタ

グループ、ポリシー、および展開戦略を定義したら、コネクタをエンドポイントにインストールできます。ここでは、手動インストールプロセスを確認しながら、コネクタユーザー インターフェイスの主な機能について説明します。

## Linux システムの要件

Cisco Secure Endpoint Linux コネクタのシステム要件は次のとおりです。Secure Endpoint Linux コネクタは、x64 アーキテクチャのみをサポートします。これらは Cisco Secure Endpoint Linux コネクタの要件であり、Linux のシステム要件やその他のアプリケーションおよびサービスは考慮していません。

Linux 専用 ClamAV 定義の使用

| | 最小ハードウェア | 推奨 |
|---|---|---|
| コア | 2 | 4 以上 |
| メモリ | 1 GB | 2 GB |
| /opt の空きディスク容量 | 1 GB | 1 GB |

完全な ClamAV 定義の使用

| | 最小ハードウェア | 推奨 |
|---|---|---|
| コア | 2 | 4 以上 |
| メモリ | 3 GB | 4 GB |
| /opt の空きディスク容量 | 2 GB | 2 GB |

**重要：**コネクタによって、/opt/cisco/amp/ に一時ファイルがインストールされて保持されます。

オペレーティングシステムの互換性については、Cisco Secure Endpoint Linux コネクタに関する OS の互換性の確認 [英語] を参照してください。Debian ベースシステムの要件については、『Debian ベースのシステム上の Cisco Secure Endpoint Linux コネクタ』を参照してください。

**重要事項：**Secure Endpoint Linux コネクタは、カスタムカーネルやサポートされていないカーネルでは正しくインストールされない、または正しく動作しない場合があります。カスタムカーネルを使用している場合は、インストールする前にサポートまで連絡してください。サポートされていないカーネルを使用している場合、そのバージョン用のカーネルモジュールをビルドできる可能性があります。詳細については、『Building Cisco Secure Endpoint Linux Connector Kernel Modules』を参照してください。

# 互換性のない Linux ソフトウェアおよび構成

Secure Endpoint Linux コネクタは現在、次のソフトウェアとの互換性がありません。

- RHEL/CentOS 6.x 上の F-Secure Linux セキュリティ（CentOS 7.4 上の互換性については、「Linux コネクタファイアウォールの例外」を参照してください）。
- Kaspersky Endpoint Security
- McAfee VSE for Linux
- McAfee Endpoint Security for Linux
- RHEL/CentOS 6.x 上の Sophos Server Security 9 （CentOS 7.4 上の互換性については、「Linux コネクタファイアウォールの例外」を参照してください）。
- Symantec Endpoint Protection
- Trend Micro Deep Security Agent

Cisco Secure Endpoint Linux コネクタでは、CentOS および Red Hat Enterprise Linux バージョン 6.x で、リムーバブルメディアまたは一時ファイルシステムが標準以外の場所にマウントされていると、アンマウントに失敗する可能性があります。ファイル シス

テム階層標準に従って、USB ストレージ、DVD、および CD-ROM などのリムーバブル メディアは /media/ にマウントし、NFS ファイル システム マウントなどの一時マウント ファイル システムは /mnt/.にマウントする必要があります。リムーバブル メディアや一時ファイル システムを他のディレクトリにマウントすると、競合が生じて、デバイスがビジーなためにアンマウントに失敗する場合があります。アンマウント エラーが発生した場合、ユーザーは cisco-amp サービスを停止して、アンマウント操作を再試行し、cisco-amp を再起動する必要があります。

```
sudo initctl stop cisco-amp
sudo umount {dir\device}
sudo initctl start cisco-amp
```

Cisco Secure Endpoint Linux コネクタは、次のバージョンのオペレーティングシステムでの UEFI セキュアブートをサポートしていません。

- CentOS 6
- Red Hat Enterprise Linux 6
- CentOS 7
- Red Hat Enterprise Linux 7
- openSUSE Leap 15.1
- SUSE Linux Enterprise 15 SP 1
- Amazon Linux 2
- Oracle Linux 6
- Oracle Linux 7 RHCK

Secure Endpoint Linux コネクタが、Red Hat Enterprise Linux 7.x または CentOS 7.x へのロード時にカーネルモジュールを使用すると、そのカーネルは汚染されます。Cisco Secure Endpoint によるカーネル汚染の発生を一時的に回避するために、Cisco Secure Endpoint サービスを無効化でき、無効化すると、システムの再起動後にカーネルモジュールがロードされなくなります。Secure Endpoint サービスを無効化すると、システムに対する Secure Endpoint の保護が実質的に無効になるため、この手順は注意して使用する必要があります。Secure Endpoint サービスを無効化するには、以下のコマンドを実行します。

```
sudo systemctl disable cisco-amp
sudo systemctl stop cisco-amp
```

カーネルをリロードし、カーネルの汚染値をリセットするには、システムを再始動する必要があります。Cisco Secure Endpoint サービスを再度有効にするには、以下のコマンドを実行します。

```
sudo systemctl enable cisco-amp
sudo systemctl start cisco-amp
```

## Linux コネクタファイアウォールの例外

Cisco Secure Endpoint Linux コネクタを適切に動作させるためのファイアウォールの例外については、「コネクタファイアウォールの例外」を参照してください。

# Cisco Secure Endpoint Linux コネクタのインストール

Debian ベースのシステムにコネクタをインストールするには、次のコマンドを実行します。

```
sudo apt-get install [deb package] -y
```

ここで [deb package] はコンピュータ上のファイルへのパスです。例：~/Desktop/amp_Audit.deb。

他のサポートされているディストリビューションにコネクタをインストールするには、次のコマンドを実行します。

```
sudo yum localinstall [rpm package] -y
```

ここで [rpm package] は、たとえば amp_Audit.rpm のようなファイル名です。

コネクタを SUSE にインストールするには、次のコマンドを実行します。

```
sudo zypper install -y [rpm package]
```

ここで [rpm package] は、たとえば amp_Audit.rpm のようなファイル名です。

**重要：**環境内にある他のセキュリティ製品によって、Cisco Secure Endpoint コネクタのインストーラが脅威として検出される可能性があります。その場合は、他のセキュリティ製品で許可リストに追加するか、対象から除外してから再度実行してください。

**重要事項：**コネクタバージョン 1.10.0 以降、ファイルスキャン操作は非特権プロセスを使用して実行されます。インストール中、cisco-amp-scan- svc という名前のユーザーとグループがシステムに作成されます。このユーザーまたはグループがすでに存在し、設定が異なっている場合、インストーラによって削除され、必要な設定で再作成されます。ユーザーおよびグループが必要な設定で作成できなかった場合、インストーラは失敗します。

## Linux コネクタの更新

プライベートクラウド環境のコネクタやパブリッククラウド環境の 1.17.0 より前のバージョンのコネクタについては、ポリシーによる更新をサポートするために、コネクタをインストール後に Cisco GPG 公開キーを手動でマシンにインポートする必要があります。[コネクタのダウンロード（Download Connector）] ページから GPG 公開キーをコピーして、RPM または DEB の署名を検証することもできます。コネクタは GPG キーを使用せずにインストールできますが、ポリシーを使用してコネクタの更新をプッシュする予定の場合は、RPM DB（RPM ベースの Linux システム）または debsig キーチェーン（Debian ベースの Linux システム）に GPG キーをインポートする必要があります。

RPM ベースの Linux システムに GPG 鍵をインポートするには、次の手順を実行します。

1. [コネクタのダウンロード（Download Connector）] ページで [GPG公開キー（GPG Public Key）] リンクをクリックして GPG キーを検証します。`/opt/cisco/amp/etc/rpm-gpg/RPM-GPG-Key-cisco-amp` にあるものとキーを比較します。
2. キーをインポートする端末からコマンド `sudo rpm -- import /opt/cisco/amp/etc/rpm-gpg/RPM-GPG-KEY-cisco-amp` を実行します。
3. 端末からコマンド `rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'` を実行してキーがインストールされていることを検証します。
4. 出力の Sourcefire から GPG キーを検索します。

Debian ベースの Linux システムに GPG キーをインポートする場合は、『Debian ベースのシステム上の Cisco Secure Endpoint Linux コネクタ』の「Verifying the DEB Package」に示されている手順に従ってください。

アップデータがシステムの init デーモンによって実行され、更新が利用可能になると、RPM の更新プロセスが自動的にトリガーされます。一部の SELinux の設定では、この動作が禁止されており、アップデータが更新に失敗する場合があります。この状態になっていると思われる場合は、システムの監査ログ（/var/log/audit/audit.log など）を調べ、ampupdater に関連する拒否イベントを探します。Updater が機能するように SELinux のルールを調整する必要がある場合があります。

# Cisco Secure Endpoint Linux コネクタの使用方法

Cisco Secure Endpoint Linux コネクタでは、グラフィカル ユーザー インターフェイスに加えてコマンド ライン インターフェイスがエンドポイントで使用されます。Cisco Secure Endpoint Linux コネクタのコマンド ライン インターフェイスは `/opt/cisco/amp/ampcli` にあります。インタラクティブ モードで実行するか、または 1 つのコマンドを実行して終了できます。`./ampcli --help` を使用して、使用可能なオプションやコマンドの完全なリストを確認します。コネクタによって生成されたすべてのログファイルは `/var/log/cisco` にあります。

## Linux コネクタのエラー

コネクタの正常な動作に影響を与える状態が検出されると、コネクタから障害発生イベントが通知されることがあります。同様に、障害解消イベントは、その状況がもはや存在しないことを示しています。詳細については、この Cisco Secure Endpoint テクニカルノートを参照してください。

## Linux コネクタサポートツール

サポート ツールは `/opt/cisco/amp/bin/ampsupport` にあります。サポート パッケージを生成するには 2 つの方法があります。

```
sudo ./ampsupport
```

これにより、サポート パッケージが現在のユーザーのデスクトップ ディレクトリ（存在する場合）に置かれます。それ以外の場合は、現在のユーザーのホーム ディレクトリにサポート パッケージが作成されます。

```
sudo ./ampsupport -o [path]
```

これは、[パス（path）] によって指定されたディレクトリ内にサポート パッケージを配置します。次に例を示します。

`sudo ./ampsupport -o /tmp` はファイルを `/tmp` に配置します。

### Linux コネクタの [無効（Disabled）] ステータス

コネクタのステータスが [無効（Disabled）] の場合は、サポートに連絡してください。

## Linux コネクタのアンインストール

Debian ベースのシステムの Cisco Secure Endpoint Linux コネクタをアンインストールするには、次のコマンドを実行します。

```
sudo apt-get remove ciscoampconnector -y
```

SUSE の Cisco Secure Endpoint Linux コネクタをアンインストールするには、次のコマンドを実行します。

```
sudo zypper remove -y ciscoampconnector
```

他のサポートされているディストリビューションのコネクタをアンインストールするには、次のコマンドを実行します。

```
sudo yum remove ciscoampconnector -y
```

**重要：**yum を使用すると、必要に応じて Orbital が子の依存関係として削除されます。

このコマンドでは、履歴や検疫されたファイル、および `cisco-amp-scan-svc` ユーザーやグループを含むローカルデータはそのまま残ることに注意してください。コネクタを再インストールする予定がなく、残りのファイルを削除する場合は、次のスクリプトを実行します。

```
/opt/cisco/amp/bin/purge_amp_local_data
```

**重要：**これにより、Orbital が子の依存関係であることが確認され、必要に応じて削除されます。

dpkg を使用する場合は、Orbital を指定して、必要に応じて Orbital が削除されるようにします。

```
sudo dpkg --remove cisco-orbital ciscoampconnector
```

コネクタを再インストールする予定がなく、Orbital を削除する場合は、次のスクリプトを実行します。

```
sudo apt-get purge ciscoampconnector -y
```

**重要：**これにより、Orbital が子の依存関係であることが確認され、必要に応じてパージされます。

dpkg を使用する場合は、Orbital も指定して、必要に応じて Orbital がパージされるようにします。

```
sudo dpkg --purge cisco-orbital ciscoampconnector
```

**重要：**コネクタは Ubuntu Software Center を使用してアンインストールできますが、ローカルデータと設定は削除されません。これらのファイルを削除するには、上記のスクリプトを実行する必要があります。

# 第 11 章

# Cisco Secure Endpoint iOS Connector

Cisco Secure Endpoint iOS Connector は、Clarity という名前のモジュールを搭載した監視対象 iOS デバイスにおけるアプリの使用とネットワークアクティビティをモニタリングすることで、前例のない可視性を提供します。Clarity は Cisco Secure Endpoint コンソール内で管理される、Cisco Secure Endpoint 導入環境全体のインシデントやデバイスアクティビティを調査するための単一の場所です。Cisco Secure Endpoint iOS Connector を展開する前に、MDM の統合を設定する必要があります。

Cisco Umbrella のインストールおよび設定の詳細については、Cisco Secure Endpoint iOS Umbrella セットアップガイド [英語] を参照してください。

## iOS システム要件

Cisco Secure Endpoint iOS Connector の最小システム要件は次のとおりです。

- デバイスは監視モードで実行されていて、Mobile Device Manager（MDM）を使用して管理されている必要があります。デバイスの設定と構成に関するその他の要件については、MDM のマニュアルを参照してください。
- 5 MB の空き容量。

また、Cisco Secure Endpoint コンソールと次のいずれかの Mobile Device Manager の間で MDM の統合をセットアップする必要があります。

- Meraki システムマネージャ（SM）
- MobileIron
- IBM MaaS360
- Jamf Pro
- MobiConnect
- Workspace ONE
- Microsoft Intune

iOS バージョンの互換性については、この記事を参照してください。

## iOS Connector の既知の問題

- Cisco Secure Endpoint コンソールでデバイスを削除しても、そのデバイスは MDM ではプロビジョニング解除されません（アプリの設定かアプリ自体を削除します）。回避策としては、MDM 経由で Cisco Secure Endpoint iOS アプリをデバイスから削除します。削除したデバイスは、手動で削除するまで Cisco Secure Endpoint コンソールに表示され続けます。
- Apple Configurator を使用して Cisco Secure Endpoint iOS Connector をインストールしている場合、シリアル番号が正しく入力されないという既知の問題があります。
- 一部の絵文字名を持つデバイスは登録されないことがあります。ほとんどの絵文字は処理されます。
- アプリがデバイスからアンインストールされたときに、Cisco Secure Endpoint コンソールに通知されないため、Cisco Secure Endpoint iOS Connector がアンインストールされてから再インストールされると、コンソール内にそのデバイスに対する重複エントリが発生します。
- デバイスがワイプされ、コネクタが再インストールされた場合、ID の同期（有効な場合）により、重複する Cisco Secure Endpoint iOS Connector がコンソールに表示されることがあります。
- Clarity は、アプリケーション単位の VPN またはアプリケーション トンネリング トラフィックに対する可視性を備えていないため、デバイストラジェクトリのトラフィックは Cisco Secure Endpoint コンソールに表示できません。
- 同じデバイスに 2 つのプロファイルを展開する場合、両方のプロファイルに同じモジュール（Clarity または Cisco Umbrella）が含まれていると、MDM でエラーが発生し、2 番目のプロファイルは展開されません。たとえば、Clarity のみを含む profile1 が最初に展開された場合、Clarity と Cisco Umbrella を含む profile2 は展開されず、profile1 に Clarity のみ設定されているアプリが実行されます。
  2 つのプロファイルに共通のモジュールが存在しない場合、両方のプロファイルが展開されます。たとえば、Clarity のみを含む profile1 が最初に展開された場合、Cisco Umbrella のみを含む profile2 も展開され、Clarity と Cisco Umbrella の両方があるアプリが実行されます。

- Cisco Security Connector 1.2.0 以前では、アクティブブロックモードでは TOR トラフィックを可視化できず、トラフィックをブロックできません。
- Cisco Security Connector バージョン 1.3.0 以降では、すべてのモードで TOR トラフィックを可視化でき、トラフィックをブロックできますが、ブロックが可能なのは IP 情報を開示するブラウザに限られています。

# iOS Connector ファイアウォール接続

デバイスがファイアウォールの背後にある Wi-Fi ネットワークを使用している場合、Cisco Secure Endpoint iOS Connector は特定のポートを介して特定のサーバーにアクセスする必要があります。Cisco Secure Endpoint iOS Connector を適切に動作させるためのファイアウォールの例外については、「コネクタファイアウォールの例外」を参照してください。

# Clarity ドメイン除外

ドメインの除外リストを使用して、Clarity で無視されるドメインを指定できます。このリストにあるドメインに対するネットワーク アクティビティはすべて Cisco Cloud に報告されず、モバイル アプリ トラジェクトリやデバイス トラジェクトリに表示されません。除外リストは、Mobile Device Manager ダッシュボードを使用して指定します。

Clarity では、ホスト名の正確な一致、またはワイルドカードを使用したサブドメインを介して除外がサポートされます。たとえば、正確なホスト名 www.cisco.com やサブドメイン *.cisco.com を除外でき、この場合、www.cisco.com、cisco.com、および cisco.com プライマリドメインに含まれるその他すべてのサブドメインが除外されます。

## Meraki ドメイン除外

1. Meraki ダッシュボードで Cisco Secure Endpoint iOS Connector を含むプロファイルを開き、[Clarityコンテンツフィルタ（Clarity Content Filter）] を選択します。
2. domain_exclusions_list キーを追加し、[タイプ（Type）] ドロップダウンから [リスト（List）] を選択します。[値（Value）] フィールドにホスト名またはサブドメインを追加し、変更を保存します。リストには複数のホスト名やサブドメインを追加できます。
3. iOS デバイスで Cisco Secure Endpoint iOS Connector を開き、[Clarity] ステータスに移動します。[ドメインの除外（Domain Exclusions）] を選択して、追加したリストを確認します。

**重要：**ドメインの除外を追加するために、Meraki ダッシュボードを使用して Clarity プロファイルを変更する場合、変更内容は、Cisco Secure Endpoint コンソールを使用して Clarity ポリシーに変更を加える際に常に上書きされます。

## Workspace ONE ドメイン除外

Workspace ONE にドメインの除外を追加するには、新しい Mobileconfig ファイルをダウンロードして編集する必要があります。

1. 「Workspace ONE を介した展開」を参照し、除外を追加するグループの Mobileconfig ファイルをダウンロードします。
2. Mobileconfig ファイルをテキスト エディタで開きます。
3. 次の例のように、ブロック内にドメインの除外リストを追加します。ファイルを保存します。

```
<key>VendorConfig</key>
    <dict>
        <key>affiliate_guid</key>
        <string>7e9d7d2a-b554-50f4-3ebb-d275f6f9aa30</string>
        <key>cloud_asn1_server_host</key>
        <string>cloud-ios-asn.amp.cisco.com</string>
        [...]
        <key>domain_exclusions_list</key>
        <array>
            <string>www.google.com</string>
            <string>*.cisco.com</string>
            <string>www.reddit.com</string>
            <string>*.office.opendns.com</string>
        </array>
    </dict>
```

4. 既存のプロファイルを更新するには、Workspace ONE ダッシュボードで、[デバイス（Devices）] > [プロファイルとリソース（Profiles & Resources）] > [プロファイル（Profiles）] に移動します。
5. Clarity プロファイルを開き、[バージョンの追加（Add Version）] をクリックします。
6. [カスタム設定（Custom Settings）] の下に、変更した Mobileconfig セクションを追加します。

## MobileIron ドメイン除外

MobileIron にドメインの除外を追加するには、新しい Mobileconfig ファイルをダウンロードして編集する必要があります。

1. 「MobileIron を介した展開」を参照し、除外を追加するグループの Mobileconfig ファイルをダウンロードします。
2. Mobileconfig ファイルをテキスト エディタで開きます。

3. 次の例のように、ブロック内にドメインの除外リストを追加します。ファイルを保存します。

```
<key>VendorConfig</key>
    <dict>
        <key>affiliate_guid</key>
        <string>7e9d7d2a-b554-50f4-3ebb-d275f6f9aa30</string>
        <key>cloud_asn1_server_host</key>
        <string>cloud-ios-asn.amp.cisco.com</string>
        [...]
        <key>domain_exclusions_list</key>
        <array>
            <string>www.google.com</string>
            <string>*.cisco.com</string>
            <string>www.reddit.com</string>
            <string>*.office.opendns.com</string>
        </array>
    </dict>
```

4. MobileIron の既存プロファイルは編集できないため、MobileIron を介した展開プロファイルの作成手順と同じ手順を使用して、既存プロファイルと編集した Mobileconfig を置き換える必要があります。

## Cisco Secure Endpoint iOS Connector のアップグレード

Cisco Secure Endpoint iOS Connector の更新バージョンは、利用可能になると App Store にプッシュされ App Store で更新されます。

## Cisco Secure Endpoint iOS Connector のアンインストール

管理対象デバイスからアプリを削除する手順については、MDM のマニュアルを参照してください。

## モバイルデータを介した Cisco Secure Endpoint iOS Connector の無効化の防止

ユーザーは、iOS 設定アプリを使用して、デバイス全体またはアプリごとの携帯電話データの使用を有効化または無効化する機能を設定できます。Cisco Secure Endpoint iOS Connector のモバイルデータの使用が無効になっていると、データの送受信に Wi-Fi ではなく携帯電話ネットワークがデバイスで使用されている場合、保護は提供されません。

管理者は、MDM ダッシュボードを使用して携帯電話データ設定へのアクセスを無効化できます。これで、Cisco Secure Endpoint iOS Connector のモバイルデータの使用をユーザーがオフにするのを防げます。

**重要：**これらの変更を行うと、ユーザーはデバイス上のすべてのアプリの携帯電話データの使用をオフにできなくなります。

## Meraki

1. Meraki ダッシュボードで、[プロファイルと設定（Profiles & Settings）] に移動します。
2. [制限（Restrictions）] を追加します（まだ追加されていない場合）。
3. [iOS の制限（監視対象）（iOS restrictions (supervised)）] の下にある [アプリの携帯電話データの使用に対する変更を許可する（iOS 7 以降）（Allow changes to cellular data usage for apps (iOS 7+)）] のチェックを外します。

## MobileIron

MobileIron の場合は、Cisco Secure Endpoint または Cisco Umbrella コンソールからダウンロードした Clarity Mobileconfig ファイルを Apple Configurator 2 アプリを使用して変更する必要があります。

1. Apple Configurator で Mobileconfig ファイルを開きます。
2. 左側のペインで [制限（Restrictions）] を選択します。
3. [携帯電話データ アプリの設定の変更を許可する（監視対象のみ）（Allow modifying cellular data app settings (supervised only)）] のチェックを外します。
4. Mobileconfig ファイルを保存し、MobileIron MDM にインポートします。

## Workspace ONE

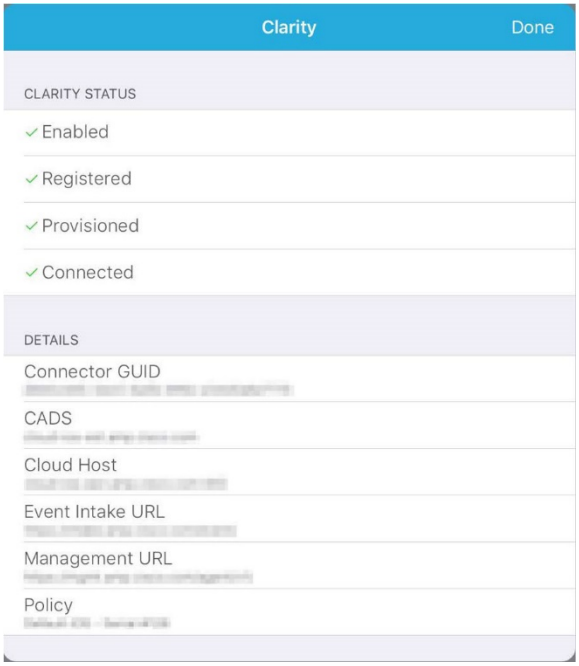
1. Workspace ONE ダッシュボードで、[デバイス（Devices）] > [プロファイルとリソース（Profiles & Resources）] > [プロファイル（Profiles）] に移動します。
2. Clarity または Umbrella プロファイルを検索して開きます。
3. [バージョンの追加（Add Version）] をクリックします。
4. [制限（Restrictions）] の下にある [アプリの携帯電話データの使用に対する変更を許可する（Allow changes to cellular data usage for apps）] のチェックを外します。

# iOS Connector ユーザーインターフェイス

Cisco Secure Endpoint iOS アプリをデバイスにインストールすると、Clarity や Cisco Umbrella が実行中であることを確認できます。

1. [Cisco Secure Endpoint iOS] アイコンをタップします。


2. メインスクリーンで [状態（Status）] をタップします。実行中の各コンポーネントの横に、緑色のチェックマークアイコンが表示されます。
3. [Clarityによる保護（Protected by Clarity）] をタップして、Clarity ステータスの詳細を表示します。トラブルシューティング時には、この画面で [コネクタGUID（Connector GUID）] を確認できます。



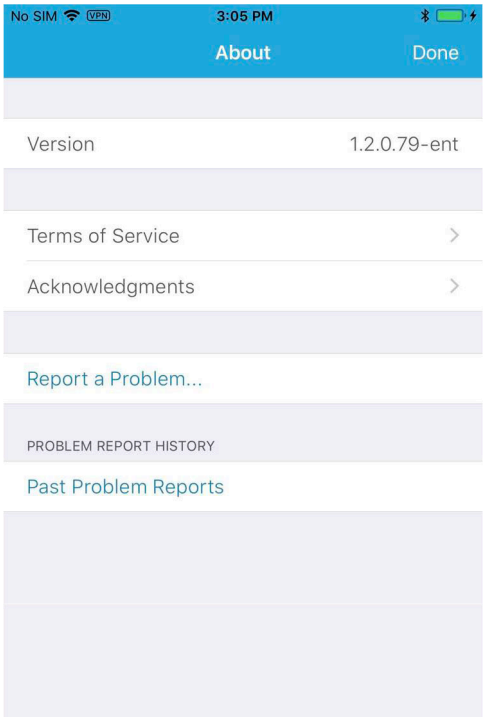
## 問題レポート

ユーザーは、アプリから問題レポートを送信することもできます。レポートの送信先の電子メールアドレスは、[MDMの統合（MDM Integration）] ページで指定できます。

**重要：**Cisco Umbrella と統合されている場合、問題レポートの送信先メールアドレスの指定は Cisco Umbrella ポータルで行います。

1. [Cisco Secure Endpoint iOS] アイコンをタップします。


2. メイン スクリーンで [詳細（Learn More）] をタップします。
3. [問題を報告...（Report a Problem...）] をタップします。




4. 画面の指示に従って、プロセスを完了します。

# 第 12 章

# Cisco Secure Endpoint Android コネクタ

Cisco Secure Endpoint Android コネクタは、Android 8.0 以降をサポートしています。

アプリは、Google Play ストアからダウンロードでき、Cisco Secure Endpoint コンソールからも直接ダウンロードできます。

コンソールから APK をダウンロードする場合は、Mobile Device Manager（MDM）を使用し、管理対象の設定を使用して組織内のデバイスにアプリをプッシュすることを推奨します。

**重要事項：**Google Play を介してアプリをインストールしたユーザーは、Google Play ストアアプリの**アプリ自動更新**設定に応じてコネクタの更新を受信します。

インストールを開始するには、ダウンロードしたファイルをタップします。

## Android コネクタファイアウォールの例外

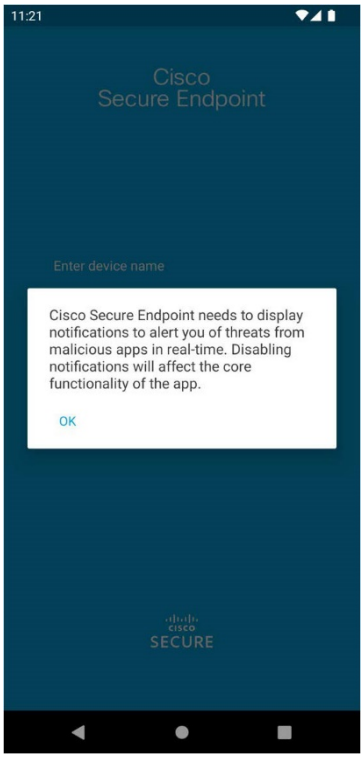
Wi-Fi 環境でシスコのシステムとの通信をコネクタに許可するには、クライアントが特定のポートを介して特定のサーバーに接続することをファイアウォールで許可する必要があります。Cisco Secure Endpoint Android コネクタを適切に動作させるためのファイアウォールの例外については、「コネクタファイアウォールの例外」を参照してください。

# Android インストーラ

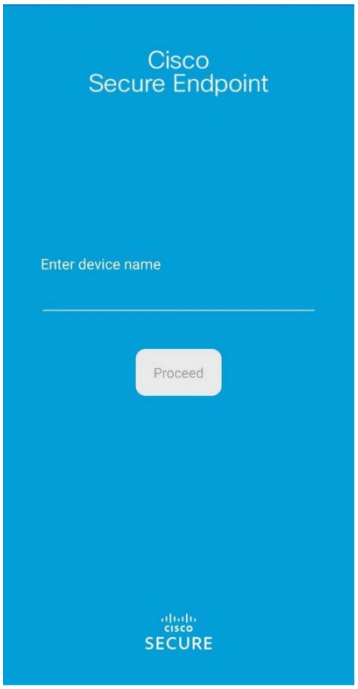
インストールを開始する前に必要な権限を確認するように要求される場合があります。

**重要：** Google Play からアプリをインストールした場合は、アプリを開く前にデバイスでアクティベーションリンクを使用する必要があります。ユーザーは、電子メールまたはブラウザウィンドウからリンクをタップする必要があります。ブラウザのアドレスバーに URL を貼り付けないでください。

1. インストールが完了したら、[開く（Open）] を選択してアプリケーションを起動します。
2. Android 13 以降で実行されているコネクタバージョン 2.5.0 以降では、通知を許可するように求められます。脅威をリアルタイムで検出するには、通知を許可してアプリのコア機能を維持する必要があります。



3. Cisco Secure Endpoint コンソールに表示されるデバイスの名前を入力し、[続行（Proceed）] をタップします。

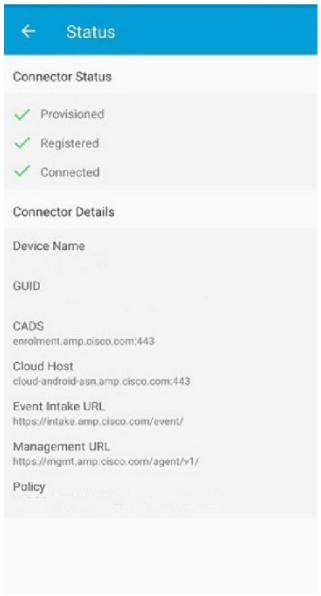



4. Cisco Secure Endpoint Android コネクタが、Cisco Cloud への接続を確立しようとします。

**重要：**Android 12 以降で新しいコネクタをインストールするには、デフォルトで Cisco Secure Endpoint コンソールの URL を開くようにコネクタアプリを設定する必要があります。これを行うには、アプリのインストール後にアプリを開き、ダイアログの指示に従ってください。

5. アプリケーションがデバイスの初期スキャンを開始して、悪意のあるアプリケーションや非準拠のアプリケーションを検索します。スキャン完了後に、[概要（Summary）] ボタンをタップすると、クリーンなアプリおよび悪意のあるアプリと、コネクタポリシーに関連付けられたカスタム検出：Android リストにあったアプリの概要が表示されます。

6. [ステータス（Status）] ページを確認することで、コネクタが正しくプロビジョニングおよび登録され、Cisco Cloud に接続されていることを確認できます。




### バッテリの最適化

Android デバイスでは、バックグラウンドで動作している特定のアプリに関するバッテリ最適化を設定できます。デバイスで Cisco Secure Endpoint アプリのバッテリ最適化が有効になっている場合、一定期間が経過すると、アプリがバックグラウンドで動作しなくなります。これにより、新しいアプリのインストール時にリアルタイムスキャンが実行されなくなります。すべてのアプリが確実にスキャンされるようにするには、デバイスの設定で Cisco Secure Endpoint アプリの最適化を無効にする必要があります。設定を無効にする手順については、使用しているバージョンの Android のマニュアルを参照してください。

## Android コネクタ ユーザー インターフェイス

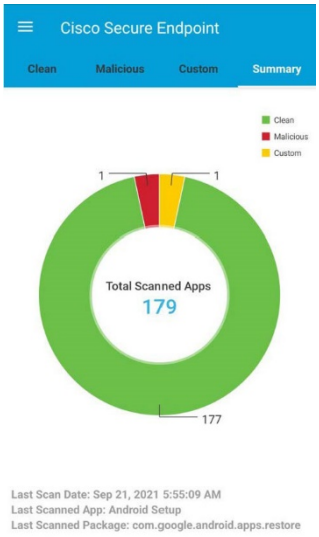
Cisco Secure Endpoint Android コネクタのアイコンをタップしてアプリを起動します。

**重要：**Android 12 以降で新しいコネクタをインストールする際には、アプリを初めて起動すると、デフォルトで Cisco Secure Endpoint コンソールの URL を開くようにコネクタアプリを設定するように求められます。ダイアログボックスの指示に従って続行してください。

## 脅威の除去

デバイス上で脅威または非準拠のアプリが検出された場合は、修正手順を実施する必要があります。脅威が検出された場合は、ステータス バーに通知が表示されます。詳細は、通知センターを展開するか、Cisco Secure Endpoint Android アプリを開くことで表示できます。

スキャン完了後に [概要（Summary）] ボタンをタップすると、チャートと、スキャンされたアプリの数、クリーンなアプリの数、悪意のあるアプリの数、およびカスタム検出：Android リスト内のエントリと一致した数が表示されます。




[クリーン（Clean）] タブをタップすると、デバイスにインストールされているクリーンなアプリのリストが表示されます。[悪意あり（Malicious）] タブをタップすると、マルウェアとして検出されたアプリのリストが表示されます。[カスタム（Custom）] タブを使用して、デバイスで検出された任意のカスタム検出：Android リストのアプリを表示することもできます。[悪意あり（Malicious）] タブと [カスタム（Custom）] タブでは、[アンインストール（Uninstall）] ボタンを使用してアプリを削除することもできます。

クリーンなアプリ、悪意のあるアプリ、およびカスタムアプリの検出に関するタブで、アプリを名前で検索できます。

### レトロスペクティブ検出

アプリが以前はクリーンであると考えられていて、後で悪意があるとマークされた場合、レトロスペクティブ検出をコネクタに送信して、アプリをクリーンなアプリのタブから悪意あるアプリのタブに移動させることができます。誤検出を、悪意のあるアプリのタブからクリーンなアプリのタブに移動させることもできます。

**重要：**アプリは、ユーザーが手動でアンインストールしていない場合にのみ、悪意のあるアプリのタブからクリーンなアプリのタブに移動させることができます。

## 問題の報告

問題の報告を使用すると、ユーザーはクラッシュログをファイルリポジトリにアップロードできます。サポートケースを開く必要がある場合は、トラブルシューティング用のファイルをシスコサポートに提供できます。

# 第 13 章

# コネクタのエンジンと機能

各コネクタは複数のエンジンと機能を使用して、マルウェア、エクスプロイト、およびランサムウェアに対する検出および対処機能を提供します。これらの設定は、ポリシーの設定によって制御されます。一部のエンジンと機能は特定のバージョンのコネクタでのみ使用可能なため、その点について説明します。

## TETRA

対象製品：

- Cisco Secure Endpoint Windows コネクタ。

TETRA は、ウイルス対策製品に完全に置き換わるものであり、別のウイルス対策エンジンがインストールされている場合は絶対に有効にしないでください。また、TETRA は、定義更新をダウンロードするときに大量の帯域幅を消費する可能性があるため、大規模環境で有効にする場合は注意が必要です。

TETRA を有効にし、設定を調整するには、ポリシーで [詳細設定（Advanced Settings）] > [TETRA] に移動します。

## ClamAV

対象製品：

- Cisco Secure Endpoint Mac コネクタ。
- Cisco Secure Endpoint Linux コネクタ。

**ClamAV** は、ウイルス対策製品に全面的に代わるものであり、別のウイルス対策エンジンがインストールされている場合は絶対に有効にしないでください。また、ClamAV は、定義更新をダウンロードするときに大量の帯域幅を消費する可能性があるため、大規模環境で有効にする場合は注意が必要です。

ClamAV を有効にし、設定を調整するには、ポリシーで [詳細設定（Advanced Settings）] > [ClamAV] に移動します。

# エクスプロイトの防止

対象製品：

- Cisco Secure Endpoint Windows コネクタ 6.0.5 以降。

エクスプロイト防止エンジンは、未修正ソフトウェアの脆弱性をターゲットとするマルウェアやゼロデイ攻撃で一般的に使用される、メモリインジェクション攻撃からエンドポイントを保護します。保護されているプロセスに対する攻撃を検出すると、その攻撃をブロックし、イベントを生成しますが、検疫は実行されません。デバイストラジェクトリを使用すると、攻撃のベクターを判定し、カスタム検出：簡易リストに追加するのに役立ちます。

エクスプロイト防止エンジンを有効にするには、ポリシーで [モードとエンジン（Modes and Engines）] に移動し、[監査（Audit）] モードは [ブロック（Block）] モードを選択します。[監査（Audit）] モードは Cisco Secure Endpoint Windows コネクタ 7.3.1 以降でのみ使用できます。7.3.1 より前のバージョンのコネクタでは、[監査（Audit）] モードは [ブロック（Block）] モードと同様に扱われます。

**重要事項：** Windows 7 および Windows Server 2008 R2 では、コネクタをインストールする前に Microsoft Security Advisory 3033929 のパッチを適用する必要があります。

## 保護されたプロセス

エクスプロイト防止エンジンは、次の 32 ビットおよび 64 ビット（Cisco Secure Endpoint Windows コネクタバージョン 6.2.1 以降）のプロセスと、各プロセスの子プロセスを保護します。

- Microsoft Excel アプリケーション
- Microsoft Word アプリケーション
- Microsoft PowerPoint アプリケーション
- Microsoft Outlook アプリケーション
- Internet Explorer ブラウザ
- Mozilla Firefox ブラウザ
- Google Chrome ブラウザ

- Microsoft Skype アプリケーション
- TeamViewer アプリケーション
- VLC メディア プレーヤー アプリケーション
- Microsoft Windows スクリプト ホスト
- Microsoft Powershell アプリケーション
- Adobe Acrobat Reader アプリケーション
- Microsoft Register Server
- Microsoft タスク スケジューラ エンジン
- Microsoft Run DLL コマンド
- Microsoft HTML アプリケーションホスト
- Windows スクリプトホスト
- Microsoft アセンブリ登録ツール
- ズーム
- Slack
- Cisco Webex Teams
- Microsoft Teams

エクスプロイト防止の実行ファイルの除外を追加することで、任意のアプリケーションをエクスプロイト防止保護から除外できます。

**重要：**エクスプロイト防止を無効にした場合は、前述の保護されているプロセスのうち、実行中だったいずれかのプロセスを再起動する必要があります。

また、次のディレクトリもモニターします。

- Windows AppData Temp ディレクトリ (\Users\[username]\AppData\Local\Temp\)
- Windows AppData Roaming ディレクトリ (\Users\[username]\AppData\Roaming\)

エクスプロイト防止は、これらのディレクトリから起動されるアプリケーションによるインジェクション試行からは通常保護されないプロセスを保護します。

## 除外されるプロセス

互換性の問題により、次のプロセスはエクスプロイト防止モニタリングから除外されます。

- McAfee DLP サービス
- McAfee Endpoint Security ユーティリティ

## エクスプロイト防止バージョン 5

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.5.1 以降。

Cisco Secure Endpoint Windows コネクタ 7.5.1 には、エクスプロイト防止の重要な更新が含まれています。このバージョンの新機能は次のとおりです。

- ネットワークドライブの保護：ネットワークドライブから実行されているプロセスをランサムウェアなどの脅威から自動的に保護します。
- リモートプロセスの保護：ドメイン認証ユーザー（管理者）を使用して保護されたコンピュータでリモート実行されているプロセスを自動的に保護します。この保護には、Kerberos、NtLmSsp、または Schannel のいずれかのトークンで作成されたプロセス（psexec など）のみが含まれます。除外リストに含まれるプロセスも、リモート実行保護から除外されます。
- rundll32 による AppControl のバイパス：解釈されたコマンドの実行を可能にする巧妙に細工された rundll32 コマンドラインを停止します。
- UAC のバイパス：Windows のユーザーアカウント制御メカニズムのバイパスを防止することにより、悪意のあるプロセスによる権限昇格をブロックします。
- ブラウザ/Mimikatz Vault のログイン情報：有効にすると、エクスプロイト防止により、Microsoft Internet Explorer および Edge ブラウザでのログイン情報盗難から保護されます。
- シャドウコピーの削除：Microsoft ボリューム シャドウ コピー サービス（vssvc.exe）の COM API をインターセプトすることにより、シャドウコピーの削除を追跡します。シャドウコピーの削除は、通常、ランサムウェア攻撃の前に行われます。エクスプロイト防止では、シャドウコピーが削除されると脅威ログが生成されます。シャドウコピーの削除は、検出されますがブロックされません。
- SAM ハッシュ：レジストリハイブ `Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users` 内のすべての SAM ハッシュを列挙および復号する試みをインターセプトすることにより、Mimikatz による SAM ハッシュログイン情報盗難から保護されます。攻撃者は、オペレーティングシステムやソフトウェアからアカウントログインおよびログイン情報の詳細（通常はハッシュまたはクリアテキストパスワードの形式）を取得するために、ログイン情報のダンプを試みる可能性があります。
- 実行中のプロセスの保護：実行中のプロセス（explorer.exe、lsass.exe、spoolsv.exe、winlogon.exe）がエクスプロイト防止インスタンスの前に起動されている場合、それらのプロセスにインジェクトします。

ポリシーでエクスプロイト防止が有効になっている場合、これらの機能はすべてデフォルトで有効になります。

## スクリプト制御

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.3.1 以降。

エクスプロイト防止エンジンは、スクリプト制御により特定の DLL が一部のアプリケーションやその子プロセスによってロードされることを防止できます。このエンジンは、プロセスまたはその子プロセスのいずれかが、ブロックされた DLL のいずれかをロードしようとすると、そのプロセスを強制終了します。

| プロセス（Processes） | 子プロセス | ブロックされた DLL |
|---|---|---|
| winword.exe<br>excel.exe<br>powerpnt.exe<br>outlook.exe | cscript.exe<br>wscript.exe<br>powershell.exe<br>mshta.exe<br>cmd.exe<br>rundll32.exe<br>regsvr32.exe<br>autoit3.exe<br>cmstp.exe<br>node.exe | wbemdisp.dll<br>System.Management.Automation.dll<br>System.Management.Automation.ni.dll |
| regsvr32.exe | cscript.exe<br>wscript.exe<br>powershell.exe<br>mshta.exe<br>cmd.exe<br>rundll32.exe<br>regsvr32.exe<br>autoit3.exe<br>cmstp.exe<br>node.exe | scrobj.dll |

### 互換性のないソフトウェア

エクスプロイト防止エンジンは、以下のソフトウェアとの互換性がありません。

- Malwarebytes
- F-Secure DeepGuard

- ByteFence
- Microsoft Enhanced Mitigation Experience Toolkit（EMET）

**重要事項：**EMET の互換性の管理手順については、この Cisco Secure Endpoint テクニカルノートを確認してください。

また、Sophos Endpoint Protection との既知の問題で、アプリケーションを閉じたときに MS Word 2016 が正常に終了しない場合があります。

# システム プロセス保護

対象製品：

- Cisco Secure Endpoint Windows コネクタ 6.0.5 以降。

システムプロセス保護エンジンは、他のプロセスによるメモリインジェクション攻撃によって重要な Windows システムプロセスが侵害されないように保護します。

システムプロセス保護を有効にするには、ポリシーの [モードとエンジン（Modes and Engines）] に進み、システムプロセス保護の判定モードから [保護（Protect）] または [監査（Audit）] を選択します。

## 保護されるシステム プロセス

システムプロセス保護は、次のプロセスを保護します。

- Session Manager Subsystem（smss.exe）
- Client/Server Runtime Subsystem（csrss.exe）
- Local Security Authority Subsystem（lsass.exe）
- Windows Logon Application（winlogon.exe）
- Windows Start-up Application（wininit.exe）

# 悪意のあるアクティビティからの保護

対象製品：

- Cisco Secure Endpoint Windows コネクタ 6.1.5 以降。

Malicious Activity Protection エンジンは、プロセスの実行時に悪意のあるアクションを特定することで、エンドポイントをランサムウェア攻撃から保護し、データが暗号化されるのを防ぎます。Malicious Activity Protection エンジンは実行中のプロセスの動作を監視することで脅威を検出するため、他のセキュリティ製品および検出テクノロジーを回避したランサムウェアの新たな亜種によってシステムが攻撃を受けているかどうかを判別できます。

Malicious Activity Protection エンジンを有効にするには、ポリシーの [モードとエンジン（Modes and Engines）] に進み、Malicious Activity Protection の判定モードで [監査（Audit）]、[ブロック（Block）]、または [検疫（Quarantine）] を選択します。Malicious Activity Protection エンジンは、現時点では、Hyper-V クラスタと互換性がありません。

**重要：**コネクタは、ランサムウェアによるデータが完全に侵害されるのを検出および防止できますが、プロセスがランサムウェアの条件を満たしているとコネクタが判断する前に、一部のファイルが攻撃によって暗号化されます。残念ながら、こうしたファイルを復号するのは不可能です。ただし、問題のプロセスによって変更された最初の 5 ファイルはコネクタからレポートされるため、必要に応じて簡単にバックアップから復元できます。しかし、コネクタによって悪意のあるプロセスが検出され、そのプロセスが正常にブロックまたは検疫されるまでの間に、さらに多くのファイルが暗号化される可能性があることに注意してください。

# エンドポイントの隔離

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.0.5 以降。
- Cisco Secure Endpoint Mac コネクタ 1.21.0 以降。

エンドポイントの隔離は、Windows コンピュータでの着信および発信ネットワークアクティビティをブロックし、データ漏えいやマルウェアの拡散などの脅威を防ぐことができる機能です。この機能は、コネクタのバージョン 7.0.5 以降をサポートする 64 ビットバージョンの Windows で使用できます。

エンドポイント隔離セッションは、Windows コネクタと Cisco Cloud 間の通信には影響しません。エンドポイントの保護と可視性のレベルは、セッション前と変わりません。アクティブなエンドポイント隔離セッション中に、コネクタによってブロックされないアドレスの IP 隔離許可リストを設定できます。

## エンドポイント隔離セッションの開始

エンドポイントの隔離により、Cisco Cloud への通信と、IP 隔離許可リストに設定されているその他の IP アドレスを除くすべてのネットワークトラフィックがブロックされます。

エンドポイント隔離セッションを開始するには、次の手順を実行します。

1. コンソールで、[管理（Management）] > [コンピュータ（Computers）] の順に移動します。
2. 隔離するコンピュータを見つけてクリックすると詳細が表示されます。
3. [隔離の開始（Start Isolation）] ボタンをクリックします。

コネクタ ユーザー インターフェイスに、エンドポイントが隔離されたことが示されます。

**重要：**Cisco Secure Endpoint Mac コネクタの場合のみ：キャッシュされたブラウザコンテンツはすべて利用できますが、ブラウザの接続は停止します。隔離セッション中に Mac コネクタをアンインストールすることもできます。

## エンドポイント隔離セッションの停止

隔離セッションを停止すると、すべてのネットワークトラフィックがエンドポイントに復元されます。

エンドポイント隔離セッションをコンソールから停止するには、次の手順を実行します。

1. コンソールで、[管理（Management）] > [コンピュータ（Computers）] の順に移動します。
2. 隔離を停止するコンピュータを見つけてクリックすると詳細が表示されます。
3. [隔離の停止（Stop Isolation）] ボタンをクリックします。
4. エンドポイントの隔離を停止した理由に関するコメントを入力します。

コネクタ ユーザー インターフェイスに、エンドポイント隔離セッションが停止されたことが示されます。

## コマンドラインからの Windows 隔離セッションの停止

隔離されたエンドポイントが Cisco Cloud への接続を失った場合、隔離セッションはコンソールから停止できません。そのような場合は、コマンドラインからローカルでセッションを停止できます。

エンドポイント隔離セッションをコマンドラインから停止するには、次の手順を実行します。

1. コンソールで、[管理（Management）] > [コンピュータ（Computers）] の順に移動します。
2. 隔離を停止するコンピュータを見つけてクリックすると詳細が表示されます。
3. ロック解除コードをメモしておきます。
4. 隔離されたコンピュータで、管理者権限を使用してコマンドプロンプトを開きます。
5. コネクタがインストールされているディレクトリ（C:\Program Files\Cisco\AMP\[version number]）に移動して、`sfc.exe -n [unlock code]` を実行します。

**重要：**ロック解除コードを 5 回間違って入力すると、30 分間はロック解除を再試行できなくなります。

コネクタ ユーザー インターフェイスに、エンドポイント隔離セッションが停止されたことが示されます。

**重要：**アクティブな隔離セッションが進行中の場合、コネクタの一部の動作はブロックされます。
– 機能をオフにするためのポリシーの更新（隔離セッションの停止と混同しないでください）。機能をオフにしないポリシーの更新は許可されます。
– コネクタのアンインストール。アクティブな隔離セッションの間にコネクタのアンインストールを試みると、コード 16010 で終了します。
– コネクタのアップグレード。隔離されている間にコネクタのアップグレードを試みると、コンソールイベントに製品の更新失敗メッセージが表示されます。

## コマンドラインからの macOS 隔離セッションの停止

隔離されたエンドポイントが Cisco Cloud への接続を失った場合、隔離セッションはコンソールから停止できません。そのような場合は、コマンドラインからローカルでセッションを停止できます。

エンドポイント隔離セッションをコマンドラインから停止するには、次の手順を実行します。

1. コンソールで、[管理（Management）] > [コンピュータ（Computers）] の順に移動します。
2. 隔離を停止するコンピュータを見つけてクリックすると詳細が表示されます。
3. ロック解除コードをメモしておきます。
4. 隔離されたコンピュータで端末を開きます。
5. コネクタがインストールされているディレクトリ（/opt/cisco/amp）に移動し、`./ampcli isolate stop [unlock code]` を実行します。

**重要：**ロック解除コードを 5 回間違って入力すると、30 分間はロック解除を再試行できなくなります。

コネクタ ユーザー インターフェイスに、エンドポイント隔離セッションが停止されたことが示されます。

**重要：**アクティブな隔離セッションが進行中の場合、コネクタの一部の動作はブロックされます。
– 機能をオフにするためのポリシーの更新（隔離セッションの停止と混同しないでください）。機能をオフにしないポリシーの更新は許可されます。
– コネクタのアップグレード。隔離されている間にコネクタのアップグレードを試みると、コンソールイベントに製品の更新失敗メッセージが表示されます。

# Orbital

**重要：**Orbital は、Cisco Secure Endpoint Advantage または上位のパッケージを使用している場合に利用できます。

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.1.5 以降。
- Cisco Secure Endpoint Mac コネクタ 1.16.0 以降。
- Cisco Secure Endpoint Linux コネクタ 1.17.0 以降。

Orbital は、エンドポイントに導入し、エンドポイントの詳細情報をクエリするために Cisco Secure Endpoint で使用できるシスコサービスです。Orbital では、クエリをすぐに実行することも、Orbital ジョブ機能を使用してクエリをスケジュールすることもできます。

Orbital の使用の詳細については、Orbital のマニュアル（https://orbital.amp.cisco.com/help/）を参照してください。

## Orbital の Windows 要件

Orbital には、Windows 10 1709 以降または Windows Server 2012、2012 R2、2016 以降が必要です。Orbital は、Cisco Secure Endpoint Windows コネクタのバージョン 7.1.5 以降で使用できます。

### 既知の問題/制限

コネクタの保護機能が有効になっている場合でも、Orbital プロセスはコネクタによって保護されません。これは、相応の権限を持つユーザーが Orbital サービスを停止またはアンインストールできることを意味します。次の更新間隔に達すると、Windows コネクタにより Orbital が再インストールされます。

## Orbital の macOS 要件

Orbital には macOS 10.15 以降が必要です。Intel プロセッサの場合は Cisco Secure Endpoint Mac コネクタバージョン 1.16.0 以降、Apple シリコンの場合はバージョン 1.20.0 以降で使用できます（Orbital Node 1.21.0 以降が必要）。

### フルディスクアクセス権を付与

Orbital でクエリを実行するには、macOS へのフルディスクアクセス権が必要です。

展開および管理にモバイルデバイス管理（MDM）ソリューション（Cisco Meraki など）を使用している場合は、MDM プロファイルの Privacy Preferences Policy Control

Payload を使用してフルディスクアクセス権が付与されます。これにより、エンドユーザーはアクションをとる必要がなくなります。Cisco Secure Endpoint Mac コネクタ 1.14.0 以降の場合は、macOS 11（Big Sur）、macOS 10.15（Catalina）、および macOS10.14（Mojave）における Cisco Secure Endpoint Mac コネクタのアドバイザリ [英語] を参照してください。

ユーザーは、デバイス登録プログラム（DEP）に含まれていない macOS 10.13.4 以降を実行している Mac で MDM プロファイルを受け入れる必要があります。

MDM を使用していない場合は、次の手順を使用します。

1. [システム設定（System Preferences）] を起動します。
2. [セキュリティとプライバシー（Security and Privacy）] をクリックします。
3. [ロック（Lock）] をクリックして、変更を加えます。
4. 左側のペインから [フルディスクアクセス権（Full Disk Access）] を選択し、次の手順を実行して、`/Library/Application/ Support/Cisco/AMP for Endpoints Connector/Orbital/Cisco Orbital.app` を追加します。

[+] ボタンをクリックし、ファイル選択ダイアログボックスで `[/Library/Application/ Support/Cisco/AMP for Endpoints Connector/Orbital/Cisco Orbital.app]` を選択します。

## ポリシーでの Orbital の有効化

エンドポイントにコネクタがすでにインストールされている場合、Cisco Secure Endpoint は Orbital を自動的に展開できます。ポリシーで Orbital を有効にすると、Orbital が展開用の Cisco Secure Endpoint Windows コネクタおよび Mac コネクタのパッケージにバンドルされます。詳細については、「Orbital」を参照してください。

Cisco Secure Endpoint Windows コネクタのバージョン 7.4.5 以降では、管理者権限を持つアカウントを使用し、コネクタのインストールディレクトリから次のコマンドを使用して Orbital を強制的に更新できます。

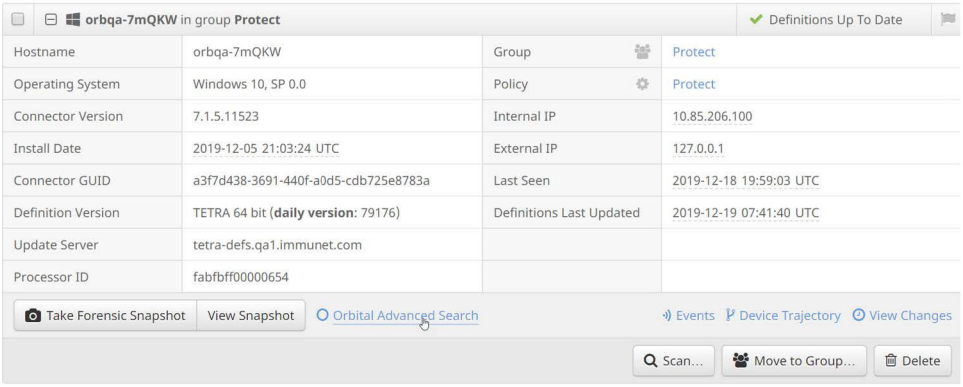
```
sfc.exe -forceOrbitalUpdate
```

このコマンドにより、失敗したキャッシュ済みバージョンがすべて削除され、現在のバージョンが再試行されます。

## Cisco Secure Endpoint コンソールからの Orbital へのアクセス

いくつかの方法で Cisco Secure Endpoint コンソールから Orbital にアクセスできます。[分析（Analysis）] > [Orbital Advanced Search] を選択して、Orbital コンソールに直接移動します。

特定のコンピュータの Orbital にアクセスするには、[管理（Management）] > [コンピュータ（Computers）] に移動し、検索するコンピュータを見つけます。そのコンピュータの [Orbital Advanced Search] リンクをクリックします。



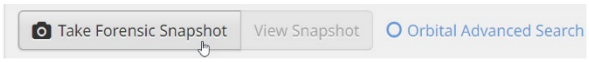

これにより、そのコンピュータでクエリを実行できる Orbital コンソールに移動します。コンピュータの GUID は、Orbital コンソールの [エンドポイント（Endpoints）] フィールドに自動的に入力されます。

Orbital でのクエリの実行については、Orbital のマニュアルのクイックスタートに関するセクション（https://orbital.amp.cisco.com/help/quick-start/）を参照してください。

## フォレンジック スナップショット

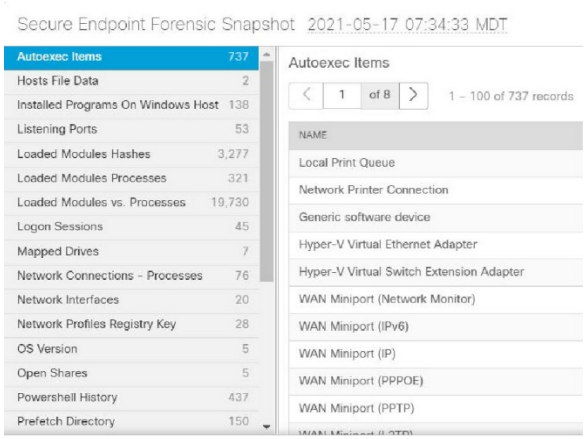
Orbital を使用すると、コンピュータのフォレンジック スナップショットを取得できます。フォレンジック スナップショットとは、エンドポイントの現在の状態に関連する情報（実行中のプロセス、ロードされたモジュール、自動実行の実行ファイルなど）をフォレンジック的に収集する事前設定された一連のクエリです。

フォレンジック スナップショット機能にアクセスするには、[管理（Management）] > [コンピュータ（Computers）] に移動し、検索するコンピュータを見つけます。[フォレンジック スナップショットの取得（Take Forensic Snapshot）] ボタンをクリックします。

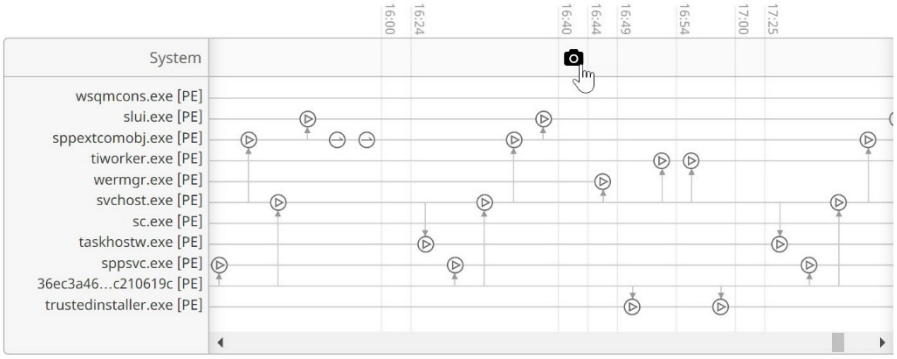



**重要事項：**一部の動作保護署名の場合、エンドポイントでのフォレンジック スナップショットを自動的にトリガーできます。

要求がエンドポイントに送信されます。スナップショットが完了したら、[スナップショットの表示（View Snapshot）] をクリックして結果を確認します。




コンピュータのデバイス トラジェクトリ ページからフォレンジック スナップショットの結果にアクセスすることもできます。




# スクリプト保護

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.2.1 以降。

スクリプト保護機能は、エンドポイントで実行されるスクリプトの可視性を提供し、マルウェアで一般的に使用されるスクリプトベースの攻撃を防ぎます。スクリプト保護により、スクリプトの実行チェーンに関するデバイストラジェクトリの可視性が向上し、エンドポイントでスクリプトの実行を試みるアプリケーションを確認できます。スクリプト保護には、Windows 10 バージョン 1709 以降または Windows Server 2016 バージョン 1709 以降が必要です。

スクリプト保護を有効にするには、ポリシーのモードおよびエンジンに進み、スクリプト保護の判定モードで監査または検疫を選択します。スクリプト保護は TETRA に依存し

ませんが、TETRA が有効になっている場合、スクリプト保護は TETRA を使用して追加の保護を提供します。

**重要：**検疫モードで動作している場合、スクリプト保護は、Word、Excel、PowerPoint などのユーザーアプリケーションに影響を与える可能性があります。これらのアプリケーションが悪意のある VBA スクリプトの実行を試みると、そのアプリケーションは停止されます。

スクリプト保護は、次のスクリプトインタープリタと連携します。

- PowerShell（V3 以降）
- Windows スクリプトホスト（wscript.exe および cscript.exe）
- JavaScript（非ブラウザ）
- VBScript
- Office VBA マクロ

**重要：**スクリプト保護は、Python、Perl、PHP、Ruby といった Microsoft 以外のスクリプトインタープリタに関する可視性や保護を提供しません。

スクリプト保護は、動作保護（コネクタバージョン 7.5.1 以降）と同じ分析エンジンを利用して、ファイルレスマルウェアからの保護を提供します。この機能では、実行中のスクリプトの一部（バッファ）が分析され、定期的に更新される悪意のあるスクリプトのシグネチャと比較されます。悪意のあるコンテンツが検出されたスクリプトは、実行がブロックされます。

## 動作保護

対象製品：

- Cisco Secure Endpoint Windows コネクタ 7.3.1 以降。
- Cisco Secure Endpoint Linux コネクタ 1.22.0 以降。

行動保護エンジンは、動作に基づいて脅威を検出および阻止する機能を強化します。これは、「Living off the land（環境寄生型）」攻撃の検出機能を強化し、シグネチャ更新を介して脅威の状況の変化に迅速に対応します。これは、コネクタのバージョン 7.3.1 以降でサポートされる 64 ビットバージョンの Windows で使用できます。

悪意のあるアクティビティが検出されると、エンジンは次のアクションを実行できます。

- プロセスを終了させる。
- ファイルを隔離する。
- 分析のためにファイルをアップロードする。
- プロセスツリーを終了させる

- Orbital Advanced Search も有効になっている場合に、特定の検出のフォレンジック スナップショットをトリガーする。

動作保護では、次のシステムアクティビティがモニターされます。

- プロセス。
- ファイルイベント。
- レジストリイベント。
- ネットワークイベント。

**重要事項：**[モードとエンジン（Modes and Engines）] でネットワークが [無効（Disabled）] に設定されている場合、または /skipdfc スイッチを使用してコネクタがインストールされている場合、動作保護ではネットワークイベントをモニターできません。

## Windows の追加要件

動作保護には、Supplemental Streaming SIMD Extensions 3（SSSE3）命令セットをサポートしている CPU も必要です。SSSE3 を含むプロセッサのリストについては、CPU の製造元の資料を参照してください。コンピュータのプロセッサが SSSE3 をサポートしていない場合、イベントリストに、シグネチャセット更新の失敗とエラーコード 50 が示されます。

**重要：**Hyper-V や VMware などの一部の仮想化テクノロジーには、ホスト CPU が SSSE3 をサポートしている場合でも、仮想マシンで SSSE3 機能をマスクできる設定があります。動作保護を使用するには、仮想マシンのマニュアルを参照して、これらの設定が無効になっていることを確認してください。

## Linux の追加要件

動作保護は、以下に示す最小カーネルバージョン以降のディストリビューションで使用できます。

動作保護のカーネルバージョン

| Linux ディストリビューション | 最小カーネルバージョン |
|---|---|
| Oracle | 3.10.0-940 |
| RHEL/CentOS | 3.10.0-940 |
| AlmaLinux/Rocky Linux | 4.18.0 |
| Amazon Linux 2 | 4.18.0 |
| SuSE | 4.18.0 |
| Debian | 4.18.0 |
| Ubuntu | 4.18.0 |

# リモートアンインストール

対象製品：

- Cisco Secure Endpoint Windows コネクタ。

  **重要：**Cisco XDR または SecureX のクラウド管理を介して展開された Cisco Secure Client は、現在サポートされていないことに注意してください。

- Cisco Secure Endpoint Mac コネクタ。
- Cisco Secure Endpoint Linux コネクタ。

Cisco Secure Endpoint 管理者は、この機能を使用してエンドポイントからコネクタをアンインストールできます。[管理（Management）] > [コンピュータ（Computers）] に移動し、アンインストールするエンドポイントを見つけます。コンピュータのペインを展開し、[コネクタのアンインストール（Uninstall Connector）] をクリックします。エンドポイントが [コンピュータ（Computers）] リストから削除され、監査ログエントリおよびイベントが作成されます。これは完全なアンインストールであり、コネクタの履歴と検疫されたファイルが削除されます。

**重要：**隔離されたコネクタはアンインストールできず、それらのエンドポイントについては [アンインストール（Uninstall）] ボタンを使用できません。隔離セッションを終了すると、 [アンインストール（Uninstall）] ボタンが使用可能になります。

ポリシーの管理機能でコネクタ保護が有効になっている場合、Cisco Secure Endpoint Windows コネクタをアンインストールするためにパスワードを入力する必要はありません。Windows では、エンドポイントにコネクタを再インストールする予定がない限り、再起動は必要ありません。Mac または Linux では、再起動は必要ありません。

管理対象外バージョンの macOS（バージョン 12.0 より前）では、Cisco Secure Endpoint Mac コネクタをアンインストールする際に管理者パスワードの入力を求められます。管理者パスワードを入力しないと、アンインストールは失敗します。詳細については、MDMを 使用した Cisco Secure Endpoint Mac コネクタおよび Orbital の権限の設定：フルディスクアクセス、システム拡張機能 [英語] を参照してください。

# 第 14 章

# エンドポイント IOC スキャナ

エンドポイント IOC（侵害の兆候）機能は、複数のコンピュータ全体で侵害後のインジケータをスキャンするための強力なインシデント対応ツールです。エンドポイント IOC はオープン IOC ベースのファイルからコンソール経由でインポートされます。このファイルは、名前、サイズ、ハッシュ、その他の属性などのファイルプロパティと、プロセス情報、実行中のサービス、Windows レジストリエントリなどのシステムプロパティをトリガーとして使用するように作成されています。

IOC 構文により、インシデント対応者が特定の観測対象を検索したり、マルウェアファミリの高度な相関検出を作成するロジックを活用したりできます。エンドポイント IOC にはポータブルであるというメリットがあり、組織内または業種別のフォーラムやメーリング リストで共有できます。

エンドポイント IOC スキャナは、Cisco Secure Endpoint Windows コネクタバージョン 4 以降で使用できます。エンドポイント IOC スキャンを実行するためには、最大 1 GB の空きドライブ領域が必要です。

IOC スキャナで現在サポートされている IOC 属性とサンプル エンドポイント IOC ドキュメントへのリンクの一覧表については、『Cisco Endpoint IOC Attributes 』ガイドを参照してください。

# インストールされたエンドポイント IOC

[インストールされたエンドポイント IOC（Installed Endpoint IOCs）] ページでは、アップロードしたすべてのエンドポイント IOC が一覧表示され、それらを管理できます。このページから、新しいエンドポイント IOC をアップロードしたり、既存のエンドポイント IOC を削除したり、それらをアクティブ/非アクティブにしたり、表示・編集したりできます。また、[すべての変更を表示（View All Changes）] をクリックすると、インストールされたエンドポイント IOC のエントリのみを含む監査ログのフィルタ処理されたビューも表示できます。

## エンドポイント IOC のアップロード

スキャンを開始するには、Cisco Secure Endpoint コンソールにエンドポイント IOC をアップロードする必要があります。[インストールされたエンドポイントIOC（Installed Endpoint IOCs）] ページに移動したら、[アップロード（Upload）] ボタンを使用して、エンドポイント IOC を転送します。単一の XML ファイルをアップロードすることも、複数のエンドポイント IOC ドキュメントを含む zip アーカイブをアップロードすることもできます。

**重要：**ファイル アップロードには 5 MB の制限があります。

複数のエンドポイント IOC を含むアーカイブをアップロードすると、すべてのファイルが抽出され、検証された時点で電子メールが送られてきます。無効な XML ファイルがアップロードされた場合は、スキャンをアクティブにすることができません。

各エンドポイント IOC のエントリには [変更の表示（View Changes）] リンクがあります。このリンクをクリックすると、特定のエンドポイント IOC のエントリだけがフィルタ処理された監査ログが表示されます。このため、IOC のアップロード、編集、有効化、無効化、変更を行ったユーザーを表示できます。

## 表示と編集

[表示（View）] ページと [編集（Edit）] ページを使用すると、個別のエンドポイント IOC を表示したり変更したりすることができます。

[概要説明（Short Description）] と [説明（Description）] がエンドポイント IOC ドキュメントの XML から最初に抽出されます。IOC 自体に影響を与えることなく、これらのフィールドを変更できます。

[カテゴリ（Categories）]、[エンドポイントIOCグループ（Endpoint IOC Groups）]、および [キーワード（Keywords）] は、各エンドポイント IOC に割り当てると、メインリストからフィルタ処理できます。これは、特定のタイプのすべてのエンドポイント IOC を有効または無効にする場合に便利です。エンドポイント IOC の変更が完了したら、変更内容を保存できます。

[編集（Edit）] ページでは、IOC を [ダウンロード（Download）] または [置換（Replace）] できます。このページは、エンドポイント IOC 内のインジケータとインジケータ項目の編集に使用できます。編集したエンドポイント IOC をアップロードする代わりに置換を使用すると、割り当てたカテゴリ、エンドポイント IOC グループ、およびキーワードも保存されます。

**重要事項：** Cisco Secure Endpoint コネクタでサポートされていない属性付きのエンドポイント IOC ドキュメントをアップロードした場合は無視されます。サポートされている IOC 属性のリストについては、『Cisco Endpoint IOC Attributes guide』を参照してください。

### エンドポイント IOC のアクティブ化

アップロードした新しいエンドポイント IOC は、有効であればすべてデフォルトでアクティブになります。[インストールされたエンドポイント IOC（Installed Endpoint IOCs）] ページで、それぞれの横にある [アクティブ（Active）] チェックボックスをクリックすることによって、個々のエンドポイント IOC をアクティブまたは非アクティブにすることができます。現在のビュー内のすべてのエンドポイント IOC をアクティブにする場合は、[すべてをアクティブ化（Activate All）] チェックボックスをクリックします。

また、[カテゴリ（Categories）]、[グループ（Groups）]、および [キーワード（Keywords）] の各フィルタを使用して特定のエンドポイント IOC を表示してから、[すべてをアクティブ化（Activate All）] を使用してそれらをアクティブまたは非アクティブにすることもできます。[すべて（All）]、[アクティブ（Active）]、[非アクティブ（Inactive）]、[有効（Valid）]、および [無効（Invalid）] の各ボタンを使用して、一覧表示された IOC ドキュメントのビューをすばやく変更することもできます。これは、エンドポイント IOC の大量のセットをソートしたり、特定の IOC のみをスキャンしたりする場合に便利です。

## スキャンの開始

コンピュータを個別にスキャンしてエンドポイント IOC を照合することも、同じポリシーを利用しているグループ内のすべてのコンピュータをスキャンすることもできます。

### ポリシーによるスキャン

ポリシーでスキャンするには、[アウトブレイク制御（Outbreak Control）] > [エンドポイント IOC - スキャンを開始（Endpoint IOC - Initiate Scan）] に移動します。スキャンを追加する [ポリシー（Policy）] を選択します。選択したポリシーを利用しているすべてのグループのすべてのコンピュータが同じエンドポイント IOC スキャンを実行します。

**重要事項：**コンピュータを個別にスキャンするには、「コンピュータ別のスキャン」を参照してください。

[スキャン実行日時（Run Scan On）] は、スキャンを開始する日付と時刻です。時刻は、Cisco Secure Endpoint コネクタが動作しているコンピュータの現地時刻です。

[フラッシュスキャン（Flash Scan）] または [フルスキャン（Full Scan）] を実行できます。どちらも同様のサブセットをスキャンしますが、フル スキャンはより包括的です。そのため IOC によっては、フラッシュ スキャンがチェックしない場所で一致を検索してもフラッシュ スキャンをトリガーしない場合があります。

次の情報は、[フラッシュスキャン（Flash Scan）] と [フルスキャン（Full Scan）] の両方でチェックされます。

- 実行中のプロセス
- ロードされた DLL
- サービス
- 購入要因
- Task Scheduler
- System information
- ユーザー アカウントの情報
- ブラウザ履歴とダウンロード
- Windows イベント ログ
- ネットワークと DNS の情報

[フルスキャン（Full Scan）] では以下の情報もチェックされます。

- ディスク上のハイブを使用している Windows レジストリ全体
- ファイル システム上のすべてのファイルとディレクトリ
- システム復元ポイント

**警告：**フル スキャンの実行には、時間がかかるうえ、大量のリソースが消費されます。大量のファイルが存在するエンドポイントでフル スキャンを実行すると数日かかる場合があります。フル スキャンは、夜間や週末などの非活動期間にのみスケジュールする必要があります。コネクタで初めてフルスキャンを実行する際には、システムがカタログ化されるため、通常のフルスキャンよりも時間がかかります。

フルスキャンを選択する場合は、スキャンの前に完全なカタログ化を実行するか、最後のスキャンより後の変更のみをカタログ化するかも選択できます（Cisco Secure Endpoint Windows コネクタ 4.4 以降でのみ選択可能）。また、カタログ化を実行せずにスキャンすることもできます。完了に最も時間がかかるのは完全なカタログ化であり、所要時間が最も少ないのはカタログ化を伴わないスキャンです。変更のみをカタログ化する場合は、最後のフル カタログ以降にファイルシステムに行われた変更のみがカタログ化されます。スキャンにかかる合計時間は、カタログ化する変更の数に応じて異なります。

**重要：**コンピュータのフル カタログ化を実行しないで、スキャン前にカタログ化をしないように選択した場合は、何もスキャンされません。

### コンピュータによるスキャン

[管理（Management）] > [コンピュータ（Computers）] では、単一のコンピュータ上でエンドポイント IOC スキャンを実行できます。スキャンするコンピュータを選択してから、[スキャン（Scan）] ボタンをクリックします。

ダイアログでエンドポイント IOC スキャン エンジンを選択し、フラッシュ スキャンとフル スキャンから選択します。ポリシー スキャンと同様に、フル スキャンの実行時もコンピュータを再カタログ化できます。

[スキャンの開始（Start Scan）] をクリックすると、次のハートビート間隔でコネクタがエンドポイント IOC スキャンを開始します。

## スキャンの概要

[スキャンの概要（Scan Summary）] ページには、Cisco Secure Endpoint 展開でスケジュール設定されたすべてのエンドポイント IOC スキャンが一覧表示されます。スケジュール設定されたポリシー スキャンと、個別のコンピュータ スキャンの両方が表示されます。[すべての変更を表示（View All Changes）] リンクを使用して、エンドポイント IOC スキャンのみが表示される監査ログのフィルタ処理されたビューを表示できます。特定のスキャンの横にある [変更の表示（View Changes）] をクリックすると、そのスキャンの記録だけ確認できます。

ポリシー スキャンの場合は、ポリシー名と共にスケジュールされた日付と時刻が表示されます。コンピュータ スキャンの場合は、コンピュータの名前が、スキャンの開始日と時刻とともに表示されます。[終了（Terminate）] ボタンをクリックすることによって、スキャンを停止できます。

**重要事項：**スキャンの停止は、コネクタにポリシーの更新を送信することで実行されます。コネクタは、次のハートビート間隔で更新されたポリシーを受信した場合にだけスキャンを停止します。

ポリシーによる別のスキャンをスケジュールするには、[新しいスキャン（New Scan）] ボタンをクリックします。これにより、[スキャンを開始（Initiate Scan）] ページが表示されます。

エンドポイント IOC スキャンの結果が、スキャンされた各コンピュータの一致する IOC トリガーとともに Cisco Secure Endpoint ダッシュボードの [イベント（Events）] タブに表示されます。

# 第 15 章

# 自動化されているアクション

[自動化されているアクション（Automated Actions）] ページでは、コンピュータで指定されたイベントが発生したときに自動的にトリガーされるアクションを設定できます。このページには、メインメニューの [アウトブレイクコントロール（Outbreak Control）] > [自動化されているアクション（Automated Actions）] からアクセスできます。

**重要：**自動アクションでは、そのアクションをサポートしているコネクタでのみアクションを実行できます。最小要件を満たしていない（またはポリシーで目的の機能が有効になっていない）コネクタやオペレーティングシステムの場合、自動アクションはトリガーされません。

## [自動化されているアクション（Automated Actions）] タブ

[自動化されているアクション（Automated Actions）] タブでは、各アクションの設定を調整し、それらをアクティブまたは非アクティブに設定することができます。

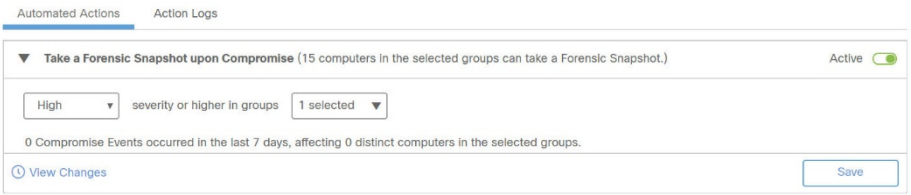
自動アクションは、設定された順序では発生しません。一部の自動アクションは、トリガーイベントが複数のアクションに対する条件を満たしていても、他のアクションより先に実行される場合があります。たとえば、隔離されたコンピュータは、隔離されている間は別のグループに移動できません。

## フォレンジック スナップショットの自動アクション

**重要事項：**フォレンジック スナップショットの自動アクションは、Cisco Secure Endpoint Advantage を使用しているお客様のみ利用できます。Orbital Advanced Search をエンドポイントで有効にしないと、フォレンジック スナップショットを取ることはできません。「Orbital Windows の要件」および「Orbital macOS の要件」を参照してください。

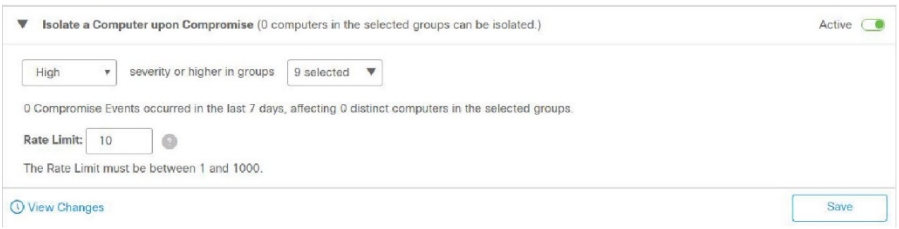
侵害が発生したときにコンピュータのフォレンジック スナップショットを取るように自動アクションを設定できます。

自動アクションを有効にするには、まず、侵害の重大度を選択します。選択した重大度以上のイベントが発生すると、自動アクションがトリガーされます。次に、アクションを適用するグループを設定し、[保存（Save）] をクリックします。アクションを作成したら、それを [アクティブ（Active）] または [非アクティブ（Inactive）] に設定します。




## エンドポイント隔離の自動アクション

侵害が発生したときにコンピュータを隔離するように自動アクションを設定できます。隔離は、Windows コネクタ 7.0.5 以降および Mac コネクタ 1.21.0 以降でサポートされています。




自動アクションを有効にするには、まず、侵害の重大度を選択します。選択した重大度以上のイベントが発生すると、自動アクションがトリガーされます。次に、アクションを適用するグループを設定し、隔離を許可するコンピュータの数のレート制限（最大 1000）を設定します。[保存（Save）] をクリックしてアクションを作成します。アクションを作成したら、それを [アクティブ（Active）] または [非アクティブ（Inactive）] に設定します。

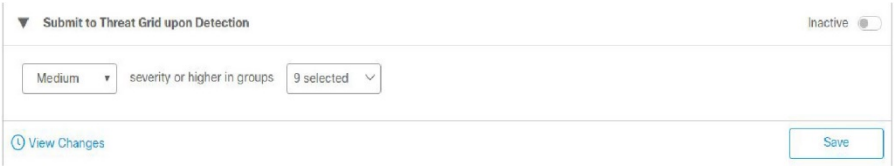
レート制限により、誤検出から保護されます。レート制限機能は、24 時間単位での隔離の総数を調べます。隔離の数が制限を超えると、それ以上の隔離はトリガーされなくなります。24 時間単位での侵害イベントの数が制限値を下回ると、または自動的に隔離されたコンピュータで隔離を停止すると、コンピュータは再び隔離されるようになります。

**重要：**組織内のエンドポイントの数、侵害の頻度、誤検出に対する許容度はすべて、レート制限を選択する際に考慮する必要がある要素です。小さい数値で始めることをお勧めします。

隔離の一括停止の詳細については、[アクションログ（Action Logs）] タブを参照してください。

## Cisco Secure Malware Analytics への送信の自動アクション

検出発生時のファイル分析のためにファイルを Cisco Secure Malware Analytics に送信するように自動アクションを設定できます。




自動アクションを有効にするには、まず、侵害の重大度を選択します。選択した重大度以上のイベントが発生すると、自動アクションがトリガーされます。次に、アクションを適用するグループを設定します。[保存（Save）] をクリックしてアクションを作成します。アクションを作成したら、それを [アクティブ（Active）] または [非アクティブ（Inactive）] に設定します。

対応する検疫イベントがある場合、[受信トレイ（Inbox）] タブでイベントが解決済みとしてマークされている場合、または誤検出であると判断された場合、自動アクションによって分析のためにファイルが送信されることはありません。また、分析のために組織によってすでに送信されたファイルは、再送信されません。

分析のために送信できるファイルの数は、[組織の設定（Organization Settings）] の [Cisco Secure Malware Analytics API] の [自動分析の日単位の送信数（Daily submissions for Automatic Analysis）] の設定によって決まります。ファイルは、**分析用の VM イメージ**で指定されたオペレーティングシステムを使用して分析されます。

ファイル分析サンドボックスには次の制限があります。

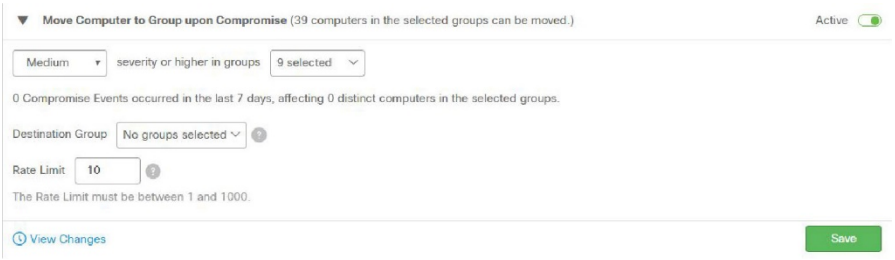
- ファイル名は 59 文字の Unicode 文字列に制限されます。
- ファイルは 16 バイト以上 20 MB 以下にする必要があります。
- サポートされているファイルタイプは、.exe、.dll、.jar、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、.vbn、.sep、および .swf です。ファイルはパスワードで保護しないでください。

**重要事項：**ファイルがコンピュータ上の別の AV 製品によって隔離されている場合、そのファイルを分析のために自動アクションによって送信することはできません。AV 製品の検疫場所からファイルを取得し、ファイル分析のランディングページから手動でファイルを送信する必要があります。

ファイル分析が完了すると、ファイル分析のランディングページで分析レポートが利用可能になります。分析を表示するには、シングルサインオン（Security Cloud Sign-on など）を使用するか、二要素認証を有効にする必要があります。

## グループへの移動の自動アクション

[グループに移動（Move to Group）] アクションがトリガーされると、コンピュータが現在のグループから別のグループに移動されます。これにより、侵害を受けたコンピュータを、より積極的なスキャンおよびエンジン設定のポリシーが適用されたグループに移動して、侵害を修復できます。




自動アクションを有効にするには、まず、侵害の重大度を選択します。選択した重大度以上のイベントが発生すると、自動アクションがトリガーされます。次に、アクションを適用するグループと移動先のグループを設定し、移動を許可するコンピュータの数のレート制限（最大は 1000）を設定します。[保存（Save）] をクリックしてアクションを作成します。アクションを作成したら、それを [アクティブ（Active）] または [非アクティブ（Inactive）] に設定します。

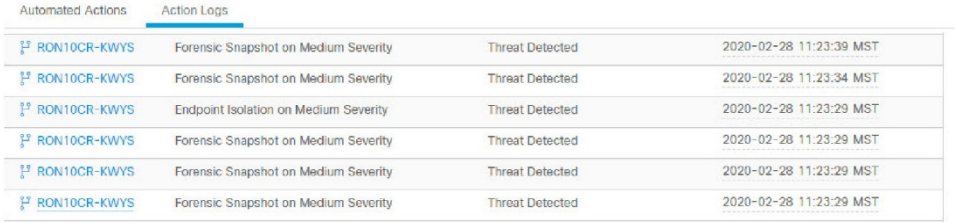
**重要：**他のアクションに含まれているコンピュータを移動する場合は、移動先グループにエンドポイント分離などの他の機能が有効になっており、グループが他のアクションに含まれていることを確認してください。

レート制限により、誤検出から保護されます。レート制限機能は、24 時間単位でのグループ移動の総数を調べます。移動の数が制限を超えると、それ以上の移動はトリガーされなくなります。24 時間単位での侵害イベントの数が制限値を下回ると、コンピュータは再び移動されるようになります。

**重要：**組織内のエンドポイントの数、侵害の頻度、誤検出に対する許容度はすべて、レート制限を選択する際に考慮する必要がある要素です。小さい数値で始めることをお勧めします。

# [アクションログ（Action Logs）] タブ

[アクションログ（Action Logs）] タブには、トリガーされた自動アクション、トリガーされたコンピュータおよび日時が表示されます。[デバイストラジェクトリ（Device Trajectory）] ページに移動するにはコンピュータを選択します。




[アクションログ（Action Logs）] タブには [すべての隔離を停止（Stop All Isolations）] ボタンがあります。誤検出があった場合またはすべてのインシデントが解決された場合は、このボタンを使用できます。ボタンをクリックすると、Cisco Secure Endpoint は、自動アクションによって隔離されているか、自動アクションによって隔離が保留されているすべてのコネクタで隔離の停止を試みます。最初に隔離をトリガーした問題が解決していない場合は、エンドポイント隔離の自動アクションを一時的に調整または無効化し、再びトリガーされないようにする必要があります。

# 第 16 章

# 検索

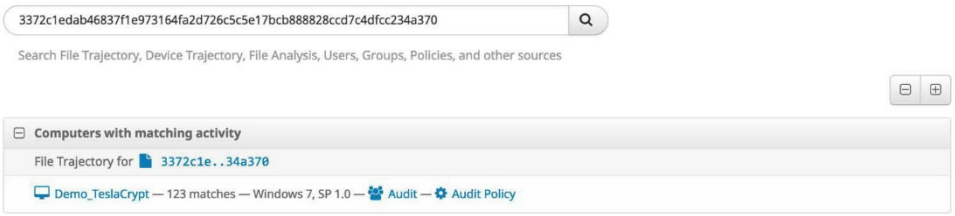
[検索（Search）] を使用すると、Cisco Secure Endpoint 展開に関する情報を検索できます。ファイル、ホスト名、URL、IP アドレス、デバイス名、ユーザー名、ポリシー名などの用語を使用して検索できます。検索機能は、ファイルトラジェクトリ、デバイストラジェクトリ、ファイル分析などのソースから結果を返します。検索機能にアクセスするには、[分析（Analysis）] > [検索（Search）] に移動するか、Cisco Secure Endpoint コンソールで SHA-256 やファイル名などのさまざまな要素を右クリックし、コンテキストメニューから [検索（Search）] を選択します。

**ヒント：**また、任意のページのメニュー バーからも検索機能にアクセスできます。

## ハッシュ検索

ファイルの SHA-256 値を入力することによって、そのファイルを監視していたデバイスを特定できます。ファイルを [検索（Search）] ボックスにドラッグすると、SHA-256 値が自動的に計算されます。ファイルの MD5 または SHA-1 値しか判明していない場合、検索機能は、それと対応する SHA-256 を照合し、その SHA-256 を探しようと試みます。

結果には、該当ファイルを確認したコネクタのファイル分析、ファイルトラジェクトリ、およびデバイストラジェクトリへのリンクを含めることができます。



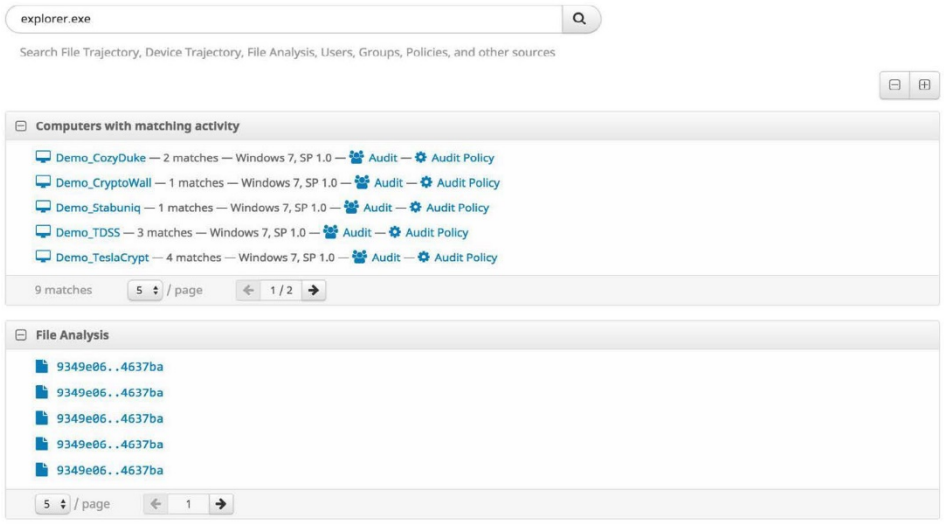

# 文字列検索

文字列を入力して検索することによって、さまざまなソースから一致するものを見つけることができます。文字列検索には、以下を含めることができます。

- ファイル名
- ファイルパス
- 検出名
- プログラム名
- プログラムバージョン
- ファイルバージョン
- Cisco Secure Endpoint ポリシー名
- Cisco Secure Endpoint グループ名
- デバイス名（プレフィックス一致のみ）
- デバイスのシリアル番号（iOS デバイス）
- 侵害の兆候の名前、説明、戦術、または手法

`.exe` や `.pdf` などの正確なファイル拡張子による検索を実行して、それらの拡張子を持つすべての観察対象ファイルを見つけることもできます。

Cisco Secure Endpoint 展開内で一致するユーザーを見つけるには、正確な電子メールアドレスまたはユーザー名を入力します。

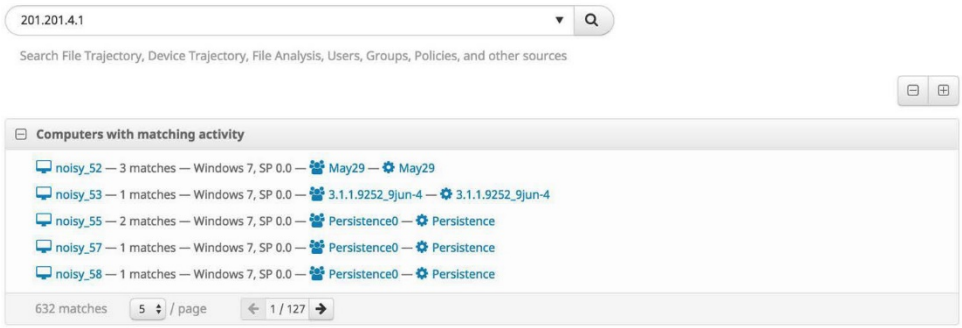



# ネットワーク アクティビティ検索

IP アドレス、ホスト名、および URL の検索を実行することもできます。

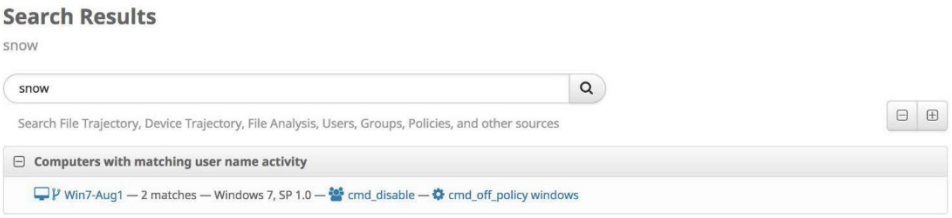
IP アドレス検索は、ドット付き 10 進表記で 32 ビットすべてを正確に指定する必要があります。IP アドレス検索の結果には、特定アドレスにアクセスしていたデバイスや、特定 IP を観察していたデバイスを含めることができます。

ホスト名検索と URL 検索では、ホスト名またはサブドメインの完全一致も使用できます。これらの検索では、コネクタが該当ホストからダウンロードしたファイルと該当ホストにアクセスしていたコネクタが返されます。




# ユーザー名検索

「ユーザー名」で検索すると、検索対象のユーザーがアクティビティを開始したエンドポイントの一覧を取得できます。検索結果には、名前が一致する組織のユーザーがすべて含まれます。「ユーザー名@ドメイン」で検索すると、完全一致のあるエンドポイントのみが返されます。




検索結果でコンピュータ名をクリックすると、そのコンピュータのデバイス トラジェクトリ や、検索したユーザー名に関連するイベントを確認できます。

**重要事項：**ユーザー名で検索するには、ポリシーで [イベント内のユーザー名を送信（Send User Name in Events）] および [コマンドラインキャプチャ（Command Line Capture）] を有効にする必要があります。

# 第 17 章

# ファイル分析

ファイル分析を使用すると、Cisco Secure Endpoint ユーザーが実行ファイルをサンドボックス環境にアップロードでき、ファイルは自動的にキューに入り、実行されて分析されます。[ファイル分析（File Analysis）] ページでは、実行可能ファイルの SHA-256 を検索して、そのファイルがすでに分析済みかどうかを確認することもできます。ファイルがすでに分析済みの場合は、その分析レポートを入手して表示できます。この機能は Cisco Secure Malware Analytics（以前の Cisco Threat Grid）で提供されます。

[ファイル分析（File Analysis）] ページに移動するには、[分析（Analysis）] > [ファイル分析（File Analysis）] の順にクリックします。

## ファイル分析のランディング ページ

[ファイル分析（File Analysis）] に移動すると、分析用に送信したファイルのリストが表示されます。ファイルを送信していない場合は、Cisco Secure Malware Analytics ユーザーが送信したファイルが表示される [グローバルファイル（Global Files）] タブが表示されます。このページで、分析用にファイルを送信したり、ファイルを SHA-256 またはファイル名で検索したり、送信したファイルのリストを表示したりできます。ファイルを検索した場合、[グローバルファイル（Global Files）] タブには、自分が Cisco Secure Malware Analytics に送信したファイルと他のユーザーが送信したファイルがすべて表示されます。[自分のファイル（Your Files）] タブには自分が分析用に送信したファイルの結果のみが表示されます。分析の結果を表示するには、ファイル名または [レポート（Report）] ボタンをクリックします。

**重要：**ファイル分析レポートは、Microsoft Internet Explorer 11 以上、Mozilla Firefox 14 以上、Apple Safari 6 以上、または Google Chrome 20 以上で最適に表示されます。

探していたファイルがまだ分析されていない場合は、そのファイル（最大 20 MB）を分析用にアップロードすることができます。アップロードするには、[ファイルを送信（Submit File）] をクリックし、[参照（Browse）] ボタンを使用してアップロードするファイルを選択し、実行する仮想マシンのオペレーティング システム イメージを選択し、[アップロード（Upload）] ボタンをクリックします。ファイルがアップロードされてから分析が可能になるまでは、システム負荷に応じて、約 30 ~ 60 分かかります。

**重要事項：**1 日に分析用に送信できるファイル数には制限があります。デフォルトでは、[組織の設定（Organization Settings）] ページでカスタムの Cisco Secure Malware Analytics API キーを入力していない限り、1 日に送信できるファイル数は 100 です。利用可能な送信数は、[送信（Submission）] ダイアログに表示されます。

ウイルス対策製品で検疫済みのファイルを分析用に送信する場合は、その前にファイルを復元する必要があります。ウイルス対策製品によっては、ファイルが検疫時に暗号化されるため、ファイルを分析可能な形式に復元するための特定のツールや手順が必要な場合もあります。詳細については、ウイルス対策ソフトウェア ベンダーのマニュアルを参照してください。

ファイル分析サンドボックスには次の制限があります。

- ファイル名は 59 文字の Unicode 文字列に制限されます。
- ファイルは 16 バイト以上 20 MB 以下にする必要があります。
- サポートされているファイルタイプ
  は、.exe、.dll、.jar、.pdf、.rtf、.doc(x)、.xls(x)、.ppt(x)、.zip、
  .vbn、.sep、および .swf です。ファイルはパスワードで保護しないでください。

ファイルが分析されたら、エントリを展開して侵入兆候 に対する脅威スコアおよびスコアを確認できます。

## 脅威の分析

特定のファイルの分析はいくつかのセクションに分割されます。セクションによっては、すべてのファイル タイプに使用できない場合があります。サンドボックスで実行されたオリジナルのサンプル（実行可能ファイル）をダウンロードすることもできます。これは、実行ファイルの詳細な分析を実行する場合に便利であり、ネットワーク上の感染を制御または削除するためのカスタム検出：簡易およびカスタム検出：高度リストの作成にも利用できます。

**警告：**ファイル分析からダウンロードされたファイルの多くは実際のマルウェアのため、極めて慎重に取り扱う必要があります。

マルウェアを分析すると実行時のビデオもキャプチャされます。このビデオにより、マルウェア感染時の動作を目で確認できます。また、たとえば大量感染が発生した場合にユーザー教育キャンペーンで使用したり、セキュリティ アナリストが脅威の動作のスクリーンショットをネットワーク ユーザーに送信して症状を警告したりする用途でも活用できます。フィッシングのような手の込んだソーシャル エンジニアリング攻撃（悪意のある偽のウイルス対策や、スケアウェアでよく見られる偽のウイルス対策アラートなど）への警告目的でも使用できます。

また、[PCAP のダウンロード（Download PCAP）] をクリックしてバイナリを分析している間に収集されたネットワーク キャプチャ全体をダウンロードすることもできます。このネットワーク キャプチャは、PCAP 形式であり、Wireshark などのネットワーク トラフィック分析ツールで開くことができます。セキュリティ アナリストは、このネットワーク キャプチャ ファイルを利用して、この脅威に関連したアクティビティを検出またはブロックするための堅牢な IDS シグニチャを作成できます。

マルウェアが実行中に他のファイルを作成した場合は、それらが [アーティファクト（Artifacts）] に表示されます。個々のアーティファクトをダウンロードして別の分析を実行できます。

## メタデータ

分析に関する基本情報が分析レポートの最上部に表示されます。この情報には、以下を含む、分析用送信の基本的な特性が含まれています。


Analysis Report

| | |
|---|---|
| ID | 31a15d41803231df445cbe1978553085 |
| OS | 2600.xpsp.080413-2111 |
| Started | 12/26/14 18:08:00 |
| Ended | 12/26/14 18:14:14 |
| Duration | 0:06:14 |
| Sandbox | bubonia (pilot-d) |
| Filename | 0b384dc42e8d31e515739e30e3e5600d9546b0941f151daec8aba4ac5cb674b8.exe |
| Magic Type | PE32 executable (GUI) Intel 80386, for MS Windows |
| Analyzed As | exe |
| SHA256 | 0b384dc42e8d31e515739e30e3e5600d9546b0941f151daec8aba4ac5cb674b8 |
| SHA1 | 4d70fde118949a6cf268658382f8b7b6875ed549 |
| MD5 | f09d1e4f5c5d97128ef68e2c71c218ad |

Warnings

Executable Failed Integrity Check

[ID]：分析用に送信されたサンプルごとに割り当てられる一意の識別子。

[OS]：サンプルが分析されたときに使用されたオペレーティング システム イメージ。

[開始（Started）]：分析が開始された日付と時刻。

[終了（Ended）]：分析が終了した日付と時刻。

[時間（Duration）]：分析が完了するまでに要した時間。

[サンドボックス（Sandbox）]：分析中に使用されたサンドボックスを識別します。

[ファイル名（Filename）]：分析用に送信されたサンプルファイルの名前または URL サンプルの送信時に入力されたファイル名。

[Magicタイプ（Magic Type）]：このフィールドは、Cisco Secure Malware Analytics によって検出された実際のファイルタイプを示します。

[分析対象（Analyzed As）]：サンプルが URL として、またはファイルして分析されたかを示します（ファイルタイプの指定による）。

[SHA256]：SHA-256 暗号ハッシュ関数の出力。

[SHA1]：SHA1 暗号ハッシュ関数の出力。

[MD5]：MD5 暗号ハッシュ関数の出力。

[警告（Warnings）]：有害な可能性のあるアクティビティの概要。

## 侵入兆候

分析レポートには、Cisco Secure Malware Analytics によって生成された侵入兆候の概要が表示されます。この指標は、悪意のある（または疑わしい）アクティビティを示す動作を簡単に説明したものです。Cisco Secure Malware Analytics では、マルウェアクティビティの分析完了後の分析中に侵入兆候が生成されます。


動作指標には、その指標を生成したアクティビティの詳細な説明が含まれます。また、マルウェア作成者がその特定のテクニックを利用した理由に加えて、分析中に指標をトリガーした特定のコンテンツに関する情報も含まれます。

### 脅威スコア

分析レポートの [侵入兆候（Behavioral Indicators）] セクションの一番上の行には、送信内容に悪意があるかどうかの一般的な指標として使用可能な全体的な脅威スコアが表示されます。

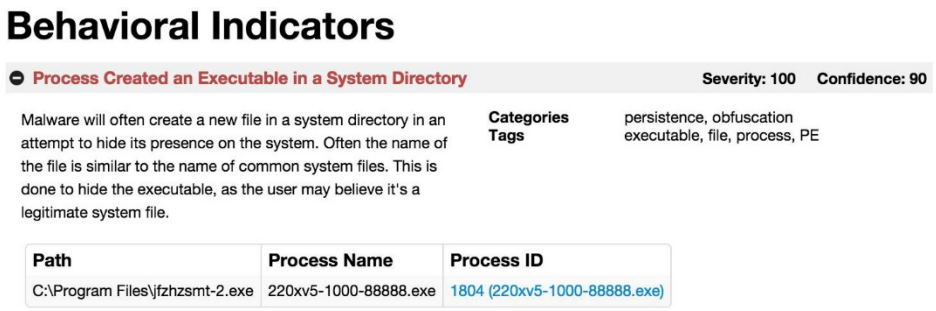
脅威スコアの計算に使用されるアルゴリズムでは、個別の信頼度スコアやシビラティ（重大度）スコアと組み合わせた侵入兆候の数とタイプなどの、多様な要因が考慮されます。

侵入兆候は、潜在的シビラティ（重大度）に基づいて色分けされた優先度（最も深刻な脅威が一番上）に表示されます。

- 赤色：悪意のあるアクティビティの高い可能性を示します。
- 橙色：疑わしいアクティビティで、アナリストは提出物を慎重に評価する必要があります。
- 灰色：これらのアクティビティが、悪意のあるソフトウェアによって利用されることは通常ないが、アナリストが独自の結論を導き出すのに役立つ新たな指標を提供することを示します。

## 侵入兆候の詳細

各侵入兆候の横にある [+] をクリックすることによって、その詳細情報を表示できます。詳細情報は、侵入兆候のタイプによって異なります。特定のタイプのアラートに関連するまたは該当する情報が画面に表示されます。




[説明（Description）]：兆候が疑わしい理由の説明。

[カテゴリ（Categories）]：特定の侵入兆候が脅威またはマルウェアのファミリに関連付けられているかどうかを示します。この情報は、関連するマルウェアを検索するときに便利です。

[タグ（Tags）]：特性とアクティビティを要約するために侵入兆候ごとに自動的に割り当てられるタグです。

分析されたサンプルのタイプに応じて、次のフィールドが含まれます。

[アドレス（Address）]：プロセスのアドレス空間。

[ウイルス対策製品（Antivirus Product）]：潜在的に悪意のあるサンプルとして、フラグを設定したウイルス対策製品の名前。

[ウイルス対策の結果（Antivirus Result）]：フラグが設定されたウイルス対策製品の結果が表示されます。

[アーティファクトID（Artifact ID）]：サンプルによって生成されたアーティファクトのID。ID 上のリンクをクリックすると、そのアーティファクトの分析レポートのセクションが表示されます。

[コールバックアドレス（Callback Address）]：侵入兆候で使用されるコールバック検証アドレス。

[コールバックRVA（Callback RVA）]：コールバックの相対仮想アドレス。

[フラグ（Flags）]：侵入兆候によって生成されたフラグのリスト。

[md5]：ファイルの MD5 チェックサム。

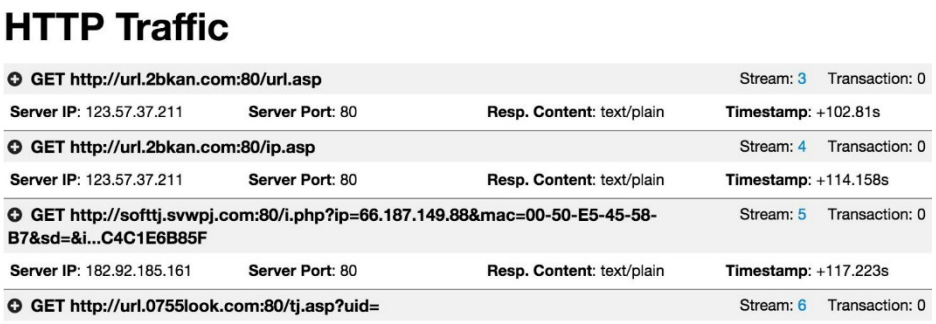
[パス（Path）]：実行中に作成または変更されたファイルのフルパス。

[プロセスID（Process ID）]：実行中に作成されたプロセスのプロセス ID。

[プロセス名（Process Name）]：実行中に作成されたプロセスの名前。

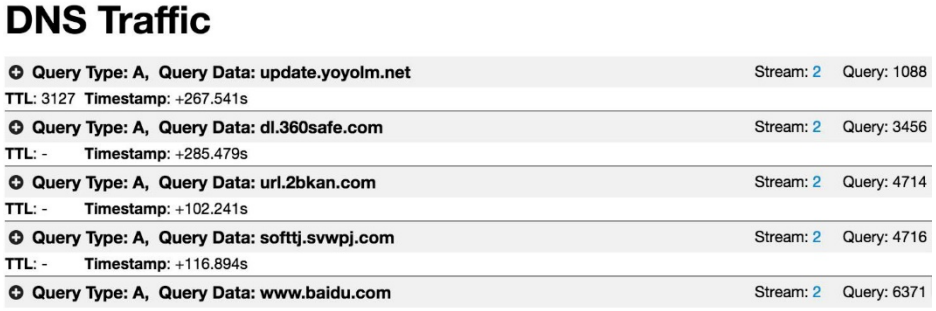
## HTTP トラフィック

Cisco Secure Malware Analytics でサンプル分析中に HTTP トラフィックが検出されると、各 HTTP 要求および応答の詳細（使用された HTTP コマンドなど）を示すアクティビティが表示されます。




## DNS トラフィック

Cisco Secure Malware Analytics で分析中に外部ホスト名の IP アドレスに対する DNS クエリが検出されると、このセクションに結果が表示されます。

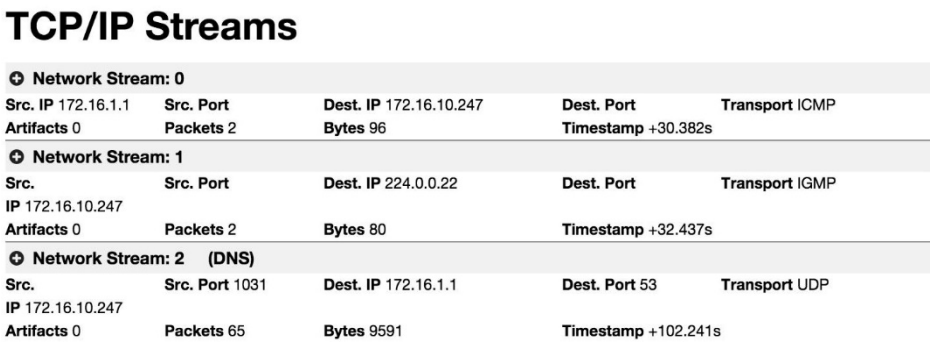



## TCP/IP ストリーム

分析レポートの [TCP/IP ストリーム（TCP/IP Streams）] セクションには、提出物によって起動されたすべてのネットワーク セッションが表示されます。

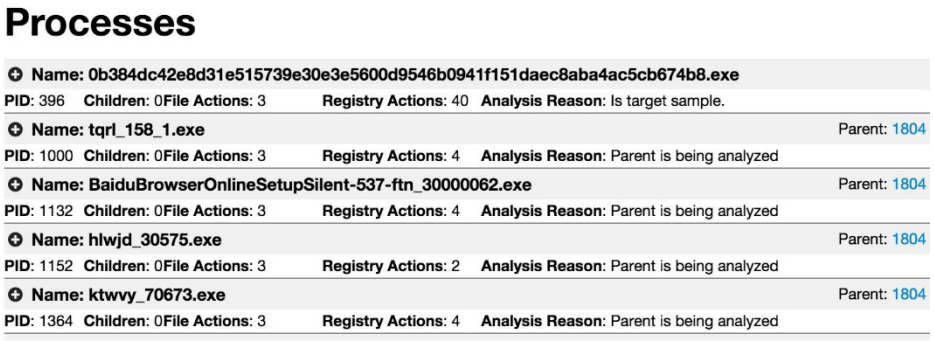
送信元 IP アドレスの上にカーソルを移動すると、分析中に Cisco Secure Malware Analytics によって検出されたネットワークストリームのすべての送信元ネットワーク IP アドレスが一覧表示されたポップアップが表示されます。

ネットワーク ストリームのいずれかをクリックすると、該当するネットワーク ストリームを含む Web ページが開きます。



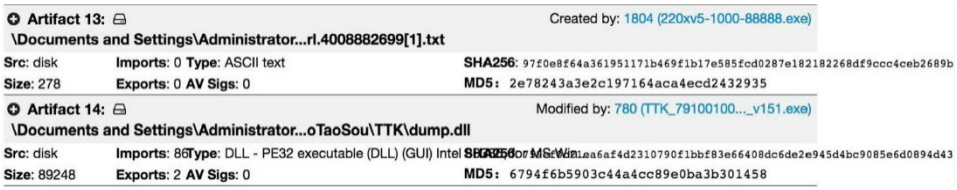

## プロセス

送信分析中に何らかのプロセスが起動された場合、Cisco Secure Malware Analytics によってこのセクションにプロセスが表示されます。プロセスの横にある [+] アイコンをクリックすると、そのセクションが展開して、詳細情報にアクセスできます。




## アーティファクト

送信分析中に何らかのアーティファクト（ファイル）が作成された場合、Cisco Secure Malware Analytics によって各アーティファクトに関する概要情報が表示されます。アーティファクトの横にある [+] アイコンをクリックすると、そのセクションが展開して、詳細情報にアクセスできます。

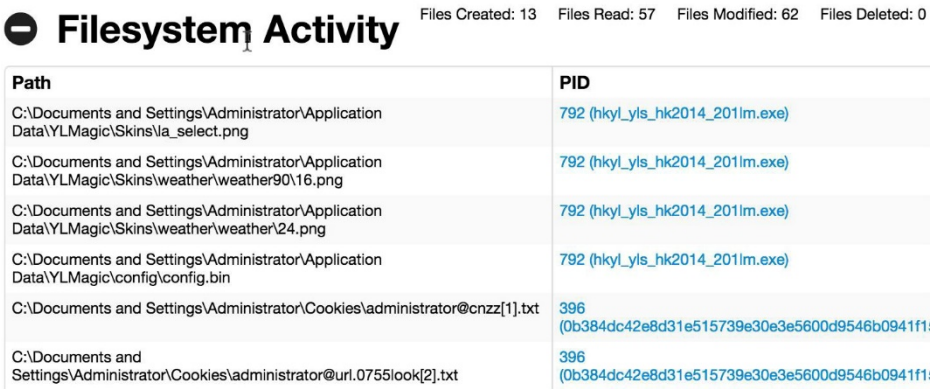



## レジストリ アクティビティ

分析によってレジストリに対する変更が検出された場合、Cisco Secure Malware Analytics によってこのセクションに変更内容が表示されます。レジストリ アクティビティ レコードの横にある [+] アイコンをクリックすると、そのセクションが展開して、詳細情報にアクセスできます。


## ファイル システム アクティビティ

送信分析中に何らかのファイル システム アクティビティ（ファイルの作成、変更、または読み取り）が検出された場合、Cisco Secure Malware Analytics によってアクティビティ情報の要約が表示されます。ファイル システム レコードの横にある [+] アイコンをクリックすると、そのセクションが展開して、詳細情報にアクセスできます。



# 第 18 章

# トラジェクトリ

トラジェクトリには、複数のコンピュータ全体、または単一のコンピュータやデバイスにおける Cisco Secure Endpoint 展開内のアクティビティが表示されます。

## ファイル トラジェクトリ

[ファイルトラジェクトリ（File Trajectory）] には、環境内でファイルが最初に観察されてから最後に観察されるまでのライフ サイクルと、ネットワーク内でその影響を受けていたすべてのコンピュータが表示されます。該当する場合は、ネットワークに脅威をもたらした親が表示されます。これには、その脅威によって作成または実行されたすべてのファイルが含まれます。ファイルのトラジェクトリを通して実行されたアクションは、コンピュータ上のウイルス対策ソフトウェアが無効にされた後も表示され続けます。

ファイル トラジェクトリは、環境内で記録された約 9,000,000 の最新のファイル イベントを保存できます。ファイルがイベントをトリガーすると、そのファイルが別のイベントをトリガーするまで一定期間キャッシュされます。キャッシュ期間はファイルの分類によって、以下のように異なります。

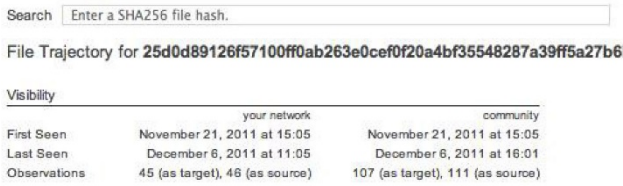
- クリーン ファイル：7 日間
- 不明なファイル：1 時間
- 悪意のあるファイル：1 時間

[ファイルトラジェクトリ（File Trajectory）] には次のファイル タイプが表示されます。

- 実行可能ファイル

- ポータブル ドキュメント フォーマット（PDF）ファイル
- MS キャビネット ファイル
- MS Office ファイル
- アーカイブ ファイル
- Adobe Shockwave Flash
- プレーン テキスト ファイル
- リッチ テキスト ファイル
- スクリプト ファイル
- インストーラ ファイル

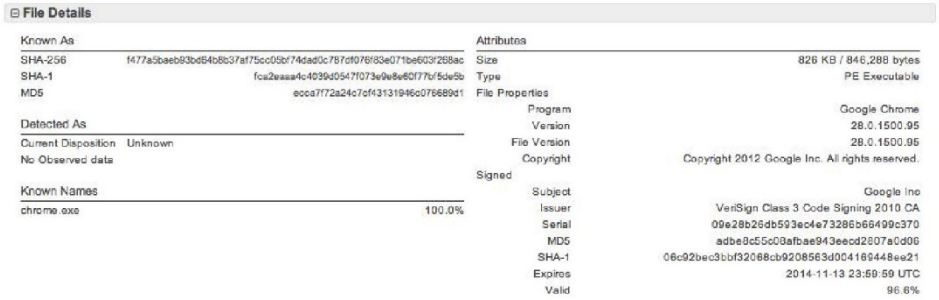
[可視性（Visibility）] にはネットワーク内にある問題のファイルの [最初の確認日時（First Seen）]、[最後の確認日時（Last Seen）]、および総観察回数が含まれます。[観察結果（Observations）] には、問題のファイルがアクティビティのソースだった回数とアクティビティのターゲットだった時期の両方が表示されます。総観察回数には、各エンドポイント上における同一ファイルによる重複インスタンスが含まれる場合もあります。




[エントリポイント（Entry Point）]：脅威が観察されたネットワーク上の最初のコンピュータを識別します。

[作成者（Created By）]：SHA-256 に基づいて、対象の脅威を作成したファイルを識別します。これには、ネットワークとすべての Cisco Secure Endpoint ユーザー間の両方でそのファイルによって脅威が作成された回数が含まれます。入手可能な場合は、ファイル名と製品情報も含まれます。この情報はファイル自体から抽出されたことに注意してください。悪意のあるファイル（赤色）に、それが正規のファイルであることを主張する情報が含まれている場合があります。

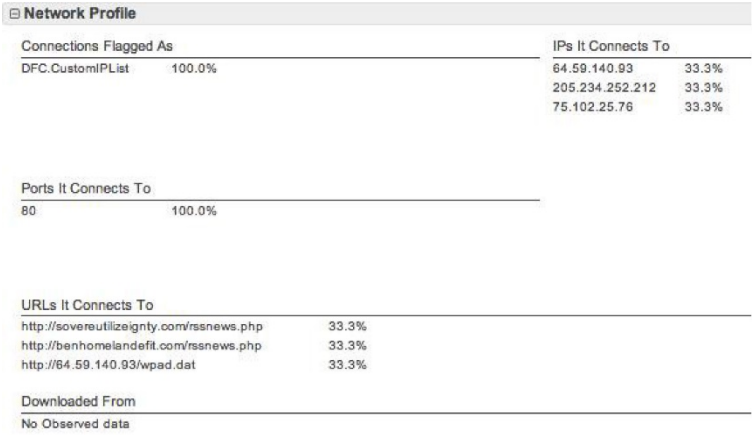

[ファイルの詳細（File Details）]：以下のような、問題のファイルに関する追加の情報が表示されます。




- [呼称（Known As）] には、ファイルの SHA-256、SHA-1、および MD5 ハッシュが表示されます。
- [属性（Attributes）] には、ファイルのサイズとタイプが表示されます。
- [既知の名前（Known Names）] には、そのファイルがネットワーク上を通過したときの名前が含まれます。
- [以下として検出（Detected As）] には、悪意のあるファイルの場合の検出名が表示されます。

> **重要事項：**脅威の名前の説明については、Cisco Secure Endpoint の命名規則を参照してください。

[ネットワークプロファイル（Network Profile）] には、問題のファイルが関与したネットワークアクティビティがすべて表示されます。セクションにエントリが存在しない場合でも、ファイルが参加できないとは限らず、ファイルが環境内に存在していても、コネクタによって参加が検出されなかった可能性もあります。コネクタでデバイス フローコリーションが有効になっていない場合、このセクションは空です。[ネットワークプロファイル（Network Profile）] の詳細は以下のようになります。




- [接続のフラグ名（Connections Flagged As）] には、IP ブロックリストエントリに対応するアクティビティが表示されます。

- [接続先の IP（IPs it Connects To）] には、ファイルが接続を開始した IP アドレスが列挙されます。
- [接続先のポート（Ports it Connects To）] には、ファイルからのアウトバウンド接続に関連付けられたポートが列挙されます。
- [接続先の URL（URLs it Connects To）] には、ファイルが接続を開始した URL が列挙されます。
- [ダウンロード元（Downloaded From）] には、対象のファイルのダウンロード元アドレスが一覧表示されます。

[トラジェクトリ（Trajectory）]：環境内で影響を受けた各コンピュータ上の脅威に関連した各アクションの日付と時刻が表示されます。


追跡されたアクションは、以下のボックスに表示されます。

| | |
|---|---|
|  | 無害なファイルがそれ自身をコピーした |
|  | 検出されたファイルがそれ自身をコピーした |
|  | 不明な分類のファイルがそれ自身をコピーした |
|  | 無害なファイルが作成された |
|  | 検出ファイルが作成された |
|  | 不明な分類のファイルが作成された |

| | |
|---|---|
|  | 無害なファイルが実行された |
|  | 検出されたファイルが実行された |
|  | 不明な分類のファイルが実行された |
|  | 無害なファイルが移動された |
|  | 検出されたファイルが移動された |
|  | 不明な分類のファイルが移動された |
|  | 無害なファイルがスキャンされた |
|  | 検出ファイルがスキャンされた |
|  | 不明な分類のファイルがスキャンされた |
|  | ファイルが TETRA または ClamAV によって有害と断定された |
|  | 無害なファイルが開かれた |
|  | 検出ファイルが開かれた |
|  | 不明な分類のファイルが開かれた |

アクションの周りに  二重丸が付いている場合は、対象のファイルがアクティビティのソースだったことを意味します。一重丸だけの場合は、そのファイルが別のファイルの影響を受けたことを意味します。

コンピュータ名をクリックすると、検査されたファイルの親アクションとターゲット アクションに関する詳細情報と SHA-256 が表示されます。

[トラジェクトリ（Trajectory）] 表示内のアクションアイコンのいずれかをクリックすると、判明しているファイル名やパスを含む追加の詳細情報を表示することもできます。


[イベント履歴（Event History）]：トラジェクトリで特定されたイベントごとの詳細なリストが表示されます。イベントはデフォルトで時系列順に表示されますが、任意の列でソートできます。


# デバイス トラジェクトリ

[デバイストラジェクトリ（Device Trajectory）] には、コネクタを展開した特定のコンピュータ上のアクティビティが表示されます。また、ファイル、ネットワーク、およびコネクタのイベント（ポリシーの更新など）が時系列順で追跡されます。また、侵害に先だってまたは侵害に続いて発生したイベントを可視化します。これには、親プロセス、リモート ホストへの接続、およびマルウェアによってダウンロードされた不明なファイルが含まれます。

デバイストラジェクトリでは、現在の環境内に 30 日分のファイルイベントを格納することができます。ファイルがイベントのトリガーとして使用されると、そのファイルが別のイベントのトリガーとして使用されるまで一定期間キャッシュされます。キャッシュ期間はファイルの分類によって異なります。

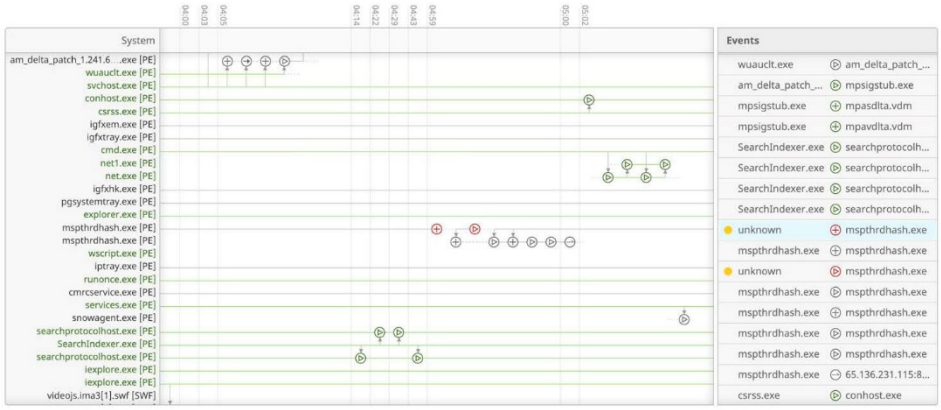
- クリーン ファイル：7 日間
- 不明なファイル：1 時間
- 悪意のあるファイル：1 時間

デバイス トラジェクトリには次のファイル タイプが表示されます。

- 実行可能ファイル
- ポータブル ドキュメント フォーマット（PDF）ファイル
- MS キャビネット ファイル
- MS Office ファイル
- アーカイブ ファイル
- Adobe Shockwave Flash
- プレーン テキスト ファイル
- リッチ テキスト ファイル

- スクリプト ファイル
- インストーラ ファイル

[デバイストラジェクトリ（Device Trajectory）] の縦軸には、コネクタによってコンピュータ上で確認されたファイルやプロセスのリストが表示され、横軸には時刻が表示されます。実行中のプロセスは実線の横線で表現され、その横線を起点としてそのプロセスが影響を与えた子プロセスとファイルが表示されます。ファイルイベントのリストは、デバイストラジェクトリの右側に表示されます。




**重要事項：**選択した行が画面外にある場合は、 または をクリックして戻ります。

イベントをクリックすると、その詳細が表示されます。


イベント詳細には、ファイル名、パス、親プロセス、ファイルサイズ、実行コンテキスト、およびファイルのハッシュが含まれます。悪意のあるファイルの場合、検出名、検出されたエンジン

ファイル、および検疫アクションも表示されます。ペイン内をスクロールして選択したイベントから離れた場合、そのイベントに戻るには、 をクリックします。

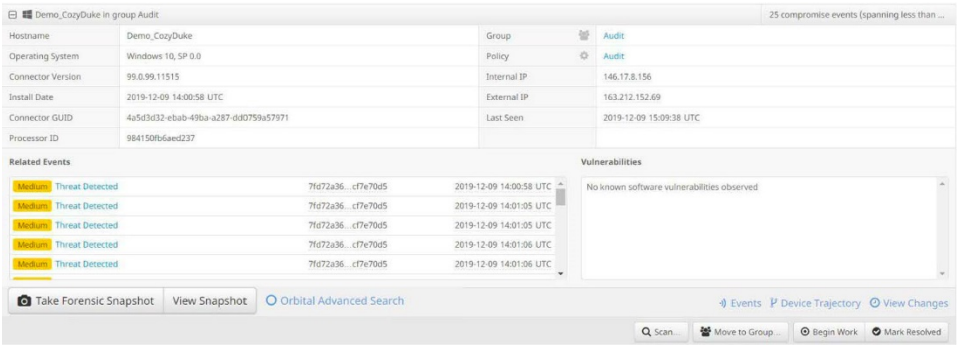
**重要事項：**脅威名の説明については、AMP 命名規則を参照してください。

ネットワーク イベントには、接続を試みているプロセス、宛先 IP アドレス、送信元ポートと宛先ポート、プロトコル、実行コンテキスト、ファイルのサイズと経過時間、プロセス ID と SID、およびファイルのハッシュが含まれます。悪意のあるサイトへの接続の場合は、検出名と実行されたアクションも表示されます。

Cisco Secure Endpoint コネクタイベントは、デバイストラジェクトリのシステムラベルの横に表示されます。コネクタイベントには、再起動、ユーザーが開始したスキャンと定期スキャン、ポリシーと定義の更新、コネクタの更新、およびコネクタのアンインストールが含まれます。

[デバイストラジェクトリ（Device Trajectory）] ビューでコンピュータ名をクリックすると、このビューから選択したコンピュータの詳細を表示できます。

**重要事項：** Share ボタンをクリックしてから、[URLのコピー（Copy URL）] をクリックすると、現在の [デバイストラジェクトリ（Device Trajectory）] ビューの URL をコピーして、他のユーザーと共有できます。

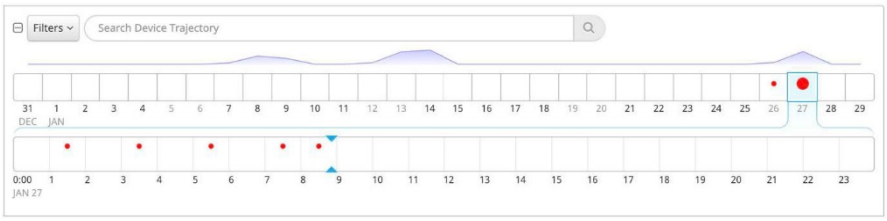



また、該当コンピュータに対して、フルスキャンやフラッシュスキャンの実行、別グループへのコンピュータの移動、診断の開始などの各種アクションを実行できます（「コンピュータの管理：コネクタの診断」を参照）。

**重要事項：** [全画面表示（fullscreen）] ボタン をクリックすると、画面全体にデバイストラジェクトリが表示されます。ボタンをもう一度クリックすると通常の表示に戻ります。

## ナビゲータ

ナビゲータを使用すると、デバイストラジェクトリ内のイベントをすばやく検索して特定することができます。上のリボンには、過去 30 日分が表示され、その上の縮小された折れ線グラフは、その期間中のコンピュータのアクティビティレベルを示しています。30 日間リボン上の赤いドットは、侵害イベントの発生状況を示しています。検索結果は青のドットで表示されます。ドットの大きさは、1 日のイベントの数に比例しています。30 日間リボンの下には、24 時間リボンが表示され、選択された日の 24 時間を示しています。



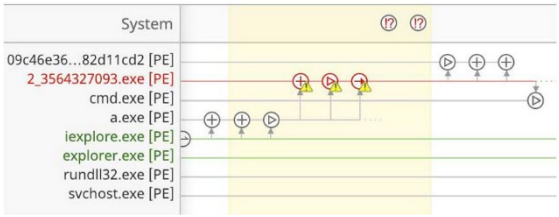

30 日間リボンの上でクリックすると、デバイストラジェクトリの該当する日に移動し、24 時間リボンには、その日のイベントが表示されます。24 時間リボンの上でクリックすると、対象の時刻のデバイストラジェクトリが中央に表示されます。

[-] ボタンをクリックするとナビゲータが折りたたまれ、リボンをもう一度クリックするか、[+] ボタンをクリックすると再び展開します。

**重要：**ドットの上にマウスを置くと、対応するイベントの数が表示されます。

## トラジェクトリの侵害の兆候

特定の一連のイベントが単一のコンピュータ上で観察された場合、それらのイベントは Cisco Secure Endpoint によって侵害の兆候と見なされます。[デバイストラジェクトリ（Device Trajectory）] では、これらのイベントが黄色で強調表示されるため、簡単に確認できます。侵害のタイプに関するトラジェクトリ内に別の侵害イベントが存在する場合もあります。侵害イベントをクリックすると、それをトリガーした個々のイベントが青色の背景で強調表示されます。また、インジケータと戦術および手法の説明が、トラジェクトリの [イベントの詳細（Event Details）] ペインに表示されます。



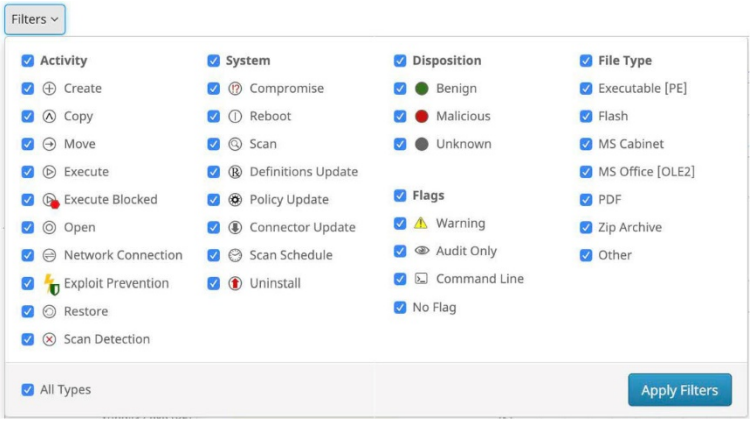

侵害の兆候の詳細については、「インジケータ」を参照してください。

## フィルタと検索

デバイス トラジェクトリには、頻繁に使用されたコンピュータに関する大量のデータが含まれている可能性があります。コンピュータのデバイス トラジェクトリ結果を絞り込むために、データにフィルタを適用することも、特定のファイル、IP アドレス、または脅威を検索することもできます。また、フィルタと検索を組み合わせて使用して、さらにきめ細かな結果を取得することもできます。

## フィルタ

デバイストラジェクトリには、[アクティビティ（Activity）]、[システム（System）]、[分類（Disposition）]、[フラグ（Flags）]、[ファイルタイプ（File Type）] の 5 つのイベントフィルタカテゴリがあります。結果を表示するには、各カテゴリから少なくとも 1 つの項目を選択する必要があります。




[アクティビティ（Activity）] は、コネクタが記録したイベントです。ファイル、ネットワーク、およびコネクタのアクティビティが表示されます。

ファイル イベントには、コピー、移動、実行、およびその他の操作を含めることができます。ネットワーク イベントには、ローカル アドレスとリモート アドレスの両方へのインバウンド接続とアウトバウンド接続の両方が含まれます。

システムイベントには、セキュリティ侵害、リブート、ポリシーまたは定義の更新、スキャン、アンインストールを含めることができます。

[分類（Disposition）] では、イベントの分類に基づいてイベントをフィルタ処理できます。悪意のあるファイルに対して実行されたイベントまたは悪意のあるファイルによって実行されたイベント、クリーン ファイル、または不明な分類のファイルだけを表示するように選択できます。

[フラグ（Flags）] は、イベントタイプの修飾子です。たとえば、悪意のあるファイルが検出されたが、正常に検疫されていないために、そのファイルのコピー イベントに警告が付加される場合があります。正常に完了しなかったスキャンや失敗したポリシー更新などの他のイベントに警告フラグが付加される場合もあります。

[監査のみ（audit only）] フラグは、問題のイベントが観察されてもアクションを実行しないことを意味します。これは、[モードとエンジン（Modes and Engines）] で [ファイル（Files）] と [ネットワーク判定モード（Network Conviction Modes）] のポリシー項目が [監査（Audit）] に設定されているためです。

[ファイルタイプ（File Type）] を使用すると、含まれるファイルのタイプでデバイス トラジェクトリ イベントをフィルタ処理でき、実行ファイルや PDF など、マルウェアの感染に最も関係が深いファイルタイプでフィルタ処理できます。[その他（Other）] フィルタは具体的にリストされていないすべてのファイルタイプ用であり、[不明（Unknown）] フィルタは不正な形式のヘッダー情報が原因でタイプが確定されなかったファイル用です。

### 検索

[デバイス トラジェクトリ（Device Trajectory）] ページの検索フィールドを使用すると、デバイス トラジェクトリを絞り込んで特定の結果だけを表示できます。

検索は、単純なテキスト文字列、`/foo/gim` 形式の JavaScript でサポートされる正規表現（ここで、`gim` はオプションフラグ）、または `X.X.X.X/Y` という形式の CIDR アドレスにできます。これをサポートするブラウザの検索ボックスにファイルをドラッグ アンド ドロップすることもできます。こうすることによって、そのファイルの SHA-256 値が計算され、文字列が検索ボックスに挿入されます。

次の用語でデバイス トラジェクトリ イベントを検索できます。

- 検出名
- SHA-256
- ファイル名
- ファイル パス
- URL
- リモート IP アドレス
- ユーザー名
- iOS バンドル ID

検索を実行するには、検索語を検索フィールドに入力するか貼り付けて、Enter キーを押します。

SHA-256 をクリップボードにコピーするには以下を実行します。

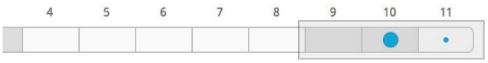
- デバイストラジェクトリの縦軸のファイルまたはプロセスを右クリックして、メニューから [SHA-256をコピー（Copy SHA-256）] を選択します。
- [イベントの詳細（Event Details）] パネルで、SHA 256 の横にあるピボットメニューボタンをクリックし、[クリップボードにコピー（Copy to Clipboard）] を選択するか、ボタンをクリックします。

## モバイル アプリ トラジェクトリ

モバイル アプリ トラジェクトリには、特定のアプリがインストールされている Cisco Secure Endpoint iOS Clarity を実行中の全デバイスからの該当アプリのアクティビティが表示されます。これは、不要または不審なアクティビティを見つけるのに役立ちます。モバイル アプリ トラジェクトリは、[ダッシュボードiOS Clarity（Dashboard iOS Clarity）] タブの [アプリトラジェクトリ（App Trajectory）] リンクをクリックするか、バンドル ID をクリックし、コンテキストメニューから [モバイルアプリトラジェクトリ（Mobile App Trajectory）] を選択して起動します。

ページの上部に、アプリに関する収集可能なすべての情報（バージョンや発行元を含む）の概要が表示されます。

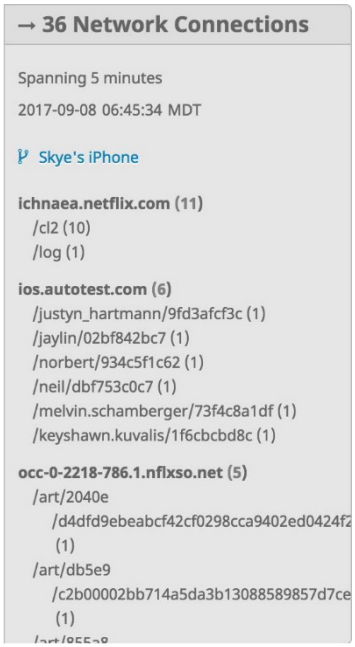

日付スライドを使用して、表示する 3 日間を選択できます。日付に付いている青いドットは、そのアプリで確認されたアクティビティの量を示してします。




[このアプリを使用しているエンドポイント（Endpoints using this App）] セクションには、スライダで選択した 3 日間にそのアプリからのネットワークアクティビティがあったデバイスのリストが表示されます。縦軸にはアプリがインストールされているデバイスのリスト、横軸には日付と時刻が表示されます。各矢印の長さは、監視対象アプリが生成しているアクティビティの量を示しています。デバイス名をクリックしてその [デバイストラジェクトリ（Device Trajectory）] を表示し、そのデバイス上の全アプリのアクティビティの完全なビューを表示します。

ある日をクリックして拡大表示したり、3 つの 8 時間の列を表示したりもできます。拡大表示は 2 秒間隔になるまで続けることができます。

アクティビティの詳細（接続数と継続時間、特定の時刻、各ネットワーク接続の詳細など）を表示するには矢印をクリックします。




[ネットワークの宛先（Network Destinations）] には、トップレベルドメイン（TLD）によって編成されているデバイスによってアクセスされるすべてのドメインのリストがあります。このリストは、アルファベット順または接続の合計数で並べ替えることができます。エントリを展開して、追加の詳細情報、特定の URL、ポート、および接続を表示することもできます。

# 第 19 章

# ファイル リポジトリ

ファイルリポジトリを使用すると、コネクタから要求したファイルをダウンロードできます。この機能は、コネクタによって観察された疑わしいファイルや悪意のあるファイルの分析を実行する場合に役立ちます。ファイルを観察した任意のコネクタからファイルを要求し、ファイルがアップロードされるのを待ってから、分析のために仮想マシンにダウンロードできます。また、追加の判断のサポートを得るためにファイル分析にファイルを送信できます。[すべての変更を表示（View All Changes）] をクリックすると、監査ログのフィルタ処理されたビューが表示され、要求されたすべてのファイルが表示されます。分析のために自動分析および動作保護から自動的に送信されたファイルは、リポジトリでも使用可能になります。

**重要事項：**コネクタからファイルを要求し、ファイルリポジトリからダウンロードするには、シングルサインオン（Cisco Security Cloud Sign-on など）または二要素認証を自分のアカウントに対して有効にする必要があります。ファイルは、Cisco Secure Endpoint Windows コネクタのバージョン 3.1.9 以降、Cisco Secure Endpoint Mac コネクタのバージョン 1.0.2.6 以降、Cisco Secure Endpoint Linux コネクタのバージョン 1.0.2.261 以降を実行しているコンピュータからのみ取得できます。

# リモートファイルの要求

ファイルリポジトリにアップロードするファイルを要求するには、Cisco Secure Endpoint コンソールで SHA-256 値を右クリックして SHA-256ファイル情報（SHA-256 File Info）] コンテキストメニューを起動します。

メニューから [ファイルの取得（Fetch File）] を選択します。ファイルがすでにリポジトリにダウンロードされている場合は、[ファイルの取得（Fetch File）] が使用できなくなり、代わりにリポジトリ内のファイルを表示するオプションが提供されます。

ファイルのダウンロード元のコネクタを選択するためのダイアログが表示されます。ファイルが複数のコネクタで観察された場合は、ドロップダウンリストを使用して、最近ファイルが観察された最大 10 台のコンピュータの中から特定のコンピュータを選択できます。デフォルトでは、ファイルが最後に観察されたコネクタが選択されます。

コンピュータを選択したら、[取得（Fetch）] をクリックしてファイル リポジトリに移動します。そこでは、ファイルとそれが要求されたエントリが表示されます。リポジトリ内のファイルは次の状態を示します。

- [要求済み（Requested）]：ファイルのアップロードが要求されましたが、まだコネクタからの応答がありません。
- [処理中（Being Processed）]：コネクタからファイルがアップロードされましたが、まだ処理中で使用できません。
- [ダウンロード可能（Available）]：ファイルをダウンロードできます。
- [失敗（Failed）]：ファイルの処理中にエラーが発生しました。

> **重要事項：**複数回取得を試みてもアップロードに失敗する場合は、サポートにお問い合わせください。

ファイルが処理されると電子メール通知が送られてきます。[ファイルリポジトリ（File Repository）] ページに移動して、ファイルをダウンロードします。ファイルが取得されたコンピュータのデバイストラジェクトリを起動したり、ファイルトラジェクトリを起動したりできます。[削除（Remove）] をクリックすると、ファイルが取得されたコンピュータではなく、リポジトリからファイルが削除されます。また、[変更の表示（View Changes）] をクリックすると、要求の監査ログエントリを表示できます。


ファイル リポジトリからファイルをダウンロードすると、元のファイルを含むパスワードで保護された zip アーカイブが生成されます。アーカイブのパスワードは「infected」です。

**警告：**ファイル リポジトリから生のマルウェアをダウンロードする場合があります。ファイルは安全なラボ環境内のアーカイブだけから解凍する必要があります。

特定の環境では、コネクタで観察されたファイルをダウンロードできない場合があります。この現象は、ファイルがコンピュータから削除された場合またはサードパーティ製ウイルス対策ソフトウェアがファイルを検疫した場合に発生する可能性があります。クリーンな分類のファイルは別の場所にコピーしなければ取得できません。このような場合は、別のコンピュータからファイルを取得することも、手動で検疫場所からファイルを取得することもできます。

# 第 20 章

# 脅威の根本原因

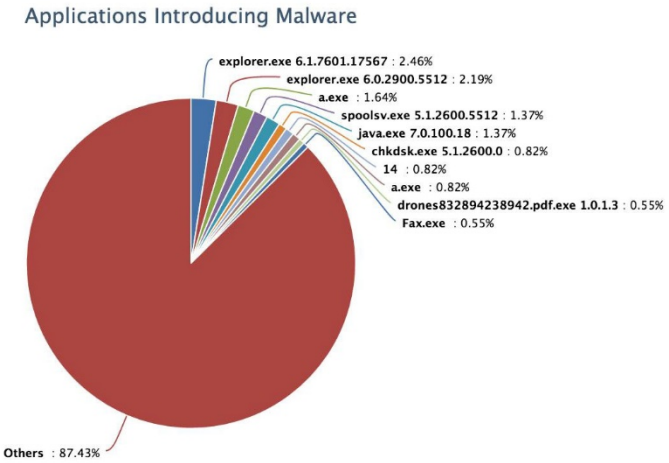
脅威の根本原因 で、正規のアプリケーションと、環境にマルウェアを導入する危険性が高い不正なアプリケーションを識別することができます。コンピュータにマルウェアをインストールする観察対象ソフトウェアに焦点が当てられます。

## 日付範囲の選択

[脅威の根本原因（Threat Root Cause）] では、表示する日付範囲を選択できます。デフォルトの日付範囲は昨日 ~ 本日です。表示する開始日と終了日を選択してから [リロード（Reload）] をクリックし、特定の日付範囲に関する脅威の根本原因を表示します。


## 驚異の根本原因の概要

[脅威の根本原因の概要（Threat Root Cause Overview）] タブには、過去に環境へのマルウェアの侵入が観察された上位 10 のソフトウェアパッケージの名前が表示されます。[その他（Others）] エントリは、比較のための、マルウェアを侵入させる他のすべてのアプリケーションの総計です。可能な場合は、アプリケーションのバージョン番号も表示されます。




# 詳細

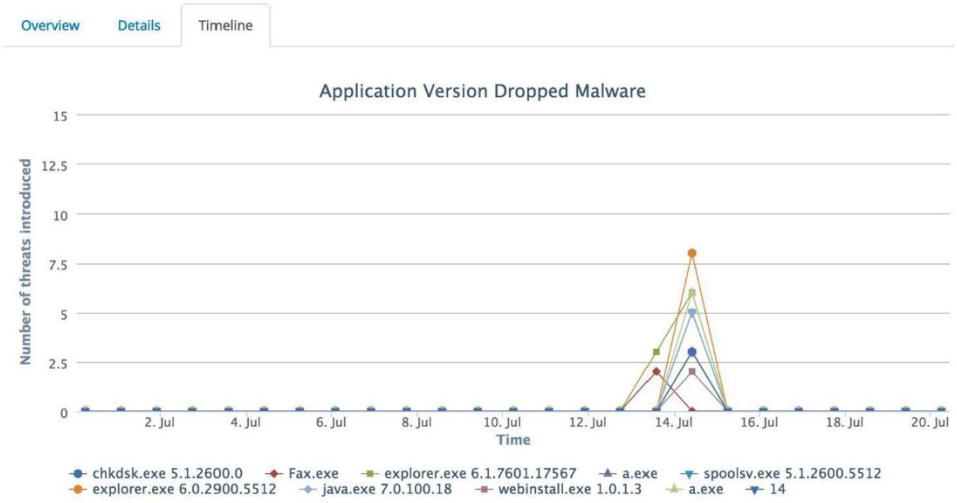
[詳細（Details）] タブには、[概要（Overview）] からの各アプリケーションと追加情報が表示されます。アプリケーションが環境に侵入させた脅威の数、影響を受けたコンピュータの数、およびイベント タイプも表示されます。情報アイコンをクリックすると、コンテキストメニューを表示できます。

| Program | Threat Name | Version | Threats Introduced | Computers Affected | Event Type |
|---|---|---|---|---|---|
| explorer.exe | | 6.1.7601.17567 | 9 | 3 | 6 created<br>3 executed |
| explorer.exe | | 6.0.2900.5512 | 8 | 4 | 4 executed<br>4 moved |
| a.exe | | | 6 | 1 | 2 created<br>2 executed<br>2 moved |
| spoolsv.exe | | 5.1.2600.5512 | 5 | 1 | 3 created<br>2 executed |
| java.exe | | 7.0.100.18 | 5 | 1 | 3 created<br>1 executed<br>1 moved |
| a.exe | W32.SPERO.Spero... | | 3 | 1 | 2 created<br>1 executed |
| chkdsk.exe | | 5.1.2600.0 | 3 | 1 | 2 created<br>1 executed |

このビューでプログラム名をクリックすると、ダッシュボードの [イベント（Events）] タブが開き、そのプログラムの下位で発生したすべてのイベントがフィルタ処理されたビューが表示されます。

# タイムライン

[タイムライン（Timeline）] タブには、前日に各アプリケーションによって環境にマルウェアがダウンロードされた頻度が表示されます。1 つのアプリケーションが一度にまたは一定期間に複数のマルウェア サンプルを侵入させたことが確認された場合は、そのアプリケーションがマルウェアのダウンローダ以外の何物でもないことを示すことができます。マルウェアのインストールに悪用された脆弱なアプリケーションが同様の動作を示す場合もあります。



# 第 21 章

# 感染率

[拡散度（Prevalence）] には、これらのファイルのグローバルな実行に関して組織全体で実行されたファイルが表示されます。これは、少数のユーザーしか観察していない未検出の脅威を抽出するのに役立つ可能性があります。大勢のユーザーが実行するファイルは一般に正規アプリケーションである可能性が高く、1 人または 2 人のユーザーしか実行していない場合は悪意のあるアプリケーション（標的型攻撃など）である可能性があります。

## 低感染率の実行可能ファイル

このページには、実行されたファイルと、それが実行されたコンピュータが表示されます。リストは OS 別に表示されるため、一般的な OS に存在する低拡散度の実行可能ファイルが（数の少なさにより）検出を免れることを防ぎます。ファイルの判定結果は、実行されたファイル名の色で示されます。赤色は悪意のあるファイルを、灰色は不明なファイルを意味します。既知のクリーンな分類のファイルは感染率リストに表示されません。

エントリを展開すると、ファイルの SHA-256 値、そのファイルの実行が観察された最大 10 のコンピュータの名前、および実行時にファイルに付けられていた可能性のある別のファイル名が表示されます。SHA-256 値の横にある情報アイコンをクリックして、[SHA-256ファイル情報（SHA-256 File Info）] コンテキストメニュー] を表示できます。[ファイルトラジェクトリ（File Trajectory）] ボタンをクリックしてファイルに関するファイルトラジェクトリを起動するか、[デバイストラジェクトリ（Device Trajectory）] ボタンをクリックしてファイルが実行されたコンピュータのトラジェクトリを表示します。ファイルリポジトリが有効になっており、そのファイルが Windows 実行ファイルの場合は、[分析（Analyze）] ボタンをクリックすることで、分析用のファイルも送信できます。複数のコンピュータでファイルが実行されていた場合は、コンピュータの名前をクリックして、[デバイストラジェクトリ（Device Trajectory）] を表示します。

**重要：**[分析（Analyze）] ボタンが使用できない場合は、ファイルがすでに送信済みである、ファイル リポジトリが有効になっていない、または現在のユーザーが管理者ではない可能性があります。

[分析（Analyze）] ボタンをクリックすると、コンピュータからファイルを取得するための要求が送信されます。ファイルリポジトリからファイル取得処理のステータスをチェックできます。ファイルが取得されると、ファイル分析に送信されます。

## 自動分析

自動分析では、特定のグループからファイル分析に低拡散度の Windows 実行ファイルが送信されます。[自動分析の設定（Configure Automatic Analysis）] をクリックしてグループを選択します。

**重要事項：**自動分析を設定する前に、ファイルリポジトリを有効にして管理者になる必要があります。

[自動分析の設定（Automatic Analysis Configuration）] ページには、低拡散度のファイルを自動的に送信するグループを選択するためのドロップダウンがあります。グループを選択してから、[適用（Apply）] をクリックします。

自動分析の設定が完了したら、低感染率の実行可能ファイルが 4 時間ごとに送信されます。Cisco Secure Endpoint は、該当ファイルを観察したコネクタにファイルを要求します（入手可能な場合）。ファイルが取得されたらファイル分析に送信されます。その後、[ファイル分析（File Analysis）] ページで分析結果を確認できます。ファイルが一定期間取得されなかった場合、ファイルリポジトリでファイル取得ステータスを確認できます。

**重要事項：**分析のために 1 日に送信できるファイル数とサイズには上限があります。デフォルトでは、[組織の設定（Organization Settings）] ページでカスタムの Cisco Secure Malware Analytics API キーを入力していない限り、1 日に送信できるファイル数は 100 で、サイズの上限は 1 ファイルあたり 20MB です。

# 第 22 章

# 脆弱なソフトウェア

実行ファイルを移動、コピー、または実行するたびに、Cisco Secure Endpoint コネクタはクラウドルックアップを実行して、ファイルの分類（「クリーン（Clean）」、「悪意のある（Malicious）」、または「不明（Unknown）」）を確認します。実行可能ファイルが、Common Vulnerabilities and Exposures（CVE）データベースに既知の脆弱性が記録されたアプリケーションである場合、この情報は [脆弱なソフトウェア（Vulnerable Software）] ページに表示されます。

現在、Windows オペレーティング システムの次のアプリケーションとバージョンが脆弱性ページでレポートされています。

- Adobe Acrobat 11 以降
- Adobe Acrobat Reader 9 以降
- Adobe Flash Player 11 以降
- Google Chrome 25 以降
- Microsoft Internet Explorer 8 以降
- Microsoft Office 2007 以降
- Mozilla Firefox 10 以降
- Oracle Java プラットフォーム SE 1.7.0 以降

デフォルトでは、すべての既知の脆弱性が表示されます。このリストをフィルタ処理して、その日またはその週に検出された脆弱なプログラムのみを表示できます。オフラインで作業するために脆弱なプログラムのリストを CSV ファイル形式でダウンロードすることも可能です。

**重要事項：**エクスポートされた CSV ファイルの日時は、タイムゾーンの設定に関係なくすべて UTC 表示です。


各リスト項目は、リスト内の任意の場所をクリックすることで展開したり折りたたんだりできます。プラス（+）記号またはマイナス（-）記号をクリックすることで、すべてのリスト項目を一度に展開したり、縮小したりすることもできます。

リスト項目には、以下のような脆弱性に関する情報の要約が含まれています。

- プログラム名とバージョン。
- 実行可能ファイルの SHA-256 値。
- コネクタがそのファイルで観察した定義済みグループ内のコンピュータの数。
- その実行可能ファイルに存在することがわかっている、重大な脆弱性の数。「Common Vulnerabilities and Exposures」を参照してください。
- 脆弱性が最も重大な実行ファイルの CVSS スコア。「共通 脆弱性評価システム」を参照してください。

## Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures（CVE）データベースは、各種アプリケーション内の既知の脆弱性を記録します。すべての脆弱性は一意の CVE ID で示されています。コンソールに表示される CVE ID をクリックして脆弱性のさらなる詳細を表示することができます。

CVE ID のリンクをクリックすると、脆弱性を定義し、利用可能なパッチをリストするページが表示されます。

## 共通脆弱性評価システム

共通脆弱性評価システム（CVSS）は、ユーザーが識別された脆弱性にどの優先度レベルを割り当てるかを判断できるように設計されています。スコアの範囲は 0（最低）から 10（最高）です。

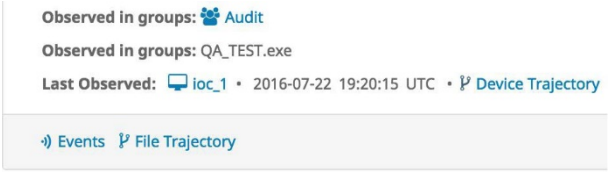
識別された脆弱なプログラムのリストで項目をクリックすると、CVSS スコアが 5.9 より高く、最も重大で最新の脆弱性が表示されます。


## 脆弱なソフトウェアの追加情報

追加情報は、展開されたプログラム リスト項目の最下部で確認できます。次のトピックでは、関連リンクを通じて追加情報を提供します。

- **複数の確認**
- **前回の確認**（コンピュータ）
- **イベント**
- **ファイルトランジェクトリ**

また、[ファイル名（Filename）] は実行ファイルのファイル名を示します。




### 複数の確認

リンク（たとえば監査）は、コンピュータが属する定義グループの名前です。詳細については、「グループ」を参照してください。

### 前回の確認

最後に脆弱性が観察された時間と日付、および観察元のコンピュータ。コンピュータ名は、そのコンピュータに関する詳細情報を提供するページへのリンクです。詳細については、「コンピュータの管理」を参照してください。

### イベント

[イベント（Events）] リンクをクリックすると [ダッシュボード（Dashboard）] が開き、[イベント（Events）] タブの内容が表示されます。詳細については、「[イベント（Events）] タブ」を参照してください。

## ファイルトランジェクトリ

[ファイル トラジェクトリ（File Trajectory）] リンクをクリックすると、ファイルトラジェクトリ詳細が表示されるページが開きます。詳細については、「ファイルトラジェクトリ」を参照してください。

## デバイス トラジェクトリ

[デバイス トラジェクトリの起動（Launch Device Trajectory）] リンクをクリックするとデバイス トラジェクトリ詳細を示すページが開きます。詳細については、「デバイストラジェクトリ」を参照してください。

# 第 23 章

# レポート

レポートを使用することで、1 週間、1 ヵ月、または 3 ヵ月（四半期）の間に組織で生成されたデータを集約して表示できます。レポートには、メインメニューの [分析（Analysis）] > [レポート（Reports）] からアクセスできます。タイトルをクリックすればレポートを表示できます。また、列見出しをクリックしてリストを並べ替えることもできます。

## レポートのカスタマイズ

週次レポートの対象となる期間は、毎週日曜の午前 0 時から次の日曜の午前 0 時（UTC）までの 1 週間です。月次レポートの対象となる期間は、月の初日の午前 0 時から月の最終日の午前 0 時までの期間です。四半期レポートの対象となる期間は、月の初日の午前 0 時から、3 ヵ月後の月の最終日の午前 0 時までの期間です。システム定義レポートは自動的に作成されますが、独自のカスタム レポートを設定することもできます。

### カスタム レポートの設定

レポートを作成、編集、削除でき、[レポート設定（Report Configuration）] ページから電子メール経由でレポートを受信するかどうかを選択できます。このページにアクセスするには、[レポート（Reports）] ページにある [カスタムレポートの設定（Configure Custom Reports）] ボタンをクリックします。いずれかの行の [変更の表示（View Changes）] ボタンをクリックすると、 単一のレポート設定に対する変更を表示で

きます。[すべての変更を表示（View All Changes）] をクリックすると、すべてのレポートの設定に対する変更を表示できます。

### レポートの作成

選択したコンピュータ グループに関する情報を表示するカスタム レポートを作成できます。[レポート設定（Report Configuration）] ページで [新規カスタムレポート（New Custom Report）] ボタンをクリックして、[新規カスタムレポート（New Custom Report）] ダイアログを表示します。レポートタイプ（週次、月次、または四半期）を選択し、レポートのタイトルを入力して、ドロップダウンメニューからレポートに含めるグループを選択します。電子メール経由でラポートを受信する場合は、[電子メール（Email）] チェックボックスをオンにし、[保存とスケジュール（Save and Schedule）] をクリックします。

### レポートの編集

編集するレポートの列で [編集（Edit）] ボタン をクリックします。ダイアログボックスでタイトルおよび選択したグループを変更し、終了したら [保存とスケジュール（Save and Schedule）] をクリックします。

**重要：**システム定義レポートを編集することはできません。

### レポートの削除

削除するレポートの列で [削除（Delete）] ボタン をクリックし、表示されるダイアログボックスで [削除（Delete）] をクリックして削除を確認します。

**重要事項：**システム定義レポートを削除することはできません。ただし、システム定義レポートを受信しない場合は、そのレポートの [電子メール（Email）] チェックボックスをオフにできます。

## レポート セクション

レポートの要素（SHA-256、コンピュータ、脅威など）は Cisco Secure Endpoint コンソールの適切なセクションにリンクされているため、データにさらにドリルダウンできます。

いくつかのセクションには、重要なメトリックを強調表示するボックスが含まれています。これらのボックス内には週ごとの傾向を示す小さな数字と矢印が表示され、該当する場合には緑または赤（それぞれ「良い」または「悪い」状況を示します）で示されます。

**重要：**コンソールに表示されるデータは、レポートの生成後にレトロスペクティブジョブが実行されると、レポートデータと正確に一致しない場合があります。

## アクティブなコネクタ

組織内のアクティブなコネクタの数が対先週比で示されます。コネクタがアクティブだと見なされるためには、レポート期間に少なくとも 1 回はチェックインしている必要があります。また、新しいインストールおよびアンインストールの数も表示されます。

## コネクタのステータス

レポート期間にスキャンされたファイルおよび IP の数と、レポート期間の最終日の時点でアクティブなコネクタの数が示されます。コネクタがアクティブだと見なされるためには、レポート期間に少なくとも 1 回は Cisco Secure Endpoint サーバーを使用してチェックインしている必要があります。このセクションには、レポート期間の最終日におけるユーザーの組織に関する現在のライセンスコンプライアンスの情報も表示されます。

## セキュリティ侵害

新しい侵害は、エンドポイントにおける脅威の検出またはマルウェア実行の結果です。前回のレポート期間からからまだ解決していない侵害の数が、現在のレポート期間で解決された侵害数とともに表示されます。侵害は、グラフでは重大度によって色分けされています。表には、レポート期間中の重大なセキュリティ侵害の観測対象の上位 5 つと、レポート期間中の侵害イベントタイプおよびそれぞれの重大度が示されています。

## ファイル検出

組織において悪意のあるファイルの検出が最も多いコンピュータの数が、最も頻繁に発生した検出とともに表示されます。日単位のマルウェア検出数レポートでは、どの曜日にコンピュータ上で最も多く検出されたかについての傾向を確認できます。ファイル検出数が多いコンピュータは、ドロッパーに感染していると考えられます。

## ネットワーク検出

環境内のデバイス フロー コリレーション検出数やエージェントレスグローバル脅威アラート数、および悪意のあるネットワーク検出が確認された組織内のコンピュータ数を示します。日単位のネットワーク検出数レポートでは、どの曜日にコンピュータ上で最も多く検出されたかについての傾向を確認できます。ネットワーク検出数が多い場合、ボット感染している可能性があります。

デバイス フロー コリレーション メトリックは、ポリシーでデバイス フロー コリレーションが有効になっているコネクタにのみ適用されます。エージェントレスグローバル脅威アラートを表示するには、グローバル脅威アラートデバイスが設置されている必要があります。

### ブロックされたアプリケーション

コネクタで実行がブロックされたアプリケーションの数が表示されます。コネクタは、ブロックされたアプリケーションリストに追加したアプリケーションのみをブロックします（「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」を参照）。

### 低拡散度の実行可能ファイル

分析用に送信された低拡散度の実行ファイルの数、それらの送信で検出された脅威の数、および実行されたアクションが表示されます。送信制限は、レポート期間中に分析へと送信されることが可能な全送信のパーセンテージです。固有検出は、悪意があると判定された低拡散度の実行可能ファイルの数です。

### 脅威の根本原因

レポート期間内に最も多くのマルウェアを環境に持ち込んだことが確認されたアプリケーションを表示します。この情報により、環境内のコンピュータに常駐（またはアクセス）するためにマルウェアが頻繁に利用しているアプリケーションを迅速に特定できます。（その他の）エントリには、環境にマルウェアを持ち込んだその他のすべてのアプリケーションが集約されています。

### 脆弱性（Vulnerabilities）

実行、移動、またはコピーされた脆弱なアプリケーションの数と、脆弱なコンピュータの数を表示します。実行ファイルを移動、コピー、または実行するたびに、Cisco Secure Endpoint コネクタはクラウドルックアップを実行して、ファイルの分類（「クリーン（Clean）」、「悪意のある（Malicious）」、または「不明（Unknown）」）を確認します。実行可能ファイルが既知の脆弱性ですでに Common Vulnerabilities and Exposures（CVE）データベースに記録されているアプリケーションである場合は、その情報が表示されます。[上位の脆弱なアプリケーション（Top Vulnerable Applications）]の表には、上位の脆弱なアプリケーションがシビラティ（重大度）、バージョン番号、実行回数、CVE 数の順に表示されます。[上位の脆弱なコンピュータ（Top Vulnerable Computers）]の表には、上位の脆弱なコンピュータと、そのコンピュータ上の脆弱なアプリケーションの数が表示されます。

### 隔離成功

コネクタによって検疫されたファイルの数が日別に表示されます。すべての検出の結果において、ファイルがコネクタによって検疫されるわけでありません。場合によっては、お使いのアンチウイルス ソフトウェアによってファイルがすでに検疫されたか、検疫される前に削除された可能性があります。

### レトロスペクティブ検出

コネクタで検出されたファイルのうち、判定結果が「悪意のある（Malicious）」に変更され、遡及的に検疫されたファイルの数が表示されます。

### レトロスペクティブ誤検出

コネクタで検出されたファイルのうち、最初は「悪意のある（Malicious）」と分類され、その後分類が「クリーン（Clean）」に変更され、遡及的に検疫状態から復元されたファイルの数が表示されます。

### Indications of Compromise

当該週の間にトラジェクトリの侵害の兆候がトリガーされた回数が表示されます。

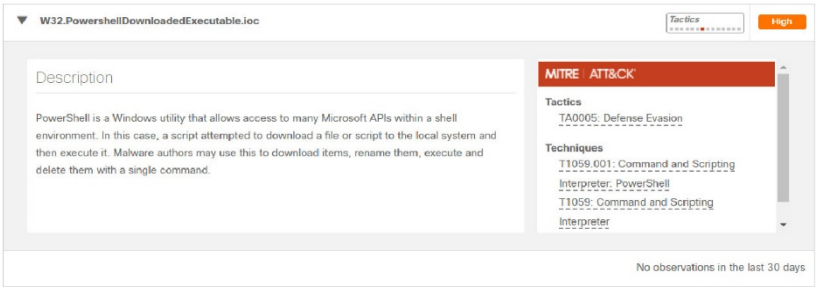
# 第 24 章

# インジケータ

Cisco Secure Endpoint は、特定の期間内にエンドポイントで観測された複数のイベントまたは一連のイベントに基づいて、クラウド侵害の兆候（IOC）を決定します。クラウド IOC の目的は、エンドポイントでの不審なアクティビティまたは悪意のあるアクティビティの通知として機能することです。ホスト上でクラウド IOC がトリガーされた場合、詳細な調査を行い、クラウド IOC の説明で概要が示されている不審なアクティビティの正確な性質と原因を特定する必要があります。単一のクラウド IOC は、エンドポイントごとに 4 時間ごとに 1 回のみ報告されます。

[インジケータ（Indicators）] ページでは、クラウド IOC と動作保護の署名を検索できます。このページには、メインメニューの [分析（Analysis）] > [インジケータ（Indicators）] からアクセスできます。各インジケータには、簡単な説明が、MITRE ATT&CK ナレッジベースに基づいて採用された戦術と手法に関する情報とともに含まれています。戦術とは、マルウェアの実行や機密情報の窃取といった攻撃の目的を表します。手法とは、攻撃者が目的を達成するまたはメリットを得るために使用する方法です。詳細については、「ATT&CK の概要」を参照してください。

特定のインジケータを名前で検索したり、戦術、手法、重大度に基づいてリストをフィルタ処理することができます。インジケータに関連付けられている組織内の侵害の数も表示され、これらだけを表示するようにリストをフィルタ処理できます。




インジケータをクリックして説明を展開すると、戦術と手法の完全なリストが表示されます。いずれかの戦術または手法をクリックすると、詳細な説明が表示されます。

侵害バッジをクリックすると、インジケータを観察したすべてのエンドポイントの [受信トレイ（Inbox）] タブのフィルタ処理されたビューが表示されます。[ダッシュボード（Dashboard）]、[イベント（Events）]、または [受信トレイ（Inbox）] リンクをクリックすると、各ページのフィルタ処理されたビューが表示され、インジケータを観察したコンピュータのみが表示されます。

# 第 25 章

# エージェントレスグローバル脅威アラート

エージェントレス インシデントは、組織のグローバル脅威アラートによって記録されるイベントです。Cisco Secure Endpoint コネクタがインストールされていないコンピュータで発生したインシデントが記録されます。イベントをこのページに表示するには、[組織の設定（Organization Settings）] ページで [グローバル脅威アラートの統合（Global Threat Alerts Integration）] を有効にし、Cisco Secure Web Appliance（旧 Cisco Web セキュリティアプライアンス）など、少なくとも 1 つの対応デバイスがイベントのグローバル脅威アラートにログを送信するように設定されている必要があります。

各行にはユーザー名（決定されている場合）、IP アドレス、および使用している対応デバイスで検出されたグローバル脅威アラートのリストが記載されています。


ユーザー名または IP アドレスをクリックすると、コンピュータの周辺で観察されるインシデントについての詳細情報が表示されます。脅威に関連したすべての Web フローなど、脅威に関する詳細を確認するには、アラート名のいずれかをクリックします。キャンペーン名（名前の最初のハッシュタグで示されている）をクリックすると、当該のキャンペーンに関連したグローバル脅威アラートが検出された、組織内のすべてのコン

ピュータが表示されます。キャンペーンは通常、次々とボットをダウンロードするトロイなど、連携して動作する脅威のセットです。

可能であれば、エージェントレスグローバル脅威アラートのリストに表示されているすべてのコンピュータにコネクタをダウンロードしてインストールしてください。インストールすることで、早い段階で脅威を検出して検疫し、デバイストラジェクトリを介してインシデントの全貌を明らかにできます 。

# 第 26 章

# アカウント

[アカウント（Accounts）] メニューの下の項目を使用すると、Cisco Secure Endpoint コンソールを管理できます。ユーザー管理、デフォルト、および監査ログのすべてにこのメニューからアクセスできます。

## ユーザー

[ユーザー（Users）] 画面を使用すると、アカウントを管理して、そのアカウントの通知とサブスクリプションを表示できます。

さまざまなフィールドと設定でユーザー リストをフィルタリングできます。[最終ログイン（Last Login）] では、さまざまな時間枠中にログインしたユーザーやログインしていないユーザーを表示できます。[ユーザー（User）] では、ユーザー名や電子メールアドレスで検索できます。[二要素認証（Two-Step Verification）]、[リモートファイル取得（Remote ）]、および [コマンドライン（Command Line）] フィルタでは、ユーザーがアカウントでこれらの機能を有効にしているかどうかに応じてフィルタ処理できます。

電子メール アドレス、名前、または最終ログイン時刻でユーザーのリストを並べ替えることができます。横に鍵が付いているアカウントは管理者で、鍵が付いていないアカウントは特権のないユーザーです。現在ログインしているアカウントを表示するには、[マイアカウント（My Account）] リンクをクリックします。このアカウントは、ユーザーリストでも青色で強調表示されます。


ユーザーアカウントの横にあるクロックアイコンをクリックすると、そのアカウントに関連しているアクティビティに関する監査ログのフィルタ処理されたビューを表示できます。また、[すべての変更を表示（View All Changes）] リンクをクリックすると、監査ログのフィルタ処理されたビューを表示し、ユーザーアカウントのすべてのアクティビティを表示できます。

アカウントの詳細を表示および編集するには、ユーザーの名前をクリックして、ユーザーアカウントページにアクセスします。自分のアカウントを選択した場合は、パスワードをリセットするオプションも表示されます。

**重要事項：**[ユーザーアカウント（User Account）] ページから、二要素認証を有効にする電子メール通知をユーザーに送信できます。

新しい Cisco Secure Endpoint コンソールのユーザーアカウントを作成するには、[新規ユーザー（New User）] をクリックします。アカウントのアクティベーション用の電子メールを受信するには、その新規ユーザーの有効な電子メールアドレスが必要です。電子メールには、必要な Cisco Security Cloud Sign-On アカウントを作成してログインする手順が記載されています。また、通知を受信する他の電子メール アドレスを追加することもできます。たとえば、作成したすべての通知を受信する場合は、配布リストに追加します。また、ユーザーが管理者または特権のないユーザーのどちらになるかを判断する必要もあります。管理者は、Cisco Secure Endpoint 展開のすべての側面を完全に制御できます。[管理者（Administrator）] ボックスをオフにすると、そのユーザーは自分のグループに関するデータしか表示できなくなります。アカウントを編集することによって、後からユーザーの特権を変更できます。詳細については、「マイアカウント」を参照してください。

ユーザー アカウントを選択する際に、そのユーザーのサブスクリプションを表示することもできます。[サブスクリプション（Subscriptions）] リストには、そのユーザーがサブスクライブしているイベントやレポートが表示されます。

## タイム ゾーン設定

Cisco Secure Endpoint コンソールに表示されるユーザーアカウントのタイムゾーンを変更するには、次の手順を実行します。

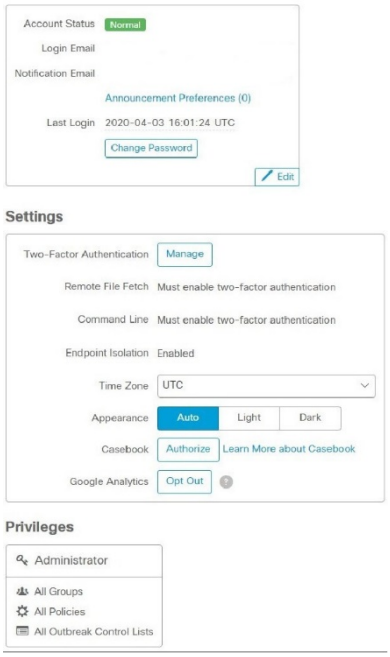
1. [マイアカウント（My Account）] をクリックするか、[ユーザー（Users）] ページに移動して、自分の名前または電子メールアドレスをクリックします。

2. [タイムゾーン（Time Zone）] ドロップダウンメニューから、希望するタイムゾーン設定を選択します。

**重要：**すべてのコネクタのイベントは、イベントを監視するコンピュータのローカルタイムゾーンではなく、設定したタイムゾーンで表示されます。

## マイアカウント

ユーザーは、[マイアカウント（My Account）] をクリックすることで、このページで自分のアカウント設定にアクセスできます。




[パスワードのリセット（Password Reset）]、[二要素認証（Two-Factor Authentication）]、[タイムゾーン設定（Time Zone Settings）]、[外観（Appearance）]、および[Casebook] の [承認（Authorize）] は、このページに表示されます。ユーザーは、[通知設定（Announcement Preferences）] リンクをクリックして、電子メールで受信する通知のタイプを選択できます。

[外観（Appearance）] の設定では、コンソールの [ライト（Light）] テーマまたは [ダーク（Dark）] テーマを手動で選択するか、[自動（Auto）] を選択して、対応しているバージョンの Windows、macOS、および iOS のオペレーティングシステム設定で選択されたテーマを使用できます。

Cisco Secure Endpoint は **Google Analytics** を使用して使用状況データを収集し、正確性を高め、製品を改善し、問題のトラブルシューティングに役立てます。ユーザーは [オプトアウト（Opt Out）] ボタンをクリックして、Google Analytics から自分のアカウントをオプトアウトすることを選択できます。

**重要事項：**[オプトアウト（Opt Out）] ボタンは、組織に影響せず、ユーザーのみに影響します。組織全体を Google Analytics からオプトアウトするには、[組織の設定（Organization Settings）] ページの機能にある設定を使用してください。

UX リサーチにオプトインすることを選択できます。これにより、Cisco Secure Endpoint の初期デザインおよび機能に関する研究に参加できます。

## アクセス コントロール

Cisco Secure Endpoint のユーザーには、管理者と非特権ユーザーの 2 種類があります。新しいユーザーを作成するときに、特権レベルを選択する必要がありますが、アクセス レベルはいつでも変更できます。

### 管理者

管理者特権を使用すると、Cisco Secure Endpoint 展開のすべての側面を完全に制御できます。管理者は、組織内のすべてのグループまたはコンピュータのデータを表示でき、グループ、ポリシー、リスト、およびユーザーを変更できます。

次の作業は、管理者のみが実行できます。

- グループの作成と編集
- ポリシーの作成
- ファイルリポジトリへのアクセスとリモートファイルの取得
- エンドポイント IOC のアップロード
- エンドポイント IOC スキャンの開始
- レポートの生成と表示
- 新規ユーザーの作成
- 既存ユーザーの編集
- ユーザー権限の変更。管理者権限の付与および取り消しを含む
- デバイス制御設定の作成
- 組織設定の変更
- デモデータの有効化
- コマンドラインデータの表示
- 監査ログの表示
- [クイック スタート（Quick Start）] へのアクセス

**重要：**さらに、管理者は、別の管理者を一般ユーザーに降格させることができますが、自分自身を降格させることはできません。

## 特権のないユーザー

特権のないユーザー/通常ユーザーは、アクセス権が付与されているグループの情報のみ表示できます。[エンドポイント IOC スキャン（Endpoint IOC scans）]、[ファイル リポジトリ（File Repository）]、[レポート（Reports）] などの特定のメニュー項目にはアクセスできません。

新しいユーザーを作成するときに、そのユーザーに管理者特権を付与するかどうかを選択できます。このような特権を付与しない場合、どのグループ、ポリシー、およびリストにアクセスできるかを選択することができます。ユーザーに次のことを許可するオプションもあります。

- 選択したグループのコンピュータからファイルと診断を取得します。
- 選択したグループからコマンドラインデータを表示します。
- 選択したグループのエンドポイント隔離ステータスを設定します。

ユーザーにアクセス権を与えるグループの選択から開始します。[クリア（Clear）] ボタンを使用すると、そのユーザーに追加されたすべてのグループが削除されます。現在のセッションで加えた変更を元に戻すには、[変更を元に戻す（Revert Changes）] ボタンを使用します。[すべての権限の削除（Remove All Privileges）] ボタンを使用すると、ユーザーに割り当てられているすべてのグループ、ポリシー、アウトブレイク コントロール リストが削除されます。

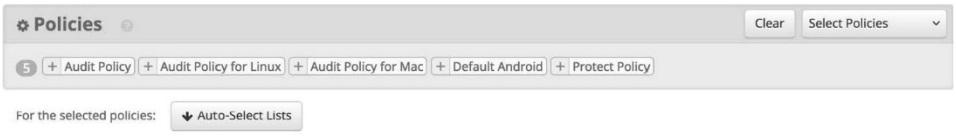
ユーザーは [グループ（Groups）] ページではグループを確認できますが、変更したり、新しいグループを作成したりはできません。ユーザーは、次のような、グループ内のコネクタからの情報も確認できます。

- ダッシュボードの [概要（Overview）] タブ、[イベント（Events）] タブ、[iOS Clarity] タブ
- ファイル トラジェクトリ（File Trajectory）
- デバイストランジェクトリ
- ファイル分析（File Analysis）
- 脅威の根本原因
- 感染率
- 脆弱なソフトウェア
- IOC スキャン

また、ユーザーに割り当てたグループ内のコンピュータからファイルを取得する権限をユーザーに付与し、ファイルリポジトリで表示したり、デバイストラジェクトリや [イベント（Events）] タブでコマンドラインデータを表示したりできます。ユーザーは、リポジトリを表示、ファイルを要求、または [トラジェクトリ（Trajectory）] ページでコマンドラインデータを表示するには、シングルサインオン（Cisco Security Cloud Sign-On など）または二要素認証を有効にする必要があります。これらのボックスのいずれかを選択解除して、これらの権限を削除することができます。

**重要：**特権のないユーザーは、アクセス権のあるグループからのファイルとコマンド ライン データのみを要求して表示できます。

ユーザーがアクセスできるグループを選択したら、ユーザーが表示または編集できるポリシーを選択できます。ユーザーに対する個別のポリシーを手動で割り当てるか、自動選択ボタンのいずれかをクリックして、選択したグループに関連付けられたポリシーおよびポリシーオブジェクトに追加できます。[クリア（Clear）] ボタンをクリックすると、ユーザーがアクセス権を付与されているすべてのポリシーが削除されます。




次に、同じ方法でポリシーオブジェクトを選択できます。ポリシーオブジェクトは、カスタム検出リスト、アプリケーション制御リスト、IP ブロックリストと IP 許可リスト、除外、およびデバイス制御設定で構成されます。各リストを選択するか、自動選択ボタンをクリックして、すでに選択したポリシーに割り当てられているリストを追加できます。各リストの横にある [クリア（Clear）] ボタンを使用すると、ユーザーに割り当てられているタイプのリストのみ削除されます。

**警告：**ポリシーおよびリストへのアクセス権を割り当てる場合は注意が必要です。一部のポリシーとリストは、ユーザーがアクセスできない他のグループが使用できる場合があります。したがって、これらのグループに影響を与える変更をユーザーが作成することも考えられます。

**重要：**IP ブロックリストと IP 許可リストは、それらのリストへのアクセス許可が付与されていないユーザーであっても、ポリシーに追加できます。それらのユーザーは、これらのリストを表示または編集することはできません。

また、ユーザーのグループ アクセス権をいつでも変更でき、ユーザーを管理者にしたり、管理者から特権のないユーザーに降格させたりすることもできます。特権のないユーザーが自分のアカウントを表示する場合は、アクセス可能なグループのリストを表示したり、自分のパスワードや電子メールアドレスを変更したり、二要素認証を有効にしたりできます。

**重要事項：**ユーザー権限を変更する場合、データの一部が検索結果にキャッシュされるため、ユーザーはグループへのアクセス権を失っても一定期間確認することができます。ただし、ほとんどの場合、キャッシュは 5 分後に更新されます。

## 二要素認証

二要素認証はセキュリティをさらに強化し、Cisco Secure Endpoint コンソールアカウントへの無許可アクセスを防止します。Google Authenticator などの RFC 6238 互換アプリケーションを使用して、パスワードと組み合わせて使用されるワンタイム認証コードを生成します。

**重要：**Cisco Security Cloud Sign-On には多要素認証が含まれているため、コンソールのニ要素認証オプションは不要なため、Cisco Security Cloud Sign-On を使用するすべてのアカウントで無効になっています。ニ要素認証が必要な機能はすべて、Cisco Security Cloud Sign-On ユーザーに対して有効になります。

アカウントの二要素認証を有効にするには、[ユーザー（Users）] ページでアカウントの [二要素認証（Two-Factor Authentication）] エントリの横にある [有効化（Enable）] または [管理（Manage）] をクリックします。

その後は、バックアップコードなど、アカウントに対する二要素認証を有効にするための手順を順番に実行します。認証アプリを使用してデバイスにアクセスできない場合に備えて、バックアップ コードのコピーを安全な場所に保管しておくことが重要です。

**重要：**各バックアップ コードは一度しか使用できません。すべてのバックアップ コードを使い切ったら、このページに戻って新しいバックアップ コードを生成する必要があります。

アカウントで二要素認証を正常に有効にすると、二要素認証の [詳細（Ditails）] を確認するためのボタンが表示されます。

二要素認証を無効にするか、または新しいバックアップコードを生成する必要がある場合には、このリンクをクリックして二要素認証の設定ページに戻ります。

次の Cisco Secure Endpoint コンソールへのログイン時に、電子メールアドレスとパスワードの入力後に認証コードの入力を求められます。

[このコンピュータを30日間記憶する（Remember this computer for 30 days）] をオンにすると、次の 30 日間は現在のコンピュータ上での二要素認証を回避するように Cookie が設定されます。Cookie でこの設定を使用できるように、ブラウザを設定する必要があります。

**警告：**パブリックコンピュータ（今後アクセスできなくなるコンピュータ）上で誤って [このコンピュータを30日間記憶する（Remember this computer for 30 days）] をオンにした場合、または二要素認証を無効にすることにした場合は、ブラウザ上で Cookie を消去する必要があります。

認証デバイスへのアクセス権がない場合、[認証コードを使用してログインできない（Can't log in with your verification code?）] をクリックし、生成したバックアップコードのいずれかを入力します。

認証デバイスまたはバックアップコードへのアクセス権がない場合は、サポートに連絡する必要があります。

# API クレデンシャル

[API クレデンシャル（API Credentials）] ページでは、特定のアプリケーションの API クレデンシャルを追加および削除できます。詳細については、Secure Endpoint API ドキュメンテーションを参照してください。

アプリケーションの API キーを生成するには [新しい API クレデンシャル（New API Credential）] をクリックします。参照のためにアプリケーションの名前を入力し、範囲を、読み取り専用、または、読み取り/書き込み権限に割り当てることができます。API ログイン情報でコマンドライン キャプチャ データにアクセスすることも選択できます。コマンドラインデータの API 要求を行うために使用されるアカウントには、管理者権限があり、シングルサインオン（Cisco Security Cloud Sign-On など）または二要素認証が有効になっている必要があります。

**重要：**API ログイン情報の範囲を読み取り/書き込みにすると、Cisco Secure Endpoint 設定の変更が可能になるため、エンドポイントで重大な問題が発生する可能性があります。Cisco Secure Endpoint コンソールに組み込まれた入力保護の中には、API に適用されないものがあります。

アプリケーションの一意の API クライアント ID と API キーは、[作成（Create）] ボタンをクリックすると表示されます。この情報は、このページから移動すると表示できないため、クレデンシャルを忘れてしまった場合、または、変更する必要がある場合は、削除してから新しく作成する必要があります。

**重要：**API クレデンシャルを削除すると、古いクレデンシャルを使用するクライアントがロックアウトされてしまうため、必ず新しいクレデンシャルに更新してください。

Cisco XDR または SecureX との統合を有効にすると、自動生成された API ログイン情報が作成されます。これらのログイン情報には読み取り/書き込み権限が付与され、「[AUTO-GENERATED] SecureX Module API Client」という名前が付けられます。これらのログイン情報は、Cisco Secure Client のインストールトークンの作成にも使用されます。

# 組織設定

[組織の設定（Oranization Settings）] 画面を使用すると、Cisco Secure Endpoint 展開のグローバルデフォルトを指定できます。

Cisco Secure Endpoint 展開から生成されたすべてのレポートに [組織名前（Organization Name）] エントリが表示されます。[編集（Edit）] をクリックして組織名を変更し、優先連絡先の電子メールアドレスを 3 つまで追加します。優先連絡先は、サポートのエスカレーション、脅威ハンティング、または Talos Intelligence Group からの連絡に使用される場合があります。

グループが割り当てられていないコンピュータが属することになるデフォルト グループを変更することもできます。同様に、[デフォルトポリシー（Default Policy）] では、初期ポリシーが 1 つも指定されていないか、親グループから継承されていない場合、作成された新しいグループの各コネクタタイプの初期ポリシーが定義されます。デフォルトのコネクタバージョンを使用すると、管理者は新規導入中にインストールする各コネクタのバージョンを指定できます。

[更新（Update）] をクリックして、この項で行った変更を保存します。

## 機能

[組織の設定（Organization Settings）] ページの [機能（Features）] セクションでは、特定の機能を有効または無効にし、Cisco Secure Malware Analytics との連携を定義できます。

ファイルリポジトリを使用するには、[エンドポイントのファイルのリクエストおよび格納（Request and store files from endpoints）] を有効にします。この設定は、組織のすべてのユーザーに適用されます。アカウントでシングルサインオン（Cisco Security Cloud Sign-On など）または二要素認証を有効にして、認証コードを入力する必要があります。

[サードパーティAPIアクセス（3rd Party API Access）] では、アプリケーション プログラミング インターフェイスを利用して、コンソールにログインせずに Cisco Secure Endpoint データやイベントにアクセスできます。API キーは [APIログイン情報（API Credentials）] ページから生成できます。詳細については、Secure Endpoint API ドキュメンテーションを参照してください。

[Mobile Device Manager] には、iOS デバイスで Cisco Secure Endpoint iOS Connector と Clarity を使用および展開するために、現在設定されている MDM の統合が表示されます。[MDM の統合（MDM Integration）] をクリックして、MDM を選択するか、Meraki SM API キーを変更します。

組織が Cisco Security Cloud Sign-On に移行していない場合は、[シングルサインオン（Single Sign-On）] をクリックしてシングルサインオンを設定できます。これで、シングルサインオンログイン情報を設定し、ログイン情報を利用して Cisco Secure Endpoint コンソールにログインできます。シングルサインオンが有効になっている場合、二要素認証は使用できませんが、二要素認証が必要な機能はすべて有効になります。

別の Cisco Secure Malware Analytics アカウントを持っている場合は、Secure Malware Analytics API キーを入力できます。入力すると、ファイル分析で Cisco Secure Malware Analytics アカウントからの分析結果を確認できます。Cisco Secure Malware Analytics API キーを入力すると、1 日に送信可能な最大数が表示されます。最大数に達した場合、[ファイル分析（File Analysis）] または [拡散度（Prevalence）] ページの [自動分析（Automatic Analysis）] からファイルを送信できなくなります。割り当てられていた初期の Cisco Secure Malware Analytics API キーに戻す必要がある場合は、[デフォルトキーの使用（Use Default Key）] ボタンをクリックします。

自動分析で使用する 1 日の送信数を制限するには、スライダを使用して、1 日の総送信に対する割合を設定します。1 日の送信数の最大 80% まで自動分析用で使用できます。また、分析用に送信したファイルが実行されるデフォルトのオペレーティング システムも、VM イメージと合わせて、分析ドロップダウンで設定できます。自動分析に送信されたすべてのファイルは、選択したオペレーティング システム イメージを使用する VM に送信されますが、ファイル分析にファイルを手動で送信する際にこの設定を変更できます。

[設定（Configure）] ボタンをクリックして、現在の Cisco Secure Endpoint 組織にリンクされているグローバル脅威アラート（旧 Cognitive Threat Analytics）アカウントを作成します。これで、2 システム間のシングルサインオンも設定されるため、自分の Cisco Secure Endpoint ログイン情報を使用してグローバル脅威アラートにログインできます。次に、Cisco Secure Endpoint からグローバル脅威アラートへの Web ログアップロードを設定し、処理を続行できます。特権のないユーザーがグローバル脅威アラートイベントを表示できるようにするには、サポートに連絡してください。

**重要事項：**すでにグローバル脅威アラートを利用しているお客様の場合は、サポートに連絡して既存のアカウントを Cisco Secure Endpoint 組織にリンクしてください。または、[設定（Configure）] ボタンを使用すると、空のグローバル脅威アラートアカウントが別に作成されます。

[AV定義しきい値（AV Definitions Threshold）] 設定では、コネクタの AV 定義が期限切れとして [コンピュータの管理（Computer Management）] ページに表示されるまでの日数（1 ～ 7）を設定できます。

Cisco Secure Endpoint は Google Analytics を使用して使用状況データを収集し、正確性を高め、製品を改善し、問題のトラブルシューティングに役立てます。[オプトアウト（Opt Out）] ボタンをクリックして、Google Analytics から組織をオプトアウトすることを選択できます。

[非アクティブコンピュータしきい値（Inactive Computer Threshold）] を使用すると、コネクタが Cisco Cloud にチェックインせずに経過すると [コンピュータの管理（Computer Management）] ページのリストから削除される日数を指定できます。デフォルト設定は 90 日です。非アクティブコンピュータはリストから削除されるだけで、生成されたイベントは Cisco Secure Endpoint 組織に残ります。コネクタが再度チェックインすると、そのコンピュータがリストに再表示されます。

**重要：**コネクタがコンピュータのページのリストから削除されても、ライセンスは再利用されません。

## Cisco XDR または SecureX との統合

Cisco XDR または SecureX はシスコの統合型セキュリティポートフォリオとユーザーのインフラストラクチャを結合させて、一貫した操作性を実現します。共有されたコンテキストと重要なメトリックを使用した統合された可視性が実現され、すぐに利用できる相互運用性を備えた組み込みの統合機能が提供され、セキュリティエコシステム全体にわたる脅威の調査および修復の迅速化によってセキュリティが強化されます。

**Cisco XDR または SecureX との統合**により、Cisco Secure Endpoint の組織を Cisco XDR または SecureX アカウントと統合できます。統合を有効にすると、Cisco Secure Endpoint のデータの一部が Cisco XDR または SecureX と共有されます。

Cisco XDR または SecureX の Cisco Secure Endpoint モジュールには、次の情報を表示できます。

- セキュリティ侵害
- 侵害数の推移
- 隔離
- 隔離数の推移
- 脆弱性（Vulnerabilities）
- コンピュータ
- 7 日以上検出されていないコンピュータ
- 定義が古いコンピュータ
- コネクタバージョンが最新ではないコンピュータ
- 観測された MITRE ATT&CK の戦術と手法

**インシデント対応促進**は、Cisco XDR または SecureX との統合を有効にすると自動的に有効になります。これにより、インシデントを Cisco XDR または SecureX Threat Response インシデントマネージャに対応促進させ、合理化できます。Cisco XDR または SecureX に自動的に対応促進されたセキュリティ侵害は、自動的に調査され、Cisco XDR または SecureX Threat Response で利用可能な追加の脅威コンテキストによってエンリッチメントされます。インシデント対応促進を無効にしても、Cisco XDR または SecureX との統合は有効のままにできます。詳細については、「Cisco XDR Incidents」または「SecureX Threat Response」を参照してください。

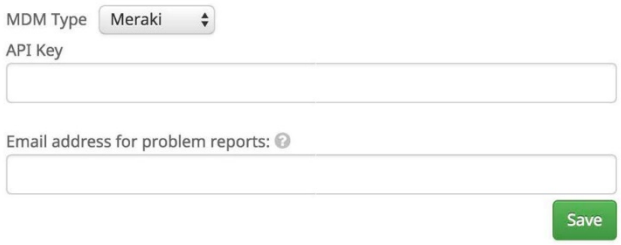
シビラティ（重大度）が低、中、高、およびクリティカルのすべてのインシデントは、デフォルトで Cisco XDR または SecureX に対応促進されます。対応促進されるインシデントが多すぎると感じ、より重大なインシデントのみを表示する場合は、シビラティ（重大度）のしきい値を調整できます。低いシビラティ（重大度）の設定から始めて、最適なシビラティ（重大度）のしきい値が見つかるまで段階的に高い設定にすることを推奨します。

**重要：**以前に Cisco Secure Endpoint の組織を SecureX と統合している場合は、SecureX の古い Cisco Secure Endpoint モジュールを削除し、新しいモジュールのみを使用する必要があります。新しいモジュールでは双方向のデータ交換が可能になりますが、古いモジュールは一方向のみです。

Cisco XDR または SecureX との統合を有効にすると、組織にも API ログイン情報が作成されます。これらのログイン情報には読み取り/書き込み権限が付与され、「[AUTO-GENERATED] SecureX Module API Client」という名前が付けられます。これらのログイン情報は、Cisco Secure Client のインストールトークンの作成にも使用されます。

## MDM の統合

Cisco Secure Endpoint iOS Connector を iOS デバイスに展開する前に、[MDMの統合（MDM Integration）] ページでお使いの Mobile Device Manager を Cisco Secure Endpoint コンソールに接続する必要があります。また、Clarity エンドポイントに表示される、問題発生時にユーザーが連絡できる電子メールアドレスを入力できます。




### Meraki

iOS デバイスに Clarity を展開するには、Meraki SM の API キーを入力する必要があります。Meraki SM の設定の詳細については、[Meraki SM Clarityの設定（Meraki SM Clarity configuration）] ページを参照してください。

Meraki ダッシュボードで以下の手順を実行します。

1. [マイプロファイル（My Profile）] に移動します。
2. [APIアクセス（API Access）] の下で、API キーを選択してコピーします。

Cisco Secure Endpoint コンソールで次の手順を実行します。

1. [ダッシュボード（Dashboard）] ページに移動して、[iOS Clarity] タブを選択します。
2. [MDMの統合（MDM integration）] リンクをクリックします。
3. Meraki API キーを [APIキー（API Key）] フィールドに貼り付けます。API キーは [組織の設定（Organization Settings）] ページでいつでも変更できます。
4. Clarity アプリに表示される、問題発生時にユーザーが連絡できる電子メール アドレスを入力します。
5. [保存（Save）] をクリックします。

Meraki SM に対するグループを変更または追加する必要がある場合は、[管理（Management）] > [Clarity for iOSの展開（Deploy Clarity for iOS）] に移動して、[Clarityの展開（Deploy Clarity）] ページから実行できます。

### Workspace ONE

まず、Clarity を Workspace ONE MDM に追加する必要があります。Workspace ONE ダッシュボードから、以下の手順を実行します。

1. [アプリとブック（Apps & Books）] > [パブリック（Public）] タブに移動します。
2. Clarity アプリがリストに表示されます。表示されない場合は、[アプリケーションの追加（Add Application）] をクリックします。
   - プラットフォームに適した Apple iOS を選択して、「Clarity」を検索します。
   - 検索結果からアプリケーションを選択して、[保存して割り当て（Save & Assign）] をクリックします。
3. [割り当てグループの選択（Select Assignment Groups）] > [割り当てグループの作成（Create Assignment Group）] をクリックして、新しいスマート グループを作成します。
   - スマートグループに [名前（Name）] を割り当てます。
   - [所有権（Ownership）] を [共有（Shared）] と [企業（Corporate）] に設定します。
   - [プラットフォームとオペレーティング システム（Platform and Operating System）] を [Apple iOS]、[より大きい（Greater Than）]、および [iOS 11.2.0] に設定します。
   - [保存（Save）] をクリックします。
4. Clarity の初回追加時には、[割り当ての追加（Add Assignment）] ダイアログが表示されることがあります。
   - [アプリの配信方法（App Delivery Method）] を [自動（Auto）] に設定します。
   - [管理型アクセス（Managed Access）] を [有効化（Enabled）] に設定します。
   - [ユーザーがインストールした場合にアプリをMDM管理対象にする（Make App MDM Managed if User Installed）] を [有効化（Enabled）] に設定します。
   - [追加（Add）] をクリックします。
5. [保存してパブリッシュ（Save & Publish）] をクリックして、[パブリッシュ（Publish）] をクリックします。
6. [アプリとブック（Apps & Books）] の下で Clarity アプリを選択します。[割り当て（Assignment）] タブに自分のスマート グループが表示されていることを確認します。

Cisco Secure Endpoint コンソールで次の手順を実行します。

1. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。

2. [機能（Features）] の下で、[MDMの統合（MDM Integration）] をクリックします。
3. [MDMタイプ（MDM Type）] プルダウンメニューから [Workspace ONE] を選択します。
4. Clarity アプリに表示される、問題発生時にユーザーが連絡できる電子メール アドレスを入力します。
5. [保存（Save）] をクリックします。

### MobileIron

まず、Clarity を MobileIron MDM に追加する必要があります。MobileIron ダッシュボードで以下の手順を実行します。

1. [デバイスとユーザー（Devices & Users）] > [ラベル（Labels）] に移動します。
2. [ラベルの追加（Add Label）] をクリックします。
   - 新しいラベルに [名前（Name）] と [説明（Description）] を割り当てます。
   - [プラットフォーム名（Platform Name）]、[開始場所（Starts with）]、および [iOS 11.2] を設定して、[条件（Criteria）] を追加します。
   - [監視対象（Supervised）]、[同等（Equals）]、および [True] を設定して、別の [条件（Criteria）] を追加します。
   - [保存（Save）] をクリックします。
3. [アプリ（Apps）] > [アプリカタログ（App Catalog）] に移動して、[追加（Add）] をクリックします。
4. [iTunes] をクリックして、Clarity を検索します。
5. 検索結果から Clarity を選択して、[次へ（Next）] をクリックします。
6. 次のページのフィールドの大部分はすでに入力されています。[説明（Description）] と [カテゴリ（Category）] を追加して、[次へ（Next）] をクリックします。
7. [デバイス登録またはサインイン時に、インストール要求またはアプリのアンマネージドからマネージドへの変換要求を送信する（iOS 9 以降）（Send installation request or send convert unmanaged to managed app request (iOS 9 and later) on device registration or sign-in）] を選択して、[次へ（Next）] をクリックします。
8. [アプリ（Apps）] > [アプリ カタログ（App Catalog）] に移動します。
   - [アクション（Actions）] > [ラベルに適用（Apply to Labels）] を選択します。
   - ステップ 2 で作成したラベルを選択します。
   - [適用（Apply）] をクリックします。

Cisco Secure Endpoint コンソールで次の手順を実行します。

1. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。
2. [機能（Features）] の下で、[MDMの統合（MDM Integration）] をクリックします。
3. [MDMタイプ（MDM Type）] プルダウンメニューから [MobileIron] を選択します。

4. Clarity アプリに表示される、問題発生時にユーザーが連絡できる電子メール アドレスを入力します。
5. [保存（Save）] をクリックします。

### その他の MDM

Cisco Secure Endpoint コンソールで次の手順を実行します。

1. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。
2. [機能（Features）] の下で、[MDMの統合（MDM Integration）] をクリックします。
3. [MDMタイプ（MDM Type）] プルダウンメニューから [汎用（Generic）] を選択します。
4. Clarity アプリに表示される、問題発生時にユーザーが連絡できる電子メール アドレスを入力します。
5. シリアル番号と MAC アドレスそれぞれに MDM の設定変数を入力します。
6. [保存（Save）] をクリックします。

**重要：**Clarity を正常に機能させるためには、シリアル番号と MAC アドレスの両方の設定変数を入力する必要があります。

### MDM 統合の削除

MDM 統合を削除するには、[組織の設定（Oranization Settings）] ページに移動し、[編集（Edit）] ボタンをクリックした後、[MDM統合（MDM integration）] の横にある [削除（Delete）] ボタンをクリックします。

## シングル サインオン

シングルサインオン（SSO）は、セキュリティを向上させながらユーザーログインプロセスを合理化する機能です。SSO を使用するには、ユーザー、サードパーティの ID プロバイダー（IdP）、および Cisco Secure Endpoint アカウントの 3 つの部分が必要です。SSO が有効になると、認証では次の手順が実行されます。

1. ユーザーは Cisco Secure Endpoint SSO ログインページに接続し、ユーザー名を入力して認証を得ようとします。
2. ユーザー名が有効な場合、ユーザーの認証要求はサードパーティの ID プロバイダーにリダイレクトされます。
3. サードパーティの ID プロバイダーがユーザーを検証します。
4. 認証に成功すると、ユーザーは自分のアカウントにアクセスできます。

Cisco Secure Endpoint シングルサインオンは SAML 2.0 をサポートしています。Cisco Secure Endpoint を設定して Cisco Secure Sign-On を使用することも、カスタムの

サードパーティ ID プロバイダーを使用することもできます。このドキュメントでは、ID プロバイダーがユーザーとともに設定されていることを前提としています。Cisco Secure Sign-Onの詳細については、https://cisco.com/go/securesignon を参照してください。

### 警告

組織でシングルサインオンを有効にする場合は、次の点に注意してください。

- すべてのユーザーは、ID プロバイダーに登録されている電子メールアドレスと同じ電子メールアドレスを持つアカウントが必要です。電子メールアドレスが ID プロバイダーのものと一致していないユーザーがいる場合、そのユーザーはコンソールにログインできません。それらのユーザーのシングルサインオンを無効にする場合は、サポートに連絡してください。
- Cisco Secure Sign-On を SAML プロバイダーとして使用する場合は、組織内のすべてのアカウントが Cisco Secure Sign-On アカウントを所有している必要があります。Cisco Secure Sign-On アカウントは https://sign-on.security.cisco.com/ で作成できます。ユーザーに電子メールが送信されますので、7 日以内にアカウントを有効化する必要があります。アカウントのないユーザーはサインインできません。
- すべてのユーザーパスワードは、標準のユーザー名とパスワード方式を使用してユーザーがログインしないようにリセットされます。管理者ユーザーは、ワンタイムパスワードを作成できます。
- 各ユーザーの二要素認証は無効になります。シングルサインオンを無効にした場合、二要素認証を再度有効にする必要があります。
- Secure Sign-On を無効にしたユーザーが必要な場合は、サポートに連絡してください。

## Cisco Security Cloud Sign-On を使用したシングルサインオンの有効化

組織で Cisco Security Cloud Sign-On を有効にするには、次の手順を実行します。

1. Cisco Secure Endpoint 管理者アカウントにログインします。
2. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。
3. [シングルサインオンの設定（Single Sign-On）] リンクをクリックします。
4. [Cisco Security Cloud Sign-On] を選択します。これにより、[SAML設定（SAML Configuration ）] ページが表示されます。

5. https://sign-on.security.cisco.com に移動し、[サインアップ（Sign up）] をクリックして、Cisco Security Cloud Sign-On アカウントを作成します。このアカウントの作成の詳細については、『Cisco Security Cloud Sign-On クイックスタートガイド』を参照してください。

   **重要事項：**Cisco Security Cloud Sign-On を SAML プロバイダーとして使用する場合は、組織内のすべてのアカウントに既存の Cisco Security Cloud Sign-On アカウントがある必要があります。Cisco Security Cloud Sign-On アカウントは https://sign-on.security.cisco.com で作成できます。アカウントのないユーザーはサインインできません。

6. アカウントが作成されたら、[SAML設定（SAML Configuration）] ページに戻り、[設定の確認（Verify Configuration）]をクリックします。
7. Cisco Security Cloud Sign-On アカウントの作成時に指定したログイン情報でサインインします。2 番目の認証要素として Duo Security でログインするように求められます。
8. 設定を確認したら、[SAML設定（SAML Configuration）] ページに表示される警告を確認し、[Cisco Security Cloud Sign-Onの有効化（Enable Cisco Security Cloud Sign-On）] をクリックしてセットアップを完了します。
9. ログイン方法が記載された電子メールが各ユーザーに送信されます。ユーザーは、ユーザー名とパスワードを入力する代わりに、ログインページで [シングルサインオンを使用（Use Single Sign-On）] をクリックし、電子メールアドレスを入力してから [ログイン（Log in）] をクリックしてログインする必要があります。ユーザーが ID プロバイダーにまだ認証されていない場合、認証を得るためにリダイレクトされます。

## カスタムシングルサインオンを使用したシングルサインオンの有効化

既存のサードパーティ ID プロバイダーを使用して組織のシングルサインオンを有効にするには、次の手順に従います。

1. Cisco Secure Endpoint 管理者アカウントにログインします。
2. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。
3. [シングルサインオンの設定（Single Sign-On）] リンクをクリックします。
4. [カスタムシングルサインオン（Custom Single Sign-On）] を選択します。これにより、[SAML設定（SAML Configuration ）] ページが表示されます。
5. [サービスプロバイダーの設定（Service Provider Settings）] で提供された情報を、ID プロバイダーの適切なセットアップページに入力します。ID プロバイダーのシステムでは項目の名前が異なる場合があります。次に例を示します。

- **アサーション コンシューマ サービス URL** は、**SAML アサーション コンシューマ サービス（ACS）**または**シングルサインオン URL と呼ばれる場合があります。**
- **エンティティ ID** は、**SP エンティティ ID** または**オーディエンス URI と呼ばれる場合があります。**

6. 次の点に注意しながら、ID プロバイダーが必要とする追加情報を入力します。
   - Active Directory の場合、[発信要求タイプ（Outgoing Claim Type）] を [電子メールアドレス（Email Address）] に設定します。
   - Okta の場合、[名前ID形式（Name ID format）] を [電子メールアドレス（Email Address）] に、[アプリケーションユーザー名（Application username）] を [電子メール（Email）] に設定します。
7. サードパーティ ID プロバイダーから SAML メタデータファイルをダウンロードするか、SAML メタデータ URL をコピーします。
8. [IDプロバイダーの設定（Identity Provider Settings）] で、SAML メタデータファイルをアップロードするか、SAML メタデータ URL を貼り付けます。
9. [SAML設定の保存（Save SAML Configuration）] をクリックします。
10. [テスト（Test）] をクリックして、設定をテストします。ID プロバイダーにログインするように求められます。テストが成功した場合は、次の手順に進みます。
11. [SAML認証の有効化（Enable SAML Authentication）] をクリックして、設定を完了します。

ログイン方法が記載された電子メールが各ユーザーに送信されます。ユーザーは、ログインページの [シングルサインオンを使用（Use Single Sign-On）] リンクをクリックし、自分の電子メールアドレスを入力してログインする必要があります。

## シングル サインオンの無効化

組織のシングルサインオンを無効にするには、次の手順を実行します。

1. Cisco Secure Endpoint 管理者アカウントにログインします。
2. [アカウント（Accouts）] > [組織の設定（Organization Settings）] に移動します。
3. [シングルサインオンの設定（Single Sign-On）] リンクをクリックします。
4. [SAML認証の無効化（Disable SAML Authentication）] をクリックしてシングルサインオンを無効にします。

パスワードリセットの電子メールが、組織でシングルサインオンを有効化しているすべてのシングルサインオンユーザーに送信されます。ユーザーは、Cisco Secure Endpoint コンソールにログインする前に、自分のパスワードをリセットする必要があります。

**重要：**シングルサインオンを無効にしている管理者は、すぐにパスワードをリセットできます。パスワードリセットの電子メールを待つ必要はありません。

# ライセンス情報

現在のライセンス情報がこのページに表示されます。ページ上部には、組織がコンプライアンスに準拠しているかどうか、使用中のシート数、および使用可能なシート数が表示されます。ライセンスおよびその開始日と終了日も表示されます。

# 監査ログ

監査ログを使用すると、Cisco Secure Endpoint 管理者は、他のコンソールユーザーに影響を与える可能性があるコンソール内の管理イベントを追跡できます。アカウントの作成と削除、パスワードのリセット、ユーザー ログイン、ユーザー ログアウト、レポートの作成と削除、ポリシーの変更などのアクションがすべて追跡されます。各エントリに関連付けられた情報には、日付、影響を受けたオブジェクト、アクション、加えられた変更（該当する場合）、アクションに関連付けられたメッセージ、アクションをトリガーしたユーザー、および接続先の IP アドレスが含まれます。監査ログエントリは 3 年間保存されます。

監査ログをフィルタ処理すると、特定のイベント タイプ、日付範囲、ユーザー、または IP アドレスを表示できます。[タイプ（Type）] には、ポリシー、グループ、感染管理リスト、およびユーザーなどが含まれます。タイプを選択したら、作成、削除、更新など、イベント タイプに固有のイベントを選択できます。[項目（Item）] には、特定のリスト、コンピュータ、グループ、およびユーザーが含まれます。

**重要事項：**5,000 台を超えるコンピュータが記載されている項目リストは、プルダウンメニューに表示することはできません。[コンピュータの管理（Computer Management）] に移動して、フィルタ使用のために監査ログを確認するコンピュータを検索し、該当するコンピュータの [変更の表示（View Changes）] リンクをクリックして、監査ログのフィルタ処理されたビューを表示します。

各監査ログ イベントを展開すると、イベントを生成したユーザー、このときにログインしているコンピュータの IP アドレス、時間と日付など、特定のイベントの詳細を表示できます。

# 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で、Cisco Secure Endpoint の仕組みを理解できます。これは、コンピュータを感染させることなく製品を評価し、その機能を実証するのに役立ちます。

デモデータを有効にすると、Cisco Secure Endpoint コンソールにコンピュータとイベントが追加されるため、マルウェアが検出されたときのダッシュボード、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、およびイベントの動作を確認できます。シミュレートされた隔離セッションを開始および停止することで、エンドポイント隔離機能をテストすることもできます。

**重要：**隔離セッションをシミュレートするには、デモデータコンピュータのグループポリシーでエンドポイント隔離を有効にする必要があります。エンドポイントの隔離は、Windows コネクタバージョン 7.0.5 以降および Mac コネクタバージョン 1.2.1 以降で使用できます。

デモデータは、Cisco Secure Endpoint 展開からのライブデータと共存できますが、一部のデモデータマルウェアのシビラティ（重大度）が原因で、ダッシュボードの侵害の兆候ウィジェットなどの特定のビューで実際のイベントが表示されない可能性があります。

[デモデータの有効化（Enable Demo Data）] をクリックして、コンソールにデータを入力します。

デモデータが有効になっている場合は、[デモデータの無効化（Disable Demo Data）] をクリックして、データを再度削除できます。

[デモデータの更新（Refresh Demo Data）] はデモデータの有効化と同様です。デモデータが有効になっている場合は、それを更新すると、すべてのイベントが更新されるため、その内容が今日のイベントに表示されます。

# アプリケーション

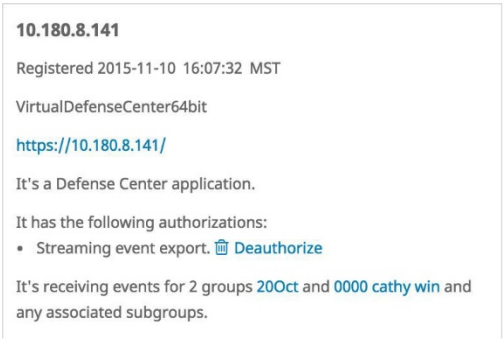
[アプリケーション（Applications）] メニューには、組織のデータへのアクセスを許可した Cisco Secure Endpoint 外部のアプリケーションが表示されます。たとえば、Cisco Secure Firewall Management Center ダッシュボードに Cisco Secure Endpoint のデータを表示できます。

Cisco Secure Firewall と Cisco Secure Endpoint の統合の詳細については、Cisco Secure Firewall のマニュアルを参照してください。

このページから、名前をクリックしてアプリケーション設定を表示したり、アプリケーションにデータを送信しているグループを編集したり、Cisco Secure Endpoint からアプリケーションを完全に登録解除したりできます。

## アプリケーションの設定

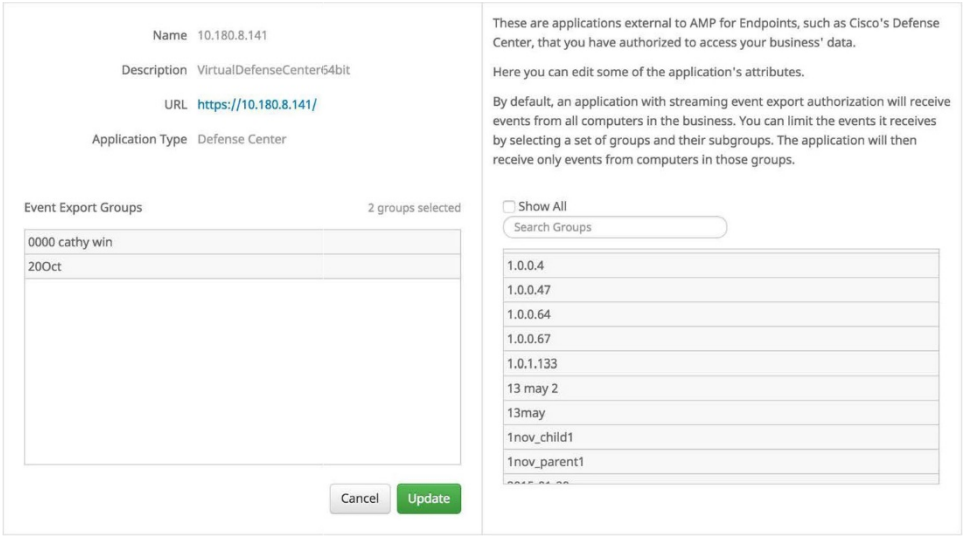
リストからアプリケーションの名前を選択すると、そのアプリケーションの現在の設定が表示されます。




アプリケーションのタイプ、その承認、およびイベントを受信しているグループが表示されます。このビューから、デバイスが受信しているデータ ストリームの認可を解除することもできます。

## アプリケーションの編集

ストリーミングイベントのエクスポートが認可されているアプリケーションは、デフォルトで組織内のすべてのグループからイベントを受信します。




Cisco Secure Endpoint 展開からアプリケーションに送信されるイベントを細かく制御する場合は、右側にあるリストから 1 つ以上のグループを選択します。グループを削除する場合は、左側にある [イベント エクスポート グループ（Event Export Groups）] リストからそのグループを選択します。[イベント エクスポート グループ（Event Export Groups）] リストが空の場合、アプリケーションは、組織内のすべてのグループのすべ

てのコンピュータからイベントを受信します。アプリケーションが Cisco Secure Endpoint からイベントを受信するのを完全に停止するには、メインの [アプリケーション（Applications）] 画面でそのアプリケーションを登録解除する必要があります。

# 第 27 章

# AV 定義の概要

このページには、定義の更新が利用可能になったときに把握できるように、利用可能なウイルス対策定義の最新バージョンが表示されます。

上部の各ボックスに、各オペレーティングシステムで利用可能な定義の最新バージョンが表示されます。各タブには、選択したオペレーティングシステム向けの AV 定義バージョンの一覧が含まれています。ボックスまたはタブをクリックすると、オペレーティングシステムを選択できます。Cisco Secure Endpoint Linux コネクタの場合、完全な ClamAV 定義セットを含むエンドポイントや、Linux 専用定義サブセットを含むエンドポイントを表示できます。

# 第 28 章

# SECUREX

Cisco SecureX はシスコの統合型セキュリティポートフォリオとユーザーのインフラストラクチャを結合させて、一貫した操作性を実現します。共有されたコンテキストと重要なメトリックを使用した統合された可視性が実現され、すぐに利用できる相互運用性を備えた組み込みの統合機能が提供され、セキュリティエコシステム全体にわたる脅威の調査および修復の迅速化によってセキュリティが強化されます。Cisco Secure Endpoint コンソールの SecureX リボンにより、製品から最も関連性の高いセキュリティコンテキストが提供され、調査とピボットを強化できます。

## SecureX のアクティベート

Cisco Security Cloud アカウントを使用して Cisco Secure Endpoint アカウントを SecureX にリンクさせる必要があります。

1. Cisco Secure Endpoint コンソールの下部にある [SecureX] リボンをクリックします。
2. [Get SecureX] をクリックします。
3. [Cisco Security Cloud Sign-Onを使用したログイン（Log in with Security Cloud Sign-On）] をクリックします。
4. [Cisco Secure Endpointの認証（Authorize Secure Endpoint）] をクリックすると、Cisco Secure Endpoint と SecureX の間でデータを共有できます。

SecureX の Cisco Secure Endpoint モジュールは、次の情報を表示できます。

- セキュリティ侵害
- エンドポイントごとの侵害数

- 侵害数の推移
- 上位の侵害の観測対象
- エンドポイントのマルウェア脅威
- 隔離
- 隔離数の推移
- 脆弱性（Vulnerabilities）
- コンピュータ
- 7 日以上検出されていないコンピュータ
- 定義が古いコンピュータ
- コネクタバージョンが最新ではないコンピュータ
- 観測された MITRE ATT&CK の戦術と手法
- SecureX 脅威ハンティング（Premier パッケージのみ）

# SecureX のリボン

SecureX リボンを使用して他の Cisco Security アプリケーションを起動し、Casebook、Threat Response、および Orbital を使用して調査とインシデントを処理できます。また、[ページ上の監視対象の検索（Find observables on page）] ボタンを使用して の現在のページにあるデータポイントを見つけて、Casebook ケースに追加したり、Threat Response でさらに調査したりできます。

SecureX の設定および使用の詳細については、SecureX ダッシュボードのマニュアルを参照してください。リボンを開き、SecureX の横にある [起動（Launch）] をクリックしてから、ページの右上にあるヘルプのアイコンをクリックします。

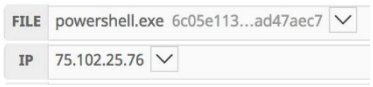
# Casebook

Casebook は、分析結果を保存、共有し、ファイルハッシュ、IP、ドメイン、ログエントリなどを実施中の調査に追加し、ケース全体を Cisco Threat Response に送信して詳細な分析を実施するためのツールです。調査担当者は、メモや説明を追加する、アクティブな Casebook をタブ間で同期させる、他のツールやシステムで使用するためにケースをエクスポートする、といった作業を行うことができます。

SecureX リボンから Casebook にアクセスして、ケースの作成、IP、ドメイン、SHA-256 などの監視対象の追加や調査を実行できます。詳細については、Cisco Threat Response ヘルプ [英語] を参照してください。

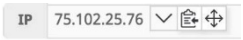
# ピボットメニュー

SecureX が有効になっている場合、すべてのページの監視対象の横にあるピボットメニューボタンをクリックして、Cisco Umbrella、Talos、Cisco Secure Malware Analytics、Cisco Threat Response などの Cisco Advanced Threat ソリューションのアクションにアクセスできます。[SHA-256ファイル情報（SHA-256 File Info）] コンテキストメニュー] はこのピボットメニューに変わります。




**重要：**ピボットメニューに表示される機能は、調査している監視対象の種類によって異なります。

ピボットメニューの上にカーソルを合わせると、2 つのボタンが表示されます。それぞれのボタンをクリックすると、監視対象をクリップボードにコピーしたり、Casebook にドラッグしたりすることができます。



# 第 29 章

# Cisco Secure Endpoint 更新サーバー

Cisco Secure Endpoint 更新サーバーは、TETRA 定義の更新プログラムをシスコサーバーから取得する際に Cisco Secure Endpoint Windows コネクタにより消費される大量のネットワークトラフィックを削減するように設計されています。このユーティリティは、キャッシング HTTP プロキシ サーバーとして動作するか、またはユーザーが設置、構成するオンプレミスの HTTP サーバーの対象となる場所に定期的に更新プログラムを取得することによって、更新による帯域幅使用量を削減します。Windows ポリシーの TETRA セクションで、ローカルの Cisco Secure Endpoint 更新サーバーを有効にする必要があります。Cisco Secure Endpoint 更新サーバーの場合、マルウェア分析クラウドからコンテンツを初めてダウンロードする際に 1 時間以上かかることがあります。

**重要：**Cisco Secure Endpoint Windows コネクタ 5.1.13 以降でのみローカルの Cisco Secure Endpoint 更新サーバーを使用できます。

## 要件

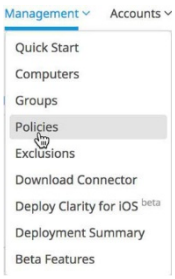
Cisco Secure Endpoint 更新サーバーは、Window Server 2012 と CentOS リリース 6.9（最終）x86_64 でサポートされています。サポートされている Web サーバーは、Apache、Nginx、IIS です。

### ハードウェア要件

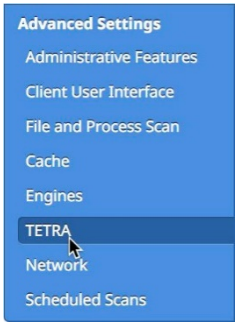
- 8 コア CPU
- 16 GB RAM
- 100 GB の空きディスク スペース

## Cisco Secure Endpoint 更新サーバーのダウンロード

1. [管理（Management）] > [ポリシー（Policies）] に移動します。




2. Windows ポリシーを選択して、[編集（Edit）] をクリックします。
3. ポリシーで、[詳細設定（Advanced Settings）] > [TETRA] に移動します。




4. [Cisco Secure Endpoint更新サーバーの設定（Secure Endpoint Update Server Configuration）] リンクをクリックします。
5. お使いのサーバー オペレーティング システムの [ダウンロード（Download）] ボタンをクリックします。このアーカイブは、お使いのサーバーに転送して解凍する必要があります。
6. サーバーがマルウェア分析クラウドの更新プログラムを確認する間隔を選択し、[ダウンロード（Download）] ボタンをクリックします。手順 5 でアーカイブをダウンロードしたサーバーの同じ場所に config.xml を移動する必要があります。
7. Cisco Secure Endpoint 更新サーバーを設定後、使用する各ポリシーの TETRA セクションに戻り、有効にして設定する必要があります。

# 取得専用モード

このモードでは、ユーザー指定の場所に TETRA 定義の更新プログラムを取得するために Cisco Secure Endpoint 更新サーバーが使用されます。コンテンツのダウンロードに使用する Apache、Nginx、IIS などの HTTP サーバーを設定する必要があります。これは、Windows でのスケジュールされたタスク、または Linux での Cron ジョブとして設定することを推奨します。

## 取得専用単一更新モード

このモードは、UNIX の cron デーモンや Windows のタスク スケジューラなどの定期的なタスク スケジューラで更新ユーティリティを実行するのに適しています。更新頻度の設定は、スケジューラによって効率的な更新頻度が決定されるため使用できません。これは、Cisco Secure Endpoint 更新サーバーを実行する場合に推奨される方法です。

### Linux Cron

更新ユーティリティが書き込む場所を MIRRORDIR 設定で指定する必要があります。

```
./update-linux-[i386 or x86-64] fetch --once --config config.xml
--mirror MIRRORDIR
```

たとえば、TETRA 定義を 1 時間ごとに更新するには、以下を crontab ファイルに追加します。

```
0 * * * * [Full path to binary]/update-linux-[i386 or x86-64]
fetch --once --config [Full path to config]/config.xml - -mirror
MIRRORDIR
```

### Windows のスケジュールされたタスク

以下の手順では、Cisco Secure Endpoint 更新サーバーが次のディレクトリ構造でインストールされていると仮定しています。

C:\AMP

C:\AMP\update-win-x86-64.exe

C:\AMP\config.xml

C:\AMP\mirror

また、ユーティリティが取得モードで 1 時間に 1 回、毎日実行されると仮定しています。

1. タスク スケジューラを起動します。
2. [新しいタスクを作成（Create New Task）] を選択します。
3. [全般（General）] タブを選択します。
   - タスクの [名前（Name）] を入力します。
   - [ユーザーがログオンしているかどうかにかかわらず実行する（Run whether user is logged on or not）] を選択します。

- [構成（Configure for）] ドロップダウンからオペレーティングシステムを選択します。

4. [トリガー（Triggers）] タブを選択します。
   - [新規（New）] をクリックします。
   - [タスクの開始（Begin the task）] ドロップダウンから [スケジュールに従う（On a schedule）] を選択します。
   - [設定（Settings）] で [毎日（Daily）] を選択します。
   - [繰り返し間隔（Repeat task every）] をオンにして、ドロップダウンから [1 時間（1 hour）] を選択します。
   - [有効（Enabled）] がオンになっていることを確認します。
   - [OK] をクリックします。
5. [Actions] タブを選択します。
   - [新規（New）] をクリックします。
   - [アクション（Action）] ドロップダウンから [プログラムの開始（Start a program）] を選択します。
   - [プログラム/スクリプト（Program/script）] フィールドに `C:\AMP\update-win-x86-64.exe` または `C:\AMP\update-win-i386.exe` と入力します。
   - [引数の追加（Add arguments）] フィールドに `fetch --config C:\AMP\config.xml --once --mirror C:\AMP\mirror` と入力します。
   - [開始（Start in）] フィールドに `C:\AMP` と入力します。
   - [OK] をクリックします。
6. [条件（Conditions）] タブを選択します。
   - （オプション）[タスクを実行するためにスリープを解除する（Wake the computer to run this task）] をオンにします。
7. [設定（Settings）] タブを選択します。
   - [タスクが既に実行中の場合に適用される規則（If the task is already running）] で [新しいインスタンスを開始しない（Do not start a new instance）] が選択されていることを確認します。
   - [OK] をクリックします。
8. タスクを実行するアカウントの資格情報を入力します。

## 取得専用定期更新モード

更新ユーティリティは、TETRA 更新を取得して「--mirror」パラメータで指定したディレクトリに格納します。スーパーユーザー モードは必須ではありませんが、更新ユーティリティを実行するユーザー アカウントは、コピー先ディレクトリ（`MIRRORDIR`）に書き込める必要があります。Cisco Secure Endpoint Windows コネクタの TETRA 更新をホストするには、Apache や Nginx などのサードパーティの HTTP サーバーが必要です。MIRRORDIR は更新が保存されるディレクトリです。

**Linux ホスト**

```
./update-linux-[i386 or x86-64] fetch --config config.xml --mirror
MIRRORDIR
```

**Windows ホスト**

```
update-win-[i386 or x86-64] fetch --config config.xml --mirror
MIRRORDIR
```

# 自己ホスト モード

このモードでは、Cisco Secure Endpoint 更新サーバーによって、ユーザーが指定した場所に Cisco Secure Endpoint サーバーから TETRA 定義とマイクロ定義が定期的にダウンロードされ、内蔵の HTTP サーバーを使用してそれらの定義がホストされます。自己ホスト モードは概念実証または小規模な導入での使用を推奨します。ユーザーが Cisco Secure Endpoint 更新サーバーを監視する必要があります。

## 自己ホスト定期取得モード

特権 HTTP ポートにバインドする必要があるため、Cisco Secure Endpoint 更新サーバーはスーパーユーザーモードで実行する必要があります。以下のすべてのケースで、「MIRRORDIR」設定は、更新プログラムを受け取るユーティリティの使用者が指定した場所に設定されており、設定ファイルが更新スクリプトと同じ場所にある場合には、設定ファイルの設定（--config）は省略可能です。

Linux ホスト

```
./update-linux-[i386 or x86-64] host --config config.xml --mirror
MIRRORDIR --server IPADDRESS
```

Windows ホスト

```
update-win-[i386 or x86-64] host --config config.xml --mirror
MIRRORDIR --server IPADDRESS
```

# コンテンツをホストするサードパーティ製 Web サーバーのセットアップ

Cisco Secure Endpoint コネクタを適切に動作させるには、**サーバー** HTTP ヘッダーが必要です。**サーバー** HTTP ヘッダーが無効になっている場合、Web サーバーに以下の設定を追加する必要があります。

### Apache

```
RedirectMatch ^/av64bit_[\d]+/(.*) /av64bit/$1
RedirectMatch ^/av32bit_[\d]+/(.*) /av32bit/$1
```

### Nginx

設定ファイルの「server」セクションに以下を追加する必要があります。

```
rewrite ^/av64bit_[\d]+/(.*)$ /av64bit/$1 permanent;
rewrite ^/av32bit_[\d]+/(.*)$ /av32bit/$1 permanent;
```

### Microsoft IIS

url-rewrite 拡張ファイルがインストールされている必要があります。次の XML スニペットをサーバー設定の /[MIRROR_DIRECTORY]/web.config に追加します。

```
<rewrite>
    <rules>
        <rule name="Rewrite fetch URL">
            <match url="^(.*)_[\d]*\/avx\/(.*)$" />
            <action type="Redirect" url="{R:1}/avx/{R:2}"
appendQueryString="false" />
        </rule>
    </rules>
</rewrite>
```

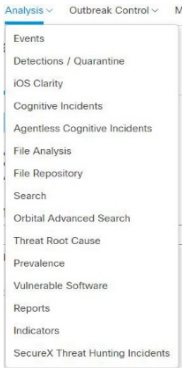
# 第 30 章

# TALOS 脅威ハンティング

Cisco Secure Endpoint Premier のサブスクリプションには Cisco Talos 脅威ハンティングが含まれています。Talos 脅威ハンティングは、Talos と Cisco Efficacy Research Team の両方の専門知識を活用して、環境内で見つかった脅威の特定を支援します。これはアナリスト中心のプロセスであり、このプロセスによって組織は、自動化された予防的および検出的制御で見逃された隠れた高度な脅威を発見できます。脅威を検出した場合、修復を開始できるようにお客様に通知します。

## Talos 脅威ハンティングへのアクセス

Cisco Secure Endpoint アカウントで Talos 脅威ハンティングが有効になっている場合は、[分析（Analysis）] メニューからアクセスできます。



コンソールの右上隅にもアイコンが表示されます。新しいインシデントの数を示すバッジが表示されます（存在する場合）。



インシデントは、[受信トレイ（Inbox ）] タブと [イベント（Events）] タブ、およびインシデントに関係するコンピュータのデバイストラジェクトリにも表示されます。各イベントは Talos 脅威ハンティング インシデント レポートにリンクしています。

# 概要

概要ペインには、組織とグローバルデータの比較情報と、実行された脅威ハントのタイプが表示されます。

## 脅威ハントの概要

脅威ハントの概要には、過去 30 日間の組織とグローバルインシデントの比較が示されます。これは、次の 3 つのカテゴリに分類されます。

- [潜在的な脅威（Potential threats）] : 脅威ハンティングチームが調査している未処理イベントの数。
- [ケース（Cases）] : 脅威ハントのタイプのいずれかをトリガーし、さらに調査する必要がある潜在的脅威イベント。
- [確認済み脅威（Confirmed threat）] : 組織に対して確認された脅威となるケース。

## 脅威ハントのタイプ

脅威ハントのタイプには、過去 30 日間に組織で実行されたハントの 1 日あたりの平均数が示されます。脅威ハントには次の 3 つのタイプがあります。

- [戦術と手法（Tactics & techniques）] : 特定のツールセットの使用、エクスプロイト、またはその他の侵害インシデントに一致する一連のイベントを示すイベントによってトリガーされる行動ベースの脅威ハント。
- [インテリジェンス（Intelligence）] : 世界中で発生している現在のイベントまたはマルウェアインシデントに基づく脅威ハント。これらには、最近公開された脆弱性に基づく脅威ハントも含まれます。
- [異常駆動型（Anomaly driven）] : 予測されるアクティビティ以外で発生したイベントによってトリガーされる脅威ハント。たとえば、通常の勤務時間外にログインしたユーザーや、これまでにログインがなかった国からログインしたユーザーなどです。

# Talos 脅威ハンティングインシデント

[Talos脅威ハンティングインシデント（Talos Threat Hunting Incidents）] ページには、組織のデータの分析によって検出されたインシデントのリストが表示されます。

各レポートには次の情報が示されます。

- 作成された日時
- アナリストによって割り当てられたインシデントの名前
- 採用された戦術および手法
- 組織内の影響を受けたコンピュータの数

レポートを表示するには、インシデントの名前をクリックします。

# Talos 脅威ハンティング インシデント レポート

各インシデントレポートは、インシデントに関する実用的な情報と、可能な場合は修復および緩和手順を提供するようにカスタム作成されます。

## インシデントレポートの概要

概要では、インシデントに関する情報を一目で確認できます。

[インシデントの開始日時（Incident Started at）] は、利用可能なデータに基づいてインシデントが開始されたとアナリストが判断した日時です。この日時は、追加の情報が明らかになると更新される可能性があります。

[インシデントの検出日時（Incident Discovered on）] は、インシデントが発生した証拠をアナリストが最初に発見した日時です。

[戦術（Tactics）] と [手法（Techniques）] には、MITRE ATT&CK ナレッジベースからの情報が含まれます。戦術とは、マルウェアの実行や機密情報の窃取といった攻撃の目的を表します。手法とは、攻撃者が目的を達成するまたはメリットを得るために使用する方法です。詳細については、「ATT&CK の概要」を参照してください。

[概要（Summary）] には、Cisco Secure Endpoint アカウントや使用している他の Cisco XDR または SecureX 製品からのデータを観察することでアナリストがインシデントについて明らかにした詳細情報が表示されます。コンテキストを示すために、インシデントに関係する方法、目的、およびその他の重要な詳細情報が含まれます。

[修復（Remediation）] には、実行できる（または実行する必要がある）アクションに関する推奨事項が含まれます。これには、インシデントから指摘される調査コンポーネントが含まれます。該当する場合は、特定のインシデントに関して可能な緩和策が含まれる場合があります。

[Orbitalクエリ（Orbital Queries）] には、インシデントに関する追加の情報や証拠を収集するために使用できる既存のクエリとカスタム Orbital クエリがあります。

## インシデントレポートのコンピュータ

このセクションには、インシデントに関係していた Cisco Secure Endpoint 展開からのコンピュータのリストが表示されます。そのため、関連するコンピュータに関連付けられているデバイストラジェクトリとイベントを容易に表示し、コネクタで使用されるポリシーに直接移動して変更を加えることができます。

## インシデントレポートのタイムライン

これには、インシデントに関連する Cisco Secure Endpoint コネクタイベントに対応する詳細な実行チェーンが表示されます。

# 付録 A

# 脅威の説明

Secure Endpoint には、独自のネットワーク検出イベントタイプと Indications of Compromise（侵害の兆候）が定義されています。ここでは、これらの検出タイプについて説明します。

**重要事項：**脅威名の説明については、AMP 命名規則を参照してください。

## ファイル分類

コネクタによって観察されるファイルは、次の 3 つの判定結果タイプに分類されます。

- [クリーン（Clean）]：ファイルは、クリーンであるか、信頼できる証明書で署名されていることが分かっています。
- [悪意のある（Malicious）]：ファイルは、マルウェアまたは有害であることが分かっています。
- [不明（Unknown）]：判定に必要なデータが足りません。

## 侵害の兆候

Cisco Secure Endpoint では、過去 7 日間にわたって観察されたイベントに基づくトラジェクトリの侵害の兆候を使用してデバイスが評価されます。単一のクラウド IOC は、エンドポイントごとに 4 時間ごとに 1 回のみ報告されます。悪意のあるファイルの検出、悪

意のあるファイルを繰り返しダウンロードしている親ファイル（ドロッパー感染の可能性）、悪意あるファイルをダウンロードしている複数の親ファイル（複数の感染したファイル）などのイベントはすべて寄与因子です。侵害の兆候には以下が含まれます。

- 脅威の検出：コンピュータ上で 1 つ以上のマルウェアの検出がトリガーされています。
- ドロッパー感染の可能性：ドロッパー感染の可能性は、1 つのファイルが繰り返しコンピュータにマルウェアをダウンロードしようとしていることを示す。
- 複数の感染したファイル：複数の感染したファイルは、コンピュータ上の複数のファイルがマルウェアをダウンロードしようとしていることを示しています。
- 実行されたマルウェア：既知のマルウェア サンプルがコンピュータ上で実行された。この場合は、マルウェアがペイロードを実行した可能性があるため、単純な脅威検出より深刻です。
- 疑わしいボットネット接続：コンピュータが疑わしいボットネット コマンドと制御システムへの外部接続を確立しました。
- [Application] 侵害：疑わしいポータブル実行可能ファイルが Adobe Reader Compromise などの名前のアプリケーションによってダウンロードされ、実行されました。
- [アプリケーション（Applications）] によるシェルの起動：指定されたアプリケーションが不明なアプリケーションを実行し、コマンドシェルが起動されています。Java によるシェルの起動など。
- 汎用 IOC：コンピュータが侵害された可能性を示す疑わしい動作。
- 疑わしいダウンロード：疑わしい URL から実行ファイルをダウンロードしようとしました。ただし、必ずしも URL やファイルに悪意がある（またはエンドポイントが侵害されている）とは限りません。動作の正確な性質を理解するために、ダウンロードの背景やダウンロードしようとしたアプリケーションを詳細に調査する必要があることを示しています。
- Cscript の疑わしい起動：Internet Explorer がコマンド プロンプトを起動し、それによって cscript.exe（Windows Script Host）が実行されました。このイベントのシーケンスは一般的に、ブラウザ サンドボックス エスケープの結果として悪意のある Visual Basic スクリプトが実行されたことを意味しています。
- 疑わしいランサムウェア：既知のランサムウェアに関連付けられた特定のパターンを含むファイル名がコンピュータで確認されました。たとえば、help_decrypt.<filename> という名前のファイルがみつかりました。
- 考えられる webshell：IIS ワーカー プロセス（w3wp）が、powershell.exe などの別のプロセスを起動しました。これは、コンピュータがセキュリティ侵害を受けており、攻撃者へのリモート アクセスが許可されたことを示唆する可能性があります。
- グローバル脅威アラート：グローバル脅威アラートは、高度なアルゴリズム、機械学習、人工知能を使用してユーザーやネットワークデバイスによって生成されるネットワークトラフィックを関連付け、コマンドアンドコントロール トラフィッ

ク、データ漏洩、および悪意のあるアプリケーションを特定します。グローバル脅威アラートによる侵害の兆候イベントは、疑わしいまたは異常なトラフィックが組織内で検出された場合に生成されます。グローバル脅威アラートがシビラティ（重大度） 7 以上を割り当てた脅威のみが Secure Endpoint に送信されます。

**重要事項：**正規のアプリケーションのアクティビティが侵害の兆候として判断される場合があります。正規のアプリケーションは検疫またはブロックされませんが、今後侵害の兆候がトリガーされるのを防ぐために、アプリケーションを [アプリケーション制御（Application Control）] > [[許可されたアプリケーション（Allowed Applications）] に追加してください。

## デバイス フロー コリレーションの検出

デバイス フロー コリレーションを使用すると、疑わしいネットワークアクティビティにフラグを付けたり、ブロックしたりできます。ポリシーを使用すると、疑わしい接続が検出されたときの Cisco Secure Endpoint コネクタの動作に加え、コネクタがアドレスを使用すべき場所（Cisco Intelligence Feed、作成したカスタム IP リスト、または両方の組み合わせ）を指定できます。デバイス フロー コリレーションの検出には以下が含まれます。

- DFC.CustomIPList：コンピュータが、デバイス フロー コリレーションの IP ブロックリストで定義された IP アドレスへの接続を確立しました。
- Infected.Bothost.LowRisk：コンピュータが、ボットネットへの既知の参加者であるコンピュータに属していると見られる IP アドレスへの接続を確立しました。
- CnC.Host.MediumRisk：コンピュータが、過去にボット コマンドと制御チャネルとして使用されたことがわかっている IP アドレスへの接続を確立しました。このコンピュータのデバイストラジェクトリをチェックして、このホストからファイルがダウンロードされ、その後実行されたか確認します。
- ZeroAccess.CnC.HighRisk：コンピュータが、既知の ZeroAccess コマンドと制御チャネルへの接続を確立しました。
- Zbot.P2PCnC.HighRisk：コンピュータが、そのピアツーピアコマンドと制御チャネルを使用して既知の Zbot ピアへの接続を確立しました。
- Phishing.Hoster.MediumRisk：コンピュータが、フィッシング サイトをホストしている可能性のある IP アドレスへの接続を確立しました。コンピュータ フィッシング サイトの多くは他の Web サイトもホストしており、このような無害なサイトのいずれかに接続された可能性もあります。

**重要事項：**デバイス フロー コリレーションは、VPN などのネットワークトンネリングを行うアプリケーションには対応していません。

# 付録 B

# コネクタファイアウォールの例外

シスコのシステムとの通信を Cisco Secure Endpoint コネクタに許可するには、クライアントが特定のポートを介して特定のサーバーに接続することをファイアウォールで許可する必要があります。組織の所在地に応じて、3 組のサーバー（欧州向け、アジア太平洋/中華圏向け、その他の地域向け）から選択できます。すべてのコネクタ（Windows、Mac、Linux、Android、および iOS）は、特定のサーバーにアクセスできる必要がありますが、それ以外は、特定の機能が有効になっている場合にのみ必要になります。

**重要事項：**ファイアウォール上で IP アドレスの除外設定が必要な場合は、この Cisco テクニカルノートを参照してください。

## 北米のファイアウォールの例外

北米にある組織のすべてのコネクタには、コネクタから次のサーバーまでの HTTPS（TCP 443）経由の接続が必要です。

- **イベントサーバー**：intake.amp.cisco.com
- **管理サーバー**：mgmt.amp.cisco.com
- **ポリシーサーバー**：policy.amp.cisco.com
- **エラーレポート**：crash.amp.cisco.com
- **リモートファイル取得**：rff.amp.cisco.com

- **コネクタのアップグレード**：upgrades.amp.cisco.com（TCP 80 および 443）

ファイルとネットワークの分類の検索および登録のためにマルウェア分析クラウドサーバーとの通信をコネクタに許可するには、ファイアウォールで次のサーバーへの TCP 443 経由の接続をクライアントに許可する必要があります。

- **Windows、Mac、および Linux 用のクラウドホスト**：cloud-ec-asn.amp.cisco.com
- **iOS 用のクラウドホスト**：cloud-ios-asn.amp.cisco.com
- **Android 用のクラウドホスト**：cloud-android-asn.amp.cisco.com
- **登録サーバー**：enrolment.amp.cisco.com

Windows、Mac、および Linux コネクタで Orbital を使用するには、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **Orbital の更新**：orbital.amp.cisco.com
- **Orbital のクエリ**：ncp.orbital.amp.cisco.com
- **Orbital のインストーラ**：update.orbital.amp.cisco.com

Windows、Mac、および Linux コネクタで動作保護機能を有効にした場合は、署名更新のために次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **動作保護署名**：apde.amp.cisco.com

Cisco Secure Endpoint Windows コネクタのいずれかで TETRA を有効にした場合は、署名更新のために次のサーバーへの TCP 80 および 443 経由のアクセスを許可する必要があります。

- **更新サーバー**：tetra-defs.amp.cisco.com
- **証明書の検証**：commercial.ocsp.identrust.com、validation.identrust.com

Cisco Secure Endpoint Windows コネクタのいずれかでデバイス制御を有効にした場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **デバイス制御**：endpoints.amp.cisco.com

Cisco Secure Endpoint Windows コネクタでエンドポイント IOC スキャナを使用する場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **エンドポイント IOC ダウンロード**：ioc.amp.cisco.com

エンドポイントに使用させるカスタム検出：高度署名がある場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **高度なカスタムシグニチャ**：custom-signatures.amp.cisco.com

## 欧州連合のファイアウォールの例外

EU 内にある組織のすべてのコネクタは、コネクタから次のサーバーまでの HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベントサーバー：**intake.eu.amp.cisco.com

- **管理サーバー：**mgmt.eu.amp.cisco.com
- **ポリシーサーバー**：policy.eu.amp.cisco.com
- **エラーレポート**：crash.eu.amp.cisco.com
- **リモートファイル取得**：rff.eu.amp.cisco.com
- **コネクタのアップグレード**：upgrades.eu.amp.cisco.com (TCP 80 and 443)

ファイルとネットワークの分類の検索および登録のためにマルウェア分析クラウドサーバーとの通信をコネクタに許可するには、ファイアウォールで次のサーバーへの TCP 443 経由の接続をクライアントに許可する必要があります。

- **Windows、Mac、および Linux 用のクラウドホスト**：cloud-ec-asn.eu.amp.cisco.com
- **iOS 用のクラウドホスト**：cloud-ios-asn.eu.amp.cisco.com
- **Android 用のクラウドホスト**：cloud-android-asn.eu.amp.cisco.com
- **登録サーバー**：enrolment.eu.amp.cisco.com

Windows、Mac、および Linux コネクタで Orbital を使用するには、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **Orbital の更新**：orbital.eu.amp.cisco.com
- **Orbital のクエリ**：ncp.orbital.eu.amp.cisco.com
- **Orbital のインストーラ**：update.orbital.eu.amp.cisco.com

Windows、Mac、および Linux コネクタで動作保護機能を有効にした場合は、署名更新のために次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **動作保護署名**：apde.eu.amp.cisco.com

Cisco Secure Endpoint Windows コネクタのいずれかで TETRA を有効にした場合は、署名更新のために次のサーバーへの TCP 80 および 443 経由のアクセスを許可する必要があります。

- **更新サーバー**：tetra-defs.eu.amp.cisco.com
- **証明書の検証**：commercial.ocsp.identrust.com、validation.identrust.com

Cisco Secure Endpoint Windows コネクタのいずれかでデバイス制御を有効にした場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **デバイス制御**：endpoints.eu.amp.cisco.com

エンドポイント IOC スキャナを使用する場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **エンドポイント IOC ダウンロード**：ioc.eu.amp.cisco.com

エンドポイントに使用させるカスタム検出：高度署名がある場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **高度なカスタムシグニチャ**：custom-signatures.eu.amp.cisco.com

# アジア太平洋地域、日本、および中華圏におけるファイアウォール除外

アジア太平洋地域、日本、および中華圏にある組織のコネクタは、コネクタから次のサーバーまでの HTTPS（TCP 443）経由の接続を許可する必要があります。

- **イベントサーバー**：intake.apjc.amp.cisco.com
- **管理サーバー**：mgmt.apjc.amp.cisco.com
- **ポリシーサーバー：**policy.apjc.amp.cisco.com
- **エラーレポート**：crash.apjc.amp.cisco.com
- **リモートファイル取得**：rff.apjc.amp.cisco.com
- **コネクタのアップグレード**：upgrades.apjc.amp.cisco.com（TCP 80 および 443）

ファイルとネットワークの分類の検索および登録のためにマルウェア分析クラウドサーバーとの通信をコネクタに許可するには、ファイアウォールで次のサーバーへの TCP 443 経由の接続をクライアントに許可する必要があります。

- **Windows、Mac、および Linux 用のクラウドホスト**：cloud-ec-asn.apjc.amp.cisco.com
- **iOS 用のクラウドホスト**：cloud-ios-asn.apjc.amp.cisco.com
- **Android 用のクラウドホスト**：cloud-android-asn.apjc.amp.cisco.com
- **登録サーバー**：enrolment.apjc.amp.cisco.com

Windows、Mac、および Linux コネクタで Orbital を使用するには、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **Orbital の更新**：orbital.apjc.amp.cisco.com
- **Orbital のクエリ**：ncp.orbital.apjc.amp.cisco.com
- **Orbital のインストーラ**：update.orbital.apjc.amp.cisco.com

Windows、Mac、および Linux コネクタで動作保護機能を有効にした場合は、署名更新のために次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **動作保護署名**：apde.apjc.amp.cisco.com

Cisco Secure Endpoint Windows コネクタのいずれかで TETRA を有効にした場合は、署名更新のために次のサーバーへの TCP 80 および 443 経由のアクセスを許可する必要があります。

- **更新サーバー**：tetra-defs.apjc.amp.cisco.com
- **証明書の検証**：commercial.ocsp.identrust.com、validation.identrust.com

Cisco Secure Endpoint Windows コネクタのいずれかでデバイス制御を有効にした場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **デバイス制御**：endpoints.apjc.amp.cisco.com

エンドポイント IOC スキャナを使用する場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **エンドポイント IOC ダウンロード**：ioc.apjc.amp.cisco.com

エンドポイントに使用させるカスタム検出：高度署名がある場合は、次のサーバーへの TCP 443 経由のアクセスを許可する必要があります。

- **高度なカスタムシグニチャ**：custom-signatures.apjc.amp.cisco.com

# 付録 C

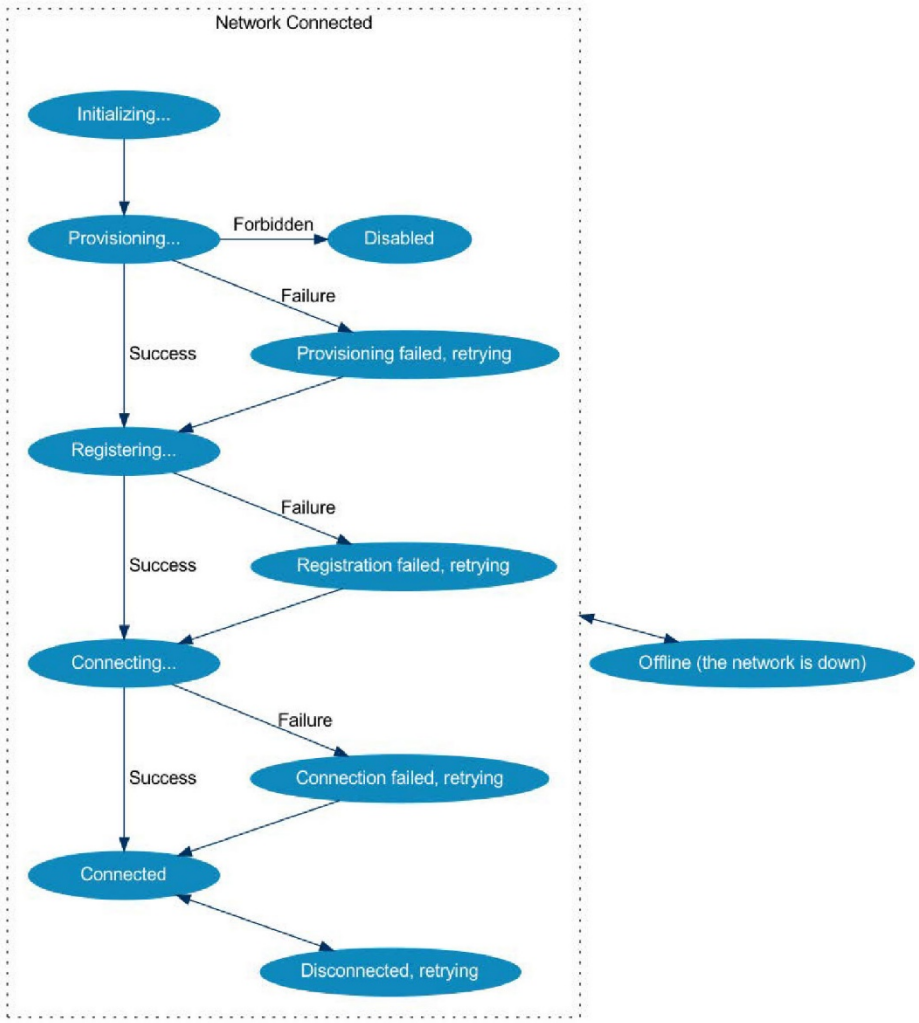
# Mac/Linux コネクタのステータス

Cisco Secure Endpoint Mac コネクタおよび Linux コネクタは、次の組み合わせを表すステータスをレポートします。

- エンドポイント アイデンティティの加入/サブスクリプション
- エンドポイント アイデンティティの登録
- 廃棄サービスの登録
- Cisco Secure Endpoint サービスの接続
- [ネットワーク ステータス（Network Status）]

ステータスは Cisco Secure Endpoint Mac コネクタ UI に表示されます。Mac と Linux の両方で ampcli から `/opt/cisco/amp/ampcli status` コマンドを使用してもアクセスできます。

次の図に、接続プロセスの一般的なフローとステータスの概要を示します。


Network Connected
Initializing...
Provisioning...
Forbidden
Disabled
Failure
Success
Provisioning failed, retrying
Registering...
Failure
Success
Registration failed, retrying
Connecting...
Offline (the network is down)
Failure
Success
Connection failed, retrying
Connected
Disconnected, retrying

次の表に、ステータスインジケータの設定方法を示します。

| ステータス | 説明 | 理由 |
|---|---|---|
| 初期化中... | プログラムを起動/ロードしています。 | 該当なし |
| プロビジョニング中... | エンドポイント アイデンティティの加入/サブスクリプション。 | 該当なし |
| プロビジョニングに失敗し、再試行中... | エンドポイント アイデンティティの加入/サブスクリプションに失敗しました。コネクタは再試行します。 | Cisco Secure Endpoint サービスに到達できません。<br>SSL 証明書が見つかりません。 |
| 登録中... | エンドポイント アイデンティティを登録しています。 | 該当なし |
| 登録に失敗し、再試行中... | エンドポイント アイデンティティの登録に失敗しました。コネクタは再試行します。 | Cisco Secure Endpoint サービスに到達できません。<br>SSL 証明書が見つかりません。 |
| 接続中... | 廃棄サービスに登録しています。 | 該当なし |
| 接続に失敗し、再試行中... | 廃棄サービスへの登録に失敗しました。コネクタは再試行します。 | Cisco Secure Endpoint サービスに到達できません。<br>SSL 証明書が見つかりません。 |
| コネクテッド | 加入および登録に成功しました。Cisco Secure Endpoint サービスに接続されました。コネクタは正常に動作しています。 | 該当なし |
| 無効 | コネクタが動作していません。 | Cisco Secure Endpoint サブスクリプションが無効か、有効期限が切れています。 |
| 切断され、再試行中... | 廃棄サービスへの初期接続が確立された後に、接続が失われました。コネクタは再接続を試行します。 | 廃棄サービスへのネットワーク接続が中断されました。 |
| オフライン（ネットワークがダウン） | ローカルネットワークが切断されました。 | ケーブルが切断されています。<br>ネットワーク インターフェイスが無効になっています。 |

# 付録 D

# 補助ドキュメント

ダウンロード可能な補助ドキュメントは次のとおりです。

## Cisco Secure Endpoint User Guide

次のリンクから、ユーザー ガイドの最新バージョンをダウンロードできます。

ユーザー ガイドをダウンロードする

## Cisco Secure Endpoint Quick Start Guide

このガイドでは、グループ、ポリシー、および除外のセットアップ方法と、Secure Endpoint コネクタ の展開方法について説明します。このガイドは、Secure Endpoint の評価に役立ちます。

クイック スタート ガイドをダウンロードする

## Cisco Secure Endpoint Deployment Strategy Guide

このガイドでは、Secure Endpoint の実稼働環境への導入に向けた準備と計画の詳細に加えて、ベストプラクティスとトラブルシューティングのヒントについても説明します。

導入戦略ガイドをダウンロードする

## Cisco Secure Endpoint Support Documentation

Secure Endpoint の設定、保守、トラブルシューティングに関するテクニカルノートです。

サポート ドキュメンテーション

# 第 D 章

## Cisco エンドポイント IOC 属性

エンドポイント IOC の属性に関するドキュメントには、Secure Endpoint コネクタに搭載されたエンドポイント IOC スキャナでサポートされる IOC の属性が詳しく説明されています。Secure Endpoint コンソールにアップロードできるサンプル IOC ドキュメントも含まれます。

エンドポイント IOC 属性をダウンロードする

## Cisco Secure Endpoint API Documentation

API を使用すると、コンソールにログインしなくても、Secure Endpoint データおよびイベントにアクセスできます。マニュアルは、使用可能なインターフェイス、パラメータ、および例について説明しています。

API マニュアルを参照する

## Cisco Secure Endpoint リリースノート

リリースノートには Secure Endpoint の変更ログが記載されています。

リリース ノートをダウンロードする

## Cisco Secure Endpoint Demo Data Stories

デモデータストーリーでは、Secure Endpoint でデモデータが有効になっている場合に表示される一部の例について説明します。

デバイス制御ドキュメントをダウンロードする

WMIPRVSE ドキュメントをダウンロードする

FriedEx ドキュメントをダウンロードする

WannaCry ランサムウェアのドキュメントをダウンロードする

Cognitive Threat Analytics（CTA）のドキュメントをダウンロードする

コマンドラインのキャプチャに関するドキュメントをダウンロードする

Low Prevalence Executable ドキュメントをダウンロードする

Cryptowall ドキュメントを ダウンロードする

PlugX ドキュメントを ダウンロードする

Upatre ドキュメントを ダウンロードする

CozyDuke ドキュメントを ダウンロードする

SFEICAR ドキュメントをダウンロードする

ZAccess ドキュメントをダウンロードする

ZBot ドキュメントを ダウンロードする

## シスコ ユニバーサル クラウド契約

クラウドオファーの利用規約

# 索引

## P



## S



## T



## W



## Z



## あ



## い



## え



## お



## か



## し

## く



## こ



## し



## す



## せ



## て



## と



## ね



## は



## ひ

## ふ



## ほ



## め



## も



## ゆ



## り



## ろ



## ん