ネットワーク セキュリティ

この章で説明する内容は、次のとおりです。

セキュリティ サービスの設定

この章で説明する内容は、次のとおりです。

セキュリティ サービスの設定の概要

Secure Web Applianceは、セキュリティ コンポーネントを使用してさまざまなマルウェアの脅威からエンド ユーザを保護します。グループ ポリシーごとにマルウェア対策と Web レピュテーション設定値を設定できます。アクセス ポリシーを設定すると、AsyncOS for Web はブロックするコンテンツを判定するときに、マルウェア対策スキャンと Web レピュテーション スコアの組み合わせを使用することを選択できるようになります。

マルウェアからエンドユーザーを保護するには、アプライアンスでこれらの機能をイネーブルにしてから、ポリシーごとにマルウェア対策と Web レピュテーションの設定値を設定します。

オプション	説明	リンク
マルウェア対策スキャン（Anti-malware scanning）	アプライアンスに統合された複数のマルウェア対策スキャン エンジンを使用して、マルウェアの脅威をブロックします。	マルウェア対策スキャンの概要（5 ページ）
Web レピュテーション フィルタ（Web Reputation Filters）	Web サーバーの動作を分析し、URL に URL ベースのマルウェアが含まれているかどうかを判定します。	Web レピュテーション フィルタの概要 （2 ページ）
Advanced Malware Protection	ファイル レピュテーションを評価し、ファイルの特性を分析することによって、ダウンロード ファイルに潜む脅威から保護します。	ファイル レピュテーション フィルタリングとファイル分析の概要（23 ページ）

関連項目

- マルウェア対策とレピュテーション フィルタの有効化 （9 ページ）
- 適応型スキャンについて （8 ページ）

Web レピュテーション フィルタの概要

Web レピュテーション フィルタは、Web ベースのレピュテーション スコア（WBRS）を URL に割り当て、URLベースのマルウェアが含まれている可能性を判断します。 Secure Web Appliance は、Web レピュテーション スコアを使用して、未然にマルウェア攻撃を特定して防ぎます。Web レピュテーション フィルタは、アクセス、復号、および Cisco データ セキュリティの各ポリシーで使用できます。

Web レピュテーション スコア

Web レピュテーション フィルタでは、データを使用してインターネット ドメインの信頼性が評価され、URL のレピュテーションにスコアが付けられます。Web レピュテーションの計算では、URL をネットワーク パラメータに関連付けて、マルウェアが存在する可能性が判定さ

れます。マルウェアが存在する可能性の累計が、-10 ～ +10 の Web レピュテーション スコアにマッピングされます（+10 がマルウェアを含む可能性が最も低い）。

パラメータには、たとえば以下のものがあります。

- URL 分類データ
- ダウンロード可能なコードの存在
- 長く不明瞭なエンドユーザ ライセンス契約書（EULA）の存在
- グローバルなボリュームとボリュームの変更
- ネットワーク オーナー情報
- URL の履歴
- URL の経過時間
- ブロック リストに存在
- 許可リストに存在
- 人気のあるドメインの URL タイプミス
- ドメインのレジストラ情報
- IP アドレス情報

（注） シスコは、ユーザー名、パスフレーズ、クライアント IP アドレスなどの識別情報を収集しません。

Web レピュテーション フィルタの動作のしくみについて

Web レピュテーション スコアは URL 要求に対して実行されるアクションに関連付けられます。各ポリシー グループを設定して、特定の Web レピュテーション スコアにアクションを関連付けることができます。使用可能なアクションは、URL要求に割り当てられているポリシー グループのタイプによって異なります。

ポリシー タイプ	操作
アクセス ポリシー（**Access Policies**）	ブロック、スキャン、または許可から選択できます。
復号ポリシー（**Decryption Policies**）	ドロップ、復号、またはパススルーから選択できます。
シスコ データ セキュリティ ポリシー（**Cisco Data Security Policies**）	ブロックまたはモニターから選択できます。

アクセス ポリシーの Web レピュテーション

アクセス ポリシーに Web レピュテーションを設定する場合は、手動で設定するか、AsyncOS for Web で適応型スキャンを使用して最適なオプションを選択することができます。適応型スキャンがイネーブルの場合は、各アクセス ポリシーで Web レピュテーション フィルタリング

をイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。

スコア	アクション	説明	例
-10 ～ -6.0	ブロック（Block）	不正なサイト。要求はブロックされ、以降のマルウェア スキャンは実行されません。	• URL がユーザーの許可なしに情報をダウンロード。 • URL ボリュームが急上昇。 • URL が人気のあるドメインの誤入力。
-5.9 ～ 5.9	スキャン（Scan）	判別不能なサイト。さらにマルウェア スキャンを行うために、DVS エンジンに要求が渡されます。DVS エンジンは、要求とサーバー応答のコンテンツをスキャンします。	• 動的 IP アドレスを持ち、ダウンロード可能なコンテンツを含む最近作成された URL。 • Web レピュテーション スコアがプラスのネットワーク オーナーの IP アドレス。
6.0 ～ 10.0	許可（Allow）	正常なサイト。要求は許可されます。マルウェア スキャンは必要ありません。	• URL にダウンロード可能なコンテンツが含まれていない。 • 歴史が長く信頼できる大規模ドメイン。 • 複数の許可リストに記載されているドメイン。 • 評価が低い URL へのリンクがない。

デフォルトでは、+7 の Web レピュテーション スコアが割り当てられている HTTP 要求の URL は許可され、さらなるスキャンは必要ありません。しかし、+3 などの低いスコアの HTTP 要求は、マルウェアをスキャンする Cisco DVS エンジンに自動的に転送されます。レピュテーションが非常に低い HTTP 要求の URL はブロックされます。

関連項目

- 適応型スキャンについて （8 ページ）

復号ポリシーの Web レピュテーション

スコア	アクション	説明
-10 ～ -9.0	削除（Drop）	不正なサイト。要求は、エンドユーザーへの通知なしでドロップされます。この設定の使用には注意が必要です。
-8.9 ～ 5.9	復号（Decrypt）	判別不能なサイト。要求は許可されますが、接続が復号され、アクセス ポリシーが復号されたトラフィックに適用されます。

スコア	アクション	説明
6.0 ～ 10.0	パススルー（Pass through）	正常なサイト。要求は、検査や復号なしで渡されます。

Cisco データ セキュリティ ポリシーの Web レピュテーション

スコア	アクション	説明
-10 ～ -6.0	ブロック（Block）	不正なサイト。トランザクションはブロックされ、以降のスキャンは実行されません。
-5.9 ～ 0.0	モニター（Monitor）	トランザクションはWebレピュテーションに基づいてブロックされず、引き続きコンテンツ（ファイルタイプとサイズ）の検査が行われます。 （注） スコアがないサイトはモニターされます。

マルウェア対策スキャンの概要

Secure Web Applianceのマルウェア対策機能は、Cisco DVS™ エンジンとマルウェア対策スキャンエンジンを併用して、Web ベースのマルウェアの脅威を阻止します。DVS エンジンは、Webroot™、McAfee、Sophos マルウェア対策スキャン エンジンと連携します。

スキャン エンジンはトランザクションを検査して、DVS エンジンに渡すマルウェア スキャンの判定を行います。DVSエンジンは、マルウェア スキャンの判定に基づいて、要求をモニターするかブロックするかを決定します。アプライアンスのアンチマルウェア コンポーネントを使用するには、マルウェア対策スキャンをイネーブルにして、グローバル設定値を設定してから、各種のポリシーに特定の設定を適用する必要があります。

関連項目

- マルウェア対策とレピュテーション フィルタの有効化 （9 ページ）
- 適応型スキャンについて （8 ページ）
- McAfee スキャン （7 ページ）

DVS エンジンの動作のしくみについて

DVS エンジンは、Web レピュテーション フィルタから転送された URL のトランザクションに対してマルウェア対策スキャンを実行します。Web レピュテーション フィルタは、特定の URL にマルウェアが含まれている可能性を計算し、URL スコアを割り当てます。このスコアは、トランザクションをブロック、スキャンまたは許可するアクションに関連付けられています。

割り当てられた Web レピュテーション スコアがトランザクションをスキャンすることを示している場合、DVS エンジンは URL 要求とサーバー応答のコンテンツを受信します。DVS エン

ジンはスキャン エンジン（Webroot および（または）Sophos、または McAfee）と連携して、マルウェア スキャンの判定を返します。DVS エンジンは、マルウェア スキャンの判定およびアクセス ポリシーの設定情報を使用して、クライアントへのコンテンツをブロックするか配信するかを判定します。

複数のマルウェア判定の使用

DVS エンジンは、1 つの URL に対して複数のマルウェア判定を下すことがあります。イネーブルなスキャン エンジンの一方または両方から複数の判定が返される場合もあります。

- **異なるスキャン エンジンによるさまざまな判定。**Sophos または McAfee のどちらか一方と Webroot を同時にイネーブルにすると、それぞれのスキャン エンジンが同じオブジェクトに対して異なるマルウェア判定を返すことがあります。イネーブルな両方のスキャン エンジンから 1 つの URL に対して複数の判定が返された場合、アプライアンスは最も制限が厳しいアクションを実行します。たとえば、一方のスキャン エンジンがブロックの判定を返し、他方のスキャン エンジンがモニターの判定を返した場合、DVS エンジンは常に要求をブロックします。
- **同じスキャン エンジンからの異なる判定。**オブジェクトに複数の感染が含まれている場合、1 つのスキャン エンジンが 1 つのオブジェクトに対して複数の判定を返すことがあります。同じスキャン エンジンが 1 つの URL に対して複数の判定を返した場合、アプライアンスは最も優先順位の高い判定に従ってアクションを実行します。以下のリストは、可能性があるマルウェア スキャンの判定を優先順位が高いものから順に示しています。
- ウィルス
- トロイのダウンローダ
- トロイの木馬
- トロイのフィッシャ
- ハイジャッカー
- システム モニター
- 商用システム モニター
- ダイヤラ
- ワーム
- ブラウザ ヘルパー オブジェクト
- フィッシング URL
- アドウェア
- 暗号化ファイル
- スキャン不可
- その他のマルウェア

Webroot スキャン

Webroot スキャン エンジンはオブジェクトを検査してマルウェア スキャンの判定を行い、判定を DVS エンジンに送信します。Webroot スキャン エンジンは、以下のオブジェクトを検査します。

- **URL 要求。**Webroot は URL 要求を評価して、URL にマルウェアの疑いがあるかどうかを判別します。この URL からの応答にマルウェアが含まれている可能性があると Webroot が判断した場合、アプライアンスは、アプライアンス独自の設定に応じて、要求をモニターまたはブロックします。Webroot によって要求が正常である評価された場合、アプライアンスは URL を取得し、サーバーの応答をスキャンします。
- **サーバー応答。**アプライアンスが URL を取得すると、Webroot はサーバー応答のコンテンツをスキャンし、Webroot シグニチャ データベースと照合します。

McAfee スキャン

McAfee スキャン エンジンは、HTTP 応答内の Web サーバからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVS エンジンが要求をモニタするかブロックするかを決定できるようにします。

McAfee スキャン エンジンは以下の方法を使用して、マルウェア スキャンの判定を行います。

- ウィルス シグニチャ パターンの照合
- ヒューリスティック分析

ウィルス シグニチャ パターンの照合

McAfee は、そのデータベース内のウィルス定義をスキャン エンジンに使用し、特定のウィルスや各種のウィルスなどの潜在的に望ましくないソフトウェアを検出します。ファイル内のウィルス シグニチャを検索します。McAfee をイネーブルにした場合、McAfee スキャン エンジンはこの方法を使用して、サーバー応答のコンテンツをスキャンします。

ヒューリスティック分析

ヒューリスティック分析は、特定のルールではなく、一般的なルールを使用して新しいウィルスとマルウェアを検出する手法です。ヒューリスティック分析を使用する場合、McAfee スキャン エンジンは、オブジェクトのコードを確認して一般的なルールを適用し、オブジェクトがどの程度ウィルスに類似しているかを判断します。

ヒューリスティック分析を使用すると、偽陽性（ウイルスと指摘された正常なコンテンツ）の報告が増加し、アプライアンスのパフォーマンスが影響を受ける可能性があります。McAfee をイネーブルにするときに、オブジェクトのスキャンでヒューリスティック分析をイネーブルにするかどうかを選択できます。

McAfee カテゴリ

McAfee の判定	マルウェア スキャン判定カテゴリ
既知のウィルス	ウィルス
トロイの木馬	トロイの木馬
ジョーク ファイル	アドウェア
テスト ファイル	ウィルス

McAfee の判定	マルウェア スキャン判定カテゴリ
ワナビ	ウィルス
不活化	ウィルス
商用アプリケーション	商用システム モニター
望ましくないオブジェクト	アドウェア
望ましくないソフトウェア パッケージ	アドウェア
暗号化ファイル	暗号化ファイル

Sophos スキャン

Sophos スキャン エンジンは、HTTP 応答内の Web サーバーからダウンロードされたオブジェクトを検査します。オブジェクトの検査後、マルウェア スキャンの判定を DVS エンジンに渡し、DVSエンジンが要求をモニターするかブロックするかを決定できるようにします。McAfee アンチマルウェア ソフトウェアがインストールされているときに、McAfee スキャン エンジンではなく、Sophos スキャン エンジンをイネーブルにする必要がある場合があります。

適応型スキャンについて

アダプティブスキャン機能は、どのマルウェア対策スキャンエンジン（ダウンロードファイルの Advanced Malware Protection スキャンを含む）によって Web 要求を処理するかを決定します。

適応型スキャン機能は、スキャンエンジンを実行する前に、マルウェアとして特定するトランザクションに「アウトブレイク ヒューリスティック（Outbreak Heuristics）」マルウェア対策カテゴリを適用します。アプライアンスでマルウェア対策設定を行うときに、これらのトランザクションをブロックするかどうかを選択できます。

適応型スキャンとアクセス ポリシー

適応型スキャンをイネーブルにした場合は、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目の一部がやや異なります。

- 各アクセス ポリシーでは Web レピュテーション フィルタリングをイネーブルまたはディセーブルにできますが、Web レピュテーション スコアは編集できません。
- 各アクセス ポリシーではマルウェア対策スキャンをイネーブルにできますが、どのマルウェア対策スキャンエンジンをイネーブルにするかは選択できません。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。

（注） 適応型スキャンがイネーブルになっておらず、アクセス ポリシーに Web レピュテーションとマルウェア対策の特定の設定項目が設定されている場合に、適応型スキャンをイネーブルにすると、既存の Web レピュテーションとマルウェア対策の設定が上書きされます。

ポリシーごとの Advanced Malware Protection の設定は、適応型スキャンがイネーブルかどうかに関わらず同じです。

マルウェア対策とレピュテーション フィルタの有効化

始める前に

Web レピュテーションフィルタ、DVSエンジン、およびスキャンエンジン（Webroot、McAfee、Sophos）がイネーブルになっていることを確認します。デフォルトでは、システムのセットアップ時にこれらがイネーブルになります。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 必要に応じて、以下の項目を設定します。

設定	説明
Web レピュテーション フィルタリング（Web Reputation Filtering）	Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。
適応型スキャン（Adaptive Scanning）	適応型スキャンをイネーブルにするかどうかを選択します。Web レピュテーション フィルタリングがイネーブルの場合にのみ、適応型スキャンをイネーブルにできます。
ファイル レピュテーション フィルタリングとファイル分析（File Reputation Filtering and File Analysis）	『ファイル レピュテーションと分析サービスの有効化と設定』を参照してください。

設定	説明
AMP for Endpoints コンソールの統合（[詳細設定（Advanced）]>[ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）]）	お使いのアプライアンスを AMP for Endpoints コンソールと統合するには、[AMP for Endpoints コンソールでのアプライアンスの登録（Register the Appliance with Secure Endpoint AMP for Endpoints console）] をクリックします。詳細な手順については、AMP for Endpoints コンソールとアプライアンスの統合 （17 ページ）を参照してください。
DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）	スキャン対象オブジェクト サイズの最大値を指定します。 指定した [最大オブジェクトサイズ（Maximum Object Size）] の値は、すべてのマルウェア対策とウイルス対策スキャン エンジンおよび Advanced Malware Protection 機能によってスキャンされる、要求と応答のサイズ全体に適用されます。これは、アーカイブ検査で検査可能なアーカイブの最大サイズも指定します。アーカイブ検査について詳しくは、アクセス ポリシー：オブジェクトのブロッキングを参照してください。 アップロードまたはダウンロードのサイズがこのサイズを超えると、セキュリティ コンポーネントは、進行中のスキャンを中断し、Web プロキシにスキャンの判定を提供しない可能性があります。検査可能なアーカイブがこのサイズを上回ると、[スキャンされていません（Not Scanned）] と示されます。
Sophos	Sophos スキャン エンジンをイネーブルにするかどうかを選択します。
McAfee	McAfee スキャン エンジンをイネーブルにするかどうかを選択します。 McAfee をイネーブルにするときに、ヒューリスティック スキャンをイネーブルにするかどうかも選択できます。 （注） ヒューリスティック分析はセキュリティ保護を向上させますが、偽陽性が生じてパフォーマンスが低下する可能性があります。
Webroot	Webroot スキャン エンジンをイネーブルにするかどうかを選択します。 Webroot スキャン エンジンをイネーブルにするときに、脅威リスクしきい値（TRT）を設定できます。TRT はマルウェアが存在する確率に対して数値を割り当てます。 独自のアルゴリズムによって URL 照合シーケンスの結果を評価し、脅威リスク レーティング（TRR）を割り当てます。この値は、TRT 設定に関連付けられます。TRR 値が TRT 以上の場合、URL はマルウェアと見なされ、さらなる処理に渡されます。 （注） 脅威リスクしきい値に 90 よりも低い値を設定すると、URL ブロッキング レートが劇的に増加し、正当な要求が拒否されてしまいます。TRT のデフォルト値 90 を維持することを強く推奨します。TRT 設定の最小値は 51 です。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- 適応型スキャンについて （8 ページ）
- McAfee スキャン （7 ページ）

Advanced Malware Protection サービスのキャッシュのクリア

AMP キャッシュ消去機能は、クリーンなファイル、悪意のあるファイル、不明なファイルについて、ファイルレピュテーションの判定結果を消去します。

（注） AMP キャッシュはパフォーマンス向上のために使用されます。**Clear Cache** コマンドを使用すると、キャッシュの再投入中に一時的にパフォーマンスが低下する可能性があります。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [セキュアエンドポイントサービス（Advanced Malware Protection Services）] セクションで、[キャッシュ消去（Clear Cache）] をクリックし、動作を確認します。

ポリシーにおけるマルウェア対策およびレピュテーションの設定

[マルウェア対策およびレピュテーションフィルタ（Anti-Malware and Reputation Filters）] がアプライアンスでイネーブルの場合は、ポリシー グループでさまざまな設定値を設定できます。マルウェア スキャンの判定に基づいて、マルウェア カテゴリのモニターまたはブロックをイネーブルにできます。

以下のポリシー グループにマルウェア対策を設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（Access Policies）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定 （12 ページ）
発信マルウェア スキャン ポリシー（Outbound Malware Scanning Policies）	発信マルウェア スキャン ポリシーによるアップロード要求の制御

以下のポリシー グループに Web レピュテーションを設定できます。

ポリシー タイプ	タスクへのリンク
アクセス ポリシー（**Access Policies**）	アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定 （12 ページ）
復号ポリシー（**Decryption Policies**）	復号ポリシー グループの Web レピュテーション フィルタの設定 （16 ページ）
シスコ データ セキュリティ ポリシー（**Cisco Data Security Policies**）	復号ポリシー グループの Web レピュテーション フィルタの設定 （16 ページ）

アクセスポリシーでのみ Advanced Malware Protection 設定を構成できます。ファイル レピュテーションと分析機能の設定 （28 ページ）を参照してください

アクセス ポリシーにおけるマルウェア対策およびレピュテーションの設定

適応型スキャンがイネーブルの場合、アクセス ポリシーに設定できる Web レピュテーションとマルウェア対策の設定項目は、適応型スキャンがオフの場合とやや異なります。

（注） 展開にセキュリティ管理アプライアンスが含まれており、この機能をプライマリ構成で設定する場合、このページのオプションは、関連するプライマリ構成で適応型セキュリティが有効になっているかどうかに応じて異なります。[Web] > [ユーティリティ（Utilities）] > [セキュリティサービス表示（Security Services Display）] ページで、セキュリティ管理アプライアンスの設定を確認します。

- 適応型スキャンについて （8 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがイネーブルの場合）

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション設定（Web Reputation Settings）] セクションで、Web レピュテーション フィルタリングをイネーブルにするかどうかを選択します。適応型スキャンによって、各 Web 要求に最適な Web レピュテーション スコアのしきい値が選択されます。

ステップ 5 [セキュアエンドポイント設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

ステップ 6 [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7 必要に応じて、ポリシーのマルウェア対策設定を指定します。

疑わしいユーザー エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、トラフィックをスキャンするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。 （注） FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー エージェントとして検出されません。
マルウェア対策スキャンを有効にする（Enable Anti-Malware Scanning）	マルウェアのトラフィックをスキャンするために、DVS エンジンを使用するかどうかを選択します。適応型スキャンによって、各 Web 要求に最適なエンジンが選択されます。
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。 （注） [アウトブレイクヒューリスティック（Outbreak Heuristics）] カテゴリは、スキャン エンジンの実行前に適応型スキャンによってマルウェアとして識別されたトランザクションに適用されます。 （注） 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- 適応型スキャンについて （8 ページ）

マルウェア対策およびレピュテーションの設定（適応型スキャンがディセーブルの場合）

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 設定するアクセス ポリシーの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] リンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション設定（Web Reputation Settings）] セクションで設定項目を設定します。

ステップ 5 [セキュアエンドポイント設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

ステップ 6 [Cisco IronPort DVSマルウェア防御設定（Cisco IronPort DVS Anti-Malware Settings）] セクションまでスクロールします。

ステップ 7 必要に応じて、ポリシーのマルウェア対策設定を指定します。

（注）
Webroot、Sophos、または McAfee スキャンをイネーブルにすると、このページの [マルウェアカテゴリ（Malware Categories）] で、追加のカテゴリをモニターするかブロックするかを選択できます。

設定	説明
疑わしいユーザー エージェント スキャンを有効にする（Enable Suspect User Agent Scanning）	HTTP 要求ヘッダーで指定されているユーザー エージェント フィールドに基づいて、アプライアンスがトラフィックをスキャンできるようにするかどうかを選択します。 このチェックボックスをオンにした場合は、ページ下部の [追加スキャン（Additional Scanning）] セクションで、疑わしいユーザー エージェントをモニターするかブロックするかを選択できます。 （注） FTP-over-HTTP 要求では、Chrome ブラウザはユーザー エージェント文字列を含まないためユーザー エージェントとして検出されません。
Webroot を有効にする（Enable Webroot）	アプライアンスがトラフィックをスキャンする際に、Webroot スキャン エンジンを使用できるようにするかどうかを選択します。

設定	説明
Sophos または McAfee を有効にする（Enable Sophos or McAfee）	アプライアンスがトラフィックをスキャンする際に、Sophos または McAfee スキャン エンジンを使用できるようにするかどうかを選択します。
マルウェア カテゴリ（Malware Categories）	マルウェア スキャンの判定に基づいて各種のマルウェア カテゴリをモニターするかブロックするかを選択します。このセクションに表示されるカテゴリは、上記でイネーブルにするスキャン エンジンによって異なります。
その他カテゴリ（Other Categories）	このセクションに表示されたオブジェクトおよび応答のタイプを、モニターするかブロックするかを選択します。 （注） 設定された最大時間に達した場合や、システムで一時的エラーが発生した場合、URL トランザクションはスキャン不可と分類されます。たとえば、スキャン エンジンのアップデート時や AsyncOS のアップグレード時に、トランザクションがスキャン不可と分類されることがあります。マルウェア スキャンの判定が SV_TIMEOUT や SV_ERROR の場合は、スキャン不可のトランザクションと見なされます。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

- アクセス ポリシーの Web レピュテーション スコアのしきい値の設定 （15 ページ）
- マルウェアのカテゴリについて （21 ページ）

Web レピュテーション スコアの設定

Secure Web Applianceをインストールして設定すると、Web レピュテーション スコアのデフォルト設定が指定されます。ただし、Web レピュテーション スコアのしきい値の設定は組織のニーズに合わせて変更できます。各ポリシー グループに応じた Web レピュテーション フィルタを設定してください。

アクセス ポリシーの Web レピュテーション スコアのしきい値の設定

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

ステップ 2 [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列で、編集するアクセス ポリシー グループのリンクをクリックします。

ステップ 3 [Webレピュテーションとマルウェア対策の設定（Web Reputation and Anti-Malware Settings）] セクションで [Webレピュテーションとマルウェア対策のカスタム設定の定義（Define Web Reputation and Anti-Malware Custom Settings）] を選択します。

これにより、このアクセス ポリシーに対して、グローバル ポリシーとは異なる Web レピュテーションとマルウェア対策の設定を指定できます。

ステップ 4 [Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがイネーブルになっていることを確認します。

ステップ 5 マーカーを動かして、URL のブロック、スキャン、許可の各アクションの範囲を変更します。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

（注）
適応型スキャンがディセーブルの場合は、アクセス ポリシーの Web レピュテーション スコアのしきい値を編集できます。

復号ポリシー グループの Web レピュテーション フィルタの設定

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [復号ポリシー（Decryption Policies）] を選択します。

ステップ 2 [Web レピュテーション（Web Reputation）] 列で、編集する復号ポリシー グループのリンクをクリックします。

ステップ 3 [Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4 [Web レピュテーション フィルタを有効にする（Enable Web Reputation Filtering）] フィールドがオンになっていることを確認します。

ステップ 5 マーカーを動かして、URL のドロップ、復号、およびパススルー アクションの範囲を変更します。

ステップ 6 [スコアを持たないサイト（Sites with No Score）] フィールドで、Web レピュテーション スコアが割り当てられていないサイトの要求に対して実行するアクションを選択します。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

データ セキュリティ ポリシー グループの Web レピュテーション フィルタの設定

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [シスコ データ セキュリティ（Cisco Data Security）] を選択します。

ステップ 2 [Web レピュテーション（Web Reputation）] 列で、編集するデータ セキュリティ ポリシー グループのリンクをクリックします。

ステップ 3 [Web レピュテーション設定（Web Reputation Settings）] セクションで、[Web レピュテーションのカスタム設定の定義（Define Web Reputation Custom Settings）] を選択します。

これにより、グローバル ポリシー グループによる Web レピュテーション設定を上書きすることができます。

ステップ 4 マーカーを動かして、URL のブロックおよびモニター アクションの範囲を変更します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

（注）
Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

AMP for Endpoints コンソールとアプライアンスの統合

お使いのアプライアンスを AMP for Endpoints コンソールと統合すると、 AMP for Endpoints コンソールで以下の操作を実行できます。

- シンプル カスタム検出リストを作成する。
- シンプル カスタム検出リストに新しい悪意のあるファイル SHA を追加する。
- アプリケーション許可リストを作成する。
- アプリケーション許可トリストに新しいファイル SHA を追加する。
- カスタム ポリシーを作成する。
- カスタムポリシーにシンプルカスタム検出リストおよびアプリケーション許可リストを関連付ける。
- カスタム グループを作成する。
- カスタム グループにカスタム ポリシーを関連付ける。
- 登録済みのアプライアンスをデフォルトのグループからカスタム グループに移動する。
- 特定のファイル SHA のファイル トラジェクトリの詳細を表示する。

アプライアンスを AMP for Endpoints コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。

統合後に、ファイル SHA がファイル レピュテーション サーバに送信されると、ファイル SHA に対してファイル レピュテーション サーバーから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。

ファイル SHA がすでにグローバルに悪意のあるものとしてマークされている場合、AMP for Endpoints コンソールで同じファイル SHA をブロックリストに追加すると、ファイルの判定結果は「悪意のあるもの」になります。

[高度なマルウェア防御（Advanced Malware Protection）] レポートページには、新しいセクション、[カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] があります。このセクションには、AMP for Endpoints コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションに [シンプルカスタム検出（Simple Custom Detection）] として表示されます。レポートの [詳細（More Details）] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。

[高度なマルウェア防御（Advanced Malware Protection）] レポートページには、新しいセクション、[カテゴリ別受信悪意のあるファイル（Incoming Malicious Files by Category）] があります。このセクションには、AMP for Endpoints コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブロックリストのファイル SHA の脅威名は、レポートの [悪意のある脅威ファイル（Malicious Threat Files）] セクションに [カスタム検出（Custom Detection）] として表示されます。AMP for Endpoints コンソールでブロックリストに登録されたファイル SHA のファイルトラジェクトリの詳細を表示するには、#unique_646を参照してください。

始める前に

AMP for Endpoints コンソールの管理アクセス権を伴うユーザーアカウントがあることを確認してください。AMP for Endpoints コンソールのユーザーアカウントを作成する方法の詳細については、Cisco TAC にお問い合わせください。

（クラスタ化された設定の場合）クラスタ化された設定では、ログインしているアプライアンスを AMP for Endpoints コンソールにのみ登録できます。アプライアンスを AMP for Endpoints コンソールにスタンドアロンモードですでに登録している場合は、アプライアンスをクラスタに参加させる前に手動で登録を解除してください。

ファイル レピュテーション フィルタリングが有効化され、設定されていることを確認してください。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「ファイル レピュテーションと分析サービスの有効化と設定 」を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 Web インターフェイスの [ファイルレピュテーションとファイル分析（File Reputation and File Analysis）] ページで、[ファイルレピュテーション（File Reputation）] の [詳細設定（Advanced Settings）] パネルにあ

る [AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックします。

[AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックすると、 AMP for Endpoints コンソールのログインページが表示されます。

ステップ 4 Web インターフェイスの [マルウェア対策レピュテーション（Anti-Malware Reputation）] ページで、[ファイルレピュテーション（File Reputation）] の [詳細設定（Advanced Settings）] パネルにある [AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックします。

[AMP for Endpointsへのアプライアンスの登録（Register Appliance with Secure Endpoint AMP for Endpoints）] をクリックすると、 AMP for Endpoints コンソールのログインページが表示されます。

（注）
AMP for Endpoints にアプライアンスを登録する前に、ファイル レピュテーション フィルタリングを有効にし、設定する必要があります。ファイル レピュテーション フィルタリングを有効にして設定する方法については、「ファイル レピュテーションと分析サービスの有効化と設定」を参照してください。

ステップ 5 ご使用のユーザーログイン情報で、AMP for Endpoints コンソールにログインします。

ステップ 6 AMP for Endpoints の認証ページで [許可（Allow）] をクリックして、アプライアンスを登録します。

[許可（Allow）] をクリックすると登録が完了し、アプライアンスの [マルウェア対策レピュテーション（Anti-Malware Reputation）] ページにリダイレクトされます。[AMP for Endpoints コンソールの統合（Secure Endpoint AMP for Endpoints Console Integration）] フィールドに、お使いのアプライアンスの名前が表示されます。アプライアンス名は、 AMP for Endpoints のコンソールページでアプライアンス設定をカスタマイズする際に使用できます。

次のタスク

次の手順：

- AMP for Endpoints コンソールページの [アカウント（Accounts）] > [アプリケーション（Applications）] セクションに移動すると、アプライアンスが AMP for Endpoints コンソールに登録されているかどうかを確認できます。アプライアンス名は、 AMP for Endpoints コンソールページの [アプリケーション（Applications）] セクションに表示されます。
- 登録されたアプライアンスは、デフォルトのポリシー（ネットワーク ポリシー）が関連付けられたデフォルトのグループ（監査グループ）に追加されます。デフォルトポリシーには、ブロックリストまたは許可リストに追加されるファイルSHAが含まれています。AMP for Endpoints の設定をお使いのアプライアンス用にカスタマイズして、ブロックリストまたは許可リストに追加されている独自のファイル SHA を追加する場合は、https://console.amp.cisco.com/docs で AMP for Endpoints のユーザーマニュアルを参照してください。
- アプライアンス接続を AMP for Endpoints コンソールから登録解除するには、アプライアンスの [ファイルレピュテーション（File Reputation）] セクションの [詳細設定（Advanced Settings）] で [登録解除（Deregister）] をクリックするか、または AMP for Endpoints のコ

ンソールページ（https://console.amp.cisco.com/）にアクセスする必要があります。詳細については、https://console.amp.cisco.com/docs で AMP for Endpoints のユーザーマニュアルを参照してください。

（注） ファイル レピュテーション サーバーを別のデータセンターに変更すると、アプライアンスは AMP for Endpoints コンソールから自動的に登録解除されます。ファイル レピュテーション サーバーに選択された同じデータセンターを使用して、アプライアンスを AMP for Endpoints コンソールに再登録する必要があります。

（注） 悪意のあるファイル SHA がクリーンと判定される場合、そのファイル SHA が AMP for Endpoints コンソールで許可リストに追加されていないか確認する必要があります。

データベース テーブルの保持

Web レピュテーション、Webroot、Sophos、および McAfee のデータベースは、Cisco アップデート サーバーから定期的にアップデートを受信します。サーバーのアップデートは自動化されており、アップデート間隔はサーバーによって設定されます。

Web レピュテーション データベース

Secure Web Applianceが保持しているフィルタリング データベースには、統計情報およびさまざまなタイプの要求の処理方法に関する情報が含まれています。また、Cisco SensorBase ネットワーク サーバーに Web レピュテーション統計情報を送信するようにアプライアンスを設定することもできます。SensorBase サーバー情報は SensorBase ネットワークからのデータ フィードに活用され、Web レピュテーション スコアの作成に使用されます。

Web レピュテーション フィルタリング アクティビティおよび DVS スキャンのロギング

アクセス ログ ファイルには、Web レピュテーション フィルタと DVS エンジンから返された各トランザクションの情報が記録されます。アクセス ログのスキャン判定情報セクションには、トランザクションに適用されたアクションの原因を把握するのに役立つ多くのフィールドがあります。たとえば、あるフィールドには、Sopho から DVS エンジンに渡された Web レピュテーション スコアやマルウェア スキャン判定が表示されます。

適応型スキャンのロギング

アクセス ログのカスタム フィールド	W3C ログのカスタム フィールド	説明
%X6	x-as-malware-threat-name	適応型スキャンから返されたマルウェア対策名。トランザクションがブロックされていない場合、このフィールドはハイフン（「-」）を返します。この変数は、スキャン判定情報（各アクセス ログ エントリの末尾の山カッコ内）に含まれています。

適応型スキャンエンジンによってブロックおよびモニターされるトランザクションは、以下のACL デシジョン タグを使用します。

- BLOCK_AMW_RESP
- MONITOR_AMW_RESP

キャッシング

以下のガイドラインは、AsyncOSがマルウェアのスキャン中にキャッシュを使用する仕組みを示しています。

- AsyncOS は、オブジェクト全体がダウンロードされたときにだけオブジェクトをキャッシュします。スキャン中にマルウェアがブロックされた場合、オブジェクト全体はダウンロードされないので、キャッシュされません。
- AsyncOS は、コンテンツの取得元がサーバーであるか Web キャッシュであるかにかかわらず、コンテンツをスキャンします。
- コンテンツがキャッシュされる時間はさまざまな要因によって異なります。デフォルト値はありません。
- AsyncOS は、シグニチャが更新されるとコンテンツを再スキャンします。

マルウェアのカテゴリについて

マルウェアのタイプ	説明
アドウェア	アドウェアには、販売目的でユーザを製品に誘導する、すべてのソフトウェア実行可能ファイルおよびプラグインが含まれます。また、これらのプログラムによってセキュリティ設定が変更されて、ユーザーがシステム設定を変更できなくなる場合もあります。
ブラウザ ヘルパー オブジェクト	ブラウザヘルパーオブジェクトは、広告の表示やユーザー設定の乗っ取りに関連するさまざまな機能を実行する可能性があるブラウザ プラグインです。

マルウェアのタイプ	説明
商用システム モニタ	商用システム モニタは、正当な手段によって正規のライセンスで取得できる、システム モニタの特性を備えたソフトウェアです。
ダイヤラ	ダイヤラは、モデムあるいは別のタイプのインターネット アクセスを利用して、ユーザーの完全な承諾なしに、長距離通話料のかかる電話回線またはサイトにユーザーを接続するプログラムです。
一般的なスパイウェア	スパイウェアはコンピュータにインストールされるタイプのマルウェアで、ユーザに知られることなくその詳細情報を収集します。
ハイジャッカー	ハイジャッカーは、ユーザーの承諾なしにユーザーを Web サイトに誘導したりプログラムを実行したりできるように、システム設定を変更したり、ユーザーのシステムに不要な変更を加えたりします。
悪意のある既知の高リスクファイル	これらは、Advanced Malware Protection ファイル レピュテーション サービスによって脅威と判定されたファイルです。
その他のマルウェア	このカテゴリは、定義済みのどのカテゴリにも当てはまらないマルウェアと疑わしい動作に使用されます。
フィッシング URL	フィッシング URL は、ブラウザのアドレスバーに表示されます。場合によっては、正当なドメインを模倣したドメイン名が使用されます。
PUA	望ましくないアプリケーションのこと。PUA は、悪質ではないが望ましくないと見なされるアプリケーションです。
システム モニター	システム モニターには、以下のいずれかを実行するソフトウェアが含まれます。 • 公然と、または密かに、システム プロセスやユーザ アクションを記録する。 • これらの記録を後で取得して確認できるようにする。
トロイのダウンローダ	トロイのダウンローダは、インストール後にリモート ホスト/サイトにアクセスして、リモート ホストからパッケージやアフィリエイトをインストールするトロイの木馬です。
トロイの木馬	トロイの木馬は、安全なアプリケーションを装う有害なプログラムです。ウイルスとは異なり、トロイの木馬は自己複製しません。
トロイのフィッシャ	トロイのフィッシャは、感染したコンピュータに潜んで特定の Web ページがアクセスされるのを待ったり、感染したマシンをスキャンしてユーザー名とパスフレーズを探したりします。

マルウェアのタイプ	説明
ウイルス	ウイルスは、ユーザーが気付かない間にコンピュータにロードされるプログラムまたはコードです。
ワーム	ワームは、コンピュータ ネットワーク上で自己を複製し、悪質なアクションを実行するプログラムまたはアルゴリズムです。

ファイル レピュテーション フィルタリングとファイル分析

この章で説明する内容は、次のとおりです。

ファイル レピュテーション フィルタリングとファイル分析の概要

Advanced Malware Protection は、次によりゼロデイやファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を常に評価し、脅威と判定されているファイルがネットワークに侵入するとユーザに通知する。

この機能はファイルのダウンロードに使用できます。アップロードされたファイル。

ファイル レピュテーションおよびファイル分析サービスでは、パブリック クラウドまたはプライベート クラウド（オンプレミス）を選択できます。

- プライベートクラウド ファイル レピュテーション サービスは Cisco AMP 仮想プライベートクラウドアプライアンスにより提供され、「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードで動作します。「オンプレミスのファイル レピュテーション サーバの設定 （32 ページ）」を参照してください。
- プライベートクラウド ファイル分析サービスは、オンプレミス Cisco AMP マルウェア分析アプライアンスにより提供されます。オンプレミスのファイル分析サーバの設定 （33 ページ） を参照してください。

ファイル脅威判定のアップデート

新しい情報の出現に伴い、脅威の判定は変化します。最初にファイルが不明または正常として評価されると、ユーザがこのファイルにアクセスできます。新しい情報が利用可能になるのに伴い脅威判定が変更されると、アラートが送信され、ファイルとその新しい判定が [AMP判定のアップデート（AMP Verdict Updates）] レポートに示されます。脅威の影響に対処する最初の作業として、侵入のきっかけとなったトランザクションを調査できます。

判定が「悪意がある」から「正常」に変更されることもあります。

アプライアンスが同じファイルの後続インスタンスを処理するときに、更新された結果がただちに適用されます。

判定アップデートのタイミングに関する情報は、ファイル基準のドキュメント（ファイル レピュテーションおよび分析サービスでサポートされるファイル （26 ページ）を参照）に記載されています。

関連項目

- ファイル レピュテーションおよびファイル分析のレポートとトラッキング （45 ページ）
- ファイルの脅威判定の変更時のアクションの実行 （49 ページ）

ファイル処理の概要

最初に、ファイルのダウンロード元の Web サイトが Web ベース レピュテーション サービス（WBRS）に対して評価されます。

サイトの Web レピュテーション スコアが「スキャン（Scan）」に設定されている範囲内である場合、アプライアンスはトランザクションをスキャンしてマルウェアがあるかどうかを確認し、同時にクラウドベース サービスに対してファイルのレピュテーションを照会します。（サイトのレピュテーション スコアが「ブロック（Block）」範囲内である場合、トランザクションはブロックされるため、ファイルをさらに処理する必要はありません。）スキャン中にマルウェアが検出されると、ファイルのレピュテーションに関係なくトランザクションはブロックされます。

適応型スキャンもイネーブルになっている場合は、ファイル レピュテーション評価とファイル分析は適応型スキャンに含まれます。

アプライアンスとファイル レピュテーション サービス間の通信は暗号化され、改ざんされないように保護されます。

ファイル レピュテーションの評価後：

- ファイルがファイル レピュテーション サービスに対して既知であり、正常であると判断された場合、ファイルはエンドユーザに対して解放されます。
- ファイル レピュテーション サービスから悪意があるという判定が返されると、このようなファイルに対して指定したアクションが、アプライアンスにより適用されます。
- レピュテーションサービスがファイルを認識しているが、決定的な判定を下すための十分な情報がない場合、レピュテーションサービスはファイルの特性（脅威のフィンガープリ

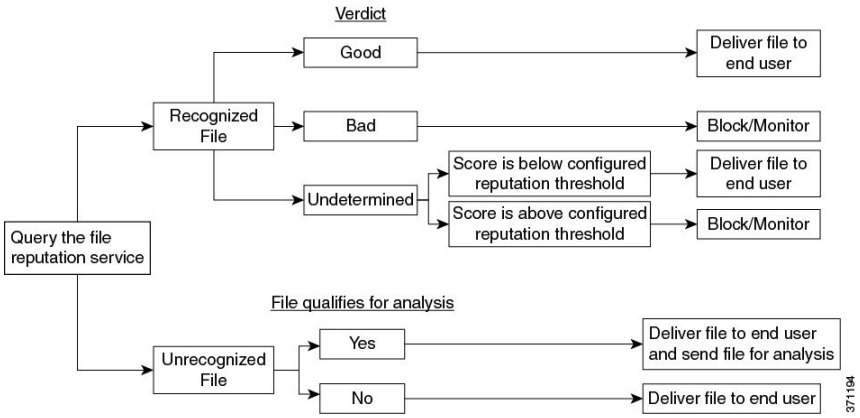
ントや動作分析など）に基づき、脅威スコアを戻します。このスコアが設定されたレピュテーションしきい値を満たすか、または超過した場合、悪意がある、またはリスクの高いファイルに関するアクセス ポリシーで設定したアクションがアプライアンスによって適用されます。

- レピュテーション サービスにそのファイルに関する情報がなく、そのファイルが分析の基準を満たしていない場合（ファイル レピュテーションおよび分析サービスでサポートされるファイル （26 ページ）を参照）、そのファイルは正常と見なされ、エンドユーザに解放されます。
- クラウドベースのファイル分析サービスを有効にしており、レピュテーション サービスにそのファイルの情報がなく、そのファイルが分析できるファイルの基準を満たしている場合（ファイル レピュテーションおよび分析サービスでサポートされるファイル （26 ページ）を参照）は、ファイルは正常と見なされ、任意で分析用に送信されます。
- オンプレミスのファイル分析での展開では、レピュテーション評価とファイル分析は同時に実行されます。レピュテーション サービスから判定が返された場合は、その判定が使用されます。これは、レピュテーション サービスにはさまざまなソースからの情報が含まれているためです。レピュテーション サービスがファイルを認識していない場合、そのファイルはユーザに解放されますが、ファイル分析の結果がローカル キャッシュで更新され、そのファイルのインスタンスの以降の評価に使用されます。
- サーバとの接続がタイムアウトしたためにファイル レピュテーションの判定の情報が利用できない場合、そのファイルはスキャン不可と見なされ、設定されたアクションが適用されます。

低リスク ファイル

当初ファイルが不明で動的コンテンツを含まないと評価された場合、アプライアンスはそのファイルを事前分類エンジンに送信し、事前分類エンジンで低リスクに指定されます。このファイルは分析用にアップロードされません。キャッシュの有効期限内に同じファイルにアクセスした場合、改めて低リスクと評価され、分析用にアップロードされることはありません。キャッシュ タイムアウトの後、同じファイルにもう一度アクセスすると、不明、低リスクと順を追って評価されます。このプロセスは低リスク ファイルに対して繰り返されます。これらの低リスク ファイルはアップロードされないため、ファイル分析レポートには含められません。

図 *1 :* クラウドファイル分析の展開における *Advanced Malware Protection* ワークフロー



ファイルが分析のために送信される場合：

- 分析用にクラウドに送信される場合、ファイルは HTTPS 経由で送信されます。
- 分析には通常、数分かかりますが、さらに時間がかかることもあります。
- ファイル分析で悪意があるとしてフラグ付けされたファイルが、レピュテーション サービスでは悪意があると識別されない場合があります。ファイル レピュテーションは、1 回のファイル分析結果でなく、さまざまな要因によって経時的に決定されます。
- オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用して分析されたファイルの結果は、ローカルにキャッシュされます。

判別のアップデートの詳細については、ファイル脅威判定のアップデート （24 ページ）を参照してください。

ファイル レピュテーションおよび分析サービスでサポートされるファイル

レピュテーション サービスはほとんどのタイプのファイルを評価します。ファイル タイプの識別はファイル コンテンツによって行われ、ファイル拡張子には依存していません。

レピュテーションが不明な一部のファイルは、分析して脅威の特性を調べることができます。ファイル分析機能を設定すると、分析するファイルタイプを選択できます。新しいタイプを動的に追加できます。アップロード可能なファイルタイプのリストが変更された場合はアラートを受け取るので、追加されたファイル タイプを選択してアップロードできます。

ファイル レピュテーションおよび分析サービスでサポートされているファイルの詳細は、登録済みのお客様に限り提供しています。評価と分析の対象となるファイルについて詳しくは、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html から入手できます。ファイル レピュテーションの評価基準、および分析用ファイルの送信基準はいつでも変更できます。

このドキュメントにアクセスするには、シスコの顧客アカウントとサポート契約が必要です。登録するには、https://tools.cisco.com/RPF/register/register.do にアクセスしてください。

[セキュリティサービス（Security Services）] > [マルウェア対策およびレピュテーション（Anti-Malware and Reputation）] ページの [DVSエンジンオブジェクトスキャンの制限（DVS Engine Object Scanning Limits）] の設定も、ファイル レピュテーションと分析の最大ファイル サイズを決定します。

Advanced Malware Protectionが対応しないファイルのダウンロードをブロックするには、ポリシーを設定する必要があります。

（注） どこかのソースからすでに分析用にアップロードしたことのあるファイルは、再度アップロードされません。このようなファイルの分析結果を表示するには、[ファイル分析（File Analysis）] レポート ページから SHA-256 を検索します。

関連項目

- ファイル レピュテーションと分析サービスの有効化と設定 （34 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （44 ページ）
- アーカイブ ファイルまたは圧縮ファイルの処理 （27 ページ）

アーカイブ ファイルまたは圧縮ファイルの処理

ファイルが圧縮またはアーカイブされている場合：

- 圧縮ファイルまたはアーカイブ ファイルのレピュテーションが評価されます。
- 選択されたファイルの種類によっては、圧縮ファイルまたはアーカイブ ファイルは圧縮解除され、すべての抽出されたファイルのレピュテーションが評価されます。

ファイル形式を含めて、検査対象となるアーカイブ ファイルや圧縮ファイルについて詳しくは、ファイル レピュテーションおよび分析サービスでサポートされるファイル （26 ページ）の情報を参照してください。

このシナリオでは、次のようになります。

- 抽出されたファイルのいずれかが悪意のあるファイルである場合、ファイル レピュテーション サービスは、その圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 圧縮/アーカイブ ファイルが悪意のあるファイルであり、抽出されたすべてのファイルが正常である場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します。
- 抽出されたファイルのいくつかの判定が「不明（unknown）」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます（そのように設定されており、ファイル タイプがファイル分析でサポートされている場合）。
- 圧縮/アーカイブ ファイルの圧縮解除中にファイルの抽出に失敗した場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「スキャン不可（Unscannable）」という判定を返します。ただし、抽出されたファイルの 1 つが悪意のあるファイルである場合、ファイル レピュテーション サービスは、圧縮/アーカイブ ファイルに対して「悪意がある（Malicious）」という判定を返します（「悪意がある（Malicious）」という判定は「スキャン不可（Unscannable）」よりも順位が高くなります）。
- 圧縮ファイルやアーカイブファイルは、次のシナリオではスキャン不可として処理されます。
  - データ圧縮率が 20 を超える。
  - アーカイブ ファイルに 5 を超えるレベルのネストが含まれる。
  - アーカイブ ファイルに 200 を超える子ファイルが含まれる。
  - アーカイブ ファイルのサイズが 50 MB を超える。

- アーカイブ ファイルがパスワードで保護されているか、または読み取り不可である。

（注） 1 つ以上の構成ファイルがファイル分析の対象となる場合、Cisco Secure Web Appliance はアーカイブファイル全体を Cisco Secure Malware Analytics に送信します。構成ファイルに悪意のあるものが見つかった場合、アーカイブファイル全体がマルウェアとしてマークされます。

Cisco Secure Web Appliance が圧縮ファイルまたはアーカイブファイルの抽出に失敗した場合、ファイルは分析のために Cisco Secure Malware Analytics にアップロードされます。

（注） セキュア MIME タイプの抽出ファイル（テキストやプレーンテキストなど）のレピュテーションは、評価されません。

クラウドに送信される情報のプライバシー

- クラウド内のレピュテーション サービスには、ファイルを一意に識別する SHA のみが送信されます。ファイル自体は送信されません。
- クラウド内のファイル分析サービスを使用している場合、ファイルが分析の要件を満たしていれば、ファイル自体がクラウドに送信されます。
- 分析用にクラウドに送信されて「悪意がある」と判定されたすべてのファイルに関する情報は、レピュテーション データベースに追加されます。この情報は他のデータと共にレピュテーション スコアを決定するために使用されます。

  オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスで分析されたファイルの情報は、レピュテーションサービスと共有されません。

ファイル レピュテーションと分析機能の設定

- ファイル レピュテーションと分析サービスとの通信の要件 （29 ページ）
- オンプレミスのファイル レピュテーション サーバの設定 （32 ページ）
- オンプレミスのファイル分析サーバの設定 （33 ページ）
- ファイル レピュテーションと分析サービスの有効化と設定
- （パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定 （41 ページ）
- アクセス ポリシーごとのファイル レピュテーションおよび分析サービスのアクションの設定 （43 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （44 ページ）

- Advanced Malware Protection 機能の集約管理レポートの設定 （45 ページ）

ファイル レピュテーションと分析サービスとの通信の要件

- これらのサービスを使用する Secure Web Appliance はすべて（オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用するよう設定されたファイル分析サービスは除く）、インターネット経由で直接サービスに接続できる必要があります。
- デフォルトでは、ファイル レピュテーションおよび分析サービスとの通信は、アプライアンスの管理ポート（M1）経由でルーティングされます。アプライアンスが管理ポートを使用してデータをルーティングしていない場合は、データ インターフェイス経由でのファイル レピュテーション サーバおよびファイル分析サーバへのトラフィックのルーティング （30 ページ）を参照してください。
- ファイルレピュテーションとファイル分析にパブリッククラウドサーバーとプライベート/オンプレミスの組み合わせを使用することはできません。オンプレミスデバイスを使用している場合は、ファイル分析とファイルレピュテーションの両方にオンプレミスのクラウドサーバーが必要です。パブリッククラウドサーバーを使用している場合は、ファイルレピュテーションとファイル分析の両方にパブリッククラウドサーバーが必要です。
- デフォルトでは、ファイル レピュテーションとクラウドベースの分析サービスとの通信は、デフォルト ゲートウェイに関連付けられているインターフェイス経由でルーティングされます。トラフィックを異なるインターフェイス経由でルーティングするには、[セキュリティ サービス（Security Services）]>[ファイル レピュテーションと分析（File Reputation and Analysis）] ページの [詳細設定（Advanced）] セクションで、各アドレスにスタティック ルートを作成します。
- 以下のファイアウォール ポートが開いている必要があります。

ファイアウォール ポート	説明	プロトコル	入力 / 出力	ホストネーム	アプライアンス インターフェイス
32137（デフォルト）または 443	ファイル レピュテーション取得のためのクラウド サービスへのアクセス。	TCP	発信	[セキュリティ サービス（Security Services）]>[マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション：[ファイル レピュテーションの詳細設定（Advanced Settings for File Reputation）] の [クラウド サーバ プール（Cloud Server Pool）] パラメータで設定された名前。	管理（データポート経由でこのトラフィックをルーティングするようにスタティック ルートが設定されている場合を除く）。
443	ファイル分析のためのクラウド サービスへのアクセス。	TCP	発信	[セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション：[ファイル分析の詳細設定（Advanced Settings for File Analysis）] で設定された名前。	

- ファイル レピュテーション機能を設定するときに、ポート 443 で SSL を使用するかどうかを選択します。

関連項目

- ファイル レピュテーションと分析サービスの有効化と設定

データ インターフェイス経由でのファイル レピュテーション サーバおよびファイル分析サーバへのトラフィックのルーティング

（[ネットワーク（Network）]>[インターフェイス（Interfaces）]ページで）アプライアンスの管理ポートがアプライアンス管理サービス専用に設定されている場合は、代わりに、データ ポートを介してファイル レピュテーションおよび分析のトラフィックをルーティングするように、アプライアンスを設定します。

[ネットワーク（Network）]>[ルート（Routes）]ページでデータ トラフィックのルートを追加します。全般的な要件と手順については、次を参照してください。 TCP/IP トラフィック ルートの設定

接続先	宛先ネットワーク	ゲートウェイ
ファイル レピュテーション サービス	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション>[ファイル レピュテーションの詳細設定（Advanced Settings for File Reputation）] セクションで、[ファイル レピュテーション サーバ（File Reputation Server）] にファイル レピュテーション サーバの名前（URL）を指定し、[クラウド ドメイン（Cloud Domain）] にクラウド サーバ プールのクラウド ドメインを指定します。 ファイル レピュテーション サーバのプライベート クラウドを選択する場合は、サーバのホスト名または IP アドレスを入力し、有効な公開キー指定します。これは、プライベート クラウドアプライアンスで使用されるキーと同じである必要があります。 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション : [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] で設定されているクラウド サーバ プールのホスト名。	データ ポートのゲートウェイの IP アドレス。

接続先	宛先ネットワーク	ゲートウェイ
ファイル分析サービス	• [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション > [ファイル レピュテーションの詳細設定（Advanced Settings for File Reputation）] セクションの [ファイル分析サーバ（File Analysis Server）] に、ファイル分析サーバの名前（URL）を指定します。 ファイル分析サーバのプライベート クラウドを選択する場合は、サーバ URL と有効な認証局を指定します。 • ファイル分析クライアント ID は、ファイル分析サーバでのこのアプライアンスのクライアント ID です（読み取り専用）。 [セキュリティサービス（Security Services）]、[マルウェア対策とレピュテーション（Anti-Malware and Reputation）] の [詳細設定（Advanced）] セクション：[ファイル分析の詳細設定（Advanced Settings for File Analysis）] で設定されているファイル分析サーバのホスト名。	データ ポートのゲートウェイの IP アドレス。

関連項目

- TCP/IP トラフィック ルートの設定

オンプレミスのファイル レピュテーション サーバの設定

プライベートクラウドのファイル分析サーバーとして Cisco AMP 仮想プライベート クラウド アプライアンスを使用する場合は、以下のように設定します。

- FireAMP プライベートクラウドのインストールおよび設定に関するガイドを含む、Cisco Advanced Malware Protection 仮想プライベート クラウド アプライアンスのドキュメントは、http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html から取得できます。

  この項目に記載されているタスクはこのドキュメントを参照して実行します。

  AMP 仮想プライベート クラウド アプライアンスのヘルプリンクを使用して、その他のドキュメントも入手できます。

- 「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードでの Cisco AMP 仮想プライベート クラウド アプライアンスを設定および構成します。
- Cisco AMP 仮想プライベート クラウド アプライアンスのソフトウェアバージョンが、Cisco Secure Web Appliance との統合を可能にするバージョン 2.2 であることを確認します。
- AMP 仮想プライベートクラウドの証明書およびキーをそのアプライアンスにダウンロードして、この Secure Web Appliance にアップロードします。

（注） オンプレミスのファイル レピュテーション サーバーを設定した後に、この Secure Web Appliance からこのサーバーへの接続を設定します。ファイル レピュテーションと分析サービスの有効化と設定 （34 ページ） のステップ 6 を参照してください。

オンプレミスのファイル分析サーバの設定

Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合：

- 『Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide』および『Cisco Secure Endpoint Malware Analytics Appliance Administration Guide』を入手してください。Cisco Secure Endpoint マルウェア分析アプライアンスのドキュメントは、https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html から入手できます。

  この項目に記載されているタスクはこのドキュメントを参照して実行します。

  追加のドキュメントは、Cisco Secure Endpoint マルウェア分析アプライアンスのヘルプリンクから入手できます。

  Administration Guide で、次のすべての情報を検索します：他の Cisco アプライアンス（CSA、Cisco Sandbox API Secure Web Appliance）との統合。
- Cisco Secure Endpoint マルウェア分析アプライアンスを設定および構成します。
- 必要に応じて、Cisco Secure Endpoint マルウェア分析アプライアンスのソフトウェアバージョンをバージョン 1.2.1 に更新します。これにより、Cisco Secure Web Appliance との統合がサポートされます。

  バージョン番号を確認し更新を実行する方法については、 AMP マルウェア分析のドキュメントを参照してください。
- アプライアンスがネットワーク上で相互に通信できることを確認します。Cisco Secure Web Appliance は、Cisco Secure Endpoint マルウェア分析アプライアンスの正常な（CLEAN）インターフェイスに接続可能である必要があります。
- 自己署名証明書を展開する場合は、 Secure Web Appliance で使用される Cisco Secure Endpoint マルウェア分析アプライアンスから自己署名 SSL 証明書を生成します。SSL 証明書とキーをダウンロードする手順については、Cisco Secure Endpoint マルウェア分析アプライアン

スの管理者ガイドを参照してください。CN として Cisco Secure Endpoint マルウェア分析アプライアンスのホスト名がある証明書を生成してください。Cisco Secure Endpoint マルウェア分析アプライアンスからのデフォルトの証明書は機能しません。

- マルウェア分析アプライアンスへの Secure Web Appliance の登録は、「ファイル レピュテーションと分析サービスの有効化と設定」で説明したように、ファイル分析の設定を送信したときに自動的に実行されます。ただし、同じ手順に記載されているように、登録をアクティブ化する必要があります。

（注） オンプレミスのファイル分析サーバーを設定した後に、この Secure Web Appliance からこのサーバーへの接続を設定します。『ファイル レピュテーションと分析サービスの有効化と設定』のステップ 7 を参照してください。

ファイル レピュテーションと分析サービスの有効化と設定

始める前に

- ファイル レピュテーションと分析サービスとの通信の要件 （29 ページ）を満たします。
- ファイル レピュテーションと分析サービスにデータ ネットワーク インターフェイスを使用する場合は、アプライアンスでデータ ネットワーク インターフェイスがイネーブルになっていることを確認します。ネットワーク インターフェイスのイネーブル化または変更を参照してください
- アップグレードおよびサービス アップデートの設定で設定したアップデート サーバへの接続を確認します。
- Cisco AMP 仮想プライベート クラウド アプライアンスをプライベートクラウドのファイルレピュテーション サーバーとして使用する場合は、オンプレミスのファイル レピュテーション サーバの設定 （32 ページ） を参照してください。
- Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合は、オンプレミスのファイル分析サーバの設定 （33 ページ） を参照してください。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [ファイル レピュテーション フィルタを有効にする（Enable File Reputation Filtering）] をクリックし、必要に応じて [ファイル分析を有効にする（Enable File Analysis）] をクリックします。

- [ファイル レピュテーション フィルタを有効にする（Enable File Reputation Filtering）] をオンにする場合、[ファイル レピュテーション サーバ（File Reputation Server）] セクションを設定するために（**ステップ 6**）、外部パブリック レピュテーション クラウド サーバの URL を入力するか、プライベート レピュテーション クラウド サーバの接続情報を入力する必要があります。
- 同様に、[ファイル分析を有効にする（Enable File Analysis）] をオンにする場合、[ファイル分析サーバの URL（File Analysis Server URL）] セクションを設定するために（**ステップ 7**）、外部クラウド サーバの URL を入力するか、プライベート分析クラウドの接続情報を入力する必要があります。

（注）
新しいファイル タイプがアップグレード後に追加される場合がありますが、デフォルトでは有効になっていません。ファイル分析を有効にしており、新しいファイル タイプを分析に含めることが必要な場合には、それらを有効にする必要があります。

ステップ 4 ライセンス契約が表示された場合は、それに同意します。

ステップ 5 [ファイル分析（File Analysis）] セクションで、適切なファイル グループ（たとえば、「Microsoft Documents」）からファイル分析のために送信する必要があるファイル タイプを選択します。

サポートされるファイル タイプについては、次のドキュメントの説明を参照してください。ファイル レピュテーションおよび分析サービスでサポートされるファイル （26 ページ）

ステップ 6 [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] パネルを展開し、必要に応じて以下のオプションを調整します。

オプション	説明
クラウド ドメイン（Cloud Domain）	ファイル レピュテーション クエリーに使用するドメインの名前。
ファイル レピュテーション サーバ（File Reputation Server）	パブリック レピュテーション クラウド サーバまたはプライベート レピュテーション クラウド クラウドのホスト名を選択します。 プライベート レピュテーション クラウドを選択する場合は、次の情報を入力します。 • [サーバー（Server）]：Cisco AMP 仮想プライベート クラウド アプライアンスのホスト名または IP アドレス。 • [公開キー（Public Key）]：このアプライアンスとプライベート クラウド アプライアンスとの間の暗号化通信に使用する公開キーを入力します。これは、プライベート クラウド サーバで使用されるキーと同じである必要があります。このアプライアンス上のキー ファイルの位置を指定して、[ファイルのアップロード（Upload File）] をクリックします。 （注） 事前にサーバからこのアプライアンスにキー ファイルをダウンロードしておく必要があります。

オプション	説明
着信サービス一覧（Routing Table）	Advanced Malware Protection サービスに使用する（アプライアンスのネットワーク インターフェイス タイプ（管理またはデータ）に関連付けられている）ルーティングテーブル。アプライアンスで管理インターフェイスと1つ以上のデータ インターフェイスがイネーブルになっている場合は、[管理（Management）] または [データ（Data）] を選択できます。
ファイル レピュテーション用の SSL 通信（SSL Communication for File Reputation）	デフォルト ポート（32137）ではなくポート 443 で通信するには、[SSL（ポート 443）の使用（Use SSL (Port 443)）] をオンにします。サーバーへの SSH アクセスを有効にする方法については、Cisco AMP 仮想プライベート クラウド アプライアンスのユーザーガイドを参照してください。 （注） ポート 32137 で SSL 通信を行うには、ファイアウォールでこのポートを開く必要があります。 このオプションを使用すると、ファイル レピュテーション サービスとの通信用にアップストリーム プロキシを設定できます。オンにする場合、[サーバ（Server）]、[ユーザ名（Username）]、[パスフレーズ（Passphrase）] に適切な情報を入力します。 [SSL（ポート 443）の使用（Use SSL (Port 443)）] がオンにされている場合、[証明書検証の緩和（Relax Certificate Validation）] もオンにすると、（トンネル プロキシ サーバの証明書に信頼できるルート認証局の署名がない場合に）標準の証明書検証をスキップできます。たとえば信頼できる内部トンネル プロキシ サーバの自己署名証明書を使用している場合は、このオプションをオンにします。 （注） [ファイルレピュテーションの詳細設定（Advanced Settings for File Reputation）] の [ファイルレピュテーションの SSL 通信（SSL Communication for File Reputation）] セクションで [SSL（ポート 443）の使用（Use SSL (Port 443)）] をオンにした場合、Web インターフェイスの [ネットワーク（Network）] > [証明書（カスタム認証局）（Certificates (Custom Certificate Authorities)）] を使用して AMP オンプレミス レピュテーション サーバー CA 証明書をこのアプライアンスに追加する必要があります。この証明書をサーバから取得します（[設定（Configuration）] > [SSL] > [クラウド サーバ（Cloud server）] > [ダウンロード（download）]）。
ハートビート間隔（Heartbeat Interval）	レトロスペクティブなイベントを確認するための ping の送信頻度（分単位）。
クエリー タイムアウト（Query Timeout）	レピュテーション クエリーがタイムアウトになるまでの経過秒数。
ファイル レピュテーション クライアント ID（File Reputation Client ID）	ファイル レピュテーション サーバ上のこのアプライアンスのクライアント ID（読み取り専用）

（注）
このセクションの他の設定は、シスコのサポートのガイダンスなしに変更しないでください。

ステップ 7 ファイル分析にクラウド サービスを使用する場合は、[ファイル分析の詳細設定（Advanced Settings for File Analysis）] パネルを展開し、必要に応じて次のオプションを調整します。

オプション	説明
ファイル分析サーバの URL（File Analysis Server URL）	

オプション	説明
	外部クラウド サーバの名前（URL）、または [プライベート分析クラウド（Private analysis cloud）] を選択します。 外部クラウド サーバを指定する場合、アプライアンスに物理的に近いサーバを選択します。新たに使用可能になったサーバは、標準の更新プロセスを使用して、このリストに定期的に追加されます。 ファイル分析にオンプレミス Cisco Secure Endpoint マルウェア分析アプライアンスを使用するプライベート分析クラウドを選択し、次の情報を入力します。 • [TG サーバー（TG Servers）]：スタンドアロンの、またはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの IPv4 アドレスまたはホスト名を入力します。最大 7 つの Cisco Secure Endpoint マルウェア分析アプライアンスを追加できます。 （注） シリアル番号は、スタンドアロンまたはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの追加順序を示しています。アプライアンスの優先順位を示すものではありません。 （注） 1 つのインスタンスにスタンドアロン サーバとクラスタ サーバを追加することはできません。スタンドアロンまたはクラスタのいずれかにする必要があります。 1 つのインスタンスに追加できるスタンドアロン サーバは 1 台のみです。クラスタ モードの場合は 7 台までサーバを追加できますが、すべてのサーバが同じクラスタに属している必要があります。複数のクラスタを追加することはできません。 • [認証局（Certificate Authority）]：[シスコのデフォルト認証局を使用する（Use Cisco Default Certificate Authority）] または [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択します。 [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択する場合、[参照（Browse）] をクリックし、このアプライアンスとプライベート クラウド アプライアンスとの間の暗号化通信に使用する有効な証明書ファイルをアップロードします。これは、プライベート クラウド サーバで使用される証明書と同じである必要があります。 （注） ファイル分析のためにアプライアンスで Cisco Secure Endpoint マルウェア分析ポータルを設定している場合は、Cisco Secure Endpoint マルウェア分析ポータル（https://panacea.threatgrid.eu など）にアクセスし、ファイル分析用に送信されたファイルを表示および追跡できます。Cisco Secure Endpoint マルウェア分析ポータルにアクセスする方法については、Cisco TAC にお問い

オプション	説明
	合わせください。
プロキシの設定	ファイル分析用アップストリーム プロキシとして設定済みの、同じファイル レピュテーション トンネル プロキシを使用するには、[ファイル レピュテーション プロキシを使用する（Use File Reputation Proxy）] チェックボックスをオンにします。 別のアップストリーム プロキシを設定するには、[ファイル レピュテーション プロキシを使用する（Use File Reputation Proxy）] チェックボックスをオフにして、適切な [サーバ（Server）]、[ポート（Port）]、[ユーザ名（Username）]、および[パスフレーズ（Passphrase）] の情報を入力します。
ファイル分析クライアント ID（File Analysis Client ID）	ファイル分析サーバ上のこのアプライアンスのクライアント ID（読み取り専用）

ステップ 8 （任意）ファイル レピュテーション判定結果の値にキャッシュ有効期限を設定する場合は、[キャッシュ設定（Cache Settings）] パネルを展開します。

ステップ 9 許容されるファイル分析スコアの上限を設定するには、[しきい値の設定（Threshold Settings）] パネルを展開します。スコアがこのしきい値を超えた場合は、ファイルが感染していることを示しています。次のいずれかのオプションを選択します。

- クラウド サービスの値を使用（95）（Use value from Cloud Service (60)）
- [カスタム値の入力（Enter Custom Value）] : デフォルトでは 95 に設定されます。

（注）
[しきい値設定（Threshold Settings）] オプションは、[レピュテーションしきい値（Reputation Threshold）] ではなく [ファイル分析しきい値（File Analysis Threshold）] として分類されるようになりました。

ステップ 10 変更を送信し、保存します。

ステップ 11 オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用している場合は、Cisco Secure Endpoint マルウェア分析アプライアンスでこのアプライアンスのアカウントをアクティブ化します。

「ユーザー」アカウントをアクティブ化するための詳細な手順は、Cisco Secure Endpoint マルウェア分析のドキュメントで説明しています。

a) ページセクションの下部に表示されたファイル分析クライアント ID を書き留めます。ここにはアクティブ化する「ユーザ」が表示されます。
b) Cisco Secure Endpoint マルウェア分析アプライアンスにサインインします。
c) **[ようこそ…（Welcome…）] > [ユーザの管理（Manage Users）]** を選択し、[ユーザの詳細（User Details）] に移動します。
d) Secure Web Appliance のファイル分析クライアント ID に基づいて「ユーザー」アカウントを見つけます。

e) アプライアンスの「ユーザ」アカウントをアクティブにします。

重要：ファイル分析設定に必要な変更

新しいパブリック クラウド ファイル分析サービスを使用する場合は、次の説明を読み、データセンターの分離を維持するようにしてください。

- 既存のアプライアンスのグループ化情報は、新しいファイル分析サーバには保存されません。新しいファイル分析サーバでアプライアンスを再グループ化する必要があります。
- ファイル分析隔離エリアに隔離されたメッセージは、保存期間が経過するまで保存されます。隔離エリアでの保存期間が経過すると、メッセージはファイル分析隔離エリアから解放され、 AMP エンジンによって再スキャンされます。その後、ファイルは分析のために新しいファイル分析サーバにアップロードされますが、メッセージがもう一度ファイル分析隔離エリアに送信されることはありません。

詳細については、https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html から Cisco AMP マルウェア分析のドキュメントを参照してください。

（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の任意のアプライアンスから分析用に送信されるファイルに関するクラウド内の分析結果の詳細が表示されるようにするには、すべてのアプライアンスを同じアプライアンスグループに結合する必要があります。

（注） マシン レベルでアプライアンスのグループを設定できます。アプライアンスのグループは、クラスタ レベルで設定することはできません。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 （電子メールゲートウェイでスマートライセンスが無効になっている場合に適用）[アプライアンスID/名前（Appliance ID/Name）] フィールドにグループ ID を手動で入力し、[今すぐグループ化（Group Now）] をクリックします。

または

（電子メールゲートウェイでスマートライセンスが有効になっている場合に適用）システムによりスマートアカウント ID がグループ ID として自動的に登録され、[アプライアンスグループID/名前（Appliance Group ID/Name）] フィールドに表示されます。

注：

- アプライアンスは 1 つのグループだけに属することができます。
- マシンはいつでもグループに追加できます。
- マシンレベルまたはクラスタレベルでアプライアンスのグループを設定できます。
- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすい ID を指定します。この ID は大文字と小文字が区別され、スペースを含めることはできません。
- アプライアンスグループ ID は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、ID はグループ内の以降のアプライアンスでは検証されません。
- アプライアンスグループ ID を更新すると、変更はすぐに有効になります。確定は必要ありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバーを使用するように設定する必要があります。
- スマートライセンシングが有効になっている場合、アプライアンスはスマートアカウント ID を使用してグループ化されます。

ステップ 3 [ファイル分析クラウド レポートのためのアプライアンスのグループ化（Appliance Grouping for File Analysis Cloud Reporting）] セクションで、ファイル分析クラウド レポート グループ ID を入力します。

- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすい ID を指定します。
- この ID は大文字と小文字が区別され、スペースを含めることはできません。
- 指定した ID は、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、ID は以降のグループ アプライアンスでは検証されません。
- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバを使用するように設定する必要があります。
- アプライアンスは 1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

ステップ 4 [アプライアンスをグループに追加（Add Appliance to Group）] をクリックします。

分析グループ内のアプライアンスの確認

手順

ステップ 1 [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。

ステップ 2 [ファイル分析クラウド レポートの用のアプライアンスのグループ化（Appliance Grouping for File Analysis Cloud Reporting）] セクションで、**[グループ内のアプライアンスの表示（View Appliances in Group）]** をクリックします。

ステップ 3 特定のアプライアンスの**ファイル分析クライアント ID** を表示するには、以下の場所を参照します。

アプライアンス	ファイル分析クライアント ID の場所
E メール セキュリティ アプライアンス	[セキュリティ サービス（Security Services）] > [ファイル レピュテーションと分析（File Reputation and Analysis）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション
Secure Web Appliance	[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション
セキュリティ管理アプライアンス	[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [セキュリティアプライアンス（Security Appliances）] ページの下部

アクセス ポリシーごとのファイル レピュテーションおよび分析サービスのアクションの設定

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] を選択します。

ステップ 2 テーブルの [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] 列にあるポリシーのリンクをクリックします。

ステップ 3 [高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで、[ファイル レピュテーション フィルタリングとファイル分析を有効にする（Enable File Reputation Filtering and File Analysis）] を選択します。

ファイル分析がグローバルにイネーブルになっていない場合、ファイル レピュテーション フィルタだけが提供されます。

ステップ 4 [悪意のある既知の高リスク ファイル（Known Malicious and High-Risk Files）] に対してアクション（[モニタ（Monitor）] または [ブロック（Block）]）を選択します。

デフォルトは [モニタリング（Monitor）] です。

ステップ 5 変更を送信し、保存します。

Advanced Malware Protection の問題に関するアラートの確実な受信

Advanced Malware Protectionに関連するアラートを送信するようにアプライアンスが設定されていることを確認します。

以下の場合にアラートを受信します。

アラートの説明	タイプ	重大度
オンプレミス（プライベートクラウド）の Cisco Secure Endpoint マルウェア分析アプライアンスへの接続をセットアップし、ファイル レピュテーションと分析サービスの有効化と設定 に説明されているようにアカウントをアクティブ化する必要があります。	マルウェア対策	警告
機能キーが期限切れになりました	（すべての機能に対する標準）	
ファイル レピュテーションまたはファイル分析サービスに到達できません。	マルウェア対策	警告
クラウドサービスとの通信が確立されました。	マルウェア対策	情報（Info）
		情報（Info）
ファイル レピュテーションの判定が変更されました。	マルウェア対策	情報（Info）
分析用に送信できるファイル タイプが変更された。新しいファイル タイプのアップロードをイネーブルにできます。	マルウェア対策	情報（Info）
一部のファイル タイプの分析が一時的に利用できません。	マルウェア対策	警告
サポートされているすべてのファイル タイプの分析が一時停止後に復旧されます。	マルウェア対策	情報（Info）
無効なファイル分析サービスキーです。このエラーを修正するには、Cisco TAC にファイル分析 ID の詳細を連絡する必要があります。	AMP	エラー（Error）

関連項目

- ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート （50 ページ）
- ファイルの脅威判定の変更時のアクションの実行 （49 ページ）

Advanced Malware Protection 機能の集約管理レポートの設定

セキュリティ管理アプライアンスでレポートを集約管理する場合は、管理アプライアンスに関するオンラインヘルプまたはユーザーガイドの Web レポーティングのトピックの「Advanced Malware Protection」セクションで、重要な設定要件を確認してください。

ファイルレピュテーションおよびファイル分析のレポートとトラッキング

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュア ハッシュ アルゴリズム（SHA-256）を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイルを処理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルはその SHA-256 値でリストされます（短縮形式）。組織のマルウェアインスタンスに関連付けられたファイル名を特定するには、[レポート（Reporting）] > [高度なマルウェア防御（Advanced Malware Protection）] を選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

ファイル レピュテーションとファイル分析レポートのページ

レポート	説明
Advanced Malware Protection	ファイル レピュテーション サービスによって特定されたファイル ベースの脅威を示します。 判定が変更されたファイルについては、[AMP 判定のアップデート（AMP Verdict Updates）] レポートを参照してください。これらの判定は、[高度なマルウェア防御（Advanced Malware Protection）] レポートに反映されません。 圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御（Advanced Malware Protection）] レポートに含まれます。 [カテゴリ別受信マルウェアファイル（Incoming Malware Files by Category）] セクションは、[カスタム検出（Custom Detection）] に分類される、AMP for Endpoints コンソールから受信したブロックリストに登録されたファイル SHA の割合を示しています。 AMP for Endpoints コンソールから取得されるブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル（Incoming Malware Threat Files）] セクションで [シンプルカスタム検出（Simple Custom Detection）] として表示されます。 レポートの [詳細（More Details）] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。 [リスク低（Low Risk）] 判定の詳細をレポートの [AMP により渡された受信ファイル（Incoming Files Handed by AMP）] セクションに表示できます。

レポート	説明
Advanced Malware Protection [ファイル分析（File Analysis）]	分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。 1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。 ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。 SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。 （注） 圧縮/アーカイブ ファイルから抽出したファイルが分析用に送信される場合は、それらの抽出ファイルの SHA 値だけが [ファイル分析（File Analysis）] レポートに含まれます。
Advanced Malware Protection レピュテーション	Advanced Malware Protection は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。 [AMP レピュテーション（AMP Reputation）] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、ファイル脅威判定のアップデート （24 ページ） を参照してください。 1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。 1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。 使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。

その他のレポートでのファイル レピュテーション フィルタ データの表示

該当する場合は、ファイル レピュテーションおよびファイル分析のデータを他のレポートでも使用できます。デフォルトでは、[高度なマルウェア防御でブロック（Blocked by Advanced

Malware Protection）] 列は適用可能なレポートに表示されません。追加列を表示するには、テーブルの下の [列（Columns）] リンクをクリックします。

[ユーザーの場所別のレポート（Report by User Location）] には [高度なマルウェア防御（Advanced Malware Protection）] タブがあります。

Web トラッキング機能と Advanced Malware Protection 機能について

Web トラッキングでファイル脅威情報を検索するときには、以下の点に注意してください。

- ファイル レピュテーション サービスにより検出された悪意のあるファイルを検索するには、Web メッセージ トラッキングの [詳細設定（Advanced）] セクションの [マルウェア脅威（Malware Threat）] エリアの [**マルウェア カテゴリでフィルタ（Filter by Malware Category**）] オプションで **[既知の悪意のある、リスクが高いファイル（Known Malicious and High-Risk Files**）] を選択します。
- Web トラッキングには、ファイル レピュテーション処理に関する情報と、トランザクション メッセージの処理時点で戻された元のファイル レピュテーション判定だけが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。

  検索結果の [ブロック - AMP（Block - AMP）] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

  トラッキングの詳細に表示される [AMP 脅威スコア（AMP Threat Score）] は、ファイルを明確に判定できないときにクラウド レピュテーション サービスが提示するベストエフォート型のスコアです。この場合、スコアは 1 ~ 100 です。（ AMP 判定が返された場合、またはスコアがゼロ の場合は [AMP脅威スコア（AMP Threat Score）] を無視してください）。アプライアンスはこのスコアをしきい値スコア（[セキュリティ サービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] ページで設定）と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ～ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアの変更は推奨されません。WBRS スコアは、ファイルのダウンロード元サイトのレピュテーションであり、ファイル レピュテーションとは関係ありません。
- 判定の更新は [AMP 判定の更新（AMP Verdict Updates）] レポートだけに表示されます。Web トラッキングの元のトランザクション の詳細は、判定の変更によって更新されません。特定のファイルに関連するトランザクションを確認するには、判定アップデート レポートで SHA-256 リンクをクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドまたはオンプレミスのファイル分析サーバーから入手できます。ファイルについて使用可能なすべてのファイル分析情報を確認するには、[レポート（Reporting）] > [ファイル分析（File Analysis）] を選択し、ファイルで検索する SHA-256 を入力するか、または Web トラッキングの詳細で SHA-256 リンクをク

リックします。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析目的で送信されたファイルの後続インスタンスがアプライアンスにより処理される場合、これらのインスタンスは、Web トラッキング検索結果に表示されます。

ファイルの脅威判定の変更時のアクションの実行

手順

ステップ 1 [AMP 判定の更新（AMP Verdict updates）] レポートを表示します。

ステップ 2 該当する SHA-256 リンクをクリックします。エンドユーザに対してアクセスが許可されていたファイルに関連するすべてのトランザクションの Web トラッキング データが表示されます。

ステップ 3 トラッキング データを使用して、侵害された可能性があるユーザと、違反に関連するファイルの名前やファイルのダウンロード元 Web サイトなどの情報を特定します。

ステップ 4 ファイルの脅威の動作を詳細に把握するために、[ファイル分析（File Analysis）] レポートを検証して、この SHA-256 が分析用に送信されたかどうかを確認します。

次のタスク

関連項目

ファイル脅威判定のアップデート （24 ページ）

ファイル レピュテーションと分析のトラブルシューティング

ログ ファイル

ログの説明：

- `AMP` と `amp` は、ファイル レピュテーション サービスまたはエンジンを示しています。
- `Retrospective` は判定のアップデートを示しています。
- `VRT` と `sandboxing` はファイル分析サービスを示しています。

ファイル分析を含む Advanced Malware Protectionに関する情報は、アクセスログまたは AMP エンジンのログに記録されます。詳細については、ログによるシステムアクティビティのモニタリングに関するトピックを参照してください。

ログ メッセージ「ファイル レピュテーション クエリーに対する受信応答（Response received for file reputation query）」の「アップロードアクション（upload action）」の値は以下のようになります。

- 1：送信。（1: SEND.）この場合、ファイル分析のためにファイルを送信する必要があります。
- 2：送信しない。（2: DON'T SEND.）この場合は、ファイル分析用にファイルを送信しません。
- 3：メタデータのみを送信。（3: SEND ONLY METADATA.）この場合、ファイル分析のためにファイル全体ではなく、メタデータのみを送信します。
- 0：アクションなし。（0: NO ACTION.）この場合、他のアクションは不要です。

ファイル レピュテーション サーバまたはファイル分析サーバへの接続失敗に関する各種アラート

問題

ファイル レピュテーション サービスまたは分析サービスへの接続の失敗に関するアラートをいくつか受信した。（単一のアラートは一時的な問題のみを示していることがあります。）

解決方法

- ファイル レピュテーションと分析サービスとの通信の要件 （29 ページ）に記載されている要件を満たしていることを確認します。
- アプライアンスとクラウドサービスとの通信を妨げている可能性があるネットワークの問題を確認します。
- [クエリー タイムアウト（Query Timeout）] の値を大きくします。

  [セキュリティサービス（Security Services）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。[高度なマルウェア防御サービス（Advanced Malware Protection Services）] セクションの [詳細設定（Advanced settings）] エリアの [クエリタイムアウト（Query Timeout）] の値。

API キーのエラー（オンプレミスのファイル分析）

問題

ファイル分析レポートの詳細を表示しようとした場合や、分析用ファイルをアップロードするのに Secure Web Appliance が AMP マルウェア分析サーバーに接続できない場合、API キーのアラートを受信します。

解決方法

このエラーは、 AMP マルウェア分析サーバのホスト名を変更し、 AMP マルウェア分析サーバーの自己署名証明書を使用する場合に発生します。また、他の状況でも発生する可能性があります。この問題を解決するには、次の手順を実行します。

- 新しいホスト名がある AMP マルウェア分析アプライアンスから新しい証明書を生成します。
- Secure Web Appliance に新しい証明書をアップロードします。
- AMP マルウェア分析アプライアンスの API キーをリセットします。手順については、AMP マルウェア分析アプライアンスのオンラインヘルプを参照してください。

関連項目

- ファイル レピュテーションと分析サービスの有効化と設定

ファイルが予想どおりにアップロードされない

問題

ファイルが予想どおりに評価または分析されていません。アラートまたは明らかなエラーはありません。

解決方法

以下の点に注意してください。

- ファイルが他のアプライアンスによる分析用に送信されているために、すでにファイル分析サーバ、またはそのファイルを処理するアプライアンスのキャッシュに存在している可能性があります。
- [セキュリティ サービス（Security Services）] > [マルチウェア対策とレピュテーション（Anti-Malware and Reputation）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] ページで設定した最大ファイルサイズの制限を確認します。この制限は Advanced Malware Protection 機能に適用されます。

クラウド内のファイル分析の詳細が完全でない

問題

パブリック クラウド内の完全なファイル分析結果は、組織のその他の Secure Web Appliance からアップロードされたファイルでは取得できません。

解決方法

ファイルの分析結果データを共有するすべてのアプライアンスをグループ化してください。（パブリック クラウド ファイル分析サービスのみ）アプライアンス グループの設定 （41 ページ）を参照してください。この設定は、グループの各アプライアンスで実行する必要があります。

分析のために送信できるファイル タイプに関するアラート

問題

ファイル分析のために送信できるファイルタイプに関する重大度情報のアラートを受け取れます。

解決方法

このアラートは、サポート対象のファイル タイプが変更された場合や、アプライアンスがサポート対象のファイルタイプを確認した場合に送信されます。これは、以下の場合に発生する可能性があります。

- 自分または別の管理者が分析用に選択されているファイル タイプを変更した。
- サポート対象のファイル タイプがクラウド サービスでの可用性に基づいて一時的に変更された。この場合、アプライアンスで選択されたファイルタイプのサポートは可能な限り迅速に復旧されます。どちらのプロセスも動的であり、ユーザによる操作は必要ありません。
- アプライアンスが再起動した（たとえば、AsyncOS のアップグレードの一環として）。

Web アプリケーションへのアクセスの管理

この章で説明する内容は、次のとおりです。

Web アプリケーションへのアクセスの管理：概要

Application Visibility and Control（AVC）または、Application Discovery and Control（ADC）エンジンを使用すると、各アプリケーションの基盤技術を完全に理解していなくても、ネットワーク上のアプリケーション アクティビティを制御するポリシーを作成できます。アクセス ポリシー グループのアプリケーション制御を設定できます。個々に、またはアプリケーションのタイプに応じて、アプリケーションをブロックまたは許可することができます。また、特定のアプリケーション タイプに制御を適用することも可能です。

アクセス ポリシーを使用して、以下の操作を実行できます。

- アプリケーションの動作やアクティビティ、またはきめ細かいゲインコントロールを制御します。

ADC には、きめ細かいゲインコントロール（FGC）または動作構成があります。複数のアプリケーションに対して FGC を設定できます。

- 特定のアプリケーション タイプで使用される帯域幅の量を制御する

（注） これは、AVC にのみ適用されます。

- アプリケーションがブロックされたときにエンドユーザーに通知する
- インスタント メッセージ、ブログ、ソーシャル メディアのアプリケーションに制御を割り当てる
- 範囲要求の設定を指定する

（注） これは、AVC にのみ適用されます。

AVC または ADC エンジンを使用してアプリケーションを制御するには、以下のタスクを実行します。

タスク	タスクへのリンク
AVC または ADC エンジンを有効にする	AVC または ADC エンジンを有効にする （53 ページ）
アクセス ポリシー グループに制御を設定する	アクセス ポリシー グループのアプリケーション管理設定 （58 ページ）
アプリケーション タイプが消費する帯域幅を制限して輻輳を制御する （注） これは、AVC にのみ適用されます。	帯域幅の制御 （59 ページ）
インスタント メッセージ トラフィックを許可し、インスタント メッセンジャによるファイル共有を禁止する	インスタント メッセージ トラフィックの制御 （62 ページ）

AVC または ADC エンジンを有効にする

[使用許可コントロール（Acceptable Use Controls）] を有効にする場合は、AVC または ADC エンジンを有効にします。

（注） [レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページの [アプリケーションの表示（Application Visibility）] レポートで、AVC または ADC エンジンのスキャンアクティビティを確認できます。

次のタスク

関連項目

- アプリケーション エンジンとデフォルトのアクション （54 ページ）
- 要求が AVC または ADC エンジンによりブロックされた場合のユーザー体験 （54 ページ）

アプリケーション エンジンとデフォルトのアクション

AsyncOS は定期的にアップデート サーバーに問い合わせて、AVC エンジンを含めたすべてのセキュリティ サービス コンポーネントについて新しいアップデートの有無を確認します。AVC エンジンのアップデートには、新しいアプリケーション タイプやアプリケーションに対するサポートが含まれることがあります。また、アプリケーションの動作が変更された場合は、既存のアプリケーションに対するサポートも更新されます。AsyncOS バージョンの更新に合わせて AVC エンジンを更新することにより、サーバをアップグレードすることなく、 Secure Web Applianceの柔軟性が保たれます。

AsyncOS for Web は、グローバル アクセス ポリシーに以下のデフォルト アクションを割り当てます。

- 新しいアプリケーション タイプのデフォルト アクションは、[モニター（Monitor）] です。
- 特定アプリケーション内のブロック ファイル転送などの新しいアプリケーション動作のデフォルト設定は、[モニター（Monitor）] です。
- 既存のアプリケーション タイプの新しいアプリケーションのデフォルト アクションは、そのアプリケーション タイプのデフォルト アクションです。

（注） グローバルアクセスポリシーでは、各アプリケーションタイプのデフォルトアクションを設定できます。これによって、AVC または ADC エンジンのアップデートにより導入された新しいアプリケーションは、指定されたデフォルトアクションを自動的に継承します。アクセス ポリシー グループのアプリケーション管理設定 （58 ページ） を参照してください。

要求が AVC または ADC エンジンによりブロックされた場合のユーザー体験

AVC または ADC エンジンによってトランザクションがブロックされると、Web プロキシはエンドユーザーにブロックページを送信します。ただし、すべての Web サイトでブロック ページが表示されるわけではありません。多くの Web サイトでは、静的 Web ページの代わりに

JavaScript を使用して動的コンテンツが表示され、ブロック ページが表示されることはありません。そのような場合でも、ユーザーは適切にブロックされているので悪意のあるデータをダウンロードすることはありませんが、ブロックされていることが Web サイトから通知されない場合もあります。

（注） HTTPS プロキシが無効で、Webroot が次の場合：

- [有効（Enabled）]：AVC または ADC エンジンは起動する場合と起動しない場合があり、判定が返されます。トランザクションは、スキャナの判定に従って処理されます。
- [無効（Disabled）]：AVC または ADC エンジンが起動し、判定が返されます。トランザクションは、AVC または ADC の判定に従って処理されます。

アプリケーション制御のポリシー設定

アプリケーションを制御するには、以下の要素を設定する必要があります。

オプション	説明
アプリケーション タイプ（Application Types）	1 つまたは複数のアプリケーションを含むカテゴリです。
アプリケーション	あるアプリケーションタイプに属している特定のアプリケーション。
アプリケーション動作（Application behaviors）	管理者が制御できるアプリケーション内でユーザーが実行できる特定のアクションまたは動作。すべてのアプリケーションに設定可能な動作が含まれているわけではありません。

アクセス ポリシー グループのアプリケーション制御を設定できます。[Web セキュリティ マネージャ（Web Security Manager）] > [アクセス ポリシー（Access Policies）] ページで、設定するポリシー グループの [アプリケーション（Applications）] リンクをクリックします。アプリケーションの設定時には、以下のアクションを選択できます。

オプション	説明
ブロック（Block）	このアクションは、最終アクションです。ユーザーは Web ページを閲覧できなくなり、代わりにエンド ユーザー通知ページが表示されます。 （注） アプリケーションがADC/AVCでブロックされるように設定されている場合、アプリケーションのすべてのサブカテゴリもブロックされます。特定のサブカテゴリは詳細なゲイン制御機能を使用してブロックできますが、この機能は smugmug、Facebook、LinkedIn などの特定のアプリに限定されます。

オプション	説明
モニター（Monitor）	このアクションは、中間アクションです。Webプロキシは引き続きトランザクションを他の制御設定と比較して、適用する最終アクション決定します。
制限（Restrict）	このアクションは、アプリケーションの動作がブロックされることを示します。たとえば、特定のインスタントメッセージアプリケーションのファイル転送をブロックすると、そのアプリケーションのアクションは制限されます。
帯域幅制限（Bandwidth Limit）	Media や Facebook などの特定のアプリケーションに対して、Web トラフィックで使用可能な帯域幅を制限できます。アプリケーション自体やそのアプリケーション ユーザーの帯域幅を制限できます。

関連項目

- 範囲要求の設定（Range Request Settings） （56 ページ）
- アプリケーション制御の設定のためのルールとガイドライン （57 ページ）

範囲要求の設定（Range Request Settings）

HTTP の範囲要求がディセーブルのときに大きなファイルが複数のストリームでダウンロードされる場合、統合されたパッケージがスキャンされます。これにより、大きなオブジェクトのダウンロードで使用されるダウンロード管理ユーティリティやアプリケーションから、パフォーマンス上のメリットが得られなくなります。

代わりに、[範囲要求の転送（Range Request Forwarding）] をイネーブルにすると（Web プロキシの設定 を参照）、着信する範囲要求の処理方法をポリシーごとに制御できます。このプロセスは「バイト サービング」と呼ばれ、大きなファイルの要求時に帯域幅を最適化するための方法です。

ただし、範囲要求の転送のイネーブル化は、ポリシー ベースの Application Visibility and Control（AVC）の効率を妨げ、セキュリティを侵害する可能性があります。セキュリティ上の影響よりもメリットの方が重要な場合にのみ、十分に注意して HTTP の [範囲要求の転送（Range Request Forwarding）] をイネーブルにしてください。

（注） 範囲要求設定は、範囲要求転送が有効で、少なくとも 1 つのアプリケーションが [ブロック（Block）]、[制限（Restrict）]、または [スロットル（Throttle）] に設定されている場合に使用できます。

ポリシーの範囲要求の設定

範囲要求の設定（Range Request Settings）	• **範囲要求を転送しない**：クライアントは特定の範囲の要求を送信します。ただし、 Secure Web Applianceは、ターゲットサーバーに送信する前に要求から範囲ヘッダーを削除します。次に Secure Web Applianceは、ファイル全体をスキャンし、バイト範囲をクライアントに送信します。 （注） クライアントが初めて範囲要求を送信すると、 Secure Web Applianceはクライアントからの後続の範囲要求を想定して、ファイル全体を送信します。同じクライアントまたは別のクライアントからの後続の要求では、 Secure Web Applianceは部分的なコンテンツのみをクライアントに配信します。 • **範囲要求を転送する**：クライアントは特定の範囲の要求を送信します。 Secure Web Applianceは、同じ要求をターゲットサーバーに送信し、部分的なコンテンツを受信してクライアントに返します。Secure Web Applianceは、スキャン結果が正確でない可能性がある部分的なコンテンツのみをスキャンします。
例外リスト（Exception list）	現在の転送先の選択肢から除外する、トラフィックの宛先を指定できます。つまり、[範囲要求を転送しない（Do not forward range requests）] を選択した場合は、要求を転送する宛先を指定できます。同様に、[範囲要求を転送する（Forward range requests）] を選択した場合は、要求を転送しない宛先を指定できます。

アプリケーション制御の設定のためのルールとガイドライン

アプリケーション制御を設定する際は、以下のルールとガイドラインを考慮してください。

- サポートされるアプリケーションタイプ、アプリケーション、およびアプリケーション動作は、AsyncOS for Web のアップグレード間で、または AVC または ADC エンジンのアップデート後に変化する可能性があります。
- セーフ サーチまたはサイト コンテンツ レーティングを有効にすると、AVC エンジンが、安全なブラウジングのためのアプリケーションを特定する必要があります。条件の 1 つとして、AVC エンジンは応答本文をスキャンし、検索アプリケーションを検出します。その結果、アプライアンスは範囲ヘッダーを転送しません。
- [アプリケーションタイプ（Application Type）] リストでは、各アプリケーション タイプの要約にアプリケーションの最終アクションが一覧表示されますが、それらのアクションがグローバル ポリシーから継承されたものか、現在のアクセス ポリシーで設定されたものかについては示されません。特定のアプリケーションのアクションについて詳細を調べるには、そのアプリケーション タイプを展開します。
- グローバルアクセスポリシーでは、各アプリケーションタイプのデフォルトアクションを設定できます。これによって、AVC または ADC エンジンのアップデートにより導入された新しいアプリケーションは、デフォルトアクションを自動的に継承します。

- [参照（Browse）] ビューでアプリケーション タイプの [すべてを編集（edit all）] リンクをクリックすると、そのアプリケーションタイプに属するすべてのアプリケーションに同じアクションを簡単に設定できます。ただし、設定できるのは、アプリケーション動作のアクションではなく、アプリケーションのアクションだけです。アプリケーション動作を設定するには、アプリケーションを個別に編集する必要があります。
- [検索（Search）] ビューでは、テーブルをアクション列でソートすると、最終アクションに基づいてテーブルが並べ替えられます。たとえば、[グローバル（ブロック）を使用（Use Global (Block)）] は [ブロック（Block）] の後に配置されます。
- 署名用ルート証明書がクライアントにインストールされていない場合は、復号により、アプリケーションでエラーが発生することがあります。

関連項目

- アクセス ポリシー グループのアプリケーション管理設定 （58 ページ）
- 全体の帯域幅制限の設定 （60 ページ）
- AVC または ADC アクティビティの表示 （63 ページ）

アクセス ポリシー グループのアプリケーション管理設定

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3 グローバル アクセス ポリシーを設定する場合：

a) [アプリケーション タイプのデフォルト アクション（Default Actions for Application Types）] セクションで、各アプリケーション タイプのデフォルト アクションを定義します。

b) ページの [アプリケーション設定を編集（Edit Applications Settings）] セクションで、各アプリケーション タイプの各メンバーのデフォルト アクションを一括して、または個々に編集できます。個々のアプリケーションのデフォルト アクションを編集する手順は、以下のとおりです。

ステップ 4 ユーザー定義のアクセス ポリシーを設定する場合は、[アプリケーション設定を編集（Edit Applications Settings）] セクションで [アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] を選択します。

ステップ 5 [アプリケーションの設定（Application Settings）] 領域で、ドロップダウン メニューから [参照ビュー（Browse view）] または [検索ビュー（Search view）] を選択します。

- **[参照ビュー（Browse view）]。** アプリケーション タイプを参照できます。[参照ビュー（Browse view）] を使用すると、特定タイプのすべてのアプリケーションを同時に設定できます。[参照ビュー（Browse view）] でアプリケーション タイプが折りたたまれている場合は、アプリケーション タイプの要約に

アプリケーションの最終アクションが一覧表示されます。ただし、それらのアクションがグローバルポリシーから継承されたものか、現在のアクセス ポリシーで設定されたものかについては示されません。

- **[検索ビュー（Search view）]。**名前によってアプリケーションを検索できます。すべてのアプリケーションのリストが長く、特定のアプリケーションをすばやく見つけて設定する必要がある場合は、[検索ビュー（Search view）] を使用します。

ステップ 6 各アプリケーションとアプリケーション動作のアクションを設定します。

ステップ 7 該当する各アプリケーションの帯域幅制御を設定します。

ステップ 8 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

関連項目

- 帯域幅の制御 （59 ページ）

帯域幅の制御

全体的な制限とユーザーの制限の両方をトランザクションに適用した場合は、最も制限の厳しいオプションが適用されます。URL カテゴリの ID グループを定義し、帯域幅を制限するアクセス ポリシーでそのグループを使用することにより、特定の URL カテゴリに対して帯域幅制限を定義できます。

以下の帯域幅制限を定義できます。

帯域幅制限	説明	タスクへのリンク
全体	サポートされるアプリケーション タイプに対して、ネットワーク上の全ユーザー向けの全体的制限を定義します。全体的な帯域幅制限は、Cisco Secure Web Appliance と Web サーバー間のトラフィックに影響を与えます。Web キャッシュからのトラフィックは制限されません。	全体の帯域幅制限の設定 （60 ページ）
ユーザー	アプリケーション タイプごとに、ネットワーク上の特定ユーザーに対する制限を定義します。ユーザーの帯域幅制限は、Web サーバーからのトラフィックだけでなく、Web キャッシュからのトラフィックも制限します。	ユーザーの帯域幅制限の設定 （60 ページ）

（注） 帯域幅制限を定義しても、ユーザーへのデータ転送が遅くなるだけです。クォータに達したかどうかに基づいてデータがブロックされるわけではありません。Webプロキシによって各アプリケーションのトランザクションに遅延が生じ、サーバーへのリンクが減速したように見えます。

全体の帯域幅制限の設定

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [全体の帯域幅制限（Overall Bandwidth Limits）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [制限値（Limit to）] オプションを選択します。

ステップ 4 メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で、制限するトラフィック量を入力します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

ユーザーの帯域幅制限の設定

ユーザーの帯域幅制限を定義するには、アクセス ポリシーの Applications Visibility and Control ページで帯域幅制御を設定します。アクセスポリシーで、ユーザーに対して以下のタイプの帯域幅制御を定義できます。

オプション	説明	タスクへのリンク
アプリケーション タイプのデフォルトの帯域幅制限（Default bandwidth limit for an application type）	グローバルアクセスポリシーで、あるアプリケーション タイプに属するすべてのアプリケーションに対してデフォルトの帯域幅制限を定義できます。	アプリケーション タイプのデフォルトの帯域幅制限の設定 （61 ページ）
アプリケーション タイプの帯域幅制限（Bandwidth limit for an application type）	ユーザー定義のアクセス ポリシーで、グローバルアクセスポリシーで定義されたアプリケーション タイプのデフォルトの帯域幅制限を上書きすることができます。	アプリケーション タイプのデフォルトの帯域幅制限の無効化 （61 ページ）

オプション	説明	タスクへのリンク
アプリケーションの帯域幅制限（Bandwidth limit for an application）	ユーザー定義のアクセス ポリシーまたはグローバル アクセス ポリシーで、アプリケーション タイプの帯域幅制限を適用するか、制限しないか（アプリケーション タイプの制限を免除）を選択できます。	アプリケーションの帯域幅制御の設定 （62 ページ）

アプリケーション タイプのデフォルトの帯域幅制限の設定

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 ポリシー テーブルで、グローバル アクセス ポリシーの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3 [アプリケーションタイプのデフォルトアクション（Default Actions for Application Types）] セクションで、編集するアプリケーション タイプの [帯域幅制限（Bandwidth Limit）] の横にあるリンクをクリックします。

ステップ 4 [帯域幅制限を設定（Set Bandwidth Limit）] を選択し、制限するトラフィック量を、メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で入力します。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

アプリケーション タイプのデフォルトの帯域幅制限の無効化

ユーザー定義のアクセス ポリシーで、グローバル アクセス ポリシー グループで定義されたデフォルトの帯域幅制限を上書きすることができます。これは [参照ビュー（Browse view）] でのみ実行できます。

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 ポリシー テーブルで、編集するユーザー定義ポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3 [アプリケーション設定を編集（Edit Applications Settings）] セクションで [アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] を選択します。

ステップ 4 編集するアプリケーション タイプの [帯域幅制限（Bandwidth Limit）] の横にあるリンクをクリックします。

ステップ 5 別の帯域幅制限値を選択するには、[帯域幅制限を設定（Set Bandwidth Limit）] を選択し、制限するトラフィック量を、メガビット/秒（Mbps）またはキロビット/秒（kbps）単位で入力します。帯域幅を制限しないことを指定するには、[アプリケーションタイプに対する帯域幅制限なし（No Bandwidth Limit for Application Type）] を選択します。

ステップ 6 [適用（Apply）] をクリックします。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

アプリケーションの帯域幅制御の設定

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3 定義するアプリケーションが含まれているアプリケーション タイプを展開します。

ステップ 4 設定するアプリケーションのリンクをクリックします。

ステップ 5 [モニター（Monitor）]を選択し、次に、アプリケーションタイプに対して定義されている帯域幅制限を使用するか、制限しないかを選択します。

（注）
帯域幅制限の設定は、アプリケーションがブロックされている場合や、アプリケーション タイプに対して帯域幅制限が定義されていない場合は適用できません。

ステップ 6 [完了（Done）] をクリックします。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

インスタント メッセージ トラフィックの制御

IM トラフィックをブロックまたはモニターすることができます。また、IM サービスによっては、IM セッションの特定のアクティビティ（アプリケーション動作）をブロックすることもできます。

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [アクセスポリシー（Access Policies）] を選択します。

ステップ 2 ポリシー テーブルで、編集するポリシー グループの [アプリケーション（Applications）] 列にあるリンクをクリックします。

ステップ 3 [アプリケーションのカスタム設定を定義（Define Applications Custom Settings）] をクリックします。

ステップ 4 [インスタントメッセージ（Instant Messaging）] アプリケーション タイプを展開します。

ステップ 5 設定する IM アプリケーションの横にあるリンクをクリックします。

ステップ 6 この IM アプリケーションのすべてのトラフィックをブロックするには、[ブロック（Block）] を選択します。

ステップ 7 IM アプリケーションをモニターしながら、アプリケーション内の特定のアクティビティをブロックするには、[モニター（Monitor）] を選択してから、アプリケーション動作として [ブロック（Block）] を選択します。

ステップ 8 [完了（Done）] をクリックします。

ステップ 9 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

AVC または ADC アクティビティの表示

[レポート（Reporting）] > [アプリケーションの表示（Application Visibility）] ページには、使用されている上位のアプリケーションとアプリケーション タイプに関する情報が表示されます。また、ブロックされている上位のアプリケーションとアプリケーションタイプも表示されます。

アクセスログファイルの AVC または ADC 情報

アクセスログファイルには、トランザクションごとに AVC または ADC エンジンから返された情報が記録されます。アクセスログのスキャン判定情報セクションには、以下のようなフィールドがあります。

説明	アクセス ログのカスタム フィールド	W3C ログのカスタム フィールド
アプリケーション名（Application name）	%XO	xAPP
アプリケーションタイプ	%Xu	x-type
アプリケーション動作（Application behavior）	%Xb	x-behavior

（注） 特定のアプリケーションに対してADCアプリケーションの動作を設定すると、そのアプリケーションのみを検索できます。それ以外の場合、カスタム動作は [不明（Unknown）] になります。

機密データの漏洩防止

この章で説明する内容は、次のとおりです。

機密データの漏洩防止の概要

Secure Web Applianceは以下の機能によってデータの安全を確保します。

オプション	説明
Cisco データ セキュリティ フィルタ	Secure Web Applianceの Cisco データ セキュリティ フィルタは、HTTP、HTTPS、FTP を介してネットワークから発信されるデータを評価します。
サードパーティ製データ漏洩防止（DLP）の統合	Secure Web Applianceは、機密データを識別して保護する代表的なサードパーティ製コンテンツ対応 DLP システムを統合します。Web プロキシは Internet Content Adaptation Protocol（ICAP）を使用して、プロキシ サーバーが外部システムにコンテンツ スキャンをオフロードできるようにします。

アップロード要求を受信すると、Web プロキシは要求をデータ セキュリティ ポリシー グループや外部 DLP ポリシー グループと比較して、適用するポリシー グループを決定します。両方のタイプのポリシーが設定されている場合は、外部 DLP ポリシーと比較する前に、Cisco デー

タ セキュリティ ポリシーと要求を比較します。ポリシー グループに要求を割り当てた後、その要求をポリシー グループの設定済み制御設定と比較し、要求に対して実行するアクションを決定します。アップロード要求を処理するためのアプライアンスの設定方法は、ポリシー グループのタイプによって異なります。

（注） サイズがゼロ（0）バイトのファイルのアップロードを試みているアップロード要求は、Cisco データ セキュリティ ポリシーまたは外部 DLP ポリシーに対して評価されません。

ネットワークから発信されるデータを制限したり制御するには、以下のタスクを実行します。

タスク	タスクへのリンク
Cisco データ セキュリティ ポリシーを作成する	アップロード要求の管理 （66 ページ）
外部 DLP ポリシーを作成する	外部 DLP システムにおけるアップロード要求の管理 （67 ページ）
データ セキュリティ ポリシーおよび外部 DLP ポリシーを作成する	データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成 （68 ページ）
Cisco データ セキュリティ ポリシーを使用してアップロード要求を制御する	アップロード要求の設定の管理 （72 ページ）
外部 DLP ポリシーを使用してアップロード要求を制御する	外部 DLP ポリシーによるアップロード要求の制御 （77 ページ）

最小サイズ以下のアップロード要求のバイパス

ログ ファイルに記録されるアップロード要求の数を減らすために、最小要求サイズを定義できます。このサイズを下回る場合、アップロード要求は Cisco データセキュリティ フィルタや外部 DLP サーバーによってスキャンされません。

これを実行するには、以下の CLI コマンドを使用します。

- **datasecurityconfig**。Cisco データ セキュリティ フィルタに適用します。
- **externaldlpconfig**。設定されている外部 DLP サーバーに適用します。

デフォルトでは、どちらの CLI コマンドでも要求本文の最小サイズは 4 KB（4096 バイト）です。有効な値は 1 ～ 64 KB です。指定したサイズは、アップロード要求の本文全体のサイズに適用されます。

（注） すべてのチャンク エンコードされたアップロードとすべてのネイティブ FTP トランザクションは、Cisco データ セキュリティ フィルタまたは外部 DLP サーバーによってスキャンされます（有効な場合）。ただし、カスタム URL カテゴリに基づいてこれらをバイパスできます。

要求が機密データとしてブロックされた場合のユーザー エクスペリエンス

Ciscoデータセキュリティ フィルタや外部DLPサーバーは、アップロード要求をブロックするときに、Web プロキシがエンド ユーザーに送信するブロック ページを提供します。すべてのWebサイトでエンドユーザーにブロック ページが表示されるわけではありません。たとえば、一部の Web 2.0 Web サイトは静的な Web ページの代わりに JavaScript を使用して動的なコンテンツを表示し、ブロック ページを表示しない場合が多くあります。そのような場合でも、データ セキュリティ違反が発生しないようにユーザーは適切にブロックされていますが、そのことが Web サイトから通知されない場合もあります。

アップロード要求の管理

始める前に

[セキュリティ サービス（Security Services）] > [データ セキュリティ フィルタ（Data Security Filters）] に移動し、Cisco データ セキュリティ フィルタを有効にします。

手順

データ セキュリティ ポリシー グループを作成して設定します。

Cisco データ セキュリティ ポリシーは、アップロード要求を評価する際に、URL フィルタリング、Web レピュテーション、およびアップロードコンテンツ情報を使用します。これらのセキュリティ コンポーネントを個々に設定し、アップロード要求をブロックするかどうかを決定します。

Web プロキシはアップロード要求を制御設定と比較する際に、順番に設定を評価します。各制御設定は、Cisco データ セキュリティ ポリシーの次のアクションのいずれかを実行するように設定できます。

アクション	説明
ブロック（Block）	Web プロキシは、接続を許可せず、ブロックの理由を説明するエンド ユーザー通知ページを表示します。
許可（Allow）	Web プロキシは、データ セキュリティ ポリシーの残りのセキュリティ サービス スキャンをバイパスし、最終アクションを実行する前にアクセス ポリシーに対して要求を評価します。 Cisco データ セキュリティ ポリシーでは、残りのデータ セキュリティ スキャンをバイパスできますが、外部 DLP やアクセス ポリシーのスキャンはバイパスしません。Web プロキシが要求に対して実行する最終アクションは、該当するアクセス ポリシー（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）によって決まります。
モニター（Monitor）	Web プロキシは、引き続き、トランザクションと他のデータ セキュリティ ポリシー グループの制御設定を比較し、トランザクションをブロックするか、またはアクセス ポリシーに対して評価するかを決定します。

Cisco データ セキュリティ ポリシーの場合、Web プロキシがクライアント要求に対して実行する最終アクションは「ブロック」アクションだけです。「モニター」および「許可」アクションは中間アクションです。いずれの場合も、Web プロキシは、トランザクションを外部 DLP ポリシー（設定されている場合）およびアクセス ポリシーに対して評価します。Web プロキシは、アクセス ポリシー グループの制御設定（または、要求をブロックする可能性がある適切な外部 DLP ポリシー）に基づいて適用する最終アクションを決定します。

次のタスク

関連項目

- 外部 DLP システムにおけるアップロード要求の管理 （67 ページ）
- アップロード要求の設定の管理 （72 ページ）

外部 DLP システムにおけるアップロード要求の管理

外部 DLP システムでアップロード要求を処理するように Secure Web Applianceを設定するには、以下のタスクを実行します。

手順

ステップ 1 [ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] を選択します。外部 DLP システムを定義します。スキャンのためにアップロード要求を外部 DLP システムに渡すには、少なくとも 1 つの ICAP 準拠 DLP システムを Secure Web Applianceで定義する必要があります。

ステップ 2 **外部 DLP ポリシー グループを作成して設定します。**外部 DLP システムを定義したら、外部 DLP ポリシー グループを作成して設定し、スキャンのために DLP システムに送信するアップロード要求を決定します。

ステップ 3 アップロード要求が外部 DLP ポリシーに一致した場合、Web プロキシは、Internet Content Adaptation Protocol（ICAP）を使用して、スキャンのためにアップロード要求を DLP システムに送信します。DLP システムは、要求本文のコンテンツをスキャンし、Web プロキシにブロックまたは許可の判定を返します。許可の判定は、アップロード要求がアクセス ポリシーと比較される Cisco データ セキュリティ ポリシーの許可アクションに似ています。Web プロキシが要求に対して実行する最終アクションは、適用されるアクセス ポリシーによって決まります。

次のタスク

関連項目

- 外部 DLP ポリシーによるアップロード要求の制御 （77 ページ）
- 外部 DLP システムの定義 （73 ページ）

データ セキュリティおよび外部DLPポリシーグループのメンバーシップの評価

各クライアント要求に ID が割り当てられ、次に、それらの要求が他のポリシー タイプと照合して評価され、タイプごとに要求が属するポリシー グループが判定されます。Web プロキシは、データ セキュリティおよび外部 DLP ポリシーに対してアップロード要求を評価します。Web プロキシは、クライアント要求のポリシー グループ メンバーシップに基づいて、設定されているポリシー制御設定をクライアント要求に適用します。

クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合

クライアント要求と一致するポリシー グループを判定するために、Web プロキシは、特定のプロセスを実行してグループ メンバーシップの基準と照合します。グループ メンバーシップの以下の要素が考慮されます。

- **ID。**各クライアント要求は、識別プロファイルに一致するか、認証に失敗するか、ゲスト アクセスが許可されるか、または認証に失敗して終了します。
- **権限を持つユーザー。**割り当てられた識別プロファイルが認証を必要とする場合は、そのユーザーがデータ セキュリティまたは外部 DLP ポリシー グループの承認済みユーザーのリストに含まれており、ポリシー グループに一致している必要があります。承認済みユーザーのリストには、任意のグループまたはユーザーを指定でき、識別プロファイルがゲスト アクセスを許可している場合はゲスト ユーザーを指定できます。
- **高度なオプション。**データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップに対して複数の詳細オプションを設定できます。一部のオプション（プロキシ ポート、URL カテゴリなど）は、ID 内に定義することもできます。ID 内に詳細オプションを設定する場合、データ セキュリティまたは外部 DLP ポリシー グループ レベルでは設定できません。

この項では、Web プロキシがアップロード要求をデータ セキュリティおよび外部 DLP の両方のポリシー グループと照合する方法について概要を説明します。

Webプロキシは、ポリシーテーブルの各ポリシー グループを順番に読み取ります。次に、アップロード要求のステータスを最初のポリシー グループのメンバーシップ基準と比較します。一致した場合、Web プロキシは、そのポリシー グループのポリシー設定を適用します。

一致しない場合は、その以下のポリシー グループとアップロード要求を比較します。アップロード要求をユーザー定義のポリシー グループと照合するまで、Web プロキシはこのプロセスを続行します。ユーザー定義のポリシー グループに一致しない場合は、グローバル ポリシー グループと照合します。Webプロキシは、アップロード要求をポリシー グループまたはグローバル ポリシー グループと照合するときに、そのポリシー グループのポリシー設定を適用します。

データ セキュリティ ポリシーおよび外部 DLP ポリシーの作成

宛先サイトの URL カテゴリや 1 つ以上の識別プロファイルなど、複数の条件の組み合わせに基づいてデータ セキュリティおよび外部 DLP ポリシー グループを作成できます。ポリシー グ

ループのメンバーシップには、少なくとも1つの条件を定義する必要があります。複数の条件が定義されている場合、アップロード要求がポリシー グループと一致するには、すべての条件を満たしていなければなりません。ただし、アップロード要求は設定された識別プロファイルの 1 つとのみ一致する必要があります。

手順

ステップ 1 [Web セキュリティ マネージャ（Web Security Manager）] > [Cisco データ セキュリティ（Cisco Data Security）]（データ セキュリティ ポリシー グループ メンバーシップを定義する場合）、または [Web セキュリティ マネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）]（外部 DLP ポリシー グループ メンバーシップを定義する場合）を選択します。

ステップ 2 [ポリシーを追加（Add Policy）] をクリックします。

ステップ 3 [ポリシー名（Policy Name）] フィールドにポリシー グループの名前を入力し、[説明（Description）] フィールドに説明を追加します。

（注）
各ポリシー グループ名は、英数字またはスペース文字のみを含む、一意の名前とする必要があります。

ステップ 4 [上記ポリシーを挿入（Insert Above Policy）] フィールドで、ポリシー テーブル内でポリシー グループを配置する場所を選択します。

複数のポリシー グループを設定する場合は、各グループに論理的な順序を指定します。正しく照合されるようにポリシー グループの順序を指定してください。

ステップ 5 [アイデンティティとユーザー（Identities and Users）] セクションで、このポリシー グループに適用する 1 つ以上の識別プロファイル グループを選択します。

ステップ 6 （任意）[詳細設定（Advanced）] セクションを展開して、追加のメンバーシップ要件を定義します。

ステップ 7 いずれかの拡張オプションを使用してポリシー グループのメンバーシップを定義するには、拡張オプションのリンクをクリックし、表示されるページでオプションを設定します。

高度なオプション	説明
プロトコル	クライアント要求で使用されるプロトコルによってポリシー グループのメンバーシップを定義するかどうかを選択します。含めるプロトコルを選択します。 [その他のすべて（All others）] は、このオプションの上に一覧表示されていないプロトコルを意味します。 （注） HTTPS プロキシをイネーブルにすると、復号ポリシーのみが HTTPS トランザクションに適用されます。アクセス、ルーティング、アウトバウンドマルウェア スキャン、データ セキュリティ、外部 DLP のポリシーの場合は、HTTPS プロトコルによってポリシー メンバーシップを定義できません。

高度なオプション	説明
プロキシ ポート（Proxy Ports）	Webプロキシへのアクセスに使用するプロキシ ポートで、ポリシー グループ メンバーシップを定義するかどうかを選択します。[プロキシ ポート（Proxy Ports）] フィールドに、1つ以上のポート番号を入力します。複数のポートを指定する場合は、カンマで区切ります。 明示的な転送接続のために、ブラウザに設定されたポートです。透過接続の場合は、宛先ポートと同じです。あるポート上に要求を明示的に転送するように設定されたクライアントのセットがあり、別のポート上に要求を明示的に転送するように設定された別のクライアントのセットがある場合、プロキシ ポート上でポリシー グループのメンバーシップを定義することがあります。 シスコでは、アプライアンスが明示的な転送モードで配置されている場合、またはクライアントがアプライアンスに要求を明示的に転送する場合にだけ、プロキシ ポートでポリシー グループのメンバーシップを定義することを推奨します。クライアント要求がアプライアンスに透過的にリダイレクトされるときにプロキシ ポートでポリシー グループのメンバーシップを定義すると、一部の要求が拒否される場合があります。 （注） このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。
サブネット（Subnets）	サブネットまたは他のアドレスでポリシー グループのメンバーシップを定義するかどうかを選択します。 関連付けられた識別プロファイルで定義できるアドレスを使用するか、または特定のアドレスをここに入力できます。 （注） ポリシー グループに関連付けられている識別プロファイルがアドレスによってグループのメンバーシップを定義している場合は、識別プロファイルで定義されているアドレスのサブセットであるアドレスを、このポリシー グループに入力する必要があります。ポリシー グループにアドレスを追加することにより、このグループ ポリシーに一致するトランザクションのリストを絞り込めます。
URL カテゴリ（URL Categories）	URL カテゴリでポリシー グループのメンバーシップを定義するかどうかを選択します。ユーザー定義または定義済みの URL カテゴリを選択します。 （注） このポリシー グループに関連付けられている ID がこの詳細設定によって ID メンバーシップを定義している場合、非 ID ポリシー グループ レベルではこの設定項目を設定できません。

高度なオプション	説明
ユーザー エージェント（User Agents）	クライアント要求で使用されるユーザー エージェント（アップデータや Web ブラウザなどのクライアント アプリケーション）ごとにポリシー グループ メンバーシップを定義するかどうかを選択します。一般的に定義されているユーザー エージェントを選択するか、正規表現を使用して独自に定義できます。メンバーシップの定義に選択したユーザー エージェントのみを含めるか、選択したユーザー エージェントを明確に除外するかどうかを指定します。 （注） このポリシー グループに関連付けられている識別プロファイルが、この詳細設定によって識別プロファイル メンバーシップを定義している場合、非識別プロファイル ポリシー グループ レベルではこの設定項目を設定できません。
ユーザーの場所（User Location）	ユーザーのリモートまたはローカルの場所でポリシー グループのメンバーシップを定義するかどうかを選択します。 このオプションは、セキュアモビリティがイネーブルの場合にのみ表示されます。

ステップ 8 変更を送信します。

ステップ 9 データ セキュリティ ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しいデータ セキュリティ ポリシー グループは、各制御設定のオプションが設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

外部 DLP ポリシー グループを作成する場合は、その制御設定を設定して、Web プロキシがアップロード要求を処理する方法を定義します。

新しい外部 DLP ポリシー グループは、カスタム設定が設定されるまで、グローバル ポリシー グループの設定を自動的に継承します。

ステップ 10 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

関連項目

- データ セキュリティおよび外部 DLP ポリシー グループのメンバーシップの評価 （68 ページ）
- クライアント要求とデータ セキュリティおよび外部 DLP ポリシー グループとの照合 （68 ページ）
- アップロード要求の設定の管理 （72 ページ）
- 外部 DLP ポリシーによるアップロード要求の制御 （77 ページ）

アップロード要求の設定の管理

各アップロード要求は、データ セキュリティ ポリシー グループに割り当てられ、そのポリシー グループの制御設定を継承します。データ セキュリティ ポリシー グループの制御設定によって、アプライアンスが接続をブロックするか、またはアクセス ポリシーに対して接続を評価するかが決まります。

[Web セキュリティ マネージャ（Web Security Manager）] > [Cisco データ セキュリティ（Cisco Data Security）] ページで、データ セキュリティ ポリシー グループの制御設定を設定します。

以下の設定項目を設定して、アップロード要求で実行するアクションを決定できます。

オプション	リンク
URL カテゴリ（URL Categories）	URL カテゴリ （72 ページ）
Web レピュテーション	Web レピュテーション （72 ページ）
目次	コンテンツのブロック （72 ページ）

データ セキュリティ ポリシー グループがアップロード要求に割り当てられた後、ポリシー グループの制御設定が評価され、要求をブロックするかアクセス ポリシーに対して評価するかが決定されます。

URL カテゴリ

AsyncOS for Web では、アプライアンスが特定の要求の URL カテゴリに基づいてトランザクションを処理する方法を設定できます。定義済みのカテゴリ リストを使用して、カテゴリ別にコンテンツをモニターするかブロックするかを選択できます。カスタム URL カテゴリを作成し、カスタム カテゴリの Web サイトに対してトラフィックを許可、モニター、またはブロックするかを選択することもできます。

Web レピュテーション

Web レピュテーションの設定はグローバル設定を継承します。特定のポリシー グループ用に Web レピュテーション フィルタリングをカスタマイズするには、[Webレピュテーション設定（Web Reputation Settings）] プルダウン メニューを使用して Web レピュテーション スコアのしきい値をカスタマイズします。

Cisco データ セキュリティ ポリシーの Web レピュテーションのしきい値には、負またはゼロの値のみ設定できます。定義では、すべての正のスコアがモニターされます。

コンテンツのブロック

[Cisco データ セキュリティ（Cisco Data Security）] > [コンテンツ（Content）] ページの設定項目を使用し、Webプロキシが次のファイル特性に基づいてデータのアップロードをブロックするように設定できます。

- **[ファイルサイズ（File size）]。**許容される最大アップロード サイズを指定できます。指定した最大値以上のサイズのアップロードはすべてブロックされます。HTTP/HTTPSおよびネイティブ FTP 要求に対して異なる最大ファイル サイズを指定できます。

  アップロード要求サイズが最大アップロード サイズと最大スキャン サイズ（[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドで設定）のどちらよりも大きい場合、アップロード要求はブロックされますが、ファイル名とコンテンツ タイプはデータ セキュリティ ログに記録されません。アクセス ログのエントリは変更されません。

- **[ファイル タイプ（File type）]。**定義済みのファイル タイプまたは入力したカスタム MIME タイプをブロックできます。定義済みファイル タイプをブロックする場合は、そのタイプのすべてのファイルまたは指定したサイズよりも大きいファイルをブロックできます。ファイル タイプをサイズによってブロックする場合は、最大ファイル サイズとして、[セキュリティ サービス（Security Services）] > [マルウェア対策（Anti-Malware）] ページの [DVS エンジン オブジェクト スキャンの制限（DVS Engine Object Scanning Limits）] フィールドの値と同じ値を指定できます。デフォルトでは、この値は 32 MB です。

  Cisco データ セキュリティ フィルタは、ファイル タイプによってブロックする場合にアーカイブ ファイルのコンテンツを検査しません。アーカイブ ファイルは、ファイル タイプまたはファイル名によってブロックできます。コンテンツによってブロックすることはできません。

（注） 一部の MIME タイプのグループでは、1 つのタイプをブロックすると、グループ内のすべての MIME タイプがブロックされます。たとえば、application/x-java-applet をブロックすると、application/java や application/javascript など、すべての MIME タイプがブロックされます。

- **[ファイル名（File name）]。**指定した名前のファイルをブロックできます。ブロックするファイル名を指定する場合は、リテラル文字列または正規表現をテキストとして使用できます。

（注） 8 ビット ASCII 文字のファイル名のみを入力してください。Web プロキシは、8 ビット ASCII 文字のファイル名のみを照合します。

外部 DLP システムの定義

Secure Web Applianceでは、アプライアンスに複数の DLP サーバを定義することにより、同じベンダーの複数の外部 DLP サーバを統合できます。Web プロキシが DLP システムに接続する際に使用するロード バランシング技術を定義できます。これは、複数の DLP システムを定義

する場合に役立ちます。外部 DLP サーバーとのセキュアな通信に使用されるプロトコルの指定については、SSL の設定を参照してください。

（注） 外部 DLP サーバーが Web プロキシによって変更されたコンテンツを送信しないことを確認します。AsyncOS for Web は、アップロード要求をブロックまたは許可する機能のみをサポートしています。外部 DLP サーバーによって変更されたコンテンツのアップロードはサポートしません。

外部 DLP サーバーの設定

手順

ステップ 1 [ネットワーク（Network）] > [外部 DLP サーバー（External DLP Servers）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

設定	説明
外部 DLP サーバーのプロトコル（Protocol for External DLP Servers）	以下のいずれかを選択します。 • [ICAP]：DLPクライアント/サーバーの ICAP 通信は暗号化されません。 • [セキュアICAP（Secure ICAP）]：DLP クライアント/サーバー の ICAP 通信は暗号化トンネルを介して行われます。追加の関連オプションが表示されます。

設定	説明
外部 DLP サーバー（External DLP Servers）	以下の情報を入力して、ICAP 準拠 DLP システムにアクセスします。 • [サーバー アドレス（Server address）] と [ポート（Port）] : DLP システムにアクセスするホスト名/IP アドレスと TCP ポート。 • [再接続の試行（Reconnection attempts）] : 失敗するまでに Web プロキシが DLP システムへの接続を試行する回数。 • [サービスURL（Service URL）] : 特定の DLP サーバーに固有の ICAP クエリー URL。Web プロキシは、ここに入力された情報を外部 DLP サーバーに送信する ICAP 要求に含めます。URL は、ICAP プロトコル（icap://）から始める必要があります。 • [証明書（Certificate）]（任意） : 各外部 DLP サーバー接続を保護するために提供する証明書は、認証局（CA）の署名付き証明書でも自己署名証明書でもかまいません。指定されたサーバーから証明書を取得し、アプライアンスにアップロードします。 • 証明書ファイルを参照して選択し、[ファイルのアップロード（Upload File）] をクリックします。 （注） この単一ファイルには、暗号化されていない形式でクライアント証明書と秘密キーを含める必要があります。 • [セキュアICAPを使用するすべてのDLPサーバーにこの証明書を使用する（Use this certificate for all DLP servers using Secure ICAP）] : ここで定義するすべての外部 DLP サーバーに同じ証明書を使用する場合は、このチェックボックスをオンにします。サーバーごとに異なる証明書を入力するには、このオプションをオフのままにします。 • [テスト開始（Start Test）] : このチェックボックスをオンにすると、 Secure Web Appliance と定義済み外部 DLP サーバ間の接続をテストできます。

設定	説明
ロード バランシング	複数の DLP サーバーを定義する場合は、Web プロキシがさまざまな DLP サーバーにアップロード要求を分散する際に使用するロードバランシング技術を選択します。以下のロード バランシング技術を選択できます。 • **[なし（フェールオーバー）（None(failover）]**。Web プロキシは、1 つの DLP サーバーにアップロード要求を送信します。一覧表示されている順序で DLP サーバーへの接続を試みます。ある DLP サーバーに到達できない場合、Web プロキシはリストの以下のサーバーへの接続を試みます。 • **[最少接続（Fewest connections）]**。Web プロキシは、各 DLP サーバーが扱っているアクティブな要求の数を追跡し、その時点で接続数が最も少ない DLP サーバーにアップロード要求を送信します。 • **[ハッシュベース（Hash based）]**。Web プロキシは、ハッシュ関数を使用して、DLP サーバーに要求を分散します。ハッシュ関数はプロキシ ID と URL を入力として使用し、同じ URL の要求が常に同じ DLP サーバーに送信されるようにします。 • **[ラウンド ロビン（Round robin）]**。Web プロキシは、リストされた順序ですべての DLP サーバー間にアップロード要求を均等に分散します。
サービス要求タイムアウト（Service Request Timeout）	Web プロキシが DLP サーバーからの応答を待機する時間を入力します。この時間が経過すると、ICAP 要求は失敗し、[失敗のハンドリング（Failure Handling）] の設定に応じて、アップロード要求はブロックまたは許可されます。 デフォルトは 60 秒です。
最大同時接続数（Maximum Simultaneous Connections）	Secure Web Applianceから設定されている各外部 DLP サーバへの同時 ICAP 要求接続の最大数を指定します。このページの [失敗のハンドリング（Failure Handling）] 設定は、この制限を超えるすべての要求に適用されます。 デフォルトは 25 です。
失敗のハンドリング（Failure Handling）	DLP サーバーがタイムリーに応答できなかった場合に、アップロード要求をブロックするか許可するか（評価のためにアクセス ポリシーに渡される）を選択します。 デフォルトは、許可（[すべてのデータ転送をスキャンなしで許可する（Permit all data transfers to proceed without scanning）]）です。
信頼できるルート証明書（Trusted Root Certificate）	外部 DLP サーバーによって提供された証明書に対して、信頼できるルート証明書を参照して選択し、[ファイルのアップロード（Upload File）] をクリックします。詳細については、証明書の管理（Certificate Management）を参照してください。
無効な証明書オプション（Invalid Certificate Options）	さまざまな無効な証明書の処理方法（[ドロップ（Drop）] または [モニター（Monitor）]）を指定します。

設定	説明
サーバー証明書（Server Certificates）	このセクションには、アプライアンスで現在使用可能なすべての DLP サーバー証明書が表示されます。

ステップ 3 （任意）[行を追加（Add Row）] をクリックし、表示される新しいフィールドに DLP サーバー情報を入力することによって、別の DLP サーバーを追加できます。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

外部 DLP ポリシーによるアップロード要求の制御

Webプロキシは、アップロード要求ヘッダーを受信することにより、スキャン用に要求を外部 DLP システムに送信する必要があるかどうかを判定するための必要情報を得ます。DLP システムは要求をスキャンし、Webプロキシに判定（ブロックまたはモニター）を返します（要求はアクセス ポリシーに対して評価されます）。

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [外部データ漏洩防止（External Data Loss Prevention）] を選択します。

ステップ 2 [接続先（Destinations）] 列で、設定するポリシー グループのリンクをクリックします。

ステップ 3 [接続先設定の編集（Edit Destination Settings section）] セクションで、[接続先スキャンのカスタム設定の定義（Define Destinations Scanning Custom Settings）] を選択します。

ステップ 4 [スキャンする接続先（Destination to Scan）] セクションで、以下のオプションのいずれかを選択します。

- **[どのアップロードもスキャンしない（Do not scan any uploads）]。**アップロード要求は、スキャンのために設定済みDLPシステムに送信されません。すべてのアップロード要求がアクセス ポリシーに対して評価されます。
- **[すべてのアップロードをスキャンする（Scan all uploads）]** すべてのアップロード要求が、スキャンのために設定済みDLPシステムに送信されます。アップロード要求は、DLPシステムのスキャン判定に応じて、ブロックされるか、アクセス ポリシーに対して評価されます。
- **[指定したカスタムおよび外部 URL カテゴリ以外へのアップロードをスキャン（Scan uploads except to specified custom and external URL categories）]。**特定のカスタム URL カテゴリに該当するアップロードの要求が、DLP スキャン ポリシーから除外されます。[カスタムカテゴリリストを編集（Edit custom categories list）] をクリックして、スキャンする URL カテゴリを選択します。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

データ損失防止スキャンのロギング

アクセス ログは、アップロード要求が Cisco データ セキュリティ フィルタまたは外部 DLP サーバーのいずれかによってスキャン済みかどうかを示します。アクセス ログ エントリには、Cisco データ セキュリティ ポリシーのスキャン判定用のフィールド、および外部 DLP スキャン判定に基づく別のフィールドが含まれています。

アクセス ログに加えて、 Secure Web Applianceには、Cisco データ セキュリティ ポリシーや外部 DLP ポリシーをトラブルシューティングするための次のようなログ ファイルが用意されています。

- **データ セキュリティ ログ。**Cisco データ セキュリティ フィルタで評価されたアップロード要求のクライアント履歴を記録します。
- **データ セキュリティ モジュール ログ。**Cisco データ セキュリティ フィルタに関するメッセージを記録します。
- **デフォルト プロキシ ログ。**Web プロキシに関連するエラーの記録に加えて、デフォルト プロキシ ログには外部 DLP サーバーへの接続に関連するメッセージが含まれています。これにより、外部 DLP サーバーとの接続や統合に関する問題をトラブルシューティングできます。

以下のテキストは、データ セキュリティ ログのエントリのサンプルを示しています。

```
Mon Mar 30 03:02:13 2009 Info: 303 10.1.1.1 - -
<<bar,text/plain,5120><foo,text/plain,5120>>
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting ns server.com
nc
```

フィールド値	説明
`Mon Mar 30 03:02:13 2009 Info:`	タイムスタンプおよびトレース レベル
`303`	トランザクション ID
`10.1.1.1`	ソース IP アドレス
`-`	ユーザー名（User name）
`-`	承認されたグループ名。

フィールド値	説明
<<bar,text/plain,5120><foo,text/plain,5120>>	一度にアップロードされる各ファイルのファイル名、ファイル タイプ、ファイル サイズ （注） このフィールドには、設定されている最小の要求本文サイズ（デフォルトは 4096 バイト）よりも小さいテキスト/プレーン ファイルは含まれません。
BLOCK_WEBCAT_IDS-allowall-DefaultGroup-DefaultGroup-NONE-DefaultRouting	Cisco データ セキュリティ ポリシーおよびアクション
ns	Web レピュテーション スコア
server.com	発信 URL
nc	URL カテゴリ

（注） サイトへのデータ転送（POST 要求など）がいつ外部 DLP サーバーによってブロックされたかを確認するには、アクセス ログの DLP サーバーの IP アドレスまたはホスト名を検索します。

エンドユーザーへのプロキシ アクションの通知

この章で説明する内容は、次のとおりです。

エンドユーザー通知の概要

以下のタイプのエンドユーザーへの通知を設定できます。

オプション	説明	解説場所
エンドユーザー確認応答ページ	エンドユーザーに、自分のWebアクティビティがフィルタリングおよびモニターされていることを通知します。エンドユーザー確認応答ページは、ユーザーが初めてブラウザにアクセスしてから一定時間経過後に表示されます。	エンドユーザー確認応答ページ （81 ページ）
エンドユーザー通知ページ	エンドユーザーに、特定のブロック理由のために特定のページへのアクセスがブロックされていることを通知します。	エンドユーザー通知ページ （85 ページ）
エンドユーザーURL フィルタリング警告ページ	エンドユーザーに、ユーザーがアクセスしようとしているサイトが組織のアクセプタブル ユース ポリシーに一致しないことを警告し、ユーザーが選択すればアクセスの続行を許可します。	エンドユーザーURL フィルタリング警告ページの設定 （90 ページ）
FTP通知メッセージ（FTP notification messages）	エンドユーザーに、ネイティブFTPトランザクションがブロックされた理由を知らせます。	FTP 通知メッセージの設定 （91 ページ）。
時間およびボリューム クォータの有効期限警告ページ	エンドユーザーに、設定されたデータ量または時間制限に達したため、アクセスがブロックされることを通知します。	これらの設定は、[セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] ページの [時間およびボリューム クォータの有効期限警告ページ（Time and Volume Quotas Expiry Warning Page）] セクションで行います。 時間範囲およびクォータも参照してください。

通知ページの一般設定項目の設定

通知ページの表示言語とロゴを指定します。制限についてはこの手順で説明します。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [全般設定（General Settings）] セクションで、Web プロキシが通知ページを表示する際に使用する言語を選択します。

- HTTP の言語設定は、すべての HTTP 通知ページ（確認通知、オンボックスのエンドユーザー通知、カスタマイズしたエンドユーザー通知、エンドユーザーURL フィルタリング警告）に適用されます。
- FTP の言語は、すべての FTP 通知メッセージに適用されます。

ステップ 4 各通知ページでロゴを使用するかどうかを選択します。Cisco ロゴを指定したり、[カスタム ロゴを使用（Use Custom Logo）] フィールドに入力した URL で参照される任意のグラフィック ファイルを指定することができます。

この設定は、IPv4 を介して提供されるすべての HTTP 通知ページに適用されます。AsyncOS では IPv6 を介したイメージはサポートされません。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

関連項目

- 通知ページの URL とロゴに関する注意事項 （92 ページ）

エンドユーザー確認応答ページ

Secure Web Appliance を設定して、Web アクティビティのフィルタリングとモニタリングが行われていることをユーザに通知できます。（そのように設定されている場合）アプライアンスは、HTTP または HTTPS を使用して Web にアクセスしているすべてのユーザーに、エンドユーザー確認応答ページを表示します。ユーザーが初めて Web サイトにアクセスを試みたとき、または設定された時間間隔の後にエンドユーザー確認応答ページが表示されます。

認証でユーザー名を使用可能な場合、Web プロキシはユーザー名によってユーザーを追跡します。ユーザー名を使用できない場合は、ユーザーを追跡する方法（IP アドレスまたは Web ブラウザのセッション Cookie のいずれか）を選択できます。

（注） ネイティブ FTP トランザクションは、エンドユーザー確認ページから除外されます。

- エンドユーザー確認ページによる HTTPS および FTP サイトへのアクセス （82 ページ）

エンドユーザー確認ページによる HTTPS および FTP サイトへのアクセス

エンドユーザー確認応答ページは、アクセプタブル ユース ポリシー契約をクリックすることを求める HTML ページをエンド ユーザーに表示することにより動作します。ユーザーがリンクをクリックすると、Web プロキシは、最初に要求された Web サイトにクライアントをリダイレクトします。ユーザーに対して使用可能なユーザー名がない場合は、ユーザーがサロゲート（IP アドレスまたは Web ブラウザ セッション Cookie のいずれか）を使用してエンド ユーザー確認応答ページを受け入れた時期を記録します。

- **HTTPS**。Web プロキシは、ユーザーが Cookie を使用してエンドユーザー確認応答ページを確認したかどうかを追跡しますが、トランザクションを復号しない限り Cookie を取得できません。エンドユーザー確認応答ページがイネーブルになっており、セッションCookie を使用してユーザーを追跡する場合は、HTTPS 要求をバイパス（パススルー）するかドロップするかを選択できます。advancedproxyconfig > EUN CLI コマンドを使用してこの操作を実行し、「セッションベースの EUA により HTTPS 要求に対して実行されるアクション（「bypass」または「drop」）」コマンドをバイパスすることを選択します。
- **FTP over HTTP**。Web ブラウザは、FTP over HTTP トランザクションに Cookie を送信することはないので、Web プロキシは Cookie を取得できません。このような状況を回避するために、FTP over HTTP トランザクションに対してエンドユーザー確認応答ページの要求が適用されないようにできます。正規表現として「ftp://」（引用符なし）を使用してカスタム URL カテゴリを作成し、このカスタム URL カテゴリに対してユーザーにエンドユーザー確認ページを表示しないようにする ID ポリシー定義します。

エンドユーザー確認応答ページについて

- ユーザーが IP アドレスによって追跡される場合、アプライアンスは最大時間間隔の最短の値と IP アドレスの最長アイドル タイムアウトを使用して、エンド ユーザー確認応答ページを再表示する時点を指定します。
- ユーザーがセッション Cookie を使用して追跡される場合、Web プロキシは、ユーザーが Web ブラウザを閉じて再起動したときや、別の Web ブラウザ アプリケーションを開いたときに、エンドユーザー確認応答ページを再表示します。
- クライアントが FTP over HTTP を使用して HTTPS サイトまたは FTP サーバーにアクセスする場合、セッション Cookie によるユーザーの追跡は動作しません。
- アプライアンスが明示的転送モードで展開され、ユーザーが HTTPS のサイトに移動する場合、エンドユーザー確認応答ページでは、最初に要求された URL にユーザーをリダイレクトするリンクにドメイン名のみが含まれます。最初に要求された URL のドメイン名の後にテキストが含まれている場合、このテキストは切り捨てられます。
- エンドユーザー確認ページがユーザーに表示されると、そのトランザクションのアクセス ログ エントリには ACL デシジョン タグとして OTHER が表示されます。これは、最初に要求した URL がブロックされ、代わりにユーザーにはエンド ユーザー確認ページが表示されたためです。

エンドユーザー確認応答ページの設定

始める前に

- 表示言語の設定、および表示されるロゴのカスタマイズについては、通知ページの一般設定項目の設定 （80 ページ） を参照してください。
- エンドユーザーに表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ （91 ページ） を参照してください。[カスタム メッセージ（Custom Message）]ボックスでできること以上のカスタマイズが必要な場合は、通知ページHTMLファイルの直接編集 （93 ページ） を参照してください。

Web インターフェイスまたはコマンドライン インターフェイスで、エンドユーザー確認応答ページをイネーブルにしたり、設定することができます。Webインターフェイスでエンドユーザー確認応答ページを設定する場合は、各ページに表示するカスタムメッセージを含めることができます。

CLI で、`advancedproxyconfig > eun` を使用します。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [ユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [確認ページからクリックすることをエンドユーザーに要求（Require end-user to click through acknowledgment page）] フィールドをイネーブルにします。

ステップ 4 オプションを入力します。

設定	説明
確認応答の時間間隔（Time Between Acknowledgements）	[確認応答の時間間隔（Time Between Acknowledgements）] では、Web プロキシがユーザーごとにエンドユーザー確認ページを表示する頻度を指定します。この設定は、ユーザー名で追跡されるユーザー、および IP アドレスまたはセッション Cookie で追跡されるユーザーに適用されます。30 ～ 2678400 秒（1 カ月）の任意の値を指定できます。デフォルトは 1 日（86400 秒）です。 [確認応答の時間間隔（Time Between Acknowledgements）] を変更して確定すると、Web プロキシは、Web プロキシに確認応答済みのユーザーにも新しい値を使用します。
無活動タイムアウト（Inactivity Timeout）	[無活動タイムアウト（Inactivity Timeout）] では、IP アドレスまたはセッション Cookie（未認証ユーザーのみ）によって追跡され確認されたユーザーが、アクセプタブルユース ポリシーに同意していないと見なされるまでに、アイドル状態を維持できる時間を指定します。30 ～ 2678400（1 か月）秒の任意の値を指定できます。デフォルトは 4 時間（14400 秒）です。

設定	説明
サロゲート タイプ（Surrogate Type）	Web プロキシがユーザーの追跡に使用する方式を指定します。 • **[IPアドレス（IP Address）]。**Web プロキシは、その IP アドレスのユーザーがエンドユーザー確認応答ページ上のリンクをクリックしたときに、任意の Web ブラウザまたはブラウザ以外の HTTP プロセスを使用して Web にアクセスできるようにします。IP アドレスによるユーザーの追跡では、ユーザーが非アクティブであったり設定された時間間隔が経過したために、新たな確認が必要になり、Web プロキシが新しいエンドユーザー確認応答ページを表示するまで、ユーザーは Web アクセスできます。セッション Cookie による追跡とは異なり、IP アドレスによる追跡では、設定された時間間隔が経過しない限り、ユーザーは複数の Web ブラウザアプリケーションを開くことができ、エンドユーザー確認に合意する必要はありません。 （注） IP アドレスが設定され、ユーザーが認証されると、Web プロキシは、IP アドレスではなく、ユーザー名によってユーザーを追跡します。 • **[セッションCookie（Session Cookie）]。**ユーザーがエンドユーザー確認応答ページ上のリンクをクリックすると、Web プロキシはユーザーの Web ブラウザに Cookie を送信し、Cookie を使用してユーザーのセッションを追跡します。[確認応答の時間間隔（Time Between Acknowledgements）] の値が失効するまで、または、ユーザーが割り当てられた時間よりも長時間非アクティブであったり Web ブラウザを閉じるまで、ユーザーは Web ブラウザを使用して Web にアクセスできます。 ブラウザ以外の HTTP クライアント アプリケーションを使用している場合、ユーザーが Web にアクセスするには、エンドユーザー確認応答ページ上のリンクをクリックできなければなりません。別の Web ブラウザ アプリケーションを開く場合は、Web プロキシが別の Web ブラウザにセッション Cookie を送信できるように、ユーザーは再度エンド ユーザー確認プロセスを実行する必要があります。 （注） クライアントが FTP over HTTP を使用して HTTPS サイトや FTP サーバーにアクセスする場合、セッション Cookie を使用したユーザーの追跡はサポートされません。
カスタム メッセージ（Custom message）	各エンドユーザー確認応答ページに表示するテキストをカスタマイズします。いくつかの単純な HTML タグを組み込んでテキストを書式設定できます。 （注） Web インターフェイスでエンドユーザー確認応答ページを設定する場合にのみカスタム メッセージを組み込むことができます。これは CLI では実行できません。 通知ページ上のカスタム メッセージ （91 ページ）も参照してください。

ステップ 5 （任意）[確認応答ページのカスタマイズをプレビュー（Preview Acknowledgment Page Customization）] をクリックして、別のブラウザ ウィンドウに現在のエンドユーザー確認応答ページを表示します。

（注）
HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

エンドユーザー通知ページ

ポリシーが Web サイトからユーザーをブロックする場合、URL 要求をブロックした理由をユーザーに通知するようにアプライアンスを設定できます。これは、以下のようないくつかの方法で実行できます。

目的	参照先
Secure Web Applianceでホストされている、事前定義され、カスタマイズ可能なページを表示します。	オンボックス エンドユーザー通知ページの設定 （85 ページ）
特定の URL にある HTTP エンドユーザー通知ページにユーザーをリダイレクトします。	オフボックス エンドユーザー通知ページ （86 ページ）

オンボックス エンド ユーザー通知ページの設定

始める前に

- 表示言語の設定、および表示されるロゴのカスタマイズについては、通知ページの一般設定項目の設定 （80 ページ） を参照してください。
- オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ （91 ページ） 以下のトピックを参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集 （93 ページ） を参照してください。

オンボックス ページは、アプライアンス上にある、事前定義されたカスタマイズ可能な通知ページです。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [通知タイプ（Notification Type）] フィールドで、[オンボックス エンド ユーザー通知を使用（Use On Box End User Notification）] を選択します。

ステップ 4 オンボックス エンドユーザー通知ページの設定項目を設定します。

設定	説明
カスタム メッセージ（Custom Message）	各通知ページに必要なテキストを追加します。カスタム メッセージを入力すると、AsyncOS は、連絡先情報を含む通知ページの末尾の文の前にメッセージを配置します。
コンタクト情報（Contact Information）	各通知ページに表示される連絡先情報をカスタマイズします。 AsyncOS は、ユーザーがネットワーク管理者に提供できる通知コードを表示する前に、連絡先情報の文をページの末尾の文として表示します。
エンドユーザー誤分類レポート（End-User Misclassification Reporting）	有効にすると、AsyncOS 14.5 から、誤分類要求が HTTPS 経由で送信されます。セキュリティアラート通知は受信しません。 イネーブルにすると、ユーザーは誤分類された URL をシスコに報告できます。マルウェアの疑いがあるため、または URL フィルタによってブロックされたサイトのオンボックス エンドユーザー通知ページには、追加のボタンが表示されます。このボタンを使用して、ユーザーは誤分類されていると思われるページをレポートできます。その他のポリシー設定によってブロックされたページには表示されません。 （注） • [SensorBaseネットワークに参加（SensorBase Network Participation）] を有効にする必要があります。詳細については、「Cisco SensorBase ネットワークへの参加の有効化」を参照してください。 • アプライアンスのシリアル番号にリンクされている有効なシスコアカウントが必要です。 • 誤分類された URL のレポートは、仮想 Secure Web Applianceでは機能しません。

ステップ 5 （任意）[通知ページのカスタマイズをプレビュー（Preview Notification Page Customization）] リンクをクリックして、別のブラウザ ウィンドウで現在のエンド ユーザー通知ページを表示します。

（注）
HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

オフボックス エンドユーザー通知ページ

すべての HTTP エンドユーザー通知ページを指定した特定の URL にリダイレクトするように Web プロキシを設定できます。

• アクセスをブロックする理由に基づく適切なオフボックス ページの表示 （87 ページ）

- オフボックス通知ページの URL 基準 （87 ページ）
- オフボックス エンドユーザー通知ページのパラメータ （87 ページ）
- カスタム URL へのエンドユーザー通知ページのリダイレクト（オフボックス） （89 ページ）

アクセスをブロックする理由に基づく適切なオフボックス ページの表示

デフォルトでは、AsyncOS は、元のページをブロックした理由に関係なく、ブロックしたすべての Web サイトを URL にリダイレクトします。ただし、AsyncOS はリダイレクト URL にクエリー文字列を追加し、それをパラメータとして渡すので、ブロックの理由を説明する固有のページをユーザーに対して表示するように設定できます。組み込みパラメータの詳細については、オフボックス エンドユーザー通知ページのパラメータ （87 ページ）を参照してください。

Web サイトがブロックされた理由ごとに異なるページをユーザーに表示する場合は、リダイレクト URL のクエリー文字列を解析できる CGI スクリプトを Web サーバーに作成します。これによって、サーバーは適切なページに別のリダイレクトを実行できます。

オフボックス通知ページの URL 基準

- 任意の HTTP または HTTPS URL を使用できます。
- URL では特定のポート番号を指定できます。
- URL では疑問符の後に引数を付けることはできません。
- URL には適切な形式のホスト名を含める必要があります。

たとえば、[カスタム URL へのリダイレクト（Redirect to Custom URL）] フィールドに以下の URL を入力したときに、

```
http://www.example.com/eun.policy.html
```

以下のアクセス ログ エントリがある場合、

```
1182468145.492 1 172.17.0.8 TCP_DENIED/403 3146 GET http://www.espn.com/index.html
HTTP/1.1 - NONE/- - BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
<IW_sprt,-,-,-,-,-,-,-,-,-,-,-,-,-,IW_sprt,-> -
```

AsyncOS は、以下のリダイレクト URL を作成します。

```
http://www.example.com/eun.policy.html?Time=21/Jun/
2007:23:22:25%20%2B0000&ID=0000000004&Client_IP=172.17.0.8&User=-
&Site=www.espn.com&URI=index.html&Status_Code=403&Decision_Tag=
BLOCK_WEBCAT-DefaultGroup-DefaultGroup-NONE-NONE-DefaultRouting
&URL_Cat=Sports%20and%20Recreation&WBRS=-&DVS_Verdict=-&
DVS_ThreatName=-&Reauth_URL=-
```

オフボックス エンドユーザー通知ページのパラメータ

AsyncOS は、HTTP GET 要求の標準 URL パラメータとして Web サーバーにパラメータを渡します。以下の形式を使用します。

```
<notification_page_url>?param1=value1&param2=value2
```

以下の表は、AsyncOS がクエリ文字列に含めるパラメータを示しています。

パラメータ名	説明
時刻（Time）	トランザクションの日付と時刻。
ID	トランザクション ID。
Client_IP	クライアントの IP アドレス。
User	要求を行うクライアントのユーザー名（該当する場合）。
Site	HTTP 要求の宛先ホスト名。
URI	HTTP 要求で指定された URL パス。
Status_Code	要求の HTTP ステータス コード。
Decision_Tag	DVS エンジンがトランザクションを処理した方法を示す、アクセス ログ エントリで定義されている ACL デシジョン タグ。
URL_Cat	URL フィルタリング エンジンがトランザクション要求に割り当てた URL カテゴリ。 **注**：AsyncOS for Web は、定義済みとユーザー定義の両方の URL カテゴリの URL カテゴリ名全体を送信します。カテゴリ名に対して URL エンコードが行われるため、スペースは「%20」と書き込まれます。
WBRS	Web レピュテーション フィルタが要求の URL に割り当てた WBRS スコア。
DVS_Verdict	DVS エンジンがトランザクションに割り当てるマルウェア カテゴリ。
DVS_ThreatName	DVS エンジンによって検出されたマルウェアの名前。

パラメータ名	説明
Reauth_URL	制限付き URL フィルタリング ポリシーによって Web サイトからブロックされた場合、ユーザーはこの URL をクリックして再度認証を受けることができます。このパラメータは、[URLカテゴリまたはユーザー セッションの制限によりエンド ユーザーがブロックされた場合に再認証プロンプトをイネーブルにする（Enable Re-Authentication Prompt If End User Blocked by URL Category or User Session Restriction）] グローバル認証設定がイネーブルになっているときに、URL カテゴリがブロックされたため、ユーザーが Web サイトからブロックされた場合に使用します。 このパラメータを使用するには、CGI スクリプトで以下の手順が実行されるようにします。 1.`Reauth_Url` パラメータの値を取得する。 2. URL エンコードされた値をデコードする。 3. 値を Base64 でデコードし、実際の再認証 URL を取得する。 4. デコードした URL を何らかの方法で（リンクまたはボタンとして）エンドユーザー通知ページに組み込み、「リンクをクリックすると、より広範なアクセスが可能になる新しい認証クレデンシャルを入力できること」をユーザーに示す使用説明を含める。

（注） AsyncOS は、リダイレクトされた各 URL に、常にすべてのパラメータを組み込みます。特定のパラメータの値が存在しない場合、AsyncOS はハイフン（-）を渡します。

カスタム URL へのエンドユーザー通知ページのリダイレクト（オフボックス）

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [エンドユーザー通知ページ（End-User Notification Pages）] セクションで、[カスタム URL へのリダイレクト（Redirect to Custom URL）] を選択します。

ステップ 4 [通知ページの URL（Notification Page URL）] フィールドに、ブロックされた Web サイトをリダイレクトする URL を入力します。

ステップ 5 （任意）[カスタムURLのプレビュー（Preview Custom URL）] をクリックします。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

エンド ユーザー URL フィルタリング警告ページの設定

始める前に

- オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ （91 ページ） 以下のトピックを参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集 （93 ページ） を参照してください。

エンドユーザー URL フィルタリング警告ページは、ユーザーが特定の URL カテゴリの Web サイトに初めてアクセスしてから一定時間経過後に表示されます。サイト コンテンツ レーティング機能がイネーブルのときに、ユーザーがアダルト コンテンツにアクセスした場合の警告ページを設定することもできます。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [エンドユーザーフィルタリング警告ページ（End-User URL Filtering Warning Page] セクションまでスクロール ダウンします。

ステップ 4 [確認応答の時間間隔（Time Between Warning）] フィールドで、Web プロキシがユーザーごとに各 URL カテゴリに対してエンドユーザー URL フィルタリング警告ページを表示する時間間隔を入力します。

30 ～ 2678400 秒（1 カ月）の任意の値を指定できます。デフォルトは 1 時間（3600 秒）です。秒、分、または日単位で値を入力できます。秒には「s」、分には「m」、日には「d」を使用します。

ステップ 5 [カスタム メッセージ（Custom Message）] フィールドで、すべてのエンドユーザー URL フィルタリング警告ページに表示するテキストを入力します。

ステップ 6 [URL カテゴリ警告ページのカスタマイズをプレビュー（Preview URL Category Warning Page Customization）] をクリックして、別のブラウザ ウィンドウでエンドユーザー URL フィルタリング警告ページを表示します。

（注）
HTML 通知ファイルを編集した場合、このプレビュー機能は使用できなくなります。

ステップ 7 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

FTP 通知メッセージの設定

始める前に

オンボックス通知を使用して表示されるメッセージをカスタマイズする場合は、通知ページ上のカスタム メッセージ （91 ページ） 以下のトピックを参照してください。[カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、通知ページ HTML ファイルの直接編集 （93 ページ） を参照してください。

FTP サーバーの認証エラーやサーバー ドメイン名に対する低いレピュテーションなど、何らかの理由により FTP プロキシが FTP サーバーとの接続を確立できない場合、FTP プロキシはネイティブ FTP クライアントに定義済みのカスタマイズ可能な通知メッセージを表示します。通知は、接続がブロックされる理由によって固有なものになります。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [エンドユーザー通知（End-User Notification）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [ネイティブFTP（Native FTP）] セクションまでスクロール ダウンします。

ステップ 4 [言語（Language）] フィールドで、ネイティブ FTP 通知メッセージを表示する際に使用する言語を選択します。

ステップ 5 [カスタム メッセージ（Custom Message）] フィールドで、すべてのネイティブ FTP 通知メッセージに表示するテキストを入力します。

ステップ 6 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

通知ページ上のカスタム メッセージ

以下のセクションの説明は、[エンドユーザー通知の編集（Edit End-User Notification）] ページで設定した任意の通知タイプの [カスタム メッセージ（Custom Message）] ボックスに入力するテキストに適用されます。

- 通知ページのカスタム メッセージでサポートされる HTML タグ （91 ページ）
- 通知ページの URL とロゴに関する注意事項 （92 ページ）

通知ページのカスタム メッセージでサポートされる HTML タグ

[カスタム メッセージ（Custom Message）] ボックスが用意された [エンドユーザー通知の編集（Edit End-User Notification）] ページでは、HTML タグを使用して、任意の通知のテキストを書式設定することができます。タグは小文字で入力し、標準 HTML 構文（終了タグなど）に従う必要があります。

以下の HTML タグを使用できます。

- <a>
-
-
- <big></big>
-
- <code></code>
-
-
- <small></small>
-

たとえば、一部のテキストを斜体にすることができます。

```
Please acknowledge the following statements <i>before</i> accessing the Internet.
```

タグにより、CSS スタイルを使用してテキストを書式設定できます。たとえば、一部のテキストを赤色にすることができます。

```
<span style="color: red">Warning:</span> You must acknowledge the following statements
<i>before</i> accessing the Internet.
```

（注） 通知ページをさらに柔軟にする必要がある場合や、JavaScript を追加したい場合は、HTML 通知ファイルを直接編集します。通知の [カスタム メッセージ（Custom Message）] ボックスに入力した JavaScript は、Web ユーザーのインターフェイスでは削除されます。通知ページ HTML ファイルの直接編集 （93 ページ） を参照してください。

通知ページの URL とロゴに関する注意事項

この項は以下のいずれかのカスタマイズ行う場合に適用されます。

- [エンドユーザー通知の編集（Edit End-User Notification）] ページで、任意の通知の [カスタム メッセージ（Custom Message）] ボックスにテキストを入力する。
- オンボックス通知の HTML ファイルを直接編集する。
- カスタム ロゴを使用する。

オンボックス通知の場合、カスタム テキストにリンクが埋め込まれた URL パスとドメイン名の全組み合わせとカスタム ロゴのあらゆる組み合わせが、以下のものから免除されます。

- ユーザー認証
- エンドユーザー確認応答
- マルウェア スキャンおよび Web レピュテーション スコアなどのすべてのスキャン

たとえば、以下の URL がカスタム テキストに埋め込まれている場合、

```
http://www.example.com/index.html
```

```
http://www.mycompany.com/logo.jpg
```

以下の URL すべてがあらゆるスキャンの対象外として扱われます。

```
http://www.example.com/index.html

http://www.mycompany.com/logo.jpg

http://www.example.com/logo.jpg

http://www.mycompany.com/index.html
```

また、埋め込まれた URL の形式が `<protocol>://<domain-name>/<directory path>/` である場合、ホスト上のそのディレクトリ パスにあるすべてのサブファイルとサブディレクトリもすべてのスキャンから除外されます。

たとえば、`http://www.example.com/gallery2/` という URL が埋め込まれている場合は、`http://www.example.com/gallery2/main.php` などの URL も対象外として扱われます。

これにより、埋め込まれたコンテンツが最初の URL に関連している限り、埋め込まれたコンテンツを使用してより高度なページを作成することができます。ただし、リンクやカスタム ロゴとして含めるパスを決定する際に注意を払う必要があります。

通知ページ HTML ファイルの直接編集

各通知ページは、 Secure Web Applianceに HTML ファイルとして保存されます。Web ベース インターフェイスの [カスタム メッセージ（Custom Message）] ボックスでできること以上のカスタマイズが必要な場合は、これらの HTML ファイルを直接編集できます。たとえば、標準 JavaScript を含めるか、または各ページの全体的なルック アンド フィールを編集できます。

以下の各項の情報は、エンドユーザー確認ページなど、アプライアンスの任意の種類のエンドユーザー通知 HTML ファイルに適用されます。

- 通知 HTML ファイルを直接編集するための要件 （93 ページ）
- 通知ページ HTML ファイルの直接編集 （93 ページ）
- 通知 HTML ファイルでの変数の使用 （94 ページ）
- 通知 HTML ファイルのカスタマイズのための変数 （95 ページ）

通知 HTML ファイルを直接編集するための要件

- 個々のカ通知ページ ファイルは、有効な HTML ファイルである必要があります。組み込むことができる HTML タグのリストについては、通知ページのカスタム メッセージでサポートされる HTML タグ （91 ページ）を参照してください。
- カスタマイズした通知ページ ファイルの名前は、 Secure Web Applianceに同梱されているファイルの名前と正確に一致する必要があります。

  `configuration\eun` ディレクトリに必要な名前を持つ特定のファイルが含まれていない場合、アプライアンスは標準のオンボックス エンドユーザー通知ページを表示します。
- HTML ファイルに URL へのリンクを含めないでください。通知ページに含まれるリンクは、アクセス ポリシーで定義されたアクセス制御ルールの対象となり、ユーザーは再帰ループで終了する場合があります。

- 特に JavaScript. が含まれている場合は、期待どおりに動作することを確認するために、サポートされているクライアントのブラウザで HTML ファイルをテストします。
- カスタマイズしたページが効果を表すようにするには、`advancedproxyconfig > EUN > Refresh EUN Pages` CLI コマンドを使用して、カスタマイズしたファイルを有効化する必要があります。

通知 HTML ファイルの直接編集

始める前に

- 通知 HTML ファイルを直接編集するための要件 （93 ページ） の要件を確認します。
- 通知 HTML ファイルのカスタマイズのための変数 （95 ページ）および通知 HTML ファイルでの変数の使用 （94 ページ）を参照してください。

手順

ステップ 1 FTP クライアントを使用して、 Secure Web Applianceに接続します。

ステップ 2 `configuration\eun` ディレクトリに移動します。

ステップ 3 編集する通知ページの言語ディレクトリ ファイルをダウンロードします。

ステップ 4 ローカルマシンで、テキストエディタまたはHTMLエディタを使用してHTML ファイルを編集します。

ステップ 5 FTP クライアントを使用して、ステップ 3 でこれらのファイルをダウンロードした同じディレクトリに、カスタマイズした HTML ファイルをアップロードします。

ステップ 6 SSH クライアントを開き、 Secure Web Applianceに接続します。

ステップ 7 `advancedproxyconfig > EUN` CLI コマンドを実行します。

ステップ 8 **2** を入力して、カスタム エンド ユーザー通知ページを使用します。

ステップ 9 HTML ファイルを更新する際にカスタム エンド ユーザー通知ページ オプションがイネーブルになっている場合は、**1** を入力して、カスタム エンド ユーザー通知ページを更新します。

これを実行しないと、Web プロキシを再起動するまで新しいファイルが有効になりません。

ステップ 10 変更を保存します。

ステップ 11 SSH クライアントを閉じます。

通知 HTML ファイルでの変数の使用

通知 HTML ファイルを編集する際に、条件変数を含めると、実行時点のステータスに応じて異なるアクションを実行する if-then ステートメントを作成できます。

以下の表は、さまざまな条件変数の形式を示しています。

条件変数の形式	説明
%?*V*	変数 %*V* の出力が空でない場合、この条件変数は TRUE に評価されます。
%!*V*	以下の条件を表します。 `else` これを %?*V* 条件変数とともに使用します。
%#*V*	以下の条件を表します。 `endif` これを %?*V* 条件変数とともに使用します。

たとえば、以下の HTML コードの一部であるテキストでは、再認証が提供されるかどうかをチェックする条件変数として %R が使用され、再認証 URL を提供する標準変数として %r が使用されています。

```
%?R
<div align="left">
  <form name="ReauthInput" action="%r" method="GET">
    <input name="Reauth" type="button" OnClick="document.location='%r'" id="Reauth"
value="Login as different user...">
  </form>
</div>
%#R
```

通知 HTML ファイルのカスタマイズのための変数 （95 ページ）に記載されている任意の変数を条件変数として使用できます。ただし、条件文での使用に最も適した変数は、サーバー応答ではなく、クライアント要求に関連する変数であり、常に TRUE に評価される変数ではなく、状況に応じて TRUE に評価される（または評価されない）変数です。

通知 HTML ファイルのカスタマイズのための変数

通知 HTML ファイルで変数を使用して、ユーザー固有の情報を表示できます。また、各変数を条件変数に変換して、if-then ステートメントを作成することもできます。詳細については、通知 HTML ファイルでの変数の使用 （94 ページ）を参照してください。

変数	説明	条件変数として使用する場合、常に TRUE に評価
%a	FTP の認証レルム	なし
%A	ARP アドレス	あり
%b	ユーザーエージェント名	なし
%B	ブロックした理由（BLOCK-SRC または BLOCK-TYPE など）	なし
%c	エラー ページの担当者	あり

変数	説明	条件変数として使用する場合、常に TRUE に評価
%C	Set-Cookie: ヘッダー行全体、または空の文字列	なし
%d	クライアント IP アドレス	あり
%D	ユーザー名	なし
%e	エラー ページの電子メール アドレス	あり
%E	エラー ページのロゴの URL	なし
%f	ユーザー フィードバック セクション	なし
%F	ユーザー フィードバックの URL	なし
%g	Web カテゴリ名（使用可能な場合）	あり
%G	許可される最大ファイル サイズ（MB 単位）	なし
%h	プロキシのホスト名	あり
%H	URL のサーバー名	あり
%i	トランザクション ID（16 進数値）	あり
%I	管理 IP アドレス	あり
%j	URL カテゴリ警告ページのカスタム テキスト	なし
%k	エンドユーザー確認応答ページおよびエンドユーザー URL フィルタリング警告ページのリダイレクション リンク	なし
%K	レスポンス ファイル タイプ	なし
%l	WWW-Authenticate: ヘッダー行	なし
%L	Proxy-Authenticate: ヘッダー行	なし
%M	要求方式（「GET」、「POST」など）	あり
%n	マルウェア カテゴリ名（使用可能な場合）	なし
%N	マルウェア脅威名（使用可能な場合）	なし
%o	Web レピュテーションの脅威タイプ（使用可能な場合）	なし
%O	Web レピュテーションの脅威の理由（使用可能な場合）	なし
%p	Proxy-Connection HTTP ヘッダーの文字列	あり

変数	説明	条件変数として使用する場合、常に TRUE に評価
%P	プロトコル	対応
%q	ID ポリシー グループの名前	あり
%Q	非 ID ポリシーのポリシー グループ名	あり
%r	リダイレクト URL	なし
%R	再認証が提供されます。この変数は、false の場合に空の文字列を出力し、true の場合にスペースを出力するので、単独で使用しても役立ちません。代わりに、条件変数として使用します。	なし
%S	プロキシの署名	なし。常に FALSE に評価
%t	UNIX のタイムスタンプ（秒 + ミリ秒）	あり
%T	日付	あり
%u	URI の一部を構成する URL（サーバー名を除く URL）	あり
%U	要求の完全な URL	あり
%v	HTTP プロトコルのバージョン	あり
%W	管理 WebUI ポート	あり
%X	拡張ブロック コード。ACL デシジョン タグや WBRS スコアなど、アクセス ログに記録された大部分の Web レピュテーションやアンチマルウェア情報をエンコードする 16 バイトの Base64 値です。	あり
%Y	設定されている場合は、管理者のカスタム テキスト文字列。設定されていない場合は空の文字列	なし
%y	エンドユーザー確認応答ページのカスタム テキスト	あり
%z	Web レピュテーション スコア	あり
%Z	DLP メタデータ	あり
%%	通知ページにパーセント記号（%）を出力します	該当なし

通知ページのタイプ

デフォルトでは、Webプロキシは、ユーザーがブロックされたことおよびその理由をユーザーに知らせる通知ページを表示します。

ほとんどの通知ページは、管理者またはCiscoカスタマーサポートが潜在的な問題をトラブルシューティングするのに役立つ可能性のあるさまざまなコードのセットを表示します。一部のコードはシスコ内部でのみ使用されます。通知ページに表示されるさまざまなコードは、カスタマイズした通知ページに含めることができる変数と同じです（通知 HTML ファイルのカスタマイズのための変数 （95 ページ） を参照）。

以下の表は、ユーザーに表示される可能性があるさまざまな通知ページを示しています。

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_ACCEPTED フィードバックを受信しました。ありがとうございます。（Feedback Accepted, Thank You）	ユーザーが [誤分類をレポート（Report Misclassification）] オプションを使用した後に表示される通知ページ。	誤分類のレポートが送信されました。（The misclassification report has been sent.）フィードバックいただき、ありがとうございました。（Thank you for your feedback.）
ERR_ADAPTIVE_SECURITY ポリシー：全般（Policy: General）	ユーザーが適応型スキャン機能によってブロックされた場合に表示されるブロック ページ。	この Web サイト <URL> は、コンテンツがセキュリティリスクであると判定されたため、組織のセキュリティポリシーに基づいてブロックされました。（Based on your organization’s security policies, this web site <*URL*> has been blocked because its content has been determined to be a security risk.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_ADULT_CONTENT ポリシーの確認（Policy Acknowledgment）	エンドユーザーがアダルトコンテンツに分類されるページにアクセスしたときに表示される警告ページ。ユーザーは確認リンクをクリックして、最初に要求したサイトに進むことができます。	明示的にアダルト向けとレーティングされたコンテンツを含む Web ページにアクセスしようとしています。（You are trying to visit a web page whose content are rated as explicit or adult.）下記のリンクをクリックし、このコンテンツタイプに対するインターネットの使用を管理している組織のポリシーを読了して同意済みであることを確認してください。（By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.）ブラウジング動作に関するデータがモニターされ、記録される場合があります。（Data about your browsing behavior may be monitored and recorded.）この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。（You will be periodically asked to acknowledge this statement for continued access to this kind of web page.） このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）
ERR_AVC ポリシー：アプリケーションの制御（Policy: Application Controls）	ユーザーが Application Visibility and Control エンジンによってブロックされた場合に表示されるブロックページ。	組織のアクセス ポリシーに基づき、タイプ %2 のアプリケーション %1 へのアクセスがブロックされました。（Based on your organization’s access policies, access to application %1 of type %2 has been blocked.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_BAD_REQUEST 不正な要求（Bad Request）	無効なトランザクション要求によって生じるエラー ページ。	システムはこの要求を処理できません。（The system cannot process this request.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If you are using a standard browser, please retry the request.）
ERR_BLOCK_DEST ポリシー：宛先（Policy: Destination）	ブロックされているWebサイトのアドレスにユーザーがアクセスを試みた場合に表示されるブロック ページ。	組織のアクセス ポリシーに基づき、この Web サイト <*URL*> へのアクセスがブロックされました。（Based on your organization’s Access Policies, access to this web site <URL> has been blocked.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_BROWSER セキュリティ：ブラウザ（Security: Browser）	マルウェアまたはスパイウェアによって侵害されていると識別されたアプリケーションからトランザクション要求が発信された場合に表示されるブロック ページ。	組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセス ポリシーに基づき、コンピュータからの要求がブロックされました。（Based on your organization's Access Policies, requests from your computer have been blocked because it has been determined to be a security threat to the organization's network.） 「<マルウェア名>」として識別されたマルウェア/スパイウェア エージェントによってブラウザが侵害されている可能性があります。（Your browser may have been compromised by a malware/spyware agent identified as "<malware name>".） <担当者名><電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <contact name> <email address> and provide the codes shown below.） 非標準のブラウザを使用しており、誤って分類されたと思われる場合は、以下のボタンを使用してこの誤分類をレポートしてください。（If you are using a non-standard browser and believe it has been misclassified, use the button below to report this misclassification.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_BROWSER_CUSTOM ポリシー：ブラウザ（Policy: Browser）	ブロックされたユーザーエージェントからトランザクション要求が発信されたときに表示されるブロック ページ。	組織のアクセス ポリシーに基づき、ブラウザからの要求がブロックされました。（Based on your organization's Access Policies, requests from your browser have been blocked.）このブラウザ「<ブラウザ タイプ>」は、潜在的なセキュリティ リスクのため許可されません。（This browser "<browser type>" is not permitted due to potential security risks.）
ERR_CERT_INVALID 無効な証明書（Invalid Certificate）	要求された HTTPS サイトが無効な証明書を使用している場合に表示されるブロック ページ。	サイト <ホスト名> が無効な証明書を提示したため、セキュア セッションを確立できません。（A secure session cannot be established because the site <hostname> provided an invalid certificate.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_CONTINUE_UNACKNOWLEDGED ポリシーの確認（Policy Acknowledgment）	警告アクションが割り当てられているカスタムURLカテゴリのサイトをユーザーが要求した場合に表示される警告ページ。ユーザーは確認リンクをクリックして、最初に要求したサイトに進むことができます。	URL カテゴリ <*URL* カテゴリ> に分類される Web ページにアクセスしようとしています。（You are trying to visit a web page that falls under the URL Category <URL category>.）下記のリンクをクリックし、このコンテンツ タイプに対するインターネットの使用を管理している組織のポリシーを読了して同意済みであることを確認してください。（By clicking the link below, you acknowledge that you have read and agree with the organization's policies that govern the usage of the Internet for this type of content.）ブラウジング動作に関するデータがモニターされ、記録される場合があります。（Data about your browsing behavior may be monitored and recorded.）この種の Web ページに引き続きアクセスした場合は、このメッセージが定期的に提示され、確認を求められます。（You will be periodically asked to acknowledge this statement for continued access to this kind of web page.） このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_DNS_FAIL DNS の障害（DNS Failure）	要求されたURLに無効なドメイン名が含まれている場合に表示されるエラー ページ。	このホスト名 <ホスト名> のホスト名解決（DNSルックアップ）に失敗しました。（The hostname resolution (DNS lookup) for this hostname <hostname> has failed.）インターネットアドレスのスペルが誤っているか、インターネットアドレスが廃止されているか、ホスト <ホスト名> が一時的に利用できないか、またはDNSサーバーが無応答状態になっている可能性があります。（The Internet address may be misspelled or obsolete, the host <hostname> may be temporarily unavailable, or the DNS server may be unresponsive.） 入力したインターネットアドレスのスペルを確認してください。（Please check the spelling of the Internet address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_EXPECTATION_FAILED 予測の失敗（Expectation Failed）	トランザクション要求がHTTP 417「Expectation Failed」応答をトリガーしたときに表示されるエラーページ。	システムはこのサイト <URL> に対する要求を処理できません。（The system cannot process the request for this site <*URL*>.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If using a standard browser, please retry the request.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FILE_SIZE ポリシー：ファイルサイズ（Policy: File Size）	要求されたファイルが許容される最大ファイルサイズよりも大きい場合に表示されるブロック ページ。	ダウンロードサイズが許容限度を超えているため、組織のアクセス ポリシーに基づき、この Web サイトまたはダウンロード<*URL*>へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the download size exceeds the allowed limit.）
ERR_FILE_TYPE ポリシー：ファイルタイプ（Policy: File Type）	要求したファイルがブロックされているファイル タイプである場合に表示されるブロック ページ。	ファイル タイプ「<ファイル タイプ>」は許可されていないため、組織のアクセス ポリシーに基づき、この Web サイトまたはダウンロード <*URL*> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site or download <URL> has been blocked because the file type "<file type>" is not allowed.）
ERR_FILTER_FAILURE フィルタの障害（Filter Failure）	URL フィルタリング エンジンが一時的に URL フィルタリング応答を配信できず、[到達不能サービスに対するデフォルトアクション（Default Action for Unreachable Service）] オプションが [ブロック（Block）] に設定されている場合に表示されるエラー ページ。	内部サーバーが到達不能または過負荷になっているため、ページ <*URL*> の要求が拒否されました。（The request for page <URL> has been denied because an internal server is currently unreachable or overloaded.） 後で要求を再試行してください。（Please retry the request later.）
ERR_FOUND 検出（Found）	一部のエラー用の内部リダイレクション ページ。	ページ <URL> は <リダイレクト先 URL> にリダイレクトされます。（The page <*URL*> is being redirected to <*redirected URL*>.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FTP_ABORTED FTP 中断（FTP Aborted）	FTP over HTTP トランザクション要求が HTTP 416「Requested Range Not Satisfiable」応答をトリガーしたときに表示されるエラー ページ。	ファイル<*URL*>に対する要求が成功しませんでした。（The request for the file <URL> did not succeed.）FTP サーバー <ホスト名> が突然接続を終了しました。（The FTP server <hostname> unexpectedly terminated the connection.） 後で要求を再試行してください。（Please retry the request later.）
ERR_FTP_AUTH_REQUIRED FTP 認可が必要（FTP Authorization Required）	FTP over HTTP トランザクション要求が FTP 530「Not Logged In」応答をトリガーしたときに表示されるエラー ページ。	FTP サーバー <ホスト名> には認証が必要です。（Authentication is required by the FTP server <hostname>.）プロンプトに従って有効なユーザー ID とパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.） 場合により、FTP サーバーが匿名接続の数を制限する可能性があります。（In some cases, the FTP server may limit the number of anonymous connections.）通常、匿名ユーザーとしてこのサーバーに接続している場合は、後で再試行してください。（If you usually connect to this server as an anonymous user, please try again later.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FTP_CONNECTION_FAILED FTP 接続の失敗（FTP Connection Failed）	FTP over HTTP トランザクション要求が FTP 425「Can't open data connection」応答をトリガーしたときに表示されるエラー ページ。	システムが FTP サーバー <ホスト名> と通信できません。（The system cannot communicate with the FTP server <hostname>.）FTP サーバーが一時的または恒久的にダウンしているか、ネットワークの問題により到達不能になっている可能性があります。（The FTP server may be temporarily or permanently down, or may be unreachable because of network problems.） 入力したアドレスのスペルを確認してください。（Please check the spelling of the address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_FTP_FORBIDDEN FTP の禁止（FTP Forbidden）	FTP over HTTP トランザクション要求が、ユーザーアクセスが許可されないオブジェクトに対して行われた場合に表示されるエラー ページ。	FTP サーバー <ホスト名> によってアクセスが拒否されました。（Access was denied by the FTP server <hostname>.）ご使用の ID にはこのドキュメントへのアクセス権がありません。（Your user ID does not have permission to access this document.）
ERR_FTP_NOT_FOUND FTP が検出されない（FTP Not Found）	FTP over HTTP トランザクション要求が、サーバー上に存在しないオブジェクトに対して行われた場合に表示されるエラー ページ。	ファイル<*URL*>が見つかりませんでした。（The file <URL> could not be found.）アドレスが間違っているか、または廃止されています。（The address is either incorrect or obsolete.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_FTP_SERVER_ERR FTP サーバー エラー（FTP Server Error）	FTP をサポートしていないサーバーにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラーページ。通常、サーバーは HTTP 501「Not Implemented」応答を返します。	システムが FTP サーバー <ホスト名> と通信できません。（The system cannot communicate with the FTP server <hostname>.）FTP サーバーが一時的または恒久的にダウンしているか、このサービスを提供していない可能性があります。（The FTP server may be temporarily or permanently down, or may not provide this service.） 有効なアドレスであることを確認してください。（Please confirm that this is a valid address.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_FTP_SERVICE_UNAVAIL FTP サービス使用不可（FTP Service Unavailable）	使用できない FTP サーバーにアクセスを試みている FTP over HTTP トランザクションに対して表示されるエラー ページ。	システムが FTP サーバー <ホスト名> と通信できません。（The system cannot communicate with the FTP server <hostname>.）FTP サーバーがビジー状態であるか、恒久的にダウンしているか、またはこのサービスを提供していない可能性があります。（The FTP server may be busy, may be permanently down, or may not provide this service.） 有効なアドレスであることを確認してください。（Please confirm that this is a valid address.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_GATEWAY_TIMEOUT ゲートウェイのタイムアウト（Gateway Timeout）	要求されたサーバーがタイムリーに応答しなかったときに表示されるエラー ページ。	システムが外部サーバー <ホスト名> と通信できません。（The system cannot communicate with the external server <hostname>.）インターネット サーバーがビジー状態か、恒久的にダウンしているか、またはネットワークの問題により到達不能になっている可能性があります。（The Internet server may be busy, may be permanently down, or may be unreachable because of network problems.） 入力したインターネット アドレスのスペルを確認してください。（Please check the spelling of the Internet address entered.）スペルが正しい場合は、後でこの要求を試行してください。（If it is correct, try this request later.）
ERR_IDS_ACCESS_FORBIDDEN IDS アクセスの禁止（IDS Access Forbidden）	設定済みの Cisco データ セキュリティ ポリシーによってブロックされているファイルを、ユーザーがアップロードしようとした場合に表示されるエラー ページ。	組織のデータ転送ポリシーに基づき、アップロード要求がブロックされました。（Based on your organization’s data transfer policies, your upload request has been blocked.）ファイルの詳細（File details）： <ファイルの詳細>

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_INTERNAL_ERROR 内部エラー（Internal Error）	内部エラーが発生した場合に表示されるエラー ページ。	ページ<*URL*>に対する要求を処理中に内部システム エラーが発生しました。（Internal system error when processing the request for the page <URL>.） この要求を再試行してください。（Please retry this request.） この状態が続く場合は、<担当者名><電子メール アドレス>に連絡し、以下に示すコードを提出してください。（If this condition persists, please contact <contact name> <email address> and provide the code shown below.）
ERR_MALWARE_SPECIFIC セキュリティ：マルウェアの検出（Security: Malware Detected）	ファイルのダウンロード時にマルウェアが検出された場合に表示されるブロック ページ。	この Web サイト <*URL*> は、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威と判定されたため、組織のアクセス ポリシーに基づいてブロックされました。（Based on your organization’s Access Policies, this web site <URL> has been blocked because it has been determined to be a security threat to your computer or the organization’s network.） カテゴリ <マルウェア カテゴリ> のマルウェア <マルウェア名> がこのサイトで検出されました。（Malware <malware name> in the category <malware category> has been found on this site.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_MALWARE_SPECIFIC_OUTGOING セキュリティ：マルウェアの検出（Security: Malware Detected）	ファイルのアップロード時にマルウェアが検出された場合に表示されるブロック ページ。	受信側端末のネットワーク セキュリティにとって有害なマルウェアがこのファイルから検出されたため、組織のポリシーに基づいてこのファイルのURL（<*URL*>）へのアップロードがブロックされました。（Based on your organization's policy, the upload of the file to URL (<URL>) has been blocked because the file was detected to contain malware that will be harmful to the receiving end's network security.） マルウェア名（Malware Name）:<マルウェア名> マルウェア カテゴリ（Malware Category）:<マルウェアのカテゴリ>
ERR_NATIVE_FTP_DENIED	ネイティブFTPトランザクションがブロックされたときに、ネイティブFTPクライアントで表示されるブロック メッセージ。	530 ログインが拒否されました（530 Login denied）
ERR_NO_MORE_FORWARDS これ以上転送なし（No More Forwards）	Webプロキシとネットワーク上の他のプロキシ サーバー間に転送ループがあることをアプライアンスが検出した場合に表示されるエラーページ。Webプロキシはループを切断し、クライアントにこのメッセージを表示します。	ページ<*URL*>に対する要求が失敗しました。（The request for the page <URL> failed.） サーバー アドレス <ホスト名> が無効であるか、またはこのサーバーにアクセスするにはポート番号を指定する必要があります。（The server address <hostname> may be invalid, or you may need to specify a port number to access this server.）
ERR_POLICY ポリシー：全般（Policy: General）	要求が何らかのポリシー設定によってブロックされた場合に表示されるブロック ページ。	組織のアクセス ポリシーに基づき、この Web サイト <*URL*> へのアクセスがブロックされました。（Based on your organization's Access Policies, access to this web site <URL> has been blocked.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROTOCOL ポリシー：プロトコル（Policy: Protocol）	使用しているプロトコルに基づいて要求がブロックされた場合に表示されるブロック ページ。	データ転送プロトコル「<プロトコル タイプ>」が許可されていないため、組織のアクセス ポリシーに基づき、この要求はブロックされました。（Based on your organization’s Access Policies, this request has been blocked because the data transfer protocol “<protocol type>” is not allowed.）
ERR_PROXY_AUTH_REQUIRED プロキシ認可が必要（Proxy Authorization Required）	続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これは明示的なトランザクション要求に使用されます。	このシステムを使用してインターネットにアクセスするには、認証が必要です。（Authentication is required to access the Internet using this system.）プロンプトに従って有効なユーザーIDとパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.）
ERR_PROXY_PREVENT_MULTIPLE_LOGIN 別のマシンからログイン済み（Already Logged In From Another Machine）	別のマシンのWebプロキシですでに認証されているユーザー名と同じユーザー名を使用してWebへのアクセスが試みられた場合に表示されるブロック ページ。これは、[ユーザーセッション制限（User Session Restrictions）] グローバル認証オプションがイネーブルの場合に使用されます。	このユーザー ID には別の IP アドレスからのアクティブセッションが存在するため、組織のポリシーに基づき、インターネットへのアクセス要求が拒否されました。（Based on your organization’s policies, the request to access the Internet was denied because this user ID has an active session from another IP address.） 別のユーザーとしてログインする場合は、下のボタンをクリックして、別のユーザー名とパスフレーズを入力してください。（If you want to login as a different user, click on the button below and enter a different a user name and passphrase.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROXY_REDIRECT リダイレクト（Redirect）	リダイレクション ページ。	この要求は、リダイレクトされます。（This request is being redirected.）このページが自動的にリダイレクトされない場合は、ここをクリックして続行してください。（If this page does not automatically redirect, click here to proceed.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROXY_UNACKNOWLEDGED ポリシーの確認（Policy Acknowledgment）	エンドユーザー確認ページ 詳細については、エンドユーザー通知ページ （85 ページ）を参照してください。	インターネットにアクセスする前に、以下のステートメントを確認してください。（Please acknowledge the following statements before accessing the Internet.） 危険なコンテンツを検出して組織のポリシーを適用するために、Web トランザクションは自動的にモニターされ処理されます。（Your web transactions will be automatically monitored and processed to detect dangerous content and to enforce organization’s policies.）下記のリンクをクリックすると、モニターリングに同意し、訪問したサイトに関するデータが記録される可能性について承認したものと見なされます。（By clicking the link below, you acknowledge this monitoring and accept that data about the sites you visit may be recorded.）モニターリング システムの存在について、定期的に承認を求められます。（You will be periodically asked to acknowledge the presence of the monitoring system.）ユーザーには、インターネット アクセスに関する組織のポリシーに従う責任があります。（You are responsible for following organization’s polices on Internet access.） このステートメントに同意してインターネットにアクセスするには、ここをクリックしてください。（Click here to accept this statement and access the Internet.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_PROXY_UNLICENSED プロキシのライセンスなし（Proxy Not Licensed）	Secure Web Appliance Web プロキシの有効なライセンス キーがない場合に表示されるブロック ページ。	セキュリティデバイスの適切なライセンスがないため、インターネットにアクセスできません。（Internet access is not available without proper licensing of the security device.） <担当者名><電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <contact name> <email address> and provide the codes shown below.） （注） セキュリティデバイスの管理インターフェイスにアクセスするには、ポートに設定されている IP アドレスを入力します。
ERR_RANGE_NOT_SATISFIABLE 範囲が不適切（Range Not Satisfiable）	Web サーバーが要求されたバイト範囲に対応できない場合に表示されるエラー ページ。	システムはこの要求を処理できません。（The system cannot process this request.）非標準のブラウザによって無効な HTTP 要求が生成された可能性があります。（A non-standard browser may have generated an invalid HTTP request.） 標準ブラウザを使用している場合は、要求を再試行してください。（If you are using a standard browser, please retry the request.）
ERR_REDIRECT_PERMANENT 永続的リダイレクト（Redirect Permanent）	内部リダイレクション ページ。	ページ<URL>は<リダイレクト先URL> にリダイレクトされます。（The page <*URL*> is being redirected to <*redirected URL*>.）
ERR_REDIRECT_REPEAT_REQUEST リダイレクト	内部リダイレクション ページ。	要求を繰り返してください。（Please repeat your request.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_SAAS_AUTHENTICATION ポリシー：アクセス拒否（Policy: Access Denied）	続行するために認証クレデンシャルを入力する必要がある場合に表示される通知ページ。これはアプリケーションへのアクセスに使用されます。	組織のポリシーに基づき、<*URL*>へのアクセス要求は、ログインクレデンシャルの入力が必要なページにリダイレクトされました。（Based on your organization's policy, the request to access <URL> was redirected to a page where you must enter the login credentials.）認証に成功し、適切な権限が付与されている場合は、アプリケーションへのアクセスが許可されます。（You will be allowed to access the application if authentication succeeds and you have the proper privileges.）
ERR_SAAS_AUTHORIZATION ポリシー：アクセス拒否（Policy: Access Denied）	ユーザーがアクセス権限のないアプリケーションにアクセスを試みた場合に表示されるブロックページ。	承認されたユーザーではないため、組織のポリシーに基づき、アプリケーション<*URL*>へのアクセスがブロックされました。（Based on your organization's policy, the access to the application <URL> is blocked because you are not an authorized user.）別のユーザーとしてログインする場合は、このアプリケーションへのアクセスを認可されているユーザーのユーザー名とパスフレーズを入力してください。（If you want to login as a different user, enter a different username and passphrase for a user that is authorized to access this application.）
ERR_SAML_PROCESSING ポリシー：アクセス拒否（Policy: Access Denied）	アプリケーションにアクセスするためのシングル サインオン URL の処理に内部プロセスが失敗した場合に表示されるエラーページ。	シングルサインオン要求の処理中にエラーが検出されたため、<ユーザー名> へのアクセス要求が完了しませんでした。（The request to access <user name> did not go through because errors were found during the process of the single sign on request.）

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_SERVER_NAME_EXPANSION サーバー名の拡張（Server Name Expansion）	自動的にURLを展開し、その更新したURLにユーザーをリダイレクトする内部リダイレクションページ。	サーバー名 <ホスト名> は省略形と見なされ、<リダイレクト先 *URL*> にリダイレクトされます。（The server name <hostname> appears to be an abbreviation, and is being redirected to <redirected URL>.）
ERR_URI_TOO_LONG URI が長すぎる（URI Too Long）	URL が長すぎる場合に表示されるブロック ページ。	要求されたURL が長すぎるため、処理できませんでした。（The requested URL was too long and could not be processed.）これはネットワークへの攻撃を示している可能性があります。（This may represent an attack on your network.） <担当者名><電子メール アドレス> に連絡し、以下に示すコードを提出してください。（Please contact <contact name> <email address> and provide the codes shown below.）
ERR_WBRS セキュリティ：マルウェアのリスク（Security: Malware Risk）	Web レピュテーションスコアが低いため、Web レピュテーションフィルタによってサイトがブロックされた場合に表示されるブロック ページ。	この Web サイト <*URL*> は、Web レピュテーションフィルタによって、コンピュータまたは組織のネットワークに対するセキュリティ上の脅威であると判定されたため、組織のアクセス ポリシーに基づいてブロックされました。（Based on your organization’s access policies, this web site <URL> has been blocked because it has been determined by Web Reputation Filters to be a security threat to your computer or the organization’s network.）このWebサイトは、マルウェア/スパイウェアと関連付けられています。（This web site has been associated with malware/spyware.） 脅威のタイプ（Threat Type）: %o 脅威の理由（Threat Reason）: %O

ファイル名および通知タイトル	通知の説明	通知テキスト
ERR_WEBCAT ポリシー：URL フィルタリング（Policy: URL Filtering）	ブロックされた URL カテゴリの Web サイトにユーザーがアクセスを試みた場合に表示されるブロック ページ。	Web カテゴリ「<カテゴリ タイプ>」は許可されていないため、組織のアクセス ポリシーに基づき、この Web サイト <*URL*> へのアクセスはブロックされました。（Based on your organization's Access Policies, access to this web site <URL> has been blocked because the web category "<category type>" is not allowed.）
ERR_WWW_AUTH_REQUIRED WWW 認可が必要（WWW Authorization Required）	要求されたサーバーが続行するために認証クレデンシャルの入力を必要とする場合に表示される通知ページ。	要求した Web サイト <ホスト名> にアクセスするには認証が必要です。（Authentication is required to access the requested web site <hostname>.）プロンプトに従って有効なユーザー ID とパスフレーズを入力してください。（A valid user ID and passphrase must be entered when prompted.）

非標準ポートでの不正トラフィックの検出

この章で説明する内容は、次のとおりです。

不正トラフィックの検出の概要

Secure Web Applianceは、すべてのネットワーク ポート全体にわたって不正なトラフィックを検出し、マルウェアがポート80をバイパスしようとするのを阻止する統合レイヤ4トラフィック モニタを備えています。内部クライアントがマルウェアに感染し、標準以外のポートとプロ

トコルを介して Phone Home を試みた場合、L4 トラフィック モニターは Phone Home アクティビティが企業ネットワークから外部に発信されるのを阻止します。デフォルトでは、L4 トラフィック モニターがイネーブルになり、すべてのポートでトラフィックをモニターするように設定されます。これには、DNS やその他のサービスが含まれます。

L4 トラフィック モニターは、独自の内部データベースを使用し、保持します。このデータベースは、IP アドレスおよびドメイン名の照合によって継続的に更新されます。

L4 トラフィック モニターの設定

手順

ステップ 1 ファイアウォールの内側に L4 トラフィック モニターを設定します。

ステップ 2 L4 トラフィック モニターが、プロキシ ポートの後ろ、かつクライアント IP アドレスのネットワーク アドレス変換（NAT）を実行する任意のデバイスの前に、「論理的に」接続されていることを確認します。

ステップ 3 グローバル設定項目を設定する

L4 トラフィック モニターのグローバル設定 （120 ページ）を参照してください。

ステップ 4 L4 トラフィック モニターのポリシーを作成する

不正トラフィック検出ポリシーの作成 （121 ページ） を参照してください。

既知のサイトのリスト

アドレス（**Address**）	説明
既知の許可アドレス（Known allowed）	[許可リスト（Allow List）] プロパティに記載されている IP アドレスまたはホスト名。これらのアドレスは、「許可リスト」アドレスとしてログファイルに表示されます。
未記載（Unlisted）	マルウェア サイトであるか既知の許可アドレスであるかが不明な IP アドレス。これらは、[許可リスト（Allow List）] や [追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] プロパティに記載されておらず、L4 トラフィック モニター データベースにも含まれていません。これらのアドレスはログ ファイルに表示されません。

アドレス（**Address**）	説明
不明瞭なアドレス（Ambiguous）	これらは「グレーリスト」アドレスとしてログ ファイルに表示され、以下のアドレスが該当します。 • リストに記載されていないホスト名と既知のマルウェアのホスト名の両方に関連付けられている *IP* アドレス。 • リストに記載されていないホスト名と [追加するサスペクト マルウェア アドレス（Additional Suspected Malware Addresses）] プロパティに含まれるホスト名の両方に関連付けられている *IP* アドレス。
既知のマルウェア（Known malware）	これらは「ブロックリスト」アドレスとしてログファイルに表示され、以下のアドレスが該当します。 • L4 トラフィック モニター データベースで既知のマルウェア サイトと判定され、[許可リスト（Allow List）] に記載されていない IP アドレスまたはホスト名。 • [追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] プロパティに記載され、[許可リスト（Allow List）] リストに記載されていない、不明瞭ではない *IP* アドレス。

L4 トラフィック モニターのグローバル設定

手順

ステップ 1 [セキュリティサービス（Security Services）] > [L4トラフィックモニター（L4 Traffic Monitor）] を選択します。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 L4 トラフィック モニターをイネーブルにするかどうかを選択します。

ステップ 4 L4 トラフィック モニターをイネーブルにする場合は、モニター対象のポートを選択します。

- **[すべてのポート（All ports）]。**不正なアクティビティに対して TCP ポート 65535 をすべてモニターします。
- **[プロキシ ポートを除くすべてのポート（All ports except proxy ports）]。**不正なアクティビティに対して、以下のポートを除くすべての TCP ポートをモニターします。
  - [セキュリティ サービス（Security Services）] > [Web プロキシ（Web Proxy）] ページの [プロキシを設定する HTTP ポート（HTTP Ports to Proxy）] プロパティで設定したポート（通常はポート 80）。
  - [セキュリティ サービス（Security Services）] > [HTTPS プロキシ（HTTPS Proxy）] ページの [プロキシを設定する透過 HTTPS ポート（Transparent HTTPS Ports to Proxy）] プロパティで設定したポート（通常はポート 443）。

ステップ 5 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

L4 トラフィック モニター アンチマルウェア ルールのアップデート

手順

ステップ 1 [セキュリティサービス（Security Services）] > [L4トラフィックモニター（L4 Traffic Monitor）] を選択します。

ステップ 2 [今すぐ更新（Update Now）] をクリックします。

不正トラフィック検出ポリシーの作成

L4トラフィックモニターがとるアクションは、設定するL4トラフィックモニターのポリシーによって異なります。

手順

ステップ 1 [Webセキュリティマネージャ（Web Security Manager）] > [L4トラフィックモニター（L4 Traffic Monitor）] を選択します。

ステップ 2 [設定の編集（Edit Settings）] をクリックします。

ステップ 3 [L4トラフィックモニターのポリシーの編集（Edit L4 Traffic Monitor Policies）] ページで、L4 トラフィックモニターのポリシーを設定します。

a) [許可リスト（Allow List）] を**定義します**。

b) [許可リスト（Allow List）] に既知の安全なサイトを追加します。

（注）
Secure Web Applianceの IP アドレスやホスト名を許可されたリストに含めないでください。さもないと、L4 トラフィック モニタは、どんなトラフィックもブロックしません。

c) **不審なマルウェア アドレス**に対して実行するアクションを決定します。

アクション	説明
許可（Allow）	既知の許可されたアドレスおよびリストに未記載のアドレスの発着信トラフィックを常に許可します。

アクション	説明
モニター	以下のような状況の下で、トラフィックをモニターします。 • [サスペクトマルウェアアドレスに対するアクション（Action for Suspected Malware Addresses）] オプションが [モニター（Monitor）] に設定されている場合、既知の許可されたアドレス以外のすべての着発信トラフィックを常にモニターします。 • [サスペクトマルウェアアドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、不明瞭なアドレスの着発信トラフィックをモニターします。
ブロック（Block）	[サスペクトマルウェアアドレスに対するアクション（Action for Suspected Malware Addresses] オプションが [ブロック（Block）] に設定されている場合、既知のマルウェア アドレスの着発信トラフィックをブロックします。

（注）
：不審なマルウェア トラフィックをブロックすることを選択した場合は、不明瞭なアドレスを常にブロックするかどうかも選択できます。デフォルトでは、不明瞭なアドレスはモニターされます。

：ブロックを実行するように L4 トラフィック モニターを設定する場合は、L4 トラフィック モニターと Web プロキシを同じネットワーク上に設定する必要があります。すべてのクライアントがデータ トラフィック用に設定されたルートでアクセスできることを確認するには、[ネットワーク（Network）] > [ルート（Routes）] ページを使用します。

- VM のセットアップでは、透過モードの要求が断続的な時間差で P1 インターフェイスと T1 インターフェイスを通過する間に、それらの要求が複製されます。そのため、一部の IP は、ブロックした後でもアプライアンスを通過する可能性があります。

d) [追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] プロパティを定義します。

（注）
[追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] のリストに内部 IP アドレスを追加すると、正当な宛先 URL が L4 トラフィック モニターのレポートにマルウェアとして表示されます。このような誤りを回避するために、[Webセキュリティマネージャ（Web Security Manager）] > [L4トラフィックモニターポリシー（L4 Traffic Monitor Policies）] ページの [追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] フィールドに内部 IP アドレスを入力しないでください。

ステップ 4 変更を送信して確定します（[送信（Submit）] と [変更を確定（Commit Changes）]）。

次のタスク

関連項目

- 不正トラフィックの検出の概要 （118 ページ）

• 有効な形式 （123 ページ）。

有効な形式

[許可リスト（Allow List）] または [追加するサスペクトマルウェアアドレス（Additional Suspected Malware Addresses）] プロパティにアドレスを追加する場合は、空白またはカンマを使用して複数のエントリを区切ります。以下のいずれかの形式でアドレスを入力できます。

- **IPv4 IP アドレス。**例：IPv4 形式：10.1.1.0。IPv6 形式：2002:4559:1FE2::4559:1FE2
- **CIDR アドレス。**例：10.1.1.0:24。
- **ドメイン名。**例：example.com
- **ホスト名。**例：crm.example.com

L4 トラフィック モニターのアクティビティの表示

Sシリーズアプライアンスは、サマリー統計情報の機能固有のレポートおよびインタラクティブな表示を生成するために、複数のオプションをサポートしています。

モニターリング アクティビティとサマリー統計情報の表示

[レポート（Reporting）] > [L4トラフィックモニター（L4 Traffic Monitor）] ページには、モニターリング アクティビティの統計的なサマリーが表示されます。以下の表示とレポート ツールを使用して、L4 トラフィック モニターのアクティビティの結果を表示できます。

表示対象	参照先
クライアントの統計	[レポート（Reporting）] > [クライアント アクティビティ（Client Activity）]
マルウェアの統計情報 ポートの統計情報	[レポート（Reporting）] > [L4トラフィックモニター（L4 Traffic Monitor）]
L4 トラフィック モニターのログ ファイル	[システム管理（System Administration）] > [ログサブスクリプション（Log Subscriptions）] • trafmon_errlogs • trafmonlogs

（注） Web プロキシが転送プロキシとして設定され、L4 トラフィック モニターがすべてのポートをモニターするように設定されている場合は、プロキシのデータ ポートの IP アドレスが記録され、[レポート（Reporting）] > [クライアントアクティビティ（Client Activity）] ページのクライアント アクティビティ レポートにクライアント IP アドレスとして表示されます。Web プロキシが透過プロキシとして設定されている場合は、クライアントの IP アドレスが正しく記録され、表示されるように IP スプーフィングをイネーブルにします。

L4 トラフィック モニターのログ ファイルのエントリ

L4 トラフィック モニター ログ ファイルはモニターリング アクティビティの詳細を記録します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。