CHAPTER 13

セキュリティ サービスの設定

セキュリティ サービスの設定の概要

Web セキュリティ アプライアンスは、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。各グループ ポリシーのマルウェア対策と 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（13-4 ページ）

オプション	説明	リンク
Web レピュテーション フィルタ（Web Reputation Filters）	Web サーバの動作を分析し、URL に URL ベースのマルウェアが含まれているかどうか判定します。	Web レピュテーション フィルタの概要（13-2 ページ）
高度なマルウェア防御（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（14-1 ページ）

関連項目

- マルウェア対策およびレピュテーション フィルタのイネーブル化（13-8 ページ）
- 適応型スキャンについて（13-7 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。Web セキュリティ アプライアンスは、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、復号化、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。
復号化ポリシー（Decryption Policies）	ドロップ、復号化、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 ポリシーで 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良の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（Score）	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、さらなるマルウェア スキャンは実行されません。	• URL がユーザの許可なしに情報をダウンロードする。 • URL ボリュームによる突然のスパイク。 • 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、要求およびサーバ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 スコアが陽性のネットワーク 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。 • 履歴が長く信頼できるボリュームが多いドメイン。 • 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（13-7 ページ）

復号化ポリシーの Web レピュテーション

スコア（Score）	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 ユーザに通知せずにドロップされます。この設定の使用には注意が必要です。
-8.9 ～ 5.9	復号化（Decrypt）	判別不能なサイト。要求は許可されますが、接続が復号化され、アクセス ポリシーが復号化されたトラフィックに適用されます。
6.0 ～ 10.0	パススルー	正常なサイト。要求は、検査や復号化なしで渡されます。

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（Score）	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、さらなるスキャンは実行されません。
-5.9 ～ 0.0	モニタ（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、コンテンツの検査（ファイル タイプとサイズ）へと進みます。 **（注）**　スコアがないサイトがモニタされます。

マルウェア対策 スキャンの概要

Web セキュリティ アプライアンス 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

- マルウェア対策およびレピュテーション フィルタのイネーブル化（13-8 ページ）
- 関連項目（13-9 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 つのオブジェクトに対する複数の判定が 1 つのスキャン エンジンから返されることがあります。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
  - 商用システム モニタ
  - 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 エンジンに送ります。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、その独自の設定に応じて、要求をモニタ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、サーバの応答をスキャンします。
- **サーバの応答。**アプライアンスが URL を取得すると、Webroot はサーバ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、そのデータベースにあるウィルス定義をスキャン エンジンで使用し、特定のウィルス、ウィルスのタイプ、その他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場合は、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

McAfee の判定	マルウェア スキャン判定カテゴリ
テスト ファイル	ウィルス
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
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 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場合に、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

適応型スキャン機能は、どのマルウェア対策スキャン エンジン（ダウンロード ファイルの高度なマルウェア防御スキャンを含む）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。

ポリシーごとの高度なマルウェア防御の設定は、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。

マルウェア対策およびレピュテーション フィルタのイネーブル化

はじめる前に

- 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 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。

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

手順 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 Analysis）	ファイル レピュテーションおよび分析サービスの有効化と設定（14-10 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）	最大スキャン オブジェクト サイズを指定します。 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 エンジンおよび高度なマルウェア防御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（10-13 ページ）を参照してください。 アップロードまたはダウンロードするオブジェクト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っている場合は、[スキャン不可（unscannable）] としてマークされます。
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。

設定	説明
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。

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

関連項目

- 適応型スキャンについて(13-7 ページ)
- McAfee スキャン(13-6 ページ)

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(13-10 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（13-10 ページ）
復号化ポリシー（Decryption Policies）	復号化ポリシー グループの Web レピュテーション フィルタの設定（13-14 ページ）
シスコ データ セキュリティ ポリシー（Cisco Data Security Policies）	復号化ポリシー グループの Web レピュテーション フィルタの設定（13-14 ページ）

高度なマルウェア防御機能はアクセス ポリシーにのみ設定できます。ファイル レピュテーション機能と分析機能の設定（14-5 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、この機能を設定マスターに設定する場合、このページのオプションは、関連する設定マスターで適応型セキュリティがイネーブル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。

関連項目

- 適応型スキャンについて（13-7 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 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。

手順 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。

手順 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。

手順 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。

手順 5　[高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

手順 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。

手順 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。

設定	説明
疑わしいユーザ 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 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 エージェントをモニタ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 エージェント文字列を含まないためユーザ 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。

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

関連項目

- マルウェアのカテゴリについて（13-16 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 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。

手順 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。

手順 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。

手順 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。

手順 5　[高度なマルウェア防御設定（Advanced Malware Protection Settings）] セクションで設定項目を設定します。

手順 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。

手順 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 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 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 エージェントをモニタ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 エージェント文字列を含まないためユーザ 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。
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。

設定	説明
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。

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

関連項目

- 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（13-13 ページ）
- マルウェアのカテゴリについて（13-16 ページ）

Web レピュテーション スコアの設定

Web セキュリティ アプライアンス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 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。

手順 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。

手順 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。

手順 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。

手順 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。

手順 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。

復号化ポリシー グループの Web レピュテーション フィルタの設定

手順 1　[Web セキュリティ マネージャ（Web Security Manager）] > [復号化ポリシー（Decryption Policies）] を選択します。

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

手順 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。

手順 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。

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

手順 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。

手順 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 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。

手順 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。

手順 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。

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

手順 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されます。

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 サーバから定期的にアップデートを受信します。サーバ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

Web セキュリティ アプライアンス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されるトランザクションは、次の 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しくみを示しています。

- 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であるか Web キャッシュであるかに関わらず、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設定の乗っ取りに関連するさまざまな機能を実行するおそれがあるブラウザ プラグインです。
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、ユーザの承諾なしにユーザを 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、高度なマルウェア防御ファイル 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	システム モニタには、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。

マルウェアのタイプ	説明
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名とパスフレーズを探したりします。
ウイルス	ウイルスは、ユーザ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。