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 （2 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 （7 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 （8 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 （11 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 （3 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 （7 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。
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。

オプション	説明
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） （5 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 （6 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、復号化により、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 （7 ページ）
- 全体の帯域幅制限の設定 （9 ページ）
- AVC または ADC アクティビティの表示 （12 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

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 （8 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 （9 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 （9 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

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 （10 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 （10 ページ）
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 （11 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

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。

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

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。

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。

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。