CHAPTER 15

# Web アプリケーションへのアクセスの管理



## 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)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できます。

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。

- アプリケーション動作を制御する
- 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
- 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

AVC 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 エンジンをイネーブルにする | AVC エンジンのイネーブル化(15-2 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制御の設定(15-5 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 | 帯域幅の制御(15-6 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(15-9 ページ) |

# AVC エンジンのイネーブル化

[使用許可コントロール（Acceptable Use Controls）] をイネーブルにする場合は、AVC エンジンをイネーブルにします。

（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 エンジンのスキャン アクティビティを確認できます。

**手順 1**　[セキュリティ サービス（Security Services）] > [使用許可コントロール（Acceptable Use Controls）] を選択します。

**手順 2**　[使用許可コントロール（Acceptable Use Controls）] の現在のステータスに応じて、[有効（Enable）] または [グローバル設定の編集（Edit Global Settings）] をクリックします。

**手順 3**　[Cisco Web 利用の制御を有効にする（Enable Cisco Web Usage Controls）] がオンになっていることを確認します。

**手順 4**　[使用許可コントロール サービス（Acceptable Use Controls Service）] パネルで、**Cisco Web Usage Controls** を選択し、次に [アプリケーションの表示およびコントロールを有効にする（Enable Application Visibility and Control）] を選択します。

**手順 5**　[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:）] に対して、[モニタ（Monitor）] または [ブロック（Block）] を選択します。

**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）]）。

**関連項目**

- AVC エンジンのアップデーとデフォルト アクション（15-2 ページ）
- 要求が AVC エンジンによりブロックされた場合のユーザ エクスペリエンス（15-3 ページ）

# AVC エンジンのアップデーとデフォルト アクション

AsyncOS は定期的にアップデート サーバに問い合わせて、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って、サーバをアップグレードすることなく、Web Security 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（Monitor）] です。
- 特定アプリケーション内でのファイル転送のブロックなど、新しいアプリケーション動作のデフォルト アクションは、[モニタ（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 エンジンの更新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制御の設定（15-5 ページ）を参照してください。

# 要求が AVC エンジンによりブロックされた場合のユーザ エクスペリエンス

AVC 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。

# 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。 |
| 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。ユーザには Web ページが表示されなくなり、代わりにエンド ユーザ通知ページが表示されます。 |
| モニタ（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。 |

| オプション | 説明 |
|---|---|
| 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 ユーザの帯域幅を制限できます。 |

**関連項目**

- 範囲要求の設定（15-4 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（15-5 ページ）

# 範囲要求の設定

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（4-3 ページ）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）　[範囲要求の転送（Range Request Forwarding）] がイネーブルになっていない場合、またはイネーブルになっているが、すべてのアプリケーションが [モニタ（Monitor）] に設定されている場合、[範囲要求の設定（Range Request Settings）] は読み取り専用になります。設定は、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（Do not forward range requests）]: ファイルの一部分に対する要求は転送されません。ファイル全体が返されます。<br>• [範囲要求を転送する（Forward range requests）]: 要求範囲が有効な場合は要求が転送され、ターゲット サーバから対象ファイルの要求部分のみが返されます。 |
| **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 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 サーチおよびサイト コンテンツ レーティングを有効にすると、安全に参照するために、AVC エンジンがアプリケーションを識別する役割を果たすようになります。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 エンジンの更新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、テーブルが最終アクションに基づいて並べ替えられます。たとえば、[グローバル(ブロック)を使用(Use Global (Block))] が [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制御の設定(15-5 ページ)
- 全体的帯域幅制限の設定(15-7 ページ)
- AVC アクティビティの表示(15-10 ページ)

# アクセス ポリシー グループのアプリケーション制御の設定

**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**　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。

**手順 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、以下で説明されています。

**手順 4**　ユーザ定義のアクセス 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。

**手順 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)] を使用して、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。

**手順 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。

**手順 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。

**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**

- 帯域幅の制御(15-6 ページ)

# 帯域幅の制御

全体の制限とユーザ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って、特定の URL カテゴリの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。

| Bandwidth 制限 | 説明 | リンク先 タスク |
|---|---|---|
| 全体（Overall） | 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向けの全体的制限を定義します。全体的な帯域幅制限は、Web Security Appliance と Web サーバ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。 | 全体的帯域幅制限の設定（15-7 ページ） |
| ユーザ（User） | 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に対する制限を定義します。ユーザの帯域幅制限は、Web サーバ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。 | ユーザの帯域幅制限の設定（15-7 ページ） |

（注）　帯域幅制限を定義しても、ユーザへのデータ転送が遅れるだけです。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、サーバへのリンクが減速したように見えます。

# 全体的帯域幅制限の設定

**手順 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。

**手順 2**　[設定を編集（Edit Settings）] をクリックします。

**手順 3**　[制限値（Limit to）] オプションを選択します。

**手順 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。

**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）]）。

# ユーザの帯域幅制限の設定

ユーザ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 ポリシーでは、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（15-8 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） | ユーザ定義のアクセス ポリシーでは、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無効に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（15-8 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（15-9 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 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**　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。

**手順 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。

**手順 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。

**手順 5**　[適用（Apply）] をクリックします。

**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）]）。

## 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

ユーザ定義のアクセス ポリシーでは、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無効に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 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**　ポリシー テーブルで、編集するユーザ定義ポリシー 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。

**手順 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。

**手順 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。

**手順 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。帯域幅制限を指定しない場合は、[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。

**手順 6**　[適用(Apply)] をクリックします。

**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)])。

## アプリケーションの帯域幅制御の設定

**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**　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。

**手順 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。

**手順 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。

**手順 5**　[モニタ(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。

**手順 6**　[完了(Done)] をクリックします。

**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)])。

# インスタント メッセージ トラフィックの制御

IM トラフィックのブロックやモニタを実行したり、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 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**　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。

**手順 3**　[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。

**手順 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。

**手順 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。

**手順 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。

**手順 7**　IM アプリケーションをモニタしながら、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（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。

**手順 8**　[完了（Done）] をクリックします。

**手順 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 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 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 Application Visibility and Control 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 | %XO | x-avc-app |
| アプリケーション タイプ（Application Type） | %Xu | x-avc-type |
| アプリケーション動作 | %Xb | x-avc-behavior |