レピュテーション ベースのルールによるトラフィックの制御

*アクセス コントロール ポリシー*内の *アクセス コントロール ルール*は、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。アクセス コントロール ルールのレピュテーション ベースの条件を使用することで、ネットワーク トラフィックを文脈によって解釈可能にし、必要に応じて制限することで、ネットワークを通過できるトラフィックを管理できます。アクセス コントロール ルールは、次のタイプのレピュテーション ベースの制御を管理します。

- アプリケーション条件を使用することで、*アプリケーション制御*を実行できます。これによって、個々のアプリケーションだけでなく、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいてアプリケーション トラフィックが制御されます。
- URL 条件を使用することで、*URL フィルタリング*を実行できます。これによって、個々の Web サイトだけでなく、Web サイトのシステムによって割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックが制御されます。

レピュテーション ベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純または複雑にすることができ、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（6-1 ページ）を参照してください。

セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部のデコードと前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。レピュテーション ベースのアクセス コントロールには、次のライセンスが必要です。

表 8-1　　レピュテーション ベースのアクセス コントロール ルールのライセンス要件

要件	アプリケーション管理	URL フィルタリング（cat.& rep.）	URL フィルタリング（手動）
ライセンス	Control	URL フィルタリング（URL Filtering）	任意

アクセス コントロール ルールにレピュテーション ベースの条件を追加する方法については、以下を参照してください。

- アプリケーション トラフィックの制御（8-2 ページ）
- URL のブロッキング（8-8 ページ）

ASA FirePOWER モジュールは、他のタイプのレピュテーション ベースの制御を実行できますが、アクセス コントロール ルールを使用してこれらを設定しないでください。詳細については、以下を参照してください。

- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録（5-1 ページ）では、最初の防御ラインとして、接続の発信元または宛先のレピュテーションに基づいてトラフィックを制限する方法について説明します。
- 侵入防御パフォーマンスの調整（10-6 ページ）では、マルウェアおよび他のタイプの禁止されたファイルの送信を検出、追跡、保存、分析、およびブロックする方法について説明します。

アプリケーション トラフィックの制御

ライセンス：Control

ASA FirePOWER モジュールが IP トラフィックを分析するときは、ネットワークで一般的に使用されるアプリケーションを識別および分類できます。

アプリケーション制御について

アクセス コントロール ルールのアプリケーション条件を使用することで、この *アプリケーション制御*を実行することができます。1 つのアクセス コントロール ルール内には、トラフィックを制御するアプリケーションを指定する方法がいくつかあります。

- カスタム アプリケーションなどの個々のアプリケーションを選択できます。
- システムによって提供される *アプリケーション フィルタ*を使用できます。このフィルタは、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいて編成されたアプリケーションの名前付きセットです。
- 選択したアプリケーション（カスタム アプリケーションを含む）をグループ化するカスタム アプリケーション フィルタを作成し、使用できます。

アプリケーション フィルタを使用することで、アクセス コントロール ルールに対しアプリケーション条件をすぐに作成することができます。このフィルタによって、ポリシーの作成と管理が簡素化され、システムは Web トラフィックを期待通りに確実に制御します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

また、Cisco は、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新し追加します。アプリケーションの特性に基づいたフィルタを使用することで、システムは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件の作成

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 つのアプリケーション条件において、最大 50 の項目を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[アプリケーション フィルタ（Application Filters）] リストからの 1 つ以上のフィルタ。この項目は、特性によってグループ化されたアプリケーションのセットを表します。

- [使用可能なアプリケーション（Available Applications）] リストでアプリケーションの検索を保存することで作成されるフィルタ。この項目は、部分文字列の一致によってグループ化されたアプリケーションのセットを表します。
- [使用可能なアプリケーション（Available Applications）] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

アプリケーション条件を持つ各ルールに対し、アクセス コントロール ポリシーを追加すると、システムは一意のアプリケーションのリストを生成して照合することに留意してください。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

(注)　暗号化されたトラフィックの場合、システムは [SSL プロトコル（SSL Protocol）] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないトラフィックでのみ検出できます。

詳細については、次の項を参照してください。

- トラフィックとアプリケーション フィルタの一致（8-3 ページ）
- 個々のアプリケーションからのトラフィックの照合（8-4 ページ）
- アクセス コントロール ルールへのアプリケーション条件の追加（8-6 ページ）
- アプリケーション制御の制約事項（8-7 ページ）

トラフィックとアプリケーション フィルタの一致

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[アプリケーション フィルタ（Application Filters）] リストを使用して、特性によってグループ化されたトラフィックを照合するアプリケーションのセットを作成します。

アクセス コントロール ルール内でアプリケーションをフィルタリングするメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成するメカニズムと同じです。アプリケーション フィルタの操作（2-13 ページ）を参照してください。また、オンザフライで作成した多数のフィルタを、アクセス コントロール ルールに新規の再利用可能なフィルタとして保存できます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[使用可能なアプリケーション（Available Applications）] リストが更新され、条件を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium フィルタに 110 個のアプリケーション、High フィルタに 82 個のアプリケーションが含まれる場合、システムはこれら 192 個のアプリケーションすべてを [使用可能なアプリケーション（Available Applications）] リストに表示します。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

この場合、システムは [中（Medium）] または [高（High）] の [リスク（Risk）] タイプと [中（Medium）] または [高（High）] の [ビジネスとの関連性（Business Relevance）] タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。また、システムによって提供されるフィルタ タイプ（[リスク（Risks）]、[ビジネスとの関連性（Business Relevance）]、[タイプ（Types）]、[カテゴリ（Categories）]、または [タグ（Tags）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択します。

フィルタを検索するには、[使用可能なフィルタ（Available Filters）] リストの上にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[使用可能なアプリケーション（Available Applications）] リストを使用してそのフィルタをルールに追加し、個々のアプリケーションからのトラフィックの照合（8-4 ページ）の手順に従います。

個々のアプリケーションからのトラフィックの照合

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[使用可能なアプリケーション（Available Applications）] リストを使用して、トラフィックを照合するアプリケーションを作成します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

照合するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[使用可能なアプリケーション（Available Applications）] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [名前で検索（Search by name）] プロンプトをクリックし、名前を入力します。入力すると、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[アプリケーション フィルタ（Application Filters）] リストを使用します（トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照）。フィルタを適用すると、[使用可能なアプリケーション（Available Applications）] リストが更新されます。

制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストにすべて一度に追加できます。

（注）　[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、しかも [使用可能なアプリケーション（Available Applications）] リストを検索した場合、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使って結合されます。つまり [フィルタに一致するすべてのアプリケーション（All apps matching the filter）] 条件には、[使用可能なアプリケーション（Available Applications）] リストに現在表示されている個々のすべての条件と、[使用可能なアプリケーション（Available Applications）] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用するか、または現在制約されているビュー内のすべてのアプリケーションを選択するには右クリックして [すべて選択（Select All）] を選択します。

単一のアプリケーション条件では、それらを個別に選択することで、最大 50 のアプリケーションを照合できます。50 を超えるアプリケーションを追加するには、複数のアクセス コントロール ルールを作成するか、またはフィルタを使用してアプリケーションをグループ化します。

条件のフィルタに一致するすべてのアプリケーションの選択

[アプリケーション フィルタ（Application Filters）] リストで検索またはフィルタを使用して制約されると、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] オプションが [使用可能なアプリケーション（Available Applications）] リストの上部に表示されます。

このオプションを使用して、制約された [使用可能なアプリケーション（Available Applications）] リスト内のアプリケーションのセット全体を [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに同時に追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

このようにアプリケーション条件を作成するときは、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加するフィルタの名前は、フィルタに表されているフィルタ タイプ + 各タイプの最大 3 つのフィルタの名前を連結させたものとなります。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks（リスク）タイプの 2 つのフィルタと Business Relevance（ビジネスとの関連性）タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。これらのフィルタ タイプは *any* に設定されています。つまり、これらのフィルタ タイプはフィルタを制約しないので、任意の値が許可されます。

[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

アクセス コントロール ルールへのアプリケーション条件の追加

ライセンス：Control

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 条件ごとに最大 50 の項目を追加でき、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。アプリケーション条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

アプリケーション トラフィックを制御するには、次の手順を実行します。

ステップ 1　アプリケーション別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[アプリケーション（Applications）] タブを選択します。

[アプリケーション（Applications）] タブが表示されます。

ステップ 3　オプションで、フィルタを使用して [使用可能なアプリケーション（Available Applications）] リストに表示されるアプリケーションのリストを制約します。

[アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択します。詳細については、トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照してください。

ステップ 4　[使用可能なアプリケーション（Available Applications）] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択するか、またはリストが制約されている場合は、[フィルタに一致するすべてのアプリケーション（All apps matching the filter）] を選択できます。詳細については、個々のアプリケーションからのトラフィックの照合（8-4 ページ）を参照してください。

ステップ 5　[ルールに追加（Add to Rule）] をクリックして、選択したアプリケーションを [選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加します。

選択したアプリケーションとフィルタをドラッグ アンド ドロップすることもできます。フィルタは [フィルタ（Filters）] という見出しの下に表示され、アプリケーションは [アプリケーション（Applications）] という見出しの下に表示されます。

ヒント　このアプリケーション条件に別のフィルタを追加する前に、[すべてのフィルタをクリア（Clear All Filters）] をクリックして既存の選択内容をクリアします。

ステップ 6　必要に応じて、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストの上にある追加アイコン（  ）をクリックすると、リストに現在含まれている個々のすべてのアプリケーションおよびフィルタからなるカスタム フィルタを保存できます。

このオンザフライで作成されたフィルタを管理するには、オブジェクト マネージャを使用します。アプリケーション フィルタの操作（2-13 ページ）を参照してください。別のユーザが作成したフィルタを含むフィルタは保存できないことに注意してください。ユーザが作成したフィルタはネストできません。

ステップ 7　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

アプリケーション制御の制約事項

ライセンス：Control

アプリケーション制御を実行する際は、次の点に注意してください。

アプリケーション識別の速度

システムは、以下の動作の前にアプリケーション制御を実行することはできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションでアプリケーションを識別する前

この識別は 3 ～ 5 パケット以内で行う必要があります。これらの最初のパケットの 1 つがアプリケーション条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、アプリケーションの識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（  ）でマークされます。

許可されたパケットは、アクセス コントロール ポリシーの*デフォルトの*侵入ポリシー（*デフォルト アクション*侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをそのアプリケーション条件に一致する残りのセッション トラフィックに適用します。

暗号化されたトラフィックの処理

システムは、SMTPS、POP、FTPS、TelnetS および IMAPS など StartTLS を使用して、暗号化される前のアプリケーション トラフィックを識別し、フィルタリングできます。また、TLS クライアントの hello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

これらのアプリケーションは、[SSL プロトコル（SSL Protocol）] とタグ付けされています。このタグがないアプリケーションは、暗号化されていないトラフィックでのみ検出できます。

ペイロードのないアプリケーション トラフィック パケットの処理

システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるトラフィックの処理

Web サーバによって参照されるトラフィック（たとえばアドバタイズメント トラフィック）を処理するルールを作成するには、参照元アプリケーションではなく、参照されるアプリケーションに関する条件を追加します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

システムは、Skype の複数のタイプの アプリケーション トラフィックを検出できます。Skype のトラフィックを制御するためのアプリケーション条件を作成する場合は、個々のアプリケーションを選択するのではなく、[アプリケーション フィルタ（Application Filters）] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。詳細については、トラフィックとアプリケーション フィルタの一致（8-3 ページ）を参照してください。

URL のブロッキング

ライセンス：機能によって異なる

アクセス コントロール ルールの URL 条件を使用することで、ネットワーク上のユーザがアクセスできる Web サイトを制限することができます。この機能は、*URL フィルタリング*と呼ばれます。アクセス コントロールを使用してブロックする（または逆に許可する）URL を指定するには 2 つの方法があります。

- 各ライセンスを使用して、個々の URL または URL のグループを手動で指定することで、Web トラフィックへのきめ細かなカスタム コントロールを実現できます。
- URL フィルタリング（URL Filtering）ライセンスを使用して、URL の一般的な分類、または*カテゴリ*、およびリスク レベル、または*レピュテーション*に基づいて、Web サイトへのアクセスを制御することもできます。システムは接続ログ、侵入イベント、およびアプリケーションの詳細にこのカテゴリとレピュテーション データを表示します。

（注）　イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのアクセス コントロール ルールを作成する必要があります。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム ページを表示できます。また、警告ページをクリック スルーすることで Web サイトのブロックをバイパスする機会をユーザに与えることができます。

メモリ リソースの制約により、ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X、および 71xx ファミリ デバイスは、他のモデル（ASA5545-X、ASA5555-X、ASA5585-X など）で使用されるデータベースよりも小規模な URL カテゴリ データベースを使用します。

この小規模なデータベースには、よく参照されるドメインのサブドメインでよく参照されるエントリは含まれません。たとえば、mail.google.com はこの小規模データベースには含まれず、その結果、mail.google.com は Web ベースのメールとしてではなく、検索エンジンとして分類されます。

表 8-2　URL フィルタリングのライセンス要件

要件	カテゴリおよびレピュテーション ベース	手動
ライセンス	URL フィルタリング（URL Filtering）	任意

詳細については、以下を参照してください。

- レピュテーション ベースの URL ブロッキングの実行（8-9 ページ）
- 手動による URL ブロッキングの実行（8-11 ページ）
- URL の検出とブロッキングの制約事項（8-13 ページ）
- ユーザが URL ブロックをバイパスすることを許可する（8-13 ページ）
- ブロックされた URL のカスタム Web ページの表示（8-15 ページ）

レピュテーション ベースの URL ブロッキングの実行

ライセンス:URL フィルタリング（URL Filtering）

URL フィルタリング（URL Filtering）ライセンスを使用して、ASA FirePOWER モジュールが Cisco クラウドから取得する要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザのアクセスを制御できます。

- URL *カテゴリ*とは、URL の一般的な分類です。たとえば ebay.com は [オークション（Auctions）] カテゴリ、monster.com は [求職（Job Search）] カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。
- URL *レピュテーション*は、組織のセキュリティ ポリシーに反する目的でその URL が使用される可能性を表します。各 URL のリスクは、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）の範囲にまたがるものとなる可能性があります。

（注） カテゴリおよびレピュテーション ベースの URL 条件を持つアクセス コントロール ルールを有効にする前に、Cisco クラウドとの通信を有効にする**必要があります**。これにより、ASA FirePOWER モジュールは URL データを取得できるようになります。詳細については、クラウド通信の有効化（41-2 ページ）を参照してください。

レピュテーション ベースの URL ブロッキングの利点

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成することができます。たとえば、[乱用薬物（Abused Drugs）] カテゴリ内の**高リスク** URL をすべて識別してブロックするアクセス コントロール ルールを作成できます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

Cisco クラウドからカテゴリ データおよびレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを期待通りに確実に制御します。最後に、クラウドは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタします。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを適用したりするペースを上回って次々と現れては消える可能性があります。

次に例をいくつか示します。

- ルールですべてのゲーム サイトをブロックする場合、新しいドメインが登録されて [ゲーム（Gaming）] に分類されると、これらのサイトをシステムで自動的にブロックできます。
- ルールがすべてのマルウェア サイトをブロックし、あるブログ ページがマルウェアに感染すると、クラウドはその URL を [ブログ（Blog）] から [マルウェア（Malware）] に再分類でき、システムはそのサイトをブロックできます。
- ルールがリスクの高いソーシャル ネットワーキング サイトをブロックし、だれかがプロファイル ページに悪意のあるペイロードへのリンクが含まれるリンクを掲載すると、クラウドはそのページのレピュテーションを [無害なサイト（Benign sites）] から [高リスク（High Risk）] に変更でき、システムでそれをブロックできます。

URL のカテゴリやレピュテーションがクラウドで不明な場合、または ASA FirePOWER モジュールがクラウドと通信できない場合は、カテゴリやレピュテーションに基づく URL 条件を含むアクセス コントロール ルールがその URL によってトリガー**されない**ことに注意してください。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

URL 条件の作成

1 つの URL 条件で、照合する最大 50 の項目を [選択済み URL（Selected URLs）] に追加できます。任意でレピュテーションによって制限された各 URL カテゴリは、1 つの項目としてカウントされます。URL 条件でリテラル URL および URL オブジェクトを使用することもできますが、これ

らの項目はレピュテーションで制限できないことに注意してください。詳細については、手動による URL ブロッキングの実行（8-11 ページ）を参照してください。

レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された URL によるトラフィックの制御

ステップ 1　URL 別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[URL（URLs）] タブを選択します。

[URL（URLs）] タブが表示されます。

ステップ 3　[カテゴリおよび URL（Categories and URLs）] リストから追加する URL のカテゴリを見つけて選択します。カテゴリに関係なく Web トラフィックを照合するには、[任意（Any）] カテゴリを選択します。

追加するカテゴリを検索するには、[カテゴリおよび URL（Categories and URLs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、カテゴリ名を入力します。入力すると、リストが更新されて一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント　右クリックして**すべてのカテゴリを選択**できますが、このようにすべてのカテゴリを追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。代わりに [任意（Any）] を使用してください。

ステップ 4　オプションで、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。レピュテーション レベルを指定しない場合、システムはデフォルトとして [任意（Any）]（つまりすべてのレベル）を設定します。

選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを選択すると、アクセス コントロール ルールはその目的に応じて異なる動作をします。

- ルールによって Web アクセスをブロックまたはモニタする場合（ルール アクションが [ブロック（Block）]、[リセットしてブロック（Block with reset）]、[インタラクティブ ブロック（Interactive Block）]、[リセットしてインタラクティブ ブロック（Interactive Block with reset）]、または [モニタ（Monitor）]）、レピュテーション レベルを選択すると、そのレベルよりも厳しいレピュテーションもすべて選択されます。たとえば**疑わしいサイト**（レベル 2）をブロックまたはモニタするようルールを設定した場合、**高リスク**（レベル 1）のサイトも自動的にブロックまたはモニタされます。
- ルールによって Web アクセスがそれを信頼またはさらに検査するかどうかを許可する場合（ルール アクションが [許可（Allow）] または [信頼する（Trust）]）、レピュテーション レベルを選択すると、そのレベルよりも厳しさが弱いレピュテーションもすべて選択されます。たとえば**無害なサイト（Benign sites）**（レベル 4）を許可するようルールを設定した場合、**有名（Well known）**（レベル 5）サイトもまた自動的に許可されます。

ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

ステップ 5　[ルールに追加（Add to Rule）] をクリックするか、または選択した項目をドラッグ アンド ドロップして、[選択済み URL（Selected URLs）] リストに追加します。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

手動による URL ブロッキングの実行

ライセンス：任意

カテゴリおよびレピュテーションで URL フィルタリングを補完するか、または選択的に上書きするには、手動で個々の URL または URL のグループを指定することで、Web トラフィックを制御できます。これにより、許可またはブロックされた Web トラフィックに対するきめ細かなカスタム制御を行うことができます。特殊なライセンスなしでこのタイプの URL フィルタリングを実行することもできます。

アクセス コントロール ルールに許可またはブロックする URL を手動で指定するには、単一のリテラル URL を入力できます。または、再利用可能で名前を URL または IP アドレスに関連付ける URL オブジェクトを使用して URL 条件を設定できます。

ヒント　URL オブジェクトを作成した後、それを使用して、アクセス コントロール ルールを作成するだけでなく、システムのモジュール インターフェイスの他のさまざまな場所で URL を表すことができます。これらのオブジェクトはオブジェクト マネージャを使用して作成できます。また、アクセス コントロール ルールの設定時に URL オブジェクトをオンザフライで作成することもできます。詳細については、URL オブジェクトの操作（2-12 ページ）を参照してください。

URL 条件で URL を手動で指定する

手動で入力することで、許可またはブロックされる Web トラフィックに対する正確な制御が実現できますが、手動で指定した URL をレピュテーションで制限することはできません。また、ルールに予期しない結果がないことを確認する必要があります。ネットワーク トラフィックが URL 条件に一致するかどうか判別するために、システムは単純な部分文字列マッチングを実行します。URL オブジェクトまたは手動で入力した URL の値が、モニタ対象ホストから要求された URL の一部に一致する場合、アクセス コントロール ルールの URL 条件が満たされます。

したがって、URL 条件（URL オブジェクトを含む）に URL を手動で指定する場合は、影響を受ける可能性がある他のトラフィックを慎重に考慮する必要があります。たとえば example.com へのすべてのトラフィックを許可する場合、ユーザは次の URL を含むサイトを参照できます。

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

別の例として、ign.com（ゲーム サイト）を明示的にブロックする場合を考えてください。部分文字列マッチングにより *ign.com* 自体だけでなく veri*sign.com* もブロックされることになり、意図しない動作が生じる可能性があります。

暗号化された Web トラフィックの手動ブロッキング

アクセス コントロール ルールの URL 条件は以下を行います。

- Web トラフィック（HTTP または HTTPS）の暗号化プロトコルを無視します。

たとえば、アクセス コントロール ルールは、http://example.com/ へのトラフィックを https://example.com/ へのトラフィックと同じものとして処理します。HTTP または HTTPS トラフィックのみに一致するアクセス コントロール ルールを設定するには、アプリケーション条件をルールに追加します。詳細については、URL のブロッキング（8-8 ページ）を参照してください。

- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、また、サブジェクト共通名に含まれるサブドメインを無視します。

  手動で HTTPS トラフィックをフィルタリングする場合は、サブドメイン情報を含めないでください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーおよびルールのトラブルシューティング（4-13 ページ）を参照してください。

許可またはブロックする URL を手動で指定して Web トラフィックを制御するには、次の手順を実行します。

ステップ 1　URL 別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（6-2 ページ）を参照してください。

ステップ 2　ルール エディタで、[URL（URLs）] タブを選択します。

[URL（URLs）] タブが表示されます。

ステップ 3　[カテゴリおよび URL（Categories and URLs）] リストから追加する URL オブジェクトおよびグループを見つけて選択します。

- URL オブジェクトをオンザフライで追加するには（後で条件に追加できます）、[カテゴリおよび URL（Categories and URLs）] リストの上にある追加アイコン（  ）をクリックします。URL オブジェクトの操作（2-12 ページ）を参照してください。
- 追加する URL オブジェクトおよびグループを検索するには、[カテゴリおよび URL（Categories and URLs）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクト内の URL または IP アドレスの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用します。右クリックして**すべての URL オブジェクトおよびカテゴリを選択**できますが、このように URL を追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。

ステップ 4　[ルールに追加（Add to Rule）] をクリックするか、または選択した項目を [選択済み URL（Selected URLs）] リストに追加します。

選択した項目をドラッグ アンド ドロップすることもできます。

ステップ 5　手動で指定するリテラル URL を追加します。このフィールドでは、ワイルドカード（*）は使用**できません**。

[選択済み URL（Selected URLs）] リストの下にある [URL の入力（Enter URL）] プロンプトをクリックし、URL または IP アドレスを入力して、[追加（Add）] をクリックします。

ステップ 6　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。設定変更の展開（4-12 ページ）を参照してください。

URL の検出とブロッキングの制約事項

ライセンス：任意

URL の検出とブロッキングを実行する際は、次の点に注意してください。

URL 識別の速度

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションで HTTP または HTTPS アプリケーションを識別する前
- システムが要求された URL を識別する前（クライアントの hello メッセージまたはサーバ証明書から暗号化されたセッションの場合）

この識別は 3 ～ 5 パケット以内で行う必要があります。これらの最初のパケットの 1 つが URL 条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、URL の識別が可能になります。便宜を図るため、影響を受けるルールは情報アイコン（  ）でマークされます。

許可されたパケットは、アクセス コントロール ポリシーの*デフォルトの*侵入ポリシー（*デフォルト アクション*侵入ポリシーでもほぼ一致するルールの侵入ポリシーでもない）により検査されます。詳細については、アクセス コントロールのデフォルト侵入ポリシーの設定（17-1 ページ）を参照してください。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをその URL 条件に一致する残りのセッション トラフィックに適用します。

暗号化された Web トラフィックの処理

URL 条件を持つアクセス コントロール ルールを使用して暗号化された Web トラフィックを評価する際、システムは以下を行います。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件はない場合、アクセス コントロール ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用する公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- （設定した場合でも）HTTP 応答ページを表示しません。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

ユーザが URL ブロックをバイパスすることを許可する

ライセンス：任意

アクセス コントロール ルールを使用してユーザの HTTP Web 要求をブロックする場合は、ルール アクションを [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] に設定することで、ユーザは警告 *HTTP 応答*ページをクリック スルーすることによりブロックをバイパスできます。システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間ブロックをバイパスすることができます。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。

ユーザがブロックをバイパスしない場合、一致したトラフィックは追加のインスペクションなしで拒否されます。また、接続をリセットすることもできます。一方、ユーザがブロックをバイパスすると、システムによってトラフィックが許可されます。このトラフィックを許可するということは、侵入、マルウェアおよび禁止されているファイルの有無について暗号化されていないペイロードを引き続き検査できることを意味します。ブロックをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があることに注意してください。

インタラクティブ HTTP 応答ページは、ブロック ルールに設定する応答ページとは別に設定することに注意してください。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。詳細については、ブロックされた URL のカスタム Web ページの表示（8-15 ページ）を参照してください。

ヒント　アクセス コントロール ポリシーのすべてのルールに対してインタラクティブ ブロッキングを素早く無効にするには、システムによって提供されるページもカスタム ページも表示しないでください。これにより、システムはインタラクションなしでインタラクティブ ブロック ルールに一致するすべての接続をブロックします。

ユーザに Web サイト ブロックをバイパスするように許可するには、次の手順を実行します。

ステップ 1　URL 条件を持つ Web トラフィックに一致するアクセス コントロール ルールを作成します。

レピュテーション ベースの URL ブロッキングの実行（8-9 ページ）および手動による URL ブロッキングの実行（8-11 ページ）を参照してください。

ステップ 2　アクセス コントロール ルール アクションが [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] であることを確認します。

ルール アクションを使用したトラフィックの処理とインスペクションの決定（6-7 ページ）を参照してください。

ステップ 3　ユーザがブロックをバイパスし、ルールに対してインスペクションおよびロギング オプションを必要に応じて選択すると仮定します。許可ルールと同様に次のようになります。

- いずれかのタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付けることができます。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（10-1 ページ）を参照してください。
- インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブ ブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけであることに注意してください。

  システムが最初にユーザに警告すると、ロギングされた接続開始イベントを [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] アクションでマークすることに留意してください。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに許可アクションが付きます。詳細については、アクセス コントロールの処理に基づく接続のロギング（33-10 ページ）を参照してください。

ステップ 4　オプションで、システムが警告ページを再表示する前にユーザがブロックをバイパスしてから経過する時間を設定します。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定（8-15 ページ）を参照してください。

ステップ 5　オプションで、ユーザにブロックをバイパスすることを許可するために表示するカスタム ページを作成し、使用します。

ブロックされた URL のカスタム Web ページの表示（8-15 ページ）を参照してください。

ブロックされた Web サイトのユーザ バイパス タイムアウトの設定

ライセンス：任意

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間インタラクティブ ブロックをバイパスすることができます。期間を 1 年に設定したり、ゼロに設定してユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

ユーザ バイパスの期限が切れるまでの時間の長さをカスタマイズするには、次の手順を実行します。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [アクセス コントロール ポリシー（Access Control Policy）] の順に選択します。

[アクセス コントロール ポリシー（Access Control Policy）] ページが表示されます。

ステップ 2　設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3　[詳細設定（Advanced）] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4　[全般設定（General Settings）] の横にある編集アイコン（）をクリックします。

[全般設定（General Settings）] ポップアップ ウィンドウが表示されます。

ステップ 5　[ブロックをバイパスするためのインタラクティブ ブロックを許可する期間（秒）（Allow an Interactive Block to bypass blocking for (seconds)）] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。

0 ～ 31536000（1 年）の間の任意の数を指定できます。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 6　[OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、設定変更の展開（4-12 ページ）を参照してください。

ブロックされた URL のカスタム Web ページの表示

ライセンス：任意

システムによってユーザの HTTP Web 要求がブロックされたときに、ユーザのブラウザに表示される内容は、アクセス コントロール ルールのアクションを使用して、セッションをどのようにブロックするかによって異なります。次から選択できます。

- 接続を拒否するには、[ブロック（Block）] または [リセットしてブロック（Block with reset）]。ブロックされたセッションがタイム アウトすると、システムは [リセットしてブロック（Block with reset）] の接続をリセットします。ただし、いずれのブロック アクションの場合でも、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドすることができます。システムではこのカスタム ページを *HTTP 応答*ページと呼んでいます。
- ユーザに警告する*インタラクティブ HTTP 応答*ページを表示する一方、ユーザがボタンをクリックすることで、処理を続行あるいはページを更新して、要求された元のサイトをロードできるようにする場合は、[インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）]。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。カスタム テキストを入力する際には、使用した文字数がカウンタで示されます。

各アクセス コントロール ポリシーで、インタラクティブ HTTP 応答ページは、インタラクションなしで、つまりブロック ルールを使用してトラフィックをブロックするために使用する応答ページとは別に設定します。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザに対しては、カスタム ページを表示できます。

HTTP 応答ページをユーザに確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。カスタム応答ページを作成する場合は、より小さいページが正常に表示されやすいことに留意してください。

HTTP 応答ページの設定方法：

ステップ 1　Web トラフィックをモニタするアクセス コントロール ポリシーを編集します。

詳細については、アクセス コントロール ポリシーの編集（4-8 ページ）を参照してください。

ステップ 2　[HTTP 応答（HTTP Responses）] タブを選択します。

アクセス コントロール ポリシーの HTTP 応答ページ設定が表示されます。

ステップ 3　[ブロック レスポンス ページ（Block Response Page）] および [インタラクティブ ブロック レスポンス ページ（Interactive Block Response Page）] の場合、ドロップダウンリストから応答を選択します。各ページには、次の選択肢があります。

- 汎用の応答を使用する場合は、[システムによる提供（System-provided）] を選択します。表示アイコン（  ）をクリックすると、このページの HTML コードが表示されます。
- カスタム応答を作成する場合は、[カスタム（Custom）] を選択します。

  ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコン（  ）をクリックすると編集できます。
- システムに HTTP 応答ページを表示させない場合は、[なし（None）] を選択します。インタラクティブにブロックされるセッションに対してこのオプションを選択すると、ユーザはクリックして続行することができなくなります。セッションはインタラクションなしでブロックされます。

ステップ 4　[ASA FirePOWER の変更の保存（Store ASA FirePOWER Changes）] をクリックします。

変更を反映するには、アクセス コントロール ポリシーを適用する必要があります。詳細については、設定変更の展開（4-12 ページ）を参照してください。