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 ルールは単純にも複雑にも設定でき、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 を参照してください。

（注） 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、および一部の復号化と前処理は、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。また、*SSL* インスペクション機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号化することができます。

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 *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	いずれか（Any）

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 ルールを使用してそれらを設定しないでください。詳細については、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トラフィックのブロックを参照してください。ここでは、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されています。侵入防御パフォーマンスの調整では、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されています。

• アプリケーション トラフィックの制御 （2 ページ）
• URL のブロッキング （9 ページ）

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 モジュールは、IP トラフィックを分析する際に、ネットワークで一般的に使用されているアプリケーションを識別および分類することができます。

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。
- システム提供のアプリケーション 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 トラフィックを想定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、 シスコでは、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および追加しています。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、システムが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することが保証されます。

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 [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 [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、[Application Filters] リストからの 1 つ以上のフィルタ。この項目は、特性を基準にグループ化されたアプリケーションのセットです。
- [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、アプリケーション名の一部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です。
- [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 ポリシーを展開すると、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 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または復号化されたトラフィックでのみ検出できます。

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、[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 を参照してください。また、アクセス コントロール ルールの設定時に作成する各種のフィルタを、新規のフィルタとして保

存して再利用することもできます。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、[Available Applications] リストが更新され、基準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 [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 タイプで Medium および High フィルタを選択し、Business Relevance（業務との関連性）タイプで Medium および High 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 HighANDBusiness Relevance: Medium OR High
```

この場合、システムは Medium または High Risk タイプと Medium または High 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。システム提供のフィルタ タイプ（[Risks]、[BusinessRelevance]、[Types]、[Categories]、または[Tags]）を右クリックして、[CheckAll] または [Uncheck All] を選択することもできます。

フィルタを検索するには、[Available Filters] リストの上にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、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、[Available Applications] リストを使用してそのフィルタをルールに追加します。個々のアプリケーションからのトラフィックの照合 （4 ページ） を参照してください。

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、[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順次確認するには、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概要情報と参照可能なインターネット検索リンクを含む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。

一致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、[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 [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、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、[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 （3 ページ） を参照）。フィルタを適用すると、[Available Applications] リストが更新されます。

制約されると、[All apps matching the filter] オプションが [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 [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、さらに [使用可能なアプリケーション（Available Applications）] リストも検索すると、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 演算を使用して結合されます。つまり [All apps matching the filter] 条件には、[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、[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 キーまたは Ctrl キーを使用します。表示されている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 [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

[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、[All apps matching the filter] オプションが [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すると、制限した [Available Applications] リストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。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。

この方法でアプリケーション条件を作成すると、[Selected Applications and Filters] リストに追加したフィルタに「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」形式の名前が付きます。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 タイプの 2 つのフィルタと Business Relevance 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,...
```

[All apps matching the filter] で追加したフィルタでは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。それらのファイル タイプは [any] に設定されます。つまり、それらのフィルタ タイプはフィルタを制約せず、任意の値を使用できるということです。

[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 [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 [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 つの条件に最大 50 の項目を追加することができ、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。無効なアプリケーション条件が検出されると、警告アイコンが表示されます。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング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を参照してください。

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

ステップ 3 必要に応じて、セーフサーチ（）または YouTube EDU（）の淡色表示アイコンをクリックし、関連オプションを設定して、コンテンツ制限機能を有効にします。追加の設定要件については、アクセス コントロール ルールを使用したコンテンツ制限の実施を参照してください。

たいていの場合、コンテンツ制限を有効にすると、条件の [Selected Applications and Filters] リストに適切な値が入力されます。コンテンツ制限を有効にするときに、コンテンツ制限に関係するアプリケーションまたはフィルタがすでにリスト内に存在している場合には、システムはリストに自動的に値を入力することはしません。

アプリケーションを絞り込んで選択内容をフィルタする手順を続行するか、またはスキップしてルールの保存に進みます。

ステップ 4 オプションで、フィルタを使用して [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。

[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 （3 ページ）を参照してください。

ステップ 5 [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したり、リストの表示を制限した場合は [All apps matching the filter] をクリックしてすべてを選択したりできます。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 （4 ページ）を参照してください。

ステップ 6 [Add to Rule] をクリックして、選択したアプリケーションを [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 [Filters] という見出しの下に表示され、アプリケーションは [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場合は、[Clear All Filters] をクリックして既存の選択をクリアしておきます。

ステップ 7 必要に応じて、[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すべての個々のアプリケーションとフィルタから成るカスタム フィルタを保存できます。

臨機応変に作成されたこの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 8 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 ポリシーを展開する必要があります（設定変更の導入を参照してください）。

アプリケーション制御の制限

ライセンス：Control

アプリケーション制御を実行する場合は、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、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。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、こうしてアプリケーションの識別が可能になります。便宜上、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。

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、暗号化されるようになる暗号化されていないアプリケーション 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 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または復号された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、[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 （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：機能に応じて異なる

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 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。

表 *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	いずれか（Any）

URL カテゴリとレピュテーションに基づく URL のブロッキング

ライセンス：URL Filtering

URL Filtering を使用して、ASA FirePOWER モジュールが Cisco Cloud 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 [Auctions] カテゴリ、monster.com は [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 カテゴリの説明は https://www.talosintelligence.com/categories を参照してください。

  すべてのカテゴリを表示するには、[Threat Categories] タブをクリックしてください。

- URL レピュテーションは、URL が悪意のあるものである可能性を表します。URL のリスクは、**[Untrusted]**（レベル 1）から **[Trusted]**（レベル 5）まであります。

  URL レピュテーションのレベルの説明は、https://talosintelligence.com/reputation_center/support を参照してください。[Common Questions] セクションを確認します。

（注） カテゴリとレピュテーションベースの URL 条件を持つアクセス制御ルールを有効にする前に、URL フィルタリングライセンスを追加し、Cisco Cloud との通信を有効にする必要があります。これで、ASA FirePOWER モジュールが URL データを取得できるようになります。詳細については、「URL フィルタリングとマルウェア検出のクラウドコミュニケーションのオプション」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、**[Illegal Drugs]** カテゴリの **[Untrusted]** のすべての URL を識別し、ブロックするアクセス制御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 Cloud のカテゴリ データとレピュテーション 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 トラフィックを想定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 をフィルタ処理できます。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展開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。

- すべてのギャンブルサイトをルールでブロックする場合は、新しいドメインが登録されて [Gambling] に分類されると、それらのサイトはシステムで自動的にブロックされます。
- ルールですべてのマルウェアサイトをブロックしており、あるブログのページがマルウェアに感染した場合、クラウドは **[Online Communities]** の URL を [Malware] に分類し、そのサイトをシステムでブロックできます。

- ルールで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、ある参加者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を含む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 **[Favorable]** から **[Untrusted]** に変更でき、システムはそのページをブロックできます。

なお、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、カテゴリまたはレピュテーションベースの URL 条件を含むアクセス コントロール ルールが 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 にカテゴリやレピュテーションを手動で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 [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 （13 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 ポリシーとルールのトラブルシューティング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 Cisco Cloud から URL カテゴリとレピュテーションデータを取得するようにアプライアンスを設定します。

クラウド通信の有効化を参照してください。

ステップ 2 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を参照してください。

ステップ 3 ルール エディタで、[URLs] タブを選択します。

[URLs] タブが表示されます。

ステップ 4 [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、[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、[Categories and URLs] リストの上にある [Search by name or value] プロンプトをクリックして、カテゴリ名を入力します。入力を開始するとリストが更新され、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することもできますが、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 [Any] を使用してください。

ルールの目的がマルウェアからの保護である場合は、https://www.talosintelligence.com/categoriesの説明に従ってすべての脅威カテゴリを選択してください。

カテゴリのページが複数存在する場合があります。カテゴリリストの下にある矢印をクリックして、すべてのページにアクセスしていることを確認します。

ステップ 5　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かった場合、システムはデフォルトで [Any]（レピュテーションが未知のサイトを含むすべてのレベル）に設定します。

必要に応じて、[不明なレピュテーションに適用（Apply to unknown reputation）] をオンにします。

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 [Block]、[Block with reset]、[Interactive Block]、[Interactive Block with reset]、または [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、[Questionable sites]（レベル 2）をブロックまたはモニタするルールを設定した場合、**[Untrusted]**（レベル 1）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 [Allow] または [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、[Favorable] サイト（レベル 4）を許可するルールを設定した場合、**[Trusted]**（レベル 5）サイトも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 6　[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、[Selected URLs] リストに追加します。

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 ポリシーを展開する必要があります（設定変更の導入を参照してください）。

URL カテゴリを変更する場合

URL フィルタリング カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせてときどき変更されます。

これらの変更は、ポリシーとイベントに関連するアクティビティの両方に影響します。

このトピックの説明どおりに設定された URL カテゴリへの更新は、新しい URL を単純に追加したり、誤って分類された URL を再マッピングする変更とは異なります。このトピックは個々の URL のカテゴリ変更には適用されません。

イベントへの影響

トラフィックが検出された時点で一致した URL カテゴリがすべてのイベントにあります。レガシーカテゴリはそのようにラベル付けされます。時間が経過するとともに、レガシーカテゴリを持つイベントはシステムからエージアウトします。

処理された時点で URL にレピュテーションがない場合は、イベント ビューア内の URL レピュテーションは空になります。

手動による URL ブロッキングの実行

URL を手動で指定してブロックし、カテゴリとレピュテーションによって URL のフィルタリングを補完または選択的に上書きすることができます。

また、この手順を例として使用して、設定によってブロックされる URL へのトラフィックを手動で許可することもできます。

手動で URL のフィルタリングを実行する方法はいくつかあります。指定した URL 文字列が URL 内の何らかの部分に一致する場合は、ほとんどのメソッドが一致します。これは、たとえば、これらのメソッドを使用して「cisco.com」へのトラフィックを許可する場合は URL の任意の部分に「cisco.com」がある他のドメインへのトラフィックを誤って許可する可能性があることを意味します。

そのため、この手順では、この目的でドメインに一致する URL をアンカーするセキュリティ インテリジェンス リストを使用する手順を示します。

暗号化された Web トラフィックの手動ブロッキングに関する注意事項

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 （9 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された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 ポリシーとルールのトラブルシューティングを参照してください。

ステップ 1 ブロックする URL を含むカスタム セキュリティ インテリジェンス リストを作成して追加します。

a) ファイル名拡張子が .txt の新しいテキストファイルを作成します。

ファイル名に「Block」と「URL」を含めることをお勧めします。

b) 各行で、1 つまたは複数の URL をファイルに追加します。

リストの詳細な要件とガイドラインについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html から入手可能な『Firepower Management Center Configuration Guide for version 6.6』の「Custom Security Intelligence Lists」のトピックを参照してください。

ステップ 2 カスタム セキュリティ インテリジェンス リストとしてテキストファイルを追加します。

a) [Object Management] > [Security Intelligence] > [URL Lists and Feeds] に移動します。

b) カスタム セキュリティ インテリジェンスのリストの操作の手順に従ってリストを追加します。

ステップ 3 アクセス コントロール ポリシーで、ブロックアクションを指定したルール内に新しいリストを指定します。

a) アクセスコントロールルールで、[URLs] タブをクリックします。

b) [URLs] タブで、[URLs] サブタブをクリックします。

c) 上で作成した新しいカスタム セキュリティ インテリジェンス リストを選択します。

d) [Add to Rule] をクリックします。

e) [追加（Add）] をクリックします。

ステップ 4 ポリシーを保存します。

次のタスク

- （任意）この手順を例として使用して、手動で許可する URL トラフィックのカスタム セキュリティ インテリジェンス リストを作成します。

  たとえば、組織に適していない Web サイトのカテゴリをブロックする一方で、アクセスできるようにする必要がある Web サイトがそのカテゴリに含まれている場合に、このようなリストを使用できます。

  このリストでは、ファイル名に「Allow」と「URL」を使用することをお勧めします。許可アクションを使用してアクセスコントロールルールにリストを追加します。リスト上の URL をブロックするルールの上にルールを配置します。

- 変更を展開します。

- カスタム セキュリティ インテリジェンス リストに URL を追加するには、セキュリティ インテリジェンス リストの更新を参照してください。

URL の検出とブロッキングのガイドラインと制限事項

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。

脅威カテゴリ

ポリシーが既知の悪意のあるサイトを識別する脅威カテゴリに明確に対応していることを確認してください。

詳細については、URL カテゴリとレピュテーションに基づく URL のブロッキング （9 ページ）の URL にある [脅威カテゴリ（Threat Categories）] タブを参照してください。

一部のパケットは URL の識別前に通過することが必要

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、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。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、こうして URL の識別が可能になります。便宜上、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。**重要**この侵入ポリシーが設定されていることを確認します。

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。

未分類/レピュテーションのない URL

URL ルールを作成するときは、まず一致させるカテゴリを選択します。[未分類（Uncategorized）] URL を明示的に選択した場合は、レピュテーションによりさらに制約を追加することはできません。

信頼できないレピュテーションの未分類 URL は、[悪意のあるサイト（Malicious Sites）] カテゴリによって処理されます。他のレピュテーション レベルを使用する未分類サイトをブロックする場合は、すべての未分類サイトをブロックする必要があります。

URL のカテゴリおよびレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリおよびレピュテーションベースの URL 条件を持つルールには一致しません。カテゴリとレピュテーションを手動で URL に割り当てることはできませんが、特定の URL はブロックできます。手動による URL ブロッキングの実行 （13 ページ）を参照してください。

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された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。
- HTTP 応答ページを表示しません（設定したとしても）。

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。

手動による URL フィルタリングのガイドライン

手動で URL を入力するか、URL オブジェクトまたはグループを使用して URL フィルタリングを指定すると、それらの URL は単純な文字列一致を使用してトラフィックを照合します。たとえば、トラフィックの通過を許可するルールに「cisco.com」を入力すると、URL 内の何らかの部分に「cisco.com」を持つすべてのドメインに対するトラフィックが許可されることを意味します。一方で、個別の URL を指定するためにカスタム セキュリティ インテリジェンス リストまたはフィードを使用すると、ドメイン名に一致している URL がアンカーされます。

URL カテゴリまたはレピュテーションの不一致

ライセンス：URL Filtering

URL に誤ったカテゴリまたはレピュテーション レベルが割り当てられていると思われる場合は、疑われるエラーをシスコに報告できます。

始める前に

シスコ アカウントのクレデンシャルが必要になります。

ステップ 1 接続イベントのリストに移動します。

ステップ 2 報告するイベントを右クリックし、[Dispute URL Category] または [Dispute URL Reputation] を選択します。

ブラウザのウィンドウに新しいページが開きます。

ステップ 3 シスコアカウントのクレデンシャルを使用して Talos の Web サイトにサインインします。

ステップ 4 ページに表示される指示に従います。

このページにはチケットのステータスを表示するリンクが含まれています。この情報は後で追跡できるようにメモします。

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 [Interactive Block] または [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、一致する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 （19 ページ）を参照してください。

SSL インスペクション機能によって復号化された Web トラフィックをブロックすると、システムは応答ページを暗号化し、再度暗号化された SSL ストリームの最後にそのページを送信します。

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。

URL カテゴリとレピュテーションに基づく URL のブロッキング （9 ページ） および手動による URL ブロッキングの実行 （13 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 [Interactive Block] または [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処理とインスペクションの決定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。

- 一方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。

システムは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 Interactive Block または 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 Allow 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 サイトのユーザー バイパス タイムアウトの設定 （18 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 （19 ページ）」を参照してください。

ブロックされた Web サイトのユーザー 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 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[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 [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 [General Settings] の横にある編集アイコンをクリックします。

[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 [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）の間の任意の秒数を指定できます。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 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを展開する必要があります。詳細については、設定変更の導入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、[Block] または [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。このカスタム ページは HTTP 応答ページと呼ばれています。

- 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最新表示して、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、[Interactive Block] または [Interactive Block with reset] を選択します。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。アクセス コントロール ポリシーの編集を参照してください。

ステップ 2 [HTTP Responses] タブをクリックします。

ステップ 3 [Block Response Page] および [Interactive Block Response Page] の場合は、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。

- [System-provided]：一般的な応答を表示します。表示アイコンをクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページを作成します。

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。

- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。 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 [Store ASA FirePOWER Changes] をクリックします。

変更を有効にするには、設定を再展開する必要があります。詳細については、設定変更の導入を参照してください。