URL フィルタリング

URL フィルタリングの概要

URL フィルタリング機能を使用してネットワークのユーザがアクセスできる Web サイトを制御します。

- カテゴリおよびレピュテーションベースの URL フィルタリング：URL フィルタリング ライセンスでは、URL の一般的な分類（カテゴリ）とリスク レベル（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ができます。これは推奨オプションです。
- 手動 URL フィルタリング：任意のライセンスで、個々の URL、URL のグループおよび URL リストとフィードを手動で指定し、Web トラフィックのきめ細かいカスタム制御を実現できます。詳細については、手動 URL フィルタリング （13 ページ）を参照してください。

カテゴリおよびレピュテーションによる URL のフィルタリングについて

URL フィルタリング ライセンスでは、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 サイトへのアクセスを制御できます。

- カテゴリ：URL の一般的な分類。たとえば ebay.com はオークション カテゴリ、monster.com は求職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。

- レピュテーション：この URL が、組織のセキュリティ ポリシーに違反するかもしれない目的で使用される可能性がどの程度であるか。レピュテーションの範囲は、[高リスク（High Risk）]（レベル 1）から [ウェルノウン（Well Known）]（レベル 5）までがあります。

カテゴリおよびレピュテーションベースの URL フィルタリングのメリット

URL カテゴリとレピュテーションによって、URL フィルタリングをすぐに設定できます。たとえば、アクセス コントロールを使用して、ハッキング カテゴリの高リスク URL をブロックできます。または、QoS を使用してストリーミング メディア カテゴリのサイトからのトラフィックをレート制限できます。スパイウェアおよびアドウェア カテゴリなど、脅威のタイプのカテゴリもあります。

カテゴリおよびレピュテーションデータを使用すると、ポリシーの作成と管理がより簡単になります。この方法では、システムが Web トラフィックを期待どおりに確実に制御します。脅威インテリジェンスは、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 をフィルタ処理します。セキュリティに対する脅威を表すサイトや望ましくないコンテンツが表示されるサイトは、ユーザが新しいポリシーを更新したり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。

システムはどのように適応するのか、いくつかの例を示します。

- アクセス コントロール 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。同様に、QoS ルールですべてのストリーミング メディア サイトをレート制限する場合、システムは新しいストリーミング メディア サイトへのトラフィックを自動的に制限できます。

- アクセス コントロール ルールですべてのマルウェア サイトをブロックし、あるショッピング ページがマルウェアに感染すると、システムはその URL をショッピング サイトからマルウェア サイトに再分類して、そのサイトをブロックすることができます。

- アクセス コントロール 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、誰かがプロファイル 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、システム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）] に変更してブロックすることができます。

関連トピック

Snort® の再起動シナリオ

Cisco Cloud からの URL フィルタリングのデータ

カテゴリおよびレピュテーションに基づく URL フィルタリングには、クラウド サービスである Cisco Collective Security Intelligence（Cisco CSI）から提供されたデータ セットが必要です。

一般に、デフォルトでは、有効な URL フィルタリング ライセンスがアクティブなデバイスに適用されると、URL カテゴリおよびレピュテーションのデータ セットが Cisco Cloud から Firepower Management Center にダウンロードされ、デバイスにプッシュされます。このローカルに保存されたデータ セットは定期的に更新されます。

ネットワーク上のユーザが URL にアクセスすると、システムはローカル（ダウンロードした）データ セット内の一致を検索します。一致がない場合、システムが Cisco Cloud で以前に検索した結果のキャッシュをチェックします。それでも一致がなければ、システムは Cisco Cloud で URL を検索し、結果をキャッシュに追加します。

URL フィルタリングのベスト プラクティス

- 手動フィルタリングではなく、カテゴリとレピュテーションに基づく URL フィルタリングを使用
- カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 （7 ページ）の手順に従います。
- 次を詳しく確認してください。 URL フィルタリングのガイドラインと制限事項 （3 ページ）

URL フィルタリングのガイドラインと制限事項

URL 識別の制限

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。
- システムによりセッションで HTTP または HTTPS アプリケーションが識別される。
- 要求された URL がシステムにより識別される（ClientHello 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、TLS/SSL ハンドシェイクのサーバ証明書交換の後に行われる必要があります。

早期のトラフィックがその他のすべてのルール条件に一致するが、識別が不完全な場合、システムは、パケットの受け渡しと接続の確立（または、TLS/SSL ハンドシェイクの完了）を許可します。システムは識別を完了した後、残りのセッション トラフィックに適切なルール アクションを適用します。

アクセス制御の場合、これらの受け渡されたパケットは、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く、アクセス制御ポリシーのデフォルトの侵入ポリシーによりインスペクションが実行されます。

URL 条件とルールの順序

- URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルール（アプリケーション ルールなど）より前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。
  - その他のルールがアプリケーション条件を含んでいる。
  - 検査対象のトラフィックが暗号化されている。
- URL は複数のカテゴリに属することができます。Web サイトの 1 つのカテゴリを許可し、別のカテゴリをブロックすることができます（明示的に行うか、デフォルトアクションに依存して）。この場合、許可またはブロックが優先されるかどうかに応じて、適切な効果が得られるように URL ルールを作成して順序付けしてください。

ルールに関するその他のガイドラインについては、ルール条件の仕組みおよびルールのパフォーマンスに関するガイドラインを含め、ルール管理：共通の特性の章を参照してください。

未分類または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。

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 URL に手動で割り当てることはできませんが、アクセス コントロール ポリシーと QoS ポリシーでは、特定の URL を手動でブロックできます。手動 URL フィルタリング （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 URL フィルタリング

暗号化された Web トラフィックに対して URL フィルタリングを実行すると、システムは次のように動作します。

- 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がない場合、ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- URL リストを使用しません。代わりに、URL オブジェクトとグループを使用する必要があります。
- 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。

- アクセス制御ルール（または、その他の設定）によってブロックされている暗号化された接続の場合はHTTP応答ページを表示しません。HTTP 応答ページの制限 を参照してください。

HTTP/2

システムは、TLS証明書からHTTP/2 URLを抽出できますが、ペイロードから抽出することはできません。

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。

高可用性展開での URL フィルタリング

高可用性でのFirepower Management Centerを使用したURLフィルタリングのガイドラインについては、URL フィルタリングとセキュリティ インテリジェンスを参照してください。

選択したデバイス モデルのメモリ制限

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによってほとんどのURLフィルタリングが実行されます。たとえば、親URLのサブサイトがそれぞれ異なるURLカテゴリとレピュテーションを持っている場合でも、一部のデバイスでは、親URLのデータのみが保存される場合があります。これらのデバイスによって処理されるWebトラフィックの場合、システムはクラウド ルックアップを実行して、ローカル データベースにないサイトのカテゴリとレピュテーションを判断できます。

低メモリ デバイスには、次のデバイスが含まれます。

- 7100 シリーズ
- ASA 5508-X および ASA 5516-X
- ASA 5515-X および ASA 5525-X

NGIPSvを使用する場合、カテゴリおよびレピュテーションベースのURLフィルタリングを実行するために正しい量のメモリを割り当てる方法については、『Cisco Firepower NGIPSv（VMware向け）クイック スタート』を参照してください。

手動 URL フィルタリング

特定のURLを手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。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。要求されたURLが文字列の任意の部分に一致する場合、URLは一致するとみなされます。

関連トピック

デフォルトの侵入ポリシー

HTTPS トラフィックのフィルタリング

暗号化されたトラフィックをフィルタリングするには、システムは TLS/SSL ハンドシェイク時に渡される情報（トラフィックを暗号化するために使用される公開キー証明書のサブジェクト共通名）に基づいて、要求された URL を決定します。

HTTPS フィルタリングは、HTTP フィルタリングとは異なり、サブジェクト共通名内のサブドメインを無視します。アクセス コントロールまたは QoS ポリシーで HTTPS URL を手動で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。たとえば、www.example.com ではなく、example.com を使用します。

また、HTTPS フィルタリングは URL リストもサポートしていません。代わりに、URL オブジェクトとグループを使用する必要があります。

ヒント SSL ポリシーでは、特定の URL に対するトラフィックの処理と復号は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。HTTPS トラフィックを復号することで、復号されたセッションをアクセス コントロール ルールによって評価できるようになり、URL フィルタリングの質が向上します。

暗号化プロトコルによるトラフィックの制御

アクセス コントロールまたは QoS ポリシー内で URL フィルタリングを実行する場合、暗号化プロトコル（HTTP または HTTPS）は無視されます。これは、手動およびレピュテーションベース両方の URL 条件で発生します。つまり、URL フィルタリングは、次の Web サイトへのトラフィックを同じように扱います。

- http://example.com/
- https://example.com/

HTTP または HTTPS トラフィックのみに一致する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。たとえば、あるサイトへの HTTPS アクセスを許可する一方で、HTTP アクセスを許可しないようにできます。そのためには、2 つのアクセス コントロール ルールを作成し、それぞれにアプリケーションと URL の条件を割り当てます。

最初のルールは Web サイトへの HTTPS トラフィックを許可します。

アクション：許可
アプリケーション：HTTPS
URL：example.com

2 番目のルールは同じ Web サイトへの HTTP アクセスをブロックします。

アクション：ブロック

アプリケーション：HTTP
URL：example.com

カテゴリとレピュテーションを使用した URL フィルタリングの設定方法

	操作手順	詳細情報
ステップ 1	NGIPSv デバイスでカテゴリおよびレピュテーションベースの URL フィルタリングを使用する場合は、必要なメモリ量を割り当てます。	Cisco Firepower NGIPSv（VMware 向け）クイック スタート
ステップ 2	正しいライセンスがあることを確認します。	Firepower システムのライセンス次のようなものがあります。 • Firepower Threat Defense デバイスの URL フィルタリング ライセンス • 従来のデバイスの URL フィルタリング ライセンス URL フィルタリング ライセンスを URL をフィルタ処理する各管理対象デバイスに割り当てます。 機能を有効にするには、そのデバイスに割り当てられた URL フィルタリング ライセンスが少なくても 1 台の管理対象デバイスにある必要があります。
ステップ 3：	Firepower Management Center はクラウドと通信して URL フィルタリングデータを取得できることを確認します。	インターネット アクセス要件、通信ポートの要件
ステップ 4：	制限事項とガイドラインを理解し、必要なアクションを実行します。	URL フィルタリングのガイドラインと制限事項（3 ページ）
ステップ 5：	URL フィルタリング機能を有効にします。	カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （8 ページ）

	操作手順	詳細情報
ステップ 6：	カテゴリとレピュテーションによってURLをフィルタ処理するポリシーを設定します。	URL 条件の設定 （10 ページ）
ステップ 7	（オプション）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できるようにします。	HTTP応答ページとインタラクティブなブロッキング
ステップ 8：	トラフィックがキールールに最初にヒットするようにルールを順序付けます。	URL ルールの順序
ステップ 9	（オプション）クラウドルックアップを必要とする URL の処理を変更します。	アクセス コントロール ポリシーの詳細設定の [URLキャッシュミスルックアップを再試行する（Retry URL cache miss lookup）] オプションに関する情報。
ステップ 10	変更を展開します。	設定変更の展開
ステップ 11	システムが将来の URL データの更新を予想どおりに受信することを確認します。	URL フィルタリングのヘルス モニタの設定 （13 ページ）

カテゴリとレピュテーションを使用した URL フィルタリングの有効化

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
URL フィルタリング	URL フィルタリング	任意（Any）	任意（Any）	Admin

始める前に

カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 （7 ページ） で説明されている前提条件をすべて満たします。

手順

ステップ 1 **[System]** > **[Integration]**を選択します。

ステップ 2 [**[Cisco CSI]**] タブをクリックします。

ステップ 3 URL フィルタリング オプション （9 ページ） を設定します。
ステップ 4 [保存（Save）] をクリックします。

URL フィルタリング オプション

次のオプションは、[システム（System）] > [統合（Integration）] ページにあります。

Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URL フィルタリング ライセンスを追加すると、[URLフィルタンリングを有効にする（Enable URL Filtering）] が自動的に有効になります。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URL フィルタリングを有効にする場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、またはURL フィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco CloudCisco Collective Security Intelligence（Cisco CSI）から URL データをダウンロードします。このプロセスには、時間がかかる場合があります。

自動更新を有効にする（Enable Automatic Updates）

URL フィルタリング脅威データを更新するためのオプション。

- [システム（System）] > [統合（Integration）] ページの [自動更新を有効にする（Enable Automatic Updates）] オプションを有効にすると、Firepower Management Center は 30 分ごとにクラウドの更新をチェックします。 このオプションは、URL フィルタリング ライセンスを追加すると、デフォルトで有効になります。
- システムが外部リソースに接触する時間を厳格に制御する必要がある場合、このページの自動更新を無効にし、代わりにスケジューラを使用して定期的なタスクを作成します。スケジュール設定されたタスクを使用した URL フィルタリング更新の自動化を参照してください。

[今すぐアップデート（Update Now）]

このダイアログ ボックスの上部にある [今すぐアップデート（Update Now）] ボタンをクリックすると、ワンタイムのオンデマンド更新を実行できますが、自動更新を有効にするか、スケジューラを使用して定期的なタスクを作成する必要があります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URLs）]

カテゴリとレピュテーションがローカル データセットにない Web サイトをユーザが閲覧するときに、脅威インテリジェンス評価のために URL がクラウドに送信されるようにします。プライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

このオプションは、少なくとも 1 台の管理対象デバイスに有効な URL フィルタリング ライセンスがある場合にデフォルトで有効になります。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致**しません**。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。

暗号化されたトラフィックを SSL ルールを使用して処理する場合は、TLS/SSL ルールのガイドラインと制限事項も参照してください。

キャッシュされた URL の期限切れ

このオプションは、リリース 6.3 以降を実行しているデバイスのみに適用されます。リリース 6.2.3 を実行しているデバイスでは、TAC に問い合わせてこの機能を設定する必要があります。

この設定は、[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）] [不明 URL を Cisco Cloud に問い合わせる（Query Cisco Cloud for Unknown URLs）]が有効になっている場合にのみ該当します。

カテゴリおよびレピュテーション データのキャッシングにより、Web ブラウジングが高速化されます。デフォルトでは、最速のパフォーマンスを得るため、URL のキャッシュされたデータの有効期限はありません。

古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。脅威データの正確性と即時性を向上させるため、短い有効期限を選択します。

キャッシュされた URL は、指定された時間が経過した後、ネットワーク上のユーザが初めてアクセスした後に更新されます。最初のユーザに更新済みの結果は表示されませんが、この URL に次にアクセスしたユーザには更新済みの結果が表示されます。

URL データのキャッシングについては、Cisco Cloud からの URL フィルタリングのデータ （3 ページ） を参照してください。

URL 条件の設定

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	URL フィルタリング（カテゴリ/レピュテーション） 任意（手動）	任意（Any）	任意（Any）	Admin/Access Admin/Network Admin

URL 条件を作成するときに、トラフィックを制御する URL カテゴリを選択します。必要に応じて、URL カテゴリをレピュテーションで制約できます。

アクセス コントロールおよび QoS ルールでは、事前定義された URL オブジェクト、URL リストとフィード、および手動のルールごとの URL を使用して個々の URL をフィルタ処理することもできます。これらの URL はレピュテーションで制約できません。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

手順

ステップ 1 ルール エディタで、URL 条件のタブをクリックします。

- アクセス コントロールまたは QoS：[URL（URLs）] タブをクリックします。
- SSL：[カテゴリ（Categoy）] タブをクリックします。

ステップ 2 制御する URL を見つけて選択します。

- カテゴリ：URL カテゴリを選択するか、デフォルトの [任意（Any）] のままにします。アクセス コントロールまたは QoS ルールでは、[カテゴリ（Categoy）] サブタブをクリックしてカテゴリを選択します。
- URL オブジェクト、リスト、およびフィード：定義済みの URL オブジェクトおよび URL リストとフィードを選択します。アクセス コントロールまたは QoS ルールでは、[URL（URLs）] サブタブをクリックして URL を選択します。

ステップ 3 （オプション）レピュテーションを選択して URL カテゴリを制約します。

[未分類（Uncategorized）] URL を明示的に照合する場合は、未分類 URL にはレピュテーションがないため、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ないことに注意してください。レピュテーション レベルを選択すると、ルール アクションに応じて、選択したレベルよりも重大または重大でない他のレピュテーションも含められます。

- [より重大でないレピュテーションを含める（Includes less severe reputations）]：ルールで Web トラフィックを許可または信頼する場合。たとえば、[無害なサイト（Benign Sites）]（レベル 4）を許可するようアクセス コントロール ルールを設定した場合、[ウェルノウン（Well Known）]（レベル 5）サイトも自動的に許可されます。
- [より重大なレピュテーションを含める（Includes more severe reputations）]：ルールで Web トラフィックをレート制限、復号、ブロック、またはモニタする場合。たとえば、[疑わしいサイト（Suspicious Sites）]（レベル 2）をブロックするようアクセス コントロール ルールを設定した場合、[高リスク（High Risk）]（レベル 1）のサイトも自動的にブロックされます。

ルール アクションを変更すると、URL 条件のレピュテーション レベルが自動的に変更されます。

ステップ 4 [ルールに追加（Add to Rule）] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 （オプション）アクセス コントロールまたは QoS ルールでは、URL を入力し、[追加（Add）] をクリックして、手動で指定する URL を追加します。

URL または IP アドレスを入力できます。このフィールドでは、ワイルドカードはサポートされません。

ステップ 6 ルールを保存するか、編集を続けます。

例：アクセス コントロール ルールの URL 条件

次の図は、すべてのマルウェア サイト、すべての [高リスク（High Risk）] サイト、およびすべての有害なソーシャル ネットワーキング サイト（）をブロックするアクセス コントロール ルールの URL 条件を示しています。また、単一サイト example.com（URL オブジェクトによって表されます）もブロックされます。

次の表では、条件を作成する方法を要約します。

ブロックする URL	カテゴリまたは URL オブジェクト	レピュテーション
マルウェア サイト（レピュテーションに関係なく）	マルウェア サイト（Malware Sites）	任意（Any）
高リスクの URL（レベル 1）	任意（Any）	1：[高リスク（High Risk）]
無害よりも大きいリスクがある（）ソーシャル ネットワーキング サイト（レベル 1 ～ 3）	ソーシャル ネットワーク（Social Network）	3：[セキュリティ リスクのある無害なサイト（Benign sites with security risks）]
example.com	example.com という名前の URL オブジェクト	なし

次のタスク

- カテゴリとレピュテーションを使用した URL フィルタリングの設定方法 （7 ページ）に戻ります。
- 変更を行った場合についてです。 設定変更を展開します。設定変更の展開を参照してください。

URL 条件を伴うルール

次の表に、URL 条件をサポートするルールと、各ルール タイプがサポートするフィルタリングのタイプを一覧します。

ルール タイプ	カテゴリとレピュテーション フィルタリングをサポートしますか。	手動フィルタリングのサポート
アクセス コントロール	Yes	Yes
SSL	Yes	なし。代わりに識別名条件を使用
QoS	Yes	Yes

URL ルールの順序

URL マッチングを最も効果的に行うには、URL 条件を含むルールを他のルールより前に配置します。特に、URL ルールがブロック ルールで、他のルールが次の条件を両方とも満たす場合には、URL 条件を含むルールを前に配置します。

- その他のルールがアプリケーション条件を含んでいる。
- 検査対象のトラフィックが暗号化されている。

URL フィルタリングのヘルス モニタの設定

次のヘルス ポリシーは、システムに URL カテゴリとレピュテーション データを取得または更新に問題がある場合は通知します。

- URL フィルタリング モニタ
- デバイスでの脅威データの更新

これらが考えているとおりに設定されていることを確認するには、ヘルス モジュールおよびヘルス モニタリングの設定を参照します。

手動 URL フィルタリング

アクセス コントロール ルールおよび QoS ルールでは、個々の URL、URL のグループ、または URL のリストとフィードを手動でフィルタリングすることで、カテゴリとレピュテーション ベースの URL のフィルタリングを補足したり、選択的にオーバーライドしたりできます。

（注） 多数の URL をフィルタリングする場合、個別の、またはグループ化された URL オブジェクトを使用する代わりに、URL リストを使用します。詳細については、セキュリティ インテリジェンスのリストとフィードを参照してください。

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ができます。手動 URL フィルタリングは SSL ルールではサポートされません。その代わりに、識別名の条件を使用します。

たとえば、アクセス コントロールを使用して組織に適していない Web サイトのカテゴリをブロックできます。ただし、カテゴリに適切な Web サイトが含まれていて、そこにアクセスを提供する必要がある場合は、そのサイトに手動で許可ルールを作成し、カテゴリのブロック ルールの前に配置できます。

警告

特定の URL を手動でフィルタリングする場合は、影響を受ける可能性のある他のトラフィックを慎重に考慮してください。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。要求された URL が文字列の任意の部分に一致する場合、URL は一致するとみなされます。

例 1:

ign.com （ゲーム サイト）を明示的にブロックする必要があります。部分文字列マッチングにより ign.com 自体だけでなく verisign.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。

例 2:

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 サイトを参照できます。

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

関連トピック

セキュリティ インテリジェンスのリストとフィード

URL フィルタリングのトラブルシューティング

特定の URL のカテゴリとレピュテーションはどのようにしたら確認できますか。

手動ルックアップを実行します。URL カテゴリとレピュテーションの検索を参照してください。

手動ルックアップ試行時のエラー：「<URL> のクラウド ルックアップに失敗しました（Cloud Lookup Failure for <URL>）」

機能が適切に有効になっていることを確認します。URL カテゴリとレピュテーションの検索の前提条件を参照してください。

URL はその URL カテゴリとレピュテーションに基づいて誤って処理されたように見えます。

問題：システムは URL カテゴリとレピュテーションに基づいて URL を正しく処理しません。

対処方法:

- URL カテゴリと URL に関連付けられているレピュテーションが想定どおりであることを確認します。URL カテゴリとレピュテーションの検索を参照してください。
- 次の問題は、カテゴリとレピュテーションを使用した URL フィルタリングの有効化 （8 ページ）を使用してアクセスできる、URL フィルタリング オプション （9 ページ）で説明した設定で対処できる場合があります。
  - URL キャッシュに古い情報が保存されている可能性があります。URL フィルタリング オプション （9 ページ）の [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定に関する情報を参照してください。
  - クラウドからの最新情報でローカルのデータセットが更新されていない可能性があります。URL フィルタリング オプション （9 ページ）の [自動更新を有効にする（Enable Automatic Updates）] 設定に関する情報を参照してください。
  - 最新のデータに関してクラウドを確認しないようにシステムが設定されている可能性があります。URL フィルタリング オプション （9 ページ）の [不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）] [不明 URL を Cisco Cloud に問い合わせる（Query Cisco cloud for unknown URLs）]の設定に関する情報を参照してください。
- クラウドを確認せずに URL にトラフィックを渡すようにアクセス コントロール ポリシーが設定されている可能性があります。アクセス コントロール ポリシーの詳細設定 で、[URL キャッシュ ミス ルックアップを再試行する（Retry URL cache miss lookup）] 設定に関する情報を参照してください。
- URL フィルタリングのガイドラインと制限事項 （3 ページ）も参照してください。
- SSL ルールを使用して URL を処理した場合は、TLS/SSL ルールのガイドラインと制限事項およびSSL ルールの順序を参照してください。
- URL を処理している思われるアクセス制御ルールを使用して URL が処理されていることを確認し、アクセス制御ルールが想定どおりに機能していることを確認します。ルールの順序を考慮します。
- Firepower Management Center のローカル URL カテゴリおよびレピュテーション データベースがクラウドから正常に更新されており、管理対象デバイスが Firepower Management Center から正常に更新されていることを確認します。

これらのプロセスのステータスは、[URL フィルタリング モニタ（URL Filtering Monitor）] モジュールおよび [デバイスでの脅威データの更新（Threat Data Updates on Devices）] モジュールのヘルス モニタでレポートされます。詳細は、ヘルス モニタリングを参照してください。

ローカル URL カテゴリおよびレピュテーション データベースを即座に更新する場合、**[System]** > **[Integration]** に移動し、**[Cisco CSI]** タブをクリックしてから [今すぐアップデート（Update Now）] をクリックします。詳細については、URL フィルタリング オプション （9 ページ）を参照してください。

URL カテゴリまたはレピュテーションが正しくありません。

アクセス コントロールまたは QoS ルールの場合：ルールの順序に細心の注意を払って、手動フィルタリングを使用します。手動 URL フィルタリング （13 ページ）およびURL 条件の設定 （10 ページ）を参照してください。

SSL ルールの場合：手動フィルタリングはサポートされていません。代わりに識別名条件を使用します。

Web ページのロードに時間がかかる

セキュリティとパフォーマンスのトレードオフがあります。いくつかのオプションを次に示します。

- [キャッシュされたURLの期限切れ（Cached URLs Expire）] 設定の変更を検討します。**[System]** > **[Integration]** をクリックしてから、**[Cisco CSI]** タブを選択します。詳細については、URL フィルタリング オプション （9 ページ）を参照してください。
- アクセス コントロール ポリシーの詳細設定の [URL キャッシュのミス検索の再試行（Retry URL cache miss lookup）] 設定の選択解除を検討します。

イベントに URL カテゴリおよびレピュテーションは含まれていません

- アクセス コントロール ポリシーに適用可能な URL ルールが含まれていること、ルールがアクティブになっていること、およびポリシーが関連するデバイスに展開されていることを確認します。
- URL ルールと一致する前に接続が処理される場合、URL カテゴリとレピュテーションはイベントに表示されません。

URL フィルタリングの履歴

機能	バージョン（Version）	詳細
URL フィルタリング情報をさまざまな場所から新しい URL フィルタリングの章に移動しました。	6.3	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。その他の特定の URL フィルタリングの情報をこの章の他の場所に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。
新規オプション：キャッシュされた URL の期限切れ	6.3	この新しいコントロールを使用して、古いデータで一致している URL のインスタンスを最小限に抑えるため、新しい URL カテゴリおよびレピュテーションとパフォーマンスとのバランスを取ります。 変更された画面：[システム（System）] > [統合（Integration）] > [Cisco CSI]。 サポート対象プラットフォーム：すべて
変更されたメニュー パス	6.3	[手動 URL ルックアップ（Manual URL Lookup）] へのパスが [分析（Analysis）] > [ルックアップ（Lookup）] > [URL] から [分析（Analysis）] > [詳細（Advanced）] > [URL] に変更されました。