ファイアウォール Web フィルタ ルールの管理

Web フィルタ ルール ポリシーでは、要求された URL またはトラフィックのアプレット コンテンツに基づいて Web トラフィックを許可または阻止するポリシーを定義します。ASA、PIX、および FWSM デバイスの場合は、FTP および HTTPS トラフィックもフィルタリングできます。

Web フィルタ ルールを設定する方法は、Cisco IOS ソフトウェアではなく、デバイスが ASA、PIX、または FWSM ソフトウェアを使用するかどうかによって異なります。

Web フィルタ ルールの使用方法については、次の項を参照してください。

Web フィルタ ルールについて

Web フィルタ ルール ポリシーでは、要求された URL またはトラフィックのアプレット コンテンツに基づいて Web トラフィックを許可または阻止するポリシーを定義します。ASA、PIX、および FWSM デバイスの場合は、FTP および HTTPS トラフィックもフィルタリングできます。

Web または URL フィルタリングを使用すると、ユーザがアクセスできる Web サイトおよび Web コンテンツを制御できます。たとえば、ある種のコンテンツは、組織のメンバーの作業環境に悪影響を及ぼすと考えられます（ポルノを提供する Web サイトなど）。安全ではないと見なされる Web サイトや、アプリケーションがウイルスの感染源となるおそれのある Web サイトもあります。Web フィルタ ルールを使用すると、これらの好ましくないサイトまたは安全ではないサイトへのアクセスをブロックできます。

Web 要求をフィルタリングするには、Websense または SmartFilter（N2H2）のいずれかの外部 Web フィルタリング サーバをインストールする必要があります。ASA、PIX、および FWSM デバイスの場合は、URL、FTP、または HTTPS のフィルタリングにこれらの外部サーバが必

要です。IOS デバイスの場合は、これらのサーバーを使用することもできますが、さらに許可リスト（常に許可）URL またはブロックリスト（常に拒否）URL のリストをローカルに作成できます。フィルタリング サーバは、Web フィルタ設定ポリシーで設定します。Web フィルタ サーバの設定 （21 ページ）を参照してください。

ヒント IOS デバイスの場合は、Web フィルタ ルールの代わりに、ゾーンベースのファイアウォール ルールを使用して Web フィルタリングを設定できます。このルールを使用すると、さらに Trend Micro Web フィルタリング サーバの使用を選択できます。詳細については、ゾーンベースのファイアウォール ルールの管理を参照してください。

URL に基づいて要求をフィルタリングする以外に、アプレットのフィルタリングを実行して ActiveX または Java アプレットを除去できます。サイトを信頼していればダウンロードを許可しますが、十分に信頼していない場合はこのフィルタリングを実行し、アプレット ダウンロードを阻止できます。特定のサイトからのアプレットはブロックし、信頼できるサイトのアプレットは許可するようにルールを設定できます。

Web フィルタ ルールを設定するポリシーおよび手順は、デバイス タイプによって異なります。詳細については、次のトピックを参照してください。

- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （2 ページ）
- IOS デバイス用の Web フィルタルールの設定 （15 ページ）

ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ASA、PIX、および FWSM デバイスの Web フィルタ ルール ポリシーでは、HTTP、FTP、および HTTPS のトラフィックを処理する方法を定義します。ActiveX および Java アプレットをフィルタリングすることもできます。Web フィルタ ルールは、Web 要求に含まれる Universal Resource Locator（URL）アドレスに基づいてトラフィックを許可または拒否します。アクセス ルールで HTTP トラフィックを許可した場合、トラフィックが好ましくない Web サイトまたは FTP サイトに向けられた場合に、あとからそのトラフィックを拒否（またはドロップ）したり、信頼できない送信元からの ActiveX または Java アプレットを除去できます。

ASA、PIX、および FWSM デバイスに Web フィルタリング ルールを設定するには、次の手順を実行します。

1. フィルタリングを適用するトラフィック、およびフィルタリング ルールを免除するトラフィックを識別するルールを設定します（手順については次を参照してください）。

2. URL フィルタリング サーバを識別する Web フィルタ設定およびその他の設定を行います。詳細については、Web フィルタ サーバの設定 （21 ページ）を参照してください。

関連項目

- Web フィルタ ルールについて （1 ページ）
- セクションを使用したルール テーブルの編成
- ルールの追加および削除
- ルールの編集
- ルールのイネーブル化とディセーブル化
- ルールの移動とルール順序の重要性
- ネットワーク/ホストオブジェクトについて
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定

ステップ 1 次のいずれかを実行して、[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （4 ページ）を開きます。

- デバイスビュー：ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- ポリシービュー：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（PIX/FWSM/ASA）（Web Filter Rules (PIX/FWSM/ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （7 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （7 ページ）を参照してください。

- [Filtering] および [Type]：フィルタリングするトラフィックを識別するルール（[Filter]）を作成するか、既存のフィルタ ルールを免除するトラフィックを識別するルール（[Filter Except]）を作成するかどうか、および実行されるフィルタリングのタイプ。
  - URL：Web アドレスに基づいてトラフィックをフィルタ処理します。
  - [HTTPS]：セキュアなサイトへの Web トラフィックをフィルタリングします。SSL VPN トラフィックは含まれません。

- [FTP]：FTP トラフィックをフィルタリングします。
- [ActiveX] または [Java]：ActiveX または Java アプレットを削除します。これらのオプションにより、アプレット タグまたはオブジェクト タグ内のすべてのエンティティが削除されます。したがって、削除できるのが ActiveX または Java アプレットだけに留まらない場合があります。

- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスやトラフィックの宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「any」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホストオブジェクトを入力します。受け入れられるアドレス形式の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。
- [Service]：モニタが必要なポートを主に定義します。いくつかのタイプの TCP サービスを指定する必要があります。通常は、事前定義されたサービスの HTTP、HTTPS、または FTP を使用しますが、これは実行するフィルタリングのタイプに合わせる必要があります。ただし、フィルタリング対象のトラフィックが含まれる可能性のある、ネットワークの任意の TCP ポートを指定できます。
- [Options]：追加するオプション（ある場合）。該当する主なオプションは、フィルタリング サーバが利用不能な場合にトラフィックを許可するかどうか、および長い URL またはパラメータが含まれる URL を切り捨てるかどうかです。URL をドロップする場合、一般には 1 つのパラメータ値が原因ではないため、通常はパラメータが含まれる URL は切り捨てることを推奨します。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。ただし、フィルタ例外ルールがフィルタ ルールの前後のいずれにあっても、常に関連するフィルタ ルールの例外が作成されるため、Web フィルタリング ルールの順序は重要ではありません。詳細については、ルールの移動とルール順序の重要性を参照してください。

[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

Web または URL フィルタリング ルールを設定するには、ASA、PIX、および FWSM デバイスの [Web Filter Rules] ページを使用します。Web フィルタリングは、HTTP インスペクションの一種です。アクセス ルールで HTTP トラフィックを許可している場合は、ルールを設定してサーバベースの Web フィルタリングを適用すると、望ましくない Web サーバへのユーザ アクセスを防止できます。

Web フィルタルールを設定する場合は、[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] ポリシーで Web フィルタ設定も設定します。これらの設定は、Web フィルタリング サーバを識別し、ポリシーの機能全体を制御するその他の設定を含みます。Web フィルタリング サーバを設定して、展開する URL、FTP、または HTTPS のフィルタ

ルールを指定する必要があります。詳細については、 Web Filter 設定ページ （23 ページ）を参照してください。

ヒント　重複するルールは作成できません。たとえば、送信元、宛先、およびサービスが同じか、重複する2つのルールを作成しても、それらのルールは展開できません。また、すべての filter-except ルールは、免除を作成するフィルタ ルールの下に配置する必要があります。

ナビゲーション パス

ASA、PIX、および FWSM デバイスの [Web Filter Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、またはFWSMデバイスを選択し、ポリシーセレクタから [ファイアウォール（Firewall）]>[Webフィルタルール（Web Filter Rules）] を選択します。
- （ポリシービュー）：ポリシータイプセレクタから**[ファイアウォール（Firewall）]>[Webフィルタルール（PIX/FWSM/ASA）（Web Filter Rules (PIX/FWSM/ASA)）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （

  マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [Webフィルタルール（Web Filter Rules）]** を選択します。

関連項目

- Web フィルタ ルールについて （1 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （2 ページ）
- Web フィルタ サーバの設定 （21 ページ）
- ルールの追加および削除
- ルールの編集
- セクションを使用したルール テーブルの編成
- ルールのイネーブル化とディセーブル化
- ルールの移動とルール順序の重要性
- テーブルのフィルタリング

フィールド リファレンス

表 *1 : [Web Filter Rules]* ページ（*ASA*、*PIX*、*FWSM*）

要素	説明
番号	順序が付けられたルール番号。
送信元 接続先	ルールの送信元アドレスおよび宛先アドレス。「any」アドレスを指定すると、ルールは特定のホスト、ネットワーク、またはインターフェイスに制限されません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IP アドレスです。複数のエントリがある場合は、テーブルセル内に個別のサブフィールドとして表示されます。ネットワーク/ホストオブジェクトについてを参照してください。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。
タイプ（Type）	ルールに対するフィルタリング処置のタイプであり、識別されたトラフィックをフィルタリングするか、または識別されたトラフィックをフィルタリングから除外（Filter Except）するかのいずれか。詳細な説明については、 [Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス （12 ページ）を参照してください。
オプション	選択したプロトコルの追加設定オプション（ある場合）。詳細については、 [Edit Web Filter Options] ダイアログボックス （13 ページ）を参照してください。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	ルールの説明（ある場合）。
最後のチケット	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。
クエリ	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。ポリシー クエリー レポートの生成を参照してください

要素	説明
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。ルール テーブルの項目の検索と置換を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性を参照してください。
[Add Row] ボタン	[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （7 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

これらのタイプのデバイスに Web フィルタリング ルールを設定するには、[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックスを使用します。

ナビゲーション パス

[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （4 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （2 ページ）
- Web フィルタ ルールについて （1 ページ）
- Web フィルタ サーバの設定 （21 ページ）

フィールド リファレンス

表 *2 : [Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化を参照してください。
フィルタリング	定義するルールのタイプを次に示します。 • [Filter]：このルールは、送信元と宛先間の識別されたトラフィックのタイプをフィルタリングします。 • [Filter Except]：このルールによって、フィルタ ルールの免除を作成します。送信元と宛先間の識別されたトラフィックはフィルタリングされません。

要素	説明
タイプ（Type）	このルールでフィルタリングする（またはフィルタリングを免除する）トラフィックのタイプ。外部サーバを使用するフィルタリングの場合は、ご使用のサーバ バージョンのマニュアルを参照して、このタイプのフィルタリングがサポートされているかどうかを確認してください。Web Filter 設定ページ （23 ページ）でフィルタリング サーバを設定します。 • [URL]：HTTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [HTTPS]：HTTPS トラフィック。SSL VPN に関連付けられているトラフィックは含まれていません。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [Java]：Java アプレットがアプレット タグで識別された場合に、HTTP トラフィックから Java アプレットを削除します。このルールでは、Java アプレットを SSL VPN トラフィックから削除しません。アプレット タグが複数のパケットに及ぶ場合、またはタグ内のコードがMTUよりも大きい場合、Javaアプレットは削除されません。 • [ActiveX]：ActiveX または Java アプレットを HTTP トラフィックから削除します。このルールによって、オブジェクトまたはアプレット タグ内のすべての項目が削除され、これにより、イメージおよびマルチメディア オブジェクトも削除される場合があります。このルールでは、SSL VPN トラフィックからアプレットを削除しません。オブジェクト タグが複数のパケットに及ぶ場合、またはタグ内のコードがMTUよりも大きい場合、オブジェクトは削除されません。 • [FTP]：FTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。

要素	説明
ソース 宛先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。詳細については、ポリシー定義中の IP アドレスの指定を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または[選択（Select）]をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応）を参照）。
サービス	動作対象のトラフィックのポート番号を定義するサービス。項目をカンマで区切って複数の値を入力できます。 サービスは TCP を使用する必要があります。仕様で、フィルタリングするポートを定義します（サービス名に意味はありません）。たとえば、ポート 80 をフィルタリングする場合は、HTTP サービス オブジェクトを使用します。ネットワーク上の HTTP トラフィックが別のポートを使用する場合は、TCP/ポート番号（たとえば、TCP/8080）を指定します。TCP を単独で入力して、すべてのポートをフィルタリングできます。 サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定を参照してください。

要素	説明
Allow traffic if URL Filter Server unavailable （URL、FTP、HTTPS のみ）	すべてのURLフィルタリングサーバが使用できない場合に、アウトバウンド接続でのフィルタリングされていないトラフィックを許可するかどうか。このオプションを選択しなかった場合は、影響を受けるすべての発信トラフィック（HTTP、FTP、またはHTTPS）は、少なくとも 1 台のフィルタリング サーバが使用できるようになるまで、ブロックされます。
HTTPプロキシサーバーへの接続をブロックする（Block connection to HTTP Proxy Server） （URL のみ）	ユーザによる HTTP プロキシ サーバへの接続を阻止するかどうか。
Truncate CGI request by removing CGI parameters （URL のみ）	URLに疑問符（?）で始まるパラメータリスト（CGIスクリプトなど）が含まれている場合に、フィルタリングサーバに送信されるURLに対して、そのURLに含まれる疑問符と疑問符のあとのすべての文字を削除する切り捨てを行うかどうか。
絶対FTPパスが指定されていない場合にアウトバウンドリクエストをブロックする（Block outbound requests if absolute FTP path is not provided） （FTP のみ）	ユーザがディレクトリを変更しようとしたときに、ディレクトリ全体のパスを提供しない対話型 FTP セッションを阻止するかどうか。
長いURL（Long URL） （URL のみ）	フィルタリング サーバで許可されている最大数（Websense の場合は 4 KB、Smartfilter [N2H2] の場合は 3 KB）よりも大きい URL を処理する方法。多くの場合、長いURLはパラメータリストが原因であり、[CGIパラメータを削除することでCGI要求を切り捨てる（Truncate CGI request by removing CGI parameters）] オプションを使用して、それらのURLを処理できます。これ以外の長いURLの場合は、次のオプションから選択します。 • [Drop]：長い URL 要求をドロップします。 • [Truncate]：URL 要求を、URL のホスト名または IP アドレス部分だけに切り捨てます。 • [Deny]：URL 要求を拒否します。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス

ASA、PIX、および FWSM デバイスの Web フィルタ ルールによって実行されるフィルタリングのタイプを編集するには、[Edit Web Filter Type] ダイアログボックスを使用します。

ナビゲーション パス

（[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （4 ページ）上で）ASA/PIX/FWSM の Web フィルタルールの [タイプ（Type）] セルを右クリックし、[Webフィルタタイプの編集（Edit Web Filter Type）] を選択します。一度に 1 つの行のタイプを編集できます。

フィールド リファレンス

表 3 : [Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス

要素	説明
フィルタリング	定義するルールのタイプを次に示します。 • [Filter]：このルールは、送信元と宛先間の識別されたトラフィックのタイプをフィルタリングします。 • [Filter Except]：このルールによって、フィルタ ルールの免除を作成します。送信元と宛先間の識別されたトラフィックはフィルタリングされません。

要素	説明
タイプ（Type）	このルールでフィルタリングする（またはフィルタリングを免除する）トラフィックのタイプ。外部サーバを使用するフィルタリングの場合は、ご使用のサーババージョンのマニュアルを参照して、このタイプのフィルタリングがサポートされているかどうかを確認してください。 Web Filter 設定ページ （23 ページ） でフィルタリング サーバを設定します。 • [URL]：HTTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [HTTPS]：HTTPS トラフィック。SSL VPN に関連付けられているトラフィックは含まれていません。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [Java]：Java アプレットがアプレット タグで識別された場合に、HTTP トラフィックから Java アプレットを削除します。このルールでは、Java アプレットを SSL VPN トラフィックから削除しません。アプレット タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、Java アプレットは削除されません。 • [ActiveX]：ActiveX または Java アプレットを HTTP トラフィックから削除します。このルールによって、オブジェクトまたはアプレット タグ内のすべての項目が削除され、これにより、イメージおよびマルチメディア オブジェクトも削除される場合があります。このルールでは、SSL VPN トラフィックからアプレットを削除しません。オブジェクト タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、オブジェクトは削除されません。 • [FTP]：FTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。

[Edit Web Filter Options] ダイアログボックス

ASA、PIX、および FWSM デバイスの Web フィルタ ルールに定義されたフィルタリング オプションを編集するには、[Edit Web Filter Options] ダイアログボックスを使用します。

このダイアログボックスに表示されるオプションは、ルールに設定されたフィルタリングのタイプによって異なります。一部のタイプにはオプションがなく、ダイアログボックスは空になります。以下の参照テーブルには、選択可能なすべてのオプションが含まれています。

ナビゲーション パス

（[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （4 ページ） 上で）ASA/PIX/FWSM の Web フィルタルールの [オプション（Options）] セルを右クリックし、[Web フィルタタイプの編集（Edit Web Filter Type）] を選択します。一度に 1 つの行のタイプを編集できます。

フィールド リファレンス

表 *4 : [Edit Web Filter Options]* ダイアログボックス

要素	説明
Allow traffic if URL Filter Server unavailable （URL、FTP、HTTPS のみ）	すべての URL フィルタリング サーバが使用できない場合に、アウトバウンド接続でのフィルタリングされていないトラフィックを許可するかどうか。このオプションを選択しなかった場合は、影響を受けるすべての発信トラフィック（HTTP、FTP、または HTTPS）は、少なくとも 1 台のフィルタリング サーバが使用できるようになるまで、ブロックされます。
HTTPプロキシサーバーへの接続をブロックする（Block connection to HTTP Proxy Server） （URL のみ）	ユーザによる HTTP プロキシ サーバへの接続を阻止するかどうか。
Truncate CGI request by removing CGI parameters （URL のみ）	URL に疑問符（?）で始まるパラメータ リスト（CGI スクリプトなど）が含まれている場合に、フィルタリング サーバに送信される URL に対して、その URL に含まれる疑問符と疑問符のあとのすべての文字を削除する切り捨てを行うかどうか。
絶対FTPパスが指定されていない場合にアウトバウンドリクエストをブロックする（Block outbound requests if absolute FTP path is not provided） （FTP のみ）	ユーザがディレクトリを変更しようとしたときに、ディレクトリ全体のパスを提供しない対話型 FTP セッションを阻止するかどうか。
長いURL（Long URL） （URL のみ）	フィルタリング サーバで許可されている最大数（Websense の場合は 4 KB、Smartfilter [N2H2] の場合は 3 KB）よりも大きい URL を処理する方法。多くの場合、長い URL はパラメータリストが原因であり、[CGIパラメータを削除することでCGI要求を切り捨てる（Truncate CGI request by removing CGI parameters）] オプションを使用して、それらの URL を処理できます。これ以外の長い URL の場合は、次のオプションから選択します。 • [Drop]：長い URL 要求をドロップします。 • [Truncate]：URL 要求を、URL のホスト名または IP アドレス部分だけに切り捨てます。 • [Deny]：URL 要求を拒否します。

IOS デバイス用の Web フィルタルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスの Web フィルタ ルール ポリシーでは、HTTP トラフィックを処理する方法を定義します。Web フィルタ ルールは、Web 要求に含まれる Universal Resource Locator（URL）アドレスに基づいてトラフィックを許可または拒否するインスペクション ルールのタイプです。アクセス ルールでインターフェイスの HTTP トラフィックを許可した場合、トラフィックが好ましくない Web サイトに向けられた場合に、あとからそのトラフィックを拒否（またはドロップ）できます。

IOS デバイスに Web フィルタリング ルールを設定するには、次の手順を実行します。

1. Web トラフィックをフィルタリングするインターフェイスを設定します（手順については次を参照してください）。
2. ローカル Web フィルタリング リストを設定して、常に許可または拒否する必要がある Web サイトを指定します（手順については、以下を参照してください）。
3. URL フィルタリング サーバを識別する Web フィルタ設定およびその他の設定を行います。詳細については、Web フィルタ サーバの設定 （21 ページ）を参照してください。

ヒント ゾーン ベースのファイアウォール ルールとして Web フィルタリングを設定することもできます。詳細については、ゾーンベースのファイアウォールルールの追加を参照してください。

関連項目

- Web フィルタ ルールについて （1 ページ）
- インターフェイス ロール オブジェクトについて
- ネットワーク/ホストオブジェクトについて

ステップ 1 次のいずれかを実行して、[Web Filter Rules] ページ（IOS） （17 ページ）を開きます。

- デバイスビュー：ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- ポリシービュー：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（IOS）（Web Filter Rules (IOS)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 HTTP トラフィックをフィルタリングするインターフェイスを設定します。フィルタリングをイネーブルにするインターフェイスごとに、次のようにルールを作成します。

a) [Webフィルタルール（Web Filter Rules）] タブがまだ選択されていない場合は選択し、次のいずれかを実行して [IOS Web Filter Rule and Applet Scanner] ダイアログボックス （18 ページ）を開きます。

- 新しいルールを作成するには、作業領域内を右クリックし、[行の追加（Add Row）] を選択します。
- 既存のルールを編集するには、ルールを右クリックし、[行の編集（Edit Row）] を選択します。

b) このルールを適用するインターフェイスを指定します。インターフェイスの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェースロールをリストから選択します。次の設定も行います。

- インターフェイスに関するトラフィックの方向：通常、デバイスがパケットの処理により多くの時間を費やす前に、望ましくないトラフィックがドロップされるように、[イン（In）] を選択します。
- J

  ava アプレットスキャン：インターフェイスで Web フィルタリングを有効にすると、パフォーマンスに影響する可能性のある Java アプレットが検査されます。通常は、Java アプレット スキャンをイネーブルにし、許可された送信元と拒否された送信元を識別して、拒否されたアプレットをスキャンしないようにできます。インターフェイスで許可されるソースと拒否されるソースの両方を設定する場合は、インターフェイスに 2 つのルールを設定する必要があります。

c) [OK] をクリックして Web フィルタリングルールテーブルにルールを追加します。

ステップ 3 （オプション）ローカルフィルタリング リストを定義する排他的ドメインのリストを設定します。このリストは、Web 要求が外部の Web フィルタリング サーバに送信される前に適用されます（ Web Filter 設定ページ （23 ページ）で定義）。常に許可（自社の Web サイトなど）または拒否する Web サイトがある場合は、ローカルリストにこれらのサイトを設定します。必要な数だけルールを設定し、すべてのリストを定義します。

a) [排他的ドメイン（Exclusive Domains）] タブをクリックし、次のいずれかを実行して [IOS Web Filter Exclusive Domain Name] ダイアログボックス （20 ページ）を開きます。

- 新しいルールを作成するには、作業領域内を右クリックし、[行の追加（Add Row）] を選択します。
- 既存のルールを編集するには、ルールを右クリックし、[行の編集（Edit Row）] を選択します。

b) 指定したドメインを許可するか拒否するかどうかを選択して、ドメイン名またはホスト IP アドレスを入力します。完全ドメイン名（特定 Web サイトの名前）または部分的な名前（同様に扱うすべてのドメイン）のいずれかを入力できます。

c) [OK] をクリックして、排他的ドメインルールをポリシーに追加します。

[Web Filter Rules] ページ（IOS）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

Web または URL フィルタリング ルールを設定するには、IOS デバイスの [Web Filter Rules] ページを使用します。Web フィルタリングは、HTTP インスペクションの一種です。アクセス規則でインターフェイス上の HTTP トラフィックを許可している場合は、規則を設定してローカルおよびサーバーベースの Web フィルタリングを適用すると、望ましくない Web サーバーへのユーザアクセスを防止できます。

Web フィルタルールを設定する場合は、[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] ポリシーで Web フィルタ設定も設定します。これらの設定は、Web フィルタリング サーバを識別し、ポリシーの機能全体を制御するその他の設定を含みます。たとえば、設定ポリシーを使用して、フィルタリングサーバーが使用できなくなった場合にすべての Web トラフィックを許可できます。詳細については、Web Filter 設定ページ （23 ページ）を参照してください。

ヒント ゾーン ベースのファイアウォール ルールとして Web フィルタリングを設定することもできます。詳細については、[Zone-based Firewall Rules] ページを参照してください。

ナビゲーション パス

IOS デバイスの [Webフィルタルール（Web Filter Rules）] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- （ポリシービュー）：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）IOS デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [Webフィルタルール（Web Filter Rules）]** を選択します。

関連項目

- Web フィルタ ルールについて （1 ページ）
- IOS デバイス用の Web フィルタルールの設定 （15 ページ）
- ファイアウォール Web フィルタ ルールの管理 （1 ページ）

フィールド リファレンス

表 *5 : [Web Filter Rules]* ページ（*IOS*）

要素	説明
[Web Filter Rules] タブ	ポリシーに定義された URL フィルタリング ルール。各ルールには、そのルールを定義したインターフェイス、ルールが着信または発信トラフィックに適用されるかどうか、および Java アプレット スキャンがイネーブルの場合に許可または拒否される Java アプレットの送信元が表示されます。Java アプレット スキャンに許可と拒否の両方を設定した場合、インターフェイスに 2 つ以上のルールが存在する場合があります。 • ルールを追加するには、[Add Row] ボタンをクリックし、[IOS Web Filter Rule and Applet Scanner] ダイアログボックス （18 ページ）に入力します。 • ルールを編集するには、ルールを選択し、[Edit Row] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。
[Exclusive Domains] タブ	ローカル Web フィルタ リスト。このリストは、Web 要求がフィルタリングサーバーに送信される前にチェックされ、Web フィルタリングを構成するすべてのインターフェイスに適用されます。 常に許可する特定のドメイン（組織の独自のドメイン名など）または禁止するドメインがあることがわかっている場合は、ここにリストすることができます。ローカルフィルタリストを構成すると、デバイスがフィルタリングサーバーからの応答を待つ必要がないため、パフォーマンスを向上させることができます。 • ドメインを追加するには、[Add Row] ボタンをクリックし、[IOS Web Filter Exclusive Domain Name] ダイアログボックス （20 ページ）に入力します。 • ドメインを編集するには、ドメインを選択し、[Edit Row] ボタンをクリックします。 • ドメインを削除するには、そのドメインを選択して [Delete Row] ボタンをクリックします。

[IOS Web Filter Rule and Applet Scanner] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスに Web フィルタリング ルールを作成するには、[IOS Web Filter Rule and Applet Scanner] ダイアログボックスを使用します。

ナビゲーション パス

このダイアログボックスを開くには、の [Webフィルタルール（Web Filter Rules）] タブを選択します。新しい [Web Filter Rules] ページ（IOS） （17 ページ）ルールを作成するには [行の追加（Add Row）] をクリックし、既存のルールを編集するには行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- IOS デバイス用の Web フィルタルールの設定 （15 ページ）
- Web フィルタ ルールについて （1 ページ）

フィールド リファレンス

表 *6 : [IOS Web Filter Rule and Applet Scanner]* ダイアログボックス

要素	説明
Enable Web Filtering	Web フィルタリング ルールをイネーブルにするかどうか。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイスロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについてを参照してください。
トラフィックの方向	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。

要素	説明
Java Applet Scanning Enable Java Applet Scanner	[Java アプレットスキャンを有効にする（Enable Java Applet Scanning）] を選択すると、デバイスは、Web サーバーから内部ホストへの HTTP トラフィックに Java アプレットが存在するかどうかをチェックします。Java アプレットが存在した場合、許可される送信元リストに Web サーバ（アプレット送信元）が含まれていれば、HTTP トラフィック内の Java アプレットは変更されません。存在しない場合、Java アプレットは HTTP ページから削除されます。 ヒント　Web フィルタリングを有効にすると、パフォーマンスに影響する可能性のある Java アプレットが検査されます。Java アプレットスキャナをイネーブルにすると、許可または拒否される送信元のリストを識別し、これらのアプレットを検査しないようにできます。送信元を拒否しない場合でも、スキャンをイネーブルにして**すべての**送信元を許可します。
Permit Traffic Applet Sources	Java アプレットを許可または拒否される送信元アドレスのリスト。許可または拒否された送信元のリストを設定するには、以下の手順に従います。 • [指定した送信元から許可する（Permit from Specified Sources）] または [指定した送信元から拒否する（Deny from Specified Sources）] を選択します。許可リストと拒否リストの両方を作成する場合は、2 つの別個の Web フィルタルールを作成します。許可リストを設定しなかった場合は、すべての送信元が拒否されます。 • [アプレットの送信元（Applet Sources）] フィールドに、許可されるアドレスまたは拒否されるアドレスのリストを入力します。このリストには、ホスト IP アドレス、ネットワーク アドレス、アドレス範囲、またはネットワーク/ホスト オブジェクトを含めることができますが、ドメイン名を含めることはできません。カンマで複数のアドレスを区切ります。アドレスを入力する方法の詳細については、ポリシー定義中の IP アドレスの指定を参照してください。

[IOS Web Filter Exclusive Domain Name] ダイアログボックス

（注）　バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスにローカル Web フィルタリング ルールを作成するには、[IOS Web Filter Exclusive Domain Name] ダイアログボックスを使用します。許可または拒否されるドメイン名または IP アドレスのリストを作成できます。デバイスは、Web フィルタリング サーバに Web 要求を転送する前に、このリストをチェックします。

ローカル フィルタリングを使用すると、常に許可または常に拒否するとわかっている Web サイトをユーザが要求した場合に、サーバから応答を受け取るまでの待機時間を節約できます。

ナビゲーション パス

このダイアログボックスを開くには、[Web Filter Rules] ページ（IOS） （17 ページ）の [排他的ドメイン（Exclusive Domains）] タブを選択します。新しいルールを作成するには [行の追加（Add Row）] をクリックし、既存のルールを編集するには行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- IOS デバイス用の Web フィルタルールの設定 （15 ページ）>
- Web フィルタ ルールについて （1 ページ）

フィールド リファレンス

表 *7 : [IOS Web Filter Exclusive Domain Name]* ダイアログボックス

要素	説明
トラフィック	一覧表示された Web サイトへのアクセスを許可するか、または拒否するかどうか。
ドメイン名	許可または拒否する Web サイトのドメイン名またはホスト IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。 ドメイン名の場合、完全な名前または部分的な名前を入力できます。たとえば、cisco.com には cisco.com ドメインのすべての Web サーバが含まれますが、www.cisco.com はワールドワイド ウェブ用の Web サーバだけを示します。

Web フィルタ サーバの設定

Web フィルタ ルール ポリシーとともに使用する Web フィルタ サーバの設定およびその他の設定を行うには、Web フィルタ設定ポリシーを使用します。Websense または Smartfilter（N2H2）のフィルタリング サーバを使用でき、（IOS デバイスの場合は）外部サーバを使用しないことも可能です。

ポリシーを設定および配置する前に、サーバのマニュアルで指示されているように Web フィルタ サーバをインストールおよび設定する必要があります。Security Manager は、サーバが存在すること、またはサーバが適切に設定されていることを確認できません。

ヒント これらの設定は、Web フィルタ ルール ポリシーでだけ機能します。ここで設定した Web サーバは、Web コンテンツ フィルタリングを設定するゾーンベースのファイアウォール ルール ポリシーでは使用されません。

関連項目

- Web フィルタ ルールについて （1 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （2 ページ）
- IOS デバイス用の Web フィルタルールの設定 （15 ページ）

ステップ 1 次のいずれかを実行して、 Web Filter 設定ページ （23 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [Web フィルタ（Web Filter）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 使用する Web フィルタリングサーバーのタイプを [Web フィルタサーバーのタイプ（Web Filter Server Type）] フィールドで選択し、サーバーを Web フィルタリングサーバーのテーブルに追加します。複数のサーバーがある場合は、優先度順に追加します。リストの先頭のサーバーがプライマリサーバーです。

- サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Web Filter Server Configuration] ダイアログボックス （26 ページ）に入力します。
- サーバを編集するには、サーバを選択し、[Edit Row] ボタンをクリックします。
- サーバを削除するには、サーバを選択し、[Delete Row] ボタンをクリックします。

ステップ 3 設定ポリシーの下半分には、設定可能なデバイス固有のオプションが含まれています。各設定の詳細については、 Web Filter 設定ページ （23 ページ）を参照してください。設定の概要は次のとおりです。

- IOS デバイス：最も重要な設定は [サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）] です。この設定では、フィルタリングサーバーが利用不能な場合に Web 接続を許可するかどうかを指定します。このオプションを選択しないと、何らかの理由でサーバがオフラインになった場合にすべての Web トラフィックが削除されます。

残りの設定では、ロギングおよびキャッシュ サイズのオプションを設定します。

- ASA、PIX、FWSM デバイス：これらのオプションでは、フィルタリング サーバで使用されるキャッシュ サイズおよびバッファ制限を設定します。また、フィルタリングサーバーの設定に応じて、キャッシュされた応答に送信元と宛先の両方を含めるか（ユーザごとに異なるフィルタリングポリシーがある場合）、宛先のみを含めるか（すべてのユーザに対して 1 つのポリシー）を制御することもできます。

Web Filter 設定ページ

[Webフィルタ設定（Web Filter Settings）] ページを使用して、Web フィルタルールポリシーとともに使用する Web フィルタサーバーの設定およびその他の設定を行います。

ポリシーを設定および配置する前に、サーバのマニュアルで指示されているように Web フィルタ サーバをインストールおよび設定する必要があります。Security Manager は、サーバが存在すること、またはサーバが適切に設定されていることを確認できません。

ヒント　これらの設定は、Web フィルタ ルール ポリシーでだけ機能します。ここで設定した Web サーバは、Web コンテンツ フィルタリングを設定するゾーンベースのファイアウォール ルール ポリシーでは使用されません。

ナビゲーション パス

[Web Filter settings] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [Webフィルタ（Web Filter）]** を選択します。

関連項目

- Web フィルタ ルールについて （1 ページ）
- Web フィルタ サーバの設定 （21 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （2 ページ）
- IOS デバイス用の Web フィルタルールの設定 （15 ページ）

フィールド リファレンス

表 *8 : [Web Filter]* ページ

要素	説明
Web Filter Server Type	使用する Web フィルタ サーバのタイプ。 • [None]：Web フィルタ サーバを使用しません。 • [Websense]：Websense サーバを使用します。 • [Secure Computing SmartFilter/N2H2]：Smartfilter サーバを使用します。このオプションを選択した場合は、通信に使用するサーバーポートを [ポート（Port）] フィールドで指定できます。 **ヒント** この設定を変更した場合は、既存のサーバ リストをテーブルから削除するように要求されます。[はい（Yes）] をクリックしても、テーブルはクリアされません。このプロンプトは、リストに間違ったタイプのサーバーが含まれている可能性があることを通知するために表示されます。
Webフィルタサーバーテーブル（Web Filter Servers table）	デバイスが Web フィルタリングに使用するサーバ。サーバはプライオリティ順に入力します。デバイスは、リストの先頭にあるサーバを使用し、そのサーバが応答しなくなると、応答を受け取るようになるまでリストの次のサーバに移行します。 フィルタタイプで [なし（None）] を選択すると、このリストは無視されます。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Web Filter Server Configuration] ダイアログボックス（26 ページ）に入力します。 • サーバーを編集するには、サーバーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • サーバーを削除するには、サーバーを選択し、[行の削除（Delete Row）] ボタンをクリックします。
IOS 固有の設定	

要素	説明
サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）	Web フィルタ サーバから応答がない場合に、デバイスが Web トラフィックを許可するかどうか。このオプションを選択しない場合は、サーバがオンラインに戻るまで、すべての Web アクセスが抑制されます。 サーバがダウンしているときの Web トラフィックを許可した場合、Web 要求はフィルタリングされず、すべての Web サーバへのアクセスが許可されます。
アラートの有効化（Enable Alerts）	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。
Enable Web Filter Server Logging	システム メッセージを URL フィルタリング サーバに送信してロギングするかどうか。デバイスは、URL ルックアップ要求の直後にログ要求を送信します。ログ要求には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。サーバーはログ要求を独自のログサーバーに記録するため、必要に応じてこの情報を表示できます。
キャッシュ サイズ（Cache Size）	デバイスでキャッシュ可能な宛先 IP アドレス（およびその認可ステータス）の最大数。デフォルト値は 5000 です。 キャッシュが 80 % まで一杯になると、デバイスは非アクティブなエントリを古い方から順に削除します。
Maximum Requests	ある特定の時点で存在する未処理要求の最大数。指定した数を超えた場合、新しい要求はドロップされます。デフォルトは 1000 です。
パケットバッファ	Web フィルタサーバーが要求を許可または拒否するのを待機している間に、デバイスのパケットバッファに格納できる HTTP 応答の最大数。最大値に達した場合、デバイスは応答をドロップします。デフォルト（最大値）は 200 です。 ユーザが Web 要求を行うと、同時にデバイスが要求を Web サイトおよび Web フィルタリング サーバに送信します。サーバーが許可または拒否の応答を提供する前に Web サイトからの応答を受信した場合、デバイスはサーバーから応答を受け取るまで、要求をパケットバッファに保持します。 サーバーが応答した場合、またはサーバーを利用できないとデバイスが判断し、[サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）] も選択している場合、応答はバッファから削除されます。

要素	説明
PIX/ASA/FWSM 固有の設定	
Cache Match Criteria	Web 要求をキャッシュする方法。 • [Source] と [Destination]：キャッシュ エントリは、要求を開始するアドレスと宛先 Web アドレスの両方に基づいています。ユーザがフィルタリング サーバ上の同じフィルタリング ポリシーを共有しない場合は、このモードを選択します。 • [Destination]：キャッシュ エントリは、宛先 Web アドレスが基になります。すべてのユーザがフィルタリング サーバ上の同じフィルタリング ポリシーを共有する場合は、このモードを選択します。
URL Buffer Memory （ASA 7.2+、PIX 7.2+ のみ）	URL バッファ メモリ プールのサイズ（KB 単位）。値は 2 ～ 10240 です。
Maximum Allowed URL Size （ASA 7.2+、PIX 7.2+ のみ）	バッファ対象の URL ごとに許容される URL の最大サイズ（KB 単位）。使用できる値はサーバ タイプによって異なります。 • [Websense]：2 ～ 4 • [Smartfilter (N2H2)]：2 または 3
キャッシュ サイズ（Cache Size）	フィルタリングサーバーからの応答を格納するためのキャッシュのサイズ（KB 単位）。値は 1 ～ 128 です。 キャッシングにより、URL アクセス権限がセキュリティアプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは Websense サーバに要求を転送する代わりに、まず URL キャッシュを検索して一致するアクセス権限の有無を調べます。
URLブロックバッファの制限（URL Block Buffer Limit）	フィルタリングサーバのフィルタリング判定を待機している間、Web サーバ応答を格納しておくバッファのサイズ。値は 1 ～ 128 です。この値は、1550 バイトのブロックの数を示しています。

[Web Filter Server Configuration] ダイアログボックス

Web フィルタ ルール ポリシーとともに使用する外部 Web フィルタ サーバを設定するには、[Web Filter Server Configuration] ダイアログボックスを使用します。Websense サーバまたは Smartfilter（N2H2）サーバを設定できます。

ナビゲーション パス

Web Filter 設定ページ （23 ページ）から、[Web フィルタサーバー（Web Filter Servers）] テーブルの下にある [行の追加（Add Row）] をクリックするか、行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- Web フィルタ サーバの設定 （21 ページ）
- Web フィルタ ルールについて （1 ページ）

表 9 : [Web Filter Server Configuration] ダイアログボックス

要素	説明
コモン接点	
IPアドレス	Web フィルタ サーバの IP アドレス。
タイムアウト（Timeout）	デバイスが Web フィルタ サーバからの応答を待機する時間の長さ（秒単位）。デフォルトは 5 秒です。 複数のサーバーを設定している場合、要求がタイムアウトすると、デバイスは次のサーバーを試行します。
PIX/ASA/FWSM 固有の設定	
インターフェイス	認証サーバが配置されているネットワーク インターフェイス（FastEthernet0 など）。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。 インターフェイスの名前またはインターフェイスを識別するインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択します。あるいは、新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。
プロトコル	Web フィルタリング サーバと通信する場合に使用するプロトコル。サーバに設定されている次のオプションを選択します。 • TCP（バージョン 1） • TCP バージョン 4 • UDP バージョン 4
Connection Number	（任意）デバイスとサーバの間で許容される TCP 接続の最大数。
IOS 固有の設定	

要素	説明
Retransmit	サーバが応答しない場合に、デバイスが要求を再送信する回数。デフォルト値は 2 回です。
[ポート（Port）]	サーバが受信に使用するポート番号。デフォルトのポートは 15868 です。

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。