CHAPTER 23

Webtype アクセス コントロール リストの追加

Web-type ACL は、クライアントレス SSL VPN のフィルタリングをサポートするコンフィギュレーションに追加されます。この章では、WebVPN のフィルタリングをサポートするコンフィギュレーションに ACL を追加する方法について説明します。

この章の内容は、次のとおりです。

Web-type ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドラインと制限事項

Web-type ACL には、次のガイドラインと制限事項が適用されます。

- スマート トンネル ACE によるフィルタリングはサーバ ベースでのみ行われるため、ディレクトリに対するアクセスの許可または拒否、および特定のスマート トンネル対応アプリケーションに対するアクセスの許可または拒否を行うためにスマート トンネル ACE を作成することはできません。
- 1 つのプラットフォーム（Windows など）上で英語以外の文字で ACL に関する記述コメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

デフォルト設定値

表 23-1 に Web-type ACL パラメータのデフォルト設定値を示します。

表 23-1　デフォルトの Web-type ACL パラメータ

パラメータ	デフォルト
deny	特にアクセスを許可しない限り、ASA によって発信元インターフェイス上のすべてのパケットが拒否されます。
log	ACL ロギングは、拒否されたパケットについてシステム ログ メッセージ 106023 を生成します。拒否されたパケットをログに記録するには、拒否パケットが存在している必要があります。

Web-type ACL の使用

この項では、次のトピックについて取り上げます。

- 「Web-type ACL および Web-type ACE の追加」（P.23-3）
- 「Web-type ACL および Web-type ACE の編集」（P.23-4）
- 「Web-type ACL および Web-type ACE の削除」（P.23-5）

Web-type ACL 設定のタスク フロー

ACL を作成して実装するには、次のガイドラインを使用します。

- ACE を追加し、ACL 名を適用して、ACL を作成します。「Web-type ACL の使用」（P.23-2）を参照してください。

- ACL をインターフェイスに適用します。詳細については、ファイアウォール コンフィギュレーション ガイドの“Configuring Access Rules” section on page 46-8を参照してください。

Web-type ACL および Web-type ACE の追加

ACE を追加する場合は、追加先となる Web-type ACL をあらかじめ作成しておく必要があります。

（注） スマート トンネル ACE によるフィルタリングはサーバ ベースでのみ行われるため、ディレクトリに対するアクセスの許可または拒否、および特定のスマート トンネル対応アプリケーションに対するアクセスの許可または拒否を行うためにスマート トンネル ACE を作成することはできません。

Web-type ACL を設定するには、次の手順を実行します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Web ACLs] の順に選択します。

ステップ 2　[Add] をクリックし、さらに次のいずれかをクリックして、追加する ACL タイプを選択します。

- **Add ACL**
- **Add IPv6 ACL**

[Add ACL] ダイアログボックスが表示されます。

ステップ 3　ACL の名前を入力し（スペースは使用できません）、[OK] をクリックします。

ステップ 4　作成したリストにエントリを追加する場合は、[Add] をクリックし、ドロップダウン リストから [Add ACE] を選択します。

ステップ 5　[Action] フィールドで、目的のアクションに対応するオプション ボタンをクリックします。オプション ボタンは次のいずれかです。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

（注） 各 ACL には、末尾に暗黙的な拒否ルールがあります。

ステップ 6　[Filter] フィールドでは、フィルタリングを URL に基づいて行うか、アドレスおよびサービスに基づいて行うかを選択できます。

a. URL に基づいてフィルタリングを行う場合は、ドロップダウン リストから URL プレフィックスを選択し、[URL] フィールドに URL を入力します。

[URL] フィールドでは、次のようなワイルドカード文字を使用できます。

- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。
- 疑問符（?）は 任意の 1 文字と完全に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、http://www.cisco.com:80/ および http://www.cisco.com:81/ を一致対象とするには、次のように入力します。**http://www.cisco.com:8[01]/**

b. アドレスおよびサービスに基づいてフィルタリングを行う場合は、[Filter address and service] オプション ボタンをクリックし、適切な値を入力します。

[Address] フィールドでは、正規表現とともにワイルドカード文字を使用できます。

- アスタリスク（*）：空の文字列を含む任意の文字列に一致します。
- 疑問符（?）は 任意の 1 文字と完全に一致します。
- 角カッコ（[]）：文字の範囲を指定する際に使用する演算子です。角カッコ内に指定された範囲に属する任意の 1 文字に一致します。たとえば、10.2.2.20 ～ 10.2.2.31 の範囲の IP アドレスを許可する場合は、
10.2.2.[20-31] と入力します。

フィールドの端にある参照ボタンをクリックして、アドレスおよびサービスを参照することもできます。

ステップ 7　（任意）デフォルトでは、ロギングがイネーブルになっています。ロギングをディセーブルにするには、チェックボックスをオフにします。また、ドロップダウン リストからロギング レベルを変更することもできます。デフォルトのロギング レベルは [Informational] です。

ロギング オプションの詳細については、21-29 ページの「ログ オプション」を参照してください。

ステップ 8　（任意）ロギング レベルをデフォルト設定から変更する場合は、[More Options] をクリックしてリストを展開し、ロギング間隔を指定します。

有効値の範囲は 1 ～ 6000 秒です。デフォルトは 300 秒です。

ステップ 9　（任意）トラフィックをどのような場合に許可しどのような場合に拒否するかを指定するアクセス ルールに時間範囲を追加する場合は、[More Options] をクリックしてリストを展開します。

a. [Time Range] ドロップダウン リストの右側にある参照ボタンをクリックします。

b. [Browse Time Range] ダイアログボックスが表示されます。

c. [Add] をクリックします。

d. [Add Time Range] ダイアログボックスが表示されます。

e. [Time Range Name] フィールドに、時間範囲の名前を入力します。ただし、スペースは使用できません。

f. [Start Time] および [End Time] に、それぞれ開始時間および終了時間を入力します。

g. 毎日または隔週でその時間範囲がアクティブになるようにするなど、時間範囲に関する追加制限を指定する場合は、[Add] をクリックし、目的の値を指定します。

ステップ 10　[OK] をクリックすると、時間範囲について任意で指定した内容が適用されます。

ステップ 11　[Apply] をクリックして、設定を保存します

（注）　ACL を追加した後は、[IPv4 and IPv6]、[IPv4 Only]、[IPv6 Only] のうち、いずれかのオプション ボタンをクリックして、メイン ペインに表示する ACL をフィルタリングできます。

Web-type ACL および Web-type ACE の編集

Web-type ACL および Web-type ACT を編集するには、次の手順を実行します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Web ACLs] の順に選択します。

ステップ 2　次のいずれかのオプション ボタンをクリックして、編集する ACL タイプを選択します。

- [IPv4 and IPv6] : IPv4 アドレスと IPv6 アドレスの両方だけが含まれる ACL が表示されます。

- [IPv4 Only] : IPv4 タイプのアドレスだけが含まれる ACL が表示されます。
- [IPv6 Only] : IPv6 タイプのアドレスだけが含まれるアクセス ルールが表示されます。

選択したルール タイプに対応するインターフェイスが、メインの [Access Rule] ペインに表示されます。

ステップ 3　編集する ACE を選択し、必要に応じて値を変更します。

特定の値に関する詳細については、「Web-type ACL および Web-type ACE の追加」（P.23-3）を参照してください。

ステップ 4　[OK] をクリックします。

ステップ 5　[Apply] をクリックし、変更内容をコンフィギュレーションに保存します。

Web-type ACL および Web-type ACE の削除

Web-type ACE を削除するには、次の手順を実行します。

ステップ 1　[Configuration] > [Remote Access VPN] > [Clientless SSL VPN Access] > [Advanced] > [Web ACLs] の順に選択します。

ステップ 2　次のいずれかのオプション ボタンをクリックして、編集する ACL タイプを選択します。

- [IPv4 and IPv6] : IPv4 アドレスと IPv6 アドレスの両方だけが含まれる ACL が表示されます。
- [IPv4 Only] : IPv4 タイプのアドレスだけが含まれる ACL が表示されます。
- [IPv6 Only] : IPv6 タイプのアドレスだけが含まれるアクセス ルールが表示されます。

選択したルール タイプに対応するインターフェイスが、メインの [Access Rule] ペインに表示されます。

ステップ 3　削除する ACE を選択します。

特定の ACE を選択した場合は、その ACE だけが削除されます。ACL を選択した場合は、その ACL およびそれに属するすべての ACE が削除されます。

ステップ 4　[Delete] をクリックします。

選択した項目が、ビュー ペインから削除されます。

（注）　誤って削除した項目を元に戻す場合は、[Apply] をクリックする前に、[Reset] をクリックします。削除された項目が再び、ビュー ペインに表示されます。

ステップ 5　[Apply] をクリックし、変更内容をコンフィギュレーションに保存します。

Web-type ACL の機能の履歴

表 23-2 に、この機能のリリース履歴を示します。

表 23-2　Web-type ACL の機能の履歴

機能名	リリース	機能情報
Web-type ACL	7.0(1)	Web-type ACL は、クライアントレス SSL VPN のフィルタリングをサポートするコンフィギュレーションに追加される ACL です。 この機能が導入されました。
IPv4 および IPv6 の統合 ACL	9.0(1)	ACL で IPv4 および IPv6 アドレスがサポートされるようになりました。送信元および宛先に対して IPv4 および IPv6 アドレスの組み合わせも指定できます。IPv6 固有の ACL は非推奨です。既存の IPv6 ACL は拡張 ACL に移行されます。移行の詳細については、リリース ノートを参照してください。 次の画面が変更されました。 [Configuration] > [Firewall] > [Access Rules] [Configuration] > [Remote Access VPN] > [Network（Client）Access] > [Group Policies] > [General] > [More Options]