



CHAPTER 23

Webtype アクセス コントロール リストの追加

Webtype アクセス リストは、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します。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アクセス リスト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。

- 「Webtype アクセス リストのライセンス要件」 (P.23-1)
- 「注意事項と制限事項」 (P.23-1)
- 「デフォルト設定値」 (P.23-2)
- 「Webtype アクセス リストの使用」 (P.23-3)
- 「次の作業」 (P.23-6)
- 「Webtype アクセス リストのモニタリング」 (P.23-6)
- 「Webtype アクセス リストの設定例」 (P.23-7)
- 「Webtype アクセス リストの機能履歴」 (P.23-8)

Webtype アクセス リストのライセンス要件

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」 (P.23-2)
- 「ファイアウォール モードのガイドライン」 (P.23-2)
- 「その他のガイドラインと制限事項」 (P.23-2)

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

Webtype アクセス リストには、次のガイドラインと制限事項が適用されます。

- **access-list webtype** コマンドは、クライアントレス SSL VPN フィルタリングを設定するために使用します。URL には、完全な URL またはファイルを除いた部分的な URL を指定できます。また、サーバのワイルドカードを含めたり、ポートを指定したりできます。URL 文字列でのワイルドカード文字の使用方法については、「[URL 文字列を含む Webtype アクセス リストの追加](#)」(P.23-4) を参照してください。
- 有効なプロトコル識別子は、http、https、cifs、imap4、pop3、および smtp です。URL には、任意の URL を表すキーワード **any** を含めることもできます。アスタリスクを使用して、DNS 名のサブコンポーネントを表すことができます。
- ダイナミック ACL が IPv6 ACL をサポートするように拡張されています。IPv4 ACL および IPv6 ACL の両方を設定した場合は、これらの ACL がダイナミック ACL に変換されます。
- Access Control Server (ACS) を使用する場合は、cisco-av-pair 属性を使用して IPv6 ACL を設定する必要があります。ダウンロード可能 ACL は ACS GUI ではサポートされません。

デフォルト設定値

表 23-1 に、Webtype アクセス リスト パラメータのデフォルトの設定を示します。

表 23-1 Webtype アクセス リストのデフォルト 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	アクセス リスト 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。

Webtype アクセス リストの使用

この項では、次のトピックについて取り上げます。

- 「Webtype アクセス リストの設定のタスク フロー」 (P.23-3)
- 「URL 文字列を含む Webtype アクセス リストの追加」 (P.23-4)
- 「IP アドレスを含む Webtype アクセス リストの追加」 (P.23-5)
- 「アクセス リストへのコメントの追加」 (P.23-6)


Webtype アクセス リストの設定のタスク フロー

アクセス リスト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、アクセス リスト名を適用して、アクセス リストを作成します。「Webtype アクセス リストの使用」 (P.23-3) を参照してください。
- アクセス リストをインターフェイスに適用します。詳細については、「アクセス ルールの設定」 (P.42-8) を参照してください。

URL 文字列を含む Webtype アクセス リストの追加

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アクセス リストを追加するには、次のコマンドを入力します。

コマンド	目的
<pre>access-list access_list_name webtype {deny permit} url [url_string any] [log[[disable default] level] interval secs][time_range name]]</pre> <p>例：</p> <pre>hostname(config)# access-list acl_company webtype deny url http://*.cisco.example</pre>	<p>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アクセス リストを追加します。</p> <p><i>access_list_name</i> 引数には、アクセス リストの名前または番号を指定します。</p> <p>any キーワードは、すべての URL を指定します。</p> <p>deny キーワードは、条件が一致した場合にアクセスを拒否します。</p> <p>interval オプションでは、システム ログ メッセージ 106100 を生成する間隔を指定します。有効な値は 1 ~ 600 秒です。</p> <p>log [[disable default] <i>level</i>] オプションでは、ACE について syslog メッセージ 106100 を生成するように指定します。log オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトのレベルは 6 (情報) です。詳細については、log コマンドを参照してください。</p> <p>permit キーワードは、条件が一致した場合にアクセスを許可します。</p> <p>time_range name オプションでは、このアクセス リスト要素に time-range オプションを関連付けるためのキーワードを指定します。</p> <p>url キーワードは、フィルタリングに使用する URL を指定します。</p> <p>url_string オプションでは、フィルタリングされる URL を指定します。</p> <p>次のワイルドカード文字を使用すると、Webtype アクセス リスト エントリに複数のワイルドカードを定義できます。</p> <ul style="list-style-type: none"> 0 個以上の任意の数の文字に一致させるには、アスタリスク「*」を入力します。 任意の 1 文字に正確に一致させるには、疑問符「?」を入力します。 範囲内の任意の 1 文字に一致する範囲演算子を作成するには、角カッコ「[]」を入力します。 <p> (注) 任意の http URL に一致させるには、http://* を入力する以前の方法の代わりに、http://*/* を入力する必要があります。</p> <p>アクセス リストを削除するには、このコマンドの no 形式を使用して、コンフィギュレーションに表示されるコマンド構文のすべての文字列を指定します。</p>

IP アドレスを含む Webtype アクセス リストの追加

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アクセス リストを追加するには、次のコマンドを入力します。

コマンド	目的
<pre>access-list access_list_name webtype {deny permit} tcp [host ip_address ip_address subnet_mask any] [oper port[port]] [log[[disable default] level] interval secs][time_range name]]</pre> <p>例 :</p> <pre>hostname(config)# access-list acl_company webtype permit tcp any</pre>	<p>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アクセス リストを追加します。</p> <p><i>access_list_name</i> 引数には、アクセス リストの名前または番号を指定します。</p> <p>any キーワードは、すべての IP アドレスを指定します。</p> <p>deny キーワードは、条件が一致した場合にアクセスを拒否します。</p> <p>host ip_address オプションでは、ホスト IP アドレスを指定します。</p> <p>interval オプションでは、システム ログ メッセージ 106100 を生成する間隔を指定します。有効な値は 1 ~ 600 秒です。</p> <p>ip_address ip_mask オプションでは、特定の IP アドレスおよびサブネット マスクを指定します。</p> <p>log [[disable default] level] オプションでは、ACE について syslog メッセージ 106100 を生成するように指定します。log オプション キーワードを指定した場合、システム ログ メッセージ 106100 のデフォルトのレベルは 6 (情報) です。詳細については、log コマンドを参照してください。</p> <p>permit キーワードは、条件が一致した場合にアクセスを許可します。</p> <p>port オプションでは、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。</p> <p>time_range name オプションでは、このアクセス リスト要素に time-range オプションを関連付けるためのキーワードを指定します。</p> <p>アクセス リストを削除するには、このコマンドの no 形式を使用して、コンフィギュレーションに表示されるコマンド構文のすべての文字列を指定します。</p>

アクセス リストへのコメントの追加

拡張アクセス リスト、EtherType アクセス リスト、IPv6 アクセス リスト、標準アクセス リスト、Webtype アクセス リストを含む任意のアクセス リストに、エンタリについてのコメントを追加できます。コメントにより、アクセス リストが理解しやすくなります。

最後に入力した **access-list** コマンドの後にコメントを追加するには、次のコマンドを入力します。

コマンド	目的
<pre>access-list access_list_name remark text</pre> <p>例： hostname(config)# access-list OUT remark - this is the inside admin address</p>	<p>最後に入力した access-list コマンドの後にコメントを追加します。</p> <p>テキストは 100 文字まで指定できます。テキストの先頭にスペースを入力できます。末尾のスペースは無視されます。</p> <p>いずれかの access-list コマンドの前にコメントを入力すると、コメントはアクセス リストの最初の行に表示されます。</p> <p>no access-list access_list_name コマンドを使用してアクセス リストを削除すると、コメントもすべて削除されます。</p>

例

各 ACE の前にコメントを追加できます。コメントはその場所でアクセス リストに表示されます。コメントの開始位置にダッシュ (-) を入力すると、ACE と区別しやすくなります。

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

次の作業

アクセス リストをインターフェイスに適用します。詳細については、「[アクセス ルールの設定](#)」(P.42-8) を参照してください。

Webtype アクセス リストのモニタリング

Webtype アクセス リストをモニタするには、次のコマンドを入力します。

コマンド	目的
<pre>show running-config access list</pre>	<p>ASA で実行されているアクセス リスト コンフィギュレーションを表示します。</p>

Webtype アクセス リストの設定例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

次の例は、特定のファイルへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url
https://www.example.com/dir/file.html
```

次の例は、任意の URL へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

次の例は、Webtype アクセス リストでワイルドカードを使用する方法を示しています。

- 次に、`http://www.example.com/` や `http://www.example.net/` などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.*ample/
```

- 次に、`http://www.cisco.com` や `ftp://www.example.com` などの URL に一致させる例を示します。

```
access-list test webtype permit url *://ww?.c*co*/
```

- 次の例は、`http://www.cisco.com:80` や `https://www.cisco.com:81` などの URL に一致します。

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上記の例の範囲演算子「`[]`」では、**0** または **1** のいずれかの文字が出現する可能性があるとして指定しています。

- 次に、`http://www.example.com` や `http://www.example.net` などの URL に一致させる例を示します。

```
access-list test webtype permit url http://www.[a-z]ample?*/
```

上記の例の範囲演算子「`[]`」では、**a** ~ **z** の任意の文字が出現する可能性があるとして指定しています。

- 次の例は、`http://www.cisco.com/anything/crazy/url/ddtscgiz` などの URL に一致します。

```
access-list test webtype permit url htt*://**/*cgi?*
```



(注)

任意の http URL に一致させるには、`http://*` を入力する以前のの方法の代わりに、`http://**/*` を入力する必要があります。

次の例は、Webtype アクセス リストを適用して、特定の CIFS 共有へのアクセスをディセーブルにする方法を示しています。

このシナリオでは、「shares」というルートフォルダに「Marketing_Reports」および「Sales_Reports」という 2 つのサブフォルダが格納されており、「shares/Marketing_Reports」フォルダへのアクセスを明示的に拒否しようとしています。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

ただし、上記のアクセス リストでは、暗黙的な「deny all」が理由で、すべてのサブフォルダ（「shares/Sales_Reports」および「shares/Marketing_Reports」）がアクセス不可能になり、これにはルートフォルダ（「shares」）も含まれます。

この問題を修正するには、ルート フォルダと残りのサブフォルダへのアクセスを許可する新しいアクセス リストを追加します。

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

Webtype アクセス リストの機能履歴

表 23-2 に、この機能のリリース履歴を示します。

表 23-2 Webtype アクセス リストの機能履歴

機能名	リリース	機能情報
Webtype アクセス リスト	7.0(1)	<p>Webtype アクセス リストは、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アクセス リストです。</p> <p>この機能および access-list webtype コマンドが導入されました。</p>
IPv4 および IPv6 の統合 ACL	9.0(1)	<p>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。</p> <p>access-list extended、access-list webtype の各コマンドが変更されました。</p> <p>ipv6 access-list、ipv6 access-list webtype、ipv6-vpn-filter の各コマンドが削除されました。</p>