CHAPTER 22

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。

- **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 Web-type ACL の追加」（P.22-3）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 22-1 に Web-type ACL パラメータのデフォルト設定値を示します。

表 22-1　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 設定のタスク フロー」（P.22-3）
- 「URL 文字列を含む Web-type ACL の追加」（P.22-3）

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.22-2）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 6-7 を参照してください。

URL 文字列を含む Web-type ACL 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 ACL 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
access-list *access_list_name* **webtype** {**deny** | **permit**} **url** {*url_string* | **any**} [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]] **例：** `hostname(config)# access-list acl_company webtype deny url http://*.cisco.example`	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 ACL を追加します。 *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。次のワイルドカード文字を使用すると、Web-type ACE に複数のワイルドカードを定義できます。 • 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。 **（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。 • **any** キーワードは、すべての URL を指定します。 **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。 **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。 **time_range** *name* オプションでは、このアクセス リスト エントリに 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。 ACL 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。

IP アドレスを含む Web-type ACL 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 ACL 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
access-list *access_list_name* **webtype** {**deny** | **permit**} **tcp** [*dest_address_argument*] [**eq** *port*] [**log**[[**disable** | **default**] | *level*] **interval** *secs*][**time_range** *name*]] **例：** `hostname(config)# access-list acl_company webtype permit tcp any`	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 を追加します。 *dest_address_argument* には、パケットの送信先 IP アドレスを指定します。 • **host** *ip_address*：IPv4 ホスト アドレスを指定します。 • *dest_ip_address mask*：IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。 • *ipv6-address*/*prefix-length*：IPv6 ホストまたはネットワーク アドレスとプレフィックスを指定します。 • **any**、**any4**、**any6**：**any** は IPv4 と IPv6 の両方のトラフィックを表し、**any4** は IPv4 トラフィックのみを表し、**any6** は any6 トラフィックのみを表します。 **eq** *port* は、次のポートのいずれかになります。**http**、**https**、**cifs**、**imap4**、**pop3**、**smtp**。 **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。 **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。デフォルトのレベルは 6（情報）です。 **time_range** *name* オプションでは、このアクセス リスト エントリに 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。 ACL 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。

ACL へのコメントの追加

拡張 ACL、EtherType ACL、IPv6 ACL、標準 ACL、および Web-type ACL を含む ACL のエントリに関するコメントを追加できます。コメントを追加すると、ACL 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
access-list *access_list_name* **remark** *text* **例：** `hostname(config)# access-list OUT remark - this is the inside admin address`	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。 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。 **access-list** コマンドの前にコメントを入力すると、そのコメントが ACL の最初の行となります。 **no access-list** *access_list_name* コマンドを使って ACL を削除すると、コメントもすべて削除されます。

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 ACL 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

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 6-7 を参照してください。

Web-type ACL のモニタリング

Web-type ACL 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
show running-config access-list	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。

Web-type ACL 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、Web-type ACL 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://wwz.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://* を入力する以前の方法の代わりに、**http://*/*** を入力する必要があります。

次の例は、Web-type ACL 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 ACL 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 ACL を追加します。

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

Web-type ACL の機能の履歴

表 22-2 に、この機能のリリース履歴を示します。

表 22-2　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。 この機能および **access-list webtype** コマンドが導入されました。
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。 **access-list extended**、**access-list webtype** の各コマンドが変更されました。 **ipv6 access-list**、**ipv6 access-list webtype**、**ipv6-vpn-filter** の各コマンドが削除されました。