CHAPTER 22

テンプレート ACL の設定

RADIUS アトリビュート 242 を使用してユーザ プロファイルを設定すると、ユーザ単位の類似した Access Control List（ACL; アクセス コントロール リスト）を単一のテンプレート ACL に置き換えることができます。これは、1 つの ACL が類似した多数の ACL を表すことを意味します。Cisco IOS Release 12.2(28)SB では、テンプレート ACL を使用することによって、Cisco 10000 シリーズ ルータで使用できる ACL の総数を増やしながら、ACL 処理によるメモリと CPU の使用量を抑えることができます。

テンプレート ACL 機能は、何万人という加入者がいるブロードバンド環境のお客様に役立ちます。それぞれの加入者に一意の ACL を使用しているネットワーク実装では、Cisco 10000 シリーズ ルータで使用できる最大リソース量を簡単に超えます。各加入者が専用の ACL を持つネットワークでは、ユーザの IP アドレスを除く、各ユーザの ACL が同じになることがよくあります。テンプレート ACL は、多数の共通の Access Control Element（ACE）を単一の ACL にグループ化して、この問題を軽減します。これによりコンパイルの速度が速くなり、システム リソースを節約できます。テンプレート ACL 機能によって、サービス プロバイダーは、RADIUS アトリビュート 242 を使用して最大 60,000 の加入者に対して一意の ACL をプロビジョニングできます。ACL の設定は、前の Cisco IOS バージョンから変わっていません。

たとえば、次の例は、アトリビュート 242 を使用して送信できる、2 人の異なるユーザの 2 つの ACL を示します。

```
ip access-list extended Virtual-Access1.1#1
permit igmp any host 1.1.1.1
permit icmp host 1.1.1.1 any
deny ip host 44.33.66.36 host 1.1.1.1
deny tcp host 1.1.1.1 44.33.66.36
permit udp any host 1.1.1.1
permit udp host 1.1.1.1 any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1

ip access-list extended Virtual-Access1.1#2
permit igmp any host 13.1.1.2
permit icmp host 13.1.1.2 any
deny ip host 44.33.66.36 host 13.1.1.2
deny tcp host 13.1.1.2 44.33.66.36
permit udp any host 13.1.1.2
permit udp host 13.1.1.2 any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1
```

テンプレート ACL 機能がイネーブルの場合、これらの 2 つの ACL が類似しているとみなされ、新しいテンプレート ACL が次のように作成されます。

```
ip access-list extended 4_Temp_<random-number>
permit igmp any host <PeerIP>
permit icmp host <PeerIP> any
deny ip host 44.33.66.36 host <PeerIP>
deny tcp host <PeerIP> 44.33.66.36
permit udp any host <PeerIP>
permit udp host <PeerIP> any
permit udp any host 192.168.2.1
permit udp any host 192.170.2.1
permit icmp host 42.55.15.4 host 192.168.2.1
permit udp 11.22.11.0 0.0.0.255 host 192.177.2.1
permit tcp any host 192.170.2.1
permit ip host 42.55.15.4 host 192.168.2.1
permit tcp 11.22.11.0 0.0.0.255 host 192.177.2.1
```

そのため、この例では、IP アドレスが次のように対応付けられます。

- Virtual-Access1.1#1　1.1.1.1
- Virtual-Access1.1#2　13.1.1.2

PXF エンジンは、パケットの送信元または宛先のユーザを認識しているので、比較するためのユーザ IP を IP アドレス テーブルから取得できます。

テンプレート ACL は、RADIUS アトリビュート 242 で設定されたユーザ単位の ACL でのみアクティブになります。その他のタイプの ACL は、テンプレート ACL の影響を受けません。デフォルトではテンプレート ACL 機能がイネーブルにされており、すべてのアトリビュート 242 ACL がテンプレート ステータスの対象になります。

access-list template *number* コマンドを使用して、*number* 以下のルール数を持つ ACL だけにテンプレート ACL ステータスを制限できます。デフォルト設定は 100 ルールです。これは、大半のアトリビュート 242 ACL よりも大きい値になります。

次のトピックで、テンプレート ACL 機能について説明します。

テンプレート ACL 機能の履歴

Cisco IOS リリース	説明	必要な PRE
12.2(28)SB	この機能が Cisco 10000 シリーズ ルータに導入されました。	PRE2
12.2(31)SB2	PRE3 のサポートが追加されました。	PRE3

テンプレート ACL の設定作業

RADIUS アトリビュート 242 を使用して ACL を設定した場合、テンプレート ACL がデフォルトによってイネーブルになります。テンプレート ACL の設定作業には、次の内容が含まれます。

テンプレート ACL の最大サイズの設定（任意）

デフォルトでは、テンプレート ACL ステータスが 100 以下のルール数を持つ ACL に制限されています。この値を低く設定できます。

テンプレート ACL の最大ルール数を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

```
Router(config)# access-list template number
```

number の有効範囲は、1 ～ 100 です。

例 22-1 に、各ユーザの ACL のルール数が 50 以下のテンプレート ACL 処理の設定を示します。

例 22-1　テンプレート ACL の設定

```
Router(config)# access-list template 50
Router(config)#
```

RADIUS アトリビュート 242 を使用した ACL の設定

テンプレート ACL の処理が行われるのは、RADIUS アトリビュート 242 を使用して設定された ACL だけです。アトリビュート 242 には、次の形式の IP データ フィルタがあります。

Ascend-Data-Filter = “ip <dir> <action> [dstip <dest_ipaddr\subnet_mask>] [srcp <src_ipaddr\subnet_mask>] [<proto> [dstport <cmp> <value>] [srcport <cmp> <value>] [<est>]]”

表 22-1 に、IP データ フィルタに対するアトリビュート 242 エントリの要素について説明します。

表 22-1　IP データ フィルタの構文要素

要素	説明
ip	IP フィルタを指定します。
<dir>	フィルタの方向を指定します。有効値は、**in**（ルータに着信するパケットのフィルタリング）または **out**（ルータから発信されるパケットのフィルタリング）です。
action	フィルタに一致するパケットに対してルータが行うアクションを指定します。有効値は、**forward** または **drop** です。
dstip <dest_ipaddr\subnet_mask>	宛先 IP アドレス フィルタリングをイネーブルにします。宛先アドレスが **<dest_ipaddr>** の値に一致するパケットに適用します。アドレスにサブネット マスクの部分が存在する場合、ルータはマスク ビットだけを比較します。**<dest_ipaddr>** を 0.0.0.0 に設定した場合、またはこのキーワードが存在しない場合、フィルタがすべての IP パケットに一致します。
srcp<src_ipaddr\subnet_mask>	送信元 IP アドレス フィルタリングをイネーブルにします。送信元アドレスが **<src_ipaddr>** の値に一致するパケットに適用します。アドレスにサブネット マスクの部分が存在する場合、ルータはマスク ビットだけを比較します。**<src_ipaddr>** を 0.0.0.0 に設定した場合、またはこのキーワードが存在しない場合、フィルタがすべての IP パケットに一致します。
<proto>	名前または番号で指定されるプロトコルを指定します。プロトコル フィールドがこの値に一致するパケットに適用されます。有効な名前と番号は、**icmp**（**1**）、**tcp**（**6**）、**udp**（**17**）、および **ospf**（**89**）です。この値をゼロ（0）に設定した場合、フィルタがすべてのプロトコルに一致します。
dstport <cmp> <value>	宛先ポート フィルタリングをイネーブルにします。このキーワードは、**<proto>** を **tcp**（**6**）または **udp**（**17**）に設定した場合にのみ有効です。宛先ポートを指定しないと、フィルタがすべてのプロトコルに一致します。 **<cmp>** は、指定した **<value>** を実際の宛先ポートと比較する方法を定義します。有効値は、**<**、**=**、**>**、または **!** です。 **<value>** には、名前または番号を指定できます。有効な名前と番号は、**ftp-data**（**20**）、**ftp**（**21**）、**telnet**（**23**）、**nameserver**（**42**）、**domain**（**53**）、**tftp**（**69**）、**gopher**（**70**）、**finger**（**79**）、**www**（**80**）、**kerberos**（**88**）、**hostname**（**101**）、**nntp**（**119**）、**ntp**（**123**）、**exec**（**512**）、**login**（**513**）、**cmd**（**514**）、および **talk**（**517**）です。

表 22-1　IP データ フィルタの構文要素（続き）

要素	説明
srcportcmp <cmp> <value>	送信元ポート フィルタリングをイネーブルにします。このキーワードは、**<proto>** を **tcp**（**6**）または **udp**（**17**）に設定した場合にのみ有効です。送信元ポートを指定しないと、フィルタがすべてのプロトコルに一致します。 **<cmp>** は、指定した **<value>** を実際の宛先ポートと比較する方法を定義します。有効値は、<、=、>、または **!** です。 **<value>** には、名前または番号を指定できます。有効な名前と番号は、**ftp-data**（**20**）、**ftp**（**21**）、**telnet**（**23**）、**nameserver**（**42**）、**domain**（**53**）、**tftp**（**69**）、**gopher**（**70**）、**finger**（**79**）、**www**（**80**）、**kerberos**（**88**）、**hostname**（**101**）、**nntp**（**119**）、**ntp**（**123**）、**exec**（**512**）、**login**（**513**）、**cmd**（**514**）、および **talk**（**517**）です。
<est>	1 に設定すると、TCP セッションがすでに確立されている場合にのみフィルタがパケットの照合を行うことが指定されます。この引数が有効なのは、**<proto>** を **tcp**（**6**）に設定した場合だけです。

例 22-2 に、4 つのアトリビュート 242 の IP データ フィルタ エントリを示します。

例 22-2　RADIUS アトリビュート 242 の IP データ フィルタ エントリ

```
Ascend-Data-Filter=”ip in drop”
Ascend-Data-Filter=”ip out forward tcp”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16
dstport!=telnet”
Ascend-Data-Filter=”ip out forward tcp dstip 10.0.200.3/16 srcip 10.0.200.25/16 icmp”
```

テンプレート ACL 設定のモニタおよびメンテナンス

テンプレート ACL 機能の設定をモニタおよびメンテナンスするには、EXEC モードで次のコマンドのいずれか 1 つを入力します。

コマンド	目的
`Router# show access-list template summary`	すべてのテンプレート ACL に関する情報を表示します。
`Router# show access-list template` *acl-name*	指定されたテンプレート ACL に関する情報を表示します。
`Router# show access-list template exceed` *number*	*number* 以上の子 ACL の親としての役割を果たすすべてのテンプレート ACL の名前を表示します。
`Router# show access-list template tree`	Red-Black データ ツリーのエントリに関する情報を表示します。
`Router# show pxf cpu access security`	PXF セキュリティ ACL の統計情報を表示します。 このコマンドは、テンプレート ACL に関連する個々の子 ACL を表示しません。関連するすべての子 ACL を表す総合的な統計情報でテンプレート ACL の親を表示します。

テンプレート ACL の設定例

テンプレート ACL は、RADIUS アトリビュート 242 で設定されたユーザ単位の ACL でのみアクティブになります。RADIUS アトリビュートの他の設定例については、第 16 章「RADIUS 機能の設定」を参照してください。

access-list template コマンド

テンプレート ACL 処理をイネーブルにするには、グローバル コンフィギュレーション モードで **access-list template** コマンドを使用します。テンプレート ACL 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

テンプレート ACL 機能は、デフォルトでイネーブルにされています。テンプレート ACL ステータスのデフォルトのルール数は 100 です。これは、アトリビュート 242 を使用して設定される大半の ACL より大きい値になります。

コマンド	目的
`Router(config)# access-list template` *number*	テンプレート ACL 処理をイネーブルにします。 *number* は、テンプレート ステータスの対象になる ACL の最大の長さを指定します。*number* 以下のルール数を持つ ACL だけがテンプレート ステータスの対象になります。 *number* 変数を省略すると、デフォルトの 100 が使用され、100 以下のルール数を持つ ACL だけがテンプレート ステータスの対象になります。 デフォルトは、100 ルールです。

access-list template コマンド履歴

Cisco IOS リリース	説明
12.2(28)SB	このコマンドが Cisco 10000 シリーズ ルータに導入されました。

access-list template コマンド モード

このコマンドは、グローバル コンフィギュレーション モードで使用します。

access-list template コマンドの使用上のガイドライン

テンプレート ACL ステータスのルール数を減らすと、CPU 利用率を低く抑えることができます。照合タスクを早期に打ち切ることができる場合は、システム内の他の既知の ACL に各 ACL を照合する処理の方が簡単です。ただし、数値を低く設定しすぎると（最大の「類似した」アトリビュート 242 ACL より小さい場合）、ルータにすでに存在する他の ACL が無視されて、テンプレート ACL の複製としてみなされた ACL が PXF に送信されるようになるので、CPU 利用率がとても高くなる可能性があります。

比較タスクは CPU を消費するので、ルール数を高く設定すると CPU 利用率が高くなる可能性があります。

（注）　CPU 利用率は、セッションの開始時にのみ変化します。定常状態の CPU 利用率は、ACL 処理のこのような変更には影響されません。

例

次の例は、50 以上のルール数を持つ ACL をテンプレート ACL ステータスの対象として指定しています。

```
Router# access-list template 50
```

show access-list template コマンド

テンプレート ACL に関する情報を表示するには、EXEC モードで **show access-list template** コマンドを使用します。

コマンド	目的
Router# **show access-list template** {**summary** | *aclname* | **exceed** *number* | **tree**}	ACL に関する情報を表示します。 **summary** は、サマリー情報を表示します。 *aclname* は、指定した ACL に関する情報を表示します。 ***exceed*** *number* は、*number* を超える個々の ACL を置き換えるテンプレート ACL を特定します。 ***tree*** は、テンプレート ACL 機能が参照する各 ACL タイプの使用頻度のサマリーを分かりやすい形式で提供します。 このコマンドの出力には、Red-Black ツリーの各エントリに対して次の情報が含まれます。 • Cyclic Redundancy Check 32-bit（CRC32）値 • 特定の CRC32 に関連する各 ACL については、次の内容です。 － プライマリ ACL の名前 － 該当する ACL のユーザ数

show access-list template コマンド モード

show access-list template コマンドは、EXEC モードで使用します。

show access-list template コマンド履歴

Cisco IOS リリース	説明
12.2(28)SB	このコマンドが Cisco 10000 シリーズ ルータに導入されました。

例

ここでは、**show access-list template** コマンドの異なる形式の例を示します。

show access-list template summary

次の例は、**show access-list template summary** コマンドの出力を示します。

```
Router# show access-list template summary
Maximum rules per template ACL = 100
Templates active = 1
Number of ACLs those templates represent = 50
Number of tree elements = 1
```

このコマンドの出力には、次の内容が含まれます。

- 各テンプレート ACL の最大ルール数
- 検出されたアクティブなテンプレート数
- これらのテンプレートによって置き換えられた ACL 数

show access-list template *aclname*

次の例は、**show access-list template** *aclname* コマンドの出力を示します。

```
Router# show access-list template 4Temp_1073741891108

    Showing data for 4Temp_1073741891108
    4Temp_1073741891108 peer_ip used is 172.17.2.62,
    is a parent, attached acl count = 98
    currentCRC = 59DAB725


Router# show access-list template 4Temp_1342177340101

    Showing data for 4Temp_1342177340101
    4Temp_1342177340101 idb's ip peer = 172.17.2.55,
    parent is 4Temp_1073741891108, user account attached to parent = 98
    currentCRC = 59DAB725
```

この出力には、次の内容が含まれます。

- 指定されたテンプレート ACL に関連するインターフェイスのピア IP
- 指定されたテンプレート ACL のプライマリ ユーザとしての役割を果たす ACL の名前
- 指定されたテンプレート ACL のテンプレートに一致する ACL 数
- 現在の CRC32 値

show access-list template exceed *number*

次の例は、**show access-list template exceed** *number* コマンドの出力を示します。

```
Router# show access-list template exceed 49
ACL name                          OrigCRC    Count     CalcCRC
4Temp_#120795960097               104FB543   50      104FB543
```

表 22-2 に、出力に表示される重要なフィールドについて説明します。

表 22-2　show access-list template exceed フィールドの説明

フィールド	説明
ACL Name	*number* ACL を超える各テンプレートのプライマリ ACL としての役割を果たす ACL の名前
OrigCRC	最初の CRC32 値
Count	テンプレート ACL に一致する ACL 数
CalcCRC	算出された CRC32 値

show access-list template tree

次の例は、**show access-list template tree** コマンドの出力を示します。

```
Router# show access-list template tree

ACL name              OrigCRC    Count   CalcCRC
4Temp_1073741891108   59DAB725   98      59DAB725
```

表 22-3 に、出力に表示される重要なフィールドについて説明します。

表 22-3　show access-list template tree フィールドの説明

フィールド	説明
ACL name	Red-Black ツリーの ACL の名前
OrigCRC	最初の CRC32 値
Count	ACL のユーザ数
CalcCRC	算出された CRC32 値