



WAE の IP ACL の作成と管理

この章では、Wide Area Application Engine (WAE) 上で Internet Protocol (IP; インターネット プロトコル) Access Control List (ACL; アクセス コントロール リスト) を作成および管理する方法について説明します。この章には、次の項があります。

- [WAE の IP ACL について、10-2 ページ](#)
- [IP ACL を使用した基本的な作業、10-5 ページ](#)
- [WAE での IP ACL の定義および有効化、10-7 ページ](#)
- [WAE での IP ACL の作成または変更、10-11 ページ](#)
- [インターフェイスでの IP ACL の有効化、10-13 ページ](#)
- [IP ACL のアプリケーションへの適用、10-14 ページ](#)
- [IP ACL の削除、10-18 ページ](#)
- [IP ACL の設定の表示、10-19 ページ](#)
- [IP ACL カウンタのクリア、10-20 ページ](#)



(注) この章全体を通じて、*IP ACL* という用語は、IP アクセス コントロール リストを指しています。

Cisco WAFS 3.0 ソフトウェアは、FE-511 File Engine と、WAE-611 および WAE-7326 Wide Area Application Engine で稼働します。簡潔にするため、説明文の中や使用例のコマンド プロンプトの部分では、単に WAE と記述していますが、特に注釈がないかぎり、3 つのプラットフォームすべてに当てはまります。

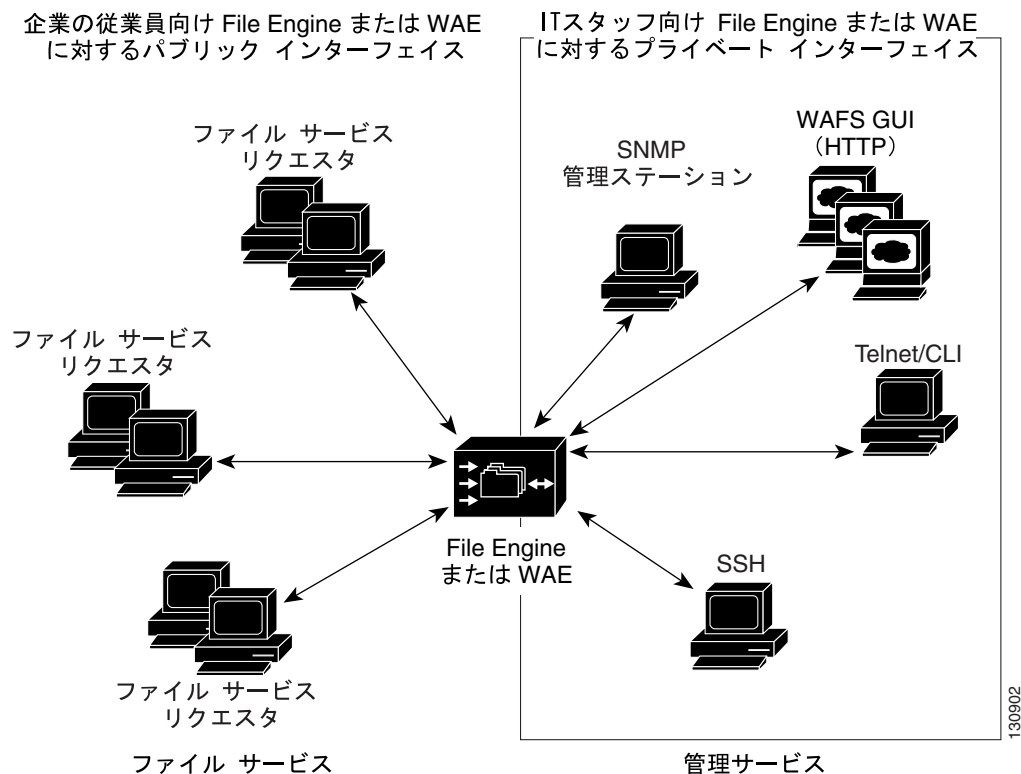
この章で取り上げる CLI コマンドの完全な構文と使用方法の詳細については、『*Cisco WAFS 3.0 Command Reference*』を参照してください。

WAE の IP ACL について

WAFS 3.0 は、IP パケット フィルタリングとともに IP ACL をサポートしています。この IP ACL は、WAE 上の特定のインターフェイスを経由してきた IP パケットの許可または拒否できるようにすることで、パケットをフィルタする手段を提供します。

WAE 上のファイル サービスと管理サービスへのアクセスを制御するために、この機能を使用する場合があります。たとえば、IP ACL を使用して、WAE にファイル サービス用のパブリック インターフェイスを定義したり、Telnet、Secure Shell (SSH)、SNMP、HTTP、ソフトウェア アップグレードなどの管理サービス用のプライベート インターフェイスを定義したりできます。図 10-1 を参照してください。

図 10-1 IP ACL を使用した WAE 上の特定のインターフェイスへのアクセスの制御



次の例は、WAE がある環境で、IP ACL を使用方法を示しています。

- WAE は顧客宅内に常駐し、サービス プロバイダーによって管理されています。サービス プロバイダーは、その管理対象のデバイスの安全性を確保することだけを考えています。
- WAE は、企業内の任意の場所に配置されます。ルータおよびスイッチと同様に、管理者は、Telnet、SSH、および WAFS Manager GUI から IT ソース サブネットへのアクセスを制限することを望んでいます。

WAE の IP ACL の実装

IP ACL を実装する手順は、次のとおりです。

-
- ステップ 1 **ip access-list** コマンドを使用して、WAE に IP ACL を定義します。
- ステップ 2 **ip access-group** コマンドを使用して、定義された IP ACL を WAE のインターフェイスの発信側または着信側のどちらかに適用します。
-



(注) また、IP ACL を使用して、この WAE への Telnet、SSH、および SNMP アクセスを許可または拒否できます。

IP ACL の定義および有効化の例

次の例は、WAE に IP ACL を定義し有効化する方法を示しています。例に示すとおり、最初の手順では、**ip access-list** グローバル コンフィギュレーション コマンドを使用して、WAE の IP ACL を作成します。この場合、IP ACL に *example* という名前を付け、特定ホストへの GRE トンネリングを許可します。

```
WAE(config)# ip access-list extended example
WAE(config-ext-nacl)# permit gre any 10.101.215.21
WAE(config-ext-nacl)# exit
```

IP ACL を作成したら、次の手順で、**interface** グローバル コンフィギュレーション コマンドと **ip access-group** コンフィギュレーション インターフェイス コマンドを使用して、WAE 上の特定のインターフェイスに IP ACL を適用し、有効化します。

```
WAE(config)# interface gigabitethernet 1/0
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```

IP ACL を定義し有効にしたら、**show running-config EXEC** コマンドを使用して、WAE の実行コンフィギュレーションを表示します。

```
WAE# show running-config
.
.
.
!
interface GigabitEthernet 1/0
 ip address 10.1.1.50 255.255.0.0
 ip access-group example in
 exit
.
.
.
ip access-list extended example
 permit gre any 10.101.215.21
 exit
.
.
.
```



(注) IP ACL は、個々の WAFS ソフトウェア デバイスだけに定義されます。WAFS ネットワーク全体に渡り、またはサービス グループを通じて、IP ACL をグローバルに管理することはできません。

IP ACL の背景情報については、次の項の「[IP ACL を使用した基本的な作業](#)」を参照してください。IP ACL の設定方法の詳細については、[10-7 ページの「WAE での IP ACL の定義および有効化」](#)を参照してください。

IP ACL を使用した基本的な作業

IP ACL は、WAE が廃棄するか、またはさらに処理するために受け入れる、パケットの種類を指定した 1 つ以上の条件エントリから構成されます。WAE は、IP ACL 内で現れる順番で各条件を適用します。デフォルトでは、この順番は、条件を設定した順番です。

2 つのタイプの IP ACL がサポートされています。

- 標準 ACL
- 拡張 ACL



(注) WAE 上で IP ACL を作成し管理するには、WAFS ソフトウェア CLI を使用する必要があります。WAFS Manager GUI は、現在、WAE 上での IP ACL の設定をサポートしていません。

標準 IP ACL を使用した作業

通常、標準 ACL は、次の理由で使用されます。

- 特定の IP アドレスを持つホストからの接続を許可するため
- 特定のネットワーク上のホストからの接続を許可するため

標準 IP ACL コンフィギュレーション モードへのアクセス

標準 IP ACL を使用して作業するには、WAE の標準 IP ACL コンフィギュレーション モードに切り替える必要があります。標準 IP ACL コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードから `ip access-list standard` コマンドを入力します。

```
WAE(config)# ip access-list standard {acl-name | acl-num}
```

標準 IP ACL の名前は最大 30 文字長で、番号は 1 ~ 99 までの範囲です。標準 IP ACL モードに切り替えると、WAE(config)# プロンプトが WAE(config-std-nacl)# プロンプトに変わります。ここで、std-nacl は指定した標準アクセスリストの略です。

次の例は、標準 IP ACL コンフィギュレーション モードに切り替えて、ACL 番号 2 の標準 IP ACL を変更する方法を示しています。CLI を標準 IP ACL コンフィギュレーション モードに切り替えると、それ以降のすべてのコマンドは、現在指定されている標準 IP ACL (たとえば、標準 IP ACL 2) に適用されます。

```
WAE(config)# ip access-list standard 2
WAE(config-std-nacl)#
```



(注) 拡張 IP ACL を作成および変更する方法の詳細については、[10-11 ページの「WAE での IP ACL の作成または変更」](#)を参照してください。

拡張 IP ACL を使用した作業

拡張 IP ACL は、一般に、次の要素を使用して接続を制御します。

- 宛先 IP アドレス
- IP プロトコル タイプ
- UDP または TCP 送信元もしくは宛先ポート
- ICMP メッセージ タイプまたはコード
- TCP フラグ ビット (確立済み)

より限定的な条件を作成するために、これらの条件に送信元 IP アドレスに関する情報を組み合わせることができます。特定の Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル) メッセージ タイプとコードとの照合に使用できるキーワードについては、『Cisco WAFS 3.0 Command Reference』を参照してください。

拡張 IP ACL コンフィギュレーション モードへのアクセス

拡張 IP ACL を使用して作業するには、WAE の拡張 IP ACL コンフィギュレーション モードに切り替える必要があります。拡張 IP ACL コンフィギュレーション モードにアクセスするには、グローバル コンフィギュレーション モードから `ip access-list extended` コマンドを入力します。

```
WAE(config)# ip access-list extended {acl-name | acl-num}
```

拡張 IP ACL の名前は最大 30 文字長で、番号は 100 ~ 199 までの範囲です。拡張 IP ACL モードに切り替えると、`WAE(config)#` プロンプトが `WAE(config-ext-nacl)#` プロンプトに変わります。ここで、`ext-nacl` は指定した拡張アクセス リストの略です。

次の例は、拡張 IP ACL コンフィギュレーション モードに切り替えて、ACL 番号 101 の拡張 IP ACL を変更する方法を示しています。CLI を拡張 IP ACL コンフィギュレーション モードに切り替えると、それ以降のすべてのコマンドは、現在指定されている拡張 IP ACL (たとえば、拡張 IP ACL 101) に適用されます。

```
WAE(config)# ip access-list extended 101
WAE(config-ext-nacl)#
```



(注)

拡張 IP ACL を作成および変更する方法の詳細については、[10-11 ページの「WAE での IP ACL の作成または変更」](#)を参照してください。

WAE での IP ACL の定義および有効化

サービス プロバイダーの展開によっては、WAE は 1 つのインターフェイスを、ファイル サービス用のお客様の IP アドレス スペース内で保持し、もう 1 つのインターフェイスを、管理者が管理目的で使用するプライベート IP アドレス スペース内で保持することができます。WAFS 3.x は、さまざまなサービスを特定のインターフェイスに結合できる制御機能を提供しているため（管理サービスをプライベート IP スペースへ結合するなど）、企業のお客様がファイル サービスを利用するために WAE にアクセスし、管理目的では WAE にアクセスできないようにすることができます。

WAE で IP ACL を使用する手順は、次のとおりです。

ステップ 1 `ip access-list` コマンドを使用して、IP ACL を定義します。

ステップ 2 `interface` コマンドおよび `ip access-group` コマンドを使用して、IP ACL を WAE 上の特定のインターフェイスに適用します。



ヒント

`ip access-group` コマンドを使用して、IP ACL をインターフェイスの着信または発信 IP トラフィックのどちらかに適用します。

使用上のガイドライン

WAE 上で IP ACL を作成したり変更したりする場合は、次のガイドラインにしたがってください。

- 標準または拡張 IP ACL のエントリを作成するには、`deny` または `permit` キーワードを使用して、WAE が廃棄する、またはさらに処理するために受け入れる、パケットのタイプを指定します。デフォルトでは、リストが暗黙の `deny any` エントリで終了しているため、アクセス リストはすべてのものを拒否します。そのため、有効なアクセス リストを作成するには、少なくとも 1 つの `permit` エントリを含める必要があります。



(注) 特定のネットワークからの接続を許可するには、`permit source-ip wildcard` コマンドを使用します。`source-ip` は、指定するネットワーク上の任意のホストのネットワーク ID または IP アドレスで置き換えます。`wildcard` には、サブネット マスクを反転させた、0 が照合する必要がある位置を示し、1 が無視する位置を示しているドット付き 10 進表記のマスクを指定します。たとえば、`wildcard` に `0.0.0.255` と指定すると、送信元 IP アドレスの最後の 8 ビットは無視されます。したがって、エントリ `permit 192.168.1.0 0.0.0.255` は、`192.168.1.0` ネットワーク上の任意のホストからのアクセスを許可します。

- また、適切なコマンドを使用して、拡張 IP ACL を特定のアプリケーションに適用することもできます。存在しない IP ACL へのリファレンスは、`permit any` 条件文と同様に作用します。
- SNMP アプリケーションには、IP ACL の使用を設定するための固有の CLI コマンドがありません。コマンドは、次のとおりです。

```
snmp-server access-list {std-acl-num | std-acl-name}
```



(注) `snmp-server access-list` グローバル コンフィギュレーション コマンドは、標準 IP ACL の名前または番号を受け入れることができるだけで、拡張 IP ACL には対応していません。

その他のアプリケーショントラフィック(たとえば、Telnet や SSH)は、WAE のインターフェイス(通常は、着信トラフィック)に IP ACL を適用することで制御できます。

- WAE が WCCP GRE 着信トラフィックに対して適用する IP ACL を指定するには、**wccp access-list** グローバル コンフィギュレーション コマンドを使用します。

```
wccp access-list {acl-num | acl-name}
```

WCCP ACL 機能は、標準 ACL と拡張 ACL の両方をサポートします。WCCP ACL の設定方法の詳細については、10-15 ページの「WAE の WCCP ACL の設定」を参照してください。

- 標準 IP ACL の場合、**ip access-list** コマンドの **wildcard** パラメータは常にオプションです。標準 IP ACL に対して **host** キーワードを指定した場合は、次の例に示すとおり、**wildcard** パラメータは許容されません。

```
WAE(config)# ip access-list standard 1
WAE(config-std-nacl)# permit ?
  A.B.C.D Source address
  any      Any source host
  host     A single host address
WAE(config-std-nacl)# permit 10.1.1.1 ?
  A.B.C.D Source wildcard bits <=== *** Wildcard parameter is optional here ***
<cr>

WAE(config-std-nacl)# permit host 10.1.1.1 ? <=== *** Wildcard parameter is not
allowed here because the host keyword is used***
<cr>
WAE(config-std-nacl)# permit 10.1.1.1
WAE(config-std-nacl)# exit
```

- 拡張 IP ACL の場合、**host** キーワードが指定されていないかぎり、**wildcard** パラメータは常に必須です。拡張 IP ACL に対して **host** キーワードを指定した場合は、次の例に示すとおり、**wildcard** パラメータは許容されません。

```
WAE(config)# ip access-list extended 100
WAE(config-ext-nacl)# permit ?
<1-255> An IP Protocol Number
gre     Cisco's GRE Tunneling
icmp    Internet Control Message Protocol
ip      Any IP Protocol
tcp     Transport Control Protocol
udp     User Datagram Protocol
WAE(config-ext-nacl)# permit ip ?
  A.B.C.D Source address
  any      Any source host
  host     A single host address
WAE(config-ext-nacl)# permit ip 10.1.1.1 ?
  A.B.C.D Source wildcard bits <=== *** Wildcard parameter is required here
because the host keyword is not specified***
WAE(config-ext-nacl)# permit ip host ?
  A.B.C.D Source address
WAE(config-ext-nacl)# permit ip host 10.1.1.1 ? <=== *** Wildcard parameter is not
allowed here because the host keyword is used***
  A.B.C.D Destination address
  any      Any destination host
  host     A single host address
```

- 標準または拡張 IP ACL コンフィギュレーション モードでは、編集コマンド (`list`、`delete`、および `move`) を使用して、エントリ (現在の条件) の表示、特定のエントリ (条件) の削除、またはエントリの評価順序の変更を実行できます。

```
WAE(config)# ip access-list standard 1
WAE(config-std-nacl)#?
delete Delete a condition
deny Specify packets to reject
exit Exit from this submode
insert Insert a condition
list List conditions
move Move a condition
no Negate a command or set its defaults
permit Specify packets to accept
WAE(config-std-nacl)#
```

- `list` コマンドを使用すると、条件のマッピング先である行番号を識別できます。このコマンドは、指定されたエントリ (または、指定されていない場合はすべてのエントリ) を一覧します。このコマンドを使用せずに、このマッピングを取得するには、EXEC モードに戻ってから、`show ip access-list EXEC` コマンドを入力する必要があります。

次の例は、`list` コマンドの使用方を示しています。

```
WAE(config-ext-nacl)# list
1 permit tcp host 10.1.1.1 any
2 permit tcp host 10.1.1.2 any
3 permit tcp host 10.1.1.3 any
WAE(config-ext-nacl)#
```

IP ACL 全体を WAE のデータベースから削除する方法の詳細については、[10-18 ページの「IP ACL の削除」](#)を参照してください。

IP ACL コンフィギュレーション モードの使用上のガイドライン

IP ACL を使用して作業する場合は、次のガイドラインにしたがってください。

- 標準 IP ACL を使用して作業するには、標準 IP ACL コンフィギュレーション モードに切り替える必要があります。

```
WAE(config)# ip access-list standard ?
<1-99> Standard IP access-list number
WORD Access-list name (max 30 characters)
```

- 拡張 IP ACL を使用して作業するには、拡張 IP ACL コンフィギュレーション モードに切り替える必要があります。

```
WAE(config)# ip access-list extended ?
<100-199> Standard IP access-list number
WORD Access-list name (max 30 characters)
```

IP ACL 名の使用上のガイドライン

IP ACL 名を作成する場合は、次のガイドラインにしたがってください。

- IP ACL 名は、WAE 内で一意でなければなりません。
- IP ACL 名が数字の場合 (たとえば、`ip access-list standard acl-num` または `ip access-list extended acl-num`):
 - 数字しか含めることはできません (たとえば、101)。
 - 数字 1 ~ 99 は、標準 IP ACL を表します。
 - 数字 100 ~ 199 は、拡張 IP ACL を表します。

- IP ACL 名が単語の場合(たとえば、`ip access-list standard acl-name` または `ip access-list extended acl-name`):
 - 非数字で開始する必要があります(たとえば、`snmpaccesslist`)
 - 30 文字に制限されています。
 - 文字ストリングに数字 0 ~ 9 を含めることができます(たとえば、`snmpaccesslist7`)
 - 空白を除き、出力可能な特殊文字はほとんど含めることができます。許容可能な特殊文字は、次のとおりです。~!@#\$\$%^&*()_+={ }[]\;':<>./ 許容されない特殊文字は、次のとおりです。|'?"

WAE での IP ACL の作成または変更

WAE で IP ACL を設定する手順は、次のとおりです。

ステップ 1 グローバル コンフィギュレーション モードで CLI にアクセスします。

```
WAE(config)#
```

ステップ 2 グローバル コンフィギュレーション モードから、適切な IP ACL コンフィギュレーション モードへアクセスし、作成、変更、または表示する IP ACL の名前または番号を指定します。

- 標準 IP ACL を作成または変更するには、**ip access-list standard** グローバル コンフィギュレーション コマンドを使用して、標準 IP ACL コンフィギュレーション モードに入ります。

```
ip access-list standard {acl-name | acl-num}
```

次の例は、ACL 番号 59 の標準 IP ACL を作成または変更する方法を示しています。

```
WAE(config)# ip access-list standard 59
```

CLI は、標準 IP ACL コンフィギュレーション モードに切り替わり、これ以降のすべてのコマンドは、現在の標準 IP ACL に適用されます。次のプロンプトが表示されます。

```
WAE(config-std-nacl)#
```

- 拡張 IP ACL を作成または変更するには、**ip access-list extended** コマンドを使用して、拡張 IP ACL コンフィギュレーション モードに入ります。

```
ip access-list extended {acl-name | acl-num}
```

次の例は、名前を指定して、拡張 IP ACL *test2* を作成または変更する方法を示しています。

```
WAE(config)# ip access-list extended test2
```

CLI は、拡張 IP ACL コンフィギュレーション モードに切り替わり、これ以降のすべてのコマンドは、現在の拡張 IP ACL に適用されます。次のプロンプトが表示されます。

```
WAE(config-ext-nacl)#
```

ステップ 3 標準 ACL 内の条件を追加、削除、または変更するには、標準 IP ACL コンフィギュレーション モードから次のコマンドを入力します。

- a. 標準 IP ACL に行を追加するには、次の構文を使用します。

たとえば、パケットを渡すか廃棄するかを指定する目的 (permit または deny) を選択して、送信元 IP アドレス、送信元 IP ワイルドカード アドレスを入力します。

```
[insert line-num] {deny | permit} {source-ip [wildcard] | host source-ip | any}
```

- b. 標準 IP ACL から行を削除するには、次の構文を使用します。

```
delete line-num
```

- c. 標準 IP ACL 内の新しい位置に行を移動するには、次の構文を使用します。

```
move old-line-num new-line-num
```

ステップ 4 拡張 ACL 内の条件を追加、削除、または変更するには、拡張 IP ACL コンフィギュレーション モードから次のコマンドを入力します。

- a. 拡張 IP ACL から行を削除するには、次の構文を使用します。

```
delete line-num
```

- b. 拡張 IP ACL 内の新しい位置に行を移動するには、次の構文を使用します。

```
move old-line-num new-line-num
```

- c. 拡張 IP ACL に条件を追加するときには、選択したプロトコルによってオプションが異なることを忘れないでください。

- IP の場合、条件を追加するには、次の構文を使用します。

```
[insert line-num] {deny | permit} {gre | ip | proto-num} {source-ip wildcard | host source-ip | any} {dest-ip wildcard | host dest-ip | any}
```

```
[no] {deny | permit} {gre | ip | proto-num} {source-ip wildcard | host source-ip | any} {dest-ip wildcard | host dest-ip | any}
```

- TCP の場合、条件を追加するには、次の構文を使用します。

```
[insert line-num] {deny | permit} tcp {source-ip wildcard | host source-ip | any} [operator port [port]] {dest-ip wildcard | host dest-ip | any} [operator port [port]] [established]
```

```
no {deny | permit} tcp {source-ip wildcard | host source-ip | any} [operator port [port]] {dest-ip wildcard | host dest-ip | any} [operator port [port]] [established]
```

- UDP の場合、条件を追加するには、次の構文を使用します。

```
[insert line-num] {deny | permit} udp {source-ip wildcard | host source-ip | any} [operator port [port]] {dest-ip wildcard | host dest-ip | any} [operator port [port]]
```

```
no {deny | permit} udp {source-ip wildcard | host source-ip | any} [operator port [port]] {dest-ip wildcard | host dest-ip | any} [operator port [port]]
```

- ICMP の場合、条件を追加するには、次の構文を使用します。

```
[insert line-num] {deny | permit} icmp {source-ip wildcard | host source-ip | any} {dest-ip wildcard | host dest-ip | any} [icmp-type [code]] [icmp-msg]
```

```
no {deny | permit} icmp {source-ip wildcard | host source-ip | any} {dest-ip wildcard | host dest-ip | any} [icmp-type [code]] [icmp-msg]
```



(注) 拡張 IP ACL の場合、**host** キーワードが指定されていないかぎり、**wildcard** パラメータは必須です。特定の ICMP メッセージ タイプとコードの照合に使用可能なキーワードのリスト、サポートされる UDP と TCP のキーワードのリスト、および拡張 IP ACL 条件のリストについては、『Cisco WAFS 3.0 Command Reference』を参照してください。

ステップ 5 標準 IP ACL に別の条件を追加するには、[ステップ 3](#) を繰り返します。拡張 IP ACL に別の条件 (エントリ) を追加するには、[ステップ 4](#) を繰り返します。

ステップ 6 WAE で IP ACL を作成または変更したら、次の手順では、**interface** および **ip access-group** コマンドを使用して、この IP ACL を有効化して、WAE の特定のインターフェイスに適用します。

IP ACL を有効化して、特定のインターフェイスに適用する方法の詳細については、[10-13 ページの「インターフェイスでの IP ACL の有効化」](#)および [10-14 ページの「IP ACL のアプリケーションへの適用」](#)を参照してください。

インターフェイスでの IP ACL の有効化

WAFS ソフトウェアは、さまざまなサービスを特定のインターフェイスに結合できる制御機能を提供します。IP ACL を WAE の特定のインターフェイスで有効化するには、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスごとに 1 つの発信 IP ACL と 1 つの着信 IP ACL を使用できます。

ip access-group コマンドを入力する前に、IP ACL を適用するインターフェイスのインターフェイス コンフィギュレーション モードに切り替える必要があります。

次のコマンドは、*acl-out* という名前の IP ACL を有効化し、GigabitEthernet インターフェイス スロット 1/ポート 0 の発信トラフィックに適用します。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)# ip access-group acl-out out
```

次のコマンドは、*example* という名前の IP ACL を有効化し、EtherChannel インターフェイス番号 1 の着信トラフィックに適用します。

```
WAE(config)# interface PortChannel 1
WAE(config-if)# ip access-group example in
WAE(config-if)# exit
```

IP ACL を有効化し、WAE の特定のインターフェイスに適用する手順は、次のとおりです。

-
- ステップ 1** IP ACL を適用するインターフェイスのインターフェイス コンフィギュレーション モードに切り替えます。たとえば、次の例は、WAE のスロット 1/ポート 0 にある GigabitEthernet インターフェイスのインターフェイス コンフィギュレーション モードに切り替える方法を示しています。

```
WAE(config)# interface GigabitEthernet 1/0
WAE(config-if)#
```

- ステップ 2** 事前に定義された IP ACL を、指定したインターフェイスに適用します。たとえば、次の例は、事前に定義された *acl-out* という名前の IP ACL を GigabitEthernet インターフェイス スロット 1/ポート 0 の発信トラフィックに適用する方法を示しています。

```
WAE(config-if)# ip access-group acl-out out
```

IP ACL のアプリケーションへの適用

SNMP には、IP ACL の使用を設定するための固有の CLI コマンドがあります。

```
snmp-server access-list {std-acl-num | std-acl-name}
```



(注) `snmp-server access-list` コマンドは、標準 IP ACL の名前または番号を受け入れることができるだけで、拡張 IP ACL には対応していません。

WAE が受信する着信 WCCP GRE カプセル化トラフィックに適用する IP ACL を指定するには、`wccp access-list` グローバル コンフィギュレーション コマンドを使用します。

```
wccp access-list {acl-num | acl-name}
```

WCCP ACL 機能は、標準 ACL と拡張 ACL の両方をサポートします。

その他のアプリケーション トラフィック (たとえば、Telnet や SSH) は、WAE のインターフェイス (通常は、着信トラフィック) に IP ACL を適用することで制御できます。

IP ACL を使用した SNMP アクセスの制御

標準 IP ACL を使用して WAE 上の SNMP エージェントへのアクセスを制御する手順は、次のとおりです。

- ステップ 1 `ip access-list standard` コマンドを使用して、WAE 上の SNMP エージェントへのアクセスを制御する IP ACL を作成します。
- ステップ 2 この IP ACL を SNMP サーバ (WAE) に関連付け、WAE 上でこの標準 IP ACL を有効化します。

```
WAE(config)# snmp-server access-list {std-acl-num | std-acl-name}
```

各パラメータの意味は、次のとおりです。

- `std-acl-name` は、この WAE に関連付ける標準 IP ACL の名前です。
- `std-acl-num` は、この WAE に関連付ける標準 IP ACL の番号です。

WAE 上の SNMP エージェントは、着信パケットを受け入れるか、または廃棄する前に、指定された IP ACL (たとえば、ACL 1) をチェックします。

```
WAE(config)# snmp-server access-list 1
```

IP ACL を使用した WCCP アクセスの制御

標準または拡張 IP ACL を使用して WAE 上の WCCP アクセスを制御する手順は、次のとおりです。

- ステップ 1 WAE 上の WCCP アクセスを制御するための標準または拡張 IP ACL を作成します。
 - a. `ip access-list standard` コマンドを使用して、WAE 上の WCCP アクセスを制御する標準 IP ACL を作成します。
 - b. `ip access-list extended` コマンドを使用して、WAE 上の WCCP アクセスを制御する拡張 IP ACL を作成します。

ステップ 2 IP ACL を WAE に関連付け、WAE 上でこの IP ACL を有効化します。

```
WAE(config)# wccp access-list {acl-num | acl-name}
```

各パラメータの意味は、次のとおりです。

- *acl-name* は、この WAE に関連付ける標準または拡張 IP ACL の名前です。
- *acl-num* は、この WAE に関連付ける標準または拡張 IP ACL の番号です。

WAE は、指定された IP ACL（たとえば、ACL 2）を WCCP GRE 着信トラフィックに適用します。

```
WAE(config)# wccp access-list 2
```

WAE の WCCP ACL の設定

WAE が受信する着信 WCCP GRE カプセル化トラフィックに適用する IP ACL を指定するには、`wccp access-list` グローバル コンフィギュレーション コマンドを使用します。

```
wccp access-list {acl-name | acl-number}
```

acl-name または *acl-number* は、標準 IP ACL または拡張 IP ACL のどちらかを表わしています。デフォルトでは、WCCP ACL は設定されていません。そのため、WCCP ACL は、WAE の設定の一部としては表示されません。

次の例は、WCCP ACL が WAE に設定されている場合の `show ip access-list EXEC` コマンドの出力例を示しています。

```
WAE# show ip access-list
Space available:
  48 access lists
  497 access list conditions

Standard IP access list test
  1 permit 10.1.1.1
    (implicit deny any:0 matches)
  total invocations:0
Extended IP access list no_www.linux.org
  1 deny tcp any host 10.1.1.1 (29 matches)
  2 permit ip any any (30 matches)
    (implicit fragment permit:0 matches)
    (implicit deny ip any any:0 matches)
  total invocations:59

Interface access list references:
  GigabitEthernet 2/0 inbound pc_test (Not Defined)

Application access list references:
  snmp-server standard test
    UDP ports:none
  WCCP either no_www.linux.org
    Any IP Protocol
WAE#
```

次の例は、WCCP ACL が WAE に定義されている場合の `show wccp gre EXEC` コマンドの出力例を示しています。強調表示された部分は、このスナップショットを取得した時点では、廃棄されたパケットがないことを示しています。

```
WAE# show wccp gre
Transparent GRE packets received:          0
Transparent non-GRE packets received:      0
Transparent non-GRE packets passed through: 0
Total packets accepted:                    0
Invalid packets received:                  0
Packets received with invalid service:     0
Packets received on a disabled service:    0
Packets received too small:                0
Packets dropped due to zero TTL:            0
Packets dropped due to bad buckets:         0
Packets dropped due to no redirect address: 0
Packets dropped due to loopback redirect:   0
Connections bypassed due to load:          0
Packets sent back to router:                0
Packets sent to another CE:                0
GRE fragments redirected:                  0
Packets failed GRE encapsulation:          0
Packets dropped due to invalid fwd method:  0
Packets dropped due to insufficient memory: 0
Packets bypassed, no conn at all:          0
Packets bypassed, no pending connection:   0
Packets due to clean wccp shutdown:        0
Packets bypassed due to bypass-list lookup: 0
Packets received with client IP addresses: 0
Conditionally Accepted connections:        0
Conditionally Bypassed connections:        0
L2 Bypass packets destined for loopback:   0
Packets w/WCCP GRE received too small:    0
Packets dropped due to IP access-list deny: 0
L2 Packets fragmented for bypass:          0
```



(注) また、`show statistics wccp gre EXEC` コマンドを入力しても、上記の出力を表示できます。

設定例

次の例は、`ip access-list extended` グローバル コンフィギュレーション コマンドを使用して、*example* という名前の拡張 IP ACL を作成する方法を示しています。この拡張 IP ACL は、一旦すべての WCCP トラフィックを許可しますが、その後、SSH を使用した特定ホスト（ホスト 10.1.1.5）の管理アクセスのみを許可します。

```
WAE(config)# ip access-list extended example
WAE(config-ext-nacl)# permit tcp any any eq wccp
WAE(config-ext-nacl)# permit tcp host 10.1.1.5 any eq ssh
WAE(config-ext-nacl)# exit
```

次の例では、WAE がインターフェイス ACL とアプリケーション ACL を使用するように設定されています。

```
WAE# show ip access-list
Space available:
  47 access lists
  492 access list conditions

Standard IP access list 1  1 permit 10.1.1.2
  2 deny  10.1.2.1
    (implicit deny any: 2 matches)
  total invocations: 2
Extended IP access list 100
  1 permit tcp host 10.1.1.1 any
  2 permit tcp host 10.1.1.2 any
  3 permit tcp host 10.1.1.3 any
    (implicit fragment permit: 0 matches)
    (implicit deny ip any any: 0 matches)
  total invocations: 0
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
    (implicit deny: 2 matches)
  total invocations: 12
Interface access list references:
  GigabitEthernet 1/0  inbound  100
Application access list references:
  wccp_server                standard  1
```

IP ACL の削除

IP ACL（ネットワーク インターフェイスおよびアプリケーションのすべての条件とリファレンスを含む）を WAE データベースから削除する手順は、次のとおりです。

ステップ 1 グローバル コンフィギュレーション モードで CLI にアクセスします。

```
WAE(config)#
```

ステップ 2 グローバル コンフィギュレーション モードから、削除する IP ACL の名前または番号を指定します。

- 標準 IP ACL を削除するため、削除する標準 IP ACL を指定します。

```
Engine(config)# no ip access-list standard {acl-name | acl-num}
```

次の例は、*test2* という名前の標準 IP ACL を削除する方法を示しています。

```
WAE(config)# no ip access-list standard test2
```

- 拡張 IP ACL を削除するため、削除する拡張 IP ACL を指定します。

```
WAE(config)# no ip access-list extended {acl-name | acl-num}
```

次の例は、*example* という名前の拡張 IP ACL を削除する方法を示しています。

```
WAE(config)# no ip access-list extended example
```

IP ACL の設定の表示

現在、WAE に定義されている IP ACL の設定を表示するには、次のように、`show ip access-list EXEC` コマンドを使用します。

```
show ip access-list [acl-name | acl-num]
```

`show ip access-list EXEC` コマンドを使用して、現在のシステム(この場合は WAE)に定義されている IP ACL に関する構成情報を表示できます。名前または番号によって特定の IP ACL を識別しないかぎり、システムは、定義済みのすべての IP ACL について、次の項目を含む情報を表示します。

- 新しいリストおよび条件用として使用可能なスペース
- 定義済みの IP ACL
- インターフェイスおよびアプリケーションによるリファレンス

次の例は、特定の IP ACL が指定されていない場合の `show ip access-list EXEC` コマンドの出力例を示しています。

```
WAE# show ip access-list
Space available:
  47 access lists
  492 access list conditions

Standard IP access list 1 1 permit 10.1.1.2
  2 deny 10.1.2.1
  (implicit deny any: 2 matches)
  total invocations: 2
Extended IP access list 100
  1 permit tcp host 10.1.1.1 any
  2 permit tcp host 10.1.1.2 any
  3 permit tcp host 10.1.1.3 any
  (implicit fragment permit: 0 matches)
  (implicit deny ip any any: 0 matches)
  total invocations: 0
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
  (implicit deny: 2 matches)
  total invocations: 12

Interface access list references:
  GigabitEthernet 1/0 inbound 100
Application access list references:
  tftp_server standard 1
  UDP ports: 69
```

次の例は、`test` という名前の IP ACL に関する `show ip access-list EXEC` コマンドの出力例を示しています。

```
WAE# show ip access-list test
Standard IP access list test
  1 permit 1.1.1.1 (10 matches)
  2 permit 1.1.1.3
  3 permit 1.1.1.2
  (implicit deny: 2 matches)
  total invocations: 12
```



(注) システムは、条件文に一致するパケットが 1 つ以上ある場合にだけ、一致したパケット数を表示します。

IP ACL カウンタのクリア

WAE 上の IP ACL の統計情報をリセットするには、**clear ip access-list counter EXEC** コマンドを使用して、IP ACL カウンタをクリアします。

```
WAE# clear ip access-list counters {acl-name | acl-num}
```

この EXEC コマンドを使用すると、すべての既存の IP ACL の条件文に関連付けられた IP ACL カウンタをクリアできます。IP ACL の名前または番号を指定した場合は、指定したリストのカウンタだけがクリアされます。