CHAPTER 36

IP 許可リストの設定

この章では、Catalyst 6500 シリーズ スイッチ上で IP 許可リストを設定する方法について説明します。

（注） IP 許可リストの機能は、VLAN Access Control List（VACL）を使用して実行することもできます。VACL はハードウェア（Policy Feature Card [PFC; ポリシー フィーチャ カード]）によって処理されるので、VACL のほうが IP 許可リストに比べて、高速に処理されます。

（注） この章で使用しているコマンドの完全な構文および使用方法の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

この章で説明する内容は、次のとおりです。

IP 許可リストの機能

IP 許可リストは、許可されていない送信元 IP アドレスによるスイッチへの着信 Telnet および SNMP（簡易ネットワーク管理プロトコル）アクセスを防止します。他のすべての TCP/IP サービス（IP traceroute、IP ping など）は、IP 許可リストをイネーブルにしても、そのまま正常に動作します。発信 Telnet、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、およびその他の IP ベース サービスは、IP 許可リストの影響を受けません。

許可されていない送信元 IP アドレスによる Telnet アクセスでは、接続が拒否されます。許可されていない IP アドレスから SNMP 要求に応答が戻されないと、要求はタイムアウトになります。コンソールまたは Syslog サーバに対する無許可アクセスのロギングを希望する場合は、「IP 許可リストのイネーブル化」（p.36-3）の説明に従って IP のロギング重大度を変更する必要があります。無許可アクセスの試行時に SNMP トラップが生成されるようにするには、「IP 許可リストのイネーブル化」（p.36-3）の説明に従って IP 許可リスト（ippermit）SNMP トラップをイネーブルにする必要があります。同じ無許可ホストから複数のアクセスが試みられた場合は、10 分ごとに通知が生成されるだけです。

許可リストには最大 100 のエントリを設定できます。各エントリには、IP アドレスとサブネット マスクのペアをドット付き 10 進表記で指定するとともに、その IP アドレスを SNMP 許可リスト、Telnet 許可リスト、または両方のリストのどれに入れるかを指定します。マスクで 1 に設定したビットは、着信パケットの送信元 IP アドレスと一致するかどうかがチェックされます。ゼロに設定したビットはチェックされません。このプロセスでワイルドカード アドレスを指定できます。

IP 許可リストのエントリにマスクを指定しなかった場合、または IP アドレスの代わりにホスト名を指定した場合には、そのホストの IP アドレスとだけ一致するように、マスクのすべてのビットが 1 となる（255.255.255.255 または 0xffffffff）暗黙的な値になります。

IP アドレスの許可リストの種類として SNMP または Telnet を指定しない場合、その IP アドレスは、SNMP 許可リストおよび Telnet 許可リストの両方に追加されます。

マスクが異なっていれば、許可リストの複数エントリに同じ IP アドレスを指定できます。アドレスは、マスクが適用されてから NVRAM（不揮発性 RAM）に保存されるので、同じ結果になるアドレスは保存されません。IP 許可リストにこのようなアドレスを追加すると、マスクが適用されたアドレスが表示されます。

IP 許可リストのデフォルト設定

表 36-1 に、IP 許可リストのデフォルト設定を示します。

表 36-1　IP 許可リストのデフォルト設定

機能	デフォルト値
IP 許可リストのイネーブル ステート	ディセーブル
許可リストのエントリ	設定なし
IP Syslog メッセージの重大度	2
SNMP IP 許可トラップ（ippermit）	ディセーブル

スイッチ上での IP 許可リストの設定

ここでは、IP 許可リストを設定する方法について説明します。

IP 許可リストへの IP アドレスの追加

SNMP 許可リスト、Telnet 許可リスト、または両方のリストに特定の IP アドレスを追加できます。

IP 許可リストに IP アドレスを追加するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストに追加する IP アドレスを指定します。	**set ip permit** *ip_address* [*mask*] [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストに IP アドレスを追加し、設定を確認する例を示します。

```
Console> (enable) set ip permit 172.16.0.0 255.255.0.0 telnet
172.16.0.0 with mask 255.255.0.0 added to telnet permit list.
Console> (enable) set ip permit 172.20.52.32 255.255.255.224 snmp
172.20.52.32 with mask 255.255.255.224 added to snmp permit list.
Console> (enable) set ip permit 172.20.52.3 all
172.20.52.3 added to IP permit list.
Console> (enable) show ip permit
Telnet permit list feature enabled.
Snmp permit list feature enabled.
Permit List        Mask                Access Type
----------------   ----------------    -------------
172.16.0.0         255.255.0.0         telnet
172.20.52.3                            snmp telnet
172.20.52.32       255.255.255.224     snmp
Denied IP Address   Last Accessed Time Type    Telnet Count   SNMP Count
-----------------   ------------------ ------  ------------   ----------
172.100.101.104     01/20/97,07:45:20  SNMP              14         1430
172.187.206.222     01/21/97,14:23:05  Telnet             7          236

Console> (enable)
```

IP 許可リストのイネーブル化

SNMP 許可リスト、Telnet 許可リスト、または両方のリストをイネーブルに設定できます。許可リストを指定しない場合は、SNMP 許可リストおよび Telnet 許可リストの両方がイネーブルに設定されます。

注意　特に SNMP を使用して設定する場合には、IP 許可リストをイネーブルにする前に、使用するワークステーションまたはネットワーク管理システムの IP アドレスが IP 許可リストに追加されていることを確認してください。IP アドレスが追加されていないと、スイッチにより接続が切断されます。IP 許可リストのエントリまたはホスト アドレスを削除する前に、IP 許可リストをディセーブルにしてください。

スイッチの IP 許可リストをイネーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストをイネーブルにします。	**set ip permit enable** [**telnet** | **snmp** | **ssh**]
ステップ 2	必要な場合、IP 許可トラップをイネーブルにし、無許可アクセスの試行についてトラップを生成します。	**set snmp trap enable ippermit**
ステップ 3	必要な場合、無許可アクセスの Syslog メッセージが表示されるよう、ロギング レベルを設定します。	**set logging level ip 4 default**
ステップ 4	IP 許可リストの設定を確認します。	**show ip permit** **show snmp**

次に、IP 許可リストをイネーブルにし、設定を確認する例を示します。

```
Console> (enable) set ip permit enable
IP permit list enabled.
Console> (enable) set snmp trap enable ippermit
SNMP IP Permit traps enabled.
Console> (enable) set logging level ip 4 default
System logging facility <ip> set to severity 4(warnings)
Console> (enable) show ip permit
Telnet permit list feature enabled.
Snmp permit list feature disabled.

Permit List          Mask              Access-Type
---------------     ---------------   ---------------
172.16.0.0         255.255.0.0         telnet
172.20.52.3                            snmp telnet
172.20.52.32       255.255.255.224     snmp

Denied IP Address   Last Accessed Time Type    Telnet Count   SNMP Count
-----------------   ------------------ ------  ------------   ----------
172.100.101.104     01/20/97,07:45:20  SNMP              14         1430
172.187.206.222     01/21/97,14:23:05  Telnet             7          236

Console> (enable) show snmp
RMON:                         Disabled
Extended Rmon:                Extended RMON module is not present
Traps Enabled:
ippermit
Port Traps Enabled: None

Community-Access     Community-String
----------------     --------------------
read-only            public
read-write           private
read-write-all       secret

Trap-Rec-Address                           Trap-Rec-Community
-----------------------------------------  --------------------
Console> (enable)
```

IP 許可リストのディセーブル化

スイッチの IP 許可リストをディセーブルにするには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	スイッチの IP 許可リストをディセーブルにします。	**set ip permit disable** [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストをディセーブルにする例を示します。

```
Console> (enable) set ip permit disable
IP permit list disabled.
Console> (enable)
```

IP 許可リスト エントリの消去

SNMP 許可リスト、Telnet 許可リスト、または両方のリストから特定の IP アドレスを消去できます。どの許可リストから IP アドレスを消去するかを指定しない場合は、両方の許可リストから IP アドレスが削除されます。

注意　IP 許可リストのエントリまたはホスト アドレスを消去する前に、必ず IP 許可リストをディセーブルにしてください。現在使用中の IP アドレスを消去した場合に、設定対象のスイッチによって接続が切断されるのを防ぐためです。

IP 許可リストのエントリを消去するには、イネーブル モードで次の作業を行います。

	作業	コマンド
ステップ 1	IP 許可リストをディセーブルにします。	**set ip permit disable** [**telnet** | **snmp** | **ssh**]
ステップ 2	IP 許可リストから削除する IP アドレスを指定します。	**clear ip permit** {*ip_address* [*mask*] | **all**} [**telnet** | **snmp** | **ssh**]
ステップ 3	IP 許可リストの設定を確認します。	**show ip permit**

次に、IP 許可リストからエントリを消去する例を示します。

```
Console> (enable) set ip permit disable all
Console> (enable) clear ip permit 172.100.101.102
172.100.101.102 cleared from IP permit list.
Console> (enable) clear ip permit 172.160.161.0 255.255.192.0 snmp
172.160.128.0 with mask 255.255.192.0 cleared from snmp permit list.
Console> (enable) clear ip permit 172.100.101.102 telnet
172.100.101.102 cleared from telnet permit list.
Console> (enable) clear ip permit all
IP permit list cleared.
Console> (enable)
```