CHAPTER 9

WAAS デバイス用の IP ACL の作成および管理

この章では、Wide Area Application Services（WAAS）の Central Manager GUI を使用して、WAAS デバイス用の IP アクセス コントロール リスト（ACL）を集中的に作成し、管理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。

（注） IP ACL 設定の表示、編集、または作成を行うには、admin 特権を持つアカウントを使用して WAAS Central Manager GUI にログインする必要があります。

（注） この章では、ネットワークに存在する WAAS Central Manager と Wide Area Application Engine（WAE）を総称する用語として「WAAS デバイス」を使用します。WAE という用語は、WAE アプライアンス、WAE ネットワーク モジュール（NME-WAE ファミリのデバイス）、および WAAS を実行する SM-SRE モジュールを指します。

WAAS デバイス用の IP ACL について

集中管理される WAAS ネットワーク環境では、管理者がさまざまなデバイスやサービスへの不正アクセスを防止できる必要があります。IP ACL は、WAAS デバイス宛ての IP パケットを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リングできます。

WAAS ソフトウェアは、WAAS デバイスへのアクセスを制限できる標準および拡張 ACL をサポートしています。WAAS ソフトウェアは、次の種類の ACL を使用できます。

- インターフェイス ACL：組み込みインターフェイス、ポート チャネル インターフェイス、スタンバイ インターフェイス、インライン グループ インターフェイスに対して適用します。この種類の ACL は、管理トラフィック（Telnet、SSH、および Central Manager GUI）の制御を目的としています。ACL ルールは、WAE 宛てのトラフィックまたは WAE から送信されたトラフィックにのみ適用され、WCCP 中継トラフィックには適用されません。インターフェイス ACL を適用するには、**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。

- 代行受信 ACL：WAAS デバイスにグローバルに適用されます。この種類の ACL は代行受信するトラフィックを定義します。この ACL で許可されるトラフィックは代行受信され、この ACL で拒否されるトラフィックは WAE を通過します。代行受信 ACL を適用するには、**interception 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。代行受信 ACL の使用方法の詳細については、「代行受信アクセス コントロール リストの設定」（P.5-29）を参照してください。
- WCCP ACL：着信 WCCP リダイレクト トラフィックに適用し、外部サーバと外部クライアント間のアクセスを制御します。WAE はファイアウォールのように機能します。WCCP ACL を適用するには、**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。
- SNMP ACL：SNMP エージェントに適用され、SNMP MIB または SNMP 統計をポーリングする外部 SNMP サーバによる SNMP エージェントへのアクセスを制御します。SNMP ACL を適用するには、**snmp-server 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。
- トランザクション ログ フロー ACL：トランザクション ロギング機能に適用し、トランザクションのログを制限します。トランザクション ログ ACL を適用するには、**transaction-logs flow 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。

次の例は、WAAS デバイスが存在する環境で、インターフェイス ACL を使用する方法を示しています。

- WAAS デバイスは、顧客の施設に常駐し、サービス プロバイダーによって管理され、サービス プロバイダーはその管理のためだけにデバイスの安全性を確保する必要があります。
- WAAS デバイスは、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 WAAS Central Manager GUI から IT ソース サブネットへのアクセスを制限する必要があります。

ACL を使用するには、最初に ACL を設定し、次に WAAS デバイス上の特定のサービスやインターフェイスに ACL を適用する必要があります。次に、さまざまな企業展開にインターフェイス ACL を使用する方法の例を示します。

- 外部インターフェイスを要塞化したアプリケーション層プロキシ ファイアウォールには、公開されるポートがありません。（「要塞化」とは、主にセキュリティ上の理由で、どのポートをアクセスに使用できるかをインターフェイスが厳しく制限している状態を意味します。インターフェイスは外部に存在するため、さまざまな攻撃の可能性があります）。WAAS デバイスの外部アドレスはインターネットからグローバルにアクセスできますが、内部アドレスはプライベートです。内部インターフェイスには、Telnet、SSH、および GUI アクセスを制限する ACL があります。
- WCCP を使用している WAE は、インターネット ルータから独立したサブネットに配置されます。WAE とルータの両方が IP ACL を持っている必要があります。ルータ上の IP アクセス リストは、最高の優先順位を持ち、WAE に定義された IP ACL より優先します。

（注）　WAAS CLI ではなく、WAAS Central Manager GUI を使用して、ACL を集中設定し、WAAS デバイスに適用することを強く推奨します。詳細については、「WAAS デバイス用の IP ACL の作成と管理」（P.9-2）を参照してください。

WAAS デバイス用の IP ACL の作成と管理

この項では、WAAS Central Manager GUI を使用して、WAAS デバイス用の IP ACL を作成し、管理するためのガイドラインと例を提供します。

IP ACL を作成するときは、次の重要事項に注意する必要があります。

- IP ACL 名はデバイス内で一意である必要があります。

- IP ACL 名は、空白や特殊文字を含まない 30 文字以下にする必要があります。
- 1 台の WAAS Central Manager デバイスで、最大 50 個の IP ACL とデバイス当たり合計 500 個の条件を管理できます。
- IP ACL 名が数値の場合、1 ～ 99 は標準の IP ACL を表し、100 ～ 199 は拡張 IP ACL を表します。数字で始まる IP ACL 名には、数字以外の文字を使用できません。
- WAAS Central Manager GUI を使用すると、標準の IP ACL を SNMP と WCCP に関連付けることができます。ACL に関連付けられたこれらのアプリケーションのいずれかにアクセスしようとするデバイスはすべて、アクセスを許可される信頼されたデバイスのリストに含まれている必要があります。
- 以前に設定した標準 IP ACL を SNMP および WCCP に関連付けることはできますが、拡張 IP ACL は WCCP アプリケーションだけに関連付けることができます。
- すべての条件とネットワーク インターフェイスやアプリケーションとの関連付けを含む IP ACL を削除できます。あるいは、IP ACL 条件だけ削除できます。すべての条件を削除すると、必要に応じ、IP ACL の種類を変更できます。IP ACL 項目はその後も IP ACL リストに現れますが、実質的には存在しません。
- WAAS によって使用される任意の種類の ACL に対して空の ACL を指定すると、すべてのトラフィックが許可されます。

WAAS Central Manager GUI を使用して、1 台の WAE 用の IP ACL を作成し、変更する方法と、IP ACL をアプリケーションに関連付け、WAE 上のインターフェイスに適用するには、次の手順に従ってください。

ステップ 1　WAAS Central Manager メニューから、[Devices] > [*device-name*] を選択します。

ステップ 2　[Configure] > [Network] > [TCP/IP Settings] > [IP ACL] を選択します。

[IP ACL] ウィンドウが表示されます。デフォルトでは、WAE 用の IP ACL は、定義されていません。[IP ACL] ウィンドウで、現在、WAE 用の IP ACL が設定されていないかどうかを確認します。

ステップ 3　タスクバーで、[Create a new IP ACL] アイコンをクリックします。

[Creating New IP ACL] ウィンドウが表示されます。次のようにフィールドに入力します。

- [Name] フィールドで、IP ACL の命名規則に従って名前（たとえば、test1）を入力します。

  デフォルトで、この新しい IP ACL は、標準 ACL として作成されます。

  （注）　IP ACL 名は、デバイス内で一意であり、30 文字以内でなければならず、余白や特殊文字を使用できません。

- このデフォルト設定を変更して、この新しい ACL を拡張 ACL として作成する場合は、[ACL Type] ドロップダウン リストから [Extended] を選択します。

ステップ 4　[Submit] をクリックして、test1 という名前の IP ACL を保存します。条件が何も定義されていない IP ACL は、個々のデバイスに表示されません。

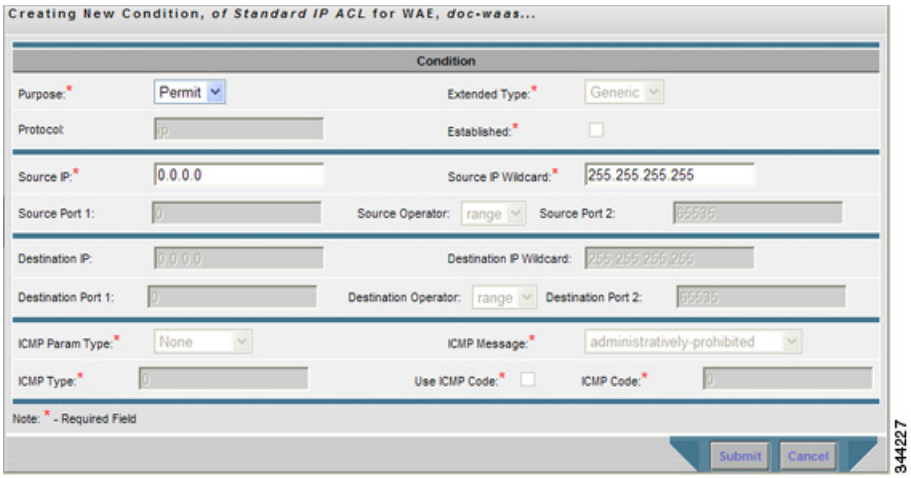
ステップ 5　作成した test1 という名前の標準 IP ACL に条件を追加します。

a.　タスクバーで、[Create New Condition] アイコンをクリックします。

[Creating New Condition] ウィンドウが表示されます （図 9-1 を参照）。

（注）　IP ACL の条件を作成するために使用できるフィールドの数は、作成した IP ACL の種類（標準または拡張）によって異なります。

図 9-1　[Extended IP ACL] ウィンドウでの新しい状態の作成



b. 次のようにして、作成する IP ACL のタイプに使用できるプロパティの値を入力します。

- 標準 IP ACL 用の条件を設定するには、ステップ 6 へ進みます。
- 拡張 IP ACL 用の条件を設定するには、ステップ 7 を参照してください。

ステップ 6　標準 IP ACL 用の条件を設定します。

a. ドロップダウン リストから、目的（[Permit] または [Deny]）を選択します。

b. [Source IP] フィールドにソース IP アドレスを入力します。

c. [Source IP Wildcard] フィールドに、ソース IP ワイルドカード アドレスを入力します。

d. [Submit] をクリックして、条件を保存します。

[Modifying IP ACL] ウィンドウが再表示され、条件と設定されたパラメータが表形式で表示されます。

e. IP ACL に別の条件を追加するには、上記の手順を繰り返します。

f. [Modifying IP ACL] ウィンドウから条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用するか、列見出しをクリックして、任意の設定済みパラメータで並べ替えます。

（注）　WAAS Central Manager GUI に表示される条件の順序は、IP ACL がデバイスに適用される順序になります。

g. IP ACL への条件の追加が完了し、すべての項目と条件の表示順序に満足したら、[Modifying IP ACL] ウィンドウの [Submit] をクリックして、デバイス データベースに IP ACL を確定します。

[Modifying IP ACL] ウィンドウの右下部に緑色の「Change submitted」インジケータが表示され、IP ACL がデバイス データベースに送信中であることを示します。表 9-1 で、標準 IP ACL のフィールドについて説明します。

表 9-1　標準 IP ACL の条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
Source IP[1]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
Source IP Wildcard[1]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。

1. 必須フィールド。

ステップ 7　拡張 IP ACL 用の条件を設定します。

a. ドロップダウン リストから、目的（[Permit] または [Deny]）を選択します。

b. [Extended Type] ドロップダウン リストから、[Generic]、[TCP]、[UDP]、または [ICMP] を選択します （表 9-2 を参照）。

表 9-2　拡張 IP ACL の条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可するか拒否するかを指定します。[Permit] または [Deny] を選択します。
Extended Type[1]	Generic	条件に適用するインターネット プロトコルを指定します。 選択すると、[GUI] ウィンドウが更新され、該当するフィールド オプションが有効になります。オプションは、[generic]、[TCP]、[UDP]、または [ICMP] です。

1. 必須フィールド。

拡張 IP ACL の種類を選択すると、選択した種類によって GUI でさまざまなオプションが使用できるようになります。

c. 選択されたタイプに対して有効になっているフィールドにデータを入力します。（詳細については、表 9-4（P.9-8）～表 9-7（P.9-10）を参照してください）。

d. [Submit] をクリックして、条件を保存します。

[Modifying IP ACL] ウィンドウが再表示され、条件と設定されたパラメータが表形式で表示されます。

e. IP ACL に別の条件を追加するには、上記の手順を繰り返します。

f. [Modifying IP ACL] ウィンドウから条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用するか、列見出しをクリックして、任意の設定済みパラメータで並べ替えます。

（注） WAAS Central Manager GUI に表示される条件の順序は、IP ACL がデバイスに適用される順序になります。

g. IP ACL への条件の追加が完了し、すべての項目と条件の表示順序に満足したら、[Modifying IP ACL] ウィンドウの [Submit] をクリックして、デバイス データベースに IP ACL を確定します。

[Modifying IP ACL] ウィンドウの右下部に緑色の「Change submitted」インジケータが表示され、IP ACL がデバイス データベースに送信中であることを示します。

ステップ 8　IP ACL から個々の状態を変更または削除します。

a. 変更する IP ACL の名前の横にある [Edit] アイコンをクリックします。[Modifying IP ACL] ウィンドウが表示され、現在、IP ACL に適用されているすべての条件が表示されます。

b. 変更または削除する条件の横にある [Edit Condition] アイコンをクリックします。[Modifying Condition] ウィンドウが表示されます。

c. 条件を変更するには、必要に応じて許容フィールドを変更します。

d. 条件を削除するには、タスクバーの [Trash]（[Delete IP ACL Condition]）アイコンをクリックします。

e. 条件のリストの順序を変更するには、[Move] 列の上向き矢印または下向き矢印を使用し、[Submit] をクリックします。

ステップ 9　標準 IP ACL を SNMP または WCCP に関連付けます。

a. 標準 IP ACL を SNMP または WCCP に関連付けるデバイスの名前の横にある [Edit] アイコンをクリックします。

b. [Configure] > [Network] > [TCP/IP Settings] > [IP ACL Feature Usage] を選択します。[IP ACL Feature Settings] ウィンドウが表示されます。

c. ドロップダウン リストから、SNMP または WCCP 用の IP ACL の名前を選択します。（詳細については、表 9-3 を参照してください）。IP ACL をアプリケーションに関連付けない場合は、[Do Not Set] を選択します。

表 9-3　IP ACL Feature Settings（IP ACL 機能設定）

WAAS Central Manager GUI のパラメータ	機能
SNMP	標準 IP ACL を SNMP に関連付けます。このオプションは、すべての WAAS デバイスでサポートされます。
WCCP	任意の IP ACL を WCCP バージョン 2 に関連付けます。このオプションは、WCCP 代行受信モードで動作中の WAAS デバイスだけでサポートされ、WAAS Central Manager デバイスではサポートされません。

d. [Submit] をクリックして、設定を保存します。

ステップ 10　IP ACL をインターフェイスに適用します。

a. IP ACL を WAE 上のインターフェイスに適用するデバイスの名前の横にある [Edit] アイコンをクリックします。

b. [Configure] > [Network] > [Network Interfaces] を選択します。

デバイス用の [Network Interfaces] ウィンドウが表示されます。このウィンドウには、そのデバイスで使用可能なすべてのインターフェイスが表示されます。

c. IP ACL を適用するインターフェイスの名前の横にある [Edit] アイコンをクリックします。[Network Interface Settings] ウィンドウが表示されます。

d. ウィンドウの下部にある [Inbound ACL] ドロップダウン リストから、IP ACL の名前を選択します。

e. [Outbound ACL] ドロップダウン リストから、ACL の名前を選択します。

WAAS Central Manager GUI から変更できるネットワーク インターフェイス プロパティはインバウンド IP ACL とアウトバウンド IP ACL だけです。他のすべてのプロパティの値はデバイス データベースから入力され、WAAS Central Manager GUI では読み取り専用です。

ステップ 11　[Submit] をクリックして、設定を保存します。

ステップ 12　代行受信されるトラフィックの定義に IP ACL を使用する方法については、「代行受信アクセス コントロール リストの設定」（P.5-29）を参照してください。

ステップ 13　（任意）IP ACL を削除します。

a. 削除する IP ACL を持つデバイスの名前の横にある [Edit] アイコンをクリックします。

b. [Configure] > [Network] > [TCP/IP Settings] > [IP ACL] を選択します。

c. 削除する IP ACL の名前（test1 など）の横にある [Edit] アイコンをクリックします。

[Modifying IP ACL] ウィンドウが表示されます。IP ACL 用の条件を作成した場合は、2 つの削除オプションがあります。

- [Delete ACL]：すべての条件とネットワーク インターフェイスやアプリケーションとの関連付けを含む IP ACL を削除します。
- [Delete All Conditions]：すべての条件を削除しますが、IP ACL 名は保持されます。

d. IP ACL 全体を削除するには、タスクバーの大型 [Trash]（[Delete ACL]）アイコンをクリックします。処理を確認するプロンプトが表示されます。[OK] をクリックします。記録が削除されます。

e. 条件だけを消去するには、タスクバーの小さい [Delete All Conditions] の [Trash]/[List] アイコンをクリックします。処理を確認するプロンプトが表示されたら、[OK] をクリックします。ウィンドウが更新され、条件が削除され、[ACL Type] フィールドが使用できるようになります。

CLI から IP ACL を定義するには、**ip access-list** グローバル コンフィギュレーション コマンドを使用でき、WAAS デバイス上のインターフェイスに IP ACL を適用するには、**ipaccess-group** インターフェイス コンフィギュレーション コマンドを使用できます。SNMP 用の IP ACL の使用を設定するには、**snmp-server access-list** グローバル コンフィギュレーション コマンドを使用できます。WAE が受信する着信 WCCP リダイレクト 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 コマンドを使用できます。代理受信 ACL を設定するには、**interception access-list** グローバル コンフィギュレーション コマンドを使用できます。

拡張 IP ACL 条件のリスト

拡張 IP ACL 用の条件を定義するときは、（「WAAS デバイス用の IP ACL の作成と管理」（P.9-2）のステップ 7 の説明に従って）条件に適用するインターネット プロトコルを指定できます。

拡張 IP ACL 条件のリストは、次のとおりです。

- Generic（表 9-4 を参照）
- TCP（表 9-5 を参照）
- UDP（表 9-6 を参照）
- ICMP（表 9-7 を参照）

表 9-4　拡張 IP ACL の Generic 条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
Extended Type[1]	Generic	任意のインターネット プロトコルと一致します。
Protocol	ip	インターネット プロトコル（[gre]、[icmp]、[ip]、[tcp]、または [udp]）。 任意のインターネット プロトコルと一致するには、キーワード **ip** を使用します。
Source IP[1]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
Source IP Wildcard[1]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Destination IP	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
Destination IP Wildcard	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。

1. 必須フィールド。

表 9-5　拡張 IP ACL の TCP 条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
Extended Type[1]	TCP	TCP インターネット プロトコルと一致します。
Established	オフ（false）	選択すると、TCP データグラムに確認応答（ACK）または RST ビットが設定され、確立した接続を示す場合、ACL 条件との照合が行われます。接続を形成するために使用される初期の TCP データグラムは照合されません。
Source IP[1]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
Source IP Wildcard[1]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Source Port 1	0	TCP ポートの 10 進番号または名前。有効なポート番号は 0 ～ 65535 です。有効な TCP ポート名は、ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www です。

表 9-5　拡張 IP ACL の TCP 条件 （続き）

フィールド	デフォルト値	説明
Source Operator	range	送信元ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
Source Port 2	65535	TCP ポートの 10 進番号または名前。[Source Port1] を参照してください。
Destination IP	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
Destination IP Wildcard	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Destination Port 1	0	TCP ポートの 10 進番号または名前。有効なポート番号は 0 ～ 65535 です。有効な TCP ポート名は、ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www です。
Destination Operator	range	送信先ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
Destination Port 2	65535	TCP ポートの 10 進番号または名前。[Destination Port 1] を参照してください。

1. 必須フィールド。

表 9-6　拡張 IP ACL の UDP 条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
Extended Type[1]	UDP	UDP インターネット プロトコルと一致します。
Established	—	UDP には使用できません。
Source IP[1]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
Source IP Wildcard[1]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Source Port 1	0	UDP ポートの 10 進番号または名前。有効なポート番号は 0 ～ 65535 です。有効な UDP ポート名は、bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp です。

表 9-6　拡張 IP ACL の UDP 条件 （続き）

フィールド	デフォルト値	説明
Source Operator	range	送信元ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
Source Port 2	65535	UDP ポートの 10 進番号または名前。[Source Port1] を参照してください。
Destination IP	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
Destination IP Wildcard	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Destination Port 1	0	UDP ポートの 10 進番号または名前。有効なポート番号は 0 ～ 65535 です。有効な UDP ポート名は、bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp です。
Destination Operator	range	送信先ポートと着信パケットを比較する方法を指定します。[<]、[>]、[==]、[!=]、または [range] の中から選択します。
Destination Port 2	65535	UDP ポートの 10 進番号または名前。[Destination Port 1] を参照してください。

1. 必須フィールド。

表 9-7　拡張 IP ACL の ICMP 条件

フィールド	デフォルト値	説明
Purpose[1]	Permit	パケットを許可する（[Permit]）か拒否する（[Deny]）かを指定します。
Extended Type[1]	ICMP	ICMP インターネット プロトコルと一致します。
Source IP[1]	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信元ネットワークまたはホストの番号
Source IP Wildcard[1]	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。
Destination IP	0.0.0.0	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定したパケットの送信先ネットワークまたはホストの番号
Destination IP Wildcard	255.255.255.255	10 進表記の 4 つの部分をドットで区切った 32 ビット量として指定した送信元に適用するワイルドカード ビット。無視するビット位置には 1、意味のあるビット位置には 0 を入れます。

表 9-7　拡張 IP ACL の ICMP 条件 （続き）

フィールド	デフォルト値	説明
ICMP Param Type[1]	なし	[None]、[Type/Code]、または [Msg] の中から選択します。 [None] : [ICMP Type]、[Code]、および [Message] フィールドを無効にします。 [Type/Code] : ICMP メッセージの種類とコードで ICMP メッセージを選別できます。また、ICMP メッセージ コード番号を設定する機能を有効にできます。 [Msg] : キーワードを使用して、種類とコードの組み合わせを指定できます。[ICMP message] ドロップダウン リストをアクティブにします。[ICMP Type] フィールドを無効にします。
ICMP Message[1]	administratively-prohibited	ドロップダウン リストから選択したキーワードを使用して、ICMP の種類とコードの組み合わせを指定できます。
ICMP Type[1]	0	0 ～ 255 の数字。このフィールドは、[Type/Code] を選択すると有効になります。
Use ICMP Code[1]	オフ	選択すると、[ICMP Code] フィールドが有効になります。
ICMP Code[1]	0	0 ～ 255 の数字。特定の種類の ICMP メッセージを ICMP メッセージ コードでさらに選別できるメッセージ コード オプション

1. 必須フィールド。