CHAPTER 8

WAAS デバイス用の IP アクセス コントロール リストの作成および管理

この章では、Wide Area Application Service（WAAS）の Central Manager GUI を使用して、WAAS デバイス用の IP Access Control List（ACL; アクセス コントロール リスト）を集中的に作成し、管理する方法について説明します。

この章の構成は、次のとおりです。

（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」は、WAE アプライアンスおよび WAE ネットワーク モジュール（NME-WAE デバイス ファミリ）を示します。

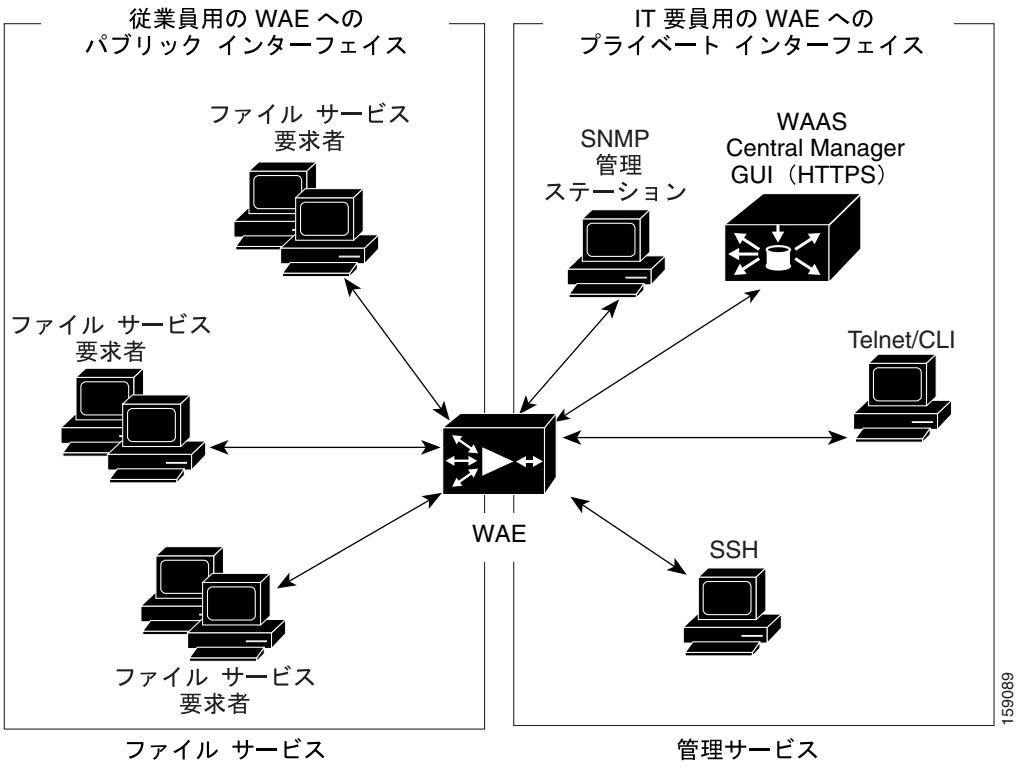
（注） ACL は、WAE にインストールされた Cisco WAE Inline Network Adapter 上のインライン インターフェイスに適用されません。

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 デバイス上の指定したインターフェイスを通過する IP パケットを許可または拒否できるようにして、パケットを選別できます。パケットの選別により、ネットワーク経由のパケットの移動を制御できます。この制御により、ネットワーク トラフィックを制限し、特定のユーザまたはデバイスによるネットワーク使用を制限できます。

WAAS 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も提供しています。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; セキュア シェル）、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 8-1 を参照）。

図 8-1　IP ACL を使用して WAE 上の特定のインターフェイスへのアクセスを制御する方法の例



WAAS ソフトウェアは、WAAS デバイスへのアクセスと WAAS デバイス経由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。IP ACL を使用すると、コーポレート ネットワークに損害を与えるハッカー、ワーム、およびウイルスの潜入を減らすことができます。

次の例は、WAAS デバイスが存在する環境で、IP 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ことを望んでいます。
- 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ことを望んでいます。

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 IP 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、主にセキュリティの理由から、インターフェイスがアクセスに使用できるポートを慎重に制限することです。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、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。
- Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）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 とルータの両方に IP ACL が必要です。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。

WAE 上の IP ACL とアプリケーション定義ポリシーの優先順位について

WAE がパススルー モードで動作しているときは、すべてのトラフィックが WAE によって処理されるため、WAE に設定された IP ACL で制御されます。WAE の着信トラフィックに適用して IP レベルでアドレス指定するポリシーを定義するには、WAE に設定された IP ACL を使用します。

WAE で定義される IP ACL は、WAE で定義されている WAAS アプリケーション定義ポリシーより常に優先します。たとえば、ブランチ オフィスの Edge WAE に、次の条件を持つ拡張 IP ACL を定義できます。

- ip access-list extended DENY_10.56.65.21
- deny ip any host 10.56.65.21
- permit ip any

この拡張 IP ACL は、次のように Edge WAE のインターフェイスに適用されます。

- インターフェイス GigabitEthernet 1/0
- IP アドレス 10.56.64.166 255.255.255.240
- IP アクセス グループ DENY_10.56.65.21 out

このインターフェイスは、Edge WAE で動作している唯一のインターフェイスです。この場合、この Edge WAE で、どのようなアプリケーション定義ポリシーが設定されているかは無関係です。Edge WAE は、IP 層での 10.56.65.21 からのすべての TCP トラフィックを削除し、トラフィックを転送しません（たとえば、Edge WAE は、トラフィックを削除し、データセンターの Core WAE へ転送しません）。

（注）　WAAS CLI の代わりに WAAS Central Manager GUI を使用して、IP ACL を集中的に設定し、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.8-4）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なければなりません。
- IP ACL 名は 30 文字以内に制限され、余白や特殊文字を使用できません。
- 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のようなアプリケーションにアクセスしようとするデバイスは、アクセスを許可されるために信頼されるデバイスのリストに含まれる必要があります。
- すでに設定されている任意の標準 IP ACL を SNMP と WCCP に関連付けることができます。ただし、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 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 GUI から、**[Devices] > [Devices]** を選択します。

ステップ 2　IP ACL を作成したいデバイス（たとえば、bd-s14 という名前の Core WAE）の名前の横にある **[Edit]** アイコンをクリックします。

ステップ 3　[Contents] ペインの上にある **[Expand All]** をクリックします。

ステップ 4　[Contents] ペインで、**[General Settings] > [Network] > [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 5　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 として作成したい場合は、[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 6　**[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。

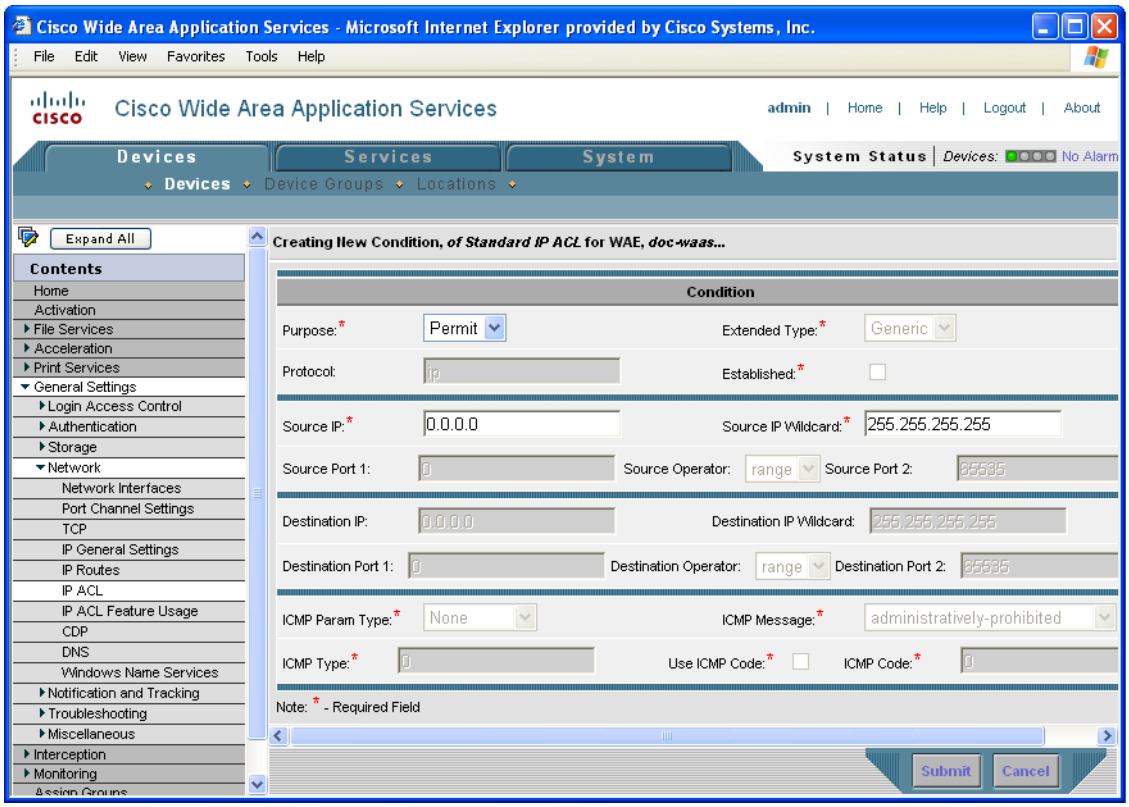
ステップ 7　作成した test1 という名前の標準 IP ACL に条件を追加します。

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 8-2 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 8-2　[Extended IP ACL] ウィンドウでの新しい状態の作成



b. 次のように、作成している IP ACL の種類に有効になってい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 8 へ進みます。
- 拡張 IP ACL 用の条件を設定するには、ステップ 9 へ進みます。

ステップ 8　次のように、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] フィールドで、送信元の IP アドレスを入力します。

c. [Source IP Wildcard] フィールドで、送信元の IP アドレスのワイルドカードを入力します。

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 8-1 に、標準 IP ACL のフィールドを示します。

表 8-1　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*	0.0.0.0	10 進法記の 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*	255.255.255.255	10 進法表記の 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。無視したいビット位置には 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 9　次のように、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 8-2 を参照）。

表 8-2　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*	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. 選択した種類に有効になったフィールドで、データを入力します（詳細については、表 8-4 ～ 表 8-7 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 10　次のように、IP ACL から個々の状態を変更または削除します。

a. 変更したい 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. 変更または削除したい条件の横にある **[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、必要に応じて使用できる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**ごみ箱**（**[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 11　次のように、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 に関連付けたい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. [Contents] ペインで、**[General Settings] > [Network] > [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 8-3 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たくない場合は、**[Do Not Set]** を選択します。

表 8-3　IP ACL Feature Settings（IP ACL 機能設定）

WAAS Central Manager GUI 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、WAE または WAAS Central Manager デバイスとして動作している WAAS デバイス用にサポートされています。
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、WAE として動作し、WAAS Central Manager デバイスとして動作していない WAAS デバイス用にサポートされています。WCCP は、WAE だけでサポートされています。WAAS Central Manager デバイスではサポートされていません。

d. **[Submit]** をクリックして、設定を保存します。

ステップ 12 次のように、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したい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. [Contents] ペインで、**[General Settings] > [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。このウィンドウは、そのデバイスで使用できるすべてのインターフェイスを表示します。

（注） [Port Type] 列には、EtherChannel 設定を示す PortChannel インターフェイスが含まれる場合があります。WAAS ソフトウェア用の EtherChannel では、最大 4 個の同じ速度のネットワーク インターフェイスを 1 つの仮想インターフェイスにグループ化することができます。

c. IP ACL を適用したい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。[Modifying Network Interface] ウィンドウが表示されます。

d. ウィンドウの一番下まで移動し、[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 プロパティは着信 IP ACL と発信 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 13 **[Submit]** をクリックして、設定を保存します。

ステップ 14（任意）次のように、IP ACL を削除します。

a. 削除したい 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. [Contents] ペインで、**[General Settings] > [Network] > [IP ACL]** を選択します。

c. 変更したい IP ACL の名前（たとえば、test1）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] —** このオプションは、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] —** このオプションは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**ごみ箱**（**[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. 条件だけを削除するには、タスクバーの小型 **[Delete All Conditions** 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** グローバル設定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、**ip access-group** インターフェイス設定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** グローバル設定コマンドを使用できます。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** グローバル設定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.8-4] のステップ 9 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 8-4 を参照してください）
- TCP（表 8-5 を参照してください）
- UDP（表 8-6 を参照してください）
- ICMP（表 8-7 を参照してください）

表 8-4　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*	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*	0.0.0.0	10 進法記の 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*	255.255.255.255	10 進法表記の 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。無視したいビット位置には 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 進法表記の 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 進法表記の 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。無視したいビット位置には 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 8-5　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*	TCP	TCP インターネット プロトコルと一致します。
Established	未選択（false）	選択すると、TCP データグラムに Acknowledgment（ACK; 確認応答）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*	0.0.0.0	10 進法記の 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*	255.255.255.255	10 進法表記の 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。無視したいビット位置には 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 ポート名は次のとおりです。ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www。
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 Port 1 を参照してください。
Destination IP	0.0.0.0	10 進法表記の 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 進法表記の 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。無視したいビット位置には 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 ポート名は次のとおりです。ftp、ftp-data、https、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、rtsp、ssh、telnet、および www。
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 8-6　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*	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*	0.0.0.0	10 進法記の 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*	255.255.255.255	10 進法表記の 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。無視したいビット位置には 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 ポート名は次のとおりです。bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp。
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 Port 1 を参照してください。
Destination IP	0.0.0.0	10 進法表記の 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 進法表記の 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。無視したいビット位置には 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 ポート名は次のとおりです。bootpc、bootps、domain、mms、netbios-dgm、netbios-ns、netbios-ss、nfs、ntp、snmp、snmptrap、tacacs、tftp、および wccp。
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 8-7　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*	ICMP	ICMP インターネット プロトコルと一致します。
Source IP*	0.0.0.0	10 進法記の 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*	255.255.255.255	10 進法表記の 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。無視したいビット位置には 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 進法表記の 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 進法表記の 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。無視したいビット位置には 1、意味のあるビット位置には 0 を入れます。
ICMP Param Type*	None	**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*	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せを指定できます。
ICMP Type*	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*	未選択	選択すると、[ICMP Code] フィールドが有効になります。
ICMP Code*	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