ACL マネージャの使用

この章では、拡張アクセス リスト（アクセス コントロール リストとも呼ばれます）を設定する方法について説明します。次の項目を取り上げます。

ACL マネージャに関する情報

アクセス コントロール リスト（ACL）は、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。ACL は、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。このリストには、行番号を指定して ACE、送信元アドレス、および宛先アドレスを挿入できます。また、ACE タイプによっては、プロトコル、ポート（TCP または UDP 用）、あるいは ICMP タイプも挿入できます。

[ACL Manager] ダイアログボックスでは、ACL を定義することにより、特定のホストまたはネットワークから別のホストまたはネットワークへのアクセス（使用できるプロトコルやポートなど）を制御できます。

ユーザ セッションに適用する ACL（アクセス コントロール リスト）を設定できます。ACL は、特定のネットワーク、サブネット、ホスト、および Web サーバへのユーザ アクセスを許可または拒否するフィルタです。

- フィルタを定義しない場合は、すべての接続が許可されます。
- ASA は、インターフェイスのインバウンド ACL だけをサポートします。

各 ACL の最後には、許可されないすべてのトラフィックを拒否する、表記されない暗黙のルールが含まれます。トラフィックがアクセス コントロール エントリ（ACE）によって明示的に許可されていない場合には、ASA がそのトラフィックを拒否します。このセクションでは、ACE をルールと呼びます。

ACL および ACE を追加する方法については、「ACL および ACE の追加」（P.21-2）を参照してください。

コンフィギュレーション内の特定の ACL および ACE を検索する方法については、「[ACL Manager] ペインでの検索機能の使用」（P.4-16）を参照してください。

ACL マネージャのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでのみサポートされています。

IPv6 のガイドライン

IPv6 がサポートされます。

その他のガイドラインと制限事項

拡張アクセス リストの作成には、次のガイドラインと制限事項が適用されます。

- アクセス リスト名は、大文字で入力します。これによって、コンフィギュレーションで名前が見つけやすくなります。アクセス リストには、インターフェイスを表す名前（INSIDE など）や、作成する目的を表す名前（NO_NAT や VPN など）を付けることができます。
- TCP プロトコルまたは UDP プロトコルの場合に限り、送信元ポートおよび宛先ポートを指定できます。使用できるキーワードおよび予約済みポート割り当てのリストについては、「TCP ポートと UDP ポート」（P.48-12）を参照してください。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、および Talk は、それぞれに TCP の定義と UDP の定義の両方が必要です。TACACS+ では、ポート 49 に対して 1 つの TCP 定義が必要です。

ACL および ACE の追加

アクセス リスト（ACL）は、1 つまたは複数のアクセス リスト エントリ（ACE）で構成されます。ACL を作成するには、まず ACE を作成し、リスト名を適用します。リストには複数の ACE を追加できますが、1 つのエントリを含む ACL もリストと見なされます。

ACL を追加してからその ACL に ACE を追加するには、次の手順を実行します。

ステップ 1　[Configuration] > [Firewall] > [Advanced] > [ACL Manager] を選択します。

ステップ 2　[Add] > [Add ACL] を選択します。IPv4 または IPv6 トラフィック用に設定可能な ACL を追加します。

ステップ 3　[ACL name] フィールドに ACL を説明する名前を追加し、[OK] をクリックします。

新規作成した ACL がウィンドウに表示されます。

ステップ 4　新たに作成した ACL を選択して、[Add] をクリックし、ドロップダウン リストから [Add ACE] を選択します。

ステップ 5　[Add ACE] ウィンドウの [Action] フィールドで、次のオプション ボタンの 1 つをクリックして、アクションを選択します。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

ステップ 6　トラフィックを許可または拒否する送信元のネットワーク オブジェクト グループ、インターフェイス IP、またはアドレスに対応する IP アドレスを、[Source] フィールドに入力します。

IPv6 アドレスを使用して ACE を設定する場合は、少なくとも 1 つのインターフェイスで IPv6 を事前にイネーブルにしておく必要があります。インターフェイスで IPv6 をイネーブルにする方法については、「IPv6 アドレッシングの設定」（P.13-16）を参照してください。

ステップ 7　宛先を選択して、[Source] セクションにリストされている IP アドレスへのトラフィックの送信を許可または拒否する IP アドレス（ホストまたはネットワーク）を指定します。

ステップ 8　この ACE が適用されるサービスを指定します。既知のサービスをウィンドウに入力するか、[browse] をクリックして、サービスのリストの中から選択できます。

サービス グループを使用すると、照合する複数の連続していないポート番号を指定できます。

たとえば、ポート番号 5、8、9 で HTTP および FTP をフィルタリングする場合は、これらのすべてのポートを含むサービス グループを定義します。サービス グループがない場合、ポートごとに個別のルールを作成する必要があります。

TCP、UDP、TCP-UDP、ICMP、およびその他の IP プロトコル用にサービス グループを作成できます。TCP-UDP プロトコルを使用するサービス グループには、TCP または UDP プロトコルを使用するサービス、ポート、および範囲が含まれます。

- [Protocol]：このルールが適用されるプロトコルを選択します。使用できる値は、ip、tcp、udp、icmp などです。[Protocol and Service] 領域のその他のフィールドは、選択するプロトコルによって異なります。次の項目で、各選択内容の結果について説明します。
- [Protocol: TCP and UDP]：そのルールの TCP/UDP プロトコルを選択します。[Source Port] 領域と [Destination Port] 領域で、ACL がパケットを照合するために使用するポートを指定できます。
- [Source Port/Destination Port]：（*TCP および UDP プロトコルの場合だけ使用可能*）演算子、ポート番号、ポート範囲、またはサービスのリストにあるウェルノウン サービス名（HTTP や FTP など）を指定します。演算子リストで、ACL がポートを照合する方法を指定します。次のいずれかの演算子を選択します。=（ポート番号と等しい）、not =（ポート番号と等しくない）、>（ポート番号より大きい）、<（ポート番号より小さい）、range（範囲内のポート番号のいずれかと等しい）。
- [Group]：（*TCP と UDP プロトコルの場合だけ使用可能*）送信元ポート サービス グループを選択します。[Browse (...)] ボタンをクリックすると、[Browse Source Port] または [Browse Destination Port] ダイアログボックスが開きます。
- [Protocol: ICMP]：定義済みリストから ICMP タイプまたは ICMP グループを選択するか、[Browse (...)] をクリックして、ICMP グループを選択できます。[Browse] ボタンをクリックすると、[Browse ICMP] ダイアログボックスが表示されます。
- [Protocol: IP]：IP プロトコル ボックスで、そのルールの IP プロトコルを指定します。このフィールドを選択した場合、他のフィールドは表示されません。
- [Protocol: Other]：ドロップダウン リストからプロトコルまたはプロトコル グループを選択、またはプロトコル グループを参照できます。[Browse (...)] ボタンをクリックすると、[Browse Other] ダイアログボックスが表示されます。

ステップ 9　（任意）このルールを簡単に説明するテキストを追加します。説明行の長さは最大 100 文字ですが、説明を改行して複数行にすることができます。

（注）　1 つのプラットフォーム（Windows など）上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

ステップ 10　（任意）[Enable Logging] チェックボックスをオンにしてロギングをイネーブルまたはディセーブルにするか、デフォルトのロギング設定を使用するよう指定します。ロギングをイネーブルにすると、[Syslog Level] および [Log Interval] フィールドが使用可能になります。

a.　ロギングをイネーブルにする場合は、ロギング アクティビティを指定するロギング レベルを選択します。デフォルトは Informational です。ログ レベルの詳細については、「重大度」（P.41-3）を参照してください。

b.　ロギング間隔を選択して、選択したログ レベルで送信できるメッセージ数を制限する際の基準となる時間間隔（秒単位）を表示します。

ステップ 11　送信元サービス（TCP、UDP、および TCP/UDP のみ）を設定します。

ステップ 12　ロギング間隔を設定して、ログ メッセージの間隔を秒数で指定します。デフォルトは 300 です。

ステップ 13　ルールが適用される時間範囲を設定します。

ステップ 14　[Apply] をクリックし、ACL および ACE を実行コンフィギュレーションに保存します。

コンフィギュレーション内のすべての ACL を概要表示するには、[ACL Manager] ウィンドウの下にある [Collapse All] をクリックします。コンフィギュレーション内のすべての ACL および ACE を詳細表示するには、[Expand All] をクリックします。

コンフィギュレーション内の特定の ACL および ACE を検索する方法については、「[ACL Manager] ペインでの検索機能の使用」（P.4-16）を参照してください。

ACL マネージャでの標準 ACL の使用

標準 ACL では、（送信元アドレスではなく）宛先 IP アドレスを識別します。標準 ACL をインターフェイスに適用してトラフィックを制御することはできません。

標準 ACL をコンフィギュレーションに追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、ドロップダウン リストから [Add ACL] を選択します。

ステップ 2　[Add ACL] ダイアログボックスで、ACL を識別するための名前または番号を入力します（スペースは使用できません）。

ステップ 3　[OK] をクリックします。

メイン ペインに ACL の名前が表示されます。

ステップ 4　新たに作成した ACL を選択して、[Add] をクリックし、ドロップダウン リストから [Add ACE] を選択します。

[Add ACE] ダイアログボックスが表示されます。

ステップ 5　（任意）特定の位置に ACE を追加する場合は、まず既存の ACE をいずれか 1 つ選択します。その上で [Insert...] をクリックすると、選択した ACE の前に目的の ACE が追加されます。選択した ACE の後に追加する場合は、[Insert After...] をクリックします。

ステップ 6　次のいずれかのオプション ボタンをクリックして、アクションを選択します。

- [Permit]：条件に合致した場合にアクセスが許可されます。
- [Deny]：条件に合致した場合にアクセスが拒否されます。

ステップ 7　[Address] フィールドに、アクセスを許可または拒否する宛先の IP アドレスを入力します。

[Address] フィールドの横にある省略符号ボタンをクリックして、ネットワーク オブジェクトのアドレスを参照することもできます。

ステップ 8　（任意）[Description] フィールドに、ACE の内容がよくわかるような説明を入力します。

この説明は、複数行に渡って入力できますが、各行に入力できるのは最大で 100 文字までです。

（注）　1 つのプラットフォーム（Windows など）上で英語以外の文字でコメントを追加し、それらの文字を別のプラットフォーム（Linux など）から削除しようとした場合、元の文字が正しく認識されないため編集や削除を実行できない可能性があります。この制限は、各種言語の文字をさまざまな方法でエンコードするプラットフォームの依存性によるものです。

ステップ 9　[OK] をクリックします。

新規作成した ACE が ACL に表示されます。

ステップ 10　[Apply] をクリックし、ACE をコンフィギュレーションに保存します。

ACL マネージャの機能履歴

表 21-1 に、この機能のリリース履歴を示します。

表 21-1　拡張アクセス リストの機能履歴

機能名	リリース	機能情報
拡張アクセス リスト	7.0(1)	アクセス リストは、ネットワーク アクセスを制御したり、さまざまな機能を適用するトラフィックを指定したりするために使用されます。拡張アクセス コントロール リストは、1 つまたは複数のアクセス コントロール エントリ（ACE）で構成されます。このリストには、行番号を指定して ACE、送信元アドレス、および宛先アドレスを挿入できます。また、ACE タイプによっては、プロトコル、ポート（TCP または UDP の場合）、または ICMP タイプ（ICMP の場合）も挿入できます。