IP アクセス リストの概要

アクセス コントロール リスト（ACL）は、パケット フィルタリングを実行して、ネットワークを介して移動するパケットと移動先を制御します。パケット フィルタリングによって、ネットワーク トラフィックを制限し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから外部に送信されるのを防ぐことで、セキュリティを実現します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。このモジュールでは、IP アクセス リストの概要について説明します。

IP アクセス リストに関する情報

IP アクセス リストの利点

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケット フィルタリングを実行します。パケット フィルタリングによってユーザーおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセス リストによってトラフィック数を減らすことで、ネットワーク リソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザー、リモート ホスト、およびリモート ユーザーの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。

- 不要なトラフィックまたはユーザーをブロックする：アクセスリストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザー認証に基づいてネットワークへのアクセスを制御できます。また、アクセスリストを使用して、デバイスインターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メールトラフィックはネットワークでルーティングすることを許可し、すべての Telnet トラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザーを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセス リストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS 攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザーを制御するように IP 発信元アドレスを指定します。TCP インターセプト機能を設定することで、接続に関する要求でサーバーにフラッディングが発生しないようにすることができます。
- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセスリストを使用する必要がある境界ルータおよびファイアウォール ルータ

アクセスリストを設定する理由は多数あります。たとえば、アクセスリストを使用して、ルーティング アップデートのコンテンツを制限したり、トラフィック フローを制御したりできます。アクセスリストを設定する最も重要な理由の 1 つは、ネットワークに対するアクセスを制御することで、ネットワークに基本レベルのセキュリティを提供することです。ルータでアクセスリストを設定しない場合、ルータを通過するすべてのパケットは、ネットワークのすべての部分で許可される可能性があります。

アクセスリストで、ネットワークの一部に対してアクセスを許可するホストと、同じ領域に対してアクセスを禁止するホストを設定できます。以下の図では、適切なアクセスリストをルータのインターフェイスに適用することで、ホスト A は Human Resources ネットワークに対するアクセスが許可され、ホスト B は Human Resources ネットワークに対するアクセスが禁止されます。

ファイアウォール ルータにはアクセス リストを使用する必要があります。多くの場合、ファイアウォールルータは内部ネットワークと外部ネットワーク（インターネット）の間に配置されます。また、ネットワークの2つの部分の間に配置されたルータにアクセスリストを使用して、内部ネットワークの特定の部分に発着信するトラフィックを制御できます。

アクセスリストのセキュリティ上の利点を実現するために、場合によっては、少なくとも境界ルータでアクセスリストを設定する必要があります。境界ルータとは、ネットワークのエッジにあるルータです。このようなアクセスリストは、外部ネットワークから、または内部ネットワークのあまり制御されていない領域から、内部ネットワークの機密性が高い領域に対する基本的なバッファとして機能します。このような境界ルータでは、ルータインターフェイスに設定されている各ネットワーク プロトコルに合わせてアクセス リストを設定する必要があります。着信トラフィック、発信トラフィック、またはその両方がインターフェイスでフィルタされるように、アクセス リストを設定できます。

アクセス リストは個々のプロトコル ベースで定義されます。つまり、各プロトコルのトラフィック フローを制御する場合、インターフェイスでイネーブルにするプロトコルごとにアクセス リストを定義する必要があります。

アクセス リストの定義

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザーおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザー アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。

アクセス リストは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アクセス リストの場合、これらのステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。

アクセスリストは名前または番号で識別および参照されます。アクセスリストはパケットフィルタとして動作し、各アクセスリストに定義されている条件に基づいてパケットがフィルタされます。

アクセスリストを構成した後でアクセスリストを有効にするには、アクセスリストをインターフェイスに適用するか（**ip access-group** コマンドを使用）、vty に適用するか（**access-class** コ

マンドを使用）、またはアクセス リストを許容するあらゆるコマンドでアクセス リストを参照する必要があります。複数のコマンドから同じアクセス リストを参照できます。

次の構成では、branchoffices という名前の IP アクセス リストがファスト イーサネット インターフェイス 0/1/0 上で構成され、着信パケットに適用されます。発信元アドレスとマスクのペアで指定されているネットワーク以外は、ファスト イーサネット インターフェイス 0/1/0 にアクセスできません。ネットワーク 172.16.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.16.2.0 上の送信元から発信されるパケットの宛先は、172.31.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.16.7.0 0.0.0.3 any
 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4
!
interface fastethernet 0/1/0
 ip access-group branchoffices in
```

アクセス リストのルール

アクセス リストには、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセス リストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセス リスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、シスコソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** ステートメントまたは **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセス リストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。
- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットが発信インターフェイスにルーティングされる前に、着信アクセス リストがパケットを処理します。ネットワークへのパケット アクセスを拒否するフィルタ条件がある着信アクセス リストは、ルーティング ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。インバウンド アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- アウトバウンドアクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットはアウトバウンドインターフェイスにルーティングされてから、アウトバウ

ンドアクセス リストで処理されます。アウトバウンドアクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。

- アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

ダイヤラリストのアクセスリストルール

次のアクセスリストルールは、Cisco ISR 4000 シリーズ プラットフォームにのみ適用されます。

- シリアルインターフェイス（BRI/PRI）のダイヤラインターフェイスは、出力 ACL を使用してダイヤルアウトします。そのため、ダイヤラリストの ACL 設定は出力 ACL である必要があります。
- ダイヤラのアイドルタイムアウトは、アウトバウンド方向で設定する必要があります。ダイヤラリストの入力 ACL リストを使用したインバウンド ダイヤラ アイドルタイムアウト設定により、セッションがアイドルタイムアウトになります。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙的な **deny** ステートメントによってアクセスに緊急の問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。permit がないと、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙的な deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは **permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは暗黙的な **deny** ステートメントで終了しますが、明示的な **deny** ステートメント（たとえば **deny ip any any**）の使用を推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny**

ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。

- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセスリストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用すると、適切なエントリが削除されます。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **deny** ステートメントを指定した **log** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、インバウンドアクセスリストでは常にフィルタ条件を適用した後に、ルーティングテーブルの検索を行います。アウトバウンドアクセスリストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

名前付きまたは番号付きアクセス リスト

すべてのアクセス リストは、名前または番号で識別されます。名前付きアクセス リストは、番号付きアクセスリストよりも便利です。タスクを思いだしやすく関連性がある、わかりやすい名前を指定できるためです。名前付きアクセスリストでは、ステートメントの順序を変更したり、ステートメントを追加したりできます。

名前付きアクセスリストは、番号付きアクセスリストではサポートされない次の機能をサポートします。

- IP オプションのフィルタリング
- 非隣接ポート
- TCP フラグ フィルタリング
- **no permit** または **no deny** コマンドによるエントリの削除

（注） 番号付きアクセス リストを受け入れるコマンドの中には、名前付きアクセス リストを受け入れないコマンドがあります。たとえば、vty には番号付きアクセス リストだけを使用します。

標準または拡張アクセス リスト

すべてのアクセス リストは、標準または、拡張アクセス リストのいずれかになります。送信元アドレスでフィルタするだけの場合、より簡易な標準アクセスリストで十分です。送信元アドレス以外のアドレスをフィルタする場合、拡張アクセス リストが必要です。

- 名前付きアクセス リストは、**ip access-list** コマンド構文のキーワード **standard** または **extended** に基づいて標準か拡張かが決まります。
- 番号付きアクセス リストは、**access-list** コマンド構文の番号に基づいて標準か拡張かが決まります。標準 IP アクセス リストには 1 ～ 99 または 1300 ～ 1999 の番号が付けられ、拡張 IP アクセス リストには 100 ～ 199 または 2000 ～ 2699 の番号が付けられます。標準 IP アクセス リストの範囲は、当初は 1 ～ 99 のみでしたが、1300 ～ 1999 の範囲に拡張されました（間の番号は、他のプロトコルに割り当てられました）。拡張アクセスリストの範囲も同様に拡張されました。

（注） Cisco IOS XE 16.9.4 以降、オブジェクトグループベースの番号付き ACL を設定するには、**ip access-list** コマンドを使用します。

標準アクセス リスト

標準アクセス リストは、パケットの送信元アドレスのみをテストします（ただし 2 つの例外があります）。標準アクセスリストは送信元アドレスをテストするため、宛先の近くでトラフィックをブロックする際には効率的です。標準アクセス リストのアドレスが送信元アドレスではない例外が 2 つあります。

- アウトバウンド VTY アクセス リストでは、誰かが Telnet を実行しようとすると、アクセス リスト エントリのアドレスは、送信元アドレスではなく宛先アドレスとして使用されます。
- ルートをフィルタする場合、送信元アドレスではなくアドバタイズされたネットワークがフィルタされます。

拡張アクセス リスト

拡張アクセス リストは、任意の場所のトラフィックをブロックするために適しています。拡張アクセス リストは、送信元アドレス、宛先アドレス、およびその他の IP パケット データをテストします。たとえば、プロトコル、TCP または UDP ポート番号、タイプ オブ サービス（ToS）、優先順位、TCP フラグ、IP オプションなどです。また、拡張アクセス リストには、次のように標準アクセス リストにはない機能があります。

- IP オプションのフィルタリング
- TCP フラグのフィルタリング
- パケットの非初期フラグメントのフィルタリング（「Refining an IP Access List」モジュールを参照してください）

（注） 拡張アクセス リストの対象となるパケットは、自律的に切り替えられません。

アクセスを制御するためにフィルタできる IP パケット フィールド

拡張アクセスリストを使用すると、IPパケットに含まれる次の任意のフィールドについてフィルタできます。送信元アドレスおよび宛先アドレスは、アクセスリストの基礎として最もよく指定される 2 つのフィールドです。

- 送信元アドレス - 特定のネットワーキングデバイスまたはホストから送信されるパケットを制御するために、送信元アドレスを指定します。
- 宛先アドレス - 特定のネットワーキングデバイスまたはホストに対して送信されるパケットを制御するために、宛先アドレスを指定します。
- プロトコル - キーワード **eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **udp** で示される IP プロトコル、あるいは 0 ～ 255 の範囲の整数（インターネット プロトコルを示す）で示されるIPプロトコルを指定します。トランスポート層プロトコル（**icmp**、**igmp**、**tcp**、または **udp**）を指定すると、コマンドは固有の構文になります。
  - ポートおよび非隣接ポート - ポート名またはポート番号で TCP または UDP ポートを指定します。ポート番号に非隣接ポート番号は指定できません。ポート番号は、Telnet トラフィックや HTTP トラフィックなどをフィルタする際に有効です。
  - TCP フラグ - TCP パケットに設定された任意のフラグまたはすべてのフラグにパケットが一致することを指定します。特定のフラグについてフィルタすることで、不正な同期パケットを回避できます。
- IP オプション - IP オプションを指定します。IP オプションに基づいてフィルタする理由の 1 つは、IP オプションを含む偽造パケットでルータが飽和状態にならないようにするためです。

アクセス リストのアドレスに対するワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較するときに、対応する IP アドレスを確認するか無視するかをソフトウェアに示すために、ワイルドカード マスクを使用します。注意してワイルドカード マスクを設定することで、許可または拒否テストのために 1 つまたは複数の IP アドレスを指定できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。ビット値は一致する必要があります。

- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。ビット値が一致する必要はありません。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0（すべての値が一致する必要があることを示します）という暗黙的なワイルドカード マスクが想定されます。

サブネットマスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

次の表に、アクセス リストの IP アドレスおよびマスクと、それに一致すると見なされる対応するアドレスの例を示します。

表 *1 : IP* アドレス、ワイルドカード マスク、および一致する結果の例

アドレス	ワイルドカード マスク	一致する結果
0.0.0.0	255.255.255.255	すべてのアドレスはアクセス リスト条件に一致します
172.18.0.0/16	0.0.255.255	ネットワーク 172.18.0.0
172.18.5.2/16	0.0.0.0	ホスト 172.18.5.2 のみが一致します
172.18.8.0	0.0.0.7	サブネット 172.18.8.0/29 のみが一致します
172.18.8.8	0.0.0.7	サブネット 172.18.8.8/29 のみが一致します
172.18.8.15	0.0.0.3	サブネット 172.18.8.15/30 のみが一致します
10.1.2.0	0.0.252.255（マスクの非隣接ビット）	10.1.2.0 ～ 10.1.254.0 に含まれる偶数のネットワークに一致します

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加する場合、アクセスリストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセスリストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

アクセス リストのロギング

Cisco IOS ソフトウェアには、単一の標準または拡張 IP アクセス リスト エントリで許可または拒否されたパケットに関するロギング メッセージ機能があります。つまり、パケットがエントリに一致する場合は常に、パケットに関する情報を提供するロギング メッセージがコンソールに送信されます。コンソールにロギングするメッセージのレベルは、**logging console** グローバル コンフィギュレーション コマンドで制御します。

アクセス リスト エントリをトリガーする最初のパケットによって、即時にロギング メッセージが作成され、表示またはロギングされるまで、以降のパケットは5分間隔で収集されます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

ただし、**ip access-list log-update** コマンドを使用して、アクセス リストに一致する場合（さらに許可または拒否される場合）に、システムでログ メッセージを生成するパケットの数を設定できます。この手順を実行するのは、5分間隔よりも短い頻度でログ メッセージを受信する場合です。

注意 *number-of-matches* 引数を 1 に設定すると、ログ メッセージはキャッシングされずにただちに送信されます。この場合、アクセス リストに一致するパケットごとにログ メッセージが発生します。大量のログ メッセージでシステムが過負荷になる可能性があるため、1に設定することは推奨されません。

ip access-list log-update コマンドを使用する場合でも、5 分タイマーは有効なままなので、各キャッシュのメッセージ数に関係なく、5 分が経過すると各キャッシュは空になります。ログ メッセージを送信するタイミングに関係なく、しきい値が指定されていない場合と同様に、ログ メッセージのキャッシュは消去され、カウントは 0 にリセットされます。

（注） ロギング メッセージが多すぎて処理できない場合、または1秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギングパケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセスリストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

アクセス リスト ロギングの代替方法

ログ オプションを使用したACL内のエントリのパケット マッチングは代替のプロセスです。ACL でログ オプションを使用することは推奨されません。Null0 の宛先インターフェイスで NetFlowエクスポートおよびマッチングを使用することを推奨します。これはCEFパスで実行されます。Null0 の宛先インターフェイスは、ACL によってドロップされるすべてのパケット用に設定されます。

その他の IP アクセス リスト機能

標準または拡張アクセス リストを作成する基本手順以外に、次のようにアクセス リストを強化できます。これらの各方法の詳細については、「Refining an Access List」モジュールを参照してください。

- 拡張アクセス リストの **permit** ステートメントまたは **deny** ステートメントを有効にする日時を指定し、アクセス リストを細かくし、絶対的または定期的な期間に限定することができます。
- 名前付きアクセス リストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセス リストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

RSP3 ポートの関連情報

発信アクセス リストは、RSP3 ではサポートされていません。

アクセス リストを適用する場所

アクセス リストは、デバイスの着信または発信インターフェイスに適用できます。アクセス リストを着信インターフェイスに適用すると、インターフェイスで着信するトラフィックが制御され、アクセス リストを発信インターフェイスに適用すると、インターフェイスから発信されるトラフィックが制御されます。

ソフトウェアは、着信インターフェイスでパケットを受信すると、アクセス リストで設定されているステートメントに対してパケットを検査します。アクセス リストがアドレスを許可している場合は、ソフトウェアはパケットを処理します。着信パケットをフィルタリングするためにアクセス リストを適用すると、フィルタリングされたパケットはデバイスに到達する前に廃棄されるため、デバイスのリソースを節約できます。

発信インターフェイスでは、アクセス リストはインターフェイスから転送（送信）されたパケットをフィルタリングします。発信インターフェイスで Rate-Based Satellite Control Protocol（RBSCP）の TCP アクセス コントロール リスト（ACL）を使用して、発信インターフェイスで TCP 確認応答（ACK）を受けるパケットの種類を制御できます。

debug コマンドを使用してアクセス リストを参照し、デバッグ ログの量を制限できます。たとえば、アクセス リストのフィルタリング基準または一致基準に基づいて、デバッグ ログを送信元または宛先のアドレスまたはプロトコルに制限できます。

アクセス リストを使用して、ルーティング アップデート、ダイヤルオンデマンド（DDR）、および Quality of Service（QoS）機能を制御することができます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IP アクセス リスト コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『Cisco IOS IP Addressing Services Command Reference』
送信元アドレス、宛先アドレス、またはプロトコルに基づくフィルタリング	『Creating an IP Access List and Applying It to an Interface』モジュール
IP オプション、TCP フラグ、非隣接ポート、または TTL に基づくフィルタリング	『Creating an IP Access List to Filter IP Options, TCP Flags, or Noncontiguous Ports』モジュール

標準

標準と RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP アクセス リストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *2 : IP* アクセス リストに関する機能情報

機能名	リリース	機能の設定情報
ACL - IP プロトコル	Cisco IOS XE リリース 3.16	Cisco IOS XE リリース 3.16 では、Cisco ASR 903 ルータのサポートが追加されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。