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その場所を制御します。このような制御によって、ネットワーク トラフィックを制限し、ユーザ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拒否攻撃の可能性を軽減し、ファイアウォールを介したダイナミックで一時的なユーザ 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。

- 機能情報の確認 （1 ページ）
- IP アクセス リストに関する情報 （2 ページ）
- 次の作業 （14 ページ）
- その他の参考資料 （15 ページ）

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

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、リモート ホスト、およびリモート ユーザ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 コントロール リストの制約事項

- **deny ip any any** コマンドは、その前に permit tcp any any *port-number* コマンドまたは permit udp any any *port-number* コマンドが使用されている場合、最初にフラグメント化されていないパケットを拒否しません。

  例:

  ```
  permit tcp any any eq 3000
  deny ip any any fragment
  ```

  ポート番号 4000 の TCP ストリームは、最初にフラグメント化されていないパケットに対して拒否されません。ACE には TCP ポート情報があるため、最初のフラグメントに対して正常に機能します。

セキュリティ ACL の制約事項

- 出力 ACL はサポートされていません。
- 入力 MAC ACL は EFP インターフェイスでのみサポートされています。
- 入力 IP ACL は EFP インターフェイスでのみサポートされています。
- IPv6 ACL はサポートされません。
- MAC ACL は、予約済み MAC アドレスではサポートされていません。
- MAC ACL では、フィルタ条件の 1 つとしてイーサネットタイプはサポートされていません。
- ACL 統計はサポートされていません。
- ACL ロギングはサポートされていません。

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。インバウンド トラフィック、アウトバウンド 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 アドレス リストの場合、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、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。

アクセスリストを設定しても、有効になるのは、アクセスリストがインターフェイスに適用されるか（**ip access-group** コマンドを使用）、仮想端末回線（VTY）に適用されるか（**access-class** コマンドを使用）、アクセスリストを受け入れるその他のコマンドで参照されてからです。アクセスリストの用途は多様なので、多くの Cisco IOS ソフトウェアコマンドの構文では、アクセスリストへの参照を受け入れています。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。

次の設定の抜粋で、先頭の 3 行は branchoffices という IP アクセスリストの例です。これは着信パケットのシリアルインターフェイス 0 に適用されます。このインターフェイスにアクセスできるのは、個々の各送信元アドレスとマスク ペアで指定されているネットワーク上の送信元のみです。ネットワーク 172.20.7.0 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 172.29.2.0 上の送信元から発信されるパケットの宛先は、172.25.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.20.7.0 0.0.0.3 any
 20 permit 172.29.2.0 0.0.0.255 host 172.25.5.4
!
interface serial 0
 ip access-group branchoffices in
```

アクセス リストのソフトウェア処理

アクセスリストがインターフェイス、vty に適用されるとき、または他の Cisco IOS コマンドにより参照されるときの、Cisco IOS ソフトウェアによる処理方法を説明した一般的な手順を次に示します。この手順は、アクセス リスト エントリが 13 以下のアクセス リストに適用されます。

- ソフトウェアが IP パケットや各パケットのテスト部分を受け取ります。これらは、アクセスリストの条件に一度に 1 つずつ（**permit** または **deny** ステートメント）照らし合わせてフィルタリングされます。たとえば、ソフトウェアは、**permit** あるいは **deny** ステートメントの送信元アドレスおよび宛先アドレスに照らし合わせてパケットの送信元アドレスおよび宛先アドレスをテストします。
- パケットがアクセス リストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リスト ステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセスリストがパケットを拒否する場合、ソフトウェアはパケットを廃棄し、ICMP ホスト到達不能メッセージを返します。
- いずれの条件とも一致しなかった場合、パケットは廃棄されます。これは、各アクセスリストが暗黙の **deny** ステートメントで終了するためです。言い換えると、パケットが各ステートメントに対してテストされたときまでに許可されないと、このパケットは拒否されます。

リリース 12.4、12.2S、12.0S などの後の Cisco IOS リリースでは、デフォルトでは、13 個を超えるアクセスリストエントリを持つアクセスリストは、13 個以下のエントリを持つアクセスリストとは異なる方法で処理されます。効率を高めるために、13 を超えるエントリが含まれるアクセスリストは、trie ベースのルックアップアルゴリズムを使用して処理されます。このプロセスは自動的に行われます。設定する必要はありません。

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、Cisco 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。
- 発信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。着信パケットは発信インターフェイスにルーティングされてから、発信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。

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。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- 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。
- 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、着信アクセス 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。発信アクセス 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 リストと番号付きアクセス リストはコマンド構文が異なります。名前付きアクセスリストは、Cisco IOS リリース 11.2 以降と互換性があります。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。用途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 リストよりも新しく、番号付きアクセス リストではサポートされていない次の機能をサポートします。

- TCP フラグ フィルタリング
- IP オプション フィルタリング
- 非隣接ポート
- 再帰アクセスリスト
- **no permit** または **no deny** コマンドでエントリを削除する機能

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、仮想端末回線では番号付きアクセスリストのみが使用されます。

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。

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）、TCP フラグ、IP オプション、TTL 値などです。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）
- 時間ベースのエントリ（「時間ベースおよび分散型時間ベースのアクセスリスト」および「Refining an IP Access List」モジュールを参照してください）
- ダイナミックアクセスリスト（「IPアクセスリストのタイプ」の項を参照してください）
- 再帰アクセスリスト（「IP アクセスリストのタイプ」の項および「Configuring IP Session Filtering [Reflexive Access Lists]」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

アドレス	ワイルドカード マスク	一致する結果
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	0.0.254.255（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。

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。

時間ベースおよび分散型時間ベースのアクセスリスト

時刻ベースのアクセス リストでは、その日または週の特定の時刻に基づいて、アクセス リスト エントリを実装します。これは、アクセス リスト エントリを常に有効にしない場合、または適用されるとすぐに有効にする場合に適した方法です。時刻と日付に基づいて許可または拒否条件の実施を細かくするには、時刻ベースのアクセス リストを使用します。

分散型時間ベースのアクセスリストは、Cisco 7500 シリーズ ルータのラインカードでサポートされているものです。時間ベースのアクセスリストを使用して設定されたインターフェイス宛てのパケットは、ラインカードを介して分散スイッチングされます。

IP アクセスリストのタイプ

複数のタイプのアクセスリストがあり、トリガー方法、一時的な性質、または通常のアクセスリストとの動作の違いによって区別されています。

認証プロキシ

認証プロキシでは、動的かつユーザごとの認証と認可、業界標準の TACACS+ および RADIUS 認証プロトコルを使用したユーザの認証が可能です。ユーザによる接続の認証と認可により、ネットワーク攻撃に対するより強力な保護が可能になります。

コンテキストベース アクセス コントロール

コンテキストベースアクセス制御（CBAC）は、ネットワーク層とトランスポート層の情報だけでなく、アプリケーション層プロトコル情報（FTP 情報など）も参照して、TCP および UDP 接続の状態を学習します。CBAC は、個々の接続の接続状態情報を管理します。この状態情報は、パケットを許可するか拒否するかについてインテリジェントな判断を行うために使用され、ファイアウォールの一時的な開口部を動的に作成および削除します。

ロックアンドキー機能を使用したダイナミックアクセスリスト

ダイナミックアクセスリストは、Telnet を使用して指定されたユーザに、ファイアウォールを通過して指定されたホストに到達するための一時的なアクセスを提供します。ダイナミックアクセスリストには、ユーザ認証および認可が関係します。

再帰アクセスリスト

再帰アクセスリストは、上位層の IP プロトコルセッションのフィルタリングを提供します。これには、新しい IP セッションの開始時に自動的に作成される一時的なエントリが含まれています。これは、インターフェイスに適用される名前付き拡張 IP アクセスリスト内でネストされます。再帰アクセスリストは、通常、内部ネットワークと外部ネットワーク間でトラフィックを渡す境界ルータで設定されます。これは多くの場合、ファイアウォールルータです。再帰アクセスリストは、アクセスリスト内でネストされ、後続のステートメントを検査する必要があるため、暗黙的な deny ステートメントで終了しません。

アクセス リストを適用する場所

アクセスリストをインターフェイスに適用する場合、**in**（インバウンド）と **out**（アウトバウンド）のいずれを指定するかについては慎重に考慮してください。着信または発信インターフェイスに対してアクセスリストを適用して、ルータのインターフェイスで発着信するトラフィックまたはプロセスレベルを制御します（TTL 値に基づいてフィルタする場合）。

- インバウンド アクセス リストをインターフェイスに適用すると、ソフトウェアはパケットを受信した後に、アクセス リスト ステートメントに対してパケットを確認します。アクセスリストでパケットが許可されている場合、ソフトウェアはパケットの処理を続行します。結果として、着信パケットに関するフィルタリングによって、フィルタされたパケットはルータを通過しないため、ルータ リソースを節約できます。

- アウトバウンド パケットに適用するアクセス リストは、ルータをすでに通過したパケットをフィルタします。アクセスリストに合格したパケットは、インターフェイスから伝送（送信）されます。
- Rate-Based Satellite Control Protocol（RBSCP）の TCP ACL 分割機能は、発信インターフェイスで使用できる機能の一例です。アクセスリストで、TCP ACK 分割の対象となるパケットを制御します。

インターフェイスに適用する以外の方法でもアクセスリストを使用できます。次に、アクセスリストを適用できるその他の場所を示します。

- 着信接続および発信接続を特定の（シスコデバイスへの）vty とアクセスリスト内のアドレスにあるネットワークデバイスとの間に制限するには、アクセスリストを回線に適用します。「Controlling Access to a Virtual Terminal Line」モジュールを参照してください。
- **debug** コマンドからアクセスリストを参照すると、表示される情報量は、アクセスリストで許可されている情報にのみ限定されます。たとえば、送信元、宛先、プロトコルなどです。
- アクセス リストは、ルーティング アップデートの制御、ダイヤルオンデマンド ルーティング（DDR）の制御、および Quality of Service（QoS）機能の制御などに使用できます。これらの機能にアクセスリストを使用する方法については、該当する設定の章を参照してください。

次の作業

最初に制限する対象を決定してから、目標を達成するアクセスリストのタイプを選択する必要があります。次に、指定したフィールドの値に基づいてパケットを許可または拒否するアクセスリストを作成し、最後にそのアクセスリストを適用します（その配置を決定します）。

制限する対象と必要なアクセスリストのタイプを決定していると想定すると、次の手順はアクセスリストを作成することです。送信元アドレス、宛先アドレス、またはプロトコルに基づいてアクセスリストを作成する方法については、「IP アクセスリストの作成とインターフェイスへの適用」モジュールで説明されています。『Creating an IP Access List to Filter IP Options, TCP Flags, Noncontiguous Ports, or TTL Values』の説明に従って、他のフィールドでフィルタ処理するアクセスリストを作成できます。仮想回線へのアクセスを制御する場合は、『Controlling Access to a Virtual Terminal Line』を参照してください。アクセスリストの目的がルーティング アップデートまたは QoS 機能を制御することの場合は、たとえば、適切な技術に関する章を参照してください。

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
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
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 Application 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』
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, Noncontiguous Ports, or TTL Values』
vty 回線へのアクセスの制限	『Controlling Access to a Virtual Terminal Line』

標準

標準	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 リリース、およびフィーチャ セットに関する MIB を探して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

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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