



## アクセスコントロールリストの概要

---

アクセスリストは、パケットをデバイスのインターフェイスで転送するかブロックするかを制御して、ネットワークトラフィックをフィルタリングします。デバイスは各パケットを調べ、アクセスリスト内で指定されている基準に基づいて、そのパケットの転送またはドロップを決定します。

アクセスリストで指定できる条件には、トラフィックの送信元アドレス、トラフィックの宛先アドレス、または上位層のプロトコルなどが含まれます。



---

(注) これらのリストは認証を必要としないため、一部のユーザは基本的なアクセスリストを回避できる可能性があります。

---

- [アクセスコントロールリストについて \(1 ページ\)](#)
- [アクセスコントロールリストの概要に関する追加情報 \(11 ページ\)](#)

## アクセスコントロールリストについて

アクセスリストは、パケットをデバイスのインターフェイスで転送するかブロックするかを制御して、ネットワークトラフィックをフィルタリングします。デバイスは各パケットを調べ、アクセスリスト内で指定されている基準に基づいて、そのパケットの転送またはドロップを決定します。

アクセスリストで指定できる条件には、トラフィックの送信元アドレス、トラフィックの宛先アドレス、または上位層のプロトコルなどが含まれます。



---

(注) これらのリストは認証を必要としないため、一部のユーザは基本的なアクセスリストを回避できる可能性があります。

---

## 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のフィルタ処理を行います。

アクセスリストを設定しても、アクセスリストがインターフェイスまたは仮想端末回線 (VTY) に適用されるか、アクセスリストを受け入れるコマンドで参照されるまでは、有効になりません。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。

次に、**branchoffices** という名前のIP アクセスリストを作成するための設定例を示します。ACL は着信パケットの **gigabitEthernet** 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
!
gigabitEthernet 1/0/1
 ip access-group branchoffices in
```

## アクセス コントロール リストの機能

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、ルーティングアップデートのコンテンツの制限や、トラフィック フローの制御などです。アクセス リストを設定する最も重要な理由の1つは、このモジュールの要であるネットワークにセキュリティを提供することです。

アクセスリストを使用することで、ネットワークにアクセスするための基本的なセキュリティレベルが実現します。デバイスでアクセスリストを設定しないと、デバイスを通ずるすべてのパケットに、ネットワーク全体へのアクセスが許可されます。

アクセスリストでは、あるホストにはネットワークの一部へのアクセスを許可する一方、別のホストにはそれと同じ領域へのアクセスを禁止することが可能です。次の図では、ホストAにはヒューマンリソースネットワークへのアクセスが許可されていますが、ホストBにはヒューマンリソース ネットワークへのアクセスが禁止されています。

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定義することもできます。たとえば、電子メールトラフィックのルーティングを許可し、同時にすべての Telnet トラフィックをブロックすることができます。

## IP アクセス リストの目的

アクセス リストは、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。この処理は、ネットワーク トラフィックを制限し、ユーザやデバイスによるネットワークへのアクセスを制限するのに役立ちます。アクセス リストの用途は多様なので、多くのコマンド シンタックスでアクセス リストが参照されます。アクセス リストを使用して、次のようなことを実行できます。

- インターフェイスでの着信パケットのフィルタリング
- インターフェイスでの発信パケットのフィルタリング
- ルーティング アップデートの内容の制限
- アドレスまたはプロトコルに基づくデバッグ出力の制限
- 仮想端末回線アクセスの制御
- 輻輳回避、輻輳管理、プライオリティおよびカスタム キューイングなどの高度な機能に使用されるトラフィックの特定または分類
- ダイアル オンデマンド ルーティング (DDR) 呼び出しのトリガー

## ACL を設定する理由

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、スイッチング 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。デバイスでアクセス リストを設定しない場合、デバイス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。たとえば、適切なアクセス リストをデバイスのインターフェイスに適用することで、ホスト A にはヒューマン リソース ネットワークへのアクセスが許可され、ホスト B にはヒューマン リソース ネットワークへのアクセスが禁止されます。

ネットワークの2つの部分の間に配置されたデバイスにアクセス リストを使用して、内部ネットワークの特定の部分で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、少なくとも境界デバイスでアクセス リストを設定する必要があります。境界デバイスとは、ネットワークのエッジにあるデバイスです。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。このような境界デバイスでは、デバイスの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、あるいはコマンドで参照されるときの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。
- 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。

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 コントロール リスト (ACL) 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。一致が見つかったら、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

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。
- パケットがアウトバウンド インターフェイスに送信される前に、インバウンド 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インバウンド アクセス リストは、ルート 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。

## 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、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、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。

## 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。

## 送信元アドレスと宛先アドレス

IP パケットの送信元アドレスと宛先アドレスのフィールドは、アクセス リストの基礎となる典型的な2つのフィールドです。送信元アドレスを指定して、特定のネットワーク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します。宛先アドレスを指定して、特定のネットワークング デバイスまたはホストに送信されるパケットを制御します。

## 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트리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

アドレス	ワイルドカード マスク	一致する結果
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。

## ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット (MAC) ACL をサポートします。

- IP ACL は、TCP、ユーザデータグラムプロトコル (UDP)、インターネットグループ管理プロトコル (IGMP)、およびインターネット制御メッセージプロトコル (ICMP) などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

## サポートされる ACL

スイッチは、トラフィックをフィルタリングする ACL の次のタイプをサポートします。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセスコントロールします。アクセスリストの各タイプ (IPv4 および MAC) のそれぞれの入力方向に、レイヤ 2 インターフェイスに対するポート ACL を適用できます。

## ポート ACL

ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL を使用できるのは、物理インターフェイスだけです。EtherChannel インターフェイスでは使用



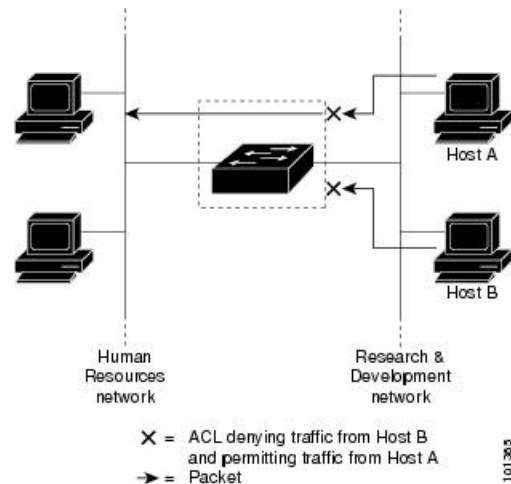
できません。ポート ACL は、着信方向のインターフェイスに適用できます。次のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエン트리とどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 1: ACL によるネットワーク内のトラフィックの制御

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマンリソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2



インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセスリストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。



- (注) レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

## アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ (ACE) の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

### ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ (ACE) には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報 (TCP や UDP などのプロトコル タイプを含む) をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。



- 注 L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

### 例 : ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセスリスト 102 を例にとって説明します。

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
Device(config)# access-list 102 deny tcp any any
```



(注) 最初の2つのACEには宛先アドレスの後に **eq** キーワードがありますが、これは既知のTCP宛先ポート番号がそれぞれシンプルメール転送プロトコル (SMTP) および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE (permit) と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。

- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが2つめのACE (deny) と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2つめのACE と一致しません。残りのフラグメントは3つめのACE (permit) と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが4つめのACE (deny) と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて4つめのACE と一致します。

## アクセスコントロールリストの概要に関する追加情報

### 関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)</i>

関連項目	マニュアル タイトル
ACL	<p>詳細については、以下を参照してください。</p> <ul style="list-style-type: none"><li>『Security Configuration Guide』の「Configuring IPv4 Access Control Lists」</li><li>『Security Configuration Guide』の「Configuring IPv6 Access Control Lists」</li></ul>