IP アクセス リストの精緻化

アクセス リストを作成している間、または作成した後に、アクセス リストを精緻化するにはいくつかの方法があります。アクセス リストのエントリの順序を変更したり、アクセス リストにエントリを追加したりできます。また、アクセス リスト エントリを日または週の特定の時間帯に制限したり、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

IP アクセス リストの精緻化に関する情報

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。

シーケンス番号を使用して、ユーザーはアクセス リスト エントリを追加し、それを並べ替えることができるようになりました。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 シーケンス番号の利点

アクセス リスト シーケンス番号は、アクセス リストで **permit** または **deny** コマンドを開始する番号です。シーケンス番号により、エントリがアクセス リストに表示される順序が決定されます。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。

シーケンス番号を設定する前に、アクセス リストの末尾にアクセス リスト エントリを追加できるため、アクセス リスト全体の再設定が必要になるリストの末尾以外の位置では、ステートメントの追加が必要になります。アクセス リスト内でのエントリの位置を指定する方法はありません。以前は、既存のリストの途中にエントリ（ステートメント）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とき、アクセス リストの目的の位置に配置されるように、シーケンス番号を選択します。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。シーケンス番号により、アクセス リストの変更を簡単に実行できるようになりました。

シーケンス番号の動作

- 以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は10ずつ増分されます。最大シーケンス番号は2147483647です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- （シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。
- 既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

- グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。
- シーケンス番号が不揮発性生成（NVGEN）されることはありません。つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号と増分に戻されます。この機能は、シーケンス番号をサポートしないソフトウェア リリースとの下位互換性を保つために提供されています。

- この機能は、名前付きおよび番号付きの標準および拡張IPアクセス リストと連動します。

時間範囲の利点

時間範囲の利点および可能な使用法として、次のことが挙げられます。

- ネットワーク管理者は、リソースへのユーザーアクセスの許可または拒否の制御をより強化できます。これらのリソースとして、アプリケーション（IPアドレス/マスク ペアとポート番号によって特定されます）、ポリシールーティング、またはオンデマンドリンク（ダイヤラへの関連トラフィックとして認識されます）があります。
- ネットワーク管理者は、次に示すような、時刻ベースのセキュリティ ポリシーを設定できます。
  - アクセス リストを使用した境界セキュリティ
  - IP セキュリティ プロトコル（IPsec）を使用したデータの機密性保持
- プロバイダーのアクセス レートが一日の時間帯によって異なるときは、トラフィックは自動的にコスト効率よく再ルーティングすることが可能です。
- ネットワーク管理者は、ロギング メッセージを制御できます。アクセス リスト エントリは、一日の特定の時間帯にトラフィックをロギングすることはできますが、常にロギングすることはできません。したがって、管理者はピーク時間中に生成された多くのログを分析することなく、単にアクセスを拒否できます。

パケットの非初期フラグメントをフィルタリングする利点

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックするには、拡張アクセス リストを使用してパケットの非初期フラグメントをフィルタリングします。まず、次の概念を理解しておく必要があります。

フラグメントを拒否する追加の IP アクセス リスト エントリで **fragments** キーワードが使用されている場合、フラグメント制御機能を使用すると、次のような利点があります。

追加のセキュリティ

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックできます。不要なフラグメントは、受信側にリアセンブリ タイムアウトになるまで残りません。これは、このようなフラグメントは受信側に送信される前にブロックされるためです。不要なトラフィックを大量にブロックすることで、セキュリティが高まり、ハッカーから攻撃を受けるリスクが軽減されます。

コスト削減

パケットの不要な非初期フラグメントをブロックすると、ブロックしたいトラフィックに注意を払う必要がなくなります。

使用ストレージの削減

パケットの不要な非初期フラグメントが受信側に届かないようにブロックすることで、宛先はリアセンブリ タイムアウトになるまでフラグメントを保存する必要がなくなります。

予期される動作

非初期フラグメントは、初期フラグメントと同様に扱われます。予期されないポリシー ルーティング結果や、ルーティングされるべきでないパケットのフラグメントが生じる可能性も低くなります。

フラグメントのアクセス リスト処理

fragments キーワードを指定するかどうかによるアクセス リスト エントリの動作は、次のようにまとめることができます。

アクセス リスト エントリの状態...	結果

...**fragments** キーワードが指定されず（デフォルト）、すべてのアクセス リスト エントリ情報が一致する	レイヤ 3 情報のみを含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	
	レイヤ 3 およびレイヤ 4 情報を含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケットと先頭フラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。非初期フラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、非初期フラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

アクセス リスト エントリの状態...	結果
...**fragments** キーワードが指定され、すべてのアクセス リストエントリ情報が一致する	アクセス リスト エントリは、非初期フラグメントにのみ適用されます。 レイヤ 4 情報を含むアクセス リスト エントリに **fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加することはできません。IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。初期フラグメントは、アクセスリストの **fragments** キーワードが設定された **permit** または **deny** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリによって許可または拒否されるまで、次のアクセス リスト エントリと比較されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには **fragments** キーワードは含まれず、初期フラグメントに適用されます。ペアの 2 番目の **deny** エントリには **fragments** キーワードは含まれ、以降のフラグメントに適用されます。同じホストに複数の **deny** エントリがあり、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセス リスト エントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

IP アクセス リストを精緻化する方法

このモジュールで説明する作業では、アクセスリストを精緻化するためのさまざまな方法を示します（アクセスリストを作成するときに精緻化しなかった場合に利用できます）。アクセス リスト エントリの順序変更、アクセス リストへのエントリの追加、日または週の特定の時間帯でのアクセス リスト エントリの制限などを実行できます。また、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

シーケンス番号を使用したアクセス リストの変更

既存のアクセスリストへのエントリの追加、エントリの順序変更、または（将来の変更に対応するための）アクセス リストのエントリの番号付けを行うには、次の手順を実行します。

（注） アクセス リストからエントリを削除する場合は、コマンドの **no deny** または **no permit** 形式を使用するか、あるいはステートメントにシーケンス番号がすでに指定されている場合は **no** *sequence-number* コマンドを使用するだけです。

（注）
- アクセス リスト シーケンス番号は、ダイナミック、リフレクシブ、またはファイアウォールのアクセス リストをサポートしていません。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list resequence** *access-list-name starting-sequence-number increment*
4. **ip access-list** {**standard**| **extended**} *access-list-name*
5. 次のいずれかを実行します。
   - *sequence-number* **permit** *source source-wildcard*
   - *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
6. 次のいずれかを実行します。
   - *sequence-number* **deny** *source source-wildcard*
   - *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]
7. 必要に応じてステップ 5 とステップ 6 を繰り返し、目的とするシーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。
8. **end**
9. **show ip access-lists** *access-list-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list resequence** *access-list-name starting-sequence-number increment* 例：	開始シーケンス番号と、シーケンス番号の増分を使用して、指定した IP アクセス リストを並べ替えます。

	コマンドまたはアクション	目的
	`Router(config)# ip access-list resequence kmd1 100 15`	• この例では、kmd1 という名前のアクセス リストを並べ替えます。開始シーケンス番号は100、増分は 15 です。
ステップ 4	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Router(config)# ip access-list standard xyz123`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。 • **standard** を指定する場合は、その後に、標準アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。 • **extended** を指定する場合は、その後に、拡張アクセス リスト構文を使用して **permit** ステートメントまたは **deny** ステートメントを指定します。
ステップ 5	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Router(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.255`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンド構文については、**permit**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **permit** コマンド構文を使用します。
ステップ 6	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは **permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。

	コマンドまたはアクション	目的
	例： `Router(config-std-nacl)# 110 deny 10.6.6.7 0.0.0.255`	• 上位層プロトコル（ICMP、IGMP、TCP、およびUDP）を許可するその他のコマンド構文については、**deny**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **deny** コマンド構文を使用します。
ステップ 7	必要に応じてステップ 5 とステップ 6 を繰り返し、目的とするシーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 8	**end** 例： `Router(config-std-nacl)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show ip access-lists** *access-list-name* 例： `Router# show ip access-lists xyz123`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストに新しいエントリが含まれることを確認します。

例

次に、**xyz123** アクセス リストを指定した場合の **show ip access-lists** コマンドの出力例を示します。

```
Router# show ip access-lists xyz123
Standard IP access list xyz123
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.5, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

日または週の特定の時間帯でのアクセス リスト エントリの制限

デフォルトで、アクセス リスト ステートメントは適用されたときに実行されます。ただし、時間範囲を定義し、各アクセス リスト ステートメントにおいて名前ごとに時間範囲を参照することで、**permit** ステートメントまたは **deny** ステートメントが有効になる日または週の時間帯を定義できます。IP および Internetwork Packet exchange（IPX）名前付きまたは番号付きの拡張アクセス リストは、時間範囲に対応します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended** *name*
4. [*sequence-number*] **deny** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]]
5. [*sequence-number*] **deny** *protocol source*[*source-wildcard*][*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] **fragments**
6. [*sequence-number*] **permit** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]]
7. アクセス リストの基本となる値を指定するまで、ステップ 4 ～ 6 を適宜組み合わせて繰り返します。
8. **end**
9. **show ip access-list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip access-list extended** *name* 例： `Router(config)# ip access-list extended rstrct4`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **deny** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例：	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非フラグメント パケットと初期フラグメントに適用されます。

	コマンドまたはアクション	目的
	`Router(config-ext-nacl)# deny ip any 172.20.1.1`	
ステップ 5	[*sequence-number*] **deny** *protocol source*[*source-wildcard*][*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] **fragments** 例： `Router(config-ext-nacl)# deny ip any 172.20.1.1 fragments`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非初期フラグメントに適用されます。
ステップ 6	[*sequence-number*] **permit** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例： `Router(config-ext-nacl)# permit tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス 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。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりに、キーワード **any** を使用して、アドレスと 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。
ステップ 7	アクセス リストの基本となる値を指定するまで、ステップ 4 ～ 6 を適宜組み合わせて繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**end** 例： `Router(config-ext-nacl)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**show ip access-list** 例： `Router# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

次の作業

アクセス リストをインターフェイスに適用するか、アクセス リストを受け入れるコマンドから参照します。

（注） IP オプションを含むすべてのパケットを効率的に除去するには、**ip options drop** グローバル コマンドを設定することを推奨します。

IP アクセス リストの精緻化の設定例

例：アクセス リストのエントリの並べ替え

次に、並べ替える前と後のアクセス リストの例を示します。開始値は 1、増分値は 2 です。後続のエントリはユーザ指定の増分値に基づいて並べられています。範囲は 1 ～ 2147483647 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router# show access-list carls
Extended IP access list carls
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any
Router(config)# ip access-list extended carls
Router(config)# ip access-list resequence carls 1 2
Router(config)# end
Router# show access-list carls
Extended IP access list carls
    1 permit ip host 10.3.3.3 host 172.16.5.34
    3 permit icmp any any
    5 permit tcp any host 10.3.3.3
    7 permit ip host 10.4.4.4 any
    9 Dynamic test permit ip any any
    11 permit ip host 172.16.2.2 host 10.3.3.12
    13 permit ip host 10.3.3.3 any log
    15 permit tcp host 10.3.3.3 host 10.1.2.2
    17 permit ip host 10.3.3.3 any
    19 permit ip any any
```

例：シーケンス番号を指定したエントリの追加

次の例では、新しいエントリ（シーケンス番号 15）がアクセス リストに追加されます。

```
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255
Router(config)# ip access-list standard tryon
Router(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

例：シーケンス番号を指定しないエントリの追加

次に、シーケンス番号が指定されていないエントリをアクセス リストの末尾に追加する方法を示します。シーケンス番号のないエントリを追加すると、自動的にシーケンス番号が割り当てられ、アクセス リストの末尾に配置されます。デフォルトの増分値は 10 であるため、エントリには、既存のアクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Router(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Router(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Router(config-std-nacl)# end
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
40 permit 10.4.4.4, wildcard bits 0.0.0.255
```

例：IP アクセス リスト エントリに適用された時間範囲

次の例では、月曜日 ～ 金曜日の 8:00 am ～ 6:00 p.m に延長した、no-http と呼ばれる時間範囲を作成します。この時間帯は **deny** ステートメントに適用されるため、月曜日 ～ 金曜日の 8:00 am ～ 6:00 p.m の HTTP トラフィックが拒否されます。

udp-yes と呼ばれる時間範囲は、正午から 8:00 p.m までの週末を定義します。この時間範囲は **permit** ステートメントに適用されるため、土曜日 ～ 日曜日の正午から 8:00 p.m の UDP トラフィックのみが許可されます。両方のステートメントを含むアクセス リストは、ファストイーサネット インターフェイス 0/0/0 のインバウンド パケットに適用されます。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 20:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface fastethernet 0/0/0
 ip access-group strict in
```

例：IP パケット フラグメントのフィルタリング

次のアクセス リストでは、最初のステートメントはホスト 172.16.1.1 を宛先とする非初期フラグメントのみを拒否します。2 番目のステートメントは、ホスト 172.16.1.1 の TCP ポート 80 を宛先とする残りの非フラグメントと初期フラグメントのみを許可します。3 番目のステートメントは、その他のすべてのトラフィックを拒否します。すべての TCP ポートで非初期フラグメントをブロックするため、ホスト 172.16.1.1 のポート 80 をはじめとするすべての TCP ポートで非初期フラグメントをブロックする必要があります。つまり、非初期フラグメントにはレイヤ 4 ポート情報は含まれないため、指定のポートで該当するトラフィックをブロックするには、すべてのポートのフラグメントをブロックする必要があります。

```
access-list 101 deny ip any host 172.16.1.1 fragments
access-list 101 permit tcp any host 172.16.1.1 eq 80
access-list 101 deny ip any any
```

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
time-range コマンドを使用した時間範囲の指定	『*Cisco IOS XE Network Management Configuration Guide*』の「*Performing Basic System Management*」章
ネットワーク管理コマンドの説明	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	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

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

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 リストの精緻化に関する機能情報

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 *1 : IP* アクセス リストの精緻化に関する機能情報

機能名	リリース	機能の設定情報
時刻ベースのアクセス リスト	Cisco IOS XE リリース 2.1	この機能は、Cisco ASR 1000 シリーズのアグリゲーション サービス ルータで導入されました。 この機能について導入または変更されたコマンドはありません。

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。