注釈付きの IP アクセス リスト エントリ

注釈付きの IP アクセス リスト エントリ機能により、**deny** または**permit** 条件に関するコメントや注釈を IP アクセス リストに含めることができます。これらの注釈は、ネットワーク管理者がアクセス リストを理解するのを容易にします。各注釈の長さは 100 文字に制限されます。

このモジュールは、注釈付きの IP アクセス リスト エントリ機能に関する情報を提供します。

../トピック/注釈付きIPアクセスリストエントリに関する情報

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 リストの注釈

任意の IP アクセス リストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** ステートメントや **deny** ステートメントの前にある場合と後にある場合とが混在すると、ユーザーが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

注釈付き IP アクセス リスト エントリの設定方法

名前付きまたは番号付きアクセス リストへの注釈の書き込み

名前付きまたは番号付きアクセス リスト設定を使用できます。作業する設定用にアクセス リストを作成したら、アクセスリストをインターフェイスまたは端末回線に適用する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list** {**standard** | **extended**} {*name* | *number*}
4. **remark** *remark*
5. **deny** *protocol* **host** *host-address* **any eq** *port*
6. **end**

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： `Device> 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： `Device# 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** {**standard**	**extended**} {*name*	*number*} 例： `Device(config)# ip access-list extended telnetting`	名前または番号でアクセス リストを特定し、拡張名前付きアクセス リスト 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	**remark** *remark* 例： `Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out`	名前付き IP アクセス リストのエントリに注釈を追加します。 • 注釈は、**permit** または **deny** ステートメントの目的を示します。
ステップ 5	**deny** *protocol* **host** *host-address* **any eq** *port* 例：	パケットを拒否する名前付き IP アクセス リストの条件を設定します。

	コマンドまたはアクション	目的
	`Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet`	
ステップ 6	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

注釈付き IP アクセス リスト エントリの設定例

例：IP アクセス リストの備考の書き込み

```
Device# configure terminal
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out
Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet
Device(config-ext-nacl)# end
```

注釈付き IP アクセス リスト エントリの追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

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

注釈付き IP アクセス リスト エントリに関する機能情報

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*: 注釈付き *IP* アクセス リスト エントリに関する機能情報

機能名	リリース	機能情報
注釈付きの IP アクセス リスト エントリ		注釈付きの IP アクセス リスト エントリ機能により、[deny] または [permit] 条件に関するコメントや備考をどの IP アクセスリストにも含めることができます。これらの注釈は、ネットワーク管理者がアクセス リストを理解するのを容易にします。各注釈の長さは 100 文字に制限されます。 次のコマンドが導入または変更されました。 **remark**

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。