IP アクセス リスト エントリ シーケンス番号

IP アクセス リスト エントリ シーケンス番号機能により、**permit** または **deny** ステートメントにシーケンス番号を適用したり、名前付き IP アクセス リストでそのようなステートメントを順序変更、追加、削除することができます。IP アクセス リスト エントリ シーケンス番号機能を使用すると、IP アクセス リストを非常に簡単に変更することができます。この機能以前は、アクセス リストの末尾にしかアクセス リスト エントリを追加できませんでした。そのため、名前付き IP アクセス リストの末尾以外のどこかにステートメントを追加する必要がある場合、アクセス リスト全体の再設定が必要でした。

IP アクセス リストのエントリ シーケンス番号に関する制約事項

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。
- また、名前付きアクセス リストよりも古くから存在する、旧式のスタイルで番号付けされたアクセス リストもサポートしていません。アクセス リストは番号で指定できるため、標準または拡張名前付きアクセス リスト（NACL）コンフィギュレーション モードでは番号を入力することができます。

IPアクセス リストのエントリ シーケンス番号に関する情報

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
- ダイヤルオンデマンド ルーティング（DDR）呼び出しのトリガー

IP アクセス リストの機能

アクセス リストは、permit ステートメントと deny ステートメントで構成される順次リストです。これらのステートメントは、IP アドレス、場合によっては上位層 IP プロトコルに適用されます。アクセス リストには、参照に使用される名前があります。多くのソフトウェア コマンドは、構文の一部としてアクセス リストを受け取ります。

アクセス リストを設定して名前を付けることは可能ですが、アクセス リストを受け取るコマンドによってアクセス リストが参照されるまで、有効にはなりません。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。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 リストのプロセスとルール

- アクセス リストの条件に対してフィルタリングされる各パケットの送信元アドレスや宛先アドレス、またはプロトコルがテストされます。一度に 1 つの条件（**permit** ステートメントまたは **deny** ステートメント）がテストされます。

- 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。
- アクセスリストでアドレスまたはプロトコルが拒否されると、パケットは廃棄され、インターネット制御メッセージプロトコル（ICMP）ホスト到達不能メッセージが返されます。
- 一致する条件がない場合は、パケットはドロップされます。これは、各アクセスリストは暗黙の **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。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。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。
- コマンドでアクセス 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。
- 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。
- インバウンドアクセスリストは、デバイスに到達するパケットを処理します。着信パケットの処理後に、アウトバウンドインターフェイスへのルーティングが行われます。インバウンドアクセスリストが効率的なのは、フィルタリングテストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンド リストの場合、**permit** とは、インバウンド インターフェイスでパケットの受信後に処理が続行されることを示します。**deny** とは、パケットが廃棄されることを示します。
- 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 リストの場合、**permit** とは、出力バッファに対して送信されることを示し、**deny** とは、パケットが廃棄されることを示します。

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。
- 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。

- 新しい ACL ステートメントを追加する前に、パーサーが削除をクリーンアップする時間を確保します。

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します。宛先アドレスを指定して、特定のネットワーキング 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。

ワイルドカード マスクおよび暗黙のワイルドカード 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際、対応する IP アドレス ビットを確認するか無視するかを決定するために、ワイルドカード マスクが使用されます。管理者は、ワイルドカード マスクを慎重に設定することにより、許可または拒否のテストに 1 つまたは複数の IP アドレスを選択できます。

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。
- 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。

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 というデフォルトのワイルドカード 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。

トランスポート層の情報

トランスポート層の情報（パケットが TCP、UDP、Internet Control Message Protocol（ICMP）または Internet Group Management Protocol（IGMP）パケットであるか、などの情報）に基づいてパケットをフィルタできます。

利点：IP アクセス リスト エントリ 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。既存のリストの途中にエントリ（ステートメント）を挿入するには、目的の位置の後ろにあるすべてのエントリを削除する必要がありました。次に、新しいエントリを追加したら、先に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。

IP アクセス リスト エントリ シーケンス番号機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、リスト内のエントリを並べ替えることができます。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エントリが挿入されるようにシーケンス番号を選択できます。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1つ入力すると、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。
- 完全修飾32ビットホストアドレスを含むエントリは、リンクされずにハッシュされます。また、サブネットを定義するエントリは、ACL分類の迅速化のために、シーケンス番号でソートされたリンクリストで維持されます。パケットが標準 ACL と照合されると、送信元アドレスがハッシュされ、ハッシュテーブルと照合されます。一致するものが見つからない場合は、リンクリストで一致する可能性のあるものが検索されます。
- ルート プロセッサ（RP）のエントリとラインカード（LC）のエントリのシーケンス番号を常に同期できるように、分散機能がサポートされています。
- 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その番号からの増分に戻されます。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。

- IP アクセス リスト エントリ シーケンス番号機能では、名前付き標準アクセス リストと拡張 IP アクセス リストが使用されます。アクセス リストの名前を番号として指定できるため、番号も使用できます。

IP アクセス リストでのシーケンス番号の使用法

アクセス リスト エントリの順序付けとアクセス リストの変更

ここでは、名前付き IP アクセス リストのエントリにシーケンス番号を割り当てる方法と、アクセス リストに対するエントリの追加または削除を行う方法を説明します。この作業を実行する場合は、次の点に注意してください。

- アクセス リスト エントリの並べ替えは任意です。この作業での並べ替えのステップは、機能の目的の 1 つであり、またその機能の説明が必要と思われることから、必要に応じて説明します。
- 次の手順で、**permit** コマンドはステップ 5 に、**deny** コマンドはステップ 6 に記載されています。ただし、その順番を入れ替えることもできます。設定のニーズに合わせた順番を使用します。

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. 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**]
8. 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**]

9. 必要に応じてシーケンス番号ステートメントを追加するには、ステップ 5 とステップ 6 を繰り返します。
10. **end**
11. **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： `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 resequence** *access-list-name starting-sequence-number increment* 例： `Device(config)# ip access-list resequence kmd1 100 15`	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。
ステップ 4	**ip access-list** {**standard**| **extended**} *access-list-name* 例： `Device(config)# ip access-list standard kmd1`	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* [	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

	コマンドまたはアクション	目的
	precedence *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-std-nacl)# 105 permit 10.5.5.5 0.0.0 255`	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。 • 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 Device(config-ext-nacl) となり、拡張 **permit** コマンドシンタックスを使用します。
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**] 例： `Device(config-std-nacl)# 105 deny 10.6.6.7 0.0.0 255`	（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。 • 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 Device(config-ext-nacl) となり、拡張 **deny** コマンドシンタックスを使用します。
ステップ7	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： `Device(config-ext-nacl)# 150 permit tcp any any log`	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シンタックスについては、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。
ステップ8	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* [	（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

	コマンドまたはアクション	目的
	precedence *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# 150 deny tcp any any log`	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シンタックスについては、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。
ステップ 9	必要に応じてシーケンス番号ステートメントを追加するには、ステップ 5 とステップ 6 を繰り返します。	アクセス リストは変更できます。
ステップ 10	**end** 例： `Device(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 11	**show ip access-lists** *access-list-name* 例： `Device# show ip access-lists kmd1`	（任意）IP アクセス リストの内容を表示します。

例

アクセス リストに新しいエントリが含まれていることを確認するには、**show ip access-lists** コマンドの出力を確認します。

```
Device# show ip access-lists kmd1

Standard IP access list kmd1
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.0, 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
```

IP アクセス リスト エントリ シーケンス番号の設定例

例：アクセス リストのエントリの並べ替え

次に、アクセス リストを並べ替える例を示します。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。

```
Device# show access-list 150

Extended IP access list 150
    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

Device(config)# ip access-list extended 150
Device(config)# ip access-list resequence 150 1 2
Device(config)# exit

Device# show access-list 150

Extended IP access list 150
    1 permit ip host 10.3.3.3 host 172.16.5.34
    3 permit icmp any any
    10 permit tcp any any eq 22 log
    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：シーケンス番号を持つエントリの追加

次に、指定のアクセス リストに新しいエントリを追加する例を示します。

```
Device# 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
```

```
Device(config)# ip access-list standard tryon
Device(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Device(config-std-nacl)# exit
Device(config)# exit
Device# 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：シーケンス番号のないエントリ

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。

```
Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Device(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Device(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255

Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Device(config-std-nacl)# end
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.0.0.0, wildcard bits 0.0.0.255
```

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』

関連項目	マニュアル タイトル
セキュリティ コマンド：コマンド構文の詳細、コマンド モード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Security Command Reference*』
セキュア シェル	セキュア シェルおよびセキュア シェル バージョン 2 サポート設定の機能モジュール。
認証と認可の設定	認証設定、認可設定、およびアカウンティング設定の機能モジュール。

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 ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、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 エントリ シーケンス番号に関する機能情報

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 エントリ シーケンス番号に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト エントリ シーケンス番号		**permit** または **deny** ステートメントにシーケンス番号を適用し、名前付き IP アクセス リストで、該当するステートメントの再整理、追加、または削除を行うことができます。この機能により、IP アクセス リストを簡単に変更できるようになります。この機能が実装される前は、アクセス リストの最後にエントリを追加することしかできませんでした。そのため、末尾以外の任意の場所にステートメントを追加する必要があるときは、アクセス リスト全体を再設定する必要がありました。 では、Cisco Catalyst 3850 シリーズ スイッチのサポートが追加されました。 次のコマンドが導入または変更されました。**deny (IP)**、**ip access-list resequence deny (IP), permit (IP)**

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。