NETCONF および RESTCONF のサービスレベル ACL

このモジュールでは、NETCONF および RESTCONF でサポートされるサービスレベル ACL とその設定方法について説明します。

NETCONF および RESTCONF のサービスレベル ACL に関する情報

NETCONF/RESTCONF のサービスレベル ACL の概要

NETCONF および RESTCONF セッションの IPv4 または IPv6 アクセス制御リスト（ACL）を設定できます。設定された ACL に準拠していないクライアントは、NETCONF または RESTCONF サブシステムへのアクセスを許可されません。サービスレベルの ACL が設定されている場合、NETCONF-YANG および RESTCONF 接続要求は送信元 IP アドレスに基づいてフィルタリングされます。

サービスレベルの ACL が設定されていない場合、すべての NETCONF-YANG および RESTCONF 接続要求がサブシステムに許可されます。

（注） 名前付き ACL のみがサポートされます。番号付き ACL はサポートされません。

NETCONF および RESTCONF のサービスレベル ACL の設定方法

NETCONF-YANG セッションの ACL の設定

NETCONF-YANG セッションの IP アクセスリストまたは IPv6 アクセスリストを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. • **ip access-list** {**standard** | **extended**} *access-list-name*
   • **ipv6 access-list** *access-list-name*
4. **permit** {*host-address* | *host-name* | **any**} [*wildcard*]
5. **deny** {*host-address* | *host-name* | **any**} [*wildcard*]
6. **exit**
7. **netconf-yang ssh** {{**ipv4** | **ipv6** }**access-list name** *access-list-name*} | **port** *port-number*}
8. **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**} *access-list-name*
		• **ipv6 access-list** *access-list-name*
		例：
		`Device(config)# ip access-list standard acl1_permit`
		`Device(config)# ipv6 access-list ipv6-acl1_permit`
			標準の IP アクセスリストを指定して、標準のアクセス リスト コンフィギュレーション モードを開始します。
			IPv6 アクセスリストを指定して、IPv6 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	**permit** {*host-address*	*host-name*	**any**} [*wildcard*] 例： `Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255`	パケットを許可する IP/IPv6 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
ステップ 5	**deny** {*host-address* | *host-name* | **any**} [*wildcard*] 例： `Device(config-std-nacl)# deny any`	パケットを拒否する IP/IPv6 アクセスリストの条件を設定します。
ステップ 6	**exit** 例： `Device(config-std-nacl)# exit`	標準の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、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**netconf-yang ssh** {{**ipv4** | **ipv6** }**access-list name** *access-list-name*} | **port** *port-number*} 例： `Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit`	NETCONF-YANG セッションの ACL を設定します。
ステップ 8	**end** 例： `Device(config)# end`	グローバル 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。

RESTCONF セッションの ACL の設定

RESTCONF セッションの IP アクセスリストまたは IPv6 アクセスリストを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. • **ip access-list** {**standard** | **extended**} *access-list-name*
   • **ipv6 access-list** *access-list-name*
4. **permit** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*}**any**
5. **deny** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*}**any any**
6. **exit**
7. **restconf** {**ipv4** | **ipv6** }**access-list name** *access-list-name*
8. **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）。

	コマンドまたはアクション	目的
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**} *access-list-name*
	• **ipv6 access-list** *access-list-name*
	例：
	`Device(config)# ip access-list standard acl1_permit`
	`Device(config)# ipv6 access-list ipv6-acl1_permit`
		標準の IP アクセスリストを指定して、標準のアクセス リスト コンフィギュレーション モードを開始します。
		IPv6 アクセスリストを指定して、標準の IPv6 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	**permit** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*}**any** 例： `Device(config-ipv6-acl)# permit ipv6 2001:db8::1/32 any`	パケットを許可する IPv6 アクセスリストの条件を設定します。
ステップ 5	**deny** {*protocol-number* | *ipv6-source-address* | *ipv6-source-prefix* | *protocol*}**any any** 例： `Device(config-ipv6-acl)# deny ipv6 any any`	パケットを拒否する IPv6 アクセスリストの条件を設定します。
ステップ 6	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**restconf** {**ipv4** | **ipv6** }**access-list name** *access-list-name* 例： `Device(config)# restconf ipv6 access-list name ipv6-acl1_permit`	RESTCONF セッションの ACL を設定します。
ステップ 8	**end** 例： `Device(config)# end`	グローバル 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。

NETCONF および RESTCONF のサービスレベル ACL の設定例

例：NETCONF セッションの ACL の設定

```
Device# enable
Device# configure terminal
Device(config)# ip access-list standard acl1_permit
Device(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Device(config-std-nacl)# deny any
Device(config-std-nacl)# exit
Device(config)# netconf-yang ssh ipv4 access-list name acl1_permit
Device(config)# end
```

例：RESTCONF セッションの ACL の設定

```
Device# enable
Device# configure terminal
Device(config)# ipv6 access-list ipv6-acl1_permit
Device(config-ipv6-acl)# permit ipv6 2001:db8::1/32 any
Device(config-ipv6-acl)# deny ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# restconf ipv6 access-list name ipv6-acl1_permit
Device(config)# end
```

NETCONF および RESTCONF のサービスレベル ACL に関するその他の資料

関連資料

関連項目	マニュアル タイトル
NETCONF-YANG	NETCONF プロトコル
RESTCONF	RESTCONF プロトコル
プログラマビリティ コマンド	プログラマビリティ コマンド リファレンス

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

NETCONF および RESTCONF のサービスレベル ACL の機能情報

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 : NETCONF* および *RESTCONF* のサービスレベル *ACL* の機能情報

機能名	リリース	機能情報
NETCONF および RESTCONF のサービスレベル ACL	Cisco IOS XE Everest 16.11.1	NETCONF および RESTCONF セッションのアクセス制御リスト（ACL）を設定できます。設定された ACL に準拠していないクライアントは、NETCONF または RESTCONF サブシステムへのアクセスを許可されません。 次のコマンドが導入または変更されました：**netconf-yang ssh access-list**および**restconf access-list** • Cisco ASR 900 シリーズ アグリゲーション サービス ルータ • Cisco ASR 920 シリーズ アグリゲーション サービス ルータ（RSP2） • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 シリーズ スイッチ • Cisco Catalyst 9200 シリーズ スイッチ • Cisco Catalyst 9300 シリーズ スイッチ • Cisco Catalyst 9400 シリーズ スイッチ • Cisco Catalyst 9500 シリーズ スイッチ • Cisco Catalyst IE 3200、3300、3400 高耐久性シリーズ • Cisco エンベデッド サービス 3300 シリーズ スイッチ • Cisco IR1101 耐環境性能 サービス統合型ルータ • Cisco Network Convergence System 4200 シリーズ • Cisco Network Convergence System 520 シリーズ

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。