



モデルベースの AAA

NETCONF インターフェイスと RESTCONF インターフェイスは、NETCONF アクセス制御モデル (NACM) を実装しています。NACM は、RFC 6536 で規定されたロールベース アクセスコントロール (RBAC) の形式の 1 つです。

- [モデルベースの AAA \(1 ページ\)](#)
- [モデルベースの AAA に関するその他の参考資料 \(7 ページ\)](#)
- [モデルベースの AAA に関する機能情報 \(8 ページ\)](#)

モデルベースの AAA

モデルベースの AAA の前提条件

モデルベースの AAA 機能を使用するには、次の内容について事前に理解しておく必要があります。

- NETCONF-YANG
- NETCONF-YANG kill セッション
- RFC 6536 : ネットワーク設定プロトコル (NETCONF) アクセス制御モデル

初期操作

NETCONF サービスや RESTCONF サービスが有効になると、/nacm サブツリーが事前に設定されていないデバイスは、特権レベル 15 のユーザ以外のすべての操作とデータへの読み取り/書き込み/実行アクセスを拒否します。これについては、/nacm サブツリーの次の設定に記述されています。

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <enable-nacm>true</enable-nacm>
  <read-default>deny</read-default>
  <write-default>deny</write-default>
  <exec-default>deny</exec-default>
  <enable-external-groups>true</enable-external-groups>
  <rule-list>
```

```

<name>admin</name>
<group>PRIV15</group>
<rule>
  <name>permit-all</name>
  <module-name>*</module-name>
  <access-operations>*</access-operations>
  <action>permit</action>
</rule>
</rule-list>
</nacm>

```

グループメンバーシップ

ユーザのグループメンバーシップは2つのソースから取得できます。1つ目は、認証に使用するAAAサーバで設定されているユーザの権限レベルです。2つ目は、/nacm/groupsサブツリーで設定されている権限レベルです。各権限レベルに対応するグループの名前は次のとおりです。

権限レベル	NACM グループ名
0	PRIV00
1	PRIV01
2	PRIV02
3	PRIV03
4	PRIV04
5	PRIV05
6	PRIV06
7	PRIV07
8	PRIV08
9	PRIV09
10	PRIV10
11	PRIV11
12	PRIV12
13	PRIV13
14	PRIV14
15	PRIV15



- (注) 従来の IOS コマンド許可 (権限レベルに基づくものなど) は、NETCONF または RESTCONF には適用されません。



- (注) 権限レベルに基づいて NACM グループに付与されたアクセスは、権限レベルが高い NACM グループには本来適用されません。たとえば、PRIV10 に適用されるルールは、PRIV11、PRIV12、PRIV13、PRIV14、および PRIV15 にも自動的に適用されるわけではありません。

NACM 権限レベルの依存関係

AAA 設定が **no aaa new-model** で設定されている場合は、ユーザに対してローカルに設定された権限レベルが使用されます。AAA 設定が **aaa new-model** で設定されている場合、権限レベルは、メソッドリスト **aaa authorization exec default** に関連付けられている AAA サーバによって決まります。

NACM の設定の管理と保守

NACM 設定は、NETCONF または RESTCONF を使用して変更できます。ユーザが NACM 設定にアクセスできるようにするには、そのための明示的な権限を持たせる必要があります。つまり、NACM ルールを使用します。/nacm サブツリーの下の設定は、**copy running-config startup-config EXEC** コマンドが発行される時、または **cisco-ia:save-config RPC** が発行される時は持続します。

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">  
  <save-config xmlns="http://cisco.com/yang/cisco-ia"/>  
</rpc>
```



- (注) NETCONF セッションに適用される NACM ルールは、セッションの確立時に /nacm サブツリーで設定されているものです。/nacm サブツリーに変更を加えても、NETCONF セッションはすでに確立されているため影響を受けません。<kill-session> RPC または **clear netconf-yang session EXEC** コマンドを使用して、不要な NETCONF セッションを強制的に終了することができます。[NETCONF Kill セッション](#)を参照してください。



- (注) 特定のデータへのアクセスを拒否するルールを作成する場合は、同じデータが複数の YANG モジュールとデータ ノードのパスを介して公開される可能性があるため、注意が必要です。たとえば、インターフェイス コンフィギュレーションは **Cisco-IOS-XE-native** と **ietf-interface** の両方を介して公開されます。同じ元データの 1 つの表現に適用される可能性があるルールは、そのデータの他の表現には適用されない場合があります。

NACM 設定のリセット

/nacm サブツリーの設定を初期設定にリセットするには、次のコマンドを使用します（「[初期操作](#)」を参照）。

```
Router#request platform software yang-management nacm reset-config
```

NACM の設定例



(注) ここで挙げている例は説明のみを目的とするものです。

次に、グループ設定の例を示します。

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <groups>
    <group>
      <name>administrators</name>
      <user-name>admin</user-name>
      <user-name>root</user-name>
    </group>

    <group>
      <name>limited-permission</name>
      <user-name>alice</user-name>
      <user-name>bob</user-name>
    </group>
  </groups>
</nacm>
```

表 1: グループ設定の設定パラメータの説明

パラメータ	説明
<name>administrators</name>	グループ名
<user-name>admin</user-name>	ユーザ名
<user-name>root</user-name>	ユーザ名

次に、モジュールルールを作成する例を示します。

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>only-ietf-interfaces</name>
    <group>limited-permission</group>
    <rule>
      <name>deny-native</name>
      <module-name>Cisco-IOS-XE-native</module-name>
      <access-operations>*</access-operations>
      <action>deny</action>
    </rule>
    <rule>
      <name>allow-ietf-interfaces</name>
      <module-name>ietf-interfaces</module-name>
```

```

        <access-operations>*/</access-operations>
        <action>permit</action>
    </rule>
</rule-list>
</nacm>

```

表 2: モジュールルールを作成するための設定パラメータの説明

パラメータ	説明
<name>only-ietf-interfaces</name>	固有のルールリスト名
< group > permission </group >	ルールリストが適用されるグループ
<name>deny-native</name>	固有のルール名
<module-name>Cisco-IOS-XE-native</module-name>	YANG モジュールの名前
<access-operations>*/</access-operations>	CRUDx の動作タイプ
<action>deny</action>	許可/拒否

次に、プロトコル操作ルールを作成する例を示します。

```

<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>only-get</name>
    <group>limited-permission</group>

    <rule>
      <name>deny-edit-config</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>edit-config</rpc-name>
      <access-operations>exec</access-operations>
      <action>deny</action>
    </rule>
    <rule>
      <name>allow-get</name>
      <module-name>ietf-netconf</module-name>
      <rpc-name>get</rpc-name>
      <access-operations>exec</access-operations>
      <action>permit</action>
    </rule>
  </rule-list>
</nacm>

```

表 3: プロトコル操作ルールを作成するための設定パラメータの説明

パラメータ	説明
<name>only-get</name>	固有のルールリスト名
< group > permission </group >	ルールリストが適用されるグループ
<name>deny-edit-config</name>	固有のルール名

パラメータ	説明
<code><module-name>ietf-netconf</module-name></code>	RPC を含むモジュールの名前
<code><rpc-name>edit-config</rpc-name></code>	RPC の名前
<code><access-operations>exec</access-operations></code>	RPC の実行権限
<code><action>deny</action></code>	許可/拒否

次に、データ ノード ルールを作成する例を示します。

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>hide-enable-passwords</name>
    <group>limited-permission</group>

    <rule>
      <name>deny-enable-passwords</name>
      <path xmlns:ios="http://cisco.com/ns/yang/Cisco-IOS-XE-native">/ios:native/enable

      </path>
      <access-operations>*</access-operations>
      <action>deny</action>
    </rule>
  </rule-list>
</nacm>
```

表 4: データ ノード ルールを作成するための設定パラメータの説明

パラメータ	説明
<code><name>hide-enable-passwords</name></code>	固有のルールリスト名
<code>< group > permission </group ></code>	ルールリストが適用されるグループ
<code><name>deny-enable-passwords</name></code>	固有のルール名
<code><path xmlns:ios="http://cisco.com/ns/yang/Cisco-IOS-XE-native">/ios:native/enable</path></code>	許可または拒否されるデータ ノードへのパス
<code><access-operations>*</access-operations></code>	CRUDx の動作タイプ
<code><action>deny</action></code>	許可/拒否

次に、すべてのグループに対して、標準の NETCONF RPC `<get>` および `<get-config>` の使用、スキーマダウンロード RPC `<get-schema>`、およびモジュール **ietf-interfaces** にあるデータへの読み取り専用アクセスを許可する NACM 設定の例を示します。

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
  <rule-list>
    <name>readonly-protocol</name>
    <group>*</group>
    <rule>
      <name>get-permit</name>
      <module-name>ietf-netconf</module-name>
```

```

        <rpc-name>get</rpc-name>
        <access-operations>exec</access-operations>
        <action>permit</action>
    </rule>
</rule-list>
<rule-list>
    <rule>
        <name>get-config-permit</name>
        <module-name>ietf-netconf</module-name>
        <rpc-name>get-config</rpc-name>
        <access-operations>exec</access-operations>
        <action>permit</action>
    </rule>
</rule-list>
<rule-list>
    <rule>
        <name>get-schema-permit</name>
        <module-name>ietf-netconf-monitoring</module-name>
        <rpc-name>get-schema</rpc-name>
        <access-operations>exec</access-operations>
        <action>permit</action>
    </rule>
</rule-list>
<rule-list>
    <name>readonly-data</name>
    <group>*</group>
    <rule>
        <name>ietf-interfaces-permit</name>
        <module-name>ietf-interfaces</module-name>
        <access-operations>read</access-operations>
        <action>permit</action>
    </rule>
</rule-list>
</nacm>

```

モデルベースの AAA に関するその他の参考資料

関連資料

関連項目	マニュアルタイトル
IOS-XE、IOS-XR、およびNX-OS プラットフォームのさまざまなリリースの YANG データ モデル	開発者に分かりやすい方法で Cisco YANG モデルにアクセスするには、 GitHub リポジトリ を複製し、 vendor/cisco サブディレクトリに移動します。ここでは、IOS XE、IOS-XR、およびNX-OSプラットフォームのさまざまなリリースのモデルを使用できます。

標準および RFC

標準/RFC	タイトル
RFC 6020	<i>YANG : Network Configuration Protocol (NETCONF)</i> 向けデータ モデリング言語
RFC 6241	ネットワーク設定プロトコル (<i>NETCONF</i>)
RFC 6536	ネットワーク設定プロトコル (<i>NETCONF</i>) アクセス制御モデル

シスコのテクニカル サポート

説明	リンク
<p>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。</p> <p>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。</p> <p>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。</p>	<p>http://www.cisco.com/support</p>

モデルベースの AAA 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、特に断りが無い限り、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 5: プログラマビリティの機能情報 : データ モデル

機能名	リリース	機能情報
モデルベースの AAA	Cisco IOS XE Fuji 16.8.1	<p>この機能は、次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • 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 • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco CSR 1000v スイッチ • Cisco ISR 1100 シリーズ サービス 統合型 ルータ • Cisco ISR 4000 シリーズ サービス 統合型 ルータ • Cisco NCS 4200 シリーズ
	Cisco IOS XE Fuji 16.8.1a	<p>この機能は、次のプラットフォームに実装されていました。</p> <ul style="list-style-type: none"> • Cisco Catalyst 3650 シリーズ スイッチ • Cisco Catalyst 3850 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

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。