

# Catalyst 9000シリーズスイッチでのSNMPv2c/v3の設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[SNMPの前提条件](#)

[ネットワーク図](#)

[SNMPv2c](#)

[SNMPv3](#)

[認証なし権限なし](#)

[認証の優先順位](#)

[認証SHA](#)

[auth-MD5 \(オプション\)](#)

[認証レベル](#)

[auth-SHA + priv-DES \(認証SHAと認証DES\)](#)

[auth-SHA + priv-AES \(認証SHAと事前認証AES\)](#)

[auth-MD5 + priv-DES \(認証\)](#)

[auth-MD5 + priv-AES \(オプション\)](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Catalyst 9000スイッチでのSNMPv2cおよびSNMPv3の基本設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- SNMPプロトコル(Simple Network Management Protocol)。
- Catalyst 9000シリーズスイッチに精通していること。
- SNMPオブジェクト識別子(OID)に精通していること。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C9200
- C9300
- C9400
- C9500
- C9600
- Cisco IOS® XE & 17.Xソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## SNMPの前提条件

SNMPv1とSNMPv2Cはどちらも、コミュニティベースの形式のセキュリティを使用します。エージェントのMIBにアクセスできるマネージャのコミュニティは、IPアドレスアクセスコントロールリスト(ACL)とパスワードによって定義されます。

SNMPv2Cには、バルク取得機能と、管理ステーションに対するより詳細なエラーメッセージの報告が含まれています。バルク検索機能は、テーブルと大量の情報を取得し、必要なラウンドトリップ数を最小限に抑えます。SNMPv2Cの改善されたエラー処理には、さまざまな種類のエラー状態を区別する拡張エラーコードが含まれています。これらの状態はSNMPv1の1つのエラーコードで報告されます。SNMPv2Cのエラーリターンコードは、エラータイプを報告します。

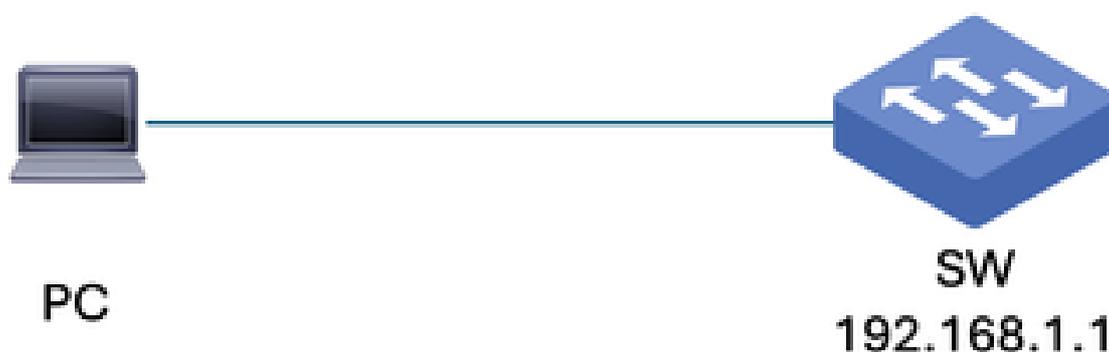
SNMPv3では、セキュリティモデルとセキュリティレベルの両方が提供されています。セキュリティモデルは、ユーザとそのユーザが属するグループに対して設定される認証戦略です。セキュリティレベルとは、セキュリティモデル内で許可されるセキュリティのレベルです。セキュリティレベルとセキュリティモデルの組み合わせによって、SNMPパケットの処理に使用されるセキュリティ方式が決まります。使用可能なセキュリティモデルは、SNMPv1、SNMPv2C、およびSNMPv3です。

次の表に、特性を示し、セキュリティモデルとセキュリティレベルのさまざまな組み合わせを比較します。

モデル	レベル	認証	暗号化	結果
SNMPv1	認証なし 権限なし	コミュニティストリング	いいえ	コミュニティストリングの照合を使用して認証します。
SNMPv2C	認証なし 権限なし	コミュニティストリング	いいえ	コミュニティストリングの照合を使用して認証します。
SNMPv3	認証なし 権限	ユーザ名	いいえ	ユーザ名の照合を使用して認証します。

モデル	レベル	認証	暗号化	結果
	なし			
SNMPv3	認証の優先順位	Message Digest 5(MD5)またはSecure Hash Algorithm(SHA)	いいえ	HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。
SNMPv3	認証レベル	MD5またはSHA	データ暗号化規格(DES)または高度暗号化規格(AES)	<p>HMAC-MD5 または HMAC-SHA アルゴリズムに基づく認証を提供します。</p> <p>次の暗号化アルゴリズムを使用して、ユーザベースのセキュリティモデル(USM)を指定できます。</p> <ul style="list-style-type: none"> <li>• CBC-DES(DES-56)標準に基づく認証に加えて、DES 56ビット暗号化。</li> <li>• 3DES 168ビット暗号化</li> <li>• AES 128ビット、192ビット、または256ビット暗号化</li> </ul>

## ネットワーク図



SNMPv2c

config

```
Switch(config)#snmp-server community cisco RW  
Switch(config)#snmp-server community cisco RO
```

```
>Read-only access with this community string  
>Read-write access with this community string
```

確認

```
Switch#show snmp community  
Community name: cisco  
Community Index: cisco  
Community SecurityName: cisco  
storage-type: nonvolatile active
```

```
~ % snmpwalk -v2c -c cisco 192.168.1.1 1.3.6.1.2.1.1.3  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111410969) 12 days, 21:28:29.69
```

## SNMPv3

認証なし権限なし

config

```
Switch(config)#snmp-server group noAuthNoPrivGroup v3 noauth  
Switch(config)#snmp-server user testuser1 noAuthNoPrivGroup v3
```

確認

```
Switch#show snmp user  
User name: testuser1  
Engine ID: 800000090300EC1D8B0A7B80  
storage-type: nonvolatile active  
Authentication Protocol: None  
Privacy Protocol: None  
Group-name: noAuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser1 -l noAuthNoPriv 192.168.1.1 1.3.6.1.2.1.1.3  
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111425887) 12 days, 21:30:58.87
```

## 認証の優先順位

### 認証SHA

#### config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser2 AuthNoPrivGroup v3 auth sha Password123
```

#### 確認

```
Switch#show snmp user
User name: testuser2
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111447478) 12 days, 21:34:34.78
```

### auth-MD5 ( オプション )

#### config

```
Switch(config)#snmp-server group AuthNoPrivGroup v3 auth
Switch(config)#snmp-server user testuser3 AuthNoPrivGroup v3 auth md5 Password123
```

#### 確認

```
Switch#show snmp user
User name: testuser3
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: None
Group-name: AuthNoPrivGroup
```

```
~ % snmpwalk -v3 -u testuser3 -l authNoPriv -a MD5 -A Password123 192.168.1.1 1.3.6.1.2.1.1.3
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111455526) 12 days, 21:35:55.26
```

## 認証レベル

auth-SHA + priv-DES ( 認証SHAと認証DES )

config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser4 AuthPrivGroup v3 auth sha Password123 priv des Password123
```

## 確認

```
Switch#show snmp user
User name: testuser4
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser4 -l authPriv -a SHA -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111472744) 12 days, 21:38:47.44
```

auth-SHA + priv-AES ( 認証SHAと事前認証AES )

config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser5 AuthPrivGroup v3 auth sha Password123 priv aes 128 Password123
```

## 確認

```
Switch#show snmp user
User name: testuser5
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser5 -l authPriv -a SHA -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
```

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (111476608) 12 days, 21:39:26.08

## auth-MD5 + priv-DES ( 認証 )

config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser6 AuthPrivGroup v3 auth md5 Password123 priv des Password123
```

### 確認

```
Switch#show snmp user
User name: testuser6
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: DES
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser6 -l authPriv -a MD5 -A Password123 -x DES -X Password123 192.168.1.1 1.3.6
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76726018) 8 days, 21:07:40.18
```

## auth-MD5 + priv-AES ( オプション )

config

```
Switch(config)#snmp-server group AuthPrivGroup v3 priv
Switch(config)#snmp-server user testuser7 AuthPrivGroup v3 auth md5 Password123 priv aes 128 Password123
```

### 確認

```
Switch#show snmp user
User name: testuser7
Engine ID: 800000090300EC1D8B0A7B80
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: AES128
Group-name: AuthPrivGroup
```

```
~ % snmpwalk -v3 -u testuser7 -l authPriv -a MD5 -A Password123 -x AES -X Password123 192.168.1.1 1.3.6
```

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (76738170) 8 days, 21:09:41.70

## 関連情報

- [ネットワーク管理設定ガイド、Cisco IOS XE 17.15.x \( Catalyst 9300スイッチ \)](#)
- [SNMP Object Navigator](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。