IEEE 802.1x-Flexible Authentication

IEEE 802.1x-Flexible Authentication 機能には、ポートに認証方式を割り当て、認証の試行が失敗したときに方式を実行する順序を指定する手段が用意されています。この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。

機能情報の確認

お使いのソフトウェア リリースが、このモジュールで説明されている機能の一部をサポートしていないことがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、「IEEE 802.1x-Flexible Authentication の機能情報」（P.10）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

目次

IEEE 802.1x-Flexible Authentication の前提条件

IEEE 802.1x：ポートベースのネットワーク アクセス コントロール

ポートベースのネットワーク アクセス コントロールの概念とシスコのプラットフォーム上のポートベースのネットワーク アクセス コントロールの設定方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*』を参照してください。

RADIUS および ACL

RADIUS プロトコルの概念と Access Control List（ACL; アクセス コントロール リスト）の作成および適用方法を理解しておく必要があります。詳細については、シスコのプラットフォームのマニュアル、および『*Cisco IOS Security Configuration Guide: Securing User Services*』を参照してください。

スイッチが RADIUS 設定されていて、Cisco Secure Access Control Server（ACS; アクセス コントロール サーバ）に接続されている必要があります。詳細については、『*Configuration Guide for CISCO Secure ACS*』を参照してください。

IEEE 802.1x-Flexible Authentication の制約事項

Cisco IOS Release 12.2(33)SXI では、Web 認証方式から 802.1x または MAB 認証方式にフェールオーバーすることはできません。そのため、認証順を設定するときは、Web 認証の後にその他の認証方式を指定しないでください。

IEEE 802.1x-Flexible Authentication に関する情報

IEEE 802.1x-Flexible Authentication 認証をセットアップするには、次の概念を理解しておく必要があります。

- 「Cisco IOS Auth Manager の概要」（P.2）
- 「認証方式」（P.3）
- 「ホスト モード認証」（P.3）
- 「認証順序と認証の優先順位」（P.3）

Cisco IOS Auth Manager の概要

指定されたネットワークに接続するデバイスの機能は異なっている可能性があるため、ネットワークはさまざまな認証方式および認証ポリシーをサポートする必要があります。Cisco IOS Auth Manager は、認証方法に関係なく、ネットワーク認証要求を処理し、認証ポリシーを強制します。Auth Manager は、すべてのポートベースのネットワーク接続試行、認証、認可、および接続解除に対する運用データを維持することで、セッション マネージャとして機能します。

Auth Manager セッションには、次のような状態が考えられます。

- Idle：idle 状態では、認証セッションは初期化されていますが、実行されている方式はありません。これは中間の状態です。
- Running：現在、方式が実行されています。これは中間の状態です。
- Authc Success：認証方式の実行に成功しました。これは中間の状態です。

- Authc Failed：認証方式が失敗しました。これは中間の状態です。
- Authz Success：このセッションに対するすべての機能の適用に成功しました。これは最終的な状態です。
- Authz Failed：このセッションに対して、少なくとも 1 つの機能の適用に失敗しました。これは最終的な状態です。
- No methods：このセッションに結果を提供する方式がありません。これは最終的な状態です。

認証方式

IEEE 802.1x-Flexible Authentication 機能は、次の 3 つの認証方式をサポートしています。

- **dot1x**：IEEE 802.1x 認証はレイヤ 2 の認証方式です。
- **mab**：MAC 認証バイパスはレイヤ 2 の認証方式です。
- **webauth**：Web 認証はレイヤ 3 の認証方式です。

ホスト モード認証

IEEE 802.1x-Flexible Authentication 機能は、次の 2 つの新しいホスト モードをサポートしています。

- **multi-auth :** マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- **multi-domain**：マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 ついう 2 つの認証を使用できます。

また、IEEE 802.1x-Flexible Authentication 機能は、シングルホスト認証とマルチホスト認証もサポートしています。

認証順序と認証の優先順位

IEEE 802.1x-Flexible Authentication 機能を使用すると、認証順序と認証の優先順位を指定できます。**authentication order** コマンドでは、デフォルトの認証の優先順位を設定します。**authentication priority** コマンドを使用すると、デフォルトの認証の優先順位よりも優先されます。たとえば、MAB、802.1x という認証順序を指定するとします。ただし、認可後に後続の 802.1x ハンドシェークを無視したくない場合があります。このような場合、802.1x 認証方式に MAB 方式よりも高い優先順位を与えます。

IEEE 802.1x-Flexible Authentication の設定方法

ここでは、次の作業について説明します。

- 「認証順序の設定」（P.4）
- 「認証の優先順位の設定」（P.6）

認証順序の設定

認証順序は個々のポートで設定し、各ポートがどの認証方式を使用するかを制御します。ここで説明する手順に従って認証順序を設定してください。

前提条件

IEEE 802.1x-Flexible Authentication 機能を使用するには、スイッチを Cisco Secure ACS に接続し、RADIUS Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウンティング) を Web 認証用に設定しておく必要があります。また、必要に応じて、ACL ダウンロードを有効にします。

認証順序に 802.1x ポート認証方式を含める場合、スイッチで IEEE 802.1x 認証をイネーブルにする必要があります。

認証順序に Web 認証を含める場合、スイッチとインターフェイスで Web 認証を可能にするフォールバック プロファイルを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **dot1x system-auth-control**
4. **interface** *type slot/port*
5. **switchport**
6. **switchport mode access**
7. **switchport access vlan** *vlan-id*
8. **mab** [**eap**]
9. **authentication port-control** {**auto** | **force-authorized** | **fort unauthorized**}
10. **authentication fallback** *profile*
11. **authentication order** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
12. **dot1x pae authenticator**
13. **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：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# 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。

	コマンドまたはアクション	目的
ステップ 3	**dot1x system-auth-control** **例：** `Switch(config)# dot1x system-auth-control`	（任意）スイッチで IEEE 802.1x 認証をグローバルにイネーブルにします。 認証順序に **dot1x** 認証方式を含める場合、IEEE 802.1x 認証をイネーブルにします。
ステップ 4	**interface type** *slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**switchport** **例：** `Switch(config-if)# switchport`	レイヤ 2 スイッチド モードでインターフェイスを配置します。
ステップ 6	**switchport mode access** **例：** `Switch(config-if)# switchport mode access`	非トランキング、非タグ付き、シングル VLAN レイヤ 2 インターフェイスを設定します。
ステップ 7	**switchport access vlan** *vlan-id* **例：** `Switch(config-if)# switchport access vlan 2`	ポートに VLAN を設定します。
ステップ 8	**mab** [**eap**] **例：** `Switch(config-if)# mab`	（任意）MAB をイネーブルにします。 認証順序に **mab** キーワード（ステップ 11）を含める場合、MAB をイネーブルにします。
ステップ 9	**authentication port-control** {**auto** | **force-authorized** | **fort unauthorized**} **例：** `Switch(config-if)# authentication port-control auto`	ポートの認証ステートを設定します。
ステップ 10	**authentication fallback** *profile* **例：** `Switch(config-if)# authentication fallback web-profile`	（任意）Web 認証をイネーブルにします。 認証順序に **webauth** キーワード（ステップ 11）を含める場合、Web 認証をイネーブルにします。
ステップ 11	**authentication order** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **例：** `Switch(config-if)# authentication order mab dot1x webauth`	認証順序を設定します。

	コマンドまたはアクション	目的
ステップ 12	**dot1x pae authenticator** **例：** `Switch(config)# dot1x pae authenticator`	IEEE 802.1x オーセンティケータ向けのメッセージに対して、ポートが応答できるようにします。
ステップ 13	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

トラブルシューティングのヒント

次のコマンドは、Flexible Authentication 機能のトラブルシューティングに役立ちます。

- **debug authentication**
- **show authentication registrations**
- **show authentication sessions**
- **show dot1x**
- **show mab**

認証の優先順位の設定

認証の優先順位は、個々のポートの方式についてフェールオーバー順を制御するために設定します。ここで説明する手順に従って認証の優先順位を設定してください。

前提条件

認証の優先順位を設定するには、「認証順序の設定」（P.4）の説明に従って認証順序を設定しておく必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**}
5. **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：** `Switch> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Switch# 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	**interface** *type slot*/*port* **例：** `Switch(config)# interface FastEthernet2/1`	インターフェイス 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	**authentication priority** {**dot1x** [**mab** | **webauth**] [**webauth**] | **mab** [**dot1x** | **webauth**] [**webauth**] | **webauth**} **例：** `Switch(config-if)# authentication priotiry dot1x mab webauth`	認証の優先順位を設定します。
ステップ 5	**end** **例：** `Switch(config-if)# end`	グローバル コンフィギュレーション モードに戻ります。

IEEE 802.1x-Flexible Authentication の設定例

ここでは、次の設定例について説明します。

「Flexible Authentication：例」（P.7）

Flexible Authentication：例

次の例では、マルチ認証ホスト モードでポートを設定します。認証順序は、802.11x が最初で、次に MAB、最後が Web 認証です。

```
enable
configure terminal
dot1x system-auth-control

aaa new-model
aaa authentication login default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization auth-proxy default group radius
aaa session-id common
ip http server

ip admission name webauth-rule proxy http
fallback profile webauth-profile
 ip access-group webauthlist in
```

```
 ip admission webauth-rule


interface GigabitEthernet2/1
 switchport
 switchport mode access
 switchport access vlan 125
 switchport voice vlan 127
 mab
 authentication port-control auto
 authentication fallback webauth-profile
 authentication host-mode multi-auth
 authentication order dot1x mab webauth
 dot1x pae authenticator
```

その他の参考資料

次の項で、IEEE 802.1.x-Flexible Authentication 機能に関する参考資料を紹介します。

関連資料

内容	参照先
認証コマンド	『*Cisco IOS Security Command Reference*』
Standalone MAB Support	Standalone MAB Support

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
• CISCO-AUTH-FRAMEWORK-MIB • CISCO-MAC-AUTH-BYPASS-MIB • CISCO-PAE-MIB • IEEE8021-PAE-MIB	選択したプラットフォーム、Cisco IOS リリース、および機能セットの 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
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/en/US/support/index.html

IEEE 802.1.x-Flexible Authentication の機能情報

表 1 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS、Catalyst OS、Cisco IOS XE ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 1　IEEE 802.1.x-Flexible Authentication の機能情報

機能名	リリース	機能情報
IEEE 802.1x-Flexible Authentication	12.2(33)SXI	この機能には、ポートに 1 つまたは複数の認証方式を設定し、各認証方式を試行する順序を指定する手段が用意されています。 導入または変更されたコマンド：**authentication fallback**、**authentication host-mode**、**authentication order**、**authentication port-control**、**authentication priority**、**authentication timer restart**、**debug authentication**、**mab**、**show authentication interface**、**show authentication registrations**、**show authentication sessions**、**show mab** 削除または廃止されたコマンド：**dot1x fallback**、**dot1x host-mode**、**dot1x port control**