802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポート

この機能により、IEEE 802.1X、MAB 認証バイパス、または Web 認証を使用した認証の後に、ポリシー適用として Cisco Access Control Server（ACS）からユーザ単位の ACL をダウンロードできます。

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートの前提条件

- AAA 認証をイネーブルにする必要があります。
- **network** キーワードを使用して AAA 許可をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にする必要があります。
- 802.1X 認証をイネーブルにする必要があります。
- RADIUS サーバにユーザプロファイルと VSA を設定する必要があります。

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートの制約事項

- ユーザ単位アクセスコントロールリスト（ACL）がサポートされるのはシングルホストモードだけです。
- この機能は、スイッチポートの標準 ACL をサポートしません。
- 1 ポートがサポートする 802.1X 認証ユーザは 1 ユーザだけです。マルチ ホスト モードがポートでイネーブルの場合、ユーザ単位 ACL 属性は関連ポートでディセーブルです。
- ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートに関する情報

ユーザ単位 ACL を使用した 802.1X 認証

ユーザ単位アクセスコントロールリスト（ACL）を設定して、異なるレベルのネットワークアクセスおよびサービスを 802.1X 認証ユーザに提供できます。RADIUS サーバは、802.1X ポートに接続されるユーザを認証する場合、ユーザ ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザセッションの期間中、その属性を 802.1X ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザ単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

RADIUS は、ベンダー固有属性などのユーザ単位属性をサポートします。ベンダー固有属性（VSA）は、オクテットストリング形式で、認証プロセス中にスイッチに渡されます。ユーザ単位 ACL に使用される VSA は、入力方向では inacl#<n > で、出力方向では outacl#<n > です。MAB ACL は、入力方向に限りサポートされます。スイッチは、入力方向に限り VSA をサポートします。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。詳細については、「ACL によるネットワークセキュリティの設定」モジュールを参照してください。

RADIUS サーバに保存するユーザ単位コンフィギュレーションを定義するには、拡張 ACL 構文形式を使用します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す *.in* または *.out* が含まれています。RADIUS サーバが *.in* または *.out* 構文を許

可しない場合、アクセス リストはデフォルトでアウトバウンド ACL に適用されます。スイッチでの Cisco IOS のアクセス リストに関するサポートが制限されているため、Filter-ID 属性は 1 ～ 199 および 1300 ～ 2699 の IP ACL（IP 標準 ACL および IP 拡張 ACL）に対してだけサポートされます。

1 ポートがサポートする 802.1X 認証ユーザは 1 ユーザだけです。マルチ ホスト モードがポートでイネーブルの場合、ユーザ単位 ACL 属性は関連ポートでディセーブルです。

ユーザ単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザ単位 ACL の最大サイズにより制限されます。

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートの設定方法

ダウンロード可能な ACL の設定

接続されたホストの認証中に RADIUS サーバからのダウンロード可能な ACL またはリダイレクト URL を受け入れるようにデバイスを設定するには、次の作業を行います。

手順

	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 モードをイネーブルにします。 • 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 device tracking** 例： `Device(config)# ip device tracking`	IP デバイス トラッキング テーブルをイネーブルにします。
ステップ 4	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 5	**aaa authorization network default group radius** 例：	許可の方法を設定します。許可の方法を削除するには、**no aaa authorization**

	コマンドまたはアクション	目的
	`Device(config)# aaa authorization network default group radius`	**network default group radius** コマンドを使用します。
ステップ 6	**radius-server vsa send authentication** 例： `Device(config)# radius-server vsa send autentication`	ネットワークアクセスサーバを設定します。
ステップ 7	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/0/1`	設定するポートを指定し、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 8	**ip access-group** *acl-id* **in** 例： `Device(config-if)# ip access-group 99 in`	ポートの入力方向のデフォルト ACL を設定します。 （注） ACL ID はアクセスリストの名前または番号です。
ステップ 9	end	`Device(config-if)# end` 特権 EXEC モードに戻ります。
ステップ 10	**show running-config interface***interface-id* 例： `Device# show running-config interface interface-id`	確認のために特定のインターフェイス コンフィギュレーションを表示します。
ステップ 11	**copy running-config startup-config** 例： `Device# copy running-config startup-config`	（任意）コンフィギュレーション ファイルに設定を保存します。

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートの設定例

例：ダウンロードポリシーのスイッチの設定

次に、ダウンロードポリシーのスイッチを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
```

```
Device(config)# aaa authorization network default local group radius
Device(config)# ip device tracking
Device(config)# ip access-list extended default_acl
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# radius-server vsa send authentication
Device(config)# interface fastEthernet 2/13
Device(config-if)# ip access-group default_acl in
Device(config-if)# end
```

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
この章で使用するコマンドの完全な構文および使用方法の詳細。	Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst 1000 Switches)

標準および RFC

標準/RFC	タイトル
IEEE 802.1X プロトコル	—
RFC 3580	「*IEEE 802.1x Remote Authentication Dial In User Service (RADIUS)*」

MIB

MIB	MIB のリンク
• CISCO–AUTH–FRAMEWORK–MIB • CISCO–MAB–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、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
★枠で囲まれた Technical Assistance の場合★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

802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポートの機能情報

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 : 802.1X/MAB/Webauth* ユーザのユーザ単位での *ACL* サポートの機能情報

機能名	リリース	機能情報
802.1X/MAB/Webauth ユーザのユーザ単位での ACL サポート	Cisco IOS リリース 15.2(7)E1	この機能により、IEEE 802.1X、MAB 認証バイパス、または Web 認証を使用した認証の後に、ポリシー適用として Cisco Access Control Server（ACS）からユーザ単位の ACL をダウンロードできます。