CHAPTER 77

Web ベース認証

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

Web ベース認証の前提条件

なし。

Web ベース認証の制約事項

- Web ベース認証は入力だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランク ポート、EtherChannel メンバ ポート、またはダイナミック トランク ポートではサポートされていません。

- Web ベース認証を設定する前に、インターフェイスでデフォルトの ACL を設定する必要があります。レイヤ 2 インターフェイスのポート ACL を設定するか、レイヤ 3 インターフェイスの Cisco IOS ACL を設定します。
- レイヤ 2 インターフェイス上では、スタティック ARP キャッシュ割り当てのあるホストを認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能で検出されません。
- デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。
- スイッチ上で HTTP サーバを実行するために、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要もあります。HTTP サーバは、ホストに HTTP ログイン ページを送信します。
- STP トポロジの変更によってホスト トラフィックが別のポートに着信する場合、2 ホップ以上離れたホストではトラフィックの中断が発生することがあります。これは、レイヤ 2（STP）トポロジの変更後に ARP および DHCP アップデートが送信されないことがあるためです。
- Web ベース認証は、ダウンロード可能ホスト ポリシーとして VLAN 割り当てをサポートしません。
- Cisco IOS Release 15.1SY では、RADIUS サーバからのダウンロード可能 ACL（DACL）がサポートされます。
- IPv6 トラフィックについては、Web ベース認証はサポートされていません。

Web ベース認証について

Web ベース認証の概要

Web ベース認証機能は、認証、許可、アカウンティング（AAA）システムの一部として機能できる Web ベース認証（Web 認証プロキシとも呼ばれる）を実装します。

Web ベースの認証機能を使用して、IEEE 802.1X サプリカントを実行していないホスト システムでエンドユーザを認証できます。レイヤ 2 およびレイヤ 3 インターフェイスで Web ベース認証機能を設定することができます。

ユーザが HTTP セッションを開始する際に、Web ベースの認証機能がホストからの入力 HTTP パケットを代行受信して、HTML ログイン ページをユーザに送信します。ユーザは資格情報を入力します。Web ベース認証はこの資格情報を認証のために AAA サーバに送信します。認証が成功すると、Web ベース認証がログイン成功 HTML ページをホストに送信し、AAA サーバによって返されたアクセス ポリシーが適用されます。

認証に失敗すると、Web ベース認証がログイン失敗 HTML ページをユーザに送信し、ログイン試行を再試行するようにユーザに要求します。ユーザが失敗ログイン試行の最大数を超過すると、Web ベース認証がログイン期限切れ HTML ページをホストに送信し、ユーザは待機する間ウォッチ リストに配置されます。

デバイスの役割

Web ベースの認証では、図 77-1 に示すように、ネットワーク上の装置にはそれぞれ特定のロールがあります。

図 77-1　Web ベースの認証装置のロール

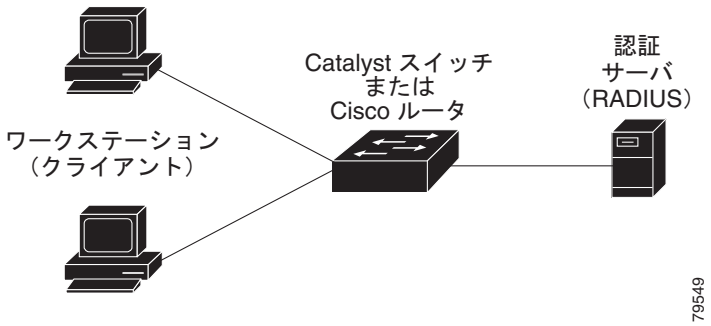

図 77-1 に示す特定の役割は、次のとおりです。

- *クライアント*：LAN およびスイッチ サービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- *認証サーバ*：実際にクライアントの認証を行います。認証サーバはクライアントの識別情報を確認し、そのクライアントに LAN およびスイッチ サービスへのアクセスを許可すべきかどうかをスイッチに通知します。
- *スイッチ*：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス トラッキング テーブルを維持します。

（注） デフォルトでは、スイッチの IP 装置追跡機能はディセーブルにされています。Web ベース認証を使用するには、IP デバイスのトラッキング機能をイネーブルにする必要があります。

レイヤ 3 インターフェイスの場合、インターフェイス上に Web ベース認証が設定されると（またはインターフェイスがサービス中になると）、Web ベース認証が HTTP 代行受信 ACL を設定します。

レイヤ 2 インターフェイスの場合、次のメカニズムを使用して Web ベース認証が IP ホストを検出します。

- ARP ベース トリガー : ARP リダイレクト ACL により、Web ベース認証は固定 IP アドレスまたは動的に取得された IP アドレスを持つホストを検出できます。
- ダイナミック ARP インスペクション
- DHCP スヌーピング : スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをチェックします。

  ホスト IP が例外リストに含まれている場合、例外リスト エントリからのポリシーが適用され、セッションが確立されていると見なされます。

- 認証バイパスをチェックします。

  ホスト IP が例外リストにない場合、Web ベース認証は Nonresponsive Host（NRH; 非応答ホスト）要求をサーバに送信します。

  サーバ応答が Access Accepted である場合、このホスト用の許可がバイパスされます。セッションが確立されていると見なされます。

- HTTP 代行受信 ACL を設定します。

  NRH 要求に対するサーバ応答が Access Rejected である場合、HTTP 代行受信 ACL がアクティブになり、セッションはホストからの HTTP トラフィックを待機します。

認証プロセス

Web ベース認証がイネーブルの場合、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログイン ページを送信します。ユーザがログイン ページにユーザ名とパスワードを入力すると、スイッチは認証サーバにそのエントリを送信します。
- クライアント ID が有効で、認証に成功した場合、スイッチは認証サーバからユーザのアクセス ポリシーをダウンロードしてアクティブにします。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザがログインを再試行し、最大ログイン試行回数を超過すると、スイッチはログイン期限切れページを送信し、ホストがウォッチ リストに配置されます。ウォッチ リストのタイムアウト後、ユーザは認証プロセスを再試行することができます。
- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセス ポリシーを適用します。ログインの成功ページがユーザに送信されます

ホストがレイヤ 2 インターフェイスの ARP プローブに応答しない場合やホストがレイヤ 3 インターフェイスでアイドル タイムアウト中にトラフィックを送信しない場合、スイッチはクライアントを再認証します。

- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。
- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- 終了処理がデフォルトの場合、セッションが停止されて適用されたポリシーが削除されます。

AAA 失敗ポリシー

AAA 失敗ポリシーは、AAA サーバが使用できない場合、ユーザをネットワークに接続するか、または接続を維持するための方式です。クライアントの Web ベース認証が必要なときに AAA サーバにアクセスできない場合、ユーザを拒否する（つまり、ネットワークへのアクセスを提供しない）代わりに、管理者はユーザに適用できるデフォルト AAA 失敗ポリシーを設定できます。

このポリシーは次の理由で便利です。

- AAA が使用不可能である場合、アクセスが制限されることはあっても、ネットワークへの接続は維持できます。
- AAA サーバが再び利用できるようになると、ユーザは再検証を受けることが可能であり、ユーザの通常アクセス ポリシーを AAA サーバからダウンロードできます。

（注） AAA サーバの停止時には、ユーザに既存のポリシーが関連付けられていない場合に限り、AAA 失敗ポリシーが適用されます。通常、ユーザ セッションで再認証が必要なときに AAA サーバが利用不可能な場合は、ユーザに対して現在有効なポリシーが維持されます。

AAA 失敗ポリシーが有効な間は、セッション ステートは AAA ダウンとして維持されます。

認証プロキシ Web ページのカスタマイゼーション

スイッチの内部 HTTP サーバは、Web ベース認証プロセスの間、認証を行うクライアントに送信する 4 つの HTML ページをホストします。この 4 つのページにより、サーバはユーザに次の 4 つの認証プロセスのステートを通知できます。

- ログイン：ユーザのクレデンシャルが要求された
- 成功：ログインに成功
- 失敗：ログインに失敗
- 期限切れ：ログインに何度も失敗したためログイン セッションが期限切れになった

4 つのデフォルト内部 HTML ページの代わりにカスタム HTML ページを使用したり、認証成功後にユーザがリダイレクトされる URL を指定して内部成功ページを効率的に置き換えたりできます。

その他の機能と Web ベース認証の相互作用

- 「ポート セキュリティ」（P.77-6）
- 「ゲートウェイ IP」（P.77-6）

- 「ACL」（P.77-6）
- 「IP ソース ガード」（P.77-6）
- 「EtherChannel」（P.77-6）
- 「スイッチオーバー」（P.77-7）

ポート セキュリティ

Web ベース認証とポート セキュリティは、同じポートに設定できます。（**switchport port-security** インターフェイス コンフィギュレーション コマンドを使用してポートにポート セキュリティを設定します）。ポート セキュリティおよび Web ベース認証をポートでイネーブルにする際に、Web ベース認証がポートを認証し、ポート セキュリティでクライアントのものを含むすべての MAC アドレスのネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

ポート セキュリティをイネーブルにする手順については、「ポート セキュリティの設定方法」（P.78-5）を参照してください。

ゲートウェイ IP

Web ベース認証が VLAN のスイッチ ポートに設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP を設定できません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホスト ポリシーが適用されます。GWIP ホスト ポリシーは、Web ベース認証のホスト ポリシーに優先されます。

ACL

VLAN ACL または Cisco IOS ACL をインターフェイス上に設定する場合、ACL がホスト トラフィックに適用されるのは Web ベース認証ホスト ポリシーが適用されたあとだけです。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの入力トラフィックについて、Port ACL（PACL; ポート ACL）をデフォルトのアクセス ポリシーとして設定する必要があります。認証後、Web ベース認証のホスト ポリシーは、PACL に優先されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN に設定済み VACL キャプチャのあるポート上に Web ベース認証は設定できません。

IP ソース ガード

同じインターフェイスでの IP ソース ガードと Web ベース認証の設定はサポートされていません。

同じインターフェイスで IP ソース ガードと Web ベース認証を設定できます。DHCP スヌーピングがアクセス VLAN でもイネーブルである場合は、2 つの機能間の競合を回避するためにグローバル コンフィギュレーション モードで **platform acl tcam override dynamic dhcp-snooping** コマンドを入力する必要があります。IP ソース ガードと Web ベース認証が組み合わされているときは、その他の VLAN ベース機能はサポートされません。

EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバ チャネルに適用されます。

スイッチオーバー

RPR 冗長モードでは、スイッチオーバー中は現在認証されているホストに関する情報が保持されます。ユーザは再認証する必要がありません。

デフォルトの Web ベース認証の設定

機能	デフォルト設定
AAA	ディセーブル
RADIUS サーバ • IP アドレス • UDP 認証ポート • キー	 • 指定なし • 1812 • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

Web ベース認証の設定方法

Web ベース認証設定時の作業一覧

認証ルールとインターフェイスの設定

Web ベース認証を設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip admission name name proxy http`	Web ベース許可の認証ルールを設定します。
ステップ 2	`Router(config)# interface type slot/port`	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、Web ベース認証をイネーブルにする入力レイヤ 2 またはレイヤ 3 インターフェイスを指定します。
ステップ 3	`Router(config-if)# ip access-group name`	デフォルト ACL を適用します。
ステップ 4	`Router(config-if)# ip admission name`	指定されたインターフェイスに Web ベース認証を設定します。
ステップ 5	`Router(config-if)# authentication order method1 [method2] [method3]`	（任意）使用される認証方式のフォールバック順序を指定します。*method* の 3 つの値のデフォルト順序は、**dot1x**、**mab**、および **webauth** です。 方式を省略すると、インターフェイス上でその方式がディセーブルになります。
ステップ 6	`Router(config-if)# exit`	コンフィギュレーション モードに戻ります。
ステップ 7	`Router(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 8	`Router(config)# end`	特権 EXEC モードに戻ります。

この例では、ポート 5/1 上で 802.1X 認証または MAB 認証をディセーブルにしながら、Web ベースの認証をイネーブルにする方法を示します。

```
Router(config)# ip admission name webauth1 proxy http
Router(config)# interface gigabitethernet 5/1
Router(config-if)# ip admission webauth1
Router(config-if)# authentication order webauth
Router(config-if)# exit
Router(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
```

```
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name webauth1
    http list not specified inactivity-time 60 minutes

Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 認証の設定

Web ベース認証をイネーブルにするには、AAA をイネーブルにして認証方式を指定する必要があります。次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 2	`Router(config)# aaa authentication login default group {tacacs+ | radius}`	ログイン時の認証方法のリストを定義します。
ステップ 3	`Router(config)# aaa authorization auth-proxy default group {tacacs+ | radius}`	Web ベース許可の許可方式リストを作成します。
ステップ 4	`Router(config)# tacacs-server host {hostname | ip_address}`	AAA サーバを指定します。RADIUS サーバの場合は、「スイッチ /RADIUS サーバ通信の設定」（P.77-9）を参照してください。
ステップ 5	`Router(config)# tacacs-server key {key-data}`	スイッチと TACACS サーバとの間で使用される許可および暗号キーを設定します。

次の例では、AAA をイネーブルにする方法を示します。

```
Router(config)# aaa new-model
Router(config)# aaa authentication login default group tacacs+
Router(config)# aaa authorization auth-proxy default group tacacs+
```

スイッチ /RADIUS サーバ通信の設定

RADIUS セキュリティ サーバは、次のいずれかによって識別されます。

- ホスト名
- ホスト IP アドレス
- ホスト名と特定の UDP ポート番号
- IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

RADIUS サーバ パラメータを設定する手順は、次のとおりです。

	コマンド	目的
ステップ 1	`Router(config)# ip radius source-interface interface_name`	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 2	`Router(config)# radius-server host {hostname | ip-address} test username username`	リモート RADIUS サーバのホスト名または IP アドレスを指定します。 **test username** *username* は、RADIUS サーバ接続の自動テストをイネーブルにするオプションです。指定された *username* は有効なユーザ名である必要はありません。 **key** オプションは、スイッチと RADIUS サーバとの間で使用する認証および暗号キーを指定します。 複数の RADIUS サーバを使用する場合は、このコマンドを再入力します。
ステップ 3	`Router(config)# radius-server key string`	スイッチと、RADIUS サーバで動作する RADIUS デーモン間で使用される認証および暗号キーを設定します。
ステップ 4	`Router(config)# radius-server vsa send authentication`	RADIUS サーバからの ACL のダウンロードをイネーブルにします。
ステップ 5	`Router(config)# radius-server dead-criteria tries num-tries`	RADIUS サーバに対する未応答の伝送数を指定します。この数を超えると RADIUS サーバが停止していると見なされます。指定できる *num-tries* の範囲は 1 ～ 100 です。

- 別のコマンドラインには、**key** *string* を指定します。
- **key** *string* には、スイッチと、RADIUS サーバ上で動作する RADIUS デーモンとの間で使用する認証および暗号キーを指定します。キーは、RADIUS サーバで使用する暗号キーに一致するテキスト ストリングでなければなりません。
- **key** *string* を指定する場合、キーの途中および末尾のスペースが利用されます。キーにスペースを使用する場合は、引用符がキーの一部分である場合を除き、引用符でキーを囲まないでください。キーは RADIUS デーモンで使用する暗号に一致している必要があります。
- **radius-server host** グローバル コンフィギュレーション コマンドを使用して、タイムアウト、再送信回数、暗号キーの値を、すべての RADIUS サーバにグローバルに設定できます。これらのオプションをサーバ単位で設定するには、**radius-server timeout**、**radius-server retransmit**、および **radius-server key** グローバル コンフィギュレーション コマンドを使用します。

（注） RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、スイッチの IP アドレス、サーバとスイッチの双方で共有するキー ストリング、およびダウンロード可能 ACL があります。詳細については、RADIUS サーバのマニュアルを参照してください。

次に、スイッチで RADIUS サーバ パラメータを設定する例を示します。

```
Router(config)# ip radius source-interface Vlan80
Router(config)# radius-server host 172.l20.39.46 test username user1
Router(config)# radius-server key rad123
Router(config)# radius-server dead-criteria tries 2
```

HTTP サーバの設定

Web ベース認証を使用するには、スイッチで HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。サーバをイネーブルにするには、グローバル コンフィギュレーション モードで次のいずれかの作業を行います。

コマンド	目的
`Router(config)# ip http server`	HTTP サーバをイネーブルにします。Web ベース認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
`Router(config)# ip http secure-server`	HTTPS をイネーブルにします。

任意でカスタム認証プロキシ Web ページを設定したり、ログイン成功時のリダイレクション URL を指定したりできます。詳細については、次を参照してください。

- 認証プロキシ Web ページのカスタマイズ
- 成功ログインに対するリダイレクション URL の指定

認証プロキシ Web ページのカスタマイズ

Web ベース認証中に、スイッチの内部デフォルト HTML ページの代わりに、ユーザに表示される 4 つの代替 HTML ページを出力するオプションがあります。

カスタム認証プロキシ Web ページを使用するように指定するには、カスタム HTML ファイルをスイッチの内部ディスクまたはフラッシュ メモリに保存してから、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip admission proxy http login page file device:login-filename`	デフォルトのログイン ページの代わりに使用するカスタム HTML ファイルの、スイッチのメモリ ファイル システムの場所を指定します。*device:* はディスクまたはフラッシュ メモリのいずれかです（例：disk0:）。
ステップ 2	`Router(config)# ip admission proxy http success page file device:success-filename`	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルのメモリ ファイル システムの場所を指定します。
ステップ 3	`Router(config)# ip admission proxy http failure page file device:fail-filename`	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 4	`Router(config)# ip admission proxy http login expired page file device:expired-filename`	デフォルトのログイン期限切れページの代わりに使用するカスタム HTML ファイルの場所を指定します。

- カスタム Web ページ機能をイネーブルにするには、4 つのすべてのカスタム HTML ファイルを指定する必要があります。4 つ未満のファイルが指定されている場合は、内部デフォルト HTML ページが使用されます。
- この 4 つのカスタム HTML ファイルはスイッチのディスクまたはフラッシュに存在している必要があります。
- イメージ ファイルのサイズには 256 KB の制限があります。
- すべてのイメージ ファイルに、「web_auth_」で始まるファイル名を付ける必要があります（例：「logo.jpg」ではなく、「web_auth_logo.jpg」）。

- すべてのイメージ ファイルの名前は、33 文字以上にすることができません。
- カスタム ページ上のイメージは、アクセス可能な HTTP サーバ上になければなりません。HTTP サーバにアクセスできるように、アドミッション ルール内に代行受信 ACL を設定する必要があります。
- カスタム ページからのすべての外部リンクでは、アドミッション ルール内で代行受信 ACL を設定する必要があります。
- 外部リンクまたは画像に必要なすべての名前解決では、有効な DNS サーバにアクセスするためにアドミッション ルール内で代行受信 ACL を設定する必要があります。
- カスタム Web ページ機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能がイネーブルである場合、成功ログイン機能のリダイレクション URL は利用不可能です。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web 形式であるため、このページについて次の注意事項に留意してください。

- ログイン形式では、ユーザ名およびパスワードのユーザ入力を受け入れて、そのデータを **uname** および **pwd** として POST する必要があります。
- カスタム ログイン ページは、ページ タイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベスト プラクティスに従う必要があります。

次に、カスタム認証プロキシ Web ページを設定する例を示します。

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

次に、カスタム認証プロキシ Web ページの設定を確認する例を示します。

```
Router# show ip admission configuration

Authentication proxy webpage
 Login page           : disk1:login.htm
 Success page         : disk1:success.htm
 Fail Page            : disk1:fail.htm
 Login expired Page   : disk1:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

成功ログインに対するリダイレクション URL の指定

ユーザが認証に成功したあとにリダイレクトされる URL を指定するオプションがあり、内部成功 HTML ページを効率的に置き換えることができます。

成功ログインのリダイレクション URL を指定するには、グローバル コンフィギュレーション モードで次の作業を行います。

コマンド	目的
Router(config)# **ip admission proxy http success redirect** *url-string*	デフォルトのログイン成功ページの代わりにユーザをリダイレクトする URL を指定します。

ログイン成功時のリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルである場合、リダイレクション URL 機能はディセーブルに設定され、CLI で利用できなくなります。リダイレクションはカスタム ログイン成功ページ内で実行できます。
- リダイレクション URL 機能がイネーブルである場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。

次に、ログイン成功時のリダイレクション URL を設定する例を示します。

```
Router(config)# ip admission proxy http success redirect www.cisco.com
```

次に、ログイン成功時のリダイレクション URL を確認する例を示します。

```
Router# show ip admission configuration

Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.cisco.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

AAA 失敗ポリシーの設定

AAA 失敗ポリシーを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip admission name rule-name proxy http event timeout aaa policy identity identity_policy_name`	AAA 失敗ルールを作成し、AAA サーバにアクセスできない場合にセッションに適用されるアイデンティティ ポリシーを関連付けます。 スイッチ上のルールを削除するには、**no ip admission name** *rule-name* **proxy http event timeout aaa policy identity** グローバル コンフィギュレーション コマンドを使用します。
ステップ 2	`Router(config)# ip admission ratelimit aaa-down number_of_sessions`	（任意）AAA サーバが稼働状態に戻ったときに AAA サーバのフラッディングを回避するために、AAA ダウン ステートのホストからの認証試行をレート制限できます。

次に、AAA 失敗ポリシーを適用する例を示します。

```
Router(config)# ip admission name AAA_FAIL_POLICY proxy http event timeout aaa policy
identity GLOBAL_POLICY1
```

次に、AAA ダウン ステートで接続されているホストがあるかどうかを判別する例を示します。

```
Router# show ip admission cache
Authentication Proxy Cache
 Client IP 209.165.201.11 Port 0, timeout 60, state ESTAB (AAA Down)
```

次に、ホスト IP アドレスに基づいて特定のセッションに関する詳細情報を表示する例を示します。

```
Router# show ip admission cache 209.165.201.11
Address              : 209.165.201.11
MAC Address          : 0000.0000.0000
Interface            : Vlan333
Port                 : 3999
Timeout              : 60
Age                  : 1
State                : AAA Down
AAA Down policy      : AAA_FAIL_POLICY
```

Web ベース認証のパラメータ設定

失敗できるログイン試行回数の最大値を設定します。失敗した試行回数がこの値を超えると、クライアントは待機期間中、ウォッチ リストに載せられます。

Web ベース認証パラメータを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# ip admission max-login-attempts number`	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 です。デフォルトは 5 です。
ステップ 2	`Router(config)# end`	特権 EXEC モードに戻ります。

次の例では、失敗ログイン試行の最大回数を 10 に設定する方法を示します。

```
Router(config)# ip admission max-login-attempts 10
```

Web ベース認証のキャッシュ エントリの削除

既存のセッション エントリを削除するには、次のいずれかの作業を行います。

コマンド	目的
Router# **clear ip auth-proxy cache** {* | *host ip address*}	認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。
Router# **clear ip admission cache** {* | *host ip address*}	認証プロキシ エントリを削除します。キャッシュ エントリすべてを削除するには、アスタリスクを使用します。シングル ホストのエントリを削除するには、具体的な IP アドレスを入力します。

次に、特定の IP アドレスのクライアントに対する Web ベース認証セッションを削除する例を示します。

```
Router# clear ip auth-proxy cache 209.165.201.1
```

Web ベース認証ステータスの表示

すべてのインターフェイスまたは特定のポートの Web ベース認証設定を表示するには、次の作業を行います。

コマンド	目的
Router# **show fm ip-admission l2http** [**all** | **interface** *type slot/port*]	Web ベース認証設定を表示します。 （任意）**all** キーワードを使用して、Web ベース認証を使用するすべてのインターフェイスを表示します。 （任意）特定のインターフェイスに対する Web ベース認証設定を表示するには、キーワード **interface** を使用します。

次に、グローバルな Web ベース認証のステータスだけを表示する例を示します。

```
Router# show fm ip-admission l2http all
```

次に、インターフェイス GigabitEthernet 3/27 の Web ベース認証を表示する例を示します。

```
Router# show fm ip-admission l2http interface gigabitethernet 3/27
```

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する