CHAPTER 11

Web ベース認証の設定

この章では、Web ベース認証を設定する手順について説明します。内容は次のとおりです。

（注） この章で使用するスイッチ コマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

Web ベース認証の概要

Web ベース認証機能（*Web 認証プロキシ*とも呼ばれます）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 ユーザを認証します。

（注） Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上で設定できます。

Web ベース認証では、ユーザが HTTP セッションを開始すると、ホストからの入力 HTTP パケットが代行受信され、ユーザに HTML ログイン ページが送信されます。ユーザが認定証を入力すると、その情報は、認証のために Authentication, Authorization, Accounting（AAA; 認証、認可、アカウンティング）サーバに送信されます。

認証に成功すると、ログイン成功 HTML ページがホストに送信され、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、ログイン失敗 HTML ページがユーザに転送され、ユーザはログインを再試行するように求められます。ユーザが試行の最大数を超過すると、ログイン期限切れ HTML ページがホストに転送され、そのユーザは一定の待機時間、ウォッチ リストに配置されます。

ここでは、AAA の一部としての Web ベース認証の役割について説明します。

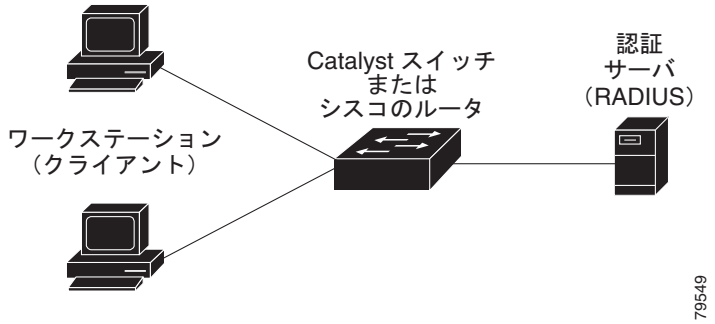
デバイスの役割

Web ベース認証では、ネットワーク上のデバイスには次のような特定の役割があります。

- *クライアント*：LAN および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）。ワークステーションは、Java スクリプト対応の HTML ブラウザを実行している必要があります。
- *認証サーバ*：クライアントを認証します。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対して LAN およびスイッチ サービスへのアクセスを許可するのか、そのクライアントを拒否するの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間の仲介デバイス（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。

図 11-1 に、ネットワーク上でのこれらのデバイスの役割を示します。

図 11-1　Web ベース認証のデバイスの役割



ホスト検出

スイッチは、検出されたホストに関する情報を保存するための IP デバイス トラッキング テーブルを維持しています。

（注） デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルです。Web ベース認証を使用するには、IP デバイス 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 2 インターフェイスの場合、Web ベース認証では次のメカニズムを使用して IP ホストが検出されます。

- Address Resolution Protocol（ARP; アドレス解決プロトコル）ベース トリガー：ARP リダイレクト Access Control List（ACL; アクセス コントロール リスト）により、スタティック IP アドレスまたはダイナミック IP アドレスで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 Dynamic Host Configuration Protocol（DHCP）バインディング エントリを作成すると、Web ベース認証が通知されます。

セッションの作成

Web ベース認証で新規ホストが検出されると、次のようにセッションを作成します。

- 例外リストを確認します。

  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ます。

- 認可バイパスを確認します。

  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、このホストの認可がバイパスされます。セッションは確立されます。

- 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、認可が開始されます。スイッチからユーザにログイン ページが送信されます。ユーザがユーザ名とパスワードを入力すると、スイッチからサーバにエントリが送信されます。
- 認証に成功すると、ユーザのアクセス ポリシーが認証サーバからスイッチにダウンロードされて、アクティブになります。ログイン成功ページがユーザに送信されます。
- 認証に失敗すると、ログイン失敗ページがスイッチから送信されます。ユーザがログインを再試行します。試行の最大数を超過すると、ログイン期限切れページがスイッチから送信され、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できます。
- 認証サーバがスイッチに応答せず、かつ AAA 失敗ポリシーが設定されている場合は、スイッチによって、その失敗アクセス ポリシーがクライアントに適用されます。ログイン成功ページがユーザに送信されます（「ローカル Web 認証バナー」（P.11-4）を参照）。
- 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、またはホストがレイヤ 3 インターフェイスのアイドル タイムアウト内にトラフィックを送信しない場合は、スイッチによってクライアントが再認証されます。
- 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 タイムアウトに適用されます。
- 終了処理が Remote Authentication Dial-In User Service（RADIUS）の場合は、非応答ホスト（NRH）要求がサーバに送信されます。終了処理は、サーバからの応答に含まれています。
- 終了処理がデフォルトの場合は、セッションが破棄され、適用されたポリシーが削除されます。

ローカル Web 認証バナー

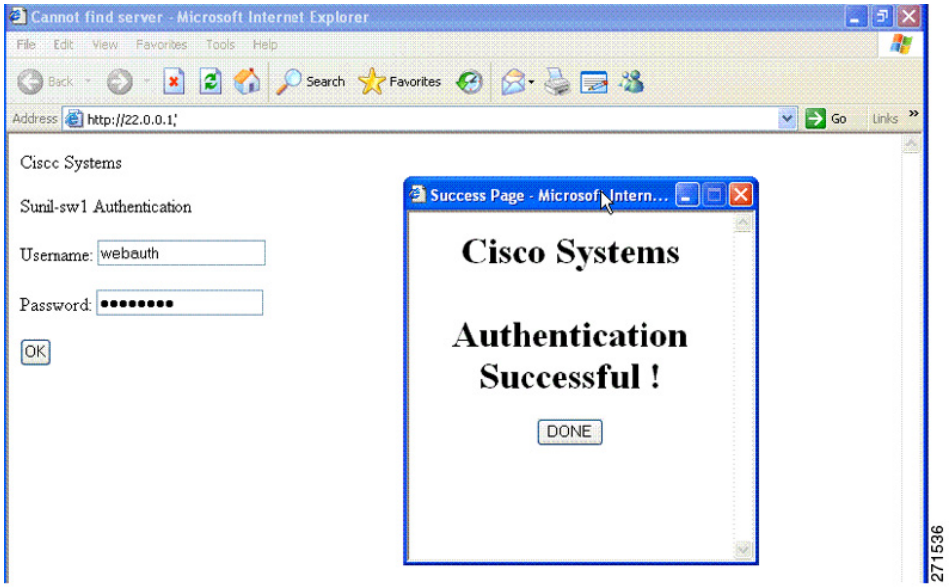
Web 認証を使用すると、スイッチへのログイン時に表示されるバナーを作成できます。

バナーはログイン ページと認証結果のポップアップ ページの両方に表示されます。

- [*Authentication Successful*]
- [*Authentication Failed*]
- [*Authentication Expired*]

バナーは、**ip admission auth-proxy-banner http** 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作成します。ログイン ページに表示されるデフォルトのバナーは、[*Cisco Systems*] および [*Switch host-name Authentication*] です。*Cisco Systems* のバナーは、図 11-2 のように認証結果のポップアップ ページに表示されます。

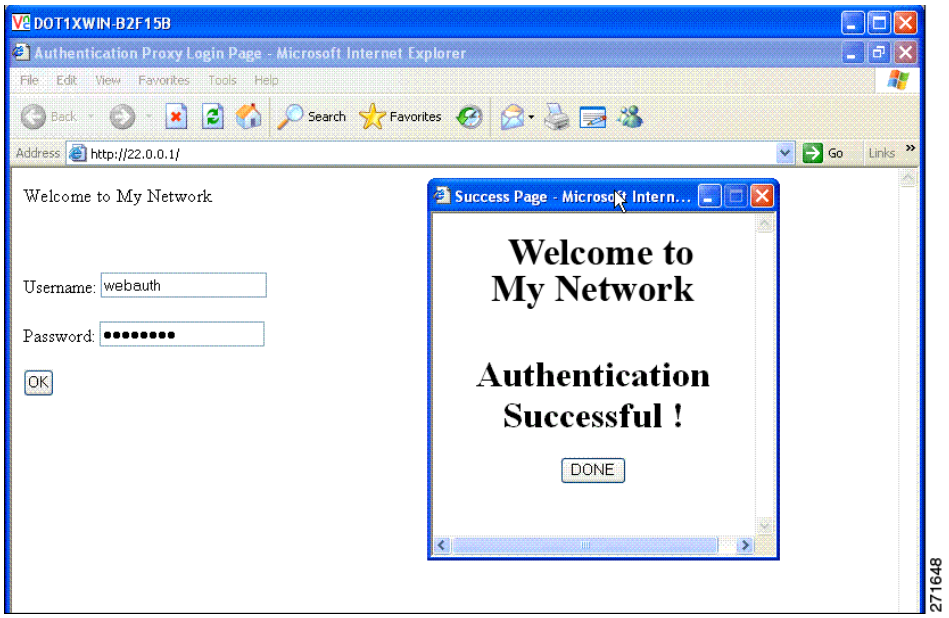
図 11-2　[Authentication Successful] バナー



バナーは図 11-3 のようにカスタマイズすることもできます。

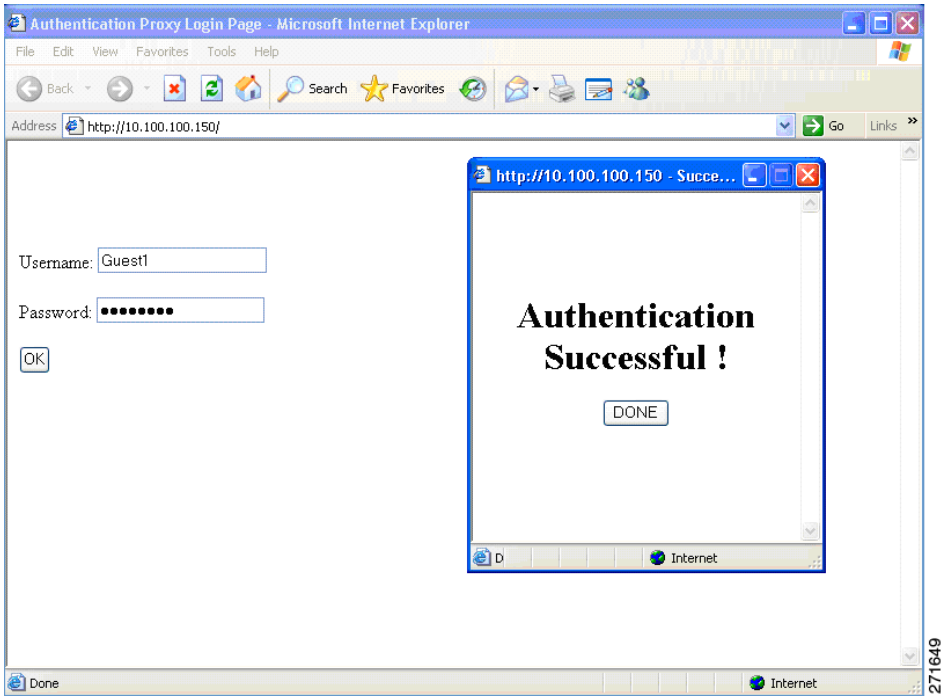
- **ip admission auth-proxy-banner http** *banner-text* グローバル コンフィギュレーション コマンドを使用して、スイッチ、ルータ、または会社名をバナーに追加します。
- **ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用して、ロゴまたはテキスト ファイルをバナーに追加します。

図 11-3　カスタマイズされた Web バナー



バナーを有効にしない場合、ユーザ名とパスワードのダイアログ ボックスのみが Web 認証ログイン画面に表示されます。スイッチへのログイン時にバナーは表示されません（図 11-4 を参照）。

図 11-4　バナーのないログイン画面



詳細については、『Cisco IOS Security Command Reference』および「Web 認証ローカル バナーの設定」（P.11-17）を参照してください。

Web 認証のカスタマイズ可能な Web ページ

Web ベース認証プロセス中、スイッチの内部 HTTP サーバは、認証クライアントに配信される 4 つの HTML ページをホストします。これらのページにより、次の 4 つの認証プロセス ステートがユーザに通知されます。

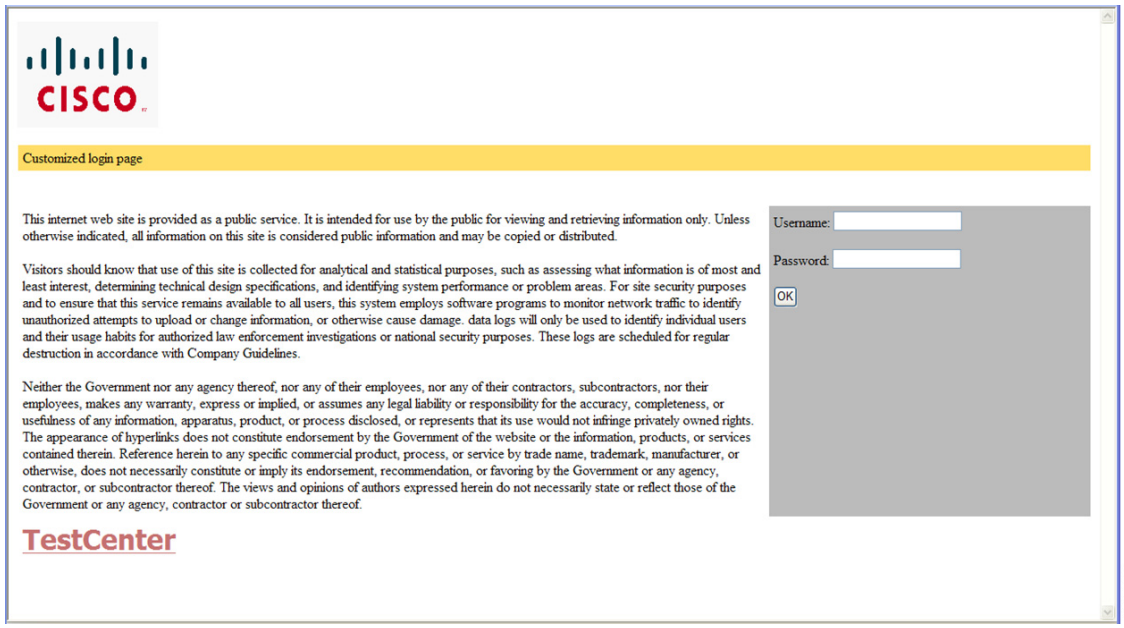
- ログイン：ユーザの認定証が要求されます。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：過剰なログイン失敗のため、ログイン セッションがログイン セッションが期限切れになりました。

注意事項

- デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。
- ロゴを使用し、*ログイン*、*成功*、*失敗*、および*期限切れ* Web ページのテキストを指定できます。
- バナー ページでは、ログイン ページのテキストを指定できます。
- これらのページは HTML 形式です。
- 特定の Universal Resource Locator（URL）にアクセスするには、HTML リダイレクト コマンドを含める必要があります。
- URL 文字列には、有効な URL（たとえば、http://www.cisco.com）を指定する必要があります。URL が不完全である場合は、Web ページ上に "*page not found*"（ページがみつかりません）または同様のエラーが表示される可能性があります。
- HTTP 認証の Web ページを設定する場合は、適切な HTML コマンド（ページのタイムアウトを設定するコマンド、非表示のパスワードを設定するコマンド、同じページが 2 回送信されていないことを確認するコマンドなど）をページに含める必要があります。
- 設定済みのログイン フォームがイネーブルである場合、ユーザを特定の URL にリダイレクトする CLI コマンドは使用できません。管理者は、Web ページ内でリダイレクションが設定されていることを確認する必要があります。
- 認証後にユーザを特定の URL にリダイレクトする CLI コマンドを入力した後で Web ページを設定するコマンドを入力すると、ユーザを特定の URL にリダイレクトする CLI コマンドは機能しません。
- 設定した Web ページは、スイッチのブート フラッシュまたはフラッシュにコピーできます。
- 設定したページには、スタック マスターまたはスタック メンバーからアクセスできます。
- ログイン ページを 1 つのフラッシュ上に配置し、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスターまたはスタック メンバー）上に配置することもできます。
- 4 つのページをすべて設定する必要があります。
- バナー ページを Web ページと一緒に設定しても効果はありません。
- システム ディレクトリ（フラッシュ、ディスク 0、ディスクなど）内に保存され、ログイン ページに表示される必要があるすべてのロゴ ファイル（イメージ、フラッシュ、音声、ビデオなど）は、ファイル名として *web_auth_<filename>* を使用する必要があります。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートします。

図 11-5（P.11-7）に示すように、デフォルトの内部 HTML ページを独自の HTML ページに置き換えることができます。認証のユーザのリダイレクト先 URL を指定することにより、内部の成功ページを置き換えることもできます。

図 11-5　カスタマイズ可能な認証ページ



詳細については、「認証プロキシ Web ページのカスタマイズ」（P.11-14）を参照してください。

Web ベース認証とその他の機能の相互作用

- 「ポート セキュリティ」（P.11-7）
- 「LAN ポート IP（LPIP）」（P.11-8）
- 「ゲートウェイ IP (GWIP)」（P.11-8）
- 「ACL」（P.11-8）
- 「コンテキスト ベース アクセス コントロール（CBAC）」（P.11-8）
- 「802.1X 認証」（P.11-8）
- 「EtherChannel」（P.11-8）

ポート セキュリティ

同一ポート上に Web ベース認証とポート セキュリティを設定することができます。Web ベース認証を使用してポートを認証し、ポート セキュリティを使用して、クライアントを含むすべての Media Access Control（MAC; メディア アクセス制御）アドレスに対するネットワーク アクセスを管理します。この場合、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またはグループを制限できます。

ポート セキュリティのイネーブル化の詳細については、「ポート セキュリティの設定」（P.26-9）を参照してください。

LAN ポート IP（LPIP）

同一ポート上に LAN Port IP（LPIP; LAN ポート IP）とレイヤ 2 Web ベース認証を設定できます。まず Web ベース認証を使用してホストが認証され、次に LPIP ポスチャ検証が実行されます。LPIP ホスト ポリシーは、Web ベース認証ホスト ポリシーを上書きします。

Web ベース認証アイドル タイマーの期限が満了すると、NAC ポリシーが削除されます。ホストが認証され、ポスチャが再び検証されます。

ゲートウェイ IP (GWIP)

Web ベース認証が VLAN のいずれかのスイッチ ポートに設定されている場合は、レイヤ 3 VLAN インターフェイス上に Gateway IP（GWIP; ゲートウェイ IP）を設定できません。

ゲートウェイ IP と同じレイヤ 3 インターフェイスに Web ベース認証を設定できます。両方の機能のホスト ポリシーがソフトウェアによって適用されます。GWIP ポリシーは、Web ベース認証ホスト ポリシーを上書きします。

ACL

VLAN ACL または Cisco IOS ACL をインターフェイス上に設定すると、Web ベース認証ホスト ポリシーが適用されたあとに ACL がホスト トラフィックに適用されます。

レイヤ 2 Web ベース認証の場合は、ポートに接続されたホストからの入力トラフィックのデフォルト アクセス ポリシーとして Port ACL（PACL; ポート ACL）を設定する必要があります。認証後、Web ベース認証ホストポリシーによって PACL が上書きされます。

MAC ACL と Web ベース認証は同じインターフェイス上に設定できません。

Web ベース認証は、アクセス VLAN が VACL キャプチャ用に設定されているポート上には設定できません。

コンテキスト ベース アクセス コントロール（CBAC）

Context-based Access Control（CBAC; コンテキストベース アクセス コントロール）がポート VLAN のレイヤ 3 VLAN インターフェイス上に設定されている場合は、Web ベース認証をレイヤ 2 ポート上に設定できません。

802.1X 認証

Web ベース認証は、フォールバック認証メソッドとして設定する場合を除き、802.1X 認証と同じポート上には設定できません。

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。

Web ベース認証の設定

Web ベース認証のデフォルト設定

表 11-1 に、Web ベース認証のデフォルト設定を示します。

表 11-1　Web ベース認証のデフォルト設定

機能	デフォルト設定値
AAA	ディセーブル
RADIUS サーバ • IP アドレス • User Datagram Protocol（UDP; ユーザ データグラム プロトコル）認証ポート • 鍵	 • 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 ベース認証の設定時の注意事項および制限事項

- Web ベース認証は入力のみの機能です。
- Web ベース認証はアクセス ポートだけに設定できます。Web ベース認証はトランク ポート、EtherChannel のメンバー ポート、およびダイナミック トランク ポート上ではサポートされません。
- Web ベースを設定する前に、デフォルト ACL をインターフェイス上に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。
- スタティック ARP キャッシュが割り当てられたレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能によって検出されません。
- デフォルトでは、スイッチの IP デバイス トラッキング機能はディセーブルです。Web ベース認証を使用するには、IP デバイス トラッキング機能をイネーブルにする必要があります。

- スイッチの HTTP サーバを実行するには、少なくとも 1 つの IP アドレスを設定する必要があります。各ホストの IP アドレスに到達するためのルートを設定する必要もあります。HTTP サーバからホストに HTTP ログイン ページが送信されます。
- 複数ホップ離れているホストでは、Spanning-Tree Protocol（STP; スパニング ツリー プロトコル）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到着すると、トラフィックが中断する可能性があります。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ていない可能性があるためです。
- Web ベース認証は、ダウンロード可能なホスト ポリシーとして VLAN 割り当てをサポートしていません。
- IPv6 トラフィックに対しては、Web ベース認証はサポートされません。

Web ベース認証設定のタスク リスト

- 「認証ルールとインターフェイスの設定」（P.11-10）
- 「AAA 認証の設定」（P.11-11）
- 「スイッチと RADIUS サーバ間の通信設定」（P.11-12）
- 「HTTP サーバの設定」（P.11-13）
- 「AAA 失敗ポリシーの設定」（P.11-16）
- 「Web ベース認証パラメータの設定」（P.11-16）
- 「Web ベース認証のキャッシュ エントリの削除」（P.11-17）

認証ルールとインターフェイスの設定

	コマンド	目的
ステップ 1	**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	**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。 *type* には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 3	**ip access-group** *name*	デフォルトの ACL を適用します。
ステップ 4	**ip admission** *name*	指定したインターフェイス上に Web ベース認証を設定します。
ステップ 5	**exit**	コンフィギュレーション モードに戻ります。
ステップ 6	**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 7	**end**	特権 EXEC モードに戻ります。
ステップ 8	**show ip admission configuration**	設定を表示します。
ステップ 9	**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。

次に、ファスト イーサネット ポート 5/1 で Web ベース認証をイネーブルにする例を示します。

```
Switch(config)# ip admission name webauth1 proxy http
Switch(config)# interface fastethernet 5/1
Switch(config-if)# ip admission webauth1
Switch(config-if)# exit
Switch(config)# ip device tracking
```

次に、設定を確認する例を示します。

```
Switch# 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

	コマンド	目的
ステップ 1	**aaa new-model**	AAA 機能をイネーブルにします。
ステップ 2	**aaa authentication login default group** {*tacacs+* | *radius*}	ログイン時の認証方式のリストを定義します。
ステップ 3	**aaa authorization auth-proxy default group** {*tacacs+* | *radius*}	Web ベース認可の認可方式のリストを作成します。
ステップ 4	**tacacs-server host** {*hostname* | *ip_address*}	AAA サーバを指定します。RADIUS サーバについては、「スイッチと RADIUS サーバ間の通信設定」（P.11-12）を参照してください。
ステップ 5	**tacacs-server key** {*key-data*}	スイッチと Terminal Access Controller Access Control System（TACACS）サーバの間で使用される認可および暗号鍵を設定します。
ステップ 6	**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。

次に、AAA をイネーブルにする例を示します。

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

スイッチと RADIUS サーバ間の通信設定

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、サーバの同一 IP アドレス上にある複数の 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 エントリを同じサービス（例えば認証など）に対して設定すると、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機能します。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には、次の作業を行います。

	コマンド	目的
ステップ 1	**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	**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* オプションを使用すると、RADIUS サーバとの接続を自動的にテストできます。*username* には、有効なユーザ名を指定する必要はありません。 **key** オプションには、スイッチと RADIUS サーバとの間で使用する認証および暗号鍵を指定します。 複数の RADIUS サーバを使用する場合は、このコマンドをサーバごとに再入力します。
ステップ 3	**radius-server key** *string*	スイッチと RADIUS サーバ上で動作する RADIUS デーモンの間で使用される認可および暗号鍵を設定します。
ステップ 4	**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。この機能は、Cisco IOS Release 12.2(50)SG でサポートされています。
ステップ 5	**radius-server dead-criteria tries** *num-tries*	サーバを非アクティブにすることを検討する前に、RADIUS サーバへの未応答の送信メッセージの数を指定します。指定できる *num-tries* の範囲は 1 ～ 100 です。

RADIUS サーバ パラメータを設定する際には、次の作業を行います。

- **key** *string* は別のコマンドラインで指定します。
- **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鍵を指定します。鍵はテキスト ストリングで、RADIUS サーバで使用されている暗号鍵と一致する必要があります。
- **key** *string* を指定する場合は、鍵の途中および末尾でスペースを使用します。鍵でスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は RADIUS デーモンで使用する暗号鍵と一致している必要があります。

- すべての RADIUS サーバについて、タイムアウト、再送信回数、および暗号鍵の値をグローバルに設定するには、**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。詳細については、次の URL の『*Cisco IOS Security Configuration Guide*』*Release 12.2* および『*Cisco IOS Security Command Reference*』*Release 12.2* を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

（注）　RADIUS サーバ上でも、スイッチの IP アドレス、サーバとスイッチの双方で共有されるキー ストリング、ダウンロード可能な ACL（DACL）など、いくつかの値を設定する必要があります。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。

```
Switch(config)# ip radius source-interface Vlan80
Switch(config)# radius-server host 172.120.39.46 test username user1
Switch(config)# radius-server key rad123
Switch(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。イネーブルにできるサーバは、HTTP または HTTPS です。

	コマンド	目的
ステップ 1	**ip http server**	HTTP サーバをイネーブルにします。Web ベース認証機能では、HTTP サーバを使用してユーザ認証用のホストと通信します。
ステップ 2	**ip http secure-server**	HTTPS をイネーブルにします。

カスタム認証プロキシ Web ページを設定するか、またはログインに成功した場合のリダイレクション URL を指定できます。

（注）　**ip http secure-secure** コマンドの実行時にセキュアな認証を保証するため、ユーザが HTTP 要求を送信しても、ログイン ページは常に HTTPS（セキュア HTTP）となります。

- 認証プロキシ Web ページのカスタマイズ
- ログインに成功した場合のリダイレクション URL の指定

認証プロキシ Web ページのカスタマイズ

Web ベース認証時に、スイッチのデフォルト HTML ページではなく 4 つの代替 HTML ページをユーザに表示する Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、スイッチのフラッシュ メモリにカスタム HTML ファイルを保存してから、このタスクをグローバル コンフィギュレーション モードで実行します。

	コマンド	目的
ステップ 1	**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 システムにおける場所を指定します。*device:* はフラッシュ メモリを表します。
ステップ 2	**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 ファイルの場所を指定します。
ステップ 3	**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	**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。

カスタマイズされた認証プロキシ Web ページを設定する場合は、次の注意事項に従ってください。

- カスタム Web ページ機能をイネーブルにするには、4 つのカスタム HTML ファイルをすべて指定します。4 つのファイルをすべて指定しないと、デフォルトの内部 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、スイッチのフラッシュ メモリ上に存在する必要があります。各 HTML ファイルの最大サイズは 8 KB です。
- カスタム ページ上のすべてのイメージは、アクセス可能な HTTP サーバに存在する必要があります。管理ルール内に代行受信 ACL を設定します。
- カスタム ページからの外部リンクには、管理ルール内に代行受信 ACL を設定する必要があります。
- 有効な Domain Name System（DNS; ドメイン ネーム システム）サーバにアクセスするには、外部リンクまたは外部イメージに必要な名前解決で、管理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 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、ログインの失敗機能のリダイレクション URL は使用できません。
- カスタム ファイルの指定を削除するには、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、このページに関する次の注意事項に従ってください。

- ログイン フォームは、ユーザ名とパスワードに対するユーザ エントリを受け入れ、**uname** と **pwd** をユーザに表示する必要があります。
- カスタム ログイン ページは、ページのタイムアウト、非表示のパスワード、冗長送信の防止など、Web フォームに関するベストプラクティスに従っている必要があります。

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。

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
```

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash: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。

```
Switch# show ip admission configuration
Authentication proxy webpage
 Login page           : flash:login.htm
 Success page         : flash:success.htm
 Fail Page            : flash:fail.htm
 Login expired Page   : flash: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
```

ログインに成功した場合のリダイレクション URL の指定

内部の*成功* HTML ページを効果的に置き換えることにより、認証後のユーザのリダイレクト先 URL を指定できます。

コマンド	目的
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、ユーザのリダイレクション URL を指定します。

ログインに成功した場合のリダイレクション URL を設定する場合は、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の場合、リダイレクション URL 機能はディセーブルになり、CLI で使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- 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 の指定を削除するには、このコマンドの **no** 形式を使用します。

次に、ログインに成功した場合のリダイレクション URL を設定する例を示します。

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

次に、ログインに成功した場合のリダイレクション URL を確認する例を示します。

```
Switch# 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

	コマンド	目的
ステップ 1	**ip admission name** *rule-name* **proxy http event timeout aaa policy identity** *identity_policy_name*	AAA の失敗ルールを作成し、AAA サーバに到達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。 **（注）** 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	**ip admission ratelimit aaa-down** *number_of_sessions*	（任意）サービスを返すときの AAA サーバのフラッディングを防ぐため、AAA ダウン ステートのホストからの認証試行回数に対してレート制限を実施します。

次に、AAA の失敗ポリシーを適用する例を示します。

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

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

```
Switch# 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。

```
Switch# 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 ベース認証パラメータの設定

ユーザを一定の待機時間、ウォッチ リストに配置するまでに許容する失敗ログイン試行の最大数を設定できます。

	コマンド	目的
ステップ 1	**ip admission max-login-attempts** *number*	失敗ログイン試行の最大数を設定します。設定範囲は 1 ～ 2147483647 回です。デフォルトは 5 です。
ステップ 2	**end**	特権 EXEC モードに戻ります。
ステップ 3	**show ip admission configuration**	認証プロキシ設定を表示します。
ステップ 4	**show ip admission cache**	認証エントリのリストを表示します。
ステップ 5	**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。

次に、失敗ログイン試行の最大数を 10 回に設定する例を示します。

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

Web 認証ローカル バナーの設定

Web 認証を設定したスイッチにローカル バナーを設定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	**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 2	**ip admission auth-proxy-banner http** [***banner-text*** | ***file-path***]	ローカル バナーをイネーブルにします。 （任意）*C banner-text C* を入力し、カスタム バナーを作成します。*C* は、バナーに表示されるファイルのファイル パスを示しています（ロゴまたはテキスト ファイルなど）。
ステップ 3	**end**	特権 EXEC モードに戻ります。
ステップ 4	**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。

次に、カスタム メッセージ *My Switch* を表示するローカル バナーを設定する例を示します。

```
Switch(config) configure terminal
Switch(config)# aaa new-model
Switch(config)# aaa ip auth-proxy auth-proxy-banner C My Switch C
Switch(config) end
```

ip auth-proxy auth-proxy-banner コマンドの詳細については、Cisco.com にある『*Cisco IOS Security Command Reference*』の「Authentication Proxy Commands」の章を参照してください。

Web ベース認証のキャッシュ エントリの削除

コマンド	目的
clear ip auth-proxy cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するにはアスタリスクを使用します。単一ホストのエントリを削除するには、特定の IP アドレスを入力します。
clear ip admission cache {* | *host ip address*}	認証プロキシ エントリを削除します。すべてのキャッシュ エントリを削除するにはアスタリスクを使用します。単一ホストのエントリを削除するには、特定の IP アドレスを入力します。

次に、IP アドレスが 209.165.201.1 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。

```
Switch# 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
ステップ 1	**show authentication sessions** [**interface** *type slot/port*]	Web ベース認証設定を表示します。 type = fastethernet、gigabitethernet、または tengigabitethernet （任意）**interface** キーワードを使用して、特定のインターフェイスの Web ベース認証設定を表示します。

次に、グローバル Web ベース認証ステータスだけを表示する例を示します。

```
Switch# show authentication sessions
```

次に、ギガビット インターフェイス 3/27 の Web ベース認証設定を表示する例を示します。

```
Switch# show authentication sessions interface gigabitethernet 3/27
```