CHAPTER 17

Manager Web コンソールの設定

この章では、ACE Web Application Firewall Manager Web コンソールの設定方法について説明します。内容は次のとおりです。

Manager SSL 証明書の変更

SSL 証明書は、Web ブラウザと ACE Web Application Firewall Manager Web コンソール（管理ポート（デフォルトでは 8243）上）間の接続をセキュアにするために使用されます。インストール時に、この接続をセキュアにするために一時的な証明書が使用されます。この証明書は、ここで説明するように ACE Web Application Firewall Manager で生成する永久的な証明書に置き換える必要があります。

（注） ACE Web Application Firewall Manager は、秘密鍵を UTF8 形式で生成できません。ACE Web Application Firewall Manager は UTF8 形式の既存の証明書と鍵をインポートできますが、生成できません。

Manager での CSR の生成

ACE Web Application Firewall Manager SSL 証明書の Certificate Signing Request（CSR; 証明書署名要求）を生成するには、次の手順に従います。

ステップ 1 `administrator` ユーザとして、操作メニューの [Administration] セクションの [Cluster Management] リンクをクリックします。

[Cluster Management] ページのこの Manager の管理コントロールにクラスタが表示されます。複数のクラスタを使用していない場合は、リストに単一クラスタ（Default Cluster）が表示されます。

ステップ 2 [Manage SSL Certificates] ボタンをクリックします。

ステップ 3 証明書署名要求（CSR）を生成するには、[Manage Certificates] ボタンをクリックし、次に [Generate New CSR]（[Manager SSL Certificates] ページの [Outstanding Certificates Signing Requests] 領域内）をクリックします。

ステップ 4　[Generate Certificate Signing Request] ページで、次のすべてのフィールドに情報を入力します。

フィールド	説明
[Common Name]	身元を証明する個人またはエンティティの名前。
[E-mail Address]	CSR に応答して署名入り証明書を受け取る電子メール アドレス。
[Company (O)]	CN が関連付けられる組織または会社の名前。
[Department (OU)]	組織内の組織ユニットまたはサブグループの名前。
[City]	証明されるエンティティの地域または市。
[State]	証明されるエンティティの州または地方。
[ISO Country Code]	エンティティの国を示す 2 文字の International Standards Organization（ISO; 国際標準化機構）コード。

ステップ 5　情報の入力が完了したら、[Generate Request] をクリックします。入力した情報を使用して ACE Web Application Firewall Manager は証明書署名要求（CSR）を生成し、これを [*Certificate Signing Request*] ページに表示します。

ステップ 6　CSR データ（「`-----BEGIN CERTIFICATE REQUEST-----`」文字列と「`-----END CERTIFICATE REQUEST-----`」文字列の間の部分）をテキスト ファイルまたは電子メール メッセージにコピーします。CSR データをお好きな認証局に送信し、署名入り X.509 証明書に変換します。

（注）　CA 依頼フォームでは、証明書タイプを指定するよう求められることがあります。求められた場合は、ACE Web Application Firewall Manager で使用する Apache 形式の証明書を要求してください。

ステップ 7　署名入り証明書が届いたら、「Manager SSL 証明書の設定」（P.17-2）で説明するように ACE Web Application Firewall Manager に署名入り証明書をインストールします。

（注）　CA は証明書を迅速に返すことができないことがあります。場合によっては、証明書署名要求を満たすのに数日間かかることがあります。

Manager SSL 証明書の設定

生成された要求に応じて署名入り証明書を受け取ると、ACE Web Application Firewall Manager の SSL 証明書を CA 署名入り証明書に置き換えることができます。

ステップ 1　CA から署名入り証明書を受け取った後に、`administrator` ユーザとして [Cluster Management] ページに戻ります。

ステップ 2　[Manage Certificates] をクリックし、次に [Upload Signed Cert] リンク（[Outstanding Certificate Signing Requests] ペイン内）をクリックします。

ステップ 3　[Upload New ACE Web Application Firewall Manager Certificate] ページで、ファイル システムまたはネットワークの場所からアップロードする証明書を指定するか、証明書のテキストをテキスト フィールドにコピーします。

ステップ 4　[Upload] ボタンをクリックします。

ステップ 5　証明書を Manager に適用するには、[Exit to Cluster Management] ボタンをクリックします。

ステップ 6　[Cluster Management] ページで証明書を使用するクラスタの隣にある [edit] リンクをクリックします。この ACE Web Application Firewall Manager から複数のクラスタを管理していない場合は、Default Cluster の隣にある [edit] をクリックします。

[SSL Certificate] フィールドに、現在使用中の証明書が表示されます。この値が「Temporary Certificate, Please Regenerate」である場合は、デフォルトの証明書がまだ置き換えられていません。この導入は、このデフォルトの証明書を CA が署名した証明書に置き換えるまで安全であると見なさないでください。

ステップ 7　[SSL Certificate] フィールドで、アップロードした証明書を選択し、[Save Changes] をクリックします。

導入時の URL ベース リソースのリロードの要求

セキュリティ上の理由から、ACE Web Application Firewall Manager はポリシーで使用されたリモート リソースを自動的に取得しません。リモートでホストされたリソース（URL から取得されたスキーマや証明書など）の最新バージョンを常に使用するために、ポリシーを導入する前にこのようなリソースをリロードしなければならないことがあります。

また、ACE Web Application Firewall Manager を設定し、ポリシーを導入する前にリソースをリロードするようコンソール ユーザに要求することもできます。

（注）　詳細については、「導入時の URL ベース リソースのリロード」（P.12-5）を参照してください。

コンソールでリソースリロードの要求を有効にするには、次の手順に従います。

ステップ 1　`Administrator` ユーザとして ACE Web Application Firewall Manager 操作メニューの [System Management] リンクをクリックします。

ステップ 2　[System Management] ページで、ACE Web Application Firewall Manager という見出しの隣にある [Manager Settings] リンクをクリックします。

ステップ 3　一般設定の [Workflow] ペインで、[Prompt users to reload URL-based resources] チェックボックスをクリックします。

ステップ 4　ページの下部にある [Save Changes] ボタンをクリックします。

ステップ 5　リソースリロードの要求がアクティブであることを確認するには、ページの上部にある [Deploy Policy] ボタンをクリックして導入の試行を開始します。

リソースリロードの要求が有効な場合は、[Step 1 of 4: URL Resource Refresh] ページが表示されます。このページが [Deploy Policy] ボタンをクリックした後に最初に表示される画面でない場合は、リソースリロードの要求が有効ではありません。

ステップ 6　導入するか、または [Cancel Deployment] ボタンをクリックして導入せずに [Policy Manager] ページに戻ります。

ユーザ アイドル タイムアウトの設定

セキュリティのために、ACE Web Application Firewall Manager Web コンソールでは、ある一定の時間（設定可能）の後にコンソールからアイドル状態のユーザをログオフさせることができます。デフォルトでは、アイドル タイムアウト セッション期間は 1800 秒、つまり 30 分です。

ACE Web Application Firewall Manager Web コンソールのアイドル タイムアウト期間を変更するには、次の手順に従います。

ステップ 1　administrator ユーザとして操作メニューの [System Management] リンクをクリックします。

ステップ 2　[Manager Settings] リンクをクリックします。

ステップ 3　[Idle Session Timeout] フィールドに新しいアイドル タイムアウト値を秒単位で入力します。この値は、[User Authentication & Security] 設定に表示されます。

ステップ 4　作業が完了したら、[Save Changes] をクリックします。変更内容はただちに反映されます。

ログイン試行に失敗したユーザのブロックの設定

コンソール ユーザが連続してログインに失敗した場合（デフォルトでは 3 回）、ACE Web Application Firewall Manager はコンソールにアクセスするユーザによるそれ以降のログイン試行をブロックできます。ユーザ アカウントは、管理者が直接有効にするまで停止された状態になります。

必要な場合は、次に説明したようにログイン失敗のブロックを無効にできます。また、組み込みの `administrator` ユーザはブロックされないことに注意してください。ただし、Administrator ロールを持つ追加のユーザ アカウントは、ログイン失敗時にブロックされます。

ブロックされたユーザを再び有効にするには、次の手順に従います。

ステップ 1　コンソールで administrator ユーザとして操作メニューから [User Administration] リンクをクリックします。

ステップ 2　無効なユーザの隣にある [Edit] ボタンをクリックします。

ステップ 3　[User Status] を無効から有効に変更します。

ステップ 4　[Save Changes] をクリックします。

この機能の一般的な動作を設定するには、Administrator ユーザとして次の手順に従います。

ステップ 1　操作メニューの [System Management] リンクをクリックします。

ステップ 2　[System Management] ページの [Manager Settings] をクリックします。

ステップ 3　[Disable User After] というラベルのコントロールを使用してこの機能を設定します。このオプションが有効な場合は、指定された回数ログインに失敗すると、ユーザがログインからブロックされます。

ステップ 4　作業が完了したら、[Save Changes] をクリックします。

変更がすぐに反映されます。

表示タイム ゾーンの設定

ACE Web Application Firewall は、内部クロックに Greenwich Mean Time（GMT; グリニッジ標準時）を使用します。GMT はタイムスタンプの確認、内部ログ データ、およびその他のタイム ベースのサービス処理アクティビティに使用されます。

ただし、ACE Web Application Firewall Manager や Firewall の通常の稼動に影響を与えずに ACE Web Application Firewall Manager が情報を表示するために使用するタイム ゾーンを変更できます。

ACE Web Application Firewall Manager の表示用のタイム ゾーンを変更するには、次の手順に従います。

ステップ 1　操作メニューの [System Management] リンクをクリックします。

ステップ 2　[System Management] ページの [Manager Settings] をクリックします。

ステップ 3　ページのインターフェイス セクションで、メニューから [Display Time Zone] を選択します。

ステップ 4　[Save Changes] をクリックします。