CHAPTER 3

最初の手順

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

Manager Web コンソールへのログイン

お使いのネットワークに ACE Web Application Firewall Manager がインストールされたら、ブラウザベース環境にログインし、ACE Web Application Firewall ポリシーの ACE Web Application Firewall Manager Web コンソールを開発できます。

ACE Web Application Firewall Manager Web コンソールは、ほとんどのタイプのブラウザの最新バージョンと連動します。Mozilla Firefox 1.5.0.*x* と 2.0.0.*x*、および Microsoft Internet Explorer 5.5 と 6 には、この Web コンソール専用のサポート機能があります。ACE Web Application Firewall Manager Web コンソールの機能を適切に動作させるには、ブラウザの JavaScript 機能が有効になっている必要があります。

ACE Web Application Firewall Manager Web コンソールにログインするには、次の手順を実行します。

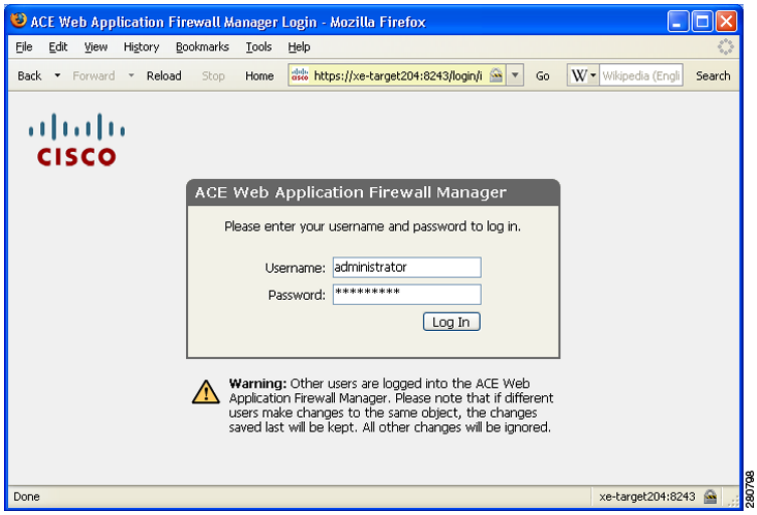
ステップ 1 ACE Web Application Firewall Manager アプライアンスにネットワーク経由でアクセスできるコンピュータ上で、ブラウザを開き、次のアドレスに移動します。

https://< *ホスト名* >:8243

< *ホスト名* > は、お使いの ACE Web Application Firewall Manager の IP アドレスまたはホスト名です。接続には安全な HTTP（HTTPS）が使用されます。ACE Web Application Firewall Manager がコンソールの要求をリッスンするデフォルト ポートは 8243 です。

図 3-1 に示すログイン ページがブラウザに表示されます。

図 3-1　ACE Web Application Firewall Manager Web コンソールへのログイン



ACE Web Application Firewall Manager のホスト名は、最初のインストール時に設定されます。インストール環境のログイン ページへのパスが不明な場合は、管理者に問い合わせてください。

ログイン ページには、すでに Web コンソールにログインした他のユーザがリストされています。他のユーザがコンソールにログインしている場合は注意が必要です。ACE Web Application Firewall Manager では、ユーザ同士による変更の上書きが制限されていません（1 つの設定ページを複数のユーザで同時に編集する場合は、最後に保存された内容が有効になります）。したがって、自身の作業内容をよく確認し、新しいポリシーを実稼動環境に導入する前に、それらのポリシーをテスト環境でテストすることが重要です。

ステップ 2　この ACE Web Application Firewall Manager を使用して ACE Web Application Firewall の複数のクラスタを管理する場合は、アクセスするクラスタ ポリシーを選択できるメニューが表示されることがあります。その場合は、編集するクラスタをメニューから選択してください。

ステップ 3　[Username] フィールドにユーザ名を入力します。たとえば、管理者の場合はこのフィールドに `administrator` と入力します。これは、コンソールに対して完全な権限を持つ、事前設定されたユーザ アカウントです。

（注）　ACE Web Application Firewall Manager Web コンソールにユーザ アカウントを追加する方法については、第 15 章「Web コンソール ユーザの管理」を参照してください。

ステップ 4　[Password] フィールドにパスワードを入力します。

（注）　管理者ユーザのデフォルトのパスワードは「swordfish」です。セキュリティ上の理由から、デフォルト パスワードは必ず変更してください。

ステップ 5　[Log In] ボタンをクリックします。

正しいユーザ名とパスワードの組み合わせを入力していない場合、エラー メッセージが表示されます。管理者の Manager アクセスの設定によっては、ユーザがログインを試行する回数が制限されており、その回数を超えると ACE Web Application Firewall Manager は無条件に終了し、そのユーザ アカウントは無効になります（デフォルトでは 3 回）。このセキュリティ機能は、administrator ユーザ アカウントを除くすべてのアカウントに適用されます （管理者ユーザ タイプで作成されたユーザ アカウントにも適用されます）。

この機能とユーザ アカウントの復元については、「ログイン試行に失敗したユーザのブロックの設定」（P.17-4）を参照してください。

有効なユーザ名とパスワードの組み合わせを入力すると、次の複数のページのうちいずれかが表示されます。

- ACE Web Application Firewall Manager のライセンスが設定されていない場合は、ライセンス エラー ページが表示されます。ACE Web Application Firewall および Manager のライセンスの取得と適用については、『*Cisco ACE Web Application Firewall Administration Guide*』を参照してください。
- ACE Web Application Firewall Manager に有効なライセンスが設定されておりサービス ルーティングのポリシーが設定されていない場合は、[Welcome] ページが表示されます。[Welcome] ページから、仮想サービスの定義を開始できます。
- ポリシーに仮想サービスが含まれている場合は、[Dashboard] ページが表示されます。[Manager Dashboard] には、システムのイベントおよび動作の概要が示されます。

最初のログイン時に割り当てられたパスワードは、変更しておくことをお勧めします。それには、ページ右上でユーザ名をクリックします。[User Information] ウィンドウで [Change Password] ボタンをクリックし、新しいパスワードを指定します。

デフォルトにより、コンソールでは最小限の複雑度に応じたパスワードが要求されます。パスワードは最低 8 文字で、パスワード全体の最小パーセンテージを超えて辞書の単語が使用されておらず、社会保障番号や国の ID 番号と同じでないものでなければいけません。一般に、パスワードには文字、数字、特殊文字を組み合わせて使用することをお勧めします。

Manager Web コンソールの操作

図 3-2 に、ACE Web Application Firewall Manager Web コンソール インターフェイスの主要な構成を示します。

図 3-2　ACE Web Application Firewall Manager ダッシュボード

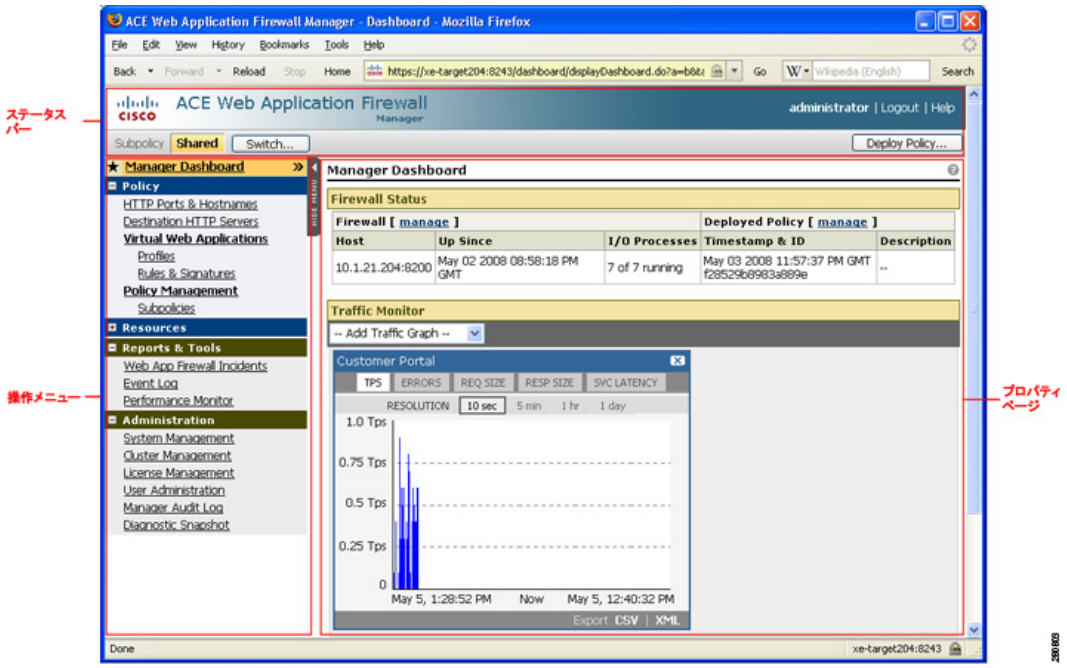


図 3-2 に示すように、ACE Web Application Firewall Manager Web コンソールは次の領域で構成されています。

- 操作メニュー
- ステータス バー
- プロパティ ページ

操作メニュー

操作メニューは、コンソールの左側に表示されます。このメニューには、コンソールの主要な設定ページとモニタリング ページへのリンクが表示され、次のカテゴリにわかれています。

- [Policy] セクションには、ACE Web Application Firewall で処理されるトラフィックに適用されるルールや操作を定義するページへのリンクが含まれています。
- [Resources] セクションには、ポリシーで使用されるリソース ファイルを管理するページへのリンクが含まれています。詳細については、第 11 章「リソース ファイルの管理」を参照してください。
- [Reports & Tools] は、ACE Web Application Firewall およびネットワークのステータスを監視するページにリンクしています。
- [Administration] には、ライセンス、ユーザ アカウント、監査ログ、診断など、コンソール管理者が ACE Web Application Firewall Manager 自体を制御できるページへのリンクが含まれています。

操作メニューの [Policy] 見出しの横に、[Quick Links] ボタン（  ）が表示されます。このボタンから、WSDL ファイルのインポート、仮想サービスの作成、オーセンティケータ（サービスへのアクセス制御に使用されるポリシー オブジェクト）の作成など、一般的なタスクにアクセスできます。

ステータス バー

ステータス バーは、コンソールの各ページの上部に表示されます。ステータス バーには、現在アクティブなサブポリシーと、現在コンソールにアクセスしているユーザ アカウントのユーザ名が表示されます。ステータス バーには、ポリシーの導入やログアウトなど、コンソールでの一般的な操作に使用するボタンがあります。

管理者ユーザは、ステータス バーに表示されるバナー テキストを設定し、たとえば他のコンソール ユーザに通知やその他のタイプの情報を送信できます。

サブポリシーは、ポリシー内のオブジェクトを整理するためのコンテナです。*Shared* サブポリシーは組み込みのサブポリシーで、ユーザが作業の整理にサブポリシーを使用しているかどうかに関係なく存在します。Shared サブポリシーには、すべてのサブポリシーで使用される共通オブジェクトが格納されています。

お使いの環境で、ポリシーの中に Shared 以外にもサブポリシーがある場合は、サブポリシー ラベルの横に [Switch] ボタンが表示されます。[Switch] ボタンをクリックすると、作業中のコンテキストを別のサブポリシーに変更できます。

サブポリシーの詳細については、「サブポリシーに関する作業」（P.13-2）を参照してください。

プロパティ ページ

プロパティ ページには、システムの動作の特定領域に関する情報または設定が表示されます。通常は、プロパティ ページから、機能に関連付けられた構成可能な設定のコントロールにアクセスできます。

サブポリシーを使用したポリシーの編成

ポリシー内の関連するオブジェクトは、*サブポリシー*を使用して整理できます。サブポリシーは、所定のポリシー内のオブジェクトのサブセットです。サブポリシーへのアクセスは、権限を持つコンソールユーザだけがそのサブポリシーを変更できるように制御できます。

システムには、*Shared* というサブポリシーが組み込まれています。新しくインストールされた ACE Web Application Firewall Manager の Web コンソールに初めてログインすると、Shared サブポリシーはアクティブになっています。他のサブポリシーからアクセスできるオブジェクトが含まれているのは、Shared サブポリシーだけです。Shared サブポリシー以外では、サブポリシーをまたいで設定やオブジェクトを使用できません。

サブポリシーに最も適した編成方法、つまり、特定のサブポリシーまたは Shared サブポリシー内で作成するオブジェクトをどのように選択するかは、実装ごとに異なる場合があります。ただし Shared サブポリシーには、ポート設定、認証局、共通のバックエンド HTTP サーバなど、プロジェクトを通して必要なリソースを格納するのが一般的です。一方サブポリシーには、通常は仮想サービスや認証オブジェクトなど、アプリケーション固有のオブジェクトを格納します。

ポリシーでサブポリシーを使用する場合は、設定変更やポリシー オブジェクトの追加を行う前に、ACE Web Application Firewall Manager Web コンソールでアクティブなサブポリシーを確認しておくことが重要です。所定のサブポリシー内にポリシー オブジェクトを作成した場合、そのオブジェクトはそのサブポリシーのコンテキストだけで編集できます。オブジェクトを編集できるユーザは、そのサブポリシーを変更する権限を持ったユーザだけです。

サブポリシーは、ポリシー作成環境の管理と保護に役立ちます。承認ベースでのポリシーの配置にも、同様の利点があります。承認ベースの配置の場合、ポリシーの導入が ACE Web Application Firewall に反映されるようにするには、コンソール管理者がその導入を承認する必要があります。この機能を利用して、ポリシーの変更や導入プロセスを制御および管理できます。

サブポリシーは、ポリシー内のオブジェクトを整理する手段となりますが、大規模な実装では、作業を分割するために異なるポリシーの使用が必要になる場合があります。ACE Web Application Firewall Manager の複数クラスタ管理機能を使用すると、所定の ACE Web Application Firewall Manager インスタンス内でさまざまなポリシーを開発し、それらを異なる ACE Web Application Firewall クラスタに配置できます。

Manager のコントロールへの Firewall の追加

『*Cisco ACE Web Application Firewall Administration Guide*』で説明されているように、ACE XML アプライアンスは Gateway、Manager、または独立型の 3 つのモードのうちいずれかで動作します。独立型モードのアプライアンスは、Gateway および Manager モードの両方で動作します。

独立型アプライアンスの場合、最初の設定後、ACE Web Application Firewall Manager はすでに自己管理用として設定されています（つまり、Manager が管理する Firewall リストに自身へのエントリが含まれています）。ユーザはポリシーの作業をただちに開始でき、Firewall を設定に追加する必要はありません。

ただし、アプライアンスが Manager 専用モードの場合は、ポリシーを配置およびテストする前に、ここで説明するように Firewall を Manager の管理コントロールに追加する必要があります。

（注） 独立型アプライアンスの場合、ACE Web Application Firewall Manager は自身の Firewall インスタンスだけでなく、他の Firewall アプライアンスも制御できます。したがって、独立型アプライアンス上で Manager の管理コントロールに Firewall を追加する場合にも、ここで説明する手順を適用できます。

一度に複数の ACE Web Application Firewall Manager で制御されるように ACE Web Application Firewall を設定できません。この制限は、実際の Manager アプライアンスによる管理、または複数クラスタ管理機能で作成された Manager インスタンスによる管理に適用されます。

Firewall を Manager のコントロールに追加する一般的な手順は次のとおりです。

1. アプライアンス シェル インターフェイスから Firewall の動作モードを設定する際に、この Firewall を制御する Manager の IP アドレスを指定します。

（注）　詳細については、『*Cisco ACE Web Application Firewall Administration Guide*』を参照してください。

2. ACE Web Application Firewall Manager の Web コンソールで、Firewall を Manager のクラスタ プールのいずれか（たとえばデフォルト クラスタなど）に追加します。
3. Web コンソールで追加された ACE Web Application Firewall のライセンス ステータスを確認します。必要な場合はライセンスを要求し、適用します。

ここでは、手順 2 の Firewall を Manager のクラスタのいずれかに追加する方法について説明します。Firewall がクラスタ グループに追加されると、Manager からポリシーの配置を受け取ります。次に、Firewall は活動に関するレポートを Manager に返し、Manager は制御下にあるすべての Firewall のロギング情報を集約します。手順 1 および 3 の詳細については、『*Cisco ACE Web Application Firewall Administration Guide*』を参照してください。

（注）　ACE Web Application Firewall Manager は、Firewall のクラスタを複数制御できます。単一クラスタ内のすべての Firewall には、同じポリシー バージョンが設定されている必要がありますが、Manager の制御下にある複数のクラスタには、異なるポリシー バージョンを適用できます。詳細については、第 16 章「Firewall クラスタの管理」を参照してください。

デフォルト クラスタへの Firewall の追加

ACE Web Application Firewall を Manager のコントロールに追加するには、Manager の設定でその Firewall をクラスタに追加します。前述したように、独立型アプライアンスではこれらの手順を実行する必要はありません。これらの手順は、Manager 専用アプライアンスを設定する、または Firewall を独立型アプライアンスの管理コントロールに追加する場合にだけ必要です。

Manager には、「Default Cluster」という事前設定されたクラスタが付属し、これに ACE Web Application Firewall を追加できます。デフォルト クラスタの名前は変更でき、名前以外の設定も変更可能です。別個の ACE Web Application Firewall 環境を維持する明確な意図がない限り、Manager の設定に新しいクラスタを追加しないでください。詳細については、第 16 章「Firewall クラスタの管理」を参照してください。

デフォルト クラスタに ACE Web Application Firewall を追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つユーザとして、Manager Web コンソールの操作メニューで [Cluster Management] リンクをクリックします。

クラスタ管理ページに「Default Cluster」というクラスタ名が表示されます。独立型モード アプライアンスの Manager では、このアプライアンスが唯一のメンバーとして [Default Cluster] に表示されます。それ以外の場合は、新規インストールに空のデフォルト クラスタが表示されます。

ステップ 2　[Default Cluster] の横にある [edit] リンクをクリックして、Firewall をクラスタに追加します。

ステップ 3　任意に、Manager Web コンソールへの SSL アクセスに使用する名前、HTTPS ポート、セキュリティ証明書など、デフォルト クラスタの事前設定を変更します。

このページに表示される **SSL 証明書**は、Web ブラウザから Manager Web コンソールへの接続に適用されます。メニューに示されるとおり、Manager にはデフォルトで使用される一時的な証明書が用意されています。この組み込みの証明書は、ユーザが作成したサーバ証明書に置き換えることをお勧めします。Manager と開発ワークステーションが安全なネットワーク内で動作する場合は、自己署名証明書の使用を選択できます。ただし、セキュリティ レベルを高めるために、特にクラスタが実稼動環境に配置される場合は、Certificate Authority（CA; 認証局）署名付き証明書を使用することをお勧めします。

ブラウザの接続に使用する新しい証明書を作成するには、[Cluster Management] ページの [Manage SSL Certificates] ボタンをクリックします。ここから [Generate CSR] ボタンを使用して、証明書署名要求を作成します。詳細については、「CSR の生成」（P.11-2）を参照してください。サーバ証明書が作成され、Manager にアップロードされたら、このページのメニューからその証明書を選択し、ブラウザ接続に適用します。

ステップ 4　[Cluster Members] テキスト フィールドに、このクラスタに追加する各 ACE Web Application Firewall の IP アドレスと管理ポートを入力します。テキスト フィールドの各 Firewall のアドレスは、次のように 1 行に 1 つずつ入力してください。

10.0.5.12
10.0.5.22

Manager と Firewall がログ イベントなどの管理情報の交換に 使用する管理ポートは 8200 です。ネットワーク固有の前提条件が原因でこのポートを使用できない場合は、この IP アドレスに別のポートを付け加えると、そのポートを指定できます。

ステップ 5　[Save Changes] をクリックします。

ステップ 6　通常、クラスタに追加された Firewall には、ライセンスを設定する必要があります。Firewall のライセンス ステータスを確認するには、Web コンソールで [License Management] ページを開きます。Firewall のライセンスが必要な場合は、『*Cisco ACE Web Application Firewall Administration Guide*』で製品ライセンスを取得してアプライアンスに適用する方法を参照してください。

ACE Web Application Firewall は、クラスタのメンバーとして [Cluster Management] ページに表示されます。これで ACE Web Application Firewall Manager のポリシーをその制御下にある ACE Web Application Firewall に導入できるようになりました。

クラスタの操作の詳細については、第 16 章「Firewall クラスタの管理」を参照してください

コンソールからの安全なログアウト

セキュリティ上の理由から、ACE Web Application Firewall Manager Web コンソールでのユーザ セッションを無人状態で放置しないようにすることが重要です。Web コンソールの使用後は、コンソールからログアウトし、使用したすべてのウィンドウを閉じます。この作業を怠ると、ユーザ セッション中にブラウザがキャッシュしたページを他のユーザに見られる可能性があります。

ACE Web Application Firewall Manager から安全にログアウトするには、次の手順を実行します。

ステップ 1　[Logout] ボタンをクリックします。

ステップ 2　確認ダイアログで [OK] ボタンをクリックし、ログアウトします。

ステップ 3　コンソール セッションで使用したブラウザ ウィンドウをすべて閉じます。

セキュリティをさらに確実にするには、ACE Web Application Firewall Manager からログアウトしたあと、ブラウザのキャッシュを消去します。