ファイアウォール デバイスでのデバイス管理ポリシーの設定

[Device Admin] セクションには、ファイアウォール デバイスのデバイス管理ポリシーを設定するページが含まれています。

この章は次のトピックで構成されています。

- セキュリティ デバイスでの AAA について （1 ページ）
- バナーの設定 （12 ページ）
- [Boot Image/Configuration] の指定 （13 ページ）
- CLI プロンプトの設定 （16 ページ）
- デバイス クロックの設定 （18 ページ）
- FIPS の有効化/無効化 （20 ページ）
- Cisco Success Network の有効化 （21 ページ）
- Umbrella グローバルポリシーの設定 （22 ページ）
- デバイス クレデンシャルの設定 （23 ページ）
- マウント ポイントの管理 （26 ページ）
- IP クライアント （29 ページ）
- アプリケーション エージェント （30 ページ）

セキュリティ デバイスでの AAA について

認証、許可、アカウンティング（AAA）によって、セキュリティ アプライアンスは、ユーザがだれか（認証）、ユーザは何を実行できるか（認可）、ユーザは何を実行したか（アカウンティング）を特定できます。認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングもまた、単独で使用することも、認証および認可とともに使用することもできます。

認証、許可、アカウンティングでは、ユーザ アクセスに関して、アクセス リストだけを使用する場合よりも、さらに高度な保護および制御が実現されます。たとえば、すべての外部ユーザに DMZ ネットワーク上のサーバにある Telnet へのアクセスを許可する ACL を作成できま

すが、サーバへのユーザ アクセスを制限する場合に、これらのユーザの IP アドレスが常に認識できるわけではないときには、AAA をイネーブルにして、認証されたユーザか認可されたユーザ、またはその両方だけにセキュリティ アプライアンスを通過させることができます（Telnet サーバも認証を強制します。セキュリティ アプライアンスは非認可ユーザがサーバにアクセスしようとするのを防ぎます）。

- **認証**：認証は、ユーザー ID に基づいてアクセスを付与します。認証は、一般的にユーザ名とパスワードからなる有効なユーザ クレデンシャルを要求することによってユーザ ID を確立します。次の項目を認証するように、セキュリティ アプライアンスを設定できます。
  - Telnet、SSH、HTTPS/ASDM、またはシリアル コンソールを使用した、セキュリティ アプライアンスへの管理接続
  - **enable** コマンド。
- **認可**：認可は、認証された後のユーザーの能力を制御します。許可は、認証された個々のユーザが使用できるサービスおよびコマンドを制御します。認可をイネーブルにしなかった場合、認証が単独で、すべての認証済みユーザに対して同じサービス アクセスを提供します。

許可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な許可を設定できます。たとえば、外部ネットワーク上の任意のサーバにアクセスしようとする内部ユーザを認証してから、認可を使用して、特定のユーザがアクセスできる外部サーバを制限できます。

セキュリティ アプライアンスはユーザごとに最初の 16 個の認可要求をキャッシュします。そのため、ユーザが現在の認証セッション中に同じサービスにアクセスする場合、セキュリティ アプライアンスは要求を認可サーバに再送信しません。

- **アカウンティング**：アカウンティングはセキュリティアプライアンスを通過するトラフィックを追跡して、ユーザーアクティビティのレコードを提供します。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。アカウンティング情報には、セッションの開始および停止時間、ユーザ名、セッション中にセキュリティ アプライアンスを通過したバイト数、使用したサービス、および各セッションの持続時間が含まれます。

AAA の準備

AAA サービスは、ローカル データベースまたは 1 つ以上の AAA サーバの使用に依存します。また、ローカル データベースを AAA サーバによって提供される大多数のサービスのフォールバックとして使用することもできます。AAA を実装する前に、ローカル データベースを設定し、AAA サーバ グループおよびサーバを設定する必要があります。

ローカル データベースおよび AAA サーバの設定は、セキュリティ アプライアンスにサポートさせる AAA サービスによって異なります。AAA サーバを使用するかどうかに関係なく、管理アクセスをサポートするユーザ アカウントでローカル データベースを設定して予想外のロッ

クアウトを防いだり、また必要であれば、AAA サーバが到達不能のときにフォールバック方式を提供したりする必要があります。詳細については、ユーザアカウントの設定を参照してください。

次の表に、AAA サービスのサポートの概要を AAA サーバタイプ別およびローカルデータベース別に示します。ローカルデータベースは、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページでユーザーアカウントを設定することによって管理します（ユーザ アカウントの設定を参照）。[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA] ページを使用して、AAA サーバーグループを確立し、個々の AAA サーバーをサーバーグループに追加します。

表 *1 : AAA* サポートの要約

AAA サービス	データベース タイプ							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
認証								
VPN ユーザ	対応	対応	対応	対応	対応	対応	対応	○ 1
ファイアウォールセッション	対応	対応	対応	×	×	×	×	×
管理者	対応	対応	対応	×	×	×	×	×
許可								
VPN ユーザ	対応	対応	×	×	×	×	対応	×
ファイアウォールセッション	×	対応 2	対応	×	×	×	×	×
管理者	はい 3	×	対応	×	×	×	×	×
アカウンティング								
VPN 接続	×	対応	対応	×	×	×	×	×
ファイアウォールセッション	×	対応	対応	×	×	×	×	×
管理者	×	対応	対応	×	×	×	×	×

1 HTTP Form プロトコルは、WebVPN ユーザだけを対象にしたシングル サインオン認証をサポートします。

2 ファイアウォールセッションでは、RADIUS 認可はユーザ固有の ACL でだけサポートされ、ユーザ固有の ACL は RADIUS 認証応答で受信または指定されます。

3 ローカル コマンド認可は、権限レベルでだけサポートされます。

ローカル データベース

セキュリティ アプライアンスにより、ユーザ アカウントを入力できるローカル データベースが保持されます。ユーザアカウントには、最低でもユーザ名が含まれます。一般的には、パスワードおよび権限レベルを各ユーザ名に割り当てますが、パスワードは任意です。ローカルユーザーアカウントは、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページで管理できます（ユーザアカウントの設定を参照）。

ローカル データベースを使用してコマンド認可をイネーブルにすると、セキュリティ アプライアンスは割り当て済みのユーザ権限レベルを参照して、どのコマンドが使用可能かを判断します。デフォルトでは、すべてのコマンドに権限レベル 0 またはレベル 15 のどちらかが割り当てられます。

（注） CLIへのアクセスは許可するが、特権モードには入れないようにするユーザをローカルデータベースに追加する場合は、コマンド認可をイネーブルにする必要があります。コマンド認可がない場合、ユーザの特権レベルが 2 以上（2 がデフォルト）あると、ユーザは自身のパスワードを使用して、CLI で特権モード（およびすべてのコマンド）にアクセスできます。また、ユーザがログイン コマンドを使用できないように、コンソール アクセスに対して RADIUS または TACACS+認証を使用することや、システムのイネーブル パスワードを使用して特権モードにアクセスできるユーザを制御できるように、すべてのローカル ユーザをレベル 1 に設定することもできます。

ローカル データベースはネットワーク アクセス認可には使用できません。

ローカル データベースのユーザ アカウントによって、コンソールとイネーブル パスワードの認証、コマンド認可、および VPN 認証と認可のフォールバック サポートが提供されます。この動作は、セキュリティ アプライアンスからの予想外のロックアウトを防ぐように設計されています。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、トランスペアレント フォールバック サポートが提供されます。ユーザは、サービスを提供しているのが AAA サーバなのかローカル データベースなのかを判断できないため、AAA サーバでローカルデータベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを使用するということは、どちらのユーザ名およびパスワードを提供する必要があるのかがユーザにはわからないということになります。

マルチコンテキストモードの場合、システム実行スペースでユーザー名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する **aaa** コマンドは設定できません。

（注） VPN 機能は、マルチ モードではサポートされません。

デバイス管理用の AAA

セキュリティ アプライアンスに対する次のすべての管理接続を認証できます。

- [Telnet]
- SSH
- シリアル コンソール
- ASDM
- VPN 管理アクセス

また、イネーブル モードに入ろうとする管理者も認証できます。管理コマンドを認可できます。管理セッションおよびセッション中に発行されたコマンドのアカウンティング データをアカウンティング サーバに送信させることができます。

[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA] ページを使用すると、AAA をデバイス管理用に設定できます（セキュリティ デバイスでの AAA について（1 ページ）を参照）。

ネットワーク アクセス用の AAA

[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] ページ（ファイアウォール AAA ルールの管理を参照）を使用すると、ファイアウォールを通過するトラフィックの認証、許可、アカウンティングのルールを設定できます。作成するルールはアクセス ルールと同様ですが、定義済みのトラフィックに対して認証、許可、またはアカウンティングを行うかどうか、およびAAA サービス要求を処理するためにセキュリティ アプライアンスが使用する AAA サーバ グループを指定する点だけが異なります。

VPN アクセス用の AAA

VPN アクセス用の AAA サービスには次のものがあります。

- ユーザーを VPN グループに割り当てるためのユーザーアカウント設定。**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページで設定します（ユーザ アカウントの設定を参照）。
- 多数のユーザーアカウントまたはトンネルグループによって参照される可能性がある VPN グループポリシー。**[ユーザーアカウントVPN（Remote Access VPN）] > [RA VPNポリシー（RA VPN Policies）] > [ユーザーグループポリシー（User Group Policy）]** または **[サイト間VPN（Site to Site VPN）] > [ユーザーグループポリシー（User Group Policy）]** ページで設定します。
- トンネルグループポリシー。**[リモートアクセスVPN（Remote Access VPN）] > [RA VPN ポリシー（RA VPN Policies）] > [PIX7.0/ASAトンネルグループポリシー（PIX7.0/ASA Tunnel Group Policy）]** または **[サイト間VPN（Site to Site VPN）] > [PIX7.0/ASAトンネルグループポリシー（PIX7.0/ASA Tunnel Group Policy）]** ページで設定します。

[AAA] の [Authentication] タブの設定

[AAA] ページには 3 つのタブ付きパネルがあり、[AAA] ページに移動すると、[認証（Authentication）] パネルが表示されます。これらのオプションを使用して、デバイス コンソールへの権限付きアクセスを制御し、接続タイプによってアクセスを制限し、アクセス メッセージを定義します。

[Authorization] タブ （9 ページ）を使用して、認証されたユーザーが使用できるサービスとコマンドを制御します。

[Accounting] タブ （10 ページ）を使用して、コンソール トラフィックのトラッキングをアクティブにして、ユーザ アクティビティを記録します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- セキュリティ デバイスでの AAA について （1 ページ）
- ユーザ アカウントの設定

[Authentication] タブの使用

[Authentication] タブを使用して、セキュリティ アプライアンスへの管理者アクセスの認証をイネーブルにします。[Authentication] タブでは、AAA サーバによって認証されたときにユーザに表示されるプロンプトとメッセージを設定することもできます。

コマンドを入力する前に、デバイスによってユーザ名とパスワードの入力を求められます。認証サーバがオフラインの場合は、コンソールのログイン要求がタイムアウトになるまで待機します。そのあとで、ファイアウォールのユーザ名とイネーブル パスワードでコンソールにアクセスできます。

フィールド リファレンス

表 2 : [Authentication] タブ

要素	説明
Require AAA Authentication to allow use of privileged commands	

要素	説明
有効	ファイアウォール上で EXEC モードでのアクセスをユーザーに許可するために、AAA サーバーからの認証を要求します。このオプションは、ファイアウォール コンソールへのアクセス試行を3回まで許可します。この数を超えた場合、「アクセスが拒否されました」というメッセージが表示されます。 オンにすると、[Server Group] フィールドがイネーブルになります。
Server Group	ユーザ認証のために接続する AAA サーバの名前を入力または選択します。
Use LOCAL when server group fails	選択したサーバで障害が発生した場合に、バックアップとしてローカル データベースを使用するには、このチェックボックスをオンにします（[Server Group] を指定しないと、このオプションはイネーブルにはなりません）。
Require AAA Authentication for the following types of connections	
認証を必要とする接続を選択します。各タイプで、ファイアウォール コンソールへのアクセス試行は 3 回まで許可されます。この数を超えた場合、「アクセスが拒否されました」というメッセージが表示されます。 次の接続オプションをそれぞれ個別に選択します。 • [HTTP]：ユーザーがファイアウォール コンソールへの HTTPS 接続を開始するときに AAA 認証を必要とします。 • [シリアル（Serial）]：ユーザーがシリアルコンソールケーブルを介してファイアウォールコンソールへの接続を開始するときに AAA 認証を必要とします。 • [SSH]：ユーザーがコンソールへのセキュアシェル（SSH）接続を開始するときに AAA 認証を必要とします。 • [Telnet]：ユーザーがファイアウォールコンソールへの Telnet 接続を開始するときに AAA 認証を必要とします。 選択した各接続で、[Server Group] を指定して、ローカルデータベースをバックアップとして使用するかどうかを指定します。 • [サーバーグループ（Server Group）]：ユーザー認証のために接続する AAA サーバーの名前を入力または選択します。 • [サーバーグループに障害が発生した場合はローカルを使用（Use LOCAL when server group fails）]：選択したサーバーに障害が発生した場合に、ローカルデータベースをバックアップとして使用するには、このチェックボックスをオンにします。（[Server Group] を指定しないと、このオプションはイネーブルにはなりません）。	

要素	説明
Authentication Prompts	
Login Prompt	セキュリティ アプライアンスにログインするときにユーザに表示されるプロンプトを入力します。
Accepted Message	正常に認証されたときに表示されるメッセージを入力します。
Rejected Message	何らかの理由で認証が失敗したときに表示されるメッセージを入力します。
Rejected Message for Invalid Credentials	不明または無効なクレデンシャルを入力したために認証が失敗したときに表示されるメッセージを入力します。 FWSM 3.2 以降のデバイスでのみ使用できます。
Rejected Message for Expired Password	期限が切れたパスワードを入力したために認証が失敗したときに表示されるメッセージを入力します。 FWSM 3.2 以降のデバイスでのみ使用できます。
Maximum Local Authentication Failed Attempts	アカウントがロックされる前に、デバイスがローカルデータベースでユーザの認証を試行する回数を指定します。有効な値は 1 ～ 16 です。 ASA/PIX 7.01 以降と FWSM 3.11 以降のデバイスでのみ使用できます。
ログイン履歴	ログイン履歴レポート機能を有効にするには、このチェックボックスをオンにします。有効にすると、ログインに成功した直後に、すべての管理ログイン試行に関する情報が収集され、ASA に表示されます。これには次の情報が含まれます。 • 最後にログインが試行された日時 • 最後にログインした場所（端末または IP アドレス） • 最後に成功したログイン以降の失敗したログイン試行の回数。 • 組織が定義した期間中に発生した、成功したログイン試行の数。 （注） この機能はデフォルトでイネーブルになっています。

要素	説明
期間（Duration）（任意）	ログインイベントを保存する日数を入力します。ここで値を指定しない場合、ログイン履歴は無制限になります。 （注）　デフォルト値は 90 日です。

[Authorization] タブ

[Authorization] タブでは、ファイアウォール コマンドにアクセスするための認可を設定できます。

ナビゲーション パス

[Authorization] タブには [AAA] ページからアクセスできます。[AAA] の [Authentication] タブの設定 （6 ページ）を参照してください。

関連項目

- セキュリティ デバイスでの AAA について （1 ページ）
- [Accounting] タブ （10 ページ）

フィールド リファレンス

表 3 : [Authorization] タブ

要素	説明
Enable Authorization for Command Access Server Group Use LOCAL when server group fails	ファイアウォール コマンドにアクセスするために認可を必要とします。 認可に使用するサーバ グループを指定します。 選択したサーバ グループで障害が発生した場合に、LOCAL サーバ グループを使用します。
execシェルアクセスの承認の有効化（Enable Authorization for exec shell access） (ASA 8.0(2) 以降のみ)	選択すると、管理許可が有効になります。 管理許可を有効にしたら、認証にリモートサーバーを使用するか、ローカルデータベースを使用するかを指定します。 • [ローカルサーバー（Local Server）]：ローカルユーザーのデータベースは、入力したユーザー名と割り当てられた Service-Type および Privilege-Level 属性のソースとなります。 • [リモートサーバー（Remote Server）]：認証と許可の両方に同じサーバーが使用されます。

要素	説明
execシェルアクセスの承認の自動有効化（Auto Enable Authorization for exec shell access） （ASA 9.1(5) 以降のみ）	十分な権限を有するユーザーは、ログイン認証サーバーから特権EXECモードに直接入れます。それ以外では、ユーザはユーザ EXEC モードになります。これらの特権は、各 EXEC モードに入るために必要な Service-Type および Privilege-Level 属性で決定されます。特権 EXEC モードを開始するには、ユーザは Administrative の Service-Type 属性およびそれらに割り当てられた 1 以上の Privilege Level 属性を有している必要があります。 このオプションは、システム コンテキストではサポートされていません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はスイッチから ASASM へのセッションにも適用されます。
HTTP接続の承認の有効化（Enable Authorization for HTTP Connection） Server Group Use LOCAL when server group fails （ASA 9.4(1) 以降のみ）	選択すると、HTTP による認証が有効になります。ユーザー名の認証はデフォルトで無効になっています。 承認に使用するサーバーグループを選択します。 選択したサーバ グループで障害が発生した場合に、LOCAL サーバ グループを使用します。

[Accounting] タブ

[Accounting] タブを使用して、ファイアウォール デバイスへのアクセスおよびデバイス上のコマンドへのアクセスのアカウンティングをイネーブルにします。

ナビゲーション パス

[Accounting] タブには [AAA] ページからアクセスできます。[AAA] の [Authentication] タブの設定 （6 ページ）を参照してください。

関連項目

- セキュリティ デバイスでの AAA について （1 ページ）
- [Authorization] タブ （9 ページ）

フィールド リファレンス

表 4 : [Accounting] タブ

要素	説明
Require AAA Accounting for privileged commands	

要素	説明
有効	選択すると、コンソールによる管理アクセス用の特権モードの開始と終了を示すアカウンティング レコードの生成がイネーブルになります。
Server Group	アカウンティング レコードが送信されるサーバか、RADIUS または TACACS+ サーバのグループを指定します。
Require AAA Accounting for the following types of connections	
接続タイプ	アカウンティング レコードを生成する接続タイプを指定します。 • HTTP：HTTP で作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • シリアル：コンソールへのシリアルインターフェイス経由で確立される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • SSH：SSHで作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • Telnet：Telnet で作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。
Server Group	アカウンティング レコードが送信されるサーバか、RADIUS または TACACS+ サーバのグループを指定します。
Require Accounting for command access	
有効	選択すると、管理者/ユーザによって入力されたコマンドのアカウンティング レコードの生成がイネーブルになります。
Server Group	アカウンティング レコードが送信されるサーバか RADIUS または TACACS+ サーバのグループを選択できるドロップダウン メニューが表示されます。
特権レベル	アカウンティング レコードを生成するために、コマンドに関連付けられている必要がある最小権限レベル。デフォルトの特権レベルは 0 です。

バナーの設定

[バナー（Banner）] ページを使用して、セキュリティアプライアンスまたは共有ポリシーの [セッション（exec）（Session (exec)）]、[ログイン（Login）]、および [本日のメッセージ（motd）（Message-of-the-Day (motd)）]、および [ADSM] のバナーを指定できます。

（注） Cisco Security Manager 4.22 では、[バナー（Banner）] ページが更新され、既存のバナーに加えて、設定可能な新しい **ASDM バナー**がサポートされます。

（注） バナーでトークン $(hostname) または $(domain) を使用すると、これらはセキュリティ アプライアンスのホスト名またはドメイン名に置き換えられます。コンテキスト設定で $(system) トークンを入力した場合、コンテキストはシステム設定で設定されているバナーを使用します。

バナーテキストのスペースは保持されますが、タブは入力できません。複数行のバナーを作成するには、追加する行ごと個別のテキスト行を入力します。各行は既存のバナーの末尾に追加されます。行が空の場合は、Carriage Return（CR; 復帰）がバナーに追加されます。

メモリおよびフラッシュ メモリの制限以外に、バナーの長さに制限はありません。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

ステップ 1 バナーを設定するには、[Banner] ページにアクセスします。

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [バナー（Banner）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [バナー（Banner）]** を選択しますポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [セッション（exec）バナー（Session (exec) Banner）] フィールドに、イネーブルプロンプトを表示する前にバナーとして表示するテキストを入力します。

ステップ 3 Telnet を使用したセキュリティアプライアンスへのアクセス時に、パスワード ログイン プロンプトの前にバナーとして表示するテキストを [ログインバナー（Login Banner）] フィールドに入力します。

ステップ 4 [本日のメッセージ（motd）バナー（Message-of-the-Day (motd) Banner）] フィールドに、本日のメッセージバナーとして表示するテキストを入力します。

ステップ 5 [ASDMバナー（ASDM Banner）] フィールドで、ログイン後にシステムが ASDM バナーとして表示する必要があるテキストを指定します。このバナーでは、テキスト内の疑問符はサポートも許可もされていませ

ん。いずれかの共有ポリシーに疑問符が含まれている場合でも、Cisco Security Manager ではアクティビティ検証エラーが表示されます。

ステップ 6 バナーを置換するには、該当するボックスの内容を変更します。

ステップ 7 バナーを削除するには、該当するボックスの内容をクリアします。

[Boot Image/Configuration] の指定

[Boot Image/Configuration] ページを使用して、起動時にセキュリティ アプライアンスが使用する設定ファイルを指定します。Adaptive Security Device Manager（ASDM）の設定ファイルへのパスも指定できます。

ブートイメージの場所を指定しない場合、内部フラッシュ メモリ上にある最初の有効なイメージがシステムの起動に選択されます。

（注） このページは ASA および PIX 7.0 以降のデバイスでのみ使用できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブートイメージ/設定（Boot Image/Configuration）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [ブートイメージ/設定（Boot Image/Configuration）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *5 : [Boot Image/Configuration]* ページ

要素	説明
Boot Config Location	システムがロードされるときに使用する設定ファイルのパスと名前を入力します。ASA では、次のいずれかの構文構成子を使用できます。 • **disk0:**/[*path/*]*filename* 値「disk0」は内部フラッシュカードを示します。「**disk0**」の代わりに「**flash**」を使用することもできます。これらはエイリアス関係にあります。 • **flash:**/[*path/*]*filename* • **disk1:**/[*path/*]*filename* 値「disk1」は外部フラッシュカードを示します。 PIX デバイスでは、次のような「flash」構文のみを使用できます。 • **flash:**/[*path/*]*filename*
ASDM Image Location	ASDM セッションの開始時に使用される ASDM ソフトウェア イメージの場所と名前（ASDM を使用して ASA と PIX の両方のデバイスをモニタできます）。 PIX デバイスでは、ブート設定のロケーションと同様、「flash」構文のみを使用できます。 ASA では、ブート設定のロケーションと同様、「disk0」、「flash」、「disk1」の構成子を使用できます。さらに、次のようにして TFTP サーバ上のイメージ ファイルを指定できます。 • **tftp:**//[*user* [*:password*]@]*server* [*:port*]/[*path/*]*filename*

要素	説明
[Boot Images] テーブル	このテーブルには、定義した代替の設定ファイルがすべて一覧で表示されます。設定ファイルは 4 個まで定義できます。[Boot Config Location] フィールドでプライマリ ファイルを指定しなかった場合や指定したファイルが使用できない場合、このリストで最初に使用できるイメージが使用されます。 これは Security Manager の標準のテーブルです。テーブルの使用で説明されているとおり、テーブルの下の上矢印ボタン、下矢印ボタン、[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] と [Edit Row] のボタンでは、[Images] ダイアログボックス （15 ページ）を開きます。これは代替の設定ファイルへのパスを追加および編集するために使用します。 （注） ASA では、このテーブルの最初のエントリだけが TFTP サーバ上の ASDM 設定ファイルを参照できます。このデバイスが TFTP サーバに到達できない場合、リストにある次のイメージ ファイルをロードしようとします。

[Images] ダイアログボックス

[Images] ダイアログボックスを使用して、[Boot Image/Configuration] ページにある [Boot Images] テーブルの設定ファイルのエントリを追加または編集します。

ナビゲーション パス

[Images] ダイアログボックスには、[Boot Image/Configuration] ページからアクセスできます。詳細については、 [Boot Image/Configuration] の指定 （13 ページ）を参照してください。

フィールド リファレンス

[Images] ダイアログボックスにはフィールドが 1 つあります。このフィールドは、次のように、ブート イメージまたは設定ファイルへのパスを定義するために使用します。

表 *6 : [Images]* ダイアログボックス

要素	説明
Image File	順番に並べられた [Boot Images] リストに追加する設定ファイルのパスと名前を入力します。 PIX デバイスでは、次のような「flash」構文のみを使用できます。 • **flash:**/[*path/*]*filename* ASA では、次のいずれかの構文構成子を使用できます。 • **disk0:**/[*path/*]*filename* 値「disk0」は内部フラッシュカードを示します。「**disk0**」の代わりに「**flash**」を使用することもできます。これらはエイリアス関係にあります。 • **flash:**/[*path/*]*filename* • **disk1:**/[*path/*]*filename* 値「disk1」は外部フラッシュカードを示します。 さらに、ASA では次のようにして TFTP サーバ上の ASDM イメージ ファイルを指定できます。 • **tftp:**//[*user* [*:password*]@]*server* [*:port*]/[*path/*]*filename* 指定できる TFTP の場所は 1 箇所だけです。また、この場所は [Boot Image/Configuration] ページにある [Boot Images] テーブルの一番上に表示されている必要があります。

CLI プロンプトの設定

[CLIプロンプト（CLI Prompt）] ページを使用して、CLI セッション中に ASA 7.2(1) 以降のデバイスによって使用されるプロンプトをカスタマイズできます。デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

（注） 使用可能な属性は、ASA のバージョンによって異なります。

cluster-unit （ASA 9.1.1以降のみ）	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。

domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
management-mode （ASA 9.2.1 以降のみ）	管理モードを表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。
state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state に対して次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。この状況は、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 グループ化の場合、state に対して次の値が表示されます。 • コントロール • データ たとえば、プロンプト ciscoasa/cl2/slave では、ホスト名は ciscoasa、ユニット名は cl2、状態名は data です。

ステップ 1 次のいずれかを実行して、[CLIプロンプト（CLI Prompt）] ページにアクセスします。

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [CLIプロンプト（CLI Prompt）]** を選択します。

（注） マルチコンテキストモードのデバイスの場合、[CLIプロンプト（CLI Prompt）] ページはシステムコンテキストでのみ使用できます。管理コンテキストでは、[CLIプロンプト（CLI Prompt）] ページは使用できません。

- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [CLIプロンプト（CLI Prompt）]** を選択します。ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 CLI プロンプトをカスタマイズするには、次の操作を実行します。

- プロンプトに属性を追加する場合は、[使用可能なメンバー（Available Members）] リストで属性を選択して、[>>] をクリックします。属性が [使用可能なメンバー（Available Members）] リストから [選択済みのメンバー（Selected Members）] リストに移動します。

プロンプトには複数の属性を追加できます。[選択済みのメンバー（Selected Members）] リストに属性が追加された順序によって、CLI プロンプトに表示される順序が決まります。

（注） ASA 9.1.1 以降では、CLI プロンプトに最大 6 個の属性を設定できます。以前の ASA バージョンでは、最大 5 個の属性のみを設定できます。

- プロンプトから属性を削除する場合は、[選択済みのメンバー（Selected Members）] リストで属性をクリックし、[<<] をクリックします。属性が [選択済みのメンバー（Selected Members）] リストから [使用可能なメンバー（Available Members）] リストに移動します。

デバイス クロックの設定

[Clock] ページを使用して、選択したデバイスに日時を設定します。

（注） このページは Catalyst 6500 サービス モジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

NTP サーバを使用してダイナミックに時刻を設定するには、[NTP] ページを参照してください。NTP サーバから取得された時刻は、[Clock] ページで手動で設定された時刻を上書きします。

（注） マルチコンテキスト モードの場合、時刻はシステム コンテキストでのみ設定します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *7 : [Clock]* ページ

要素	説明
Device Time Zone	デバイスのタイム ゾーンを選択します。これらのオプションは、Greenwich Mean Time（GMT; グリニッジ標準時）との時差に従って表されます。 （注） デバイスでタイム ゾーンを変更すると、取り付けられているいずれかの Security Services Module（SSM; セキュリティ サービス モジュール）への接続がドロップすることがあります。
Daylight Savings Time (Summer Time)	夏時間のオプションを選択します。また、必要に応じて、夏時間を適用するタイミングと方法を指定します。 [なし（None）]：夏時間を自動的に修正しない場合は、このオプションを選択します。 [日付により設定（Set by Date）]：特定の年の夏時間の開始日時と終了日時を指定する場合は、このオプションを選択します。このオプションを使用する場合、日付を毎年リセットする必要があります。 [日により設定（Set by Day）]：夏時間を開始および終了する月、週、日を使用して、夏時間の開始日および終了日を指定する場合、このオプションを選択します。このオプションを使用すると、日付の範囲が自動更新されるように設定できるため、毎年変更する必要はありません。
Set by Date [Start] セクションと [End] セクションには、次の 3 つのパラメータが表示されます。2 つのセットを使用して、夏時間を開始する日時と終了する日時を定義します。	
日付	夏時間を開始する日時と終了する日付を MMM DD YYYY 形式（Jul 15 2011 など）で入力します。カレンダーアイコンをクリックして、ポップアップ カレンダーから日付を選択することもできます。
時間（Hour）	夏時間の開始時間（時間）または終了時間（時間）を 00 ～ 23 から選択します。
毎分	夏時間の開始時間（分）または終了時間（分）を 00 ～ 59 から選択します。
Set by Day	

要素	説明
Specify Recurring Time	このチェックボックスをオンにすると、[Start] と [End] のパラメータがイネーブルになります。これらのパラメータは、夏時間の開始時間と終了時間の日付を毎年変更する必要がないように、自動更新するために使用します。
[Start] セクションと [End] セクションには、次の 5 つのパラメータが表示されます。2 つのセットを使用して、夏時間を開始する日時と終了する日時を定義します。	
月	夏時間が開始または終了する月を選択します。
週（Week）	夏時間が開始または終了する週を選択します。週に対応する数値を 1 ～ 4 の範囲で選択できます。または、[最初（first）] または [最後（last）] を選択して、月の最初の週または最後の週を指定できます。たとえば、日付が第 5 週の途中にあたる場合は、[last] を指定します。
Weekday	夏時間が開始または終了する曜日を選択します。
時間（Hour）	夏時間の開始時間（時間）または終了時間（時間）を 0 ～ 23 から選択します。
毎分	夏時間の開始時間（分）または終了時間（分）を 00 ～ 59 から選択します。

FIPS の有効化/無効化

4.15 以降、Cisco Security Manager には、ASA デバイスで連邦情報処理標準（FIPS）モードを有効化または無効化するオプションが用意されています。FOM で FIPS モードを有効にすると、Cisco SSL バージョンに実装されているレガシーメソッドの代わりに、FOM に実装されている FIPS 140-2 標準準拠の暗号化メソッドがシグネチャおよび検証の目的で使用されます。この機能は、ASA 9.8.2 以降のデバイスでのみサポートされています。

（注） デバイスで FIPS モードを設定するには、デバイスを手動で再起動する必要があります。

FIPS を有効にする前に、ASA で次の内容が設定されていることを確認してください。

1. DH グループが 14 に設定されている、または ECDH グループが 19、20、21 に設定されている。
2. デバイス ID 証明書のキータイプが RSA に設定されていて、キーサイズが 2048 以上である。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [FIPS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [FIPS]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 8 : [FIPS] ページ

要素	説明
FIPS	チェックボックスをオンにして、デバイスでFIPSを有効にします。このオプションは、ASA 9.8.2 以降でのみ使用できます。 （注） 設定を有効にするには、FIPS を有効または無効にした後で、デバイスを再起動する必要があります。

Cisco Success Network の有効化

バージョン 4.20 以降、Cisco Security Manager には、カスタマー サクセス ネットワークを有効にするオプションが用意されています。これにより、ASAデバイスで有効になっている機能を利用し、Smart Call Home（SCH）の同じメカニズムを利用できます。SCHが収集するデータはほとんどが古く、SCH のリリース以降に追加された機能は正確なステータスを報告しないため、カスタマー サクセス ネットワークが導入されています。この機能は、ASA 9.13.1 以降のデバイスでサポートされています。

（注） 機能は、設定済みで、使用する準備ができている場合にのみ、「有効になっている」と見なされる必要があります。機能を設定しても動作しない場合、その機能を「有効になっている」と見なすことはできません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [カスタマー サクセス ネットワーク（Customer Success Network）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [カスタマー サクセス

ネットワーク ポリシー（Customer Success Network Policy）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *9 : [カスタマー サクセス ネットワーク（Customer Success Network）] ページ*

要素	説明
[カスタマーサクセス ネットワーク（Customer Success Network）]	[カスタマー サクセス ネットワークの有効化（Enable Customer Success Network）] チェックボックスをオンにして、デバイスで有効にします。このオプションは、ASA 9.13.1 以降のデバイスでのみ使用できます。

Umbrella グローバルポリシーの設定

バージョン 4.18 以降、Cisco Security Manager は Umbrella グローバルポリシーの設定をサポートしています。Cisco Umbrella Branch は、最初に DNS トラフィックを検査し、次に不審な HTTP/HTTPS トラフィックを検査するクラウドベースのセキュリティサービスです。Cisco Umbrella コネクタは、DNS パケットをインターセプトし、関心を引く DNS クエリを解決のために Cisco Umbrella リゾルバにリダイレクトします。DNS 応答を受信すると、その応答をホストに転送します。この機能は、ASA 9.10.1 以降のデバイスでのみサポートされています。

Cisco Umbrella サービスを設定したら、Cisco Umbrella DNS ポリシーマップも設定されていることを確認します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [Cisco Umbrella（Umbrella）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [Cisco Umbrella（Umbrella）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *10 : [Cisco Umbrella（Umbrella）] ページ*

要素	説明
Umbrella	選択したデバイス（ASA 9.10.1 以降）のグローバル Cisco Umbrella 設定を適用するには、チェックボックスをオンにします。

要素	説明
トークン	Cisco Umbrella サーバーへの登録時の ASA デバイスのトークン値。この値が 64 文字未満の場合、Cisco Security Manager からエラーメッセージがスローされます。
公開キー（3Public Key）	Cisco Umbrella サーバーへの登録時の ASA デバイスの公開キー値。この値は 64 桁の 16 進数で 80 文字未満である必要があります。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[EDNS フロータイムアウト（EDNS Flow Timeout）]	設定されている EDNS タイムアウト値。EDNS フローの Cisco Umbrella タイムアウトは、<0:0:0> ～ <1193:0:0> である必要があります。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[IPv4 リゾルバ（IPv4 Resolver）]	DNS 要求を解決するために使用するデフォルト以外の Cisco Umbrella DNS サーバーの IPv4 アドレス。有効な IPv4 であることを確認してください。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[IPv6 リゾルバ（IPv6 Resolver）]	DNS 要求を解決するために使用するデフォルト以外の Cisco Umbrella DNS サーバーの IPv6 アドレス。有効な IPv6 であることを確認してください。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[正規表現クラス（Regular Expression Class）]	正規表現クラスを使用して、Cisco Umbrella をバイパスする必要があるローカルドメインバイパスを照合します。
正規表現	正規表現を使用して、Cisco Umbrella をバイパスする必要があるローカルドメインバイパスを照合します。

デバイス クレデンシャルの設定

[Credentials] ページを使用して、このデバイスに接続するときに Security Manager が使用するユーザ クレデンシャルを指定します。デバイスで [Enable Password] および [Telnet/SSH Password] を変更することもできます。

このユーザ名とパスワードの組み合わせを使用すると、HTTP、HTTPS、Telnet または SSH セッションを使用してセキュリティ アプライアンスに接続する場合に、EXEC モードでデバイスにログインできます。Telnet セッションおよび SSH セッション専用に個別のパスワードを指定することもできます（さらに、[Device Properties] ウィンドウの[Device Credentials] ページでは、HTTP/HTTPS 接続用の個別のクレデンシャルを定義できます）。

[Enable Password] を使用すると、ログイン後に特権 EXEC モードにアクセスできます。

ヒント　このページの [Username]、[Password]、[Enable Password] は、[Device Properties] ウィンドウの [Credentials] 設定にリンクされています。これらのパラメータを更新して、その変更をデバイスに展開すると、Security Manager は [Device Properties] に定義されている既存のクレデンシャルを使用してデバイスにログインし、変更を展開します。変更が正常に展開されると、これらの設定に一致するように [Device Properties] のクレデンシャルが更新されます。[Device Properties] の [Credentials] の詳細については、[Device Credentials] ページを参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クレデンシャル（Credentials）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [クレデンシャル（Credentials）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

危険　各デバイスには複数のユーザ アカウントが存在できるため、共有のクレデンシャル ポリシーを複数のデバイスに適用すると、各デバイスの [Enable Password] だけが更新されます。共有ポリシーに指定されている [Username] と [Password]（または [Telnet/SSH Password]）は適用されません。AAA や TACACS+ などの外部認証が設定されていない限り、PIX/ASA/FWSM デバイスには [Enable Password] だけでもアクセスできます。外部認証が設定されている場合は [Enable Password] だけでは不十分です。この場合、外部認証を使用する各デバイスで [Username]、[Password]、[Enable Password] を手動で更新する必要があります。

関連項目

- ユーザ アカウントの設定

フィールド リファレンス

表 *11 : [Credentials]* ページ

要素	説明
[ユーザー名（Username）]	デバイスにログインするためのユーザ名を入力します。名前は 4 文字以上である必要があります。最大は 64 文字です。エントリは、大文字と小文字が区別されます。

要素	説明
パスワード 確認（Confirm）	指定した [Username] でデバイス（ユーザ EXEC モード）にログインするためのパスワードを指定します。このパスワードは 3 文字以上である必要があります。最大は 32 文字です。エントリは、大文字と小文字が区別されます。 [Confirm] フィールドにユーザ パスワードもう一度入力します。 （注） 8 文字以上の長さのパスワードを推奨します。
特権レベル	このユーザの特権レベルを選択します。使用可能な値は 1 ～ 15 です。レベル 1 では、EXEC モードのアクセスのみが許可されます。ログインのデフォルト レベルである 15 では、特権 EXEC モードのアクセスが許可されます。つまり、イネーブル モードにアクセスできます。他のレベルは、明示的にデバイスで定義する必要があります。
イネーブル パスワード	
[暗号化されたパスワード（Password as encrypted）]	[プレーンテキスト（Plain Text）] または [暗号化（Encrypted）] を選択します。
[パスワード暗号化タイプ（Password encrypt type）]	[MD5] または [PBKDF2] を選択します。
パスワードを有効にする（Enable Password） 確認（Confirm）	[パスワードの有効化（Enable Password）] を指定すると、このユーザーはログイン後に特権 EXEC モードにアクセスできます。入力は大文字と小文字が区別されます。 [Confirm] フィールドにイネーブル パスワードをもう一度入力します。 （注） プレーンテキストパスワードの場合： • MD5 パスワードの長さは 3 ～ 32 文字にする必要があります。 • PBKDF2 パスワードの長さは、33 ～ 127 文字にする必要があります。展開の失敗を避けるために、PBKDF2 パスワードに正しい `sha` キー値が使用されていることを確認します。 （注） イネーブル アクセスのユーザ認証を設定する場合は、ユーザごとに専用のパスワードを指定します。このパスワードは使用しません）。詳細については、[AAA] の [Authentication] タブの設定 （6 ページ）を参照してください。

要素	説明
Telnet/SSH パスワード 確認（Confirm）	Telnet セッションまたは SSH セッション経由でデバイスに接続するときに、EXEC モードにアクセスするためのパスワードを指定できます。このパスワードは 3 文字以上である必要があります。最大は 32 文字です。エントリは、大文字と小文字が区別されます。 [Confirm] フィールドに Telnet または SSH のパスワードもう一度入力します。 （注） Telnet または SSH アクセスのユーザ認証を設定する場合は、ユーザごとに専用のパスワードを指定します。このパスワードは使用しません。詳細については、[AAA] の [Authentication] タブの設定 （6 ページ）を参照してください。

マウント ポイントの管理

[マウントポイント（Mount Points）] ページを使用して、Common Internet File System（CIFS）または File Transfer Protocol（FTP）ファイルシステムがセキュリティアプライアンスにアクセスできるようにします。

（注） FTP タイプのマウントポイントを作成する場合、FTP サーバーには UNIX のディレクトリ リストスタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

[ファイルマウントポイント設定（File Mount Point Configuration）] テーブルには、設定されたマウントポイントが一覧表示されます。[ファイルマウントポイント設定（File Mount Point Configuration）] テーブルは、Security Manager の標準のテーブルです。このテーブルには [行の追加（Add Row）]、[行の編集（Edit Row）]、[行の削除（Delete Row）] ボタンがあります（テーブルの使用に説明されているとおり、これらは標準のボタンです）。[行の追加（Add Row）] ボタンでは [DHCP リレーエージェント設定の追加（Add DHCP Relay Agent Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] では [DHCP リレーエージェント設定の編集（Edit DHCP Relay Agent Configuration）] ダイアログボックスが開きます。タイトルを除き、この 2 つのダイアログボックスは同じです。詳細については、[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス （27 ページ）を参照してください。

（注） この機能は ASA 8.0(2)+ のデバイスでのみ使用できます。マウントポイントはルータモードでのみサポートされます。8.0(2) と 9.x の間の ASA バージョンの場合、マウントポイントはマルチコンテキストモードではサポートされません。マウントポイントは、マルチコンテキスト、ルーテッドモードの ASA 9.x+ デバイスの管理コンテキストでサポートされます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [マウントポイント（Mount Points）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [マウントポイント（Mount Points）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス

[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックスを使用して、[マウントポイント（Mount Points）] ページの [ファイルマウントポイント設定（File Mount Point Configuration）] テーブルでマウントポイントエントリを追加または編集します。マウントポイントを使用して、Common Internet File System（CIFS）または File Transfer Protocol（FTP）ファイルシステムがセキュリティアプライアンスにアクセスできるようにします。

ナビゲーション パス

[マウントポイント（Mount Points）] ページから [マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックスにアクセスできます。詳細については、マウント ポイントの管理 （26 ページ）を参照してください。

フィールド リファレンス

表 *12 : [マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス*

要素	説明
[マウントポイントの有効化（Enable Mount Point）]	ファイルシステムをマウント対象または非マウント対象（使用可能または使用不能）に設定します。

要素	説明
接続タイプ	マウントするファイルシステムのタイプを選択します。 • [CIFS]：マウント対象のファイルシステムとしてCIFSを指定します。CIFSは、CIFS共有ディレクトリにボリュームマウント機能を提供するファイルシステムです。 • [FTP]：マウント対象のファイルシステムとしてFTPを指定します。FTPはLinuxカーネルモジュールであり、仮想ファイルシステム（VFS）をFTPボリュームマウント機能で強化し、FTP共有ディレクトリをマウントできるようにしたものです。 （注） FTPタイプのマウントポイントを作成する場合、FTPサーバーにはUNIXのディレクトリ リストスタイルが必要です。Microsoft FTPサーバーには、デフォルトでMS-DOSディレクトリ リスト スタイルがあります。
[マウントポイント名（Mount Point Name）]	マウントの名前を指定します。マウントポイント名は、セキュリティアプライアンスにすでにマウントされているファイルシステムを他のCLIコマンドが参照するときに使用されます。マウントポイント名は31文字以下にする必要があります。
Server Name/IP Address	CIFSまたはFTPファイルシステムサーバーの定義済みの名前（またはドット付き10進表記のIPアドレス）を指定します。
ユーザー名	ファイル システムのマウントが認可されているユーザ名を指定します。
パスワード 確認（Confirm）	ファイル システムのマウントのための認可されたパスワードを指定します。
パスワードの暗号化	選択すると、指定されたパスワードが暗号化された形式であることが示されます。
共有名 （CIFSのみ）	サーバ内のファイルデータにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
ドメイン名 （CIFSのみ）	CIFSファイルシステムの場合のみ使用します。この引数にはWindows NTドメイン名を指定します。最大63文字が許可されます。
[モード（Mode）] （FTPのみ）	FTP転送モードをアクティブまたはパッシブとして識別します。

要素	説明
パス（Path） （FTP のみ）	指定された FTP ファイル システム サーバーへのディレクトリ パス名を指定します。疑問符とスペースはパス名に使用できず、表示されません。

IP クライアント

[IPクライアント（IP Client）] ページには、インターフェイス名と IP バージョンが一覧表示されます。設定済みの IP クライアントを使用して、Firepower 2100 シリーズデバイスでの統合ルーティングおよびブリッジングサポートを使用できます。[IPクライアント（IP Client）] ページには、エントリを追加、編集、および削除するための標準オプションがあります。

（注） この機能は、ASA 9.8.2+ Firepower 2100 シリーズのシングル コンテキスト デバイスでのみ使用できます。IP クライアントのマルチコンテキストサポートはありません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [IPクライアント（IP Client）] を選択します。

（注） メニューは、Firepower 2100 シリーズデバイスでのみ表示されます。

- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [IPクライアント（IP Client）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックス

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックスを使用して、[IPクライアント（ IP Client）] ページの [IPクライアント（IP Client）] テーブルの IP クライアントエントリを追加または編集します。IP クライアント設定を使用して、Firepower 2100 シリーズ デバイスで統合ルーティングとブリッジングをサポートします。

ナビゲーション パス

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックスには、[IPクライアント（IP Client）]ページからアクセスできます。詳細については、IP クライアント （29 ページ）を参照してください。

フィールド リファレンス

表 *13 : [IP*クライアントの追加（*Add IP Client***）*]/[IP*クライアントの編集（***Edit IP Client***）*]* ダイアログボックス**

要素	説明
IPバージョン	デバイスの IP アドレス。アドレスは IPv4 または IPv6 アドレスです。
インターフェイス	Firepower 2100 シリーズ デバイスに関連するインターフェイスを選択します。

設定のプレビューページには、IPv6 インターフェイスに IPv6 サフィックスが付いた IP クライアント設定が表示されます。IPv4 インターフェースの場合、インターフェース名のみが表示されます。

アプリケーション エージェント

[アプリケーションエージェント（App Agent）]ページを使用して、アプリケーションエージェント設定を行います。ハートビート間隔とリトライ回数を指定できます。

（注） App-Agent は、Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズデバイスでのみ使用できます。Cisco Security Manager では、Firepower 2100 シリーズデバイスの App-Agent は 9.8.2+ 以降でサポートされています。 Firepower 4000 シリーズおよび Firepower 9000 シリーズデバイスの App-Agent は、9.6.2+ 以降でサポートされています。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アプリケーションエージェント（App Agent）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [アプリケーションエージェント（App Agent）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *14 : [*アプリケーションエージェント（*App Agent***）*]* ページ**

要素	説明
インターバル	アプリケーション エージェントのハートビート間隔を入力します。ASA 9.6.2 から ASA 9.8.1 では、App-Agent ハートビート値は 300 ～ 6000 ミリ秒にすることができます。 ASA 9.8.2+ デバイスの場合、App-Agent ハートビート間隔の値は 100 ～ 6000 ミリ秒です。 （注） 100 の倍数の値を入力しない場合、Cisco Security Manager はエラーメッセージを表示します。
再試行回数（Retry Count）	3 ～ 10 で再試行回数を入力します。
保存	クリックして、設定を保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。