# ロールベース アクセス コントロールの保護

ユーザーロールには、そのユーザーがシステムで実行できることを定義する特権が割り当てられます。システムには、次のユーザ ロールが用意されています。

**管理者**

システム全体に対する完全な読み取りと書き込みのアクセス権。デフォルトの admin アカウントは、デフォルトでこのロールが割り当てられ、変更はできません。

**読み取り専用**

システム設定に対する読み取り専用アクセス権。システム状態を変更する権限はありません。

**操作**

NTP の設定、Smart Licensing のための Smart Call Home の設定、システム ログ（syslog サーバとエラーを含む）に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

**AAA アドミニストレータ**

ユーザ、ロール、および AAA 設定に対する読み取りと書き込みのアクセス権。システムの残りの部分に対する読み取りアクセス権。

FXOS Chassis Manager Web インターフェイスまたは FXOS CLI を使用して、システムの各ユーザーアカウントに次の設定を構成できます。

- [ユーザーロール（User Role）]：ユーザーアカウントに割り当てる権限を表すロール。

  すべてのユーザはデフォルトでは読み取り専用ロールが割り当てられます。このロールは選択解除できません。複数のロールを割り当てるには、**Ctrl** を押したまま、目的のロールをクリックします。

- アカウントの有効期限日

- [アカウントステータス（Account Status）]：ステータスが [アクティブ（Active）] に設定されている場合、ユーザーはログイン ID とパスワードを使用して Firepower Chassis Manager と FXOS CLI にログインできます。

ローカルで認証されたアカウントで最大限のセキュリティを確保するには、暗号化されたセッションに SSH を構成します。



# パスワード管理

パスワードはリソースまたはデバイスへのアクセスを制御し、管理者は要求を認証するためのパスワードを定義します。FXOS がリソースまたはデバイスへのアクセス要求を受信すると、要求はパスワードと ID の検証のチャレンジが行われ、結果に基づいてアクセスが許可、拒否、または制限されます。セキュリティのベストプラクティスでは、パスワードは LDAP、TACACS+、または RADIUS 認証サーバーで管理する必要があります。ただし、LDAP、TACACS+、または RADIUS サービスが失敗した場合は、アクセス用にローカルに設定されたパスワードが引き続き必要です。デバイスは、NTP キーや SNMP コミュニティストリングなど、他のパスワード情報をその設定内に持つこともできます。

# ローカル認証されたユーザーアカウントの強化

個々の内部ユーザーロールを設定する場合、管理者アカウントユーザーは次の設定を使用して、Web インターフェイスのログインメカニズムを利用した攻撃に対してシステムを強化することができます。

- ロックアウト前にユーザーに許可されるログイン試行の最大回数を設定します（set max-login-attempts）。この回数を超えると、指定した時間だけ Firepower 4100/9300 シャーシからロックアウトされることになります
- ログイン試行の最高回数を超えた後、ユーザーがシステムからロックアウトされる時間を指定します（set user-account-unlock-time）
- パスワード長の最小値を適用します（set min-password-length）
- ローカル認証されたユーザーが、新しく作成したパスワードを変更する前に待機する最小時間数を指定します（set no-change-interval）
- ローカルユーザーアカウントが有効な日数を設定します（set expiration）
- 強力なパスワードを要求します（set enforce-strong-password yes）
- ユーザーが必要とするアクセスのタイプにのみ適したユーザーアクセス権限を割り当てます（create role）

# リモート認証されたユーザーアカウントの強化

リモート認証されたユーザ アカウントとは、LDAP、RADIUS、または TACACS+ を通じて認証されたユーザ アカウントのことです。リモート認証では、最大 16 の TACACS+ サーバー、16 の RADIUS サーバー、および 16 の LDAP プロバイダー（合計 48 のプロバイダー）が許可されます。

AAA は、コンピュータ リソースへのアクセスを制御し、ポリシーを使用し、使用率を評価することでサービス課金に必要な情報を提供する、一連のサービスです。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

ユーザーがローカルユーザーアカウントとリモートユーザーアカウントを同時に保持する場合、ローカルユーザーアカウントで定義されたロールはリモートユーザーアカウントに保持された値を上書きします。

TACACS+は、FXOS シャーシがリモート AAA サーバーに対して管理ユーザーを認証するために使用できる認証プロトコルです。これらの管理ユーザーは、SSH、HTTPS、Telnet、または HTTP を介して FXOS シャーシにアクセスできます。FXOS シャーシにアクセスするときは、最大限のセキュリティのために SSH をお勧めします。多数の認証方法により、セキュリティが強化されています。

TACACS+認証（より一般的にはAAA認証）では、ネットワーク管理者ごとに個別のユーザーアカウントを使用できます。単一の共有パスワードに依存しない場合、ネットワークのセキュリティが向上し、責任が強化されます。

RADIUS は、TACACS+ と似た目的のプロトコルですが、ネットワーク経由で送信されるパスワードのみを暗号化します。一方、TACACS+ は、ユーザー名とパスワードの両方を含む TCP ペイロード全体を暗号化します。このため、AAA サーバーで TACACS+ がサポートされている場合は、RADIUS ではなく TACACS+ を使用することをお勧めします。

LDAP は、Microsoft Active Directory などのディレクトリサービスにアクセスするためのクライアント サーバー プロトコルです。LDAP では、クライアントとサーバー間のセキュリティは必要ありません。ただし、SSL を使用することにより、LDAP はクライアントとサーバー間のユーザーセッションを暗号化できます。これにより、ネットワーク経由で LDAP トランザクションにより転送されるすべての情報が安全に保たれます。このため、TLS よりも LDAP を使用することを強くお勧めします。

FXOS シャーシで RADIUS、TACAS+、および LDAP を設定する方法の詳細と詳細な手順については、『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』の「Platform Settings」の章の「Configuring AAA」セクションを参照してください。

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。