



アクセスコントロールルール:レールムとユーザ

次の項では、ネットワークでユーザ トラフィックを制御する方法について説明します。

- [レールム、ユーザ、ユーザ グループ、および ISE 属性のアクセスコントロールルール条件 \(9-1 ページ\)](#)
- [ユーザ アクセスコントロールルールに関するトラブルシューティング \(9-2 ページ\)](#)
- [アクセスコントロールルールへのレールム、ユーザ、またはユーザ グループ条件の追加 \(9-3 ページ\)](#)
- [アクセスコントロールルールへの ISE 属性条件の追加 \(9-3 ページ\)](#)

レールム、ユーザ、ユーザ グループ、および ISE 属性のアクセスコントロールルール条件

ライセンス:Control

ユーザ制御を実行する(レールム全体、個々のユーザ、ユーザ グループ、または ISE 属性に基づいてアクセスコントロールルール条件を作成する)前に、次のことを行う必要があります。

- モニタ対象の Microsoft Active Directory または LDAP サーバのそれぞれに対し、レールムを設定する。レールムに対してユーザのダウンロードを有効にすると、FirePOWER Management Center は定期的および自動的に、新規に報告されたかすでに報告済みの権限のあるユーザおよびユーザ グループのメタデータをダウンロードするようサーバに照会します。
- レールムを認証方式に関連付けるために、アイデンティティ ポリシーを作成する。
- 1 つ以上のユーザエージェントまたは ISE デバイス、あるいはキャプティブ ポータルを設定する。ISE 属性の条件を使用するには、ISE を設定する必要があります。

ユーザエージェント、ISE およびキャプティブ ポータルは、アクセスコントロールルール条件でユーザ制御に使用できる、権限のあるユーザ データを収集します。アイデンティティ ソースは、指定したユーザがホストにログイン、ログアウトしたり、LDAP または AD クレデンシャルを使用して認証する際にモニタします。



(注) ユーザエージェントまたは ISE デバイスのモニタ対象に多くのユーザグループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、FirePOWER Management Center のユーザ制限が原因で、システムがグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レールム、ユーザ、またはユーザ グループ条件をもつアクセスコントロールルールが想定どおりに適用されない可能性があります。

1つのユーザ条件で、最大50のレلم、ユーザおよびグループを[選択されたユーザ(Selected Users)]に追加できます。ユーザグループを持つ条件は、そのグループのメンバー(サブグループのメンバーを含む)のいずれかが送信元/宛先であるトラフィックを照合します。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

ユーザグループを含めると、自動的に、すべてのセカンダリグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセスコントロールルールでセカンダリグループを使用する場合は、明示的にセカンダリグループを含める必要があります。



(注)

アクセスコントロールルールがネットワークトラフィックを評価する前に、ハードウェアベースの高速パスルール、セキュリティインテリジェンスベースのトラフィックフィルタリング、SSLインスペクション、ユーザ識別、および一部のデコードと前処理が行われます。

ユーザアクセスコントロールルールに関するトラブルシューティング

ライセンス:Control

ユーザアクセスコントロールルールの予期しない動作に気付いたら、ルール、アイデンティティソース、またはレلمの設定を調整することを検討してください。

レلم、ユーザ、またはユーザグループに対するアクセスコントロールルールが適用されない

ユーザエージェントまたはISEデバイスのモニタ対象に多くのユーザグループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、FirePOWER Management Centerのユーザ制限が原因で、システムがユーザレコードをドロップすることがあります。その結果、レلمまたはユーザ条件を使用するアクセスコントロールルールが想定どおりに適用されない可能性があります。

ユーザグループまたはユーザグループ内のユーザに対するアクセスコントロールルールが想定どおりに適用されない

ユーザグループ条件を含むアクセスコントロールルールを設定する場合は、LDAPまたはActive Directoryサーバでユーザグループを設定する必要があります。サーバが基本的なオブジェクト階層でユーザを整理している場合、FirePOWER Management Centerはユーザグループ制御を実行できません。

セカンダリグループ内のユーザに対するアクセスコントロールルールが想定どおりに適用されない

Active Directoryサーバのセカンダリグループのメンバーであるユーザを含めるか除外するユーザグループ条件を含むアクセスコントロールルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directoryサーバはセカンダリグループから報告するユーザの数を制限します。この制限は、セカンダリグループ内のすべてのユーザがFirePOWER Management Centerに報告され、ユーザ条件を含むアクセスコントロールルールでの使用に適するようにカスタマイズする必要があります。

アクセスコントロールルールが、初めて表示されたユーザに一致していない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバから情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するアクセスコントロールルールによって処理されません。代わりに、ユーザセッションは、一致する次のアクセスコントロールルール(またはアクセスコントロールポリシーのデフォルトアクション)によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザグループのメンバーであるユーザが、ユーザグループ条件を含むアクセスコントロールルールに一致しない。
- ユーザデータ取得に使用されたサーバが **Active Directory** サーバである場合に、ISE またはユーザエージェントによって報告されたユーザがアクセスコントロールルールに一致しない。

これにより、システムがユーザデータをイベントビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

アクセスコントロールルールへのレルム、ユーザ、またはユーザグループ条件の追加

ライセンス:Control

はじめる前に

- [ユーザアイデンティティソース \(30-1 ページ\)](#) の説明に従って、1 つ以上の権限のあるユーザアイデンティティソースを設定します。
- [レルムの作成 \(29-5 ページ\)](#) の説明に従って、レルムを設定します。アクセスコントロールルールでレルム、ユーザ、またはユーザグループ条件を設定できるようにするには、その前にユーザによるダウンロード(自動またはオンデマンド)が実行される必要があります。

-
- ステップ 1** アクセスコントロールルールエディタで、[ユーザ (Users)] タブを選択します。
- ステップ 2** [使用可能なレルム (Available Realms)] リストで名前または値で検索してレルムを選択します。
- ステップ 3** [使用可能なユーザ (Available Users)] リストで名前または値で検索してレルムを選択します。
- ステップ 4** [ルールに追加 (Add to Rule)] をクリックするか、ドラッグアンドドロップします。
- ステップ 5** ルールを保存するか、編集を続けます。
-

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-12 ページ\)](#) を参照してください。

アクセスコントロールルールへの ISE 属性条件の追加

ライセンス:Control

はじめる前に

- [ISE 接続の設定 \(30-6 ページ\)](#) の説明に従って ISE を設定します。

-
- ステップ 1** アクセスコントロールルールエディタで、[ISE 属性 (ISE Attributes)] タブを選択します。
- ステップ 2** [使用可能な ISE セッション属性 (Available ISE Session Attributes)] リストで名前または値で検索して属性を選択します。
- ステップ 3** [使用可能な ISE メタデータ (Available ISE Metadata)] リストで名前または値で検索してメタデータを選択します。

ステップ 4 [ルールに追加 (Add to Rule)] をクリックするか、ドラッグ アンド ドロップします。



ヒント

[ロケーションの IP アドレスの追加 (Add a Location IP Address)] フィールドを使用して、条件にロケーションの IP 属性を追加することもできます。システムは、各リーフ ドメインに個別のネットワーク マップを作成します。マルチドメイン展開では、実際の IP アドレスを使用してこの設定を抑制すると、予期しない結果になる可能性があります。

ステップ 5 ルールを保存するか、編集を続けます。

次の作業

- 設定変更を展開します。[設定変更の展開 \(4-12 ページ\)](#) を参照してください。