



アクセスコントロールルール：レルムとユーザ

ライセンス：Control

ユーザ制御を実行する（レルム全体、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、レルムを設定する。レ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。



(注) SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイントロケーション、またはエンドポイントプロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- レ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/ISE-PIC 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/ISE-PIC 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/ISE-PIC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、グループに基づいてユーザマッピングがドロップされることがあります。その結果、レルム、ユーザ、またはユーザグループ条件を持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のレルム、ユーザおよびグループを[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、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自動的に含まれます。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、および一部の復号化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問題のトラブルシューティング（2ページ）](#)
- [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（3ページ）](#)
- [ISE属性条件の設定（4ページ）](#)

ユーザアクセスコントロールルールに関する問題の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、またはレルムの設定を調整することを検討してください。

レルム、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/ISE-PIC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、レルム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編成している場合、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/ISE-PIC 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**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**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の条件を設定する前に、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、[Users] タブを選択します。

ステップ2 [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 [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 [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。

ISE 属性条件の設定

ライセンス：Control

はじめる前に

- **レルムの作成**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ISE属性条件を設定するには、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。



(注) SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイントロケーション、またはエンドポイントプロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- **ISE/ISE-PIC 接続の設定**の説明に従って ISE を設定します。



(注) ISE-PIC アイデンティティソースでは、ISE 属性データを提供しません。ISE を設定する必要があります。

ステップ1 アクセスコントロールルールエディタで、[SGT/ISE Attributes] タブをクリックします。

ステップ2 [Available 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 [Available 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 [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 [Add a Location IP Address] フィールドで、IP アドレスによりルールを制約します。

(注) ISE 属性条件を制約するために、ISE 割り当てセキュリティグループタグ (SGT) を使用できません。アクセスコントロールルールでカスタム SGT を使用するには、[ISE SGT およびカスタム SGT ルール条件](#)を参照してください。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

