レルムとアイデンティティ ポリシー

次のトピックでは、レルムとアイデンティティ ポリシーについて説明します。

レルムとアイデンティティ ポリシーについて

レルムは、同じディレクトリ クレデンシャルを共有する 1 つ以上の LDAP または Microsoft Active Directory サーバで構成されます。ユーザおよびユーザ グループ クエリやユーザ制御を実行したり、権限のあるアイデンティティ ソースを設定したりするには、レルムを設定する必要があります。1つ以上のレルムを設定すると、アイデンティティ ポリシーを設定できます。

アイデンティティポリシーは、ネットワーク上のトラフィックを権限のあるアイデンティティ ソースおよびレルムと関連付けます。1 つ以上のアイデンティティ ポリシーを設定した後、1 つをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを管理対象デバイスに展開できます。

レルムについて

レルムとは、Firepower Management Center とモニタリング対象のサーバ上にあるユーザ アカウントの間の接続です。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループを指定する。
- 権限のあるユーザ、および権限のあるユーザ以外の一部のユーザ（トラフィック ベースの検出で検出された POP3 および IMAP ユーザ、およびトラフィック ベースの検出、ユーザ

エージェント、TS エージェント、ISE によって検出されたユーザ）のユーザ メタデータについてユーザ リポジトリに照会する。

レルム内のディレクトリとして複数のドメイン コントローラを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または Active Directory（AD）サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 Firepower Management Centerがサーバに照会するときに適用されます。

ユーザ認識を行うには、レルムがサポートされているサーバのレルムを設定する必要があります。システムは、これらの接続を使用して、POP3 および IMAP ユーザに関連するデータについてサーバにクエリし、トラフィック ベースの検出で検出された LDAP ユーザに関するデータを収集します。

システムは、POP3 および IMAP ログイン内の電子メールアドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザ制御を実行するために以下のいずれかを設定できます。

- ユーザ エージェントまたは ISE 用の AD サーバのレルム
- TS エージェント用の AD サーバのレルム
- キャプティブ ポータル用の AD、Oracle Directory、OpenLDAP サーバのレルム

。

ユーザ ダウンロードについて

特定の検出されたユーザの、次のユーザとユーザ グループのメタデータを取得するために、Firepower Management Center と LDAP サーバまたは AD サーバとの間の接続を確立するためのレルムを設定することができます。

- キャプティブ ポータルで認証された、あるいはユーザ エージェントまたは ISE で報告された LDAP および AD ユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出で検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メールアドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

レルム内の 1 つのディレクトリとして、個々のサーバ接続を設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[アクセス コントロールのためのユーザおよびユーザ グループのダウンロード（Download users and user groups for access control）] をオンにする必要があります。

Firepower Management Centerは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名

- 姓と名
- 電子メール アドレス（Email address）
- 部署名（Department）
- 電話番号（Telephone number）

ユーザ アクティビティ データについて

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザのアイデンティティ データはユーザ データベースに保存されます。アクセス制御で保存できる使用可能なユーザの最大数は Firepower Management Center モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス制御パラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザの数をメッセージセンターの [タスク（Tasks）] タブ ページで報告します。

（注） ユーザ リポジトリからシステムによって検出されたユーザを削除しても、Firepower Management Centerはユーザ データベースからそのユーザを削除しません。そのため、手動で削除する必要があります。ただし、LDAP に対する変更は、Firepower Management Center が次に権限のあるユーザのリストを更新したときにアクセス コントロール ルールに反映されます。

レルムおよび信頼できるドメイン

Firepower Management Center でレルムを設定すると、そのレルムは Active Directory または LDAP ドメインに関連付けられます。

互いに信頼する Microsoft Active Directory（AD）ドメインのグループ化は、一般的にフォレストと呼ばれます。この信頼関係により、ドメインは異なる方法で互いのリソースにアクセスできます。たとえば、ドメイン A で定義されたユーザ アカウントに、ドメイン B で定義されたグループのメンバーとしてマークを付けることができます。

Firepower システムは、信頼できる AD ドメインをサポートしていません。つまり、Firepower システムは、どのドメインが互いに信頼しているかを追跡せず、どのドメインが互いの親ドメインまたは子ドメインかを認識しません。また、Firepower システムでは、信頼関係が Firepower システム外で実施される場合でも、クロスドメイン信頼を使用する環境のサポートを保証するテストがまだ行われていません。

詳細については、レルムとユーザのダウンロードのトラブルシューティング （6 ページ）を参照してください。

レルムがサポートされているサーバ

レルムを設定して次のサーバ タイプに接続すると、Firepower Management Centerからの TCP/IP アクセスを提供できます。

サーバタイプ（**Server Type**）	ユーザ認識によるデータ取得のサポート	ユーザエージェントによるデータ取得のサポート	**ISE** によるデータ取得のサポート	**TS** エージェントによるデータ取得のサポート	キャプティブポータルによるデータ取得のサポート
Windows Server 2008 と Windows Server 2012 上の Microsoft Active Directory	○	○	○	○	○
Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	[はい（Yes）]	[いいえ（No）]	[はい（Yes）]	[いいえ（No）]	○
Linux 上の OpenLDAP	[はい（Yes）]	[いいえ（No）]	[いいえ（No）]	[いいえ（No）]	○

（注） TS エージェントが別のパッシブ認証 ID ソース（ユーザ エージェントまたは ISE）と共有されている Windows サーバ上の Microsoft Active Directory にインストールされている場合、Firepower Management Center は TS エージェントのデータを優先します。TS エージェントとパッシブ ID ソースが同じ IP アドレスによるアクティビティを報告した場合は、TS エージェントのデータのみが Firepower Management Center に記録されます。

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行するには、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。
- グループ名は LDAP で内部的に使用されているため、**s-** で開始することはできません。

  グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用すると、それらのグループまたは組織単位内のユーザはダウンロードされず、アイデンティティ ポリシーでは使用できません。
- サーバのサブ グループのメンバーであるユーザを含める（または除外する）Active Directory レルムを設定する場合には、Active Directory サーバがレポートするユーザ数が、Windows

Server 2008 または 2012 の Microsoft Active Directory のグループ 1 つにつき 5000 ユーザに制限される点にご注意ください。

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるよう Active Directory サーバの設定を変更できます。

- ターミナル サービス環境でサーバにより報告されるユーザを一意に識別するには、Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを一意に識別できるようになります。

  TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

サポートされるサーバ フィールド名

Firepower Management Center がサーバからユーザ メタデータを取得できるようにするには、レルム内のサーバが、次の表に記載されているフィールド名を使用する必要があります。サーバ上のフィールド名が正しくない場合、Firepower Management Centerはそのフィールドの情報を使ってデータベースに入力できなくなります。

表 *1 : Firepower Management Center* フィールドへのサーバ フィールドのマッピング

メタデータ	**Management Center** のフィールド	**Active Directory** フィールド	**Oracle Directory Server** フィールド	**OpenLDAP** フィールド
LDAP ユーザ名	[ユーザ名（Username）]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn
メール アドレス	E メール	メール アドレス userprincipalname（mail に値が設定されていない場合）	メール アドレス	メール アドレス
部署	部署名（Department）	部署 distinguishedname（department に値が設定されていない場合）	部署	ou
電話番号	電話	telephonenumber	適用対象外	telephonenumber

レルムとユーザのダウンロードのトラブルシューティング

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。関連の他のトラブルシューティングについては、次を参照してください。

- ユーザ エージェント アイデンティティ ソースのトラブルシューティング
- ISE アイデンティティ ソースのトラブルシューティング
- TS エージェント アイデンティティ ソースのトラブルシューティング
- キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング
- ユーザ制御のトラブルシューティング

症状：アクセス コントロール ポリシーがグループのメンバーシップと一致しない

この解決策は、他の AD ドメインとの信頼関係にある AD ドメインに適用されます。以下の説明で、外部ドメイン ドメインは、ユーザがログインするドメイン以外のドメインを指します。

ユーザが信頼されている外部ドメインで定義されたグループに属している場合、Firepower は外部ドメインのメンバーシップを追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン コントローラ 1 と 2 は相互に信頼している
- グループ A はドメイン コントローラ 2 で定義されている
- コントローラ 1 のユーザ `mparvinder` はグループ A のメンバーである

ユーザ `mparvinder` はグループ A に属しているが、メンバーシップ グループ A を指定する Firepower のアクセス コントロール ポリシー ルールが一致しません。

解決策：グループ A に属する、すべてのドメイン 1 のアカウントを含むドメイン コントローラ 1 に同様のグループを作成します。グループ A またはグループ B のすべてのメンバーに一致するように、アクセス コントロール ポリシー ルールを変更します。

症状：アクセス コントロール ポリシーが子ドメインのメンバーシップと一致しない

ユーザが親ドメインの子であるドメインに属している場合、Firepower はドメイン間の親/子関係を追跡しません。たとえば、次のシナリオを考えてください。

- ドメイン `child.parent.com` はドメイン `parent.com` の子である
- ユーザ `mparvinder` は `child.parent.com` で定義されている

ユーザ `mparvinder` が子ドメインに属しているが、`parent.com` と一致する Firepower アクセス コントロール ポリシーが `child.parent.com` ドメインの `mparvinder` と一致しません。

解決策：`parent.com` または `child.parent.com` のいずれかのメンバーシップに一致するようにアクセス コントロール ポリシー ルールを変更します。

予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが実行されていることに気付いたら、ユーザ エージェント、ISE、TS エージェント サーバの時間が Firepower Management Centerの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

レルム設定で指定したようにユーザが含まれない、または除外されない

サーバのサブグループのメンバーであるユーザを選別できる Active Directory レルムを設定する際は、Microsoft Windows サーバが報告するユーザの数を以下に制限することに注意します。

- Windows サーバ 2008 または 2012 では、グループごとに 5000 ユーザまで。Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0

必要に応じて、より多くのユーザをサポートするため、このデフォルトの制限を引き上げるようサーバの設定を変更できます。

ユーザがダウンロードされない

グループ名または組織単位名に特殊文字が使用されている Active Directory グループのユーザは、アイデンティティ ポリシー ルールで使用できない可能性があります。たとえば、グループ名または組織単位名にアスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字が含まれている場合、これらのグループ内のユーザはダウンロードされず、アイデンティティ ポリシーで使用できません。

解決策：グループ名または組織単位名から特殊文字を削除します。

未知の ISE とユーザエージェントのユーザのユーザデータが Web インターフェイスで表示されない

システムはデータがまだデータベースにない ISE、ユーザエージェントまたは TS エージェントユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Microsoft Windows サーバからこの情報を正常に取得するためにさらに時間がかかることもあります。データ取得が成功するまで、ISE、ユーザエージェント、TS エージェントユーザから見えるアクティビティは Web インターフェイスに表示されません。

これにより、アクセス制御ルールを使ったユーザトラフィックの処理も妨げられることがある点に注意します。

イベントのユーザデータが想定外の内容になる

ユーザやユーザアクティビティイベントに想定外の IP アドレスが含まれる場合は、レルムを確認します。複数のレルムに同一の [AD プライマリ ドメイン（AD Primary Domain）] の値を設定することはできません。

ターミナルサーバでのログインによるユーザが Web インターフェイスで一意に特定されない

導入されている構成にターミナルサーバが含まれ、これに接続されている 1 つまたは複数のサーバにレルムが設定されている場合は、ターミナルサーバ環境でのユーザログインを正確に

報告するため Cisco Terminal Services（TS）エージェントを設定する必要があります。TS エージェントをインストールし、設定すると、このエージェントは各ユーザに別個のポートを割り当て、Firepower System はこれらのユーザを Web インターフェイスで一意に識別できるようになります。

TS エージェントの詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。

アイデンティティ ポリシーについて

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- **[システム（System）] > [統合（Integration）] > [レルム（Realms）]** でアイデンティティ ポリシー外のレルムを設定します。詳細については、レルムの作成 （9 ページ）を参照してください。
- パッシブ認証のアイデンティティ ソースであるユーザ エージェントと ISE は、**[システム（System）] > [統合（Integration）] > [アイデンティティ ソース（Identity Sources）]** で設定します。詳細については、ユーザ制御のためのユーザエージェントの設定およびユーザ制御用 ISE の設定を参照してください。
- パッシブ認証のアイデンティティ ソースである TS エージェントについては、Firepower システムの外で設定します。詳細については、『*Cisco Terminal Services (TS) Agent Guide*』を参照してください。
- アクティブ認証のアイデンティティ ソースであるキャプティブ ポータルについては、アイデンティティ ポリシー内で設定します。詳細については、ユーザ制御のためのキャプティブ ポータルの設定を参照してください。

単一のアイデンティティ ポリシーに複数のアイデンティティ ルールを追加した後、ルールの順番を決めます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールがそのトラフィックを処理するルールです。

1 つ以上のアイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーの 1 つのアイデンティティ ポリシーを呼び出す必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致する場合、システムはトラフィックを指定されたレルムと関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、システムはユーザ認証を実行しません。

関連トピック

ユーザ アイデンティティ ソース

レルムの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Access Admin、Network Admin

レルム設定フィールドの詳細については、レルム フィールド （10 ページ）を参照してください。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 新しいレルムを作成するには、[新規レルム（New Realm）] をクリックします。

ステップ 5 その他のタスク（レルムの有効化、無効化、削除など）を実行する場合は、レルムの管理 （21 ページ）を参照してください。

ステップ 6 レルム フィールド （10 ページ）で説明したように、レルム情報を入力します。

ステップ 7 （オプション）レルムへの接続をテストするには、[テスト（Test）] をクリックします。

（注） レルム テストが成功するには、[AD 結合ユーザ名（AD Join Username）] と [AD 結合パスワード（AD Join Password）] の両方のフィールドに値を入力する必要があります。

ステップ 8 [OK] をクリック

ステップ 9 レルム ディレクトリの設定 （13 ページ）で説明したように、少なくとも 1 つのディレクトリを設定します。

ステップ 10 ユーザとグループのダウンロード （14 ページ）の説明に従って、（アクセス コントロールに必要な）ユーザとユーザ グループのダウンロードを設定します。

ステップ 11 [レルム設定（Realm Configuration）] タブをクリックします。

ステップ 12 [認証済みユーザ（Authenticated Users）]、[認証に失敗したユーザ（Failed Authentication Users）]、および [ゲスト ユーザ（Guest Users）] にユーザ セッション タイムアウト値（分単位）を入力します。

次のタスク

- レルム ディレクトリの設定 （13 ページ）

- レルムの編集、削除、有効化、または無効化を行います。レルムの管理 （21 ページ）を参照してください
- レルムの比較 （22 ページ）。
- 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示を参照）。

レルム フィールド

次のフィールドを使用してレルムを設定します。

レルムの設定（Realm Configuration）フィールド

これらの設定は、レルム内のすべてのサーバまたはコントローラ（別名ディレクトリ）に適用されます。

[名前（Name）]

レルムの一意の名前。英数字や特殊文字に対応しています。

説明

（オプション）レルムの説明を入力します。

AD プライマリ ドメイン（AD Primary Domain）

Active Directory レルム専用です。ユーザ認証が必要となる Active Directory サーバのドメインです。

（注） [AD プライマリ ドメイン（AD Primary Domain）] 値のすべてのレルムが一意である必要があります。

AD 参加ユーザ名（AD Join Username）、AD 参加パスワード（AD Join Password）

Kerberos のキャプティブ ポータルのアクティブ認証を目的とした AD レルムでは、クライアントをドメインに参加させる適切な権利を有するユーザのユーザ名とパスワードとが区別されています。

アイデンティティ ルールの **[認証タイプ（Authentication Type）]** に **`Kerberos`** を選択する場合（または Kerberos をオプションとして **`HTTP Negotiate`** を選択する場合）、Kerberos キャプティブ ポータル アクティブ認証を実行するには、[アクティブディレクトリ参加ユーザ名（AD Join Username）] と [アクティブディレクトリ参加パスワード（AD Join Password）] を使用して、選択した [レルム（Realm）] を設定する必要があります。

[ディレクトリ ユーザ名（Directory Username）] と [ディレクトリ パスワード（Directory Password）]

取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

ベース DN（Base DN）

Firepower Management Center がユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベース識別名（DN）には企業ドメイン名および部門を示す基本構造があります。たとえば、Example 社のセキュリティ部門のベース DN は、**ou=security,dc=example,dc=com** となります。

グループ DN（Group DN）

Firepower Management Centerがグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。

（注） グループ名または組織単位名には、アスタリスク（*）、イコール（=）、バックスラッシュ（\）などの特殊文字は使用できません。使用した場合、それらのグループのユーザはダウンロードされず、アイデンティティ ポリシーで使用できないためです。

グループ属性（Group Attribute）

（オプション）サーバのグループ属性：メンバー、または一意のメンバー。

タイプ（Type）

レルム、AD、LDAP のタイプ。

（注） キャプティブ ポータルのみ、LDAP レルムをサポートします。

レルムの設定（Realm Configuration）フィールド

Active Directory 情報
Active Directory 情報のフィールドについては、このセクションの前半で説明しました。

[ユーザ セッション タイムアウト（User Session Timeout）]
ユーザセッションがタイムアウトするまでの分数を入力します。デフォルトは1440分（24時間）です。

（注） ユーザ セッションタイムアウト値は、アクティブ認証（キャプティブ ポータル）とパッシブ認証（TSエージェント、ユーザエージェント、ISE）の両方に適用されます。大きな値を設定すると、ユーザセッションが終了しない可能性があり、他のユーザによってこれらのセッションが要求される場合があります。

レルムのディレクトリ フィールド（Realm Directory Fields）

これらの設定は、レルム内の個々のサーバ（ディレクトリ）に適用されます。

暗号化（Encryption）

Firepower Management Center サーバ接続に使用する暗号化方式。

- **STARTTLS**：暗号化 LDAP 接続
- **LDAPS**：暗号化 LDAP 接続
- **なし**：非暗号化 LDAP 接続（保護されていないトラフィック）

ホスト名/IP アドレス（Hostname/IP Address）

サーバのホスト名または IP アドレス。[暗号化（Encryption）] 方式を指定する場合は、このフィールドでホスト名を指定します。

[ポート（Port）]

Firepower Management Center サーバ接続に使用するポート。

SSL 証明書（SSL Certificate）

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するにために、STARTTLS または LDAPS を [暗号化（Encryption）] タイプとして設定できます。

認証に証明書を使用する場合、証明書のサーバ名は、サーバの [ホスト名/IP アドレス（Hostname/IP Address）] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用しているのに、証明書で **computer1.example.com** を使用している場合は、接続が失敗します。

ユーザのダウンロード（User Download）フィールド

[使用可能なグループ（Available Groups）]、[含むに追加する（Add to Include）]、[除外するに追加する（Add to Exclude）]

ダウンロードしてユーザ認識やユーザ制御に使用できるようにするグループを特定します。

- [使用可能グループ ボックス（Available Groups）] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する（Add to Include）] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- [除外に追加する（Add to Exclude）] ボックスにグループを移動させると、グループがダウンロードされ、ユーザデータはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ（Groups to Include）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。
- 除外されないグループのユーザを除外するには、[除外するグループ（Groups to Exclude）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。

自動ダウンロードの開始、繰り返し設定（Begin automatic download at, Repeat every）

自動ダウンロードの回数を指定します。

ユーザおよびグループのダウンロード（ユーザアクセス制御に必須）

ユーザ認識用およびユーザ制御用にユーザとグループをダウンロードできるようになります。

レルム ディレクトリの設定

この手順では、ドメイン コントローラなどのサーバに対応するレルム ディレクトリを作成できます。それぞれ異なるユーザやグループを認証する複数のドメイン コントローラを 1 つのユーザ リポジトリ（Active Directory など）に設定することができます。

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

レルム ディレクトリの設定フィールドに関する詳細については、レルム フィールド（10 ページ）を参照してください。

始める前に

オプションで SSL 証明書を使用してディレクトリで認証するには、Firepower Management Center のアクセス元となるマシンで証明書を作成するか、証明書データとキーを利用可能にします。

手順

ステップ 1 まだ実行していない場合は、Firepower Management Center にログインし、[統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 2 [レルム（Realms）] タブ ページで、ディレクトリの設定対象となるレルムの名前をクリックします。

ステップ 3 [ディレクトリ（Directory）] タブ ページで、[ディレクトリの追加（Add Directory）] をクリックします。

ステップ 4 [サーバのホスト名/IP アドレス（Hostname / IP Address）] と [ポート（Port）] を入力します。

ステップ 5 [暗号化モード（Encryption Mode）] を選択します。

ステップ 6 （オプション）リストから [SSL 証明書（SSL Certificate）] を 1 つ選択するか、追加アイコン（  ）をクリックして証明書を追加します。

ステップ 7 接続をテストするには、[テスト（Test）] をクリックします。

ステップ 8 [OK] をクリックします。

ステップ 9 [保存（Save）] をクリックします。[レルム（Realms）] タブ ページに戻ります。

ステップ 10 レルムをまだ有効にしていない場合は、[レルム（Realms）] タブ ページで、[状態（State）] を有効にします。

次のタスク

- ユーザとグループのダウンロード （14 ページ）.

ユーザとグループのダウンロード

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

このセクションでは、Active Directory サーバから Firepower Management Center にユーザとグループをダウンロードする方法について説明します。含めるグループを指定しなかった場合、システムは指定されたパラメータと一致するすべてのグループのユーザデータを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

Firepower Management Center がサーバから取得可能なユーザの最大数は Firepower Management Center モデルによって異なります。レルムのダウンロードパラメータの範囲が広すぎる場合、Firepower Management Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数を Message Center の [タスク（Task）] タブで報告します。

（注） Firepower Management Center では、Unicode 文字を含むユーザ名は表示されません。ユーザやグループをダウンロードする前に、Unicode 文字を英数字に置き換えてください。

レルム設定フィールドの詳細については、レルム フィールド （10 ページ）を参照してください。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 [統合（Integration）] > [レルム（Realms）] をクリックします。

ステップ 3 ユーザとグループを手動でダウンロードするには、ユーザやユーザ グループをダウンロードするレルムの横にあるダウンロード アイコン（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。残りの手順をスキップできます。

ステップ 4 自動でユーザとグループをダウンロードするようにレルムを設定するには、自動でユーザやグループをダウンロードするように設定するレルムの横にある編集アイコン（  ）をクリックします。

ステップ 5 [ユーザアクセス制御（User Access Control）] タブ ページで、[（ユーザアクセス制御に必要な）ユーザとグループをダウンロードする（Download users and groups (required for user access control)）] をオンにします。

ステップ 6 一覧から [自動ダウンロードの開始時間（Begin automatic download at）] の時間を選択します。

ステップ 7 [繰り返し設定（Repeat Every）] 一覧からダウンロード間隔を選択します。

ステップ 8 ダウンロードにユーザ グループを含めるか除外するには、[選択可能なグループ（Available Groups）] 列からユーザ グループを選択し、[含めるに追加（Add to Include）] または [除外に追加（Add to Exclude）] をクリックします。

複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

（注） そのグループのユーザに対してユーザ制御を実行する場合は、[含めるに追加（Add to Include）] をクリックする必要があります。

次の注意事項に従ってください。

- [使用可能グループ ボックス（Available Groups）] にグループが残っている場合、グループのダウンロードは行われません。
- グループを [含むに追加する（Add to Include）] ボックスに移動させた場合、そのグループはダウンロードされ、ユーザ データはユーザ認識やユーザ制御に利用できます。
- [除外に追加する（Add to Exclude）] ボックスにグループを移動させると、グループがダウンロードされ、ユーザデータはユーザ認識に利用できますが、ユーザ制御には利用できません。
- 含まれないグループのユーザを含めるには、[含めるグループ（Groups to Include）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。
- 除外されないグループのユーザを除外するには、[除外するグループ（Groups to Exclude）] の下のフィールドにそのユーザ名を入力し、[追加（Add）] をクリックします。

アイデンティティ ポリシーの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

始める前に

- レルムの作成 （9 ページ）の説明に従って 1 つ以上のレルムを作成し、有効にします。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[ポリシー（Policies）]** > **[アクセス コントロール（Access Control）]** > **[ID（Identity）]** をクリックし、[新しいポリシー（New Policy）] をクリックします。

ステップ 3 [名前（Name）] を入力し、必要に応じて [説明（Description）] を入力します。

ステップ 4 [保存（Save）] をクリックします。

ステップ 5 ポリシーにルールを追加するには、アイデンティティ ルールの作成 （16 ページ）で説明されているように、[ルールの追加（Add Rule）] をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 7 キャプティブ ポータルのアクティブ認証を設定するには、ユーザ制御のためのキャプティブ ポータルの設定で説明されているように、[アクティブ認証（Active Authentication）] タブをクリックします。

ステップ 8 [保存（Save）] をクリックして、アイデンティティ ポリシーを保存します。

次のタスク

- 照合するユーザおよび他のオプションを指定するルールを、アイデンティティ ポリシーに追加します（アイデンティティ ルールの作成 （16 ページ）を参照）。
- 指定したリソースへのアクセスを特定のユーザに許可またはブロックするには、このアイデンティティ ポリシーをアクセス コントロール ポリシーに関連付けます（アクセス制御への他のポリシーの関連付けを参照）。
- 設定変更を管理対象デバイスに展開します（設定変更の導入を参照）。

アイデンティティ ルールの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

アイデンティティ ルールの設定オプションに関する詳細については、アイデンティティ ルール フィールド （18 ページ）を参照してください。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）]** をクリックします。

ステップ 3 アイデンティティ ルールの追加先となるアイデンティティ ポリシーの横にある [編集（edit）]（  ）をクリックします。

代わりに表示アイコン（  ）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 [ルールの追加（Add Rule）] をクリックします。

ステップ 5 名前を入力します。

ステップ 6 ルールを**有効**にするかどうかを指定します。

ステップ 7 既存のカテゴリにルールを追加するには、ルールを [挿入（Insert）] する場所を指定します。新しいカテゴリを追加するには、[カテゴリの追加（Add Category）] をクリックします。

ステップ 8 一覧からルール [アクション（Action）] を選択します。

ステップ 9 [レルムおよび設定（Realms & Settings）] タブをクリックします。

ステップ 10 [レルム（Realms）] 一覧から、アイデンティティ ルールのレルムを選択します。各アイデンティティ ルールにレルムを関連付ける必要があります。

レルム要件の唯一の例外は、ISE SGT 属性タグのみを使用してユーザ制御を実装する場合です。この場合は、ISE サーバのレルムを設定する必要はありません。ISE SGT 属性条件は、関連するアイデンティティ ポリシーの有無にかかわらずポリシーで設定できます。

ステップ 11 キャプティブ ポータルを設定する場合は、ユーザ制御のためのキャプティブ ポータルの設定を参照してください。

ステップ 12 （オプション）アイデンティティ ルールに条件を追加するには、ルール条件タイプを参照してください。

ステップ 13 [追加（Add）] をクリックします。

ステップ 14 ポリシーエディタで、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。ルールには 1 から番号が付けられます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。トラフィックが一致する最初のルールは、そのトラフィックを処理するルールです。適切なルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

ステップ 15 [保存（Save）] をクリックします。

関連トピック

Snort® の再起動シナリオ

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

[有効（Enabled）]

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

アクション（Action）

指定したレルムでユーザに対して実行する認証のタイプを指定します。これには、[パッシブ認証（Passive Authentication）]（デフォルト）、[アクティブ認証（Active Authentication）]、または [認証なし（No Authentication）] があります。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

注意 SSL 復号が無効の場合（つまりアクセス コントロール ポリシーに SSL ポリシーが含まれない場合）に、アクティブな最初の認証ルールを追加するか、アクティブな最後の認証ルールを削除すると 設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

アクティブ認証ルールには [アクティブ認証（Active Authentication）] ルール アクションが含まれているか、または **[パッシブ認証でユーザを識別できない場合はアクティブ認証を使用する（Use active authentication if passive authentication cannot identify user）]** が選択された [パッシブ認証（Passive Authentication）] ルール アクションが含まれています。

Firepower システムのバージョンでサポートされるパッシブおよびアクティブ認証方式の詳細については、ユーザ アイデンティティ ソースについてを参照してください。

レルム

指定された**アクション**を実行するユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルムを完全に設定する必要があります。

（注） [Kerberos]（または [Kerberos] をオプションとする場合は [HTTP ネゴシエート（HTTP Negotiate）]）を、アイデンティティ ルールの [認証タイプ（Authentication Type）] として選択する場合、選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行できるように、[AD 参加ユーザ名（AD Join Username）] と [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

パッシブ認証がユーザを識別できない場合は、アクティブ認証を使用します。

このオプションを選択すると、パッシブまたは VPN 認証でユーザを識別できない場合にキャプティブ ポータル アクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アイデンティティ ポリシーでキャプティブ ポータル アクティブ認証を設定する必要があります。

このオプションを無効にすると、VPN ID を持たないユーザまたはパッシブ認証では識別できないユーザは、「不明（Unknown）」と識別されます。

認証でユーザを識別できない場合は特別 ID/ゲストとして識別する（Identify as Special Identities/Guest if authentication cannot identify user）

ルール アクションとして [アクティブ認証（Active Authentication）]（つまり、キャプティブ ポータル認証）を設定している場合にのみ、このフィールドが表示されます。

認証タイプ

キャプティブ ポータル アクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証（BA）接続を使用してユーザを認証するには、[HTTP 基本（HTTP Basic）] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

  ほとんどの Web ブラウザは、**HTTP 基本**ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザを認証するには **NTLM** を選択します。この選択は AD レルムを選択するときにのみ使用できます。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

- Kerberos 接続を使用してユーザを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP（LDAPS）が有効になっているサーバに対して AD レルムを選択する場合にのみ可能です。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

（注） 選択する [レルム（Realm）] は、Kerberos キャプティブ ポータル アクティブ認証を実行するために、[AD 参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） Kerberos キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバを設定する必要があります。FQDN は、DNS の設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services および Firepower Threat Defense デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- キャプティブ ポータル サーバが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP ネゴシエート（HTTP Negotiate）] を選択します。このタイプは AD レルムを選択するときにのみ使用できます。

（注） 選択する [レルム（Realm）] は、[HTTP ネゴシエート（HTTP Negotiate）] で Kerberos キャプティブ ポータル アクティブ認証を選択するために、[AD 参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] を使用して設定する必要があります。

（注） [HTTP ネゴシエート（HTTP Negotiate）] キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決する DNS サーバを設定する必要があります。キャプティブ ポータルに使用するデバイスの FQDN は、DNS の設定時に入力したホスト名と一致している必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は ASA FirePOWER モジュールの FQDN です。

レルムの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

このセクションでは、[レルム（Realms）]ページ上のコントロールを使用して、レルムに関するさまざまなメンテナンス タスクを実行する方法について説明します。次の点に注意してください。

- コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 レルムを削除するには、削除アイコン（）をクリックします。

ステップ 5 レルムを編集するには、レルムの横にある編集アイコン（）をクリックし、レルムの作成（9 ページ）の説明に従って変更を行います。

ステップ 6 レルムを有効にするには、[状態（State）]を右にスライドします。レルムを無効にするには、左にスライドします。

ステップ 7 ユーザおよびユーザ グループをダウンロードするには、ダウンロードアイコン（）をクリックします。

ステップ 8 レルムをコピーするには、コピー アイコン（）をクリックします。

ステップ 9 レルムを比較する方法については、レルムの比較 （22 ページ）を参照してください。

レルムの比較

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator、Security Approver、Access Admin、Network Admin

手順

ステップ 1 Firepower Management Center にログインします。

ステップ 2 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 3 [レルム（Realms）] をクリックします。

ステップ 4 **[システム（System）] > [統合（Integration）]** をクリックします。

ステップ 5 [レルム（Realms）] をクリックします。

ステップ 6 [レルムの比較（Compare Realms）] をクリックします。

ステップ 7 [比較対象（Compare Against）] リストから [レルムの比較（Compare Realm）] を選択します。

ステップ 8 [レルム A（Realm A）] および [レルム B（Realm B）] リストから比較するレルムを選択します。

ステップ 9 [OK] をクリック

ステップ 10 個々の変更を選択するには、タイトル バーの上の [前へ（Previous）] または [次へ（Next）] をクリックします。

ステップ 11 （オプション）[比較レポート（Comparison Report）] をクリックして、レルム比較レポートを生成します。

ステップ 12 （オプション）[新しい比較（New Comparison）] をクリックして、新しいレルム比較ビューを生成します。

アイデンティティ ポリシーの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（**Access**）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）]** をクリックします。

ステップ 3 ポリシーを削除するには、削除（）をクリックします。コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 ポリシーを編集するには、ポリシーの横にある編集（）をクリックし、アイデンティティ ポリシーの作成 （15 ページ） の説明に従って変更を行います。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 5 ポリシーをコピーするには、コピー アイコン（）をクリックします。

ステップ 6 ポリシーのレポートを生成するには、現在のポリシー レポートの生成の説明に従ってレポート アイコン（）をクリックします。

ステップ 7 ポリシーを比較する方法については、ポリシーの比較を参照してください。

アイデンティティ ルールの管理

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス（Access）
任意（Any）	Control	任意（Any）	任意（Any）	Administrator/Access Admin/Network Admin

手順

ステップ 1 まだ Firepower Management Center にログインしていない場合は、ログインします。

ステップ 2 **[ポリシー（Policies）] > [アクセス コントロール（Access Control）] > [ID（Identity）]** をクリックします。

ステップ 3 編集するポリシーの横にある編集アイコン（）をクリックします。代わりに表示アイコン（）が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ステップ 4 アイデンティティ ルールを編集するには、編集アイコン（  ）をクリックし、アイデンティティ ポリシーの作成 （15 ページ）の説明に従って変更を行います。

ステップ 5 アイデンティティ ルールを削除するには、削除アイコン（  ）をクリックします。

ステップ 6 ルール カテゴリを作成するには、[カテゴリの追加（Add Category）] をクリックし、位置とルールを選択します。

ステップ 7 [保存（Save）] をクリックします。

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。