レルムの作成および管理

次のトピックでは、ユーザの認識と制御のためのユーザ ストアであるレルムの作成方法と管理方法について説明します。

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/ISE-PIC 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 または OpenLDAP 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/ISE-PIC 用の AD サーバのレルム

  ユーザ エージェントまたは ISE/ISE-PIC 用の AD サーバのレルム

（注） SGT ISE 属性条件を設定すること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、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。

- 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 または 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か、あるいはユーザ エージェントまたは ISE/ISE-PIC で報告された LDAP および AD のユーザ。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。

レルム内のディレクトリとして、LDAP サーバまたは Active Directory ドメイン コントローラ接続を設定します。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、次に権限のあるユーザのリストを Firepower Management Center が更新したときにアクセス 制御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ト （16 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 エージェントによるデータ取得のサポート	ISE/ISE-PIC 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	Yes	Yes	Yes	Yes
Linux 上の OpenLDAP	いいえ	なし	なし	○

（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-PIC）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。
- サーバ上のサブグループのメンバーであるユーザを含む（または除外する）Active Directory レルムを設定するには、Windows Server 2008 または 2012 では、Active Directory のグループあたりのユーザ数が 5000 人以下であることが Microsoft により推奨されていることに注意してください。詳細については、MSDN の「Active Directory Maximum Limits—Scalability」を参照してください。

  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。
- リモート デスクトップ 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。（Microsoft

により、ターミナル サービスという名称はリモート デスクトップ サービスに変更されました）。

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。

サポートされているサーバ オブジェクト クラスと属性名

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属性名を使用する必要があります。サーバ上の属性名が正しくない場合、Firepower Management Center はその属性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* フィールドへの属性名のマップ

メタデータ（**Metadata**）	**FMC** 属性	**LDAP** オブジェクト クラス	**Active Directory** 属性	**OpenLDAP** 属性
LDAP user name	[ユーザ名（Username）]	• user • inetOrgPerson	samaccountname	cn uid
first name	名		givenname	givenname
last name	姓		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
部署	部署名（Department）		部署 distinguishedname（department に値が設定されていない場合）	ou
電話番号	電話		telephonenumber	telephonenumber

（注） グループの LDAP オブジェクト クラスは、`group`、`groupOfNames`（Active Directory の場合は `group-of-names`）、または `groupOfUniqueNames` です。

オブジェクト クラスと属性の詳細については、次のリファレンスを参照してください。

- Microsoft Active Directory：
  - オブジェクト クラス：MSDN の「All Classes」

- 属性：MSDN の「All Attributes」

- OpenLDAP：RFC 4512

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 （7 ページ）を参照してください。

（注） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。ユーザとグループが適切に識別されないため、同じ [AD プライマリ ドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザとグループに割り当てるために発生します。そのため、システムは特定のユーザまたはグループを明確に識別できません。

手順

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

ステップ 2 **[System]** > **[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 （15 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 （7 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）[AD参加のテスト（Test AD Join）] をクリックして、レルムへの接続をテストします。

（注） Microsoft Active Directory のレルム テストを成功させるには、[AD参加ユーザ名（AD Join Username）] フィールドと [AD参加パスワード（AD Join Password）] フィールドの両方に値を入力し、ドメインにコンピュータを追加するための十分な権限がユーザにある必要があります。詳細については、レルム フィールド （7 ページ）を参照してください。

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 （12 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 （13 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 [ユーザエージェントおよびISE/ISE-PICユーザ（User Agent and ISE/ISE-PIC Users）]、[TSエージェントユーザ（TS Agent Users）]、[キャプティブポータルユーザ（Captive Portal Users）]、[失敗したキャプティブポータルユーザ（Failed Captive Portal Users）]、および [ゲストキャプティブポータルユーザ（Guest Captive Portal Users）] のユーザ セッション タイムアウト値を分単位で入力します。

次のタスク

- レルム ディレクトリの設定 （12 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 （15 ページ）を参照してください
- レルムの比較 （16 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 Active Directory サーバまたはドメイン 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。

- アイデンティティ ポリシーにレルムを使用する場合、英数字や特殊文字に対応しています。
- RA VPN 設定でレルムを使用する場合は、英数字、ハイフン（-）、下線（_）、プラス（+）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）

Microsoft 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） すべての Microsoft Active Directory（AD）レルムに固有の [ADプライマリドメイン（AD Primary Domain）] を指定する必要があります。ユーザとグループが適切に識別されないため、同じ [AD プライマリ ドメイン（AD Primary Domain）] を使用して複数のレルムを指定することはできません。これは、システムが一意の ID を各レルムのすべてのユーザとグループに割り当てるために発生します。そのため、システムは特定のユーザまたはグループを明確に識別できません。

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

Kerberos キャプティブ ポータル アクティブ認証を目的とした Microsoft Active Directory レルムでは、Active Directory ドメインでドメイン コンピュータ アカウントを作成するための適切な権限を持つ Active Directory ユーザの識別用のユーザ名とパスワード。

次の点を考慮してください。

- DNS は、ドメイン名を Active Directory ドメイン コントローラの IP アドレスに解決できる必要があります。
- 指定するユーザは、コンピュータを Active Directory ドメインに参加させることができる必要があります。
- ユーザ名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

アイデンティティ ルールの **[認証プロトコル（Authentication Protocol）]** 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アクセス権を持っているユーザの識別用のユーザ名とパスワード。

次の点に注意してください。

- Microsoft Active Directory では、ユーザに昇格された特権は必要ありません。ドメイン内の任意のユーザを指定できます。
- OpenLDAP では、ユーザのアクセス権限は、OpenLDAP の仕様書のセクション 8 で説明されている `<level>` パラメータにより決定されます。ユーザの `<level>` は、`auth` 以上にする必要があります。

- ユーザ名は完全修飾名である必要があります（たとえば、**administrator** ではなく **administrator@mydomain.com** を使用します）。

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。サポートされているグループ属性の一覧については、サポートされているサーバ オブジェクト クラスと属性名 （5 ページ）を参照してください。

（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）

レルムのタイプで、Microsoft Active Directory 用の **AD** またはその他のサポートされている LDAP リポジトリ用の **LDAP** です。サポートされている LDAP リポジトリの一覧については、レルムがサポートされているサーバ （3 ページ）を参照してください。

（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。

既存のレルムを編集する場合、次のフィールドを使用できます。

[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、ユーザのログイン イベントから 1440 分（24 時間）後です。このタイムアウトを過ぎると、ユーザのセッションは終了します。ユーザが再度ログインせずにネットワークにアクセスし続けている場合、ユーザは Firepower Management Center により不明として認識されます（[失敗したキャプティブポータルユーザ（Failed Captive Portal Users）] を除く）。

次のタイムアウト値を設定できます。

- [ユーザエージェントおよびISE/ISE-PICユーザ（User Agent and ISE/ISE-PIC Users）]：パッシブ認証タイプであるユーザ エージェントまたは ISE/ISE-PIC によってトラッキ

ングされるユーザのタイムアウト。詳細については、ISE/ISE-PIC アイデンティティ ソースを参照してください。

- [TSエージェントユーザ（TS Agent Users）]：パッシブ認証タイプである TS エージェントによってトラッキングされるユーザのタイムアウト。詳細については、ターミナル サービス（TS）エージェントのアイデンティティ ソースを参照してください。
- [キャプティブポータルユーザ（Captive Portal Users）]：アクティブ認証タイプであるキャプティブ ポータルを使用して正常にログインしたユーザのタイムアウト。詳細については、キャプティブ ポータルのアイデンティティ ソースを参照してください。
- [失敗したキャプティブポータルユーザ（Failed Captive Portal Users）]：キャプティブ ポータルを使用して正常にログインしていないユーザのタイムアウト。Firepower Management Center によってユーザが認証失敗ユーザとして認識されるまでの、[最大ログイン試行回数（Maximum login attempts）] を設定できます。アクセス コントロール ポリシーを使用して、認証失敗ユーザにネットワークへのアクセス権を付与することもできます。この場合は、そのユーザにこのタイムアウト値が適用されます。

  失敗したキャプティブ ポータル ログインの詳細については、キャプティブ ポータル フィールドを参照してください。
- [ゲストキャプティブポータルユーザ（Guest Captive Portal Users）]：キャプティブ ポータルにゲスト ユーザとしてログインしているユーザのタイムアウト。詳細については、キャプティブ ポータルのアイデンティティ ソースを参照してください。

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（Active Directory ドメイン コントローラなど）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）

Active Directory ドメイン コントローラのホスト名または 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 コントローラ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。
- グループを [除外するに追加する（Add to Exclude）] ボックスに追加すると、グループ名のみがダウンロードされます。グループ内のユーザはダウンロードされません。
- 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。

（注） Firepower Management Center にダウンロードされるユーザは、数式 **R = I - (E+e) + i** を使用して計算されます。

- R はダウンロードしたユーザのリストです。
- I は含まれているグループです。
- E は除外されているグループです。
- e は除外されているユーザです。
- i は含まれているユーザです。

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、LDAP サーバまたは Microsoft Active Directory ドメイン コントローラ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 Active Directory サーバ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 （7 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 LDAP サーバまたは Active Directory ドメイン コントローラの [ホスト名/IPアドレス（Hostname / IP Address）] と [ポート（Port）] を入力します。
システムにより、指定したホスト名または IP アドレスに LDAP クエリが送信されます。ホスト名が LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される場合は、[テスト（Test）] が成功します。

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 （13 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 （7 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）] > [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。

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 **[System]** > **[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（6 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 （16 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 **[System]** > **[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 **[System]** > **[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。

レルムとユーザのダウンロードのトラブルシュート

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/ISE-PIC 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
- リモート アクセス VPN 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：レルムとグループは報告されますが、ダウンロードされません

Firepower Management Center のヘルス モニタは、次のように定義されたユーザまたはレルムの不一致を通知します。

- [ユーザの不一致（User mismatch）]：ユーザはダウンロードされることなく Firepower Management Center に報告されます。

  ユーザの不一致の一般的な理由は、ユーザが Firepower Management Center へのダウンロードから除外したグループに所属していることです。レルム フィールド （7 ページ）で検討した情報を確認してください。

- [レルムの不一致（Realm mismatch）]：Firepower Management Center に通知されていないレルムに対応するドメインにユーザがログインしています。

たとえば、Firepower Management Center で **domain.example.com** というドメインに対応するレルムを定義していても、**another-domain.example.com** というドメインからログインが報告される場合にレルムの不一致となります。このドメイン内のユーザは Firepower Management Center によって不明（Unknown）と識別されます。

不一致のしきい値をヘルス警告がトリガーされる値を上回るパーセンテージとして設定します。次に例を示します。

- デフォルトの不一致しきい値に 50% を使用しており、8 つの着信セッションに 2 つの不一致レルムがある場合、不一致のパーセンテージは 25% であり、警告はトリガーされません。
- 不一致のしきい値を 30% に設定し、5 つの着信セッションに 3 つの不一致レルムがある場合は、不一致のパーセンテージは 60% となり、警告がトリガーされます。

アイデンティティ ルールに一致しない不明なユーザに、適用されているポリシーがありません。（不明ユーザに対してアイデンティティ ルールをセットアップすることはできますが、ユーザとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

詳細については、レルムまたはユーザの不一致の検出 （20 ページ）を参照してください。

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。

症状：レルムまたはレルム ディレクトリのテストが失敗する

ディレクトリ ページの [テスト（Test）] ボタンは、入力したホスト名または IP アドレスに LDAP クエリを送信します。失敗した場合は、次を確認してください。

- 入力した [ホスト名（Hostname）] が、LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- 入力した [IPアドレス（IP Address）] が有効である。

レルム設定ページの [AD参加のテスト（Test AD Join）] ボタンは、次のことを確認します。

- DNS が、[ADプライマリドメイン（AD Primary Domain）] を LDAP サーバまたは Active Directory ドメイン コントローラの IP アドレスに解決される。
- [AD参加ユーザ名（AD Join Username）] と [AD参加パスワード（AD Join Password）] が正しい。

  [AD参加ユーザ名（AD Join Username）] は完全修飾名である必要があります（たとえば、**`administrator`** ではなく **`administrator@mydomain.com`** を使用します）。

- ドメイン内にコンピュータを作成し、ドメインに Firepower Management Center をドメイン コンピュータとして参加させるための十分な権限がユーザにある。

症状：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/ISE-PIC、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。

症状：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。

症状：ユーザがダウンロードされない

考えられる原因は次のとおりです。

- レルムの [タイプ（Type）] が正しく設定されていない場合は、FirePOWER システムにより必要とされる属性とリポジトリにより提供される属性が一致しないため、ユーザとグループをダウンロードできません。たとえば、Microsoft Active Directory レルムの [タイプ（Type）] を [LDAP] として設定すると、FirePOWER システムでは `uid` 属性が必要になり、この属性は Active Directory では `none` に設定されています。（Active Directory リポジトリでは、ユーザ ID に `sAMAccountName` が使用されます。）

  ソリューション：レルムの [タイプ（Type）] フィールドを適切に設定します。Microsoft Active Directory の場合は [AD] に設定し、サポートされている別の LDAP リポジトリの場合は [LDAP] に設定します。

- 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。

症状：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/ISE-PIC、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/ISE-PIC、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。

症状：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。

症状：ターミナル サーバからログインしたユーザが、システムによって一意に識別されない

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。

レルムまたはユーザの不一致の検出

この項では、レルムまたはユーザの不一致を検出する方法について説明します。これらは次のように定義されています。

- [ユーザの不一致（User mismatch）]：ユーザはダウンロードされることなく Firepower Management Center に報告されます。

  ユーザの不一致の一般的な理由は、ユーザが Firepower Management Center へのダウンロードから除外したグループに所属していることです。レルム フィールド （7 ページ）で検討した情報を確認してください。

- [レルムの不一致（Realm mismatch）]：Firepower Management Center に通知されていないレルムに対応するドメインにユーザがログインしています。

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ト （16 ページ）を参照してください。

アイデンティティ ルールに一致しない不明なユーザに、適用されているポリシーがありません。（不明ユーザに対してアイデンティティ ルールをセットアップすることはできますが、ユーザとレルムを正確に識別することによってルールの数を最小限に保つことをお勧めします。）

手順

ステップ 1 レルムまたはユーザの不一致の検出を有効にします。

a) 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。
b) **[システム（System）]** > **[ヘルス（Health）]** > **[ポリシー（Policy）]** をクリックします。
c) 新しいヘルス ポリシーを作成するか、または既存のポリシーを編集します。
d) [ポリシーの編集（Editing Policy）] ページで、[ポリシーのランタイム間隔（Policy Runtime Interval）] を設定します。
これは、すべてのヘルス モニタ タスクが実行される頻度です。
e) 左側のペインで、[レルム（Realm）] をクリックします。
f) 次の情報を入力します。

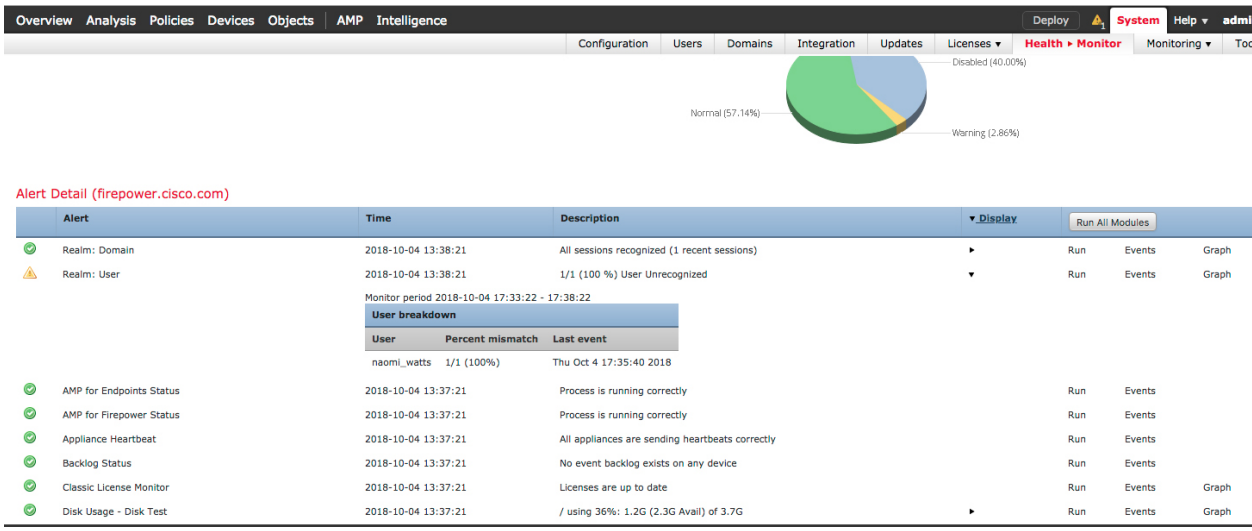
- [有効（Enabled）] : [オン（On）] をクリックします
- [一致しきい値（%）のユーザへの警告（Warning Users match threshold %）] : ヘルス モニタで警告をトリガーしたレルム不一致またはユーザ不一致のいずれかのパーセンテージ。詳細については、レルムとユーザのダウンロードのトラブルシュート （16 ページ）を参照してください。

g) ページの下部で [ポリシーを保存して終了（Save Policy & Exit）] をクリックします。
h) 正常性ポリシーの適用 の説明に従って、管理対象デバイスにヘルス ポリシーを適用します。

ステップ 2 次の方法のいずれかでユーザとレルムの不一致を表示します。

- 警告しきい値を超過した場合は（  ）をクリックし、 Firepower Management Center の上部のナビゲーションで [ヘルス（Health）] をクリックします。これにより、ヘルス モニタが開きます。
- **[システム（System）]** > **[ヘルス（Health）]** > **[モニタ（Monitor）]** をクリックします。

ステップ 3 [ヘルス モニタ（Health Monitor）] ページの [表示（Display）] 列で、[レルム：ドメイン（Realm: Domain）] または [レルム：ユーザ（Realm: User）] を展開し、不一致に関する詳細を表示します。
次に、100% のユーザ不一致の例を示します。この例では、Firepower Management Center で **naomi_watts** は検出されているものの、ダウンロードされていませんでした。



関連トピック

- 正常性ポリシー
- ヘルス モニタリングの設定
- ヘルス モニタ ステータスのカテゴリ