ISE/ISE-PIC によるユーザの制御

次のトピックでは、ISE/ISE-PIC によりユーザ認識とユーザ制御を実行する方法について説明します。

ISE/ISE-PIC アイデンティティ ソース

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を Firepower システムと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA を使用して認証するユーザに関するユーザ認識データを提供します。さらに、Active Directory ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） Firepower システムは IEEE 802.1x マシン認証を解析しませんが、802.1x ユーザ認証を解析します。ISE で 802.1x を使用している場合は、ユーザ認証を含める必要があります。802.1x マシン認証は、ポリシーで使用できる FMC にユーザ ID を提供しません。

Cisco ISE/ISE-PIC の詳細については、*Cisco Identity Services Engine* 管理者ガイドおよび『*Identity Services Engine Passive Identity Connector (ISE-PIC) Installation and Administrator Guide*』を参照してください。

ISE/ISE-PIC のガイドラインと制限事項

Firepower システムで ISE/ISE-PIC を構成する際に、このセクションで説明されているガイドラインを使用してください。

ISE/ISE-PIC バージョンと設定の互換性

ご使用の ISE/ISE-PIC バージョンと設定は、次のように Firepower との統合や相互作用に影響を与えます。

- ISE/ISE-PIC サーバと Firepower Management Center の時刻を同期します。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- ISE または ISE-PIC データを使用してユーザ制御を実装するには、レルムの作成 の説明に従って、pxGrid のペルソナを想定して ISE サーバのレルムを設定し有効にします。
- ISE サーバに接続する各 Firepower Management Center ホスト名は一意である必要があります。そうでない場合、Firepower Management Center のいずれかへの接続は廃棄されます。
- ISE のバージョン 2.0 パッチ 4 以降には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE の展開で ISE Endpoint Protection Service（EPS）が有効で設定されている場合は、ISE 接続を使用して、相関ポリシー違反に関与している送信元または宛先ホストに対する ISE EPS 修復を実行できます。
- ユーザの EPSStatus が変更された後でユーザの SGT を更新するように ISE の展開を設定した場合は、ISE EPS 修復により、Firepower Management Center 上の SGT も更新されます。
- ISE-PIC は、ISE 属性データを提供しないか、または ISE EPS の修復をサポートしません。

システムのこのバージョンと互換性がある特定のバージョンの ISE/ISE-PIC については、『*Cisco Firepower Compatibility Guide*』を参照してください。

ISE でのクライアントの認証

ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。

セキュリティ グループ タグ（SGT）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内のトラフィックの送信元の権限を指定します。Cisco ISE および Cisco TrustSec は、ネットワークに入るときに、セキュリティ グループ アクセス（SGA）と呼ばれる機能を使用して、パケットに SGT 属性を適用します。これらの SGT は、ISE または TrustSec 内のユーザの割り当てられたセキュリティ グループに対応します。ID ソースとして ISE を設定すると、Firepower システムは、これらの SGT を使用してトラフィックをフィルタリングできます。

（注） 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、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。詳細については、ISE 属性条件の設定を参照してください。

（注） 一部のルールでは、カスタム SGT 条件が ISE によって割り当てられなかった SGT 属性にタグ付けされたトラフィックを照合できます。これはユーザ制御とみなされず、アイデンティティ ソースとして ISE/ISE-PIC を使用しない場合にのみ機能します。カスタム SGT 条件 を参照してください。

ISE と高可用性

プライマリ Firepower Management Center が失敗すると、次の処理が行われます。

- スタンバイがプライマリに昇格するまで、セカンダリ Firepower Management Center ユーザ データベースは読み取り専用になります。

  リポジトリに追加されたユーザ（Active Directory など）は Firepower Management Center にダウンロードされず、それらのユーザは [不明（Unknown）] と識別されます。

  新しい SGT は使用されません。

- スタンバイがプライマリに昇格すると、すべての動作が正常に戻ります。つまり、ユーザがダウンロードされ、SGT が使用され、可能な場合はユーザが識別されます。

ISE プライマリ サーバが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。

エンドポイント ロケーション（Endpoint Location）（またはロケーション IP（Location IP））

[エンドポイント ロケーション（Endpoint Location）] 属性は、ISE によって識別される、ユーザの認証に ISE を使用したネットワーク デバイスの IP アドレスです。

[エンドポイント ロケーション（Endpoint Location）]（[ロケーション IP（Location IP）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ISE 属性

ISE 接続を設定すると、ISE 属性データが Firepower Management Center データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。 これは、ISE-PIC ではサポートされません。

エンドポイント プロファイル（Endpoint Profile）（またはデバイス タイプ（Device Type））

[エンドポイント プロファイル（Endpoint Profile）] 属性は、ISE によって識別されるユーザのエンドポイント デバイス タイプです。

[エンドポイント プロファイル（Endpoint Profile）]（[デバイス タイプ（Device Type）]）に基づいてトラフィックを制御するには、アイデンティティ ポリシーを設定し、展開する必要があります。

ユーザ制御用 ISE/ISE-PIC の設定方法

ISE/ISE-PIC は、次の設定のいずれかで使用できます。

- レルム、アイデンティティ ポリシー、および関連付けられたアクセス コントロール ポリシーを使用。

  レルムを使用して、ポリシー内のネットワーク リソースへのユーザ アクセスを制御します。ポリシーでは、ISE/ISE-PIC セキュリティ グループ タグ（SGT）のメタデータを引き続き使用できます。

- アクセス コントロール ポリシーのみを使用。レルムまたはアイデンティティ ポリシーは必要ありません。

  SGT メタデータのみを使用してネットワーク アクセスを制御するには、この方法を使用します。

関連トピック

レルムなしで ISE を設定する方法 （4 ページ）
レルムを使用したユーザ制御用 ISE/ISE-PIC の設定方法 （5 ページ）

レルムなしで ISE を設定する方法

このトピックでは、SGT タグを使用してネットワークへのアクセスを許可またはブロックできるように ISE を設定するために必要なタスクの概要について説明します。

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（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

手順

	コマンドまたはアクション	目的
ステップ 1	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバ、およびFMCの間で安全に接続するために必要です。FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）を参照してください
ステップ 2	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザ アクティビティを制御できます。ユーザ制御用 ISE/ISE-PIC の設定 （10 ページ）を参照してください。
ステップ 3	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元の SGT メタデータを使用できます。アクセス コントロール ルールの概要を参照してください。
ステップ 4	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開を参照してください。

次のタスク

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）

レルムを使用したユーザ制御用 ISE/ISE-PIC の設定方法

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（NGIPSv を除く）	任意（Any）	Administrator/Access Admin/Network Admin

始める前に

このトピックでは、ユーザ制御用 ISE/ISE-PIC を設定し、ユーザまたはグループによるネットワークへのアクセスを許可またはブロックできるようにするために必要なタスクの概要について説明します。ユーザおよびグループは、レルムがサポートされているサーバに記載されている任意のサーバに保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	ISE/ISE-PIC からシステム証明書をエクスポートします。	証明書は、ISE/ISE-PIC pxGrid、モニタリング（MNT）サーバ、およびFMCの間で安全に接続するために必要です。FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）を参照してください
ステップ 2	レルムを作成します。	レルムの作成は、選択したユーザおよびグループによるネットワークへのアクセスを制御するためにのみ必要です。 レルムの作成を参照してください。
ステップ 3	ユーザおよびグループをダウンロードし、レルムを有効にします。	ユーザおよびグループをダウンロードすると、それらをアクセス コントロール ルールで使用できるようになります。ユーザとグループのダウンロードを参照してください。
ステップ 4	ISE/ISE-PIC アイデンティティ ソースを作成します。	ISE/ISE-PIC アイデンティティ ソースを使用すると、ISE/ISE-PIC によって提供されるセキュリティ グループ タグ（SGT）を使用してユーザ アクティビティを制御できます。ユーザ制御用 ISE/ISE-PIC の設定 （10 ページ）を参照してください。
ステップ 5	アイデンティティ ポリシーを作成します。	アイデンティティ ポリシーは、1 つ以上のアイデンティティ ルールのコンテナです。アイデンティティ ポリシーの作成を参照してください。
ステップ 6	アイデンティティ ルールを作成します。	アイデンティティ ルールは、ユーザおよびグループによるネットワークへのアクセスを制御するためにレルムがどのように使用されるかを指定します。アイデンティティ ルールの作成を参照してください。

	コマンドまたはアクション	目的
ステップ 7	アクセス コントロール ポリシーとアイデンティティ ポリシーを関連付けます。	これにより、アクセス コントロール ポリシーがレルム内のユーザとグループを使用できるようになります。
ステップ 8	アクセス コントロール ルールを作成します。	アクセス コントロール ルールは、トラフィックがルール基準に一致する場合に実行するアクション（許可またはブロックなど）を指定します。アクセス コントロール ルール内の一致基準として、送信元の SGT メタデータを使用できます。アクセス コントロール ルールの概要を参照してください。
ステップ 9	管理対象デバイスにアクセス コントロール ポリシーを展開します。	ポリシーを有効にするには、事前に管理対象デバイスに展開しておく必要があります。設定変更の展開を参照してください。

次のタスク

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）

ISE/ISE-PIC の設定

次のトピックでは、FMC のアイデンティティ ポリシーで使用するように ISE/ISE-PIC サーバを設定する方法について説明します。

FMC での認証を行うには、ISE/ISE-PIC サーバから証明書をエクスポートする必要があります。

関連トピック

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）

FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート

ここでは、次のことを行う方法について説明します。

- ISE/ISE-PIC サーバからシステム証明書をエクスポートします。

  これらの証明書は、ISE/ISE-PIC サーバに安全に接続するために必要です。ISE システムの設定に応じ、次のうち 1 つまたは最大 3 つの証明書をエクスポートする必要があります。

  - pxGrid サーバ用の証明書
  - モニタリング（MNT）サーバ用の証明書
  - FMC 用の証明書（秘密キーを含む）

- これらの証明書を FMC にインポートします。

関連トピック

システム証明書のエクスポート （8 ページ）
ISE/ISE-PIC 証明書のインポート （9 ページ）

システム証明書のエクスポート

選択したシステム証明書とその証明書に関連付けられている秘密キーをエクスポートできます。証明書とその秘密キーをバックアップ用にエクスポートする場合は、それらを必要に応じて後で再インポートできます。

始める前に

次のタスクを実行するには、スーパー管理者またはシステム管理者である必要があります。

手順

ステップ 1 **[管理（Administration）] > [システム（System）] > [証明書（Certificates）] > [システム証明書（System Certificates）]** を選択します。

ステップ 2 エクスポートする証明書の横にあるチェックボックスをオンにし、[エクスポート（Export）] をクリックします。

ステップ 3 証明書のみをエクスポートするか、証明書と証明書に関連付けられている秘密キーをエクスポートするかを選択します。

ヒント 値が公開される可能性があるため、証明書に関連付けられている秘密キーのエクスポートは推奨しません。秘密キーをエクスポートする必要がある場合（たとえば、ワイルドカードシステム証明書をエクスポートしてノード間通信用に他のノードにインポートする場合）は、その秘密キーの暗号化パスワードを指定します。このパスワードは、証明書を別の Cisco ISE ノードにインポートするときに指定して、秘密キーを復号化する必要があります。

ステップ 4 秘密キーをエクスポートする場合は、パスワードを入力します。パスワードは、8 文字以上にする必要があります。

ステップ 5 [エクスポート（Export）]をクリックして、クライアントブラウザを実行しているファイルシステムに証明書を保存します。

証明書のみをエクスポートする場合、証明書は Privacy Enhanced Mail 形式で保存されます。証明書と秘密キーの両方をエクスポートする場合、証明書は Privacy Enhanced Mail 形式の証明書と暗号化された秘密キー ファイルを含む .zip ファイルとしてエクスポートされます。

ISE/ISE-PIC 証明書のインポート

この手順は任意です。ユーザ制御用 ISE/ISE-PIC の設定 （10 ページ）で説明されているように、ISE/ISE-PIC アイデンティティソースを作成するときに ISE サーバ証明書をインポートすることもできます。

始める前に

システム証明書のエクスポート （8 ページ）の説明に従って、ISE/ISE-PIC サーバから証明書をエクスポートします。証明書とキーは、FMC へのログイン元のマシンに存在している必要があります。

次の 2 種類の証明書オブジェクトをインポートします。

- ISE/ISE-PIC で認証するための FMC の内部証明書と秘密キー。
- pxGrid および ISE モニタリング（MNT）サーバ用の 1 つ以上の信頼できる認証局（CA）。

  これは、ISE/ISE-PIC システムのセットアップ方法に応じ、2 つの個別の証明書である場合と 1 つの証明書である場合があります。

手順

ステップ 1 FMC にまだログインしていない場合はログインします。

ステップ 2 **[オブジェクト（Objects）]** > **[オブジェクト管理（Object Management）]** をクリックします。

ステップ 3 [PKI] を展開します。

ステップ 4 [内部証明書（Internal Cert）] をクリックします。

ステップ 5 [内部証明書の追加（Add Internal Cert）] をクリックします。

ステップ 6 画面の指示に従って、証明書と秘密キーをインポートします。

ステップ 7 [信頼できるCA（Add Trusted CAs）] をクリックします。

ステップ 8 [信頼できるCAの追加（Add Trusted CA）] をクリックします。

ステップ 9 画面の指示に従って、pxGrid サーバ証明書をインポートします。

ステップ 10 必要に応じ、上記の手順を繰り返して MNT サーバの信頼できる CA をインポートします。

次のタスク

ユーザ制御用 ISE/ISE-PIC の設定 （10 ページ）

ユーザ制御用 ISE/ISE-PIC の設定

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）	任意（Any）	任意（Any）	グローバルだけ	Admin/Access Admin/Network Admin

始める前に

- Microsoft Active Directory サーバまたはサポート対象の LDAP サーバからユーザ セッションを取得するには、レルムの作成の説明に従って、pxGrid ペルソナを想定し、ISE サーバのレルムを設定して有効にします。
- ISE または ISE-PIC への接続を設定します。詳細については、ISE/ISE-PIC アイデンティティ ソース （1 ページ）およびISE/ISE-PIC 設定フィールド （11 ページ）を参照してください。
- ISE/ISE-PIC サーバから証明書をエクスポートし、必要に応じて、FMC で使用するための ISE/ISE-PIC サーバからの証明書のエクスポート （7 ページ）の説明に従って証明書を FMC にインポートします。

手順

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

ステップ 2 **[System]** > **[Integration]** をクリックします。

ステップ 3 [アイデンティティの送信元（Identity Sources）] タブをクリックします。

ステップ 4 [サービス タイプ（Service Type）] で [Identity Services Engine] をクリックし、ISE 接続を有効にします。

（注） 接続を無効にするには、[なし（None）] をクリックします。

ステップ 5 [プライマリ ホスト名/IP アドレス（Primary Host Name/IP Address）]、およびオプションで [セカンダリ ホスト名/IP アドレス（Secondary Host Name/IP Address）] を入力します。

ステップ 6 [pxGrid サーバ CA（pxGrid Server CA）] および [MNT サーバ CA（MNT Server CA）] リストから該当する認証局を、[FMC サーバ証明書（FMC Server Certificate）] リストから適切な証明書をそれぞれクリックします。また、追加アイコン（  ）をクリックして証明書を追加することもできます。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ステップ 7 （オプション）CIDR ブロック表記を使用して [ISE ネットワーク フィルタ（ISE Network Filter）] を入力します。

ステップ 8

ステップ 9 接続をテストするには、[テスト（Test）] をクリックします。

テストが失敗した場合、接続障害に関する詳細については、[その他のログ（Additional Logs）] をクリックします。

次のタスク

- アイデンティティ ポリシーの作成の説明に従い、アイデンティティ ポリシーを使用して、制御するユーザおよびその他のオプションを指定します。
- アクセス制御への他のポリシーの関連付けの説明に従って、アイデンティティ ルールをアクセス コントロール ポリシーに関連付けます。このポリシーは、トラフィックをフィルタし、オプションで検査します。
- 設定変更の展開の説明に従って、使用するアイデンティティ ポリシーとアクセス コントロール ポリシーを管理対象デバイスに展開します。
- ワークフローの使用の説明に従って、ユーザ アクティビティをモニタします。

関連トピック

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 （12 ページ）
信頼できる認証局オブジェクト
内部証明書オブジェクト

ISE/ISE-PIC 設定フィールド

次のフィールドを使用して ISE/ISE-PIC への接続を設定します。

プライマリおよびセカンダリ ホスト名/IP アドレス（Primary and Secondary Host Name/IP Address）

プライマリ（およびオプションでセカンダリ）pxGrid ISE サーバのホスト名または IP アドレス。

指定するホスト名により使用されるポートには、ISE と Firepower Management Center の両方から到達可能である必要があります。

pxGrid サーバ CA（pxGrid Server CA）

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT サーバ CA（MNT Server CA）

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

FMC サーバ証明書（FMC Server Certificate）

ISE/ISE-PIC への接続時、または一括ダウンロードの実行時に Firepower Management Center が ISE/ISE-PIC に提供する必要がある証明書およびキー。

（注） [FMC サーバ証明書（FMC Server Certificate）] には、clientAuth 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE ネットワーク フィルタ（ISE Network Filter）

オプションのフィルタで、ISE が Firepower Management Center にレポートするデータを制限するために設定できます。ネットワーク フィルタを指定する場合、ISE はそのフィルタ内のネットワークからデータをレポートします。次の方法でフィルタを指定できます。

- **任意（`Any`）**のフィルタを指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。
- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの Firepower システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

関連トピック

信頼できる認証局オブジェクト
内部証明書オブジェクト

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

関連の他のトラブルシューティングについては、レルムとユーザのダウンロードのトラブルシュートおよびユーザ制御のトラブルシューティングを参照してください。

ISE または ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE と FirePOWER システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。

- プライマリ サーバが失敗した場合は、セカンダリをプライマリに手動で昇格させる必要があります。自動でフェール オーバーすることはありません。
- ISE サーバと Firepower Management Center の間の接続が成功するには、ISE でクライアントを手動で承認する必要があります。（通常、接続テスト用と ISE エージェント用の 2 つのクライアントがあります）。

  『*Cisco Identity Services Engine Administrator Guide*』の「Managing users and external identity sources」の章で説明しているように、ISE で [新しいアカウントを自動的に承認（Automatically approve new accounts）] を有効にすることもできます。
- [FMC サーバ証明書（FMC Server Certificate）] には、[clientAuth] 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。
- ISE サーバの時刻は、Firepower Management Center の時刻と同期している必要があります。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。
- 展開にプライマリとセカンダリの pxGrid ノードが含まれている場合は、
  - 両方のノードの証明書が、同じ認証局によって署名される必要があります。
  - ホスト名により使用されるポートが、ISE サーバと Firepower Management Center の両方により到達可能である必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE または ISE-PIC によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- 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。ISE ユーザから見えるアクティビティは、システムがユーザのダウンロードで情報の取得に成功するまでアクセス コントロール ルールで処理されず、Web インターフェイスに表示されません。
- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- Firepower Management Center は、ISE ゲスト サービス ユーザのユーザ データを受信できません。
- ISE が TS エージェントと同じユーザをモニタした場合、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 ISE が同じ IP アドレスによる同一の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。
- 使用する ISE バージョンと構成は、Firepower システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （1 ページ）を参照してください。

- Firepower Management Center に高可用性を設定しており、プライマリに障害が発生した場合は、ISE/ISE-PIC のガイドラインと制限事項 （2 ページ）のISE と高可用性に関する項を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。
- ISE-PIC は ISE EPS の修復を実行できません。
- アクティブ FTP セッションは、イベントの **Unknown** ユーザとして表示されます。これは正常な処理です。アクティブ FTP では、（クライアントではない）サーバが接続を開始し、FTP サーバには関連付けられているユーザ名がないはずだからです。アクティブ FTP の詳細については、RFC 959 を参照してください。

サポートされている機能に問題がある場合は、ISE/ISE-PIC アイデンティティ ソース （1 ページ）で詳細を参照してバージョンの互換性を確認してください。

ISE/ISE-PIC の履歴

機能	バージョン（Version）	詳細
ISE-PIC との統合	6.2.1	ISE-PIC のデータを使用できるようになりました。
ユーザ制御用の SGT タグ。	6.2.0	ISE セキュリティ グループ タグ（SGT）データに基づいてユーザ制御を実行するために、レルムまたはアイデンティティ ポリシーを作成する必要がなくなりました。
ISE との統合。	6.0	導入された機能。シスコの Platform Exchange Grid（PxGrid）に登録することで、Firepower Management Center で追加のユーザ データ、デバイス タイプデータ、デバイスロケーションデータ、およびセキュリティ グループ タグ（SGT：ネットワーク アクセス コントロールを提供するために ISE によって使用される方式）をダウンロードできます。