ユーザーアイデンティティの概要

次のトピックでは、ユーザー ID について説明します。

ユーザー アイデンティティについて

ユーザアイデンティティ情報を使用すると、ポリシー違反、攻撃、ネットワークの脆弱性の発生源を特定し、特定のユーザまで遡って追跡することができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者。
- 内部攻撃またはポートスキャンを開始した人物。
- 特定のホストへの不正アクセスを試みている人物。
- 過度に大量の帯域幅を使用している人物。
- 重要なオペレーティング システム更新を適用しなかった人物。
- 会社のポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物。
- ネットワーク上の侵害の兆候に関連付けられている人物。

この情報を入手すれば、システムの他の機能を使用して、リスクを軽減し、アクセス制御を実行し、他のユーザーを破壊行為から保護するためのアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザー アイデンティティ ソースを設定してユーザー データを収集すると、ユーザー認識とユーザー制御を実行できます。

アイデンティティソースの詳細については、ユーザー アイデンティティ ソースについて （3 ページ）を参照してください。

関連トピック

アイデンティティの用語 （2 ページ）
ユーザー アイデンティティ ソースについて （3 ページ）
アイデンティティ導入 （6 ページ）
アイデンティティ ポリシーの設定方法 （7 ページ）

アイデンティティの用語

このトピックでは、ユーザアイデンティティおよびユーザ制御の一般的な用語について説明します。

ユーザー認識

アイデンティティソース（TSエージェントなど）を使用して、ネットワーク上のユーザーを識別します。ユーザー認識によって、権限のあるソース（Active Directory など）および権限のないソース（アプリケーションベース）の両方からユーザーを識別できます。Active Directory をアイデンティティ ソースとして使用するには、レルムおよびディレクトリを設定する必要があります。詳細については、ユーザー アイデンティティ ソースについて （3 ページ）を参照してください。

ユーザー制御

アクセス コントロール ポリシーに関連付けるアイデンティティ ポリシーを構成します。（アイデンティティ ポリシーは、アクセス コントロール サブポリシーと呼ばれるようになります。）アイデンティティ ポリシーはアイデンティティ ソースを指定し、オプションで、そのソースに属するユーザおよびグループを指定します。

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ることで、ネットワークのトラフィックでユーザまたはユーザアクティビティをモニタ、信頼、ブロックまたは許可するかどうかを決定します。詳細については、アクセス制御ポリシーを参照してください。

権限のあるアイデンティティ ソース

信頼できるサーバによってユーザ ログインが検証されています（たとえば、Active Directory）。権限のあるログインから取得したデータを使用すると、ユーザー認識とユーザー制御を実行できます。権限のあるユーザー ログインは、パッシブ認証とアクティブ認証から得られます。

- パッシブ認証は、ユーザーが外部リポジトリ経由で認証されるときに発生します。サポートされているパッシブ認証ユーザーリポジトリは、ISE/ISE-PIC、TS エージェント、および Microsoft Active Directory です。
- アクティブ認証は、ユーザが事前設定済みの管理対象デバイス経由で認証されるときに発生します。アクティブ認証はキャプティブポータルとも呼ばれます。アクティブ認証は通常、パッシブ認証と同じユーザーリポジトリを使用します（例外として、ISE/ISE-PIC、 および TS エージェントはパッシブのみです）。

権限のないアイデンティティ ソース

ユーザー ログインの検証を行った不明または信頼できないサーバー。トラフィックベースの検出は、システムでサポートされている唯一の権限のないアイデンティティ ソースです。権限のないログインから取得されたデータを使用すると、ユーザー認識を実行できます。

ユーザー アイデンティティ ソースについて

次の表に、システムでサポートされているユーザー アイデンティティ ソースの概要を示します。各アイデンティティ ソースは、ユーザー認識のためのユーザーの記憶域を提供します。これらのユーザーは、アイデンティティおよびアクセス コントロール ポリシーで制御できます。

ユーザーアイデンティティ ソース	サーバー要件	ログインタイプ	認証タイプ（Authentication Type）	ユーザ制御	詳細については、次を参照してください。
キャプティブ ポータル	OpenLDAP Microsoft Active Directory	権威あり	アクティブ	はい	キャプティブ ポータルのアイデンティティ ソース
パッシブ認証	OpenLDAP Microsoft Active Directory	権威なし	アクティブ	はい	LDAP レルムまたは Active Directory レルムおよびレルム ディレクトリの作成
TS エージェントによるパッシブ認証	Microsoft Windows Terminal Server	権威あり	パッシブ	はい	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
リモート アクセス VPN	OpenLDAP または Microsoft Active Directory	権威あり	アクティブ	はい	リモート アクセス VPN アイデンティティ ソース
	RADIUS	権威あり	Active	非対応、認識のみ	
ISE/ISE-PIC	Microsoft Active Directory	権威あり	パッシブ	はい	ISE/ISE-PIC アイデンティティ ソース
トラフィック ベースの検出 （ネットワーク検出ポリシーで設定）。	—	権威なし	—	非対応、認識のみ	トラフィック ベース検出のアイデンティティ ソース

展開するアイデンティティ ソースを選択する際には、以下を検討してください。

- 非 LDAP ユーザー ログインにはトラフィック ベースの検出を使用する必要があります。
- 失敗したログインまたは認証アクティビティを記録するには、トラフィック ベースの検出またはキャプティブ ポータルを使用する必要があります。失敗したログインまたは認証試行で新しいユーザーがデータベース内のユーザーのリストに追加されることはありません。
- キャプティブ ポータルのアイデンティティ ソースには、ルーテッド インターフェイスを備えた管理対象デバイスが必要です。キャプティブ ポータルでインライン（タップ モードとも呼ばれます）インターフェイスを使用することはできません。

これらのアイデンティティ ソースからのデータは、Secure Firewall Management Center のユーザー データベースとユーザー アクティビティ データベースに格納されます。Secure Firewall Management Center サーバー ユーザー ダウンロードを設定して、新しいユーザー データがデータベースに自動的かつ定期的にダウンロードされるようにできます。

必要なアイデンティティ ソースを使用してアイデンティティ ルールを設定したら、各ルールにアクセス コントロール ポリシーを関連付け、ポリシーを有効にするために管理対象デバイスに展開する必要があります。アクセス コントロール ポリシーおよび展開の詳細については、アクセス制御への他のポリシーの関連付けを参照してください。

ユーザーアイデンティティの一般情報については、ユーザー アイデンティティについて （1 ページ）を参照してください。

ユーザーアイデンティティのベストプラクティス

アイデンティティポリシーを設定する前に、次の情報を確認することを推奨します。

- ユーザー制限を把握します
- ヘルスモニター
- ISE/ISE-PIC の最新バージョン、2 種類の修復を使用します
- ユーザーエージェントのサポートは 6.7 で終了します
- キャプティブポータルには、ルーテッドインターフェイスと、いくつかの個別のタスクが必要です

Microsoft Active Directory および LDAP

システムは、ユーザーの認識および管理のために、Active Directory、LDAP などのユーザーレポジトリをサポートしています。Active Directory または LDAP リポジトリと Secure Firewall Management Center の間の関連付けは、レルムと呼ばれます。LDAP サーバーまたは Active Directory ドメインごとに 1 つのレルムを作成する必要があります。サポートされているバージョンの詳細については、レルムがサポートされているサーバーを参照してください。

LDAP でサポートされるユーザー アイデンティティ ソースは、キャプティブポータルのみです。（ISE/ISE-PIC を除く）他のアイデンティティソースを使用するには、Active Directory を使用する必要があります。

Active Directory の場合のみ：

- ドメインコントローラごとに 1 つのディレクトリを作成します。

  詳細については、「LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成」を参照してください。

- 2 つのドメイン間の信頼関係にあるユーザーとグループは、すべての Active Directory ドメインとドメインコントローラを、それぞれレルムとディレクトリとして追加した場合にサポートされます。

  詳細については、レルムおよび信頼できるドメインを参照してください。

ヘルスモニター

Secure Firewall Management Center ヘルスモニターは、次のようなさまざまな Secure Firewall Management Center 機能のステータスに関する重要な情報を提供します。

- ユーザー/レルムの不一致
- Snort メモリ使用率
- ISE 接続のステータス

ヘルスモジュールの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Health Modules」を参照してください。

ヘルスモジュールをモニターするポリシーを設定するには、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Creating Health Policies」を参照してください。

デバイス固有のユーザー制限

すべての物理または仮想 Firewall Management Center デバイスには、ダウンロードできるユーザー数に制限があります。ユーザー制限に達すると、Firewall Management Center がメモリを使い果たし、結果として機能の信頼性が低下する可能性があります。

ユーザー制限については、Microsoft Active Directory のユーザー制限 （14 ページ）で説明しています。

ISE/ISE-PIC アイデンティティ ソースを使用する場合は、オプションで、アイデンティティ ポリシーの作成で説明されているようにアイデンティティ マッピング フィルタを使用して、Firewall Management Center がモニターするサブネットを制限し、メモリ使用率を減らすことができます。

ISE/ISE-PIC の最新バージョンの使用

ISE/ISE-PIC アイデンティティ ソースを使用する場合は、常に最新バージョンを使用して、最新の機能とバグ修正を確実に入手することを強く推奨します。

pxGrid 2.0（バージョン 2.6 パッチ 6 以降、または 2.7 パッチ 2 以降で使用）も、ISE/ISE-PIC で使用される修復を、エンドポイント保護サービス（EPS）から適応型ネットワーク制御（ANC）に変更します。ISE/ISE-PIC をアップグレードする場合は、修復ポリシーを EPS から ANC に移行する必要があります。

ISE/ISE-PIC の使用に関する詳細については、ISE/ISE-PIC の注意事項と制限事項を参照してください。

ISE/ISE-PIC アイデンティティ ソースを設定するには、ユーザー制御用 ISE/ISE-PIC の設定方法を参照してください。

キャプティブポータルの情報

TS エージェントの情報

TS エージェントのユーザー アイデンティティ ソースは、Windows Terminal Server 上のユーザーセッションを識別するために必要です。『Cisco Terminal Services (TS) Agent Guide』で説明されているように、TS エージェントソフトウェアをターミナルサーバーマシンにインストールする必要があります。また、TS エージェントサーバーと Secure Firewall Management Center の時計を同期させる必要があります。

TS エージェントのデータは [ユーザ（Users）] テーブル、[ユーザ アクティビティ（User Activity）] テーブル、および [接続イベント（Connection Event）] テーブルに表示され、ユーザ認識とユーザ制御に使用できます。

詳細については、TS エージェントのガイドラインを参照してください。

アイデンティティポリシーとアクセス コントロール ポリシーの関連付け

レルム、ディレクトリ、およびユーザーアイデンティティ ソースを設定したら、アイデンティティポリシーでアイデンティティルールを設定する必要があります。ポリシーを有効にするには、アイデンティティポリシーとアクセス コントロール ポリシーを関連付ける必要があります。

アイデンティティポリシーの作成の詳細については、アイデンティティ ポリシーの作成を参照してください。

アイデンティティルールの作成の詳細については、アイデンティティ ルールの作成を参照してください。

アイデンティティポリシーとアクセス コントロール ポリシーを関連付けるには、アクセス制御への他のポリシーの関連付けを参照してください。

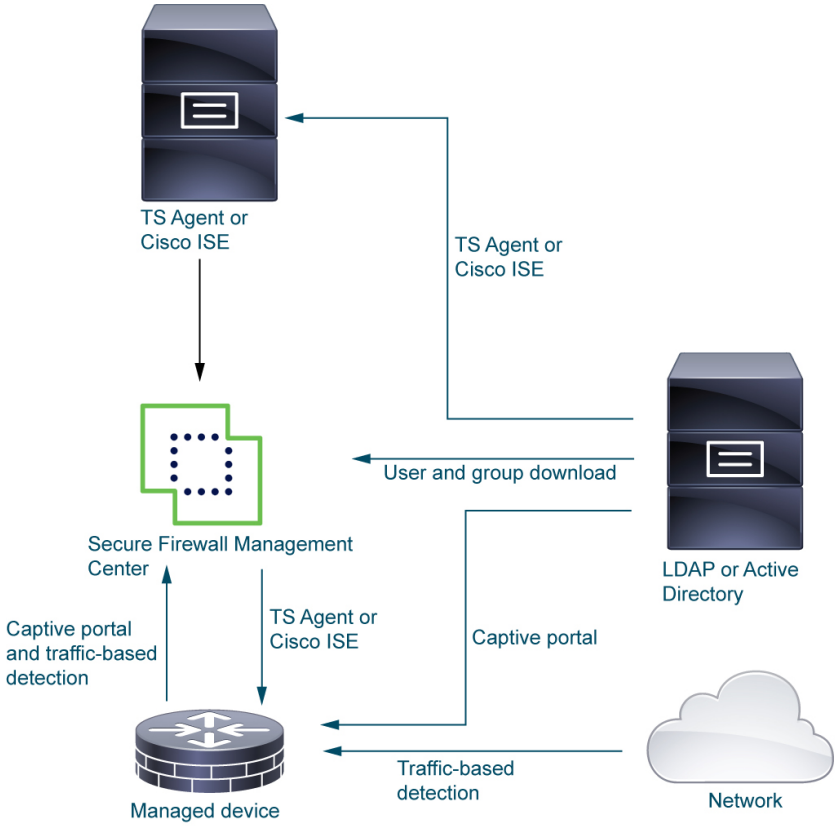
アイデンティティ導入

システムがユーザー ログイン、またはアイデンティティ ソースからのユーザー データを検出すると、そのログインからのユーザーは、Secure Firewall Management Center ユーザー データベース内のユーザーのリストに照らしてチェックされます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP

トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザーは Secure Firewall Management Center で確認されるとすぐに、そのユーザーが属するグループと関連付けられます。

次の図は、ユーザーデータの収集および保存の仕組みを示しています。



アイデンティティ ポリシーの設定方法

このトピックでは、使用可能な任意のユーザー アイデンティティ ソース（TS エージェント、ISE/ISE-PIC、キャプティブポータルを使用してアイデンティティポリシーを設定する方法の概要を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意）レルムとディレクトリを作成します。ユーザー制御で使用するユーザーを含むフォレスト内のドメインごとに1つのレルムを作成します。また、ドメイ	次のいずれかに該当する場合、レルム、レルムディレクトリの作成はオプションです。

	コマンドまたはアクション	目的
	ンコントローラごとに1つのディレクトリを作成します。アイデンティティポリシーでは、対応する Firewall Management Center レルムとディレクトリを持つユーザーとグループのみを使用できます。	• SGT ISE 属性条件を設定することを計画しているものの、ユーザー、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。 • ネットワークトラフィックをフィルタ処理するためだけにアイデンティティポリシーを使用している。 レルムとは、信頼されたユーザおよびグループの領域で、Microsoft Active Directory リポジトリなどがあります。Firewall Management Center は、指定した間隔でユーザーとグループをダウンロードします。ユーザとグループは、ダウンロードに含めることも、ダウンロードから除外することもできます。 LDAP レルムまたは Active Directory レルムおよびレルムディレクトリの作成を参照してください。レルムを作成するためのオプションの詳細については、レルム フィールドを参照してください。 ディレクトリとは、コンピュータ ネットワークのユーザーとネットワーク共有に関する情報を編成する Active Directory ドメイン コントローラのことです。Active Directory コントローラはレルムにディレクトリ サービスを提供します。Active Directory は、ユーザー オブジェクトやグループ オブジェクトを複数のドメイン コントローラ間に分散させます。これらのドメインコントローラは、ディレクトリ サービスを使用してローカルの変更を互いに伝達するピアです。詳細については、MSDN の『Active Directory technical specification glossary』[英語] を参照してください。 1つのレルムに複数のディレクトリを指定できます。この場合、ユーザー制御用のユーザー クレデンシャルとグループ クレデンシャルを照合するために、その

	コマンドまたはアクション	目的
		レルムの[ディレクトリ（Directory）]タブ ページにリストされている順序で、各ドメイン コントローラがクエリされます。 （注） SGT ISE 属性条件の設定を計画しているものの、ユーザー、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、レルムまたはレルムシーケンスの設定はオプションです。
ステップ 2	レルムからユーザーとグループを同期します。	ユーザーとグループを制御するには、それらを Firewall Management Center と同期する必要があります。必要に応じて手動でユーザーとグループと同期することも、指定した間隔でシステムがそれらと同期するように設定することもできます。 ユーザーとグループを同期するときに、例外を指定できます。たとえば、そのレルムのすべてのユーザー制御から Engineering というグループを除外したり、Engineering グループに適用されるユーザー制御から **joe.smith** というユーザーを除外したりできます。 参照先 ユーザーとグループの同期
ステップ 3	（任意）レルムシーケンスを作成します。	レルムシーケンスは、レルムの順序付きリストであり、アイデンティティポリシーで使用すると、システムは指定された順序でレルムを検索して、ルールに一致するユーザーを見つけます。レルムシーケンスの作成を参照してください。
ステップ 4	ユーザ データやグループ データを取得するための手法（アイデンティティ ソース）を作成します。	レルムに保存されたデータを使用してユーザーやグループを制御するには、固有の設定を使ってアイデンティティソースをセットアップします。アイデンティティソースには、TSエージェント、キャプティブポータル、またはリモートVPN

	コマンドまたはアクション	目的
		が含まれます。次のいずれかを参照してください。 • ユーザー制御のためのキャプティブ ポータルの設定方法 • ユーザー制御用 RA VPN の設定
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 ポリシーには、1つ以上のアイデンティティ ルールが含まれており、 必要に応じてこれらをカテゴリにまとめることができます。アイデンティティ ポリシーの作成を参照してください。 （注） SGT ISE 属性条件を設定することを計画しているものの、ユーザー、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、または ID ポリシーのみを使用してネットワークトラフィックをフィルタ処理する場合、レルムまたはレルムシーケンスの設定はオプションです。
ステップ 6	1つ以上のアイデンティティ ルールを作成します。	アイデンティティルールを使用すると、認証の種類、ネットワークゾーン、ネットワークまたは地理位置情報、レルム、レルムシーケンスなど、多数の一致条件を指定できます。アイデンティティ ルールの作成を参照してください。
ステップ 7	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 コントロール ポリシーはトラフィックをフィルタリングし、必要に応じてトラフィックを検査します。アイデンティティポリシーを有効にするには、アクセス コントロール ポリシーを関連付ける必要があります。アクセス制御への他のポリシーの関連付けを参照してください。
ステップ 8	少なくとも1つの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。	ポリシーを使用してユーザー アクティビティを制御するには、クライアントの接続先となる管理対象デバイスにそのポ

	コマンドまたはアクション	目的
		リシーを展開する必要があります。設定変更の展開を参照してください。
ステップ 9	ユーザー アクティビティをモニターします。	ユーザー アイデンティティ ソースによって収集されたアクティブ セッションの一覧、またはユーザーアイデンティティ ソースによって収集されたユーザー情報の一覧を確認します。Cisco Secure Firewall Management Center アドミニストレーション ガイド の「ワークフローの使用」を参照してください。 次のすべてに該当する場合、アイデンティティ ポリシーは必要ありません。 • ISE/ISE-PIC アイデンティティ ソースを使用できます。 • アクセス コントロール ポリシーのユーザまたはグループは使用しません。 • アクセス コントロール ポリシーのセキュリティ グループ タグ（SGT）を使用します。詳細については、「ISE SGT とカスタム SGT ルール条件との比較」を参照してください。

関連トピック

トラフィックに基づくユーザー検出の設定

ユーザー アクティビティ データベース

Secure Firewall Management Center のユーザ アクティビティ データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたネットワーク上のユーザ アクティビティのレコードが含まれています。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき。
- 新しいユーザを検出したとき。
- システム管理者が手動でユーザを削除したとき。
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ数の制限に達したためにそのユーザを追加できなかったとき。

- ユーザーに関連付けられている侵害の兆候を解決したとき、またはユーザーに対して侵害の兆候ルールを有効または無効にしたとき。

（注） TS エージェントが別のパッシブ認証のアイデンティティソース（ISE/ISE-PIC など）と同じユーザーをモニターする場合、Firewall Management Center では TS エージェントのデータを優先します。同じ IP アドレスからの同じアクティビティが TS エージェントと別のパッシブソースから報告される場合、TS エージェントのデータだけが Firewall Management Center に記録されます。

システムで検出されたユーザーアクティビティは、Secure Firewall Management Centerを使用して表示できます（**[分析（Analysis）] > [ユーザー（Users）] 見出し > [ユーザーアクティビティ（User Activity）]**）。

ユーザ データベース

Secure Firewall Management Center のユーザー データベースには、設定されたすべてのアイデンティティ ソースによって検出または報告されたユーザーごとのレコードが含まれています。権限のあるソースから取得したデータをユーザ制御に使用できます。

サポートされている権限のないアイデンティティ ソースと権限のあるアイデンティティ ソースの詳細については、ユーザー アイデンティティ ソースについて （3 ページ） を参照してください。

Microsoft Active Directory のユーザー制限 （14 ページ） で説明されているように、Secure Firewall Management Center で保存できるユーザーの合計数は Secure Firewall Management Center のモデルによって異なります。ユーザ制限に達した後、システムは、アイデンティティ ソースに基づいて未検出ユーザ データを次のように優先順位付けします。

- 新しいユーザーが権限のないアイデンティティ ソースからである場合、ユーザーはデータベースに追加されません。新規ユーザを追加できるようにするには、手動またはデータベースの消去によってユーザを削除する必要があります。
- 新しいユーザーが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザーを削除し、データベースに新しいユーザーを追加します。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは Secure Firewall Management Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。システムによって保存されるデータのタイプの詳細については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「*User Data*」を参照してください。

Firewall Management Center の高可用性が設定済みで、プライマリに障害が発生した場合、キャプティブポータル、ISE/ISE-PIC、TS エージェント、またはリモートアクセス VPN デバイスから報告されるログインはフェールオーバー ダウンタイム中に識別不能になります（ユーザーが以前に確認されて Firewall Management Center にダウンロードされている場合も同様）。識別さ

れていないユーザーは、Firewall Management Center で [不明（Unknown）] のユーザーとして記録されます。ダウンタイム後、不明のユーザーはアイデンティティ ポリシーのルールに従って再確認され、処理されます。

（注） TS エージェントが別のパッシブ認証の ID ソース（ISE/ISE-PIC）と同じユーザーをモニターしている場合、Firewall Management Center は TS エージェントのデータを優先します。同じ IP アドレスからの同じアクティビティが TS エージェントと別のパッシブソースから報告される場合、TS エージェントのデータだけが Firewall Management Center に記録されます。

システムが新しいユーザ セッションを検出すると、そのユーザ セッションのデータは、次のいずれかが発生するまでユーザ データベースに残ります。

- Firewall Management Center のユーザーが手動でユーザーセッションを削除した。
- アイデンティティ ソースがそのユーザー セッションのログオフを報告した。
- レルムがレルムの [ユーザーセッションのタイムアウト：認証されたユーザー（User Session Timeout: Authenticated Users）] 設定、[ユーザー セッションのタイムアウト：認証に失敗したユーザー（User Session Timeout: Failed Authentication Users）] 設定、または [ユーザー セッションのタイムアウト：ゲスト ユーザー（User Session Timeout: Guest Users）] 設定で指定されているユーザー セッションを終了した。

Firepower システムのホストとユーザーの制限

Secure Firewall Management Center モデルにより、展開でモニターできる個別のホストの数、モニターし、ユーザー制御を実行するために使用できるユーザーの数が決定されます。

ホスト制限（Host Limit）

システムは（ネットワーク検出ポリシーで定義されている）モニタ対象ネットワークで IP アドレスに関連付けられたアクティビティを検出すると、ネットワーク マップにホストを追加します。Secure Firewall Management Center がモニタでき、ネットワーク マップに保存できるホストの数。モデルによって異なります。

表 *1 : Secure Firewall Management Center* モデル別のホスト制限

Firewall Management Center モデル	ホスト
MC1000	50,000
MC1600	50,000
MC2500	150,000

Firewall Management Center モデル	ホスト
MC2600	150,000
MC4500	600,000
MC4600	600,000
仮想	50,000

ネットワーク マップに存在しないホストのコンテキスト データは表示できません。ただし、アクセス制御は実行できます。たとえば、コンプライアンス allow リストを使用してホストのネットワーク コンプライアンスをモニターできない場合でも、ネットワークマップに存在しないホストとの間のトラフィックでアプリケーション制御を実行できます。

（注） システムでは、IPアドレスとMACアドレスの両方によって識別されるホストとは別に、MAC専用ホストがカウントされます。1つのホストに関連付けられているすべてのIPアドレスは、まとめて1つのホストとしてカウントされます。

ホスト制限への到達とホストの削除

ホスト制限に到達した後に新しいホストを検出すると、ネットワーク検出ポリシーが制御を行います。新しいホストをドロップするか、または非アクティブになっている期間が最も長いホストを置換することができます。また、システムが非アクティブであるためネットワークからホストを削除するまでの期間を設定できます。ホスト、サブネット全体、またはすべてのホストをネットワーク マップから手動で削除できますが、システムは、削除されたホストに関連付けられたアクティビティを検出した場合は、ホストを再追加します。

関連トピック

ネットワーク検出のデータ ストレージ設定

Microsoft Active Directory のユーザー制限

ユーザー制限について

Firewall Management Center モデルにより、モニターできる個々のユーザー数が決まります。ユーザーは、次の場合に Firewall Management Center ユーザーデータベースに追加されます。

- ユーザーはレルムからダウンロードされます。
- キャプティブポータルまたは RA-VPN のユーザーがログインします。
- ユーザーは、任意のアイデンティティソース（たとえば、TS エージェント）から検出されます。

権限のあるユーザのみがアクセス コントロール ポリシーによるユーザ制御を使用できます。

次の点に注意してください。

- ダウンロードユーザーの最大数は、Firewall Management Center モデルによって異なります。
- 同時ユーザーセッション（つまり、ログイン）の最大数は、管理対象デバイスモデルによって異なります。1 人のユーザーが、異なる固有の IP アドレスから複数のセッションを持つことができます。

（注） システムは、すべてのユーザーセッションをすべての Firewall Threat Defense デバイスにダウンロードします。異なるユーザーの同時ユーザーセッション制限を持つデバイスがある場合、メモリが設定された制限に達すると、制限が最小である Firewall Threat Defense が正常性警告を報告します。（たとえば、Firewall Management Center が Firepower 2110 と 4125 を管理している場合、同時ユーザーセッション数が最大の 64,000 に近づくと、2110 が正常性警告を報告します。）

Microsoft Active Directory のユーザー制限

表 *2 : Firewall Threat Defense* 別の最大同時ユーザーログイン制限

Firewall Threat Defense モデル	レルムあたりの最大同時ユーザーログイン数
Firewall Threat Defense Virtual 5、10、20、30、50（サポートされる任意のハイパーバイザ）	64,000
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130 Cisco Secure Firewall 3105、3110、3120	64,000
Firepower 2140 Cisco Secure Firewall 3130、3140 Firepower 4112、4115、4125	150,000
Firepower 4145 Firepower 9300	300,000

ユーザー制限は、Microsoft Active Directory レルムごとに適用されます。1 つのレルムに最大ユーザー数を超えるユーザーをダウンロードしようとした場合、最大数に達するとダウンロードが停止し、正常性アラートが表示されます。一方、最大ユーザー数を超えるユーザーを複数のレルムにダウンロードする場合は、ダウンロードは成功します（いずれか 1 つのレルムのユーザー数が 150,000 を超える場合を除きます。この場合、そのレルムのダウンロードは失敗します）。

表 *3 : Firewall Management Center* モデルごとの最大ダウンロードユーザー数

Firewall Management Center モデル	最大ダウンロードユーザー数
FMC 1000	50,000
FMC 1600	50,000
FMC 2500	150,000
FMC 2600	150,000
FMC 4500	600,000
FMC 4600	600,000
Firewall Management Center Virtual（サポートされる任意のハイパーバイザ）	50,000
Firewall Management Center Virtual 300（サポートされる任意のハイパーバイザ）	150,000

制限に達してから、新しい、以前検出されなかったユーザーをシステムが検出すると、アイデンティティ ソースに基づいてユーザー データに優先順位が付けられます。

- 新しいユーザが権限のないソースからである場合、権限のないユーザはデータベースに追加されません。新規ユーザを追加できるようにするには、手動でユーザを削除するか、データベースを消去する必要があります。
- 新しいユーザが権限のあるアイデンティティ ソースからである場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザを削除し、データベースに新しい権限のあるユーザを追加します。

  権限のあるユーザー以外いない場合、システムは最も長い期間にわたって非アクティブのままになっている権限のないユーザーを削除し、データベースに新しいユーザーを追加します。

トラブルシューティング情報は、ユーザー制御のトラブルシューティングにあります。

ヒント トラフィック ベースの検出を使用している場合、プロトコルによるユーザー ロギングを制限すると、ユーザー名の散乱を最小限に抑え、データベースのスペースを残しておくことができます。たとえば、システムが AIM、POP3、および IMAP トラフィックで検出されたユーザーを追加できないようにすることができます（モニターを望んでいない特定の契約業者または訪問者からのトラフィックであることがわかっているため）。

アイデンティティ レルムの制限

Firewall Threat Defense モデルに関係なく、最大 25 のレルムに制限されます。同じ制限が クラウド提供型 Firewall Management Center にも適用されます。

システムにダウンロードできる ユーザー の数は、次に記載されている情報に従って制限されます。

Microsoft Active Directory のユーザー制限 （14 ページ）

Microsoft Azure Active Directory レルムのユーザー制限

Microsoft Azure Active Directory のユーザー制限

ユーザー制限について

Firewall Management Center モデルにより、モニターできる個々のユーザー数が決まります。

次の点に注意してください。

- ダウンロードユーザーの最大数は、Firewall Management Center モデルによって異なります。
- 同時ユーザーセッション（つまり、ログイン）の最大数は、管理対象デバイスモデルによって異なります。1 人のユーザーが、異なる固有の IP アドレスから複数のセッションを持つことができます。

（注） システムは、すべてのユーザーセッションをすべての Firewall Threat Defense デバイスにダウンロードします。異なるユーザーの同時ユーザーセッション制限を持つデバイスがある場合、メモリが設定された制限に達すると、制限が最小である Firewall Threat Defense が正常性警告を報告します。（たとえば、Firewall Management Center が Firepower 2110 と 4125 を管理している場合、同時ユーザーセッション数が最大の 64,000 に近づくと、2110 が正常性警告を報告します。）

次の表を参照してください。

表 *4 : Firewall Management Center* モデルごとの最大ダウンロードユーザー数[1]

Firewall Management Center モデル	Cisco Secure 動的属性コネクタ コネクタの数	最大ダウンロードユーザー数
FMC1600、FMC1700	10	50,000

Firewall Management Center モデル	Cisco Secure 動的属性コネクタ コネクタの数	最大ダウンロードユーザー数
FMC2600、FMC2700	20	150,000
FMC4600、FMC4700	30	600,000
Firewall Management Center Virtual（サポートされる任意のハイパーバイザ）	10	50,000
Firewall Management Center Virtual 300（サポートされる任意のハイパーバイザ）	20	150,000

[1]：Firewall Management Center モデルは、生産終了および販売終了の対象となります。詳細については、サポート終了と販売終了のお知らせを参照してください。

表 *5 : Firewall Threat Defense* 別の最大同時ユーザーログイン制限

Firewall Threat Defense モデル	最大同時ユーザ ログイン
Firewall Threat Defense Virtual 5、10、20、30、50（サポートされる任意のハイパーバイザ）	50,000
Firepower 1010、1120、1140、1150 Firepower 2110、2120、2130 Secure Firewall 3110、3120、3130、3140	50,000
Firepower 2140 Cisco Secure Firewall 3130、3140	150,000
Firepower 4140、4145、4150 Firepower 9300	225,000

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。