ユーザ エージェントによるユーザの制御

次のトピックでは、ユーザエージェント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。

ユーザ エージェントのアイデンティティ ソース

Cisco Firepower User Agent は、パッシブ認証方法で、信頼できるアイデンティティ ソース（つまり、信頼された Active Directory サーバでユーザ情報が提供されます）でもあります。ユーザエージェントは、Firepower システムと統合されると、ユーザが Active Directory クレデンシャルでホストにログインする、またはホストからログアウトするときに、そのユーザをモニタします。ユーザ エージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。

ユーザ エージェントは、各ユーザを IP アドレスと関連付けます。これにより、ユーザ条件を使用するアクセス コントロール ルールをトリガーすることができます。1 つのユーザ エージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタでき、最大 5 つの Firepower Management Center に暗号化データを送信できます。

ユーザ エージェントは失敗したログイン試行を報告しません。

ユーザ エージェントのガイドライン

ユーザ エージェントは、以下を含む段階的な設定が必要です。

- ユーザ エージェントがインストールされている少なくとも 1 台のコンピュータ 。
- ユーザ エージェントがインストールされたコンピュータまたは Active Directory サーバと Firepower Management Center との間の接続。

- ユーザ エージェントからユーザ データを受け取る各 Firepower Management Center で設定されたアイデンティティ レルム。

段階的なユーザ エージェントの設定とサーバの要件の詳細については、『*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド』を参照してください。

（注） コンピュータまたは Active Directory 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。

Firepower Management Center接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ エージェント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は、そのようなユーザ名のログイン データは Firepower Management Center に報告されません。ユーザ エージェントのデータは、Firepower Management Center のユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を Firepower Management Center に送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを防ぐ方法の詳細については、『*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド』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

ユーザエージェント接続に問題が起こった場合は、*Cisco Firepower* ユーザ エージェント コンフィギュレーション ガイド を確認してください。

このガイドの関連するトラブルシューティング情報については、レルムとユーザのダウンロードのトラブルシュートと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。

ユーザ エージェント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ユーザ 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。ユーザのアクティビティ

は、システムがユーザのダウンロードでユーザに関する情報の取得に成功するまで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。

- Firepower Management Center のハイ アベイラビリティが設定されており、プライマリが失敗した場合、たとえ以前ユーザを確認できており、Firepower Management Center にダウンロード済みであっても、フェールオーバーダウンタイム中にユーザエージェントが報告したすべてのログインが特定不能となります。未確認のユーザは Firepower Management Center には不明なユーザとして記録されます。ダウンタイム後、[不明（Unknown）] ユーザはアイデンティティ ポリシーのルールに従って再び識別され、処理されます。
- ユーザ エージェントが TS エージェントと同じユーザをモニタした場合、システムは TS エージェントのデータを優先します。TS エージェントとユーザエージェントが同じ 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ログに記録されます。
- 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。

ユーザ エージェントの履歴

機能	バージョン（Version）	詳細
ユーザ制御用のユーザ エージェント。	—	バージョン 6.0 よりも前に導入された機能です。ユーザエージェントにより Active Directory ユーザのログインの詳細が提供され、ユーザ認識とユーザ制御に使用できます。