ユーザエージェントの概要

バージョン 2.5 のユーザエージェントは、バージョン 6.4 以降の Firepower システム管理対象デバイスと連携してユーザデータを収集します。ユーザアクセス制御を実装するためにもユーザエージェントが不可欠です。

ユーザエージェントは最大 5 つの Microsoft Active Directory サーバをモニタし、Active Directory によって認証されるログインとログオフをレポートします。Firepower システムは、これらのレコードと、管理対象デバイス上でのトラフィックベースの検出により収集した情報を統合します。

注意 ユーザエージェントのサポート期間の終了が近づいています。Firepower Management Center バージョン 6.6 が、ユーザエージェントを有効にできる最後のバージョンです。Firepower Management Center 6.7 ではユーザエージェントを有効にできません。6.7 にアップグレードすると、アップグレードする前にユーザエージェントを無効にするように警告されます。

FMC バージョン 6.7 にアップグレードする前に、Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）に移行する必要があります。

詳細については、ユーザエージェントでの FMC サポートの終了（1-6 ページ）を参照してください。

注 バージョン 2.5 のユーザエージェントは、Firepower Management Center バージョン 6.4 以降でのみ動作します。ユーザエージェントとご使用の Firepower Management Center のバージョンに問題がある場合は、ユーザ エージェントのトラブルシューティング（2-36 ページ）の説明に従ってバージョン 2.5 のユーザエージェントをそれ以前のバージョンのユーザエージェントに置き換えることができます。

ユーザエージェントについて

このセクションでは、Firepower システムにユーザ検出を実装する上でユーザエージェントが果たす役割に焦点を当てています。ユーザ検出、ネットワーク検出、およびアイデンティティソースに関連するすべての概念のより詳細な説明については、ご使用のシステムのコンフィギュレーション ガイドを参照してください。

詳細については、次の項を参照してください。

- ユーザ エージェントの基礎（1-2 ページ）
- 複数のユーザ エージェントの展開（1-5 ページ）
- レガシー エージェントのサポート（1-6 ページ）
- バージョン 6.x のユーザ エージェント、ISE、およびアクセス制御について（1-6 ページ）

ユーザ エージェントの基礎

Firepower システム は、組織の Active Directory サーバからユーザ ID とユーザアクティビティ情報の両方を取得できます。ユーザ エージェントでは、ユーザが Microsoft Active Directory サーバと認証する際に、そのユーザをモニタできます。

注　ユーザ制御を実行するには、組織で Microsoft Active Directory が使用されている*必要*があります。Firepower システムは、Active Directory サーバをモニタするユーザ エージェントを使用してユーザと IP アドレスを関連付けます。その結果、アクセス制御ルールをトリガーできるようになります。

ユーザ エージェントのインストールと使用により、ユーザ コントロールを実行できるようになります。エージェントはユーザ名と 1 つ以上の IP アドレスを関連付け、この情報によりユーザの条件でアクセス制御規則をトリガーできます。

ユーザ制御を実行するためのユーザ エージェントの完全な設定には以下が含まれます。

- エージェントがインストールされているコンピュータ。
- Management Center とユーザ エージェント コンピュータとの間の接続。
- 各 Management Center から監視対象 Active Directory サーバへの接続。
- このバージョンのユーザ エージェントは、Firepower Management Center 6.2.3 以降でサポートされています。

ユーザ制御の詳細については、各システムの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 エージェントは、監視対象の Microsoft Active Directory サーバに TCP/IP でアクセスできる任意の Microsoft Windows Vista、Microsoft Windows 7、Microsoft Windows 8、Microsoft Windows Server 2008、または Microsoft Windows Server 2012 コンピュータにインストールできます。サポートされるオペレーティング システムの 1 つを実行する Active Directory サーバ上にエージェントをインストールすることもできますが、そのようにすると安全性は低くなります。

注　ユーザ エージェントを Windows Server 2003 またはそれ以前のオペレーティング システムにインストールする場合、ユーザ エージェントは Active Directory コンピュータからのリアルタイム統計を収集できません。

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。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 Management Center に報告されません。

エージェントのモニタリング、ポーリング、およびレポート

各ユーザ エージェントは、定期スケジュールされたポーリングまたはリアルタイム モニタリングのいずれかによって、暗号化されたトラフィックを使用して権限のあるログインをモニタできます。

次に示すのは、ユーザ エージェントが Management Center に報告するいくつかのイベントです。

- **ユーザ ログイン**:ユーザが、最後に表示されたユーザ名に関連していない IP アドレスを持つコンピュータにログインするときに発生します。

  つまりたとえば、月曜日にユーザ名 `james.harvey` が IP アドレス 192.0.2.100 にログインしたとします。火曜日に、`james.harvey` は IP アドレス 192.0.2.105 にログインします。このログインでは、Management Center でユーザ ログイン イベントがトリガーされます。

ユーザ ログイン イベントは、ユーザがワークステーションに直接ログインするか、またはリモート デスクトップを使用するときに発生します。

- **ユーザ ログオフ**：ユーザが IP アドレスからログアウトするときに発生します。ユーザ ログオフ イベントは、コンピュータからユーザがログオフした直後ではなく設定可能な間隔で Management Center に報告されます。
- **新規ユーザ ID**：ユーザ名が IP アドレスに初めて関連付けられたときに発生する 1 回限りのイベント。
- **ユーザ ID の削除**：Management Center 管理者がユーザ ID を削除すると発生します。

ログイン データとログオフ データを組み合わせることで、ネットワークにログインしたユーザをより完全に把握できます。

Active Directory サーバのポーリングによって、エージェントは定義されたポーリング間隔でユーザ アクティビティ データをまとめて取得できます。リアルタイム モニタリングは、Active Directory サーバがデータを受信するとすぐに、ユーザ アクティビティ データをエージェントに送信します。

特定のユーザ名または IP アドレスに関連付けられたログインまたはログオフの報告を除外するように、エージェントを設定できます。これはたとえば次への繰り返しログインを除外するために役立てることができます。

- 共有サーバ（ファイル共有、プリント サーバなど）
- ユーザ エージェント コンピュータ
- Active Directory サーバ
- トラブルシューティング目的のコンピュータへのログイン

最大 5 つの Active Directory サーバをモニタし、暗号化されたデータを 5 つの Management Center に送信するように、エージェントを設定できます。

バージョン 6.2.3 以降を使用してアクセス制御を実行すると、ユーザエージェントが報告したログインによってユーザと IP アドレスが関連付けられ、その結果としてユーザ条件によるアクセス コントロール ルールがトリガーされます。

注　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。これを防止する方法の詳細については、アイドル セッション タイムアウトの有効化（2-5 ページ）を参照してください。

表 1-1　ポーリングおよびモニタリングについての注記

概念	注記
ログイン検出	エージェントは、バージョン 6.2.3 以降を実行している Firepower Management Center に対して、IPv6 アドレスを持つホストへのユーザ ログインを報告します。 エージェントは、バージョン 6.2.3 以降を実行している Firepower Management Center に対して、権限のないユーザ ログインと NetBIOS ログインを報告します。 Active Directory サーバへのログインを検出するには、サーバの IP アドレスを使用して Active Directory サーバの接続を設定する必要があります。詳細については、ユーザ エージェントの Active Directory サーバ接続の設定（2-24 ページ）を参照してください。
ログオフ検出	エージェントは、検出されたログオフを Firepower Management Center バージョン 6.2.3 以降に対して報告します。 ログオフはすぐに検出されない場合があります。ログオフに関連付けられたタイムスタンプは、ユーザがホストの IP アドレスにマップされなくなったことをエージェントが検出した時間であり、ユーザがホストからログオフした時間とは一致しない場合があります。
リアルタイム データの取得	Active Directory サーバで Windows Server 2008 または Windows Server 2012 を実行している必要があります。 ユーザ エージェント コンピュータは、Windows 7、Windows 8、Windows 10、または Windows Server の Server 2003 より新しいバージョンを実行している必要があります。

ユーザ エージェントのログイン データ

ユーザ エージェントは、ユーザがネットワークにログインするか、またはアカウントがその他の理由で Active Directory のクレデンシャルに対して認証されるときに、ユーザをモニタします。ユーザ エージェントは、ホストへの対話型ユーザ ログイン、リモート デスクトップ ログイン、ファイル共有認証、およびコンピュータ アカウント ログインを検出します。

ユーザエージェントは*権限を有した*ユーザのログインを報告します。権限のあるログインのデータ（たとえば、リモート デスクトップ ログインや、ユーザによるホストへの対話型ログインなど）によって、ホスト IP アドレスにマップされた現在のユーザが新たなログインからのユーザに変更されます。

ネットワーク検出のトラフィックベース検出では、*権限を持たない*ユーザによるログインが報告されます。権限のないログインでは、現在のユーザを変更しないか、ユーザも権限がない場合にのみ現在のユーザを変更します。

ただし、次の警告に注意してください。

- エージェントがファイル共有認証用のログインを検出した場合は、ホストに対するユーザ ログインを報告しますが、ホスト上の現在のユーザは変更しません。
- エージェントがホストに対するコンピュータ アカウント ログインを検出した場合は、NetBIOS Name Change 検出イベントを生成し、ホスト プロファイルに NetBIOS 名の変更が反映されます。
- 除外されたユーザ名のログインを検出した場合、エージェントは Management Center にログインを報告しません。

エージェントは、すべてのログインについて次の情報を Management Center に送信します。

- ユーザの LDAP ユーザ名

注　Unicode 文字を含むユーザ名は、Management Center により正しく表示されない場合があります。

- ログインまたはその他の認証の時刻
- ユーザのホストの IP アドレス、およびエージェントがコンピュータ アカウント ログインの IPv6 アドレスを報告した場合のリンクローカル アドレス

注 ユーザが Linux コンピュータでリモートデスクトップを使用して Windows コンピュータにログインした場合、エージェントはログインを検出すると、Linux コンピュータの IP アドレスではなく Windows コンピュータの IP アドレスを Management Center に報告します。

Management Center はユーザ アクティビティ データベースにログイン情報とログオフ情報を記録し、ユーザ データをユーザ データベースに記録します。ユーザ エージェントがユーザ ログインまたはログオフからのユーザ データを報告すると、報告されたユーザがユーザ データベース内のユーザのリストと照合してチェックされます。報告されたユーザがエージェントから報告された既存のユーザと一致した場合、報告されたデータがそのユーザに割り当てられます。報告されたユーザが既存のユーザと一致しなかった場合、新しいユーザが作成されます。

除外されたユーザ名に関連付けられたユーザ アクティビティは報告されませんが、関連するユーザ アクティビティは報告される場合があります。エージェントがコンピュータへのユーザ ログインを検出し、その後 2 人目のユーザ ログインを検出したときに、2 人目のユーザ ログインに関連付けられたユーザ名が報告対象から除外されていた場合、エージェントは元のユーザのログオフを報告します。ただし、2 人目のユーザのログインは報告されません。その結果、除外されたユーザがホストにログインしていた場合でも、IP アドレスにユーザはマップされません。

エージェントによって検出されるユーザ名に関する次の制限事項に注意してください。

- ドル記号で終わるユーザ名は他のバージョンの Management Center に報告されません 。
- Management Center では、Unicode 文字を含むユーザ名の表示が制限される場合があります。

Management Center で保存できる検出済みユーザの総数は、以下の内容によって異なります。

- バージョン 6.x では、Management Center モデル

ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザをデータベースから手動で削除するか、データベースからすべてのユーザを削除する必要があります。

複数のユーザ エージェントの展開

ドメインごとに複数の Active Directory サーバがある場合は、複数のユーザ エージェントのインストールを検討できます。Active Directory サービスは認証情報は共有しますが、セキュリティ ログ(ユーザ エージェントが一部の情報を収集する場所)は共有しません。

したがって、ドメイン内に複数の Active Directory サーバがある場合、以下のいずれかを実行できます。

- 複数の Active Directory サーバと通信する 1 つのユーザ エージェントをインストールします。

  1 つのユーザ エージェントは、最大 5 つの Active Directory サーバと通信できます。

- 複数のユーザ エージェントをインストールし、それぞれが異なる Active Directory サーバまたはドメイン コント ローラと通信するようにします。

  次のような状況ではこのタイプの展開をお勧めします。

  - Active Directory サーバが地理的に分散している。Active Directory サーバに地理的に近接しているコンピュータには、ユーザ エージェントをインストールすることをお勧めします(または Active Directory サーバ コンピュータ自体にもインストールできますが、これは安全性が低くなります)。
  - Active Directory サーバのトラフィックの負荷が高い。

注　各ユーザ エージェントを、ドメイン コントローラの完全修飾ホスト名または IP アドレスと通信するように構成する必要があります。マルチドメイン システムでは、各ドメイン コントローラが別々の IP アドレスまたはホスト名を持つのが一般的です。

レガシー エージェントのサポート

Active Directory サーバにインストールされているバージョン 1.0（レガシー）のユーザエージェントは、引き続き Active Directory サーバから 1 つの Management Center にユーザ ログイン データを送信できます。レガシー エージェントの導入要件と検出機能に変更はありません。

レガシーエージェントを Active Directory サーバにインストールして、1 つの Management Center のみに接続する必要があります。ただし、ユーザ エージェントのステータス モニタ ヘルス モジュールではレガシー エージェントはサポートされないため、レガシー エージェントが接続されている Management Center ではこのモジュールを有効にしないでください。

今後のリリースでレガシー エージェントのサポートが停止される場合に備えてできるだけ早くバージョン 2.5 のユーザ エージェントを使用するように導入環境をアップグレードしてください。

バージョン 6.x のユーザ エージェント、ISE、およびアクセス制御について

バージョン 6.0 では、ユーザ エージェントに代わって、Cisco Identity Services Engine（ISE）がサポートされるようになりました。ユーザ エージェントと ISE は、ユーザ アクセス制御のためのデータを収集するパッシブなアイデンティティ ソースです。バージョン 6.x でユーザ制御を実行するには、エージェントまたは ISE デバイスに接続されている Management Center 上の監視対象 Active Directory サーバに、アイデンティティ レルムを設定できます。レルム、アイデンティティ ソース、および ISE/ISE-PIC の詳細については、ご使用のシステムの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での FMC サポートの終了

Firepower Management Center バージョン 6.6 が、ユーザエージェントを有効にできる最後のバージョンです。Firepower Management Center 6.7 ではユーザエージェントを有効にできません。6.7 にアップグレードすると、アップグレードする前にユーザエージェントを無効にするように警告されます。

可能な限り早くユーザエージェントの使用を停止し、Cisco Identity Services Engine/Passive Identity Connector（ISE/ISE-PIC）の使用に切り替えることを強く推奨します。

ユーザエージェントでは使用できない次の機能を活用できるようになります。

- バージョン 2016 までの Microsoft Active Directory のサポート
- 最大 10 の Microsoft Active Directory ドメインコントローラからの認証データの収集
- Kerberos SPAN をサポートするスイッチからの Active Directory 認証データの収集
- パッシブ/アクティブ冗長性のサポート
- ISE-PIC から ISE にアップグレードし、既存の Cisco ISE クラスタに Passive Identity Connector ノードを追加することができます。
- KVM、VMware、および Hyper-v のサポート
- 組織に適合するよう、ライセンスに応じて 3,000 および 30 万のセッションをサポートします。

次のいずれかの現在のサポート契約をお持ちの場合、無料の ISE-PIC ライセンスの対象となります。

- 任意の FMC ハードウェアモデル
- Virtual FMC v25
- Virtual FMC v300

先行モデルの場合は、パーツ番号 `L-FMC-ISE-PIC=` を要求してください。

FMCv2 および FMCv10 を使用してる場合は、標準の ISE-PIC 部品番号を使用する必要があります。

詳細については、Cisco Firepower ユーザーエージェントの耐用年数末期およびサポート終了を参照してください。

このリリースで修正される問題

このリリースでは、次の問題が修正されました。

不具合 ID 番号	説明
CSCvo61952	ユーザ エージェント バージョン 2.4 は、バージョン 6.3 にアップグレードした後、ASA with FirePOWER Services デバイスで通信できます。
CSCvo24540	ユーザ エージェント バージョン 2.4 は、脆弱性に対処するために Microsoft SQL Server Compact Edition サポートをアップグレードしました。
CSCvo08211	バージョン 2.5 のユーザエージェントでは、Firepower 管理システムを使用してユーザエージェントを認証するためのパスワードを設定することができます。デフォルトのパスワードを使用する場合は、何もする必要はありません。 パスワードを設定するには、次のすべてを実行する必要があります。 • Firepower Management Center（管理対象デバイス以外）で `configure user-agent` コマンドを使用して、パスワードを作成します。詳細については、『*Firepower Management Center Configuration Guide*』の「Firepower Management Center CLI Reference」の章を参照してください。 • ユーザエージェントで同じパスワードを設定し、ユーザエージェントサービスを再起動します。詳細については、「ユーザ エージェント パスワードの変更（2-29 ページ）」を参照してください。