ユーザ エージェント入門

Version 2.3 のユーザ エージェントは、Firepower System の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。Firepower System のバージョン 5.x または バージョン 6.x とともにエージェントを使用する場合は、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 System 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。

ユーザ エージェントに関するリリース固有の用語や機能サポートについては、次の表を参照してください。

表 1-1　　リリース固有のユーザ エージェントの用語

概念	バージョン 5.x	バージョン 6.x
システム	FireSIGHT システム	Firepower System
ユーザ検出専用の機能	ネットワーク ディスカバリ	ネットワーク検出とアイデンティティ
ユーザ アイデンティティとユーザ アクティビティ データの分析	ユーザ認識	ユーザ認識
ユーザ制御へのユーザ アイデンティティとユーザ アクティビティの使用	アクセス コントロール	アクセス コントロール
管理側アプライアンス	防御センター	Management Center
管理対象アプライアンス	管理対象デバイス	管理対象デバイス
サーバデータベース接続	ユーザ認識オブジェクト	レルム

ユーザ エージェントについて

このセクションでは、Firepower System 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。ユーザの探索、RNA/ネットワーク探索、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構成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

Firepower System 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。バージョン 5.x では、これらを*ユーザ認識オブジェクト*として設定します。バージョン 6.x では、これらをアイデンティティ *レルム*として設定します。

ユーザ制御の詳細については、各システムの構成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できるようにするだけでなく、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

エージェントは、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 に送信するように設定できます。

バージョン 5.x またはバージョン 6.x 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制御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 1-2　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 5.2 以降を実行している 防御センター 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 5.0.1 以降を実行している 防御センター 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（2-22 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、検出したログオフをバージョン 5.2+ 防御センター に報告します。 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。

- ファイル共有認証のログインを検出した場合、エージェントはホストに対するユーザ ログインを報告しますが、ホストの現在のユーザは変更しません。
- ホストへのコンピュータ アカウントのログインを検出した場合、エージェントは NetBIOS 名変更のディスカバリ イベントを生成し、NetBIOS 名の変更をホスト プロファイルに反映します。
- 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。

- ドル記号文字($)で終わるユーザ名がバージョン 5.0.2+ の 防御センター に報告されると、ネットワーク マップは更新されますが、そのユーザ名はユーザ ログインとして表示されません。エージェントは、ドル記号($)で終わるユーザ名を他のバージョンの Management Center に報告しません。
- 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 5.x では、RNA または FireSIGHT ライセンス
- 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 Version 2.3 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 5.x のユーザ エージェントとアクセス制御について

ライセンス：Control

組織で Microsoft Active Directory サーバが使用されている場合、ユーザ エージェントをインストールして、Active Directory サーバを使用してユーザ アクティビティをモニタすることを推奨します。バージョン 5.x でユーザ制御を実行するには、ユーザ エージェントをインストールし、Defense Center への接続を設定する*必要があります*。

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

従来型ライセンス：Control

Smart ライセンス：Any

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構成ガイドを参照してください。