
# アイデンティティ データの概要

アイデンティティ ポリシーは、ユーザ エージェント、ISE/ISE-PIC デバイス、またはキャプティブ ポータルを使用して、ネットワーク上のユーザに関するデータを取得するように設定できます。詳細については、ユーザ アイデンティティ ソース（33-1 ページ）を参照してください。

## アイデンティティ データの用途

アイデンティティ データを収集することにより、以下を含む多くの機能を活用できます。

- レルム、ユーザ、ユーザ グループ、および ISE 属性の条件を使用してアクセス コントロール ルールを作成することによるユーザ制御の実行
- システムが特定のインパクト フラグ付きの侵入イベントを生成したときの電子メール、SNMP トラップ、または syslog によるアラート

## ユーザ検出の基礎

アイデンティティ ポリシーを使用して、ネットワーク上のユーザ活動をモニタすることができます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ アイデンティティ情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。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
- ホスト重要度の高いサーバの不正アクセスを試みている人物
- 不合理な容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 IT 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

この情報を利用して ASA FirePOWER モジュールの他の機能を使用すると、リスクを軽減し、アクセス コントロールを実行し、その他を中断から保護するアクションを実行することができます。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。

ユーザのアイデンティティ ソースを設定すると、ユーザ認識とユーザ制御を実行できます。

**ユーザ認識**

ユーザ データを表示し、分析する機能

**ユーザ制御**

ユーザ認識から得られた結論に基づいて、ネットワーク トラフィックでユーザまたはユーザ アクティビティをブロックするようにユーザ アクセス コントロール ルール条件を設定する機能。

ユーザ データは、正規のアイデンティティ ソース（アイデンティティ ポリシーにより参照される）から取得できます。

アイデンティティ ソースは、権限のあるサーバがユーザ ログインを検証した場合に権限のあるようになります。権限のあるログインから取得したデータを使用すると、ユーザ認識とユーザ制御を実行できます。権限のあるユーザ 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、ユーザが外部サーバ経由で認証されるときに発生します。ASA FirePOWER モジュールでサポートされているパッシブな認証方式は、ユーザ エージェントと ISE/ISE-PIC だけです。
- *アクティブ認証*は、ユーザが FirePOWER デバイス経由で認証されるときに発生します。ASA FirePOWER モジュールでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

次の表に、ASA FirePOWER モジュールでサポートされているユーザ アイデンティティ ソースの概要を示します。

*表 31-1*

| ユーザ アイデンティティ ソース | サーバ要件 | ソース タイプ | 認証タイプ（Authentication Type） | ユーザ認識 | ユーザ アクセス コントロール | 詳細 |
|---|---|---|---|---|---|---|
| ユーザ エージェント | Microsoft Active Directory | 権限のあるログイン | パッシブ | ○ | ○ | ユーザ エージェントのアイデンティティ ソース（33-3 ページ） |
| ISE/ISE-PIC | Microsoft Active Directory | 権限のあるログイン | パッシブ | ○ | ○ | ISE/ISE-PIC アイデンティティ ソース（33-4 ページ） |
| キャプティブ ポータル | LDAP または Microsoft Active Directory | 権限のあるログイン | active | ○ | ○ | キャプティブ ポータル アクティブ認証のアイデンティティ ソース（33-7 ページ） |

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。

- キャプティブ ポータルを使用して、失敗した認証アクティビティを記録する必要があります。失敗した認証試行によって新しいユーザがデータベース内のユーザのリストに追加されることはありません。

- キャプティブ ポータルを使用するには、センシング インターフェイス（ルーテッド インターフェイスなど）に IP アドレスがあるアプライアンスを展開する必要があります。

#### ユーザ アイデンティティの展開

システムがユーザ ログイン時に任意のアイデンティティ ソースからのユーザ データを検出すると、そのログインから検出されたユーザは、ユーザ データベース内のユーザのリストに照らして確認されます。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 アクティビティ データベース

デバイス上のユーザ アクティビティ データベースには、設定済みのすべてのアイデンティティ ソースによって報告された、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
- 手動でユーザが削除されたとき
- 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 データベース

ユーザ データベースには、設定済みのアイデンティティ ソースによって報告された、各ユーザのレコードが含まれています。

デバイスが保存できるユーザの総数は、モデルごとに異なります。制限に達した場合、新規ユーザを追加できるようにユーザを（手動またはデータベースの消去により）削除する必要があります。

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 ASA FirePOWER モジュールに報告されません。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。

## 現在のユーザ ID

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが ASA FirePOWER モジュールに報告されるユーザです。

システムは、同じホストに対して異なるユーザによる複数のログインを検出すると、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

# ユーザ データベースの制限

モニタできるユーザの数、およびユーザ制御を実行するために使用できるユーザの数は、デバイス モデルによって決まります。

ASDM によって管理される ASA FirePOWER モジュールを展開する場合、ユーザ データベースには、最大 2,000 の正規ユーザを保存できます。