CHAPTER 17

ユーザに基づくトラフィックの制御

*アクセス コントロール ポリシー*内の*アクセス コントロール ルール*は、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。アクセス コントロール ルールのユーザ条件を使用することで、*ユーザ制御*を実行し、ホストにログインする LDAP ユーザに基づいてトラフィックを制限することによって、ネットワークを通過できるトラフィックを管理できます。

ユーザ制御は、*アクセス コントロールされたユーザ*と IP アドレスを関連付けることによって機能します。展開されたエージェントは、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory クレデンシャルで認証する場合に、指定されたユーザをモニタします。たとえば、組織は一元化された認証のために Active Directory に依存するサービスまたはアプリケーションを使用できます。

トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。個々のユーザまたはユーザが属しているグループに基づいてトラフィックを制御できます。

ユーザ条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純または複雑にすることができ、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

（注） ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部のデコードと前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL インスペクション*機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号することができます。

ユーザ制御には Control ライセンスが必要であり、ユーザ エージェントのモニタリング Microsoft Active Directory サーバによって報告されるログインおよびログアウトのレコードを使用している、LDAP ユーザおよびグループ（アクセス制御されたユーザ）に対してのみサポートされます。

しかし、FireSIGHT ライセンスのみを使用して、ユーザ制御の基盤である*ユーザ認識*を引き続き活用できます。ユーザ認識によって、管理対象デバイスが検出データについて許可されたネットワーク トラフィックを検査するときにシステムが検出できる、エージェントによって報告されたユーザ アクティビティ、および*アクセス制御されていないユーザ*の追加のアクティビティを表示できます。システムは、さまざまなプロトコル（AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP および MDNS）を介したログイン試行を識別できます。

システムによって報告されたユーザ アクティビティにコンテキストを追加するには、展開環境で LDAP サーバにクエリを行い、アクセス制御されたユーザだけでなく、一部のアクセス制御されていないユーザ（ユーザ検出によって検出された POP3 および IMAP ユーザ、およびアクティビティがユーザ検出またはユーザ エージェントによって検出される LDAP ユーザ）のメタデータを取得できます。

ユーザ認識によって、「何が」の背後にある「誰が」を決定するためのすべてのタイプの展開が可能になります。たとえば、以下について決定できます。

- 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
- 脆弱（レベル 1：赤）影響レベル（保護 が必要）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（保護 が必要）

この情報を入手すれば、リスクを軽減したり、その他の人を中断から保護するための措置を講じたりするための的を絞ったアプローチを取ることができます。ユーザ制御によって、LDAP ユーザとユーザ アクティビティをブロックする機能が追加されます。また、ユーザ認識および制御の機能によって、監査制御が大幅に向上し、法規制の遵守が強化されます。詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

次の表に、ユーザ認識および制御に関する要件を示します。ユーザ エージェントの詳細および最新情報については、『*User Agent Configuration Guide*』を参照してください。

表 17-1　ユーザ認識および制御の要件

要件	ユーザ認識	ユーザ制御
ライセンス	FireSIGHT	Control
デバイス	Any	すべて（シリーズ 2 または X-シリーズ を除く）
Defense Center	Any	任意（DC500 を除く）
ユーザ エージェント（User Agent）	モニタする Defense Center および Microsoft Active Directory サーバとの間の TCP/IP アクセスが行われる、次のいずれかを実行している Windows コンピュータに、バージョン 2.2 のユーザ エージェントをインストールします。 • Windows Vista、Windows 7、または Windows 8 • Windows Server 2008 または 2012 また、Microsoft .NET Framework バージョン 4.0 クライアント プロファイルと Microsoft SQL Server Compact（SQL CE）バージョン 3.5 もインストールする必要があります。	
ユーザのメタデータ取得のための LDAP サーバ	Defense Center からの TCP/IP アクセスがある、次のいずれか。 • Windows Server 2008 上の Microsoft Active Directory（ユーザ制御に必要） • Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0（ユーザ認識のみ） • Linux 上の OpenLDAP（ユーザ認識のみ）	

詳細については、以下を参照してください。

- アクセス コントロール ルールへのユーザ条件の追加（17-3 ページ）
- アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-4 ページ）
- Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）

アクセス コントロール ルールへのユーザ条件の追加

ライセンス：Control

サポートされるデバイス：シリーズ 2 と X-シリーズを除くすべて

サポートされる防御センター：任意（DC500 を除く）

FireSIGHT システム のユーザ制御機能は、アクセス制御されたユーザをホストの IP アドレスに関連付けることで機能します。配置されたユーザ エージェントは、指定したユーザが Microsoft Active Directory クレデンシャルで認証するときにモニタします。トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。

ユーザ制御を実行する前に、以下を行う必要があります。

- Defense Center と Microsoft Active Directory サーバとの間に接続を設定します。アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-4 ページ）を参照してください。
- Active Directory サーバへの TCP/IP アクセスがある Microsoft Windows コンピュータにユーザ エージェントをインストールします。Active Directory のログインを報告するためのユーザ エージェントの使用（17-11 ページ）を参照してください。

注意　モニタする多数のユーザ グループを設定する場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、ユーザ グループに基づくアクセス コントロール ルールが想定どおりに起動しない可能性があります。

1 つのユーザ条件で、最大 50 のユーザおよびグループを [選択されたユーザ（Selected Users）] に追加できます。ユーザ グループを持つ条件は、そのグループのメンバー（サブグループのメンバーを含む）のいずれかが送信元/宛先であるトラフィックを照合します。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

（注）　グループの条件を使用してユーザ制御を実行する前に、システムはそのグループ内の少なくとも 1 人のユーザからのアクティビティを検出する必要があります。この最初の接続は、一致するアクセス コントロール ルールによって処理**されません**が、代わりに一致する次のルール、またはアクセス コントロール ポリシーのデフォルト アクションによって処理されます。

ユーザ条件を作成する際、警告アイコンは無効な設定を示します。アイコンの上にポインタを置くと詳細が表示されます。また、アクセス コントロール ポリシーおよびルールのトラブルシューティング（12-25 ページ）を参照してください。

ユーザ トラフィックを制御するには、次の手順を実行します。

アクセス: Admin/Access Admin/Network Admin

手順 1　LDAP ユーザまたはグループ別にトラフィックを制御するデバイスを対象とするアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集（14-3 ページ）を参照してください。

手順 2　ルール エディタで、[ユーザ（Users）] タブを選択します。

[ユーザ（Users）] タブが表示されます。

手順 3　[有効なユーザ（Available Users）] リストから追加するユーザおよびグループを見つけて選択します。

ユーザおよびグループは異なるアイコンでマークされます。追加するユーザおよびグループを検索するには、[有効なユーザ（Available Users）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、ユーザまたはグループの名前を入力します。入力していくと、リストが更新されて一致する項目が表示されます。

項目を選択するには、その項目をクリックします。複数の項目を選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [すべて選択（Select All）] を選択します。

手順 4　[ルールに追加（Add to Rule）] をクリックし、選択したユーザおよびグループを [選択されたユーザ（Selected Users）] リストに追加します。

選択したユーザおよびグループをドラッグ アンド ドロップすることもできます。

手順 5　ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得

ライセンス: FireSIGHT または Control

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

ユーザ制御を実行する（つまり、ユーザ条件を含むアクセス コントロール ルールを作成する）前に、Defense Center と組織の 1 つ以上の Microsoft Active Directory サーバ間の接続を設定する必要があります。Defense Center は、定期的かつ自動的に LDAP サーバにクエリを行い、アクセス制御されたユーザ（つまり、ユーザ エージェントでアクティビティをモニタするユーザおよびグループ、およびトラフィックの制限時に条件として使用できるユーザおよびグループ）のメタデータを更新します。Defense Center は、アクティビティがユーザ エージェントによってすでに報告されているアクセス制御されていないユーザのメタデータも取得します。または、オンデマンド クエリを実行できます。

ユーザ制御を実行していない場合は、追加のタイプの LDAP サーバにクエリを行い、ユーザ認識データ（POP3 および IMAP ユーザのみならず、アクティビティがユーザ エージェントによって報告されるものではなくユーザ検出によって検出される LDAP ユーザに関連付けられているメタデータ）を取得できます。システムは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server Enterprise Edition サーバ上の LDAP ユーザに関連付けます。この場合、Defense Center は定期的に LDAP サーバにクエリを行い、アクティビティが最後のクエリ以降にシステムによって検出されたユーザの新規および更新されたメタデータを取得します。

詳細については、以下を参照してください。

- ユーザ認識および制御のための LDAP サーバへの接続（17-5 ページ）
- オンデマンドによるユーザ制御パラメータの更新（17-9 ページ）
- LDAP サーバとの通信の一時停止（17-10 ページ）

ユーザ認識および制御のための LDAP サーバへの接続

ライセンス：FireSIGHT または Control

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

Defense Center と組織の LDAP サーバとの間の接続によって以下を行うことができます。

- アクセス制御されたユーザおよびグループ（ユーザ エージェントでアクティビティをモニタするユーザおよびグループ、およびアクセス コントロール ルールによるトラフィックの制限時に条件として使用できるユーザおよびグループ）を指定します。
- アクセス制御されたユーザと、一部のアクセス制御されていないユーザ（ユーザ検出によって検出される POP3 および IMAP ユーザ、およびアクティビティがユーザ検出またはユーザ エージェントによって検出される LDAP ユーザ）のメタデータ取得のためにサーバに対してクエリを実行できます。

これらの接続、または*ユーザ認識オブジェクト*は、LDAP サーバに対して接続設定および認証フィルタ設定を指定します。これらは、FireSIGHT システム の Web インターフェイスへの外部認証を管理するために設定する認証オブジェクトに似ています。認証オブジェクトの管理（61-5 ページ）を参照してください。

ユーザ制御を実行するには、Microsoft Active Directory LDAP サーバに接続する**必要があります**。LDAP ユーザ メタデータを簡単に取得したい場合、システムは他のタイプの LDAP サーバへの接続をサポートします。表 17-1（17-2 ページ）を参照してください。

システムがユーザ アクティビティを検出すると、システムはそのユーザのレコードを Defense Center ユーザ データベース（ユーザ アイデンティティ データベースとも呼ばれます）に追加できます。Defense Center は、定期的に LDAP サーバにクエリを行い、最後のクエリ以降にアクティビティが検出された新しいユーザおよび更新されたユーザのメタデータを取得します。ユーザがデータベースにすでに存在している場合、システムはメタデータが過去 12 時間更新されていなければ更新します。システムが新しいユーザ ログインを検出してから、Defense Center がユーザ メタデータで更新するまで数分かかる場合があります。

システムは、POP3 と IMAP ログイン内の電子メール アドレスを使用して LDAP サーバ上のユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインを管理対象デバイスが検出すると、システムは LDAP ユーザのメタデータをそのユーザに関連付けます。

（注）　LDAP サーバからシステムによって検出されたユーザを削除しても、Defense Center はユーザ データベースからそのユーザを削除**しません**。そのため、手動で削除する必要があります。ただし、LDAP 変更は、Defense Center が次にアクセス制御されたユーザのリストを更新したときにアクセス コントロール ルールに反映**されます**。

次の表に、モニタ対象ユーザに関連付けることができる LDAP メタデータを示します。LDAP サーバからユーザのメタデータを正常に取得するには、サーバはこの表にリストされている LDAP フィールド名を使用する**必要がある**ことに注意してください。LDAP サーバ上のフィールド名を変更すると、Defense Center はそのフィールドの情報を使ってデータベースに入力できなくなります。

表 17-2　シスコ フィールドへの LDAP フィールドのマッピング

メタデータ	Defense Center	Active Directory	Oracle Directory Server	OpenLDAP
LDAP user name	[ユーザ名（Username）]	samaccountname	cn uid	cn uid
first name	名	givenname	givenname	givenname
last name	姓	sn	sn	sn
メール アドレス	E メール	メール アドレス userprincipalname（mail に値が設定されていない場合）	メール アドレス	メール アドレス
部署	部署名（Department）	部署 distinguishedname（department に値が設定されていない場合）	部署	ou
電話番号	電話	telephonenumber	適用対象外	telephonenumber

LDAP 管理者と密に連携し、LDAP サーバが正しく設定され、そのサーバに接続して LDAP 接続の作成時に提供する必要がある情報を確実に取得できるようにします。

サーバ タイプ、IP アドレス、およびポート

プライマリ LDAP サーバ（オプションでバックアップ LDAP サーバも）のサーバ タイプ、IP アドレスまたはホスト名、およびポートを指定する必要があります。ユーザ制御を実行する場合は、Microsoft Active Directory サーバを使用する**必要があります**。

LDAP 固有パラメータ

Defense Center が認証サーバ上のユーザ情報を取得するために LDAP サーバを検索する場合は、その検索の出発点が必要です。ベース識別名、すなわち*ベース DN* を提供することで検索する*名前空間*またはディレクトリ ツリーを指定できます。通常、ベース DN には、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、`ou=security,dc=example,dc=com` となります。プライマリ サーバを特定したら、そのサーバから使用可能なベース DN のリストが自動的に取得され、該当するベース DN を選択できることに注意してください。

取得するユーザ情報に適切な権限を持っているユーザのユーザ クレデンシャルを指定する必要があります。指定したユーザの識別名はディレクトリ サーバのディレクトリ インフォメーション ツリーで一意でなければならないことに注意してください。

また、LDAP 接続の暗号化方式を指定することもできます。認証に証明書が使用される場合は、証明書内の LDAP サーバの名前と Defense Center Web インターフェイスで指定したホスト名が一致する**必要がある**ことに注意してください。たとえば、LDAP 接続を設定するときに `10.10.10.250` を使用し、証明書内で `computer1.example.com` を使用した場合は、接続が失敗します。

最後に、無応答の LDAP サーバへの接続の試みがバックアップ接続にロールオーバーされるタイムアウト期間を指定する必要があります。

ユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータ

ユーザ制御を実行するには、アクセス コントロール ルールで条件として使用するグループを指定します。

グループを含めると、自動的に、すべてのサブグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでサブグループを使用する場合は、明示的にサブグループを含める必要があります。また、グループと個別のユーザを除外することもできます。グループを除外すると、ユーザが他のグループのメンバーであっても、そのグループのすべてのメンバーが除外されます。

アクセス コントロールで使用可能なユーザの最大数は FireSIGHT ライセンスによって異なります。含めるユーザとグループを選択するときに、ユーザの総数が FireSIGHT のユーザ ライセンス数より少ないことを確認します。アクセス コントロール パラメータの範囲が広すぎる場合、Defense Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

（注） 含めるグループを指定しなかった場合、システムは指定された LDAP パラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、シスコでは、アクセス コントロールで使用するユーザを代表するグループだけを明示的に含めることを推奨しています。ユーザ グループまたはドメイン ユーザ グループを含めることは**できない**ことに注意してください。

また、Defense Center がアクセス コントロールで使用する新しいユーザを取得するために LDAP サーバに対してクエリを実行する頻度を指定する必要もあります。

LDAP 接続を作成した後、削除アイコン（）をクリックして、選択内容を確認することで、その接続を削除できます。LDAP 接続を変更するには、編集アイコン（）をクリックします。接続が有効になっている場合は、Defense Center が LDAP サーバ対して次回クエリを実行したときに保存した変更が反映されます。

ユーザ認識またはユーザ制御用の LDAP 接続を作成するには、次の手順を実行します。

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ユーザ（Users）] の順に選択します。

[ユーザ ポリシー（Users Policy）] ページが表示されます。

手順 2　[LDAP 接続の追加（Add LDAP Connection）] をクリックします。

[ユーザ認識認証オブジェクトの作成（Create User Awareness Authentication Object）] ページが表示されます。

手順 3　オブジェクトの [名前（Name）] と [説明（Description）] を入力します。

手順 4　[LDAP サーバタイプ（LDAP Server Type）] を選択します。

ユーザ制御を実行する場合は、Microsoft Active Directory サーバを使用する**必要があります**。

（注）　ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を Defense 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。

手順 5　プライマリ LDAP サーバ（オプションで、バックアップ LDAP サーバも）の [IP アドレス（IP Address）] または [ホスト名（Host Name）] を指定します。

手順 6　LDAP サーバが認証トラフィックに使用する [ポート（Port）] を指定します。

手順 7　ユーザがアクセスする LDAP ディレクトリの [ベース DN（Base DN）] を指定します。

たとえば、Example 社の Security 組織で名前を認証するには、`ou=security,dc=example,dc=com` と入力します。

ヒント　使用可能なすべてのドメインのリストを取得するには、[DN の取得（Fetch DNs）] をクリックして、ドロップダウンリストから該当するベース識別名を選択します。

手順 8　LDAP ディレクトリへのアクセスを検証するために使用する識別 [ユーザ名（Username）] と [パスワード（Password）] を指定します。パスワードを確認します。

たとえば、ユーザ オブジェクトに `uid` 属性が設定されており、Example 社の Security 部門の管理者用のオブジェクトの `uid` 値が `NetworkAdmin` である OpenLDAP サーバに接続している場合は、`uid=NetworkAdmin,ou=security,dc=example,dc=com` と入力することになります。

手順 9　[暗号化（Encryption）] 方式を選択します。暗号化を使用する場合は、[SSL 証明書（SSL Certificate）] を追加できます。

証明書内のホスト名は、手順 5 で指定した LDAP サーバのホスト名と一致する**必要があります**。

手順 10　無応答の LDAP サーバへの接続の試みがバックアップ接続にロールオーバーされるタイムアウト期間（秒単位）を [タイムアウト（Timeout）] に指定する必要があります。

手順 11　オプションで、オブジェクトのユーザ認識設定を指定する前に、[テスト（Test）] をクリックして接続をテストします。

手順 12　手順 4 で選択した LDAP サーバのタイプによって 2 つの選択肢があります。

- Active Directory サーバに接続している場合は、[ユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータ（User/Group Access Control Parameters）] を有効にして、アクセス コントロールで使用するユーザを指定できます。次の手順に進みます。
- 他の種類のサーバに接続している場合、または、ユーザ制御を実行しない場合は、手順 17 までスキップします。

手順 13　[取得グループ（Fetch Groups）] をクリックし、指定した LDAP パラメータを使用して、使用可能なグループ リストに値を入力します。

手順 14　グループを追加または除外するための右矢印ボタンと左矢印ボタンを使用して、アクセス コントロールで使用するユーザを指定します。

グループを含めると、自動的に、すべてのサブグループのメンバーを含む、そのグループのすべてのメンバーが含まれます。ただし、アクセス コントロール ルールでサブグループを使用する場合は、明示的にサブグループを含める必要があります。グループを除外すると、ユーザが他のグループのメンバーであっても、そのグループのすべてのメンバーが除外されます。

手順 15　特定の [ユーザの除外（User Exclusions）] を指定します。

ユーザを除外すると、そのユーザを条件として使用するアクセス コントロール ルールを作成できなくなります。複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

手順 16　LDAP サーバに対するクエリを実行して新しいユーザとグループの情報を取得する頻度を指定します。

デフォルトでは、Defense Center は 1 日 1 回午前零時にサーバに対するクエリを実行します。

- [開始（Start At）] ドロップダウン リストを使用して、クエリを実行するタイミングを指定します。**0** は午前零時を意味し、**1** は午前 1 時を意味します。
- [更新間隔（Update Interval）] ドロップダウンリストを使用して、サーバに対してクエリを実行する頻度を時間単位で指定します。

手順 17　[保存（Save）] をクリックします。

ユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータを追加または変更したら、変更の実行を確認します。オブジェクトが保存され、[ユーザ ポリシー（Users Policy）] ページが再度表示されます。

手順 18　作成した接続の横にあるスライダをクリックして接続を有効にします。

接続を有効にして、接続にユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータが含まれている場合は、すぐに LDAP サーバに対するクエリを実行してユーザとグループの情報を取得するかどうかを選択します。すぐに LDAP サーバに対するクエリを実行しない場合は、クエリはスケジュールされた時刻に実行されます。タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）で、クエリの進捗をモニタリングすることができます。

オンデマンドによるユーザ制御パラメータの更新

ライセンス：Control

サポートされるデバイス：シリーズ 2 と X-シリーズを除くすべて

サポートされる防御センター：任意（DC500 を除く）

LDAP 接続内のユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータを変更する場合、または、LDAP サーバ上のユーザまたはグループを変更しその変更をすぐにユーザ制御に反映させたい場合は、Active Directory サーバからのオンデマンド ユーザ データ取得の実行を Defense Center に強制できます。

Defense Center がサーバから取得可能なユーザの最大数は FireSIGHT ライセンスによって異なります。LDAP 接続内のアクセス コントロール パラメータの範囲が広すぎる場合、Defense Center はできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

オンデマンド ユーザ データ取得を実行するには、次の手順を実行します。

アクセス: Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ユーザ（Users）] の順に選択します。

[ユーザ ポリシー（Users Policy）] ページが表示されます。

手順 2　LDAP サーバへのクエリに使用する LDAP 接続の横にあるダウンロード アイコン（ ）をクリックします。

クエリが開始されます。タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）で進捗をモニタリングすることができます。

LDAP サーバとの通信の一時停止

ライセンス: FireSIGHT または Control

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

LDAP 接続が有効になっている場合にのみ、Defense Center は LDAP サーバに対するクエリを実行できます。クエリを停止するには、それらを削除するのではなく、一時的に LDAP 接続を無効にします。

アクセス制御に使用される LDAP 接続を再度有効にすると、更新されたユーザおよびグループの情報を取得するために、すぐにサーバに対するクエリを実行するように Defense Center に強制するか、または最初に予定されているクエリが行われるまで待機することができます。

LDAP 接続を無効または再度有効にするには、次の手順を実行します。

アクセス: Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ユーザ（Users）] の順に選択します。

[ユーザ ポリシー（Users Policy）] ページが表示されます。

手順 2　作成した接続の横にあるスライダをクリックして、接続を一時停止または再度有効にします。

接続を有効にして、接続にユーザ アクセス コントロール パラメータとグループ アクセス コントロール パラメータが含まれている場合は、すぐに LDAP サーバに対するクエリを実行してユーザとグループの情報を取得するかどうかを選択します。すぐに LDAP サーバに対するクエリを実行しない場合は、クエリがスケジュールされた時刻に実行されます。タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）で、クエリの進捗をモニタリングすることができます。

Active Directory のログインを報告するためのユーザ エージェントの使用

ライセンス：FireSIGHT

Microsoft Windows のコンピュータに導入されたユーザ エージェントは、Microsoft Active Directory サーバをモニタし、組織の LDAP ユーザがホストにログインおよびホストからログアウトしたとき、または他の理由で Active Directory クレデンシャルで認証したときに Defense Center に通知できます。たとえば、組織は一元化された認証のために Active Directory に依存するサービスまたはアプリケーションを使用できます。

このエージェントによって報告される情報は、組織におけるユーザ アクティビティの記録としてだけでなく、ユーザ制御の基盤として役立ちます。トラフィックがユーザ条件を持つアクセス コントロール ルールに一致するには、モニタ対象のセッション内の送信元ホストまたは宛先ホストいずれかの IP アドレスがログインしているアクセス制御されたユーザに関連付けられている必要があります。個々のユーザまたはユーザが属しているグループに基づいてトラフィックを制御できます。

(注)　ユーザ制御を実行する場合は、ユーザ エージェントをインストールして使用する**必要があります**。ただし、ユーザ エージェントは Active Directory の認証に関連するユーザ アクティビティのみ報告します。ユーザ認識によって、エージェントによって報告されたすべてのユーザ アクティビティ、および管理対象デバイスごとの許可されたネットワーク トラフィックで検出された他のアクティビティを表示できます。システムは、検出機能を使用して、さまざまなプロトコル（AIM、IMAP、LDAP、Oracle、POP3、SIP、FTP、HTTP および MDNS）を介したログイン試行を識別できます。詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

ユーザ認識またはユーザ制御のためにユーザ エージェントを使用して LDAP ユーザ認証レコードを取得するには、最初にエージェントからの接続を許可するように各 Defense Center を設定します。ハイ アベイラビリティ展開では、プライマリ Defense Center とセカンダリ Defense Center の両方でエージェント通信を有効にします。ユーザ エージェントは同時に最大 5 つの Defense Center に接続できます。Defense Center でユーザ エージェントの通信を有効にした後、Windows コンピュータにエージェントをインストールできます。表 17-1（17-2 ページ）を参照してください。

最後に、Microsoft Active Directory サーバからデータを取得してその情報を Defense Center に報告するようにユーザ エージェントを設定します。また、レポートから特定のユーザ名および IP アドレスを除外したり、ローカル イベント ログまたは Windows アプリケーション ログにステータス メッセージをロギングするようにエージェントを設定できます。ユーザ エージェントのステータス モニタ ヘルス モジュールは、Defense Center に接続されたエージェントをモニタします。ユーザ エージェント ステータス モニタリングの設定（68-32 ページ）を参照してください。

ユーザ エージェントに接続するようにDefense Centerを設定するには、以下を行います。

アクセス：Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ユーザ（Users）] の順に選択します。

[ユーザ ポリシー（Users Policy）] ページが表示されます。

手順 2　[ユーザ エージェントの追加（Add User Agent）] をクリックします。

[ユーザ エージェントの追加（Add User Agent）] ポップアップ ウィンドウが表示されます。

手順 3　エージェントの**名前**を入力します。

手順 4　エージェントをインストールするコンピュータの**ホスト名またはアドレス**を入力します。IPv4 アドレスを使用する**必要があります**。IPv6 アドレスを使用してユーザ エージェントに接続するように Defense Center を設定することはできません。

手順 5　[ユーザ エージェントの追加（Add User Agent）] をクリックします。

これで、Defense Center は指定したコンピュータ上のユーザ エージェントに接続できます。接続を削除するには、削除アイコン（ ）をクリックして、その削除を確認します。

手順 6　指定したコンピュータにユーザ エージェントをインストールします。Microsoft Active Directory サーバからデータを取得してその情報を Defense Center に報告するように設定します。

詳細および最新情報については、『*User Agent Configuration Guide*』を参照してください。