



# ダイナミック ファイアウォール について

以下のトピックでは、ダイナミック ファイアウォールに関する一般情報を提供します。

- [ダイナミック ファイアウォール について \(1 ページ\)](#)

## ダイナミック ファイアウォール について

これまで、Cisco Secure Firewall Management Center は、Microsoft Active Directory、パッシブ ID エージェント、Cisco Identity Services Engine (Cisco ISE) などの設定されたアイデンティティソースからのみユーザーに関する情報を収集していました。この情報には通常、ユーザー名、グループ、IP アドレスが含まれていました。

ダイナミック ファイアウォール を使用すると、アイデンティティソースが提供する情報に Cisco アイデンティティ インテリジェンスからのユーザーリスクスコアを追加できるため、常に最新のユーザーポスチャとリスクに基づいてポリシーを設定することが可能です。ユーザーアイデンティティとインテリジェンスを組み合わせ、その情報をレポートおよびアクセスコントロール ポリシーで使用できるようにします。

ダイナミック ファイアウォール を使用するには、次の条件を満たしている必要があります。

- アイデンティティ インテリジェンス テナントがあること。  
『[Duo Identity Security with Cisco Identity Intelligence](#)』を参照してください。
- 動的属性コネクタの有効化
- アイデンティティソースをセットアップしていること。
  - Cisco Identity Services Engine (Cisco ISE)
  - pxGrid クラウド  
pxGrid クラウドは同じフィールドでアイデンティティとポスチャを組み合わせます。  
詳細については、「[What is pxGrid?](#)」を参照してください。

認証情報に加えて、Cisco ISE と pxGrid クラウドは次の情報を提供できます。

- SGT Exchange Protocol over TCP (SXP) バインディングおよびディレクトリセッション情報（必要に応じて）。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。
- ポスチャおよびモバイルデバイス管理のコンプライアンス。詳細については、『[Compliance](#)』を参照してください。
- アイデンティティレルムをセットアップしていること。
  - [LDAP](#) レルムまたは [Active Directory](#) レルムおよびレルムディレクトリの作成
  - [パッシブ認証用の Azure AD \(SAML\)](#) レルムの作成

アイデンティティソースは、認証情報（ログイン、ログアウト）とポスチャを提供します。アイデンティティソースは、必要に応じて SXP バインディングおよびセッションディレクトリ情報も提供できます。

アイデンティティレルムは、ユーザー、グループ、および IP アドレス情報を提供します。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。