



# セキュリティとインターネットアクセス

動的属性コネクタがクラウドサービスプロバイダーおよびFMCと通信するときに使用するURLのリスト。

- [セキュリティ要件 \(1 ページ\)](#)
- [インターネットアクセス要件 \(1 ページ\)](#)

## セキュリティ要件

Cisco Secure 動的属性コネクタを保護するには、保護された内部ネットワークにそれをインストールしてください。動的属性コネクタは、使用可能なサービスとポートのうち必要なもののみを持つように設定されていますが、攻撃が到達できないように確保する必要があります。

動的属性コネクタとFMCが同じネットワーク上に存在している場合は、FMCを動的属性コネクタと同じ保護された内部ネットワークに接続することができます。

アプライアンスの展開方法に関係なく、システム間通信は暗号化されます。それでも、分散型サービス拒否 (DDoS) や中間者攻撃などの手段でアプライアンス間の通信が中断、ブロック、または改ざんされないよう何らかの対策を講じる必要があります。

## インターネットアクセス要件

デフォルトでは、動的属性コネクタは、ポート 443/tcp (HTTPS) で HTTPS を使用してインターネット経由で Firepower システムと通信するように構成されています。動的属性コネクタがインターネットに直接アクセスしないようにするために、プロキシサーバーを構成できます。

次の情報により、FMC および外部サーバーとの通信に動的属性コネクタが使用する URL が通知されます。

表 1: 動的属性コネクタ **FMC** アクセス要件

URL	理由
<a href="https://fmc-ip/api/fmc_platform/v1/auth/generatetoken">https://fmc-ip/api/fmc_platform/v1/auth/generatetoken</a>	認証
<a href="https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects">https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects</a>	GET および POST ダイナミックオブジェクト
<a href="https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects/object-id/mappings?action=add">https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects/object-id/mappings?action=add</a>	マッピングを追加します
<a href="https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects/object-id/mappings?action=remove">https://fmc-ip/api/fmc_config/v1/domain/domain-id/object/dynamicobjects/object-id/mappings?action=remove</a>	マッピングを削除します

表 2: 動的属性コネクタ **vCenter** アクセス要件

URL	理由
<a href="https://vcenter-ip/rest/com/vmware/cis/session">https://vcenter-ip/rest/com/vmware/cis/session</a>	認証
<a href="https://vcenter-ip/rest/vcenter/vm">https://vcenter-ip/rest/vcenter/vm</a>	VM 情報を取得します
<a href="https://nsx-ip/api/v1/fabric/virtual-machines/vm-id">https://nsx-ip/api/v1/fabric/virtual-machines/vm-id</a>	仮想マシンに関連付けられた NSX-T タグを取得します

### 動的属性コネクタ **AWS** アクセス要件

動的属性コネクタは、組み込みの SDK メソッドを呼び出してインスタンス情報を取得します。これらのメソッドは内部的に、動的属性コネクタに指定されたリージョンに基づいて、サービスエンドポイント URL をクエリします。それらは AWS Web サイト <https://docs.aws.amazon.com/general/latest/gr/ec2-service.html> に文書化されています。

### 動的属性コネクタ **Azure** のアクセス要件

動的属性コネクタは、組み込みの SDK メソッドを呼び出してインスタンス情報を取得します。これらのメソッドは、<https://login.microsoft.com>（認証用）と <https://management.azure.com>（インスタンス情報の取得用）を内部的に呼び出します。

## 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。