



Cisco 動的属性コネクタについて

Cisco Secure 動的属性コネクタでは、クラウドプロバイダーからデータ（ネットワークやIPアドレスなど）を収集し、それを Cisco Secure Firewall Management Center（management center）に送信して、アクセス制御ルールで使用できるようにします。

次のトピックでは、動的属性コネクタに関する背景について説明します。

- [Cisco Secure 動的属性コネクタについて（1 ページ）](#)

Cisco Secure 動的属性コネクタについて

Cisco Secure 動的属性コネクタにより、さまざまなクラウドサービスプラットフォームのサービスタグとカテゴリを Secure Firewall Management Center（management center）アクセス制御で使用できます。

サポートされるコネクタ

現在、次をサポートしています。

表 1: Cisco Secure 動的属性コネクタ バージョンおよびプラットフォームでサポートされているコネクタのリスト

CSDAC バージョン/ プラットフォーム	AWS	GitHub	Google クラウド	Azure	Azure サービススタグ	Microsoft Office 365	vCenter
バージョン 1.1 (オンプレミス)	対応	×	×	対応	対応	対応	対応
バージョン 2.0 (オンプレミス)	対応	対応	対応	対応	対応	対応	対応
バージョン 2.2 (オンプレミス)	対応	対応	対応	対応	対応	対応	対応

コネクタの詳細は次のとおりです。

- Amazon Web Services (AWS)

詳細については、[Amazon ドキュメントサイトの「AWS リソースのタグ付け」](#)などのリソースを参照してください。

- **GitHub**

詳細については、[GitHub コネクタの作成](#)を参照してください。

- **Google クラウド**

詳細については、[Google Cloud ドキュメントの「環境設定」](#)を参照してください。

- **Microsoft Azure**

詳細については、[Azure ドキュメントサイトのこのページ](#)を参照してください。

- **Microsoft Azure サービスタグ**

詳細については、[Microsoft TechNet の「仮想ネットワークサービスタグ」](#)などのリソースを参照してください。

- **Office 365 の IP アドレス**

詳細については、[docs.microsoft.com の「Office 365 URL および IP アドレス範囲」](#)を参照してください。

- **vCenter と NSX-T によって管理される VMware のカテゴリとタグ**

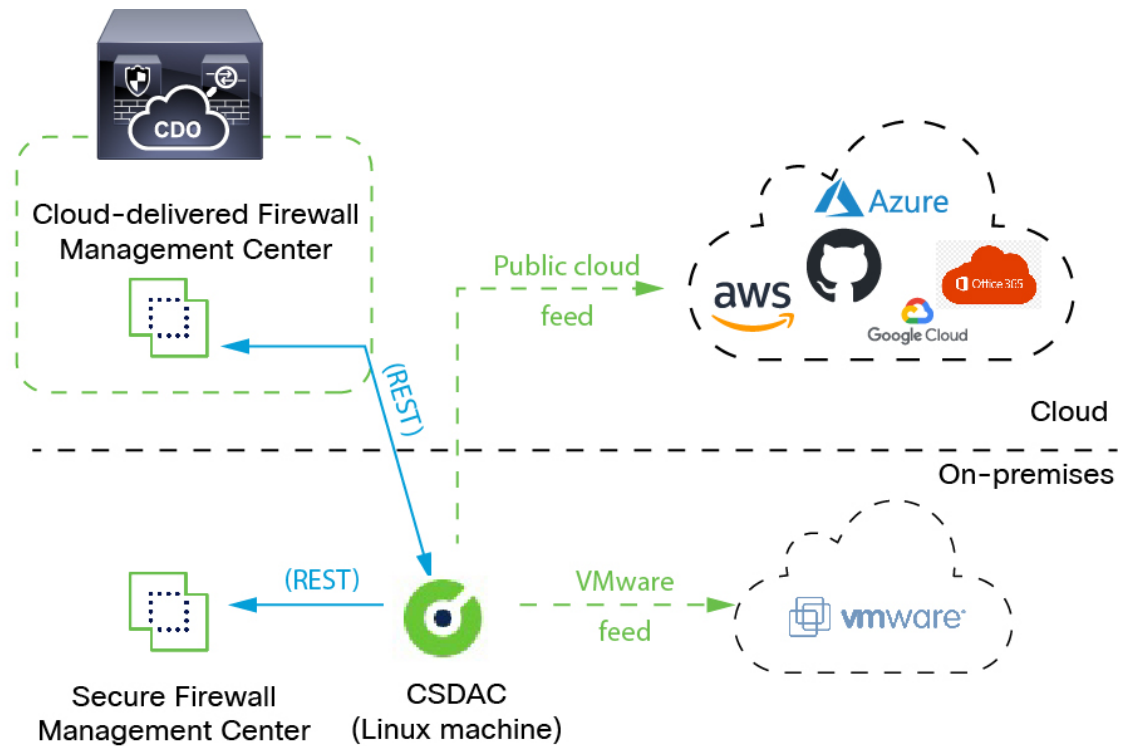
詳細については、[VMware ドキュメントサイトの「vSphere タグと属性」](#)などのリソースを参照してください。

機能の仕組み

ワークロードの動的な性質と IP アドレスの重複の必然性により、IP アドレスなどのネットワーク構造は、仮想、クラウド、およびコンテナ環境では信頼できません。お客様は、IP アドレスや VLAN が変更されてもファイアウォールポリシーが持続するように、VM 名やセキュリティグループなどの非ネットワーク構造に基づいてポリシールールを定義する必要があります。

これらのタグと属性は、Ubuntu、CentOS、または Red Hat Enterprise Linux 仮想マシンで実行されている動的属性コネクタ Docker コンテナを使用して収集できます。Ansible コレクションを使用して、Ubuntu ホストに動的属性コネクタをインストールします。

次の図は、システムが高レベルでどのように機能するかを示しています。



- サポートされている Linux 仮想マシンに 動的属性コネクタ をインストールします。
詳細については、[サポートされているオペレーティングシステムとサードパーティソフトウェア](#)を参照してください。
- システムは、特定のパブリック クラウドプロバイダーをサポートします。
このトピックでは、サポートされているコネクタ（これらのプロバイダーへの接続）について説明します。
- 動的属性コネクタ によって定義されたアダプタは、これらの動的属性フィルタをダイナミックオブジェクトとして受け取り、アクセス制御ルールで使用できるようにします。
次のタイプのアダプタを作成できます。
 - オンプレミスの Management Center デバイスの場合、オンプレミス *Firewall Management Center*。
このタイプ of Management Center デバイスは、Cisco Defense Orchestrator (CDO) によって管理されるか、スタンドアロンである可能性があります。
 - CDO が管理するデバイスの場合、クラウド提供型 *Firewall Management Center* 。

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。