

プライベートチャットGPTを設定し、他のジェネレーティブAIアプリケーションへのアクセスを制限する

内容

[はじめに](#)

[概要](#)

[ステップ1：プライベートチャットを許可するWebルールの作成GPT](#)

[ステップ2：他のすべてのジェネレーティブAIアプリをブロックする](#)

[DNSポリシー](#)

[Web Policy](#)

はじめに

このドキュメントでは、プライベートChatGPTを設定し、他のジェネレーティブAIアプリケーションへのアクセスを制限する方法について説明します。

概要

人工知能の世界は急速に進化しており、その進化の中でも特に注目されているのがジェネレーティブAIの発展です。その中でも、ChatGPTは大きな効果をもたらしました。

組織がこれらの強力なツールをワークフローに統合しようとするにつれ、ジェネレーティブAIアプリケーションへのアクセスを制御する必要性がますます明らかになっています。独自のプライベートChatGPTインスタンスを開発している企業にとって、他のジェネレーティブAIアプリを制限しながら、これがチームがアクセスできる唯一のAIツールであることを確認することは、重要なセキュリティ対策です。

幸いなことに、Umbrellaダッシュボードを使用してこれを実現する簡単な方法があります。この記事では、他のAIアプリケーションの使用を厳密に制御しながら、組織がプライベートChatGPTの恩恵を受けるために必要な手順を説明します。

ステップ1：プライベートチャットを許可するWebルールの作成GPT

まず、Umbrellaダッシュボードにログインする必要があります。その後、DNSルールまたはWebルールを作成できます。

このルールには、プライベートChatGPTの特定のURLを含む「許可」アクションと「宛先リスト」が必要です。

この手順により、組織内のユーザが制限なくプライベートChatGPTにアクセスできるようになります。

ステップ2：他のすべてのジェネレーティブAIアプリをブロックする

許可ルールを作成後すぐに、2つ目のルールを作成する必要があります。

このルールには「ブロック」アクションが必要で、ジェネレーティブAIカテゴリを含む「アプリケーションリスト」を含める必要があります。

これにより、ChatGPTの公開バージョンを含む、幅広い一般的なジェネレーティブAIアプリケーションへのアクセスを防ぐことができます。

DNSポリシー

WebポリシーではなくDNSポリシーを使用する際に、これらのルールが効果的に適用されるようにします。

シームレスなエクスペリエンスを実現するには、インテリジェントなプロキシとSSL復号化を有効にすることが重要です。また、SSL復号化が適切に機能するには、Cisco Umbrellaルート証明書のインストールが必要です。

DNSポリシーの設定に関する包括的なガイダンスについては、[こちら](#)の公式ドキュメントを参照してください。

また、DNSポリシーの効果を最適化するには、[ここ](#)のベストプラクティスを確認してください。

Web Policy

Webポリシーの管理と、組織の要件に合わせたポリシーの調整の詳細については、[ここ](#)を参照してください。

これらの対策を実装することで、組織はプライベートChatGPTを最大限に活用しながら、他のジェネレーティブAIアプリの使用に伴うデータ漏洩や妨害のリスクを軽減できます。セキュリティとアクセシビリティの適切なバランスは、組織のデータとリソースを十分に保護しながら、ジェネレーティブAIの可能性を活用するための鍵となります。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。