

ChatGPTによる機密データの使用を防止するためのDLPの設定

内容

[はじめに](#)

[概要](#)

はじめに

このドキュメントでは、データ損失防止(DLP)を使用して、ChatGPTによる機密データの使用を防止する方法について説明します。

概要

人工知能の世界は、OpenAIの言語モデルであるChatGPTのようなイノベーションが訴追をリードし、賑やかさを増しています。このAIを活用した企業は急速に成長し、スマートでコンテキスト認識型の会話によって多くの業界を変革してきました。しかし、こうした画期的な進歩によって、特にデータ損失のリスクなど、いくつかの潜在的な課題が生じます。

ChatGPTは、フィードに基づいてテキストを生成する超スマートな会話パートナーと考えてください。機密情報が混在していて、適切に処理されない場合、データ漏洩のリスクがあります。包括的なデータ損失防止(DLP)計画を立てることが非常に重要である理由が明らかになります。

貴社のUmbrella DLPソリューションは、このようなリスクから組織を守るように設計されています。ここでは、シスコのソリューションが迅速に対応し、実装に約5分しかかからない、緊急のユースケースを3つ示します。

A. GDPR、HIPPA、PCI-DSSなどのデータプライバシー規制への準拠：

1. Umbrellaダッシュボードで、Policies > Management > Data Loss Prevention Policyの順に選択します。
2. 新しいDLPルールを作成を開始します。右上のAdd Ruleをクリックして、Real Time Ruleを選択するだけです。
3. ルールに「ChatGPT Protection」などの認識しやすい名前を付け、ニーズに合った重大度レベル（低から重大まで）を選択します。
4. [分類]セクションで、組織に関連する組み込みのコンプライアンス分類を1つ以上選択します。たとえば、「組み込みGDPR分類」や「組み込みPCI分類」などです。
5. Identitiesセクションで、モニタおよび保護するすべてのIDを選択します。可能であれば、包括的なカバレッジの幅広い選択肢を推奨します。
6. Destinationsセクションに進み、Destination Lists and Applications for Inclusionを選択してから、OpenAI ChatGPTを選択します。
7. 今こそ行動する時だ。Actionセクションでは、MonitorまたはBlockのいずれかを選択します。初めてご使用になる場合は、「Monitor」アクションから始めることをお勧め

します。これにより、使用パターンを観察し、潜在的なリスクと利点について、より多くの情報に基づいて決定することができます。

8. 「モニタ」アクションを選択した場合は、1週間または1カ月後にDLPレポートを必ず確認してください。これにより、ChatGPTで機密情報を共有しているユーザと、そのタイミングが分かり、「ブロック」アクションが必要かどうかを判断できます。

B.個人情報(PII)の保護：組織のPIIをChatGPTリスクから保護するには、上記と同じ手順を使用しますが、ステップ4で、コンプライアンス分類の代わりに「組み込みPII分類」を選択します。

C.ソースコードと知的財産の保護：ソースコードやその他の知的財産に関するアクティビティでChatGPTを使用する場合は、次の手順に従います。

1. 最初に、新しいソースコードデータ分類を作成します。Policies > Management > Policy Components > Data Classificationの順に移動します。右上のAddボタンをクリックして、データ分類に「Source Code Classification」などの認識可能な名前を付けます。
2. Built-In Data IdentifiersのリストからSource Codeを選択します。
3. [Save] をクリックします。
4. 保存後、上記の「データプライバシー規制への準拠」の手順を再度参照してください。ただし、ステップ4では、組み込みデータの代わりに新しく作成されたソースコードデータ分類を選択します。

このプロセスは簡単で、ほんの数分で完了しますが、組織のセキュリティとコンプライアンスに対するメリットは非常に大きなものです。お客様のデータ保護を強化するために、これらの措置を可能な限り迅速に講じることを強くお勧めします。

ジェネレーティブAIのリスクとUmbrellaがあなたを守る方法について詳しくは、ウェビナー「[ChatGPTの使用から機密データを保護する](#)」をご覧ください。

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。