Solution Brief

THALES
CYBERSECURITY

CipherTrust Tokenization：イノベーションを妨げることなくAIを安全に保護するトークナイゼーション

cpl.thalesgroup.com

THALES

CYBERSECURITY

次のようなニーズがある場合

- **プロンプトや検索処理時に規制対象データを露出させることなくAIを導入したい**
- **ログ、埋め込みデータ、AI生成出力に機密データが残存することを防ぎたい**
- **AIを活用したワークフロー全体で、PCI DSS 4.0およびプライバシー要件への継続的な準拠を維持したい**
- **データ使用時のリスクを拡大させることなく、生成AI、基盤モデル、AIエージェントへのデータ投入前に適切な保護を適用したい**

課題

今日の経営層は、競争力を維持するためにAIを導入するという大きなプレッシャーにさらされています。しかし、AIチャットボットや大規模言語モデル（LLM）は、データセキュリティ上の重大なリスクをもたらします。機密データがプロンプトに入力されると、その情報がモデルのメモリやログに取り込まれてしまう可能性があるためです。AIを活用したイノベーションを実現しながら、新たな脆弱性を生み出さないことが、現代の経営幹部が直面する最重量課題となっています。

AIとの1回のやり取りであっても、複数のシステムにわたる検索処理を引き起こし、派生的な成果物を生成し、データベースに書き込まれる新しいデータレコードを作成し、組織内の他の場所で再利用される出力を生み出す可能性があります。AIシステムは単にデータにアクセスするだけでなく、データを複製、変換、要約、埋め込み、再利用を実行します。

機密データが平文のまま伝播してしまうと、ガバナンスは指数関数的に複雑化し、場合によっては取り返しのつかない事態を招きます。

セキュリティとプライバシーの両面から、もはや問うべきは「誰がデータにアクセスできるか」ではありません。今や問うべきは、「データはどこへ伝播し、その場所でもガバナンスを維持できるのか」です。

タレスのソリューション

タレスのCipherTrust Tokenizationソリューションは、組織がAIシステムに対して「目隠し」を施すことを可能にします。これにより、ビジネス分析の処理内容を変更することなく、AIにおける2つの重量なデータ露出境界を越える前に機密データを除去できます。

1. 実行時の露出境界 - AIシステムはデータ処理時にPII、PCI、PHIを受け取る可能性があります。
   - ユーザーのプロンプトを受け取る
   - 質問に答えるために企業データを検索する
   - 規制対象情報を含む可能性のある応答を組み立てる
2. 永続的な露出境界 - AIが処理後にデータを保存または伝播する場所に機密データが残存する可能性があります。
   - 学習およびファインチューニング用データセット
   - ベクトルデータベースおよび埋め込みデータ
   - プロンプトログおよびテレメトリシステム
   - AIエージェントおよびオーケストレーションワークフロー
   - 人によるレビュー環境
   - 業務システム全体で再利用される生成出力
   - 外部AIサービス

CipherTrust Tokenizationソリューションは、データがAIワークフローに入る前に機密データをトークンに置き換えるアーキテクチャ上の保護策です。トークナイゼーションにより、AIシステムは規制対象データを平文で受け取ることなく、コンテキスト、構造、参照整合性を取得できます。

CipherTrust Tokenizationソリューション

実行時および永続的な露出境界の保護

CipherTrust Tokenizationソリューションには、データが組織のアプリケーション層に入った瞬間から機密データの保護を開始するための、相互運用可能な3つのコネクタが含まれています。これら3つのコネクタは、ポリシー、鍵管理、トークンを共有します。

相互運用性により、アプリケーション層で適用された保護が、API、データベース、分析システム、AIプラットフォーム全体で一貫して維持されます。

単一ポリシーモデルにより、アプリケーション、API、データパイプライン、AIプラットフォーム全体で一貫した保護が実現し、断片化した制御や不整合な適用が排除されます。

- CipherTrust Application Data Protection (CADP SDK)
- CipherTrust RESTful Data Protection (CRDP RESTful API)
- CipherTrust Data Protection Gateway (DPG)

CADP SDK

CADPは、SDKを通じてアプリケーションやAI対応サービスに直接統合されます。

開発者は、プロンプトが処理される前やレコードが取得される前に機密フィールドをトークン化します。デトークナイゼーションは厳密に制御され、ポリシーに基づいて実行されます。きめ細かなコードレベルの制御により、ガバナンスを損なうことなく高パフォーマンスなAIワークロードを実現できます。

CRDP RESTful API

CRDPは、API中心のアーキテクチャ向けに、RESTfulなトークナイゼーションおよびデトークナイゼーションを提供します。

組み込みSDKを必要とせず、マイクロサービス、サーバーレスワークフロー、AI駆動型アプリケーションを保護できます。

組織は、柔軟でクラウドネイティブなAIアーキテクチャを実現しつつ、一元化されたポリシー管理を維持できます。

DPG API Gateway

DPGはプロキシとして動作し、RESTfulサービス間を流れるデータを透過的にトークン化またはデトークン化します。

アプリケーションを書き換えることなく、レガシーデータベース、検索パイプライン、RAGアーキテクチャを保護します。

セキュリティチームは、近代化の取り組みを妨げることなく、AIワークロードへの保護を拡張できます。

下流工程での信頼性

CipherTrust Tokenizationソリューションは、アプリケーション、API、データパイプライン、AIプラットフォーム全体で一貫したトークンを生成し管理することで、後続システムへの信頼性を確保します。この一貫性により、以下が可能になります。

- AIが生成した出力を、安全にCRMシステムに連携
- 分析プラットフォームがPII（個人識別情報）を再導入することなくデータセットを結合
- 不正検知システムが生の識別子を使用せずにパターンを検出
- BIシステムがコンプライアンス範囲を拡大させることなく運用

セキュリティ、プライバシー、イノベーションが、互いに矛盾することなく同時に前進できるようになります。

CipherTrust Tokenizationソリューションのメリット

- ハイブリッド、マルチクラウド、オンプレミスを含むあらゆる環境のAIシステムから機密データの除外
- PCI DSS 4.0およびプライバシー関連のコンプライアンス範囲の縮小
- 分析、RAG、機械学習（ML）の機能を維持
- 断片化した制御や不整合な適用を排除
- アプリケーション層で適用した保護を、API、データベース、分析システム、AIプラットフォーム全体で一貫して維持

主なユースケース

- AIチャットボットおよびCopilotの保護
- 安全なRAG（検索強化生成）の実現
- AIの学習およびファインチューニング
- ベクトルデータベース、SQLデータベース、データレイクハウスの保護

各ユースケースは、「機密データが平文のままAIシステムに入らない」という一つの目的に基づいています。

結論

CipherTrust　Tokenizationソリューションは、機密データを使用することなく、AIワークフローやBI分析をそのままの形で実行できるようにします。システムから機密データを除去することで、機密データが平文のままAIシステムに入ることも、意図した境界を越えて伝播することもありません。これにより、コンプライアンス対応と導入が簡素化され、監査コストが削減され、規制当局、顧客、取締役会に対して自信を持って対応できる体制が整います。

アプリケーション層、API層、データ層にわたる統一されたポリシー駆動型のトークナイゼーションにより、AIは機密データを学習することなく、パターンだけを学習できます。

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に、かつ最高の投資対効果（ROI）で保護できるよう支援しています。フォーチュン・グローバル500企業の58%を含む3万社以上の顧客を抱え、そのソリューションは世界148カ国で導入されています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心で信頼性の高いデジタルエクスペリエンスを提供します。

お問い合わせ先 – 連絡先情報につきましては、cpl.thalesgroup.com/ja/contact-us をご覧ください。