Product Brief

CipherTrust Cloud Key Manager クラウド暗号鍵のライフサイクル管理

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

クラウドセキュリティアライアンス（CSA）が定義する業界のベストプラクティスでは、暗号鍵はクラウドサービスプロバイダーおよび関連する暗号化操作から切り離して保管し管理する必要があるとされています[1]。クラウドサービスプロバイダー（CSP）は、BYOK（Bring Your Own Key; 独自の鍵の持ち込み）やHYOK（Hold Your Own Key; 独自の鍵の保持）サービスを提供して、データの暗号化に使用される鍵を顧客が管理できるようにすることで、ベストプラクティスに準拠できます。顧客は鍵を制御することで、暗号鍵、またはその鍵の作成に使用されるテナントシークレットの分離、作成、所有、管理、および失効が可能になります。CipherTrust Cloud Key Manager（CCKM）は、すべてのクラウド鍵がネイティブ鍵である場合でも、運用負担を軽減して効率の向上を実現できます。ライフサイクル管理、クラウド内およびクラウド間での一元管理、クラウド暗号鍵の可視性を顧客に提供することで、鍵管理の複雑さと運用コストを軽減します。顧客の報告では、異種混合環境での鍵管理から脱却して、クラウドへの安全な移行を実現するためにCCKMに投資したことで、クラウド利用が飛躍的に増加し、管理のオーバーヘッドと潜在的なセキュリティホールを削減できたと評価されています。

クラウド暗号鍵の制御

- BYOKやHYOKサービスの価値を活用してクラウド暗号鍵の完全なライフサイクル管理を実現します。
- 鍵の検出、ネイティブクラウド鍵の管理、鍵の自動ローテーションなど、ハイブリッド、シングルクラウド、マルチクラウド環境にわたる鍵を一元管理することで、効率の向上を実現します。
- セキュアな鍵作成により、極めて厳格なデータ保護要件に対応します。
- 優れたUIを備えた強固なマルチクラウドプラットフォームを使用することで、ネイティブ鍵のメリットを増大させます。

ベストプラクティス

業界や社内のデータ保護要件により、クラウド上の機密データに対する保護の強化が求められています。一方、CSAや業界アナリストは、クラウドの暗号鍵は顧客が管理すべきであるとしています。鍵管理システム（KMS）は、1つのKMSにつき数百ものマスター鍵にまで拡大する可能性があり、鍵のバックアップ、監視、ローテーション、失効、アーカイブ、停止、復元、破棄に加えて、暗号鍵がいつ、誰に、どのように使用されているかを把握する必要があります。CCKMは、包括的な鍵のライフサイクル管理を実現し、単一のコンソールに可視化し、複数のクラウドにわたる安全で包括的な鍵管理を自動化して要件を満たします。

効率の向上

CCKMは、効率向上をサポートする複数の機能を提供しています。

- 複数のクラウド、リージョン、アカウント、サブスクリプション、プロジェクト、アプリケーション、組織IDなどにまたがる、ネイティブ、BYOK、HYOKのクラウド鍵を単一のブラウザウィンドウから安全に一元管理できます。
- クラウドプロバイダーですでに何千ものクラウドネイティブ鍵を作成している場合でも、鍵の一元管理でクラウドコンソール固有の鍵操作を把握できるように自動同期します。
- 鍵の自動ローテーションや、鍵の有効期限切れのサポートにより、貴重な時間を節約しながらコンプライアンスを確保します。
- メタデータは、すべてのクラウドプロバイダーに対して同じ順序で収集し配置されるため、さまざまな場所でデータを探す必要がありません。

単一のコンソール

複数のアカウント、リージョン、サブスクリプション、プロジェクトにわたり、単一のコンソールからそれぞれのクラウドプロバイダーにアクセスできるため、企業は複数のクラウドにまたがるワークロードがどのように保護されているかを容易に把握できます。タレスは、管理者が鍵へのアクセスを数日ではなく数分で容易に管理および制御し、脅威を迅速に阻止できるよう、常に鍵の可視性向上を図っています。

暗号鍵に対する強力なセキュリティ

顧客による鍵管理には、安全な鍵生成と保管が必要となります。CCKMは、CipherTrust Manager、Luna Network HSM、またはVormetric Data Security Manager (DSM)のセキュリティを活用し、最大FIPS 140-2 Level 3のセキュリティで鍵を生成します。

HYOK（Hold Your Own Key; 独自の鍵の保持）

CCKMサービスは、クラウドプロバイダーからの暗号鍵のリクエストに対応します。AWS External Key Store (XKS)、Google Cloud External Key Management (EKM)、Google EKM Ubiquitous Data Encryption (UDE)、Google Workspaceのドライブ / Gmail / Googleカレンダー / Google Meetのクライアントサイド暗号化、Salesforce Cached Keysなど、数多くの新しいHYOKサービスをサポートしています。

必要不可欠なコンプライアンスツール

可視化レポートは、ミッションクリティカルなワークロードについて、規制当局にコンプライアンスを証明します。ログはsyslogサーバーやSIEM（Security Information and Event Management; セキュリティ情報イベント管理）ツールに転送することもできます。

1 CSA CCM EKM-04を参照してください。

イニシアチブをサポートする自動化ツール

CCKMの機能は、RESTful APIを使用してプログラム的に利用可能であり、クラウド暗号化の一元管理のメリットを自動化やセルフサービスイニシアチブに活用できます。組み込みのAPIプレイグラウンドでAPIをインタラクティブに探索できます。

柔軟な展開オプション

展開環境には、パブリッククラウド、プライベートクラウド、ハイブリッドクラウド、物理アプライアンス、As-a-Cloudベースのサブスクリプションサービスがあります。

CCKMを展開する方法や場所にかかわらず、CCKMは、サポートされているクラウド上で、鍵や鍵へのアクセスを管理できます。

CCKMは、さまざまな組織のニーズを満たすために、仮想および物理フォームファクタで提供されています。仮想CCKMは、簡単に導入できるオールソフトウェア製品です。クラウドまたはオンプレミスで実行でき、さまざまなクラウドプロバイダーのマーケットプレイスで見つけられ、迅速にインスタンス化できます。オンプレミスのソリューションをご希望の場合は、物理アプライアンスをご利用いただけます。CCKMサービスは、Thales Data Protection on Demand（DPoD）マーケットプレイスおよびCSPマーケットプレイスを通じてオンデマンドで利用可能です。

マルチクラウドデータセキュリティソリューション

CCKMは、クラウドサービスの暗号鍵の制御と管理の必要性を簡素化し、業界や組織のデータ保護要件を満たすための重要なソリューションです。CCKMをはじめ、さまざまなBring Your Own Advanced Encryptionサービスを含む数多くのタレスマルチクラウドセキュリティ製品は、すべて鍵の一元管理が可能であり、クラウド上の全データを保護する最適な方法に関して、幅広い選択肢を提供します。クラウド上のデータは自ら保護する必要があるのです。

タレスについて

皆様が信頼して個人情報を預けている事業者の多くは、そのデータを保護するためにタレスのテクノロジーを採用しています。データセキュリティに関して組織が決断を求められる局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の遵守のいずれであっても、デジタルトランスフォーメーションの推進と保護をタレスはお手伝いします。

決断の瞬間のための、確実なテクノロジー。

サポート対象のクラウドと鍵管理の所有権モデル:

顧客による制御範囲が拡大

Amazon Web Services (AWS) KMS	ネイティブ	BYOK	
AWS CloudHSM	ネイティブ		
AWS XKS			HYOK
AWS China	ネイティブ	BYOK	
AWS GovCloud	ネイティブ	BYOK	HYOK
Google Cloud Platform CMEK	ネイティブ	BYOK	
Google Cloud Platform EKM			HYOK
Google Cloud Platform EKM UDE			HYOK-CC*
Google Workspace CSE			HYOK
IBM Cloud HPCS	ネイティブ	BYOK	
IBM Cloud Key Protect	ネイティブ	BYOK	
Microsoft Azure Cloud	ネイティブ	BYOK	
Microsoft Azure China	ネイティブ	BYOK	
Microsoft Azure GovCloud	ネイティブ	BYOK	
Microsoft Azure Managed HSMs	ネイティブ	BYOK	
Microsoft Office 365		BYOK	
Oracle Cloud Infrastructure	ネイティブ	BYOK	HYOK
Salesforce.com	ネイティブ	BYOK	HYOK **
Salesforce GovCloud Plus	ネイティブ	BYOK	HYOK **
Salesforce Sandbox	ネイティブ	BYOK	HYOK **
SAP Data Custodian	ネイティブ	BYOK	

*HYOK-CCは、Confidential Computing用のHYOK
** キャッシュのみの鍵サービス

cpl.thalesgroup.com

お問い合わせ先 – Email: cpl.jpsales@thalesgroup.comすべてのオフィスの所在地と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。