ソリューションブリーフ

Thales CipherTrust Cloud Key Managementと Oracle Cloud Infrastructureの統合

cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

THALES
Building a future we can all trust

メリット

- PCI DSS、GDPR、Schrems II、CCPAなどのコンプライアンス要件に準拠
- シームレスな鍵ローテーションでデータ暗号化管理を合理化
- 職務分掌を可能にし、自社のデータをより細かく制御
- 鍵とポリシーの一元管理により、管理コストを削減
- FIPS 140-2 Level 3ハードウェアセキュリティ（オプション）

課題

Oracle Cloud Infrastructure（OCI）の採用が急激に増え続けています。従来のオンプレミスの実装からOCIへの移行を成功させるには、組織はまず機密データのセキュリティに対処する必要があります。OCIのネイティブ暗号化は、機密データの安全なOCIへの移行を実現しますが、管理やコンプライアンスに新たな影響も与えます。OCIの価値を最大限に引き出すには、機密データの制御を維持し、セキュリティ管理を合理化する方法を見つける必要があります。幸い、タレスはオラクルとともに、機密データをOCIに移行する際のデータ保護管理の課題を軽減します。

ソリューション

タレスのCipherTrust Cloud Key Management（CCKM）は、セキュリティ管理を効率化し、可視性を提供します。OCI External Key Management Service（EKMS）とCCKMの統合により、組織はOCIの外部で鍵を物理的に保管し、単一のコンソールを使用してOCIサービスやその他のクラウド暗号化ソリューションの暗号鍵ライフサイクルをシームレスに管理できます。OCIは、クラウド上のデータを保護するために、可視性とセキュリティを統合した鍵管理を提供します。OCIの暗号化とCCKMの組み合わせにより、組織はシームレスなエンドツーエンドのセキュリティを実現できます。顧客による暗号鍵の制御を可能にするため、タレスのソリューションは、Oracle Native Key Management、BYOK（Bring Your Own Key; 独自の鍵の持ち込み）、HYOK（Hold Your Own Key; 独自の鍵の保持）サービスに対応しています。

ネイティブ鍵

ネイティブ鍵はOCI Vaultから利用できます。CCKMは、鍵のインベントリとローテーションを自動化してコンプライアンスを簡素化し、すでに何千ものネイティブクラウド鍵を作成していたとしても、OCI鍵の操作をタレスの集中型鍵マネージャーから確認できるようにします。

BYOK（Bring Your Own Key; 独自の鍵の持ち込み）

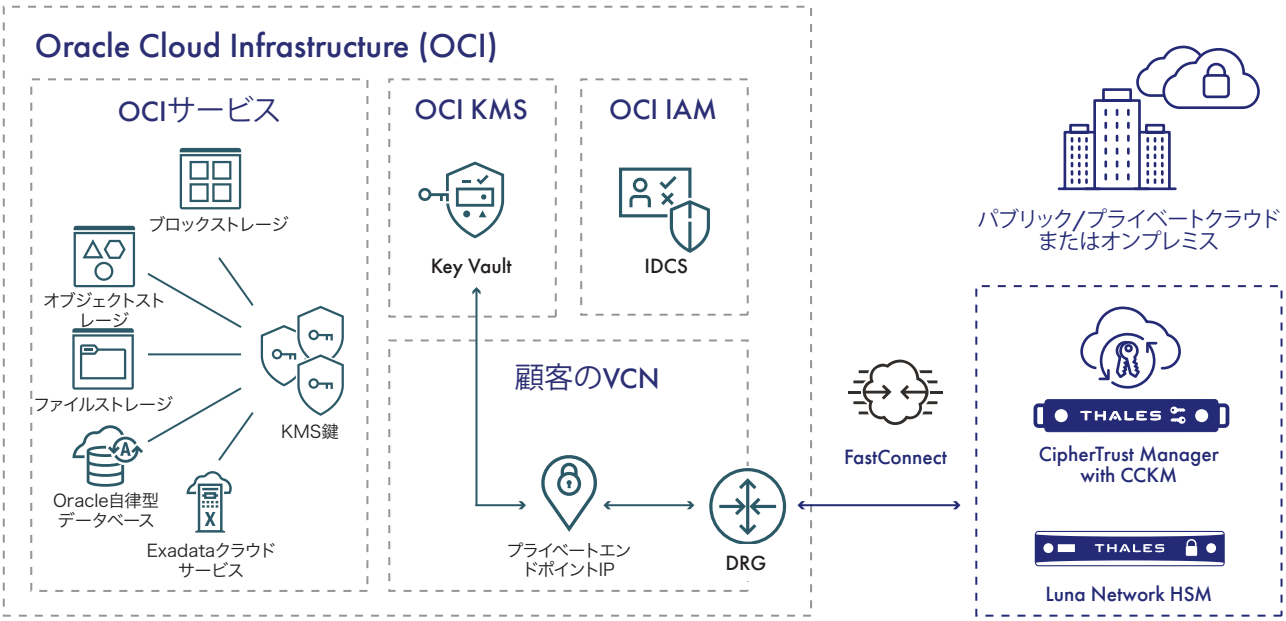
顧客が鍵を管理して、暗号鍵を分離、作成、所有、管理、失効することが可能です。CCKMは、クラウドプロバイダーのBYOK APIを活用し、一元管理と可視性を備えたクラウド暗号鍵のライフサイクル管理を提供することで、鍵管理の複雑さと運用コストを軽減します。

HYOK（Hold Your Own Key; 独自の鍵の保持）

OCI EKMSを使用すると、OCI顧客は暗号鍵をHYOKモデルでクラウドの外部に物理的に保管できます。そのため、職務分掌が可能になり、自社のデータ保護をより細かく制御できるようになります。タレスはOCIと共同でEKMSサービスを開発し、その結果、OCI顧客が利用できる最初のHYOKソリューションが実現しました。CCKMを使用することで、組織はOCI暗号鍵の保管とライフサイクル管理を、OCI以外の暗号化に使用するものと同じ集中型鍵マネージャーに統合できます。

CCKMは、CipherTrust ManagerまたはLuna Network HSMに保管されている鍵をサポートします。管理者は、外部に保管された鍵をOCIで使用できるようにする前に、共有を明示的に許可する必要があります。CCKMでOCI暗号化サービスを利用できるにもかかわらず、顧客は暗号鍵、ひいてはデータの制御をしっかりと維持できます。

図1. 導入アーキテクチャ例 - OCIの外部でホストされたCCKM



サポート対象のOracle Cloud Services

以下のサービスはOCI EKMSと統合されており、顧客管理の鍵の使用をサポートし、それぞれの指定されたリソース内のデータを暗号化します。

- ブロックボリューム
- Kubernetes用コンテナエンジン
- データベース
- ファイルストレージ
- オブジェクトストレージ
- ストリーミング

ポリシーを一元的に定義および管理して職務分掌を実現

管理者はCCKMを使用して、どのユーザーとプロセスに暗号化データへの平文アクセスを許可するかを定義する認証・認可ポリシーを設定できます。組織は、これらの制御を通じて機密データのガバナンスを強化します。適切に調整されたポリシーベースのアクセス制御は、IT管理者とセキュリティ管理者の明確な職務分掌が求められる組織に、重要なセキュリティ層を提供します。

監査およびレポート要件に対応する詳細なロギング機能

CCKMは、鍵の状態とアクセスに関する詳細なデータを一元化されたログに記録し、監査人や規制当局へのレポートを簡素化します。鍵の使用状況とアクセス要求を一元的に追跡することで、盲点を減らし、データセキュリティを向上させます。CCKMのレポートは、OCIのネイティブ暗号鍵のセキュリティを強化するのと同時に、コンプライアンスレポートプロセスを合理化するのにも役立ちます。

合理化、簡素化された暗号化管理

ベンダーが提供する暗号化は、適切に管理しなければ、簡単にセキュリティサイロの集合体になってしまいます。CCKMは、OCIの暗号鍵を使いやすいプラットフォームに統合します。これにより、さまざまな暗号化ソリューション（透過的暗号化、アプリケーションデータ保護、データベース保護、OASIS Key Management Interoperability Protocol（KMIP）標準をサポートするベンダーの増え続けるリスト等）の鍵と一緒に、OCI鍵を管理できます。

あらゆるニーズに対応する柔軟な導入オプション

CCKMは、仮想マシン、物理アプライアンス、アズアサービスとして提供されます。仮想CCKMは、OCI、オンプレミス、さまざまなサードパーティの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、マルチクラウド、物理アプライアンス、そしてクラウドベースのサブスクリプションサービスに容易に導入、実行できるオールソフトウェアソリューションです。暗号鍵の保管や管理をオンプレミスで行いたい組織には、最も厳しい要件を満たす物理アプライアンスのオプションが用意されています。

まとめ

OCIのネイティブ暗号化機能は、顧客が機密データをクラウドに移行する際に必要なセキュリティを提供します。タレスの暗号鍵管理を使用すると、データを保護するためのさらなる制御が提供され、自社のデータが自社のデータセンターの壁の外に存在していても、そのデータを自社のみが管理していることを証明するために必要なツールが提供されます。タレスとオラクルの組み合わせにより、顧客はクラウドの普及に伴うセキュリティ、コンプライアンス、主権に関する課題に対する強力なソリューションを手に入れることができます。

タレスについて

今日の企業は、決定的な意思決定を行うために、クラウド、データ、ソフトウェアに依存しています。そのため、世界で評判の高いブランドや最大手の組織は、クラウドやデータセンターからデバイス、ネットワーク全体に至るまで、作成、共有、保存場所を問わず機密情報やソフトウェアを保護し、それらへのアクセスを安全に確保するために、タレスに信頼を寄せています。当社のソリューションは、企業がクラウドに安全に移行し、自信を持ってコンプライアンスを達成し、何百万人もの消費者が毎日利用するデバイスやサービスにおいて、ソフトウェアからより大きな価値を生み出すことを可能にします。

Oracle Cloud Infrastructureについて

Oracle Cloud Infrastructure（OCI）は、クラウドインフラストラクチャサービスの深く幅広いプラットフォームです。スケーラブルでセキュアな、高可用性、高性能の環境に、さまざまなアプリケーションを構築および実行できます。アプリケーション開発やビジネスアナリティクスから、データ管理、インテグレーション、セキュリティ、AI、KubernetesやVMwareを含むインフラサービスまで、OCIは比類のないセキュリティ、パフォーマンス、コスト削減を実現します。さらに、マルチクラウド、ハイブリッドクラウド、パブリッククラウド、専用クラウドのオプションを備えたOCIの分散クラウドは、複数のクラウドにまたがる場合でも、データレジデンシー、ローカリティ、権限をより細かく制御できるクラウドのメリットを提供します。結果として、顧客は極めて厳しい規制コンプライアンス要件を満たしながら、企業ワークロードを迅速かつ効率的にクラウドに移行できます。

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。