cpl.thalesgroup.com

THALES
Building a future we can all trust

アジアの大手金融保証グループが、DXとコンプライアンスを実現
タレスソリューションによりビジネス課題を解決

要旨

アジア太平洋地域の大手金融保証グループが、高度にスケーラブルなタレスのソリューションを導入することで、保存データの保護と、さまざまな環境に分散したデータの保護および鍵管理を実現しています。これらはすべて、事業をどこで展開していても各地域の規制コンプライアンスを満たすモデルを提供しながら実現しています。

組織

このグループは、アジア太平洋地域でトップクラスの金融保証グループとして知られています。生命保険および健康保険ソリューションを通じて顧客を支援するために、構造的な成長市場に焦点を当てたアジア主導の事業ポートフォリオを構築しています。同グループはアジア太平洋地域において強力なプレゼンスを維持しており、シンガポール、香港、インドネシア、韓国、日本、ベトナムなど数カ国に数百万の顧客を抱えています。

現在、同グループは世界中の40以上の拠点にタレスのソリューションを展開しメリットを得ています。

ビジネスニーズ

デジタルトランスフォーメーションにより、同グループでは、データ分析、ビジネスアプリケーション、およびインフラストラクチャにおいてクラウドを活用するビジネスニーズが高まっています。これには、ハイブリッド環境やマルチクラウド環境で機能し、さまざまな環境にわたってデータ保護と鍵管理を提供する、高度にスケーラブルなソリューションが必要となります。

また、データをクラウドに移行すると同時に規制コンプライアンスを満たし、責任共有モデルを実践するための安全な道を顧客に提供することが不可欠です。

コンプライアンスの規制要件には、次のものがあります。

- PDPA（Personal Data Protection Act; 個人情報保護法）
- HIPAA（Health Insurance Portability and Accountability Act; 医療保険の携行性と責任に関する法律）
- PCI DSS（Payment Card Industry Data Security Standard; PCIデータセキュリティ基準）
- GDPR EU（General Data Protection Regulation; EU一般データ保護規則）

課題

金融機関の一部として、同グループは膨大な個人データ、医療データ、財務データを扱っています。保険会社として、重要な監査の課題に対処するためにコンプライアンスを満たしつつ、すべての顧客データを侵害から保護する法的責任があります。事業を展開している各国・各地域のデータプライバシー法に準拠していない場合は、重大な結果に直面します。たとえば、PCI Security Standards Councilによると、準拠していなければ、莫大な訴訟費用や和解金の支払い、さらに売上の減少に苦しむ可能性があります。

タレスは多くの国で事業を展開しており、さまざまな地域のプライバシー法についてお客様に助言する戦略的な役割を果たしています。

タレスは、保存データの保護に必要なツールを提供し、そのデータの暗号鍵をハードウェアの信頼の基点で安全に生成、保管、管理できるようにすることで、同グループの既存のインフラストラクチャを拡張する最初で唯一のベンダーとして選ばれました。

ソリューション

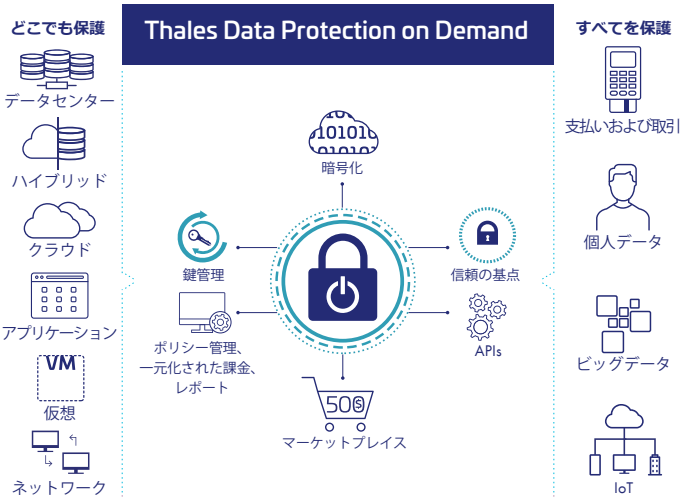
タレスは、同グループのデジタルトランスフォーメーションとコンプライアンスに関するビジネス課題を把握し、保存データの保護に必要なツールを提供してセキュリティインフラストラクチャを拡張するために、次のソリューションを推奨しました。

コンプライアンス要件への対応

個人データの脆弱な性質と、その使用、保存、処理方法を考えると、データの保護は不可欠です。データを保護するために、HIPAA、GDPR、PCI-DSSなどの規制が導入されており、データセキュリティ上の懸念やプライバシー規制に対処しています。

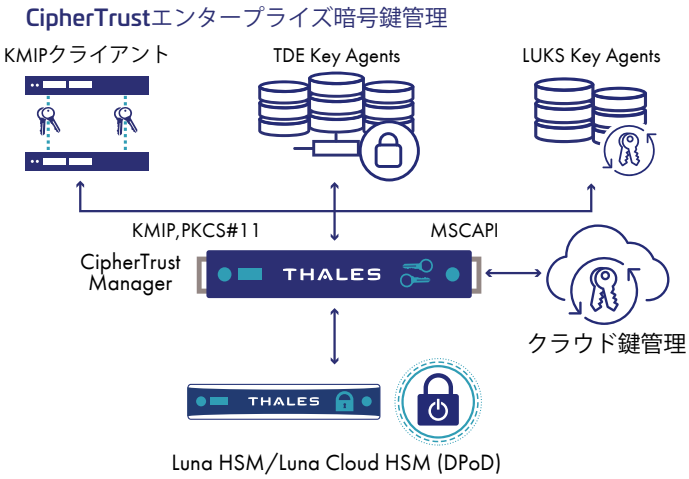
同グループは目標を達成するために、段階的なアプローチを採用しました。最も優先度の高いフェーズ1はコンプライアンスを満たすことであり、同グループはThales Data Protection on Demand Luna Cloud HSMサービスとCipherTrust Managerを選択しました。これにより、**FIPS 140-2 Level 3**の認定を受けた実証済みの暗号化ソリューションで、データセキュリティコンプライアンスのニーズを満たすことができます。

- Thales Data Protection on Demand は、シンプルなオンラインマーケットプレイスを通じて、さまざまなLuna Cloud HSMおよびCipherTrust Key Managementサービスを提供するクラウドベースのプラットフォームです。Data Protection on Demand（DPoD）では、ハードウェアの購入、導入、保守が不要なため、よりシンプルで費用対効果が高く、管理しやすいセキュリティ対策が可能になります。簡単な操作で必要な保護を導入し、サービスをプロビジョニングし、セキュリティポリシーを追加でき、使用状況レポートをわずか数分で取得することができます。DPoDが提供するさまざまなクラウドベースのLuna HSMサービスにより、クラウドでデータの暗号化に使用される暗号鍵を保管および管理でき、鍵の完全な制御を維持して幅広いユースケースや環境全体にわたる統合に対応できます。Luna HSMは、オンプレミスのハードウェア、またはクラウドやハイブリッド環境で利用可能な、FIPS 140-2認定の強固な耐タンパ性のアプライアンス内で暗号鍵を安全に管理、処理、保管します。



- CipherTrust Manager は、業界をリードするエンタープライズ暗号鍵管理ソリューションで、企業が暗号鍵を一元管理し、きめ細かなアクセス制御を提供し、セキュリティポリシーを策定できるようにします。CipherTrust Managerは、CipherTrust Data Security Platformの中央管理ポイントとしての役割を果たします。暗号鍵生成、ローテーション、破棄、インポート、エクスポートなどの暗号鍵のライフサイクルタスクを管理し、暗号鍵とポリシーへの役割ベースのアクセス制御を提供し、強力な監査とレポートをサポートし、開発者に優しいREST APIを提供します。

  CipherTrust Managerは、FIPS 140-2 Level 3に準拠したThales Luna HSM（オンプレミス/DPoDを通じたクラウドサービス/ハイブリッド環境での統合）またはサードパーティのハードウェアセキュリティモジュール（HSM）と統合する仮想アプライアンスと物理アプライアンスの両方で使用でき、最高レベルの信頼の基点を確保して暗号鍵の安全な保管を実現します。

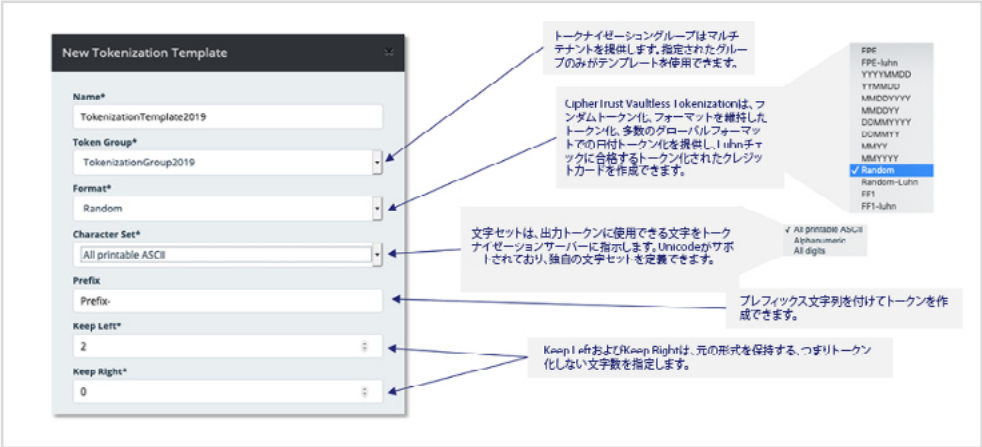


Vaultless Tokenizationによるオンプレミスからクラウドインフラストラクチャへのデータの安全な移行

フェーズ2では、タレスは、データをオンプレミスからクラウドインフラストラクチャに安全に移行するために**Vaultless Tokenization**を推奨しました。

Tokenization（トークナイゼーション/トークン化）により、セキュリティポリシーや、GDPR（EU一般データ保護規則）やPCI-DSS（PCIデータセキュリティ基準）などの規制要件に準拠するために必要なコストと労力が削減されます。

- CipherTrust Tokenization は、Dynamic Data Masking（動的データマスキング）によるVaultless TokenizationとVaulted Tokenizationという、お客様に完全な柔軟性を提供する2つの利便性の高いソリューションによって、アプリケーションレベルのデータトークン化サービスを提供します。どちらのソリューションも、機密性の高い資産を、データセンター、ビッグデータ環境、クラウドのいずれに所在するかを問わず保護および匿名化します。



Vaultless Tokenizationは、明確な職務分掌を実現するために、一元的な設定を提供します。

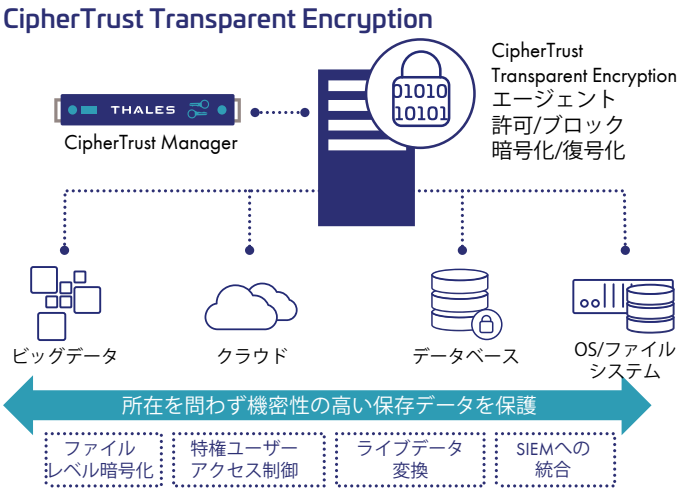
独自の鍵使用(BYOK; Bring Your Own Key)

タレスは、同グループがパブリッククラウドソリューションプロバイダーの鍵保管庫でBYOKアプローチを活用できるように、**Ciphertrust Cloud Key Manager**(CCKM)を導入しました。Thales CCKMを導入する主な目的は、クラウドに保存されたデータやコラボレーション用アプリケーションで使用されるデータに対して生成および保管される暗号鍵が、パブリッククラウドソリューションプロバイダーによって生成される代わりに、その暗号鍵の所有権を確保することでした。このソリューションにより、同グループは厳格な監査とコンプライアンスを満たしながら、強力な鍵管理の実現できます。

BYOKの導入から2年後、同グループは、独自の鍵使用(BYOK; Bring Your Own Key)から**独自の暗号化使用(BYOE; Bring Your Own Encryption)**へと移行しました。これは、クラウドセキュリティの最高レベルの保護です。

変化する環境の中でのデータベース暗号化

機密データを保護するには、データセンターのオンプレミスのデータベースとファイルを保護するだけでは不十分です。CipherTrust Manager の導入に加え、膨大な個人データ、医療データ、財務データを保護しつつデジタルトランスフォーメーションの旅をサポートするために、CipherTrust Transparent Encryption を推奨しました。



- CipherTrust Transparent Encryption は、鍵の一元管理、特権ユーザーアクセス制御、詳細なデータアクセスの監査ログ記録によって、保存データの暗号化を実現します。これにより、データの所在を問わず、データを保護するためのコンプライアンスとベストプラクティスの要件を満たすことができます。

  さらに、CipherTrust Transparent Encryptionにより、物理環境、仮想環境、クラウド環境でアクセス制御とデータアクセスの監査ログ記録を有効にしながら、ファイル、ボリューム、およびリンクされたクラウドストレージを保護する、実績があるハードウェアアクセラレーション暗号化ソリューションを使用して、暗号化、アクセス制御、データアクセスのログ記録に対するコンプライアンスとベストプラクティスの要件を満たすことが可能になります。

メリット

セキュリティとコンプライアンスの強化

タレスのデータ保護製品とソリューションは、さまざまなセキュリティおよびプライバシー要件への準拠に対応します。これには、eIDAS(electronic IDentification, Authentication and Trust Services; 電子識別およびトラストサービス)規則、PCI DSS(Payment Card Industry Data Security Standard; PCIデータセキュリティ基準)、GDPR(General Data Protection Regulation; 一般データ保護規則)、HIPAA(Health Insurance Portability and Accountability Act; 医療保険の携行性と責任に関する法律)、FISMA(Federal Information Security Management Act; 連邦情報セキュリティマネジメント法)、各地域のデータ保護とプライバシーに関する法律などが含まれます。

スタッフとリソースの効率の最適化

タレスは、連携して機能するように設計された製品、グローバル支援に対する単一のライン、進化する脅威から保護する確かな実績、業界最大のデータセキュリティのパートナーエコシステムにより、業界で最も幅広いデータセキュリティユースケースのサポートを提供します。タレスでは、使いやすさ、自動化のためのAPI、応答性の高い管理に重点を置いており、お客様のチームがビジネスの保護を迅速に導入、保護、監視できるようにします。さらに、タレスのプロフェッショナルサービスとパートナーは、設計、実装、トレーニングの支援を提供し、お客様のスタッフの時間使用を最小限に抑えながら迅速かつ信頼性の高い実装を保証します。

総所有コストの削減

タレスのデータ保護ポートフォリオは、包括的なデータセキュリティ製品とソリューションのセットを提供しており、新しいユースケースに容易に拡張可能で、新しいテクノロジーと従来のテクノロジーを保護してきた確かな実績を持ちます。タレスを採用すれば、運用コストと設備投資を削減しながら、将来にわたって投資を有効活用できます。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な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順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を保護するためにタレスに頼ることができます。

決断の瞬間のための、確実なテクノロジー。

> cpl.thalesgroup.com <

お問い合わせ先 – 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。