cpl.thalesgroup.com

THALES
Building a future we can all trust

導入事例（大学）：医療研究機密データの保護

概要

オーストラリアを代表する研究大学は、1958年に設立され、科学、法律、医学に関する主要な研究施設を有しています。世界のトップ75大学に常にランクインしており、3大陸にキャンパスを構えています。

ビジネス課題

同大学は研究施設であり、多くの医療施設と連携して、評価と研究を目的とした機密の医療データを大量に集めています。機密の医療データの各種ソースは、さまざまな場所のデータウェアハウスに保存されています。これらすべての機密データの扱いについて、同大学は、各地域のプライバシー規制に準拠する必要があると同時に、機密データを保護する必要性を認識していました。

技術的な課題

同大学は、保存中および転送中の機密の医療データを保護するために、オープンソースの暗号化ソリューションをいくつか導入していました。しかし、オープンソースの暗号化ソリューションには、次のような多くの課題がありました。

- 製品開発ロードマップがないため、これらのオープンソースソリューションは継続性が保証されていない。
- さまざまなソリューションプロバイダーのメンテナンスとサポートを行うために内部リソースを費やしており、高いオーバーヘッドが発生していた。
- 導入したオープンソースソリューションは、セキュリティ認定を取得していない。
- オープンソースの暗号化ソリューションは、暗号化したデータから暗号鍵を分離する機能を提供していない。

ソリューション

同大学の課題に対処するため、タレスは、さまざまな環境の暗号鍵を安全に管理するために、「ハードウェアベースの鍵管理ソリューション（DSM：Data Security Manager）」を提案しました。

DSMを使用することで、同大学は、安全な鍵の生成、バックアップ/復元、クラスタ化、非アクティブ化、削除など、すべての暗号鍵のライフサイクル全体を管理できます。さらに重要なことに、これにより、さまざまなVMクラスタやデータベースサーバーに保存されている機密データから暗号鍵を分離できるため、セキュリティが強化されます。

成果とメリット

同大学が採用したソリューションは、暗号鍵を管理するという現在の要件だけでなく、次のような将来の要件にも対応する柔軟性とスケーラビリティを備えています。

- 追加の暗号鍵を一元管理することで、データストレージを他の物理環境やクラウド環境に拡張できる
- クラウドに移行するときにBYOK（Bring Your Own Key：独自の鍵使用）またはBYOE（Bring Your Own Encryption：独自の暗号化使用）を実装する
- DSMの透過的なアプリケーション暗号化機能を使用して機密データを保護する
- FIPS 140-2 Level 1～3認定などのコンプライアンス要件を満たすことができる

ビジネスニーズ:

- さまざまな環境に保存されているデータから暗号鍵を分離する機能
- 単一のソリューションプロバイダーですべての暗号鍵の管理が可能

技術的なニーズ:

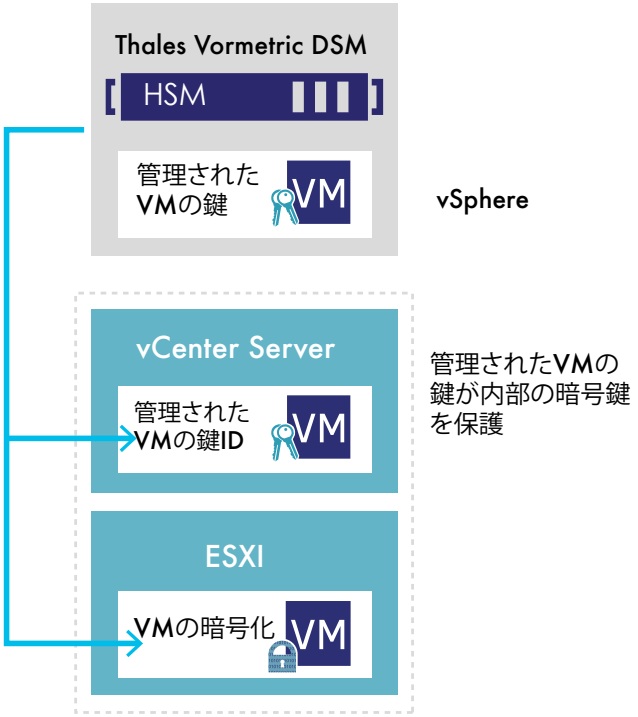
- すべての暗号鍵のライフサイクル全体を管理するソリューション
- 同大学の将来の要件も満たす、明確に定義された開発ロードマップを備えたソリューション

ソリューション:

- Thales Data Security Manager (DSM)

成果:

- 同大学の変化する要件をサポートできる世界クラスの暗号鍵管理の実装
- データセキュリティポリシーと鍵管理の一元管理を可能にし、トレーニング、展開、運用を効率化するソリューション



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。