cpl.thalesgroup.com

# VMwareとタレスがセキュアな仮想マシン暗号化ソリューションを提供

## 概要:

**デジタルトランスフォーメーションの中心にある仮想マシン（VM）の保護**

仮想マシン（VM）は、高まりつつあるデジタルトランスフォーメーションイニシアチブの中心にあります。そのテクノロジーを信頼して効果的に使用できることを保証するには、VM上で実行される重要なアプリケーションと機密データを保護する必要があります。情報漏えいは、厳しい罰金や、費用のかかる修復作業、評判の低下につながる可能性があります。

## 課題:

**管理オーバーヘッドと運用の柔軟性への影響を最小限に抑えながら、VMの入出力と保存データを暗号化する**

VMの入出力を暗号化することは新たな標準であり、ITインフラストラクチャの不可欠な要素です。ITインフラストラクチャは、企業のデジタルトランスフォーメーションを達成しようとするニーズを満たすために拡大しています。もう1つの必須要件は、保存データを保護することです。暗号化は一般に、特に増え続ける暗号鍵の管理に関して、操作に多大な労力を要すると見なされています。そのため革新的なテクノロジーと標準ベースのプロトコルによって、暗号化の操作および使用時により透過的になるようにします。

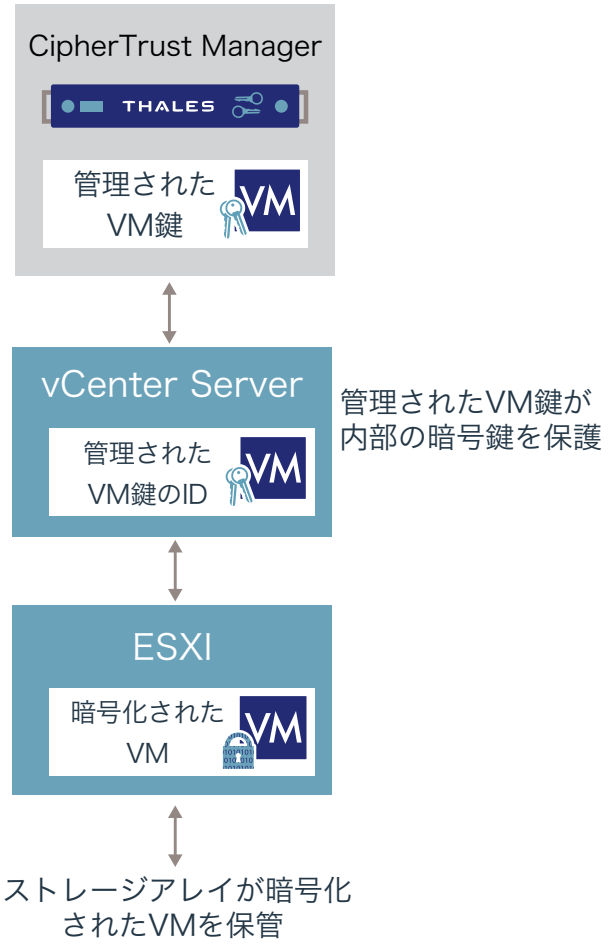
## ソリューション:

**VMware vSphere®仮想マシン暗号化とThales CipherTrust Manager**

VMware vSphere®は、業界をリードする仮想化プラットフォームであり、ユーザーはアプリケーションのスケールアップとスケールアウトを確実に実行できます。vSphereは、使用中のインフラストラクチャとアプリケーションから最高のパフォーマンス、可用性、効率性を引き出すことができます。これは、あらゆるクラウド環境にとって理想的な基盤です。

VMware vSphere VM暗号化は、vSphere 6.5で導入された機能で、仮想マシンの暗号化を可能にします。VM暗号化は、仮想マシンからの入出力をディスクに保存する前に暗号化することにより、仮想マシンファイル、仮想ディスクファイル、コアダンプファイルを保護します。このソリューションは、暗号鍵管理と鍵保管にKey Management Interoperability Protocol（KMIP）を使用します。

vSphereは、ソフトウェア仮想アプライアンスからFIPS 140-2 Level 3の物理的に保護された境界まで、お客様のリスクプロファイルに一致する柔軟な鍵管理の信頼の基点（Root of Trust）を実現します。vSphereをタレスのCipherTrust Managerと組み合わせて使用することで、鍵管理と役割分離に対する幅広い保護機能が提供されます。この組み合わせによるソリューションは、非破壊的な暗号化を提供し、VM、VMで実行されるアプリケーション、さらにVMで処理される機密データのセキュリティを確保します。この組み合わせは、最も厳しいセキュリティ要件を満たす、費用対効果の高い包括的なソリューションを提供します。ハードウェアベースのデータ暗号化を利用するため、システムのパフォーマンスにも悪影響はありません。




一般的なユースケースには、データセンターの統合、アプリケーションのパフォーマンスと可用性の強化、インテリジェントな運用管理と優先順位付けが含まれます。VMware vSphere VM暗号化とThalesCipherTrust Managerの組み合わせを使用すると、容易にコンプライアンスも実現できます。

## Thales CipherTrust Managerを使用するメリット?

セキュリティキーは、サイト固有のセキュリティポリシーを満たすように即座に再プログラムできます。セキュリティメカニズムにより、HIPAA、PCI DSS、SOX標準などに定められた保存データ暗号化要件への準拠が可能になります。CipherTrust Managerは以下を提供します。

- 暗号鍵の一元的な鍵管理
- コンプライアンスと監査性を向上させつつ、VMware vSpher VMインフラストラクチャ全体の鍵管理を一元化および簡素化
- マルチテナントデータ分離を実現して共有リソースを活用すると同時に、複数の部門、ビジネスユニット、または顧客のデータを分離するビジネスポリシーによってデータを保護
- クラウド規模の展開をサポートする高可用性を実現
- 複数のThales CipherTrust Managerアプライアンスをクラスタ化して、地理的に分散したデータセンターでも暗号化されたデータの可用性を維持
- 監査、ロギング、アラートが可能
- 否認防止の監査証跡を使用して、Vmware環境全体の規制コンプライアンスを向上

CipherTrust Managerは、タレスのデータセキュリティ製品とサードパーティの暗号化ソリューションの暗号鍵管理を一元化する高可用性アプライアンスです。鍵の生成、ローテーション、破棄、インポート、エクスポートなどの鍵ライフサイクルタスクを管理します。

CipherTrust Managerは、便利なバックアップサービスを提供し、セキュリティを高める強力な職務分掌を可能にすることで、鍵管理をさらに強化します。CipherTrust Managerは、鍵管理環境専用の論理エンティティまたはドメインに分離でき、追加のセキュリティと究極的な職務分掌を提供するため、1人の管理者がすべてのドメインにアクセスするようなことはできなくなります。

CipherTrust Managerは、ハードウェアまたは仮想アプライアンスのいずれかで利用可能です。k470 CMハードウェアアプライアンスは、FIPS 140-2 Level 2に準拠しています。k570 CMハードウェアアプライアンスにはハードウェアセキュリティモジュール(HSM)が搭載されており、FIPS 140-2 Level 3に準拠しています。仮想アプライアンスのK170Vは、FIPS 140-2 Level 1に準拠しています。

エンタープライズ暗号鍵管理の統合により、システム間で一貫したポリシーを実装でき、トレーニングとメンテナンスのコストを削減できます。

## 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。

## VMware

VMwareは、クラウドインフラストラクチャとビジネスモビリティのグローバルリーダーであり、お客様のデジタルトランスフォーメーションを加速させます。VMwareは、VMware Cross-Cloud Architecture™や、データセンター、モビリティ、セキュリティのソリューションを提供して、企業がビジネスとITに対してソフトウェア定義(Software Defined)のアプローチを活用できるように支援しています。

詳細な技術仕様については、cpl.thalesgroup.comまたはwww.vmware.comをご覧ください。



> cpl.thalesgroup.com <

**お問い合わせ先 –** jpsales.cpl@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。