

NetAppとタレスが費用対効果の高い一元的な鍵管理ソリューションを提供



課題

機密データの保護

機密データを保護する必要性は、かつてないほど高まっています。組織は、データ侵害の持続的な脅威に対処しながら、仮想データセンターとクラウド環境への移行を続けています。規制要件 (PCI/DSS、HIPAA/HITECH、GDPR、GLBA、SOX) は増え続けています。不正使用を防ぐために、多くの組織が現在、暗号化を利用してデータを保護しています。一元的な場所から複数の暗号鍵を作成、管理、保護することは、プロセスの不可欠かつ重要な部分です。強力な暗号化は極めて重要ですが、適切な監査制御を行って鍵を適切に保護することはさらに重要です。

タレスとNetAppは連携して、物理環境と仮想環境の両方の一元的な鍵管理、鍵保管、監査制御を備えたエンタープライズ鍵管理ソリューションを提供します。お客様は、FIPSレベル認定とパフォーマンス要件に応じて、物理アプライアンスか、すでに所有しているサーバー上で仮想マシン (VM) として実行される強固なソフトウェア (仮想アプライアンス) のいずれかを選択できます。

ソリューション

柔軟で安全な鍵管理

NetAppはタレスとの提携により、暗号化の柔軟性をもたらし、効率性を高め、保管されている情報の盗難や不正アクセスのリスクを軽減する包括的なストレージセキュリティを提供します。clustered Data ONTAP®オペレーティングシステムとThales CipherTrust Managerエンタープライズ鍵管理 (EKM) を組み合わせた独自の機能を提供するネットワークストレージ環境により、ユーザーおよび重要なワークロードに対して、暗号化されたデータを常に利用可能な状態に保つことができます。

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。

Thales 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。Thales 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。

統合ソリューションの主なメリット

- 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、NetApp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
- 否認防止の監査証拠を使用して、NetApp環境全体の規制コンプライアンスを向上

実績のある鍵管理

タレスは、重要度の高い情報資産の保護に特化した最大の企業であり、セキュリティチームが多層防御戦略を一元的に採用できるようにする幅広いソリューションを提供します。

- エンタープライズ鍵管理のリーダー
- クラウド規模の展開をサポートする高可用性
- 実績のあるパフォーマンスプロファイル
- 複数の鍵タイプの一元管理: 対称、非対称、秘密データ、およびX.509証明書

Thales CipherTrust Managerは、物理アプライアンスまたは仮想アプライアンスの柔軟性を提供して、お客様のビジネスニーズに対応します。タレスは、パブリッククラウドで利用できるハードウェアの信頼の基点(Root of Trust)と統合された仮想鍵管理アプライアンスを提供する、唯一のソリューションプロバイダーです。

NetAppストレージ環境におけるThales CipherTrust Managerのメリット

- 最高レベルのセキュリティ。Thales CipherTrust Managerでは、鍵の署名、ロールベースの管理、クォーラムコントロール、暗号鍵のバックアップと配布など、すべての鍵管理アクティビティが一元化されます。複数の管理者からの複数の資格情報の承認を規定できます。機密データに対するセキュリティ操作については、複数の管理者による複数の資格情報承認を条件として要求することができます。
- 復元性と高可用性。複数のCipherTrust Managerアプライアンスをクラスタ化して、構成情報の複製により高可用性を実現できます。

標準への適合性

Thales CipherTrust ManagerはKMIPをサポートしているため、主要なセキュリティポリシーを統合し、異種の暗号化システム、自己暗号化ドライブ、テープアーカイブ、ストレージエリアネットワーク、仮想ワークロードなどに対する投資を保護できます。

- **HSM統合によるセキュアな展開:** Thales CipherTrust Manager仮想アプライアンスは、お客様の環境で作成されたすべての鍵の信頼の基点(Root of Trust)であるHSMにあるマスター鍵を参照できます。CipherTrust Manager仮想アプライアンスは、サブスクリプションベースのAWS環境ではAmazon Web Services CloudHSMを、オンプレミス展開ではThales Luna SAをサポートします。
- **物理および仮想ストレージ環境の保護:** NetApp、IBM、Hitachi Data Systems、Dell EMC、Quantum、HPE、Nutanix、VMware vSANなど、多くの一般的なNAS、テープ、バックアップストレージデバイスをサポートします。
- **複数のプライベート/パブリッククラウドのサポート:** Thales CipherTrust Manager仮想アプライアンスは、AWS、VMware (VMwareをサポートするパブリッククラウドを含む)、OpenStack、Microsoft Azure、Microsoft Hyper-V、Googleなど、複数のプライベートおよびパブリッククラウド環境をサポートできます。

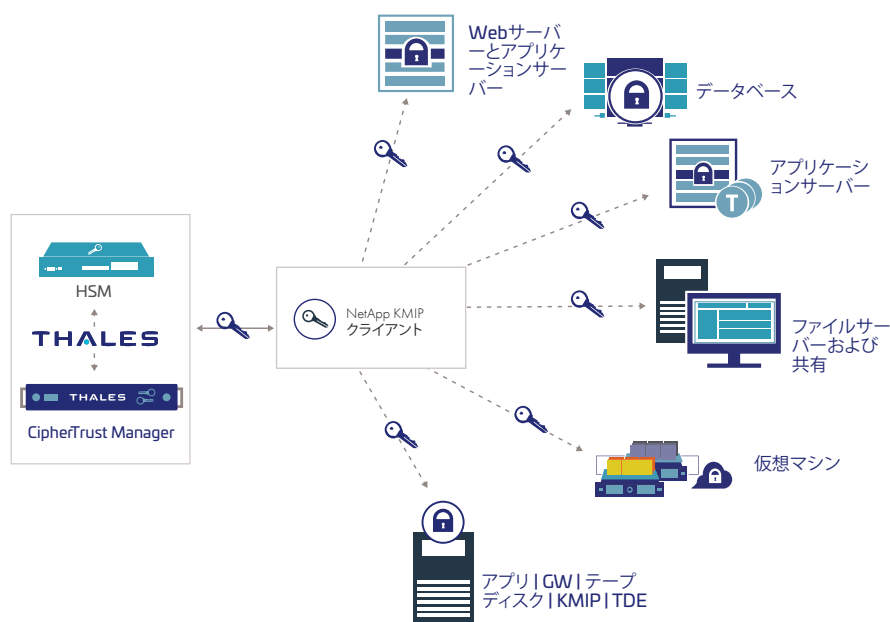


図1: 保管データ、アーカイブデータ、仮想ワークロードにわたるアプリケーションデータ保護と一元的な鍵管理。

主なメリット

鍵のライフサイクル全体のサポート

- 自動化されたポリシー駆動型の操作により、安全な鍵生成、保管とバックアップ、鍵の配布、非アクティブ化、削除などのライフサイクル全体にわたる鍵管理を簡素化します。

一元化された鍵管理

- 一元管理では、複数の暗号化展開にわたり、アクセス、許可制御、職務分掌をきめ細かく定義できます。

インテリジェントな鍵共有

- 地理的に分散したセンターやサービスプロバイダー環境でも、柔軟かつ可用性の高い構成で導入できます。

監査証跡

- 一元管理には、すべての鍵の状態変化、管理者アクセス、およびポリシー変更の詳細なロギングと監査証跡が含まれます。

NetApp ONTAP用のThales CipherTrust Manager

Thales CipherTrust Managerは、効率的で一元的な鍵管理と、データアクセスに関するカスタマイズされたセキュリティポリシーの適用により、NetApp Cloud ONTAP上のデータの機密性を維持します。この最新のストレージインフラストラクチャとタレスの鍵管理の組み合わせは、データとその暗号鍵が不正アクセスから保護されるという安心感をもたらすと同時に、ストレージへの投資の最も効率的な使用を可能にします。Thales CipherTrust Managerを使用すると、管理者は、ONTAP 9.3以降のNetApp Storage Encryption (NSE)、NetApp Volume Encryption (NVE)、さらにタレスに関連する鍵を同時に管理できます。

CipherTrust Managerの購入オプション

	CipherTrust Manager		
	オプションI:	オプションII:	オプションIII:
購入オプション	仮想アプライアンス(お客様提供のサーバー上で仮想マシンとして実行)	ハードウェアセキュリティモジュール(HSM)なしの専用アプライアンス	ハードウェアセキュリティモジュール(HSM)搭載の専用アプライアンス
鍵保管のタイプ	強固なソフトウェア	ハードウェアベース	ハードウェアベース
外部HSMによるハードウェアベースの鍵保管庫を追加するオプション	あり	あり	該当せず(HSM搭載済み)
FIPS 140-2認定レベル	Level 1 - 暗号化アルゴリズムは承認基準を達成 - 外部HSMでLevel 2および3に対応可能	Level 1および2 - ハードウェア上に改ざん検出の証拠を追加(アプライアンス上の不正開封防止シールなど) - 外部HSMでLevel 3に対応可能	Level 1、2、3 - 改ざん検出と応答回路を追加 - PCI-DSSなどのより厳しいコンプライアンス基準を達成
タレス製品提供(例)	CipherTrust Manager - K170V	CipherTrust Manager - K470	CipherTrust Manager - K570

広範なエコシステムのサポート

Thales CipherTrust Managerは、暗号鍵の一元管理とセキュリティのための業界をリードするアプライアンスです。タレス製品とサードパーティ製品を網羅するThales CipherTrust Managerは、ストレージ内の機密データ、仮想ワークロード、従来型と仮想化されたデータセンターおよびパブリッククラウド環境にわたるアプリケーションを保護するための幅広い暗号化エコシステムをサポートします。

NetAppについて

NetAppは、ハイブリッドクラウドにおけるデータ管理のエキスパートです。クラウド環境からオンプレミス環境にわたるアプリケーションとデータの管理を簡素化し、デジタルトランスフォーメーションを加速する包括的なハイブリッドクラウドデータサービスを提供しています。NetAppは、グローバル企業がデータのポテンシャルを最大限に引き出し、顧客との接点増加、イノベーションの促進、業務の最適化を図れるよう、パートナー企業とともに取り組んでいます。詳細については、www.netapp.comをご覧ください。#DataDriven

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。