cpl.thalesgroup.com

THALES

CipherTrust Manager
（サイファートラスト マネージャー）

概要

CipherTrust Manager を使用すると、タレス製品とサードパーティ製品の暗号鍵を一元的に管理できます。これにより、セキュアな鍵の生成、バックアップ／リストア、クラスタリング、非アクティブ化、消去などの鍵ライフサイクル管理タスクを簡素化できます。

CipherTrust Manager は、鍵とポリシーに対するロールベースのアクセス制御、マルチテナンシーサポート、すべての鍵管理と暗号化操作の強力な監査とレポートを提供します。

CipherTrust Manager の一元管理コンソールでは、タレスの包括的な一連のデータ保護コネクタを使用して、データを容易に検出および分類でき、機密データをその所在にかかわらず保護できます。

CipherTrust Manager は、仮想および物理フォームファクタの両方で提供されておりFIPS 140-2検証済みのタレスLunaまたは他社のハードウェアセキュリティモジュール（HSM）を使用して、セキュリティの高い信頼の基点（Root of Trust）でマスター鍵を安全に格納できます。これらのアプライアンスは、オンプレミスだけでなく、プライベートまたはパブリッククラウドインフラストラクチャにも導入できます。これにより、データセキュリティのコンプライアンス要件、規制要件、業界のベストプラクティスのすべてに対応できます。

メリット

- 複数のオンプレミスデータストアとクラウドインフラストラクチャの鍵管理を一元化
- データの検出と分類、機密データの保護により、ビジネスリスクを軽減
- セルフサービスのライセンスポータルと使用中ライセンスの可視化により、管理を簡素化
- AWS、Azure、Google Cloud、VMwareなどをサポートするクラウドフレンドリーな導入オプション
- 拡張ハードウェアセキュリティモジュール（HSM）のサポートにより、優れた鍵管理を実現
- 主要なエンタープライズストレージ、サーバー、データベース、アプリケーション、SaaSベンダーとの統合による比類のないパートナーエコシステム

基本機能

- **鍵のライフサイクル全体の管理と自動操作:** CipherTrust Manager は、セキュアな鍵の生成、バックアップ／リストア、クラスタリング、非アクティブ化、消去などのライフサイクル全体にわたり、暗号鍵の管理を簡素化します。自動化されたポリシー駆動型の操作を容易に実行できるようにし、対象イベントのアラームを生成します。
- **一元化された管理とアクセス制御:** ロールベースのアクセス制御によって鍵管理操作を一元化し、完全な監査ログのレビューを提供します。既存のADおよびLDAP資格情報を使用して、管理者と鍵ユーザーを認証および承認します。
- **データの検出と分類:** 包括的な一連のデータ保護コネクタと統合された、機密データの検出と分類を行う一元コンソールを提供し、データを暗号化またはトークン化して、ビジネスリスクを軽減し、コンプライアンス規制を満たします。
- **セルフサービスライセンス:** 新規のお客様向けのライセンスポータルを通じて、コネクタライセンスのプロビジョニングを合理化します。新しい管理コンソールにより、使用中のライセンスの可視性と管理性が向上します。
- **秘密管理:** プラットフォームで使用する秘密および不透明オブジェクトの作成と管理を行うための機能を提供します。
- **マルチテナンシーサポート:** マネージドサービスプロバイダー（MSP）によってホストされている多数の拠点や複数企業を有する大規模組織をサポートするために、職務を分離した複数ドメインの作成に必要な機能を提供します。
- **開発者フレンドリーなREST API:** KMIPおよびNAE-XML APIに加えて、新しいRESTインターフェイスを提供します。これにより、リモートで鍵を生成および管理でき、暗号操作をクライアントからCipherTrust Manager アプライアンスにオフロードできます。
- **柔軟なHAクラスタリングとインテリジェントな鍵共有:** 物理アプライアンスや仮想アプライアンスをクラスタ化して、高可用性を確保し、暗号化トランザクションの処理能力を向上させるオプションを提供します。
- **強力な監査とレポート:** すべての鍵の状態変化、管理者アクセス、ポリシー変更を追跡して複数のログ形式（RFC-5424、CEF、LEEF）で記録し、SIEMツールと統合しやすくします。また、事前構成済みの／カスタマイズ可能な電子メールアラートを生成できます。監査証跡は安全に保管され、否認防止のために署名されます。
- **NICボンディングによる高速インターフェイス:** 新しいk470およびk570アプライアンスは、オプションの2x1GB/2x10GBネットワークインターフェイスカード（NIC）とNICボンディングを提供し、利用可能な帯域幅を増やします。
- **多様な暗号化のユースケース:** CipherTrust Manager は、タレスのデータ保護コネクタとパートナーエコシステムを通じて、包括的な暗号化のユースケースをサポートしています。

さらなる情報

その他のタレス鍵管理ソリューション

アプライアンスの仕様

CipherTrust Manager の物理アプライアンス

機能	k470	k570
最大鍵数	1,000,000	1,000,000
最大同時セッション	1000	1000
FIPS 140-2認定	タレス LunaNetwork及びCloudHSM、その他のサードパーティHSMと連携	内蔵のLuna HSMでLevel 3認定
ネットワークインターフェイスカード（NIC）オプション	• 4x1GB • 2x1GB / 2x10GB • NICボンディングのサポートを含む	
APIのサポート	• REST • JCE • NAE-XML • NET • KMIP • MSCAPI • PKCS11 • MS CNG	

CipherTrust Manager の仮想アプライアンス

機能	k170v	k470v
最大鍵数	25,000	1,000,000
最大同時セッション	100	1000
システム要件	• HD: 100GB • RAM: 4-8 GBB • NICs: 1 -2 • CPUs: 2 or more	• HD: 200GB以上 • RAM: 16 GB以上 • NIC:2個以上 • CPU:4個以上
FIPS 140-2認定	タレス LunaNetwork及びCloudHSM、その他のサードパーティHSMと連携	
APIのサポート	• REST • NAE-XML • KMIP • PKCS#11 • JCE, • NET, • MSCAP, • MS CNG • NAE-XML	

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。