Product Brief

CipherTrust Manager

cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

THALES
Building a future we can all trust

CipherTrust Managerは、タレスのCipherTrust Data Security Platformとサードパーティ製品の暗号鍵を一元管理可能にすることで、安全な鍵の生成、バックアップ/リストア、クラスタリング、非アクティブ化、削除などの鍵ライフサイクル管理タスクを簡素化します。

鍵とポリシーに対するロールベースのアクセス制御、マルチテナントサポート、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 Data Security Platform (CDSP)の中央管理ポイントとして、CipherTrust Managerは統合管理コンソールを提供することで、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。CDSPは、Secrets ManagementやRansomware Protectionといった、タレスの包括的な一連のCipherTrustデータ保護コネクタや、カスタムソリューション用のREST、KMIP、NAE XML APIを利用できるようにします。

展開オプション

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 NetworkまたはCloud HSM（ハードウェアセキュリティモジュール）と統合し、最高レベルの信頼の基点でマスター鍵を安全に保管します。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展開できます。これにより、データセキュリティに関する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に対応できます。

メリット

- オンプレミスのデータストアとクラウドインフラストラクチャの鍵とポリシー管理を一元化
- 統合されたデータ検出と分類、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
- パブリック、プライベート、ハイブリッドクラウドをサポートするクラウドフレンドリーな展開オプション。パブリック: AWS、Azure、Google Cloud、Oracle Cloud、Alibaba Cloud。プライベートイメージファイル: VMware vSphere OVA、Microsoft Hyper-V VHDX、Nutanix AHV VMDK、OpenStack QCOW2。ハイブリッドクラウドイメージファイル: Azure Stack HCI、Azure Stack Hub

- 拡張HSM（ハードウェアセキュリティモジュール）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

主な機能

- **鍵のライフサイクル全体の管理と自動操作:** CipherTrust Managerは、安全な鍵の生成、バックアップ/リストア、クラスタリング、非アクティブ化、削除などのライフサイクル全体にわたって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。
- **クォーラム認証:** 管理者は機密性の高い操作に対して複数の承認者を要求できます。
- **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る鍵管理操作を一元化します。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。不正なパスワード変更を防止し、同一ユーザーの同時ログインに警告を発します。
- **セルフサービスライセンス:** 新たなユーザー向け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や不透明オブジェクトの作成と管理を行う機能を提供します。
- **マルチテナントサポート:** 複数ドメイン内でのユーザー管理の委任による職務分掌をサポートします。
- **開発者フレンドリーなREST API:** KMIP (Key Management Interoperability Protocol) やNAE-XML APIに加えて、新しい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るようになります。
- **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。
- **広範なパートナーエコシステム:** CipherTrust Managerは、KMIPを介してさまざまなストレージパートナーに、Transparent Database Encryption（TDE）を介してデータベースパートナーに、一元的な鍵管理を提供します。

CipherTrust Managerの機能

機能	仮想アプライアンス		物理アプライアンス	
	k170v	**k470v**	**k470**	**k570**
管理インターフェイス	管理コンソール、REST API、kscfg（システム構成）、ksctl（コマンドラインインターフェイス）			
ネットワーク管理	SNMP v1、v2c、v3、NTP、Syslog-TCP			
監視	Prometheus、Splunk			
APIのサポート	REST、NAE-XML、KMIP、PKCS#11、JCE、.NET、MCCAPI、MS CNG			
セキュアな認証	Local User、AD/LDAP、LDAPS、証明書ベースの認証、Open ID Connect（OIDC）のサポート			
システムフォーマット	RFC-5424、CEF、LEEF			
信頼の基点対応HSM	Luna Network HSM、Luna T-Series Network HSM、Luna Cloud HSM、AWS Cloud HSM、Azure Dedicated HSM、IBM Cloud HSM、IBM Cloud Hyper Protect Crypto Services Cloud HSM、nShield Network HSM	Luna Network HSM、Luna T-Series Network HSM、Luna Cloud HSM、AWS Cloud HSM、Azure Dedicated HSM、IBM Cloud HSM、IBM Cloud Hyper Protect Crypto Services Cloud HSM、nShield Network HSM	Luna Network HSM、Luna T-Series Network HSM、Luna Cloud HSM、AWS Cloud HSM、Azure Dedicated HSM、IBM Cloud HSM、IBM Cloud Hyper Protect Crypto Services Cloud HSM、nShield Network HSM	**組み込み型HSM**、Luna Network HSM、Luna T-Series Network HSM、Luna Cloud HSM、AWS Cloud HSM、Azure Dedicated HSM、IBM Cloud HSM、IBM Cloud Hyper Protect Crypto Services Cloud HSM、nShield Network HSM
自動展開サポート	あり（Terraform、Cloud-Init経由）	あり（Terraform、Cloud-Init経由）	なし	あり（Secure Transport Mode経由）
最大鍵数	最大100万個の鍵までテスト済み（適切なサイズの仮想環境ではさらに可能）	最大100万個の鍵までテスト済み（適切なサイズの仮想環境ではさらに可能）	100万個	100万個
最大ドメイン数（マルチテナント）	100	1000	1000	1000
FIPSのサポート	FIPS 140-2 L1 (Certificate #4430)			
	セキュアな信頼の基点として外部のFIPS認定の物理HSMまたはCloud HSMと統合			組み込み型PCI-HSM FIPS 140-2 Level 3認定– パスワードと多要素（PED）（Certificate #4090）

アプライアンスの仕様

物理アプライアンス	k470	k570
寸法	19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)	
ハードドライブ	2TBのSATA SE(スピニングディスク)x 1個	
CPU	Xeon E3-1275v6プロセッサ	
RAM	16GB	
NICのサポート	1GB x 4個または10Gb x 2個/1Gb x 2個(NICボンディング可能)	
ラックマウント	標準1Uラックマウント可能なスライドレールをオプションで購入可能	
信頼性	ホットスワップ可能な二重化電源	
安全性とコンプライアンス	CSA C-US, FCC, CE, VCCI, C-TICK, KC Mark, BIS	
平均故障間隔	165,279時間	153,583時間

仮想アプライアンス	k170v	K470v
システム要件	• RAM(GB): 16 • ハードディスク(GB): 100 • NIC: 1個以上 • CPU: 最大4個	• RAM(GB): 16以上 • ハードディスク(GB): 200以上 • NIC: 2個以上 • CPU:5個以上
サポートされているクラウド/ハイパーバイザー	• パブリッククラウド: AWS Cloud、Microsoft Azure、Google Cloud Enterprise(GCE)、Oracle Cloud Infrastructure(OCI)、Alibaba Cloud • プライベートクラウド/ハイパーバイザー: VMware vSphere(6.5、6.7、7.0)、Microsoft Hyper-V、Nutanix AHV, OpenStack(QCOW2) * AWS GovCloud、Azure Government Cloudもサポート • ハイブリッドクラウド/ハイパーバイザー: Azure Stack HCI、Azure Stack Hub	

cpl.thalesgroup.com

お問い合わせ先 – Email: 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。