Product Brief

THALES
CYBERSECURITY

暗号鍵とポリシーを一元管理する
集中管理プラットフォーム

CipherTrust Manager

cpl.thalesgroup.com

THALES

CYBERSECURITY

CipherTrust Managerは、タレスデータセキュリティプラットフォーム「CipherTrust Data Security Platform」およびサードパーティ製品の暗号鍵を一元管理することで、鍵の生成からバックアップ／リストア、クラスタリング、無効化、削除まで、鍵ライフサイクル全体の管理を簡素化します。

鍵およびポリシーに対するロールベースのアクセス制御、マルチテナント対応、ならびにすべての鍵管理および暗号化操作に関する包括的な監査・レポート機能を提供します。

CipherTrust Data Security Platform（CDSP）の中核となる管理コンポーネントとして、CipherTrust Managerは統合管理コンソールを提供し、データの検出と分類を容易にするとともに、保存場所を問わず機密データを保護します。CDSPは、Secrets ManagementやRansomware Protectionを含むタレスの包括的なCipherTrust Data Protection Connectorsに加え、カスタムソリューション向けのREST API、KMIP、NAE XML APIを提供します。

主な機能

- **鍵ライフサイクル全体の管理と自動化された運用：**CipherTrust Managerは、安全な鍵生成、バックアップ／リストア、クラスタリング、無効化、削除など、暗号鍵のライフサイクル全体にわたる管理を簡素化します。また、ポリシーに基づく自動運用を容易に実現し、重要なイベントが発生した際にはアラートを生成します。
- **クォーラム認証：**機密性の高い操作に対して、複数の承認者による承認を必須とするよう設定できます。
- **一元化された鍵管理及びアクセス管理：**ロールベースのアクセス制御により、鍵管理を一元化します。既存のADおよびLDAPの認証情報を活用して管理者および鍵利用者の認証・認可を行い、不正なパスワード変更を防止します。また、同一ユーザーによる同時ログインを検知した場合はアラートを通知します。
- **セルフサービス型ライセンス管理：**新しいお客様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割り当てと管理を効率化します。さらに、新しい管理コンソールにより、利用中のライセンス状況をより容易に把握し、きめ細かな管理を実現します。
- **Secrets Management（シークレット管理）：**プラットフォーム上で利用するシークレット（機密情報）およびオペークオブジェクトの作成と管理を行う機能を提供します。
- **マルチテナント対応：**複数のドメインにわたる委任型のユーザー管理をサポートし、適切な職務分掌を実現します。
- **開発者向けの使いやすいRest API：**KMIP（Key Management Interoperability Protocol）およびNAE-XML APIに加え、新たなRESTインターフェースを提供します。これにより、お客様はリモートから鍵の生成および管理を行うことができます。
- **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柔軟にクラスタ化し、高可用性を確保するとともに、暗号化トランザクションのスループットを向上させます。
- **包括的な監査・レポート機能：**すべての鍵の状態変更、管理者によるアクセス、およびポリシー変更を追跡し、RFC 5424、CEF、LEEFなどの複数のログ形式で記録します。これにより、SIEMツールとの容易な統合を実現します。
- **幅広いパートナーエコシステム：**CipherTrust Managerは、KMIPを介して幅広いストレージパートナー製品に対する一元的な鍵管理を提供するとともに、**Transparent Database Encryption（TDE）**を介してデータベースパートナー製品に対する一元的な鍵管理を提供します。

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オンプレミスのデータストアおよびクラウドインフラストラクチャにおける鍵とポリシーを一元管理
- 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利用中ライセンスの可視化により、管理を簡素化
- パブリッククラウド、プライベートクラウド、ハイブリッドクラウドに対応した柔軟な導入オプション。パブリッククラウド：AWS、Microsoft Azure、Google Cloud、Oracle Cloud、Alibaba Cloud。プライベートクラウド向けイメージ：VMware vSphere OVA、Microsoft Hyper-V VHDX、Nutanix AHV VMDK、OpenStack QCOW2。ハイブリッドクラウド向けイメージ：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ベンダーとの幅広い統合を実現する充実したパートナーエコシステム

THALES

CipherTrust Manager

導入オプション

CipherTrust　Managerは、仮想アプライアンスと物理アプライアンスの両方で提供されており、 FIPS　140-2　認証済みのタレス Luna Network HSMまたはLuna Cloud HSM（ハードウェアセキュリティモジュール）と連携して、マスター鍵を最高レベルのRoot of Trustで安全に保管します。これらのアプライアンスは、オンプレミス環境に加え、プライベートクラウドおよびパブリッククラウド環境にも導入できます。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、各種規制、および業界のベストプラクティスへの対応を支援します。

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、 認証書ベースの認証、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、Google Cloud 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、Google Cloud 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、Google Cloud 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、Google Cloud 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 およびFIPS 140-3 Level 3認定

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 1.75” (482.6mm x 533.4mm x 44.45mm)	
ハードドライブ	2TBのSATA SE（スピニングディスク）x1個	
CPU	4コア、8スレッド、プロセッサーの基本周波数：3.8 GHz	
RAM	16 GB*	
NICのサポート	1GBx4個または10Gbx2個/1Gbx2個（NICボンディング）	
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 Azur 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	

安全規格認証	適用国・地域
CBスキーム	50か国
CSA-UL	カナダ・米国
エミッション規格認証	
FCCパート15、サブパートB、クラスB	米国
EN55032:2010, EN55035:2017, EN61000-3-2:2006 +A1:2009 +A2:2009EN61000-3-3:2008	欧州
ICES-003 Issue 7 （2020年10月発行）	カナダ
AS/NZ CISPR 32:2015	オーストラリア・ニュージーランド
VCCI V-3/2009.04	日本
KN22・ KN24・ KCマーク	韓国
NOM	メキシコ
BIS	インド

* 16 GB以上

cpl.thalesgroup.com

お問い合わせ先 – 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。