cpl.thalesgroup.com/ja

THALES
Building a future we can all trust

タレスLuna PCIe HSM

タレス Luna PCIe HSMで暗号鍵を保管、保護、管理することで、機密データや重要なアプリケーションを保護できます。Luna PCIe HSMは、高保証の、耐タンパ性を備えたPCIeカードであり、特別に設計された高性能な暗号プロセッサへの専用アクセスをアプリケーションに提供します。この費用対効果の高いソリューションをサーバーやセキュリティアプライアンスに直接組み込むだけで、FIPS 140-2認証取得済みの保証が得られます。

Luna PCIe HSMは、暗号鍵のライフサイクル全体を通じて完全性と保護を保証します。詳細について、ぜひ当社にお問い合わせください。

主な機能と利点

優れたパフォーマンスと操作性

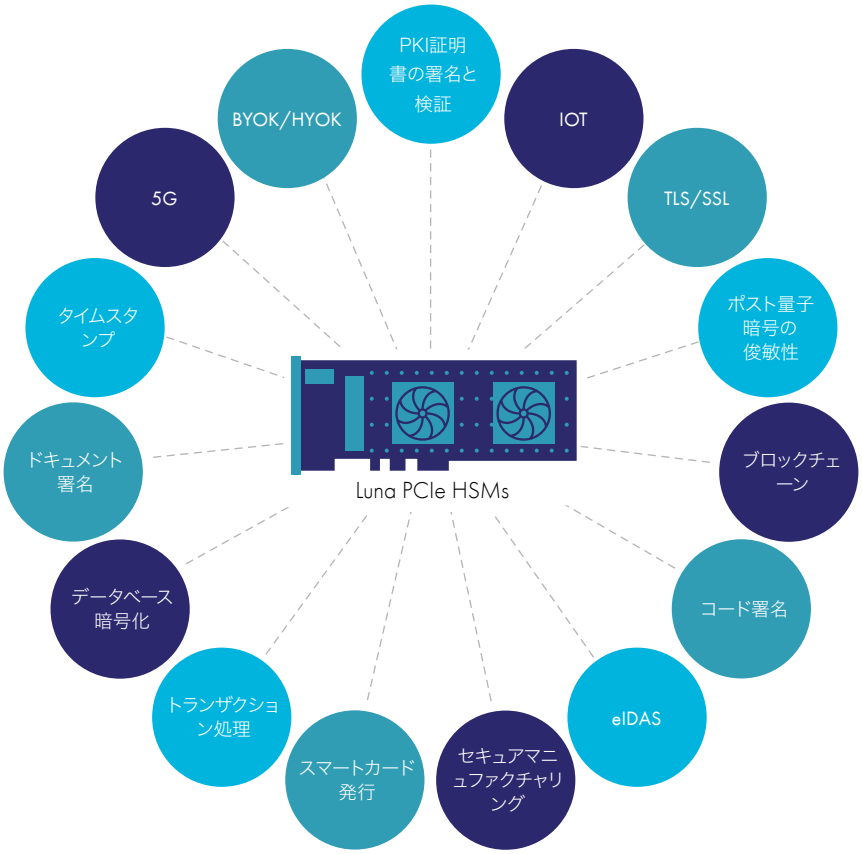
- 毎秒20,000以上の楕円曲線暗号と10,000以上のRSA暗号の処理能力を備えた市場最速のHSMであり、高性能ユースケースに対応
- レイテンシを短縮して効率を向上
- アプリケーション専用アクセス
- ロープロファイルPCIeカード

機能モジュール

- ネイティブHSMの機能を拡張
- HSMの安全な範囲内でカスタムコードの開発と展開が可能

最高レベルのセキュリティとコンプライアンス

- 鍵は常にFIPS認証取得済みの耐タンパ性のハードウェアに保管
- GDPR、eIDAS、HIPAA、PCI-DSSなどのコンプライアンス要件に対応
- 複数の役割を設けることで、強力な職務分掌を実現
- セキュリティを強化する多要素認証を備えたマルチユーザーMofN
- セキュアな監査ロギング
- セキュアな転送モードによる高保証の配信



技術仕様

OSサポート

- Windows, Linux

APIサポート

- PKCS#11、Java（JCA/JCE）、Microsoft　CAPIおよびCNG、OpenSSL

暗号化

- Suite Bの完全サポート
- 非対称:　RSA、DSA、Diffie-Hellman、名前付き曲線、ユーザー定義曲線、Brainpool曲線による楕円曲線暗号（ECDSA、ECDH、Ed25519、ECIES）、KCDSAなど
- 対称:　AES、AES-GCM、Triple　DES、DES、ARIA、SEED、RCS、RC4、RC5、CASTなど
- ハッシュ/メッセージダイジェスト/HMAC: SHA-1、SHA-2、SHA-3、SM2、SM3、SM4など
- 鍵導出: SP800-108カウンターモード
- 鍵ラッピング: SP800-38F
- 乱数生成: NIST 800-90A準拠のCTR-DRBGとともにHWベースの真のノイズ源を使用して、AIS 20/31からDRG.4に準拠するように設計
- デジタルウォレット暗号化: BIP32

セキュリティ認定

- FIPS 140-2 Level 3—パスワードと多要素（PED）
- eIDAS Protection Profile EN 419 221-5に対するコモンクライテリアEAL4+（AVA_VAN.5およびALC_FLR.2）
- eIDAS規則準拠の適格電子署名生成装置（QSCD）のリストに掲載
- シンガポールNITESコモンクライテリアスキーム*

物理的特徴

- ロープロファイルPCIeカード
- 寸法: 69.6mm x 167mm x 18.7mm（2.74” x 6.57” x 0.74”）
- 消費電力: 最大18W、標準14W
- 熱放散: 最大61.4 BTU/時、標準47.8 BTU/時
- 温度: 動作時 0°C～50°C、保管時 -20°C～60°C
- 相対湿度: 5%～95%（38°C）非結露

安全・環境コンプライアンス

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC MARK
- RoHS2, WEEE
- TAA

ホストインターフェース

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

信頼性

- バックアップ/リストア
- 高可用性（HA）
- 平均故障間隔（MTBF）997,508時間

*進行中

利用可能なモデル

Luna Network HSMには2つのシリーズがあり、各シリーズに用意された3種類のモデルからお客様のニーズに合わせてお選びいただけます。

Luna Aシリーズ:

管理を容易にするためのパスワード認証

標準パフォーマンス **A700**	エンタープライズパフォーマンス **A750**	最大パフォーマンス **A790**
2 MBメモリ	16 MBメモリ	32 MBメモリ
パフォーマンス: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**パフォーマンス:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**パフォーマンス:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna Sシリーズ:

高保証ユースケース向けの多要素(PED)認証

Standard Performance **S700**	Enterprise Performance **S750**	Maximum Performance **S790**
2 MBメモリ	16 MBメモリ	32 MBメモリ
パフォーマンス: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**パフォーマンス:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**パフォーマンス:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = transactions per second

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/ja <

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。