

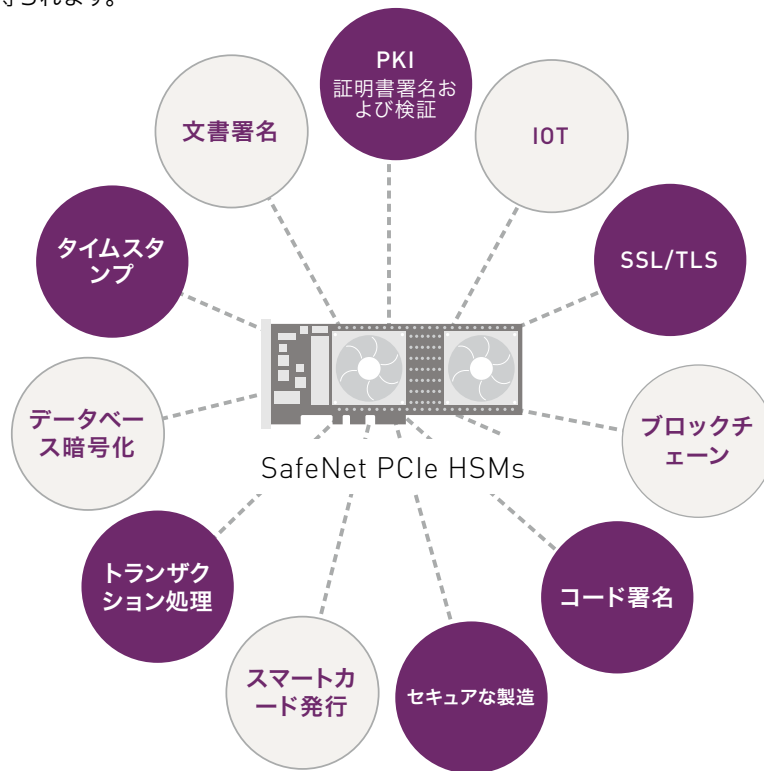


プロダクト プリーフ

# SafeNet Luna PCIe HSM

SafeNet Luna PCIe HSM (ハードウェアセキュリティモジュール) は、信頼性の高い耐タンパー性のPCIeカードです。HSMで暗号鍵を保護および管理することにより、機密データおよび重要なアプリケーションを守ることができます。アプリケーションは専用に作られた高性能な暗号プロセッサのみにアクセスします。このコスト効率の良いソリューションをサーバとセキュリティアプライアンスに簡単に直接差し込むだけで、FIPS 140-2検証済みの保証が得られます。

SafeNet Luna PCIe HSMは、暗号鍵のライフサイクル全体を通じてその完全性と保護を保証するのに役立ちます。方法については、ジェムアルトまでお問い合わせください。



**特長:**

**優れた性能とユーザビリティ:**

- > 市場で最も高速なHSM (毎秒20,000以上のECC処理と10,000以上のRSA処理が可能) により高性能が必要なユースケースに対応
- > 低レイテンシにより効率性を向上
- > アプリケーションに専用アクセスを提供
- > ロープロファイルPCIeカード

**最高レベルのセキュリティとコンプライアンス:**

- > FIPS検証済みの耐タンパー性のハードウェアに鍵を保管
- > GDPR、HIPAA、PCI-DSS、eIDASなどのコンプライアンスニーズに対応
- > 複数ロールによる強力な職務分掌
- > MofN多要素認証によるセキュリティ向上の実現
- > セキュアな監査ログ

## 技術仕様

### サポート対象のオペレーティングシステム

- > Windows, Linux

### APIサポート

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

### 暗号化

- > フルスイートBサポート
- > 非対称: RSA, DSA, Diffie-Hellman, 名前指定、ユーザー定義、およびBrainpool曲線による楕円曲線暗号化 (ECDSA, ECDH, Ed25519, ECIES)、KCDSA
- > 対称: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RCS, RC4, RC5, CAST
- > ハッシュ/メッセージ Digest/HMAC: SHA-1, SHA-2, SM3
- > 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: FIPS 140-2承認のDRBG (SP 800-90 CTRモード)、BSI DRG.4に準拠

### セキュリティ認定

- > FIPS 140-2レベル3—パスワードとマルチファクタ (PED) \*
- > FIPS 186-4

### 物理的特性

- > ロープロファイルPCIeカード
- > 寸法: 69.6mm x 167mm x 187mm (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: 動作温度0°C~50°C、保存温度 -20°C~-60°C
- > 相対湿度: 5%~95% (38°C) 結露なきこと

### 安全および環境コンプライアンス

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

### ホストインターフェイス

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

### 信頼性

- > バックアップ/復元
- > 高可用性

\* 保留中

## 利用可能なモデル

SafeNet Luna PCIe HSM AおよびSシリーズの各3種類のモデルから要件に合ったものをお選びください。

### Luna Aシリーズ: 管理しやすいパスワード認証。

A700	A750	A790
2 MBメモリ	16 MBメモリ	32 MBメモリ
標準性能:	エンタープライズ性能:	最高クラス性能:
> RSA-2048: 1,000 tps	> RSA-2048: 5,000 tps	> RSA-2048: 10,000 tps
> ECC P256: 2,000 tps	> ECC P256: 10,000 tps	> ECC P256: 20,000 tps
> AES-GCM: 2,000 tps	> AES-GCM: 10,000 tps	> AES-GCM: 17,000 tps

### Luna Sシリーズ: 高保証が必要なユースケースに対応するマルチファクタ (PED) 認証

S700	S750	S790
2 MBメモリ	16 MBメモリ	32 MBメモリ
標準性能:	エンタープライズ性能:	最高クラス性能:
> RSA-2048: 1,000 tps	> RSA-2048: 5,000 tps	> RSA-2048: 10,000 tps
> ECC P256: 2,000 tps	> ECC P256: 10,000 tps	> ECC P256: 20,000 tps
> AES-GCM: 2,000 tps	> AES-GCM: 10,000 tps	> AES-GCM: 17,000 tps

**お問い合わせ先:** 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、[safenet.gemalto.jp](http://safenet.gemalto.jp) をご覧ください。

**フォローする:** [blog.gemalto.com/security](http://blog.gemalto.com/security)

 **GEMALTO.COM**

  
security to be free