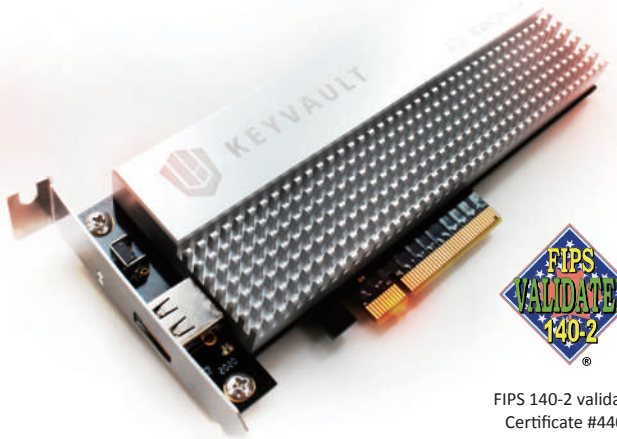
wisecuretech

KEYVAULT




FIPS 140-2 validated
Certificate #4409

# サーバー高速暗号エンジン「kvHSM」

*Fulfilling applications with agility and flexibility*

KeyVault Hardware Security Module（kvHSM）は、物理デバイスとしての機能を持ち、暗号キーを安全に保管および管理する専用装置です。この高度なセキュリティ・デバイスは、暗号キーの生成から配布、保管、廃棄、および記録に至るまでのライフサイクル全体を管理します。また、暗号化（encryption）、復号化（decryption）、署名（signing）、および検証（verification）といった重要なセキュリティ操作を行います。kvHSM はハッキング、物理的侵入、タンパリングなど、様々な外部脅威に耐えるように設計されており、暗号化プロセスに必要な堅牢な環境を提供します。CC EAL 5+ の認定を受けたこの装置は、軍事レベルの安全性を誇り、暗号キーの漏洩リスクを低減、サイドチャネル攻撃（SCA）などの脅威から保護します。

## 暗号通貨の取引用キーの保全管理

最近、ビットコインをはじめとするブロックチェーン技術に基づく暗号通貨が世界中で注目を集めています。これらの通貨のデジタル署名に使用されるプライベートキー（秘密鍵）の安全な管理は非常に重要です。取引所や販売所では、セキュリティを確保しつつ、複数アカウントに紐付けられた暗号キーを使いやすく、かつコスト効率の高い方法で管理する必要があります。
安全性を犠牲にして利便性を追求することは許されません。
kvHSM は、このようなニーズに応えるための高度にカスタマイズ可能なプラットフォームを提供します。秘密鍵の生成、配布、保存、廃棄、記録といったライフサイクル全般を管理し、暗号通貨トランザクションの暗号化、復号化、署名、検証、ハッシュ化を行うコアエンジンを搭載しています。これにより、セキュリティの高さと実行パフォーマンスのバランスを実現しています。例えば、デジタル署名の実行パフォーマンスは最大秒間 10,000 回にも達しますが、
プロセスの安全性は軍事レベルのセキュリティ基準に準拠しています。さらに、kvHSM は物理的侵入を検知し、適切な対策を講じることができます。サイドチャネル攻撃、リバースエンジニアリング、タンパリングといった脅威に対する防御も充実しています。

### 暗号アルゴリズム

- ハッシュ: SHA-2, SHA-3, HMAC
- RSA 2048
- ECC (楕円曲線暗号：最大521 bits)
  ※エドワード曲線を含む
  ECCプロトコル：ECDSA, ECIES, ECDH, EdDSA (FIPS186-5)
- AES 256 モード：ECB, CBC, CFB, OFB, GCM, XTS
- 乱数発生器：AIS-31 (class PTG2)
  ※Hash_DRBG in NIST SP800-90A に準拠
- ECC及びAES向けのFPGAベースのカスタマイズ可能な暗号化エンジン

### パフォーマンス

- AES (256 bits XTS モード) データ暗号化/復号化速度 1.6GB/秒以上
- ECDSA(256 bits) 秒間最速1万回 (10,000tps)以上

### インターフェース

- PCIe gen 2×8

※実際の発注仕様は、お客様の要件に基づいて決定されます。

## 認証サーバー（IoT エコシステム）とクラウド暗号化サービス

IoT（Internet of Things）エコシステムは、データセンター（パブリック or プライベートクラウド）、ゲートウェイ（インターネットへの中継地点）、エンドポイントデバイス（分散 IoT デバイス）で構成されます。上記のセキュリティレベルはそれぞれに重要で、手を抜いて良いポイントというものはありません。

データセンターは、ゲートウェイによって送信された集計データ受信します。その際ゲートウェイの通信経路上には「盗聴」と「改ざん」といった 2 つの大きなリスクが存在します。ハッカーはメッセージを傍受したり、クラウドサーバーへの不正なアクセス方法を取得したりする可能性があります。その為、通信や認証時のデータ暗号化は安全で持続可能なシステム運用に不可欠です。PCIe カード形式でクラウド上に組み込まれた KVHSM の提供サービスには、「データ保護」「ユーザ認証」「ブロックチェーン」の為にそれぞれ AES 暗号化、ECC ベースでの署名 / 検証と暗号キーの確立、SHA2、SHA3 ハッシュ計算機能が含まれます。また、デジタル署名の認証局としても機能し、承認されたデバイスの証明書に署名し、デバイスのファームウェアのアップデートとマスターキーのライフサイクルを管理します。

### 認証機関による証明書

- FIPS 140-2 Level 3
- CAVP: AES (ECB, CBC, CFB, OFB, GCM, XTS), ECDSA, HMAC, DRBG, SHA-2, SHA-3
- CE/FCC

### サポートするミドルウェア

- PKCS#11
- ネイティブAPI

### 実装攻撃への対策

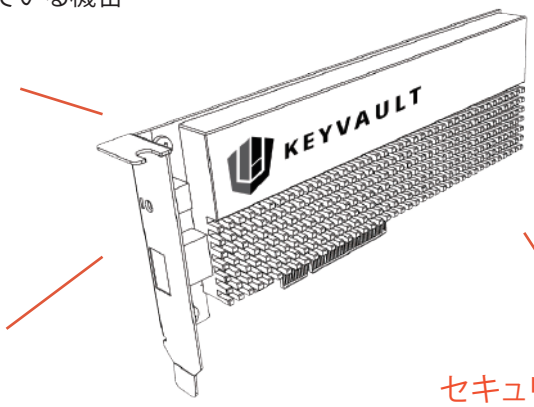
- SPA/DPA対策
- セキュリティチップ（CC EAL 5+に準拠）
- 耐タンパー技術

### データ消去ボタン

セキュリティ上の緊急事案発生時にも対応可能なモジュール内に保管されている機密データの消去ボタンです。

### データ保護シェル

物理的な侵入を検知するか、この保護シェルが破壊された場合に、機密データは自動的に消去されます。




### 暗号化アクセラレーター

アクセラレーターは暗号操作のパフォーマンスを大幅に向上させます。デジタル署名の実行速度は 1 秒あたり最大 10,000 回にも達することが可能です。（その暗号化速度は 1.6GB/ 秒を超えています）

### セキュリティチップ

モジュール内に組み込まれたセキュリティチップは、CCEAL 5+ に準拠しています。これは、軍事レベルの安全性を担保している証拠です。その洗練された設計技術はサイドチャネル攻撃やリバースエンジニアリングといった危険性も排除します。

**ワイセキュア株式会社 WiSECURE Inc.**

〒105-6490 東京都港区虎ノ門1丁目17-1 虎ノ門ヒルズ ビジネスタワーCIC Tokyo, 15F
連絡担当：Rose Lin (日本語対応可)　048-400-3057　rose@wisecure-tech.jp

https://wisecure-tech.jp