WiSECURETECH

KEYVAULT

世界初、新しい形態

kvM2HSM

エッジコンピューティング環境をシームレスにセキュア化
組込み型のハードウェア信頼の基点

ハッカーの新たな標的、エッジデバイスが直面するリスク

近年、クラウドと現場をつなぐエッジデバイスが攻撃の新たな焦点となっている。2024 年には米欧でルーターへの悪意あるファームウェア埋め込みが確認され、日本でも複数の IoT 機器にゼロディ脆弱性が発見された。これにより、セキュリティ更新、セキュアブート、トラステッドデザインの欠如といった問題が露呈し、企業の知的財産やインフラを脅かすだけでなく、社会全体の安全にも影響を及ぼす可能性がある。各国の監督機関はすでに、エッジおよび IoT 機器に対するセキュリティ要件の強化を進めている。

再設計は不要 ！ 既存デバイスをセキュリティと効率を向上

小型デバイスでは従来の ICT セキュリティ対策が適用しづらい課題に対し、WiSECURE は世界初の M.2 インターフェース HSM を開発。大型 HSM の制約を克服し、既存の OT/IoT/ エッジ機器が短期間でコンプライアンスを満たし、長期的なセキュリティ基盤を確立できるようにした。

NIST SP 800-82 Rev.3
OT システムの完全性確保を含むセキュリティ対策を強化。

EU AI Act / CRA
AI システムのリスク管理やデジタル製品全般のセキュア要件。

JC-STAR (★3) / CPSF
ファームウェア完全性の確保やデバイス認証の推奨。

Why kvM2HSM?
既存機器でも容易に強化可能！

01 多様な暗号応用を実現可能
ハードウェアレベルで改ざん防止、データ漏洩防止、鍵管理を実現。

02 システム性能を最大化
様々な暗号処理をオフロードし、CPUリソースをアプリケーション処理に集中。

03 最小限の変更で導入可能
標準M.2スロットに対応し、ボードの変更不要。

Use Cases

■ AI モデルの知的財産保護
エッジ環境に配布される AI モデルの不正取得・解析・改ざんを防止し、知的財産と収益モデルを保護

■ ロボティクス / 自律システム
センサー入力や制御ロジックの改ざんを防止し、ミッションクリティカルな動作の安全性と信頼性を向上

■ スマートファクトリー
製造設備のなりすましや不正接続を防止し、生産ライン全体の信頼性と稼働継続性を確保

■ 高度なセキュア・ゲートウェイ
多数デバイス接続環境における鍵管理と通信セキュリティを統合し、運用負荷とリスクを低減

※世界初という内容は、弊社2025年10月の調査結果を基づいています

kvM2HSMの主要特徴

高速暗号処理
暗号処理を高速化し、通信・AI・データ処理のボトルネックを解消。AES/ECCに対応し、CPU負荷を低減。エッジ環境でも高性能を維持。

高い拡張性
システム規模に応じて処理能力を柔軟に拡張。複数HSMの同時動作により、大規模環境でも安定した性能を確保。

強固な物理セキュリティ
鍵情報をハードウェアレベルで隔離し、物理攻撃から保護。不正アクセスや改ざんリスクを低減し、高信頼な運用を実現。

量子コンピュータ攻撃に対応
将来の脅威に備えたポスト量子暗号とハイブリッド方式に対応。長期運用におけるセキュリティリスクを低減。

主要仕様

インターフェース
M.2 2242 M Key
PCIe Gen3 x4

対応アルゴリズム
■ **対称鍵暗号**
AES-128/192/256
GCM/XTS対応

■ **公開鍵暗号**
ECC
ECDH/ECDSA
SECP256R1/SECP384R1/SECP521R1/SECP256K1/
Brainpool P256R1/Brainpool P384R1/Brainpool P521R1

■ **ハッシュ/MAC**
SHA-2/SHA-3/HMAC

■ **ポスト量子暗号(PQC)対応**
ML-KEM(Kyber)　512/768/1024
ML-DSA(Dilithium):　44/65/87

■ **TRNG**
NIST SP 800-90 B
AIS31

■ **DRBG**
NIST SP 800-90 A

物理セキュリティ設計
セキュアブート及びファームウェア完全性保護
CCEAL5+軍用レベルの鍵保護(容量256kB)
改ざん防止設計(Active Shield/Digital Sensor)

API
PKCS#11
Native SDK
OpenSSL

対応OS
Linux
Windows

※受注する規格はお客様のニーズに応じて調整いたします。

ワイセキュア株式会社　WiSECURE Inc.
〒113-0033東京都文京区本郷7丁目2-5 6階
03-6824-6088
https://wisecure-tech.jp