世界初、新しい形態

M.2 HSM

— 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

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機器にゼロデイ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。

米国国立標準技術研究所（NIST）は2023年に『**NIST SP 800-82**』を公表し、OTシステムにおけるアイデンティティ認証とファームウェア完全性の検証を重視するよう求めている。

欧州連合は2024年に『**人工知能法（AI Act）**』と『**サイバーレジリエンス法（CRA）**』を可決し、AIシステムにはモデルガバナンスを、ネットワーク機器にはファームウェア署名、セキュアブート、デバイス認証および更新機構の実装を義務付けている。

日本の経済産業省は『**サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**』の派生ガイドラインにおいて、機器のファームウェア完全性の確保およびデバイス認証の実施を求めている。

再設計は不要！M.2 HSMで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 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。

M.2 HSMが実現可能なセキュリティ応用

- ✓ AIモデルの保護
- ✓ アイデンティティ認証
- ✓ ファームウェア改ざん防止
- ✓ デバイスデータの暗号化
- ✓ データベース暗号化
- ✓ アクセス制御
- ✓ デバイス証明書の発行
- ✓ 安全通信

M.2 HSM — 4つの主要特徴

高速暗号処理
AESハードウェア加速により、高速な暗号化・署名・認証を実現。
RSA・ECCにも対応し、エッジ環境でも安全な暗号サービスを提供。

強固な物理セキュリティ
コア鍵をチップ内で物理的に隔離保護。リモート侵入や改ざんを防ぐ軍用レベルのセキュリティ設計。

高い拡張性
1台のデバイスで複数HSMを同時稼働。
処理能力の拡張・スケーラビリティを確保。

次世代量子コンピュータ攻撃に対応
ポスト量子暗号（PQC）対応チップを搭載。次世代量子攻撃（HNDL）をハードウェア層で防御。

主要仕様

インターフェース
- M.2 2242 M key
- PCI Gen3x4

対応アルゴリズム
- AES
  - • NIST FIPS 197（標準AES 128 / 192 / 256）
  - • NIST FIPS SP 800-38A（動作モード：ECB / CBC / CFB / OFB / CTR）
  - • NIST FIPS SP 800-38D（動作モード：GCM / GMAC）
  - • NIST FIPS SP 800-38E（動作モード：XTS）
  -
- ECC
  - ECDH/ECDSA
  - SECP256R1/SECP384R1/SECP521R1/SECP256K1/Brainpool P256R1/Brainpool P384R1/Brainpool P521R1
- RSA
  - 署名：1024 / 2048 / 3072 / 4096
  - 暗号化：1024 / 2048 / 3072 / 4096
  - 鍵生成：1024 / 2048
  -
- Digest
- HMAC
  - NIST FIPS 180-4 (SHA2)
  - NIST FIPS 202 (SHA3)
  - NIST FIPS 198-1 (SHAKE)
- ポスト量子署名標準（ML-DSA）
  - 44 / 65 / 87
- ポスト量子鍵共有標準（ML-KEM）
  - 512 / 768 / 1024
- TRNG
  - NIST SP 800-90 A
  - AIS31
- DRBG
  - NIST SP 800-90 B

物理セキュリティ設計
- セキュアブート（Secure Boot）
- ファームウェア保護機構
- CC EAL5+ 準拠・軍用レベルの鍵保護（容量256 kB）
- 改ざん防止設計
  - ActiveShield
  - Digital Sensor

ソフトウェアインターフェース（API）
- PKCS#11
- Native SDK

対応オペレーティングシステム（OS）
- Linux/Windows

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 平清ビル6階
連絡担当：Rose Lin　03-6824-6088　rose@wisecure-tech.jp

https://wisecure-tech.jp