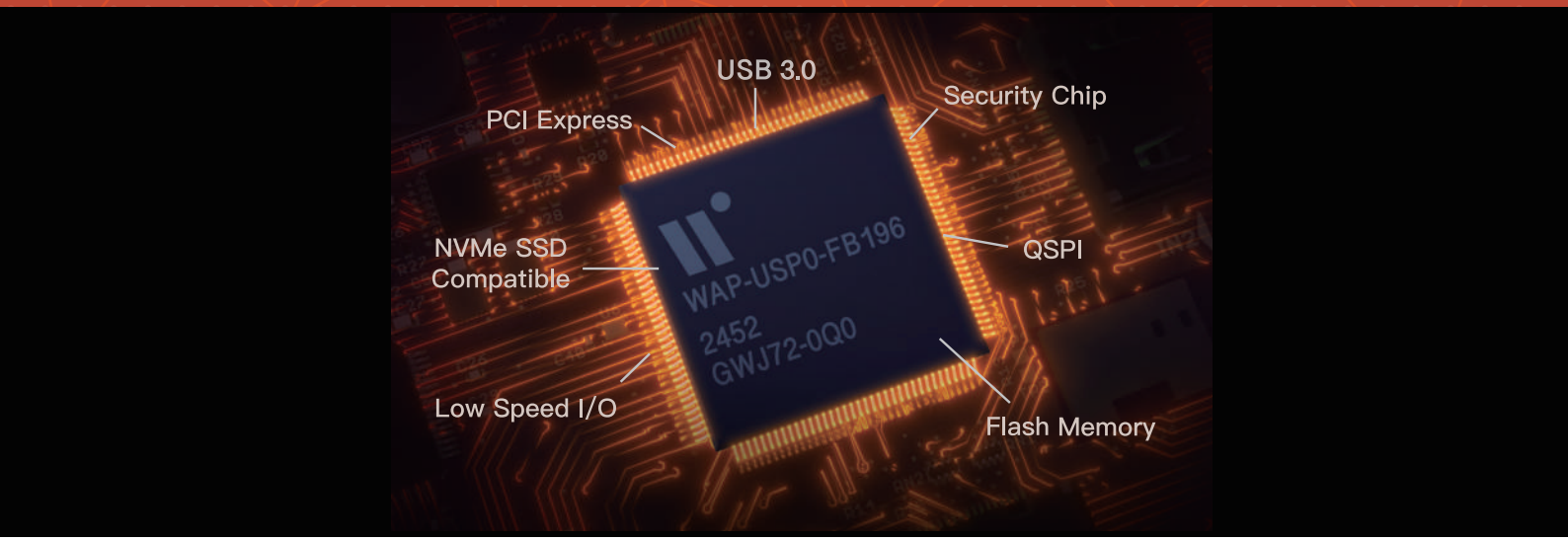
WAP – 量子耐性付きの次世帯高性能暗号アプリケーションプロセッサ



次世代の暗号プラットフォーム：セキュリティ・性能・柔軟性を高次元で両立

WAP（WiSECURE Application Processor）は、ポスト量子時代の進化するサイバーセキュリティ要件に対応するために設計された、高性能な暗号処理プロセッサです。信頼の基点（Root of Trsut）として機能し、カスタマイズ可能なアプリケーションファームウェアや専用ASIC実装への対応が可能。堅牢が柔軟性に乏しい従来のセキュリティチップと、柔軟だがセキュリティに課題のある一般的なMCU（マイクロコントローラ）の中間に位置し、強固なセキュリティ、優れた処理性能、高い設計自由度を兼ね備えています。
ドローンやセキュアブート、ブロックチェーン用コールドウォレット、ハードウェア認証デバイス、HSM（ハードウェアセキュリティモジュール）など、ミッションクリティカルなエッジデバイスに最適なセキュリティ基盤として機能します。

量子コンピュータ時代を見据えた未来対応型設計 - 耐量子計算機暗号へのスムーズな移行を実現

量子コンピュータの進展により、RSAやECCといった従来の暗号方式は急速に脆弱性が高まりつつあります。世界のサイバーセキュリティは「Y2Q（Year to Quantum）」と呼ばれる大きな転換期を迎えており、量子耐性のある暗号技術への早急な移行が求められています。これを受けて、米国国家安全保障局（NSA）はCNSA 2.0ポリシーにおいて、2025年までに全ての政府機関およびそのサプライチェーンにおいてポスト量子暗号（PQC）アルゴリズムの導入を義務化。
WiSECUREはこれに応えるべく、最新のNIST標準アルゴリズム（鍵カプセル化のML-KEM、デジタル署名のML-DSA）に完全対応したPQC対応プロセッサ「WAP」を発表しました。RSAやECCとの互換性も保持しており、既存インフラやデバイスから量子耐性のあるシステムへの併用も可能です。

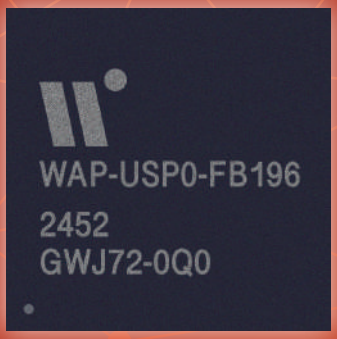
WAPチップの特長

国際標準 PQC に対応
- ML-KEM（**暗号鍵交換**）および ML-DSA**(デジタル署名)**に対応。
- ハイブリッド署名を実装可能で、将来製品・デバイスは再設計なしで量子攻撃に対応可能。

ハードウェア安全設計と高速暗号処理
- **PUF（Physical Unclonable Function）**技術によるマスターキーの安全性を強化。
- **130MB/s**の高速AES暗号化および低消費電力設計 により、高性能と省エネを両立。

専用 ASIC チップとしてのカスタマイズが可能
- 利用シーンに応じたアーキテクチャ設計が可能で、専用の ASIC暗号チップ に最適化。チップの開発コストとリスクを避ける。

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



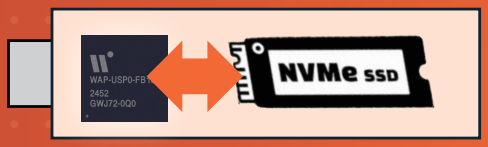
フルカスタム ASIC

幅広い活用シーン

- FIDO 認証用セキュリティキー
- HSM（ハードウェアセキュリティモジュール）
- ブロックチェーン ハードウェアウォレット
- スマートメーター のセキュリティ保護
- オンライン決済・金融セキュリティ

HSM / FIDO 認証用セキュリティキー

エッジデバイス向け SoC のセキュアブートおよび暗号アクセラレータ



ストレージ保護

決済端末

製品規格

対応暗号アルゴリズム

共通鍵暗号方式（AES）

- AES-128 / AES-192 / AES-256 に対応し、NISTに準拠したすべてのモード（例：ECB、CBC、GCM など）をサポート。

データスループット：最大1Gbps

従来型公開鍵暗号（Classic PKC）

- ECC（楕円曲線暗号）
- RSA（最大4096ビットまで対応）

耐量子計算機暗号（Post-Quantum Cryptography, PQC）

- Kyber（FIPS 203準拠）
- Dilithium（FIPS 204準拠）

ハードウェアインターフェース

- USB 3.0
- QSPI / SPI
- GPIO
- PCI Express（PCIe）
- NOR フラッシュ対応

ハードウェア構成

- プロセッサ：ARM 32ビット コア
- メモリ：SRAM 512KB
- 永続ストレージ：非搭載（内部に保存領域なし）

セキュリティ機能

- NIST SP 800-90B 準拠の真性乱数生成器（True Random Number Generator, TRNG）
- 外部からの攻撃に対する環境センサー搭載（温度、電圧などの異常検知）
- センシティブな回路領域を保護する遮蔽マスク（シールド）構造
- セキュアインターフェースバインディングによるデバイス認証制御

認証および準拠規格

- CNSA2.0
- FIPS 140-3（レベル3）認証申請中（CAVP認証も含みます）