wisecuretech

VeloCrypt® MicroSD HSM

世界最小サイズ
同クラス最高速のHSM

暗号システムにおける最も重要な「鍵（キー）」は、安全な環境で保管され暗号演算を行う必要があります。「ハードウェアセキュリティモジュール（HSM）」は、システムセキュリティの信頼の根幹（Root of Trust）として、世界中の重要インフラ、軍事・行政機関、金融機関において不可欠な存在です。しかし従来の HSM は拡張カード型が主流であり、モバイル端末やエンドポイントデバイスでは直接利用できません。

VeloCrypt MicroSD は、世界最小クラスの HSM として、モバイルやエンドポイントにおける高度なセキュリティ要求に対応。高速なデータ暗号化保存、鍵の生成と管理、デジタル署名、認証などの暗号機能を提供し、安全な認証、起動、機密データ保護、安全通信を実現します。新たな応用領域における高まる安全ニーズに応え、正しいセキュリティ基盤のもと、安定した業務運用を支援します。

物理セキュリティ

CC EAL5+ 認証のセキュリティチップと精密な内部回路設計により、サイドチャネル攻撃などのハードウェア攻撃を防ぎ、軍用レベルの高度な鍵保護対策を実現します。

システムセキュリティ

セキュリティ重視のファームウェア設計を採用し、機密データや鍵が静的に保存されている場合も、動的に転送される場合も、システム全体で保護します。

静的データ暗号化

512MB～32GB の暗号化領域を確保し、強力な認証機構でアクセスを制御。保存データの暗号化を実現します。

インターフェース互換性

SDIO インターフェースとシンプルなサービスアクセス設計により、各種組込みシステムやデバイスに幅広く対応。ハード・ソフト両面の開発負担を軽減し、製品の開発期間とコストを削減。市場投入を加速します。

暗号サービスと性能

各種標準暗号アルゴリズムを内蔵し、幅広いセキュリティニーズに対応。AES 暗号化ストレージは最大 10MB/s の高性能を実現し、高い安全性と処理能力で強固な防御環境を構築します。

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

Secure Boot

VeloCrypt SA シリーズは、デバイスにハードウェアレベルの信頼の基点（RoT）を提供し、改ざん防止機構と高度な認証により、鍵の安全を確保。起動時にはシステムの整合性を検証し、信頼されたファームウェアと OS のみを実行させることで、マルウェアの侵入やネットワーク乗っ取りを防止。起動から稼働まで、常に信頼された環境を維持します。

FIDO Device OnBoard (FDO)

VeloCrypt SA シリーズは、kvFDO サービスと組み合わせることで、既存の IoT 機器に搭載可能。FDO 標準プロトコルを通じて、企業の SaaS 型デバイス管理システムに接続し、自動化された迅速な機器展開を実現。運用効率とライフサイクル管理の透明性を大きく向上させます。

機密データの暗号化と保存

VeloCrypt SA シリーズは、高速な暗号化ストレージ性能とセキュリティチップによる軍用レベルの保護を両立。柔軟に設定可能な暗号化領域により、さまざまな用途で高いセキュリティとスムーズな処理性能を維持し、デバイスのデジタル資産を守ります。

エンドツーエンドのセキュア通信

VeloCrypt SA シリーズは、ハードウェアベースの保護に加え、ソフトウェア開発キット（SDK）を提供。メーカーは既存アプリとの統合が可能で、複数の通信プロトコル間におけるデータ転送の安全性を確保。盗聴や改ざんへの耐性を強化します。

製品仕様 VeloCrypt SA Series

外形サイズ：SD メモリーカード形式
フラッシュタイプ：SLC / MLC
ストレージ容量：512MB / 8GB / 16GB / 32GB
動作温度範囲：0℃ ～ 70℃ | 保存温度範囲：-40℃ ～ 125℃
動作電圧：2.7V ～ 3.6V
消費電流：160mA + 35mA

ハードウェア特長

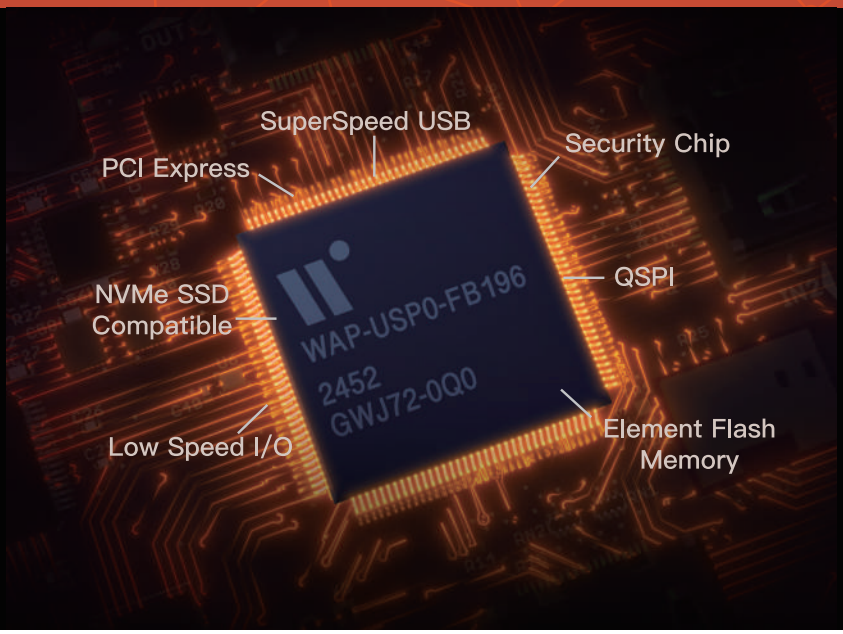
- SD Default Speed / SD High Speed / SD UHS-I に対応
- CC EAL5+ 認証取得の高セキュリティチップ採用
- CE / FCC / VCCI / BSMI 各種安全規格に準拠
- PKCS#11 / ネイティブ API 対応

暗号アルゴリズム対応一覧

- メッセージダイジェスト：SHA-2 / SHA-3 / HMAC
- 公開鍵暗号：RSA 2048bit
- 楕円曲線暗号（ECC）：
- 素数域カーブ（最大 521bit）
- エドワーズ曲線対応
- 対応プロトコル：ECDSA / ECDH
- 対称鍵暗号（AES）：ECB / CBC モード対応
- 乱数生成：
  AIS-31（PTG.2）認定ハードウェア TRNG
  NIST SP800-90A 準拠の Hash-DRBG

WAP 耐量子計算機暗号チップ

量子時代に備える高性能暗号プロセッサ（AP Processor）



量子コンピューティング技術の進展により、「Y2Q（Year to Quantum）」によるセキュリティリスクが現行の公開鍵暗号システムに深刻な影響を及ぼすことが予測されています。WiSECUREは、この新たな脅威に対応する最先端のチップレベルソリューションとして、高性能・高セキュリティ・高柔軟性を兼ね備えた**耐量子計算機暗号（PQC）チップ**を提供し、量子時代のサイバーセキュリティ課題に対応します。

WAP 耐量子計算機暗号チップとは

WAPは、高性能な**暗号プロセッサ（AP Processor）**であり、次世代の暗号システムに対応する設計が施されています。米国標準研究院（NIST）が定めた国際標準耐量子計算機暗号アルゴリズム ML-KEM および ML-DSA に対応するとともに、従来の ECC や RSA などの公開鍵暗号にも対応し、量子コンピューティング時代におけるハイブリッド移行戦略を実現します。さらに、チップ内部の機能は柔軟にカスタマイズ可能で、迅速なシステム統合と実装を支援します。

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。

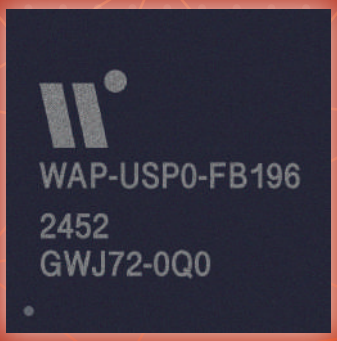
ハードウェア安全設計と高速暗号処理

- **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



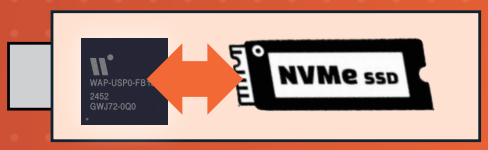
フルカスタム ASIC

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

- FIPS 140-3（レベル3）認証申請中
- CAVP（Cryptographic Algorithm Validation Program）準拠
- CMVP（Cryptographic Module Validation Program）申請予定

ワイセキュア会社案内

サイバー攻撃が進化しても、
貴重なデジタル資産を守れます。

Security wisely empowered

お問い合わせ先
ワイセキュア株式会社 WiSECURE Inc.
〒105-6415 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15F CIC Tokyo
TEL: 048-400-3057
担当者名：Rose Lin
メール：rose@wisecure-tech.jp

https://wisecure-tech.jp

ワイセキュア株式会社
WiSECURE Inc.

〒105-6415 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 15F CIC Tokyo

TEL: 048-400-3057
https://wisecure-tech.jp

暗号学に特化したデザインと実績を持つチーム

ワイセキュア株式会社（WiSECURE Inc.）は、アジア地域におけるハードウェアセキュリティのパイオニアとして、国際的な政府機関や軍事施設など、極めて高いセキュリティ要件を持つシステム設計に携わってきました。当社のチームは、暗号学の実践と最先端のセキュリティ技術に精通しており、豊富な経験を積んでいます。
私たちは、最新の暗号技術と急速に進化するサイバー攻撃のトレンドに基づいた専門知識を駆使し、暗号鍵の保護、デジタル資産のセキュリティ強化、身元認証ソリューションを提供しています。
さらに、システムインテグレーター（SI）との密接な連携を通じて、中小企業を含む幅広いクライアントのデジタル資産を守るための包括的なサービスを展開しています。

USBをはじめとする「lightweight HSM」のリーダー

ワイセキュアは、量産効果によるコスト削減と最先端の半導体技術を活用し、高いコストパフォーマンスと優れた処理能力で他社と一線を画しています。市場の多くサプライヤーが特定の形状やソリューションに依存している中で、ワイセキュアは世界でも数少ない、USB、MicroSDなどコンパクトフォームファクターを含めシステム全体に対応する幅広いソリューションを提供するメーカーです。
この柔軟なアプローチにより、さまざまなクライアントの多様なニーズに応え、セキュリティ業界における「lightweight HSMのリーダー」としての地位を確固たるものにしています。

安全設計サービスと多様な製品を提供

当社は、アルゴリズムの設計から実装まで、さらにチップやモジュール、ソフトウェア製品に至るまで、幅広いニーズに対応しています。多様なソリューションを通じて、あらゆる段階で高品質なセキュリティ設計サービスを提供しています。

デザインサービス

- Silicon IP of Algorithms
- KVSoftKey with SRAM PUF
- Authentication Chip
- iBadge Device Management
- S97 Security Chip
- Fusion FPGA Security Module
- Cryptocurrency Hardware Wallet

コンポーネント/モジュール


FIDO2 Level 2 Chip


WAP - WiSECURE PQC Application Procceser


FIDO2 L2 USB Security Key


USB HSM


MicroSD HSM
Secure Messaging
IoT Secure Boot


USB data protector with FIDO2


FIDO2 NFC/BLE/USB Card


FIPS140-2 L3 certified PCIe HSM

システム（クラウド/オンプレミス）

Zero Trust Network Access

Secure File Mgmt Platform


BYOK for Cloud HSM

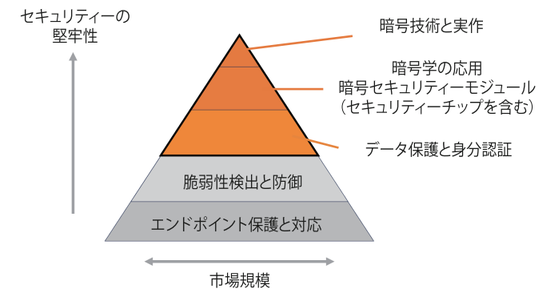

Secure NAS

FIDO2 Server

セキュリティ市場の進化とワイセキュアの役割

過去 10 年間、情報セキュリティの世界は主にネットワークの防御に注力してきましたが、最近では、セキュリティ戦略がデータを中心に据える方向へと移行しています。これは、攻撃手法の進化に伴い、企業にとってデータセキュリティがますます重要になっていることを反映しています。
しかし、市場にはデータセキュリティに関する誤解が広がっています。多くの人が、「データを暗号化するだけで、安全性が確保される」と考えています。実際には、暗号化や認証、署名などの技術を使用しても、鍵が漏洩すればデータの安全性は失われます。不正アクセスを試みる者は、漏洩した鍵を使用してデータを改ざんしたり、偽装したり、暗号化されたデータを解読したりする可能性があります。
このような背景から、WiSECURE が提供するセキュリティソリューションは、暗号アルゴリズムの採用だけではなく、鍵の保護と管理にも重点を置いています。私たちは、企業のニーズに合わせてコスト効率、柔軟性、およびセキュリティのバランスを最適化します。

WiSECURE の市場における立ち位置に関する詳細は、下のグラフィックを参照してください。
長年にわたる暗号技術の経験を活かし、WiSECURE はハードウェア暗号モジュールとその応用に関するカスタマイズサービスを提供しています。これにより、IT サービスプロバイダー、システムインテグレーター、製造業者は、さまざまな分野やアプリケーションにおいて、統合や開発を行うことができます。
また、WiSECURE は最近、NIST 800-207 標準に準拠したゼロトラストモデルに基づくデータ保護システムと身分認証ソリューションを提供しています。この特許技術により、WiSECURE は企業のセキュリティニーズにより密接に対応しています。



ODM及びOEMサービスについて

WiSECURE では、高度な ODM（オリジナルデザイン製造）サービスを提供しています。
これには、ハードウェアセキュリティモジュール（HSM）、セキュリティキー、そして FileAegis セキュアファイルストレージのカスタムデザインが含まれます。私たちは、標準化された製品の提供から、特定の暗号化ベースのセキュリティコアやアプリケーションエンジンの開発まで、幅広いニーズに応えることが可能です。
お客様は、共同での設計と製造プロセスに参加することも、お客様独自のブランドロゴを用いた製品の製造を選択することもできます。これにより、企業は自社の製品ラインを拡大し、市場における差別化を図ることができます。
WiSECURE の ODM および OEM（オリジナル機器製造）サービスは、高品質で信頼性の高いセキュリティソリューションをお客様のブランドで市場に提供したい企業に最適です。

顧客実績

Google AMERICAN EXPRESS CYCRAFT Chunghwa Telecom
SMARTdisplayer A PC-like Smart Card KeyXentic Inc. UDSEC

©2024 WiSECURE Inc. All rights reserved