

CryptoAir

USBフォームファクターのHSMとして、
データ・端末・クラウド環境を包括的に保護



Feature



ポータブルなハードウェア暗号エンジン

CryptoAirはデータの暗号化および鍵保護機能に対応。強固な認証やデジタル署名など、システムに必要な暗号機能を一元的に提供します。



PQCと移行に不可欠なハイブリッド方式に対応

暗号アジリティに加え、耐量子計算機暗号 (PQC) にもいち早く対応。現在のHNDL攻撃から将来の量子コンピュータによる脅威まで、長期にわたるデータ保護を実現します。



ハードウェアレベルの高度な鍵保護

CC EAL5+認証取得済み産業用最高レベルのセキュアエレメントにより暗号鍵を保護。物理攻撃やサイドチャネル攻撃に対しても高い耐性を備えています。

CryptoAirの代表的な適用領域

- **セキュアデータ交換**
機密データの暗号化・安全な送信を実現
- **クラウドデータ保護**
BYOK・Local Key Vaultによるデータ主権を実現
- **エンドポイント/エッジ保護**
PC・産業機器へハードウェア鍵保護を追加
- **IoT・組み込み用途**
既存機器へHSM機能を容易に導入

想定される活用例

セキュアNAS: 内部不正・外部攻撃によるデータ漏洩を防ぐ

組織内で利用されるNAS (Network Attached Storage) には、内部不正アクセスや外部からの攻撃によるデータ漏えいリスクが存在します。特に、保存データが十分に保護されていない場合、ストレージへ直接アクセスされることで、重要情報が流出する可能性があります。

CryptoAir は、NASなどのストレージ環境に保存されるデータを暗号化し、セキュアなデータ保護基盤を実現します。



想定される活用例

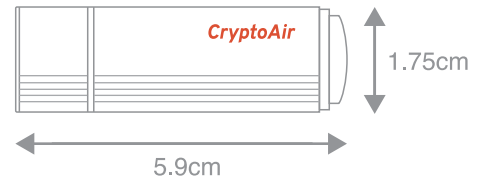
クライアントサイド暗号化: 大規模組織向けのクラウド主権の実現

クラウドサービスやデジタル環境の普及に伴い、組織は重要データを自ら管理し、利用範囲やアクセス権限を制御する「デジタル主権 (Digital Sovereignty)」の確立が求められています。

CryptoAirは、クラウドを含むさまざまなデジタル環境において、組織が暗号鍵とデータ保護を自律的に管理するためのセキュリティ基盤を提供します。

例えば、Google Workspace (GWS) のクライアントサイド暗号化 (CSE) 環境では、CryptoAirをローカル鍵管理基盤として利用することで、暗号鍵を企業自身が安全に保管・制御することが可能になります。さらに、アクセス制御、監査機能などを統合可能、クラウド時代における企業データの主権確保とゼロトラストセキュリティの実現を支援します。





仕様

対応アプリケーション	ファイル保護アプリケーションパッケージ 鍵共有アプリケーションパッケージ WEB USB
認証機能	暗号ベースの認証 ログイン試行回数を制限するポリシー
暗号アルゴリズムとサービス	■ 対称鍵暗号 AES(GCM / ECB / CTR / CBC) ■ 公開鍵暗号 ECDSA / EdDSA ECIES / ECDH / ECMQV RSA(最大4096) ■ ハッシュ/MAC SHA256 / SHA3 / SHA384 / MAC / HMAC ■ 耐量子計算機暗号 PQC ML-DSA(Kyber): 512/768/1024 ML-KEM(Dilithium): 44/65/87 ※ ハイブリッド方式を対応 ■ 鍵導出関数 PBKDF / KBKDF ■ 乱数生成 DRBG(SP 800-90A) TRNG(SP 800-90B/AIS-31 準拠)
API	PKCS#11 ネイティブAPI OpenSSL
認証	CC FCC RoHS VCCI
製品仕様	USB 2.0 複合型 HID(Human Interface Device)、USB マスストレージクラス チップカード型インターフェースデバイス
ストレージ	CC EAL 5+ Secure Element Key Storage 256KB

※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。

量子コンピュータ時代に備えるCrypto Agility

将来の量子コンピュータによる暗号解読やHNDL (Harvest Now, Decrypt Later) の脅威に備え、すでに暗号基盤の移行準備が求められています。

CryptoAirは、Crypto Agilityを備えた暗号コアにより、PQCへの移行、既存暗号とのハイブリッド運用、新規暗号規格への対応を柔軟に実現。暗号アルゴリズムの更新時にもハードウェア交換を不要とし、長期的にアップデート可能なセキュリティ基盤を提供します。

セキュリティの未来を共に創る、WiSECUREの強み



クラウドからエッジまで対応する包括的なセキュリティ基盤

クラウドからエッジデバイスまで幅広く対応する暗号モジュールにより、WiSECUREはコストパフォーマンスに優れたサイバーセキュリティソリューションを提供します。お客様のユースケースに潜むリスクを明確化するコンサルティングと、ニーズに応じた最適な製品の提供を行っています。



高度な暗号技術と柔軟な開発対応力

WiSECUREは、暗号機能からセキュリティ設計まで、お客様の要件に応じて提案可能です。セキュリティモジュールのODM、OEMサービスも提供しています。



運用支援によりHSMの最大限に活用させる

WiSECUREは、長年のセキュリティ技術と鍵管理の知見をもとに、製品を提供するだけでなく、お客様が本当に安全な鍵管理を実現できるよう伴走します。NIST SP 800-57に基づく設計・運用支援により、HSMの性能を最大限に活用したセキュアな環境を提供します。