WiSECURE会社案内

Security wisely empowered

IKV-Techは、ハードウェア製品とセキュア設計サービスを提供する情報セキュリティ（Data Security）企業です。

主な顧客には、以下のような分野が含まれます。

- 政府
- 航空宇宙機器産業、通信業
- デバイスベンダー
- エンタープライズ

©2024 WiSECURE Inc. All rights reserved

InfoKeyVault Technology 会社概要

2006年設立

弊社は、組み込みセキュリティを専門とするサービス企業です。

インフィニオンなどのグローバルチップベンダーが提供するチップを活用し、セキュリティソリューションを提供する独立系デザインハウス（IDH）です。

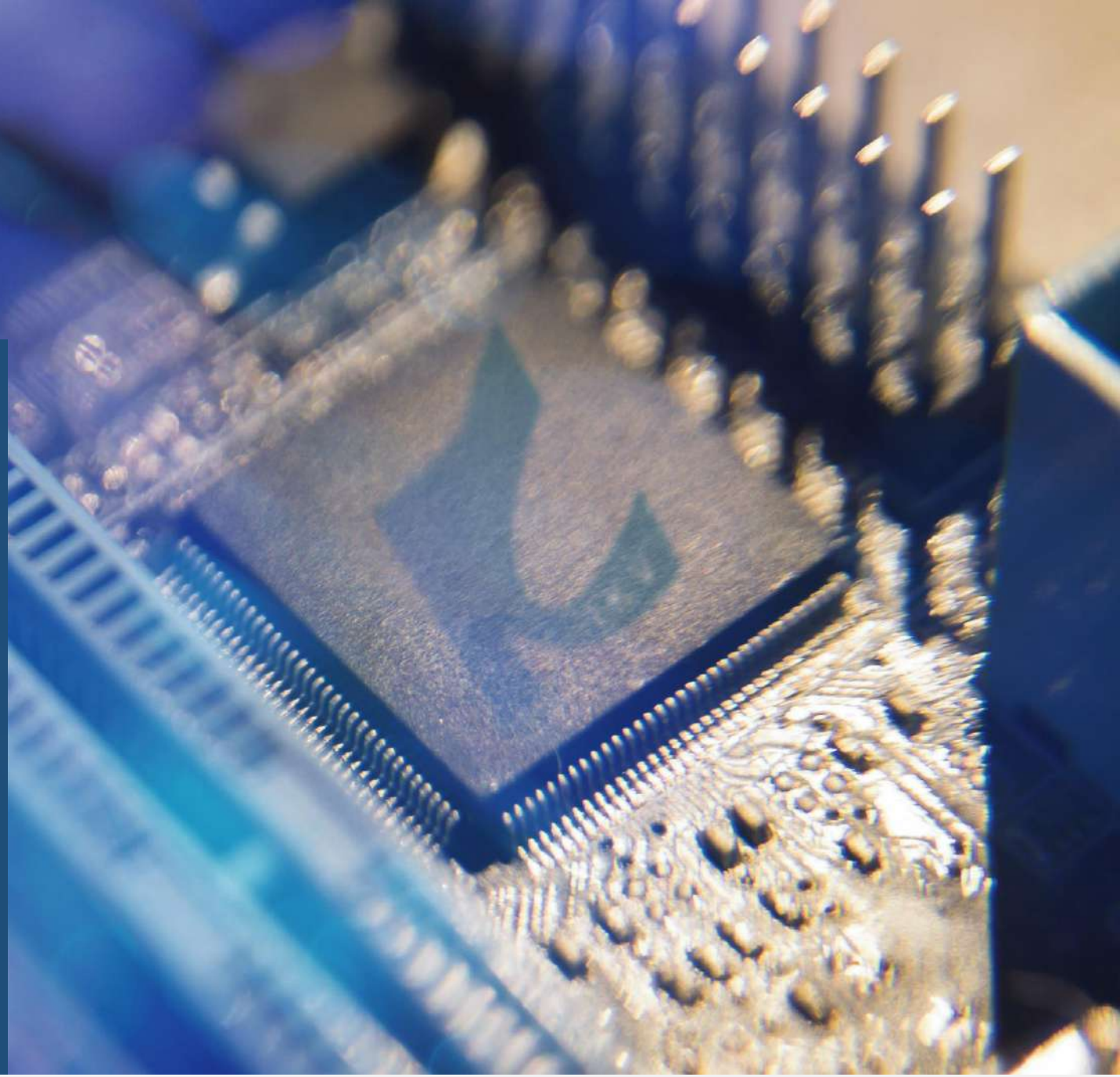
- 資本金　3百万ドル
- 従業員数　45 人
- 売り高　8.5Mドル（売上総利益は6.5Mドル）
- 認証　ISO27001（2025年6月取得予定）

©2024 WiSECURE Inc. All rights reserved

infokeyVault

EXPERTISE

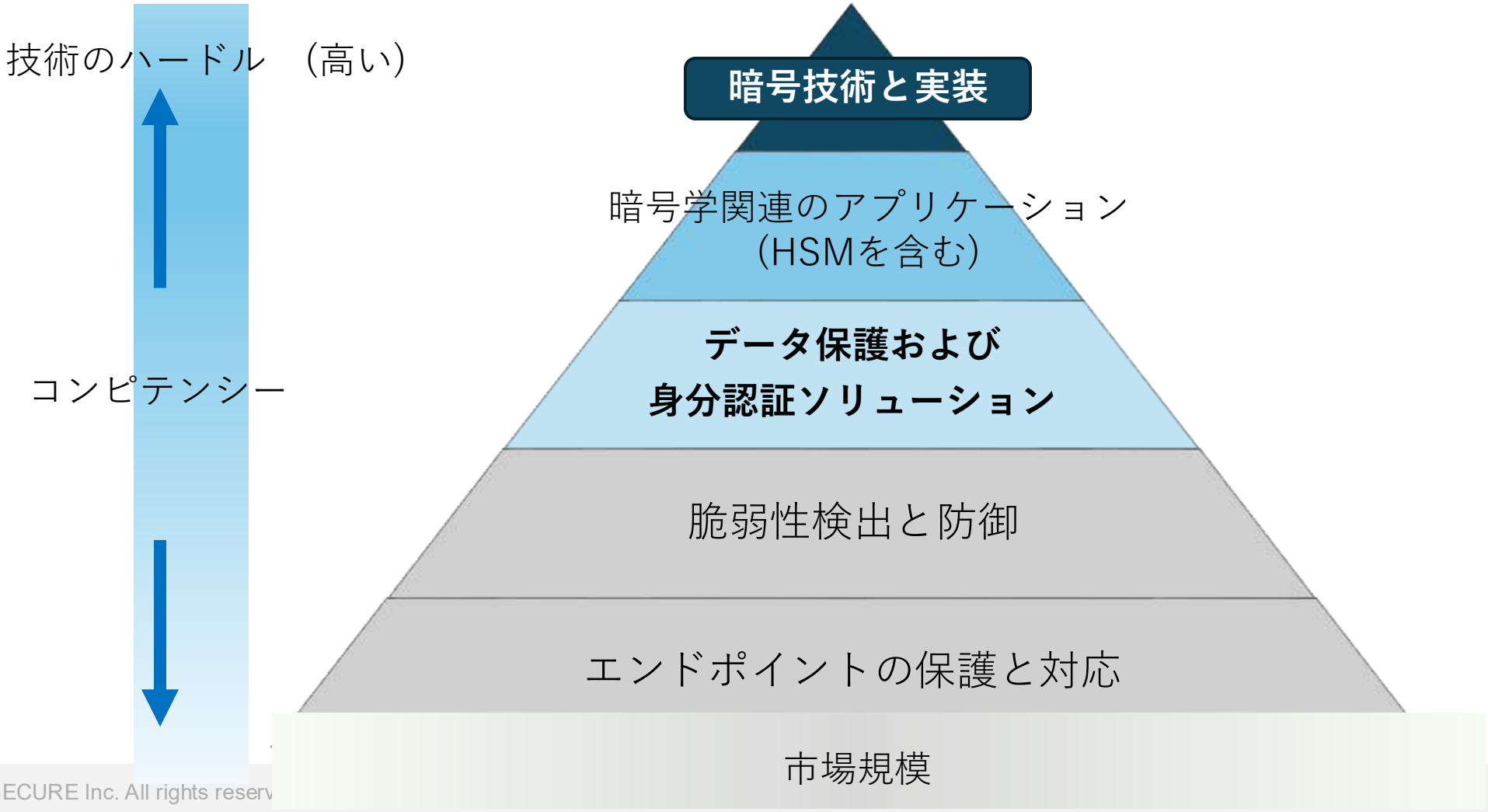
私たちの強みは、暗号技術と鍵管理にあります。多様なデバイスやプラットフォームに対して、ハードウェアベースのセキュリティを実現しています。



©2024 WiSECURE Inc. All rights reserved

wisecuretech

サイバーセキュリティの基盤：暗号技術



©2024 WiSECURE Inc. All rights reserv

SERVICE & SOLUTION

- Silicon IP of Algorithms
- KVSoftKey with SRAM PUF
- S97 Security Chip Solutions
- Fusion FPGA Security Module
- microSD Card with FPGA
- Storage Protection Hardware

©2024 WiSECURE Inc. All rights reserved

コマーシャルの実績

Google

AMERICAN EXPRESS

ASUS

ADVANTECH

AUTHENTREND

SecuX

CoolBitX

SAINT-FUN

I•X

SMARTdisplayer
A PC-like Smart Card

CYCRAFT
奧義智慧科技

中華電信
Chunghwa Telecom

VIVE

inJoy
Joy Motion

旭聯資安
SUNNET CYBER

DCloak

PTSC
北祥科技服務

ARES 資通電腦

QNAP

©2024 WiSECURE Inc. All rights reserved

高度なセキュリティに特化した製品実績

※ 製品中のセキュリティチップはCC EAL5+（軍用レベル）という認可を取得しました。

※ 弊社製品はすべて台湾で設計・製造されております。

ハードウェアOTP

サーバーディスク暗号化
※ FIPS140-2 Level 3 認証取得

NASストレージ暗号化

暗号通貨保護
コードウォレット

産業コンピューター

通信暗号化
IoTセキュリティ

暗号化USBメモリ

高速暗号エンジン

PCファイル暗号化
パスワードレス認証
※ FIDO2 Level 2 認証取得

VRゴーグル

©2024 WiSECURE Inc. All rights reserved

さらに民間に広がるための
ブランド社：ワイセキュア

2024年8月に埼玉に設立
事業内容：

- ハードウェア・セキュリティ・モジュール（HSM）
- データ保護関連ソリューション
- アイデンティティアクセス管理ソリューション
- IKV-Techの安全設計サービス

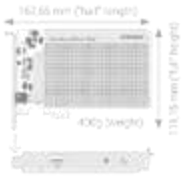
世界でも数少ない「軽量」暗号モジュール

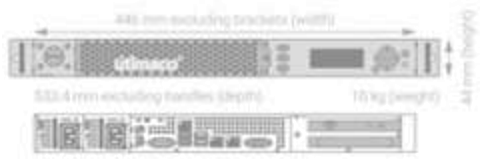
wisecuretech

nCIPHER
AN ENTRUST DATACARD COMPANY

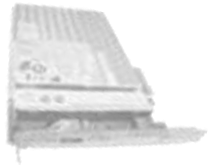
THALES

utimaco®





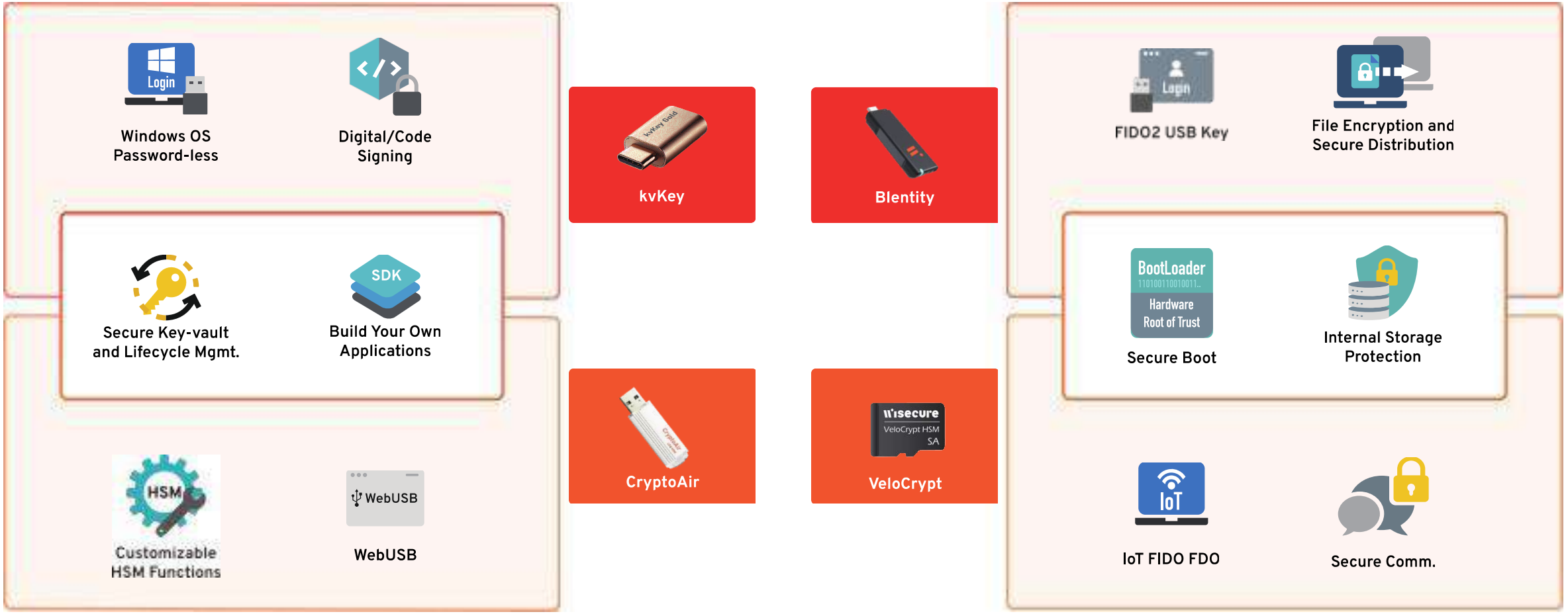
IBM



©2024 WiSECURE Inc. All rights reserved

コンパクト仕様のHSMシリーズ

高速暗号化　コピー･改ざん防止　鍵管理と保護　デジタル署名　多要素認証



©2024 WiSECURE Inc. All rights reserved

ユースケース

Web USB
FIDO2 External Authenticator

IoT Edge Security
On the Fly Encoding

Wi-Fi WPA
Remote Security
Branch Office
Work form home

BYOK (Bring your own key)
Secure Cloud Data
Protection
Cloud Security

Data at Rest
Secure NAS Standalone
Cloud File Protection

IP Protection
Embedded Safeguard

Blockchain Cryptocurrency
Blockchain Cold Wallet
Blockchain Smart Contract

Cipher Platform

Document DRM
Content Protection

©2024 WiSECURE Inc. All rights reserved

前蔡英文総統、現頼清徳総統、
アメリカ前国土安全長官が弊社を訪問

アメリカ前国土安全保障省長官
ジャネット・ナポリターノ氏が
特にワイセキュアを指名訪問し
ました。

©2024 WiSECURE Inc. All rights reserved

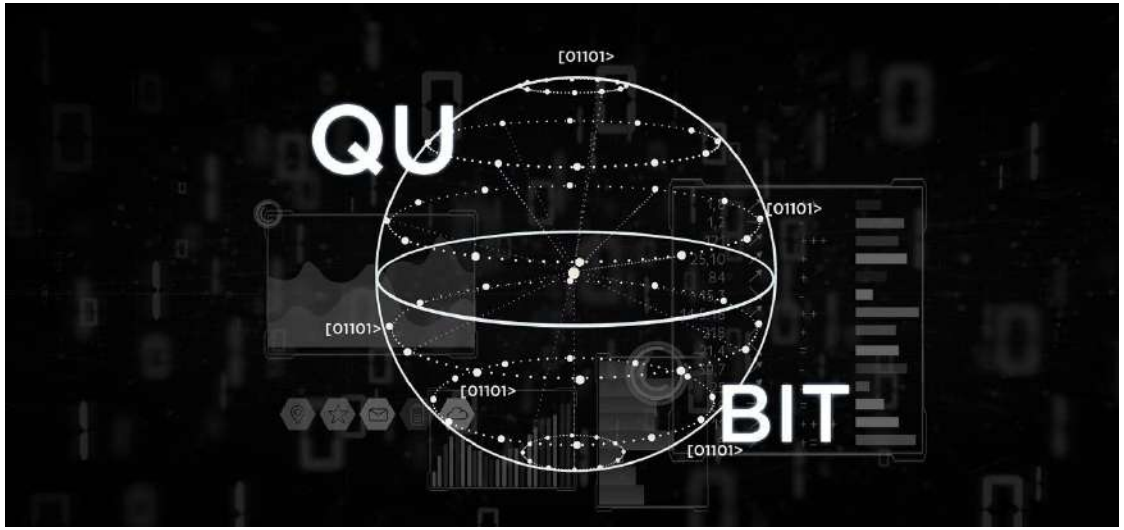
本日ご紹介する製品

1. 世界中に先端的な耐量子暗号ソリューション
2. Google Workspace クライアントサイド暗号化
3. 脱PPAP！USBセキュリティデバイス

©2024 WiSECURE Inc. All rights reserved

1. PQC対応の
アプリケーションプロセッサ

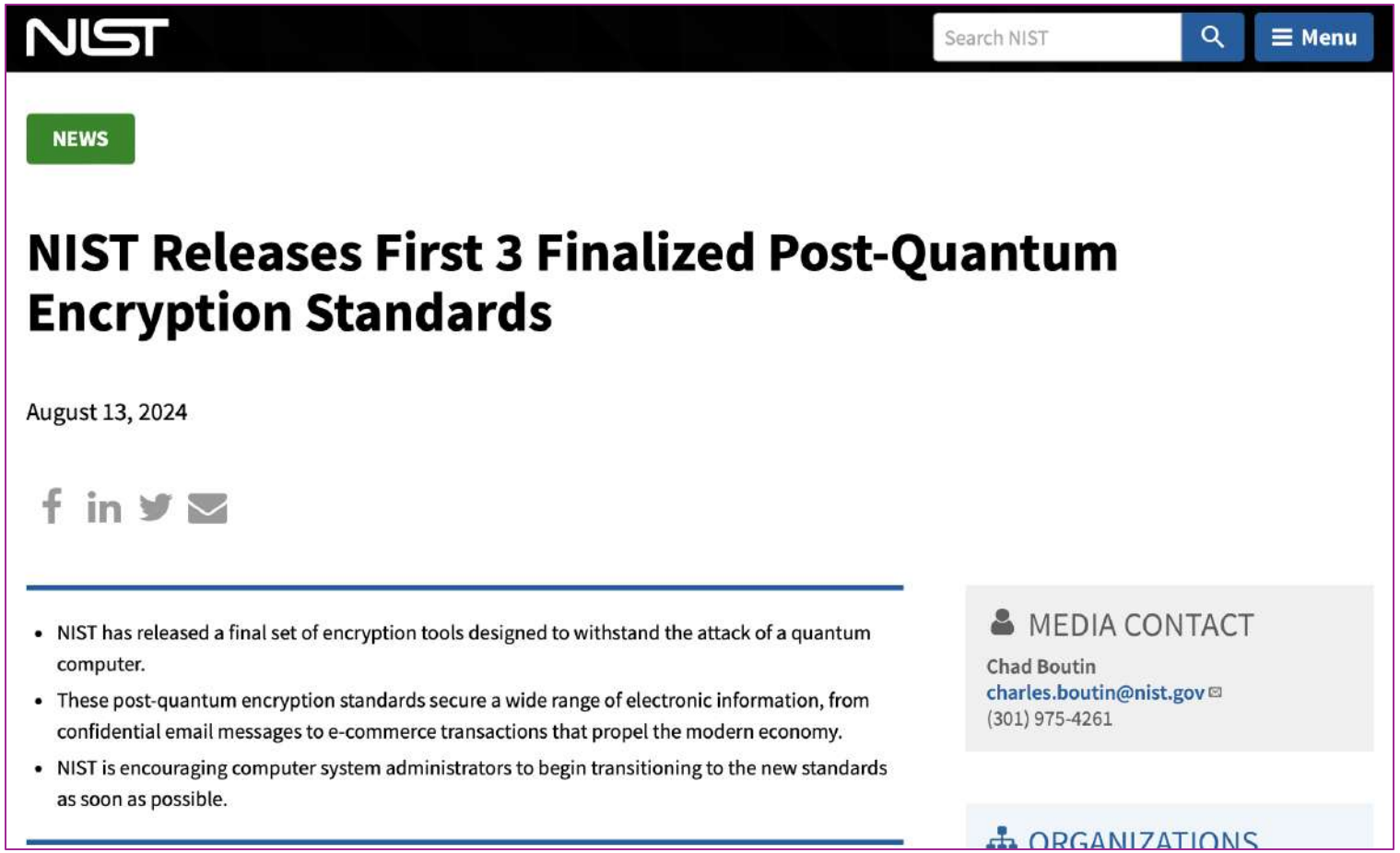
耐量子計算機暗号技術が必要となる次の時代へ



公開鍵暗号方式については、量子コンピュータの脅威に対応するために再設計が必要です。こうした新しい暗号方式は、耐量子計算機暗号（Post Quantum Cryptography, PQC）と呼ばれます。

©2024 WiSECURE Inc. All rights reserved

NISTから耐量子計算機暗号標準がリリース



NIST

Search NIST

Menu

NEWS

NIST Releases First 3 Finalized Post-Quantum Encryption Standards

August 13, 2024

- NIST has released a final set of encryption tools designed to withstand the attack of a quantum computer.
- These post-quantum encryption standards secure a wide range of electronic information, from confidential email messages to e-commerce transactions that propel the modern economy.
- NIST is encouraging computer system administrators to begin transitioning to the new standards as soon as possible.

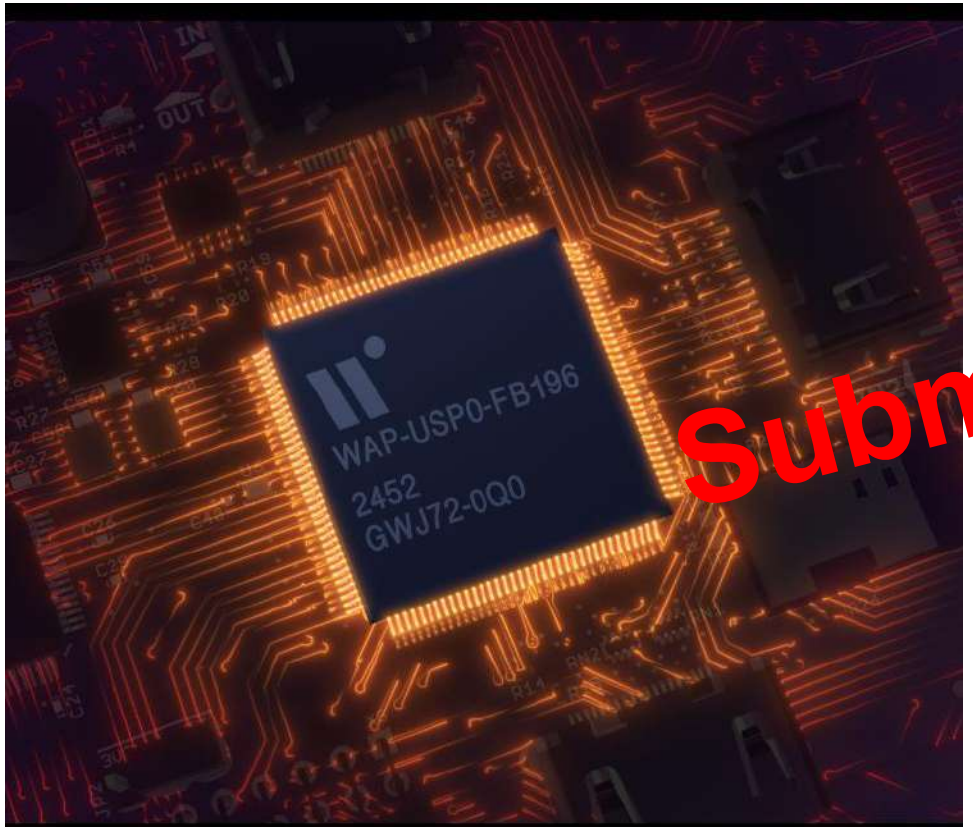
MEDIA CONTACT

Chad Boutin
charles.boutin@nist.gov
(301) 975-4261

ORGANIZATIONS

©2024 WiSECURE Inc. All rights reserved

当社WAPチップ：
ワイセキュア・アプリケーション・プロセッサ



WAPチップの主な特長：対応アルゴリズム

対応アルゴリズム

- AES-128/192/256　NIST全モード対応 スループット：最大1Gbps
- 従来型公開鍵暗号（Classic PKC）：ECC、RSA
- PQC: Kyber（FIPS 203準拠）、Dilithium（FIPS 204準拠）

内部に永続ストレージなし

- 512KB SRAM搭載
- ARM 32ビットプロセッサ内蔵

ハードウェアインターフェース

- USB3/QSPI/SPI/GPIO/PCIe/NOR-Flash 対応
- セキュアインターフェースバインディング対応

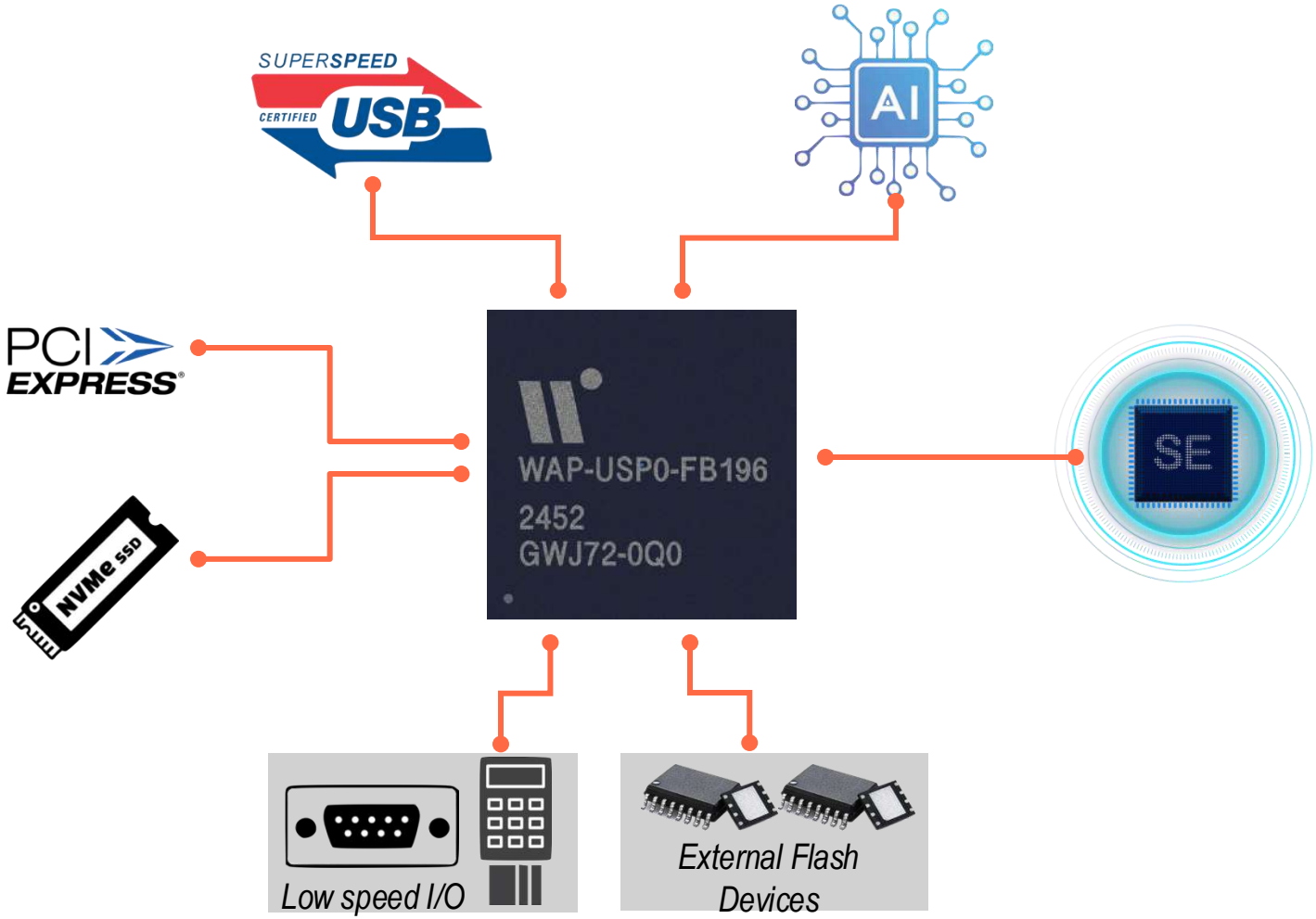
セキュリティ機能

- SP 800-90B 準拠の真性乱数生成器（TRNG）
- 外部攻撃を検知する環境センサー
- 機密回路を保護するシールドマスク

Submitting FIPS 140-3
CAVP
CMVP (Level 3)

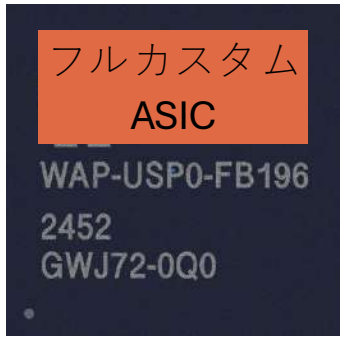
©2024 WiSECURE Inc. All rights reserved

WAPチップのインタフェース



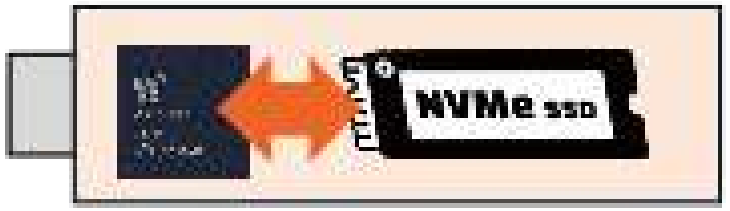
©2024 WiSECURE Inc. All rights reserved

主なアプリケーション分野

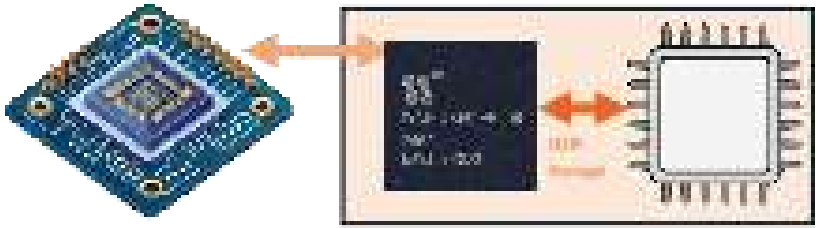


スタンドアロン型**USB**セキュリティドングル：
USB-HSM または **FIDO**認証器

ストレージ保護



エッジデバイス向け**SoC**：
セキュアブート＆暗号アクセラレーター



決済端末

©2024 WiSECURE Inc. All rights reserved

2. Google Workspace
クラアントサイド暗号化

データを取られても中身が漏洩されない対策とは？

データ保護の最後の砦：「暗号化」

©2024 WiSECURE Inc. All rights reserved

USB HSMを活用したGoogle Workspace！

高度な安全性と管理主導権を企業に与える

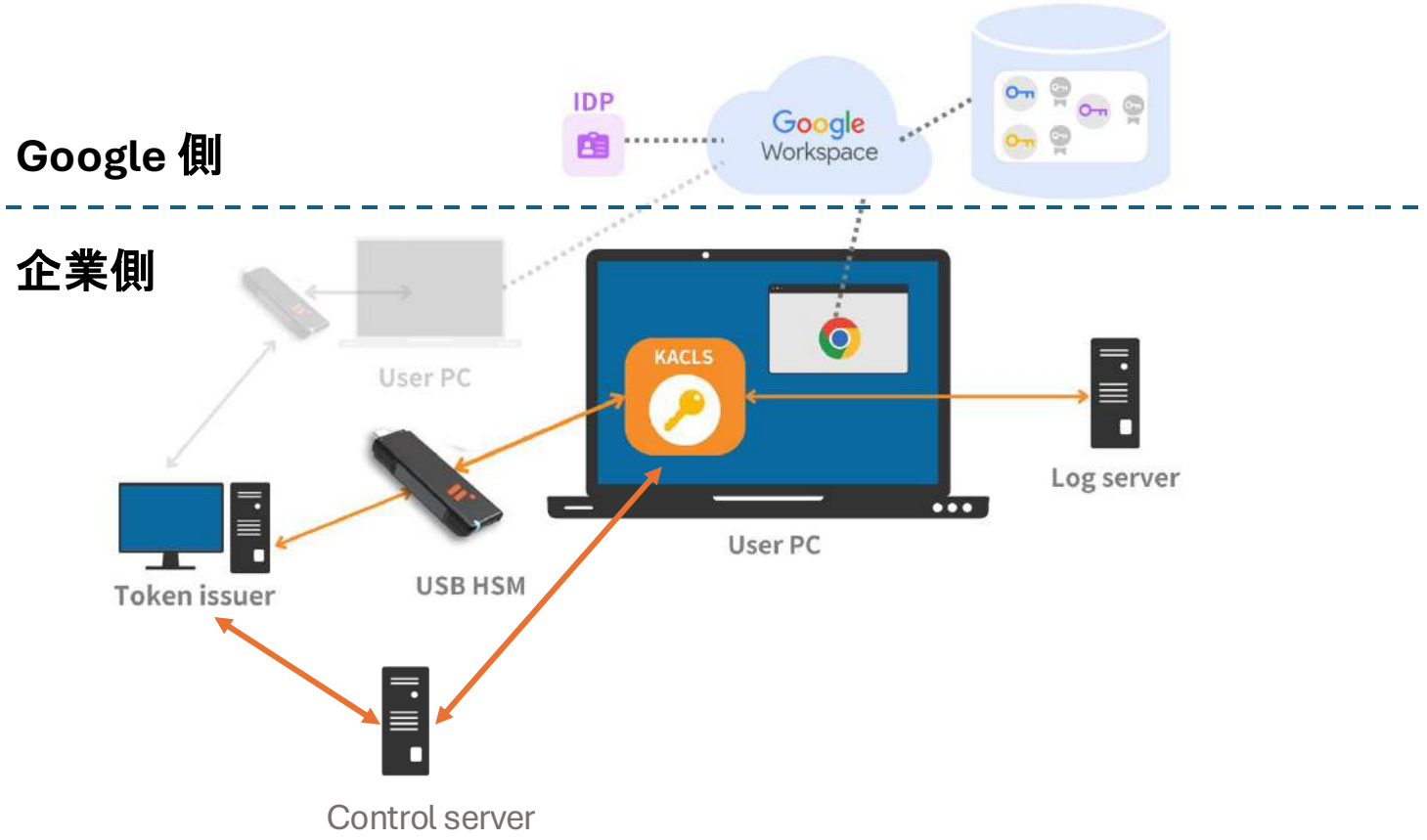
クライアントサイド暗号化（CSE）ソリューション

”データの読み取り権限は
ハードウェアの保有で確保！

©2024 WiSECURE Inc. All rights reserved

WiSECURE CSE（クライアントサイド暗号化）

暗号鍵を管理する主導権は企業に安全に返しました。



©2024 WiSECURE Inc. All rights reserved

3. 脱PPAP！USB セキュリティデバイス

USB HSM（Hardware Security Module）

多機能アーミーナイフのように、日常で活用するセキュリティツール

特徴

- PCファイル暗号化
- フィッシング耐性のある認証
- 暗号化メモリ
- 暗号鍵の保管庫
  （CCEAL5+チップ）

©2024 WiSECURE Inc. All rights reserved

SAMURAI Keyの多様な機能

標準化製品

カスタマイズ
ソリューション

ファイル暗号化と
ファイル共有

FIDO2 認証キー

内蔵された
暗号化ストレージ

セキュアブート

企業サーバー経由の
リモート管理

ソフトウェアの
ライセンス管理

©2024 WiSECURE Inc. All rights reserved

PGP暗号化USB：「脱PPAP」対策

USBがなければメールを傍受されても読みとれません。
解読用の鍵をこのUSBで安全に保管。
取引先からファイルを受け取りたい方にはおすすめ！

PPAPとは？

P
＝Password付きZIP暗号化
ファイルを送る

P
＝Passwordを送る

A
＝暗号化

P
＝プロトコル

※ PPAP廃止：政府は2020年11月にデジタル改革担当大臣がPPAPの利用をやめる方針を発表し、2022年1月4日からは文部科学省でもPPAPの廃止が発表されました。

©2024 WiSECURE Inc. All rights reserved