ZETA Alliance　TOPPAN

狙われる「IoTデバイス」へのセキュリティ対策

「セキュアアクティベートサービス®／セキュアエレメント Edge Safe®」

提供ソリューション　IoTデバイスの認証強化と運用効率化 「セキュアアクティベートサービス®」

- ✓ IoTデバイスの認証に、電子証明書を用いた「PKI（Public Key Infrastructure）認証」を採用
- ✓ IoTデバイスへのハードウェアセキュリティ導入と、その運用業務の安全性確保と効率化を支援

サービス① 電子証明書・認証鍵配信サービス： IoTデバイスの、電子証明書によるライフサイクルのリモート管理ASP

サービス② IoTデバイス向けSE(Edge Safe®)提供・発行サービス： IoTデバイスの認証情報保護に向けた、SEのプログラム開発・発行・提供

【運用フェーズ】
管理面での安全性・効率性確保

- IoTデバイスの証明書・鍵を「一元管理」
- IoTデバイスの証明書・鍵の「ライフサイクル」を管理
- IoTデバイスの証明書・鍵を「安全に配信・更新」

提供機能
- ID管理
- 認証鍵配信
- SE認証
- 認証鍵更新
- セキュア接続
- 認証鍵消去

【開発・製造フェーズ】
ハードウェア面のセキュリティ強化

- デバイス内の重要情報を保護する「セキュアストレージ・耐タンパー性」
- 「暗号演算をSE内部で実行」し、重要情報を外部に出さない処理
- SEの「セキュアなプログラミング」、「セキュアな環境での発行」

提供機能
- 正規プログラムの証明
- 各種設定、アップデート時の認証
- データの真正性の証明
- 動作制御の認証

「Edge Safe®」　トッパンのセキュアエレメントブランド。組込み・外付けのラインナップ

- ✓ IoTデバイスに搭載することで、重要情報を保護～セキュアな認証等を可能とするトッパンのセキュアエレメント製品
- ✓ IoTデバイスの用途に応じたICモジュールに、トッパンが適切なソフトウェアを搭載してご提供

基板組込みタイプ

幅広い用途に対応
Edge Safe®
EMB-GNシリーズ

車載用途に最適
Edge Safe®
EMB-AMシリーズ

※画像はイメージです

外付けタイプ

USBスロットを持つ機器向け
Edge Safe®
USBシリーズ

SIMカードスロットを持つ機器向け
Edge Safe®
SAMシリーズ


※画像はイメージです

CC認定における、評価保証レベル5+/6+のハードウェアを採用。（※CC認定＝ISO15408:Common Criteria認定）

技術検証ボード　「Edge Safe®」組込み拡張ボード。試作環境での実装・試作を容易に

- ✓ 本ボードを活用し、PoCや実証実験において簡単にIoTデバイスへのセキュリティを組み込み、実施することが可能
- ✓ 「Edge Safe®」への自由度の高いアプレット搭載や、SEとの通信・暗号ライブラリ提供によるOTAにも対応

Raspberry Pi向け拡張シールド

IoTゲートウェイなどのハイエンドデバイス向け


※画像はイメージです

ボード名		REB-02
対応機種		Raspberry Pi 3
SE提供機能	暗号機能	RSA (～2048bit) ESDSA AES (256bit) DES, Triple-DES
	ハッシュ機能	SHA-2
	生成機能	鍵生成(RSA, ESDSA, AES, DES) 真性乱数生成
通信インターフェース		I2C
ライブラリ仕様書		SEとの通信ライブラリ サンプルのセキュリティアプレットAPI OTAライブラリ（アプレットダウンロード、鍵配信）

Arduino向け拡張シールド

センサーデバイスなどのローエンドデバイス向け

※画像はイメージです

ボード名		AEB-01
対応機種		Arduino UNO R3
SE提供機能	暗号機能	RSA (～2048bit) ESDSA AES (256bit) DES, Triple-DES
	ハッシュ機能	SHA-2
	生成機能	鍵生成(RSA, ESDSA, AES, DES) 真性乱数生成
通信インターフェース		SPI
ライブラリ仕様書		SEとの通信ライブラリ サンプルのセキュリティアプレットAPI

凸版印刷株式会社

ZETA Alliance　TOPPAN

セキュアエレメントとは？　ICカードのセキュリティ技術を応用した、デバイスへ組込み可能なICチップ

✓ デバイス本体とは分離して、守るべき情報を堅牢に保護する機能をワンチップで実装可能

セキュアエレメント（SE）の特長

組込みセキュアエレメント（SE）

特徴❶：　セキュアストレージ/鍵管理

- 重要データや暗号鍵、認証鍵を安全に保存
- データを暗号化して保存、データの読み出しには認証と認可が必要。

特徴❷：　暗号演算

- 暗号鍵をSEから読み出すことなく、SE内部で暗号演算を行う
- 共通鍵、公開鍵、鍵生成、乱数生成、ハッシュ関数等を容易に実装可能。

特徴❸：　耐タンパー性

- 物理的・論理的アクセスによる解析、改ざん、偽造ICからIoTデバイスを保護。
- ICカードと同等の耐タンパー性を持つSEによって、IoTデバイスにICカード並のセキュリティをワンチップで実現

セキュリティ対策が脆弱なメモリなどに、
重要情報を保持するIoTデバイスの設計・運用はもはや危険

デバイス上の認証情報・処理の保護
＝認証の信頼性の確保

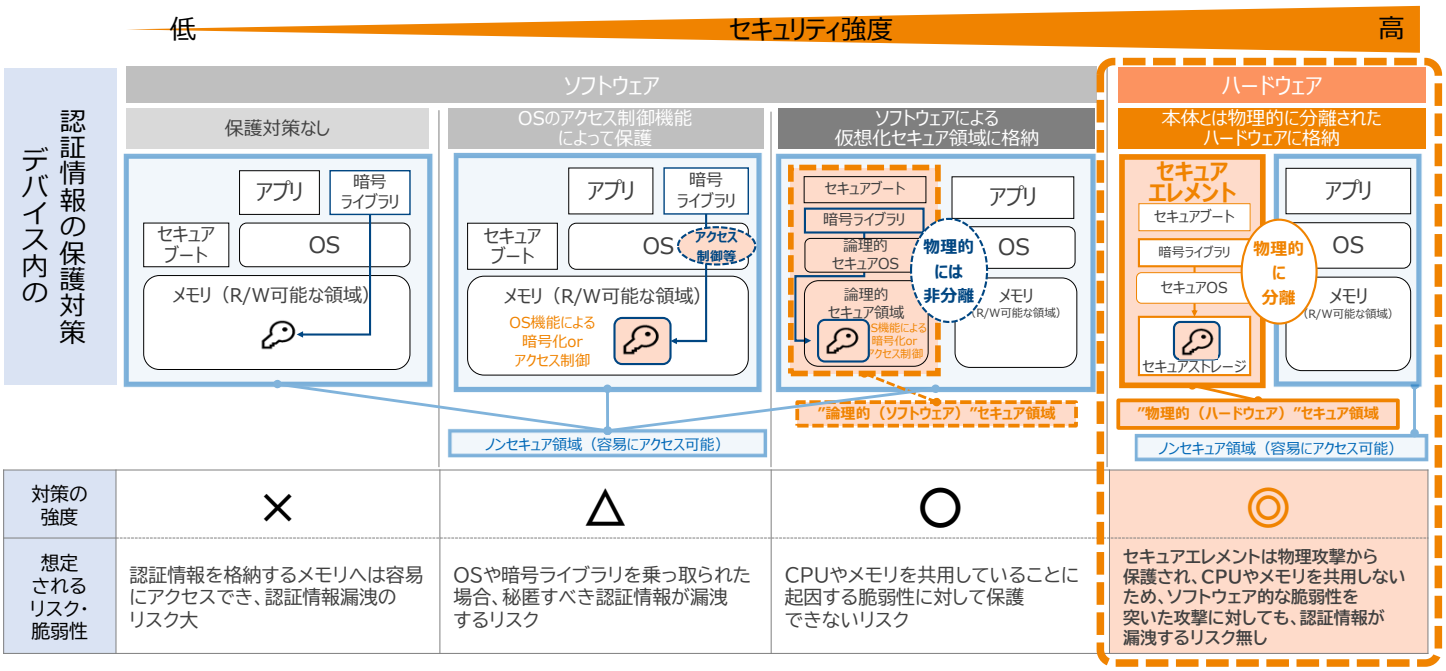
IoTデバイスの守るべき重要資産の保護に

- プログラム
- コンフィギュレーション
- データ
- 制御

・正規プログラムの証明
・各種設定、アップデート時の認証
・データの真正性の証明
・動作制御の認証

セキュアエレメントの有用性　IoTデバイス内での認証情報のセキュアな保持は、認証において「信頼の要」

✓ ソフトウェアや、論理的なセキュア領域を持つマイコン等のセキュリティと比較して、
「セキュアエレメント」がハードウェアとしてセキュリティを確保している点で、セキュリティ強度が高い



対策の強度	×	△	○	◎
想定されるリスク・脆弱性	認証情報を格納するメモリへは容易にアクセスでき、認証情報漏洩のリスク大	OSや暗号ライブラリを乗っ取られた場合、秘匿すべき認証情報が漏洩するリスク	CPUやメモリを共用していることに起因する脆弱性に対して保護できないリスク	セキュアエレメントは物理攻撃から保護され、CPUやメモリを共用しないため、ソフトウェア的な脆弱性を突いた攻撃に対しても、認証情報が漏洩するリスク無し

より詳細な資料もございます。
是非お気軽にお問い合わせください。

お問合せ先　secure-iot@toppan.co.jp

凸版印刷株式会社