セキュリティミドルウェア

expist® IoTA

「expist® IoTA」とは

あらゆるIoT機器に搭載可能な「IoT機器向けセキュリティミドルウェア」です。

セキュリティ課題

- 暗号化せず、平文のままデータを送ってしまっている (情報漏洩の課題)
- デバイスのHWスペックが低すぎてセキュリティ対策を講じることが難しい
- 鍵の管理や漏洩のリスク、長期運用による暗号危殆化のリスクを抱えている

「expist® IoTA」で解決

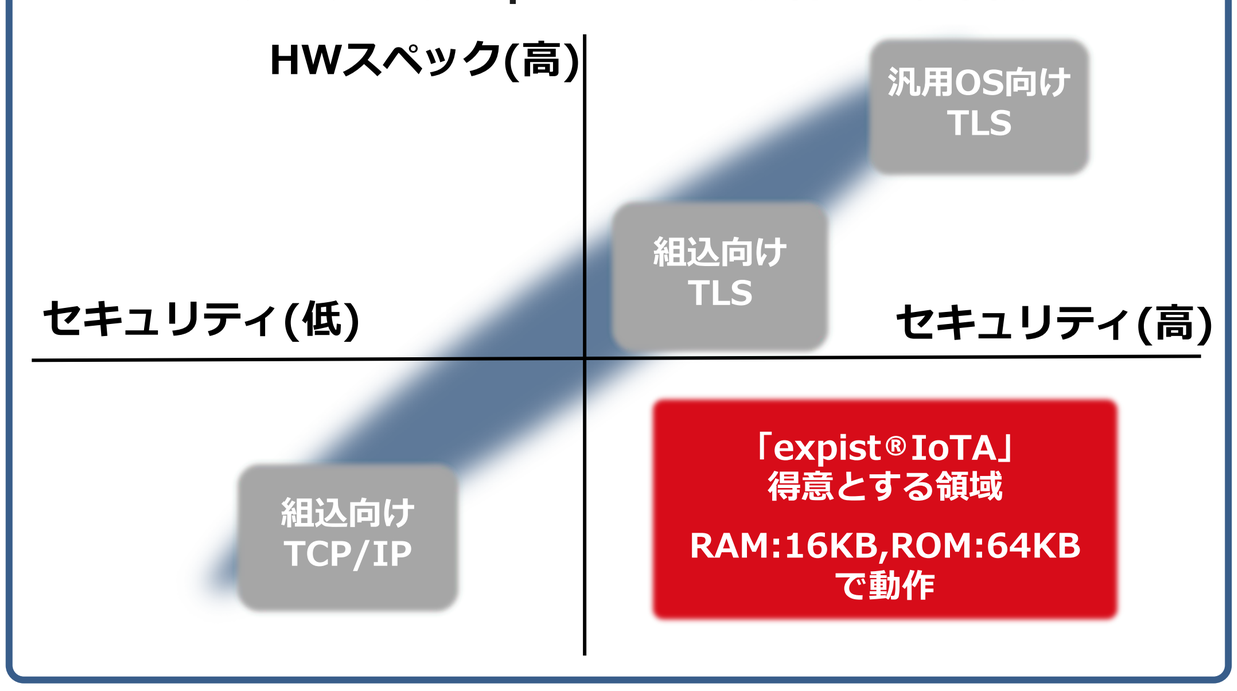
- 量子計算機による危殆化に対応出来ると期待される「256bit ブロック暗号機能」を導入
- 低スペックHWでも快適動作を実現
- 特許出願の秘密分散法と暗号機能の組み合わせで情報漏洩のリスクを排除

「expist® IoTA」特徴とHW領域

3つの特徴

軽量暗号 (SPECK)	IoT機器に適した暗号技術を実装
秘密分散法	強固な情報漏洩対策
低CPU上で動作	対象HWを選ばない

<HWスペックと expist® IoTA が得意とする領域>



HWを選ばず、データ漏洩しても完全性が無い限りデータの復元ができない

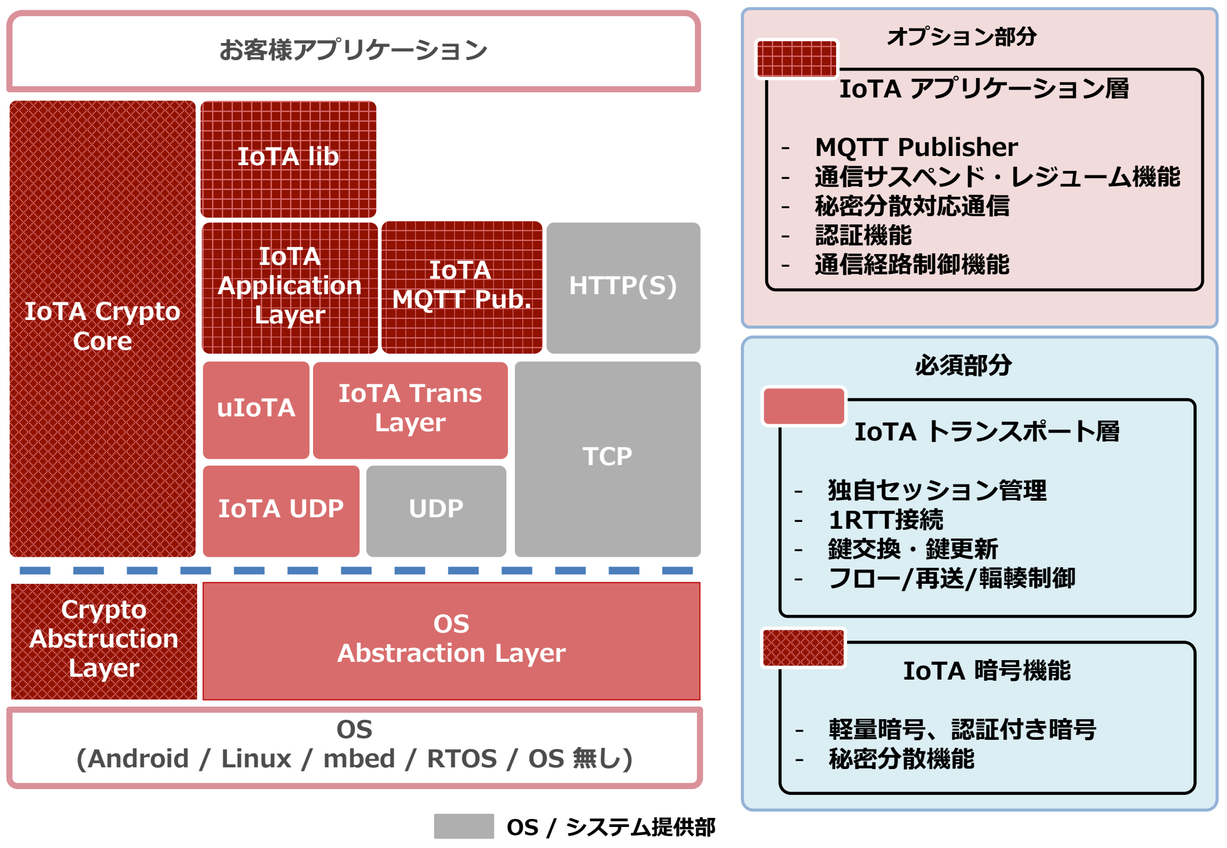
「expist® IoTA」機能とモジュール構成

機　能

- UDP上で動作する独自プロトコル
- 軽量暗号サポート
- AONT による秘匿性向上

- 通信レジューム
- マルチセッションmTCP対応
- MQTT サポート
- パケット全体の暗号化

- Rust によるセキュア実装
- ISO 26262, ISO21434 対応(予定)



IoT × セキュリティ

その IoT ソリューションを、よりセキュアに

エイチアイが開発した expist® IoTA と ZETA を組み合わせることで

高信頼な IoT システム構築が可能です。

IoT 機器で よくある セキュリティ課題

- ✓ 暗号化せず、平文のままデータを送ってしまっている
- ✓ デバイスの HW スペックが低すぎて、セキュリティ対策を講じることが難しい
- ✓ 平文のデータが第三者のサーバに置かれるので漏洩リスクを気にしている
- ✓ 鍵の管理や漏洩のリスク、長期運用による暗号危殆化のリスクを抱えている

そのお困りごとを
expist® IoTA で解決できます！

IoTA とは

「セキュアに」「確実に」「効率的に」届けることをコンセプトとした、セキュア通信ミドルウェアです。

低スペックなシングルボードコンピュータに対して通信とセキュリティを導入

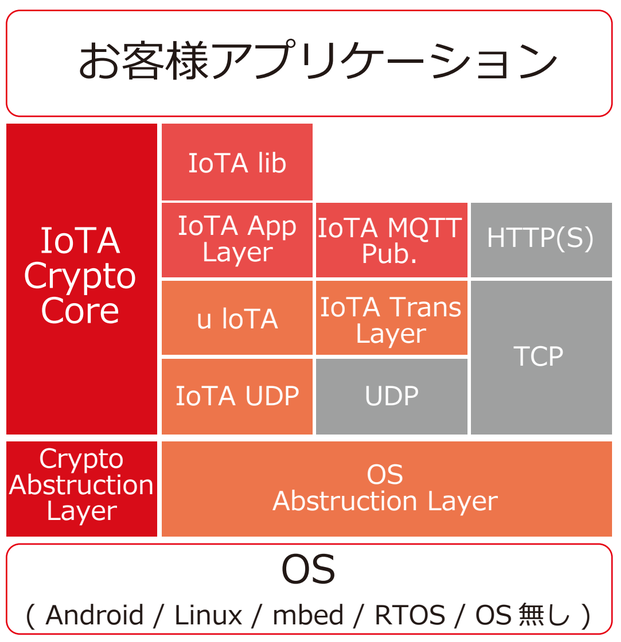
LPWA 通信を意識した軽量設計 暗号アルゴリズムを実装

通信オーバーヘッドの削減により少ない帯域を有効活用

①導入目的別に expist® IoTA と expist® IoTA mini の２モデルを用意

②お客様の要望に応じたカスタム対応が可能

expist® IoTA ミドルウェア構成



IoTA 暗号機能
- 軽量暗号、認証付き暗号
- 秘密分散機能

IoTA アプリケーション層
- MQTT Publisher
- 通信サスペンド・レジューム機能
- 秘密分散対応通信
- 認証機能
- 通信経路制御機能

IoTA トランスポート層
- 独自セッション管理
- １RTT 接続
- 鍵交換・鍵交換
- フロー / 再送 / 輻輳制御

... OS / システム提供部

expist® IoTA + ZETA

expist® IoTA の導入にハードウェアの追加は必要ありません。
expist® IoTA を組み込むことで現在運用されているシステムをよりセキュアに、信頼性を高めることが可能です。
また、LPC1768 を始めとする低スペックなボードにおける動作実績が豊富です。

LPC1768

ZETA 評価キット

HI CORPORATION