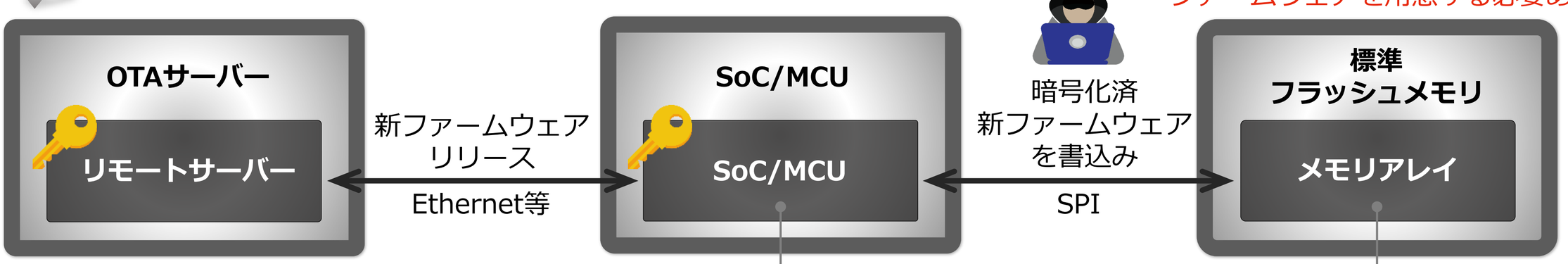
winbond

開発労力とコストを低減

IoT機器へのセキュアOver-the-Air実装に貢献する
W77Qセキュアフラッシュメモリの利用例

ファームウェアの更新

現在の方法



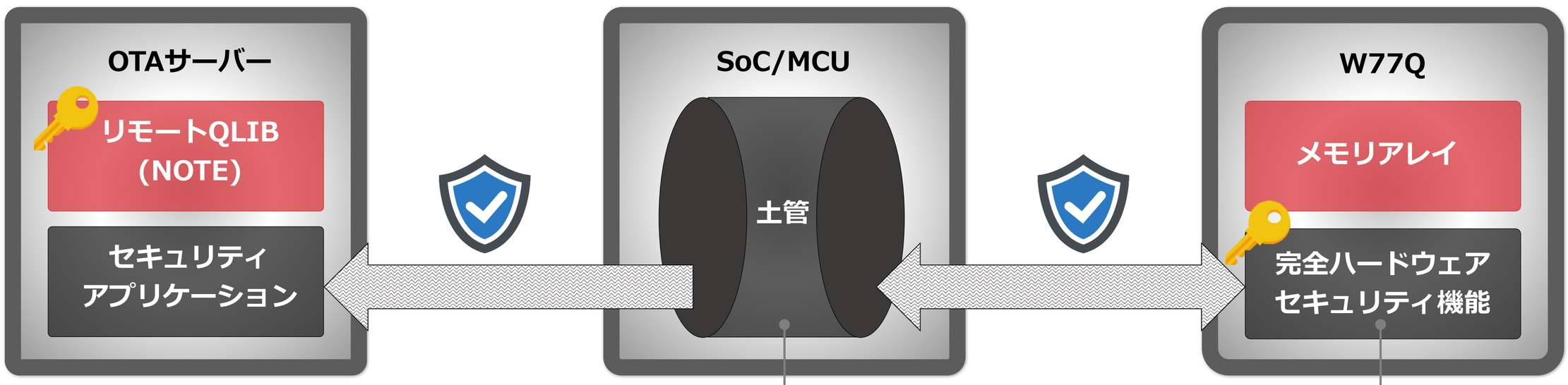
第一に事前に暗号化
ファームウェアを用意する必要あり

・ファームウェア検証のためのソフトウェアの作り込み、セキュリティホールは？
・ハードウェアとソフトウェアの機能を使ってファームウェアを検証、SoC/MCUのオーバー ヘッド処理が増加

・メモリ単体への強制書込みなど改竄・破壊が可能
（例：サプライチェーン攻撃）

新提案（True End-to-End セキュリティチャネル）

完全ハードウェアによるセキュリティ機能は高いセキュリティ強度を発揮します。
ロールバックは、過去のファームウェア更新の情報を悪用し、正当なバージョンアップを妨げる攻撃です。



(NOTE)
QLIB:はウィンボンドが提供する
Cソースコードのライブラリ

・上位通信からのペイロードを抽出してバイパスするのみ

・ファームウェアの検証をハードウェアで自動実行、アンチロールバックにも対応、書込みや読出し保護機能でソフトウェア資産を保護

その他 提供できるセキュリティ機能

	セキュリティ機能	W77Qの処理	SoC/MCUの処理
1	自己正真性保護＆セーフフォールバック（ファームウェアレジリエンス）	パワーオンリセット後から実行するブートコードの正真性をW77Q内蔵のハードウェアロジックが自動検証します。ブートコードに異常があった場合、自動的に冗長なブートコードから実行します。	ブートコードの検証は不要です。既存のブートコードを通常通りメモリからフェッチ・実行してください。
2	プラットフォームレジリエンス	SoC/MCUのレスポンスをリモートサーバーのような第三者のホストと連携評価し、ハッキングの可能性があった際にはSoC/MCUをクリーンリセットします。	SoC/MCU側でセキュリティ機能は不要です。リモートサーバーとW77Q間のコマンドレスポンスをブリッジしてください。この通信パスで異常が発生した場合、W77QがSoC/MCUをクリーンリセットします。
3	デバイス構成認証(例：Chain-of-Trustのチェック)	ハードウェアとソフトウェアのユニーク性からRoTE(Root-of-Trust Engine)を使って認証子を自動生成します（TCG/DICEライク）。	SoC/MCU側でセキュリティ機能は不要です。リモートサーバーとW77Q間のコマンドレスポンスをブリッジしてください。
4	セキュアデータストレージ	W77Qでは選択したメモリのセクションをセキュアストレージに設定できます。SPIバス上のペイロードは暗号化されサインされます。鍵を知らないハッカーは内容の読出しや書換はできません。	SoC/MCU側でQLIBを搭載すれば、セキュアストレージにアクセスできます。必要なセキュリティ機能はQLIBがは行うので開発労力は軽減されます。

ウィンボンド・エレクトロニクス株式会社 | 045-478-1883 | mkt.online_jp@winbond.com