winbond

TrustME®

セキュアフラッシュメモリ-W77Q

標準SPIフラッシュメモリの置換え “Drop-In Replacement”から始める セキュアフラッシュメモリ - IoTセキュリティに革新を

Overview 概要

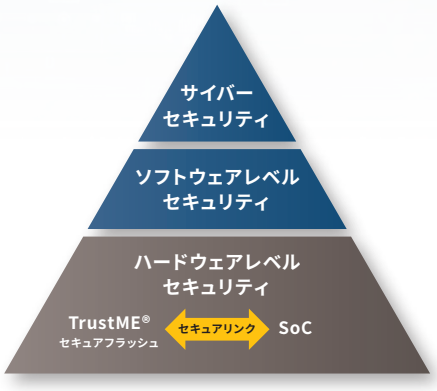
実装の信頼性と拡張性を提供するセキュアフラッシュメモリ

ハードウェアセキュリティは堅牢なサイバーセキュリティの基盤となります。
セキュアストレージはハードウェアセキュリティの中核となります。

Features 主な特長

W77Qは既存のSPI NORフラッシュメモリ W25Qファミリを継承

- ●標準SPIフラッシュメモリを完全置換え可能 (Drop-In Replacement)
- ●PCB基板やMPUの再設計不要
- ●コスト重視のプラットフォームに最適



斬新なセキュリティ機能を搭載

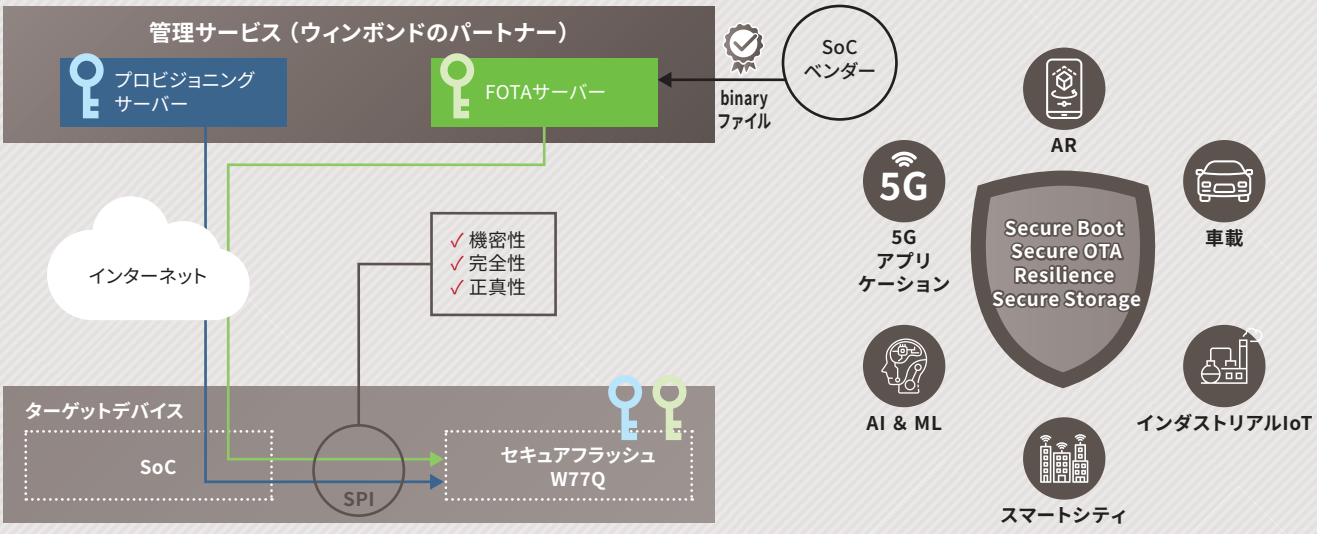
- ●Root of Trust とセキュアブート
- ●セキュアOTA※ ファームウェアアップデート
- ●レジリエンシー(保護、検知、回復)
- ●セキュアデータストレージ
- ●CPUを用いないピュアなワイヤードロジックアーキテクチャー

第三者機関による認定メモリ＝信頼を約束するソリューション!

- ●外部ラボにおける検証と評価　●CC EAL2+, SESIPレベル2

※ OTA：Over-The-Air

ウィンボンド セキュアフラッシュメモリ(W77Q)による “End-to-End” セキュリティアプリケーション例



柔軟かつ幅広いメモリセキュリティ機能セット

W77Q TrustME®セキュアシリアルフラッシュメモリは、小パッケージで低消費電力を要求されるシステムにセキュアストレージを追加します。そのセキュリティレベルは、コモンクライテリア（Common Criteria）EAL2 セキュリティ認定要件を満たします。

W77Qは標準シリアルNORフラッシュメモリを完全置換え可能なメモリになっており、これまでのNORフラッシュメモリと同じように使いつつ、さらに柔軟かつ高性能なセキュリティ機能を利用できます。すなわち、従来と同じeXecute In Place（XIP）によってコードフェッチ可能なセキュアコードストレージであり、またセキュアな鍵管理システムによってセキュアデータストレージにもなります。

W77Qは洗練された暗号学的な通信チャネル（SoCとW77Q間、あるいはサーバーとW77Q間）を構築し、ユニーク鍵に紐づくデバイス個体認証、暗号学的なフラッシュメモリへのライトロック、データ正真性検証機能、セキュアファームウェアOver-The- Air（OTA）更新、Root-of-Trust（RoT）機能, セキュアリード・ライト・イレース動作機能を持っています。

W77QシリーズのSPIは、Single, Dual および Quad モード、QPIモード動作（命令発行時からQuadモードを有効化）をサポートし、SPIクロック周波数は最大 133MHzまで、また Dual Transfer Rate（DTR）時は最大66MHzまでサポートします。

サイバーセキュリティベストプラクティスを想定

- ●コモンクライテリア（CC）EAL2+に準拠
- ●IoTデバイスのためのセキュアRoot-of-Trust(RoT)
- ●高速セキュアブート
- ●セキュアコード&データストレージ
- ●アンチロールバック攻撃
  高速ファームウェアスワップ機能
- ●セキュアファームウェア
  Over-The-Air（OTA）更新
- ●ローカルおよびリモートでのセキュアチャネル構築
  （認証、暗号化、アンチリプレイ攻撃）
- ●ファームウェア正真性保護
- ●オンチップデータハッシュで
  高速コード認証処理
- ●認証ウォッチドッグタイマーによる
  プラットフォームレジリエンシー
- ●セキュアユニークデバイスID
- ●暗号学的セキュアライト保護
- ●セキュアな鍵プロビジョニングとストレージ
- ●リプレイ保護モノトニックカウンター

標準SPI NORフラッシュメモリを完全置換（Drop-In Replacement）

- ●業界最高速セキュアシリアルフラッシュメモリ
  - ✓ Execute In Place（XIP）
  - ✓ 133MHz SPI Single/Dual/Quad/QPI
  - ✓ 66MHz Dual Transfer Rate（DTR）Mode
  - ✓ 1ブロック当たり10万回のイレース・ライトサイクル
  - ✓ 20年のデータリテンション
- ●リード・ライトアクセス制御
- ●Continuousリードとバーストリードモード
  (4KB境界で自動ラップアップ)
- ●柔軟な4Kバイト単位のメモリ管理
  - ✓ 4Kバイト単位のイレースブロック
  - ✓ ページプログラムモード(1コマンド当たり256バイトまで)
  - ✓イレースプログラムSuspend & Resume
- ●ローパワー、1.8V or 3.3Vシングル電源動作
- ●広温度範囲動作
  - ✓-40°C ～ +105°C（産業グレードプラス）
- ●パッケージ:SOP8/SOP16、WSON 8、TFBGA 24
- ●Known Good Die（KGD）をウェハーで提供

お問い合わせ先
ウィンボンド・エレクトロニクス株式会社 横浜市港北区新横浜2-3-12 新横浜スクエアビル9階
TEL:045-478-1883 URL:www.winbond.com e-mail:mkt_online.jp@winbond.com
2023年7月現在