アマゾン FreeRTOS を 使用した RISC-V 無線IoT システムでの 遠隔ソフトウエア更新（OTA = Over-the-Air）と ハードウエア ルートオブトラスト（RoT = Root of Trust）統合デモ

2021年11月17日
SHコンサルティング株式会社（SHC）

概要

このデモンストレーションでは、32ビットRISC-Vが、オープンソースのリアルタイム オペレーティング システム である FreeRTOSと、ハードウェアルートオブトラスト（RoT = Root of Trust）を使い、安全に、IoTのソフトウエアを無線（OTA=Over-the-Air）アップデートする機能を見せます。IoTは、RISC-V RTOSを使用しており、アマゾン ウエブ サービス（AWS）IoTコア サービスをWiFi経由で使用しOTAを実行します。

IoTデバイスを社会実装する際、IoTサービスプロバイダーは、メッセージングゲートウェイと通信するIoTデバイスのアイデンティティを確認する必要があります。IoTデバイスの電源を初めて入れた際、ハードウェア信頼基点（RoT）が、ネットワーク トラフィックの認証と暗号化に使用されるIoTデバイスに固有の鍵ペアを生成します。この鍵ペアはハードウェア ルートオブトラスト（RoT）内部で生成されるため、外部プログラムからプライベート鍵を取得しようとする企てを防御することができます。

ハードウェアの信頼のルートとセキュアブートの機能に加えて、ハードウェア ルートオブトラスト（RoT）は、ハードウェアのk鍵の格納場所としても使われます。秘密鍵はハードウェアによって保護されており、ソフトウェアによる鍵の保護よりもはるかに優れた保護機能を提供します。システム集積としては、ハードウェアルートオブトラスト（RoT）へのインターフェイスとしてPKCS＃11プロトコルを利用します。

本デモでは、ハードウエアルートオブトラストが、鍵ペアを生成した後、RISC-V SoCがFreeRTOS MQTTライブラリとOTAエージェントを利用してAWSクラウドに接続し、OTAソフトウエア遠隔更新を実行し新ソフトウエアに入れ替えます。

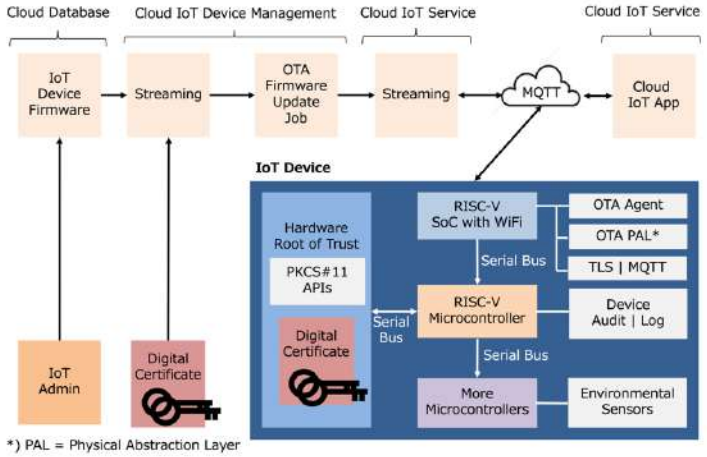

図1：RISC-V で構成される AWS IoT コアデバイス と クラウド の 全体図

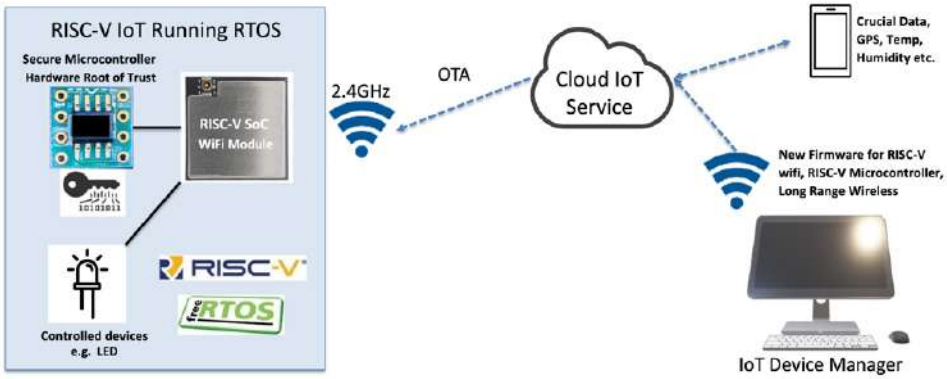

図2：RISC-V OTA および RoTデモ の セットアップ

今回のデモでは、RISC-Vプロセッサによる OTA機能の初期段階を示しています。 さらに複雑なシステムを対象とした、複数のプロセッサのソフトウエア対して安全にOTAを実行しシステム全体のソフトウエア更新を行うことを次のステップと考えています。

無線による（Over-the-Air＝OTA）ソフトウエアの遠隔更新

無線による（OTA）ソフトウエア遠隔更新では、ユーザーはソフトウエアをIoTデバイスに対し物理的に介入せずに新ソフトウエアを遠隔地から更新し、更新完了後、デバイスを自動的に運用再開します。新ソフトウエアのセットはデジタル署名されており、IoTシステムはファイルを受信した際に、署名を確認します。 プログラマーがOTAアップデートを作成し、IoTデバイスの管理者は、OTA アップデート マネージャ サービスを使い、AWSIoTジョブを作成して、アップデートが利用可能であることをデバイスに通知します。 OTAデモアプリケーションは、AWS IoTジョブの通知トピックにサブスクライブし、遠隔更新メッセージをリッスンするデバイス上のFreeRTOS中のタスクを使い実行されます。 クラウドサービス側から、アップデートが利用可能になると、OTAエージェントはAWS IoT Coreにリクエストを公開し、HTTPまたはMQTTプロトコルを使用してアップデートを受信します。 SHCデモでは、MQTTプロトコルが使用されます。 OTAエージェントは、ダウンロードされたファイルのデジタル署名をチェックし、ファイルが有効と判断した場合は、ソフトウエアアップデートをインストールします。 ソフトウエアの遠隔更新が完了すると、ボードは自動的にリセットされ、新しいソフトウエアによるサービスが開始されます。

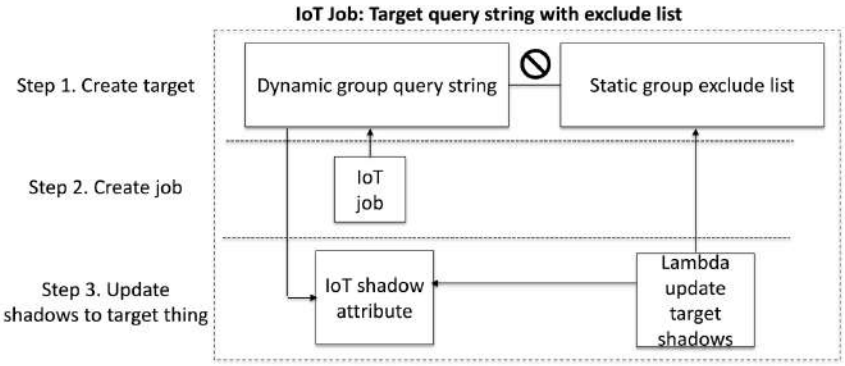

図3：AWSクラウドサービスにおける　OTA　ソフトウエア遠隔更新ステップ

RISC-VによるOTAソフトウエア遠隔更新の性能測定

クラウド接続はWi-Fi接続された、160KHzで動作するRISC-Vは、QPIフラッシュを80MHzで動作させます。MQTTを介して277ファイルブロックに分割された、1,135,872バイトのRISC-Vソフトウエアイメージを遠隔更新しました。イメージの転送に2分23秒（143秒）かかりました。 1秒あたり8Kバイト程度転送された計算になります。 。

必要なメモリ容量

商用ハードウエアルートオブトラスト（RoT）チップとRISC-Vを使用してAWS IoT Coreに安全に接続するには、（219.5KB + アプリケーションプログラムのサイズ）より大きいフラッシュメモリと、32.87KBより大きいランダムアクセスメモリ（RAM）が必要です。 ハードウェアルートオブトラスト（RoT）とRISC-Vを使用した（OTA）遠隔ソフトウエア更新の場合、（251.36KB +ソフトウエアのサイズ）を超える容量を持つフラッシュメモリと、最小36.07KBのRAMが必要です。 500KB以上のフラッシュメモリが理論的には必要ですが。 自信を持ってOTAソフトウエアアップデートソリューションを実装するには、1MB以上のフラッシュメモリが必要であると考えます。

MARMOT ＝　マルウェア、改竄、物理攻撃に対抗する　マイクロコントローラ　アーキテクチャ

図５は、開発されたMarmot WirelessIoTシステムを示します。 Marmot（**Marmot = M**icrocontroller **A**rchitecture to **R**esist **M**alware, **O**bstructions, and **T**ampering）は、（1）高速応答時間、（2）低メンテナンス、（3）高信頼性、（4）高セキュリティを提供することを意図として設計されたRTOS IoTシステムです。マルウエア、改竄、物理攻撃に対抗する機能を備えています。

図4：マーモット (MARMOT) エンブレム

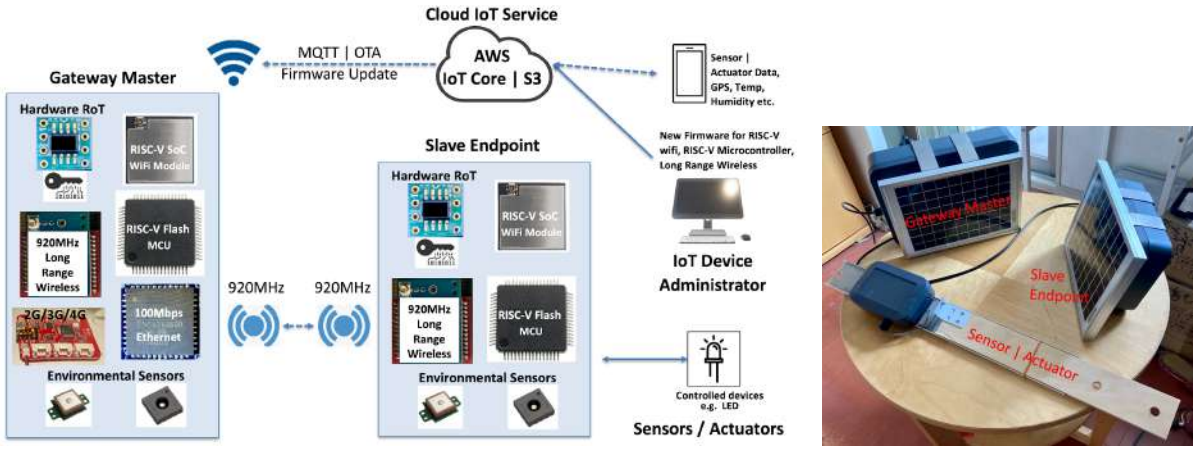

図5：マーモット 無線 IoT システム例

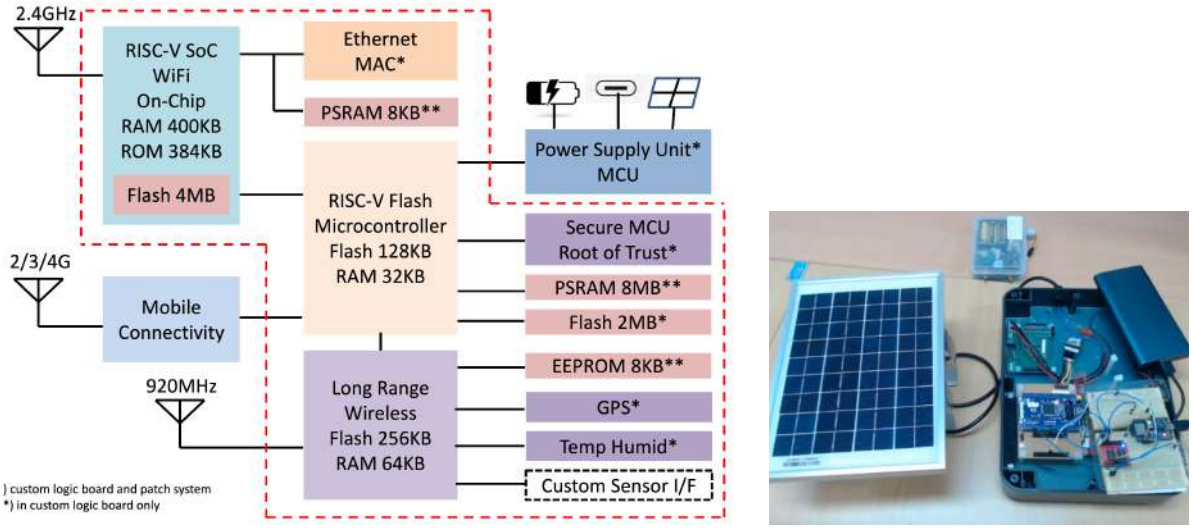

図6：マーモット システム の ブロック図（左）と デモに使用するパッチボード（右）

RISC-V システムオンチップ（SoC）の 仕様

RISC-V SoCは、Wi-FiとBluetooth Phyを備えており、AmazonFreeRTOSに認定されたRISC-Vプラットフォームの1つです。 SoCには、160MHzで動作する32ビットRISC-Vシングルコアプロセッサ、4MB外部フラッシュ、384KBのROMおよび400KBのSRAM、GPIO、I2C、PWM、SPI、およびUARTが付属しています。 さらにワイヤレス機能を備えています：（1）IEEE 11 b / g / n準拠、（2）最大150Mbpsのデータレートの1T1Rモード、（3）MPDUおよびA-MSDUアグリゲーション、（4）4μsガードインターバル、（4）2,412MHz～2,484MHzの動作周波数

ハードウェア信頼基点 または ハードウエア ルートオブトラスト（RoT）チップ の 仕様

ハードウェア信頼基点（RoT）またはハードウェアルートオブトラスト（RoT）は、IoTエンドポイントデバイスのセキュリティに対する、物理的な改ざんやサイドチャネル攻撃に対する対策を提供します。ハードウェアの信頼のルート（RoT）は、IoTエンドポイントがデバイスIDを確立するために使用される秘密鍵を保護し、なりすましやその他の悪意のあるアクティビティのためにプライベートデータがデバイスから取り出されるのを防ぎます。

私たちが使用した特定のハードウェアルートオブトラスト（RoT）チップは、複数の秘密鍵とそれに関連する公開鍵および証明書を安全に保存するように設計されています。デバイスの内部でランダムな秘密鍵の生成をサポートし、デバイスの外部で秘密鍵が認識されないようにします。保存された秘密鍵に対応する公開鍵は、鍵が生成されるときに常に返され、オプションで後で計算される場合があります。内部乱数ジェネレーターは、NIST 800-90A、800-90B、および800-90Cのドキュメントに記載されている要件を満たすように設計されています。これらの乱数は、デバイスの暗号化プロトコルの一部として使用するために使用できます。

各乱数は、このデバイスまたは他のデバイスでこれまでに生成されたすべての番号から本質的に一意であることが保証されているため、暗号化プロトコルの計算に含めることで、リプレイ攻撃（つまり、以前に成功したトランザクションの再送信）が常に失敗します。以下にその詳細仕様を示します。

安全なハードウェアベースのキーストレージを備えた暗号化コプロセッサ：
–最大16個のキー、証明書、またはデータ用の保護されたストレージ
非対称署名、検証、鍵共有のハードウェアサポート：
– ECDSA：FIPS186-3楕円曲線デジタル署名
– ECDH：FIPSSP800-56A楕円曲線ディフィーヘルマン
–NIST標準P256楕円曲線のサポート
対称アルゴリズムのハードウェアサポート：
–オフチップコンテキストの保存/復元を含むSHA-256およびHMACハッシュ
– AES-128：暗号化/復号化、GCMのガロア体乗算
ネットワーキングキー管理サポート：
– TLS1.2および1.3のターンキーPRF / HKDF計算
–SRAMでの一時的なキー生成とキー合意
–キーが完全に保護された小さなメッセージの暗号化
セキュアブートのサポート：
– ECDSAコード署名検証、オプションの保存されたダイジェスト/署名
–セキュアブート前のオプションの通信キーの無効化
–オンボード攻撃を防ぐためのメッセージの暗号化/認証
各種機能
– 内部高品質NISTSP 800-90A / B / C乱数ジェネレーター（RNG）
– 2つの高耐久性単調カウンター
– 保証された固有の72ビットシリアル番号

クラウドIoTサービス（Amazon IoT Core）

AWS IoT Coreは、接続されたデバイスがクラウドアプリケーションや他のデバイスと対話できるようにするマネージドクラウドサービスです。 AWS IoT Coreはデバイスとメッセージをサポートし、それらのメッセージを処理してAWSエンドポイントと他のデバイスにルーティングします。 AWS IoT Coreを使用すると、アプリケーションは、OTAまたはメッセージのプッシュのために、すべてのデバイスを常に追跡して通信できます。

謝辞 その他

この開発は、新エネルギー・産業技術総合開発機構（NEDO）から委託されたプロジェクトJPNP16007から得られた結果に基づいています。 マーモットシステムの特許および商標権を申請中です。

SHコンサルティンググループについて

SHコンサルティンググループ（SHC）には、ベトナム、および日本のエンジニアがいて、RTOS、デバイスドライバー、およびH8、SH、ARM、RISC-VなどのMCUのワイヤレス接続の安定性を提供することを専門としています。　長年にわたり、MCU用のQNX、.NETMF、Linux、WindowsなどのOSと、Lora、WiFi、Bluetoothなどのワイヤレスソリューションを統合してきました。　彼らはWindows、Android、iOSプラットフォームで動作しました。 近年、SHCエンジニアは、大手半導体企業向けにARMおよびRISC-VのFreeRTOSを開発しました。

Software Hardware & Consulting LLC（米国）
1325A Church Street, San Francisco, CA 94114-3900 USA

SHコンサルティング株式会社 （日本）
東京本社：東京都中央区銀座7-18-13-502 郵便番号 104-0061
電話番号：03-3833-3717
東京デザインセンター：東京都東大和市芋窪2丁目2038番13-02号　郵便番号　203-0033
www.swhwc.com

SH CONSULTING VIETNAM COMPANY LTD. (VIETNAM)
(Local Name: CÔNG TY TNHH SH CONSULTING VIỆT NAM)
Quang Trung Software Park, Tan Chanh Hiep Ward, District 12 Ho Chi Minh City
Phone: 84-8-3715-0060