

アンデス N25 RISC-V AWS IoT Core へ マイクロチップ RoT を集積するデモ
FreeRTOS と Amazon IoT Core を搭載した Andes RISC-V SoC

2020 年 10 月 31 日

SH コンサルティング グループ

デモンストレーション紹介

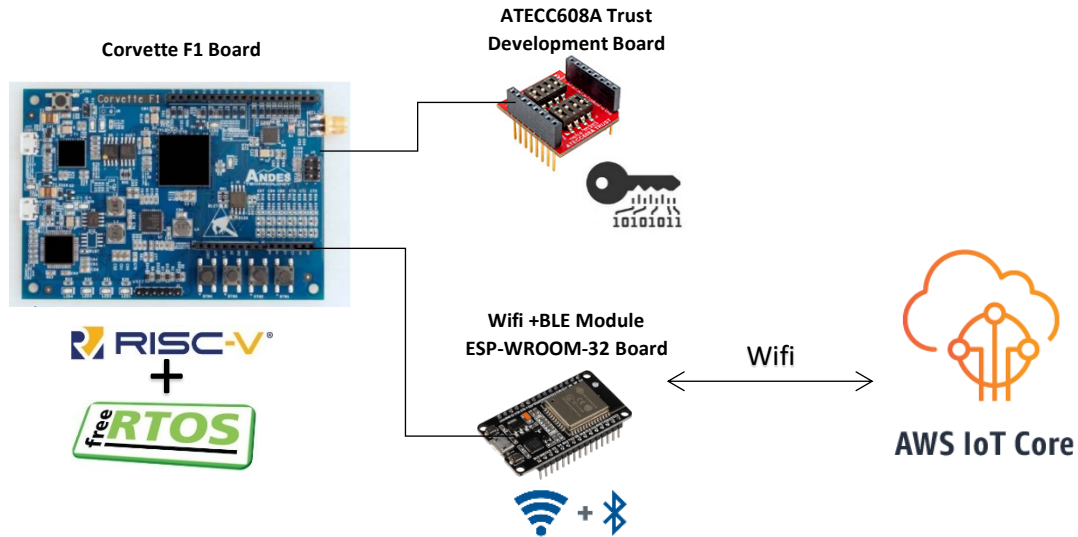


図 1 : AmazonFreeRTOS のデモを使用した CorvetteF1 ボードを中心とした AWS IoT コアシステム

このデモンストレーションは、Corvette-F1 ボードを使用したセキュアな IoT ソリューション、32 ビットの AndesCoreN25 と AndeShapeAE250 プラットフォームを完全にサポートする評価キットを示し、Amazon WebServices のマイクロコントローラー用のオープンソースオペレーティングシステムである AmazonFreeRTOS を実行します (AWS)。ESP32-WROOM ボードを外部 Wi-Fi モジュールとして使用します。ATECC608A-TFLXTLS チップは、トラステッドプラットフォームモジュール (TPM) などに統合されており、ハードウェアベースのエンドポイントデバイスセキュリティを提供します。この統合により、デバイス ID の確立に使用される秘密鍵を改ざん防止ハードウェアデバイスに安全に保存して、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デバイスから秘密鍵が取り出されるのを防ぐことができます。

IoT ソリューションの展開では、メッセージングゲートウェイと通信しているデバイスの ID を確認することが重要です。初めてデモを実行すると、TPM はデバイスのキーペアを生成し、トラフィックの認証と暗号化に使用されます。キーは TPM 自体の内部で生成されるため、外部プログラムによる取得から保護されます。実際、ハードウェアの信頼のルートとセキュアブートの機能を利用しなくても、TPM はハードウェアのキーストアとしても価値があります。秘密鍵はハードウェアによって保護されており、ソフトウェア鍵よりもはるかに優れた保護を提供します。この統合では、TPM へのインターフェイスとして PKCS # 11 プロトコルを使用します。

キーペアを生成した後、このデモでは FreeRTOSMQTT ライブラリを使用して AWS Cloud に接続し、AWS IoT MQTT ブローカーによってホストされている MQTT トピックにメッセージを定期的に公開します

Corvette F1 ボード特長



利点を活用できます。

ますます多くのテクノロジーがインターネットに導入されるにつれて、IoT 市場は多種多様なアプリケーションで成長しています。RISC-V 命令セットアーキテクチャ (ISA) は、柔軟性、拡張性、スケーラビリティを強化し、IoT の新しい可能性を生み出し、この成長する市場を活用するためのコンパクトな IoT ハードウェアの設計を容易にします。Andes Technology は、RISC-V プラットフォームを Amazon FreeRTOS、AWS IoT Greengrass、AWS IoT Core などのソリューションと組み合わせることで、開発者が包括的で競争力のある RISC-V ベースの IoT システムを作成できるよう支援します。

Corvette-F1 N25 プラットフォームは、AmazonFreeRTOS に認定された最初の RISC-V プラットフォームの 1 つです。Corvette-F1 N25 プラットフォームは、FPGA ベースの Arduino 互換の評価プラットフォームです。60MHz で動作する 32 ビット RISC-V AndesCore™N25、4MB フラッシュ、256KB 命令 SRAM および 128KB データ SRAM、および GPIO、I2C、PWM、SPI、および UART。ユーザーは、Arduino 標準 IDE とフル機能の AndeSight™IDE で IoT デバイスのプロトタイプとアプリケーションを簡単に構築できます。

ATECC608A チップ特長

- 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 : FIPSP800-56A 楕円曲線ディフィーヘルマン
 - NIST 標準 P256 楕円曲線サポート
- 対称暗号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：
 - 完全な 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

- 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
- 保証された一意の 72 ビットシリアル番号
- 利用可能な 2 つのインターフェイスオプション：
 - 1 つの GPIO ピンを備えた高速シングルピンインターフェイス
 - 1MHz 標準 I2C インターフェース
- 1.8V ~ 5.5V IO レベル、2.0V ~ 5.5V 供給電圧
- <150nA スリープ電流
- 8 パッド UDFN および 8 リードパッケージ

アプリケーション

• ネットワーク/IoT ノードエンドポイントセキュリティ

ノード ID 認証とセッションキーの作成と管理を管理します。 TLS 1.2 (およびそれ以前) および TLS1.3 を含む複数のプロトコルのエフェメラルセッションキー生成フロー全体をサポートします

• セキュアブート

コードダイジェストを検証し、オプションで成功時に通信キーを有効にすることで、MCU ホストをサポートします。パフォーマンスを向上させるためのさまざまな構成が利用可能です。

• スモールメッセージ暗号化

PII 情報などの小さなメッセージやデータを暗号化および/または復号化するためのハードウェア AES エンジン。 AES-ECB モードを直接サポートします。他のモードは、ホストマイクロコントローラーの助けを借りて実装することができます。 AES-GCM をサポートするための追加の GFM 計算機能。

• ソフトウェアダウンロードのキー生成

ダウンロードした画像のローカル保護キー生成をサポートします。それぞれが同じ復号化キーを持つ多くのシステムへの1つのイメージのブロードキャスト、またはシステムごとの一意のイメージのポイントツーポイントダウンロードの両方がサポートされています。

• エコシステム制御と偽造防止

システムまたはコンポーネントが本物であり、銘板に示されている OEM からのものであることを検証します。

暗号化操作

ATECC608A は、楕円曲線暗号と ECDSA 署名プロトコルに基づく完全な非対称 (公開/秘密) 鍵暗号署名ソリューションを実装します。このデバイスは、NIST 標準 P256 ブライムカーブのハードウェアアクセラレーションを備えており、高品質の秘密鍵生成から ECDSA 署名生成、ECDH 鍵合意、および ECDSA 公開鍵署名検証までの完全な鍵ライフサイクルをサポートします。

このデバイスは、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。ランダムな秘密鍵の生成はデバイスの内部でサポートされており、秘密鍵がデバイスの外部で認識されないようになっています。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。

ATECC608A 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た、内部乱数ジェネレーターを使用して高品質の乱数を生成できます。

これらの乱数は、デバイスの暗号プロトコルの一部としての使用を含む、あらゆる目的に使用できます。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、プロトコル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。

マイクロチップのトラストプラットフォームによるルートオブトラスト

IoT の時代では、ハードウェアベースのセキュリティは、物理的な攻撃やリモート抽出から秘密鍵を保護する唯一の方法です。ただし、各デバイスを構成およびプロビジョニングするには、セキュリティに関する幅広い専門知識、開発時間、およびコストが必要です。Microchip は、CryptoAuthentication ファミリ用に Microchip の Trust Platform と呼ばれる主要なセキュリティサービスを開発しました。これは、小規模または大規模の OEM がハードウェアデバイスに安全な認証を実装するための簡単な方法を提供します。このサービスは、デバイスキーを製造するための安全なシステムと、カスタム部品番号を生成するためのサプライチェーンを提供します。

ATECC608A のセキュアエレメントに基づいて、トラストプラットフォームは、すぐに使用できる事前プロビジョニングから完全にカスタマイズ可能なものまで、ユーザーのニーズを満たすために 3 つの層で利用できます。ATECC608A は、コモンライテリアジョイントインタープリテーションライブラリの (JIL) の「高」評価のセキュアキーストレージを提供し、デバイスが業界で実証済みのセキュリティプラクティスと最高レベルのセキュアキース

ストレージを実装していることをお客様に確信させます。ハードウェアベースの信頼のルートストレージと暗号化対策は、既知の物理的攻撃の最も幅広いクラスからデバイスを保護します。

3つの製品は、Trust&GO、TrustFLEX、および TrustCUSTOM です。

•マスマーケット向けの Trust&GO (TNGTLS) は、ゼロタッチの事前プロビジョニングされた安全な要素を、最小注文可能数量 (MOQ) が 10 ユニットという低さで提供します。デバイスの資格情報は、自動クラウドまたは LoRaWAN 認証のオンボーディングのために、事前にプログラムされ、出荷され、ATECC608A 内でロックされます。

•TrustFLEX (TFLXTLS) は、事前構成されたユースケースの恩恵を受けながら、顧客の認証局を使用する柔軟性を提供します。これらのユースケースには、任意の証明書チェーンを使用して任意の IP ベースのネットワークに接続するためのトランスポート層セキュリティ (TLS) 強化認証、LoRaWAN 認証、セキュアブート、無線 (OTA) 更新、IP 保護、ユーザーなどのベースラインセキュリティ対策が含まれます。データ保護、およびキーローテーション。

•TrustCUSTOM (TCSTM) は完全なカスタマイズを可能にし、顧客固有の構成機能とカスタム資格情報のプロビジョニングを提供します。

Microchip は AmazonWeb Services (AWS) と連携して、Microchip TrustPlatform のすべてのバリエーションで設計された製品の AWSIoT サービスへの簡単に簡素化されたオンボードプロセスを可能にしました。ATECC608A セキュアエレメントは、任意のマイクロコントローラおよびマイクロプロセッサと組み合わせることができます。

Amazon IoT コア特長

デバイスをクラウドに簡単かつ安全に接続します。数十億のデバイスと数兆のメッセージに確実に拡張できます。

AWS IoT Core とは何ですか？

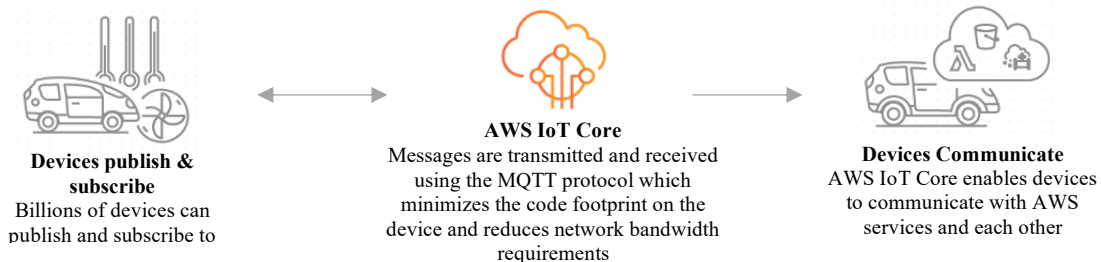
AWS IoT Core は、接続されたデバイスがクラウドアプリケーションや他のデバイスと簡単かつ安全に対話できるようにするマネージドクラウドサービスです。AWS IoT Core は、数十億のデバイスと数兆のメッセージをサポートし、それらのメッセージを処理して AWS エンドポイントや他のデバイスに確実かつ安全にルーティングできます。AWS IoT Core を使用すると、アプリケーションは、接続されていない場合でも、すべてのデバイスを常に追跡して通信できます。

AWS IoT Core を使用すると、AWS Lambda、Amazon Kinesis、Amazon S3、Amazon SageMaker、Amazon DynamoDB、Amazon CloudWatch、AWS CloudTrail、Amazon QuickSight、Alexa Voice Service などの AWS および Amazon サービスを簡単に使用して、収集、処理する IoT アプリケーションを構築できます。、インフラストラクチャを管理することなく、接続されたデバイスによって生成されたデータを分析して処理します。

AWS IoT Core はどのように機能しますか？

デバイスを接続して管理する

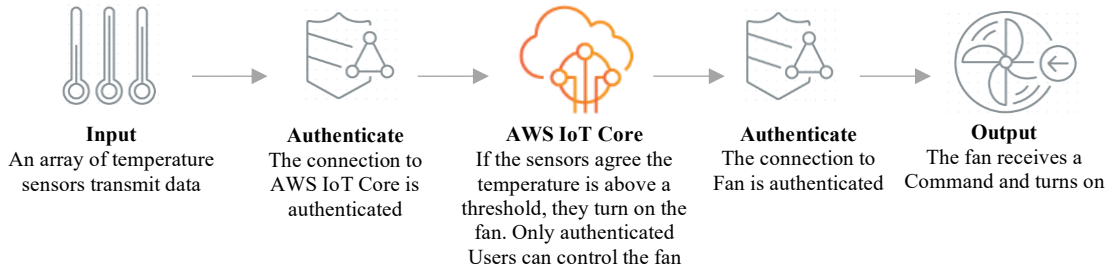
AWS IoT Core を使用すると、任意の数のデバイスをクラウドや他のデバイスに簡単に接続できます。



安全なデバイス接続とデータ

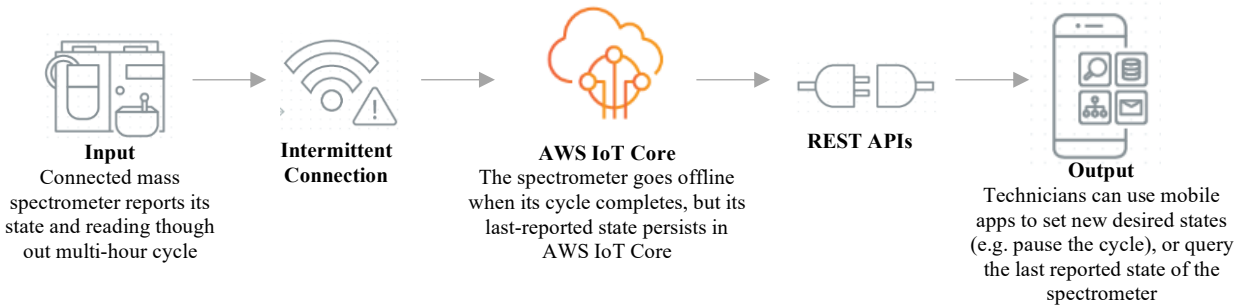
AWS IoT Core は、デバイスが AWS IoT Core に最初に接続したときに自動構成と認証を提供し、すべての接続ポイントでエンドツーエンドの暗号化を提供するため、証明された ID がないとデバイスと AWS IoTCore の間でデー

タが交換されることはありません。さらに、きめ細かい権限を持つポリシーを適用することで、デバイスやアプリケーションへのアクセスを保護できます。



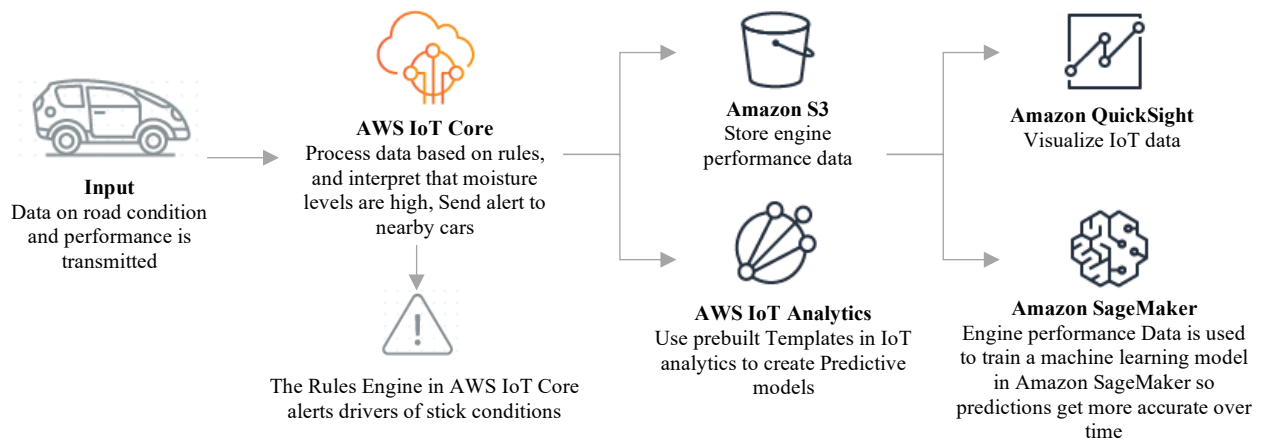
いつでもデバイスの状態を読み取って状態を設定できます

AWS IoT Core は、接続されたデバイスの最新の状態を保存して、いつでも読み取りまたは設定できるようにします。これにより、デバイスは常にオンラインであるかのようにアプリケーションに表示されます。



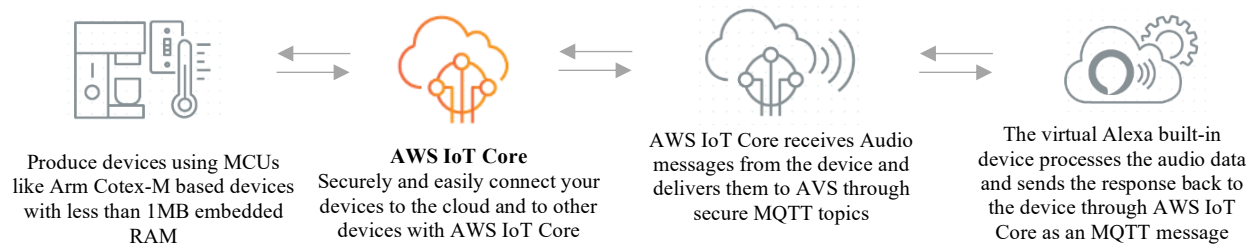
デバイスデータを処理して処理する

AWS IoT Core を使用すると、定義したビジネスルールに基づいて、デバイスデータをオンザフライでフィルタリング、変換、処理できます。



費用対効果の高い方法で数億の Alexa ビルトインデバイスに拡張

AWS IoTCore の AlexaVoice Service (AVS) 統合により、クラウドに新しい仮想 Alexa ビルトインデバイスが導入されます。これにより、お客様は、予約済みの MQTT トピックを介してオーディオメッセージを送受信し、デバイスのマイクとスピーカーとインターフェイスし、同じ安全な IoTCore 接続を使用しながらデバイス側の状態を管理できます。



SH コンサルティンググループ紹介

SH コンサルティンググループ (SHC) には、米国、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、および H8、SH、ARM、RISC-V などの MCU のワイヤレス接続に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 ARM プラットフォーム上の大規模な半導体企業向けに FreeRTOS をエネーブリングした後、FreeRTOS の取り組みを RISC-V に向けています。

SH コンサルティング株式会社

- 東京本社

〒104-0061 東京都中央区銀座 7 丁目 18 番 13-502 号 TEL: 03-3833-3717

- 東京国分寺設計センタ

〒185-0021 国分寺市南町 3 丁目 23-12 山元ビル 5 階

SH CONSULTING K.K.

Tokyo Head Office: 7-18-13-502 ginza, Chuo-ku, Tokyo, Japan 104-0061

Phone: 03-3833-3717

Tokyo Design Center: Yamamoto Building 5F, 3-23-12 Minami-cho, Kokubunji-shi, Tokyo 185-0021, Japan

SH CONSULTING VIETNAM COMPANY LTD.

(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

SOFTWARE HARDWARE & CONSULTING LLC

San Francisco Bay Area USA:

Software Hardware & Consulting LLC

1325A Church St, San Francisco, CA 94114-3900

Phone: (408) 510-8221