

マイコン・ファームウェアは ネットで更新! OTA機能を試す

古城 隆

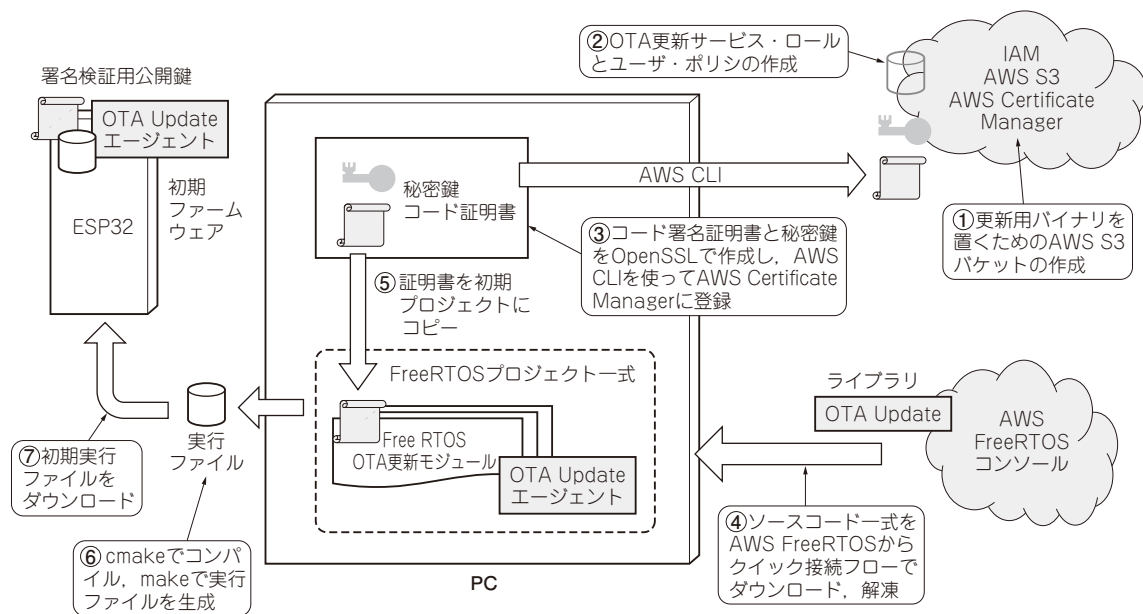


図1 OTA対応の初期バージョンのファームウェアを準備するフロー
OTA用ライブラリ、秘密鍵、証明書を加えたFreeRTOSを構成する

● IoTデバイスは遠隔でファームウェア更新もできる

実際のIoTデバイスは、長期間使われることが多く、運用中にファームウェアの更新が必要になる場合があります。

広い範囲に分散して設置されるデバイスは、ネットワーク経由による遠隔アップデートを可能にしておくことも重要ですが、相手の見えないネットワーク経由の更新を安全に行うためのセキュリティも重要です。このような要求に応えるのがOTA (Over The Air) によるファームウェア更新です。

本稿では、AWS IoTで提供されているファームウェア更新機能について解説します。

● 便利な仕組みだけど…セキュリティが超重要!

ファームウェアの更新をする上で通信視点で重要なのは、ネットワークを越えて安全に更新イメージを届けることと、届いたイメージが正しいものであるかを検証することの2つです。ネットワーク上で安全に通信するためには、TLS (Transport Layer Security) の上で動くMQTT (Message Queuing Telemetry Transport) プロトコルを使います。他人にファームウェア・イメージを盗まれないようにするとともに、TLSのデバイス認証によって届け先のデバイスがなりすましなど偽物ではないことを保証します。

ファームウェア・イメージの検証を確実にするために、AWS IoTのOTAでは公開鍵署名を使います。本稿では主に、公開鍵署名がAWS IoTのOTAでどのように使われているか解説します。