ライブラリを使うだけの人でも知っておきたい

IoTマイコン×クラウド通信のセキュリティ基礎知識

短期連載 第1回 ネットワークに潜むわな

廣垣 匡紀

● はじめに…連載で体験すること

IoT端末がクラウドに接続する際に，その通信を堅牢にしたいのなら暗号化は欠かすことができません．

暗号化には「対称鍵暗号」と「公開鍵暗号」の2つがあります．前者はある鍵によって元データを理解できないデータへ変換する（またはその逆の変換を行う）と考えると理解しやすいです．一方，後者では，暗号化に使った鍵を用いても暗号化されたデータを復号できません．復号には対になる別の鍵を使用します．この性質によって公開鍵暗号は単なる暗号化だけではなく，データが改ざんされていないかといったことを確かめることにも利用できます．

今日，安全にインターネット上のサービスを利用できるのは，このような技術の恩恵に他ならないです．しかし，公開鍵基盤（PKI）やTLSといった関連する技術を学ばないと，公開鍵暗号の良さを理解することは難しいです．そこで本稿では，あえてPKIやTLSは削ってしまい（＝公開鍵暗号を使わず），理解しやすい対称鍵暗号を使って，公開鍵暗号を真似した基礎的な仕組みを作ってみます．これにより公開鍵暗号の良さを理解したら，PKIやTLSを学び，本物の公開鍵暗号の良さを体感してほしいです．

きっかけ

● クラウド・サーバにデータを保存する記事が散見される

本誌には，Arduinoやラズベリー・パイ，ESP32などのマイコンで取得したデータを，クラウド基盤上に保存する記事がたくさんあります．

皆さんはどのような方法で実現するでしょうか．例えば，1日分のセンサ・データをCSVファイルにまとめて，その日の終わりにクラウド・ストレージ（Googleドライブなど）にアップロードするという方法があります．より洗練された手法としては，MQTTを用いて，外部のサーバへ送信するという方法もあるでしょう．

● 個人で使えるクラウド・サービスが多数ある

今日，IoTデバイス向けにさまざまなクラウド・サービスが提供されています．センサのデータをクラウドに保存する目的であれば，これらを使用することが最良でしょう．クラウド・サービスと言っても，趣味の範囲からエンタープライズ用途まで，さまざまな種類があります．例えば，Ambient[注1]やBlynk[注2]は，設定やグラフ化が容易であり，趣味の範囲でよく利用されています．ただし，簡素であるが故に複雑な処理（複数のセンサの値を参照し，条件を満たしていれば制御機器に何らかの指示を出すなど）の実装には苦労するかもしれません．

一方でAzure IoT Hub[注3]やAWS IoT Core[注4]は，エンタープライズ用途でよく使われています．複雑な処理も自在に実装できますが，幾つかのサービスを組み合わせて利用することが前提であるため，専門的な知識がなければ扱いづらいかもしれません．

クラウド・サービスとは異なりますが，自宅サーバやVPSなどにNode-RED[注5]を導入し，オリジナルのシステムを一から構築するという方法もあります．

● セキュリティを気にしましょう

手法の選定に関し，気にすべきことがもう1つあります．それはセキュリティ対策です．十分な対策がなされていなければ，IoTデバイスが生成するデータ（単なる数値や動画ファイルなど，多岐にわたる）が不特定多数に公開されることになり得ます．家電などをクラウド基盤上で制御しているのであれば，第三者に制御を乗っ取られるかもしれません．

注1：https://ambidata.io/
注2：https://www.blynk.cc/
注3：https://azure.microsoft.com/ja-jp/services/iot-hub/
注4：https://aws.amazon.com/jp/iot-core/
注5：https://nodered.jp/