第1章 設計時に検討すべき事項から定番AESの実装まで

IoTシステムにおける暗号技術

足立 英治

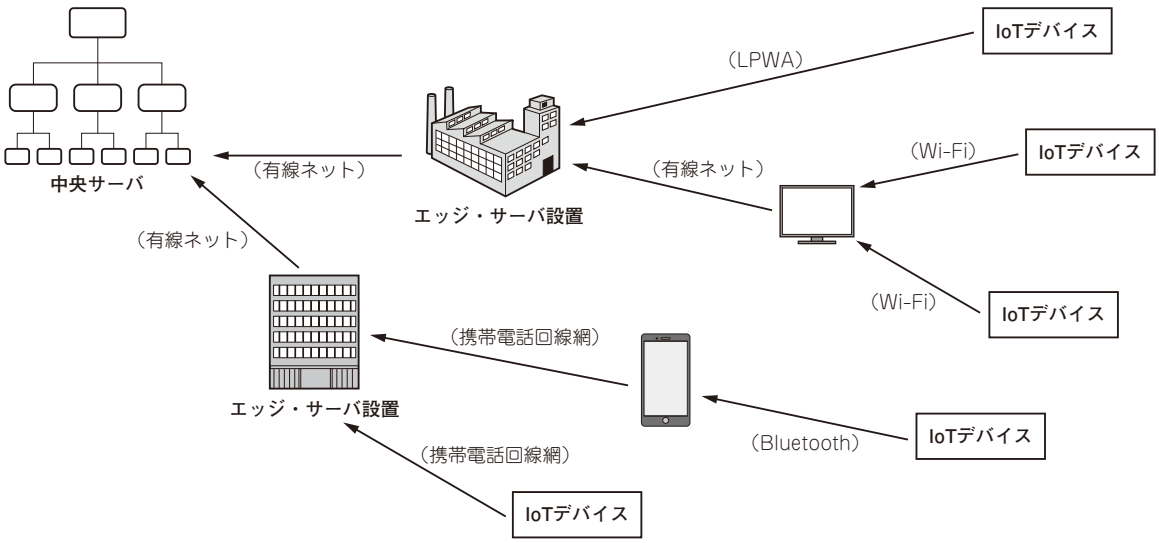

図1 IoTシステムは多様なネットワークの階層構造になっている

本稿では，特にIoT（Internet of Things）機器のセキュリティに注目します．暗号実装の際に検討すべきことを解説し，ブロック暗号のAESの実装，およびそれを用いた暗号利用モードの実装を行います．本稿はIoT機器に焦点をあてているため，C言語のソースコードで解説します．Pythonコードも本誌サポート・ページからダウンロードできます．あわせてご覧ください．

● IoTの利便性とセキュリティをどう両立させるかが問題

IoTはあらゆるものをネットワークに接続して，あらゆる事象をディジタル化して利用する考え方です．一般家庭，企業，工場，農場，交通網など，単純にネットワークにつながるだけではなく，あらゆるものが相互に接続されることにより利便性は拡大します．その反面，セキュリティ・リスクもそれだけ高くなっています．

例えば，屋外からの家電操作やスマート・ロックの開閉などに対する不正操作やアクセス・ログの盗聴，ヘルスケア機器やスマート・ウォッチなどのデータ盗難や改ざんなど，ネットワークにつながる利便性はリスクの裏返しになります．さらに，これらの機器は常に動作を監視しているわけではないので，ハッキングを受けても気付きにくく被害を避けにくいものです．また，あらゆるものがネットワークでつながっているので，1つの障害や攻撃が与える影響も広大なものになる可能性も考える必要があります．

このような攻撃からデータを守る技術の1つに暗号があります．身近なところでは，PCやスマートフォンでインターネットを利用するとき，ブラウザからの通信は常時SSL化によってほとんどが暗号化されます．

IoTシステムのセキュリティを考えるときのポイント

● 構成が複雑

IoTでは，**図1**のようにシステムの構成は多段階で複雑です．末端のデバイスと中央のサーバに間では通信は何段階にも分割されることもあり，個々の通信経路を暗号化するだけでは，エンド・ツー・エンドのセ