第1章 通信情報の秘匿性／改ざん検知／通信相手の認証など

ネットワーク上に潜む脅威から通信を守るセキュリティ・プロトコル

古城 隆

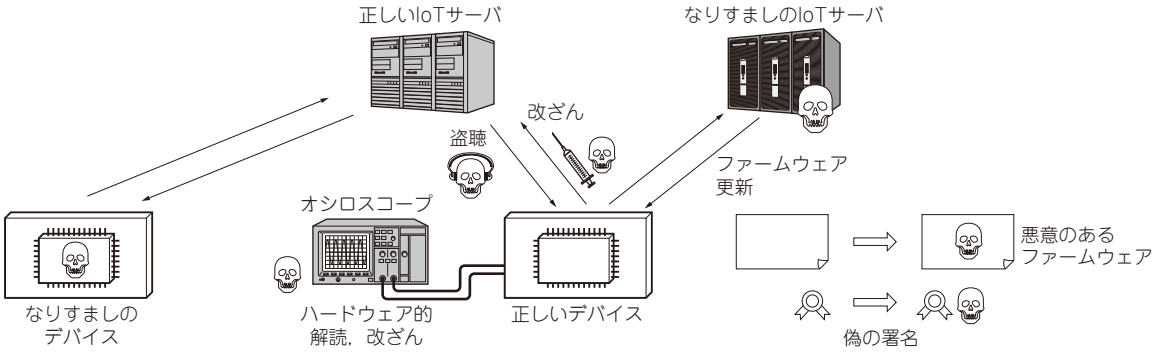

図1 IoTシステムはさまざまな脅威にさらされている
セキュリティの観点で見たIoTサーバとデバイスの関係

● IoTに潜むセキュリティの脅威

最近では，多くのIoT（Internet of Things）デバイスがクラウド・サーバにつながって，さまざまなシステムが運用されるようになってきました．

IoTの世界でもセキュリティの重要性が認識されるようになってきています．IoTは情報システムの1つです．そのためセキュリティに関しては，従来の情報システムと重なる部分も多くありますが，IoT特有の問題もあります．

▶その通信相手…正しいですか？

図1に示すのは，セキュリティの観点で見たIoTサーバとデバイスの関係です．重要なのは，正しいサーバとデバイス間で通信することです．多くのIoTシステムの場合，パブリックなネットワークを介してデバイス-サーバ間の通信が行われます．その間には盗聴や改ざんなど，どんな攻撃者が潜んでいるか分かりません．

相手の見えないネットワーク越しの通信なので，誤ってなりすましのサーバに接続するかもしれません．サーバ側から見ると，逆になりすましのデバイスが悪意のあるデータを送りつけてくるかもしれません．

▶なりすましデバイスから攻撃を受ける可能性も

実際，個々の小さなIoTデバイスには盗まれて困るような情報がなかったり，なりすましデバイスがサーバにアクセスしても追加の料金が発生するわけではなかったりします．そのため，デバイス側にはあまりセキュリティの必要性が感じられないかもしれません．

しかし，デバイスを相手にするサーバの立場だとそうはいきません．セキュリティ・レベルの低いプロトコルで送られてきたデータが改ざんされた情報だったり，なりすましデバイスから送られてきた偽情報だったりすると，システムがかく乱されてしまうかもしれません．サーバ側は，パブリックなインターネットで世界中からアクセスを許す状態で，常にセキュリティ上の強い脅威にさらされています．セキュリティ・プロトコルを使わないデバイスからのアクセスを許すわけにはいきません．

● 脅威から通信を守る「セキュリティ・プロトコル」

前述のリスクからシステムを守るために，サーバ-デバイス間の通信にはセキュリティ・プロトコルを使う必要があります．セキュリティ・プロトコルの目的は次の3つにまとめられます（**図2**）．

(1) 通信情報の秘匿性
通信内容を暗号化することで，悪意を持った第三者に情報を盗まれないようにする

(2) 通信情報の改ざん検知
受け取ったメッセージが改ざんされたものでないこと，送信された内容そのものであることを保証する