ご購入はこちら

第2章 使いこなせばクラウド上のさまざまなサービスや機能にアクセスできる

インターネット界の標準セキュリティ・プロトコル「TLS」

古城 隆

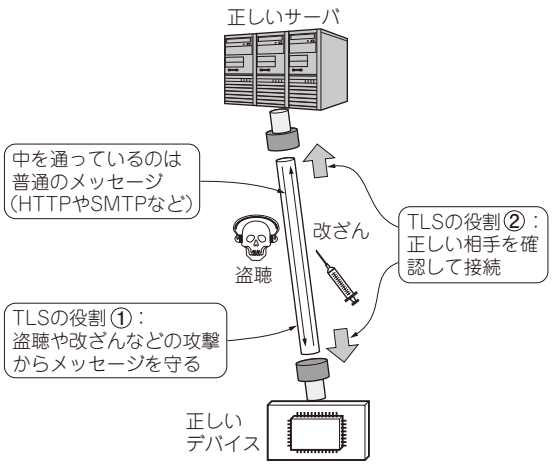

図1　セキュリティ・プロトコル「TLS」の役割
なりすまし/盗聴/改ざんの脅威から通信メッセージを守る

● 多くのプロトコルに採用されている

インターネットの世界では，幸いにもセキュリティ・プロトコルが標準化されています．非常に多くのプロトコルがある中で，セキュリティの部分にはTLS（Transport Layer Security）という共通のセキュリティ・プロトコルが採用されています（**図1**）．

TLSの有名な採用例の1つに，HTTPSがあります．ウェブ・サーバは，セキュリティなしの場合，TCP（Transmission Control Protocol）の上のHTTP（Hypertext Transfer Protocol）で通信しています．HTTPにセキュリティを追加したものがHTTPSです．このHTTPSですが，実はTCPの上にセキュリティ・プロトコルTLSを乗せ，その上でHTTPによる通信をするものです．

同じようにメール・サーバで使われるSMTP（Simple Mail Transfer Protocol）にセキュリティを追加するSMTP/SやStartTLSも，TLSを利用したものです．

● 使いこなすメリット

HTTPは当初，ウェブ・サーバとブラウザのためのプロトコルとして開発され，広く利用されてきました．最近ではウェブ・サービスという形でデータ・ストレージ，データベース，AI，地図，自然言語や翻訳といったさまざまな分野のサービス機能をクラウド上で提供するために使われています．こうしたウェブ・サービスの提供する機能をIoTに取り込むことで，従来では考えられなかったような高機能システムを簡単に実現できます．

TLSを使いこなせるようになると，ネットワーク上のさまざまなサービス，機能にアクセスできるようになって，実現できるIoTの世界も格段に広がっていきます．

TLSの役割①…盗聴や改ざんからメッセージを守る「暗号化」

● TLSの暗号化により守られる部分

IP層の上でTLSを実現するためには，TCP層の助けが必要です．IPパケットは世界中に送り届けられますが，パケットが時々ロストしたり，重複して受信したり，順番が入れ替わって届いたりする可能性があり，不安定な通信となるためです．TCP層は，ロストしたと思われるときは再送を要求したり，届いたパケットをバッファリングして順序を正しく入れ替えたりすることで，通信の不安定さを取り除きます．

ネットワークには，他の多くのノードのパケットも行き交っているので，混雑でパケットが詰まらないための制御（輻輳制御）もします．

TLSは，**図2**のようにTCP上で安定したメッセージのやりとりができる状態でセキュリティの実現に専念します．ここでのセキュリティとは，第1章でも紹介した(1)通信情報の秘匿性，(2)通信情報の改ざん検知，(3)通信相手の認証の3つです．

● 実際に暗号化された様子を見てみる

TCPだけで通信しているパケットと，TLSでセキュリティを実現しているパケットを比較してみます．ここでは，**図3**(a)のように，クライアントからサーバ，サーバからクライアントに短いメッセージを1往復だ