IoT時代の必読！ 押さえておこう！技術仕様の基本 インターネット・プロトコル教科書

第8回 IoT無線ネットワークに必須のセキュリティDTLS

笠野 英松

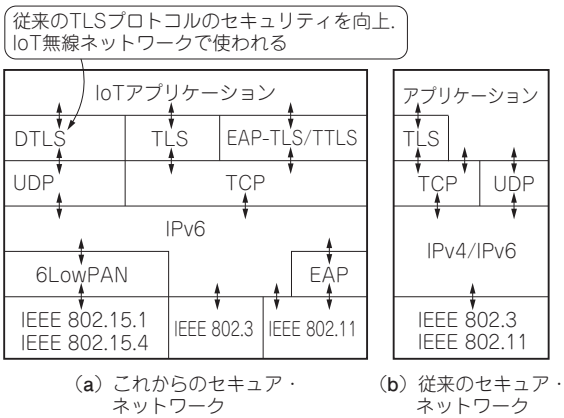

図1 今回紹介するプロトコル…IoT無線ネットワークで使われるセキュリティDTLS

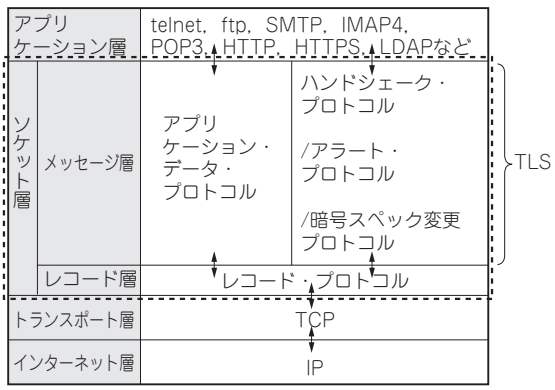

図2 DTLSのベースとなるネットワーク・セキュリティの基本プロトコルTLSの階層構造

最近では映像や音声，音楽，ゲームなど多くのアプリケーションがUDP（User Datagram Protocol）と呼ばれるプロトコルを使用することが多くなってきています．とくに，無線伝送が一般的なIoT/M2M（Internet of Things/Machine to Machine）では，TLS（Transport Layer Security）のセキュリティを向上させたDTLS（Datagram Transport Layer Security）を用います．今回はこのDTLSについて解説します．

● TCP/IPセキュリティ

図1はアプリケーションに直接関係するTCP/IPセキュリティのうちトランスポート関連の部分を示しています．従来はTLSだけでしたが，現在では，DTLSやEAP関連TLS（Extensible Authentication Protocol - Transport Layer Security）が出てきています．IoT/M2M関連では下位層にIEEE 802.11（無線LAN）＆EAPやIEEE 802.15.1/4＆6LowPAN，そしてIPv6を使用することになります．ここで，セキュリティの核心的なプロトコルがDTLSです．

ベースとなる基本セキュリティ・プロトコルTLS

DTLSプロトコルはTCP上で稼働するTLSプロトコルの「一つのバリエーション/差分」ということができます．そのため，DTLSを理解するためにはベースとなるTLSの仕様を押さえておくことが前提です．

● 階層構造

TLSは**図2**のような階層構造（2階層）を持っています．トランスポート層（TCP）の上にはTLSレコード・プロトコルがあり，上位層を暗号でカプセル化します．TLSの上位層としては，TLSハンドシェーク・プロトコルやアラート・プロトコル，暗号スペック変更プロトコル，アプリケーション・データ・プロトコルがあります．

● セキュリティ保護時のコネクション状態

TLSは特有のコネクション状態を保持します．このコネクション上でアプリケーションの各セッションを実行します．TLSコネクション状態は，暗号化アルゴリズムや圧縮アルゴリズム，認証アルゴリズムなどを表す，TLSレコード・プロトコルの動作環境で，以下のようなものがあります．

- 圧縮状態（compression state）：圧縮アルゴリズムのカレント状態．
- 暗号状態（cipher state）：暗号化アルゴリズムのカレント状態．
- MAC秘密鍵（MAC secret）：コネクションのため

第1回 ネットを使うときの隠れ常識! 技術文書RFC（2015年9月号）
第2回 考えとかないとマズい！ IPv6プロトコルの全体像（2015年10月号）
第3回 IPv6プロトコルこれだけは…パケット/アドレス/ソケット（2015年11月号）