巻頭言

IoT時代のセキュリティ課題

徳田 英幸
慶應義塾大学環境情報学部教授
一般社団法人 重要生活機器連携セキュリティ協議会 会長

IoTの進化

世界中でIoT（Internet of Things）化の流れが加速しています。国内においても昨年10月に官民連携でスタートしたIoT推進コンソーシアムは、当初約900社の企業がメンバーでしたが、現在、2,200社以上の企業が参加しており、まさに、“IoT x ビジネス”といった社会的創発現象が起きています。IoTは、単に、モノ（物）のインターネットと訳されることが多いですが、実際には、身のまわりの物や人工物だけではなく、人や生物、ビジネス上のデータやプロセス、空間上の位置情報などあらゆるモノ（Everything）がインターネットに接続され、情報を交換し、相互利活用される環境です。更に、これらのIoT環境の中で、つながれたモノたちがサイバー空間と物理（フィジカル）空間をまたいで制御されているシステムのことをサイバーフィジカルシステム（CPS）と呼んでいます。IoTがInternet of Connected Thingsであるのに対し、CPSは、Internet of Controlled Thingsを指しています。ITSに代表される交通系のシステムや気象情報と連動して水資源を管理しているようなシステムを“システムにつながれたモノたちを制御するシステム”という意味でCPSと呼んでいます。

IoT/CPS環境では、ビジネスドメインを飛び越えて、いろいろな機器、サービス、データ、プロセスなどがつながり、連携することで新しい価値や新しいコネクテッドサービスが創出されています。また、AI技術を使ってシステムから送られてくる様々なデータを解析し、システム内の機械やデバイスなどの故障予防や予知にも積極的に活用され、より信頼性の高いシステムなどの構築に役立ってきています。

IoTのセキュリティ

一方、IoT環境では、第４次産業革命のように期待され“メリット”が強調されている反面、従来のインターネット環境でのセキュリティ脅威とは異なる新たなIoT環境での脅威や“リスク”に対しても“先回りした対応”をしていかなければ、社会システムのあらゆるところで混乱が発生する懸念があります。IoT環境で対象となるシステムは、大きく２つのグループに大別されます。１つは、CPSに代表される電力管理システムやITSシステムなど、社会インフラとしてしっかり管理されている機器やサービス群から構成されている重要インフラ系システム。もう１つは、個人の家庭に設置され、一度設定された後は、あまり管理が行き届かないIoTゲートウェイ、スマートホーム、スマート家電、スマート健康機器、スマホ、パーソナルロボットなどの生活関連系システムです。重要インフラ系も、生活関連系システムもいずれも複数のシステムが連携しているので、機器に障害が発生した場合や攻撃を受けた場合には他のシステムや連携しているサービスに伝搬し、被害が大きく広がってしまうリスクがあります。また、コネクテッドカー・サービスなどのように、自動車と連携したサービスの場合、車載器の脆弱性を突いてモバイルネットワーク経由で侵入し、ファームウェアを書き換え、車のエアコン、ワイパー、ブレーキ、変速、ステアリング機能などを乗っ取られたクライスラー社のJeepのような事例も報告されています。また、IoT環境では、多くの個人に関連したデータがクラウド内やスマートデバイス内にストアされる場合、それらの情報が漏洩や改ざんされてしまうリスクに対しても対処する必要があります。このように、スマートデバイス層、ネットワーク層、クラウド層、コネクテッドサービス層の４つのレイヤにおける新しい脅威に対して、システムの企画、設計時からセキュリティを意識し、ライフサイクル全体を考慮した“Security by Design”やプライバシー保護を考慮した“Privacy by Design”の実践が必須になってきています。

CCDSの活動

このような状況の中、一般社団法人 重要生活機器連携セキュリティ協議会（Connected Consumer Device Security Council）は、2014年10月に設立され、我が国の重要生活機器全体のセーフティ＆セキュリティレベルの向上を目指し、重要生活機器のセキュリティ技術に関する調査研究、ガイドラインの策定や標準化の検討、及び普及啓発を行い、ものづくり産業の発展、新規事業創造、そして国民生活の向上を目指して活動しています。2016年６月には、安心・安全に利用できるIoTサービスの実現に不可欠な“Security by Design”の考え方を広くIoT製品開発ベンダーでの普及を目指し、車載・IoT ゲートウェイ・金融端末（ATM）・決済端末（POS）の４分野の製品分野別セキュリティガイドライン第１版を公開しました。また、本ガイドラインは、IPAが策定した「つながる世界の開発指針」とも連携しており、各製品分野の視点で脅威やリスクをより具体的に想定してあり、関連文書として位置付けして構成されています。

今後も、IPA技術本部ソフトウェア高信頼化センター（SEC）、内閣サイバーセキュリティセンター（NISC）、IoT推進コンソーシアムなどと連携し、我が国における安心・安全なIoT環境の実現に向けて尽力していきたいと考えております。