情報セキュリティに関わる最近の動きについて

JNSA 理事
東芝ソリューション株式会社
遠藤　直樹

社会、経済、文化、技術などは常に変化をしていると思うが、その中で最近私が経験した情報セキュリティに関わる動きについて考えてみたい。それらの動きにおいては、技術者として考えていかねばならないことがたくさんあり、今後、皆さんと協力していければ良いと思う。

まず、１月下旬に那覇市で開催された「SCIS2017暗号と情報セキュリティシンポジウム」である。700名を超える多くの方々が参加されたと聞いたが、今回も先進的な領域の技術が多く発表され、熱心な討論が繰り広げられた。今回新しく設けられたセッションとして「機械学習セッション」がある。人工知能（AI）、ロボット応用、多くの産業機械応用として脚光を浴びている技術領域である。セッションの内容は大きく２つが含まれる。一つは、セキュリティ要素技術の一つとして機械学習を活用し、攻撃対策やプライバシー保護に役立てようという考え方である。もう一つは、機械学習を含むAIシステムへの攻撃（例えば学習器への入力を改ざんするなどして結果としてAIアプリケーションの誤判定を誘発させる、など）を如何に検知して防御するか、である。今後AIシステムの活用がさらに広まっていった時を考えると機械学習に関するセキュリティ面の研究は非常に重要と思われる。AIシステム全体の脆弱性をなくし、ユーザが困らないようにする必要がある。

次に欧州において検討が進むデータ流通に関する規制の動きである。2016年4月のEU一般データ保護規則（General Data Protection Regulation：GDPR）において、個人情報関連データのEU域外への持ち出しは原則禁止、行う場合は条件や義務を伴う、という解釈がある。一方、非個人情報で機械生成データに関しては上記GDPRではカバーされていないため、次のステップを定義してカバーできるような制度を作っていこうというわけである。今年1月10日にEUのDigital Single Market Newsletterで公表された。これらの動きは、情報流通を支えるITインフラに対して何を要求することになるのだろうか。EU域外の企業等も場合によっては対象となる可能性があり、私たちも慎重に見極め対応を考える必要がある。

最後にIoTの一種としてのHEMS（家庭のエネルギー管理）について述べたい。ある場において私はHEMSの安心安全対策検討に参加した。その検討においては情報セキュリティの視点だけでなく、PL法、個人情報保護法、電気用品安全法などを重要視した検討を実施した。つまり、身近なシステムの安心安全は情報セキュリティだけで語るのは困難ということである。今後私たちは広い視野で広い領域を学習して世の中の安心安全に貢献しなければならない。技術者としていつまでも学ぶ姿勢を維持するのが重要と言えそうである。