ネットワーク事業者における セキュリティ対策

JNSA 理事
KDDI 株式会社
技術開発戦略部　三宅　優

今年の5月23日に、「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が公布されました。電気通信事業法の改正には、深刻化するサイバー攻撃への通信事業者の対処の促進も含まれています。皆さんもご存じのように、セキュリティの観点から問題があるIoT機器がネットワークに大量に接続されたことにより、サイバー攻撃の標的がIoT機器に移行し、マルウェアに感染したIoT機器が増加しています。そこで、サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進するための法律改正が行われました。

インターネットワークを使っている方には、ネットワーク事業者側でもっとサイバーセキュリティ対策を行ってほしいと思っていらっしゃる方も多いと思います。私は、国連傘下の電気通信に関わる標準化活動に参加しておりますが、その場においても多くの国から国際連携によるサイバーセキュリティ対策を求める声が上がりますが、各国の法律・規制や政策の違いから統一的なものを作るのは容易ではありません。例えば、日本では憲法で通信の秘密が保証されており、原則として通信の内容を見ながら判断することはできません。この制約の下で日本は、消費者保護の観点から、政府と通信事業者を含む民間企業が連携してサイバーセキュリティ対策を行ってきており、ネットワーク側でのセキュリティ対策の重要性を認識しているとともに、他国よりも先んじた取り組みを行っていると思います。

IoT時代になり、これまでのセキュリティ対策では不十分になるとともに、多くの人々(機器製造者、機器設置者、利用者、等) がセキュリティについて考えなければ、安全性が確保できなくなりつつあります。しかし、多くのものはセキュリティ機能が無くても動きますし、セキュリティの知識が無くても利用できてしまいますので、この状況 (期待するセキュリティ対策が行われない) を踏まえた対応が必要です。前述の通り、ネットワークにおいては法律改正により以前より踏み込んだ対策が取られようとしており、今後対策が進むと考えられますが、ネットワーク側での対策には通信の秘密等の制限がありますし、すべての通信を詳細に解析して対策することも困難です。IoT時代に向けて多くのセキュリティ対策が検討されていますが、ネットワーク側の対策はその1つであり、さらに多くの種類の対策が必要な状況です。ネットワーク利用者がセキュリティの知識が無くても安全に利用できる環境を構築していくことが必要とされている中で、多種多様な企業、団体が参加するJNSAの場において、セキュリティに対する課題を共有し、新たなセキュリティ対策や取り組みが相互に作用して効果を発揮するような活動ができればと思います。