資料５－２

IoT 機器のサイバーセキュリティに関する取り組み

2017.12.11

一社）ビジネス機械・情報システム産業協会
情報セキュリティ委員会

IoT（Internet of Things）の進展にともない、これまでインターネットへの接続が想定されなかった機器がインターネットに接続されるようになり、サイバー攻撃の起点の拡散や新たな攻撃パターンの急増などサイバーネットワークについて新たな脅威が生じてきている。

コンピュータの周辺機器であるオフィス向けのプリンタや複写機・複合機等の事業者により構成されている当協会や会員企業では、ネットワーク接続機器に対するお客様からの要望に応えるため、複写機・複合機を中心に国際規格に基づく CC 認証*取得を進めている他、これらの製品の海外でのセキュリティ標準等の検討にも関わってきている。

＊Common Criteria: ISO/IEC15408 に基づく認証

我々は IoT 機器について何等かのセキュリティを確保することは必要であるが、そのためには、個々の IoT 機器が取り扱う情報や機器の構成といった特性や性質を考慮することが必要であり、一律に規制することは効果的ではないと考えている。セキュリティを確保するための具体的な手段については、種類や構成の異なる IoT 機器について、その設計開発をしたベンダ自身により最適なセキュリティ対策を実施することが効果的であり、その結果を開示し、可視化する自己宣言型が経済合理性の観点からも現実的であると考える。

以上の基本的考え方に基づき、我々は時々刻々と変化するグローバルでのセキュリティの脅威に対応するため、以下の諸点をポイントとして検討を進めていきたいと考えている：

① 各社で既に実施されている国際規格（CC 認証）を活かした自主認証・自己宣言
② グローバルにつながっている IoT 社会やグローバルなサイバーセキュリティリスクに対応できる国際的整合性の確保

更に、ネットワークシステム全体のセキュリティ確保の実現のためには、各 IoT 機器のセキュリティ確保だけでなく、以下についての横断的な対応が必要と考えている。

① 端末機器だけでなく、ネットワークシステム全体でセキュリティを確保する総合的な対策
② それぞれのネットワークシステム（応用領域、目的）で想定される脅威（攻撃の方法や想定される損失・危害の程度）を考慮したセキュリティ対策

こうしたセキュリティ対策の実施にあたって、まずは早急に対応が必要な製品や DDoS 攻撃について優先して検討することに同意する。また、消費者・顧客に真にセキュリティ確保された製品を提供するため、サプライチェーン全体でサイバーセキュリティが確保できるような取り組みの実施に向けて協力していきたいと考えている。

以　上