資料３－２

CyberDefense

IoTセキュリティ対策の中長期的課題
（ビジネス及びサイバー脅威の変化の見通しから）

2017年3月

サイバーディフェンス研究所
名和 利男

（今後の変化の見通しから考える）IoTセキュリティ対策の中長期的課題の克服

- IoTの設計、開発、製造、販売、インテグレーション、運用管理、保守管理等における**全ての利害関係者**が、IoTに係るサイバー脅威を**適切に認識**し、その脅威に相応する**必然的な行動（対策）**を取る環境を構築することが必要。しかし、政府が推進する成長戦略の足枷になってはならない。
- この観点で、IoTセキュテリィ対策の中長期課題を克服する取り組みの方向性の私案は、次のとおり。

– 法的義務の活用による脅威認識の誘導

- 例：善管注意義務（*民法644条; 善良な管理者の注意を持って、委任事務を処理する義務を負う*）が適用可能となるような**サイバーセキュリティ文化の醸成**につながる施策の推進。
- 例：核物質管理の領域において、2014年核セキュリティ・サミットにおいて、核セキュリティ文化の醸成に関するコミットを行い、2015年原子力規制庁による**行動指針*の策定***と、5つの行動原則の提示という施策が参考になる。

– 業界団体の協力による公的ルールの浸透

- 例：官公庁が発行するIoTセキュリティ対策に関連するガイドライン、手引（書）、マニュアル、基準、ハンドブックで記載されている要求事項を整理し、業界団体の協力を得て**調達仕様等に積極的に反映**していただく。

– 高度なセキュリティテスト技術の開発と提供によるIoTセキュリティ確保の支援

- 例：Hardware Trojan 検知や Fuzzing の**技術開発**と、重要領域に対する**積極的な提供と利用**により、IoT調達におけるセキュリティ確保を公的な立場で支援。（重要領域の組織・団体のセキュリティ投資の圧縮に繋がり、より高度なセキリティレベルが期待できる。）

本資料に関する連絡先

名和 利男（Toshio NAWA）
サイバーディフェンス研究所
専務理事／上級分析官

Email: nawa@cyberdefense.jp
SNS: about.nawa.to
Tel: 03-3242-8700

Office: www.cyberdefense.jp
Response Team: www.cirt.jp