IoT が進まない現状とセキュリティからみた将来

(名工大) ○(正)橋本芳宏*

０．はじめに

「IoT の進まない現状」を語るだけでなく、「セキュリティからみた将来」までをたった20分で語るというのは無謀な試みであり、それを1 枚の要旨に論旨が理解できるようにまとめるのは困難を極めることである。

ここでは、講演の目次と簡単な解説を添えることで、要旨原稿としたい。

１．ドイツが Industirie 4.0なら日本は Society 5.0

「超スマート社会」という名の下、国は高圧ガス保安法改定なども含め、多額の予算を拠出して IoT、Big Data, AI を推進しようとしており、企業経営者も「なにかしろ」と社員にはっぱをかけている状況が3年以上過ぎているが、目新しい成果は得られていないのが現状であろう。

２．そもそも IoT の革新性は

IoT は Buzzword といわれ、その定義を議論することに意義があるとは思わないが、Internet of Things であるので、モノについての革新性を考える。①蒸気機関②電気回路③マイコンにより、モノはより高機能に高性能になってきた。特に③ではモノ自身がインテリジェンスを持つようになり、日本はマイコン家電で強みを発揮した。新たな革新が④IoT で講演者は、これをモノからインテリジェンスが離れてクラウドに移行することと捉えている。Siri は i-phone だけでは機能せず、インターネット上の i-Cloud と接続して初めて利用できる。インテリジェンスがちゃっちい CPU とケチくさいメモリから解放されることが、どのような革新性につながるのかは、講演で説明するが、クラウドにインテリジェンスが集まることで、本来の目的とは異なるサービスが生まれ、つながる世界が革新を導く。Google Map の渋滞情報は、Map ユーザー自体は自分のナビをしてもらうために GPS 情報を Cloud に上げ、Google はたくさん集まるから渋滞を推定でき、他のユーザーに情報提供できるというのも一例であろう。

３．System から SoS (Systems of Systems)へ

まず、目的を特定し、それに必要な要素を洗い出し、要素を設計し、組上げるという Systematic Approach は仕事を進める根本ではあるが、IoT を進めるのは、もっと他人が利用できるように情報を提供しあう SoS という考え方である。Industrie 4.0 では Reference Architecture Model が議論されているが、Sociey 5.0でその議論が見えないのも、日本での議論には SoS の世界観を欠くからだと感じる。

IIoT (Industrial Internet of Things)という用語があるが、工場操業で必要なら金をかけてでもセンサーを取り付けていただろうし、チープな無線センサーの導入で解決できるようなものがどれだけあろうか。IIoT が従来の目的から離れずに議論されているので、IoT 推進ラボが募集しても、革新性を感じるものが得られないという事態に陥っているのではなかろうか。

４．IBM Watson にみる日米の情報力の絶望的な格差

IBM の Watson は、クイズ番組のチャンピオンに勝ったことで有名になったが、過去のクイズを覚えるだけでなく、文章をつないで、虫食いのクイズを自分で合成するという機能が利用されている。文章を扱うのが Cognitive Engine であるが、IBM は言語ごとにこの Engine を用意している。またコンプライアンスのために、顧客のデータは他に渡せないので、IBM から提供されるのは赤ちゃん Watson に限られる。日本人には、日本語が利用できるのはありがたい話であるが、情報力を向上させるスタッフに、日本とアメリカでは各段の差があり赤ちゃんの能力に大きな差が発生する。

５．成功体験に甘んじたボトムアップ経営の結果

日本では、多くの会社で、「IoT, AI, Big data なんかやれ」という号令が氾濫しているように思われる。そして、どこかで、うまくいったら、横展開するぞと考えているように思える。これまでは、それでうまくいったのであろう。GE が500億円の経費削減ができたと報告したものと、同じようなことができないのではなく、各事業所ではそれだけ投資する規模の仕事がないという理由で実現しない場合が多いのではなかろうか。500億円も全社的な規模での話で削減割合は2%に過ぎないので、日本企業でもトップダウンで大きな予算を確保すれば、同様な成果を得られた例ができたかもしれない。前述の痩せた日本語 Watson の赤ちゃんは育つ場も与えられないというのが現状となっている。

６．サイバーセキュリティからみたプラントの将来

セキュリティに関する紙面があまり残っていないので、トピックスを箇条書きに記す。

① サイバー攻撃の脅威は現実のものになっていて、すでに日本でも被害があり、爆発も起こりえる。
② サイバー攻撃は「悪意の誤動作・誤操作」とみなせ、ものを中心に検討すれば、想定外の攻撃でも、安全の枠組の検討の延長上で議論できる。
③ インテリジェンスはセキュリティホールの源で、クラウドで集中管理すべき。
④ 内部は見えないが、複数のバックアップを有し、コントロールというサービスを継続できる Fog を事業所においてリアルタイム性のサービスを実現し、その他を Cloud に上げ、フィールドはシンプルな機能と通信だけというデバイスで制御する構造が、プラント操業の将来像となる。
⑤ 想定外の攻撃からの防御には、多様性多重性が必要である。全滅を防げれば、検知や対応の可能性が生まれ、安全も確保できる。一人勝ちではなく、多様性を尊ぶ優しい世界に。

http://www.manage.nitech.ac.jp/Security/
に、この発表に関係する既発表資料を置いている。

*hashimoto@nitech.ac.jp