第１回サイバーセキュリティリスクと企業経営に関する研究会要旨

日　時：平成２７年１月２９日（木）１３：００～１５：００
場　所：IPA　１３階　会議室Ａ・Ｂ
出席者：岩井委員、川口委員、佐々木委員、徳田委員、名和委員、林委員、松浦委員、
　　三輪委員、山口委員

概　要：

●今回の研究会での「セキュリティ経営」の定義は、セキュリティ対策をトップマネジメントで行い、政策的出口を求めるというもの。
●米フレームワークは、最初は義務化も検討されていたが、民間からの反発もあってか、任意のものとなった。このようなものは、国から強制力を持ってやらないと難しいのでは。
●業種等によって想定シナリオ、想定影響が違う。「仮想的」を想定し対策を考えないといけない。日本では、各業種のベスプラがないとよく言われる。
●米フレームワークは、その先にある管理策として膨大な基準等などがあるが、これを全てできる会社はない。優先度でやる事になるが、この日本版があってもよいのではないかと思う。
●経営層にボトルネックがあるという前提だと、彼らにやる気を持ってもらうには、日本では国からのお墨付き等がないと難しい。第三者評価等で「ここまでやればいい」と示すのが重要。
●サイバー保険の普及率は日本では、かなり低い。しかしながら米国でも３割程度の普及率。
●セキュリティについては、インシデント事案のデータで話が進むことが多いが、平時におけるデータを定常的に取ることにより分かることもある。
●サイバー保険については、サイバー攻撃に遭ったことについて国への報告義務等がないので、保険発動のタイミングが難しい。セキュリティ産業はその能力が重要で、規模の経済だけで図れる話ではない。
●事前にセキュリティ対策を取らずに事案が起きた際に謝罪する方が、事前にコストをかけて対策を講じるより、コストが低いと経営者の多くは考えているように思う。経営者を動かすには、目に見える何か（資金、法令等）が必要では。
●地方の企業にとって、簡単なセキュリティ対策の実施がレベル的に困難と言われるケースも多い。
●日本の IT 技術者のほとんどは IT を使う企業よりも IT 企業に分布している。このため、セキュリティ関連業務も IT 企業に偏重して分布していると考えられ、施策対象として、IT 企業へリーチするのが即効性のある可能性。

（以上）