第８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９月４日（金）１０：００～１２：００
場　所：ＩＰＡ　１６階　会議室
出席者：佐々木委員長、川口委員、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：
【サイバーセキュリティ経営ガイドライン（案）について議論】
●経営者に向けて、最低限やるべきところとそれ以外分かるように、あるいは、経営者が読む部分、担当者に読ませる部分が分かるように書いてはどうか。
●全ての項目に対応できるのは、大企業でお金のある企業しかないのではないか。他方、これがあることにより、政府全体・社会がこういっていると、経営層以下の担当役員が経営者に説明できるのではないか。
●全社でできないということに同意。例えば、1番上の項目のみやると決め、リーダーシップの下で体制をつくり、やるという宣言ならできる。どうやるかは企業により異なるのではないか。
●企業がやることを宣言したらどうか。宣言したことに違反して、サイバー攻撃を受けたら、宣言に対する違反というコミットメント責任というのはあり得る。
●まずはガイドラインを出してみて、効果や使われ方を見てはどうか。
●脅威＝情報漏洩に重きをおいているが、インターネットや IT 技術使ったビジネスは運用阻害のリスクがある。制御システム部門への適用を含みうるとすれば、企業も売り上げ直轄の問題として取り扱うのではないか。
●経営者にとって大事なのは、ヒトの確保とカネの確保。それ以外はプライオリティを下げてもよいのではないか。
●今までは、１つの攻撃者によるばらまきが多かったが、委託業者等を使って、大手企業との契約を経由して広範囲に攻撃が広がるので、中小企業もガイドラインの対象に入るというロジックで書いてはどうか。

（個別内容にかかる主な意見）
●１．１と、それ以降の関係を整理すべき。
●「分離」「多重防御」とあり、「監視」が抜けている。早く見つけて対応することが大事。
●「残留リスク」が受容できないときに保険に入ることにより、リスクが減るわけではない。保険は、残存リスクをみて、対応できず、コストに対応できないときの対応策。
●J-CSIP のような体制は、他の企業にはない。情報共有体制について受け皿がないのではないか。

（以　上）