第６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７月７日（火）１０：００～１２：００
場　所：ＩＰＡ　１６階　会議室
出席者：佐々木委員長、岩井委員、川口委員、名和委員、林委員、三輪委員、山口委員

概　要：主な意見は以下のとおり。

●経営者のリーダーシップの下、攻撃を前提として、例えばログをどう残すか等が重要な判断。
●いざというときのためのログ保存は、インシデントレスポンスを短期間で終わらせてダメージを少なくするために行うという、その目的を明記してほしい。
●セキュリティと効率性のトレードオフを考え、現実的に実行できる対策にすることが必要。
●セキュリティ対策を実施するにあたっては、現実の仕事の効率性とのバランスが大事。通常業務がどうなっているのか把握してからリスク評価しないと意味がない。
●セキュリティ対策は、他者に迷惑をかけないためにも必要との観点を追加すべき。
●事故発覚後、どのくらいのスピード感で公表するのがよいか等のアドバイスも有用。
●見つからないサイバー攻撃事案も多い。見つかったとしても、個人情報以外はその適切な公表が不十分なおそれがある。このため、インシデント時に公表すべき調査内容や調査結果を踏まえた対策の実施、その効果確認及び平時への移行などの公表すべき内容について記載したインシデント公表に関するガイドラインにより、こうした状況に一石を投じる必要があるのではないか。また、インシデント対応に経験のない企業は、外部のセキュリティベンダとの連携も必要。その旨も公表ガイドに書くべき。
●個々の企業が、リスク評価を行い最適な対策を見極めるのは限界がある。認証制度によりセキュリティ強度に必要な一定の対策を促し、また、評価することが必要ではないか。
●セキュリティ対策手法そのものを書くことは、いくつかある対策手法の選択肢の芽を摘んでしまう。みな同じ対策手法を執るおかしな状況さえ生まれる。そうではなく、ガイドラインでは対策目的を規定して、最適な具体的な対策手法は各企業に任せるのがいいのではないか。
●ガイドラインの普及・広報が大事。
●大学も含めた人材育成では、セキュリティの知見だけではなく、セキュリティ利活用とセキュリティの双方の知見を有する人材の育成が課題。
●サイバーセキュリティリスクの評価ができる人材の増加が必要ではないか。

（以　上）