第７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３１日（火）１３：３０～１５：３０
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に関して議論。主な意見は以下のとおり。

●「経営層」とは、経営と執行の分離、つまり取締役と執行役は分離していることが前提か。日本では分離していない企業が多いと思うが、分離している企業から見ると、監査は執行役ではなく取締役の担当になる。どのように考えるか検討すべき。
●経営者のインセンティブをあげるため、経営者に責任を負わせるならば、経営者の報酬を高くしてもよいと株主総会で認める流れにできたらよいのではないか。
●一般的にクラウドが安全かどうかは別にして、中小企業においては、サーバーをクライアント側に持って行き、規模のメリットを活かして監視する仕組み等の対策を入れること自体はリスクを下げるのではないか。
●クラウドにも様々あるので、クラウドを使えば安全というわけではなく、それによるリスクの増加もある。それよりも、大事なデータを分離する方向についても検討すべき。
●インシデント対応として、事態の把握、被害の範囲の特定を行う体制が必要。
●このガイドラインは、経営者に対して心構えを説くようなものだと理解している。よくある攻撃で被害を受けるのは、従業員含めて基本の徹底ができていないということ。業務のひとつひとつの行動に注意深くなることで、競争力の向上にもつながるのではないか。
●インシデントが起きた結果、何が起きたのか、具体的な事例を入れると分かりやすくなるのではないか。
●経営者等から、他の幹部のセキュリティ対策に関する意識があがらない、どのようにしたらよいのかという声を聞く。逆に、CSIRT のトップの役員からも、上の幹部にどう認識してもらうかという声を聞く。方法論が分からず、内部の指揮者に頼るところも見られるので、できるだけ方法論を入れるとよいのではないか。
●日本のＣＩＳＯのポジションは低い。その役割や責任を認める仕組みが必要ではないか。
●自社にはそういった事案は起きないという過信がある。事故の発生を前提に考えるということは頭に入っていても、本当に起きたあとのことを考えることが大事。
●セキュリティのリスクは、一般的なリスクとの共通項も多い。その特異性を訴える必要性もあるが、一般的リスクと大きく変わったことではないということも理解してもらいたい。

（以　上）