第４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４月２３日（木）１０：００～１２：００
場　所：ＩＰＡ　１３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

概　要：主な意見は以下のとおり。

●セキュリティ経営ガイドラインができた後は、どのように普及していくのか。
●上場企業等では外部からのサイバー攻撃は意識している事が多いが、内部からのサイバー攻撃に弱い傾向がある。内部犯行を意識したセキュリティ経営ガイドラインを作った方が良い。
●新たな認証制度について、政府から求められても企業はメリットがないとほとんど実施しない。インセンティブが沸くような仕組みが重要。中小企業についても、昔から問題になっているが、進んでおらず、踏み込んだ対策が求められる。
●新たな認証制度について、これはあくまで手段であって、取得すれば良いというような事にならないようにすべき。
●サイバー攻撃が巧妙化・複雑化している中では、あまりに何でも情報共有すると、共有された側も消化不良になる。業種毎に仮想敵、どういう攻撃が売上げにインパクトがあるのかという事から、対処にも優先付けする必要がある。セキュリティ経営ガイドラインは仮想敵、想定される被害を検討することも入れた方が良い。
●日本でも、グローバルな企業では、米国のサイバーセキュリティフレームワークを基準にしているところもあるが、日米の企業文化の違いもあり、日本ではドキュメントがあるかどうかが重要視され、サイバーセキュリティフレームワークにある運用の部分が意識されておらず、基準を満たしているとは言えない部分がある。
●IOT が進むと、IP アドレスを持ったセンサーが増えていく。どこかで分散化、階層化していくので（フォグ・コンピューティング）それを意識した対策（フォグ・セキュリティ）を考慮した対策が必要。
●組織の中に SOC を持つことと、組織トータルでセキュリティを考えることの縦横関係で考えることが重要。マイナンバーやオリパラでも官庁だけでなく企業をどう集めるのか。オリパラで構築する新システムと既存の CSIRT との連携も考えるべき。
●世界の IOT 市場は、M&A 等によりどんどん進んでおり、日本は乗り遅れている。日本製品だと思ったら、部品は外国製ということもあり、セキュリティリスクが内在化している。これを意識した経営が求められる。切迫感を共有できるようなセキュリティ経営ガイドラインを作成すべき。
●海外のセキュリティは政府でもインテリジェンスの部分が進んでいるが、日本では現在構築中。日本では企業が自分の力で分析することになるが、どこまでを求めるのか。
●中小企業でも千差万別であり、規模感で言うと年商１０億円を超えると IT 投資できる余裕がある。年商３～５億円では、業務もコロコロ変わったりして、これをやれとゴリ押しは難しい。
●日本の IT 投資におけるセキュリティ投資は少ない。株主の意識もセキュリティになく、例えば、日本では個人情報が漏洩した被害者が訴訟を起こすことはあるが、漏洩した会社の株主が訴訟を起こした例は少ない。

（以上）