第３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３月１７日（火）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、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：

●各種データ、統計等は、全ての攻撃等の情報が現れている、と考えることは難しく、氷山の一角。もちろん、顧客相手のセキュリティサービスを提供している企業等が提供するデータ等は、一定の実態を反映しているだろうが、全てを網羅している、とはなかなか言いがたいだろう。そうした限界を想起しつつ、データ等を活用することになろう。
●エネルギー関係など重要インフラに対する攻撃が増加しているという懸念が米国においても聞かれる。
●情報共有について、欧米では、発生したインシデントだけでなく、インシデントが発生したかもしれないというような曖昧な情報を含め、さらには、攻撃に関する情報についても共有している。さらに、それらの判断を手動でなく、機械化して行うようなことも検討されている。これは、その情報の扱いを判断できる人を育てるには訓練が必要であり、ここを機械化しようとしたもの。また、今後 M2M が進むことも考えれば、こうした自動化の取組みに日本もどう対処するか考えるべきではないか。以上の点を踏まえた新たな情報共有の在り方を検討すると良いのではないか。
●日本の情報共有の仕組みの方向性についての参考として、イギリスでも情報共有の仕組み（WARPs）があり、米国の仕組み（ISAC/ISAO）と比較しながら、日本における仕組みとして、良いところを取っていくとよいと思う。日本の情報処理学会での取組も参照して検討すると良いのではないか。
●技術的能力を高めるにも、ログの取得・提供等の情報共有を進めるための仕組み作りは重要。
●情報共有を行う人を育てる事、さらには、育成する人を育成することも必要。そのためにも、インシデントの現場だけでなく、研究開発の現場にも情報共有を行い、人材育成していく事が重要。
●人材育成では、欧州には、Ｔ３（Training The Trainer）という取り組みがあり、日本でも参照したらどうか。
●情報共有の問題においても、人、組織、制度が重要ではないか。懸念されるのは、まず、組織内がセクション縦割りで必要な情報共有ができていない。さらに、企業はローテーション人事で異動し、企業間の人材流動性がないので、プロのコミュニティーの構成が難しい。通信の秘密との関係も、具体的な事例に即した検討も必要になりつつあるのではないか。
●日本は、サイバー攻撃を受けてマルウェア感染した企業に対する感度がいまひとつではないか。重要情報が漏洩したかどうか、個人情報の漏洩があるかどうか、という点は重要だが、こうした点にのみ意識がいってしまい、経営層等も、かかる漏洩がなければ問題がない、としてしまっていないか。そうではなく、マルウェアに感染してしまった、ということをもっと大変な事と捉える意識も必要ではないか。そうして対策を考えていく雰囲気醸成も重要なのではないか。

●日本での情報共有の推進においては、各省庁がそれぞれの目的で実施しているスキーム間での適切な共有等の可否も検討することが適当ではないか。
●サイバー保険を考えるとき、どの程度の金額が保険金支払い額として期待されるか、というデータが十分ではないところをどう改善できるか、も視点として必要ではないか。現状は、そこが十分わからないので、結果として、インシデント時に要請することとなるセキュリティサービスに要する費用とほぼ同じような金額が想定されることとなってしまっている。また、そうしたセキュリティサービスを要請する際に、実績のある企業等を適切に選択できるための情報共有、という仕組みも検討課題の一つだろう。

（以上）