JNSA ワーキンググループ紹介

リスク評価検討 WG

住商情報システム株式会社
WG リーダー　二木　真明

リスク評価検討ワーキンググループは、本年度から活動を開始した新しいワーキンググループです。情報セキュリティにおけるリスク評価は、これまで、情報資産の洗い出しと価値の評価、脅威や脆弱性の分析を経てボトムアップで行われてきました。この手法では、相対的なリスクの分布、大きさや対策手段などについて明確にできるのですが、一方でリスクの絶対値、つまり被害想定額の算出という意味合いでは、評価の粒度が荒く、最終的な積み上げ誤差が大きくなりすぎるため、使い物にならないという問題があります。これまで様々な形で、より精緻な評価を行うモデルが検討されてきたものの、いまだ課題も多いのが現状と言えるでしょう。

企業においては、情報セキュリティ以外にも、様々な「リスクマネジメント」が行われています。実際、これらの中で定量的にその大きさを決定する必要があるものの多くが、過去の事例や様々な傾向、要因をもとに統計的な手法を使って算出されています。つまり、個々のリスク要因に遡るのではなく、統計的に総量を予測するというトップダウン手法がとられることが多いのです。

従来型のボトムアップ評価はリスクへの対策を考えるという意味合いでは必須ですが、たとえば、その対策のための予算の総枠を他のビジネスリスクとの対比で検討する、といった経営サイドのニーズには十分にこたえられるものではありません。このため、過去には過少投資や過大投資が多く発生しています。そこで、総量についてはトップダウンで統計的に算出し、その分布や対策方法、優先順位についてはボトムアップ評価の結果をもとにするという合わせ技を考えてみてはどうだろうというのが、昨年までの議論で得られたひとつの方向性でした。

ボトムアップリスク評価の精度向上については、より精度の高い評価の前段階としての脅威と対策のマッピングの作成作業が、「セキュリティ対策マップ検討ワーキンググループ」で続けられています。一方、過去に発生した情報セキュリティインシデント、とりわけ情報漏えい事故についての被害額調査や傾向調査が、この数年にわたって「セキュリティ被害調査ワーキンググループ」で行われてきました。リスク評価検討ワーキンググループでは、これら他のワーキンググループと情報交換しながら、相互に補完的な役割を保ちつつ、まずはトップダウンでのリスク定量化に取り組んでいきます。

今年、上期は、まず作業に必要な基礎知識と情報を得るために、一般の企業リスクマネジメントで使

用される統計的な手法について勉強します。企業のリスク管理、とりわけ、いわゆるオペレーショナルリスクの管理は、広い意味では情報セキュリティリスクを含むべきとの考え方もあります。一方、情報セキュリティリスクというカテゴリを独立させた方がいいという考え方もあり、これらのバランスを見極めながら、オペレーショナルリスクの管理で使われる手法を学びます。当然ながら、すでに多くの人が忘れつつある（苦笑）算数（統計解析）、の知識も復習しながら進め、下期には、情報セキュリティリスクのトップダウン評価のためのモデルと、そのためのインプット情報として何が必要かなどについて議論していく予定です。

議論は月２回程度の会合と、メーリングリストやブログを介したオンラインで進めていきます。年度末にはこうした検討結果をとりまとめた報告書を作成する予定です。

さらに、将来、他のワーキンググループの成果も踏まえながら、より精緻な定量化モデル検討へ進むことができればと考えていますので、興味がある方はぜひご参加ください。

リスク評価検討ＷＧ

氏名	所属
リーダー 二木　真明	住商情報システム(株)
大谷　尚通	(株) NTTデータ
吉田　哲朗	グローバルセキュリティエキスパート(株)
井口　洋輔	(株)損保ジャパン・リスクマネジメント
赤間　健一	トレンドマイクロ(株)
大森　潤	日本オラクル(株)
菊地　正人	日本オラクル(株)
藤井　裕一	富士ゼロックス(株)
高橋　弘志	富士通(株)
佳山　こうせつ	富士通(株)
奥原　雅之	富士通(株)
井上　孝彦	三井物産セキュアディレクション(株)