第２回　サイバーセキュリティ経営ガイドライン改訂に関する研究会

日時・場所　　令和元年 11 月 27 日（水）14:30-16:30　　独立行政法人情報処理推進機構（IPA）

出席者

[委員]　佐々木委員長、稲垣委員、小松委員、林委員、松下委員、丸山(司)委員、丸山(満)委員、宮下委員、三輪委員

[事務局]　経済産業省 商務情報政策局 サイバーセキュリティ課 鴨田企画官、西野課長補佐、野村係長

IPA セキュリティセンター 瓜生センター長、小川グループリーダー、ジリエ研究員、半貫研究員

[オブザーバー]　IPA　横山グループリーダー、江島研究員、塩田研究員

議事概要

経済産業省サイバーセキュリティ課より、サイバーセキュリティ経営ガイドラインをベースとした可視化ツール作成方針と同方針に基づき作成した評価指標(エクセル表)を紹介した。可視化ツールについて自由討議を行ったところ、成熟度モデルを活用する評価方式に大きな異論はなかった。また、可視化ツール作成方針に対するいくつかの修正意見が得られた。委員からの意見は以下の通り。

【可視化の評価について】

- 経営者自身による詳細なセキュリティ技術の把握は必須ではないが、リスクを評価し最終的な判断をするのは経営者でなければならない。
- 可視化評価を行うチェック者は経営者でなく、権限を委譲しているのであれば CISO や実務者でもよい。
- 可視化結果は、今後、可視化ツールを評価する中で、投資家向け等、目的が変化していく可能性があるが、当初は、可視化ツールの普及を優先し、企業内部で使うことが推奨される。
- 評価者がチェックする際、成熟度の項目だけでは若干曖昧さが残るため、例えば、「文書化されている」であれば「社内規定がある」、「文書が評価されている」であれば「委員会が開かれて監査している」等、選択肢の内容を補足するわかりやすい例示が必要。
- 評価結果はレーダーチャートで示して、経営者を含む複数の人が比較できるようにするとよい。
- 経営ガイドラインや付録Aの中で書ききれない内容や、チェックシートの使い方を「経営ガイドライン実践のためのプラクティス集」の中で書くという選択肢もある。
- セルフチェックは主観が入るため、機密情報の度合いによっては第三者機関に客観的な評価をしてもらう点を示す必要がある。

【可視化ツールのチェック項目について】

- 技術的な対策の細かい内容は質問項目に盛り込むよりも、NIST 等既存の文書にリンクし、チェック項目としては例えば SP800 等の技術的規格を使って評価改善の実施を行っているか問うようにするとよい。
- 経営層が把握すべき内容、例えば、クラウドの勝手な運用の有無を確認するチェック項目はガバナンスの評価としてあってもよい。
- M&A など企業全体の資産価値評価に際して、セキュリティ評価も取り入れられ始めているが、現時点では一般的ではない。将来的には、セキュリティの成熟度評価が、資産価値評価に活用されることが望まれる。

【可視化結果の使い方について】

- 可視化結果に経営が関与しないというのは問題がある、善管注意義務の順守度合いの立証に法的証拠として使われる可能性もあると書いてもよい。
- 成熟度レベルが明確化され、改善計画が立てられる等の効果が期待されるので、可視化結果をベンチマークとして業界標準を作ることを検討すべきである。

以上