第3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2年2月21日(金) 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(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 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、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の案と今後の方針を説明。委員各位と討議を行い、可視化ツールの修正対応指針とした。委員からの意見は以下の通り。

【可視化ツールの項目修正方針】

- 同じ意味の選択肢の述語がぶれている等の表記ゆれを直す。

[可視化チェック項目]

- 指示1: ユーザが法令・契約の他に参照するガイドラインについて、「業界の」という限定を入れる必要があるか再検討する。
- 指示4: 「サイバー攻撃で自社に起こりうる『経営的に深刻な事態』を想定して、経営陣が把握した上でセキュリティ対策を指示しているか」がわかる質問にするとよいのではないか。
- 指示5: シャドーITの質問はあってもよいが、聞き方を工夫する必要がある。シャドーITは使ってはならないと意識しているか、対策しているか等を聞きたい。
- 指示5: 5-3、5-4は5-4を5-3に吸収することで合意した。他の項目は、別途委員と協議の上事務局で修正する。
- 指示7: 標的型攻撃メール訓練等は「怪しいメールが来た」等当事者から報告させることが大事である(備考に関する意見)。
- 指示7: 報道発表は公表内容のルールを事前に決めておくべき。サプライチェーン内の報告、情報共有も大事である。

[成熟度モデル選択肢]

- 選択肢は成熟度が基本で良いが、質問によっては成熟度が合わないものもあるので、無理に合わせなくてよい。
- 成熟度の選択肢は主体性を持たせた言い方にするか、成熟度モデルの一般的な言い回しも参照して再検討する。
- 選択肢が4段階になっているものはレーダーチャートへのアウトプットを考慮し5段階にする。
- 経営ガイドラインが経営者の責任を根拠づける一つの証拠として使われる可能性が十分ある点をリリース文に記載する。

[使い方ガイド]

- 従業員300名以上とあるが、300名以下でもグループ会社であれば対象とすることを明記する。
- 評価者がチェックした結果を経営者と共有することが重要である。

【可視化ツール策定の今後の方針】

- 業界比較できるように、企業の規模、業界等、属性値を聞く必要がある。
- 可視化ツール項目の大きな修正方針はこの会議で決定し、詳細は委員の個別意見を踏まえて修正を行った上で今年度中にβ版を作成する。来年度はユーザ企業においてβテストを実施する。
- 経営ガイドライン付録Aは、可視化ツールFIXまで改訂しない。
- 経営ガイドラインによるセキュリティ対策の可視化結果とプラクティスを結びつける取組みや、企業から得たセキュリティ対策のTipsを自動的に収集する仕組みを検討する。

以上