第１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 8 月 28 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 奥家課長、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

委員の互選により佐々木良一氏を委員長に選出するとともに、本研究会は非公開とし、議事要旨のみ公開することとなった。第一回の研究会では、経済産業省よりサイバーセキュリティ経営ガイドラインの改訂方針について、可視化が重点であることを説明。IPAより可視化の検討事項案について説明。その後、可視化のターゲット・目的や可視化ツールについて自由討議を行った。委員からの意見は以下の通り。

【可視化のターゲットや目的について】

- ターゲットについては、単に300人以上の企業とするのではなく、サプライチェーンのガバナンスを重視して企業グループ内の中小企業を含めることも想定する。
- 可視化で何をするのか、他社比較・業界内の位置づけを明らかにして何をするのか、経営層の意識向上をどうするのか等、可視化の目的を明確にすることが重要である。
- セキュリティ対策の可視化によって、経営層が対策状況を認識できるようしたい。
- 可視化は企業のサイバーセキュリティについての健康診断に相当し、改善点を明らかにするのが大事だと考える。
- JUASでガイドライン実施状況を付録Aの項目について5段階評価したところ、対策ができているグループとできていないグループの差が明確になり、改善の方向性がわかった。
- 教育やメディア等、組織には所属しているが個人で業務を回しているところへのセキュリティ対策の導入は大きな壁がある。
- 経営ガイドラインは中長期的には、IoT、AI、DX、製品のセキュリティ対策及びサイバー・フィジカル・セキュリティ対策フレームワーク等との連携等を含める必要があるが、現状では企業のITセキュリティ対策が未だ不十分であることから、引き続き従来システムの基本的な対策強化が必要と考える。今回の改訂はその範囲で行う。
- ガイドラインはある程度曖昧でも経営者にわかりやすいことを大事にしたほうがよい。

【可視化ツールについて】

- チェックリストの実施者選定や情報収集の仕方に関して課題が伴うが、経営層・担当部門・現場等、複数のメンバがチェックすることにより、回答の歪みを是正することが課題解決の一案として挙げられる。
- チェックリストは、41項目程度であれば企業の情報セキュリティ部門の担当者がセルフチェックできると思われる。
- チェックリストの粒度は多様なIoTやOTを意識する粒度ではないと考える。
- 経営層とのコミュニケーション向けには付録Aの41項目でチェックする一方、現場が評価する場合、各項目の評価を多段階にして具体的に実施するのが大切である。評価基準やチェックリストの使い方を示した解説書の作成に注力する必要がある。
- 多段階の基準の決め方は様々なので、よく検討した上で決めなければならない。

以上