第 1 回　サイバーセキュリティ経営プラクティス検討会

日時・場所　　平成 30 年 7 月 10 日（火）15:30-17:00　　独立行政法人情報処理推進機構（IPA）

出席者

[委員]　橋本委員長、荒川委員、上野委員、落合委員、教学委員、秋元様(小松委員代理)、宮下委員

[オブザーバー]　経済産業省 商務情報政策局 サイバーセキュリティ課　石見課長補佐、元木係長

[事務局]　IPA 江口理事、横山グループリーダー、大谷氏、小川グループリーダー、木内研究員、ジリエ研究員

議事概要

委員の互選により橋本正洋氏を委員長に選出するとともに、本検討会は非公開とし、議事要旨のみ公開することとなった。第一回検討会では、経済産業省より「経済産業省のサイバーセキュリティ政策とプラクティスの位置づけ」、IPAより「経営ガイドラインプラクティス作成に関連する活動と今後の計画」について説明の後、サイバーセキュリティ経営プラクティスの作成及び対策実施の可視化の課題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。

【プラクティスの課題について】

- 重要インフラに課せられたセキュリティレベルは高いなど、社会的要求度によって求められるセキュリティレベルが違う。全ての業種を一緒に扱うとプラクティスの利用者をミスリードするおそれがある。
- 製造業や非製造業という大きい区分だと、各企業にとってプラクティスが自社に関係しないように思われ使いづらい。
- 企業規模によっても異なるセキュリティのアプローチが必要である。企業規模をある程度想定しないと対策イメージが見えてこない。
- 事例の公開は難しい(業界団体内などクローズドな範囲では共有されやすい)。事例の最終公開イメージを用意するなど工夫が必要である。
- 事例で、組織名を公開するとその組織の脆弱性を開示することになる。匿名化すると意識喚起のレベルが下がる。バランスが難しい。
- 組織がシステムの状況把握をした上でセキュアな環境を作っていかないと、プラクティスを出しても実効性が乏しい。
- 機器の接続やソフトウェアのバージョンなど、構成管理の正確さと迅速な対応が、セキュリティ対策における大事なポイントである。
- サプライチェーン全体にまたがる基準を出し、セキュリティ経営ガイドライン10項目のそれぞれどこまでやるべきか明らかにする必要がある。
- セキュリティ対策をどこまで実施すべきかは、それをやらないときの社会の反応を描いて考えるとよい。
- サイバーセキュリティ経営ガイドライン10項目に対して具体的に何をどこまでどうやって伝えればいいかがわかるアウトプットイメージがよい。
- リスクマトリクスそのものを示すよりは、自社に合わせてリスクマトリクスを作るプロセスとプロセスにおける課題があるとわかりやすい。
- サイバーリスクをビジネスリスクとしてとらえ、経営に理解してもらうためのマテリアルコンテンツを提供したい。
- 事例収集するときにどう公開されるのか説明できるよう、成果物のイメージを事前にまとめておくとよい。
- 収益とリスクのバランスを考える必要がある。例えば、シンクライアントとSaaSの組み合わせのようなトータルのサービスの中で考えていかないと難しい。
- アンケート結果はセキュリティ対策の参考というより、全体の傾向を俯瞰するために用いるのがよい。

【可視化の課題について】

- 規模の異なる企業をひとつの可視化ツールにのせて評価することは厳しい。
- 可視化ツールの項目の中でサプライチェーンにおける個々の二者間チェック項目がある程度標準化されていると有効である。
- 可視化ツールのセキュリティ対策項目は具体的な実施イメージをもって作成するとよい。例えば従業員への教育は具体的にどうすべきか、など。

以上