第３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 11 月 14 日（水）15:00-17:00　　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、小松委員、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
IPA 横山グループリーダー、大谷氏、木下主任研究員

[事務局]　IPA 瓜生セキュリティセンター長、小川グループリーダー、木内研究員、ジリエ研究員
PwC あらた有限責任監査法人　平岩ディレクター、海老原マネージャー、高木氏、石川氏

議事概要

第三回検討会では、IPAより「サイバーセキュリティ経営プラクティス作成」のためのアンケート・インタビュー実施状況、プラクティスドラフトの作成状況の説明ならびに、「可視化方式調査」状況についての説明の後、委員と意見交換を行った。委員からの意見は以下の通り。

【サイバーセキュリティ経営プラクティスの作成方針について】

①　情報セキュリティとサイバーセキュリティの関係整理について

- 従来からの個人情報保護といった内部対策としての情報セキュリティ対策を踏まえながらも、外部攻撃者を想定したサイバーセキュリティ対策のプラクティスを提供するアウトプットが良いと考える。その上では、サイバーセキュリティとは何か、情報セキュリティとは何か、本プラクティスにおける用語の使い方を整理するべきである。
- サイバーセキュリティ経営ガイドラインは、サイバーセキュリティだけを意識している訳ではないと考える。情報セキュリティ対策はサイバーセキュリティ対策の前提、並びに足場であることを伝え、想定活用企業が求めるサイバーセキュリティ対策のプラクティス、特にサイバー目線でのリスク管理や教育について、提示することが有用である。

②　プラクティスの内容について

- サイバーセキュリティに関する教育プログラムは少ない。特に e-learning は情報セキュリティに関するものが主であるため、サイバーセキュリティ教育コンテンツは重要であり、今後の課題となるものである。
- 構成管理については、定量的に把握することが重要である。ただし、システムの運用委託先がマルチベンダとなる場合は、各ベンダが自身の担当部分の構成しか把握したがらないこともあるため、「構成管理」よりも、「数えられる」や「どこに何がある」と言い方を工夫した方がよい。
- サプライチェーンの考え方は、委託先管理と調達の 2 系統がある。サイバーセキュリティ経営ガイドラインとして求めるサプライチェーンの基準を明確にして 2 系統を出すのがよいのではないか。
- JUAS ワーキングで共有している各社のクラウドに関する委託チェックシートを共通化するとプラクティスにできるのではないか。

③　プラクティスの構成について

- 指示項目の順序に則り、ポリシーに関する事項を冒頭で記載すると、企業がポリシーを策定することで安心してしまうことが懸念される。サイバーセキュリティに関するインシデント事例や危険喚起のメッセージを先に伝えてから、後にポリシーの話を出してもよいのではないか。

【可視化方式調査について】

- IPA のベンチマークの拡張を考えたい。その場合、海外のメジャーな可視化方式とのマッピングができたほうがよい。
- 自己評価の結果を認識し、これからどうしたら良いのか、どういうアプローチをしていけば良いのか、How を求めている企業が多い。実効性のあるツールにするために、How を明確にして企業が従うべき道筋となるようにした方が良い。

以上