第５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 31 年 2 月 21 日（木）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、小松委員、教学委員、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　加畑課長補佐、元木係長

IPA 大谷氏、桑名副部長、塩田研究員

[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　綾部パートナー、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５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」の成果物および、今後の方針について説明の後、委員と意見交換を行った。委員からプラクティス集についての意見は以下の通り。

第１章

- サイバー攻撃は大企業だけにとどまらず、子会社や取引先が狙われる傾向にある。サイバー攻撃の被害は自社だけでなく、ネットワークで繋がる取引先や関係会社に及ぶため、加害者となるリスクがあることを伝えたらどうか。
  また、グループセキュリティとサプライチェーンは今後のキーワードにもなるため、強調したほうがよいと考える。
- サイバー攻撃件数は増加しているが、被害をもたらしている件数だと減少傾向になっている。サイバー攻撃を受けても、自社への損害にとどまる場合は、公表していない企業が多く、メディア報道もされていない。経営者の中にはサイバーセキュリティの危機感が落ち着いてしまった人もいるため、伝え方を工夫したほうがよい。
- サイバーセキュリティリスクという言葉に馴染みのない人も多い。サイバーセキュリティリスクはどのようなものかを伝え、理解させるような内容を追加することが望まれる。

第２章

- 指示１でそもそもサイバーセキュリティリスクとは何か、例示があってもよい。
- 指示３について、育成よりは人材の確保を強調したらどうか。
- 例えば、標的型メールは 10 年近く前までは９割以上をアンチウィルスソフト等で検知できていたが、今は防ぐことが難しくなってきているため、エンドポイント・セキュリティの管理は重要なポイントであると考える。

第３章

- 経営者へのサイバーセキュリティリスクの意識付けとして、経営者を対象とした社内外の研修やセミナーへの参加は良案だと考える。経営者同士の情報交換や意識共有することでサイバーセキュリティへの危機感も強化されると考える。
- 「インシデント対応経験がない要員で CSIRT を構築したが対応に不安がある」という悩みについては、経験のない人たちでのローテーションは難しい。専門家からのナレッジトランスファーが重要である点を記載すべきと考える。
- クラウドサービスの利用がセキュリティレベルの向上に繋がるわけではないので、伝え方を工夫したほうがよい。自社で守るべき部分とクラウドベンダーが担う部分を切り分けて考える必要があると考える。
- サイバー保険では、個人情報漏えい保険とサイバー保険の補償内容の違いを記載したらどうか。サイバー保険では、個人情報以外の重要な預かり情報の改ざん・漏えいやシステム停止等による業務中断に対する補償が可能なケースもある。
- インシデント発生時のフォレンジックに係る調査費用が高額であるために稟議に時間を要してしまう懸念から、即時で対応できるようサイバー保険を利用しているケースもある。
- セキュリティマネジメント認証については、セキュリティ管理体制の一取組みとして推奨するような伝え方がよいと考える。

構成について

- IPA資料の図は一番前にあってもよい。
- 経営ガイドラインチェックシートに対応したプラクティス一覧がプラクティス集と別刷りであるとよい。

以上