サイバーセキュリティ経営プラクティス検討会 第２回

日時・開催方法　令和５年９月４日（月）10:00-12:00　Teams によるオンライン会議

出席者

[委員]　橋本委員長、小川委員、落合委員、教学委員、佐藤委員、土佐委員、丸山委員

[事務局]　IPA 小山グループリーダー、安田エキスパート、小杉研究員
みずほリサーチ＆テクノロジーズ(株)　冨田氏、鈴木氏、石岡氏

[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 三田課長補佐、岩佐係長
産業横断サイバーセキュリティ検討会 荒川事務局長代理

配布資料

資料１　議事次第・委員名簿等
資料２　インタビュー概要等
資料３　追加プラクティス案
資料４　現行プラクティス集更新案

議事概要

第一回に続き、橋本正洋氏に委員長を務めていただく。また、本検討会は非公開とし、議事要旨のみ公開する。本検討会では、事務局より、企業へのインタビュー概要等と追加プラクティス案・現行プラクティス集更新案について説明の後、自由討議を行った。委員からのご意見は以下の通り。

【追加プラクティス案について】

案① 経営層やスタッフ部門等の役割に応じた、リテラシーにとどまらないセキュリティ教育実践

- 訪問介護サービスでは、ITに詳しくない契約社員／非常勤のヘルパーさんが多く、顧客の個人情報保護も重要な課題である。ヘルパーさんに対する教育もケアマネージャ（正社員、事業部門）の仕事である。
- 教育において「なぜこのルールがあるのか」を丁寧に伝えることが大切である。「なぜ」が分かると、目的に応じた改善や提案が現場から出てきたり、応用がきいたりする効果がある。

案② 「サイバーセキュリティ経営可視化ツール」を用いたリスク対策状況の把握と報告

- グループ会社や仕入れ先にも可視化ツールを紹介して使ってもらうことを入れるとよい。

案③ サイバーセキュリティ対策において委託すべき範囲の明確化とその管理

- ステークホルダ・顧客対応等、外部に任せられないものもある。第一者の当事者責任は委託できないということを明示しておいた方がよい。
- ルールの策定や教育コンテンツの作成など外部に頼む必要がある場合もあるため、コンサルともコミュニケーションをとる必要があるということを追記するとよい。
- 自社対応と外部委託を比較した表で、2番目の項目を通常のマネジメントとして「通常のセキュリティマネジメントノウハウの蓄積」と表現としてはどうか。

案④ ITサービスの委託におけるセキュリティ対策を契約と第三者検証で担保

- 「第三者検証」という言葉の使い方と実施タイミングについて表現を検討してほしい。第三者の診断で問題が判明した場合

の処理をどう位置付けるかについても触れておくとよいのではないか。

- いくつかのプラクティスでクラウド活用が出てくるが、クラウドには設定ミスなどのリスクもあるので、参考として共有モデルについて入れるべきではないか。

案⑤ 事業部門によるDX推進をセキュリティ確保の観点から支える仕組みづくり

- 200人規模の組織では、セキュリティルール見直しと試行実施の間はもっとインタラクティブになるのではないか。試行段階でもフィードバックがあってもよい。
- 事業部門もプラスセキュリティ教育を受けることを追加してはどうか。

案⑥ CSIRT業務の属人化回避も兼ねたインシデントや脅威に関する情報の共有・蓄積

- 参考資料の表示順について、参考資料のFIRSTのフレームワークは専門的なので順番を下げ、NCAの構築ガイドラインを先に示した方がよい。

案⑦　無理なく実践するインシデント対応演習

- IT 系・OT 系を完全に分けて行う印象を与えないよう、一部の演習では一緒に実施した旨を記載した方がよい。

案⑧ サプライチェーンで連携する各社が『自社ですべきこと』を実施する体制の構築

- 8000人規模の企業では、事業部へのお願いが悩みどころで、協力体制やネゴシエーションが必要になるのではないか。
- アンケート調査項目はレベルごとに異なり、小規模事業者に対しては厳しいことは尋ねないとしてはどうか。
- 第三者認証を取得していて適用範囲に入っていればアンケートを省略できるような観点があってもよい。
- サプライヤーを管理している購買部門の教育も必要である。IT部門からダイレクトにサプライヤーにアプローチできるのかという視点があってもよい。
- 委託先への要請については、独禁法の優越的地位の濫用に違反しないか、下請法に違反しないか、という観点がある。
- 優越的地位の濫用については公正取引委員会が指針を出している。
- 再委託先を含める／一次委託先だけにする、これらについて整理して記載してほしい。
- 「違反」は「満たされなくても」や「未達」の方がよい。「パートナーシップ構築」は「取引先連携」などの表現がよい。
- 「重要な業務においてはすべての委託先を把握することが重要となる場合があります／考えられます」と記載してはどうか。重要な業務や社会的な影響が大きな場合、「全てを把握した委託先にしか提供しない」という考え方もあるということを記載しておく方がよい。
- 一次委託先が実は大企業でしかも顧客である場合や、再委託先が大企業である場合など、チャネルによっては末端の委託先までたどり着けないことがある。そういった場合を考慮して、一次委託先である程度担保するための工夫の記載があってもよい。

原案⑨ 『情報の共有・公表ガイダンス』に基づくCSIRTと社内外関係者との連携推進

- 委任による弁護士との連携や弁護士費用についての保険の考慮などにも触れておくとよい。

【現行プラクティス集更新案について】

プラクティス 4-1

- サイバー攻撃の事例としてランサムウェアを入れるとよい。

プラクティス 7-3

- 追加プラクティスと内容が被る印象を受けるが、別内容ということであればよい。

プラクティス 8-2

- 扱う事例が小さいので、演習のプラクティスにメンテナンスに関する内容として記載する方がよい。

プラクティス 10－2

- これは対策に関する「情報共有」であることが分かるように記載した方がよい。

取組(３)

- 海外の拠点に対して担当者を集めているという記載があるが、施策としては現地に行って状況を見るほうが有効ではないか。

取組(15)

- 保険会社はインシデント対応の支援を行っており、CSIRT の代替的機能を持っているので、中立的なインフラとして活用可能であることを記載してはどうか。

その他

- 第三者認証を取得していても事故を起こすことがあり安心はできない。重要な業務であれば、委託先に対して踏み込んでやり方等について確認することも必要になる。

事務局からの回答などは以下の通り。

- 頂いたご指摘について、対応方法を検討する。
- 案⑧について、現在の２ページを３ページに拡張して対応する。

決定事項

- プラクティス集 PDF のリリース時期について、10 月末予定とする。

以上