サイバーセキュリティ経営プラクティス検討会

日時・開催方法　令和 5 年 6 月 26 日（月）15:00-17:00　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 高柳セキュリティセンター長、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、栗山氏、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　第一回会合　議事次第・委員名簿（本資料）
資料 2　情報の取扱い等について
資料 3　プラクティス集の改訂方針等
資料 4　経営 GL とプラクティス集の対応関係
資料 5　追加プラクティス原案

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。本検討会では、事務局よりプラクティス集の改訂方針と追加プラクティス原案について説明の後、自由討議を行った。委員からの意見は以下の通り。

【プラクティス集改訂について】

全体

- テーマの優先度付けはどうなっているのか。
- 公開方法について、Web形式で段階的にリリースするなど、従来のPDF形式にこだわらない方法をとってもよいのではないか。
- ３月の経営GL改訂はどこまで意識しているのか。
- 当時のサイバー保険は経済的に補償する機能であったが、昨今は、インシデントレスポンスで専門家の知見をプラットフォームとして活用できる機能を提供している。インシデント対応の体制構築（指示７）のプラクティスとして、サイバー保険の活用により専門家の知見をプラットフォームとして活用というシナリオもよいのではないか。
- インタビュー先は、１か月の期間でカバーできるのか。
- プラクティス集は現在のものだと100ページ程度あるが、タグ等を活かして検索性を高めた方がよい。WEB版サービスのプラクティス・ナビは、プラクティス集と内容を一致させるとよい。
- 状況が変わっており、既掲載プラクティスで古くなった部分については修正・更新の必要性をセットで検討すべきではないか。
- プラクティス集の想定読者は、おそらく経営ガイドラインの読者と同じと認識している。

原案① 経営層やスタッフ部門を対象とした、セキュリティ意識向上の教育や訓練など、プラスセキュリティの浸透に関する取組

- プラスセキュリティの定義を明確にし、プラスセキュリティに関する教育は、全社員向けのリテラシー教育のようなものではなく、もう少し業務ごとにバリエーションをもたせた教育をするようなことのほうが相応しいのではないか。

- 現在のリテラシーに何を足せばプラスセキュリティになるのかがわかるプラクティスにするとよいのではないか。

原案② 実施状況を定量的に把握し、成熟度レベルの継続的な改善など、可視化ツールの効果的な活用に関する取組

- 可視化ツール Web 版の診断結果で、対策ができていないものについて、プラクティスのテーマとして考えられるのではないか。
- 対応できていないものに対する残留リスクの承認を経営層がしっかり請け負うことで、システム部門が動きやすくなるという事例があるとよい。
- 自社の内容を可視化ツールで評価することに加えて、取引先、グループ、委託先などに可視化ツールを使ってもらうように働きかける、あるいは自分のところの評価結果をそういったところに提示するようなことを入れ込むとよいプラクティスになるのではないか。
- なぜ可視化ツールなのかが欲しい。「可視化ツールを使って経営層にこのように説明するとこのようなよいことがある」というシナリオに経営層を登場させるなど、可視化ツールのベストな使い方等が示せればよいのではないか。

原案③ 内部対応した場合と外部委託した場合のコスト、メリット、デメリットを比較した上で最適な切り分けを実践する取組

- 「コスト」という用語は削減しようという意識が働くので、「コスト」とは別の単語（予算金額、投資額、対策費など）に置き換えてはどうか。
- 外部委託する領域がどのような部分なのかの説明があると、よりわかりやすい。
- 責任分担の切り口でもうすこし先鋭化してもよいのではないか。「責任分担といっても実際はあいまいになりがちだが、ここはしっかりやった」というものにしてはどうか。

原案④ コスト以外の観点も含めた外部委託先の選定基準を策定することで、委託先に起因するリスクを低減する取組

- 「コスト」という用語は削減しようという意識が働くので、「コスト」とは別の単語（予算金額、投資額、対策費など）に置き換えてはどうか。
- セキュリティ業者に関する9-2の観点も加えてもよいのではないか。サービス品質や技術力だけではなく、セキュリティ業者のセキュリティ評価をクローズアップしてもよいのではないか。
- IT製品やサービスの選定ではコスト優先になりがちである。セキュリティ面を強調した検討が必要というメッセージを示すことが重要なのではないか。
- ITサービスを外部委託する際のIT事業者の選定基準なのか、あるいはセキュリティ領域（どういう領域）を外部委託するのか分かりにくい。調達先のセキュリティが大丈夫かどうかを知りたい場合の方法論に関する説明を事例として出すことにしたい。
- ITベンダーにIT業務を委託しているのが、セキュリティの観点で適切なのかどうかを知りたい。それをさらに外部委託するような局面もあると思うので、そのようなことに対応できる企業なのかどうかを確認した上でストーリーを書くほうがよい。

原案⑤ DX推進に伴うサイバーセキュリティリスクの変化をアセスメントし、その結果を踏まえた対策の見直しを実践する取組

- データを守るのか、システムを攻撃から守るのか、プラクティスにするのであれば、もっとシンプルに書いたほうがよい。
- DX白書によると、デジタル化は行ったがデータドリブンはまだという状況かもしれない。データドリブンなプラクティスを求めることは、時期尚早かもしれない。システムを守ることになるのかもしれない。

原案⑥ 過去のインシデント対応履歴を整理・分析することで、人材育成及び組織の知見向上に活用する取組

- インシデント管理は、過去の自社の蓄積よりも、次々に起こる新しい出来事を外から学ぶ観点で表現するのがよい。トレーニーの指導をプラクティスとして書くのであれば、新しいことを学び、技術の進展に追従してけるCSIRTにしていくニュアンスを入れるとよい。

原案⑧ サプライチェーン内にサイバーセキュリティリスクを理解できる人材を状況に応じて配置することで、各社の置かれている状況に応じた対策の実践を進める取組

- 建設業協会でかなり意識が高く、高い責任感を持っている企業がある。そのようなところにヒアリングしてはどうか。
- サプライチェーンについて課題感をもっている企業が多く、うまくいっている企業のほうが正直少ない状況であるので、課題を抽出していけるのはないか。
- 元受けが孫請け以降までを本当に見なければならないのかというように解釈されることにならないよう、読者にどのように受け止められるかを考慮した上で、モデルを工夫するのがよい。

原案⑨ 社内で観測されたインシデントやその未遂となる事象について、予め定められた手順に基づき社外に情報提供・共有する取組

- モデル企業としてMSSなどを利用せず自社でやっている大企業に限定すべきではないのではないか。
- インシデント情報の出し方は、何でも出しますというのでは誤解を招く。開示は企業にとっての重要なポイントなので、そのあたりは慎重にプラクティスを作ることが重要なのではないか。

事務局からの回答は以下の通り。

- テーマの優先度付けについて、追加プラクティス原案９件のうち、必須の２件を含め７件までをやりたいと考えている。
- 公開方法について、Web形式の実現性については今後検討する。
- ３月の経営GL改訂について、経営GLの改訂内容を意識しつつも、プラクティスの中身が重要であると考えている。
- インタビュー先の確度について、これまでの経験上2～3割のお断りはあっても、現在ノミネートしている企業のどこか1社に回答いただけるのではと考えている。
- 既掲載プラクティスについて、委員の皆様で「ここは少なくとも直すべき」というものがあれば別途ご連絡いただきたい。
- プラクティス集の想定読者について、基本的に経営GLと同じ300名以上の企業・組織をターゲットとし、規模に関係ない読者層を想定している。

以上