【総論的な意見】

・該当箇所　　全体

・意見内容

●当該ガイドラインに沿った施策をしている場合の財政上・税制上の支援を今後セットで検討いただきたい(特に中小企業対策)

●政府として、企業内部でのセキュリティの意識レベルの向上を図るだけでなく、一般社会のセキュリティ意識の向上を図るため、啓発活動を強化すべきである。

・理由

●当該ガイドラインに沿った施策を進めるためには、特に中小企業では経済的なメリットがセットでないと難しい面がある。必要な経費の補助、借入優遇、税制支援等の検討が必要。

●まずはできるところ、例えば大手からというのは本末転倒であり、中小企業こそがねらわれやすい。中小企業のインターネットサイトがハッキングされ、そこから流出したメルアドとＰＷで、セキュリティー対策をしている大手も不正アクセスされる可能性もある。したがって、中小企業を含めた対策の推進が必要不可欠。

●日本社会全体のセキュリティレベルを向上させるには、企業だけでなく利用者への啓発活動の強化も必要不可欠である。たとえば、一般インターネットユーザーには、ID、メールアドレス、パスワードを利用するサービスごとに変えるようにすることを訴求する必要がある。

[個別意見①]

・該当箇所

ｐ９(３)目標と計画の策定

P10.(４)ＰＤＣＡと対策の開示

・意見内容

経営層への説明フォーマットとして参考になるものを開発して横展開を図るべきである。

・理由

●企業ボードメンバーによるセキュリティ対策に対する意識を向上させるためには、事務方からの効果的な説明手法が開発されている必要がある。例えば、ストーリー・テリングを活用して共通目標を設定する手法の標準化と横展開である。セキュリティ事故が自社の売り上げ利益にどれだけ影響を与えるかなどを経営層に認識してもらうとともに、社内関係者間で対立構造を乗り越え共通の目標を設定する手法を開発すべきでその手法や成功事例を各企業へ展開してくことが必要。

[個別意見②]

・該当箇所

P12. 3.3.（6） サイバーセキュリティ対策のための資源確保

・意見内容

●社員へのセキュリティ教育の重要性とそれへの資源確保を記述していただきたい。

(例)

①情報にアクセスする社員向けの、情報セキュリティ教育の促進

・新入社員・中途入社社員に対する基本教育の実施

・毎年の定期教育の実施(変化するＩＴ技術、セキュリティ脅威に合わせて内容更新)

・管理者権限(特権)所有者(ＩＴ管理者や経営層)向け教育の実施

②セキュリティチェックの促進

・チェック徹底による各企業・社員のセキュリティ意識の標準化

・例えば、1 年に 1 度、50 名以上の事業所を対象

・チェック結果に対しての相談先を官民連携で用意し改善サイクルをまわす

・理由

●会社のセキュリティを向上させるには、直接担当する者だけでなく全社員を中心とした意識向上とそれのための具体的な仕掛けが必要である。

[個別意見③]

・該当箇所

p14.（8） 情報共有活動への参加

・意見内容

民間団体等で行われている情報共有の仕組みも積極的に活用するべきであることを追加で記述してもらいたい

・理由

●情報共有の場の必要性が従来より訴えられており、民間等でもそのような動きを作る試行錯誤の動きがあり、そのようなところへの積極的な参加も期待される。

[個別意見④]

・該当箇所

P.25（4）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

・意見内容

以下の要素の追加を検討いただきたい。

●PDCA サイクルの中に、情報システム部門だけでなく、各部門による定期確認を含めること。

●端末の利用状況をモニタリングし、自組織内の端末利用内容（操作ログ）を確認し不審な動きが無いかを確認する等、部門ごとのセキュリティ対策を講じること。

●端末の操作ログはクライアント端末に最低３ヶ月以上保管すること。

●企業ごとに「不審な動き」を定義すること。また、インシデント発生後、セキュリティインシデント情報をもとに証跡であるログから原因を分析し規定やルールを随時見直しすること。

・理由

●それぞれのチームごとに不審である内容の定義が異なるため、各チームでの管理が必要。

●また、情報システム部門のみでの管理の場合、管理コストを多大に費やす。部門ごとに管理することで、管理コストを低減させることができ、さらに、何かインシデントが発生した際に、即座に対応が可能となる。

●長期間ネットワークに接続できない場合でも、証跡を残すため、最低でも３ヶ月はクライアント側に履歴を残し、後日収集できる仕組み・体制があることが望ましい。

●定義を明確にすることで管理者が判断しやすくなり、チェックしやすくなるため管理コストを抑えることができる。また、社内と社外問わず、発生するインシデントは常に新しくなるため発生する度に規程やルールを見直ししなければ、セキュリティホールが大きくなりリスクが高くなってしまうため。

（了）