サイバーセキュリティタスクフォース 情報開示分科会（第２回）議事要旨

1. 日 時：平成 30 年 2 月 1 日（木）13:00～14:30

2. 場 所：中央合同庁舎２号館 ８階　第１特別会議室

3. 出席者：

【構成員】

岡村主査、秋保構成員、石原構成員(代理：教学)、鵜飼構成員、大杉構成員、加藤構成員、源田構成員、野口構成員

【オブザーバー】

小柳聡志(経済産業省)

【総務省】

谷脇政策統括官（情報セキュリティ担当）、柳島情報流通行政局参事官（行政情報セキュリティ担当）、木村サイバーセキュリティ課長、澤谷サイバーセキュリティ課課長補佐

4. 配布資料

資料２－１ リスクマネジメントの視点による情報開示

資料２－２ セキュリティ対策に関する情報開示とサイバー保険について

資料２－３ 情報開示分科会（第２回）プレゼンテーション資料

資料２－４ 論点の整理

資料２－４－１ サイバーセキュリティ総合補償プランのご提案

資料２－４－２ サイバーセキュリティ総合補償プラン ヒアリングシート

資料２－４－３ 設立目的・機能と全体像（案）

資料２－４－４ CRCC が想定するサイバー保険の構造（イメージ）

資料２－４－５ CRCC（サイバー版 JAF）の三位一体機能・効果

資料２－５ 第１回分科会における構成員の御意見

資料２－６ 情報開示分科会の今後のスケジュール（案）

参考資料１ サイバーセキュリティタスクフォース 情報開示分科会（第１回）議事要旨（事務局）

5. 議事概要

(1) 開会

(2) 議事

◆ 野口構成員より、資料２－１「リスクマネジメントの視点による情報開示」について説明 (省略)

◆　秋保構成員より、資料２－２「セキュリティ対策に関する情報開示とサイバー保険について」を説明 (省略)
◆　石原構成員(代理：教学)より、資料２－３ について説明 (省略)
◆　源田構成員より、資料２－４「論点の整理」について説明 (省略)

◆　構成員の意見・コメント

岡村主査)

インシデント発生後に、事前の告知事項として規定されている事項の申請内容が、実際の状況と一致しているかどうかを事後的に確認・検証することになるが、申請されている内容が実際の状況と一致していなかった場合のペナルティについては、どのような規定となっているか。

秋保構成員)

約款上で告知義務違反を規定しており、例えば保険の引受可否の判断に影響するような重要な項目について違反があった場合等は保険金を支払わないという対応もあり得る。保険料算出のための要素等、引受可否に影響しない項目の違反については､追徴等により告知違反がなかった場合の正しい保険料に修正をした上で保険金をお支払いするという対応になる。

石原構成員(代理：教学)

日本国内では初の保険だったため、当社がこの保険を開発するときには契約時に提出していただく質問書の位置づけはかなり検討した。当社では質問書で 36 問の質問を聞いているのだが、現時点の我が国のサイバーセキュリティを取り巻く環境を踏まえると、例えば企業によって CSIRT の基準が異なるなど質問項目に対する回答基準も各社ごとに異なる可能性が高いこと、また、ウィルス対策ソフトウェアを入れていますか？との質問に対して PC 1 台でも導入していれば OK なのか､全ての PC に導入していなければならないのかというように保険会社が作成する質問書の内容も定義が明確でない部分が存在するなど、現行の引受実務で告知義務違反を厳格に運用すること自体が非常に困難であることから、告知事項ではなく単なる保険料割引の質問項目としてのみに使用する運用とした。

今後は企業のセキュリティ意識の向上やセキュリティ基準の明確化により、より適切な運用が可能になる時代が来ると考えているが、現時点ではセキュリティ対策の実施状況に関する基準が明確となっていないため、割引もマイルドなものとなっている。

源田構成員)

約款上は、告知義務違反を問うことができるようになっている。たとえば、自動車保険の場合で、免許証の色を間違えて申請する人が多くいらっしゃるが、このようなケースで、告知義務違反に問えるのかという議論はある。

どのような内容の質問をしているのかを確認の上、個々のケースごとに対応することになる。

保険を引き受ける時にどのようにしたのかということも確認することになる。

岡村主査)

火災保険の場合で、故意免責の対象となったケースがある。サイバーセキュリティの場合は、どのようになるのか。

実効性の確保が課題となるのではないか。

大杉構成員)

保険のモラルリスクの問題がある。保険に加入することにより安心してしまい、セキュリティ対策をしなくなるという問題である。商品の設計・運用で、どのような対策を行っているのか。

秋保構成員)

保険事故があった企業に対しては、契約更新の際に改善策実施の有無を確認し条件変更や保険料引上げ等の対応を取っている。また、全く改善する気がないような場合には引受けをお断りする可能性もあるため、そういったモラルリスクに対する一定の抑止力にはなっているのではないか。事故の有無に関係なく保険加入後のセキュリティ対策状況を確認するといたことは現状、行っていない。

石原構成員(代理：教学)

加入時には質問書でリスク対策の実態を確認することで、リスク対策を行っている企業は保険料が安くなり、対策を怠っていれば保険料が高くなるという評価の仕組みがあることで一定程度の防御策となっていると思われる。ただし、保険加入後に保険会社が企業のセキュリティ対策を継続的に促すことには限界がある。当社としては、これらへの対策としてサイエンス社との提携による企業毎のリスク実態分析により、当該企業のリスク実態を直接評価できるアンダーライティング体制の構築を検討している。

源田構成員)

保険に加入することにより安心してしまい、セキュリティ対策をしなくなるということはないと理解している。

新たなリスクへの対応については､契約者に対して継続して注意喚起や対策実施推進を行うためのツールを用意している。

サイバーセキュリティ保険は、説明が難しいので、企業に対してアドバイスを行うための体制も必要である。

岡村主査)

資料２－５に基づいて議論したい。①について、いかがでしょうか。

鵜飼構成員)

開示内容の正確性を担保することが難しい。保険でセキュリティを担保しているということを開示対象とするということもあってよい｡サイバーセキュリティリスクを定量的に測定することができないと､サイバーセキュリティ保険は難しい。前提として、セキュリティ対策がどこまで担保できているかが重要である。

サイバーセキュリティ保険が普及していないのは、リスクが保険料に上乗せされている結果、保険料が高くなってしまっていることもあるのではないか。セキュリティ対策を実施している企業については保険料を下げるということをしないと、普及は難しいのではないか。

加藤構成員)

開示の方法、開示内容の粒度、開示内容の正確性の担保について、有価証券報告書に記載した場合の社会へのインパクトという観点で考える必要がある。サイバーリスク全体を開示対象とするのか。開示対象を広げると、人の問題を含めて難しくなる。提言としてまとめるには、開示の観点や、誰が見るのか等について、レベルや広さを規定する必要がある。既存の取組との整合をとるということでは、ISMS を取り込んでもよいのではないか。

サプライチェーン全体への影響について、どのように考えているのか？

石原構成員(代理：教学)

現在、大企業がその子会社、関連会社を包括的に付保する動きはある。一方で資本関係のない下請け会社はそこには入れない。

サプライチェーンの上流にいる企業が取引先にサイバーセキュリティ保険に加入していないと取引しないということを求めるというようなことになっていけば､インシデントが発生した場合に保険を活用して調査を迅速に実施することができ、サプライチェーンの復旧を迅速に行うことができるというメリットはあるが、誰が保険料を負担するのかなど現実的には難しい部分もある。

岡村主査)

続いて、② について、いかがでしょうか。

大杉構成員)

重要なのは、サイバーセキュリティ人材に対する適切な評価が行われているか、サイバーセキュリティが会社全体の課題として捉えられているか､PDCA サイクルに基づいてサイバーセキュリティの継続的な改善が行われているかということであるが、有価証券報告書のリスク情報の欄に記載することにより、サイバーセキュリティに対する取組が改善されることにはならないのではないかという懸念がある。むしろ、保険会社への告知など、個々の企業間で相対で情報提供を行う方が効果的ではないか。

野口構成員)

誰にとって望ましいのかという観点が抜け落ちている。開示することにより、どのような効果があるとよいのか。フォーカスが明確になっていない。セキュリティ対策についてどこにも書いていないというのは、この事業者は、セキュリティに関心がなく、書く能力もないという、一種の情報開示になっている。

社会全体のリスクという観点でみると、サイバーセキュリティ保険によってリスクを負担する主体が変わるだけで、全体としてのリスクは何も変わっていない。

岡村主査)

誰にとって望ましいのかという観点は重要であると考える。

源田構成員)

サプライチェーンという観点においては、取引先にサイバーセキュリティの重要性を理解してもらうことが重要である。

サイバーセキュリティ上の事故・インシデントが発生した場合の経済的な損失をカバーするための一つの方法がサイバーセキュリティ保険である。企業価値の向上という観点でサイバーセキュリティを捉えるべきである。

また、複数の企業がつながることにより、サプライチェーン全体の強化につながるという観点が重要である。

事務局)

サプライチェーンという観点で考えると、サプライチェーンに一箇所でもセキュリティが弱い部分があると、製品・サービスのセキュリティに影響するということになる。サプライチェーンの中に、サイバーセキュリティへの取組に関する情報を開示していない企業が存在すると､サプライチェーン全体が弱くなる可能性があるということに留意する必要がある。本日いただいた意見を踏まえて、今後の進め方を検討する。

第３回分科会を２月下旬に、第４回分科会を３月中旬に開催する予定である。

岡村主査)

本日以降、何か意見がある場合に、電子メールにより事務局に提出することは可能か。

事務局)

可能。

以上