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３回）議事要旨

1. 日 時：平成 30 年 2 月 27 日（火）10:00～12:00

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、鵜飼構成員、大杉構成員、梶浦構成員、加藤構成員(代理：栗野)、源田構成員、野口構成員

【オブザーバ】

曽我部雄太(経済産業省) 、山下浩司(内閣サイバーセキュリティセンター)

【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)、福島サイバーセキュリティ課調査官、澤谷サイバーセキュリティ課課長補佐

4. 配布資料

資料３－１ 企業のセキュリティ対策に係る情報開示の実態等に関する調査

資料３－２ 「情報開示分科会」論点整理

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２回）議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆ 事務局より、資料３－１ 企業のセキュリティ対策に係る情報開示の実態等に関する調査を説明 (省略)
◆ 事務局より、資料３－２「情報開示分科会」論点整理を説明 (省略)

◆ 構成員の意見・コメント

野口構成員)

資料３－２ P2 の 3 番目の項目・内容が論理的ではない。サイバーセキュリティに関する情報開示は、投資家保護・ステークホルダーへの情報開示が目的であり、開示したからといってサイバーセキュリティ対策のレベルが向上するわけではない。今の情報セキュリティは担当部署と経営者だけでなく、むしろ組織全体でどうやって情報を共有するかということが大事。

③ について、サイバーセキュリティ対策の向上との関連がみえない。

市場評価が変わる、セキュリティの差異が出るような情報開示の内容は何かということを示すべき。

P6 について、サイバーセキュリティ保険というようなリスク対応の話は、情報開示と直接的な関係はないのではないか。

P7 について、これまでのように、行政が用意した仕組みにのっかるのがよいのかについて、もう少し議論が必要ではないか。

P12 について、情報セキュリティ保険に加入してくださいというメッセージにみえる。情報開示の方法としてはやり過ぎではないか。分析が必要である。

情報開示が情報セキュリティの向上につながるのかということについて、もう少し分析が必要ではないか。

大杉構成員)

P2 情報を開示することにより経営者が自覚するかどうかについては、必ずしも明らかではないが、一定の書類については、取締役会にかけることになっている。会社法上の事業報告書に記載するのが法律上は確実であるが、その記載事項とするのは、やり過ぎという感もある。

有価証券報告書のリスク情報は、投資家に対するリスク開示なので、情報セキュリティ対策を実施しているので安心ですというような楽観的なことは書くべきではない。

取締役会・経営会議で横の共有がされると同時に、社外取締役・監査役が目を光らせている必要がある。上場企業を対象とするのであれば、社外取締役・監査役の目に留まるような形での開示がよいのではないか。

どの文書において情報を開示するのかということについては、有価証券報告書とコーポレートガバナンス報告書は必ず作成するものであるので、これらのどこかに記載しておき、ウェブサイトにもアップロードしておけばよいのではないか。CSR 報告書を作成している先進的な企業の場合、開示情報が記載されている文書を参照先として記載しておくことでもよい。

岡村主査)

社内全体の問題ということは当然のことである。技術に詳しくない経営者の場合、サイバーセキュリティに関する内容が反映されないことが多い。経営者と担当部署の関係は、引き続き押さえておくことが重要である。

岡村主査)

大杉構成員に、会社法上の内部統制の管理体制のディスクロージャーシステムがどのようになっているのかということと、事故発生時の情報開示について補足をお願いしたい。

大杉構成員)

内部統制システムには、リスクの所在を把握し、誰が、どの部署が責任をもって対処するのかを取締役会で決めておき、担当者がそれぞれの役割を果たすことにより、マイナスを防ぐというだけではなくて、会社の中の情報の流れを把握することにより、ビジネスチャンスをつかむようなプラス面にも反映していくことが期待されている。内部統制システムの運

用は企業に任されていて、どこまで詳細に規定するのかについては法律で規定されていない。上場企業は、会社法上の記載事項として事業報告書に記載し、ウェブサイトに掲載することになっている。考え方として、社長、担当者が適切に運用・監視するということ以外に内部統制の責任者を任命して会社全体をチェックさせる。取締役、社外取締役も基本ラインを共有して、会社全体で適切に運用できるのかということをチェックする。

梶浦構成員)

情報開示について、経団連としては推奨したいが、そのやり方についてはフォーマット等を決められるべきものではないし、業種・企業によって異なる。何を開示したらいいというぐらいの推奨が好ましいと考える。たとえば、組織体制であれば、ボードメンバーの直下に IT 部門・CISO が設置されている企業と、各事業部に IT 部門があって、取締役会からはその存在がみえない企業とで、いずれがよいかは明らかである。CSIRT 協議会への参加等、社会全体のサイバーセキュリティに貢献する活動についても加点ポイントとなるのではないか。

ただ、現時点では、報告書に記載しても取引先や投資家が見ると言うことは少なく、ホームページに掲載することにより、リスクヘッジに留まっている可能性がある。

中長期の課題として、開示されている情報の内容を投資家に伝える中間的な役割が必要と考える。具体的には、情報セキュリティ関連の記載事項や、どのようなサイバーセキュリティリスクがあるのかについて、投資家に対して説明するサービスが事業として起きないかと期待している。

サイバーセキュリティリスクへの取組状況を開示することにより、企業価値が向上するようにするための仕組みが必要である。

鵜飼構成員)

マザーズに上場している企業としての立場で意見を述べる。前回の分科会でも申しあげたが、多くの企業において、開示されている情報の内容がコピーペーストになっている。このような状況においては、開示を促しても効果は期待できないのではないか。何らかのインセンティブあるいはやや強い要請・お願いがないと、開示されないか、開示内容がコピーペーストになるという状況が継続するのではないか。

有価証券報告書においても投資家に求められている情報しか記載しない傾向がある。これまで多くの機関投資家に会社の説明を行ったが、サイバーセキュリティについて質問されたことは一度もない。

何らかのインセンティブあるいは強制力がないと、進展しないか、あるいは、形骸化するのではないか。

岡村主査)

損保会社に教えて欲しいのだが、金融検査マニュアルにおいて顧客情報保護に関する項目があると思うが、そのような制度があることによって規律を正すということはあるか。

秋保構成員)

サイバーセキュリティ対策の強化、個人情報保護については、検査の有無に関わらず企業として取り組んでいるというのが全ての企業の考え方ではないか。

上場企業に対する情報開示の要請やサイバーセキュリティ対策の必要性は、メリット・デメリットによってその内容が決まるのではないか。サイバーセキュリティリスクに対してどのような対策を実施しているのか、リスクがどのような範囲に及ぶのかを記載している企業は少ない。

中小企業や非上場企業を対象とする情報開示についてもスコープに入れるのかということについて検討するべきである。上場企業に限定するのであれば、整理の仕方が変わってくる。

サイバーセキュリティ保険への加入については、記載したいのであれば記載すればよいと考える。サイバーセキュリティインシデントにより予想される損害が 1,000 億円考えられるため、1000 億円の保険に入っているという情報であれば開示することに意味があるが、対策の 1 つとして保険に入っているというだけでは意味がなく、保険に加入しているから大丈夫であるというような誤解を与える可能性がある。

石原構成員)

情報開示のインセンティブについて、英国では、もともとセキュリティ対策は大丈夫だと言っていた企業にセキュリティインシデントによる被害が発生し、それを契機として、消費者に対するサイバーセキュリティ対策の開示が進んだということである。日本においては、情報を開示していたとしてもセキュリティインシデントが発生した場合の言い訳にならないため、何らかのインセンティブがないと開示にはつながらないのではないか。

サイバーセキュリティ保険については、大企業を中心に保険金額の引き上げの要請があるが、金額が大きくなると、保険会社としてはどのようなセキュリティ対策を実施しているのかについての詳細な評価が必要になるが、そのような評価がしっかりできるようになると情報開示に対する意識も高まってくるのではないか。

源田構成員)

単にサイバーセキュリティ保険に加入していることを開示しても誤解を与える可能性がある。サイバーセキュリティ保険は、経済的な損失を補填するだけであり、実際にサイバーセキュリティ対策を実施しているということの方が重要である。

岡村主査)

P2 サプライチェーン全体でのセキュリティ対策について、委託先選定基準を作成し、それに準拠している企業を取引先として選定するという方法もあると思う。

取引先に対して、コンプライアンスレターを送付して確認するということもある。

CSIRT については、一見緊急対応に関するものにも思われるが、日ごろから予防策として何をやっていけばいいのかという情報交換、情報共有を社内あるいはサプライチェーン全体でやるための 1 つの大きな手段となっている。

大杉構成員)

P7 中小企業について、IPA の『５分でできる！情報セキュリティ自社診断シート』の診断結果は、第三者開示の対象として適当だろうか。 第二者開示の対象ではないかと思う。

これまでに出された意見をまとめると、開示によってできることには限界がある。また、開示するべき項目とそうではない項目がある。上場企業に対して、P8 の考え方に記載されている 5 項目の開示を要請することについては、これが投資家にとって投資情報として重要かどうかというのはともかく、開示させることを通じて各社で責任を持った体制の整備を行うというので、私としては納得感がある。

セキュリティの専門家を設置しているということだけでなく、体制を整備することによって組織全体のサイバーセキュリティの向上につながっているということが重要である。

P11 - P13 の内容については、中身は良いが、せいぜい例示であって、強力に開示を促していくということは必ずしもよい結果につながらないとか、あるいは、あまり意味がないという感触である。実務からの感想をうかがいたい。

鵜飼構成員)

P8 について、開示の粒度は調整可能と考える。これら項目について一定の記載があれば、最低限の項目については実施できていると考えられる。一方で P11 について、発生したインシデントやインシデント発生後の対策については、記載することは大変ではないかという認識である。P8 の項目がベースであり、その他の項目については適宜記載するというのが現実的ではないか。

梶浦構成員)

P11 について、製品の事故においても同様であるが、事故が発生した後の対応を適切に実施し、どのように対応したのかの詳細を公表することにより、信頼度が向上する場合がある。インシデント対応の詳細や、インシデント対応を通じて得られた知見を公開することは期待したい。

P8 について、開示する場合、取締役会にかける必要があるので、会社としてのサイバーセキュリティに対する意識が変わることが期待される。社内のサイバーセキュリティ体制の強化にもつながるのではないか。

大杉構成員)

任意での開示を推奨するということで議論がされてきたところであるが、P8 の項目については、上場企業であれば、取締役会における決議を経たうえでコーポレートガバナンス報告書に記載するか、あるいは、ウェブサイトにおいて公開されているものを引用するということを東証に依頼して実施するようにするということも考えられるのではないか。

野口構成員)

P8 に記載されている項目は基本的な項目であり、記載する分量は企業によって異なるとしても、上場企業だけでなく、中小企業でも記載可能な項目であって、項目として問題ないと思う。

総務省として、なぜ情報開示が必要なのか、どのレベルでの開示を目指すのかについて再度整理をしていただきたい。そのような観点でみると、P1 と P2 が構成として逆になっているのではないか。どのレベルで開示してどのような効果を得るのかについての問題設定、情報開示の意義や必要性・有効性等について、内容の精査をしてほしい。

加藤構成員(代理：栄野)

セキュリティへの取組の状況は、企業規模や業種・業態によって異なる。サイバーセキュリティ対策をどこまで求めるのかということと、情報をどこまで開示させるのかということを検討する必要がある。

サイバーセキュリティ保険については、リスクの移転でしかなく、リスクの低減にはつながらない。サイバーセキュリティ保険に加入していることの記載が、サイバーセキュリティ対策ができているという誤解を招く可能性があるということについては同意する。

岡村主査)

インセンティブということでは、サイバーセキュリティ保険は一つの選択肢になりうるのではないかと考えるが、過度の期待はできないということである。サイバーセキュリティ保険よりも効果的なインセンティブがあるのかどうか、皆さまの知恵をお借りしたい。

野口構成員)

サイバーセキュリティ保険をインセンティブにするのであれば、開示内容に応じて保険料を下げるということを保険会社に推奨するということがあってよい。

岡村主査)

開示されている内容と実際の状況とが異なることが明らかになった場合には、ペナルティが課されるという運用も行われている。サイバーセキュリティ保険がもう少し普及してもよいのではないかと考える。

事務局)

P1 と P2 の順番については、P1 についてはまずこの分科会はこの検討課題から議論を始めましたということで挙げており、その後、議論の中で開示すること自体が目的化してはいけないという共通の認識を持ったということで、考え方を整理したものを P2 に挙げている。P7 については、中小企業を対象として、情報開示のハードルを下げるにはどうすればよいかということで、情報開示に向けた導入施策として、IPA の情報セキュリティ自社診断シートが有効ではないかと考えた。

岡村主査)

対象を上場企業だけにするのか、非上場企業も含めるのか、グループ企業の扱いをどのようにするのかということも含めて、現行の強制開示、任意開示の制度をマッピングし、もしそれが足りないということであれば、必要に応じて枠組を見直すということも考えられる。

石原構成員)

P11 のインシデントに関する情報の開示は、次の被害を防止する上で有効である。

大杉構成員)

現在の枠組では、セキュリティインシデントの発生に関する情報は上場企業の場合は適時開示の中で開示対象となっているが、インシデント発生後に実施した対策については対象ではない。一方で、対策の実施を自社のリスク管理体制の運用状況として捉えれば、開示することも考えられる。対策についても開示した方が良いのだろうか。

岡村主査)

改正前の個人情報保護法では、情報漏えいを起こした企業は、漏えい防止策を含め、主務官庁へ報告することになっているが、公表する義務はない。電気通信事業者については、事故報告制度がある。

大杉構成員)

対策の実施について主務官庁への報告を超えて一般社会に開示するように促すということは合理的ではあると思う。どのぐらい強制的で、一般的なものとするかは難しいと思うが、P11 の内容の開示を促していくのは考え方として正しいと思う。

事務局)

第 4 回分科会の日程については後日連絡をさせていただく。

岡村主査)

本日はこれで終了とさせていただく。

以上