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６回）議事要旨

1. 日 時：平成 31 年 1 月 18 日（金）16:00～18:00

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(代理：教学)、鵜飼構成員、大杉構成員、梶浦構成員、源田構成員(代理：土井)

【オブザーバ】

大能直哉(内閣サイバーセキュリティセンター) 、木村隼斗(経済産業省)

【総務省】

竹内サイバーセキュリティ統括官、泉審議官(国際技術、サイバーセキュリティ担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤サイバーセキュリティ統括官室参事官(国際担当)、篠崎サイバーセキュリティ統括官室統括補佐、相川サイバーセキュリティ統括官室参事官補佐

4. 配布資料

資料６－１ 情報開示分科会開催要綱改定案

資料６－２ 総務省のサイバーセキュリティ推進体制

資料６－３ セキュリティ対策情報開示ガイドライン（仮称）に係る論点（案）

資料６－４ 今後のスケジュール（案）

参考資料１ 情報開示分科会報告書（平成３０年６月）

参考資料２ サイバーセキュリティ戦略（平成３０年７月）

参考資料３ サイバーセキュリティ２０１８（平成３０年７月）

参考資料４ 企業経営のためのサイバーセキュリティの考え方（平成２８年８月）

5. 議事概要

(1) 開会

(2) 議事

◆ 事務局より、資料６－１ 情報開示分科会開催要綱改定案、資料６－２ 総務省のサイバーセキュリティ推進体制、資料６－３ セキュリティ対策情報開示ガイドライン（仮称）に係る論点（案）、資料６－４ 今後のスケジュール（案）を説明 (省略)

◆ **構成員の意見・コメント**

（資料６－３の論点１について）

秋保構成員)

ガイドラインの活用主体を、自主的・能動的な情報開示に一定の関心のある企業とするのであればおのずと任意開示を想定したガイドラインになると思うので、それをどのように普及させるかというところが重要と考える。

名前については、ガイドラインにするとマニュアルや手引きよりも強制的な感じが出るかもしれない。

石原構成員(代理：教学))

大手企業や中堅・中小企業、業界によってさまざまな企業が対象と考えると、優良事例を載せると、きれいな情報開示だけになって、それを読んでも同じテイストになってしまう。読みたいと思うようなモチベーションが沸かなくなる。例えば、対策の情報を出せばハッカーの攻撃対象になる可能性があり、企業はそのような情報を出したくはないが、この企業はこういうところまで踏み込んで書いているといった特異性のある事例を採り上げた方が目を引くものになる。

名前については、普及促進を考えるのであれば、強制力があった方がよい。ガイドラインよりも緩いものにしない方がよい。

大杉構成員)

コーポレートガバナンス元年と呼ばれる 2015 年には、コーポレートガバナンスコードが出来て、上場会社は強行法規ではないが、これを守るのが原則であるということになった。その前の 2013 年、2014 年頃に、上場企業の優良事例を紹介しながら、出来る企業から順に実施していくという方針を経済産業省の会議で打ち出したときには、ガイドラインではなく、マニュアルや手引きのようなものが策定された。最近は、経済産業省は、やる気のある企業を育てるというスタンスのもと、底上げをしていくために、強行法規や制定法ではないが、上場している限りは、楽をすることを認めない強い意志をもって、ガイドラインや指針と似たような言葉づかいをするようになってきていると感じている。今回、総務省で検討しようとしているものは、直感的にみて、その手前のマニュアルや手引きのようなものではないかと考えている。

業種や業態など、さまざまな要因によってやるべき事が異なる。ある会社をみて、その事例が模範的な事例や優良事例であることはいくらでもある。こういう前提の会社において、優良事例を挙げていくという方法が、自社の立ち位置を自己診断するうえで役に立つという印象を持っている。

段階ごとの開示の在り方として３段階が記載されているが、インシデントに係る情報開示が第３段階に分類されるかどうかは微妙である。悪いことが起きて投資家に知らせないといけないときに作成する臨時報告書を公表する場合は、金融商品取引法上では第１段階の情報開示になる。インシデント発生直後の情報開示は今回の検討では対象外であるため、インシデントに係る情報開示を削除することもあり得る。

米国連邦政府において関連する法律があるのか、またはそれに近い官庁が策定したガイドラインのようなものがあるのか、またはもう少し法的拘束力の緩い、自社の立ち位置を把握するための手引きや分析ツールのようなものがあるのかといった主要国の動向があると議論しやすい。

インセンティブについて検討するときに、例えば、コーポレートガバナンスや ESG は企業側からみると情報開示になるが、機関投資家側からみると ESG 投資という話もある。機関投資家ごとに、考えていることや、何に着眼して株の売買を行うかはかなり異なる。むしろ人と違うことをするからこそ儲けることができる。一般的に、機関投資家がどういうところに着眼して企業の開示情報を見ているかを発信する側は気にしているが、今回のセキュリティ対策情報開示であって

も、受け手側の反応やそれを受けた発信する側の行動や修正、フィードバックを通じて、双方が対話をしていることが重要である。読み手が育っていくことや、発信する側も選別や評価を受けることが上手く絵になるとよい。

相川サイバーセキュリティ統括官室参事官補佐)

主要国の動向については、「情報開示分科会報告書」の中で、米国の SEC が日本の有価証券報告書にあたる Form 10-K でリスク要因の情報開示を求めていることや、SEC の企業財務局がサイバーインシデントに関するリスクやこれに伴う事業への影響に関する情報開示のあり方に係るガイダンスを策定・公表していること、EU では EU 会計指令でリスクの情報開示が義務付けられていることについて、簡単ではあるが報告させていただいている。セキュリティ対策を取っていることよりは、リスクに着目して情報開示を要求するという流れが諸外国では大きいと思われる。また、セキュリティリスクそのものの開示については、法令そのものというよりはガイドラインの中に含まれていて、運用上法令に紐付いている傾向にあるように思われる。

読み手の関係については、例えば、投資家の声を代弁する証券会社の意見を聞くなど、サイバーセキュリティ対策に関する情報開示が読み手にどのように受け止められているかという部分について、意見交換や情報収集を行っていくことが考えられる。

岡村主査)

諸外国ではリスクを重視して金融当局が情報開示を要求するガイドラインを出しているということであるが、その目的は、投資家の評価や投資判断という視点に限定されているのかどうか。具体的に開示のレベルや開示の内容がどの程度のものであるか。法令で義務付けられているというレベルよりは、ガイドライン的なものであるということであるが、どの程度の実質的な強制力に準じるものを持っているか。そのような部分については、「情報開示分科会報告書」を作成する際に行った調査で活かせるものがあるか。

大杉構成員)

諸外国でリスク情報を有価証券報告書で開示するという部分については、ルールとしては日本と同じである。そこを深堀りするというよりも、今回作成しようとしているガイドラインや手引きに準じるものとして、企業がどういう対策を講じるべきか、また実施している対策をどのように開示するべきかという視点における、米国や EU のガイドライン的なものがあるのかどうか、ある場合にはどのような内容であるのか、そのような方向から深堀りすることができれば参考になる。

岡村主査)

現在の ISO/IEC 27000 シリーズは、もともとは英国の BS7799 というセキュリティに特化した基準から発展して、ISO 化されたものである。それと認証をセットにして、ISMS の認証基準となり、改定を行ってきている。そのような繋がりがあるということは参考になる。米国の NIST は、現在 SP800 シリーズを出している。そういう趣旨であれば、論点３にも関わる。

大杉構成員)

英国では、上場企業の開示書類を監査法人が監査するときに、財務情報だけでなく、財務情報の基礎となっている非財務情報も監査している。今までは監査報告書は定型文言があって、それをきちんと実施していれば監査がクリアされたが、最近ではこのような監査報告書を長文化して、KAM（Key Audit Matters）という主要な監査事項を、監査法人が監査先の企業名ごとに書いている。監査法人の監査意見の表明を具体化したり、監査意見を表明したりする前提として、セキュリティ対策が十分であるかといった財務情報以外の点について一定程度のチェックをかけて、その結果を公表しているという印象を持っている。

鵜飼構成員)

有価証券報告書などでの制度開示を検討していくことになると、今回議論できる時間が短く、その短い時間内でいろいろと考えないといけない。またきちんとしたものを作らないと、大きな混乱が生じる可能性もあるので、先ずは任意開示について検討していくことが現実的である。

経済産業省から「サイバーセキュリティ経営ガイドライン」が公表されている。それをもとにサイバーセキュリティ対策の取り組み状況が記載されるのが１つの流れになる可能性があり、何かしら開示をしていくことは重要であるが、いきなり制度開示の方に入っていくのは危険であるという気がする。

上場企業という立場で当社の情報開示がどうなのかについて考えると、制度開示は取り組まないといけないものであるが、現状、サイバーセキュリティに関する取り組みについて何か開示することに繋がるプレッシャーや開示することによるうれしさのようなものがあるかというと、実はない。仮にガイドラインや手引きのようなものが世の中に出てきたときにも、どれぐらいのインパクトがあるのかどうか。当社は有価証券報告書の中に一般的な文言を記載している程度の状況である。また IR でも機関投資家からサイバーセキュリティに関する取り組みについて聞かれたことは１回もない。開示を促進させるという意味では、どういうところで半ば強制力を持たせるのかについて段階的に検討し実施していくのがよい。

梶浦構成員)

経団連としては、上場企業だから一律に情報開示を強制するということに対しては反対である。社会を支える重要インフラ企業とそれを直接支える Tier1 の企業というところに関しては、業界として最低限これだけは情報開示すべきであるという開示基準を監督官庁が示すことはあり得ると考えている。業界ごとに本来開示する内容や開示の深さが異なる。同じ業界の中で、事業者 A、事業者 B、事業者 C がお互いの状況を見比べるにあたって参考になる情報が開示されていて、そのような情報を機関投資家などの外部も見ることができるという環境があってもよいのではないかと考えている。

自主的な開示はあればあるほどよい。ただし、情報の出し方はいろいろとあるので、こういう開示をすればよいのではないかという参考となるベストプラクティスの事例やベースラインの事例のようなものがあると、初めての企業でも取り組みやすくなる。情報を開示すれば株価が上がるというモデルを構築しなければ、リソースを手当てできない。インシデントが発生したことのある企業 20 弱社を対象に調査を実施した JCIC のレポートによると、その後の株価については、６ヶ月間の平均でみると 10％下がっており、その後の利益額については、企業間の差が大きいものの、６ヶ月間の平均でみると 20％下がっていることが分かった。経営幹部や取締役会、機関投資家などの株主が、どういう情報があれば、自社や株を持っている会社の状況を判断できるのかをあぶり出していくことが重要になる。

サプライチェーン全体を考えた場合に、企業の成熟度や見える化という話は今後検討しなくてはいけない話である。お客さま側からも侵入される可能性があるが、お客さま側に検査に入るのは難しいので、自分がお客さまの立場であっても情報開示を行うという文化を醸成していく必要がある。M&A のデューデリジェンスの場合も同じである。このような場合にどういう情報を開示するべきかについて海外の事例も含めて調べておくことは重要である。

源田構成員(代理：土井))

望ましい情報開示のレベルは段階的に設定すべきではないかという点については、まさに NISC が公表している、「企業経営のためのサイバーセキュリティの考え方」の中に、企業の視点別の取組という３つのレベル感が出ている。この３つで情報開示のレベル感は相当異なる。NISC の３つのレベル感と、今回検討する第１段階から第３段階までのレベル感がどう絡むのかが論点になると考えている。

開示された情報を活かす側の視点でいうと、最近、保険業界として、お客さまのリスクを評価することがあるが、付き合いのあるサイバーセキュリティのスコアリングを行う会社に聞くと、保険会社の次にお客さまとして増えているのが、投資銀行となっている。M&A のデューデリジェンスを行う際に、サイバーセキュリティのスコアリングを使っているのが実例として出ているので、投資銀行へのヒアリングを行った方がよい。

岡村主査)

個人的な見解を申し上げると、20 年程前から大きく変わったのは、ICT が実体経済や社会生活に溶け合っている状態になっていることである。企業の競争力や経済、さらには国民生活においても ICT を何とか底上げしないといけないということで、そのために何らかの開示手段が投資家保護を超えてできないのかが先ずは検討の原点になる。企業においても、投資家や投資家以外においても、そういう視点で見るような状態になってきているのではないかと考えている。

名称については、どの程度、年度末までに議論が成熟するかで決まってくる。ひとまず手引きのようなものから始めて、上手くいけば、きちんとした名称にするといった、小さく生んで大きく育てるという考え方もあり得る。事務局でもう少し検討してほしい。

（資料６－３の論点２について）

秋保構成員)

これまでの分科会での議論において、中小企業もガイドラインの読み手からはずさないという結論になっているが、今回短期間でガイドラインをまとめることになるので、啓発が比較的容易な上場企業レベルの大企業を読み手と想定したものを作るというのが現実的ではあると思慮。情報開示にあまり関心がない中小企業にも見てもらえるようなガイドラインを作るのかの方針を整理して作成する方がよい。

また、有価証券報告書の事業リスクのところにセキュリティリスクが記載されていることが投資家に理解されているように、各ステークホルダーにどこを見ると、セキュリティに関する取り組み方針等が分かるかが理解されていることが非常に重要と考える。例えば、任意開示を促すけれども媒体を指定しない場合、どこにその情報が載っているかが分からず、誰もその情報にアクセスできないというアクセシビリティに問題が生じる。まずは開示を促進しアクセシビリティについてはメンテナンスしていくというやり方もあるが、せっかく報告書を作って開示してもらう以上、見てもらえるような手をうつのも情報開示分科会の役目になる。その点についても留意してほしい。

岡村主査)

サプライチェーンの問題があるので、大企業としても中小企業を放置できない。有価証券報告書などの法的な強制力を持ったものは、中小企業にはもともと効かないので、その部分をどのように埋めていくかについて考えていかないといけない。

梶浦構成員)

中小企業といっても幅が広いので、一括りに議論ができない。従業員 20 人未満の零細企業は、事実上対応は無理である。IT 要員すらいないので、ガイドラインで情報開示を行うことになっても、全く不可能である。できないことをガイドラインに記載するのは反対である。中小企業の場合に可能性があるところとしては、地域クラウドや業種クラウドのようなものになっていかざるを得ない。サイバーセキュリティの観点から、個々の中小企業を評価するのではなく、中小企業が使っているクラウド事業者を評価する部分はあってもよい。中小企業がサプライチェーン上でサイバーセキュリティに取り組むことを取引先から要求されたときに、そういうクラウドに誘導していくという大きな流れがあり、中小企業が使っているクラウド事業者を評価し選定するという方向に将来的に持っていきたい。そういう方法であればできる。

鵜飼構成員)

中小企業に開示してもらうのはほぼ不可能である。当社の創業当初は、そのようなことよりも、もっとリスクの大きいものがいっぱいあったので、情報開示にかまっていられないところがあった。中小企業が使っているクラウドを評価するのは可能性として考えられるが、例えば、IT 補助金をもっと使いやすいものにして、IT 投資やセキュリティ投資をある程度賄ってあげる代わりに、簡単な事項について情報を開示してもらうといった褒賞を用意すると、開示が進むのではないかと思う。

梶浦構成員)

来年度から中小企業庁の助成金制度の中で、中小企業をグルーピングして IT 導入補助金を使えるようにする制度ができた。取りまとめ役の企業も補助金が使える仕組みが出来ている。そういうものがないと、中小企業の IT 導入やセキュリティ導入はできないと考えているので、参考にしてほしい。

岡村主査)

個人情報保護法の平成 27 年改正で、小規模事業者の除外の特例が外れて、義務規定が適用されることになった。個人情報保護法第 6 条に基づいて、個人情報保護委員会がガイドラインを出している中で、プライバシーポリシーの考え方の中に、どれだけのセキュリティ対策を論じるべきなのかという部分について、通常の事業者の場合と小規模事業者の場合を分けて記載している。国会決議で小規模事業者の過重な負担にならないようにすることが決まったため、そのような対応になっている。開示は無理だと言うよりは、プライバシーポリシーの中で、ある程度、対策を記載することになっており、ガイドラインでは記載すべしということになっている。それが守られているかどうかは今後注目する必要がある。

（資料６－３の論点３について）

梶浦構成員)

既存の仕組みを使って、あまり大きな負担にならないような形で情報開示の真正性を担保してほしいが、それよりも重い真正性を要求するのかどうか。虚偽記載を行った場合に、何らかの罰則を課すという話になると、運用上、かなり難しい問題になる。社外取締役の意見など、今ある制度を最大限使い、その範囲で運用するという話であれば、問題はないと考えられる。実際に開示書類を見て取引を開始したが、虚偽記載であったというケースにおいては、場合によっては民事訴訟に発展するかもしれない。また取引がご破算になれば、それがもれ伝わってよろしくない状況に陥り、それがディスインセンティブになって正しい開示に向かうことになる。それが妥当な線ではないかと考えている。

源田構成員(代理：土井))

情報開示の真正性のところで気になるのが、ある企業で個人情報漏えいの事故があったときに、当該企業が P マークを取得していたため、P マークと当該企業が却って非難を浴びてしまったようなことが起きないかどうかという点である。同じことが起きないように、どのように情報開示制度を作っていくことができるかが結構大事である。事故は起きるかもしれないが、ここまでの対策を実施していたから対応が早かった、被害を最小化できたというプラスの部分において、情報開示の真正性が使えるようなものになるとよい。

岡村主査)

情報セキュリティ報告書については、経済産業省の方で雛形を作られていることや、実質的には、大杉構成員から意見があったような、CSR 報告書、サステナビリティ報告等の中にこういう趣旨だから入れるのが望ましいということがあって、名称そのものを変えるという話でもないと思うので、そのような点を加味して、書きぶりを工夫するということで意見を受け取った。

大杉構成員)

情報開示の真正性の確保については、書面に限定せずに、幅広く考えた方がよい。ESG の場合は、企業が取り組んでいるセキュリティ対策を開示するのは、G（ガバナンス）に分類される。つまり、一般的に会社の中でそれぞれの部署が抱えている問題に対し、横串しで対応する部署が決まっていて、１つの生き物であるかのように企業が有機的に動いている。また、リスク管理の一環としてセキュリティ対策に取り組んでいて、それが第一者開示から第三者開示までの範囲の中で適切な範囲で開示されているということ。開示しているセキュリティ対策の内容が正しいかどうかを保証するにあたっては、認証の取得や、監査法人の監査意見の書き方、監査の対象が考えられるが、それ以外に、その企業が業種・業態・業容に応じて合理的なセキュリティ推進体制を構築して、それを PDCA サイクルとして回していることが考えられる。事故は必ず起きるものでゼロにはならない。ゼロにならないものを責めても仕方がないので、事故が起きようと起きまいと合理的にセキュリティ対策を推進していることを外部から何となく安心感を持って見られることが大事である。

岡村主査)

かつて事故前提社会という言葉があった。仮に事故が起きたときに、このような体制で対応を進める用意が出来ていることを開示することもあり得る。

秋保構成員)

情報開示の真正性をあまり厳しく求め過ぎると、情報開示のハードルが高くなり幅広く普及させるという部分に影響が懸念されるが、比較可能性の担保には情報の真正性はある程度必要になってくるためうまくマッチングできる形が示されるとよいのではないか。例えばＰマークのような認証制度は、同じ業種の中で取得している、取得していないという形で比較のための分かりやすい基準にもなる。

岡村主査)

どちらかと言うと、サプライチェーンの話に関連して、取引先から要請されて ISMS を取得するパターンもある。更なる検討が必要な部分である。

（資料６－３の論点４について）

梶浦構成員)

企業の場合、インセンティブになるのは業績である。情報を開示すれば、株価が上がるような情報開示が何であるか、機関投資家や個人投資家などの株主を含めて、何の情報を見て、その企業を評価しているかを本音ベースで少し調べる必要がある。

サイバーセキュリティというものに対する機関投資家を含めた世間の認識がまだまだ全然足りないので、そういう広報活動や株主教育を併せて実施しないといけない。そうすれば、取引先が増えるというチャンスが広がる。M&A の機会も増える。開示だけを実施しても、なかなかインセンティブには繋がらない。

岡村主査)

社会的にみてセキュリティに対する認識がそこまで成熟化していない。成熟化を図るべきではないかという指摘は重要な指摘である。

大杉構成員)

どの開示書類で情報開示を行うかについては、有価証券報告書の場合は、虚偽記載を行うと民事責任や、場合によっては刑事責任が発生する開示書類になっているため、思い切った書き方が採りづらい。よく慣れた機関投資家が深く読み込むと、企業の本気度が分かる場合もあるが、一般的には、有価証券報告書よりも法的責任に直結しないものの方が創意工夫を発揮しやすい。上場企業でより大手に属する企業になれば、標準的に CSR 報告書やサステナビリティ報告書での情報開示を行うことになるのではないかと考えている。ESG に関連して、そのような企業にヒアリング調査を行った際には、サステナビリティ報告書の説明を受けたが、サステナビリティ報告書が企業の中でこういうことを実施しようという全社を統制する手段となっているということであった。現場で実際に働いている従業員の創意工夫によるやりがいや喜びのようなものに繋がっているので、優良事例やベースラインの事例が、そういうものに繋がるようなことにできるとよい。各企業の創意工夫を認めれば認めるほど、比較可能性のような性質が失われる可能性もあるので、そのあたりについては、業種ごとに雛形やベースラインを具体的に定めていくことも考えられる。

（資料６－３の論点５について）

大杉構成員)

2014 年、2015 年頃、個々の企業において、コーポレートガバナンスに対応せざるを得なくなったのは、アベノミクスの一丁目一番地に位置づけられたことが大きい。今回検討しているセキュリティ対策情報の開示についても、同じぐらい大事でコーポレートガバナンスと重なる部分も十分あるので、政権がこの課題に対して本気で取り組んでもらえるように、内閣がやろうとしている政策リストにどうやってねじ込むことができるが１つの論点になる。

相川サイバーセキュリティ統括官室参事官補佐)

次回以降の進め方と少し関連するが、実際に情報開示を行っている側の意見と、開示を行っている書類の読み手側の意見を把握する必要がある。事例の調査と併せて、ヒアリング調査を行うことを考えている。

（事務的な連絡について）

相川サイバーセキュリティ統括官室参事官補佐)

今後の会合の日程については既に各構成員と調整してご案内を差し上げているが、確認として、第７回情報開示分科会の開催は 2 月 22 日（金）、第８回情報開示分科会の開催は 3 月 19 日（火）を予定している。具体的な議題や開催場所については、後日事務局から連絡させていただく。

以上