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

1. 日 時：平成 29 年 12 月 13 日（水）13:30～15:30

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

【オブザーバー】

山下浩司(内閣サイバーセキュリティセンター)、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、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１－１ 「情報開示分科会」開催要綱（案）

資料１－２ 民間企業におけるセキュリティ対策に関する情報開示の現状について (事務局)

資料１－３ 経営リスクとしてのサイバーセキュリティ対策 (経済産業省)

資料１－４ 有価証券報告書におけるリスクの記載 (加藤構成員)

資料１－５ 会社法・金商法上のリスク情報の開示の現状と課題 (大杉構成員)

資料１－６ サイバーセキュリティの強化を求める (梶浦構成員)

5. 議事概要

(1) 開会

(2) 議事

◆ 谷脇政策統括官より、本分科会の開催にあたって挨拶

2017 年 10 月に IoT セキュリティ総合対策を公表した。セキュリティ対策について情報開示を行うということがマーケットにおいて評価をされ、それが更に企業価値を高めるという循環をうまくつくれないかと考えており、どのような政策を展開していくことが民間企業にとって良い環境づくりにつながるかという点について、皆様方の知見を生かして御議論を賜りたい。

◆　事務局より、資料１－１　「情報開示分科会 開催要綱（案）」について説明 (省略)

事務局より、開催要項について説明されるとともに、主査について、サイバーセキュリティタスクフォースの安田座長より岡村構成員が指名されている旨の報告があり、資料１－１の開催要項（案）が承認された。

◆　事務局より、資料１－２　「民間企業におけるセキュリティ対策に関する情報開示の現状について」を説明 (省略)
◆　経済産業省より、資料１－３　「経営リスクとしてのサイバーセキュリティ対策」について説明 (省略)

事務局からの説明を踏まえ、本分科会の検討事項について承認された。

◆　構成員の意見・コメント

野口構成員)

NISC 等で検討されている情報開示は、情報開示が各社のサイバーセキュリティの強化につながるということが前提となっている。情報開示の目的として多いのが、ブランド価値の向上となっており、情報開示を推進する主体(監督省庁)と情報を開示する主体(企業)との間で意識にずれが発生している。認証を取得することによりブランド価値を高める、あるいは、新規ビジネスに参入するときの根拠にするというような、形式を整える目的だけに使用され、サイバーセキュリティの向上につながらないということが懸念される。総務省の施策としては、サイバーセキュリティの向上ということを目的とするべきである。

議論の前提として、情報開示の位置づけについて明確化するべきである。

また、関係省庁は NISC と経済産業省だけでよいのかということについても検討が必要ではないか。

事務局)

システムやサービスにおけるサイバーセキュリティを確保することが目的であるということについては、サイバーセキュリティタスクフォースの議論の中でも前提としている。

情報開示の本来的な目的とそのインセンティブとが少しまざってしまっているということについては、御指摘の通りである。情報を開示することは悪いことではなく、よいことであるということを企業に理解・認識してもらえるようなものにしたいと考えている。

関係省庁については、本件に最も関連がある省庁として NISC と経済産業省を記載した。必要に応じて追加することを想定している。

野口構成員)

期待される効果の中に、サイバーセキュリティが強化されるという項目がない。どのような情報開示を行えば、実際のサイバーセキュリティの強化につながるかということが重要である。情報開示の究極的な目的は、企業においてサイバーセキュリティをきっちり確保することである。情報開示そのものが目的となってしまうことを懸念している。

また、情報開示はよいことだということを前提とすると、情報開示が持っているリスクが軽視される恐れがある。情報開示が本当にサイバーセキュリティにつながるということをきちっと検証する必要がある。

岡村主査)

検討事項１に記載されている社会全体のセキュリティ対策を促進する観点等について、どのような軸で議論するべきであるかということについても考える必要がある。

過去の経済産業省の報告書において、IT、ICT は現代社会における神経系の役割を担っており、欠くべからざるインフラであるという指摘がされている。サイバーセキュリティ対策を実施することの重要性は明らかであるということと、前向きのインセンティブという側面で情報開示を促進したいという事務局の意向とを考慮しながら検討を進める必要がある。

◆　加藤構成員より、資料１－４　「有価証券報告書におけるリスクの記載」について説明 (省略)
◆　大杉構成員より、資料１－５　「会社法・金商法上のリスク情報の開示の現状と課題」について説明 (省略)
◆　梶浦構成員より、資料１－６　「サイバーセキュリティの強化を求める」について説明 (省略)

鵜飼構成員)

リスクを開示するのか、対策も含めて開示するのか、また、開示内容が正しいのかどうか、十分に網羅された開示になっているのか、更にそれがわかりやすく開示されているのかをどのようにして判断するのかという課題がある。さらに、開示内容が正しいかどうかの判断が非常に難しいという課題がある。これらのテクニカルかつ専門的な課題への対処方法についての検討が必要である。

情報開示の媒体については、有価証券報告書は上場企業だけが対象になっているので、未上場企業についてはどうするのかという課題がある。

一方、有価証券報告書に記載するということは、企業にとっては非常に大きな責任を伴うものなので、有価証券報告書に記載させるということは非常に効果があるのではないか。

セキュリティリスクを含めた開示すべき情報の範囲についても議論が必要である。

野口構成員)

リスクマネジメントにおいて、何が重要視されるのか、何が重要視されないのかということは、インシデントの影響の大きさと発生確率だけで決まるわけではなく、何が原因で起きたかということが非常に大きな決定要因である。

その意味において、サイバーセキュリティをどの程度整備するかというのは、自分の企業はどういうものであるかということについての経営者の自己認識のあらわれであるという視点が必要になるのではないか。

情報開示のインセンティブについて、サイバーセキュリティを強化するということと、それが事業成長にどう関わるかということについての考え方が整理されていないのではないか。

サイバーセキュリティの強化なしでは事業成長はないが、それを裏付ける論理が明確になっていない。情報開示がその開示のテクニックを争うものになってしまっても困る。投資家や市場の評価が強く影響するというだけであれば、それは市場に任せればいい話であるが、情報開示によるサイバーセキュリティの強化や他のインセンティブとの関係については、きちんと整理を行うことが必要である。

リスクマネジメントの観点では、経営者を巻き込むためには、これまでのリスク管理からリスクマネジメントへと考え方を変える必要があるのではないか。

さらに、情報開示と経営についての問題の検討を通じて、情報の問題を情報管理の問題からサイバーセキュリティマネジメントの問題へ格上げする時期ではないか。

石原構成員(代理：教学))

大企業においては、既にいろいろなセキュリティ対策が実施されていて、実質的に有価証券報告書にサイバーセキュリティリスクを開示しているケースがある。一方、中小企業においては、IT の利活用がまだ全然進んでいないので、サイバーセキュリティについてはまだ手つかずであるという話を聞くケースが多い。企業の規模によって、情報開示に対する意識は全く違うと考えている。

また、中小企業においては、どの層に向けて開示を行うのかということを明確にしたほうがよい。中小企業と話をしていると、開示するほどのセキュリティ対策がまだできていないという意識が強いので、サプライチェーンの川上にある発注元からセキュリティ対策の情報開示を求められたりするような動きがないと、なかなか自主的に開示をすることにはならないと感じる。

源田構成員)

サイバーリスクは、サプライチェーンのように、複数の企業がつながっている場合につながっている全ての企業に影響するという点において通常のリスクと異なる。また、つながっている企業が同質でないという点や、それらのつながっている同質でない企業が１つのリスクを受容しているという点がポイントとなる。

サイバーリスクに対しての対応力の向上を図ることが、情報開示の一つの大きな目的であるとすると、情報開示によって大企業・中小企業それぞれのレベルに合わせてどういうことをしてもらうのかということについての１つの方向性を打ち出す必要があるのではないか。

複数の企業がつながっている場合のリスクを回避するためには、大企業・中小企業によって場合分けをしなければいけないのではないか。複数の企業がつながっている場合のリスク回避においては、情報の共有が重要である。

同じ情報でも、大企業・中小企業によってその意味や価値が異なる。また、ステークホルダーによってもその意味や価値が異なる。したがって、情報共有の仕組みだけでなく、誰が情報を共有するのか、情報をどのように評価するのかについても検討が必要である。

秋保構成員)

情報開示の内容が、どのようなリスクがあるか、どのような対策をしているかというものであれば、保険料を決める要素になるとか、どんな保険が適しているかという判断の材料にするのは難しい。

保険商品としてはある程度定型化したものを中堅・中小企業様向けには用意しており、規模の大きい企業様になれば個別設計して保険料等を決めている。保険料の算出にあたっては現状、告知書という形でシステム等に関する質問項目に回答してもらっており、開示情報の内容に基づき保険料を決定するというよりは、告知書で取得した情報に基づいて保険料を決定するほうが現実的ではないか。

加藤構成員)

有価証券報告書に開示する場合、正確性の担保という点において、ある程度強制力をもたせなければならないという側面もあるのではないか。

正確性の担保については、セキュリティ監査やシステム監査のように、客観的にかつ独立性を持ってチェックを行うための経験や専門性、能力を有する人材を育成しなければ、なかなか難しいのではないか。

誰かが内容をチェックしたというだけでは恐らく情報開示に対する期待には応えられないのではないか。

鵜飼構成員)

有価証券報告書で開示している企業もあるが、内容が形骸化していて、同じような内容のコピーペーストの域を出ない企業が多く、正確性はほとんどないのではないかと思われる。そのような情報に基づいて保険料を決めることはできないと思われる。

開示の方法について、開示する情報の粒度や開示する媒体を検討する必要がある。

また、開示されている情報をチェックする人の資格要件も重要であるが、形骸化しないようにするためには、簡単かつその時代の状況に即した方法で誰がやってもある程度正確性を持って開示できるような仕組みを検討する必要がある。

大杉構成員)

米国でも有価証券報告書を開示している企業では、集団訴訟への対策として、考えられるリスクは何でも書いておくという対応になりやすい。そのような企業の場合には、日本での有価証券報告書での開示情報も行き過ぎた開示になっている可能性がある。

サイバーセキュリティの強化という目的に照らして考えると、企業が自社のサイバーリスクの所在をちゃんと把握していることが重要で、リスクを開示するのであれば有価証券報告書が適切ということになり、セキュリティ対策の開示であればコーポレートガバナンス報告書が適切ということになるのではないか。

全てのサイバーリスクを有価証券報告書に記載するのが適切かどうかについては議論が必要である。

セキュリティ対策についてもやっているということをステークホルダーに説得力を持って開示できればよい。

自社のサイバーセキュリティについて説明するケースとして、中小企業の場合は、取引先企業や保険会社に対してということが想定されるが、開示資料として誰でも見られるような書面を作成するということではないのではないか。

中小企業の場合には、しっかりサイバーセキュリティ対策が実施されるようにするために、情報開示義務を課すことが必ずしも意図したような効果につながらないかもしれない。

上場会社であっても有価証券報告書の記載が形骸化して他社のコピペになっているというのは、ゆゆしき事態である。

岡村主査)

資料１－４の有価証券報告書の記載については、一般論が長文で並んでいる部分がほとんどであるが、そうしなければ逆に営業秘密等々が出てきたりするということがあるため、やはりこういう書き方しかできないという面があるのではないか。日米の法的なフレームワークの違いというものも背景にあるのではないか。

インシデント発生時の適時開示について、大杉構成員から補足をお願いいたします。

大杉構成員)

社長が記者会見などを開いて説明をする、第三者調査委員会を設置して、例えば１ヵ月とか３ヵ月というふうなタイムフレームで報告書を外部に公表するというのが一般的である。

優良企業であれば、インシデントの原因を探求して、改善に結びつけるという方向に向かう大きな要因となっていると考えられる。

もっとも、第三者調査委員会の活動や調査報告書については、玉石混交であり、まだまだ評価が定まっていないというのが現状である。

岡村主査)

各種業法との関連について補足をさせていただきたい。第一者認証とは自らの判断で適合性ありと宣言することであり、その結果として、保険料割引の対象になる事項があり、公表の対象となる。第二者認証については、特定顧客に対する情報の開示であるが、これはいわゆる公表という類いとは少し性格が異なるものである。第三者認証については、公的な基準に基づく認証およびそれに基づく一定限度の公表がある。第一者、第二者、第三者で認証といっても公表との関係では違いがある。

梶浦構成員)

企業が保有する資産として、情報以外に、設備や予算がある。設備や予算については比較的チェックがしやすいが、人が有機的に機能していなければ、設備も予算も 100% 機能を発揮しない。

人の見える化を通して企業の見える化ができないかということを研究している。セキュリティ人材マーケットの活性化というようなことについても一部研究を始めている。

情報とサイバーセキュリティという観点では、これまで、情報窃盗の防止については余り重きが置かれておらず、サービスの停止、電力の停止、鉄道の停止をどうやって防ぐかということに重点が置かれていた。

現行の法制度では、無体財物である情報については、窃盗罪は成り立たないが、直接的な情報の窃盗というものが裁けないというのは今後の社会として、情報化社会、Society 5.0 としては課題であると考えている。

岡村主査)

公開すべき情報の重要度、種類等々についてどのような議論があるのか。

梶浦構成員)

業種、業態等によって異なるので、ユースケースを持ってきて議論をしないと難しいのではないか。

◆ 事務局より、資料１－２ 「民間企業におけるセキュリティ対策に関する情報開示の現状について」に基づき、今後のスケジュールについて説明(省略)

事務局からの説明を踏まえ、本分科会の今後のスケジュールについて承認された。

以上