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７回）議事要旨

1. 日 時：平成 31 年 2 月 22 日（金）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(代理：教学)、鵜飼構成員、大杉構成員、梶浦構成員、加藤構成員(代理：三澤)、源田構成員、野口構成員

【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】

泉審議官(国際技術、サイバーセキュリティ担当)、竹内サイバーセキュリティ統括官、赤阪サイバーセキュリティ統括官室参事官(政策担当)、木村サイバーセキュリティ統括官室参事官(総括担当)、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７－１ 「セキュリティ対策情報開示の手引き（仮称）」の骨子（案）

資料７－２ セキュリティ対策の情報開示の事例調査について

資料７－３ セキュリティ対策の情報開示に係るインセンティブについて

参考資料　情報開示分科会第６回議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆ 事務局より、資料７－１ 「セキュリティ対策情報開示の手引き（仮称）」の骨子（案）、資料７－２ セキュリティ対策の情報開示の事例調査について、資料７－３ セキュリティ対策の情報開示に係るインセンティブについて、を説明 (省略)

◆ **構成員の意見・コメント**

梶浦構成員)

全体の流れとして、情報開示分科会のアウトプットが手引きになっていくということは賛成である。情報開示では最後にインセンティブの話が出てくるが、この議論は長くかかりそうな気がしている。先ずは情報開示に取り組みたい企業がどのようにすればよいかを考えるときに、開示している事例を見ることができるようにするのが大変よい。

開示した内容の裏には膨大な作業があるはずである。IT ガバナンスを根付かせるという意味で、そういうものをどのようにして把握していくかという作業が、セキュリティ対策の情報開示の前に膨大に存在する。米国政府が出している IT ガバナンスに関する報告書を見たが、そのようなレポートを含めて、資料７－１の骨子案のⅠの６の関連ガイドラインを紹介することは重要である。

資料７－３のどのような課題を感じているかというヒアリングも重要だが、例えば、IT ガバナンスを実施しようとした際、グループ会社が多数あってレベルが合わなくて困った。この部分はベンダーにアウトソーシングを行っているため、情報が出てこないといった自分が克服した課題についても一緒にヒアリングできると、情報開示に取り組みたい経営者がそういう課題があることを見て、予算をつけたり、人材の配置を行ったりしやすくなる。

岡村主査

情報開示のバックグラウンドにある作業がアウトプットにつながっているという指摘は貴重である。

大杉構成員)

まず各社の IT ガバナンスがあって、その出来具体が開示書類の質に影響するが、いうまでもなく IT ガバナンスはコーポレートガバナンス全体と連動している。形のガバナンスではなく、社長や管理本部がしっかりしている、社外役員と上手くコミュニケートできているという実際に回っているガバナンスが出来ているかどうかで、IT ガバナンスの質も決まってくる。

開示を通じて情報セキュリティを良くしていくという作業には、それが結果的に IT ガバナンスを高め、更に上場企業のガバナンス全般を高めることに繋がるという「逆の経路」を通して改善効果が期待できる。その意味で、この会合はとても意味のある事に取り組んでいると感じる。

資料７－２について、P3 の(2)において建設業界で開示が進んでいると記載されている点が、おもしろいと思った。P5 の(4)で業界ごとに違いを生む要素として①～⑤が記載されている。私がこれを見ながらなぜ建設業界が進んでいる方に分類されているのかを考えたときに、例えば、③については建設の元請けは下請けに対して強い立場にいるので、開示する理由としては考えにくい。感覚的には、④が開示が進んでいる理由ではないかと感じた。もう１つの理由としては業界の中にリーディングカンパニーがあって、そこが実施しているからという理由が考えられ、資料７－３でも、同業他社の取組みをよく見ているという話があった。このような仮説について、みなさんや事務局のご意見をいただきたい。

梶浦構成員)

建設業界は、環境問題に対してセンシティブな業界であり、環境問題への取組みが企業を測る尺度のようになっていると言われている。そのような広報に力を入れている。また、ゼネコン、サブコンというピラミッド構造がはっきりしていて、③に関係するかもしれないが、CSR に関してゼネコンがサブコンを指導する立場になっているという気がする。さらに建設業界では CAD や CIM/BIM、データのデジタル保存などのデジタライゼーションが進展している。またそんなに業務が多いわけではないので、IT の世界からみると、ガバナンスしやすい業界のように見える。

相川サイバーセキュリティ統括官室参事官補佐)

次回の分科会では建設業界の事例も載せたいと考えている。事例を眺めると、幾つか特徴がある。１つは定量的な目標を立てたり、実績をトレースしたりしている例が多い。例えば、当該年度のセキュリティ事故はゼロ件であるので、当該年度の取組みは A という評価になることを記載している事例や、目標として、セキュリティ事故ゼロ件を達成することを対外的に宣言している事例、グループ会社に対して監査を何件したか記載している事例がある。定量的な数値を示す事例が他の業界と比べて多いという印象を持っている。

岡村主査)

厚生労働省の労働基準監督局が開催する労働安全衛生法の情報管理に関する委員会に委員として出ているが、リスク管理慣れしている業界のように見える。請負完成物の管理との両面で開示が進んでいるのではないかという印象を持っている。

野口構成員)

学術会議でも議論を行っているが、事故ゼロとリスクゼロは意味が全く異なる。事故ゼロの方が難しいように思うが、１年間事故が起きなければゼロになる。ただしリスクはゼロになっていない。牽制という概念で考えているからそうなるが、事故ゼロとリスクゼロを同じに考えているというのは意味がよく分からない。サイバーセキュリティを考えるときに、今年はセキュリティ事故がゼロ件だったから、来年もセキュリティ事故がゼロ件になるという保証は全くない。そのような点は重要であり、本質的なサイバーセキュリティのリスクの考え方をきちんと整理しておかないと痛い目にあう。

岡村主査)

１つの考え方として、ヒヤリ・ハットということになるのか。

野口構成員)

小集団活動のヒヤリ・ハットと、事故件数やリスクはフェーズが異なる。労災の観点でヒヤリ・ハットとリスクはかなり綿密な世界の小集団活動であるが、そういうものがサイバーセキュリティの世界に流れ込まれると困る。リスクのフェーズが違うので、それを厳密にしておかないと、今までの安全の枠組みの延長でサイバーセキュリティの議論が出来る部分とそうでない部分があるので、手引書を策定する上で重要な議論である。

大杉構成員)

建設業界は 2000 年前後に談合でたたかれた業界である。その直後には法務部長の力が強くなった。当時、執行役員になっていなくても、社長が法務部の言うことを聞きなさいと全社に宣言した事例もあった。もともといろいろなことがあって安全や開示への意識が高いということと時系列の繋がりがあるのではないかと思う。

事故をゼロ件にするという単純なリスクの捉え方は、大企業でサイバーセキュリティを担う人や、IT ガバナンスを主導する人は絶対に持ってはいけない。しかし、その反面として、実際に建設現場で働いている人、平たく言うと現場の作業員がリスク概念を正確に理解することは絶対にあり得ない。誰に向かって、単純なリスクの捉え方は許されないという話をするのかと関連がある。建設業界で事故をゼロ件にすると言っているのは、言っている人の頭が悪いからではなく、現場

の人がリスクの概念を把握するのは難しいので、分かりやすい表現で現場を統制しているというように見れば、理解できるのではないかと思う。

資料７－２の P6 の(5)で、場合によっては国内外の取引先への監査や点検等を実施するということが記載されているが、ここで言う監査の実施主体は、取引をしている会社の内部監査部門というイメージになるか。上場企業を監査している監査法人がいて、取引先にも監査に入るというイメージになるか。

相川サイバーセキュリティ統括官室参事官補佐)

どちらかというと前者のイメージである。ただ実際は監査法人に委託をしているが、それについては書いていないケースもある。

大杉構成員)

資料７－２の P6 の(6)で、グループ単位のセキュリティ対策が進んでいるので開示も進んでいるということが記載されているが、おそらく平成 26 年に会社法が改正されて、また翌 27 年に会社法施行規則が改正されたことと関係がある。それまで内部統制システムは基本的に個社の問題であると理解・誤解されていたが、グループ全体で内部統制システムの構築や運用、改善をしなければいけないことが同年改正で明確化され、そのような文言修正があった。おそらくそれが大きな原因ではないかと考えている。

岡村主査)

金商法的に見れば、グループ統制は関係がないのか。

大杉構成員)

金商法の内部統制報告は基本的には財務報告に限定されているが、財務報告は連結（グループ）と単体（個別）の両方で行う。財務数値について投資家等に詳しく開示するときに、その数字が正確であるだけでなく、数字を作っている社内の財務・経理のプロセスがしっかりとしていることについて、監査法人に見てもらっている。資料７－２の P6 の(6)に関係がない訳ではないが、連結子会社についても当然金商法の内部統制が及ぶので、その意味では内部監査部門のみならず、監査法人が一定程度チェックする形になっていると考えてよいだろう。

加藤構成員(代理：三澤))

会計監査の世界ではセキュリティはダイレクトには対象に入っていない。金商法の内部統制監査でも財務報告の監査という位置づけになっているので、セキュリティについてはダイレクトに見にいかない。取引先への監査について内部監査人が見に行っているという話が出たが、セキュリティに関して外部監査人が見にいくことはないので、自社の内部監査人が見にいかれている。外部監査人が入っている場合はあくまで委託先となる。

米国の SEC では、サイバーセキュリティに関するリスクの開示が、ガイドラインを通じて求められている。これについて監査法人内では、その部分も対象にしないといけないことになってきている。実務上も見るようになってきている。ただし日本では、法的な根拠に基づいて見ないといけないということにはなっていない。

岡村主査)

金商法の場合は、企業の内部で連結子会社やグループ会社を含めて内部統制を報告書の形で仕上げられるようにチェックを行って、その内部統制報告書に関して、きちんと出来ているかどうかを監査法人にチェックしてもらっている。このように２段階になっているという理解でよいか。

加藤構成員(代理：三澤))

連携子会社の分も含めてグループ会社全体として、連結の財務諸表に対しての内部統制報告ということになる。

岡村主査)

企業が行うべきことと、監査法人にしてもらうことの２段階になっているという理解でよいか。

加藤構成員(代理：三澤))

そのような理解でよい。企業が内部で報告書を作って、それに対して自社でチェックを行うのが第１段階で、その後監査法人はその報告書をみて、きちんと対応しているかを見るという二段構えになっている。

監査や内部統制の対象をはっきりとした方がよいと考えている。手引書で言われているセキュリティの対象が情報セキュリティ、サイバーセキュリティのどの範囲なのか。実務上は、双方は大きく異なる。リスクの観点でも、情報セキュリティの場合は守るべきものがはっきりしており、CIA の中の C に注目する。サイバーセキュリティの場合は、どこから、どういう目的で攻撃されるか分からないので、実務上、CIA の中の A が重要になってきている。このあたりを手引書の趣旨や目的のところでクリアにしておかないといけない。使う側にとって自分たちに関係するものなのかどうかが分かりにくいのではないかと思う。

相川サイバーセキュリティ統括官室参事官補佐)

企業側は情報セキュリティとサイバーセキュリティの両方を意識しないといけない。実際の開示の事例を見ると、開示は情報セキュリティの方に寄っているという印象を持っている。個人情報を守るという話や、ISMS 認証や P マークを取得しているという話が開示の内容として多い。他方、制御システムの可用性や完全性を確保するという話の記載はあまりない。手引きで実際の優良事例を載せると、情報セキュリティの方に寄ってしまう可能性がある。クリティカルな指摘であるので、方向性を少し検討したい。

岡村主査)

情報セキュリティを定義したものは、ISO/IEC 27000 シリーズや OECD のガイドラインであり、CIA 全般を対象にしている。サイバーセキュリティに関しては、サイバーセキュリティ基本法で実定法上の概念になっている。同法では、情報、情報システム、情報システムを繋ぐところの ICT といった３段階に分けて、実質 CIA を中心とした概念で定義されている。CIA の C ばかりが重視されていて、I や A がどちらかというと二番手扱いとなり、注目度が弱すぎるのではないかという指摘は大変重要な指摘であると思う。

加藤構成員(代理：三澤))

CIA の A は重要インフラシステムの制御系システムが狙われやすいというところから重要になってきている。

資料７－３の開示企業のインセンティブについて、インセンティブの中で悪影響の話として P1 があるが、インセンティブを示すという意味では、数字について開示されている企業において、このように数字が上がったという形で KPI の情報が取れるとよいのではないかと思うが、なかなか難しい。具体的な事例として、こういう好事例があるというものをヒアリングの中で聞いてもらいたい。

資料７－３の P6 で、B 社が情報開示を行うきっかけとなったのが軽微なインシデントの発生であったと記載されているが、この部分が上手く理解できない。軽微なインシデントがあっても開示をしたいということにはならないのではないか。

相川サイバーセキュリティ統括官室参事官補佐)

B 社は JFE である。軽微なインシデントが起きたので、社内の対応体制をきちんと整備するために JFE-SIRT を作った。それを PR 要素と考えて情報開示を行うようになったという印象を持っている。

セキュリティ対策を取った企業において、これぐらい株価が上がるという部分についてのクリアカットな指標という話が出たが、結構難しいと考えている。証券会社の話では、セキュリティ対策を取っているということは、株価にはほとんど影響がないということであった。セキュリティ対策を取っているから事故が起きていないのか、そもそも事故が何も起きていないのかが分からない状況がある。現状では投資家はセキュリティ対策を意識して見ていない。

加藤構成員(代理：三澤))

数値については、難しいとは思うが、株価だけでなく、セキュリティを学んでいる学生からの志望状況など、何らかの数値が取れるとよいのではないかと考えている。そういうことができないのであれば、JFE-SIRT が開示のきっかけとなったように、具体的な事例として、せっかく人をかけて、お金をかけて、手間をかけて取り組むのであれば、開示した方がよい、それによってこのような良いことがあったということが示されるのであれば、開示を行う企業がイメージしやすくなる。

岡村主査)

某大手教育産業が情報漏えいした際には、先ずは決算短信を出すということで CFO が動いて出した。まだ個人情報保護委員会の発足前だったので、監督官庁の経済産業省に対して個人情報保護法に基づいて原因究明や再発防止策の実施を行った。当然株価は上がる訳ではないので、顧客に対する信頼回復策を徹底的に行うという観点で、これまで実施してきた対策と比べて、200%に高めないと信頼回復につながらないという意識で対策に取り組んだ。大手のセキュリティベンダーとの JV を立ち上げて、そこに情報管理を行わせる仕組みづくりを行ったり、監視委員会を立ち上げて、外部有識者を招聘して管理体制を構築したりした。これが１つの分かりやすい事例にあたるのではないか。

石原構成員(代理：教学))

レベル感として任意開示の取り組みであること、まだ情報開示に取り組んでいない企業にとって参考となる事例を提供するという位置づけであることを考えると、手引きという方向でもよい取り組みであると思う。

インセンティブについては、ステークホルダーからの影響はまだまだ少ない。それよりも営業的な意味合いが多いのではないかと思う。実際に開示の目的を考えると、企業のどのような部門の人が読むのかが結構ポイントになる。手引きの目的や活用主体を明確に定義し、整理した方がよい。

同じような取組みが経産省の産業サイバーセキュリティ研究会の WG2 の中でサイバーセキュリティ経営ガイドラインの内容を可視化する取組みとして行われている。ベストプラクティス集を作る SWG にも出ているが、その中でも、サイバーセキュリティ経営ガイドラインの指示 6 の中に情報開示の項目があって、この取組みをいかに推進していくかという整理を行っている。読む人が混乱しないように両方の取組みの棲み分けが必要である。経産省の取組みは経営者が上から落とすもの、今回の総務省の取組みは事例集なので実務の人が見るものということで、双方の取り組みがお互いを補完するものになればよいと感じた。

相川サイバーセキュリティ統括官室参事官補佐)

現時点の想定では、実務的な手引きを目指していきたい。開示書類を作っている企業のさまざまな部門の人に読まれることを想定している。他省庁を含めいろいろな取組みがある中で、企業の方が混乱しないように、クリアカットな役割分担ができるように調整させていただきたい。

岡村主査)

経産省は、SP800 シリーズを含めて膨大な形でガイドラインを作っている。総務省は、これまで見えていなかった論点も見えてきており、情報開示の観点で深堀りするという意味合いで手引きの作成に取り組んでいる。横断的なものと深堀りするものの両方があってもよいのではないか。それぞれ意義が大きいと思う。

野口構成員)

手引きという方向でいくことができればよい。手引きの内容を充実させるための質問になるが、総務省が情報開示を進める目的は何か。

相川サイバーセキュリティ統括官室参事官補佐)

資料７－３の P2 に記載しているとおり、昨年度の情報開示分科会報告書でセキュリティ対策の好循環という概念を示しているが、セキュリティ対策の情報開示を通じて、最終的に各社や社会全体のセキュリティ対策の質の向上に繋げていくことが重要であると考えている。

野口構成員)

資料７－３の P2 に記載されているのは企業の開示の目的であって、総務省が開示を進める目的ではない。総務省は開示を進めれば社会全体のセキュリティ対策の質の向上につながるという仮説のもとで検討を進めている。そのときに総務省が進めたいのは、企業のセキュリティ向上、社会全体のセキュリティ向上のどちらであるか。

相川サイバーセキュリティ統括官室参事官補佐)

基本的には個社というよりは社会全体のセキュリティ向上である。

野口構成員)

目的が社会全体のセキュリティ向上で、そのために企業の情報開示があるべしという建てつけはよいと思うが、そうすると、企業にとって都合の悪いことでも推進しなければいけないことがあるが、それをどう考えるか。調査を何のために行っていて、ヒアリングを何のために実施しているかという部分がだんだんぼやけてきている。その部分は最初の目的に照らし合わせてしっかりと実施しなければいけないと思う。

事故とリスクの違いの話をしたが、何の情報の開示をすれば、どういうセキュリティ向上に繋がるのかというロジックを考える際に、セキュリティのためには、現場のレベルで実施してもらうことや、情報システムなどの専門的な部署で詰めないといけないこと、経営者の観点から詰めるべきことがあって、それぞれのサイバーセキュリティの要素をきちんと整理を行い、その中で何をどのように開示するかというプラットフォームがあるべきである。今のやり方は、社会全体のセキュリティ向上に繋がるかは、甚だ怪しい。情報開示をしたというエビデンスを作るために非常に膨大な作業をさせて、それがセキュリティ向上に繋がっていないとすると企業としても困る。社会としても無駄なコストをかけることになるので、一度きちんと整理しなければならない。それは必ずしもヒアリングやアンケートから導くものではなく、サイバーセキュリティと企業との関係について、どこかできちんと整理しておいた方がよい。

社会のことを考えると、企業に情報開示を促すだけでなく、社会が開示企業をきちんと受け止めて、社会が開示企業をきちんと評価する受け手側の仕組みを作ってあげないといけない。開示された情報をいかに活用するかという流れを作るべきと企業の努力を促すことは難しいと思う。情報開示をすれば、本当に社会全体のセキュリティ対策の質の向上につながると言うなら、それこそが企業の最大のモチベーションやインセンティブではないか。それが出来ていないから、途中経過のものを挟む必要が出てくる。総務省として社会全体のセキュリティ対策の質の向上を目指すのであれば、いつまでも企業が持っている営業上のモチベーションに頼るのではなく、情報開示がいかに社会全体のセキュリティ対策の質の向上に繋がるかという部分のロジックを示すべきである。P2 の絵だと経産省の考えと同じになってしまう。総務省で検討する必要はなくなる。

P2 の絵で多少気になるのは、現状はアピールかもしれないが、本来の情報開示はアピールではなく、正しい情報を出して正しい判断を仰ぐことになる。総務省の資料としては現状の姿として示した方がよい。資料を作るときの精査が必要である。

鵜飼構成員)

上場会社の経営者であり、開示を行う側の立場になる。また、サイバーセキュリティベンダーということもあり、開示を行ってほしいと言われる立ち位置の会社の代表になる。そういう位置づけで話をすると、手引きという形でアウトプットを出すということについては賛成である。ただ最終的な目標として、開示を行う企業が増えて、世の中のサイバーセキュリティの質の向上に繋げることを目指しているが、ここから先について、どのようにしていくか考えていかないといけないと思う。企業自身が開示を行う場合、非常に大きなペナルティ、または非常に大きなインセンティブかのどちらかがないと実施しない。自分自身についてみても、開示を行ってほしいという圧力があった場合、どちらかがないと実施しないと思う。ヒアリングで開示企業からいろいろな話を聞いてきたと思うが、本音と建前のような話があって、本音の部分についてはなかなか見えないところもあるのではないかと思う。自分自身がヒアリングを受けた場合を想定して答えると、企業としてはやらなくてもよいことは全くやりたくない。大企業でも中小企業でも同じであるが、企業は生きるか死ぬか

という経営環境にさらされながら事業を行っている。そのような状況の中で、やらないといけないことしかできないのが現状である。一方で CSR の取組みはいろいろなところで活発であるが、やらないといけないという切実な状況があって取り組んでいる。例えば、ブラック企業だが、現実的にそう見せたくないとか、長時間労働があるなかで少しでも良い格好したいというブランドイメージが効いている。

資料７－３の P2 に記載されている情報開示を行っている企業の開示の目的のうち、インシデントや不祥事からの信頼回復は腹落ちする。何か問題が起きたときに総会で株主からいろいろと言われる。他の目的は腹落ちがしない。これは建前の部分が結構入っている。顧客との安定的な取引関係の維持については、開示まで行う必要がないのではないかと思う。お客さまやパートナーから開示してほしいと言われたことはない。ヒアリングに来る場合があるが、それで十分であると思う。販促ツールとして活用している事例については、理解できないこともない。自社で導入・運用したものをお客さまに営業することはあるとパートナーが言っていたが、開示まで行う必要はないと思う。もう１つ想定される話としては、経営改善のところで、適切な利益管理をアピールというよりも、セキュリティ対策をきちんと実施していることを対外的にアピールしたいということはあるかもしれない。これは経営者からみるとアピールしたくなければ、開示書類を作りたくはないが、IT 部門やセキュリティ部門の人は自分たちの責任にされるため、本当はいろいろなセキュリティ対策に取り組まないといけないことが分かっているが、予算を要求しても通らないというジレンマを抱えている。そのときに世の中にこういう情報開示の流れがあって、大企業では情報開示をしなければいけないというストーリーを作って、経営者を半ばだまして開示まで持ってゆき、予算を付けてもらいながら自分たちがやるべきセキュリティ対策を進めるという画策はあるのではないかと思う。その部分は本音としては出てこないと思う。良い意味で経営者がだまされるという話であるので、そういうものを上手く利用できる何かを作っていった方がよい。

岡村主査)

腑に落ちるかどうかという議論は、経営者の本音というところで説得力があると思う。

大杉構成員)

資料７－３の P2 に情報開示を行っている企業の開示目的が４つ出ているが、平たく言えば顧客との安定的な取引関係の維持については、守りでダウンサイドリスクに対応するもの、販売促進と製品・サービスの差異化については、攻めでアップサイドリスクに対応するものという印象を持っている。インシデントや不祥事からの信頼回復については、攻めか守りかの 2 択で言えば守りで、経営改善については、攻めではないかと思う。この部分は外部にこんなに素晴らしいとアピールするというよりも、社内の管理部門がいろいろ策を弄して、理解のない経営者を動かすために関連する部署を巻き込んで取り組むという社内政治であると思う。そういう会社は絶対にある。インセンティブやモチベーションという意味ではそのような部分は大事である。手引きを作成する際に、単純化すると、インシデント部分が守りで、経営改善部分が攻めである。そのような分類が正しいかどうかはともかく、４つあると頭に入れるのが困難なので、単純なラベリングを張ってそこから入っていくようにすると理解しやすい。

相川サイバーセキュリティ統括官室参事官補佐)

情報開示を行っている企業の開示目的の４つについては、ヒアリングを行う前に、かつ実際にビジネスを行っていない立場で作っているものになる。腹落ちする、しないという部分が出ているが、このような分類でよいのかどうか、４つにはそれぞれ重み付けがあるのかという話があるので、引き続き整理をしていきたい。

野口構成員)

セキュリティに関する情報開示において、話をしていて多少無理があると思っているのは、セキュリティは自分たちが提供する IoT サービスの機能に付随しているものである。付随している部分だけの情報開示には無理があって、本来はこれから自分たちの会社がいかに IoT を使って、このような素晴らしいシステムを活用しているということを開示したいと思っている。それが高度なものになればなるほど、当然セキュリティも高いレベルで取り組んでいるということについて、自分たちが使っている IoT 機能とセキュリティをセットにして情報開示していきたいと思うのが普通の流れではないかと思う。

あまり IoT の活用が進んでいない企業は、セキュリティについてもそれなりでよい訳で、逆にすごい取組みを実施しようとすればするほど、セキュリティについては言及せざるを得なくなるはずである。セキュリティの向上に関する情報開示を行うときに、IoT 機能全体の押し出しということも踏まえて、情報開示を支援すべきである。セキュリティだけの情報開示には無理がある。

大杉構成員)

資料７－３の P2 に関連して、企業の開示目的の４つから矢印が下へ向いていて、受発注への影響や株価への影響が書かれているが、これは開示という言葉の定義とも関わっている。先ほどインシデントや不祥事からの信頼回復という目的以外で開示することはないという意見が出たが、それは第三者開示のことだと思う。第三者開示するかと言われれば、しないかもしれない。インシデントや不祥事からの信頼回復と経営改善は株価に影響をもたらすものであるので、第三者開示に関わる話である。第三者開示を行うべきだというのはよく分かる。他方、顧客との安定的な取引関係の維持と、販売促進と製品・サービスの差異化は、多くの場合は第二者開示であり、実務的には下請け企業にアンケートを行い、それを回収してサプライチェーン全体のセキュリティ確保に繋げるためにチェックを行っている。そういう意味では開示という言葉を使うことが、誤解を生んでいる部分もある。第二者開示まで含めて考えると、全く開示していない訳ではないが、一般向けには開示をしていないということになる。取引先には開示しないと買ってもらえなかったり、開示を向こうから求められたりすることがあるので、構成員の間で、また構成員と事務局の間に、それほどの認識の差はないと感じた。

源田構成員)

今回、手引きという形を目指していくことになったが、実務者の立場で御願いしたいと思っているのは、事例がたくさん紹介されるというだけでなく、事例を活用して、自分たちがどのようにエッセンスを得ていくのかという部分について、より分かりやすいような形での出し方を工夫してもらいたい。

資料７－１のⅠの３－１のセキュリティ対策が非開示または限定的である事業者という表現がよいか悪いかは別にして、まだ取組みが進んでいない事業者に対して、どのように体制を作っていくのかという部分についても、丁寧な形で出し方を工夫してもらいたい。大企業の先進的な事例について、横並びのような観点を利用して、大企業を中心に対策が進んでいき、取引先などのいろいろな企業にも対策を促して、社会全体のセキュリティ向上に繋げていくという話になると考えている。いろいろな企業における体制の構築が非常に重要な観点になる。丁寧な形で手引きに記載してほしい。

秋保構成員)

資料７－１のⅠの３－１で、媒体ごとの記載ではなく、あくまで項目の紹介だけを行うとされているが、項目を紹介するだけでは、非開示である事業者がそれを見て本当に開示に動き出すかとは言い切れないと考える。例えば、こういう項目

を載せるのが望ましいであるとか、どの媒体で開示した方がよいという部分についても手引いてあげないと意味のある手引きにならないのではないか。

また、「限定的である事業者」はイメージとしては分かるのだが、「既に開示に取り組んでいる事業者」との違いが何なのかを明確にした方がよい。個人的には、主要５項目の開示にすら至っていない事業者を限定的である事業者と呼んでいるように思っているが手引きとしては、どの企業がどちらを見ればよいかという部分について明確に分かるようにしておく必要がある。

竹内サイバーセキュリティ統括官)

本来あるべき情報開示の姿をきちんと打ち出して、企業を誘導していくような形にする。ヒアリングを行った結果、現実的にはこのような状況になっているという部分を認識したうえで、こういう方向にしていくべきだというところはきちんとメッセージとして伝わるようなものを作っていった方がよいと考えている。そのような部分を丁寧に検討しようとすると、これまで年度末を目途にまとめるというスケジュールで進めてきたが、構成員の同意がいただけるのであれば、今後の開催回数や日程など相談をさせていただきたい。本日有益な意見を多数頂いており、せっかくエネルギーを費やしてまとめていくものになるので、きちんと社会に対して伝えるべきものは伝え、それによって世の中が動いていく形に繋がるものを引き続き、構成員の協力をいただきながら作り上げていきたいと考えている。理解を賜りたい。

相川サイバーセキュリティ統括官室参事官補佐)

次回の第８回会合については、3 月 19 日火曜日の 14 時から開催を予定している。第９回会合以降の日程については、引き続き調整させていただく。具体的な議題については、後ほど事務局から連絡をさせていただく。ご協力よろしく御願いいたします。

岡村主査)

今お話があったように、必ずしも年度末の第８回会合で議論が終了ということに限らず、必要に応じてもう少し議論を深めるべきところがあれば、深めていくというような柔軟な形で進めるという理解でよいか。

相川サイバーセキュリティ統括官室参事官補佐)

その方向で問題はない。

岡村主査)

そのような方向になるので、引き続きよろしく御願いいたします。以上で本日の第７回情報開示分科会を終了させていただく。

以上