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８回）議事要旨

1. 日時：平成 31 年 3 月 19 日（火）14:00～15:30

2. 場所：中央合同庁舎２号館１０階 共用１００１会議室

3. 出席者：

【構成員】

岡村主査、秋保構成員(代理：沢井)、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、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】

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)、木村サイバーセキュリティ統括官室参事官(総括担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、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８－１　「サイバーセキュリティ対策情報開示の手引き（仮称）」の骨子（案）

資料８－２　サイバーセキュリティ対策の情報開示について

資料８－３　情報開示分科会の今後のスケジュール（案）

参考資料　　情報開示分科会第７回議事要旨（案）

5. 議事概要

(1) 開会

(2) 議事

◆　事務局より、資料８－１　「サイバーセキュリティ対策情報開示の手引き（仮称）」の骨子（案）、資料８－２　サイバーセキュリティ対策の情報開示について説明 (省略)

◆　関係者の意見・コメント

野口構成員)

「サイバーセキュリティリスクの増大と対策の重要性について触れる」という記述について、セキュリティリスクと対策の重要性というのはだれのリスク、だれにとっての重大性ということを意図しているのか。

岡村主査)

基本的には、これは趣旨からすると社会全体という非常に漠然としたものに対する呼び掛けということを念頭に置かざるを得ないのではなかろうかと思う。

野口構成員)

同じ意見であるが、企業のリスクや企業にとっての対策の重要性を書くのではなく、総務省であれば、社会にとってのリスクと社会にとっての対策の重要性を書くべきである。こういう状況だから企業はちゃんとセキュリティ対策をやるべきだということを書くべき。セキュリティ対策の情報開示の意義のほかに必要性みたいなこともあってもよい。

一方で、情報開示の手段が、有価証券報告書、コーポレートガバナンス報告書というのが本当に社会とか消費者を想定しているのか。消費者やほかのステークホルダー全体に届くものとは限らない書き方になっていて、企業を守るための報告書になっているのが気になる。資料 8-2 で、投資家、株主、アナリスト、市民、消費者が同じオレンジの矢印が指している対象にまとめられているが、市民やユーザーが必要としている情報と投資家とその株主が必要としている情報は違う。これら全てを第三者開示のようにやるというのは、情報開示が企業目線で、本当にこの情報を必要としている人の目線になっていないのではないか。第三者開示と上のほう（取引先等）のもう少し詳しい話があるというのはとてもいい分類だと思うが、だれの視点に立って企業に対して情報開示を求めるのかということについては、企業サイドの見方ではなくて、社会から見た企業への要求と期待という格好で書いたほうが総務省らしいのではないか。

また、プロの攻撃者だったら当然青の矢印が指している対象もウォッチする。この分科会の議論としては、前提条件が余りにも単純すぎるのではないか。もうちょっと上のほうの情報開示においてどのような注意をすべきかという点が情報開示のポイントで、ちょっと分類が粗いのではないか。

大杉構成員)

資料 8-2 のオレンジの矢印は２つに分けて、真ん中の吹き出しから投資家に向かっている矢印と市民、一般消費者に向かっている矢印の２本に分けてはどうか。あと右の一番下の黒いところから出ている悪意の攻撃者のウォッチ対象の矢印の向かい先というのは、現在の黒い矢印に加えて、上のほうの青色の矢印に対しても点線で下から上に上がっている矢印を付け加えておけば、より現実に起こっていること、起こり得ることをビジュアルで理解できる概念図としてわかりやすいのではないか。大本の骨子案の最初に書くべき点については、野口構成員の御指摘のようになるのではないか。

加藤構成員)

今のお二方の意見に基本的には同じ考え方であるが、野口構成員の御指摘のような形をもう少し推し進めたほうが総務省のガイドラインとしてはよいのではないか。

有価証券報告書等は、開示媒体としてイメージしやすいものではあるが、この報告書の目的等を考えると、社会全体に対して、最終的には消費者を初めとする一般の国民を対象とするということになるので、それぞれバラバラに出すのではなく、共通的な考え方を求めているというのがちょっと見えにくい。そういう情報が必要であるというメッセージを出して、あくまでその実現手段として、今あるような仕組みや何かしらの報告書が使えれば、最初のステップとしてはいいのではないか。

大杉構成員)

資料 8-1 のⅠの 2.の「情報開示の手段」は、企業を初めとする組織、情報を持っている側はこういった媒体を使っていますというので次につながる話であると共に、ここに挙げられているものはだれでも見ることができる典型的な第三者開示の例ですので、開示する側と見る側にとってこういう意味のある文章だということを一言書いていただければよいのではないか。

梶浦構成員)

私も皆さんの意見に賛成だが、矢印の中にもう一組織必要ではないか。企業としては、今定義されているものを開示するのが精一杯であるが、それを右側に記載されている人たちが解釈できるかというと、なかなか難しい。例えば投資家、株主、アナリストに対しては、証券会社がインタープリターとなって、開示されている情報に基づく投資方針の解説を行うことは意味がある。市民、一般消費者に対しては、これは業種によって全然違うが、たとえば、週刊誌のようなメディアがインタープリターとなることにより、情報が手に入り易くなる。開示される側との間にもう一つ組織が必要ではないか。その組織をどうやって育てるかというのが課題であり、企業の努力は当然前提として、ステークホルダーに対して説明をする人をどうやって育てるかというのが今後の課題となるのではないか。株式であれば証券会社等の金融機関、一般消費者向けならば一般的なメディアがその役割を担うことになるのではないか。

石原構成員(代理・教学))

1.の趣旨・目的のところがやはり一番腹落ちするのに重要で、入口のところで企業もしくは担当の方が、そのとおりと思うところが一番重要である。野口構成員の御指摘にあったように社会のためということは重要であるが、開示する側の企業の担当者が、社会のためにこうしようというところまで意識していればよいが、最終的には情報開示の目的は企業間の競争や、自社のアピールであるので、情報開示の意義の重要性と企業の開示に対するモチベーションとの橋渡しをうまくするような内容、目的があればよい。

岡村主査)

情報通信は社会に不可欠なインフラとして定着をしているので、国民生活や企業活動のインフラとして守らなければならないものである。そうした中で、情報開示の手段は、典型的な開示書類に尽きるものではなくて、メディアや、ウェブページ、SNS を利用している企業もある。開示のインセンティブを高めていくかという意味では、コンペティション的な形で開示が進めばよいのではないか。特に御異論なければ、今の点に御留意いただいて、事務局のほうでお進めいただくということでよろしいか。

石原構成員(代理・教学))

競争力維持のために何かやるべきということを言いたいわけではなくて、競争力維持ということがモチベーションになっているというデータが前回提示されたが、そういうことが背景にある人が書こうとしているということを背景にしてそのメリットを示すべきであって、競争力が高まるから書けばいいということをダイレクトに言いたかったわけではない。

岡村主査)

あくまでもインセンティブということか。そこは特に誤解はないと思うので、その点も含めてお願いしたい。

木村サイバーセキュリティ統括官室参事官)

御指摘いただいた趣旨が、骨子だとなかなか反映しづらい部分がある。それを本文に文章化するときに、そういったいろいろな要素を盛り込んで、しっかり反映する。

岡村主査)

そのような方針でお願いしたい。次回は、今の点を踏まえた、たたき台について、1.、2.の点について吟味していただくようにお願いしたい。

秋保構成員(代理・沢井))

社内で開示されたら参考になる項目についてヒアリング調査を行った。予算の実額や、予算が上がったのか下がったのか、どれぐらい上がったのか、全体的な予算のトレンドがわかれば、サイバーセキュリティ予算の確保において非常に重要であるということであった。

岡村主査)

例えばどれだけの人員を充てているかとかいうようなことは、上を説得するに際して非常に効果的な材料ではないか。

大杉構成員)

沢井構成員の発言内容を元の概念図に置いていくと、この③情報は元々企業内に存在するという意味で第一者開示のものが同業他社や業界にとっては関心があるという意味で自発的な第二者開示や、情報を欲している側が取りに行くという場合においても価値が高いということを示している。また、攻撃する側にとっても一番欲しい情報であり、絶対第三者開示されてはいけない情報であるので、第二者開示の価値が高く、第三者開示を行うことの危険性が極めて高い情報というように整理できるのではないか。この 3.「企業における情報開示の在り方」というのは、情報をとる側から見て単に媒体のルート、3.は中身の性質、種類の話なので、全体像をわかるように、いろいろな立場の読み手にわかる文章にしていただきたい。

岡村主査)

3.とおっしゃっているのは③という趣旨か。

大杉構成員)

3.の意味である。

野口構成員)

3.の⑩の「情報共有活動への参加」というのは、どういう内容を書くのか。

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 ISAC や CSIRT 協議会に加盟しているとか、インシデントやサイバーセキュリティ対策に関する情報共有活動、あるいは団体に加盟しているといったことである。

野口構成員)

この内容の必要十分性というのはその内容のどこを強調するかによるので、本来の目的である情報開示方針というのはどこにあるのか。我が社はサイバーセキュリティの情報に対してこういう方針で開示するという、そのリスクマネジメント方針と同じく、当然情報開示方針というのがなければならない。情報開示を訴えようとしているときに最初に書いてあってもいいものが抜けているのは何か変ではないか。

岡村主査)

方針とは、例えば当社はセキュリティに関してはアニュアルレポートで詳しく訴えかけるという手段を中心にやるということか。

野口構成員)

例えばこういうレベルまで開示しますとか、逆にこういうものはここに書きますということ。また、いつまで「管理」という言葉を使うのか。リスク管理とリスクマネジメントは違う。「管理」というと、経営者ではなくていわゆるサイバーセキュリティ部署の仕事に見える。経営者まで含んでサイバーセキュリティを考えるときは「マネジメント」という言葉に移行したほうがよい。「リスク管理」と「リスクマネジメント」はきちっと明確に書き分けるべきである。

岡村主査)

後者の概念にはガバナンスも含まれているということか。

野口構成員)

例えば、運用であるとかリスクの在り方の目標設定であるとか、ほかの目標との相対比較によってどうするかという決定であるとか、いわゆる経営の母体が入る。「管理」というと、それぞれの業務担当者が決められたことをきちっとやってくというイメージ。リスクマネジメントの世界では「リスク管理」と「リスクマネジメント」は明確に分けていて、経営者まで含んでいるときは「マネジメント」を使用する。ISO の規格の「マネジメント」の日本語ももう「管理」ではな

い。経営者を巻き込むのだったら「マネジメント」にしておいたほうがよいし、現場対応レベルであれば「管理」でもよい。サイバーセキュリティのような最先端のものを扱うときには、言葉として使い分けておいたほうがよい。

大杉構成員)

法律とか組織論、経営学のほうでは「リスク管理体制」とか「リスク管理体制の構築」という言葉はもう完全に定着しているので、これを「リスクマネジメント体制の構築」というのに置き換えるとかえって通じなくなる。②番については冒頭に「経営者によるリスク管理体制の構築」と書き加えるのがよい。「管理」という言葉をこの分野の議論から放逐するのは現時点では尚早ではないか。

野口構成員)

情報共有活動への参加が、情報開示も含んでいるのかという点を確認した。

木村サイバーセキュリティ統括官室参事官)

最初の方針について、まさに①のところでそういったことを書くことになる。情報開示の手引きなので、開示に当たっての考え方はここに包含し得ると考えている。

リスク管理なのかマネジメントなのかについては、「リスク管理体制」を残しながら、例えば経営におけるリスク管理体制等、用語の工夫をする。

野口構成員)

用語に関しては、世の中の流れは見てもらったほうがよい。セキュリティ対応方針の中に情報開示方針を入れるとのは、若干無理があるのではないか。

岡村主査)

ISO/IEC 27000 シリーズは、ガバナンス、マネジメント、個々の管理策というような書き分けをしている。

野口構成員)

それが一番近いかもしれない。

岡村主査)

「対策」という言葉を遣うと、個々の管理策と混同されるということか。

野口構成員)

マネジメントシステムの中では「コミュニケーション」と「トリートメント」(対応)とは明確にステップとして分離しているので、対応の中にコミュニケーションを入れるのはマネジメントシステムとしてはきついという意味である。

岡村主査)

会社法上の内部統制に関して「リスク管理体制の」で終わるのではなくて、会社法の、「基本方針の決定」とか「基本方針」というのがついているということ、会社法上の概念を明確化するというような形でまとめさせていただくことでいかがか。

大杉構成員)

本文にしていくときには岡村主査がおっしゃったとおりである。②のあたりの最初の小見出しで、経営者にとって自分に関係がある話だということがわかるような言葉がついていればよい。

岡村主査)

「サイバーセキュリティ経営ガイドライン」、ISO/IEC 27000 シリーズの規定等に留意しつつ、3.は進めていただきたい。文案はできるだけ事前に御意見を募るということで進めたい。

梶浦構成員)

①の対応方針、それから⑩の情報共有活動について、攻撃を受けた場合の被害状況や対処方法を第三者開示する場合の方針があるのが望ましい。さらに、ウィルスの検体、攻撃元の IP アドレス、攻撃手法についても情報共有活動の中で共有をして、協力していることを開示するのが、社会全体のセキュリティを高める上では意味がある。

岡村主査)

何をどう開示したらいいのか、秘匿すべき情報と開示すべき情報について、注か何かに記載していただきたい。

源田構成員)

前回の資料にあった主要５項目との比較で、前回あった③の人材育成や教育という項目がなくなっている。それについてはどういう扱いになるのか。

相川サイバーセキュリティ統括官室参事官補佐)

③の中に人材育成や教育が一応含まれているという認識である。

源田構成員)

人材を育成して、PDCA を回し、時代が変わっていってもその体制が維持できるようにすべきであるという意味で人材育成は極めて重要であると考える。

岡村主査)

次に 4.の「手引きのメンテナンスのプロセスについて」及び 5.「関連ガイドライン等の紹介」分について。

加藤構成員)

項目は ISO/IEC 27000 シリーズをベースにということなので、本当にそれぞれの項目を網羅しているのか。例えばガバナンスレベルとマネジメントレベルで同じモニタリングということであったとしても、粒度が違ったりする。本当に漏れや重複がないのかについて確認をしていただきたい。今回、ぜひその２つの制度、ガイドラインの間でどう整合性をとるかというところの対応していただけるとありがたい。

鵜飼構成員)

普通の会社の反応としては、そもそもこれはなぜ開示するのかということになる。今回、ガイドラインから手引きになったが、インセンティブについての議論は煮詰まっていない。手引きのメンテナンスのプロセスに加えて、普及策についても今後検討する必要がある。

第三者開示に対するニーズが株主からも社会からもそれほどないというのは、経営者から見るとよくわかる。将来的なビジョン、普及をさせていくのだという意気込みが見えるとよい。自分ごとであるという意識を持っていただくために、これを普及させていくのであるという意気込みがあるとよい。

木村サイバーセキュリティ統括官室参事官)

普及促進、あるいは開示へのインセンティブは、この手引きの内容と並行して検討することとしている。この手引きをどうやって普及させていくかという意気込みについては、何かしらメッセージ的なものは入れておいたほうがよいと考えている。

岡村主査)

Ⅱの部分、「サイバーセキュリティ対策の情報開示に係る事例集」についてはどうか。他社は何をやっているのでうちもやらなければというような形のインセンティブはやりやすいのではないか。

石原構成員(代理・教学))

事例があるのはよい。事例や業界、企業規模のバリエーション、こういうところでもこういう開示をやっている例があると実効性がある。

梶浦構成員)

事例については、なるべく具体的な数字で、セキュリティ投資が IT 投資の何%みたいな数字だけでもかなり意味がある。人材についても、CISSP 保持者が何人や、研修受講者が何人というような具体例を出していただけると大変ありがたい。インシデントについても基本的に開示すると一行書いてあるとよい。

大杉構成員)

事務局が集めることができる事例は、ほぼ第三者開示に限られる。実際に企業に求められる開示としては、むしろ第二者開示であるので、第二者開示であれば秘密性・匿名性が守られるが故に、もう少し踏み込んで開示することが推奨されるといったようなことを、注記または解説することになる。

梶浦構成員)

金融 ISAC でも第二者開示までは行っていない。守秘義務を持った状態でインシデント情報やその他の情報を共有するということか。

大杉構成員)

それも含むが、第二者開示というと、事後だけではなくて事前にうちの会社はこういう体制なので、うちと取引すると得であるというのも含む。

梶浦構成員)

ある程度一般解があって、かつ第二者開示的なものというと、組織的なものとしては日本の中にはそれほどないと思う。そういうものもあるという宣伝文句のようななものが入っていれば、今の段階としてはよいのではないか。

ある程度の一般性を持った第二者開示については、このようなものが日本でもできるので、そういうのも利用していく、利用していることを開示することそのものも意味がある。

加藤構成員)

例えば第二者開示の中に含まれるのは、我々が出しているような委託先の保証報告なども含まれるが、中身は一律ではない。どういった項目が基本的にはカバーされているのか、それは共有可能であるが、レポートの読者にどこまで訴求するのか。目的やこのようなやり取りに使える制度・報告があるということを示すことでよいのではないか。

第三者開示の中なので難しいところはあるが、特定の企業の開示の全体を紹介するというよりも、この観点での好事例・ベストプラクティスと、全体としてという両面で出していただけるとつくりとしてはこうなのだ、この観点についてはこういうことまで書けるのだという両面で使えるのではないか。

野口構成員)

実際の開示書類を事例集として添付するというのが制限になっている。非常にいい例がたくさんあればいいが、現実にはそうではないので、これでいいのだと思われる懸念がある。情報開示の「モチベーション」「インセンティブ」という発想から脱却して、サイバーセキュリティは製品やサービスの取引において必須事項なのだという認識を持ってもらうことが大事なのではないか。今後のサイバーセキュリティ社会における企業取引や商売に必須のものであるという認識を前提とするのがよいのではないか。実際の開示書類を事例集としてつけるのであれば、なぜこれを入れてどこを見てほしいかという解説をつけたほうがよい。実際にあったものの事例から考えていくという手段でよいのか既存のものを単に紹介して、これでいいのだと思われないように気をつけていただきたいということと、サイバーセキュリティの情報開示の位置づけを行政が指導するということではなくて、ビジネスを行う上においては当然であるという位置づけに持っていくことが重要である。

岡村主査)

一般論として結構踏み込んだことを書いているのは、委託契約に関しての部分で、個人情報、あるいはマイナンバーに関して個人情報保護委員会が出しているガイドラインの中に、どういう項目をチェックせよというようなことが書かれている。子会社であれば、親会社からの資本の論理であれをやってください、これをやってくださいということは言えるが、取引先については契約によらざるを得ない。委託先選定基準については、FISC が詳しい文書を出しているが、そういうガイドライン類の中でどういう事項を二者間でやるのかということが委託先選定基準でこれを出せというような形で書かれているようなものがあれば参考になるのではないか。

梶浦構成員)

普及について、霞ヶ関と産業界だけでは成り立たない。インタープリターが必要である。メディアの役割は大きく、こういう開示をしている企業はすばらしい、あるいはインシデント情報を隠さずに出した企業はすばらしいと言っていただきたい。情報漏洩があった企業は加害者みたいなたたかれ方をされるが、それだと経営者は隠そうとする。メディアは意識を改めて、これは確かに悪いところはあったかもしれないが、もっと悪いやつは別にいるという目で見ていただく。それら全体の考え方を変えていくようなシンポジウムみたいなものがあればいいと考えている。

岡村主査)

今後、たたき台となる文章が案として出てくるので、それが次回、御提示となる予定である。本日の会合で言い尽くせなかった点があれば、22 日金曜日までに事務局に連絡をお願いしたい。

（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)

次回の会合の具体的な日程につきましては後日、事務局から連絡、調整をさせていただく。

以上