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９回）議事要旨

1. 日時：平成 31 年 4 月 26 日（金）10:30～12:00

2. 場所：中央合同庁舎２号館１０階 第一会議室

3. 出席者：

【構成員】

岡村主査、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、中尾構成員(代理：島村)、野口構成員

【オブザーバ】

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９－１　サイバーセキュリティ対策情報開示の手引き（案）

参考資料　　「情報開示分科会」開催要綱

5. 議事概要

(1) 開会

(2) 議事

◆　事務局より、資料９－１ サイバーセキュリティ対策情報開示の手引き（案）を説明 (省略)

◆　関係者の意見・コメント

（本編の１．本手引きの趣旨・目的について）

野口構成員)

１．本手引きの趣旨・目的の内容はかなりすっきりしていて、この内容であれば、他省庁の活動とも矛盾することなく、整合性が取れている形になっていると思う。

７ページの「（２）サイバーセキュリティ対策の情報開示の意義」について、総務省の社会に対する位置付けをよりクリアにするためには、７ページの一番下の段落に書かれていることが、最初の段落に書かれていた方がよいのではないか。

そのうえで、高度情報化社会では、情報開示を活用してより良いセキュリティ体制を確保するためには、情報を開示する者と開示された情報を受け取る者の双方が正しい理解と評価を行うことが大切であるという文言が入るとよい。

梶浦構成員)

開示された情報を読む人の視点が一番重要だと思う。そのような視点を追記することについて全く異論はない。

加藤構成員(代理・三澤))

総務省として、社会的な意義としてセキュリティの質を上げていくことが重要であるというメッセージを書くのであれば、２ページの冒頭の「はじめに」の部分に入れた方がよい。７ページと重複してもよいと思う。

野口構成員)

強調していただく分には何回でも入っていた方がよい。７ページの「（２）サイバーセキュリティ対策の情報開示の意義」が、普通に読むと企業にとっての意義のように見えてしまうので、重要となる社会的意義を「はじめに」の部分に書いて、７ページの「（２）サイバーセキュリティ対策の情報開示の意義」を企業にとっての意義に限定して記載する方法もある。どちらでもよい。

梶浦構成員)

手引きとしては、読む人の視点が重要であるが、意義としては、どちらに記載されていてもよい。

相川サイバーセキュリティ統括官室参事官補佐)

７ページの「（２）サイバーセキュリティ対策の情報開示の意義」を、もう少し分かりやすくした方がよいという意見だと思うので、上記（２）の書く順番や、「はじめに」の部分に入れることについて、書き方を工夫したいと思う。

野口構成員)

事務局と主査に一任したいと思う。

10 ページの「（３）本手引きについて」で、「①本手引きの目的」がきちんと書いてあって、目的が明確になったと思う。ただし、情報開示の媒体や手法については、今後さまざまなものが出てくると考えられ、そこにも踏み込んで記載した方がよい。例えば、情報開示に関しては、今後新たな媒体や手法が出てくる可能性もあるので、開示の媒体や手法については、状況に応じて使われる最適な媒体や手法の中で選択するという未来志向のことを記載しておいた方がよい。

岡村主査)

「（3）本手引きについて」の「①本手引きの目的」の部分に、なお書きで入れる方法と、「③本手引きで扱う情報開示について」の部分に、なお書きで入れる方法が選択肢としてある。

野口構成員)

「（3）本手引きについて」の「①本手引きの目的」の部分に入れるイメージであり、経営判断で開示の媒体や手法を選択してくださいと入れることで必要十分であるが、さらに媒体や手法が広がる可能性まで含めて幅広く選択してもよいということが記載されていた方がよい。

岡村主査)

「本手引きの目的」のなお書きの部分に、「また」で続けて記載することにしたい。

木村サイバーセキュリティ統括官室参事官(総括担当))

頂いた意見をもとに修正をさせていただきたい。指摘のあった企業の方向性については、今でもさまざまなものがある中で最適なものを選択してくださいというトーンで記載しているので、その流れから大きく外れたものではないと考えている。書く場所についても、「①本手引きの目的」のなお書きの部分に追記する方法と、58 ページの「４．今後の方向性について」の部分に未来志向のこととして入れる方法もある。落ち着きのよい方を選びたい。

野口構成員)

そのとおりだと思うので、事務局と主査に一任したいと思う。

加藤構成員(代理・三澤))

11 ページのサイバーセキュリティの定義について、サイバーセキュリティ基本法の定義が記載されているが、※印を付けて参考情報として原文を付けておいた方がよい。後半の記載例は情報セキュリティが中心になるので、それを含めた意味合いで 11 ページで定義しておいた方がよい。

岡村主査)

サイバーセキュリティ基本法の定義の原文を付けることはできると思うが、その場合に、情報と情報システム、情報システムを繋ぐ ICT の３つが対象となって、それぞれについて何を保護するのかという話になってしまい、CIA 概念そのものについて正面から書かず、それらを示唆するような微妙な書き方になってしまう。また、情報セキュリティの定義についても、改訂版の OECD ガイドラインを含めてさまざまな定義があり、これらを定義するだけで一つの論文になってしまうようなテーマを扱うことになり、本手引きの趣旨から外れる可能性もある。参考としてサイバーセキュリティ基本法の法文を入れるだけにとどめて、それ以上深入りすることは得策ではないのではないか。

加藤構成員(代理・三澤))

情報セキュリティの定義の方については、あまり入っていかない方がよいのではないかと考えている。サイバーセキュリティの定義の中に、情報セキュリティの定義を含めて記載できるようにした方がよい。

木村サイバーセキュリティ統括官室参事官(総括担当))

記載例の中に、情報セキュリティに関わる事例が多いのは事実である。一方で、制御系のセキュリティの取組みについて書かれている事例もある。元々の考え方どおり、サイバーセキュリティを対象として、脚注としてサイバーセキュリティの定義に関する法文を引用し整理するということにしたいと思う。

加藤構成員(代理・三澤))

それで問題ない。

石原構成員(代理・教学))

情報セキュリティ、サイバーセキュリティの定義という論点について、4～5 ページの部分に、個人情報漏えい事案が記載されているが、サイバーセキュリティに関しても事業停止や改ざんなどのさまざまな被害形態があるので、そういう事例も含めて記載することで、サイバーセキュリティを対象とするということを示した方がよい。ただし事例が少ないので、絶対に記載するということは難しいかもしれない。

岡村主査)

可用性や完全性についても視野に入れないといけない。具体例としてはあまり数が多くないが、例えば、東日本大震災時に携帯電話基地局が流出し、携帯電話が通じなくなった事例や、某メガバンクの 3 行統合時に ATM システムが 1 ヵ月停止し、預金の預け入れや引き出しができなくなった事例、大阪 06 区域でワン切りが横行して電話交換機の輻輳が相次いで、有線電気通信法の改正による刑罰によって封じることになった事例などがある。それらを 58 ページあたりに注釈を付けて入れるかどうかについて、事務局の方で検討してもらった方がよい。

相川サイバーセキュリティ統括官室参事官補佐)

4～5 ページの部分で、個人情報漏えい事案が前面に立ってしまっているので、制御系システムの可用性が損なわれるインシデントは日本ではなかなかないものの、DDoS 攻撃によるシステム停止事案というところまで広げれば、可用性をカバーできると考えられる。事例をもう少し調べて何が反映できるか検討したうえで主査に相談させていただきたい。

加藤構成員(代理・三澤))

個人情報漏えい事案以外の事例を入れることは賛成である。海外の事例を入れるかどうかは論点になる。最近の事例を入れるとすると、ワナクライのようなランサムウェアによってネットワークが停止し、事業が継続できなくなったという事例や、病院で手術ができなくなった事例もある。

岡村主査)

今の指摘も踏まえて検討する。

3 ページの「１．本手引きの趣旨・目的」の「（１）サイバーセキュリティリスクの増大と対策の必要性」の第二段落について、ICT 分野のブロードバンド化、クラウド化、モバイル化、IoT 化に伴いという部分の文章で、IoT 化の後ろに「等」を入れた方がよい。AI 等もあるので、趣旨を限定しているように思われないように修正した方がよい。

大杉構成員)

10 ページの１．本手引きの趣旨・目的の「（３）本手引きについて」の「③本手引きで扱う情報開示」についてであるが、今回の情報開示の一種の定義が記載されており、情報開示分科会ではこれまで第三者開示に絞って検討してきた。保険については、開示の対象であり、本手引きの対象になると考えられるが、中小企業の場合は第二者開示あたりになると考えられる。情報開示の定義の話と本手引きへの要望の話が入り混じっているが、最終的に文章の整合性を確保する必要があり、それについて、事務局と主査に一任したいと思う。

（本編の「２．情報開示の手段」について）

大杉構成員)

13 ページの図 5 について、注釈の※1 がどこを指しているかについて明記されていない。図 5 のタイトルの後ろに※1 を入れておいた方がよい。

相川サイバーセキュリティ統括官室参事官補佐)

ご指摘のとおりである。修正したいと思う。

岡村主査)

その他特段意見がないので、「２．情報開示の手段」については、フィックスしてもよいか。

全構成員)

よい。

（本編の「３．企業における情報開示の在り方」の「（１）企業において実施されるのが望ましいサイバーセキュリティ対策」について）

石原構成員(代理・教学))

14 ページの④リスクの把握と対応計画策定について、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策と記載されているが、同じ文言が 30 ページの記載のイメージの部分にも記載されている。双方の用語をそろえた方がよい。またサイバー保険の活用は、リスク移転策であるが、専門ベンダへの委託をリスク移転策と言ってよいのかどうかが気になる。リスクの軽減やリスクの把握が専門ベンダの役割ではないか。

相川サイバーセキュリティ統括官室参事官補佐)

表記の揺れの部分については、統一するようにしたいと思う。

サイバー保険の活用は、リスクの移転やリスクの共有になるのではないかと思う。専門ベンダへの委託については、少し議論の余地がある。例えば、書き方として、リスク移転策ではなく、対策とすることも考えられる。

サイバー保険を例示するかどうかについては、サイバーセキュリティ経営ガイドラインの方でもサイバー保険の活用が明確に記載されており、それを受けての対応であることを考えると、対策の一環として例示があることについては、あってもよいのではないかと考えている。

岡村主査)

リスク移転策が誤解を与えるのであれば、対策とすることも一つの方法である。

石原構成員(代理・教学))

リスク移転という言葉を取ってほしいという趣旨ではなく、サイバー保険の活用はリスク移転の一つの手段であるので、それらはセットで置いておきたい。一方で専門ベンダへの委託については、対策とすることで、それらを分けて考えたい。どちらかと言うと、そのような趣旨になる。

岡村主査)

14 ページの具体的な修正文としては、その際以下の文章で、専門ベンダへの委託を含めた対策・サイバー保険の活用などリスク移転策も検討した上でという形で修正したいと思う。その方向でもう少し文章を練りたいと思う。

木村サイバーセキュリティ統括官室参事官(総括担当))

サイバー保険の活用と専門ベンダへの委託の２つを一緒に括って記載しているので誤解を与えている。その部分を分けて記載するように修正したいと思う。

（本編の「３．企業における情報開示の在り方」の（「２）開示にあたってのポイント」について）

（特段意見はなし）

（本編の「３．企業における情報開示の在り方」の「（３）記載例」について）

石原構成員(代理・教学))

記載例について、さまざまな業界の事例をこのような形で整理したことがないので、業界の横比較ができて、分かりやすい。書きぶりについても業界で統一感がなく、ポジティブに考えると独自性があるということになる。記載例を一箇所に集めてみることの価値が出ていて、面白いという感想を持った。

一方で懸念される点として、一年後二年後になると、直近の事例がないのかという問合せがきて、メンテナンスの労働が大変になると考えられる。

業種が情報開示に積極的な IT ベンダやカメラ機器メーカーにある程度偏っているので、いろいろな業種やいろいろな規模の企業に広がるなど、内容的にももう少し広がればよい。保険業界としては、保険を使ってリスクをヘッジしている事例があまりないのが残念である。そのような事例が出てくると、株主に対して、リスクを把握して、抱えきれないリスクについては保険という手段を使って処理しているというメッセージを出せるようになる。サイバー保険について記載していることの理由付けや意義がもう少し伝わるとよい。

大杉構成員)

記載例の考え方として、日経 225 の対象企業を対象としているので、今回は中小企業が対象外となっている。将来的に中小企業まで裾野を広げることについては賛成である。

大杉構成員)

記載例が長く続くので、企業名からページに飛べるような索引的なものがあるとよい。

岡村主査)

それについても検討したいと思う。特定企業の宣伝になるのは、役所としてはやりにくい面があると思うので、その部分は慎重に検討するということにしたい。

木村サイバーセキュリティ統括官室参事官(総括担当))

企業名とページが上手くリンクするような方法について、やり方も含めて検討したいと思う。

岡村主査)

35 ページの「⑥PDCA の実施」に関する情報開示の記載のイメージの部分に KPI という言葉が出てくる。究極的に、経営者に本手引きを見せるという観点に立つと、経営系、技術系など経営者の背景が多様にわたり、経営者の中には KPI という言葉が分かりにくい人もいると思うので、注釈で簡単な説明を付け加えた方がよい。他の言葉についても、一言あれば分かりやすいものがあれば、それも含めて同様の説明を付け加えることについて必要に応じて検討した方がよい。

大杉構成員)

日本語で言うと KPI は主要業績指標という言葉になる。KPI（主要業績指標）とするのも一案である。

梶浦構成員)

KPI は、会社全体の業績のイメージよりも、サイバーセキュリティ部門の KPI というイメージになると思う。そうなると、KPI（主要業績指標）では意味が通らなくなるので、Key Performance Indicator とそのまま記載した方がよいと思う。サイバーセキュリティ部門の KPI は、なかなか設定が難しく、設定の仕方もさまざまである。インシデント 0 件と設定することがあるが、自分たちでコントロールできない Key Performance Indicator を設定してもよいのかという議論がある。Key Risk Indicator との絡みも難しい。本手引きでは、サイバーセキュリティ部門や IT 部門、CIO/CISO の効率に関する目標値を設定して、それがクリアできたかどうかという意味合いで記載されていると思うので、単純に Key Performance Indicator と記載するだけでよいと思う。

大杉構成員)

日本語の業績と英語の Performance ではそれぞれ思い浮かべるものがずれて、英語の Performance の方が正しい方向に読者が辿り着けるので、指摘のとおりである。

加藤構成員)

KPI の話は一例になる。それ以外の単語や 3 文字系の略語についても、どの人が読むかによって説明を付け加えた方がよいものもあるので、全体を通して確認してほしい。

岡村主査)

57 ページの「⑩情報共有活動への参加」に関する情報開示の記載のイメージに、ISAC やセプター、J-CSIP が記載されているが、これらは 16 ページの注釈で説明がなされている。57 ページにおいても、注釈で詳細は 16 ページ参照という形で記載するなど経営者への心配りを考えてみたいと思う。

源田構成員)

読み手にとっての見やすさや分かりやすさが重要であると思う。「３．企業における情報開示の在り方」の「（３）記載例」の文章とそれより前の文章でフォントや文字列などが異なるように見受けられる。また、現実的に正しいことを書くことと、読み手が分かりやすいということは若干異なる部分があるのではないかと思う。分かりやすさに焦点を当てて検討してほしい。例えば、〇〇性という言葉は正しいが、いろいろなレベルの読み手がいるので、本当に伝えたいことは何かという観点で分かりやすさを検討してほしい。

岡村主査)

フォントや文字列等や、注釈を入れるかどうかについて、事務局において見直し作業を御願いする。

（本編の４．今後の方向性について）

野口構成員)

ここに記載されている内容について異議はない。もし追加ができるならば御願いしたい点について要望を申し上げたい。最後の部分に、「さらに、サイバー技術の変化やサイバーシステムの社会における位置づけの重みが増すということを鑑みた場合に、その変化に適宜対応するために、本手引きの改訂を適宜行っていく。」という趣旨の文章があるとよい。さらに、「また、本手引きについて今回は情報開示を行う企業の視点で解説を行ったが、情報社会において情報開示を適切に進めていくためには、開示された情報を適切に評価するステークホルダーの存在が重要である。今後のそのような視点における手引きについても検討していく。」という趣旨の文章も追加してほしい。

大杉構成員)

現時点で本手引きの改訂の予定が組織の内側になければ、書けないのではないか。

岡村主査)

58 ページの第４段落に、適宜見直しの検討を行うこととすると記載されている。この部分に、適宜頂戴した意見を付け加えるなどの対応を行いたいと思う。

相川サイバーセキュリティ統括官室参事官補佐)

そういった形で対応させていただく。

（参考資料①、参考資料②、全体を通して）

加藤構成員)

今後の方向性として、対象を中小企業や NPO にまで広げるということは意識されていると思われるが、自治体や学校といった対象においても、サイバーセキュリティのリスクは存在している。そういったところまで含めて、カバー範囲は日本全体になるのであれば、将来的にそういったところまで対象にする必要があるといったことを記載した方がよい。カバー範囲はどこまで考えるのかを考えた方がよい。総務省であれば、対象を日本全体にまで広げてもよいと思う。

岡村主査)

自治体や学校はそれぞれの所管の問題もあるので、どのように記載するかは事務局と検討を進めさせていただく。

梶浦構成員)

当然、対象を日経 225 の対象企業に留めてよい話ではない。今後、本手引きをどのように使ってもらうかが重要な話になる。キャンペーンやイベントについて検討してもらいたい。例えば、経団連のトップセミナーにゲストとして参加し、紹介してもらうなど、アピールをしていってほしい。

開示された情報を見て、誰かが噛み砕いて伝えていくことが重要である。一つの候補として証券会社が、A社とB社のサイバーセキュリティの取り組みを評価して、サイバーセキュリティの観点からみると、A社の株が買いであると言ってもらえるような仕組みについて考えていくことができるとよい。証券会社に仕組みづくりを主導してもらえるようにするためのアピールや日経 225 の対象企業を対象とした情報開示の項目や書きぶり、レベル合わせの標準化を進めていってほしい。

岡村主査)

本手引きの活用を広げるための普及策について賛成である。また証券業界でそのような構図を作ることができるとうれしい。企業としても、マスメディアに対しこれだけ取り組んでいるということを積極的にプレスリリースしていくような時代になるとなおさらよい。

相川サイバーセキュリティ統括官室参事官補佐)

本手引きの普及のための方策が重要であると考えている。いろいろなところでの露出に努めていきたい。また、本手引きを使って、どのように情報開示が進んでいくのかといったメカニズムや仕組みについても考えていきたい。

岡村主査)

頂戴しました意見への対応や本手引きの修正については、事務局と相談のうえで実施する。最終的には。主査に一任とさせていただきたい。

全構成員)

主査に一任する。

（今後の会合日程などの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)

手引き案の確定の後、３週間程度パブリックコメントにかける予定である。パブリックコメント後、大きな修正がなければ、次回の会合はメールでの審議.にさせていただくことも視野に入れながら、次回の会合日程については主査と相談のうえ連絡をさせていただく。引き続きご協力のほどよろしく御願いしたい。

以上