サイバーセキュリティ戦略本部　重要インフラ専門調査会
第３回会合　議事概要

１　日時
平成27年10月27日(火)　9：00～11：00

２　場所
中央合同庁舎７号館　13階　共用第一特別会議室

３　出席者（敬称略）
伊澤　雅和　委員　（一般社団法人日本ケーブルテレビ連盟）
石川　広己　委員　（公益社団法人日本医師会）
稲垣　隆一　委員　（稲垣隆一法律事務所　弁護士）
大高　利夫　委員　（神奈川県藤沢市）
大林　厚臣　委員　（慶應義塾大学）
荻島　　敦　委員　（日本通運株式会社）
真田　博規　委員　（住友生命保険相互会社）
鈴木　栄一　委員　（一般社団法人日本損害保険協会）
高橋　泰宏　委員　（石油連盟）
竹原　　達　委員　（電気事業連合会）
千葉　邦史　委員　（株式会社三菱東京ＵＦＪ銀行）
手塚　　悟　委員　（東京工科大学）
西村　敏信　委員　（公益財団法人金融情報システムセンター）
西村　佳久　委員　（東日本旅客鉄道株式会社）
橋本　伊知郎委員　（野村ホールディングス株式会社）
平田　真一　委員　（日本電信電話株式会社）
細川　　猛　委員　（石油化学工業協会）
増子　明洋　委員　（日本放送協会）
松田　栄之　委員　（ＮＴＴデータ先端技術株式会社）
若林　武夫　委員　（公益社団法人日本水道協会）
和田　昭弘　委員　（全日本空輸株式会社）
渡辺　研司　委員（会長）　（名古屋工業大学）

(事務局)
髙見澤將林　内閣サイバーセキュリティセンター長
永井　達也　内閣審議官
谷脇　康彦　内閣審議官
三角　育生　内閣参事官
栁島　　智　内閣参事官
柳原　拓治　内閣参事官

(オブザーバー)
金融庁総務企画局政策課
総務省情報流通行政局情報セキュリティ対策室

総務省地域力創造グループ地域情報政策室
厚生労働省医政局研究開発振興課医療技術情報推進室
経済産業省商務情報政策局情報セキュリティ政策室
国土交通省総合政策局情報政策課
警察庁警備企画課
外務省大臣官房情報通信課
防衛省整備計画局情報通信課サイバーセキュリティ政策室
内閣府防災・災害緊急事態対処

4　議事概要

(1)　開会（挨拶）

髙見澤内閣サイバーセキュリティセンター長から挨拶。

○（髙見澤内閣サイバーセキュリティセンター長）前回会合から３カ月余りの間に、８月にはサイバーセキュリティ戦略本部において日本年金機構における個人情報流出事案に関する原因究明調査結果が決定され、９月４日には、サイバーセキュリティ戦略が閣議決定されるなど様々な出来事があった。戦略においては、サイバーセキュリティ対策の抜本的強化策ということで、NISCの機能強化、政府全体の取組強化のほかに、重要インフラに関する取組の強化も盛り込まれている。

日本年金機構の原因究明調査において、重要インフラにも共通する話として、３点、大きな指摘があった。

１点目は、研修等の充実である。標的型攻撃の対処法を含めて、しっかりと対応し、情報提供も有効に機能するようにということである。

２点目は、インシデントに備えた対策の強化である。CSIRTの整備や、監査も含めて、しっかり進めていくということである。

３点目がシステムの構築、維持、運用の強化である。特に多重防御の取組を加速化させるということで、標的型攻撃も含めて、様々なリスクにきちんと対応できるようにしようということである。

戦略においては、重要インフラの関係については、具体的に大きな２点がうたわれている。

１点目は、社会環境の変化、あるいはこれまでの知見の集積を踏まえて、重要インフラの対象範囲を継続的に見直すということである。この見直しには、深掘りをしていくということと、外縁を広げていくという、両方の意味がある。

２点目が、情報共有の環境構築や体制整備を行い、更に演習・訓練の実施によって、継続的な改善を図るということ。12月には分野横断的演習が予定されており、説明会には、昨年の本番参加者と同じぐらいの人数が参加し、今年は1,000人を超える規模と聞いているが、そういった演習の継続的実施が非常に重要である。

いずれにしても、日本年金機構の事案に限らず、最近のサイバー攻撃への対応を考えると、まず、基本的な事項をしっかりと確認をし、それをさらに定着させ、それを継続しながら、変化にも着実に対応して、マンネリに陥らないようにするということが基本である。

今後、各重要インフラ分野においては、おかれましては、サイバーセキュリティ戦略にもありますように、コストではなくて、投資であるという認識をさらに徹底していただき、また、サイバーセキュリティ水準の一層の向上というのが、企業としても、社会的責任であると同時に、企業の付加価値を高めるという認識を徹底し

ていただいて、さらに発展をさせていただきたい。
本日は、有識者の方々も含めまして、いろいろな御指摘をいただき、また、新たなアイデアをいただいて、率直な議論をお願いしたいと思います。私は途中で抜けますけれども、その後の議論のときには、また帰ってまいりますので、今日は、ひとつよろしくお願いいたします。

渡辺会長から挨拶。
○（渡辺会長）皆様、おはようございます。本日もお忙しい中をお集まりいただきまして、ありがとうございます。
先ほどのセンター長の御挨拶に重なるところもありますが、本専門調査会は、今年の３月に発足いたしまして、第２回を７月に開催して、今日は３回目になります。
その間、これもございましたが、日本年金機構における情報流出事案を初め、サイバー攻撃によるものと思われる事案、こういったニュースが後を絶たない状況が続いてきております。むしろ増加しているということになります。
特定の企業あるいは政府機関を狙った、いわゆる標的型攻撃が、我が国において広く社会的に問題化したのは、思い起こせば、４年前ぐらい、23年ぐらいだったと思いますけれども、以降、年々増加の傾向にあるだけでなく、その手口自体が巧妙化しているということと、目的もかなり複雑になっている、あるいはターゲットが絞られてきている。そういう意味では、今回の年金機構のことは、非常に大きな事案として、個人情報が大量に流出していたことが、現実に確認されたという事案としては、大変大きなインパクトがあったと認識しております。
我が国の重要インフラにつきましては、幸い、まだ大規模な攻撃に遭うことはなくて、国民の生活、あるいは社会経済活動に多大な影響を及ぼす事態には、まだかかっていないということでありますが、これは前回も申し上げたと思いますが、既に攻撃を受けているけれども、気づいていない部分があると思います。こういった潜在的事案が、恐らく事務システムとか、業務系のシステム、あるいは制御システムに対して、いつ大規模な攻撃を受けてもおかしくないという状況を醸し出している可能性が高いとも言えると思います。
このような状況におきまして、我が国の重要インフラのサイバーセキュリティに関する調査・検討の場であります、この専門調査会の重要性は、ますます高くなってきている。これは間違いないということです。
本日の会合は、お手元の議事次第にありますように、NISC、各省庁から施策の取組状況について、まず御報告をいただきます。それから、これは皆様方からの御意見をいただきたいところですが、重要インフラ分野の範囲の見直しの方向性、情報共有の体制等について議論いただく。ここが大きな論点になると思います。
毎度のことではございますが、委員の皆様におかれましては、本専門調査会での審議及び検討というものが、我が国全体の重要インフラ分野において、大変重要な役割を担っているということを、改めて御認識いただいた上で、闊達な御議論をお願いいたします。
以上でございます。
それでは、早速、本日の議事に入らせていただきます。
まず本日の会合の配付資料及び出欠の確認等について、事務局よりお願いいたします。

(2)　報告事項

【第３次行動計画等に基づく施策の取組状況等について】

総務省から、資料２－３に沿って説明。質疑応答は次のとおり。

○（増子委員）細かいことで恐縮なのですけれども、今、いろいろ施策を聞いていて、現場に近い人間なので、教えてください。

この中で、③の個人番号利用事務関連システムからの端末データの持ち出し不可設定というのは、現場的には一番大変なような気がするのですけれども、もう少し具体的に何をやろうとしているか、教えていただけますか。

例えばやり方としては、私どもも似たようなことがあるのですけれども、全員パソコンを２台持ちにするとか、いろんなやり方があるのですが、自治体ではどうやられているのでしょうか。業務上、やっている方が、全国に恐らくいっぱいいる中で、変えようとしているのは、現場的にはどういうことをされようとしていますか。

○（総務省）まさに自治体の取組に関しましては、今、自治体と意見交換をさせていただいているところでございますが、いろんなやり方があろうかと思います。ただ、１つのやり方といたしましては、端末にソフトウェアを組み込むことによって、USB等を入れても、情報が取り出せない、そういう形が１つの対策としてあり得るだろうということで、考えているところでございます。それ以外の方法であっても、構わないとは思いますけれども、１つとしては、そういうことを考えているところでございます。

○（稲垣委員）総務省におかれては、マイナンバーは大変だと思うので、ぜひ頑張っていただきたいと思います。

大高委員がおられる前で発言するのは、いかがかと思うのですけれども、自治体といっても、御案内のとおり、規模は相当偏差があります。聞くところによると、1,000人以下の自治体も多数あるわけで、その中で、一番の困難は、こうした番号制度に限らず、システム調達の際の仕様決定とか、調達要件をどういうふうに定めるのか。ここにセキュリティ要件をどう入れるのかとなると、非常に難しくて、今度、保守・運用になってくると、ほとんど自力でやることは困難だということになるので、例えばISMSとか、セキュリティ監査とか、調達に際してのシステム監査とか、そういう能力が必要になってくるというのは、前々から言われているところです。その辺も自治体の特性があると思いますので、外部調達も大事ですけれども、自力でそうした人材を整備する方向での集中的な予算の投下が、この時期、必要なのではないかと思っている次第です。

それがないと、結局、自治体事務というのは、これからどんどん広がっていく可能性を秘めていて、日本の中でも重要な産業分野というか、大事な分野になると思うのですが、全体を底上げすることが、自治体の細かい事務があったりしますので、自力で人材を内製化する作業が必要だと思います。ですから、その辺も含めて、この時期に集中的に検討いただけると、底上げになるのではないかと思っておりますので、どうぞよろしくお願いします。

○（総務省）ありがとうございます。

抜本的強化の中でも、まさに市町村さんに対する都道府県さんの支援的な役割だとか、あとは、政府全体の中での人材育成の促進、こういうものについては、自治体の方々に対しても、同じようにやらせていただければと思っておりますし、また、今の内製とはまた別ではございますけれども、専門人材とのマッチング、こういうものもあわせてやらせていただいて、全体としての底上げを図らせていただければと

思います。引き続きどうぞよろしくお願い申し上げます。
事務局から、資料２－１に沿って説明。
金融庁から、資料２－２に沿って説明。
総務省から、資料２－４に沿って説明。
経済産業省から、資料２－５に沿って説明。
警察庁から、資料２－６に沿って説明。
全体を通しての質疑応答は次のとおり。
○（稲垣委員）警察庁に対して、質問とお願いがあります。
サイバーフォースセンターへの情報の集約、それを社会に寄与する形で、アウトプットするという取組が強く始められたことについては、非常にありがたいことだと思っております。現実に基づくこれを生かした対策がないと、空理空論に基づくものになってしまう。
お願いなのですが、お伺いすると、技術的な知見については、相当フィードバックがなされるように思うのですけれども、例えば社会においては、経営層あるいはその下のマネジメント層がどういう管理とか、統制をしていけばいいのか。
例えばここでも安全基準などをつくるときに、ISOの27000シリーズとか、制御系についても、マネジメント層あるいは経営層に関する企画などもありますし、被害に遭う主体とか、防護の主体の経営とか、統制に関する知見も、事件を通じて、相当集まるのではないかと思います。そうしたことについても、フィードバックという意識があるのではないかと思うのですが、その辺を明らかにしていただいて、具体的な今後の展開のあり方についても、十分にお願いしたいと思うのですが、いかがなものでしょうか。
○（警察庁）稲垣先生、どうもありがとうございます。
先生が御指摘のとおり、技術的な知見については、Policeというポータルサイトを通じて、広く公に注意喚起しているところでございます。確かにそれぞれの事業者の皆さんとの意見交換を通じて、いろいろなノウハウが蓄積されてきたところでございます。
他方、それぞれの事業者の皆さんは、所管省庁もございますので、今、NISCを通じて、政府機関内での情報共有を進めておりますので、その中で、経営層にさらに高い意識を持っていただくような方向で、動けるような施策を、関係省庁と協力しながらやっていきたいと考えております。
以上でございます。
○（稲垣委員）連続で申しわけありません。
今、情報とか、ネットワークのセキュリティに関しては、報告があったのですが、それぞれが所管している省庁で、事業者が持っている制御系のシステムについては、経産省からCSSCの話がありましたけれども、それぞれ重要な問題があろうかと思います。しかも、オリパラは、制御系についても大事なことがあるのですが、やはり分野が少しずれるということで、遅れているように思います。
座長の御専門でもあるので、恐縮なのですけれども、この辺は、各省庁あるいはNISC全体で現状把握の取組とか、今後に向けた取組が進んでいるということで、承っていいと確信しているのですが、その辺は、念のためお聞きいたします。
○（栁島内閣参事官）今、御指摘いただきました、制御系についての取組みというのは、M2Mとか、IoTというところで、非常に重要になってきているという認識につきましては、我々としても共有しているところでございます。

その一環といたしまして、先ほど経済産業省からも御報告がありましたとおり、CSSCという取組も始まっているところでございます。
一方で、その他、いろんな各分野におきましても、いわゆる制御系というくくりもありますけれども、各分野において、そういった制御系を使ってきているところもあると思っておりまして、そういったところの分析なども進めていかなければいけないと考えているところでございます。
この場合におきましても、今回、次回につきましては、違うテーマでございますけれども、制御系の取組みについても、この場において、今後、議論していただいて、方向性を出していきたいと考えてございます。
取組みについて、十分かと言われれば、まだ十分ではない部分もあるかと思いますけれども、ただ、セキュリティの分野は、一朝一夕に、全てが一気に解決するということではなくて、着実にステップ・バイ・ステップでやっていかなければいけないと思っておりますので、その点につきましても、皆様方からの御意見を拝聴しながら、進めていきたいと考えております。

○（稲垣委員）認証規格などは、国際的に見ても、必ずしも十分ではない。機器認証についてはできるけれども、全体のシステムについては、まだ不十分なものが多かったりして、例えば我が国がサイバーセキュリティ戦略の中で、国際的な優位を確立するために、非常にいい分野がまだ残されていると思いますので、国際競争力の強化とか、認証も含めて、ぜひ強く進めていただけたらと思います。
以上です。

○（渡辺会長）ありがとうございます。
そういう意味では、今、経産省が所管されている、４分野が走っておりますけれども、その他の分野についても、各省庁で確認ができるような論点を、討議項目として入れていただくことを、事務局にお願いしたいと思います。
そのほか、いかがでございましょうか。よろしゅうございますか。
特段ないようでしたら、ここで、質疑応答は切り上げさせていただきたいと思います。
そういう意味では、これにて、本件の報告事項は、了解したということにいたしたいと思います。どうもありがとうございました。

その他、特段の意見・質問はなく、報告事項について了解された。

(3) 討議事項

【重要インフラ分野の範囲見直しの方向性及び情報共有体制等について】

事務局から、資料３に沿って説明。資料及び討議内容は非公開。

(4) その他

その他、各委員からの特段の発言はなかった。

(5) 閉会