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５回会合　議事概要

１　日時
平成28年３月25日(金)　10：00～12：00

２　場所
中央合同庁舎４号館　12階　全省庁共用1208特別会議室

３　出席者（敬称略）
有村　浩一　委員　（一般社団法人ＪＰＣＥＲＴコーディネーションセンター）
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）
大平　充洋　委員　（一般社団法人日本クレジット協会）
荻島　　敦　委員　（日本通運株式会社）
金子　　功　委員　（一般社団法人日本ガス協会）
真田　博規　委員　（住友生命保険相互会社）
神保　　謙　委員　（慶應義塾大学）
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）
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）
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）
盛合　志帆　委員　（国立研究開発法人情報通信研究機構）
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
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
外務省大臣官房情報通信課

4　議事概要

(1)　開会（挨拶）

渡辺会長から挨拶。

○（渡辺会長）本専門調査会は、今回で第５回、前身の重要インフラ専門委員会から早くも１年が経っている。この１年間、日本年金機構に対するサイバー攻撃事案を初め、民間、行政機関を問わずサイバー攻撃に関する大きな報道があった。その矢先に、昨年12月にウクライナで大規模な停電があり、この原因がサイバー攻撃であったということが確認されたという意味では、最初の事例であるという形で報じられています。そういう意味で、海外の事例ではあるが、重要インフラがいよいよサイバー攻撃によってサービスが止められるという状況が現実にあったということを認識しなければいけないと思っている。この報道によると、電力供給を遮断するスイッチが巧妙に操作されたとか、バックアップのシステムが使えないようにしてあったということは、事前にそういった制御系の情報が筒抜けになったということが原因かと思われる。さらに、それを自由に操作できる状況にもあったということになる。我が国の重要インフラはその状況にはないと信じたいわけだが、それを具現するためには、まずは行動計画に基づく取組を一つ一つ確実かつスピード感を持って実行していくことが大事であると考えている。それに加えて、重要インフラを取り巻く状況は、自由化を含めて常に変化しているうねりが来ており、こういったことに対する対応をより柔軟に行っていく必要がある。今回の議論は、こういった環境の変化、あるいは強化が必要な取組の方向性について、来年度末の行動計画見直しに向けたロードマップの討議をお願いしたい。

(2)　報告事項

事務局から、資料２から資料７までに沿って説明。

ここまでの説明についての質疑応答は次のとおり。

○（有村委員）分野横断的演習について、中長期的な課題というかサジェスションについて、１点目は各事業者のところでファシリテートをしていたサブコントローラーの方々は、かなり業界独特の、あるいはその分野の企業の皆さんがはっとするような事例をシナリオとして仕込むということをやっており、かなりロード（負荷）がかっているのは間違いないと思う。そういう方々に対して、例えば３回サブコンをやったら、認定するとまでは言わないが、政府の業界横断の演習の中でしかるべきロールをやったということで、表彰というようなことを今後考えてもよいのではないかと思う。

　また、大阪会場、東京会場、それから今度は九州もやるという話だが、特に地方の会社の幹部の方々に、VIPの見学をしていただき、少し見ていただくのが良いと思う。

○（事務局）我々も取組を進めたいと思っているので、また検討会の中でも今の意見を紹介して、検討してまいりたい。

○（稲垣委員）セキュリティに関するさまざまな取組については、サイバーセキュリティ戦略の中で、現実にセキュリティの効果を確保する、PDCAを回す体制を整える、それをやるという段階から、そうした取組を日本の産業の、あるいは取組の主体の品質に付加価値としてきちっと表明して、国際競争力に結びつけ、日本の産業やサービス強靭性を高めることで、元気な日本、価値のある日本を作る。そういう目的との関係で、今のサイバーセキュリティ戦略の中でのセキュリティの位置付けというものが変化してきたと思う。安倍内閣での戦略がそうした変化を鮮明にしている。今まで、ここは現実のシステムセキュリティを確保するために連携するというところから始まり、今やそんなことは当たり前のことであって、これをどういうふうに日本のためにしていくかという機能なり作用というところで考えている状況。そうした時に、今の有村委員の御指摘、つまり真面目にやっている、あるいは役に立っている企業、あるいはそうした実績を積んでいる企業については、具体的に言うと例えば演習参加とか演習に対して寄与ができる企業であるということを対外的に表明して、それを企業の価値に使えるようにしてあげるというのは、すごく現実的にサイバーセキュリティを価値にしていくためには重要な方法の一つだと思う。そういう意味で、ただ単に表彰するというレベルを超えて、戦略の目的に適合する仕事になると考えるので、検討していただきたい。

また、VIPの参加ということがあったが、これも戦略の中でやっと経営層のところまでたどり着いたというところがある。私もあるCSSCの中での演習に参加、傍聴したが、後の「ざわざわ会」に出て何が語られているかというと、この議論をぜひ経営層に届けたいのだが、なかなかうまくいかない。全部潰されるという声が聞かれる。だから、それこそ外からそういう声を直にVIPに聞かせるというのもすごく大事なことで、それはただ聞かせて認知させるというだけではなくて、そうした声が伝わらないガバナンスがあるということ。そういうことに気づきを与えることが経営課題としてのセキュリティに対する取組の一番大事な事柄になる。

あわせて、同じ問題意識に基づいて言うが、これまでの取り組みの中で物すごく評価すべきことがあると思う。それは参加者のセグメントをどんどん広げていったということです。特に御報告を伺っていてすばらしいと思ったのは、例えば今回の演習ではCSSC、FS-ISAC、T-ISAC、その他さまざまなチャンネルとの連携を図りながら演習をしていったということはすばらしい広がりへの取組だと思う。この背後には、例えばFS-ISACなんかは、もう日本の中で非常に多くの、ほぼ全ての金融機関が参加している。Telecomー ISACもきっとそうでしょう。つまり、ここが取り組むことによって、オールジャパンでの取り組みが一部の演習、限られたリソースを最大限に利用するという効果を生んでいると思うので、是非こうした広がりを大事にして取り組める環境を作っていってあげたい。そして、参加者が価値を自分で表明できるような仕掛けを作る。経営もそれが分かるような仕掛けを作ることが大事だと思うので、検討していただきたい。

最後に、広がりという点と、あとは競争戦略という観点であるが、我々に欠けているのは、何をしろというところまでは初期段階でやった。何をするということで、セキュリティ、つまりシステムを使っているユーザーのところまでは行っている。だから、演習などはユーザー企業が来て、運用をやっている。ここで課題があって、是非これをユーザーを助ける主体、つまりベンダー、システムベンダー、セキュリティベンダー、コンサル、さまざまな事業者がいる。ユーザーが何をすべきかを認識したときに、実際にやらせるのは自分ではなくて、そういうセキュリティベンダーなど業者を使うのです。そうすると、そこの業者が何をやるべきかということの市場がきちっと見えれば、日本独自の商品開発に結びついていくということがあると思うので、参加するセグメントを

広げるという目標を持ちながら、どういうふうに公開するかはすごく難しい課題があると思うので、その目標を持って拡大、拡張していく。つまり、現実の作り手まで広げていくという方法を今後、討議していただきたい。

○（渡辺会長）今、両委員から、やっている方々の場で組織のインセンティブとかモチベーションを確実にするということであったり、経営陣を含めたガバナンスの話であったり、今後の演習の進め方におけるセグメントをシステマティックに広げていくという、有機的につながるようなことが今後の課題であると認識しました。

○（大高委員）今、稲垣委員から話があった、いろいろな関係者というのは、重要インフラの組織だけではなくて、関わりのあるところにお願いしなければいけないところもかなり多い。今回、演習の部分については参加者がものすごく増えて、300を超えたということだが、それでもまだまだ組織の中では全体からすると１割というところもあり、将来的に全てが参加というのは現実的ではないので、このセプター訓練というのは非常に重要だと思う。訓練と演習の違いで、演習で与えられた課題だとか、特にサブコントーラーさんがいろいろなシチュエーションを考えていただいたことに対するものを、逆に訓練の素材として、重要インフラの事業者全体の中で考える課題として、特にサイバーセキュリティに対してはこういう状況になったら自分のところではどうするのだと考えることが非常に重要である。そういう意味では、いろいろな関係者にこれはお願いしないとできないもの、自分たちでできるものというようなことを常々考えることが必要だと思うので、セプター訓練で行う、さらに組織内で考える、そういう流れを作って、その組織が演習に参加しても違和感がないようにという形の流れが作れないかと、検討をしていただきたい。

(3)　討議事項

【重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップについて】

事務局から、資料８－１から資料８－２までに沿って説明。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

髙見澤内閣サイバーセキュリティセンター長から挨拶。

○（髙見澤センター長）　前回からちょうど１年経って、課題についてこの間いろいろな議論をいただき、感謝申し上げる。これからのことを考えると、さらに、できるだけ前広に皆様方の考えを取り入れながらパワーアップしていかなければいけないと思う。幾つかは今後を考える上での要素であるが、まず一つは、今回、重要インフラということをめぐって、オリンピックもあるし、サミットもあるわけだが、やはり重要インフラ13分野だけではなくて、それに関連するようなところも捉えて、いろいろな取り組みをしていかなければいけないということが、はっきり今出てきているのかと実感した。これはマイナンバーの話でもそういった話があったが、例えばサミットならサミットということをとっても、単なる重要インフラというだけではない、より幅広いところというのも考えていかなければいけない時代になっているのかなということが一つである。

２つ目の要素としては、東京オリンピック・パラリンピックがあるが、今回のフランスのパリのテロであるとかブリュッセルのテロというようなことを考えると、やはりそういったテロとの

関係ということを考えても、いろいろなセキュリティでサイバーの世界におけるいろいろな情報のやりとりというようなことも含めて、従来以上に課題が増えているという感じがしているところである。

３点目として、私どももいろいろな行動計画を作ったり、いろいろな基準を出したりしているわけだが、やはり変化が激しいということであるので、常にアップデートを図っていく。また、我々自身も柔軟性を持っていかなければいけないというようなことが、より明らかになっている。

サイバーセキュリティ基本法も、考えてみると、できて、施行されて、やっとというところで日本年金機構の問題が起き、そして昨年来また議論をして、また法案を審議いただくというようなことになっているので、我々としては感度よく先進的な取り組みをしていきながら、それで足りないところはまた法的措置も考えるというような、こういうことの繰り返しになるかなと思っており、皆様方におかれても、それぞれの現場で感じておられるような問題意識をできるだけ前広に私どもの方にいただき、我々もまた問題提起をしていきたいと思っているので、引き続きよろしくお願いしたい。