サイバーセキュリティタスクフォース（第 42 回）議事要旨

1. 日 時）令和 5 年 2 月 1 日（水）16：00～18：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、鵜飼構成員、岡村構成員、小山構成員、篠田構成員、園田構成員、辻構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、安田構成員、吉岡構成員、若江構成員

【オブザーバー】

内閣サイバーセキュリティセンター、デジタル庁、経済産業省、地方公共団体情報システム機構

【総務省】

山内サイバーセキュリティ統括官、内藤官房審議官（国際技術、サイバーセキュリティ担当）、小川サイバーセキュリティ統括官室参事官（総括担当）、酒井サイバーセキュリティ統括官室参事官（政策担当）、佐藤サイバーセキュリティ統括官室企画官、廣瀬サイバーセキュリティ統括官室統括補佐、井上サイバーセキュリティ統括官室参事官補佐、高地官房サイバーセキュリティ・情報化審議官、須藤自治行政局住民制度課デジタル基盤推進室課長補佐

【発表者】

松原実穂子（NTT）、小宮山功一朗（JPCERT コーディネーションセンター）、今宮拓也（総務省近畿総合通信局）

4. 配付資料

資料 42－１－1 国際連携に関する最近の取組
資料 42－１－2 ウクライナ情勢と今後の台湾情勢への示唆（NTT）（非公開資料）
資料 42－１－3 サイバー安全保障がもたらす国際連携の新たな課題（JPCERT/CC）（非公開資料）
資料 42－２―1 関西サイバーセキュリティ・ネットワーク（地域 SECUNITY）の取組について（総務省近畿総合通信局）
資料 42―２－2 ナショナルサイバートレーニングセンターの取組（園田構成員）

5. 議事概要

（1）開会

（2）説明

◆議題（１）「「国際連携に関する取組状況と課題について」について、事務局より資料 42-1－1、NTT 松原氏より資料 42－１－２、JPCERT 小宮山氏より資料 42－１－３を説明。

◆構成員の意見・コメント

小山構成員）

松原さんと小宮山さんにそれぞれ一つずつ質問したい。松原さんには、今年 5 月に広島で G7 が開催される予定であり、今まで以上に攻撃を受けるリスクが高まっていると誰もが考えていると思うが、注視すべきポイントをご教示いただきたい。小宮山さんには、資料最後の一行に「ルールの空白地帯にいる通信事業者」という記載について詳しく教えていただきたい。

NTT　松原氏）

G7 のような政治的な大きなイベントでは、ハクティビストによるイデオロギーを発露するための攻撃は注意しなければならない。今回はおそらく G7 の期間中も現在のウクライナ情勢が継続している可能性が十分にあるので、昨年日本に対して DDoS 攻撃を行ってきたキルネットのように、ウクライナを支援している国の一つとしての日本に対する攻撃を、見せしめのために行う可能性は十分にあると考えている。もちろん今回の情勢において活動している親ロシア派のハクティビスト集団はキルネットだけではないため、こういった集団がどのような攻撃目標を立てているのかはテレグラムのチャンネルなどを見ながら脅威インテリジェンスに注意する必要があると思っている。

JPCERT コーディネーションセンター　小宮山氏）

松原さんの説明で、ウクライナで通信事業者が非常に過酷な環境にあるという話が出てきたが、昨年長崎の NTT ワールルドエンジニアリングマリン社の資料館で資料を見たところ、これまで日本が関わった戦争を振り返ると通信事業者は絶えず過酷な環境に置かれていた事が分かる。例えば戦前、日本と上海間で電信のラインがあったが、それを保守運用していたのがその後の総務省や NTT、KDDI の母体となる逓信省だった。逓信省は軍隊ではないのにもかかわらず上海事変の際には通信局の稼働を継続するために文字とおり血を流しており、その後の日中戦争、太平洋戦争へと続く。元逓信省の方々が海底ケーブルを敷設したが、敷設のための船は常に他国の標的となり多くの方が命を落とした。同様のことは今後の戦争にも起きると思われ、21 世紀においてはデータセンターへのミサイル攻撃や、発電所に何かが起きるという形かもしれないが、通信事業者が真っ先に狙われるという認識が日本にはまだあまりないのではという問題意識を持っているため、保護されていない通信事業者という形で記載した。

吉岡構成員）

小宮山さんがおっしゃった安全保障のジレンマの話はそのとおりと思う。大学の研究でサイバー攻撃やスキャンの観測などを行っているが、以前はスキャンによるセキュリティ環境の偵察行為は感覚的な敷居がもっと高かった気がするところ、今はお互いやらないと情報を取っていない方が不利になるため 10 年前と比べて毎年その数が増えている感覚があり、それと似ていると思った。一方でそのジレンマを解消する方法が見当たらず増える一方で、特にサイバー攻撃の場合は自分たちのポリシーや行動を情報発信したところで誰がどうやっているかは分かりにくいため、お互いの信頼関係も得にくく改善が非常に難しいと思う。この状況を改善するためにどのようなアプローチがあるのかアイデアがあれば教えていただきたい。

JPCERT コーディネーションセンター　小宮山氏）

そのような状況において必要になってくるのが規範である。今我々はインターネット上で色々な機器をスキャンしているが、政府だけではなく民間企業や大学の研究者などもスキャンを行っている。攻撃ではなくあくまでスキャンであるため問題無いが、サイバー空間における行動として、NOTICE よりも踏み込んだもう少し緊張感の高い行動を取るのであれば、それは民間企業ではなく政府が行うべきというルールを作れば、少なくとも何かが起こった時の責任の所在は明確になり、意見や抗議をする対象も決まってくる。既にいくつかのルールが提案されているため、もう少し調べて今後お話ししたい、

吉岡構成員）

おっしゃるとおり、スキャン行為には割と表立って行われているものと完全にアンダーグラウンドで行われているものがあり、実際にログインして機器に侵入できるかどうかの情報がアンダーグラウンドでは売り買いされているが、実際にはどこで誰がスキャン行為をしているかはわからないので、やり合うという状況が生まれているのかと思い質問した。

林構成員）

普段取り上げないテーマを適任の方に発表いただき勉強になった。今回の安保関連の文書を読むと情報がいかに大切かということが随所に書いてあって、いよいよそういう時代になったという思いを強くした。小宮山さんの発表に関連して、太平洋戦争終戦時に樺太で最後まで電話を止めないために殉職した「9 人の乙女」の話があるが、人が接続しなければ通信が成り立たない時代があったことを思い出した。いずれにしても、この問題は情報という概念でインテリジェンスと非常に関連した仕事であるにも関わらず、インテリジェンスの在り方をどうするのか中々方向が定まっていないのは問題だと思っている。総務省の所管ではないかもしれないが、色々な機会でどうあるべきかを固めたうえで、日本の立場が生かされるように国際的なフォーラム等にインプットしていければいいと思う。

藤本構成員）

日々企業等のリスクマネジメントなどを考えていると、能動的サイバー防御の話などを聞くと遠い話のような気がしていたが、小宮山さんのお話にあった「予防的な対応」については、一般の企業でも予防の観点から能動的サイバー防衛などについて何か準備をする必要があるのか。例えば能動的サイバー防御に関するルール形成がされるのを待ってから、ルールを踏まえた対応を各一般企業が行うスタンスになるのか、今から収集して置くべき情報等、準備をしておいた方がいいことがあればお伺いしたい。

JPCERT コーディネーションセンター　小宮山氏）

能動的サイバー防御がどういうものかは明確に定義されていないので、日本の重要インフラ企業の方が何かをするというフェーズではないと思っている。その一方で、重要インフラ企業に関して気がかりなのは、日本が能動的サイバー防御をした際に、その相手国からの報復が重要インフラ企業に為される危険性である。

NTT　松原氏）

「アクティブサイバーディフェンス」という言葉はかなり問題のある言葉で、定義をする組織によって意味が異なる。最初は米軍が定めた言葉だが、米軍も NSA もイギリス政府も基本的には防衛のみで攻撃能力は含めないと定義している。あくまでも脅威インテリジェンスを活用することで積極的に自分たちの防御に穴がないかを探し、「アクティブサイバーディフェンス」は実際に攻撃被害を受ける前に悪用されてしまうような脆弱性の穴を埋めて、被害を受ける可能性を限りなく小さくしていくというものが当初の意図である。防衛の用語には「アクティブサイバーディフェンス」以外に「アクティブディフェンス」という言葉があり、これには反撃能力も含まれている。「サイバー」の言葉の有無によって反撃能力が含まれるか含まれないかが変わってくるため、おそらくそこから混乱が始まり、人によっては、アクティブサイバーディフェンスに反撃能力が含まれる理解となったのだろう。今回の防衛 3 文書に出てくる「能動的サイバー防御」に反撃能力も含まれるのであれば、そうした攻撃には企業が関わることはできない。小宮山さんがおっしゃったように、大規模な攻撃被害を受けた際には国家として、制裁や反撃など何らかの対応が求められる。場合によっては、エスカレーションが発生するかもしれない。そういったことも見越して、前広に防衛能力を高めていくことは、これからどの国の企業においても求められて

くると思う。

安田構成員）

松原さんに質問で、ウクライナ情勢においてメディア（放送局）に対するサイバー攻撃の状況に関する情報はあるか。

NTT　松原氏）

まさに先週起きたばかりで、ウクルインフォルムというウクライナ政府系のメディアがあるのだが、これに対してロシアから 5 種類ものワイパー攻撃が仕掛けられたとウクライナ側は主張している。

（以下チャット欄より抜粋）
若江構成員）

感想になるが、小宮山さんの指摘のとおり、国際法などの観点から、許容されるサイバー活動と許容されない活動についてのルール作りは急務だと思う。一方で、条約レベルまで拘束力のある合意を形成するのは難しいかと思うが、今後の日本がそういった議論において一定の主導権を握って進めていくために必要だと思うことがあれば教えていただきたい。国際的なルールメーキングの場でルールを作ることのできる人材の育成も必要だが、どのような素養が必要で、どう育成していけばいいのか。

JPCERT コーディネーションセンター　小宮山氏）

一発の会議では英語でのプレゼンテーションなどの個人技が大事だが、ルール形成は短くても数年かかるため根気のほうが大事。国際法と技術が両方分かる人材が必要。

NTT　松原氏）

国際会議で渡り合える人材に必要なのは、語学や専門知識だけでなく、教養とユーモアなどの人間力、そしてその場でぱっと反論、場をなごませられるか、とりまとめられるかという即応力だと思う。また、明るい人柄でないと、周りの人はついてこない。許容されるサイバー活動の線引きについては、2022 年末にキーウの地下鉄構内でハッカソンが開かれた際、IT 軍の扱いについても議論された。ただし、ウクライナの人々の間でも意見が分かれたそうだ。

篠田構成員）

国境を超えた意見交換・人材交流・人材育成にこれまで積極的に取り組んできた。GCC なども他国組織と協力して教育しているが、サイバーセキュリティ教育はどうしても技術面での教育に寄りがちで、これは海外の大学なども認めている。そのため、技術ではない部分を考えるきっかけづくりをより強化していきたいと改めて思った。今日言及がなかったサイバー空間の分離について、具体的にどのような状況になりえるのか、私自身も研究していこうと思う。

NTT　松原氏）
篠田様からのコメントについて、米国の大学・大学院では、必ずしも技術寄りではないサイバーセキュリティの学位が取れるようになっている。MBA、法律、安全保障、インテリジェンスなどとも組み合わされていると思う。

篠田構成員）
米国の大学・大学院での学位が技術寄りではない点については、確かにそうである。国内の日本語でのサイバーセキュリティ教育はさまざまな課題があり、整備に向けて IPA の委員会でも議論中。個人的な勝手な妄想だが、NISC に変わる新たな組織が統率して、米国のような、雇用側・教育側・受講側の双方の Wants が交わるフレームワークを提示し、認定していく仕組みを、「個人的に」勝手に期待している。

JPCERT コーディネーションセンター　小宮山氏）

サイバー空間の分離のご指摘については、性能的には申し分ない有名海外製品を日本企業の多くが採用していない実情からもその分離を見て取れる。信頼醸成の手段として教育段階での連携があるので、国際的な教育の場は益々重要になると思う。

篠田構成員）

有名海外製品を使わない例えは非常に分かりやすい。信頼を醸成しようと集まった若者たちの新鮮な知恵にも問いかけて一緒に考えていきたい。

辻構成員）

国家によるサイバー攻撃、サイバー戦争は多くの人、民間企業にとってまだまだ身近に感じられないものであり、特に国外の情勢となると更に遠く感じるだろう。国外の情勢については日本への飛び火について騒がれるが、どのようなことが起きるのかについては可能性を挙げればキリがない上、人々の恐怖を煽りすぎてオオカミ少年になることも避けなければいけない。その点情報の伝え方で気を付けている点はあるか。

JPCERT コーディネーションセンター　小宮山氏）

問題を語るときには解決策をセットで、というのは意識しているが難しい。

辻構成員）

注意喚起をする側からすると起こりうる可能性のある事例をできるだけ挙げたくなるわけだが、そうすると受け手は「結局何をすればいいのか？」となってしまう。その結果、何も対処しないとなることも考えられ、そういう状況を避けるためにある程度の情報のフィルタが必要なのかもしれない。

徳田構成員）

実際ウクライナでは、ネットワークのダメージが大きく、一部の方はスターリンク（米民間企業が運用している衛星コンステレーション）経由でインターネットアクセスをしていると報道されているが、国や自治体が提供している公的サービスは、ほぼ 100%継続運用されているのか。

NTT　松原氏）

ウクライナの通信インフラが、相当規模の破壊または破損を受けているしていると国連の報告書が出ているそうだ。ただ、私は今のところ、国連のウェブサイトで報告書そのものは見つけられていない。
https://kyivindependent.com/news-feed/un-reports-saysukraine-will-need-at-least-1-79-billion-to-restore-telecommunications-sector
NetBlocks などによると、占領地域での通信はクリミア経由に切り替えさせられている。また、公的サービスがどの程度継続しているかは、統計値を見たことがないためなんとも申し上げられない。エネルギー施設、電力

施設へのミサイル攻撃により、ウクライナ国内のデータセンターの電力確保が難しくなっているとの報道もある。
（チャット欄より抜粋はここまで）

◆議題（２）「普及啓発・人材育成に関する取組状況と課題について」について、近畿局より資料 42－１－１、NICT 園田氏より資料 42－2－2 を説明。

◆構成員の意見・コメント
後藤座長）

地域コミュニティの話とナショナルサイバートレーニングセンターの話は、それぞれが地域にリーチをしようとしているところだと思う。各地の総合通信局等とのヒアリング等もされているということだったが、お互いの情報交換を深める取り組みはあるのか。

園田構成員）

私は地域 SECUNITY の取組で挙げられていたインシデント演習のような事業にも実施者として関わっているが、そういった事業を行うことが現場レベルでの情報交換に役に立つと感じている。

中尾構成員）

NICT に籍を置いているところ言いにくいが、例えば総合通信局等と CYDER との役割分担や連携が非常に重要な気がしており、一般的なサイバーセキュリティのケイパビリティを高めていくという NICT の基本的な活動に加えて地域に根差したところとの連携など、具体的にはカフェやスクールといった少し特化したような取組がうまく組み合わされると効果があると感じた。また、今宮さんの発表で文系の方がセキュリティの仕事に関係しているとおっしゃっていたところに非常に共感した。国際標準化やセキュリティに携わる人の中で、文系出身の特に女性が多く活躍されている。社内のセキュリティのルール作りやポリシーの作成などはマネジメントの仕事であり、マネジメント能力のスキルアップは、今お二人にご紹介いただいた以上に重要で強化するファクターになるのと思う。

近畿総合通信局　今宮氏）

NICT の取組と地域の取組の連携について、当局は近畿総合通信局というところで地元の自治体ともやり取りをしており、各地域の自治体で CYDER や NICT の取組の紹介等も各地方公共団体に行うなどの連携はしている。文系人材の点については、実際に我々が連携していた SE の方からの意見で、具体的にどのような啓発をしていくかはこれから考えていきたいが、一つのポイントとして進めていきたい。

篠田構成員）

サイバーセキュリティスクールについて、リーディングサイバーレディース（LCL）という女性向けのコミュニティを立ち上げており、学生のグループと一緒に働いている方がいる。PwC の愛甲氏が女性のキャリアやブランドづくりについて研究されており、その中で、特に女性の文系出身のセキュリティ人材が過半数を占めていることが分かった。それは日本だけではなさそうな予感がしており、理系に特化したセキュリティ人材のターゲティングではなく、もう少し広くすそ野を取るべきと強く思う。また、セキュリティの仕事のイメージを持てる方が良いと学生からも強く言われており、LCL の中で、例えば研究職はどういうことをやってるのかという短いトークを紹介するような場を作ってはどうかという話が出ている。加えて、セキュリティイベントの集客に苦労するのは当然という気もしており、CTF の場合は CTF コミュニティがあり人口も多いためそこに開催の情報を流す

のでよいが、セキュリティゲームなどはゲームコミュニティに訴求すべき部分があるため、提案としてはバンドル型の開催はできないのかということ。自分たちだけでやるのではなく、例えば大阪でやるのであればもっと多くの人を巻き込み、大阪の別のイベントのどこかのコーナーで周知させてもらう等、自分たち単独で集客するのは大変なでありそのような形でやるのが良いと思いました。

徳田構成員）

今宮さんの発表に関し、地域ごとのコミュニティづくりは非常に大変だが価値があると思っている。集客で苦労しているという事例がいくつかあったが、私が手伝いをしている情報処理学会や電子通信学会には全国に各支部があり、そのメーリングリストを使うとアウトリーチとして一般企業や学生などに情報が届く。特に情報処理学会にはジュニア会員があり、小中高生でも無料で学会に参加できる制度になっている。総通局が狙っている年齢層がどれくらいかにもよるが、各学会の持つリストに広報をしてもらえば少し集客がやりやすいかと思い情報共有する。総通局だけで広報を行うのは大変であるため、色々な横展開でうまく集客とコミュニティづくりをしたらどうか。情報処理学会では関西支部の方々が関西の企業とタイアップして連続セミナーのアナウンスなど色々なことをやっていただいており、支部のメーリングリストに情報を投げてもらうだけでもアウトリーチが広がるのではないかと思う。

岡村構成員）

セキュリティ分野における文系人材に関し、先程社内ルール作りの話があったが、これは、この分野に精通した弁護士でも難しく、その一因はセキュリティに関係した遵守すべき法律やコンプライアンスが多すぎるためである。NISC で法令集を作ったものの、遵守しなければならないセキュリティ関係の法体系がどれだけあるかの拾い出しすら途上であり、現在改定作業を進めている。つまり、社内ルールの作成など内部統制的な事柄に関しては、全国的な課題であるため総務省あげてのヘルプをお願いしたい。

辻構成員）

地域 SECUNITY に関し、様々なセキュリティイベントを開催しているが、これらについてどのように効果測定をされているか。また、参加者はイベントで得た知識や技術を所属組織にどのように展開しているかなど情報はあるか。

近畿総合通信局　今宮氏）

効果測定が最も難しいと考えており、例えば企業に参加していただき、サイバーセキュリティを強化することでセキュリティ上の被害や脅威を防げたという効果が見られれば良いが、なかなか数字として見ることができない。今後の一つの方法としては、イベント後のアンケートを活用してセミナーで得た知識をどのように生かすかを問うことで、参加者自身でもその点を認識していただいて今後に生かしていくということは考えられる。効果測定結果を数値化することは難しいというのが現実かと思う。

（3）閉会

以上