# ICT サイバーセキュリティ政策分科会（第 3 回）議事要旨

1. 日 時）令和 6 年 3 月 13 日（火）15：00～17：00

2. 場 所）WEB 開催

3. 出席者）

【構成員】

後藤主査、新井構成員、栗原構成員、小山構成員、篠田構成員、辻構成員、蔦構成員、盛合構成員、吉岡構成員

【オブザーバー】

内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、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、豊嶋大臣官房審議官（国際技術、サイバーセキュリティ担当）、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、田畑サイバーセキュリティ統括官室企画官、牧野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

【発表者】

横浜信一（NTT セキュリティホールディングス株式会社）、小宮山功一朗（一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））、井出博之（独立行政法人国際協力機構（JICA））、林大輔（世界銀行）

4. 配付資料

資料３－１　国際連携に係る取組状況
資料３－２　サイバーセキュリティの国際連携（NTT セキュリティホールディングス）
（一部非公開資料）
資料３－３　サイバーセキュリティ国際連携の紹介（JPCERT/CC）（一部非公開資料）
資料３－４　海外における人材育成に係る取組状況
資料３－５　JICA サイバーセキュリティ協力事業概要（JICA）
資料３－６　サイバーセキュリティ分野における世界銀行の途上国向け能力構築支援（世界銀行）
参考資料１　ICT サイバーセキュリティ政策分科会第 1 回　議事要旨
参考資料２　ICT サイバーセキュリティ政策分科会第 2 回　議事要旨

5. 議事概要

（1）開会

（2）議題

◆議題（１）「国際連携に係る取組状況について」、事務局より資料３－１、NTT セキュリティホールディングス横浜氏より資料３－２、JPCERT/CC　小宮山氏より資料３－３を説明。

◆構成員の意見・コメント

蔦構成員）

海外連携について、JCDC において安全保障も含めた情報共有の取組に関連して、先月末に日本においてもセキュリティクリアランスに関する法案が出され、法案ではクリアランスとして保全すべき情報の具体例としてサイバー対策情報が挙がっていると承知している。米国などの海外のコミュニティに貢献する際に、こちらから情報を提供したり、海外から情報提供を受けたりする場合もあると思うが、その際、クリアランスなどといった観点で障壁になることはあるか差し支えない範囲で教えていただきたい。また、この法案によってそれが改善されるかについてもコメントいただきたい。

NTT セキュリティホールディングス横浜氏）

JCDC について、米国のクリアランスを持った現地の米国人社員 2 名がメンバーとして様々なワーキンググループに参加している。その社員は私にも話せることと話せないことがあり、いわゆるアンクラシファイド（Unclassified）の情報だけ報告を受けている。もし日本のクリアランス法案により、日本のクリアランスシステムが米国のクリアランスシステムとインターオペラブルになれば、壁が無くなり、よりリッチな情報を使えるようになるというメリットはあると思う。法案の詳細を把握していないが、どれだけインターオペラビリティが確保できるかがポイントだと思う。

盛合構成員）

NTT は海外にも研究拠点があり官民での情報共有をされているが、例えば日本の研究者が海外において研究開発を共同で行うといった場合に、半年を過ぎると現地の居住者となってしまい、例えば米国の場合、米国の輸出規制が課せられてしまうため、米国で研究開発された技術を日本に帰国時に持ち帰り、日本の研究者と議論するといった場合には米国の輸出規制を考える必要がある。また、最近は更に有志国以外との接触についても大変厳しいところがある。今後、研究開発や海外との情報交換・共同研究、日本の組織が海外に有する拠点と連携する場合にも同様の問題が生じるかと思う。NTT は他の組織より一歩も二歩も先に進まれているが、この問題に関連して工夫されている点や苦労されている点、この課題が解決されればよいといった課題意識があれば教えていただきたい。

NTT セキュリティホールディングス横浜氏）

例えば 5 年ほど前から NIST にゲストリサーチャーを送り出しているが、NIST は米国民の税金で運営されているためいかに米国に貢献するかを考えて研究するよう言われる。研究者が実際に行ってみて、現地でどういった環境で仕事をするのか一つずつ適合していくしかないものだと思っている。いわゆる同盟国との間ではそういった状況だが、もっと不確実の高い国との協力の場合はマネジメントレベルで気をつけなければいけないと思う。実際に現地に行くリサーチャーが気をつけるのは前提として、リサーチャーではコントロールできないようなところをマネジメント層がどれだけ気をつけてあげるかという 2 層で対応していくことが大切だと思う。

後藤主査）

X.1060 が普及すると、国同士でも企業同士でも、お互いが同様の組織のコンセプトでできていることにより更に深い連携が可能になることは期待できるか。

JPCERT　小宮山）

サイバーセキュリティインシデントレスポンスという言葉について、誰もがそれぞれの解釈で理解するが、特に海外のセキュリティコミュニティだと同じようなイメージを共有していないことが多くある。日本国内でも会社が異なれば言葉が違うことが多々あると思う。そういった場合にサイバーセキュリティフレームワークが理解を統一する手助けとなる。可能であればこのようなフレームワークに則った日本の製品やサービスを採用することで日本のサイバーセキュリティビジネスの支えになれば良いと考えている。

後藤主査）

ビジネスやサービスに繋がるのは今後もまだ時間がかかるのか。

JPCERT　小宮山）

だいぶかかりそうである。

蔦構成員）

いつも大変な調整をされていることが伝わった。FIRST の加盟国について、アフリカの国はそれほど加盟していない現状だが、一方で今後アフリカなどにも X.1060 を普及していくという話があった。現在、アフリカの加盟国数が少ない理由というものはどういったところになるか。

JPCERT　小宮山）

おそらく御想像いただけるように、アフリカは ICT 全般の取組が他の地域と比べて遅れているという点が非常に大きい。また、FIRST のコミュニティも会員資格を維持するのに年会費が日本円で 30 万円程度必要であり、それもアフリカの国々にとってはちょっとした負担になるなどの理由で伸び悩んでいる。この問題について今は亡き山口英先生が最初に取り組み、今でも FIRST にはスグル ヤマグチ フェローシッププログラムがあり、年にアフリカから 2 組織程度、奨学金のようなお金を出して FIRST のコミュニティに入ってもらう活動と続けているが、道半ばである。

小山構成員）

X.1060 は国内では、大規模スポーツイベントの SOC のオペレーションや構築などの参考になったものだと理解している。関わった人の話では、更地から組み上げていく場合にはとても使いやすいフレームワークだったと聞いている。他方、私のように既にサイバーセキュリティフレームワークなど、他のフレームワークでの組織づくりやオペレーションの設計の経験がある人だと、X.1060 の特定の業務が既存のフレームワークで何が該当するかなど、読み替えで混乱することがある。既に構築された組織に対して、X.1060 の考え方を上手く導入している優良事例があれば、御紹介いただきたい。

JPCERT　小宮山）

X.1060 はスクラッチから組織を作る時に役立つものであり、既に組織が出来ている場合は必ずしも CDC を使う必要性はないと思う。特に NIST のサイバーセキュリティフレームワーク 2.0 が非常に良くできているため、NIST のサイバーセキュリティフレームワークを既に使っているところに敢えて X.1060 を推奨するのは良くないと感じている。

小山構成員）

理解した。追加で JPCERT として海外と情報連携している中で、1 対 1 で情報共有する際には貴重な情報を得られる一方で、複数の組織が関与すると 1 対 1 の時ほどの情報が共有できなくなるということを経験されていると思うが、先ほどもセキュリティクリアランスの制度導入後に関する質問があったが、セキュリティクリアランスが日本に導入されることで、他国、特にアメリカとの情報共有はどう変わっていくか、観測で結構なので、小宮山様の御見解を教えていただきたい。

JPCERT　小宮山）

私の経験では海外とのやりとりにおいて、日本にクリアランスシステムがないことで情報が得られないということはそれほどないので、あまり気にしていないが、ファイブ・アイズではないからという理由で会議に招待されない参加させてもらえないといったがかなり多くあると感じている。

◆議題（２）「海外における人材育成に係る取組状況ついて」、事務局より資料 3－4、JICA　井出氏より資料 3－5、世界銀行　林氏より 3－6 を説明。

◆構成員の意見・コメント
吉岡構成員）

幅広い協力事業を推進している中で、サイバーセキュリティ分野、特にニーズの高い技術領域や取組はあるか。国や地域ごとに傾向や違いがあれば、その点も御教示いただきたい。

JICA　井出氏）

特にニーズの高い技術について、国によって異なる点もあるが、どの国も共通してサイバーセキュリティエンジニア向けの基礎教育へのニーズがある。例えば EC-Council の CEH レベルのもののニーズと、市民向けのアウェアネス強化のニーズが共通で出てくる。その他、中進国から先進国に移行している国と、まだ始まったばかりの国とではニーズが異なり、例えばインドネシアのような国の場合、重要インフラの組織がこれからサイバーセキュリティ対策を打たなければいけないこと、そしてやらなければならないことは認識しているが、どのようにマスタープランを作成すればよいのか、先ほどの CDC の話も関わってくると思うが、企業として何をやっていけば良いのかについてコンサルテーションしてほしいといった要望を受ける。また、エンジニアからはどうしても上の人を説得して予算をとることができない状況においてどのように上の人を啓発すれば良いかといった要望が中進国以降の国で出てくる。他方、対策を始めたばかりの国では政府の中枢にもエンジニアがいないため、そういった人材を集中的にトレーニングする要望や法制度分野に関する要望を受ける。外国人のコンサルタントが相手国の法律をつくることはできないが、日本の例を示しその国では何が足りないのかについてトレーニングを依頼されることは多い。

辻構成員）

「海外における人材育成に係る取り組み状況」について、CTF やサイバー対応演習などは様々なところで行われており、参加者の反応として満足度は高い傾向にあると思っているが参加者のアンケートやコメントという観点以外での効果測定などは行っているか。もしあれば教えていただきたい。演習などの効果はすぐには見えづらいものだと思うが、今後参加者を増やしていくために必要な情報だと思う。また、参加された方が得たものをどのように広めている、実践しているかについての情報もあればあわせて教えていただきたい。

JICA　井出氏）

これは CTF やサイバー演習では当然満足度調査を実施しているが JICA がお金を出している事情や受講側の礼儀もあり、どうしても皆「満足した」としか回答しない。プリテストとポストテストを実施しどれくらい能力が向上したか定量的に見る仕組みも導入しており大半のケースで成績が上がっていることが多いが、中にはトレーニングに来る時の前提条件が合っていないためいないためプリテストもポストテストも同じ成績だったという方もいて、いかに適切な人を受け入れていくかが JICA の課題の一つになっている。

世界銀行　林氏）

基本的には JICA からお話があったような認識と同じ。そもそも参加者にとっては、制度面、技術面両面で何が足りないかが分からないことが非常に多いと思うので、そういった差分を埋めていく作業が必要である。

篠田構成員）

AJCCBC の取組に関連して、ENISA が発起人の ICC という国際 CTF 大会があり、世界 60、70 ヵ国と一緒に開催している。地域でチームを組み最終戦に挑む形式だが、Cyber SEA Game の参加者がチームアジアとして参加することはできるのか。現在、日本の SECCON には参加されていると思うが、Cyber SEA Game の参加者が参加するのは日本の大会でないといけないのか。

JICA　古川氏）

可能性はあると思う。現在は日本に行く前提で契約等も既にできてしまっているが、もし他の SECCON に参加できる、CTF の大会に参加できるということであれば、予算をどうやって捻出するかも含めて議論は必要だが、検討することはできるので、少し御相談させていただければと思う。

篠田構成員）

ENISA の方が JICA のカンボジアのプログラムにも一緒に同行されていたようで、イギリスの大学の能力開発のエキスパートの方が AJCCBC プログラムに感激されていた。Cyber SEA Game についてもなぜ ICC に参加できないのかとおっしゃっているぐらいなので、是非前向きに御検討いただきたい。我々も ICC へ送る Team Asia の選抜大会「ACSC」を手弁当でやっているが、なかなか恒久的に継続するのは難しく、先ほどの話にもあったようにミスマッチが見られるのでうまくマッチできると良い。昨年の AJCCBC 大会で優勝したシンガポール国立大学のメンバーはワールドクラスの実力があり、昨年 ICC 参加した Team Asia のメンバーで、能力構築の CTF にはマッチしていなかった。また、CTF づくりについても、これまで東アジアを含めた ASEAN の国と協力して前述したアジア選抜 CTF 大会「ACSC」やアジア 10 ヵ国で共同開催する 1 週間のトレーニング「GCC」をやっているので、トレーニングも含めて一緒にやることも考えられると思う。先日タイでの GCC というグローバルサイバーセキュリティキャンプでも NCSC の AJCCBC 担当の方が来られたり、国連の方に基調講演をいただいたが、我々や各トレーナーにトレーニングのカリキュラムについて協力を求めていましたし、トレーニングのコンテンツはどこも必要としていることを体感した。JICA としてもそういったコミュニティとの協力について前向きに御検討いただければと思う。

新井構成員）

資料３－５の 22 スライド目に長期研修プログラムについて、修正や博士の学位を得る機会を提供されていると

いうことだが、どれくらいまで JICA が費用負担しているのか。学位を取る費用に加えて滞在費やその他も全面的に支援されているのか。先ほども辻構成員からの質問への回答でどういう人を招いて、受け入れていくかが課題だという話があったが、どれくらいの支援があればこういったものに積極的に参加してもらえるのかといった実態をお伺いしたい。

JICA　井出氏）

家族の分は負担していないが、本人の学費と滞在費と渡航費、それ以外は全部 JICA 側が負担している。人選について、これまでの例だと、修士は相手国政府で政策立案に関わっている人、具体的にはデジタル開発庁や通信省といったところの方が来ている。また、博士の学位については今回初めてだが、マスターしか持っていないインドネシア大学の先生の方で、帰国してもサイバーセキュリティを教えるという確証がある方を選んでいる。

後藤主査）

グロービス経営大学院のマスターに４人、また、ドクターの修得については今回九州大学１人のみという状況か。

JICA　井出氏）

ドクターについては他にも希望者がいるが、今マッチングを行っているところ。

後藤主査）

世界銀行からの説明の中にあった、支援対象国が中所得国、最貧国という区分について、国の全体の所得の大小が基準となるのか、国民１人あたりの所得の大小が基準になるのか。

世界銀行　林氏）

DAC（開発援助委員会）で定める基準等に基づき、国の経済のレベルや実際の所得の水準等、様々な要素を組み合わせて判断している。最貧国と呼ばれるのはアフリカや島しょ国など非常に貧しい国が該当する。中所得国は、中南米の国のほとんどや北アフリカなどなので、最貧国に該当するのはそれ以外の経済規模の小さな国と考えていただくのが分かりやすいと思う。

後藤主査）

国によっては政府自体が安定していないなど、国の規模とは別の難しさもあると思うが、その辺りについてお悩みなどはあるか。

世界銀行　林氏）

政治的な安定性については支援を円滑に進める上で、非常に難しいところがあり、JICA も同じような課題を感じていると思う。世界銀行は ODA と同じように国側からの依頼を基に取り組んでいるので、依頼を受けた以上、我々としてはできる限り支援が可能となるよう検討している。ただし、支援を進める段階で、サイバーセキュリティや情報プライバシー等の観点から制度面での対応が必要になる場合がある。特こうした法的整備が円滑に進む国となかなか進みづらい国が非常に極端に分かれるという実態がある。

（3）閉会

以上