サイバーセキュリティタスクフォース（第 37 回）議事要旨

1. 日 時）令和 4 年 4 月 22 日（金）10：00～12：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、鵜飼構成員、宇佐美構成員、岡村構成員、小山構成員、篠田構成員、園田構成員、辻構成員、戸川構成員、徳田構成員、中尾構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバー】

扇慎太郎（内閣サイバーセキュリティセンター）、石巻克基（経済産業省）、鈴木一弘（地方公共団体情報システム機構）

【総務省】

巻口サイバーセキュリティ統括官、山内官房審議官（国際技術、サイバーセキュリティ担当）、梅村サイバーセキュリティ統括官室参事官（総括担当）、高村サイバーセキュリティ統括官室参事官（政策担当）、安藤サイバーセキュリティ統括官室企画官、佐々木サイバーセキュリティ統括官室統括補佐、廣瀬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、須藤住民制度課デジタル基盤推進室課長補佐（代理出席）

【発表者】

窪田歩（KDDI 株式会社 情報セキュリティ本部）

4. 配付資料

資料 37－1　サイバーセキュリティを巡る最近の動向

資料 37－2－1　情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題

資料 37－2－2　5G ネットワークにおけるセキュリティ確保に向けた調査・検討及び 5G セキュリティガイドライン（第 1 版）について（KDDI 株式会社）

資料 37－3　国際連携の現状と課題

参考資料 1　5G セキュリティガイドライン（第 1 版）

参考資料 2　サイバーセキュリティタスクフォース第 36 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「サイバーセキュリティを巡る最近の動向について」について、事務局より資料 37-1 を説明。議題（２）「情報通信ネットワークの安全性・信頼性の確保に係るサイバーセキュリティ対策の現状と課題について」について、事務局より資料 37-2-1、KDDI　窪田氏より資料 37-2-2 を説明。

◆構成員の意見・コメント

①　電気通信事業者におけるサイバーセキュリティ対策の推進

戸川構成員）

5G 特に 5G SA（5G スタンドアローン）は、ソフトウェア化とオープン化が一層進んでおり、攻撃者にとって攻撃しやすい環境になっている。こうした中、5G や Beyond 5G のセキュリティ確保に向けた調査・実証の継続は重要かつ有用である。（資料 37－2－2 では）5G ネットワークセキュリティの重要性をまとめていただいたが、様々なレイヤで広範なユーザが 5G ネットワークを使用することを踏まえ、ポイントを絞った上で、どういったセキュリティ対策をしていくべきかを分かりやすく伝えることも非常に重要。

小山構成員）

前々回のタスクフォースでも紹介したとおり、昨年の秋から 2016 年の Mirai に匹敵する規模の DDoS 攻撃が起き、通信ネットワークが混雑するような状況が断続的に見られる。現状、日本のインターネットに影響は見られないが、国内の攻撃先に一斉に攻撃されたときには日本のインターネットに影響しかねないことを考えると、指をくわえて見ているわけにはいかない。今まで通信の秘密の考え方というのは、自社の通信設備に影響が出てから正当業務行為や緊急避難に該当するかどうか検討することが中心だったが、影響が出る前に通信の秘密との関係でどういった対策が行えるかというところについても是非検討いただきたい。

中尾構成員）

小山構成員の指摘は重要。米国でもランサムウェアに関して攻撃前の対策に関する議論が進むなど、世界的にも注目されている話題である。総務省の施策としてサイバー攻撃に対する観測、分析及び対応は既にかなり実施してきたところ、今後、取組むべき施策をきれいに洗い出していく必要があるが、その中で、具体的な攻撃の前にいかにそれを把握し、周知し、対策できるのか、考えていく必要があるのではないか。

梅村サイバーセキュリティ統括官室参事官）

戸川構成員の 5G ネットワークセキュリティに関する指摘について、調査結果のアウトプット方法等を今後検討していければと思う。また、小山構成員の電気通信事業者における攻撃対策と通信の秘密との関係に関する指摘については、諸般の課題を踏まえつつ、引き続き検討していきたい。

若江構成員）

（電気通信事業法の改正案について、）電気通信事業者におけるセキュリティ対策を強化する方向性はもちろん良いと思うが、前提として、電気通信事業者に本来含まれるべき事業者が十分に取り込まれていないのではないかという問題がある。（電気通信事業ガバナンス検討会の中で出ていた）クラウド事業者がコアな通信機能を提供する場合、一定の条件で報告義務を課すという案の法制化が見送られたことについては、日本の通信の安全性の確保という面から考えて非常に問題が大きく残念なことだと思う。見送りになった理由と、今後どのような観点で再検討する予定なのか教えていただきたい。

廣瀬サイバーセキュリティ統括官室参事官補佐）

若江構成員からの質問については、事業者等への聞き取りによれば実際にクラウド事業者がコアな通信機能を提

供するサービスが進められている状況ではないということであったため、今後のサービス実装動向等も見つつ、さらに必要となった段階でしっかり考えていこうという結論になったと聞いている。今後の検討課題として（電気通信事業ガバナンス検討会の）報告書にも記載しており、今後 IP ネットワーク設備委員会等でも議論はありうると認識している。

若江構成員）※チャット

先ほどは言葉足らずだったかもしれないが、クラウド事業者がコアな通信機能を提供するケースが日本でまだ全く始まっていないという説明はいささか疑問。日本の通信の安全性確保という面から考えると、実質的に通信サービスを提供している事業者を電気通信事業者として適切に規制できないことは問題だと感じている。日本の電気通信事業者のセキュリティへの取り組みはすばらしいと思うが、伝統的な「電気通信事業者」のセキュリティのレベルを上げるだけでは漏れてしまう部分が大きくなってきていると思う。早急な見直しをお願いしたい。

林構成員）※チャット

若江構成員の意見に賛同する。

後藤座長）

私も同じ問題意識を持っているが、この点については、電気通信事業ガバナンス検討会の方で議論して進めるのが良いかと思う。

② IoT セキュリティの確保

辻構成員）

NOTICE の http・https への拡大が、思っていたより早く対応されていることは素晴らしい。こうした新たな取組みを広報し、ある種注目を集めるようなこともした方がよいのではないか。また、バナー情報等を活用して脆弱性が発見された機器の特徴を共有したり、チェックするポートの範囲を、手軽な侵入経路として活用されがちな RDP（で用いられる TCP／UDP の 3389 番ポート）まで拡大するのも一案であり、検討いただきたい。

徳田構成員）

NOTICE に現場で従事する職員と意見交換したところを共有したい。まず、NOTICE 業務は増加する方向性である一方、NICT の人的リソースは非常に限られている。NOTICE 関係企業からの出向者数も NOTICE 開始時に比して減りつつあるが、透明性の高い産官学連携の枠組みにおいて健全に NOTICE 業務が継続、拡張、改善されることが望ましいと考えるところ、NOTICE 参加企業におかれては、改めて産学官の枠組み強化をお願いさせていただきたい。また、ドローン等の、私たちの生活に密着したより高度で新しい IoT 機器が出てきているところ、総務省、経産省、IPA、NICT 等で策定した IoT セキュリティガイドラインから一歩踏み込んで、IoT 機器のラベリング制度を検討する時期に来ているのではないか。

鵜飼構成員）

NOTICE や NICTER はリアルタイム情報収集等を可能とした成功事例だと認識している。ただ、やはりランサムウェアや Emotet といったマルウェア被害が足下では一番深刻であることを考えると、NOTICE や NICTER と同じ枠組みか分からないが、今後、実効性のある対策を普及させつつ、マルウェアに関するデータを広く集める必要があると思う。CYNEX ではデータを収集して解析する技術的な仕組みは準備できており、どう拡張する

かを検討する段階だが、マルウェアについては、そもそも広くデータを集める方法から検討が必要。データが海外に集約されることは、安全保障上の観点でも良くない。

中尾構成員）

IoT 機器の販売時にその機器がきちんとしたセキュリティの機能を持っているかを確認するところについては、認証基準となるガイドラインの策定が、ISO/IEC 及び ITU-T で進められており、ほぼ完成している（中尾構成員はエディタを担務）。また、既存の IoT 機器の脆弱性等に対する対応としての NOTICE や NICTER については、徳田構成員がおっしゃったような方向の検討に加え、ライフタイムが切れている機器や脆弱性への対処が難しい機器に対しての技術、性能の検証を検討する必要がある。この件に関連し、ICT-ISAC で法人向けの IoT 機器の悪用によるサイバー攻撃防止ページを作成しているので共有する（https://www.ict-isac.jp/iot_security/）。法人向けだが、IoT 機器が抱えるリスクについての啓蒙に非常に良い内容になっており、横浜国立大学が運営するマルウェア感染・脆弱性診断サービスの「am I infected?」もリンクされている。

小山構成員）

NOTICE の取組みから分かったのは、IoT 機器は設置した瞬間から劣化していくということ。脆弱になった機器の取扱いに係る規定も端末設備等規則に追加いただき、脆弱化した機器の接続に対して何らかの法的な制限をかけられるようにできないか。また、脆弱化した機器を産官学でハニーポットとして活用し、飛んでくる攻撃や検体を解析して、技適の仕組みを活用しながら IoT のセキュリティ対策エコシステムを上手く回していくことができないかと考えている。

吉岡構成員）

IoT 機器の脆弱性調査・注意喚起について、「am I infected?」の運用から、必ずしも専門的知識が十分でない一般ユーザに対しては、状況や問題意識を正しくはっきり伝え、手厚いサポートとインタラクティブな情報提供を行うことで、注意喚起の浸透や対策の実効性を向上できるのではないかと考える。また、国内の主要 Wi-Fi ルータ等のメーカと頻繁に意見交換を行っているが、メーカもユーザがどのように機器を使っているのかは把握できておらず、ユーザにリーチできないことで手詰まりがあるという旨をよく聞いている。機器ベンダとの連携も重要ではないか。

高村サイバーセキュリティ統括官室参事官）

NOTICE は、端的に言うと拡大したいと思っているが、徳田構成員がおっしゃったように、金銭コストを誰が負うかはさておいたとしても、人的リソースの観点で中々厳しい。仕事を単に増やすのではなく、どこから人を増やすのか、どの仕事に重きを置くのかを考えなければいけない。是非とも、こちらにいらっしゃる方だけではなく、産業界・学術界全体の御協力を得ながらやっていくことができれば良いと思う。また、NOTICE は不正アクセス禁止法で本来禁止されていることまでやってなお対処しなければならないという整理で実施している取組のため、何でも NOTICE の営みに含めてしまうと、他のセクションとの情報共有が難しくなるという問題がある。せっかく CYNEX を昨年度に立ち上げているので、こちらと NOTICE の役割分担についても考えながらやらせていただければ嬉しい。吉岡構成員が指摘されていた機器ベンダからユーザへのリーチの部分についても、是非とも色々な方から御知見を賜ればと思っているので、引き続きご指導いただきたい。

③　その他の取組（クラウドサービスのサイバーセキュリティ確保）

辻構成員）

「クラウドサービス利用・提供における適切な設定のためのガイドライン（仮称）」については、「こういう設定にしたつもり」になっていないか、外から確認する手順を内容として含められていると良いのではないかと思う。

藤本構成員）

クラウドサービスの設定ミスについて、学生の研究などを通してによれば、ユーザ企業においてセキュリティを担当している部署とクラウドサービスを利用している部署が分かれているケースがあり、両者の連携が上手く取れている企業もあれば、必ずしもそうではない企業もあるというような状況があるのではないかと考えている。ついては、「クラウドサービス利用・提供における適切な設定のためのガイドライン（仮称）」を、普段セキュリティを担当していない部署の方々等へいかにして届けるのかというところまで含めて考えていただけると良い。

宇佐美構成員）

我々の中でも、IT 部署が絡まない形で独自に SaaS のサービスを使いたい、特に新規事業等々で手軽に使えるものを使いたいというようなケースが増えている。そうした際に特に悩ましいのは、海外事業者のサービスを用いるケース。通常行っている事業者側へのチェックシート送付によるセキュリティ対策の確認は難しく、ホームページの公開情報から判断せざるをえないこともある。事業者が提示している公表情報をどう判断すれば良いかという枠組みのようなものがあると良い。

岡村構成員）

クラウドサービスにおける問題として、国内ベンダに依頼したつもりが海外ベンダへの再委託になっていることが多いという点が挙げられる。また、インシデント発生時におけるベンダとユーザ企業間における裁判管轄、準拠法の問題というのも実務的に大きな論点となる。海外ベンダの場合、自らに有利なように、海外の法律を引用した規定を契約書に掲載していて、裁判で争うまでもなくコストの観点からユーザ側が負けを認めざるを得ないというような状況もあるので、（各種ガイドライン等の策定にあたっては）契約面についても考慮をお願いしたい。

◆議題 3「国際連携の現状と課題について」について、事務局より資料 37-3 を説明。

◆構成員の意見・コメント

篠田構成員）

二国間・多国間連携における日本の功績は大きく、今後、シンガポールや韓国等の国に移っていく可能性は否定しないが、現状アジアのリーダー的役割の需要に応えていると認識している。（自らの取組として、）セキュリティ・キャンプの中に国際連携グループを作り、その中で ASEAN、東アジア地域の 8 ヶ国と共に若手向けのトレーニングを提供しているが、将来政府や企業で国際連携のために活躍できるような強い人材が育っており、好評を得ている。また、ENISA が行っていた EU 圏の CTF 競技 ECSC を ENISA が世界レベルに展開した ICC（International Cybersecurity Challenge）について、アジア 8 ヵ国と協力してアジア大会 ACSC（Asia Cyber Security Challenge）を催しアジア選抜チームを作って ICC に送り出すのだが、こちらは私 1 人と数名の学生ボランティアが主に運営している状況。今後も毎年開催される予定であり、政府と協力できると良いと思っている。

中尾構成員）

篠田構成員が日本の代表として取組まれている内容は国際連携において非常に効果が出ていると思う。また、二国間・多国間の国際的な官民連携においては、相手国が複数の場合は難しいが、開始段階で具体的に連携しよう

とする動機の方向性やそのレベルを日本ときちんと合わせることが非常に重要。国内企業のサイバーセキュリティ製品・ソリューションの展開については、特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)で取組んでいるが、ASEAN 諸国においては重要インフラにアメリカ等の製品が既にきっちり入っているなど、牙城を崩しにくい状況であり、SIer のような土台に入り込んでいく必要がある。ISAC 間連携については、ICT-ISAC が国内外 ISAC 連携-WG を作り積極的に実施しているので、ぜひ総務省とさらに連携して進めていければと思う。

徳田構成員）

NICT として、ASEAN IVO という形で ASEAN 諸国の様々な地域課題を ICT によって課題解決していく研究プログラムに投資している。日本のリーダーシップという観点も重要だが、ステアリングコミッティの中に各国から代表 2 組織を入れ、各国の参加意識を高めることで、地域課題の自主的な解決につながるよう工夫した。また、篠田構成員の、ASEAN 諸国とセキュリティ・キャンプ等をインターナショナルにやっていく提案に賛成する。国際的な枠組みの中でトレーニングされるという機会が少ないことが日本の若手人材の弱点の 1 つであり、リモートで英語でコミュニケーションしながら人的ネットワークを広げ、インターナショナルに協議できるというカルチャーを作っていくのが重要なため、なるべくフラットな協力関係ができる場を提供するのが大事だと思う。

篠田構成員）※チャット

中尾構成員の意見に賛同。また、徳田構成員の意見もおっしゃる通りで、千葉工業大学の嘱託研究員として、大学連携も視野に入れて活動している。

園田構成員）※チャット

篠田構成員も手弁当、Cyber SEA Game の作問に関わってきた SECCON も手弁当、といった人的リソースの弱さは何とかしていきたい。

篠田構成員）※チャット

SECCONは過去に 1 回で4,000名強の参加者を集めており、（自らが関わる）ACSCも 2 週間の周知で1,000名超の参加者を集めたことを考えると、協業により更なる拡大が望める。これらのコミュニティを官民連携に加えられると、ポテンシャルのある人材を良い方向に繋げられると思う。

（3）閉会

以上