サイバーセキュリティタスクフォース（第 22 回）議事要旨

1. 日 時：令和 2 年 3 月 18 日（水）16:00～17:30

2. 場 所：中央合同庁舎 2 号館 8 階　第 1 特別会議室

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、齋藤構成員、園田構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、吉岡構成員、若江構成員

【オブザーバ】

尾崎洸(経済産業省)、神谷征彦(内閣官房 IT 総合戦略室)、鮫島清豪(内閣サイバーセキュリティセンター)、浦船利幸(地方公共団体情報システム機構)、三宅優(KDDI 総合研究所)

【総務省】

竹内サイバーセキュリティ統括官、二宮審議官(国際技術、サイバーセキュリティ担当)、岡崎サイバーセキュリティ・情報化審議官、大森サイバーセキュリティ統括官室参事官(総括担当)、赤阪サイバーセキュリティ統括官室参事官(政策担当)、近藤サイバーセキュリティ統括官室参事官(国際担当)、森下宇宙通信政策課長、中村電気通信技術システム課長、安達地域情報政策室課長補佐、相川サイバーセキュリティ統括官室参事官補佐、佐々木サイバーセキュリティ統括官室統括補佐

4. 配布資料

資料 22－1　IoT・5G セキュリティ総合対策プログレスレポート 2019（案）（事務局、構成員限り）

資料 21－2　5G 以降の時代に向けたセキュリティ標準化（KDDI 総合研究所）

参考資料 1　サイバーセキュリティタスクフォース第 21 回　議事要旨

5. 議事概要

(1) 開会

(2) 議事

◆　議事（１）IoT・5G セキュリティ総合対策の進捗状況と今後の取組について、事務局より、「資料 22－1　IoT・5G セキュリティ総合対策プログレスレポート 2019（案）」を説明(省略)

◆　構成員の意見・コメント

若江構成員)

17 ページの公衆無線 LAN のセキュリティ対策や、38 ページのサイバーコロッセオについて、東京 2020 大会に向けて、ホテル等の事業者や未受講の自治体における取組を進めていく計画が記載されているが、新型コロナウイルスの対応でな

かなか実施できないような状況になってきている。この部分がどのような状況になっているか、またもし実施できない場合に何か代替策について考えているのかについて教えてほしい。

赤阪サイバーセキュリティ統括官室参事官(政策担当))

例えば、CYDER については、東京 2020 大会前にまだ受講していない自治体向けに集中的に実施できる期間を設けたいと考えている。現在、都道府県と調整しながら、実施する地域をどこにするのか相談しているところである。当初の計画では、出来れば４月から実施したいと考えていたが、新型コロナウイルスの影響もあるので、今のところ５月以降に開始できないかといったところを模索している。状況を見ながら実施時期や実施できるかどうかを柔軟に判断していきたいと考えている。未受講の自治体に参加を促していくために、今までは個別に NICT や各地方の総合通信局を通じて働きかけを行っていたが、都道府県との協力体制が大分出来てきている。都道府県にグリップしてもらうことでまだ未受講の自治体に計画的に受講してもらうといった連携が進んできている。仮に実施時期が後ろになっても、未受講の自治体にしっかりと参加してもらう体制が出来てきていると考えている。

また、来年度には、リモート環境で試行的に演習を実施することを計画している。離島等の自治体は県庁所在地まで出向くことが難しいため、リモート環境で演習を受けられるような仕組みを作り、東京 2020 大会前というのは時間的に難しいが、来年度中には実施していきたいと考えている。

齋藤構成員)

17 ページの公衆無線 LAN のセキュリティ対策について、「IoT・5G セキュリティ総合対策プログレスレポート 2019（案）」は、「IoT・5G セキュリティ総合対策」をベースに作成されていると考えられるが、緊急提言の際には、公衆無線 LAN のところで詐称されたアクセスポイントに関する記述があったが、それが触れられていない。別紙の資料にはそのようなことが記載されているため、17 ページの公衆無線 LAN のセキュリティ対策の中で触れる必要がないか検討してほしい。今後の課題として、IoT 機器のチェックを行っているということも踏まえて認識しておいた方がよいと考えている。

中尾構成員)

全体的な話になるが、総務省としては、国内の IoT や 5G、クラウド等の事象に関する活動を行い、国内のセキュリティを高めていくための主な施策についてまとめているという理解をしている。例えば、IoT の場合は、既に存在する IoT 機器や IoT システムと、これから出てくる商用化された IoT 機器や IoT システムを分けて考えると、機器認定や端末認定は後者の脆弱なところを抑え込むものであり、前者については、NOTICE を含めて、国内の脆弱なところを抑え込むものである。非常に良いと思うが、東京 2020 大会に向けて、いろいろな攻撃が国内の脆弱なポイントから来るのではなく、海外の脆弱なポイントから来ることが想定される。ここ２～３日、NICT の NICTER では、不明な発信元で非常に広域なところから DDoS 攻撃のような SYN-ACK パケットを山のように観測しており、NICTER の画面が一面、該パケットの観測情報で全体が黄色く（SYN-ACK 観測の表示色）なるほどである。それがどのような攻撃元から来ているかは分からないが、基本的には国外からのパケットであり、米国と欧州からが多い状態である。日本で実施している NOTICE などのいろいろな活動をこれから海外にも展開を行い、既存に動作中の IoT 機器の脆弱なところを国際的な連携で抑え込むという活動が重要になってくるのではないかと考えている。「IoT・5G セキュリティ総合対策プログレスレポート 2019（案）」というよりも、今後の施策の方向性としてぜひ検討してほしい。

近藤サイバーセキュリティ統括官室参事官(国際担当))

ご指摘いただいたとおり、国内の NOTICE 等の活動については、国際的なサイバー協議の場や ICT 政策対話の場、あるいは個別の二国間協議の場で紹介させていただくとともに、NICTER について海外にも多々センサーが設置されているが、そういったものの拡大についても海外への働きかけを行っている。直近では、一昨年、イスラエルと協力覚書を締結しており、NICTER のセンサーについても設置できるように調整を行っているところである。国際連携は非常に重要であると認識しており、今後もしっかりと進めていきたいと考えている。

岡村構成員)

情報開示分科会の主査を務めさせていただいたが、これに関する内容が 51 ページに記載されている。どちらかというと未然にどういう体制で守りを固めているのかという部分について情報開示の促進として実施してきた。他方、最近では例えば、電機会社の事例に代表されるように、事後的にどのように発表するのかという部分についてもいずれ問題にしなければいけないということで以前から議論がなされてきたが、そろそろ具体化していくべき時期に来ていると感じている。具体的には強制するという類のものではないので、従前の重大なインシデント事案で企業がどのように発表してきたのかということについて事例などを振り返り調査することによって、その結果を他の企業に参考にしてもらうような形にすることも重要なことではないかと考えている。

企業が発表したものを、ステークホルダーに対して、どのように伝えていくかということについて、実例を踏まえて、マスメディアや格付け機関、証券会社、マーケットというところにどのように波及していくのか、どういう流れになっているか、それらについてもそろそろまとめるべき時期に来ていると考えている。そういう方向性についても検討をしてほしい。

後藤座長)

「IoT・5G セキュリティ総合対策プログレスレポート 2019（案）」というよりも、次のステップとしての提言として捉えることができる。

鵜飼構成員)

9 ページの 5G のセキュリティ対策について、今年度は 5G ネットワークにおけるソフトウェアの脆弱性調査を実施して、対策メニューを深堀りしていくことが記載されている。脆弱性調査について、5G が主流になってくると何か致命的な問題があったときに、かなり大きな影響を与える可能性があるが、この種の調査は、どれぐらい深く実施するか、どの程度の規模感で実施するかで、調査できる内容や深度が結構大きく変わってしまうという問題がある。１週間で出来る調査もあれば、１年ぐらいかかるような調査もある。そういう意味合いでは、規模感が重要なポイントになる。4G や LTE のチップに対して、いろいろな脆弱性やバックドアが昨年度報告されている。5G をきちんと普及させていく中で、安全性を担保していくにあたり、ある程度の規模感で解析を実施していかなければ問題が出てこないのではないかと考えている。脆弱性の発見手法については、ある程度自動化されていたり、手法としてまとめられていたりするが、加えてこの先にバックドアの調査を実施していくことについても考えると、バックドアは仕込むのは簡単であるが、発見するのは格段に難しくなり、より時間と工数が必要になる。対応していくにあたっては、それなりの規模感で実施していく必要がある。

後藤座長)

重要な課題であるが、次のステップにどのように反映していくかということについて考えていきたいと思う。

名和構成員)

9 ページや資料 12 に記載されているホワイトハッカーによる脆弱性調査について、ホワイトハッカーの定義が公的文書に見当たらないと感じている。ホワイトハッカーはおそらく人間であり、脆弱性調査を行った結果、弱さをよく知っているということになるが、この人間がずっと裏切らないという保証があるのか。セキュリティクリアランスへの配慮がどのようになっているか。その部分が気になった。今後の検討の見通しはどのようになっているか。発言した根拠は、イスラエルや米国で、ホワイトハッカーであった人間が裏切って、ブラックハットハッカーになるケースが結構出てきている。確か逮捕もされている。このような状況が日本に来るのは数年後になるのではないかと予想される。他国の状況をみて、日本としては、どのように対応するのかについて気になった。

また、ホワイトハッカーのレベルも気になった。第三者が認めたホワイトハッカーであっても、第三者が異なるとレベルが乱高下するので、何をもってレベルを測っているのかというところが気になった。

大森サイバーセキュリティ統括官室参事官(総括担当))

ご指摘いただいたとおり、ホワイトハッカーについては定義が曖昧なところがある。現段階ではこれから取り組むことになっているが、ご指摘の内容を踏まえながら、検討していきたいと考えている。ホワイトハッカーのレベルについても、いろいろなレベルがあることを承知している。

名和構成員)

個人の信頼性の確認という観点で、原子力分野では法改正を行っている。いろいろなアクターについて考えてみると、ホワイトハッカーが一番危険な人間ではないかと考えている。日本だけの国籍を持っている、万が一裏切っても何らか強く出れるような配慮がなされているということが必要なのではないかという気がする。

藤本構成員)

40 ページから記載されている地域のセキュリティ人材育成について、地域経済活性化の観点からも、今後どのように育成していくのかが重要な課題である。リーダーを育成しなければいけない、人材のシェアリングを進めなければいけない、という２つの観点から試みが行われているところであるが、どのような知識やバックグラウンドがある方々をリーダーとしてまず育成するのかといった、もう少し戦略的な取組計画について、「IoT・5G セキュリティ総合対策プログレスレポート 2019（案）」の中に入れられるとよい。41 ページに、監査やリスクマネジメント経験のあるシニア人材や、女性人材について触れられているので、そういった方々をリーダーとして育成していくという方法も可能ではないかと考えている。もう少し具体的なアプローチに展開してもらいたい。

後藤座長)

今後の取組の方に反映していきたい。

徳田構成員)

30 ページに、衛星通信におけるセキュリティ技術の研究開発が記載されており、NICT のチームの取組に関連する部分がある。国際連携と関連するが、安全な衛星通信のニーズが世界的に広がっている。ドイツの DLR やフランスと話をすると、当分野においては日本の研究開発が進んでおり、良い技術を持っているので、日本と一緒にぜひ国際連携を実施したいと提案してきている。日本の強みのある技術分野で国際連携を実施するのは非常に良いと考えている。スマートシティの取組は EU-Japan (日欧国際共同研究)の枠組みで進んでいるが、衛星通信の取組も同じ枠組みで進められると良い機会になるのではないかと考えている。

8 ページの 5G のセキュリティ対策について、ソフトウェア脆弱性への対応が記載されているが、ハードウェア脆弱性への対応も同様に重要であるが、機能と機器が分離されてきて、ソフトウェアによって 5G コアなどいろいろな部分が提供されるようになっている。先ずはソフトウェアのオープン化や透明性が担保されていないと、ソースコードが容易に解析できないので、脆弱性のチェックが困難である。ソフトウェア化が着々と進んでいくという前提のうえで、一般の方々や企業、研究所の方々が使える検証ツールが日本ではまだまだ足りていない。自動運転のソフトウェアについても同じニーズがある。例えば、企業では自動運転のソフトウェアを OTA（Over-the air）でアップデートして、過負荷が起きないかどうかや、動的にソフトウェアの構成を変更したときに変な挙動をするか、しないかをアップデートする前にチェックできるような検証ツールを米国では数年前から業界が作っている。国内ではオープンな形でステークホルダーが使えるそのような検証ツール群がまだまだ足りないので、ぜひ SCOPE の枠組みでもよいので、ソフトウェアの専門家を幅広く集めて作ってもらえるとよい。

後藤座長)

2 つ目の話は、今後の展開として、9 ページの今後の取組に記載されているオープンソースソフトウェア等の解析の部分の内容を膨らませていくべきであるという話になる。１つ目の話は、衛星通信の話と国際連携の話が掛け算で今後いろいろと出てくるという話になる。

吉岡構成員)

全体として対策が進んでいるということは素晴らしいと思う。NOTICE や広域スキャンの技術についての研究開発が進んでいて、広域で IoT 機器のセキュリティの状態を把握する試みがある。一方で CCDS が機器の認証を進めていて、そのような機器が出てきている。また、DLPA においても、推奨の Wi-Fi ルーターが出てきているが、これらの機器が NOTICE や広域スキャンで認識できるのかどうかが気になった。認証されたような機器がどれほどネットワークで使われているかということを認識できるようになっているかという点が気になった。２つの施策の情報がどれぐらい連携されているかという意味合いになる。つまりそのようなことが分かってくると国内で認証されている機器がどれぐらい使われていて、不明な機器がどれぐらいあるかということを把握しようとすると、せっかく認証まで実施しているので、ネットワークプロファイルがどのようになっているのかということがある程度分かるはずである。そういう情報を広域スキャンのデータベースにしっかりと登録しておくべきだと考えている。脆弱性情報の共有という話も出たが、それぞれの施策でかなり具体的な情報がいろいろと出てきている。連携すると更に価値が生まれる状況になるのではないかと考えている。

NOTICE や NICTER で注意喚起が行われているが、現在は ISP を介してエンドユーザに注意喚起を行う仕組みになっている。この注意喚起を更に徹底するという意味合いで、別のチャネルで注意喚起の情報をエンドユーザに提供することも検討するとよいのではないかと考えている。エンドユーザまで注意喚起が本当に届くかという点については、海外の事例を

見ていても、なかなか厳しいと感じている。一例として、一般の国民に身近なチャネルとして、スマートフォンアプリのようなものもあると思う。専用アプリを使って周知する方法もあり得る。また、既に日本国内で相当幅広く使われているSNSのアプリもある。そのような既存のチャネルを上手く使うとそのような情報提供が実は効果的に幅広くエンドユーザーに届く可能性があるのではないかと考えている。そのようなことも検討すると、この施策が更に有効なものになるかもしれないと思う。

後藤座長)

今後の取組のところで追記していくとよいと思う。

小山構成員)

NTTコミュニケーションズとFFRIが共同出資を行い、セキュリティ人材育成を目的とした会社を設立している。「IoT・5Gセキュリティ総合対策プログレスレポート2019（案）」の中に記載されているセキュリティ人材育成については、セキュリティを志す人をどのように伸ばすかという観点を考えているのに対して、セキュリティ人材を社内・社外で募集しても人材が枯渇している中では人材が集まらない前提で考えるべきである。そこで会社を設立して、若手の社員を無理矢理連れてきて、仕事を通じてセキュリティをしっかりと勉強してもらった。仕事に触れて、セキュリティに興味を持つことによって、自発的に更に勉強し成長するようになった。この取り組みを育成プログラムとして導入したところ、半年ぐらいで、文系出身の社員でも疑似マルウェアを開発するぐらいのレベルに、もう１～２ヵ月経つとワナクライやオリンピックデストロイヤーの解析が技術として身につくレベルにまで育成できることが分かった。並行して道徳的な教育や倫理的な教育もしっかりと実施した。セキュリティを志す若者がいないという前提で、どのようにして人材育成のレールに乗せるかというその部分の仕組みから作る必要があるのではないか。そのような考えで取り組んでいるところである。

後藤座長)

次のステップとして大事なコメントを頂戴した。

名和構成員)

ホワイトハッカーという言葉であるが、米国の白人が住む地域では特に問題がないが、差別意識の強い国や地域やでは差別的な用語と見られることがある。英語に訳すときには、エシカルハッカーにした方がよい。他国の一部の公文書でもホワイトハッカーという言葉を使うことはNGになっているので、気を付けられた方がよいと思う。

後藤座長)

構成員の皆様から貴重な意見を頂いた。「IoT・5Gセキュリティ総合対策プログレスレポート2019（案）」に一部加筆する部分もあるが、次のステップに向けた大きな議論のスタートについての意見が多かったと思う。今後、頂いた意見をもとに加筆し、事務局の方で修正案をまとめてもらいたい。修正案はメール等で構成員の皆様に回覧させていただき、然るべきタイミングで公表するという形で進めさせていただきたいと思う。4月以降の公表になると思う。そのようなステップで進めさせていただいてよいか。

全構成員)

（異議なし）。

後藤座長)

そのようなステップで進めさせていただきたいと思う。

◆ 議事（２）国際標準化の現状について、三宅優氏（KDDI 総合研究所）より、「資料 22－2　5G 以降の時代に向けたセキュリティ標準化」を説明(省略)

◆ **構成員の意見・コメント**

後藤座長)

ITU-T 等のセキュリティ標準化活動と、中身を作る ORAN Alliance のようなコンソーシアム活動があるが、それらの関係性はどのようになっているか。例えば、セキュリティ標準化団体が公表している検討内容が、コンソーシアム活動の中にしっかりと入り込むような形になっているかなど、そのような状況はどのようになっているか。

三宅優氏（KDDI 総合研究所）)

残念ながらセキュリティについては後回しにされるところがある。コアで動く部分を上手く作って、その後から、セキュリティをどうするかを考えるという流れが多いのではないかと感じている。ORAN Alliance についても、後からいろいろと相談を受けることがあって、セキュリティが問題無いかを検討しながら、どう作っていくか、対策をどうするかを考えているような状況である。

名和構成員)

脅威の想定がいろいろと記載されていたが、宇宙についてはそれが見当たらない。PTP と呼ばれる高精度時刻同期のプロトコルの影響評価について検討されているか。GPS やみちびきに対するスプーフィング攻撃が発生した場合やタイムスプーフィング攻撃が発生した場合には、システム間が不同期になる可能性がある。このような脅威に対する対応について検討されているか。

三宅優氏（KDDI 総合研究所）)

今のところは大きな議論になっていない。モバイルに関しては、GSMA が取り仕切って、脆弱性情報を集めて外部に公表し、それをもとに各社が対応するという流れになっている。ご指摘いただいた内容は声としては挙がっているが、ガイドラインを作成したり、共通の対策を採ったりするという段階にはない。各機器を作っているベンダーが個別に対応しているような状況である。

岡村構成員)

15 ページに法制度等の整備という記載があるが、どのような法制度のことを具体的に考えているか。

三宅優氏（KDDI 総合研究所）)

セキュリティ対策を実施してほしいといったときに事業者側もなかなか動いてくれない。ある程度、ここまで実施してほしいという基準を政府として設定して、事業者にそれに従ってもらうことが必要ではないか、セキュリティレベルを一定に保つための何らかの仕組みが必要ではないかと考えている。強制力が働くものがあれば、事業者のセキュリティ担当者も従いやすくなるのではないかと考えている。それがすべての事業者であるかどうかまでは分からない。

岡村構成員)

今の話の事業者は電気通信事業者のことを指すという理解でよいか。

三宅優氏（KDDI 総合研究所）)

そのとおりである。

小山構成員)

5G の構成は確かに複雑で、対処すべきところが多い。全体像についての理解が難しいというのはそのとおりである。一方で５G システム全体を制御系システムとして俯瞰した場合には、他分野の制御系システムと同じ課題は残るのではないかと思う。今までの制御系システムは既存システムに対して対策の手を打てないという課題があったが、新しく作る制御系システムに対しては、何か新しい試みが出来るのではないかと考えている。そのあたりについて何か動きがあれば教えてほしい。

三宅優氏（KDDI 総合研究所）)

今の意見に賛成であるが、本当に上手くいくかどうかは分からない。実際にはその部分の議論は進んでいない。セキュリティ関係者は考えているかもしれないが、システムを作る側の関係者がどこまで対処しようと考えているかがよく分からない。

小山構成員)

最先端分野のセキュリティ対策に注目が集まるのは仕方がないが、古いアーキテクチャの影響を受けないように問題提起をしていきましょう。

相川サイバーセキュリティ統括官室参事官補佐)

サイバーセキュリティタスクフォースの次回以降の会合については、開催の仕方を含めて、いろいろな事情を勘案しながら検討しているところである。決定次第、構成員の皆様に御連絡を差し上げる。具体的な議事と開催場所についても、後

日事務局から連絡させていただく。構成員の方々には個別の相談をさせていただくこともあるため、引き続き協力をお願いしたい。

以上