サイバーセキュリティタスクフォース（第 31 回）議事要旨

1. 日 時）令和 3 年 5 月 13 日（木）13：00～15：00

2. 場 所）オンライン

3. 出席者）

【構成員】

後藤座長、安達構成員、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、戸川構成員、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

【オブザーバー】

扇慎太郎（内閣サイバーセキュリティセンター）、篠崎美津子（内閣官房情報通信技術（IT）総合戦略室）、尾崎洸（経済産業省）

【発表者】

窪田歩（KDDI 株式会社）

【総務省】

田原サイバーセキュリティ統括官、藤野審議官（国際技術、サイバーセキュリティ担当）、中溝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）、海野サイバーセキュリティ統括官室参事官（国際担当）、恩賀電気通信技術システム課安全・信頼性対策室長、佐々木サイバーセキュリティ統括官室統括補佐、横澤田サイバーセキュリティ統括官室参事官補佐

4. 配付資料

資料 31-1　5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）の策定について

資料 31-2　電気通信事業ガバナンス検討会について

資料 31-3　「IoT・5G セキュリティ総合対策 2021（仮称）」の方向性（案）について

参考資料 1　（案）公表版：5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）

参考資料 2　サイバーセキュリティタスクフォース第 30 回 議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（1）「5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）」について、KDDI 窪田様より「資料 31-1　5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）の策定について」を説明、議題（2）「電気通信事業ガバナンス検討会」について、事務局より「資料 31-

2　電気通信事業ガバナンス検討会について」を説明、議題（３）「「IoT・5G セキュリティ総合対策 2021（仮称）」の方向性」について、事務局より「資料 31-3　「IoT・5G セキュリティ総合対策 2021（仮称）」の方向性（案）について」を説明。

◆構成員の意見・コメント

戸川構成員）

資料 31-1 及び資料 31-3 に関連する 5G ネットワーク構築におけるセキュリティに関する対策等の留意点について、リファレンスモデルがきちんと MEC 等を含めて定義され、詳細な対策・留意点がまとめられており、非常に有意義なものだと思う。今後、5G・ポスト 5G・6G に向けて、こういったリファレンスモデルをベースとした具体的なセキュリティ対策というものは非常に重要になる。資料 31-1 の 2 ページ目、冒頭の MEC や仮想化の進展による汎用ハードウェア、オープンソース利用に伴うセキュリティ課題というものが非常に重要であるというような指摘があるが、国際的なサプライチェーンの中でも非常に重要な課題となっており、今後も継続していくと思う。これについても、資料 31-3 の（1）③の 5G の本格的な普及に向けたセキュリティ対策の強化というところでサプライチェーンのセキュリティについてしっかりと触れられており、対策に整合性が取れていると考えている。今後もどういった状況で進んでいくのかについては観察し続けていくことが重要。

林構成員）

LINE 社の問題について、行政指導を迅速にしたことに加えて、検討会で議論を進めるというやり方が大変素早いため感心している。現実に問題が発生して、対策を考えなくてはいけないケーススタディの教材のような意味でこの問題は大変意義がある。ただ、基本的には電気通信ビジネスは民間企業主体でやっているので、経営の自主性というのは尊重しなければいけない。重要インフラに準ずる基幹インフラになっているようなサービス、あるいは提供者については公益的な見地から何らかの規律を求めるというのもあって然るべきだと思うが、現行法でこれらが必ずしも全部解決できるような仕組みになっているとは限らない。そうすると次の立法として何が必要かというのが議論にもなるので、大変発展性を持っているケースではないか。このグループの検討が迅速に進むことを期待している。

中尾構成員）

資料 31-3 の 3 ページ目に IoT・5G の総合対策の方向性についてまとめていただいている。デジタル改革・DX 推進を前提としてのサイバーセキュリティの確保というのを大きな傘にして、冒頭で背景や主要な課題を記載するという構成は非常に良い。具体的には、情報通信のサービス・ネットワークの個別分野の具体的な施策と横断的な施策の二つに分かれているが、個々の事案についても基本的にこれまで色々議論をさせていただいた内容と合致しているように思うので、分類学としては非常に分かりやすい。可能であれば今後、総合対策の中で（1）情報通信サービス・ネットワークの個別分野の具体的な施策で、通信事業者における安全・信頼性の高いネットワークの確保のためのセキュリティ対策の推進とあった時に、その直後に総務省として考えている方針や意向を書いた方が良いのではないか。いわゆる（1）～（4）についての方針の下で色々な具体的な施策をまとめていくというのが分かりやすい。全体的の構成なり分類学は良いと思うが、対策がいきなり出てきても読者に響きにくいので、それに対する方針を冒頭にまとめて、その後個別の対策の推進を記述してはどうか。

中溝サイバーセキュリティ統括官室参事官）

今現在の記載ぶりとしても、資料 31-3 の 4 ページ目では具体的施策（1）の考え方を書いており、これを踏まえて①②③の個別の施策に進んでいく。また、具体的（2）についても 8 ページ目に書いてある。今の指摘を踏ま

えて、これをさらに膨らますという方向で良いと感じている。

若江構成員）

資料 31-3 の 6 ページ目に記載されているフロー情報分析の箇所について、フロー情報分析の必要性というのは理解しており、検討を進めていくことが必要な問題だと思っているが、この資料に記載のある「通信の秘密への配慮」は、具体的にはどういう配慮なのかを教えて欲しい。C&C サーバの検知ということだと実際に大量通信が発生して非常事態になる前、つまり緊急避難や正当防衛の法理が使えない、その前の段階に、正当業務行為として日常的なチェックをするということだと思うが、その理解でいいのか。その場合、日常的なチェックをどういうレベルでやろうとしているのか、それが通信の秘密との関係でどういうことになるのか。その基準がはっきりしない状態のまま実証を始めるというのはどうなのかと考える。本資料だと「5G を狙った攻撃は依然として多く、利用が拡大することが予想される中、対策が十分ではないという恐れ」と記載されている。しかし、リスクが高まることは抽象的には分かるが、抽象的なリスクの記載にとどまっており、その状態で日常的な通信を分析するというのも、どうなのか。何かの歯止めや基準が必要だと思う。具体的なところについて、もし総務省のどこかで検討しているのであれば、それを教えていただきたい。また、サプライチェーンリスクについての検討というのは非常に重要だと思っているので、電気通信事業ガバナンス検討会にはとても期待しているが、サプライチェーンリスクを考える上では、電気通信事業法でカバーできる事業者だけだと、問題に対処するにはなかなか難しいということについてどのように今後考えていくのか。例えば電気通信事業者でなくても、通信サービスをユーザに提供している事業者は多様化しており、スマホのアプリでもメッセージ機能を持っているようなところであれば、電気通信事業法でカバーできるかもしれないが、事業法の対象外のゲームアプリでも多くの情報を中国や海外等の外部にも送信しているような状態になっている。まずは、総務省として現在の設備を中心に見ている電気通信事業法の規制対象の範囲というものを見直していく必要があるのではないかと思うので、今後はそういうことも含めて検討していただきたい。

中溝サイバーセキュリティ統括官室参事官）

ご指摘のとおり、通信の秘密に十分に配慮した上で、サイバー攻撃の脅威への対策をしっかりとれるようにするといったバランスは大事なので、いかにバランスを確保するかという観点で、これから検討を深めていく必要がある。これまでは正当業務行為としてどこまで可能なのかということを整理する時に、行為の目的の正当性、行為の必要性、手段の正当性といったものについて、一つひとつ丁寧に整理をし、明確に解釈を示してきた。ここで制度的な観点から対策の検討が必要か、重要ではないかというのも、従来やってきたことと同じように適切に解釈を整理した上で、何ができるかというのを検討していく。当然どういった情報であればできるのかといったことも含めて整理をしていく必要がある。そういった形で通信の秘密にもしっかり配慮して対策を講じていきたい。

鵜飼構成員）

今回の LINE の話について、最終的に落としどころがどうなるのかによって、出し方が大分変わってくるかと思う。今回の件は様々な背景があると思うが、安全保障という軸で極めて政治的な判断もあると思っており、総務省のスタンスとして、最終的にどのような落としどころを考えているのか。他にも海外からデータアクセスできるようなサービス、しかも国名を示していないサービスがいくつかある中で、こういったサービスに対して積極的に何か総務省としてやっていくべきではないかという声があるのか、あるのであれば、するべきかどうかといった方向性について教えていただきたい。

中溝サイバーセキュリティ統括官室参事官）

電気通信事業ガバナンス検討会は、昨日第 1 回が開催されたばかりなので、現時点で落としどころや方向性が示せる段階ではない。また、当検討会の会議自身は機微情報を取り扱うので非公開という形でやっているが、資料で公開できるものは公開し、議事概要を公表する。昨日の議論の検討課題案について、この場で全部お話することはできないが、例えば、昨今の色々な事案を踏まえた検討課題として、委託先や連携先等への対策をどうするのかというのが一点目。それから色々なシステムのソフトウェア化やサービスを提供するにあたっての多様な者の関与、いわゆるマルチステークホルダー化の進展を踏まえて、内部の設定ミスあるいは連係ミスによる情報漏洩が増えているので、それについてどういう対応をしていくかというのが二点目。そのサイバー攻撃の複雑化・多様化・悪質化を踏まえ、外部からの攻撃に対してどう対応していくかというのが三点目。そういったものをどう確保するかというガバナンスも含めての対策の確保の在り方というのが四点目となっており、そういったところに大きく検討課題を整理して出している。当検討会において様々な構成員から意見をいただいたので、今の時点で方向性は見えていないが、優先順位を付けつつ、やれるところは早めに方向性を示し、中長期的課題として議論すべきことは引き続き議論していく必要があると思っている。総点検ということで各電気通信事業者に対して対策の現状のアンケート調査をやっているため、その結果を当検討会の場にフィードバックし、現状どのような運用が行われているのかをしっかり把握した上で、今の制度が十分なものなのかどうか、足りないとすれば何が足りないのかといったことを洗い出した上で、方策を検討していくというようなことを考えている。

岡村構成員）

民事法上は委託先の中国・韓国企業は履行補助者に該当するので、それらの委託先の行為について、委託元である LINE がユーザに対する責任を負うという法律構造になっている。そのあたりと通信の秘密について、もう少し踏み込んだ議論をすべきレベルの問題であり、別の検討会を作るなどしてもっと深掘りしていただきたい。

安達構成員）

資料 31-3 の 3 ページ目、その他の具体的施策の中で、②に放送分野のセキュリティ対策というのがあるが、放送分野のセキュリティとなるとかなり広範囲に渡るが、どのような範囲とレベルでの対策を想定されているか。

横澤田サイバーセキュリティ統括官室参事官補佐）

昨年策定した総合対策 2020 の中で、放送分野における対策として放送分野も重要インフラ分野の一つとして指定をしているので、その関係で対策を記載している。総務省の取組としては放送法関連の規則の中で放送設備についてサイバーセキュリティ対策の実施を求めるような改定を行ってきたと今の総合対策 2020 には記載しているので、その現行の記載に関連して、今後アップデートできるようなものがあれば、今回の改定の中で記載していきたい。

小山構成員）

被害者が情報発信した段階で加害者のように扱われることが無いよう関係者で被害者を守れる社会的なコンセンサスを作っていただきたいと申し上げたが、その趣旨を採用していただき感謝している。具体的な成果に繋げるためには事例研究が必要。例えば地震における都市防災や災害対策、危機管理等は色々なケーススタディをしており、研究分野にもなっている。例えば、昨年は日本だけではなく、世界中で重要インフラ企業を狙ったサイバー攻撃が発生している。これら事例研究を行って、その端緒となった脆弱性の発生から収束までを考えた場合に、例えば昨年の 12 月の SolarWinds の例、あるいは今年の 1 月にゼロデイとして起きた Microsoft の Exchange サーバの例を研究し、攻撃に至るまでのどの段階で誰がどう動けば一番被害が少なく収束が早かったのかというようなことも見えてくる。そのプロセスの中で被害企業の情報発信はどうあるべきかベストプラクティスの積み上げなしに、被害企業に情報発信や共有を求めることはややまだ乱暴だと思う。Exchange の例でいうと 1 月に

Microsoft のゼロデイ攻撃が起きていることを理解しながらもパッチがないので 3 月まで発表しなかった。その結果、ものすごい数の被害が発生して、FBI はリモートから攻撃者が埋め込んでいる webshell を削除するというようなことで令状をもらってアクションを起こした。そこまでしないと収まらない、被害者が情報発信しただけでは収まらないような事例も実際あるため、そういったことまで幅広に踏まえたケーススタディと被害極小化の研究をセットで行わないと社会的なコンセンサスを得ることは難しいのではないか。

後藤座長）

FBI が刈り取りに動いたという件について、小山構成員からもう少し詳しくご説明は可能か。

小山構成員）

Microsoft の Exchange サーバに外から侵入し、不正プログラムが埋め込まれ、後からでも攻撃者が自由に悪用できる状況に何万台というコンピューターが陥った。それを重く見た FBI が、裁判所の許可を得て不正プログラムである webshell をリモートから削除する権限を与えられ、その権限を行使して削除した、といった事例だったと思う。ただ、この対応はやって良いことと悪いことの線引きもなされており、さらに踏み込んでパッチを当てるといったことはやっていないが、ギリギリのところで悪影響が出る webshell だけを削除したといった事案だったかと思う。

中溝サイバーセキュリティ統括官室参事官）

ご指摘の点は前回 JPCERT/CC からの報告内容、議論いただいたことをベースに書かせていただいたが、JPCERT/CC がやった研究成果を生かす形で外向きにガイダンスを作るようなことを検討するとともに、今ご指摘いただいたような社外的なコンセンサスづくりの観点から今の事例研究も並行して検討していきたい。

藤本構成員）

資料 31-3 の 3 ページ目、全般的なところについて、全体を通してユーザ企業の目線で話をお伺いしていた。5G ではユースケースによって確保しなければいけないセキュリティの考え方がそれぞれ違う。さらに IoT を含む DX 推進においてもサービス内容によって見なければいけないセキュリティの側面というのは大きく違う。このように考えると、やはりユーザ企業の中で、考えなければいけないセキュリティ確保というのは今後も引き続き非常に重要になってくると思う。この資料を拝見していて、電気通信事業者が安全になったものを提供してくれると読み、安心してしまうというのは良くないと感じた。本取り組みは素晴らしい取組であることは言うまでもないが、やはりユーザ企業の方でもセキュリティに関する必要なリソースや人材育成を含めて、主体的に取り組んでいただきたいと思う。人材育成の現状を見ると、ベンダー企業や電気通信事業者など、提供者側の方にセキュリティ人材が偏っている。もっとユーザ企業側にセキュリティの知見や人材というものが育ってこないと、DX の推進も 5G の利活用も進まないのではと思っているため、どこかにユーザ企業向けにメッセージングしていただくことは可能か。ユーザ企業向けに 5G 利活用される方、DX 推進される方も主体的にセキュリティに取り組んでくださいというようなメッセージを含めると良いのではないか。

吉岡構成員）

NOTICE で構築した広域スキャンのシステムや技術というのはこの施策の元々の目的である IoT 機器の脆弱の状態を把握したり、それによって DDoS 攻撃への対策を行うということだと思っているが、本来はもっと広い問題に対して様々な情報を得るための有効な技術だと思っている。つまり、グローバルからリーチできるあらゆるシステムや機器が侵入や攻撃に対してどれくらい準備ができているかを調査する機能を持ちうると思っている。

IoT セキュリティの枠組みの中で動いているので問題はないと思うが、実はテレワークの観点でも VPN のサーバやルータの状況を調べれば、テレワークのセキュリティの役に立つし、クラウドの状況を調べれば、クラウドセキュリティの観点でも役に立つし、インフラや 5G など色々なところで出てきたキーワードに対して、NOTICE のような方法で調べた情報が実はすごく有効なのではと思っている。攻撃する方もわざわざ IoT だけ狙うことはないはずで、どこにあってもリーチできて攻撃出来れば悪用するし、重要な情報があれば、使ったりランサムにかけたりするし、そういう観点では対策を行う方もあまり始めから目的を絞ってやるというよりも、そこで得られるポテンシャルをしっかり活用できるように目的や手法を再整理する等によって得られた有益なインテリジェンスを活用できると良いのではないか。当然 NOTICE の場合はログイン試行する等、一歩踏み込んだこともやることで得られる情報も価値があると思うが、そこまでやらなくても、かなり良い情報が集まっているのではと思っているので、上手く整理をすることで色々な施策に有効活用できると思った。

高村サイバーセキュリティ統括官室参事官）

NOTICE で実施した広域スキャンを応用について、無限に活用できるというのは吉岡構成員のおっしゃるとおりと思っている。その一方で、こちらからスキャンをかけ、アクティブに調べるということが良いのかという議論が昔からある。つまり、政府が日本国内のものを全部なめるということに対してアレルギー的な抵抗感を感じる方がたくさんいる時に、本当にアクティブスキャンをかけなくてはいけないような状況なのか、拒否感を上回る利益や拒否感を乗り越えてでもやらなくてはいけないと説得できるだけの状況やネットワークの危険性という意味での雰囲気が高まっている状況でないとなかなか難しい。今回は不正アクセス禁止法という法制があるということで明確に時限立法という形をとったわけでだが、そこで違法性が無いとしてもアカウンタブルな状況を作らなければいけないと思っている。実際 NICT がメインで回している NICTER というのも結局のところ、パッシブなものだし、警察庁が設置されているようなセンサー類もメインで見ているのはリフレクションで、警察庁の IP アドレスになりすまして何かアクセスをしたものに対するレスポンスをメインで測っていたりと、みな基本的に口は開けているが、こちらからパケットは投げないという形でやっているものがメインかと思うので、法律や大きな仕立てをなしにアクティブなセンシングするというのは難しいところがある。もちろん、この場においてそれでも今やるべきネットワーク環境だというお話があるのであれば、是非ともそれを前提に検討させていただきたい。

後藤座長）

いずれにしろ、NOTICE のノウハウは整理しておくと良い。

名和構成員）

資料 31-3 の 15 ページの横断的施策、サイバーセキュリティ情報に関する産学官での連携・共有等の促進について、産学官連携の加速について賛同する。少し気になっているのは、官官の連携の加速というのはどのようになっているのか。全く違うところで警察庁・経産省との横の連携の加速というのは存在しているのか。

中溝サイバーセキュリティ統括官室参事官）

産学官連携は具体的にいうと資料 31-3 の 16 ページ目に記載されている CYNEX を念頭においているが、質問の趣旨はこの CYNEX についての他の政府機関との連携に関するという理解でよいか。

名和構成員）

CYNEX において官が研究機関からいただいた情報を総務省が利活用すると思うが、それを警察、経産省、防衛省、内閣官房にどのように生かされるのかというところの連携と理解してしていただければと思う。

高村サイバーセキュリティ統括官室参事官）

CYNEX については、土台になるのは今 NICT が実際にやっている STARDUST となるが、STARDUST では当活動に興味がある他省庁もアクティビティに参加している。ただし、STARDUST の場合には個別の組織がそれぞれに参加しているという状況であり、STARDUST を使っているユーザ間の連携はないという仕組みになっている。CYNEX はそれを一歩進めて、今度はそういったものを使う人たちの中で一緒にやるというアクティビティを作っていきたいと思っている。そこに官が入ってくるのかという話になるが、そこはギブアンドテイクであり、きちんと自分たちの情報も提供してくれる組織であれば当然歓迎するが、情報を獲得するだけで提供する気はないという人たちはこのコミュニティには入ることはできないと思っている。加えて、その情報のオーナーが誰なのかという部分があるので、そこはコミュニティとしての総意をもって政府に共有しようというのがあれば NISC を通じて広く共有する等もあると思うが、いずれにせよセキュリティに関しての情報は誰が権限をもっている情報かという問題があり、基本的にはみんなで共有するという前提を考えているので、まずは情報を欲しがるだけの人は入れる気はないと理解いただきたい。

名和構成員）

資料 31-3 の 15 ページの 4 ポツ目のところについて、メッセージと具体的な施策についての繋がりというか必要十分条件が見えなかったため質問した。産学官連携の官というのは総務省のみと理解した。

高村サイバーセキュリティ統括官室参事官）

ここは総務省のみではなく、今実際に STARDUST を利用している官庁には当然声はかけていく。ただし、他の省庁が入るかどうかということは最終的には他の省庁の意思になるので、そこについては現時点で我々として皆様にお約束できる状況にない。

中尾構成員）

資料 31－3 の 7 ページの 5G の本格的な普及に向けたセキュリティ対策の強化のところについて、具体的に様々な取組をサプライチェーンの対策、技術検証、情報共有、色々なオープン化、多様化、5G の導入促進、国際連携と非常に多岐にわたって記載されている。具体的に多岐にわたったような考え方を整理していかないといけないというのはもちろん同意するところだが、進め方としてかなり色々なオプションがありそうな気がしている。この中でも考慮されていると思うが、各国でどのくらい 5G が推進されているのか、市場としてどのくらい使われていて、アプリケーション等どのように考えられているのか、NIST や欧州等の各国が規格として何かサイバーセキュリティに関係する動きがあるのか、日本は先ほど KDDI の窪田氏から説明があったような流れを受けて国際的な連携をすることでサイバーセキュリティの対策のリファレンスをつくり、それに基づいて国内だけではなく国際も含めた様々な 5G の運用者、構築者、ユーザに対して同等のセキュリティの対策の実装や運用を施していこうという方向性もあるかと思うが、その辺りは 7 ページに含まれているか。もし入っていないのであれば、加えていただくとありがたい。また、ユーザの視点に関して、まだ具体的な 5G のユースケースに基づいたセキュリティ検証はできていない。多岐にわたるユースケースが考えられているが、それはこれから検討する内容であり、その辺りも今後の取組の中に入っていくと理解している。もう一つは資料 31-3 の 12 ページ目の IoT について、IoT 推進コンソーシアムで総務省、経産産業省が中心となって策定したセキュリティガイドラインがある。それに基づいて、NICT もかなり関与したところだが、国際規格 ISO（ISO/IEC 27400）の規格を作っており、それがとうとう DIS（Draft International Standard）となった。この国際規格では IoT の実際のサービスの提供者、開発事業者、ユーザというステークホルダーに対して具体的なセキュリティとプライバシーのコントロールを提供しているので、この国際規格を上手く活用していくというのを視野に入れて 12 ページのところは

膨らませていただけるとありがたい。

中溝サイバーセキュリティ統括官室参事官）

5G のご指摘の点は、IoT・5G セキュリティ総合対策の案においては基本的には踏まえた記述になっていると認識している。例えば、資料 31-3 の 7 ページ目の 4）でオープン化・ベンダー化、いわゆる O-RAN 規格の推進は国際的にも進めていくということで、国際的な場でも色々議論しており、6）の国際連携でも、様々な各国の市場動向や政策動向や、O-RAN の規格等の話も含めて連携をして普及に取り組んでいくといったことを、当然セキュリティにも配慮しつつ関係国と議論、意見交換しているという状況なので、基本的にご指摘の内容は踏まえられていると認識している。もし不十分ということであれば、また検討したい。また、IoT のセキュリティガイドラインの国際規格化の取組についても、当国際規格を踏まえて今の記述を膨らませていけたらと考えている。

後藤座長）

5G のセキュリティについて、インフラ設備に関するサプライチェーンは大体カバーされているが、ユーザ側のセキュリティの取組、例えば最初に窪田氏のお話にあった MEC のあたりはアプリケーションと密接に絡んできている。ユーザとの線引きも幅広くあり得るため、5G における事業者とユーザとの間のセキュリティの役割分担や共同の取組に関しては今回どうか。

中溝サイバーセキュリティ統括官室参事官）

先ほど中尾構成員から指摘があったとおり利用がこれからのため、実際の利用の真意を踏まえた取組というのはこれからという部分が現実としてはあるが、例えば、3）の ICT-ISAC において 5G セキュリティ推進グループが活動推進中というのがあるが、ローカル 5G を提供していく方々に対してもこの場で情報共有していくことで、しっかりとセキュリティ対策を講じた上で、取り組んでいくことを進めるといった場がある。まだ具体的な個別のサービスのユーザまで含めて網羅的にはやれていない部分もあるが、当然そういったユーザの視点も念頭に置きながら進めていくことに引き続ききちんと目を向けていく必要があると理解している。

後藤座長）

今後スマートシティ等も 5G の展開場所になるので、そういう観点でも期待したい。

岡村構成員）

JPCERT/CC も関与した Emotet のケースは、捜査当局が裁判所の令状を取って犯人自体のアジトを押さえたというケースであり、いわゆる被害ユーザ企業に対して法的強制力によって情報共有を行わせたという事案ではない。被害を受けたユーザ企業自体が漏洩したことを理由に世間から袋叩きにあうというような状態のもとでは、ケーススタディのもとになるような素材も含めて、被害ユーザ企業に情報共有を求めることは極めて難しい状態。やはり何らかの仕組みを考えていく必要があるのではないか。それから二点目の人材不足という点は、私も非常に深刻な状態であると考えている。中小企業の場合はさらに深刻な状況なので、まずは当たり前の管理措置ができているかどうかといった基本的な点について社員教育の機会の場を作るということも重要なのではないか。

篠田構成員）

セキュリティ企業や政府がユーザ企業に向けてガイドラインの整備など様々な取組を進めているが、提案された施策を受け入れて実施したいが、特に中小企業などのユーザ企業の中に、例えば社内システム担当者等、実施する人材がいないから困っているというのが、最近すごく見て取れて、ガイドラインや施策の提案もありがたいが、

困っているのはそこではないというような声も聞こえてくる。ギャップが存在する。高度なセキュリティ人材の開発も大切だが、現場のニーズは、もう少し基本的なことを担える人材の供給が大切なように見える。このギャップを埋めるためにどうすべきか有志で話し合っている。情報共有に関しても、インセンティブが働かないところでどうするのか、私も妙案がないが、他国だと法律等で強制力を持たせている。その辺りについてはガイドラインで促進すると書いてあったので、強制力がそこに入るのかと期待しつつ、あとは被害者を責めない文化づくりが重要だと思う。

名和構成員）

インシデント対応支援を日頃から行っているが、言葉を選ばずに言うと、助けてくれるところがない、助けてくれるところはお金がかかって仕方ないというのをいつも聞いているので、公的機関からの公助というところを拡大する、あるいはもっと加速する必要があるのではないか。その観点では、現在の公助の取組は現場とのギャップが激しすぎて、上手く当てはまるところが少ない、あるいは無いところもあると現場の方で感じている。

園田構成員）

被害の事例を共有することあるいは公開することに関する抵抗感というのも炎上や評判を毀損するというところで、かなり抵抗感として大きい部分があると思う。それを避けるために専門家がしっかりと冷静な分析をして、セットで出すような形での情報共有をするというようなことを考えていくと、少しは炎上を避けられるのと考えた。

中尾構成員）

資料 31-3 の 14 ページ目のスマートシティについて、5G というのを考えた時に、例えば車に 5G 関係のエージェントのセンサーを置き、それを近くの MEC で色々と計算処理をして、安全な運航のためのアラートをあげるという車のアプリケーションや遠隔医療等、スマートシティはそういうものを全部含んでいる大きなアプリケーションとなっているので、5G の今後の活用としては、セキュリティのガイドラインとバインドするように 5G をどう上手く活用していくかというのも考慮した方が良いと思った。それに加えてスマートシティのガイドラインは基本的にスマートシティの構築側や運用側、またはスマートシティのユーザで活用するものだと思うが、セキュリティという視点からすると、一般的によくあるスマートシティの中で、セキュリティの基盤・インフラをきちんと作り、様々なサービスアプリから API を叩いてセキュアな基盤を使っていく、その基盤が 5G の環境で動いていくといったような構図を書くと、ひょっとしたら 14 ページに書いているスマートシティの内容と 5G のユーザやユースケース的な話と上手く結合するのではないかという気がする。可能であれば、その辺も加筆していただきたい。

後藤座長）

今の件は構成を色々組み替えると良くなると思う。ご意見も出尽くしたようなので、意見交換を終了する。

（3）閉会

以上