サイバーセキュリティタスクフォース（第 29 回）議事要旨

1. 日 時）令和 3 年 3 月 9 日（火）10：00～12：00

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、戸川構成員、徳田構成員、中尾構成員、林構成員、藤本構成員、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）、穂積直樹（地方公共団体情報システム機構）

【発表者】

佐々木勇人（一般社団法人 JPCERT コーディネーションセンター）

【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）、箕浦サイバーセキュリティ・情報化審議官、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、高田消費者行政第二課企画官、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、安達地域情報政策室課長補佐（代理出席）

4. 配付資料

資料 29－１　スマートシティセキュリティガイドライン改定の方向性について
資料 29－２　電気通信事業者のネットワークの安全・信頼性の確保に向けた取組について
資料 29－３　サイバー攻撃被害情報の共有と公表のあり方について
資料 29－４　サイバーセキュリティ分野における国際連携について【関係者限り】
参考資料１　マルウェアに感染している機器の利用者に対する注意喚起について
参考資料２　サイバーセキュリティタスクフォース第 28 回　議事要旨

5. 議事概要

（1）開会

（2）説明

◆議題（１）「スマートシティセキュリティガイドライン改定の方向性」について、事務局より「資料 29-1　スマートシティセキュリティガイドライン改定の方向性について」を説明、議題（２）「電気通信事業者のネットワ

ークの安全・信頼性の確保に向けた取組」について、事務局より「資料 29- 2　電気通信事業者のネットワークの安全・信頼性の確保に向けた取組について」を説明、議題（３）「サイバー攻撃被害情報の共有と公表のあり方」について、JPCERT/CC 佐々木様より「資料 29-3　サイバー攻撃被害情報の共有と公表のあり方について」を説明。

◆構成員の意見・コメント

中尾構成員）

スマートシティのセキュリティのガイドラインの改定ということで、方向性は非常に良いと思うが、今後、ガイドラインをどういう形で進めていき、誰のために発信するかというのを、もう少しクリアにした方が良い。また、スマートシティは色々な街や地方自治体などの環境によって、大分構成が変わってくるので、リスク分析などを行った上で、かなりセキュリティに対する要求が変わってくるはず。当ガイドラインではそれを一般化していると思うが、その辺の議論はガイドラインの中に含まれているか。また、スマートシティは、サプライチェーンやサイバー・フィジカル・セキュリティ対策フレームワーク、IoT、5G など、色々なことをベースにした１つの非常に有効なアプリケーションなので、関連する外部の活動とのリンケージ（ガイドラインからの参照等）というのも明確にしていただいた方が良い。

藤本構成員）

スマートシティのガイドラインにあるマルチステークホルダについて、一般論としてマルチステークホルダのガバナンスは難しいと考える。そういう意味で、こういったガイドラインが出てくるのは非常に有用だと思う。監査について一点質問がある。スマートシティのガバナンスでは対応のルールを決めたり、色々体制を作ったりするなど、計画を立てて実施するという流れになるかと思うが、それが本当にできているのかを確認する監査を組み合わせることが重要。ガイドラインの中で、監査に関する記述はどのようになっているか。

若江構成員）

マルチステークホルダの定義に、市民が入っていないように見受けられる。そもそもスマートシティリファレンスアーキテクチャの定義で市民が入っていないのもどうかと考える。サービス提供事業者に向けたガイドラインだということは理解しているが、誰のためのスマートシティかという視点が抜け落ちてしまわないか不安を感じる。特にセキュリティの場合、情報漏洩が発生すれば被害を受けるのは市民であり、インシデントの被害者は関与しないというのはどうなのか。セキュリティガイドラインの定義として、また考え直すというようなことはありうるか。

中溝サイバーセキュリティ統括官室参事官）

中尾構成員の１点目、スマートシティセキュリティガイドラインの今後の取り扱いについて、もう少しクリアにすべきではないかというご指摘をいただいた。私も今後のことはまだ使い方が色々ありうると思っており、これしかないということは思っていない。ただ少なくとも、作ったものを政府の様々なスマートシティの取組の中にインプットしていき、スマートシティの構築や運用にあたって、セキュリティをしっかり加味した形で構築できるようにしていくという、国内での安全安心なスマートシティの実現に貢献するという意味でインプットしていくことが一つとして考えられる。それから海外の様々な機関にもこれを提供し、国際的にもセキュリティが確保されたスマートシティの実現に貢献していきたい。例えば、普段のメール等でのやり取りや二国間協議、あるいは多国間の枠組みといった場で、日本発のセキュリティガイドラインを紹介していき、普及を進めていくことも

考えていきたい。それに加えて、さらにこうすべきではないかという点があれば、ご意見をいただきたい。2 点目の質問の、それぞれのスマートシティにおいて、構成等が様々なものとなっているのではないかということだが、まったくその通りだと思っている。当然、各スマートシティによってシステムの作り方もバラバラ、あるいは関係主体の関係性もバラバラということかと思うので、一般化して 1 つに言い切るのは難しいことは当然承知している。本ガイドラインの中でもそういった様々なケースに応じて、柔軟にこのガイドラインの記述を活用して、それぞれのシステムに合った安全・信頼性の確保のあり方を検討すべき、というような趣旨を色々な所に盛り込んでいる。3 点目として、例えばサイバー・フィジカル・セキュリティ対策フレームワークや、IoT セキュリティ等々とのリンケージがあるのではないか、そこを明確にすべきではないかというようなご指摘だったかと思うが、昨年の 10 月に第 1.0 版の公表時に本タスクフォース会合で紹介した際にも少し触れたが、このスマートシティセキュリティガイドラインの対策要件を作るにあたっては、IoT 推進コンソーシアムで作った IoT セキュリティガイドラインや経済産業省のサイバー・フィジカル・セキュリティ対策フレームワーク、NIST の SP800-53 や 171 などのドキュメントに記載されているものを融合し、織り交ぜて対策要件を作ったという経緯があり、基本的には整合性を取っていると認識している。その点はガイドラインの中でもしっかり明記していきたい。次に監査に関するコメントだが、監査という言葉が具体的にガイドラインの中に書かれていたか、今ただちに確認しきれていないが、このガイドラインの中で所々、例えば第三者認証などの客観的な評価が必要であること、マルチステークホルダなので、色々契約先・委託先に連携する時には、委託先がちゃんと客観的な評価を受けていることを確認することであること、定期的なリスクのアセスメント、脆弱性の診断が必要といったような記述を色々な所に盛り込んでいる。監査という言葉があるかどうかはともかく、第三者の客観的な評価を促すということは、色々な所に盛り込んでいると認識している。それから最後、マルチステークホルダの中に市民が入っていないのではないかという指摘だが、こちらの資料の 4 ページ目で、関係主体について記載している。先ほど、ガイドラインのスコープの所で、事業者が実施するセキュリティ対策と記載しているが、これは裏を返すとユーザが実施するセキュリティ対策については記載していない。スマートシティサービスを提供する事業者側が、こういった対策を講じるべきであるということを記載し、それを通じてオープンデータやユーザの個人データなど、様々なデータを守りましょう、という趣旨のガイドラインのため、市民が入っていない。ただ、当然市民のデータを守るという視点は入っていることはご理解いただきたい。

戸川構成員）

スマートシティセキュリティガイドラインについて、改定の方向性は非常に妥当なものだと考える。多くのマルチステークホルダが関与しているという特徴を全面に出すというような形での構成となっていると思う。章構成等を含めて割と大胆な改定で、良い方向性だと思っているが、改定前後で上手く整合性が取れている、言ってることが少なくとも一貫しているということに注意を払う必要がある。そこを今一度、ご確認いただきたい。それから実際にスマートシティのセキュリティガイドラインを活用する方々が、改定によって何か混乱が生じてしまうと元も子もないので、この部分がこういったような整合性がある、ここは対応している、という点が上手く見えると良い。

小山構成員）

ガイドラインのスコープの中の細かい点について、データの取扱いを含むという中で、オープンデータのほか個人情報等のデータも取り扱うとあるが、個人情報等という言葉が、ガイドライン全体にどういう影響を及ぼすのかという点について、やや心配をしている。個人情報を軽視するという考えは全くないが、こういったスマートシティにおいては、オープンデータの活用というものが、データ駆動社会という言葉も出てきているように、極めて重要なポイントになってくると思う。どちらかというと、まず活用することを念頭にしっかり検討を進めて

いくということが重要で、個人情報という言葉が入るとガイドライン全体に萎縮効果を及ぼしかねないと思う。ヨーロッパなどでは、欧州のデータ戦略やデータのガバナンス法などが出てきているが、そこでは、個人情報はGDPRでしっかり守っているため、データ戦略の中に混ぜて再整理することなく、データの利活用にのみフォーカスをした法体系などを作ろうとしているようだ。つまり、データの利活用をどう進めるかということに主眼を置いたスコープを、まずしっかり設定すべきと考えている。

徳田構成員）

実際にマクロ的な視点でスマートシティが連携している状況を考慮するというように枠組みを大きくしたのは、非常に良いと思っている。いくつか事例を差し上げると、私たち、EUと日本で色々スマートシティに関するプロジェクトを10年くらい前からやっていたが、例えば藤沢市の中に藤沢市の自治体がやろうとしているスマートシティの枠組みと民間企業、第3セクターが合意して、藤沢サステナブルスマートタウンというものが中に包含されているようなケースもある。豪雨があった時に、スマートサステナブルタウンの方が、局地的な気象情報の予測が精度良くできているので、避難しないで良いという結果を出している一方、藤沢市は、藤沢市の広範囲な予測なので、緊急避難をしてくださいという判断となった。そういう行政側のラージスケールのサービスと非常にタウンレベルで小さく600戸くらいある中のサービスでコンフリクトが起きた時にどうするかみたいな事象が現実にも起きている。また、サービスを提供する側のマルチステークホルダの件で、サービス事業者向けに整理したというのは、それはそれで筋は通っていると思うが、スマートIoT推進フォーラムでIoTのガイドラインを作った時には、一般ユーザという項目があった。つまり、例えば推進主体である地方自治体が、一般市民に対して何をどう提供していくか、同じようにある種のイリーガルな、あるいはイレギュラーなことが起きた時に、そういうのもガイドラインがないと、サービス提供側だけがマルチステークホルダであるという仕切りは、セキュリティガイドラインとしてはまだ不十分で、80パーセントくらいと思う。一般市民と自治体が協力して作るのがスマートシティという概念だと個人的に思っており、サービスを受ける側の方に対しても、最低限これとこれとこれは自覚して行動しましょうということが、シティレベルだったりタウンレベルでもいいが、ガイドラインの中にないと、そのガバナンスを任された方たちが誤解すると思う。誰のためのスマートシティか、ということが非常に概念が歪んでしまって、サービスを提供する事業者だけが全部やっているから、あなたたちは何も知らなくてもいいですよというのは、古い発想だと思う。そういった概念を上手く入れないと、今後ますますスマートシティやスマートタウンやスマートビレッジなどガバナンスの範囲が小さいレベルで様々な構成が違うものが出てきた時に、どのようにこのリファレンスアーキテクチャで整理するのかが課題である。現実、資料29-1の5ページ目に書いてあるようなことをやろうとすると、技術的にも非常に難しいと思う。かつて、スマイルクーポンという商業施設の割引をその人の笑顔の度合いや天候、時間などに応じてダイナミックプライシングと顔写真を入れるクーポンを配る実験を日本とスペインでやったが、スペインはGDPRがあり、12歳以下の子どもの顔写真をカメラの前で撮るというのは、親の承諾がないとできないという制約があった。そういうのもサービスとして連携しようとしても、先ほどのデータの取り扱いなども変わるので、きれいにまとめられているのは素晴らしいが、これを実現するのはかなり難しいと思った。

岡村構成員）

少し違った角度から付言すると、スマートシティ実現といっても端末は住民で、そこにスマートホームという名前で呼んでいいかどうかはともかくとして、そういうものがある。機密性の観点から、ゼロトラスト的な観点で、端末であるホームの方にも目を向ける必要がある。それから可用性・完全性という観点からすると、十分な連携性を確保するためには、プロトコルやフォーマットの共通性や互換性についても考慮が必要ではないか。また当然、技術向上に即して必要に応じた見直しが必要。ベンダーロックインという言葉もあるので、あまりロックイ

ンされないような形にしようということになると、ある程度、公の方で QM 作りということを考えていかなければならない。日本初であって欲しいと思うが、日本初の国際基準的な形のものに発展させていくような考え方をしていただく必要がある。また、先ほどの個人情報保護について、実は昨年の個人情報保護法の改正で、仮名加工情報という制度が導入されたが、これは現段階ではどの程度利用できるか不明。その前の改正時に導入された匿名加工情報制度というのも敷居が高いので、必ずしも利用が容易といえない。もう少し小山構成員の発言のとおり、利活用とのバランスを図るような観点を制度の方で持っていただきたいと個人的に考える。

安達構成員）

5 ページ目の図を見て、全体を俯瞰するセキュリティ体制も必要だと思った。フジテレビでは各県まではいかないが 27 の系列局があり、経営も立地条件も体制も全て違うという中でネットワークを組んでいるが、このスマートシティと非常に近いものがあると思う。そうなると、全体をまとめるのに 1 つの俯瞰したものがあってもいいと感じた。また、ライフラインや末端のスマートホームのような各サービスとでは、セキュリティ対策の方法や重要度が違う。先ほど系列局の話とも関連するが、同じようにスマートシティ間の連携では、セキュリティに関する共通的なインタフェースがあると、今後スムーズに進んでいくと思った。

中溝サイバーセキュリティ統括官室参事官）

第 1.0 版との整合性という点については、基本的には第 1.0 版と第 2.0 版で考え方を大きく変えたわけではなく、むしろ足りない部分を補強しているため、整合性が取れていないということはない。ただ構成が大幅に変わるので、変化があった部分については丁寧に説明することが必要ということに留意する。2 点目のデータの重要性、利活用については、今回スマートシティのプライバシーのガイドラインではなくて、セキュリティのガイドラインなので、プライバシー情報・個人情報の取り扱い方、プライバシー保護の観点から何をすべきかということを踏み込んで書いているものではない。おそらく、そういう取組は、また政府内の別の場所で検討が行われる部分もあると思うので、今回はセキュリティを中心に考えている。ただ、データとしてはオープンデータの他に、パーソナルデータ、オープンではないけどパーソナルでもない非パーソナルデータといった分類があり、これらについても多分、異なる扱いが必要だということも、我々は検討の中で議論が出ているので、そういったデータによって取り扱いが異なりうるということも、しっかり書いておく必要があると、お話を伺って感じている。また、特にユーザをちゃんと含めないといけないのではないかという点は、大変重要なご指摘だと思っており、今後の補強ということもあるが、今の時点でも何か少し記述すべきことがあるかどうかというのは、よく検討していきたいと考えている。別でご指摘があったスマートホームというのは、多分同じようなユーザ視点の話かと思うので、同じような視点から考えたいと思う。共通的なインターフェースという点については、先ほど紹介した SIP でやっているリファレンスアーキテクチャーの方にも一定程度そういう記載があったかと思うので、ここはあくまでもセキュリティの確保であるということでご理解いただきたい。将来的に国際基準へといったことも含めて、我々としてもこのガイドラインを今後どう扱っていくかということを検討する際に、参考にさせていただく。

後藤座長）

スマートシティは、すべてを含んでいるので、色々な考えが出てくるのは当然。まず今日、事務局としては構成員からの様々なコメントを集めるということでよいか。

中溝サイバーセキュリティ統括官室参事官）

認識の通り。今日いただいた意見も踏まえて、第 2.0 版を最終的なものにしていきたい。

若江構成員）

先ほど、個人情報という言葉が入ると萎縮効果を及ぼす懸念があり、利活用に主眼を置いたスコープを設定すべきというようなお話があった。産業データやオープンデータのみを扱うということであればそれでいいが、スマートシティでは住民に良いサービスを展開する上で個人に関する情報を活用しないわけにはいかないので、そこをどう取り扱うかは正面から検討すべき。データを提供する側は個人なので、データ利活用のためにも個人情報を大切にするという姿勢を打ち出していただかないと、データは出てこなくなり、利活用も難しくなる。

中尾構成員）

先ほど国際標準化という話が出たが、実は、IoT 推進コンソーシアムをベースに ISO や ITU-T で標準化活動をしているが大変で、IoT だけで大変なのにこれだけのステークホルダがたくさん出てきた標準化は、多分人生を捧げるレベルの話になってしまうので、上手くもっていけるかもしれないが、考えていただきたい。多分セキュリティの対策というのは、3 章に記載されているが、各ステークホルダに対する対策というのをユーザも含めて整理できると良いが、実は IoT の国際規格でも全然できていなくて、ユーザは整理できるが、ユーザ以外は一色淡にまとまっている。相互に関係しているので中々難しくて、標準化も簡単ではないと理解している。

林構成員）

電気通信事業者のネットワークの安全信頼性の確保というテーマについて、私自身も長い間、研究者として関心を持ち続けている。昨年、「サイバーセキュリティと通信の秘密に関する提言」という、長文の論文に一通り私の考えをまとめたので、今回こういう形で、さらに組織的に検討を続けていただけることは大変喜ばしい。私たちは通信ログという、いわば事後的な追跡のための情報を念頭に置いてきたが、今回フロー情報という形で、リアルタイムで動いている情報を念頭に書かれている点に注目している。そこで、2 点ばかりこういう視点で詰めていただきたいと考えていることを紹介させていただきたい。1 つは総論的なマクロ的な視点で、もう 1 つは各論的なミクロな視点である。マクロ的に言うと、このタスクフォース会合でも随分前にセキュリティ対策でデータ負けしないような仕組みが必要であるということが強く打ち出された。しかもそれは、個別の企業、あるいはサプライチェーンの問題にとどまらず、サイバーハイジーン的に社会全体の問題にもなっている。そういう意味でいうと、情報を持っている人は誰かということが大事になるが、おそらく日本国においては、ISP がベストポジションにいると思う。セキュリティベンダーも OTT も強力な組織があれば、そちらの方がよりベストポジションに近いということになるかもしれないが、日本においては残念ながら相対的に ISP 等に依存するということになる気がする。そういう意味で、こういう取組を進めていただくことは、データ負けの問題の解決にもつながるものであることは忘れてはならない。2 点目の各論的な方だが、もし、ISP あるいは電気通信事業者が最も大きな情報源を持っており、その情報に期待するということであると、その人たちにインセンティブを与えるような方法が必要である。ムーアの法則が今日もなお有効であるということは、消費者余剰はどんどん高まるけれども、事業者の方の財務はどんどん苦しくなることを意味する。そこでまた、最もプロフィタブルである携帯電話について、大幅値下げがトレンドということになっていくと、そもそも ISP や電気通信事業者は、何をメインのビジネスにしていくのかという瀬戸際に立たされることになる。そこで単なる情報の運び屋ではなくて、セキュリティのマネジメント付きの運び屋、つまりマネージドセキュリティサービスプロバイダーを志向するというのが、大手の事業者にとっては、方向性の 1 つになると思う。そうした事業者が、インセンティブを持ち寄えるような設計にしていただくというのが、制度として 1 番効率が上がると思う。

戸川構成員）

電気通信事業者のネットワーク安全信頼性全般に関して、このような場で議論させていただくのは、非常に重要だと思う。繰り返しになるが、5G、6G を見据えて、ソフトウェア化に関連する所のセキュリティリスクが十分に考えられて、今後ますます大きくなると思っているので、ここは繰り返し啓発も含めて指摘していくことが非常に重要になる。リスクが十分にあるということを、皆で認識するところが非常に重要。それから、いわゆるグローバルサプライチェーンリスクの高まりも、その通りとなっている。検証体制も含めて、いかに確立するかが重要な課題かと思っているので、継続して、この場も含めて、有識者の皆様方で議論していくということが非常に重要。いずれにしても、色々な観点から電気通信事業者のセキュリティの確保に十分に取り組む必要があるので、引き続きこうした活動を続けていただきたい。

小山構成員）

資料 29-2 の 4 ページの最後に書かれている電気通信事業者による積極的なセキュリティ対策の実施の必要性ということで、こういった施策を進めていただけるということで、大変嬉しい。2002 年にテレコム・アイザックが設立され、ICT-ISAC に名を変えて現在に至るまで、ISAC メンバの通信事業者自身が、通信サービスに関するセキュリティ対策を進めることが難しかった歴史がある。そこで、ウイルス対策など他業界の方でもできるようなセキュリティ対策が中心となり、情報共有に関しても通信目線の通信事業者ならではの情報共有というものが、かなり制限された状況となっている。それは何よりも通信の秘密が重要であり、お客様の情報をしっかり守っていくという理念が浸透していたからだが、最近の IoT の時代になってくると、エンドポイントのセキュリティ対策も不十分な状態で、ネットワークの接続をするデバイスがどんどん増えていき、セキュリティ対策が不十分なデバイスに対して通信事業者から注意喚起などを行ったとしても、自分が管理しているものかどうか分からないというような、当事者能力が十分でない利用者が増えている中で、セキュリティ対策をどう進めていくかという本当に袋小路の状態に入っていると考えている。一方、海外ではここに書かれているようなフローを見て、C&C サーバを分析するというようなことは早くから行われており、まずそういったことが、研究的に取り組めるだけでも大きな 1 歩だと思う。フロー情報分析を行って、本当に C&C サーバを検知することができるのか、通信業界でもトライアルをさせていただけるのであればありがたい。いきなり通信を遮断するのではなく、C&C サーバの検知が本当にできるのかということを、通信の秘密との関係や法的な課題や技術的な課題を整理するという所から始めさせていただけるのであれば、非常にありがたいと思っている。

　これまでは、接続ログによる契約者の特定や、サーバへの過去のアクセス履歴から送信元を特定する際の通信の秘密の取り扱いについて論じられてきたが、今後は今、目の前を流れている通信の外形情報を分析することによって、もっと言うとエンドポイントやサーバなどのすぐ利用者に直結してしまうような情報ではなくて、利用者とは遠い情報を分析することで、セキュリティ対策につなげられれば、通信の秘密の侵害の度合いも限定的と言える可能性もあるので、ぜひ私も前向きに関わらせていただきたい。

安達構成員）

安全な通信ネットワーク構築に関して、ユーザとして期待したい。

中尾構成員）

以前から通信事業者のフロー情報だけではなくて、例えば、5G も考えた時に、MEC でのデータ保管など、データの扱いについては、法的課題や技術的な課題の整理というのも必要と思うので、ここでやられている内容というのは非常に重要。可能であれば、NICT 的に申し上げると、電気通信事業者のフロー情報だけではなくて、例えば NICT での色々な知的基盤が集まっているデータとのコリレーションなどを行うことによって、精度の高い C&C サーバの検知などへの活用ができると良い。最近 1 月 27 日に Emotet の C&C サーバがテイクダウンされ

て、大きな効果が出てきているので、そういう活動につながると良い。

小山構成員）

弊社がサイバー攻撃を受けた経験の中で、情報をどう公開していくのか、あるいは必要とする人にどう届けるのかという点について、自社の課題として取り組んできた。その経験を踏まえ、資料 29-3 を拝見すると、目的として何のために情報公開をするかというところをしっかり見据えないと、単に他社のセキュリティ対策のために情報公開をするだけでは、被害を受けた当事者の方は情報発信に踏み切れないというのが、実情ではないだろうか。攻撃を受けた被害者のつもりが、情報公開、あるいはご迷惑をかけたお客様に説明した瞬間に、加害者に変わる。また、そこから報道関係者が記事に書いた瞬間、社会的な悪者にもなったりする。被害情報の発信を考えると、ステークホルダとのこじれていく関係を、どのように修復しながら進めるかということを抜きに情報公開ができないということを身をもって経験している。願わくばこの情報公開の取組が、被害者を取り巻くステークホルダのあるべき振る舞いというものを世の中的にもコンセンサスを得ていく取組につなげてほしい。ステークホルダが被害情報を聞いた時の反応として、例えばそれですべてか、100 パーセント安全を保障されるのかということを言われると、何も言えなくなってしまうので、ステークホルダに対して情報公開をする人を、どう見守っていくのか、支援していくのかという所を、ぜひとも世の中の合意事項として持てたら良いし、そういったことにも触れていただけると、今後の議論にもつながる。

藤本構成員）

情報共有について、質問とコメントがある。今、JPCERT/CC への情報提供が、組織のどういった部門から出されているのかというのをお聞きしたい。それが時として情報システム部門の方だったりした場合は、コンテキストに関する情報を例えば、組織内の別の部署に聞きにいくなどの作業が必要になる可能性がある。そういった意味で、今回ご発表の中で時間軸を設定されたというのは、非常に有効的な考え方かと思うが、さらに有効に活用・促進していくためには、組織内でのヒアリング方法、たとえば何のためにそのヒアリングが重要なのか、正直に話をしてもらっても大丈夫なんだというように、説明の仕方を工夫しないと、中々話してはいただけないかなと思うので、そういったテクニック的な面についてもヒントのようなものが併せてあると、情報提供がより進むのではないか。

JPCERT/CC 佐々木氏）

1 つ目のご意見の共通理解という部分に関して、今回の報告書を今後活用いただく中で、社会全体で共通理解としていただけるような形のものを作りたい。資料の 2 ページ目の方に、小さく書いたが、情報の公表後に対応について叩かれるというようなものが非常に多いと感じた。そういった中で、JPCERT/CC では、年間で 1 万件か 2 万件ほどインシデント対応させていただいているが、特に非常に重たい案件、標的型攻撃をはじめとした長く時間がかかる案件、ステークホルダが多数関与する案件であればあるほど、残念ながら被害組織様の頑張り、努力に対して、非常に正反対のような反応が各方面からされているのが現状。その中で、ステークホルダとの関係においてという部分について、何のために公表を被害組織がやりたいと考えているのかという部分について、必ずしもステークホルダの理解を得られておらず、そういったトラブルになっているケースがある。公表後の意味合いや公表の記載内容の部分について、当然公表前に例えば所管省庁であったり、あるいは取引先等説明するが、この時にどうしても理解を得られないようなケース、どうしても攻撃被害を発生させてしまったことへの責任追及や先ほどのお話にもあった本当に大丈夫なのかといったような追求するようなやり取りが非常に多い。当然、リスクコミュニケーションの問題なので、サイバーの範疇を超える問題だとは思うが、例えば公表しようとしている情報、あるいは調査で判明したものが一体どういうことを意味しているのかといったような部分の共通理解

に至れるような参考となる、例えばそれがメトリクスや様々な情報の性質の定義みたいなものについてお示しできればと思う。両者がともにご参考いただけるようなものを通じてコミュニケーションをとっていただいて、誤解の無いようにコミュニケーションを進められれば良いのではないかと考えている。現状、そういったものがないのではないかと考えている。また、2 点目のご意見について、現状弊センターに公表前の情報共有段階、あるいは公表の段階で情報提供をいただく部門としては、CSIRT をはじめとした情報システム部門、セキュリティ担当部門の方々が大多数を占めている。一方で、指摘の通りだが、情報の公表に向けて、社内的なコンセンサスを作っていくにあたって、残念ながら情報をどれを書いてどれを書いちゃダメかというのは、業務の部分であまり上手くいってないケースがあり、そういった場合には、その企業の法務の方から弊センターの方にご質問をいただいたり、あるいはリスク管理部門・広報部門といった対外的な情報発信の判断をする部門から CSIRT 部門・情報システム部門を飛び越えて、質問が来るというケースがある。ここは、そのタイムスパンの中で、社内合意に至れていないケースだと考えている。こちらも、必ずしも CSIRT チーム・セキュリティチームの皆さん方の理解不足とか説明不足ということではなくて、共通理解に至るような物差しみたいなものがない中で、バタバタとコミュニケーションをとるので、そういった理解不足に至っていると思っているので、これも同じようにお互いにこういったものだというように頭を整理していただくための物差しとなるような形でお伝えできればと考えている。

後藤座長）

私も実は、情報共有の対象となるインシデントにおいても、大きなインシデントと小さなインシデントが入れ子構造になっている場合はどうなるのかなど、そういう所についても興味を持っている。これまでの議題について既にチャットでもコメントが色々と来ているが、今後補足のコメントが有ればチャットに残していただきたい。また、傍聴の音声はここまでとさせていただきたい。

◆議題（4）「サイバーセキュリティ分野における国際連携」について、事務局より「資料 29-4　サイバーセキュリティ分野における国際連携について」を説明し、質疑応答、意見交換を実施（非公開）。

【別紙】

◆時間内にご発表できなかったチャット欄のコメント

＜議事（１）について＞

篠田構成員）

スマートシティについて、私からは意見は特にございません。現状あるガイドラインなどで事務局の方でよく検討されているのだと信じます。個人には日本国民以外も含まれると思うので、そうした個人を含むユーザからのフィードバックで柔軟に変化されることを期待します。

＜議事（３）について＞

徳田構成員）

COIVD－１９に感染した人達に対する差別などと同じで、ステークホルダとしての基本的な考え方を書かれているとよいと思いました。

JPCERT/CC 佐々木氏）

>徳田構成員 ご指摘の通りかと考えます。これからお示しさせていただくものは必ずしも被害組織側の理解を高めるだけのものではなく、公表前の報告を受ける所管省庁なり各ステークホルダ側の理解の向上にもつなげていただくためのものと考えております。

岡村構成員）

２０２０年個人情報保護法改正に基づき、重大な漏えい事故などが発生したおそれが判明したときは、委員会に報告するとともに、本人に通知する義務を負うことになった（２２条の２）。漏えい原因となったサイバー攻撃の「確報」を個情委規則案で６０日以内に行うことになった。攻撃が、高度化、複雑化、グローバル化する中で一律にこの期限への限定は困難ではないか。

JPCERT/CC 佐々木氏）

>岡村構成員 ご指摘の通りかと考えます。これまでもありましたが、侵入原因が多様化・複雑化する中で原因究明の難しい事案が増えていると考えますので、報告期日はケース毎に柔軟であるべきと感じております。

鵜飼構成員）

小山さんの意見に賛同しております。やはり社会的コンセンサスをいかに作るのかが重要で、これが出来ていないと情報共有・情報公開をするインセンティブは現実的には生まれてこないと思います。情報公開のためのプロセスの検討を行う事に加え、社会的コンセンサスを作るための広報活動（マーケティング）にしっかりコストをかけらえる状況を作り、有効な施策について検討できればと思います。

JPCERT/CC 佐々木氏）

>鵜飼委員 同じことを弊センター側でも日々感じております。特に「公表」が懲罰的な意味を持たれてしまつ

たりする傾向があるように感じるケースが多いところ、事案対応支援にあたる側としては誰もが「被害者」ですので、被害組織が（業法等による義務的な公表は別として）自主的な積極的な判断で公表をされることに対しては最大限、被害組織の対応結果（事案対応）への（前向きな）評価を前提として理解されるべきで、その点も本報告でまずは示していきたいと考えています。

篠田構成員）

JPCERT/CCの報告に関して。
「どんな情報をいつどこに出してよいかわからない」はそのとおりだと思います。なんらかのフォーマットやガイドラインはあってほしいし、広く周知してほしいと思います。
濡れた犬を更に叩く。。。
報告のインセンティブはなかなか上がらないと思います。
災害だと捉えられるといいのですが、真には攻撃者が悪いこと、を折に触れて発信していくことは、大切な運動だと思います。
規制業種などでは事故報告などはどうしているのでしょうか。
報告義務があるから、事故報告があり、二度と起きないようなプラクティスにつながるのでしょうか。

以上