サイバーセキュリティタスクフォース（第 27 回）議事要旨

1. 日 時：令和 2 年 12 月 3 日（木）10:00～11:45

2. 場 所：オンライン

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、安達構成員、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】

鮫島清豪（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）

【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）、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 27-1　サイバー攻撃をめぐる最近の動向
資料 27-2　VPN 脆弱性とランサムウェアの直近の状況（鵜飼構成員）
資料 27-3　IoT 端末等を踏み台にしたサイバー攻撃への対策の強化の必要性（小山構成員）
資料 27-4　今後の検討課題について
参考資料 1　サイバーセキュリティタスクフォース第 26 回　議事要旨
参考資料 2　サイバーセキュリティタスクフォース　開催要綱

5. 議事概要

（1）開会

（2）議事

◆「サイバー攻撃をめぐる最近の動向」「今後の検討課題について」について、事務局より「資料 27-1、資料 27-4」を説明。「VPN 脆弱性とランサムウェアの直近の状況」について、鵜飼構成員より「資料 27-2」を説明。「IoT 端末等を踏み台にしたサイバー攻撃への対策の強化の必要性」について、小山構成員より「資料 27-3」を説明。

◆構成員の意見・コメント

小山構成員）

鵜飼構成員のコメントにもあったが、VPN を張るということは先端側が固定 IP ということで、ユーザ名の特定に通信

の秘密の侵害は伴わない。しかし、仕組みとしてプロバイダの顧客データベースを見なければならないということもある。例えば JPNIC に IP アドレスの管理者が登録されているかというと、固定 IP を 1 個しか使っていないケースの場合は、プロバイダの 1 ユーザだとしか見えないため、固定 IP を誰が使っているかをアドレス管理組織上で見れるような仕組みがあると、対策は円滑に進んでいくと思う。脆弱性が公開された場合、大企業だと調査部隊を持っていたりして調べたりすると思うが、問題となるのは中小企業である。中小企業が SSL-VPN 等で侵入されると、影響を受けるのはそこに仕事を発注している大企業となり、サプライチェーン問題に直結してくるので、ユーザ特定をするところについて、従来型から一歩踏み出した取組が出来ると素晴らしいセキュアな社会に繋がるのではないかと思う。

若江構成員）

VPN の脆弱性は去年から公表されていたが、脆弱性情報を末端まで伝えるのがなかなか難しく、結局攻撃されてから慌ててしまったという現状もあった。提供しているメーカに聞いた話では、ユーザ企業にパッチ適用を呼びかけたくても、間にベンダが何社も入っていてユーザ企業まで情報が届かなかったこともあったという。脆弱性対応に慣れていない中小企業もテレワーク導入で VPN を使い始めたという現状もある。それを考えると鵜飼構成員のアイデアはとても良いと思う。問題は費用をどこが負担するのかということで、場合によっては国の事業として行い、受託のような形で任せるのも良いと思った。

吉岡構成員）

VPN に関連して最近の経験も含めてだが、少し前に NHK の番組に少し協力することがあり、Windows のリモートデスクトップのサービス等もテレワークで使われるということで調査をしたり、実際どうしてそういうものが外から見える状況で動いているのかということを調べた。そこで凄く感じたこととして、中小企業では VPN すら使っていないという状況が相当多いような気がした。VPN すら分からないというような感じで、Windows サーバのリモートデスクトップがそのまま晒されていて、10 年前の脆弱性を持ったまま動いており、そこにはユーザ名や組織名がそのまま出ていたといった、目も当てられないような状況が相当数あった。そういう意味では、VPN の話もそうだがもっとひどい状況が沢山あるというのを最近実感したので共有する。それを踏まえると、当然のように脆弱性パッチを当てていないようなケースもあると思った。また、大学の方では最近学生が大学に来て授業を受けられないので、リモート接続、リモートデスクトップ等でプログラミングの演習等をやっているが、そういうサービスを公開するとやはり相当数の攻撃が来る。当然攻撃が来ることが分かっているので、デフォルトポートではなく、推測されにくいポートで動かすが、目ざとく探してきて、あっという間に攻撃対象になるということで、攻撃者からはものすごく探索されていて、狙われているなという感覚を持っている。

徳田構成員）

小山構成員からの発表で NOTICE の 2020 年と 2021 年以降の比較を表にまとめていただいたものが最後にあるが、整理していただいているように、注意喚起の到達性というか、エンドユーザの方たちに行動変容していただかない限り、危ない機器が減っていかない。そういう意味で言うと、私たちがスキャンした後の行動変容を本当に促せるような作戦を 2021 年に向けて改善していくことを的確にご指摘していただいたので、NOTICE チームとも話をしたいと思う。それから、調査ポートの拡大について、先ほどの VPN の件とも関係するが、そのあたりも少し前広に議論をしたいと思うが、私たちがシステムとして裏からどんどん調査枠を広げていくと、不要な不安や心配も増えてしまうと

いう副作用もあるため、そのあたりの拡大は合意形成をしながらやっていければと思っている。

中尾構成員）

NOTICE について、昨日 ICT-ISAC を中心として NICT が主催し、関係する NOTICE プロジェクトに関連する ISP に参加いただき、「IoT 機器のセキュリティ対策に係る問題と動機づけに関するワークショップ」を開催した。その中で、小山構成員にご指摘いただいた問題や 2021 年度以降の考え方や進め方という点も含めて、色々な議論をさせていただいた。大きな問題として全員が認識したことが、NOTICE は検出の数があまり多くないので、逆に ISP やエンドユーザ・利用者のインパクトに関連し、どういった問題があり、これがどういった組織やユーザにインパクトを与えて、対応しなくてはいけないかという理由付けが上手く出し切れていないのではないかということが認識された。皆さんがご存知のように、実際にマルウェアに感染している CCC（サイバークリーンセンター）と違って、NOTICE の場合は機器に脆弱性があるという状態が具体的にどのような脅威に繋がっているかが不明確であり、そのような認識がユーザ側にあるのではないかという議論もなされた。また、NOTICE がどのくらい効果があるかといった効果測定が十分にできていないので、効果測定用のツールや利用者側で簡易に検知、設定等が自動的にできるようなツールというものも開発するべきではないかという議論もあった。CCC との比較もワークショップでは実際に行われ、最近個人情報の取扱いも厳しくなっているという問題もあり、NOTICE は CCC とは環境が大きく違うと考えられた。また、通知方法だが、現在はメール、郵送、電話、訪問などを用いて通知しているが、SMS はまだ利用していない。このあたりも具体的に利用者が法人か個人かによって異なってくるのではないかと考えられる。また、現在の NOTICE では、トラッキング ID のようなものが明確にないので、問い合わせ ID というものを上手く使っているが、それでもなかなかうまく効果も測定できていないという状況である。また、NOTICE は総務省が主導で進めているプロジェクトなので、例えばハガキに対して総務省の名前を出す等、メディアへの活用を組み合わせて行うと、より効果があるのではないかと思う。そのような中で、NICT では今週末あたりから、エンドユーザを実際に訪問して、どのようなシステム環境、利用環境なのか、または組織にどういった課題があるのか等をヒアリングし、具体的な問題点をあぶりだそうという活動を始める予定である。総務省的に、それが法制度の見直しやこのタスクフォース、また対処の在り方といったところに、どのように反映させていくかということが今後の課題になると思うので、徳田構成員がおっしゃるように、この点については全体で方向性を議論することも重要だと感じた。

岡村構成員）

かつてのランサムウェアのイメージと違い、現在のランサムウェアは、まず情報をバックドアから盗み出しておいてその後でランサムウェアの本来のロックをかけるという二重攻撃になっているものが登場している。一部マスメディアでは報道されているが、そうした攻撃が登場していることは広くは行き渡ってはいない。すなわち、一般の企業、あるいは特に中小企業が持っているような認識と実際の認識が全く違う。また、証明書はいいが、実際の証明書は数日前に東欧の一部あたりの証明書発行機関が発行した証明書をつけて配布されるような形でオーダーメイドで送ってくる。あるいは中のマルウェアを分析しようと思っても、分析ブロッカーが二重三重についているといった形で、悪質化、高度化している。感染しないことが一番であるが、実際のところ扱っているのは現場の社員であるため、そのあたりに対してもエンドユーザへの啓発が必要であるが、情報のギャップがあるというのが現状だと思う。したがって、NISC や警察庁が行っているような Twitter 等の SNS も活用して、特に現実にそのハンドリングをする社員（エンドユーザ）向けに分かるような形で啓発を進めていく方が良いと思う。

藤本構成員）

注意喚起の情報を伝えるとして、セキュリティ人材に関する統計のデータ等を見ると、受け手側の人材が圧倒的に不足しているので、そのような人材育成に関する取組が急務だと思う。オンラインによる教育等も最近は進んできているが、オンサイトの教育とはコンテンツの作り方が少し違ったり、教育をする側もそれに慣れなければいけない等、色々な課題はあるので、その辺のコンテンツの開発や試行錯誤をしていく必要がある。それにより、注意喚起もさらに実効性が高まると思う。

林構成員）

デジタル庁について、これがセキュリティとどう関係するかということを検討するいいチャンスではないかと思う。まず、どのような進捗状況か教えていただきたいというのが質問としてあるが、実は質問よりもこの機会をどう捉えるかということが役立つと思うのでコメントしたい。心配していることと、これはチャンスではないかという両面があり、心配していることは、セキュリティの人材が不足しているのは会社だけではなくて政府もそうだと思うが、デジタル庁設立の過程でセキュリティに関する知識、経験あるいはリソースが分散されてしまうのではないかと感じている。逆に今度は、せっかくそういった変化があるのであればこの機会にセキュリティについて今までの考え方を見直すことも意義があると感じている。本日説明があった資料、あるいは皆様のご発言というものはそれぞれもっともなことで、反対する余地もないが、社会全体を見るとここまでリスクが拡散してくるとセキュリティ疲れのようなことになって、今までしてきたこと全てそのまま線で伸ばすということにはいかないかもしれないという感じがしている。そういった意味でいくと、デジタル庁が推進する DX のところで使い勝手の良さとセキュリティという、対立傾向にある両要素をどのように両立させるのかということを検討するので、そこのところから学ぶものがたくさんあり、さらに言えば、参考資料で配っていただいた色々な政府関係の諸機関で検討していることを総ざらいして、特に総務省の件数は非常に多いと思うので、場合によっては選択と集中でどれかにフォーカスして短期間でまとめるというような全く新しいアプローチも良いのではないかと思った。

名和構成員）

最近の脅威・リスクがソフトウェアのマルウェア感染より、リソースのアクセスのための資格情報、認証情報の窃取が多くなっているという印象がある。これは VPN に対するプロービングやフィッシングもそうだと思っており、そちらの急増しているリスクに対する措置を考えた方がいいと思っている。冒頭、総務省からゼロトラストについて言及されていたが、あくまで米国や欧州ではゼロトラストは、Always verify あるいは Contextual access と解釈されており、その定義に基づく対応の方に思想転換していく方が良いのではないかと考えている。日本ではまだ従来のやり方が多いように感じる。今申し上げたコメントの前提として、ユーザに対する教育あるいは啓発とあったが、私の認識ではもう無理ではないかと思っている。教育効果を上げるというところは、ユーザのリソースに対するアクセスの頻度や数がこれ以降全く増えないのであれば、それを前提として教育効果を積み上げていくことが期待できると思う。しかし、今後 DX やクラウドサービスの利用が増大し、それは自治体でも同様である。一人当たりのリモートでのリソースへのアクセスの頻度と、その数が増大していくということについては、教育では事実上不可能であるし、必ず裏切られると思う。したがってユーザを信じない形でリソースアクセスの環境を提供するということについては、ゼロトラストあるいは Always verify という考え方に対する研究開発をしていくことが良いと思う。一つのアイディアとしてクラウドアナリティクスがあると思う。

戸川構成員）

中長期的な視点でコメントしたいと思う。Beyond5G や 6G に向けていわゆる DX が加速してくることと思うが、ここに及んでも IoT や Beyond5G、6G のセキュリティの重要性がさらに増していくものだと思っている。中長期的な戦略として、これまで IoT・5G セキュリティ総合対策等で謳われていたことが全て何かに置き換わるということは無く、研究開発も含めて現状の IoT・5G セキュリティの対策をある時点で止めてしまわずに継続して、こういった政策を続けていくことが非常に重要であると思っている。それに加えて、どこまでできるか等色々な問題はあると思うが、Beyond5G、6G に向けて新たなセキュリティ対策が必要で、たとえばネットワークの仮想化といったところは Beyond5G、6G を構成する上で、非常に重要になってくる。そこにセキュリティ的な脆弱性が存在し、そこを突かれてしまうような可能性もあると思うので、その点は新たに研究開発要素も含めて、攻撃やそれに対する防御などを考えていく必要があるのではないかと思っている。現状で IoT・5G セキュリティ総合対策 2020 が出ているが、非常によくまとまっている内容かと思っているので、是非これをベースに膨らませるようなことをお考えいただけると幸いである。

篠田構成員）

ユーザ向けの注意喚起は継続して APWG（Anti-Phishing Working Group）で米国、欧州を中心にやっているが、専門家のきれいな言葉やイラストがあったとしても響かない。コロナ禍ではオンライン詐欺も大幅に増えたが、被害件数の推移だけでは利用者の想像力への働きかけが弱いため、先日のイベントでは実際の被害額が世界で国家予算規模の数兆円だったといった数字やランサムウェアの被害にあった声を顔出しで話していただいた。クライムウェア、仮想通貨の被害といったサイバー犯罪にしても、一般的な企業への攻撃にしても、メールやサイトを踏んでやっていくことが多い。何かしらそういった被害の結果をインパクト与え、想像力を働かせるという面も出していけると良い。

若江構成員）

海外との連携について、日本だけで NOTICE の取組を行っていても結局海外からの攻撃が減らなければ意味がない。CCC の時には日本の取組が海外でも評価されて、例えば日本の取組をドイツでも採用するといったことがあったと記憶している。そのような形で海外同士の事業者団体と協定を結んで日本の NOTICE 方式を輸出するというか、広めていくような方法を考えることも良いのではないかと思った。

後藤座長）

鵜飼構成員から最初の方で VPN を慌てて使いだして色々な問題が起こっているという話があった。クラウド等のセキュリティ問題も大部分は技術的な問題というよりも、ユーザの設定ミスが多い等のレポートもよく聞く。今回、啓発活動で注意が必要だというのと同時に、分かりやすい使い方というものに関してはユーザとサービス提供者側の両方で色々努力しないとなかなかうまくいかないという思いがある。そういう意味でサービス事業者と両方でできればと思った。

安達構成員）

インターネット環境の中で、この間標的型メール IcedID が着信したが、巧妙なメールでどうしてもアクセスしてしまう。経験上、エンドユーザにどのような教育をしても絶対繋げてしまう人が出てしまう。ISP 側で知らないうちに不正通信先の IP 等のバンクのようなものを作って、ISP 側で行かせないようにするという仕組みはできるものなのか。

小山構成員）

今の安達構成員の件について、C&C サーバを調査し、ブロックして遮断する仕組みというのは技術的には可能である。総務省とも 10 年ほど議論しているが、まだ通信の秘密の侵害度合いが大きいということで、手続き的には望まない人へのそういったことが行われない環境の提供とセットであるというところで、中々前に進めていない状況。こういったことについても検討しなければならない環境がますます悪化しているので、私としてもまた総務省に働きかけて進めていきたいと思っている。

中尾構成員）

今後の検討課題について、何点か気がついたところがある。資料 27-4 2 ページ目の「我が国のサイバーセキュリティ情報の収集・産学官の連携による分析のために NICT に構築する」については、ご存知の統合知的・人材育成基盤の効果的な活用という話だが、是非やっていただきたいと思っている。実は NICT で今年の 12 月 21 日に色々な標的型攻撃等を含めたマルウェアの解析をやっているメンバーが「クリスマスワークショップ」を開催し、そこで統合知的・人材育成基盤の活用方法について意見交換をやる予定。また、来年の 2 月 17 日には NICT のシンポジウムを予定しており、そこでも大々的に本件の話をさせていただき、色々な意見交換ができる場を作りたいと思っている。タスクフォースの中で進めていただくことは良いと思うが、NICT の中でも色々な効果的な活用ということでいつも意見交換の場を持っている。もう一つ同じページで NICT の運営の NICTER、DAEDALUS 等の取組について、リソース上の課題等もある中どのような国際連携をするかという話があるが、何年か前に総務省の肝入りで ASEAN 諸国を対象にした JASPER というプロジェクトがあった。基本的には ASEAN 諸国にダークネットを NICT に提供してもらい、DAEDALUS という NICT のシステムを用いてマルウェアの侵入や DDoS があった場合に関連するアラート情報をあげるという施策を現在も進めている。様々な活動の一つとして基本的に NICTER や DAEDALUS の活用は、世界中にかなりアピールはしているが、データをもらった時にそれがうまく活用できるかというのがなかなか難しい問題となる。例えば、CCC をドイツが上手く活用したというのはドイツ流のやり方で上手い考え方、運営をしたということであり、他の国が日本と同じような環境が揃っていないということを考えると、NICT の情報をうまく活用する中で相手方との連携をどのように取っていくかというのは、JASPER をどのように有効活用しているかというのを含めて今後の課題になると思う。NICT 的には、ポジティブに対応できると考えるが、全部を NICT に丸投げされると大変になるので、本活動に関連するステークホルダーとの連携が重要と思った。また、クラウドについて、総務省、経済産業省、NISC の中で ISMAP という活動をやっている。クラウドサービス事業者がセキュリティの対策を考えているかどうかを評価するというような話だが、クラウド上で C&C サーバが動いていたり、攻撃者がそこに入り込んで色々な活動をしているというのが見える中で、クラウドにおけるハイパーバイザ上の不正検知やクラウドそのものの分析をもう少し詳細にやるという検討もこれからは重要になると思う。

徳田構成員）

国際連携について整理すると、今まで総務省中心にやっている JASPER があるわけだが、MOU という国と国レベルの信頼関係の構築というような話もあれば、組織と組織、インスティテューションレベルでの agreement があり、それから最終的には、研究者と研究者レベルの信用の agreement があり、その上で NICTER のセンサーを置いてみる、こういう DAEDALUS を使ってみようという話となる。組織までのレベルで行くにも限界があるので、やはり国レベルでどこまでをどう整備していくかということと、例えばソフトウェアをインストールしてどことどこの情報を連携するかという組織レベルと、研究者レベルでこういう課題をどのように解決していくかという 3 つのレイヤでうまく協調していくといいのではないかと思う。それから最終的には先ほどの統合知的・人材育成基盤の話が今後の課題の中に出てきているが、私が期待しているのはセキュリティインテリジェンス情報を、NICT が持ってる WISDOM X などの自然言語処理のソフトウェア等を高度に活用して、Machine to Machine である程度枝刈りを行い、最終的な判断は少し人間に頼らなければいけない部分があるかと思う。極力トラステッドパーティ間で API を叩くことによって膨大な量の情報を集計し、しかも優先度の高いものをリストアップしてくれるというように、人と機械の協調を進めてうまくやりくりしないと出来ないようなことである。膨大なレベルの情報がやり取りされるので、是非セキュリティプロパーの方たちだけではなくて、自然言語処理であったり AI のチームをここのコミュニティに巻き込むというのが私たちも含めて課題と思っている。

後藤座長）

米国の会合等で膨大な情報を AI を駆使して 20 分以内に整理するという目標が出ていたように思う。大事なポイントだと思う。

中溝サイバーセキュリティ統括官室参事官（総括担当）

検討状況の詳細について今お答えできることはあまりないが、整備における検討の座組の状況についてご紹介する。政府全体の検討状況ということで、デジタルガバメント閣僚会議の下で有識者の方々に集まっていただき、デジタル改革関連法案の見直しに関するワーキンググループと、データ戦略のタスクフォースとがあり、データ戦略の在り方とデジタル庁の在り方をはじめとするデジタル改革関連法案の議論が政府内で進行している。年内にも何らかの方向性が出る見通しと承知しているが、当然その中で、デジタル庁とこれまで NISC が担ってきた政府全体のサイバーセキュリティの取りまとめ的な役割といった分担をどうするのか等も含めて検討の中では当然議論になっている。まだ、デジタル庁にどのような業務を持たせるのか等、最終的なところがまだ政府全体で確定している段階ではないが、NISC の関係をどう整理するのかとかいうのも含めて、政府全体でサイバーセキュリティの強化について、在り方をどうするのかをデジタル庁ができた後もしっかりと整理するというような形で議論を行われている。また、並行してデータ戦略の在り方というのも議論されており、その中でもトラスト、いわゆる信頼性の高いデータというのをどう確保するのかという観点から、そのトラストサービスの在り方といったことも検討の中に入っており、データのセキュリティやトラストといった観点でも検討が進んでいる。

園田構成員）

悪い人たちのビジネスモデルを阻害するような整備が必要だと感じていて、特にサイトをテイクダウンすることが今なかなかできないというのは悪者のビジネスモデルを加速させている要因ではないかと思っており、それをできるよ

うな法律や社会制度が必要だと考えている。あと啓発ということも話題に出ていたが、一般のユーザを啓発するというのはなかなか効果が見込めない難しい部分があると思っており、知ってほしい人に届かないというジレンマ状態がこの業界はずっと続いている。そういうことを考え続けることも大事な部分だが、やろうとするなら小学校から刷り込みのように交通安全のような感じでやるしかないのではないかという気がする。また、それをやるのと同時に、感染したらネットが使えなくなる等の少々インパクトのあるようなことをやらないと、被害の広まりというのが抑えられないのではないかと思う。

吉岡構成員）

一般のユーザにセキュリティ対策を色々期待するというのは結構難しいのではないかというような話があったが、私もその通りだと思うし、色々なところで注意喚起等の関係で関わらせていただいてもそう思う。高度な対応を期待するのは無理だと思う一方で、非常にシンプルなメッセージ、例えばパスワードをどう設定してどう更新するのが適切なのか、Emotet 等にも関係するが、添付ファイルにパスワード zip して送り、その後別メールでパスワードを送ることがよくあると思うが、それがセキュリティ上意味がないという方もいるし、そういった身近で普段疑問に思うようなことに対して、一般ユーザに向けてこのようにすべきといったメッセージの投げかけがどのくらい出ているかが気になった。そういう取組を十分にやっているということがあるのであれば教えていただきたいし、もしそうでなければそういったことも未だにセキュリティの根幹がパスワードで守られているということは色々なところで多いと思うので、意外に大事かなと思った。一方で安全なパスワードをユーザに設定してもらうということは未だにトップの国際会議でも議論されるほどユーザビリティとのバランスという意味では研究要素もあるような難しい問題だと私は認識しているので、そこも実は重要な課題となり得ると思っている。

岡村構成員）

JPCERT/CC の Twitter フォロワー数を見ていても順調に伸びているので、頭からダメだというような決めつけは少し早計ではないかと思う。それから実際に事件を扱ってみて思うのは、国際共助というのはいかに難しいかということで、特に国家間、政府間はほとんど無理なので、民間間も含めて考えていくということが重要だと思う。

（3）閉会

◆以下、チャットでのやりとり（上記発言に含まれている内容は除く）

岡村構成員）

JPCERT/CC では「マルウェア Emotet の感染拡大および新たな攻撃手法について」を公表している。それには本年８月末以来、感染爆発という状況が示されている。https://www.jpcert.or.jp/newsflash/2020090401.html

篠田構成員）

ISP 側での制御は小山構成員が言われている通りだが、世界的には、ブラウザのブロッキング DB に、フィッシング

サイトの報告が反映されるよう努力している。サイトのテイクダウンを国が強制的にできるのはロシアや中国くらいしか聞こえず、日本を含む他の国は中々難しく、ブロックが精一杯な状況との認識だ。国際連携について、現在も発信・協業はされてると思うので、どこまでやっていて、どこの組織と協業していて、どこに難しさがあるのかがわからないと効果的なコメントも難しいのではないかなというのが、正直な感想。統計データの提供だけでも、プレゼンスは保てるし、有益と思う。

鵜飼構成員）

VPN 脆弱性への対応があまり進んでいない理由だが、これは一般的な中小企業のサイバーセキュリティ対策が中々進まないのと同じで、そもそもユーザは状況を把握していない、把握したとしても対策の優先度が極めて低い、ベンダもユーザーサポートを直接行わないし個別にこのようなサポートを行うコストを価格に転嫁できない、販売店もこの手のサポートを行うモチベーションが無いなど、良いか悪いかは別として、ともかく現状のエコシステムでは対策は現実的には困難かと思う。対策を進めるためには、対応コストをこのエコシステムの外（国等）が負担するか、大きなペナルティが無いと進まないかと思う。

名和構成員）

そろそろ現場のユーザに期待をすることはやめた方が良いのではないかと感じた。コロナ対策でも「現場に一層の負担をかける」という日本のお家芸が見られるが、「行政機関や専門機関が一層の自らの努力」を増強した方が良いのではないかと思った。