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

1. 日 時：令和3年2月8日（月）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、辻構成員、徳田構成員、中尾構成員、名和構成員、林構成員、藤本構成員、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）、穂積直樹（地方公共団体情報システム機構）

【発表者】

久保田実（NICT）

【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

4. 配付資料

資料 28-1　サイバーセキュリティ統合知的・人材育成基盤 CYNEX の構築について
資料 28-2　テレワークセキュリティガイドライン等について
参考資料1　サイバーセキュリティタスクフォース第27回 議事要旨

5. 議事概要

（1）開会

（2）議事

◆議題（1）「サイバーセキュリティ統合知的・人材育成基盤」について、NICT より「資料 28-1　サイバーセキュリティ統合知的・人材育成基盤 CYNEX の構築について」を説明、議題（2）「テレワークセキュリティガ

イドライン」について、事務局より「資料 28-2　テレワークセキュリティガイドライン等について」を説明。

◆構成員の意見・コメント

岡村構成員）

産学官中核拠点の確立という点について、NISC、特にサイバーセキュリティ協議会との関係について教えてほしい。

久保田所長）

具体的にどのような連携をするのかというところまでは至っていないが、NISC とも情報共有をしながら進めていきたい。

小山構成員）

国産製品の運用と検証についてあまり詳しい説明がなかったため、もし検討中であれば教えてほしい。昨年 12 月にはアメリカ政府で、SolarWinds というネットワークマネジメントを行う、企業の IT の神経網とも呼べるような製品が乗っ取られ、重要な情報の流出等にもつながっているという報道があった。導入した製品が原因で情報が盗聴されるというようなことが実際にアメリカ政府のお膝元で起きてしまったという重大な事件だと思う。これに関してどこで侵入されたかということは明らかになっていないが、可能性として開発段階から侵入されたのではないかという報道もあり、私もそこについては盲点となっていると思う。サードパーティの部品を組み合わせてソフトウェアもハードウェアも組んでいくことから、リスクがあるということについては過去のサイバーセキュリティタスクフォースでも何度か発言があった。優れた製品であるかということを検証していくと同時に、それが本当に使う上で安全な製品であるかということも重要だと思っており、そういったことについて検討しているのであれば教えてほしい。

久保田所長）

CYNEX の中で置こうとしている国産セキュリティ製品の運用検証環境というのは、スコープが今の話とは少し違っており、国産で開発をしている方々に入ってもらい、そこでブラッシュアップをしてもらうことを想定している。SolarWinds のような話については、NICT の研究の本体の方でそういった検証も研究の一つとしてできるようにしたいと考えている。CYNEX の枠組とは別となるが、そういったこともやっていきたい。

藤本構成員）

人材育成という点で、NICT の多様な取組というものは非常に大きな効果があると思う。それを更に発展させる、特に自給率を高めるといった側面でも、ユーザ企業の理解というものは不可欠だと考えている。ユーザ企業では DX の取組等も推進されていることから、関心は高まっていると思うが、担当される方々が必ずしもセキュリティや IT に詳しいとは限らないという事情もある。そういった方々が NICT の取組にあるようなコミュニティに参加したり、交流できる機会があれば、知識や状況の理解にもつながると思うので、そういった面も併せて考えてほしい。

久保田所長）

人材育成のスコープとしては、企業等でセキュリティを担当する方の育成というものがある一方、前回のサイバーセキュリティタスクフォースの議論でもあったように、一般の方にスコープを広げる必要があるのではないかという意見もある。どこまでできるかは分からないが、やり方は検討していきたい。

若江構成員）

参加資格や参加条件をどのようにするのかが気になっている。オープン化するということは手の内を見せるということにもなるため、どうやって攻撃者が混ざらないようにするのか。今は既存のサイバー攻撃解析分科会や、既に分かっている人たちを初期の参画組織として始めるため問題はないと思うが、今後もし色々な希望が来た場合にはどこで切るのか、考えについて教えてほしい。

久保田所長）

基本的には初期参画メンバーはそういった形としており、今後入っていただくとしても闇雲に 100 や 200 の方々に入っていただくようにすべきとは思っていない。NICT の事務局を回している部隊とよく協議をして、これに賛同していただいて我々としても安心できる方に入っていただく必要がある。どのようにするかについては明確に今は答えられないが、そのあたりは慎重に進めていく必要があると考えている。

林構成員）

方向性としては大賛成であり、ぜひこの方向で情報を拡充してほしい。そうすると理想通りいけばいくほど、情報管理や資格審査をどうするのかという問題になる。扱われる情報が特定秘密に該当すれば、特定秘密保護法でいろいろな仕組みがある。安全保障に著しい支障を与えるおそれがある情報ばかりを扱うわけではないということから、特定秘密保護法の適用というのは難しいように思う。むしろ特定秘密保護法に当たれば楽なのかもしれないが、そうでないのであれば NICT で別途通常より厳密な情報管理と資格審査の仕組みを作らなければならないという気がしている。その場合は NIST SP800 シリーズのような手続きを導入するということになると思う。特に適正評価が重要であり、仮に特定秘密に該当しない場合であっても、実績を積み上げていかなければ改善ができないため、着手は早ければ早いほど良いと思う。情報セキュリティ大学院大学を作った早期の頃から国家安全保障に関わるセキュリティ問題をどう扱うのか考えていたが、初期にはそれが間に合わないため、技術系中心の大学院として発足した。10 年近く経った頃にアメリカの安全保障の学者にヒアリングをしようとしたが、先方から「セキュリティクリアランスを受けているのか」と逆に聞かれたことがある。アメリカは 500 万人くらいセキュリティクリアランスを受けた人がおり、それは人口の 1.5%程度に当たり、学者も当然受けている。こういった制度があると、「誰が入れるのか」という質問についての答えに近いものを提供することになるのではないか。私はアメリカの学者に対し「持っていない、日本にそういう仕組みはまだない」と回答したため、結局深いヒアリングを行えなかった。日本も防衛調達にからんで徐々に NIST SP800 シリーズのペースになっていき、ISMS の時代が終わり次の新しい時代になるというのが民間の方でも進むと考えるため、情報管理をどうするかというのは早期に検討を開始した方がよいのではないかと思う。

久保田所長）

セキュリティ管理については、情報をどう守るのかと参加者のクリアランスをどうするのかという二つの側面がある。情報に関してはNICTではサイバーセキュリティ情報についてかなり厳密に管理をし、例えばいくつかの段階に分けて情報開示の選択をして運用する仕組みを作っている。参加資格のクリアランスに関しては、議論をする必要があると思っている。これについてはアライアンスを本格的に立ち上げようとしている1～2年の間に慎重に検討していきたい。

後藤座長）

情報に関しては漏洩だけでなく、外から汚染される可能性もあるので考慮していただきたい。

篠田構成員）

本基盤の利用者の顔があまり見えてこない。また、ローンチまでにインターフェイスを含めフィードバックを得ながら作り上げていくのにお金がかかると思うが、どのようにトライ＆エラーをしていくつもりなのか。

久保田所長）

統合知的基盤の方のユーザイメージとしては、第一に日本のセキュリティ製品を作っているメーカ、ベンダの方や研究機関の方で、一緒にサイバー攻撃の分析やセキュリティ製品のブラッシュアップをする方を想定している。あるいは比較的大きな企業で、高度なセキュリティのオペレーションが求められる場でのセキュリティ人材を育成したい方が想定される。

篠田構成員）

そういった人たちは何に困っていてこのサービスを利用するのか。

久保田所長）

まずセキュリティ製品という意味ではデータがなかなか集まらない。データドリブン、データオリエンテッドな開発をするための基盤として作るということである。

篠田構成員）

高度なオペレーションをしたい企業が模擬的に利用するということか。

久保田所長）

人材育成という意味ではNICTのネットワークに様々なセキュリティ製品を導入しており、その中には海外の製品もあるので、高度なSOC人材はそこでいろいろと使ってみる、あるいは分析をしていくという使い方がある。

また、国内の中小のセキュリティベンダの方も利用できる。人材育成基盤は、現状でニーズが多いのは中小の自前で基盤を構築する財力が厳しいような、教育事業者や教育機関などへの共通基盤として提供ができる。これまでそういったサービスはなく、あるとしてもクラウドを使用して自分で開発する必要があったので、そういう意味ではユーザのニーズがあるように思える。

篠田構成員）

すぐに使えるという状態でお届けするのか。

久保田所長）

既にあるコンテンツを利用したい場合はすぐに使うということもできる。もう少し突っ込んで、特定の対象向けに共同で作っていくというニーズにも応えられるようにしたい。

名和構成員）

教育あるいは育成を受ける人材側のモチベーションやキャリアに関する説明がなかったように感じた。そのあたりの検討はしているか。

久保田所長）

どちらかといえば人材育成基盤の方は人材育成を行っていく事業者との連携をメインに考えている。コンテンツの中で実際に研修を受ける方のモチベーションやセキュリティの資格を維持するためのものに関しては、ナショナルサイバートレーニングセンターで検討している。

後藤座長）

質問の意図としては、研修を受ける側にとってキャリアパスや資格になるのか、という意味か。

名和構成員）

様々な取組で類似したものが多く見られる。医者や法曹界では素晴らしいモデルだったが、育成に失敗する、あるいは過剰・過少であるということが日本で数十年多かったように思え、いずれも育成される側に寄り添った施策が少なかったように思っている。そういった過去の失敗や反省から見られるような議論がどこまで進んでいるのかということを知りたかった。

久保田所長）

教育事業者の方とよく話しながら作っていく必要があるので、心して取り掛かりたい。

鵜飼構成員）

我々もサイバーセキュリティ製品ベンダだが、インセンティブが見えにくいので、はっきりしたものがあると良い。ベンダからすると、この取組で最もインセンティブになりそうな点は競合の情報が得られることである。海外の有力製品も複数稼働し比較することができ、弊社の競合になっている海外の製品と比べて詳細を調べることができる。しかし、海外ベンダからするとそのようなことはやりたくない、こういった取組をやりますと言った途端に売ってくれなくなるので、この点はどう考えるか。メリットとしては、競合は海外のみで日本は一社だけというようなベンダだと非常にメリットがある。一方で資産管理ベンダなどは国内で競合になっており、そうなると競合に情報を渡したくないため、やりにくいように思う。また、ほかのインセンティブについてはよくわからないところがあり、例えばリアルな攻撃に対してきちんと検知・防御できるのか、運用が回るのかというようなことは、ベンダは企業や大学に無料でライセンスを出している、あるいはベンダ側が費用を出してパイロットになってもらい使ってもらうケースがある。これができるとリアルなデータが手に入り、場合によっては製品に不具合があったり上手く検知・防御できなかったりしても情報が競合に漏れない、弱点をお客様に知られないということにメリットがある。かつ企業や大学では何千何万の単位で実施できるため有用である。こういった状況があり、ベンダもそういう取組をやっているので、それと比較してどういったメリットがあるのか。

久保田所長）

海外セキュリティ製品に関しては、既に NICT の中にかなり有力なものを導入済みであり、そういったものとの比較はできる。今後売ってくれなくなるかどうかは分からないが、そうならないようにしたい。国内の製品の検証という意味では、国内の会社同士で情報が漏れてしまってはお互いに良くないということもあるので、国内の他社の製品は見られないようなやり方を考える必要があるし、当然そうしていく。CYNEX で検証したことが製品の売りになるようなブランドイメージを作っていきたいと思っている。

鵜飼構成員）

国内のベンダ同士はお互いにファイアウォールを作って競合に情報が漏れないようにすることができるが、海外ベンダからすると海外ベンダの情報だけを手に入れ、国内ベンダの情報は漏らさないというような状況となってしまうので、難しいのではないか。

久保田所長）

やり方としては、例えば NICT の製品のパイロット版を入れていただくとともに NICT に出向などで何人か来ていただき、NICT のキャップをかぶれば NICT で運用している海外製品のアラートが見えるので、そういった比較ができるのではないか。

鵜飼構成員）

キャップを脱いでベンダに戻っても情報の共有ができないため、やりにくいような気がする。先ほどブランドという話があったが、ベンダが最も困っているところはマーケティングで、この一番大きな課題をどうにかできるような取組に結び付けられるかがポイントだと思う。今回の事業はあくまでもテクニカルなところに寄っているが、ブランド化して産業を成長させるということについて具体的なアクションというのはこれからなのか、それ

ともスコープには入っているのか。

久保田所長）

スコープには入っているが、具体的にどうするかというアイデアがあるという段階ではない。

岡村構成員）

中堅企業等でも初心者から段階的にスキルアップができるような階層化というのも、人材育成の考え方としてはあり得るのではないか。

久保田所長）

階層化に関しては、現在でもかなり初歩的なところからやっているところもあるかと思うが、内容に関してはナショナルサイバートレーニングセンターとも検討し、実施していきたい。

安達構成員）

人材育成については異動や配属によって変わるケースが多々ありなかなか定着しない。そのための定期的な情報交換の場や、知識のある人たちと若い人たちが話をするような場もあるのか。

久保田所長）

今は演習授業をするような仕組みで、セキュリティオペレーションをしている人の中で後輩に教えるというのは各企業でやっていただいているが、そういった場が欲しいということか。

安達構成員）

セキュリティについては範囲が広いと考えている。一つのことだけではなくいろいろな知見のある方々が話をできる場があるとスキルも上がっていくと思う。

久保田所長）

CYNEX の人材育成基盤は、人材育成を行っている企業・事業者と連携していくものである。ナショナルサイバートレーニングセンターでは人材育成の受講者のコミュニティについても検討していると聞いているので、そこでそういったニーズも拾っていきたい。

後藤座長）

安達構成員の件は、もう少し広く教育機関等も含めた人材育成の全体の課題として、別件で私が NISC の方でやっている委員会でも考えさせていただきたい。それと、データの共有や活用という点において政府全体の取組として期待したいのは、経産省の IPA や JPCERT/CC も色々な情報を持っており、警察系の JC3、大規模なデータ

ということになると文科省系の NII の次世代のクラウドをどう共有していくかという話もある。そのような中、国全体の役割分担という点をどこかで議論する場が欲しいと考えたので、どこかで議論できればと思う。

辻構成員）

STARDUST のセミオープン化に関して質問をしたい。今までの様々な攻撃を見ていると、政府機関等への情報窃取型の標的型攻撃というものがある。加えて外堀から埋めていくようなサプライチェーン攻撃というもの、例えば MSS 等を狙ってそこから間接的に入ってくるというようなものも珍しくなくなってきており、情報を持っていないといけない範囲が広くなってきている。さらに最近流行っている人が操作をする、いわゆる標的型ランサムといわれるような攻撃、そういったものは業種や業態、規模に関係なく攻撃をしてくる。発表資料の内容にある共同解析する場をオールジャパンでやっていくのは素晴らしく重要だと思うが、そういったところで得られた情報、知見というものを効率的に伝えていく手段というものに関しては何か具体的に検討しているのか。NICTER の情報やブログを出していることは知っているが、それらは本当に必要な人たちに届いているのかが疑問。そういったところのブラッシュアップや、詳しい人のためだけの情報ではなく、ここを見ればこの情報を知ることができるという場を作るということについて検討しているのかを教えてほしい。

久保田所長）

正直なところ、最良なアプローチ方法を考えているかというとアイデアはまだない。まず STARDUST を一緒にやっている仲間内で、隠すところは隠しつつ、できるだけ情報を共有したいと思っている。それをより広く効果的に情報を出していくというのは確かに重要だと思うので、一緒に考えていただきたい。

岡村構成員）

サイバーセキュリティ保険について、果たしてテレワーク時の漏洩までカバーができているのかどうかが保険の形態によって違い、それによるリスクの移転ということも考えられるため、この点についても調べておく必要があるのではないか。

高村参事官）

サイバーセキュリティ保険は、外に情報を持ちだした際、例えば端末の紛失といったトラブルなどに対しどこまで対応できるのかという問題があるため、保険が絶対に安心なものではない。いずれにせよ保険でリスクヘッジはしておくというのはあるが、それに頼りすぎるのも良くない。原則論としては、できるだけシステム上安全となるように管理・運営をしてもらうようガイドラインに記載すべきと考えている。

岡村構成員）

地方自治体においては、個人情報や住民情報の持ち出しにかなり気をつかっており、一度個人情報が漏洩すると巨額の対応費用が必要となる。かといってテレワーク関係の漏洩で、最終的に保険で何とかなるのかというところも企業その他の団体にとっては大変気になることだ。

高村参事官）

テレワークに限った話ではないが、経営者の重要な役割として、セキュリティ脅威と事業影響リスクの特定・整理がある。まずはそれをいかにやるか、それがない状態で保険に全部頼るというのもなかなか難しい。そもそも業務がどうあるべきなのかをきちんと考えてもらえるようメッセージし続けることが重要。

林構成員）

アンケート調査について、「テレワークをやめた」というケースが多々ある点が気になった。理由として、延々と続く会議もありビジネスプロセス・リエンジニアリングをやらずに、今までやってきたことを遠隔でできないかという単純移行のようなケースが多いことが考えられる。それは経営者の自覚とも関係すると思うので、次の調査があればそのあたりを知りたい。

高村参事官）

アンケート調査でも継続していない理由を聞いてはいるが、クロス集計がまだ出来ていないので、詳細が出た段階で皆様に可能な範囲で情報提供をさせていただき、議論、提言等をいただければと考えている。

若江構成員）

実態調査において既に活用をやめたという事業者について気になった。どういった理由でどういった規模の事業者が止めてしまう傾向にあるのかを分析することで、そこに対処できるといった点でもこの調査は重要だと思う。今後その理由等がわかれば共有してほしい。

高村参事官）

一次調査から垣間見えていた雰囲気としては、無理やりテレワークを始めたが、やはり厳しいという事業者がかなりいる気がしている。実際に総務省もテレワークをしているが、業務の進め方がデジタル化していないところが多々あるため、仕事や人材育成に支障が出ている場合もある。いずれにしても、クロス集計が出た段階でご議論させていただきたい。

中尾構成員）

テレワークについては、ICT-ISAC でもテレワークの環境をどのようにセキュアに設定するかという意味でガイドラインを作っているが、総務省のガイドラインは整理されており良かった。第 4 版から第 5 版に改定される際にゼロトラストという項目を追加していたが、具体的にどういう形で行っていくのか。ゼロトラストは認証・認可を受けた利用者やデバイスのみがアプリケーションやデータにアクセスできるようにするという、周りをほとんど信用しないというコンセプトから来ている。基本的には End to End の暗号化だけではなく、認証・認可のプロセスの強化がポイントとなるがそのあたりの説明がなかった。具体的にゼロトラストがどのように組み込まれたのかを教えてほしい。

高村参事官）

例えば、特権管理というシステム管理者権限について最小限の付与やアクセス経路の限定、アカウント認証管理、アクセス制御・認可といったところで、アクセスポリシーの管理において必要最小限としていくということを定めていくといったことが様々なところに記載されている。そのため、具体的にゼロトラストを前提とした項目があるというよりは、個々のパーツの中で方法を提示している。

園田構成員）

前回のガイドラインの修正点から気になって紐解いたところ、偽のアクセスポイントについて触れられている部分が薄いように感じた。その点を改めて具体的な事例として触れてほしい。また、エンドユーザーに対してどのように教えていくかという整理も必要ではないか。

小山構成員）

NTT コミュニケーションズの社員がテレワーク前後でどう変わっていったかという点をインシデント未満のヒヤリハット等で見ていくと、色々なことが起こっている。例えば、飛行機の緊急時のガイダンスのように講習会等をくどいほど見せなければ、自分がいざ標的型攻撃メールを踏んでしまった時に頭が真っ白になってしまい、どうして良いか分からないという事例もある。そういったことも踏まえて、教育という面についてスポットを当て、日本の企業の大多数が参考になるような２～３分のビデオのようなものをガイドラインの付録に付けて共有できるというようなことができればありがたい。

高村参事官）

園田構成員の偽装アクセスポイントについては、公衆無線 LAN に関するトラブル事例のような形で別途記載しているところである。ただ、事例はありすぎると読んでもらえないというところが有るため、ある程度絞り込んでいる。事例集は別途章立てで分けており、アップデート等は容易に可能なので、足りないもの、広く知らしめていくべきものが有れば御指摘いただけるとありがたい。一般従業員に向けた教育については、テレワークを始める人に対してフルパッケージのセキュリティポリシーを投げつけたところで読んでくれるのかという問題は別途ある。テレワークだから大事になっている部分と、テレワークに関係なく大事なことが多々あり、そういった点も含んでテレワークのガイドラインで言及してしまうとテレワークを止めようという方向になってしまうため、その塩梅が難しい。どちらかというとテレワークだからこそ気を付けるべき点を強調して記載している。

名和構成員）

経営層の積極的な関与について、なぜセキュリティガイドラインが必要なのかについて根拠が薄いように感じた。経営層が納得のいく根拠や理由を記述した方がよいのではないか。

高村参事官）

今回はシステム・セキュリティ管理者が責任を問われた際の反論根拠になるようにという思いで記載している。

テレワークセキュリティガイドラインに限った話ではないが、サイバーセキュリティ全体として、経営者が最も重要であるというところは別途繰り返し伝えて行く必要がある。

鵜飼構成員）

こういったガイドラインが中小企業でサイバーセキュリティ担当がいないところの拠り所になる。一方で、中小企業などにどう普及させるのかがポイントとなる。対象が重要インフラや大企業であればサイバーセキュリティ部門の人たちのアンテナが高くガイドラインを積極的に取り入れてくれるが、中小企業は自ら情報収集をしないため、中小企業向けに広く知らしめることがポイントとなる。そのための施策があれば教えてほしい。アイデアとしては中小企業に関連しているディストリビュータ等を巻き込んでガイドラインを普及できれば有用だと思う。

高村参事官）

中小企業に対してどうリーチするのかは本当に難しい。政府のテレワーク普及のための助成金や補助金の枠組に乗じて広めていくということも当然必要であろう。今回の話に直接的に関わるわけではないが、NOTICE をやっている中で、アラートの発出先が VPN 装置であるケースが増えており、そこの経路をたどる中で VPN ルータがどのように流通してお客様のところに行くのかが少しずつ分かるようになってきた。ここで得られたルートも活用しながらガイドラインを広めていきたい。またこういったガイドライン類は WEB サイトに置いておくだけでは広がらない。今回のガイドラインや手引きはなるべく印刷物にしてチャンスがあれば配付するような取組も進めて行きたい。

徳田構成員）

経営者の役割という部分をまとめていただいたことを評価する。経営者目線からすると、コロナ禍で仕方なくテレワークを導入したという人もいるため、テレワークにすると得られるビジネス上のメリットをいくつかストーリー的に見えると経営者が読みたいと感じると思う。今のロジックではセキュリティファーストで始まってしまっており経営者的には読む気が起きないため、もう少し働き方改革などのメリットが書かれていても良いのではないか。また、例えば中小企業がランサムウェアにどう対処するのか等、トラブルが起きてしまった時の問い合わせ先に関しての配慮はあるのか。

高村参事官）

テレワーク導入に向けたガイドラインは、厚労省も含めて「情報通信技術を利用した事業所外勤務の適切な導入及び実施のためのガイドライン」という、助成金や雇用契約等も含んだより大きな形のものがある。今回はテレワークにおけるセキュリティの部分に限定しており、一般の経営者になじみのある話とは別の話として作成している点について、ご理解いただきたい。トラブルについては正直ガイドライン的には手に負えない部分があるため、本来であればシステム管理会社に電話してもらうしかない。できれば付録のような形で連絡シートのようなものを作った方が良いとも思うが、それは個々の会社にやっていただくしかなく、総論でまとめられるものではないため具体的な話は難しいと考えている。

小山構成員）

届いたメールに書いてあることを本当に実行してしまう人がリモートワークだと出てきてしまっている。隣の人に気軽に質問や相談ができない環境が、詐欺グループや犯罪グループの活動の場を与えることになってしまうことが考えられる。

安達構成員）

資料の中にテレワーク方式のフローチャートがあったが、業務によっては個人でフローチャートの方式の組み合わせを実施している場合もある。VPN を導入しているといったセキュリティレベルの高いパターンは良いが、そうではないところでテレワークに移行した際に個々の知識レベルに依存するため、従業員全体のセキュリティ教育とセットになる。放送局の場合はどうしてもテレワークにならない業務や、テレワーク移行の設備投資までの時間の中で、テレワークを想定に入れたセキュリティ対策が必要になってくると感じた。

高村参事官）

実際の業務システムを突き詰めていった場合、全社的に方式を一つ選ぶということにはなりにくいというのは感じている。ただ、個々の事情まで斟酌してしまうとガイドラインとしてまとめられないのでご容赦いただきたい。安達構成員の話を聞いて思ったことが、現場として LAN に閉じない仕事があるケースというのは、その段階で他の業務とは切り離されたテレワークの仕組みが存在する必要がある。ここまで半年間やってきて、これまでオフィスにあるものを外に引っ張るという前提で進めてきたが、そもそも中で働くことを想定してない人達向けのテレワークというケースもあることから、在宅勤務やサテライトオフィス、モバイル勤務のような形からさらに踏み込んだ形で、テレワークという観点を広く捉える必要があると感じた。

後藤座長）

各省庁から役割分担で様々なガイドラインが出ているとあったが、どこにどういう観点のガイドラインが出ているかのマップがあると良いと思った。昨今では副業問題とテレワークの関係や clubhouse での会話に企業秘密の漏洩が多いと聞くので、どこに何があるかのマップがあると分かりやすいと思った。

高村参事官）

テレワーク全体のマップは「テレワーク総合ポータルサイト」という厚労省のサイトにある。働き方に関することのため、一番大きなところとしては厚労省のサイトにあり、総務省をはじめ関連省庁のテレワークに関する資料が掲載されている。

以上