情報通信審議会　情報通信政策部会
総合政策委員会（第２回）議事録

第１　開催日時及び場所

令和３年１１月１９日(金)　１６：００～１８：００

於、ウェブ開催

第２　出席した構成員（敬称略）

森川　博之（主査)、三友　仁志（主査代理)、江﨑　浩、大橋　弘、
桑津　浩太郎、根本　直子、増田　悦子、山中　しのぶ、岩浪　剛太、
鈴木　一人、手塚　悟

第３　出席した関係職員

（１）総務省

(国際戦略局)

大森　一顕（国際戦略課長）

新田　隆夫（技術政策課長）

(情報流通行政局)

飯倉　主税（放送政策課長）

高田　義久（郵政行政部企画課長）

(総合通信基盤局)

木村　公彦（電気通信事業部事業政策課長）

荻原　直彦（電波部電波政策課長）

(サイバーセキュリティ統括官室)

梅村　研（参事官（総括担当))

(情報通信政策研究所)

高地　圭輔（所長）

（２）事務局

竹村　晃一（官房総括審議官）

辺見　聡（官房審議官）

大村　真一（情報通信政策課長）

西潟　暢央（情報通信政策課企画官）

西村　邦太（情報通信政策課統括補佐）

第４　議題

（１）「2030年頃を見据えた情報通信政策の在り方」について【令和３年９月30日付け 諮問第26号】

（２）その他

開会

○田熊係長　本日はお忙しい中御出席いただきまして、誠にありがとうございます。委員会開催に先立ちまして、事務局から御案内をさせていただきます。

本日はオンライン会議となりますので、進行を円滑に行うため、御発言を希望される方はチャット機能により御発言がある旨をお知らせください。主査から御指名がございましたら、マイクとカメラをオンにしていただき、お話しください。その際、参加されている皆様が発言者を把握できるようにするため、御発言いただく際には、冒頭にお名前をお伝えいただきますようお願いいたします。

また、ハウリングなどの防止のため、発言時以外はマイクとカメラをオフにしていただきますよう、併せてお願いいたします。

なお、音声がつながらなくなった場合には、チャットでお知らせいただければと思います。

それでは､以後の議事進行につきましては､森川主査からよろしくお願いいたします。

○森川主査　承知しました。主査の森川です。本日もお忙しい中、先生方、お集まりいただきまして、ありがとうございます。ただいまより第２回の総合政策委員会を開催いたします。

本日は１３名中１１名に御出席いただいております。

議事

（１）「2030年頃を見据えた情報通信政策の在り方」について

○森川主査　それでは、議題に移りたいと思いますが、まず、資料につきましては、委員の皆様におかれましては、事務局から送付されたメールの添付資料を御覧いただき、傍聴の皆様に関しましては、事務局からのメールに記載された総務省ウェブページのＵＲＬから御覧いただければと思います。よろしいですか。ありがとうございます。

本日の議題は、お手元にございますとおり、令和３年９月３０日付諮問第２６号「２０３０年頃を見据えた情報通信政策の在り方」についてとなります。

本日は、鈴木専門委員と手塚専門委員から、それぞれ話題提供をいただきます。その後、事務局から第１回会合の概要を御紹介いただきます。残り１時間程度でフリーディスカッションをさせていただければと思いますので、ぜひ、委員の皆様から、いろいろな御視点からの御意見をいただければと思っております。よろしくお願いいたします。

それでは、まず鈴木専門委員から御説明をお願いできますでしょうか。よろしくお願いいたします。

○鈴木専門委員　ありがとうございます。

トップバッターで話題提供として意見表明をさせていただくことになりました。私は経済安全保障を専門としておりますので、それを踏まえてお話をさせていただければと考えております。私は、国際政治の中でも、近年、大きな話題になっています経済安全保障をテーマに、情報インフラの問題についても考えているところですが、経済安全保障とは何かについて考えを述べた上で、情報通信インフラの問題がどのように関係するのかということについてお話をさせていただきたいと思っております。

前回の資料の最後のほうに参考で骨太の方針にも書かれている経済安全保障の部分について言及されており、その中でも基幹インフラの維持がテーマとして挙げられていたかと思います。また、新しく岸田政権の下で経済安全保障担当大臣となられた小林大臣が関わっていらっしゃる経済安全保障一括推進法案という法案があるわけですが、ここでは４つの柱ということで、基幹インフラの維持のほか、技術基盤の維持・発展、非公開特許、クリティカルな産品のサプライチェーンの強靭化を軸に検討が進められています。その中で、情報通信と関連があるのは重要インフラの基盤維持・強化ということになると思っています。

自民党や政府が掲げる経済安全保障は、少し整理をしてあげないと概念としては分かりにくいところがあります。経済安全保障がなぜ今問題になっているのかが実はあまり明らかになっていないので、それをお話しさせていただくと、１つには、政治と経済が接合しながら分断している状態というのが、今、起きています。一方では、第二次大戦後、自由貿易体制、ＧＡＴＴ＝ＩＭＦ体制が発達して、１９９５年にマラケシュ協定ができてＷＴＯに結びつくわけですが、世界的な貿易が自由貿易になっていくということの本質的な意味は何かというと、資本の移動の自由がどんどん加速化し、国際的な分業というのが進んでいくということです。これは簡単に言うと、生産の最適化というのが行われて、例えば、生産のコストや法制度、税率などのいろんな条件が重なる中で、それぞれの製品が１つのところで作られるのではなくて、世界中様々なところで作られて、それがあるところに集められ、組み立てられて最終製品になって輸出されるという、国際的な分業というのが非常に広まっています。それがさらにＴＰＰのような自由貿易制度が発達することによって国境を行き来するものの関税というのがどんどん低まっていったことで、こうしたグローバルなサプライチェーン、分業体制というのが確立しました。

その中で、日本やアメリカ、多くの国がサプライチェーンの中に中国を取り込む格好になったというのが一番大きな問題で、中国は、言ってしまえば１つの世界市場の大きな一部になっているわけですけれども、その大きな一部が今、アメリカや日本と安全保障も含めて緊張関係にあるわけで、言うなれば、経済は既に完全に一体化してつながっているにもかかわらず、上部構造である政治の一部ではギャップが生じている関係にあるわけです。かつての冷戦のように、経済も政治も軍事も全く２つの陣営に分かれているうちはそんなに心配することのなかった安全保障における経済的な問題というのを考えなければいけなくなったというのが現状になるかと思います。

こうした構造の中で経済安全保障を考えると、実は３つ大きなポイントがあると思っていまして、１つは供給の安全保障です。これはかなり重視されていますけれども、例えば半導体を作るにしても、マスクを作るにしても、いろんな物の流れがグローバルに結びついているがゆえに、互いのチョークポイントを握っている状態にあります。かつては世界中で最も効率のいい生産体制を各国がつくっていこうとした。その結果、ある国に比較優位が集まって、そして比較優位上、この国でこの物を作るというのが最適化される。となると、その国が世界シェアのかなり大きなパーセンテージを取るようにな

って、そういった世界的なシェアを持つ国は、自動的に、国際社会においてある種のパワーを持つことになる。つまり、この国家が国内で生産される財の輸出を止めるという権限を持つので、それを行った場合、ほかの国がみんな困る状況になるわけです。こうした国際社会におけるある種の生産の集中、寡占化が、結果として政治的なレバレッジとして機能する状態が起きている。これをチョークポイントといいますが、ある物を作るプロセスの中で、材料から部品、部品から完成品というふうにどんどんとつながっていくサプライチェーンの中で、どこかの国が集中してある特定の部品を作る（例えば、半導体などを集中的に作る）ことになって、この国がそれを輸出することをやめれば、このサプライチェーン全体が止まる。言ってしまえば、ほかの国を困らせるために、経済的な手段を使って相手に大きな損害を与えることができる。軍事的な手段ではないものの、貿易を武器化することで他国に対して圧力をかけることで経済的な強制力を持つことになる。だから供給の安定化というのが非常に重要になる。経済的な強制力をいかに回避するかは、簡単に言うと、ある特定の国に依存しないようにすることや、特定の品目が寡占化されていたとしても自国で生産していくのが解決策になっていきます。ただし、これは経済的に合理的でない場合もあるので、高いコストを払ってでもそうしたリスクを回避するという選択を政治的にすることになるわけで、５Ｇや半導体の話でもそうですが、情報通信に関しても、多少コストがかかったとしても、やはり一つのところに集中させるのは危険だから、国内のリスク分散のために、例えば、データセンターをいろんなところに置くなどといったことをしていかなければならないということになります。

もう一つが技術の不拡散の問題ということで、技術は、ある特定の国に集中しがちであるが、その技術が貿易等を通じて技術が拡散していくことで、その国の技術的な優位性が失われることがあります。技術の多くは軍民両用の技術であって、例えば、現在注目されている技術でいうとＡＩやデータ分析に関してですが、これらは軍事的に転用可能な技術であり、これらの技術を通常の経済活動として輸出することを通じて、軍事的な優位まで失う可能性がある。そういうことに対する意識を持たなければならないということで、技術不拡散というのが経済安全保障の枠組みの中に入ってきます。これは今議論されている中では非公開特許などが該当すると思います。

もう一つ、経済安全保障の問題で少し大きな問題になっているのが、他国の規制からの安全保障という問題で、他国の規制は自分たちでコントロールできない。アメリカだ

と、グローバルマグニツキー法と言われる人権問題に対して制裁を科す法律がありますし、また、例えば、イランの核制裁、核合意からアメリカが離脱した後制裁をかけていますが、このようなアメリカの一方的な行為が、域外適用、つまり日本の企業にも適用され、影響を及ぼすようになってくる。つまり、自国では関係していない、自国の問題ではないにもかかわらず、それが経済的な損害を生じさせる結果になっているということで、自国の規制を域外にも適用することによって他国の行動をコントロールしようとする動きにどう対処していくのか、そういうことも経済安全保障の枠組みに入ってくるのではないかと思いますが、これは現在、経済安全保障推進法案の中では、あまり議論されていないことであります。

ポイントになるのは「依存」です。依存というのは、裏返すと脆弱性ということになるわけですが、経済安全保障の鍵となるのは、やはりこの依存です。特定の国、例えば中国に特定の品目を依存している状態というのは、その国に脆弱性をもたらすということで、こうした脆弱性を狙い撃ちにする「Economic Statecraft」（経済的な手段を用いて地政学的な国益を追求する政策）が行われています。

典型的な例が２０１０年のレアアースを日本に輸出することを止めた件です。これは尖閣諸島をめぐる問題で、当時、日本の海上保安庁がつかまえた船長の釈放という政治的な目的のために中国はレアアースの輸出停止という手段を使って日本に経済的な圧力をかけたわけです。こうした特定の品目で日本は中国に依存していたわけです。レアアースはハイブリッド車の磁石に使われているものですが、こうした特定の品目を依存していることによって、政治的な圧力をかけられる脆弱性が存在していたということで、例えば、しばしばマスクの話なんかも出てきますが、マスクのような誰でも作れる汎用品はあまりレバレッジにならないわけです。マスクの場合は中国が寡占的に生産をしていたので懸念されたわけですが、こうした独占、寡占の状態であることと、それに依存していることが脆弱性となり得ます。マスクのようなものは頑張れば日本でも作れますけれども、レアアースは頑張っても作れないので、そうなると脆弱性が残ることになるわけです。その脆弱性を回避する手段としては、例えば、備蓄や、供給源の多元化が挙げられます。レアアースの場合、全てではないですが、例えばカナダやオーストラリアなどからも供給を受ける。また、レアアースのケースで見られるように、中国からのレアアースを使わない代替品を作るといったことも１つの方法としてあると思います。

この脆弱性を回避するためには、最終的に、信頼できる相手、同盟国や友好国との取

引を増やし、敵対的な国家との取引を減らしていくということが１つの方法になると思います。

５Ｇの話が経済安全保障の文脈でよく議論されるのですが、これも結構誤解があるようなので、少し整理してみますと、５Ｇは、まず技術的な覇権をめぐる問題ではないということが言えると思います。高度な技術を使っていますが、５Ｇの技術そのものは日本だけでもなく、アメリカだけでもなく、ヨーロッパだけでもなく、中国だけでもない。つまり、いろんな国に既にあるわけで、むしろ５Ｇが問題になってくるのは、ファーウェイ等の中国製品が非常に競争力を持っているということだと思います。つまり、競争力があるのでマーケットシェアを取っている。そして、安くていいものを提供している中国製品に依存しなければいけないという状態が安全保障上のリスクであると考えるから、ファーウェイを排除する、中国製品を排除するという法律が、先日、アメリカで決まったわけですけれども、こういうことが起きていくのは、言ってしまえば、主要な重要なインフラを他国の製品に依存するということはリスクが伴うという考え方に基づくものであるわけです。

しかし、ここも重要なポイントですが、アメリカはファーウェイや中国製品を５Ｇの構築から排除しても、アメリカ製品で代替することができないわけです。アメリカでこうした５Ｇのインフラを整える事業をやっている会社がないので、結果的にＮＥＣやノキア、エリクソンといった外国の企業に発注する形になるわけですが、これは友好国、同盟国からの製品のほうが安心できるという、非常に主観的な安全保障上の観点から、こうした選択をしているのだろうと思います。

こうした他国の製品に依存するリスクというのは、結局、何が問題かというと、安くていいものであるファーウェイの製品を使い続けるというのは経済的に合理的な行動なわけですけれども、同時にそれをやるということは、安全保障上の合理性とは必ずしも一致しないということが問題になるわけで、経済安全保障というのは、まさにこうした経済合理性を取るか、それとも安全保障上のリスクを取るかということになるわけです。安全保障上のリスクを減らす選択をするのであれば、どのくらいのコストをかけて５Ｇを整備するのかが問題になるわけで、アメリカはそこで、高くてもいいから例えば日本のＮＥＣのものを買うと言って、今どんどん買っているわけです。それは日本の産業にとってはいいことですが、アメリカの５Ｇの利用者から見ると、その分のコストが利用料金に跳ね返ってきたりするので、必ずしもいいことだけではないわけです。それ

でも、やはり安全保障上のリスクを回避するためには、それだけのコストをかけなければならないと考える。逆に言うと、選択肢として５Ｇを整備しないという選択肢もあるわけですが、そんなことをすると、結局、例えば、Ｓｏｃｉｅｔｙ５．０の実現のための基礎的なインフラの整備が遅れていくわけで、Ｓｏｃｉｅｔｙ５．０を実現するために、これだけのコストをかけるべきだとポジティブに考えていく捉え方もあると思います。

という話をしていきますと、結局、経済安全保障と通信インフラの問題は、主観的なものでもあるわけですが、安全保障上のリスクをどのくらい多く見積もるかということと、それにどのくらいのコストをかけるべきなのかというバランスの中で、最終的な便益の確保を目指していく。場合によっては、リスクを取りたくなくコストも払いたくないから諦めるという選択肢、これは途上国ではしばしば取られる選択ですけれども、そういうことをやるか、それとも、中国の製品を使うことによってリスクはあるかもしれないが、中国の製品を使ったところで今まで何か困ったことがどのくらいあったのかと考えると、多少のリスクは受容可能であろうということで、リスクよりもコストを重視して中国の製品を買うという選択もあり得ます。逆にアメリカのように、中国製品は安全保障上望ましくないので、リスクを重視し、高いコストをかけて同盟国や友好国の製品を買うというような選択もあるというバランスの中で決められていくことになると考えています。

ということで、時間になりましたので、私の話はここで終わりにしたいと思います。

また後ほど、いろいろと御議論いただければと思います。

○森川主査　鈴木専門委員、ありがとうございました。

それでは、続きまして、手塚専門委員から御説明お願いできますか。

○手塚専門委員　はい。それでは、今回の話題提供として、デジタル分野について、私のほうから御説明させていただきたいと思います。

目次にありますように、今後の社会において「バイ・デフォルト」というのをどのように考えるのか、こういう情報通信の分野においてはどうなのかという視点。２０３０年を目指していく中で、今後の社会構造のバイ・デフォルトをどういう形に持っていくのかというのが１つ大きなテーマになると考えました。

１つは「デジタル・バイ・デフォルト」ということで、今、デジタルという言葉はさかんに言われていますが、実際のところはまだ紙の文化が中心で、これは特に法制度が一番遅れていると思うのですが、「原本は紙」が基本にあって、世の中では、いくらデジ

タル化しても、最後は紙だということで、その紙の出力に頼るためになかなかオールデジタル化につながっていかないということが言えると思います。

そういうことから、１つは「通用性」という概念の中で、電子文書を広く利用するため、例えば、法令上の交付、保存、提出における電子文書の有効性をしっかり定めていくことが大事です。それと、民ー民間の取引における有効性についても、電子的だという理由で効力を否定することはできないという考え方で、デフォルトはデジタルであり、ペーパーではないという考え方を推し進める必要があると思っています。

こういうことを進めていくと、もう一つ、システムアーキテクチャー的な概念が必要になる。そうなってきますと、「クラウド・バイ・デフォルト」ということがもう一つ重要だと思っています。この辺につきましては、政府の「世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画」（令和２年７月１７日閣議決定）等でも記載されておりまして、クラウド・バイ・デフォルト原則、すなわち情報通信システムを整備する際にはクラウドサービスの利用を第１候補とするということで、こういうことからデジタルガバメントの実行計画等でもガバメントクラウドの話が出てきています。この辺を日本としてどれだけしっかりと構築していくかが大事になる。

特にアメリカなどを見ると、ＦｅｄＲＡＭＰの世界でしっかりとしたクラウド環境が整備されますので、この辺を我が国としてもしっかりと環境整備していく必要がある。これには結構時間かかると思います。５年ぐらいはすぐ経ってしまう。ですから、２０３０年度にクラウドがバイ・デフォルトである状態にするにはどうするか、そのための政策という点をよくよく考えていかないといけないということで、この２つのデジタル・バイ・デフォルトとクラウド・バイ・デフォルトが今後の非常に重要なポイントになると考えております。

続いて、トラストについて、今、私がどういうふうに考えているかということをお示ししたいと思います。

視点としては、トラストの対象としては①社会保障、②安全保障、③国際相互連携、こういうポイントでお話しさせてもらいたいと思います。

まず、社会保障ですけれども、世界を見たときに、この辺を非常に強く打ち出しているのがＥＵだと言えます。特にＥＵでは、資料にありますeIDAS Regulationでトラスト関連の法律が整備されてきておりまして、ＥＵの２７か国の中でデジタルシングルマーケットを確立するためにやっている。つまり、我が国においても、我が国の中でのデジ

タルシングルマーケットという概念を作っていく必要があると思っています。

ＥＵの事例を調べたりして見ていきますと、法体系の上では、資料にあるような電子署名や電子シール、電子タイムスタンプ、電子書留送付サービス、ウェブサイト認証等々、通信インフラの上のミドルウエアのレイヤーでのトラストをどのように構築していくのか、それを社会基盤としてどのように提供するか。それらを法制度とリンクした形で整備していくことがパブリックトラストの実現ということ点で非常に重要だと思っています。プライベートトラストであれば様々なところでやっていますが、これをパブリックな世界でやるにはどうするかという視点、これは１つ大きなポイントだと思っています。

その考え方として、先ほど挙げていた法律に基づいたサービス群（トラストサービス）と、それを活用するアプリケーション群（トラストアプリケーションサービス）という２階層モデルで、この場では議論が出ております。

続いて、もう一つ重要なことは認定制度であり、この辺の法整備もしっかりとやっていく必要があります。我が国にも国家監督機関のようなものを置いて、適合性評価機関がトラストサービスプロバイダーなどを認定していくということで、パブリックなトラストを整備・確立していくという考え方でございます。

この辺を我が国として、２０３０年度に向かって、どのように整備していくか。特に通信インフラですと、様々な通信機器が影響していくわけです。ＩｏＴ機器などもこういう概念に入ってくると考えております。

続いて安全保障の視点です。

安全保障は、先ほど鈴木専門委員からもお話があったように、日本では経済安全保障の切り口で見ますが、アメリカでは軍事的なところを含めた安全保障がかなり色濃く出てきています。資料Ｐ．１１はグローバルサプライチェーンの絵を描いておりまして、アメリカはもう、資料の赤いポイントをトラストアンカー、またはルートオブトラストとして、世界各国のエンティティーを巻き込んだ安全保障の仕掛けをつくっています。言わずもがな日本の企業もこの傘下に入るという構造が取られています。この図は軍需産業を描いているものなので、日本とアメリカの非対称性が激しいのはこの分野ではやむを得ないと思います。しかし、私としては、通信分野、電力分野、鉄道分野、自動車分野等は日本が強い産業で、このような分野については、日本がトラストアンカーになる構造が実現されていかないといけないと考えておりまして、そういう構造をどうやっ

てつくり上げていくのかというのが大事だと思っています。

そのときに、データのClassification、データの分類をどうやっていくのかということが１つ考え方として大事なポイントで、アメリカでは大統領令１３５２６というのがございまして、そこでデータの分類学についてきちんと規定されております。資料の下にありますように、その内容に従って、Classified information とUnclassified informationというデータの分類があり、Classified informationについては、基本的にはアメリカではアメリカの市民の資格を持っていないと一切触ることができない。我々がアメリカへ行って議論しても、この分野はタッチできないということです。そういう厳格な安全保障を含めたデータの分類学がしっかりとできている。そこにさらにＣＵＩ（Controlled Unclassified Information）という概念も出てきておりますが、こういうデータの分類をちゃんとしないといけないということでございます。

それと、アメリカでは、これらのデータにアクセスできる人の分類もしっかりとやっていて、セキュリティクリアランスの問題についても大統領令で整理されています。

これにおいては、日本では国家公務員等の専用のカードというものはまだないわけですけど、アメリカはＰＩＶカード（ＰＩＶ：Personal Identity Verification）というものがございまして、これを使ってすべての政府職員は様々な形で情報へのアクセスがコントロールされているということでございます。

それに加えて、ＰＩＶ－Ｉカードというインターオペラブルなものがございまして、これは政府のコントラクターである民間人が発行してもらうことになっております。

資料Ｐ．１３の下のカードを見ますと、実はこれ、マイナンバーカードと非常に似ています。似ているというよりも、テクノロジーは同じものを使っています。アメリカがすごいのは、さらに暗号化のテクノロジーも、ＰＫＩ（パブリックキーインフラストラクチャー）のＸ．５０９の世界でやっていますので、完全に日本のマイナンバーカードと同じアーキテクチャー、テクノロジーを使っているのですが、さらに暗号化がされていまして、Ｓ／ＭＩＭＥと言うと分かるかもしれませんが、メールの暗号化をもう既に実現していて、政府内の方たちでは全部それで情報のやり取りをしている。そうすることでＡＴＰ攻撃のようなことが回避できるわけです。

アメリカ政府を大きな１つの会社のように見ると、この政府という組織に対して、しっかりと安全保障の視点が取り入れられている。セキュリティクリアランスですから、まさにそのクリアランスをしっかりとやって、こういう環境をつくり上げているという

ことです。

それに対する認証局のトポロジーですが、既にこういう巨大なトポロジーが出来上がっていまして、資料にＰＩＶと書いてあるのは各省庁の認証局で、そこから省庁ごとの職員に全部ＰＩＶカードが発行されている。ＰＩＶ－Ｉカードは民間側の認証局から発行して、これでなりすましや改ざんのない世界をつくり上げているということです。

驚いたことに、ここにオーストラリアの「Australian Defense Organization」と書いてありまして、実は、これ以外の資料も調べたところ、イギリスも入っている。つまりファイブアイズは安全保障のレベルでもこういう環境をつくり上げているということがございまして、こういう点で我が国の社会保障と安全保障におけるこうした部分をどうやって整備していくのか、これを旗振るのは一体どこなのか。その基盤は全部情報通信インフラですから、ここはしっかりと総務省の下でクリップしながら見ていく場所なのだと私は捉えています。

続いて、国際相互連携について、少しお話しさせてもらいます。

先ほどファイブアイズなどは米国政府とつながっているという話がありました。それと、社会保障では、ｅＩＤＡＳがあり、やはりアメリカやＥＵと相互連携していかないといけないということになりまして、日本においてもトラストの部分をしっかりとやっていく必要があります。今、デジタルトレードという点では、日ＥＵ間でＥＰＡが締結され、アメリカとの間でもＦＴＡが締結され、この２０２１年の１月には英国ともＦＴＡを批准したという流れができておりまして、日本である契約をするものでアメリカも契約をするもの、これを電子レベルで契約する、デジタルの世界で全てやり上げる（ＤＸ）とすればどういうことが必要になるのか。２０３０年頃にはワールドワイドにデジタルで全てやり上げることが普通の行為、つまりデジタル・バイ・デフォルトの概念でいくと、こういうことが必要なことになるわけです。実は、日ＥＵ間でデジタルトレードを批准するときのコミュニケの中に、エレクトリックオーセンティケーション、エレクトリックシグネチャーという具体的なテクノロジーが書かれています。ですから、テクノロジーサイドでいうと、かなり標準もあり、やれてきているのですが、問題はポリシーサイドで、こちらのほうをどうやって整備していくか、国家間におけるイコールフッティングをどういうふうにつくるのかというところが次のフェーズとしては非常に重要で、２０３０年ぐらいにそういうところを目指すというのは、当然やっていかなければいけない。やらないと、こういう相互承認（Mutual Recognition）ができないとい

うことになるわけです。

アメリカにおいても、資料を見ると、日本とアメリカでやったときに同じことが書かれています。ですから、テクノロジーから見ると、まさにそこを整備し、今度、法制度のほうも、こういうところをきちっとまとめていくということが大事だと思います。

それをＤＦＦＴの議論の流れの中でまとめますと、私としては、資料Ｐ．１９のようなイメージを持っています。トラストサービスプラットフォーム、その上にトラストデータ流通基盤、それとトラストアプリケーションサービスという３層構造です。ライクマインデッドカントリーの概念も組み合わせてワールドワイドに見ますと、日本、ヨーロッパ、アメリカといった中心的な経済圏で考えるとこういう格好になる。

資料の一番下のトラストサービス基盤を相互承認しないといけない。概念的にはこういう絵を描いて、しっかりと整備していく必要がある。

先ほどアメリカの絵はお見せしました。非常にたくさんのトポロジーの中で認証局がある。ＥＵはＥＵで２７か国が相互承認する仕掛けができ上がっています。じゃあ、我が国はどうかということで、この我が国とアメリカ、我が国とＥＵ、こういうところをクロスサーティフィケーションする仕掛け、こういうものをデジタルの世界では整備していくという、これは情報通信インフラと併せて、セットで考えていかないといけないと思います。

１つの例でいいますと、自動車のエレクトリックコントロールユニット（ＥＣＵ）の一つ一つにテクノロジーでいうと鍵のようなものが入ってＩｏＴ機器になっています。自動車そのものを１つのＩｏＴ機器として見ると、自動車会社がそれをトラストサービスの一番のプラットフォームのところで鍵配送して、それによって相互承認していく。つまりトヨタや日産、ホンダがルート認証局の下で鍵を自分の自動車に組み込むルートになっていますから、それを相互承認しないといけないわけです。ヨーロッパのドイツの車もそういう状態です。それらが相互認証していないと、ＩＴＳ上で走るときに、制御するところが相互認証できないわけです。そういうようなことが２０２５年以降、３０年ぐらいに向かってきちっと整備されていかないと、自動走行などにも影響が出る。自動車分野以外の分野でも、いろいろな相互認証するということによる影響が出てくるということになります。こういうことを私としてはデジタル分野というところで、我が国として、しっかりとやっていくということがデジタル安全保障、デジタル社会保障において必要で、トラストというところを絡めてやっていくということが重要だと考えて

おります。

以上です。

○森川主査　手塚専門委員、ありがとうございました。

それでは、事務局から説明をお願いできますか。

○西潟企画官　事務局でございます。鈴木専門委員、それから手塚専門委員、話題提供をありがとうございました。

先ほど主査からご紹介いただきましたけれども、今後のフリーディスカッションに入る前に、前回での御議論を思い出していただくのを含めて、資料の２－３にまとめております。

柱立てとして見やすくするということもありまして５つほど柱を立てておりますけれども、あくまで便宜上のものであって、今後の議論の幅がこれにとどまるとかそういうことでは決してなくて、むしろこの柱をどんどん増やしていただく、そういった方向で御審議を進めていただければ大変ありがたく存じます。

では、早速入りますけれども、総論といたしまして、これまでの議論の転換やその候補、あるいはその切り口として、例えば、脱炭素化や人権への配慮、ＳＤＧｓ、ＥＳＧといったものをどういう形で成長戦略に結びつけていくのか等の御指摘をいただきました。

それから、情報通信インフラの部分につきましては、私のほうからもブロードバンドの整備状況を御紹介いたしましたけれども、このインフラを、もっと使う、付加価値を出していくという方向にどうやって活用していくのか、あるいは伝送インフラからデータ、電気通信事業者からＯＴＴの事業者へと目線を少しシフトしていく必要もあるのではないかという御指摘もございました。

それから、宙のインフラ、宇宙のことにつきましても、例えば、トラストやグローバルコンセンサスの構築に当たっての貢献といったような日本からも発信できるものがあるのではないかという御指摘がございました。

次のページに移りまして、情報通信産業の自律性ということで括っております。

前回の会合､あるいはその前の総会､部会でも御指摘をいただいておりますけれども、情報通信分野の経済安全保障の議論が必ずしも国産優先、国産誘導に閉じたとすべきではないというご指摘がございました。経済成長については、人口動態を踏まえると、アメリカや中国同様の成長率は期待できない中では、国際競争力を持つ製品の開発に投資

をして、海外展開までの取組をシームレスに展開していくべきではないかという御指摘がございました。

それから、私どもからＩＣＴ産業の輸入超過についてもデータで御紹介いたしましたが、国内供給が需要を満たしていない部分があるのではないか、その意味で付加価値の高いサービスの提供に向けた取組が強化されるべきではないか、それがひいては情報通信産業全体の成長につながるのではないかということでございました。

それから、今日、鈴木専門委員から話題提供いただきましたけれども、ハードウエアとサービスに分けたときに、経済安全保障の観点からはそれぞれ見るべきところが違うということがございまして、ハードウエアの場合は、最終製品が作られるプロセス全体の中でサプライチェーンの中での経済安全保障上のリスクを検証することが必要です。他方でサービスにつきましては、特に現在の市場の状況を踏まえますとクラウドサービスの安全性の確保が１つ急務なポイントになっていくのではないかとのご指摘がございました。

おめくりいただきまして、中国の成長を脅威と捉える向きがある一方で、アメリカが特にＩＣＴに関して重要な部分で高いシェアを維持していることもございますので、特にアメリカとどのように組んでいくのかという点について議論したほうがいいのではないかとのご指摘がありました。それから、その裏返しの部分でございますけれども、一定の分野においては、ある程度「国産」という形で一通り供給できる体制が確保されているべきではないか、それがではどの分野に適用されるべきなのかについて議論していく必要があるというご指摘がございました。

続きまして、デジタルトラストにつきまして、本日、手塚専門委員から話題提供のインプットをいただいておりますが、欧州との相互連携あるいはイコールフッティングについて御指摘がございました。それからサイバーセキュリティと通信の秘密の関係についても法律によってきちんと整備していく必要があるのではないかとのご指摘もございました。

最後のページになります。デジタルの受容促進ということで、国民のＩＴリテラシーの底上げが急務であること、情報のアクセスについてはまだまだ改善の余地があること、バーチャルとリアルを融合していくという意味ではさらなる技術革新が必要であること、社会課題の解決やそのための社会貢献の部分についてはもっと場づくりといったものが必要ではないかという御指摘をいただいております。

それから、デジタル・バイ・デフォルトの徹底ですとか、情報通信分野の関係法令についてもそれこそデジタル・バイ・デフォルトということでデジタルを前提とした形にするという意味では見直しの余地があるのではないかという御指摘もいただいておりました。

前回のディスカッションにおいて御議論いただいた部分の御説明は以上になります。ありがとうございました。お返しいたします。

○森川主査　ありがとうございました。

それでは、これからフリーディスカッションとさせてください。

鈴木専門委員、手塚専門委員からの話題提供に対するご質問、事務局説明に関する質問あるいはコメント、また、前広にこのような観点も議論していくのがいいのではないかというような御指摘等も大歓迎でございますので、ぜひ、皆様方からコメントをいただければと考えております。どなたかいかがでしょうか。

ありがとうございます。江﨑委員から挙手いただいています。江﨑委員、お願いいたします。

○江﨑委員　どうもありがとうございます。

お二人のお話に関連して、まず、鈴木専門委員から５Ｇは基本的にはそれ自体が問題ではないとのお話をいただいたと思いますが、５Ｇが外交でほかの切り札を使うためのツールになっている可能性がある点については留意する必要があると思います。ほかのカードと組み合わせて、ここを許すのでほかのカードをちゃんとやってもらうといった政治的なところが働いている可能性があります。ファーウェイに関しては非常にいじりやすかったという側面があったのではないかというふうに観察しています。

関連して、この件が出てきた最大の原因は、中国で彼らがインターネット法をつくったときに、インテリジェンス活動に関して中国国籍を持っている人はどこにいようが協力しなきゃいけないという規定できたところから、ものすごい報告が発生したと認識しています。そういう意味でいうと、技術の話もありますけれども、どのような法律がつくられたかということがポイントではなかったか。少なくとも５Ｇに関しては、この中国のインテリジェンスに関する法律が非常に大きなポイントになったと認識しておりますし、グローバルなコミュニティの中では、そういう話がされていると認識しています。

それからもう一つ、先生のお話を聞いていて、総務省としてやるべき具体的な施策と

しては、どうやって研究開発に関するポートフォリオを検証するか。つまり、現在のマーケットを見たときに選択肢が取れるような研究開発のところに我々がちゃんと手を出しているかという検証の機能が必要になってきます。結果として、施策として何をやるべきかというところに落としていけば、総務省の中での研究ポートフォリオというのをグローバルなサプライチェーンの経済安全保障の観点からしっかりと検証して、選択肢があるものを残していくということを考えるべきだということを再認識いたしました。

これは実は第６期の総合技術会議でも、研究の多様性はいろんな意味での安全保障の観点から必要であると言われていました。どこかに集中するという体制ではまずいというようなところにも通じるお話だと思います。

それから、手塚専門委員のお話で、バイ・デフォルトというのは、まさにおっしゃるとおりです。具体的に総務省で言えば、ユニバーサルサービスが音声とファクス通信になっているのは、そろそろ見直していいのではないかというのが２０３０年に向かってインフラストラクチャーにものすごく影響を与えることになってくると認識しています。バイ・デフォルトとしてのユニバーサルサービスの音声とファクス通信というのは根本的に見直すべきだろうという議論が出てくる。先生のお話から、例えば、クラウド・バイ・デフォルトというのはどのように考えたかというと、ハードウエアからのバンドルによるロックイン防止というのが一番大きなところで、つまりビジネス上のロックインをどうやって防ぐかということになります。そうすると、現在グローバルに認識されている問題はデータの利用に関するロックインと寡占であるということを考えると、バイ・デフォルトとしては、オープンアクセスバイデフォルトみたいなところまで持っていかないといけないだろう。バイ・デフォルトをどこで起用していくのかということを考えた場合に、単純にクラウドに行けというのがバイ・デフォルトではなくて、何のためにクラウドに持っていったかというところまで、ちゃんと原点回帰をして、何をすべきかを考えなきゃいけない。つまり、クラウド・バイ・デフォルトの場合には、ハードウエアのロックインを防止させるというためにやったので、ちゃんとやらないと、クラウドベンダーにロックインされるということはハードウエアの次の段階として起こることになるし、それはデータに関するロックインにもなっていくというところまでにらんだところで、バイ・デフォルトというのを考えなきゃいけないと思いました。また、バイ・デフォルトというのを、ちゃんと見直して、総務省としてつくっていくというの

は大変重要なことだと思います。

それから、デジタル化のバイ・デフォルトからすると、総務省からいえば、地方自治体のサポートというのは総務省の仕事だと思いますので、これは非常に重要な案件として入れていくことができると思います。

最後に、手塚専門委員からＤＦＦＴの話をいただいていて、これは当然やらなきゃいけないことですが、一番気になっているところはアジアが入っていないところです。やはりこれから伸びるところ、それからアジアの諸国はやはりアメリカ、ヨーロッパに対する信用の問題、それから中国との問題もあるとすれば、トラストを一番取り得る可能性があるところがアジアです。当然ながらデフォルトとして欧米というのは入るわけですが、アジアという戦略が入らなきゃいけないでしょう。

もう一つは、欧米としたときの中国との連結をどう位置づけるかというところが、我が国としては非常に鍵になっていくところではないかと思います。

○森川主査　江﨑委員、ありがとうございました。

それでは、ほかの委員の皆様方、いかがですか。

岩浪専門委員、お願いできますか。

○岩浪専門委員　本日、鈴木専門委員と手塚専門委員、大変重要な話、ありがとうございました。

全体的に、今回は経済含む安全保障の話だと思いますが、前回に、今後国のやるべき仕事が多くなるのではないかと、あるいはやるべきことが整っていないのではないかと発言しましたけれども、この分野も典型的にそういうテーマだと思っています。しかも、非常に重要で、両専門委員からも御指摘ありましたけど、この話も政府内や軍事に限ってという話ではなくて、明らかに民間にも影響のある話だと思います。

お話の中で出てきたＣＩからＣＵＩへのシフトというところで、ＣＵＩのカテゴリー一覧などで見ますと、農業から始まってあらゆる分野にわたって項目が広がっております。

それから、ＮＩＳＴのＳＰ８００シリーズに関しても、５３から１７１への準拠が求められるわけですが、ＩＳＯ２７００１をやっていれば安心というだけでは済まなくなり、１７１シリーズを民間まで求められると実装の技術レベルまで求められてしまう。例えば、２７００１ではパスワードの設定をしますということで済んでいたところが、１７１では、どんな暗号技術でどんな強度で実装するのかといった話まで来ると思いま

す。

やるべきものが整っていない部分があると手塚専門委員が指摘されましたが、そもそもセキュリティクリアランスは制度自体がまだないわけです。Ｇ７やファイブアイズ、韓国ではあるが、日本だけがない。そうすると、そのレベル、例えば、ゼロデイ情報に日本人はアクセスできないという話になりかねない。これではセキュリティについて議論できるはずもない。これは制度自体がない状態を早く何とかしないといけません。

オーストラリアなどはセキュリティクリアランスの保有人材数が産業競争力に直結するという認識で、審査制度も含めてそういう産業競争力の観点から捉えているという話も聞きます。日本のこの分野は本当にやるべきことをやっていない筆頭ではないかと思います。

もう一点、これは鈴木専門委員からの依存という話、これも非常に重要なキーワードだと思いますけれども、これはいわゆるネットワーク機器やクラウド、ソフトウエアというレベルもさることながら、アプリケーションやコンテンツサービスレイヤーにおいても全く同じ議論だと思います。

具体的に言うと、シェア５０％を超えるような大手のショッピングサイトが市場を牛耳っていて、そこが恣意的な行動をしたら一体どうなるのか。言うなれば産業全体がコントロールされてしまう虞がある話であり、台湾ではこうしたところに非常に気をつけているという話があります。

一番分かりやすい例は、ＹｏｕＴｕｂｅも含め、ＳＮＳです。去年、アメリカでＴｉｋＴｏｋを規制するという話がありましたけれども、ＳＮＳについては、情報を操作する、もしかしたら人間の行動や頭の中にも影響を与えているのではないかという話もあります。ウォールストリートジャーナルでは、１３歳から１５歳の子どもたちの状態を調査した結果として、ＳＮＳの利用は子どもたちへの攻撃ではないかという議論すら出ているくらい人間に大きな影響を与えかねない話であり、これは政府として何とか規制すべきなんじゃないかという議論も出て来るでしょう。このようなことも含めて、安全保障の議論が上位レイヤーにもあるという認識でおります。

以上でございます。

○森川主査　岩浪専門委員、ありがとうございます。

それでは、ほかの皆様方、いかがですか。

○鈴木専門委員　では、江﨑委員と岩浪専門委員からお話のあった点について少しコメン

トさせていただきます。アメリカが５Ｇからファーウェイを追い出したのは、ほかの切り札との関係にあるのではないかという御指摘ですが、恐らくは違うのではないかと思っています。

最初にきっかけになったのは、イラン、スーダン等に制裁をかけるに当たって、ファーウェイがイランなどに通信機器を売ったということで、日本でいうところの外為法違反がありました。こうしたアメリカの緊急国際制裁に関する法律、ＩＥＥＰＡの違反として問題が発覚して、そこから５Ｇの問題に発展していきました。それは政権の問題だけではなくて議会の問題でもありまして、つい先日中国の通信機器をインフラストラクチャーの契約から外すということを法律として決めたのは議会であり、これはバイデン政権のイニシアティブではないので、政権が何か意図的にカードとして使っていたというよりは、やはり全体的なアメリカにおける反中国のムードを極めて強く体現した議会の結果というのが一般的な見方ではないかと思っています。

中国の国内における法律の整備、データ安全法などが大きな転機になったのはそのとおりだと思っていますが、それはある意味そうしたアメリカにおける反中感情の火に油を注いだという格好になっているのではないかと思っています。

また、江崎委員からアジアを取らなきゃいけないとございました。これは手塚専門委員からのお話の文脈でおっしゃられたのですが、我々が少し注意しておかなければいけないのは、東南アジア諸国が中国を排除するという選択肢を持てないと考えているということです。彼らは日本やアメリカにつくのも嫌だし、中国につくのも嫌だし、できる限り両方と均等な距離を取りながら、でも、中国を排除するという選択肢はないという認識を持っているので、それを踏まえてどちらかのサイドを取るという態度を見せられない、そのように認識されない形でアジア諸国との関係をつくっていくことが重要だと思っています。

岩浪専門委員からいただいたコメントで、依存はアプリケーションやコンテンツにも係るのだろうというのはおっしゃるとおりだと思うのですが、これはまさに、ある特定のサービスが独占的になっているということです。今、バイデン政権の下では、そうした独占的なサービスに対する反トラスト法の適用というのが検討されている状態で、法律として特定のサイトないしは特定のサービスが独占的であるということが社会に害を与えているという認識があれば、法律を作る、もしくは、独禁法のような既存の法律でも適用可能だと思いますので、それを積極的に活用していくべきではないかと考えて

おります。

以上です。

○森川主査　鈴木専門委員、ありがとうございます。

手塚専門委員、何かございますか。

○手塚専門委員　ありがとうございます。まさに今、鈴木専門委員がおっしゃった点などで、私も５Ｇの件では、ＤＯＤから大学の先生になった方と議論する機会が多く、そういう方が、四、五年前ぐらいに、アメリカでは５Ｇの状況がまずいとおっしゃっていた。５Ｇはレイテンシーが良く、つまりリモートコントロールで全てのことがやり切れるような世界ができていくわけで、アメリカは軍として世界網を持っており、ＤＯＤは米軍のシステムを５Ｇ網にしていっていたが、その５Ｇ網に中国製品が入ること自体、アメリカからすると危機であり、それが５Ｇの状況がまずいと言う一番端的な理由だというのです。

その後、ファーウェイの問題などがいろいろ出てきました。アメリカは自ら５Ｇの設備を作る力がなくなっていて、この分野はまさに中国やノキア、エリクソン、日本くらいしか作れないと気づいた。その中で中国のシェアが大きいところは安全保障の視点から気になっていたところです。そうなるとアメリカもライクマインデッドカントリーのメンバーの国でまとめていくというデカップリングの世界が色濃く出ている中で、日本がどのようにしていくのかがこれから大事になってきます。単なる経済だけの文脈では語れない世界がもう起きているということだと思っています。

その中で、我が国として、ハイレベルなクラウド環境をどうやって持つのかというのは非常に重要で、ＦｅｄＲＡＭＰ等のアメリカの環境を参考に、なぜ我が国でつくらないのかということを言う人たちが多くいます。これを民間の大手企業と議論すると「１社では作れない」と言われる。また、１社で作ったとしても、維持費がペイできないといわれる。ただ、複数社で割り勘する形でまとめ上げるのであれば十分対応できると言う企業が多く、制度や政策等と絡めて考えていかざるを得ないと思いました。

アジア圏のことについては、鈴木専門委員のおっしゃることは非常に私も感じています。ただ、我が国がアジア圏に対して影響力を持つという点で、どのように仲間づくりをしていくか、そこにどのように提供していくかというのは、今の情勢を踏まえて、通信レイヤーからセキュリティ、トラストを我々の陣営のほうに持ってくる努力が絶対に必要だと思います。

それと、岩浪専門委員がおっしゃったセキュリティクリアランスの話はヒューマン系の話でとても重要な部分だと思っています。日本はどちらかというと性善説で動いているので、「あの企業の人だったら信用する」という場合がありますが、アメリカの場合は徹底的に一人一人のバックグラウンドチェックからやるような世界になっていることもあり、この辺のところをどのように日本の文化に合わせた形でやることができるのかということは、今後政策と絡めて重要だと思います。

そういう点で、人の分類とデータの分類がちゃんとできて、それに合わせたアクセスコントロールができれば、環境としてはできます。これはゼロトラストにもみんな関係していると思います。今後、システムアーキテクチャーとしてもそういう概念ができて、それとクラウドとの組合せというのが今後のＩＴ分野の動きだと思いますので、それに見合ったテクノロジーや機能をしっかりと見ていくことが、今後、ますます重要になると思います。

以上です。

○森川主査　ありがとうございました。

桑津委員、お願いできますか。

○桑津委員　桑津です。ありがとうございます。

私も経済安全保障絡みのところで、１点、御指摘したいと思います。

本日も御議論いただいている５Ｇ、クラウド、さらに半導体が、いずれもデカップリング等を含めて経済安全保障の領域にもかなり被ってきた、中心テーマになったと理解しています。加えて、セキュリティやＳＮＳという上位レイヤーのほうにもかなりの重点がある中で、昔はベンダー・ロックインだったが、データをオープンアクセスに変えていかなきゃいけないというのも、まさにテーマの変遷としては正しいと思います。

一方で、データセンターの議論も、これは江﨑委員が御専門ですが、これも少し考えておく必要が出て来たと思っています。

今、データセンターのマーケットでは、アメリカ等の伸びに対して日本が非常に遅れております。もちろん事業者があまりいないことやクラウドのイニシアティブをアメリカに握られたことが一番大きな理由ですが、日本でサービスをしていただくに当たって、アクセスの関係上から、日本に物理的なクラウド拠点、物理的な施設を持っていただくというのはすごく重要性が高いものになってきたと思います。

また、経済安全保障に少し絡みますが、東日本大震災以降日本にはデータセンターを

置かずに香港やシンガポール、台湾に移していたものが、かなり日本側に戻ってきています。それは別に日本が高く評価されたわけではなくて、日本以外に置くところがなくなったという状況です。手をこまねいてそのまま待っていればどんどん元に戻ってくれるのであればいいですが、残念ながらそうはいかないと思っております。印西市などでいろんな会社がデータセンターをつくっていますが、日本においてもアメリカ等のようなハイパークラウドに対応できる施設や設備の展開が必要で、本来、民間企業が主になってやるべきですが、半導体やクラウドと同じ状況で、日本企業では支えられない。先ほど１社ではできないという議論がありましたが、正しい表現だと思っていまして、産業政策の観点、もしくは経済安全保障の観点でデータセンターの環境整備をするべき時期が来ていると思っています。

ＳＮＳやほかのハイテク技術の最先端領域と比較すると、データセンターはマーケットの特性上半分は不動産ビジネスですので、まだ投入を増やすことで追いつける、もしくは投入する価値があると思っています。その仮定で、例えば、再生可能エネルギーとデータセンターのセットをある程度北海道などの適地に置いていく。あるいは沖縄を再評価すること等を経済安全保障の次のテーマとして上位レイヤーと並行して議論の対象に入れていくべきだと思いました。

以上です。

○森川主査　桑津委員、ありがとうございます。

では、鈴木専門委員、どうぞお願いいたします。

○鈴木専門委員　今の桑津委員のお話にコメントさせていただきます。おっしゃるとおり、データセンターの議論は経済産業省の半導体デジタル産業戦略検討会議で進められていて、政府にも問題意識はあると思っています。

日本の場合、データセンターが大都市、東京や大阪に集中していることが大きな問題で、物理的に１か所に集中していると、当然ながら自然災害等のリスクが大きくなるため、分散をしていく必要があるということも、経済産業省を中心に認識していると思っています。

一番問題になるのは、再生エネルギーの電気しか買わないというようなケースや日本の電力料金の高さが大きな問題となるという認識があるかと思います。最適解はないですが、例えば、省エネ・省電力型の半導体を作り、それを日本の売りとすべきであるという議論もあり、データセンターを日本に招致するために魅力的な環境を作りつつ他方

でリスクを分散するということがデータセンターをつくる戦略に課せられた課題であって、半導体デジタル産業戦略会議でも議論されている状況であるということを御報告いたします。

○森川主査　ありがとうございます。

どうぞお願いします、江﨑委員。

○江﨑委員　１つ抜けているポイントとしては、データセンターの拠点だけではなく、ネットワークや通信回線がしっかりしていないと分散できないことも意識しなきゃいけないところです。これは５Ｇに関してもＢｅｙｏｎｄ５Ｇにしても、結局フロントホールまでのバックホールのファイバー・インフラストラクチャーが肝になってくる。これが地方分散したときのファイバー・インフラストラクチャーをどうするかというのはまさに総務省としての戦略の中に入ってくる。これがちょうどデジタル田園都市構想の中でバンドルされてくる。やはりハードウエアのレイヤーのインフラストラクチャーをどのように整備するかというのは、光ファイバーは生ものであるため、しっかりアップグレードしていかなくてはならない。そうすると、そのインフラをどう設計しておくかという話は非常に重要で、総務省と経済産業省と連携して進めるべき施策になると思います。

○森川主査　ありがとうございます。鈴木専門委員、江﨑委員。

今、御説明いただきましたように、経済産業省の情報産業課や総務省のデータ通信課がデータセンターとネットワークまわりを何とかしていこうと仕込んでおられますので、ぜひ、その辺りも含めて、皆様方からいろいろな御意見等をいただければと思っております。ありがとうございます。

いかがですか。山中委員、お願いいたします。

○山中委員　ありがとうございます。電機連合の山中です。

私のほうからは、電機連合に加盟をしております企業の方からいろいろ御意見もこれまでいただいておりまして、そちらを踏まえて、御意見させていただければと思っています。

話題提供いただきましてありがとうございます。デジタル・バイ・デフォルトを実装していくべきだと思っておりまして、コロナ禍でかなり進んできていると思いますが、いろいろな目詰まりがあるとも思っています。

加盟組合の企業からは、建設業法や工事関係に関する対応について、なかなかデジタ

ル化できないといった声があります。また、監査関係で、データをデジタルで提出するものの、立会いの監査において紙で全て打ち出してくれと言われていることもあります。

それから、年末調整等の書類で、一部、控除申請系のものをデータで提出ができるようになっておりますが、企業側からは、そのデータと書類が二重にあることによって従業員に対する説明や手続で工数が多くかかるという御意見もいただいております。デジタル化はトラストの面で進まないという観点もありますが、一方で、紙とデジタルが２つあることによって進まない。コロナ禍で詰まっている部分でしっかり対応していくことが必要ですし、旗を上げつつも、細かなところにも対応していく必要があると思っています。

それから、セキュリティの観点で、ＳＰ８００－１７１の関係で、一部の企業では、もう既に対応していますが、企業負担の大きさがネックになっています。日本においてもそういった体制をしっかり築いていく必要があると思いますが、手続の対応との観点での目配せも必要になってくると思っています。

以上です。ありがとうございました。

○森川主査　ありがとうございます、山中委員。非常に貴重な御意見いただきまして、ありがとうございます。増田委員、お願いいたします。

○増田委員　消費者の立場からということでお話ししたいと思いますが、自治体のＩＴ化の遅れについてはこの１年で消費者のほうから多く指摘があったと思います。また、デジタル化と言ったときに、小規模事業者の場合のセキュリティがきちんと確保されているのかという懸念もありまして、そこに情報を提供することについての心配や不安もあろうかと思いますので、機器や通信回線でのセキュリティの負担ができるのかという問題があると思います。

これから５Ｇがさらに普及すれば、ＩＴリテラシーが一定程度あれば多くの人が普通に使えていく時代になっていくと思いますが、そこに至るまでにはサポートが必要で、例えば裁判のＩＴ化ということも議論されていますけれども、裁判をする権利というのを阻害しないためにどういう工夫が必要なのかが議論されている状況ですので、全てデジタルにすることについては様々な工夫が必要だと思います。

それから、経済合理性と安全性というところで、レベル感が違いますが、例えば、商品を選択するときに、インターネットが普及したことによってすごく価格重視になってしまっていて、価格重視がゆえに事業者が費用負担して安全性を高めているところが消

費者側から見えていない。適切な商品を選択する場合に、経済合理性プラス安全性というのがなければ絶対にうまくいかないと強く思います。デジタルの安全性に関しても本質的には同じだと思いました。

以上です。

○森川主査　ありがとうございます、増田委員。

鈴木専門委員、何かございますか。

○鈴木専門委員　増田委員のおっしゃるとおり、安全保障に関しても、個人レベルの消費に関しても同じだと思いますが、安全にコストがかかることに意識を持つことが大事です。しかし、それがなかなか消費者の側から見えず、恐らく、経済安全保障という国と国との関係で見ても、なぜファーウェイを使ってはいけないのかというようなことはなかなか見えないと思います。経済的合理性と安全上の合理性、安全保障上の合理性はどうしてもトレードオフの関係になってしまうので、そこで正当化するというか納得できる説明が大事なポイントになると思います。なぜこの価格なのか、なぜこれだけのコストを払わなきゃいけないのかということを、安全保障上のリスクがあるから、安全なものを手にしてもらいたいから等の納得できる説明がないと、ただただコストが高いだけだとネガティブに見えてしまうので、きちんとみんなが納得するような説明をして理解してもらう。これだけのコストが必要だということを、国際的な安全保障の文脈から理解してもらうということが大事なので、国民にも一定のリテラシーや国際政治の知識が求められると思いますが、それでも説明していくのが政府の役割、責務ではないかと思った次第です。どうもありがとうございました。

○森川主査　鈴木専門委員、ありがとうございます。

江﨑委員、お願いいたします。

○江﨑委員　１つ共有しておいたほうがいいと思ったのは、「誰一人取り残さない」とデジタル庁が打ち出しているところで、障害がある方をはじめ様々な状況で普通のコミュニケーションができない場合にそれをどのように助けていくかということが、最終的にはイノベーションにもつながり、インクルーシブな社会の実現との両方を狙えることから、それをきちんと目的にしていく必要があります。そう思うと、何をバイ・デフォルトにするのかというところで、様々なメディアを使うことによって全員がコミュニケーションできるようなインフラストラクチャーにする、例えば、ウェブページが目で見てしか読めないというのはおかしいですよねというような議論でちゃんとリーダーシップ取

っていくというのは総務省にとって重要なポイントになっていくと思いますし、その研究開発をしっかりリードし、そこを担保していくというのは非常に重要だと思います。

○森川主査　江﨑委員、ありがとうございます。

今、江﨑委員が言われたことに関して、お話をさせてください。

誰一人取り残さないというのはとても重要で、やはり最終的にはそこになりますが、最初からそれを考えると、全ての人が受容できるものを作らなければいけなくなり、なかなか進まないので、まずは一部の人からでも使っていただけるようなものというように、進め方としてはある程度割り切ってしまうことも重要だと思っております。

山中委員、お願いいたします。

○山中委員　今の誰も取り残さないという観点で、特に視覚障害者の組合員から幾つか声をいただいております。視覚障害者の方にとってデジタル化というのは望ましく、様々な活動においてパソコン上でやり取りができるということをかなり好意的に捉えているところがあります。

一方で、アクセス環境において、ウェブについては過去から対応していただいていますが、クラウド化によってアクセスしづらくなる状況がたまにあります。また、ソフトによっても、スクリーンリーダーが対応していない部分があり、アメリカに比べて日本ではその対応が遅れていることが課題であるとの声もいただいております。デジタル化を好意的に捉え、ぜひ利用していきたいという障害者の方もかなりいらっしゃいますので、そのアクセス環境の整備をしっかりしていただくことによって様々な仕事をできたり、対応できたりというところにつながると思いますので、対応できていない部分も頑張って対応していくというような観点で進めていただくことも必要だと思っています。ありがとうございます。

○森川主査　山中委員、ありがとうございます。江崎委員、お願いいたします。

○江﨑委員　ありがとうございます。まさに森川主査がおっしゃったようなところを気にしていくべきで、かつ、どのようにそれをユニバーサルアクセスとして定義すべきかと点はデジタル庁でも議論しているところであり、デジタル田園都市構想の中でも、そういう環境を提供することが極めて重要な国としての政策であるとしています。そのときにどのように多様性のある人を助けるための研究開発に我々が投資をするかというところは、研究開発がしっかりとサポートしなきゃいけないというのが共通的な理解だと思います。

○森川主査　江崎委員、ありがとうございます。非常に心強い御発言ありがとうございます。増田委員、お願いいたします。

○増田委員　先週の金曜日、私どもの協会で、高齢者のデジタル・ディバイドを解消するためにというテーマでシンポジウムを開いたところです。

デジタルは皆さん使いたい状況にあって、それをどうサポートしたらいいのかということをメインのテーマにしておりました。

その環境整備を事業者や国のほうでやっていただくのと同時に、私たちみたいな立場の者がそこに誘導するような形でのサポートをするということをしていくという話になっているため、ぜひ、皆さんの活動に期待したいと思っております。

以上です。

○森川主査　ありがとうございます。増田委員がされているような活動は非常に重要だと思っております。引き続きよろしくお願いいたします。

それでは、何かほかにございますか。よろしいでしょうか。ありがとうございます。

（２）その他

○森川主査　それでは、次回の日程等、事務局からありましたら、お願いできますか。

○田熊係長　本日はありがとうございました。次回の総合政策委員会につきましては、来週、１１月２５日木曜日１０時ちょうどからウェブ方式にて開催いただきます。

以上でございます。

○森川主査　ありがとうございます。

引き続き皆様方からいろいろな御意見等いただけますよう、お願いいたします。

それでは、これをもちまして、第２回の総合政策委員会を終了とさせてください。本日はお忙しいところをお集まりいただきまして、ありがとうございました。

（以上）