資料５

基幹インフラに関する検討会合（第１回）議事要旨

１　日時

令和３年 12 月 10 日（金）午前９時から午後 10 時 20 分までの間

２　場所

オンライン開催

３　出席委員

青木　節子	慶應義塾大学大学院法務研究科 教授
阿部　克則	学習院大学法学部 教授
大橋　　弘	東京大学公共政策大学院 院長
兼原　信克	同志社大学 特別客員教授
小林いずみ	ANA ホールディングス株式会社 社外取締役
土屋　大洋	慶應義塾大学大学院政策・メディア研究科 教授
原　　一郎	一般社団法人 日本経済団体連合会 常務理事
渡井理佳子	慶應義塾大学大学院法務研究科 教授

４　議事概要

（１）事務局説明

事務局から、資料の内容について説明があった。

（２）意見交換

《論点①　基幹インフラ機能の維持等のための新しい仕組みの必要性》　及び
《論点②　基幹インフラ機能の維持等のための新しい仕組みの方向性》

○　本年の G7 コーンウォールサミットのパネルで議論された強靱性レポートにおいても、国家のレジリエンスの根幹としてサイバーセキュリティに向けた取組の必要性が記載されており、国家だけでなく民間主体も取組を推進する必要があるとされている。また、DX の進展に伴い、あらゆる領域がサイバー攻撃の対象となっており、平時にシステムなどにマルウェアを仕込まれ、後になってシステムが停止させられるという事態に対処すべき。政府全体の横串をとおして日本の重要なインフラを守る必要がある。インフラ事業者が用いるシステムには、アップデートを要するソフトウェアも組み込まれており、一度導入してしまうと取り返しがつかない。日本はこれまでの新自由主義的な潮流の中で、安保を考慮せずに規制改革を進めてきたことから、外為法を除き、既存の経済分野の多くの法律に安全保障の観点が含まれて

いない。

○　サイバーセキュリティの観点からは、完璧なセキュリティは存在せず、国家ぐるみの攻撃であれば防ぐことは相当困難という前提がある。特に、サプライチェーンの段階からリスクを仕込まれていた場合や内部協力者がいる場合は確実に攻撃を防げない。そのような認識のもと、多層の防御を築くことで対応を図る必要がある。既にNISC、経産省、防衛省、総務省などで行っているサイバーセキュリティ対策と違った観点から新しい仕組みを設けることで、新しい防御の層が築かれるという意義がある。米国におけるCFIUS、旧Team Telecom(Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector)といった関係省庁の協力枠組も参考に検討していく必要がある。また、企業側の視点からは、政府に自らの情報を明け渡すだけではなく、制度に参加することによるメリットも存在するという点を訴える必要がある。データ面ではサイバー攻撃には国境はないが、島国である日本にとって設備面では国境がある。具体的には、海底ケーブルの陸揚局がまず始点となり、そこからデータセンターなどへつながっていく。このようなポイントで対策を講じる必要がある。

○　サイバー攻撃は防御が難しく、実行主体が多様で、仮に認定できたとしても時間がかかるといった特徴がある。そのため、事前に防ぐ必要がある。例えば、甚大な被害が起こる可能性がある重要なシステム等について、攻撃の意図を有しているような非友好国家から間接的にでも影響を受けているとの証拠がある製造者から提供される設備は利用しないといった対応が必要。その上で、同盟国及び友好国とうまく調和できる制度作りが必要。

○　新しい仕組みの必要性があることに賛同。外国の取組も参考にしながら制度を検討していくべき。サービスへの障害が問題であることからすれば、サプライチェーンも含め、包括的に見ていく必要がある。一方で、新たな仕組みを設けるのであれば、既存の法律との関係を整理して、必要最小限の規制にすることも必要。設備やサービスの提供をめぐるリスクについては、外為法では対応が難しい。また、基幹サービスの利用者である市民のデータについては、内外を問わず、流出を防止することが重要である。さらに、新制度の検討・運用に当たっては、基幹インフラ事業者の設備の導入や維持管理の委託について現状やリスクを把握・調査できるようにすることが必要。

○　基幹インフラとしては、電気通信その他様々な種類があるが、いずれについても、技術的な領域はこれまで事業者の自主的な内部統制で対応していたのではないか。今でも産業界で民間委託を進める流れがある。経済安全保障の議論を進めていく際には、個別に分散して対応するのでは時間がかかり、ムラができるので、上流から縛る必要があるのではないか。民間の努力と合わせ、共同規制的なものも含め、政府が包括的に進めていく仕組みが必要。日本のこれまでの制度は事業者の善意に基づいたものが多く、根本的な哲学から変えていく必要がある。

○　この分野においては、明らかに新しい仕組みが必要であると思う。一方で、これまでサイバーセキュリティなどは個社の努力に任されてきたと感じており、基幹的なインフラであるという認識の程度や、経済安全保障に対する意識には個社ごとにムラがある。そのため、個社の自助努力に任せる仕組みではなく、産業別でもなく、網羅的・産業横断的に政府としての対応を図るような仕組みを作る必要がある。

○　サイバーセキュリティの確保は、非常に重要な課題である一方で、難しい課題でもある。そうした中、基幹インフラの安全性・信頼性の確保は、多層防御の一つとして、他の取組との適切な役割分担が必要である。経済安全保障を確保する方法は必ずしも規制一色ではないと理解しているが、今回検討されている４分野のうち、この基幹インフラに係る分野が最も規制色の強いものであると認識している。そのため、出来るだけ対象を限定する必要がある。米国については、当初案では、事前承認制度はなかったが、その後、予見可能性の面から事前承認制度が必要なのではないかという議論になり、現在検討をしているものと承知している。今回の検討でも、予見可能性の点から事前審査はやむを得ないと思うが、対象は絞るべきである。また、米国の様に国や企業を特定することは難しいと思うので、予見可能性を高めるという観点から、ドイツの例なども参考に審査基準を検討してほしい。なお、サイバーセキュリティの確保という観点から、サプライチェーンの強靭化に関する検討とも整合をとる必要がある。

○　最初の段階として、インフラ事業者のシステムを規制することが必要。システムは定期的にアップデートされるものであり、そうしたサービスを担う委託先についてもどのように捉えていくかを検討すべき。また、データについてはクラウド事業者に預けることが一般的だが、クラウド事業者が実際にどこにサーバーを置いているかは分からないし、外国でバックアップを取っているかもしれない。そのため、クラウドの利用についても捉えることができる制度を検討すべき。

《論点③　経済活動の自由と国家及び国民の安全を両立させるための考え方》

○　対象となる事業者を絞ることにより、経済活動の自由と国家及び国民の安全を両立させる必要がある。

○　国際法の観点からいくつか述べたい。まず、対象となる事業や事業者を絞っていく必要があるとの事務局案には賛成。その上で、国際法との整合性を確保していくことが重要。二国間や多国間の投資協定の有無など立場の違いや、安保例外についての考え方の違いにも留意すべき。事務局が検討しているような制度自体は国際法上も実現可能なものだと考えられるが、かなり広い産業を対象とするものであれば精査が必要である。我が国が締結している各種の投資協定についての留保の状況やGATSの例外規定などについて検討しておくことも重要。

○　国家・国民の安全と事業者の経済活動の自由との間でのバランスをとる必要。規制の対象となる事業者は価格ではなく安全性を重視して設備等を調達することになり、これは企業の負担、翻って国民の負担にもなり得る。そのため、企業の考えだけではなく、国民全体が安全に係る高い意識を持つことが必要であり、そのような意識付けのための発信も併せてやっていく必要。また、企業にとっては事業判断が遅れないことも重要であり、もし政府が設備等を審査する場合は、なるべく事業者に負担をかけない形で速やかに判断する体制整備が必要。

○　国家及び国民の安全は効率性という競争領域の話を議論する前の、取引の前提となる規律。今回の検討はそのような前提を一つ加えるという話と理解。しかし、我が国だけでこのような取組を進めるのではなく、国際的な動向を見定める必要がある。

○　中小企業まで過度な負担を課すことは好ましくないが、防御が手薄な所を入口としたサイバー攻撃も考えられることから、中小企業についても意識を高めることなどを検討する必要がある。

○　中小企業への対応という観点からは、ISOなどのサイバーセキュリティに関する民間の標準を導入する必要性をまずは周知することが考えられるのではないか。

《論点④　基幹インフラ事業の特定に係る考え方》　及び
《論点⑤　基幹インフラ事業者の特定に係る考え方》

○　守るべき対象としては、安定供給が脅かされた場合に、国民の生存に支障をきたすものや、国民生活や経済活動に広範囲・大規模な混乱が生ずるもの等、例えば航空、空港、鉄道、電力、通信、銀行などをカバーする必要があるのではないか。対象の基幹インフラ事業を特定していく際には、NISC のガイドラインや国民保護法の例が参考になるであろう。

○　基幹インフラ事業の役務が安定的に提供されることは重要であるが、一方で対象は限定していく必要がある。見方によっては、現在存在している事業は全て重要だから存在しているということもできるため、規模といった形で限定をかけていく必要性はある。例えば、中小企業すべてを対象に含めるとすると、やりすぎではないだろうかと感じる。設備の導入や保守等の委託は民間同士の取引であり、最後はお金がかかってくる話。事業者の視点からも納得がいくようにバランスをとった制度を考える必要がある。

○　事業や事業者の限定に加えて、事前審査の対象に含める設備等の範囲を出来るだけ絞る必要がある。

○　近年、産業の垣根を超えた事業展開が増えてきているので、業界別に考えるだけではない柔軟な考え方が必要ではないか。例えば、金融業界と通信業界の垣根がなくなってきている。

○　今回、安全保障の政策を横串で様々な産業に適用することを考えると、事業法の中に新たな規制を入れるのみならず、産業横断的な発想で検討していく必要がある。

○　対象となる事業・事業者は絞ることを前提としつつも、ネットワーク産業については規模の大小を問わず１つが機能停止するとネットワーク全体が機能停止する場合などもある。そういった観点からも考える必要があるのではないか。また、規制を及ぼす際は公正な競争条件との関係も念頭において検討を進める必要があるのではないか。

以上