第二百十三回国会　衆議院　内閣委員会議録　第六号

令和六年三月二十八日（木曜日）

午前九時開議

出席委員

委員長　星野　剛士君

理事　上野賢一郎君　理事　髙木　啓君

理事　冨樫　博之君　理事　中山　展宏君

理事　太　栄志君　理事　森山　浩行君

理事　堀場　幸子君　理事　庄子　賢一君

青山　周平君　井野　俊郎君

石原　正敬君　泉田　裕彦君

大西　英男君　大野敬太郎君

勝目　康君　神田　潤一君

小森　卓郎君　杉田　水脈君

鈴木　英敬君　土田　慎君

西野　太亮君　鳩山　二郎君

平井　卓也君　平沼正二郎君

牧島かれん君　宮澤　博行君

簗　和生君　山本ともひろ君

逢坂　誠二君　中谷　一馬君

本庄　知史君　山岸　一生君

山崎　誠君　阿部　司君

金村　龍那君　住吉　寛紀君

河西　宏一君　吉田久美子君

塩川　鉄也君　浅野　哲君

緒方林太郎君　大石あきこ君

内閣府大臣政務官　神田　潤一君

内閣府大臣政務官　平沼正二郎君

内閣府大臣政務官　土田　慎君

参考人（東京大学未来ビジョン研究センター教授）　渡部　俊也君

参考人（TMI総合法律事務所パートナー弁護士）　境田　正樹君

参考人（日本弁護士連合会副会長）　齋藤　裕君

参考人（公益財団法人笹川平和財団特別研究員）　大澤　淳君

参考人（弁護士）（博士（法学））　三宅　弘君

内閣委員会専門員　尾本　高広君

委員の異動

三月二十八日

辞任　補欠選任

小森　卓郎君　勝目　康君

鈴木　英敬君　西野　太亮君

同日

辞任　補欠選任

勝目　康君　石原　正敬君

西野　太亮君　鈴木　英敬君

同日

辞任　補欠選任

石原　正敬君　小森　卓郎君

本日の会議に付した案件

重要経済安保情報の保護及び活用に関する法律案（内閣提出第二四号）

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律の一部を改正する法律案（内閣提出第二五号）

○星野委員長　これより会議を開きます。

内閣提出、重要経済安保情報の保護及び活用に関する法律案及び経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律の一部を改正する法律案の両案を議題といたします。

本日は、両案審査のため、参考人として、東京大学未来ビジョン研究センター教授渡部俊也君、TMI総合法律事務所パートナー弁護士境田正樹君、日本弁護士連合会副会長齋藤裕君、公益財団法人笹川平和財団特別研究員大澤淳君、弁護士、博士（法学）三宅弘君、以上五名の方々から御意見を承ることにいたしております。

この際、参考人各位に一言御挨拶申し上げます。

本日は、御多用中のところ本委員会に御出席を賜りまして、誠にありがとうございます。両案について、それぞれのお立場から忌憚のない御意見をお述べいただき、審査の参考にいたしたいと存じますので、よろしくお願い申し上げます。

次に、議事の順序について申し上げます。

まず、渡部参考人、境田参考人、齋藤参考人、大澤参考人、三宅参考人の順に、お一人十分程度御意見をお述べいただき、その後、委員の質疑に対してお答えをいただきたいと存じます。

なお、参考人各位に申し上げますが、御発言の際にはその都度委員長の許可を得て御発言くださるようお願い申し上げます。また、参考人は委員に対して質疑をすることができないことになっておりますので、あらかじめ御承知おき願いたいと存じます。

それでは、渡部参考人にお願いいたします。

○渡部参考人　おはようございます。

本日は、お招きいただきまして誠にありがとうございます。

私からは、実証分析系の政策研究を行っている立場から、重要経済安保情報の保全制度の必要性、及びその方法としての人的クリアランスが必要であること、そして、本制度の運用における留意点の三点についてお話を申し上げたいと存じます。

お手元の資料の表に要点、裏に参考文献をつけさせていただきましたので、御参照いただければと思います。

本制度整備については、かねてから産業界の強い要望があるところであります。背景としましては、制度がないことが原因で、海外の情報共有から締め出されているのではないかという懸念があります。もとより、日本国民が米国等のセキュリティークリアランスを取得することはできませんが、我が国が他国と同等の制度を整備していないため、政府間で情報共有されたものが民間には提供されないということが問題になります。

例えば、米国で、何社かちょっと現地で調査をいたしましたが、サイバー技術開発に従事する日本企業の米国現地法人は、米国人を採用してセキュリティークリアランスを取得しておりましたが、日本に同等の制度がないため、例えばサイバー攻撃に関する致命的な情報を得たとしても、その情報を日本の本社には提供できない、また、本社の技術がその対策として使えたとしても、そのことを本社に伝えることができないということを伺いました。

先端的な技術開発においては、官民協力が不可欠であり、政府だけが重要情報を持っていても、対応には限界があると思います。英国との関係でも、同様の問題を抱えている企業がありました。

本制度を有するG7各国ではお互い官民協力が可能であるのに、我が国だけ制度を有していないということが重大な問題であるということは想像に難くないと思います。

では、そのような機密情報を民間に提供する場合の問題点について述べたいと思います。

情報が提供される相手は民間企業ですから、そこからの漏えいが問題になるわけであります。これを検討するには、企業の保有する営業秘密が現

在どの程度漏えいしているかというような実態を踏まえるべきであります。

以前から、企業の営業秘密漏えいに関する調査はしばしば行われてきましたけれども、おおよそ五％から一〇％程度の企業が営業秘密の漏えいを経験したという回答をしております。この数字自身は大変大きいと思いますけれども、更に深刻なのは、これは全体のごく一部、氷山の一角であり、実際は、その何倍、さらには一桁多い漏えいが疑われるということです。

私が二〇一四年当時に行った研究でありますけれども、漏えいしていても全く気がついていない企業が極めて多いことが分かりました。

これを踏まえ、政府に営業秘密保護の強化を提言し、二〇一五年の不競法改正、これは海外重課、非親告罪、未遂罪などを設けていただいた経緯がございます。ちなみに、罰則は、十年以下の懲役若しくは二千万円以下の罰金、海外重課は三千万円ということで、当然、単純な比較はできないですけれども、今回の法案より罰則は厳しいものです。

その結果、以前は営業秘密の事件はほとんどなかったんですけれども、この制度整備後は徐々に摘発件数が増えてきました。ただ、他国と比べてまだ件数は少ないです。氷山の全貌は、まだ姿を現していないと思われます。

その漏えいの原因がポイントなんですけれども、重要なものはほとんど人を通じた漏えいで、現職従業員又は退職者によるものということが分かっています。この状態で政府さらに他国の機密情報の提供が行われたら、諜報活動は常に弱いところが狙われるということになりますので、大変深刻なことになるというふうに想像されます。少なくとも、他国と同等の保護制度、人を通じた漏えいを防止する適性評価を行わなければ、情報共有を行う相手国にとって信頼できるものにはならないというふうに考えます。

その点、今回の法案にある適性評価制度も、運用実績や諸外国の動向などを踏まえ、リスクが残っていないかどうかは検証していく必要があるものと思います。

他方、今後法案が成立した際の運用については、幾つか留意点があると思います。

まず、プライバシー、労働法制との関係。そして、本人の意思に反する適性評価を決して行ってはいけないこと。機密情報の提供が真に必須であり、任意の了解の下で行われること、これは本制度の根幹であると思います。個人情報を含む調査結果についての目的外利用の禁止。そして、何より重要なのは、クリアランスホルダーの民間人は、今回、我が国にとって極めて大事な人材であるということだと思います。

参考文献三に示しておりますけれども、我が国は、バブル崩壊後の経済低迷の間、多くの貴重な技術者が海外に職を求めて移籍したことで、日本は技術を失ってきたという苦い経験があると思っています。今回は、特に政府の制度を支える貴重な人材の話になりますので、その処遇や雇用に不具合があってはならないと思います。罰則だけで健全な官民協力体制は形成されません。経済安全保障政策全体として考えるべきことですけれども、施策を担う民間人を大切に扱う制度であるべきだと思います。

また、個人のクリアランスだけでなく、施設や組織のクリアランスについて運用を定めていくことが重要であります。米国では、個人のセキュリティークリアランスと同等に、組織や施設のクリアランスがしっかり行われていまして、特に研究開発を行う場合はこれが非常に重要になる。

他方、その組織の経営者を含む指揮命令系統にある人物、これは監査などとか、いろいろな形でそれをチェックするという機構があるわけですけれども、全ての個人に機械的にクリアランスを必須としてしまいますと、現実的には対応できないということも懸念されます。その点を考慮し、産業界とは適切な運用方法を検討していくことが重要だと思います。

いろいろ課題はあるわけですけれども、これらに取り組みつつ、今回このセキュリティークリアランスの運用が始まるということになれば、我が国の経済安全保障に係るエコシステムを発展させる上で、まさに大きな一歩になると思います。それは、単にクリアランスの適用対象に限って政府の機密情報の活用が進むということだけではなく、その外側にある、いわゆるデュアルユース技術の研究開発の規範、これを確立させていくためにも重要と考えられます。

例えば、防衛技術との境目が曖昧な民間のデュアルユース技術について、やっていらっしゃる方は、どこから機密性の高い研究開発とすべきかということについて、深刻な問題を抱えています。

これは米国の調査結果からの私見でありますけれども、我が国では、セキュリティークリアランスを必要とする機密研究が今まで存在しなかった、そのために、セキュリティークリアランスを必要とするそういうような機密研究とそうでないものの境目があって、境目が認識されるということがなかったということで、結局その境目が分からない、だから全体としてグレーみたいに捉えられてしまうというような傾向もあったんじゃないかと思います。

今後、本制度の運用が始まることで、その境目がはっきりする、認識ができるということで、それが判断しやすくなるということを期待しますし、同時に、機密研究でない基礎研究における管理についても、そこの制度を整備していくという課題がはっきりしてくる。

今回の法案の次の課題になりますけれども、最近Ｇ７で合意された人や組織に関するデューデリジェンスの徹底、さらに、米国で言う、ＣＵＩと言っていますけれども、管理された非機密情報に相当する情報管理、こういうものについては、ガイドラインを整備するというようなことが次のステップでは重要になると思います。これらが整備されれば、クリアランスの外と内が組み合わされた経済安全保障のエコシステムが形成されていくということが期待できます。

もっとも、このようなエコシステムは、制度をつくればすぐに機能するというものではありません。制度を運用しながら人材も育て、徐々に形成されるものと考えられます。逆に、できるだけ早くこのプロセスをスタートさせなければ、既に大きく劣後している可能性の高い、我が国の戦略的自律性を補う時期が更に遅れるということになるかと思います。

そのような観点から、本法案の早期の成立を強く望むものでございます。

私からは以上です。ありがとうございました。

（拍手）

○星野委員長　ありがとうございました。

次に、境田参考人にお願いいたします。

○境田参考人　境田でございます。

本日は、このような貴重な機会をいただき誠にありがとうございます。

今回、重要経済安保情報の保護活用に関する法律案ということについての審議が行われていますけれども、これの法案の検討のための有識者会議の委員を務めておりまして、一年間、合計十回にわたり、そこの検討に加わらせていただきました。その一年間、この作業に加わる中で感じてきたことを少しお話しさせていただきたいと存じます。

この法案は、特定秘密保護法から、それのもう少し範囲を拡大する、こういうふうなことで立案されているわけですけれども、その特定秘密保護法が作られた十年前から大きく環境が変わったな、立法事実が変わったなというのを痛感しております。私は法律事務所に勤めておりまして、いろいろな企業とか、国立研究開発法人とか大学の、経営者の方々と話をしていますけれども、危機感がこの十年間で半端なく高まっているということです。

まず、二〇一六年には、ダボスで行われた世界経済フォーラムの年次会議で、第四次産業革命、産業革命というのは、教科書で、昔、一六〇〇年代に行われたというのは覚えていましたけれど

も、今は第四次産業革命なんだということが周知されたわけです。この中では、ロボット工学とかＡＩ、ブロックチェーン、ナノテクノロジー、バイオテクノロジー、半導体、量子技術、インターネット、３Ｄプリンター、仮想技術、拡張技術など、様々な先端ハイテクノロジーが社会、産業、教育、経済、全てを変えるんだ、こういうふうなことが提唱されたわけです。

日本政府も、翌年にはソサエティー五・〇という、サイバー空間とフィジカル空間を高度に融合させたシステムにより、経済社会と社会的課題の解決を両立する人間中心の社会を提唱したわけです。

さらに、ここから拍車をかけたのが、皆さん御案内のとおり、チャットＧＰＴなどの生成ＡＩの技術ですね。二〇二二年十一月に米国のオープンＡＩ社がチャットＧＰＴを提唱して、生成ＡＩ時代が到来したわけです。これが今、この第四次産業革命とか言われるものをはるかに加速させる革命をもたらすというふうに私は認識しております。

特に、主要企業の時価総額、これは三月二十二日時点のものですけれども、日本のトヨタは六十三兆円、断トツで、次に三菱ＵＦＪグループが十九・七兆円、東京エレクトロンが十九兆円、キーエンスが十七兆円、そういう時価総額ですけれども、例えば、アメリカのマイクロソフト社は四百七十七兆円ですね、それから、アップルは三百九十九兆円、エヌビディアは三百四十兆円。特に、チャットＧＰＴができてから、この各社、百兆円ずつ時価総額が上がっているんです。

これはどういうことかというと、この先端デジタル技術、生成ＡＩなどと、ビッグデータ、あと情報プラットフォームを掌握すれば、産業競争力と経済的利益を独占するということだと思うんです。その気になれば、他国政府とか他国の企業にとって潜在的なチョークポイントを多数握ることが可能だということだと思っています。

つまりは、武力を伴わずに他国を実質的に支配下に置く、コントロールする可能性があるということに我々は留意しなければいけない。江戸時代末期に黒船が来て、我々は大砲を、我々というか我々の先祖は、アメリカの艦船を見て、大砲を見て驚いたわけですが、その大砲というような有形物ではなくて、もっと様々な脅威が日本国とか若しくは日本の企業に迫っているということです。

他方、そういった企業を味方につける必要もあって、御案内のとおり、ロシアによるウクライナ侵攻の際には、スペースＸ社、あのイーロン・マスクさんがウクライナに提供したスターリンクインターネットサービス、これを契約していたことによって、即時の侵攻を免れ、侵攻というか制圧を免れたということもあるわけです。

なので、こういった企業とうまくつき合うかということも重要であると同時に、そこにリスクを感じるということも必要で、ゆえに、米国は中国のファーウェイを規制し、中国はグーグルやメタなどのＳＮＳの大手を規制しているわけですね。そういったことに留意が必要だということです。

こういった日本における重要技術の保護と活用のためには、同盟国と同志国との緊密な連携が必要であるし、官民の情報共有、連携の推進が重要だということです。

ソサエティー五・〇、生成ＡＩ時代には、国を守る安全保障のための政策と産業競争政策、この守りと攻めを一体的に検討するということが必要だと思っています。

次に、私はいろいろ政策に関わることがあるんですが、こういったセキュリティークリアランスほか経済安全保障戦略に加えて、生成ＡＩ・デジタル戦略、半導体・量子戦略、カーボンニュートラル戦略のような重要な政策などにもちょっと関わらせていただいておりますが、その四つも、実は相互に相関関係があるんですよね。生成ＡＩで大規模データを解析しようとすると物すごく電力を食うわけです。そこのエネルギーの省エネ化を図らなければいけないし、そのための半導体を開発しなきゃいけないんです。

そういうふうに、こういった各政策に相互の深い相関関係があるということを考えなきゃいけなくて、そのときの共通検討事項としては、世界における経済マーケットシェア、産業競争力を日本全体でどうやって強めていくか、攻めをどうやって確立するかということ、それから、逆に守りで、セキュリティー対策とかレジリエンシー体制を確立するということも重要です。と同時に、そういう中で戦略的自律性とか戦略的不可欠性を獲得していくということも重要であるし、ウクライナ侵攻とか台湾有事リスクなど様々な地政学的リスクとか、米中の覇権争いのリスクとか、エネルギー供給リスクとか、様々なリスクを洗い出した上で政策を立案しなければいけない。

さらに、生成ＡＩ等ハイテク技術が政治、社会、経済、教育をどう変えていくのかをイメージしながら、そのための支援と規制をしていく。そのためには、各国の政策や最新技術情報の収集とか、解析とか、研究開発テーマの立案とか、国政全般を見渡した戦略立案、産学官の連携のマネジメントが必要であると思っています。ここで難しいのは、やはり、各省は基本縦割りで、自分の省で担ぐとなるとどうしてもそこにそごが出ることがあるので、ここは先生方の政治主導というのが非常に重要であるというふうに痛感をしております。しかも、これはかなり難易度が極めて高いので、ある程度の失敗は許されると思っていて、トライ・アンド・エラーというＰＤＣＡサイクルをいかに回すかということが重要なんだと思っております。

それで、最後に、今回のセキュリティークリアランス制度に関する有識者会議の中で、少し外れるかもしれませんが、一番感じたことを申し上げさせていただきます。

今回、先生方御存じのとおり、取り扱う情報の中では、トップシークレット、シークレット、これは特定秘密保護、その下の機微度がやや下がるコンフィデンシャルが重要経済安保情報保護活用法、これの対象になったということでございますが、実は、産業界が一番期待していたのは、その下のＣＵＩという、コントロールド・アンクラシファイド・インフォメーションという、ここに関する何らかのガイドラインとかを作ってほしいというのが、実は産業界の一番の希望でございました。

ここは、ただ、今回はコンフィデンシャルを中心にということで法案が進んでいるわけですけれども、産業界からすると、今申し上げたような様々なサイバーリスクとか、それから、例えば米国の輸出管理法、ＥＡＲの規制があれば、中国がそれに対抗する中国輸出管理法の規制を講じる。それぞれ守っているとどっちかから制裁を受けたりとかするという、企業の経営者からするといろいろなところから矢が飛んでくる。そのときに、ガバナンスをしっかりするためには、施設クリアランス、組織クリアランス、人のクリアランスをしっかりしなきゃいけないわけですね。それが、人のクリアランスというのは、企業というのは、職業安定法の考え方という部分もあってなかなか人の管理ができないんです。

アメリカの場合は、ここのところが、ＣＵＩというものに対して政府がきちんとそこの情報を決めて、これに対してＳＰ８００―１７１という規制で人的なクリアランスもするという制度があるんです。ここを日本で、政府でもつくってほしいというのが、実は産業界の大きな課題というか希望だったんですね。今回これはかなえられなかったわけでありますが、やはり、本当の産業界のニーズというのを酌んだ法制度というものを、法制度なのか、ガイドラインなのかもしれませんが、ここに対応していただくということが非常に重要なのかなというふうに考えております。

以上でございます。ありがとうございました。

（拍手）

○星野委員長　ありがとうございました。

次に、齋藤参考人にお願いいたします。

○齋藤参考人　おはようございます。日本弁護士連合会副会長の齋藤でございます。

資料の十六ページ以下を御覧いただければと思います。

私の方は、秘密指定の適正化の問題、二つ目、秘密指定される情報の範囲が不明確であること、三つ目、適性評価の在り方の問題、四つ目、民間企業への悪影響についてお話しさせていただければと思います。

秘密指定の適正性についてまずお話しさせていただきます。

秘密保護法も本法案も、元々アメリカの制度を参考に作られているとされておるわけです。しかし、秘密保護法においては、秘密指定のチェックがきちんとされておりません。よって、アメリカに比べて秘密が水膨れになっている可能性があると考えております。そうであれば、日本の方が秘密が拡大しやすく、市民の知る権利が制限されるということになりかねません。

つまり、例えば、アメリカでは強制的秘密解除というシステムがございまして、市民が秘密の解除を求めるシステムがございます。二〇一五年時点で、全体としてこのシステムで解除された文書が二十四万七百十七件、部分的な解除でいいますと十万九千三百四十九件。対して、日本では、独立公文書管理監や情報監視審査会の監督によって秘密の要件を満たさないということで解除された文書はないわけでございます。

なぜこのようになっているのかということですけれども、アメリカでその制度を管轄しているＳＯＯというところが、ノーリターンルールという人事のルールを設けております。しかし、日本の場合、独立公文書管理監にはそういうルールがない、そういうことが一つの原因かもしれません。

もう一つ、アメリカでは、秘密の指定も解除も文書ごと、つまり、具体的な秘密の内容に沿って秘密指定や解除をしているわけであります。具体的な文書に記載されている中身が秘密の要件を満たすかどうかをチェックしているわけです。

しかし、日本ではそうではありません。例えば、国家安全保障会議の結論というものが秘密指定されておりますのでこれを例に取りますけれども、どういうふうに秘密指定されるかというと、例えば令和四年度の国家安全保障会議の結論というような形で秘密指定されているわけです。そうしますと、独立公文書管理監のチェックだと、例えば二月一日の議事録に書いてある結論が、もうこれは公になっている情報だ、だから秘密の要件を満たさない、だからこの日の議事録は解除するんだ、そういうチェックはしないことになっております。あくまで全体として、令和何年度の議事録における結論という形で秘密指定されておりますので、チェックされるのはそれだけということでございます。

そういう形で、アメリカのようにきめ細かいチェックがなされない、だから秘密指定が解除されないというところがあると思います。ですから、本当は公知で全然秘密として保護するに値しないような議事録が日本では秘密のままになっている、アメリカではそうではない、そういう違いがあるということでございます。

アメリカを参考に制度をつくったということなんですけれども、特定秘密保護法では、アメリカよりはるかに知る権利について制限的なものとなっております。今回の法案もほぼ同じようなものでございますので、独立公文書管理監が仮に秘密指定についてチェックするんだとしても、決して十分なチェックはなされないだろうと考えております。

さらに、今回の法案では、情報監視審査会によるチェックが想定されていないということも問題でございます。

二つ目でございますが、どのような秘密が指定されるか不明確であることについてお話しさせていただきます。

秘密保護法と違いまして、今回の法案は、別表で具体的に秘密とされる類型が規定されておりませんので、立法時点においてどのようなものが秘密指定されるのか見えにくくなっております。審議の中でも、大臣は余り、何が秘密指定の対象になるのか御説明されておられないようです。

処罰範囲は、国民の代表である先生方から構成される国会が決めるべきです。そして、市民がその行動について予測可能性を持つことができるように処罰範囲はあくまで明確であるべき、これが罪刑法定主義という考え方でありまして、それは憲法三十一条に由来するわけであります。

法案は、どのような情報が秘密となり得るのか明確性を欠いており、罪刑法定主義の観点から大きな問題をはらんでいるというふうに考えております。政府の方は、官僚が作る運用基準で特定するんだということをおっしゃられているようですが、そうではありません。国民の代表者である先生方が基準を作らないといけないんです。それが罪刑法定主義であり、憲法の精神なのであります。

政府としては、政府から民間に提供した情報のみが対象となる、だから絞りがあるんだとおっしゃられるようであります。しかし、政府と民間の契約が締結される時点で、民間はどのような情報が来るのかというのは分かりません。既に知っていた情報、つまり、契約を結ばなければ秘密として扱う必要がなかった情報が来るかもしれません。さらに、国が民間の情報を義務として吸い上げて、少しだけ情報をプラスして民間に戻すかもしれません。

このように、元々知っていた情報、あるいは、企業から吸い上げて国がちょこっとだけプラスアルファして戻したような情報の漏えいが処罰範囲外であると言える根拠は条文上はないように思います。よって、秘密の絞りが十分とは思えません。

このような仕組みの下では、民間は、国に情報を上げたりするとかえって面倒なことになるので情報を上げないようになる、情報の共有が阻害されるということもあり得ると考えております。

三つ目でございます。適性評価の在り方でございます。

適性評価では、かなり機微な情報を国が取得することになります。渡航歴も問題になりますので、適性評価の対象者が自粛をして外国にも行けないということにもなりかねません。

中小企業では、クリアランスがないと、ほかにする仕事がなくて解雇という問題になるかもしれません。

あと、政府の方は、対象者から同意を得るからよいということをおっしゃられているようですけれども、調査対象となる親族や同居者は同意なく情報を集められるわけであります。決して、対象者は親族や同居者の同意を勝手にする権限を持っているわけではありません。本来は、同居者、親族からは同意を得なければならないはずであります。また、中小企業ですと、クリアランスがないと解雇される可能性がありますので、従業員としてはやむなく同意をするということもあり得るわけであります。

不服申立てについても、行政不服審査の対象ではありません。解雇につながるようなものであるのに非常に不合理であります。

情報監視審査会は適性評価を監督する権限を持っておりますが、独立公文書管理監はございません。そうしますと、法案では適性評価の在り方がきちんと監督されないことになりかねません。

企業の代表者についてクリアランスが必要かどうかという議論が有識者会議や国会でもなされております。代表者にもクリアランスが必要ということになると非常に大きな影響があるわけですけれども、このような肝腎な問題についても曖昧なままとなっております。

調査が一元的になされるというのも問題であります。犯罪を犯した疑いもない、犯す懸念もない多くの無辜の市民の機微情報を国の機関が一元的に収集する、そういう制度は日本の歴史上初めてなのであります。このような制度をつくるに当たって、どのようにその機関の権限行使の濫用を防ぐ仕組みをつくるか、これも全く議論されていない。これでは人権侵害に至る可能性が大きいと

言わざるを得ません。

最後に、民間企業に対する悪影響についてお話しいたします。

大川原化工機事件は、経済安保の名の下に捜査機関が暴走し、発生したものでございますが、同じような事件が発生する可能性は否定できないと考えております。大川原化工機事件の民事訴訟で敗訴した国は上訴しておりますし、担当検察官も謝罪していないようです。国は反省していないわけです。ひどい取調べがなされた事件でございますが、それを防ぐために取調べへの弁護人の立会いというのも有用でございますが、そのようなことも国は認めていないわけであります。

さらに、この法案についていきますと、秘密漏えいが刑事事件になった場合に、弁護人がその秘密を知り得るということが法案では全く保障されていないわけです。この法案でひっかけられて逮捕された人の弁護をしようとしても、何を漏らしたということで逮捕されたんですかというふうに被疑者に聞くことが許されるのかどうかもよく分からない。これでは人権が保障されるわけはありません。

こういうことを申し上げますと、民間は、新法で外国での取引や情報提供などの参入機会を与えられるからメリットもあるというお話もあるかもしれません。

しかし、この法案が対象としているコンフィデンシャル級につきましては、既にそのようなコンフィデンシャル級の秘密というのは、イギリス、フランスでは廃止されているわけですね。

アメリカでも、ＩＳＯＯというところが廃止を勧告し、二〇二一年時点でコンフィデンシャルのオリジナルシークレット指定権者は三人しかいないわけです。ＩＳＯＯが、同盟国でコンフィデンシャル級の廃止の動きがあるということで、省庁にコンフィデンシャル級をやめましょうというふうに言ったわけでございます。コンフィデンシャル級、一九九九年時点では、指定権者は二百六十人いたんです、それが今は三人です。二〇二一年でいうと、トップシークレットの指定権者は七百二人、シークレットは九百四十六人です。つまり、コンフィデンシャル級というのはほぼ絶滅しつつあるわけですね。

そのような、コンフィデンシャル級という非常にニッチなものを保護するためにわざわざなぜ法律を作らなければならないのか、非常に不明だと言わざるを得ません。そうしますと、法律を作って、民間企業の負担は増えたけれども、民間企業が国際案件に参加できるようになったわけでもない、そういう落ちもあり得るというふうに考えております。

以上でございます。ありがとうございました。

（拍手）

○星野委員長　ありがとうございました。

次に、大澤参考人にお願いいたします。

○大澤参考人　おはようございます。笹川平和財団の大澤と申します。

本日は、参考人として意見を表明する機会をいただきましたこと、心より感謝申し上げます。

私は、本日、両案につき、法案に賛成の立場から意見を述べさせていただきたいと思いますけれども、何よりもまず、サイバー安全保障の政策実務及び研究に携わる者といたしまして、民間にセキュリティークリアランス制度を導入するこの重要経済安全保障の保護及び活用に関する法律案の策定に際しまして、類いまれなるリーダーシップを発揮された高市早苗大臣及び政府・与党の関係者の皆様の御尽力に心より敬意と御礼を申し上げる次第でございます。

最初に、両案に賛成である結論の理由を簡潔に申し上げます。

第一は、安全保障環境の変化でございます。体制間競争の中で経済安全保障が重要になってきておりますので、民間も含めて情報の保全が求められる時代になっていると考えております。

第二に、私が専門としておりますサイバー安全保障の実務において、民間、特に重要インフラ事業者へのサイバー攻撃に関する機微情報の共有が死活的に重要になってきております。外国からの情報提供もありますので、情報共有のために情報を保全するということが必要になってきております。

第三に、個人的な過去の経歴の経験から、我が国の安全保障を確保する上で、機微な情報を扱う資格と情報の取扱いに関する教育を通じた取扱者の自覚というものが重要というふうに考えているからであります。

まず、第一の安全保障環境の変化でございますが、今、我々は、かつての二次大戦後の米ソの冷戦期のような、安全保障で厳しく対立し、スパイ映画ではありませんけれども、情報を守り、奪い合う、そういう厳しい体制間競争の時代に逆戻りしつつあるということであります。

これは、一九八九年以降の冷戦後の経済重視のグローバリゼーションの様相が大きく転換をしたということでありまして、米国では、二〇二一年に研究機関のアトランティック・カウンシルから発表されたザ・ロンガー・テレグラムというペーパーの中で、中国の長期戦略に対抗するという、米中体制間競争の時代に入ったという認識が共有をされております。

昨年五月の広島のＧ７サミットでも、経済的強靱性と経済的安全保障のコミュニケが採択をされております。その中では、経済的強靱性及び経済安全保障をグローバルに確保することは、経済的な脆弱性の武器化に対する最善の防御であるというふうに述べられております。この首脳宣言は、既に日本を含む西側社会が民間の経済をも巻き込む米中体制間競争のただ中にあるということを示しております。

参考資料にございますように、米国ではＤＩＭＥという概念が使われておりますけれども、外交、安全保障の確保に当たって、外交、情報、そして軍事、経済、この四つ全てを動員する競争が行われるわけでありますけれども、民間企業でも、安全保障において重要な意味を持つ情報の取扱いに慎重さが求められるということになります。今後の国際関係の時代の潮流を考えますと、民間をカバーするセキュリティークリアランスは時代の要請というふうに言えると思います。

第二は、サイバー安全保障の実務におけるサイバー脅威対策等に関して、基幹インフラ事業者との情報共有の重要性でございます。

サイバー空間は、近年、従来のサイバー犯罪とか情報窃取の段階から、重要インフラへの攻撃や情報戦と呼ばれるような国民の認知領域への攻撃など、安全保障領域としての対処が求められるような、国家が支援する主体によるサイバー攻撃が増大をしております。

その中でも、ここ一年の技術的な特徴といたしまして、参考資料の図に描いてありますように、国家に支援されたサイバー攻撃の手法が、従来の一本釣りの標的型攻撃から、一網打尽のネットワーク貫通型攻撃へと大きく変化をしております。この新しい攻撃技術は、組織のネットワークを防御しているネットワーク機器の脆弱性、いわば裏口に当たるようなところから攻撃者が侵入する手法でございまして、同じネットワーク防御機器を使用している企業、政府機関、これらが同時多発的に狙われるという攻撃を観測をしております。

参考資料の三枚目に、ネットワーク貫通型サイバー攻撃の昨年六月以降の日本における現状をお示ししておりますが、例えば、昨年七月に名古屋港のコンテナターミナルのシステム攻撃がされた手口は、上から二番目の米国製機器の脆弱性が悪用されております。このような点からも、港湾運送事業者が特定社会基盤に指定されますことは非常に重要なことというふうに考えております。

重要インフラ以外にも、ＪＡＸＡなどの先端技術が狙われました攻撃、医療機関へのランサムウエアによる攻撃、政府機関の情報を狙った攻撃が、いずれもこのネットワーク貫通型攻撃で被害を受けておりまして、詳細は申し上げませんが、いずれも国家が支援する主体によるサイバー攻撃の可能性が高いというふうに判断をしておりま

す。

また、ここ一年、攻撃側の攻撃実施の自動化が進んでいるというふうに考えてございます。脆弱性の公表から具体的に攻撃者がこれを悪用するまでの時間が、最短で二十四時間という短い期間で攻撃をされるという事例も観測をされております。そのため、ネットワーク貫通型サイバー攻撃から重要インフラを守るためには、脆弱性公表の前に情報共有を行って、このような裏口を防ぐという措置をリアルタイムで取ってもらうことが不可欠になってきております。

現行の体制では、参考資料に書いてございますように、民間事業者との間でセキュリティークリアランス制度がございませんので、政府機関で脆弱性の届出を受けましても、公表直前までこの脆弱性情報を民間事業者と共有することができないということが起きております。

また、被害対処とか不正アクセス届けの情報から、特定国の攻撃グループの犯行と思われるサイバー攻撃キャンペーンが見えてくることがございます。半導体産業や航空産業など特定の企業が狙われている、こういった分析の結果、サイバー脅威情報として我々、技術者とか政府機関が把握しているもの、また、外国からインテリジェンス情報として提供されるサイバー脅威情報、こういったものが、現状ではクリアランスがないために、標的となり得る企業に対してサイバー脅威の情報を共有することができずに、サイバー攻撃を事前に防ぐことができない、こういったことが起きてございます。

このため、一日も早く、民間にセキュリティークリアランス制度が導入されまして、サイバー脅威、攻撃に関する情報がスムーズに共有されることが、我が国のサイバー安全保障を確保する上で欠かせないというふうに思っております。

最後に、第三として、個人的な経験からも、民間において安全保障に関係する情報を取り扱う上で、機微な情報を取り扱う資格の認定と、情報の取扱いに関する教育を通じた取扱者としての自覚、これが重要だというふうに考えております。

私自身、民間のシンクタンクに現在おりますけれども、何回か、非常勤の国家公務員ですとか任期付の国家公務員として政策策定の実務に携わった経験がございます。直近では、二〇一四年の四月から一六年の十二月末まで、国家安全保障局に初代の民間任用局員として転籍出向しておりました。その際、資格認定を受けて、情報保全の教育を受けております。

近年は、安全保障政策を議論する政府の意思決定の過程に民間人が参入する機会というものが非常に増えております。私も実際に政策策定の現場で、素性の怪しい民間の方が現場に紛れ込むという事例も目にしておりますので、民間人の政策形成への参加の際に、安全保障の議論に際しては、セキュリティークリアランスによる資格認定が不可欠であるというふうに考えております。

大学卒業後から現在まで安全保障の研究をしておりますけれども、残念ながら、我が国の教育課程では情報を取り扱うという教育はなされませんので、どういうふうにして機微な情報を扱うかということに関しては全く教えられる機会がないということでありますけれども、どのように具体的に機微情報を取り扱うのか、そしてどのように注意をするのか、こういった教育を通じて情報を取り扱う個々人の自覚というものを持ってもらうことが、安全保障上重要な情報を今後我が国の中で守るためには大切であるというふうに考えております。

そのような点からも、民間へのセキュリティークリアランス制度の拡大を通じまして、自覚を持った方が民間企業にも増えていく、それによって社会全体の情報セキュリティーの感度が上がっていくということが強靱な社会をつくる上で重要であるというふうに考えております。

ありがとうございました。（拍手）

○星野委員長　ありがとうございました。

次に、三宅参考人にお願いいたします。

○三宅参考人　弁護士の三宅でございます。

専門は情報公開法と公文書管理法でございまして、学位論文も取らせていただきましたが、国のいろいろな役職を経て、最後は公文書管理委員会の委員長代理を務めさせていただきました。こういう情報公開法と公文書管理法に関する専門家からの立場として、今回の法案についての問題点を指摘させていただきたいと思います。

このような御発言の機会を与えていただいたこと、初めにお礼申し上げます。

私の意見の骨子は、メモに書いてあります三つでございまして、重要経済安保情報が、特定秘密保護法における特定秘密との区別が曖昧であるということでございます。これに対して、五年以下の拘禁刑又は罰金により処罰をするということは、罪刑法定主義の観点から問題があるということでございます。もう少し刑法学者の御意見も聞いていただきたいと思います。昨日、ちょうど審議がされているときに、日本弁護士連合会が主催で、この国会内で刑法学者の御意見を聞かせていただきましたが、後ほどそれについても触れさせていただきます。

それから、二つ目は、適性評価制度でございますが、現在も特定秘密保護法の適性評価制度で対象になる者が十三万人ぐらいいるということでございましたが、今回、重要経済安保情報の取扱いによる適性評価になると、この数はもっと増えるだろうと言われています。政府の最終取りまとめにおいても、アメリカでは四百万人、それからそれ以外の国で数十万人ということでしたから、日本でも数十万人に上るのではないかと思いますが、その人たちの機微な情報が政府に集められる、しかもその調査が内閣総理大臣の下で行われる、内閣官房にそういう情報が集まるわけでございますが、これにおけるプライバシーの保護ということをどう考えるか。私は、たまたま個人情報保護法の制定とかマイナンバーの制定にも関わりましたので、この辺については非常に懸念を持っているところでございます。

三つ目は、衆参両議院の情報監視審査会が特定秘密保護法にはございます。私も、二〇一九年に情報監視審査会で意見を述べさせていただきました。今日の資料の後ろの方の別表というところは、そのときの意見を少しつけたものでございます。それは後ほど参考にしていただければと思いますが、七ページ以下でございます。今回の法案には、この情報監視審査会に対する対象になっていないというところは、これはもう根本的な問題でございまして、こんな法律は出し直していただかないと政府法案としては不十分であると考えておるところでございます。

以上の点をもう少し詳しく説明しております。

先ほど来の参考人の意見の中にも、今回の法律はコンフィデンシャルの情報を対象にするものだということが言われていましたし、政府の昨日の委員会答弁でも、コンフィデンシャル級という言葉が説明されていました。この、級というのがどうもみそですね。衆議院内閣委員会の参考資料を送っていただきました、この三十ページの特定秘密と重要経済安保情報の横に、トップシークレット級、シークレット級、コンフィデンシャル級、こういう分け方がしておりますけれども、今回の法律は各省庁におけるトップシークレットとシークレットを含むものであることは明々白々でございます。

実は、特定秘密保護法が制定される際、その頃、私は公文書管理委員会の委員長代理になる前の委員でございました。それで、特定秘密保護法ができたすぐ後に公文書管理法を直すということを始めたわけでございます。その中で、秘密文書と秘文書というものを行政文書の管理に関するガイドラインの中に入れるということにしました。

その関係がどうなるのかということをずっとその後もウォッチングしてまいりましたが、例えば、令和二年の独立公文書管理監の報告書の中では、令和二年六月十九日の報告書の中では、特定秘密を保有する省庁は十四省庁、国家安全保障会議、内閣官房、内閣法制局、内閣府、警察庁、総務省、消防庁、法務省、外務省、文部科学省、経

済産業省、海上保安庁、防衛省、防衛整備庁、この十四で、秘密の件数は三千八百七十八、延べ件数が五千二百六十九。これ以外の省庁でトップシークレット、シークレットがないなんということはあり得ません。

ただ、十年の拘禁刑が科せられるような特定秘密の法律の対象になる省庁になりたくないという省庁がたくさんあるということを当時も聞いておりました。そのために、公文書管理法を直して、整備して、行政文書管理ガイドラインの中で秘密文書と文書というものを明確にしたわけでございます。そのときは、コンフィデンシャル情報というのは、いわば、事実上、取扱注意という判こが押されるようなものだったということで理解しています。

そういうことからしますと、政府の最終報告を踏まえた今回の法律のトップシークレット、シークレット並びにコンフィデンシャルに関する法律の仕分というものは前提から間違っているということでありますので、ここの点は出直していただきたいと考えているところでございます。

それから、コンフィデンシャル情報というのは、実は、情報公開法を一九九九年に作って、二〇〇三年に見直しの検討会がありました。私もその見直しの検討会の委員でございまして、この場合には、情報公開法五条二号ロで、公にしないとの条件で任意に提出されたものについても、当時の状況等に照らして合理的であると認められるもの以外は原則開示義務があるという、ここの基本から考えていただかなきゃいけません。

基本は、民間における情報流通こそが経済発展に資するんだと。ただ、昨今の世界における状況の中で、サイバー攻撃等、先ほど御指摘がありましたが、そういうものについての秘密として整備しなきゃいけないということであれば、その例外である、例外的措置であるというような観点から、経済基盤保護情報について原則開示義務の例外としての取扱いというようなことが、最終報告では全く欠けております。情報公開法でこれが請求されるときにどうなるのかというようなことも議論しなきゃいけないところだろうと思います。

それから、先ほど申しました、セキュリティークリアランス制度に関する、適用対象になるものが大変多いということについては、私のメモの四ページのところに、線を引いたところでございますが、特定秘密保護法でさえ十三万人、保有者の比率が、官が九七、民が三％。今度はここに、コンフィデンシャルの情報で民の部分がかなりの部分が上がってくるわけですから、恐らく十三万を超えることになると思います。そういうものに対して個人情報をどうやって保護するのかということがとても大事になると思います。

しかも、数年前には、デジタル社会形成法とデジタル庁設置法によって、内閣総理大臣の下に全てのデータが集められることが可能になった、そういうところでございます。

一つの例で申しますと、今日は、岩波新書、「学問と政治」というのを持ってまいりました。これは、学術会議の任命拒否で、六名が任命拒否されたもの。ここの岩波新書の帯に書いてあるこの書面は、九月二十四日付、外すべき者、副長官。副長官に、外すべき者六名を集めるための、データが集められたんですが、私どもが情報公開請求をし、本人情報開示請求をしたところ、情報公開ではここしか出なかった。議会でもここまで御協力いただきました。その後、それぞれ一人ずつが開示請求をしてきたら、自分が書かれているという六名の方が一人ずつ個人情報保護法に基づく本人情報開示請求で出て、しかも、この九月二十四日が、六月から内閣官房と事務局の間でやり取りしているということまで分かりました。

個人情報の取扱いというのは、それほど機微なものが現に内閣官房で明らかになっているということでございますので、今回の問題については特にその辺について慎重に検討していただきたいと思います。

もう時間になりましたので、あとは御質疑に委ねますけれども、情報監視審査会というものを育てていただきたい。ここで審議をすることによって特定秘密も制約されていました。ここに重要経済安保情報が対象にならないというのは、これはおよそ、この法案の不備な点の最大のところでございますので、こういうものは出し直していただきたい。そうでないと、今日必要性を唱えられた方々についても不十分な意見にすぎないということになろうと思います。

ありがとうございました。（拍手）

○星野委員長　以上で各参考人からの御意見の開陳は終わりました。

○星野委員長　これより参考人に対する質疑に入ります。

質疑の申出がありますので、順次これを許します。中山展宏君。

○中山委員　自由民主党の中山展宏でございます。

今日は、法案審議に当たり、貴重な御意見を賜りました。ありがとうございました。

時間の関係もありまして、お一方ずつ質問をさせていただきます。

まず、渡部参考人からお願いをいたします。

いわゆる研究インテグリティー、研究公正と研究セキュリティー、研究安全保障についての両立、整合性に大変腐心されたと思いますが、その点について御所見をいただきたいのと、先ほど、情報管理について、官民協力のエコシステムが育まれることが重要であるとおっしゃっていただきました。民間のホルダーがそのエコシステムにどのように貢献されると期待されておられるか、御説明いただきたいと思います。

○渡部参考人　御質問ありがとうございます。

セキュリティー・アンド・インテグリティーについては、今回議論しているセキュリティークリアランスの対象になるリストリクテッドリサーチの外側ではありますけれども、これは実は、先ほど言いましたクリアランスの内と外のエコシステムという意味でお話をいたしました。

これは日本も合意いたしましたけれども、G7で最近、このセキュリティー・アンド・インテグリティーの考え方については、統一的な考え方、プリンシプルを発表し、そのベストプラクティスも出されています。

基本、ここで言われているのは、何が大切かというと、学問の自由とかそういうことは大切なんです、その大切なところにバッドフェースアクターがオープンな環境を利用して知財の窃盗とかをやるのを防がないといけないのでセキュリティーが必要だ、そういう構造になっています。

そのために、いろいろな施策の中で、実行部隊としての例えば大学、研究機関がやるべきことしては、デューデリジェンスを一番筆頭に挙げている。これはバックグラウンドチェックとは違います。例えば、オープンソースデューデリジェンス、あなたがつき合おうとしている人たちあるいはその機関はどういう人なのか、あなたは分かってそれを説明できますかということをオープンソースの中でも説明をしてくださいというようなことであります。これは非常に重要だと思いますし、当然できること。

ただし、オープンソースであっても、それをやるときに、やはりバイアスのかかったような調査をしてはいけないとか、そういうガイドラインもつけてそれをやるようなことを、政府の方でガイドラインを作ってほしいというようなことを申し上げたいと思っております。

それから、先ほどのエコシステム、今申し上げましたが、セキュリティークリアランスホルダー、アメリカの場合は四百万人もいますので、この人たちは、実は、例えばセキュリティークリアランスホルダーの期間を経てまたファンダメンタルリサーチに行ったりとか、行き来をしています。この人たちはここの部分を分かっているので、本当に、基礎研究をやるときに、ここまでやったら機密研究になりますよというのは分かっている。そういう人たちが要所要所にいること

で、それで健全な、ある意味、公開の研究もできるし、本当にこれは秘密にしないといけないことができる。

我が国の場合はそれがなかったので、どこまでいっていいか分からないとか全部グレーだとか、そんな感じになっていたんじゃないかというふうに感じます。アメリカで取材しますと、そういうようなことを感じました。

以上でございます。

○中山委員　ありがとうございます。

続いて、境田参考人にお願いいたします。

今次のセキュリティークリアランス制度は、同盟国、同志国と機能的に適合しているかどうか、いわゆる通用するかどうか、情報のクラシフィケーションが同等のものになっているかどうか、そういう観点からお話をいただきたいのと、科学や研究領域における知財、機微技術情報、エマテク情報のサプライチェーンをどのように制御していくかという上において、セキュリティークリアランス制度以外の何か方策があるかどうか、アイデアがありましたらお教えいただきたいと思います。

○境田参考人　まず、同盟国、同志国の制度と整合させる、これは今も、特定秘密保護法におきましても、その分野においては、同盟国、同志国と連携しながら情報の共有などができる仕組みになっていると理解しておりますが、今般のこのセキュリティークリアランス制度ができた暁におきましても、同様の、同盟国、同志国との連携ができるような、これは政府の努力が必要だと思うんですけれども、それが必要だというふうに考えております。

それから、あと、やはり、研究に関するインテグリティーというか、知財をどうやって保護するか、これは非常に重要なところです。御案内のとおり、去年、産総研の中国人研究者の漏えい事件というのが起きましたけれども、企業とか大学とか国立研究開発法人の立場から立つと、基本的に研究というのは、自由に、グローバルに、いろいろな世界のトップ研究者と一緒にするというのが重要なんですが、他方、そういう中に実は各国のそういう工作員だったり技術情報を盗もうとしている人が紛れ込んでいるわけで、そこのクリアランスというのがなかなか難しいという状況があります。とはいっても、個人のバックグラウンドを組織としてなかなか把握することができないという課題があります。

それから、あとは、日本というのはやはりインテリジェンス情報というのになかなかアクセスできないというのがあって、その人がこういう背景があるというのが分かっていても、そこがどういうリスクがあるかも実は研究機関としては分からないんですね。なので、できれば、そういうインテリジェンス情報をきちっと契約の下に入手できるようなそういった公的なサービス、これがあれば、より安心して研究ができるようになるのではないかというふうに考えております。

○中山委員　ありがとうございます。

先ほどSP800―171の話にも触れていただきまして、今、社内デカップリングということも、企業において研究環境のデカップリングということも様々なところで議論はされていると思いますが、なかなか、実装に向けては非常に配慮しないといけないところもあると思いますので、また御指導をいただければと存じます。

それでは、齋藤参考人、お願いをいたします。

このセキュリティークリアランスのホルダーになられた方の人生においての影響というか、また、その施設、民間事業者、組織の影響、これは様々あると思いますが、弊害の部分も多少なりともあるんだと思います。それを低減する方策はありますでしょうか。

○齋藤参考人　ありがとうございます。

ホルダーになった方の人生に対する影響ということでございますけれども、まさにおっしゃられたとおり、先ほども申し上げましたけれども、例えば、海外渡航というものが調査項目に入ってくるということになると、なかなか海外旅行も行けない。そして、例えば、配偶者の国籍だけで排除はしないんだというふうには言われているけれども、やはり重要な要素であるようにも思われるので、結婚の自由も侵されるかもしれない。

そして、組織に関して言うと、社長さんあるいは取締役会議長が本来であればセキュリティーの対象になるとか、経営陣に対するセキュリティーというのもアメリカ的にいえば本当は必要なんだろうということになってくると、あとは株主の国籍とかも調べるということになると、今のような国際的に事業をやっている会社が多いという状況の下では経営的にも非常に困難だということになるんだろうと思うんです。

組織的な問題については、あくまでそれを、少なくとも今回の法案でいえば、情報を受け取りたい、クリアランスの対象になるかどうか、自分たちはデメリットがあっても受けたいという会社が自己判断すればいいんですけれども、対象となる個人については、有識者会議の中では、例えば国が十万円報酬を払うとか、そういうことも議論されていました。もう一つは、例えばそういう制度を導入する前に労使協定を必須化するとか、そういう方策も検討する必要があるんだろうと思っております。

ありがとうございました。

○中山委員　ありがとうございます。

ホルダーになりたくないというような動機が生まれないように、これはしっかりこの委員会でもその懸念については議論をさせていただいた上で、払拭していきたいと思います。ありがとうございます。

大澤参考人、お願いをいたします。

今次、重要インフラが、十四分野から、港湾の分野も含めて重要インフラとして指定をさせていただくことになりますが、議論の中で、港湾から更にほかの領域、ほかの分野、私はかねがね、いわゆるプラットフォーマーであったりとか医療分野であったりとかということ、議論もされておりますけれども、そういったことの必要性をどのようにお考えかをお伺いしたいと思います。

それから、サイバーセキュリティー、データセキュリティーの上で、これは通信の秘密に関わりますが、シギント、いわゆる通信における情報活動、諜報活動というものの必要性は感じておられるかどうか、お伺いしたいと思います。

○大澤参考人　中山先生、ありがとうございます。

まず、基幹事業者の指定の拡大についてでございますが、これは多分、その基幹事業者がサプライチェーンでボトルネックになるか、そして代替性があるかどうかという視点から考える必要があろうかと思います。医療機関ですと代替性が利きますので、一つの医療機関がサイバー攻撃を受けてもその周辺の機関がカバーをするということが可能になりますので、仮に、その地域でもうそこしかない、それが潰れると代替性がないということであれば、指定の拡大というものは検討していく必要があるだろうというふうに思います。

それから、シギントの必要性でございますけれども、我が国は、恐らく諸外国の中で唯一、インターネットでシギントの収集ができない国だというふうに考えております。これは、現在、サイバー安全保障法制を政府の方で検討されておりますけれども、サイバー攻撃に関する情報、特に攻撃者に関する情報はシギントを得ないと攻撃者の特定ができませんので、そういった点では、インターネット上のシギントというものは安全保障を守る上で必要であるというふうに考えております。

ありがとうございます。

○中山委員　ありがとうございます。

これも議論を深めないといけないところだと思っております。さらには、ダークウェブでの取引について、関与というか監視ができる環境についてもしっかりと行っていかないといけないと思っております。

三宅参考人、お願いをいたします。

参考人は、情報は民主主義の通貨、公文書管理

は民主主義の基盤とおっしゃられて、そのとおりだと思います。

今、環境の変化、世界の安全保障環境の変化もあって、米国のＣＦＩＵＳ、対米外国投資委員会は、我が国もそうですけれども、インバウンド投資、対内投資に関しては審査を行う環境になっています。他方、アウトバウンド投資、対外投資も、安全保障に資する対外投資を行うということが今議論されているかと思いますが、情報においても、その行き来において制御をする必要性はあると思います。

その中で、先ほど参考人からの御懸念も伺いましたけれども、情報の制御は、例外的な規定ということではなくて、能動的に私たちが制御をしていく、安全保障に資する情報の共有の仕方、また保護の仕方、活用の仕方、こういった考えに基づくというところで今般の法案は議論されていると思いますが、能動的に情報を管理していくことについて御所見をいただければと思います。

○三宅参考人　私も、経済安保情報についての保護が要らないという立場ではございません。能動的に管理をするということは、それは当然あり得ることだと思いますが、先ほど来申しましたように、それが国の情報法制の根本、情報公開法、公文書管理法との関係において、いささか整理が不十分ではないかということはありました。

もう一つ、先ほどの説明につけ加えますと、例えば特定秘密保護法の中のテロ、スパイ等の部署のところには、サイバー攻撃に対して対応するということは運用基準の方で整理されて中に入っておりますが、そもそも、そういうようなものを活用しないで、今回、そういうことの検討を、この十年のレビューもしないでこの法案が作られているのではないかということで、いささか、情報監視審査会でこの十年積み上げてきた議論が軽視されているのではないかと。あの委員会は本当に重要な委員会だと思います。それで、大きく育てていかなきゃいけない委員会だと思っております。

そういう意味で、これは適性評価についても不利益を受けないというようなことを情報監視審査会でチェックをするということが当然できることになっていますが、今回、能動的とおっしゃる割には、そういう、特定秘密保護法のときに議論の末できた情報監視審査会の制度などがすっぽり抜けているということが一つでございます。

それから、私、今日、六ページの最後に福田元総理大臣のお話を引用しておきましたけれども、国の歴史をつくり上げていくのがこの公文書だ、公文書は、石垣を積み上げて基礎をつくり、その上に城を築く、国で作成した文書、資料が歴史をつくっていく、そのパーツが公文書なんだと。

ですから、重要経済安保情報も、政府が作成又は取得したものは行政文書になりますから、この法案の四条六項などはとても大事なところですね。余り議論されていませんけれども、重要経済安保情報が国立公文書館に移管されて将来チェックされるというようなシステムまで入れていただいている点は、こういう国の歴史の在り方、石垣という言葉にある、そういうものの重要性ということを踏まえていると思っておりますので、そういう点は尊重しながらもう一度作り直していただきたいというのが私の立場でございます。

○中山委員　ありがとうございました。

済みません、以上です。

○星野委員長　次に、太栄志君。

○太委員　太栄志でございます。どうぞよろしくお願いいたします。

五人の先生方、参考人の皆さんにおかれましては、高い御見識からの御発言をいただきましたこと、まず心から感謝申し上げます。

それでは、早速質問に入ります。

まず、三宅先生にお伺いしたいと思います。

三宅先生、今も御発言されました福田元総理の御発言を含めて、公文書の、あるいは情報管理の大切さということを御教示いただきましたが、先生、冒頭の御発言の中で明確におっしゃいました。この法案の最大の問題というのは、まさに衆参の情報監視審査会、この審査手続がないこと、根本的にこれが問題だということで御発言をされました。

実際、重要経済安保情報を特定秘密と同様に情報監視審査会の対象とすることに政府として不都合はないということを、昨日、この内閣委員会におきまして高市大臣が御発言をされましたが、もちろん、先生、先ほど来、この大切さ、しっかりと対象としていくべきだと御発言されていました。

それでは、ちょっと視点を変えて先生にお伺いさせていただきたいのが、例えば、もし情報監視審査会の対象としなかった場合にはどんな問題が生じてくるのか、その点に関して、先生の御見解をお聞かせください。お願いいたします。

○三宅参考人　対象にしなかったことでどういう問題が出てくるのかということは、逆に言えば、十年間で、対象にしたことによってどんなことが分かったのかということをお話しすればよろしいかと思います。

例えば、私、この資料の中に少し入れておきましたが、別紙の七のところでありますが、法制定当時は、保存期間一年未満の特定秘密が年間で四十四万件を超えて存在する。一年未満で廃棄される特定秘密が四十四万件あるわけですよね。一年以上ということでずっと保存されていく、特定秘密は五年、五年、五年、五年ということでいきますし、今回の重要経済安保情報も五年、五年、五年というような形で、特定秘密保護法の枠が、同じようにつくられていますけれども、情報監視審査会があればこそ、そのようなことが分かったわけでございまして、果たして一年未満で廃棄されるものが四十四万件もあっていいのだろうかということが言えると思います。

それからもう一つ、指摘のところで申しますと、十ページのところに、適性評価の実施に当たり、評価対象者が不同意とした場合や、評価の結果不適格とされた、不利益を受けないことを担保する制度を設けるべきだということで、これはまだ、情報監視審査会でもこういうことまで十分な審議はされておりませんけれども、やはり、膨大な個人情報が内閣に集められて、それがどういうふうに運用され、あるいは漏れるかということは、国民にとっては最大の関心事でございます。

先ほど、学術会議の委員の例をお話ししましたけれども、これは一般市民にとっても同じようなことが言えるわけでございまして、セキュリティークリアランスの対象になる人についてこういうことが起きたときに、苦情申立ての制度だけでは不十分だと。今でも情報監視審査会では苦情申立てが若干あるような報告がありますけれども、報告書、特定秘密保護法についての報告を見ているだけでもまだまだ不十分ですが、しかし、情報監視審査会があればこそ、これから改善の余地があります。

そういうところも、秘密会があれば政府に情報を出しますよということがよく積極派の方々に言われますが、やはり常設の委員会として情報監視審査会があるというのはとても大事なことでございます。

今言った二点が、今回、この制度の中で情報監視審査会が制度となっていないことの大きな問題点と逆に言えると思います。

以上でございます。

○太委員　先生、どうもありがとうございました。明確に御答弁いただきまして、今後の審議にしっかりと生かさせていただきたいと思います。

次に、齋藤先生に質問させていただきます。

先生が、どのような秘密が指定されているか不明確であるということ、国民の代表である国会でしっかりと処罰範囲は明確にすべきだ、官僚が作る運用基準で特定しても不十分だということ、本当に大いに賛同させていただいた次第なんです。

先生にいただきました資料の、一月の報告書ですか、そこにも記載があります。適正な秘密指定がなされているかどうかをチェックするために政府から真に独立した機構をつくることが大事だということなんですが、ここをもう少し具体的に教えていただけますでしょうか。お願いいたしま

す。この後の兼ね合い、関係で。

○齋藤参考人　ありがとうございます。

ごめんなさい、真に独立したというのは、秘密指定についてのということですね。（太委員「そうですね、これとどう関係してくるのか、含めてお願いします」と呼ぶ）はい。

秘密指定についてきちんとチェックするところが必要だというのは、今は独立公文書管理監というものがございますけれども、ノーリターンルールというものが適用されない。ですから、どうも見ていると、最高検の検事さんとかがやってきてまた戻っていくみたいな形で、腰かけみたいな形でやられているんだと思うんですね。

ところが、ＩＳＯＯというアメリカの秘密指定解除に関わる機関のトップは、例えばＣＩＡとかから人がやってくるわけですけれども、そういう人は戻らない。戻らないから腰かけではないわけですね、一生懸命やるわけですね。

やはり、どこかからやってきてまたどこかに戻るということになると、自分の出身の省庁のことを忖度するというのは人情としてあるんだろうと思うんです。でも、ＣＩＡからやってきて、ここに骨をうずめるんだということであれば覚悟もできる。しかも、知見もあるわけですね。そういう知見と覚悟を使ってチェックをするということが、ノーリターンルールを作れば可能なのではないかと思っています。それが、独立した第三者によるチェックというのは、最低限そういうノーリターンルールによる、そういう人事体制が取られた機関によるチェックが必要だろうということだと思います。

ちなみに言うと、情報監視審査会も、そういう意味では第三者機関性はあるとは思っているんです。ただ、三宅さんがおっしゃられたように、非常に情報監視審査会は重要なんですけれども、毎年、情報監視審査会、衆議院、参議院は報告書を出しておりますけれども、見ておりますと、やはり独立公文書管理監や行政の対応が非常に不十分だということを毎年おっしゃられているようです。例えば、特定秘密については情報監視審査会に出さなきゃいけないということになっているけれども、それ以外の秘密もちゃんと出してくれというようなことを毎年報告書の中で言われているようです。

ということは、逆に言うと、余りちゃんと出してくれない。つまり、行政の方が情報監視審査会の先生方にきちんと情報を出さないということがあるんだと思うんですね。

あとは、特定秘密を提示することを求めるについては、過半数の決議がないと提示を求められないということになっていますので、そうすると、なかなか簡単には特定秘密を出せというふうにも言えない。

そういう意味では、情報監視審査会も非常に重要な機関ではあるけれども、もうちょっと改善の余地がある。そこら辺も、もうちょっと今申し上げたところを改善していくと、第三者機関として秘密指定をきちんとチェックできるものになる可能性はあるだろうと思っております。

ありがとうございます。

○太委員　先生、ありがとうございました。

では、次に移りたいと思います。

次に、境田先生にお伺いしたいと思います。

先生が最後にお話しされた中で、今回の法案で産業界が一番期待していた部分、まさに一番ニーズがあった部分で、残念ながらそこが十分に期待に沿えなかったという先生の御発言がありました。民間保有の情報であるＣＵＩですが、ここに関して、今回、今、法案審議が進んでいますが、今後どういった形で、国会に期待していくのか。

それと、なぜ今回、これだけ重要な、私も、ほかの有識者会議のメンバーの方からも、やはりここが一番進まなかったという、先生と同じ御意見をいただいたんですが、なぜここをうまく盛り込めなかったのか、障害があったのか、その点に関して教えてください。お願いいたします。

○境田参考人　御質問ありがとうございます。

私が先ほどのお話の中でさせていただきましたとおり、本当に今、日本の国もそうですし、企業も、恐ろしいほどのリスクにさらされている。リスクというとあれなんだけれども、実は犯罪行為なんですよね。海外からのサイバーテロというのは犯罪なんですよ。情報を盗まれ、重要技術を盗まれ、ノウハウを盗まれ、企業が潰される。場合によっては日本国もダメージを受ける。国内だったらまだ刑法で及ぶところもあるんだけれども、海外からのアタックというのはそれができないという、とてつもない危機に企業の経営者はさらされているわけです。企業は、当然、警察権、そういう行使もできないし、強制的に何か開示もできない。何とかしてくれという話があるわけです。

その中で、今回のセキュリティークリアランスの法案、重要経済安保情報の保護、これも実はすごく大切で、これができることによって、施設クリアランス、組織クリアランス、人のクリアランスができるわけで、すごくありがたいんです。

でも、これはあくまでも国から情報をもらうときの要件というか、そういう効果なので、そうではなくて、元々自分が持っている重要情報をどうやって管理するのかということを考えたときに課題が山積している、これが実はＣＵＩの制度なんだ、こういうことなんだと思います。

なので、ＣＵＩをどういうふうに守るかというと、ＣＵＩというのは恐らくアメリカでもかなり数が多くて、これはアメリカも国が、政府がバックグラウンドチェックをしているわけではありません。でも、先ほど言ったＳＰ８００―１７１という基準によっていろいろなチェックをしているわけで、それと類似の制度を日本でも導入すべきだ、こういうのが恐らく産業界、特にグローバルで活動されている企業の方々の御意見だというふうに思っております。

○太委員　どうもありがとうございました。

ちょっと時間がありませんので次に移りますが、大澤参考人と、また境田先生の方にお伺いしたいと思っております。

今回、セキュリティークリアランス制度が導入された後、まさに我が国として、同盟国であるアメリカだけじゃなくて、同志国、ほかの国々とも様々な連携というのが期待されると思うんですが、まさに、ファイブアイズやＡＵＫＵＳも含めて、今後どういった形で、連携の在り方、可能性が見えていくのか、国際的な枠組みとしてどういうふうに進んでいくべきなのか、その点に関しての御見解をお聞かせください。お願いいたします。

○大澤参考人　太先生、ありがとうございます。

特に、このセキュリティークリアランス制度が導入されますと、サイバー面に関しては、今後、第六世代というか、次期支援戦闘機の共同開発とか装備品の共同開発がなされると思いますけれども、こういった当該国、連携国から、日本の防衛産業のサイバーセキュリティーを守るために攻撃情報を共有したいという意見を寄せられております。

ただ、彼らが気にしておりますのは、情報を渡したときに有効に活用されるのか、また、情報がちゃんと保全されるのかというところを気にしておりますので、そういう点では、諸外国ときちっと同等の制度をつくって、情報交換、脅威情報の交換がシームレスに行われるようになるということが期待をされるというふうに考えております。

ありがとうございます。

○境田参考人　ありがとうございます。

本当に同盟国、同志国との連携というのが不可欠で、私、先ほど申し上げましたように、日本の政府もそうかもしれないし、あと、企業は、様々な犯罪に今巻き込まれているというか、被害に遭っているし、遭おうとしている。これは実は、海外の同盟国、同志国の企業とか政府も同じなんですよね。海外政府がサイバーアタックに遭うということはよくあります。それから、海外の企業が、これによってインフラが停止したとか、甚大な被害を受けたとか、そういう財産的被害を受けたというのは枚挙にいとまがないわけで、これを同盟国、同志国、それからそういった企業が連携

してそれに対応しなきゃいかぬ、こういうふうな切迫した事態なんだというふうに思います。

なので、これはもうファイブアイズもＡＵＫＵＳもそうですし、そういったところに、今まで実は、セキュリティークリアランス制度がないために、日本は参加できなかったんですよ。これは日本の国を、非常に困難な状況に陥っていた一つの原因なので、この原因を除去してもらうというのは私は重要だというふうに思っております。

以上です。

○太委員　どうもありがとうございました。

時間になりました。先生方、御知見をいただきまして、どうもありがとうございました。

○星野委員長　次に、堀場幸子君。

○堀場委員　日本維新の会・教育無償化を実現する会の会派を代表しまして、本日、先生方に御質問をさせていただきたいと思います。

今日は、本当にたくさんのお話をありがとうございました。もう十分ではなくて、もっともっとたくさんお話を聞きたいところだったんですが、そして、質問時間も十五分しかないということで、思い切り聞けるかどうかなというのが心配なんですけれども、始めさせていただきたいと思います。

私たちの会派というのは、このセキュリティークリアランス法案もそうなんですけれども、ハイブリッド戦争という時代において、サイバーとか宇宙とか無人兵器とか、そういった様々な、今までとは違う新しい時代に来たという認識に立っております。それは当然なんですけれども、それと、一方で、新しい国際秩序を経済安全保障という分野で構築していきましょうということを二年前の経済安全保障の法案のときもさせていただいてきたところでございます。そして、私たちとしては国際的なインテリジェンス体制についても言及をさせていただいておりますし、これを機微情報の流通のインフラとして捉えるということをさせていただいているのが我が会派でございます。

その視点に立ちまして、少し御質問をさせていただきたいと思います。

まず、大澤先生に、私は、この法案でつくるセキュリティークリアランス体制が本当に国際的に互換性があるのか、これが一番気になっているところなんですけれども、大澤先生の御所見をお願いいたします。

○大澤参考人　堀場先生、ありがとうございます。

私が、例えば欧米諸国のカウンターパートとこのクリアランスを持っているか持っていないかという話をした感じからしますと、やはり日本の制度と同じような教育ですとか情報のクライテリアを持っていますし、相手も、クリアランスを持っているよねということが確認できると、情報の会話の中身の濃さというのは一段上がりますので、そういった経験からしても、現在の特定秘密保護法もそうですし、今回の民間へのセキュリティークリアランスの拡大も国際基準にのっとっているというふうに考えております。

○堀場委員　ありがとうございます。

国際的な互換性がなければこの法案を一生懸命やっても余り意味がないなというところでございますので、細かいところを見ていくと、本当に大丈夫なのかなと。例えば、調査の項目が七項目、アメリカは十三項目ですよね。そういったところもありますし、様々なところでちょっと不安があるんですね。これは、どんなシステムを構築するのかということも非常に重要なんだろうというふうに思っております。

渡部先生に少しお尋ねをさせていただきたいんですけれども、やはり先生のお話の中でも、他国との同等性というお話がありました。なので、この部分をもう少しお伺いしたい。例えば、具体的にこういう点が他国との同等性というものがあるんじゃないかなということをお一つお聞きしたいのと、先ほど話題になっておりましたけれども、この法案の中には入っていないＣＵＩについてもデュアルユースのところで本当に重要になってくると思いますので、そこに対する御所見もお願いしたいと思います。

○渡部参考人　御質問ありがとうございます。

他国との同等性、それがないと意味がない、全くおっしゃるとおりです。

ここまで検討してきた中で、あるいは特定秘密、その運用の内容は我々は知り得ないんですけれども、そういうのをベースにして、今の形であればこれは情報共有の基盤になるだろうということなんですけれども、一方、例えば、項目が何か、もうちょっと明確にみたいな話はよく出てくるんですけれども、アメリカなんかは、実は余り、そんなにはっきりしたことは書いていないんですよね。経済安全保障に関係するところでいえば、安全保障に関する経済的、技術的、科学的だったかな、何かそういうような情報というようなことで、これは、余り細かくしてしまうと、かえってそこは同等でなくなってくるというか、幅を狭めてしまう。

実は、以前、経済安全保障法の中で特許非公開に関しても、我々はまとめもやらせていただいたんですけれども、これも各国で元々ある制度なのでそれほど細かいことは書いていないんですが、日本の場合は、予見可能性ということをかなり言われましたので、かなり細かく、ＩＰＣ分類番号も書いてあるんです。これは、本当の意味でよかったかどうかというのは、実は、各国との関係でいうと、若干逆の部分もあるかと思います。

日本の場合は、今までにないものを入れるのでそういうことになるんですけれども、今回の場合も、ないものを入れるので、いろいろやはり、そこに、明確化したいというのは当然だと思いますが、その部分で、余りやり過ぎると逆に同等性がなくなってしまうというようなことがございます。

それから、ＣＵＩなんですけれども、これは、アメリカの制度でもＣＵＩの運用というのは若干課題があるというふうに言われていまして、各省庁でかなりばらばらだったりとか、そういうのをそのまま入れるということではなくて、我々としては、足下で、今、経済安全保障の施策で、重要インフラ、特定物資、いろいろな支援をしていく中で、そこで出てくる情報、これは民間の営業秘密で、守ってくださいということになるわけだけれども、やはりちょっと特段の考え方を持った方がいいのではないかなというふうに思います。

そういう意味では、先ほどのデューデリジェンス、これはどちらかというと大学のアカデミアみたいなものを対象としていますけれども、そこにガイドラインをきちっと作って、人的な面でも、どういう考え方をするのか、人権侵害になるようなことのないようにというのをちゃんとガイドラインで示すということは重要ではないかというふうに思っております。

以上でございます。

○堀場委員　ありがとうございます。

互換性のためには余り細かく書いちゃいけないというところもすごく今勉強になりましたので、それも併せてやっていきたいなと思います。

境田先生にお尋ねさせていただきたいと思います。

私は、この法案でできるシステムというものが国際的なインテリジェンス体制を構築する一歩目になるようにというふうな思いを込めています。先生のお話の中で一元化ということがあったと思うんですけれども、それについてもう少しお詳しくお願いしてもいいですか。

○境田参考人　企業とか大学とか国立研究開発法人の立場に立ちますと、今までは、恐らく研究者の情報をきちっと、情報管理の観点から厳密にするということはなかなかハードルが高かったわけで、これを今、まさに政府の指導もあって取り組んでいるんですが、それだけでは足りなくて、そういう様々なインテリジェンス情報と組み合わせてリスクチェックをしなきゃいけないわけですね。

ただ、これは言うはやすく行うは難しで、実際、じゃ、誰がどうやってそういうインテリジェンス情報、機微情報を入手するのか、それをどう

いう条件でそのニーズのある企業とか大学とかに渡すのかというのは、これはかなり工夫が必要だと思っておりまして、いろいろな類似の制度、例えばサイバー攻撃などは、恐らく国のあるどこかの機関に情報が、警察でなくて、サイバーセキュリティー対策、済みません、名前が明確でないんですが、そういったところに情報が集まるような仕組みがあって、そこと連携するという仕組みがあるやに聞いていますが、そのような仕組みをこれから構築することを検討していただければというふうに思っております。

○堀場委員　ありがとうございます。

私たち、こういう、本当に体制をつくっていくという懸念とともに、この法案に一つ二つ、私は本会議登壇でも質問をさせていただいておりまして、やはり憲法との関係性ということで、先ほど先生方おっしゃっておりましたけれども、秘密を指定することと知る権利の関係性であったり、適性調査における個人情報の保護の関係であったり、秘密が何か分からないということが罪刑法定主義に対してどうなんだみたいなことというのは問題意識として持っているんですけれども、齋藤先生に少しお尋ねさせていただきたいなと思っています。

やはり個人情報等を保護することは当たり前なんですけれども、それをしっかりと明確にしていく必要性があるかなというふうに思っているんですけれども、先生のこの法案全体に対する、一つ一つ、憲法との関係性に対する御所見をもう一つお願いいたします。

○齋藤参考人　ありがとうございます。

今お話しいただきましたけれども、適性評価で集められた個人情報については、きちんと運用基準の中で定められた基準に沿って管理されるとか、目的外利用が禁止されるというふうに言われていますけれども、ただ、じゃ、それが、違反した場合に罰則があるかというのは、ないわけでございますし、本当に守られているのかどうかというのを誰がチェックするのかということはやはり考えないといけないんだろうと思うんですね。

先ほど来申しましたけれども、やはりこれは、我が国の歴史上初めて、犯罪を犯したわけでもない、犯すおそれがあるわけでもない無辜の市民の情報、機微情報を大量に集める、非常に希有な機関でございますので、そのような機関の個人情報の目的外利用をしないかどうかということも含めてチェックする第三者機関というのが必要なんだろう、そのようなものがなければ、やはり個人情報というものが濫用されて、プライバシー権が侵害されるということはあり得るんだろうと思います。

ありがとうございます。

○堀場委員　ありがとうございます。

三宅先生にもお尋ねさせていただきたいんですね。

情報法制のところで、やはり情報監視審査会、絶対私も必要だと思っておりまして、第三者としてどのようにチェックしていくのかというのは非常に課題があります。

この審査する人たちの、メンバーに対してのクリアランスはどうなのか、そういったことも含めて昨日様々な議論があったところなんですけれども、やはりそもそもの、この法を作るときにこういう体制がなかったということが非常に大きな欠陥だというふうにおっしゃっていたと思うんですけれども、そのほかに、情報、特に私が一番気になっているのは、情報指定の範囲と知る権利というところと公共の福祉というもののバランスというものも含めて気にはなっているんですが、そこの辺りの、情報に関する先生の御所見をお願いしたいと思います。

○三宅参考人　情報監視審査会が大事だということを御理解いただいたのは大変ありがたいところでございます。メンバーは同じ議員の先生方でございまして、国民を代表されている方々でございますが、そこに秘密情報が来るということになりますと、やはり国会法、それから国会の職員にも秘密が来る、インテリジェンス情報が来るということについての守秘義務をきっちり整備していただかないといけないと思っております。

そういうことを踏まえて、この法案については、特定秘密保護法と同じような守秘義務規定を、国会法の改正とか国会職員法の改正等をしていただかないといけないので、このままではとても、お話にならないと考えているところでございます。

秘密指定の在り方についての審議までは、まだ特定秘密保護法の中でも十分な審議がされていませんが、諸外国では、そこの情報監視審査会に類似する議員は大変、元総理大臣とか大物がなることが多いんですが、日本の場合は大体一年で交代されるので、私もかつて、なるべく大物を入れてくださいと言ったことがございます。

重要な、情報監視審査会に御理解をいただいて、これからも活性化するように、国会法並びに国会職員法を改正し、また運用においても十分な整備をしていただくのが、まずこの法案の前提になろうかと考えておるところでございます。

○堀場委員　力強いお言葉、ありがとうございます。私どももこの議論をまた引き続きさせていただきたいなと思っております。

後半というか、最後の方になってきましたので、一つ、経済安全保障推進法の改正、こちらについても、少し大澤先生にお尋ねをさせていただきたいと思います。

先ほども自民党さんの方からありましたけれども、医療に関しては代替性があるので、基幹インフラの指定は大丈夫なんじゃないかというお話があったんですけれども、先ほど先生がおっしゃっていたとおり、地方に行きますと代替性はあるのかなというのが私の疑問点であります。

なので、医療は指定されるべきではないかというふうに思っていますし、同様に、地方自治体というのは、国がつくっているシステムの中に入れば大丈夫でしょうというところはあるんですが、現状を見回してみると、やはり独自のシステムの中でやられている自治体さんも非常に多うございますので、こちらについても指定が必要なのではないかというふうに思っているんですけれども、この辺りもお聞きした上で、先生、もう一度、指定について御所見をお願いします。

○大澤参考人　堀場先生、ありがとうございます。

医療機関の指定なんですが、一つ、視点として、技術的な視点があると思っております。

各医療機関で同じような電子カルテシステムを使っておりますと、当然、サイバー攻撃の入口の脆弱性が同じになりますので、多様化をしていれば代替性が利くんですが、同じシステムを使うようになる、ないしは共通の、厚労省等の連携システムを使うということであれば、これは攻撃を受けると一網打尽で医療機関が、電子カルテが止まってしまうということになりますので、技術の進歩、技術の導入を見た上で、必要性があれば医療機関も指定をした方がいいというふうに考えております。

ありがとうございます。

○堀場委員　電子カルテが、それぞれ皆さん個々のシステムを使っている方が逆に安全だという面もありますけれども、これからマイナンバーが普及してきて医療のＤＸが進んでいったときには、恐らくシステムというのは同じ方向に向かっていくんじゃないのかなということが想定されておりますので、その想定の上に立ったら、やはり指定が必要なんじゃないかなというふうに私自身は思っているところでございます。

我々は今、すごく、非常に厳しい国際環境の下にありますし、日本という国の、一つの分水嶺にあると思っていますので、この法案の質疑、しっかりとやっていきたいと思います。

本日はありがとうございました。

○星野委員長　次に、河西宏一君。

○河西委員　おはようございます。公明党の河西宏一でございます。

本日は、五人の先生方から様々貴重な御意見をいただきました。本法律案は、必要性とまた許容

性のそれぞれの観点が非常に重要であるということを大変勉強させていただきまして、こうした観点でそれぞれ御質問をさせていただきたいというふうに思っております。

まず初めに、渡部先生と大澤先生に、事業者に対する適性評価、いわゆるＦＣＬの部分についてお伺いをさせていただきたいというふうに思っております。

本法律案は、政府と適合事業者が契約を結ぶ場合には、様々、業務管理者の指名でありますとか、従業員への教育ですとか、施設設備の導入とか、いろいろあるわけであります。私も以前、ちょっと情報セキュリティー関係の仕事に携わったことがありまして、やはりこの世界というのは、イニシャルコストとともにランニングコストがどうしてもかかってくる。専門人材あるいは専門部署、情報のアップデートも必要でありますし、あってはなりませんけれども、漏えいの事案があった場合には対応を迫られる。大企業ならまだ耐え得ると私は思うんですが、やはり中小企業。防衛産業などでも、やはり四次、五次のベンダーまでいくとどうなんだろうかという議論が、昨年、安保委員会でもございました。

こういった中で、我が国、今政府は、防衛産業については、防衛産業の基盤強化法において、非格付情報に対するサイバーセキュリティー基準を設定をして、しかもそこに対応コストを財政支援していくと法定化をしたわけでございます。米国においても、セキュリティークリアランスに関係するコストというのは連邦政府が負担をしていくというような文献も拝見をいたしました。

こういう中において、今回のセキュリティークリアランス、我が国にも導入をされるわけでありますけれども、中小企業まで目くばせをした今後の国の支援の在り方等について、御所見があれば是非お聞かせを願いたいというふうに思っております。どうぞよろしくお願いいたします。

○渡部参考人　ありがとうございます。

ファシリティークリアランス、これは組織のクリアランスも含めてということだと思います。例えば、アメリカも含めて、どういう施設を造るか、例えば窓を作らないとか、いろいろなことをやらないといけない、そんな建物がなかったら造らないといけないので、これはかなりの負担になるわけです。

大企業で防衛関係をやっているところであればそういう対応ができているかもしれませんけれども、今後、それこそいろいろな分野でということになったときに、これはやはり官需でありますので、官需に対応できないということについて、それはやらないといけないとなったら、どうしても支援は必要だというふうに思います。

それから、今、財政支援の話で、アメリカの、ランニングコストまで支援をしているというような話は、ちょっと私、今存じ上げないんですけれども、実際そこで、最後に結局、さっきから、エコシステムというのは成り立たないといけないということなんですよね。

その仕事を官需で事業者にやらせる、それから、あと、クリアランスホルダーになっていただく、その人たちがちゃんと成り立つようにしないといけないというのはもう原則だと思います。それがこの制度の根幹にあるところなので、必要な支援はすべきだというふうに考えております。

以上でございます。

○大澤参考人　河西先生、ありがとうございます。

やはり、中小企業のことを考えますと、こういった世の中ですので、できるだけ安く調達したい、入札も競争入札であるということが政府の予算を使うときに求められるわけでありますけれども、安全保障に関わる政府調達等においては、情報管理のコストもきちっと乗せていただいて調達を考えていただく、さらに、大企業と下請の間の関係も、こういった情報調達のコスト、情報の保全をするコストをきちっと契約の金額の中へ乗せていく、そういったことを政府の側から御指導いただくということが重要でないかというふうに思っております。

ありがとうございます。

○河西委員　ありがとうございます。

大変示唆に富む、また参考になる御所見をいただきました。ありがとうございました。

続きまして、境田先生にお伺いをしたいと思います。

先ほど先生の意見陳述の中にもございましたけれども、いわゆるＣＵＩ、非格付情報に対する対応、実はこれはニーズが非常に高いんだということでございました。米国の方では、いわゆる人的スクリーニングと申しますか、バックグラウンドチェックというもの、セキュリティークリアランスは要しないんだけれどもそういったことをやっているということであります。

人の管理の方法に関するガイドライン等も政府においては早急に策定すべきというような御意見も有識者会議の中であったというふうに伺いましたし、また、民間事業者の自主的な取組というのも非常に求められる、どういったものが今後重要経済安保情報になっていくのか、そういう予見可能性も獲得をしながら対応が必要だということでございました。

こういった点についていま一度御所見を伺いたいのと、先般も様々意見交換をさせていただいたときに、やはり、労働法制とのバランス、いかに調和を持って取り組んでいくのかというところも大事な部分なのではないかというふうに思っているわけでございますけれども、御所見をいただきたいと思っております。よろしくお願いいたします。

○境田参考人　ありがとうございます。

本当に、ＣＵＩのところについては多くの企業経営者から、希望というか要望というか、そういった御意見をいただきました。

実際、会社の、特に上場企業などグローバル企業の社長というのは、本当に、情報がサイバーテロで盗まれたり、あるそういう工作員がいてデータを盗まれたり機微情報を盗まれると、その人の責任、善管注意義務違反で個人として賠償責任を受けたりするわけです。なので、会社の役員にとっては、先ほどから申し上げましたように、いわゆる今日の様々なリスクにどう対応するかというのは本当に喫緊の課題なんですよね。

そういう中で、できればちゃんと人の管理もしたい、ただ、日本の労働法制において個人のいろいろなバックグラウンドを聞くというのはなかなか難しいので、逆に言うと、どこまで何を聞けばよいかというような基準があれば非常に助かるというのが企業の経営者の方の多くの御意見でございます。

○河西委員　大変にありがとうございました。

今後の取組ということで、鋭意進めさせていただきたいというふうに思っております。

続きまして、齋藤先生、また三宅先生にお伺いをしたいというふうに思っております。

先ほどにお示しいただいた資料の中頃、あるいは三宅先生は後段の方にもお示しいただきましたが、不利益な取扱いを受けないという点についてお伺いをさせていただきたいと思っております。

今回のセキュリティークリアランスにおいては、適性評価、これは、政府は、処分その他の公権力の行使には当たらないという整理をしております。その上で、不利益な取扱いを受けないことについては法律の中で明記がされているわけではございません。ただ、評価対象者についての適性評価の結果については、要は目的外使用を禁ずることをもって担保をしている、こういうことでございますけれども、他方で、特定秘密保護法においては、解雇とか減給とか、不利益な取扱いを受けないということが法文の中で明記をされているわけでございます。

政府は、この点については今後の運用基準できちっと示していくんだということで、これが当然、民間事業者に対してもしっかりと理解をしていただくということが大事になろうかと思いますけれども、この点に関する御所見を両先生方から

お伺いをしたいと思っております。

○齋藤参考人　ありがとうございます。

今御指摘のあったとおりであるとは思うんですけれども、不利益な取扱いを受けるのをどうやって防ぐかということですけれども、一つは、適性評価についてきちんと監督するところをつくらないといけないということですね。第三者機関をきちんとつくってチェックしなければならない、そして罰則もきちんと設けなければならないんだろうというふうに思っております。

そして、もちろん、目的外利用をされたら損害賠償請求の対象になるんだということが国会答弁でも言われていましたけれども、それだけでは不十分でありまして、目的外利用をされた場合に、罰則で、裁判をやるというのはかなりの手間ですから、きちんと刑事司法の方で対応するという体制をつくらないとなかなか目的外利用というのを抑止できないのではないかというふうに考えております。

ありがとうございます。

○三宅参考人　齋藤さんとほぼ同旨ですが、つけ加えるところとしまして、先ほど、特定秘密保護法や公益通報者保護法において不利益取扱いを受けないことについての明文規定があることとの比較でお話しされましたが、それとの比較で、同じような規定をまず設けていただくことはとても大事だと思います。

それから、機微情報、これはパーソナルデータ、個人情報ですので、当然、個人情報保護委員会、こういうものもきっちり動かないといけないと思います。

そういう意味では、マイナンバーの制度とかそういうものと一体で、個人情報保護委員会がもっと強い権限を持つ委員会になって運用していただくということにも併せて、できたら、法案、出し直しなら、その辺も含めていろいろなものを入れていただけるといいかなと考えているところでございます。

○河西委員　大変にありがとうございます。

最後、一問、これは渡部先生と境田先生に改めてお伺いをしたいテーマが実はございます。これは、セキュリティークリアランスと、余り今まで話題になっていないですけれども、ＡＩとの関係をちょっとお聞きしたいというふうに思っております。

米国のセキュリティークリアランス制度に係る適性評価の日数ですけれども、これは文献で拝見をしましたら、二〇二〇年度の統計ですが、トップシークレットで平均百五十八日、シークレットで平均八十一日、あと、クリアランスホルダーに対する定期的な再調査で百七十六日ということで、三か月前後から半年間ぐらいかけていて、先日、本会議でも総理の答弁がありましたが、期間短縮は今後恐らくこの運用の中で課題になってくるんだろうと思っております。

その中で、アメリカでは、商用データベースとか連邦政府のデータベースを自動的に随時チェックをしながら、要は、継続評価をして、継続審査をして、そして効率化を図っていく。こういうシステムをつくっていくとなると、必ずＡＩを使いたいという欲求が私は絶対出てくるだろうと思うわけであります。他方で、先日、欧州議会で今後のＡＩ法に関する合意がされましたけれども、様々、多分課題はあるんだろうというふうに思うわけであります。

適性評価にＡＩを活用していくことに関しまして、何か現時点でもし御所見があれば是非お伺いをさせていただきたいというふうに思っております。どうぞよろしくお願いいたします。

○渡部参考人　大変先端的な御質問をいただいたと思います。

私自身は、現在、ＡＩ事業者ガイドラインの策定の委員長をやらせていただいていまして、やはりＡＩというものの特徴というのが非常にリスクをはらんでいるということは、国民的にも、今、知財の方でもかなりいろいろなことを指摘されています。

そういうものをここに入れていくということは、先ほど来ありましたいろいろな議論で、基本はガバナンスの問題だと思うんですね。ガバナンスとして、そういう機能を入れたときに本当にそこをコントロールできるんですかというような話が基本必ず出てきます。

私としては、アメリカは百五十八日かかっているものを、じゃ、簡単にそういうＡＩを使って短くできるかというと、アメリカでもやはり同じ問題は発生すると思いますので、そんなに簡単ではないんじゃないかなと思いますが、ＡＩの多面的な活用、これは政府でなかなかやはり活用が進んでいないと思いますので、その辺も含めて将来的な課題かというふうに存じております。

以上でございます。

○境田参考人　日本政府も広島ＡＩプロセスなどでＡＩの国際的なルール策定に様々な形で協力していると存じておりますが、やはりＡＩというのは、本当に人間が分からない新しいことが分かる代わりにそれが悪用されたり、それから、ＡＩのディープラーニングというのは、まだ間違いがあったり、それが偏見を生んだりというリスクはありますので、今、渡部委員がおっしゃったとおり、ガバナンスをきちんとする。

僕は、ＡＩというのはトライ・アンド・エラーだと思っていて、まずはエラーしても更にもう一回トライする、もう一回そこでエラーが出たらトライするというような、そういうサイクルを回すというのが、恐らく世界どこもそうなっていきますので、日本もそういうことも一つ検討した方がよいかなというふうに思っております。

○河西委員　先生方、大変にありがとうございました。

以上で終わります。

○星野委員長　次に、塩川鉄也君。

○塩川委員　日本共産党の塩川鉄也です。

今日は、皆様、貴重な御意見を賜り、ありがとうございます。

最初に、齋藤参考人と三宅参考人にお尋ねをいたします。

今回の法案は、特定秘密保護法を拡大をする、スキーム的にはそういう中身となってまいります。その際に、秘密保護法の方ですけれども、今回、秘密保護法については、特定秘密の範囲を、法改正をせずに運用基準の見直しで拡大しようとしております。政府の裁量で勝手に秘密の範囲を広げることになるのではないのか、法律によらず罰則の対象を広げるものでもあり、こういったやり方についてはどのようにお考えか、お答えいただければと思います。

○齋藤参考人　ありがとうございます。

そもそも、秘密保護法と今回の法案ですけれども、もちろん対象が違うんですけれども、安全保障という概念が両方使われている、同じ言葉が使われているんですが、その言葉の意味が実質的には違うというふうに思っています。安全保障の概念の中に、国民の安全という言葉が両方とも含まれているんですね。これも概念が違うと思っています。

特定秘密保護法の国民の安全というのは、注釈とかあるいは別表とかを見ますと、国民の生命や身体が害される場合をいうというふうに多分解されると思うんですね。今回の法案について言うと、重要基盤とかの関係で国民の生活や経済が害される場合が含まれていて、それが漏れた場合に安全保障が害されるという形になるので、多分、安全保障という概念の中には、国民の生命身体が害される場合だけじゃなくて国民生活、経済が害される場合も含まれるわけです。

その上で、今回の法案でいうと、例えば半導体のサプライチェーンみたいなものは多分対象になるんだろうと思うんですけれども、大臣の答弁とかを聞いていると、じゃ、そういうものの保護の必要性が高い、コンフィデンシャル級じゃなくてシークレット級、トップシークレット級のものは恐らく秘密保護法で保護されるんだろうというようなことをおっしゃられているんですよね。そうだとすると、国民生活や経済には影響するけれども国民の生命身体には直接影響しないような情報

を秘密保護法で対処しようとしているんだろうと思うんです、政府の方は。

先ほども申しましたけれども、秘密保護法というのは、恐らく国民の生命身体を害するような事態を対象としていて、国民経済や国民生活だけを害するようなものは多分対象としていない。ところが、どうもそこに、秘密保護法の解釈の中に、生命身体には影響しないけれども経済、国民生活に影響するようなものも含ませようとしているように見えますので、そうしますと、立法のときの経過や文言からして明らかに想定されていなかったものをそこに含ませようとしているということだと思いますので、罪刑法定主義の観点から非常に問題だろうというふうに思っております。

ありがとうございます。

○三宅参考人　先ほど御質問の御説明の中に、特定秘密法の拡大のスキームだという御説明がありましたが、私の資料の中でも二ページのところで、特定秘密というのは別表に掲げる事項に関する情報という、まず別表の限定がございますが、重要経済安保情報にはそれがない。それから、その漏えいが我が国の安全保障に著しい支障という、その著しい支障のところが、特定秘密の場合には要件とありますが、今回の場合はないということで、トップシークレット級、シークレット級と、コンフィデンシャルを分けて、二分しているという説明にはなっておるわけでございますけれども、残念ながら、別表の中の適用のところの見直し、審議というようなことがまだ尽くされていないのではないかなと思います、この十年。だからこそ、省庁で十四しかない、特定秘密法の対象となっているものを扱っている省庁。

それは、特に特定秘密指定ということを、枠を決めてもそこに対象情報がないような場合はその枠を外せということを特定秘密保護法における審議の過程で国会で議論されたものですから、いろいろな省庁で特定秘密という箱をつくってもそこに入れる情報がない、そんな特定秘密の箱は要らないじゃないかということが審査されて、対象になる府省庁が少ないわけでございます。

本来は、今日お話しになったところの刑罰法規の問題は、別表である程度書いて構成要件を整備して、それで刑罰法規が適用対象になるということになると、特定秘密保護法の見直しというようなことをちゃんと実績を踏まえてするということがないと、この法律との兼ね合いが不明確になってくる。

なおかつ、重要経済安保情報の定義自体が、先ほど齋藤参考人がお話しになったように、国民の生命身体というよりは、国民生活というのは経済情報ですから、そこまで広げると、かえって今度は刑罰法規というところの構成要件がやはり曖昧になるので、特定秘密保護法の場合は別表で掲げるということで辛うじて構成要件が、罪刑法定主義の観点から刑罰法規としてオーケーだとしても、今回のものは別表がないものですから、運用基準で広がって、それが最高刑五年の拘禁刑になってしまう、そういう問題があるので。立法を進める方からいえば痛しかゆしの問題だろうと思いますが、我々からいえば、刑法学者とかのお話を聞くと、とても刑罰法規として堪えられるようなものではないというところになっておりますので、特定秘密保護法から見直していただくところを初めからやり直してもらう方がベターだと。

必要性のところは、刑罰法規とかかわらず、ガイドラインで、刑罰法規のないもので作っていただいてもいいような、お話を今日お聞きして、特に大事だというようなことからは、思うように、今の段階では考えているところでございます。

○塩川委員　ありがとうございます。

次に、渡部参考人にお尋ねいたします。

先ほど冒頭の陳述の際に、齋藤参考人が、コンフィデンシャルの扱いについて、イギリスやフランスでは廃止をしている、アメリカでもＩＳＯＯが廃止を勧告をする、同盟国、同志国でコンフィデンシャル廃止の動きがある中で今回の法案を作ることへの疑問を呈されたところでありますが、この点については渡部参考人はどのようにお考えでしょうか。

○渡部参考人　実態として今アメリカでどれぐらいコンフィデンシャルが使われているかという統計等はちょっと把握はしていないんですけれども、アメリカで、私の、ハーバードでクリアランスホルダーを持っている人をよく知っているんですけれども、よくブリーフィングやなんかでやっているものに関してはコンフィデンシャル級のものが含まれているということを聞いております。

詳しくその辺どういう動向になっているかということを踏まえては必要だとは思いますが、一方、これは我が国の制度ですから、我が国として、例えば今経済産業省は特定秘密はないわけですけれども、コンフィデンシャル級の技術的な情報があるという前提でこれを運用するというふうに理解をしております。

○塩川委員　ありがとうございます。

その点について、どうでしょうか、齋藤参考人の方で何か補足することとかございますか。

○齋藤参考人　ありがとうございます。

先ほども申し上げたんですけれども、コンフィデンシャルで指定された秘密というのは、過去には指定されておりますし、そういう判こを押しているわけですから、急にコンフィデンシャルというものがぱっと消えるわけではないわけです。

ただ、扱いとしては、やはり、コンフィデンシャルというものを廃止して、ほかのトップシークレット、シークレットの二段階の中でやっていくという方向には間違いなく動いているし、ＩＳＯＯもそういうふうに勧告しているわけです。

アメリカの情報を特に入手したいということで制度をつくるのであれば、そして、アメリカのＩＳＯＯは、イギリスのようなアライアンスを組んでいる国がコンフィデンシャルを廃止しているからアメリカも廃止しなきゃ駄目だというふうにまさに勧告しているわけですから、ほかの国から情報を取りたいということであれば、やはり日本の秘密制度というのもほかの国に合わせていかないといけない。

そうであれば、やはりトップシークレット、シークレットという二段階の秘密区分に合わせた法制を作らなければならないのであって、日本だけガラパゴス的にコンフィデンシャル級の法律を作るというのは、私は非常に、何というか、成果がないだろうというふうに思っております。

ありがとうございます。

○塩川委員　ありがとうございます。

渡部参考人にお尋ねいたします。

セキュリティークリアランスについての今回の情報保全体制の必要性について、ちょっと個別の案件ですけれども、今回の法案の意義の一つとして同盟国、同志国との協力関係を強化するものを強調しているわけですが、昨年六月に政府がまとめた宇宙安全保障構想、この中では、同盟国、同志国との各種衛星データの互換性の確保や相互運用性の確保が必要であり、そのためにセキュリティークリアランスを含む情報保全体制が必要だと指摘をしております。

現状は何が足りないとしているのか、その上で、今回の法案はこのような要請に対応するものとなっているのか、その点について教えていただけないでしょうか。

○渡部参考人　宇宙関係につきましてはニーズがあるということは承知しております。

現在、宇宙関係、特にスタートアップに日本はかなり力を入れようとしているときに、必ずそこでアメリカとの関係が問題になる。そこの中で、実態的に今の三階級のどこが問題になるのかということはちょっと把握はしておりません。その点については、今後もアメリカとのやり取りを、これはつくってから説明をするでしょうから、その中で処理をしていくということかと思っております。

○塩川委員　これは、コンフィデンシャル級だけで対応するようなスキームというのがあるということなんでしょうか。要するに、トップシークレット、シークレットはかかわらず、コンフィデンシャルにおいて、相互の秘密の情報の共有をす

るような、そういう共同開発とかいうのがあるというのが想定されているということなんでしょうか。

○渡部参考人　共同開発をどういう形でやっていくのかということについては承知をしておりません。

今、トップシークレット、シークレットに関しては特定秘密があって、それで、報告書に関しては、仮に別にする場合はシームレスな制度にするという表現になっています。その中でどれぐらいのことができるかということになるかと思います。

○塩川委員　重ねて渡部参考人に伺います。

有識者会議の議論の中で、第八回のときに、同盟国、同志国との情報保全の仕組みについて、「先ほど他の委員から「合わせ技」で信頼を得ればよいのではないかという話があった点に関し、おそらくアメリカに対してはそれなりの相互のやり取りがあるため、ある種の相場観があると思うが、今後の経済安全保障上の重要機微情報に関しては、アメリカだけではいけないのではないか。例えば、防衛の特定秘密保護法の話になるかとは思うが、ＧＣＡＰのようなイギリス・イタリアといった国々との関係や、将来的にはＡＵＫＵＳでのいわゆる新興技術を含めた技術協力だとか、そういったことに広がりが出てくることを考えると、日米間特有の理解が他国に共有されるかどうかということは考えておくべきだと思う。」と。

アメリカとの間では、いろいろ、この間、積み重ねもずっとある。しかし、イギリスとかイタリアとかオーストラリアの場合では違うんじゃないのかと。そういった場合に、現行、アメリカとの関係と、それ以外のイギリス、イタリア、オーストラリアのような国々との間には、クリアランスの対応が異なっているものなんでしょうか。今回の法案は、このような多国間の共同開発の障害を除くものとなっているということなんでしょうか。

○渡部参考人　御質問ありがとうございます。

この手の制度は、例えば特許非公開の制度をつくったときに、これは当然アメリカも、いろいろな国にあるわけでございますが、じゃ、どういう運用をしていてどういう形でそれは連携していけるのかということについては、制度がないとまず話をできないという状態でございました。

そういう意味で、先ほど申しましたように、アメリカと比べると少し変わった形の制度をつくったわけですけれども、今まさにそういうコミュニケーションが取れる状態にはなってきたというふうに理解をしています。

今回の場合も、先ほど申しましたけれども、ほぼ、ほかのＧ７の各国で制度を持っているわけでありますが、日本にはない。前提として、民間に広く提供されるような形では制度を持っていないわけですから。それを今回、初めてつくる。先ほど申しましたように、制度をつくればすぐシステムが機能するというものではないと考えています。逆に言うと、一遍に大量に、例えばアメリカは四百万人ですけれども、拡大するということは現実的にはできないし、あり得ないと考えています。

そういう意味で、ステップを踏んで、今のようなことが現実にどういうふうにできるのかということを検討していくということが現実的だと思います。

ほかの国についてはもっとよく分かりません、残念ながら。

○塩川委員　終わります。ありがとうございました。

○星野委員長　次に、浅野哲君。

○浅野委員　国民民主党の浅野哲でございます。

今日は、皆様、大変御多忙の中、様々な知見を先ほどからいただきまして、ありがとうございます。

私からも、数点質問させていただきたいと思います。

まず伺いたいのは、本日の境田参考人の資料の中で、やはり、新たな制度が国際的に通用する制度でなければいけないし、また、同盟国、同志国との間で新たに必要となる国際的な枠組みについても取組を進めるべきだ、そういう御指摘がありました。

あわせて、大澤参考人にも後ほど同様の趣旨で伺いたいと思いますが、今聞いているところによりますと、今回、新たな制度、各省庁単位で情報の取扱いというのをしていく予定だというふうに聞いております。さらには、諸外国とのやり取りも省庁が中心となってやっていくということなんですが、これまで諸外国で、国同士、こういったコンフィデンシャル情報のやり取りというのが、いわゆる省庁単位でやられるというのがスタンダードなのかどうか、ちょっと御認識の範囲内で教えていただきたいということと、私が懸念しておりますのは、やはり、省庁単位となりますと、非常に、省庁ごとに独自性、独自のやり方だとか、独自の基準だとかというものが広まっていって、国として統一性が取れなくなるおそれがあるんじゃないか。日本でいえば、そこに内閣がどう関与していくべきなのか。国としての一体感、統率性というものがちゃんと担保されるのかどうかというところについて少し懸念を持っておりますので、この観点から、境田参考人、そして大澤参考人から御知見を賜れればと思っております。

〔委員長退席、中山委員長代理着席〕

○境田参考人　御質問ありがとうございます。

かつて特定秘密法があって、今回、その拡大みたいなお話もありましたけれども、私がちょっと考えておりますのは、やはり、先ほど申し上げましたとおり、今、ハイブリッドの中で、企業とか政府とか自治体とかが、海外の様々な機関とか組織から様々な攻撃を受けて、サイバーのみならず、宇宙からを通じてでも、インフラを通じてでもいろいろ受けている中で、どう守るかという話だと思うんです。

そういう中で、各役所が、今回はこの半導体の技術、これを、例えばこういうふうな開発をして、それを民間の事業者を募って、海外の政府とやり取りをして、この技術を育てましょうとか、この技術によってサイバー対策を打ちましょうとか、そういう話だと思うんです。

なので、これは、基本的に各役所がどの技術を特定技術にするかを判断し、信頼できる民間の事業者と組んで、それでこれを対応する、恐らくこういうふうなことを目指しているんだろうと思うんです。

なので、特定秘密保護法のようなときの重要技術を守るかという話と、今まさに、この五年、十年の間に物すごく日本中がリスクにさらされている中で、どういうふうに国を守ったらいいかと考えるときに、各役所がそこは責任を持って、どういう技術を持ってどう守るかというのを判断するというのが、私はよろしいんじゃないかというふうに思っております。

それで、今までも、恐らく特定秘密法のときも、各役所が、幾つかの役所がアメリカなど、政府などとそういった連携をしてきた、そこを私、ごめんなさい、正確ではないんですが、恐らく役所役所でそういったやり取りをしながら、そういった保護制度を使った運用をやってきたんだというふうに理解をしております。

○大澤参考人　浅野先生、ありがとうございます。

諸外国、特に米国においても、情報の作成者がクライテリアを指定していくというのは共通の文化だろうと思いますので、その点では、この日本の制度も同じような運用をされると思います。

ただ、日本の省庁の場合、例えば国会答弁一つ取っても、関係するところは全部合い議をかけて調整をしますので、恐らく、クリアランス制度ができても、情報の指定というのは、関係する省庁に関しては全部相談をして調整をした上で情報の指定をしていくだろうというふうに、日本の官僚文化からするとそういうふうに考えておりますので、御懸念の、省庁別になってしまって、日本政府全体として統一が取れないということは発生しないだろうというふうに、官庁の文化を考えます

とそういうふうに考えております。

ありがとうございます。

○浅野委員　ありがとうございます。

続いて、適性評価の実行方法について伺っていきたいと思います。

やはり、今回、適性評価に多くの注目が集まっておりますし、先ほど議論にもありましたように、今後は特定秘密のときよりも対象者が増えていく。そういった中で、いかに効率的にこの評価を行っていくかという問題と、もう一つは、今回、十年その資格が保持されるということなんですが、やはり、十年間の中では様々なリスクにさらされることになりますし、環境変化も起こるだろう、その十年間の間の信頼性が変化していないかどうかの評価をいかに行うかという、この二つの問題があるように思っております。

こちらも大澤参考人、そして渡部参考人に伺いたいんですが、この適性評価、今回、内閣が行うということになっていくと聞いておりますけれども、非常に対象者が膨大になる中で、現状の体制面について懸念や留意事項等あれば御開陳いただきたいということと、十年間という期間の間の信頼性確認の在り方についても御知見があれば教えていただきたいと思います。

○大澤参考人　ありがとうございます。

資格を得るためのプロセスなんですけれども、まず、資格を申請者が自分で条項について記入をして提出をするということになりますので、その一部について、うその記述がないか、間違ったものがないか、又は隠されたものがないかというものを、恐らく内閣で内閣総理大臣が指定した者がチェックをしていくというプロセスになっていくだろうというふうに考えております。

そういった点では、全ての人の全ての面をチェックするというよりは、重点的に怪しいところをチェックするということになると思うんですが、それでも民間の事業者の人間を全て審査をするということになりますと、やはり、審査をする内閣官房、若しくはその代行として警察庁というこももあり得ると思いますが、そこに負担がかかることは間違いないことでありますので、人員の増というものは体制面からは必要になるというふうに思っております。

また、十年間の資格の保持ですけれども、今回、特定秘密保護法もそうなんですが、資格者のチェックだけではなくて、資格者が外国から働きかけを受けたりとか特定の働きかけを受けた場合には窓口に相談をするないしは報告をするということが特定秘密保護法でも運用されておりますので、そういった意味では、逆に、資格者をチェックするだけではなくて、資格者の安全を守る制度、それも担保されているというふうに考えておりますので、十年間維持する中で、情報の取扱いをするという自覚をそれぞれの人が持ってもらえれば、そのような外からの働きかけに対して自己申告で通報をしていく、その制度がきちっと整っている、ケアもちゃんとしてもらえる、そういう、逆に、資格者を保護する体制をきちっと整えていくというのが十年間の保持を担保するためには必要であろうというふうに思っております。

ありがとうございます。

○渡部参考人　ありがとうございます。

これは非常に重要なところなんですけれども、現在、最初に二十人でしたか、何十人というようなレベルでやるというような話を聞いています。実際にこれはかなり大変な作業になると思いますので、できる範囲は当初は非常に限られている。

先ほど申しましたけれども、これは一遍に大きくしようとしてもやはり難しいと思います。逆に、人数がいればいいかというと、その中でやはりノウハウだとか知見だとかも必要になりますので、これは徐々に大きくしていくということが重要であって、一遍に拡大するということを想定をするべきではないというふうに思います。

先ほども言いましたけれども、これはエコシステムができないと実際機能しないんですね。ガバナンスの話もそうなんですけれども、ガバナンスするにもいろいろな機能が要ります。そういうものが全体として整ってくるという過程においてこれを実現させていくというふうに考えた方がよろしいかと思っております。

それから、十年間は結構長い期間ですので、確かにおっしゃるとおり、ここをしっかりそれが管理されるということは重要だと思います。

今参考人が言われましたように、これは自己申告で、事情が変わったらと。これも言葉だけではなくて、これも私申し上げたように、人に優しい制度、全体としてそういうことが円滑に行われるようにしていかないといけないというふうに申し上げておりますが、その環境自身も重要で、コンタクトをしている方がどういう働きかけをしているのか、どういうことを、コミュニケーションしやすい環境をつくっているのかとか、そういうようなことも含めて整備をする必要があるというふうに考えております。

以上でございます。

〔中山委員長代理退席、委員長着席〕

○浅野委員　ありがとうございます。

もう一問、渡部参考人に伺いたいことがあります。この留意点にも書かれていますように、人材流出の懸念があるということであります。

実は私も、前職は民間企業の研究所に勤めておりまして、特許等、書いておりました。実際に、就業時間中に知らない電話番号からかかってきまして、うちで働きませんかというような声かけをいただいたことも何度かあります。

ですので、実際、この参考文献にも書かれているように、出した特許だとか、その人のこれまでの実績を実際に参照して、ピックアップをされて、声をかけるという活動は実際行われていると思うんですね。

となると、このセキュリティークリアランスホルダーの方が、そういった海外の企業に行くだけならまだしも、そこで何らかの保持している情報を間違っても言ってはいけないわけです。

こういったことを未然に防ぐためには、これは、大切に扱う制度であることと書いてあるんですが、もう少し具体的なものを教えていただきたいということと、一方で、これは今回、プロジェクトドリブンで、誰がクリアランスホルダーになるべきかというのを事業者側がピックアップを最初するわけですけれども、個人としてホルダーになりたいという人もこれから出てきかねないと思います。こういった方に対してはどういうふうに対応していくべきなのか。これについて教えていただきたい。

○渡部参考人　最後、個人としてホルダーになりたいというのは、これはあくまでやはり政府としてこういうことをやるので、必要に応じてそのクリアランスを取るという形なので、手を挙げるということとはちょっと違うのだと思います。

それで、おっしゃったように、これは非常に、今までの経験からして、さっきおっしゃった、私も実は昔、民間企業にいましたけれども、誘いの手が来るわけですね。だから、そういうようなことは、当然、クリアランスを持っているような方だとターゲットになってしまうわけで、そこはかなり注意をしないといけないというふうに思います。

では、優しい制度というのは何ですかと、おっしゃるとおりなんですけれども、このプロジェクトで、何らか、例えばこういう技術開発が必要だというようなことであれば、そこにちゃんと雇用環境とか処遇だとか、そういうことが継続的にできるような形で、それは、このクリアランスの制度ではない、その外側の経済安全保障の施策の中でいろいろなものがございますので、それが例えば組み合わされているとか、そういうことも配慮した上で行っていかないと、これは罰則があればそれが防げるかということでは恐らくないという部分がございますので、かなり総合的な施策としてここを検討していく必要があるのではないかというふうに思っております。

以上でございます。

○浅野委員　時間があと僅かですので、最後、三宅参考人に伺いたいと思います。

やはり、コンフィデンシャルに指定された情報を公開を要求したときに、齋藤さんの資料を見ますと、チェックの仕方が包括的なので、秘密解除されない可能性があるということが指摘されておりましたが、この点について、是非、三宅参考人の立場から一言いただきたいと思います。懸念事項等あれば、お願いいたします。

○三宅参考人　私の資料だと三ページのところで、コンフィデンシャル情報の情報公開というのを当時随分議論したんですね。それで、そのとき初めてコンフィデンシャルというのが出たんですが。

コンフィデンシャルというのは、そもそも、当時は今とちょっと状況が違いましたけれども、しかし、その中で、情報公開法の中では、法人又は個人における通例として公にしないこととされているもの、通例としてというので、そこで、例えば、刑罰法規にかさるとかは別ですけれども、重要経済安保情報をカテゴリカルに定めて、それがコンフィデンシャル情報としてのものということがある程度明確になるとすれば、それは通例として公にしないものということになろうかと思いますが、その当該条件をつくる、公にしない条件で任意で提供、任意で提供で企業から来るものもございますし、企業とやり取りしている、これも全部行政文書になりますけれども、そういうものについては、公開請求があったときの、当時の状況等という等のところに、今の状況も照らして、それが五年、十年たって、もう陳腐化したようなデータになることもあると思います。

そうすると、その時点では公開をされるということもありますので、原則秘密ということで今日は議論されていますけれども、そもそも、重要な経済情報というのは、流通することによって経済発展していくという側面もございます。

そういうことからすると、情報公開法の五条二号ロというのがかなり大きな意味を持ってくるんだろうと思いますが、例えば、それに基づいて担当者が開示したときに、それがたまたま間違って、経済安保情報としてこの法律の刑罰法規に触れるんだというような話になると、これは過失犯として処罰されるかというような議論が具体的に出てくるんですけれども、そういうことについてどう対応するのかというところはもう少し議論を深めていかないと、単に刑罰法規として特定秘密保護法と同じ刑罰の水準で、枠組みで書いているということだけでは、違う問題がこの重要経済安保情報についてはあろうかと考えているところでございます。

○浅野委員　終わります。

○星野委員長　次に、緒方林太郎君。

○緒方委員　よろしくお願いいたします。

五人の参考人の皆様方、今日は、貴重な陳述をありがとうございました。

私、一度、三宅先生から御意見をお伺いしたいと思っていたことがかねてからございまして、今日は本当に貴重な機会ですので、まず、全ての情報の基礎となる公文書についてお伺いをさせていただきたいと思います。

公文書管理法というのは、福田総理の下で作られた、非常に格調高い、私はいい法律だとずっと思っているんですが、この十年にわたって醜悪な解釈がどんどんつけ加わって、結果として、私、公文書管理法というのは体裁は今でもすごく立派なんだけれども、その運用において極めておかしなことになっているんじゃないかと思うんですが、生みの親としての御意見をお伺いできればと思います。三宅先生。

○三宅参考人　自公政権で福田総理大臣のときに御提案されて、麻生大臣のときに通りまして、それで、民主党の政権のときに運用が始まりまして、そのときに委員を拝命しまして、安倍政権でずっと委員をやっておったという、八年やったわけですが、その中で、森友問題が出たときに、原則一年以上の保存にしましょうというルールも決めたんですね。ただし、コピーは一年未満でいいとか、日程表なんかは一年未満で廃棄をしていいとか、あらかじめ決めたものは廃棄をしていいんだということで。

一番大きな問題だったのは、桜を見る会の招待者名簿で、総理大臣のときの、持っている名簿は一年未満で廃棄するという。こういうものは、私、森友のときにチェックをして、重要又は異例な取扱いをしたときには、これは原則一年以上保存しましょうということをガイドラインで決めたんですね。そのときに、審議の中で、総理大臣夫人がいろいろ議論されたデータが出てくるようなお話のことは全部これに含まれるんですねということで重要又は異例なということにしましたので、恐らく桜を見る会の招待者名簿というのは重要又は異例な問題として残るものだと思ったら、それが消えたというようなことで。

醜悪な解釈と先ほどコメントがございましたが、いろいろな手だてをその中に、法律とガイドラインの中につくったんですね。だから、今日のコンフィデンシャルの情報についても、公文書管理法の中でどういう扱いをするのかということはとても大事で、五年ごとの指定ということが、でも、三十年たったら公文書館に移管しますよという、これは特定秘密保護法と同じですけれども、これは本当にちゃんとしていただければ、今の時点では秘密になっているものも、やがては国民のものとして開示される。もちろん、国立公文書館の方では、三十年、五十年、八十年、百年というルールも作りました。百年たつともう歴史になっていますので、百年たったら開示されるというようなルールまで整備したものでございますので。

公文書管理法は、先ほどの福田先生の高尚な理念の下に立派なものができたと思っているんですが、その後の解釈が曲げられておるという点では残念でございますが、それを本当はならないようなガイドラインまでは作っておるというところは御留意いただければと思います。

○緒方委員　ありがとうございました。

個人メモの定義等々も含めて、何か変なことになっているなという思いがありまして、あれだけ崇高な法律である中、気がついたら何か変なことが起きているというのは、すごい違和感を持って今でも受け止めております。

それでは、渡部参考人にお伺いをさせていただきたいと思います。

陳述をお伺いしながら、私、地元が福岡県北九州市でございまして、地元の日本製鉄八幡製鉄所の電磁鋼板の事件をすぐに思い出しました。電磁鋼板の技術がポスコに移り、そして、それがポスコから宝山鋼鉄の方に移っていったという非常に残念な事件が起きたことは、恐らく御承知だと思います。

それを受けて不正競争防止法の改正が行われたわけでありますが、私自身、民間企業が保有するデータについて、余り国の方でいろいろ手を突っ込むということは控えるべきだというふうに思うんですが、現在、不正競争防止法が整備された中、これ以外に何か、我々法律をつかさどる者としてやるべき、追加的にやる対策として思い浮かぶものがあれば、是非お聞かせいただきたいと思います。渡部先生。

○渡部参考人　ありがとうございます。

ポスコの事件は非常にインパクトのあった事件で、これで学ぶべきことが幾つかある中で、実はこれは、韓国に行って、それから中国に行ってという事件でございます。韓国で、実は、裁判の中身を見ていますと、通常の韓国の不競法というのと、それから、国家重要技術については別途の保護する制度がありまして、それで分かった理由は、中国に漏えいした社員が、韓国の技術だと言うと、今度はこっちに触れてしまうので、罰則が厳しくなるので、これは実は日本から盗んだ技術だということを言ってしまった、そういう経緯のものですね。

ここで分かることとして、やはり、この不競法等もそうなんですけれども、競争しているんですね。罰則とかいろいろな形で、やはりそれが、こっちが厳しいと、こっちに流れるというようなことがある。これは現実に、不競法に関してはかなり頻度の多い改正をしていますけれども、実

は、日中韓だけ比較しても、こっちが改正すると、こっちがまた改正する、こういう状況になっています。

まさに、そういう感覚で今回のものを捉える必要があるというふうに思っておりまして、私は、やはりスタートすることは重要だという考えでありますが、スタートして検証していくことは非常に重要だと思っていますのは、今のようなことであります。

したがって、適性評価の考え方とかそういうようなことについても、しっかりしていく、それは、検証していくということの中で、リスクがないかということを検討していくことが必要だと思います。

それから、二番目のお話で、不競法以外にということでありますが、先ほど来出ています、ＣＵＩと言っていますが、これは基本的には民間情報ですね。ただし、政府が支援したようなものとか、あるいは、それこそ今回、特許の非公開制度なんかでも、そこで指定されるとこれは別途の仕組みになるわけだけれども、そこでコミュニケーションがあった部分とか、いろいろなものに関して、やはり様々な保護、一般の民間情報としての保護に少し追加したような形のガイドラインみたいなものは必要なのではないか。特に、デューデリジェンスあるいは民間の場合は必要最小限のバックグラウンドチェックみたいなものもガイドラインで定めていかないと、そこの手当てができないんじゃないかという話は、先ほども出ているとおりでございます。

以上でございます。

○緒方委員　ありがとうございました。

続きまして、齋藤先生にお伺いをいたしたいと思いますが、罪刑法定主義についてですが、私も、大学で法学部で芦部信喜先生の憲法を学んだときに、明確性の原則という言葉がございました。

今回、経済安保情報が特定秘密に含まれるかどうかということについて、私も、必ずしも一〇〇％の明確性があったとは言えないのではないかと思うんですが、法律の専門家として、刑事法制が明確でなくてはならないその明確というのは、どの程度のものが問われるというふうに思われますでしょうか。齋藤先生。

○齋藤参考人　ありがとうございます。

なかなか難しい問いだと思うんですけれども、例えば、国家公務員法とか地方公務員法という法律があって、そこでは全然具体的には規定していないんですよね。では、それが憲法三十一条違反と言われるかというと、決してそうではない。それに比べれば、はるかにましだろうという意見もあるとは思うんです。

ただ、そうはいっても、法定刑が五年だということもあるし、例えば、裁判所に行ったときに、これは罪刑法定主義違反で、憲法違反ですよみたいなことが言われるかどうかという話とは別として、そういうレベルではないけれども、ただ、やはり国民にとっての予見可能性というのは当然あるべきだし、あとは、国会は、国民の代表者で、国権の最高機関ですから、そこで国民の権利についてはきちんと決めるべきだということも当然尊重されなければならない。

だから、裁判所で違憲判決が出るかどうかということとは別に、やはり立法府としてはできる限り明確な法律を作らなければならない。それは罪刑法定主義の要請なんだろうというふうに考えております。

その観点でいきますと、やはり特定秘密保護法で別表があったというのはかなり明確化に役に立っているけれども、今回はないということと、もう一つは、安全保障という概念の中に国民の安全という概念があって、特定秘密保護法で言う国民の安全というのは国民の生命身体を意味しているように思われて、今回の法案では国民生活や国民経済まで含んでいるように思われるんですが、ただ、そこら辺の定義規定がないので、必ずしもはっきりしないんですよね。政府もそこら辺を非常に曖昧にしたまま解釈論を展開しているようですが、その公にというところはやはり時とともに経過していくと思いますので、インターネットの時代に、しかもＡＩの時代にいろいろなツールで集まってくるということでは、公になっているというところの要件はかなり広がっているんだろうと思います。

だからこそ、こういう重要経済安保情報として保護しようというようなお話が出てくるんだと思いますが、今日のお話を聞いている限りだと、それと刑罰法規というのがなかなか難しいところがあるように思いますので、やはり秘密の指定のところの、不正競争防止法における営業秘密、私、かつてそれを随分研究したことがございますが、論文も書きましたが、その辺の秘密とか、それから、国家公務員法違反の、外務省機密漏えい事件からなる、国における、安全保障における非公知性というようなものまで、もう一回ちゃんときっちり見直さないといけないのではないかなと今日は思っているところでございます。

○緒方委員　最後に、境田先生にお伺いをさせていただきたいと思いますが、今回の法制度は、情報を指定して、それに対してセキュリティークリアランスをかけるということなんですが、私、昨日の質問でも問うたんですけれども、そうではなくて、将来的にそういう情報に接する可能性がありそうな人に対してもセキュリティークリアランスをかけていくという可能性を残すべきではないかと思うんですけれども、先生の御見解をお伺いしたいと思います。

○境田参考人　非常に的確な御指摘だと思います。

有識者会議でも議論になったんですけれども、クリアランスホルダーになる人が、実はアメリカでは、ＣＥＯとかＣＴＯとか、そういう役員のトップの人も通常取るんですよね。日本はそれはないんです。当然のことながら、会社の経営をしている者として、実際にセキュリティークリアランスを取って活動している。何をやっているかを知らないと、正しい判断ができないでしょうと。

○三宅参考人　なかなか難しい問題で、どう答えていいのかということをちょっと考えますが。

秘密の三要件の中に、非公知性、公にされていないものというのがございました。例えば、情報公開法の中で、公にしていないかどうかというのは、昔は、図書館に行って、そこで調べられるかどうかぐらいの話で、情報公開の最初の頃はやったんですが、今は大体インターネットで、一見してばあっと出るかどうかというような感じが、公にされているかどうかというような感覚でずっと持っておるんですけれども。

その辺のところが、秘密の三要件の中の、秘指定ですから、形式秘と、それから要保護性、秘密にしなきゃいけないというのがありますが、それが、その公にというところはやはり時とともに経過していくと思いますので、インターネットの時代に、しかもＡＩの時代にいろいろなツールで集まってくるということでは、公になっているというところの要件はかなり広がっているんだろうと思います。

だからこそ、こういう重要経済安保情報として保護しようというようなお話が出てくるんだと思いますが、今日のお話を聞いている限りだと、それと刑罰法規というのがなかなか難しいところがあるように思いますので、やはり秘密の指定のところの、不正競争防止法における営業秘密、私、かつてそれを随分研究したことがございますが、論文も書きましたが、その辺の秘密とか、それから、国家公務員法違反の、外務省機密漏えい事件からなる、国における、安全保障における非公知性というようなものまで、もう一回ちゃんときっちり見直さないといけないのではないかなと今日は思っているところでございます。

○緒方委員　最後に、境田先生にお伺いをさせていただきたいと思いますが、今回の法制度は、情報を指定して、それに対してセキュリティークリアランスをかけるということなんですが、私、昨日の質問でも問うたんですけれども、そうではなくて、将来的にそういう情報に接する可能性がありそうな人に対してもセキュリティークリアランスをかけていくという可能性を残すべきではないかと思うんですけれども、先生の御見解をお伺いしたいと思います。

○境田参考人　非常に的確な御指摘だと思います。

有識者会議でも議論になったんですけれども、クリアランスホルダーになる人が、実はアメリカでは、ＣＥＯとかＣＴＯとか、そういう役員のトップの人も通常取るんですよね。日本はそれはないんです。当然のことながら、会社の経営をしている者として、実際にセキュリティークリアランスを取って活動している。何をやっているかを知らないと、正しい判断ができないでしょうと。

こういうことで、ニード・トゥー・ノウが、今までは恐らくそういったところが射程に入ってこなかったんだけれども、今後はその可能性のある人も恐らく入るんだろうということだと思っています。

○緒方委員　終わります。

○星野委員長　次に、大石あきこ君。

○大石委員　れいわ新選組、大石あきこです。

参考人の皆様、よろしくお願いします。

まずは、セキュリティークリアランスの制度の有識者会議の座長もお務めになった渡部参考人にお伺いしたいです。

本日のこの参考人の意見陳述の中で、齋藤参考人の方から、コンフィデンシャルという情報が、少なくともイギリスやフランスではもう周回遅れというか廃止になって、アメリカに対しても、もうコンフィデンシャルは要らないんだという流れになっているのに、日本で今この時点で法制化されるということは合理性に欠くというような御指摘があったと理解しておりますが、それに対して、渡部参考人の御意見をお聞かせください。

○渡部参考人　ありがとうございます。

現時点で整理をすると、トップシークレット、シークレット、コンフィデンシャル、各国が制度を持っているということであります。それに対して、特定秘とシームレスな制度として、コンフィデンシャルという部分はないということですので、そこは特に経済安保の、今回、民間提供をするという前提であれば、かなり、技術的な情報とかはそこに当たるのではないかというふうに判断をしたということだと思います。

一方で、諸外国において、じゃ、そこのカテゴリーがどうなっていくのかということについては、これは、やはり状況変化、先ほども申しましたけれども、この手の制度は、まずコミュニケーションをするためには持っていないといけないということで、徐々にそこを、立ち上げていく過程の中で検討していくことではないかというふうに思っております。

以上です。

○大石委員　ありがとうございます。

引き続き、渡部参考人にお伺いしたいです。

先ほどの三宅参考人の御意見の中で、又は齋藤参考人もおっしゃっていましたけれども、二点お伺いしたいんですけれども、こういう問題点があるんだと言っているんです。

情監審を育てていかないといけないという御指摘がありました。しかしながら、今回の法案にはそのようなチェックの部分が行き届いていないので、そこを入れるべきだ、絶対必要なんだというふうにおっしゃっていたので、その点について、確かに必要だなと思われるかということが一つ。

もう一つ、特定秘密保護法の別表で何が刑罰に当たるのかということが、罪刑法定主義の観点からも、特定秘密でもあるのに、今回のこのセキュリティークリアランス法のコンフィデンシャル級に関してそれがないというのは不備であるという、この二点の指摘された不備に関して、やはりこれは不備だな、必要だな、あるいはあった方がよいと思われますか。

○渡部参考人　何かだんだん政府側の答弁みたいになってきちゃってあれなんですけれども……（大石委員「もう座長まで務められた方なので、済みません」と呼ぶ）

ガバナンスをしっかりすることは前提だと思います。これは国会との関係においてもそうだと思いますし、そこはやはりこの制度の根幹に関わるところで、例えば個人情報についての問題とかそういうようなことについて、やはり信頼ができるようなガバナンス制度として、必要な制度であればそれは導入はしていくということはあるのではないかと思います。

それから、もう一つは何でしたか。済みません。

○大石委員　情監審に関する部分が欠けているということと、あと、特定秘密保護法上の別表があったが、ないということに関して。

○渡部参考人　だから、結局、対象の問題ですよね。客体がどうかということで、今、三要件で説明しているということなんですけれども、じゃ、これを事細かに書いた方がいいかということに関しては、先ほどもちょっと申しましたけれども、そこは、むしろ国際的な関係とかを考えたときに、そんなに細かく書いているということではないので、そこはバランスを取るということが必要なのではないかというのが私の意見でございます。

以上です。

○大石委員　どうもありがとうございました。

続きまして、笹川平和財団の大澤参考人にお伺いしたいです。

大澤参考人に、ほかの委員からの御質問の中でありました、ファイブアイズへの参画に関して、今回のセキュリティークリアランス法でその参画に前向きな要素があるのかというような御質問があったと思います。

このファイブアイズというのは、アメリカとかイギリスの対中包囲網の軍事情報ネットワークのようなものと理解していますけれども、さすがに、こういった分野と考えたときに、特定秘密のトップシークレットとかシークレット級のものではないのかなというふうに思うんですけれども、セキュリティークリアランスができればそういったファイブアイズへの参画が可能というのは、どのようなメカニズムというか考えでそうなるのか。特定秘密でいいのではないのか。特定秘密ではなく、なぜセキュリティークリアランス法によってこれが進むのかというところに御意見をいただきたいです。

○大澤参考人　大石先生、ありがとうございます。

情報を守る文化、国がそれぞれ安全保障を担保するために、政府の中だけではなくて、当然、その安全保障に関わる民間事業者も機微な情報を扱いますので、その文化が全体としてその社会にあるかどうか、それが恐らくファイブアイズに入る最初の資格要件だろうというふうに思っております。

そういった点では、今回、民間のセキュリティークリアランス制度が導入されますと、特にサイバーセキュリティー面ではサイバー攻撃の情報を、これは政府で保持していても十分に生かし切れないので、やはり民間の事業者を守るために共有をすることになります。ただ、そこに共有をする、ファイブアイズから情報が来て民間事業者に共有するといったときに、全く制度がない状態では、やはり情報の安全が担保できない。ファイブアイズの国からすると、情報を取り扱ったことのない、マイナーリーグの国なんじゃないかということになります。

渡部参考人からもありましたけれども、この制度をきちっと社会に根づかせて運用していく、それによって、情報を取り扱う自覚を持った人たちがこの安全保障関連の民間事業者の中にも一定数コミュニティーとして出てくる、そういった中で安全が担保されるということですので、必ずしも資格要件とか罰則があるからというわけではなくて、社会全体が、コミュニティーとして情報を守る、そういう文化がきちっと根づいているのか、そういうお作法をちゃんと知っているのかということが、恐らく、ファイブアイズからすると、情報をちゃんと提供できるのかどうかというところの肝になります。

そういった点では、政府だけではなくて民間の企業においてもきちっとクリアランスを持って、そういう情報の取扱いを長期間にわたってしていく、そういうことによって社会がちゃんと形成されていく、そこが一番の肝なのではないかなというふうに思っております。

ありがとうございます。

○大石委員　もう少しお伺いしたいんですけれども、今の、ちゃんと情報を守るという話であれば、特定秘密で対象を広げるというやり方もあろうかと思います。それの是非はともかく、そういうやり方もあろうと思いますが、大澤参考人の考えでは、セキュリティークリアランスでよりよく

広がるというのは、もう少し、罰則が低かったりですとか、ハードルが低いものでたくさんの労働者、民間の方々をセキュリティークリアランスの対象にすることによって、実際にはファイブアイズに入るという要件でやり取りする中身は特定秘密なので特定秘密の方でやるんですけれども、耕すような、裾野を広げるような意味で必要だという認識で合っていますか。

○大澤参考人　特定秘密の保護はかなり厳密に決められていますので、例えば金庫の中へしまわなきゃいけないとか、そういうものを含めて、情報の利用という点ではかなり制限があるというふうに思っております。

　サイバーの世界ですと、例えばデイリーにどういう脅威があるのかとか、それを、民間事業者、特に通信事業者とか電力とか、重要インフラ事業者との間でデイリーに情報を共有するというのがアメリカだとコンフィデンシャルレベルで扱われておりますので、そういった情報の利用を考えると、特定秘密保護法の中でやっていくというのはちょっと、情報の流通を妨げることになりますので、それよりは、より広範に共有できるような仕組みということで今回の法案は考えられているのではないかなというふうに思っております。

　ありがとうございます。

○大石委員　もう一度お伺いしたいんですが、そう考えますと、ファイブアイズは直接的には特定秘密でやり取りしますよという想定でもなく、セキュリティークリアランスで対象になった方もファイブアイズのプロジェクトに直接関わる可能性も想定されるだろうということでよろしいでしょうか。

○大澤参考人　ファイブアイズのプロジェクトに参画をすることになるかどうか、それは個別の案件だと思いますので、恐らく個々に判断を、相手の国がすることだろうと思いますけれども。

　そもそも、日本社会に対して情報を共有する、特に機微な情報を共有する、その取扱いが、ちゃんと教育をなされている人が取り扱う、そういう安心感が相手国に与えられる、それがベースになりますので、それに基づいて、じゃ、個々の案件、例えば、戦闘機の開発ですとか、よりサイバーの懸念国からの攻撃についての情報共有、それは個々の、ケース・バイ・ケースで、相手国が判断をすることだろうと思いますので、そこは一概には何とも申し上げられないと思います。

○大石委員　ありがとうございます。

　このセキュリティークリアランス法もそうですし、私は国会議員になって二年半になるんですけれども、二年前に成立した経済安保推進法のときもそうですし、それ以外でも様々な、今、関連するような経済安全保障に関する法律が成立していっていますけれども、この狙いを考えたときに、参考人の方もおっしゃいましたが、安全保障というのがこの十年で大きく様変わりしているんだということなんですが、その核心というのは、やはり中国の、経済面でも軍事面でも非常に大きくなって、アメリカと肩を並べるようになって、そういう危機感の中で、アメリカが、中国はアメリカを追い越すなという、特に二〇一〇年台後半から対中強硬路線というものに切り替えてきたんだろうと思います。その中で、同盟国の日本というのもその対中包囲網に巻き込まれていくといいますか、私は批判的な立場ですので、そのような流れの中にあると考えています。

　今回の質疑でほかの委員がおっしゃいましたけれども、ハイブリッド戦争ということで、まさにそれは言い得て妙だと思うんですけれども、日本もそのような対中包囲網の中に軍事的にも経済的にも巻き込まれていくんだ、参戦するしかないんだ、そのような空気が覆っていて、その中で、日本もせめてビジネスチャンスにしていく、一部の資本の方がもうけていくという流れしかもう残されていないかのように、私にはそのような空気に感じております。

　今回のセキュリティークリアランス法というのは、思ったよりも小さなパズルのピースなのかなという気もしましたけれども、やはりこのピースが必要なピース、そのような流れに日本が進んでいく必要なピースなのであろうと思い、これはやはり世界の緊張を高める、軍事的緊張も高めるものですので、私は本当に、一人の小さな人間として震撼しております。何とかこの流れは止めたいと私は考えています。

　本当に、正直一人で、私という立場で何ができるのかという思いもありますが、この国会の外にいる少なくない国民の皆さんも、この流れは駄目なんだという思いの方がたくさんおられると思いますので、私は、諦めずにやれることをやっていきたいと思います。

　それはすなわち、軍事ビジネスではない、本当の意味での国民を守る安全保障であり、それは徹底した平和外交ができる政権を樹立することなしには無理だと考えております。

　私の考えを述べて、終わります。

　以上です。

○星野委員長　これにて参考人に対する質疑は終了いたしました。

　この際、一言御挨拶申し上げます。

　参考人各位におかれましては、貴重な御意見をお述べいただきまして、誠にありがとうございました。委員会を代表して厚く御礼を申し上げます。（拍手）

　この際、お知らせいたします。

　経済産業委員会との連合審査会は、来る四月二日火曜日午前九時から開会いたします。

　次回は、来る四月三日水曜日午前八時五十分理事会、午前九時委員会を開会することとし、本日は、これにて散会いたします。

　午前十一時五十五分散会