経団連総合政策研究所新書／2024年12月

シンポジウム

企業が直面するリスクとチャンス

～変化し続ける経済安全保障環境を踏まえて～

Keidanren
Policy Research Institute

経団連総研

シンポジウム（2024年12月17日開催）

開会ごあいさつ……井上　隆　日本経済団体連合会 専務理事　4

講演1
「経済安全保障と知財」プロジェクトの意義と位置づけ……渡部　俊也　経団連総合政策研究所 研究主幹／東京大学未来ビジョン研究センター 教授　7

講演2
企業が直面するリスクとチャンス
～激動の経済安全保障環境にどう備えればいいのか～……峯村　健司　経団連総合政策研究所 研究委員／キヤノングローバル戦略研究所 主任研究員　27

講演3
機微技術・営業秘密の保護に必要とされる措置の最新動向……上野　一英　経団連総合政策研究所 研究委員／TMI総合法律事務所 パートナー 弁護士　43

パネルディスカッション・質疑応答……61

【パネリスト】（順不同）

経団連総合政策研究所 研究主幹／東京大学未来ビジョン研究センター 教授	渡部　俊也
経団連総合政策研究所 研究副主幹／キヤノン株式会社 顧問	長澤　健一
経団連総合政策研究所 研究委員／キヤノングローバル戦略研究所 主任研究員	峯村　健司
経団連総合政策研究所 研究委員／ＴＭＩ総合法律事務所 パートナー 弁護士	上野　一英
経団連総合政策研究所 研究委員／一橋大学イノベーション研究センター 准教授	吉岡（小林）徹
経団連総合政策研究所 研究委員／三菱重工業株式会社知的財産部 マネージングエキスパート	森　達也

役職は開催日現在のものです。２０２５年５月をもって、21世紀政策研究所は経団連総合政策研究所に名称を変更しており、関連する役職は新たな名称に直しています。

ごあいさつ

会員企業の皆さまには平素より当研究所の活動にご支援を賜り、心より御礼を申し上げます。また、本日は多数お集まりをいただき、ありがとうございます。

さて、近年、技術革新や国際情勢の急激な変化が世界経済、あるいは企業経営に大きな影響を及ぼしており、そのような中で、経済安全保障の観点が事業の継続や成長に直結する重要な課題となってきています。そこで当研究所では今年（２０２４年）４月、新しく経済安全保障と知財研究プロジェクトを立ち上げました。本日のシンポジウムは、企業が直面するリスクと可能性を再確認し、未来を見据えた取り組みへの支援を目的としています。本日は、研究主幹の渡部俊也東京大学教授をはじめ各分野でご活躍の専門家の皆さまから、最新の知見と事例をもとに、多角的な視点から議論を深めていただき

たいと考えています。この内容が会員企業の皆さまの、将来を見据えた経営戦略を考える上での一助となれば幸いです。

本日のシンポジウムが皆さまの活動の参考となることを祈念して、私からのごあいさつとさせていただきます。本日はどうぞよろしくお願いします。

二〇二四年十二月十七日

日本経済団体連合会 専務理事　井上　隆

【講演1】

「経済安全保障と知財」プロジェクトの意義と位置づけ

経団連総合政策研究所 研究主幹／
東京大学未来ビジョン研究センター 教授

渡部　俊也

経済安全保障政策の背景

ご紹介をいただきました渡部です。こちらのプロジェクトの研究主幹を務めさせていただいています。本日のシンポジウムには「経済安全保障と知財に関わるリスクとチャンス」という言葉、もう一つは「経済安全保障環境における」という二つのキーワードがあります。経済安全保障の環境について、このプロジェクトでは五つの視点を大事にし、研究を進めていこうとしています。そのような背景について、まず簡単にお話を申し上げたいと考えています（資料1）。

このプロジェクトの対象範囲は経済安全保障と知財です。知財は皆さんご案内のとおりで、知的財産基本法で法律的にも定義がしっかりされています。ただ、経済安全保障に関しては必ずしも法律での定義がなされているわけではありません。国会等の答弁で政府がどのように考えているかということを集約すれば、経済安全保障はわが国の生存・独立及び繁栄を経済面から確保すること、すなわち経済政策であるということです。

そして、その基本的な概念は戦略的自律性と戦略的不可欠性です。自律性については脆弱性を解消すること、弱みを補完することということで、「守り」ということになり

資料１　本プロジェクトの五つの視点

- 経済安全保障に関係する制度と産業エコシステムの相互作用
- AI・データなどにおけるガバナンスと経済安全保障の観点
- 国際標準や知財ライセンスについて経済安全保障の視点で着目
- スタートアップのおかれた環境に着目
- 経済安全保障機能を担う主体である企業経営の観点

（出所）渡部作成

ます。不可欠性については強みを磨くという表現がされています。国際社会に欠かせない存在となる意味で、「攻め」と言っては語弊が多少あるかもしれませんが、そういう要素が含まれているものです。

経済安全保障は英語でEconomic Securityと訳せるのかもしれませんが、そうすると、ニュアンスがかなり多義的になります。経済安全保障は官需の経済政策であるという特徴を持っているわけですが、そのような政策が重要になってきた背景がいくつかあると思います。

一つは、経済安全保障は地政学的な背景があることはご案内のとおりかと思います。それだけではなく、後ほど峯村先生からも説明があるかもしれませんが、競争の変質があります。産業政策は市場経済の需給関係に基づき成り立っているものですが、そうではない考え方の産業政策を行っている国

があり、それが国家安全のためというような考え方であるとすると、そうでない国との間にはコンフリクトが生じます。

それから、新興技術の台頭です。以前は大量破壊兵器などの安全保障上重要なものは主に輸出管理で境目を極めてはっきりさせてきたわけですが、今はデータとＡＩです。自律的なＡＩ兵器などであれば、安全保障上の直接の脅威もあります。しかし、それ以上に世論の誘導や分断など、いろいろなことにＡＩを使われてしまいます。これは逆に言うと、民生と軍事の境界という面では、デュアルユースという以上に全く分け隔てなく機能していくものであり、そこの区分が非常に難しいのです。また、公共財の提供になるようなデジタル技術の役割が増すに従い、例えばスマートシティにＡＩが関わってくると、その対応を非常に難しくしてしまうと言えます。

そして、これらの新興技術は、もちろん大きな企業も担うわけですが、世界的に見れば宇宙開発やＡＩなどにおいてはスタートアップの役割が非常に重要になっています。ということは、このガバナンスを考えるときに、スタートアップは欠かせない対象であることも言えるかと思います。

渡部研究主幹

経済安全保障関連制度の制定

また、日本の制度に欠けていたものがあります。例えば特許の秘密特許制度、あるいは特許非公開制度とわが国では呼びますが、世界のほとんどの国にある制度がなかったということです。それから、今回法律が成立し、いま運用基準をつくっているところですが、セキュリティ・クリアランスも極めて限定的な特定秘密保護法という形でしかありませんでした。このような制度が欠けていることにより、わが国にどのような機会損失があるのか、あるいはどういうリスクが生じているのかということすら分からなかったという背景があります。

では、現在のわが国の状況はどうなったのか

というと、特に情報管理という観点で脆弱性があることを背景とし、経済安全保障政策が重視されるようになってきたと考えてよいかと思います。そのときに、もう一つのテーマである知財はどういう関係にあるのかというと、主に経済安全保障のための手段です。それだけではありませんが、そういう側面が非常に強いというような整理ができるかと思います。

経済安全保障関連の制度は、２０２２年から経済安全保障推進法が制定されましたが、それ以前からある輸出管理等も関連制度であると言うこともできます。２０２２年以降も、重要な制度として整備が進められてきたものがいくつかあります。その一つは特定重要物資と称しています。例えば、抗菌剤に関して特定の国に原料を依存しているために、手術ができなくなる状況であったことは記憶にある方もおられるかもしれません。そのようなサプライチェーンについての問題があります。それから、先ほど「攻め」と言いましたが、どちらかというと不可欠性を確保していくための官民技術協力についてです。「K Program」という言い方をしていますが、いま海洋技術等々が指定され、重要技術の育成支援が行われています。また、電力などさまざまな基幹インフラについて

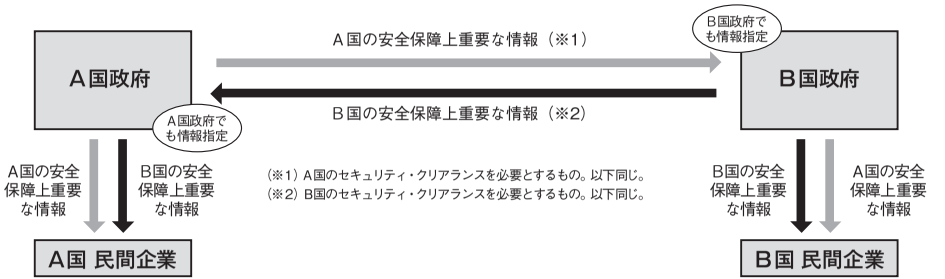
です。ちょうどこの前の国会で一つ、港湾関係が基幹インフラとして加わっています。昨年（２０２３年）７月、名古屋港でサイバーアタックがあり、荷積みが全くできない状態になりました。そういう脆弱性があるところについての対応。そして、特許出願非公開制度というようなものが制定され、順次、施行されました。それに加え、今年（２０２４年）、法律制定した重要経済安保情報保護活用法にて、セキュリティ・クリアランスのことですが、機微情報を取り扱う人や設備の認証という制度ができたところです。

重要経済安保情報保護活用法（セキュリティ・クリアランス制度）とは

セキュリティ・クリアランスを一つ例に取り上げ、タイトルにある「経済安全保障の環境」について説明をしてみたいと思います。

セキュリティ・クリアランスの対象は、国家における情報保全措置の一環として政府が保有する情報です。ここが重要なところで、民間情報に対し指定を行うことがあるわけではありません。官民協力で何らかの目的のプロジェクトを行うといった場合には、

資料２　民間機関が、他国の政府機密情報を共有する際の仕組み



□ 政府が保有する安全保障上重要な情報へのアクセス権（セキュリティ・クリアランス）は、基本的には自国民を対象に付与される。
□ 外国政府の安全保障上重要な情報にアクセスするためには、自国政府を通じて行う必要がある。

（出所）https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyo_sc/index.html

政府が保有している情報にアクセスする必要がある者、通常は政府職員が多いわけですが、その当該者の信頼性を確認した上でアクセスを認める制度です。そのための適正調査・適正評価が行われるというものです。この制度に関しては、実は民間の要望があったことが大きな背景としてあります（資料2）。

何が一番問題であったかというと、G7各国はほとんど同じような制度を持っています。日本だけが特定秘密保護法で極めて限られた範囲でしか制度を持っていなかったわけです。例えば、米国がセキュリティ・クリアランスの制度を持っていて、そこから情報提供され民間事業者とプロジェクトが行われているとします。それと同等の制度を持っている国の企業であれば、直接米国のクリアランスホルダーになれるわけではありませんが、米国と協定等を結んだ国との関係が担保されれば、その国の企業に対しても情報の提供ができる。そのようなことがあり得るわけですが、ここに日本の企業が入れなかったということです。

アメリカに子会社をつくった場合、基本的に米国籍がないと対象になりませんので米国の方を雇用し、セキュリティ・クリアランスを取ることはできます。しかし、そこで

得られた情報については日本の本社に提供することができないことになります。ですから、そのプロジェクトに対し、実は日本の本社の持っている技術が極めて有効であると分かっていたとしても、それを伝えられませんでした。また、その技術の輸出は外為法の管理上にあるので、日本側から輸出を行おうとしても目的が伝えられない。したがって、成り立たないということです。

法律制定の過程で幾つかのそういう企業の経験を聞きましたが、「ここから先はクリアランスホルダーだけが対象なので、席を立ってください」というような話をよく聞きます。こういう中で、どれだけの機会損失があったのか。あるいは、その情報を持てないことにより、どのようなリスクがあるのか。そういうことすら分からなかったのです。

どういう情報が指定されるのか？

では、どういう情報が指定されるのかというと、法律の条文を読んでもそれほどはっきりしません。今回、重要経済基盤保護情報該当性として運用基準のほうで1号から4号まで、もう少し詳しく出ています。1号のところは措置という名詞、2号のところは

技術を含む情報ということですが、これだけ読んでも何が該当するのか分かりません。この間も、「わが社のこういう技術について、これが該当するのでしょうか」と質問をいただきましたが、残念ながらこれはなかなか分からないと思います。

ただ、これを解釈して該当するかしないかということはあまり重要ではありません。重要なのは、政府のイニシアチブによるプロジェクトで情報の提供が必要となるかどうかです。実際にそのような必要性があり、プロジェクトがつくられるかどうかに依存するので、そこは政府とのコミュニケーションが前提となるということです。

現在、この制度についてはパブリック・コメントが出ており、期間がもう少しあります（2024年11月28日から2024年12月27日）。まず運用基準についてパブリック・コメントにかかっていますが、具体的にどういう制度なのかというところでリンクを見ていただくと、現在議論されている諮問委員会の資料があり、それと併せて見ていただく必要があります。例えば、「運用基準の補足として、今後定めることを予定しているガイドライン」で、このようなQ&Aを検討中というものが出ています。

この中で言うと、例えば「適合事業者の認定のために必要な施設」というのは検討さ

資料３　ガイドラインおよびＱ＆Ａ

● 運用基準の補足として、今後定めることを予定している「ガイドライン」もしくは「Q&A」の中で、明示していくもの

Qの例としては…

2－(2)「重要経済安保情報を取扱うことが見込まれる者」には、たとえば、求職者などは含まれるのか。含まれるのであれば、その際の留意事項なども含めて明らかにすべき。

3－(5)適合事業者の認定のために必要な施設として、どのようなことが求められるのか。

(6)適性評価を得ている者を対象に手当を支給することは可能なのか。

(8)適合事業者の認定に必要となる施設設備の整備に際し、行政機関から何らかの支援を受けることは可能なのか。

（出所）https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/shimon/kaigi_5/shiryou_5.pdf

れている会社があろうかと思います。特定秘密保護法では、「窓をつくってはいけない」などとかなり厳しいものになっているので、そこの考え方は本件ではどうなるのかということです。あるいは、組織のクリアランスについて、例えば社長がクリアランスホルダーにならないといけないのかといったことが、Ｑ＆Ａの形で検討されています（資料３）。

パブリック・コメントのほうに意見をお寄せいただくと、恐らくＱ＆Ａで対応していくことになろうかと思います。よく利用いただければと思います。適正評価が実際にどういう手続きでなされるのかについても、これは運用基準の項目には入っていませんが、Ｑ＆

Aに説明があるので、それを見ていただければと思います。

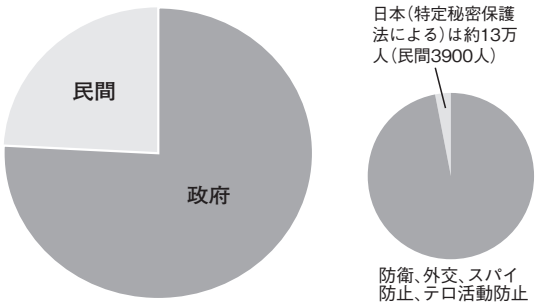
経済安全保障が促す新たな産業エコシステム

このような制度ができてくるわけですが、それが経済安全保障の環境にどうつながるのか、私の私見も交えてお話ししたいと思います。

現在米国のクリアランスホルダーは４００万人いると言われています。民間が１２０万人で、かつ、その目的はかなり広くなっています。米国の場合は対象が記載されていますが、他の国だともう少し漠然とした、抽象的な表現になります。いずれにしても、日本の特定秘密保護法では防衛、外交、スパイ防止、テロ防止の４分野になるので、比べると対象には幅がかなりあります。そして、日本の場合は13万人（民間３９００人）なので、本当の比率でいくと図の円グラフの比較よりもっと小さいことになります。

この米国の人たちがどういう役割を果たしているのかというと、当然、政府の機密情報を受け取る事業、あるいはプロジェクト等に関わっていることになります。しかし実

資料４　米国のクリアランスホルダー



①軍事計画・兵器システム又は軍の運用　②外国政府情報　③インテリジェンス活動・情報源・方法又は暗号　④機密情報源を含む連邦政府の外交関係又は対外活動　⑤国家安全保障に関連する科学的・技術的・経済的事項　⑥核物質又は核施設の防護策のための政府プログラム　⑦国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性又は能力　⑧大量破壊兵器の開発等

（出所）渡部作成

際は、機密研究だけではない、あるいは機密情報の必要なプロジェクトだけではない Unclassified な領域にも、さまざまなクリアランスホルダーの経験者がいます。何しろ１２０万人いるので、その人たちは非常に注目される役割を担っていると私どもは考えています（資料４）。

　Unclassified 領域においても Classified の管理や経験が極めて参考にされていることにより、政府機密研究だけではなく、産業のエコシステム全体に対して管理や

情報の活用がなされていると考えています。大学もそういう傾向があります。例えば、ＭＩＴでは Lincoln Laboratory というところで機密研究をやっているわけですが、その経験者が基礎研究のほうのリーダーもやっています。そういう中で、政府の要求する安全保障環境に貢献していると見ています。

経済安全保障の観点で危惧される機密情報流出

機密情報流出についてのわが国の状況については、以前、質問票調査で確認をしたことがありますが、実は相当の漏えいが今でも続いているのではないかと思います。調査では「わが社では何も流出は起きていない」と答える会社がかなり多いです。本日参加されている企業は皆さん注意をされていると思いますが、いろいろ注意する施策を増やすと実は流出は起きていたのだと分かるようになります。そのようなデータが具体的に取れています。実際は水面下にある流出というものが極めて多いのではないかということですし、その中でも特に人を通じた情報流出のインパクトが大きいと言えます。例えば特許データから見ると、他の国に行って活動している方のデータがかなり取れます。

この中で、さらに諜報活動に関係した者はなかなか発覚しにくいです。例えば、普通の民間の会社から営業秘密の窃盗を狙っている場合、会社が注意していれば相手が警戒をするということがあるのですが、諜報活動の場合はいくら注意しても相手は警戒しないし、事業に使うわけではないので、実際はもっと発覚しにくい状態になってきているのではないかと思います。２０２２年にソフトバンクの機密情報の窃盗が新聞にも出ましたが、これは実はごくわずかな例ではないかと思います。

そういうことを念頭に、しっかり対策に取り組まなければいけません。アメリカのUnclassified領域にもクリアランスホルダーの方がおられ、環境としてそういうことを整えないといけないという前提で、例えばＯＳＩＮＴと言われているOpen Source Intelligence（公開情報収集）の活用や、雇用する場合のデューデリジェンス（適正評価）も行われています。機密情報を提供する相手の適正評価だけではなく、こういうところにも気を付けないと全体の環境が整備されないことを、留意すべきではないかと思います。

経済安全保障政策の特徴として、一方的に政府が規制を行うという性格のものではな

資料５　企業経営の視点で重要なこと

- 官需の経済政策によって新たに形成されるエコシステムに適合した経営戦略と経営管理
- そこに参加するためには従来から行われてきた「自社の知財を守る」機能の一層のブラッシュアップは前提となる（人の管理、OSINTの活用、DDなど）
- 他方官需の経済においてもたらされる新たな機会を最大限生かすための技術戦略が求められる
- これらの基礎となる制度の理解と政府との対話（情報交換、相談）は重要であり、経済団体においてはそのようなインターフェースを担うプラットフォームも必要ではないか

（出所）渡部作成

いと考えています。今回のセキュリティ・クリアランスの適合事業者の選定においても、「事業者からの相談などを踏まえながら」という一文が付け加えられています。そのような双方向のやりとりが前提となっています。そしてまた、セキュリティ・クリアランスホルダーは企業の方でありますが、国にとっては極めて重要な人的資源なので、組織の処遇等も非常に重要になってきます（資料５）。

特許非公開制度でも同じことが言えて、保全審査中に特許出願を取り下げることもできるし、手上げもできるような制度になっています。何を意図しているかというと、これらの制度が経済安全保障の法目的に沿って運用されるために

は、企業側の経済安全保障に関する理解と協力があって初めて機能するということです。すなわち、経済安全保障制度は官民協力を前提としたものであると考えてよろしいかと思います。

制度の理解と政府との対話が重要

このような環境における企業経営には何が重要になるかということについてお話しします。「官需」という言葉を使っていますが、これは政府の目的で、民間の需給関係の取引以外の需要に応じる制度になるので、その経済政策により新たに形成されるエコシステムに適合した経営戦略と経営管理が必要になります。具体的なアクションについては、後ほど先生方からもう少し詳しくお話しいただけると思います。ただ、その一つとして、知財を守る機能についてはブラッシュアップが必要だと考えます。また他方、官需の経済において新たな機会がもたらされることになるので、これを最大限生かすような戦略が必要になってきます。あるいは、それがまた新たな機会をもたらすことになります。

そのためには、これらの基礎となる制度の理解と政府との対話や相談が重要です。対話という言葉は政府も使っています。経済団体においては、そのようなインターフェースを担う役割も期待できるのではないかと考えています。

本プロジェクトについてはただいま申し上げたようなことを背景とし、「本プロジェクトの5つの視点」に書かれた視点を重視し、研究を進めていきたいと考えています。

私の話は以上です。ありがとうございました。

【講演2】

企業が直面するリスクとチャンス
～激動の経済安全保障環境にどう備えればいいのか～

経団連総合政策研究所 研究委員／
キヤノングローバル戦略研究所 主任研究員

峯村　健司

中国の政策意思決定メカニズム

峯村です。よろしくお願いします。渡部先生から話があったとおり、いま国際政治経済の秩序が大きく変わっていることが一つのキーワードだったと思います。よく言われているのは、重商主義がまた新たに到来しているのではないか、新重商主義的なものが新たなルールになっているのではないかというのが一つあります。

もう一つは、キーワードで言うとインテリジェンスです。ＯＳＩＮＴの話もありましたが、どのように情報収集をするのかということです。シンポジウムのタイトル「企業が直面するリスクとチャンス」の特にリスクの部分を今回、私から説明をさせていただこうと思います。特にいま皆さんの一番の懸念事項は中国でしょう。中国がいま何を考えていて、どういう経済政策、産業政策をとろうとしているのか、中国の観点でお話しさせていただこうと思います。

まず、中国版の経済安全保障についてです。日本で経済安全保障の法律をつくったときに、一体それは何だと中国の政府の関係者からも聞かれました。よくよく突き詰めていくと、中国も１９６０年代から、言葉はなかったけれども経済安全保障的なこと

峯村研究委員

はやっていました。さらに、いわゆる国家安全という、日本や欧米で言われているnational securityよりももっと大きな意味を込めていることがわれわれを少し混乱させ、理解を苦しめていると見ています。いま14億のトップに立っている習近平国家主席の意思の下、全て上意下達でいろいろな政策が決まっている状況にあります。

もう一つは、サプライチェーンを重視していますが、国産化がキーワードになっています。国産化といっても、日本や欧米の言葉とは少し違う意味があります。一つ代表的な言葉として、2020年4月、中国共産党の中央財経委員会における習近平の言葉が非常に象徴的だと見て

います。訳が少し難しいですが、「伝家の宝刀的な重要な技術というものを自分たちは確立し、高速鉄道、電力設備などのサプライチェーンの優位性を高める」というのがまず一つあります。そして、「相手国の中国への依存度を高める」。さらには、「外部からの人為的な供給遮断に対する強力な反撃力と抑止力を持たなければならない」というように、何か軍事用語を聞いているような感じですが、中国的な経済安全保障というといわゆる安全保障的な思考が極めて強い考え方です。相手を依存させ、これに対し供給遮断をしてきた場合には、自分はそれに対抗できるようなシステムをつくらなければいけないというものになっています。

最近、私は企業の皆さんに講演をする機会があります。今の習近平政権の産業政策について質問されることが少なくありません。習近平氏の財経委員会の発言以降、中国では国産化というものが急ピッチで進められています。例えば、オフィス機器には２０２０年にいわゆる国家規格というものを策定し、政府調達をしなければならないという指示を出しています。あとは、情報システムをできる限り２０２７年までに国内企業の製品に切り替えるようにしろとか、ＥＶの国産化とか、そういう形で国産化が矢継

ぎ早に打ち出されているのが今の習近平体制の特徴になります。

経済インテリジェンスの重要性

では、これは一体、誰が指示を出し、どういうコンセプトでやっているのかということです。渡部先生からお話があったとおり、経済インテリジェンスが重要になってきます。中国で産業政策から何から意思決定をしているのは政府ではなく、実はその上位に位置づけられている中国共産党です。共産党の中でも最も重要な組織は、特にサプライチェーンや産業政策をつかさどっている中央国家安全委員会という、国家主席の弁公室（事務局）に直結しているところです。これは２０１４年に新しくできた組織で、習近平氏自らがトップに就任しています。この中では当然、国家安全は非常に重要視され、軍事、経済、外交、イデオロギー、科学技術、産業、金融も全てこの国家委員会がグリップしています。その指示を下の政府機関に出しているのが今の状況です。

いま日本政府のカウンターパートナーとしては、例えば外務省だったら中国の外交部、経産省だったら中国の商務部とやりとりしているわけですが、政府機関と話をしても意

図がなかなか分からない、返答が来ないという悩みを政府の方々からよく聞きます。それは当然で、彼らはよく分かっておらず、その政策決定のプロセスに入っていないから説明できません。「上の国家安全委員会、共産党からやれと言われました」と言うしかないわけです。だからこそ、いくら政府とやりとりをしていても真相は分からないというのが中国の現状です。

例えば、いま中国における邦人拘束が非常に増えています。計17人の日本人が拘束されています。日本の経済団体が訪中したときに「邦人保護をしてくれ」と言い、商務部の幹部が「分かりました」と言ったところで、何のギャランティーにもならないということです。誰を捕まえるのか、誰を釈放するのかということは、その上位である国家安全委員会が決めています。だから、政府とやりとりをしていても真相が分かりません。そうなってくると、できる限り共産党にアプローチをしなければなりません。とは言っても、共産党は中南海と呼ばれている北京の中心部にありますが、ここの電話番号が書いてあるわけでもないですし、ホームページにもほとんど何も書いていません。したがって、情報収集がなかなか難しい現状であるということです。

政府機構の中で唯一違うところで言うと、工業情報化部は少し異色なところになります。外資企業をどう誘致するのか、参画するのか、排除するのかという決定を比較的しているところですが、ここは他の政府機構よりはインテリジェンス要素というものがかなり増えています。ただ、ここへのアプローチも非常に難しい。そういうことで言うと、いま中国の産業政策は外国からはほとんど分からない状況にあります。

中国製造２０２５とは

そのような状況でも、私なりに国家安全委員会の関係者らと議論をしていく中で、いくつか分かってきた点を列挙します。

まず、サプライチェーンの国産化政策です。先ほど申し上げたとおり、国家安全委員会が政策を決め、執行していくものを上意下達で政府機関にどんどん指示しています。その中でもターゲットになっているのが、まさに日本が強みを持っているファンダメンタル技術で、これを国産化しようとしています。皆さんも「中国製造２０２５」という政策を聞いたことがあると思いますが、２０２５年までにＡＩ、量子コンピュータなど

資料6　中国版経済安全保障の3つのポイント

①サプライチェーン国産化政策の継続

「上意下達」の構造

- 官邸と省庁が意思疎通しながら政策立案・執行を行う日本とは異なり、党が政策立案を行い、その執行を政府が行う
- 現在の**「習近平一強体制」**下において、一度決定された産業政策・経済安全保障政策は、方向性を変えずに目的達成まで突き進むこととなる

②日本が強みを持つ基礎技術こそが現在の「国産化」のターゲット

上流から下流までの自前化

- 2020年前後、中国はITやAIといった情報産業や組み立て産業の自前化に自信を持つようになった
- 現在は、機微技術に加えて、**上流中流領域である「材料・素材・部品」や「製造装置」**などの日本の産業競争力を支える基礎技術分野も国産化のターゲットとなっている

③技術獲得方法の高度化

伝統的な技術獲得方法

- 合弁会社の設立や、人材の引き抜き
- 最近は電子部品及びその材料領域等でさらに活発化

近年とられる技術獲得方法

- ①政府調達、②国家標準の設定により、中国内での開発・設計・生産・保守などを義務化。**日本企業に規格の遵守 or 撤退を迫る**
- 特に日本企業に対して**Tier1、Tier2 企業の買収戦略**

（出所）峯村作成

含めた先端技術の水準をアメリカ並みに上げていくというもので、目下それを進めているところです。その中でターゲティングされているのが、材料、素材、部品、半導体を含めた製造技術で、ある意味日本がターゲットになっています。

では、どのようにその技術を獲得しているのかというと、合弁会社を設立しましょうという形で、日本企業にアプローチします。あと、古典的な人材の引き抜きをやっています。最近はだんだん高度化、ステルス化して見えなくなっていて、政府調達から日本製品を排除したり、日本企業に規格を守りなさいという指示を出し、技術を開示させて中国側に持ってくるように促していたりします。中国が比較的優位性を持っている分野、例えばＥＶのバッテリーなどでこういうことが起きています。さらには、これは規格外だという形で撤退に追い込みます。かなり洗練化されたやり方をするようになっています（資料６）。

中国は「中国製造２０２５」に向けた3段階ステップというものを採用しています。ステップ1で言うと、「どうぞ皆さん、中国に来てください」と日本企業にもアプローチしていましたが、「本土化しましょう」というところに話を持っていきます。中国政

府は中国企業に対し、例えば「海外技術をどんどん取得しましょう」「中国企業製品を使いなさい」という形で指示を出します。さらには、この間も報道になっていましたが、輸出管理という形で、ガリウム、ゲルマニウムの輸出を規制し、ある意味でそれを人質にする形で誘致させるようなことをやっています。

ステップ2で言うと、得られた技術を使い、過剰生産をして価格を下げ、他国の製品を排除していきます。今、これが特に問題になっています。ここには当然、共産党の補助金が注ぎ込まれるというアンフェアな状況になっており、そのため半導体などは世界市場の中で特に中国製品のボリュームが増えています。例えば、黒鉛でも輸出管理で他国の製品を排除していて、ステップ3にかなり近づいています。

ステップ3では、技術を獲得して他の国よりも優位になると、今度は逆に中国のほうが優位性のある技術を守るほうに入ります。その例を挙げると、バッテリー、磁石、モーター装置などがあります。したがって、いまフェーズが相当変わってきたと言うことができます。今までは、中国に技術をどう取られないように防衛するのかというところでしたが、今は逆の立場になっている分野もかなり増えてきています。しかも、中国政

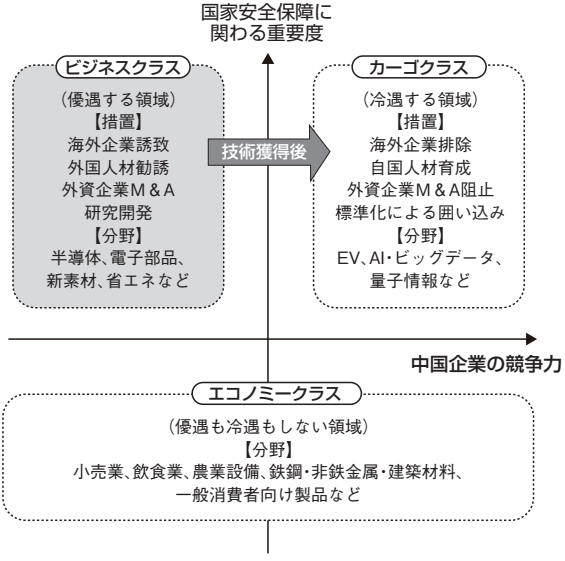
府は今まではいろいろな内部文書で指示していましたが、口頭だけで指示するなど非常に見えにくくなっているのが現状です。

日本企業がとるべき対応

では、日本企業としてどうすれば良いのかということです。先ほど渡部先生から説明がありましたが、いわゆる戦略的不可欠性を日本企業としてどのように確保できるのか、維持できるのかというところが重要です。そもそも、皆さんの企業が中国側からターゲットになっているかどうかも見極めなければいけないところです。個社にとっては重要な技術であっても、実は中国から見ると、「こんなものはいらない」というのも結構あったりします。ここはインテリジェンスでしっかりと補強した形で、どこの技術は守るべきものなのか、もっと攻めで売ったほうがいいのかを選別していかなければなりません。

特に重要なのは、日本が技術優位性を持つ領域です。具体的にはシリコンウエハー、光ファイバー、複合機、液体クロマトグラフ。この辺りが機微技術の流出防止をしなけ

資料７　中国版経済安全保障に関わる分野



（出所）峯村作成

ればいけない部分として、注目していく分野だろうと思います。もちろん、中国だけに限らず、世界がどんどん競って開発していく分野として、技術革新が進んでいる先端半導体とか量子コンピュータもあります。しかし、実は見落としがちなのが、いま日本の中でも特定の会社が持っている技術優位性をいかに守るかということです。ここはしっかり見極めていかなければいけないポイントになってきます。

「中国版経済安全保障に関わる分野」として在中国の欧州企業の団体「中国ＥＵ商会」が発表したものがあります。中国が一番優遇している分野は、半導体、電子部品、新素材など、彼らが「ビジネスクラス」と呼んでいる領域です。ここはとにかく優遇します。「企業の皆さんどんどん来てください」「人材も来てください」とまさに秋波を送っている分野になります（資料７）。

ただ、これも技術を獲得してしまうと、まさに「カーゴクラス（貨物室）」に落とし込まれるように、「もう要りません」と冷遇されるようになります。それが今の中国の状況です。例えば、ＥＶの分野では排除されています。その辺りも中国が優位性を持ったから要らなくなったという形で、シビアにやられています。

もう一つ、「エコノミークラス」の領域があります。ここは技術の優位性うんぬんに関わりません。例えば、小売や飲食など、中国でも売り上げを比較的伸ばしている日本企業も多いと思いますが、この辺りはあまり左右されない分野です。ですから、自分たちの技術がどこにあるのかを見極めることが重要になってきます。

対話が重要

本日のまとめとして申し上げると、まず国家安全が習近平政権の政策のコアになってきており、そのための中国版経済安全保障が進んでいるということです。二つ目は、中国版経済安全保障の基本的な枠組みを決定している、国家安全委員会を含めた個々のインテリジェンスが極めて重要になります。三つ目は、中国版経済安全保障における自社サービスなり商品なりは、今どこに立ち位置があるのか、それを精査していくことが重要です。

四つ目に、ではそのためにどうすればいいのかというと、実は情報交換が重要です。渡部先生から対話という話がありましたが、役所との対話はもちろんのこと、取引企業

との対話も重要です。あともう一つ、実は意外と重要なのが同業他社同士との対話です。中国のこれまでのいろいろな産業政策によって被害を受けた日本企業の皆さんの話を聞いていると、いわゆる囚人のジレンマにうまく持っていくケースがあります。つまり、同業他社同士が情報交換していないことを逆手に取り、「B社はこんな技術を出していましたが、A社さんは大丈夫ですか」というように、違うささやきをして分断をしていきます。そういうやり方で技術を引き出したりもしています。そういうところから言うと、さらにはひょっとしたら異業種も含めた横の連携、対話が重要だろうというのが今回のポイントになってくると思います。

駆け足になりましたが、私の講演は終わらせていただきます。ご清聴、ありがとうございました。

【講演3】

機微技術・営業秘密の保護に必要とされる措置の最新動向

経団連総合政策研究所 研究委員／
TMI総合法律事務所 パートナー 弁護士

上野 一英

本質的に経済安全保障の問題は、個々の会社ごとに対応策が違う

ＴＭＩ総合法律事務所の弁護士、上野と申します。こういった機会をいただき、どうもありがとうございます。

今日を迎えるまで、研究会の各メンバーの方々とたくさんディスカッションをさせていただいたうちのほんの一部ですが、成果としてこちらで伝えさせていただければと思います。

私は弁護士なので、二つの視点を持っていると思います。日々の業務の中ではお客さまである依頼人に徹頭徹尾応え、必要な対応をします。それは経済安全保障の分野で言えば、法令上必要な対応をする、体制構築をするという平時の対応です。あと、場合によっては有事というのもあり、違反があったときの調査手続きをするなどのインシデント対応があり、その報道対応も含めて考えるようなことをやっています。

もう一つ、この分野を担当させていただくときの自分の視点として大事だと思っているのは、過去に２０１５年から２年ほど経済産業省に出向させていただいた経験です。あとは、日々の業務の中で政府の方々と意見交換をさせていただくこともあり、どこを

上野研究委員

国の政策の経済安全保障として描いているのかを理解しながら、企業の対応を考えることです。

なるべく具体的なことを伝えないと意味がないとは思っていますが、本質的に経済安全保障の問題は、個々の会社ごとに対応策が違うところにポイントがあります。

ただ、この時間を使って有益だと思う点としては、法制度も踏まえ、大きな体系的なところを伝えるところです（46ページ資料8）。

経済安全保障に関する政策の内容と技術に対する「育てる」「守る」の関係

経済安全保障の法令はたくさんあります。それは主に「育てる」と「守る」の二つから成っ

資料８　経済安保に関連する政策動向（半導体関連の例）

育てる（Promotion）	守る（Protection）
●補助等 ◆2030年度までに10兆円規模の公的支援をする「AI・半導体産業基盤強化フレーム」の閣議決定（2024.11.22） ◆今後10年間で50兆円を超える官民投資を誘発し、また、半導体生産等に伴う約160兆円の経済波及効果を実現 **◆減税** 戦略物資生産基盤税制を創設(準備中) ー 半導体について、事業計画認定から10年間 ＋ 繰越期間3年、法人税最大20%控除可能 **●人材育成**（産学の協議、大学等の取組） 6つの地域での産学官連携による取組開始	**●輸出管理** 外為法の下位省令において、先端半導体の製造装置等23品目を許可対象品目に追加（2023.7.23施行） MLCC、SAW・BAWフィルタ、半導体用のリソグラフィに使用するレジスト（248ナノメートル以下の波長の光で使用最適化のもの）について、国外の技術移転の事前許可対象を強化（官民対話スキーム：2024.12.30施行） **●投資規制** 外為法に基づく対内投資管理強化（半導体や蓄電池等の9物資関連業種を追加：2023.3.9） **●秘密特許** 経済安全保障推進法に基づいて創設 **●セキュリティクリアランス**（2025年前半まで運用開始） **●契約上の規制（「ガードレール条項」など）** 特定重要物資、特定重要技術の補助金等に紐づく

（出所）経産省資料に基づき上野作成

ています。

例えば、制度が大きく進展している一つとして半導体関連のものがあるので、これを参考として挙げさせていただきました。「育てる」ところに関して言うと、２０２４年11月22日に政府で閣議決定した「ＡＩ・半導体産業基盤強化フレーム」で、２０３０年までに10兆円規模の公的支援をするとしています。これは単年度予算の原則のもとで、複数年度にわたり国がこういったコミットを示すところに意味があったわけです。経済的な波及効果も踏まえると１６０兆円を超えるものと言われています。あとは減税措置も検討されています。これは事業計画認定から10年間にわたり効果が受けられるということなので、逆に言うと、計画も10年間にわたり立ててくださいというようなことが政府からのメッセージとしてあるわけです。人材育成としても産学の協議や大学等の取り組みが重要だという政策が示されており、これも国内六つの地域で産官学連携による取り組みが開始されているところです。

「守る」ほうは、細かな製品の話になりますが、いずれも安全保障の観点でつながっている重要なところです。ＭＬＣＣ、ＳＡＷ・ＢＡＷフィルタが特定重要物資として指

定され、補助の対象となっています。これに合わせて守りとして、同じ製品に対して２０２４年12月30日施行の官民対話スキームが輸出管理の内容として定められてきています。輸出管理を行うためには、輸出管理の手前の、外国から投資を受ける段階でも技術流出を防止すべきだろうという考え方の下、投資規制も輸出管理の枠と同じ範囲、ないしはそれより広い形でできています。

秘密特許に関しては、さらに先端的な技術分野に限られるわけですが、ゲームチェンジャーとなるような技術を対象とするものです。それが経済安全保障推進法に基づき創設され、運用が始まりつつあります。セキュリティ・クリアランスは渡部先生にお話しいただいたとおりですが、２０２５年の前半までに運用が開始される状況です。

もう一つ重要なのが契約上の規制です。具体的には政府から補助金をもらうときの交付要綱、つまり政府との約束の中で定められた内容です。「ガードレール」条項は懸念国に技術を移転することが禁止される条項で、アメリカのＣＨＩＰＳ法にもあるようなものが日本の中でも定められてきています。特定重要物資、特定重要技術に関しては、補助金を交付するのと同じタイミングで、一定の技術の流出防止策を講じなければいけ

ないとされています。

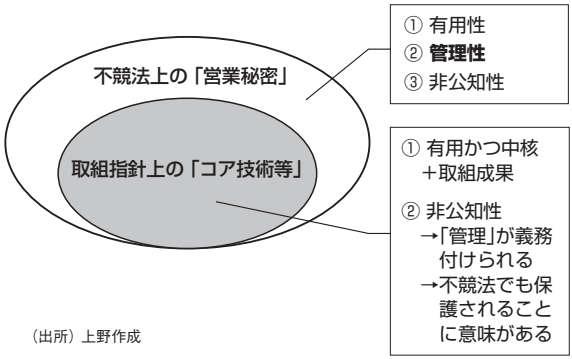
このようなことから、「育てる」ところに対して政府の関与があると、当然、「守る」部分についても連動して規制が出来上がっていく流れがあります。

政府補助金を受けると課される秘密保護義務

もう少し具体的に定義のところを見ると、半導体については、特定重要物資として指定された場合には、この技術流出防止措置が必要となります。その技術流出防止措置の対象はコア技術とされています。それは供給計画の認定を対象とする取り組みにおいて、「生産に有用かつ中核的な技術」であり「取り組みの成果である技術」、流出防止を図るべきものは「コア技術等」と定義されています。いかにも技術的ですが、「コア技術等を守る」の「等」の部分は、「漏れてしまえばコア技術の内容が推知されてしまうような事実」とされています。これについて、技術流出防止措置が必要となってくるということです。

技術の概念として、コア技術等とは何でしょうか。いろいろな用語があり、分かりに

資料９　技術の概念整理



（出所）上野作成

くいところもありますが、先ほどお伝えした「有用かつ中核」であり「取り組み成果の内容」となるものです。これに加えて非公知性が求められます。管理性は要件にはなっていませんでした。なぜなら、管理が義務付けられる対象を定めているのがコア技術等だからです。その外延に、不正競争防止法上の営業秘密というものがあります。この中では管理性が求められ、管理性というものが相まって、不競法上、営業秘密として保護されることになっています（資料９）。

特定重要物資の補助金の交付に伴い、技術流失防止措置を守らなければどうなるかということです。助成金の交付の条件として、一部努力義務のところもありますが、流出防止義務の整備とか流

出後の対処義務が定められているので、これらをやらないということは当然、最終的には交付決定の取り消し、返還義務にもつながります。実際にそれが行われるかどうかはまた別として、制度としてはそのようなものになっているということです。

義務付けられたものでなくても守ることが重要

今の内容は法令で義務付けられる範囲ですが、企業の経済安全保障の観点からは、義務付けられたものでなくても守ることが重要だというところがポイントとなっているわけです。それは峯村さんからお話しいただいたところでもありますが、結局、外部から狙われているからです。外部から狙われているものについて、これまで自社でとっていた措置で足りるのかということを再検討する必要があります。狙われている会社の資産を適切に守るのは自主的な行動ではありますが、ステークホルダーに対しては当然、いかに適切に行っているのかと、説明が求められます。技術を流出させてしまった場合には、国も含めステークホルダーの期待にも反してしまうことになるので、レピュテーション上の大きな損失にもなってしまいます（52ページ資料10）。

資料 10　法令上の義務付けがなくとも「守る」ことが望まれる

育てる（Promotion）	守る（Protection）
•（国のプログラム対象でなく）社内で開発する重要な戦略的技術	• 不正競争防止法（各国） • 民法（不法行為法） • 特許法 • 著作権法 • 意匠法

• 重要技術の流出リスクが増大。流出の企業価値への影響も大きい。
• 自主的な守りが、ステークホルダー（投資家、株主、国）から求められる。レピュテーション上の問題にも発展。

（出所）上野作成

技術を守るためには、義務付けられている法律ではなく、技術に保護を与える法律に従い、適切な体制を組んでいくことが必要になります。不正競争防止法について「不正競争防止法（各国）」と書かせていただいたのは、日本で不法行為が起これば日本の不競法ですが、グローバルな企業として各国に拠点があれば、各国法上で守られるような体制を構築する必要があるからです。それで「各国」と書かせていただいています。

企業が行うべきこと

一つ目は自社の重要技術を認識するということです。技術が流出してしまわないようにする。そのために守るべきものは何かというと、懸念国から狙わ

資料 11　経済安全保障上を考慮し、企業が行うべきこと

① 自社の重要技術を認識
※それぞれの定義・概念にズレがある

② 重要技術に対して必要な措置を講じる
※保護する根拠によって、対応すべき性質・レベルが異なる

③ 必要な範囲で、対応している内容をステークホルダーに伝えること
※ここまで行うことで、**「リスクからバリュー」**に転換
※国への報告義務、有価証券報告書への任意開示事項であることも
※対応が困難な場合や制度の不備等は、政府にフィードバック・協議

（出所）上野作成

れているものが何かを理解することが、大前提として重要です。それで諜報活動技術、情報を集める活動が重要だということは峯村さんからお伝えいただいたところです（資料11）。

あと、法的な保護が与えられるに十分かというところは、例えばその時々に起こっている事例も参考にしながら、ベストのものをその都度改訂していくことだと思います。

ちょうど先週の今の時間帯、私も産総研の裁判を傍聴していましたが、最後の検察官の論告求刑が行われたタイミングで、改めて弁護人側の意見も述べられていました。ここでは無罪を主張していて、2025年2月25日が判決ですが、過去に流出したときの営業秘密について、管理が十分であったかど

うかが4〜5年後に見られていくわけです。ですから、過去にさかのぼって見たときにも管理として十分だったと言えるのかというところを念頭に、体制を置いておく必要があります。とは言え、過度に対応する必要はなく、ポイントを押さえて必要な対応をすることが必要です。この事件で言えば、裁判に影響を与えるつもりは全くないですが、例えば「当時研究していた内容は兼業先のプロジェクトのものであり、その情報を兼業先のほうに送ったにすぎない。ゆえに研究所の技術ではなかったのだ」という弁論をしていました。それが認められれば無罪になる可能性があるのだと思います。ただ、兼業をたくさんしている方がいらっしゃる会社であれば、外部の機関の営業秘密とも混ざりやすい状況がある中でどのように管理をしていくのかということの難しさも、そこではテーマになっているのではないかと思っていました。

これは個々に対応を検討すると、本当に悩ましい場合もあります。もしかしたら後ほど議論をさせていただければと思いますが、では営業秘密はどのように分類し、誰が幾つ持っていて、どのように安全措置を講じればよいということなのか考える必要があります。この部署で保有している技術の内容は何かということについて、「管理するとき

に全部教えて」と言うと、それもまた管理として不適切になってしまいます。それは管理している責任者の方が把握する必要があれば十分ですが、では、それがどのように行われているのかを全社的にどのように管理していくのがよいでしょうか。技術が何個あるかというカウントすら難しいところも、結構あるのではないかとも思います。

あとは、自社の重要技術が何かを特定するときには、ここでも渡部先生からも説明いただいた、政府との対話が重要になってきます。何が狙われているかという情報を直接海外に取りに行くことは非常に危険で、それは政府から得られる情報もあると思いますし、守り方も政府からもらう情報が大変参考になる状況だと思います。企業の視点からすると、政府とはあまり「やぶから棒」が出るような形でやりとりしたくありません。「ここを守らなければいけないのか」と聞くと、「いや、こちらも守ってください」「こちらも守ってください」となるのは怖いところもあるとは思います。しかしそれは、同じ方向をきちんと向いているという、よりコミュニケーションを充実化することで整えられる部分ではないかとも思います。相談する範囲は会社自身が決めればいいことでもありますし、コミュニケーションを何もしないことのほうが、現在はリスクになってい

る部分が多いのではないかと感じています。

二つ目として、重要技術に対して必要な措置を講じることです。お伝えしたとおり、いろいろなものから守ることが求められているので、それぞれに応じ自社が必要な保護レベルを設定し、それに従って対応することになります。セキュリティ・クリアランスの対象にもなるようであれば、窓のない部屋が必要な場合もあるということですし、取締役の方がセキュリティ・クリアランスを取る必要が出てくる場合もあります。米国のビジネスにも参画するのであれば米国基準の情報管理措置が必要になるので、それに対応すべきという話になります。そういったところで自社それぞれ必要な範囲を定めるということだと思います。

その上で三つ目として、必要な範囲で、対応している内容をステークホルダーに伝えることで、自社の対応がただ内部的に完結するわけではなく、それが競争優位性にもつながる話になりうるのではないかと思います。ここは明確な事例があるかと言われると、なかなかなく、これからだと思います。分かりやすいのは、「セキュリティ・クリアランスがあるから私たちとしてはこの分野にも参画できます」ときちんと伝えることもあ

ります。また、「このような保護ができる体制にあるので『K Program』に参画できます」「わが社の技術をより開発して伸ばすべきだと思うので、内閣府のほうでのプログラムの設定が必要ではないでしょうか」というような形のアプローチができると思います。もし脆弱で何か漏えいのリスクを抱えていると、そういったところにも積極的なコミュニケーションがなかなかとりにくいと思います。

他にもいろいろ対応することはあります。狙われている側の技術からすると、直接盗られないにせよ、それに基づきたくさんの製品が中国から来る可能性があれば、またそれを守るための措置が必要です。あとは来年以降、トランプ政権になったときに、経済安全保障を守りながらどういう形で自社の利益を確保していくのかという、さらに大きな問題もあるとは思いますが、技術管理という面では、大きくは以上の三つに集約されるかと思います。

どのような措置を取ればよいか

あとは少しだけ補足で、どのような措置を取ればよいかというところです。各社必要

な対応をされるのだと思いますが、特定重要物資に関する取り決めをされているのであればアクセス管理なども必要になりますし、コア技術に関する守秘義務の制約とともに、取引先の管理もしなければいけないことになります。取引先の管理はかなり重たいものだと思います。

では、サプライチェーンをどこまでやるかというところですが、まずは直接の取引先を中心に契約上、対応します。そこで、ただ契約上押し付けると下請法の問題にもなるので、厳しく守るという北風の部分だけではなく、一緒になってやる必要があります。予算がないと措置をとれないというのは、自社の対応の中でもよく理解いただいているところだと思います。それと同じように、サプライチェーンの中で支援するという持ちかけ方が重要だと考えています。

あと一つ、研究会の議論の中でも、技術に関する横のやりとりをするときに過度に萎縮してしまう事例があると伺ったことがあります。ここは適切に弁護士がアドバイスをすべき部分だと思いますが、競争法的に言うと、共同研究は基本的には競争促進的効果があるものです。開発コストを削減したり、リスクを分散したり、技術が促進されるも

のなので、これは競争にとっていいものだというのが独禁法上の基本的な理解ではあります。

ただ、それに付随して、競争制限的な部分がよくないのです。単なる技術の交換から、ではそれを使うときにどこにライセンスしようとか、どこに使おうとか、それに関して価格はこう設定しようとか、そういうことを含めた瞬間に真っ黒になってしまいます。だから、真っ黒にならない範囲での情報交換という形で限定する必要があり、そうする限りにおいては競争法的にも望まれることではあります。個別の問題は、顧問弁護士にご相談下さい。

いろいろなものを参考にするべきだと思いますが、共同化の必要性として、環境対策とか、安全対策とか、いわゆる外部性の対応の目的とするものについてはやっても構わないというものが例になっています。そういったものも参照にしながら、具体的な横での連携も図るべきだと考えています。

なかなか悩ましい問題で、スライドもつくらせていただきましたが、またディスカッションの中ででも触れられればと思います。私からの説明は以上となります。

パネルディスカッション・質疑応答

【パネリスト】（順不同）

渡部　俊也　経団連総合政策研究所 研究主幹／東京大学未来ビジョン研究センター 教授

長澤　健一　経団連総合政策研究所 研究副主幹／キヤノン株式会社 顧問

峯村　健司　経団連総合政策研究所 研究委員／キヤノングローバル戦略研究所 主任研究員

上野　一英　経団連総合政策研究所 研究委員／ＴＭＩ総合法律事務所 パートナー 弁護士

吉岡　徹　経団連総合政策研究所 研究委員／一橋大学イノベーション研究センター 准教授

森　達也　経団連総合政策研究所 研究委員／三菱重工業株式会社知的財産部 マネージングエキスパート

長期的な視点を持つ

渡部　私がお話しさせていただいた後、峯村さまから今の経済安全保障環境、中国の話をしていただきました。われわれがどういう環境にあるのかということかと思います。その後で上野先生から、「守る」「育てる」ということの少し具体的な内容についてお話をいただきました。少しずつ具体的になってきたわけですが、そうは言っても聴いていらっしゃる企業の皆さんにとっては、もう少し具体的なことを聞きたいというのが多数あろうかと思いますので、ぜひ質問していただきたいと思います。

このディスカッションにはこの3人に加え、あとお三方に加わっていただきます。

まず、長澤さまから、簡単に自己紹介と問題意識をお話しいただければと思います。

長澤　経済安全保障の業務については、私自身も含め、産業界の認識や知見は深い意味ではまだまだ育っていないように感じます。国家安全局は当然そういう業務もされていると思いますが、今は法を立ち上げ、つつがなく施行しなければならないために、時間が相当割かれ、産業界への周知まで手が回っていない感じがします。

しかし、これはある意味で仕方がない面もあり、峯村先生が話されたような政情等に

長澤研究副主幹

関する深い知見に関しては、全ての企業の経済安全保障担当が知っているわけではありません。法律も、知的財産基本法は詳細まで知っているが、「経済安全保障関連法って何だろう」という状況でしょうし、外為法等の関連法も含めて企業内で把握している人はまずいないと思います。そのような状況にありますので、多忙な企業の経済安全保障の責任者は、全てを完璧に理解するというのではなく、感覚で少しずつ把握していくことになります。それから、時の流れや変化をつかんでいくことが大事だと思います。

私も知財部門の責任者を担っていましたが、そのために視点的には長期を見ています。経済安全保障も長期を見なければいけませんが、知

財とは一つだけ違うことがあります。知財の場合は、産業の流れと法律の流れだけなので、ある意味ある程度は将来を読むことができます。そこに地政学リスクが絡んでくると、長期的な視点でありながら、話が急に変わってしまうことが起こり得ます。したがって、長期的な視点を持ちながら、英断をしていかなければいけない。そういうところが経済安全保障の仕事の難しさであると思います。

今回こういうプロジェクトに参加させていただき、経団連参加企業の皆さまのリテラシー向上に少しでもお役に立てられればと思います。

大事な情報をしっかり特定していく

渡部　ありがとうございます。

続きまして、吉岡先生にお願いしたいと思います。今日参加の方の中には、イノベーションとか研究開発に取り組んでいる立場で話を聴いていただいている方もおられるかもしれません。吉岡先生にはそういう専門の立場で参画していただいています。よろしくお願いします。

吉岡研究委員

吉岡　よろしくお願いします。私はイノベーション・マネジメントを幅広く研究しています。今日の話を伺っていて感じたことが2点ありました。

　1点は、技術のマネジメントの観点から申し上げると、ここで求められていることはある種、古典的なマネジメントでも求められてきたことではないかと思います。競争力の源泉をしっかり特定し、また競合が何を欲しているかをしっかり分かった上で自社の戦略を立てていくことです。時代の流れが変わってきて、その重要性が増してきたとはいえ、大事な情報をしっかり特定していくことが重要だというのは変わりないのではないかと感じました。

一方で、難しさというところで申し上げると、一つは政府の政策の役割が徐々に変わってきています。これはイノベーションの分野で特に言われています。政府が地球規模の課題を解決するための政策を実行していくということで、Mission-oriented Innovation Policy というものが出ています。そこには当然ながら、国家の競争力につながる、いわゆる重要技術にかかるところが含まれています。国家の力があり、国家の力を借りて大きなイノベーションを興すようになってきているので、情報の扱いに対し重要性が増しているのではないか。ただ、同時にいろいろなプレーヤーと関わらなくてはならないので、関わるときの情報の出し方、見せ方の難度が増しているのだと、今日伺っていて思いました。

質問いただいた中にもありますが、技術をどう特定していくかはなかなか難しいところがあるように思います。それに対し、オープンソースの情報でどこまで分析できるのか。また、組織内の情報でどこまで分析できるのかが論点かと思います。

知財だけで何かができるわけではない

森研究委員

渡部　ありがとうございます。

最後に、森さまに企業の立場からお願いします。

森　会社では知財を主に見ていますが、経済安全保障の中で知財の果たす役割とは何なのかということを日々考えています。渡部先生からは手段であるという説明もいただいていますが、まさに知財だけで何かができるわけではありません。安全保障の枠組み全体の中で、どのようなポジショニング、どのような役割を背負っていけるかということについて、いろいろ議論できればと思います。よろしくお願いします。

自社の重要技術を認識するには

渡部　ありがとうございます。

それでは、質問を受けているので、順次、回答をさせていただきたいと思います。加わった3人に対しても質問をいただければと思います。

最初は、峯村先生、上野先生に質問です。「自社の重要技術を認識することはとても重要ですが、上野先生の言われるとおり、技術の特定は非常に難しい作業です。技術特定を行ったということであっても終わりのない議論になりそうで、むしろ大事なのは情報の出口をふさぐこと。そこに注力しようという方針に変えたということですが、その取り組みの一つの例として、他に具体的なアイデアがあれば」ということです。

峯村さまからお願いします。

峯村　なかなか難しい質問です。まずは基本的なことかもしれませんが、Need to Know の原則を徹底するところが結構重要ではないかと見ています。これはインテリジェンス機関などでも必ずやるところで、知るべき人のみが知るということです。役所も含め日本の組織を見ていると、何だか適当に扱われているように思います。この間も

海上自衛隊の内部の事件がありましたが、よく分からない上下の関係があって、知るべきではない人に情報を共有していました。意外と、そういうところから情報は漏れていると思います。

もう一つ、いくつかの例を見ていると、中国だけに限らず、最近の情報収集のやり方、重要技術の取り方のアプローチがだいぶ変わってきていると感じます。かつてはプロの人間や組織、いわゆる諜報機関の人間を送り込んだり、ある会社をターゲットにして特定の情報が欲しいから人を潜り込ませたりという形でやっていました。ここ数年のアプローチを見ると、あるターゲットにした技術を持つ会社にいる人を見つけ出し、その方に対するリクルーティングという形で情報を取っています。ですから、この辺りも含め、先ほどの上野先生のおっしゃっていたセキュリティ・クリアランスが重要だろうというのが、今の私の見方であり、対策です。

上野　ご質問の中で、技術の選別がなかなか難しかったので、一つの解決策として出口をふさぐことに注力しようという話をいただいています。私もそのとおりかと思います。ふさぎ方には幾つかのパターンがあると思います。全てを同じように厳しくふさぐこ

とができないのだとしたら、どこまでコストをかけるかという問題もあるので、そのふさぎ方にパターンを設け、少なくともふさぎ方のパターンに応じただけの技術の類型は設ける必要があるのだろうと思います。どの技術を流通させていくかは、ふさぎ方に応じて決まるのではないかというのがまず、大きくあると思います。そのふさぎ方として、どこでどれが求められるかというときに、制度を参考にする余地があると考えています。

その中で、さらにNeed to Knowの原則はそれぞれの段階の中で守る必要があります。具体的には、一番厳しい管理をしなければいけない層の中で、さらにNeed to Knowの原則を徹底させることです。構造的にはそうなるとは思いますが、企業によって他にもいろいろ考えがあるのではないかと思います。

渡部　たぶん、実務でいろいろ経験があると思うので、長澤さま、森さま、いかがでしょうか。

長澤　私から少しだけ。先ほど、上野先生がおっしゃったとおりだと思います。広く網を掛けると網が薄くなってしまい、また抜けやすいわけです。ところが、会社の中では売り上げの高い事業部の声が大きいなど、さまざまな要素が影響して、経済安全保障の

責任者に考えがあっても、その責任者だけではなかなか決定はしにくい面があります。だから、声が大きい人から、峯村先生が説明したカーゴクラスの技術に関して「これは最先端だ、わが社にとっても大変重要なのだ」と言われて、「まあまあ、そうではなくて」と説明しなければいけないので、それができるための知見が必要になってくるということだと思います。

それを実現するには、知財の責任者ではなくても、さまざまな方と垣根なく普通に話ができる人を育てていく必要があります。そういう方を経済安全保障の責任者に置いていくことが大事ではないかと個人的には思います。

森　知財の視点からなので、あまりお答えになら

ないかもしれませんが、特許を出す出さないにおいても出口でしっかり管理していくことは重要ですし、どのように管理するかというノウハウも知財部門の重要な役割だと思います。

セキュリティ・クリアランス制度と労働基準法の矛盾

渡部　次に「セキュリティ・クリアランスの適正評価において、中国の国防動員法、国家情報法が懸念されています。そのことにより、適正評価時に中国籍の方を排除することがあるとすると、労働基準法の第3条（国籍で差別をしてはいけない）に違反する。つまり、セキュリティ・クリアランス法と労基法が矛盾するということはないでしょうか」という質問です。

これは制度の解釈なので、上野先生、いかがでしょうか。

上野　おっしゃるとおり、制度としては矛盾する関係にあると思うので、どちらを優先すべきかというところが問題となります。

それは法律上の必要性がある場合に、セキュリティ・クリアランスに基づく適正評価

に当たるという解釈がされていくと考えています。それは今後、Q&Aなどでも具体化されていくのではないかと思いますが、その必要性があれば、それは差別ではなく必要な区別ということになると考えています。

渡部　今の説明のとおりだと思います。これはQ&Aの中でも新たに反映されるかもしれません。それから、実は適正評価の対象になるものとして、どこの国でも国籍は見ています。それに加え、では特定重要物資を扱うために国の補助を受けた会社は何も見ないでいいのかという議論も、実際には実務的にもっと重要になってきます。そこは現在行われているガイドライン等との関係をどう解釈するか、いずれ論点になるかと思います。

補足

渡部　では、ここまでで何か皆さんから追加的なコメントがあればお願いしたいと思います。

吉岡　まさに上野先生の発表資料にもありましたが、では会社としてどういう体制をつ

くっていくのかというところについては、情報はある程度分散して管理したほうがいいというか、現場に近いところで管理したほうがいい面があります。一方で、先ほど峯村さんがおっしゃったように、知るべき人が知っておくところを考えると、ある程度集約しておいたほうがいいことになります。この辺りのバランスは考える必要があります。

峯村　先ほどの上野先生の「区別する必要性があれば」というお話に若干重ねて言うと、国防動員法、国家情報法への対応は、いわゆる国籍の問題ではなく、あくまでも国の問題です。中国政府は２０１７年に国家情報法をつくり、「中国籍を持っている全ての人間が国家の諜報活動（スパイ活動）に協力する義務がある」という立て付けになっているわけです。そのリスクのある者をヘッジするという意味では、私もこれは差別に当たるものではないと思います。労働基準法とも相反しないものだろうと考えているところです。

上野　私はレジュメでお伝えできなかった部分が一つあります。従業員の管理というと

ころで「特定重要物資に関する取組方針」の中では、「従業員に対し相応の待遇（賃金、役職等の向上）を確保する等の手段により、当該従業員の退職等を通じたコア技術等の流出を防止する措置を講じる」という一文もあります。これはセキュリティ・クリアランスの議論や、技術を「守る」「育てる」というエコシステムを構築する議論には、常に出てくる話の一つではないかと思います。

極端な話、セキュリティ・クリアランスであれば渡航制限などにも関わるようなものを、待遇も上がらずに果たして受けられるのかという問題です。そこまでではないとしても、いろいろな事務手続き上の煩雑さが増すものを従業員に課していいのかという議論があり、そのためにはある程度待遇も向上させることが望ましいのではないかという問題意識として表れてきていると思います。さらに言うと、技術を育てても退職してしまっては意味がないので、給料を上げないといけない、魅力的な職場にしないといけません。とは言うものの、日本は各国との給与水準で差があります。そういう話はアカデミアの中にもあるかと思います。

そういう問題意識が凝縮していて、やや不明瞭な文章になっていると思います。実際

に待遇を上げれば技術流出防止措置として十分なわけではないので、これをどう実装するかは非常に悩ましい問題ではあります。ただ、締め付けと待遇は常に両方考えるべきだという視点はここで表れていて、非常に重要なテーマだと思います。

渡部　そこに着目していただいたのは大変ありがたいことです。

セキュリティ・クリアランス側の議論だと、目的外利用という概念とのコンフリクトの範囲をどのように整理するかということはありますが、基本は同じ考え方です。適正評価を受けたから直ちに給与が上がることは目的外利用に当たるけれども、そういう重要な役割を果たす業務に対しての処遇であれば可能であるというのは、確かQ&Aのほうにも書かれているので、その辺は参考にしていただければと思います。

本音で話ができる場をつくる

長澤　先ほど申し上げましたように、経済安全保障関係の問題をどうやって処理するか、営業秘密をどうやって守るかという話は、非常にたくさんの知見が必要になります。そういう意味では、上野先生の資料に「旗振り役を設ける」と書いていただいていますが、

資料12　おわりに

➢ **旗振り役を設ける**

コアメンバー　＋　関係部署メンバー　＋　外部専門家
法務、輸出管理、経営企画、調達、研究開発、人事、「経済安全保障室」
目線合わせのための社内研修は必須。
いずれは内製化を目指す。

➢ **分断をつなぎとめる原動力は、民間企業以外にあり得ないのではないか**

能動的に政府と関わる姿勢が必要。
良い製品を作れば売れるというわけではない状況の認識。
リスクからバリューへ。

（出所）上野作成

組織に「経済安全保障室」のようなものをつくると、とりあえず枠組みができます。その枠組みの中で、ここに書かれている法務の専門家、外為法の専門家、経営企画の方々、それから処遇を考えると、ここに人事を入れるのはすばらしいと思います。まず、こういったメンバーが本音で話せる場をつくることが第一歩になると思います（資料12）。

場をつくった上で、誰かがその課題を拾い、ある程度の決断をしていかなければなりません。その中で非常に大事な点は、「うちの会社は何でめしを食っているのだろう」というところに一度戻り、それを中心に守っていくことです。そのための経済安全保障の営業秘密管理や人事制度をこう

いうメンバーで話し合い、まず土台をつくるのです。そして、できれば、「とにかく自分がこれをやっていくのだ」という責任感のある旗振り役を育てていくことです。企業にとってはそれが一番の早道ではないかと思います。

渡部　これは組織をどのようにつくっていくかということですが、企業の立場で森さま、いかがでしょうか。

森　事業を進める上で何が秘密で何が秘密でないかというのは、旗振り役が全ての業務に関わっていく必要があります。また、事業によっては、国の方針や国際的な情勢をにらんでの長期的なものになるので、何を秘密にする、しないというのは、1社ではなかなか決めにくいところもあります。先ほど企業同士で横連携というのがありましたし、関係省庁等とも相談をして、秘密にする、しないといったところをまとめていければと思います。

渡部　先ほど、企業の横の情報共有というような話もありましたが、これは日本の企業同士ということに加え、海外と共有するとまた異なるメリットがあるのではないかと思いますが、その辺はいかがでしょうか。

峯村　これはむしろ海外のほうが進んでいます。例えば、中国に関しては中国ＥＵ商会があり、アメリカにも似たような団体があります。こういうところとの連携は非常に有益です。基本的に中国のアプローチについては、特に産業政策ではその辺りの団体から情報を拾っていくと、彼らの狙いは何なのかというところが見えてきます。そこからプロテクト（守り）をどうすればいいのか考えられるようになります。

ただ、これをやるには、インテリジェンスの基本はエクスチェンジ（情報交換）なので、ただ日本側がくださいと言うのでは全く相手にされません。だから、そこはしっかりと知的な理論武装をした上で行くことになります。まず、そのためのプラットフォームが必要だというところは強調しておきたいと思います。

長澤　いわゆる同志国のような国々でも、われわれ日本企業よりもはるかに高い知見を持っている場合があります。例えば、韓国や台湾です。そういったことに対する認識は彼らのほうがはるかに高いと思うことがよくあり、彼らから出てくる言葉はかなり参考になった記憶があります。

それから、もちろんアメリカです。ヨーロッパよりもむしろアメリカの方々がこれを

すごく懸念されているので、雑談になるとその片鱗が次々と出てきて、同業であっても「ここは組まなければね」という話になる可能性は高いと思います。上野先生がおっしゃったように、工業会などを利用して日本企業同士で徒党を組んでおいたほうがいいのはもちろんですが、海外の方と話をするメリットはあると思います。

渡部　時間が来てしまいましたので、これで終了させていただきたいと思います。

こちらの「経済安全保障と知財」のプロジェクトは、実は今まで毎月のようにディスカッションしてきました。今日はその中で公表できる話をさせていただきました。引き続き研究活動を続けていくので、個別のご相談も含め、皆さまとまたさまざまな形でディスカッションができればと思います。

以上です。ありがとうございました。

シンポジウム

企業が直面する リスクとチャンス
～変化し続ける経済安全保障 環境を踏まえて～

2025年9月2日発行

編集　一般社団法人 日本経済団体連合会
経団連総合政策研究所

〒100-8188 東京都千代田区大手町1-3-2

TEL　03-6741-0901
FAX　03-6741-0902

ホームページ　http://www.21ppi.org

Keidanren

Policy Research

Keidanren

経団連総合政策研究所