技術情報等の適正な管理の在り方に関する研究会

報告書

平成２０年７月

目　　次

Ⅰ．総論 5
はじめに 5
技術情報等の保護の重要性 7
（１）基本的視座 7
（２）産業の国際競争力確保の視座 7
（３）安全保障の確保の視座 9
技術情報等の流出ルートの整理 10
検討のアプローチ 18

Ⅱ．各論 23
第１章　競争力の視点 23
１　イノベーションを生み出す制度整備について 23
第１節　現状と問題点 24
（１）無形の知的資産の重要性と情報保護の必要性 24
（２）オープン・イノベーションの促進のための環境整備 31
第２節　具体的対応 33
（１）技術情報等の適切な法的保護の在り方に関する検討 33
（２）営業秘密保護のためのガイドラインの見直し 35
（３）企業における技術情報等の権利帰属問題に関する検討 36
（４）技術情報等の開示・共有インセンティブを創出するための仕組み 38
（５）企業買収を通じた技術情報等の流出への対応 39
２　グローバル競争時代における国富増大のための環境整備 39
第１節　現状と問題点 40
（１）海外からの人材の受入れと活用の必要性 40
（２）オープンなグローバル競争の成果を我が国の国益へ還元する仕組み 44
第２節　具体的対応 46
（１）バイドール制度の見直しによる国費研究成果の流出防止 46
（２）第一国出願制度の検討 47
（３）ボランティア等を通じた海外への重要技術の流出への対処 48

第２章　安全保障の視点 52
第１節　現状と問題点 52
（１）安全保障上の機微技術と民生技術の区別の曖昧化・流出ルートの多様化 52

（２）安全保障関連の機微技術情報を共有する基盤 53
第２節　具体的対応 55
（１）重要情報の区分ルールの導入 55
（２）機微技術リスト・ガイドラインの作成 58
（３）秘密保護法制の在り方 60
（４）秘密特許制度の検討 63
（５）外為法の技術取引規制の強化 64
（６）投資を通じた安全保障上重要な技術の海外への流出防止 66
（７）不審アクセス情報の報告と注意喚起の仕組み 66

第３章　企業における情報管理 70
１　企業の情報管理の促進について 70
第１節　現状と問題点 70
（１）技術情報等を秘密として管理することの困難性 71
（２）棚卸し・価値付けの重要性 72
第２節　具体的対応 74
（１）適切な情報資産管理の促進 74
（２）官民フォーラムの立ち上げ 74
（３）技術情報等の適切な法的保護の在り方に関する検討 76
（４）営業秘密保護のためのガイドラインの見直し 77
（５）特許公開を通じた我が国の有用な技術情報等の流出への対処 77
２　海外への技術情報等の流出防止 78
第１節　現状と問題点 78
第２節　具体的対応 79
（１）官民フォーラムの立ち上げ 79
（２）技術移転に伴う技術流出の防止 79
（３）技術情報等の保護のための国際協力の枠組みの検討 79
（４）海外アウトソーシング時のリスクチェック手法の検討 79
３　中小企業からの技術情報等の流出への対応 80
第１節　現状と問題点 80
（１）中小企業における不十分な管理による技術情報等の流出 80
（２）取引先を通じた中小企業の有する技術情報等の流出 81
第２節　具体的対応 82
（１）中小企業の管理の実態に沿った営業秘密保護のためのガイドラインの策定 82
（２）秘密保持契約締結の重要性の周知徹底 82

（３）中小企業の情報管理支援 83
（４）取引適正化の取組の推進 83
（５）情報管理策に関する中小企業向け普及啓発 83

第４章　大学における情報管理 86
第１節　現状と問題点 87
（１）今日の大学の役割（知のプラットフォームとしての機能） 87
①産業との新しい役割分担 87
②知のプラットフォームの提供 88
（２）大学における情報管理の在り方 91
①大学組織の特殊性について 91
②学問の自由 93
③研究者倫理について 95
第２節　具体的対応 97
（１）研究情報の外部公表の可否判断：組織的管理の実践と支援 97
（２）政府資金で行われた研究成果の公開原則の見直し 98
（３）外為法の施行支援 100
（４）ミスコンダクトへの制度的対応：研究者倫理の在り方 100
（５）アカデミアと安全保障関係者の対話 101

第５章　政府における情報管理 104
第１節　現状と問題点 104
第２節　具体的対応 106
（１）重要情報の区分ルールの導入 106
（２）セキュリティ・クリアランスの導入 107
（３）秘密保護法制の検討 107
（４）政府及び政府契約企業における情報保全の在り方 108

委員名簿 111
検討経過 112

Ⅰ．総論

はじめに

近年、企業、大学、政府からの重要な技術情報等[1]の流出が、産業競争力及び安全保障上の観点から大きな問題となっていることが指摘されている。こうした技術情報等の流出は、様々なかたちで発生し、不法行為として行われるものもあれば、合法的な取引のかたちで行われるものもある。技術情報等の流出により損なわれる利益も、企業の競争力を喪失させるものから国家の安全保障を脅かすようなものまで様々である。

技術情報等の適正な管理については、これまでも個々の企業のレベルから政府の各省庁のレベルに至るまで、個々の局面の対応がなされてきたところであるが、それぞれの政策部門が縦割りで部分的・局面的に対応を検討し措置するに止まっており、我が国社会全体として整合性のある検討が十分になされてきていない。このように技術情報等の適正な管理の在り方に関して総合的な対応がなされないと、十分に実効的な対応ができなくなる可能性がある。

技術情報等の流出形態や流出によって失われる利益は多様であることを踏まえれば、新たにグローバル競争時代において我が国が適切に国益を確保するための情報管理のあるべき姿についてゼロベースで見直してみることが必要である。本研究会では、技術情報等の管理に関して、「情報」の種類、「流出経路」、「失われる利益」のそれぞれについて、包括的な検討を行い、全体を鳥瞰する基本的な考え方及び今後の政府全体の基本的検討の方向を提示することを目指すものである。

（参考）近年発生した技術情報等の流出の具体例

○　外国政府によるデュアル・ユース技術の不正取得

元在日ロシア通商代表部員が、光学系機器メーカー従業員から、軍事転用されるおそれのある光通信の機密部品を不正に入手した。元在日ロシア通商代表部員は警察の出頭要請に応じず帰国し、元従業員についても起訴猶予処分となった。

○　外国人従業員による機密情報の不正な持ち出し

自動車部品メーカーに勤務する外国人従業員が、図面データを貸与パソコンに大量にダウンロードし、繰り返し自宅に持ち帰っていた。同社が従業員に事情聴取を行ったところ、貸与パソコンにデータは残っておらず、私用パソコンは破壊されており、データの使用や外部への持ち出しについて確認することはできなかった。

[1] 本報告書における「技術情報等」は、技術、ノウハウ、図面、デザイン、仕様書、作業手順書といった技術的な情報のみならず、経営計画、顧客・取引先情報、政府の重要情報・機密文書等も含めた、所有者にとって資産性又は価値を有する情報のことを指すものとする。

以前から母国への渡航を繰り返していたその従業員は、パソコンの横領罪で逮捕されるも、起訴猶予処分となり、既に母国へ帰国している。

○　元従業員による営業秘密侵害と刑事事件化の断念

A 社の元従業員 X が、在職当時にアクセス権のあった営業秘密をコピーして保有しており、退職後に海外競合企業 B 社に営業秘密を開示したことが明らかになった。以前、B 社からはライセンス供与の申し出があったが、A 社はこれを断った経緯がある。

A社は、B 社に対して厳重な抗議を行うとともに、元従業員 X の刑事告訴を検討したが、裁判で営業秘密の内容が明らかにされてしまうおそれがあるため、刑事告訴を断念した。元従業員は A 社との示談に応じたものの、営業秘密侵害によって生じた損害を埋め合わせるものではなかった。

○　元従業員による営業秘密の不正な持ち出しと二次被害の拡大懸念

ある従業員が、転職前にアクセス権限のない秘密情報を持ち出し、自宅のパソコンにコピーして保存していたところ、その情報がウィニーにより流出した。企業は当該職員の刑事告訴を検討するものの、営業秘密が流出していることが法廷の場で明らかになることによって、二次被害が拡大することを懸念して、刑事告訴に踏み切らなかった。

○　新製品データの不正流出

ある企業の新製品データが正式公表前に雑誌にスクープされ、経営戦略上の大きな痛手となった。

流出させた人物を特定しようとし、当該情報にアクセス可能性のあった者の中から数名にまで絞り込んだものの、最終的に犯人は特定はできなかった。

○　ジョイントベンチャーによる新設工場レイアウトの流出

ある企業では、外国企業とジョイントベンチャーを組むこととなり、新設工場レイアウトについて秘密保持契約を締結した上で開示した。しかし、外国企業は当該プロジェクトを遅延させるような行動を取るとともに、独自に同様のレイアウトで工場を建設してしまった。

当該海外企業に対して文書で抗議をするものの、実効的な法的措置は採ることができなかった。

○　発注元企業による中小企業からのノウハウの持ち出し

大手企業から、試作品を製品化するよう持ちかけられ、その間、特許出願の方法については後日相談するからそれまでに絶対に公知にしないように言われた。半年経っても連絡が来ないため、確認をしたところ、当該大手企業が独自に特許出願をし、製品化されてしまった。クレームを申し入れたところ、当該大手企業は、従前から当該商品に関する研究開発をしていたと主張して取り合ってもらえなかった。

○　イージス艦中枢情報の流出

自衛隊員が自宅に隠し持っていたイージス艦中枢情報の資料が流出した。自衛隊員は、日米相互防衛援助協定等に伴う秘密保護法違反容疑で逮捕された。

出所：経済産業省知的財産政策室による企業ヒアリング
特許庁『平成 19 年度産業財産権制度問題調査研究報告書（知的財産としての技術情報等の保護・管理のあり方に関する調査研究報告書）』
新聞報道等

技術情報等の保護の重要性

（１）基本的視座

技術情報等の適正な管理の在り方を検討するに当たり、まずもって踏まえるべき点を述べれば下記のとおりである。

第１に、知識社会の進展に伴い、有形資産から無形資産へと価値の源泉が移行しつつあり、企業の競争力の源泉も、こうした無形資産たる情報をいかに創出、管理、利用していくか、換言すれば、無形資産たる情報をいかに緻密にコントロールしていくかという点に移転しつつあるという点である。

第２に、こうした情報は、そもそも投資活動の結果であり、個別財産的に捉えることができる一方で、様々な個々の財産を生み出す源としての性質（根源性）を有していることである。すなわち、「財物」にあっては１度しか消費できないが、「情報」にあっては何度でも消費することができ、何度でも売れる商品・サービスを生み出す力がある。また、ある一つの情報が、産業競争力の観点から重大な意義を有することもあれば、安全保障の観点から重大な意義を有することもあるという具合に、多面的な機能を発揮する場合がある。

第３に、技術情報等は、いったん伝播すると、瞬時に拡散する可能性を有することとなり、その伝播の流れを発信者がコントロールすることが著しく困難又は不可能であるという性質（コントロール不可能性）を有する。すなわち、「財物」にあっては、占有者の下に戻せばコントロール可能性を回復することができるが、「情報」にあっては、いったん他者が知ることとなった以上、その者からの情報の伝播ルートについて限定を加えることはほぼ不可能である。また、別の捉え方をすれば、外部性を強く有するとも言えるのであり、いったん、発信された情報は、それを直接知ることとなった者のみならず、間接的に知り得た者も自由に活用することができることとなる。

（２）産業の国際競争力確保の視座

グローバル化した今日の国際競争環境の中で我が国が競争力を維持・強化していくためには、グローバルな文脈で対外的にオープンな姿勢を貫きつつ資金、知的財産、人材等を受け入れながら価値創造を行うことが不可欠となっている。そうしたオープンな市場を追求する流れの中で、競争力の源泉たる無形資産の取扱いについて基本的な考え方を確立する必要がある。

無形資産の重要性が高まる時代においては、根源的であるにもかかわらず、いったん発信されるとその流れをコントロールするのは不可能であるという性格を有する技術情報等について、仮に法的な保護を与えない場合には、他者にフリーライドされることをおそれ、技術情報等自体の生産が躊躇されるか、他者に開示しないこととなり、いずれにせよ技術情報等の市場への提供が過小供給になるおそれがある。こうした状況に陥るのを防止する

ため、現行制度では、特許法、実用新案法、意匠法、商標法、著作権法、不正競争防止法等の知的財産関係法により、一定の限度において、情報それ自体を資産として保護することとし、これを前提に市場の関係者は行動しているということができる。

もっとも、こうした制度をグローバルな視点から検討する場合には、新たな問題が生起する。すなわち、IT 技術の進展によって「技術情報等」がグローバルに伝達される可能性は著しく高くなっているところ、知的財産関係法の適用は、原則として国内に限定されると考えられるから、意図した伝達であれ、意図せざる伝達であれ、技術情報等がグローバルに伝達されることとなる場合には、公開することによりデファクトを形成して今後のビジネスチャンスに繋げるための情報でない限り、基本的にフリーライドされる懸念に直面することとなる。これまでのように、改善・改良型の企業活動によってキャッチ・アップが求められた時代には、こうした事情に特段の配慮を行う必要はなかったが、創造型・革新型の企業活動によって収益を得ていかなければならない今日にあっては、この懸念は、より深刻化することとなる。したがって、公開情報、非公開情報の別、意図した公開か意図せざる公開かの別を問わず、我が国の情報の取扱いに関する制度設計が、グローバルな視点においてフリーライドされる制度設計になっていないか、について十分に検証する必要がある。

なお、このような視点は、技術情報等の囲い込みを行い、オープンな市場を目指す流れに逆行するものではないことに留意が必要である。すなわち、グローバルにオープンな市場とは、一方が他方に完全にフリーライドされるのではなく、知的資産の創出のために一定の投資をした者が、それに応じたリターンを公正に得ることができる市場を意味するからである。確かに、他者に一方的にフリーライドされることになっても、時として国際経済全体としての利益の最大化に資する場合もあり得るが、我が国の市場においてなされた投資に見合った利益の配分が我が国に帰属していないとすれば、我が国が自由な市場競争の配当を十分に受け取ることができてないことを意味し、我が国経済にとっては、望ましくないことである。

知的資産の創出のために一定の投資をした者が、それに応じたリターンを公正に得ることができるようになっているかという視点からは、特許法等の公開することを前提に保護を図る制度にあっては、こうした制度の安定的な運用が求められるほか、我が国の資源を利用してなされた成果については、我が国においてまずもって権利化がなされる環境整備を図ることが求められる。

また、不正競争防止法等の秘密管理をすることを前提に保護を図る制度にあっては、その制度が真に実効的に機能することが求められる。すなわち、企業が秘密管理している情報に対する不正な侵害行為が実効的に抑止されない場合には、更なる莫大な費用を掛けて管理を行わざるを得なくなり、国際競争を勝ち抜く上で大きなコスト負担を生じさせることになる。更に、自前の技術・ノウハウのみに固執せず、他者の技術・ノウハウをも活用して事業化を図るいわゆるオープン・イノベーションの推進が求められる昨今にあって、

不正な領得行為が実効的に抑止されない環境では、自らの秘密情報を他者と共有しようという状況が構築されることが著しく困難になり、特に、グローバルな企業連携を構築することに大きな支障が生じかねない。情報の流通が不完全な状況では、市場機能が有効に発揮されることは困難なのであり、いかにして情報をコントロールした状態で、限定的に公開するかが求められる。

こうした制度環境が整備されれば、当該情報を生み出したリターンの帰属・管理責任の所在が明らかになり、それによって相互に連携が高まることが期待される。逆に言えば、当該情報を生み出したリターンの帰属・管理責任の所在が明らかにならなければ、既存の技術分野を超えた異種技術を組み合わせることで、新たな付加価値を創造するということを実現するのは、困難なものと考えられる。

（3）安全保障の確保の視座

安全保障を巡る国際社会の変化、技術革新による民生・軍事技術の融合により、安全保上の機微技術の流出リスクが高まっている。すなわち、昨今、安全保障上の機微技術と民生技術の区別が曖昧化した結果、そうした技術がもたらす社会的影響の見極めが困難になるという事態が生じている。また、こうした機微技術が流出するルートも、デジタル情報等の無体物に「化体」したものも含め、非常に多様なものになりつつある。こうした中での機微技術の流出は、我が国及び他国の安全保障に対する脅威並びに我が国の信頼低下につながる問題をもたらしかねない。

したがって、特許出願等の合理的な経済活動としてなされた行為を通じた公開情報が、安全保障上の機微技術を流出させることとなれば、結果として社会に対して回復し難い損害を与えるものとなり得ることに留意する必要がある。また、国費を用いて得られた研究成果は、国民に当然に還元されるべきであることを踏まえれば、その成果を公開すべきことになるが、当該技術が安全保障的な側面を有する場合にこれを公表することになれば、先述した情報の外部性により、国民の安全安心を損なわしめることとなり、かえって納税者の不利益にもなりかねないことに配意する必要がある。したがって、そのような安全保障上機微な情報の公表の是非、及び公表する場合にはその望ましい在り方について慎重な対応が求められる。

また、（2）で論じたことと同様に、安全保障の確保の観点からも、秘密情報の不正な侵害行為に対する抑止が実効的になされる制度環境を整備することが必要である。すなわち、こうした環境が整備されなければ、一定の関係者の間で機微な技術情報等を共有するという体制を構築することが不可能となり、我が国が安全保障上有用な技術情報の提供を受けることが極めて困難になる。このように本来必要とされる関係者との間での情報共有が実現しない場合には、当該技術のさらなる発展やカウンターメジャー（対抗手段）の開発に向け、技術の精度を言論市場の中で精査し、高めていくということが困難になるため、我が国の安全保障を充実させることに必ずしもつながらない。

技術情報等の流出ルートの整理

技術情報等の流出は、様々なかたちで発生し、不法行為として行われるものもあれば、合法的な取引のかたちで行われるものもある。技術情報等の流出により損なわれる利益も、企業の競争力を喪失させるものから国家の安全保障を脅かすようなものまで様々である。

このように技術情報等の流出形態は多様であることを踏まえれば、技術情報等の流出の防止のための十分な政策効果を得るためには、それぞれの流通形態における課題を包括的に検討する必要がある。

本研究会では、こうした認識に基づき、技術情報等の流出に係る「情報」の種類（帰属の別、秘密情報／公開情報）、「流出経路」、「失われる利益」のそれぞれについて、包括的な検討を行い、総合的な対策を講ずることを目指すこととした。

図表１は、上記に従い、「情報」の種類、「流出経路」、「失われる利益」について、企業や有識者からのヒアリングを基に整理を行ったものである。

図表１．技術情報等の流出問題の類型整理

【秘密情報の必ずしも違法でないと考えられる流出】

事例Ａ１：企業が秘密管理している技術情報等を、外国政府を利するために窃取した

→第３章１第２節（３）技術情報等の適切な法的保護の在り方に関する検討

現行の法体系では、外国政府を利する目的で行われる技術情報等の窃盗・領得・複製の作製等が、必ずしも処罰されない。

これは我が国の産業競争力のみならず、安全保障等の観点からも重大な問題を提起する。

今後は、こうした行為を規制の対象とするための法的枠組みの創設について検討すべきである。

事例Ａ２：特定懸念国とつながりのある投資家による買収を通じて安全保障上の機微技術が流出

→第２章第２節（６）投資を通じた安全保障上重要な技術の海外への流出防止

自由な投資活動の結果として、我が国の国益としての安全が阻害され、企業買収により安全保障上の機微技術が海外に流出することがあってはならない。

昨年、安全保障上の機微技術が海外に流出することを防止する観点から、外為法の外資規制の対象に、軍事転用の蓋然性が大きい先端素材や工作機械、電子部品等の製造業を追加する等の抜本的な改正が行われた。今後とも、OECD ガイドラインに則して、引き続き外為法の規制により対応することとすべきである。

事例Ａ３：海外の企業が、世界有数の技術力を有する我が国企業を買収し、技術情報等が流出

→第１章１第２節（５）企業買収を通じた技術情報等の流出への対応

企業買収により技術情報等が流出し、ひいては我が国の産業競争力への影響があるのではないかとの指摘があるが、海外の資本により企業が買収されることとなっても、現に当該企業が我が国で活動する以上は、当該企業の有する技術が海外に流出する訳ではないことに加え、実際には、倒産しかねない状態にある企業が、海外資本から救済を受けることにより、当該技術を利用した我が国での企業活動が引き続き可能になり、国内の雇用が確保されることも期待されることに配慮が必要である。

したがって、相互主義の下、グローバル市場の恩恵を享受している状況を踏まえつつ、基本的には、投資規制については、OECD ガイドラインに則して、引き続き外為法の規則

により対応することとすべきである。

事例Ａ４：自宅作業用に極秘資料を持ち帰り、私用パソコンにコピーしたところ、ファイル交換ソフトを介して秘密情報が流出 事例Ａ５：重要情報の入った鞄の置き忘れ、メール誤送信、不用意な会話、データ消去が不十分なパソコンの廃棄等を通じて秘密情報が流出

→第３章１第２節（１）適切な情報資産管理の促進

従業員が就業規則や秘密保持契約に適切に従っている場合であっても、様々ないわゆる「うっかり流出」が発生する可能性があり、現にそうしたかたちでの企業からの秘密情報の流出が相次いでいる。

こうした事象は、各個別企業の競争力に影響を与えることは言うまでもないところ、まずもって各個別企業の自主的な管理を促すことが求められる。

企業内の技術情報等の管理に際しては、各企業において、いかなる情報を秘密管理し、いかなる情報を公開するかの判断を適切に行うことが重要であり、そうした判断を前提として、秘密管理が行われることとなる。

こうした情報管理を推進するためのガイダンスとして、「情報システム・情報セキュリティに係る内部統制ガイダンス」（仮称）の検討を行うとともに、情報管理等に関する先進的な取組を集めた事例集についても検討すべきである。

また、個別の「うっかり流出」に対処するためには、就業規則等において社外における企業情報の管理について言及する等の対策の深堀が必要である。

事例Ａ６：刑事裁判の公開原則による訴訟時の情報流出

→第１章１第２節（１）技術情報等の適切な法的保護の在り方に関する検討

企業秘密の侵害行為の救済を求める刑事裁判では、技術情報等の内容がその手続を通じて公開されることとなり、違法行為を抑止すべき公的手続自体が第２の法益侵害を招来するため、その結果として、違法性・有責性の高い者ほど、刑事手続で処理されないという矛盾を抱えている。

技術情報等の保護に関する法執行が確実になされるよう、こうした矛盾を改善するための手当を検討すべきである。

事例Ａ７：安全保障上の機微技術を保有する企業において、外国人従業員に技術提供した結果、技術情報が流出

→第２章第２節（５）外為法の技術取引規制の強化

情報技術の進歩やグローバル化に伴う人・モノの流動化によって、外為法で規制している安全保障上の機微技術について、新しい規制の在り方が求められている。

具体的には、現行制度が対象としている「居住者・非居住者」間の規制では捉えることのできない外国籍居住者による安全保障上の機微技術の国外への持ち出し等についても、新たに「ボーダー規制」として捕捉する手法について検討すべきである。

また、安全保障上の機微技術が懸念者によって取得された場合には、回復が困難になることにかんがみ、安全保障上特に機微な技術の保有者に対する内部管理の義務付けについて検討すべきである。

【秘密情報の違法と考えられる流出】

事例Ｂ１：外部からのアクセス（ハッキング、盗聴等）により技術情報等が流出
事例Ｂ２：従業員が、金銭目的で競合他社に技術情報等を漏洩した。
事例Ｂ３：事業提携により一方の企業が他方の企業に対して自らの企業秘密を開示し秘密保持契約を結んだところ、企業秘密の開示を受けた企業がこれを秘密保持契約に違反して自ら独自のプロジェクトのために利用した。
事例Ｂ４：高付加価値製品の製造工場を海外に移転したため、現地従業員を通じてその製造方法が海外に流出

→第１章１第２節（１）技術情報等の適切な法的保護の在り方に関する検討
→第２章第２節（７）不審アクセス情報の報告と注意喚起の仕組み
→第３章１第２節（３）技術情報等の適切な法的保護の在り方に関する検討

現行の不正競争防止法における営業秘密侵害罪は、原則として使用・開示行為を実行行為として捕捉することとしている。

しかしながら、営業秘密の使用・開示行為は、侵害行為者の自宅等といった企業の外部で行われることが多く、その立証も極めて困難であり、営業秘密侵害行為に対して十分な抑止力を果たしていないとの指摘があり、また、侵害者の取得行為により営業秘密が保有者の管理の及ばない状態にさらされることは、営業秘密の瞬時に公開されてしまう性質や、公知化されてしまえば元に戻すことは不可能であるという性質にかんがみれば、それ自体保有者にとっては脅威であると言える。

こうした指摘を踏まえ、不正な手段による領得行為を実効的に抑止することができる法的な枠組みを検討すべきである。

また、外部からの情報への不審アクセス行為については、その警戒度を上げるため、米国に倣い、不審情報報告制度の導入について検討すべきである。

事例Ｂ５：取引先である中小企業の管理が適切でないことにより、技術情報等が流出

→第３章３第２節（３）中小企業の情報管理支援

中小企業においては、人材・資金面の不足から、十分な技術情報等の管理体制を構築することができず、最終製品を製造する企業においていかに情報管理を厳格に行おうとも、部品等を供給する取引先中小企業が情報流出の抜け道になっているとの指摘がある。更に言えば、海外競業企業が、情報管理の不十分な中小企業を狙って情報を入手するケースもあるという。

これを放置することは、重要な技術情報等の海外流出を招くとともに、中小企業にとっても場合によっては民事上・刑事上の法的責任を問われることにもなりかねないことから、中小企業及び取引先が管理策のチェックリストとして活用することができる情報セキュリティ標準フォーマットの作成、知的資産の「見える化」を通じて適正な技術情報等の管理を促進する知的資産経営報告書の作成支援等、中小企業の情報管理能力を高めるための政策支援について検討すべきである。

事例Ｂ６：法令上の要請に基づき提出した技術情報等が、政府当局より流出

→第５章第２節（３）秘密保護法制の検討

政府職員は、国家公務員法上の規定により、おおよそ実務上取り扱う全ての情報について、その重要度にかかわらず一律に秘密保持義務が課せられている。

しかしながら、これに違反して秘密を漏らした場合は、一年以下の懲役又は五十万円以下の罰金に処するとされているのみであり、諸外国に比して罰則が緩いのではないかとの指摘があり、事実、累次の政府からの情報漏洩事件によって、我が国の信頼の低下等の弊害を生じている。

そのため、我が国の国益の保護を図る観点から、我が国にふさわしい秘密保護法制の在り方を検討すべきである。

【公開情報の必ずしも違法でないと考えられる流出】

事例Ｃ１：競合他社が、製品の部品構成や部品納入企業の情報を入手・解析することで重要な技術情報等を入手
事例Ｃ２：競合他社が、HP 等の公開情報を入手・解析することで重要な技術情報等を入手
事例Ｃ３：工場見学、展示会、見本市等を通じた技術情報等の流出

→第３章１第２節（１）適切な情報資産管理の促進

企業間競争が激化する中で、公開情報を通じてライバル企業の重要情報を入手する活動が盛んに行われている。こうした活動は合法的である限り、それを防止することはできないことから、技術情報等の公開に当たっては、何を公開し、何を秘密管理するかの判断を適切に行うことがまずもって重要である。

このような技術情報等の格付けは CIO（Chief Information Officer：最高情報責任者）等が先頭に立ち、経営戦略と技術開発戦略との整合性を考慮しながら、経済的視点及び技術的視点の双方から判断することが適切であり、こうした CIO が適切に機能するための方策として、例えば CIO の職務執行の管理について監査役による監査の対象とすること等、技術情報等の格付けを促進するために、内部統制ルールの在り方を含めて総合的に検討すべきである。

→第３章１第２節（２）官民フォーラムの立ち上げ

企業が技術情報等を管理する際、どのような対策をどのレベルで講ずるかが各企業にとって大きな悩みとなっている。そうした企業の情報管理体制の構築に資するため、産業界と政府とが一体となったコンソーシアムを形成し、技術情報等の漏洩事案の収集及び企業へのフィードバック、事故情報データベースの構築、企業向け指針の策定等を通じて、一層の技術情報等の管理の促進策について検討すべきである。

事例Ｃ４：政府資金による研究成果の公開原則による技術情報等の流出

→第４章第２節（２）政府資金で行われた研究成果の公開原則の見直し

政府資金で行われた研究成果については、産業の発展や更なる研究活動の発展等に役立てるために社会に還元するとの原則に基づき、ある種当然のこととして公表されていると

ころであるが、その内容によっては、公にすることでかえって安全保障上の問題を招いたり、技術情報の流出によって国家の競争力の毀損に至る場合も想定され得るものである。

したがって、研究成果の取扱いについては、成果の公表という原則を遵守しつつも、安全保障や競争力の問題を生じさせないようなかたちでの管理や公表に配慮することが必要である。特に政府資金で行われる研究に関しては、研究中における情報管理の在り方、成果発表の在り方について、真に国益に適う対応をすべきである。

事例Ｃ５：研究成果の学会発表・講演等を通じた機微技術情報等の流出

→第４章第２節（１）研究情報の外部公表の可否判断：組織的管理の実践と支援

大学は研究成果を公表することが使命であるとの一般的な認識の下、研究成果の学会発表や講演において、重要な先端技術情報や機微技術情報等が公開されていることから、我が国の学会発表等は格好の技術情報等の収集の場となっているとの指摘がなされている。このような状況を看過することは、我が国の国際競争力及び安全保障の観点から大きな問題となりかねない。

したがって、大学においても、大学組織の特殊性を踏まえつつ、適切な情報管理が必要となる。具体的には、現在、各大学で行われている利益相反のマネジメントを参考にしつつ、研究情報の公表の是非、また公開する場合にはその望ましいあり方について、大学の執行機関が組織として判断を行うことにより対処するか、又は研究者に対して適切な助言を与えることとすべきである。その際には、例えば利益相反アドバイザーの機能を参考にしつつ、大学当局に研究情報の開示についてのアドバイザーを設け、教職員が行おうとする研究情報の公表に際しての指導・助言機能を持たせる等の対応が考えられる。また、こうしたマネジメントに違反するような行為に対する適切な処分の在り方も検討すべきである。

事例Ｃ６：特許公開情報への海外からのアクセスによって、我が国企業の有用な技術情報等が国外に流出

第３章１第２節（５）特許公開を通じた我が国の有用な技術情報の流出への対処

世界における特許制度の原則では、すべての特許出願は公開されることとなっており、日本の特許制度も同様の取扱いとなっている。この点について、我が国企業の有用な技術が海外において無許諾で使用されているのではないかとの指摘がある。この原因として、我が国の企業の中には開発した技術を漫然と日本で特許出願するだけで、海外での権利取得を行っていない企業が少なくなく、その結果、我が国企業の技術情報が流出しやすい環

境を自ら作り上げているともいえる。

したがって、特に特許の出願公開によってかえって特許取得の予定のない海外においてフリーライドを招くおそれのあるような技術情報については、特許出願をせずに営業秘密として管理することも重要な知財戦略の一つである。この観点から、各企業において戦略的に技術情報を管理し、特許を出願すべきか、営業秘密として秘匿化すべきかを判断すべきである。

なお、営業秘密として秘匿化した後に、仮に他者が同一技術について特許権を取得した場合であっても、一定の要件の下で先使用権が認められる。企業が先使用権を活用しようとする際の指針として、「先使用権制度ガイドライン」が発出されているところであり、このガイドラインにおいてまとめられている技術情報の管理手法を参照して、企業が戦略的な技術情報の管理を行うよう促していくべきである。

【公開情報の違法と考えられる流出】

事例Ｄ１：外為法上の許可を得ないまま、大量破壊兵器の開発等に転用可能な製品が不正輸出された結果、安全保障上の機微技術情報が流出

→第２章第２節（５）外為法の技術取引規制の強化

大量破壊兵器の開発等に転用可能な貨物の不正輸出等、日本及び世界の安全保障上ゆるがせにできない外為法違反事案が増加していることにかんがみ、貨物・技術双方の罰則強化について検討すべきである。

検討のアプローチ

上記の技術流出問題の類型整理によると、「情報」の帰属主体から、様々な「流出経路」を経由して、複数の「問題点」を生じることとなる。例えば、企業の保有する情報が、従業員の手を経た流出の結果として、競争力の低下という問題を引き起こすこと、大学の保有する情報が、不正アクセスによって流出した結果、安全保障上の問題を惹起する等、様々なケースが想定される。このように、技術情報等の流出は「情報」の帰属、「流出経路」、「問題点」の組合せによって様々であることから、包括的な検討が必要となるものである。

包括的な検討を行うアプローチは以下のようなものとなる。

まずは、流出の結果どのような問題が発生するかという観点から、「競争力」及び「安全保

障」の横断的な課題について議論する。
次いで、「情報」の帰属主体ごとに、どのような技術流出の問題が発生するかについて、「企業」「大学」「政府」の情報帰属主体において、それぞれの主体に固有の問題について議論する。

各章の構成は、以下のとおりである。

第１章においては、イノベーションを生み出す仕組み、国富増大のための環境整備の在り方について議論する。
企業価値の源泉が無形の知的資産へと大きくシフトする中で、イノベーションを最大化するための技術情報等の保護の在り方はどのようなものか、また、グローバル競争が激化する中で、海外から受け入れる資本や人材を我が国の産業競争力に変えていくための仕組みはどのようなものか、について議論する。

第２章においては、安全保障上の機微技術の管理の在り方について議論する。
科学技術の発展の結果として、民生用途に開発された技術情報が安全保障上の機微技術となるデュアル・ユースの問題が指摘されており、情報化の進展とともに、こうした技術情報が国内外に容易に流出することによる安全保障上の問題が懸念されている。このような観点から、安全保障上の機微技術の管理の在り方について議論する。

第３章においては、企業における情報管理の在り方について議論する。
企業の保有する技術情報等が相応の価値を生み出すためには、そうした情報が適切に管理されていることが必要である。しかしながら、技術情報等はその価値を容易に把握することができないという性質（不可視性）を有するが上に、その価値判断が難しく、情報管理には大きな困難が伴う。また、グローバル化によって企業の国際展開が拡大する中で、技術情報等が流出するリスクが高まっている。さらに、中小企業においては、固有の問題として、不十分な管理や取引先等を通じて意図しないかたちで技術情報等が流出している。こうした視点から、企業における情報管理の在り方について議論する。

第４章においては、大学における情報管理の在り方について議論する。
大学が保有する先端技術情報は、その重要度や広範な活用可能性に比して、必ずしも十分な管理がなされていないという実態がある。これは、組織を超えたアカデミアのつながりや学問の自由といった、企業とは異なる大学の特殊性に起因するものと考えられる。こうした大学の組織体制を十分に踏まえつつ、大学における情報管理の在り方について議論する。

第５章においては、政府における情報管理の在り方について議論する。

政府が保有する情報については原則公開されるべきであるとしつつも、公表によってかえって我が国においての国益を損なうようなものについては厳格な管理がなされるべきであり、どのような政府情報を公表し、何を非公開とするかの哲学が求められている。そうした観点から、政府における情報管理の在り方について議論する。

委員のコメント（概要）：総論

○ 制度設計に当たっては、まずはマーケットメカニズムや技術で解決することを優先し、最後の手段として権力による強制によって解決するというのが、社会的にはコストの一番少ない方法ではないか。

○ 重要情報が漏れるという状況は、我が国の国益上ダメージが非常に大きい。例えば、米国の最先端の戦闘機を導入しようとしたときに、日本の情報管理の杜撰さについて指摘され、情報提供を拒まれたことがある。

○ 機微情報の範囲、人に付く情報、会社に帰属する情報等に関して、非常に曖昧な部分が多いと感じている。また、情報の価値や情報が流出した際のインパクトに関して理解していない人が多いと感じている。

○ 不正競争防止法が営業秘密侵害罪に対して適用可能であっても、現実問題として告訴や捜査が行い難い状況がある。法制度を整備して、民事・刑事において適切に対応できるようにしなければいけない。

○ オープンなかたちでインターフェースやインテグレーションの方法をサーチしていくところでは、国民性あるいは産業構造上の特性として、我が国に比較優位があると考えられる。そうしたオープンなサーチプロセスの機能を壊さないような、トレードシークレットに関する保護を考えていかなければいけない。

○ 特許制度や菌株寄託制度等の公開を前提とした制度において、制度を利用するとかえって関係者にとって損害をもたらすようなことがあるのであれば、早急に対応を検討する必要があるだろう。

○ 漏れないようにするためには、一切出さないというのが一番良い。見せない、しゃべらない、触らせないという原則を重視し、製品でいえば生産や加工といった途中段階も含めて必要な人以外を近づけさせないということが重要である。

○ 営業秘密は知的財産の一種という理解になっているが、一般的な知的財産のように権利の範囲を明確にして公開するということは馴染まず、そのような保護とは違ったかたちで営業秘密を守る体系を構築していかないといけないのではないか。

○ 危険な病原菌の再現が技術的に可能になっていることや、デュアル・ユース技術が増加している中で、科学者にとってどのような倫理規範又は行動規範をとっていくべきなのか、あるいはセンシティブな情報の公開方法といったような、研究開発に関するガバナンスにまで踏込んで議論していく必要があるのではないか。

○ 内部統制の問題と同様に、情報について、企業の管理力、あるいは国家の管理力が備わっているのかどうかというところを問題にし、それは自己宣言を基本として、重要度のラベリング、コントロール等をしていくことが必要ではないか。

○ 今後の我が国の競争力強化のために、ハイテク移民と言われる外国人頭脳労働者をいかに引き込んでいくかということと、技術流出の問題を同時に考えていかなければいけない。

○ 検討に当たって、アカデミアにおける学問の自由、ベンチャーにおける人材の流動性の重要性、将来重要な課題となると考えられる優秀な外国人受入れ等を考慮することが非常に重要である。

○ バイドールが適用されて技術を得た企業が外国企業に買収される場合にどうなるかということ等に関して十分に確認できていない状況がある。

Ⅱ．各論

第１章　競争力の視点

１　イノベーションを生み出す制度整備について

（ポイント）

【現状と問題点】

（１）無形の知的資産の重要性と情報保護の必要性

- 知識社会の進展に伴い、企業価値の源泉が、企業の保有する技術情報等のような無形の知的資産へ大きくシフトしている。
- 我が国企業において、こうした無形資産を国内外から取り込み、これを有効に保護・活用することのできる環境を整備しなければ、今後の発展はあり得ない。
- しかしながら、実務の現場からは、侵害を救済するための刑事手続きにおいて技術情報等が漏洩するおそれがある等、営業秘密侵害行為に対する法的救済が機能していないと指摘されている。

（２）オープン・イノベーションの促進のための環境整備

- いわゆるオープン・イノベーション（外部の知識・技術を活用しつつ研究開発や事業化を行うモデル）の実現のためには、事業者間で技術情報等を共有する体制を構築することが前提。
- 情報の開示を受けた主体が、その情報を適切に保護し利用することが担保されなければ、事業者間で技術情報等を共有する体制は構築されない。
- すなわち、技術情報等を保護する制度整備がなされなければ、国内における事業提携はもとより、国際的な事業提携にも、大きな滞りが出ることとなり、企業のグローバル展開にも大きな支障が生じるおそれがある。

【具体的検討事項】

- **技術情報等の適切な法的保護の在り方に関する検討**
- **営業秘密保護のためのガイドラインの見直し**
- **企業における技術情報等の権利帰属問題に関する検討**
- **技術情報等の開示・共有インセンティブを創出するための仕組み**

第１節　現状と問題点

（１）無形の知的資産の重要性と情報保護の必要性

知識社会の進展に伴い、企業価値の源泉が、企業の保有する技術情報等のような無形の知的資産へと大きくシフトしつつある。IT 化、知識経済化の中で、我が国企業がグローバル競争を勝ち抜いていくためには、自らそうした有用な技術情報等を生み出すのみならず、国内外を問わず社外から有用な技術情報等を取り込み、これを有効に活用することのできる環境整備を図ることが必要である。

この場合において、各企業が有用な技術情報等を有効に活用することができる環境とは、

- 各企業が自社固有の強みや特徴について的確な把握・管理（知的資産経営[2]）をしていれば、それらが有効に保護されること
- 各企業が他者との取引を通じて、他者の技術情報等との組み合わせが有効になされること（自らが信頼できる相手に自らの技術情報等を開示した場合には、そこから漏れることがないという保障があること）

をいうものと考えられる。

以下では、各企業が有する技術情報等を保護・活用し、先行技術開発と後続技術開発の双方に最適な誘因を与える技術情報等の適切な法的保護の範囲について問題提起を行う。

技術情報等の保護について：特許化と秘匿化の選択

自社にとって重要な技術情報等を保護する手法としては、特許等の取得による排他的実施権としての保護を図る方法と、営業秘密として自社で秘密管理を行うことにより法的保護を図る方法があり、両者のメリット・デメリットを考慮した戦略的な判断が求められる。

特許権等の産業財産権による保護は、排他的独占権の取得が認められるというメリットがある反面、例えば特許については出願後１年６ヶ月で発明内容が公開されるため、模倣や周辺特許を押さえられてしまう可能性があるといったデメリットがある。

これに対して、営業秘密として秘密管理する場合は、他社に秘密の内容を知られることがないため、競合他社との関係で差別化が容易になること（特許はその内容が公開されるため、企業の事業戦略ベクトルが競合他社に明らかになる可能性がある）、特許になじまないノウハウのような概念も保護対象となりうること、リバースエンジニアリング[3]ができな

---

[2] 「知的資産経営」とは、企業の競争力の源泉となる各社固有の知的資産（人材、技術、組織力、顧客とのネットワーク、ブランド等の目に見えない資産）を認識し、これを有効に組み合わせて活用していくことを通じて収益につなげる経営のことをいう。

[3] 「リバースエンジニアリング」とは、機械、製品等を分解・解析すること等により、機械、製品等の構造を分析し、そこから製造方法、動作原理、設計図等を調査することをいう。

い限り事実上保護される期間に制限がなく、非公開情報として永続的な利用が可能となること、といったメリットがある[4]。また、技術開発の迅速化、製品サイクルの短期化等により、市場競争においては革新的な技術をもっていかに早期に市場を席巻するかが重要な要素となっていることから、登録・審査手続において一定の時間を必要とする特許権の取得は必ずしも有効でなく、この点においても営業秘密として秘密管理することに優位性が認められる。

他方、営業秘密として管理することのデメリットとしては、営業秘密の譲渡やライセンスに際して登録制度等を通じた法的効力がないために、資産としての客観性が特許等に比べて低いという点があろう[5]。また、営業秘密侵害罪の構成要件が厳格に過ぎるため、その犯罪行為の立証が困難であり、十分な救済が受けられないという現行法上の問題が指摘されている。さらに、後述するように、営業秘密保護の法的要件である秘密管理性の考え方について、必ずしも企業実務の実態にそぐわない司法の判断（「適切な秘密管理レベルの考え方について」で後述）によって秘密管理性が否定されているとの指摘があり、法的救済が受けられないケースがあり、イノベーションの在り方との関係で問題視されている。

秘密管理による技術情報等の法的救済の問題点

企業等の保有する技術情報等の不正取得に対する罰則としては、不正競争防止法における営業秘密侵害罪が挙げられる。

不正競争防止法の営業秘密侵害罪の保護法益としては、公正な競争秩序（社会的法益）及び企業が保有する営業秘密として秘密管理された技術情報等の財産的価値が挙げられるところ、同法では、基本的に、詐欺等行為又は管理侵害行為により不正に取得した後の「使用」又は「開示」といった実行行為が処罰対象となっており、「取得」はそれらの準備的行為として例外的にのみ処罰されている。

経済産業省のアンケート調査[6]によれば、35%以上の製造関係企業が技術流出を経験したと回答しているにもかかわらず、これまでに営業秘密侵害罪で起訴された事例はない。この理由として、営業秘密侵害罪の構成要件が、「営業秘密」の「使用」又は「開示」をもってこれを実行行為としているが、処罰範囲が相当に限定的であること、その結果として、捜査当局にとっても超えるべきハードルが必ずしも少なくないことが挙げられる。すなわち、実際の営業秘密として秘密管理された技術情報等の使用・開示行為は、その取得行為のように保有者たる企業の内部で行われるものではなく、相手企業や行為者の自宅等といった被害者たる企業の支配の及ばない領域で行われることが多く、その立証が極めて困難

[4] Levin [1987] によれば、特にプロセスイノベーションを強調する化学産業等では、イノベーション保護のために営業秘密に大きく依存する傾向にある。

[5] ノウハウ等のように特許権取得が適切でないものの、他者が同内容の権利を取得しても引き続き事業が継続できるよう、「先使用権」の活用を検討することも有効な手段である（Levin [1987] "Appropriating the Returns from Industrial R&D"）。

[6] 経済産業省『我が国製造業における技術流出問題に関する実態調査』（2006 年 12 月）

を来たすことは夙に指摘されており[7]、結果として、営業秘密侵害罪が必ずしも十分な抑止機能を果たしていないことが指摘されている[8]。

加えて、仮に起訴に至ったとしても、刑事手続を通じて技術情報等が公開されてしまうおそれがあるために、秘密管理されているからこそ意味がある技術情報等の保護の観点からは元も子もなくなってしまうため、営業秘密として秘密管理されていた重要な技術情報等を窃取された場合ほど被害者が告訴に踏み切らないという矛盾についても指摘されている。

上記の点を改善するためには、技術情報等の保護法益に関する考え方を再構成した上で、企業が秘密管理する技術情報等を不正に領得した行為そのものを捕捉する必要があるものと考えられる。

他方で、法的救済の前提として、格付けされた技術情報等の管理を行うに際して、そもそも技術情報等の価値は相対的なものであり、また、時間の経過とともに変化するものであることからすると、全ての企業に対して画一的な技術情報等の管理レベルを要求することは、必ずしも現場感覚にそぐわない。

実際、企業が技術情報等の流出というリスクに対処するための予防的な取組を行う上で、リスクの発見、分析・評価、対応策の決定という、一連のリスク管理の視点が欠かせない。なぜなら、技術情報等の管理体制に完璧を期し、無限のコストをかけることは現実的には不可能であるとともに、行き過ぎた管理はかえって企業内の技術情報等の共有を阻害しかねない。したがって、業務の効率性と受容可能なリスクをバランスすることが必要である。このような実態にかんがみ、技術情報等の管理の在り方の検討に際しては、これまでの画一的な対応よりも、むしろ、技術情報等の重要度や自社のリソースに応じた技術情報等の管理を行うことを許容するフレキシブルな仕組みづくりが求められているのではないか。具体的には、経営実態に即して事案ごとに費用対便益が考慮されるような秘密管理レベルの判断がなされることが必要である。このような企業のレベルに応じた柔軟な仕組みは、完璧主義に陥らず、まずは核となる部分を押さえつつ、全体として秘密管理レベルの底上げにつながるものである。

---

[7] 被害企業を担当する弁護士の意見として、「被害者の立場になると、営業秘密が使用・開示されたことに関して十分な説明をする告訴状を作成することは困難であり、結果的に警察に動いてもらうことができない」、「警察においても多分起こったということは感じているが立証できない」といった立証の困難性を述べている。

[8] 営業秘密侵害罪の構成要件が、慎重に対処しすぎて構築されたきらいがあるという点について一例を挙げれば、例えば、従業者等が在職中に、持ち出しやコピーが禁じられていない営業秘密について、不正の競争の目的で、自己の USB メモリを会社へ持って行き、その USB メモリに会社の PC の営業秘密情報をコピー・ダウンロードした上で、退職後に、不正の競争の目的でそれらを領得・使用したような場合にも処罰されない。

適切な法的保護の範囲について

特許権、著作権等のいわゆる知的財産権制度には、知的財産権の保護範囲についてのジレンマ（スコープのジレンマ）が存在するものと論じられてきた。

スコープのジレンマとは、知的財産権によって保護される範囲が広くなれば発明者の権利が広く保護されるため、新しい市場を開拓するような先発的な発明（イノベーション）が促進される一方で、保護される範囲が狭くなれば、後に続く発明者が既存の技術を改良・発展させることができ、累積的なイノベーションが促進されるという考え[9]であり、これは営業秘密として管理された技術情報等の法的保護の範囲の議論について論じる際にも妥当するものと考えられる。

このジレンマについては、産業ごとの特殊性を考慮した上で、先発的発明を重視するか、累積的な後続発明を重視するかについて検討する必要があろう[10]。すなわち、イノベーションのかたちは産業ごとに様々であり、それぞれの技術は、製品ライフサイクルや開発コスト、開発期間、市場特性等に依存していると考えられる。

このような考え方を前提としたイノベーションの創造に知財が果たす役割に関する理論的分析においては、パイオニア・イノベーションを促進すべきと考えられる産業（バイオ（遺伝子）、化学（農薬、製薬））では、特許の保護の範囲を広く認めることが重要であり、累積的イノベーションを促進すべきと考えられる半導体、電子機器、ソフトウェア等は保護の範囲を狭くすることが望ましいとされている。

図表２．イノベーションの創造に知財が果たす役割に関する理論における産業の特性

	バイオ	ビジネスモデル	化学・医薬	ソフトウェア	電子機器・半導体
特徴	・長期にわたる開発と試験のための準備期間が必要 ・ジェネリックな生産者の費用及び不確実性は発明者に比べて相当低い ・単純な設計上の迂回を排除する必要あり ・権利が狭いと製品の生産時に複数の特許保有者と交渉が必要になる	・巨額かつ継続的な研究開発を必要としない ・比較的単純なアイデアであるか発見であることが多い ・競争的な市場であれば、より効率的なビジネスモデルが差別的であるから、保護がなくとも開発インセンティブがある	・研究開発、医薬品設計、臨床試験に長期間（９～17年）かかり、開発コストも他産業に比べ研究開発費の占める割合が大きい ・化合物であるため不確実性が高い ・一製品一特許 ・模倣者の費用に対する発明者の費用比率は効果的な保護がなければ極めて大きい	・既存の製品に対する多数の反復的な改善 ・既存のアイデアはプログラムコードの上に構築される ・開発コストは比較的低く、出荷までのリードタイムも短い ・ライフサイクルが短い ・素早く、漸増的なイノベーションが必要	・長期間にわたる開発と巨額な投資が必要であるが、製品ライフサイクルは短い ・複数の特許が同一のものを対象としている場合が多い ・一製品複数特許 ・製品の一部品の特許であることが多いため、排他的効果よりもライセンスを許諾する道具として有益であることが多い

[9] Boldrin and Levine [2002] によると、強力な知的財産の保護はイノベーションを促進するというよりも弊害となる（Boldrin and Levine [2002] 'The Case Against Intellectual Property'）。

[10] Merges and Nelson [1990] 'On the Complex Economics of Patent Scope' Columbia Law Review 839 vol. 90

					・業界内で互いに訴えるリスクを排除するためにクロス・ライセンス契約を行っている
望ましい保護の範囲	広	狭	広	狭	狭
イノベーション理論	アンチコモンズ理論	競争的イノベーション理論	プロスペクト理論	累積的イノベーション理論	特許の藪理論
考慮すべき重要評価指標	開発期間、投資額、市場環境（模倣リスク）	開発期間、投資額、市場環境	開発期間、投資額、市場環境（模倣リスク）	開発期間、投資額、製品ライフサイクル	開発期間、投資額、市場環境（訴訟リスク）

出所：Burk and Lemley [2003] 'Policy Levers in Patent Law'、山崎昇（訳）[2007]『知的財産法政策学研究』Vol.14, 15、総務省統計局『平成17年科学技術研究調査報告』（2005年12月）を基に経済産業省知的財産政策室において作成

イノベーションを促進するための技術情報等の法的保護の範囲に関する議論においては、イノベーションを取り巻く様々な環境要素についても考慮する必要があろう。環境要素がイノベーションに影響した典型例として、IT 産業の特性を踏まえた技術情報等の流通を重視した（保護範囲を狭くした）結果成功した「シリコンバレー」と、厳格な技術情報等の管理を行った結果として衰退した「ルート 128」がある。

下記参考の整理で見るように、シリコンバレーの半導体産業も、ルート 128 のコンピュータ産業も、保護の範囲を狭めることでイノベーションを促進する産業であるが、ルート 128 では広範な技術情報等を厳格に秘密管理する体制や企業への忠誠と長期雇用の促進等といった自己完結型の企業形態（従業員の転職という人を介しての情報流通にも抑制的）を選択したために衰退したものと考えられている[11]。

（参考）シリコンバレーとルート 128 の比較

シリコンバレー（Intel、Apple、Oracle、Google、yahoo、HP 等）

半導体の製造で 1970 年代から成長を続ける産業集積地。シリコンバレーにおいては、細かく張り巡らされた社会のヨコのネットワークとオープンな労働市場の存在が、現在までの発展の成功を可能にした。ここでは企業は互いに競争しながらも、同時に、社外の供給会社や取引先等との非公式なコミュニケーションを通じて、市場や技術の変化について情報交換することにより、相乗的な成長を実現している。

ルート 128（DEC、Prime、Wang、Status、Lotus 等）

ミニコンピューター市場の隆盛により経済成長を成し遂げた実績がある。ルート 128 の企業の多くでは従業員の会社への忠誠が重んじられ、転職は感心できない行為と考えられ、「長年勤続している」プロフェッショナルを好む傾向が強い。分別・高潔を重んじる企業文化等、日本と類似している点が多い。

機密保持と企業への忠誠を重んじる自己完結型企業が集合しており、80 年代以降下降線を辿っ

[11] Saxenian [1994] 'Culture and Competition in Silicon Valley and Route128'

ている。衰退した原因には、当該企業では満足に力を発揮できなくとも転退職できない従業員の滞留（労働インセンティブの低下）、秘密主義等が挙げられている。

シリコンバレーとルート 128 の比較整理図

	シリコンバレー	ルート 128
起源	スタンフォード大学を中心に、知識拡散（Knowledge Spillover）により発展（特にエレクトロニクス産業）	ハーバード、MIT を中心に、Federal research fund 等が原資となり発展（特に軍事産業）
雇用体系	流動性の高い雇用	長期雇用
知識拡散	会社間	会社内
競業避止	弱い※1	強い
文化	オープン	保守的
結果	新しい価値を持った製品の創出	硬直的価値観による製品の創出

※1 California business and Professions Code section 16600（職業選択の自由を保障）が有効であるため、シリコンバレーでは暗黙知（Tacit Knowledge）がイノベーションを商業ベースに転換し、人の往来により暗黙知が企業間で拡散することで、産業が発展した。

出所：Gilson [1999] 'The legal infrastructure of high technology industrial districts: Silicon Valley, Route 128, and covenants not to compete' を基に経済産業省知的財産政策室において作成

適切な秘密管理レベルの考え方について

技術情報等の法的保護の在り方を検討するにあたり、もう一つ問題となるのが、法律が要求する技術情報等の秘密管理の水準である。

不正競争防止法の営業秘密として保護されることを期待して秘密管理された技術情報等が、営業秘密として認められるためには、①有用な情報であること（有用性）、②公然と知られていないこと（非公知性）、③秘密として管理されていること（秘密管理性）、が求められている[12]。そして、このうち、企業側に求められる秘密管理とは、具体的には、(i) アクセス制限と (ii) 客観的認識可能性が備わっていることを意味するものとされるのが一般であり、判例上も施錠管理や持出・入退室の制限、秘密情報の表示等の具体的な管理方法が問われることとなる。ところで、こうした秘密管理性の判断においては、その基本的な発想として、画一的な秘密管理体制をすべての企業に求めるのではなく、個々の産業の特性や情報の性質の違いを前提として、経済的に合理性のある判断が必要であると考えられる。

例えば、米国におけるトレードシークレットに関する秘密管理性の判定に関しては、事案ごとの費用と便益を比較考量する必要性が述べられ、保護に要する費用、そしてより高

[12] 不正競争防止法第２条第６項

い保護を行ったことによって生じる追加的な便益（保護レベルの向上）が費用を超えるかどうかという点を判断基準として考える裁判例[13]がある。その他の裁判例においても、あまりにも厳格な秘密管理を行わせることは、「巨額の費用を投下させて子供のいたずらを防がせるようなものであり、過分の義務を負わせるのは相当ではない」旨の説示を述べている[14]。

一方で、近年の日本の判例[15]を分析すると、例えば、小規模の企業において業務上頻繁な利用を要する情報に対して、施錠管理やパソコンのパスワード管理を求める等、当該企業の業務実態に照らせば、過剰ともいいうるような秘密管理を求める裁判例等、事案ごとの費用対効果を比較考量するというよりも、一般的な基準に基づく秘密管理体制に重点をおいているように見受けられる[16]。つまり、企業において事業上重要な情報であり、営業秘密として法的保護を受けたいと考えたとしても、そのビジネスモデルや情報の性質上、法で求められるレベルの秘密管理を行うことが困難な場合が生じかねない。

このような秘密管理性を厳格に解する判例の傾向については、結果として紛争予防的機能が認められると考えられるとしても、イノベーションの観点からは効率性を著しく阻害するものと考えられる。したがって、我が国企業のイノベーションを促進するための秘密管理性の基本的な考え方を検討する必要がある。

（参考）日本と米国における秘密管理に係る裁判例への指摘

日本

◆人工歯事件（京都地判平 13.11.1）

医療用具・医薬品の製造等をしている会社である原告が、元従業員である被告 A が原告の営業秘密である人工歯原型を持ち出し、被告会社（被告Aの転職先）に対し開示し、被告会社が故意又は過失によって同営業秘密を使用して商品を製造、販売しているとして提訴。

秘密管理性については、被告は原告の企業秘密において、就業規則にて守秘義務が課されており、さらに社内の者であっても、担当のグループの承諾なくして、自由に搬出することができない等の管理体制が敷かれていたにもかかわらず、原告会社において人工歯原型について保管場所が特定されておらず、外部の専門家に評価をしてもらう際に秘密保持契約は締結されていなかったこと等を理由に、原告とその内部の従業員に対する関係では秘密管理はされていなかった旨を判示している。

---

13 小島立 [2007]「アメリカにおける営業秘密保護について」『不正競争防止法研究「権利侵害警告」と「営業秘密の保護」について』レクシスネクシス・ジャパンによる（Rockwell Graphic Systems,Inc.v.DEV Industries.Inc., 925 F.2d 174 (7th Cir.1991)）

14 同上（E.I.duPont deNumours & Co. v. Rolfe Christopher et al.,431 F.2d 1012(5th Cir.1970)）

15 京都地判平 13.11.1（人工歯事件）、名古屋地判平 11.11.17（コンベヤーライン）、大阪地判平 12.7.25（人材派遣業社員名簿事件）、大阪高判平 17.6.21（高周波電源装置事件）、東京地判平 16.4.13（ノックスエンタテイメント事件）等。

16 日本における秘密管理に係る判例の流れは大きく分けて２つあり、一方は、情報にアクセスする者に対して秘密として管理されていることが認識可能であったかという観点から判断する裁判例（大阪地判平 8.4.16（男性用かつら事件））等であり、他方は、そのような認識可能性とは別個に、一定のレベルの管理体制を画一的に要求する裁判例（京都地判平 13.11.1（人工歯事件））等であるが、近年は後者の秘密管理性を厳格に捉える傾向が強くなっている。

◆ノックスエンタテイメント事件（東京地判平 16.4.13）

原告は被告（原告の元従業員）が設立した競合会社において、被告が原告に在職中に得た登録アルバイト員の住所及び経歴に関する情報を使用したとして提訴。

秘密管理性については、従業員が数人という小規模企業においては、パスワード等でアクセス制限を行わなくとも、履歴書等の綴られたファイルの背表紙には「社外秘」と記載されており、口頭でその確認を行うこと等によって、従業員間で営業秘密に関する認識を共有することは可能であり、むしろそれが小規模企業の利点であるにもかかわらず、保管されている書棚に扉がなく、アクセスする者を一定の者に制限するといった措置を執らなかったこと、原告と従業員との間で厳格な秘密保持契約を定める等の措置や、コピー時に、その配布枚数の確認と使用後に回収する等の厳格な措置を執らなかったことから、原告は上記履歴書等の記載された本件情報を客観的に秘密として管理していたということはできない旨を判示している。

米国

◆Rockwell 事件（925 F.2d 174 (7th Cir.1991)）

原告 Rockwell 社は新聞印刷機等の部品製造会社であり、原告の元社員である被告（原告を退職後、競合会社を設立）が原告の所有する部品図面を保有していることに対し、営業秘密の窃取であるとし提訴。

原告における秘密管理体制は、当該部品図面を貴重品保管室で保管し、身分証明書を有した従業員しか入れないような秘密管理を行っており、下請企業に製造を依頼する場合においても、用務終了後には図面を返却させるべく契約書を取り交わしていた。しかしながら、部品の再注文時には、再度図面が必要になることを理由に、原告はこの契約を強制することはなく、結果的に下請先等も含めた原告を取り巻く環境に当該図面が流出している状況であった。

上訴審において Posner 判事は、秘密管理性の判断基準については、事案ごとに費用と便益を比較考慮する必要があるとし、本件では、原告は確かにより高いレベルの予防策を講じることが可能であったが、原告が図面へのアクセスをより制限したとすると下請け業者の作業がより困難になったであろう可能性を考慮し、より高い保護を行ったことによって生じる追加的な便益が費用を超えるかどうかが問題になる旨を判示した（事案を事実審に差し戻した）。

（2）オープン・イノベーションの促進のための環境整備

オープン・イノベーションの重要性

グローバル化や情報化の進展は、社会の在り方を大きく変えつつある。労働力の流動性が高まったことにより、長年企業の中で蓄積された知識が社会に分散し、大企業・中小企業を問わず、全体の知識レベルが向上した。さらに技術革新によって、製品サイクルや研究開発プロセスが短期化しつつある。その結果として、旧来の我が国製造業が得意としてきたクローズド・イノベーションは必ずしも全ての場合において効率的なプロセスとはいえなくなってきた。代わって、社会環境の変化を踏まえると、必要となる知識は必ずしも組織内にある訳ではなく、組織の外部と内部の知識を有機的に結合させるプロセス、すなわちオープン・イノベーションが効率的な価値創造のかたちとして位置づけられ始めている。

以下では、オープン・イノベーションを進める際の技術情報等の開示及び共有の重要性について問題提起する。

オープン・イノベーションにおける技術情報等の開示・共有の重要性

オープン・イノベーションを活用する際、相手にアイデアが取られてしまう、又は、複数の者から預かった技術情報等を混在させてしまうことによって意図しない権利侵害の危険性が発生するといったリスクを回避することで、結果的に技術情報等の共有の機会を減少していることがある。

また、購買前に相手方の技術情報等の詳細が知りたいが、購買の決定をしないと十分な技術情報等を提供してくれない（特にそれが企業の根幹をなす重要な技術情報等であればあるほど)、したがって、購買前の不完全な技術情報等に基づいて意志決定をしなくてはいけないというジレンマ（＝情報のパラドックス）に陥っている状態においては、オープン・イノベーションは進展しない[17]。

したがって、技術情報等の共有と開示を促進することが、オープン・イノベーションにとって不可欠な要素となる。

技術情報等の開示を促す機能として、お互いの技術情報等が歪められることなく、相手に伝達されることが保障される必要があり、この技術情報等の伝達の役割を担うものとして、中立的第三者の必要性が指摘されている[18]。

また、開示された技術情報等を共有する際に、当該共有技術情報等が適切に相手方で保護されないと、技術情報等の提供者は提供インセンティブが減少することになる。したがって、共有技術情報等の受入者が当該技術情報等を契約等に違反して不正に使用したり、開示したりしないよう、適切な措置が機能することが不可欠である。

（参考）オープン・イノベーションの促進の障害となる不安定な情報共有の基盤

（事例１）
研究開発プロジェクトの参加企業は、共同研究契約に定められた手続に従い了解を得ることで、共同研究の一環として、厳重に秘密管理されている企業 A の営業秘密を閲覧することができた。しかしながら、企業 B は契約に定められた手続に反して必要な了解を得ることなく営業秘密の複製を作成した。企業 B の悪質な契約違反行為に、企業 A は刑事告訴を検討したが、不正な競争目的での使用･開示についての立証が困難であったことから､最終的に告訴を断念することとなった。

（事例２）
取引の相手方メーカーと秘密保持契約を結び、図面・ノウハウを開示したところ、なぜか当該図面を別のメーカーが保有していることが判明した｡取引の相手方が明らかに秘密保持契約に違反していると認められたので、訴訟提起も検討したが、損害の立証が十分にできず、結果的に泣き寝入りすることとなった。

出所：経済産業省知的財産政策室による企業ヒアリング

[17] チェスブロウ [2007]『オープンビジネスモデル』翔泳社
[18] 中馬宏之ほか [2007]「共同研究開発における情報共有」RIETI Discussion Paper 2007 年 3 月

第２節　具体的対応

（１）技術情報等の適切な法的保護の在り方に関する検討

企業の従業員等の信頼に基づいて正当に営業秘密として管理された技術情報等へのアクセスを認められた者が、図利加害目的等の不正な目的をもって、複製が禁じられたそれらの複製を行う場合、又は、アクセス権があっても、不正な目的をもって行われる、大量データのダウンロード等の正当な理由のないアクセス行為等については、そのような行為それ自体を刑事罰の対象とすることについて検討すべきである。

そもそも、刑法上の財産犯は、基本的に「財物」を保護客体としており、財物の移転を伴わない「情報」の窃取・盗用等を捉えて処罰することはできなかった。このように措置されてきたのは、「財物」が窃取された場合にあっては、行為者の占有取得に対応して被害者に直ちに法益侵害が生じるのに対し、「情報」が不正に取得された場合にあっては、情報それ自体は被害者の手元にあり、被害者に直ちに法益侵害が生じるとは言えないという情報の「非移転性」を主たる根拠とするとの指摘がされてきた。

そもそも技術情報等を保護しなければならないのは、これが非公知であり、その処分・利用可能性が特定の者のコントロール下におかれていることによって、ポテンシャルとしての財産的な価値が認められるからであると考えられる。そして、「情報」には、「非移転性」のほかにも、「財物」とは異なる以下の性質を有することを指摘することができる。

第１に、先述したとおり、技術情報等は、個別財産的に捉えることができる一方で、様々な個々の財産を生み出す源としての性質（根源性）を有していることである。すなわち、「財物」であれば１度しか消費できないが、「情報」は何度でも消費することができ、何度でも売れる商品・サービスを生み出す力がある。この点は、いわゆる「財物」を盗られた時よりは、企業秘密を盗られた時の方が、「ヒヤリとする」との企業家の実務感覚に合致するものである。

第２に、技術情報等は、いったん侵害されてしまうと、侵害者のもとに留まり、また、侵害者のもとに留まった状態において、さらに瞬時に拡散されてしまうことが考えられ、秘密状態の回復が困難又は不可能であるという性質（回復困難性・不可逆性）を有する。すなわち、「財物」であれば、返還すれば損害の回復は一応可能であるが、「情報」は損害の回復がほぼ不可能である。

第３に、技術情報等は、その性格からある種当然であるが、その管理・予防は物的・人的・組織的に十全の努力を尽くしてもなお管理・予防しえない性質（予防困難性）を有している。

秘密管理された技術情報等における「ポテンシャルとしての財産性」が、このような性格を有していることを踏まえれば、当該法益が侵害された場合における違法性は、当該情

報の生み出しうる個々の個別財産の累積ないしそれ以上と評価することが可能であり、法益侵害が現実に発生する以前の準備的行為に既に法益侵害性を肯定することができるものと考えられる。すなわち、当該準備行為自体に十分な違法性（発生する法益侵害×当該結果が発生する危険性）を認めることができ、その違法性は、例えば通常の個別財物に対する罪の既遂時点のそれと比較しても見劣りするものではないと考えられる。

上記の営業秘密のポテンシャルの理解を踏まえれば、「使用」・「開示」のみならず、「取得」行為についても法益侵害性を認めることができるものと考えられる。

また、現行の法体系では、外国政府を利する目的で行われる技術情報等の窃盗・領得・複製の作製等が、必ずしも処罰されないが、これは我が国の産業競争力のみならず、安全保障の観点からも重大な問題を提起することから、こうした行為を規制の対象とするための法的枠組みの創設についても検討すべきである。

なお、米国においては、経済スパイ法により、トレードシークレットを海外で使用する目的で、又は、図利・加害目的で窃盗、無許可複写、不正に取得した場合には、最高 15 年以下の懲役又は 50 万ドル以下の罰金又はその両方が科されることとなっているほか、秘密情報の不正取得行為それ自体に対して刑事罰則を科そうとするのが主要国における一般的な傾向である。

加えて、企業秘密の侵害行為の救済を求める刑事裁判では、技術情報等の内容がその手続を通じて公開されることとなり、違法行為を抑止すべき公的手続自体が第２の法益侵害を招来するため、その結果として、違法性・有責性の高い者ほど、刑事手続で処理されないという矛盾を抱えている。技術情報等の実効的な救済がなされるよう、こうした矛盾を改善すべきである。

（参考）米国経済スパイ法の概要（18 U.S.C.§1831-1839）

デジタル化の進展とともに物理的な侵害行為を伴わないかたちでの営業秘密（トレードシークレット）の窃取が容易になったことを背景に、1996 年に発効した連邦レベルの刑事法規。

基本的な禁止行為

① トレードシークレットを窃盗、無許可占有、取得、持ち出し、隠匿、あるいは欺罔、偽計、又は詐術によって入手すること
② 許可なく複写、複製、写生、作図、撮影、ダウンロード、アップロード、変更、破壊、写真複写、模写、送信、引き渡し、送達、郵送、通信、又は運搬すること
③ 盗まれたこと、あるいは許可なく占有、入手、又は横領されたことを知りつつトレードシークレットを受領、購入、もしくは所持すること
④ その他、これらの未遂・共謀等も処罰対象とされている

犯罪類型

①経済スパイ（§1831）

外国政府、外国の関連団体、あるいは外国の代理人を利することを目的としつつ又はこれを知りつつ、一定の禁止行為によってトレードシークレットを窃取等すること（法定刑は、50 万ドル以下の罰金若しくは 15 年以下の懲役又はその併科。両罰規定として、団体に 1,000 万ドル以下の罰金）

②トレードシークレットの窃取（§1832）

所有者以外の何者かの経済的利益のために横領する目的で、当該トレードシークレットの所有者に損害を与えることを目的としつつ又はこれを知りつつ、一定の禁止行為によってトレードシークレットを窃取等すること（法定刑は、25 万ドル以下の罰金若しくは 10 年以下の懲役又はその併科。両罰規定として、団体に 500 万ドル以下の罰金）

（2）営業秘密保護のためのガイドラインの見直し

技術情報等が営業秘密として保護されるためには、❶有用性、❷非公知性、❸秘密管理性の３要件を満たすことが必要となるところ、秘密管理性の要件については、「運用が画一的で現場の実態に合っていない」、「マクロ的な視点から見たイノベーションの在り方と齟齬をきたす」等の指摘がある。

そこで、秘密管理性の基本的な考え方として、例えば米国の裁判例のような費用対便益という考え方を考慮し、企業規模、競争環境、商品のライフサイクル、技術情報等の性質、侵害行為の態様等の重要と考えられる要素を抽出して、営業秘密保護のためのガイドラインの改訂を検討すべきである。

（参考）望ましい秘密管理水準の決定に影響を与えると想定される要素

《保護対象の範囲が狭くなる方向に働くものと想定される要素》

企業・事業規模

企業・事業規模が大きい場合には、厳格な秘密管理が可能な経済基盤を有すると考えられる。一方で、規模の小さい企業に対しては、厳格な管理が困難である場合が想定される。

企業の属する業界の競争環境（ライバル数、市場規模等）

競業他社の数が多い（市場規模が大きい）ほど模倣リスクが高まるため、厳格な管理が求められると想定される。

人材の流動性（離職率、中途採用率等）

労働市場が比較的流動化している市場においては、厳格な管理が求められることが想定される。

《保護対象の範囲が広くなる方向に働くものと想定される要素》

商品の特性（ライフサイクル、将来キャッシュ・フロー等）

ライフサイクルが長い製品や、将来キャッシュ・フローへの寄与度が大きいものは、権利範囲を広く解釈し保護を図ることが必要（開発へのインセンティブ）と考えられる。逆に、ライフサイクルが短いもの等は、権利範囲を狭く解釈する方向に働くことが想定される。

投資規模（開発コスト、開発期間）

投資規模・開発コストが巨大なもの、不確実性が高く開発期間が長いものは、平易な迂回の排除や開発インセンティブの付与の観点等から、保護の範囲を広くすることが求められると想定される。

情報の性質や業務の形態上最低限必要なアクセス者数

情報の性質や業務の形態上、複数人がアクセスせざるを得ない場合には、保護の範囲を広くすることが求められると想定される。

（3）企業における技術情報等の権利帰属問題に関する検討[19][20]

営業秘密とイノベーションを考える際に重要な論点として、情報の帰属先について検討する必要がある。これは研究開発への使用者と労働者のインセンティブ付けや情報管理に関係する論点であり、使用者における研究開発投資へのインセンティブ、従業員における開発へのインセンティブ（報奨金、賃金等）、両者の情報管理能力の違い等を踏まえて、総合的に議論する必要があるものと考えられる。

典型的な論点の一つを挙げれば、「X 社従業員 Y が、在職中に自ら職務上開発したノウハウ又は営業活動によって自ら取得した顧客情報について、それを在職中又は転職先で、X に無断で使用又は開示した場合における Y の行為は不正な競争行為に当たるかどうか」

19 ここで「情報の帰属先」は、制度的スタンダードを論ずるものであり、契約によって、その情報のコントロール権を当事者間で決することを妨げるものではない。

20 柳川範之 [2006]『法と企業行動の経済分析』日本経済新聞社

という問題であり、職務発明の際に議論された論点が、営業秘密の分野で生じている。

使用者及び従業員の研究開発投資へのインセンティブ、両者の情報管理能力の違い、今後の労働市場の在り方等を勘案して、適切なルールの策定を検討すべきである。

（参考）権利帰属問題における従業者帰属、使用者帰属の論点

下記において、①を選択すれば不正競争行為でないことになるが、②であれば不正競争行為に該当することとなる。

① 従業員帰属の場合

従業員帰属とは、契約等がない限り、情報は従業員の支配権に服し続けることを意味する。したがって、この場合には、使用者たる企業側が、契約によって当該情報の支配権を取得する必要があり、契約締結交渉・契約無効の危険・契約の立証の負担は使用者がこれを負うこととなる。

かかる制度においては、従業員は原則的には自己の資産となる開発活動を精力的に行うインセンティブが与えられ、情報の利用方法についても原則的には自由が認められるため、情報交換が促され、かつ、労働者の流動化の萌芽につながるとすれば、マクロレベルでのイノベーションが期待される。

また、使用者との間の契約設計次第では、従業員は当該研究開発から企業が将来取得するであろうリターン全体を大きくしようとして、より高い努力水準を選択することが考えられる。

他方で、使用者と従業者の間の契約が、使用者に一方的な内容によることなく、かつ、使用者の投資インセンティブや事業活動の利便性を考慮しつつ、その事業上コア情報と考える情報については、使用者に支配権を認めることが担保されるような合理的な契約が可能となるような整備をすることが望ましい。

② 使用者帰属の場合

使用者帰属とは、個別に従業員に契約によって支配権を認められた情報以外の情報は、すべて使用者に支配権が認められるというものである（もっとも、暗黙知や職業人格的性質の情報については、性質上従業員に固有に帰属するものと考えられる。）。

この制度においては、使用者が情報について一元管理ができるため、意図せざる情報の流出等を回避できる可能性が高いとともに、研究成果を様々に組み合わせて、その後の研究開発や事業計画に活かしていくことが容易になり、知的資産経営の実現に資すると考えられ、企業内でのイノベーションに資する。

また、イノベーションの成果は、会社の資産を用いることにより得られたものであるから、公平感に合致する場合が多いと考えられるほか、開発が成功した場合には報奨金を支払うことを事前に契約等で設定しておくことで、情報の帰属先を使用者としても、労働者へインセンティブを与えることも可能となる。

他方で、一般的に使用者・従業員のパワーバランスから、使用者の裁量次第で、適切な契約による情報の支配権の従業員への委譲が認められないことになり、従業員の研究開発へのインセンティブが低下してしまう懸念に対処する必要が生じる。

（参考文献）

柳川範之 [2006]『法と企業行動の経済分析』日本経済新聞社
田村善行・山本敬三 [2005]『職務発明』有斐閣
Merges [1999] 'The Law And Economics of Employee Inventions' "Harvard Journal of Law & Technology"
Burk [2004] 'Intellectual Property and the Firm' 71 U. CHI. L. Rev.3

（4）技術情報等の開示・共有インセンティブを創出するための仕組み

技術情報等の共有のコンソーシアムを構築するためには、多くの困難が伴う。

例えば、秘密管理している技術情報等を開示することとなる者は、開示を受けることとなる者が開示をする者に対して秘密保持義務を負うことを期待する。

他方で、開示を受けることとなる者は、秘密保持義務を負うこととなると、仮に、当該技術情報等を従前から保有していた場合であっても、当該コンソーシアムの目的以外には、当該技術情報等を用いることはできなくなるため、「従前から当該技術情報等を保有していた場合には、これを自ら用いることは妨げない」旨の例外条項を入れることが通例である。

しかしながら、開示を受けた者が仮にコンソーシアムの目的以外の用途に情報を用いた場合でも、この例外条項に違反したことについて、開示をした者が証明するのはほぼ不可能であり、結果としてコンソーシアムの構築が頓挫することとなる。

その一つの対応として、中立的第三者の果たす役割が重要であると考えられる。この第三者は、コンソーシアムを組もうとする当事者間を媒介して事業提携の締結に努める者であり、①企業内部の状況を正確に認識し、各企業から開示された情報の信憑性を確認することができ、適切に技術評価することが可能であるような専門性を有し、②協働を行っているどの企業の利害からも中立で、技術情報等の伝達を歪めて行わないことが求められる。

その他、事後的に企業が技術情報等の開示を恣意的に制限又は歪めていることが判明した場合は、それに対する何らかのペナルティを科す制度的仕組みも必要ではないか。そのペナルティとしては、罰則や共同研究から生成する利益の分配比率等、いかに企業の技術情報等の共有・開示を促進するかという視点から、広範な検討が求められる。

このように、関係者間で有用な技術情報等をタイムリーに共有することができるよう、民事的ルールの在り方を含めて総合的に検討を行うべきである。

（参考）適切な情報共有とイノベーションの事例

工作機械産業　～日米独の比較調査～

日本の製造業の強みとされている生産現場の知的熟練がより有効に活用されるイノベーションシステムとしての部門間情報共有システムの重要性を示唆。

工作機械産業にとって、新製品開発に際しCNC[21]メーカーと戦略的企業連合を結成することの必要性を論じるとともに、反証として、米国とドイツの工作機械産業が衰退した理由を工作機械・CNCメーカー間の関係が、距離を置いた関係だった（70年代から80年代にかけて）ことを挙げている。

[21] CNCはComputerized Numerical Controlの略。コンピュータを内蔵した数値制御装置のこと。

半導体露光装置産業　～日本企業と欧米企業の比較調査～

日本企業と欧州の半導体露光装置企業の競争力の違いを、従来展開されてきたモジュール化や企業の境界線の議論による説明を否定し、両者の違い（差別化の要因）を、ユーザーサイドの要望を情報の漏洩のないかたちで効率的に吸い上げる仕組みを作っているか否かという情報共有手法の仕組みに言及している。

出所：中馬宏之 [2002]「日本的もの造り方式とイノベーションの関係」伊藤秀史編著『日本企業変革期の選択』東洋経済新報社、中馬宏之・青島矢一 [2002]「半導体露光装置産業の競争力はなぜ低下したか」伊藤秀史編著『日本企業変革期の選択』東洋経済新報社

（5）企業買収を通じた技術情報等の流出への対応

企業買収を通じた優れた技術の取得は、自ら同様の技術開発を行うことに比して効率的であるが故に、優れた技術を持つ企業は買収のターゲットになり易いと考えられることから、こうした企業買収により技術情報等が流出し、ひいては我が国の産業競争力への影響があるのではないかとの指摘がある。しかしながら、海外の資本により企業が買収されることとなっても、現に当該企業が我が国で活動する以上は、当該企業の有する技術が海外に流出する訳ではないことに加え、実際には、倒産しかねない状態にある企業が、海外資本から救済を受けることにより、当該技術を利用した我が国での企業活動が引き続き可能になり、国内の雇用が確保されることも期待されることに配慮が必要である。

したがって、相互主義の下、グローバル市場の恩恵を享受している状況を踏まえつつ、基本的には、投資規制については、OECD ガイドラインに則して、引き続き外為法の規則により対応することとすべきである。

2　グローバル競争時代における国富増大のための環境整備

（ポイント）

【現状と問題点】

（1）海外からの人材の受入れと活用の必要性

- 少子高齢化社会を迎え、グローバル競争が激化する中で持続的イノベーションを実現するためには、海外から優秀な人材を取り込み、我が国が活用することが不可欠となる。

（2）オープンなグローバル競争の成果を我が国の国益へ還元する仕組み

- 他方で、こうした施策は外国への技術情報等の流出のリスクを増大させることから、海外から優秀な外国人人材を呼び込むと同時に、こうした人材が生み出した知的資産が不正な手段で海外に流出することを防ぎ、我が国の国富に変えていくスキームが必要である。

【具体的検討事項】

- バイドール制度の見直しによる国費研究成果の流出防止
- 第一国出願制度の検討
- ボランティア等を通じた海外への重要技術の流出への対処

第１節　現状と問題点

（1）海外からの人材の受入れと活用の必要性

現代のグローバル競争時代における我が国の経済活動は、国内のみならず海外も視野に入れた市場展開、企業連携、人材戦略を前提とするようになってきている。結果として、大企業のみならず中小企業であっても、国際化による事業機会の拡大の恩恵を享受することができる。このことは、我が国の経済活動が、グローバルな文脈で、資金、知的資産、人材等を取り込みながら価値創造を行わない限り、競争力を維持・強化することはできないことを意味している。

特に、我が国における少子高齢化の進展、学生の理工系離れは、技術とイノベーションを基盤とする我が国経済の成長を長期的に損ないかねない問題である。このような環境下において持続的なイノベーションを実現させるためには、人材政策は対外的にオープンな姿勢を堅持し、優秀な外国人人材を取り込みながら我が国産業の基盤を維持・強化していくことが不可欠となってくる[22]。優秀な外国人人材の取り込みは、直接的には、以下の効果をもたらす。

- 少子高齢化の進展や、学生の理工系離れにより、国内では技術者・研究者を十分に育成・確保できないところを補完する効果
- 頭脳労働者の受け入れがもたらす先端知識や知的刺激といったダイバーシティ（多様性）による相乗効果[23]

---

[22] グローバル環境下においては、開放度と生産性・競争力の増大は、正の相関を示すとされている。Edwards [1997] 'Openness, Productivity and Growth: What Do We Really Know?' NBER Working Paper 5978.

[23] 移民問題の議論においては、とかく単純労働者（Low-Skilled Immigrants）の流入による国内雇用・治安等への影響が注目されがちだが、Saxenian による米国シリコンバレー地域の分析においては、外国籍研究者・エンジニアのようなハイテク移民労働者（Highly Skilled Labor）の存在が、同地域の成長の要因のひとつとして挙げられている。シリコンバレーの議論では、グローバル経済化においては、移民政策は必ずしもネガティブな話としては捉えられていない。当地のハイテク移民は、母国の産業とも強い関係を構築しており、両国に労働市場のグローバル化、企業・貿易・投資機会の拡大等の波及効果をもたらしている。したがって、移民政策と貿易政策はゼロサム・プロセスではない（Saxenian [1999] 'Silicon Valley's Skilled Immigrants: Generating Jobs and Wealth for California'）。

（参考）外国人留学生の割合の日米比較

米　国

○　外国出身の科学技術者の割合：14%（1990 年）→22%（2000 年）
　　うち、重要科学技術分野の博士号保持者：24%（1990 年）→38%（2000 年）
○　2006 年の卒業者のうち、博士号を保持している技術者の約 50%は外国出身（うち、自然科学、コンピュータ・サイエンス、ライフ・サイエンス分野の博士号保持者の 45%は外国出身）
○　数理、コンピュータ・サイエンスの博士号保持者の 44%、自然科学の 35%は外国出身（非科学技術分野における外国人博士号保持者は 10%以下に留まる）

米国は科学技術で後れをとっていることからすると、国として、移民の頭脳が単に必要というのではなく、それに依存しなくてはならない、という事実を受け入れざるを得ないだろう。

出所：The Deemed Export Advisory Committee [2007] 'The Deemed Export Rule in the Era of Globalization'

日　本

○　大学院博士課程修了者に占める外国人留学生の割合は約 16%（大学学部卒業者に占める外国人留学生の割合は約３%）（2005 年度）
○　上記の博士号取得者のうち、理学・工学の博士号取得者の占める割合は約 36%（一方、人文科学・社会科学の博士号取得者の占める割合は約９%）（2005 年度）
○　理工系高度人材における外国人への依存度は、米国ほどではないが、高いものとなっている

出所：文部科学省『文部科学統計要覧（平成 19 年度）』、日本学生支援機構 [2007]『外国人留学生進路等状況（平成 17 年度版）』を基に、経済産業省知的財産政策室において作成

海外では、優秀なインド・中国の人材が米国や欧州を目指し、そして本国の産業との連携強化や帰国の動きが活性化しており[24]、こうした人材が日本を回避するかたちで環流する「ブレイン・サイクル」の仕組みが形成されつつある。翻って我が国における優秀な外国人人材の取り込みは極めて低調である[25]。グローバル競争が激化する中で持続的イノベーションを実現するためには、我が国がこのブレイン・サイクルの流れに取り残されないように、優秀な外国人人材の受入れ及び定着を促す取組が必要となろう[26][27][28]。

---

[24] OECD [2002] によると、中国人留学生全体に占める帰国者の割合は、7.6%(1980)から 41.9%(1998)に増加している（OECD [2002] 'International Mobility of the Highly Skilled'）。

[25] 熟練外国人労働者の比率は、米国 6.0%、英国 4.5%、豪州 7.1%に対して、日本はわずか 1.1%に止まっている（経済産業省『グローバル人材マネジメント研究会報告書』（2007 年５月））。

[26] この点、例えば、米国においては就労者のスポンサーとなる米国企業・研究所の推薦を得た高度技術人材に対して H1-B と呼ばれる特殊職業就労者用の労働ビザを発給している。また世界最大の留学生人口を排出する中国においては、国会の経済建設と社会発展のために、国家戦略（人発（1996）75 号）として、海外留学生等を積極的に帰国させる『海亀政策』を行っている。

[27] Saxenian [1999] によると、1990 年には、シリコンバレーの研究者・エンジニアの 32%はアジア出身で、そのうち 51%が中国系、23%がインド系。1998 年には、中国・インド系エンジニアは、シリコンバレーの企業の約 1/4 を経営し、1680 億ドルと約６万人の雇用を創出している。

[28] 「アジア人財資金構想」においては、我が国企業に就職意志のある能力・意欲の高いアジアからの留学生に対し、奨学金や人材育成から就職支援までの事業を通じて、我が国産業界で活躍する専門イノベーシ

（参考）各国におけるブレイン・サーキュレーション（頭脳循環）の状況

米国

知識労働者等の専門性の高い職業に携わる外国人に対して H1-B ビザ枠（有効期限３年、最長６年まで延長可能。代表的な職種としてコンピュータ関連、会計士、財務アナリスト等）があり、米国雇用者の下で就労が可能となる。2000 年に新規 H1-B ビザを取得した外国人のうち、約４分の３に当る 10 万人弱がアジアからの入国であり、アジアが米国にとって専門労働者の重要な供給源となっている。

特にシリコンバレーではアジア系民族が 21.8%を占めており、この中で中国系が全体の 8.2%と最大である（2000 年）。シリコンバレーの特徴として地域的な技術コミュニティがあり、リクルート等の雇用に関する情報は勿論、特殊な技術知識、経営ノウハウや市場の情報を交換する場として機能している。このような場から派生するネットワークは同じ民族間を中心としつつも、ネイティブの技術やビジネスに関するネットワークにも上手く適合している。また、外国人労働者は母国とも密接な関係を保ち続けており、特に台湾系、中国系、インド系の多くの者は、定期的に母国と米国とを往復し、企業に対してビジネスに関する情報交換、ベンチャー企業やファンドへの投資、政府高官への助言を行う等、ネットワーク資源を積極的に提供・活用している。

ドイツ

ドイツでは 2005 年に新移民法が施行され、従来４種類に分かれていた滞在許可を、期限付きの滞在許可と無期限の定住許可の２種類に整理統合し簡素化した。また、高度技能者の受入促進のため、高度技能者はドイツ入国後直ちに無期限定住許可を取得できるものとなった。また、外国人留学生は自分の取得した学位に適合した職を見つけるために卒業後１年間ドイツに留まることができる。

バイオテクノロジー産業では、公的研究の資金調達を民間投資で実現することを目指した「バイオレジオ（Bio-regio）」制度によって、バイオテクノロジークラスターの基盤を創り上げることに成功し、ドイツ人研究者と科学者を米国から呼び戻すことに寄与したと言われている。

英国

2000 年に IT 関連産業や医療部門等での技能労働者不足を補うため、就労許可証のビザの規制の緩和を行った。さらに、2002 年より科学、金融等の高度な専門技術者の受入れをより増やすために、「高度技能移民プログラム」を導入し、「学歴」、「職歴」、「過去の収入（年収）」、「就労希望分野での業績」、「一般開業医特別枠」の５種類の得点エリアの合計が所定以上であることを条件として、求人に有無にかかわらず、１年間滞在が許され、最大３年間の滞在延長が可能となった。また、合計４年間高度技能移民として就労した後は、定住を申請することもできるものとなっている。

また、英国では 2008 年から外国人受入制度を大幅に再編する方針を示し、ポイントベース制（スキルや経済的利益を生み出す可能性、英語力等に応じてポイントが付与され労働が許可される仕組み）を全ての受入分野に適用する方向で制度見直し進めている。

英国政府はウルフサン（Wolfson）基金と共同で、ロイヤルソサエティーが運営する「研究メリット賞」（Research Merit Award）制度に資金を拠出しており、優秀な研究者の引止めや、産業界や外国から優れた研究者の招聘に活用されている。

フランス

受入区分は原則として大きく４区分からなり、期間や対象者等により細分化されている。また、国際競争力の向上のため、新規に入国する外国人のうち、上級管理職等、一定の条件を満たす高度技能労働者については、臨時滞在許可証がスピード発行される等、高度技能者の入国条件や受入手続の緩和措置を行っている。臨時滞在許可証は１年間有効で更新が可能である。別途、国内各分野の発展に寄与すると考えられる「能力と才能」という区分に該当する場合は、３年間有効な滞在許可が付与される。

ョン人材の育成を促進している。こうした取組を通じて、国際的な知的ネットワークの形成による、我が国の国際競争力の強化を図ることとしている。

中国

「第十一次五ヵ年計画」（2006 年３月）において人材強国戦略の推進が打ち出されるように、中国政府は科学技術人材の重要性を認識した上で、留学生等の在外研究者の帰国を支援する、いわゆる「海亀[29]」支援政策を展開し、祖国のために貢献することを推奨している。

例えば、中国科学院の「百人計画[30]」 は、1994 年に中国で開始された「高目標、高基準、高強度」の人材招致・養成策であり、海外の第一線で活躍する研究者を中国に帰国させる計画で、研究資金を重点的に配分する等の資金面でのインセンティブを与えている。

最近では、流出する学生に対する帰国する学生の割合が上昇に転じる等、徐々に還流の傾向が強まっている。

韓国

専門技術者の外国人労働者はＥ系統のビザによって入国が許可される。韓国では積極的に専門技術者の受入れを推進すべく３種のカード（ゴールドカード、IT カード、サイエンスカード）制度が設けられ、ビザ発給の時間を大幅に短縮する等の優遇策がとられている。

また、海外人材の獲得のため科学技術省が運営する「ブレイン・プール・プロジェクト」は、公的又は民間研究機関で２年を上限として海外の優秀な科学者やエンジニア等を獲得することを目的としており、1994 年～2006 年で 207 機関に 1220 名の研究者が雇用された。

研究者交流事業では、2004 年～2006 年で、海外からの 225 名の科学者に対して資金援助が行われ、海外へ 282 名の韓国人科学者が渡航した。

日本

ポジティブリスト制（一定の要件を満たす場合に本邦における就労を許可する方法）の外国人受入制度となっており、「技術」、「人文知識・国際業務」枠等、27 の在留資格に基づき外国人を受け入れている。2001 年～2005 年において、「技術」及び「人文知識・国際業務」枠での外国人登録者数はそれぞれ約１万９千名から約２万９千名、約４万名から約５万５千名であり、特に技術分野における人材の増加が顕著である。これは IT 技術者資格の相互認証を幾つかの国と行ったことに伴い、「技術」の資格要件の緩和が行われた結果と考えられる。

また、日本学術振興会では研究者国際交流の支援制度を実施しており、例えば「外国人特別研究員」枠では、渡航費、滞在費等を用意することで、海外から優れた研究者の受入れを推進している。

（参考文献）

- 本山康之 [2003]『シリコンバレーにおけるハイテク移民労働者の役割』
- 経済産業省『通商白書 2003』
- OECD [2002] 'The International Mobility of the Highly skilled'
- 内閣府経済社会総合研究所 [2007]『平成 18 年度内閣府経済社会総合研究所委託調査（英独仏における外国人問題への取組及びその課題に関する調査研究報告書）』
- 日中科学技術交流会 [2005]『日中科学技術』No.115
- 独立行政法人科学振興機構 中国総合研究センター中国科学院「百人計画」 <http://crds.jst.go.jp/CRC/plan/m4-3-3.html>
- Park [2007] 'Policy and approach for enhancing the international mobility of researchers : the Korea cases'
- 遠藤誉 [2001]『中国がシリコンバレーにつながるとき』日経ＢＰ社

29 海外から帰国して研究者又は創業者として活躍している高度技術人材のことをいう。

30 1997 年に「傑出人材導入計画」と「国内百人計画」に分割され、2001 年には「海外有名学者計画」が追加された。

（参考）国際的な人材強化としての高度人材の受入拡大に関する施策

骨太の方針 2008（抄）

第２章成長力の強化
１．経済成長戦略
Ⅱグローバル戦略
③国際的な人材強化
ｉ）高度人材の受入拡大
経済成長のカギは人材であり、今、多くの国が高度人材を集めることにしのぎを削っている。我が国においても、能力に見合った高い処遇での人材誘致や、企業の幹部・基幹業務への登用を始め、より魅力的な雇用環境、生活環境の整備を早急に進め、高度人材の受入れを拡大する。
・ 世界から高度人材の受入れを拡大するため、産官学労で構成する「推進会議」を設置する。「推進会議」の場で、数値目標の設定や必要な施策について検討し、平成 20 年度中に関係府省でアクションプログラムを策定する。

戦略実行プログラム（別紙）
（３）国際的な人材強化
A 高度人材の受入拡大
政府内に産官学労からなる「推進会議」を設置する。高度人材の受入れの数値目標設定や下記の事項等について、「推進会議」の場で検討を進め、平成２０年度中に関係府省が協力してアクションプログラムを策定する。

（ア） 企業等における外国人活用の推進
① 企業における人事評価・給与評価の公平さと透明性の向上
② 国際化指標を策定・公表し、企業の人材の国際化を後押し
③ 社会保障協定（国際的な年金通算等）の締結の加速
④ 高度技能実習制度の導入についての検討
⑤ 企業の幹部や基幹業務への外国人高度人材の登用拡大
⑥ 留学生向けの採用枠の設定・拡大等、企業における積極的な採用促進
⑦ 中央官庁等における外国人活用（特に観光庁、JETRO 等）
⑧ 在留資格の明確化
（イ） 高度人材の範囲の検討
（ウ） 外国人が住みやすい生活環境作り
① 先進的な英語教育を推進するインターナショナルスクールに係る税制面の支援等を引き続き推進。都道府県の各種学校への認可基準（土地建物の自己所有要件等）の見直しを促進
② 内外での日本語教育を強化
③ 外国人の受診しやすい医療環境の整備の推進（医師等の相互受入れの拡大等）
④ 有能な高度人材を受け入れるために、永住資格の付与を促進

（２）オープンなグローバル競争の成果を我が国の国益へ還元する仕組み

先に述べたとおり、グローバル化した国際競争環境の中で我が国が競争力を維持・強化していくためには、グローバルな文脈で対外的にオープンな姿勢を貫きつつ資金、知的財産、人材等を受け入れながら価値創造を行うことが必須となっている。逆に言うと、相互主義の下でグローバル市場に参加しながらそうしたメリットを享受するためには、排外的な姿勢は選択肢となり得ないものである。

そして、国際市場から受け入れた資金、知的資産、人材等を最大限に活用し、その成果を適切に我が国の国富としていくことが重要な視点である。これは、我が国において創造された価値には、その生成の過程において何らかのかたちで我が国のリソースが投入されていることを考えれば、その成果を我が国が享受することは当然のものとして理解されることであろう。事実、諸外国においては、いまやグローバル市場で取り込んだ技術情報等をいかに自国の国富に還元していくかについての取組が強化されつつある[31]。

一方で、オープンな受入れ姿勢でグローバル市場に参加することは、不可避的に外に向かうリスク、すなわち国内で創出された価値が国外に流出し、我が国がその価値を享受する機会を失うことが起こりうる。いかにオープンなつながりを深化しようとも、その成果を適切に受けることができなければ、それはみすみす国益を失っているにすぎない。

したがって、オープンなグローバル競争の成果を、適切に我が国の国益へと還元するための仕組みについて検討するべきである[32]。

（参考）グローバル競争時代において想定される海外への技術情報等の流出リスク

グローバル競争時代において、以下のような技術情報等の流出リスクが想定される。

- ○ 留学生・外国籍の大学教員による技術の持ち出し
- ○ 外国人従業員による技術の持ち出し
- ○ 我が国企業の経営に参画した外国資本による技術の持ち出し
- ○ 終身雇用の崩壊による企業への帰属意識の低下、早期退職等のリストラ、処遇への不満に基づく技術情報等の持ち出し
- ○ 企業の海外展開に伴う国際的な人材の移動に伴う持ち出し
- ○ アジア諸国において高まる日本人技術者・研究者（特に、成熟産業における熟練者・経験者、最先端分野における高度技術人材）の需要を端緒とした持ち出し

31 このような状態を、グローバル化の恩恵にあずかりながら国益の確保を図る新しいかたちでの国家利益の追求がなされていると分析する論者もいる。グローバル化による市場環境の変化を国家レベルの視点で見ると、2001 年の中国の WTO 加盟に象徴されるように、グローバル化は、国家の在り方に影響を与える重要なファクターであり、国境は融解し、主権国家の役割は低下し、それに代わる超国家的なアクターの出現が予想された。しかしながら、識者のそうした予想に反して、グローバル化によって国家の役割は必ずしも低下していない。むしろ、グローバル化の進展によって、新しい国家間の競争の時代に入ったとの分析が有力である。

32 この点、米国のみなし輸出規制（Deemed Export Rule）の議論においても、米国が競争力を持ち続けるためには外国人人材の能力を最大限に活用していくことが不可欠であることを強調しながら、同時に発生するリスクとして外国人を通じた重要技術の持ち出しについて適切な対応が必要であることを論じている（The Deemed Export Advisory Committee [2007] 'The Deemed Export Rule in the Era of Globalization'）。

第２節　具体的対応

（1）バイドール制度の見直しによる国費研究成果の流出防止

いわゆるバイドール制度は、研究成果の社会への還元が、教育、研究に続く大学の「第三の使命」と位置づけられるという大学の伝統的な役割の変化を受けて、大学から産業界への技術移転活動を促進するための制度として、1980 年に米国で導入されて以降、各国において同様の制度が導入されてきたところである[33]。我が国においても、1999 年に日本版バイドール制度が導入されている。

米国の制度においては、政府資金による研究開発の受託は外国企業にもオープンとする一方で、研究受託者自身に対して法令の規定等により米国内での製造を優先することとなっている。さらに、バイドール法の規定により研究受託者からバイドール適用特許の排他的ライセンス（専用実施権の場合を含む。）を得ようとする第三者に対しても国内製造優先が義務付けられている。このように、外国企業を含めた研究受託者が行った研究の果実（＝成果）を米国内に取り込み、適切に米国の国富とするという米国の競争力強化の考えを具体化する仕組みであるといえる。

翻って我が国のバイドール制度においては、研究受託者自身に国内製造優先は義務付けられていない。このため、国費を投じた研究成果が、国外の第三者への実施権許諾や譲渡等を通じて、我が国の国富とならずに海外へ流出することが懸念されているところである[34]。

今後、グローバルな文脈で優れた人材や知識を取り込みながら価値創造を行うことが、これからの我が国の国際競争力を維持・強化の在り方となることにかんがみると、我が国のバイドール制度においても、国内優先実施を規定すること等により、国費研究成果の海外への流出を防止し、我が国が適切に研究成果を享受できるような方策を検討すべきである。

（参考）日米バイドール制度の概要

日本（産業技術力強化法第 19 条）

1999 年に産業活力再生特別措置法第 30 条として、研究活動の活性化とその成果の民間事業活動における効率的活用の促進を目的として立法化された（平成 19 年に産業技術力強化法 19 条に移管された。）。委託事業において生じた、特許権、実用新案権、意匠権、プログラム著作権・データベースの著作権、回路配置利用権、育成者権等の知的財産権を対象としている。

＜バイドール適用の条件＞
① 研究開発成果が得られた場合、遅滞なく、国にその旨を報告する。
② 国が公共の利益のために特に必要があるとした場合に、受託者は無償で利用する権利を国に許

[33] 中山一郎 [2007]「日米バイドール制度と大学発明の特許化・ライセンス」椙山敬士・高林龍・小川憲久・平嶋竜太編『ライセンス契約（ビジネス法務体系１）』日本評論社
[34] その他の海外流出の形態として、企業買収による移転等により、特許権が日本国内で生産しない海外事業者の保有となるケース等も想定される。

諾する。
③ 正当な理由なく当該特許権等を相当期間活用していない場合、国が求めるときは、受託者は当該特許権等を利用する権利を第三者に許諾する。

＜国内優先実施に係る要件（契約上で規定）＞
法律上では規定されていないが、例えば、NEDO 業務委託契約書においては、契約者以外に業務委託で得られた発明の専用実施権等を許諾する場合には、NEDO に対して承認申請書を提出し、承認を得る必要があることが規定されている（「ただし、日本国内において生産されることを当該第三者に約させた場合は、この限りでない」とされている。）。

米国（ Bayh-Dole Act 1980（35 U.S.C. §200-§212））
1980 年に Bayh-Dole Act として、連邦政府資金から生じた発明に関する権利の帰属に関する政府共通的なルールが示された。連邦政府資金の性格を問わずに受領者に対して適用され、特許を受ける権利が対象となる（1980 年当初は、中小企業及び大学等の非営利法人が適用対象であったが、1984 年以降は大企業にも適用されることとなった。）。

＜バイドール適用の条件＞
① 発明をした時から２ヶ月以内に政府へ通知（発明開示）、特許権の所有を希望する場合は政府への申出。
② 通知又は申し出をしなかった場合には、政府が所有することができる。特許申請を怠った場合にも、政府の所有とすることができる。
③ 例外的な状況（原子力駆動装置・兵器関連プログラム等の場合）である場合は、政府は中小企業・非営利法人による権利の保有を認めないことができる。
④ 合理的期間内に発明の実用化が期待できない等の場合、政府は第三者に実施権を許諾する権利を行使することができる。

＜国内優先実施に係る要件（法律上で規定）＞
（§204 Preference for United States industry）
法律上の規定で、バイドール法の適用を受ける特許権についての独占的実施権の許諾は、米国内で実質的に製造することを約した者に対してのみ認められる、とされている。

（２）第一国出願制度の検討[35]

グローバルに外部からの知恵を取り込んで国内の価値と結びつけるグローバルな価値創造が、今後の我が国の競争力の強化の在り方となる中で、日本市場においてなされた投資に見合う効果を我が国に帰属させることが肝要である。

我が国で生み出された研究開発の成果について考えるとき、日本国内で知的財産の創造、保護、活用のサイクルが機能することが重要である。そうした知的創造サイクルがうまく機能するためにも、当該成果が特許というかたちで日本国内に蓄積されることが必要となる。

米国では安全保障上の観点から秘密特許制度（第２章第２節（３）で後述）の一環として、すべての特許出願について、特許商標庁長官の許可無く他国に先に出願することができないという第一国出願の義務[36]があり、事実上、特許化される研究成果はすべて米国で特

[35] 第一国出願制度は、「第２章　安全保障の視点」において議論される秘密特許制度の一部である。
[36] 米国特許法においては、秘密特許制度の実効性を担保するため、国費研究成果であるか否かにかかわら

許出願することが強いられている。

一方、我が国の現行特許制度においては、第一国出願の義務を課す規定は設けられておらず、我が国で開発された技術について、国内で出願せずに他国にのみ出願することが可能となっている。これは、我が国で生み出された研究開発の成果が国内の知的創造サイクルの好循環に結びつかず、競争力の損失となっているのではないか、との指摘もある。

したがって、我が国において、後述する秘密特許制度が導入されることになった場合に、日本国内における企業の研究活動への影響に配慮しつつ、第一国出願制度の導入について検討すべきではないか。

（3）ボランティア等を通じた海外への重要技術の流出への対処

日本人技術者・研究者が技術移転（意図せざる流出を含む。）を行うのは、「働きがいやボランティア精神」、「当該技術者等がおかれた境遇に対しての不満」等を理由とするものであると考えられる。こうした事態への対処については、各企業において技術者の処遇を今一度見直すことを促すとともに、能力に応じた成果や環境が選択できる雇用環境の整備を図ることが適切である。

また、退職した日本人技術者自身による重要な技術情報等の海外流出を懸念する指摘があるが、これまでの経済成長を支えた技術者は、我が国に無形な価値をもたらしてくれた功労者なのであるから、彼らのノウハウ、使命感に応えるべく、人材バンクの活用[37]、ボランティア・ネットワークの形成を通じて、彼らが有する技術・ノウハウを我が国の今後の経済成長に繋げていくための仕組みについて検討することとすべきである。

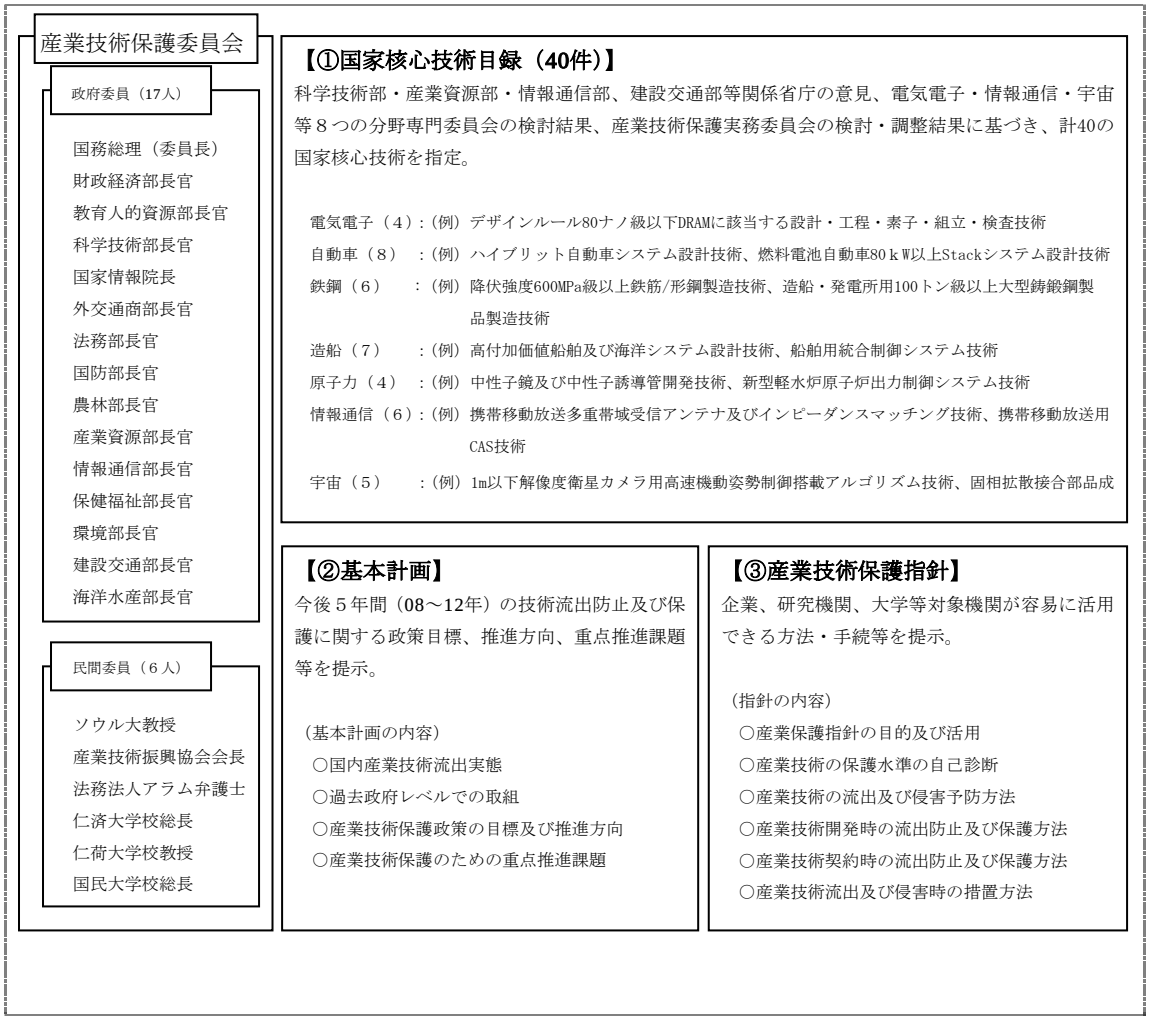
（参考）韓国における重要産業技術の流出防止体制

「産業技術の流出防止及び保護に関する法律」に基づき、産業技術のうち経済的価値が高く、海外に流出した場合に国家の安全保障及び国民経済の発展に重大な悪影響を与えるおそれのあるものを「国家核心技術」として指定、当該技術の保有・管理者に対し、流出防止のための保護措置、輸出承認の義務外国で使用し又は使用される目的で流出及び侵害する行為に対する罰則等を規定している。

同法に基づき、関係省庁及び民間有識者からなる「産業技術保護委員会」が組織され、同委員会は、①国家核心技術の指定、②産業技術の流出防止及び保護に関する基本計画の策定、及び③産業技術保護指針の策定を行う。

ず、「米国内でなされた発明は、何人も、米国特許商標庁長官の許可がある場合を除き、米国出願から６ヶ月が経過するまでは、外国へ出願等をしてはならない」（35 U.S.C. 184）としており、関係省庁において、当該出願内容を秘密特許とすべきかどうか判断する期間を確保している。また、米国出願なしに外国へ出願等する場合や外国出願のために技術データを国外へ持ち出す場合等にも、同長官の許可が必要とされている（37 CFR 5.11）。これらの規定が、いわゆる「第一国出願制度」と呼ばれている。

[37] 「企業等 OB 人材マッチング事業」においては、長年の企業における実務経験を退職後に活かしたいと考える OB 人材と、新事業展開や事業革新に取り組みたい中小企業のマッチングを行う事業であり、本事業を採択した民間企業・公的機関が全国各地でマッチング事業を通じて起業支援を行っている。



（参考）中華人民共和国科学技術進歩法の概要

「中華人民共和国科学技術進歩法」は、科学技術の進歩を促進と、科学技術が経済発展に貢献することを目的として制定された法律である。2007 年に修正された改正法においては、これまで以上に科学技術の発展の促進を強調するとともに、海外からの技術の導入、科学技術の経費に投入する財政資金の投入の増加、知的財産の囲い込み等を打ち出している。

革新型国家の創設

- 科学技術による国家建設戦略を実施する。また、革新型国家を建設する。
- 学校及び教育機関による科学精神の育成を重要視する。
- 研究開発の奨励・科学技術の応用を通じ、従来型産業の改造、ハイテクノロジー産業と社会事業の発展を推進する。

技術革新を支援する環境の整備

- 軍事部門と民需部門における双方向の技術移転を促進し、科学技術資源の配置も軍事部門と民需部門を調和させる。
- 知的財産戦略を制定し、知的財産権を尊重する社会環境を構築し、法に基づき知的財産権を保護する。
- 基金の設立、税制面・減価償却での優遇措置、知的財産権担保業務、融資の提供、資本市場の整備を行う。
- 政府資金を利用した科学技術基金プロジェクト又は科学技術計画プロジェクトの成果である知

的財産権は、当該プロジェクトの実施者が取得する。

海外技術の導入

- 国の産業政策と技術政策に基づいて、国外から先進的な技術と設備の導入を奨励する。
- 導入した技術を消化・二次革新する。

企業を主体とする技術革新

- 企業を主体とし、市場を基礎とし、企業・研究開発機関・大学機関が連携した技術革新体系を構築する。
- 企業が研究開発と技術革新に向けた投入を拡大し、自主的な研究開発テーマの選定を奨励する。

科学技術者に対する奨励

- 外国の優秀な科学技術者が中国において研究開発に従事する場合、中国における永久移住権を優先的に取得できる。
- 模索性が強く、リスクの高い科学技術研究開発プロジェクトを実施し、勤勉な態度で責任と義務を果たしたものの、当該プロジェクトを完了できなかった場合には、当該科学技術者に寛容を与える。

研究開発費の投入

- 国が科学技術の経費に投入する財政資金の増加幅は、国家財政における計上収支の増加幅を超えるものとする。

知的財産の囲い込み

- 財政資金を利用した科学技術基金プロジェクト又は科学技術計画プロジェクトの成果である知的財産権は、先に国内で使用することを奨励される。
- 国内で独自に革新した製品、国が重点的に支援する製品について、政府は初めて発売されたものを率先して購入する。
- 国は科学技術機密保持制度を実施し、国の安全と利益に関連する科学技術の秘密を保護する。

委員のコメント（概要）：競争力の視点

○ 知的財産政策、イノベーション政策及び移民政策はセットにして考えないといけない問題である。また、ハイテク移民を引きつけるという観点からは、外交政策もセットにして考えていく必要がある。

○ ハイテク移民は、進出先と本国の橋渡しとなりグローバルなネットワーク化に貢献する等、受入国及び送出国の双方に貢献があると数々の研究で指摘されているが、日本はこのポテンシャルを活かしきれていない。

○ ハイテク移民を活かしていくためには、対外的にオープンな姿勢を示していくことが必要であるが、それに加え、移民が我が国にとどまるようなインセンティブや、本国への帰還を思いとどまらせるような動機付けが必要ではないか。

○ 国益の観点から、優秀な海外人材の取り込みを進めつつ、同時に技術流出リスクを低減する対策をとることが必要であり、これを入管政策も含めて考えることが必要。

○ 大学は、経産省から留学生に対する機微情報へのアクセスの配慮を求められ、文科省からは留学生受入れを増やすよう求められている状況にある。そのため、大学に対して、誰にどのような情報のアクセスを許すべきかといったガイドライン的なものを作成できないか。

○ 外為法で役務提供が制限される非居住者は６ヶ月で居住者になるが、「６ヶ月」という期間は妥当か。罰則の強化を行えば、抑止効果を高めることが可能ではないか。

○ 米国のバイドール制度は原則、国内企業を優先に考えている。日本のバイドールもそうあるべきであり、制度の見直しが必要。

○ 諸外国において第一国出願制度が実施されており、我が国企業もその制度に従って事業を行っている状況において、我が国に第一国出願制度を導入しても弊害はないと考える。しかし、医療方法の特許等、我が国では認められず外国では認められる権利等については、第一国出願制度が問題となり得る可能性がある。

○ 米国の好事例をそのまま我が国に導入しても根付かないことも考えられるため、我が国の立場で見て国益に資するかどうかという前提で考えるべき。

○ 米国を初めとするいくつかの諸外国では「ディスカバリー制度」が設けられており、日本企業がこれによって商業秘密を強制開示されることもあり得る。我が国も、司法手続きに基づく証拠開示請求について、然るべき法改正や運用制度の整備・充実化を図ることが必要。

○ 現在の技術開発はアライアンスなしには不可能であるとの意見はもっともだが、海外とアライアンスを結ぶ際には、準拠法が国ごとに異なり、情報が保護されなくなる可能性があるため、保護法制の水準が世界的に同じレベルであることが必要。

○ アライアンスが求められているからこそ厳格な情報管理が求められ、その実効性を担保するためには、違反に対する罰則の脅威が必要である。

○ 韓国は国家核心技術を指定する等、国家の競争力に重大な影響を及ぼす技術流出に対する罰則を厳格に規定している。我が国も同様に厳格な刑事罰があってしかるべきであると考える。

第２章　安全保障の視点

（ポイント）

【現状と問題点】

（１）安全保障上の機微技術と民生技術の区別の曖昧化・流出ルートの多様化

- 軍事転用可能なデュアル･ユース性を有した先端民生技術が多くの分野において登場しており、純粋な経済取引・学問研究が安全保障上の側面を有することとなっている。
- 技術情報等の伝達手段も、デジタル情報等の「無体物に化体」したものが主流となりつつあり、そのルートも多様化している。

（２）安全保障関連の技術情報を共有する基盤

- 我が国において安全保障的な影響を有する技術情報を保護する制度整備がなされなければ、我が国及び他国の安全保障に対する脅威をもたらすとともに、我が国の信頼を失墜させ、安全保障上の機微技術情報の受入れに重大な支障を来たし、我が国の防衛産業の技術力・生産力の毀損につながるものである。

【具体的検討事項】

- **重要情報の区分ルールの導入**
- **機微技術リスト・ガイドラインの作成**
- **秘密保護法制の在り方**
- **秘密特許制度の検討**
- **外為法の技術取引規制の強化**
- **投資を通じた安全保障上重要な技術の海外への流出防止**
- **不審アクセス情報の報告と注意喚起の仕組み**

第１節　現状と問題点

（１）安全保障上の機微技術と民生技術の区別の曖昧化・流出ルートの多様化

安全保障上の機微技術の流出は、懸念国家への流出や大量破壊兵器やテロへの転用等によって、我が国及び他国の安全保障に対する直接的な脅威となる。したがって、安全保障上の機微技術の流出に対しては、国際社会における我が国の責任として厳格に対処することが必要不可欠である。

こうした中で、急速な技術進歩により、今日では多くの民生技術が軍事転用可能である

ことが指摘され、こうした軍事転用可能なデュアル・ユース性を有した先端民生技術があらゆる分野において登場している（安全保障上の機微技術と民生技術の区別の曖昧化）。

これは、従来は合理的であると考えられた経済取引や学問研究が、安全保障上の視点から重大な支障を生じさせる場合があることや、これまで純粋な不法行為・債務不履行として民々関係において処理すべきとされていた案件が、安全保障的な側面を有することを意味する。

また、近年のグローバル化、人材の流動化、IT 化等による情報の拡散のスピード、量、範囲の増大に伴い、安全保障上の機微技術の流出の経路が、従来のように、「モノ」に化体した流出から、ヒトやデジタル情報等の「無体物」に化体した流出へとウェイトが移りつつある（流出経路の普遍化・多様化）。

これは、これまでの「モノ」や「サービス」の取引に着目した規制のみでは必ずしも実効的でない場合があり、場合によっては取引以前の「ヒト」の基本的な行動の在り方にまで踏み込んで議論をしなければならないことを意味する。

翻って我が国の現状を見るに、こうした安全保障上の機微技術と民生技術の区別の曖昧化、流出経路の普遍化・多様化といった近年の趨勢変化に十分に対応できているとは言えない状況にあるのではないか。

例えば、安全保障上の機微技術であっても、特許出願がなされれば公開され、誰でも当該技術にアクセスが可能となるほか、大学における研究のほとんどが軍事転用可能になっているとの指摘があるにもかかわらず、こうした研究実施及び成果公表の是非の判断は現場の研究者に任され、適切な規律が存在しない状況にある。

また、外為法による輸出管理規制は大量破壊兵器の拡散を防止し安全保障上の機微技術の移転を禁じているものの、安全保障上の問題を提起しかねない技術情報等の内容をインターネットや学術誌、専門誌、又はその他のメディア上に公開して世界中に開示してしまうことは止められないほか、増加する外国人従業者・留学生等を介した機微技術情報の流出への対処の方法も検討を要する状況にある。

（2）安全保障関連の機微技術情報を共有する基盤

安全保障上の機微技術を適切に管理する別の理由として、安全保障上の機微技術を受け入れるための情報保護体制を構築するという側面がある。我が国において安全保障上の機微技術を保護する制度整備がなされなければ、安全保障上の機微技術の受入れや共有に重大な支障を来すことになる。

このように、安全保障上の機微技術の流出は、我が国及び諸外国に対する安全保障上の問題をもたらすのみならず、我が国の国際社会における信用を失墜させ、機微技術情報の提供が受けられず、我が国の防衛産業を始めとする機微技術情報を用いる産業の技術力・

生産力の基盤を毀損するおそれがある。このような観点からも、安全保障上の機微技術情報の適切な管理について検討することが必要である。

（参考）先端科学技術等をねらった対日有害活動

平成 18 年に警察庁が発行した「先端科学技術等をねらった対日有害活動」によると、北朝鮮、中国、ロシアが我が国の先端科学技術に強い関心を有し、これら技術情報をターゲットにした対日諸工作を行っていることが報告されている。

北朝鮮

「北朝鮮は、これまで、科学技術の発展に力を注いできています。・・・二〇〇六年（一八年）四月に開催された最高人民会議第一一期第四回会議では、科学技術の発展が議題として上程され、次のような報告がされています。・・・『先端技術を導入するという原則の下に海外同胞商工人ら及び各外国企業との合営・合作も実現するなど、対外経済協力事業を活発に展開していくであろう』・・・これらからもうかがえるように、今後、我が国の企業との共同経営や在日朝鮮人である商工人、科学者等との協力の強化に伴い、先端科学技術並びにそれに関する情報及び物資の違法な流出が懸念されるところです。

一方、我が国には、朝鮮総聯の傘下団体として在日本朝鮮人科学技術協会（以下「科協」という。）という在日朝鮮人科学者等で構成された団体が存在しており、様々な活動を通じて、北朝鮮の科学技術発展に寄与することを目指しているとされています。

このような団体による情報の違法な持ち出し等を通じて、我が国から先端科学技術等が流出するようなことがあってはなりません。また、こうして我が国から持ち出された先端科学技術等が、核開発や大量破壊兵器の開発等に悪用されるようなことがあってはなりません。このため警察は、先端科学技術等の流出に対する監視を徹底するとともに、違法な事案が把握された場合には、厳正に対処することとしています。」

主な検挙事例

一　大量破壊兵器関連物資等の不正輸出事件

① シンクロ・スコープ等不正輸出事件（一九八七年（昭和六二年）静岡）

② 集積回路等不正輸出事件（一九八九年（平成元年）新潟）

③ フッ化ナトリウム等不正輸出事件（一九九六年（平成八年）兵庫）

④ スクーバ用ダブルバルブ不正輸出事件（一九九八年（平成一〇年）警視庁）

二　北朝鮮に関連するその他の事件

① ジェット・ミル調達動向の判明

② 科協幹部による薬事法違反事件

中国

「中国は、一九九二年（四年）九月、全国の省・軍の幹部に対し、『中国共産党中央七号文件』を配布し、対外情報活動の強化等について指示をしたと言われており、現在もこの指示にのっとり積極的な情報収集を行っているものとみられています。」

「中国は、科学立国の建設のためには、我が国からの技術移転が必要不可欠と認識しており、先端科学技術の習得のため、多数の学者、技術者、留学生、代表団等を我が国に派遣し、多面的かつ活発な情報収集活動を行っているものとみられます。また、これらの目的で来日した中国人、在日中国大使館員等を介して、我が国の技術者等に対する幅広い工作を活発に行っており、我が国からの技術移転の拡大を図っているものとみられます。

しかも、中国の情報収集活動は極めて巧妙であり、多数の中国人が、断片的で些末であると思われる情報を収集していることが多いため、情報収集活動が行われていることが認識されにくいという特徴があるとみられます。

警察は、平素から情報収集に努めるとともに、違法行為に対しては、厳正な取締りを行うこととしております。」

主な検挙事例

① 汪養然事件（一九七六年（昭和五一年）警視庁）
② 横田基地中ソスパイ事件（一九八七年（昭和六二年）警視庁）

ロシア

「ロシアの情報機関員は、旧ソ連崩壊後も各国において外交官等を装って諜報活動を活発に展開していることが明らかになっています。我が国においても、過去、旧ソ連及びロシアの情報機関員によると認められる諜報事件を十数件検挙しており、このうち旧ソ連が崩壊した一九九一年（三年）以降は八件を検挙しています。こうした諜報活動は、冷戦期のイデオロギー対立に根ざした特有の動向ではなく、ロシアが、日米間の軍事動向や我が国の内外政策のみならず、先端科学技術にも依然として強い関心を示し、我が国に諜報活動の重点を置いていることを示すものといえます。

諜報活動の対象は、先端科学技術製品から、当該製品の製造工程が分かる資料、研究中の新技術の将来性等にまで及び、その製品等の種類も汎用性の高いものから、用途の限られたものまで多岐にわたっています。

ロシアは、先進諸国の先端科学技術を積極的に導入する姿勢を示しており、プーチン大統領が二〇〇六年（一八年）五月に行った年次教書演説では、『国の経済発展は主としてその科学と技術の優位性によって決まる。残念ながら、今日ロシア工業において使用されている大半の機械設備は、先進レベルから数年単位ではなく数十年単位で立ち遅れている』などと述べて、自国産業の弱点を克服するためには、『国家が国外での現代的テクノロジーの獲得においても助力を与えなければならない』と指摘するなど、国家が早急かつ積極的に関与していく必要性を力説しています。」

今後、ロシアは、先進諸国の企業の誘致活動、合弁・技術提携、買収等を活発化させ、自国の企業に対し財政支援を行い、積極的な先端科学技術の導入を推進していくものとみられますが、他方、情報機関員の違法情報収集活動による先端科学技術の移転工作も、並行して活発に展開していく可能性があります。

ロシアでは、経済成長を背景とした国家税収の増加が、情報機関員の海外における各種諜報活動を活発化させることも懸念されます。これまでのように在日ロシア大使館員や在日ロシア通商代表部員を装った情報機関員が違法行為を行う可能性があるほか、今後、活発化する日露間の経済交流を通じて、経済代表団、我が国に進出する企業の社員等を装った情報機関員が、企業間提携、技術交流等を口実とした各種諜報活動を展開する可能性があります。」

主な検挙事例
① 黒羽・ウドヴィン事件（一九九七年（平成九年）警視庁）
② チェルヌィーフ事件（一九九七年（平成九年）警視庁）
③ ボガチョンコフ事件（二〇〇〇年（平成一二年）警視庁・神奈川）
④ シェルコノゴフ事件（二〇〇二年（平成一四年）警視庁）
⑤ サベリエフ事件（二〇〇五年（平成一七年）警視庁）
⑥ 在日ロシア通商代表部員らによる窃盗事件（二〇〇六年（平成一八年）警視庁）

出所：警察庁『先端科学技術等をねらった対日有害活動』焦点第 273 号（2006 年 12 月）

第２節　具体的対応

（１）重要情報の区分ルールの導入

一定の組織間で情報共有がなされる場合、情報の重要度レベルとカテゴリの区分に関するルールが規定されることによって、各情報保有主体における統一的な対応が可能になる。米国では、国家安全保障に係る情報の分類方法の考え方を定めた国家安全保障情報区分“Classified National Security Information”[38]が存在し、このルールによって安全保障情報

[38] CNSI (Classified National Security Information) : 大統領令によって発出される安全保障情報の統一的

が定義、区分され、各種秘密保護法制や情報保全規程における保護・保全対象の基礎となっている。

これに対し、我が国においては、安全保障に係る情報についての定義付けの明確なルールが定められていない[39]ために、①省庁縦割りごとにバラバラに定義付けられ、同じ重要度の情報が省庁間で取扱いが異なるといった事態が生じうる、②政府情報の原則公開という社会の要請に反し、秘密化される重要情報が増産されうる、③特に秘密管理することが必要となる重要情報にアクセスする者の適格性の確認が行えない、といった問題を生じている[40]。

したがって、我が国においても、既に導入されている政府統一基準に加え、政府において特に秘密管理することが必要となる重要情報の区分や取扱方法をルール化することで重要情報管理の確実性を高めるとともに、これらを扱う職員の適格性の確認を行う制度を導入すべきである[41]。また、こうした重要情報管理区分のルールには、過剰に情報が秘密化されていないか、重要情報が適切に区分されているか等について不断の見直しがなされるようなレビューシステムを併せて導入すべきである。

（参考）国家安全保障情報区分の概要（Classified National Security Information : Executive Order 13292）

国家安全保障情報（National Security Information）の統一的な機密区分（Classifying）、保全（Safeguarding）、機密区分解除（Declassifying）を行うために発せられた米大統領令（13292）である。機密区分を適格に行うことで、国家安全上において極めて重要な情報の確実な保護を行う。

機密区分すべき情報

機密区分すべき情報は、以下の内容を全て満たすものである。

① 米国政府に所有・作成され管理されている情報
② 機密区分する情報分野に該当する情報
③ 許可なく公開することによって国家安全を害することが容易に想定できる情報

機密区分レベル

機密区分は以下のいずれかに区分される。

TOP SECRET : 国家安全に「非常に重大なダメージ」を及ぼす可能性のある情報

な区分ルールで、重要度（Top Secret, Secret, Confidential）、カテゴリ（軍事情報、外国政府情報、諜報活動、外交情報、国家安全保障に係る科学技術・経済情報等）、識別・表示、区分の見直し、その他の区分ルールを定めている。

39 『政府機関の情報セキュリティ対策のための統一基準（政府機関統一基準）』において、政府情報の管理の際の情報の格付けの区分基準は導入されているものの、どのような分野の安全保障情報について区分するかの判断は情報所有者に委ねられているために、上に記したような問題を生じている。適切に保全されるべき安全保障情報には、防衛省や警察庁関連のみならず、国土インフラや公衆衛生等に関する情報等を含めるべきであるとの指摘もなされている。

40 政府と独立行政法人や企業等との間で情報共有をする際にも、定義や情報の重要度の取扱基準がバラバラになることがある。

41 この点、『カウンターインテリジェンス機能の強化に関する基本方針』（2007 年８月）においても、「特別に秘匿すべき情報（特別管理秘密）」について、物的管理及び人的管理の必要性に関し方針が示されている。

SECRET　　：　国家安全に「重大なダメージ」を及ぼす可能性のある情報
CONFIDENTIAL　：　国家安全に「ダメージ」を及ぼす可能性のある情報

機密区分する情報分野

- 軍事計画、武器システム又はその運用
- 海外政府情報
- 諜報活動、諜報源・諜報方法又は暗号
- 米国の外交関係及び外交活動
- 国家安全に関する科学的、技術的又は経済的事項（国際テロ対策含む）
- 核物質若しくは設備の保護のための米国政府プログラム
- 国家安全に関係するシステムの脆弱性又は性能、施設、インフラ、プロジェクト、計画、防衛活動（国際テロ対策含む）
- 大量破壊兵器

機密区分解除のルール

機密区分解除は、以下の３つのルールによる。

① 区分期間 10 年を迎えた場合の自動区分解除（延長は最大 25 年まで）
② 25 年以上経過した区分解除レビュー（適用除外有）
③ 外部からの開示請求等に伴う強制解除レビュー

マーキング

機密区分をしたときに以下の内容をマーキングする。

① 機密区分レベル
② 区分者の名称や役職
③ 所属部署
④ 機密区分解除の期日
⑤ 情報分野に対応した分類の簡単な説明

（参考）米国国立公文書記録管理局(NARA)の役割

米国国立公文書記録管理局（The U.S. National Archives and Records Administration（NARA））は、政府情報の適切な管理及び歴史的価値のある記録等の収集及び保管を行っており、それらの情報及び記録等について、検索、利用及び学習ができるようにすることで、民主主義への貢献、市民教育の促進及び過去の歴史的出来事の理解の促進を図っている。

また、米国国立公文書記録管理局に属する情報保全監督部（Information Security Oversight Office（ISOO））は、政府情報の国家安全保障情報区分（Classified National Security Information : Executive Order 13292）の運用等について監視を行っている。

このように、米国においては、国立公文書記録管理局の権限によって政府の機密情報の適切な管理（区分、マーキング、区分見直し等）を監督することで、第三者的な立場から、秘密情報が過剰に作成されることを抑制するチェック機能を果たしている[42]。

[42] 我が国においても、各府省の具体的な運用レベルが区々である等公文書管理体制が不十分であり、そうした不適切な管理は国に対する信頼を失わせるものであることからその再発防止が不可欠との認識に立ち、「公文書管理の在り方等に関する有識者会議」において新たな公文書管理システムの構築について議論されてきた。中間報告（平成 20 年 7 月 1 日）においては、国の機関における公文書の作成から利用までのライフサイクルを通じた新たな文書管理法制の確立、国立公文書館制度の拡充等について提言がなされている。こうした取組は、政府統一の重要情報管理にも資するものと思われる。

（2）機微技術リスト・ガイドラインの作成

軍事転用可能ないわゆるデュアル・ユース技術は、その潜在的危険度の特定が難しいことから、硬直的になりがちな法制度によって対処することは必ずしも適切でない。

こうしたデュアル・ユース技術の意図せざる流出に対する規律のため、米国国防省は軍事機微技術リスト(MCTL)[43]を発出している。このリストは、軍事転用可能な技術を保有する者が当該技術を移転・公表等する場合における危険度の判定基準として利用することが期待されている。

こうした参照リストによる手法は、必ずしも硬直的な法制度によって対処することが適切でないデュアル・ユース技術の緩やかな規制として有効であり、経済活動の抑制を回避し、企業の自主的な安全保障への取組を促進しつつ、新たに脅威となりうる民生技術の拡散防止に役立つものである。我が国においてもこのような参照リストを整備することを検討すべきである。なお、こうした機微技術リストは技術の進歩とともに変化・陳腐化するものであることから、米国では将来の科学技術開発リスト(DSTL)[44]を有している。

これら機微技術リストの作成に際し、米国では国防省が中心となり莫大な資源を投入して、企業ヒアリング、各種文献の精査等を通じてあらゆる技術情報等を調査し、最新の技術動向の把握に努めているという。

加えて、個々の技術だけであれば、格段、懸念すべきデュアル・ユース性が見受けられないような場合でも、それらを組み合わせることで深刻なデュアル・ユース性が生じることもあるため、このような機微技術の特定の困難さを考慮する必要もある。

技術大国である日本発の機微技術の多様性にかんがみ、我が国においても、機微技術の管理の観点から、このような技術動向の把握に取り組むとともに、関係省庁の連携により、独自にリスト又はガイドライン等を整備することを検討すべきである[45]。

（参考）軍事重要技術リスト（MCTL）、科学技術開発リスト（DSTL）の概要

米国国防総省（DOD）は技術動向の把握等のため、軍事重要技術リスト（MCTL）及び科学技術開発リスト（DSTL）を作成している。

---

[43] MCTL (Militarily Critical Technologies List)：貿易管理リストとは異なり、企業等が行おうとする技術移転や学術文献の発出に際し危険度を参照するためのリスト。

[44] DSTL (Developing Science and Technologies List)：まだ評価の定まっていない開発中の技術であるが国防省の関心領域にあるものについて幅広く包含した技術リスト。将来の国防技術の開発の基礎として利用されるものだが、将来の重要技術リストであるが故に、情報保全の対象となる蓋然性が高いものでもある。

[45] 我が国においては、将来の社会を見据えた産学官の研究開発の共有シナリオたる「技術戦略マップ（経済産業省）」や、「科学技術の中長期発展に係る俯瞰的予測調査（科学技術政策研究所：文部科学省）」等、世界にも類を見ない網羅的かつ詳細な科学技術調査のストックを有していることから、こうした情報をベースとして関係省庁が連携の下デュアル・ユース性の観点から判定を行うことで、機微技術に関するリストを作成する等の手法が考えられる。

MCTL（Militarily Critical Technologies List）

MCTL は、現在存在する製品及び技術であって、開発、生産、防衛利用において敵対者のポテンシャルを大きく進歩させる可能性があると国防総省が認識したものを示している。

MCTL は輸出管理リストではなく、技術移転及び技術レポート・科学論文を公表する際の危険評価の参考として使われる。

DSTL（Development Science & Technologies List）

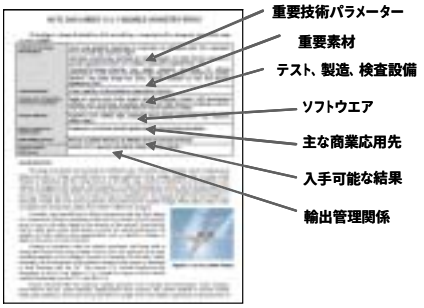
世界中で行われている科学技術の開発動向であって、将来、米国の軍事力を大幅に向上する可能性があるもの、若しくは米国の軍事力を低下させる可能性のあるものを示している。

DSTL はまだ評価の定まっていない開発中の技術であるが国防省の関心領域にあるものについて幅広く包含している。将来の国防技術の開発の基礎として利用されるものだが、将来の重要技術リストであるが故に、情報保全の対象となる蓋然性が高いものでもある。

MCTL、DSTL に共通の 20 技術分野

航空技術、武器及びエネルギー素材技術、
生物技術、生物医学技術、化学技術、
ビームシステム技術、エレクトロニクス技術、
エネルギーシステム技術、陸上システム技術、
情報セキュリティ技術、情報システム技術、
レーザー・光学及びイメージング技術、
製法及び製造技術、海洋システム技術、
資材及び加工技術、核兵器システム技術、
位置・ナビゲーション及び時間技術、
シグナチャーコントロール技術、
宇宙システム技術、武器システム技術

＜MCTL データシート例＞



（参考）デュアル・ユース研究に対処するガイドラインの例

ライフサイエンス研究から得られる情報は人間の生命の機能を理解する非常に重要な役割を持つとともに、その誤用は人間や地球環境にとって破滅的な損害をもたらしかねない。こうした「デュアル・ユース研究」の成果である新技術がどのようなポテンシャルを有するかを評価するため、アカデミア及び政府安全保障関係者から構成される NSABB（National Science Advisory Board for Biosecurity）が設立され、政府に対して適切な対応策について助言することとしている。

NSABB は、“Proposed Framework for the Oversight of Dual Use Life Sciences Research”において、デュアル・ユース研究の監視システムの７つの視点（①ガイドライン、②アウェアネス、③教育、④現場における研究の評価とレビュー、⑤リスクアセスメントとリスクマネジメント、⑥定期的評価、⑦ルール遵守）を提言している。このうち、ガイドラインについては、少なくとも以下の項目を含むべきと

している。

○　目的と適用範囲
○　定義
○　対象となる研究（デュアル・ユース研究の特定基準、基準適用の際に考慮すべき点）
○　研究レビューの方法（リスクアセスメントにおいて考慮すべき点、リスクマネジメントの方法）
○　ライフサイエンス研究に従事する研究者の役割と責任
○　現場レベル・連邦レベルにおける問題対処の基準
○　連邦レベルにおけるデュアル・ユース研究への対処の方法と手順
○　ガイドラインの遵守と不履行時の罰則

また、ガイドラインは、関係者のみならず一般市民にも明確で分かり易いものであるとともに、技術の進歩に併せて適宜見直されるべきであるとしている。

出所：NSABB [2007] “Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information”

（3）秘密保護法制の在り方

米国においては、国家安全保障の観点から、防衛情報、諜報活動情報、米国の安全に影響を及ぼす情報等の安全保障情報について、国を侵害し、外国を利することを意図した収集等の行為に対する罰則が科されている。

一方、我が国においては、安全保障に係る政府情報のうち、防衛秘密、特別防衛秘密、原子力施設の防護に関する秘密等の漏洩行為に対して罰則が科されているものの、秘密の対象、行為主体、対象行為は非常に限定的であるとともに、個別法によって処罰の差異が大きく、その抑止力は十分でない等の問題がある。

こうした不十分な秘密保護法制は、累次の政府からの情報漏洩事件を招き、結果として、安全保障上の問題、対外的な信用の低下等の大きな弊害をもたらしているとの指摘も数多い。

漏洩することにより国家の安全保障上重大な問題が発生する可能性のある情報については、秘密化の義務と不法な漏示に対する適切な規律を設けるべきである[46][47]。

---

46 一連の「官邸における情報機能の強化」の議論においては、官邸における情報機能の強化を政府部内で検討することを目的として、2006 年 12 月に情報機能強化検討会議（議長：内閣官房長官）が設置され、以降、『官邸における情報機能の強化の基本的な考え方』（2007 年２月）、『官邸における情報機能の強化の方針』（2008 年２月）がとりまとめられたところ。WG において、情報の集約・共有及び基盤整備の前提としての政府統一基準の策定のほか、秘密保護法制の検討として、諸外国の現状、真にふさわしいあり方の研究を継続中。

47 2000 年のいわゆる「アーミテージ報告」においても、日米間における情報共有関係の強化のため、「日本の指導者たちは、機密情報を保護する法律の立法化にも向け、国民の支持と政治的指示を得なければならない」としている（米国防大学国家戦略研究所 [2000]『米国と日本：成熟したパートナーシップに向けて』（通称：アーミテージ報告）2000 年 10 月）。

図表３．米国の秘密保護法制の概要

	秘密の対象	根拠	対象者	対象行為	罰則
防衛情報	防衛情報（国家防衛に係る船舶、航空機、防衛活動等、又は危機的状況時に重要となる場所等の文書、地図、写真、モデル等）	18 U.S.C. §793 Gathering, transmitting or losing defense information	一般国民も対象	合衆国を侵害し、又は外国を利することを意図した収集、移転、紛失	10年以下の懲役、罰金又は併科
		18 U.S.C. §794 Gathering or delivering defense information to aid foreign government	一般国民も対象	外国政府、外国の政党、軍、公務員、市民等に対する通報、引渡し、移転	死刑、無期・有期懲役（結果的に米国エージェントの死につながった場合又は直接的に原子力爆弾や特に機微な情報であった場合は死刑となる。また、軍人であった場合はArticle106aに従い死刑となる。）
防衛施設関連情報	国防施設及び設備の写真、スケッチ等	18 U.S.C. §795 Photographing and sketching defense installations 18 U.S.C. §797 Publication and sale of photographs of defense installations	一般国民も対象	国防施設及び設備の写真、スケッチ等の作成、公表、販売、譲渡	１年以下の懲役、罰金又は併科
諜報・暗号情報	Classified Information（コード、暗号、暗号システム、通信傍受に関する情報）	18 U.S.C. §798 Disclosure of classified information	一般国民も対象	故意の公開、伝達、提供	10年以下の懲役、罰金又は併科
政府財産	政府の財産、記録等	18 U.S.C. §641 Public money, Property or records	一般国民も対象	個人利用又は他の利用のための横領、窃盗、転用	10年以下の懲役、罰金又は併科（財産の価値が$1,000を超えない場合は、１年以下の懲役、罰金又は併科）
外交情報	公式外交コード又はコードのために用意された資料、外国政府と交わした通信で入手した資料	18 U.S.C. §952 Diplomatic codes and correspondence	米国の従業員	許可なしの故意の公開又は他人への提供	10年以下の懲役、罰金又は併科
政府情報	Classified Information（大統領令又は法令の要求に準拠した情報）	18 U.S.C. §1030 Fraud and related activity in connection with computers	一般国民も対象	合衆国を侵害し、又は外国を利することを目的とした不正アクセス	10年以下の懲役、罰金又は併科 再度罪を犯した場合は20年以下の懲役
政府情報	Classified Information（大統領令又は法令の要求に準拠した情報）	18 U.S.C. §1924 Unauthorized removal and retention of classified documents or material	米国の公務員、従業員、契約者、コンサルタント等	許可なしのClassified Informationの持ち出し及び許可されていない場所での保持	１年以下の懲役、$1,000以下の罰金又は併科

原子力関係情報	原子力エネルギー法に定義される制限されたデータ（原子力兵器、核物質、原子力発電に関する全てのデータ）	42 U.S.C. §2274 Communication of Restricted Data	一般国民も対象	①米国に危害を与えること又は外国を利することを目的とした開示、②米国に危害を与えることに使われることに対しての開示	①に対して無期・有期懲役、$100,000 以下の罰金又は併科 ②に対して、10 年以下の懲役、$50,000 以下の罰金又は併科
秘密エージェントに係る情報	秘密エージェントの正体に関する情報	50 U.S.C. §421 Protection of identities of certain United States undercover intelligence officers, agents, informants, and sources	秘密エージェントの正体についての情報へのアクセスを有する者又は有していた者	秘密エージェントの正体を知る者が、秘密エージェントの正体を機密区分情報の受領許可のない人等へ公開すること	10 年以下の懲役、罰金又は併科
			機密区分情報へのアクセス権を有する者	機密区分情報への正当アクセスを通じて秘密エージェントの正体を知り、機密区分情報の受領許可がない人等へ公開すること	５年以下の懲役、罰金又は併科
			一般国民も対象	行動パターンにより秘密エージェントの正体及び存在を知り、機密情報の受領許可がない人等へ公開すること	３年以下の懲役、罰金又は併科
政府情報	Classified Information（米国の安全に影響を及ぼす情報）	50 U.S.C. §783 Offenses	米国の公務員、従業員	外国政府のエージェント又は代理人へ Classified Information を提供すること	10 年以下の懲役、$10,000 以下の罰金又は併科、事務所保有の禁止、直接的及び間接的に違法となる全ての権利及び違法を助長する権利の没収
秘密特許	秘密発明法に従った秘密保持命令に基づく特許	35 U.S.C. §181 Secrecy of certain inventions and withholding of patent 35 U.S.C. §186 Penalty	一般国民も対象	秘密発明法の秘密保持命令に基づく発明及び情報の故意の出版又は公開の許可、外国への出願	２年以下の懲役、$10,000 の罰金又は併科

図表４．我が国の秘密保護法制の概要

	秘密の対象	根拠	対象者	対象行為	罰則
公務員法等に規定する秘密	職務上知ることのできた秘密	国家公務員法第 100 条第１項、外務公務員法第４条第１項、自衛隊法第 59 条第１項、地方公務員法第 34 条第１項	一般職の公務員（自衛官や大使等含む）【国務大臣、副大臣、大臣政務官等の特別職の国家公務員は含まれない】	漏えい行為【企て、教唆、幇助行為も規定。ただし、漏えい未遂・過失犯、探知・収集行為は規定せず。】	１年以下の懲役又は 50 万円以下の罰金等
防衛秘密	自衛隊法別表第四に掲げる事項（運用計画、電波情報・画像情報、武器・弾薬・航空機等の種類又は数量、暗号、性能情報等）	自衛隊法第 96 条の２第１項	防衛秘密を取り扱うことを業務とする者（防衛省職員、公務員、防衛省との契約事業者）	漏えい行為【共謀、教唆、煽動行為、漏えいの未遂・過失犯も規定。ただし、探知・収集行為は規定せず】	５年以下の懲役（漏えいの正犯）
特別防衛秘密	MDA 協定等に基づき、米国政府から供与された装備品等に関する情報及びその情報に係る文書、図画又は物件等	日米相互防衛援助協定等に伴う秘密保護法第１条第３項	一般国民も対象	漏えい行為【陰謀、教唆、煽動行為、漏えいの未遂、過失犯、探知・収集行為も規定】	10 年以下の懲役（不当目的探知収集行為・業務者の漏えい等）
特定核燃料物質の防護に関する秘密	特定核燃料物質の防護に関する秘密（脅威情報、設備情報、連絡・体制情報、緊急時対応計画、貯蔵施設情報、運搬情報等）	核原料物質、核燃料物質及び原子炉の規制に関する法律第 68 条の３	原子力事業者及び従業員並びに従業員であった者、国等から委託を受けて特定核燃料物質の防護に関する業務を行う者	漏えい行為	１年以下の懲役若しくは百万円以下の罰金、又は併科

（４）秘密特許制度の検討

諸外国においては、秘密保護法制の一環として、安全保障上の機微技術について国防関連省庁の判断に基づいて出願後公開を行わない、いわゆる「秘密特許制度」が導入されている[48]。その趣旨は、安全保障上の機微技術の「秘密保護」と、特許制度の全件公開主義による「発明の奨励」という、相反する二つの利益を調和させるものである。すなわち、秘密保護制度の下で特許出願が禁じられることになるが、この出願禁止による不利益を解消するため、特許制度上、公開を行わないまま出願日を確保し、かつ、出願人の損害に対して国防関連省庁から補償するという、全件公開主義の例外を許容するものである。

[48] 日本を除く OECD 加盟国 29 ヶ国及びその他の主要国の中で秘密特許制度を導入している国は、欧米諸国、中国、インド等 34 ヶ国。

一方、我が国の現行特許制度の下では軍事関連技術、軍事転用可能技術等の機微技術については、特許出願がされた場合にはすべて公開される。

我が国においても、秘密保護法制の一環として秘密特許制度の導入を検討すべきではないか。

この場合において、対象技術の実施を禁止することが経済活動に与える影響や、特許制度の全件公開主義の例外を設けることが企業の創造的活動に与える影響[49]について、検討する必要がある。

（参考）米国の秘密特許制度の概要

米国特許法に基づき、出願公開による公表・開示が国防関連機関（国防総省、原子力委員会等）の長によって国家の安全にとって有害と判断された特許出願について、米国特許商標庁（USPTO）長官は、秘密保持（公表禁止）命令を発することができる。これにより国家安全上の重要な情報の秘密保護と、特許の公開原則との調整を図っている。

禁止行為と罰則

秘密保持命令が発せられた場合、出願人は、許可なく発明を開示・ライセンス・外国出願することができない。命令に違反した場合は、１万ドル以下の罰金又は２年以下の懲役（又はその併科）。

秘密保持命令の期間と補償

秘密保持命令は、１年ごとに見直され、必要に応じ更新される。出願人は、秘密保持命令と政府による当該発明の利用によって生じた損害について、秘密保持命令を実質的に判断した国防関連機関に対して補償金請求権を有する。

第１国出願義務と外国出願の禁止

秘密特許制度を担保するため、米国でなされた発明は、USPTO 長官の許可がある場合を除き、米国に第一国出願しなければならず、また出願後６ヶ月は外国出願をすることは禁止される。

他国の状況

米国以外にも、英国・ドイツ・フランス等の欧米諸国、中国、インド等が同様の秘密特許制度を有している。

（５）外為法の技術取引規制の強化

情報技術の進歩やグローバル化に伴う人・モノの流動化によって、外為法で規制している安全保障上の機微技術について、新しい規制の在り方が求められている。

具体的には、現行制度が対象としている「居住者・非居住者」間の規制では捉えることのできない外国籍居住者による安全保障上の機微技術の国外への持ち出し等についても、新たに「ボーダー規制」として捕捉する手法について検討すべきである[50]。

---

[49] 特許の出願公開は、社会的な重複投資を防ぎ、社会の技術水準の向上させることで、更なる発明を奨励するためのものであるとされている。

[50] 外為法の運用については、関係機関の連携が不可欠である。例えば、米国商務省 BIS (Bureau of Industry

また、安全保障上の機微技術が懸念者によって取得された場合には、回復が困難になることにかんがみ、安全保障上特に機微な技術の保有者に対する内部管理の義務付けについて検討するべきである。

加えて、大量破壊兵器の開発等に転用可能な貨物の不正輸出等、日本及び世界の安全保障上ゆるがせにできない外為法違反事案が増加していることにかんがみ、貨物・技術双方の罰則強化について検討すべきである。

（参考）米国の「みなし輸出（Deemed Export）」規制の概要

米国の輸出管理規則（EAR：Export Administration Regulations）では、米国産の技術やソース・コード（ソフトウェア）を米国内で外国人に技術を開示することを輸出とみなし、EAR の規制対象としている。

技術の開示の定義

① 視察による開示
② 口頭による開示
③ 米国で修得した知識や技術経験を海外で活用すること

対象者

以下に該当しない外国人
① 米国市民権を得た外国人
② 永住権（グリーンカード）を得た外国人
③ 8 U.S.C §1324b（a）（３）に基づく「保護を受ける人（難民等）」

対象技術

EAR の規制対象となる米国産技術（ただし、以下のものを除く）
① 公開情報（何らかの形態によって公になったもの）
② 基礎研究情報（科学コミュニティで発表及び共有される基礎及び応用科学技術の研究成果）
③ 教育上の情報（大学等の研究室で使用される教育文書）
④ 特許出願情報（全て外国起源の技術データで構成される米国特許出願に関するもの）

（参考）米国輸出管理規則（EAR）とは
EAR とは、国家安全保障、外交政策の推進等を目的とした制度。（１）特定の国に対する輸出の原則禁止、（２）特定の品目の原則輸出禁止、（３）特定の最終用途（end-use）又は最終使用者（end-user）への輸出禁止を柱としており、米国から兵器以外の兵器の開発に利用可能な貨物・ソフトウェア・技術（デュアル・ユース）を海外へ輸出する際に許可を得ることを義務付けている。
日本の外為法に該当する制度であるが、再輸出（輸出先から第３国への輸出）規制、みなし輸出規制の部分について、日本よりも規制範囲が広い。

and Security) 主催の Update 2007 Conference on Export Controls and Policy 等においては、政府当局者(BIS)による輸出管理規制動向の解説に加えて、FBI から米国内における外国籍研究者による経済スパイ活動の現状について、経済スパイ法（The Economic Espionage Act of 1996）の解説や摘発事例の紹介とともに注意喚起がなされている。

（6）投資を通じた安全保障上重要な技術の海外への流出防止

自由な投資活動の結果として、我が国の国益としての安全が阻害され、企業買収により安全保障上の機微技術が海外に流出することがあってはならない。

昨年、安全保障上の機微技術が海外に流出することを防止する観点から、外為法の外資規制の対象に、軍事転用の蓋然性が大きい先端素材や工作機械、電子部品等の製造業を追加する等の抜本的な改正が行われた。今後とも、OECD ガイドラインに則して、引き続き外為法の規制により対応することとすべきである。

（7）不審アクセス情報の報告と注意喚起の仕組み

外部からの情報への不審アクセスに対する警戒度を上げることは、そうしたアクセスに対する効果的な防御となる。

米国では、フィードバック・ウォーニング（不審情報報告）制度[51]が運用されており、どのような分野の技術情報に、どの国・地域からのアクセスがあったかといった報告が、機微情報を保有する防衛関連企業に提供されている。

情報流出への懸念が高まる中で、現実にどのような脅威が存在するかの注意喚起及び予防策の提供のため、我が国においても同様の不審情報報告制度について検討すべきである。

（参考）米国防衛関連企業に対する技術収集動向（Technology Collection Trends）

国家産業保全プログラム運用マニュアル（NISPOM）の通則に従い、米国施設保全適格証明書を有する防衛関連企業からの「外国からの接触及び収集企図の明確化及び報告」に基づいて、国防保全局（DSS）によって報告書が作成されている。外国からの不審な技術情報収集動向について明らかにし、米国防衛関連企業の注意喚起及び対処方針等を提示することにより、保全の促進を行っている。

報告内容例

（不審接触報告の動向）

2005 年は 971 件の不審報告があり、前年に比べて約 40%増加している。

（不審活動国の動向）

不審接触報告に基づき、106 カ国を明らかにした（具体的国名は報告書では明らかにされていない）。トップ 10 の国々で全不審活動の 79.9%を占めており、トップ５の国々で全不審活動の 57.4%を占める。不審活動の国名は明らかにされていないものの、地域としては東アジア及び中近東からの不審接触が多いと報告されている。

（最も頻繁に報告された技術標的）

2005 年において、最も頻繁に外国の関心があったとして報告された技術は「情報システム技術（21.8%）」、「レーザー、光学及びイメージング技術（10.7%）」「航空技術（9.7%」等であった。

（最も頻繁に報告された情報収集手法）

2005 年において、最も頻繁に使われた情報収集手法は、「情報提供依頼（34.2%）」、「技術の取得・購入等（32.2%）」、「マーケティング・サービスの要請（9.6%）」等である。

[51] 米国 DSS（国防保全局）が、防衛関連企業に対する不審な情報収集活動の報告義務を課し、これら報告を分析・評価して企業に公開することにより、そうした脅威に対する注意喚起を行うもの。

付録として提示されている企業が注意すべき指標と対策

（指標例１）

・依頼者は、公式の政府機関の代表であると主張しているが、正当な依頼チャネルの利用を避けている。

（対策例１）

・依頼者はいかなる組織を代表するのか、及び情報依頼要請の理由は何かを訊ねる。

（指標例２）

・全ての費用が相手持ちとなっている外国での講義招待を受ける。

（対策例２）

・参加者に対し、脅威についてブリーフィングを実施するとともに、情報漏えいリスク軽減策について話し合う。

・ 旅行準備に際しては、真に必要な開示可能情報だけに制限する。

（参考）外国の経済情報収集・産業スパイ活動に関する年次報告書(Annual Report to Congress on Foreign Economic Collection and Industrial Espionage)

外国の経済情報収集・産業スパイ活動に関する年次報告書は、1995 年度情報活動権限法第 809 条（b）項に基づき、国家防諜責任者室（ONCIX）によってとりまとめられた外国による経済情報収集及び産業スパイ活動の網羅的なレポートである。

このレポートは、カウンター・インテリジェンス・コミュニティの協力の下に作成され、毎年議会に報告される。

報告内容例

（外国の収集活動の動向）

2005 年は 108 カ国が収集活動を行ったとしている。

（米国技術及びトレードシークレットの持ち出しに対する摘発の動向）

FBI は、この 1 年に 89 件の経済スパイ事件を摘発し、122 件は係争中となっている。入国管理局及び税関において、輸出管理規則違反等について 2400 件の調査を行い、101 件の逮捕、70 件の刑事告発、85 件の有罪判決という結果となっている。

（グローバル化が機微技術へのアクセスを可能に）

2004 年は 3000 万人が一時滞在ビザで入国している。ほんの数パーセントが米国のトレードシークレットを盗み、外国政府が関係していると疑っている。米国技術を盗んで捕まった大部分は、彼らの母国が非常に望む情報にアクセス権を持っていたように思われる。

（企業買収やサプライチェーンに外国企業が入ることによるリスクの高まり）

光ネットワークプロバイダーである Global Crossing や IBM の PC 事業がシンガポール及び中国の企業に買収されることや、外国企業が重要な IT インフラを提供すること等は、重要技術が海外へ流出リスクが高まり、国家安全に対する脅威も増す可能性がある。

（インターネットが機微技術の入手を容易にしている）

カウンター・インテリジェンス・コミュニティは、インターネットが機微情報を入手する上で非常に有効なツールとなってきているとしている。また、誰もサイバー盗難によってどれくらいの機微情報が取られているかを認識していないだけでなく、インターネットは容易、安価、匿名で機微情報を持ち出すことを可能としている。

（全ての技術が狙われている）

軍事重要技術リスト（MCTL）に記載されている技術は全て狙われている。

委員のコメント（概要）：安全保障の視点

○ 情報の収集とは、些細で断片的な情報をジグソーパズルのように集めていくと、そのうちにくっきりと必要な情報が浮かび上がってくるものである。

○ 秘密保護法を整備して、情報を不正に持ち出したときの罰則を強化していく必要がある。特別防衛秘密の漏洩は最大懲役 10 年、防衛秘密の漏洩は最大懲役５年となっているが、それ以外については、国家公務員法に基づき最大懲役１年となっており、諸外国に比べて罰則が非常に甘い状況にある。

○ 防衛秘密等に関する裁判において、他国では非公開裁判制度が確立されているところ、我が国では全て公開ということは問題ではないか。

○ 政府による情報の秘密区分について、各省庁の縦割りになっているので、どのようなものが重要技術情報なのかというような政府統一の指定をすべきでないか。

○ 特許を取ると広く公開されることになってしまうので、機微技術に関しては、秘密特許制度を導入して、限られた人しか接しないようにすべきではないか。また、秘密特許制度が導入されたとしても、特許として申請されない機微技術や公開を制限した技術の改良技術が制度をすり抜けてしまう可能性があるため、それらの扱いについても検討が必要である。

○ Need to Know の原則、すなわち関係のない人には知らせないという原則を貫くべきではないか。また、特定の技術に関しては、職員採用の際にセキュリティ・クリアランス（身元の確認）等が行われれば、かなりの情報漏洩の抑制につながるのではないか。

○ 我が国では、現場が持っている情報量が非常に多いように思われる。その結果、全体としてのセキュリティの管理が難しい状況になっている。

○ 戦後、我が国にはセキュリティや保全といったことに関してアレルギーのようなものがあり、その結果として、諸外国並みの秘密保護法制が存在していない等の状況になっている。

○ かつては、外交や軍事・防衛といった伝統的な安全保障分野と、民生分野が比較的明確に分類できる状況であったが、現在では情報技術や科学技術の革新により、両分野が融合するようなデュアル・ユース技術、又は汎用技術の領域が著しく拡大している。ほぼ全ての科学技術が何らかのデュアル・ユースの側面が見受けられる状況となっている。

○ 米国が膨大な経済活動等の中で、軍事転用のおそれがある輸出等を指摘できるのは、軍事的なセンスを持っているからだと考えることができる。

○ 研究者自身が「平和研究」と信じて行ってきた様々な研究開発の成果が、他の人々に悪用されてしまう可能性に対する発想が、現在の大学や研究機関ではすっぽり抜け落ちてしまっているのではないかという懸念がある。

○ 技術を兵器転用するケース、悪意のために使用するケース、単なる不注意に起因して事故が発生するケース等、様々なケースに対してどのように対応していくべきなのか、考える必要がある。

○ 「科学には国境がないが、科学者には祖国がある」と言われており、安全保障・科学技術コミュニティに対して大きな課題を投げかけている。極めて対応が困難な問題であるが、無視できない問題でもある。

○ ネズミ痘や天然痘等に関する非常に機微な研究成果にもかかわらず、一般大衆向けの雑誌等で詳しく紹介されてしまうことがある問題や、危険なウイルスの DNA やポロニウム 210 のような放射性物質等がインターネットで手軽に購入できてしまう問題について、まだ世間では深刻な問題としてみなされていないことに懸念がある。

○ 研究情報の流出に対する法的規制が厳しくなることにより、生物兵器テロ対策等のカウンター・メジャーを作り出していく能力をも損ないかねないことが懸念される。また、柔軟性を欠いた法的規制では、日々めまぐるしく進歩する科学技術に効果的に対応することができない。教育プログラム等を通じて、科学者コミュニティ自身が問題意識を持ち、ガバナンス体制の強化を行っていくことが必要である。

○ 守ることばかり考えてしまうと、強固に守ったものの情報が使われないということになりかねないので、情報を利用してより優位性を保つといった観点でもセキュリティを考えないといけない。

第３章　企業における情報管理

１　企業の情報管理の促進について

（ポイント）

【現状と問題点】

（１）技術情報等を秘密として管理することの困難性

- 企業内において秘密管理されたビジネス上のノウハウ、顧客情報、取引先情報等を含む技術情報等は、企業の収益力の源であるにもかかわらず、その価値を容易に把握することができない性質（不可視性）を有するため、これを管理することには大きな困難が伴うという宿命にある。

（２）棚卸し・価値付けの重要性

- 技術情報等を保護する法制をいかに整備しようとも、いかなる技術情報等を秘密管理するかは企業自身が自主的に判断しなければならないところ、我が国企業においては、情報の出生の段階から情報の棚卸し・価値付けを行うシステムが構築されていないと指摘されている。

【具体的検討事項】

- **適切な情報資産管理の促進**
- **官民フォーラムの立ち上げ**
- **技術情報等の適切な法的保護の在り方に関する検討**
- **営業秘密保護のためのガイドラインの見直し**
- **特許公開を通じた我が国の有用な技術情報等の流出への対処**

第１節　現状と問題点

情報化の進展により、今日の企業活動における技術情報等の活用は不可欠なものとなった。共有化されたプラットフォームである「情報インフラ」にアクセスすることで、企業は業務の迅速化・効率化といった面で多大な恩恵を享受している。また、垂直統合型から水平連携型への移行、サプライチェーンの深化により企業間関係は複雑さを増している。こうした情報インフラへの依存による、企業間の相互依存関係の深化の結果として、一企業の事業活動の破綻は、単に一企業の損害にとどまらず、他企業の活動にも甚大な影響を与えることがある[52]。

[52] 2005年6月に発生した米国でのクレジットカード決済代行会社の情報漏洩事故では、状況確認やカードの再発行のために世界中の企業が対応を迫られるという世界的な被害拡大を招いた。その後同社は、

また、技術情報等そのものについて着目すると、企業間の相互依存関係の深化によって、企業の営業秘密として管理された技術情報等を共有することが業務遂行上不可欠であることや、他者の技術情報等との組み合わせによって新しい付加価値を生むようなことが起こっている。こうしたコンソーシアム内における「営業秘密として管理された技術情報等の共通資産化」においては、当該共有化された技術情報等がそうしたコミュニティ外に漏洩することによって競争力を失うことにならないよう、自らの資産を開示する相手方においても適正な技術情報等の管理がなされることが前提となる（またその逆も求められる。）。すなわち、そのコミュニティの参加者は、相互に当該技術情報の秘密管理を厳格に行うという責任を有することになる。

上述のとおり、現在のオープン・イノベーション環境下においては、技術情報等の適正な管理は、自らの競争力の源泉の確保を目的とすることのみならず、他者との関係を意識しながら行うことが求められている。このような現状認識の下、以下において、企業における技術情報等の適正な管理の在り方について議論する。

（1）技術情報等を秘密として管理することの困難性

そもそも「情報」とは、以下の性格を有することを指摘することができる。

第１に、「情報」は、言うまでもなく、企業にとって資産であるということである。企業の保有する技術情報等が企業の収益力の源なのであって、企業の様々な個々の製品・サービスを生み出す総体としての性質（根源性）を有している。更に、情報は、適切な「組合せ」によって、その情報単体で有する価値とは全く異なる新しい価値を創造することができるという性格を有する[53]。特に、冒頭で論じたとおり、近年、サプライチェーンや共同事業体等の企業間での情報の組合せを行う機会が頻繁に発生しているところ、この場面において共有されることとなる情報については、他者情報の預かり保管者として果たすべき管理の責任が生ずることになる。これは、情報がまさしく資産性を有することを受けてのものである[54]。

第２に、そうした「情報」が企業経営にとって重大な資産性を有するにもかかわらず、その価値の可視化が容易ではないということである。したがって、情報の管理が適切になされていない企業において、情報の不用意な流出により企業に損害が生じているという実態は、流出時よりもタイムラグを生じて判明し、場合によっては手遅れということにもなりかねない。

技術情報等の管理の在り方の検討に際しては、こうした「情報」の有する特徴に配慮しながら行うことが必要である。

VISA や American Express 等から契約を打ち切られた。

[53] 加護野[2006] は、組合せの効果は、情報の「自然蓄積性」、「多重利用可能性」及び「結合価値」という特性から発生するものであるとしている（加護野忠男 [2006]「新しい事業システムの設計思想と情報の有効利用」『国民経済雑誌』Vol.192 No.6 神戸大学）。

[54] もっとも、「情報」の中には、十分に価値を見出せないものも存在する。

（２）棚卸し・価値付けの重要性

上で論じたとおり、「情報」はクリティカルな資産性を有しながら、必ずしも可視化できないという特性を踏まえつつ、その管理をいかにして行うかが問題となる。この場合において配意すべきは、不正競争防止法等により、秘密管理された情報は法的に保護されるが、こうした法的保護を受けるためには、その情報が秘密管理されていることが前提であり、どの情報を秘密管理するか否か自体は、当該情報の保有者たる企業が自ら判断しなければならないものである。

したがって、法的救済の前提として、企業において、情報について秘密管理するか否かの決定をする体制をどのように構築するか、重要な情報を保有する企業自身が、そもそも自らの資産のうち何が重要な情報であるのかといった点につき、「気付き」を得るシステムをいかに構築するかが、まず問題となる。

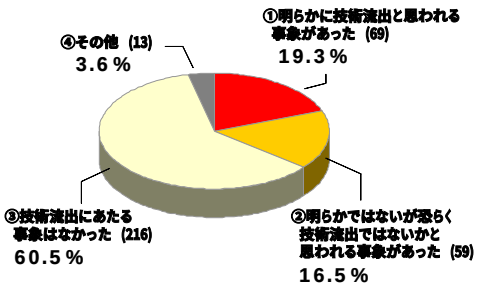
企業における情報の発生の実態を観察すると、重要な情報は、企業の現場の一従業員の企業活動の中で発生することが多い。しかしながら、こうした企業のトップの経営陣から距離がある現場レベルでは、「この情報が企業戦略の中で重要な位置付けを占める」という認識が欠如し、みすみす重要な経営資源としての情報が流出してしまうことがある。また、労働市場の流動化により、中途採用者が持ち込んだ情報が原因となってライバル企業から訴えられる等、情報の混在が懸念されているのも、企業内の情報資産の棚卸しが十分に機能していないことによるものと考えられる。

したがって、技術情報等の出生・生成の段階から情報の棚卸し・価値付けを行うシステムをいかに構築するかが、企業における技術情報等の管理の促進のための重要な要素である。

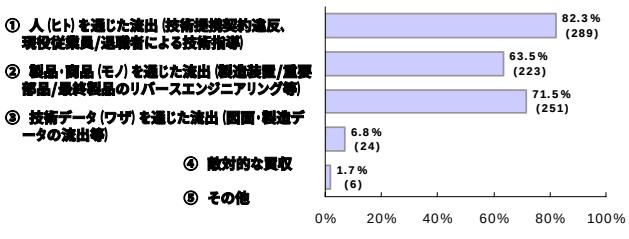
（参考）企業からの技術情報流出の実態について

経済産業省が平成 18 年に行った製造業関係企業に対するアンケート調査（回収企業：357 件）によると、約 35%以上の製造関係企業が過去に技術流出があったと回答している。流出していることに気付いていないケースも含めると、実際には多くの情報流出が発生していると考えられる。

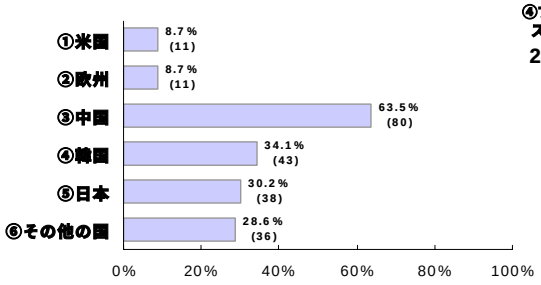
貴社において国内又は海外で
技術流出が発生したことがありますか



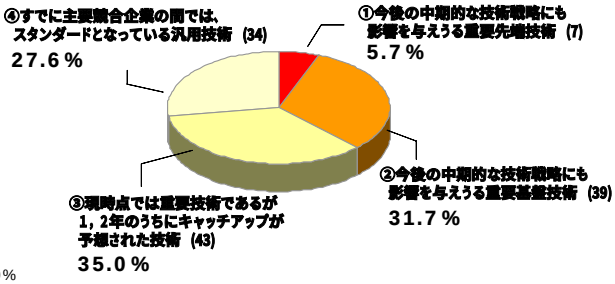
貴社の競争力の源泉の外部への流出に関して
主にどのようなリスクを感じていますか



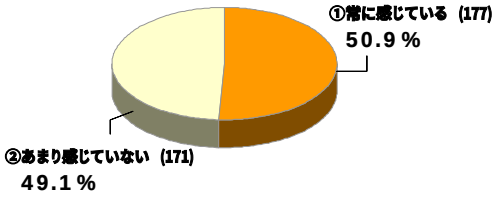
どこで（又はどこへ）技術流出が発生しましたか（発生したと考えられますか）



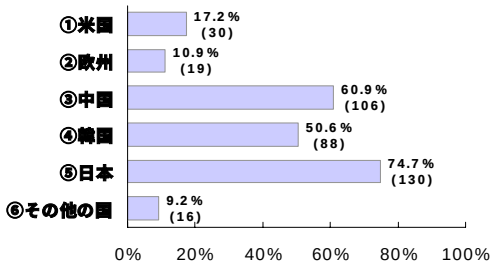
流出した技術はどのような技術ですか



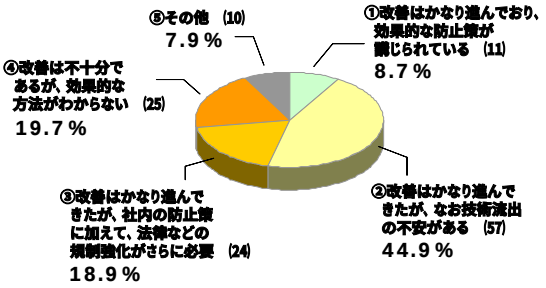
コア人材の引き抜きに脅威を感じていますか



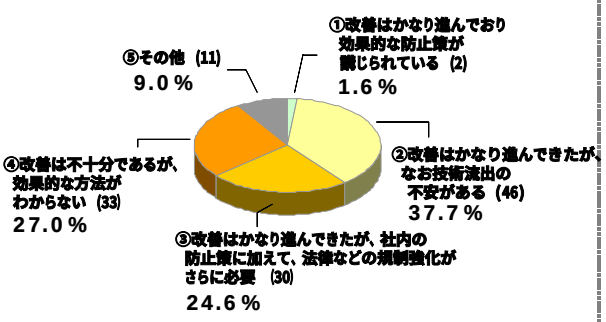
どこの国・地域からの引き抜きに脅威を感じますか



技術流出に対して国内事業所における再発防止策は十分ですか



技術流出に対して海外事業所における再発防止策は十分ですか



出所：経済産業省『我が国製造業における技術流出問題に関する実態調査』（2006 年 12 月）

第２節　具体的対応

（１）適切な情報資産管理の促進

企業内の技術情報等について、何を秘密管理し、何を公開するかの判断に際しては、企業が自ら何が重要な技術情報等であるかという「気付き」を得るシステム、すなわち、技術情報等の格付けを行う体制を整備することが必要である。この場合において、技術情報等の格付けは CIO（Chief Information Officer：最高情報責任者）等が先頭に立ち、経営戦略と技術開発戦略との整合性を考慮しながら、経済的視点及び技術的視点の双方から判断されるとともに、経営者層と対策実施の現場との間で適切に意識共有がなされることが重要である。

リスク管理、コンプライアンスの観点からのいわゆる技術情報等の管理については会社法においても規定されているところであるが[55]、こうした企業内の技術情報等の活用の視点から技術情報等の格付けの体制について、会社法が定める内部統制の機能と一体に運営されるべきものであると考えられる。例えば CIO の職務執行の管理について監査役による監査の対象とすること等、技術情報等の格付けを促進するために、内部統制ルールの在り方を含めて総合的に検討すべきである。

また、企業において、経営戦略との整合性を考慮しつつ現場と一体となった情報管理を推進するためのガイダンスとして「情報システム・情報セキュリティに係る内部統制ガイダンス」（仮称）[56]の検討を行うとともに、経営戦略に整合的な情報管理の先進的な取組を集めた事例集についても検討すべきである。

さらに、技術情報等を格付けした結果として、技術情報等の価値の重要性が客観的に評価されるような環境が創設されれば、その価値に応じた管理ができるようになるのではないか。すなわち、技術情報等の流通を促進する技術情報等の流通市場の整備等を通じて技術情報等の格付けの動機付けとする方策について検討すべきである。

（２）官民フォーラムの立ち上げ

企業の技術情報等の管理に資するため、米国 OSAC を参考にしつつ、産業界と政府とが一体となったコンソーシアムを形成し、技術情報等の漏洩事案の収集及び企業へのフィードバック、事故情報データベースの構築、企業向け指針の策定等を通じて、一層の技術情報等の管理の促進策について検討すべきである。

---

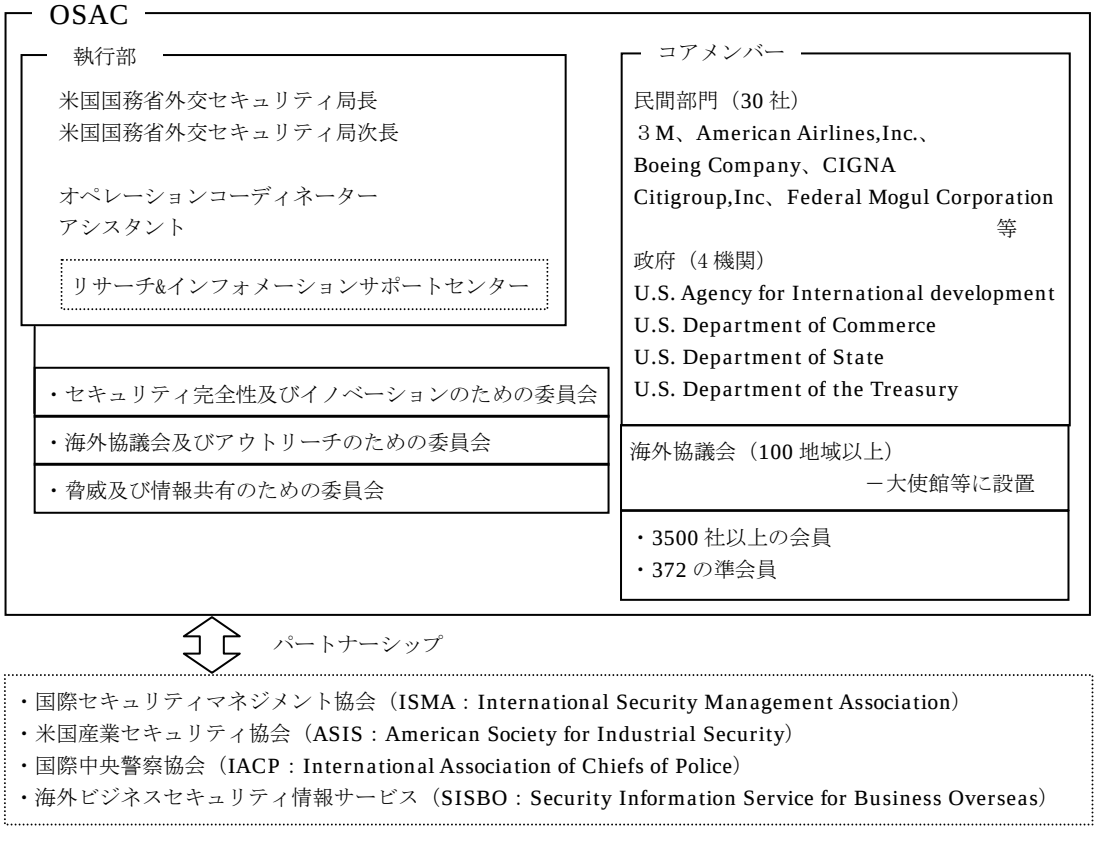
[55] 会社法においては株式会社の業務の適正を確保するため、内部統制システムの確立が義務付けられている。その具体的な体制については同法施行規則において規定されており、重要情報等の漏洩を防止するための体制整備について決定することが求められている（会社法施行規則第 100 条第１項第１号・第２号関係）。

[56] 経済産業省「情報セキュリティガバナンス研究会」において、経営戦略、技術開発戦略に基づく情報管理方針や実施計画の策定方法、法令遵守等の管理策の構築、各管理策の実施状況を経営層に報告するメカニズムの構築等を記述したガイダンスが検討される予定。

（参考）米国海外セキュリティ・アドバイザリー協議会（Overseas Security Advisory Council）の概要

米国は、海外における米国企業のセキュリティ環境を向上させるために、米国民間部門と米国政府からなる海外セキュリティ・アドバイザリー協議会（OSAC：Overseas Security Advisory Council）を設置している。OSAC における民間及び政府の情報交換や議論等を通じて、ガイドラインやレポートを発行し、海外において取り組むべき対策の提示及び脅威のトレンド等を提供している。

OSAC の体制



・国際セキュリティマネジメント協会（ISMA：International Security Management Association）
・米国産業セキュリティ協会（ASIS：American Society for Industrial Security）
・国際中央警察協会（IACP：International Association of Chiefs of Police）
・海外ビジネスセキュリティ情報サービス（SISBO：Security Information Service for Business Overseas）

OSAC 設立の経緯

テロの増加及び絶え間ない海外における米国の国益に対する脅威が続き、1985 年に、著名な米国企業から出向している幹部公務員数名が、セキュリティ問題における米国政府と民間部門の協力を国務長官に促したことから、OSAC が設立された。

OSAC の目標・活動

・米国国務省のセキュリティ機能と民間部門の間の、連携の継続及びセキュリティ協力の提供
・海外のセキュリティ環境を向上させる、民間部門及び米国国務省の通常及びタイムリーな情報交換
・セキュリティ計画のコーディネート及びセキュリティ・プログラムの実行のための手法の推薦及び素材の提供
・世界的な米国の産業競争力の保護に関する手法の提案

OSAC の出版物

（ガイドライン）
- 海外における米国企業情報保護ガイドライン
- 海外における米国企業セキュリティガイドライン
- 海外における米国人ビジネス危機対策ガイドライン
- 米国人ビジネストラベラーのためのセキュリティガイドライン
- 海外におけるセキュリティ完全性　　等

（レポート等（例））
- 経済スパイの情報収集手法
- 電子デバイスのためのサイバーセキュリティ
- 不正入手：全ての事業で知っておくべき従業員の窃盗
- 危機管理ハンドブック　　等

報告窓口の設置

ホームページ上に、セキュリティ事故及び重大な問題の報告窓口が設置されている。

（３）技術情報等の適切な法的保護の在り方に関する検討

企業等が秘密管理する価値ある技術情報等の適切な法的保護の在り方に関する検討を行うべきである。

具体的には、秘密管理された技術情報等の使用・開示は、これを侵害した企業や行為者の自宅等、被害者たる企業の支配の及ばない領域で行われるため、その立証が極めて困難であり、技術情報等の不正な侵害行為に対して十分な抑止機能を有していない等の現状にある。また、秘密管理された技術情報等の性質として、これがいったん開示されるとその価値は永遠に失われ、回復しがたい損害が発生することから、企業の実務の場においては、こうした危険を招来する使用・開示を未然に防止することで、実効的な技術情報等の保護を図ることが求められている。したがって、技術情報等の使用・開示ではなく、不正な領得行為自体を基本的な実行行為として捕捉する体系に改めるとともに、構成要件を明確化・簡素合理化する等、不正競争行為の予防や停止が実効的になされるための措置が検討されるべきである。

加えて、企業秘密の侵害行為の救済を求める刑事裁判では、技術情報等の内容がその手続を通じて公開されることとなり、違法行為を抑止すべき公的手続自体が第２の法益侵害を招来するため、その結果として、違法性・有責性の高い者ほど、刑事手続で処理されないという矛盾を抱えている。技術情報等の実効的な救済がなされるよう、こうした矛盾を改善すべきである。

（参考）不正競争防止法の営業秘密侵害罪について

現行の不正競争防止法における営業秘密侵害罪については、詐欺等行為又は管理侵害行為により不正に取得した営業秘密の「使用又は開示」が処罰の対象行為として規定されているものの、そうした「使用又は開示」行為は、通常、被害企業の管理の及ばない社外で行われることから、その立証は極めて困難であり、十分な抑止力となっていないことが夙に指摘されている。

経済産業省のアンケートによると、35%以上の製造関係企業が技術流出を経験したと回答しているにもかかわらず、こうした法的保護が機能していない現状は憂慮すべき事態。

（4）営業秘密保護のためのガイドラインの見直し

政府が発出する技術情報等の流出防止のためのガイドライン[57]について、より企業の技術情報等の管理の実態に即し、かつ、現場レベルの従業員にも伝わるようなガイドラインへと改正すべきである。また、技術情報等の管理の要求事項・水準は企業規模、業界の特性に応じて異なるものであることにかんがみ[58]、企業規模や業界ごとに最適な秘密管理の基準を定めることを検討すべきである[59]。

（5）特許公開を通じた我が国の有用な技術情報等の流出への対処

世界における特許制度の原則では、すべての特許出願は公開されることとなっており、日本の特許制度も同様の取扱となっている。この点について、我が国企業の有用な技術が海外において無許諾で使用されているのではないかとの指摘がある。この原因として、我が国の企業の中には開発した技術を漫然と日本で特許出願するだけで、海外での権利取得を行っていない企業が少なくなく、その結果、我が国企業の技術情報等が流出しやすい環境を自ら作り上げているともいえる。

したがって、特に特許の出願公開によって、かえって特許取得の予定のない海外においてフリーライドを招くおそれのあるような技術情報等については、特許出願をせずに営業秘密として管理することも重要な知財戦略の一つである。この観点から、各企業において戦略的に技術情報等を管理し、特許を出願すべきか、営業秘密として秘匿化すべきかを判断すべきである。

なお、営業秘密として秘匿化した後に、仮に他者が同一技術について特許権を取得した場合であっても、一定の要件の下で先使用権が認められる。企業が先使用権を活用しよう

---

57 現在、経済産業省『営業秘密管理指針』（2003 年 1 月 30 日）及び『技術流出防止指針』（2003 年 3 月 14 日）が発出されているところ。

58 「第 1 章　競争力の視点」で議論したとおり、知的財産権の保護の範囲についてのジレンマ（スコープのジレンマ）は営業秘密の保護の範囲についても妥当するものであり、厳格な情報管理が要求される産業（バイオ、製薬等）と、緩やかな情報共有によるイノベーションを指向する産業（IT 産業等）では、必然的に情報管理の水準が異なるものと考えられる。

59 経済産業省『平成 19 年度産業情報保全に関する調査研究』におけるアンケート調査によれば、「企業規模別に応じた情報管理の指針を提示して欲しい（56.2%）」、「業界別の情報管理の指針を示して欲しい（45.9%）」という回答が多くあがっている。

とする際の指針として、「先使用権制度ガイドライン」が発出されているところであり、このガイドラインにおいてまとめられている技術情報等の管理手法を参照して、企業が戦略的な技術情報等の管理を行うよう促していくべきである。

２　海外への技術情報等の流出防止

（ポイント）

【現状と問題点】

- 我が国企業の国際展開の拡大に伴い、不可避的に様々な技術情報等の流出リスクにさらされていることへの対応が求められている。
- 我が国企業の海外子会社が有する技術情報等について不正な領得がなされた時に適切な保護がなされない場合には、グローバルにオープン・イノベーションを展開する際の大きな障害となる。

【具体的検討事項】

- **官民フォーラムの立ち上げ**
- **技術移転に伴う技術流出の防止**
- **技術情報等の保護のための国際協力の枠組みの検討**
- **海外アウトソーシング時のリスクチェック手法の検討**

第１節　現状と問題点

グローバル化に伴い、企業の規模を問わず、国際的な合従連衡や新しい市場への進出が一般的になっている。安価な人件費、市場の確保等を目的としたこうした国際的な企業活動によって、国際競争力を確保しようと努めている。

一方で、進出先地域における法制度や外国人従業員の労働慣行の違い等の様々な要素が技術情報等の流出リスクとなっており、適正対価の確保の機会の損失、海外企業の急速なキャッチ・アップの加速化、これらを通じた競争力の低下が懸念されているところである。この点において、我が国企業は当地の欧米企業に比して対応が遅れているとの指摘もなされている[60]。

我が国企業の国際的な活動が、適切に競争力の維持・強化に結びつくために、どのような対応がなされるべきか。

---

60 例えば、欧米企業では、海外に渡航する従業員に対して、渡航前トレーニング及び帰国後ブリーフィングを行い、注意すべき事項の伝達、現地でインテリジェンス活動を受けていないかといった確認がなされている。取引先に関しても、その信頼性に関する入念な調査がなされ、軍事転用や不正取引に巻き込まれないための未然防止の措置が取られている。

第２節　具体的対応

（１）官民フォーラムの立ち上げ

企業の情報管理に資するため、米国 OSAC を参考にしつつ、産業界と政府とが一体となったコンソーシアムを形成し、技術情報等の漏洩事案の収集及び企業へのフィードバック、事故情報データベースの構築、企業向け指針の策定等を通じて、一層の技術情報等の管理の促進策について検討すべきである。

（２）技術移転に伴う技術流出の防止

諸外国への技術移転については、企業の保有する技術情報等の移転の可否の判断は当該企業が行うものであるが、移転先国の事情は様々であることにかんがみ、あくまで我が国企業が長期的に競争力を確保する観点に留意しつつ、移転に伴う意図せざる技術情報等の流出への十分な対応が講ぜられるべきである。このような視点から、「技術流出防止指針」について、最新の取組事例を紹介する等の見直しについて検討すべきである。

（３）技術情報等の保護のための国際協力の枠組みの検討

海外において我が国企業から営業秘密として管理された技術情報等が流出した際に、現地において企業が適切な法的救済を受けるための国際協力の在り方について、各国の法制度・法執行能力に相当程度の差があることも勘案しつつ、検討すべきである[61]。

（４）海外アウトソーシング時のリスクチェック手法の検討

企業のグローバル展開に伴って増大する技術流出リスクに対して、企業が適切な対策を行えるよう、海外アウトソーシング時の技術流出等のリスクに関するチェック手法[62]について検討すべきである。

---

61 例えば、「特許取得手続における APEC 協力イニシアチブ」は、APEC 域内における貿易・投資の円滑化の支援及び同地域経済の発展のため、特許取得手続きの改善のための APEC エコノミー間の協力を増進することを目的としており、各エコノミーのキャパシティ、発展レベル、法制度を考慮しながら適切な手法を選択するボランタリー・ベースの取組である。

62 海外アウトソーシング先になる主な国々の商慣習、宗教文化、治安、社会インフラ、法制度、就労等について日本との違いを分析し、アウトソーシングをする際にどういったところにリスクが存在し、注意をする必要があるのか、どういった対策が必要か等をチェックリスト形式にまとめるものである。

3　中小企業からの技術情報等の流出への対応

（ポイント）

【現状と問題点】

（1）中小企業における不十分な管理による技術情報等の流出

- 中小企業においては、人的・物的制約から、十分な技術情報等の管理体制を構築することができないため、最終製品を製造する企業において、いかに情報管理を厳格に行おうとも、部品等を供給する中小企業から流出してしまうとの指摘がある。

（2）取引先を通じた中小企業の有する技術情報等の流出

- 取引先の企業を通じての意図せざる技術情報等の流出の被害を受けているとの実態もあり、国内での連携を目指さずに、高価でノウハウを買い取ってくれる外国企業に対して売却しようという動きも出始めている。
- 我が国産業の基盤たる中小企業から、このように様々なかたちで技術情報等が流出することは、我が国の競争力の観点から憂慮すべき事態である。

【具体的検討事項】

- **中小企業の管理の実態に沿った営業秘密保護のためのガイドラインの策定**
- **秘密保持契約締結の重要性の周知徹底**
- **中小企業の情報管理支援**
- **取引適正化の取組の推進**
- **情報管理策に関する中小企業向け普及啓発**

第１節　現状と問題点

（1）中小企業における不十分な管理による技術情報等の流出

我が国企業の９割以上を占める中小企業は、最終製品の高度な機能や品質を実現する優れた部品や材料を供給したり、様々な試行錯誤によりイノベーションのシーズを提供したりする我が国産業を支える産業の基盤であり、我が国の競争力を維持・強化する上で不可欠の存在であるところ、中小企業の強みは「精度・品質の保証力」、「コア技術の高さ」、「即応力（スピード）」といった部分にあり、「コスト競争力」、「財務体質」、「リスク管理能力」等については必ずしも十分でない[63]。中小企業からの技術情報等の流出リスクは、このような中小企業の特性に起因するものである。

すなわち、技術情報等の適切な管理に当たっては、相応の知識を備えた人材や適切な管

[63] 経済産業省・厚生労働省・文部科学省 編『ものづくり白書 2007 年版』

理の組織が不可欠であるところ、中小企業の場合には、人材・資金面の不足[64]からそうした専門部署の設置が困難である等[65]、必ずしも技術情報等の管理への対応が十分できないことが多い。また、このような状況から、いかに最終製品を製造する企業において情報管理を厳格に行おうとも、部品等を供給する中小企業から流出することとなってしまうとの指摘がある。

（参考）中小企業ならではの問題点

- ➢ 中小企業は、情報管理を専門に担当する部署や人員を配置できない。専門家によると、300 人以上の規模でないと専門の部署を置くことは事実上難しいのではないかと言われている。
- ➢ 中小企業経営者が情報管理体制を構築しようとしても、従業員に理解されずに取組が進んでいないという状況がある。
- ➢ 発注企業側は、本来求める情報管理体制を妥協して、中小企業に対して発注しているケースがある。

出所：経済産業省知的財産政策室による有識者ヒアリング

（2）取引先を通じた中小企業の有する技術情報等の流出

中小企業が取引を通じて意図せざる技術情報等の流出被害を受けている実態がある。例えば、主に取引先であるところの大企業が、発注者の立場や価格交渉力等の力関係によって、工場見学、納品時における詳細な仕様書の提出等を要求するといったケース等が挙げられる。

（参考）取引先を通じた中小企業の有する技術情報等の流出事例

- ➢ ユーザーが金型の見積りとしていろいろな金型メーカーから金型構造図を集め、最も見積りが安いメーカーへ別のメーカーの図面を使って発注することがある。図面を転用されたメーカーには何も支払われない。
- ➢ 取引上、QC 工程表を作成し、親事業者に見せて承認をもらわなければならず、どういうふうに作っているか親事業者が全て把握している。その結果、親事業者が海外に工場を移転した場合には、そのノウハウに基づいて同じ管理をしてしまう例がある。
- ➢ 取引先の新部品開拓ニーズに対して工法を提案し、ユーザーがノウハウに関するデータを欲しがるので開示すると、特許申請時にはユーザーが既に申請済み、という例がある。
- ➢ 大手企業から、試作品を製品化するよう持ちかけられ、その間、特許出願の方法については後日相談するからそれまでに絶対に公知にしないように言われた。半年経っても連絡が来ないため、確認をしたところ、当該大手企業が独自に特許出願をし、製品化されてしまった。クレームを申し入れたところ、当該大手企業は、従前から当該商品に関する研究開発をしていたと主張して取り合ってもらえなかった。
- ➢ 試作品を大手企業に提供したところ、大手企業から不具合が出たので修理をして欲しいと言わ

[64] 中小企業庁 編『中小企業白書 2007 年版』
[65] 経済産業省『平成 19 年度産業情報保全に関する調査研究』

れたため、修理に応じたところ「対価」の提供があった。後日、当該試作品を勝手に製品化されたためクレームを申し入れたところ、先述の「対価」は、修理代ではなく、ノウハウ代だと言われた。

➢ 秘密保持契約を結び、図面・ノウハウを開示したところ、なぜか当該図面が別のメーカーが保有していることが判明した。明らかに秘密保持契約に違反していると認められたので訴訟提起も検討したが、自らの資産力では損害の立証が十分にできなかった。

出所：経済産業省知的財産政策室による企業ヒアリング
経済産業省『素形材産業取引ガイドライン』（2007 年６月）

こうした経験を踏まえて、中小企業・ベンチャー企業の一部には、国内大企業との事業提携及び事業売却を回避し、ノウハウ等を高く評価してくれる外国企業と事業提携をしたり、外国企業に技術を売却するような動きも出始めている。

（参考）中国企業による我が国中小企業の買収

明治に創業された工作機械メーカーの経営が悪化し、経営破たんの危機に直面していたところ、中国企業が約５億円の出資をして当該企業を買収した。その後は新工場を設立する等、好調な事業を行っている。

出所：新聞報道等

このようなかたちで我が国産業の基盤たる中小企業から技術情報等が流出することは、我が国の競争力の観点から憂慮すべき事態である。

第２節　具体的対応

（１）中小企業の管理の実態に沿った営業秘密保護のためのガイドラインの策定

全ての企業に一律の管理手法を求める営業秘密管理指針については、特に中小企業にとっては過剰な要求であると指摘もなされているところ、中小企業の事業規模に配慮した秘密管理性の要件を定めるべく、ガイドラインの策定を検討すべきである。

（２）秘密保持契約締結の重要性の周知徹底

多くの中小企業は単一事業に特化しており、企業の価値は企業の存立基盤に直結していることから、技術情報等の企業秘密の保護の必要性は極めて高く、企業秘密に関する取引においては、当該秘密の保護の観点から適切な秘密保持契約を締結することが重要である。

しかしながら、未だに取引の現場においては、商慣行として口頭による約束に基づいているケースや、中小企業の能力的問題により不利な契約を交わされてしまうといった問題が生じている。

したがって、まずは金型図面流出防止指針[66]の再徹底等、秘密保持契約の締結の重要性について周知徹底を行うとともに、現場の実務の実際を踏まえつつ、契約書作成支援の在り方について検討すべきである。

（３）中小企業の情報管理支援

中小企業が自ら所有する技術情報等や取引先から受け取った技術情報等の適正な管理を推進するため、情報管理支援策について検討すべきである。

具体的には、中小企業及び取引先が管理策のチェックリストとして活用することができる中小企業向け情報セキュリティ標準フォーマットの作成、知的資産の「見える化」を通じ適正情報管理を促進する知的資産経営報告書の作成支援等が考えられる。

また、国内製造拠点の海外シフトに伴い、海外に進出する中小企業が増加しているが、人材や資金不足によって、技術情報等の流出リスクは高まる一方である。海外進出する中小企業から技術情報等が流出することを防止するために、どのような対策を講じるべきかについて検討すべきである。

（４）取引適正化の取組の推進

取引関係を利用した違法な技術流出を防止するため、下請適正取引ガイドライン[67]等の更なる普及啓発を行い、中小企業に対する商慣行の改善を促していくべきである。

（５）情報管理策に関する中小企業向け普及啓発

業界団体等の協力を得て、情報管理の具体的な方策に関する中小企業向けセミナーを全国各地で開催すべきである。

また、情報管理に対する中小企業の意識向上のための方策について検討すべきである。

---

66 経済産業省『金型図面や金型加工データの意図せざる流出の防止に関する指針』（2002 年７月）

67 経済産業省『素形材産業取引ガイドライン』（2007 年６月）、経済産業省『自動車産業適正取引ガイドライン』（2007 年６月）等が発出されている。

委員のコメント（概要）：企業における情報管理

１．企業の情報管理の促進について

○ 経営陣等が頭でっかちに考えて押し付けているルールや枠組みが、企業の中では全くワークしていないということをできるだけ早く認識していかなければいけない。

○ 技術認定評価機関のような組織が、客観的な技術評価又は認証といったことにより、技術や価値評価の担保をすることが必要かもしれない。

○ 企業の中で情報が生まれてから格付されるまでの間は、全く管理されていないという状況がある。この情報格付される前の漏洩が危惧される。

○ リスク管理の基本は、リスクを定義し、実際に対策を講じることである。同じような事故が継続して起こっていることが多く、未知の脅威に対応するよりは、現在起こっていることを起こらないようにすることが重要である。

○ すべての脆弱性が許せなくて、何でもかんでも塞がなければということになる場合があるが、これはコストの面で見合わない。リスクを定義し、適正な対策を考えていくべき。

○ 情報の内容が多岐にわたり、ボリュームが多く、専門的な知識が必要である場合、相当なレベルまで個々人あるいは個々の部局の自己的な管理に依存せざる得ない状況となることが考えられる。

○ 企業戦略を認識できることと、情報の技術的な評価あるいは社会的な評価を理解できるという要件がないと、客観的な価値評価はできないと考えられる。副社長クラスの人間が CIO として責任を持って取り組むべき。

○ 議論は予防に大きくフォーカスしているが、漏洩した際の早期発見及び実態調査も重要である。企業において脅威を察知して速やかに対処する体制を築くことが重要であるが、国においてもそれらをサポートするような体制作りをもっと考えていくことが必要と感じている。

○ 情報が絶えず生まれている状況の中で、情報が具体化して文書や伝達可能な状態になっていくと、漏洩時の影響も高まっていくと考えることができる。

○ 採用した従業員が他社の情報を自社に持ち込んでしまうリスクに関して、全く関心のない企業がある。法令遵守や世評リスクを考えれば、採用する従業員に対してきっちりとした確認や対応が必要である。

○ 被害者が、自分の営業秘密が使用・開示されたとして告訴状を作成しようとしても、転職先企業等がそれを認めない限り、十分な説明することがほぼ不可能である。また逆に、警察に営業秘密が使用・開示されたことについて訴えがあった場合であっても、証拠等が不十分である場合には令状も出ない。このため、転職企業等に協力者でもいない限りは対応することが大変難しいというのが現状である。

○ 情報というのは多義性のようなものがあり、どこをどう見るかや、見る時点によって価値がかなり変わってくる。このため、情報の価値を社会的にどのようにうまく認識するかということは悩ましい問題である。

○ 企業が研究成果を事業化するためには、相当な資金を投入して知財活動を行うことが必要になるが、万一、成果が流出しており、別の者が特許出願をしていたら、多大な損害を被ることになる。そうした損害が発生するおそれが看過されている状況では、企業はリスクを背負って事業活動できなくなる。

○ 技術流出によって実際に損害を被ることだけでなく、他者による特許取得によって予定されていた事業化ができなくなることも一つの被害ではないか。したがって、不当に事業化が阻まれることがないような制度構築に向けた議論を行う必要があるのではないか。

２．海外における企業からの技術流出の防止

○ 日本企業は取引先企業の事前調査が非常に弱い。海外企業は、契約前に、取引先企業の資本状況、取引関係、過去の実績、懸念される関係の有無等について入念に調査している。

○ 日本企業は、本社から物理的に距離が遠くなると管理レベルが低くなる傾向がある。特に海外においては、管理にかけるコストよりもオペレーションにかけるコストの方が高いケースが多い。

○ 事業所の「縮小・撤退時の漏洩」というものもあり、従業員がごくわずかになった最終的な手続時において、例えばパソコンが通常の管理がなされないケース、図面が放置されているケース等がある。

○ 欧米企業においては Counter Intelligence Training が実施されている。海外出張時の注意事項について、渡航前のトレーニングと帰国後のブリーフィングが行われる。これによりリスク対応能力が高められる。

○ 競合企業等がどのような情報を欲しがるかについては、時代や環境によって刻々と変わってくる。企業が機密ではないと判断した情報であったとしても、競合企業が機密と考えている場合もありうる。

○ 不正に情報を取得した場合に法律に基づいた制裁が科される脅威がなければ、いくら制度を議論してもそれは実効的にならない。また、本当の意味で技術流出防止ができるような支援や育成に対して、もっと国が力を入れるべきだろうと思う。

３．中小企業からの技術流出への対応

○ 中小企業の技術の内容についての判断や技術を持っていたということを証明するために、公正な第三者が技術判定や技術の封印作業を行えると良いのではないか。中小企業がどんどん外へ出て活躍できるような環境を整備していくことが必要である。

○ 中小企業は、訴訟を起こすだけの体力があるかという問題と、実際に証拠収集できるのかという問題がある。そうした中小企業の特徴を踏まえた対応が必要。

○ 特定性や管理性を強めていくのではなく、環境に応じて、ここのものは全部秘密とみなすというような扱いをしてあげることも必要なのではないか。中小企業に限らず、特定性と管理性ばかりを強調しても守れない。

第４章　大学における情報管理

（ポイント）

【現状と問題点】

（１）今日の大学の役割（知のプラットフォームとしての機能）

- 大学は、その研究成果を広く社会に還元すべき存在。すなわち、様々な主体が新たなアイデア・技術情報を獲得することが可能となる知的活動のプラットフォームとして機能することが期待される。
- 大学が知的活動のプラットフォームとして有効に機能するには、不確実性が高く完成度の低い技術情報は慎重なレビューをかけた上、原則として公開していくこととする一方で、プラットフォームへの参加者が提供した技術情報は、一定のルールに基づいて適切に管理していくこととするという舵取りが求められる。
- 大学においても国際競争力強化のため、広く海外から人材を受け入れなければならないという状況では、こうした一定のルール整備の必要性は以前にも増して高い。

（２）大学における情報管理の在り方

- 大学においても、研究されている科学技術の多くに何らかのデュアル・ユース性が確認されうるという前提の下、安全保障面で機微な情報を保有することとなった際の管理体制について対応方針を定めるとともに、こうした情報管理について大学が社会的法的責任を負っていることを前提に、利益相反管理的な手法の導入等を促進していくことが重要。

【具体的検討事項】

- **研究情報の外部公表の可否判断：組織的管理の実践と支援**
- **政府資金で行われた研究成果の公開原則の見直し**
- **外為法の施行支援**
- **ミスコンダクトへの制度的対応：研究者倫理の在り方**
- **アカデミアと安全保障関係者の対話**

第１節　現状と問題点

（１）今日の大学の役割（知のプラットフォームとしての機能）

第１に、大学は、これまでどおり、学術研究を深めることで真理を探求するとともに、その成果を社会に還元し、公益的な役割を担い続けることが求められる。

こうした中では、公共インフラ的な成果は広く社会に還元していくことが求められる一方で、社会的に悪用される可能性のある成果が適切に管理されないときは、大学本来の社会的使命に反することにもなりかねない。

第２に、国立大学の法人化を始めとする一連の大学改革を通じて、新たな役割が期待されている。すなわち、以下に記載するとおり、産業界との連携を果たすべきこと、その中でも特に、知のプラットフォームを提供することが求められている。

前者については、国立大学法人法では、大学の業務として、受託研究又は委託研究を業務として行うこと、研究の成果を普及しその活用を促進すること、大学の技術を移転する機関に対して出資すること等が規定されている[68]。実際、法人化後の国立大学法人においては、民間企業との共同研究や、知的財産の活用が着実に進捗している。

また、後者については、大学が知のプラットフォームとして有効に機能するためには、プラットフォームへの各参加者が提供した情報は、一定のルールに基づいて適切に管理され、各参加者がお互いに信用しあえるという環境を確保する必要がある。

このような今日の社会における大学の役割にかんがみれば、大学においても、ある種企業と同じように、中に留めるべき技術情報等と、広く社会に公表していくべき技術情報等とを適切に選別するといった適切な技術情報等の管理の在り方を模索する必要がある。

①産業との新しい役割分担

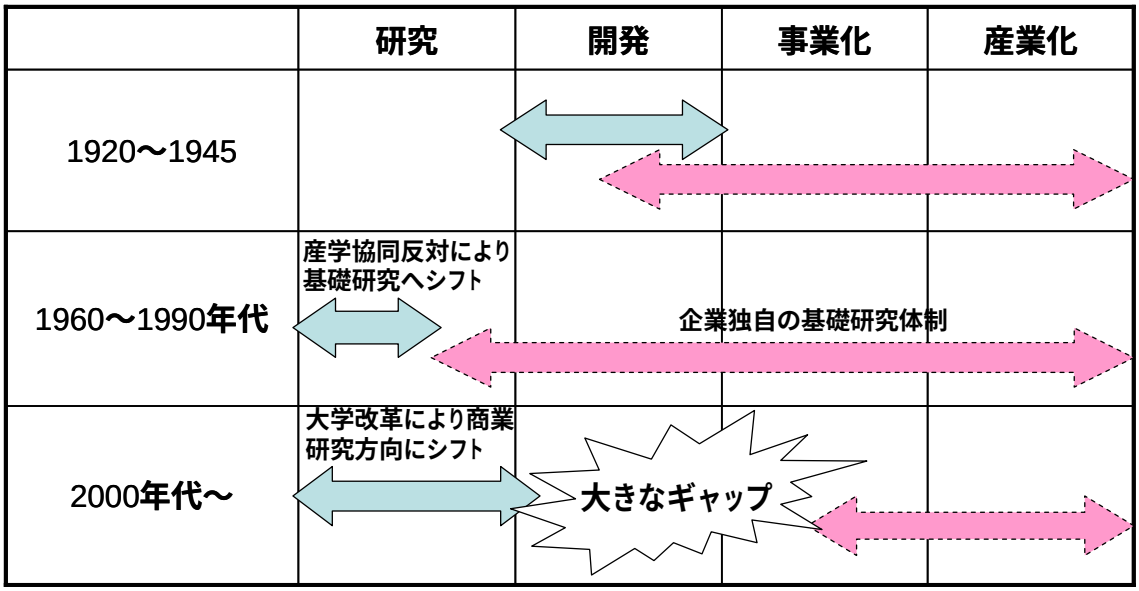
1980 年代の我が国においては、多くの大手企業が基礎研究から応用・開発までを一気に手がける中央研究所を設立したのに対し、当時の大学は産学共同反対の風潮から産業界と接点を持たない基礎研究へとシフトした[69]。その後、グローバル化や情報化による産業構造の変化を受けて、企業は製品開発に直結する川下の研究開発へとシフトした結果、大学における研究との間に大きなギャップを生じることになった。

今世紀に入り、教育基本法の改正、国立大学の法人化等を契機として、各大学は社会のニーズに素早く対応する新しいかたちの研究主体へと変わり、企業との研究ギャップを埋め、産業界との適切な役割分担を果たしつつ、独自性を発揮していくことが期待さ

[68] 国立大学法人法第 22 条第 1 項
[69] 長平彰夫・西尾好司 [2006]『競争力強化に向けた産学官連携マネジメント』中央経済社

れている。

図表５．日本の企業・大学の研究開発体制の変遷



実線：大学の研究開発体制、波線：企業の研究開発体制

出所：長平彰夫・西尾好司 [2006]『競争力強化に向けた産学官連携マネジメント』中央経済社を基に経済産業省知的財産政策室作成

②知のプラットフォームの提供

近年、科学技術の発展スピードが増し、技術が高度化・複雑化した結果、各事業主体が新しい技術開発に単独で取り組むことが難しくなってきており、広範囲に分散・分断されている断片的な情報を結合させて価値を増大させ、新たな価値を創造するネットワークの機能が重視されている。このようなネットワークの機能を活用することは、複数の技術開発に伴う莫大な投資を避け、自らが得意な分野に集中投資を行うことを可能とする。大学は、こうした知の結合を行うためのプラットフォームを提供する機関として位置付けることができる[70][71]。

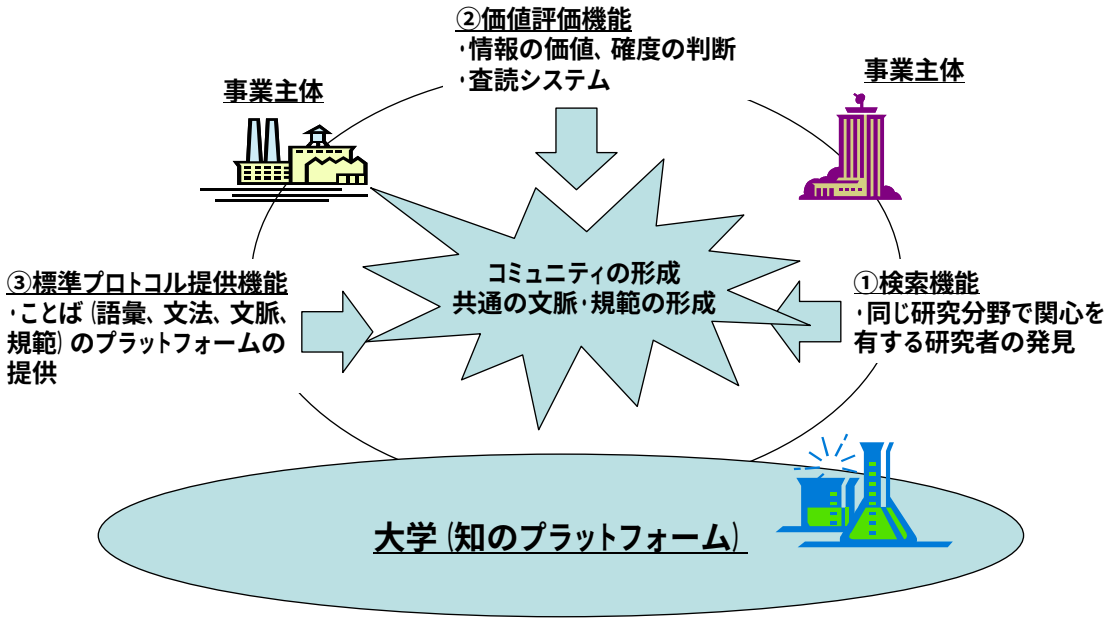
ここで、大学が知のプラットフォームとして機能するとは、様々な事業主体がめぐり合い、お互いに信用し、結合の作業を行うことのできる場として機能するという意味で

[70] 國領二郎[2001]「大学教育・研究組織のオープン・アーキテクチャ戦略」青木昌彦・澤昭裕・大東道郎・通産研究レビュー編集委員会編『大学改革　課題と争点』東洋経済新聞社

[71] これはチェスブロウ [2003] のオープン・イノベーションに相当するものと言えるが、オープン・イノベーションへの批判として、社外の知識に依存することのリスクが挙げられる。例えばインテルは、マイクロプロセッサの開発に際し他社の優れた基礎研究成果に全面的に依存した成長によってリーダーとなった結果、業界全体の研究投資は縮小し、Moore の法則（半導体チップの集積度は２年ごとに倍増する）が成り立たたず、技術的な成長が停滞する状態になった。したがって、大学については、単なる知の結合に終始しない継続的イノベーションのための知のプラットフォームの提供を通じたオープン・アーキテクチャの方がよりふさわしい表現といえる（チェスブロウ [2003]『OPEN INNOVATION』産業能率大学出版部）。

ある[72]。

図表６．知のプラットフォームとしての大学の役割



出所：今井賢一・國領二郎編著［1994］『プラットフォーム・ビジネス』情報通信総合研究所、國領二郎［1999］『オープンアーキテクチャ戦略』ダイヤモンド社、國領二郎［2001］「大学教育・研究組織のオープン・アーキテクチャ戦略」青木昌彦・澤昭裕・大東道郎・通産研究レビュー編集委員会編『大学改革　課題と争点』東洋経済新報社を基に経済産業省知的財産政策室作成

（参考）国立大学法人化以降の予算シフト等の状況

国立大学法人化以降の予算シフトの状況

		19年度予算	16年度比増減率	16年度比増減額
経常費補助	国大運営費交付金で特別研究費以外	11,199億円	96	▲476億円
	私立大学等経常費補助	3,281億円	101	18億円
重点配分資金	国大運営費交付金のうち特別教育研究経費	845億円	114	104億円
	国公私立大学を通じた大学教育改革支援	615億円	137	165億円
競争的資金	科学研究費補助金	1,913億円	105	83億円
	JST戦略創造研究事業	474億円	102	11億円
	厚生労働科学研究費補助金	409億円	108	30億円

出所：経済産業研究所［2007］『大学が提供する教育・研究に係る競争環境に関する構造的分析』

[72] 今井賢一・國領二郎[1994] の概念においては、ネットワーク上で取引が成立するためには、（１）取引相手の検索、（２）信用情報の提供、（３）経済価値評価、（４）標準取引手順、（５）物流等諸機能の統合、の５つの機能の提供が必要としている（今井賢一・國領二郎編著 [1994]『プラットフォーム・ビジネス』情報通信総合研究所）。

国立大学等における知財管理活用体制・規定策定状況

知財管理活用体制		
整備済	19年度以降策定予定	策定予定なし
72(78%)	8	12

利益相反ポリシー		
整備済	19年度以降策定予定	策定予定なし
60(65%)	21	11

産学連携ポリシー		
整備済	19年度以降策定予定	策定予定なし
42(46%)	32	18

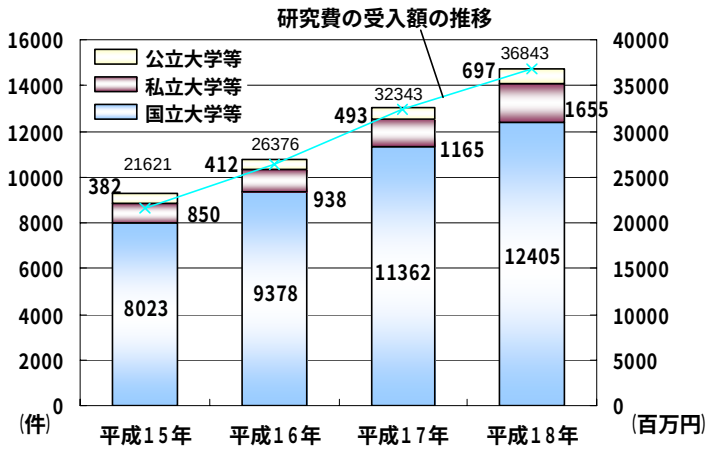
職務発明規程		
整備済	19年度以降策定予定	策定予定なし
88(96%)	3	1

知的財産ポリシー		
整備済	19年度以降策定予定	策定予定なし
73(79%)	9	10

※平成19年4月1日現在
※国立大学等とは大学・高等専門学校・大学共同利用機関。回答機関数は92。
※策定予定なしは主に教育大学

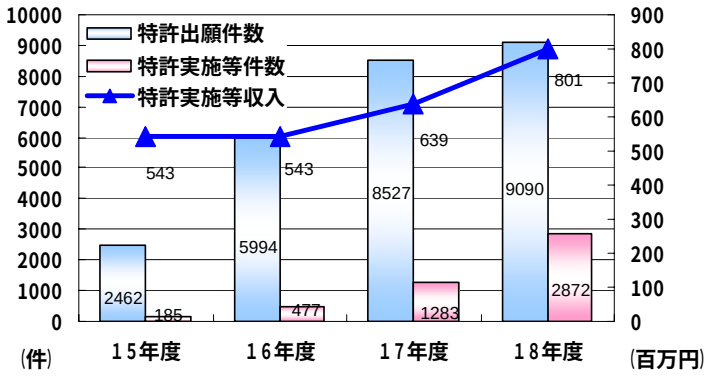
出所：科学技術・学術審議会『イノベーションの創出に向けた産学官連携の戦略的な展開に向けて（審議会まとめ）』（2007 年 8 月 31 日）

民間企業との共同研究の進捗状況



出所：文部科学省『平成 18 年度 大学等における産学連携等実施状況について』

知的財産権の管理・活用状況



出所：文部科学省『平成 18 年度 大学等における産学連携等実施状況について』

（2）大学における情報管理の在り方

（1）で述べたとおり、大学が保有する技術情報等についても、企業と同様に適切な管理を行うことが必要であるが、技術情報等の管理手法の在り方の検討に当たっては、以下で論じる大学の特殊環境を踏まえることが重要となる。

①大学組織の特殊性について

既に議論したとおり、大学には、学術の中心として広く知識を授けることを目的として教育研究を行い、その成果を社会に提供し、社会の発展に寄与するという使命を有している[73]。そうした大学の使命を果たすために、大学は重要度が高く広範な利用可能性がある様々な技術情報等が集積する知のプラットフォームとしての機能を有している。

我が国が激化する国際競争を勝ち抜くためには、これら産業競争力強化のために有用な技術情報等を我が国企業が適切に利用できるようにすることが必要であり、そのためには大学における技術情報等の適正な管理が必要不可欠であるが、大学においては、以下の点で特殊性を有していることに留意しなくてはならない。

研究情報の管理困難性

一般的に、学術研究は研究室単位で実施され、研究の実務戦力は雇用契約に拘束されない学生やポスドクが中心になることが多いため、組織的ガバナンスが機能せず、技術情報等の管理が困難な状況にある。

ボーダーレスな学術情報の交流

アカデミアの世界では、研究者は自らの所属する組織にとらわれず、グローバルに学術的な交流や技術情報等の交換を行っている。例えば、論文の査読等が日常的に行われているが、これらの技術情報等の秘密性は研究者個人の自主的な管理に委ねられているため、こうした部分には大学の統治が十分に働かない状況にある。

外国人留学生

現在、我が国の大学では、多くの国々から多数の留学生を受け入れている。少子高齢化、大学全入時代を迎え、外国人留学生は、今後、我が国の大学を支える不可欠な要素となるであろう。優秀な外国人留学生の受入れは、大学における知の創造を加速し、我が国競争力への貢献が期待される。一方、留学生を通じた本国への技術情報等の流出もまた懸念されるところである。

---

[73] 教育基本法第 7 条、学校教育法第 83 条

こうした大学の風土が存在するために、産学共同研究を行う際に、特に企業側が危惧する問題として、学生、大学院生、ポスドク、外国人留学生等の研究への関与による技術情報等の漏洩や、秘密保持契約を結んでいても大学側が共同研究の成果（その中には企業が提供した営業秘密として管理されている技術情報等が含まれることもある。）を学会や論文で発表してしまうこと、が挙げられている。

前者については、学生は大学にとっての「お客様」であるので秘密保持契約を交わすにはなじまない、学生から大学での幅広い学問の修得の機会を奪うべきではないといった指摘もある。しかしながら、企業では製品化に向けて莫大な額の開発投資を行っており、こうした技術情報等が漏洩することは企業にとって致命的な損害となりかねないため、共同研究プロジェクトを行う上で技術情報等の適切な管理を求めることは当然の社会的要求である。したがって、例えば大学院生についてはリサーチ・アシスタントとして秘密保持契約を交わすといったことや、そもそも企業との共同研究には当初から学生を参画させないこと等も選択肢に入れ、技術情報等の管理のための適切な対応がなされるべきであろう[74]。

また、後者については、大学側の明らかな秘密保持契約違反であるが、企業にとっては、必ずしも代替する共同研究先が簡単に見つかるものでないことや、大学の研究室が有力な人材供給源であること等から、大学の契約違反行為に対する適切な責任追及がなされないケースがある。さらに、他国にとっては、こうした学会等が我が国の最新の研究成果の格好の技術情報等の収集の場になっているとの指摘もある。こうした状況も踏まえつつ、技術情報等の管理について適切な対応が求められる。

近年、多くの大学が知的財産本部・産学連携本部等を立ち上げる過程で、知財管理の実務経験を有する企業の知財担当者を採用するケースが目立つが、大学においては、企業の情報管理の在り方を参考にしながら[75]、研究者の能力が発揮されるような環境整備と技術情報等の管理の徹底の両立が図られるべきである[76]。そのためには、大学が、トップマネジメントの下で適切な技術情報等の管理の方針を策定・実施することも必要であろう。

---

74 米国の大学が企業と共同研究をする際には、研究に従事する学生に対し対価を支払うのと併せて秘密保持契約を締結している例もある。

75 例えば、情報管理体制の構築されていない大学・研究機関と共同研究を行う際に、企業側から情報管理に関する指導・教育を行うケースもある。

76 例えば、ある機微技術の研究をしていた研究者は、当該研究が悪用された際の安全保障上の問題を懸念して研究成果を完全に秘匿化した結果、その優れた研究業績が特許取得や論文発表のかたちで適切に評価されることなく、当該研究者は退官することとなった。この事例のように、適切に研究業績が評価されなければ、当該研究分野の発展やカウンターメジャー（対抗手段）の開発にも支障を生じ、結果的に社会的な利益の損失となる。したがって、機微技術情報の管理が徹底されるとともに、当該分野の研究者が能力を発揮できるような環境整備の両立が必要となろう。

②学問の自由

大学おける技術情報等の適切な管理を論ずる際に、「学問の自由」との関係をどのように調整するかは避けて通ることのできない問題である。すなわち、学問の自由の内実である研究の自由、結果の公表の自由等には高次の保障が与えられるべきことは疑いが無い一方で、その研究成果が適切に管理されずに経済社会活動に悪影響を与えるときは、大学の社会的使命にも反し、学問の自由が本来目指した目的に反することにもなりかねない。

この点につき、まずアカデミアの自主的な規制を期待すべきであるとする立場があり得る。すなわち、研究成果の公表が人間の生命や健康を侵害する可能性が高いと認められるもの等についても、原則として法規制ではなく、学者自身と学問の府の自律や自主的判断に委ねられるべきであるとする立場である。

これに対し、一定程度の法規制に基づく国家的関与を追及していくべきであるとする立場がある。すなわち、この立場は、急速な科学技術の発展は、生命、身体、環境、生命倫理に重大な危険を生じさせ、又は、危険の発生を予見することを困難にしているのであるから、明白かつ差し迫った危険の発生が予測できなくとも、危険発生のおそれが合理的に論証できれば、科学技術の規制は許されると解するものである[77]。

この立場は、研究者の自主的・倫理的自己規制による対応は、これが破られた場合に有効に対処することが困難であることを指摘するとともに、社会的妥当性といった曖昧な基準で対処するときは、かえって研究の自由を阻害することになりかねず、法律による対応に基づくことが、かえって科学技術の研究を促進することにつながるものと主張する。

実際の制度構築に当たっては、後者の立場を基本としながら、科学技術の急速な発展により、クローン技術、大量破壊兵器等のように、生命、身体、環境、生命倫理等に甚大な影響を与えかねない技術情報については、特に強い正当化理由がある場合には、その研究成果の「管理」や「公表」には、一定の法的規制を行うことも視野に入れるべきである[78]。ただし、こうした情報を関係者に対して完全に公開しないこととするときは、こうした技術に対する抑止策を検討することも不可能になり、真に国民の安全安心の確保に資さないことも想定される。したがって、一定の関係者間における技術情報等の流通性を確保する

---

77 戸波は、①科学技術研究の制限によって達成される利益は「人間の尊厳」の確保という憲法上の価値に他ならないこと、②先端技術研究がもたらす損害・被害の程度は的確に予測することは不可能であること、③研究の内容が人間の生命活動の根源に関わることから自由な研究に委ねることは倫理的に適当でないこと、から科学技術を相当程度に規制する合憲性があるとしている（戸波江二 [1993]「科学技術規制の憲法問題」『ジュリスト』1993 年５月 No.1022 有斐閣）。

78 既に導入されている規制の例として、ヒトに関するクローン技術等の規制に関する法律（ヒトクローン規制法）がある。同法においては、人の尊厳の保持、人の生命及び身体の安全の確保並びに社会秩序の維持の観点から、クローン技術より作成される胚を人又は動物の胎内に移植することを禁止するとともに、クローン技術等による胚の作成、譲受及び輸入を規制している。

「限定された公開」のスキームが可能になるようにすべきである。

なお、企業から入手し秘密管理することとされた技術情報等や、国費による研究であって、国民の安全・安心に大きな影響を与える情報については、情報管理を要請することは当然であると考えるべきである。

（参考）米国における学問の自由の議論

911 テロ以降、米国においては学問の自由とテロ対策を目的とした規制について、アカデミアを中心として活発な議論が行われている。議論の対象は、論文・ジャーナルへの投稿、外国人の研究アクセス、アカデミアによる自主規制等々、多岐にわたる。

学問の自由に対する規制の根拠は、レーガン政権時代に発出された大統領令のひとつ「科学技術情報の移転に関する国家政策（National Policy on the Transfer of Scientific, Technical and Engineering Information, National Security Decision Directive-189）」に遡る。NSDD-189 においては、アカデミアにおける基礎研究は最大限の自由を享受するとしつつも、国家安全保障上の要請がある場合には、国費原資の基礎研究に関して情報管理がなされうることを明示している。この米大統領令は、冷戦当時、東側による米国大学・研究所からの先端技術の獲得が安全保障上の重大な脅威となっていたことによるものである。

論文発表

Stanford 大学の Lawrence M. Wein 氏らの「ミルクを利用したバイオテロの危険性の論文」について、2005 年 5 月に米国科学アカデミー紀要（PNAS: Proceedings of National Academy of Sciences）誌に掲載される予定となっていたところ、米国保健福祉省（HHS）から「テロの手引きになる」と批判され、いったん掲載が中止された。しかし、その後議論を経て、６月末に PNAS 誌に掲載された。


Lawrence M. Wein氏らの論文
(PNAS July12,2005 vol.102(no.28))

論文発表に関する自主的審査の取組として、例えば、米国「サイエンス」誌は、掲載論文の科学的意義と信頼性について編集委員会が審査（ピアレビュー）を行う。特に安全保障上の問題を引き起こす可能性の論文については、更なる審査と、必要に応じて外部審査委員の意見を求めることになっている。

外国人アクセス

大学・研究機関等で働く高度専門人材のための就労ビザとして、H1-B ビザが広く認知されているが、911 テロ以降、入国管理規制の強化によるビザ発給の遅延等により、外国人の研究アクセスが制限された。これに対し、アカデミアは研究活動に不可欠な人材交流を妨げるものとして反発している。

アカデミアの自主規制

911 テロ以降、テロ対策という名目で研究分野にも様々な規制が導入された。炭疽菌テロにも悪用が可能となるバイオ分野はその一例で、指定病原体の保管や移動に関して厳格な規制（Public Health Security and Bioterrorism Preparedness and Response Act of 2002 等）が導入され、研究活動に大きな影響を及ぼしたとされている。

一方、アカデミアからの反応として、政府による過剰介入を回避し、適切な規制のあり方を議論するため、バイオ関係者及び政府の安全保障関係者による NSABB（National Science Advisory Board for Biosecurity）が設立され、バイオセキュリティ対策のためのガイドラインの公表、科学者の行動規範等の作成によるアカデミアの自主的取組が推奨されている。

（参考文献）

- Wein and Liu [2004] ‘Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk’ “PNAS” July 12,2005 vol.12 no.28 PNAS
- American Association of University Professors [2003] ‘Academic Freedom and National Security in a Time of Crisis’ “ Academe” vol.89, no.6 American Association of University

Professors
- American Association for the Advancement of Science 'Scientific Freedom & National Security ' <http://www.aaas.org/>
- National Science Advisory Board for Biosecurity <http://www.biosecurityboard.gov/>

③研究者倫理について

②において議論されたとおり、学問の自由が確保されるという一般原則の中で、いかにして科学技術がもたらす公益への危険を排除するかを考える際には、大学におけるガバナンスの徹底が企業と比較して難しいことに加え、科学知識の増大、研究の加速度的な発展・高度化、研究内容の多様化・複雑化、科学技術の社会的な影響の増大、研究機関の競争的要素の増大等を踏まえると、研究活動の実施や公表の当事者である研究者レベルでのガバナンス、すなわち、研究者個人を規律する倫理の在り方が非常に大きな意味を持つことになる[79]。

現在の研究者倫理の議論は、ミスコンダクト、すなわち広く社会規範からの逸脱行為も含んだ倫理的、道徳的概念とされているが、具体的な対象は、ねつ造（Fabrication）、改ざん（Falsification）、盗用（Plagiarism）を中心とした部分（これらは「FFP」と呼ばれる。）に限られており、研究者が「社会からどう見られるか」といったある種内向きな議論に止まり、研究者が「社会に対してどういった責任を負うか」という視点からの議論は必ずしも十分であるとはいえない[80][81]。

他方で、科学技術の急速な発展によって進歩し続けるデュアル・ユース技術等が社会にどのような影響を与えるかという問題については、そうした日々進歩しつつある技術について制度的な対応が追いつかない場合が多いことから、研究の当事者が自らの責任として社会的影響を踏まえた自制を行うことが期待される。

---

79 学問の自由の例外を認めない立場の学者も、「研究者・科学者の高度な倫理観が、（これは法律外の問題であるけれども）今日ほど求められる時代はないといえよう」としているが、これは学問に携わる当事者によって解決されるべきものであるとの主張からきているものと解される（小林直樹 [1980]『憲法講義』東京大学出版会）。

80 ミスコンダクトへの対処の手続きに関しても、手続規程を整備しているのは 148 学会、整備されていないのは 689 学会という現状にある（『科学におけるミスコンダクトの現状と対策』日本学術会議（2005 年 7 月 21 日））

81 國領二郎 [2001] によると、学術界の大きな特徴は知的貢献を競うインセンティブ構造にあり、成果の対価は必ずしも金銭的なものではない（例えば論文の投稿数、引用数等の名声等が挙げられる。）。こうした成果は法的保護では不十分であり、社会的規範によって保護されることが必要となる。研究者にとって共通の倫理観が求められるのはこうした理由による（國領二郎 [2001]「大学教育・研究組織のオープン・アーキテクチャ戦略」青木昌彦・澤昭裕・大東道郎・通産研究レビュー編集委員会編『大学改革　課題と争点』東洋経済新聞社）。

この点、例えば、EU においては、第７次フレームワーク・プログラム（FP７）における研究者倫理として、データ保全とプライバシーの問題、デュアル・ユース技術等も対象にした広範な倫理ルールを研究者が守るべき義務として定めており、EU 出資研究における「最高度のプライオリティ」として位置づけられている[82]。

このように、世界の研究者倫理の議論は FFP に止まらない広範な社会規範からの逸脱行為を視野に入れていること、我が国の先端技術をテロ行為等に悪用されることによる公益の侵害と信用の失墜を招きかねないことにかんがみ、我が国においても、デュアル・ユース技術への対応等、科学技術がもたらす社会的影響に関する研究者倫理の議論がなされるべきである。

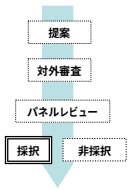
（参考）ＥＵ・米国のグラントにおける倫理遵守のルール

ＥＵ

EU は、こうした EU 出資研究における倫理規範を「責任ある学術出資モデル（a model of responsible science funding)」の確立として重視している。第７次フレームワーク・プログラム（FP7）への研究提案者は、研究倫理に対してどのように取り組むかを示すとともに、Ethics Review Panel において個別に審査を受けることが求められる。

＜倫理の視点＞
・インフォームドコンセント
・ヒト胚／胎児に関する研究
・データ保全及びプライバシー
・動物に関する研究
・発展途上国に関する研究
・デュアル・ユース

（グラント審査の流れ）



＜審査の視点＞
・応募者の倫理面の認識と提案する研究の社会的な影響
・研究者が FP7 の倫理的な規則と規格を尊重しているかどうか
・関連ヨーロッパ法規に適合しているかどうか
・応募者が関係分野の倫理委員会の承認を求めているかどうか
・関連国際協定及び宣言に適合しているかどうか
・研究目的と手法のバランス

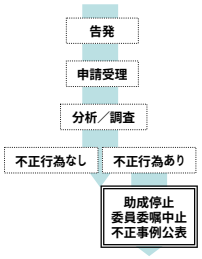
出所：EUROPEAN COMMISSION [2007] “ETHICS FOR RESEARCHERS”

米国

米国では、公衆衛生庁（PHS：Public Health Services）の助成研究について、ミスコンダクト（捏造、偽造、盗用）の調査・指導・監督をするための機関として研究公正局（ORI：Office of Research Integrity）が設置されている。ミスコンダクトが実証された研究者に対して、数年間の助成金申請停止、政府関連委員への委嘱中止、不正行為事例の公表等の制裁が科される。米国研究者は助成に依存するところが大きいことから、極めて重い懲罰となる。

[82] EUROPEAN COMMISSION [2007] “ETHICS FOR RESEARCHERS”

（ミスコンダクトの審査の流れ）



※ ORIが発行している「ORI Introduction to the Responsible Conduct of Research」において、不正行為を報告しないことは、それ自体が犯罪とみなされ、罰則につながるとしている。

※ 米国科学アカデミーが発行している「ON BEING A SCIENTIST」においても、不正行為を告発することは科学者の義務としている。

出所：黒川清ほか [2006]『科学者のミスコンダクト』財団法人日本学術協力財団
Nicholas H. Steneck [2007] “ORI Introduction to the Responsible Conduct of Research”
NATIONAL ACADEMY OF SCIENCES [1995] “ON BEING A SCIENTIST”

第２節　具体的対応

（１）研究情報の外部公表の可否判断：組織的管理の実践と支援

前節（１）において大学組織の特殊性を述べたが、大学組織としての適切なマネジメントが働かないと、何らかの技術情報等の流出が発生した場合に、現場の研究者個人が責任を問われることになりかねない。これは、現場の研究活動を萎縮させるとともに、事故の原因究明・再発防止につながらないといった問題を生じることになる。したがって、まずは組織的管理の実践に努めるべきであろう。

現在、各大学では利益相反のマネジメント[83]を行っているが、機微な研究情報の学会・論文等を通じた外部への公表によって、我が国の競争力に対する甚大な影響や安全保障上の脅威が懸念されるような場合にも、その公表の是非や公表する場合の望ましい方法について、大学の執行機関が組織として判断を行うことにより対処することとすべきである。その際には、例えば利益相反アドバイザーの機能を参考にしつつ、大学当局に研究情報の開示についてのアドバイザーを設け、教職員が行おうとする研究情報の公表に際しての指導・助言機能を持たせる等の対応が考えられる[84]。また、こうしたマネジメントに違反するような行為に対する適切な処分の在り方も検討すべきである。

また、組織的管理の実践として、国家プロジェクトの研究等外部からの複数の企業の参加が見込まれ、かつ、特に秘密化の要請の高い技術情報等の管理に当たっては、通常の大

[83] 大学が利益相反のマネジメントに取り組む目的としては、大学の社会的信頼を維持し、産学官連携の推進を図るとともに、法令違反に至る行為を事前に防止し、教職員個人の責任と利益を大学が適切に分担することにある。現在、多くの大学で利益相反ポリシー及びマネジメント規程が定められ、利益相反の生じる可能性がある事案について大学組織として許容性の判断を行っており、組織的に利益相反の判断を行う体制が確立されている。

[84] 現在、利益相反アドバイザーは利益相反マネジメント体制を構築している大学の多くに置かれており、教職員の利益相反行為に関する質問又は相談に応じるとともに、必要な助言又は指導を行っている。また、一部には、教職員からの開示情報等について一定の基準の下に判断を行い、利益相反委員会に報告する責務を持たせている大学も存在する。

学の研究活動とは一線を画した技術情報等の管理のための「特別情報管理区域」を設け、ここに参加するメンバーの特定、秘密保持契約の徹底、知財マネジメント等を独自に徹底して行うことも考えられる[85]。

加えて、技術情報等の管理に関する大学の理解を一層深化させるため、「大学における営業秘密管理指針作成のためのガイドライン」等の周知の強化、相談窓口の設置等、大学に対して技術情報等の管理面での支援を行っていくことを検討すべきである。特に、政府資金で行われる研究開発については、優先的な取組が求められる。

また、安全保障面で機微と考えられうる研究成果については、その公表の是非や公表の仕方について、学術誌や専門誌等の編集部においても、自発的なレビューを推奨することが望ましい。

（２）政府資金で行われた研究成果の公開原則の見直し

政府資金で行われた研究成果については、産業の発展や更なる研究活動の発展等に役立てるために社会に還元するとの原則に基づき、ある種当然のこととして公表されているところであるが[86]、その内容によっては、公にすることでかえって安全保障上の問題を招いたり、技術情報の流出によって国家の競争力の毀損に至る場合も想定され得る。

したがって、研究成果の取扱いについては、成果の公表という原則を遵守しつつも、安全保障や競争力の問題を生じさせないようなかたちでの管理や公表に配慮することが必要である。特に政府資金で行われる研究に関しては、研究中における情報管理の在り方、成果発表の在り方について、真に国益に適う対応をすべきである[87][88]。

---

[85] 近年、大学を研究開発拠点とする大型の国家プロジェクトにおいては、大学側の研究員を含め秘密保持契約を結ばない者のあらゆるアクセスを禁止し、研究現場の厳重な施錠管理を行う等の取組がなされており、こうした取組を大学一般に広めていくことが望ましい。

[86] 政府資金で行われた研究成果全般についての公表を直接規定するものはないが、研究開発成果についてはその活用を図る観点から「科学技術基本法」に基づいて公開することが規定されている。また、研究教育機関の責務として成果の公表を規定するものとして「民間学術研究機関の助成に関する法律」、「学校教育法」、「国立大学法人法」がある。さらに、研究の成果はそもそも国民の税金を原資として行われた結果であることからして、当然に出資者である国民に還元することが大原則であるものと解され、それらは、以下においても説明されるところ。

- 情報公開法：国民主権の理念にのっとり、行政文書の開示を請求する権利につき定め、行政機関の保有する情報の一層の公開を図るもの。本法に規定される非公開情報の範囲（第５条各号関係）は極めて限定的なものであると解すことが適当であると思われる。
- 国立国会図書館法：国立国会図書館は、政治、行政、国民一般に対し図書館が蒐集した文献を提供することにより、同法の前文にある「真理がわれらを自由にするという確信に立って、憲法の誓約する日本の民主化と世界平和に寄与する」ものであり、国はこれにより発行した図書等を納入する義務が課され（第 24 条）、委託研究の報告書等を納入している。
- その他に、国民の安心・安全等を確保するための研究の促進等を目的として成果の公表を規定する法令がある（化学物質排出把握管理促進法、オゾン層保護法、大気汚染防止法等）。

[87] 米国では、表現の自由に関連し、政府の補助金の拠出に対し一定の条件を課すことや補助の条件に一定の権利の放棄を求めることについて、許容性を認めた最高裁判例が存在する（Rust v. Sullivan, 500 U.S.173(1991)/ National Endowment for the Arts v. Finley, 524 U.S 569(1998)）。これは、公的資金が拠出された研究について一定の関与を求める議論にも参考になるものと考えられる。

[88] 国の委託事業として行われる研究開発の中には、学会発表、論文投稿等を含め、契約書上の規定で国の許可無く内容を公表してはならないとしているものもあるが、これは、必ずしも上記の視点で研究成果の

（参考）機微と考えられる公開研究情報の例

遺伝子操作で誕生した究極のネズミ痘ウイルス

- ネズミの爆発的な増加を食い止めるため、不妊ウイルスの研究において、ネズミの免疫の働きを抑える遺伝子をウイルスに組み込んだところ、予想もしなかった殺傷能力を持つウイルスが出来上がってしまった。このウイルスに感染したネズミは、たとえワクチンが投与されたとしても100%死滅してしまうという。
- これが応用され、人間の免疫システムを遮断してしまう究極の生物兵器が作り出される可能性に対して大きな懸念があるが、この機微な研究成果は、英科学誌において「究極の生物化学兵器の誕生から一歩手前の段階へ」と紹介され、学術誌において全ての研究成果が公表された。

出所：Malcolm Dando [2006] “Bioterrorism and Biowarfare” Oneworld Publications

小児麻痺ウイルスの人工合成

- 2001 年、ニューヨーク州立大学の研究者らが、インターネットで公開されているゲノム・マップを基に、各種 DNA のセグメントを通販で購入して、毒性の高い小児麻痺ウイルスを人工的に作り出した。

出所：FEDERATION OF AMERICAN SCIENTISTS , Case Studies in Dual Use
<http://www.fas.org/biosecurity/education/dualuse/FAS_Wimmer/index.html>

薬投与を目的とした新型エアゾール・スプレー技術の開発

- 1997 年、ペンシルバニア州立大学の研究者が、ポーラス構造分子を利用して薬投与を目的とした新型エアゾール・スプレー技術を科学誌に掲載した。これは、これまでよりも効果的に多くの薬を肺の奥まで運ぶことができる革新的な方法であった。
- 当初、この革新的な技術はメディアに注目されていなかったが、2001 年に炭疽菌を吸入した 5 名が死亡した事件が発生した後に本技術との関連性が明らかになり、デュアル・ユース性が注目されることとなった。

出所：FEDERATION OF AMERICAN SCIENTISTS , Case Studies in Dual Use
<http://www.fas.org/biosecurity/education/dualuse/FAS_Edwards/index.html>

1918 年スペイン風邪ウイルスの人工合成

- ある科学者チームが 1918 年スペイン風邪ウイルスの再現に成功し、その結果は科学誌に公表された。
- これについて、科学者のコミュニティではこの実験の実施の是非や今後の取扱いについて激しい議論がなされた。議論はウイルス配列の公表に関連したデュアル・ユース上の懸念といったものから、ウイルスの取扱方法や環境面でのおそれにまつわる懸念にまで及んでいる。
- もっとも、全ての反応が否定的だったわけではなく、実験はスペイン風邪ウイルスがどれほど致死的だったかという理由を明らかにするとともに、鳥インフルエンザの病理と人間への感染についての視座を与えてくれるとの議論もある。

出所：Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats [2006] “Globalization, Biosecurity, and the Future of the Life Sciences” THE NATIONAL ACADEMIES PRESS

取扱いに配慮したものではないと考えられる。

（３）外為法の施行支援

外為法の適切な遵守に関しては、同法の該否判定に高い専門性を有する専門人材が必要である等の理由により、累次の文部科学省・経済産業省の通知[89]にもかかわらず、大学における対応状況は必ずしも十分でない。同法輸出管理制度の理解促進のためガイダンス[90]を発出したところであるが、今後とも更なる周知・徹底が不可欠である。

また、大学における専門人材不足に対処するために、経済産業局の活用、大学外部の相談組織の設置・強化や大学内部の体制強化に対する国の支援等について検討すべきである。

併せて、大学に対する国等の研究資金の配分に当たって、原子力、航空宇宙分野等については、外為法の適切な遵守がなされているかどうかも評価の視点に加えてはどうか。

（４）ミスコンダクトへの制度的対応：研究者倫理の在り方

研究者の社会的責任をも含めた研究者倫理の議論及びミスコンダクトへの対応については、アカデミアの自発的な取組に委ねるべきか、あるいは、政府が一定の関与をすべきかの議論があるが、現在の我が国における学会レベルでの取組を見る限り、政府による統一のルール整備が必要である。

その際、まずは、EU の FP７のように、政府資金によって行われる研究については、倫理規程の策定及び遵守の義務付けをしても良いのではないか。そして、ミスコンダクトを起こした研究者に対しては、研究資金の返納、申請停止、公表等の厳しい措置を採るべきではないか。特に研究資金は研究者の活動の生命線であることから、効果的な抑止力になるとの指摘もなされている[91]。政府関連部分からこうした行動を起こすことによって、他への波及が期待される。

この場合において、不要に研究活動を抑制することが無いように、取締りよりも予防に重点を置き、研究者倫理を高めるための教育・普及活動を重視する必要がある。このような活動は研究者のみならず、大学の経営陣に対しても行われることが望ましい。

また、ミスコンダクトを防止するためには、職業研究者として従事する以前の段階から不正行為の研究活動や科学技術に与える影響等に関する意識を高めていくことが重要であることから、大学院生等を対象に倫理教育を行うことが効果的であると考えられる。既に一部の大学ではこうした取組が行われている[92]ものの、一般には大学や研究者によって倫理

---

89 『大学における輸出管理の強化について』（平成 18 年３月３日付）が文部科学大臣経由で各大学・公的研究機関あてに発出されている。

90 経済産業省貿易管理部『安全保障貿易管理に係る機微技術管理ガイダンス』（2008 年１月）

91 米国 NIH(National Institute of Health)の助成する研究資金の監視機関である ORI(Office of Research Integrity, Public Health Services)は、ミスコンダクトが実証された研究者に対してこうした措置を取るとともに、研究者の所属機関から解職等の措置が取られる。http://ori.dhhs.gov/

92 一般的な倫理教育を旧来より開講している大学もあるが、早稲田大学では、昨年度より RCR(Responsible Conduct of Research)研究会を立ち上げ、今年後期から、研究者を目指す大学院生を対象に、安全保障の観点等を含めた旧来の倫理教育よりも幅広い視点での新しい倫理教育を開始することとしている。

観の醸成に関する意識は千差万別であり、我が国学術界が一体となって倫理感が醸成されつつあるとは言える状況にない。

そのため、政府においても、研究者倫理を高める活動を推進させるため、政策的な取組を行っていくことが必要ではないか。

（5）アカデミアと安全保障関係者の対話

デュアル・ユース技術に対する予見可能性を高める意味では、第２章で論じた機微技術リスト・ガイドラインの作成は有効であると考えられるが、将来の発展・活用可能性について不確実性の高い先端・複合領域における技術についてはリスト化が困難であることから、そうした技術がもたらす社会的影響の予見性を高めるため、個別技術の関係者だけでなく、幅広い関係者によって多角的に議論されることが必要である。したがって、先端技術情報の管理の在り方を議論するため、規制当局とアカデミアの対話の場を設けることを検討すべきである[93][94]。

[93] 規制当局とアカデミアの対話の一例として、例えば米国のバイオセキュリティ分野においては、バイオ関係者及び政府の安全保障関係者によって NSABB (National Science Advisory Board for Biosecurity) が設立されている。NSABB は、社会に損害をもたらすようなデュアル・ユース性のあるバイオ研究の在り方について、政府がガイドラインや科学者の行動規範の作成等の規制を検討する際に、これに資する提案を行うこととしている。

[94] 我が国でも、生物テロに平時から備えるべく、東京慈恵会医科大学の浦島準教授の主催の下、産官学の専門家（中央省庁や自治体、医師や研究者、企業等）が集う勉強会が発足され、炭疽菌や天然痘等の性質や対処法を学ぶ等の取組が実践されている（日本経済新聞（2007 年 7 月 16 日）による）。

委員のコメント（概要）：大学における情報管理

○ 大学での研究に関しては、組織的管理を受けるという習慣があまりなく、むしろ、アカデミアの中での自由な情報交換を基礎とする規範が成り立っている。

○ 例えば、論文の査読では、公表前の投稿論文が面識のないエディターから突然送られてくることがある。送付先を間違えて、学生に査読依頼が来たという例も聞いたことがある。

○ 大学の研究のような不確実性の高い技術情報は、公開して応用可能性の開拓を行うことで進歩していくものであり、企業が利用できるフェーズの技術とは異なった次元のものとして考えるべき。

○ 大学が中小企業と共同研究を行うのは、受託金額は少ないものの、ライセンス契約が将来のロイヤリティとなっているからである。我が国では米国と違いバイドール条項に中小企業優遇規定がないが、大学の知財活動は結果として中小企業優遇になっているのではないか。

○ 逆に、大学の研究情報について、企業に特許出願されてしまうような例も存在する。大学の管理が強化されても、「大学の技術情報は利用自由」という通念は、大学内外において依然根強い。

○ 大型研究プロジェクトについては、複数の企業と大学で進めていく場合に、自社の秘密の漏洩をおそれれば議論自体ができなくなる。参加者の情報共有をやりやすくするためには、公的研究機関等の中立的な組織に管理を移行するか、プロジェクト自体を特別管理区域に指定し、一般の研究とは異なるより厳格な管理システムを構築することが必要ではないか。

○ 大学のガバナンスの特徴を踏まえて、大学のカルチャーを利用した管理システムを用いることが有効。

○ これまで大学において安全保障管理規程がほとんど作成されていないのは、大学のガバナンスが強く働かないことや、情報管理よりもアカデミアの規範の方が尊重されてきたからではないか。

○ 米国の研究現場では、例えば、国防関連の研究部署でも非友好国との共同研究が行われている等、優秀な人材を引き留めるために、オープンに学術交流が行われている。

○ 技術情報の管理を研究者任せにするのは、研究者や教員にとっても大きな負担である。そうした判断について、第三者に確認を取れるシステムがあることが重要。

○ 外国人が研究プロジェクト参加することはより良い研究のために必要であるが、帰国する際には研究の成果を我が国に残してもらうことが重要である。

○ この点、バイドール法に関して、米国よりも条件が緩和されていることは問題。国内に良い産業を興すことが本来の目的であり、それを実現する方向で改善がなされるべき。

○ 被害実態を十分に把握した上で、適切な制度を構築することが必要。抽象的な実態把握のまま大きな網をかぶせてしまうと、生産性の低下につながりかねない。

○ 企業と大学において情報管理の認識に乖離があるのは、そもそもガバナンスに関する文化の違いが根底にあるのではないか。

○ 大学における研究成果の中で、特別な情報管理が求められるものは相対的に少ないため、例外として特別な管理を規定する方が良いと考える。

○ 研究成果の公表については、どんなに潜在的なリスクがあっても、因果関係が不明であるため、基本的にはそれを制限することはできないが、研究によって予測されるリスクに応じて研究のプロセスや公表方法等に差を設けても問題はないと考える。

○ 学問の自由の下に、学問研究に対して政府がファシリティーを与えることを保障したものではないし、研究内容や公表に制限をかけることも、価値中立的な原則に則っている限りは、ファシリティーを与える者の自由があるべきであると考える。

○ 研究成果の公表について、研究者の倫理に任せることは、かえって過剰規制を生むことになりかねないことに注意が必要。

○ 秘密特許制度を設けるのであれば、対象となる技術を一定期間外国に出すことができない制度とバランスを取らないと、国内で特許出願せずに海外に技術を出すことが抜け道となり問題。

○ 企業が産学連携の成果を事業化するためには、相当な資金を投入して知財活動を行うことが必要になるが、万一、成果が海外に流出しており、別の者が特許出願をしていたら、多大な損害を被ることになる。企業としては、損害が発生するリスクを背負って事業化はできない。

第５章　政府における情報管理

（ポイント）

【現状と問題点】

- 政府が保有する情報については、原則公開されることが政府の民主的コントロールの観点から望ましい。
- 一方、これが無制限に公表されることとなると、かえって我が国の国益を損なうことにもなりかねない。
- 我が国において、どのような政府情報を公表し、何を非公開とするかの哲学が求められている。

【具体的検討事項】

- **重要情報の区分ルールの導入**
- **セキュリティ・クリアランスの導入**
- **秘密保護法制の検討**
- **政府及び政府契約企業における情報保全の在り方**

第１節　現状と問題点

企業・大学とともに政府は重要な情報管理の主体である。しかしながら、イージス艦情報等の防衛秘密の流出、捜査情報の漏洩等政府機関からの情報流出が相次いでおり、政府組織内における情報管理体制の不備が指摘されている。こうした重要情報の流出は、安全保障上の問題を引き起こすものであるとともに、国家の信頼の低下につながりかねないものである。

そもそも国が保有する情報については、これを公開することが政府の民主的コントロールの見地から望ましい一方で、これを無制限に公表することとするときは、かえって我が国の国益を損なうことにもなりかねない。我が国においては、こうした何を公表し何を非公表とするかの明確な哲学が欠けており、この哲学なしには適切な管理もおぼつかない。

政府が保有する情報は、行政情報、外交情報、安全保障情報等、非常に多岐にわたり、これらは自ら作成した情報もあれば、民間や他国政府等から受け取った情報もある。これら政府情報の大きな特色は、その公共性にあるものと考えられる。すなわち、政府情報はその利用を通じて最終的には政府の政策の企画立案や行政のかたちで国民生活に間接・直接に影響を及ぼすことから、原則として公開が求められることになる[95]。しかしながら、情

[95] 情報公開法第１条（目的）この法律は、国民主権の理念にのっとり、行政文書の開示を請求する権利に

報の内容よっては必ずしも公開することが適切でないものも当然のことながら存在し、こうした情報については適切に管理されることが必要となる[96]。

そうした一部の重要な政府情報をなぜ管理するかという理由については、①政府内における情報共有の促進、②重要情報の流出防止による国益の損失の回避、の２つがあろう。一つめの理由については、官邸の意志決定を支えるためには、各省庁からの適切な情報の集約の枠組みが構築されることが必要であり、そのためには、各省庁が提出する重要度の高い情報が必要な関係者の間で適切に管理されることが前提となる[97][98]。二つめの理由については、重要な政府情報の流出によって我が国の競争力の損失や安全保障上の問題を生じさせないよう、ある意味国民によって管理を付託された国民の財産であるところの政府情報の預かり者としての責任を果たすことである。

適切な政府情報の管理の必要性を考えるに当たって、現在の政府における情報管理の大きな問題点として、極めて限定された場合を除き、政府情報は一律に扱われており、情報の重要度に応じた価値付けとそれにふさわしい管理のルールが定められておらず、預かり責任者としての責任を果たしていないという情報管理の実態が挙げられる。

（参考）政府からの漏洩の実態

「報酬と引換に政府情報がロシアへ」
- ○ 内閣情報調査室の事務官は、内部情報等を基に作成した資料を、ロシア政府の情報機関員とみられる在日ロシア大使館員に渡していた。
- ○ 事務官は懲戒免職処分となり、収賄と国家公務員法違反で書類送検され、不起訴処分（起訴猶予）となった。在日ロシア大使館員は、贈賄に関し国家公務員法違反（教唆）で書類送検されたが、不起訴処分（起訴猶予）になっている。

「報酬と引換に戦術等の秘密文書がロシアへ」
- ○ 海上自衛隊三等海佐が、在日ロシア大使館に勤務する海軍武官から工作を受けた。
- ○ 報酬と引換えに、戦術や護衛艦の性能をまとめた秘密文書をロシアに提供した。
- ○ 三等海佐は、自衛隊法違反で懲役 10 ヶ月の実刑判決を受けた。（自衛隊法改正前）
- ○ ロシア武官は、事件発覚後帰国した。

つき定めること等により、行政機関の保有する情報の一層の公開を図り、もって政府の有するその諸活動を国民に説明する責務が全うされるようにするとともに、国民の的確な理解と批判の下にある公正で民主的な行政の推進に資することを目的とする。

96 情報公開法第５条柱書きで､開示請求に係る行政文書の開示義務を規定すると共に､同条各号において、公にすることにより公共の安全と秩序の維持に支障を及ぼすおそれのあると認められる情報等について例外的に不開示としている。

97 政府部内での情報共有のための情報管理の必要性に加え、日本政府の情報保全体制が不十分であったために、他国との情報協力に際し大きな障害であったとの指摘もある（PHP「日本のインテリジェンス体制の変革」研究会 [2006]『日本のインテリジェンス体制　変革へのロードマップ』株式会社 PHP 総合研究所）。

98 一連の「官邸における情報機能の強化」の議論においては、官邸における情報機能の強化を政府部内で検討することを目的として、2006 年 12 月に情報機能強化検討会議（議長：内閣官房長官）が設置され、以降、『官邸における情報機能の強化の基本的な考え方』（2007 年２月）、『官邸における情報機能の強化の方針』（2008 年２月）がとりまとめられたところ。WG において、情報の集約・共有及び基盤整備の前提としての政府統一基準の策定のほか、秘密保護法制の検討として、諸外国の現状、真にふさわしいあり方の研究を継続中。

「Winny により捜査情報１万件が流出」

○ 警視庁巡査長の私物パソコンから、捜査資料等約１万件の文書類や画像がインターネット上に流出し、ネット掲示板に「警察情報が流出している」との書き込みがあったことから発覚した。
○ 流出した文書類や画像には、捜査報告書及び供述調書、捜査対象者の銀行口座の分析等、機微な情報が多数含まれていた。
○ 巡査長のパソコンには、ファイル交換ソフト Winny がインストールされており、ウィルスに感染していた。
○ 警視庁は、Winny が入ったパソコンはないと内部調査に虚偽の申告をしていたことや、流出情報に機微な情報が大量に含まれていた重大性から、巡査長を懲戒免職とした。

「自衛隊内部でイージス艦情報が拡散」

○ イージス艦中枢情報の資料が流出した。事件は自衛隊員がイージス艦の中枢情報資料を自宅のハードディスクに隠し持っていたことから発覚した。
○ 元プログラム業務隊に所属していた３等海佐が、当時海自第１技術学校で教官であった知人隊員に漏えいしたことから起こった。
○ その後、教官隊員から同僚教官に資料を渡したこと等によって情報が拡散したことが判明している。
○ ３等海佐が、特別防衛秘密を漏らしたとして、日米相互防衛援助協定等に伴う秘密保護法違反容疑で、逮捕された。防衛省・自衛隊は、当該３等海佐を含めた計５８名について処分を下した。

出所：新聞報道等

第２節　具体的対応

（１）重要情報の区分ルールの導入

情報は、重要度レベルとカテゴリの区分がなされることによって、適切に保護され、各情報保有主体における統一的な対応が可能になる。米国では、国家安全保障に係る情報の分類方法の考え方を定めた国家安全保障情報区分“Classified National Security Information”[99]が存在し、このルールによって安全保障情報が定義、区分され、各種秘密保護法制や情報保全規程における保護・保全対象の基礎となっている。

これに対し、我が国においては、安全保障情報についての定義付けの明確なルールが定められていない[100]ために、①省庁縦割りごとにバラバラに定義づけられ、同じ重要度の情報が省庁間で取扱いが異なるといった事態が生じうる、②政府情報の原則公開という社会の要請に反し、秘密化される重要情報が増産されうる、③特に秘密管理することが必要となる重要情報にアクセスする者の人的管理手法である適格性の確認が行えない、といった

[99] CNSI (Classified National Security Information) : 大統領令によって発出される安全保障情報の統一的な区分ルールで、重要度（Top Secret, Secret, Confidential）、カテゴリ（軍事情報、外国政府情報、諜報活動、外交情報、国家安全保障に係る科学技術・経済情報等）、識別・表示、区分の見直し、その他の区分ルールを定めている。

[100] 政府統一基準は導入されているもののどのような分野の安全保障情報について区分するかの判断は情報所有者に委ねられているために、上に記したような問題を生じている。

問題をはらんでいる。

したがって、我が国においても、既に導入されている政府統一基準に加え、政府において特に秘密管理することが必要となる重要情報の区分や取扱方法をルール化することで重要情報の管理の確実性を高めるとともに、これらを扱う職員の適格性の確認を行う制度を導入すべきである（適格性確認制度については（２）で議論する）[101]。また、こうした重要情報の管理区分のルールには、過剰に情報が秘密化されていないか、重要情報が適切に区分されているか等について不断の見直しがなされるようなレビューシステムを併せて導入すべきである。

（２）セキュリティ・クリアランスの導入

諸外国においては、特に秘密にすべき情報を扱う組織の職員に対しては、国家安全保障上の観点から、信頼性確認（クリアランス）を行うことが一般的であるところ、我が国においても着実に同制度の導入を図っていく必要がある。

この場合において、信頼性確認制度の導入に際し、確認により期待される効果、確認の実施方法、実施上の問題、実効性、基本的人権に係る憲法上の要請との調整、国民的合意形成の必要性等、多くの論点・課題について議論が必要である[102]。

（３）秘密保護法制の検討

米国においては、国家安全保障の観点から、防衛情報、諜報活動情報、米国の安全に影響を及ぼす情報等の安全保障情報について、国を侵害し、外国を利することを意図した収集等の行為に対する罰則が科されている。

一方、我が国においては、安全保障に係る政府情報のうち、防衛秘密、特別防衛秘密、原子力施設の防護に関する秘密等の漏洩行為に対して罰則が科されているものの、秘密の対象、行為主体、対象行為は非常に限定的であるとともに、個別法によって処罰の差異が大きく、その抑止力は十分でない等の問題がある。

こうした不十分な秘密保護法制は、累次の政府からの情報漏洩事件を招き、結果として、安全保障上の問題、対外的な信用の低下等の大きな弊害をもたらしているとの指摘も数多い。

漏洩することにより国家の安全保障上重大な問題が発生する可能性のある情報については、秘密化の義務と不法な漏示に対する適切な規律を設けるべきである。

---

101 この点、『カウンターインテリジェンス機能の強化に関する基本方針』（2007 年８月）においても、「特に秘匿すべき情報（特別管理秘密）」について、物的管理及び人的管理の必要性に関し方針が示されている。

102 総合資源エネルギー調査会原子力安全・保安部会原子力防災小委員会『原子力施設における内部脅威への対応について』（2005 年６月）において、「核物質防護対策を真に実効あるものとするため」、原子力施設における内部脅威対策の検討を行っている。この検討の結果として、分野横断的な信頼性確認制度の創設及び現行制度で可能な信頼性確認措置について、それぞれ引き続き検討することとしている。

（4）政府及び政府契約企業における情報保全の在り方

政府機関及び政府契約企業等、国家の重要情報を知り得る者が守るべき情報保全のための措置について、我が国では、防衛省の装備品の調達に係る契約企業に対しては、契約に基づき秘密保全が義務付けられているが、あくまで防衛秘密等の秘密保護法制の対象企業に限定されるものであり、広く防衛調達企業以外の安全保障技術を保有する企業をスコープとしたものではない[103]。

米国では国防省の「国家産業保全プログラム運用マニュアル」に基づき情報保全のための総合的な対策を講じているところ、我が国においても同様の総合的な保全対策の在り方を検討すべきである。

（参考）国家産業保全プログラム運用マニュアル（NISPOM）について

米国国防総省（DOD）は、政府契約企業が政府の機密情報を確実に保全するため、国家産業保全プログラム（NISP：National Industrial Security Program）に基づき、本運用マニュアルを策定した。

本運用マニュアルでは、施設及び人的セキュリティ・クリアランス、情報の機密区分及びマーキング、訪問及びミーティングへの対応等、機密情報保全のための取り組むべき総合的な要件が示されている。

なお、我が国においても、防衛省の装備品の調達に係る契約企業に対しては、契約に基づき秘密保全が義務付けられているが、あくまで防衛秘密等の秘密保護法制の対象企業に限定されるものであり、広く防衛調達企業以外の重要情報を保有する企業を対象としたものではない。

NISPOM の内容

・Chapter 1. 通則
  Section1. イントロダクション
  Section2. 一般要件
  Section3. 報告要件
・Chapter 2. セキュリティ・クリアランス
  Section1. 施設クリアランス
  Section2. 人的セキュリティ・クリアランス
  Section3. 外資系企業
・Chapter 3. セキュリティトレーニング及びブリーフィング
  Section1. セキュリティトレーニング及びブリーフィング
・Chapter 4. 機密区分とマーキング
  Section1. 機密区分
  Section2. マーキング要件
・Chapter 5. 機密区分情報の保護
  Section1. 一般保全要件
  Section2. 管理及び実施義務
  Section3. 保管及び保管設備
  Section4. 伝達
  Section5. 公開
  Section6. 複製
  Section7. 廃棄
  Section8. 建造要件
  Section9. 侵入探知システム

[103] 防衛省契約企業に対しては、財団法人防衛調達基盤整備協会が防衛装備品の生産等に関する情報保全に係る講習及び施設保全調査を行っている。

・Chapter 6. 訪問及びミーティング
　Section1. 訪問
　Section2. ミーティング
・Chapter 7. 下請関係
　Section1. 次委託事業者の責任
・Chapter 8. 情報システムセキュリティ
　Section1. 責任及び義務
　Section2. 証明及び認可
　Section3. 一般要件
　Section4. 保護手法
　Section5. 特別分野
　Section6. 保護要件
　Section7. 相互システム
・Chapter 9. 特別要件
　Section1. 制限されたデータ及び過去に制限されたデータ
　Section2. 国防総省重要核兵器設計情報
　Section3. 諜報情報
　Section4. 通信セキュリティ
・Chapter10. 国際的セキュリティ要件
　Section1. 一般及び背景情報
　Section2. 海外利益となる米国情報の公開
　Section3. 海外政府情報
　Section4. 国際取引
　Section5. 国際的訪問及び外国人の管理
　Section6. 契約者の海外活動
　Section7. NATO 情報セキュリティ要件
・Chapter11. その他の情報
　Section1. テンペスト
　Section2. 防衛技術情報センター（DTIC）
　Section3. 研究開発活動の独立

委員のコメント（概要）：政府における情報管理

○ 国家安全保障上の重要技術情報については、政府における統一した管理基準を設ける必要があるのは当然である。

○ 内部統制や情報管理が機能している企業は、机周りが非常に整理されているが、各省庁は机が書類だらけであり、外部者としては目をつむって歩く必要があるかと思ってしまう。それで情報管理の取組が進んでいると言われても疑問である。情報管理の観点からすると、我が国の役所の執務スペースはあまりにも狭すぎるのではないか。

○ 政府内部に厳格に守るべき情報があるのは明らかであるから、適切に情報管理が機能しているか、制度的に第三者機関にチェックをしてもらう仕組みが必要ではないか。

○ 情報管理に当たって、関係省庁間の相互牽制の仕組みが必要ではないか。

○ 情報漏洩時の罰則が低く、これが公務員の情報管理に意識の低さにつながっている。

○ 機密情報へアクセス権を有する者に対するバックグラウンド・チェックをできる仕組みが必要ではないか。併せて、機密情報を保有している者に対する定期的なモニタリングが必要ではないか。

○ 機密情報はレベルに応じて管理方法が違うはずであるのに、企業が提出する重要情報も、全て国家公務員法上の守秘義務の下で管理されることが問題。

○ 外交・防衛・警察に関する情報のみならず、非国家的脅威やサイバー攻撃等に関しても安全保障上の脅威として扱っていく必要があるため、外務省や防衛省が持っている機密情報管理体制を各省庁に広げていく必要がある。

○ 政府における機微情報の管理について、議会がこれを指導する場合には、当該案件を審議する委員会において、機微情報の秘密義務及び違反した場合の厳重な罰則を規定する必要がある。

○ 政府情報の漏洩につき、刑事罰に関して警察が捜査する際には、各省が持っている重要情報について警察に知らしめるような仕組みが必要であり、エンフォースメントの在り方も同時に考えていく必要がある。

○ 情報漏洩に対し、刑事罰で担保することだけではなく、内部統制や内部規律の確立を中核として考えるべき。

○ 国が保有する情報の管理と企業が保有する情報の管理は異なるべき。政府が保有する情報は、国民主権の観点から取材・報道の自由に配慮し透明性を高めるべきであり、時期をずらした公開についても検討されるべき。

技術情報等の適正な管理の在り方に関する研究会
委員名簿

安念　潤司	中央大学法科大学院教授
太田　文雄	防衛大学校安全保障・危機管理教育センター長
影山　正	クロール・インターナショナル・インク リージョナル・マネジング・ディレクター　日本/韓国
後藤　啓二	後藤法律事務所　弁護士
武田　圭史	慶應義塾大学大学院政策・メディア研究科教授 カーネギーメロン大学日本校客員教授
中馬　宏之	一橋大学イノベーション研究センター教授
◎土肥　一史	一橋大学大学院国際企業戦略研究科教授
畑村　洋太郎	株式会社畑村創造工学研究所　代表取締役　東京大学名誉教授 工学院大学グローバルエンジニアリング学部機械創造工学科教授
林　紘一郎	情報セキュリティ大学院大学副学長兼セキュアシステム研究所長
古川　勝久	独立行政法人科学技術振興機構社会技術研究開発センター 主任研究員
牧野　二郎	牧野総合法律事務所　所長　弁護士
丸島　儀一	キヤノン株式会社　顧問　弁理士 金沢工業大学大学院知的創造システム専攻教授
山田　敦	一橋大学国際・公共政策大学院教授
吉川　良三	東京大学大学院経済学研究科ものづくり経営研究センター 特任研究員
渡部　俊也	東京大学先端科学技術研究センター教授

（敬称略、50 音順、◎：座長）

検討経過

第１回
　日時：平成１９年１０月２３日（火）
　議題：論点について

第２回
　日時：平成１９年１１月３０日（金）
　議題：安全保障の視点

第３回
　日時：平成１９年１２月２１日（金）
　議題：技術情報とイノベーション

第４回
　日時；平成２０年１月２５日（金）
　議題：企業における情報管理

第５回
　日時：平成２０年２月２８日（木）
　議題：企業における情報管理

第６回
　日時：平成２０年３月３１日（月）
　議題：大学における情報管理

第７回
　日時：平成２０年４月２１日（月）
　議題：中小企業からの技術流出への対応
　　政府における情報管理
　　非公知情報の保護の在り方について

第８回
　日時；平成２０年６月２４日（火）
　議題：報告書（案）について

第９回
　日時：平成２０年７月８日（火）
　議題：報告書（案）について