CISTEC journal

2014.11
No.154

CISTEC 一般財団法人 安全保障貿易情報センター
Center for Information on Security Trade Control

〈1〉大学が震撼する日

―今そこにある、大学発の懸念国での大量破壊兵器開発、軍拡促進リスク

CISTEC　専務理事　**押田　努**

1　はじめに

大学での安全保障輸出管理については、平成17年4月に経産省、文科省から大学、研究機関向けに輸出管理の強化に関する要請が初めてなされ、更に平成18年3月には不正輸出事件の続発を受けた経産省からの大臣通達、文科省からの事務次官通達が発せられました。そして、平成19年の知的財産推進計画、同20年の総合科学技術会議決定などの政府決定においてその必要性が謳われ、以降、大学関係者によって、積極的な取組みが進められてきています。産学連携学会や国際・大学知財本部コンソーシアム（UCIP）等の関係団体によるガイダンス、モデルCPの作成や各種の啓発活動や、九州地域内大学輸出管理実務者ネットワークのような地域での問題意識や取組事例の共有など、取組みは幅を広げてきています。

そのような取組みが進む一方で、現行の外為法に基づく輸出管理制度・運用が、大学での輸出管理にそぐわない点や輸出管理だけでは足りない点などについての問題意識も同時に醸成されてきており、それが今年6月に関係6団体連名で経産省、文科省、外務省の局長級宛てに提出された包括的改善要請書や、国大協から9月に提出された要請書となって表れてきていると思います。

大学は、産業界と異なり、組織的な上から指示命令による運営はなじまない面があることは確かです。研究、教育の自由があり、「知の拠点」として、新たな知見を研究、発見し、それらを世の中の公共財として発信していくのが大学に期待されている役割でもあります。したがって、企業のように、新たな知見は特許や企業秘密として独占、有償提供するというものとはベクトルが異なり、基本的には公開、自由利用というのが基本的なベクトルとなっています。近年は、産学連携による共同研究開発や、大学発ベンチャー等も積極的に推進されており、状況が少し変化してきてはいますが、基本的ベクトルに変化があるわけではありません。

このため、各大学での取組みは進められてきてはいますが、各大学内で、輸出管理担当部門と各々の研究者との間での問題意識や必要性の認識の程度の濃淡はあるのではないかと思われます。このような問題意識、認識の濃淡は、組織的管理統制が可能なはずの企業においても見られます。経営幹部や上司の無理解を嘆く声は、依然として少なからずあり、しばしば「何か事件が起きれば引き締まるのに……」という冗談ともつかぬ会話がなされることもあります。たしかに事件が起きれば引き締まるのでしょうが、しかし、往々にして事件後に生じるのは、規制の強化です。該非判定を間違えたというミスであれば、実害が生じていない限りそう問題になるわけではありませんが、安全保障輸出管理のルールを破り、それによって我が国や国際的な平和と安全保障を脅かすような事態が生じたか、あるいは生じるだろうと受けとめられるような不正行為であれば、それに対する社会、政治、行政からの「指弾」は容易ならざるものとなり、しばしば言われるように、「企業の存亡に関わる」ことになりかねません。それが過失によるものだったとして、実害が生じれば、同様の「指弾」にさらされます。

もちろん、「不正輸出事件」というだけで条件反射的に誇大な？報道をしがちなマスコミに問題がないわけではありませんし（押田努「マスコミ報道に際して期待したい留意点」CISTECジャーナル2012年11月号、No142所収）、当局からのものも含めてそれらの「指弾」がすべて正当なものかといえば、

必ずしもそうとは言えない場合もあります。行政は理解していても、政治とマスコミが過大に反応しているということもあり得ることです。しかし、いったん火がつけば、それを消火することは容易ではありませんし、消火が即ち企業の倒産ということは、食品安全その他の世界では実際に生じていることです。

産業界は、安全保障輸出管理に取り組んできた長年の経験から、次のような教訓を得ています。

①国際社会からの指弾
安全保障に関する国際政治の中でいったん問題視されれば、往々にして、法律違反かどうかは関係なくなる。平和と安全を損なったと受けとめられれば、厳しい批判にさらされる。

②社会的評価のダメージ
いったん不正輸出の嫌疑をかけられると、マスコミによる長期間の報道で、企業の社会的評価に大きなダメージを受ける。商談、株価等へも影響する。

③全部門の活動への影響
輸出管理の対象製品は少なくても、いったん不正輸出事件を起こすと、関税当局からもコンプライアンスの実効性を問われ、全社的な国際物流部門に多大な影響。

これらは、大学についても潜在的には当てはまる点です。

日本の産業界の場合は、このような経験に立って、単に「外為法の法令遵守」だけで事足りるとしているわけではありません。グローバルな国際展開をする企業であれば、現地の国の法令を遵守することは当然として、広く域外適用される米国法（しかも、輸出管理規則のEARだけでなく、経済制裁を担うOFAC（財務省外国資産管理局）の一連の規則や各種制裁法等）をフォローすることは日常的な基本作業となっています。輸出管理を行う基本的スタンスとしても、「法令上に規定されていることを遵守する」という範囲に留まるのではなく、法令の有無に関わりなく、「自社の社会的信用を損なようなことはしない」というものが柱になっています。

考えてみれば当然の話ではあります。常識や良識に期待できることは、法律で決めるまでもありません。政治家がしばしば、「法律では禁止されていないから、問題ない」という抗弁を堂々と行うことがありますが、それはおよそナンセンスな話であり、政治を志すような人間であれば、少なくとも社会での平均的な常識は持ち合わせているだろうということが立法の前提となっています。しかし、「法律で禁止されていない」ことを盾にとって、自らの行為を正当化するようでは、政治不信を招くことは必至です。

それと同様で、大学における安全保障輸出管理も、広義には、単に外為法だけの世界ではありません。普遍的な「科学技術を、懸念国家やテロリストの懸念用途に使わせない」というものが上位の価値としてあって、そこから外為法を含む諸々の規範の遵守が求められるというのが全体の管理の構図になると思います。

大学が定めている学術憲章では、その趣旨が盛り込まれています。例えば、ある大学では、次のような条項がありますが、同趣旨の規定は他大学にもあることでしょう。

「科学が自然環境と人類の生存とに重大な影響を与えることをつねに顧慮し、自らの良心と良識とに従って，社会の信頼に応え得る研究活動の遂行に努める。」

「大学の理念としての真理探求の精神を堅持すると共に、その研究活動を通じて，長期的な視野のもと、人類の福祉と文化の発展，ならびに世界の平和に貢献してゆくべく努める。」

世界最先端のハイテク研究の拠点である日本の大学には、注目が集まっています。懸念国からは狙われ、それが世界の平和と我が国の安全保障への脅威となって跳ね返ってくる可能性は、多分にあります。産業界の関係者が、「何か事件が起きれば引き締まるのに・・・」と呟くことがあると書きましたが、今回の記事では、それを大学に当てはめた場合、どういう事例が想定しうるのかについて、いくつか書いてみたいと思います。そしてそれらの事例の参考になる事実についてもご紹介してみたいと思

います。それらの事例は、外為法違反に当たるものもあれば、当たらないものもあります。大量破壊兵器の開発や、通常兵器の革新につながるような先端技術の、大学からの流出パターンには様々なものがあるということです。

ここで書く事例は、フィクションです。フィクションではありますが、実際に、筆者やCISTEC関係者が見聞きした実例に基づき（大学関連だけでなく企業関連の事例もあります）、一定の脚色をしたフィクションです。ですから、これらの事例は、もしかすると明日にも起こるかもしれません。それが起これば、その当事者である大学は激震に襲われる可能性が大きいですし、大学幹部の責任問題に発展する可能性が多分にあります。

実際に事件が起きてからそれを教訓に引き締めるというのでは不幸であり、起きるかもしれないことを想像して、そうならないように対処するということが望ましいのは言うまでもありません。そういう対処のための材料としてお役に立てば幸いです。

2　大学で起こり得る仮想事例

【仮想事例１】「国立大学教員が北朝鮮のミサイル、核実験に協力していた」

国立のある有名大学の教員は北朝鮮籍であるが、日本で生まれ、日本人同様に教育を受けた在日三世である。朝鮮総連傘下の祖国への科学技術面での貢献を旨とする科学技術協会（科協）のメンバーであり、北朝鮮のミサイル発射や核実験の前後に、頻繁に海外出張していた。警察庁などは、科協は対日有害活動の懸念があり、警戒対象としている。

同教員は、北朝鮮や第三国で関係者と接触し、ハイテク技術を提供し、北朝鮮のミサイル発射や核実験の成功や高度化に寄与していた。警察は、薬事法その他の様々な法令違反事案における家宅捜索により、科協メンバーの名簿を押収していると言われており、押収したパソコンの記録から渡航目的が判明したため、任意同行を求め事情聴取したところ、北朝鮮側への技術提供を認めたので、逮捕に至った。この大学は、旧帝大系の国立大学であるだけに、その社会的衝撃は大きかった。

大学側は、出張を含めて研究者の自由に任せており、特に大学が受け入れている研究費の使用を伴わないような場合には、出張目的等についてチェックする仕組みがなかった。

【仮想事例２】「居住者扱いとなった留学生に提供した技術が核・ミサイル開発に使われた」

Ａ大学の大学院教授は、外為法上、核、ミサイル関連技術として規制されている研究を行い、未発表の機微技術を研究室の留学生にもアクセスできるようにしている。同教授は、来日後６カ月が経過すれば「居住者」となり、外為法の国内の技術提供規制（みなし輸出規制）は適用されないとおおまかに思っていた。ところが、留学生といっても様々で、個人の資格で来た者もいれば、自国の勤務先から派遣されてきている者もいるということで、必ずしも、一概には言えないということの認識が十分ではなかった。

Ｂ留学生は、外国ユーザーリストにも掲載されている研究所に勤務経験があるが、退職して個人の資格できており、また来日後、語学研修等で６カ月経過していることから、特に留意することなく、留学生を機微なハイテク研究にタッチさせていた。ある日、某懸念国での核・ミサイル関連技術が大きな進展を見せたらしいと報じられ、それがＢ大学の研究室の技術が使われたらしいとの報道がなされた。研究室に来ていた複数の留学生が関与しているらしいとのことだった。

同研究室の教授は、外為法上の管理が面倒臭いと考え、ともかく６カ月経ったら制約なく留学生を研究に従事させることができると割り切っており、その研究室の技術が懸念国において、どういう軍事的波及を与え得るのか、という点に思いを十分致していなかったことが判明し、批判を浴びることになった。

【仮想事例３】「知財推進で供与した先進技術が、近隣国の軍拡に使われた」

知財立国の旗印の下に、大学の知的財産の活用が推進されているが、Ｃ大学では、その一環で、大学が保有する特許技術を国内外を問わず積極的にPRしていた。大学に対する交付金や補助金も減少しており、それを補うためにも、知財活用による収入は貴重な財源確保策であった。そういう中、米国企業から、先端的な電子関連特許のライセンス供与の依

頼があった。併せてその技術の適用に関するアドバイスの依頼もあった。オファーされた金額は高額で、収入源として魅力的に思えた。

もともと、特許技術は公知のものであり、外為法では技術移転許可対象にはなっていなし、その関連のアドバイスであれば、特に問題とはならないだろうと考えた。そのオファーのあった米国企業の役員の一人が東アジア系らしき名前であったことには気が付いたが、米国企業であるし問題はないと判断し、ライセンス供与と関連の技術アドバイス契約を結び、役務供与した。その年の大学の知財収入は大幅に伸び、知財活用のモデル例として高く評価された。

……が、ある日、香港の新聞報道を知り愕然とした。あの供与した先進IT関連の特許技術が、軍備増強著しいD国のハイテク装備に使われたらしいというのだ。供与した先の米国企業は、実はD国の企業の資本下にあり、同社が得た情報は本国にすべてシェアされていたことが後に判明した。D国が補強すべき技術分野のひとつとしてその技術が位置付けられていたことを知った。その大学教授らによる技術アドバイスは、特許技術からはみ出る部分もあったので、外為法で許可対象となるはずの技術提供行為だったが、そういう認識は持っていなかった。

【仮想事例４】「中国人教授が、人民解放軍系研究所と軍事関連共同研究を行っていた」

E大学は、国際化は当然の流れであり、内外から広く人材を求めるとの理念の下、教員も文系理系を問わず、外国人教員を多数採用している。そして研究・教育活動も、できる限りそれら教員の自主性に委ねている。研究費も、国からの補助金等だけでは賄えないため、内外の様々な組織との共同研究を積極的に推奨している。

F教授は、理系研究室を主宰し、先進技術研究をしている中国人の教授である。同教授は、様々な共同研究をこなしているが、その中に中国の研究機関との共同研究があり、内容は航空分野に関するハイテク研究であった。その研究機関は、人民解放軍とも関係のある組織であり、その共同研究も解放軍の軍備増強の一環として位置づけられるものだった。

E大学では、安全保障輸出管理のことは聞いたことはあるが、基本的には各教員の自主性に委ねていたし、大学が行っている研究は、規制対象外の基礎科学分野の研究だと漠然と捉えていたために、特に大学当局として十分なチェックをするということはなかった。

同大学が、日本にとって脅威となりつつある中国の軍備強化に貢献するような共同研究を行っていたということはマスコミで大々的に報じられ、社会から指弾された。それに伴い、大学のイメージは悪化し、もともと学生数も小規模な中で受験者が激減、国からの研究費も減らされ、大学としての存立に関わる事態となってしまった。

【仮想事例５】「米国政府から突然、大学が経済制裁対象として指定されてしまった」

ある日、米国政府が、日本国内でも有数のG大学を、経済制裁対象として指定したと発表した。G大学としては青天の霹靂で、何が起こったのかわからず、マスコミも殺到し、大混乱となった。経産省も事情聴取に動き出し、警察当局も関心を見せ始めた。

弁護士を米国当局に派遣し、指定理由を探ったところ、どうやら、同大学のH教授が、テロ支援対象として指定しているイランの研究所の研究者と海外で接触し、機微な技術を教えていたらしいことが判明した。米国では、EARによる米国原産製品・技術の輸出管理規制や、米国財務省（OFAC）による経済制裁を科す規制（SDNリスト＝国連制裁国、米国禁輸国、テロ支援国の政府関係機関、関連企業等の企業・個人のリスト。米国人の接触禁止）があり、米国原産品や米国人向けの規制だから、あまり関係ないと思っていた。しかし、米国では、それ以外にも、イラン・北朝鮮・シリア不拡散法のように、個別の懸念国を対象に、大量破壊兵器開発等を支援するような行為を行った者に対して、米国人・法人以外も含めて制裁を発動する個別制裁法があるとは全く認識していなかった。

制裁対象となったことによって、米国の政府、組織、個人等は取引ができなくなるため、米国の大学との研究交流や留学生の相互受入れ等の活動が停止されてしまい、窮地に陥ることとなった。制裁対象指定理由、行為が明確にわからず、弁明や解除の手続きもよくわからないため、困惑するばかりである。同大学の輸出管理部門では、教員、研究者らが

海外出張する際には、携行品が輸出規制対象ではないかの注意喚起は行っているが、海外での活動については研究活動として特に把握はしていない。

【仮想事例６】「研究交流協定を結んでいる中国の大学による軍事技術開発に、当方の技術が使われてしまった」

大学の国際化の一環で、海外の大学と研究交流協定を結ぶことは一般的である。独立行政法人の研究機関でも海外諸国の研究機関と包括研究協力協定を結ぶ例が少なくない。こういう状況も踏まえ、Ｉ大学では、米国、欧州、中国、東南アジアのいくつかの大学と協定を結び、幅広く研究交流を行っている。中国で交流協定のある大学は、経産省が出している外国ユーザーリストには掲載されているが、同リストは取引禁止リストではないし、基礎科学研究は規制対象外であるとの認識の下、共同研究や留学生の受入れを続けていた。民生分野の研究であることから、特に問題があるとの認識はなかった。

しかし、どうやらその共同研究の成果が、中国の軍備近代化に貢献しているらしいことがわかってきた。その研究分野は、人民解放軍が、デュアルユース戦略上の重点分野のひとつであることや、リスト非該当分野であっても、中国ではハイエンドの電子部品などを作るノウハウを持っていないために、それらの技術、ノウハウを取得する手段として、民生分野の研究協力を利用していたらしいことがわかってきた。

また、日本の輸出管理関係者に聞くと、安全保障輸出管理上、最新のハイテク技術分野が規制対象になるまでは、かなりのタイムラグがあるために、単にリスト規制の該非判定だけをしていればいいわけではなく、該非に関わらず用途、需要者の懸念についての審査の重要性は、産業界では広く認識されていることもわかってきた。

【仮想事例７】「海外校に派遣した教員が、無許可技術提供の嫌疑で立件された」

Ｊ大学では、大学の国際化の一環として、海外校を設置したり、海外の姉妹校に教員や研究者を派遣したりしている。海外に出れば、その国の法令に従うことが基本であり、日本の法令が適用されることはないと漠然と考えていた。

そのような認識の下に、同大学から派遣された教員は、海外キャンパスの大学院で、国際レジームで規制対象となっている機微な研究内容（未発表）を当地の院生に教えた。これが某国情報機関の耳に入ったらしく、その機微度や情報が流れた相手方、利用のされ方等が問題視され、日本の経産省に通報されたため、同教授は同省から事情聴取を受け、外為法違反容疑により警察からも強制捜査が入った。

同大学や派遣された教授は、日本の外為法で規制対象となる「居住者」が、大学の身分を残したまま、同大学の活動のために海外に派遣される場合も含まれることや、海外においても技術提供行為は規制対象になることについて十分認識しておらず、漠然と、出国したから「非居住者」となるので外為法はもう関係ないと思い込んでいた。そして、海外キャンパスでも、様々な「留学生」「研究者」がいることに思いが及んでいなかった。

【仮想事例８】「論文発表した遺伝子研究内容が、懸念国の生物兵器開発に使われた」

遺伝子研究を進めているＫ大学のＬ教授は、難病の遺伝子治療法について新たな研究結果を論文発表し、注目された。これは、難病に影響していると考えられる特定の遺伝子のみに効果を与える手法を開発したもので、これまで治療が難しいとされてきた難病でも対応できる可能性が出てきた。

しかし、一方で、この手法を使えば、例えばある特定の遺伝子を共通に持つ民族をターゲットに攻撃する遺伝子攻撃兵器を作ることも可能となってくるため、悪用懸念を指摘する声も出てきた。この研究の推進に当たっては、近隣アジア諸国の関係大学や研究機関と研究協力協定を結び、情報や研究成果のシェアを行ってきた。それらの研究協力国のある国の軍関係者にこれが遺伝子兵器の原理として注目されているとの情報が伝えられた。

バイオ分野では、合成生物学による絶滅ウィルスの人工的合成、人工ゲノムで合成した細菌の増殖等、ワクチン生産、バイオ燃料の効率的生産などの民生分野で役立つ一方で、テロ悪用懸念も真剣に議論されるようになってきている。2004年に全米科学アカデミーで発表されたフィンクレポートで、この点の警告と取組みの提言がなされ、続いて2007年に王立オランダ科学アカデミーが作成した、バイオセ

キュリティ行動規範など、科学界の中で、安全保障と自由な研究活動の両立を図る努力がなされてきている。また、2012年には、WHOがトリインフルエンザに関する貴重な２編の研究論文の学術雑誌発表を止めるよう勧告している。この論文は人工的にウィルスを変異させ、ヒトへの感染能力を持たせる可能性を研究したもので、将来の流行に備えたワクチン開発に役立つと研究者たちからは評価されていた。しかし、テロリストにバイオ兵器を持たせる可能性があるとして公開差止めを勧告したものだった。しかし、L教授らには、このような懸念が自らの研究にも当てはまるとの認識がなく、また大学としてもこのような観点からのチェックが十分に行われないままに、今回の論文発表となった。

【仮想事例９】「防衛省との共同研究内容が、大学経由で近隣懸念国に漏れていた」

防衛省では、2014年春に、長年維持されてきた武器輸出三原則に代わり、新たに防衛装備移転三原則が決定されたことを受け、2015年より防衛装備庁を新たに発足させた。同庁では、民間の優れた技術を積極的に防衛装備に取り入れるとの方針の一環として、大学との共同研究を推進することとした。大学では、まだ「軍事研究」にアレルギーを示すところもあったが、201X年頃になってくると、平和と安全への貢献の観点のみならず、研究費の確保という実利的観点の必要もあり、防衛省との共同研究を行う大学も目立つようになってきた。ノーベル賞を受賞した中村修二氏が、米国籍を取得した理由として、「機密を要する軍の研究費を得ることにより研究室予算を確保するため」との旨をインタビューで述べたことが、関係者にインパクトを与えた面もある。

が、M大学において、その機密保持義務をかけた共同研究の内容が、近隣懸念国に漏れていたことが判明した。それまで、防衛産業の企業であれば、機密保持体制は堅固なものであり、社内でも完全なファイアーウォールがあって、機密が漏れることはめったになかった。しかしそういう中でも、孫請けに入った朝鮮総連傘下の企業を通じて情報が漏れたことがあった。今回漏洩のあった大学の研究室では、防衛省との共同研究のデータの管理体制は十分なものではなく、留学生が比較的自由に出入りできるようになっていたために、データを抜かれてしまったようだ。防衛省としても、大学との共同研究体制の見直しと整備を急ぐ契機となった。

【仮想事例10】「研究室の研究データを、丸ごと盗まれ近隣国に流出してしまった」

N大学大学院のO教授の研究室では、産学連携の一環として、防衛関連企業との共同研究を秘密保持契約の下に行っていた。ある日、研究室のパソコンからデータがコピーされた痕跡があることに気が付いた。そのパソコンには、共同研究のデータや共同研究先の企業から得た秘密データが入っており、今後特許を出願する上でも重要なものだった。が、数ヵ月後、近隣国で、同研究を踏まえたものと思われる特許出願がなされていたことが判明した。

共同研究先の企業は事態を重く見て、経過の徹底調査と管理上の過失による損害賠償請求の動きが出てきた。技術データを窃取したり流出させたりする行為は、不正競争防止法が平成21年に改正され、不正競争行為のひとつとして追加され、刑事罰の対象となった。しかし、前提として、そのデータがきちんと秘密扱いとして指定され、他からアクセスができないよう然るべく管理がなされているという秘密管理性が前提だった。ところが、同研究室では、秘密管理が十分ではなく、秘密指定もせず、物理的にも研究にタッチしない院生や留学生が出入りできる場所に不用意に置いてあった。このため、不正競争防止法による立件は難しい一方、管理上の賠償責任を問われるという事態になってしまった。

(注) 経産省では、産業スパイ対策を強化するため、不正競争防止法上の「営業秘密」の要件を緩和すべく、本年12月にも管理指針を改定する旨報じられている（読売新聞2014年10月29日付他)。

【仮想事例11】「サイバー攻撃により、ハイテク研究データを丸ごと盗まれてしまった」

P大学では、工学系大学院のある研究室で、特許取得を前提にハイテク研究を進めていた。その研究は軍事応用可能性もあるものだった。ある日、そのHPが書き換えられたという事件が発生したことを契機に、大学内のIT関係のセキュリティチェックが行われた。その結果、同研究室が使用しているサーバーに侵入の痕跡が発見され、ハイテク研究の

データ全体に不正アクセスされていたことが判明した。

同大学では、学部横断的にIT関係の管理は行われておらず、セキュリティ上問題となりうるサーバーや端末、ソフトの管理等はバラバラで、不要なソフトも更新されないまま、研究室のパソコン等に残ったままだった。サーバーへの侵入ルートは複数あることが判明した。ひとつは、未更新ソフトのセキュリティホールを悪用して侵入したものだった。便利な無料ソフトをダウンロードしたときにおまけで付いてくるソフトを一緒にダウンロードし、ダウンロードしたことさえ認識しないまま放置していたものだった。もうひとつは、標的型攻撃メールによる侵入だった。海外の学会に参加した時に多くの参加者と名刺交換したが、しばらくした後に「学会参加者向け追加補足資料の配布の件」との英文タイトルでメールが送られてきたため、何気なしにメールに書かれているリンクをクリックしたが、内容は関係ないものだった。変だなとは思ったが、そのまま忘れてしまったが、それによってパソコン経由でウィルスがサーバーに侵入し、データにアクセスされたものだった。

企業や官庁では被害が続いたため、万全の対策をとっていたが、同大学では当事者意識を持たないまま、警告やIT回りのきめ細かい管理をしなかったことによって、被害に遭ったもの。盗まれた研究データを利用した軍備ハイテク化のブレークスルーがなされたらしいと報じられたのは、それから１年後だった。

【仮想事例12】「近隣国で名誉学位を受け技術提供していた研究者が、外為法違反で逮捕された」

Q大学の研究者Rは、この２－３年、近隣国への出張が目立つようになった。その研究内容について、大学で講演してほしいとの依頼が発端で、その後、先方の大学とハイテク製品設計製造に関する共同研究を行うまでになった。当初は、既に論文発表した内容をわかりやすく講演するだけだったが、次第に未公表の研究内容も紹介するようになっていき、共同研究ではかなり細部に亘る研究データも提供するようになった。それらの出張旅費や講演謝金、共同研究費は、すべて先方の大学持ちであった。このため、大学の輸出管理部局も、お金の支出を伴わないということで、ノーチェックだった。

その近隣国は、非ホワイト国であるが、大学は特に外国ユーザーリストにも掲載されておらず、教授も外為法の規制の存在は漠然とは知っているつもりだったが、論文で公表したり、特許取得済みのものだったり、公知のものの説明が中心だったこと、また、大学での研究であれば、基礎科学研究として規制除外されるだろうと漠然と考えて、特に外為法の許可対象になり得る可能性については深くは考えなかった。

他方で、同大学からは、教授の貢献に対して、名誉学位を授けられ、今後とも同大学からの資金拠出による継続的な共同研究を依頼されていた。このような資金と名誉に訴える手法は、2008年に逮捕され実刑判決を受けた米国テネシー大学ロス教授の事例が典型的だが、大学当局はその教訓を生かすことはなかった。

【仮想事例13】「名誉教授が、中国の外専千人計画で招聘され、軍需産業に協力していた」

S大学のT教授は、定年で退職し、名誉教授となったが、もともとハイテク分野で優れた研究者であった。中国は、この数年、核、宇宙、軍需産業を含めて、弱い技術分野のブレイクスルーを目的として、海外ハイレベル人材招致千人計画や外国人専門家千人計画により、多数の外国人専門家を高待遇で招いている。日本人も多数含まれていると言われている。そういった中、大学に勤務していた頃から研究交流で中国と行き来のあったT教授は、退職を契機に声が掛かり、中国で研究を進めることとなった。日本での研究環境と比べれば天地の差であり、自分の研究者としての能力を高く評価してくれることは喜びでもあった。かくして、同教授の研究は中国で一段と進歩を見せたものの、それは中国の宇宙、ミサイル技術の質的向上に直結するものであった。既にS大学を退職しているにも拘わらず、マスコミでは「S大学名誉教授が中国の軍拡に協力」と報じられ、同大学の社会的評価を貶めることになってしまった。

ちなみに、同教授は、中国の研究所に雇用されていたので、外為法上は「非居住者」であり、外為法による技術提供規制の適用対象外であった。

【仮想事例14】「原子力関連の出願特許情報をもとにして懸念国が核開発を進展させた」

原子力発電は、福島事故以降、一時よりも比重は低下したものの、今後も一定割合が維持される見通しであるほか、海外向け輸出可能性は大きく拓けているし、核燃料サイクルの確立に向けた取組みも進められている。

U大学でも内外から学生を確保し、大学院研究室の維持を図り、原子力政策を技術的側面から支えるべく努力している。研究基盤を維持するためにも、特許を積極的に取る方針で、研究成果は逐次、特許出願している。改良研究も含めて特許取得している。

ある日、このU大学の一連の特許技術を使って核関連研究が行われているらしいとのニュースが飛び込んできた。特許技術は、出願すれば1年半後には公報に明細書含めてすべて公開され、成立すれば特許公報に掲載される。実施可能な最良ケースを記載するのが原則であるため、その手順通りに実施すれば再現は可能なはずである（実際には若干のノウハウが必要な場合も少なくないが）。某国では、日本の特許情報を組織的に集め、それをフル活用していた模様である。日本の特許公報には、原子力関連の特許技術が多数掲載されており、懸念が大きいとの指摘もなされていた。

かつての紙公報の時代には、日本の特許庁まで来て紙公報をめくってコピーするという牧歌的時代だったが、いまではインターネットで瞬時に全世界誰でも検索し、入手できるようになっている。それを利用して、産業技術が流出し、更には大量破壊兵器開発、通常兵器革新につながるような技術も、瞬時に共有されるようになってしまった。U大学の研究室では、次世代原発の開発、核燃料サイクルの確立という国の政策を踏まえて、あくまで平和利用のために研究に取り組んでいたのだが、こういう結果になったことに臍をかんでいる。

3　仮想事例の参考となる事実

【事実1】中国は、5カ年計画において、軍民融合による国防強化と軍隊の現代化を目標として掲げ、軍需企業集団、大学において軍事関連技術の開発を行っている。

⇒（参照）（独）科学技術振興機構HP内SPC（Science Portal China）サイト掲載の「第12次五カ年計画」第15編「軍民融合　国防強化と現代化」、
CISTEC「対中国輸出管理入門－中国顧客情報収集・分析の手引き」
同　「軍事転用・拡散顧客情報分析ガイド－中国の軍及び軍需産業の構造と軍事四証制度 －」

【事実2】警察庁は、毎年の警察白書等で、北朝鮮、中国、ロシアについて、大学での研究者、留学生も関係する対日有害活動について警告している。

⇒（参照）「警察白書」（「対日有害活動の動向と対策」の項目）

【事実3】世界各地で、大学や研究機関を舞台に技術流出事件が頻繁に発生している。

⇒（参照）本号の加藤もえ「【参考資料】最近海外メディア等で報道されている大学・研究所関連の違反事例」

【事実4】米国政府が大量破壊兵器開発、テロ等関与の疑いで取引・関与を制限・禁止しているEntityリスト、SDNリストには、イラン、中国、北朝鮮その他の大学・研究機関が相当数掲載されている。

⇒（参照）米国商務省Entityリスト、米国財務省SDNリスト

【事実5】米国防総省国防保全局（DSS）が発表した諸外国による米国機微技術情報収集・調達活動についての分析報告書によれば、その手口としては、「大学を利用した情報収集」が、地域を問わず、1～2位と上位に来ている。

⇒（参照）本号の風間武彦「狙われる米国の機微技術―諸外国の対米情報収集活動の動向―」

【事実6】中国、北朝鮮の在日科学者組織には大学院生も多く、組織的に日本のハイテク技術情報収集の場となっているとの指摘がある。

⇒（参照）本号の野村旗守「近隣諸国の対日有害活動の実態について―様々な手法で狙われる日本の

最先端技術」

【事実７】米国議会の米中経済安全保障調査委員会（USCC）は、「中国のスパイ活動は米国の技術に対する唯一最大の脅威である」（2007年）、「全世界の無数のコンピューター・システムが侵入の対象となっており、そのうちいくつかは中国政府又は中国軍によるものと思われる」（2013年）旨述べている。

⇒（参照）米国大使館HP、防衛省HP内「米中経済安全保障調査委員会報告書」

【事実８】米国テネシー大学事件の背景と顛末

2008年、米国テネシー大学のロス教授が、中国人大学院生に、無許可で国防関連技術データを開示したとして逮捕、実刑判決を受けたが、同教授はその10年前から中国を頻繁に往復し、精華大学等から名誉博士号を授与され、研究室に留学生を迎え入れていた。大学が立件されなかったのは、ロス教授に警告を発していたため。

⇒（参照）「考察　―米国テネシー大学教授の不正輸出事件―」（CISTECジャーナル2009年１月号No.118。CISTECのHP内「大学の輸出管理」サイトに掲載）

４　おわりに

国際競争、国際化の一方でリスクも増える

以上の仮想事例を見ていただくと、単に外為法による安全保障輸出管理の世界だけで、大学からの先端技術流出が防止できるわけではないことを理解していただけるのではないかと思います。特に、大学間の国際競争が激しくなり、国際化が推進されていくことにより、国際交流も拡大される一方でリスクも増えることになります。

それだけに、より高次の見地に立って、我が国の大学のハイテク技術が、懸念国やテロリストによる大量破壊兵器開発や軍拡に使われることを避けるために、リスクを認識し、予防策を講じる必要があると思われます。

大学は、知の中核拠点であり、できる限り自由な研究教育環境が担保されることが望ましいところです。一連の規制も少ないに越したことはなく、規制が課されるとしても、予見可能性、透明性が担保されるべきことは、６月に６団体連名で提出された「大学に係る安全保障輸出管理行政に関する包括改善要請書」においても述べられているところです。

しかし他方で、いったん事が起き、大きなインパクトを与えるような技術流出事件が生じた場合には、必要以上に規制が強化されてしまいかねないということもまた、産業界が教訓として得た事実です。社会的、政治的問題になってしまえば、狭い法律論だけを主張しても、はなかなか通りにくいということも、経験則から言えることです。

自由な研究教育環境と、機密保持必須の軍関連研究の双方がある米国大学

しばしば、米国の大学における、国際的にオープンな研究教育環境や、予見可能性、透明性のある規制について言及され、上記要請書においても、中期的にはそのような方向を目指すことが望ましい旨述べられています。しかし他方で、やはり要請書でも言及されている通り、米国には、国家的秘密保護制度や国防高等研究計画局（DARPA）による軍事転用可能技術の囲い込み等の制度が別途存在しており、我が国とは前提条件が異なることも否定できないところです。スタンフォード大学のように、すべて公表前提の研究のみとすることにより、EARや武器輸出管理法等の輸出管理規制に囚われずに、世界から頭脳を集め研究拠点としているような例もある一方で、はからずも、今回のノーベル賞受賞の際の中村修二氏の談話から明らかとなったように、米国の大学では、軍からの研究資金がそれなりの比重を持っているということも事実です。中村氏は、朝日新聞のインタビューに答えて、国籍を米国籍にしたことについて、次のように述べています（朝日新聞2014年10月18日付）。

「米国の大学教授の仕事は研究費を集めること。私のところは年間１億円くらいかかる。その研究費の大半は軍から来る。軍の研究費は機密だから米国人でないともらえない。米国で教授として生きるなら、国籍を得ないといけない。」

理系研究室のすべてがすべて、こういう状況というわけでもないでしょうが、米国の大学は、軍からの資金を得ることに特段の抵抗はないように思えます。実際、先般話題となった国防高等研究計画局

(DARPA) が主催した災害救助ロボットコンテストでは、大学のチームからの応募が多数ありました。東大では参加が認められず、ベンチャー企業として飛び出したSCHAFT社が圧倒的強さで優勝したことも話題となりましたが、同コンテストでは、カーネギー・メロン大学、マサチュセッツ工科大学(MIT)、バージニア工科大学その他多数の大学がチームを組んで覇を競いました。MITなどは、ロボット分野だけでなく、航空宇宙分野や各分野の博士号を持つ人物をチームに迎えるなど万全の布陣で臨んだとのことです。

軍からの資金を得るということは、他方で、機密保持体制は万全のものが求められるということになります。米国で逮捕され実刑判決を受けたテネシー大学のロス教授が、「基礎科学研究だから」と抗弁したそうですが、国防総省からの受託研究をしていながら、そのような台詞が通るはずもありません。

防衛装備関連研究の有無に関わらず、意図せざる流出防止は必須

日本の大学の場合には、これまで、大学で防衛装備関係の研究開発は行ってきませんでしたから、そういう機密保持についての意識や体制が必ずしも十分ではなかった面があるかもしれません。しかし今後は、昨年末に政府決定された「国家安全保障戦略」において謳われた「産学官の力を結集」との方針の下で、防衛装備の充実に資する研究開発資金が大学にも流れていくことになると思われます。その場合には、形式的なものだけでなく、実質的に、あらゆる技術流出リスクに備えた体制整備が求められることになるでしょう。しかし、そういう防衛装備関連資金の受入れの有無に関わらず、「日本の大学は最先端研究の宝庫として狙われている」という意識を持ち、意図せざる技術流出に備えるということが必要と思われます。

省庁横断的に政府全体での機微技術流出防止の注意喚起を

大学・研究機関からの機微技術流出リスクの防止にためには、大学・研究機関側自らの自覚と取組みが必要とは思いますが、やはり、全般的意識向上や体制整備を促すためには、省庁横断的に政府全体での注意喚起が必要と思われます。6月に6団体連名で提出した「包括的改善要請書」の「要請17」において、「大量破壊兵器拡散防止等に係る大学の取組みに関する政府全体の指針の提示」を掲げていますが、これは、上記に縷々述べた仮想事例を念頭に置き、そういうことが現実のものにならないようにするために必要との考えに立ったものです。大学を所管する文科省と、関係する経産省、外務省、更にはビザ発給や入出国管理を担当する法務省、国家安全保障戦略を担当する内閣官房などが、大学・研究機関が我が国のセキュリティ・ホールにならないよう、省庁横断的な取組みを期待したいところです。

技術流出は、不可逆的とよく言われますが、いったん流出してしまっては取り戻すことはできないという性格があります。そのことを念頭に置きつつ、科学技術研究の自由や国際化の円滑な推進を担保するためにも、不必要な規制、形骸化した規制の合理化の是正や、予見可能性、透明性向上のための改善等は不断に求めつつも、平和と安全の確保のために、守るべきところはしっかり守る（＝メリハリをつける）ということが期待されるところであり、そのために、本稿や本ジャーナルの関係記事が関係者の皆様のお役に立てば幸いに存じます。

【参考資料】最近海外メディア等で報道されている大学・研究所関連の違反事例

情報サービス・研修部　副主任研究員　加藤　もえ

（1）アルゼンチン出身の物理学者とその妻、米研究所の機密の核兵器情報を提供したとして有罪[1]

・アルゼンチン出身で米国の大学で博士号を取得した物理学者とその妻が、ベネズエラ政府関係者を装っていた米国のおとり捜査官に機密の核兵器情報など提供し有罪となった事例。

米司法省は2013年６月21日、ロスアラモス国立研究所（LANL）の元請負業者夫婦を、ベネズエラ政府関係者を装っていた米国のおとり捜査官に機密の核兵器情報などを提供したとして、原子力エネルギー法（AEA）などの下、有罪であると判決を下した。

アルゼンチン出身の米国籍保有者で、物理学者で（米カリフォリニア大学バークレー校；University of California, Berkeleyで）博士号を取得しているPedro Leonardo Mascheroni（当時77歳）は、1979年から1988年までLANLに務めており、「制限されたデータ（Restricted Data；核兵器の設計、製造もしくは使用、特別な核物質の製造、またはエネルギー生成における特別な核物質の使用を含む機密情報）」にアクセスが許可されていた。

米国人の妻Marjorie Roxby Mascheroni（当時70歳）も1981年から2010年まで、同研究所で技術文書の作成・編集に従事しており、やはり「（上記の）制限されたデータ」にアクセスが許されていた。

被告らは2010年９月に起訴されており、夫Mascheroniは2008年11月から2009年10月にかけて、ベネズエラ政府関係者向けに「制限されたデータ」の提供を共謀し、米連邦捜査局（FBI）の訪問を受けた際に著しい虚偽の陳述をしていた。妻Mascheroniは2007年10月から2009年10月にかけて、ベネズエラ政府関係者向けに「制限データ」の提供を共謀し、FBIの訪問を受けた際には、やはり著しい虚偽の陳述していた。

夫Mascheroniは24ヶ月から66ヶ月の実刑後、10年間の監視下の保釈となる見込みだが、量刑裁判の日程は未定である。なお妻Mascheroniは、当時は12ヶ月から24ヶ月の実刑後、９年かの監視下の保釈となる見込みとされていたが、米司法省が2014年８月20日、AEA違反であるとして、１年と１日の実刑後、３年間の監視下の保釈となることが公表されている。

[1] 同事例は以下を参照。The Office of Public Affairs, the U.S. Department of Justice, "Former Workers at Los Alamos National Laboratory Plead Guilty to Atomic Energy Act Violations," *Justice News*, June 21, 2013, <http://www.justice.gov/opa/pr/2013/June/13-nsd-702.html>. 被告が米国の大学で博士号を取得した情報は以下を参照。Lawrence Spohn, "Physicist Recalls Own Charges of Spying," *Daily News*, February 25, 2000, page 15-C. なお妻Mascheroniの量刑判決の公表は以下を参照。The Federal Bureau of Investigation, the U.S. Department of Justice, "Former Los Alamos National Laboratory Worker Sentenced for Violating Atomic Energy Act Violations," *Press Releases*, August 20, 2014, <http://www.fbi.gov/albuquerque/press-releases/2014/former-los-alamos-national-laboratory-worker-sentenced-for-violating-atomic-energy-act-violations>.

（2）米国の大学等、中国からのサイバー攻撃や産業スパイの対応に苦慮[2]

・米国の大学等に対して、主に中国からのサイバー攻撃が激増しているだけではなく、中国人の研究者が機密情報の窃盗を試みて逮捕されるなど、大学等がサイバー攻撃や産業スパイの対応に苦慮しているという報道。

New York Times紙は2013年７月16日、米国の大学等に対して、主に中国からのサイバー攻撃が激増していると報道した。関係者によるとサイバー攻撃はロシアも多く、最近はベトナムからも多いが、やはり中国からが最も多いとのことである。

米ウィスコンシン大学（University of Wisconsin）は、中国から１日10万件ほどの攻撃を受けているという。また同大学が研究を進めている「１プログラム」のために、100万米ドル以上を費やし、コンピュータのセキュリティのアップグレードを行ったと関係者が吐露している。

米カリフォリニア大学バークレー校（University of California, Berkeley）では、１週間で数百万のサイバー攻撃にさらされているとのことであり、既に数百万米ドルに達している対サイバー攻撃における予算が、2012年から２倍になったという。

2012年からウィスコンシン大学は、ハッキングの恐れから教授らにノートパソコン、携帯を持ち出さないよう伝えているが、多くの大学ではまだそこまでの対策を講じてはいないという。一方教授らに米国の法規則に基づいて機微な情報やデータを国外に持ち出すことを禁止している或いは独自に更に厳しく規制している大学にも少なくないとのことである。

またサイバー攻撃だけではなく、Medical College of Wisconsinで、2013年４月に（新たな？）抗癌剤関連の情報を盗もうとした中国からの研究者が逮捕されている。

ハッカーや産業スパイなど機微な情報の窃盗は企業にとって既に大きな悩みであったが、大学にとっては新しい悩みである。米国の大学等は今後、セキュリティを強化し、アカデミアの開放的であることが重要な風土に制限を設け、何が盗まれたかを判断することを強いられ苦慮しているという。

（3）豪当局、中国人のポスドク学生が産業スパイの容疑があるため調査していると公表[3]

・オーストラリアで国防省関係機関や中国の一流大学らともプロジェクトで従事・協力しているナノテク研究所の「CSIRO：Commonwealth Scientific and Industrial Research Organization」で働いている中国人のポスドク学生に産業スパイの疑惑が浮上しているという報道。

Phys.orgは2013年12月４日、オーストラリア当局が前日３日に公表した、非常に機微なナノテク研究所「CSIRO：Commonwealth Scientific and Industrial Research Organization」で働いている中国人のポスドク学生が、産業スパイの容疑があるため調査をしていると報じた。

CSIROは、研究所の従業員によるコンピュータの不正使用を確認しており、オーストラリア国防省傘下の「国防科学技術機構（DSTO：Defense Science and Technology Organization）」とも密接にプロジェクトに従事している。また同研究所は近年、複数の中国の一流大学とナノテクノロジーのプロジェクトで連携しているとの報道もあるという。

---

[2] 同事例はの以下の記事は2013年７月16日に一回公開されたが、２日後の18日に内容の修正があった。 Richard Pérez-Peña, "Barrage of Cyberattacks Challenges Campus Culture," *The New York Times*, July 16, 2013, <http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html?ref=global-home&_r=1&>.

[3] 同事例は以下を参照。"Australia probes spy case at top science authority," *Phys.org*, December 4, 2013, <http://phys.org/news/2013-12-australia-probes-spy-case-science.html>.

（4）イラン出身の米国籍保有者が共謀し、イラン初のリモートセンシング（地球観測）・通信衛星の打ち上げを実施[4]

・米国の大学で理工学系の学位を取得したイラン出身の米国籍所有者が、元イランの在スイス大使などイラン政府関係者らと共謀し、ロシア国有の航空宇宙関連の企業を通して、ロシアの射場から初のイラン製の衛星の打ち上げを成功させたが、その後有罪となった事例。

米国移民・税関執行局（ICE）は2013年12月20日、米メリーランド州在住の以下のイラン出身の米国籍保有者を衛星関連のサービスを提供したとして、8年間の実刑後、3年間の監視下の保釈の判決を下したことを公表した。

・Nader Modanlo（別名：Nader Modanlou、Nader Modanlu（当時53歳））

被告は不法にイランに衛星関連のサービス提供を共謀し、国際緊急経済権限法（IEEPA）とイラン禁輸（1995年大統領令によるイランへの貿易禁輸）の違反や、マネーロンダリング、破産手続の妨害なども行っていた。被告は更に1000万米ドルの没収も命じられた。

Modanlo被告は、米ジョージ・ワシントン大学（George Washington University）で理工学系の学位を修めており、米国防総省や航空宇宙局（NASA）の航空宇宙関連のプロジェクトなども従事した経験を有していた。

被告は1992年から米メリーランド州拠点の企業「Final Analysis Inc.（以下「FAI」と称す）」の主要株主で、会長および社長を兼務していた。「FAI」が購入した衛星を打ち上げるために、1994年からロシア国有の航空宇宙関連の企業「POLYOT」と契約を結んだ。1995年から2000年にかけて「FAI」と「POLYOT」は、「FAI」が購入した衛星をロシア・プレセツク（Plesetsk）から打ち上げを行った。

被告は2001年11月に「New York Satellite Industries, LLC（以下「NYSI」と称す）」を設立した（「FAI」は倒産し、「NYSI」が「FAI」の所有全財産を買収した）。被告は「NYSI」の会長および業務執行社員を兼務した。

2002年6月、元イランの在スイス大使のSirous Naseriを含めたイラン政府関係者らと被告は、被告の衛星打ち上げの資金などをやり取りするに当たって、米国からの制裁を逃れるため、スイスの企業「Prospect Telecom」を設立した。イラン政府関係者は、「Prospect Telecom」の口座から被告の「NYSI」の米国の口座に1000万米ドルを送金した。

これらの被告らの共謀の結果、2005年10月27日にロシアの国有企業「POLYOT」によって、ロシアの射場からイラン製のリモートセンシング（地球観測）・通信衛星が打ち上げられ、初のイラン製の同衛星が軌道に投入され、成功した。

またModanlo被告は、2005年から2007年にかけて、「Prospect Telecom」の破産手続きの際に、イランの関与を隠蔽するために、被告および共謀者が同社

---

[4] 同事例は以下を参照。The Counter Proliferation Investigation Unit, Immigration and Customs Enforcement, U.S. Department of Homeland Security, "Potomac, Maryland, Man Sentenced to 8 Years for Conspiring to Provide Satellite Services to Iran," *News Releases*, December 20, 2013, <http://www.ice.gov/news/releases/1312/131220greenbelt.htm>. 以下も参照。The Counter Proliferation Investigation Unit, Immigration and Customs Enforcement, U.S. Department of Homeland Security, "Potomac man sentenced to 8 years for conspiring to provide satellite services to Iran," *News Releases*, June 10, 2014, <http://www.ice.gov/news/releases/1306/130610greenbelt.htm>. Ann E. Marimow , "Montgomery businessman convicted of helping Iran on satellite project," *The Washington Post*, June 10, 2013, <http://www.washingtonpost.com/local/montgomery-businessman-convicted-of-helping-iran-on-satellite-project/2013/06/10/759e6214-cc65-11e2-8845-d970ccb04497_story.html>. "Nader Modanlo, U.S. Space Entrepreneur, Accused Of Aiding Iran," *The Huntington Post*, June 2, 2011, <http://www.huffingtonpost.com/2011/06/27/nader-modanlo-space-entrepreneur-iran_n_884986.html>.

を設立したことを含め、同社の設立および所有について虚偽の申告をしていた。

（5）台湾でリモートセンシング分野の第一人者が中国に亡命し、中国の著名な研究所が採用[5]

・台湾でリモートセンシング（Remote Sensing）分野で第一人者である以下の台湾技術者が無断欠勤を経て密かに中国に亡命後、中国の著名な研究所で採用されたことから台湾の安全保障に懸念が高まったという報道。

Want China Timesは2014年5月24日、前日の23日に台湾教育部（部は日本の省に相当）が公表した、台湾でリモートセンシング（Remote Sensing）分野で第一人者である以下の台湾技術者が無断欠勤後、密かに中国へ亡命したと報道した。

・陳錕山（Chen Kun-shan）

陳氏は、2001年から台湾の国立中央大学「宇宙リモートセンシング研究所（Center for Space and Remote Sensing Research）」で所長を務めていたが、2013年11月時点で2ヵ月にわたって無断欠勤を続けていたため、停職処分にされていたという。

亡命の事実が発覚したのは、2014年3月に中国で、陳氏が中国の「遥感科学国家重点実験室（State key laboratory of remote sensing science）」に採用されたと報じられていたという。

「遥感科学国家重点実験室」は、北京師範大学（Beijing Normal University）および中国科学院遥感与数字地球研究所(Institute of Remote Sensing and Digital Earth, China Academy of Science)が共同で設立した研究所であり、海外の研究者の獲得にも熱心であるとのことである。

台湾当局によれば、「陳氏の亡命は台湾の安全保障にとって深刻な脅威」であるという。背景として陳氏は、台湾および中国の軍事動静を偵察するスパイ衛星の画像にアクセスする権限が付与されていただけではなく、台湾の機密情報も取り扱うことができることから、中国への訪問も制限される立場であったためであるとのことである。

（6）米国武器製造請負業者で元陸軍将校が大学院生の中国人女性に核兵器等の機密情報を提供[6]

・米国武器製造請負企業で元陸軍将校が国際会議で出会った大学院生の中国人女性に核兵器等の機密情報を提供し、有罪となった事例。

Washington Timesは2014年9月18日、当時27歳であったという中国人女性に核兵器等の機密情報を漏らしたとして起訴されていた米ハワイの武器製造請負企業で元陸軍将校Benjamin Pierce Bishop（60歳）に7年の実刑判決が下されると米司法省が明らかにしたと報道した。

被告は以前勤務していた米太平洋軍から複数の機密文書を入手し、国際会議で出会い、恋愛関係となった中国籍の女性に提供していた。女性は米VISAを保有する大学院生とのことであり、事前に被告のよ

---

[5] 同事例は以下を参照。"Top Taiwanese scientist Chen Kun-shan defects to China," *Want China Times*, May 24, 2014, <http://www.wantchinatimes.com/news-subclass-cnt.aspx?id=20140524000026&cid=1103>. 本記事は当初以下で確認。Ys-K,「台湾人技術者、無断欠勤後に中国へ亡命」『Intelligence News and Reports』May 26, 2014, <http://blog.livedoor.jp/intel_news_reports/archives/38310646.html>.「遥感科学国家重点実験室」については、以下を参照。『遥感科学国家重点実験室』<http://www.slrss.cn/index>.

[6] 同事例は以下を参照。The Federal Bureau of Investigation, U.S. Department of Justice, "Defense Contractor Charged in Hawaii with Communicating Classified Information to Person Not Entitled to Receive Such Information," *Press Releases*, March 18, 2013,
<http://www.fbi.gov/honolulu/press-releases/2013/defense-contractor-charged-in-hawaii-with-communicating-classified-information-to-person-not-entitled-to-receive-such-information>.
Phillip Swarts, "Defense Contractor Sentenced to 7 Years for Giving Secrets to Chinese Woman," *The Washington Times*, September 18, 2014,
<http://www.washingtontimes.com/news/2014/sep/18/defense-contractor-sentenced-to-7-years-for-giving/?page=1#!>.

うな人物に接触を図るのが目的であったのではと疑惑も生じている。一方女性の身元は公開されていない。

被告は2013年３月に逮捕されていたが、同女性に連絡を取ろうとするなどといった行為が続いたため、当局の関係者から量刑を見直すべきであるという声も上がっているという。

〈3〉国立大学協会による「留学生等受入れに係る安全保障上の入口管理等に関する要望」について

CISTEC

CISTECジャーナルの2014年7月号（No.152）の「特集　大学における輸出管理」でご紹介のとおり、CISTECは、関係団体と連名で「大学に係る安全保障輸出管理行政に関する包括的改善要請書」を、経済産業省、文部科学省、外務省の局長クラス宛てに提出しており、その写しを一般社団法人国立大学協会（以下「国大協」という）にも送付し、会員大学との問題意識の共有や今後の支援、協力を要請しています。

同記事でも触れていますが、国大協の教育・研究委員会において、その下部組織として立ち上げられた「留学生等受入れに係る安全保障上の入口管理等に関するワーキンググループ」にてご議論がなされていたところ、先般、「留学生等受入れに係る安全保障上の入口管理等に関する要望」と題する要望書が取りまとめられ、本年9月に、文科省を始めとする関係3省庁宛てに提出されました。

国大協は、平成22年6月にも「大学における技術提供にかかる安全保障貿易管理について」にて要望しているところですが、今回の要望はそれに続くものです。

国大協では、知の創造拠点としての大学の役割の推進とともに、社会のグローバル化に対応した教育・研究環境の確保、異文化の相互理解、学生や教職員の相互交流、大学の国際競争力の向上をめざすとともに、政府が推進する「留学生30万人計画」の実現にむけ、留学生の受入環境の整備に取り組んでいるとのことです。

一方、留学生等受入れに伴う安全保障上の入口管理等の場面においては、その管理方法・ルールが確立されておらず、各大学が種々工夫して実施している状況であり、その対応に苦慮する状況が報告されているため、このたび改めて要望書を提出したとしています。

要望の柱は、以下の3点です。

① 政府関係機関の対応窓口の一本化、もしくは明確化
② 入口管理の重点化について（在籍身分と学問領域の観点から）
③ 政府機関と大学が継続的に検討・協議する場の設置

本要望書においては、6月にCISTECを始めとした関係6団体連名で提出した包括的改善要請書にも言及しつつ、改善に向けた配慮を求めていますが、同包括的改善要請書には、上記の3点も含まれています。

これにより、大学関係の主要団体の共通コンセンサスとして、統一的要望内容が揃いましたので、関係省庁において、その趣旨を理解していただき、然るべき改善が逐次なされていくことを期待したいところです。

なお、要望書の全文は国大協ホームページで閲覧できます。

http://www.janu.jp/news/whatsnew/20140922-wnew-youbou.html