


外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007年)
(ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE 2007)

平成21年3月

財団法人 防衛調達基盤整備協会 ®

はしがき

本出版物「外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007年)」は、米国の国家対情報局 (Office of the National Counterintelligence Executive : ONCIX) が作成した「Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, FY07」を翻訳したものです。

同報告は、1995年度情報権限付与法 (公法103359) の809条 (b) の規定に従い、提出されたもので、今回で第13回となり同法は、米国企業に対する外国からの経済情報収集および企業スパイに係わる最新脅威情報については、大統領が議会に年次報告することを要求しています。

本報告は、企業秘密として、金融、ビジネス、科学、技術、経済、または工学に関する図形、計画、編集物、プログラム装置、製法、デザイン、試作物、方法などあらゆる形態と種類の情報をあげ、それらの情報(企業秘密)を不正に取得するための活動について、記述・紹介しております。

企業秘密を標的とする「産業スパイ」に該当する広範な活動を調査対象としており、これらは、我が国の企業に対する外国の経済情報収集及び産業スパイ活動の脅威を理解する上で大いに参考になるものと思われます。

本出版物が、わが国における技術情報管理の向上にいささかでも貢献できれば、望外の幸せです。

平成21年3月

財団法人 防衛調達基盤整備協会
理事長 宇田川 新一

**ANNUAL REPORT
TO CONGRESS ON**



**FOREIGN ECONOMIC
COLLECTION AND
INDUSTRIAL ESPIONAGE**

2007



2008. 9. 10

外国の経済情報収集および産業スパイに関する議会への年次報告(2007会計年度)

本報告は、国家対情報局 (Office of the National Counterintelligence Executive : ONCIX) により作成された。意見と質問は、次の電話番号により国家対情報局 (ONCIX) の分析・収集課までご連絡ください。電話番号 (571) 204-5063 または秘匿電話 2517

目 次

| | |
|---|----|
| 1. 主 要 な 調 査 結 果 | 1 |
| 2. 適 用 範 囲 | 3 |
| 3. 衰 え な い 脅 威 | 7 |
| 4. 広 範 な 活 動 家 グ ル ー プ | 9 |
| 5. 永 続 的 な 方 法 | 11 |
| 6. 標 的 と な っ た 情 報 と 技 術 分 野 | 17 |
| 7. 別 紙 1 : 技 術 を 保 護 す る た め の 対 情 報 コ ミ ュ ニ テ ィ の 努 力 | 19 |
| 8. 別 紙 2 : 2007 会 計 年 度 に 経 済 情 報 収 集 お よ び 産 業 ス パ イ に よ り 逮 捕 さ れ 有 罪 判 決 を 受 け た 事 例 | 23 |

1. 主要な調査結果

米国は、その世界的な科学技術のリーダーシップと技術革新により、経済情報収集および産業スパイの主要な標的となっている。対情報コミュニティが収集した情報によると、2007会計年度に、世界中の収集家（民間部門のビジネスマン、科学者、技術者および学生、ならびに外国の軍および情報機関の情報員）が米国に対する経済情報収集活動に関与したが、同盟国および敵対国を含む10カ国足らずの国の収集家の標的活動（targeting activity）が大半を占めている。

外国の収集家は、“秘密に指定されていない（unclassified）”ものから“秘密に指定された（classified）”ものまで、広範な分野の様々な情報と技術を標的とし続けている。デュアル・ユース品目（汎用品）、輸出管理規制下の品目、および軍用品目を標的とする外国の収集取組みに関する最も詳細な情報を保有している対情報コミュニティによると、最も激しく標的にされた分野は、航空技術、情報技術（IT）、レーザー、感知技術、光学、ならびに武器およびエネルギー材料である。さらに、最先端の製品やサービスを製造するために使用される独特の製造プロセスや企業秘密も標的となっている。

収集家によって使用される方法は、収集家の数と同じくらい様々である。それらには、情報の要求、売込みや市場取引、技術や会社の取得、会議あるいはその他の公開の場における標的活動、共同研究の利用、公式訪問、および海外の米国人旅行者を標的とするものが含まれる。収集家は、サイバー攻撃やインサイダーの利用など、ますます技術的に高度な方法を使用している。このため、彼らの身元や目的を解明することは困難となっている。

ますますグローバル化する市場における多国籍企業の増大にともない、外国の収集取組みを追跡・分析・対処することは、

次第に困難な挑戦となっている。このようなことから、米国に対する脅威は、不鮮明でわかりにくくなっている。

2. 適用範囲

本報告は1995会計年度の情報権限付与法809条(b)(公法103-359)の規定に従い提出されたものである。同法は、大統領に対し、米国企業を対象とする外国の経済情報収集および産業スパイの脅威に関する最新情報を議会に年次報告することを要求している。本報告は、2006年度の外国の経済情報収集および産業スパイに関する第12回年次報告に2007年度のデータを加え更新したものである。

本報告は、米国企業に対する、外国の経済情報収集および産業スパイの脅威を調査するとともに、産業スパイを行っている外国政府の実態、スパイの標的となっている情報および技術の産業分野、ならびにスパイが使用する方法などの傾向を特定するものである。

本報告は、前年と同様に、企業秘密を標的とする“産業スパイ”に該当する広範な活動を調査対象としている。この文脈において、“企業秘密 (trade secret)”とは次のものをいう。金融、ビジネス、科学、技術、経済、または工学に関する図形、計画、編集物、プログラム装置、製法、デザイン、試作品、方法、技術、プロセス、手順、プログラム、またはコードを含むあらゆる形態と種類の情報をいう。それらの情報は、有形であろうと無形であろうと、物理的に、電子的に、図表として、写真として、または文書として保存、または編集されていようとなかろうと、所有者（すなわち、その秘密の合法的もしくは正当な所有権、またはライセンスを有する個人または団体）がそれらを秘匿するため合理的な措置を講じており、それらが一般にはあまり知られていないことから現実にはまたは潜在的に独立した経済的価値を有しており、かつ一般の人々が適正な手段によっても簡単に解明することができないものならば、それらの情報は企業秘密である。企業秘密を不正に取得するための活動には次がある。

- ・ **経済スパイ**とは、外国政府、外国政府の影響下にある組織、または外国政府の職員の利益になることを承知または意図して、企業秘密を意識的かつ意図的に横領することである。横領には、企業秘密を許可なく盗み、複写し、改ざんし、破壊し、伝達し、送付し、受領し、購入し、所有し、または横領を共謀することが含まれる。しかし、これに限定されるものではない。1996年経済スパイ法(Economic Espionage Act of 1996: EEA)のセクション1010(a)は経済スパイを刑事罰の対象としている。
- ・ **産業スパイ**とは、その企業秘密の所有者に損害を与えることを承知または意図して、所有者以外の誰かの経済的利益のために、州間通商または外国貿易のために製造された製品に関連した企業秘密を意識的かつ意図的に横領することである。横領には、企業秘密を許可なく盗み、複写し、改ざんし、破壊し、伝達し、送付し、受領し、購入し、所有し、または横領を共謀することが含まれる。しかし、これに限定されるものではない。

経済スパイ法（EEA）は、産業スパイも刑事罰の対象としている。

• 輸出規制違反

デュアル・ユースの装備品や技術の移転には、輸出規制された米国のデュアル・ユース品目（軍事及び民間双方での利用が可能）を、米国の利益を損なう目的で国または個人が無許可で取得することが含まれる。これらの品目には、特定の国の軍事力とテロリズム活動を強化することができる大量破壊兵器とその運搬手段の拡散に関連する製品と技術が含まれる。商務省の産業保全局（BIS）は、国家安全保障、外交政策、および拡散防止の観点から、輸出を規制し、これらの規制を執行する責任を有している。連邦捜査局（FBI）と移民関税執行局（ICE）は、これらの規則の違反を取り締まるための共同管轄権を有している。連邦捜査局（FBI）は、連邦行政規則集（28FR § 0.85（d））に従って、輸出事件のカウンターインテリジェンス面を担当している。これらの組織は、あらゆる訴追オプションを確保するために連携している。

防衛品目の移転には、防衛製品、防衛サービス、および関連技術データ（総称して米国軍需品リストとして知られている）の無許可輸出が含まれる。軍需品リスト品目には、米国製の武器や軍用品が含まれる。国務省の防衛通商管理局（Directorate of Defense Trade Controls）は、国際武器取引規則（International Traffic in Arms Regulation : ITAR）を管理し、移民関税執行局（ICE）は、武器輸出規制法（Arms Export Control Act）と国際武器取引規則（ITAR）の違反を取り締まる。国務省は、輸出禁止指定国に対するあらゆる軍需品リスト品目の輸出拒否政策を堅持している。

司法省は、2007年に米国の兵器とセンシティブ技術の違法輸出の調査と訴追手続きを改善するために、初代の国家輸出管理調整官（National Export Control Coordinator）を任命した。司法省や法執行機関、輸出許可機関、情報機関などの輸出取締りで役割を果たす様々な機関が緊密に調整することが、将来の訴追手続きの成功にとって不可欠である。

本報告は、次に示す広範な米国政府機関から提供された資料に基づき、国家対情報局（ONCIX）によって編纂されたものである。

- 空軍特別捜査局（Air Force Office of Special Investigations : AFOSI）
- 陸軍対情報センター（Army Counterintelligence Center : ACIC）

- 中央情報局 (Central Intelligence Agency : CIA)
- 国防情報局 (Defense Intelligence Agency : DIA)
- 国防保全局 (Defense Security Service : DSS)
- 商務省 (Department of Commerce : DC) 産業保全局 (Bureau of Industry and Security : BIS)
- エネルギー省 (Department of Energy : DOE)
- 国土安全保障省 (Department of Homeland Security : DHS) 、移民関税執行局 (Immigration and Customs Enforcement : ICE)
- 国務省 (Department of State : DS)
- 連邦捜査局 (Federal Bureau of Investigation : FBI)
- 国家空間情報局 (National Geospatial-Intelligence Agency : NGA)
- 国家偵察局 (National Reconnaissance Office : NRO)
- 国家安全保障局 (National Security Agency : NAS)
- 海軍犯罪捜査局 (Naval Criminal Investigative Service : NCIS)
- 国家情報官事務局 (Office of the Director of National Intelligence : ODNI)、公開情報センター (Open Source Center : OSC)

3. 衰えない脅威

「我々は、科学および技術分野におけるリードを失うことを恐れている。一旦リードを失えば、たとえ、それが回復できるとしても、リードを取り戻すことは困難なことである。

全米科学アカデミー、2007年」

米国は、その技術およびビジネス分野における世界的なリーダーシップにより、外国の経済情報収集および産業スパイの主要な標的であり続けている。事実、米国の強い国際競争力が、米国の情報と技術を標的とする外国の情報収集活動家の関心を引き付けている。

脅威の対象範囲を分析し、それを追跡することは、ますます困難な挑戦となっている。グローバル化と多国籍企業の増大は、外国と国内企業の境界をあいまいにし、研究開発のアウトソーシングを促進し、事業拠点の海外設置につながっている。そして、それは、米国の情報と技術を標的とする外国組織に多くの情報収集の機会を提供するとともに彼らの収集活動を隠蔽することに役立っている。

これらによって産業スパイの全貌を明らかにすることは益々難しくなっているが、2007年度においても脅威は厳しいままであるという十分な証拠が存在する。

- 連邦調査局（FBI）は、当該年度に、51件の事件を解決し、さらに53件の訴訟中の事件に取り組んでいる。
- 移民関税執行局（ICE）は2,600件以上の輸出関連の調査を行った。調査の結果は、188件の逮捕、178件の起訴、そして127件の有罪判決となった。
- 商務省の産業保全局（BIS）は783件以上の調査に参加し、497件について司法措置を講じた。この結果、16件の有罪判決、2,500万ドルの罰金、140万ドルの没収、75件の行政罰、および600万ドルの民事罰となった。
- 国防保全局（DSS）は、施設保全適格証を有する国防事業契約者から、疑惑のある外国からの接触に関して6,034件の報告を受取り、その内2,879件を調査した。そして、国防保全局（DSS）は、876件を、同適格証を有する国防事業契約者に対するカウンターインテリジェンス脅威に分類した。

4. 広範な活動家グループ

報告対象期間の2007年度に収集された情報によると、多数の国の政府情報機関の他に、ビジネスマン、科学者、技術者、学者も米国の情報と技術を標的し続けている。収集活動の大半は、中国とロシアを含む10カ国足らずで構成される中核グループに属する収集家が行っている。

欧州諸国も同様の脅威を経験：公開情報による展望

メディアによると、多くの欧州の国々は、米国が直面している脅威と同様に中国、ロシア、およびその他の国からの産業スパイの脅威に直面している。これらの公開情報源によると、中国の経済スパイは、工業技術および科学技術分野を重点的に標的とし、ロシアのスパイは、主として産業、科学、および技術分野を標的としている。フランスは、経済スパイに対応するために国家レベルの政府機関を設立したが、一方その他の欧州の諸国は、企業秘密を窃盗から防護することや知的財産権を行使することを主として個々の企業に任せている。欧州における産業スパイの標的は、軍事秘密へのアクセスを有する防衛企業からエネルギーおよび薬品会社に及んでいる。

5. 永続的な方法

収集家によって使用される方法は、収集家と同じくらい多様である。対情報コミュニティの報告によると、最も頻繁に使用される手口は次のとおりである。

- ・情報の要求
- ・売込みおよび市場取引
- ・技術および会社の買収
- ・公式訪問
- ・共同研究および交流の利用
- ・学会、会議、および見本市
- ・サイバー攻撃等
- ・海外の米国人旅行者に対する標的活動

・情報の要求

直接および間接の情報要求は、対情報コミュニティにより報告される最も頻繁に使用される手口のリストの最上位に位置し続けている。要求された情報には、秘密に指定された情報、センシティブ情報、または輸出規制品目に関連した情報が含まれる。国防保全局（DSS）、空軍特別捜査局（AFOSI）および陸軍対情報センター（ACIC）は、外国政府および民間双方の収集家がこの方法を使用していると報告している。

- ・陸軍対情報センター（ACIC）の数字は、直接請求に関連した標的活動の85%以上が、本人の直接訪問、Eメール、電話、またはFAXで請求したものであることを示している。
- ・国防保全局（DSS）の報告は、標的活動の26%がこの分類に入ることを示している。

・売込みおよび市場取引

外国企業は、センシティブもしくは秘密に指定された情報、技術、またはプロジェクトへアクセスすることができる取引関係を求め、米国企業への接近に努めている。例えば、

外国のビジネスマンは、センシティブ技術に関連した仕事をしている米国の軍事施設に対して、製品デザイン、ソフトウェア、またはエンジニアリングなどの様々な頼まれもしない事業提案を持ち込んでいる。

・技術の取得

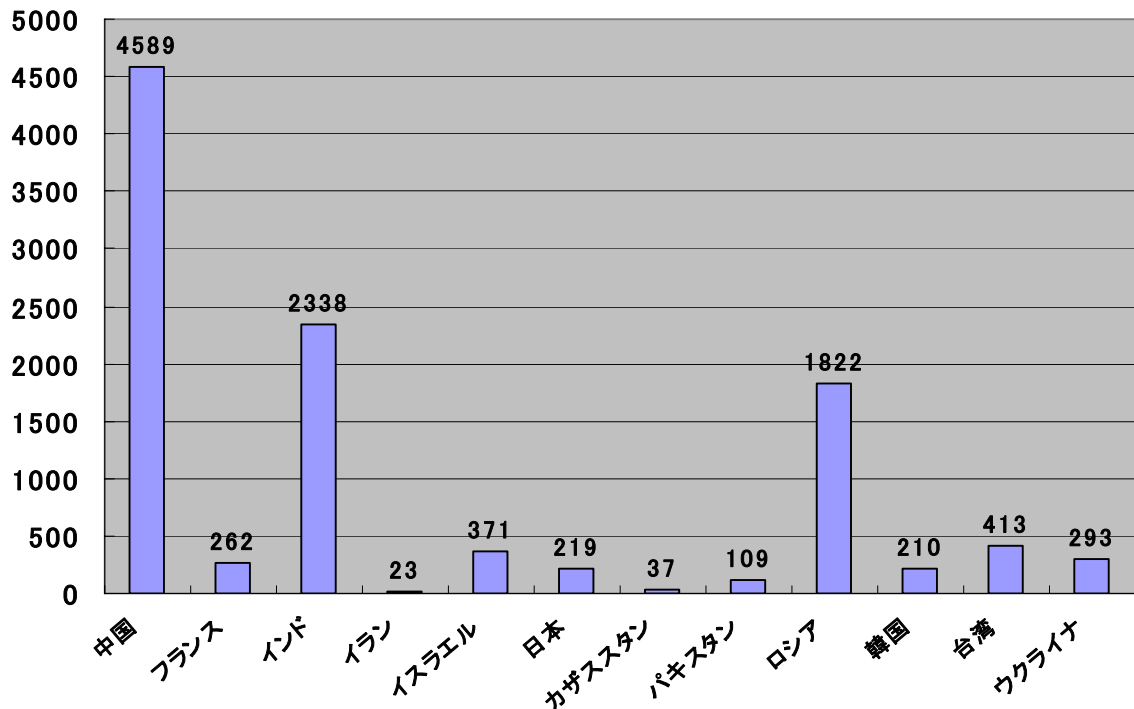
2007年度のデータによると、第三国やトンネル会社を通しての技術および情報の直接および間接の買収、ならびに米国企業または技術の直接買収は、収集家が利用しつづけている取得方法である。米国の輸出規制の影響をほとんど受けない米国と緊密な関係を有する国は、しばしばセンシティブな米国技術の転用を望む国の主要な活動拠点となる。外国の収集家は、米国技術を、架空の会社、いくつもの輸送会社、複数の国、又は自由経済圏を通過させるなどして彼らの活動を偽装している。また、彼らは、活動を隠蔽するために、不正貿易と合法貿易とを織り交ぜて行っている。

・学界、会議、および見本市

これらの公共の場は、外国の収集家にとって、米国の専門家と交流する機会、ならびにデュアル・ユースおよびセンシティブ技術に関する情報を探り出す機会に溢れている。国防保全局（DSS）は、これらの公開の場での収集が2007年度中の不審事案の4%以上を占めていたことを指摘している。

その他の大規模な国際的イベント、特に、スポーツイベントが、米国に対するさらなる経済スパイの場として登場してきた。米国企業は、しばしばそれらのイベントのスポンサーとなり、何千人もの従業員を行事に派遣している。今年の中国での夏季オリンピック、2010年の上海での世界博覧会、および2014年のロシアのソチでの冬季オリンピックは、大きな脅威環境の中で開催されるであろう。このようなイベントは、主催国の情報機関に対して米国民間分野の中に新しい情報提供者を発見し、評価し、そして勧誘する機会を提供するとともに、企業によってイベントに持ち込まれた技術を通して当該企業のネットワークおよびデータベースへ電子的にアクセスする機会を提供するであろう。

エネルギー省関連施設への外国人訪問者数、07年会計年度



・公式訪問

外国の政府機関や、その情報および保全機関は、頻繁に公式の交流および米国への訪問を通して情報を収集している。訪問先には、軍施設、兵器製造センター、および国の研究所が含まれる。

・共同研究の利用

最先端の研究開発は、米国と外国の専門家の共同研究として行われている。最近公表された商務省（DOC）が資金援助して実施された研究においても、“個々の米国企業は、国際的競合企業と協力して、グローバルな研究機関を創設している。また、米国の大学は、海外に分校を創設し、外国の大学と共同教育プログラムを創造し、そして、最先端の研究を進める上で外国の学部と連携している。”ことが指摘されている。エネルギー省（DOE）は、分野別の研究所を横断した研究には科学的情報の交換が不可欠であると報じている。多くの政府機関と民間企業は、不正な技術移転および企業秘密の損失を防止するために損失の緩和戦略（mitigation strategies）を採用しているが、進行中の多数の共同研究は、人との交流あるいは技術的手段による情報収集の最高の機会となっている。2007年度だけ

でも、エネルギー省（DOE）への外国の訪問者は一万人以上であった。その内、4, 500人以上が中国人であった。（上の図を参照）

・サイバー攻撃等

様々な報告によると、2007年度においてもサイバー脅威は衰えていない。連邦捜査局（FBI）は、2007年度に、48件の新しいサイバー関連事件の調査を開始し、4件の事件の調査を終了した。年度を通して、米国政府および施設保全適格証を有する防衛企業のそれぞれのネットワークは情報収集を目的としたと見られる侵入を経験した。

- ・2002年以來、米国は、中国が関連したコンピュータネットワークへの侵入を確認している。そして、それらは、数千のホストおよび数十万のユーザアカウントのセキュリティをすり抜け、米国、同盟国、並びに外国の政府、軍、および民間のコンピュータネットワークからテラバイト単位のデータを密かに漏洩させた。

- ・侵入の一部を実行する中国の傘下にある活動家は、施設保全適格証を有する防衛企業のコンピュータに侵入するために、メールの件名を工夫するなどの社会工学的手法が使われたEメールを使用した。

米国政府のネットワークは、合法的な科学的共同研究を含む様々な理由により、外国政府および非国家の活動家双方から標的にされ続けられている。中国のネットワークは、米国のコンピュータを標的とした悪意ある活動の拠点となっているが、しばしばそれらの活動の発信源や意図を突き止めることは困難である。なぜならば、多くの国々および犯罪者は、米国の標的に対する彼らの攻撃の発信源を分かりにくくするために、中国のネットワークに侵入してそのインターネット・プロトコール（IP）を使用することができるからである。

“スピーアフィッシング（Spear phishing）”（特定の人物を標的としたフィッシング詐欺）は、センシティブ情報へアクセスするためにハッカーによって使用される社会工学を基礎とした方法であり、最近急増している。マイクロソフトの警告によると、“スパミング”（メールを無差別に大量配信すること）として知られているより広範なフィッシングとは対照的に、スピーアフィッシングは、受信が、悪意のある添付メールを開封または悪意のあるウェブサイトへアクセスするよう誘惑するために、信頼できる情報源から発信され、かつ価値のある情報が含まれているように見せかけるために公開情報を使用してEメールメッセージを作成している。そして、より価値の高いより少数の個人を標的としている。

2007年2月に、数人の高い地位にある企業幹部は、米国商事改善協会（US Better Business Bureau）と偽ったスピーアフィッシングEメールを受け取った。コンピュータ犯罪（コンピュータ・フォレンジック）の専門家によれば、Eメールは、当該企業に対する苦情が寄せられているので、記載されたウェブサイトへアクセスし、苦情をダウンロードするよう命じていた。同情報源によると、一旦ダウンロードされたならば、そのサイトは、受信者がアクセスした財政的なウェブサイトや、政府のウェブサイトに関連した全てのキーストロークを窃取するために受信者のシステムにキーロガーをインストールするよう設計されていた。

・海外の米国人旅行者に対する標的活動

外国の収集家は、海外の米国人旅行者—ビジネスマン、政府職員、および請負業者—を標的としている。収集方法には、一見無害な会話から情報を聞き出すことから、個人的な電話会話の盗聴、密かにホテルの部屋に侵入しラップトップまたはその他の電子記憶媒体からの情報のダウンロードまでの全ての方法が用いられる。

囲み記事：事例研究：中国人収集家

2007年度に米国の技術または企業秘密を外国へ移転するために窃盗した罪で有罪判決を受けた人々の多くは、民間部門の人々であった。他方、外国の情報機関との関連は明らかではないが外国政府の収集家の活動も同様に活発であった。例えば、米国で20年以上情報収集活動を続けて2007年に有罪判決を受けた中国系米国人のエージェントの事例は、米国が外国情報機関からの巧みな収集脅威に直面していることの例証である。

当該エージェント（中国人技術者）は、1978年に香港経由で米国に入国した後、米国の主要な情報・防衛企業に勤務し、着実に地位を向上しながらセンシティブ情報へのアクセスを増加した。当該エージェントは、逮捕後の連邦捜査局（FBI）の取調べで、1983年初頭に、センシティブなプロジェクトに関する情報を中国へ渡したことを認めた。彼と彼の妻は、1985年に帰化し米国市民となった。さらに、彼は、1996年に保全適格証を付与された。彼は、中国のためにスパイ活動を継続し、約2年に一度、妻を同行して中国に旅行し、人民解放軍でエージェントを運営する者（handler）に情報を届けるとともに、新たな任務を受領した。

当該エージェントの弟（元解放軍宣伝工作将校）は、2001年5月、妻と息子と共に米国に移住した。彼らは永住権を取得する一方で、解放軍のために運び屋として活動した。当該エージェントは、米国のセンシティブ情報を可搬式磁気媒体に記録し、それ

を弟に渡した。弟と彼の妻は、旅行先の最終目的地を隠すために、しばしばバンクーバーから香港経由で中国を訪れた。さらに、彼らの成人した息子も中国へ旅行し、そこで解放軍の将校に接触して任務を受領し、米国に帰国後直ちに当該エージェントに伝えた。

この事例により、中国情報機関が、彼らの活動を隠蔽するために使用する秘密工作方法が明らかになった。例えば、通信保全のため、エージェントとその仲間は、米国から中国への電話連絡を避けた。また、彼らは航空機による直行便の使用を避けた。さらに、彼らは、ラップトップおよびデスクの情報を暗号化し、さらに隠語を使用した。しかし、最も重要なことは、この事例が、人民解放軍のスパイ工作における忍耐強いかつ断固とした取り組みを示していることである。つまり、エージェントには、企業に浸透してからセンシティブ情報にアクセスできる地位に就くまで十分な時間が許容されていることである。

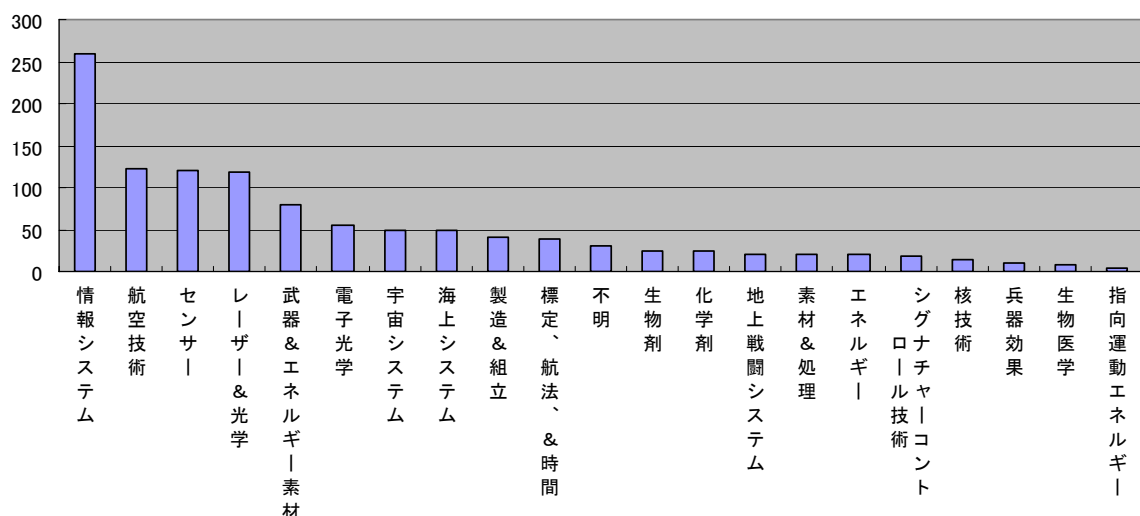
また、この事例は、中国がエージェントに対して収集を命じる情報と技術の範囲を明らかにした。連邦捜査局（FBI）が押収した命令書には、“より専門的組織に所属し、専門的主题のセミナーにより多く参加し、そして講演の配布資料を収集せよ”という指示が含まれていた。さらに、命令書には、エージェントが標的とすべき宇宙応用・推進技術、核攻撃技術、および多数のその他のセンシティブ技術を含む軍事技術のリストが含まれていた。

6. 標的となった情報および技術分野

外国の収集家は、“秘密に指定されていない”情報から“秘密に指定された”情報まで、広範な情報と技術を求め続けている。

- ・国防保全局（DSS）は、2007年度に、外国の収集家が、“開発段階にある技術リスト”（Developing Sciences and Technologies List：DSTL）の20分野の情報と技術を手に入ろうとしていたことを突きとめた。“開発段階の技術リスト（DSTL）”は、世界中で開発されている科学技術能力のうち、将来の米国軍事能力を大きく強化させるか、または劣化させる可能性があると考えられるものかを判断する科学技術能力のリストである。国防保全局（DSS）の調査によると、特に、情報システム、航空技術、センサー、ならびにレーザーおよび光学が標的となった。（下図参照）
- ・陸軍対情報センター（ACIC）は、同年に、航空システム、センサー技術、製造、および組立技術、ならびにエネルギーおよび電力システムが外国の団体から最も頻繁に標的にされたことを突きとめた。（下図参照）
- ・空軍特別捜査局（AFOSI）は、最も多く標的となった分野と技術は、航空システム、製造および組立技術、ならびに情報システムであったことを強調した。
- ・全機関を通じて、最も激しく標的となった分野は、航空技術、情報技術、レーザー、センサー、ならびに武器およびエネルギー素材であった。

07会計年度に標的となった米国の防衛技術、国防保全局



7. 別紙1

技術を保護するための対情報コミュニティの努力

米国の対情報コミュニティは、連邦政府の広範な機関で構成されている。各機関は、外国からの不正な取得からセンシティブ情報および技術を保護することに努力している。対情報コミュニティには、情報収集要員、情報分析要員、および法執行要員が存在する。彼らは、適宜な情報共有および主要事件の迅速な訴追手続きのために、定期的に様々な会議で顔を合わせている。コミュニティの構成メンバーである各機関から提供される支援の例は次のとおりである。

- **国家対情報局（ONCIX）** は、本報告を含むいくつかの取組みの先頭に立っている。例えば、国家に対する対情報脅威を追跡する資源を統合するための組織的な拠点となり、コミュニティに推進力を提供している。対情報コミュニティは、国家対情報局（ONCIX）のコミュニティ取得脅威セクション（Community Acquisition Risk Section : CARS）を支援する。そして、コミュニティ取得脅威セクション（CARS）は、外国企業と取引を行う米国民間団体によってもたらされる脅威の情報コミュニティ（IC）に対する影響を評価するとともに、対情報コミュニティの支援を得て、対米外国投資委員会（Committee on Foreign Investment in the United States : CFIUS）に対して外国投資が米国の戦略的利益にもたらす脅威に関する評価を提出する。
- **空軍特別捜査局（AFOSI）** の研究・技術保護（Research and Technology Protection : RTP）プログラムは、クリティカルな空軍技術を特定し、これらの技術に対する脅威を分析し、脅威を軽減する方策を指導するとともに、正当な理由があるなら外国人による不審な活動を調査する。また、空軍特別捜査局（AFOSI）は、研究・技術保護（RTP）プログラムに関連した情報を他の米国政府機関と共有・協力して、米国技術に対する脅威の性格の変化を追跡・分析する。
- **陸軍対情報センター（ACIC）** は、国防省が、クリティカルな米国の技術、企業秘密、および専有技術情報に対する外国の政府、および民間団体の不法な標的活動や取得活動の性格を分析・評価するのを支援する。また、陸軍対情報センター（ACIC）は、技術や技術情報などの無許可の移転または開示から米国技術を保護するために、センチネル対情報データベース（SENTINEL CI database）に保管されているデータに基づき、技術プログラムの評価を行うとともに、外国の能力と意欲を評価する。

- ・**国防情報局（DIA）**は、“秘密に指定された”クリティカルな米国技術を手に入れようとする外国情報機関の取組みとそれらが盗み取られた場合の影響を評価する。また、国防情報局（DIA）は、外国の情報収集に対処するために、国家対情報局（ONCIX）のコミュニティ取得脅威セクション（CARS）と協力し、国防省の取得業務を支援する。さらに、国防情報局（DIA）は、米国資産に対する外国の所有権、統制、および影響を調査する情報コミュニティの取組みへの参加を通して、クリティカルな国防技術の保護に寄与するとともに対米外国投資委員会（CFIUS）へ情報を提供する。
- ・**エネルギー省（DOE）**の施設および国立研究所は、クリティカルな核技術の紛失を防止するために様々な対情報対策を適用している。エネルギー省の情報・対情報オフィス（Office of Intelligence and Counterintelligence）は、外国の情報収集脅威に対処することを目的としたいくつかのプログラムを監督している。プログラムには、対策の開発、現場の監督要領、専門的訓練、意識向上訓練、対情報脅威の分析、ならびに調査および作戦支援が含まれる。エネルギー省の対情報要員の調査権限は、連邦捜査局（FBI）の対情報調査および対情報作戦の遂行を支援するためだけに限定されている。2007年度報告書の報告対象期日を過ぎてから、議会は、エネルギー省と国家核安全保障局（Nuclear Security Administration）の対情報プログラムの再統合を承認した。これにより、エネルギー省における情報関連活動の全てを完全に統合・強化する道が開けた。
- ・**国防保全局（DSS）**は、施設保全適格証を保有する企業の約12,000施設に対して国家産業保全プログラム（National Industrial Security Program）を実施した。国防保全局（DSS）の対情報専門官は、07年度に同適格証保有企業の19,163名以上の従業員に対し、524回の意識向上教育を行った。また、彼らは、8,743件の不審な事案について調査機関へ照会した。そして、その内868件が調査された。国防保全局（DSS）は、899件の情報報告書を作成し、対情報コミュニティ全体に配布した。国防保全局（DSS）の対情報部門は、企業から通報された不審な事案に基づき、米国技術に対する脅威の性格の変化を調査・分析した。対情報専門官は、同適格証保有企業の保全対策を最新脅威に適合するよう改善するのを支援するために、産業保全専門官と協力して同適格証保有企業の約191件の施設について保全調査を行った。
- ・**連邦捜査局（FBI）**の対情報部門（Counterintelligence Division）は、米国内の経済スパイを訴追・防止するという連邦捜査局（FBI）の努力の大部分について責任を負っている。対情報部門は、説明会を開催したり、戦術的および戦略的な情報資料を発刊したり、会議や作業グループ会同を開催したりして、米国の企業、研究所、および団体に対して外国の脅威の重大性を周知させている。対情報部部門の対スパイ・セクション（Counterintelligence Section）は、1996年経済スパイ法の権限内の調査を指揮すると

ともに、これらの調査を実行する現場部門に対して管理および作戦支援を提供した。2005年8月に発足した対情報部門のドメイン・セクション(Domain Section)は、対情報上の脆弱性およびクリティカルな技術に対する脅威を特定・対処する活動を統制している。また、ドメイン・セクションは、産学との協調プログラムを通して、国家安全保障に関連した連携イニシアチブを保持するとともに、全国および地域の作業グループを通して、戦略的対情報作戦におけるリーダーシップを発揮している。

- **国家空間情報局 (NGA) の対情報オフィス(Office of Counterintelligence)**は、自己組織の能力、人員、および施設の保護を任務としている。国家空間情報局 (NGA) は、作戦保全、産業保全、および情報保証などの分野の努力をより一層統合・強化する目的で、脅威軽減センターを設置しているところである。対情報コミュニティと法執行コミュニティとの間の相乗効果を上げるために、国家空間情報局 (NGA) は、国家対情報局 (ONCIX) のコミュニティ取得脅威評価センター (CARS) に常時要員を派遣している。また、国家空間情報局 (NGA) は、取得、研究、開発、試験、および評価プロセスの全ての段階で、新しい技術の保護に必要な、戦術、技術、および手順を設計、開発、実用、および評価するための研究・技術保護監視会議 (Research Technology Protection Oversight Council) を創設した。
- **国家偵察局 (NRO)** は、非伝統的に脅威となっている国およびグループ(nontraditional threat countries and groups)からの標的活動を認識する能力を向上するだけでなく、作戦、プログラム、および人員に対するスパイからの脅威を識別する能力の向上に努めた。国家偵察局 (NRO) の対情報部門 (Counterintelligence Division)は、技術に対する最新の脅威と標的とする方法に関するブリーフィングを提供するなど国家偵察局 (NRO) の契約業者コミュニティを支援している。対情報部門が運営する対情報ネット (CINet) システムは、外国人との接触および外国旅行の報告を効率化するための電子フォームを使用した安全、かつ、自動化されたウェブベースのシステムである。これにより、脅威情報および説明資料をセキュリティ担当官および政府機関内外の許可された使用者に配布することが可能である。また、対情報ネット (CINet) は、使用者に対して特定の対情報サービスを要請するための手段を提供する。対情報部門は、国家偵察局 (NRO) の資源を保護するためおよび研究開発保護 (RTP) プログラムを強化するために、連邦捜査局 (FIB) のドメイン・タスクフォースおよびその他の任務パートナーと緊密に連携している。また、対情報部門は、コミュニティ取得脅威セクション (CARS) に代表者を配置し、国家偵察局 (NRO) の要求事項を伝えるとともにコミュニティ取得脅威セクション (CARS) の任務全体を支援している。
- **国家情報官 (DNI) の公開情報センター (Open Source Center : OSC)** は、脅威の徴

候を探知するために外国語の出版物やインターネットのウェブサイトを監視している。法執行機関を含む関係機関との間でこの情報を共有することにより、中国に対処する対情報コミュニティの取組みに貢献している。公開情報センター（OSC）は、公開情報から重要な対情報上の問題を察知している。公開情報センター（OSC）は、経済スパイや産業スパイに関する欧州の報道を監視している。公開情報センター（OSC）は、特定の対情報課題に対処するためコミュニティの会議や作業グループの設置に主導権を発揮するとともに情報コミュニティの各機関からの様々な要請に応えた。

8. 別紙2

2007会計年度に経済情報収集および産業スパイ容疑により逮捕され、有罪判決を受けた事例

| 国 | 技術 | 状況 | 出典 |
|------|--|--|--|
| 中国 | 輸出規制された暗視装置データ | 米国企業は、規制された暗視装置データを違法輸出した罪および武器輸出報告書の重要事項の未記載の罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| 中国 | 現在及び将来の米海軍艦船に関する技術データの輸出を共謀 | 帰化して米国市民権を取得し、海軍の請負業者で働いていた男が、2007年5月に裁判で有罪となった。中国の未登録エージェントとして働いていた彼の妻も2007年6月に起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| 中国 | 軍のソースコードを中国海軍研究センターへ違法輸出 | 中国系カナダ人は、2007年8月、経済スパイ法（EEA）違反の罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 USA Today、2006. 12. 14 |
| 中国 | 輸出規制されたマイクロ波回路 | 米国人は、2007年8月、商務省の許可なしでマイクロ波回路を違法に輸出した罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| 中国 | 輸出規制されたレーダへの応用が可能なマイクロ波増幅器 | 米国企業と米国人は、無許可の物品と知りながら輸出したこと、および虚偽の申告書を提出したことで、44件の経済スパイ法（EEA）違反の罪に問われ罰金を支払った。 | 商務省、産業保全局、主要な輸出関連事件、2008. 2 |
| 中国 | 企業秘密の窃盗 | 米国人と中国人は、2007年9月、経済スパイおよび企業秘密の窃盗の罪で起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 PC world紙、2007. 9. 28 |
| キューバ | 輸出規制された情報通信機器（国家安全保障、反テロ、および暗号の観点から輸出規制） | 米国企業は、2007年4月、輸出管理規則(Export Administration Regulations: EAR)違反の罪を認めた | 商務省、産業保全局、主要な輸出関連事件、2008. 2 |

| 国 | 技術 | 状況 | 出典 |
|--------|---|---|---|
| インド | 衛星打上げロケット および弾道ミサイル 関連情報の違法輸出 | インド出身のシンガポールのパスポート保有者とインド系の米国永住者は、違法輸出の罪で裁判所に召喚された。 | 2007司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 インディアン・プレス紙、2007. 4. 1 |
| インド | 振動増幅器、ケーブルアセンブリ、振動処理装置 | 米国企業のマネージャーは、2007年7月、米国により拡散懸念のあるエンドユーザーに指定されているインドの施設に違法輸出した罪で起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| インドネシア | 機関銃、狙撃用ライフル、およびその他の武器を購入し、インドネシアへ違法輸出を計画。また、被告は、インドネシアへ違法輸出する目的でサイドワインダーミサイルおよび機銃弾の購入について照会をしていた。 | インドネシア人は、2007年1月、武器輸出管理法（Arms Control Act）および資金洗浄規正法違反を共謀した罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 ホノルル・スター・ブリテン紙、2007. 1. 19 |
| イラン | 3つの主要なオリジナルソフトウェアの違法輸出 | 原子力発電所の元技師であったイラン出身の帰化米国人は、2008年4月、違法輸出の罪で逮捕・起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 アリゾナリ・リパブリック紙、2007. 4. 21 |
| イラン | 米軍機F-14ジェット戦闘機の部品および整備用具一式 | 米国人は、2007年4月、国際緊急事態経済権限法（International Emergency Economic Powers Act）違反で有罪判決を受けた。 | 司法省ファク・シート：この1年間の主要な輸出関連事件、2007. 11. 11 オレンジ・カントリー・レジスター紙、2007. 5. 9 |
| イラン | 実験装置の違法輸出 | 米国人は、2007年7月、2つの実験装置システムの輸出を共謀した罪を認めた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |

| 国 | 技術 | 状況 | 出典 |
|-----|---|---|--|
| イラン | F-14の構成部品の違法輸出 | パキスタン人は、2007年7月、イランを最終目的地として、マレーシアへ違法輸出した罪で逮捕された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11/アソシエイト・プレス紙、2007. 7. 19 |
| イラン | 航空機部品をイランに違法輸出 | 米国企業の最高経営責任者（CEO）は、2007年7月、懲役5年と罰金の判決を受けた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |
| イラン | 暗視装置と軽機関銃の違法輸出未遂 | イラン生まれの米国人は、2007年8月、有罪の申し立てをした。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11/アソシエイト・プレス紙、2007. 8. 30 |
| イラン | 航空機用アルミニウム、航空機部品、およびその他の機器の違法輸出 | オランダに拠点を置く航空機サービス会社、その会社のオランダ人所有者、およびその他の2つのオランダの会社が、2008年9月に起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| イラン | F-4およびF-14の構成部品 | 2人の米国人は、輸出規制されている構成部品を、イランを最終目的地として、カナダへ違法輸出しようとした未遂罪で起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| イラン | “トラクターのガasket、ボールベアリング、オイルまたは燃料フィルター、ならびにその他の部品およびアクセサリー”などの機器に関する16件の輸出船積み | 米国企業の社長は、2007年10月、無許可送金ビジネスを支援・教唆した罪で有罪判決を受けた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |
| イラン | パイプ切断機 | スイス人、イラン人、および米国会社は、パイプ切断機をドイツ経由でイランへ輸出しようとした際に、虚偽の申告書を作成したという訴因を2007年8月20日に認めた後、同年10月に有罪判決を受けた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |

| 国 | 技術 | 状況 | 出典 |
|----------|--|---|--|
| イラン | ニッケル合金パイプを、英国とアラブ首長国連邦経由でイランへ違法輸出 | 輸出許可なしで輸出しようとした罪で国際緊急事態経済権限法違反に問われた英国企業は、2007年8月、米国の地方裁判所で罪状を認めた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |
| イラン | 米国で開発された石油化学バブル | 米国人は、石油化学バルブをオーストラリア経由でイランへ輸出するための共謀を支援・教唆した罪で有罪判決を受けた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |
| イラク | 情報通信機器/技術 | 中国出身の帰化米国人は、2007年4月、連邦捜査局（FBI）に虚偽の陳述をした罪および中国政府の調達部門の代表として活動した罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 司法省ニュースリリース、2006. 5. 1 |
| イラク | 情報通信機器およびその他の機器 | 2人の米国人は、2007年7月、国際緊急事態経済権限法違反、資金洗浄の共謀罪、および偽証罪で起訴された。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| パキスタン | 輸出規制された、原子炉および弾道ミサイルのノーズ・コーンに使用可能な黒鉛製品 | 米国企業は、2007年10月、2003年にパキスタンを最終目的地としてアラブ首長国連邦へ輸出した黒鉛製品の違法輸出について、文書改ざんおよび虚偽の陳述を共謀した罪で有罪判決を受けた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| スリナム | 輸出規制の弾道ヘルメット | 米国企業は、2007年3月、無許可の輸出活動および輸出申告における虚偽申し立ての罪を認めた。 | 司法省ファクト・シート：この1年間の主要な輸出関連事件、2007. 11. 11 |
| 台湾 | 輸出規制のニッケル粉末 | ある人物が、2007年10月、ニッケル粉末の違法輸出に関連した虚偽の申し立てをした罪状を認めた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |
| アラブ首長国連邦 | 輸出規制の黒鉛 | 米国企業の社長とその代理人は黒鉛製品の輸出に関連して、幾つかの連邦法違反犯罪の共謀、連邦機関の捜査妨害、および文書の改ざんの罪を認めた。 | 商務省産業保全局、主要な輸出関連事件、2008. 2 |

平成20・21年の発刊・平成21年度発刊予定資料

- B S K 第20－ 1号『対情報訓練資料(企業秘密を盗み出す手口とその対策)』
B S K 第20－ 2号『人的セキュリティ：脅威、挑戦、および対策』
－ 英国における人的セキュリティの取り組み －
B S K 第20－ 3号『我が国をめぐる兵器技術情報管理の諸問題(平成19年度)』
B S K 第20－ 4号『技術情報セキュリティの現状と動向(平成19年度)』
B S K 第20－ 5号『米国における情報セキュリティ関連のユーザー教育、資格付与及び管理について(平成19年度)』
B S K 第20－ 6号『インサイダー犯罪防止のための監視・監査体制の在り方(平成19年度)』
B S K 第20－ 7号『新しい防衛調達モデルの探索的調査研究(総論)』
B S K 第20－ 8号『国の安全保障に係わる装備品等を生産している企業に対する外国資本による買収に関する各国の法規制の状況』
B S K 第20－ 9号『管理者用情報セキュリティ・ハンドブック』(保全講習受講用)
B S K 第20－10号『効果的な意識向上促進の取組み方』『携帯電話、携帯用パソコン、携帯情報端末(PDA)、その他電子装置を携帯する海外旅行』
B S K 第20－11号『雇用中の人的セキュリティ：優れた実践事例ガイド』
- B S K 第21－ 1号『我が国をめぐる兵器技術情報管理の諸問題(平成20年度)』
B S K 第21－ 2号『米国における情報システムの不測事態対応計画について(平成20年度)』
B S K 第21－ 3号『外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007年度)』

当協会の保全小冊子は、より多くの方々に呼んでいただくため当協会のホームページに適宜掲載していきます。

外国の経済情報収集および産業スパイ活動に関する議会への年次報告(2007年度)

平成21年3月 発行
非売品 禁無断転載・複製
発行：財団法人 防衛調達基盤整備協会
編集：防衛調達研究センター刊行物等編集委員会
〒160-0003 東京都新宿区本塩町21番3-2
電話：03-3358-8754
FAX：03-3358-8735
メール：hozen@bsk-z.or.jp
BSKホームページ：<http://www.bsk-z.or.jp>