視点

安全保障上機微な技術の収集動向の分析
—“2015 Targeting U.S. Technologies”から—

慶應義塾大学　法学部　非常勤講師／CISTEC　輸出管理アドバイザー　**森本　正崇**

1. はじめに

米国国防省傘下の国防保全局（Defense Security Service（DSS））は、毎年、諸外国による安全保障上機微な情報の収集動向（以下、「DSS報告書」という。）を公表しており、2015年８月11日に2015年版報告である“2015 Targeting U.S. Technologies”が公表された[1]。

これまでにもCISTECジャーナルではDSS報告書の概要が紹介されている。過去の記事と内容的に重複する箇所については、注釈で適宜過去のジャーナル記事を参照することとし、本稿では、DSS報告書の作成・分析手法に焦点を当てて分析し、その後に2015年版のDSS報告書の概要を紹介することとしたい[2]。

2. NISPOMとDSS報告書

DSSは産業界が管理する国家秘密の保護を監視している[3]。その根拠になっているのが、国家産業保全計画（National Industrial Security Program（NISP））である。NISPはブッシュ（父）大統領時代の1993年１月に発出された大統領令12829が根拠となっている[4]。同大統領令を受けて、国防長官が国家産業保全計画実施マニュアル（National Industrial Security Program Operating Manual（NISPOM））を作成している[5]。NISPOMは、契約者が政府から秘密情報の開示を受けるために認証を受けるための手続きや、認証を受けた契約者である“cleared contractors”（以下、「認証契約者」という。）の遵守事項が規定されている。NISPOMでは、認証契約者は不審な接触をDSSに報告することが義務付けられており、認証契約者から提供された情報をDSSが整理・分析したものがDSS報告書である。ちなみにDSS報告書には秘密版と公表版があり、本稿の分析対象は言うまでもなく後者である。先に秘密版が作成され、その後に公表版が作成される[6]。

3. 不審な接触とは

NISPOMでは、不審な接触として以下の事項が列挙されている[7]。

・国籍に関わらず、違法または許可なく

[1] Defense Security Service, “2015 Targeting U.S. Technologies”, August 11, 2015（http://www.dss.mil/documents/ci/2015_DSS_Trend_Report.pdf）.2015年版は17回目の年次報告である。
[2] 2012年版のDSS報告書は、風間武彦「狙われる米国の機微技術と有名無実化するMCTL問題－ネットワーク時代の到来でC4ISR関連技術が標的に－」CISTECジャーナルNo.145、2013年５月、60-72頁で詳しく紹介されている。2013年版のDSS報告書は、風間武彦「中国が注力するC4ISR関連技術－軍近代化戦略における位置づけと軍民融合化での開発状況－」CISTECジャーナルNo.147（2013年９月）56頁に紹介がある。2014年版のDSS報告書は、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－」CISTECジャーナルNo.154（2014年11月）33-40頁を参照。
[3] Defense Security Service, “2015 Targeting U.S. Technologies”, p.4.
[4] Executive Order 12829（January 6, 1993）.
[5] Department of Defense, “National Industrial Security Program Operating Manual”, February 28, 2006.
[6] Defense Security Service, “2015 Targeting U.S. Technologies”, p.4-5.
[7] NISPOM 1-302 b.

（unauthorized）秘密情報を入手しようとしたり、（秘密情報を保有する）認証を受けた職員を危険にさらす者[8]

・いかなる国であろうが、既知の情報機関員、または情報機関員ではないかと疑われる者と、認証を受けた職員の接触

・他国の情報機関の工作活動に職員が標的とされている可能性を示唆する接触

DSSが啓発用に作成しているパンフレットでは、これらに加えて、さらに報告を要する不審な接触が列挙されている[9]。

・認証を受けた職員が、脅迫や強制を受ける可能性がある状況に巻き込まれそうな活動

・外国の顧客が、輸出許可の制限を超えてハードウェアや情報へのアクセスを得ようとする行為

・認証を受けた職員が、特別な接待や特典、贈り物、金銭を通じて義務を負う状況への試み

・価格や引合い、市場調査等を偽装した保護された情報の要求

さらに、不審な引合いは、より詳細に事例が列挙されている。主なものを以下に紹介するが、これらの「兆候」は、輸出管理において「明らかガイドライン」や、取引審査におけるリスク管理等と内容が多分に重複しているので、輸出管理担当者にとっては理解しやすい内容である[10]。

・最終需要者が倉庫や、他社に輸送を手配する企業となっている

・最終需要者の証明がない

・数量、仕向地、顧客について内容があいまいである

・技術内容の修正要求

・急ぎの配送

・最終需要者の住所が第三国

・住所が私書箱等であいまいである

・同一住所を使う複数の企業

・引合いしている者のことを知らない職員や、営業部門に所属しない職員に対する引合い

・民生用途に軍事専用技術が要求されている

・引合い者の事業の範囲外の技術を要求している

・訪問者が最後の最後で輸出管理の対象となっている技術等、協議内容の変更を要求する

・送付するのではなく、引合い者が自分で持ち帰ることを提案する

・要求している技術について、担当者に技術的知識が欠けている

不審な接触を受けた認証契約者は、DSSが定めた報告様式に従って接触内容を報告する。報告様式では接触相手の氏名や企業等の情報に加え、（参考１）に規定したような情報の提供が求められている。

こうして毎年数万件にも上る情報がDSSに報告されており、分析の対象とされている。

（参考１）不審事案提出フォーム

どのように事案の情報を入手、又は事案に遭遇したか
①email
②電話
③施設訪問
④Webカード提出
⑤サイバー（侵入）
⑥不明

技術
本事案は、特定の技術又は軍事計画に関係するか
①はい
②いいえ
③不明

①はい、の場合何の技術、軍事計画か
（　　）

当該技術は秘密指定されているか
①はい
②いいえ
③不明

[8]「職員」とあるのは、原文では"employee"である。秘密情報の開示を受けるのは企業だけではなく、大学や研究機関もあり得るので、これらの機関の"employee"である研究員等も対象となる。大学や研究機関も重要な情報収集の標的となっていることについては後述。また、「認証を受けた」とあるのは、原文では“cleared”と記述されている。いわゆる「クリアランスを受けた」ということであるが、秘密情報取り扱い資格の認証を受けたという意味である。

[9] Defense Security Service, “Counterintelligence Awareness”（http://www.dss.mil/documents/ci/CIAwareness.pdf）.

[10] Ibid.「明らかガイドライン」を使った懸念の兆候等、輸出管理における個別取引の際の注意点について、拙著『安全保障貿易管理の情報分析』（安全保障貿易情報センター、2008年）32-48頁参照。

当該技術は輸出管理の対象か
①はい
②いいえ
③不明
ECCN（　　）

当該技術はITAR規制の対象か
①はい
②いいえ
③不明

当該技術は誰のためのものか
（例：米国陸軍、海軍、ミサイル防衛庁　　）

契約番号（　　）

どのような対応をしたか
（　　）

また接触してくることが予想されるか
①はい
②いいえ
③不明

事案の概要を教えて下さい
（　　）

（出典）DSS Submission Form

4. 分析の枠組み

①報告情報の分類

DSSは報告を不審接触報告（suspicious contact report（SCR））、確証のない接触報告（unsubstantiated contact report（UCR））、評価対象外(assessed no value（ANV））に分類している[11]。SCRは機微な情報や技術を入手しようとした可能性がある、そうした可能性が高い、あるいは、ほぼ確実に入手したと考えられるものである。UCRはSCRの可能性は低いと考えられるものの、報告を蓄積することで外国の情報活動を特定する可能性もあることから、DSSは情報を保持する。ANVと評価された情報はDSSで保持しない。なお、その後に入手した情報や再評価により、SCRからUCRに分類変更するといった形で、これらの分類は変更になることがあり得る。

②情報収集手口

情報収集手口は次のように分類される。

（参考２）情報収集手口

1. 学術に関する依頼[12]（Academic Solicitation）	学術論文や発表のチェック（peer）や教職員に対する相談、教職員や学生、研究員、職員としての研究機関、学部、学科、プログラムへの応募
2. 技術獲得活動（Attempted Acquisition of Technology）	フロントカンパニーや第三国経由、または直接の企業買収。装置そのものや図表、概略図、計画、仕様表等の規制技術が化体した保護の対象となっている情報を獲得しようとする
3. 犯罪行為（Criminal Activities）	窃取。合法的な入手のそぶりもなく保護の対象となっている情報を獲得しようとする
4. コネクションを利用した情報収集（Exploitation of Relationship）	合弁事業や正式な合意、外国政府への武器販売、業務提携等を利用。既存の合法的または表面上無害な関係を使って、許容されていないアクセスを狙う
5. 訪米（Foreign Visit）	認証契約者への訪問を利用。事前に外国側代表団と調整している場合と、全く予告なしの場合がある。許可を受け、意図していた情報共有以上に、保護の対象となっている情報にアクセスし、収集しようとする
6. 情報提供要求（Request for Information）	電話、email、webカードを利用。価格見積や市場調査等を偽装して保護の対象となっている情報を収集しようとする
7. 検査・没収（Search/Seizure）	人員や持ち物等を物理的に検査する。一時的あるいは恒久的に持ち物を没収したり、移動の自由を制限したりする

[11] Defense Security Service,“2015 Targeting U.S. Technologies”, p.5. 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－」33頁。
[12] 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－」34頁では、「大学を利用した情報収集」と訳されているが、必ずしも大学だけを標的としていないことから、本稿ではAcademic Solicitationを直訳した。その他も基本的に“2015 Targeting U.S. Technologies”の記述に準拠しているため、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－」とは順番や言いぶりが異なる箇所もあるが、基本的には内容は同一である。

8. 求職 （Seeking Employment）	履歴書の提出等を利用。外国政府機関に有用になる可能性がある保護の対象となっている情報へアクセスできる人物を送り込む
9. 勧誘・マーケティング （Solicitation or Marketing Services）	販売や代理店、技術サービスや業務サービスへの入札を利用。外国組織が保護の対象となっている情報の流出に脆弱な認証契約者と関係構築を狙う
10. 観察 （Surveillance）	目視、口頭、電子的手段、映像等の手段を利用。装置や施設、敷地や人員の組織的な観察を行う
11. ネット上の不審活動 （Suspicious Network Activity）	サイバー侵入、ウイルス、マルウェア、バックドア攻撃、ユーザー名やパスワードの獲得等を利用。認証契約者のネットワークへ侵入し、保護の対象となっている情報を抜き出そうと試みる

（出典）Defense Security Service,“2015 Targeting U.S. Technologies”, p.50-51.
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－」34頁

DSSではこうした情報収集手口に関連して、様々な状況における注意事項をパンフレットとしてまとめ、啓発活動を行っている。以下、パンフレットで指摘されている内容から、興味深いと思われる点につき紹介する。なお、【 】は各パンフレットの名称である。

【学術に関する依頼】[13]

DSSは学術に関する依頼を機微な、もしくは秘密指定された情報を不適切な方法で入手するために、学生や教授、科学者、研究者を利用するものと定義している。上記（参考２）で説明したような収集手口が例として挙げられている。学術に関する依頼は急激に増大しており、2013年においては最も活発な手口であった。学術コミュニティは予見しうる将来にわたり、最大の標的となる可能性が高いとDSSは警告を発している。

DSSのパンフレットによると、報告した方がよいかもしれないものには次のようなものがあり得る。

・学部、修士、博士やその他の研究員への応募や要望
・研究論文等の研究関係の報告や文書に対するアクセスへの要望
・論文や出版原稿等研究関連の援助や査読の要望
・国際会議への参加や発表の招待

これらの要望や招待が全て懸念があるものと判断されるわけではなく、“unsolicited”なものとされている。“unsolicited”とは、辞書によると「頼んでもいない」といった意味であり、「しつこく押し掛けてくる」といったような意味合いであろうか。

【会議・展示会】[14]

DSSのパンフレットでは、会議や大会、展示会に参加するに当たり、まずは自らの業務で話してもよい内容を理解することだと指摘する。また、自らが有する情報の価値を低く見てはいけない。疑念を持たない人は情報の価値が分かっていないので、情報収集者に狙われやすいと警告している。その上で、パンフレットでは次のように述べている。

情報収集者は参加者や展示者、科学者かもしれない。収集者は機微または秘密指定された情報について直接質問するかもしれないし、公式行事の間や、その後の何気ない会話から情報を引き出そうとするかもしれない。

報告した方がよいかもしれない行為には次のようなものがある。

・あなたの業務内容に向けて会話を仕向けたり、機微な情報や技術へのアクセスを試みる
・秘密保全が保たれていない環境下で議論できる内容を超えて執拗に質問する
・過剰な写真撮影、特に撮影禁止区域における撮影
・様々な認証を受けた職員と話をしようと何度も同じブースに戻ってくる者
・知り合いでもないのに仕事を離れて個人的関係を構築しようとする者
・異常または不審な継続的接触、例えば、フォローアップのメールなど
・複数の者が同じ内容の質問をし、回答できる以上のものを引き出そうとする

[13] Defense Security Service,“Academic Solicitation”（http://www.dss.mil/documents/ci/AcademicSolicitation.pdf）.
[14] Defense Security Service,“How to Prepare for Conference, Conventions & Trade Shows”（http://www.dss.mil/documents/ci/Conferences,ConventionsandTradeShows.pdf）.

・ブースや展示物から者が盗まれたり、なくなったりする

技術的な情報だけでなく、職員の個人情報も狙われている。こうした情報を元に関係構築を図ろうとする。

【海外旅行の危険性】[15]

海外旅行時は国内よりもリスクが大きいと警告している。DSSのパンフレットでは、次のような一般的な注意事項を記述している。強力な情報機関や公安組織のある国では、外国人旅行者の行為（ホテル内も含む）は全て監視され、記録されている可能性がある。不必要な電子機器は国内に置いて行くことである。ホテルの部屋を出る前に、部屋の様子を覚えておき、戻ってきた際に（誰かが侵入したかどうか）比較をする。機微な話は制限する。公的な空間は機微な情報の議論にふさわしいことはめったにない。

【外国人訪問客の受入準備】[16]

DSSのパンフレットでは、訪問者が情報を引き出すために使われる手法がいくつか紹介されている。まず、【会議・展示会】で指摘されていたことと同様に、訪問者が同じ質問を手を変え品を変え聞いてきたり、同じ訪問者が別々の職員に同じ質問をする手口が紹介されている。

他に訪問者がウロウロして、エスコートから逃れようとする手口がある。逃れることに成功したら立ち入り制限区域に入ったり、機微な情報へのアクセスを試みる。

反対に訪問者がエスコートだけを引き離して隅に連れていき、承認されていないトピックについて議論しようとする手法もある。また、直前に新たな訪問者を追加して、訪問者の適正性を確認する時間的余裕を与えないこともある。さらに到着後に別の案件について協議しようと試みることもある。

訪問者の質問に回答がなかった際、心理的に回答を強制するために、不快感を示し、気まずい雰囲気を醸し出すことも手口として挙げられている。

受入準備としては次のようなことが指摘されている。

・訪問前にエスコート担当者や訪問者に同行する担当者に議論してよい内容と、議論してはいけない内容を説明する
・ありそうな質問に対する標準的な回答を用意する
・訪問者が機微な、または秘密指定された情報を見聞することにならないかを確認するために、訪問前に施設内を見て回る

軍事、情報関連契約に関する質問や、デュアルユース技術に関する質問は、事前に承認されたものでない限りは不審な行動と考えるべきである。

【内部脅威】[17]

DSSのパンフレットには、いわゆる内部脅威（insider threat）に関するものもある。2において、不審な接触として、「既知の情報機関員、または情報機関員ではないかと疑われる者と、認証を受けた職員の接触」や、「他国の情報機関の工作活動に職員が標的とされている可能性を示唆する接触」が挙げられていたが、こうした接触は工作員が職員に接触してくるだけでなく、工作員に職員が（自らの意思で）接触するという場合もあり得る。こうしたケースでは、職員は様々な情報にアクセスする資格を有しており、組織内部の弱点なども把握し、利用することも考えられる。

個々の兆候は些細であっても、他の兆候と合わせることで行動様式が明らかになることもある。こうしたスパイ活動をしている可能性がある兆候には、次のようなものが挙げられる。

・報告が必要であるにもかかわらず、海外渡航や外国人との接触を報告しない
・アクセスが許可されていない区域に入ろうとする
・業務に関係のない時間帯に勤務したり、一人で仕事をしたいと異常に固執する
・繰り返し又は不必要な執務時間外の労働
・秘密指定された情報に資格なしにアクセスしよ

[15] Defense Security Service,“Foreign Travel Vulnerability”（http://www.dss.mil/documents/ci/ForeignTravelVulnerability.pdf）.
[16] Defense Security Service,“Preparing for Foreign Visitors”（http://www.dss.mil/documents/ci/ForeignVisitors.pdf）.
[17] Defense Security Service,“Insider Threat”（http://www.dss.mil/documents/ci/InsiderThreat.pdf）.

うとする
・怪しいダウンロード
・可搬メディアの許可なき利用
・不必要な秘密情報のコピー

その他、生活上のストレスや、アルコールやギャンブル依存、金銭面のトラブル等が、生活上の兆候である。また、こうした兆候は職場における暴力発生の可能性を指し示す兆候でもある。

③情報収集主体と技術分野

情報収集主体は（参考３）のように、収集を図っている技術分野については（参考４）のように分類されている。これらは昨年版と同様である。

（参考３）情報収集主体[18]

1. 企業
2. 政府関係
3. 個人
4. 政府
5. 不明

（参考４）技術分野の分類（29分類）[19]

1.航空システム	2.農業	3.装備・残存性	4.生物	5.化学
6.認知神経科学	7.指揮・統制・通信・コンピュータ（C4）	8.人間行動計算モデリング	9.指向性エネルギー	10.エレクトロニクス
11.エネルギー物質	12.エネルギー・システム	13.地上システム	14.レーザー	15.製造装置・製造加工
16.海洋システム	17.材料（原料・加工）	18.医療	19.ナノテクノロジー	20.原子力
21.光学	22.測位・航法・時間	23.量子システム	24.レーダー	25.センサー（音響）
26.シグネチャー・コントロール	27.ソフトウェア	28.宇宙システム	29.合成生物学	

5. 分析の活用

DSSは報告を受領し、分析しているだけではない。必要に応じて法執行機関や情報コミュニティに通報している。また、産業界には脅威削減に向けた取り組みについて情報提供を行っている[20]。2014年は、34,000件を超える通報から、989件の捜査等に至ったという[21]。

6. 2015年版DSS報告書

①概要

2014年にDSSにもたらされた報告の概要は（参考５）のとおりである。

②特集：偽造電子機器（マイクロエレクトロニクス）

DSS報告書では、毎年、「特集」として標的とされる技術分野がクローズアップされてきた。2015年版では技術分野ではなく、偽造電子機器の特集が組まれている[22]。国防省や認証契約者が、直接、疑惑のある取引に従事することは稀であると思われるものの、米国内の個人の販売店やブローカーが、偽造疑惑のある電子機器を海外から輸入し、認証契約者に売り込んでいる事例をDSSは確認していると指摘している。さらに、こうした企業は、輸出管理が必要な電子機器を外国政府機関のために調達しようともしているという。国防省では旧式の部品に依存しているため、こうしたリスクが生じる。これは必ずしも維持・管理のためだけでなく、開発の場面でも旧式のマイクロエレクトロニクスを利用することがあるという。

報告書では、認証契約者は次のような場合には注意をすべきであると警告している。

・低価格に注意：認定販売店の価格よりもかなり安い提案
・短いリードタイムに注意：本来の製造者よりも

[18] Defense Security Service, “2015 Targeting U.S. Technologies”, p.7.
[19] Defense Security Service, “2015 Targeting U.S. Technologies”, p.9. 2013年以前の分類との比較は、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－」36頁参照。
[20] Defense Security Service, “2015 Targeting U.S. Technologies”, p.4.
[21] Defense Security Service, “2015 Targeting U.S. Technologies”, p.3.
[22] Defense Security Service, “2015 Targeting U.S. Technologies”, p.14-16.

（参考５）2014年にDSSにもたらされた報告の概要

地域	東アジア・太平洋	中近東	南・中央アジア	欧州・ユーラシア	西半球	アフリカ
報告数	38%	21%	15%	12%	７％	１％
脅威度	深刻	高	中	中	中	低
最も狙われた技術	エレクトロニクス	航空システム	エレクトロニクス	C4	エレクトロニクス	航空システム
収集手口	学術に関する依頼	学術に関する依頼	求職	技術獲得活動	情報提供要求	情報提供要求
収集主体	企業	政府関係	企業	企業	企業	企業

かなり短いリードタイムの提案
- 外部検査機関の調査：偽造探知に外部検査機関を利用する場合、当該施設が信用できる機関であることを確認
- 目視だけでは不十分
- ライフサイクルを考慮した購入：本来の製造者は、前もって１年前には製造中止を発表する。もし今後も必要であるならば、疑惑の取引に手を染めるリスクやコストよりも、予め購入しておくコストの方が低いかもしれない

③東アジア・太平洋地域の動向[23]

2015年版DSS報告書の東アジア・太平洋地域の分析は、以下のとおりである。

東アジア・太平洋地域の機関は、認証を受けた産業基盤にある機微または秘密指定された情報や技術を、依然として最も活発に収集している。狙われた技術のトップ５は、エレクトロニクス、C4、航空システム、ソフトウェア、海洋システムの順で、2013年と技術の構成は同じである（順位に変動あり）[24]。報告されたものは、宇宙開発計画に貢献する構成品であることが多く、この地域の近代化で焦点が当てられている分野であるからだと思われる。認証を受けた産業は、数多くの宇宙関連エレクトロニクスに関する要求があったことをDSSに報告しており、中にはITARで規制されているものもある。東アジア・太平洋地域における軍事技術の近代化は、特に地域のライバルに対抗する選択肢を提供する衛星や海軍に関するものが、今後とも主要な分野となろう。A2/AD能力[25]とともに、宇宙や海軍の優位性を達成するために、東アジア・太平洋地域の国家はC4システムの向上を図っている。ソフトウェアも基本的には衛星に使われるものが狙われているが、航空機やミサイル等の超音速機に使われるものもある。

多くの東アジア・太平洋地域の学術団体は、先進的な軍事研究活動に統合することによって、研究開発を進展できる基礎的な知識を獲得するために、自らの地位を利用している。2014年において最も用いられた収集手口は学術に関する依頼であり、全体の24%を占める。軍事分野に関心を有する大学や研究活動での身分を求めるものである。多くの東アジア・太平洋地域の研究機関は、民生用途やデュアルユースの技術を研究しているが、軍事用途の研究開発の主要な貢献者でもある。米国の情報コミュニティは、これらの研究機関と技術を共有することは危険であり、軍需品の生産ラインに技術を組み込まれる可能性があると評価している。

2013年からの最大の変化はネット上の不審活動である。昨年は収集手口の第１位であったが、2014年は第４位に後退している。米国政府等により、東アジア・太平洋地域からのコンピュータ・ネットワークへの侵入が公表され、ネット上の不審活動の利用を一時的に中断させたか、減少させた。東アジア・

[23] Defense Security Service, “2015 Targeting U.S. Technologies”, p.18-23. 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－」でも指摘されているとおり、「東アジア・太平洋地域」において基本的に示唆されているのは、中国の動向であると推測されるが、本稿では原文通り「東アジア・太平洋地域」と表記する。大学に対するサイバー攻撃については、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」CISTECジャーナルNo.154（2014年11月）52頁参照。

[24] 加藤もえ「米国違反事例2014（１）」CISTECジャーナルNo.156（2015年３月）83頁では、「ここ数年同様の傾向が見られるように、中国向けはマイクロエレクトロニクスなど電子部品が多く」と指摘されており、法執行案件でも同様の傾向が伺える。

[25] A2/ADとは、Anti-Access/Area-Denialのことで、「アクセス（接近）阻止／エリア（領域）拒否」と訳される。具体的には、A2能力とは敵対者がある作戦領域に入ることを阻止するための能力を指し、AD能力とは、作戦領域内で敵対者の行動の自由を制限するための能力を指す。A2/ADに用いられる兵器としては、弾道ミサイル、巡航ミサイル、対衛星兵器等があげられる。防衛省『平成27年版 防衛白書』（日経印刷、2015年）３頁参照。

太平洋地域の主体は、引き続き認証を受けた産業のネットワーク防御を打ち破ろうとしている。幸いなことに、認証契約者からのネット上の不審活動の継続的な報告によって、他社の計画中の事業や現在進行形の事業の変更、脅威の軽減に役立つ指標や警告を提供している。

情報提供要求では、最終需要者を示さなかったり、用途があいまいであったりする。さらに、訪米による情報収集も利用している。多くの報告されたケースでは、訪問団に既知の情報機関員や、情報機関員が疑われる者が含まれている。

7. 日本への示唆

ここまでDSS報告書の作成方法から2015年版の概要を見てきたが、最後に日本への示唆について簡単に触れておきたい。言うまでもなく、DSS報告書の本来の目的である諸外国による情報収集活動の態様こそが直接的な示唆であり、先端技術を数多く有する日本でも同様の事案が生起する可能性が考えられ、重要な警告を与えてくれる。同時に、DSS報告書の作成過程を振り返ることにより、他にも様々な示唆を見出すことができる。

第一に日本にはDSSに相当する機関がない。2015年10月に防衛省に防衛装備庁（装備庁）が設置されたことから、所掌上は装備庁が最も近似しているが、現時点において、装備庁内にDSSに相当する部局はないものと思われる[26]。各政府機関がそれぞれ保有する秘密を管理しているが、そもそも特定秘密の保護に関する法律（特定秘密保護法）上の特定秘密に該当する秘密以外には、政府部内においてすら守秘義務以上の秘密保護制度はないのが実情である。契約者に秘密情報の管理を要求する以前に、政府部内の秘密保護が問われている[27]。

第二に、政府機関から秘密情報の開示を受けた者の管理義務や、不審な接触の報告義務をいかなる形で設定するか、という論点が考えられる。特定秘密保護法上の特定秘密の場合には、同法の規定に従った契約等で義務付けることが考えられる（特定秘密保護法第８条）。特定秘密に該当しない秘密の場合には、秘密情報の開示を受ける形態や規制を受ける法によって様々な方法が考えられる。例えば、武器等製造法上の製造許可に条件を付すことができるので（武器等製造法第21条）、許可条件として履行させることがあり得る。他方で、武器等製造法上の武器は、外国為替及び外国貿易法（外為法）で輸出許可対象とされる武器（輸出貿易管理令別表第１の１の項に該当する品目）と比べて、その範囲が著しく狭い上、日本の場合、武器そのものだけでなく、デュアルユース品の管理も重要であることを踏まえれば、外為法上の輸出者等遵守基準（外為法第55条の10）に規定することも考えられる。さらに、大学や研究機関への不審な接触に対する報告であれば、研究費や補助金等を受託する際の条件として規定することが最も効果的ではないかと考える。例えば、厚生労働省の科学研究費補助金では、研究の過程において、国民の生命や健康に重大な影響を及ぼす情報を把握した場合には、厚生労働省へ報告するように依頼されている[28]。例えば、バイオテロ等で利用され得るような情報（たとえ研究開始時点では意図していなかった成果だとしても）が想定されるのではないかと思われるが、こうした形で不審な接触についても報告を依頼することが考えられる。

第三に、収集・分析した情報を政府内や、不審な接触の報告者である企業や大学・研究機関等と、どのように共有していくかも考える必要がある。一方

---

[26] 防衛省設置法第36条では、装備庁の任務として「装備品等について、……研究開発、調達、補給及び管理の適正かつ効率的な遂行……を任務とする」とするとあり、本稿で検討してきたようなDSSの任務は文字通り、装備品等に関する情報「管理の適正」さを保つ業務と言えよう。

[27] 特定秘密に当たらないが、秘密保護の必要性が検討されるべきものとしては、例えば、原子力関連の情報やロケット関連の情報が考えられよう。原子力関連情報の秘密保護については、八木雅浩「特許制度に基づく技術情報の公開による大量破壊兵器の拡散リスク」CISTECジャーナルNo.154（2014年11月）８-18頁、拙稿「原子力基本法と特許法－秘密特許制度との関連を考える－」CISTECジャーナルNo.161（2016年１月）65-72頁も参照。ロケットについて、秘密保全のための法制の在り方に関する有識者会議「秘密保全のための法制の在り方について（報告書）」（2011年８月８日）４頁（https://www.kantei.go.jp/jp/singi/jouhouhozen/dai3/siryou4.pdf）では、人工衛星やロケットの機微技術が秘密保護の多少として含められるべきだと指摘されている。さらに、これらの情報の場合、情報作成・保有の主体は政府に限られず、国立研究開発法人等であることも想定される。

[28] 厚生労働省大臣官房厚生科学課「平成27年度厚生労働科学研究費補助金事務処理要領」（2015年４月10日）（http://www.mhlw.go.jp/file/06-Seisakujouhou-10600000-Daijinkanboukouseikagakuka/kitei2_1.pdf）。

的に報告を受けるだけで、その情報がどのように活用されたのか、そもそも活用されたのか、が分からなければ、報告側にもインセンティブがない。DSS報告書は、報告書自体が報告者に対するフィードバックになっている。また、政府内でも適切な部署、例えば、違法行為であれば警察に対して適時に情報共有がなされる態勢になければ、せっかく収集した情報を有効に活用することができない。

第四に、秘密情報の提供を受ける企業や大学・研究機関の立場から考えてみよう。DSSが啓発用に作成しているパンフレットは、技術情報がどのような形で狙われ、流出するのかについて、豊富な事例を提供している。狙われる側である企業や大学・研究機関にとっては、技術情報の管理に対する考え方が示されている。技術情報の管理に当たっては、輸出管理は大事な要素の一つではあるが、むしろ人事や情報セキュリティ面からの対応が求められている側面も強い。こうした対応と組み合わせて、組織全体としての技術流出防止のための措置が講じられることが必要であることが分かる。

2015年版のDSS報告書は、冒頭でウッドロー・ウィルソン元大統領の言葉に言及しているが、本稿では最後に当該部分を引用し、他山の石としたい。

> 「私は自らの頭脳を利用するだけでなく、借りてこられるものも利用する」、ウッドロー・ウィルソンはかつてこう言った。米国の認証を受けた産業基盤が保有する「頭脳」を借用しようとし、知的財産を盗み取ろうとする外国からの収集活動は、米国に対する持続的な脅威となっている[29]

[29] Defense Security Service, “2015 Targeting U.S. Technologies”, p.3.