〈2〉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―

情報サービス・研修部　調査課長　**風間　武彦**

1. はじめに

米国の軍事技術・情報を保護する任務にあたっている米国防総省国防保全局（Defense Security Service：DSS）は2014年８月11日、“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”を公表した。本報告書は、DSSが秘密区分指定資料にアクセス権を持つ防衛関連企業（Cleared Defense Contractor：CDC）から受けた「不審接触報告（Suspicious Contact Report：SCR）」などを基に、2013会計年度（FY2013）の諸外国による米国の機微技術の情報収集・調達活動等を分析したものである。

本稿では、８月11日に公表された2014年版と共に過去３年間に公表された同報告書を基に、米国の機微技術の獲得を狙う諸外国、特に中国を始めとする東アジア・太平洋地域を中心に、その情報収集活動の動向を紹介する。

2. 米DSSの調査分析方法

（1）概要

米DSSは、“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry”（以下、「米DSS報告書」と呼ぶ）の中で、米防衛関連企業（CDC）が自社及びその従業員に対して行われた不審な接触及び潜在的情報収集活動に関する報告（SCR）を基に、情報収集主体（Collector Affiliation）の収集手口（Method of Operation）や収集対象技術を定義・分類し、世界を６地域に分けて対米情報収集活動を分析している。なおDSSは情報分析に当たり、2014年版の報告書より、CDCからの報告を新たに３分類、すなわち１）不審接触報告（SCR）、２）確証の無い接触報　告（Unsubstantiated Contact Report：UCR）、３）評価対象外（Assessed No Value：ANV）の３つに分類し、１）「不審接触報告（SCR）」は従来と同様全て集計・分析の対象とする一方、２）「確証の無い接触報告（UCR）」は一部のみ集計・分析の対象とし、３）「評価対象外（ANV）[1]」は全て集計・分析の対象から外している。これにより2012会計年度までSCRに分類されていた類の報告が2013会計年度からUCRに分類され、2013会計年度の分類基準では集計・分析対象から外れる可能性もあるという。2012会計年度以前と2013会計年度の集計・分析結果を比較する場合には、この点を予め考慮しておいた方が良いだろう。

（2）情報収集主体

米防衛関連企業（CDC）に対して不審な接触を行った情報収集主体は、①企業（Commercial）、②政府関係（Government Affiliated）、③個人（Individual）、④政府（Government）、⑤不明（Unknown）の５つに分類され、〔図表１〕のように定義されている。

（3）情報収集手口

情報収集の手口についてDSSは、①大学を利用した情報収集、②サイバー攻撃等を用いた情報収集、③企業買収・フロントカンパニー等を利用した技術獲得、④求職活動を利用した情報収集、⑤電話・E-mail等による情報提供依頼、⑥勧誘あるいはマーケティングを利用した情報収集、⑦訪米を利用した

[1] ANVは、例えば電子メール或いはクレジットカード詐欺などのようなCIの間接的懸念のみの報告である。

情報収集、⑧米国企業等とのコネクションを利用した情報収集、⑨会議及び見本市を利用した情報収集、⑩窃盗などの犯罪行為、⑪米国人旅行客を標的にした情報収集の11の手口に分けており、それぞれの定義は〔図表２〕の通りである。なお、各手口の英語表記はFY2012以降（米DSS報告書2013年版以

〔図表１〕米防衛関連企業に不審な接触を行った情報収集主体の分類と定義

分　類	定　義
①企業	防衛部門を含む商取引を行うエンティティ（防衛関連企業などの企業を含む）
②政府関係	米国の機微なあるいは機密扱いの情報や輸出管理対象情報の獲得という共通の目的を持つ外国の政府関係機関、すなわち、調査研究所、実験所、大学、政府と契約関係にあるエンティティなど。
③個人	報酬を得るため、あるいは表面上は学術研究目的で、米国の機微なあるいは機密扱いの技術や情報、輸出管理対象の（技術）情報を獲得しようとする人物。
④政府	外国の国防省及びその下部機関、外国の軍関係者、軍事連絡機構関係者など。
⑤不明	－

（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014, p.6 を基に筆者作成

〔図表２〕米防衛関連企業に対する情報収集の手口

分　類	定　義
①大学を利用した情報収集（Academic Solicitation）	大学を利用した情報収集には、大学に在籍する仲間への情報提供依頼、大学への要員（仲間）配置、学術論文あるいは発表資料に対する広範な科学的レビュー、教職員との研究あるいは相談の依頼、教職員／生徒／研究者／職員として学術研究機関・学部・学科あるいはプログラムに入学／入会／参加／就職等の申請を通じて情報収集活動を行うものである。
②サイバー攻撃等を用いた情報収集（Suspicious Network Activity）	サイバー侵入、ウィルス、マルウェア、バックドア攻撃（裏口攻撃）、ユーザーネームとパスワードの取得などを通じたもの。これらは、米防衛関連企業のネットワークへ侵入し、保護情報を獲得しようとする企みである。
③企業買収・フロントカンパニー等を利用した技術獲得（Attempted Acquisition of Technology）	企業買収あるいはフロントカンパニーや第三国を介して、保護情報（protected information）、すなわち装置、設計図、概念図、計画、仕様書などを獲得しようとするものである。
④求職活動を利用した情報収集（Seeking Employment）	履歴書の提出、応募、照会（問い合わせ）など求職活動を利用した情報収集。これらは、外国政府当局に有用な米国の保護情報を入手できる人物を紹介させようとする企みである。
⑤電話・E-mail等による情報提供依頼（Request For Information）	電話、E-mailあるいはwebカード[2]を通じて情報提供を依頼する方法。これらは、架空の見積もり依頼、市場調査、あるいはその他の直接／間接的手段を通じて保護情報を収集しようとする企みである。
⑥勧誘あるいはマーケティングを利用した情報収集（Solicitation or Marketing Services）	販売、説明（representation）、代理店オファー（Agency Offer）あるいは技術サービスあるいはビジネスサービスへの入札を通じたもの。これらは、保護情報を入手しやすい米防衛関連企業とのコネクションを確立しようとする外国のエンティティによる企みである。
⑦訪米を利用した情報収集（Foreign Visits）	諸外国の訪米派遣団が、事前に手配等された米国防衛関連企業（CDC）施設への公式訪問を通じ、機密情報などの保護情報へアクセスし、情報を収集しようとする企みである。
⑧米国企業等とのコネクションを利用した情報収集（Exploitation of Relationships）	米国企業等とのジョイントベンチャー、契約、軍事品の販売、業務提携などの（情報収集主体の国の企業と米国企業の間で）確立されたコネクションを利用した情報収集活動。これらは、機密情報へアクセスするため、既存の合法的あるいは表面上悪意の無い関係を利用しようとする企みである。
⑨会議及び見本市を利用した情報収集（Surveillance）	デュアルユース技術や機微技術（保護情報を含む）に関する会議や見本市における写真撮影やスケッチあるいは詳細な技術的質問などの疑わしい行動を指す。
⑩窃盗などの犯罪行為（Criminal Activities）	窃盗などの犯罪行為で保護情報を獲得しようとする企みである。
⑪米国人訪問客を標的にした情報収集（Search / Seizure）	自国を訪れる米国人（米防衛関連企業の従業員等）の身体検査や身柄拘束等を実施、その際に所有物（コンピュータ等）を検査・没収するなどして保護情報を収集しようとする企みである。

（注）分類の日本語訳は（ ）内の英語を分かりやすく意訳したもの。
（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2012”, December 7, 2012. 及び同2014年版（August 11, 2014）を基に作成。

降）から若干変わっているが、定義内容は殆ど変わっていないので比較する際はさほど気にする必要は無いだろう。

（4）地域区分

DSSが情報収集主体の国籍を把握していることは言うまでもないが、公表される報告書では、世界を以下の6地域に分類した上で、SCRの集計・分析結果が報告されている。

①東アジア・太平洋（北朝鮮、中国、台湾、韓国、日本、東南アジア諸国、豪州など）
②中近東（イラン、イラク、イスラエル、シリア、UAE、エジプト、リビアなど）
③欧州・ユーラシア（EU諸国、ロシア、ウクライナ、トルコなど）
④南・中央アジア（インド、パキスタン、アフガニスタン、タジキスタン、ウズベキスタンなど）
⑤アフリカ（ケニア、カメルーン、ナイジェリア、南アフリカなど）
⑥西半球（北米及び中南米諸国など）

DSSがこのように国の特定を避けながら地域毎にSCRを分析報告している背景には、特定国との摩擦回避等があると考えられるが、一方で報告書に掲載された違反事例では、中国或いは中国系米国人等が関与した違反事例等が毎年のように掲載されている。これは、米防衛関連企業（CDC）に対する不審接触報告（SCR等）が最も多い東アジア・太平洋地域の情報収集主体が主に中国であることを意味すると同時に、米国が最も懸念を抱いているのが中国による情報収集活動であることを示すものである。

（5）技術区分－MCTLに基づく分類を中止してIBTLに基づく分類に変更

標的となる技術は2012会計年度まで、軍事機微技術リスト（Militarily Critical Technologies List：MCTL）に基づき20分野に分類されていたが、2013会計年度より産業基盤技術リスト（Industrial Base Technology List：IBTL）に基づき29分野に分類されている。主な変更点として、1）MCTLの情報システム及び情報セキュリティが再編されてC4（指揮・統制・通信・コンピュータ）とソフトウエアに分類される一方、レーザー、光学及びセンサーは、それぞれレーザー、光学、センサー（音響）、レーダーに再分類されている、2）兵器効果（Weapons Effects）が分割されて原子力、化学及び生物学の各分野に編入されている、3）新しく合成生物学（Synthetic Biology）、ナノテクノロジー、農業、認知神経科学（Cognitive Neuroscience）、人間行動計算モデリング（Computational Modeling of Human Behavior）の5分野が追加されているなどの点が挙げられる。このため、過去の報告書と比較する際はこうした変更点に注意が必要である。なお、MCTLとIBTLの対応関係は〔図表3〕の通りである。

3. 全体傾向

（1）増加する不審接触報告（SCR）件数

諸外国のエンティティによる米防衛関連企業への不審な接触（SCR）等は年々増加している。DSSによると、2010会計年度（FY2010）は対前年比60％増、2011会計年度（FY2011）は同75％増、2012会計年度（FY2012）は同50％増、2013会計年度（FY2013）は同33％増となっており[3]、FY2013のSCR件数は30,000件を超えるという[4]。

（2）不審接触報告件数の地域構成比－東アジア・太平洋が最多、近年は南・中央アジアが急増

FY2013の不審接触報告件数の地域構成比は、東アジア・太平洋地域が最も大きく43％、次いで中近東地域の18％、南・中央アジア地域の16％、欧州・ユーラシア地域の11％、西半球の6％、アフリカの1％となっている。過去4年の地域構成比の推移をみると、東アジア・太平洋地域や中近東地域が概ね横ばいで推移しているのに対し、南・中央アジア地域がFY2010の9％からFY2013には16％に拡大する一方、欧州・ユーラシア地域はFY2010の15％から

[2] webcard：インターネットで送ることのできるポストカード
[3] DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry ”の2012年版、同2013年版、同2014年版
[4] DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014, p.71.

〔図表３〕MCTLとIBTLの対応関係

軍事機微技術リスト（MCTL）の分類		産業基盤技術リスト（IBTL）の分類
情報システム（Information Systems）	⇒	指揮、統制、通信・コンピュータ （Command, Control, Communication, & Computers）
情報セキュリティ（Information Security）		ソフトウエア（Software）
レーザー、光学及びセンサー （Lasers, Optics, & Sensors）	⇒	レーザー（Lasers）
	⇒	光学（Optics）
	⇒	センサー（Sensors）〔音響（Acoustic）〕
	⇒	レーダー（Radars）
地上システム（Ground Systems）	⇒	地上システム（Ground Systems）
航空システム（Aeronautic Systems）	⇒	航空システム（Aeronautic Systems）
海洋システム（Marine Systems）	⇒	海洋システム（Marine Systems）
宇宙システム（Space Systems）	⇒	宇宙システム（Space Systems）
原子力システム（Nuclear Systems）	⇒	原子力（Nuclear）
化学（Chemical）	⇒	化学（Chemical）
生物学（Biological）	⇒	生物学（Biological）
生医学（Biomedical）		
	⇒	医療（Medical）
軍備とエネルギー物質 （Armaments & Energetic Materials）	⇒	軍備と生き残り可能性 （Armament & Survivability）
	⇒	エネルギー物質（Energetic Materials）
指向性エネルギーシステム （Directed Energy Systems）	⇒	指向性エネルギー（Directed Energy）
エネルギーシステム（Energy Systems）	⇒	エネルギーシステム（Energy Systems）
エレクトロニクス（Electronics）	⇒	エレクトロニクス（Electronics）
加工及び製造（Processing & Manufacturing）	⇒	製造装置及び加工 （Manufacturing Equipment & Processes）
測位、航法、及び時間 （Positioning, Navigation, & Time）	⇒	測位、航法、及び時間 （Positioning, Navigation, & Time）
シグネチャー コントロール（Signature Control）	⇒	シグネチャー コントロール（Signature Control）
材料・加工（Materials & Processes）	⇒	材料（原料及び加工）（Materials (Raw & Processed)）
	新規	合成生物学（Synthetic Biology）
		ナノテクノロジー（Nanotechnology）
		農業（Agricultural）
		認知神経科学（Cognitive Neuroscience）
		人間行動計算モデリング （Computational Modeling of Human Behavior）
兵器効果（Weapons Effects）	⇒	（原子力、化学及び生物学へ編入）

（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014, pp.76-77

FY2013には11％に縮小している〔図表４〕。全体でみれば依然として東アジア・太平洋地域のエンティティからの不審接触が圧倒的に多いと言えるが、南・中央アジア地域のエンティティからの不審接触が急増している点が近年の動向で注目すべき点となっている。

（３）情報収集主体の動向

情報収集主体は地域により違いが鮮明になっており、また年度によっても大きな変化がある地域が少なくない。東アジア・太平洋地域は、「政府」、「企業」、「政府関係」が27～28％で多くなっているが、「政府」の比率が低下する一方、政府関係の比率が上昇している。中近東地域は政府関係が全体の4割強を占めるなど最も多いが、個人の比率も高まって

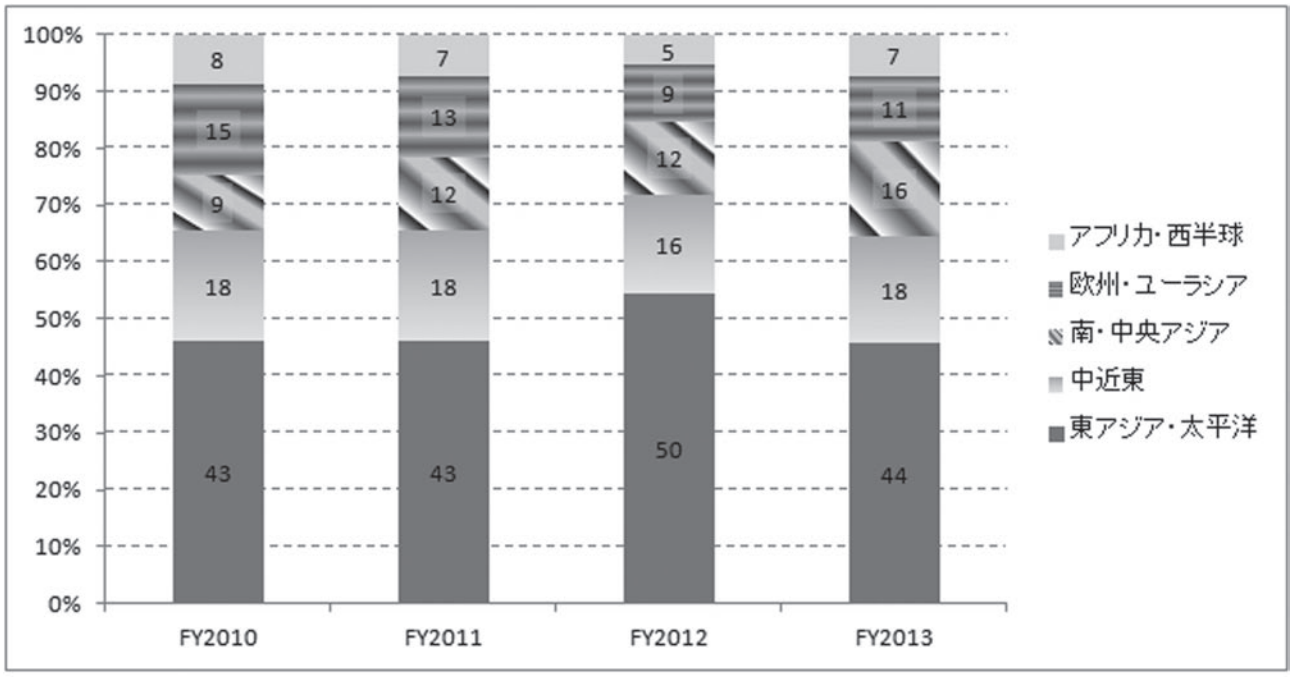
いる。南・中央アジアは個人の急増が際立っている。欧州・ユーラシアは、企業の比率が全体の約4割を占める一方、個人の比率が過去１年で２倍になっている〔図表５〕。

（４）情報収集手口の動向

情報収集手口は、地域毎に大きく異なっており、各地域で最も多い情報収集手口は、東アジアが「サイバー攻撃等を用いた情報収集（30％）」、中近東が「大学を利用した情報収集（46％）」、南・中央アジアが「求職活動を利用した情報収集（40数％）」、欧州・ユーラシア地域が「企業買収・フロントカンパニー等を利用した技術獲得（27％）」となっている〔図表６〕。

（５）獲得を狙う技術

情報収集主体や情報収集手口は地域毎の違いが顕著だったが、獲得を狙う技術は似通っている。東アジア・太平洋、南・中央アジア、欧州・ユーラシアはいずれもエレクトロニクスが最も多く、次いでC4（指揮・統制・コンピュータ・通信）となっている。これらの地域と異なる傾向が見られるのが中近東で、最も多いのが海洋システムで次いでエレクトロニクスとなっている〔図表７〕。



（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry ”の2012年版、同2013年版、同2014年版

〔図表４〕不審接触報告件数の地域構成比の推移

〔図表５〕主要地域の情報収集主体の構成比

	東アジア・太平洋		中近東		南・中央アジア		欧州・ユーラシア	
	FY2012	FY2013	FY2012	FY2013	FY2012	FY2013	FY2012	FY2013
１位	政府（41％）	政府（28％）	政府関係（47％）	政府関係（44％）	政府関係（37％）	個人（36％）	企業（43％）	企業（38％）
２位	企業（28％）	企業（27％）	企業（28％）	企業（22％）	企業（36％）	政府関係（33％）	政府関係（19％）	個人（31％）
３位	政府関係（17％）	政府関係（27％）	個人（11％）	個人（17％）	個人（17％）	企業（24％）	個人（15％）	政府関係（15％）
４位	個人（7％）	個人（10％）	政府（10％）	政府（11％）	政府（6％）	不明（4％）	政府（11％）	政府（10％）
５位	不明（7％）	不明（8％）	不明（5％）	不明（5％）	不明（4％）	政府（3％）	不明（11％）	不明（5％）

（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014.

〔図表６〕地域別にみた情報収集手口の構成比

	東アジア・太平洋	中近東	南・中央アジア地域	欧州・ユーラシア地域
１位	サイバー攻撃等を用いた情報収集（30%）	大学を利用した情報収集（46%）	求職活動を利用した情報収集（40数%）	企業買収・フロントカンパニー等を利用した技術獲得（27%）
２位	大学を利用した情報収集（20%）	企業買収・フロントカンパニー等を利用した技術獲得（16%）	大学を利用した情報収集（20数%）	求職活動を利用した情報収集（24%程度）
３位	勧誘あるいはマーケティングを利用した情報収集（14%）	求職活動を利用した情報収集（9%）	企業買収・フロントカンパニー等を利用した技術獲得（15%程度）	電話・E-mail等による情報提供依頼（18%）
４位	企業買収・フロントカンパニー等を利用した技術獲得（12%）	電話・E-mail等による情報提供依頼（9%程度）	電話・E-mail等による情報提供依頼（7～8%）	訪米を利用した情報収集（8%程度）
5位	電話・E-mail等による情報提供依頼（9%）	訪米を利用した情報収集（9%程度）	勧誘あるいはマーケティングを利用した情報収集（5%程度）	勧誘あるいはマーケティングを利用した情報収集（5%程度）

（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014.

〔図表７〕各地域のエンティティが獲得を狙う技術

	東アジア・太平洋	中近東	南・中央アジア	欧州・ユーラシア
１位	エレクトロニクス（6%）	海洋システム（10%）	エレクトロニクス（9%）	エレクトロニクス（12%）
２位	C4（5%）	エレクトロニクス（8%）	C4（5%）	C4（7%）
３位	航空システム（4%）	航空システム（8%）	レーダー（4%）	航空システム（6%）
４位	海洋システム（4%）	宇宙システム（7%）	ナノテクノロジー（4%）	レーダー（4%）

（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014.

4. 東アジア・太平洋地域

SCR等の件数が最も多いのは東アジア・太平洋地域で、その大半は中国であると見られていることを踏まえながら、安全保障上の中国の対外情報収集活動の懸念度の大きさを考慮し、以下、中国が主体となっている東アジア・太平洋地域の情報収集活動をクローズアップして紹介する。

（１）情報収集主体

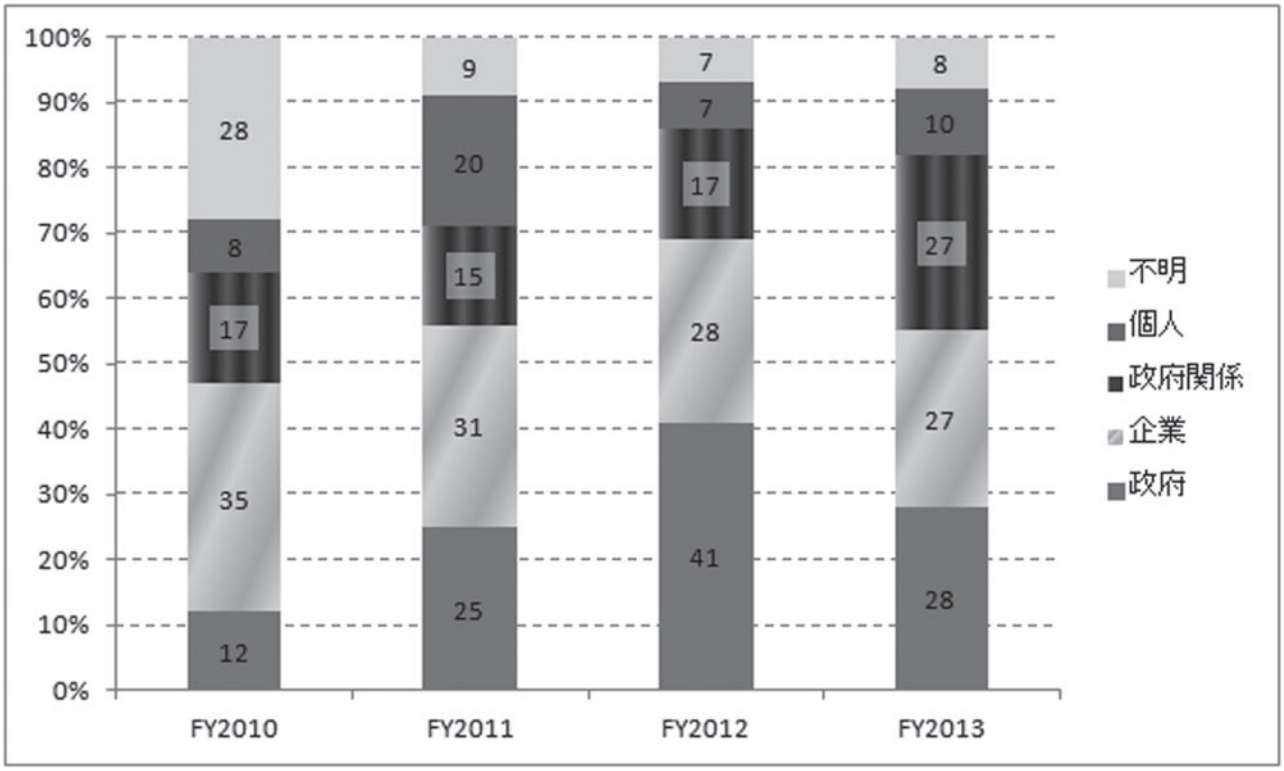
東アジア・太平洋地域の情報収集主体（主に中国）は、2011会計年度まで「企業」が最も多かったが、2012会計年度は「政府」の構成比が41%で最も多くなった。2013会計年度は、「政府」、「企業」、「政府関係」の構成比が27～28%でほぼ拮抗している〔図表８〕。東アジア・太平洋の情報収集主体の収集手口の特徴は、様々なそして執拗なアプローチをとる点であるという。しばしば複数のエンティティと収集手口を使って同時に技術を獲得しようとしており、あるエンティティが情報獲得に失敗すれば、次のエンティティが別の手口でという形で、国家ぐるみで収集を試みている可能性が高いとされている[5]。

（２）情報収集手口

東アジア・太平洋地域（主に中国）の情報収集手口をみると、2010会計年度は「電話・E-mail等による情報提供依頼」の比率が41%と最も大きかったが、同手口は2011会計年度以降に激減し、2013会計年度の比率は9%に留まっている。他方、2011会計年度以降は「サイバー攻撃等を利用した技術獲得」が最も多い手口となっており、2013会計年度は30%を占めている。また、「大学を利用した情報収集」や「企業買収・フロントカンパニー等を利用した技術獲得」は近年拡大傾向に有り、2013会計年度はそれぞれ20%、14%を占めている〔図表９〕。

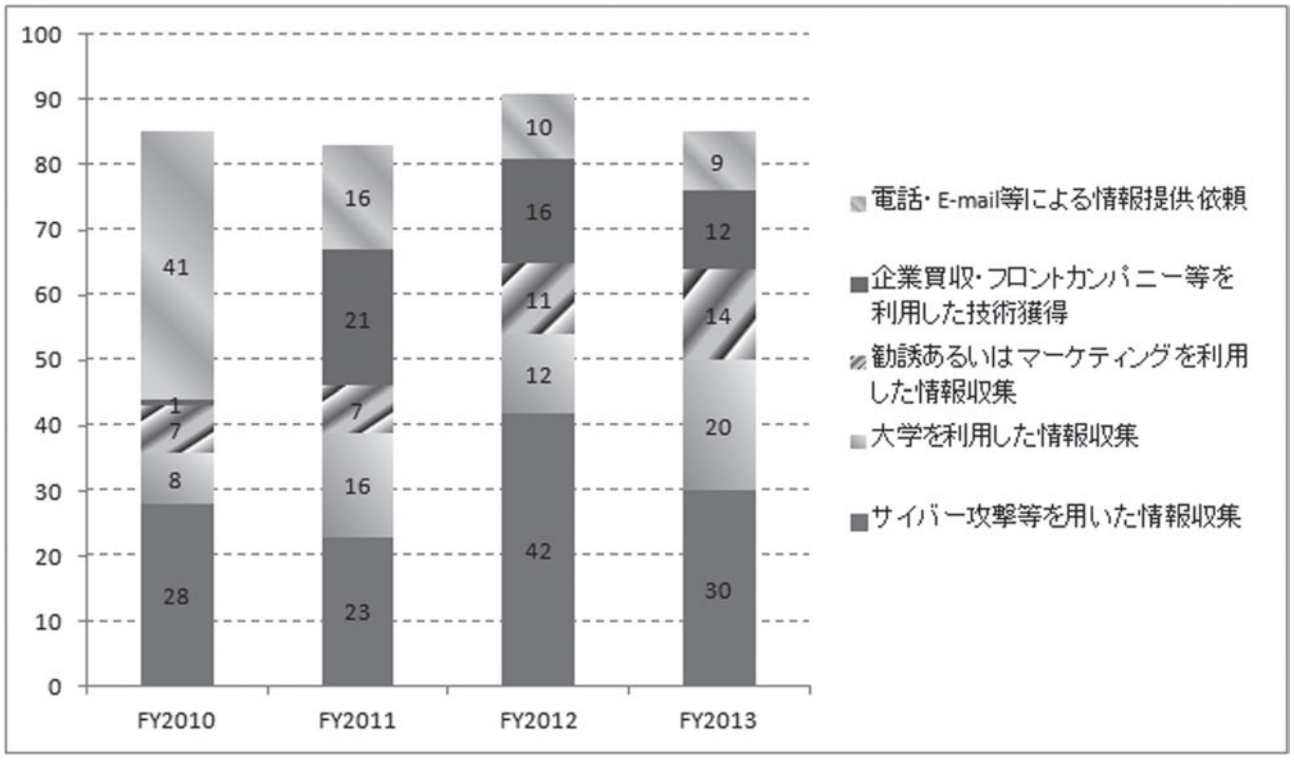
「サイバー攻撃等を利用した技術獲得」で最も多い手口は、スピアフィッシングであるという[6]。ス

[5] DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2012”, December 7, 2012, pp.24-25.



（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry”の各年版。

〔図表８〕東アジア・太平洋地域の情報収集主体の構成比の推移



（出所）DSS,“Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry”の各年版。

〔図表９〕東アジア・太平洋地域（主に中国）の情報収集手口の推移

ピアフィッシングはフィッシング詐欺の一種で、特定のターゲットに対して重要なデータや個人情報を奪おうとする手法のことである。この手法で米防衛関連企業の担当者にマルウエアを送りつけて、機微情報のアクセスに必要な情報を盗もうとしているとされる。「企業買収・フロントカンパニー等を利用した技術獲得」で最も多い手口は、外国のエンティティが、防衛関連企業（CDC）に製品の発注メールを送るというものであるとされる一方、「電話・E-mail等による情報提供依頼」は技術やシステムに関して「Yes」「No」で回答する一般的な内容の質問とされる。これら２つの手口を用いて低リスクで収集できると分かれば、更なる技術情報の獲得に動くという[7]。

（３）標的にする技術

東アジア・太平洋地域（主に中国）が標的にしている米国の機微技術は主に、エレクトロニクス、C4（指揮・統制・コンピュータ・通信）、航空システム、海洋システムで、2013会計年度のSCR等の件数の比率は、それぞれ6%、5%、4%、4%となっている。

エレクトロニクス分野で標的となっている技術は、宇宙機器向けの耐放射線集積回路、モノリシックマイクロ波集積回路（MMIC）、半導体、パワーアンプ（Power Amplifier）であり、C4分野では、導波管、航空機の機上データ取得システム（Airborne Data Acquisition System：ADAS）、携帯式衛星通信端末（Man-portable Satellite Communications Terminals）となっている。また、航空システム分野では戦闘機、無人航空機（UAV）、海洋システム分野では水中無人機（AUV）、数値流体力学（Computational Fluid Dynamics; CFD）であるという[8]。

米DSS報告書では毎年、標的となる特定の技術がクローズアップされている。FY2010は無索無人潜水艇（AUV）、FY2011は耐放射線半導体、FY2012はミサイル技術、そしてFY2013は慣性航法装置（INS）が取り上げられている。

FY2013のSCR動向を分析した最新の米DSS報告書2014年版（2014年公開）では、米国の慣性航法装置（INS）の主要部品の技術全てが諸外国の標的となっており、特に中国[9]の企業等が長年にわたって米国のINS技術の獲得を試みてきたと指摘されている。INSは、慣性計測装置（Inertial Measurement Unit：IMU）とコンピュータで構成され、IMUは通常、ジャイロスコープ及び加速度計から構成されている。中国などが狙っているのは、最先端のジャイロスコープ、特にリングレーザージャイロ（Ring Laser Gyroscope：RLG）及び光ファイバージャイロ（Fiber Optic Gyroscope：FOG）であるという[10]。

5. おわりに

日本は世界有数のデュアルユース技術先進国でもある。米国同様、諸外国、特に中国の標的になっている可能性は十分にあり、米国のSCR動向などを参考にしながら、技術流出を防ぐべく必要な対策を講じていく必要がある。特にサイバー攻撃関連は既に米国も深刻な被害を受けており他人ごとではない。100％確実に防ぐ手段はきわめて難しいが、国益、企業利益を守ると言う観点でも十分な対策が必要だろう。

---

[6] DSS, “Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014, p.27.
[7] DSS, “Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2012”, December 7, 2012, pp.27-28.
[8] DSS, “Targeting U.S. Technologies: A Trend Analysis of Reporting from Defense Industry 2014”, August 11, 2014, p.31.
[9] 原文では「East Asia and the Pacific」とあるが、紹介されている関連の違反事例は中国人が関係しているものであり、主に中国を指すと考えられる。
[10] Defense Security Service , “Targeting U.S. Technologies: A Trend Analysis of Cleared Industry Reporting”,August 11.2014, p.20.