日経・CSISバーチャル・シンクタンク
CSIS-NIKKEI VIRTUAL THINKTANK

政府のインテリジェンス機能強化に向けて

―― 対外情報収集・分析能力のネットワーク化試案 ――

2015年9月23日

インテリジェンス問題検討チーム

本提言における意見、見解等は、すべて検討チームに所属するメンバーに帰するものであり、当該メンバーが現在所属し、あるいは過去に所属したいかなる組織の意見を代表するものではありません。

インテリジェンス問題検討チーム
チームの会合日程等は本提言の巻末付録に示す。本提言をまとめるにあたり、日本や米国のインテリジェンスや安全保障をはじめとする各分野の一線級の識者から多くのご指摘・ご助言を頂戴した。その所属や名前を明らかにすることはできないが、この場を借りて深く感謝いたしたい。無論、本提言内容については、全てインテリジェンス問題検討チームの責に帰するものである。

エグゼクティブサマリー

2013 年 12 月に国家安全保障会議、2014 年 1 月に同会議の事務局たる国家安全保障局が相次いで発足し、政府の外交・安全保障政策の企画・立案機能は大きく変化した。そして、政策立案の基礎となる「対外情報の収集・分析」のあり方については、これまで様々な提言がなされてきた。とはいえ、提言を実際に反映するような改革の試みは、必ずしもこれまでうまくいっていない。プライバシー保護等の観点から政府による情報機能強化を巡る議論は慎重に進められるべきであるが、他方で近年、国の安全や経済的繁栄の維持、国民の生命・財産の保護に必要な情報がますます多様化・専門化していることに鑑み、政府の情報機能強化は「常にアップデートすべき課題」との認識も必要である。

本報告書では、これまで制度改革への関心が偏る傾向が見られたこれまでの提言とは異なるアプローチで、とりわけ民間の視点強調する立場から我が国のインテリジェンスの課題について再点検を行った。その際に、政府の情報機能（以下「インテリジェンス」）の定義を「国民の生命・財産や企業のグローバルな活動に対する脅威の発現を未然に防ぎ、対策を検討するための一助となる情報を提供すること」とした。その結論として、「官民双方の協力による（日本型）インテリジェンス・ネットワークの拡充」をここでは提言している。なお、この報告書をとりまとめたメンバーの多くは、一般企業や社団法人など民間部門に所属しており、提言の内容はそれらの実務経験や専門知識に基づいて、より総合的で多面的なかたちで報告をまとめることになった。その要旨は、以下の通り。

＜総論＞

提言1. 政府は、インテリジェンスにおける省庁間の「縦割り」がもたらす問題を克服する努力を継続するのみならず、多様化・専門化するさまざまな領域につねに関心を配るべきである。また、インテリジェンスにおいて、必要に応じ民間や非政府部門と連携できる環境を整備し、より高度な「オールソース・アナリシス」を追求すべきである。特に、以下の３分野（在外邦人保護、科学技術情報、サイバーセキュリティー）におけるインテリジェンス機能の強化に注力すべきである。

＜在外邦人保護のためのインテリジェンス強化＞

提言2. 海外で活動する日本企業や非政府組織、研究者などは現地社会の幅広い層と接点を持っており、海外安全情報を収集する上で重要な情報リソースとなりうる。政府はこれら非政府部門との情報交換を重視し、より積極的にアプローチすべきである。

提言3. 日本人がテロの標的となりうる状況にある中、企業の海外派遣社員やその家族の安全確保が重要課題となっている。しかし、特に中東のイスラム諸国や東南・南アジア諸国など重要な地域の専門家は恒常的な不足状態にある。現地の言葉や文化を理解する人材の養成を政府として後押しする一方、国内の大学・シンクタンクによるこれら諸国の識者招聘や留学生受け入れ、国際セミナーの開催などを積極的に支援し、地域研究と人材交流の厚みを増していくべきである。

提言4. 短期旅行者への海外安全情報の提供機能の強化を進め、また安全情報に対する国民への啓発を継続・強化すべきである。

＜科学技術安全保障のためのインテリジェンス強化＞

提言5. 先端的な科学･技術はわが国の安全､及び経済的繁栄に資する財産との認識のもと、インテリジェンスに「科学技術安全保障」の観点を導入し、その強化を図るべきである。

提言6. 科学技術や軍事転用可能な資機材等を巡るヒト・モノ・カネのフロー（流れ）について、情報の収集・集約・分析・蓄積・共有・活用を推進すべきである。

提言7. 科学技術情報の収集において、関連する分野の知見や情報を持つ国内の関係団体・機関、企業、大学・研究機関とのネットワークを構築すべきである。

提言8. 企業・大学・研究機関などの人材交流において、科学技術に関する重要情報の流出がわが国の安全の脅威とならないよう、啓蒙活動を行うべきである。

＜サイバーセキュリティーのためのインテリジェンス強化＞

提言9. サイバーセキュリティーと国家安全保障の両方に関するスタッフレベルの識見を深め、想定されるサイバー攻撃への対応策を国家安全保障の観点から常にアップデートすべきである。

提言10. サイバーセキュリティーに関する情報共有のリアルタイム化、情報精度の向上、及び民間企業による情報共有のインセンティブ向上と協力の獲得を図るべきである。

提言11. サイバー攻撃の予防策としてのアトリビューション能力の向上、及びサイバーインテリジェンスと伝統的インテリジェンスの連携強化を推進するべきである。

提言12. インテリジェンスの所作を身に着けた IT プロフェッショナルの獲得と特殊語学の能力向上、各国機関との情報共有を進めるべきである。

以　上

目次

第１章　総論

１．本提言の目的

今回の提言の目的を明確にするために、そもそもインテリジェンスによって守られる国益とは何なのかについて、改めて確認しておきたい。過去の提言では、守られる国益とはすなわち、①国家・国民の安全確保、②経済的繁栄の確保、を目標（＝守るべき国益）として定義している。より細かくみると特徴的な提言もあり、例えば<安防懇 2009>では、「日本の安全」のみならず「海外で活動する国民の安全」もインテリジェンス強化の目的としている。

こうした中で、私たちは<閣議決定 2013>における表現に注目した。そこでは、まず「わが国の平和と安全を維持し、その存立を全うすること」を目的に掲げつつも、「経済発展を通じて平和と安全をより強固なものにする」という項目も掲げている。この点は、とかく一部の軍事分野や治安分野の機能とみられがちなインテリジェンスに対する見方を広げている点で画期的である。そこで今回の提言では、国家インテリジェンス強化の目的について、**「国民の生命・財産や企業のグローバルな活動に対する脅威の発現を未然に防ぎ、対策を検討するための一助となる情報を提供することを通じ、国家・国民の安全と経済的繁栄を維持・確保すること」**と定義し、既往の概念にとらわれずにゼロベースでの議論を行うこととした。

２．過去の提言の整理

ここで、今回の提言を少しでも付加価値のある内容とするために、各論に先立ち、インテリジェンスを巡って過去 10 年程度の中でなされてきた代表的な政策提言・意見について振り返る。これまでインテリジェンスをめぐる議論が何を論点にし、どういう議論の蓄積をしてきたのか。また、インテリジェンスを現在の政治社会情勢に照らし再点検した時に、議論のスコープ（範囲）にどういった点を追加すべきなのかを知ることが目的である。

インテリジェンスに関する提言を下表にまとめた。重要な点は、過去 10 年にわたり、国家インテリジェンスの強化について、ほぼ毎年のように繰り返し提言がなされてきたことである。組織設計のあり方や重点を置くべき分野こそ違え、継続的に多くの提言がなされてきたことは、わが国のインテリジェンス強化に対する関心が民・官・学を問わず高いことを示している。このような各種提言については、2009 年に内閣情報調査室がいったんそれまでの論調をまとめている（<内調 2009>）が、その後は過去の提言を大きく踏み越える提言は見当たらず、概ね主な論点は出尽くしているとの印象をうける。

＜表：国家インテリジェンスを巡る主要提言＞

年月	提言名	文中略称
2004 年 10 月	安全保障と防衛力に関する懇談会	安防懇 2004
2005 年 9 月	対外情報機能強化に関する懇談会	情報懇 2005

2006 年 5 月	小谷賢「わが国におけるインテリジェンスの現状と課題」	小谷 2006
2006 年 6 月	自由民主党「国家の情報機能強化に関する提言」	自民 2006
2007 年 10 月	PHP 研究所「日本のインテリジェンス体制」	PHP2007
2008 年 2 月	情報機能強化検討会議「官邸における情報機能の強化の方針」	情報会議 2008
2009 年 2 月	内閣情報調査室「わが国の情報機能」	内調 2009
2009 年 8 月	安全保障と防衛力に関する懇談会	安防懇 2009
2010 年 8 月	新たな時代における日本の安全保障と防衛力の将来構想	新時代 2010
2011 年 7 月	外交安全保障調査会 NSC・インテリジェンス分科会提言	外安 2011
2013 年 12 月	閣議決定「国家安全保障戦略について」	閣議決定 2013

主な論点とはすなわち、（1）国家のインテリジェンス機能をどこに集約するのかという組織の問題、（2）組織間の連携が不足しているという情報共有の問題、（3）分析能力の不足という能力・態勢の問題、（4）インテリジェンスに関する人材を育成すべきという人材育成・教育の問題、（5）インテリジェンス機能の監視・監督というガバナンスの問題、などである。言い換えれば、このようにインテリジェンスを巡る論点は既に飽和状態にあるといえ、これがインテリジェンスを巡る新たな提言の停滞につながっているのではないか、それが私たちの現状認識と議論の出発点である。

３．本提言の位置づけと射程

果たしてインテリジェンスを巡る議論は今のままで良いのか。足りない部分はないのか。政治社会情勢や科学技術が毎年のように変化・多様化し、情報の所在が分散化し、かつ専門性を高めていく中にあって、インテリジェンスを巡る議論が停滞して良いはずがない。そうした視点から改めてゼロベースで点検した時に、出尽くしたと思われていたインテリジェンスの分野にいくばくかの「アップデート」が必要であることが見出された。それはすなわち、分散し分断されたインテリジェンスを、分野別にも、官民の間でも、接続し共有していくことの重要性である。こうした新領域におけるインテリジェンスのネットワーク化を進めなければ、冒頭に掲げた「脅威の発現を未然に防ぐ」ための国家インテリジェンスの強化は難しいと私たちは考える。

今や、国家インテリジェンスが求められる領域は、「諜報」や「スパイ」というような言葉でイメージされる伝統的な枠を大きく超えている。金融制裁・宇宙開発・海洋資源・エネルギー確保・サイバーセキュリティー・科学技術・産業育成・海外邦人保護など広範囲に拡散しており、必要な情報の質も高度化・専門化している。これら新領域からのインテリジェンスの要請に応えるには、必ずしも伝統的な外交・安全保障面からのアプローチや、政府職員の伝統的なローテーション人事では追いつかない。加えて、日本国民および日本企業の活動領域がグローバルに広がっている現代においては、日本国民・企業はかつてないほど多様なリスクにさらされるようになっており、インテリジェンスそのものへの国民的ニーズはかつてないほど切実なものとなっている。民間レベルで可能な危機管理策には限界があり、コ

ストもかかる一方、リスクが顕在化した場合には当該企業にとどまらず、(海外での邦人人質事件のように) 政府としても切迫した対応を迫られることになろう。こうしたことから、リスクの顕在化を未然に防ぐためのインテリジェンス網の構築が、官民双方の潜在的なニーズとして浮かび上がる。そこで私たちは、インテリジェンス分野における「官民ネットワークのアップデート」をキー・ワードとして、以下にいくつかの具体策を提言することにした。

本提言の構成は以下の通り。まず、民間部門の視点から特に重要性を痛感している、①在外邦人保護（第 2 章)、②科学技術安全保障（第 3 章)、③サイバーセキュリティー（第 4 章) に焦点をあてて、これら分野のインテリジェンスがどのように機能し強化されるべきか、その論点を提示することにした。そのうえで、以上３つの領域に共通する総論としての提言を本章に記し、最終章で国家機構としてのインテリジェンス組織の問題についても触れつつ、将来の課題を提示した。なお繰り返しになるが、今回の提言はあくまで民間部門からの視点から出された「アップデート」であり、軍事機密の収集・分析など、いわゆる伝統的領域は主要な論点ではないことを最初に断っておく。[1]

提言1. オールソース・アナリシスを拡充・高度化すべき

私たちが提言の中でとりわけ強調したいのは、オールソース・アナリシス（政府が保有するあらゆる情報手段を活用した総合的な分析）を徹底することの重要性であり、そのために幅広い視野から対外情報の収集・分析に取り組むことである。インテリジェンスにおける省庁間の縦割排除のための努力は続いているが、この取組みをさらに一歩進め、行政機関の枠を超え、独立行政法人や民間企業、NGO（非政府組織）の協力を得ることも検討に値する。例えば、青年海外協力隊などの海外ボランティアを派遣する国際協力機構（JICA）は援助相手国の治安情勢など草の根情報を豊富に保有する。また、日本貿易振興機構（JETRO）や国際協力銀行（JBIC）や商社も海外事務所を通じて情報収集しており、カントリー・リスクやビジネス・リスクに関する多くの情報を有する。加えて、後述する科学技術情報やサイバーセキュリティー情報の収集についても、様々な機関・企業が関係している。こうした幅広い分野に高度に分散している情報の中から、価値あるインテリジェンスを導くことはたやすい作業ではないが、伝統的な外交・安全保障を超えた、いわば「新領域の情報」を集めようとすれば、行政機関の外側に広がる民間・非政府部門からの情報収集が重要になっていくのは間違いない。オールソース・アナリシスのインフラとして、こうした情報収集ネットワークの拡充を進めるべきであることをまず提言する。

---

[1] 本提言では取り扱わない分野の整理：相応に議論が尽くされている分野は、例えば２．（４）の人材育成については、①インテリジェンス関連の研修の強化、②インテリジェンスに特化したキャリアパスの設置と地位向上、③ローテーションの長期化（３年超)、④他の情報組織への出向を昇進の条件とする、⑤セキュリティー・クリアランスの実施、などが主要な論点となっており、既に議論は「どう実現するか」という具体策の提示に移っている。また、２．（５）にあるインテリジェンスの監視体制については、情報組織の暴走をいかに食い止めるかという観点で様々な議論がなされており、(外安 2011）がインテリジェンス機能の強化に関して「法的問題点と政府のインテリジェンス活動の監視」として注意喚起し、裁判官の経験者を情報組織トップに据える、という人事面での工夫が議論されている。やはり国家のインテリジェンス機能が安心して任せられる健全な組織であるためには、安全装置としての監視機能の強化について、引き続き議論されるべき点であろう。

また、情報の集約・共有において、国際協力の強化も重要である。わが国の関係行政機関は通常、個別のニーズに応じて外国政府機関と個々に情報交換・情報収集活動を行っていると考えられるが、各機関における情報のギブアンドテイクの活動をモニタリングすることで、わが国としての「情報の収支バランス」をうまく取りながら対外協力を強化することが可能となる。こうした情報の集約・共有は、情報を巡る国際協力や緊急時の情報交換体制を構築していく上で、今後より一層議論を深める分野であろう。

第２章　在外邦人保護のためのインテリジェンス強化に関する提言

問題意識

2013 年 1 月、アルジェリアにおいてガスプラント施設がイスラム過激派武装集団に襲撃され、日本人 10 名を含む多数が犠牲となる痛ましい事件が発生した。この事件を受け、在外邦人および日本企業の安全確保の強化のために政府は様々な措置を講じているところである。しかし近年は、さらに邦人の安全をとりまく国際環境の変化や以下のようなリスク要因が顕在化する事例が相次いでいる。

① 日本人がテロの標的となりうる：シリアにおける邦人殺害テロ事件（2015 年）は、２名の日本人が犠牲となり、さらに過激派組織のＩＳＩＬは、今後どこにおいても日本人の殺害を続ける旨を表明している。また、これまでにもアルカイダ幹部らが日本をテロの対象に名指ししている。したがって、今後は日本人が「テロに巻き込まれる」のではなく、「テロの標的」になり得るということを認識する必要がある。

②短期旅行者のテロ被害が発生している：チュニジアにおけるバルドー国立博物館銃撃テロ事件（2015 年 3 月）のように、海外の「在留邦人」のみならず、「短期旅行者」もテロの被害者となった事件が発生している。

③先進国でのテロの危険性が高まっている：中東・北アフリカのみならず、先進国でもテロの被害を受ける可能性がある（2014 年 10 月：カナダのオタワにおける銃撃事件、2014 年 12 月：オーストラリアのシドニーにおける人質立てこもり事件、2015 年 1 月：フランスのパリにおける連続テロ事件等）。欧米諸国など先進国に居住したまま ISIL 等のテロ組織に感化され、居住国でテロを実行する「ホームグロウン・テロリスト」は世界的な拡がりを見せている。

④テロ以外のリスクへの対処が必要：企業活動のグローバル化に伴い、邦人が海外においてテロ以外にも感染症や自然災害など多種多様なリスクに晒されるようになっている。

このような最近の環境変化を踏まえ、外務省の「在外邦人の安全対策強化に係る検討チーム」は 2015 年 5 月に「在外邦人の安全対策強化に係る検討チームの提言」を公表した。その中で、①公開情報の収集・蓄積・活用の強化、②情報収集体制の確立、③「情報専門官」

の育成と外部専門的知見の活用等、④先端技術等の活用による情報収集・分析の強化、⑤遠隔地等の安全情報に係る情報収集・調査の拡充等が具体的施策例として提案されている。別途、政府の国際組織犯罪等・国際テロ対策推進本部（本部長：菅義偉官房長官）による本年5月の決定に基づき、外務省内に「国際テロ情報収集ユニット」を新設し、イスラム過激派組織の動向等の国際テロ情勢に関する情報収集を含む国際テロ対策を強化することとするなど、この分野の動きは活性化しつつある。本提言は上記提言と一部重複するものの、以下の点を重要な施策として提言したい。

提言2. 海外安全情報の収集における現地ネットワークを強化すべき

海外安全情報については、国際協力機構（JICA）や非政府組織（NGO）、商社、金融機関など日本の民間国際人脈がもつ情報収集能力は非常に価値の高いものであり、平素からの情報収集の一環として政府がより有効に連携する余地がある。現在、各在外公館においては「安全対策連絡協議会」（在外公館と在留邦人の双方向の意見交換・情報交換の場）が定期・不定期に開催されているが、当協議会をより重視するべきである。同時に、都市部だけでなく、よりリスクの高い周辺地域に関する安全情報の提供や研修の充実を図ったり、民間の情報セキュリティーに関する専門家を活用した現地安全対策情報を提供したりすることにより、安全情報に係る情報交換機能を一層向上させる余地があると考える。

一方、邦人を対象とした事案が発生した際の情報収集については、民間コミュニティーからの情報に頼ることは、その情報源の安全確保の観点からも現実的ではない。むしろ、より直接的な情報を収集するとの観点から、例えば米国国民が対象となった場合に米中央情報局（CIA）がどのような活動を行っているのかについて研究のうえ、日本もそのような能力を身につけるべきか否か、議論を行っていく必要があるのではないか。

提言3. 現地事情・人脈に精通した人材を養成すべき

情報収集活動にあたり、現地事情や現地語に精通した人材の育成が課題となる点については、これまでも過去の提言において繰り返し指摘されてきた。特にアラビア語やトルコ語、ペルシア語といった言語の運用能力があり中東の地域情勢・人脈に精通したアラブ専門家の不足は深刻な課題となっている。これらの専門家の育成に、長期的な育成戦略と計画が必要である。一方、喫緊・緊急の課題に対応するためには短期的視点でのナレッジの強化策も必要である。こうした要請に応えるために、海外の中東専門家、大学教授等の招聘と国内有識者やシンクタンク等の専門家集団とのネットワークの構築を強化する戦略と計画の策定が望まれる。

提言4. 短期旅行者への海外安全情報の提供と啓蒙を進めるべき

現状、3ヶ月未満の短期滞在者については在留届の提出義務がなく、渡航の実態把握と危険に関する情報が入った場合の情報提供が困難な状況である。もちろん、危険地域への渡航制限については日本国憲法が保障する移動の自由の観点から慎重に議論を進める必要があるが、危険地域への渡航（旅行）を予定している邦人の連絡先を把握したうえで、現地の危

険に関する情報が入った場合に、迅速に連絡と情報提供を可能とする仕組みについては強化することが急務であると考える。また、渡航者自身も危険に関する情報への感度を高めることが求められる。こうした観点から、外務省の３ヶ月未満の短期渡航者の登録システム「たびレジ」の更なる普及に努めていく必要がある。

第３章　科学技術安全保障のためのインテリジェンス強化に係る提言

問題意識

大量破壊兵器、国際テロ、様々な不法行為などの想定される脅威に対し、わが国は外交力、防衛力、警察権、各種法令に基づく権能等を駆使しながら適切に対応しており、それぞれにインテリジェンスが活用されている。今後も、想定される様々な脅威を未然に防止するために、インテリジェンスの取り組みを継続することは必要であるが、より幅広くヒト・モノ・カネのフロー（流れ）を捉えたインテリジェンスの再構築も期待される。この観点に立ったとき、わが国の有する優れた科学技術も、ひとたび流出すれば脅威となりうるとの認識がきわめて重要である。わが国が有する先端技術は、生活をより安全で快適なものにする上で欠かせないだけでなく、わが国の安全保障及び経済的繁栄にも資する財産であるとの認識を持ち、「科学技術安全保障」とも言うべき視点で防護の対象とすべきである。

この観点から振り返ったとき、実はわが国の科学技術安全保障を脅かす事例は多い。具体的には、2007 年から 2014 年の間に報じられた、技術者による自動車部品や工作機械の設計図面の持ち出し、元社員や関係者による鋼材、プレス機器、半導体技術の外国企業への開示・提供などが挙げられる。また、わが国あるいは高度な科学技術を有する先進諸国の高度な技術や製品の中には、使用方法によっては兵器や大量破壊兵器開発・製造に転用可能なデュアルユースの製品や技術（ミサイル技術、撮影機材、重機、着艦拘束装置、エンジン、航空アビオニクス等）も多くみられる。こうした技術・製品群が、様々な国（その中には民間技術の積極的な軍事転用を政策として掲げる国すらある）に流出している旨の報道が散見されるが、事実とすればわが国の脅威となっている可能性があるものとして深刻に受け止めるべきであろう。この課題に国家インテリジェンスとしてどう対処すべきなのかについて、以下提言する。

提言5.　「科学技術安全保障」への認識を高め、必要な措置を講じるべき

上述の通り、わが国の企業などで技術系社員による営業秘密の不正入手やインサイダー情報の漏洩が発生し、わが国の安全保障や国際的競争力に脅威を与える国や他国企業に情報や製品群が渡る事例などが報道されている。こうした事例は氷山の一角に過ぎないとの見方もある中、科学技術の流出は安全保障面でも経済面でも多大なる損失であるとの「科学技術安全保障」の概念を官民双方で定着させる必要がある。同時に、関連する企業や研究機関、大学などでもインテリジェンスの観点から自ら保有する情報の管理を強化すべきである。

提言6. 先端技術等に関わるヒト・モノ・カネのフローの情報収集を推進すべき

わが国の脅威となり得る軍事力、テロ、各種不法行為等のいわゆる「想定脅威」が実際に具体的な形となって現れるまでに、様々なヒトが介在する。先端技術情報や軍事転用可能な製品や素材等も例外ではなく、ヒトを介して技術や情報を含むモノが世界中から集められ、これらの活動に必要な巨額のカネが動いている。先端技術を巡るこうしたヒト・モノ・カネのフロー（流れ）は分野、組織、国境を越えて複雑につながっているため、点ではなく線や面で捉えようとしなければ全体像は判らない。科学技術を巡る様々なフローがどのような「想定脅威」に寄与しようとしているのか、全容を把握するには、分野横断的なアプローチが必要であり、提言１で取り上げたオールソース・アナリシスの観点からの情報の収集・集約・分析・蓄積・共有・活用を推進する必要がある。具体的なインテリジェンス情報としては、高度な科学技術に関する不正な調達事例に関する報道・関連の報告書を手がかりに、国連制裁委員会が輸出に際し注意喚起している製品や技術（モノ）、ルール違反者や違反が疑われる人物（ヒト）、事例を巡る資金の動き（カネ）の流れに関する現場レベルの情報の整理と分析が必要になる。

提言7. 科学技術分野における情報収集ネットワークを構築すべき

情報収集の対象となる分野は、軍事への転用・活用が可能な先端技術関連分野や、資金源となる武器や違法薬物の分野、資源関連分野等が中心になると思われる。その際、関連する分野の知見や情報との接点のある国内の関係団体・機関、企業、大学・研究機関と政府との間で、信頼関係の醸成と情報共有に関するネットワークの構築が必要となる。提言６とあわせ、これらの一連の公開情報の収集・集約・分析によって、わが国で狙われる可能性の高い製品や技術、諸外国が狙っている製品や技術がより明確になるものと思われる。

提言8. 官民学間の信頼・協力関係を構築すべき

大学や研究機関が諸外国からの留学生、研究生を積極的に受け入れ、国際的な研究連携や産学連携を進めることは望ましいことではあるが、同時に、受け入れる留学生や研究生および連携先の大学や研究機関の情報管理体制の不徹底が、わが国にとって経済的・軍事的な脅威につながる可能性がないかについて、カウンター・インテリジェンスの観点から審査を十分に行う必要がある。同時に、わが国の企業や大学・研究機関などに「科学技術安全保障」についての認識をもってもらい、政府との間で情報共有ができるように両者の意識を高めることが望ましい。こうした活動を通じて、大学・研究機関や民間部門における何らかの違和感や懸念がある場合の所管官庁への照会やインサイダー脅威に関する政府への報告なども活発化していくことが期待される。

第４章　サイバーセキュリティーのためのインテリジェンスの強化に係る提言

問題意識

サイバーセキュリティーを必要とする分野は、軍事・防衛分野に限らない。「モノのインターネット化：Internet of Things」という言葉に表されるように、私たちの身近な分野、例えば列車運行システム、電力・水供給システム、自動車制御システムなど多岐にわたっており、国民生活の安全・安心はサイバー空間の安全が確保してこそ成立する。こうした状況下、サイバーセキュリティーとインテリジェンスの関係については、2015 年 1 月に施行された「サイバーセキュリティー基本法」において、「サイバーセキュリティー戦略の策定にあたっては国家安全保障会議の意見を聴き、重要事項の策定にあたっては国家安全保障会議との緊密な連携を図る」旨が規定された。国家安全保障をサイバーの側面でサポートする観点からこれは大きな前進といえ、「脅威を想定しそれに備える」ための準備を進める素地が整ったと考えてよい。そこで私たちは今回、上記の様々な分野を念頭に、サイバーセキュリティーにおける情報収集活動で強化すべき点は何か、という目線で議論を行った。

提言9. サイバーセキュリティーのインテリジェンス・サイクルを底上げすべき

サイバーセキュリティーで収集・分析すべき情報は、攻撃者の攻撃能力、プログラミングのクセ、行動様式、掲示板や SNS などを通じたハッカーコミュニティーの動向、攻撃発生に至る前段階での偵察など、多岐にわたる。こうした情報収集活動を強化していく上で、以下を提言する。

第一に、サイバーセキュリティーと国家安全保障についてスタッフレベルの知見向上が課題である。例えば国家安全保障局のスタッフの多くは法律分野の知識がバックグランドとなっているとされ、必ずしもサイバーインテリジェンスを理解するための技術的知識を有しているわけではない。他方、内閣サイバーセキュリティセンター（NISC）のスタッフにおいても、国家安全保障のためのセンスを備えているわけでは必ずしもない。両者の情報ニーズの溝を埋めるべく、スタッフレベルの識見の共有が必要である。

第二に、情報収集の手段としての「合法的傍受（裁判所または行政の命令による権限に基づいて、ターゲットに対して電子的監視を実行するプロセス）」[2]の議論を深めるべきである。通信の秘密が守られるべきことは大前提としても、例えば海外から明白な悪意のあるプログラムが送信されている時に、そのルート上にあるサーバなどに対する傍受について、どういった形で実施するのが最適なのか、議論を深めるべきである。

第三に、「限定的なサイバー事態対処」についての研究が不足している点が課題である。例えば、サイバー空間で国家安全保障に対する明確な脅威を探知した場合、その通信を遮断したり、脅威を排除したりするための積極的な活動について研究を進めるべきであろう。他

[2] 例えば、民間のコンピュータネットワーク機器開発会社が「合法的傍受」について詳述している。
http://www.cisco.com/cisco/web/support/JP/docs/RT/ServProviderEdgeRT/10000RT/CG/005/3426_05_about.html?bid=0900e4b182529511

国の例では、英国の GCHQ（政府通信本部）のハッカー対策などが参考になると思われる[3]。

提言10. 情報共有のリアルタイム化のため民間部門からの協力を獲得すべき

重要なインフラ設備や通信ネットワークに対する、いわゆるゼロデイ攻撃や複数目標への一斉攻撃に即応するためには、日頃から関心事項を共有する関係者間の意思疎通を活性化しておき、攻撃を受けた際に、情報を必要としている組織に即時に過不足なく届けるシステマチックな対応が必要となる。このために、以下を提言する。

第一に、民間企業による情報共有のインセンティブを高める必要がある。攻撃情報を収集するにしても、そもそも民間企業がサイバー攻撃を政府に報告する義務はないし、無分別に公表して混乱を招くといった事態も避けたいだろう。このため、情報提供に対する民間企業のインセンティブをどう向上させるか、そのための工夫を検討すべきである。

第二に、リアルタイムでの情報共有の精度向上が課題である。不必要な情報を排除し、情報ニーズに適切に応える情報提供を実現していくためには、現状より細かいレベルでの攻撃情報の仕分けが必要である。この点につき、英国の情報共有システム（攻撃の特徴やタイプを分別し、関心の高い組織に情報発信する学習型システム）が参考になると思われる。

第三に、サイバー攻撃に詳しいスタッフを即応体制に組み込む必要がある。サイバー攻撃に関し的確に情勢を把握し、技術情報を即時に理解し、一方で各省庁の対処方針やカルチャーをも理解したスタッフによる補佐を通じ、攻撃を受けた際に NISC（特に GSOC：政府機関情報セキュリティー横断監視・即応調整チーム）と NSC による連携や、官邸の対応方針とをリアルタイムで連結させることが期待される。

提言11. サイバー攻撃に対するアトリビューション能力を向上すべき

サイバー攻撃を受けた場合の動かぬ証拠を集めるため、アトリビューション（攻撃者の属性情報の収集）の能力を強化すべきである。サイバー攻撃には必ず攻撃者のクセが出るため、その属性情報や攻撃の証跡を保全し、攻撃者の特定作業に活用することができる。これらの能力を向上させる上で、以下を提言する。

第一に、証拠保全の議論を高めるべきである。例えばサイバー攻撃の痕跡（証跡）は、攻撃を受けた情報端末やサーバ上にログの形で残る場合がある。これらを、十分な証拠能力を保持したまま保全することが必要である。電気通信事業法の定める「通信の秘密」などとの整合性を図りつつも、特に政府や国家安全保障に重要な影響を与えるインフラ産業などにおいて、精確なログの保全が重要である。

第二に、サイバーインテリジェンスと伝統的インテリジェンスの連携を深める必要がある。サイバー空間の捜査は、いずれ攻撃の主体となった人物や組織にたどり着く。この際、サイバー空間から実社会への受け渡しが必要となるが、この際のスムーズな連携が重要である。また平時においても、サイバー攻撃に関して、各国のインテリジェンス機関と情報を共有し、

[3] 例えば、ハッカー集団「アノニマス（Anonymous）」などに対して、GCHQ が分散型のサービス妨害（DDoS 攻撃）を仕掛けていたとする 2014 年の報道がある。

提供していくことで政府一体となった知識の向上を図っていくことが重要である。

提言12. IT プロフェッショナルの語学能力向上と組織運営への参画を推進すべき

サイバーインテリジェンスの所作を身に着けた IT のプロフェッショナルの獲得や育成と、責任あるポジションへの登用が不可欠である。この点について、以下を提言する。

第一に、サイバーインテリジェンスに携わる IT プロフェッショナルの語学能力の育成を急ぐべきである。サイバー攻撃に関する情報収集のためには、国外の様々な関係者との公式･非公式な情報交換､ハッカーのコミュニティーに入りこむ形での情報収集が必要となる。攻撃のプログラムは英語に限らず､様々な外国の言語を用いている可能性が高い。こうした業務においては、IT プロフェッショナルといえども語学能力の涵養が極めて重要である。

第二に、IT プロフェッショナルについてもセキュリティー・クリアランスを実施すべきである。上記で登用する IT プロフェッショナルについては、国家安全保障に関する情報に接する機会も多い。このため、サイバーセキュリティー関連の技術者についても特定秘密保護法の「適性評価制度」を実施すべきである。

第三に、組織運営に対する IT プロフェッショナルの関与を深めるべきである。サイバーインテリジェンスやサイバーセキュリティーを強化していく上で､予算獲得や人材の選定といった組織運営の面でも、IT プロフェッショナルのアドバイスに基づく無駄の排除が有用であると思われる。

第５章　終わりに――インテリジェンス組織にかかわる今後の課題

総論でも触れたとおり､わが国のインテリジェンス機能の強化については、これまで様々な議論や提言がなされてきた。その中で、特に情報収集の側面については「日本は不十分ながらもそれなりに活動している」（小谷 2006）との評価であり、日本の国家的な弱点はむしろ、こうして集められた膨大な情報の「集約・共有の問題」にあるという指摘に私たちは共感した。これまで指摘してきたように、わが国の安全や繁栄を保障するために必要な情報がますます多様化・専門化・分散化する中で、情報の受け皿たる「集約・共有」機能が未整備なままでは、政策部門が「何を知るべきかを知らない状態」に陥っていく恐れがある。こうした問題意識から、（組織論はさておき）国家インテリジェンスでカバーすべき分野は拡大しているのだ、という警告が必要だと考えた。今回の提言は、そうした中で特に重要だと考えられる分野を例示したものである。

無論、私たちも、情報の「集約・共有」機能を強化するための組織のあり方に関し、政府組織の見直し、とりわけ「必要な情報をどの組織が取りまとめ NSC に報告するのか」という行政機構の改革は避けて通れない課題だと認識し、あるべき改革の内容について議論・検討を重ねてきた。例えば、情報系の政府組織をより中央集権的にしてはどうか、各省や内閣にインテリジェンスのアドバイザー職を設けてはどうか､人事ローテーションの長期化を図

ってはどうか等の意見が出た。しかし、人員配置の見直しを含め、行政機構の再編は実現に多大な困難を伴う政治課題であり、再編の青写真となる的確な制度設計はもちろん、時の政権の強い意思とそれを支える国民の理解が欠かせない。本提言は「民間部門・非政府部門の視点」に立脚したインテリジェンス強化に主眼を置いた提言であることに鑑み、行政組織の見直しに関する具体的な立論にはあえて踏み込まない。ただし、この「集約・共有」機能強化の問題が政府に残されたいわば「永遠の政策課題」であることは、過去の提言同様に強調しておきたい点である。

2020 年の東京五輪開催は日本のインテリジェンス能力にとって試金石となる。第 2 章で言及した政府の国際組織犯罪等・国際テロ対策推進本部は本年 5 月の決定で、喫緊の課題の一つとして、テロ関連情報が関係省庁で「速やかに共有されること」を挙げており、本提言も政府一体としての取り組みを強く望むものである。同時に、テロ行為を防ぐためには国内での情報共有だけでなく、他国の情報機関とも緊密な連携が必要となる。他国から重要な情報を得るためには日本も相応の情報を提供することが求められ、そのためにも、国際的に見てもレベルの高い、アップ・トゥ・デートでバラエティに富んだインテリジェンス機能の獲得が不可欠となる。2020 年まで残された時間はけっして多くない。政府が本提言の内容を検討し、望むらくはその実行に向けて検討を進めることを求めたい。

以　上

巻末付録

日経・CSIS バーチャル・シンクタンク
インテリジェンス問題検討チーム

春日　剛
加藤　もえ
岡部　貴士
児玉　啓佑
寺岡　弘達
本堂　聡
他、3 名

＜会合記録＞

第 1 回	平成 25 年 12 月 10 日	キックオフ・ミーティング
第 2 回	平成 26 年 2 月 24 日	アカデミック・フェローによる講義
第 3 回	平成 26 年 4 月 8 日	専門家（インテリジェンス分野）との勉強会
第 4 回	平成 26 年 5 月 30 日	各メンバーの問題意識の整理
第 5 回	平成 26 年 7 月 24 日	主な論点の整理と意見交換
第 6 回	平成 26 年 9 月 26 日	各論点に関するアカデミック・フェローとの協議
第 7 回	平成 26 年 10 月 24 日	中間報告と米側専門家からのコメント聴取
第 8 回	平成 27 年 1 月 26 日	専門家（インテリジェンス分野）との勉強会
第 9 回	平成 27 年 2 月 12 日	執筆態勢に関する協議
第 10 回	平成 27 年 3 月 16 日	専門家（サイバー分野）との勉強会
第 11 回	平成 27 年 4 月 22 日	執筆原稿のドラフトに関する協議
第 12 回	平成 27 年 5 月 18 日	専門家（在外邦人保護の分野）との勉強会
第 13 回	平成 27 年 6 月 11 日	執筆原稿のドラフトに関する協議
第 14 回	平成 27 年 8 月 6 日	最終稿に関するアカデミック・フェローとの協議