日本政府の情報機能（第７回）
～その課題と機能強化への処方箋を考える～

市ヶ谷台論壇　会員
斉藤　敏夫

今回（第７回）は、第２章　日本政府がいう「情報機能の強化」とその課題についての最後として、⑥カウンターインテリジェンス、及び⑦先行報告書等で取り扱われていない課題・論点について論考する。

第２章　日本政府がいう「情報機能の強化」とその課題

第６節　カウンターインテリジェンス

安保戦略は、カウンターインテリジェンス機能の強化について、「こうした情報機能を支えるため、特定秘密の保護に関する法律（平成２５年法律第１０８号）の下、政府横断的な情報保全体制の整備等を通じ、カウンターインテリジェンス機能を強化する。」としている。

第１章第５節（第３回）で解説した通り、カウンターインテリジェンス（ＣＩ）活動とは、自国及び自国の国益にとって脅威となる外国等の情報活動を特定し対処することであり、ＣＩの主たる関心事項は、外国勢力、外国機関若しくは外国人又はそれらの代理人（スパイ）、又は国際テログループのような非国家主体による情報活動である。そして、ＣＩ活動の第一は、自国の保全すべき情報及び重要資産を外部から不法に取得されないよう保全する、防御的ＣＩ活動である。ＣＩ活動のもう一つの側面は、攻撃的ＣＩ活動である。それは、外国等の情報機関がどのような活動をしようとしているのかその計画を見極め、彼らの狙いをより効果的にくじくことである。

（１）　カウンターインテリジェンス機能に係る政府の認識と課題

安保戦略が発表された２０１３年 12 月 17 日時点では、その４日前に公布されたばかりの特定秘密保護法は、その施行までまだ約１年を経る必要があったが、同法に基づき政府横断的な情報保全体制が整備可能となったことから、「カウンターインテリジェンス機能を強化する」ための素地はできたと言えよう。しかしながら、安保戦略が策定された当時、政府は、カウンターインテリジェンス機能として、どの範囲まで想定し、どのような方法で当該機能の強化を図ろうと考えていたのであろうか。

政府はカウンターインテリジェンスの定義は明示していないが、その目的を「国の重要な情報や職員等の保護を図ること[1]」としており、このことから推察するに、ＣＩ活動のうち「攻撃的ＣＩ活動」については、目的としては明示的には位置づけられていない。もっとも、特定秘密保護法の施行により、例えば、不正取得罪（同法第 24 条）[2]の新設、すべての者の国外犯処罰の適用（同法第 27 条）等、罰則の適用範囲が拡大されており[3]、これら罰則規定と犯罪の未然防止活動により、自国の保全すべき情報及び重要資産を外部から不法に取得されない

よう抑止する効果を期待できることとなった。また、犯罪がある場合には、国内外を問わず全ての被疑者に対し刑事訴訟法に基づく手続きが取られることとなろう。このことは、攻撃的ＣＩ活動、すなわち、外国等の情報機関がどのような活動をしようとしているのかを見極め彼らの狙いをより効果的にくじくこと、と同義ではないが、司法警察権の行使により相手方の情報収集活動を結果として妨害する効果をもたらす場合もあろう。

このように、特定秘密保護法の施行により、一定レベルのカウンターインテリジェンス機能の強化を図り得る状況とはなったが、次に述べる課題には、十分には対応できないことに留意する必要があろう。

一つは、特定秘密以外の保全すべき情報（機密性３情報（秘密）や機密性２情報（注意）など）を漏えい等した場合の取り扱いについては、日米相互防衛援助協定等に伴う秘密保護法（昭和 29 年法律第１６６号）に規定される「特別防衛秘密」を除き、現行の国家公務員法（昭和 22 年法律第１２０号）第１００条第１項、自衛隊法（昭和 29 年法律第１６５号）第 59 条第１項等の規定に基づき、処罰されるのみであり、例えば、過失漏えいは罪に問えないし、また、特定秘密保護法に規定された不正取得罪は規定されていないことである。したがって、特定秘密や特別防衛秘密以外の保全すべき情報の漏えい又は不正取得に対しては、既存法に即して措置するということであり、また、当該情報の共有を図るための政府横断的な保全手続きは、別途措置する必要があるということである。

二つ目の留意事項は、無線通信傍受により特定秘密を取得する者には不正取得罪の適用は困難であるということである。例えば、内閣衛星情報センターが運営する情報収集衛星又はデータ中継衛星から地上局へ暗号化されている画像データを送信する際に、当該画像データを当事者以外の者が傍受し、かつ、暗号解読の上、処理・解析していた場合には、通例衛星画像データは特定秘密に相当する以上、当事者以外の者が特定秘密を取得することとなるが、不正取得罪の適用は困難であろう。そもそも、傍受され解読等されていたとしても、相手の情報収集能力や収集活動の実態を我が方が知らなければ、傍受・解読等されていることも分からないかもしれない。本邦と在外公館等との通信手段として衛星通信を利用している場合にも、そのような通信データは傍受・解読されている恐れは常にあるが、当該通信データに特定秘密があったとしても、無線通信を情報伝達の手段として使用する以上は、現在のところ、暗号強度を高め解読されないよう常に改善に努める以外方法はないものと考える[4]。

以上述べたように、特定秘密保護法の施行により、カウンターインテリジェンス機能は、一定レベル強化されるが、それは、防御的ＣＩ活動としては、特定秘密に関し、相手方の不正な人的情報収集活動や有線通信の傍受、サイバースペースにおける不正アクセス等を抑止する点であり、積極的ＣＩ活動としては、不正取得罪の新設により、犯罪防止活動の実施や犯罪の被疑者を司法警察手続きに載せることにより、相手方の情報収集活動を妨害し得る点で強化される、というところまでである。

ＣＩ活動では、まず、脅威となる対象国等（情報機関、団体、人）の情報活動を特定する必要がある。対象国等も、人的情報、信号情報、地理空間情報及びマシントに関する情報収集活動を日本に対して行っているとともに、日本政府による情報収集活動に対処する保全措置を取っていると考えるべきであろう。したがって、対象国等の情報活動を特定するというこ

とは、彼らが行っている人的情報の収集活動を特定するだけではなく、対象国等の領域に所在する固定の信号情報（サイバー領域における情報を含む）や地理空間情報の収集拠点・施設、更には移動体である有人・無人の情報収集機、情報収集艦（潜水艦を含む)、各種情報収集衛星等による情報活動も特定する必要がある。

このようなことから、日本政府の情報コミュニティにおける、対象国等による人的情報活動に対処するＣＩ機関（部署）は、警察庁警備局や公安調査庁、防衛省・自衛隊の情報保全を担任する自衛隊情報保全隊などに限らず、どの情報機関（部署）にも情報漏えい及び不正取得を防止するためのＣＩ担当部署が必要である。更に、信号情報や画像情報の収集能力がある機関（防衛省情報本部画像・地理部、電波部及び通信所、自衛隊関係部隊、内閣衛星情報センター等）は、そのシングルソース情報の収集能力を活かして、対象国等の信号情報、画像情報、マシント等の収集能力及び収集活動に関する情報を収集し、ＣＩプロダクトを作成する必要があろう。

（2）　カウンターインテリジェンス・コミュニティの構築

現在、「カウンターインテリジェンスについて、関係行政機関相互の緊密な連携を確保し、その強化に向けた施策の総合的かつ効果的な推進を図るため、内閣にカウンターインテリジェンス推進会議（以下「推進会議」という。）が設置」されており[5]、「内閣情報官をセンター長とするカウンターインテリジェンス・センターが内閣情報調査室に置かれ、カウンターインテリジェンス機能の強化に関する基本方針（平成19年８月９日カウンターインテリジェンス推進会議決定）の施行に関する連絡調整等を行っている」とされている[6]。この基本方針は、その目的を「国の重要な情報や職員等の保護を図ること」とし、そのための施策としては情報管理の徹底を掲げ、「特定秘密その他秘密保全を必要とする情報の管理について、適切に管理する。また、行政機関に対する情報の窃取・破壊等を目的としたサイバー攻撃が脅威となっていることから、情報セキュリティの強化・充実を図る」としている[7]。これらのことから分かることは、政府がいうカウンターインテリジェンス（ＣＩ）は、本論考で先に解説してきた範疇より制限的である、ということである。また、推進会議の構成員が全省庁となっていることからも分かるように、この推進会議は、安全保障に関する政府の情報機能強化策の一環としてＣＩコミュニティを構成するために設置されたものとは必ずしも言えない、との見方もあろう。

ＣＩの機能を全うするためには、防御的ＣＩ活動として、各ＣＩ機関（部署）が収集し分析・作成したプロダクトを共有することが、まずは必要であろう。その場合ＣＩコミュニティを構成する必要があるが、そのコミュニティのコアメンバーとしては、各情報機関（のカウンターインテリジェンス部署）やＣＩ専門組織である自衛隊情報保全隊が上げられる。このコミュニティにおいては、国の重要な情報や職員等の保護を図るため、ＣＩプロダクトが随時共有されることが必要である。また、同盟国・友好国には、ＣＩコミュニティが存在しているが[8]、自国及び自国の国益にとって脅威となる外国等の情報活動を特定するためにも、利害関係が重なる分野における、同盟国・友好国のＣＩ機関との協力関係の構築及び情報交換は重要であると考える。

第７節　先行報告書等で取り扱われていない課題・論点

さて、安保戦略に記載された「情報機能の強化」について、その内容を評価し、課題・論点を述べて来たが、この安保戦略を含め、過去の政府（内閣官房等）が取りまとめてきた情報機能の強化に関する報告書や提言では取り扱われていないが、重要だと考える課題・論点について触れることとする。

（１）　情報機関と法執行機関との分離と連接

情報機関（カウンターインテリジェンス（ＣＩ）機関を含む）と犯罪捜査等の司法警察権を行使する法執行機関とは、それぞれの組織の設置目的が違うことや、そもそも情報と政策・運用（この場合は司法警察活動）を分けるべきとの観点から、別の組織とするか、同一組織に置くとしても、情報部署と司法警察活動を行う部署を分けて編制すべきである、との論点がある。情報機関の任務は外国等の情報（ＣＩを含む）をカスタマーに提供するとともに、重要な情報と資産（職員、施設、システム等）の保全を保つためのＣＩ活動を行うことである。一方、司法警察権を行使する法執行機関の任務は、ＣＩ活動自体ではなくて、犯罪の取り締まりである。情報活動に関する犯罪としては、秘密漏えい罪、特定秘密の不正取得罪などの他、刑法や関係特別法に規定される犯罪である。

例えば、情報機関所属の職員が外国の人的情報収集機関のスタッフ又はその代理と接触し秘密情報を漏えいする、又は外国等が特定秘密を不正取得する疑いがある場合、ＣＩ活動としては、当該疑いの情報をＣＩコミュニティで共有するか、少なくとも、その職員が属する情報機関のＣＩ部署へ通報し、当該職員に対し事情聴取を実施の上、情報漏えいの未然防止（本人の異動を含む）と当該職員の安全確保を図るか、既に犯罪行為の疑いがある場合には、司法警察機関又は検察当局に犯罪事実を申告（告発）することとなろう。更に我が方が攻撃的ＣＩ活動を行うとすれば、当該職員の協力を得て相手方に保全上問題のない情報又は偽情報を流し、相手方の情報収集ルート等を探り我が方にとって有用な情報（ＣＩ）の収集を図るとの方策もあろう。一方、犯罪取り締まりを任務とする組織が上記秘密漏えいの疑い情報を入手した場合、その情報を関係情報機関へ通報するかは不明である。なんとなれば、犯罪取り締まり機関は、秘密情報や職員等の保全が主たる目的ではなく、情報漏えいや不正取得を行った犯罪事件の捜査、被疑者の逮捕、その他の司法警察活動を行うことが主任務であるからである。被疑者である職員等を泳がせた上で、秘密情報の授受現場を押さえて現行犯逮捕しそれを取り締まり当局が公表すれば、社会的インパクトは大きくなるが、これを防御的ＣＩ活動の観点から考えると、保全情報の漏えい、被疑者の司法手続き及び行政処分、保全情報を取得（しようと）した相手国との関係の悪化等、望ましからざる状況を招くことになろう[9]。防御的ＣＩ活動は、国の秘密情報及び重要資産（職員、施設等）を保全することであるから、犯罪（情報漏えい）の未然防止のための措置をとることが第一である。そのためには、不自然な接触等の疑いの情報を入手した機関は、その機関に司法警察の機能があったとしても、ＣＩコミュニティの一員として関係情報機関へ当該情報を通知し、情報漏えいの未然防止と関係職員等の保全を図るようにすべきである。司法警察権を行使するため、他のＣ

Ｉ機関へ情報提供できないということであれば、司法警察活動を担う部署とＣＩを含む情報部署は分離して組織立てすることを検討する必要がある。もちろん、既に犯罪行為の疑いがある場合には、関係機関は司法警察機関又は検察当局へ通知（告発）し、容疑者がしかるべき司法手続きに付されるよう措置すべきことは当然である。

現在、政府の情報コミュニティに属する機関のうち、司法警察活動に関わる機関は、警察庁警備局（及び各都道府県公安担当部署）及び海上保安庁警備救難部（及び各管区本部の警備救難部署）である。警察庁警備局には、警備企画課、公安課及び警備課の他に外事情報部が置かれており、同部には外事課と国際テロリズム対策課が置かれている[10]。このうち警備課を除く各課は、それぞれの所掌に関する警備情報の収集・整理又は分析を行うと共に、所掌事務に係る犯罪取り締まりを併せて行うこととされている。また、海上保安庁警備救難部警備情報課も、警備情報の収集、分析等の他、テロリズム等に関する犯罪について、海上における捜査又は被疑者の逮捕を所掌しており[11]、情報活動と司法警察活動を同一の課で行っている。情報機関とされている警察庁警備局と海上保安庁警備救難部の双方とも、組織令又は組織規則の規定のとおり、それぞれの課内で情報業務と司法警察活動を分離せずに行っているとすれば、例えば職員等の秘密情報の漏えい疑惑に関する情報が捜査上の情報だとしてＣＩコミュニティ内で共有されないことが懸念される。

大統領令 EO12333 の 2.6 は、米国情報コミュニティ各部局（elements）の法執行機関や他の非軍事（civil）当局に対する支援について規定している。それによると、米国情報コミュニティの各部局は、次の事項を行うことを認められている。

・情報コミュニティのいずれかの部局の職員、情報（インフォメーション）、資産及び施設を保全する目的のため、適切な法執行当局に協力する。

・法令により除外されていなければ、外国勢力又は国際テロリストによる秘密情報活動や麻薬取引活動を調査し妨げるため、法執行活動に参加する。

・いずれかの省や局が使用するため、又は命が危険にさらされている時に現地の法執行当局を支援するため、特殊器材、技術的な知見、専門職員の援助を提供する。（なお、専門職員による援助を提供する場合には、個別に提供部局の承認を要する。）

上記記載内容からも分かるように、情報コミュニティ（ＣＩ機関を含む）と法執行機関は別の部署であることを前提に、前者が後者を支援する場合を規定している。また、その目的は、ＣＩ活動の目的、すなわち、情報及び重要な資産（職員、器材及び施設）の保全を図ることであり、外国勢力又は国際テロリストによる秘密情報活動を調査し妨げることである。

日本政府の司法警察活動を担う組織のうち、警察庁警備局と海上保安庁警備救難部は、情報コミュニティのメンバーとされているが、政府全体のＣＩ活動を強化する視点からは、情報部署と司法警察活動を担う部署を分けて組織立てする必要があるのではないかと考える[12]。

（２）　軍事（防衛）情報機関と非軍事（外交・テロ対策等）情報機関との関係

主要各国の情報コミュニティでは、その資源（ヒト・モノ・カネ）の分配先としては、国防・軍事組織に所属する情報機関に比重がおかれているのが通例である。歴史的に見ても、安全

保障の主たる手段である軍事力の運用に必要な情報を収集、分析等する機関が国防・軍事組織に所属することは必然であった。安全保障の手段は、もちろん軍事力だけではなく、外交力や経済力も当然重要な手段であり、更には、武力行使に至らない諸活動（警察力）も手段として認識されている。また、安全保障の脅威は、軍事的脅威のみならず、国際テロリズムやサイバースペースにおける攻撃や情報の不正取得にも及んでいることから、これら各般にわたる脅威情報の収集、処理・解析、分析・作成及び配布に至る活動は、国防組織に属する情報機関に限らず、外交、警察、経済等の政府内各組織に属する情報部署においても行われている。それぞれの組織は、個別に情報活動を行っているが、必要に応じ共同して情報活動を行っている。このように、軍事部門の情報機関と非軍事部門の情報機関は、共同体（コミュニティ）を構成することによって、シングルソース情報を共有し、国家安全保障会議（ＮＳＣ）を含む政府のカスタマーの要求により良く応える総合分析情報プロダクトを提供し得るよう努めている。

日本政府においても、各種課題はあるものの、情報コミュニティとして一定の進展が図られている。しかしながら、重大緊急事態[13]や有事（武力攻撃事態、存立危機事態等）の際、情報コミュニティとしての情報活動をどのように行うべきかについて、公にされているものは特にないものと思われる。過去、内閣官房が取りまとめてきた情報機能の強化に向けた取り組みは、そもそも重大緊急事態や有事に対応できるような制度設計になっているのであろうか。内閣情報調査室（内閣衛星情報センターを除く。）は、職員数が約２００人であるが[14]、そのうち、総合的な分析（オール・ソース・アナリシス）を担う内閣情報分析官は８人[15]、総務部門、国際部門その他関係スタッフを含めても限られた人員で、24 時間体制を組み、重大緊急事態又は有事における判断に資する適時的確な総合分析されたインテリジェンス・プロダクトを、政府首脳やＮＳＣ（ＮＳＳ）へ提供できるのか、よく検証すべきかもしれない。仮に、内閣情報調査室の現体制で重大緊急事態や有事の際に対応困難ということであれば、まずは、政府の情報コミュニティの現状の能力を踏まえた重大緊急事態や有事における情報業務のあり方につき、検討する必要があろう。

組織上、防衛省・自衛隊に属する情報組織は、情報本部（職員数約２５００人[16]）の他、陸海空各幕僚監部に情報部署が置かれている[17]。また、各自衛隊には、それぞれの情報専門部隊として、陸上自衛隊（陸上総隊）中央情報隊、海上自衛隊情報業務群及び航空自衛隊作戦情報隊があり、更に、司法警察権を有しないカウンターインテリジェンス（ＣＩ）専門の自衛隊統合部隊として自衛隊情報保全隊（約１０００人）がある[18]。その他本論考で既に説明した情報収集部隊を含めると、日本政府の外国等の情報収集等を行っている機関の人員の大半が、防衛省・自衛隊に所属する情報機関及び部隊に属している[19]。各自衛隊の情報機関（部隊）は、政府の情報コミュニティとしては明示的には含まれていないが、例えば、米国の場合、情報コミュニティ 17 機関に陸海空海兵隊４軍の情報機関が含まれている[20]ことからしても、自衛隊の各情報機関を政府の情報コミュニティに明示的に加えることも検討すべきであろう。

いずれにせよ、重大緊急事態や有事の際、政府首脳、ＮＳＣ等における政策判断及び意思決定を支援する情報活動のあり方については、現況も踏まえてよく検討すべき課題であると思われる。その検討の際には、24 時間体制で平時とは異なる情報活動（ＣＩ活動を含む。）が求められ、かつ、同盟国である米国や友好国との防衛協力や共同対処を円滑に行うためには密接な情報協力が必要であるとの観点も念頭におくべきであろう。　次回（第８回）に続く

[1] 『カウンターインテリジェンス機能の強化に関する基本方針（平成 19 年８月９日カウンターインテリジェンス推進会議決定）の概要』の「１　目的」(http://www.cas.go.jp/jp/seisaku/counterintelligence/pdf/basic_decision_summary.pdf)（２０１８年 10 月 17 日）

[2] 外国の利益若しくは自己の不正な利益を図り、又は我が国の安全若しくは国民の生命若しくは身体を害すべき用途に供する目的で、（中略）特定秘密を保有する者の管理を害する行為により、特定秘密を取得した者は、十年以下の懲役に処し、又は情状により十年以下の懲役及び千万円以下の罰金に処する、とされた（特定秘密保護法第 24 条第１項）。また、未遂も処罰される（同条第２項）。

[3] 内閣官房特定秘密保護法施行準備室『特定秘密の保護に関する法律（逐条解説）』平成 26 年 12 月９日、第７章　罰則（第 23 条－第 27 条）。

[4] 傍受に対する防御性が高いといわれている量子暗号による通信が実用化されたとしても脆弱性があるとの見解がある。Stockholm University, ‘Swedish researchers reveal security hole’ December 18, 2015 (http://www.su.se/english/research/research-news/swedish-researchers-reveal-security-hole-1.262179)（２０１８年８月 31 日）

[5] 「カウンターインテリジェンス推進会議の設置について」（平成 18 年 12 月 25 日内閣総理大臣決定、最新改正平成 30 年４月 26 日）第１項。推進会議の議長は内閣官房長官、副議長は内閣官房副長官（事務）、構成員は内閣危機管理監、国家安全保障局長、内閣官房副長官補（事態対処・危機管理担当）、内閣情報官他、全省庁の情報保全担当責任者である。また、「推進会議の円滑な運営を図るため、推進会議に幹事会を置くこととし、その構成員は、関係行政機関の職員で議長の指名する官職にある者とする」とされている（第３項）。

[6] 内閣情報調査室 HP (http://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa.html)（２０１８年８月 31 日）

[7] 前掲『カウンターインテリジェンス機能の強化に関する基本方針（平成 19 年８月９日カウンターインテリジェンス推進会議決定）の概要』の「２情報管理の徹底」。

[8] 米国インテリジェンスコミュニティでは、ＯＤＮＩにＮＣＳＣ (National Counterintelligence and Security Center) が置かれており、ＮＣＳＣは米国政府のための国家ＣＩ機関のトップ (head) の任を負い、ＣＩコミュニティに戦略レベルの指導を示している、とされている。Office of the Director of National Intelligence, Frequently Asked Questions（以下「ODNI FAQ」という。），P11. (https://www.dni.gov/index.php/about/faq?tmpl=component&format=pdf)（２０１６年 12 月 21 日）

[9] 例えば、２０００年９月のボガチョンコフ事件（萩崎事件）では、防衛庁防衛研究所（当時）の所員であった萩崎三等海佐は、前年から公安当局の監視対象となっていたが、在京ロシア大使館のボガチョンコフ大佐への資料手交現場を当局が取り押さえ、萩崎は任意事情聴取に応じ、その後秘密漏えいの容疑で逮捕された。事案が公になるまで、防衛庁は本件保全事案を組織としては承知していなかった。(『朝日新聞』２０００年９月 30 日他）

[10] 警察庁組織令（昭和 29 年政令１８０号）第 36 条から第 41 条まで。

[11] 海上保安庁組織規則（平成 13 年国土交通省令第４号）第 21 条。

[12] 例えば、米国情報コミュニティの一員である連邦捜査局（ＦＢＩ）及び沿岸警備隊（ＵＳＣＧ）では、情報部署は組織内で分離されており、それぞれ、前者は Intelligence Branch (https://www.fbi.gov/about/leadership-and-structure/intelligence-branch)、後者は本部機構（USCG HQ Organization）のＣＧ－２として、Intelligence & Criminal Investigations (https://www.dco.uscg.mil/Portals/9/DCO%20Documents/DCO_3-0_ORGANIZATIONAL_DIAGRAM.pdf)がある。（２０１８年 10 月８日）
また、オーストラリアの情報コミュニティに関する報告文書、Flood, Philip “The Report of the Inquiry into Australian Intelligence Agencies (The Flood Report),” Australian Government, 20 July 2004, p71 には、’Security intelligence and law enforcement are two distinct functions with separate methodologies, networks of relationships and constituencies.’ と明記している。(https://fas.org/irp/world/australia/flood.pdf)（２０１８年 10 月８日）

[13] 国家安全保障会議設置法第２条第１項第 12 号。
[14] 衆議院国家安全保障に関する特別委員会（平成 25 年 11 月５日）今村洋史委員（日本維新の会）質疑に対する菅義偉国務大臣答弁。
[15] 『政官要覧平成 29 年秋号』政官要覧社、６４４ページ。
[16] 『行政機構図（2017.8 現在)』によれば、情報本部の定員は２４８８人（内訳：自衛官１９１１人、事務官等５７７人）である。
(http://www.cas.go.jp/jp/gaiyou/jimu/jinjikyoku/satei_01_05.html)（２０１８年８月 31 日）
[17] 陸上及び航空幕僚監部には運用支援・情報部、海上幕僚監部には指揮通信情報部がある。統合幕僚監部には情報部門はなく、その機能は情報本部の統合情報部が担っている。なお、防衛省内部部局には防衛省・自衛隊における情報機能（情報収集整理及び保全）を担当する防衛政策局調査課が置かれている。
[18] 衆議院安全保障委員会（平成 20 年４月 11 日）で、松本政府参考人は、自衛隊情報保全隊の人員数を「平成二十年度予算では、（中略）計九百六十六名」と答えている。
[19] 各機関の定員は、内閣情報調査室約５００人（内閣衛星情報センターを含む。)、公安調査庁１６０９人、外務省国際情報統括官組織１４１人、警察庁警備局外事情報部２６６人である。（内閣情報調査室を除き、前掲書『行政機構図（２０１７.８現在)』による。）
[20] 大統領令 EO12333 (PART1, 1.7 Intelligence Community Elements)に、 (f) The intelligence and counterintelligence elements of the Army, the Navy, the Air Force, and the Marine Corps; とある。