日本政府の情報機能（第３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

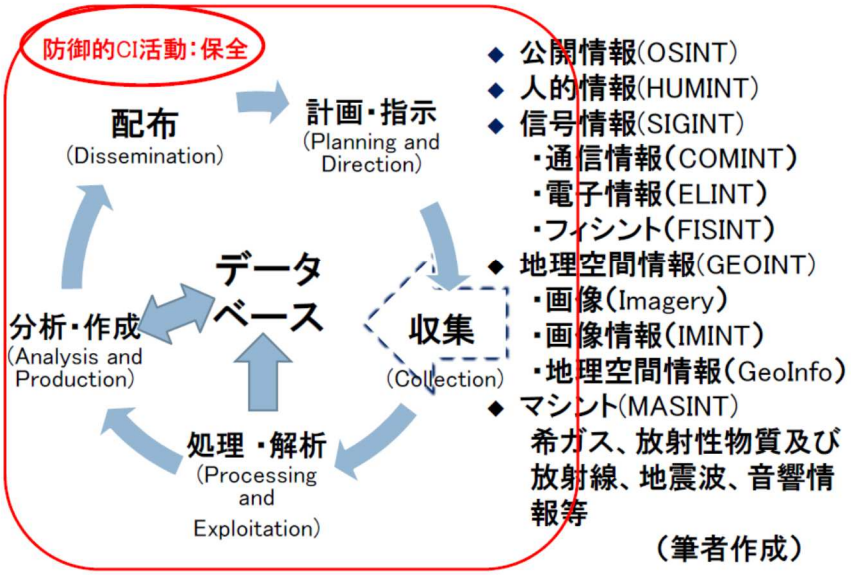
今回（第３回）は、第１章　情報機能の概要のうち、⑤カウンターインテリジェンス及び⑥政策・運用部門と情報部門との分離と連接について述べることとする。

第５節　カウンターインテリジェンス（Counterintelligence）[1]

カウンターインテリジェンス（ＣＩ）とは、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）、又は国際テロリスト組織若しくはテロ活動のために又はそれらに代わって行われる、スパイ行為、その他の情報活動、破壊工作、又は暗殺行為を特定し、たぶらかし、活用し、妨害し又は防護するため、収集するインフォメーションから生成されるインテリジェンスをいう。「対情報」と呼ぶ場合もある。換言すると、ＣＩ活動は、自国及び自国の国益にとって脅威となる外国等（外国、（潜在的に）敵対する軍隊又は武装集団等をいう。）の情報活動を特定し対処することである。したがって、ＣＩの主たる関心対象は、外国（軍）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。

このようなＣＩ活動は、日本政府の情報活動の保全を確保するために必要不可欠な活動である。ここでは、ＣＩ活動を、「防御的ＣＩ活動」、「攻撃的ＣＩ活動」及び「ＣＩサイクル活動」の三つに分けて解説する。

＜図３＞情報サイクル活動とCI活動



（筆者作成）

（１）　防御的ＣＩ活動

前回（第２回）、情報機関の任務で最も留意すべき点として、情報はカスタマーに対して提供され、カスタマー以外へ漏えいしてはならない旨述べた。このためには、情報サイクル活

動全般に亘り、保全上の手続きに依らない故意又は過失による情報の漏えいや情報の不正取得が発生しないように保全措置を行うことが必要不可欠である。

このように、情報機関におけるＣＩ活動の第一は、＜図３＞に示すように、情報サイクル活動全般に亙り、国の保全すべき情報及び重要資産（Assets[2]）を外部から不法に取得されないよう保全することである。本論考では、これを「防御的ＣＩ活動」と呼ぶこととする。保全すべき情報としては、特定秘密保護法別表に掲げる、防衛、外交、特定有害活動[3]の防止及びテロリズムの防止に関する事項に関する情報のうち、行政機関の長が特に秘匿すべきものとして指定したもの（特定秘密）その他秘匿を要する情報が上げられる。

保全の対象としては、まずは人である。情報機関に所属するか否かに拘わらず、保全すべき情報を扱う人[4]が故意又は過失により当該情報を漏えいしないように、部外者との接触届を含め、保全に関する法令や内部規則を遵守させるとともに、部外からの不自然な働きかけ等があり保全すべき情報を漏えいした（又はその恐れがある）場合には、関係者が包み隠さず組織の保全担当へ報告する職場環境を醸成することが必要である。

施設に関する保全措置も必要である。物理的に立ち入り制限を行うほか、施設内から不用意に電磁波が漏れないようにテンペスト[5]対策を行う必要がある。秘匿度の高い情報を扱うために、施設自体の地下化を図ることも方策の一つである。

情報通信システム（暗号を含む）の保全も重要である。外部からの情報の不正取得を防ぐために、システムを扱う人が保全規則を遵守することや、情報通信システムを情報コミュニティ内の閉じたイントラネットシステムとするなどの措置をとったとしても、施設外の回線や無線（衛星通信を含む）を使って情報が伝達される以上、そのような通信情報は傍受されているとの前提で保全対策を講ずることが必要不可欠である。主たる対策は、通信情報が傍受されたとしても解読されないよう暗号化を図ることだが、この世界はいわばイタチごっこの世界であり、解読されているのではとの懸念を持ち常に改善措置を施すことが必要である。また、第三者（政府内の統一機関か、特定秘密に係るクリアランスを保有する契約邦人企業）が、各機関の暗号化された通信情報を傍受しそれを解読できるか、秘匿強度を随時確認することも必要であろう。

（２）　ＣＩサイクル活動

攻撃的ＣＩ活動を説明する前に、ＣＩ分野においても情報サイクル活動があることを説明する。ＣＩ活動は、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る旨述べたが、そのためには、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。彼らのスパイ活動や多彩な情報収集の脅威、破壊活動、テロリズムその他の関連脅威に関するデータ及びインフォメーションを収集し、処理・解析の上、総合的な分析を行ったＣＩプロダクトを作成し、そのプロダクトを必要とする関係部署及びその責任者に提供・共有する活動が行われなければならない。このようなＣＩ活動は、情報部門に限らず、政策・運用部門も含めた、ＣＩプロダクトを必要とする関係部署からの（潜在的な）要求に応えるべく行われる情報サイクル活動となる。

（３）　攻撃的ＣＩ活動

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。より効果的にくじくとは、対象国等の情報活動を制圧する(neutralize)こと、例えば、彼らの活動が犯罪行為に当たれば被疑者を逮捕することのみを指すのではなく、逆に有効に活用する(exploit)という意味も含まれている。例えば、対象国等のスパイを我が方の味方に付け我が方の情報源とする（いわゆる二重スパイ化する）とか、偽情報を流して対象国等の情報収集ルートをつかみ、広範囲なＣＩインフォメーションを収集する等が上げられる。

第６節　政策・運用部門と情報部門との分離と連接

情報機能の概要のポイントとして、「政策・運用部門と情報部門との分離と連接」という原則を日本政府の例を参考にしながら解説する。

（１）　政策・運用と情報の分離

政策と情報との分離の必要性については、官邸における情報機能の強化に関する過去の報告書等に指摘されている。例えば、２００８年（平成 20 年）２月に情報機能強化検討会議[6]が取りまとめた、「官邸における情報機能の強化の方針」（以下「官邸情報機能強化方針」という。）には、「２ 情報機能の強化（１）政策との連接①政策と情報の分離」に「情報部門においては、政策部門の情報関心に基づいて、情報を収集し、収集された情報の集約・分析を行い、その成果を政策部門に提供する。他方、政策部門は、提供された情報を政策立案及びその実施に活用し、その上で、新たな情報関心を提示する。適正な政策判断を行うためには、収集された情報を政策部門から独立した客観的な視点で評価・分析する別個の部門が必要であることから、官邸における政策部門と情報部門は、官邸首脳の下、別個独立の組織とし、政策と情報の分離を担保する[7]。」（下線は筆者記載）と記されている。上記内容から、政策と情報との分離の必要理由は、「政策部門から独立した客観的な視点で評価・分析する」ためであることが読み取れる。要するに、政策部門と情報部門を別組織（部署）としないと、政策部門（政策決定者）の恣意的な判断を支えるように情報部門の情報プロダクトがゆがめられる、又は、行いたい政策にとって都合のよい情報（インフォメーション）をつまみ食いされるおそれがある、ということである。

政策部門と情報部門の分離と同様、部隊行動を担任する運用（作戦）部門と情報部門との分離も必要である。通例、軍事組織の統合司令部機構では、部隊の作戦計画・実施を担当する部署を第３部（Ｊ３）、情報部署を第２部（Ｊ２）と呼んでおり、運用と情報は別部署となっている。部隊司令官は、本人の独断や恣意的な判断ではなく、正確で総合的な分析により作成された情報（インテリジェンス）に基づき、適切な意思決定を行うことが必要であり、そのためにも両者は別の部署となっている。自衛隊の統合司令部に相当する統合幕僚監部（統幕）の場合は、その組織内にＪ２は存在しない。この点は、米国の統合参謀本部（JCS: Joint

Chiefs of Staff）の場合も同様であり、ＪＣＳ内にＪ２は存在しない。その代わりに、自衛隊の場合は、防衛省・自衛隊の中央情報組織である情報本部（DIH : Defense Intelligence Headquarters）、とりわけＤＩＨ内の統合情報部が自衛隊の部隊運用に必要な情報を統幕等に提供している[8]。米国の場合は、国防省の情報機関である国防情報局（DIA: Defense Intelligence Agency）の J2 Directorate for Intelligence がＪＣＳ等に対する情報提供を行っているとみられる。

一方、緊急事態が発生して迅速な対応が求められるときには、政策・運用部門と情報部門が、危機行動チーム（Crisis Action Team）を組んで、物理的にも同一のオペレーションルームで相互に連携して対処する場合がある。これは、時間的な制約の中で、政策判断者及び部隊司令官がより迅速で適切な意思決定を行うことができる支援態勢を整えるための緊急時における措置である。政策・運用部門と情報部門の分離原則は、その目的が適切な政策・運用判断を図るということにある以上、緊急事態における柔軟な対応は当然であろう。

（２）　情報部門を分離するもう一つの理由

政策・運用部門と情報部門とを分離する理由として、日本の政府内外の報告書や研究文献では明示的には余り指摘されてはいないが、本論考ではもう一つ重要な理由を指摘したい。それは保全のためである。カウンターインテリジェンス（ＣＩ）活動の第一は、防御的ＣＩ活動、すなわち、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に保全を図ることである。

政策・運用部門に属する者は、情報のカスタマーとして、それぞれの者が認められた保全レベルの情報プロダクトにアクセスするクリアランスを保持しているはずである。したがって、カスタマーが必要な情報プロダクトにアクセスしそれを活用することは、当然である。一方、カスタマーは、情報サイクル活動のうち、例えば、収集や処理・解析に関するインフォメーション（情報源や収集能力、収集データの解読状況等）については、原則知る必要はない。更に言えば、そのような機微にわたるインフォメーションをカスタマーが承知し不用意にカスタマーの間で共有された場合、予期せぬ情報漏えい事案となり、ひいては収集能力上の損失になりかねないことから、そういった事態にならないよう、まずは、情報部門と政策・運用部門（カスタマー）を分離し、カスタマーとしては知るべきでない情報収集源や処理・解析能力などのインフォメーションにはアクセスさせないよう措置することである。

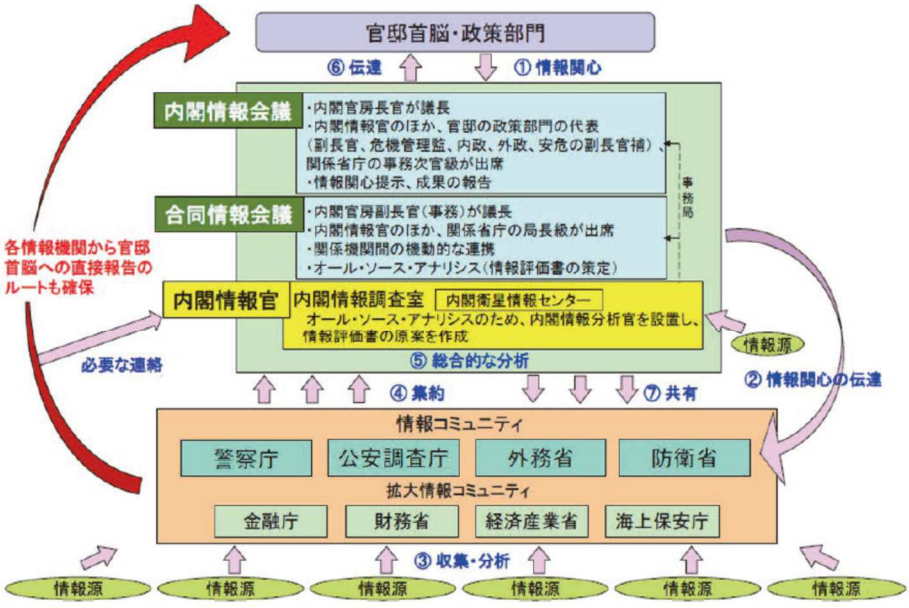
情報部門と政策・運用部門の分離は、組織や人の分離に止まらず、使用する施設や情報通信システムの分離も必要である。例えば、仮に情報通信システムを政策・運用部門と情報部門が共用している（電子的に分離していない）機関[9]があるとしたら、保全すべき情報がカスタマー以外の知るべきでない者へ当該機関内で漏えいするおそれがあることから、そのようなことがないように情報部門とそれ以外が使用する情報通信システムは別個のものとする必要がある。政策・運用部門と情報部門の分離について十分な保全措置をとっていない機関は、情報サイクル活動（同盟国・友好国の情報機関との協力を含む）及びＣＩ活動の両面において、外国等による情報収集活動に脆弱であり、保全すべき情報の漏えいを許しかねないこととなり、情報機能の強化や情報コミュニティ発展の障害となろう。

（３）　政策・運用と情報の連接

「官邸情報機能強化方針」の「２　情報機能の強化（１）政策との連接　②政策と情報の有機的な連接」には、「政策と情報の分離を前提としつつ、政策判断に資する情報の提供を確保するためには、両者の有機的な連接が必要である。そのため、官邸首脳の指揮の下、官邸の政策部門からの情報関心が明確かつタイムリーに情報部門に伝えられ、他方、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（オール・ソース・アナリシス）によりその価値が最大化された情報が政策部門に提供されるよう、内閣情報会議、内閣情報官及び各情報機関が連携して機能する[10]。」と記載されている。

＜図４＞「我が国の情報体制」は、２０１３年（平成 25 年）３月に「国家安全保障会議の創設に関する有識者会議」の第３回会合において内閣官房が提示した資料の抜粋である。これによれば、官邸首脳・政策部門との連接については、内閣情報会議等を通じた官邸政策部門からの情報関心の伝達、同部門に対する情報の提供、及び日常的な結節点としての内閣情報官が機能することにより、有機的な連接を図るとされている[11]。

＜図４＞我が国の情報体制[12]



（出所）「国家安全保障会議の創設に関する有識者会議（第３回会合）」配布資料

２０１３年 12 月に安全保障に関する重要事項を審議する機関として国家安全保障会議（NSC: National Security Council）が内閣に置かれ[13]、また、翌２０１４年１月にＮＳＣの常設事務局である内閣官房国家安全保障局（NSS: National Security Secretariat）が発足した[14]。情報の要求及び提供に関して、ＮＳＣと政府の情報機関（が属する行政機関）との関係を規定する条文は、国家安全保障会議設置法（昭和 61 年法律第 71 号）第６条である。すなわち、①情報機関は、ＮＳＣに対し、我が国の安全保障に関する情報であってＮＳＣの審議に資するものを適時提供するものとする旨（同法同条第１項）、②情報機関は、ＮＳＣ議長（内閣総理大臣）の求めに応じ、ＮＳＣに対して我が国の安全保障に関する情報を提供及び説明その他必要な協力を行わなければならない旨（同法同条第２項）、規定された。そして、ＮＳＳは、上記①及び②に係る情報を総合して整理する事務をつかさどることとされている（内閣法（昭和 22 年法律第５号）第 17 条第２項第３号）。このように、ＮＳＣ及びＮＳＳ発足後は、法的

根拠に基づき、内閣情報調査室を含む各情報機関に対し、ＮＳＣの審議に資する情報を適時又は求めに応じ提供することが義務付けられ、安全保障に関する政策部門と情報部門との連接は法定化された。しかしながら、法定化より重要なポイントは、ＮＳＣ及びＮＳＳが安全保障に関する外交・防衛政策の最終調整・審議機関として機能するようになり、そのため情報要求に応じた又はそれを見越した情報プロダクトのタイムリーな提供が必須となり、このことにより情報サイクルが活性化されるようになったということであろう[15]。

一方、ＮＳＣ及びＮＳＳ以外の政府内の政策・運用部門と情報部門との連接については、基本的には省庁レベルでの問題であるが、いまだ、政策・運用と情報との分離と連接に課題を有する省庁があるとみられている。

次回（第４回）に続く

---

[1] Counterintelligence: Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons or their agents, or international terrorist organizations or activities. (DOD Dictionary) なお、この定義ではＣＩ活動を含めているが、本論考ではＣＩとＣＩ活動を分けて記述していることから、本文のような記述とした。

[2] Assets には、モノ（重要施設、装備品や情報通信システム）のほか、ヒトも含まれる。

[3] 「公になっていない情報のうちその漏えいが我が国の安全保障に支障を与えるおそれがあるものを取得するための活動、核兵器、軍用の化学製剤若しくは細菌製剤若しくはこれらの散布のための装置若しくはこれらを運搬することができるロケット若しくは無人航空機又はこれらの開発、製造、使用若しくは貯蔵のために用いられるおそれが特に大きいと認められる物を輸出し、又は輸入するための活動その他の活動であって、外国の利益を図る目的で行われ、かつ、我が国及び国民の安全を著しく害し、又は害するおそれのあるものをいう。」（特定秘密保護法第 12 条第 2 項第１号）

[4] 保全情報を扱う人は、保全チェックの手続きを事前に受け、いわゆるクリアランスを付与された者であることは、言うまでもない。特定秘密の取扱いの業務を行う者は、原則、特定秘密保護法の規定に基づく「適正評価」の手続きを経て、特定秘密情報を漏らすおそれがないと評価された者（クリアランス付与者）でなくてはならない。

[5] TEMPEST(transient electromagnetic pulse surveillance technology): 電磁波盗聴、コンピューターや周辺機器が発する微弱な電磁波を傍受する技術の総称。

[6] 官邸における情報機能の強化を検討するため、内閣に設置された検討会議。議長は内閣官房長官。
(http://www.kantei.go.jp/jp/singi/zyouhou/konkyo.html) (２０１８年 10 月 10 日)

[7] 官邸情報機能強化方針１~２ページ。

[8] 統合情報部は、「緊急に処理することを要する情報（緊急情報）及び外国軍隊等の動態に関する情報（動態情報）の集約に関すること」等の事務をつかさどり、自衛隊の統合運用に必要な情報の集約を担当している。（情報本部組織規則第８条各号）

[9] 例えば、外務省は、本省と在外公館の通信システムに関し、情報機関が扱う情報とそれ以外の事務が使用する通信システムを分離していないのではないか、と言われている。

[10] 官邸情報機能強化方針２ページ。

[11] 「我が国の情報機能について」『国家安全保障会議の創設に関する有識者会議（第３回会合）』内閣官房、平成 25 年３月 29 日、５ページ。

[12] ＜図４＞我が国の情報体制は、国家安全保障会議の設立や国家安全保障局の発足前の政策部門と情報部門の連接を表現している図として内閣官房が取りまとめたものである。

[13] 国家安全保障会議設置法第１条

[14] 内閣法（昭和 22 年法律第５号）第 17 条

[15] ２０１５年ＰＨＰ報告書、41 ページ。