

目 次

1	英国の対情報機関（M15）の概要	1 頁
2	IAQG（国際航空宇宙品質グループ）について	16 頁
3	現役時代を振り返って思うこと（その2）	19 頁
4	防衛関連企業に求められている総合的 情報保全体制の重層的構築について	20 頁

英国の対情報機関（MI5）の概況

客員主任研究員 横山恭三

はじめに

筆者は本紀要第一巻第四号（平成20年3月）に「カウンターインテリジェンスの日本語表記」と題して、米国の法律等を調査・考察した小論を寄稿した。その後、英国では「カウンターインテリジェンス」をどのように定義しているのかに興味を持ち、英国の国家情報機構や関連法律等を調査（インターネットに公開されているオープンソースに限定）したところ、英国では「カウンターインテリジェンス」という用語を使用していないことを知った。

米国が使用している「カウンターインテリジェンス」は、エスピオナージ、サボタージュ、テロリズム及びその他のインテリジェンス活動（合法的な情報収集等）への対応全てが包摂された概念であるが、一方、英国では、米国のような包括的なカウンターインテリジェンスの概念は存在せず、米国のカウンターインテリジェンスのサブセットである、カウンターテロリズム、カウンターエスピオナージの個別の概念がそのまま使われている。米国と英国は同じ英語を使用するが別々の国であり、歴史も違えば文化も違う。両国の情報コミュニティの使用する言葉や考え方が違って何ら不思議なことではないのかもしれない。

本稿は、英国の主要なセキュリティ機関である MI5 の概況を紹介する目的で、英国情報コミュニティの各組織のホームページ（HP）の記載内容と関連法律の内容を整理・摘記したものである。何故、MI5 かといえば、筆者は、MI5こそが正真正銘のカウンターインテリジェンス（対情報）機関であると考えているからである。

以下、MI5 の役割・組織・業務と予算・活動・統治（ガバナンス）について順次述べる。本稿が我が国のカウンターインテリジェンス体制を構築する一助となれば幸甚である。

1. MI5 の役割

MI5 の正式名称はセキュリティ・サービス（Security Service）であるが、かつて MI5（Military Intelligence section 5）という名称であったことから、今日でも広く MI5 と称されている。それゆえ本稿でも MI5 を使用する。

MI5 の役割は、1989年セキュリティ・サービス法に「国の安全を保護するものとする。とりわけ、エスピオナージ、テロリズム及びサボタージュからの脅威、外国勢力のエージェントの活動からの脅威並びに政治的、産業的、及び暴力的手段による議会制民主主義を転覆又は弱体化しようとする活動の脅威から国の安全を保護するものとする。」と定義されている。この法律に定められた役割を遂行するための MI5 の目標は次のとおりである。

- ・テロリズムの企てを阻止する。
- ・外国のエスピオナージ及びその他の隠密の活動からもたらされる英国の損害

を予防する。

- ・ 拡散国が、大量破壊兵器に関連した物質・技術・専門知識を調達するのを阻止する。
- ・ 新しい又は再現しつつある脅威を監視する。
- ・ 政府のセンシティブな情報及び資産並びに重要な国家インフラストラクチャーを防護する。
- ・ 秘密情報局 (Secret Intelligence Service : SIS、所謂 MI6 以下 MI6 という) 及び政府通信本部 (Government Communications Headquarters : GCHQ) が法令に定められた機能を果たすのを支援する。
- ・ MI5 の能力と強靱性を強化する。

2. MI5 の組織

MI5 は、内務大臣の法的権限の下で活動するが、内務省には属していない。MI5 の長は長官 (Director General) であり、長官は MI5 を統轄するとともに内務大臣に対する説明責任を有する。長官は副長官によって補佐される。MI5 は政策及び戦略方針の策定に責任を有する理事会とそれぞれが特定の分野に責任を有する 6 つの部 (ブランチ) で構成される。全職員数は約 3, 000 名であるが、2008 年には約 3, 500 名に増員予定である。

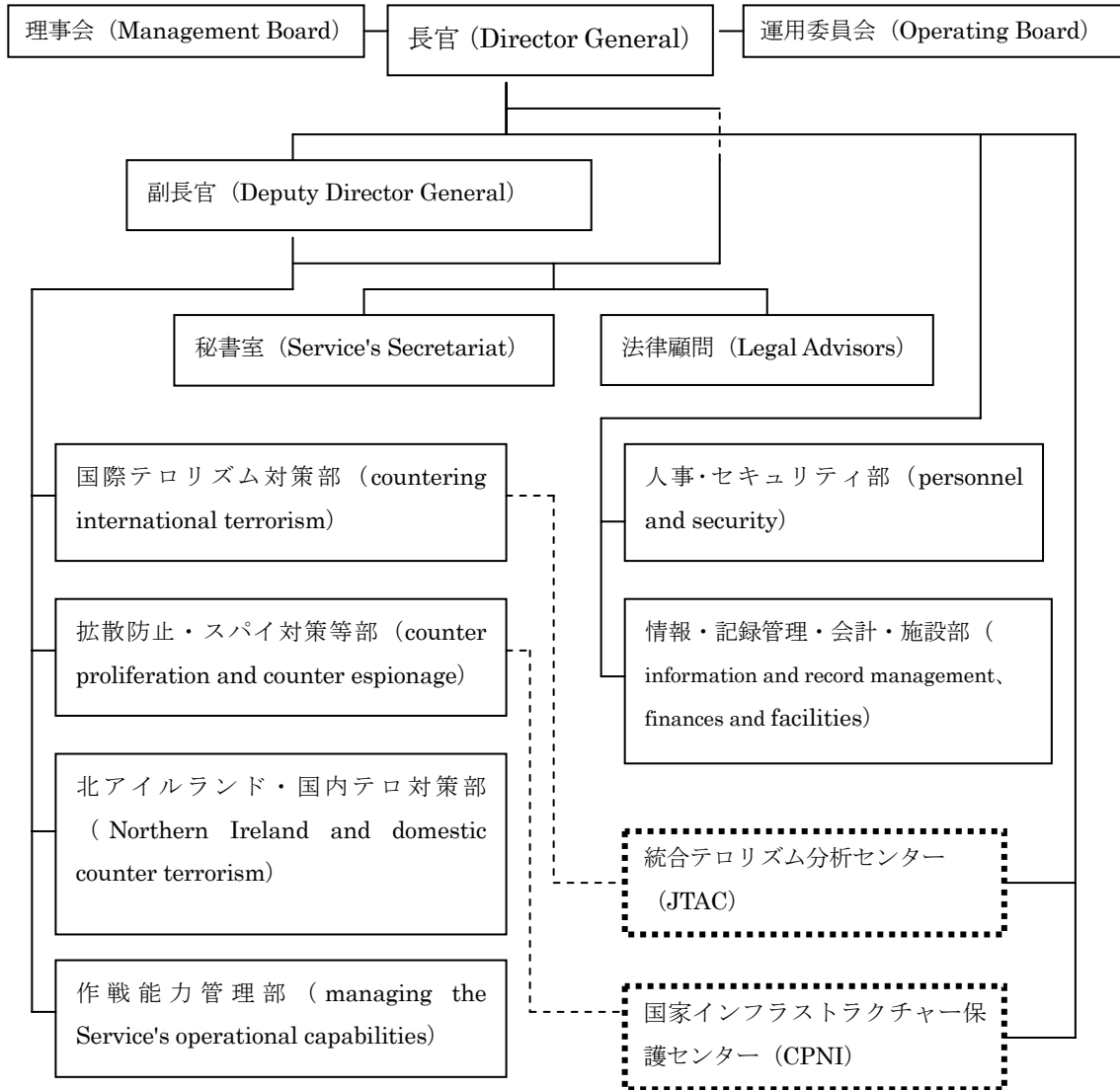
(1) 理事会等

理事会 (Management Board) は、長官、副長官、各部長、及び法律顧問で構成され、政策と戦略を検討するために定期的開催される。理事会は、部外の視点及び民間部門の専門知識等を取り入れて意思決定を強化するために、組織外から任命された 2 名の非常勤役員 (Non-Executive Director) によって支援される。非常勤役員は MI5 の業務運営に関する責任は有せず、純粋に助言者としての役割を果たす。また、理事会とは別に、運用委員会 (Operating Board) が開催される。同委員会は、MI5 の日々の活動に関する指示、調整及び優先事項並びに運用について責任を有する。

(2) 各部等の責任

6 つの部は、それぞれ一人の部長 (Director) に率いられる。そのうち副長官の隷下にある部は 4 つある。①国際テロリズムを担当する部、②拡散対策やエスピオナーズ対策を実施するとともに様々な脅威に対する保護セキュリティ対策に関するアドバイスを提供する部、③北アイルランドと国内テロ対策を担当する部及び④技術や監視作戦のような MI5 の作戦能力を管理する部である。残りの 2 つの部は長官の隷下にある。①人事とセキュリティを管理する部と②情報、記録管理、予算、及び施設に関する責任を有する部である。以上の 6 つの部以外に秘書室と法律顧問が置かれ、両者とも長官と副長官の双方を補佐する。

MI5 の組織図



(3) 関連組織

ア. 統合テロリズム分析センター (JTAC)

統合テロリズム分析センター (Joint Terrorism Analysis Centre : JTAC) は、国際テロリスト脅威の増大に対応し、主要な政府機関の保有する対テロの専門知識を結集するため 2003 年に創設された。同センターは MI5、MI6、政府通信本部 (GCHQ)、国防情報局 (Defense Intelligence Staff : DIS)、外務省及び内務省等の 16 の政府省庁からの代表者で構成され自立した組織として運営される。同センターは、脅威レベルを設定し、脅威警報をタイムリーに発出する他、テロ

リストのネットワークや能力に関する報告を提供する。同センターは MI5 本部の建物内に位置し、とりわけ、MI5 の国際テロリズム対策部門と緊密に連携する。同センターは MI5 には属していないが、同センターの長は MI5 長官に対する説明責任を有している。

イ. 国家インフラストラクチャー保護センター (CPNI)

国家インフラストラクチャー保護センター (Centre for the Protection of National Infrastructure : CPNI) は、国家インフラストラクチャーセキュリティ調整センター (National Infrastructure Security Coordination Centre : NISCC) と MI5 の一部であった国家セキュリティ・アドバイス・センター (National Security Advice Centre : NSAC) が 2007 年 2 月に統合して創設された。同センターは、重要な国家インフラストラクチャーを運営する企業と組織に対しセキュリティ・アドバイスを提供することを任務とする。同センターは、とりわけ MI5 の拡散防止・スパイ対策部と緊密に連携する。同センターは MI5 に属していないが、同センターの長は MI5 長官に対する説明責任を有する。

3. MI5 の業務と予算

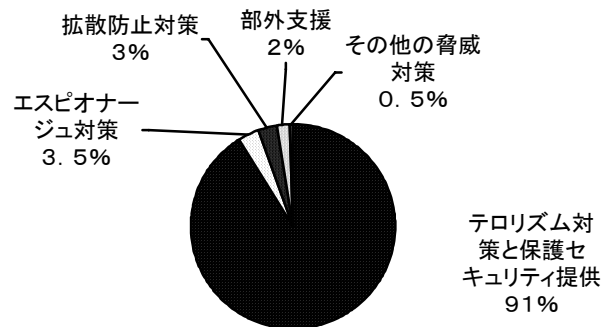
英国は、安全に対する様々な非公然の脅威に直面している。MI5 は唯一、それらに対処する資源を保有している。

MI5 にとって、合同情報委員会 (Joint Intelligence Committee : JIC) (後述「国内の情報機関」) が定めた情報収集の優先事項を考慮しつつ、これらの脅威に優先順位を付け、それに応じて資源を配分することは極めて重要である。MI5 の予算は、単一情報会計 (Single Intelligence Account : SIA) (注) から支出される。2007/08 の単一情報会計 (SIA) の総額は 15 億 5300 万ポンド (約 3,730 億円) である。

	2004/05	2005/06	2006/07	2007/08
資源の部 Resource	1,126.6	1,266	1,336	1,381.8 (£ million)
資本の部 Capital	150.8	231.8	232.4	238 (£ million)
合計	1,313.7	1,361.3	1,480	1,553 (£ million)

(注) MI5 と MI6 と政府通信本部(GCHQ)は合わせて、三機関 (the Agencies) と総称される。三機関は、ヒューミント (HUMINT : Human Intelligent) やシグイント (SIGINT : Signal Intelligence) による秘密情報の収集等を主たる任務としているため、法律によって、その行動が厳しく規制され、かつ監視される。三機関の予算は、各省庁の予算から独立した単一情報会計 (SIA) から支出される。

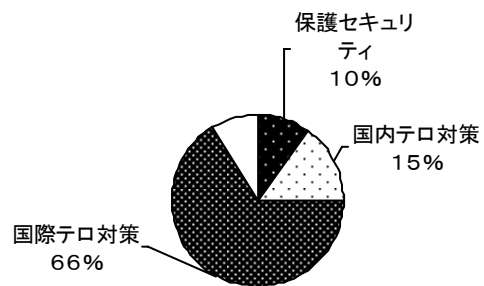
セキュリティ上の理由から、単一情報会計（SIA）の各機関への配分は公表されていないが、MI5の主要業務毎の予算配分はMI5のホームページに公表されている。それによると、2008年4月の主要業務毎の予算配分は、①テロリズム対策と保護セキュリティの提供に91%、②エスピオナーズ対策に3.5%、④大量破壊兵器の拡散防止対策に3%、⑤部外支援に2%、その他の脅威対策に0.5%である。



(1) テロリズム対策と保護セキュリティ対策

MI5の主たる活動は、国際及び国内（大部分は北アイルランドとの関連）双方のテロリズム対策とその任務を支援する保護セキュリティ対策である。現在、MI5の予算の約91%がテロリズム対策と保護セキュリティ対策に投入されている。この分野へ投入された予算のレベルは、国際テロリズム脅威の増大に伴い、過去2、3年に顕著に増加している。

国際テロリズムとの戦いが、テロ対策支出の66%を占め、15%が北アイルランド関連のテロ対策に投入されている。また、保護セキュリティ対策への支出は10%を占めている。



ア. テロリズム対策 (Counter-Terrorism)

1960年代より、MI5は、英国の国内及び国外両方で、英国の利益に対するテロ脅威との戦いに関与してきた。テロに関連した多くの組織が、2000年テロリズム法 (Terrorism Act 2000) により非合法化され、非合法化された組織のメンバーになること又はそれらを支援することは刑事上の犯罪となった。テロリズムは同法によって次の様に定義されている。「テロリズムとは、①人に対する重大な暴力、②財産に対する重大な損害、③人命に対する脅威、④一般市民の健康と安全に対する重大なリスク、⑤電子システムに対する重大な干渉又は混乱をもたらす行動の実施又は脅迫、⑥政府に影響を及ぼすこと又は一般市民若しくはその一部を脅すことを企図した行動の実施又は脅迫、並びに⑦政治的、宗教的又は思想的理想を促進する目的のための行動の実施又は脅迫を意味する。」

隠密に行動し、かつ、高度に組織化されたグループの意図と活動に関する正確な情報を入手することは非常に難しい。特に、その様なグループの多くは海外の近づき難い地域を根拠にし、幾つかは彼らの活動から利益を得ている外国政府の保護下にある。海外で計画され、実行される攻撃を防止するためにできることは

限られている。したがって、MI5は、国内及び国外で他の機関と協力している。

イ. 保護セキュリティ対策

MI5は、政府のセンシティブな情報及び資産並びに重要な国家インフラストラクチャーを防護する役割を有している。このため、広範な組織に対し、その組織の脅威に対する脆弱性を低減させることを目的に、セキュリティ・アドバイスの提供を含む保護セキュリティ対策を促進している。官庁に対する保護セキュリティ対策（アドバイスを含む）はMI5が実施するが、一方、国家インフラストラクチャーを運営する組織や民間企業に対するセキュリティ・アドバイスは、国家インフラストラクチャー保護センター（CPNI）が実施している。同センターのアドバイスの目的は、テロリズム及びその他の脅威に対する国家インフラストラクチャーの脆弱性を低下し、英国の重要なサービス（通信・救急・エネルギー・金融・食料・行政・衛生・輸送・水道サービス）の安全を確保することである。

（2）エスピオナージ対策（Counter-Espionage）

冷戦間、ソビエトとワルシャワ条約加盟国のエスピオナージ（スパイ行為）との戦いがMI5の業務の重点であった。ソビエトの崩壊以後、脅威は大きく減少したが、敵対的な外国の活動、特にロシアや中国の情報機関の活動は依然として懸念事項である。スパイ対策はMI5の資源の3.5%を占めている。これは5%を占めていた2007年1月よりも小さくなっているが、MI5全体の支出額が増加しているので、この分野の支出レベルは一定のままである。

1911年秘密保護法（Official Secrets Act 1911）は、「英国の安全と利益を害する目的で、①立ち入り禁止場所の近傍に、接近・調査・通過・若しくは存在する、又は禁止場所に侵入する行為、②敵に有益若しくは有益だろうと推定し、又は直接又は間接に役立てることを意図して、スケッチをし、図面を作成し、模型を作成し、若しくはメモ書きを作成する行為、③敵に有益若しくは有益だろうと推定し、若しくは直接又は間接に役立てることを意図して、暗号、パスワード、スケッチ、図面、模型、品物、メモ書き若しくは文書を、取得・収集・記録又は公表すること若しくは他人に伝達する行為」をスパイ行為（'spying'）と定義している。

MI5は、その漏洩が英国の安全保障と経済的利益に損害をもたらすことになるセンシティブ情報がエスピオナージにより窃取されることを防止する。この目的のため、MI5は、英国のセンシティブ情報及び装備を他国に漏洩しようとするものを探知し、その企てを阻止することを目指している。同時に、MI5は、有害である又は潜在的に有害であると判断される外国情報員（intelligence officers）の活動を調査・妨害する。妨害の方法は様々である。例えば、工作員（agent）を徴募しようとする外国情報機関の意図を当該者に警告するとともに、その接触を如何に回避するか又は対応するかの助言を提供する。また、センシティブ情報及び装備を所有している企業や組織に対し、彼らの資産の保護方法に関する助言を提供することにより外国情報機関の活動をより困難にすることを目指している。

もし、外国情報員の活動が著しく侵害的であるか又は英国の利益に対し真に損

害を与える恐れがある場合は、その外国情報員は、外務省から国外退去を要求されるであろう。また、MI5 は、国務大臣に対して、外国情報員へのビザ発給を、国家安全保障を理由に拒否することを勧告することができる。

(3) 部外支援

MI5 は、英国の国家安全保障に携わる他の機関、特に政府通信本部 (GCHQ) と MI6 と非常に緊密に協力している。MI5 の資源の 2 % がこの分野で使用されている。三機関 (MI5、MI6、政府通信本部 (GCHQ)) は異なるが関連した機能を有する。そして、相互支援の範囲は広い。例えば、MI6 と MI5 は、重複を避けるために、ある支援領域で資源を共有している。

(4) 拡散対策 (Counter-Proliferation)

大量破壊兵器の拡散は重大な懸念事項である。それは英国の国家安全保障に対し潜在的な脅威をもたらしている。1992 年以来、MI5 は、この分野で主導的な役割を果たしている政府機関の業務を支援することで、この脅威との戦いの一翼を担っている。拡散防止対策に資源の 3 % を支出している。

MI5 は、国内外の他の政府機関と緊密に連携し、大量破壊兵器プログラムに関連する英国の材料、技術又は専門知識を取得しようとする拡散懸念のある国の企てを調査し、そして阻止することを目指している。これには、知識の取得及び輸出 (又は “無形技術移転”) を防止することも含まれる。例えば、懸念国から英国に留学している学生又は研究者は、彼らの国の大量破壊兵器プログラムに直接利益になるテーマについて学ぶことができる。このため、MI5 は、英国の企業、ビジネスリンク (中小企業支援のためのワンストップショップ)、商工会議所、専門職/貿易協会、大学及びその他の教育又は研究機関に対し、拡散懸念のある国及び人物の意図や活動について警告するとともに、企業等とそれらの人物等との取引に関する情報を収集する。

(5) 新しい脅威

技術の急激な発展、セキュリティ問題の様相の変化及び過激派活動の出現は、英国の将来の国家安全保障に対する挑戦となっている。このため、MI5 は、英国固有の過激派からもたらされる可能性のある新しいリスクを特定する技術開発に努力している。これらの業務に資源の 0.5% を支出している。

(6) もはや担当していない業務

英国の国家安全保障に対する脅威は変化し続けている。今日英国が直面している多くの脅威は、20 年又は 40 年前に直面した脅威とは種類と規模において非常に異なっている。このため、MI5 がもはや活動していない 2 つの分野がある。一つは、重大犯罪 (違法な麻薬輸入、武器密輸等) の分野である。1996 年に重大犯罪に取り組むようになった MI5 は、重大犯罪の脅威と戦うために、伝統的なテロリストやエスピオナーズに使用したスキルと資源の全てを動員した。しかし、重

大組織犯罪局（**Serious Organized Crime Agency : SOCA**）の設立と国際テロリズムからの増大する脅威に対応するために、資源を転用する必要性によってこの分野の活動は2006年4月に中止された。もう一つは政府転覆活動（**subversion**）（破壊分子の組織が民主主義を弱体化又は転覆しようとする脅威）の分野である。20世紀の大部分の間、転覆活動はMI5の大きな懸念事項であった。この脅威は、冷戦の終焉に伴い急激に減少した。MI5は、もはや政府転覆対策を担当していない。しかし、新しい脅威の出現を監視している中で、転覆活動の脅威の増加を示す兆候がある場合には再び対策に着手するであろう。

4. MI5の活動

MI5は、文民組織（**civilian organization**）であり、職員は、拘留又は逮捕する権限などの執行権を有していない。このため、刑事犯罪を犯し又は計画している人物を逮捕する見込みがある場合の調査・捜査は、警察又は法執行機関と共同して行われる。

また、国家安全保障上の脅威は、海外から、例えば、外国の情報機関又は海外に拠点を置くテロリストグループからしばしばもたらされる。したがって、国家安全保障の範囲はイギリス諸島を超えて拡大し、世界中の英国の利益、即ち、外交施設、英国企業及び海外で生活する英国市民又は旅行者を守ることもMI5の業務に含まれる。この様な海外のセキュリティ上の脅威に取り組むために、MI5は、海外情報を収集する責任を有するMI6、政府通信本部（**GCHQ**）及び外務省と緊密に協力するとともに外国の警察及び情報機関とも協力する。MI5の活動の重点は次のとおりである。

- ・脅威に関する秘密情報を入手、照合、分析及び評価するために、疑わしい個人及び組織を調査する。このために効果的な情報収集と情報管理が必要となる。
- ・脅威の源泉に対処し、証拠を集めることにより、容疑者を法廷に立たせる。
- ・脅威に関する注意を喚起するために政府等に助言するとともに、保護セキュリティ対策を含む適切な対応策を助言する。
- ・他の機関、組織及び行政省庁の脅威との戦いを支援する。特に、英国の国家情報機構との共同作業に貢献するとともに、英国及び海外の他の組織とのパートナーシップを構築する。

（1）情報の収集

情報の収集はMI5の業務の中心である。公開情報は背景を理解するためには有効であるものの、国家安全保障に脅威をもたらしている組織や個人の意図と行動を看破する最善の方法は、彼らに関する秘密情報を入手することである。MI5は、時間を掛けて、これらの秘密情報を収集・照合し、そして、対象組織や人物の主要な特徴・基盤・計画・能力に関する詳細な知識を獲得している。

MI5は、多くの手段で情報を入手している。情報入手の主要な技術は次のとおりである。

- ・ 隠密の人的情報源（即ち、エージェント）。“エージェント”とは、調査対象に関する秘密情報を提供する人的資源である。エージェントは MI5 職員ではない。
- ・ 特定監視（調査対象の尾行及び／又は観察等）
- ・ 通信傍受
- ・ 侵害的な監視（家又は車の中での盗聴等）

これらの技術の全ては、2000 年調査権限規制法（ Regulation of Investigatory Powers Act ）に定められた要件に従って運用される。調査権限規制法の取り決めに従うことにより、MI5 は、不必要な官僚主義により妨げられることなく、迅速に調査・捜索を進めることが可能となっている。

1989 年セキュリティ・サービス法は、長官に対し、MI5 内で何時、如何に情報を入手・開示するかを統制する効果的な取り決めを作成・保持する責任を与えている。この統制の主要な側面は、国家安全保障上の真の脅威に対してのみ MI5 が調査・捜査することを保証する内部統制システムである。

情報を収集するために侵害的な技術を使用する際の要点は、最小の侵害で脅威と比例した効果的な手段を取ることである。令状が必要となるような最も侵害的な方法を使用する場合は、内務大臣に次のことが正当であると認められなければならない。

- ・ 必要性：海外の脅威から国の安全を保障するため、英国の経済的利益を守るため、又は重大な犯罪を探知若しくは防止するために必要であること。
- ・ 比例：達成しようとするものとの均衡。即ち、獲得しようとする情報は、調査対象への侵害及び調査対象以外の個人に対する不可避免的な“副次的侵害”を正当化するほど十分に大きいこと。

さらに、獲得しようとする情報がその他の手段では獲得することが合理的に不可能であることが内務大臣に納得されなければならない。これらの重要な基準に明らかに適合した場合のみ内務大臣へ令状の申請が行われる。

（2）情報管理

情報活動は、質の高い保存記録と情報管理システムに依拠する。いくつかの情報は、即座に価値をもつにはあまりに断片的であり、かつ不正確である。しかし、たとえ僅かであっても詳細な情報は重要である。何故ならば、それらから、新しい情報が判断されたり、さらなる調査が開始されたりするからである。情報と記録の管理は、MI5 の中核の業務である。正確な記録は業務にとってきわめて重要である。記録は、MI5 の業務を支える研究及び分析を支援する。記録には、紙及び電子ファイルの両方が含まれる。紙ファイルは依然と重要であるが、電子ファイルとデータも益々重要なものとなっている。したがって、MI5 は電子記録管理システムの整備事業を継続している。

（3）証拠と開示

1990 年代になり、MI5 が対処する脅威の変化と法律の進展により、MI5 は犯

罪司法プロセスに関わることが増大した。MI5 の刑事裁判手続きへの係わりの増大は、起訴に繋がる情報調査を計画・実行する際に、証拠に関する法令と開示義務の両方の要件を考慮しなければならないことを意味している。これらの理由により、適切な内部統制と調査権限規制法に基づく法的義務の順守を確実にするとともに、エージェントとの会合、盗聴、搜索・監視工作を含む活動の詳細な記録を保存することが義務づけられている。

MI5 の職員が刑事裁判で検察側の証人となる場合、職員が衝立の後ろに位置することを含めて、法廷において匿名で証言することが認められている。これにより MI5 の職員の身元が暴露しないよう配慮されている。

センシティブな情報を保護するために、時には、記録が弁護側へ開示されないことも必要である。法律は、開示義務とセンシティブな情報を保護する必要性とは調和されなければならないことを認めている。例えば、その情報の開示が国家安全保障などの公的利益の重要な側面を害するなどの場合は開示されない。そのような場合、検察官は裁判官にその資料を開示しない許可を申請することができる。そのような申請は「公益を理由とする秘匿特権」(public interest immunity: PPI) を申請する様式でおこなわれる。「公益を理由とした秘匿特権」(PII) の申請に対する適否の判断は、裁判官がおこなう。

(4) 他機関との協力

MI5 は、英国及び海外の様々な組織と緊密に連携している。このパートナーシップのネットワークは MI5 の業務の基盤である。

ア. 英国の行政省庁

MI5 はとりわけ、内務省と緊密に協力するとともに外務省、内閣府、北アイルランド省、貿易産業省及び国防省とも強い繋がりを有している。

イ. 英国の情報機関（英国の国家情報機構：下図参照）

MI5 の業務と他の情報機関との調整は、国家情報機構を通じて行われる。英国の国家情報機構 (intelligence machinery) は、内閣府の中央情報機構 (central intelligence machinery based in the Cabinet Office)、MI6、政府通信本部 (GCHQ)、MI5、国防情報局 (DIS) 及び統合テロリズム分析センター(JTAC) で構成される。

首相は情報の問題に関して全般的な責任を有するとともに、情報機関全体に共通する問題に関し国会に報告する責任を有する。内務大臣は MI5 に対する責任を有し、外務大臣は MI6 と政府通信本部 (GCHQ)、そして国防大臣は国防情報局 (DIS) に対する責任を有する。

内閣府の中央情報機構は、関係省庁間で合意された要求事項と優先事項に従って、三機関に任務付与するとともに、資金支出と活動の監視に責任を有す。内閣府情報担当事務次官 (Permanent Secretary, Intelligence, Security and Resilience) は、中央情報機構を統括する。また、同事務次官は、単一情報会計

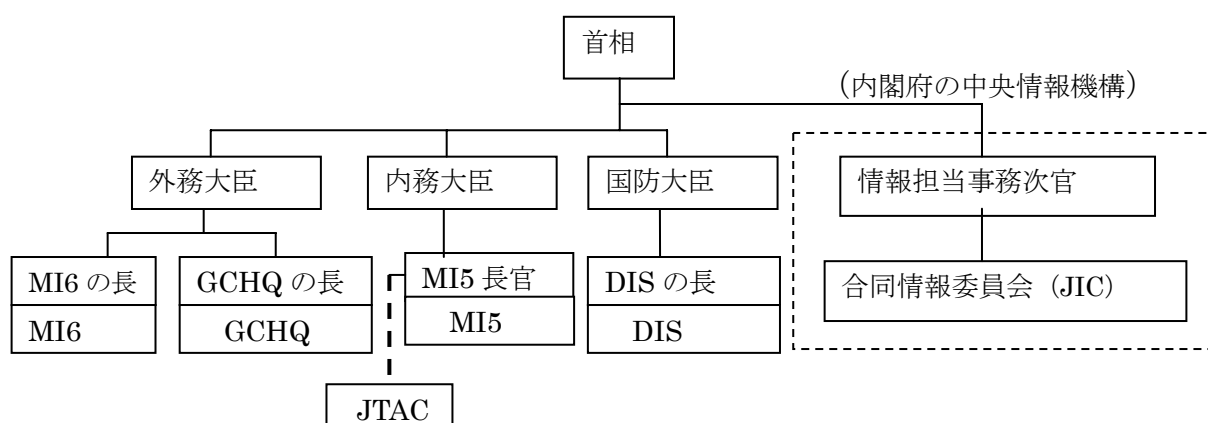
(SIA)の首席会計担当官であり、かつ合同情報委員会(JIC)の議長である。合同情報委員会(JIC)は、三機関の長並びに国防情報局(DIS)、外務省、貿易産業省、内務省及び財務省等の上級代表で構成される省庁間機構であり、毎年、情報コミュニティ業務の要求事項と優先事項を設定するとともに、その活動実績を評価する。

MI6の主要な役割は、セキュリティ、国防、重大犯罪並びに外交及び経済政策の分野における英国の最重要な利益に影響する問題に関する外国の秘密情報を収集することである。

政府通信本部(GCHQ)は、通信傍受による情報収集(シギントとして知られている)と情報保証(Information Assurance)に関するサービスと助言の提供を主要な任務としている。

国防情報局(DIS)の主要な役割は、①政策、国際公約及び軍隊の派遣に関する意思決定、②防衛調達決定及び③軍事作戦を直接支援するために、情報プロダクト・評価・助言を国防省に対し適時に提供することである。

英国の国家情報機構



ウ. 英国の法執行機関及び軍隊

MI5は、英国の56の警察機関、重大組織犯罪庁(SOCA)、及び歳入税関局(HM Revenue and Customs)などの法執行機関と強い関係を有している。MI5は、警察から多くの分野で支援を受けているが、一方、彼らに現在の脅威に関する情報と評価を提供するとともに刑事訴訟手続きに結びつく捜査について彼らと緊密に協力している。また、広範なセキュリティ問題について軍と協力している。

エ. 海外の情報・セキュリティ機関

MI5は、英国及び海外の双方で国の安全を保障する責任を担っている。主要な関心は国内であるが、国家安全保障の概念は英国以遠に広がっている。このため、MI5は、海外における英国の利益を守るために、世界中で100を越える機関と連

携している。

5. 統治（ガバナンス）

民主主義の社会で情報機関がその活動を阻害されることなく、かつ出来る限りの透明性を確保するためには、情報機関が法律により規制され、かつ厳しい監視の対象になることは極めて重要である。MI5 はこれらの要件を満足する明確に定義された統治の枠組みの中で活動する。

（1）活動の法的枠組み

MI5 の業務は、過去 20 年に亘り制定された複雑な法的枠組みにより統治されている。次の 5 つの主要な法律が MI5 の活動の根拠となる法的枠組みである。

- ・ 1989 年セキュリティ・サービス法（Security Service Act 1989）
- ・ 2000 年テロリズム法（Terrorism Act 2000）
- ・ 2001 年対テロリズム、犯罪及びセキュリティ法（Anti-Terrorism, Crime and Security Act 2001）
- ・ 2005 年テロリズム防止法（Prevention of Terrorism Act 2005）
- ・ 2006 年テロリズム法（Terrorism Act 2006）

以下上記の法律について簡単な説明を加える。

1989 年セキュリティ・サービス法には MI5 の役割と責任が定められており、これにより MI5 は、はじめて法的基盤を得ることとなった。

2000 年テロリズム法は、これ以前の対テロリストの法律を改正・拡大し、より恒久的なものとなった。これ以前の法律は、北アイルランドに関連したテロリズムを対象としていたが、本法により、その法令措置は全ての形態のテロリズムに適用できるようになった。

2001 年対テロリズム、犯罪及びセキュリティ法は、2001 年 9 月 11 日の米国の同時多発テロを受けて 2001 年 12 月に成立した。同法には、テロリズムに直接又は間接に係わる脅威に対処する権限をより効果的にする様々な対策が含まれている。主要な規定は次のとおりである。

- ・ テロリストの資金
 - ①テロリスト組織/個人が英国又は英国人に脅威をもたらした場合の彼らの資産を凍結する警察権力、②金融機関の開示義務の強化と外貨交換所の監視強化対策
- ・ 情報へのアクセス
 - ①歳入税関局が情報を情報機関及び法執行機関に開示するのを認める条項、②輸送業者が保有する情報（乗客及び貨物データ）へのアクセスの改善、③通信データの保存に関する実施基準
- ・ 航空機、化学・生物・核セキュリティ
 - ①セキュリティ上の理由で航空機を抑留し、乗客を検査するための権限に関する広範な条項、②有害な物質に関連する悪戯に関する新しい犯罪と危険な病原菌を保管している研究所に関するより厳しい規制、③民間原子力産業の

セキュリティ

- ・移民条項

このセクションは 2005 年テロリズム防止法により取って代わられた。

- ・警察権

①警察権の範囲、例えば、変装を見破ることを含む身元確認するための撮影、
捜索、検査する権限、②英国空港警察と軍警察などの裁判管轄権の明確化

2005 年テロリズム防止法は、2001 年対テロリズム、犯罪及びセキュリティ法のセクション 4 に取って代わるものである。同法は、英国人であろうと外国人であろうと、テロリスト容疑者に対して監督命令 (Control Orders) を出す権限を内務大臣に与えている。監督命令には、携帯電話又はインターネット使用の禁止、移動と旅行の制限、名前をあげられた個人との交際の制限及び外出禁止を監視する追跡タグの使用などの様々な条件が含まれる。

2006 年テロリズム法では、過激派の書籍やインターネットを通じてテロリズムを称賛したりすること、テロリスト出版物を配布すること、テロリスト行為を準備又は実行を計画すること、他の者がそうすることを支援すること及びテロリズム訓練を与えたり若しくは受けたり又はテロリスト訓練キャンプに参加することを刑事犯罪とした。

(2) 監視システム

MI5 の業務は常に監視の対象である。これは、MI5 が法律の範囲内で活動し、その活動が目的に比例しかつ必要性に基づくものであり、正しい作業優先順位を保有し、そして、資源を最善に使用することを保証するためのものである。MI5 の業務は閣僚による監視、議会による監視及び司法による監視の 3 つの方法で監視される。

MI5 に対する監視メカニズムは、次の 3 つの主要な法律から生じる。

- ・ 1996 年の改正 1989 年セキュリティ・サービス法 (Security Service Act 1989 as amended in 1996)
- ・ 1994 年情報サービス法 (Intelligence Services Act 1994)
- ・ 2000 年調査権限規制法 (Regulation of Investigatory Powers Act 2000)

ア. 閣僚による監視

1996 年制定された改正 1989 年セキュリティ・サービス法によって MI5 は、国務大臣、実際には MI5 のために国会で答弁する内務大臣の権限の下に置かれている。また、本法は、MI5 が如何なる政党の利益のためにも行動しないことを確実にするための長官の責任を定めている。

また、法的根拠はないが、MI5 をはじめとし情報機関の政策を常時チェックするために、内閣に「情報に関する閣僚委員会」(Ministerial Committee on the Intelligence Services : CSI) が設置されている。メンバーは首相 (議長)、副首相、内務大臣、外務大臣、国防大臣及び財務大臣である。同様に、これら閣僚を補佐するとともに、情報機関の支出と活動を監視するために、情報担当事務次官

を議長とする「情報に関する事務次官委員会」(Permanent Secretaries' Committee on the Intelligence Services : PSIS)が設置されている。

イ. 議会による監視

三機関(MI5、MI6、及び政府通信本部(GCHQ))に対する議会による監視は、1994年情報サービス法で創設された情報委員会(Intelligence and Security Committee : ISC)が行う。同委員会は、首相によって指名される超党派の9名の議員で構成される。同委員会に付託された権限は、三機関の支出、管理、及び政策を調査することである。加えて、同委員会には、政府の合意に基づき、国防情報局(DIS)や合同情報委員会(JIC)の活動を調査する権限が与えられている。

ウ. 司法による監視

(ア) コミッショナー

三機関は、2000年調査権限規制法に基づき任命された「情報サービスコミッショナー」(Commissioner for the Intelligence Services)と「通信傍受コミッショナー」(Commissioner for Interception)の二人のコミッショナーによって監視される。情報サービスコミッショナーは、三機関及び国防省の行う工作のために関連する国務大臣が発行する令状・許可の発行・付与状況、すなわち、情報サービス法に基づく令状の発行状況並びに調査権限規制法に基づく監視及びエージェントに関する令状・許可の発行・付与状況を調査する。通信傍受コミッショナーは、三機関、国防省及び法執行機関の行う封書の開封、通信の傍受並びに通信データの取得に関する令状・許可の発行・付与状況及びその活動などを調査する。

各コミッショナーは、彼らにより詳細に調査したいあらゆるケースについて意見聴取するために各機関や関連する省庁を訪問することができる。また、法律によって、彼らが必要とする如何なる文書及び情報へのアクセス権が与えられている。各コミッショナーは、各報告年の最後に首相に報告書を提出しなければならない。これらの報告書は、国会に提出された後に公表される。

(イ) 調査権限審判所 (Investigatory Powers Tribunal)

調査権限審判所は、三機関が行った行為又は通信の傍受に関する個人からの訴えを調査するために2000年調査権限規制法に基づき創設された。調査権限審判所は、1998年人権法に基づく訴えを調査し、訴訟を審問する。

国籍に関係なく、誰でもが、彼らの通信又は人権を、三機関のいずれかの機関によって侵害又は迫害されたと信じたならば訴えることができる。審判所は、それぞれの訴えを調査し、三機関が不適切に行動したかどうかを調査する。もし、審判所が原告の訴えを支持するならば、審判所は、原告に対する損害賠償などの適当な救済処置を命ずる権限を有する。

おわりに

元 MI5 職員のピーターライトは、1987 年に MI5 の内情を暴露した著書『スパイキャッチャー』を発表した。その中で、彼は、1974 年に、MI5 の 30 人以上が当時のハロルド・ウイルソン政権の転覆を企てたと述べている。また、彼は、1960 年代に MI5 の長官であったロジャー・ホリスがロシアのスパイであったという疑惑を述べている。その後の政府の調査で、それらの陰謀や疑惑は存在しなかったとされているが、1989 年セキュリティ・サービス法や 2000 年調査権限規制法の制定は、『スパイキャッチャー』で投げかけられた問題に対する回答であったのだろう。

長く情報調査室長を勤められた大森義男氏はその著書『日本のインテリジェンス機関』で、「インテリジェンスは毒である。中略。しかし、これは社会の安全を守るために必要な「毒」である。それを容認する以上、①「毒」を用いるには高度のエキスパートズ(専門技能)が必要である。毒は一匙でなくてはならない。②「毒」を解毒する社会的装置を備えなくてはならない。民主主義の枠内に毒を使いこなすシステムを構築する工夫である。」と述べている。

本稿で述べた英国の情報・セキュリティ機関を統治する法的枠組みや監視システムは、民主主義の枠内で毒を使いこなすシステムであろう。英国の監視システムの法的根拠は 1989 年セキュリティ・サービス法、1994 年情報サービス法及び 2000 年調査権限規制法の 3 つである。1989 年セキュリティ・サービス法は、MI5 を内務大臣の支配化におくこと及び長官の政治的中立義務を定めている。1994 年情報サービス法は議会の情報委員会 (ISC) を創設し、2000 年調査権限規制法は、二人のコミッショナーと調査権限審判所を創設した。そして、これらが、国家情報機構に対する監視システムの必須の要素となっている。

以上の各制度は、我が国のカウンターインテリジェンス体制の構築の際に参考になる事項であろう。

IAQG（国際航空宇宙品質グループ）について

主任研究員 伴野 道彦

1. はじめに

防衛調達基盤整備協会（BSK）システム審査センターは、品質マネジメントシステム、環境マネジメントシステム及び情報セキュリティマネジメントシステムの認証機関として活動しているが、BSKの認証の半数以上を占める航空宇宙品質マネジメントシステム規格（IAQG 9100/JIS Q 9100）は、他の品質マネジメントシステム規格（ISO 9001/JIS Q 9001）、環境マネジメントシステム規格（ISO 14001/JIS Q 14001）及び情報セキュリティマネジメントシステム規格（ISO/IEC 27001/JIS Q 27001）と異なり、ISO規格ではないセクター規格（IAQG 9100）である。

このセクター規格を制定し管理しているのは、国際航空宇宙品質グループ（以下、IAQGという）であり、我が国では航空宇宙品質センター（以下、JAQGという）がIAQG活動に対応する活動を担っている。

本研究では、IAQG/JAQGについて概要を説明するとともに、IAQG活動と認証機関であるBSKシステム審査センターの係わりについて述べるものとする。

2. 国際航空宇宙品質グループ（IAQG: International Aerospace Quality Group）

航空宇宙産業では、1994年から始まった米軍の調達改革によりMIL規格体系の見直しが行われ、その結果、品質システム規格MIL-Q-9858Aも廃止され、代替規格としてISO 9001が使われるようになった。ボーイング、エアバス等の主要契約者（プライムメーカ）はそれぞれISO 9001を補う事項を供給者（サプライヤ）に要求していたが、これらを共通の要求事項として統一し、ISO 9001の要求事項に追加する必要が生じてきた。

このため、1998年に世界の主要な航空宇宙関係企業が、互いの信頼に基づいて強力な協力体制を構築・維持することにより、価値創造の流れの全段階において品質の著しい改善とコストの削減を実現する活動を推進するために、IAQGを設立し、品質の向上とコストダウンを目的とする航空宇宙品質マネジメントシステムの国際統一規格（以下、9100QMSという）を制定した。

IAQGの活動目標は、「航空宇宙及び防衛の分野における品質システムの共通化を図る」、「継続的な品質改善プロセスを確立する」、「航空宇宙及び防衛産業におけるベストプラクティスを共有する方法を確立する」及び「各国政府、規制当局及びその他利害関係者との連携を取る」というものであり、世界の主要な航空機メーカーと航空エンジンメーカーのほとんどが参加している。

IAQGは南北アメリカ、ヨーロッパ及びアジア太平洋の3セクターに分かれて活動している。南北アメリカセクターはAAQG（Americas Aerospace Quality Group）と言い、米国輸送機技術協会（SAE: Society of Automotive Engineers）が事務局を担当し、ヨーロッパセクターはEAQG（European Aerospace Quality Group）と言い、欧州航空宇宙防衛産業連合（ASD: Aero Space and Defense Industries Association of Europe, 旧AECMA: European Association of Aerospace Industries）が事務局を担当している。日本が参加するアジア太平

洋セクターは APAQG (Asia Pacific Aerospace Quality Group) と言い、2002 年 7 月に、日本、韓国、中国、台湾、オーストラリアの各国企業により設立され、日本航空宇宙工業会 (SJAC: Society of Japan Aerospace Companies) が事務局を担当している。

9100 QMS 審査登録制度はこれまでにスキームが完成し、成熟段階に入った。このため IAQG 設立の当初の目的である品質向上とコスト削減をさらに追求すべく、新しい戦略目標を設定し広範な活動を展開しているが、それらの活動計画は IAQG 評議会 (IAQG Council Meeting) で審議と決定がなされ、IAQG 総会 (General Assembly) にて関係者に発表される。

IAQG 評議会は、3 セクターを統括し活動全般の方針事項や活動目標を設定するものであるが、IAQG 総会 (General Assembly) は、IAQG の諸活動を全世界の航空宇宙業界に周知徹底するとともに業界全体のコミュニケーションをはかるもので、共に毎年 4 月と 10 月に各セクター持ち回りで開催される IAQG 会議の主要行事である。

3. 航空宇宙品質センター (JAQG : Japan Aerospace Quality Group)

JAQG は、日本の航空宇宙関連企業が IAQG 活動に対応すべく品質に関する国際統一規格の普及、国際認定制度の確立などの品質改善とコスト削減を目的に、2001 年社団法人日本航空宇宙工業会 (以下、SJAC という) 内に設置された組織である。JAQG の活動目標は、「IAQG 活動に参画し、日本の要求を盛りこんだものとする。」、「国際品質規格を関係官庁、諸機関と調整し、日本国内への普及を図る。」、「JIS Q 9100 に対応する航空宇宙審査登録制度を確立し、運用を監督する。」及び「APAQG との連携を図る。」というもので、航空宇宙関連の国内企業および関係機関が JAQG メンバーとして活動に参加しており、参加企業数は 152 社 (2008. 7. 8 現在) に上っている。

JAQG は、運営委員会、幹事会、ワーキンググループ (以下、WG という)、航空宇宙審査登録管理委員会 (JRMC : Japan Registration Management Committee) 及び事務局で構成され、主に JAQG メンバーから集めた会費により運営されている。

航空宇宙審査登録管理委員会 (以下、JRMC という) は JIS Q 9100 認証制度の運営を行うもので、JAQG 幹事会代表メンバー 3 名以上で構成されるが、必要に応じ、後述の関係機関に出席を求め、助言を受ける仕組みを有している。

4. 関係機関と IAQG/JAQG との係わり

航空宇宙品質マネジメントシステムの認証制度を担う関係機関は、認定機関 (JAB)、認証 (審査登録) 機関 (CB)、審査員認証機関 (JRCA) および研修提供者 (TP) からなるが、JAQG の活動に於いては、これら関係機関は運営委員会にて発言権を有するのみでなく、JRMC の主催する拡大 JRMC 会議に参加し、個別の課題について意見交換や討議を実施し、JAQG 幹事会や各種ワーキンググループの活動を支援している。

一方、IAQG の活動に於いて、各セクターの関係機関は IAQG 会議に際して IAQG 評議会への参加権や投票権は無いものの、国際統一規格の制定/改訂や国際認定

制度のスキーム維持を担う、OPMT (Other Party Management Team) 等の WG の活動に積極的に参加し、各セクターの立場で闊達に意見を述べている。

しかしながら、アジア太平洋セクターからの関係機関の参画は、認定機関のみにとどまり、日本の認証機関の代表者が IAQG 会議に参加することはまったく無かった。

本年 10 月に横浜で開催された IAQG 横浜会議は、地元での開催と言うこともあり、WG の中核である OPMT 会議に BSK 及びロイドレジスタークオリティアシュアランスリミテッド(LRQA) から代表者が参加するとともに、これまで空席であったアジア太平洋セクターの認証機関の代表者に BSK の伴野が指名され、今後の活動のフォーカルとして期待されている。

5. おわりに

航空宇宙品質マネジメントシステム (AS/EN/JIS Q 9100) の認証を取得し IAQG-OASIS データベースに登録された企業はこれまでに約 9,000 事業所を超えている。それらの企業は、IAQG 活動を通して、国際標準化による品質向上とコスト削減の効果がますます増加するとともに、世界規模でのビジネスチャンスを獲得する絶好の機会を世界の航空宇宙関連企業に提供している。

また、航空宇宙品質マネジメントシステム規格は民間航空宇宙企業のための規格に留まらず、各国の航空局、宇宙関連機関、更には防衛関連機関にも認知されつつあり、今後更に航空宇宙産業全体のグローバルスタンダードとしての地位を築きつつある。

JAQG の活動は、幹事会社 9 社が中心となり、日本国内の航空宇宙関連企業約 150 社の会費により運営されているが、各種活動の多様化が進み、また国際的な場での日本の重要度が高まってきている。JAQG 活動を今後も円滑に進めるには更に多くの企業の参画を得ていくと共に、認証審査の実務に詳しい関係機関、とりわけ実際の審査を担当する認証機関の積極的な参画と幹事会社に対する支援活動が必要である。そのため、我が国における航空宇宙品質マネジメントシステムの認証の半分以上を担っている BSK システム審査センターの果すべき役割が注目されている。

現役時代を振り返って思うこと（その2）

主任研究員 草地八寿郎

昭和40年代後半当時の調達実施本部に入庁した時、一新人にとってそこは古い伝統のある仰ぎ見るような組織と思われた。しかし今から思えば創立20年に満たない若い組織であり、その後退職するまでに勤務した30数年の方が遥かに長い期間となった。その間における予定価格算定基準に関する訓令の変遷については、第一巻第三号で述べたとおりであるが、では訓令は理論的により優れたものになったかということ決してそうとは言い切れない。自然科学の分野でこの間の進歩は何世紀分かにも相当することを認めない訳にはいかないが、原価計算、特に予定価格算定のための訓令といえは言葉は悪いが結構片務的なところがある。国の契約といっても戦時はともかく平和時における契約は双務的になされることであることから、理論的に理屈の通っている色々な見方、考え方の中で、時代の要請にも適い、またパブリックコメントと言うかどうかは別にして業界の意見も採り入れられたものでなければならぬ。決して最新の会計理論の研究成果を反映したというものではなく、むしろ色々出尽くされている多数のオプションから取捨選択されていると言える。この間に種々の研究、試みがなされているが、それがある収束点に向かっていくというようには思われない。

この間に著しい発展があったのはIT技術がもたらした事務の効率化である。入庁当時はワープロが使われ始めた頃であったが、業務といえば手書きが中心であり、正式文書ではタイプライターが用いられていた。程なくワープロはパソコンに代わり、予定価格作成等をそれで作成する職員も出始めてきた。パソコンを用いるのも当初はタイプ代わりに字を綺麗にするくらいと思われ、そのために膨大な資料を打ち込むことは趣味の世界でありこそすれ、大きな無駄としか思われなかった。ところがいったん打ち込んでしまえば後の作業が大変楽になる。またインターネットを用いて市況の状況等もたやすく入手できるようになる。後日、わが身の不明を恥じる他なかった。

入庁当時、女性職員で原価計算を担当している人は皆無であった。現在では全体的に女性職員の比率が高くなっていると思われるが、原価計算に当たる女性職員の数は格段に増えた。これも小生が某課に在任中、原価計算に女性を起用し始めたのがほぼ最初だったような記憶があり、これらのことが現在に繋がっていることは感慨深い。彼女達は期待を裏切らず多大の貢献をしている。

防衛関連企業に求められている総合的情報保全体制の重層的構築について

研究員 榊 勝

1 保全を必要とする技術情報巡廻の現状と問題点について

現在、防衛省と防衛関連企業との中央調達及び地方調達における装備品等の契約において、甲・防衛省から乙・防衛企業に対して、貸付品等として各種多様な電子・ハードコピーの技術情報が移管され、それらに基づいて作成、製作された各種多様な電子・ハードコピーの技術情報の提出書類及び納入品が乙・防衛企業から甲・防衛省に移管されている。

更に、以降の契約において、その提出書類及び納入品が新たな契約相手企業に渡されて、新たな提出書類及び納入品として納入され、膨大な技術情報が巡回している。

このような現状において、各自衛隊等の要求に基く個々の契約において、契約基本条項及び特約条項に基づき、防衛企業に対して技術情報の保全措置を要求し、その実施状況を防衛省が確認するという制度が構築されている。

しかしながら、巡回している膨大な技術情報の中から保全を必要とする技術情報が各自衛隊等の要求元からの的確に指定され、当該要求内容が適切に仕様書に盛り込まれ、当該仕様書の内容が的確に契約書に盛り込まれて契約相手方に伝わっているか等、全体的実施状況を監査し、問題点及び改善点を是正して当該制度を充実させていくという体制にはなっておらず、制度とその運用が乖離している部分が発生してきている。ましてや、契約相手方において、各自衛隊等の要求元への提出書類の作成並びに納入品の製造される過程で生成された各種多様な技術情報の把握は困難な状況にある。

このような状況において、防衛企業としては、契約上、保全を必要とする技術情報が何なのか契約担当官等、特に各自衛隊等の要求元と確認するということが最も重要なことになる。その理由としては、保全を必要とする技術情報を明確にしておかないと、情報セキュリティ構築が焦点の定まらないものとなり、情報漏洩のリスクを増大させるものとなる。仮に、不幸にして情報漏洩事件が発生した場合、漏洩した情報が甲・防衛省にとって保護情報でなくても、企業に対して幅広い、より深い再発防止策を求めてくることから、先ずは、契約上、保全を必要とする技術情報が何なのかを明確にしておくことが最も重要なことである。

2 防衛企業に求められている情報保全体制の総合的スキームについて

現在、防衛省が防衛企業に要求している最も保全レベルの高い情報保全施策は、防衛省秘、防衛秘密及び特別防衛秘密の特約条項(以下「秘密保全特約条項」という。)に基づく秘密保全体制であり、防衛企業が秘密保全規則及び秘密保全実施要領を作

成しそれを防衛省が確認し、秘文書等を保管する保全施設を整備しそれを防衛省が確認し、秘密取扱従事者を届出し、当該秘密取扱従事者に対する保全教育実施計画とその実施状況を届出させて確認している。運用面においても防衛企業に秘密保全状況の点検をさせてた上で、防衛省の保全検査官が保全検査するという従来からのスキームになっている。

平成19年度に、各秘密保全特約条項を補足する「装備品等の調達に係る秘密保全対策ガイドライン」が新たに創設され、それに基づき、防衛企業が秘密保全規則の他に「秘密保全実施要領」を作成し、それを防衛省が確認するという重層的なスキームが構築された。装備品等の調達に係る秘密保全対策ガイドラインにおける情報保全の要求事項としては、秘密保全事項と情報セキュリティ事項からなっており、情報セキュリティ事項のウエートが高くなっているように思われる。

また、日米間における技術資料等の取扱いについては、装備品の購入、ライセンス生産、共同研究開発までにいたる日米了解事項覚書(MOU)の締結に基づく、日米了解事項覚書に関する特約条項により、当該防衛企業に必要な保全措置を講じさせ、その管理規程を作成させて、防衛省の確認を受けるという体制をとっており、秘密の技術資料等も対象となっている。

一方、平成19年8月、秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定(GSOMIA)、いわゆる軍事情報包括協定が締結された。この協定は、我が国の国内法令の範囲内で実施可能な行政取極めであることから、日米両政府によりとられる主な措置の一つの「契約企業に関する政府の措置」に基づいて防衛省の秘密保全特約条項も改正されましたが、その内容としては、「送達」及び「秘密の表示等」の措置であり、従来からの秘密保全措置と同様なものとなっている。

このように防衛企業に求められている秘密保全体制は、複雑に組み合わされて、かつ、重層的になつてきている。

次に保全レベルの高い保護情報については、防衛企業は、情報セキュリティの確保に関する特約条項に基づき、防衛省が定める情報セキュリティ基本方針及び基準に適合した当該防衛企業の情報セキュリティ基本方針、基準及び実施手順を作成しそれを防衛省が確認し、そのとおり実施しているか防衛省の情報セキュリティ監査官が監査するというスキームになっている。

同様なスキームとして、武器等の技術資料の管理に関する特約条項においては、当該防衛企業に必要な保全措置を講じさせ、その管理規程を作成させて、甲・防衛省の確認を受け、実際にその管理規程どおり管理しているか、一般監督の一環として監督官がチェックしている。この特約条項は、昭和54年に制定されたもので現在の情報セキュリティ特約条項の先駆けみたいなものであることから、その管理規程は、どちらかという秘密保全規則に近く、電子情報に関する保全策については、十分でない感がする。

しかしながら、一部の自衛隊等の要求元においては、情報セキュリティ特約条項が制定されても、以前として、武器等の技術資料の管理に関する特約条項を要求

してきている。どちらの特約条項が技術資料の情報保全上、適切か早急に検証する必要がある。

3 防衛企業に求められている重層的な情報保全の対応について

現在、防衛企業においては、前述した秘密保全及び情報セキュリティの確保に加えて、監督・完成検査において、防衛省からの設計書、各種データ等の貸付品について、適切な管理が要求されており、その管理状況は監督官がチェックすることになっている。このように、一つの防衛企業が防衛省との契約において保有している保全すべき技術情報について、それぞれの特約条項及び仕様書において要求されている保全管理体制を構築し、保全検査官、情報セキュリティ監査官、又は監督官の検査・監査を受けるという重層的な対応が求められている。

これらの情報保全体制は、個々の契約の特約条項及び仕様書に基づき、防衛省から防衛企業に移管される秘密・保護情報に対する保全管理策の構築であり極めて限定的である。しかしながら、当該秘密・保護情報以外の関連情報の漏洩事件が発生した場合は、適用範囲を拡大した再発防止策の策定及び展開が求められ、防衛省の監査を受けるという契約範囲を超えて、適用範囲と対象情報が拡大するという事例も見受けられる。

4 情報セキュリティマネジメントシステム認証取得の位置付けと各種情報保全体制との整合性について

企業は、置かれた社会経済的環境の中で所定の事業活動を行っており、その活動を効果的に進め、また継続的に改善していくためには、一定の方針のもとで目的・目標を定め、その目的・目標を達成していくマネジメントシステムを構築して対応している。

そのマネジメントシステムの一部として、その企業の事業活動で直面するリスクに対応する情報セキュリティマネジメントシステム(以下「ISMS」という。)には程度に差があるものの構築せざるを得ないし、その企業が存続する限り継続せざるを得ないものである。その一つの対応策として、近年、品質マネジメントシステム、環境マネジメントシステムに次いで ISMS 認証取得の企業が多くなってきている。

ISMS 認証取得は、国際規格 ISO/IEC27001:2005 に基づいたものであり、国際規格の要求事項に合致した ISMS を構築することにより、企業内の情報整備により安全な情報の共有化と業務の効率化を図るとともに、企業の価値、サービス品質の向上と信頼性をアピールし同業他社に対する優位性を確保するものである。

この ISMS の構築は、経営責任者のトップマネジメントに基づき、適用範囲と境界を明確にし、企業全体で企業資産に対するリスクと受容基準を明確にし、その管理策を選択・実行し、ISMS 内部監査をし、その結果等をインプットしたマネジメントレビューを行い、そのアウトプットに基づき経営責任者は経営資源の提供を行い、新たな管理策を選択・実行するという情報セキュリティに関して企

業全体で行うというマネジメントシステムである。

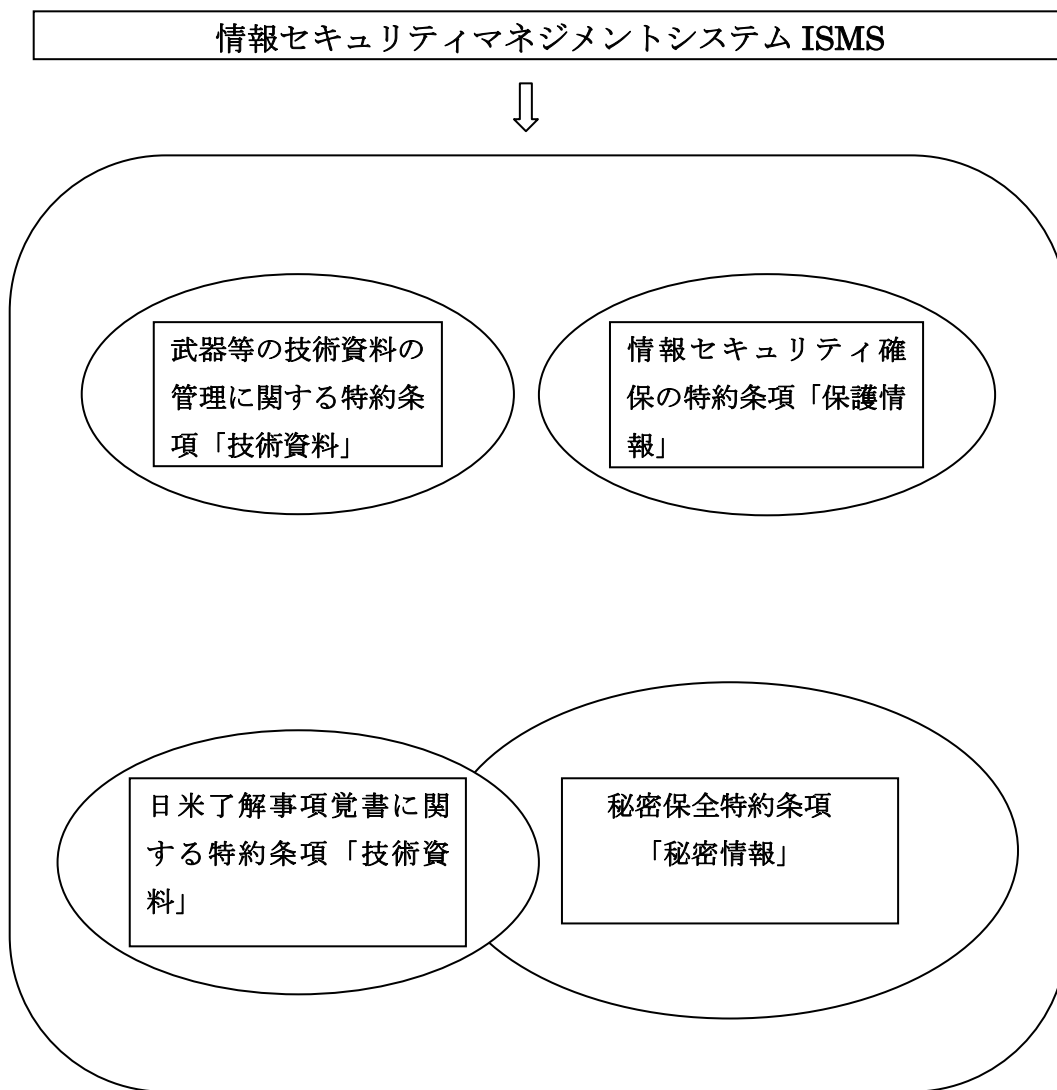
この ISMS の中に、防衛省との契約に基づく各種情報保全体制が、限定的に、総合的に、そして重層的に構築されていることになる。防衛省との契約のウェイトが大きい企業については、限定的ということではないが、いずれにしても ISMS という大きなスキームの中で各種情報保全体制が重層的に構築されていることに変わりはない。

情報保全体制における管理策は、特定の情報を対象として構築され、限定的適用範囲から必要に応じて拡大していき、ISMS と重なり合っていくことになる。このように、ISMS の管理策と情報保全体制における管理策には大差無く、共通する部分が多い。しかし、ISMS という大きなスキームの中の管理策は、ISMS 内部監査によりチェックされ、その結果がマネジメントレビューにインプットされ、そのアウトプットは、マネジメントシステムの流れの中で選定・実施・改善を繰り返して、その企業の ISMS の有効性をグレードアップしていくことになる。

更に、近年、企業の ISMS は、IT サービスマネジメントシステム(ITSMS : ISO /IEC20000-1)や事業継続マネジメントシステム(BCMS : BS25999-2)との整合性を図りながらその有効性を高めてきている。

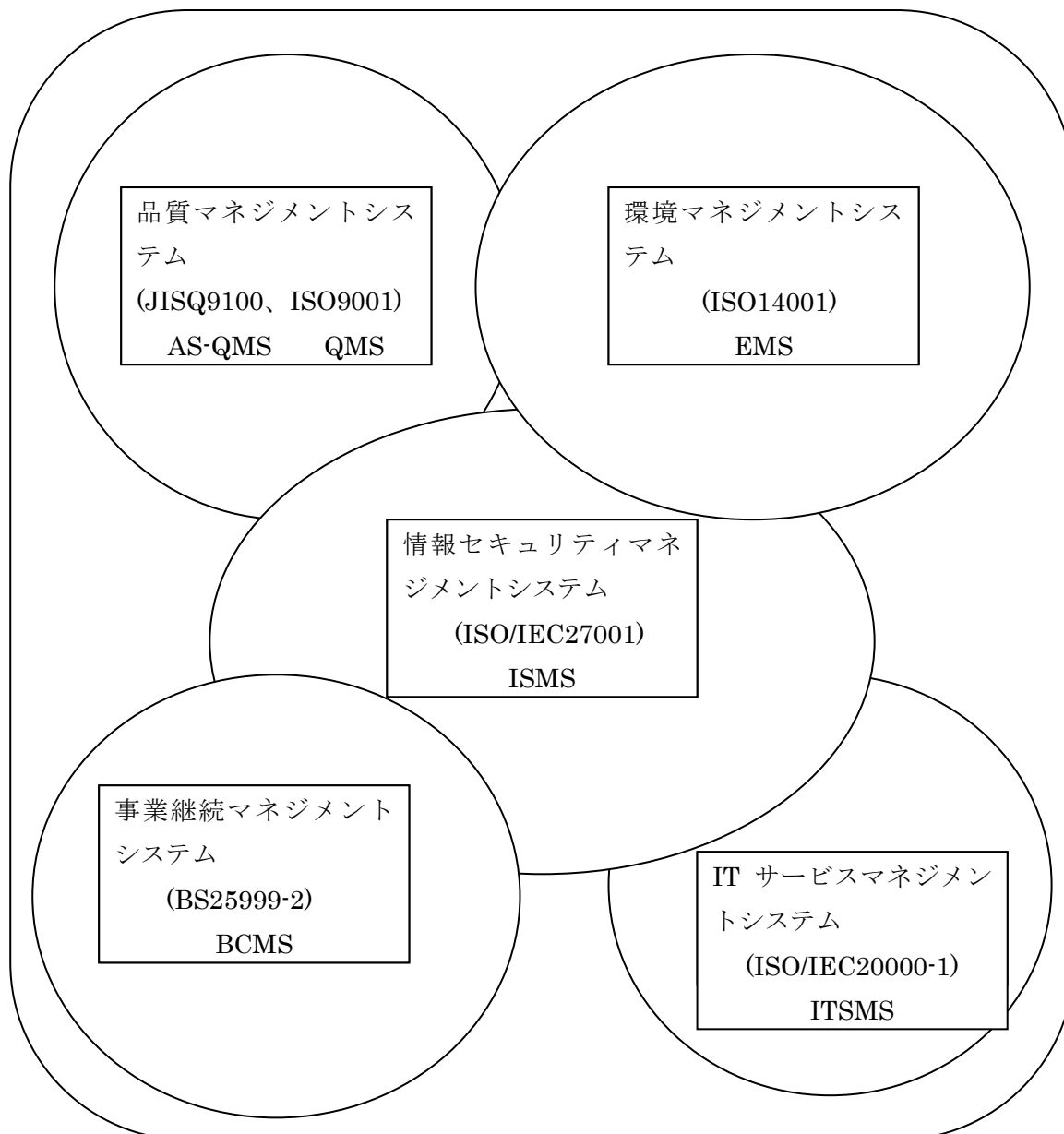
そして、繰り返しになりますが、このように、ISMS は、国際規格の要求事項に合致したものであり、他のマネジメントシステムや防衛省の情報保全体制との整合性を図りながら、安全な情報の共有化と業務の効率化を実現するとともに、企業の価値、サービス品質の向上と信頼性をアピールし同業他社に対する優位性を確保する重要な役割を担っているものである。

[情報セキュリティマネジメントシステムと各種情報保全体制との関係図]



[各種マネジメントシステムの関係図]

MS : 企業のマネジメントシステム



◎ 「防衛取得研究」掲載の署名記事と見方は、いずれも執筆者個人のもので、
(財)防衛調達基盤整備協会ないし執筆者の所属する機関の見方を代表する
ものではありません。

なお、記事の無断転載は禁じます。転載する場合には当協会迄、御連絡下
さい。

発行人 宇田川 新一

編集者 島 健治

発行所 (財)防衛調達基盤整備協会 防衛調達研究センター

TEL 03-3235-0711