防　衛　取　得　研　究　　第六巻　第一号　平成２４年６月

艦艇用燃料の調達について

研究員　白　　井　　均

はじめに

昨年 12 月に映画「連合艦隊司令長官　山本五十六」を観る機会があり、日米開戦の発端となったのが、米、英、蘭の 3 国による対日石油輸出禁止協定であったことを改めて認識した。この協定は、年間石油生産量わずかに 30 万 KL に過ぎない当時の日本にとって国家存亡に関わる大問題であった。資料によれば、海軍は大正 4 年から燃料の備蓄を始め、開戦日（昭和 16 年 12 月 8 日）には、約 650 万 KL の燃料（原油、重油、航空揮発油等）を保有していた。平時における海軍の燃料消費量は年間約 100 万 KL であり、もし戦争に突入すれば、その所要量は平時所要の 4 倍の約 400 万 KL とされていたことから開戦時の備蓄量は、約 1 年半の所要量でしかなかった。これをもって、長官は、「是非やれと言われれば、初めの 1 年や 1 年半は存分に暴れて見せます。しかし、2 年、3 年となれば、責任は持てません。」と発言している。

これは、海軍の戦闘力の第 1 は武器ではなく、行動力であり、この行動力の根元は燃料であるということを示唆している。本稿では、海上自衛隊艦艇の使用する燃料の調達について考えてみたい。

1　海上自衛隊の使用する艦艇用燃料

海上自衛隊（以下「海自」という。）の艦艇は、一部の例外[1]はあるものの、軽油 2 号（艦船用）を使用している。

海自は、1975 年に艦艇の使用する燃料を軽油 2 号（艦船用）に統一した。軽油 2 号（艦船用）の規格は、JIS の軽油 2 号の規格のうち引火点の規定「50℃以上」が「61℃を超えるもの」に変更されたものを防衛省仕様としている。***軽油 2 号（艦船用）***と**軽油 2 号**の比較は表のとおりである。

（表：JIS K 2204-2007 及び*防衛省仕様書*から一部抜粋したものである。）

試　験　項　目	種　　類					
	特 1 号	1 号	**2 号**	***2 号（艦船用）***	3 号	特 3 号
引火点℃	**50 以上**			***61 を超える***	45 以上	
蒸留性状 90%留出温度℃	360 以下		**350 以下**	***360 以下***	330 以下	330 以下
流動点℃	＋5 以下	－2.5 以下	**－7.5 以下**	***－5 以下***	－20 以下	－30 以下
目詰まり点℃	－	－1 以下	**－5 以下**	***-2 以下***	－12 以下	－19 以下
10%残油の残留炭素分%	***0.1 以下***					
セタン指数	50 以上		***45 以上***			
動粘度（30℃）mm²/s	2.7 以上		***2.5 以上***		2.0 以上	1.7 以上
硫黄分%	***0.0050 以下***					
密度（15℃）g/cm³	***0.86 以下***					
備　　考	夏季用		**冬季用**	***艦船用***	寒冷地用	

[1] 2009 年に就役した「そうりゅう型」潜水艦は、ケロシン（灯油）と酸素を使用

このように、軽油 2 号（艦船用）は、軽油 2 号をベースとして、① 引火点、②蒸留性状、③流動点及び④目詰まり点の 4 か所の規定値を変えている。これは、海自艦艇の行動範囲の特性（赤道直下から極地まで）等によるものである。また、軽油 2 号（艦船用）は、JIS 規格にある軽油 2 号の一部に分類できるとされている。

2　艦艇用燃料（軽油 2 号）の調達

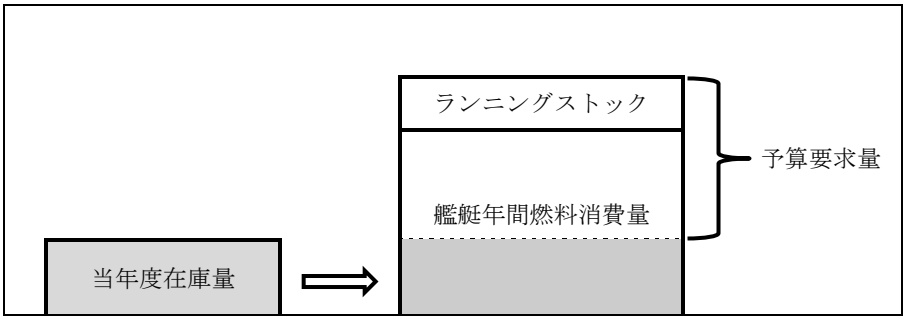
軽油の JIS 規格は流動点の違いにより、特 1 号から特 3 号までに分類されている。また、表の備考欄にあるように、夏季は特 1 号又は 1 号、冬季は 2 号（寒冷地は 3 号、特 3 号）と季節により使い分けるようになっており、季節及び場所に適合した軽油が流通するよう「軽油使用ガイドライン」に細かく決められている。

一方、海自は季節及び場所に関係なく、軽油 2 号（艦船用）（以下「艦艇用燃料」という。）を「特注品」として調達しており、その調達量は国内における軽油販売量の１％に満たないといわれている。

（1）艦艇用燃料の予算要求

予算要求量は、次の年度に艦艇が行動するのに必要な燃料の量を基準に要求することとされている。その「予算要求量」は、極めて大雑把な記述ではあるが、次のとおり表すことができる。

「全艦艇の年間燃料消費量」＋「ランニングストック」－「当年度末在庫量」（下図参照）



（図：次年度の予算要求量関係を表したものである。）

燃料は、すべて歳出予算で調達されるため、当該年度の予算が執行できる 4 月に当年度に使用する燃料を調達する。そのため、4 月当初は契約され、部隊に納入されるまでの間に使用する燃料が不足する。それを補うために、この間に使用する燃料を確保する必要があり、これを「ランニングストック」と呼んでいる。

予算要求は、最終的には予算要求額を要望することになり、次のとおり表すことができる。

「予算要求額」＝「予算要求量」×「燃料単価」

（2）艦艇用燃料の調達

海自は当該年度の所要量を当年度の歳出予算で調達（例：24 年度の所要量は 24 年度の歳出予算で調達する。）し、調達は年間４～５回に分けて実施されている。

調達・納入された艦船用燃料は、海自補給部隊の燃料タンクに保管され、所要に応じて艦艇に供給される。艦艇用燃料を保管する燃料タンクは、海自各艦艇基地の補給部隊に整備されており、そのタンク容量は所要量に比べ十分とはいい難い。そのため、艦艇用燃料は前述のように年間４～５回に分けて調達され、更に、小分けにされ分割納入されているのが現状である。各部隊の燃料タンク容量がその所要量に比べ少ないという要因のほか、燃料受給施設等のインフラ整備が燃料を搭載する海自大型艦艇及び燃料を納入する民間大型タンカー（以後「大型艦船」という。）に対して不十分[2]であることなども分割納入の要因となっている。

原油価格（WTI[3]）は、1982～2003 年にかけて 10～30 ドル／バレルの範囲で比較的安定した数値で推移していた。しかし、2004 年を境として急激な上昇に転じ、2008 年 7 月には、147.27 ドル／バレルの最高値を記録するなど、原油価格の高騰が続いている。当然艦艇用燃料の単価も上昇を続け、成立した予算額（当初予算）だけでは、予算要求量を確保することができず、補正予算により確保しているという不安定な状況が常態化している。これは、予算の成立は予算額（∵「予算額」＝「予算要求量」り「燃料単価」）をもって金額で示されるため、予算が成立し予算執行の段階では、燃料単価が高くなればなるほど、その調達可能量が少なくなるためである。更に、防衛関係費[4]（以下「防衛予算」という。）は、「平成 23 年版防衛白書」によると、2003 年以降減少しており、当初予算のうち人件・糧食費及び歳出化予算が約 80%を占め、これらが一般物件費を圧迫しているという構図を示している。このため、一般物件費のうち約 10%で大きなウェートを占める燃料費（油購入費）の予算額を抑えざるを得ないのも事実であり、これが当初予算だけでは予算要求量を確保できない状況に拍車をかけている。

３　艦艇用燃料調達上の問題点

「燃料受給施設等」及び「調達環境の変化」への対策の遅れは、艦艇の行動力の基本である即応性、機動性、柔軟性、持続性及び多目的性にとって障害となる恐れがある。（今は官民の各担当者による多大の努力でこれを回避しているが・・・）

（１）艦艇用燃料の受給施設等に起因する事項

海自は、所要量に対応した燃料タンクの整備に努めている。しかし、燃料タンクの建設場所等各種制約により、予算の確保は困難を極め、その整備目標を達成していない。また、燃料の納入及び艦艇への搭載に必要な燃料受給施設の整備についても、防衛予算の減少等の制約により、十分な予算が確保できない状況が続いている。このため、大型艦船に整合した燃料タンク及び受給施設整備が十分とはいえず、艦艇用燃料の受給施設等は脆弱であるといわざるを得ない。

---

[2] 受入桟橋周辺の喫水が浅いなどの影響により、大型タンカーが接岸できないなど

[3] ウェスト･テキサス･インターメディエイトの略。テキサス州を中心として産出される原油であり、世界三大指標原油のひとつ。

[4] 防衛関係費は、「人件・糧食費」、「歳出化経費」及び「一般物件費」の三分類に分けられることが多い。

（２）艦艇用燃料の調達環境の変化に起因する事項

一般的な軽油は、「軽油使用ガイドライン」により、季節ごと、また、地域ごとにその流通が決められている。

軽油２号（艦船用）は、軽油２号に区分されるとはいえ、一部の規定値が異なる特注品である。更に、その調達規模が国内軽油販売量の 1%にも満たないという調達環境の下、海自はこの艦艇用燃料を年間通じて安定的、かつ、継続的に調達する必要がある。

艦艇用燃料を調達するための予算の確保は、原油価格の高騰により年々厳しくなっている。ここ数年、艦艇用燃料の調達は当初予算だけでは予算要求量を確保することができず、補正予算等を活用して、どうにかその要求量を確保しているという不安定な現状である。この主たる原因が原油価格の高騰にあるのは当然であるが、人件･糧食費及び歳出化予算が 80%を占める硬直化した当初予算にもその原因がある。一般物件費の約 10%を占める油購入費の歳出予算を削減せざるを得ない問題がそこに内在している。

４　調達上の問題点解決の検討及び提案

（１）方策の検討

ア　年間を通じた燃料の寄託保管

整備目標を達成するため燃料タンク及び受給施設の整備を早急に実施する必要がある。

しかし、①防衛予算が減少傾向にあること。②危険物貯蔵施設である燃料タンク及び同関連施設の新設・拡大整備には整備場所に制限があること。など、その整備は多方面に影響を及ぼす諸問題を抱えており、整備目標に沿った計画的な整備は極めて困難な状況である。そのため、既存の施設を利用する方策を検討してみる。

石油業界は、国内における石油製品の需要減少に伴い、関連施設の廃棄を促進している。石油会社等の保有する燃料施設に艦艇用燃料を寄託保管できれば、海自は必要最小限の燃料関連施設を維持・整備するだけで所要量の保管が可能となる。

寄託保管の方式は、混蔵寄託契約[5]とし、石油会社等が他の民間企業への売却用軽油との混蔵保管を許可する。艦艇用燃料である軽油 2 号（艦船用）は、その規格から一般軽油の夏季・冬季用を満たすことは可能であり、石油会社等は、多大なコストをかけることなく寄託保管を行うことができるとともに、施設の有効利用も図ることができる。更に、寄託保管契約の実施により、海自全体での燃料保管可能量が増加し、地政学的リスクに対し敏感に反応する原油価格の推移を考慮した調達（安い時に調達するなど経費の削減にもつながる。）が可能となる。ま

[5] 受寄者が複数の寄託者から物の預託を受ける場合、その物を他の同種類・同質の受寄物と混合して保管し、その返還に当たっては各寄託者に対しその寄託額と同数量の物を返還することができるとする特約のある寄託契約のこと。

た、寄託保管された燃料は不測の事態（有事）においては、艦艇へ迅速な供給をすることが可能となり、艦艇の特徴である即応性等の維持・向上にも寄与できる。

イ　備蓄用燃料として国庫債務負担行為（国債）による燃料の予算要求

東日本大震災の教訓から備蓄用燃料の保有が、部隊の迅速かつ継続的な行動に如何に必要かが認識された。

寄託保管する艦艇用燃料を6か月分とし、これを「ランニングストック」に置き換え、有事対応の「備蓄用燃料」とする。

しかし、備蓄用燃料を6か月分確保するためには、予算所要量が従来の約1.5倍となり、更なる歳出が必要となる。この対策として、備蓄用燃料は3年計画で要求・調達することとして、その経費を歳出ではなく国債とする。これにより、次年度の予算要求は、

「全艦艇の年間燃料消費量」＋「備蓄用燃料（2か月分）」－「当年度末在庫量」となる。（備蓄用燃料（2か月分）の経費は歳出でなく国債を活用）

また、次年度、次々年度、次々々年度（3年間）までは、同式によるが、4年度目以降は

「全艦艇の年間燃料消費量」－「当年度末在庫量」

となり、予算要求量が減少する。（ただし、備蓄用燃料が何等かの理由により不足する場合には、不足する備蓄用燃料を要求する。）

（2）提　案

前項の結果から、以下の2点について提案したい。

ア　混蔵寄託契約により備蓄用燃料を石油会社等に寄託保管する。

イ　備蓄用燃料は6か月分の所要量（3年計画）を国債で予算要求する。

おわりに

海自には、1999年に海自創設以来初の海警行動[6]（海上警備行動）が発令（能登半島沖不審船事件）され、2004年には2度目となる海警行動が発令（漢級原子力潜水艦領海侵犯事件）された。また、現在も続いているソマリア沖海賊対策は、当初は海警行動で発令され、その後は特別措置法で対処している。更に、多くの尊い命が失われた「3.11東日本大震災」では、災害派遣[7]（大規模震災災害派遣）が発令され、震災発生直後から同年8月31日までの長期にわたり、艦艇約60隻以上、航空機約20機以上、人員に至っては約16,000名の規模でこれに即応した。

このように海自を取り巻く環境は、ここ十数年で大きく変化し、事態発生に際しては艦隊編成を伴う迅速な展開が求められるようになった。特に、自己完結型を旨とする艦艇には、迅速かつ長期にわたり継続した行動が要求され、これを支える燃料の確実な調

---

6 防衛大臣が、海上における人命若しくは財産の保護又は治安の維持のため特別の必要があると判断した場合に命ぜられる自衛隊の部隊による海上における必要な行動をいう。

7 地震、水害等の大規模な天変地異及び大量の死傷者の発生が伴う大規模な事故などといった各種災害の発生に際して、救助活動や予防活動などの対応限界を超えた地域に陸海空の自衛隊部隊を派遣し、その組織を以て救援活動を行うことをいう。

達は、正に艦艇の行動力を支える根幹である。

ISMSにおけるプロセスアプローチとその対応について

主任研究員　榊　　勝

１．ISMSにおけるプロセスアプローチとは

プロセスアプローチについては、情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項（JIS Q 27001:2006）0.2.2 プロセスアプローチにおいて、次のように規定している。

（１）この規格は、組織の ISMS の確立、導入、運用、監視、レビュー、維持及び改善のために、プロセスアプローチを採用する。

（２）組織が有効に機能するためには、多くの活動を明確にし、また、それらを運営管理する必要がある。インプットをアウトプットに変換することを可能にするために経営資源を使用して運営管理するあらゆる活動は、プロセスとみなすことができる。多くの場合、一つのプロセスからのアウトプットは、次のプロセスへの直接のインプットとなる。

（３）そのようなプロセスを明確にし、かつ、相互作用させることと合わせて、それらのプロセスをシステムとして組織内に適用し、かつ、運営管理することを“プロセスアプローチ”と呼ぶ。

（４）この規格が規定する情報セキュリティマネジメントのためのプロセスアプローチでは、利用者が次の点を重視することを期待する。

①組織の情報セキュリティ要求事項を理解し、かつ、情報セキュリティのための基本方針及び目的を確立する必要性を理解する。

②その組織の事業リスク全般に対する考慮のもとで、組織の情報セキュリティリスクを運営管理するための管理策を導入し、運用する。

③その ISMS のパフォーマンス及び有効性を監視し、レビューする。

④客観的な測定に基づいて継続的に改善する。

２．プロセスアプローチの目的

組織が強固な情報セキュリティを構築するためには、さまざまなプロセスを組み合わせて実践する。従って、ISMS をプロセスアプローチの視点からみると、組織のセキュリティに関わるプロセスを明らかにし、個々のプロセスを適切に運用管理して、セキュリティの品質を高めることがプロセスアプローチの目的の一つと言える。

３．ISMSにおけるプロセスアプローチの構造

ISMS におけるプロセスアプローチの構造は、次のようになっていると考えられる。

（１）大きくは、 Plan-Do-Check-Act（計画―実行―点検―処置）（PDCA）モデルからなっており、ISMS プロセスすべての構築に適用される。

（２）このプロセスアプローチは、ISMS が利害関係者からの情報セキュリティ要求事項

及び期待をインプットしてどう取り入れ、必要となる活動及びプロセスを経て、その要求事項及び期待を満たした情報セキュリティの成果をどう生み出すかを表すことになる。

（３）ご存知のように、 Plan-Do-Check-Act（計画―実行―点検―処置）（PDCA）モデルは、箇条４，５，６，７及び８に規定するプロセス間のつながりを表すことにもなる。

（４）さらに、この箇条４，５，６，７及び８に規定するプロセス間のつながりに、附属書Ａ（規定）の管理目的及び管理策１３３項目が関連する箇条に展開していることになる。

４．プロセスの捉え方・考え方

組織は、色々な活動のユニット（かたまり）から成り立っており、そのユニットをプロセスと呼ぶ。従って、組織の業務は、たくさんのプロセスから出来ていることになり、そのプロセスの管理とともに組織のセキュリティに関わるプロセスも明らかにしなければならない。その結果、必然的に、組織の業務をいくつかの小さなプロセスに分け、それらのいくつものプロセスのつながり方を整理・理解して大きなプロセスとして管理していく。その大きなプロセスを組み合わせて組織のセキュリティも明らかにしながら組織の業務全体を管理していく。これがプロセスアプローチの捉え方・考え方である。

５．プロセスアプローチの展開パターン

プロセスアプローチの展開パターンを、JIS Q 27001:2006 の規格上から代表的な事例から検証してみることとする。

（１）先ずは、本文（箇条４，５，６，７及び８）におけるプロセスアプローチ

①4.2.1c)～j) 情報資産の特定→リスクアセスメント→適用宣言書の作成
→4.2.2a)リスク対応計画の策定

②5.2.2a)～d) 要員の力量の決定→教育・訓練→有効性評価→記録の維持

（２）次に、管理策におけるプロセスアプローチ

①A.6.2 外部組織　A.6.2.1 リスクの識別→A.6.2.2 対処の明確→A.6.2.3 契約へ

②A.10.2 第三者が提供するサービスの管理　A.10.2.1→A.10.2.2→A.10.2.3

③A.13.2 情報セキュリティインシデントの管理及びその改善
A.13.2.1 責任体制・手順→A.13.2.2 学習→A.13.2.3 証拠の収集

④A.14 事業継続管理　A.14.1.1→A.14.1.2→A.14.1.3→A.14.1.4→A.14.1.5

（３）本文及び管理策からなるプロセスアプローチ

①4.2.1a)ISMS 基本方針の定義→A.5.1 情報セキュリティ基本方針の承認・公表・通知・レビュー→4.2.3b) ISMS の有効性のレビュー→7.2a)レビューへのインプッ

ト

②A.8.1.1 役割と責任　→　5.2.2a)～d) 教育・訓練、意識向上及び力量

↑

A.8.2.2 情報セキュリティの意識向上、教育及び訓練

６．プロセスアプローチの具体的な展開

この度(23.11.15)の防衛省の「調達における情報セキュリティの確保に関する防衛省の取り組みについて」における情報セキュリティ要求事項を ISMS（JIS Q 27001:2006）のプロセスアプローチにリンク付けて展開することとする。

防衛省の情報セキュリティへのプロセスに、ISMSの管理策をリンク付けてプロセスアプローチが具体的に展開していることを確認する。

(1)防衛省への迅速な報告

①防衛省へ報告することを義務化

JIS Q 27001の管理策	A.6.1.6	**関係当局との連絡**

組織は、次のプロセスから報告する適用範囲を明確にしておく必要がある。

明確にするプロセス	JIS Q 27001の管理策	
1）保護すべき情報を取扱う施設を明確にする。	A.9.1.1	物理的セキュリティ境界
・情報及び情報処理施設のある領域を保護するために用いなければならない。		
2）対象となるサーバ/パソコン/ネットワークを明確にする。	A.10.6.1	ネットワーク管理策
・ネットワークを適切に管理し、制御しなければならない。		
3）報告するウイルス等への感染及び不正アクセスの事象を定義しておく。	A.10.4.1	悪意のあるコードに対する管理策
・悪意のあるコードから保護するために、検出、予防及び回復のための管理策、並びに利用者に適切に意識させるための手順を実施しなければならない。		

②責任者・連絡担当者を明らかにした連絡系統図の作成

ここで、組織としては、適切な連絡体制が維持されるスキームを構築しなければならない。一つのプロセスアプローチを展開してみる。

明確にするプロセス	JIS Q 27001の管理策	
1）関係当局との適切な連絡体制を維持しなければならない。	A.6.1.6	関係当局との連絡
2）契約上のセキュリティ義務を考慮する。	4.2.1b)2)	ISMSの確立
3）契約上の要求事項を満たすための組織の取組み方を、明確に定め、文書化し、また、最新に保たなければならない。	A.15.1.1	適用法令の識別
4）全ての従業員、契約相手及び第三者の利用者は、組織の方針及び手順についての適切な意識向上のための教育・訓練を受けなければならない。	A.8.2.2	情報セキュリティの意識向上、教育及び訓練
5）管理策の有効性を測定する。	4.2.3c)	ISMSの監視及びレビュー
6）期待したように実施されているか内部監査を実施する。	6.d)	ISMS内部監査
7）ISMSをレビューしなければならない。	7.3c)5)	ISMSマネジメントレビュー

(2)セキュリティ対策の強化

①少なくとも週１回以上、ウイルス対策ソフトによるフルスキャンを実施

組織としては、フルスキャンは、システムに負荷と時間がかかることから、次のプロセスを明確にしておく必要がある。

明確にするプロセス	JIS　Q　27001の管理策	
１）対象となるサーバ/パソコン/ネットワークを明確にする。	A.10.6.1	ネットワーク管理策
２）システム上、問題が無いか確認する。	ネットワークを適切に管理し、制御しなければならない。	
３）スキャン対象を絞り込む。	A.12.5.4	情報の漏えい
４）ウイルス対策ソフトを常に最新版にする。	情報漏えいの可能性を抑止しなければならない。	
５）実施時間、時間帯を設定する。		

②保護すべき情報が社外へ漏えいしていないか、２４時間３６５日監視

ここで、組織としては、次のプロセスから成る監視の管理基準を作成しておく必要がある。

明確にするプロセス	JIS　Q　27001の管理策	
１）どのような監視を設定するか。	A.10.10.2	システム使用状況の監視
２）監視・運用スタッフの配置をどうするか。	情報処理設備の使用状況を監視する手順を確立しなければならず、また、監視活動の結果を定めに従ってレビューしなければならない。	
３）検知した障害をどのように通知するか。		
４）だれ（どのチーム）が障害を切り分けるか。		
５）だれ（どのチーム）が障害対応をするか。		
６）障害対応後の報告はどうするか。		

③保護すべき情報へのアクセス記録については、３か月以上保存(現在は任意の保存期間)

組織は、次のプロセスから成るログの管理体制を明確にしておく必要がある。

明確にするプロセス	JIS　Q　27001の管理策	
１）取得するログの種類、保管方法、保管期間を定める。アクセスログ、操作ログ等	A.10.10.1	監査ログ取得
２）OS、アプリケーションのログ機能及び取得したログ自体が変更されないよう管理する。	A.10.10.3	ログ情報の保護
３）不正の牽性効果や、その本人の作業の正当性を担保する役割があります。	A.10.10.4	実務管理者及び運用担当者の作業ログ
４）障害の暫定処置及び恒久処置を行うために、障害原因を解明する。	A.10.10.5	障害のログ取得
５）操作元及びその時刻の正当性を確保し、デジタルフォレンジックにおいては、重要な証拠を保証する。	A.10.10.6	クロックの同期

④暗号化対策の強化(電子メールによる伝達については、暗号化を規定済)

組織としては、暗号化する対象・プロセスを明確にしておく必要がある。

明確にするプロセス	JIS　Q　27001の管理策	
１）全情報を定期的に洗出しする。	A.10.8.1	情報交換の方針及び手
２）フォルダの中に埋もれている情報を見逃すことなくリストアップを繰り返していく。	情報交換を保護するために、正式な交換方針、手順及び管理策を備えなければならない。	
３）保護すべき情報を明確にする。	A.10.8.1	電子的メッセージ通信
４）システム上でアクセス権の有無を明確にしておく。	通信の情報は適切に保護されなければならない。 （その他の対応策） ・データベースのアクセス監視 ・事前に制御するフィルタリング機能の導入 ・社内メールのやり取りの暗号化 ・スパム制御機能の整備 ・誤送信対策機能の整備	
５）情報の流れのプロセスを検証する。		
６）不要な情報にアクセスしない業務手順を確立する。		
７）持ち出すノートパソコンの暗号化を図る。		
８）社外の委託先のデータファイルの分割化		
９）電子メールのウイルス対策が基本である。		

(3)企業における教育・訓練の強化

社員への教育・訓練の実施状況を監査により確認
（なりすましメールへの対応状況を重点的に確認）

組織は、次のプロセスにより教育・訓練の有効性をシステム的にレビューする。

明確にするプロセス	JIS　Q　27001の管理策	
1）教育の対象者を明確にする。 従業員、契約相手、第三者の利用者	A.8.2.2	情報セキュリティの意識向上、教育及び訓練
2）役割及び責任に対応した教育計画の策定	組織の方針及び手順についての適切な意識向上のための教育・訓練を受けなければならない。	
3）教育及び訓練の有効性を評価する。		
4）教育及び訓練の実施、技能、経験及び資格を記録し、要員の力量を管理する。	5.2.2	教育・訓練、意識向上及び力量
5）教育及び訓練の管理策の有効性を測定する。	a)要員の力量を決定する。 b)その力量が持てるように教育・訓練する。 c)とった処置の有効性を評価する。 d)記録を維持する。	
6）上記の活動を内部監査する。		
7）以上の活動をインプットしてマネジメントレビューし、改善点等をアウトプットする。		

以上、展開してきた防衛省の情報セキュリティ要求事項に対応するプロセスは、ポイントとなるプロセスをまとめてみると、次のようなプロセスアプローチとなっていることを確認することが出来る。

①防衛省へ報告することを義務化

↓

A.6.1.6 関係当局との連絡、 A.15.1.1 適用法令の識別

②責任者・連絡担当者を明らかにした連絡系統図の作成

↓

4.2.1b)2) ISMS の確立　契約上のセキュリティ義務を考慮
A.8.2.2 情報セキュリティの意識向上、教育及び訓練

③少なくとも週１回以上、ウイルス対策ソフトによるフルスキャンを実施

↓

A.10.6.1 ネットワーク管理策
A.12.5.4 情報の漏えい

④保護すべき情報が社外へ漏えいしていないか、２４時間３６５日監視

↓

A.10.10.2 システム使用状況の監視

⑤保護すべき情報へのアクセス記録については、３か月以上保存

（現在は任意の保存期間）

A.10.10.1 監査ログ取得

↓

⑥暗号化対策の強化(電子メールによる伝達については、暗号化を規定済)

↓

A.10.8.1 電子的メッセージ通信

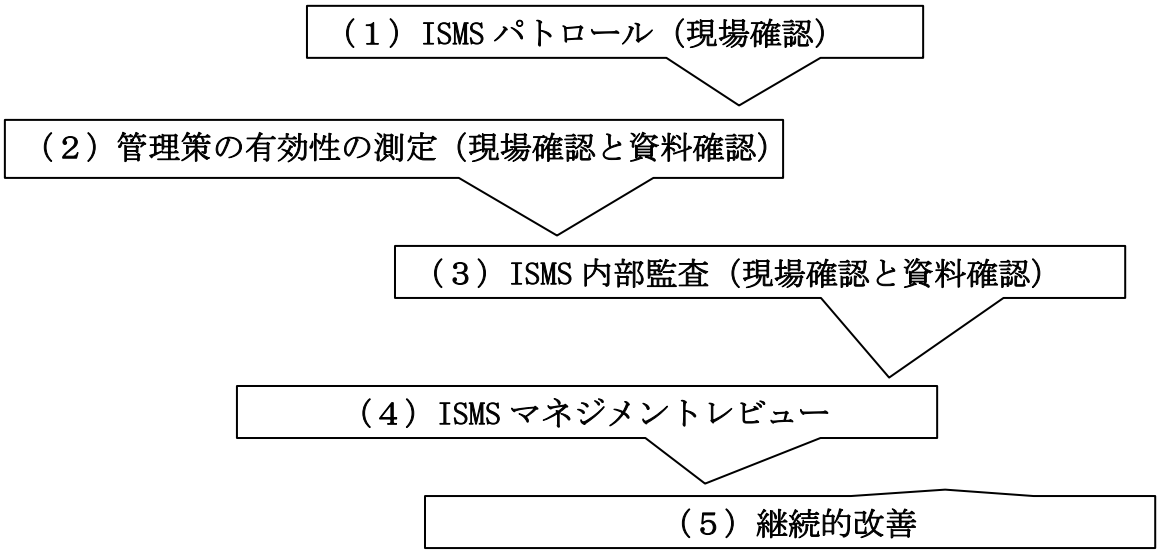
⑦社員への教育・訓練の実施状況を監査により確認

（なりすましメールへの対応状況を重点的に確認）

6 ISMS 内部監査の実施
7 ISMS のマネジメントレビューの実施

７．プロセスアプローチの有効性のレビュー

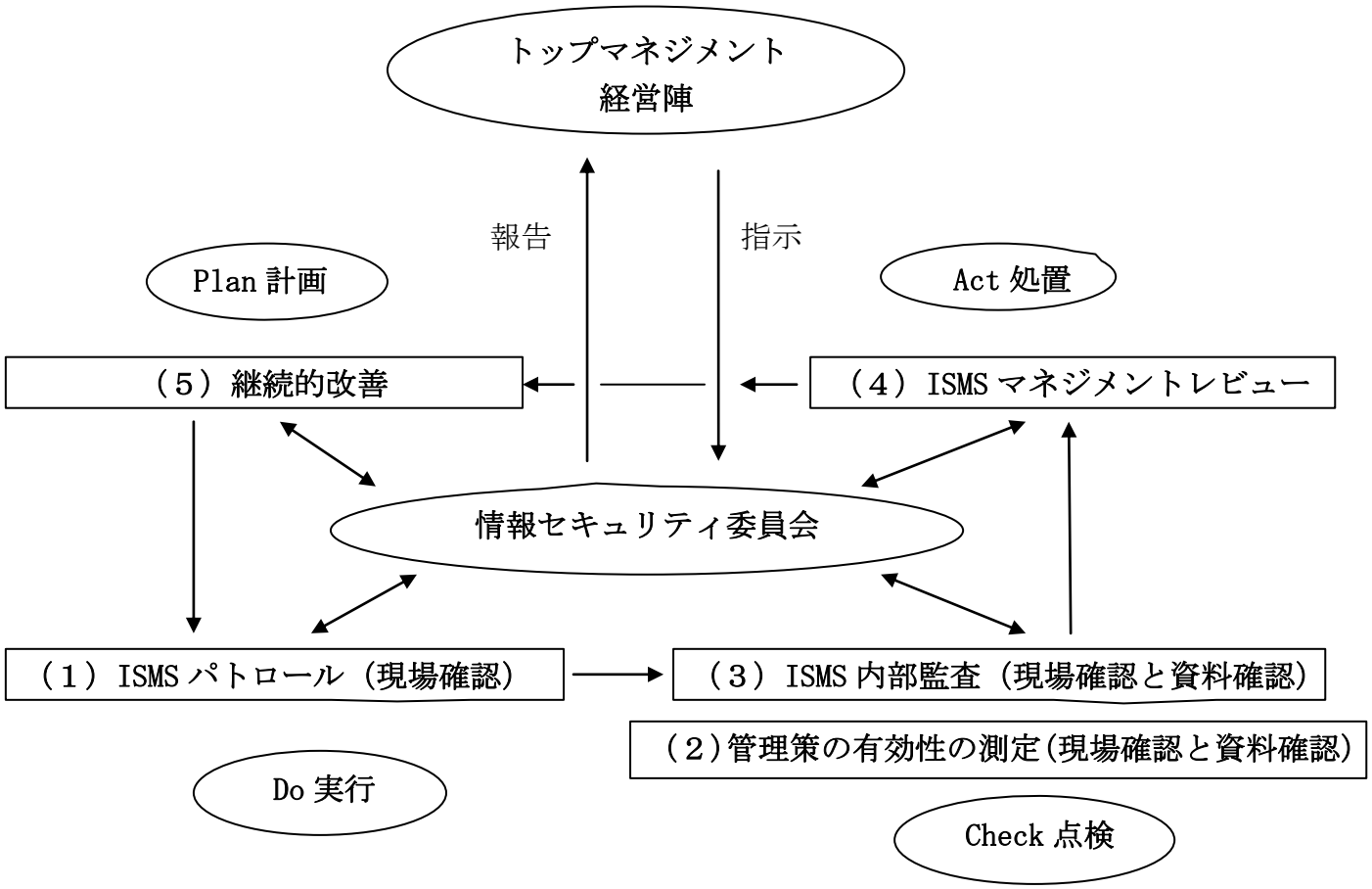
これまで展開してきたプロセスアプローチが組織にとって適切で、有効で、妥当であるか定期的に確認して、問題点等を抽出して継続的に改善していくという、次のようなプロセスアプローチが必要であることはご理解いただけると思います。



８．プロセスアプローチにおける最重要要素・視点

このようなプロセスアプローチが、JIS Q 27001:2006 4.2.3ISMS の監視及びレビューa)3)において「組織は、“人力にゆだねて又は情報技術を導入して実施しているセキュリティ活動が期待どおりかどうかを経営陣が判断することを可能にする”ことを実行しなければならない。」と規定しているとおり、最終的には、トップマネジメン

ト・経営陣が把握可能な有効なセキュリティガバナンスが構築されていることが最重要要素・視点である。



戦前と現在のスパイ防止法

客員主任研究員　横山恭三

目次

はじめに

今年 5 月に発覚した在日中国大使館李春光一等書記官のスパイ疑惑は、多くの国民の関心を呼び起こした。我が国では国外におけるインテリジェンス活動（スパイ活動）がオーソライズされていないため、日常的になじみのない存在であるスパイ活動の国内での摘発は、国民にとって驚きの原因となる。同様に、海外旅行中の日本人が軍港などを背景に記念写真を撮りスパイ容疑で身柄を拘束されるという話は、スパイ活動に全くなじみのない日本人の能天気さを示している。

ある全国紙は、「今回の事件の教訓を踏まえ、スパイ防止法の導入に向けた議論を検討することが必要である」[8]という意見を紙上で表明した。新聞紙上では「スパイ」や「産業スパイ」という言葉が使用されているが、日本の現行法では「スパイ」という言葉は定義されていない。現行刑法が昭和 22 年に改正されるまで、現行刑法には“間諜”という言葉が存在していた。このような事実を知っている人は少ないであろう。

本来スパイ活動には、諜報、謀略、宣伝等の活動があるが、本稿では、スパイの行う

[8] 読売新聞平成 24 年 6 月 1 日朝刊

諜報活動に焦点を当てている。

冷戦時代には、旧ソ連をはじめとする旧共産圏諸国は、外交官、通商代表部、ジャーナリスト等を隠れ蓑として相当数の情報機関員を西側諸国に送り込み、内外政策や軍事に関する諜報活動を活発に行ってきた。（本稿ではこれらのスパイを軍事スパイと呼ぶ。）しかし、冷戦後は、各国とも経済・産業情報の収集に一層力を入れるようになってきた。このため、従来からの情報機関員によるスパイ行為という脅威に加えて、ロシア、中国を含む幾つかの国のように、研究者、留学生等を先進諸国に派遣し、先端技術情報を窃取させるなどの、新しい脅威が出現してきた。（本稿ではこれらのスパイを産業スパイと呼ぶ。）

こうした動きに対応し、米国では、1996 年には経済スパイ法が制定され、企業に対する情報収集活動の取締りが強化された。我が国では、2009 年（平成 21 年）の不正競争防止法及び「外国為替及び外国貿易法」（以下、外為法という）の改正により産業スパイを取り締まることが一応は可能となった。

本稿では、戦前のスパイ防止法を紹介するとともに、最近のスパイ防止法を巡る議論や関連する法律の改正の動向を取り纏めた。

以下、はじめにスパイ対策の全体像を紹介し、次に戦前のスパイ防止法、次に現在のスパイ防止法を「守秘義務に関連する法律」と「スパイを直接取り締まるための法律」に区分して実態を紹介する。次にスパイ防止法の制定に対する反対意見を、1985 年に国会に提出されたが廃案となった「国家秘密に係るスパイ行為等の防止に関する法律案」を例に紹介する。最後に、あるべきスパイ防止法について簡単に私見を述べる。

本稿が、スパイ防止法の導入に向けた議論の資となれば幸甚である。

1. スパイ対策の全体像

スパイ対策には二通りの方策がある。一つは、一般に秘密保全といわれる予防措置である。予防措置には標的（人的、物的）の防護強化や外国情報機関員等の合法的な諜報活動の監視などがある、もう一つは、外国情報機関員等の非合法の諜報活動を探知し、スパイを逮捕する制圧行為である。制圧行為の法的根拠となるのがスパイ防止法である。図 1 は、旧軍のスパイ対策の概念を図示したものである。旧軍では武力行使や政治、外交の表面的手段に対し、スパイ活動などを裏面的手段と呼び、裏面的手段による闘争を秘密戦と称していた。

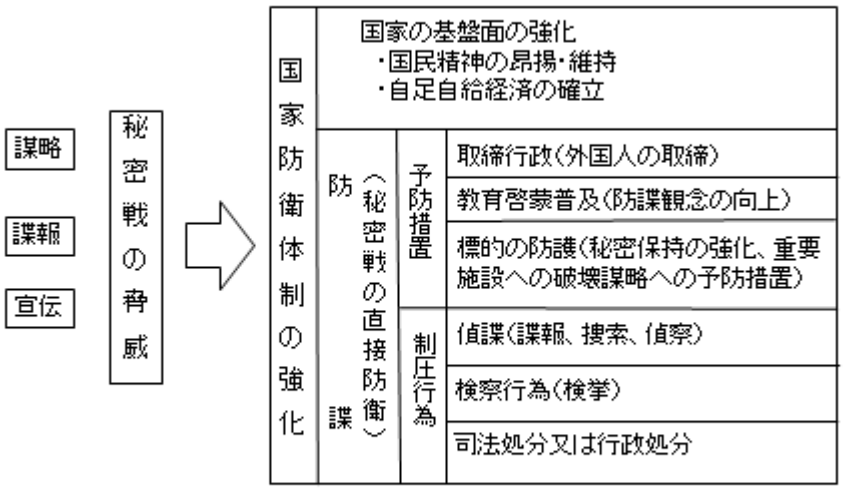


図1　旧軍における秘密戦の概念

我が国では近年、スパイ対策の一環として秘密保全体制の強化が図られてきた。2001年（平成13年）10月29日に成立した改正自衛隊法により防衛上特に秘匿を必要とする秘密を漏えいした場合の罰則が強化される等の措置が講ぜられた。具体的には、「防衛秘密」が創設され、処罰の対象に、「防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者」が含まれた。

また、2007年（平成19年）8月9日にカウンターインテリジェンス推進会議が策定した「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」に基づき、「政府機関の情報セキュリティ対策のための統一基準」や「秘密取扱者適格性確認制度」などが政府機関において統一的に運用されている。

以上の対策は、いずれも予防措置である。即ち、我が国では戦後から今日を通じて制圧行為の強化がほとんど図られてこなかったと言っても過言でない。このため、我が国には他国のようにスパイを直接取り締まる法律がなく、司法当局は他国と比べ、厳しい対応を迫られている。例えば、スパイは多くの場合、隠密に行動する。時には地下にもぐり活動する。この様なスパイ活動に対抗するには、疑わしい個人や組織を事前に探知（又は偵知）しなければならない。そのための有効な手段の一つが、通信傍受である。2000年11月に成立した「犯罪捜査のための通信傍受に関する法律」は、我が国において犯罪捜査のための通信の傍受を合法として認めた最初の法律である。しかし、この法律は通信傍受の対象となる犯罪を“薬物関連犯罪，銃器関連犯罪，集団密航の罪，組織的殺人”に限定し、さらに、“犯罪が行われたと疑うに足りる十分な理由”がなければ通信傍受は許可されない。これらの犯罪がスパイ（組織）と繋がる可能性もあるが、隠密に行動するスパイ（組織）に対応するのは困難であろう。

２．戦前のスパイ防止法

戦前のスパイ防止に関連する法律には刑法、軍機保護法、及び国防保安法がある。これらについて簡単に条文等を紹介する。

〇刑法

日本で最初の近代刑法といわれる旧刑法（明治 13 年太政官布告第 36 号）の第 131 条は、「本国及ヒ同盟国ノ軍情機密ヲ敵国ニ漏泄シ若クハ兵隊屯集ノ要地又ハ道路ノ険夷ヲ敵国ニ通知シタル者ハ無期流刑ニ処ス。２　敵国ノ間諜ヲ誘導シテ本国管内ニ入ラシメ若クハ之ヲ蔵匿シタル者亦同シ」と規定している。

明治 40 年に制定された現行刑法には、外患誘致、外患援助、通謀利敵、未遂、予備陰謀、戦時同盟國ニ対スル行爲など外患に関する罪が定められていた。

現行刑法は、昭和 22 年に大幅に改正された。新旧条文の比較は次のとおりである。

新条文（1947 年（昭和 22 年）の改正後）	旧条文（1947 年（昭和 22 年）の改正前）
第 81 条［外患誘致］ 外国と通謀して日本国に対し武力を行使させた者は、死刑に処する。	第 81 条［外患誘致］ 外國ニ通謀シテ帝國ニ對シ戰端ヲ開カシメ又ハ敵國ニ與シテ帝國ニ抗敵シタル者ハ死刑ニ處ス
第 82 条［外患援助］ 日本国に対して外国から武力の行使があったときに、これに加担して、その軍務に服し、その他これに軍事上の利益を与えた者は、死刑又は無期若しくは二年以上の懲役に処する。	第 82 条［外患援助］ 要塞、陣營、軍隊、艦船其他軍用ニ供スル場所又ハ建造物ヲ敵國ニ交附シタル者ハ死刑ニ處ス 兵器、彈藥其他軍用ニ供スル物ヲ敵國ニ交附シタル者ハ死刑又ハ無期懲役ニ處ス
第 83 条 削除	第 83 条［通謀利敵］ 敵國ヲ利スル爲、要塞、陣營、艦船、兵器、彈藥、汽車、電車、鐵道、電線其他軍用ニ供スル場所又ハ物ヲ損壞シ若クハ使用スルコト能ハサルニ至ラシメタル者ハ死刑又ハ無期懲役ニ處ス
第 84 条 削除	第 84 条［同前］ 帝國ノ軍用ニ供セサル兵器、彈藥其他直接ニ戰鬪ノ用ニ供ス可キ物ヲ敵國ニ交附シタル者ハ無期又ハ三年以上ノ懲役ニ處ス
第 85 条 削除	第 85 条［同前］ 敵國ノ爲メニ間諜ヲ爲シ又ハ敵國ノ間諜ヲ幇助シタル者ハ死刑又ハ無期若クハ五年以上ノ懲役ニ處ス 軍事上ノ機密ヲ敵國ニ漏泄シタル者亦同シ

第 86 条 削除	第 86 条［同前］ 前五條ニ記載シタル以外ノ方法ヲ以テ敵國ニ軍事上ノ利益ヲ與ヘ又ハ帝國ノ軍事上ノ利益ヲ害シタル者ハ二年以上ノ有期懲役ニ處ス
第 87 条［未遂］ 第八十一条及び第八十二条の罪の未遂は、罰する。	第 87 条［未遂］ 第八十一条及び第八十二条の罪の未遂は、罰する。
第 88 条［外患予備・陰謀］ 第八十一条又は第八十二条の罪の予備又は陰謀をした者は、一年以上十年以下の懲役に処する。	第 88 条［外患予備・陰謀］ 第八十一條乃至八十六條ニ記載シタル罪ノ豫備又ハ陰謀ヲ爲シタル者ハ一年以上十年以下ノ懲役ニ處ス
第 89 条 削除	第 89 条［戦時同盟國ニ対スル行爲］ 本章ノ規定ハ戦時同盟國ニ對スル行爲ニ亦之ヲ適用ス

以上のように、戦前の刑法では軍人、軍属を問わず広く国民の秘密保護について厳しく規定しているが、敵国のスパイを直接取り締まることを規定した条文は存在しない。また、漏洩する対象は、明治 13 年太政官布告第 36 号から通して、一般的な外国でなく敵国（又は敵国のスパイ）と限定されている。

○軍機保護法

1899 年（明治 32）に制定された軍機保護法は、1937 年（昭和 12 年）の盧溝橋事件が起こった翌月に改正されている。改正軍機保護法の条文（第 1 条から第 5 条のみ）は次のとおりである。

第一条　本法ニ於テ軍事上ノ秘密ト称スルハ作戦、用兵、動員、出師其ノ他軍事上秘密ヲ要スル事項又ハ図書物件ヲ謂フ

2　前項ノ事項又ハ図書物件ノ種類範囲ハ陸軍大臣又ハ海軍大臣命令ヲ以テ之ヲ定ム

第二条　軍事上ノ秘密ヲ探知シ又ハ収集シタル者ハ六月以上十年以下ノ懲役ニ処ス

3　軍事上ノ秘密ヲ公ニスル目的ヲ以テ又ハ之ヲ外国若ハ外国ノ為ニ行動スル者ニ漏泄スル目的ヲ以テ前項ニ規定スル行為ヲ為シタル者ハ二年以上ノ有期懲役ニ処ス

第三条　業務ニ因リ軍事上ノ秘密ヲ知得シ又ハ領有シタル者之ヲ他人ニ漏泄シタルトキハ無期又ハ三年以上ノ懲役ニ処ス

2　業務ニ因リ軍事上ノ秘密ヲ知得シ又ハ領有シタル者之ヲ公ニシ又ハ外国若ハ外国ノ為ニ行動スル者ニ漏泄シタルトキハ死刑又ハ無期若ハ四年以上ノ懲役ニ処ス

第四条　軍事上ノ秘密ヲ探知シ又ハ収集シタル者之ヲ他人ニ漏泄シタルトキハ無期又ハ二年以上ノ懲役ニ処ス

3　軍事上ノ秘密ヲ探知シ又ハ収集シタル者之ヲ公ニシ又ハ外国若ハ外国ノ為ニ行動スル者ニ漏泄シタルトキハ死刑又ハ無期若ハ三年以上ノ懲役ニ処ス

第五条　偶然ノ原由ニ因リ軍事上ノ秘密ヲ知得シ又ハ領有シタル者之ヲ他人ニ漏泄

シタルトキハ六月以上十年以下ノ懲役ニ処ス第三条　業務ニ因リ軍事上ノ秘密ヲ知得シ又ハ領有シタル者之ヲ他人ニ漏泄シタルトキハ無期又ハ三年以上ノ懲役ニ処ス

○国防保安法

大東亜戦争（太平洋戦争）の半年前の 1941 年（昭和 16 年）5 月に施行された国防保安法の条文（第 1 条から第 8 条のみ）は次のとおりである。

第一条　本法ニ於テ国家機密トハ国防上外国ニ対シ秘匿スルコトヲ要スル外交、財政、経済其ノ他ニ関スル重要ナル国務ニ係ル事項ニシテ左ノ各号ノ一ニ該当スルモノ及之ヲ表示スル図書物件ヲ謂フ

一　御前会議、枢密院会議、閣議又ハ之ニ準ズベキ会議ニ付セラレタル事項及其ノ会議ノ議事

二　帝国議会ノ秘密会議ニ付セラレタル事項及其ノ会議ノ議事

三　前二号ノ会議ニ付スル為準備シタル事項其ノ他行政各部ノ重要ナル機密事項

第二条　本章ノ罰則ハ何人ヲ問ハズ本法施行地外ニ於テ罪ヲ犯シタル者ニ付亦之ヲ適用ス

第三条　業務ニ因リ国家機密ヲ知得シ又ハ領有シタル者之ヲ外国(外国ノ為ニ行動スル者及外国人ヲ含ム以下同ジ)ニ漏泄シ又ハ公ニシタルトキハ死刑又ハ無期若ハ三年以上ノ懲役ニ処ス

第四条　外国ニ漏泄シ又ハ公ニスル目的ヲ以テ国家機密ヲ探知シ又ハ収集シタル者ハ一年以上ノ有期懲役ニ処ス

2　前項ノ目的ヲ以テ国家機密ヲ探知シ又ハ収集シタル者之ヲ外国ニ漏泄シ又ハ公ニシタルトキハ死刑又ハ無期若ハ三年以上ノ懲役ニ処ス

第五条　前二条ニ規定スル原由以外ノ原由ニ因リ国家機密ヲ知得シ又ハ領有シタル者之ヲ外国ニ漏泄シ又ハ公ニシタルトキハ無期又ハ一年以上ノ懲役ニ処ス

第六条　業務ニ因リ国家機密ヲ知得シ又ハ領有シタル者之ヲ他人ニ漏泄シタルトキハ五年以下ノ懲役又ハ五千円以下ノ罰金ニ処ス

第七条　業務ニ因リ国家機密ヲ知得シ又ハ領有シタル者過失ニ因リ之ヲ外国ニ漏泄シ又ハ公ニシタルトキハ三年以下ノ禁錮又ハ三千円以下ノ罰金ニ処ス

第八条　国防上ノ利益ヲ害スベキ用途ニ供スル目的ヲ以テ又ハ其ノ用途ニ供セラルル虞アルコトヲ知リテ外国ニ通報スル目的ヲ以テ外交、財政、経済其ノ他ニ関スル情報ヲ探知シ又ハ収集シタル者ハ十年以下ノ懲役ニ処ス

軍機保護法及び国防保安法は、刑法と違い平時にも適用する法律となっている。しかし、当時は現実的には戦時であったと言える。また、軍機保護法と国防保安法は、守秘義務とスパイを取り締まる法律となっている。

３．現在のスパイ防止法

（１）守秘義務に関連する法律

今日の日本の法律で、安全保障に関連する守秘義務を規定している法律は、国家公務員法（地方公務員法及び外務公務員法は、国家公務員法に準ずる。）、自衛隊法、「日米相互防衛援助協定等に伴う秘密保護法」、「日米安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法」、「核原料物質、核燃料物質及び原子炉の規制に関する法律」である。また、それぞれの法律には罰則規定が定められている。以下、それぞれの守秘義務に係る条文のみを紹介する。

○国家公務員法

第百条には「職員は、職務上知ることのできた秘密を漏らしてはならない。その職を退いた後といえども同様とする」と規定されており、この規定に違反して秘密を漏らした者（そそのかし又はそのほう助をした者を含む）は「一年以下の懲役又は五十万円以下の罰金」に処せられる。

○自衛隊法

第五十九条には「隊員は、職務上知ることのできた秘密を漏らしてはならない。その職を離れた後も、同様とする」と指定されており、この規定に違反して秘密を洩らした者（教唆し、又はそのほう助をした者を含む）は、「一年以下の懲役又は三万円以下の罰金」に処せられる。さらに、同法第百二十二条 には、「防衛秘密を取り扱うことを業務とする者がその業務により知得した防衛秘密を漏らしたときは、五年以下の懲役に処する。防衛秘密を取り扱うことを業務としなくなった後においても、同様とする」と規定されており、この規定する行為の未遂犯及び過失犯並びに行為の遂行を共謀し、教唆し、煽動した者も処罰される。ここで、「防衛秘密を取り扱うことを業務とする者」とは、① 防衛省職員、② 国の行政機関の職員のうち防衛に関連する職務に従事する者、及び③ 防衛省との契約に基づき防衛秘密に係る物件の製造若しくは役務の提供を業とする者、と解される。

○「日米相互防衛援助協定等に伴う秘密保護法」

第三条には「特別防衛秘密を取り扱うことを業務とする者で、その業務により知得し、又は領有した特別防衛秘密を他人に漏らしたもの」は、十年以下の懲役に処すると規定されている。「特別防衛秘密」とは米国から供与された船舶・航空機・武器・弾薬などの装備品や資材に関する非公開情報をいう。

○「日米安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法」

第六条には、「合衆国軍隊の機密で、通常不当な方法によらなければ探知し、又は収集することができないようなものを他人に漏らした者」は、十年以下の懲役に処すると規定されている。

○「核原料物質、核燃料物質及び原子炉の規制に関する法律」

第六十八条の三には「原子力事業者等及びその従業者並びにこれらの者であつた者は、正当な理由がなく、業務上知ることのできた特定核燃料物質の防護に関する秘密を漏らしてはならない」と規定されており、この規定に違反した者は、「一年以下の懲役若しくは百万円以下の罰金に処し、又はこれを併科する」と定められている。

（2）スパイを直接取り締まるための法律

現在、スパイを直接取り締まるための法律と言えるのは、「日米相互防衛援助協定等に伴う秘密保護法」、「日米安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法」、「不正競争防止法」、及び「外国為替及び外国貿易法（以下、外為法という）」である。前者の二つは、我が国又は合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、軍事機密を探知し、又は収集した者を処罰の対象としている。後者の 2 つは、いわゆる産業スパイに適用できる法律である。以下それぞれの関連する条文を紹介する。

ア．軍事スパイを取り締まるための法律

○「日米相互防衛援助協定等に伴う秘密保護法」

第三条には、「わが国の安全を害すべき用途に供する目的をもつて、又は不当な方法で、特別防衛秘密を探知し、又は収集した者」は、十年以下の懲役に処すると規定されている。

○「日米安全保障条約第六条に基づく施設及び区域並びに日本国における合衆国軍隊の地位に関する協定の実施に伴う刑事特別法」

第六条には、合衆国軍隊の機密を、合衆国軍隊の安全を害すべき用途に供する目的をもつて、又は不当な方法で、探知し、又は収集した者は、十年以下の懲役に処する」と規定されている。また同法には、「施設又は区域を侵す罪」や「軍用物を損壊する等の罪」、「制服を不当に着用する罪」等も規定されており、スパイの諜報活動のみならず、破壊活動も取り締まる条文が定められている。

上記の 2 つの法律は、一見十分なスパイ防止法に見えるが、米国軍隊の機密を保護することを目的としており、日本の機密を保護することを目的としていないという不備がある。

イ．産業スパイを取り締まるための法律

日本にはスパイの定義がない。ましてや産業スパイの定義もない。本稿では、外国政府、外国政府の影響下にある組織、又は外国情報機関員の利益のために、技術情報を取得する者を産業スパイと定義する。

ちなみに、米国には米国スパイ行為法（U.S. Espionage Act）と経済スパイ行為法（Economic Espionage Act）の 2 つのスパイ防止法がある。米国スパイ行為法では、軍事スパイ行為（あるいは国家スパイ行為）とは「取得した情報が、米国に損害を与えるため又は外国の利益のために使用されることを意図し又は承知して、国家防衛に関する情報を取得すること」と定義している。経済スパイ行為法では、経済スパイ行為（Economic espionage）と産業スパイ行為（Industrial Espionage）の両方が定義されている。経済スパイ行為とは、「外国政府、外国政府の影響下にある組織、または外国政府の職員の利益になることを承知又は意図して、企業秘密を意識的かつ意図的に取得すること」、産業スパイ行為（Industrial Espionage）とは、「その企業秘密の所有者に損害を与えることを承知又は意図して、所有者以外の誰かの経済的利益のために、州間通商または外国貿易のために製造された製品に関連した企業秘密を意識的かつ意図的

に取得すること」と定義している。

ところで、我が国の産業スパイ活動を取り締まる法律には、「不正競争防止法」と「外国為替及び外国貿易法（以下、外為法という）」がある。以下、それぞれについて考察する。

〇不正競争防止法

不正競争の防止を目的として、平成 5 年 5 月に制定された（旧）不正競争防止法では、適用対象が、同業などのライバル会社に対して営業面で重要な情報を漏らし、公平な競争が妨げられた場合に限られ、しかも、海外を含めて情報の流出先を特定する必要があるため、立件自体が難しく、スパイが起訴されたケースはこれまで一度もなかった。

ところが、海外への日本企業の情報流出が深刻化する中、平成 21 年度に本法は改正され、目的の如何を問わず、営業秘密を取得した者を取り締まることができるようになった。経済産業省が作成した不正競争防止法説明資料では、改正趣旨[9]について次のように述べている。現行法においては、構成要件上「不正の競争の目的」が要求されていることから、不正の利益を得るため海外政府等に営業秘密を開示する行為や、保有者を単に害するため営業秘密をネット上の掲示板に書き込む愉快犯的な行為など競争関係を認め得ない場合は処罰の対象外であった。しかし、こうした行為も営業秘密に対する違法性（当罰性）の高い侵害行為として処罰対象とする必要がある。他方で、不正な行為によるものとはいえ、保有者のために行った場合や正当な目的で行った場合にまで構成要件に該当するものとすべきではない。そこで、正当な目的等で行われる場合を処罰範囲から明確に除外しつつ、当罰性の高い行為を処罰対象とするため、「不正の競争の目的で」を、「不正の利益を得る目的で、又はその保有者に損害を加える目的で」（図利加害目的）と改めた。」

この改正不正競争防止法により、従業員、とくに外国人従業員による産業スパイ行為などにより、日本企業の技術情報が他国のライバル企業に流出したり、軍事転用されたりするのを防止することが可能となった。事実、2012 年 3 月、愛知県警は産業スパイ行為を働こうとした可能性がある中国人社員を不正競争防止法違反（営業秘密の領得）容疑で逮捕した。別紙第 1 の No20「中国人従業員の営業秘密の領得事件」がこの例である。

〇外為法

我が国の安全保障輸出管理制度は、「リスト規制」と「キャッチオール規制」の２つから成り立っている。そして、外為法を根拠として、輸出貿易管理令及び外国為替令の別表でリスト規制・キャッチオール規制の対象となる貨物・技術が明示されている。

安全保障貿易管理とは、国際社会における平和と安全を維持するため、大量破壊兵器の開発を行っている国家やテロリスト（非国家主体）などの懸念のある相手に、兵器になる材料（貨物）や知識（技術）を渡さないようにするため、先進国を中心とした国際的な枠組み（国際輸出管理レジーム）を作り、国際社会と協調して輸出等の管理を行っ

[9] http://www.meti.go.jp/policy/economy/chizai/chiteki/unfair-competition.html#21

ていることを指している。

旧外為法では、日本に短期滞在する者が国内で取得した機微技術を国外に送付する場合や機微技術を記録した USB メモリ等を持ち出し国外で提供する場合の規制が不十分であったが、2009 年（平成 21 年）11 月に施行された改正外為法では、安全保障上懸念のある技術の対外取引をすべて許可対象にするとともに、これを確実に実施するため、USB メモリ等の国境を越えた持ち出しについても許可対象とし、さらに無許可輸出等について罰則を強化するとともに不正な手段による許可取得を罰する規定を導入した。

これにより、例えばロケットやミサイルに転用できる技術情報を外国人従業員や短期滞在者（留学生を含む）が取得し、外国に電子メールで送信、あるいは他人に提供する目的で USB メモリ等に情報を入れて国外に出た場合でも、取り締まることができるようになった。

４．「国家秘密に係るスパイ行為等の防止に関する法律案（1985 年）」の概要

すでに戦後 67 年を経たがスパイ防止法は未だ制定されていない。ただし、1980 年代前半には、コズロフ事件（1980 年）やレフチェンコ証言（1982 年）などの一連のスパイ事件があり、スパイ防止法の必要性が自民党内において活発に議論されるようになった。当時の中曽根総理は、国会答弁で「日本ぐらいスパイ天国であると言われている国はない（昭和 60 年第 102 会参議院決算委員会）」と述べている。このような中、我が国においてもスパイ防止法案が衆議院に提出されたが廃案となった経緯がある。以下、何故、廃案になったのか、その理由について考察する。

1985 年 6 月 6 日に伊藤宗一郎衆議院議員ら 10 名が、「国家秘密に係るスパイ行為等の防止に関する法律案」を衆議院に議員立法として法案を提出した。

全 14 条及び附則により構成される同法案は、「外国のために国家秘密を探知し、又は収集し、これを外国に通報する等のスパイ行為を防止することにより、我が国の安全に資することを目的とする」（第 1 条）もので、「国家秘密」とは、別表に掲げる「防衛のための体制等に関する事項」、「自衛隊の任務の遂行に必要な装備品及び資材に関する事項」、「外交に関する事項」並びにこれらの事項に係る文書、図画又は物件で、我が国の防衛上秘匿することを要し、かつ、公になっていないものとされた（第 2 条）。罰則に関しては、最高刑は死刑とされた。

しかし、野党、弁護士会、マスメディア等が反対に回ったため、政府は同法案を内閣法案として提出することを断念し、議員立法として提出したが、第 102 通常国会において同法案は継続審議となり、第 103 臨時国会で審議未了廃案となった。当時どの様な反対意見があったか、はじめに、国会での発言、次に、日本弁護士連合会の決議文を紹介する。

第 102 回国会・議院運営委員会（昭和 60 年 6 月月 25 日）における各委員の反対意見は次のようなものであった。[10]

[10] http://kokkai.ndl.go.jp/SENTAKU/syugiin/102/0440/10206250440040c.html

○広瀬委員（旧社会党）「日本国憲法の平和主義、民主主義そして基本的人権尊重の三つの理念のいずれにも反する」、「国権の最高機関である国会の審議にも多かれ少なかれ必ず影響を及ぼして、守秘義務を盾にとって国会、国権の最高機関にすら、国家機密あるいは防衛機密、外交機密というようなことを理由にして国民の代表である国会の審議権すら無視される大きな危険をはらんでいる。まさに議会制民主政治瓦解の方向にすらつながりかねない」

○平石委員（公明党）「我が国の平和憲法の立場から考えましたときに、この法案はまさに憲法上疑義のある法案である」、「国家秘密の件でありますが、秘密とは一体何か
という概念が明らかにされておりません」

○西田（八）委員（旧民主党）　「少なくとも、こうした国家秘密を守るためには国民的コンセンサスを得る必要がある」「国家秘密の定義そのものが極めて抽象的であり、あいまいであります」「国のいろいろな問題を知る権利を持った国民の権利を抑圧することになる」

○東中委員（共産党）「この法律がスパイ防止を口実にして、広範な国民の知る権利、言論、出版の自由を抑圧する」「戦前の法律で言えば、昭和十二年の八月、日中戦争が起こった明くる月につくられた軍機保護法、そして太平洋戦争が始まる半年前にできた昭和十六年の三月の国防保安法、ここで外交事項を入れたわけです。その二つを合わせたものを今出してきた。しかも、それに対する漏えいは、外国への通報ということになれば死刑と無期懲役だけしかない。こういう法体系というのはまさにファッショ的な戦時立法なんです」「日本国憲法によって軍機保護法、国防保安法が廃止になった。ところが、憲法はそのままであるのに、自衛隊ができたからということで、その軍隊の秘密を守るのだと称して今度のこの法案が出されてきている。これは憲法を完全に踏みにじる、日本国憲法はもうなくなったのだという姿勢をとっているわけです」

次に、日本弁護士連合会が昭和 60 年 10 月 19 日に発表した「国家機密に係るスパイ行為等の防止に関する法律案に反対する決議文」[11]の骨子を紹介する。同決議文では次の４つを問題点として挙げている。

①防衛・外交にかかわる「国家秘密」の内容が、実質的に、広範囲・無限定であり、行政当局の恣意的専断を許すことになる。

②「探知・収集」、「外国に通報」、「他人に漏らす」などの実行行為及び過失犯など、その行為類型もすべて、広範囲・無限定であり、調査・取材活動、言論・報道活動、日常的会話等のすべてが含まれる。

③死刑を含む重罪の提案は、合理的な根拠を欠き、時代の流れに逆行して、著しく異常なものである。

④予備・陰謀罪と独立教唆犯の提案も、また、罪刑法定主義と行為責任主義の原則に

[11]http://www.nichibenren.or.jp/activity/document/civil_liberties/year/1985/1985_2.html

違反する。

５．あるべきスパイ防止法に関する一考察

（１）スパイ防止法の必要性

軍事スパイ防止法は、突き詰めれば我の軍事行動を成功ならしめるためのものである。相手国の軍事スパイは、我の軍事行動を阻止又は妨害するために、軍事情報を収集するのである。軍事情報の漏えいは、兵士（隊員）の命を危険に晒し、軍事作戦を失敗させ、ひいては国の命運を左右することになる。現憲法下において、国の命運を左右するような軍事行動は想定できないであろう。このため、軍事スパイ防止法に関する国民のコンセンサスを得ることは難しい。しかし、近年、自衛隊の海外活動が増加した。これまでのところ、安全な地域への派遣であったが、将来は紛争地域における派遣任務が付与されることがあるかもしれない。このような場合、部隊の安全を確保するための国内外のスパイ対策が必要となるであろう。

産業スパイ防止法には、安全保障上の側面と経済的な側面がある。安全保障上の側面では、軍事技術情報の漏えいは、相手国の軍事戦闘能力を短期間で増強し、我の防衛力の弱体化を招くであろう。経済的な側面では、最先端技術等の企業秘密の漏えいは、直接、企業に大きな金銭的損失を与えるとともに、企業ひいては国家の国際競争力を低下させるであろう。また、昨年末の政府の武器輸出三原則の緩和の決定を受け、今後、米国をはじめとする安全保障の協力関係国との「防衛装備品の国際共同開発・生産」が進展するであろう。このような中での重要な技術情報の漏えいは、我が国の国益を損なうとともに国際的な我が国の信頼低下につながる。さらに、スパイ防止法の必要性は上記の実質的な利害の他に以下のような様々な側面がある。

一つ目は、主権国家にとって不可欠な機能であるということである。スパイ活動はインテリジェンス活動の一部である。諸外国では、インテリジェンス活動は政府の通常の機能であると考えられており、行政機関の一つとしてインテリジェンス組織を保有し、そして、国内外のインテリジェンス活動を行っている。国外におけるインテリジェンス活動の一つがスパイ活動である。スパイ防止法の制定は主権国家としての責務である。

二つ目は、スパイ行為に対する抑止力である。外国から日本は「スパイ天国」であると侮られるようでは、スパイをのさばらせることになるであろう。これは主権国家の威信にかかわる問題である。

三つ目は、諸外国からの信頼の獲得である。軍事情報の交換や国際共同開発・生産が進展する中で、諸外国の信頼を得るためには分かりにくい個別法での対処でなく、包括的なスパイ防止法が不可欠である。

（２）スパイ防止法の制定に際しての考慮事項

・スパイ対策はカウンターインテリジェンス活動の一部である。カウンターインテリジェンス活動には国内と国外の活動がある。国外活動においてその存在を看破し、その目的・技術等を知得することが肝要である。我が国ではカウンターインテリジェンスの

国外活動がオーソライズされていない。スパイ防止法の制定努力と併行してこのような状況の改善が必要である。

・現憲法下で軍事スパイ防止法の制定に対する国民の理解を得ることは困難であろう。前述したが、軍事スパイの脅威が最大になるのは我が国が軍事行動を行う場合である。そのような場合には国民の理解も得やすいであろう。当面は、自衛隊の海外活動の安全確保のためにスパイ対策に関する何らかの措置が必要であろう。

・外国人従業員が増大する中、産業スパイ防止法の制定が不可欠である。軍事スパイ防止法より国民の理解は得やすいであろう。現在は、不正競争防止法と外為法が産業スパイ対策の根拠法となっているが、複雑で分かりにくい。一本の産業スパイ防止法に集約すべきである。

・最近のスパイ活動は、コンピュータネットワークを利用したサイバー攻撃による情報窃取へと移行している。即ちサイバー・エスピオナージである。伝統的なスパイ活動への対処とともにサイバー・エスピオナージへの対処も喫緊の課題である。

・「インテリジェンスは毒である」[12]、とも言われるが、諜報、防諜に対する拒否反応が少なからず国民にあることを認識することがスパイ防止法制定の出発点である。これを国民の食わず嫌いであると看過せず、対策を講ずることが重要である。英国ではインテリジェンス活動を、閣僚による監視（情報に関する閣僚委員会)、議会による監視（情報委員会)、及び司法による監視（コミッショナー制度、調査権限審判所）により多元的に監視するシステムを構築している。これなどを参考にすべきであろう。

おわりに

スパイ防止法制定の目的は国益を守ることである。しかるに、国会議員が「日本列島は日本人だけの所有物じゃない」[13]と発言したり、国益を守るために海外に派遣されている大使が東京都の尖閣購入を批判したりするなど、我が国の指導者層の国家意識・国益意識は希薄だと言わざるを得ない。政務三役の守秘義務については国務大臣、副大臣、大臣政務官の規範及び官吏服務紀律で定められているが、その他の政府の機密情報に接する機会の多い国会議員にも守秘義務を課すべきであろう。岡田副総理は 24 年 3 月 2 日の記者会見で、「外交を進めるためには、与野党の議員が外交機密を共有しながら議論することは必要で、その際は公務員と同じ守秘義務をかけるべきだ」[14]と述べている。

最後に指摘したいことは、インテリジェンス機能に対する理解の深化とその強化である。既述したが、インテリジェンスは国家指導者の重要な意思決定と密接に関連するものである。インテリジェンスには危険な側面もあるが、それでも各国指導者はインテリジェンスの有用性を認め、インテリジェンス機関を国家の行政機能の一つとして保持している。そして、国外におけるインテリジェンス活動、すなわちスパイ活動を公然・非公然に行っていることは世界の常識である。

---

12 大森義夫「日本のインテリジェンス」（文春新書）

13 http://www.nicovideo.jp/watch/sm7244363

14 読売新聞平成 24 年 3 月 4 日朝刊

今年 4 月 15 日のテレビ番組で、渡辺防衛副大臣は、4 月 13 日の北朝鮮による事実上の弾道ミサイル発射の際に、アメリカから早期警戒衛星の情報が入ったものの、日本のレーダーで捕捉できず、確認に時間を要したことから、「今後、日本も情報収集のため、独自の静止衛星を持つ必要がある」[15]との認識を示した。このように各国の国益がぶつかり合う国際社会において日本の国益を守るためには、独自の情報（インテリジェンス）が必要であることは火を見るより明らかである。（了）

[15] http://www.nicovideo.jp/watch/sm17555288

（参考資料１）

戦後から今日までの日本におけるスパイ活動の概要

１．昭和 29 年 1 月　ラストボロフ事件

米国に亡命した在日ソ連通商代表部二等書記官ラストボロフは、ソ連の秘密情報機関が日本のあらゆる政府機関に手先（日本人工作員）を送り込ませ、自身が情報機関員で外交官を装って日本の内外政策について情報活動に従事していた事件。（焦点第 265 号）

２．昭和 46 年 7 月　コノノフ事件

在日ソ連大使館付武官補佐官ハビノフ陸軍中佐及びコノノフ空軍中佐が、米軍基地に出入りしていた通信機器部品の販売ブローカーである A に巧みに働き掛けを行い、多額の現金と引換えに米軍機密資料等の入手を企てていた事件。（焦点第 269 号）

３．昭和 51 年 1 月　汪養然事件

香港において貿易商社を経営していた香港在住中国人、汪養然は、46 年ころ、中国情報機関員から「香港において中国と取引する中国人業者は、祖国の建設と祖国防衛に協力する義務がある」と迫られ、日本における軍事、産業技術等の情報収集活動を行うよう指示され、以後、汪養然は、貿易業務を装って頻繁に来日し、「我が国の政治、経済、産業技術に関する情報」等の幅広い情報収集活動を行った事件。（焦点第 269 号）

４．昭和 51 年 5 月　マチェーヒン事件

昭和 51 年 5 月、米海軍空母の乗組員 A 一等兵曹は、50 年 5 月、横浜港祭りを見物中、「あなたの撮った写真がほしい。」と言葉巧みに近づいたソ連のノーボスチ通信社東京支局特派員マチェーヒン（38）と知り合い、以後、マチェーヒンから、「子供の誕生日のプレゼントだ。」と称して高価なおもちゃを贈られ、レストラン等で食事に誘われるなど家族ぐるみの交際を続けた。「アメリカ海軍の軍事機密を持って来てくれれば、1 件につき 1,000 ドル支払う。」と持ち掛けられ、機密文書や暗号表の入手を要求されたが拒否した事件。（昭和 52 年警察白書）

５．昭和 51 年 6 月　趙昌朝事件

昭和 51 年 6 月 16 日、東大阪市内に潜伏して活動中の北朝鮮スパイ趙昌朝が、我が国の政治、経済、防衛等に関する情報を収集することと補助者をスパイに養成し韓国に対する諸工作を行わせることを主たる任務として、毎月北朝鮮から暗号放送による指令を受けてその任務を実行していた事件。

６．昭和 55 年 1 月 9 日　レポ船第 18 和晃丸事件

北方領土に駐留するソ連国境警備隊の指令によって根室の漁民 S（48）とその配下の

第 18 和晃丸船長、同機関長の 3 人が情報活動を行っていた事件。（昭和 56 年警察白書）

7．昭和 55 年 1 月　コズロフ事件（宮永事件）

ソ連諜報機関の手先となって、元陸将補 M（58）と、M に防衛庁の秘密情報資料を提供していた現職自衛官二等陸尉 K（45）、准陸尉 O（49）が軍事関係情報の収集を行っていた事件。（昭和 56 年警察白書）

8．昭和 57 年 12 月　レフチェンコ証言

KGB 機関員のノーボェ・ブレーミヤ誌東京支局長レフチェンコが、多数の日本人工作員を運営して、政治工作を行っていた事件。（焦点第 269 号）

9．昭和 62 年 5 月　横田基地中ソスパイ事件

在日ソ連大使館員の働き掛けを受けた中国情報ブローカーA と、中国公司関係者から働き掛けを受けた親中団体幹部 B が、在日米軍横田基地従業員 C 及び軍事評論家 D らとともに、在日米空軍軍事資料の盗み出し・持ち出しグループを形成し、約 8 年間にわたり、主として米空軍戦闘機等のテクニカル・オーダーを、多額の報酬を得てソ連及び中国に売却していた事件。（焦点第 269 号）

10．昭和 62 年 7 月　東京航空計器スパイ事件

アエロフロート・ソ連国営航空東京支社に勤務していたＹ．Ｎ．デミドフは、我が国の航空機関係の高度科学技術の不正入手を企て、59 年末、東京航空計器株式会社第一事業部輸出部長Ｓ（55）に接近し、現金等を与えて、同社所有のフライト・マネージメント（飛行管理）システムに関する研究成果報告書等の産業秘密情報を提供させるというスパイ活動を行っていた。また、外交特権を有する在日ソ連通商代表部代表代理Ｙ．Ｇ．ポクロフスキーは、61 年 6 月に離任帰国したデミドフから引継ぎを受け、Ｓから航空機技術に関する情報資料等多数の提供を受け、その見返りとして現金等を交付するなどのスパイ活動を行っていたほか、ココム（対共産圏戦略物資輸出統制委員会）規制対象品であるＮＣ工作機械用のコンピュータソフト等の産業秘密情報の提供を要求していた事件（警察白書 63 年）

11．昭和 62 年 8 月　在日チェコスロバキア大使館員による諜報事案（シメック事案）

在日チェコスロバキア大使館二等書記官Ｖ．シメックは、61 年 4 月から 11 月までの約 8 箇月間にわたり、日本の高度科学技術関連企業のテクニカル・アドバイザーとして勤務する在日エジプト人のコンピュータ技師Ｋ（32）に接近し、高度科学技術情報の収集とココム規制対象品であるコンピュータ機器のチェコスロバキア向け輸出を目的とする会社設立を働き掛けていた。また、この働き掛けの過程で、シメックは、Ｋに対し勤務先のコンピュータ論理回路図の提供を執拗に要求したが、Ｋは、これを受け、勤務先より不正に入手してシメックに提供した事件。（警察白書 63 年）

12. 平成 9 年 7 月　イリーガル機関員による旅券法違反事件（黒羽・ウドヴィン事件）
ロシア対外情報庁（SVR）に所属するイリーガル機関員（国籍を偽るなど身分を偽装して入国しスパイ活動を行う者）が、福島県内から失踪した黒羽一郎という男性になりすまし、昭和 40 年頃から約 30 年にわたり我が国内外においてスパイ活動を行い、SVR 本部と連絡を取っていた事件。（焦点第 269 号及び第 273 号）

13. 平成 12 年 9 月　ボガチョンコフ事件（萩碕事件）
GRU 機関員とみられる在日ロシア大使館付海軍武官ボガチョンコフ大佐が、日ロ防衛交流を奇貨として知り合った海上自衛官から自衛隊内の秘密文書を入手していた事件で、警視庁と神奈川県警察の合同捜査本部が、同自衛官を自衛隊法違反（秘密漏えい罪）で検挙。自衛官は、同武官から現金等を受け取り、その見返りとして自衛隊内の秘密文書や内部資料を渡していた。（焦点第 269 号）

14. 平成 14 年 3 月　元通商代表部員に係る秘密保護法違反事件（シェルコノゴフ事件）
GRU 機関員とみられる在日ロシア通商代表部員アレクセイ・シェルコノゴフが、防衛調達関連会社社長（空自 OB の技術コンサルタント会社社長）に対し、米国から供与された情報で我が国の「防衛秘密」であるレーダ誘導ミサイル等に関する情報入手をそそのかしていた事件。（焦点第 269 号）

15. 平成 17 年 5 月　サベリエフ事件
在日ロシア通商代表部員が、2004 年（16 年） 9 月ころから 2005 年（17 年） 5 月ころにかけて、日本人会社員から、その勤務先の会社の先端科学技術に関する機密情報等を不正に入手し、対価として日本人会社員に多額の報酬を支払っていた事件。（焦点第 273 号）

16. 平成 17 年 12 月　上海総領事館員自殺事件
在上海総領事館の館員が平成 16 年 5 月 6 日に自殺。在上海総領事館員の死亡の背景には、現地の中国側公安当局関係者による条約国の義務に反すると見られる遺憾な行為があった事件。（外務省ホームページ、報道官会見記録、平成 17 年 12 月）

17. 平成 18 年　在日ロシア通商代表部員らによる窃盗事件
在日ロシア通商代表部員の工作を受けた日本人の元会社員が、その勤務先の企業が所有するミサイルの制御や誘導に転用できる「VOA 素子」を窃取し、これを在日ロシア通商代表部員に提供した事件。（焦点第 273 号）

18. 平成 19 年 3 月　中国人技術者の先端科学技術情報の横領事件
国内大手自動車部品メーカーに勤務する中国人技術者が、約 13 万件もの電子設計図

データを不正にダウンロードした社有パソコンを持ち出した事件。（焦点第 277 号）

19. 平成 20 年 1 月　内閣情報調査室職員のスパイ事件

内閣情報調査室に勤務する内閣事務官が、ロシアの情報機関員とみられる在日ロシア連邦大使館二等書記官のそそのかしにより職務上知り得た秘密を同人に漏らしたほか、現金 10 万円の賄賂を受け取っていた事件。（焦点第 277 号）

20. 平成 24 年 3 月　中国人従業員の営業秘密の領得事件

大手工作機械製造会社「ヤマザキマザック」が管理する設計図のデータファイルを不正に複製したとして、愛知県警が、中国籍の同社社員唐博容疑者を不正競争防止法違反（営業秘密の領得）容疑で逮捕した事件（読売新聞平成 24 年 3 月 28 日）

（参考資料２）

日本における安全保障輸出管理違反の概要

参考（関連法令の改正経緯）

・昭和 20 年 1 月、対共産圏輸出統制委員会（ココム）発足
・平成 6 年 3 月、ココム解体に伴い外国為替管理令及び輸出貿易管理令の一部改正
・平成 7 年 12 月、「ワッセナーアレンジメント」設立
・平成 8 年 10 月、大量破壊兵器の開発等にも利用が可能である技術的な水準の低い汎用品等を規制する新たな補完的輸出規制を行うため、外国為替管理令及び輸出貿易管理令の一部改正
・平成 9 年 4 月、「化学兵器の開発、生産、貯蔵、及び使用並びに廃棄に関する条約」の発効を受け外国為替管理令及び輸出貿易管理令の一部改正
・平成 14 年 4 月、「キャッチオール規制」導入

1．昭和 62 年　東芝機械ココム違反事件

大手工作機械メーカー東芝機械は、ソ連の情報機関員とみられる全ソ技術機械輸入公団幹部から働き掛けを受けた対ソ連貿易商社和光交易の仲介で、昭和 57 年 12 月から 58 年 6 月までの間に、ココム規制対象品である 9 軸同時制御の大型金属工作機械 4 台を輸出するに際し、ココム規制を受けない 2 軸同時制御の工作機械であると偽って通商産業大臣の「非該当証明」を受け、ソ連に不正輸出していた。さらに、同社は、59 年 6 月及び 7 月、通商産業大臣の承認及び許可を受けずに、上記工作機械の部品及び修正プログラムをソ連に不正輸出していた事件。（警察白書 63 年）

2．昭和 62 年　東明貿易ココム違反事件

在日中国人経営の対中国貿易商社東明貿易は、59 年 7 月から 61 年 1 月までの間に、通商産業大臣の承認及び税関長の許可を受けずに、ココム規制対象品であるシグナル・ジェネレーター（信号発生機）等を従業員に携帯させて持ち出し、中国に不正輸出していた事件。（警察白書 63 年）

3．昭和 62 年　東明商事ココム違反事件

在日朝鮮人経営の対北朝鮮貿易商社東明商事は、60 年 11 月から 61 年 8 月までの間に、通商産業大臣の承認を受けず、また、虚偽の通関手続をし、あるいは税関長の許可を受けずに、ココム規制対象品であるシンクロ・スコープ等を北朝鮮に不正輸出していた事件。

（警察白書 63 年）

４．昭和 63 年　極東商会等ココム違反事件

対中国貿易商社極東商会及び新生交易は、昭和 60 年 6 月ころから 61 年 11 月ころまでの間、通商産業大臣の承認及び税関長の許可を受けずに、ココム規制対象品であるデジタルメモリ等を従業員に携帯させて持ち出し、中国に不正輸出していた事件。（警察白書元年）

5．平成元年　朝鮮総連傘下団体幹部によるココム違反事件

在日本朝鮮人商工連合会幹部K（63）は、通商産業大臣の承認を受けず、税関長に衣類、日用品と偽って申告をした上で、ココム規制対象品であるパソコン等を、朝鮮総連の関係事務所を経由して、63 年 9 月 5 日、新潟港を出港する北朝鮮貨客船三池淵号でひそかに北朝鮮へ送り込もうとしていた事件。（警察白書元年）

6．平成元年　ダイキン工業ココム違反事件

大手空調機メーカーダイキン工業は、61 年 2 月ころから 62 年 5 月ころまでの間、通商産業大臣の承認を受けず、税関長に虚偽の品質証明書を作成、提出するなどして、ココム規制対象品であるハロン 2402 をソ連に不正輸出していた事件。（警察白書元年）

7．平成元年　プロメトロンテクニクス・ココム違反事件

機械器具の製造販売及び輸出入を行っているプロメトロンテクニクス社は、昭和 62 年 2 月から 3 月の間、ココム規制対象品であるハフニウムワイヤー（原子炉の制御棒としても転用可能な稀（き）少金属）を、また、62 年 6 月から 9 月までの間、同じくココム規制対象品であるマスクアライナー（半導体製造装置）を、それぞれ通商産業大臣の承認及び税関長の許可を得ず、東ドイツに不正輸出していた事件。（警察白書 2 年）

8．平成 3 年　大手航空電子機器会社によるミサイル部分品不正輸出事件

大手航空電子機器会社は、Ｆ－4 ファントム戦闘機に装備するミサイルの部分品（ローレロン）について外国企業から修理の依頼を受け、同部分品を修理の上、シンガポール経由でイラン向けに不正輸出していた事件。（警察白書 4 年）

9．平成 6 年　中国向けココム違反事件

ハイテク兵器に転用可能で、ココムで共産圏への輸出が規制されている電子機器（イメージ増強管）を中国へ不正輸出した事件。（警察白書 7 年）

10．平成 8 年　毒ガスの原材料の北朝鮮への不正輸出事件

毒ガスの原材料になるなどとして輸出禁制品に指定されているフッ化ナトリウム等がコメ支援船によって北朝鮮に輸出された事件。（警察白書 9 年）

11．平成 11 年　測定装置の中国への不正輸出事件

通商産業大臣の許可が必要な核関連貨物である測定装置を、中国向けを韓国向けであると偽って不正輸出した事件。（警察白書 12 年）

12. 平成 12 年　対戦車ロケット砲専用光学照準器部分品のイランへの不正輸出事件

通商産業大臣の許可が必要な対戦車ロケット砲専用光学照準器の部分品をイラン向けに通商産業大臣の許可を受けずに不正輸出した事件。（警察白書 12 年）

13. 平成 15 年　ジェットミル（超微粉砕機）のイランへの不正輸出事件

ミサイル関連機材として輸出規制されたジェットミル（超微粉砕機）をイラン向けに不正輸出した事件。（警察白書 16 年）

14. 平成 15 年　直流安定化電源の北朝鮮への不正輸出事件

核兵器等の開発に用いられるおそれがあるものとして、輸出許可が必要な直流安定化電源を、経済産業大臣の許可なくタイ王国経由で北朝鮮向けに輸出した事件。（警察白書 16 年

15. 平成 16 年　周波数変換器の中国への不正輸出事件

核兵器等の開発に用いられるおそれがあるものとして、輸出許可が必要な周波数変換器を、経済産業大臣の許可なく中国向けに輸出した事件。（警察白書 16 年）

16. 平成 18 年　凍結乾燥機の北朝鮮への不正輸出事件

東京都内の商社の元代表取締役(58)は、14 年 9 月、核兵器等の開発等のために用いられるおそれがあるものとして輸出許可が必要な凍結乾燥機 1 台を、経済産業大臣の許可なく台湾経由で北朝鮮向けに輸出した事件（警察白書 19 年）

17. 平成 18 年　三次元測定機の不正輸出事件（リビア、イラン）

神奈川県内の精密機器メーカーの代表取締役社長(67)ら 5 人は､13 年 10 月及び 11 月、核開発等に転用可能であることから輸出規制されている三次元測定機 2 台を、経済産業大臣に対する許可申請の不要な機器であると偽って、シンガポール経由でマレーシア向けに輸出した事件。（警察白書 19 年）

18. 平成 19 年　無人ヘリコプターの中国への不正輸出事件

静岡県内の自動二輪車等製造販売会社の事業部長（58）ら 3 人は、17 年 12 月、大量破壊兵器の運搬等に用いられるおそれがあるものとしてその輸出が規制されている無人ヘリコプター1 台を、経済産業大臣の許可を受けることなく、中国に向け輸出しようとした事件。（警察白書 20 年）

19. 平成 20 年　真空ポンプ等の北朝鮮への不正輸出事件

東京都内の貿易商社代表取締役（66）は、15 年 7 月、大量破壊兵器の開発等に用いられるおそれがあるものとしてその輸出が規制されている真空ポンプ等を、経済産業大臣の許可を受けることなく、台湾経由で北朝鮮向けに輸出した事件。（警察白書 21 年）

20．平成 21 年　タンクローリーの北朝鮮への不正輸出事件

貿易会社代表取締役（50）は、20 年 1 月、大量破壊兵器等の開発等に使用されるおそれがあるものとして輸出が規制されている中古タンクローリー2 台を、経済産業大臣の許可を受けることなく、北朝鮮に輸出するための経由地として、韓国に不正に輸出した事件。（警察白書 22 年）

21．平成 21 年　パワーショベルの北朝鮮への不正輸出事件

貿易会社社長らは、大量破壊兵器の開発等に使用されるおそれがあるものとして、経済産業大臣により外為法に基づき輸出許可を要するとの通知を受けていたパワーショベル 1 台を、同大臣の許可を受けないで、21 年 4 月、中国経由で北朝鮮向けに不正に輸出した事件。（警察白書 23 年）

22．平成 21 年　高性能工作機械の韓国への不正輸出事件

工作機械メーカー「ホーコス」（広島県福山市）が、核兵器開発に転用可能な工作機械を不正輸出したとされる事件。（MSN 産経ニュース平成 21 年 3 月 25 日）

23．平成 22 年　イラン人留学生の受入を拒否した東工大が敗訴した事例

2003 年に来日し、08 年に難民認定を受けた男性は、平成 22 年 6 月、がんの放射線治療を研究するため東工大原子炉工学研究所に入学願書を提出した。大学は、イラン人への核関連分野の教育が行われないよう要請する国連安全保障理事会決議や文部科学省の指導を踏まえ、男性が安全保障上、管理対象となっている技術情報にアクセスする可能性があるとして同年 9 月、入学を拒んだ。東京地裁は平成 23 年 12 月 19 日、法の下の平等を保障する憲法と教育の機会均等を定める教育基本法に反すると判断、不許可決定を無効とした。

（日本経済新聞平成 2312 月 20 日）（注：本事例は、安全保障輸出管理に関する大学の取組みを紹介するために付け加えた。）