

# 米国の軍事技術移転管理体制

——審査・移転実務メカニズムと日本の選択肢——

松 村 昌 廣

は じ め に

第1章 管理体制の構造—審査メカニズム

第2章 管理体制の構造—移転実務メカニズム

第3章 管理体制の特徴と役割

終わりに—日本の選択肢

キーワード：軍事機密，一般保全協定，産業保全協定，GSOMIA，武器輸出

## はじめに

軍事覇権を握る米国はその中核を自国とイギリス、カナダ、オーストラリア、ニュージーランド、四ヶ国の諜報同盟国で固め、その外側に同心円状に、二国間及び多国間の相互安全保障条約による同盟国、次に、様々な公式、非公式の友好国を従えている。この政治秩序の核心は二国間の安全保障関連条約・協定の束として明示することが可能であり、その要は外交チャンネルを通じて二国の政府間で交渉・締結される「軍事情報に関する一般保全協定 (GSOMIA)」(以下、一般保全協定)<sup>(1)</sup>にある。強固な同盟関係には戦略情報や軍事技術情報など、機密情報の共有が不可欠であるが、その前提として価値観、脅威認識、利害関係を共有し、同盟国、とりわけ盟主とともに実力行使も辞さない政治的決断を示すことが必要である。一般保全協定の有無は米国の同盟国に対する信頼感の有無を示唆し、協定の内容は信頼感の水準を表している。

一般保全協定は機密の定義などの基本事項、機密漏洩の防止に関する基本方針、第三者への情報提供、知的財産権、秘密が漏洩した場合の対処方針などを定めるものであっても、個別の機密事項を開示、譲渡するかどうかの決定やその実務上の処理を扱うものではない。関連施設へのアクセス許可、人物証明、機密情報の取り扱い、伝達など、政府間及び民間契約者への軍事機密情報の開示・移転に関する実務的な取り決めは、一般保全協定の付属文書 (annex) である産業保全協定 (ISA: Industrial Security Agreement) によって規定される。つまり、産業保全協定は米国の軍事機密情報を外国政府や当該国の産業部門 (軍事関連企業など) にかかに委ねるべきかを定めたものである。(形式的には、産業保全協定は米国と当該第三国との相互的な内容になっているが、機密情報の開示・移転が圧倒的に米国から第三国になされることを踏まえると、米国による機密情報管理を確立し、そのことによって当該第三国・同盟国との支配・被支配関係を構築する効果がある。)

一般保全協定と産業保全協定は実質的に共同生産や共同開発などの個別のプログラムやプロジェクトの契約内容と重複しており、その雛形となっていると思われる。2000年現在、米国は50数カ国と一般保全協定を締結しており、このうち、筆者が確認した限りでは、機密性の低いフランスとイスラエルとの協定が公開されている<sup>(2)</sup>。残念ながら、筆者の知る限り、産業保全協定には公開されたものがない<sup>(3)</sup>。

そこで本稿では、まず、インターネット上に公開されている関連法令、マニュアル、その説明書・解釈書を基本的な概念、制度、手続きなど、実務面に焦点を当てて検討することによって、米国の軍事技術移転管理体制とその中で産業保全協定の役割を把握する。基本的には、この作業はこれらの資料の重要部分の翻訳と編集であり、この部分には筆者による独自のアイデアは全く含まれていない。しかし、この分野に関する邦文の公開資料・情報は皆無である一方、上記の関連の英文資料を理解するには、国防総省や軍の組織、軍事調達、軍事諜報などに関するある程度の専門知識が必要である。その上、多くの軍事専門用語が文献の容易な理解を阻んでいる。

次に、このように米国の軍事技術移転管理体制における一般保全協定や産業保全協定の枢要性を実務面から具体的に理解した上で、米国と一般保全協定を締結しておらず、また、当然その結果、その付属文書である産業保全協定も締結していない日本が米国からの軍事技術の移転を容易には（また、円滑には）享受できない点を考察する。約三年前に発表した拙論<sup>(4)</sup>では、米国と日本を含めた主要同盟国との二国間安全保障関連条約・協定体制を比較分析し、構造的な視角から概括的に一般保全協定の枢要性を指摘した。この意味で、本稿は前稿を補完する。

## 1 管理体制の構造—審査メカニズム

米国の軍事技術移転管理体制は外国政府や国際機関に対する個別事案を精査して、武器・武器システム、軍事技術、軍事サービスの売却、移転、

輸出を許認可するかを決める審査メカニズムと、許認可に基づいて具体的にその細部を決め移転作業を遂行する実務メカニズムに大別することができる。

審査権限は「武器輸出管理法（AECA: Arms Export Control Act）」、「国家安全保障機密情報に関する大統領行政命令（Executive Order “Classified National Security Information” 12958）」、そして、国家開示政策を定めた「国家安全保障決定覚書（NSDM: National Security Decision Memorandum）119」によって規定されている。

武器輸出管理法は、国防関連の物品やサービスを他国に販売ないし貸与する場合には、受け入れ国がその権原や所有権を第三者に移転しないこと、米国が指定した使用目的以外に用いないこと<sup>(6)</sup>、且つ、米国が施すように付随・関連する機密情報を保全することを要求している。国務省国防貿易管理室（the Office of Defense Trade Controls, Department of State）がその審査権限を有する。

行政命令12958は、米国政府が指定する機密情報を伴う物品やサービスへのアクセスに関して、受け入れ国の行政府が米国政府により当該機密情報に施される保全措置と同じ水準の措置を確保しない場合には、当該国の行政府以外（つまり、立法府や司法府）によるアクセスを認めないと定めている<sup>(7)</sup>。また、アクセス資格は政府により合法的に権限を付与された使用目的を果たす上での必要性と使用者の信頼性によって判断されねばならず、使用目的以外のアクセスには別途、米国の許可を要する。さらに、第三国の情報には瑕疵がある、つまり正確ではないと推定することになっている。つまり、機密情報は常に開示国から直接に入手せねば、「正しい」情報として使用できない。この仕組みもまた機密情報の保全を強化する効果を持つ。

大統領によって裁可された国家安全保障決定覚書119は諸省庁を構成員とする開示審査メカニズム（国家開示政策委員会）の設置と審査手続きを定め、その具体的な開示基準や限界を公表している。同委員会は関連情報の審査だけでなく、被開示国（機関）が米国の軍事機密情報を守る意図を<sup>(8)</sup>

持つかどうかを裁定するために一般保全協定締結の交渉を行い、さらに、米国と同水準の機密保全能力を持つかどうかを裁定するために現場での調査を行うこととなっている。この調査を踏まえて、同委員会は被開示国（機関）に対してどの水準の機密を開示するか、その被開示国（機関）専用の開示政策を策定するかどうか、そして、当該被開示国から出される国家開示政策を執行する上での例外要請を認めるかどうかを決定する。さらに、同委員会は大統領府の国家安全保障会議（NSC: National Security Council）に対して審査活動に関する年次報告の提出を義務付けられている。

覚書119に基づいて、1988年10月、国防長官は國務長官、エネルギー省長官、中央情報局（CIA）長官の同意を得て、「外国政府ならびに国際機関に対する軍事機密情報の開示に関する国家政策と手続き」、いわゆる、国家開示政策（NDP-1: National Disclosure Policy One）を制定した。この基本政策によれば、軍事機密情報は保存、保護されねばならず、米国に明確に定義された利益をもたらす場合にのみ、外国政府や国際機関と共有される。具体的には、米国の外交政策、米国の軍事安全保障、被開示国の機密情報を保全する意図と能力、米国政府に対する利益、米国の目的を充足するために機密情報を開示する必要性、これらの政策目標を考慮する。

ただし、覚書119は国防関連の物品やサービスに係わる軍事機密のみを扱うのであって、中央情報局が管轄する諜報・防諜プログラム、国家通信情報システム保全委員会（NTISSC: National Telecommunications and Information Systems Security Committee）の所管である通信保全情報・装置と信号諜報、1954年制定の原子力法により管理される原子力関連諜報、さらに国家安全保障局（NSA）長官と中央情報局長が責任を有する特定区分の機密（SCI: Sensitive Compartmentalized Information）、国防長官、その補佐を担う幹部（副長官、次官、次官補など）及び統合幕僚会議が管轄する戦略計画などは除外している。

国家開示政策（NDP-1）は外国政府や国際機関に対する軍事機密情報の開示を決定する際に用いる基準や条件を定めている。決定は開示を受ける

外国政府や国際機関（以下、被開示国・機関と呼ぶ）に対する米国政府の外交政策と合致しておらねばならず、具体的には以下の七つの条件が含まれる。（ただし、その全てではない。）

- 1) 被開示国（機関）は、米国の軍事・政治目標と両立する軍事・政治目標を履行する際に米国と協力すること。
- 2) 外交や軍事の分野で、特定の米国の国家目標に役立つこと。
- 3) 当該機密情報が米国と被開示国（機関）の相互的な軍事・安全保障上の目標の実現を支援する形で用いられること。
- 4) 機密開示が米国の軍事安全保障を脅かさないこと。（例えば、高度な技術情報の開示が軍事技術における米国の地位に過度のリスクを与えないこと。）
- 5) 機密開示に際して相互的な軍事・外交政策の目標の追求と米国の軍事機密情報の保全との二つのバランスを保つ必要性を考慮すること。
- 6) 被開示国（機関）は米国の機密保全の措置と実質的に同程度の保全措置を採ること。
- 7) 機密開示が少なくとも当該機密開示の価値と同程度の利益を米国にもたらすこと。例えば、
  - (1) 米国が被開示国から必ず見返りの機密情報の提供を受けること。
  - (2) 機密情報の交換ないし共同プロジェクトへの参加が技術的ないし軍事的視点から米国に有利であること。
  - (3) 被開示国の軍事力ないし軍事的効果を発展ないし維持することが米国にとって有利であること。
  - (4) 機密開示が必要な開示目的に限定されて用いられること。

さらに国家開示政策（NDP-1）は軍事機密情報を八つに分類し、各分類において被開示国（機関）の資格別、機密度の段階別<sup>(9)</sup>に開示権限の所在を明示し、その実施を委任している。その内容は特定の国際機関と殆どの外

国政府に対して決められている。八つに分類は以下のとおりである。

- 1) 部隊の組織編成, 訓練, そして, その使用に関する情報。戦術, 技法, 戦術ドクトリン・諜報, そして防諜ドクトリン・技法に関する一般的な情報であり, 次の分類(2)や(3)に含まれる特定の機器に関する操作, 訓練, 整備に必要な情報を除く。
- 2) 軍事物資と弾薬に関する情報。既に生産ないし使用されている機器の特定の項目に関する情報とその操作, 整備, 訓練に必要な情報。「米国弾薬表 (The U.S. Munitions List)」にある項目はこの分類にあたる。この分類は研究・開発には関係ない。
- 3) 応用研究・開発情報と関連資料情報。基本理論, 設計, 軍事的応用への試験調査に関する情報であって, 生産に必要な概念や軍事的特性に関する情報を含む。開発段階は, 機器が適合試験を終了し, 使用や生産に採用された段階で終わる。
- 4) 生産情報。設計, 仕様書, 製造技法, 物資や弾薬を製造するために必要な関連情報。
- 5) 合同軍事作戦とその計画・準備に関する情報。被開示国と米国が共同目標として戦力を向上するため, ないしは, 特定の合同戦術作戦・演習を計画, 準備, 支援するために必要な情報であって, 戦略的次元での計画や指導に関する情報。北米大陸の防衛に関する情報を含まない。
- 6) 米国の戦闘指令に関する情報。つまり, 特定の地域における米軍部隊に関連し, 一般的に, 米軍が駐留する国々かその周辺地域の国々に限定された情報。
- 7) 北米大陸の防衛に関する情報。データや機器を含め, 北米大陸の防衛に直接に関連する計画, 作戦プログラム, プロジェクトに関する情報。
- 8) 軍事諜報。外国に関する軍事的性格を有する情報であり, 中央情報局 (CIA) 長官と国家安全保障局 (NSA) 長官の権限の下にある特

定区分の機密（SCI）を含まない。

軍事技術移転の管理に関する審査権限は、委員会の議長である国防長官が他の関連省庁の同意を得て行使することになっている。この審査メカニズムは国家開示政策委員会（NDPC: National Disclosure Policy Committee）と呼ばれ、覚書119を行政府の中で実行することが任務である。ただし、開示の執行権限は、当該機密情報を管轄する省庁の責任者に委任されている。この委員会は全ての審査事項に広い利害関係を持つ国務省、国防総省、陸軍省、海軍省、空軍省、統合幕僚会議からの代表者と、特定の審査事項にだけ利害関係を持つ中央情報局（CIA）、国防情報局（DIA）、エネルギー省、国防総省の調達・技術・兵站担当次官官房、同省政策担当次官官房、同省ネットワーク統合担当次官補官房、同省ミサイル防衛庁、同省核エネルギー担当部局の代表者から構成される。審査はまず同委員会事務局、次に、上に挙げた様々な省庁の検討を経て、通常、10日間でなされる。委員会の審査プロセスで異論が出された場合には、同委員会委員長が30日以内に開示・非開示の決定を開示申請者（企業など）に対して行う。非開示決定に同意しない場合、申請者は10日以内に国防長官もしくは国防副長官に上訴できる。毎年、約12000件の審査を行い、100件前後の非開示が決定されている。<sup>(10)</sup>（1994年には145件、99年度には92件、98年度には98件<sup>(11)</sup>）。

要するに、審査メカニズムは機密情報の開示・移転が必ず米国の国益に資するように裁定を下す仕組みになっている。また、被開示国（機関）が十分な機密保全を行う意思と能力を持つかを確認する仕組みとなっている。

## 2 管理体制の構造—移転実務メカニズム

米国の軍事技術移転管理体制におけるもう一本の重要な柱は移転作業に関する実務メカニズムである。審査メカニズムにおいて妥当な政策判断がなされた場合でも、移転作業の実務が杜撰であり、その過程で機密情報が漏洩すれば、かえって国益を損なう。このような可能性をできるだけ排除

するため、堅牢な仕組みが構築されている。

武器輸出管理法や国家開示政策 (NDP-1) の下では、米国の民間契約者が開示国 (外国政府) の機密情報を保管・管理している場合であっても、当該被開示契約者に管轄権を有する米国政府が機密情報を保護する責任を最終的に負う。この義務は一般保全協定、その付属文書である産業保全協定、または、個別契約の機密保全条項を介して、米国政府と外国政府の相互的なものとなっている。したがって、民間契約者が機密情報を保管・管理していても、その国の政府は被開示国として当該機密情報を保全せねばならない。その意味で他国の民間契約者に対する開示・移転であっても、それは政府間の移転と位置付けられる。

機密情報を移転する政府間チャンネルには外交封印袋 (diplomatic pouch, 外交関係に関するウィーン条約第27条)、軍事書留郵便、軍事輸送、秘匿電子通信がある。もっとも、機密情報を移転する側とそれを受ける側の二カ国間合意が成り立てば、具体的な移転指示に則って機密取り扱い資格を持つ携行配達業者による代替方法をとることもある。なお、米国の場合、このための資格審査は国防捜査局 (Defense Investigative Service) が被開示国の政府と共同でその実務を行う。

軍事機密情報を伴う国際商業取引の移転実務は国務省の「国際武器取引規則 (ITAR: International Traffic in Arms Regulations)」と「国家産業保全プログラム運用マニュアル (NISPOM: National Industrial Security Operating Manual, DoD 5105.38-M)」(以下、運用マニュアル) に従わねばならない。これらの規定は米国政府と軍事機密情報を伴う物品・サービスの購入・販売を行う契約者だけではなく、米国の現行法令の法的、実務的制約を受ける範囲で米国政府から免許、補助金、証書を受けているものにも適用される<sup>(12)</sup>。

軍事機密開示の是非を見極める際に、被開示者が「米国人」であるか否かは決定的に重要であるが、運用マニュアルと国際武器取引規則では「米国人」の定義が異なる。運用マニュアルでは、「米国人」は米国市民権の保持者のみとされているが、国際武器取引規則では米国永住権保持者

など特定の移民資格を持つ外国籍の保有者であっても機密指定を受けていない技術情報ならば、輸出認可なしでもアクセスを与えるように、「米国人」はより広義に定められている。ただし、後者の場合でも、米国市民権を持たない者には機密情報に対するアクセスは与えられない。もっとも、米市民権も持たない者でも特定の機密情報に関して限定的なアクセス権（LAA: Limited Access Authorization）が与えられることがあるが、このアクセス権は機密情報を伴う輸出を認可するものではない。

運用マニュアルによれば、米国の管轄下にある契約者が雇用した者は外国政府の機密情報を扱う上での責任について米当局から説明を受けた後に、機密情報秘匿合意書（a Classified Information Nondisclosure Agreement）への署名を求められる。契約者及びその被雇用者は外国政府から事前の書面による同意なく当該政府の機密情報を第三国の代理人や国籍保持者に開示してはならない。開示の禁止対象には、第三国出身の米国の永住権保持者も含まれる。機密保全是相互性の原則の上に立脚しているから、米国からの機密情報にも同様の保全措置が要求され、事前に書面による米国政府の同意がなければ、米国の機密情報は第三国には開示されない。

ただし、米英間の場合、英国の同意に基づき、英国の「制限情報」（restricted information）は政府間のチャンネルを経由せず、直接、英国の契約者から米国の契約者へ民間のチャンネルを用いて開示することができる。英国の「制限情報」は米国の機密情報の分類では「秘（confidential）」として扱われ、米国の管轄下にあるかぎり、米国政府に最終的な保全責任がある。英国の「制限情報」を伴う機密情報の発信を米企業から英企業に行う際には、当該英企業は適切な機密情報アクセス資格と機密保全能力を持たねばならない。一旦、この資格と能力が認められれば、その後は、第一種軍事郵便、オーバーナイト商業配達サービス、資格を持つ者による携行配達、または、政府により許可された暗号機能を用いた秘匿通信（ファックスもしくはパソコン通信）のいずれかの方法により、契約者間で「制限情報」を伴う情報発信を行うことができる。

さらに、北大西洋条約機構（NATO）の軍事機密情報の分類で「機密

(secret)」とそれ以下の機密度に分類される情報を含む資料は NATO 登録システム (the NATO Registry System) に記載された制御地点の間ならば、開示側と被開示側の保全担当者の合意に則って行われる限り、資料の発信者から受信者への直接の携行配達が認められている。NATO 分類で「秘 (confidential)」と「制限情報 (restricted information)」にあたる情報に関しても同様である。つまり、新たに NATO 登録システムを用いることも、当該資料を米国の機関に配達する必要もない。

最後に、機密情報移転の実務に関する法令は常に厳格に適用されるが、兵器・兵器システムの共同生産や共同開発を実施するために、多国間のプログラムやプロジェクトにおいて、多国間産業安全保障ワーキング・グループ (MISWG: Multilateral Industrial Security Working Group) を臨機応変に結成し、機密情報の移転に関する多国間での政府間許可を促進することがある。

要するに、移転実務メカニズムは同盟国に機密情報を開示・移転しようとする米企業に米国政府が要求する機密保全措置を採らせるだけでなく、同盟国政府やその管轄の下にある企業に対しても同様の保全措置を採らせるように構築されている。具体的には、機密情報へのアクセス資格の基準や審査、そして開示・移転の通信・輸送手段の選定や実行手続きなどの詳細が定められている。相互性の原則の下、米国と同盟国の関係は形式上、平等であるが、機密情報の流れが圧倒的に米国から同盟国に流れている実態を踏まえると、米国の機密情報保全の仕組みは同盟国を軍事技術移転管理体制に取り込む効果を持つことは明らかである。

### 3 管理体制の特徴と役割

一般に、米国は同盟国に自国の兵器・兵器システムを供与、売却することによって、または、軍事技術を移転することによって同盟関係を強化してきたといわれる。しかし、「同盟強化」の具体的内容を本稿で分析した米国の軍事技術移転管理体制の視点から観れば、これらの二要因は同盟国

を米国の国益に沿ったように行動させるための強力な手段ともなっていることが分かる。

そもそも同盟国は自国の軍事安全保障を確保する手段として圧倒的な軍事技術力の優位を持つ米国の兵器・兵器システムを導入するのであるが、一旦、導入してしまえば、同盟関係を主従関係ないし支配・被支配関係に転化するように作用する。米国が軍事技術の革新能力で卓越し、他の追従を許さないため、導入後の兵器システムの性能向上（version-upgrade）や更新に際して、同盟国は米国の軍事技術標準に依拠せざるをえなくなる。システム統合技術として情報通信技術が急速に発展し、ここでも米国が卓越性を強化しているため、この傾向には拍車がかかっている<sup>(13)</sup>。

軍事技術における対米依存関係が定着すると、目的と手段の倒錯が起こる。当初、同盟国は手段として米国の兵器・兵器システムを導入したのであるが、逆に、対米依存関係を維持し、米国製の兵器・兵器システムの継続的な供与と米国の軍事技術への継続的なアクセスの確保そのものが目的になってしまう。したがって、米国の軍事技術移転管理体制は米国が同盟国の対米依存関係を管理し、同盟国を支配する仕組みであるともいえる。

本稿で記述したように、この管理体制は軍事機密情報の管理を軸に構築されている。同盟国の対米依存関係を維持・強化するためにはある程度の機密技術情報の開示・移転は不可避であるから、管理上の焦点は必要最低限の機密情報をいかに効果的に開示・移転するかにある。ただし、様々な省庁やその外局の存在に示されるように、特定の外交・安全保障の「政策目標」や同盟国の「対米依存関係」といっても、米国の国益は多面的であり容易に一義的には定義できないため、省庁間調整メカニズムとして国家開示政策委員会<sup>(14)</sup>が設けられているのである。

ここで注目すべきは、二国間協定である一般保全協定（GSOMIA）と産業保全協定（ISA）が米国の国内法令等の束である軍事技術移転管理体制の一部を構成しているわけではなくとも、両者は実質的に表裏一体の関係にあることである。確かに、形式論的には、個別の機密情報の開示・移転はこれらの二協定がなくとも、個別の契約に機密保全条項を含めることで

可能ではある。しかし、この方式では多数の案件、とりわけ複雑な技術情報を含むものを迅速に審査することは極めて困難であるし、包括的な機密保全措置を必ずしも確保できない。というのは、個別契約方式では、管理・保全対象はあくまで当該機密情報であることから、保全活動の人的側面に関しては、米国が直接制御できない同盟国の国内刑事法制に依存せざるをえないからである。一般保全協定を締結すれば、米国が是とする機密情報保全に関する定義と原則を同盟国に受け入れさせ、関連する国内刑事法制を改定させることによって包括的な保全措置を採らせることができる。さらに、産業保全協定を締結すれば、実質的には、米国の是とする機密取り扱い資格の分類、その審査基準及び方法、機密情報の移転・運搬の実務を同盟国に受け入れさせることができる。

同盟国が一般保全協定と産業保全協定を米国の軛と捉えるかどうかは米国からどの程度の機密情報の開示・移転を受けることができるかだけでなく、米国からどのような地位を与えられるかにも左右される。米国の軍事機密情報は機密度によって段階的に分類されており、どの同盟国がどの水準の機密をどの程度、米国より開示・移転されるかも階層的な序列構造を有している。高い序列でなければ、機密性の高い情報を継続的に与えられることがないのが実態である。この序列と米国の覇権システム全体における序列は概ね一致しており、米国が諜報同盟を結んでいる英国、カナダ、オーストラリア、ニュージーランドに特別の地位を与えていることは既に本稿の冒頭で述べた。

### 終わりに一日本の選択肢

現在、日米間には「相互協力及び安全保障条約」は存在しても、一般保全協定は締結されていない。当然、その付属文書である産業保全協定もない。筆者が本誌創刊号（2003年3月）の拙論で示したように、<sup>(15)</sup>基本的には、従来、日本政府は米国政府からの機密情報の開示・移転を個別の契約に伴う保全条項に基づきおこなってきた。近年、日本が米国から導入する兵器

・兵器システムに伴う機密情報が急増し、かつ、情報通信分野のシステム統合技術が重要な部分を占めるに至って、従来の個別契約方式では対処できなくなりつつある。システム統合技術は様々な個別技術、戦略・戦術データ、暗号情報技術を統合しているから、個別に分離して保全措置をとっても必ずしも有効ではなく、包括的な保全措置が必要となるからである。本来なら、日本は一般保全協定と産業保全協定を締結し、それらに基づき関連刑事法を改正すればよいのだが、歴代政権はこの国内法上の改正措置が政治的に困難とみて、二協定の締結を避けてきた。ただし、日本政府は米国から見た日本の機密保全体制の信頼性を高めるため、平成十四年（2002年）には、自衛隊法と「日米相互防衛援助条約等に伴う秘密保護法」を改正して機密漏洩に関する罰則を強化した。しかし、罰則強化だけでは移転実務手続きの詳細が依然として欠落したままであり、米国の軍事技術移転管理体制の多くの基準を満たしていないと思われる。

本誌創刊号の拙論で、筆者は二国間安全保障関連条約・協定体制を比較分析し、その視角から一般保全協定の重要性を指摘した。そこでは、日本が米国と多面的で強い同盟関係を有しながら、一般保全協定を締結していないために、システム統合技術や暗号技術情報などの移転に関する米国との覚書きが結ばれていないなど、英国を筆頭に米国が親密な関係を有する同盟国と比べて歪な対米同盟関係の構造を有することを明らかにした。他方、本稿では、米国の軍事技術移転管理に関する国内法令を精査し、同盟国への機密情報の開示・移転の審査・移転実務メカニズムを把握することによって、一般保全協定と産業保全協定とが米国の関連国内法令を有効に機能させるには不可欠であることを明らかにした。また、これら二協定と関連国内法令とが表裏一体の関係にあることを指摘した。

確かに、一般保全協定と産業保全協定は米国から軍事技術に関する機密情報の開示・移転を受けるための必要条件であり、決して十分条件ではない。<sup>(16)</sup> 開示・移転の是非は米国の政策判断であり、二協定を締結していても、是とされないことは十分ありえる。とはいえ、二協定が締結されていることは、米国との二国間同盟関係が極めて緊密であることを意味し、開示・

移転の可能性を高める。今後、日本政府が日米同盟の強化の是非を検討する際には、その議論の焦点として一般保全協定と産業保全協定の締結問題は避けることができないであろう。

(追記) 日本政府は米国政府と一般保全協定を締結する必要性を認識し、その具体的検討に入った。(『日本経済新聞』2006年1月5日。)

(註)

- (1) 拙論「米国の主要同盟国との二国間安全保障関連条約・協定体制の比較分析—軍事情報に関する一般保全協定 (GSOMIA)」『桃山法学』創刊号, 2003年3月。
- (2) Peter F. Verga, Deputy Under Secretary of Defense (Policy Support), Office of the United States Under Secretary of Defense for Policy, mimeo, October 31, 2000 <<http://www.dami.army.pentagon.mil/pub/dami-fa/10.31.2000.1300.ppt>>, accessed on May 14, 2005.
- (3) 拙論, 前掲, 収録資料を参照。
- (4) Arms Export Control Act, International Traffic in Arms Regulations, Presidential Executive Order 12356 (National Security Classification), Presidential Executive Order 12958 and 13292, National Security Decision Memorandum 119, National Industrial Security Operating Manual (DoD 5220.22-M), Security Assistance Management Manual (DoD 5105.38-M); “Fact Sheet: United States National Disclosure Policy” <<http://fpt.die.net/mirror/cryptome/us-ndp.htm>>, accessed on May 12; Verga, *op.cit.*; Industrial Security Letter <<http://www.dss.mil/isec/isl961.htm>>, accessed on May 14, 2005.
- (5) 拙論, 前掲。
- (6) 所定の目的通り米国製の軍事物資, 訓練, サービスが用いられているかどうかを監視するために, 最終用途監視 (EUM: the End-Use Monitoring) プログラムが存在する。国防総省のコードネームは Golden Sentry である。このプログラムによる監視対象は品目やサービスの誤用ないし不法な移転を防止する全ての行動を含み, 当該品目を移転の時点から廃棄の時点まで保護する。この監視プログラムは国防安全保障協力庁 (DSCA: Defense Security Cooperation Agency) がプログラムの全般的

な管理を行い、国防安全保障援助管理研究所（DISAM: Defense Institute of Security Assistance Management）、陸海空省とその外局、戦闘司令部、在外公館の駐在武官事務所や安全保障援助を任務とする外交代表部安全保障援助組織などが、窓口になり責任を分担している。See, Security Assistance Management Manual, DoD 5105.38-M.

- (7) 「軍事機密情報」とは、行政命令12958という国家安全保障上の利益のために保護することを要求される情報であって、国防総省もしくはその外局の管理もしくは管轄の下にある情報をいう。
- (8) 大統領行政命令12958によれば、米国に開示された外国政府ないし国際機関の機密情報に関しても、米国政府が開示国（機関）により元来付された機密分類を保つか、もしくは、開示国（機関）が当該機密に与えた保全措置と同程度の措置を与えねばならない。さらに、米国の当該機関は機密情報を開示した外国政府が要求する保全措置と同程度の保存措置を施す基準の下で外国政府の情報を保護しなくてはならない。
- (9) 最高機密 (top secret), 機密 (secret), 秘 (confidential)。
- (10) “Fact Sheet,” *op.cit.*, p. 2.
- (11) Verga, *op.cit.*,
- (12) 国家産業保全プログラム運用マニュアルは本来、軍事機密情報の保全を念頭に置いたものであるが、機密扱いを受けていない情報であっても規制されるかどうか注意を要する情報を伴う輸出にも言及している。  
また、米国の分類では機密指定を受けていない情報でも、NATOの「制限情報」からの引用・抜粋を含む情報については、「制限情報」として扱わねばならない。当然、NATOの機密指定を受けている情報は米国に機密指定を受けている情報として取り扱わねばならない。結果的に、NATOによって機密指定された情報を含む米国の資料は同じ情報を含む米国の資料よりも高い水準の保全措置や責任を求められることがある。
- (13) 拙著『軍事情報戦略と日米同盟—C4ISRによる米国支配』芦書房、2004年。
- (14) 例えば、日本へのイージス・システム関連技術の移転においてその弾道計算ソフトの移転に関する国防総省安全保障協力庁（DSC）と国務省政治・軍事問題局軍事貿易管理理事会（DDTC）との確執については、拙論「アーミテージ氏政権離脱が落とす影—イージス・システム日米研究の舞台裏」『時事 Top・Confidential』2005年7月5日号、p.6。
- (15) 拙論「米国の主要同盟国との二国間安全保障関連条約・協定体制の比較分析」、前掲。

- (16) 拙論「日米共同開発の限界—軍事技術提供に消極的な米国」『時事  
Top・Confidential』2005年6月24日, p.6。

参考資料

- ・“Classified Information” <[http://en.wikipedia.org/wiki/Classified\\_information#Restricted](http://en.wikipedia.org/wiki/Classified_information#Restricted)>.
- ・“Security Clearance” <[http://en.wikipedia.org/wiki/Security\\_clearance](http://en.wikipedia.org/wiki/Security_clearance)>