主 要 記 事 の 要 旨

軍事情報包括保護協定(GSOMIA)の比較分析

福 好 昌 治

① 米国はオーストラリア、フランス、イスラエル、インド等、六十数か国とGSOMIAを締結していると言われているが、そのすべてが公開されているわけではない。

② GSOMIAというのは、米国が各国と結んでいる秘密軍事情報の保護に関する二国間協定の総称である。GSOMIAは互換的な協定であり、米国から相手国に提供される秘密軍事情報だけでなく、米国へ提供される秘密軍事情報も保護の対象になる。

③ このうちオーストラリアやインドとのGSOMIAは比較的詳細な内容になっているが、その他の国とのGSOMIAは比較的簡素な内容になっている。

④ 各国のGSOMIAに共通する主な内容は以下のとおりである。

・受領国は提供国の承認なしに、提供される秘密軍事情報を第三国に提供しない。
・受領国は提供された情報に対して、提供国と同等の保護措置をとる。
・受領国は提供国の承認なしに、提供された情報を本来の目的以外に使用しない。
・受領国は提供された情報に含まれる特許権、著作権、企業秘密等の私権を尊重する。
・提供される情報には、文書、口頭で伝達される情報、映像等あらゆるものが含まれる。
・秘密情報の伝達は政府間のチャンネルで行う。
・契約企業とその施設も、秘密軍事情報取扱資格（セキュリティ・クリアランス）を取得しなければならない。
・提供国は受領国の秘密保護措置を査察するため、受領国の施設を定期的に訪問できる。

⑤ オーストラリアやインドとのGSOMIAには、個人に対するセキュリティ・クリアランスの規定があるが、その他の国とのGSOMIAには、そのような規定はない。一方の締約国が秘密軍事情報の保護に関する法令を改正した場合、すみやかに相手国に通知して、GSOMIAの改正について協議する、という条項の有無も相違点である。

⑥ 日米両政府は2007年８月に、GSOMIAを締結した。その背景には、日米軍事協力の進展や日米防衛企業の協力の進展がある。

⑦ 我が国とのGSOMIAは、オーストラリアやインドと同じくらい詳細な内容になっている。特に論点となる可能性のある条項は第７条と第18条、すなわち政府職員や契約企業従業員の秘密軍事情報取扱資格をどのような方法で付与するか、という問題である。現在の我が国の秘密軍事情報保護法制には、秘密軍事情報取扱資格の付与に関する規定はない。また、将来的には、罰則の強化も課題になるかもしれない。

軍事情報包括保護協定（GSOMIA）の比較分析

福　好　昌　治

（本稿は、外交防衛課が執筆を委託したものである。）

目　　次

はじめに

2005年10月29日に開催された日米安全保障協議委員会（２プラス２）で、いわゆる米軍再編に関する報告書『日米同盟：未来のための変革と再編』が公表された。その中に「情報共有及び情報協力の向上」という項目があり、「共有された秘密情報を保護するために必要な追加的措置をとる(1)」と書かれている。

この時点では、「追加的な措置」とは何か明記されていないが、2007年５月１日に開催された日米安全保障協議委員会（２プラス２）の共同発表文『同盟の変革―日本の安全保障及び防衛協力の進展』には、以下のように「追加的な措置」の内容が明記されている。

「軍事情報包括保護協定（General Security of Military Information Agreement, GSOMIA）としても知られる、秘密軍事情報の保護のための秘密保持の措置に関する両政府間の実質的合意。GSOMIAは、情報交換を円滑化し、情報並びに防衛装備計画及び運用情報の共有に資する情報保全のための共通の基礎を確立するものである(2)。」

つまり、「追加的な措置」とは、General Security of Military Information Agreement（GSOMIA（ジーソミア））の締結であった。このような経緯を経て、2007年８月10日、日米両政府はGSOMIA（正式名「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」）を締結した。

ところで、GSOMIAの締結に関しては、1988年５月17日の衆議院内閣委員会で取り上げられている。その際に、外務省の岡本行夫・北米局安全保障課長は「私どもは現在のやり方で十分である、我が国が軍事情報の保全のための一般的な協定を米国と結ぶつもりは全くないという方針で首尾一貫しておったということでございます(3)」と答弁している。

このような経緯があるにもかかわらず、なぜ政府は米国とのGSOMIAを締結したのであろうか。GSOMIAの締結によって、我が国の秘密保護体制はどう変わるのだろうか。こうした点を考察するためには、米国が我が国以外の国と結んでいるGSOMIAの内容を精査し、我が国とのGSOMIAと比較する必要がある。

久間章生・防衛大臣によると、米国は六十数か国とGSOMIAを結んでいる(4)というが、その内容は我が国ではほとんど紹介されていない(5)。そこで、本稿では米国が各国と締結して

---

(1)「日米同盟：未来のための変革と再編」の日本語訳は『朝雲』（自衛隊準機関紙）, 2005.11.3 に掲載されている。外務省のウェブサイト〈http://www.mofa.go.jp〉と防衛省のウェブサイト〈http://www.mod.go.jp.〉にも、正文である英語〈http://www.mofa.go.jp/region/n-america/us/security/scc/doc0510.html〉;〈http://www.mod.go.jp/j/news/youjin/2005/10/1029_2plus2/29_e.htm〉と日本語訳〈http://www.mofa.go.jp/mofaj/area/usa/hosho/henkaku_saihen.html〉;〈http://www.mod.go.jp/j/news/youjin/2005/10/1029_2plus2/29_03.htm〉が掲載されている。

(2)「同盟の変革―日本の安全保障及び防衛協力の進展」の日本語訳は『朝雲』2007.5.10 に掲載されている。外務省のウェブサイト〈http://www.mofa.go.jp〉と防衛省のウェブサイト〈http://www.mod.go.jp〉にも、正文である英語〈http://www.mofa.go.jp/region/n-america/us/security/scc/joint0705.html〉;〈http://www.mod.go.jp/j/news/youjin/2007/05/01e.html〉と日本語訳〈http://www.mofa.go.jp/mofaj/area/usa/hosho/2plus2_07_kh.html〉;〈http://www.mod.go.jp/j/news/youjin/2007/05/01j.html〉が掲載されている。

(3) 第112回国会衆議院内閣委員会議録第12号　昭和53年５月17日　p.2.

(4) 衆議院国際テロリズムの防止及び我が国の協力支援活動並びにイラク人道復興支援活動等に関する特別委員会における答弁（第166回国会衆議院国際テロリズムの防止及び我が国の協力支援活動並びにイラク人道復興支援活動等に関する特別委員会議録第２号　平成19年２月21日　p.4.）

(5) GSOMIAの具体例を紹介した文献は、松村昌廣『軍事情報戦略と日米同盟』芦書房, 2004だけである。同書では、米国とフランス、米国とイスラエルの間で締結されたGSOMIAの原文が紹介されているが、日本語訳は掲載されていない。

いるGSOMIAの具体例をくわしく紹介し、その後で、我が国とのGSOMIAの内容を検討し、それに伴う論点を考察する。

Ⅰ　我が国の秘密軍事情報保護法制

GSOMIAを理解するためには、まず、我が国の秘密軍事情報保護法制の現状を把握する必要がある。秘密軍事情報を保護する法律には、自衛隊法（昭和29年法律第165号）、日米相互防衛援助協定等に伴う秘密保護法（いわゆる「MSA秘密保護法」昭和29年法律第166号）、「日本国とアメリカ合衆国との間の相互協力及び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」（いわゆる「日米刑特法」昭和27年法律第138号）がある。

1　自衛隊法

自衛隊法では、第96条の２で防衛秘密の取り扱いを規定しており、第122条で秘密漏洩に関する罰則を定めている。これらの規定は2001年の自衛隊法改正で大きく変わった。

それまで、自衛隊の秘密には、MSA秘密保護法に基づく「防衛秘密」とそれ以外の自衛隊の秘密である「庁秘」（防衛庁の省移行に伴い「省秘」となった）の二種類しかなかったが、新たに庁秘のうち「我が国の防衛上特に秘匿することが必要であるもの」を「防衛秘密」と呼ぶことになった。これに伴い、従来の「防衛秘密」は「特別防衛秘密」と呼ばれることになった。つまり、自衛隊の秘密は、特別防衛秘密、防衛秘密、防衛秘密以外の庁秘の３種類になったのである。

さらに、特別防衛秘密は重要度に応じて、機密、極秘、秘の三つに区分される。防衛秘密は機密に指定されているものと、そうでないものの二つに区分される。防衛秘密以外の省秘は、機密、極秘、秘の三つに区分される。この中には、件数ゼロの秘密区分もあり得る。

この時の自衛隊法改正では、「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に、政令で定めるところにより、防衛秘密の取扱いの業務を行わせることができる」（自衛隊法第96条の２）という内容が追加され、防衛企業の従業員も法律に基づく防衛秘密の取扱者とされた。防衛秘密の漏洩に関する罰則は、従来の１年以下の懲役から５年以下の懲役に強化された。過失の場合は、１年以下の禁錮または３万円以下の罰金となる。防衛秘密の漏洩を共謀、教唆、煽動した者は３年以下の懲役となる。

2　MSA秘密保護法

MSA秘密保護法は、MSAに基づいて、米国から日本に提供された装備品等に関する秘密（特別防衛秘密）の保護を規定している。ここで言う「装備品等」とは、「船舶、航空機、武器、弾薬その他の装備品及び資材をいう」（第１条の２）とされており、「装備品等」以外の秘密、たとえば日米共同作戦計画の内容等は、MSA秘密保護法の対象にはならない。もちろん、「装備品等」以外の情報で、防衛秘密に該当するものは、自衛隊法第96条の２の対象となる。

特別防衛秘密の漏洩に関する罰則は、第３条で規定されており、①我が国の安全を害すべき用途に供する目的をもって、または不当な方法で、特別防衛秘密を探知し、または収集した者、②我が国の安全を害する目的をもって、特別防衛秘密を他人に漏らした者、③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、または領有した特別防衛秘密を他人にもらした者は10年以下の懲役となる。②、③以外の者が特別防衛秘密を他人にもらした場合は、５年以下の懲役となる。過失の場合は、２年以下の禁錮または５万円以下の罰金となる。

このようにMSA秘密保護法は、特別防衛秘密の取扱者だけでなく、それ以外の者も罰則の対象としている。また、前記①の行為の「陰謀

をした者」、「教唆又はせん動した者」は５年以下の懲役となり、前記②の行為の「陰謀をした者」、「教唆又はせん動した者は」３年以下の懲役となる（第５条）。

３　日米刑特法

日米刑特法第６条は在日米軍の秘密保護を規定している。同条１項は「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」となっている。機密漏洩も十年以下の懲役となる（同条２項）。第７条は第６条の陰謀罪を規定している。すなわち、第６条の罪の「陰謀をした者」、「罪を犯すことを教唆し、又はせん動した者」は、５年以下の懲役になる。

このように日米刑特法とMSA秘密保護法の罰則は、自衛隊法の罰則よりも重い。しかも、自衛隊法が秘密漏洩のみを罰則の対象としているのに対し、日米刑特法とMSA秘密保護法は、秘密の探知・収集（いわゆるスパイ行為）も罰則の対象にしている。自衛隊の秘密よりも米軍の秘密のほうが、厳重に保護されているのである。

以上の法律のほかに、自衛隊法施行令にも秘密保護規定があり、MSA秘密保護法施行令も制定されている。さらに、防衛省内部の規定として、秘密保全に関する訓令、特別防衛秘密の保護に関する訓令、防衛秘密の保護に関する訓令、秘密保全に関する達などがあり、秘密保全に関する措置はひととおり整備されている。

Ⅱ　GSOMIAの具体例

１　GSOMIAとは何か

GSOMIAというのは、米国が各国と結んでいる秘密軍事情報の保護に関する二国間協定の総称であって、各協定の名称は多少異なる。GSOMIAは互換的な協定であり、米国から相手国に提供される秘密軍事情報だけでなく、米国へ提供される秘密軍事情報も保護の対象になる。また、GSOMIAは秘密軍事情報全般を保護の対象にしており、研究開発に関する秘密だけを保護の対象にしたものや、特定の装備に関する秘密だけを保護の対象にしたものは、GSOMIAではない。

前述したように、米国は六十数か国とGSOMIAを締結していると言われているが、すべての存在が明らかになっているわけではない。米国務省が発行している条約・協定等のリストTreaties in Force 2007 によると、米国は以下の38の国々とGSOMIAを締結している。

アルゼンチン、オーストラリア、ブルガリア、チリ、コロンビア、チェコ、デンマーク、エクアドル、エジプト、エストニア、フィンランド、フランス、ギリシャ、ハンガリー、インド、イラン、アイルランド、イスラエル、イタリア、ラトビア、リトアニア、ルクセンブルグ、オランダ、ノルウェー、パキスタン、パナマ、ポーランド、ポルトガル、シンガポール、スロバキア、スロベニア、南アフリカ、スペイン、スウェーデン、タイ、ウクライナ、アラブ首長国連邦（UAE）、ベネズエラ

残る二十数か国の名前はわからない。しかし、米国、イギリス、カナダ、オーストラリア、ニュージーランドは「軍事情報の交換に関する了解覚書（Memorandum of understanding concerning multilateral exchange of military information）」を締結しており(6)、イギリス、カナダ、ニュージーランドとの間にも、GSOMIAが存在することは確実である。

イランとのGSOMIAは、親米のパーレビ政権時代である1974年に締結されており、現在は

(6)　*Treaties in Force 2007* に了解覚書の名称が掲載されている。TIAS（Treaties and Other International Acts Series）に掲載なし。

実質的な機能は果たしていないであろう。旧ソ連・東欧圏諸国とのGSOMIAは、冷戦終結後に締結されている。

2　オーストラリアとのGSOMIA

オーストラリアは米国と安全保障条約（ANZAS（アンザス）条約）を締結しており、両国は同盟関係にある。米国とオーストラリアは1962年に、「包括的情報保護協定（General Security of Information Agreement）」を締結した。この協定は2002年に改定され、「秘密情報の保護のための措置に関するオーストラリア政府とアメリカ合衆国政府との間の協定（Agreement between the government of Australia and the government of the United States of America concerning security measures for the protection of classified information）[7]」となった。

同協定は17条からなる。第１条は同協定の総論に相当する部分で、「各締約国は他方から直接的、間接的に受領した秘密情報を保護する」と規定している（以下、「　」内は条文の引用である）。

第２条は秘密情報の定義を規定している。すなわち、秘密情報とは、両国の国家安全保障上、保護する必要のある政府の秘密情報で、政府によって秘密区分された情報を指す。この秘密情報は、口頭、映像、電子、文書の形態、もしくは装備ないし技術の形態をとる。

第３条は秘密区分を規定している。米国の秘密区分は、秘密度の高いほうから順に、トップシークレット（機密）、シークレット（極秘）、コンフィデンシャル（秘）の三段階である。オーストラリアの秘密区分は、秘密度の高いほうから順に、トップシークレット、ハイリー・プロテクテッド（Highly Protected）、シークレット、プロテクテッド（Protected）、コンフィデンシャル、リストリクテッド（Restricted）の六段階になっている。

オーストラリアのトップシークレットは、米国のトップシークレットに相当する。オーストラリアのハイリー・プロテクテッドとシークレットは、米国のシークレットに相当する。オーストラリアのプロテクテッドとコンフィデンシャルは、米国のコンフィデンシャルに相当する。オーストラリアのリストリクテッドに相当する秘密区分は、米国にはない。しかし、「オーストラリア政府によってアドバイスされないかぎり、アメリカ政府はコンフィデンシャルと同様にこれを保護する」ことになっている。

同条Cによると、各締約国は相手国から受領したすべての秘密情報に、相手国の名前を記入することになっている。その際に、受領国は自国の秘密区分にしたがって、受領した秘密情報に秘密区分を付ける。その場合、提供国の秘密区分を下回るような秘密指定をしてはならないと規定されている。たとえば、米国からシークレットに区分された情報を提供された場合、オーストラリアはその情報をシークレット、ハイリー・プロテクテッド、トップシークレットのいずれかに指定しなければならない。

第４条は秘密情報の保護について規定しており、同協定の中で最も重要な条文である。「階級、地位、セキュリティ・クリアランス（秘密軍事情報取扱資格）だけでは、相手国から提供された秘密情報にアクセスできない。秘密情報にアクセスする必要があり、規定の基準に基づくセキュリティ・クリアランスを得ている者だけが、秘密情報にアクセスできる」。そのうえで、受領国は以下の事項を保障しなければならない。

A 受領国は、提供国の文書による事前の承認なしに、第三国の政府、個人、会社、機関、組織等に情報を提供しない。

B 受領国は、提供された情報に対して、提供国と同等の保護措置をとらなければならない。

(7)　TIAS 2208

C 受領国は、提供国の文書による事前の承認なしに、提供された情報を本来の目的以外に使用してはならない。

D 受領国は、提供された情報の中に含まれる特許権、著作権、企業秘密のような私権を尊重する。

E 提供された情報を取り扱う施設や官庁は、セキュリティ・クリアランスを得ている者を登録しておく。

F 提供された情報の配布や情報へのアクセスを管理するために、責任と管理に関する手続きを定めておく。

G 提供国が提供した情報の使用、開示、譲渡、アクセスに関して、追加の制限を課した場合、受領国はそれに従う。

第5条はセキュリティ・クリアランスについて規定している。「個人にセキュリティ・クリアランスを与えるかどうかの決定は、国家安全保障上の利益に基づいて行われる。具体的には、対象者の忠誠心、誠実さ、信頼度、性格に関するあらゆる情報に基づいて決定される」。さらに、締約国は、相手国のセキュリティ・クリアランス制度が適切かどうか、検査を行う。「提供国が秘密情報を相手国の代表に提供する前に、受領国は代表のセキュリティ・クリアランスを保障しなければならない」という規定もある。

第6条は契約企業への秘密情報の開示について規定している。「受領国は、契約企業が、秘密情報を保護する能力を有していることを保証しなければならない。受領国は、企業の施設に適切な秘密保護措置を与えなければならない。受領国は、秘密情報へのアクセスを要するすべての者に、適切なセキュリティ・クリアランスを与えなければならない。受領国は、秘密漏洩がないか、定期的に施設を検査しなければならない。秘密情報へのアクセスは、知る必要のある者に制限される」。このように第6条は、GSOMIAの対象が契約企業にも及ぶことを示している。

第7条は秘密情報の管理責任を規定している。輸送中の秘密情報の管理は、輸送している側が責任を持つ。

第8条は施設の責務について規定しており、締約国はすべての官庁、施設の秘密保護措置に責務を負うとされている。

第9条は秘密情報の保管について規定しており、「セキュリティ・クリアランスを得ている者のみがアクセスできるような方法で、秘密情報を保管しなければならない」と明記されている。

第10条は秘密情報の伝達について規定している。「秘密情報の伝達は、事前に文書で相互に承認した政府間のチャンネルを通じて行う」とされており、伝達手段についても細かく規定されている。たとえば、秘密文書は二重に密封された封筒で運び、内側の封筒にのみ秘密区分を明記する。最終受領者は受領書を発行し、送信者に送付する。電子的手段によって伝達される秘密情報は、暗号化したうえで送信する。

第11条と第12条は訪問に関する規定で、締約国は相手国の秘密保護措置を検査するために、相手国の官庁や施設を訪問できるとされている。

第13条は保護基準に関する規定で、「相手国から要求された場合、秘密保護の基準、手続き、実施要領に関する情報を提供する」とされている。また、「一方の締約国が秘密情報の保護に関する法律や規則を改正した場合、すみやかに相手国に通知する。その場合、両国は協定の改正を要するかどうか協議する」という規定もある。例えば、一方の締約国が秘密漏洩に関する国内法の罰則を変更した場合は、相手国にすみやかに通知し、協定を改正する必要があるかどうか協議することになる。

第14条は秘密情報のコピーについて規定している。「秘密情報を含む文書等をコピーした場合は、オリジナルの保全マークをコピーにも付ける。コピーに関しても、オリジナルの資料と同様の保護措置を採る。コピーの数は必要最小

限とする」。

第15条は秘密情報の破棄について規定している。「相手国から受領した秘密情報を含む文書等は、焼却、裁断、パルプ化等の秘密情報の再生を防げる方法で破棄する」。

第16条は秘密区分の変更と秘密解除について規定している。「提供国は、秘密区分の格下げや秘密指定の解除に関する裁量権を持つ。受領国は提供国の文書による事前の同意なしに、提供された秘密情報のランクを下げてはならない」。

第17条は紛失または漏洩について規定している。「秘密情報の紛失や漏洩（その可能性も含む）が発生した場合、受領国はただちに提供国に通知し、捜査を開始する。受領国は捜査結果や再発防止措置を提供国に通知する」。

第18条は論争に関する規定で、締約国間で協定に関して見解の不一致が生じた場合、協議を通じて解決するとされている。法廷闘争には持ち込まないことも明記されている。

第19条は費用に関する規定で、協定の実施に要した費用は、両国で負担するとされている。

第20条と第21条は協定の発効、改正、終了に関する規定で、協定の有効期限は25年、以降は５年ごとに自動延長される。なお、第21条には、「この協定は、米国の原子力エネルギー情報のように、特別な協定で規定されている情報には適用されない」という規定もある。

以上のように、オーストラリアとのGSOMIAは、公開されているGSOMIAの中では、詳細な規定を有するものになっている。

3　フランスとのGSOMIA

フランスはNATO（北大西洋条約機構）加盟国であるが、米国と一定の距離を保つ独自の外交を展開している。フランスとのGSOMIAである「秘密情報の保護協定（Protection of Classified Information Agreement）[8]」は、1977年に締結された。同協定は８条から成り、オーストラリアとのGSOMIAと比べて簡素な構成になっている。

同協定の核心的な部分は第１条で、秘密情報の保護に関する原則を規定している。その内容は以下のとおりである。

「a 受領国は、提供国の承認なしに、第三国政府に情報を提供しない。
b 受領国は、提供された情報に対して、提供国と同等の保護措置をとる。
c 受領国は提供された情報を、本来の目的以外に使用しない。
d 受領国は、提供された情報に含まれる特許権、著作権、企業秘密のような私権を尊重する。
e 提供された秘密情報が漏洩した場合（その可能性も含む）、受領国は迅速かつ詳細な方法で相手国に通報する。」

aの「提供国の承認なしに」という部分は、オーストラリアとの協定では「提供国の文書による事前の承認なしに」とより厳密な規定になっている。

第２条は「秘密情報・資料は政府間でのみ伝達する」と規定している。

第３条は、提供される秘密情報には、口頭で伝えられた情報、映像、資料等すべての情報が含まれることを規定している。

第４条は保護措置について規定しており、受領国は、提供された情報に対して、提供国と同等の保護措置をとらなければならない、とされている。

第５条は同協定の例外を規定しており、「別の秘密保護協定に基づいてすでに秘密指定されている情報に対しては、この協定は適用しない」となっている。「別の秘密保護協定」の例として、「産業保全協定（Industrial Security Arrangement）」が明記されている。

第６条は秘密保護専門家の相互訪問を規定し

(8)　TIAS 8914

ており、相手国の秘密保護措置が適切かどうかを調べるために、定期的に訪問することになっている。その場合、受領国政府は専門家の訪問を支援することになっている。

第７条は、国防省の仕事を受注した契約企業に秘密情報を提供する場合の規則を定めている。この場合、受領国政府は以下のことを保証しなければならない。

・契約企業が適切な秘密保護能力を有していること。
・契約企業の施設に適切な保全措置がとられていること。
・秘密情報へのアクセスを要するすべての者が、適切なセキュリティ・クリアランスを得ていること。
・秘密情報へアクセスできるすべての者に、秘密保護の責務を有していることを自覚させること。
・施設の秘密保護措置に関して、定期的な検査を行うこと。
・公用のために知る必要がある人に、秘密情報へのアクセスを制限すること。

第８条は査察に要する費用負担について規定している。

以上のように、フランスとの協定はオーストラリアとの協定に比べて、簡素なものになっている。

たとえば、フランスとの協定には、秘密区分が明記されていない。米国の場合、秘密区分はトップシークレット、シークレット、コンフィデンシャルの三区分になっているが、フランスの場合、どうなっているのか不明である。

また、フランスとの協定には、政府職員のセキュリティ・クリアランスに関する規定がない。契約企業従業員のセキュリティ・クリアランスについて規定されているだけである。秘密情報の伝達方法も簡単にしか規定されていない。輸送中の秘密情報に関する管理責任も規定されていないし、伝達方法についての詳細な規定もない。秘密保護に関する国内法を改正した場合、すみやかに相手国に通知するという規定、秘密情報のコピーや破棄の方法に関する規定、秘密区分の変更や秘密解除に関する規定、両締約国間で見解の不一致が生じた場合の規定もない。

4　イスラエルとのGSOMIA

イスラエルは米国と安全保障条約を締結してはいないが、実質的に米国と極めて密接な関係にある。イスラエルとのGSOMIAである「情報保護包括協定（General Security of Information Agreement）[9]」は、1982年に締結されているが、同協定の前文によると、1963年にジョンソン米国務長官とイスラエルのハーマン駐米大使が「秘密情報の保護に関する覚書（notes）」を交わしている。しかし、同協定の脚注で、「（この覚書は）印刷されていない」と書かれているので、この覚書は非公開になっていると思われる。

同協定の前文で、米国の秘密区分として、トップシークレット、シークレット、コンフィデンシャルの三段階が明記されているが、イスラエルの秘密区分は明記されていない。イスラエルでは、秘密区分そのものが秘密なのかもしれない。

同協定の本文は９条から成る。第１条は以下のような秘密保護の原則を規定している。

「a 受領国は、提供国の承認なしに、第三国等に情報を提供しない。
 b 受領国は、提供された情報に対して、提供国と同等の保護措置を採る。
 c 受領国は、提供された情報を本来の目的以外に使用しない。
 d 受領国は、提供された情報の中に含まれる特許権、著作権、企業秘密のような私権を尊重する。」

第２条は秘密情報の伝達方法を規定してお

(9)　TIAS 10617

り、「秘密情報・資料は政府間でのみ伝達し、適切なセキュリティ・クリアランスを得ている者だけが伝達する」となっている。

第３条は提供される秘密情報・資料の種類を規定しており、文書、口頭による伝達、映像等あらゆるものが含まれる。資料には、文書、メモ、ハードウェア、装置、写真、記録装置、コピー、地図、書簡等が含まれるが、これらに限定されない。

第４条は提供された情報に対して、提供国と同等の保護措置を採ることを規定しているが、これは第１条ｂと同じ内容である。

第５条は協定の適用範囲を規定している。「この協定は、両政府の全省庁と承認された全当局者によって行われる、すべての秘密情報の交換に適用される」。伝達経路に関する詳細事項は、産業保全協定のような専門的な取り決めで規定される。

第６条は秘密保護専門家の相互訪問を規定しており、相手国の秘密保護措置が適切かどうかを調べるために、定期的に訪問することになっている。この際、受領国政府は専門家の訪問を支援する。

第７条は秘密漏洩に対する処置を規定しており、「提供された秘密情報を紛失したり、承認されていない者に開示された場合（その疑いがある場合も含む）、受領国政府は必ず調査を実施する。受領国政府は事案の詳細、調査結果、再発防止策を迅速に提供国政府へ知らせる」ことになっている。

第８条ａは、政府または政府と契約した企業が、相手国の領域内で、秘密情報に接する仕事を行う場合の措置を規定している。この場合、仕事を行う地域の政府が、自らの基準に従って、秘密保護措置を講ずることになる。たとえば、イスラエルの企業が米国で仕事をする場合は、米国の秘密保護措置に従わなければならない。

第８条ｂは契約企業に秘密情報を開示する前に、受領国政府が行う責務について規定している。その責務は以下のとおりである。

「⑴契約企業とその施設が秘密情報を適切に保護する能力を有していることを保証する。
⑵契約企業の施設に対して、適切なセキュリティ・クリアランスを与える。
⑶職務上、秘密情報へのアクセスを要するすべての人に、適切なセキュリティ・クリアランスを与える。
⑷秘密情報にアクセスするすべての人に、法律に従い、情報を保護する責務があることを自覚させる。
⑸セキュリティ・クリアランスを与えられた施設に対して、定期的な検査を実施する。
⑹秘密情報へのアクセスは、知る必要のある人に限定する。秘密情報へのアクセスを含む施設訪問は、当該国政府省庁の承認を要する。この要求は、米国の場合、テルアビブにいるアメリカの駐在武官を通じて提出し、イスラエルの場合、米国にいるイスラエルの駐在武官ないし調達派遣団を通じて行う。要求書には、訪問者の地位とセキュリティ・クリアランスの証明書、訪問目的を明記する。要求された政府は、企業への勧告と訪問の承認に責務を負う。」

第９条は査察に要する費用負担について規定しており、費用は返済しないことになっている。

5　NATO諸国とのGSOMIA

⑴　イタリアとのGSOMIA

NATO加盟国で、国内に多数の米軍基地を有するイタリアは、1964年に米国と「秘密情報保護協定（Safeguarding of Classified Information Agreement）[10]」を締結した。同協定は本文と「包括保護手続きに関する添付書類（Annex of General Security Procedures）」から成るが、本文は条項に分かれておらず、一つの文章になってい

⑽　TIAS 5629

る。本文の主な内容は以下のとおりである。

「両国政府は、1950年1月6日の北大西洋協議会で承認されたNATO（北大西洋条約）加盟国による秘密保護協定と、1955年3月2日の北大西洋協議会で承認された秘密保護に関する最小限基準と同様の原則に基づいて、秘密情報の保護措置を適用する」。ここで明らかなように、NATOは独自の秘密保護協定を締結しているが、その内容は明らかになっていない。

同協定本文では、提供された秘密情報の取り扱いに関し、以下のような原則が明記されている。

「a 受領国政府は、提供国の承認なしに、第三国政府に情報を提供しない。
b 受領国政府は、提供された情報に対して、提供国と実質的に同じ保護措置を採る。
c 受領国政府は、提供された情報を本来の目的以外に使用しない。
d 受領国政府は、提供された情報の中に含まれる特許権、著作権、企業秘密のような私権を尊重する。」

続いて、この協定でカバーされる情報には、文書、覚書、見取図、写真、計画書、模型、仕様書、デザイン、それらの原案等、広範なものが含まれることが明記されている。伝達手段に関しても、口頭、映像、文書によるものすべてが含まれる。装備や資料の伝達も含まれる。

秘密区分に関しては、「アメリカ政府によって、トップシークレット、シークレット、コンフィデンシャルに指定された情報に適用されるが、秘密の原子力エネルギー情報のように、特別な協定を要する情報には適用されない」とされており、イタリア側の秘密区分は、トップシークレット、シークレット、ハイリー・コンフィデンシャル（Highly Confidential）、コンフィデンシャルの4区分になっている。

契約企業への秘密情報の開示については、添付資料で規定されている。その内容は以下のとおりである。

「相手国政府の国内で、他方の政府と契約した企業が仕事をする場合、相手国政府が秘密保護措置に責務を負う」。たとえば、イタリアの企業が米国内で、米国から提供された秘密情報に接する仕事を行う場合、米国の秘密保護措置に従わねばならない。

「契約企業にコンフィデンシャル以上の秘密情報を開示する前に、政府は、職務上、秘密情報へのアクセスを要する全従業員と当該企業の施設に適切なセキュリティ・クリアランスが与えられていることを保証しなければならない」。

添付資料には、以下のような政府の責務も明記されている。

・受領国政府は、秘密情報に接するすべての者に、法律に従って、秘密情報を保護する責務があることを自覚させなければならない。
・受領国政府は秘密情報を取り扱っている施設に対して、秘密保護措置に関する検査を実施する（この検査は、定期的なものとは書かれていない。提供国政府が受領国の施設を査察するという規定もない）。
・受領国政府は、業務上知る必要がある人に、秘密情報へのアクセスを制限していることを保証しなければならない。秘密情報を扱っている施設への訪問は、政府に申請しなければならず、訪問者のセキュリティ・クリアランスを要する。

添付資料には、「情報や資料は政府間でのみ伝達する」という規定もある。

イタリアはNATO加盟国で、米国と同盟関係にあるが、その割にはイタリアとのGSOMIAは比較的簡素な内容になっている。NATOの秘密保護協定があるため、個別の協定で詳細な事項を定める必要がないのかもしれない。

⑵ ノルウェーとのGSOMIA

ノルウェーはNATO加盟国であるが、国内に常設の米軍基地はない。ノルウェーと米国のGSOMIAである「秘密情報保護協定（Safeguarding of Classified Information Agreement）[11]」は、

1970年に締結された。イタリアと米国間のGSOMIAと同様に、ノルウェーとのGSOMIAも、本文と添付資料から成り、本文は条項に分かれていない。内容も以下の部分が追加されている以外は、イタリアとの協定とまったく同じである。

「両締約国政府は、双方に便利な時、提供された秘密情報保護措置について、受領国の秘密保護担当者と論議するために、提供国の秘密保護専門家の定期的な訪問を認める。提供国政府の秘密保護専門家が、提供した秘密情報が適切に保護されているかどうかを判断するにあたって、受領国政府は提供国の専門家を支援する」。

ノルウェーの秘密区分は、米国と同様に、トップシークレット、シークレット、コンフィデンシャルの三区分になっている。

⑶　デンマークとのGSOMIA

デンマークもNATO加盟国であるが、国内に米軍基地はない。デンマークとのGSOMIAである「軍事情報保護協定（Security of Military Information Agreement）[12]」は1981年に締結された。協定文はイタリアやノルウェーとのGSOMIAよりも長くなっているが、条項には分かれていない。添付資料もない。協定の主な内容は以下のとおりである。

・受領国は、提供国の同意なしに、提供された情報を第三国等に開示しない。
・受領国は、提供国と同等の秘密保護措置を採る。
・受領国は、提供された情報を本来の目的以外に使用しない。
・受領国は、特許権、著作権、企業秘密のような私権を尊重する。
・秘密情報は政府間でのみ伝達する。適切なセキュリティ・クリアランスを得ている者だけが、秘密情報にアクセスできる。
・秘密情報には、文書、口頭で伝えられた情報、映像等、あらゆる形態のものが含まれる。
・受領国政府は提供国の保全専門家の定期的な査察を承認し、支援する。
・提供された秘密情報が紛失したり漏洩した場合、受領国政府はその詳細を迅速に提供国政府に通知し、捜査結果と再発防止策を伝える。
・提供された情報を契約企業に開示する場合、受領国政府は、契約企業とその施設が適切な秘密保護能力を有していることを保証しなければならない。情報は知る必要のある者にのみ提供し、その者はセキュリティ・クリアランスを取得しなければならない。施設への定期的な査察も実施する。

なお、同協定には、デンマークの秘密区分は明記されていない。

6　アジア諸国とのGSOMIA

⑴　タイとのGSOMIA

タイには、米軍基地はないが、米タイ共同演習「コブラ・ゴールド」が毎年実施されており、両国は軍事面で密接な関係にある。タイとのGSOMIAである「軍事情報保護協定（Security of Military Information Agreement）[13]」は、1983年に締結された。

同協定は９条から成る。第１条は他の協定と同様に、以下のような原則を規定している。

「a 受領国政府は、提供国政府の承認なしに、提供された情報を第三国の政府等に開示しない。
b 受領国政府は、提供国と同等の秘密保護措置を採る。
c 受領国政府は、提供された情報を本来の目的以外に使用しない。
d 受領国政府は、特許権、著作権、企業秘密のような私権を尊重する。」

第２条は伝達方法を規定しており、適切なセ

⑾　TIAS 6836
⑿　TIAS 10109
⒀　TIAS 10678

キュリティ・クリアランスを得ている政府職員の間だけで、秘密軍事情報の伝達を行う。

第３条は秘密軍事情報の範囲を規定しており、文書、口頭で伝達された情報、映像情報等あらゆるものを含む。

第４条は秘密区分の指定を規定しており、提供された秘密軍事情報は提供国と同等の秘密区分に指定する。

第５条は例外規定で、同協定は既存の秘密保護協定で保護されている情報には適用されない。

第６条は査察に関する規定で、受領国政府は提供国政府による定期的な査察を許可し、支援しなければならない。

第７条は紛失ないし漏洩に関する規定で、そのような事案が発生した場合（疑いのある場合も含む）、受領国政府は当該事案の詳細を迅速に相手国政府に通知し、捜査結果と再発防止策も通知しなければならない。

第８条は秘密軍事情報にアクセスする契約企業について規定している。その概要は以下のとおりである。

・受領国の契約企業が提供国の国内で業務に従事する場合、提供国の秘密保護規定に従う。
・受領国政府は、契約企業とその施設が適切な秘密保護能力を有していることを保証しなければならない。
・受領国政府は、契約企業の施設に適切なセキュリティ・クリアランスを与えなければならない。
・受領国政府は、秘密軍事情報にアクセスする必要のある者全員に、適切なセキュリティ・クリアランスを与えなければならない。
・受領国政府は、秘密軍事情報にアクセスできる者全員に、秘密保護の責務を有していることを自覚させねばならない。
・受領国政府は、契約企業の施設に対して、定期的な査察を実施する。
・秘密軍事情報へのアクセスは、職務上知る必要のある者に制限する。秘密軍事情報を扱っている施設への訪問には、受領国政府の承認を要する。訪問者はセキュリティ・クリアランスを取得しなければならない。

第９条は査察の費用負担について規定している。

なお、同協定には、タイ側の秘密区分は記載されていない。

⑵　シンガポールとのGSOMIA

シンガポールは小さな島から成る都市国家だが、国内に米軍基地があり、米軍との共同演習も実施されている。シンガポールとのGSOMIAである「軍事情報保護協定（Security of Military Information Agreement）[14]」は、1983年に締結された。その内容はタイとのGSOMIAと同じである。シンガポールの秘密区分は明記されていない。

⑶　インドとのGSOMIA

インドは冷戦時代には、米国よりもソ連と密接な関係にあったが、近年、安全保障面でも急速に米国との関係を強化している。インドとのGSOMIAである「秘密軍事情報の保護措置に関する米国・インド間の協定（Agreement between the United States and India Concerning Security Measures for the Protection of Classified Military Information）[15]」は、2002年に締結された。同協定は23条から成り、他国の協定よりかなり長い。以下、主要な部分を紹介する。

・締約国は秘密軍事情報の保護に影響を与える法令を改正する場合、相手国に通知し、同協定の改正について協議する（第２条）。
・インドの秘密区分は、トップシークレット、シークレット、コンフィデンシャル、リストリクテッド（restricted）の４区分で、リストリクテッドもアメリカのコンフィデンシャル

⑭　TIAS 10819
⑮　TIAS 記載なし、CTIA（Consolidated Treaties & International Agreements）10138.000

に相当する。秘密文書には、口頭で伝達された情報、映像、電子、磁気、文書等あらゆる形の情報が含まれる（第３条）。

・業務上、秘密軍事情報にアクセスする必要があり、セキュリティ・クリアランスを得ている者だけに、秘密軍事情報へのアクセスが認可されている。受領国は、提供国の文書による事前の承認なしに、第三国の政府、個人、企業、機関、組織等に情報を提供しない。受領国は、提供された情報に対して、提供国と同等の保護措置を採らなければならない。受領国は、提供国の文書による事前の承認なしに、提供された情報を本来の目的以外に使用してはならない。受領国は、提供された情報の中に含まれている特許権、著作権、企業秘密等の私権を尊重する。秘密軍事情報を取り扱う施設や官庁は、セキュリティ・クリアランスを得ている者を登録しておく（第５条）。
・セキュリティ・クリアランスを与えるかどうかの決定は、対象者の忠誠心、誠実さ、信頼度、性格に関するあらゆる情報に基づいて行われる（第６条）。
・締約国はセキュリティ・クリアランスを得ている者に対する調査を実施する（第７条）。
・秘密軍事情報を取り扱っている施設、官庁への相手国代表の訪問は、両国間の協力的防衛活動を促進するために必要な範囲に限定される（「両国間の協力的防衛活動を促進するために必要な範囲」という表現は、他国のGSOMIAには見られない）。訪問要求はそれぞれの駐在武官室を通じて行う（第９条）。
・締約国は輸送中および保管中の情報の保護にも責任を負う（第10条）。
・秘密軍事情報の伝達は政府間のチャンネルを通じて行う。秘密文書は二重に密封された封筒で運び、外側の封筒には秘密区分を明記しない。最終受領者は受領書に署名し、送信者に送付する。電子的手段によって伝達される秘密情報は、暗号化したうえで伝達する（第13条）。
・秘密情報の破棄は、焼却、裁断、パルプ化等、秘密情報の再生を防止できる方法で行う（第16条）。
・秘密情報を含む文書等をコピーした場合、オリジナルと同じ保全マークを付ける。コピーの数は必要最小限とする（第18条）。
・秘密軍事情報の翻訳も、セキュリティ・クリアランスを得ている者によって行う（第19条。このような条項はインドおよび日本とのGSOMIAにのみ存在する）。
・インドの政府系法人を含む契約企業に秘密軍事情報を提供する前に、受領国は、契約企業が秘密保護能力を有していること、当該施設が適切なセキュリティ・クリアランスを得ていること、情報へのアクセスを要する者全員が適切なセキュリティ・クリアランスを得ており、秘密保護の責務を自覚していること、当該施設に対する定期的な査察を実施すること、秘密情報へのアクセスを知る必要がある者に限定していることを保証しなければならない（第20条）。
・秘密軍事情報の紛失または漏洩が発生した場合（その可能性がある場合も含む）、ただちに相手国に知らせ、受領国は捜査を開始する。また、捜査結果と再発防止策を相手国に通知する（第21条）。

以上のように、インドとのGSOMIAは、オーストラリアとのGSOMIAと同じぐらい詳細な規定になっている。その背景には、近年の米印軍事協力の進展がある。ただし、インドはいまでもロシア製兵器の調達を続けているので、米国とインドが同盟関係になったとまでは言えない。したがって、両締約国の緊密度（同盟関係かどうか）とGSOMIAの詳細度は、必ずしも比例しないと言える。

⑷　パキスタンとのGSOMIA

インドと長年対立しているパキスタンは、米国の同盟国ではないが、冷戦時代は米国から軍事援助を得ていた。パキスタンとのGSOMIA

である「軍事情報保全協定（Security of Military Information Agreement）[16]」は、1982年に締結された。同協定は9条から成り、主要部分は以下のとおりである。

受領国は、提供国の承認なしに第三国に情報を提供しない。受領国は、提供された情報に対して、提供国と同等の保護措置を採る。受領国は本来の目的以外に情報を使用しない。受領国は情報の中に含まれる特許権、著作権、企業秘密等の私権を尊重する（第1条）。

秘密軍事情報の伝達は、適切なセキュリティ・クリアランスを得ている政府関係者だけで行う（第2条）。秘密軍事情報には、文書、口頭で伝達された情報、映像等、あらゆる情報が含まれる（第3条）。

締約国は相手国政府の秘密保護専門家の定期的査察を承認し、支援する（第6条）。提供された秘密軍事情報の紛失または漏洩が発生した場合（その疑いがある場合も含む）、受領国政府は捜査を行う。受領国政府は迅速かつ詳細に、当該事案の内容を提供国政府に通知する。捜査結果と再発防止策も通知する（第7条）。

契約企業が相手国の国内で仕事をする場合、相手国政府が秘密保護の責務を負う。政府は、秘密軍事情報を契約企業に開示する前に、契約企業とその施設が秘密保護能力を有しており、施設と秘密情報へのアクセスを必要とする者全員が、セキュリティ・クリアランスを得ていることを保証しなければならない。政府は、その施設に対して、定期的な査察を実施する。秘密情報へのアクセスは、知る必要のある者に限定する。施設への訪問には、政府の事前認可を要する（第8条）。

7　各GSOMIAの共通点と相違点

これまでに紹介したGSOMIAは、大きく二つに分類できる。一つはオーストラリアやインドとのGSOMIAのように、比較的詳細なGSOMIAである。もう一つはその他の国とのGSOMIAのように、比較的簡素なGSOMIAである。両方に共通する主要項目は以下のとおりである。

・受領国は提供国の承認なしに、提供された情報を第三国に提供しない。
・受領国は提供された情報に対して、提供国と同等の保護措置を採る。
・受領国は提供国の承認なしに、提供された情報を本来の目的以外に使用しない。
・受領国は提供された情報の中に含まれる特許権、著作権、企業秘密等の私権を尊重する。
・提供される情報には、文書、口頭で伝達される情報、映像等、あらゆるものが含まれる。
・秘密情報の伝達は政府間のチャンネルで行う。
・契約企業とその施設も、セキュリティ・クリアランスを取得しなければならない。
・提供国は受領国の秘密保護措置を査察するために、受領国の施設を定期的に訪問できる。
・秘密情報の紛失または漏洩が起きた場合、受領国は迅速に提供国に通知し、捜査結果と再発防止措置も通知する。

相違点は、個人に対するセキュリティ・クリアランスの規定があるかないか、という点である。オーストラリアやインドとのGSOMIAには、「個人にセキュリティ・クリアランスを与えるかどうかの決定は、対象者の忠誠心、誠実さ、信頼度、性格に関するあらゆる情報に基づいて決定される」という規定があるが、その他の国のGSOMIAには、このように明確な規定はない。「一方の締約国が秘密保護に関する法令を改正した場合、すみやかに相手国に通知し、GSOMIAの改正を要するかどうか協議する」という項目があるかどうかも、相違点の一つである。

---

⑯　TIAS 10455

Ⅲ　日米間のGSOMIA

1　なぜ、GSOMIAが必要なのか

これまで、米国から我が国に装備を提供したり、日米共同研究・開発を行う場合、MSA秘密保護法に基づく個別の取決め（実施取極、実施細則、細目取極、覚書等）が、その都度締結されてきた。この方式でも大きな不都合は生じていない。では、なぜ、GSOMIAが必要になったのだろうか。

その主たる要因は、日米防衛企業の協力関係の進展である。近年、ミサイル防衛システムの日米共同開発等で、装備の開発に関する両国の連携が急速に進んでいる。また、北朝鮮の動向監視等、自衛隊と米軍の共同作戦も進展している。さらに、イラクへの自衛隊の派遣等に見られるように、国際平和協力活動での日米協力も進展している。これに伴い、米国から提供される秘密軍事情報も増えている（例えば、北朝鮮のミサイル基地を撮影した偵察衛星の情報やテロ組織の動向に関する情報等である）。

当然、こうした秘密軍事情報を保護する規定も必要になる。その場合の規定として、個別の秘密保護取極だけでなく、GSOMIAも必要とする理由について、松村昌廣・桃山学院大学教授は、「現在、日米の軍事技術協力は個別の兵器やプラットフォームをめぐる水準からコンピューター情報通信技術を中心にシステム統合技術を含む水準に達している。この水準では、様々な個別技術、戦略・戦術データ、暗号情報技術が統合・融合され、全ての秘密は相互に密接に関連しているから、どうしても包括的な秘密保全が必要になる[17]」と説明している。

また、宝珠山昇・元防衛施設庁長官はGSOMIAを必要とする理由として、「GSOMIAが締結されていないことは、米国では、日本の機密情報保護体制が他の締約国より弱いものと受け取られ、日本との機密情報の交流・共有の検討・審理にあたって懸念する論議を招きやすくしている[18]」と指摘している。最近、イージス・システムに関する秘密情報が、自衛官ではあるが取扱資格のない者にまで広がっていることが明らかになるなど、自衛隊の秘密漏洩事案が何度も発生している。こうした事案に対する米国の懸念を払拭するために、GSOMIAが必要になったとも言えるであろう。

さらに、宝珠山は以下のような理由も挙げている。

「核・生物・化学兵器やミサイル、即ち、大量破壊兵器の拡散等によってもたらされる無差別で突発性の高い脅威への対応措置の複雑・困難さは、研究、開発、生産、運用、修理、備蓄、補給、訓練などにおいて、先進諸国及び官民が緊密に協力する対応体制（多層のネットワーク）の構築を必要としており、民間企業も含めた機密情報の交流・共有体制の向上が緊要となっている。例えば、現在米国まで運んで行っている『ブラックボックス』の修理を日本で行えるようにして、整備や補給を効率化し、共同の訓練や作戦の効率も高めるためには、日本企業がセキュリティ・クリアランスを取得し得る基盤を日本国政府が提供（即ちGSOMIAを締結）しなければならない[19]」。米国からの受注を拡大するためには、GSOMIAが必要ということである。

GSOMIAの締結には、米国内の手続きをスムーズにさせるという効果もあるようだ。この点に関して、久間章生・衆議院議員（初代防衛大臣）は以下のように述べている。

「米国側の事情を推察すると、GSOMIAという取決めを各国と結んでいるわけですから、

---

⑰　前掲注(5), p.99.

⑱　宝珠山昇「日米軍事情報保護協定（GSOMIA）」『RIPS' Eye』No. 57, 2006.1.20, pp.1-2.平和安全保障研究所のウェブサイト〈http://www.rips.or.jp/Institute/rips_eye_no57.html〉

⑲　同上

『GSOMIAの枠組みで秘密が守られているから、日本にも供与する』といえば、米国政府内の行政手続が進みやすい、というのは理解できます。会社の方はよくお分かりだと思いますが、普通の取引でも、一々契約内容を詰めるより、統一契約書でやったほうが、社内審査が楽でしょう[20]」。ただし、GSOMIAが締結されても、個別事案ごとの協議に要する時間が短縮されるだけで、個別事案ごとの秘密保護取極が不要になるわけではない[21]。

2　協定の具体的内容

日米両政府は2007年8月10日、日米間のGSOMIAである「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（Agreement Between the Government of Japan and the Government of the United States of America Concerning Security Measures for the Protection of Classified Military Information）」を締結した。同協定は19条から構成されており、その主要部分は以下のようになっている。

第1条は用語の定義で、「秘密軍事情報は、口頭、映像、電子、磁気若しくは文書の形態又は装備若しくは技術の形態をとることができる」とされている。

第2条は、各締約国は受領した秘密軍事情報を本協定の規定が国内法令に合致する限りで保護することを規定している。これは、新規立法は不要という我が国政府の説明とも一致する規定だが、他方で締約国による国内法令の自発的な制定・改正も可能とも読める。この点に関連して、久間章生・防衛大臣は2007年5月15日、衆議院安全保障委員会で、「（国内の立法措置）は必ずしもとらなければならないということじゃなくて、これから先そういうようなことでやったときに、現在の国内法で守られているような体制だけでいいかどうか、そういうのを含めて、むしろ国内で検討がされるべきじゃないかと思うんです[22]」と答弁している。

第3条は国内法令の変更で、「一方の締約国政府は、この協定の下で秘密軍事情報の保護に影響を及ぼす自国の国内法令のいかなる変更についても、他方の締約国政府に対し通報する。この場合には、両締約国政府は……この協定の可能な改正につき検討するために協議する」と規定されている。例えば、我が国が秘密漏洩に関する罰則を変更した場合は、米国に通報し、協定の改正が必要かどうか協議しなければならない（罰則を変更すれば、必ず協定を改正しなければいけないということではない）。

第4条は秘密区分を規定している。米国の秘密区分は単純で、秘密度の高いほうから順にトップシークレット、シークレット、コンフィデンシャルの三つに区分されている。これに対し、日本の秘密区分は以下のように複雑な規定になっている。

「自衛隊法に従って、『防衛秘密』に指定される秘密軍事情報は、『防衛秘密』と表示され、『防衛秘密』に指定されない他の秘密軍事情報は、当該情報の機微の程度に従って『機密』、『極秘』、又は『秘』と表示される。

『防衛秘密』であって追加的な表示である『機密』が付されるものには、合衆国の“Top Secret”と同等の保護が与えられる。『防衛秘密』には、合衆国の“Secret”と同等の保護が与えられる」

本稿の「Ⅰ　我が国の秘密保護法制」で説明したように、2001年の自衛隊法改正で「防衛秘密」という新しい概念が設定されたために、このようにわかりにくい秘密区分になった。

まとめてみると、日本側の秘密軍事情報は①

---

⑳　2005年度第6回日米安全保障戦略会議における基調講演、2005.11.11, 安全保障議員協議会のウェブサイト〈http://www.ja-nsrg.or.jp/kyuma11.pdf#search= ‘GSOMIA’〉

㉑　前掲注⑱

㉒　第166回国会衆議院安全保障委員会議録第9号　平成19年5月15日　p.8.

防衛秘密であり、かつ機密に指定されている情報、②防衛秘密であるが、機密には指定されていない情報、③防衛秘密ではないが、機密に指定されている情報、④防衛秘密ではないが、極秘に指定されている情報、⑤防衛秘密ではないが、秘に指定されている情報の五つに分類できる。

日米の秘密区分を対比すると、①と③は米国のトップシークレットに相当する。②と④は米国のシークレットに相当する。⑤は米国のコンフィデンシャルに相当する。

第５条では、両締約国政府の権限のある当局は、補足実施取極を締結できる、と規定されている。

第６条は秘密軍事情報を保護するための原則を規定している。その内容（趣旨）は以下のようになっており、ほぼオーストラリアやインドとのGSOMIAと共通する。

・提供国政府の事前の書面による承認なしに、第三国の政府、個人、企業、機関、組織または他の団体に、秘密軍事情報を提供しない。
・受領国政府は提供された秘密軍事情報に対して、提供国政府によって与えられている保護と実質的に同等の保護措置をとる。
・受領国政府は、提供国政府の事前の書面による承認なしに、提供された秘密軍事情報を本来の目的以外に使用しない。
・受領国政府は、提供された秘密軍事情報に関係する特許権、著作権および企業秘密のような知的財産権を遵守する。
・秘密軍事情報を取り扱う政府の各施設は、秘密軍事情報取扱資格を有し、かつ、当該情報にアクセスすることを許可されている個人の登録簿を保持する。
・両国政府は、秘密軍事情報の識別、所在、目録および管理の手続きを定める。

第７条は秘密軍事情報への職員のアクセスを規定しており、最も論点になりそうな部分なので、全文を紹介する。

「(a) いかなる政府職員も、階級、地位又は秘密軍事情報取扱資格のみにより、秘密軍事情報へのアクセスを認められてはならない。

(b) 秘密軍事情報へのアクセスは、政府職員であって、職務上当該アクセスを必要とし、かつ、当該情報を受領する締約国政府の国内法令に従って秘密軍事情報取扱資格を付与されたものに対してのみ認められる。

(c) 両締約国政府は、政府職員に秘密軍事情報取扱資格を付与する決定が、国家安全保障上の利益と合致し、及び当該政府職員が秘密軍事情報を取り扱うに当たり信用できかつ信頼し得るか否かを示すすべての入手可能な情報に基づき行われることを確保する。

(d) 秘密軍事情報へのアクセスを認められる政府職員に関して、(c) に規定する基準が満たされていることを確保するために、適当な手続きが、両締約国政府により自国の国内法令に従って実施される。

(e) 一方の締約国政府の代表者が他方の締約国政府の代表者に対し秘密軍事情報を提供する前に、当該情報を受領する締約国政府は、当該情報を提供する締約国政府に対し次の事項についての保証を与える。

(ⅰ) 当該情報を受領する締約国政府の代表者が、必要な水準の秘密軍事情報取扱資格を有すること。

(ⅱ) 当該情報を受領する締約国政府の代表者が、公用の目的でアクセスを必要とすること。

(ⅲ) 当該情報を受領する締約国政府は、自国の国内法令に従って、当該情報について当該情報を提供する締約国により与えられている保護と実質的に同等の保護を与えるために適当な措置をとること。」

この条文に基づいて、我が国政府も、秘密軍事情報を取り扱う政府職員に対して、セキュリティ・クリアランスを実施しなければならない（秘密軍事情報を取り扱うにふさわしい人物であることを確認する）。

第８条は訪問手続きを規定している。一方の政府代表者が他方の政府の施設を訪問し、秘密軍事情報にアクセスする場合の手続きについて定めており、アメリカ政府の訪問者は東京のアメリカ大使館または在日米軍司令部を通じて申請する。我が国政府の代表者はワシントンの日本大使館を通じて申請する。第９条は秘密軍事情報の送付について規定している。秘密軍事情報の送付は政府間の経路を通じて送付され、送付に際しては、受領国政府が当該情報の保管、管理および秘密保持に責任を有する。

第10条は秘密軍事情報を保管している施設の保安について規定している。施設の保安（セキュリティ）とは、当該施設にある秘密軍事情報の盗難、紛失を防ぐことである。日米両政府は施設ごとに、秘密軍事情報の管理および保護の責任と権限を有する政府職員を指名する。

第11条は秘密軍事情報の保管について規定している。秘密軍事情報取扱資格を得ている者のみが、秘密軍事情報にアクセスできるような方法で、秘密軍事情報を保管するとされている。具体的な方法は防衛省内の規則で定められるはずだが、秘密軍事情報を保管している部屋には、暗証番号方式で入室するといった方法が考えられる。

第12条は送付中の秘密保持について規定している。文書を送付する場合は、秘密保持は比較的容易だが、大きな装備品の秘密保持は容易ではない。そのため、第12条は、送付中の装備品に関して、「その細部が識別されることを防止するために、封印され、被覆された車両により輸送され、又は確実に包装」されることなどを要求している。また、電子的手段によって送付する場合は、暗号を使用することになっている。

第13条は秘密軍事情報の破壊について規定しており、焼却、破砕（シュレッダーにかけること）、パルプ化など、情報の復元を防止できる方法で破壊することになっている。第14条は複製（コピー）について規定しており、複製物も原本と同様の管理下に置くことになっている。

第15条は秘密軍事情報の翻訳について規定しており、翻訳も秘密軍事情報取扱資格を有する者によって行うことになっている。第16条は契約企業、すなわち防衛省と契約した企業への秘密軍事情報の提供について規定しており、企業の従業員に対しても、政府職員と同等の秘密保持義務を要求している。同条は15項目から成るが、とくに重要な項目を引用しておく。

「職務上秘密軍事情報へのアクセスを必要とするすべての個人が、秘密軍事情報取扱資格を有すること。

秘密軍事情報取扱資格が、第７条に規定する方法と同様の方法により決定されること。

秘密軍事情報へのアクセスを認められる個人に関して、第７条（c）に規定する基準が満たされていることを保証するために、適当な手続きが実施されること。

秘密軍事情報を受領する締約国政府は、当該情報を提供する締約国政府の当該情報がこの協定において求められているとおりに保護されていることを確保するために、当該情報が保管され、又は当該情報へのアクセスが行われている契約企業の各施設において、最初の及び定期的な保安検査を実施すること。

秘密軍事情報取扱資格を有し、かつ、当該情報取扱資格を有し、かつ、当該情報にアクセスすることを許可されている個人の登録簿が、各施設において保持されること。」

第17条は紛失または漏せつについて規定している。このような事態が発生した場合、受領国政府は提供国政府に直ちに通知し、調査を開始する。調査結果と再発防止策も通知しなければならない。第18条は代表者による訪問について規定しており、秘密保持制度に関して議論する

ために、相手国へ訪問できるとされている。第19条は協定の効力発生、改正、有効期間、終了について規定している。有効期間は１年で、一方の政府が90日前に通告しないかぎり、自動延長になる。

以上のように、日本とのGSOMIAは、オーストラリアやインド並みの詳細な協定になっている。日本、オーストラリア、インドとの協定は、いずれも21世紀になってから締結されており、近年は詳細な協定を締結することにしているのであろう。

おわりに――何が論点になるか

我が国とのGSOMIAで最大の論点となるのは、第７条と第16条であろう。つまり、政府職員と契約企業従業員の秘密軍事情報取扱資格をどのような方法で付与するか、という問題である。

現在、防衛省・自衛隊の秘密軍事情報取扱資格はどのようになっているのであろうか。

防衛省の内部規則である「秘密保全に関する訓令」には、秘密軍事情報の取扱者に関する規定（第３条）があるが、「取扱者は、管理者又はその職務上の上級者が指定するものとする」と書かれているだけである。保全責任者についての規定や関係職員の範囲の制限等に関する規定（いずれも第４条）はあるが、秘密軍事情報取扱資格の付与方法に関する規定はない。

契約企業に秘密軍事情報を提供する際には、契約企業と「秘密の保全に関する特約条項」を締結することになっている（同訓練第27条）が、秘密軍事情報取扱資格の付与に関する規定はない。

「防衛秘密の保護に関する訓令」は「秘密保全に関する訓令」より若干詳細になっているが、それでも秘密軍事情報取扱者については、「防衛秘密の取扱いの業務に従事する職員を指定するに当たっては、防衛秘密に関する事務を行う者としてふさわしい者を充てるものとし、その範囲は必要最小限にとどめなければならい」とされているだけである（第16条）[23]。

「秘密漏えい防止のための取扱い環境の整備等について[24]」という防衛省の事務次官通達を見ても、秘密軍事情報取扱資格の付与に関する規定はない。

このように現在、秘密軍事情報取扱資格の付与に関する規定は存在しないが、GSOMIAに基づいて、秘密軍事情報を取り扱う政府職員と契約企業従業員の身上調査を実施することになれば、個人情報保護との兼ね合いが問題になるであろう。この点に関連して、防衛省の「平成20年度業務計画」では、各自衛隊の情報保全隊を統合し、情報保全機能を集約化した自衛隊情報保全隊の新設と、防衛省カウンターインテリジェンス委員会の新設が計画されている[25]。

将来的には、罰則の強化も課題になるかもしれない。今のところ、GSOMIAの締結に伴う国内法の改正は予定されていないが、前述したように、MSA秘密保護法に基づく罰則の最高刑が懲役10年なのに対し、自衛隊法に基づく秘密漏洩の罰則は最高刑５年である。両者のバランスを取るため、自衛隊法の罰則強化が課題になるかもしれない。

なお、GSOMIAに拘束されるのは、政府職員と契約企業の従業員だけで、それ以外の者（報道関係者等）は対象にならない。したがって、GSOMIAの締結は、報道の自由、言論・表現の自由の制約に直接的には関係しない。

（ふくよし　しょうじ　大阪経済法科大学
アジア太平洋研究センター客員研究員）

㉓「秘密保全に関する訓令」と「防衛秘密の保護に関する訓令」は、『防衛実務小六法』（内外出版）各年版に掲載されている。

㉔ 事務次官「秘密漏えい防止のための取扱い環境の整備等について（通達）」、2000.12.１、情報公開法で入手。

㉕「平成20年度業務計画」は『朝雲』2007.９.６.と防衛省のウェブサイト〈http://www.mod.go.jp/j/library/archives/yosan/2008/yosan.pdf〉に掲載されている。