

## 調査・研究報告書の要約

書名	平成 19 年度国際的制度調和に向けた安全保障貿易管理制度の比較・分析に関する調査研究報告書 (米国における安全保障貿易管理制度に関する調査研究)				
発行機関名	社団法人 日本機械工業連合会・財団法人 安全保障貿易情報センター				
発行年月	平成 20 年 3 月	頁数	105 頁	判型	A4

### [目次]

序（金井会長の序）

序（黒田理事長の序）

目次

総論

1. 調査目的
2. 調査内容
3. 調査の結果と得られた結論

各論

1. 米国の輸出管理法制度における技術移転規制
2. 米国企業に求められる技術移転管理の概要
3. 米国の企業・大学・研究機関における輸出管理の運用実態
4. 米国の技術移転管理規制に関する最近のトピック
5. 日本企業が技術移転を行う上での留意点
6. まとめ

### [要約]

米国の輸出管理法制度における技術移転規制、米国企業に求められる技術移転管理の概要、米国の企業・大学・研究機関における輸出管理の運用実態を把握し、日本企業が技術移転を行う上で参考になるよう整理すると共に技術移転を行う上での留意点をまとめた。米国は技術移転規制を強める傾向にある。日本企業は、米国の輸出規則に違反しないよう

米国の輸出管理制度を把握して自社の輸出管理システムを構築すると共に、最新の米国の輸出規制動向を踏まえながら、そのシステムの実効性を絶えずレビューしていくことが求められている。

## 各 論

### 1. 米国の輸出管理法制度における技術移転規制

米国の安全保障貿易に関する輸出規制は、商務省産業安全保障局（BIS）の輸出管理規則（EAR）、国務省防衛貿易管理局（DDTC）の国際武器取引規則（ITAR）、財務省外国資産管理局（OFAC）の 31CFR Parts 500～595 などで実施されている。

EAR は、デュアル・ユース技術の提供を規制している。技術とは広い意味で、「製品の“開発”“生産”又は“使用”のために必要な情報」である。BIS は最近、「使用」技術とは、製品の「操作、設置(現場での設置も含む)、保守(確認)、修理、点検そして修復」のために必要な特定情報を指し、適用可能な「使用」規制を発動するためには、情報にこれら 6 項目全てが含まれていなければならない、との見解を明確にした。技術の定義には「技術資料」と「技術支援」も含まれており、「技術支援」には指示又は専門家との相談が含まれ、「技術資料」の移転に関しては、青写真（ブループリント）、計画、図、モデル、手順書、説明書が含まれる。EAR のみなし輸出規則は、米国にいる外国人へのソースコード(読み手にわかりやすいプログラム説明)の開示がされた場合のみ、ソフトウェアにも適用する(一般的に EAR は米国からのソフトウェア輸出に適用)。

EAR 規制技術の移転を管理するための管理体制に関する業界の標準的なガイドラインである TCP(Technology Control Plan)は、1) 米国の国家安全保障を実現するため機密性を持つデュアルユース技術の拡散を防止し、2) 技術移転を管理することにより企業の知的財産を保護することを目的としたもので、「規制情報、機密情報、独占的な企業秘密情報」を保護し、「外国人に対する技術提供」を管理し、「非米国人の従業員等に対する技術提供」を管理するための指標となっている。

ITAR は、軍物品目及びサービスに関連する技術資料の開示を制限する。技術資料には、「軍物品目の設計、開発、生産、製造、組み立て、操作、修理、検査、保守、又は改良に必要な青写真、設計図、写真、計画、説明書、書類の形(を含めた)」情報が含まれる。ITAR はさらに、防衛物資・サービス関連の機密情報及び発明機密保持命令により保護された情報を、技術資料の定義に含む。技術資料には、ソースコードとオブジェクト・コードの両ソフトウェアを含む。

ITAR 規制技術を管理するための管理体制に関するガイドラインは、TTCP(Technology Transfer Control Plan)であり、防衛関連産業は DTSA に対する許可申請の際に TTCP を使用するべきとされている。ITAR(22 CFR 120-130)では、防衛物資の輸出を規制しているが、TTCP には輸出許可に関連する最新の全書類が添付されており、TTCP に基づく運用を行うことで、輸出許可に関する資料について漏れやミスを防止することが出来る。

米国財務省 (OFAC) は、米国外交政策及び国家安全保障を推進するために、対象国・団体・個人に対する米国経済制裁と禁輸処置を管轄している。一般的に、包括的禁輸処置(例：キューバ、スーダン、イラン)の対象国に対する OFAC 規制は、輸出禁止の枠を超え輸入、金融及びその他取引や取引の支援、場合によっては人の移動をも規制する。すなわち OFAC 規制は、金融取引やサービス提供などの事業活動・商行為にも対象を広げており(完全に定義づけられていない)、列挙されている技術や商品に限定されていない

OFAC は、米国から、または米国人 (海外在住を含む) により、指定された国・団体・個人に向けて行われる全ての製品・サービス (技術サービスを含む) の輸出を管理する。

「サービス」と「技術サービス」は規制には定義づけられていないが、OFAC は対象範囲について非常に拡張的な見解を持つ。米国人は、米国人により実行された場合に禁止されている取引に間接的に関わることを、または同様の取引を促進することを禁止されている。

## 2. 米国企業に求められる技術移転管理の概要

### (1) 技術移転管理を求められる企業

技術移転は、“製造や技術開発が海外に移転される時”や“物理的輸出や電子メールのやり取り、電子商取引、海外の第3者への開示を行う時”などに起こりうるが、こうしたケースでは意図せぬまま事実上技術を移転してしまうケースがある。このため、米国企業は、技術移転を管理する EAR,ITAR,OFAC 規制を遵守するため、社内実効性ある運用体制を構築する必要がある。

厳格な技術移転管理を求められるのは、以下に挙げるようなインフラあるいは取引面での特徴を有する企業である。

### 【ネットワーク関連】

- ・複数の国にネットワーク化されたデータセンターがある。
- ・サーバーの所在地－米国外にあるサーバーのストレージは、もし米国親会社が海外の子会社へストレージを移動しただけであっても、ホスト国への輸出である。
- ・サーバーの所在地－外国親会社・子会社が制裁国と取引をしている場合、米国がホストするサーバーは、米国のホストに対する OFAC 問題を浮上させる可能性がある。
- ・リースされているコンピュータを使用している。
- ・国境を越えた社内電子コミュニケーションを行っている。
- ・外部委託・海外のサーバーにあるデータストレージを行っている。

### 【取引関連】

- ・軍事請負業者または軍事請負業者への下層供給者である。
- ・政府資金による研究開発を行っている。
- ・グローバル供給チェーンを展開している。
- ・IT の外部委託(例：コンフィギュレーション管理設計)がある。

### 【その他】

- ・多国籍の技術者を雇用する企業
- ・技術集約型の外国合弁企業
- ・グローバル知的財産権 (IP) 資源を所有するグローバルテクノロジー企業
- ・重要なハイテク知的財産権(IP)ポートフォリオを有する企業
- ・国際研究開発センター(特に中国・インド)を有する企業

## (2) 法令遵守プログラムの構築

米国企業は、輸出規制のリスクを最小限に抑えるため、企業の特質・性格に応じた独自の法令遵守プログラムをトップダウン伝達で構築・運用し、効果的且つ効率的に輸出規制関連法を遵守することが求められている。

法令遵守プログラムにおいて最も重要な要素の1つは経営トップによるステートメントであり、企業経営責任者はこのステートメントで適用可能な輸出規制法を会社が遵守する方針を明確に示さなければならない。企業経営者は、構築した法令遵守プログラムを管理・

運用するための体制を整備し、輸出規制法の遵守が重要であることを全従業員に自覚させる必要がある。また、輸出管理責任者は輸出担当者に輸出規制遵守手順の重要性を理解させ、他の社員には輸出規制遵守スタッフの注意を喚起できるように輸出取引の見分け方を学ばせる必要がある。

輸出規制遵守プログラムの審査は、注文処理の枠組みで取り扱う。これは審査がどこで誰によって実施されるのが最もよいかは会社の注文処理方法に表れるからである。すべての輸出出荷をどのような方法で誰が行うかを決定したら、会社は輸出規制遵守プログラムの必須要素の最良の構築方法を決定して、必要な遵守機能を最も早い段階で確実に実施でき、最終段階でも確実に実施できる。有効な規制遵守手順は、特定の企業が既に事業を遂行している手順に完全に適合するものでなければならない。

親会社の 1 つがその会社の監査を行わない場合は（もしくは親会社の監査に加えて）、法務担当責任者は会社の法令遵守プログラムに含まれる問題点を熟知しているが日常の輸出業務に関係しない者を指名して、輸出規制遵守プログラムの徹底した監査を定期的実施しなければならない。監査役は、その会社に属さない者もしくは法務担当責任者か社長に対して責任を負う者で、輸出規制遵守管理者の究極の支配下にない者でなければならない。監査役は、BIS が適宜配布する監査モジュール／チェックリストを 1 つの参考として使用するべきである。輸出規制遵守管理者は業務の抜き打ち検査を適宜実施しなければならない。

### （3）みなし輸出への対応－従業員の国籍管理

外国籍従業員の雇用および管理の手順は大きく 4 つのステップに分けられる。まず初めに、企業が使用している技術を特定する共に、どの技術が **EAR** 又は **ITAR** で規制されるかを把握する。次に、従業員の国籍、出生国、市民権を保有する国、居住国（複数可）を含む情報を収集・整理する。そして、規制される技術と国籍を照合して、外国籍従業員へのアクセスを管理する必要があるかどうかを確認する。その際、雇用候補者が **SDN** リストの掲載者の場合は要注意である。追加調査を行うよりは如何なる取引も自制すべきであると指摘する専門家もある。最後に、アクセス管理を行う必要がある場合は、外国籍従業員が規制技術へアクセスするための許可を取得すべきか、あるいは外国籍従業員が規制技術へアクセスすることを制限すべきかを決定する。

### 3. 米国の企業・大学・研究機関における輸出管理の運用実態

#### (1) IT 産業

インテルは、規制対象地域の従業員の管理、ファイアウォール、電子アクセス管理、データ保護などの面で特徴的な輸出管理を行っている。規制対象地域の従業員への対応では、規制対象国(CC: Controlled Country)の国籍を持つ従業員に別のドメインを割り当て、その他地域(米国、欧州、アジアなど)のドメインとは区別している。セキュリティ・インフラの中で CC 国籍保有者を特定するための一つの方法としてもドメイン管理を行っている。

ファイアウォールは、インテル社内と社外(インターネットなど)の間にある外郭ファイアウォールと世界中のインテルを結ぶネットワークの内部ファイアウォールで構成されている。機密と見なされる知的財産又は情報を保護するために、多くの事業グループにより使用されアクセスは各事業グループによって管理されている。規制国内と、インテル内の CC と CC 以外の間で、IP 及び特定規制技術や機密データを保護するために使用されている。また、CC を含む地域レベルで使用されている。

電子アクセス管理についてインテル社では、規制技術又はソフトウェアを、共通サーバー、データベース、又は電子ボードにアクセス制限なしで掲載をすることを禁止している。また、物理的なアクセス、コンピュータアクセスを管理するとともにデータの隔離も行っている。アクセスを管理するために、様々な承認方法を活用する(例: NT 認証、パスワード、暗号化など)。規制情報は一般的にパスワードにより保護されているか、規制対象外の情報と区分され管理されている。

ソースでのデータ保護に関しては、サーチ・エンジン・ツールを使用し、インテル・ネットワーク内のコンテンツにキーワード・サーチを実行し、四半期毎にインテル内の様々なプラットフォーム(例: NT、Unix、Linux、FTP など)をスキャンし、漏洩(解読可能な)情報を探す。また、特定された対象機密情報と規制技術に対して検索スキャンをかける。スキャン結果について評価し、必要に応じてコンテンツにセキュリティをかける。情報の安全を確保するために、コンテンツ所持者・システム管理者と直接対応する

## (2) 航空・宇宙産業

ボーイング社の現在の輸出管理体制は 2004 年にできたものであり、企業の最高責任者は副社長である。それ以前は現在のような中央集権体制ではなく、各部門に分散した体制となっていた。ボーイング社はここ数年来 ITAR 違反事件に絡んで 4 度 DDTC との和解文書にサインをしている。その都度罰金の支払いと共に当局から強い改善指導を受けており、その結果として現在の体制が出来上がった。また、外部から雇用した **Special Compliance Officer** を置いている。同社の輸出管理状況は DDTC によって常に厳しく管理されている。ボーイング社は ECP (**Export Compliance Program**) のモデル版を会社が策定し、各事業部門がそれぞれに準じて独自に ECP を制定、運用している。またライセンスを取得した案件毎に必要な輸出管理内容を規定した ICP (**Internal Control Plan**) を策定し、管理に漏れが生じないように万全を期していることに特徴がある。

## (3) 素材・エネルギー産業

**Applied Materials** には、グローバルに適用される一連の「業務上の行動指針」を有している。この指針ではコンピュータに保存された情報を保護するための措置として、以下の点を従業員に義務付けている。

- 1) いかなるコンピュータ・システムにも、「電源投入時」のパスワード保護を常に設定しなければならない。
- 2) 利用可能なソフトウェアセキュリティシステムを適所に使用しなければならない。これには最低でも **Windows** のスクリーンセーバーパスワードが含まれる。
- 3) 自分が使用しているコンピュータ・システムの画面を注視している可能性のある者を意識する必要がある。乗客が隣り合って着席する航空機もしくはその他の一般輸送機関での移動中には、専有情報もしくはデータを取り扱うことを避けなければならない。
- 4) **Microsoft Access**、**Word**、**Excel**、**Word Perfect** 等のプログラムを使用している間は、パスワードによる保護機能を活用して、データファイルを保護しなければならない。
- 5) 会社の要求がない限り、他の従業員とパスワードを共有してはならない。この単純な規則によりデータが安全に保たれ、他の従業員の行為の責任を問われることが回避できる。



#### (4) スタンフォード大学

スタンフォード大学は、世界における知識の蓄積への貢献を目的として、非機密・非専売の研究のみを行っている。「開放的研究政策」の下、大学の研究管理室(ORA: Office of Research Administration)は、同管理室の指導の下行われる研究に出版制限をかけるような研究機会は、受け入れないように義務付けられている。研究へのアクセス制限又は研究への参加者に対する制限を与えるものに対しても、スタンフォードは契約又は助成金の受け入れを拒否することになる。

この方針は、1891年に創設者により支持された「学問の自由」の原則から築き上げられたものだが、EAR及びITARの両規則に基づいた米国輸出管理規則は、「基礎研究」を対象範囲から除外しているため、このスタンフォードのアプローチは、都合の良いものである。基礎研究は、これらの規則によると、「科学及び工学分野における基礎・応用研究で、その成果は幅広く分配されるか、公共に属することを目的とする」と定義付けられている。

スタンフォード大学は、輸出管理を徹底させるため、輸出規制に対する内部法令遵守のためのコミュニケーションと訓練を行っている。大学輸出規制法令遵守オフィサー(ECCO: Export Control Compliance Officer)の支援活動及びその他の活動がプログラムの根幹となり、また、ECCOへの容易なアクセスが、法令遵守プログラムの認知度を確実なものにする決定的な要因となっている。ナノテク、ゴキブリのDNA、プラズマ物理から文化人類学まで、全ての学問的探求課題に実際に関わる学部教員や研究管理者とのECCO会合の影響は、いくつかの活動に反映されている。

#### (5) アメリカ航空宇宙局 (NASA)

NASAには、ECPと呼ぶ輸出規制プログラムがある。ECPはNASAの内部プログラムで、1995年11月にハンドブックとして発行されたものがベースとなっており、現在はNPR 2190.1として承認されている。これにより、輸出政策と法令遵守がNASA本部の一部署に集約され、各部門には輸出法令に関する専門家である輸出管理者と輸出顧問が任命されている。これに従って、輸出管理の責任者が割り当てられ、各種手続きが標準化されている。NASAプログラムのもとでは、その輸出が、承認された契約や国際協定、ならびに米国輸出規制法令に適合しているという確信を輸出者が持っていない限り、規制品目を

外国企業体に輸出することは禁止され、NASA から外国企業への輸出は、NASA の国際協定または契約を推進する場合に限って実施されている。

#### 4. 米国の技術移転管理規制に関する最近のトピック

米国は、世界情勢の変化などを踏まえて技術移転管理規制をレビュー・改定している。技術移転管理規制に関わる最近の注目される動きとしては、米国みなし輸出規制に関する「みなし輸出諮問委員会（DEAC : The Deemed Export Advisory Committee）」の報告、中国軍事最終用途規則、違反輸出に対する罰則強化などがある。

「みなし輸出規制」を巡る注目すべき動きとしては、DEAC が 2007 年 12 月 20 日に国務省へ提出した最終報告書「The Deemed Export Rule in the Era of Globalization」が挙げられる。同報告書は、みなし輸出規制に関する問題点として次の点を指摘している。

- 1)近年、米国以外の国からも技術を容易に入手できる状況になりつつある
- 2)CCL の規制が広範囲に及んでいる
- 3)規制内容が複雑かつ定義があいまいであることを挙げている。
- 4)大学や産業界はみなし輸出に、まだあまり注意を払っていない可能性がある。
- 5)国家安全保障の観点からみても、みなし輸出には法の抜け穴が多い。
- 6)EAR の技術規制の「使用」について、「及び」と「又は」「及び」で接続されているため 6 つの要件の一つでも満たさなければ技術の「使用」には当たらないという現象が起きている。
- 7)みなし輸出の規制対象となる外国人の国籍の定義が国家安全保障という規制の主旨とそぐわない場合がある。

みなし輸出諮問委員会は上記の問題点の改善提案として、1) みなし輸出制度をより簡潔なものとし、米国の安全保障と産業界の国際競争力を増進する、2) BIS によるみなし輸出規制のアウトリーチ活動をより拡大することをあげている。

中国軍事最終用途規則を巡っては、BIS が 2006 年に対中国輸出規制リストから除外されていた品目を再び規制リストに掲載するという規則案を発表、この規則案は議論を呼んだが 2007 年 6 月には最終規則を発表するに至っている。

違反輸出に対する罰則強化を巡る動きとしては、国際緊急経済権限強化法がある。同法は2007年6月26日に上院において満場一致で承認され、下院に付託されている。同法が施行されればIEEPAに基づいて科することのできる民事および刑事罰の上限が引き上げられる。S.1612により民事制裁金の上限は違反1回あたり5万ドルから、25万ドルまたは取引額の2倍のうちいずれか大きい額に引き上げられ、刑事罰金の上限は違反1回あたり100万ドルに引き上げられる。

## 5. 日本企業が技術移転を行う上での留意点



企業は、海外への技術移転を行う過程の中で、輸出管理上の様々なリスクを抱えている。この複雑な輸出規制のリスクを最小限に抑えるためには、企業の特質・性格に応じた独自の法令遵守プログラムを構築・運用し、効果的且つ効率的に輸出規制関連法を遵守する必要がある。企業経営責任者は、構築した法令遵守プログラムを管理・運用するための体制を整備すると共に、輸出管理責任者は輸出担当者に輸出規制遵守手順の重要性を理解させ、他の社員には輸出規制遵守スタッフの注意を喚起できるように輸出取引の見分け方を学ばせる必要がある。

法令遵守プログラムの構築にあたっては、グローバル化に伴って世界中から数多くの人材が流入し、従業員の中には輸出規制の対象となる国籍を有する者が少なくなく、みなし輸出規制違反を回避するために、こうした外国籍従業員の管理が重要であることを考慮する必要がある。

輸出管理システムの運用、監視、レビューもまた重要である。優れた法令遵守プログラムを策定し、万全な輸出管理体制を整備したとしても、適切かつ効果的に運用されていないければ何の意味も持たなくなる。企業経営責任者が主導する形で、構築した輸出管理システムを監視すると共に、その運用に問題あるいは改善すべき点があるかどうかを定期的にレビューして必要に応じて輸出管理システムを見直す必要がある。

## 6. まとめ

経済のグローバル化の進展に伴って製造拠点の海外移転や技術移転が進む中、企業には安全保障貿易管理の観点から、技術移転を適切かつ厳格に管理することが求められている。国際化に伴い従業員の国籍も多様化しており、知らず知らずのうちに規制対象国の従業員に規制技術を開示して輸出規制違反を犯すリスクが増大している。企業は、こうした点を踏まえて、日本企業は米国等の輸出規制動向にも注意を払いながら、社会的あるいは経済的リスクを回避するために法令順守プログラムを策定し、確固たる輸出管理体制で運用していくことが望ましい。

	<p>この事業は、競輪の補助金を受けて実施したものです。</p> <p><a href="http://ringring-keirin.jp/">http://ringring-keirin.jp/</a></p>	
--	---	--