

Trust Sixty Foundation

# 国際商取引に伴う法的諸問題(6)

トラス60研究叢書

平成9年9月

財団法人 トラス60

## 発刊にあたって

平成3年開始の「国際金融・貿易に係わる法務に関する研究会」は、国際法、国際取得法、国際私法、企業組織法、無体財産法、租税法などの研究者が参集し、それぞれの立場から活発な議論を展開してまいりました。

本研究会はこれまで年間のテーマを特に定めずに研究をするスタイルをとっておりましたが、平成8年度は、「電子マネーと暗号政策」を共通テーマとしてヒアリング並びに研究会を行って参りました。この度、その成果を中心に「国際商取引に伴う法的諸問題(6)」として論文集を刊行することとなりました。

本書では、

- ・電子マネーと暗号政策——21世紀金融インフラの構築に向けて——（石黒）
- ・GATSと電気通信（小寺）
- ・金融と特許法（序）（相澤）
- ・ヨーロッパにおける租税情報の国際的な交換（中里）

の4論文を収録しています。

電子マネーは欧米においてはすでに導入されている地域もあり、また日本でもその試行が一部はじまっています。また、インターネットを通じての商品の購入などの際には、電子決済に近い形態が取られていますが、その安全性については疑問視せざるを得ません。電子マネーの周辺には未だ解決されていない問題が山積しているという状態であることは周知の事実です。

電子マネーは単に国内の問題であるばかりでなく、その性格上国際的な問題でもあります。政策的として「電子マネー問題」をどう考えていくべきか。本書がその指針の一助になれば幸いです。

本研究会にゲスト・スピーカーとしておいいただき、貴重なお話を賜りました、NTT 太田和夫、成蹊大学 藤田友敬、弁理士 谷義一、FISC 木下信行、日銀金融研究所 岩村充氏、東京大学 岩原紳作の各氏に改めて御礼申し上げます。

平成9年8月

トラスト60

## 国際金融・貿易に係わる法務に関する研究会

### 委員名簿

相澤英孝	筑波大学第2学群助教授
石黒一憲	東京大学法学部教授
岩沢雄司	東京大学教養学部助教授
落合誠一	東京大学法学部教授
小寺彰	東京大学教養学部教授
穴戸善一	成蹊大学法学部教授
中里実	東京大学法学部教授
水野忠恒	一橋大学法学部教授
村上政博	横浜国立大学大学院国際経済法学研究科教授

(五十音順、敬称略)

# 目 次

電子マネーと暗号政策——21世紀金融インフラの構築に向けて——（石黒一憲）	1
GATSと電気通信（小寺彰）	45
金融と特許法（序）（相澤英孝）	63
ヨーロッパにおける租税情報の国際的な交換（中里実）	101

電子マネーと暗号政策  
——21世紀金融インフラの構築に向けて——

石 黒 一 憲

## 目 次

はじめに

- I 私の従来を検討“経緯”から見たその後の問題展開における留意点
- II OECD 暗号政策ガイドライン（最終案）の内容
- III アメリカの暗号製品輸出規制とキイ・エスクロ構想——国家管轄権との関係を含めて
- IV 1996年9月のアメリカ財務省主催の会議とその周辺事情から見た「電子マネーと金融政策」
- V 小 括

## はじめに

(財)トラスト60に置かれた我々の研究会では、平成8年度の共通テーマとして“電子マネーと暗号政策”を取り上げ、この問題についての暗号技術・暗号特許・金融取引・金融政策等の諸側面を、集中的に検討して来た。従来は、その時々には生起する国際的な金融・貿易のホット・イシューの理論的・体系的そして実務的解明を“機動的”に行うことに主眼を置いて来たが、平成8年度においては、一つの試みとして上記の方針を立てて見た訳である。本稿は、この1年を振り返り、検討の結果を私の視角からまとめ、かつ、展開したものである。

## I 私の従来への検討“経緯”から見たその後の問題展開における留意点

ここで、私自身のこれまでの、この問題に関する検討の“経緯”について、一言して置こう。時間軸をしっかりと立てて、わずかここ数年の出来事を冷静に振り返ることが、既にして今の日本における“電子マネーと暗号政策”問題に対する、「先へ先へと草木もなびく」式の、根無し草的な情緒的問題把握——「羅針盤なき日本(!)」の悲しい性癖——への、重大な警鐘でもあるからである。また、それを通して、当面する問題群の一応の見取り図も、それなりに描けるはずだと、私には思えるからである（なお、参照論文や重要な論点 [キイ・ワード] 等には、適宜アンダーラインを付することとする）。

まず私は、①石黒「国際的な金融システムの安定と危機管理」国際問題（(財)日本国際問題研究所）425号 [1995年8月号——「焦点：国際システムと危機管理」の特集号] 21頁以下において、クロスボーダーなデリバティブ取引におけるリスク管理上の問題（それについては、金融法務事情1471号 [平成9年1月5・15日号] 53頁以下の座談会における石黒発言をも参照）等々に言及しつつ、その28頁以下で「通信ネットワーク高度化との関係」を扱った際に、本稿の問題について、若干論じて置いた。そこでは、私が別途、1995年2月下旬にバンクーバーで開催された GII（世界情報通信基盤）関係の国際シンポジウ

ム (OECD/APEC/PECC 共催) で行った報告の一部を引用しつつ、ジョージタウン大学 D・デニング教授 (クリントン政権における当時のクリッパー・チップ構想——アルゴリズム非公開型の暗号チップの通信端末への強制的埋め込み政策——の技術面での推進者) の提唱する国際的なキイ・エスクロ構想の危険性を指摘し、国家管轄権論 (それについては、石黒・国際民事訴訟法 [平成8・新世社] 13頁以下)、そして憲法上の通信の秘密との関係での深刻な問題がそこから派生してくることへの警鐘を、鳴らして置いた (その後、後述の OECD 暗号政策ガイドライン作りのための専門家会合において、日本代表 [郵政省] がわが憲法21条の通信の秘密の問題を提起するに至ったのは、これと関係する)。そして、同上・31頁に、私は次のように記しておいた。即ち、——

「私はチャウムのデジタル・キャッシュ構想と米国の新暗号政策とが、いずれドッキングし、その国際的な技術標準化と国際的な鍵 (暗号解読の鍵) の保管システムの構築が意図されることになろう、と踏んでいる。そして、そのような“危険管理”システムのなかに日々の国際金融取引がスッポリと包まれることになる。言うまでもなく暗号は、とりわけ米国にとっては、どこまでもしがみつきたい国家安全保障上の鍵である。それと金融 (そしてテレコム) における覇権願望が結び付いた上でのこと、ということになろう。その存在自体が最も危険な“危機管理”システム、との印象が私にはあるが、どうなのであろうか。」

この①の論文は、当時執筆中だった②同「アメリカの新暗号政策とデジタル・キャッシュ構想——その接点をめぐる覚書(上)(下)」貿易と関税 ((財)日本関税協会) 1995年9月号30頁以下、同10月号40頁以下を踏まえつつのものだった。この②論文の副題で、私は「接点」という言葉を用いたが、それは以下の理由による。

この論文の執筆当時は、意外にも「電子マネー」の問題と「暗号政策」(既述のアメリカのクリッパー・チップ構想) とを切り離して論ずることが、むしろ一般の傾向であった。勿論、電子マネーの技術的側面は暗号技術によって固められている訳だが、この二つの問題をあえて分け、暗号政策は別途論ずる、というのが (後述の、元 NSA [アメリカ国家安全保障局] の S・ベイカー氏を含めての) アメリカ側の“戦略”だったように思える。その“分断作戦”に安易に同調してしまっていたのが、当時の日本だったことになる。

だが、私と電子マネー問題との出会いは、1994年11月30日から数日、パリで開催された OECD インフォメーション・インフラ専門家会合においてであった (同・貿易と関税95年

9月号30頁)。そこで異例の長時間の報告が、D・チャウム氏自身によって、そのデジタル・キャッシュのシステムについて、なされていたのである。モンデックスとは異なるネットワーク型電子マネー（電子現金）についての報告のみが、あえてOECDで、なされていたのである（一般討論と別枠のものとして、他には、通常のインターネットを通じてのデモンストレーションとして、パリのOECD本部からハリウッドが呼び出され、音声・音楽を含めた低次元の“実演”がなされたのみ）。それは、GIIの基本的アプリケーションの具体像とセキュリティ問題への強い関心との「交点」において、とくに強調してなされたものであり、アメリカとEUとの事前合意がなければ、そうしたことはなされ得なかったはずである。しかも、ゴア副大統領の右腕としてインターネット・NII/GIIの推進役となっていたM・ネルソン氏がこの会議の総括議長として、「暗号化（エンクリプション）」と「匿名性（アノニミティ）」の二つのキイ・ワードをもって会議を締めくくったのである。

その後、OECDでは、暗号政策のみが（前記のアメリカの意図に従い？）切り離されて討議され、1995年12月以来数次の暗号専門家会合（96年5月のワシントンD.C.での会合以来、専らガイドライン作りが目指された。ちなみに、この96年5月の会議以来、従来は通産・郵政とNTT、そしてごく一部の金融機関のみだった日本代表に、警察関係者が加わるようになった。当時、私はNTT分割問題で郵政省と全面对決していたが、上記の“転換”を強く主張したのは、私である。なお、後掲③論文、そして後掲④論文63頁参照）を経て、1997年2月27日～28日の最終会合を受け、同年3月末のOECD理事会で審議され、最終案が公表されることになっている（後述）。

以上の経緯、とくに1994年11月末以来の前記OECD会合でのいきさつからして、郵政省電気通信局・暗号政策と電子現金（1996年4月）の報告書冒頭頁が、1995年12月の暗号専門家会合から説き始める（といってもわずか1頁）のは、若干問題であったと言えよう（この点については、後掲④論文【オープン・ネットワーク1996年8月号】63頁、ちなみに、そこで示したように、郵政省側の上記報告書における主たる関心は、上記②論文の線で暗号と電子“現金”とを結び付けて考えつつ、「すべての要となる認証機関【CAと呼ばれることもある】……を電気通信事業者と位置付けて、郵政省が電子取引【その後、EC等という紛らわしい用語が一般に用いられるようになってしまった】の要を掌握する」点に置かれていた。また、当時のキイ・エスクロ構想（その後のOECD暗号政策ガイ

ドライン作成作業における用語では、“政府による” lawful access を前提とした key management system との関係での問題) にも若干好意的な (というよりは様子見的な) 指摘もあり、それが クロスボーダーな問題展開 (後述) をどこまで見据えたものが懸念された (日本国内でのこの CA ネットワークの構築の仕方をどうするかが延々と議論されつつ、関係各金融機関の思惑の違いからいまだすっきり解決がつかずにいる現状は問題である。だが、そこに「国際的視点」が欠けていることは、深刻な問題を提起する。アメリカ連邦盗聴法、および後述のアメリカ輸出管理法に基づく規制 [とくに後者に注意! —後述] が、はっきりと海外での出来事にターゲットを絞って クロスボーダーな盗聴 をせんとしているからである)。

なお、上記②論文では多様な問題に言及しているが、ここで、1点のみ補足しておく。本研究会のゲスト・スピーカーとしてお話しいただいた 岩原紳作教授 は、ディジキャッシュ 構想においても、その後は オフラインでなくオンライン志向 になっているとの指摘をされたが、私は終始、電子マネーの二重使用の発見が「事後的」なものではあまりに危険 であり、この点何とかならないか、との点を別途強調していた。

1988年から始まっていた NTT の電子マネー研究 においては、現金の性格をネットワークを経由する「情報」で置き換えられないか、との点が主たる関心事となった。そこで、店で現金を受け取った者が一々その場で日銀に「偽札」かどうか確かめなくて流通するのが現金ゆえ、それだけの信頼を得られる技術の開発が意図された。ちなみに、この点について、やはり我々の研究会においてゲスト・スピーカーとしてお話しいただいた NTT 情報通信研究所太田和夫主幹研究員の「セキュリティ応用——ディジタルキャッシュ——」 電子情報通信学会誌79巻2号 [1996年2月] 131頁以下でも、技術的には、「各小売店が各利用者の購買時に必ずセンターにアクセスすることは、処理時間 (利用者の待ち時間)、通信コスト、管理センターでのオンライン処理コストおよびデータベース維持管理コスト等を考えると、決して現実的な解とは言えない。従って、通常の現金使用時に、各小売店が視覚、触覚で現金の正当性を判断し、ローカルに (オフラインで) 処理を行っているように、[電子] 現金支払い時の処理はオフラインで処理できることが望ましい、とされている (太田・同上132頁。なお、石黒、前掲[②]貿易と関税95年9月号33頁の注5とそれに相当する本文、同・35頁以下、等参照。なお、同・35頁の 二重使用判明率50% との点については、岩村充・電子マネー入門 [平成8・日経文庫] 93頁以下と適宜対比して

考えよ)。

だが、私がこのシステムを悪用する立場なら、かかる「事後チェック」のなされる前に、悪用するだけ悪用して、姿をくらますであろう。しかも、その不正使用額がいわゆる電子マネー発行上の上限規制（なお、本稿IVで後述する1996年9月のアメリカ財務省主催の会議に提出されたアメリカ通貨監督庁 [Comptroller of the Currency] の E. A. Ludwig, infra, at p. 3 によれば、かかる上限規制 [load limits] が work するのは、すべての国においてそのリミットが同じ場合のみだ、との指摘が同会議でなされたようである。これも、本質的にクロスボーダーな存在たる電子マネーの性格を反映した問題把握であり、すべてがドメスティックな日本での議論においては、十分注意すべき点である）の枠内である保証は、どこにもない、ということに注意すべきである（後述のエコノミック・チェルノブイリという言葉、そしてスーパー・ペイメントとの関係、そして、やはり後述のH銀・NTTの共同研究の成果に注意せよ）。

さて、上記②論文で基礎的な検討を若干詳細に行った（その内容はここでは再叙しないが、同・貿易と関税95年9月号36頁に、an anonymous digital-cash Clipper Chip とある点、そして、そこに「これは……21世紀世界における覇権をかけた、国家対国家の烈しい、国家安全保障レベルでの対立にも発展し得る問題なのである。これを単に金融、あるいはテレコムに閉じた問題と考えるのは、既にして問題の矮小化であり、危険極まりない事だ」、とある点には、とくに注意せよ）後、事態の急速な展開（といっても終始曖昧な日本での問題展開 [? —— 一体“展開”なのか、鼠花火に過ぎないのか。私見は後者]ではなく、海外のそれである）に鑑み、私は“行動”に徹しつつ、折りにふれていくつかの小論を発表して行った。

まず、警察関係者の雑誌に寄稿したものとして、③石黒「アメリカの新暗号政策（国際的盗聴政策）と国際金融」月刊治安フォーラム（立花書房）1996年6月号13頁以下、がある。ちなみに同じ号の2頁以下には、OECD暗号専門家会合に出席していた辻井重男中央大学理工学部教授の「電子情報世界からの開国論」がある。

辻井教授は、当時のアメリカのキイ・エスクロ構想（暗号解読鍵の供託計画——KEI [Key Escrow Initiative]）とEU側のTTP (Trusted Third Party)、つまり“信頼し得る第三者機関”の考え方との微妙な温度差（アメリカ側は政府の合法的盗聴に力点を置くが、EU側は、この点が域内各国の問題ゆえ、アメリカに反発しつつも同調するフラン

ス、アメリカとかなり共通の認識のイギリス、そして懐疑的なドイツと、一枚岩ではあり得なかった。この点については、石黒・後掲[⑤]エコノミスト論文83頁、等）はともかくとして、KEIとTTPとの暗号技術面での「共通」性を、まず指摘する（辻井・同上3頁）。その上で、同上・6頁以下で「電子マネーの課題」、同・8頁以下で「情報化と文明構造・文化概念の変容」を論じるのだが、政策面でのインプリケーションとしては、若干弱い印象を受ける。

さて、私が上記③論文でまず強調したことは、冒頭の「これは怖い話である」の一文から知られるように、国家安全保障と国際金融との接点での問題関心が不可欠なこと、である。その際、私は、同上・14頁において、「米市場での邦銀の突発的なドル資金不足に際し……FRBは邦銀の信用リスクを一切負わず、邦銀に関しては日銀が円だけでなくドルで“最後の貸手”の役割を負う」旨の合意がなされたとの、1996（平成8）年3月17日日経新聞朝刊の報道を、かの大和銀行事件と関係付けつつ、論じてもいた。この報道の真價の程は措くとしても、中央銀行の役割論（なお、石黒・国際的相剋の中の国家と企業61頁以下、とくに89頁以下、石黒他・国際金融倒産 [平成7・経済法令研究会] 3頁以下 [石黒]、等）との関係で私が従来から論じていたことと、「電子マネー」問題とは無縁ではない。

内外の一般的な印象論的受け止め方とは別に、電子マネー関連で「エコノミック・チェルノブイリ」的な「金融破綻」の生じ得ることは、既に指摘されていた（石黒・前掲[②]貿易と関税95年9月号37頁参照）。そのことは、同上・39頁以下の注(27)で引用した岩井克人教授の所説（但し、それ自体はインタビュー形式だが、その後同教授との意見交換を直接行い、この点を多面的に確認した。私が上記②論文以来有していた危機意識は、実は岩井教授自身のそれと、完全なまでに同じであったのである！）とも相通ずるものである。そしてそれは、果たしていわゆる「電子マネー（電子現金）」が専ら日常的な少額決済、即ちマイクロ・ペイメント用のものだと考えてよいのか否かの問題と直結する。

この点で、岩井教授が基軸通貨国の通貨の“過剰発行”への欲求を懸念し、かつ、最初に主導権を握った者が圧倒的な力を持つに至る点を指摘しておられること（石黒・同上の注参照）に最も注意せよ。私流に言えば、アメリカの21世紀に向けた覇権願望の問題である（それ [米ドル] と、EUのCAFEプロジェクト [石黒・前掲[②]論文・貿易と関税95年9月号31頁以下参照] での技術的検討を経た EU統一通貨ユーロとの覇権争い、の構図である。なお、EU域内のその後の動向を把握する上では、EUがICカードに独特の

愛着[?]を伝統的に有しつつ、CAFEプロジェクトではあえてアメリカ・ベース [ディ  
ジ・キャッシュ社がオランダ・ベースの会社とされているのは、正しくない。同・31頁]  
のチャウムのネットワーク・キャッシュ主体の研究に力を入れてきた、という EUの動向  
における二重性に、まずもって注意すべきである)。

その意味で、後述の1996年9月にアメリカ財務省主催で開催された会議において、アメ  
リカの金融当局者が遂に揃い踏みをするに至ったことの意味は、重大である。前掲②論文  
執筆当時のアメリカ金融政策の当局者の消極姿勢 (アメリカがWTOでの「貿易と競争」  
論議に最も消極的、と通産省等に思わせつつ、別途WTO基本テレコム交渉を主戦場と  
して、強烈な「貿易と競争」論議を展開していたのと同様のそれ!——石黒・貿易と関税  
97年3～5月号の連載論文参照) は、いつものフェイントであろうと思っていたが、やは  
りそうだったとの思いを、私は新たにしている。

但し、事態がまだ流動的な現時点において、アメリカのフェイントがまだ続いてい  
ることには、別途注意を要する。つまり、96年9月の (岩原教授も大いに注目しておられ  
た) 後述の財務省主催の会議においては、いまだ電子マネーがマイクロ・ペイメント用に  
用いられることを前提としたかのごときスタンスが、全体としては取られている。アメリ  
カからの風に容易に (まさに赤子の手を振るような容易さで!) 反応する日本では、再  
び、電子マネー問題はやはりマイクロ・ペイメント・オンリーのものなのだ、との意識が  
高まるのかも知れない。だが、石黒・前掲[③]治安フォーラム論文22頁と岩村・前掲書109  
頁以下、そして前記の岩井教授の所説は、実は同じことを懸念している。岩村・前掲書110  
頁の「スーパー決済」、つまり、スーパー・ペイメントの問題である (但し、岩村説のこの  
点での位置付けについては、後述する)。

当初私が前記②論文を公表した段階での、日本の関係者の一般的意識は、マイクロ・ペ  
イメント一本槍であり、散々いやな思いもさせられたが、その後徐々に金融関係者も、巨  
額の投資に見合わないかかる議論の前提への不自然さ (私はこの点を強く指摘して来た)  
を反省してか、スーパー・ペイメント用の電子マネー (電子現金) の利用に言及し始めた。  
私がよく言うように、1ドル送るのも1兆ドル送るのも、技術的には同じであり、仮に  
(!) 「マイクロ決済の分野で利用されることを念頭に開発されたものであったとしても」  
そのスーパー・ペイメントへの展開という「大きな変化を見落としてはならない」 (岩村・  
前掲書110頁)、というべきである (岩村・同上130頁以下が「電子マネーは国境を越える」

の項において、米・イラン、米・リビア金融紛争等に言及していること、そしてその意味に、十分注意せよ。ちなみに、同・134頁では、光栄にもこれらの事例についての私の研究がリファーされている。但し、石黒・国際私法 [平成6・新世社] 41頁以下、等をも参照せよ)。

なお、岩村充「電子現金は世界を変えるか」日本経済新聞社編・強い銀行 (日経フィナンシャル96 [平成8]) 所収161頁以下、とくに168頁以下は、「マイクロペイメントとスーパーペイメント」と題して、「証券発行資金とか会社買収資金の送金などの非常に大口の資金決済」(「百億円」から「千億円単位のカネ」の移動、即ちスーパー・ペイメント) 「にともなうリスク」回避のために「電子現金のような技術が使えれば、問題解決のための有力な代替案 [従来のEFTに対する代替案!]」になるだろう。これはこれまであまり意識されなかった“現金”の使い方である。要するに、電子現金は、紙の現金に特有の現物輸送のネックを取り除くことによって、これまで紙の現金が不得手としていたスーパー・ペイメントの世界に“現金”が進出する可能性を開いているわけだ (同・169頁以下) として、「米ドル札の国外流通」の実態 (なお、米・リビア金融紛争に関する石黒・ボーダレス社会への法的警鐘 [平成3・中央経済社] 76頁以下、とくに80頁参照。ちなみに、本稿IVで言及するアメリカ財務省のスタッフによるDOT, infra, at, p.17では180億枚発行された米ドル札 [4,000億ドル相当] のうち、2,700億ドル相当が海外流通分だとされている。上記の米・リビア金融紛争のときより、海外流通分の比率が高まっているようであり、若干注意を引く) を含めた「国境を越える現金」の問題へと議論を進めている。こちらの方が、一層端的な指摘と言えるし、私の認識とも、ぴたりと符合する。

ところで、私が前掲③治安フォーラム論文で強調したもう一つの点は、NTTの暗号技術の“実績”について、である (同・15頁以下)。即ち、1996 (平成6) 年3月13日付の日経産業新聞に「ネットビジネス死角アリ」、「米シティ銀“電子マネー特許”の衝撃——寝耳に水、都銀大あわて」のタイトルのもとに報道された内容を注意深く読めば分かるように、電子マネー、そして電子商取引に広範な特許の網をかぶせようとしたシティ・バンクの日本での特許出願は、NTTの先行する日本特許 (基本特許!) の存在により、電子マネー問題との関係で比喩的に言えば、いわばドーナツ型の、中心部分を欠くものとしてしかなされ得なかったのである (なお、我々の研究会では、シティ・バンクの特許それ自体の検討も、谷・阿部特許事務所の谷義一弁護士を招いて行った。その場では、NTTの

先行特許との関係は十分に詰められなかったが、ともかくシティ・バンクの日本特許の出願書類は、顧客側をも取り込んだ全体的なシステムとしてその特許クレームが書かれており、いざその侵害を訴える際には、若干同銀行側としてやりにくい面があるのでは、との点も明らかとなった)。もっとも、シティ・バンクのアメリカでの出願においては、NTTの対応特許がとくにバリアとはならなかったようで、特許審査のやり方が（邦銀側がクレームをつけている同銀行の日本出願の場合と同様に！）気にはなる（いずれにしても、とくにこうしたNTTの技術レベルの高さ、しかもここでは純然たる基礎研究に基づく基盤技術の開発、及び、基本特許の取得とその威力が示されている訳で、アメリカが国家安全保障の観点からも、こうしたNTTの底力を“脅威”と感ずることは、むしろ自然である。それが「NTT分割論への国際的視点」という、もう一つの問題と結び付くことも、私はしばしば指摘して来ていた。

問題は、日本の中でNTT（そして三菱電機、日本電気、等）の暗号技術のレベルへの認識が十分ではなく、徒に“舶来物”でお化粧して電子マネーを論じる、との雰囲気が強すぎることである（これは、わが自動車・家電・半導体産業等と異なり、わが金融界、とくに国際金融界が、独自の技術ないし金融手法の開発を殆どすることなく、そのユーロ市場での活動を含めて、英米の金融機関の開発した技術・手法に単に相乗りしてこれまで来たという、開発面でのその非主体性にそもそもの原因がある。なお、石黒・国際摩擦と法——羅針盤なき日本 [平成6・ちくま新書] 39頁以下参照。つまり、例えば自国法上の相殺法理の先進性に着目せず、英米からネッティング構想が持ち出されるや、専らそれを前提としてダウン・ストリームであれこれ論ずるのみで、アップ・ストリームな営みに欠けていたのと、同じ現象である。)。その意味では、例えば、田中辰雄「日本にも電子マネー特許がある——世界水準のNTT特許を活用せよ」エコノミスト1996年8月6日号76頁以下にも注目すべきだが、田中・同上76頁には、D・チャウム氏の営みに対してNTTの側は「実用化の点で大きな差」をつけられている、との問題ある指摘もある。それでは、D・チャウム氏自身が再三日本を訪れ、NTTとのクロス・ライセンスを狙っている事実は、どう評価されるのか。

実は、ディジ・キャッシュ社の、つまりはD・チャウム氏の側の構想においては、「イシューア・顧客・店のトライアングル」（チャウムの技術においては、イシューアが別に銀行と限定される訳ではないことを含めて、石黒・前掲②論文で論じておいた）が常に閉じた

状態で、一回一回発行されたディジ・キャッシュはイシューアに戻る形になっている。これに対して、「現金をネットワーク上の情報に置き換えたらどうなるか」との、全くの基礎研究から自然に出発したNTTの技術においては、（イシューアに一々戻す事なく）第三者に譲渡すること、そして、「分割利用性」が、初めからインプットされていた（太田・前掲論文132頁、そして同・137頁のチャウム等との技術比較の表を参照せよ。「譲渡可能性」・「分割可能性」がNTTの電子マネー「電子現金」技術のポイントなのであり、チャウム氏はそこが欲しいのである。）。

なお、D・チャウム氏（ディジ・キャッシュ社）以外の電子マネーは「不純だから……」と言い切った（但し口頭）のは岩井克人教授だが、全く私も同感である。日本の金融界がなぜ暗号の鍵の長さがわずか40ビットの「危ないモンデックス」（しかも、技術非公開!）などに投資したがるのか（また、アメリカでの特許出願との関係や日本のプリペイド・カード法との関係等をどこまで「調査」した上での判断なのか、等々）、私個人としては、全く不可解である。

CRYPTOという暗号の国際学会での検討の経緯を数年間追っただけでも、いかに危ないかは、分かるはずであろう。太田・前掲論文136頁にも、「ICカードは多数発行され、不特定多数に所有〔所持〕されるので、悪意をもった人がカードを分解して、電子現金の偽造を試みる恐れが大きい。この方式で、カードの物理的安全性だけに安全性の根拠を求めるのは大変危険である」、とある。これは国際的な暗号学会（学界）での常識のはずである（!——なお、太田・同上134頁の「表1：決済方式の比較」の「インターネット」上の「オンラインチェック」はディジ・キャッシュ社のシステムに、「ICカード」はモンデックスのそれに、それぞれほぼ対応するので、注意すべきである）。

その意味で、岩村・前掲書「電子マネー入門」を一体どう読むべきかが問題となる。同書は、むしろモンデックスを画期的なものとするかのごとくだからである（再度本稿執筆のため読み直しても、その印象は変わらなかった）。岩村・前掲書26頁以下には、「モンデックスの設計上の最大のポイントは、そうしたICメモリーへのタンパーつまり物理的な侵入は絶対に不可能という前提で作られていることです」、とある。ことあるごとに私は一般の注意を喚起しているが、この部分を同・25頁の「ICカードは本当に安全か」とのコラムと対比して考えるべきである。このコラムには、次のごとくある。即ち——

「ICカードのメモリーを……読む手順はあるかといえ、それはカードの裏側を削

って溶媒に浸してという具合で、技術力のある人にはおおよそわかっているようですが、だからといって、まだ実験段階の電子マネーを誰も攻撃したりはしません。そんなことをしても何の得にもならないし、リバース・エンジニアリングへの連想もあって評判を落とすだけです。だから現状では、ICカードは読まれるかもしれないと覚悟して、万一読まれた場合のことを考えてデータを追跡したり、被害を最小限に食い止めることなどの対策を考えておくことでしょう。それがパチンコカードの教訓です。」

この25頁・27頁の指摘が相互に矛盾するのではないかとの点、そして、上記引用の27頁の指摘に説得力があるかとの点を、太田・前掲論文136頁の学界常識と対比して考えるべきである。また、モンデックスのシステムが、岩村・同上27頁の引用部分後半の「対策」をどこまでとっているか、また、どこまでそれをとり得る性格のものなのかも、別途考えるべきである（リバース・エンジニアリングは別にそれ自体が「評判」を落とす性格のものではないはずだし、ともかく順次私人間で譲渡がなされてゆくICカードにあまりに頼り切ったシステムは、太田・前掲の言うように極めて危険である）。

ところで、NTTの側が「実用化の点で大きな差」をつけられている、との前記のそれ自体問題ある指摘に対して（既述のごとく、私はそうは思っていない）、私は種々の水面下での“活動”をして来た。一つには、（恐らくは「ネットワーク」・キャッシュとなると郵政省が前面に出るし、「キャッシュ」だとなると大蔵省・日銀マターになる、ということでは？）「ハード」たるICカード・ベースでの電子マネーしか実用化の可能性がないとする通産省のスタンスが、ことさらに示されていたこと（そうだとするならば、なぜGIIの実現に向けたOECDの1994年11月末からのOECDインフォメーション・インフラ専門家会合で、専らD・チャウム氏の報告がなされたのか！）の当否を、国会の場で明らかにしてもらうことである。この点については、④石黒「マルチメディア・ネットワークとナショナル・セキュリティ——迫られるセキュリティへの危機意識」オープン・ネットワーク（株）アスキー 1996年8月号58頁以下、とくに63頁の注7に引用したように、国会での質問もその後しかるべくなされるようになってはいる（なお、大津修一「電子商取引——その特徴と必要な対応」立法と調査197（1997年1月）号11頁以下、とくに「ネットワーク型の電子マネーに現実味を帯びさせる」ドイッチェ・バンクの動向を踏まえた同・12頁

の指摘にも注意せよ)。

次に、私は、明確に NTT と日銀とを結び付けることで「日本の活路」を見いだすべきだと考え、それなりに活動した。もとより水面下において、である。それは、⑤石黒「電子マネーで覇権を狙う米国の暗号=盗聴政策の思惑」エコノミスト1996年8月6日号81頁以下、とくに同・82頁で言及した「日本発の具体的提言」の緊急的必要性に鑑みてのものでもあった。

そして、NTT から平成 8 (1996) 年 9 月 11 日に、日銀金融研究所と NTT 情報通信研究所との「共同研究」(NTT の従来技術に対する「改良」) についての NEWS RELEASE がなされた。この共同研究の骨子を私なりに整理すれば、既述のオフライン志向を若干改め、不正使用に対するオンライン・チェックも織り混ぜるようにした点、「電子マネーの発行機関を別に設けることにより、複数の銀行が同一の電子マネーを提供可能なシステム」とした点、二重使用チェックのためのデータベースへの負担を軽減した点、「電子マネーの分割、利用者間での譲渡」の処理速度を速めた点、等が挙げられる(発行機関と登録機関は一応別物として想定されている)。

なお、⑥石黒「日本の電子商取引の現状と課題」1000万人の PC ((株)ソフトバンク) 1996年12月号71頁以下において、私は、日本版ワイアード1996年11月号107頁以下に訳出された S・ペイカー「勃発!! 暗号戦争」(この種の雑誌の題名の付け方は独特であるが、まずもって論述の内容に注意すべきである——なお、「すべてのカギは日本が握っている」という同論文の副題に注意せよ) にも言及しつつ、その72頁以下(石黒・前掲[⑥]1000万人の PC1996年12月号) で、「電子マネーと日銀・NTT の結び付き」の政策的重要性を力説した。同年 9 月 19 日に、後述の財務省主催の会議を踏まえつつ、「アメリカのルービン財務長官が、電子マネー普及のために G 7 協調を行うことについての、日米欧 7 カ国合意を発表した」こと(同上・73頁に私が「やはり思ったとおりの展開だったな、との感慨」がある旨記した点については、既述の「アメリカのフェイント」論を想起せよ) との関係において、である。

だが、平成 8 (1996) 年 9 月 11 日の既述の画期的な発表(日銀金融研究所と NTT 情報通信研究所との「共同研究」) のあと、既に約半年が過ぎようとしている現在、私は猛烈な苛立ちの中にある。日銀のアジア各国の中央銀行との密接な結び付きを足掛かりとして、まずアジアにこの発想を中央銀行ベースで広げて行く一方、ISO や ITU での国際標

準化を、(適宜地域的な標準化を経つつ) 進めるべきだ、というのが私の当面の戦略なのだが、全然何も動いていないに等しい(口銀は口銀法改正で、NTTは「分割」の変形たる組織変えとの関係で、動けないのか。そんなことを言っている場合ではないはずなのに! )。

案の定、OECD 暗号政策ガイドライン作成作業においては「標準化」、とくに国際的なその推進が強調されるに至っている。一体、関係者は何を足踏みしているのか。のろのろしていてEDIの場合の二の舞いになってしまったら何にもならぬのに、と嘆くことしきりである。そうした中で、私は⑦石黒「暗号政策の知られざる相貌 (INVISIBLE WAR OVER ENCRYPTION)」日本版ワイアード1997年4月号91頁以下において、OECD 暗号政策ガイドラインの1996年12月最終案を中心とする多少立ち入った検討も、しておいた(これから論ずるように、更なる変更が、その後97年1月になされている)。

以上、私自身としては、今のところ長短計7本の論文によって「電子マネーと暗号政策」の問題を論じて来ている。それらを踏まえつつ、ここでとくにまとめて論ずる必要のある点としては、当面――

- (1) OECD 暗号政策ガイドライン (最終案) の内容
- (2) アメリカの暗号製品輸出規制とキイ・エスクロ構想――国家管轄権との関係を含めて
- (3) 1996年9月のアメリカ財務省主催の会議とその周辺事情から見た「電子マネーと金融政策」

――の3項目であろうと、私は判断する。以下、その順での論述を行う。

ただ、WTO 基本テレコム自由化交渉 (1997年2月15日に、深刻な問題をはらみつつ、一応決着) や、日本の金融関係者 (とくに民間) が全く関係がないと思込んでいる「フジ・コダック」問題 (1996年6月にアメリカが日本をWTOに提訴――GATT・GATSそれぞれで、いわゆる違反申し立て・非違反申し立ての双方がなされている) が、底流において電子マネー問題と無縁ではありえず、日本側対応が極めて危険な状況にあることだけは、一言しておきたい (石黒・貿易と関税1996年3・4月号、同・11月号、97年3～5月号の連載論文を、当面参照せよ)。

## II OECD 暗号政策ガイドライン（最終案）の内容

まだ、書いたばかりのものゆえ、石黒・前掲[⑦]論文（「暗号政策の知られざる相貌 [INVISIBLE WAR OVER ENCRYPTION]」日本版ワイアード1997年4月号91頁以下）をベースとし、それに、その後入手し得た1997年1月段階でのバージョンでの変更点（問題が問題なだけに、“最終案”に対する更なる変更等もある）等を適宜付加する、という論述方針をとりたいと考える。

上記の⑦論文で検討したのは、1996年12月の最終（となるはずだった？）ドラフトであるが、まず一言しておくべきことがある。即ち、OECDでの既述の検討の当初から、OECD側がパリに本部のあるICC（国際商業会議所）との連携を意図していたことに注意する必要がある。実際にも、こうした流れの中で、検討が山場を迎えた1996年5月7日にワシントン D.C. で、既に ICC 側が用意していた暗号政策ガイドライン案をベースに、まず「グローバルな暗号政策に関する ICC/BIAC/OECD 共催の Business-Government Forum」が開催された（BIACのフル・ネームは、Business and Industry Advisory Committee to the OECDであり、正確には、上記のドラフトは ICC/BIAC 共同提案によるものであった。そしてその翌日の5月8日に、やはりワシントン D.C. で、まさに上記のドラフトをベースにして(!)、OECDの暗号専門家会合が開催されている）。ICCは世界中の民間企業が集まって種々の問題を検討する場と考えてよいが、実はアメリカの意向が強く反映され易い。結論を先に言えば、暗号のような問題については、アメリカの官民が対立しつつ、安全保障（経済安全保障）絡みの局面で微妙に連携する、といったことが起き易いのである。（アメリカの官民間での頻繁な人事交流も、若干関係する。この点に関して、ここで一言すべきは次のことである。即ち、日本語版ワイアード1996年11月号107頁以下に既述の「勃発!! 暗号戦争」を執筆している スチュワート・ベイカー氏は、実は元 NSA（国家安全保障局）代表顧問であり、NSAをやめた後も、OECDの暗号専門家会合・日本政府等の政策動向調査等で一定の重要な役割を果たしつつ、他方で、暗号製品に対するアメリカ政府の輸出規制について、弁護士としての立場でアメリカ企業の側に立って種々の調整をしていたのである。そしてそのことが、ICC/BIACのドラフト作成作業にも深く関係する。同氏のこの微妙な立場は、本文で示した点との関係で、極めて象

徴的な意味を有するのである)。

暗号との関係で言えば、国際的なテロ対策等(「等」が重要である)のために、アメリカ政府は、後述のごとく、一定ビット数以上の暗号解読鍵を有する暗号製品の輸出を輸出管理法で規制している。だが、そうした政府の政策は、国際競争力が強いとされるアメリカの暗号製品や暗号関連産業の国際展開を阻害する。そこにアメリカの官民の対立があったことは、周知のとおりである(この点については、石黒・前掲[②]論文(下)貿易と関税1995年10月号43頁を見よ)。

これは、アメリカ産業の国際競争力強化をどこまでも志向するアメリカ政府自身にとっても、悩ましい問題である。だから、一定ビット数までの暗号解読鍵を有する暗号製品については、アメリカ政府の認める者(それが誰かが問題である)に鍵を寄託した上でなら輸出を認める、ということになる。そして、アメリカ政府は実際に若干の規制緩和を、この点についてするに至ってはいる(詳しくは後述)。他方アメリカの民間の側も、政府が安全保障目的等で暗号通信の内容を、連邦盗聴法の枠内で解読する必要性自体は否定していない。両者の妥協点の模索がそれなりに舞台裏でなされ、そして、ともかくそうした前提の下に、ICCと協力しつつ、OECDでの議論が進むことになったのである(EU域内諸国の動向については既に略述した。ちなみにカナダも、アメリカの政策に対してドイツ同様懐疑的だった)。

さて、OECD暗号政策ガイドライン最終案(1996年12月)の位置付けだが、各国がそれぞれ暗号政策を検討する際の指針、そして、各国が何らかの国際協調をする際の指針となる、というのがその基本的性格である(もとよりこの点は1997年1月の、いわば最終案の改訂版においても、変わっていない。OECD, Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure, Draft Guideline for Cryptography Policy—January 1997 version, DSTI/ICCP/REG/AH(96)10/REV 4, Dist. 06-Feb-1997参照。ちなみに、このGroup of Experts云々の表記は、既述の1994年11月末からのパリでのインフォメーション・インフラ専門家会合の、正式名称である)。96年12月最終ドラフト、そして97年1月の上記改訂最終案において合意された8原則を、まず列挙しておく(便宜、パラグラフの番号の整理された後者[97年1月]の最新のものパラグラフをも、「パラ[63]」のごとく示しておく)。

(1) 皆が信頼できる暗号手法(cryptographic method)を目指すべきこと(パラ

[63]-[65])、

- (2) 利用者はいかなる暗号手法の選択も各国の関係法令の下で自由たるべき (should) こと (パラ [66]-[69])、
- (3) 暗号手法の開発は市場主導でなされるべきこと (パラ [70]-[71])、
- (4) 暗号手法のための技術標準等 (technical standards, criteria and protocols) が国内・国際両レベルでオープンな形で整合的に作成されるべきこと (パラ [72]-[73])、
- (5) プライバシー・個人情報保護の尊重 (パラ [74]-[76])、
- (6) 各国当局の「合法的アクセス」 (lawful access: 平文・暗号解読鍵・暗号化されたデータへのアクセス) は、このガイドラインの他の諸原則を最大限尊重した上で、容認され得る (may allow) こと (パラ [77]-[80])、
- (7) 暗号解読鍵の所持者やそれにアクセスする個人・機関の「責任 (liability)」が、契約、国内立法あるいは国際協定 (条約) によって明確に定められるべきこと (パラ [81]・[82])、
- (8) 暗号政策の名の下に正当化されない貿易障壁が設けられないようにすること、あるいはそれを除去することを含む、各国政府の国際協力の必要性 (パラ [83]-[88])。

——以上の8原則がそこで示されている。

言うまでもなく、最も問題なのは(6)の合法的アクセスである。(6)で may とあるにとどまることは、それ自体が烈しい議論の末の妥協である。アメリカはもともと数年前より、合法的盗聴のための各国当局間の国際的なネットワーク作りをするべく、(日本も含めた) 主要諸国と協議して来ていたようである (石黒・前掲[②]論文(下)貿易と関税95年10月号41頁で、この点を示すアメリカの文書も引用しつつ、論じてあるので、適宜参照されたい)。そうした方向を制度的に推進する (つまり各国に何らかの義務を負わせる) 形でこのガイドラインが出来上がることを、私は最も恐れていたが、最悪の事態は、かくともかくも避けられそうな状況である。

だが、要するにこの点も含めて、(1)の原則にも若干示されているように、各国が自国の主権に基づいて適宜判断するということになっただけである (97年1月の上記改訂最終案パラ [26] ——96年12月版ではパラ [21] ——) にあるように、このガイドラインは各国

の sovereign rights に影響を及ぼすものではない、というのが基本的前提になっている。  
また、97年1月の上記改訂最終案パラ [78] ——96年12月版ではパラ [69] ——にあるように、このガイドラインは lawful access を認める立法をすべきだとも、すべきでないとも言っていない。この点については完全にニュートラルなのである。各国が別途国際盗聴メカニズム作りをするために条約を結ぶ、等の展開になることは、十分あり得ることである。

この点で、注意すべきは、(8)の原則の中に、「国境を越えた合法的アクセスは、二国間または多国間の協力ないし協定によって行われ得る (may be achieved)」とあることである (97年1月の上記改訂最終案パラ [86] ——96年12月版ではパラ [74] のあとのパラ [new 7])。だが、この曖昧な書き振りからは、ある国が一方的に自国盗聴法の域外適用をすることは、必ずしも排除されない (ちなみに、1996年6月段階での OECD ドラフト一般原則(6)の「キイ・マネージメント」の項には、“In an international context, government access... should be achieved through international agreement and cooperation, where necessary for the supply of keys or deciphered data across national borders.” とあったことに注意すべきである。should がトーンダウンして may となったのである)。

そもそもアメリカが、政府の認める者に鍵の寄託をした上で外国 (例えば日本) への暗号製品の輸出を認める、というスタンスであることの実地上的意味を、じっくり考えるべきである。要するにそれは、必要があったらアメリカ政府が合法的に (アメリカ法の下で合法と言うのみ、他国の法制度において合法かは問わない?)、日本の企業や個人の暗号化された通信内容を、その通信がアメリカ国内でなされたのでない場合にも (!) 解読できるようにする、ということである。

そこに、1995年の日米自動車摩擦の際に日米のマスコミで報道された CIA の盗聴の問題をインプットして考えたとき、問題の本質が明らかとなるはずである。テロや脱税、マネー・ローンダリング等の犯罪防止のために、「合法的アクセス」という名の盗聴が当局により行われること自体は、厳格な法的条件 (要件) の下でなら、誰も一概には否定できない。だが、この種の制度が容易にスピルオーバーする危険性が、問題なのである。また、国ごとに、個人の人権保障に深く絡む当局の盗聴を、一体どんな条件の下に認めるかが異なるのに、勝手に他国の側から盗聴をされてしまう、というあり得べき事態の展開

を、どうやって防いだらよいのか。そこが問題の本質なのである。

既述のごとく、日本の場合には、憲法21条の定める「通信の秘密」との関係での問題である。注意すべきは、仮に合法的盗聴のための条約が作られ、日本がそれを批准したとしても、条約で憲法の規定を骨抜きに出来るのか（答えは否）、という大問題があることである。また、日本の当局に対しては、自らが盗聴をする背後で、外国の当局（通商摩擦の関係当局を含み得る！）が外国で日本での通信を傍受しているという構図が相当程度の現実味を帯びていることに、十分留意したうえでの政策決定が、強く望まれる。とかくゲート・キーパーが不在で国際感覚の乏しいのが霞ヶ関の実態だが、事柄は日本の安全保障、そしてほかならぬ人権保障（但し、クロスボーダーなそれ）に、深く絡むのである。

古典的な戦争よりも、「見えざる戦争 (invisible war)」としての通商摩擦、そして経済安全保障が、ここでの主たる関心事となる。暗号化された通信が、アメリカの領域を通過しておれば、それを盗聴・傍受するのは何ら「域外」適用ではないから、アメリカが自国法のみを基準に自由に出来る、ということも言われ得ないではない。

だが、この点については、OECD 暗号政策ガイドライン最終案にも、(8)の原則との関係で、暗号データが自国領域内を通過する際に、それを暗号政策のみに基づいて阻害すべきではない (should)、という条項がある (97年1月の上記改訂最終案パラ [87] —— 96年12月版ではパラ [74] のあとのパラ [new 8])。こうした阻害行為が十分に起こり得ることを意識した条項である。だが、そこでの押さえは十分でない。やんわりとした should だし、他の政策、例えば通商政策と合体しておればよい、ということにもなる。

この点で再度注意すべきは、この OECD 暗号政策ガイドライン作成作業において、以前の案には次のような条項があったが、それが消えていることである。すなわち、1996年6月段階での OECD ドラフトでは、IVの一般原則(7)の「責任」の項に、“No key holder should be liable for disclosure of a key to a lawfully authorised agency within the same country as a key holder, or to an agency in another country in accordance with an international agreement.”との条項があり（上記のアンダーライン部分をつなげて見よ。なお、そこで国境を越えた外国当局への鍵のリリースが、国際協定に基づくものとして想定されていたことにも注意せよ！）、暗号解読鍵の寄託を受けている者が「外国の」当局からの命令で鍵をリリースした際の「責任」を、否定する方向で考える規定が、上記のごとくあったのだが、結局それが消え、前記の(7)の原則の中で、この点で多少曖

味な条項が置かれるのみとなっているのである。前記最終案の規定を、ここで示しておく。97年1月の上記改訂最終案パラ [82] 後段（96年12月版ではパラ [72] 後段）である。そこには――

“A keyholder should not be liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.”

――とある。「国境を越えた lawful access」の真の問題点が規定上明示されず、かつ、国際協定によってそれを行うべきだ、といった縛りもなくなり、あいまいなものとなってしまったのである。

なお、“lawful access”には、暗号解読の鍵をユーザーが紛失した場合の問題も含まれている（例えば97年1月の上記改訂最終案パラ [80] ——96年12月版ではパラ [70] 参照）。ちなみに、“lawful access”の定義は、97年1月の上記改訂最終案パラ [56]（96年12月版ではパラ [49]）において、“access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law”となっているが、「政府による合法的アクセス（盗聴!）」の問題を一緒に規定したため、問題の焦点がボケてしまった観があることは、否めない。

ここで一点注意しておけば、鍵の寄託等が国際取引との関係を含めてなされる際に、契約準拠法が問題となる。その契約関係にどこの国の法が適用されるかの問題である。その準拠法を例えばアメリカのどこかの州の法としてしまうと、知らない間に自分の鍵がリリースされた場合等の紛争（民事紛争）について、日本の裁判所で争ったときにも、基本的にその州法（そしてそこで妥当するアメリカの連邦法）に基づいて判断されることになる。鍵の寄託を含むメカニズムは、前記ガイドライン案では「キイ・マネージメント・システム」と呼ばれるに至っているが、ともかく、例えばアメリカ系の寄託機関（認証機関）の日本進出等との関係でも、注意を要する点である。ちなみに、前記の第1原則との関係で97年1月の上記改訂最終案パラ [65] ——96年12月版ではパラ [57 bis]。若干の文言の変更があるので前者の文言を示す――には、以下の規定がある。即ち――

“In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdictions whose laws apply to that system.”

——との規定である。あまりうまい表現ではないが、上記の契約準拠法選択の問題がそこで扱われているのである。

さて、外国での出来事について自国の盗聴法を域外適用したりすると、正確にはそれが露見すると（後述のごとく、1996年12月の暗号製品〔ソフト及びハード〕に関するアメリカ輸出管理法上の規制とこのOECDガイドラインとは、重要な部分において、極めて微妙な主義の不整合を生じさせている〔!〕。97年1月の上記改訂最終案パラ [79] [89] ——96年12月版ではパラ [68][70] ——との関係での問題である）、ユーザーや外国側の反発を招いたりして、とかく面倒である。この点について、自国テレコム関連産業の国際競争力の維持発展をはかる意図をも強く有しつつ、自国を国際通信のハブとし、極力世界中の通信が自国を経由するように持って行ければ、実に都合がよい。——私がアメリカの当局者だったら、まずそう考える。

この観点からは、日本企業のインターネット・サーバーが好んでアメリカ国内に置かれる傾向にあるという現象も、また、主としてアメリカの事業者による国際コールバック・サービスが通信料金の安さのみの理由で注目されることも、誠に都合がよい。特に、国際コールバック・サービスの場合には、例えば日本から中国への通話が、アメリカ発日本へ、アメリカ発中国へ、の二本の通話に置き換えられる。第三国間の通信も、すべてアメリカ発となるのである。しかも、法執行目的での合法的盗聴をサポートする通信システム作りをアメリカのキャリア等に命ずる連邦法は、既に1994年10月に成立している（石黒・前掲 [②]論文(下)貿易と関税95年10月号43頁以下で検討した Communications Assistance for Law Enforcement Act である。連邦盗聴法 [Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510-2520] を含め、こうした法規はアメリカの管轄下の企業、つまりアメリカに拠点を置き、もしくはアメリカとの関係で一定程度以上の事業活動を営む者には、広汎に適用され得る)。もはや、準備万端整ったり、という感じである。

そこにさらに、スパイ衛星用の軍事技術の転用による、イリジウム計画等の低軌道移動衛星システムの登場である。そしてそれが GII の一つの理想的な姿だ、という見方がアメリカ経由で世界に広がりつつある。どこの国の領土（領空は別！）をも経由せずに、世界中どこからどこへでも、ダイレクトになされ得る通信である。そのシステムの根幹を握っておれば、一層世界中の通信は筒抜けになる（但し、単に聞かれるのみなのか。そこが問題でもある）。たしかに誠に都合のよい「理想」である。

かくて、かつてのローマ帝国でも出来なかったような隠微（淫靡？）な世界制覇が、着々と世界のどこかで準備されている、といったら言い過ぎであろうか。私はそうは思わない。

ここにおいて、暗号製品に関するアメリカの輸出管理について、若干見ておく必要が、出て来ることになる（関係者の間で若干混乱があるようなので、はっきりさせておかねばならない）。

### III アメリカの暗号製品輸出規制とキイ・エスクロ構想——国家管轄権との関係を含めて

1996年10月1日、アメリカのゴア副大統領により、暗号製品の輸出規制（輸出管理）の緩和をする旨の声明が出された（Gore Statement on Encryption Proposal, Oct. 1, 1996）。56ビットまでの鍵の長さのものについて、一定の条件のもとに今後は輸出を認めるとの内容のものだが、問題はその条件（要件）であり、それについては——

“...contingent upon industry commitments to build and market future products that support key recovery.”

あるいは——

“...contingent on commitments from exporters to explicit benchmarks and milestones for developing and incorporating key recovery features into their products and services, and for building the supporting infrastructure internationally[!].”

とある。とくに、最後の“internationally”に注意すべきである(!)。

「キイ・リカヴァリー」とあるが、この時点において既に、アメリカ政府は「キイ・エスクロ」のことを、こう呼ぶようになっていた。56ビットまでの暗号解読鍵の長さのものについては、輸出ライセンスを与える時点でキイ・エスクロ、つまり政府の側の合法的盗聴を担保するための鍵の寄託のシステムを現に有していなくとも、当該企業がその方向で鋭意努力し、その成果を実施する旨のコミットメント（約束）をするなら、ライセンスを与える、ということである。だが、“The relaxation of controls will last up to two years.”

とそこにあるように、この規制緩和は、あくまで「時限的」なものである (“the temporary relaxation of [export] controls” ともある。なお、ソフト・ハードともに対象となる)。

それがなぜかの理由についての私なりの考えを、(殆ど自明に近いことだが) あらかじめ示しておこう。従来のアメリカ輸出管理法による規制においては、40ビットまでの鍵長のものがリミットだった。この程度ならば、NSA や CIA 等が十分自力で解読できるから、というのがその理由のようである。だが、一方では、既述のごとくアメリカの強い暗号製品が海外でのシェアを十分取れぬことの問題と不満もあり、他方では、とにかくアメリカの息のかかった暗号製品で極力世界を席卷しておいて、同時進行的に国際的なキイ・エスコロ・ネットワークを築き (企業側にそれを築かせ)、いつでもアメリカ政府が国際的盗聴をできるようにする。そして、その一方的措置(!)の裏付けをもって、他の諸国との国際盗聴ネットワーク作り (二国間・多国間の国際協定による「共助」枠組みの設定) を行う、というのが全体戦略であろう (後述の諸点がこれを見事に裏付ける)。日本で言う CA (認証機関ないし登録機関) も、もとよりそのターゲットである (既述。邦銀等においても十分この点を認識すべきであり、かつ、この種の「盗聴」が、制度のスピルオーバーの問題として、単に通信内容を「聞かれる」のみでなく、殆ど立証不能の状況においてデータ改ざん・捏造・消去、等の破壊活動をも、もたらし得ることに、注意すべきである。とくにメッセージ蓄積型通信サービスが最も危ない)。

このゴアの声明においては、“Exporters of 56-bit DES or equivalent encryption products would make commitment to develop and sell products that support the key recovery system that I announced in July.” 云々とあり、かつ、暗号製品についての規制権限が国務省から商務省に移されている (それ自身は、いわばポーズの類いであり、実際の規制とはあまり関係しない)。他方で、アメリカ政府が政府用のいわゆる key recovery products の購入拡大を続けるから頑張れ、といったメッセージもそこにある。そのかわり、56ビットのものについてのライセンス (1回の審査で6カ月有効) は、上記のコミットメントに基づく進捗状況を更新の際に審査され、かつ、2年経ってもいまだキイ・リカヴァリーをサポートしていないなら、もはや輸出は認められないとされている。

こうした国家安全保障 (経済安全保障を含む!)の裏付けを鮮明に有する、極めて戦略的な規制緩和 (しかも是が非でも輸出をしたいアメリカ企業を飴と鞭で巧妙に政策誘導す

る“暫定的”な緩和措置)の真の意図が、日本側ではかなり情緒的に受け取られているようで、私は重大な懸念を有している。この点は、1996年12月の商務省の規則に即して更に後述する。ここでは、補足的に2つの点を示しておこう。

まず、モンデックスの場合の暗号鍵が40ビットのみだったという点について。モンデックスは当面アメリカの領域外での実験等を行っているが、アメリカでそれを行うことが既述のCRYPTOという暗号国際学会のここ数年の議論(特許関連でのそれを含む!)との関係でどうか、との既述の点は措くとしても、アメリカ輸出管理法上の再輸出規制(reexport controls)との関係が有り得る。もともとアメリカの輸出管理法は、同国の反トラスト法以上に烈しく「域外適用」されて来たものであり(石黒・前掲国際的相剋の中の国家と企業3、36、98頁、同・前掲国際民事訴訟法93頁注230、小原喜雄・国際的事業活動と国家管轄権[平成5・有斐閣]279頁以下、等参照)、ポスト・ココムの問題状況においても、むしろその牙は、規制範囲を限定しつつ、逆に強化されている(小原・同上319頁以下)。その独特の「再輸出」概念は、常にエンド・ユーザーが誰かを直視し、かつ、一国の中でのユーザーの移転も「再輸出」(アメリカからのダイレクトな輸出に対する「再輸出」)である)にあたるとされる。当該技術が一体誰の手にわたるのかを、常に問題とする規制方針の現れが、この再輸出規制なのである。モンデックスの場合も、あるいはそこを意識して、問題のない40ビットまでに鍵長を下げているのではないかと、とも思われる。だが、その点(安全性のレベル)を顧客に開示しないことの問題は、別にある。

次に、1996年7月16日のネットスケープ社のプレス・リリース(Netscape Granted Approval by U.S. Government to Distribute Highly Secure Versions of Navigator, July 16, 1996)において、同社が初めて128ビットの鍵長の暗号ソフトをインターネット(ないしイントラネット)のダウンロード用に使用できる旨、アメリカ政府の許可を得た、との点であるが、そこにも“International versions of Netscape Navigator... are limited to a 40-bit key as required by the U.S. government.”とあるように、あくまでこれはアメリカ国内でのダウンロード用である(なお、石黒・前掲[⑥]論文71頁の\*1[暗号技術]の注参照)。それが認められたということは、アメリカ国内から更に海外に流れることの抑止のためのメカニズムとしてアメリカ政府を納得させるだけのものが、そこにビルト・インされている、ということの意味する。そして、その後に56ビットまでの緩和「等」(後述)が、既述のコミットメントを代償としてなされた、ということになる。

さて、以上を前提として1996年12月30日のアメリカ商務省“暗号輸出規制”を、見ておくこととする (Department of Commerce Encryption Regulations, Federal Register Vol. 61 No. 251, pp. 68572-68587)。もとよりこれは既述のゴアの声明を具体化したものであり、アメリカ輸出管理法のもとでの輸出管理規則 (EAR: Export Administration Regulations) の、(既述の意味における極めて戦略的な)「暫定的 (interim)」改正 (1998年12月31日まで) である (なお、時限立法たる輸出管理法は1994年8月20日に失効したわけだが、大統領が同年8月19日の Executive Order 12924 [60 FR 42767, 42527] により国際緊急経済権限法を発動して、その後も効力を有しつづけている [Department of Commerce, supra, at p. 68576])。

事実、この規則の冒頭頁 (Id. at p. 68573) には――

“The plan [of the Administration announced on Oct. 1, 1996] envisions a world-wide key management infrastructure with the use of key escrow and key recovery encryption items to promote electronic commerce and secure communications while protecting national security and public safety. To provide for a transition period for the development of this key management infrastructure, this rule permits the export and reexport of 56-bit key length DES or equivalent strength encryption items under the authority of a License Exception, if an exporter makes satisfactory commitments to build and/or market recoverable encryption items and help build the supporting international infrastructure. This policy will apply to hardware and software.”

――とある。そこにすべてが示されている、と言える (Ibid には、“This initiative will preserve such [export] controls and foster the development of a key management infrastructure necessary to protect important national security and law enforcement concerns.” とある。これが、私が最初から懸念していた「国際的盗聴ネットワーク」作りの問題である。しかも、一方的措置としてアメリカは、それを実行しようとしているのである。なお、Ibid において、“all destinations, except Canada” とあることにも、若干注意を要する。カナダは、OECD での暗号政策ガイドライン作成作業において、アメリカのキイ・エスクロ構想を警戒していた国の一つである。アメリカが国際通信関連のいわゆる国際計算 [清算] 料金についてのベンチマーク規制を、やはり1996年12月に行った際

にも、カナダに対してはベンチマーク設定を見合わせていたことが、ここで想起される。  
石黒・貿易と関税1997年3-5月号連載論文参照)。

ところで、実はこの規則では、56ビットの鍵長までのもののみでなく、他のものについての規制方針も決定されている。 Department of Commerce, supra, at p. 68573ffによれば、商務省のこのライセンス・ポリシーでは、(1) 一定の mass-market encryption software, (2) Key Escrow, Key Recovery and Recoverable software and commodities, (3) Non-recovery encryption items up to 56-bit key length DES or equivalent strength supported by a satisfactory business and marketing plan for exporting recoverable items and services, (4) All other encryption items とに分けた規制がなされている。日本では上記の(3)のみが注目されている訳だが、それ自体、アメリカの全体的意図を見失うものとして、極めて危険である。

さて、順に(1)から規制の概要を見て行こう。この(1)について、40ビット(まで)の鍵長のこのカテゴリーのものは従来から規制が緩いが、ただ、オブジェクト・コードのかたちのもののみ (encryption software in object code only) について緩い規制なのであって、ソース・コードについては、別途審査がなされる(他のカテゴリーについても同様。Id. 68575.)。そこで規制外とされないと、カナダ以外への輸出及び再輸出は個別審査が必要で、これはケース・バイ・ケースで審査される(なお、Id. 68583fのこの(1)のカテゴリーに関するガイドライン [Supplement No. 6 to Part 742] においては、鍵長40ビットまでのデータ暗号化アルゴリズムであること等の要件の下に簡略な許可が与えられるとする際、“the key exchange used in data encryption must be... [a] public key algorithm with a key space less than or equal to a 512 bit modulus and/or;... [a] symmetrical algorithm with a key space less than or equal to 64 bits; and... [t]he software must not allow the alteration of the key management mechanism and its associated key space by the user or any other program...”等々の、鍵の交換等についてのややこしい規制が伴っていることが示されている。この点も十分注意すべきであろう。もとよりこうした点は、このカテゴリーだからアメリカからの輸出規制が緩和されたはずなのに、アメリカ側のパートナーがいろいろと我が国企業の側での行動に注文を付けてくる、といった形で顕在化するであろう)。

(2)のカテゴリー (Key Escrow, Key Recovery and Recoverable software and

commodities) が、重要である。鍵長のビット数にかかわらず個別審査の例外がこれについても認められる（但し、その仕向先国はキューバ・イラン・イラク・リビア・北朝鮮・シリア・スーダンを除く）。その申請が favorable consideration を受けるためには、輸出及び再輸出に先立って（prior to）商務省を満足させる key recovery agent が特定され、かつ、同じく商務省を満足させるような security policies for safeguarding the key(s) or other material/information required to decrypt [!] ciphertext as described in Supplement No. 5 to part 742 が確立され、更に、輸出及び再輸出後もそれが維持されることが必要だ、とされている（輸出者又は再輸出者が自分で key recovery agent たらんとするときも同じ要件。なお、Supplement No. 5 to part 742 については後述）。

さらに、この(2)のカテゴリーについても次の方針が示されていることに、注意すべきである。即ち――

“Requests for one-time review of recoverable products which allow government officials to obtain, under proper legal authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications will also receive favorable consideration.”

純然たる犯罪捜査やテロ防止ならばともかく、広範に定義されたホワイトカラー犯罪や企業不祥事等（ここでも「等」が重要）を念頭に置いて考える必要がある。犯罪者に盗聴を告知することは馬鹿げているが、そうでない場合について、既述の制度のスピルオーバーの実例をもインプットして考えたとき、とくに上記引用部分の「ユーザーの協力なしに、あるいはその者が知ることなしに」官吏が盗聴をするという構図が、そこに示されている。しかも、こうしたシステムの国際的定着を foster するのが、この規制緩和政策の実像なのである。「規制は悪」・「競争は善」といった昨今の教条主義的市場原理主義者の子供じみた発想とは無縁の、「国益剥き出しの規制緩和」、なのである。

なお、ここであらかじめ既述の OECD 暗号政策ガイドライン に今一度立ち戻って考えるべき点がある（若干、予告しておいた点である）。1997年1月の前記改訂最終案パラ [79][80]（96年12月版ではパラ [68][70]）には、lawful access のプロセスは、国内法にしたがって audited or reviewed できるように、記録されるべきだ (should) とされている。その前の文は must ゆえ、これ自体、トーンダウンした規定ぶりではある。また、そこには、暗号解読鍵への lawful access のプロセスにおいては、「秘密をプロテクトする

ための鍵」と「他の目的オンリーに使用される鍵」との間で区別せよ (must) とあり、続いて――

“A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of individual or entity in lawful possession of that key.”

――とある。猛烈な論争の結果の妥協であろうが、微妙な鍵の分類問題等は別として、前記の商務省規則に「ユーザーの協力なしに、あるいはその者が知ることなしに」官吏が盗聴をするという構図が示されていた点との関係が、問題となる。

実は、Department of Commerce, supra, at p. 68575 における recovery encryption products の定義自体が “encryption products (including software) that allow government officials to obtain, under proper legal authority and without the cooperation or knowledge of the user, the plaintext of the encrypted data and communications” となっているのである。

しかも(!)、若干先走ってここで言及しておけば、Id. 68582 の “Supplement No. 4 to Part 742—Key Escrow or Key Recovery Products Criteria” には、ユーザーの協力なしに、また、ユーザーが知ることなしに、政府の官吏が復号化のための鍵を手に入れられるようになるまで、その暗号製品の機能が inoperable でなければならない (shall) といったことも示されているし、更に、この 新規制方針の基本を示す次のような一文も見いだせる。即ち――

“Since the establishment of a key management infrastructure and key recovery agents may take some time, BXA [DOC] will, while the infrastructure is being built, consider exports of key recovery encryption products which facilitate establishment of the key management infrastructure before a key recovery agent is named.”

――との一文である。そこの “facilitate” の語に注意すべきである。明らかにそこで商務省 (アメリカ政府) は、今すぐ起こるかも知れぬ外部からのテロ等への対策よりも、長期的な key management infrastructure のグローバルな整備を、優先させている(!) からである。まず輸出させておいて、その上でかかるシステムの構築を急ぐ (急がせる) の

である。

また、Id. 68582f の “Supplement No. 5 to Part 742—Key Escrow or Key Recovery Agent Criteria, Security Policies, and Key Escrow or Key Recovery Procedures” にも、いろいろと恐ろしいことが書かれている。

とくに、かかるエイジェント (Key Recovery Agent) の備えるべき Security Policies の(3)には、lawful access の要請のあった事実、鍵を渡したか否か、誰が要請をしたのか、等の点についての [当局の] 許可なき情報の開示 (unauthorized disclosure of information) をプロテクトするポリシーを実施せよ (shall)、とある。この点など、前記の OECD 暗号政策ガイドライン案の規定 (1997年1月の前記改訂最終案パラ [79][80]—96年12月版ではパラ [68][70]) の基本的趣旨との関係で、大いに問題となる点であろう。「アメリカ政府の合法的盗聴を担保する」のみならず、「盗聴の事実・要請の有無、等に対する守秘義務」を、アメリカ側事業者が、法的に負う、ということである (その事業者の日本の拠点がいかなる立場に置かれるか[!] は、従来の輸出管理法の域外適用事例から推察すべきことである)。商務省は、かかるエイジェントがしかるべき基準を満たさない場合には、いつでも輸出ライセンスを取り消す権限を保有しているが、とくにアメリカの領域外に Key Recovery Agent が置かれる場合には、(当該国の政府との協議を適宜まじえつつ [as appropriate(!)]) それを商務省にとって acceptable ならば (いかなる意味でアクセプタブルとされるかが問題である!)、これを認める旨の注 (Note) を別途付している (Id. p. 68582)。

次に、前記の(3)のカテゴリー (Non-recovery encryption items up to 56-bit key length DES or equivalent strength supported by a satisfactory business and marketing plan for exporting recoverable items and services) についてのこの商務省規則の概要を見て置こう (Id. at p. 68574)。輸出段階ではアメリカ政府のキイ・リカヴァリーへの要求を満たしていないが、当該企業側が2年間のこの暫定規則の有効期限内 (1997年1月1日から始まるそれ) においていかなるステップでキイ・リカヴァリー・システムへの移行を行うかが、一々、そして定期的にチェックされる。そこでも、アメリカ政府がアメリカ国内だけを考えている訳ではないことに、十分注意すべきである。「連邦盗聴法の (過度な) 域外適用を輸出管理法・同規則でサポートする」構図は、鮮明である。そして、このカテゴリーについては、Supplement No. 7 to part 742 (Id. at p. 68584) に従う事が必要とさ

れる。そこで必要とされるコミットメント・プランの中には、“benchmarks and milestones for incorporating key recovery features into products and services, and for supporting key management infrastructure, including key recovery agent(s)” を含むべきである (should)、ともされている (ここだけのことではないが、「サービス」とある点にも十分注意せよ!)。なお、かかる個別ライセンスの例外措置の更新のためには、6カ月毎に商務省に対して上記マイルストーンの進捗状況の報告が義務づけられている。

最後の(4)のカテゴリー (All other encryption items) は従来通りケース・バイ・ケースで処理される。

なお、以上すべての前提として Id. at p. 68574 に示されていることは、アメリカ以外のソースから同等の暗号製品が入手可能であっても、かかる規制がかけられる、ということである (大統領の Executive Order 13026, section 1(a) が引用されている)。なお、U.S. person によるアメリカの外での技術指導への規制 (禁止——Id. at p. 68584) との関係では、学会や講義で暗号関連の議論をすることが、それ自体としては (by itself) 違反の意図 (intent) ありとはされない、とある。従来は、こうしたことでも、輸出管理法上の「再輸出規制」への違反とされ、大きな問題となっていたことを、想起すべきである (石黒・前掲国際的相剋の中の国家と企業9頁、等参照)。

以上が、1996年12月のこの商務省規則の概要である。単純な規制緩和でないことは明らかである。また、すんなりとアメリカの高度な暗号製品が(安く!)手に入ったということでそれに飛びつくと、クロスボーダーな国際的盗聴(それがあつたこと自体に対しても守秘義務がかかっている)の餌食になり得る、といったことを事前に考えて置く必要のあることも、それなりに理解できるはずである。

さらに、継続的な暗号自主技術開発レベルの維持・発展の、(経済面を含めた)国家安全保障上の重大性も、以上の点からして、明らかであろう (NTTの研究所の分断は、かかる意味で、自衛力の一方的放棄を意味する。絶対にしてはならない!)

なお、1997年1月28日に、新任の「暗号特使 (US Envoy for Cryptography)」たる Ambassador David Aaron の、“International Views of Key Recovery” と題した講演が、RSA Data Security Conference の場においてなされた。そこでも——

“Second, and very important, the Administration will license the export of encryption products, of any algorithm and any key length, if they incorporate key

recovery.”

——との点が示されている（if 以下が重要）。アーロン特使は外国政府との暗号政策協調のために任命されたのであり、“My goal is an international consensus on the development of a global key management and key recovery architecture—one that will foster robust and dependable security for the global information infrastructure while protecting public safety and national security.” との目的意識（私が前記①論文以来懸念して来た事柄！）が、鮮明に示されている（同特使の日本訪問も、そこでメンションされている！）。

面白いのは、そこに、殆どすべての国の政府が、56ビット鍵長の non-key recovery products の輸出規制緩和を（前記のコミットメント付きであったとしても）、自国の安全を危険にさらす unhappy なものとしている、との指摘のあることである。アメリカ国内でのコントロールのないこと（absence）が懸念されているようである。その前後の指摘を併せ考えると、私には、今回の輸出規制緩和は、外国政府に危機意識を抱かせつつ、上記のコンセンサス作りを加速化・確実化するための、相当高度な国家戦略に基づくもののように、思われて来る（なお、“As many of you know, we have included as many US business representatives as possible on the US delegation to the OECD meetings on encryption.” ともされている。日本の OECD 戦略は全くなっていないし、企業側も、同じバリの ICC が前記暗号政策ガイドライン作成作業に、既述のごとく深く関与していたのに、殆ど無関心であったことも考えると、こういう国が生き延びられる訳がない[!]、との嘆きを、今更ながら深くせざるを得ない。残念である）。

#### IV 1996年9月のアメリカ財務省主催の会議とその周辺事情から見た「電子マネーと金融政策」

1995年9月19～20日にワシントンD.C. でアメリカ財務省主催の会議が、既述のごとく開催された（U.S. Department of the Treasury Conference: Towards Electronic Money & Banking: The Role of Government, held on Sept. 19-20, 1996）。アメリカの金融当局者（FDIC や通貨監督庁 [OCC] を含む）のほか IRS や FTC、税関、そして海

外からは BOE（イングランド銀行）等、多彩な顔触れであり、アメリカ側はまさに、既述のごとく「揃い踏み」状態であった。なお、この会議の概要については、吉永高士「米財務省が電子マネーセミナーを開催——普及は50～70年先との J・リード・シティコープ会長見解も」金融財政事情1996年9月30日号32～34頁の簡単な紹介もあるが、何たる副題の付け方か、とまず思う。吉永・同上34頁によれば、「財務省代表をはじめ米政府関係者からは、電子マネー分野でアメリカが主導的役割を担っていくとの姿勢が異口同音に繰り返された」とある。本稿でこれまで論じてきた諸点は、いわばこうしたアメリカ当局者の意図を根底において支えるインフラ整備との関係での営為だ、ということになる（D・チャウム氏とそのディジキャッシュ社がアメリカにいわば根っこを置いていること、まさにアメリカ主導のインターネットを利用したのがそのディジ・キャッシュであることを、再度想起せよ！）。吉永・同上頁には、上記引用部分にすぐ続いて、「ただし、いずれの講演者も、具体的政策について踏み込んだ見解を打ち出すというよりも、歴史的考察を含めた現状分析と今後の方向性に対する認識を示すにとどまった」とある。だが、遂にアメリカ政府が直接動き出した(!)、との点がまずもって重要なのである。

さて、ここでは、この会議のたたき台として財務省のスタッフが用意した非公式ペーパー（“An Introduction to Electronic Money Issues, prepared for the U.S. Department of the Treasury Conference: Toward Electronic Money and Banking: The Role of Government, Sept. 19-20, 1996, Washington, D.C., written by staff from the U.S. Department of the Treasury offices”……以下、DOT, supra として引用する）のほか、この会議に提出されたものを含め、関係するいくつかのペーパーを適宜参照しつつ、若干の点を示しておこう。まず上記の会議に提出されたものとして——

- ・ Keynote Address by Secretary Robert Rubin（以下、Rubin, supra として引用）
- ・ Remarks by Alan Greenspan, Chairman, Board of Governors of the Federal Reserve System（以下、Greenspan, supra として引用）
- ・ Remarks by Eugen A. Ludwig, Comptroller of Currency（以下、Ludwig, supra として引用）

関連する文書として——

- ・ FDIC General Council's Opinion No. 8 (August 2, 1996): Stored Value Cards, 61 Fed. Reg. 40490（以下、FDIC, supra として引用するが、頁は Fed. Reg. に載る前の

Notice のもので示す)

- ・ Comptroller of the Currency, Stored Value Card System [Guidance on Smart Card/Stored Value Card Risks], OCC Bulletin 96-48 (September 3, 1996) (以下、OCC, supra として引用)
- ・ Remarks by William J. McDonough, President, Federal Reserve Bank of New York, before the BAI Conference: The National Payment System, Washington, D.C. (October 8, 1996) (以下、McDonough, supra として引用)
- ・ Remarks by Governor Edward W. Kelley, Jr., FRB: At the Seminar on Banking Soundness and Monetary Policy in a World of Global Capital Markets, Sponsored by IMF, Washington, D.C. (January 29, 1997) (以下、Kelley, supra として引用)

まず DOT, supra, Executive summary から見ておく。そこで目立つ点として、(いつものことではあるが)「電子現金 (electronic cash)」は、ヨーロッパ諸国では relatively common だが、アメリカではいまだ初期の発展段階にある、との認識が、ともかくも示されている。ただ、政府の役割を考える上で the issuance of legal tender: and the management of the money supply and the payments system 等の点が消費者の権利等々とともに挙げられている点は、重要である。しかしながら、不十分な分析に基づく premature and uncoordinated action among government agencies of decisions は、技術革新を、そして恐らくは (perhaps) グローバル市場でのアメリカ企業の実効的競争を阻害し得る、との指摘もなされている。

ヨーロッパとの対比という点では、以下の2点が重要であろう。まず、電子マネー(電子現金——この2つの語がさしたる区別なく用いられる傾向が、上記の各文書においては見られる)の イシューアーを銀行(banks)に限るか否かの問題がある。Id. at p. 25, 31, 35 に示されたように、EUの1994年のレポート(Id. at p. 35では Working Group on EU Payment System, Report to the Council of the European Monetary Institute on Prepaid Cards [May, 1994] が参照されている)で、電子マネー(electronic money)の イシューアーを銀行(ないし credit institutions)に限定する考え方が示されているが、それに対する反発が強い。Id. at p. 25 では、これは「競争と技術革新に対する不必要なバリア」であって、この点も含めて市場に委ねるべきだ、とされている(アメリカ側からの同様の声として、例えば Kelley, supra, at p. 4. なお、Rubin, supra, at p.3 における

impediments 極小化の考え方にも、この点が裏打ちされているのであろう)。

次に、若干屈折した形でヨーロッパとの対比がなされている点として、DOT, supra, at p. 26, 34fは、EUのプライバシー保護を問題とする (Directive 95/46/EC of the European Parliament——郵政省電気通信局・電子情報とネットワーク利用に関する調査研究会報告書 [平成7年8月] 10頁以下の言及する1995年のEU個人情報保護指令である)。便宜、上記郵政省報告書を引用すれば、その25条(4項)は、「EC委員会が、第三国が……十分なレベルの保護を保証していないと認定した場合には、メンバー国は当該第三国へのデータの流通を阻止するために必要な措置を講じなければならない」、とある(なお、日本がザル法としてのいわゆる個人情報保護法を有するのみの寂しい状況であることと、それがゆえのEU側から日本へのTDF [越境データ流通] ストップの危険については、私は再三注意を喚起して来ている。例えば、石黒・ボーダーレス社会への法的警鐘 [平成3・中央経済社] 293頁以下)。

ところが、DOT, supra, at p. 35は、この規定によってEUメンバー国が、アメリカ政府の investigation のために必要な、コンピュータで処理された個人データの転送を禁止すること、の可能性を懸念しているのである。もっとも、この点は、本稿IIIまでの論述と関係する点ではある(なお、Id. at p. 28, 45は、不正行為防止という法執行上の観点からThe Bank Secrecy Act 上の取引記録の保存・提出の問題にも言及している。従来は金融機関に対して然るべく命令をすることで対処できたが、電子マネーの普及による金融機関の data chokepoints としての機能の希釈化が、そこで懸念されているのである。同じ問題が、わが外為法の今般の大幅規制緩和によっても生じ得ること[!]に、最も注意すべきであろう)。

さて、電子マネーに関するアメリカでの論議(既述の各ペーパーから判断した限りでのそれ)においては、概してそれがリテイル中心の小口支払いで用いられる、との前提がある(Id. at p. 5; Rubin, supra, at p. 2; Kelley, supra, at p. 3. なお、Greenspan, supra, at p. 8は、後述の seigniorage との関係を論ずる際にこの点を前提としているし、McDonough, supra はペーパーのタイトル自体が“The Transformation of the Retail Payments Business”というものであった)。また、Rubin, supra, at p. 4が言及する1996年6月のG-7デンプー・サミットでの、電子マネー(その international dimensions!)の問題を検討すべきだとするアメリカ政府の提案においても、リテイル分野でのその検討

が主眼であったようである (DOT, supra, at p. 35)。

など、Id. at p. 30 には “By any measure, electronic money plays a minor role in the U.S. economy and . . . that role is not likely to increase any time soon.” とある (南北戦争前のアメリカから説き起こす Greenspan, supra にも、全体としてそうしたニュアンスが感じ取れる)。だが、DOT, supra, at p. 14 には、とくにインターネットのようなオープン・システム経由で電子マネーが、アメリカで広範に用いられるようになるには少なくとも2年はかかる (at least two years away) とあり、さらに ATM と同様の展開になるとすれば、最初の5年を過ぎれば劇的に利用が増大する可能性もある、としている。

上記の各文書において、電子マネー問題のマグニチュードがどうとらえられているのかを、更にここで見ておこう。まず、G-10諸国の中央銀行によるバーゼル支払・決済システム委員会 (BIS) での電子マネー問題の検討 (Id. at p. 36) との関係で、同委員会の委員長でもある FRB ニューヨークの McDonough, supra の見解が重要と思われる。そこに示された彼の見解は、グリーンズパン氏のそれとは若干異なる。紙ベースの非効率なシステムが次第に置き換えられて行くであろうこと (Id. at p. 1) を前提に、電子マネーを多額のドル支払いに用いる企業が出て来れば状況が変化すること (Id. at p. 2) を含め、一定のクリティカル・マスを超えた場合の普及の加速化が、予期されている (Id. at p. 4)。この点で、DOT, supra, at p. 12f が言及する PC-based electronic cash について、それが separate payments system を構成する可能性を有している旨の認識が、それなりにそこで示されていることにも、注意すべきである。いずれにしても、Id. at p. 36 の結論部分において、この DOT の文書は、電子マネー・システムにより、将来的には国内的及び国際的な支払いシステムに大きな変革の生じ得ることを、示しているのである。

それはまた、電子マネー取引がそれなりの (大きな) リスクを伴い得ることを、裏から示している。G-10諸国の前記バーゼル委員会は、その意味で注意深く事態の展開を監視して行く方針だが (McDonough, supra, at p. 2)、それとは別に、OCC, supra が stored value card 中心ながら、電子現金 (electronic cash) に関するリスクの分析を行っていること、そして、通貨監督庁の Ludwig, supra, at p. 2 が、“the need to plan for and develop risk management systems for e-money systems” を訴えていることに、注意すべきである (この点についてはコンセンサスがある、とされている)。

このことを、顧客 (消費者) の側から見た場合に問題となるのが、Id. [Ludwig], at p.

3fの言う“informed choices”の問題である。消費者（顧客）への情報開示がモンデックスの場合に十分か、といった点がまずもって想起されるが、ディスクロージャーの規制はどうなっているのか。まず、DOT, supra, at p. 24ff, 42ffによると、連邦EFT法やFederal ReserveのRegulation Eのディスクロージャーの規制は、消費者向けの電子的debit取引（ないしシステム）には適用されるが、電子的cash取引（ないしシステム）へのそれらの適用は明確でないとのことである。ただ、Regulation Eについては、FRBが同ルールを改訂し、限定的ながらstored value cardsをカバーする意向、とされている（Id. at p. 43—61 Fed. Reg. 19696 [May 2, 1996] が引用されている。この改訂がadequate disclosure of risks involved with electronic moneyを確保するためのものであることについては、McDonough, supra, at p. 3）。

なお、DOT, supra, at p. 22ffは電子マネー問題についての「政府の役割」に言及するが、通常の「小さな政府論」とは別に、ここでは政府が前面に出て行くべきだ（“if not be the exclusive issuer of electronic cash”とあるところ [Id. at p. 22f] がむしろ注意を引く）、との議論のあることも、そこに示されている。だが、現状で不用意に政府が動くことには慎重たるべきだというのが、このペーパーの、そして、既述のごとくアメリカでの現在の論調の基本である。つまり、（1）消費者への適切な保護、（2）電子マネー犯罪への実効的規制の程度、（3）国際的な諸フォーラムでアメリカ政府の提言すべき問題、等を考慮しつつ、市場に当面解決を委ねてはどうか、ということである（Id. at p. 23）。新味はない。その際、上記の（1）の消費者への適切な保護に関して、Id. at p. 24が、電子的なdebit systemsに対して「電子的なcash systems、つまり、E-cash instruments」への従来の法規制の適用はless clearだ」、としている点が、ディスクロージャーに関する上記の点の前提となる。

本研究会における岩原教授の報告においては、アメリカのEFT法の適用可能性が議論されていた。そして、私の記憶が正しければ、同教授は、イシューア・顧客・店のトライアングルが維持される限りにおいてはEFT的法律構成で「電子マネー」問題を把握できるとも言えるが、第三者にそれが直接譲渡される形になるとそうも行かず、結局は「金券（貨幣ないし通貨）」としての法律構成をするほかない、との方向に相当程度傾くものだった（ちなみに、私及び岩井克人教授は、一層端的にそう考えている。そして、相当程度電子マネーが普及した段階でこれは「貨幣（通貨）だ」という政策変更が、一体なされ得る

のかを、強く疑うのが私、及び「これも私の記憶が正しければ」、岩井教授の立場、というか基本的な危機意識の内実となる)。なお、Ibid では、電子現金の most issuers は、“in all likelihood, will continue to be subject to some form of regulation” という奥歯に物の挟まったような言い方をしているが、これは、イシューア―を銀行に限るべきか否か、という既述の論点 (Id. at p. 24f) と関係する。但し、アメリカ的なシナリオに沿って純然たる一般企業等がイシューア―となる場合を考えると、いかなる規制がそこでなされ得るかは、興味深い問題として残る (ちなみに、既述の EFT 法の適用可能性と絡むが、Id. at p. 48 において、“[I]t is questionable whether electronic cash systems involve the issuance of a payment order . . .”、との指摘のあることにも、注意すべきであろう)。

DOT, supra, at pp. 55ff は “Financial system risk [!] oversight” を取り扱っている。電子マネーを「システム・リスク」との関係で検討する視点は、極めて重要である (なお、岩村・前掲書が既述のごとく説くように、スーパー・ペイメントの一層の効率化のために電子マネーを用いることは、いわば必然の流れであろうが、その際私としては、処理時間の短縮が、かえってリスク顕在化の際の対策 [それも一層の緊急を要することにもなり得る] を立てる上で、扱いつらい事態を生じさせないか、若干危惧してもいる)。一般的な金融監督や金融倒産問題とは別に、ここでは預金準備率規制と預金保険の点を、若干見て置こう。

Federal Reserve によるマネー・サプライのコントロール手段でもある預金準備率規制 (12 C.F.R. 204.1 の列記する対象機関に対するそれ——DOT, supra, at p. 59) についての、この reserve requirements については、次の指摘が Ibid でなされている。即ち——  
“The Federal Reserve has informally indicated that balances of bank-issued electronic cash on stored value devices would be treated as transaction account “deposits” subject to reserve requirements. (See Statement of Vice Chairman Alan S. Blinder before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services, U.S. House of Representatives [October 11, 1995], at p. 12.)”

そこに devices とある点、「非公式」といっても議会の公聴会の場でのものたることに、注意すべきであろう。

なお、ここで、岩村・前掲書 (電子マネー入門) に戻って考えよう。「電子マネーが金融

政策の運営を難しくする」かどうかの問題（岩村・同上153頁以下）である。「預金者の大半が預金の引き下ろしを現金でなく電子マネーのかたちで求めるようになれば、金融機関が必要とする現金や準備預金の量は大きく減ってしまう」ため、「金融政策の効果に影響しように思える」が、「オーソドックスな金融理論の立場」（以上、同上・160頁）からは、そうはならない、とされる。だが、そこには「電子マネー発行残高という債務負担は当然に法定準備率の対象となるでしょう」、との前提がある。「電子マネーの発行額をハイ・パワー・マネー供給を通じて乗数的にコントロールする……法定準備率の効果を重視すれば、電子マネーが登場しても金融政策の有効性は損なわれそうにない、そう考えることもでき」（以上、同上・161頁）る、とされているのである。だが、つづく162頁には「本当にそうでしょうか」とあり、「何事にも程度問題というのがあ」る、とある。岩村・同上（163頁以下）は、そこから「通貨発行益」（seigniorage）の問題に移行し、「もし、民間金融機関の発行になる電子マネーが銀行券を押しつけて通貨の首座に就くとすれば、この膨大な通貨発行益が国庫に納付されずに民間金融機関のものとなるはずで……そうした予想が生じれば……19世紀のゴールド・ラッシュさながらに電子マネー発行ビジネス」への「殺到」現象が、金融機関のみならず「他の業界の人たちも」巻き込んで生じ得る、とされている。そして、その「副作用」として（岩村・同上164頁）、「一つにはインターバンク金利の予想を超える上昇」が考えられ、「例えば準備率の引き上げ」でそれに対処することも考えられる（同上・168頁）、とされている（DOT, supra, at p. 32では、Federal Reserveの側で電子現金[cash]をdepositと見るかどうかが、それに対して準備率規制がかけられるかどうかの点の境目となることについて、注意が喚起されている）。

だが、ノン・バンク・イシューアはどうなるのか（岩村・同上159頁では「普通の銀行」をイシューアとして「取り敢えず」想定している）。当面イシューアを銀行には限定せず、市場に委ねる、というのがアメリカの政策スタンスである。DOT, supra, at p. 59fには、既述のごとく非公式ながらFederal Reserveが準備率規制をかける意向を示していることとの関係で、こうなるとノン・バンク側にcost advantageが与えられる、という点を指摘する。だが、その先は、かえってそれが銀行側に対し、自分自身ではなくnonbank entitiesによって電子マネーを発行しようとする強いインセンティブを与えることになる、とされるにとどまっている（なお、既述の通貨発行益 [seigniorage] の問題については、DOT, supra, at p. 33も一言のみしているが、Greenspan, supra, at 7ff は、かつて

のアメリカ [National Bank Act 制定前のアメリカ]において、まさに seigniorage を狙って private currency が発行された歴史を回顧しつつ、“Today, there continue to be incentives for private businesses to recapture seigniorage from the federal government.” [Id. at p. 7] とする。だが、プリペイド・カードやトラベラーズ・チェックの場合も同じだ、との角度から、むしろこの流れを肯定的に評価するかのごとくである。そして、stored value cards or “digital cash” のイシューアの側での、strong balance sheets and public credit rating を有する specialized issuing corporations の設立にも、言及がなされている。複雑なものを、私は感ずる)。

もしそうなれば、岩村・前掲書の前提も狂ってしまう。「電子マネーに対して準備率が適用されている限り」(岩村・前掲書164頁)、というのが議論の前提だったからである。そこで生じるパニックを、私は(恐らくは岩井克人教授も)、最も懸念するのである。しかも、日本の中のみをどう固めたとしても、インターネット経由等で、日本の中には外国でイシューされた電子マネーがどんどん流入する(円建てのものも含む!)。外為法の大幅規制緩和が折り悪しく(!)この時期になされることにより、既述の “data chokepoints” (DOT, supra, at p. 28) の意味をも有する、「“外為関所”としての銀行」も、機能しなくなる。これがパニックでなくて、何であろうか。単なる「国内空洞化」の加速化のみで済めば、むしろ御の字だ、とさえ言いたくなるのが昨今の日本の制度改正(改革)論である、と私は思う。

ところで、電子マネーの deposits 性は、預金保険制度との関係でも、大きな問題となる。DOT, supra, at p. 25 は、銀行の発行する電子現金 (cash) の中には預金保険の対象となるものもあろうが (some... may)、ノン・バンク・イシューアが発行したものはその対象外だとし、銀行の発行したものについても、預金保険で担保されるものとそうではないものとの間で、顧客 (customers) の側で混乱のないようにする政策上の必要性を指摘する。この点は Ibid fn. 20 にも示されているように、FDIC, supra を踏まえたものである。この文書は、FDIC の側で、Id. at p. 6 fn. 6 に示されたシステム・リスク・準備率規制・通貨政策 [monetary policy]、等々の問題のあることを別に意識しつつも、預金保険支払いの前提となる「預金性」を、それぞれの電子マネー・システムごとに細かく分析・判断したものである。その詳細はともかくとして、微妙な方式の違い(最も分かりやすい例で言えば、例えばカードに電子マネーをダウンロードした段階で顧客のアカウントから

預金が引き落とされるか否か、[Id. at p. 5]) によって預金保険の対象となったり、ならなかったりするとの点が、そこに示されている（それを踏まえた DOT, supra, at p. 55 では、“[O]nce the funds are withdrawn from the account, they become unprotected unless placed in some other insured deposit account.” とされている。ちなみに、FDIC が管財人として行動する場合にどうなるかは、この分析とは別だ、とされている点にも注意を要する。FDIC, supra, at p. 24)。こうした点の顧客への適切なディスクロージャーが、別途大きな問題となろう。

以上、アメリカの金融関係政府当局者の指摘を若干追って見たが、一連の論述の最後に、Ludwig, supra, at p. 4 の次の言葉を引用して置こう。

“While we are mindful of the dangers of acting prematurely, waiting too long to address problems also will impede the full development of this promising market.”

だが、私は、電子マネーの普及よりも前に手を打って置かないと、もはや手遅れとなるのではないかと、との危機意識を強く有する（恐らくは岩井教授とともに——なお、同教授は、電子マネー問題は、典型的な「合成の誤謬」と、それによる「市場の失敗」の予測される場合だとされ、技術面からの西垣通教授の危機感、そして私のそれとの間で、かくて三者の認識は見事に一致した）。なお、この点では、McDonough, supra, at p. 3 が——

“[O]ne can imagine that government might face stiff resistance to any policy initiatives late in the development cycle after large amounts of money have been invested by the private sector.”

——としていることが注意されるべきである（但し、同氏のこれに続く指摘は、国内的・国際的な教育・研究の努力でかかる policy risks に対処せよと言うのみで、説得力がない）。

## V 小 括

電子マネーと暗号政策に関して、多くの法律問題が派生することは、私も十分承知している（本研究会でも、岩原教授が、その大論文たる岩原「電子資金移動 (EFT) および

振込・振替取引に関する立法の必要性」ジュリスト1083号55頁以下、1084号97頁以下、1085号80頁以下、1086号80頁以下、1087号136頁以下、1089号306頁以下、1090号132頁以下、1092号85頁以下、1093号95頁以下、1094号121頁以下 [平成8] で詳細に展開された解説論の応用可能性、との見地から、重要な報告をして下さった)。だが、それが通貨(貨幣) だと言った途端に、状況がガラリと変わる場面も相当程度予想される(なお、外貨の取り扱いについては、石黒「外貨とは一体何なのか?——外国金銭債務論序説」貿易と関税1994年4月号110頁以下、同5月号44頁以下、同6月号46頁以下、参照)。私は、岩井教授とともに(同教授がこの点について適宜執筆をされるのを心待ちにしつつ!)、早い段階でその旨明確な国家的宣言をするべきだ、という立場である。

岩原教授は、岩原「銀行の決済機能と為替業務の排他性」鴻常夫先生古希記念・現代企業立法の軌跡と展望 [平成7] 529頁以下、とくに570頁以下で、「預金通貨以外の決済手段……の規制の必要性」を、「プリペイド・カードの規制」を含めた検討において、論じておられる。同上・581頁末尾の行以下の慎重な指摘をさらに一步進め、清水の舞台から思い切って飛び降りる覚悟で臨まないといけない問題が、私にとっての電子マネーであり、また、暗号政策なのである。日銀とNTTとを是が非でも結び付けねば、と私が固執したのも、それが故である。

なお、我が国での電子マネー(そして信じられぬことに暗号も!?)の検討が、殆ど完全な「丸ドメ(まるでドメスティック)」状態にあることは、遺憾である。その意味では、既述の Rubin, supra, at p. 4が、“[E]lectronic modes of payment are international, and all these issues are going to have to be considered in an international context.”と明確に断じていることを、想起すべきである(Ludwig, supra, at p. 3fも同様であり、borderless nature of electronic commerce ; jurisdiction、そして準拠法問題の存在に言及しつつ、“[E]lectronic money is truly an international phenomenon.”と述べている)。

そこから先は、ズバリ私の専門領域での問題となる。かつて私は、従来の私の国際金融取引・国際金融規制(域外適用問題や共助の問題も含む)に関する研究の全体像を一覧性のある図にまとめた(石黒「国際金融の抵触法的考察(1)」貿易と関税1992年6月号47頁の、多数のキ・ワードを繋げた“配線図”である)。「電子マネーと暗号政策」に係する事項にマークを付けて見ようと思って付け出したが、全く意味がないことに気づいた。殆ど全項目が関係するのである。そして、それを握った者(国)が21世紀の金融、そして

世界を掌握することになるのである。

# GATS と電気通信

小 寺 彰

## 目 次

- I はじめに——電気通信と国際規律——
  - II GATS とは
    - 1 GATS の WTO 協定上の位置
    - 2 サービス貿易の意義
    - 3 GATS の基本原則
  - III 電気通信サービス規律の特色
    - 1 電気通信附属書
    - 2 基本電気通信規律
    - 3 参照文書の意味——ベンチマーク制の評価——
  - IV 結 語
    - 1 GATS の評価
    - 2 電気通信サービス規律の意味
- 付録 参照文書

## I はじめに——電気通信と国際規律——

電気通信は、かつては無線周波数と国際通信のみが国際電気通信連合（ITU）の国際規律に服していた。これ以外の電気通信分野は多数国間条約の射程内ではなく、通信主権の一部として<sup>(1)</sup>、各国が独自に規制すべき分野であると考えられてきた。ところが1980年代になると、サービス貿易という観点から、サービス一般について各国の国内規律に踏み込んで国際的規律を及ぼしていこうという主張が、アメリカを中心に出始め、その中の有力分野として電気通信が位置けられた<sup>(2)</sup>。ガット・ウルグアイラウンド交渉でも、電気通信はサービス貿易の重要分野と位置付けられ、そこで作成された「サービスの貿易に関する一般協定」（GATS）の主要な対象と考えられた<sup>(3)</sup>。

GATSとはどのようなものか。またその中において、電気通信はどのように規律されているか。またその特色は何か。

〔注〕

（1） 通信主権については、小寺「電気通信と主権」国際法外交雑誌90巻3号(1991)、pp.7-11.参照。

（2） たとえば、ロナルド・K・シュルプ(佐藤浩訳)『サービス取引の自由化』（1982）参照。

（3） ウルグアイラウンド交渉におけるGATS交渉の経緯については、宮家邦彦『解説 WTO サービス貿易一般協定』（1996）、pp. 4-17.参照。

## II GATS とは

### 1 GATS の WTO 協定上の位置

GATSとは、「貿易及び関税に関する一般協定（GATT）」及び「知的所有権の貿易関連の側面に関する協定（TRIPS）」と並んで、世界貿易機関（WTO）が所轄する主要な3つの協定の1つで、サービス貿易を対象とするものである。GATSには、附属書が8つ付いており、その中に、「電気通信に関する附属書」（テレコム・アネックス）と「基本電気通信の交渉に関する附属書」がある。さらに国によってGATS上の義務の程度を変

えることが可能になっており、そのために各国の約束の内容が約束表という形で付けられている。約束表は、当然国ごとに異なり、それに応じてそれぞれの国が負う義務が決まる。

WTOの大きな特色は、非常に精緻な紛争解決手続<sup>(4)</sup>を備えていることである。WTO紛争解決手続は、GATSについても、原則としてGATTと同様に適用されることになっている。したがって、GATS本体・附属書・約束表は、各国が自由に解釈・適用すればすむものではなく、他の加盟国から条約義務違反等<sup>(5)</sup>があるという申立がWTOに対してなされると、WTO紛争解決手続が起動して、申立に理由があれば、被申立国に対して措置の是正が要求されるという仕組みになっている点に、注意を払わなければいけない。

なお、GATSについて、WTO紛争解決手続で判断が出た例はいまのところないが、現在わが国は、大規模店舗法がGATSに反しているとしてアメリカから訴えられている<sup>(6)</sup>。

## 2 サービス貿易の意義

GATSの対象であるサービス貿易とは何か。そもそも貿易という概念はモノについて言われてきたわけで、「サービス貿易」という概念を使うときには、何が「サービスの貿易」なのかから議論を始めなければならない。

GATS上は、サービス貿易として、4つの態様が規定されている（1条2項）。

(a)いずれかの加盟国の領域から他の加盟国の領域へのサービスの提供。これは、電気通信を通じて外国からサービスを購入するようなものを想定している（例えば、電話による外国宝くじの購入）。かつてはこの(a)の形態がサービス貿易の本来的な形態であると言われることが多かった。つまり、領域から領域にサービスが移動するので、貿易という概念で最も説明しやすいからである。しかし、GATSはそれ以外に、以下に挙げる(b)(c)(d)も、サービス貿易の中に加えている。

(b)いずれかの加盟国の領域内におけるサービスの提供であって、他の加盟国のサービス消費者に対して行われるもの。これは、消費者が移動することによって外国のサービスを購入する形態である。例えば、外国に観光に行った人が現地で通訳を雇う場合がこれにあたる。

(c)いずれかの加盟国のサービス提供者によるサービスの提供であって、他の加盟国の

領域内の業務上の拠点を通じて行われるもの。これは外国に投資をして、そこでサービスを提供する場合をさし、貿易量という観点からは最も取引量が大きい。これは本質的には投資の問題であるが、サービス貿易のカテゴリーに入れれば、現在最も重要な形態と位置づけられる。このことは、GATSが投資の自由化にも一部踏み込んでいることを意味している。

(d)は、(c)が投資であるのに対して、自然人が外国に移動することによってサービスを提供する形態である。この形態ではそれほど大きい取引量はなく、重要性は低い。

この4モードについてできる限り自由化を図ろうというのが、GATSの基本精神である。

### 3 GATSの基本原則

GATSにおける自由化とは何か。GATSの主要原則は、①最恵国待遇原則、②内国民待遇原則、③透明性、④市場アクセスの4つである。

最恵国待遇原則、内国民待遇原則は、GATTにおいても従来から基本原則の位置を占めてきた。最恵国待遇原則は、すべての国のサービス及びサービス提供者を等しく扱うこと(2条)、また内国民待遇原則は内外のサービス及びサービス提供者を等しく扱うこと(17条)を義務づける。両者を合わせて、サービス貿易の「自由・無差別」が保障される。なお、従来各国のサービス規制のなかには、他国が自由化する限度で、自国の自由化も行うというものが少なからずあった。これが相互主義である。最恵国待遇原則または内国民待遇原則は、ともに他国の自由化の程度とは関わりなく、外国事業者の提供するサービス等と同じ程度に自由化し、また自国事業者の提供するサービス等と同一に扱うことを要求するのであり、相互主義とはまったく異なる原理であることを理解しておく必要がある。

GATTでは、最恵国待遇や内国民待遇とは別に国内規制自身を問題にすることはほとんどなかった。しかし、サービスの場合、各国の国内規制はモノの場合よりも一般的には強く、そのために、サービス貿易に単純に内国民待遇原則を適用しても、外国からのサービス提供が円滑には行われないう問題点が指摘された。言い換えると、国内規制自身に自国サービス産業を守る面がある。そこでサービス貿易の自由化を実質的に保障するために各国の国内規制それ自身が狙上りのせられ、まず透明性と市場アクセスという新しい

原則を導入して、国内規制自体の問題に対応することとした。

透明性とは、国内規制措置が外国からも十分知りうる状態を言う。そのため、GATSは、具体的に、①加盟国の措置や関連協定の公表、②法令上、行政上の指針を変更した場合に、WTOの機関であるサービス貿易理事会に通報する、そしてまた③他の加盟国が知りたい場合にはきちんと知ることができるような措置をとることを規定している（3条）。これが透明性の基本である。透明性の第1の目標は、外国事業者に国内措置を周知してその予測可能性を高めてサービス貿易の自由化を推進することにあるが、それにとどまるものではなく、第2に漸進的自由化を促進するという役割も期待されている。各国の国内規制をはっきりさせて諸国が正しい認識をもち、その上ではじめて unnecessaryな規制を減らしていけるというポリシーなのである。

国内規制を直接的に減らすことを目指すのが、市場アクセス（16条）である。市場アクセスは、先ほど述べたように、現行の国内規制では外国からのサービスの提供が十分円滑に行われないうことへの対処であり、まず第1に問題にしているのは、サービス提供者の数の制限をはじめとする、さまざまな数量的な制限であり、それを禁止した。たとえ内外無差別、つまり、内国民待遇原則の観点からは問題のないような国内規制であっても、数量的制限を採用する規制をとることはできない。わが国では、サービス産業について、従来、国が需給調整を行うことが多かったが——例えば電気通信事業法にも第1種電気通信事業者についての需給調整条項（10条2号）があったが、本年2月の改正によって削除された——、GATS上はもはや許されない。

市場アクセスの第2番目の意味は、事業体の法的形態を制限してはいけないことである。つまり、特定の形態に事業体を制限することが、外国からのサービス提供、特に投資によるサービス貿易を難しくするためである。

第3番目は外国資本参加制限の禁止である。これは、市場アクセスをそのまま適用すれば、現在の第1種電気通信事業者についての30%、それからNTT、KDDの20%外資制限が許されないことを意味する（詳しくは後述）。

以上のように、市場アクセスでは、国が供給量について制限をしてはいけないという原則が基本になっている。それでは、このような量的制限ではない、質的制限については、GATSはどのような態度をとっているのか。

質的制限については、少なからず必要なものがあり、すべてを廃止することはできな

い。自動車の運転免許を考えれば、このことは容易に理解できよう。ただし、質的制限であれば、すべてが許容されるとは言えず、必要な規制と不必要な規制の仕分けが必要になる。GATSが仕分け基準として採用したのは、国内規制の合理性、客観性、公正性である。つまり質的制限による国内規制はこの3条件を満たさなければならない。そこで具体的に、合理的、客観的、公正な国内規制とは何かが問題になる。GATSでは、特に重要なポイントだけが具体的に規定されている（6条）。①行政上の決定についての独立の機関による審査、救済。②申請に対する合理的期間内の応答または処理の義務。③資格要件等の客観性、合理性。④国内規制に関する国際基準の将来の作成。⑤ただし、他の加盟国の利益を無効化侵害するような措置は直ちにやめなければいけない。

①の独立の機関は、憲法上、三権分立まで要求するものではなく、独立性さえ確保されれば足りる。②については、わが国には従来規律がなく、GATSに入る直前に作られた行政手続法9条によって、②の義務を担保した(7)。

ここで注意する必要があるのは、最恵国待遇原則には、すべてのサービス分野で各国が従う義務を負っているが、内国民待遇原則、市場アクセス及び質的制限規律については、各国が選択的に受け入れた範囲で義務を負えばよいことである。つまり、各締約国が別途に提出した約束表記載分野でのみ義務を負えばよく、最恵国待遇原則より緩やかな規律になっている。もちろんこのような約束表記載分野については、その後、交渉によって適用例外を減らしていくことが想定されており、現在のままで永久にとどまってよいわけではない。

とくに質的制限規律は、合理的、客観的、公正な国内規制の実施にとどまっており、市場アクセスや内国民待遇と比較すると、義務の程度はより緩やかである。つまり市場アクセスや内国民待遇と比較すると各国は受け入れやすく、そのため適用範囲を各国が出す特定の約束に限定したことに対しては批判が強い。国内措置に関する6条は内国民待遇や市場アクセスと比べると、条約の前の部分、すなわち市場アクセスや内国民待遇原則を収める「第3部 特定の約束」中ではなく、最恵国待遇原則規定に近い箇所におかれている。この規定の位置は、将来的には質的制限規律の適用を特定の約束分野に限定しないようにする方向性を暗に示すものと見ることができよう。

このように、GATSはサービス貿易の自由化を規定するが、GATTと比べると非常に緩やかな段階にとどまっている。

{注}

- (4) WTO 紛争解決手続については、小寺「WTO 紛争解決手続」経済セミナー1997年1月号、pp.74ff；岩澤雄司「WTO 紛争処理」(1995) 参照。
- (5) WTO 紛争解決手続では、条約違反に関わらない「非違反 (non violation)」または「状態」申立も手続の対象になる。この点については、岩澤前掲書、pp.75-77. 参照。
- (6) 大規模店舗法がGATS16条2項(a)号で禁止されている「サービス提供者の数」の制限に当たるとどうか争点である。なお、3の市場アクセスの箇所参照。
- (7) Cf. Koji Tsuruoka, "The General Agreement on Trade in Services," *Japanese Annual of International Law*, No.38(1995), pp.40-41.

### III 電気通信サービス規律の特色

それではGATSは電気通信についてどのような意味を持つのか。電気通信がサービスと捉えられることは当然であるが、電気通信サービスはサービスの中で特異な性格を持っている。電気通信サービスは、一方では、提供されるサービスであるが、他方では、サービス貿易の第1モードを実施するための手段であるという二重の役割を担っている。つまり電気通信サービスを自由に使えなければ、そもそもサービスの貿易自由化が全体的に不十分になるという関係がある。そのため電気通信サービスには、他のサービスと比べてより厳しい規制が必要になる。

#### 1 電気通信附属書

「電気通信に関する附属書」、いわゆるテレコム・アネックスは、電気通信の2重の意味に即して、加盟国に対して、自国の公衆電気通信サービスへの合理的かつ差別的でないアクセス及び利用を他の加盟国のサービス提供者に確保することを義務づける。ここでいう公衆電気通信サービスとは、「公衆一般に提供されることを明示的に又は事実上要求している電気通信の伝送サービス (3.(b))」——「公衆電気通信の伝送サービス (public telecommunications transport service)」とよばれる——及び、公衆電気通信の基盤 (infra-structure) (同(c))——「公衆電気通信の伝送網 (public telecommunications network)」とよばれる——を指す。わが国では電気通信事業法上の第1種電気通信事業

者の提供するサービスが「公衆電気通信の伝送サービス」に、また第1種電気通信事業者のもつ回線設備が「公衆電気通信の伝送網」に該当する。附属書は、両者について、いわゆる付加価値通信（電気通信事業法上の第2種電気通信事業）がそれらを円滑に利用できるように国が一定の措置をとることを義務づける。

具体的な義務としては、①公衆電気通信へのアクセス等に関する情報の公開（4条）。これはGATS本体の透明性の特別則に当たる。②公衆電気通信への合理的かつ無差別なアクセス・利用（5条）。これはGATS本体の最恵国待遇・内国民待遇原則の基本精神を公衆電気通信に当てはめたものである。ただし、GATS本体の最恵国待遇・内国民待遇原則は国の取扱いに関する義務であって、事業者への義務付けを含むものではなく、サービス事業者が誰と取引するかは、あくまで事業者の自由である。公衆電気通信については、さらに一步進んで、公衆電気通信事業者の取引にまで、最恵国待遇・内国民待遇原則を適用することを要求している。なお、これ以外に、この附属書は、③技術協力の実施（6条）。④ITUとの整合性の確保（7条）を規定している。

## 2 基本電気通信規律

基本電気通信についての交渉は、1994年のウルグアイラウンド終結時までにはまとまらず、さらに「基本電気通信の交渉に関する附属書」が予定した昨年4月末の継続交渉の期限にも妥結せず、結局今年の1月の半ばに交渉が再開されて2月15日になってようやくまとまった(7a)。その結果出来上がったのが「サービス貿易に関する一般協定の第4議定書」である。この議定書は、「基本電気通信に関する関係加盟国の特定の約束に係る表」（参照文書のこと）と「第二条の免除に係る表」からなる。なお、基本電気通信については、GATS上定義はなく、以下の定義が関係国の了解であったと言われる。「基本電気通信サービスとは、電磁的手段による信号の送受信によって行われる電気通信サービスのうち、顧客が提供する情報を2以上の地点の間で、その情報の形態又は内容の終端における変更を伴わずに、リアルタイムで伝送することを典型的に行うサービスであって、電信、電話、テレックス及びデータ通信が該当する。」(8)

基本電気通信交渉がまとまったことは、本当の意味で、基本電気通信がGATSの枠内に入ったことを意味する（なお、1998年1月1日発効予定）。

第1は、基本電気通信サービスについても最恵国待遇原則が適用されることが確定した

ことである。基本電気通信交渉がまとまるまで、基本電気通信については、GATS上、すべてのサービス分野で適用されるべき最恵国待遇原則が、適用されないことになっていった（基本電気通信附属書1.）。アメリカはこの点を利用して、1995年11月に、外国市場が開かれているかどうかを審査し、アメリカと同程度に開かれていないときには市場参入を拒否するというエコシステム（Effective Competitive Opportunities）を採用して、相互主義的な政策をとり、実際にも衛星通信等に適用してきた<sup>(9)</sup>。エコシステムをとりえたのは、基本電気通信サービスについては最恵国待遇原則が適用されていなかったためである。アメリカも、基本電気通信規律の交渉妥結を受けて、エコシステムの廃止に向けた作業を開始したようである<sup>(10)</sup>。

第2に、基本電気通信に、内国民待遇原則や市場アクセスをどのように適用するかは、未解決の問題であった。たとえば、わが国が内国民待遇原則、市場アクセスについては、第2種電気通信事業及び第2種電気通信事業によって提供される付加価値サービスについてのみ約束し、基本電気通信には、内国民待遇原則や市場アクセスを適用しなくてもよい状態であった。今回の継続交渉で、基本電気通信サービスについて、内国民待遇原則、市場アクセスをどの範囲で約束するかが議論され、各国は、基本電気通信サービスについて、広い範囲で、内国民待遇原則、市場アクセスの義務を負った。たとえば、わが国はNTT及びKDDについて、20パーセントの外資制限を維持することを留保したが、それ以外は完全に内国民待遇原則及び市場アクセスに服することを約束した。第1種電気通信事業者について、KDDとNTTを除いて外資規制を完全に撤廃することになったのである。

第3に、国内規制に関する「参照文書（Reference Papers）」（付録）が作成されたことが重要である。質的制限を行う国内規制（質的国内規制）については、GATSは、既述のように（II 3）、原則的な規定をおくにとどめていたが（6条）、参照文書は、基本電気通信分野の質的国内規制について、具体的な規律に踏み込んだ。ここでは、各国の基本電気通信に関する規制の枠組みとして、①競争条件確保のためのセーフガード、②相互接続、③ユニバーサル・サービス、④免許の基準の公の利用可能性、⑤独立規制機関、⑥稀少資源の分配・利用を定める。

①は、主要な供給者の反競争的行為を防止するための措置を締約国がとるべきことを命じたもので、GATSがはじめて競争政策に立ち入った点で重要である。そして具体的な

反競争措置が例示された——たとえば「反競争的な内部相互補助」が挙げられている——。

②は、主要なサービス提供者との接続確保措置の義務付けである。わが国で本年行われた電気通信事業法の改正（38条から39条の4まで等）は、これらの規定に沿った内容になっている。

③、④、⑥は、それぞれの事項について、最恵国待遇、内国民待遇、透明性を満たすべきことを規定する。また⑤は、電気通信について、伝統的に規制機関と事業者が分離されていない国が多かったために、あえてGATS本体と同一内容の規定が書き込まれた。

この参照文書上の義務は、当初から先進国はそれに等しく拘束されることが要求され、それに対してASEAN諸国のような中進国や開発途上国については、選択的に加わることが認められるとされ、実際にもそのような結果になっている。

### 3 参照文書の意味——ベンチマーク制の評価——

参照文書の中で重要なのは、「競争条件確保のためのセーフガード」（競争確保セーフガード）である。電気通信の中に競争法の観点が入ったのは、一般的には、公正自由な競争秩序が維持されることによってはじめて、サービス貿易の自由化が達成されるからだと説明できる。しかし、電気通信に競争法の視点を入れることは、実はそれを超えた意味をもつ。この点を現在、アメリカが導入を企て、他方わが国をはじめ諸外国からの批判が強い、国際清算料金のベンチマーク制<sup>(11)</sup>を例にとって考えてみたい。

国際電気通信は、従来から電気通信事業者（キャリア）間で計算料金のやりとりをして、相手側の電気通信サービス利用分を補填して実施されてきた。わが国からKDDを使ってアメリカに国際電話をかける場合を想像してみよう。電話をかけた人は、KDDに対してかけた時間に応じて一定額の料金を支払う。このときに利用者がKDDに支払う料金を収納料金と呼ぶ。ところで利用者が電話をかけるためには、日本側のKDDの設備だけではなく、アメリカ側の事業者、たとえばAT&Tの設備をアメリカ側では利用できるからこそ、アメリカにいる人と電話で話しができる。しかし、日本の利用者はAT&Tには何も料金を支払っていないし、もちろんアメリカで電話がかかってきた人がAT&Tに利用料を支払うわけではない。そこでAT&Tのサービス利用分が問題になるが、KDDが徴収した収納料金の一部を計算料金とし、その額をKDDとAT&T間で決めて、KDD

がAT&Tに支払うことでAT&Tのサービス利用分を補填してきた。このような計算料金の遣りとりは1通話ごとに行われるのではなく、一定の期間を切って、日本側KDDからアメリカ側AT&Tに支払うべき計算料金とアメリカ側AT&Tから日本側KDDに支払うべき計算料金を相殺して、発信時間数の多いキャリアーが相手側キャリアーに差額を払ってきた。しかし伝統的にアメリカ発の国際通信が多いために、計算料金が高いとアメリカのキャリアーが支払う金額が多くなるという結果を招いていた。

アメリカ連邦通信委員会(FCC)が現在導入を目指しているのは、清算料金(計算料金の半額)について目標値(ベンチマーク)を決め、実際の清算料金をその額以下にすることである。これは、①アメリカ側キャリアーの清算料金支払いが年間50億ドルに上り、②清算料金の額が補填しなければならない相手側キャリアーのサービス相当額(コスト)を上回っているとFCCが考えたためである。つまり、本来は国内の収納料金引き下げの原資に回るべきお金が、支払う必要のない相手国側キャリアーに支払われている、その意味で清算料金が反競争的な補助金の性質をもっていると言うのである。

そこでFCCは、国ごとにベンチマークを決め、清算料金がその額以下になるようにキャリアーに交渉を促し、一定期間内に協議が整わないと、FCCはベンチマークよりも高い清算料金をアメリカのキャリアーが支払うことを禁ずるとというのが、制度の骨子である。

これについては、現在FCCが他国政府や他国キャリアーからコメントを求めている段階であるが、わが国をはじめ諸国から批判が強いと言われる。確かにベンチマークの金額を、FCCが一方的に、しかもきわめてラフな基準に基づいて決定する等細部について問題は多い。しかし、先に紹介した清算料金規制の根幹部分が、GATSに反しているかどうかは改めて考えてみなければならない。この点の解明の鍵は、アメリカがこの制度を競争政策の一環として打ち出している点にある。

アメリカ政府は、おそらく、このベンチマーク制を、その根幹部分は参照文書で締約国がとらなければならないとされる競争条件確保セーフガードとして正当化するつもりであると推測される。逆に多くの批判は、細部の点をおくと、従来から清算料金がキャリアー間の協定によって定めてきた点を中心的な根拠にして非難しているように見受けられる。すなわちアメリカの一方性が非難のポイントなのである。しかし、事業者間の協定は良く、政府の一方的行為はいけないと、アプリオリに決められるのであろうか。古くから国

際通信は、各国のキャリア間協定によって実施され、国際通信の実質的な一般規律さえ、キャリア間協定に委ねられることがあった。たとえば、キャリア間で決められた旧 D 1 勧告が、国際専用線利用の中心的な規律と考えられた時代があった。しかし、2.でも説明したように、電気通信の世界でも、事業者と規制機関は完全に分離された。他方で、競争確保セーフガードは、明確に締約国が一方的に反競争防止措置をとることを認めている。また競争法の世界では、事業者間の協定自身が反競争的なトラストと評価される可能性をもっていることも忘れてはならない。つまり、アメリカのベンチマーク制は、その根幹において、競争確保セーフガードとして肯定される可能性を相当な程度もっているのである。もちろん、最終的な結論を出すことは、本稿の目的でもないし、また根幹部分が GATS に抵触しないとしても、国ごとにベンチマークの金額を変えることが最恵国待遇原則違反と評価される可能性等は否定できない。しかし、金額の算定方法等の部分が GATS 違反と認定されても、先ほどから説明してきたベンチマークの根幹部分さえ肯定されれば、金額の算定方法等の細部を修正すればすむのであるから、逆に制度自身は GATS 上のお墨付きを得たことになるのだということを忘れてはいけない(12)。

従来電気通信の世界は協定万能の世界であり、その目から見れば、ベンチマーク制は奇異に映る。しかし、GATS が電気通信の規律体系となり、さらに競争法を導入したことは、キャリア間協定によってすべてを律するという時代が終焉したことを意味する。競争確保セーフガードが参照文書に規定されたことの実質的な意味は、GATS が通信、とくに国際通信の規制の基本原則を根本的に変えたことを白日の下に曝したことである。

〔注〕

(7a) 基本電気通信交渉については、外務省経済局サービス貿易室編『WTO サービス貿易一般協定』(1997), pp.17-28. 参照。

(8) 宮家前掲書、pp.265-266.

(9) 通商産業省通商政策局編『1997年版不公正貿易報告書』(1997), pp.241-242. 参照。

(10) 日本経済新聞1997年6月5日版夕刊

(11) ベンチマークについては、KDD 総研『R&A』1997年2月号, pp.3-11. 参照。【追記】ベンチマーク制は、1997年8月7日のアメリカ連邦通信委員会の決定によって、1998年1月1日から実施されることになった (FCC 97-280)。

(12) この点は、アメリカが基本電気通信交渉を国内措置と戦略的に絡めて行ったことの証であろう。

なお、この点については、石黒一憲「WTO基本テレコム交渉と国際計算料金制度(上)」貿易と関税1997年3月号, pp.57-68. 及び同(下)貿易と関税1997年5月号, pp.61-69. 参照。

## IV 結 語

### 1 GATSの評価

GATS全体は、非常に枠組的な性格が強くて、具体的な義務の内容については今後交渉によって決めるというものが多い。サービスは、各国で国内的な規制が非常に強い分野であるために、とりあえずは枠組みをつくったというのが現状である。つまり現在のGATSは、内外無差別の原則を打ち立てたうえで、国内措置がサービス貿易の障害とならないものに改廃する前提として、国内措置の透明性、つまり、だれでも規制内容がわかるようにすることを、各国の絶対的な義務として課している。今後の焦点は、GATSの適用範囲を拡大し、合わせて国内措置をサービス貿易の障害とならないものに改廃することである。サービス貿易交渉については、1998年に交渉再開が予定されており、この交渉妥結をまって初めてGATSの本来の意味が出てくると考えるべきである。

さらにWTOの枠外に目を転じると、OECDで現在交渉中の多数国間投資協定(MAI)に注目する必要がある。MAIは、当初の交渉期限である本年5月に妥結はできなかったが、近い将来にはまとまると予想されている。MAIはより広範囲をカバーし、当然サービス分野も含み、また、より強化された形で、国内規制のあり方に踏み込むことが目指されている。サービス貿易の最重要分野が対外投資による形態であることはすでに述べたが、この点を踏まえると、GATSとMAIは手を携えて、もっぱら国内規律に服してきたサービス分野を、徐々に国際規律のもとに収めて自由化を進めていこうとしていることが分かる。その意味でも、GATSは第1歩である。

### 2 電気通信サービス規律の意味

このような全体的な見取り図の中で電気通信サービスは、やや特殊な位置を占める。電気通信には、ウルグアイラウンド後に金融サービス、海運サービスと並んで個別分野交渉が行われ、その中で唯一成功した分野である。つまり、電気通信分野では、今回の参照文書に見られるように、単なる枠組みを越えた実体的な自由化規律が始まった。参照文書で競争法的規律が入ったことは、今後のGATS、さらにはサービスの国際規律の方向性を示すものとして重要である。

(注)

(13) 宮家前掲書, pp.15—17.

## [付録]

### 参 照 文 書

#### 適用範囲

この文書は、基本電気通信サービスの規制の枠組みに関する定義及び原則について定める。

#### 定 義

「利用者」とは、サービス消費者及びサービス提供者をいう。

「不可欠な設備」とは、次の(a)及び(b)の要件を満たす公衆電気通信の伝送網又は伝送サービスに係る設備をいう。

(a) 単一又は限られた数のサービス提供者により専ら又は主として提供されていること。

(b) サービスの提供において代替されることが経済的又は技術的に実行可能でないこと。

「主要なサービス提供者」とは、次のいずれかの結果として、基本電気通信サービスの関連する市場において（価格及び供給に関する）参加の条件に著しく影響を及ぼす能力を有するサービス提供者をいう。

(a) 不可欠な設備の管理

(b) 当該市場における自己の地位の利用

#### 1 競争条件の確保のためのセーフガード

##### 1.1 電気通信における反競争的行為の防止

単独で又は共同で主要なサービス提供者であるサービス提供者が反競争的行為を行い又は継続することを防止するために適切な措置を維持する。

##### 1.2 セーフガード

1.1の反競争的行為には、特に次の行為を含む。

(a) 反競争的な内部相互補助を行うこと。

(b) 競争者から得た情報について反競争的な結果をもたらすように利用すること。

(c) 他のサービス提供者に対し、当該地のサービス提供者がサービスを提供するために必要な、不可欠な設備に関する技術的情報及び商業上の関連する情報を適時に利用できるようにしないこと。

#### 2 相互接続

2.1 この2の規定は、特定の約束を行った範囲において、公衆電気通信の伝送網又は伝送サービスを提供するサービス提供者との接続であって、一つのサービス提供者の利用者が他のサービス提供者の利用者と通信し又は他のサービス提供者によって提供されるサービスへアクセスすることを可能にするものに適用する。

##### 2.2 確保すべき相互接続(注)

注 この2.2の規定については、不可欠な設備を管理する主要なサービス提供者についてのみ適用する。

主要なサービス提供者との相互接続については、伝送網の技術的に実行可能でないかなる接続点においても確保する。主要なサービス提供者が提供する相互接続は、次の要件を満たすものとする。

(a) 差別的でない条件（技術上の基準及び仕様を含む。）及び料金に基づき、自己の同種のサービス、提携していないサービス提供者の同種のサービス又は自己の子会社若しくは提携する会社の同種のサービスに提供する品質よりも不利でない品質によって提供されること。

(b) サービス提供者がそのサービスの提供のために必要でない伝送網の構成部分又は設備に対して

支払をする必要がないように十分に細分化された、透明性のあるかつ経済的実行可能性を考慮した合理的な条件（技術上の基準及び仕様を含む。）及び料金（原価に照らして定められるもの）に基づいて適時に提供されること。

- (c) 請求がある場合には、必要となる追加的な設備の建設費を反映する料金が支払われることを条件として、利用者の多数に提供されている伝送網の終端地点以外の接続点においても提供されること。

### 2.3 相互接続に関する交渉のための手続の公の利用可能性

主要なサービス提供者との相互接続に適用される手続は、公に利用可能なものとする。

### 2.4 相互接続に関する取決めの透明性

主要なサービス提供者は、確実に、相互接続に関する協定又は参照用の相互接続に関する提案を公に利用可能なものとする。

### 2.5 相互接続に関する紛争解決

主要なサービス提供者との相互接続を請求しているサービス提供者は、相互接続の適当と認められる条件及び料金があらかじめ設定されていない場合には、これらに係る紛争を合理的な期間内に解決するために、次のいずれかの時期に、独立した国内機関（5に定める規制機関を含む。）に申し立てることができるものとする。

- (a) 随時  
(b) 公に周知された合理的な期間の経過後

## 3 ユニバーサル・サービス

いずれの加盟国も、当該加盟国が維持することを希望するユニバーサル・サービス義務の内容を定義する権利を有する。この義務は、反競争的とはみなされない。ただし、透明性のある、差別的でない及び競争中立的な態様で履行され、かつ、当該加盟国が定める内容のユニバーサル・サービスを確保するために必要である以上に大きな負担にならないことを条件とする。

## 4 免許の基準の公の利用可能性

免許が必要とされる場合においては、次の(a)及(b)の事項を公に利用可能なものとする。

- (a) すべての免許の基準及び免許の申請に係る決定を行うため通常必要とされる期間  
(b) 個別の免許の条件

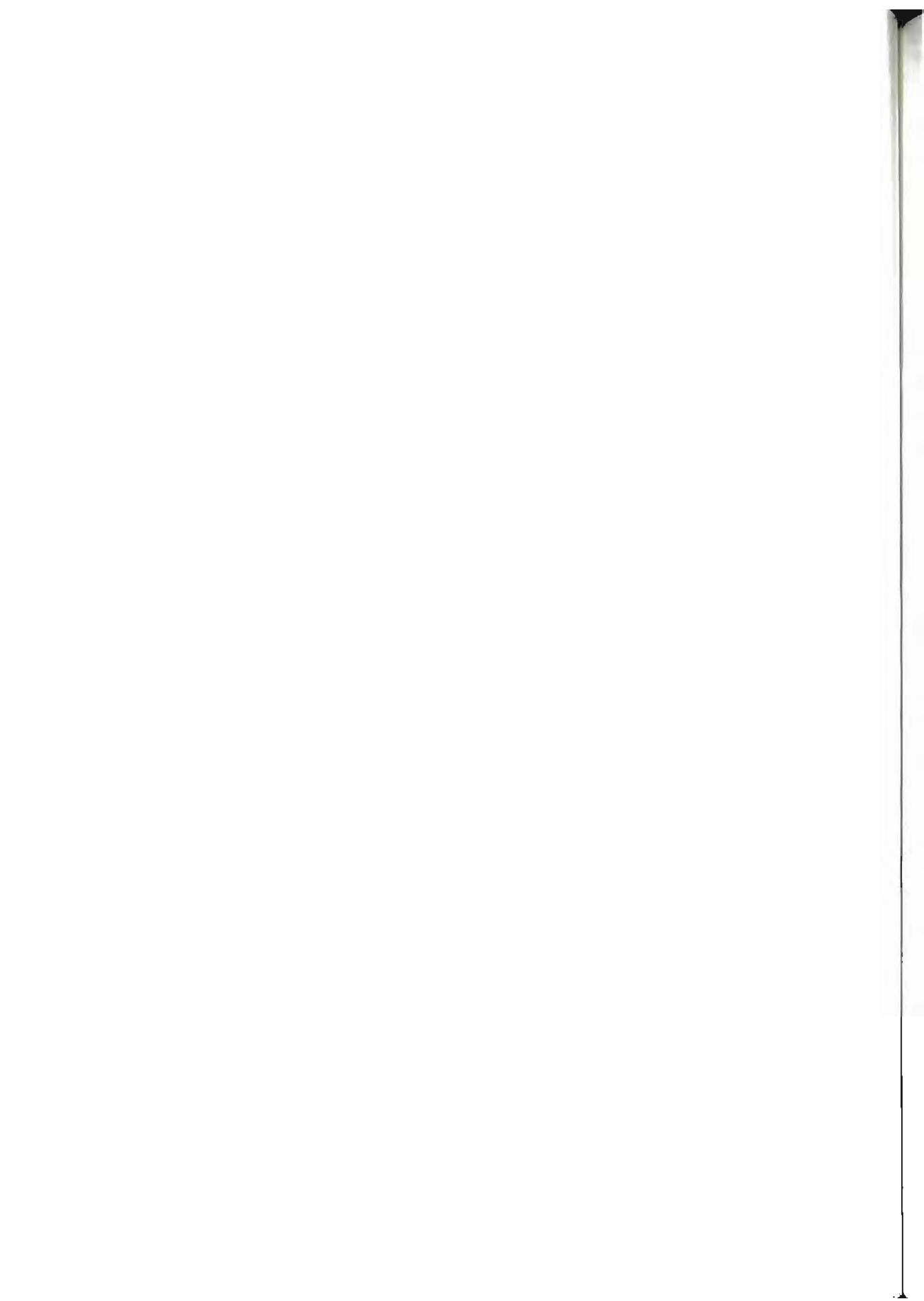
免許を拒否した理由は、請求があるときは申請者に通知する。

## 5 独立の規制機関

規制機関は、いかなる基本電気通信サービスの提供者からも分離され、かつ、いかなる基本電気通信サービス提供者に対しても責任を負わない。規制機関が行う決定及び規制機関が用いる手続は、市場のすべての参加者について公平でなければならない。

## 6 稀少な資源の分配及び利用

稀少な資源（周波数、番号及び線路敷設権を含む。）の分配及び利用に係るいかなる手続も、客観的な、透明性のあるかつ差別的でない態様で適時に実施する。分配された周波数帯の現状は、公に利用可能なものとする。ただし、政府の特定の利用のために分配された周波数を詳細に明らかにすることは、要求されない。



# 金融と特許法（序）

相澤英孝

# 目 次

はじめに

## I コンピュータ・ソフトウェアの特許法による保護

1 沿 革

2 特許法の保護の対象としてのコンピュータ・ソフトウェア

3 コンピュータ・ソフトウェアの特許法による保護から生じるいくつかの問題

## II 金融分野におけるコンピュータ・ソフトウェアの特許法による保護

(序)

1 保護の対象

2 特許の効力

## はじめに

20世紀の中頃に誕生し<sup>(1)</sup>、20世紀の後半に急速に発達したコンピュータは、社会の隅々で利用され、我々の生活をコンピュータ以前の時代では考えられないほど豊かなものとしている。金融機関にとっても、コンピュータはなくてはならない技術となっている。電子マネーなどの将来を期待されている金融システムはコンピュータを不可欠な要素としている。金融システムがコンピュータという技術を不可欠の要素としたことから、金融システムは技術開発にインセンティブを与える制度である特許法<sup>(2)</sup>との関りが生まれてくることとなった。金融システムを考える場合には、特許法によって、金融システムのどのような側面がどのように保護されるかということを検討することが必要になったと思われる。そこで、金融システムが特許法によって保護されるかということを検討してみたい。

現代においては、コンピュータ技術におけるコンピュータ・ソフトウェアの重要性が増している<sup>(3)</sup>。そのコンピュータ・ソフトウェアを特許法によって保護することについては、これまでに様々な議論があった。そこで、コンピュータ・ソフトウェアを特許法によって保護することについての議論を振り返った上で、金融システムと特許法を考えてみよう<sup>(4)</sup>。

## I コンピュータ・ソフトウェアの特許法による保護

### 1 沿革

コンピュータ・ソフトウェアはコンピュータに関連する技術であり、バイオテクノロジーなどの他の技術と同様に、特許法によって保護されるとするのが素直な考え方であろう。しかしながら、特許法の保護の対象を決定する「発明」概念は、19世紀の科学技術を前提として作られたためにコンピュータ・ソフトウェアを特許法で保護することに、法技術的な問題が生じたのである。特に、アメリカ合衆国では、最高裁判所の判決が動揺したことなどもあり、混乱が生じていた。そこで、まず、これまでの沿革を振り返ってみよう。

1964年、アメリカ合衆国特許商標庁審判部は、コンピュータ・ソフトウェアを特許法の保護の対象にならないとした(5)。1966年の大統領諮問委員会(6)の報告書でも、コンピュータ・ソフトウェアを特許法の保護の対象から除外すべきであるとした。これに対して、1968年、関税特許控訴裁判所(7)は、In re Prater 事件の判決で、コンピュータ・ソフトウェアが特許法の保護対象となり得ると判断した(8)。この判決後も、特許商標庁は、引き続き、コンピュータ・ソフトウェアの特許法による保護に対して消極的な態度をとり続けた。関税特許控訴裁判所は、1969年の In re Bernhart 事件の判決(9)、1970年の In re Mohony 事件の判決(10)、In re Musgrave 事件の判決(11)、In re Foster 事件の判決(12)、1971年の In re Benson 事件の判決(13)、In re Wadbaum 事件の判決(14)などで、特許商標庁審判部の審決(拒絶を維持する審決)を覆すことにより、コンピュータ・ソフトウェアの特許法による保護に対して積極的な態度をとっていた。1972年に、最高裁判所は、Gottschalk v. Benson 事件で、アルゴリズムは特許法の保護対象にはならないと判断した(15)。Gottschalk v. Benson 事件の最高裁判所の判決の後、関税特許裁判所は、1973年の In re Christensenn 事件の判決(16)、1977年の In re Wadbaum 事件の判決(17)などで、Gottschalk v. Benson 事件の最高裁判所の判決に従いつつも、1974年の In re Johnston 事件の判決(18)、1976年の In re Noll 事件の判決(18a)、In re Chatfield 事件の判決(19)、1977年の In re Deutsch 事件の判決(20)、In re Flook 事件の判決(21)、1978年の In re Freeman 事件の判決(22)、In re Toma 事件の判決(23)、などで、Gottschalk v. Benson 事件の最高裁判所の判決を限定的に解釈し、特許商標庁審判部の審決(拒絶を維持する審決)を覆すことにより、コンピュータ・ソフトウェアの特許法による保護に対して積極的な態度をとっていた。1978年に、最高裁判所は、Parker v. Flook 事件で、新規性のある唯一の特徴がアルゴリズムにある場合は、アルゴリズムを保護対象にするものであるから特許の対象にならないと判断した(24)(25)。その後、関税特許控訴裁判所は、1978年の In re Sarker 事件の判決(26)などで、Gottschalk v. Benson 事件、Parker v. Flook 事件の最高裁判所の判決に従って、特許商標庁審判部の審決(拒絶を維持する審決)を維持しつつ、1978年の In re Johnson 事件の判決(27)、1979年の In re Bradey 事件の判決(28)、In re Diehr 事件の判決(29)などで、特許商標庁審判部の審決(拒絶を維持する審決)を覆して、コンピュータ・ソフトウェアの特許法による保護を認めていた。

1980年に、最高裁判所は、Diamond v. Chacrabarty 事件の判決で、特許に対する消極

的な態度を変更した<sup>(30)</sup>。1982年のDiamond v. Diehr事件の判決で、加硫時間をコンピュータ・ソフトウェアによって制御するゴムを加硫させる方法を特許の対象であるとした<sup>(31)</sup>。この判決後、特許商標庁はコンピュータ・ソフトウェア技術の特許法で保護する方向へとその実務を変更した。

1989年に、特許商標庁は、Patentable Subject Matter Mathematical Algorithm and Computer Program を発表して、再び、コンピュータ・ソフトウェア技術の特許法による保護に、やや消極的な姿勢へと変化した<sup>(32)</sup>。これに対して、連邦巡回控訴裁判所<sup>(33)</sup>は、1994年のIn re Donaldson事件の判決<sup>(34)</sup>、In re Alappat事件の判決<sup>(35)</sup>、In re Lowry事件の判決<sup>(36)</sup>などで、特許の対象に含まれるコンピュータ・ソフトウェアを狭く解釈する特許商標庁審判部の審決を覆すことにより、コンピュータ・ソフトウェアの特許法による保護について積極的な姿勢を示した。アメリカ合衆国特許商標庁は、1996年2月28日、コンピュータ関連発明の審査ガイドライン (Examination Guidelines for Computer-Related Invention Final Version) を発表した。このガイドラインは、1990年代の特許商標庁のコンピュータ・ソフトウェアの特許法による保護に対して示していた消極的な姿勢が連邦巡回控訴裁判所の判決によって否定されたことを踏まえて、コンピュータ・ソフトウェアを技術的性格をもつものとして捉えようとしたものと評価することができるであろう。

日本では、1975年に、特許庁が「コンピュータ・プログラムに関する発明についての審査基準 (その1)」、1982年に、「マイクロコンピュータ応用技術に関する発明についての運用指針」を発表し、コンピュータ・プログラムそのものを特許の対象として保護することは否定しつつ、コンピュータ・ソフトウェアの特許法による保護を緩やかに進めようとしていた<sup>(37)</sup>。ここでは、従来技術の延長線上にコンピュータ・ソフトウェアを捉えて、特許法による保護を与えようとしていたと評価することができるであろう。特許庁は、1988年に、「コンピュータ・ソフトウェア関連発明の審査上の取扱(案)」を、1993年に、「審査基準 (改訂版)」を発表したが、これらは、基本的な考え方の整理という趣旨を持つものというべきものであり、それまでの考え方を踏襲するものであったと評価すべきものであろう<sup>(38)</sup>。特許庁は、1997年3月に、「産業上利用することができる発明の審査の運用指針、特定技術分野の審査の運用指針 第1章コンピュータ・ソフトウェア関連発明」を発表した。この運用指針では、コンピュータ・ソフトウェアを技術的性格をもつものと

して正面から捉える方向への萌芽をみてとることができると思われよう。

## 2 特許法の保護の対象としてのコンピュータ・ソフトウェア

### (1) 問題の所在

特許法は、産業革命時代に、産業革命を担う技術を保護し、現代の花形技術の一つであるバイオテクノロジーを保護してきたことからすれば、コンピュータ・ソフトウェアも、技術として特許法によって保護することは奇異なことではないと思われる。コンピュータ技術の中でも、ハードウェアに関する技術は、特許法によって保護されてきた。それにもかかわらず、コンピュータ・ソフトウェアを特許法によって保護することを中心として、コンピュータ・ソフトウェアの保護の議論がなされなかったことにはいくつかの理由があったように思われる。もっとも、日本とアメリカ合衆国では、特許法によるコンピュータ・ソフトウェアの保護の流れも、議論も異なっているように思われる。

日本でコンピュータ・ソフトウェアの特許法による保護について緩やかな歩みであったことには、実質的な理由と法技術的な理由がある。

実質的な理由としては、コンピュータ・ソフトウェアを特許法で保護するだけでは十分ではないことがあげられる。コンピュータ・ソフトウェアを特許法で保護するだけでは十分ではないとする理由は、コンピュータ・プログラムの寿命が短く、特許法による保護が審査のためのタイム・ラグが大きいこと、模倣が極めて容易であるところから特許の公開によってプログラムの模倣が行なわれること、バージョン・アップの毎に特許を出願することは困難であること、特許庁における審査が困難であること、進歩性のあるものが少ないこと、などがあげられている(39)。

法技術的な理由としては、特許法に「発明」の定義があり、その定義によれば、「発明」とは「自然法則を利用した技術的思想」であるとされていることから、コンピュータ・ソフトウェアが「自然法則を利用した技術的思想」であるか、特に、「自然法則を利用」しているか、という点について、解釈上の議論があり、特許庁がコンピュータ・ソフトウェアを特許法で保護することに慎重であったことがあげられる。

アメリカ合衆国では、コンピュータ・ソフトウェアを特許法によって保護することに審査を担当する特許商標庁が反対したことが大きな理由であると思われる。特許商標庁がコンピュータ・ソフトウェアを特許法によって保護することに反対した理由は、当時特許商

標庁は、大量の未審査特許出願を抱えていたこと、コンピュータ・ソフトウェアに関する先行技術を有していないというところにあったとされている(40)。また、1980年代までは、特許法による保護に対して、最高裁判所は消極的であり、最高裁判所の特許の保護の対象に関する判例理論との整合性の問題もあった。

問題の核心は、コンピュータ技術は課題解決のための新しい処理技術であるというところにある。実質的には、これまで特許法によって保護されてきた技術とは異なる性格を有し、特許制度の保護の対象外とされてきたビジネス・システム、ゲームなどを含む極めて広い応用分野を持っている処理技術であるコンピュータ・ソフトウェアを特許法によって保護することが妥当かという問題がある。法技術的には、これまで、物理学的な手法あるいは化学的な手法などによってなされる課題解決技術を保護してきた特許法によって、アルゴリズム（論理的手法）による課題の解決を行うコンピュータ・ソフトウェアを保護の対象とすることによって生じる問題がある。

## （2）特許制度の在り方

コンピュータ・ソフトウェアをさらに発展させるために、技術開発に対するインセンティブを与えていくことが必要であるかというところにも議論がある。コンピュータ・ソフトウェアを発展させるためにインセンティブを与える必要がない、コンピュータ・ソフトウェアの模倣を自由におくべきだという考え方も無いわけではない。しかしながら、コンピュータ・ソフトウェアは技術開発投資に対して、生産のために必要な投資は極めて小さく、その模倣からの保護をしなければ、技術開発投資が十分になされなくなるおそれがある(41)。従って、現在なされている議論の中心はどのようにしてコンピュータ・ソフトウェアを保護することが望ましいかということについてなされている。

コンピュータ・ソフトウェアを特許法によって保護することについての批判がある(42)。この批判は二つの側面を有する。一つは特許法という法技術によってコンピュータ・ソフトウェアを保護することが妥当であるかというのであり、もう一つは特許法は何を保護すべきで何を保護すべきではないかという理念的なことである(43)。

特許法による保護の妥当性に関しては、①特許法が保護対象としている技術とコンピュータ・ソフトウェアは異なるとの主張(44)、②現在では、抽象的一般的なアルゴリズムが特許による保護を受けにくい、それでは十分な保護とはならないし、抽象的一般的なア

ルゴリズムを対象とするクレームを認めることは保護が過剰になるとの主張(45)、③現在行なわれている開示が不十分であるとする主張(46)、④特許法による保護が十分な保護を与えないとの主張(47)、⑤科学的研究を阻害するとの主張、⑥法的処理に費用を要するとの主張、⑦特許法の運用に関しては、先行技術の調査が難しいことによる審査の困難であるとの主張がある(48)(49)。しかしながら、これらの批判は特許法の運用において、その解消をはかることができるものであるか、特許法の誤解(特許法は科学的研究には効力が及ばない)あるいは法制度全般に対する批判(特許法以外でもなんらかの法的保護を行えば費用は発生する)であって、特許法による保護を否定する理由とはなりえない。

理念的には、コンピュータ・ソフトウェアの特許法による保護は、特許法によってアルゴリズムの保護することになり、アルゴリズムを特許法によって保護することは認めるべきではないとする主張がある(50)。この主張は、19世紀以来のサイエンスとテクノロジーの分け方を前提にするもので、アルゴリズムはサイエンスに属し、サイエンスは万人共有のものであるとする基本的な考え方に基づく主張である。しかしながら、前述のように、19世紀のサイエンスとテクノロジー区分が不明確となった現在、このような考え方に基いてコンピュータ・ソフトウェア技術の特許法による保護を否定することには疑問がある。インセンティブを与えることなしにコンピュータ技術の発展がなされるかどうかの問題なのである。

特許法によるコンピュータ・ソフトウェアの保護に反対する論者は、著作権法あるいは特別法による保護を主張する(51)。

コンピュータ・ソフトウェア特別法(sui generis)による保護を主張する説(52)は、コンピュータ・ソフトウェアの技術的特性に応じた保護をなすべきであるとするものであるが、現状の特許法、著作権法による保護に代えて特別法を世界中でつくらなければならず現実的であるかどうか疑わしい(53)。著作権法による保護を主張する論者は、①登録なしに権利が発生すること、②独自開発が認められること、③著作権法による保護の範囲が狭いこと、を挙げている。しかしながら、著作権法による保護は、権利の発生に登録を要しないことは多数の国で保護を受けるためには有効であるが、①開示がないため権利の存在及び範囲が不明確であるために第三者は不安定な立場に置かれるとともに、②保護の期間が長いこと、③保護の範囲について様々な議論があり過小な保護と過剰な保護の可能性があること、④独自開発を主張することは事実上難しいこと(53a)、等の問題点が存在する。

このような議論が誤謬をともなった議論であるかないかはともかく、コンピュータ・ソフトウェアを特許法によって保護することは、日本、アメリカ合衆国、ヨーロッパで行なわれており、このような方向から外れることは、それにより生じる国内的混乱あるいは国際摩擦が余りにも大きいものと推測されるので、コンピュータ・ソフトウェアを特許法によって保護しないとする選択肢は、現実の選択肢としては、取りえないものと思われる(54)。これから必要とされるのは、具体的な問題について、コンピュータ・ソフトウェアの特許法による保護が与える影響なども考慮しながら、どのような制度設計を行なうことが、コンピュータ・ソフトウェア、コンピュータ、経済の発展に好ましいかという見地からなされるべきものであろう。

### (3) 制度設計

現在では、コンピュータ・ソフトウェアを特許法によってどの程度保護すべきかという観点から、保護の対象をどうすべきかという検討が加えられている段階にあると見てよいであろう。ここでは、コンピュータ・ソフトウェアに関する産業政策的判断が問われることになる。

コンピュータ・ソフトウェアがアルゴリズムによる処理を行うことはその性質上当然のことであり、アルゴリズムをどの程度保護していくかということの一つの論点として考えていくべきであろう。アルゴリズムには汎用性のあるものも、特定の技術にのみ利用されるものもあるであろう。そこで、どの程度の汎用性まで特許の保護の範囲を認めていくかということを考えていくべきであろう。汎用性の高いアルゴリズムは技術的貢献が大きいことから広い保護の範囲を認める事がその開発に対するインセンティブを与えることになる反面、特許による技術の独占による弊害が生じるおそれがあるので、そのバランスを考えることが重要となろう。アルゴリズムを特許法で保護することに対しては、批判的な考え方もある。しかしながら、コンピュータ・ソフトウェアを特許法によって保護する以上、その実質は、アルゴリズムを保護するものになることは避け難いのである。

これまで、特許法の保護の対象とされていなかった営業方法 (doing business)、暗号などがコンピュータ・ソフトウェアによって実現される時代となってきた。そこで、コンピュータ・ソフトウェアを特許法の保護の対象とすることによって、従来、特許法の保護の対象に含まれなかったこれらの技術が、保護の対象に取り込まれることに対しては疑問

も示されている。これまで、営業方法、暗号などが特許法の保護の対象とされてこなかった理由は、技術的色彩が希薄である（営業方法）こと、数学的色彩が濃厚である（暗号）こと、特許法による保護が与えられなくてもその発展が妨げられない（特許法による保護がなくても営業方法の改善は進んだ）こと、特許法によるインセンティブが影響があまりない（暗号技術は軍事技術として開発が進められた）ことによるものと推測される。しかしながら、20世紀後半、特に、最近のコンピュータ技術の発展において、コンピュータ技術を利用した営業方法、暗号などが特許法による保護の対象の外に置かれたままでよいかということを考えなければならない。コンピュータを利用する営業方法、暗号などは技術的色彩を有し、コンピュータ技術を利用した営業方法はコンピュータ・ソフトウェアを模倣することにより模倣が容易になり、暗号技術は軍事技術から民生技術へと進んできた。そして、現代社会においては、コンピュータ技術の発達によって、営業方法、暗号等の技術の社会的な役割が増大している。そう考えれば、コンピュータ技術を利用した営業方法、暗号などを特許法の保護の対象として、その開発に対してインセンティブを与えることに消極的となるべき理由はないのではないかとと思われる。もっとも、これらの技術をどの程度保護していくかということは別の問題である。例えば、既存の営業方法にコンピュータ技術を利用した方法が特許による保護を取り込まないような配慮などが必要とされるであろう。

#### (4) 法技術的問題

##### (i) 日本

日本の特許法は、特許の保護の対象を発明であるとし、「発明とは、自然法則を利用した技術的思想のうち高度のものをいう」と定義している（特許法第2条）が、コンピュータ・ソフトウェアは、「自然法則を利用した技術」にあたるかということが問題となる。

アメリカ合衆国におけるガイドラインの再検討という状況を受けて、日本でも、1995年の秋頃から、審査基準の検討作業が開始され、「産業上利用することができる発明の審査の運用指針、特定技術分野の審査の運用指針 第1章 コンピュータ・ソフトウェア関連発明」（以下単に「運用指針」という）が作成された<sup>(55)</sup>。そこでは、コンピュータ・ソフトウェアを特許法によって保護することについての理論的・解釈的な再検討がなされた<sup>(56)</sup>。

「審査基準（改訂版）」は、従来の解釈を原則として踏襲するものであり、「自然法則を利用した」というところにかなり重きを置いた解釈となっていた。「産業上利用することができる発明」の審査の運用指針でも、これまでの「発明」に関する考え方が継続しているように見える。しかしながら、「運用指針」を合わせ読むと、従来からの考え方を変えていこうという姿が見て取れる。

「運用指針」においては、「コンピュータを用いた処理」のみである場合には、「自然法則」は利用しているが、保護の対象とされない自然法則以外の法則（具体的には、アルゴリズム）そのものを特許法の保護対象とすることになるので認められないとしている。これは、従来の「自然法則の利用」の概念を変更するものである。

「運用指針」においても、コンピュータ・プログラムそのものを指すクレームは認められないとしている。ただし、その理由を、コンピュータ・プログラムは、物か方法かが不明確であるから第36条に反するので認められないというところに置いている（1.3）。「審査基準（改訂版）」では、技術的思想ではないから特許の対象とはならないとしていたが、コンピュータ・プログラムの技術的性格を認めて変更したものであり、コンピュータ・ソフトウェア技術の性格に則した解釈になっている（57）（58）。

これは、19世紀の技術に基づく概念である「自然法則の利用」から、20世紀末のコンピュータ時代の特許法へと動いてきていることを示すものと言えよう。このことは、技術の現代的把握による特許法の現代への対応というものであり、特許制度の捉え方として前向きな考え方といえることができるであろう（59）。

## （ii）アメリカ合衆国

アメリカ合衆国の特許法は、特許の保護の対象は「方法（process）、機械（machine）、製品（manufacture）、もしくは、組成物（composition of matter）」であると規定している（特許法第101条）。現在この条文の解釈の基本となっているのが、「太陽の下、人によってつくられたすべてのもの（anything under the sun that is made by man）」が特許の対象になるとする1980年の *Diamond v. Chakrabarty* の最高裁判所の判決である（60）。そして、コンピュータ・ソフトウェアについて、*Diamond v. Diehr* 事件の判決はこの判決に倣った（61）が、この判決以前の *Gottschalk v. Benson* 事件の判決及び *Parker v. Flook* 事件の判決の判例を明示的に変更しなかったため、これらの判決との整

合性を保った解釈がなされることとなった。そして、関税特許裁判所は、Gottschalk v. Benson 事件の判決及び Parker v. Flook 事件の判決を踏まえた1978年の In re Freeman 事件の判決<sup>(62)</sup>、1980年の In re Walter 事件の判決、Diamond v. Diehr 事件をも踏まえた1982年の In re Abele and Marshall 事件の判決<sup>(63)</sup>などで、数学的アルゴリズムを保護の対象とはしないとしつつ、数学的アルゴリズムの応用は保護の対象となるとする理論をとった。連邦巡回控訴裁判所の、1994年の In re Donaldson 事件の判決<sup>(64)</sup>、In re Alappat 事件の判決<sup>(65)</sup>、In re Lowry 事件の判決<sup>(66)</sup>などの判決も、この理論を否定するものではなかった。しかしながら、コンピュータ・ソフトウェアの特許法による保護はアルゴリズムの特許法による保護を意味するものであり、理論的には無理のあるものであった。そして、1996年の特許商標庁のガイドラインは従来の特許商標庁の考え方から、実質的な転換を示そうとしているものと理解することができるであろう。

このガイドラインでは、抽象的な概念 (abstract idea)、自然法則 (law of nature)、自然現象 (natural phenomenon) が、判例によって特許法の保護の対象とならないとされているとした上で、特許の対象 (subject matter) は技術 (technological art) で、実用的な応用 (practical application) を有しなければならないとしている<sup>(67)</sup>。これは、従来のアルゴリズムに捕らわれた解釈から、コンピュータ・ソフトウェアの技術的性格に着目した解釈へと、実質的な脱皮を意味するものと解釈することができるであろう<sup>(68)</sup>。

### (iii) ヨーロッパ

ヨーロッパ特許条約第52条は、「…(2)…(a)…数学的方法 (mathematical method) …(c)精神作用 (mental acts)、遊技 (playing game)、営業方法 (doing business) を実行するための体系 (schemes)、規則 (rule)、方法 (method)…コンピュータ・プログラム…(d)情報の提示 (presentation of information)」を特許の保護の対象から除外している。コンピュータ・ソフトウェアを特許の保護の対象とする場合には、この規定との関連が問題となる。コンピュータ・ソフトウェアは数学的方法やコンピュータ・プログラムを含むものであり、遊技や営業方法のコンピュータを用いた処理を可能とするものだからである。ヨーロッパ特許庁技術審判部 (Technical Board of Appeal) は、VICOM 事件 (T208/84) で、ヨーロッパ特許条約第52条の規定は、数学的方法、コンピュータ・プログラムそのものに向けられた発明を特許の対象から除外しているのであって、数学的方

法、コンピュータ・プログラムを含む発明であっても、技術的方法 (technological process) に向けられた発明を特許の保護の対象から除外するものではないとした。ヨーロッパ特許庁のガイドラインは、抽象的なもの (abstract)、非技術なもの (no-technical) を特許の対象から除外するとした上で、コンピュータ・プログラムが装置 (implementation) に含まれているからといって特許性 (patentability) は否定されないとしている。

#### (iv) 小括

コンピュータ・ソフトウェアを特許法によって保護することによって生じた理論的問題は、コンピュータ技術の核心である論理的課題のコンピュータによる解決というところに由来すると思われる。これまで、特許制度は物理的課題、化学的課題などの解決をはかる技術を保護する制度として発達してきた。それに対し、コンピュータ・ソフトウェアは、ビジネスの方法やゲームなどの技術的課題とされていなかった課題を、アルゴリズムという技術によって解決するということにより、それまでの特許法の考え方の変換を迫ったのである。一方、コンピュータ技術は、これまで、人間が行ってきた論理的な課題の解決を技術的に行うことを可能にしたところに現代社会の中核となる技術となりえる汎用性をもったのである。そこで、特許法による論理的な課題の解決技術の保護という新しい局面に対する法制度的な対応の遅れが上述のような混乱を招いたものということができるであろう。このような混乱は時間的経過にしたがって解消されるものであり、現に、時間的経過によって特許制度はコンピュータ技術開発成果の保護の方向へと動いてきたということができるであろう。

コンピュータ・ソフトウェアの特許法による保護は、アルゴリズムの特許法による保護という性格を私拭することはできない。サイエンスとテクノロジーを分け、特許法はテクノロジーを保護する制度であるとする考え方に立ち、アルゴリズムはサイエンスに含まれると考えると、特許法でコンピュータ・ソフトウェアを保護することに対する疑問が生じる。しかし、そもそも、サイエンスとテクノロジーを分け、特許法はテクノロジーを保護する制度であるとするのは、機械技術時代であった19世紀の技術状況を前提とした議論であって、コンピュータ・テクノロジー時代、バイオテクノロジー時代の現代に19世紀的な考え方をあてはめることは困難である。19世紀の産業政策を、20世紀、21世紀に行うべきであるというのは、両者の技術環境、経済環境を無視した議論というべきである。現代で

は、サイエンスとテクノロジーの両者は峻別できるものではない。アルゴリズムを特許法によって保護することを特許法の理論上の問題とするところにこそ問題があるというべきであろう。コンピュータ・ソフトウェアが特許法によって保護されるべきかいは、アルゴリズムの開発に対するインセンティブを与えるために、特許法による保護が必要かという政策的な判断によって決定すべきものである。

日本の特許法の解釈として、コンピュータ・ソフトウェアがコンピュータという「自然法則」にしたがって作動する装置を作動させることを目的とする技術である以上、「自然法則を利用」しているとし、課題のコンピュータを利用した解決という技術的性格を有するところから技術的思想であるとして、特許法の保護の対象としての「発明」であることに大きな法解釈上の問題はないといえるであろう。新しい技術を法解釈上の問題から保護の射程外に置くということは、日々発展を遂げている技術の保護を目的とする特許法の解釈としては妥当とは思われない。どのような課題のどのような処理方法による解決を特許法によって保護していくかということが問題である。そのメルクマールとなるのが「技術思想」であると思われる。特許法が技術の保護によって技術開発へインセンティブを与えることを目的とし、「自然法則の利用」という概念が機能しなくなっている以上、「技術思想」という概念によって、保護の対象を確定するという解釈論が取られるべきであると思われる。

### 3 コンピュータ・ソフトウェアの特許法による保護から生じるいくつかの問題

(1) どのようなクレームが認められるか

(a) クレームの役割

クレーム（請求の範囲）は、特許の保護の対象を特定し、特許の保護の範囲決定する基礎となる。クレームによる保護の対象の特定は、特許の保護の対象となるべきものかどうかという判断の基礎になり、特許庁における審査の対象を特定するという機能を営むことになる。クレームは保護の範囲の決定の基礎として、侵害訴訟において侵害の成否を左右する機能を営むことになる<sup>(69)</sup>。特許庁が、どのようなクレームを認めるかということは、そのクレームによって特定される保護の対象が特許法によって保護されるものかどうか、どの範囲の保護を認めるべきものかという見地から判断されることになる<sup>(70)</sup>。この特許庁の判断は、裁判所の再審査を受けるものであり、アメリカ合衆国においては、特許

商標庁が示した判断が、しばしば、巡回控訴裁判所（関税特許裁判所）によって覆され、裁判所の判決が認められるべきクレームを決定してきた。これに対して、日本では、特許庁の認めるクレームに関して不服が申し立てられることが少なく、クレームは事実上特許庁によって決定されている。

コンピュータ・ソフトウェアに関する特許について、特許法によって保護されるべきかという観点からどのようなクレームが認められるかという問題については、①クレームによって特定されているものによって生じる問題、②クレームによって特定されている特許の用いている手法によって生じる問題、③クレームの特定されている技術によって解決される課題によって生じる問題に大別することができるであろう。①の問題には、1) コンピュータ・プログラムそのものを特定するクレームと、2) コンピュータ・プログラムを格納した媒体を特定するクレームの問題がある。②の問題には、アルゴリズムによって特定しているクレームの問題がある。③の問題には、営業方法を実現することを内容とするクレーム、ゲームを行うことを内容とするクレームなどの問題がある。

(b) クレームによって特定されているもの

(α) コンピュータ・プログラムそのものを対象とするクレーム

コンピュータ・プログラムそのものを対象とするクレームについては、特許庁は、一貫してこれを否定している。「コンピュータ・プログラムに関する発明についての審査基準（その1）」、「審査基準（改訂版）」のいずれにおいても、コンピュータ・プログラムそのものを特定したクレームは認められないとしていた。その理由は、「コンピュータ・プログラムに関する発明についての審査基準（その1）」では、「極めて抽象的なもの」であることにあるとされ、「審査基準（改訂版）」では、「技術的思想ではない」とされた。

アメリカ合衆国特許商標庁は、コンピュータ・プログラムは単なる思想（mere idea）であるか、抽象的概念（abstract intellectual concept）であるか、記述的なものの集合（collection of printed matter）であるので、特許法の保護対象に含まれないとしていた(71)。

ヨーロッパ特許条約第52条(c)は、コンピュータ・プログラムそのものを特許の対象としないものとしている(72)。

コンピュータ・プログラムは、コンピュータを制御する機能を営むものであり、技術的

性格を有することは否定できないであろう。コンピュータ・プログラムは記述的な性格を有するけれども、機械の特許でもその対象である発明を図面で記述することができる。それは、コンピュータ・プログラムの場合には紙の上に記述されたプログラムを利用することが、機械の図面にしたがって機械を組み立てることよりも容易であるという程度問題に過ぎないというべきである。問題は、コンピュータ・プログラムは、「物」のカテゴリーに含むと考えるか「方法」のカテゴリーに含まれると考えるのかというところにあるというべきであろう。コンピュータ・プログラムを「方法」のカテゴリーに含むものとする、コンピュータ・プログラムという用語を用いなくてもクレームすることができることになり、コンピュータ・プログラム・クレームを認めたとしても意味がないことになる。コンピュータ・プログラムを「物」のカテゴリーに含むものとする、①コンピュータ・プログラムを記録した記録媒体の製造・販売などに特許権の効力が及ぶことが明確となること、②コンピュータ・プログラムを通信によって輸入・販売することに特許の効力を及ぼすこと、にコンピュータ・プログラム・クレームを認める意義があることになる。①は、後述のコンピュータ・プログラムを記録した記録媒体のクレームを認めることにより解決できる一方、②は「物」の通信による輸入・販売という、これまでの「物」のカテゴリーに属するとされているものによっては考えられない行為に特許権の効力を及ぼすことになる。コンピュータ・プログラムの通信による輸入・販売は、マルチメディア・ネットワーク社会においては、コンピュータ・プログラムの主要な流通形態となるので、特許の効力を及ぼせるか否かは重要な問題であるが、これまでの「物」のカテゴリーについての考え方の変化を迫るものであり、更なる検討が必要であろう。

#### (β) コンピュータ・プログラムを記録した記録媒体を特定するクレーム

特許庁は、コンピュータ・プログラムを記録した記録媒体を特定するクレームを否定していた。「コンピュータ・プログラムに関する発明についての審査基準（その1）」、「審査基準（改訂版）」のいずれにおいても、コンピュータ・プログラムを記録した記録媒体のクレームは認められないとしていた。その理由は、「コンピュータ・プログラムに関する発明についての審査基準（その1）」では、単に「手順が記録された物にとどまり、情報が表現媒体をとおして形式付与された著作権と変わるところはない」とされ、「審査基準（改訂版）」では、「情報の単なる提示」で「技術的思想でないもの」とされた。

アメリカ合衆国特許商標庁は、コンピュータ・プログラムを記録した媒体を特定するクレームを認めることはコンピュータ・プログラムそのものを認めることになるから、コンピュータ・プログラムそのものを認めないのと同様の理由で、コンピュータ・プログラムを記録した記録媒体を特定するクレームが特許法の保護の対象に含まれないとしていた。

ヨーロッパ特許庁は、プログラムに特徴のあるコンピュータ磁気テープは、「単に情報の内容にのみ特徴のある情報の提示」にあたり、特許の保護対象とはならないとしている。

コンピュータ・プログラムを記録した記録媒体を特定するクレームを情報の単なる提示であるとしていた日本の特許庁の考え方は、コンピュータ・プログラムの記述的なところを捉え、そのコンピュータ・プログラムが記述された記録媒体を、音楽を録音したCDなどと同じように考えたものということがいえるであろう。この考え方は、コンピュータ・プログラムとCDなどの録音されている音楽を同じく技術的思想ではないと考えるところに基礎を置いている。コンピュータ・プログラムを技術的な性格を持つ機能的なものと考えれば、そのコンピュータ・プログラムを記録した記録媒体は、組換え遺伝子を含む宿主細胞と同様に考えられ、特許法の保護の対象となるとすることができるであろう。

コンピュータ・プログラムを記録した記録媒体を特定するクレームを認めないことの問題点は、装置あるいはシステムなどを特定するクレームを有するコンピュータ・ソフトウェアの特許がある場合に、そのクレームを内容を実現するコンピュータ・プログラムが媒体に記録されて販売された場合に、間接侵害が成立しないと解釈されるおそれがあるところにあった。コンピュータ・プログラムが技術的性格を持ち、コンピュータ・プログラムを記録した記録媒体が「物」として存在を有し、コンピュータで直接に実行されるものであることに思いを致せば、このようなクレームを認めることに大きな問題はないと考えられるであろう(73)(74)。

なお、特許庁は、記録媒体を特定するクレームを認めることとした「運用指針」の適用を平成9年4月1日以降の出願に限定するものとしている(75)が、これには疑問がある。特許庁の審査基準などのガイドラインは、あくまでも特許法の適切な適用のための基準であり、「運用指針」によるガイドラインの変更は過去の不適切なガイドラインの変更という性格を持つものであり、これまでに、出願公告された例もあり(76)、継続中の出願につ

いて過去の不適切なガイドラインを適用することは、適切な法の執行とは言えないと思われる。そして、現在手続継続中の記録媒体のクレームを含まない特許出願については、特許庁の審査基準に従って記録媒体のクレームを含めていなかったのであるから、補正によって記録媒体のクレームを認めるべきものと思われる。

#### (c) クレームによって特定されている特許の用いている手法

特許庁は、クレームにおけるアルゴリズムの記載については、アルゴリズムそのものは「自然法則を利用していないもの」であり特許法の保護の対象に含まれないから、アルゴリズムそのものをクレームすることは認められないとしてきた。しかし、アルゴリズムそのものをクレームしたと解される特許も、カーマーカー法の特許も認められている(77)。

アメリカ合衆国におけるコンピュータ・ソフトウェア技術に関する混乱は、アルゴリズムの取扱に関する混乱とも言える。1988年には、いわゆるカーマーカー法に対して特許が付与される(78)など、この混乱が収束されるかに見えたが、1989年に、特許商標庁は新たな方針を発表し、混乱が続くこととなった。

コンピュータで用いられるアルゴリズムそのものをクレームすることを認めたとしても、そのようなアルゴリズムはコンピュータで実行されるという技術的性格を有するものであり、特許法の保護対象にすることにさほど大きな理論的問題があるというものではないと思われる。問題は、そのようなアルゴリズムの応用範囲が多岐に亘る場合に、特許の保護の範囲が広くなり過ぎないかというところにある。これについては、バイオニア発明で応用範囲が多岐に亘る場合には、広い範囲の保護が認められるべきであって、これは、他の分野の特許発明の場合にもことならないとする説もある(79)。この点については、なお、将来的な検討が必要であると思われる(80)。

#### (d) クレームの対象とされている技術によって解決される課題

特許庁は、審査基準(改訂版)で、「自然法則以外の法則(例えば、経済法則)、人偽的な取り決め、数学上の公式、人間の精神活動、を利用しているときは、自然法則を利用したものとはいえず、「発明」に該当しない、クレームされた発明を特定するための事項に自然法則を利用しない部分があっても、クレームされた発明が全体として自然法則を利用していると判断されるときは、その発明は、自然法則を利用したものとする、どのような

場合に、全体として自然法則を利用したものとするかは、技術の特性を考慮して判断する」としている。

この審査基準はやや解りにくいだが、前段からすると、ビジネス・システム、ゲーム、暗号は、特許の対象から除外されるように読めるが、後段で、クレームでコンピュータ技術との関連が示されていれば、自然法則が利用されているとして特許の対象に含まれると理解される<sup>(81)</sup>。このような審査基準の記述は、日本において「自然法則の利用」という概念が独り歩きしていたことの名残ともいってよいものであろう。

アメリカ合衆国では、裁判例を通じて、抽象的な概念は特許の対象とはならないとしていた。ただ、コンピュータを利用するビジネス・システム、ゲーム、暗号などがこれにあたるものとして拒絶されることは余りないようで、裁判例にもみられない<sup>(82)</sup>。

この問題は、従来特許の対象とされてこなかった課題とその解決方法がコンピュータ・ソフトウェアを利用して解決される場合に、特許の保護の対象とするかという問題である。コンピュータ技術の応用範囲の拡大にしたがって、その応用技術の取扱いについての問題で、コンピュータの技術的性格からすれば、当然、特許の保護の対象とされるべきものと思われるが、先行技術の発見の難しさから、従来から存在していた処理に特許が付与されてしまう可能性があり、この点には注意が必要であろう。

## (2) 特許の効力

### (a) 特許の効力の及ぶ範囲

特許の効力は、①特許の対象となっている物の生産、使用、譲渡、貸渡、輸入、譲渡または貸渡の申出、②特許の対象となっている方法の使用、③特許の対象となっている生産方法により生産した物の使用、譲渡、貸渡、輸入、譲渡または貸渡の申出（第68条、第2条第3項）に及ぶものとされている。したがって、コンピュータ・ソフトウェアを含む特許が、「物」としてクレームされている場合には、その「物」の生産、使用、譲渡、貸渡、譲渡または貸渡の申出、輸入に、「方法」としてクレームされている場合には、その「方法」の使用に、「生産方法」としてクレームされている場合には、その「方法」により生産された物の使用、譲渡、貸渡、輸入、譲渡または貸渡の申出に及ぶこととなる。

このように、特許の効力は「物」を対象とするか、「方法」を対象とするかによって異なっている。「物」か「方法」かは、特許のクレームの解釈によって決定される。コンピ

ユーザ・ソフトウェアに関連する特許についてのクレームは、本質的にはコンピュータの利用の仕方という方法的色彩を有するけれども、特許庁がハードウェアと組み合わせるクレームを認めるという実務を取ったこと、「方法」のクレームの特許の効力が限定的であることから、装置、システムなどの「物」のクレームの特許が多い。また、特許庁の認めるクレームについての判断基準が変更されてきていることから、クレームの把握にあたっては、保護の対象とされている技術思想を慎重に決定する必要があるものと思われる。

特許の効力は、さらに、①特許の対象となっている「物」の生産にのみ使用する物の生産、使用、譲渡、貸渡、輸入、譲渡または貸渡の申出、②特許の対象となっている方法にのみ使用する物の生産、使用、譲渡、貸渡、輸入、譲渡または貸渡の申出に、特許の効力が及ぶこととしている（間接侵害）。間接侵害は特許の対象になっている物の生産あるいは特許の対象となっている方法に「のみ」使用される物に限定されている。その物がその他の用途を有していた場合には、特許の対象となっている生産あるいは特許の対象となっている方法に「のみ」使用される「物」とはされないとされている<sup>(83)</sup>。この日本の特許法の間接侵害の規定は、アメリカ合衆国やヨーロッパ各国の特許法<sup>(84)</sup>と比較しても制限的な規定となっている。そこで、ハードウェアとの組合せた「…装置」<sup>(85)</sup>あるいは「…システム」<sup>(86)</sup>というクレームを持つ特許のソフトウェア部分のみが製造、販売についての取扱が問題となる。その「装置」あるいは「システム」に使用するコンピュータ・プログラムを格納した媒体がその装置にのみ使用する「物」といえるかいなか問題となる。コンピュータ・プログラムを格納した媒体をコンピュータ・プログラムを格納した「物」として考えれば、特許の対象とされた「…装置」あるいは「…システム」にのみ使用するものということができると思われるけれども、この解釈に対しては疑問を示す考え方もある。また、特許の対象となっている「…装置」あるいは「…システム」に用いられる以外の機能を有するコンピュータ・プログラムをも含んでいる媒体については、「のみ」という要件を満たすか否かが問題となる。この問題を解決するものとして、「媒体」クレームがある。「媒体」クレームは、コンピュータ・プログラムを格納した記録媒体の生産などを直接侵害とするものであり、「…装置」クレームの本質であるコンピュータ・ソフトウェアの保護を適切になそうとするものである。そのような趣旨で、特許庁は、「運用指針」で、「媒体」クレームを認めることを明示した<sup>(87)</sup>けれども、「媒体」クレームを含まない特許も存在するのであり、そのような特許については、間接侵害の要件である「のみ」を適切

に解釈することにより保護を図っていかなければならないであろう。

コンピュータ・プログラムを記録した「媒体」のクレームで、マルチメディア・ネットワーク時代におけるコンピュータ・プログラムの通信による販売に対して、どのように対処するかという問題がある。ネットワークなどの通信によるコンピュータ・プログラムの販売は、記録媒体が販売されないので、「媒体」クレームを持つ特許の直接侵害とすることはできない。通信回線を通じて販売されるのはコンピュータ・プログラムのみであり、「…装置」あるいは「…システム」の生産にのみ使用する「物」ということは難しく、間接侵害とすることも難しいものと思われる。この問題に対処するためには、アメリカ合衆国のように特許の侵害を誘導する (induce) する行為を特許の侵害とするか、コンピュータ・プログラム・クレームを「物」のクレームとして認め、ネットワークなどの通信によるコンピュータ・プログラムの販売を直接侵害とすることなどが考えられる。

#### (b) 保護の範囲—クレームの解釈—

コンピュータ・ソフトウェアを特許法によって保護するという方向で特許が付与されるようになって、付与された特許がどのような保護の範囲を持つかということが検討されるべき課題となってきている。

特許の保護の範囲は、クレームを基礎として決定されることになっている。しかしながら、コンピュータ・ソフトウェアに関連する特許のクレームは、コンピュータ・ソフトウェアを特許法によって保護することにより生じた理論的問題を回避するために取られた基準によって決定されてきたという性格を有する。このクレームを認める基準は、必ずしも、どのような保護の範囲を認めるかという観点からのみなされているものではない。そこで、このようなクレームについての保護の範囲については慎重な配慮がなされるべきものであると思われる。第三者の保護の範囲についての予測可能性にも配慮をしつつ、適切な保護の範囲を与えるように解釈が為されなければならない。

ハードウェアとの関連づけをしているクレームに関しては、コンピュータ技術の発展による装置構成の変化に対応して解釈されるべきものであるから、異なった装置構成によって、文言上は含まれないシステムであっても、特許の対象とされている技術思想を用いている場合には、均等論を適用することにより、適切な保護をなすべく配慮がなされなければならない。

これに対して、ハードウェアとの関連づけが強調される余り、システムで利用されているアルゴリズムについての限定が為されていない場合がある。このようなクレームの場合には、たとえ、装置構成が同じであるため、文言上、特許の侵害であるとされる場合でも、そのシステムで利用されているアルゴリズムが異なるために、技術思想が異なるものである場合には、クレームの文言を限定的に解釈することにより、適切な保護をなすべく配慮がなされなければならない。

具体的なアルゴリズムを特定することなく、手順によって特定されているクレームについても、その手順を実現する明細書などで開示しているアルゴリズムをも踏まえて、その特許の保護の範囲を考えていかなければならない。

### (c) 国境を越えた特許の効力

これまで、特許法の効力は、その特許を付与した国内に限られていた（属地主義）、従って、国外において、特許の対象とされている「物」の生産、使用、譲渡などがなされても特許の侵害とはされなかった。特許の対象とされた「物」あるいは特許の対象とされた「方法」によって生産された物が輸入された場合に、特許の効力が及ぶものとされてきた。しかしながら、マルチメディア・ネットワーク時代における技術は、物の移動を伴わないコンピュータ・ソフトウェアの流通、国境を越えたコンピュータ・システムの実現を可能とした。これによって、特許の効力に対する従前の考え方が再検討を迫られることとなった。

コンピュータ・ソフトウェアは通信によって、国境を越えて、販売される。通信を利用したコンピュータ・ソフトウェアの個々の取引を捉えて、国内の購人者に対して特許権を行使することは事実上不可能である。インターネットのホーム・ページを利用した広告などに特許の対象とされたコンピュータ・ソフトウェアの譲渡の申出であるとして特許権を行使しようとしても、譲渡人は国外において行為をなしているので、従来の方に基づけば特許権の効力を認めることは難しい。もし、国境を越えたコンピュータ・ソフトウェアの通信による販売に特許権の効力が及ばないとすれば、特許による保護がないパテント・ヘブンにコンピュータ・ソフトウェアの送信基地を置くことによって、特許権の行使を受けることなく、特許の対象とされたコンピュータ・ソフトウェアを販売することが可能となる。

あるいは、コンピュータを利用したシステムにおいては、そのシステムの構成要素をすべて一国の中に置いておく必要はない。ユーザーの所に端末を置いておけば、ホスト・コンピュータはどこに置いておいても構わない。システムを処理するプログラムとそれを利用するホスト・コンピュータが国外に置かれている場合は、国内において、特許の侵害があるということは難しい。特許による保護がないパテント・ヘブンにシステムを処理するプログラムとそれを利用するホスト・コンピュータを置くことによって、特許権の行使を受けることなく、特許の対象とされたシステムを実現することが可能となる。

このような国境を越えた技術の利用に対する一つの対策は、特許法の域外適用である。国外におけるインターネットのホーム・ページを利用した広告、国外からコンピュータ・ソフトウェアの通信による販売、あるいは、国際的な通信を利用したシステムも特許権の侵害とすることである<sup>(88)</sup>。Playboy Enterprises v. Chuckleberry Publishing 事件の判決<sup>(89)</sup>などを見ると、アメリカ合衆国では、特許法の域外適用で、このような問題を解決する方法を取るかもしれない。しかしながら、特許法の域外適用は、外国における行為に特許権の効力を及ぼすものである。一つの国で特許を取得すれば、その国の特許でネットワークで繋がれているすべての国で特許権を行使できることになる。特許の対象とされている技術を利用しようとする者はネットワークで繋がれているすべての国で許諾を得ることが必要になる。

これは、TRIPS 協定、バリ条約、MAI（多国間投資協定）などの前提としている国際的な特許法の枠組みと異なるものであり、慎重な検討を必要とする。また、域外適用から生じる国際法上の問題も検討しなければならない。

## II 金融分野におけるコンピュータ・ソフトウェアの特許法による保護(序)

### 1 どのような特許が認められるか

#### (1) 金融システムに関する特許<sup>(90)</sup>

金融分野における特許としては、金融システムに関連する特許がある。従来、金融サービスの方法は営業の方法に含まれると考えられ、営業の方法は単なる精神活動として特許

の対象とはならないと考えられていた。けれども、コンピュータを利用した金融に関するシステムは特許の対象とされている(91)。

アメリカ合衆国では、営業の方法(Business System)について、20世紀の初めには、ウェイターによるごまかしを防ぐためのレストランの帳簿維持の方法は特許の対象とはならないとしていた(92)が、コンピュータを用いた会計方法(93)、Cash Management Account(94)については特許の対象になるものとしている。そして、特許商標庁も、金融システムに関する特許を認めている(95)。しかしながら、最近でも、特許を否定する判例もあり(96)、クレームによっては特許を否定される可能性を残している。

営業の方法である金融システムを保護の対象とすることには疑問が無いわけではない。営業方法は単なる精神活動として特許法の保護がなされなかったのであり、コンピュータ・システムによる営業方法についてのみ特許法の保護を与えるべきかということが議論されなければならない。反面、営業方法がコンピュータ・システム化されることにより、技術的性格を帯びるものとなってきていることも忘れてはならない。コンピュータ・システムによる営業方法に特許法による保護を与えることとコンピュータによらない営業方法に特許法の保護が与えられないこととのバランス、コンピュータ関連技術に特許を与えることとコンピュータの応用技術の一つであるコンピュータ・システムによる営業方法に特許を与えることとのバランスなどの諸要素を勘案して決定されなければならない。

金融システムを特許法の保護対象とする場合には、どのようなクレームを認めるかにも注意しなければならない。金融システムの方法のみを記述し、その具体的な実現方法を記述していないクレームは技術的な特徴が記述されていないので、クレームとして問題がないとは言えない。クレームは特許の保護の範囲を決定する基礎となるものであり、金融システムに関する特許の場合にも、その技術的な特徴が記述されるべきものではないかと思われる。

金融システムを特許の対象として認めた場合には、その金融システムを実現する技術に新規性、進歩性がなくてはならないと考えるべきであろう。金融システムが特許の対象とされるのは、その技術的な特徴に着目したからにはほかならないからである。また、金融システムを実現する具体的な方法が明細書において開示されていなければならないと考えるべきであろう。具体的な実現方法の開示されていない金融システムの特許は、単なる営業の方法と異なるところがないというべきだからである。

## (2) 暗号に関する特許

インターネットを用いた金融システムでは、安全な情報伝達のために暗号技術は不可欠の要素とされている。この暗号技術に関して、暗号作成方法は、特許の対象とはならないとした判例がある(97)けれども、現代におけるコンピュータを利用した暗号については、インターネット社会において大きな需要があり、その技術開発へのインセンティブを与えることが重要であると思われるので、他の、コンピュータ・ソフトウェアと同様に、特許の対象とすべきものと考えられる。暗号技術でも、コンピュータを用いなくても実現できるような暗号の取扱が問題となる。このような暗号は、旧来の暗号と異なるところがないのであり、コンピュータの利用に伴う技術的な特徴がないのであり、特許の保護の対象とすべきか否か問題がある。

暗号に関する特許のクレームには、暗号の手順を示すクレーム、暗号の手順とその手順を実現するアルゴリズムを含むクレーム、暗号装置のクレーム、具体的なアルゴリズムのクレームなどがある。暗号は、アルゴリズムそのものであり、その者を特定するクレームはアルゴリズムを保護の対象としないとする特許庁の運用指針、特許商標庁のガイドラインと抵触するおそれがある。しかしながら、暗号技術の本質であるアルゴリズムそのものを特定するクレームは対象が明確であり、これを否定することは過去への郷愁にすぎないといふべきではなかろうか。また、暗号の手順のみを記述するクレームは暗号作成方法が特許の対象とはならないとした判決と抵触するおそれがある。その暗号がコンピュータによって実現される暗号の手順を記述している場合には、そのクレームを否定すべきものではないであろう。

暗号を特許の対象として認めた場合には、その暗号を実現する技術(アルゴリズム)に新規性がなくてはならないと考えるべきであろう。暗号が特許の対象とされるのは、その技術的な特徴に着目したからにほかならないからである。また、クレームが暗号の手順のみを記述している場合には、その暗号を実現する具体的なアルゴリズムが明細書において開示されていなければならないと考えるべきであろう。具体的な実現方法の開示されていない暗号の特許は、単なる暗号作成方法と異なるところがないといふべきだからである。

## 2 特許の効力

### (1) 金融システムに関する特許

金融システムの特許の効力は、その金融システムを実現する行為に及ぶ。特許の対象とされている金融システムを金融機関が自社の端末などによってその発明を実現した場合に、特許の効力が及ぶことには問題がないとしても、金融システムには複数の当事者が関与することにより問題が生じることがある。金融システムがネットワーク・システムであれば、特許の構成要素とされている装置などが、端末が利用者によって所有されている汎用端末である場合に特許侵害についての問題が生じる可能性がある。ネットワーク・システムの特許発明にとって端末はなくてはならない構成要素であり、端末がなければ技術思想を異にすると思われるので、端末を除外した金融システムに効力を及ぼすことには疑問がある。そこで、利用者の用いている端末を利用する行為を金融機関の行為として直接侵害とするか、金融システムのホストコンピュータとプログラムを用いている金融機関の行為が、特許の対象とされている金融システムのためにのみ使用される「物」として、間接侵害に当たると解釈することが考えられる。しかしながら、端末を使用する利用者の行為を金融機関の行為とすることにもやや無理があるし、金融システムを金融機関以外が作成した場合には、金融機関の行為は、特許の対象となっているシステムにのみ使用される「物」を使用する者に過ぎず、間接侵害の要件である特許の対象となっている「物」の生産などをする者には当たらないので、間接侵害とはならない。もっとも、アメリカ合衆国の場合には、ネットワークを通じて実現する金融システムの主たる構成要素であるホストコンピュータとプログラムを設置する行為を特許侵害を誘導する行為であるとして、間接侵害であるとする事ができるかもしれない。

金融システムに関する特許では、システムの構成要素がクレームに記載されている例がある。このような特許は、実質的には、同一目的の同一の方法による処理であっても、その構成要素を異にするために、文言上の侵害とならない場合もある。コンピュータによる処理を含む金融システムの特許の場合には、これまでの特許庁の審査に関する実務から、クレームにおけるハードウェアとの関連づけがなされている。このような場合には、必ずしも、その技術思想にとって必須ではないハードウェアがクレーム中に含まれていることもあるので、明細書に記載された処理の対象、処理の方法を勘案して、技術思想を同じくする場合には、均等論を適用する積極的な要素として勘案されるべきものであると思われる。反対に、このようなクレームでは、処理の際に用いられるアルゴリズムが特定されていない場合が多い。このような場合には、システムの構成要素を同じくするとしても、明

細書に記載された処理の方法を勘案して、明細書の開示の範囲を超えたアルゴリズムを用いることは特許発明の技術思想を超えるものと考えられるので、そのようなシステムに特許の効力が及ばないように解釈が為される必要がある。

金融システムの構成要素の一部（例えば、CPU）が国外に置かれるなど、国境を越えたシステムが構築される可能性がある。このような場合には、従来の属地的な考え方によると、その侵害行為が国内において行なわれていることが必要になる。システムの構成要素の一部しか国内には存在しないため、文言上の侵害が成立しないのみならず、国外に置かれているシステムの構成要素の一部が重要な要素である場合には均等論も難しく、国内に置かれている構成要素が端末などの汎用性があるものである場合には、日本法では間接侵害の適用も難しい。アメリカ合衆国では、特許侵害を誘導する行為として間接侵害とされるかもしれない。しかし、通信回線を通じて国境を越えて実現されるネットワーク・システムの場合に、特許侵害の成立がないとすると、金融機関はバテント・ヘヴンに本拠あるいはホスト・コンピュータを置くことにより特許侵害を免れようとするであろう。そこで、その国外にあるシステムの構成要素をも加味して、侵害の正否を判断すべきであるとする考え方もありうるであろう。この考え方は、ネットワークを利用した金融システムの実現という見地からは、妥当なものかもしれないが、従来の特許侵害はその国内で実施をする場合に成立するものであり、国境を越えた実施には及ばないとしていることからすると、特許の効力を国外に置ける実施行為の一部へも及ばすことになり、さらに検討が必要とされるであろう。構成要素の一部が国外にある場合にも特許の侵害を認める場合でも、国内にある構成要素が汎用性のある端末のみである場合には、更に、問題が生じるおそれがある。オープンネットワークにおいては、あらゆる国からアクセスが可能であり、汎用端末があるのみで特許の効力が及ぶこととすると、一つの国の特許の効力が世界に及ぶことになる。

このような国境を越えた金融システムについては、その特許訴訟の裁判管轄権と準拠法も問題となる。金融システムを運営する金融機関などの所在地の裁判管轄権、金融システム運用の本拠（ホスト・コンピュータの所在地などが考えられるが、分散処理システムの場合にはどこになるのだろうか）の裁判管轄権、金融システムの構成要素の一部である端末がある国の裁判管轄権、などが考えられるが、その判決の承認執行も含めて検討する必要があるであろう。準拠法についても、金融システムを運営する金融機関などの所在地

の準拠法、金融システムの運用の本拠の準拠法、金融システムの構成要素の一部である端末がある国の準拠法、などが考えられるが、どのような解釈が取られるかを検討する必要があるであろう。いずれの問題も、従来の特許法の地理的限界に関する議論を大きく超えるものであり、検討の必要性は大きい。

## (2) 暗号に関する特許

暗号に関する特許で、その暗号に使用されるアルゴリズムがクレームに含まれている場合には、そのアルゴリズムを中心として特許の効力を考えるべきであろう。従米の審査実務から、クレームには暗号のアルゴリズムに加えてハードウェアの構成が含まれている場合には、ハードウェアなどの構成要素や異なる場合であっても、用いられているアルゴリズムが同じである場合には、積極的に均等論あるいは間接侵害を適用すべき理由があるものと思われる。暗号の特許のなかには、アルゴリズムそのものが技術思想となっている特許もあり、そのような場合には、ハードウェア構成に関らず、特許の効力を認めていく必要が多いものと思われる。

クレームに暗号の手順のみが記載されている場合には、その暗号の手順を実現する具体的なアルゴリズムに特許の効力が及ぶものと解釈されるべきであろう。ただし、その暗号の手順に新規性がない場合には、明細書に記載されている具体的なアルゴリズムのみが保護されるべきものと考えられるであろう。

暗号が国内において利用されている場合には、特許権の侵害となるがその場合でも、公開鍵暗号システムのように複数の当事者が関与している場合には問題が生じる。公開鍵暗号は、送り手と受け手が無くては成立しない暗号システムであるから、送り手あるいは受け手である金融機関の行為だけでは、特許の侵害が生じないのではないかという疑問がある。そこで、金融機関の取引先の行為も金融機関の行為と見て直接侵害とするか、金融機関の暗号を生成するソフトウェアを作成する行為が、特許の対象とされた暗号にのみ使用される「物」を生産するなどの行為ととらえて間接侵害とすることができるかという考え方がありうる。しかし、取引先の行為を金融機関の行為とすることにはやや無理があり、金融機関が暗号のソフトウェアを使用する行為は、特許の対象とされた暗号にのみ使用される「物」を使用する行為に過ぎず、間接侵害とはならないので、金融機関が外部で開発された暗号を使用した場合には間接侵害に問うことはできない。アメリカ合衆国では、公

開鍵に対応する秘密鍵を使用する行為あるいは秘密鍵に対応する公開鍵を使用する行為が特許侵害を誘導する行為にあるものとして間接侵害とされるかもしれない。

金融に関連する暗号が国境を越えて利用される場合には、さらに複雑になる。公開鍵暗号システムの当事者の一方が国内に存在しない場合に、特許侵害に問えるかという問題である。金融機関が国内にいる場合は、金融機関の暗号を生成するソフトウェアなどを生産する行為などが間接侵害となるかという問題であるが、個人の取引先のみが国内にいる場合は、「業として」とはいえないので、特許侵害とはならないし、企業の取引先を特許侵害とすることも現実的には難しい。しかし、これを特許侵害としないと、金融機関はパテント・ヘヴンに本拠あるいはホスト・コンピュータを置くことにより特許侵害を免れようとするであろう。そこで、ネットワークで結ばれている暗号システムの場合には、ネットワークで結ばれている海外の金融機関の行為も国内で行われたとみることができるかという考え方が取れるか、あるいは、アメリカ合衆国であれば、国内で行われている暗号を実現する行為の一部が特許侵害を誘導する行為にあたるものとして間接侵害とされるかという問題である。

このような国境を越えた暗号システムについては、その特許訴訟の裁判管轄権と準拠法とが問題となる。暗号システムを利用している金融機関などの所在地の裁判管轄権、暗号システムを利用している端末がある国の裁判管轄権、などが考えられるが、その判決の承認執行も含めて検討する必要があるであろう。準拠法についても、暗号システムを利用している金融機関などの所在地の準拠法、暗号システムを利用している端末がある国の準拠法、などが考えられるが、どのような解釈が取られるかを検討する必要があるであろう。いずれの問題も、従来の特許法の地理的限界に関する議論を大きく超えるものであり、検討の必要性は大きい。

(注)

- (1) どのような計算機を有する機械をコンピュータというかという問題に関しては、星野力『誰がどうやってコンピュータを創ったのか』(1995年)など。
- (2) 特許制度は、技術の開発者にその技術についての一定期間の排他的利用を内容とする財産権を与えることによって、技術開発インセンティブを与える制度である。その経済的効果については議論がある (N.T. Gallini, Patent Policy and Costly Imitation, 23 Rand Journal of Economics 52 (1992), R.Gilbert and C.Shapiro, Optical Patent Length and Breadth, 21 Rand Journal of Economics 106

(1990)、野口悠紀雄『情報の経済理論』(1974年) 185頁以下ほど)。

- (3) コンピュータ・ハードウェア技術の発達の上に現在のコンピュータ・ソフトウェア技術が築きあげられているのであり、現在においても、コンピュータ・ハードウェア技術が重要ではないという意味ではなく、そのハードウェア技術の発達によりコンピュータ・ソフトウェア技術の比重が高まったというべきであろう。なお、コンピュータ・ハードウェアを特許法によって保護することについて当然のこととされ、もっぱら、コンピュータ・ソフトウェアについての議論がなされている。
- (4) コンピュータ・ソフトウェアについては、単純に特許制度によってインセンティブを与えるという制度にはなっていない(バイオテクノロジー技術についても、単純に、特許制度によって保護しているのではない。その事情は、バイオテクノロジーが農業に影響を与えるところからくる問題である。拙著『バイオテクノロジーと特許法』(1994年))。特許法と著作権法(著作権制度は、著作物の創作者にその表現についての一定期間の排他的利用を内容とする財産権を与えることによって、創作にインセンティブを与える制度である。)によってコンピュータ・ソフトウェアにインセンティブを与える制度となっている。著作権法によってコンピュータ・ソフトウェア技術が保護されることとなったのは沿革的な理由によるものである(中山『コンピュータ・ソフトウェアの法的保護(新版)』9頁以下)。それは、アメリカ合衆国におけるコンピュータ・ソフトウェア技術の急速な発展に対する特許制度の対応の遅れとコンピュータ・ソフトウェア技術を著作権法によって保護することによって利益を得るコンピュータ関連事業者によるロビイ活動に起因すると思われる。

このような沿革によって、コンピュータ・ソフトウェア技術は特許法と著作権法によって保護されることとなったのであるが、現在では、著作権法によるコンピュータ・プログラムの保護はその沿革とはやや異なった意義を持つようになってきたと考えられる。運送技術・通信技術が発達した現在において、知的財産権の国際的な保護は欠かすことができないものとなっている。特に、マルチメディア・ネットワーク時代になって、コンピュータ・ソフトウェア技術の国際的な保護の重要性が増している。コンピュータ・プログラムは極めて容易に複製することができ、通信回線を通じて世界中へ頒布されることが可能であるため、模倣に対する保護手段としての著作権法が着目されるものとなった。WTOのTRIPS協定によって、コンピュータ・プログラムを著作権法で保護することが紛争解決手続の担保を持って規定された。これによって、コンピュータ・プログラムの製作者は、WTO協定の締約国であれば、登録を要すること無く保護を受けることができることとなった。これは、発展途上国におけるコンピュータ・プログラムの模倣に対して、有効な対策となるであろう。今後は、コンピュータ・ソフトウェアの技術思想を保護する特許法とコンピュータ・プログラムをその模倣から保護する著作権法という住み分けが期待されるであろう。

- (5) Ex Parte King, 146 USPQ 590
- (6) President Committee on the Patent System
- (7) Court of Customs and Patent Appeals (C.C.P.A.)
- (8) 162USPQ541、なお、この判決は、再審理後、別の理由により取り消されている(163 USQ 611 (1969))
- (9) 163 USPQ 611

- (10) 421 F.2d 742
- (11) 167 USPQ 280
- (12) 169 USPQ 99
- (13) 169 USPQ 548
- (14) 173 USPQ 430
- (15) 178 USPQ 35
- (16) 183 USPQ 172
- (17) 194 USPQ 465
- (18) 183 USPQ 172
- (18a) 191 USPQ 721
- (19) 191 USPQ 730
- (20) 193 USPQ 645
- (21) 195 USPQ 9
- (22) 197 USPQ 464
- (23) 197 USPQ 852
- (24) 435 U.S. 584
- (25) 特許商標庁と最高裁判所がコンピュータ・ソフトウェアを特許法の保護対象とすることに対する消極的姿勢を示している状況で、1978年に、CONTU (National Commission on New Technological Uses of Copyrighted Works) は、コンピュータ・プログラムを著作権法の保護対象に含める法改正を答申した(中山信弘「アメリカ著作権法とコンピュータ・プログラム」法学協会百周年記念論文集第3巻507頁)。1980年に、アメリカ合衆国は著作権法を改正し、コンピュータ・プログラムを著作権法の保護対象とした。
- (26) 200 USPQ 132
- (27) 200 USPQ 199
- (28) 202 USPQ 480
- (29) 203 USPQ 44
- (30) 206 USPQ 192 (1980)
- (31) 450 U.S. 175 (1981)
- (32) USPTO, Patentable Subject Matter Mathematical Algorithms and Computer Programs (1989)
- (33) Court of Appeals Federal Circuit (C.A.F.C.)
- (34) 29 U.S.P.Q. 2d 1845
- (35) 31 U.S.P.Q. 2d 1545
- (36) 32 U.S.P.Q. 2d 1031
- (37) 一方、コンピュータ・プログラムの模倣の防止を目的とする検討が行われた。1972年に、通商産業省重工業局ソフトウェア法的保護調査委員会は特別法によるコンピュータ・プログラムの保護を

提案し（通商産業省重工業局ソフトウェア法的保護調査委員会中間報告）、1973年に、文部省文化庁著作権審議会第二小委員会は著作権法によるコンピュータ・プログラムの保護を提案した（文部省文化庁著作権審議会第二小委員会）。1983年に、通商産業省産業構造審議会情報産業部会は、コンピュータ・プログラムを保護する特別法であるプログラム権法の立法を提案し（通商産業省産業構造審議会情報産業部会中間報告）、1984年に、文部省文化庁著作権審議会第六小委員会はコンピュータ・プログラムの著作権法による保護を提案した（文部省文化庁著作権審議会第六小委員会中間報告）。このような状況の中で、アメリカ合衆国政府が日本政府に対し、コンピュータ・プログラムを著作権法で保護することを強く主張したため、1985年に、コンピュータ・プログラムを著作権法の保護対象とする改正がなされた（中山信弘『ソフトウェアの法的保護（新版）』9頁以下）。

- (38) 1993年の「審査基準（改訂版）」については、それまでの審査実務をやや厳しい方向へと変更する意図を持つものであるか否かが議論になったが、結果的には、1989年のアメリカ合衆国のGuidelineのような大きなインパクトは与えなかったようである。
- (39) 中山注(37)161頁以下
- (40) N.Moskowitz, *The Metamorphosis of Software-Related Invention Patentability*, 3 *Computer Law Journal* 281 (1982)
- (41) 技術開発投資をする者は、契約によって投資の保護を図ろうとするであろう。そうすると、契約によって保護を図ることのできる専用ソフトウェアはともかくとして、市場に流通する汎用ソフトウェアに対する投資は契約によって十分な保護を得ることは難しいので、十分な投資が為されなくなるおそれがある。
- (42) 例えば、P. Samuelson, R. Davis, M. D. Kaor & J. H. Reichman, *A Manifesto Concerning the Legal Protection of Computer Program* 94 *Columbia Law Review* 2308（小泉直樹『アメリカ著作権制度—原理と政策』（1996年）93頁以下は、この論文を詳しく紹介している）、今野浩「技術者と法律家の対話」今野浩（中川淳司編『ソフトウェア／アルゴリズムの権利保護』179頁）、玉井哲雄「ソフトウェアの抽象化思想特性と特許」（同書50頁）など。なお、今野教授は、筆者の「他の技術分野とのバランスをとるためにも特許法による保護を行うべきであるとする」議論をソフトウェア技術の発展を損なってもなすべきであるかのごとく記述されている（今野前掲論文188頁）が、筆者は技術全体のバランスのとれた発展とコンピュータ・ソフトウェアの発展の為に特許法による保護をなすべきであるとしているのである。
- (43) この両者の考え方は混在している、妥当性についての疑問の背景には理念的なものが感じられる、例えば、今野前注(42)など。
- (44) P. Samuelson, *Benson Revisited: The Case against Patent Protection for Algorithms and Other Computer Program-Related Inventions*, 39 *Emory Law Journal* 1143 (1990)
- (45) 玉井前注(42)58頁
- (46) 今野前注(42)188頁
- (47) P. Samuelson, R. Davis, M. D. Kaor & J. H. Reichman, *supra* note (44)
- (48) 1960年代に、アメリカ合衆国特許商標庁がコンピュータ・ソフトウェア技術の保護に消極的な態

度を取った理由として、先行技術の調査が難しいことによる審査の困難さをあげている。

- (49) 現在でも、先行技術調査への懸念は存在する（ソフトウェア情報センター『ソフトウェア関連技術の保護の在り方の研究 報告書』（1996年）17頁）
- (50) 今野浩「カーマーカー特許への異議申立て」今野浩 中川淳司編前注(42)105頁など
- (51) 玉井前注(42)、今野前注(42)
- (52) P. Namuelson 中川淳司訳「ソフトウェア保護に対する新たな法体系の提案」今野浩（中川淳司編 前注(42)）
- (53) マルチメディア・ネットワーク時代のコンピュータ・ソフトウェアの保護のためには、世界中で保護の制度を確立する必要があり、このころが制度設計にあたっての一つの視点となる。新技術に対してそれぞれに対し特別法を作っていくことは、半導体集積回路配置のようにその主たる製造国がアメリカ合衆国と日本に集中していたという状況においてははともかく、世界的に拡散する技術については難しいものと思われる。このような *suigeneris* は、20年前であれば可能であったかもしれないが、コンピュータ・ソフトウェア技術が世界に広がった現在で不可能であろう。
- (53a) 問題となっているコンピュータ・プログラムが販売されている場合、インターネット上で利用可能である場合などは、専門家である当事者がそのプログラムの内容を知らなかったという主張は通りにくいであろう。
- (54) 産業政策では、現状の変更に伴って生じるおそれのある社会的費用にも注意が払われなければならない。
- (55) ソフトウェア情報センター『ソフトウェア関連技術の保護のあり方の研究 報告書』は、この検討作業の一部である。
- (56) その他に、特許による保護を有効なものとするためのクレームの多様性を認めること—具体的には、媒体クレームを認めること—が含まれている。
- (57) この解釈は柔軟な解釈で、将来、コンピュータ・プログラムそのものをクレームすることを認めたとしても、それは特許法の保護対象についての解釈を変えたのではなく、クレームの記載方法についての解釈を変えたということになり、将来に対して含みを持たせた解釈ということができるであろう。「プログラムを記録した媒体」について、「審査基準（改訂版）」で特許法の保護の対象とならないとした解釈をしていたのを、わずか3年で変更しなければならなくなった轍を踏まないという趣旨であり、審査基準の在り方としては隠当なものと思われる。
- (58) コンピュータ・プログラムを記録した記録媒体についても、コンピュータ・プログラムの技術的性格を認め、そのコンピュータ・プログラムが記録媒体に記録されることによって、「もの」としての性格を有するとともに、コンピュータでそのまま利用できるものとなることから、技術的性格を有する「もの」として特許の保護の対象に含まれるとする解釈になっている。また、特定のデータ構造（データ・ストラクチャー）を有する媒体のクレームを認められるとしている。
- (59) もっとも、「運用指針」では、解決手段が、「ハードウェア資源に対する制御又は制御に伴う処理」、「対象の物理的性質又は技術的性質に基づく情報処理」、「ハードウェア資源を用いた処理」である場合には、「自然法則を利用」しているとしている。この解釈によれば、ハードウェア資源と

関連させることにより、コンピュータ・ソフトウェア技術は特許法の保護の対象に含まれることとしている。これには、従来の考え方も踏襲する趣旨（大きな変更ではないとする趣旨）を示そうとする意図が窺える。

(60) 447 U.S. 303

(61) Diamond v. Diehr 事件の判決では、Gottschalk v. Benson 事件の判決、Parker v. Flook 事件の最高裁判所の判決を変更しなかったけれども、Diamond v. Chakrabarty の判決と同じ基本的な考え方を適用すべきものとした考えることが適当であろう。アメリカ合衆国では、イギリスほどの先例拘束性の原理はとられていないが、明示的な判例変更の例は多くない。したがって、実質的には判例変更が為されたと見るべきであろう。

(62) 179 USPQ 464

(63) 214 USPQ 902

(64) 29 U.S.P.Q. 2d 1845

(65) 31 U.S.P.Q. 2d 1545

(66) 32 U.S.P.Q. 2d 1031

(67) 認められるクレームについては、①非機能的で記述的なもの (non-functional descriptive material) は認められないが、機能的な記述的なもの (functional descriptive material) は、記録媒体に記録されている場合には認められる。②数 (number)、抽象的な概念 (abstract concepts or ideas)、それらを表現する信号 (representing signals) だけを扱う方法クレームは、認められないとしている。このような方法は応用されることによって、特許の保護の対象となるとしている (このガイドラインの体裁は、これまでのガイドラインが裁判所を整理する体裁を有するものであったのに対し、コンピュータ・ソフトウェアの発明として特許法によって保護される物あるいは方法を特定するクレームとして認められるべきものを明らかにしようとするものである)。すなわち、このガイドラインは、これまでの裁判例を踏まえつつ、プログラムの記述的性格を認めつつ、その技術的性格をも認めることによって、記述的な性格を持つコンピュータ・プログラムが記録媒体に記録されることによって、コンピュータによって処理されるものになるところからより記述的な性格が薄くなり、機能的な性格が強調され、特許の保護対象となるというように読むことができるであろう。

(68) 特許商標庁が旧来の判決例を引用したのは、特許商標庁の運用を正当化するためであったとみるべきであろう。

(69) この両者は密接に関連している。抽象的な思想 (idea) を保護すべきでないという考え方は、抽象的な思想を保護の範囲に含むようなクレームを否定することを意味する。

(70) 先行技術を保護の対象に含むクレームが認められないことはもちろんであるが、これは何を保護すべきかという政策的な判断という問題ではなく、新技術を保護するという特許制度の性格に基づくものである。

(71) MANUAL OF PATENT EXAMINING PROCEDURE, Rev. 8 Oct, 1981, 538. 3

(72) この規定によって、ヨーロッパ特許庁はコンピュータ・プログラムそのものを特定するクレーム

する特許を認めていない。

- (73) その他の技術でも、効果的な保護のためのクレームを認めている。用途に技術的特徴のある治療薬という「物」のクレームが認められているのはその一例である。
- (74) しかしながら、このコンピュータ・プログラムを記録した媒体のクレームで、コンピュータ・ソフトウェア技術の特許権者に十分な保護を与えることになるかについては、疑問が残っている。一つは、マルチメディア・ネットワーク時代におけるコンピュータ・プログラムの通信による輸入・販売に対して、どのように対処するかという問題である。もう一つは、媒体クレームを認めたとしても、そのクレームがコンピュータ・ソフトウェア技術の変化に付いていけるかという問題である。
- コンピュータ技術、コンピュータ・ソフトウェア技術は、間断なく進歩を続けている。特許法はこのような技術進歩に合わせて、新たな技術の開発者を保護していかなければならない。したがって、今回の新たな運用指針は新しい時代へ第一歩を示すものではあるけれども、来るべき技術変化に対応して、絶えず見直しを図っていかなければならないであろう。
- (75) 特許庁審査第二部調整課審査基準室「『産業上利用することができる発明』の審査の運用指針』の適用について」(平成9年1月)、特許庁「『特定技術分野の運用指針 第1章 コンピュータ・ソフトウェア関連発明』の適用について」(平成9年2月)
- (76) 「[請求項3] 車両の運行状態を示す予め定められたデジタル運行データが記録されるデジタル運行データ記録領域を有する記録媒体においては、初期化が誰によって行なわれたかを識別する初期化識別情報と、前記デジタル運行データ記録領域の一部分をデジタル運行データ以外のオプション領域として指定するオプション領域指定情報とが記録される共通データ記録領域を有する。
- (77) 特公平5-64672、なお、この特許に対しては、反対の考え方もある(今野浩「カーマーカー特許への異議申立て」(今野浩 中川淳司編「ソフトウェア/アルゴリズムの権利保護」105頁)
- (78) USP4744028
- (79) D. S. Chisum, The Patentability of Algorithms, 47 University of Pittsburgh Law Review 985 (1987)
- (80) なお、特定のアルゴリズムを含まないクレームは包括的にアルゴリズムをクレームしていることになるので、クレームの広狭はアルゴリズムの視点だけから議論されるべきものではないと思われる。
- (81) ビジネスシステムに関する特許例として、医療事務システム(特公昭58-43779号)、財務在庫等の管理のための装置(特公平1-23814)、鏡りの電源機処理装置(特公平3-25812)など、ゲームの例として、ゲーム装置(特公昭56-31990)などがある。
- (82) ビジネスシステムに関する特許例として、Securities Brokerage-Cash Management System (USP 4346442), Self-Implementing Pension Benefits System (USP 4969094) などがある。
- (83) 中山信弘『工業所有権法(上)』
- (84) 共同体特許条約第30条は、特許の効力は、特許の対象となっている発明の実施のために使用される本質的な要素(essential element)に関する手段(means)を、第三者がその手段が発明の実施(putting...into effect)に適し、発明の実施を目的とすることを知って(知っていることが明白

である場合を含む)、発明を実施する権利を有する者以外の者に供給することあるいは供給を申し出ること (supplying or offering) に及ぶとしている。発明を個人的非営利目的で実施する者、実験目的のために実施する者、調剤行為を行なう者に対する供給には特許の効力が及ぶものとしている。ただし、その手段がありふれた商品 (staple commercial product) である場合には、第三者が供給された者に直接侵害をすることを誘導する (induce) 場合を除いては適用しないとしている。

アメリカ合衆国の特許法第271条(b)は、特許の効力は、特許の侵害を誘導することにも及ぶものとしている (誘導侵害 (Inducing infringement))。第271条(c)は、特許の対象である発明の本質的な部分であり、特許された物あるいは特許された方法を実施するために使用される物を、特許を侵害しないで使用されることが適当でないことを知っている販売に及ぶとしている (寄与侵害 (Contributory Infringement))。

- (85) 財務在庫等の管理のための装置 (特公平1-23814)、競りの電算機処理装置 (特公平3-25812) など。
- (86) 医療事務システム (特公昭58-43779号) など。
- (87) この「運用指針」以前にも、「媒体」クレームを含む特許が広告されている。
- (88) 具体的な法の解釈としては、海外でなされた行為もネットワークで繋がれている以上、国内でなされた行為として特許権の効力を及ぼすこと、海外でなされた行為が間接侵害 (inducement) となることなどが考えられる。
- (89) 39 USPQ 2d 1746
- (90) 金融システムに関する特許に関しては、斎藤治 森田泰子 加藤壮太郎「金融業務における特許権の正否—特許法の保護対象について」金融研究14巻2号99頁 (1995年)
- (91) 金融システムに関する特許として、「オンライン会計システムを有する発行銀行と、前記発行銀行の流動負債として前記オンライン会計システムにおいて貸し越される通貨の電子的象徴と、前記通貨の電子的象徴を発生するために前記銀行に関連装備された金銭発生モジュールと、前記通貨の電子的象徴をストアするとともに、前記通貨の電子的象徴を含む銀行取引を中継することができるように前記発行銀行に関連装備された出納モジュールと、前記通貨の電子的象徴をストアし、前記発行銀行とオンライン取引を行い、さらに、前記通貨の電子的象徴をオンライン取引において他の取引モジュールとの間で交換することができる取引モジュールを備え、前記通貨の電子的象徴の各々が前記金銭発生モジュールにより生成された初期の貨幣的価値を含むものであり、前記出納モジュール及び取引モジュールが前記通貨の電子的象徴の一つの振込先モジュールに移転する振出元モジュールとして機能するときにおいて、移転された貨幣的価値を有する移転レコードを発生し、かつ前記移転された通貨の電子的象徴に置いて前記移転レコードを含むことができるプロセッサを有するものであることを特徴とする電子通貨システム」というクレームを持つ特許などが認められている。(特公平7-111723)
- (92) Hotel Security Checking Co. v. Lorraine Co., 16 F. 467 (2d Cir. 1908)
- (93) In re Johnston, 1883 USPQQ 172 (C.C.P.A. 1974)
- (94) Pain, Webber v. Merrill Lynch, 218 USPQ 2d 212

- (95) Securities Brokerage-Cash Management System (USP 4346442)、Self-Implementing Pension Benefits System (USP 4969094) など
- (96) In re Schrader, 30 USPQ 2d 1455
- (97) 最判昭和28年4月30日民集7巻4号461頁
- (98) DES (Data Encryption Standard) に関連する特許として、「入力されたデータを1 ( $1$ は正数) ビット毎に分割してそれぞれ  $m$  ( $m$ は正数) バイト内に配置し、次に前記1ビットの各々についてそれぞれ  $n$  ( $n$ は正数) ビットへの拡大処理あるいは縮約処理を行って  $m$  バイト内に配置し、次に前記  $n$  ビットの各々についてそれぞれ1ビットへの縮約処理あるいは拡大処理を行って  $m$  バイト内に配置することから成る処理を複数回繰り返すことを特徴とするデータ変換方法」というクレームを持つ特許が認められている。

ヨーロッパにおける  
租税情報の国際的な交換

中 里 実

# 目 次

はじめに

## I 異なる二つの対応

- 1 スイスにおける消極的対応
- 2 アメリカにおける積極的対応
- 3 世界の趨勢

## II ドイツ

- 1 総 説
- 2 納税者等の協力義務
- 3 国際的情報交換——総説
- 4 ドイツ租税行政庁による、外国への情報提供
  - (1) 概 観
  - (2) 相手国の情報要求に対して情報提出義務のある場合  
——EG Amtshilfegesetz に基づく場合
  - (3) 相手国の情報要求に対して情報提出義務のある場合  
——租税条約に基づく場合
  - (4) 相手国の情報要求に対して情報提出義務のない場合  
——租税通則法117条3項による場合
  - (5) 国内法上の調査権の根拠

## III イギリス

- 1 調査権限一般
- 2 情報交換

## IV フランス

- 1 情報交換の国内法上の根拠
- 2 情報交換に関する条約上の定め

## V 日本に関する若干の検討

- 1 日本の状況
- 2 改革の方向

## はじめに

本稿は、租税条約に基づく情報交換と、国内法に基づく租税行政庁の調査・情報収集権（日本でいえば、質問検査権）との関係について、ヨーロッパ諸国、特に、ドイツ、イギリス、および、フランスの状況を概観し、日本との比較の参考に供しようとするものである。

この問題は、つまるところ、これらの各国の国内法において、調査対象者（すなわち、納税者）に対する、あるいは、その他の第三者に対する課税処分の前提としての調査・情報収集以外の、調査・情報収集のための権限が認められているか否かという問題である。換言すれば、外国における外国課税当局による課税処分のために、自国において調査・情報収集を行うことが、その国の国内法上可能か（あるいは、要求されているか）という問題である。

租税条約における情報交換に関する規定は、国際法レベルにおける締約国の義務に関するものであるから、それについての議論においては、基本的に、各国の国内法における調査・情報収集権限に関する議論が行われることは必ずしも多くはない。しかし、調査・情報収集が基本的には国内法に基づいて行われる以上、国内法に関する議論を無視するわけにはいかない。したがって、この問題について検討を行うためには、とりもなおさず、各国の国内法上認められた調査・情報収集権限の法的範囲について調べ、かつ、各国における租税条約と国内法との関連性についても正確に理解することが必要となる。

もちろん、本稿におけるようなテーマに関して、一人の人間が短期間の間にいくつもの国の状況について調査を行うことには、自ずから限界がある。にもかかわらず、本稿においては、そのような困難を自覚しつつも、調査しうる範囲の全資料をもとに、できるだけ正確に各国の状況について概観したいと考えている。

以下においては、まず、外国から情報提供の依頼を受けた場合に、ある国家がいかなる対応を行うかという点について、これに積極的なアメリカと、消極的なスイスとを比較することによって、世界の趨勢についておおまかに述べておく（I）。そして、しかる後に、本稿の直接の対象国であるドイツ（II）、イギリス（III）、および、フランス（IV）について、概観を示す。その上で、日本の質問検査権の抱える問題点と、今後の改革の方向につ

いて若干の検討を行うこととしたい (V)。

なお、ドイツも、イギリスも、フランスも、皆、ヨーロッパ共同体の加盟国であるから、EC法(ないし、EU法)が重要な意味をもたらしてくるので、それに関する叙述が、当然のことながら重複することになる。そこで、本稿においては、この点に関する叙述は、ドイツに関する箇所においてまとめて行うこととする。

## I 異なる二つの対応

外国から、租税条約等にもとづいて、租税事項に関する情報提供の依頼があった場合の対応は、国によりかなり異なる。これについてもっとも積極的なのがアメリカ、また、これについてもっとも消極的なのがスイスであると思われる。そこで、ここでは、イントロダクション的な意味合いで、この二つの国を比較したうえで、ドイツ、イギリス、フランスの三国が、両者の間のどのような位置づけになるのかという点について、簡単に整理しておくこととする。

### 1 スイスにおける消極的対応

スイスは、承知のように、特に銀行秘密の保護に熱心であり、その帰結として、国際的な情報交換にもっとも不熱心な国である。この点について、スイスのある論者は次のように述べている。

「スイスは、以前から、租税法上の行政協力の領域において、最も抑制的な態度をとってきた。1950年代になってはじめて、租税条約の中に行政協力の条項が設けられた〔これは、すなわち、スイスのアメリカとの条約、フランスとの条約、イギリスとの条約においてである〕が、そのような条項の採用は、当該領域におけるスイスの条約政策の転換を意味するものではなかった。このように抑制的な態度は、租税事項において司法的協力の供与を確固として拒否する態度と組合わさって、海外における〔スイスに対する〕批判の増大を引き起こしている。なぜなら、このような態度とは対照的に、諸外国や国際機関は、ますます、租税事項においてすでに存在する協調関係を拡大しようと希望しているからである。」<sup>(1)</sup>

このように、租税上の国際的な行政的・司法的協力に関するスイスの態度は、従来、租税事項に関して一定の条件の下に司法共助の供与を定める1973年5月25日のアメリカとの間の刑事事件に関する司法共助条約を除けば、きわめて消極的なものであった。このような傾向の転換点となったのは、1981年3月20日の、刑事事項に関する国際的司法共助に関する連邦法の制定である(2)。

現在、租税に関する国際的な行政協力の分野において、スイスは、租税条約締結国に対して、一定の限定された協力を行っている。そして、租税条約は、当該条約が情報交換に関する定めをおいているか否かにかかわらず(たとえば、日本との間の租税条約には、この点に関する定めがない)、相手国に対して情報を提供する一定の義務を当然に内包するものであるというのが、スイスの立場である。ただし、スイスは、租税条約上の情報提供の義務をかなり限定的にとらえ、それは、もっぱら、租税条約の適正な執行と、脱税等の防止に必要な情報についてのみ及ぶという立場をとっている。したがって、営業上の秘密、銀行秘密、職業上の秘密等々に係わる情報の提供は、認められない。このようなスイスの立場は、行政協力に関する条項を含む租税条約や、OECDモデル租税条約におけるスイスの留保において明確に表明されている。たとえば、現在のOECDモデル租税条約は、租税条約の適正な執行と、脱税等の防止に必要な情報についての交換を超えて、広く締約国の国内法の実施に必要な情報の交換をも定めているが、スイスは、これに対して留保をおいている。すなわち、スイスの立場によれば、租税条約の適正な執行と、脱税等の防止に必要な情報は、当然に、相互協議条項等に基づいて交換されるのであり、その意味で、租税条約における情報交換条項は、単に確認的な規定にしかすぎないということになる(3)。

スイスは、現在までのところ、アメリカ、フランス、イギリス、ドイツ、デンマーク、オーストリア、カナダ、イタリア、ベルギー、オーストラリア、オランダとの間の租税条約においてのみ、情報交換に関する条項をおいている〔ただし、日本との間の租税条約にはなし〕が、対米条約の場合を除けば、条約の適正な執行に必要な情報についてのみの情報交換を定めているだけである。しかし、前述のように、このような情報は、明文の条約上の規定が存在しなくともスイスにより提供されるので、そのような条項は、確認規定にすぎないとされている(4)。

これに対して、対米租税条約には、アメリカのこの点に関する積極的な態度を反映して

か、より包括的な情報交換条項が含まれている。すなわち、その16条によれば、条約の適正な執行に必要な情報のみならず、詐欺等の防止に必要な情報も交換の対象とされているのである。スイスの連邦最高裁判所は、その二つの基本的な判決において、この条項の意義等について判示している（BGE 96 I 737, 101 Ib 160）<sup>(5)</sup>。すなわち、そこで確定されたのは、租税条約に基づく、詐欺等の防止のためのアメリカ課税当局に対する情報の提供に際して、必要に応じて、銀行調査も行われうるのであり、銀行秘密は、そのような調査やその調査に基づく情報提供と対立するものでない、という点であった。ただし、もちろん、16条の規定は、情報提供の依頼を受けた国の国内法上、入手可能な情報のみを対象とするものであり、特別な措置をとること（証言をとったり、文書を作成したり）までを対象とはしていない<sup>(6)</sup>。そのような措置は、より包括的な共助義務の下ではじめて行われる<sup>(7)</sup>。

スイスは、租税条約の適正な執行と脱税等の防止に必要な情報については、特別な規定がない場合でも提供するのが、租税条約上の義務であると考えている。情報提供に関する定めのないスウェーデンとの租税条約に関する判決において、スイスの連邦最高裁判所は、このような実務上の扱いを確認した上で、次のように述べた。すなわち、条約の相互協議条項は、また、条約の適正な執行と脱税等の防止に必要な情報を提供するという目的にも奉仕しうるものであり、その場合、租税秘密〔の保護の要請〕は、情報の提供を妨げはしない<sup>(8)</sup>と述べた<sup>(9)</sup>。

国際的な情報交換における関係者の法的地位については、基本的に、1968年12月20日の行政手続法に定められている。のみならず、租税条約に関する様々な施行命令も、また、情報の交換の際に従うべき手続きや、関係者の法的地位に関して定めている。それは、スイス連邦の課税当局が外国の課税当局に対して情報を提供する前に、関係者に対して、情報の提供についての態度を決定するための機会と、外国への情報提供をやめさせるための意思表示を行う機会を与えようというものである。課税当局が、関係者により持ち出された根拠は、外国への資料提出を拒否するのに十分ではないという結論に達するか、あるいは、関係者が外国からの情報要求について意見を述べることを怠ると、スイス課税当局は、そのための処分を行うが、この処分に対しては、スイス連邦裁判所に対して行政訴訟を提起することが認められている。そして、スイス課税当局の原処分が法的効力を有するとされる場合に、はじめて、外国の課税当局が要求する資料の提出が行われる<sup>(10)</sup>。

なお、以上のような、租税条約に基づく通常の情報交換のほかに、スイスにおいては、源泉所得税の外国税額控除のための情報交換、相互協議にもとづく情報交換、条約漁りに対抗するための情報交換等が存在する(11)。

〔注〕

- (1) Daniel Lüthi, Informationsaustausch im internationalen Steuerrecht der Schweiz, in Ernst Höhn (hrsg.), Handbuch des internationalen Steuerrechts der Schweiz, S. 478(1984). なお、以下におけるスイスに関する記述は、ほとんどすべてが、この書物の該当箇所の要約か翻訳であるという点をおことわりしておく。したがって、煩瑣になることを避けるために、引用頁数は、まとめて段落ごとにしめしておくこととする。
- (2) Lüthi, supra Fn 1, S. 483.
- (3) Lüthi, supra Fn 1, S. 483-S. 484.
- (4) Lüthi, supra Fn 1, S. 484.
- (5) もっとも、BGE 101 Ib 160 においては、租税条約の要求しているのは司法共助ではなく情報交換であるから、租税条約に基づいて提供される情報が、アメリカにおける司法手続で利用可能な形式である必要性はないとされた。
- (6) OECD の1963年モデルにおける立場と同様であろう。
- (7) Lüthi, supra Fn 1, S. 485.
- (8) BGE 96 I 733.
- (9) Lüthi, supra Fn 1, S. 485.
- (10) Lüthi, supra Fn 1, S. 486.
- (11) Lüthi, supra Fn 1, S. 486-S. 488.

## 2 アメリカにおける積極的対応

スイスが各国と結んでいる情報租税とは逆に、きわめて幅広い情報交換が定められているのが、アメリカとカナダの間の1980年の租税条約である(12)。この条約には、(スイスとは対照的な)アメリカの情報交換についての積極的な姿勢が明確に表現されている。

すなわち、この租税条約に基づいて情報提供の要求がなされた場合、要求を受けた側は、要求をなした国の国内租税法自体が関連していたとするならば当該(要求をなした)国家が入手可能であるのと同じ程度において、情報入手し、要求された形式で提供しなければならない(同条約27条(2))。この条項は、OECDモデル租税条約にはみられないが、この点について、アメリカの連邦上院の Committee on Foreign Relations は、次の

ように述べている(13)。

「その意味するところは、要求を受けた国は、自らの目的のためには必要のない情報であっても、subpoenaの権限や、summonsの権限や、あるいは、相手国により要求された情報を収集するための国内法上のその他の権利、を用いなければならないということである。要求を行っている国が、自らの法律の下で行使できないような権限であっても、要求を受けた国は行使しなければならないことが意図されている。したがって、当該規定が厳密な意味で相互主義的であることが意図されているわけではない」

特に、要求を受けた国は、自らの国における目的のためには必ずしも必要のない情報であっても、それを入手し、相手国に対して提供しなければならないとされている点が重要である。これは、この問題に関するアメリカにおける著名な判決である、United States v. A.L. Burbank & Co., Ltd., 525 F.2d 9(2d Cir. 1975), cert. denied, 96 S. Ct. 2647(1976)判決において示された考え方を、租税条約上取り入れたものである。

もちろん、租税条約に基づく情報交換は、大きく国内法に依存している。すなわち、国内法上入手不可能な情報を提供することはできないのである。したがって、一方の国が租税条約にもとづいて提供すべき情報は、その国の租税法律の通常の執行の過程において入手可能なものである。

(注)

(12) William Innes and Janice McCart, Transfer-Pricing Disputes: Access to and Disclosure of Information, 43 Canadian Tax Journal 821, 852-859(1995). なお、アメリカに関する叙述は、もっぱら、この論文にもとづくものである点を、ここに明らかにしておく。

(13) Report of the Senate Committee on Foreign Relations Accompanying the 1980 U.S.-Canada Income Tax Treaty and 1983 and 1984 Protocols, Exec. Rep. no. 98-22, 98th Cong., 2d sess.(1984).

### 3 世界の趨勢

ここでは、II以下における叙述の鳥瞰図を得るために、スイスとアメリカ以外の国の状況について、その傾向を、スイス・アメリカとの比較において、ごく簡単に整理しておくこととする(14)。

国際的な司法共助に関する条約が租税行政庁により用いられることは、實際上ほとんど

ない。これは、おそらく、租税行政庁が情報を必要とするのが、司法手続に移行するよりもはるかに以前の段階だからであろう（あるいは、一種の国際的な縦割り行政のために、租税条約が課税・財政当局により、他の分野の条約とは独立に発展させられてきたことも、その一因なのかもしれない）。いずれにせよ、この意味で、租税条約にもとづく情報交換の果たす役割は大きい。

国際的な情報交換においては、国により、提供できる情報の内容と形式に差が生ずる。このような差異は、主として、情報収集に関する各国の国内法（日本でいえば、質問検査権に関する定め）の差異から生ずる。その結果、上述のように、スイスは、租税条約にもとづく情報交換について、きわめて制限的な立場をとっており、OECDモデル租税条約26条に対しても留保をおいている。

これに対して、合衆国は、スイスの対極に位置し、租税条約の情報交換条項の目的との関連において、ある国の租税行政庁の権限が、自国の租税の執行に関してのみならず、条約相手国の租税の執行のためにも用いられるべきであるとして、情報交換について、これをきわめて広く認める立場をとっている。その結果、合衆国は、第一に、租税条約に定める租税のみならず、すべての租税に関して、情報交換を行おうとする（1981年のアメリカモデル租税条約26条(6)）。また、第二に、合衆国は、情報提供の要求を受けた国は、自らの課税のまったく関係のない場合であっても、情報提供により課税されることになる租税が自国のものであるかのように、自らの執行権限を完全に利用する義務を負う、という立場をとっている(15)。

この点について、ある書物は、次のように述べている(16)。

「合衆国の裁判所は、内国歳入庁が、それに対して認められている通常の権限を用いて、租税条約に基づく要求に応じて情報を入手することを認め、また、合衆国外の情報収集を行うことさえ認めた。……(U.S. v. Bache, Halsey, Stuard, 563 F. Supp. 898(1982))。さらに、当該権限の国内問題に関する使用が、他の理由で認められないような場合においても、外国の要求に応じて権限を行使できるとした。……(U.S. v. Stuart et al., 489 U.S. 353(1989))。』

しかし、これに対して、アメリカ以外の国は、必ずしも、これほど積極的ではない(17)。特に、イギリスの国税庁(Inland Revenue)の立場はかなり消極的なもので、これが情報提供できるのはすでに保有している情報のみであって、外国により要求された情報

の収集がイギリスの課税の根拠となる可能性を十分に示している場合でなければ、外国の課税当局のために調査を行うことはできないというものである。これは、現在の日本の立場とかなり類似したものである。そして、これは、シティーの金融センターとしての地位が脅かされることを危惧した結果であるとの考え方も存在する。1972年のECの行政協力に関するディレクティブができるときも、イギリスの対応は、きわめて消極的なものであった。

もっとも、イギリスも、結局は、Finance Act 1990の125条により、やっと、EC加盟国の租税に関しては、調査官に対して国内法上認められたすべての権限を行使することが認められ、現在にいたっている。しかし、これは、あくまでもEC加盟国との関係のみにおいてのことである。なお、Income and Corporation Taxes Act 1988の788条(2)は、条約相手国の法律を執行するために必要な情報交換に関する規定を含む条約の定めに対応するための法的権限を定めているが、イギリスの租税とまったく関係のない場合にまで、外国のために情報収集を行う権限までそこに含まれているかは、明らかではない。しかし、實際上、多くの場合において要求されるのは、国税庁の手元にすでに存在する情報であろう。

(注)

(14) この部分は、ほとんどが、Sol Picciotto, *International Business Taxation*, 272-282(1992)の叙述の紹介である。

(15) *U.S. v. A.L. Burbank & Co.*, 525 F. 2d 9(1975)は、OECDモデル租税条約が、内国歳入庁のサモンズの権限の行使を、合衆国の課税が関係なく、相手国がその国内法上そこまでの調査を行うことができないような場合においても、認めるものであると解した。裁判所は、その際に、"types of administrative measures authorised for the purpose of the requested state's tax must be utilised, even though invoked solely to provide information to the other contracting state"と述べるOECDモデル租税条約のコンメンタリーに言及した。アメリカのモデル租税条約は、このような広い権限行使を行うことができる点を明確にしている。また、この点に関連して、Philip Baker, *Double Taxation Conventions and International Tax Law, A Manual on the OECD Model Tax Convention on Income and on Capital of 1992*, 441-442(2nd ed. 1994)を参照のこと。

(16) Picciotto, *supra* note (14), at 275-276.

(17) Picciotto, *supra* note (14), at 276-277.

## II ドイツ

ドイツにおける、国際的な情報交換に関する状況を正確に理解するためには、ドイツ行政庁による国際課税に関する情報収集権限と、情報交換の二つに分けて議論することが必要である(18)。

(注)

(18) Vgl. Harald Schaumburg, Internationales Steuerrecht, § 19, 1993; Volker Kluge, Das deutsche Internationales Steuerrecht, 3., völlig überarb. Aufl., §34, 1992; Günter Dreßler, Gewinn- und Vermögensverlagerungen in Niedrigsteuerränder und ihre steuerliche Überprüfung, 2., wesentlich erweiterte Auflage, III, 1995; Marion Farnschläder, Internationale Steuerauskunft, in Michael Maßbaum, Dir Meyer-Scharenberg und Helmut Perlet (hrsg.), Die deutsch Unternehmensbesteuerung im europäischen Binnenmarkt, Besteuerungsgrundlagen und grenzüberschreitende Steuerplanung in Deutschland, S. 1043 ff., 1994; Kurt Michler, Sachverhaltsgestaltungen mit Auslandsberührung in der Verfahrenspraxis, in Wilhelm Haarmann (hrsg.), Grenzen der Gestaltung im Internationalen Steuerrecht, Mißbrauchsverhütung in der Diskussion: EU-Recht · DBA · Hinzurechnungsfinanzierung · Verrechnungspreise · Verfahrenspraxis, S. 5 ff., 1994; Klaus Tipke und Heinrich Wilhelm Kruse (hrsg.), Abgabenordnung, Finanzgerichtsordnung, Kommentar zur AO 1977 und FGO (ohne Steuerstrafrecht), 15. Aufl., § 117. なお、以下の叙述は、主に、Schaumburg, a.a.O.の記述を翻訳し、要約したものにすぎないという点に留意されたい。

### 1 総説(19)

ドイツ租税通則法88条1項によれば、租税行政庁(Finanzbehörde)は、納税義務の成立等に関する事実関係に関して、職権で調査しなければならないが、このことは、国際課税の領域についても同様である。そして、この職権による事実解明義務(Sachaufklärungspflicht)と対応するのが、租税通則法90条に基づく関係者の協力義務(Mitwirkungspflicht)である。

この事実解明義務を果たすことを可能にするために、租税行政庁には、法の制限の下に、様々な手段が認められている。このような制限には、他国の領域で調査活動を行うこ

とはできないという国際法上の制限も含まれる。そこで、国際課税の領域においては、関係者の協力義務が強化されることになる。

〔注〕

(19) Schaumburg, a.a.O. Fn. 18, S. 837-839.

## 2 納税者等の協力義務

この問題は、それ自体が、日本の状況との比較において興味深いものであるが、ここでは、以下における議論の前提として必要な範囲で、納税者等の協力義務について、その概要を示しておく。

### (1) 一般的協力義務

租税通則法88条1項の職権による調査義務 (Sachaufklärungspflicht) をみたすために、租税行政庁は、租税通則法90条にしたがって納税義務者あるいはその他の関係者に対して課された協力義務 (Mitwirkungspflicht) を利用する。租税通則法90条1項が、一般的な協力義務を定めている。

協力義務がみたされない場合は、行政庁の事実解明義務が解除され、推計が可能となる (租税通則法162条)。

### (2) 国際課税における協力義務の強化

国際法上の制限により、租税行政庁は、他国の領域内において調査を行うことはできない (それは、重大な国際法違反となる) ところから、租税通則法90条2項は、関係者の協力義務を強化している。

また、対外関係課税法 (Außensteuergesetz) の17条1項は、協力義務の強化を定めた租税通則法90条2項の特則であり、特に、タックス・ヘイヴン対策税制を念頭においた特別な定めである。

### (3) 特別な協力義務

租税通則法90条1項の一般的協力義務を具体化した、国内課税問題にも国際課税問題にも適用される各論的定めとしては、租税通則法93条から100条にかけて、第三者の情報提供義務 (93条)、宣誓による尋問 (94条)、宣誓にかわる保証 (95条)、等々が定められている。

また、国際課税問題に関しては、いくつかの特別な定めも存在する。すなわち、租税通則法123条（ドイツ国内に住所も居所も本社住所も管理支配の場所もない関係者は代理人を指名すべきことを定める）、138条2項（無制限納税義務者が租税行政庁に対して国外事業等に関して要求なしに報告すべき義務を定める）、146条2項（国外事業所に関する会計帳簿を国内で作成し、租税行政庁がいつでも見られる状態にしておくことを定める。なお、さもないと、そのような支払について控除・損金算入が認められない。この点については、さらに、対外関係課税法16条により強化されている）等がそれである。しかし、ここでは、これらについて、これ以上詳しくはふれない。

〔注〕

(20) Schaumburg, a.a.O. Fn. 18, S. 839-849.

### 3 国際的情報交換——総説<sup>(21)</sup>

以上のような、租税行政庁の事実解明義務（Sachaufklärungspflicht）と関係者の協力義務（Mitwirkungspflicht）は、かなり広範なものである。しかし、たとえそれが国際的な取引に関するものであるとしても、それは、あくまでも、ドイツ国内における義務にすぎない。しかし、国際取引に対して適正な課税を行うためには、このような国内に限定された調査等には、やはり限界がある。そこで、重要な意味を有することになるのが、国際的な情報交換（Internationaler Informationsaustausch）<sup>(22)</sup>を通じた海外における情報の収集である。

ドイツにおける、国際的な情報交換の法的根拠としては、次のようなものがあげられている。

#### ・ EG Amtshilfegesetz

EG Amtshilfegesetz（EC 行政共助法）は、2つのECの指令（EG-Richtlinien 77/799/EWG vom 19. 12. 1977 と 79/1070/EWG vom 6. 12. 1979）を国内法化したものである。これは、EC 諸国間の所得税、資産税、付加価値税に関する情報交換を定めるものである。EC 指令を国内法化したものであるから、これによる情報交換は国際法的に義務的なものである。その1条3項は、他の根拠による情報交換との競合が存在する場合、それを認めているので、ドイツの租税行政庁は、この法律の2条1項の定める義務を超えて、

租税通則法を117条3項に基づく自発的な情報提供を行うことができる。なお、この法律の実際の運用は、大蔵省の覚書（Merkblatt zur zwischenstaatlichen Amtshilfe durch Auskunftsaustausch in Steuersachen）<sup>(23)</sup>に基づいて行われているので、この法律の理解のためには、その覚書を参照することが必須となる。

#### ・ Amtshilfe-Verordnung der EG

これは、EC 諸国間の付加価値税に関する情報交換を定めている。これによる情報交換も国際法的に義務的なものである。しかし、他の根拠による情報交換との競合が存在する場合、それを認める。

#### ・ 租税条約における情報交換条項

租税条約締結相手国との情報交換を定める。これによる情報交換も国際法的に義務的である。租税条約も、他の根拠による情報交換との競合が存在する場合、それを認めている（否定していない）。租税条約が、単に、租税条約の適正な執行に関する情報交換のみを認めているにすぎない場合も、同様である。したがって、条約上の義務を超えて、ドイツ租税行政庁は、租税通則法117条3項に基づく自発的な情報提供を行うことができる。実際の運用は、大蔵省の覚書（Merkblatt zur zwischenstaatlichen Amtshilfe durch Auskunftsaustausch in Steuersachen）に基づいて行われている。

#### ・ 租税事項における行政協力を定めた特別な条約

これは、行政協力条約締結相手国との情報交換を定める。これによる情報交換も国際法的に義務的である。実際の運用は、大蔵省の覚書（Merkblatt zur zwischenstaatlichen Amtshilfe durch Auskunftsaustausch in Steuersachen）に基づいて行われている。

#### ・ 租税通則法117条

これは、国内法に基づく自発的な情報提供等について定めている。これによる情報提供は義務的ではない。実際の運用は、大蔵省の覚書（Merkblatt zur zwischenstaatlichen Amtshilfe durch Auskunftsaustausch in Steuersachen）に基づいて行われている。

これらの法的根拠は、必ずしも、相互に適用を排除しあうものではなく、したがって、重なりあって適用されることがある。もっとも、それぞれの根拠の射程範囲は異なる。このような、国際的な情報交換の法的根拠が重なりあった場合、すなわち、具体的には、ドイツの租税行政庁が、（EG Amtshilfegesetz, Amtshilfe-Verordnung der EG、租税条約、租税事項における行政協力を定めた特別な条約、上の義務をはたす際に、それをこえて）

租税通則法117条3項にもとづいて外国に対して情報提供を行った場合、納税者にとってもっとも有利な保護が優先される。具体的には、租税通則法117条3項に基づいて外国に対して情報提供を行う場合、同項に定める要件の他に、EG Amtshilfegesetzの3条、4条に定める（情報提供の制限に関する）要件や、租税条約に定める国際的な租税秘密の保護の要件を遵守しなければならない。これに対して、EG Amtshilfegesetzによる情報提供は、原則として、他の国際的情報交換に関する法規の制限を受けないこととされている。

EG Amtshilfegesetz, Amtshilfe-Verordnung der EG、租税条約、租税事項における行政協力を定めた特別な条約、上の義務をこえた情報提供は、租税通則法117条の制限の下においてのみ許される。すなわち、租税通則法117条3項の要件をみなさない限り、好意による情報（Kulanzauskünfte）の提供は許されないのである。なお、情報を外国に対して提供すべきか否かについての決定（これは、行政処分とはされない）は、連邦大蔵大臣の裁量に委ねられている。

〔注〕

(21) Schaumburg, a.a.O. Fn. 18, S. 849-854.

(22) この問題についての詳しい参考文献リストは、Schaumburg, a.a.O., S. 849に掲げられている。

(23) BMF-Schreiben v. 1. 12. 1988, BStBl, 1988 I 466. なお、この覚書については、vgl. Matthias Werra, Die Grenzen der zwischenstaatlichen Amtshilfe in Steuersachen, Zum 3. Entwurf eines Merkblatts der Bundesministers der Finanzen, Betriebs-Berater 1988, 1160 ff. 参照。なお、国際的な租税の徴収共助に関する覚書（Merkblatt zur zwischenstaatlichen Amtshilfe bei der Steuererhebung (beitreibung), BStBl. 1987 I 402）も存在する。

#### 4 ドイツ租税行政庁による、外国への情報提供

##### (1) 概観<sup>(24)</sup>

ドイツ租税行政庁による外国への情報提供については、行政庁の事実解明義務（租税通則法88条1項）の要請と、納税者等の権利保護の要請の対立の中で考えなければならない。その結果、納税者の権利保護の要請をみたすために、一定の要件をみたす場合においてのみ、外国への情報提供が許されることになる。なお、国際的な情報交換の際には相互主義が要件とされるから、ドイツの方から情報を提供しないと、相手国からも情報の提供

を受けられないということになる。したがって、情報の提供は、結局は、国内問題なのである。

ドイツ租税行政庁から外国への情報提供の根拠となる条文としては、以下のものが存在する。

- ・ EG Amtshilfegesetz の 1 条 2 項、 2 条 1 項・ 2 項
- ・ Amtshilfe-Verordnung der EG の 4 条、 7 条
- ・ 租税条約の規定
- ・ 租税事項における行政協力を定めた特別な条約<sup>(25)</sup>
- ・ 租税通則法117条 2 項・ 3 項

これらは、互いに、他の適用を排斥するものではなく、重畳的に適用することが可能である。しかも、それぞれの射程範囲と情報の提供の態様が異なっている。このように、複数の根拠が重なる場合、前述のように、納税者等にとってもっとも有利な要件が適用される。

ドイツ租税行政庁が自発的に行うのではなく、外国から要求を受けて行う情報提供は、義務的な場合（すなわち、ドイツが、情報提供に関して国際法上の義務を負う場合）と、任意的な場合の二つに分けられる。義務的な場合とは、次の根拠に基づいて情報提供が行われる場合である。

- ・ EG Amtshilfegesetz の 1 条 2 項、 2 条 1 項
- ・ Amtshilfe-Verordnung der EG の 4 条、 7 条
- ・ 租税条約の規定
- ・ 租税事項における行政協力を定めた特別な条約

これに対して、租税通則法117条 3 項の情報提供は、義務的なものではなく任意的なものであり、その意味で、一般的に、好意による情報（Kulanzauskünfte）の提供と呼ばれている。もっとも、租税通則法117条 3 項は、EG Amtshilfegesetz の 1 条 3 項が認め、また、租税条約の情報交換条項が禁じていないところを、単に明確にしているだけであると解される。

これに対して、相手国からの要求がないにもかかわらず自発的になされる情報提供は、EG Amtshilfegesetz の 2 条 2 項と、Amtshilfe-Verordnung der EG の 4 条、 7 条により認められており、また、租税条約の情報交換条項も、一般的には、これを禁じていない

(例外あり)。

なお、米独租税条約26条に関するプロトコール26は、ドイツが諸外国と結んだ租税条約の中では特別なものであり、ドイツの情報提供を、EG Amtshilfegesetz の範囲に拡大している。

(2) 相手国の情報要求に対して情報提出義務のある場合(26)

—EG Amtshilfegesetz に基づく場合

外国からの情報要求が、EG Amtshilfegesetz, Amtshilfe-Verordnung der EG、租税条約、租税事項における行政協力を定める特別な条約により認められる場合、ドイツは、国際法上、当該情報を相手国に対して提供すべき義務を負う。このうち、EG Amtshilfegesetz の1条2項と2条1項は、EC加盟国間の情報交換についてのみ適用される。この情報交換に加えて、EC加盟国は、相互の間で、Amtshilfe-Verordnung der EG と、租税条約に基づいて、義務的情報（国際法上の義務として提供される情報のこと）を要求することもできる（EG Amtshilfegesetz 1条3項）。租税通則法117条2項も、これを確認している。

EG Amtshilfegesetz に基づいて義務的情報が提供されるのは、同法1条2項の要件が満たされ、かつ、3条1項の情報提供禁止事由が存在しない場合である。同法3条2項は、さらに、一定の場合における情報提供拒絶権を認めている。なお、提供を拒絶できるにもかかわらず提供された情報は、任意的に提供された情報として扱われる。

以下が、EG Amtshilfegesetz に基づいた義務的情報の提供の要件である。

・義務的情報が提供されるのは、要求国自身の所得税・資産税・付加価値税の確定に関して重要な情報についてのみである。したがって、たとえば、第三国の課税のための情報要求や、租税上の付随義務の確定のための情報要求や、徴収のための情報要求は、対象とはならない。

・EG Amtshilfegesetz の1条2項に基づく義務的情報は、租税通則法117条4項の要件の下においてのみ提供される。それによれば、情報要求の処理に際して、ドイツ租税行政庁は、ドイツの租税の課税標準の算定に関して認められるのと同じ権利・義務を有するとされる（租税通則法117条4項第1文）。また、租税通則法117条4項第3文は、関係者の前もっての聴問を要求している。

・EG Amtshilfegesetz の3条2項は、ドイツが情報提供を行う必要はないが、自発的に

行うことのできる（好意で行うことのできる）要件を定めている。すなわち、次のような場合に、ドイツ租税行政庁は、情報提供を拒否することができるが、拒否しなくともよいとされている。

- ・相手国が自らの調査をつくしていない場合（EG Amtshilfegesetz の 3 条 2 項第 1 文）
- ・相互主義の要件がみたされない場合（EG Amtshilfegesetz の 3 条 2 項第 2 文）
- ・情報提供を行うのに多額の費用を要する場合（EG Amtshilfegesetz の 3 条 2 項第 3 文）
- ・ドイツ租税行政庁が、自らの義務の履行を危うくされる場合（EG Amtshilfegesetz の 3 条 2 項第 4 文）

・EG Amtshilfegesetz の 3 条 1 項は、ドイツによる外国への情報提供が禁止される場合について定めている。すなわち、外国から情報提供の依頼を受けたドイツ租税行政庁は、ドイツ法上認められた手段では入手できない情報や、その入手がドイツの行政実務に反するような情報については、提供してはならないとされている。すなわち、情報提供の依頼を受けたドイツ租税行政庁がドイツ法上できないことは、情報交換の目的のためにもできないのである（同項第 1 文）。

・また、租税条約に反する課税をもたらすような情報の提供も認められない（EG Amtshilfegesetz 3 条 1 項第 2 文）。

・公序を侵害するような場合についても、情報提供は行われぬ。同様に、人権、安全保障等にかかわる情報は、提供してはならないとされている（EG Amtshilfegesetz の 3 条 1 項第 3 文）。

・また、営業秘密等の保護を目的とした情報提供の禁止も存在する（EG Amtshilfegesetz の 3 条 1 項第 4 文）。実務上、最も重要なのは、これであろう。ここで対象となるのは、情報提供により損害が生ずるおそれがある場合である。営業上の秘密の絶対的な保護を定める租税条約上の情報交換規定とは異なり、EG Amtshilfegesetz 上のそれは、損害のおそれのある場合についての留保をおいたことにより、その効力は相対化されたものとなっている。なお、租税条約上の情報交換規定と、EG Amtshilfegesetz とは、前述のように、重疊的に適用することが認められているので、関係者に有利な方が優先される。

(3) 相手国の情報要求に対して情報提供義務のある場合<sup>(27)</sup>—租税条約に基づく場合

租税条約における情報交換条項の人的射程範囲は、租税条約の他の条項におけるそれよりも広いので、情報要求国において制限的納税義務を負うにすぎないような者にもその適用が及ぶ。

ドイツの租税条約は、原則として、租税条約の適正な執行のための情報交換のみを定めるもの (kleine Auskunfts klausel) ではなく、1977年の OECD モデル租税条約と同じく国内租税法の執行のための情報交換をも認めるもの (große Auskunfts klausel) である。なお、いずれの場合においても、この他に、租税回避・脱税の防止といった目的のための情報交換が認められることがある。

国際的な情報交換の中でも、移転価格課税に関連した情報交換は、實際上、かなり重要であるが、そのような情報の提供は、租税条約のうち、国内租税法の執行のための情報交換をも認めるもの (große Auskunfts klausel) の下においてのみ認められる点に留意しなければならない。

なお、第三国における事実関係等の解明のために国際的な情報要求がなされる場合がある。たとえば、移転価格課税のために、情報要求を受ける国と第三国の両方で活動を行う企業の情報が要求される場合等が、これである。このような情報交換も、租税条約が国内租税法の執行のための情報交換をも認める場合 (große Auskunfts klausel) にのみ認められる。これに対して、ある国家Aが情報を第三国Cから直接的に入手できない場合に、相手国Bに対して、当該第三国Cで活動するその相手国Bの企業の情報の提供を求めたでしょう。この場合、確かに、このA・B二国間の租税条約に国内租税法の執行のための情報交換をも認める規定 (große Auskunfts klausel) が含まれていれば、その情報提供の要求は認められる。しかし、情報提供の要求を受けた国Bからの (当該情報提供義務を果たすための) 当該第三国Cに対する追加的情報提供要求が、そのA・B二国間の租税条約の適正な執行とも、Bの国内租税法の執行とも関係がない場合においては、租税条約の適正な執行のための情報交換のみを定める規定 (kleine Auskunfts klausel) によっても、国内租税法の執行のための情報交換をも認める規定 (große Auskunfts klausel) によっても、AのBに対する情報提供の要求は認められない。なぜなら、租税条約に基づく情報提供の要件は、一般的に、租税条約の適正な執行と、国内租税法の執行にとって必要があるということだからである。

租税条約にもとづく情報提供は、国際的な相互主義の前提においてのみ認められる。特に、提供される情報が、情報を要求した国において、情報を要求した国の国内法にもとづいて入手された情報と同じように秘密とされる、ということが重要である。

情報提供の拒否については、ドイツ連邦大蔵大臣に裁量を認められる。この裁量は、情報の提供を求められた国の法律と行政実務の留保の下にある（すなわち、当該国の国内法上あるいは行政実務において入手可能な情報のみが提供される）ので、この情報収集に関して国内法が権限を認めていない場合は、情報の提供はなされない。すなわち、情報提供を求められたドイツ租税行政庁がドイツ国内法上できないことは、情報提供のためにもできないのである。

国際的な情報交換に関する規定においては、一定の場合に、情報提供拒否権が認められている。ドイツは、自国の国内法律や行政実務によって入手できない情報や、相手国が自国の法律や行政実務によって入手できない情報（これは、相互主義の結果である）について、提出義務を負わない。この制限の範囲内において、情報提供を求められた国は、自国の国内租税のために用いることを認められた行政手続を用いて、情報を入手しなければならない。したがって、国内法上の調査権限の制限は、租税条約上もかなり重要な意味をもつことになる。

租税条約上の秘密の保護については、EG Amtshilfegesetz の 3 条 1 項第 4 文や、租税通則法 117 条 3 項第 4 文の場合とは異なり、関係者の保護のための秘密保護のみならず、ドイツの国益の擁護のための産業スパイ防止も重要な意味をもつ。なお、秘密の概念は、国内法によって決定される。

(4) 相手国の情報要求に対して情報提出義務のない場合<sup>(28)</sup>—租税通則法 117 条 3 項による場合

この点に関しては、租税通則法 117 条の規定について検討を行う必要がある。同条は、次のように規定している。

「租税通則法 117 条 租税事項における国際的な司法・行政上の協力

(1) ドイツ租税行政庁は、ドイツ国内法にしたがって、国際的な司法・行政上の共助の要求を行う。

(2) ドイツ租税行政庁は、国際的な司法・行政上の共助の要求を、国内的に適用される国際法、国内的に適用される EC 法、および、EG Amtshilfegesetz にしたがっ

て行う。

(3) その他の場合においても、ドイツ租税行政庁は、次の場合においては、要求にもとづく国際的な司法・行政上の共助を、義務的裁量にしたがって行うことができる。

- 1 相互主義の保証がなされていること
- 2 供与される情報と資料が、要求国の課税手続と租税処罰手続（秩序罰手続を含む）のためにのみ用いられること、および、供与される情報と資料が、租税事項の調査と租税犯罪の訴追にたずさわる者、行政庁、裁判所に対してのみ入手可能とされることの2点を、要求国に保証すること
- 3 所得税、収益税、資産税においては、生じうる二重課税を、相互協議において、課税ベースの適正な制限により避ける用意があることを、要求国が保証すること
- 4 情報要求の処理が、連邦あるいはその領域団体の主権、安全保障、公序、およびその他の基本的利益をそこなわず、また、商業上、産業上、営業上、および職業上の秘密、若しくは、要求によって明らかにされるべき事業過程がもらされる場合においては、国内関係者に司法・行政上の共助の目的と調和しない損害が発生するという危険が存在しないこと

国際的な司法・行政上の共助が、ラントの租税行政庁により執行される租税に関する場合には、連邦大蔵大臣は、管轄権を有する最高のラント官庁と協力して、決定を下す。

(4) 司法・行政上の共助の執行にあたっては、租税行政庁の権限と、関係者およびその他の者の権利・義務は、〔租税通則法〕1条1項の意味の租税について適用される諸規定にしたがう。……〔以下、省略〕

このうち、相手国の要求に応える義務がないにもかかわらず情報提供を行える場合について定めているのが、3項である。そこに上げられた要件は、他国において同様の規定を設ける際に、大いに参考となるであろう。

なお、ここで、本稿の目的との関連で特に重要な意味を有すると思われるのは、4項の規定である。承知のように、ドイツの租税通則法は、直接的には、あくまでも、その1条1項の意味におけるドイツの租税について適用され、外国の租税については適用されない。そこで、国際的な情報交換の前提として、外国の租税に関してもドイツ租税行政庁の

手による調査等を可能にするために、租税通則法117条4項は、租税通則法の調査に関する定めを、外国の租税に関する行政共助の場合においても認めることとしたのである(29)。

この点について、ある論者は、次のように述べている。少し煩雑となるが、本稿におけるテーマと直接的に係わるものなので、ここに引用しておく(30)。

「調査権限を有するドイツの租税行政庁は、他国の要求する情報を一その要求が許されるか否かを決定した後に一ドイツの課税が関係している場合と同じ方法で、入手しなければならない(租税通則法117条4項)。……情報提供の禁止は、国内法を根拠としてあるいは条約に反する課税の結果として(たとえば、租税通則法101条以下の情報・資料拒絶権)生ずる(その場合、相互協議が行われる)。さらに、禁止は、秘密保持の観点、および、営業・事業上の秘密保護の観点から生ずる。これについては、Merkblattの3.3.1をみよ。

ドイツの課税が関係している場合と同じように調査する権限が与えられている(租税通則法117条4項)ことにより、それ以上の問題が解消される。なぜなら、外国の課税当局により要求される情報は、多くの場合、国内者がそれを用意している場合にのみ供与可能だからである。それに対応する(行政庁への)情報提出義務〔=行政庁の質問検査権〕が存在しないと、そのように用意していることにはなりにくい。実務的には、(行政庁への)情報提出義務〔=行政庁の質問検査権〕の存在とその範囲に関しては、しばしば争いが存在する。連邦財政裁判所は、スウェーデンからドイツ連邦共和国に対してあてられた情報要求に関する問題について、スウェーデン法人の株式をドイツの銀行に預けているあるスウェーデン居住者の氏名に関する情報が要求がなされた事件において、見解を表明した。所轄のドイツ租税行政庁は、スウェーデンに対して提供するために、当該情報をその銀行に求めたが、無駄であった。これについて、連邦財政裁判所は、その提出を銀行に対して義務づけた(BFH, BStB1, 1979 II 268)。確かに、国内課税のためにのみ関係者およびその他の者の情報提供義務(租税通則法93条)は存在するのに対して、外国のためにそれが存在するのは、その義務が、特別な法規範により定められている場合のみである。スウェーデンとドイツの関係におけるそのような法規範は、スウェーデンの依拠している1935年5月14日の行政・司法共助に関するドイツ・スウェーデン条約である。しかし、そのような法規範

に基づいて外国に対する情報提供義務が存在するならば、国内者は、当該情報が国内における課税のために必要ではない、という点を主張することができない。しかし、この問題は、租税通則法117条4項により、明らかにされている。」

このように、ドイツ租税通則法117条4項は、課税庁の調査権限の根拠として非常に重要な意味を有しているのである。

#### (5) 国内法上の調査権の根拠

ドイツにおける課税庁の調査権限一般の問題に関しては、ここで議論する余裕はない。それについては省略するが、それは、上の説明で、本稿における問題に対して答えるには十分であると考えたからである。

〔注〕

(24) Schaumburg, a.a.O. Fn. 18, S. 857-860.

(25) これについて、詳しくは、Tipke/Kruse, a.a.O. Fn. 18, § 117, Tz. 7, Übersicht B 参照。

(26) Schaumburg, a.a.O. Fn. 18, S. 861-865.

(27) Schaumburg, a.a.O. Fn. 18, S. 865-872.

(28) Schaumburg, a.a.O. Fn. 18, S. 872-875.

(29) Tipke/Kruse, a.a.O. Fn. 18, § 117, Tz. 14.

(30) Volker Kluge, Das deutsche Internationale Steuerrecht, 3., völlig überarb. Aufl., 1992, S. 331-332.

### III イギリス

#### 1 調査権限一般

ここで、イギリスにおける租税行政庁の国内法上の調査権限一般について詳しく議論する余裕はない。ここでは、本稿の問題に答えるのに必要な範囲で、租税行政庁の調査権限一般について概観的に述べておくこととする。

イギリスにおける租税行政庁の国内法上の調査権限一般に関して、ある論者の述べるところを次に示しておく(31)。

「国税庁 (Inland Revenue) は、納税者以外のソースから、ある者の所得に関する

情報を入手することができる。すなわち、たとえば、雇用者からは、被用者の氏名と支払の詳細（TMA 1970 s.15）を；商人等からは、被用者以外の者に対するサービス対価支払、すなわち、コミッションや backhanders の詳細（TMA 1970 s.16）；銀行からは、預金口座に関してその課税年度中に15ポンドを超える利子を支払った先の顧客の氏名（TMA 1970 s.17）；グロスで利子を支払っている者（すなわち、Director of National Savings）からは、利子の受取人の氏名と支払額（TMA 1970 s.18）；政府部局とその他の公権力主体からは、サービスに対する支払や助成金・補助金支払の詳細；および、賃借人その他の土地利用者から、賃料その他の土地利用の対価としての支払の詳細（TMA 1970 s.19）である。

加えて、国税庁は、その取引が調査の対象となっている者に関する情報を入手する広範な権限を有している。たとえば、TMA 1970 s.20によれば、その者、あるいは、第三者は、関連文書を提出する義務を負わされることがある。この規定は、キース委員会によりなされた勧告の結果として、Finance Act 1989により修正された。その結果、関連文書の提出を要求することに加えて、納税者に対して質問に文書で答えることを要求することが可能となった。情報が当該納税者の現実の知識として存在（第三者から書面の回答を求めることができない）する場合に、この改正は意味あるものであり、そのような手段がなければ文書の山を調査しなければならないような際に、国税庁の手間を省くこととなろう。この条文のもう一つの改正点は、文書提出義務を負う「第三者」の定義を、一定の範囲の者（おおまかにいって、事業者と、納税者の親族）から、すべての者へと拡大したことである。租税調査官が、納税者や第三者に対して関連文書を提出することを正式に要求しうようになる前に、彼は、まず、その情報をインフォーマルなかたちで要求し、ついで、正式の命令に関して、General Commissioner、あるいは、Special Commissionerの同意を得なければならない。

情報が privileged である（すなわち、弁護士等の守秘義務により守られている場合）、第三者に対する情報要求権は制限される。……」

〔注〕

(31) Chris Whitehouse, Revenue Law—Principles and Practice, 12-14 (11th ed. 1993). なお、イギ

リスにおける租税行政の国内法上の調査権限一般に関しては、たとえば、David Jeffery, Brian Sturgeon and Michael O'Brien, *Tolley's Tax Investigations*, 1988; *Simon's Taxes*, part A3; *Halsbury's Laws of England*, vol.23, 1373-1560 参照。

## 2 情報交換

イギリスにおいても、租税条約に基づく情報交換そのものについて国際租税法的な見地から議論した文献はそれなりに存在する<sup>(32)</sup>が、国際的な情報交換に関するイギリス課税当局の対応や、国際的な情報交換に関するイギリス国内法の状況等について論じたものは少ない<sup>(33)</sup>。この点は、この問題に関する日本における状況と似通っているといえよう。

この国際的な情報交換に関するイギリス課税当局の対応や、国際的な情報交換に関するイギリス国内法の状況等の点については、上の I の 3 で多少の叙述を行っておいたが、ここでは、さらに、この点に関してふれた文献における記述を、以下に、多少詳しく紹介しておく。

「情報交換に関する国税庁の権限に対する最人の潜在的制限は、国内租税法律において定められた情報収集権限（の限界）と、租税条約と EEC の 1977 年ディレクティブにおいて定められた、外国課税当局への情報の開示に関する権限との関連で検討することができる。しかし、制度が実際にどのように運用されているかという点に関して完全に理解したり、情報収集権限の制限について正確に述べることは、ほとんど不可能である。これには、二つの理由が存在する。すなわち、第一に、国税庁は、この分野における活動についてまったく最小限の情報しか出さない。また、第二は、納税者が自らの取引に関する情報について、外国への開示がなされるであろうことを前もって知らされるべきであるという定めが存在しないために、開示の可否が裁判所で争われることがほとんどないという点である。なぜなら、この点に関して納税者に対して認められている権利というのは、裁判所に訴え出て、開示を禁止する決定を求めることであるが、そうするためには、納税者は、開示が行われるであろうことを前もって知っていなければならないからである」<sup>(34)</sup>。

「イギリスは、その国内法によれば、情報交換その他の外国の課税当局に対する協力形式、に関するユニラテラルな措置を提供しないことになっている。

国税庁は、納税者と第三者の両方から情報を入手するための、非常に広範な権限を

保有しているが、このような情報収集が行われるのは、もっぱらイギリスの課税に関する義務を確定するためであり、情報収集は、Taxes Management Act 1970……に定められた厳格な秘密保護の要請に服する。国税庁のコミッショナーは、その職務遂行上入手したいかなる情報をも、職務目的のためを除けば、開示しないという約束に署名しなければならない。……Finance Act 1989 の182条は、租税行政庁の職員が、その職務遂行の過程で入手した情報を違法にもらした場合には、guilty of an offenceになると定めている。この結果、国税庁の外の者にそのような情報をもらすことを認める、イギリス法の定めが存在しない限り、秘密保持の要求は厳格である。

イギリスが、行政共助に関する1977年のECのディレクティブにしたがうことを可能とするために、Finance Act 1978 の77条が制定されたことにより、〔上に述べたような〕秘密保護の責任は特別に解除された。さらに、イギリスは、ここ40年ほどの間に、情報交換の定めをもつかなりの数の租税条約を締結したけれども、政府は、1986年に、租税条約に関するIncome & Corporation Taxes Act 1970 の497条の定めが情報交換に関する十分な権限を〔イギリス租税行政庁に対して〕与えるものではないという点を指摘され、それに応えて、Finance Act 1987 の70条という新たな定めがおかれた。この定めは、今は、Income and Corporation Taxes Act 1988 の788条におかれている。〕<sup>(35)</sup>

「行政共助の提供の際には、2つの制限が存在する。すなわち、第1に、国税庁自身がその職務を遂行する際に入手することを認められている情報の制限であり、第2に、そのようにして入手された情報のうち、どの程度が、情報交換条項の文言の下に相手国に対して提供されるかという点に関する制限である」<sup>(36)</sup>

#### 「国内法上の制限

国税庁は、特定の納税者に対してのみならず、銀行や共同事業者のような第三者に対して適用されるところの、広範な情報収集権限を保有している。しかしながら、これらの権限は、国税庁がその権限を果たす過程における情報を入手するという目的のみにために認められており、この権限は、イギリスの課税に関する義務を確定するためのものに限定されている。その結果、国税庁は、イギリスの納税義務に関連のない情報を入手することが国内法上できないので、条約相手国の課税に関する定めについてのみ関連する情報を適法に入手することができず、それ故に、提供を要求された情

報が、要求を受けた国の租税行政庁の手元にあるか否かにかかわらず、要求を受けた情報の交換を行うことを要求する租税条約上の規定を、守ることはできない。

しかしながら、イギリスは、すべてのイギリス源泉の所得、内国法人の全世界所得・利得、イギリス居住者の全世界所得・利得に対して課税している。このように、課税の対象がきわめて広いので、国税庁の手元に存在しないにもかかわらず、外国の課税当局からの要求の対象となりうるという情報は、イギリス源泉の所得・利得と外国から現実にイギリスに送金された所得・利得についてのみ納税義務を負うところの、非永住者 (resident but not domiciled individuals) の国外源泉の所得・利得に関する情報のみであろう。したがって、実務上は、国税庁は、租税条約の相手国により要求された情報を保有していることが多い。……」(37)

「(1977年12月の EC のディレクティブの77/779号には) 加盟国が自らの国における課税目的上は必要としない情報をも、他の加盟国に対して提供すべきであるという定めが存在する。しかし、イギリスは、定めにしたがうための国内法律をいまだ制定してはいない (1989年の段階において)。……

しかし、EC のディレクティブについては、事態が急速に進展している。1977年のディレクティブの改正に関する1989年2月2日の草案は、国内法および行政慣行の下において入手できない情報については情報交換の義務はないと定めている1977年のディレクティブの1条を改正するための定めを含んでいる。この改正は、加盟国が一定の状況において情報提供を行うべきことを義務づけ、また、行政慣行によれば情報の入手要請に応えることができないという事実 に 依 拠 (して情報提供を拒否) することを不可能とするものである。この草案は、また、1990年7月1日までに草案の条件にあわせて必要な国内法を制定することを加盟国に義務づける定めを含んでいる。しかし、イギリスが、この草案の提案にしたがうための立法を行うべきであるか否かの議論においては、これ以上の改正は不必要であると一般に考えられている。」(38)

結局、Finance Act 1990 の125条により、イギリスは、EC 加盟国の租税との関連においては、どうやら、租税行政庁はその有するすべての権限を行使することができることが認められたが、これを租税条約の相手方のすべてに対して適用すべき義務があるわけではないのである (39)。

〔注〕

- (32) この点については、たとえば、David Davies, *Principles of International Double Taxation Relief*, 212-218(1985); Philip Baker, *Double Taxation Conventions and International Tax Law*, 441-452 (2nd ed. 1994); Asif H. Qureshi, *The Public International Law of Taxation, Text, Cases and Materials*, ch. 6(1994) 等、参照。
- (33) この点について述べた書物としては、Picciotto, *supra* note 14, at 276-277 と、Jill C. Pagan, *Country Report for the United Kingdom*, 75b *Cahiers de droit fiscal international* 455 (1990) くらいしか、見出すことができなかった。
- (34) Pagan, *supra* note (33), at 455.
- (35) Pagan, *supra* note (33), at 455-456.
- (36) Pagan, *supra* note (33), at 462.
- (37) Pagan, *supra* note (33), at 462-463.
- (38) Pagan, *supra* note (33), at 466-467.
- (39) Picciotto, *supra* note (14), at 276. また、Halsbury's *Laws of England*, vol.23, 1477-1478 参照。

## IV フランス

以上のように、ドイツにおいては、国内法的な整備がほぼ完成していて、ドイツ租税行政庁は、租税条約に基づく情報交換のための広範な情報収集権限を国内法により認められている。これに対して、同じ EC 加盟国とはいっても、イギリスにおいては、(EC 加盟国との間の情報交換の場合の国内法規の整備はほぼ完了しているが) 租税条約の情報交換規定に基づいて、イギリスの租税と関連のない調査を行うことは、国内法上、認められていない。

以上の二国と比べて特徴的なのが、フランスである。フランスにおいては、もっぱら、国内法上の広範な調査権限に基づいて条約上の義務に応えようとしている。ここでは、フランスの状況について、簡単に記述しておこう。

### 1 情報交換の国内法上の根拠

フランスの国内租税法には、国際的な情報交換に関する明文の定めが存在する。ある論者は、この点について、次のように述べている(40)。

「租税手続法典は、その114条に基づいて、外国との間で情報の交換がなされることを定めている。同条は、いう。

『租税行政庁は、海外自治領その他の特別な租税制度に服するフランス共和国の領域的団体の租税行政庁、および、フランスの行政庁との間で情報交換のために租税に関する共助条約を締結した国家と、情報を交換することができる。』

この定めは、職務上の秘密に関する定めの特例の一つであり、フランスの租税行政庁が、その保有することのできる情報を外国の租税行政庁に対して提供することを可能にする。

EC共同体のディレクティブの定めは、租税手続法典のL.114A条、R.114A 1条からR.114A 5条において、フランス国内法に取り入れられている。L.114A条は、次のように定めている。

『相互主義の留保の下に、フランスの租税行政庁は、ヨーロッパ経済共同体の加盟国の行政庁に対して、所得税、資産税、ならびに付加価値税の賦課および徴収のために、情報を提供することができる。』

したがって、国内法は、外国の行政庁との情報交換に際して、情報交換を規定した租税条約の存在と、相互主義を要求しているのである。」

このような国内法の定めは、条約の定めを国内法的に確認しているだけである。したがって、これらの条文に関して、詳しい解説等が存在するわけではない。

(注)

(40) Patrick Michaud, National Report, 75b Cahiers de droit fiscal international 339, 340 (1990).

## 2 情報交換に関する条約上の定め

フランスにおいても、情報交換に関する条約上の定めに関して、ドイツやイギリスにおける同様の解説がなされている。たとえば、ある論者は、この問題に関して、次のように述べている(41)。

「情報の交換は、各国家の領土主権の通常原則に反する。すなわち、情報交換に関しては、租税行政庁の権限と行為手段が、国家の課税を行うために行使されるのではなく、外国の租税法の適正な執行を確保することを助けるために行使される。

情報の提供を求められた国は、たとえ、情報の提供を求めた国が当該事項についてより広範な権限を保有している場合であっても、自らの立法と通常の行政実務により課される制限を超えて行動することはできない。

反対に、仮に、外国の行政庁が、フランスの法律と行政実務を適用して通常収集することのできない情報を要求してきた場合においては、フランスの行政庁は、この要求に応えることが不可能であることを主張することができる（Instruction du 27 mai 1969, BOCB 1969-II-4530, n.134）。

『通常保有する』という表現は、国内法により定義されるところの、各国の租税行政庁の調査・監督権限の行使に関するものであり、より負担が重くなる強制的な手続による拡大を意味するものではない。もっとも、1993年の統一市場の計画の中で、行政共助の執行は、加盟国の行政実務により制限されてはならないと定める、1989年2月13日のECディレクティブの Scrivener 草案により、以上のような制限は、〔EC内においては〕もはや適用されなくなるおそれがある。』

しかし、フランスの行政庁が、（フランスの課税にかかわりなく、もっぱら外国の租税に関して）外国からの依頼にもとづき情報収集を行う（ドイツの租税通則法117条4項のように、それを認める明文の定めはないのであるが）ことを国内法が認めているか否かという点に関しては、国際租税法に関するフランスにおけるもっとも権威ある書物である、Tixier と Gest の教科書<sup>(42)</sup>をはじめとして、筆者の知るかぎりの文献においては、特に言及はなかった。しかし、これは、次の書物にあるように、実際には認められていると解されているのではないかとと思われる<sup>(43)(44)(45)</sup>。

「国家は、外国の要求に応えるために、自らの立法や通常の行政実務の範囲を超えることはできない。しかし、フランスに関していえば、このような制限は、行政庁の権限が広いことを考慮するならば（租税手続法典 L.81条下に定める droit de communication の権限）、あまり重要ではない。」

〔注〕

(41) Michaud, *supra* note (40), at 348-349.

(42) Guy Gest et Gilbert Tixier, *Droit fiscal international*, 2<sup>e</sup> éd. refondue, 1990.

- (43) Bruno Gouthière, *Les impôts dans les affaires internationales*, Trente études pratiques, 622-623(1989). なお、「ドイツにおけるように、一定の国においては、納税者は、自らに関する情報の交換に関して告知を受けることになっているが、このようなことは、アメリカ、イギリス、フランスにおいては、要求されていない。」(ibid.)
- (44) なお、フランスで開設された銀行口座の存在と、そこでなされた取引についての外国の行政庁によりなされた情報の要求に関して、Patrick Dibout, *Assistance fiscale internationale*, *Juris-classeur fiscal*, Fasc. 17, p.8 参照。
- (45) *droit de communication* については、Olivier Fouquet, *Droit de communication*, *Juris-classeur fiscal*, Fasc. 1451 参照。

## V まとめ

### 1 日本の状況

日本においては、質問検査権が個別の租税法上にばらばらに規定されているところからみても、国内法上、外国の租税の賦課徴収のための質問検査権は、認められていないものと解されている。そもそも、質問検査権の行使権限は、客観的な必要性等の様々な制限によりかなり限定されたものなので、所得税・法人税等の賦課・徴収のための抽象的な必要性（すなわち、調査を行うともしかすると賦課処分を行うことができるかもしれないといった程度のもの）のみでは、質問検査権の行使が正当化されない<sup>(46)</sup>可能性があり、簡単に結論づけることは必ずしもできないが、この点が、アメリカやドイツやフランスにおける広範な調査権限とは少し異なったものとなっているとってよいのではないかと思われる。

また、この問題に関しては、租税条約上の情報交換の義務を定めた規定が国内法として self-executing であると考えすることはできないであろう。なぜなら、第一に、租税条約それ自体が、国内法による制限を前提とした情報提供義務を定めている。また、第二に、租税条約においては調査権限がだれに存在するか等々の具体的な点について、必ずしも明確に定められていないから、国内法の定めなくして、租税条約の規定を直接適用することは困難である。

しかし、国際協調主義を一種の国是とする日本のような国において、ドイツ租税通則法

117条のような、外国の租税に関する情報・資料の収集権限の行使を認める国内法の規定が存在しない点は、不可思議とさえいえるかもしれない。その意味で、この点に関する日本の状況は、スイスやイギリスと似たものなのである。

〔注〕

(46) 質問検査権については、それがもっぱら確定処分のためのものか、あるいは他の処分（たとえば、青色申告の承認等の処分）のためにも行使できるのかという点が議論されている（最終昭和48年7月10日刑集27巻7号1205頁は、後者の場合をも肯定）のであるから、調査すると何かでてくるかもしれないというのでは、その行使は認められないであろう。

## 2 改革の方向

しかし、上の点に関連して、国内法上の特別な定めを設けるとしても、その際に留意しなければならない点が少ない。ここでは、次の三つをあげておこう。

第一に、租税条約上の情報交換規定に基づく、国内法上の調査権限の定め方である。この点については、ドイツの租税通則法117条のように、所得税法・法人税法等における質問検査権を定めた規定にいう租税には、外国の租税も含まれるという条文をおく形式と、フランスにおけるように、国内法上の広い一般的な調査権限を認める方式の二つが考えられようが、単純さと明確さからいって、前者の方式の方がのぞましいのではなかろうか。もちろん、一つの考え方としては、フランスやアメリカにおけるように国内法上の調査権限を（租税条約上の情報交換規定と直接的に関連させた明文の定めをおかないで）広く定めるといことも考えられる。日本の質問検査権の範囲がかなり狭いものであると思われることを考慮するならば、厳格な手続的保障の留保の下に質問検査権の範囲を広げるとは、情報交換の問題とは切り離しても、必要なことなのかもしれない。しかし、そのような改正には時間がかかるであろうことを考えるならば、とりあえず目的をしぼり、日本の租税のみならず外国の租税に関して質問検査権を行使できる権限を租税行政庁に対して与えることで十分であろう。

第二に、いかなる規定を設けて、情報交換のための質問検査権の行使を認めるにせよ、秘密保護の見地からの手当てが必要であろう。まず、形式的な点からいえば、外国に情報を提供する場合には守秘義務が解除されるという定めをおくことが必要であるかもし

れない。また、外国からの情報要求を拒否できる場合を、プライバシー保護等の観点から明確化した規定をおく必要性があろう。

第三に、納税者等に対する手続的保障の確保が必要である<sup>(47)</sup>。すなわち、外国からの情報提供の要求に応じて、日本の課税当局が質問検査権を行使し、その結果得られた情報を外国の課税当局に提出した結果として、納税者が当該外国の課税当局から不測の課税を受ける可能性もあると思われるところから、少なくとも、外国の当局に対して情報を提供する旨を納税者等に対して知らせることが必要となってくるかもしれない。考えかたにもよるが、場合によっては、通常の国内的な質問検査権の行使の場合よりも、厳格な要件が必要な場合もありえよう。

いずれにせよ、先進国の趨勢としては、スイスとイギリスの他は、かなり広い権限が租税行政庁に対して認められているのであり、スイス・イギリスが自国の金融市場の保護の見地からそのような姿勢をとっている点に対しては、批判の対象とさえされているのが現状である。したがって、この点に関して、日本も世界の趨勢にあわせることが望ましいのではなかろうか。

そうすることが、また、相互主義の原則の下に行われる情報交換を日本が外国に対して要求する場合の便宜ともなり、ひいては、日本における課税の公平性を確保する道でもあるからである。

〔注〕

(47) 調査権限の拡大と手続的保障の確保はバラレルに考えていくべきであろう。

(禁無断転載)

(非売品)

平成9年9月30日印刷

平成9年9月30日発行

国際商取引に伴う法的諸問題(6)

報 告 書

発 行 ©財団法人 トラスト60

東京都中央区八重洲2-3-1

住友信託銀行八重洲ビル内

Tel. 03-3286-8100 (代表)

印刷：(株) ディグ