先進国におけるサイバーセキュリティの社会的課題
-デンバーサミットコミュニケ40番の示唆

高橋郁夫
弁護士

概要

デンバーサミットのコミュニケ40番は、コンピュータセキュリティとその法的インフラの整備と産業界の努力課題という観点からして、きわめて注目に値するものである。そこでは、ハイテク犯罪者に対する捜査、訴追、処罰のために、濫用の察知、証拠保全、犯人の所在の特定が必要であることが述べられており、そのために、産業界および司法界のなすべきことが強調されている。ハイテク犯罪のクロスボーダー的性格は、いままであまり注目されていなかった国際刑法的な側面を強調してくることとなる。特に国際捜査共助においては、ハイテク犯罪者のアクセスログに対する捜査についての特別の手続きの創設が、先進国の課題となろう。

The Social Subjects of Cyber Security in P 8
-suggestions of communique 40 of the Denver Summit

Ikuo Takahashi
lawyer-Bengoshi

The communique 40 of the Denver Summit is very suggestive for the Cyber Security from the point of industrial effort and legal analysis. It emphasizes the necessities of the recognition of the unauthorised access, securing the evidence and specification of the location of the criminals. High tech crime has the cross-border nature and the combat against such crimes need the legal analysis of the international criminal law. Especially, the special procedure to seize the access logs of the network will be discussed from the point of international cooperation.

序 本稿の目的

デンバーサミットにおいて、先進主要7か国とロシアとは、1997年7月22日に、コミュニケを発表している(注1)。そのコミュニケのなかで、40番の「我々は、リヨンでの勧告を実施するための取組みを強化しなければならない。これからの1年、我々は、重大な関心を有する2つの領域に焦点を当てる。1つは、コンピュータ及び電気通信技術に対して国境を越えて介入するようなハイテク犯罪者についての捜査、訴追及び処罰である。もう1つは、犯罪者の所在地にかかわらず、すべての政府がハイテク犯罪に対応する技術的及び法的能力を有することとなる体制である。」という部分は、コンピューターセキュリティと法律との関係という見地から極めて、興味深いものである。本稿の目的は、このコミュニケの40番の意味を分析することにある。

第1章 サミットにおけるコミュニケ40番の位置づけ

1 デンバーサミットでの位置づけ

デンバーサミットのコミュニケの90項目うち、38番から、41番までは、「国際的犯罪組織」について、また、44番から46番までは、「テロリズム」についての各国の合意である。テロリズム対策や国際的な組織犯罪に対する対応は、緊急を要する課題であるというのが、G7各国における共通認識といえるであろう。（たとえば、この経緯を示すものとして、テロリズムに対する宣言(27/7/1996)がある(注2)。）そして、コンピューターのセキュリティの観点からしたとき、前述

の40番に加えて、45番で、「各国のテロ対策能力の要覧を創設すること、暗号の使用に当たって、テロリズムと闘うための政府の合法的なアクセスが、OECDガイドラインに沿って可能となるよう、すべての国に対し奨励することが含まれる。」という部分、および「 電子・コンピュータ・インフラへのテロ攻撃を抑止するための手段を開発すること、(中略)並びに国際協力及び協議を強化し拡大することである。 」という部分は、きわめて注目を要するであろう。

2 サミットの流れのなかでのコミュニケ40番

ここ数年のサミットの流れのなかで、従来の経済的な議論にもまして組織犯罪対策、テロリスト対策が重要な課題となってきた経緯に関連して、アルシュサミット(1989年)ナポリ経済宣言(1994)ハリファックス・サミット議長声明(1995)をへて、リヨン・サミット議長声明へとつながる経緯については、注目しておく必要がある。そして、この議長声明を実現に写すために、リヨン上級専門家グループの勧告がだされている(注3) 。 とくに、この勧告では、 国際組織犯罪に対する対策に際しての国際協力と、それにおける共罰性の要件の撤廃や電子的監視の重要性が、強調されていることは注目を要する(注4) 。

3 バーミンガムサミットへの流れのなかで

前述のデンバーサミット・コミュニケ40番の先進国における取り組みは、その後、さらに深みを増していくことになる。 そのなかで注目されるべきことは、1997年12月 10日のワシントン特別区における8ケ国司法・内務閣僚級会合である(注5) 。この会合では、「我々は、本日の閣僚レベルの会合において、二つの重要な任務の達成に向けた具体的な行動計画について意見の一致をみた。一つはハイテク犯罪を捜査訴追する能力を高めることであり、もう一つは世界のいかなる場所にも犯罪人にとって安全な避難先が存在しないことを確保すべく、犯罪人引渡し及び捜査扶助に関する国際的な法体制を強化することである。」ということが決議され、ハイテク犯罪に対する先進国の決意が固いことをよみとれるものとなっている。

4「ハイテク犯罪者」の概念

40番のコミュニケの最初の問題設定は「コンピュータ及び電気通信技術に対して国境を越えて介入するようなハイテク犯罪者についての捜査、訴追及び処罰である。」ということであり、「ハイテク犯罪者」の概念をみておく必要がある。

コミュニケ40番における議論の対象としての「ハイテク犯罪」の概念は、国際組織犯罪との関係で、どのような論点をふくんでいくかという観点から考えるが合理的であろう。そうだとすれば、「ハイテク犯罪」を、「コンピュータおよび電気通信の新技術が悪用された犯罪的行為」として考えることができるであろう。コンピュータおよび電気通信の新技術の発達により、二つの脅威が増大するに至ったといえるであろう。すなわち、「第一に、技術に習熟した犯罪者が、コンピュータ及び電気通信システムを標的として貴重な情報を権限なく入手または改竄し、更には重要な商業及び公共システムを混乱させようと試み得ることである。 第二に、組織的な犯罪グループの構成員やテロリストを含む犯罪者が、旧来の犯罪の実行を容易にするために、このような新たな技術を利用することである。」という脅威である。これらの脅威を合理的にコントロールするためにどうすべきか、という議論の射程を決めるものとして、「ハイテク犯罪」という用語を用いることが許されるべきである。もっとも、この用語は、従来の議論に比して(注6) かなり広いものとなる点は注意を要する。そして、この「ハイテク犯罪」が国際的な活動・組織とともにあることも注目すべきである。

第2章　国際的ハイテク犯罪捜査の技術上の問題点

1 具体的な問題点

ハイテク犯罪についての捜査・裁判についての技術的な問題点について、8か国司法・内務閣僚級会合は、産業界にたいして、地球規模のネットワークを設計、展開及び維持するのは産業界であり、また、技術基準の発展に第一義的に責任を負うのも産業界であるとの要求をし、また、産業界は、コンピュータ及び人員についての優れた安全対策を講じつつ、コンピュータの濫用を防ぐための安全システムを開発供給することにつき、その役割を果たす義務がある、そして、そのシステムはコンピュータの濫用の察知、電子データの証拠保全、犯人及びその所在の特定にも資するようにも設計されるべきであるとしている。 濫用の察知の問題点、犯人追及の問題点、証拠保全の問題点の3つの問題が、技術的な問題としてクローズアップされるべきであるということが明らかになる。

2 コンピュータ濫用の察知の方法とその問題点

前章でみた「ハイテク犯罪」のうち、無権限アクセスによってひきおこされるものは、かなりの程度にのぼる。これにたいしては、検知対策として、「セキュリティ監視」すなわちシステム稼働状況の監視と解析、そしてその結果の管理者への通報が有効である。このような機能は、実際にもソフトとして実用化されており、むしろ、ネットワークの管理にあたっては、必需品であるということがいえよう。 現実にも、「ネットレンジャー」などの製品がある。

そして、この「監視」によって、なんらかの犯罪的な行為が検知されるときには、ネットワーク管理者が、その経由している、ないしは、アクセス行為がなされているサイトに警告を出すことが行われているといわれている。

3 ハイテク犯罪者に対する追求の技術上の限界

技術的には、すくなくても、現在のインターネットにおいては、接続したコンピューターの特定は可能である。しかしながら、インターネットカフェや携帯電話などから、また、ダイヤルアップによる侵入行為がなされる場合には、どうやって、その侵入者を特定していくかという問題が、でてくる。また、そもそも、犯罪者の追跡には、基本的にリアルタイムの追跡がもっとも有効なものとなろう。だとすれば、時差のむこうからやってくる犯罪者を迎え撃つ体制ができなくてはならないことになる。この観点からすると、上述したような既存のネットワーク管理者における警告の慣行の制度化と24時間体制の整備、また、捜査当局におけるハイテク犯罪に対する捜査体制の拡充が、緊急の課題となるものと思われる。 もっとも、技術的にネットワークのシステムが、「犯人およびその所在の特定に資するように設計されるべき」とすべきか、また、それが、そもそも、技術的に可能なのかは別問題であろうと思われる。

4 裁判における技術上の問題点

4.1暗号問題

犯罪を実行するための謀議の手段として、ハイテクがもちいられ、また、その組織の構造をさしめす直接な証拠が、暗号技術によってアクセスできなくなっていく。しかし、逆に犯罪の捜査、謀議の状況の確定には、その通信の内容の確保が大事である。アメリカにおけるクリッパーチップをめぐる議論やキーリカバリー政策をめぐっての議論などが、有名であり、また、OECDにおいても暗号政策についてのガイドラインを発表しているところである。この暗号政策をめぐっての問題は、きわめて大きな問題であり、産業界における具体的なソリューションとして、HPのICFやTISのRecovery Keyをめぐるシステムなどがあることを紹介しておく(注7) 。

4.2 証拠の改ざん

次に、証拠にアクセスができ、その証拠を保全収集した時に、後に裁判ということになり、その証拠の改ざんがなされていないことを証明しなくてはならない。技術的には、信頼しうる機関が、その差し押さえ当時のデータが、そのようなものであると証明することで、この点は足り、また、技術的には、認証技術の応用によって確保されよう。

第3章　ハイテク犯罪に対する捜査の法的な諸問題（注8）

最初に、通信の秘密というのは、どこまでを守備範囲とするのかという問題がある。とりわけ、通信の主体の問題とその内容についての問題の区別をして、保護の程度を変えるべきかいなか、また、通信の一方の同意の効力がどのようなものか(注9)などが問題である。

次にSteve Jackson Games事件(注10) で示唆された捜索・差押えの際の問題点の検討が必要になる。この点で、米国において司法省が、電子的な捜査についてのガイドラインを作成しており、非常に詳細なもので、きわめて参考になる(注11) 。

また、電気通信事業者等の協力等についての問題点 については、種々の問題点が指摘できる。ネットワークのこれを管理すべき地位にあるものについては、電気通信サービスを提供する電気通信事業者(第1種)(第2種)である場合もあれば、有線電気通信者などの場合もある。 これらの者は、それぞれ通信の秘密を守る義務を負うこととなるが、その範囲がどの程度のものか、また、アクセスログが、法的にどのような性格をもち、法的にどのように取り扱うことができるかが問題になる。

第4章 ハイテク犯罪のクロスボーダー化の引き起こす法的問題

1 国際的な犯罪的行為に対する対応

ネットワークには、国境は関係なく、クロスボーダー化する組織犯罪、テロリストが、いわば、ハイテク犯罪化の傾向を強めてきている状況においては、各国において、協調した特別の取組みが必要になるものといってよいであろう。そこでは、各国の主権や国民の通信の秘密、プライバシーを考慮に入れつつ、国際ハイテク犯罪の捜査にあたって特に頻繁に必要とされるものと考えられるリアルタイムでの捜査情報の国際的な収集・交換を可能にすべきではないかということが議論されてくるのである。 このために、8ケ国司法・内務閣僚級会合においては、引渡し及び捜査共助における一層の協力の必要性が重大であることの認識で一致し、そして、双罰性の問題に柔軟に対処するなどの措置により既存の協力体制上の障害を除去することとしている。また、コンピュータの重大な濫用に対し、引渡しを可能とするに足る十分な刑事罰を規定することを確保し、さらに、国際的な犯罪について、捜査及び訴追の衝突または重複を最小限にするため、国家間の調整を一層推進し、どの国での訴追が最適であるか、また、証拠の収集及び共有についての責任の割当てにつき協議するということになったのであり、きわめて注目に値するといえるであろう。

2 国際的な捜査協力とその問題点

この捜査については、二つの種類が考えられる。中央当局を通す場合と、 ICPOルートである(警察庁「不正アクセス対策法制に関する調査研究報告書」(41ページ以下)。以下、「警察庁報告書」という)) 。中央当局をもちいる場合とは、いわゆる国際捜査共助法に基づいてなされる場合である。

国際捜査共助法に基づく場合における捜査の実際の手続きについては、警察庁報告書(41ページ以下)を参照のこと。かかる手続きは、講学上は、「狭義の司法共助」のうち、嘱託書に基づくものということになろう。一方、ICPOルートは、要請国における刑事事件の捜査に有益な資料を提供するものである。要請にかかる行為が双罰性の要件を満たすものであることが必要であり、また、

手続き的に迅速性があるが、捜索・差押などの強制処分が不可能であるという問題点があるといわれている。

ログの保存の期間との関係で、捜査が十分におこなわれない可能性があるといわれている(注12)。そうだとすると、なんらかの形で、しかるべき期間の保護があるように誘導する必要がある。そのための方策としては、どのようなことが考えられるか。 このための具体的な方法を考える必要があろう。また、実際に、この捜査をリアルタイムでおこなえるようにすることが重要である。もっとも、その過程において、何故に共助法のような、ある意味で非常に迂遠な方法がとられているかという観点からも考察が必要である。 要は、執行管轄権と、外国における適正な刑事処罰の要請との調和ということであろうか。

共罰性の要件について、わが国での不正アクセスについての規制がないことから、これをみたさないとされることも問題である(後述)。

従来の犯罪捜査については、従来の共助の方法がとれるとして、ネットワークにおけるアクセスログについての証拠収集においては、それが通信の内容に関係しない点、リアルタイム検知の必要性の観点から、ネットワーク型の捜索・差押え類型が考慮されて然るべきべきと思われる。なお、検討を要する。

第5章 国際的ハイテク犯罪者に対する訴追の法的な問題

1 実体的な問題点

わが国で、いわゆる不正アクセスに対する刑事的処罰がかけており、共罰性の観点からも問題があるとして、これに対する法的な処罰が議論されている(注13)。もっとも、わが国ではなにをもって「不正アクセス」というかが問題である。従来は、

・侵入
・利用不能攻撃
・なりすまし
・トロイの木馬・Webトロイの木馬

などすべてについて、「不正アクセス」という用語をもちいて論じており、その議論の焦点がさだまっていないものであった 。すくなくても、「不正アクセス」という用語を無権限アクセスという趣旨に限定してもちいて議論すべきであろう(注14)。また、行為態様にしても、領得の意思のある場合と、データ正確性の侵害の場合、見せびらかしの場合とでは、その違法性に違いがあるようにも思える。

2 わが国刑事法の立法管轄権-属地主義

クロスボーダー的な行為に対して刑事法が、どのように適用されるかという観点(国家管轄権の観点からいえば、立法管轄権の問題となろう)からすれば、属地主義の原則がある。しかしながら、コンピュータ犯罪については、

「保護主義」
・公務員等により作られるべき電磁的記録の不正作出・供用(刑法2条5号)
・電磁的公正証書原本不実記載・同供用
「属人主義」
・2条5号以外の電磁的記録の不正作出・供用
・電子計算機使用詐欺

ということになる。

その属地主義の一般論を考えたときに、いわゆる不正アクセスにともなっておこなわれる行為については、かかる規定の必要性があるのか否かという問題がある。刑法の属地主義については、犯罪地の決定が重要な意義をもっているとされている。そして、一般的には、混合説がとられているとして、「行為(身体の動静)のなされた地と結果の発生地たちとは、ともに犯罪地に含まれることになる。」とされているのである(注15)。そうだとすると、コンピュータ犯罪で問題となりそうなものは、わが国の領土内で管理されるコンピュータであろうから、そのコンピュータの機能不全に関する限り、わが国の刑法典が適用さることになる。すると、上記の保護主義、属人主義の規定は、不必要になる。 また、パケットが、わが国の領土を通過した場合は、どうか。この場合には、従来の一般的な刑法の理解によれば、この場合にも属地主義の適用があるとされるものと考えられる。しかしながら、このような場合について、わが国の刑法が適用されるという考えは、やや、実際の感覚にあわないところである。また、サミット等の議論を見ていると、不正アクセスについては、どうも、行為地主義を念頭において議論がなされている。そうすると、コンピュータ犯罪については、一般犯罪とは異なり、犯罪地とは、行為地をいうということになるのであろうか。問題はあるところである。

(注1) http://www.mofa.go.jp/mofaj/gaiko/kaidan/summit/denver/com_kari.html

(注2)http://www.mofa.go.jp/mofaj/gaiko/kaidan/summit/lyon/tero.html

(注3)http://utl1.library.utoronto.ca/disk1/www/documents/g7/40pts.htm なお、「基本資料集 組織的犯罪と刑事法 -国際的動向とわが国の状況」法務省刑事局刑事法制課(有斐閣)P13に抄訳がある。

(注4) 共罰性の要件について前注の勧告3、電子的監視について勧告26参照

(注5)http://www.usdoj.gov/opa/pr/1997/December97/518cr.html

(注6)従来の議論の紹介として「情報システムの安全対策に関する中間報告書」情報システム安全対策研究会・警察庁・ http://www.npa.go.jp/soumu/jreport.htm第1編・3参照

(注7)http://www.tis.com/docs/products/recoverkey/rkeynews.html
http://www.hp.com/gsy/security/icf/main.html などを参照

(注8)安富潔「刑事手続きとコンピュータ犯罪」慶応義塾大学出版会株式会社・1992が、この問題を全般的に扱っている。

(注9)なお、安富・前出 p196参照

(注10) http://www.eff.org/pub/Legal/Cases/SJG/

(注11)http://www.epic.org/security/computer_search_guidelines.txt

(注12) 警察庁報告書 34ページ

(注13)警察庁報告書のほかにも、「高度情報通信社会に向けた環境整備に関する研究会報告書」(郵政省) (http://www.mpt.go.jp/pressrelease/japanese/tsusin/980310j502.html) その他

(注14)拙稿「不正アクセスについて」プレビュー版
(http://www.isc.meiji.ac.jp/~sumwel_h/junc/cmp_crime/cmp_crime-1998-1.htm)

(注15)森下 忠「国際刑法入門」悠々社 P.30

/e