平成 15 年度社会安全研究財団委託調査研究報告書

「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書

「犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得」
(司法省マニュアル)の翻訳とその解説

平成 16 年 3 月

序　「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書について

本報告書は、財団法人社会安全研究財団からの委託に基づいて、サイバー犯罪刑事手続調査委員会において、なした委託による調査の結果報告書である。サイバー犯罪刑事手続調査委員会は、米国のサイバー犯罪に対する刑事手続法の研究に、造詣の深い研究者で構成された研究会である。この調査報告書は、アメリカ合衆国司法省のコンピュータ犯罪および知的財産部刑事課の作成した「Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations(犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得)」と題するマニュアル(以下、便宜的に司法省マニュアルという)を翻訳・解説することにより我が国での今後のハイテク犯罪捜査における捜査手続についての検討に資することを目標とするものである。この報告書は、司法省マニュアルの翻訳と、そのマニュアルを理解するにあたって必要となる①基礎的な知識②参考となる判例③日本法との論点比較及び④コンピュータ法科学に関しての基礎的な知識とを併せて報告しているものである。

報告書自体は、上記司法省マニュアルが極めて大部なため、司法省マニュアルの翻訳である翻訳編とそれ以外の解説にかかわる解説編とに分けて作成されている。サイバー犯罪に対する米国の取り組みは、組織的、体系的、戦略的なものと評することができ、本研究会の翻訳した司法省マニュアルは、その米国の経験を、法的見地から記載したものとしては、きわめて優れたものと評価することができると思われる。研究会が、そのような貴重なマニュアルの翻訳に携わることができたことは極めて栄誉なことである。また本報告書が、今後の我が国におけるサイバー犯罪に対する適切な法執行の実現という目標のために、役に立てることがあれば、調査委員会としては、非常な喜びである。

平成 16 年 3 月

サイバー犯罪刑事手続調査委員会
委員長　高橋郁夫

サイバー犯罪刑事手続調査委員会委員
(なお、肩書は、平成 16 年 4 月現在)

高橋郁夫　弁護士・宇都宮大学工学部講師

安富　潔　　慶応義塾大学法学部教授

石井徹哉　千葉大学法経学部助教授

小島　淳　岡山大学法学部助教授

小川佳樹　筑波大学大学院人文社会科学研究科専任講師

(お断り)

なお、本報告書は、その対象としてアメリカ合衆国における連邦の法執行機関におけるハイテク犯罪に対する捜査を取り扱っている。そのために解説編および翻訳編において、連邦であることを当然の前提とした記述がある点については、ご了承いただきたい。

「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書

目　　次

第１章　アメリカ・ハイテク犯罪の歴史的意義と法執行機関の対応

第 1　前ハッキング時代-「ハッカー」の用語の発生(1960 年代から 1983 年まで)

コンピュータ犯罪・ハイテク犯罪という形態の犯罪の歴史は、古くから存在する[1]。しかしながら、１９８０年代以前については、ひとまとまりにして説明することが合理的なようにおもえる。１９６０年代以降、コンピュータが軍事用の目的から一般の民生用に用いられるようになり(銀行業務や資産移動も電子的業務に変わっていった)、そして、大学の研究機関での利用もはじまった。この当時の事情について「コンピュータ技術は、変革の時期を迎えた。」ということがいわれている。確かに従来に比較してコンピュータ利用者の数は急激に増加し、コンピュータ犯罪が議論されはじめ、セキュリティの問題が報道され始めたということはいえるが、しょせんは、まだ、一般化というのにはほど遠いものであった。また、実際のコンピュータ利用者のなかには、特殊のコミュニティが発生し、そのなかで、優秀なプログラミングの能力を持つものにたいして、「ハッカー」という尊称が与えられるようになっていった。この点について、ブルース・スターリングは、「ハッカーを追え」という本[2]の中で、「 『ハッカー』の精神的な祖先は、技術エリートの世界に、とくに 1960 年代の MIT やスタンフォート大学にたどることができる。」としており、メインフレームを備えていた大学の設備は、ハッカーの活躍の場となっていたのである。また、この言葉の意義を伝える記述として「ハッキングは、コンピュータと情報へのできる限り自由でオープンなアクセスへの決意ともいえる。」ともいわれているのである。

もっとも、この時期に（悪質な）ハッカー[3]が存在しなかったというわけではない。John Draper は、電話回線を開通させる特定の音をならすことによって長距離電話をタダ掛けした。この Draper は、"Captain Crunch" というハンドル名を拝命するにいたったのである。Yippie という社会活動が始まり、YIPL/TAP (Youth International Party Line/Technical Assistance Program)という雑誌が、長距離電話をタダでかけようとする電話ハッカー（ "phreaks"ともいわれる）の技術的後押しをしたのである。 また、電話システムをハックするのに使われる"blue boxes"という機械を作っていた California's Homebrew Computer Club の二人のメンバー、すなわち二人のスティーブ（Steve Jobs、ハンドル名は"Berkeley Blue"と Steve Wozniak、ハンドル名は"Oak Toebark" ）は、後にアップルコンピュータを設立するのである。

---

[1] 大橋充直「ハイテク犯罪捜査入門」（東京法令出版、2004）178 頁以下は、通信犯罪の歴史を紹介している。

[2] ブルース・スターリング著、今岡清訳「ハッカーを追え（原題“ Hacker Crackdown ”)」74 頁

[3] なお、本稿は、ハッカーという用語について、悪質なハッカーと尊称としてのハッカーを特にわけずに記載している。ご容赦いただきたい。

第 2 「ハッカー」出現時代(1983 年から 1988 年まで)

1．1983 年

1893 年は、世の中に「ハッカー」という名称を広く意識づけた年ということができるであろう。この年に、「ウォーゲーム」(ワーナー映画・高校生のデビットという少年は、核戦略プログラムにアクセスして、全面核戦争の脅威がおとずれるというストーリー)という映画が公開され、「ハッカー」という用語が、大衆の前にあらわれたということができる。この映画の影響について、「これがきっかけとなってその年のクリスマス・プレゼントでモデムが、バカ売れした。そして、突然、技術的にも、精神的にも、真のハッカーでない人間がハッキング・シーンに大挙して現れるようになった。電子掲示板システム(bbs)が、大流行し、相当な数の BBS が（悪質）ハッカーや warez doods(ソフトウェア海賊)やアナキストに娯楽を提供し、落ち着きをうしなった若者があふれだしたのだ」と述べられている。

セキュリティの観点からは、この年、いわゆるオレンジブック（NCSC(米国コンピュータ・セキュリティ・センター)が、国防省・「信頼しうるコンピュータシステム評価クライテリア」(TCSEC/Trusted Computer System Evaluation Criteria)が発表さていることが注目される。

2．1984 年および 1985 年まで

1894 年には、わが国で、外部者が、大阪工業大学中央研究所計算センターのコンピュータにアクセスし、保存されていたプログラムや研究データ、学生の成績を破壊したという事件が報道されている。1984 年には、米国においては、機密情報および機密外情報の保護指令が発表され、各政府機関の枠をこえてコンピューターセキュリティの推進を目的とする体制がつくられた。ハッカーコミュニティでは、1984 年には、「2600」マガジンが、創刊されており、その翌年の 1985 年 11 月 17 日には、セントルイスでオンライン雑誌「フラック」や、タラン・キングとナイトライトニングが運営するメタル・ショップ・プライベート BBS が創刊されている。また、Legion of Doom （「破滅の軍団」）（米国）やカオス・コンピュータ・クラブ（ドイツ）の活動が盛んであった。

3.1986 年から 1987 年

まず、法律的な観点から、1986 年には、いわゆる Computer Fraud and Abuse Act が定められ、無権限アクセスに対する処罰が、定められている点は注目に値する。

(1)「カッコウの卵」事件

天文学者であったクリフォード・ストールが、1986 年 8 月 1 日に、75 セントの課金のあやまりから、侵入者を発見していくことになる。この経過を記したのか、「カッコウは、コンピュータに卵を産む」であり[4]、ベストセラーになった。彼は、侵入者が、管理者の「スヴェンテク」というものの名義になりすまし、電話を用いてダイアルアップでポート tt23 にアクセスしている(1200 ボー)ことを発見して、そのキー操作をプリントアウトとしていった。それをみると、カッコウが、他の鳥の卵でも返すように、偽のプログラムを実行させて、

[4] クリフォード・ストール著、池　央耿訳「カッコウは、コンピュータに卵を産む」（草思社、1991）

スーパーユーザーになりすますというテクニックを用いていた。そして、その経路を探索している内にこの悪質なハッカーは、軍用のネットワークに侵入し、アニストン陸軍兵站部に侵入をしていたことに気がついた。この悪質なハッカーは、CIA にも、侵入しようとしたのである。この侵入に対する捜査の結果、マーカス・ヘスが、逮捕され、また、「カオス・コンピュータ・クラブ」が、コンピュータシステムに侵入していたことが判明している。もっとも、ヘスについては、嫌疑不十分で、釈放されている。

（2） シャドウ・ホーク事件

1987 年 6 月 6 日には、シャドウ・ホークというクラッカーが、逮捕されている。彼は、本名をハーバード・ジンといい、「FBI やシークレットサービスや犯罪調査 service やシカゴ警察をきりきり舞いさせながら、AT&T への侵入だけではなく、NATO や合衆国空軍のコンピュータへも侵入して 100 万ドル相当以上のソフトウェアを盗み出したのである」とされている。この事件は、「この事件が重要なのは、これが、1986 年に制定されたコンピュータ詐欺乱用法が初めて適用された例」とされている。(文献によっては、シャドウ・ホーク事件については、1987 年 9 月 17 日に司法省が発表したものとされている)

（3） 逮捕された（悪質）ハッカー達

マクドナルトに侵入した "Fry Guy"という（悪質）ハッカーが逮捕され、また、アトランタでは、「破滅の軍団」のメンバーである "Prophet," "Leftist" "Urvile"などが逮捕された[5]。

第３ ジャイアントワームとサンデビィル作戦(1988 年から 1990 年)

1. ジャイアントワーム事件（1988 年）

「コンピューターセキュリティの基礎」という本[6]は、1988 年のジャイアントワームの襲来をその書き出しにしており、また、「Cyberpunk-Outlaws and Hackers on the Computer Frontier」[7]でも、その第 3 章 rtm は、このウイルスの作者であるロバート・モリスについて詳細に触れている。

この事件の内容を若干詳細に照会すると、1988 年 11 月 2 日、コンピューターワームといわれるプログラムが、ネットワークを通じてコンピュータからコンピュータに伝染していった。このウイルスは、sendmail というプログラムのセキュリティホールなどをついて「偵察兵」プログラムを送り、それを用いて、コンピュータに侵入し、侵入すると、バックグランドで走ったりしながら、プロセスを生成し、たちまち、メモリ領域を食いつくし、ついに他の処理をストップさせてしまうというものであった。このプログラムの作者は、ロバート・タッパン・モリスであった。彼は、NSA(国家安全保安局)のコンピュータ・セキュリティ・

---

[5] フライガイの逮捕については、前出（注 2）152 頁、破滅の軍団の３名の逮捕については、同 162 頁

[6] Deborah Russell ,G.T.Gangemi Sr. 共著、山口英翻訳「コンピュータセキュリティの基礎」アスキー (1994)

[7] ケイティー・ハフナー＋ジョン・マルコフ著、服部桂訳「ハッカーは笑う」（NTT 出版、

センターの主任研究員であるボブ・モリスの息子であった。彼は、このワームを作るに際して、悪意をもって、システムを破壊していこうとしたものではなかったとされており、感染率の数字のミスをしてしまったことが原因でこのような結果を導いてしまったのである。プログラムを見ただけで、彼がワームをなるべく多くのコンピュータの中に住まわせようとしただけで、害を与えようとデザインしたのではないことは明らかであった。

結局、彼は、1990 年 1 月 23 日に 1986 Computer Fraud and Abuse Act 違反で有罪の認定がなされて、1990 年 5 月 4 日に、執行猶予 3 年 罰金 1 万ドル・400 時間の社会奉仕の刑が言い渡された。

2. サンデビィル作戦（1990 年）

米国におけるスティーブ・ジャクソンゲームズ事件は、わが国におけるコンピュータの捜索・差押の問題について、具体的な問題を紹介してくれる。この事件は、有名な「サンデビィル作戦」に関連して起こった。(もっとも、この「サンデビィル作戦」は、厳密になにをその対象としてかたるかという点では、微妙な争いがあるようである。) その点は、さておき、スティーブ・ジャクソン事件は、前出（注２）の「ハッカーを追え」に詳しく述べられている（事実関係については、その第 5 章などを参照されたい)。また、本解説編の第２章 Steve Jackson Games 事件の判決紹介においても、このサンデビィル作戦ついての事実関係が触れられている。

3. EFF の結成

スティーブ・ジャクソンゲームズ事件は、従来からのネットワークコミュニティの住人達にとっては、法執行機関が、かれらの領域に「土足で」あがりこんできたように見えた。そこでオンラインでの個人の権利を擁護するために、ション・ペリー・バーロウ(グレイトフル・デッドの作詞家)とミッチ・ケイポア(ロータス 1-2-3 の作家)は、1990 年の 6 月に EFF（http://www.eff.org）を設立した。EFF は、その後、スティーブ・ジャクソンゲームズ事件の支援や暗号問題における市民の啓蒙などで重要な役割を果たし、その後のオンラインでの人権を擁護する市民団体の先駆けとなったということができる。

第４　インターネットの夜明けと「伝説のハッカー」（1991 年から 1995 年）

1.ネットワークの一般化とインターネットの夜明け

商用のネットワーク利用者の数は増え続け、特に米国では、1990 年代に入ると、大手商用ネットワークが大きな人気を集め、また、同行者による草の根ＢＢＳなども人気を集めた。商用ネットワークでは、当時ＢＩＧ５といわれた Prodigy，CompuServe，AmericaOnline，GEnie，DELPHI が、規模の大きな所は、それぞれ 100 万人単位の会員を擁しており、合計で、1994 年には 400 万人から 500 万人の会員を集めていた。

1995）

また、1993 年には、クリントン＝ゴア政権が誕生する。ここで、ＮＩＩ構想が語られ[8]情報スーパーハイウエイ構想として、一世を風靡することとなる。その頃、ＮＣＳＡの Mosaic が開発された。従来のネットワーク環境は、主として文字だけの情報提供だったのに加えて、写真などの情報を豊富に表現する能力をそなえたこのブラウザがいかに革命的であったか、いうまでもないことであり、まさにその後のインターネットの爆発を支える大きな転換点となったのである。

前述したスティーブ・ジャクソンゲームズ事件における判決が言い渡されたのは、1993 年３月のことであり、これにおいて、捜査に際して、関連する法律や技術について十分な知識が必要であるという観点から、司法省において、捜索・差押えガイドラインが準備された[9]（1994 年）。

また、その一方で暗号技術の進化と法執行の利益との調和という観点から、暗号技術についていわゆるクリッパーチップ構想が発表された[10]。この暗号をめぐる問題は、きわめて激しい論争を提起し、これらをめぐる一連の論争は、暗号問題といわれた。とくに初期において、デジタル式の電話を巡って、一定の解読方法を準備しておくべきではないかという観点から議論されていたのであるが、すぐに、むしろ、コンピュータにおける暗号によるデータの保存やメールの暗号化の問題として、議論されるようになっていったのは、ちょうど、この時期において、ネットワークが如何に急速に一般化していったかを物語っている。

2. ケビン・ミトニック事件

このような時代のなかで、ケビン・ミトニックの逮捕をめぐる報道は、いわゆるダークサイドハッカーをめぐる逮捕劇として米国の話題をさらった。ケビン・ミトニックという「一人でいるのが好きで、女の子に対しても奥手であった」男の子は、17 才の時にパシフィック・ベルのコンピュータに不正侵入し、電話料金を書き換えるなどの行為をなし、それ以外にも、サンフランシスコの企業から 20 万ドル相当のデータを盗み出したと噂されていた。その後、更生施設に 6 か月入った後、保護観察付きで釈放された。1988 年に再度、逮捕(DEC のコンピュータに400万ドルの損害を与えたとの被疑事実-司法取引では16万ドルと主張が変更される)され、メトロポリタン拘置所の独房で 8 ケ月、海岸沿いのロムポックで 4 ケ月、中間施設で 6 ケ月過ごした後、実社会に復帰という経歴を有していた。彼は、実社会に復帰する際に、保護観察に付されていたが、その後、1992 年 12 月 7 日に保護観察を逃れて、逃亡した。彼を逮捕するべく、シモムラ・ツトムおよび作家のジョン・マーコフにより追跡が

---

[8] アジェンダについては、
http://www.eff.org/Infrastructure/Govt_docs/nii_agenda_govt.paper 参照。

[9] “FEDERAL GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS”（http://www.epic.org/security/computer_search_guidelines.txt）

[10] なお、暗号論争については、情報セキュリティ調査研究会「情報セキュリティ調査研究報告書」（http://www.npa.go.jp/hightech/sec_repo/title.htm）や情報セキュリティビジョン策定委員会「情報セキュリティビジョン策定委員会報告書～安全なネットワーク社会を目指

なされ、1995 年 2 月 15 日 逮捕 された。逃亡生活中の追跡劇をめぐって、「テイクダウン」「ハッカーは笑う」「FBI が恐れた伝説のハッカー」「ハッカーを撃て」などの本が、相対立する観点から著された。それらは、ベストセラーにもなり、ミトニックを逮捕したシモムラ・ツトムは、有名人になった。捜査の結果、ミトニックは、3 年以上にわたって多くのコンピュータ・ネットワークに侵入し、何千ものクレジットカード番号にアクセスし、ソフトウェアを盗んだことを認め、結局、アメリカ連邦地裁は 1999 年 8 月 9 日(米国時間)、禁固 3 年 10 月、罰金 4125 ドルの有罪判決を言い渡した。このケビン・ミトニックをめぐる逮捕劇は、マスメディアでも取り上げられ、一般社会の注目を集めることとなった。

3. シティバンク侵入事件

また、1995 年には、シティバンクのコンピュータに対する侵入事件が起きる。これは、ロシアのコンピータープログラマーであった Vladimir Levin Levin が、ロシアのサンクト・ペテルブルグ市所在のパーソナルコンピューターを用いてアメリカのニュージャージーのシティバンクのコンピュータに侵入し、Levin は、プログラマーとしてのスキルを用いて、顧客の取引をモニターして、ロシアの共犯者の口座に振り込ませたという事件である。Levin は、英国に旅行した時に Heathrow 空港で逮捕され、合衆国政府からの要請により犯罪人引渡法のもと拘留され、その後、有線詐欺、銀行詐欺、およびそれらの罪を共謀したということで、起訴された。しかしながら、有線詐欺ないし銀行詐欺の構成要件に匹敵するものは、英国にはなく、検察当局は、行為と行動の詳細を論じ、イングランドとウエールズにおいてコンピューター・ミスユース法の無権限アクセスと無権限改変を含む 66 の犯罪を成立させているとしたのである。1998 年２月、米国の裁判所は、彼に３年の懲役と $240,000 ドルを賠償金として支払うように命じている。

4.ウインドウズ 95 の発売とインターネットの爆発的な普及

1995 年 8 月(米国)に発売されたマイクロソフト社のウインドウズ 95 は、爆発的な人気を見せ、これをきっかけにインターネットは、普及期にはいったものということができよう。

第 5　ハイテク犯罪の多様化と対応への努力(1996 年から 1999 年)

1.コンピュータ侵入テクニックの一般化

この頃から、いわゆるコンピュータ侵入は、きわめて一般的な出来ごとになって行ったとされる。ハッカーは、アメリカ司法省、アメリカ空軍、ＣＩＡ、ＮＡＳＡその他を含む連邦のウェブサイトに侵入して、サイトを書き換えたりした。会計検査院によるレポートで、国防総省コンピュータが 1995 年だけでもハッカーによって 250,000 の攻撃を継続して受けたことが明らかになっている。

スーパーボウル XXXII(1998 年 1 月)の TV 中継においては、 Network Associates 社は、きわめて膨大な広告料を支払い、ハッカーから、虚偽の命令がくるのではないかと心配するミ

して～」（http://www.npa.go.jp/hightech/secv_repo/about.htm）を参照のこと。

サイル技師の姿を描写した反ハッカーのテレビ広告をながした。また、同月、労働統計局は、虚偽の申請情報によって機能不善に陥らされた。また、ハッカーは、ペンタゴンのネットワークに侵入して、軍事衛星システムのソフトウェアを窃取したりした。

2. コンピュータウイルスをめぐる事件の出現

また、モリス事件以来、コンピュータウイルスに関連する法的事件は、注目すべきものは報告されていなかったが、1996 年以降、アメリカ合衆国対サブラン （アメリカ合衆国連邦控訴審裁判所第九巡回区裁判所 1996 年)、アメリカ合衆国対ツビンスキ （アメリカ合衆国連邦控訴審裁判所第一巡回区裁判所 1997 年)、バウチャー対グリーンフィールド教育委員会（アメリカ合衆国連邦控訴審裁判所第七巡回区裁判所 1998 年）などが出現している。

3. デンバーサミット・コミュニケ 40 での「ハイテク犯罪対策」にむけての動き

1997 年 7 月の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、コミュニケの４０番において、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、訴追及び処罰に対応する態勢と、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態勢とを目指すとハイテク犯罪に対する対応を宣言している。これを受け、1997 年 12 月 10 日には、ワシントンで 8 ケ国司法・内務閣僚級会合が開かれ、ハイテク犯罪を捜査訴追する能力を高めることと犯罪人引渡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合意した。ワシントンでの 8 ケ国司法・内務閣僚級会合の後も、翌 98 年のバーミンガム・サミットでもハイテク犯罪対策が議論されているし、ハイテク犯罪対策に対しての各国の協力にむけての動きは、さらに活発に、そして、産業界との協力も含めてますます盛んになっている。

4. ハイテク犯罪対応部局の整備

NII 構想の成功は、アメリカの経済をより効率的にかつ強靱にしたものと言うことができる。しかし、同時に電子情報テクノロジーによって、リンクされている重要な経済インフラ-電気、エネルギー、交通、電信電話、銀行・金融、医療サービス、政府機能などは、より攻撃に対して脆弱になってきているということができる。 これらの認識を前提に、1996 年 7 月 15 日には、重要インフラ防衛について、大統領令 13010 が発表され[11]た。この大統領令に基づいて委員会(President's Commission on Critical Infrastructure Protection)が組織された(http://www.info-sec.com/pccip/web/index.html) 。その委員会は、 度々会議を重ね 1997 年 10 月には、レポートを発表している[12] 。

これらの考察の結果として、レポートは、「サイバースペースにおけるルールの変更-新思考の必要性」「未来を防衛するためにいま行動すべき」「インフラの保証は、分割責任」という結論に達している。「サイバースペースにおけるルールの変更-新思考の必要性」というの

---

11 http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us/1996/7/15/1.text.2

12 会議の経緯については http://www.info-sec.com/pccip/web/whatsnew.html、レポートについては http://www.info-sec.com/pccip/web/report_index.html

は、とくにサイバースペースには国境がないこと、および、物理的な証拠を残さずに攻撃をなすことができることによるものである。そのために、国防と国内の法執行の責任をわけていた従来の公式は当てはまらなくなるというのである。「未来を防衛するためにいま行動すべき」というのは、現時点では、重大な攻撃や脅威があり国家的な危機を招いているというわけではないことを前提としている。しかしながら、攻撃にかける費用が低下している以上、脆弱性が増しているということはいえるのであって、嵐のやってくる前に準備をしなくてはならないのである。 「インフラの保証は、分割責任」国防は、軍事的力以上のものを必要とする。国際社会での地位、影響力、生活力などは、経済的反映と国民の自身に裏付けられている。その一方で、軍事力の効率的な運用は、インフラの利用にかかってきている。とくに通信および輸送次第であるといえる。 これらの結論を前提に「意識と教育の広範なプログラム」「産業界の協力および情報シェアを通じたインフラ防衛」「インフラ防衛に関連する法律についての再検討」「調査・開発についてのプログラムの改定」「国家的機構構造」が提案された。

上述の PCCIP レポートの提案に呼応し、1998 年の 2 月には、NIPC が FBI 本部に設立されている[13]。この組織は、犯罪捜査および国家安全保証部合同セクションとなっている。

この NIPC の使命は、重要インフラに対して脅威となり、ないしは、それを対象とするコンピュータ侵入や違法行為を探知し、防止し、評価し、警告し、対応し、捜査するための、国家安全および法執行の努力することである。 また、1998 年５月２２日に、クリントン大統領は、テロリズムやその他の従来的ではない脅威に対応するための二つの大統領令を発表した。そのうちでとくに PDD63 は、重要インフラを物理的ないしはサイバー攻撃から防衛することに注目するものである。 この内容については、ホワイトペーパー (http://www.usdoj.gov/criminal/cybercrime/white_pr.htm) に詳細である。

なお、コンピュータ捜索差押ガイドラインは、1997 年と 1999 年に改定されている。

5. Melissa ウイルス事件

1999 年 3 月末に流行した Melissa マクロウイルスは、Microsoft の Outlook というメーラの MAPI と呼ばれるインタフェィスと Word というワードプロセッサ機能を利用するものである。電子メールに添付されてきた Word 文書ファイルのマクロの中に、この Melissa マクロウイルスがある場合、ユーザがこの添付ファイルを開くと勝手にメーラにあるアドレス張の中の電子メールアドレス宛に自己の複製を送信してしまうものである。

その後、その犯人として David L. Smith がニュージャージー州法に基づいて逮捕された。Smith はまず、8 月の時点で自らが Melissa ウイルスを作り出したことを認めた。そして 12 月 8 日には 100 万のコンピュータシステムに影響を及ぼして、8000 万ドルの損害を引き起こしたことを認め、司法取引に応じた。この司法取引のリリースを分析することによって、メリッサ事件に対するアメリカにおける刑罰法規の適用状況が明らかになる。一般情報、司

---

[13] http://www.fbi.gov/nipc/nipc.htm なお、NIPC については、情報処理振興事業協会「米国政府関連のコンピュータウイルス対策等組織調査報告書」5 頁以下参照。

法取引の申し入れの書類、当時のプレスリリースなどから、David Smith は、故意に、意図的に "Melissa virus"を送信し、その結果として、保護されたコンピュータを権限なしに損害を惹起したのであって、これは、連邦刑法の Title 18、Sections 1030(a)(5)(A) and 2.違反である。 ニュージャージー地区連邦検察官は、これを認めるのであれば、その他の訴因については、これを維持しないという申し入れをしているのである。
また、翌 12 月 9 日に発表されたプレスリリースによれば、Smiths は、州法違反としては、第 2 級コンピュータ関連窃盗の訴因を認め、州は、もっとも長期の 10 年の服役を要求している。また、損害を惹起する意図で、コンピュータウイルスを故意に拡散した罪で、有罪を認めている。

第 6 パトリオット法と現代社会におけるハイテク犯罪(2000 年以降)

1.商用サイトに対する分散サービス妨害(2000 年 2 月)

米国時間の 2 月 7 日から 8 日にかけて、インターネットの有名サイトが相次いで悪質なハッカーに攻撃され、一般利用者がアクセスできなくなった。7 日はヤフーが狙われ、約 3 時間一部のサービスがアクセス不能に陥り、8 日に入ってから e ベイやアマゾン・コム、バイ・コム、CNN が軒並み同じ被害を受けた。この犯人については、16 才のカナダの「マフィアボーイ」というハンドルをもつ少年が逮捕され、罪を犯したことを認めたと報道されている。

2. ラブレターウイルス事件 (2000 年 5 月)

これは、2000 年 5 月 5 日には、世界的に相当な被害が報告されたコンピュータウイルスである。このウイルスは「I LOVE YOU」と題した電子メールで送られ、添付された「LOVE-LETTER-FOR-YOU」というファイルを開くと感染したコンピュータに登録されている住所録すべてにウイルスの付いた電子メールを送信し、「増殖」する。米国では、国防国防総省、中央情報局など政府機関や国連本部、大企業などに被害が広がった。ある報道によると、「米カリフォルニア州のコンピューター・エコノミクス社の推計では、世界で 4500 万台が感染メールを受け取り、被害額は 4 日だけで約 26 億ドル（約 2820 億円）、最終的には 100 億ドルに達する恐れもあるという。」とされた。ラブレターウイルスの作者については、フィリピン・マニラ市在住の銀行勤務の女性と内縁の夫が逮捕されたが、拘束を続ける十分な証拠がないとして釈放されており、真相はいまだに明らかではない。

3.司法省捜索差押マニュアルの公開（2001 年）

1994 年に公開された司法省「コンピュータ捜索差押ガイドライン」であるが、その後、何度かの改訂を経ていたものの、2001 年には、「捜索差押マニュアル」として全面的に新しく生まれ変わった。1994 年版においては、初歩的な技術用語の説明などにもページが割かれていたが、この 2001 年版においては、むしろ、法的な解釈論や具体的な判決の解釈などが中心におかれるようになっている。

4. 911 事件とパトリオット法などの成立

2001 年９月 11 日の米国に対する同時多発テロは、サイバーセキュリティに対しても、き

わめて大きな影響与えている。特にパトリオット法といわれるテロ防止法案(“Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001”)の内容は、きわめて重要な変革を及ぼすものである。法案の中で、2005 年 12 月に失効しない条項で、ネットワーク上のセキュリティに関連する条項としては、以下のようなものがあげられる。

(ア)　連邦検事もしくは各州の検事総長は、連邦捜査局(FBI)の電子メール傍受システム『カーニボー』の設置を命令し、訪問したウエブページのアドレスや電子メールのやりとりを記録できる。この際、裁判官による許可は不要とされている。これは、これまで、カーニボーなどのインターネット監視技術の使用には、厳しい法的規制が定められていたものを改めたものである。

(イ)　裁判所命令がなくとも、FBI が「国際的テロ活動防止を目的とした正式な捜査に関連する記録」だと主張した場合、インターネット・サービス・プロバイダ(ISP)あるいは電話事業者各社は、発信した相手先の電話番号も含む顧客情報を FBI に提出しなければならないとされている。

(ウ)　テロリズムについての現在の定義を根本的に見直し、これを拡大して、生物化学兵器による攻撃やコンピュータへのハッキング行為も含めることとする。これによれば、現在横行しているいくつかのコンピュータ犯罪――米連邦政府のコンピュータシステムへの不正侵入行為や、インターネットに接続されたコンピュータに侵入して被害を与える行為など――もこれでカバーされることになる。

(エ)　その上、「サイバーテロ」という新しい犯罪項目を追加する。これは、年間「少なくとも合計 5000 ドル」の金銭的損失、医療機器への被害、「人間に対する身体的危害」の原因となるハッキング行為を指す。有罪判決を受けた場合、刑期は 5～20 年とされている。

このパトリオット法による改正の詳細については、本解説編・石井論文参照のこと。また、パトリオット法の改正を受けて捜索・差押マニュアルが、2002 年７月に改訂版が発表されている。翻訳の対象としたのは、この版である。

また、2002 年には、「2002 年国土安全保障法（Homeland Security Act of 2002）」が成立し、米国内の安全保障を総括する「国土安全保障省（The Department of Homeland Security）」が新設されることとなった。「国土安全保障省」は、安全保障に関連する 22 の政府機関を統合した。

5.セキュアなサイバースペースのための国家戦略[14]（The National Strategy to Secure Cyberspace）など

2003 年 2 月 14 日、ホワイトハウスより「セキュアなサイバースペースのための国家戦略」が、発表された。その戦略は、その戦略目標として①アメリカの重要インフラに対して、

[14] http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

サイバー攻撃を予防すること、②サイバー攻撃に対する国家的な脆弱性を減少させること、③起きてしまったサイバー攻撃からの損害と回復にかかる時間を最小限にすることを戦略的目標としている。そして、そのために、特に、以下の 5 つの国家的な優先事項を明記している。その優先事項とは、① 国家的なサイバーセキュリティ対応システム ② 国家的なサイバースペースの脅威と脆弱性の低減計画③ 国家的なサイバースペースセキュリティの啓発と訓練計画 ④ 政府サイバースペースのセキュリティ確保、そして⑤ 国家安全保障と国際的なサイバースペースセキュリティの協力国際的対策の発展などである。

付録１　司法省連邦検察官 De Marco 氏との会議録

日時：2003 年 12 月 11 日午後３時より午後５時 30 分（現地時間）
場所：司法省連邦検察官ニューヨーク南部地区事務所

参加者：

米国側：連邦検察官 Joseph De Marco
日本側：高橋郁夫(弁護士、宇都宮大学講師)
石井徹哉(奈良産業大学助教授、刑事法)
小島　淳(岡山大学助教授、刑事訴訟法)

会談に先立ち、本件におけるコメントが De Marco 氏個人のものであり、連邦政府、司法省を代表するものではないとの断りがあった。会談は、あらかじめ送付してあった質問事項に基づきおこなわれた。

１　法執行と司法省に関する概要

まず、司法省および連邦検察官事務所等、コンピュータ犯罪捜査にかかわる組織・リソースの概要について説明がなされ、その概要は以下の通りである。

(1)　連邦検察官事務所について

連邦検察官事務所は、合衆国の各州にすくなくとも一つ存在しており、全部で 92 の事務所が存在している。ニューヨークには四つの事務所があり、本会談の場所である南部地区事務所は、マンハッタン、ブロンクスの他、ニューヨーク州のアルバーニーより南側の地区をその所轄としている（カリフォルニア州には五つ事務所がある）。これらの事務所に勤務する連邦検察官は全部で 180 名で、いくつかの部門(Unit)に分かれて配属されている。そのような部門としては、麻薬関係の部門、暴力犯罪の部門、租税犯罪部門およびコンピュータ犯罪関係の部門があり、この南部地区事務所のコンピュータ犯罪関係の部門では、De Marco 氏を含め５名の連邦検察官とパラリーガル１名が配属されている。

コンピュータ関連犯罪は、通常、連邦レベルで取り扱われる。それは人材およびリソースが充実していることによる。これを担当するコンピュータ犯罪に関する部門は、二つのカテゴリーについて訴追等の責任をもつ。第一はいわゆるコンピュータ犯罪であり、ハッキング、コンピュータスパイ、ワーム、ウイルス、ウエブページの破壊、インターネットを通じての脅迫（恐喝）、詐欺などがこれにあたる。第二は知的財産権に関する犯罪であり、著作権・商標権の侵害、ソフトウェアの海賊版作成、産業スパイなどがこれに含まれる。

なお、児童ポルノは一般犯罪に関する部門が担当している。それは捜査がさほど困難ではないことによる。たしかに児童ポルノの犯罪の数は多いものの、各州の法執行機関も問題なく仕事をこなしているからである。さらに、児童ポルノと犯罪組織(Gang)とのつながりはそ

れほど強くはなく、買春ツアーなどのほうが犯罪組織との結びつきが強いといえる。

連邦検察官事務所は、FBI、シークレットサービス、連邦郵政監査局などの捜査機関と協力して捜査を行い、これらの機関において一定の捜査が完了したのちに、事件が、各種の証拠とともに連邦検察事務所に上がってくる仕組みになっている。これは日本の場合と同様であろう。

(2) 司法省（ワシントン D.C.）の組織について

ワシントンの本部（司法省）には、コンピュータ犯罪および知的財産部(CCIPS)があり、その他にも多種の問題に応じていろいろな部局が存在し、政策問題や立法問題までも取り扱っている。司法省では、司法長官の下に、各犯罪局の局長がおり、その下に各部の部長が配置されるという構造になっている。各地方にも同様の組織が存在しているものの、ワシントンの本部と上下関係に立つわけではない。

(3) CTC について

各事務所の連邦検察官が CTC として任命され、ここニューヨーク南部地区事務所では、De Marco 氏が CTC として任命されている。CTC になるには、特別なトレーニングおよび外部機関でのプログラムに参加することが必要であり、それにより CTC の資格を得ることができる。CTC に任命されると、特別の器具等を付与され、担当のアシスタントがつくことになる。また年間を通じてワシントンの本部が用意する各種の会議に参加し、関連法規およびテクノロジーについて遅れを取らないよう努めることになる（CTC 以外にも、医師や安全保障に関する専門官もある）。FBI のアカデミーでトレーニングを受けた FBI 捜査官のなかに、専門技術を持った者がおり、そのような者と協力して CTC のトレーニングの特別なプログラムを用意することもある。

法執行官は、CCIPS に対してきわめて頻繁に連絡をとっており、捜査権限が中央に集中していないことに諸外国の人は驚くようである。たとえば、オランダでは検察官の１つのグループがが全国の犯罪を手がけている。合衆国の場合、50 州のそれぞれに郡(county)が存在し、そこでコンピュータ犯罪を担当する者がいる。司法省および連邦検察官事務所の組織の構造が水平的であるため、誰がなにを担当しているかという質問に答えるのは、合衆国の場合難しいことになる（オランダの場合は簡単であろう）。また、インターネットは、境界が存在しないため、相互によく連絡をとるようにしており、各地区の境界を越えて共同して作業するようになっている。このような共働のために創設されたのが CTC であり、CTC の存在により担当する者が容易にわかるようになっており、境界を越えた作業が容易になっている。たとえば、ニューヨークにいても、マイアミの捜索令状を現地の担当者に依頼して、取得してもらうことができる。

２　司法省の捜索・押収マニュアルの意義

司法省のマニュアルは、一般的なガイドであり、実務に関する最良の提言をなすにすぎず、捜索・押収をなす理想的な状況があるときにどうしたらよいかを述べたものである。もっと

も、理想的な状況というのはあまりない。

令状の起草や捜索を計画するときにチームをどのように編成するのかという点では、これは事案によってはチームを編成することが困難な場合があることに注意を要する。たとえば、証拠を破損するとかラップトップを抱えて逃げてしまうということがありえ、その場合に１時間以内に令状を取得することや、そのために各方面の関係者に対して短時間で調整するのはたいへんである。

令状を作成するまでに時間を要した事案を例としてあげる。この事案では、ISP を自宅で提供しており、その顧客も多かったのであるが、たった一人が通常のビジネスマンで、犯罪に関与していたものである。繰り返すと、重要なのは、犯罪の証拠を手に入れるということとホームビジネスとして ISP を運営していたというものである。その ISP のオーナーが最初からその顧客の犯罪関与を認識していたのか、あるいはその犯罪自体に関与していたかは、わからない状況にあった。この場合において、捜索令状を請求する前にオーナーに事情聴取することは望ましくない。もし相手が犯罪行為に関与していたならば、事情聴取によって、証拠を隠滅・毀損してしまうおそれがあったからである。そこで、令状を入手してから、事情をきくことにした。

次に、令状を執行する際に、自宅に乗り込んでいき、そのコンピュータを全部押収してしまえば、正当な業務を侵害することになる。そこで、この事件では長い期間をかけて捜索のための準備をおこなう捜査をおこなった。幸いにも十分な時間があり、どのような形で捜索を行うかを、捜索実施機関とともに十分に検討することができ、原案を作る過程でどのような形態で対応するのかを検討した。大規模なチームを編成し、多くの捜索のための器具・機器を用意し、次に述べるような各種の詳細な事項を記載した捜索令状を用意した。捜索の実施にあたっては、対象者の家に赴き、コンピュータおよびサーバを５セットに区分してミラーリングをして、捜索をおこなった。すべてのコンピュータを一度に全部まとめてミラーリングをせずに、コンピュータを５セットに分けてミラーリングをし、各セットごとに 20 分以内でミラーリングしましたので、合計しても 100 分以内ですべてのコンピュータをミラーし終え、ビジネスへの影響を最小限に食い止めることができた。

もっとも、一般的には、個人のラップトップを捜索することのほうが多いわけで、この場合にも、担当の捜査官と話し合ったりすることはあるものの、重要なのは押収するデータと捜索対象との同一性が確保されていればたりるといえる。

３　データに対する捜索・差押

データ自体について捜索･差押が有体物に対する場合と比較してどのように異なるのかということについていえば、両者にその相違はないといえる。要は「証拠」を収集することは認められており、捜索・差押えでは、対象物が証拠となりうるか、犯罪の道具となっているか、その成果物か、という観点からみているのである。ラップトップ・コンピュータでウイルスを生成したものが証拠となる場合もあれば、無形のデータが証拠となる場合もある。

合衆国では、有体物かそれ以外かということでは区別は存在しない。企業秘密はその一例である。企業秘密は盗まれるものであり、隠匿され、持ち去られるものであり、「相当な理由」があれば、無形でもいい。ウイルスそれ自体は無体物であっても、捜索の対象物件は有体物となり、証拠は無体物である。証拠が頭のなかに入っていれば、捜索の対象は人の頭になりうる。令状の対象になるデータの含まれている有体物であるコンピュータについては、たとえばこのベットルームにおかれているという特定がされなくてはならない。モデルナンバーやシリアルナンバーもはっきりさせなければならない。部屋番号もはっきりさせなければならない。ただし、捜索の対象となるのは有体物であるが、証拠として押収されるのはデータである。日本でも、実務上の取り扱いは同様であろう。

４　無令状捜索に関する問題

無令状捜索が可能となる例外要件に該当する場合であっても、できれば令状をもって捜索する方が望ましいといえる。既存の令状に関する要件は（例外の点も含め）コンピュータ犯罪にも適用される。実際にも、無令状捜索が可能であっても、あらかじめ令状を用意していくことがある。たとえば、同意がとれるかどうかはっきりしないときなどは、令状をとっておくことがある。令状がないとみると、同意をせずに、その場で証拠が隠滅されるおそれがあるからである。念のため令状を用意しておく場合として考えられるのは、押収品目録作成のための捜索がある。たとえば、逮捕されたときに住所録をもっている場合には、それをみてもかまわない。一方、コンピュータ関連の文脈においては、ポケットベルや携帯電話をみつけた場合に同様のことをしてよいのかについては、判例は分かれている。通信履歴をスクロールしてもよいと判示した裁判所もあれば、それをしてはいけないとする裁判所もある。そこで、実際にも捜査官がポケベルの住所録をみていいかどうかについて電話をかけてきいてくることがあるが、令状をとった方が無難であると回答することにしている。

５　証拠の原本性を確保する方法

データそれ自体とそのコピーのいずれについても証拠として許容される。これはコンピュータのデータの場合であっても同様である。コピーであったとしても、公正かつ正確な複製であるといえればたりるのである。原本を証拠として使用できる場合はそのまま証拠として提出することもある。たとえばラップトップを捜索してそのなかにウイルスを発見した場合、当該ラップトップ自体を証拠として提出する。なぜなら、その物自体に、指紋が付着しているなどして、証拠として独自の価値がある場合もあるからである。あるいは、直接陪審員に対してこれを示し、被告人がまさにこのコンピュータを用いてウイルスを発生させたということを説明するということもできる。原本を証拠とするか、コピーを原本として扱うのかということは、陪審ではなく、裁判長が決める。日本の場合は、コピーを新たな原本として扱うのであろうか。

６　現場外でのコンピュータを捜索する場合

通常、コンピュータの捜索は現場外でおこなわれ、令状にその旨を記載している。たいていは環境の整備されたラボで捜索されることになる。現場でのコンピュータの捜索は時間がかかりすぎるという問題がある。

ネットワークドライブに対する捜索・差押、いわゆるリモート捜索は難しい問題である。一般的に捜査機関はリモート捜索をすることはできないといってよい。これに関する規則は次の通りである（マニュアルにも同様の記載がある）。

まず捜索の対象が ISP のコンピュータである場合、電子メールが未開封または発信から 180 日以内であるとき、ISP に対する令状（提出命令としてのサピーナ）が必要である。この場合、ISP 自身が捜索をおこない、ディスク等を捜査機関に提出することになる。電子メールが開封済みであり、あるいは、発信から 180 日をこえているときは、2703 条ｄに基づく命令が必要となる。この場合、要求される証明のレベルは若干緩和されることになる。ISP 以外の第三者のコンピュータを捜索の対象とする場合には、提出命令または当該第三者の同意が必要となる。

たとえば捜索対象となっている被疑者のコンピュータがネットワークドライブをマウントしているからといって、そこからネットワークを通じてリモートドライブにアクセスしてよいのかといえば、それはできないといえる。プレイン・ビューの法理を使用できそうにも思えるかもしれないが、プレイン・ビューの例外原則を適用できるのは、スクリーンに表示されているものについて妥当する。ネットワークドライブの存在が表示されていても、その存在だけをみることができるのであり、ネットワークドライブの内容はプレイン・ビューではカバーされないものである。その場合には、改めて令状を取得して、当該ドライブを保有しているプロバイダを捜索することになる。場合によっては、提出命令を使用することもあるし、プロバイダの自発的な提供によることもある。

７　従来のタイトルⅢとパトリオット法

タイトルⅢは、１年以上の拘禁刑に相当する犯罪（重罪）対象として、これを電子的に監視するためには、裁判所に行き、令状を取得しなければならないことを定めている。正当な理由が存在しているだけでなく、その他の手段がすべて失敗したことを明らかにしなければならず、また実施可能な期間は 10 日以内に限られている。

パトリオット法は、電話の世界で通用していたことをコンピュータの世界でも通用させることにしたものである。パトリオット法以前は、電子メールについて電話の場合と同様に取り扱ってよいのかはっきりしていなかったのであり、その制定によって、メールのヘッダーをみることが許されるようになった。しかし、そのためには裁判所の審査が必要である。パトリオット法、大陪審の提出命令があれば、アカウント情報等を開示することを認めている。これは ISP を電話会社と同じように解釈することを認めたものといえる。もっとも、アカウントの保有者、解説の日付などの情報にしか捜査機関はアクセスできないのであり、権利侵

害はそれほど大きくないといえる。

いずれにせよパトリオット法とタイトルⅢとの違いは、そこで監視する対象が通信内容そのものであるかあるいは通信内容でないのかによって区別することができる。

８　その他

現在のマニュアルでは対応しきれない問題やさらに新しい問題などがあるのかということについては、外国人によりおこなわれ、あるいは、外国にいる者によっておこなわれる（外国からの）犯罪などについては、このマニュアルではカバーされていないといえる。昨今、ヨーロッパ、とりわけ東ヨーロッパなどからの犯罪が増加しており、一つの傾向となっている。また、犯罪者の若年化が進んでいるという問題もあり、さらにはワイヤレス機器についての問題などもマニュアルではカバーされていない。

第２章　アメリカにおける判決例検討

この章では、アメリカにおけるハイテク犯罪の刑事手続きを理解する上で、参考になる判決例をとりあげる。

なお、研究会としては、マニュアルの理解に役立つ様に判決例をもれなく抽出し、それに対して解説を加える予定であったが、検討の結果、そのような作業に適切な判決例はあまり数が多くないことが判明した。そのために第５において、むしろ、コンピュータ法科学の観点から、興味深いと思われる証拠の保全という問題についての裁判所の判断を紹介することとなった。その点については、ご容赦ねがいたい。

第１　コンピュータ捜索の諸問題の黎明-Steve Jackson Games 事件（W.D.Tex.1993）

［事案の概要］

1990 年 1 月に電話の障害が起き、シークレットサービスは、ハッカーグループに対する捜査を開始した。これが、サンデビィル作戦とも呼ばれるものである。 1 月 18 日「ナイトライトニング」に対する事情聴取がなされ、 同 19 日捜索押収 がなされた。そして、2 月 6 日ごろ、クループフェルは、e911 文書が、BBS「フェニックス」にアップロートされていることに気がつき、これを、ダウンロードして、シークレットサービスに連絡した。この「フェニックス」を運営していた Blankenship(「メンター」)は、イリノイの"Illuminati"の共同シスオペ でもあり、それを運営する Steve Jackson Games (以下、SJG という)社の従業員であった。SJG は、テキサス州オースチンの(一般の)ゲーム製造およびそれに関連する出版の会社(設立 1984)であった。そして、宣伝とアイディアなどのフィードバックのために電子掲示板(「Illuminati Bulletin Board System」)を有していた。SJG の商品は、 GURPS CYBERPUNK という SF のロールプレイング・ゲームであった。GURPS CYBERPUNK が出荷される予定の数週間前のこと、Tim Foley をはじめとする合衆国のシークレットサービスが、 SJG の捜索・押収にはいった。その捜索・押収の結果、 （1） GURPS CYBERPUNK のドラフト、設計に使われていたコンピュータ(3 台－電子掲示板を運営していたコンピュータも含む)などを押収(ハードディスク 5 台)。（２）会社まわりのすべてのソフトウェアを(フロッピー300 枚)押収 （３） 押収したコンピュータにあった会社の業務記録をすべて、押収 （4） 会社の中を荒しまわったし、（５）すべての 出版間近の GURPS CYBERPUNK のゲームブックは、没収された。この結果、SJG は、会社休業を余儀なくされた。

しかしながら、捜査の結果、SJG は、全く違法行為に無関係であった。そうであるにもかかわらず、シークレットサービスは、押収物を保管し続けて、結局、6 月の下旬になって、やっと押収していた物を変換するに至ったのである。その上、GURPS CYBERPUNKS の原稿など書類については、保管しつづけた。また、押収時にあったサーバ上の 162 のメッセージについては、だれかが、これを読み、また、削除されていた。なお、ユーザで捜査の対象となったものはいない。

このシークレットサービスの行為によって、会社のオーナーである Steve Jackson は、きわめて大変なダメージを受けた。会社は、その従業員の約半数を解雇せざるを得なかったし、GURPS CYBERPUNK の出荷は非常に遅れた。また、彼自身が、雑誌においてコンピュータ犯罪者であるかのように書かれたという事実があった。これに対して、Steve Jackson と SJG 社、そして、その BBS のユーザの三人は、合衆国シークレットサービスなど を相手に、「プライバシー保護法 1980(the Privacy Protection Act of 1980)」「 電気通信プライバシー法(the Electronic Communications Privacy Act)」および憲法の第 1 および第 4 修正条項違反などを理由として、損害賠償の民事訴訟を提起したというのが、この事件である。

［判決の趣旨］

これらの争点について、Sam Sparks 判事は、事実関係について認定した上、上記の各論点について以下のように分析する。

１　プライバシー保護法について

Foley 捜査官は、実際には、プライバシー保護法を知らなかったけれども、仮に知っていたとしても、SJG 社が、本や資料などを作成し、交換物として公表する意図を有した会社であるという情報を有していなかったことを認定し「裁判所は、Foley 捜査官が、事業の遂行に実質的な影響を及ぼす財産を押収しようという内容を有する Steve　Jackson　Games 社の捜査にあたって、合理的な調査を欠いたものと感じる」と述べている。そして「シークレットサービスが、Steve　Jackson　Games 社の情報と書類を含む財産の押収を 1990 年の６月末まで継続していたことはあきらかである。押収されたすべての情報のコピーをなしえたのであり、３月２日に早急に対応が可能であったのであり、また、そうすべきであった。捜査当局は、会社の代表者である Steve　Jackson 氏を協力させ、法のもとで利用可能な情報を提供させることが可能であったのであり、そうすべきであった。シークレットサービスが、Jackson 氏の要請を断り情報と財産を返還するのを拒絶したことは、制定法違反を構成する」と判示されている。

２　　電気通信プライバシー法における「傍受」違反について

この事件においては、原告らは、捜査・押収の過程で、プライベートなメールにたいしての「傍受」が発生しており、それが電気通信プライバシー法に違反すると主張した。事実、この事件では、シークレットサービスが、電子メールの通信を読み、しかも、故意または過失により消去もしくは破壊してしまっていたのである。この点については、「傍受」という表現自体について、機具をもちいた一時的な取得をいうとされているので、この定義からいって、この事件のシークレットサービスの行為は、この「傍受」にふくれまないという判断がなされた。

３　有線電気通信および取引記録アクセス(18　U.S.C. Sec.2701 et seq.)違反について

「SJG 社の提供する Illuminati 掲示板は、2711 条における『リモート・コンピューティング・サービス』である。そして、シークレットサービスにおいて電気通信の内容について「開示」を取得する方法は、この制定法に従うことによる。」ことになるが「Foley 捜査官は、治安判事に対して、宣誓供述書などで、Illuminati 掲示板が、プライベートな電気通信を含み、また、この捜査が、どの程度、これらの通信と関連するかということを示すことをなさなかった。Foley 氏の知っていたことは、911 文書の一部と解読情報を Phoenix 掲示板に公開した Blankenship が、Steve　Jackson　Games 社に勤務していたことであり、それらの違法なドキュメントを同社の Illuminati 掲示板に保存し消去しうるということだったのである」。その結果、この制定法に示されている安全弁をシークレットサービスは、消去してしまったのである。そして、これらの捜査当局の行為は、捜査当局に与えられた権限を超過するものと考えられる。

４ SUMMARY

判事は、「これは、複雑な事件である。」として、911 ドキュメントの重要性が明らかではないことや、解読スキームがどれだけ危険であるのか、明らかではないことを指摘している。そして、判事は「この事件の複雑性は、シークレットサービスが不十分な捜査をなし、1990 年の 2 月 28 日の行為に適用しうる法律についての知識を欠いていたからでる。政府の官吏も、原告もその法律家も、1990 年の 2、3、4、5、6 月に起きた事件についてその制定法について熟慮していなかったことは明らかである。しかし、これは、この事件の抗弁を助けるものではない。シークレットサービスとその担当者は、原告のような市民が頼り、彼らの権利と財産を守るべきものなのである。シークレットサービスの行為は、制定法が保護すべきものとしていた財産、製品、ビジネスレコード、ビジネス書類、そして会社および４人の個人の電子通信の差押をすることになったのである。」と述べた。

判事は、原告が主張の根拠とするこれらの制定法の適用可能性について、「政府が、違法な行為を示している情報やコンピュータ書類を取得するのに極めて、困難を感じるかもしれない。」と政府・法執行機関の立場に理解をしめしながら、「 本法廷は、含まれる制定法を修正したり、書き換えることはできない。シークレットサービスは、議会に行き、救済を求めなければならない。しかし、それまでは、法廷は、より研修をつむことと、調査、そしでこの制定法に記載されたことを遵守することを推薦するのである」として、原告ら勝訴の判決を言い渡したのである。具体的には、シークレットサービスとアメリカ合衆国は、SJG にたいして、費用として、$8,781.00 と経済的損害として $42,259 の賠償を命じており、また、BBS 利用者である各原告に対して 1000 ドルの賠償を命じたのであった。

［解説］

１　サンデビィル作戦

このスティーブ・ジャクソンゲームズ事件は、有名な「サンデビィル作戦」に関連して起こった。そして、この事件は、「ハッカーを追え」という単行本に詳しく述べられており、捜索・差押がなされるまでの経緯は、その第 5 章などに詳しい。そのもともとのサンデビィル作戦とは、「911 プログラム(ただし、実際は英語の文書)」とよばれる(電子的)文書のコピーをめぐる一連の動きである。911 システムは、警察署、消防署への緊急電話をつなくたそのシステムが、きわめて脆弱だったという認識があったところに、911 システムが「ハッカー」達の攻撃にさらされ、たびたびダウンさせられていたこともあった。このような前提のもとに、この「911 プログラム(ただし、実際は英語の文書)」というコンピュータ・ファイルが、全米での一斉ハッカー取り締まりにまでいたったものである。このような過程のなかで、「事実の概要」のような経緯で事件がおきたのである。

2 法的な争点と司法省マニュアルにおける位置づけ

(1)PPA との関係については、「現在までに公刊されているもののうち、この問題に直接対処した唯一の判断において、ある地方裁判所は、PPA によって保護された資料を不注意に押収したことにつき、シークレットサービスに責任があると判示した」ものの例としてこの

判決があげられている。しかしながら、評価としては、「残念なことに、裁判所の理由付けの精確な枠組を見極めることは困難である。例えば、同裁判所は、シークレットサービスが押収した資料のうちのどの資料が精確には PPA で保護されたものであるかについて説明しなかった。」というコメントがなされている。

(2)「傍受」の解釈

この点については、本判決は、「伝達と同時に得られる時だけ，有線・電子通信が傍受されると判決している。言い換えると，通信の傍受は，通信の関係者の間の伝達の時点でのリアルタイム獲得だけに言及する。その後，保存された通信のコピーにアクセスする機会をもつ捜査官は，通信を「傍受」するものではない。」という一般的な解釈によっているものであり、注目すべき要素は余りないであろう。

(3)保存された通信についての解釈

この判決の判事は、マニュアルにおいては「同裁判所の判示は、ECPA が捜索令状も 18 U. S. C.§2703(d)及び§2703 に規定された様々な通知要件に従うことを要求しているという誤った考えに基づいているように思われる。」と批判されている。もっとも、この判決は、当該捜査官が、法の種々の規定を顧みず、十分な調査をせずに、捜索・押収をした点を避難するものであるということから「Steve Jackson Games 判決の結論と ECPA の明確な文言を調和させる最も適切な方法は、インターネット接続サービス業者や保存された有線ないし電気通信を保有するその他の第三者に対する捜索を実施する必要がある場合に、捜査官が細心の注意を払うことである。」(翻訳 67 ページ)とされているところでもある。

(4)その他の論点

侵害性の少ない手段という趣旨から「ネットワーク全体を運び去ることにより、PPA（42U.S.C.§2000aa）および ECPA（18U.S.C.§§ 2701-11）に基づく民事訴訟が国に対して提起される可能性があるのみならず、合法かつ営業中の事業を停止させ、非常に多くの人々の生活に支障をきたす可能性もある」(翻訳 57 ページ)とされているところでもある。

また、捜査に関わる捜査官の態度という観点から、「善意の抗弁」との関係について「捜索すべきコンピュータシステムに憲法第 1 修正文書やネットワークアカウントが果たして保存されているのか、保存されているとしてどこに保存されているのかにつき、捜査官は周到な調査を行うべきである。捜査官がそのような調査を行わない場合には、これらの法律上の責任に対する捜査機関側の善意の抗弁が失われると判示した裁判所」として紹介されている。

３　評価

この Steve Jackson Games 事件をきっかけにオンライン人権団体が結成され、いわゆるネットワークコミュニティの活動が盛んになるなど、ネットワーク社会の発展にとっては、きわめて歴史的な意義を有する事件であったということができるであろう。また、その内容が特に捜査官の法律に対する無知・調査の不十分さを鋭く指摘するものであり、捜査当局に対して、ネットワークにたいする捜査・押収の際に、考慮すべき法的規範等を明確化して、捜査についてのガイドラインを作成する必要があるのではないかという動きのきっかけとなっ

た事件であるとも言え、意義は、きわめて大きいものといえよう。

もっとも、法的な解釈論のレベルからみるとき、マニュアルでもコメントされているように、曖昧なものと評することができる。その意味で、議論されている論点について現時点での先例としての価値は、あまりないものであろう。しかしながら、その、いわば社会的な意義は、きわめて多大なものであったといえる判決であり、アメリカにおけるハイテク犯罪の捜査を論じる際には基礎知識として絶対に必要な判決例であると思われる。

［高橋郁夫］

第２　コンピュータ関連事件における包括的押収と合衆国憲法第 4 修正－ Guest v. Leis, 255 F.3d 325 (6th Cir. 2001)

［事案の概要］

オハイオ州ハミルトン郡保安局（Sheriff's Department）、および、同局に属する RECI（Regional Electronic Computer Intelligence Task Force）は、オンライン上のわいせつ画像に関する情報を入手し、1995 年初頭、同州クレアモント郡の Robert Emerson によって運営されている電子掲示板である CCC BBS（Cincinnati Computer Connection Bulletin Board System）について捜査を開始した。この CCC BBS は、会員数が数千人に及ぶともいわれ、ユーザは、パスワードを入力することにより、他の者に電子メールを送ったり、画像ファイルをダウンロードしたりすることなどが可能であった。

RECI の捜査官は、身分を秘匿してこの CCC BBS のアダルト関係の部分にアクセスし、サンプル画像をダウンロードした。捜査官が 100 個を超えるこれらサンプル画像をハミルトン郡の裁判所の裁判官に提示したところ、そのうち 45 個がわいせつに当たる、との判断が示されたので、RECI は捜索・押収を行う準備を進め、わいせつ画像入手の仲介（pandering obscenity）等を被疑事実とし、犯罪で使用されたコンピュータハードウェア、ソフトウェア、会員およびコンピュータに関する記録（financial and computer records）、個人的な通信（personal communications）を捜索・押収の対象とする令状が用意された。

同年 6 月、RECI の捜査官らは Emerson の自宅に赴き、前記の令状を執行した。そして、捜査官らが、Emerson に対し、わいせつ画像が彼のコンピュータのどこにあるのか教えて欲しい、そうすれば、それらのファイルのみを押収すれば済む、と伝えたところ、Emerson は、コンピュータにわいせつ画像があることなど知らない、と言い、弁護士に電話をかけた。その後、弁護士から電話の返事を待っていたが、やがて、Emerson は、コンピュータのどこに画像があるのか知らない旨を述べた。

捜査官らが Emerson の自宅に到着してから数時間が経過したのち、弁護士から依然として連絡がないという状態で、捜査官らは、コンピュータシステムを運び出す準備を始めた。その際、Emerson が、画像は大きな方のファイル・サーバに入っている、と述べたが、捜査官らは彼の言葉を信用せず、大きな方と小さな方のファイル・サーバを両方とも押収し、警察署に運び去った。

その後、Emerson は、1996 年に刑事訴追を受け、オハイオ州クレアモント郡の裁判所で有罪答弁を行ったが、それとは別に、以上のような捜索・押収に関して、1995 年 8 月、CCC BBS のユーザである Steven Guest らにより、ハミルトン郡保安局長である Simon L. Leis, Jr らの民事責任を追及する訴えがオハイオ州南部地区連邦地方裁判所に提起された。しかし、同裁判所は原告らの訴えを斥けたので、原告らによって第 6 巡回区連邦控訴裁判所に上訴が

なされ、下されたのが本判決である[15]。

［判決要旨］

本件で争点となったのは、1 つには、前記のような、電子掲示板の会員に関する情報や電子メールをも含まれるコンピュータの包括的な押収が、令状の効力が及ぶ範囲を超えたものであり、したがって、合衆国憲法第 4 修正に違反するものであるか否か、である[16]。この点について、第 6 巡回区連邦控訴裁判所は、次のように述べて、原告らの主張を斥けた。

「本件の令状は、犯罪に関係する個人的な通信の押収を認めたものであった。コンピュータには犯罪とは関係のない通信が記録されていたかもしれないが、しかし、『捜索は、令状に記載されていない（not covered by a warrant）物をも押収したからといって、それだけで違法となるわけではない』。United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988). この Henson 判決は走行距離計の不正表示に関する事案であり、そこで、当裁判所は、第一審の有罪判決を維持するに際して、犯罪とは無関係の文書およびコンピュータ・ファイルの押収は第 4 修正に違反する、という主張を斥けたのであった。というのも、当裁判所は、令状に記載されていないそれらの物（those items that were outside the warrant）を分離するため、膨大なファイルを被疑者のオフィスで選別するよう警察に求めることは、不合理である、という結論に至ったからである。Id. at 1383-84; see also Davis v. Gracey, 111 F.3d 1472, 1481 (10th Cir. 1997) (被告によって押収された電子掲示板のコンピュータに、捜査対象であった犯罪とは無関係の個人的な通信が含まれていた、という事案について、第 4 修正違反はなかった、とした); United States v. Hay, 231 F.3d 630, 637-38 (9th Cir. 2000) (児童ポルノに関する事件の捜査の過程でなされたコンピュータ・システムの捜索・押収について、第 4 修正違反はなかった、とした); United States v. Upham, 168 F.3d 532, 536 (1st Cir. 1999) (同旨). 本件においては、押収の際、被告らには、関連性を有するファイルと無関係のファイルを分離することは不可能であった。それ故、彼らは、文書を現場以外の場所で選別するために、コンピュータを運び出したのである。被疑者の家でコンピュータの捜索を行うことについては技術的困難（technical difficulties）が存在したが故に、本件においては、犯罪に関係するファイル（offending files）の所在を明らかにするために、コンピュータの押収は――それらの中身

---

[15] 本判決は、被告が同一であり、共通の争点を含む Guest v. Leis 事件と O'Brien v. Leis 事件の 2 つについて、第 6 巡回区連邦控訴裁の判断が示されたものであるが、ここでは前者の事案のみを取り上げた。

[16] このほか、本件では、その他の理由に基づく合衆国憲法第 4 修正違反、同第 1 修正（言論・出版の自由などを保障する）違反、電気通信プライバシー法（Electronic Communications Privacy Act, ECPA）違反、および、プライバシー保護法（Privacy Protection Act, PPA）違反の有無も争点となっているが、ここでは、省略する。なお、PPA に関する本判決の判断については、司法省によるコンピュータの捜索・押収に関するマニュアルの第 2 章 B.2.c)で紹介されている。*See* U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 71-75 (2d ed. 2002).

（content）の押収も含めて――合理的なものであった、といえるのである。」

［解説］

本判決において、第 6 巡回区連邦控訴裁判所は、被疑者が管理する、被疑者以外の犯罪とは無関係の者に関する情報をも含まれる複数のコンピュータを一括して押収することは合衆国憲法第 4 修正に違反しない、とする。

合衆国憲法第 4 修正は、「捜索・押収（search and seizure）」の規律について定め、令状には「捜索すべき場所」「押収すべき物」が明示されなければならない、とするが、これは、わが国の憲法 35 条の保障に相当する。ただ、アメリカでは、令状の対象となるのは必ずしも有対物に限られず、例えば、記録媒体中の情報のみの「押収」も可能であり、むしろそれが要求される場合もあるが[17]、わが国においては、刑事訴訟法上の「差押え」（刑訴法 99 条）の対象物は、一般に、有体物に限定される、と解されていることに注意を要する[18]。

本判決で扱われたのと同様の問題は、わが国においても生じている。すなわち、差押えにあたっては、差し押えようとする物の内容を捜査官が現場で確認し、それが令状に「差し押さえるべき物」として記載されたものに該当するか否かを判断する必要がある。しかし、フロッピーディスクのような記録媒体の差押えについては、それらの記録媒体にはそのままでは可読性がないため、この該当性判断を現場で行うことが困難である場合が生じるが、これにどのように対処すべきか、という問題である。このような問題を扱ったのが、最二小決平成 10 年 5 月 1 日・刑集 52 巻 4 号 275 頁である[19]。そこでは、捜査官が現場で内容を確認して選別を行うことなく、108 枚のフロッピー・ディスク等を差し押さえたことが問題となったが、最高裁は、①差し押さえようとするフロッピー・ディスク等の一部に被疑事実に関する情報が記録されている蓋然性が認められ、②そのような情報が実際に記録されているかどうかをその場で確認していたのでは、記録された情報を損壊される危険がある、という場合には、フロッピー・ディスク等を包括的に差し押さえることが許される、とされた[20]。今後

---

17 *See, e.g.*, U.S. DEP'T OF JUSTICE, *supra* note 2, at 62.

18 この点につき、例えば、安冨潔『ハイテク犯罪と刑事手続』163-164 頁（慶應義塾大学出版会、2000 年）参照。

19 この平成 10 年決定については、担当調査官による解説として、池田修・最高裁判所判例解説刑事篇（平成 10 年度）78 頁（2001 年）参照。

また、この問題に関する下級審裁判例としては、大阪高等裁判所平成 3 年 11 月 6 日判決・判例タ 796 号 264 頁がある。この判決については、解説として、山田道郎・平成４年度重要判例解説（ジュリスト臨時増刊 1024 号）192 頁（1993 年）、吉田統宏・研修 580 号 63 頁（1996 年）、小津博司・刑事訴訟法判例百選（第 7 版）（別冊ジュリスト 148 号）54 頁（1998 年）参照。

20 なお、学説上は、フロッピー・ディスク等を現場から運び出すことを、差押えではなく――別の場所で選別を行うことを含めて――捜索・差押えに必要な処分（刑訴法 111 条）と捉える見解も有力である（例えば、酒巻匡「捜索・押収とそれに伴う処分」刑法雑誌 36 巻 3 号 444 頁〔452-454 頁〕（1997 年））。このような見解に対する批判としては、寺崎嘉博「電磁的記録に対する包括的差押え」『田宮裕博士追悼論集 下巻』249 頁（2003 年）参照。

は、②の「情報損壊の危険」は存在しないが、しかし、内容の確認を行ったのでは選別に長時間を要する場合や、現場での内容確認が技術的に困難である場合についてはどのように考えるべきかが、問題となろう[21]。

これに対し、第 6 巡回区連邦控訴裁による本判決は、包括的押収を認める理由を、直裁に、捜査官らが現場で犯罪に関連性を有するコンピュータおよびファイルの選別を行うことが技術的に困難であったことに求めている。そして、本判決でも引用されているように、連邦裁判所においては、同旨の裁判例が積み重ねられてきているのである[22]。ただ、アメリカにおいては、上述のように、わが国とは異なり、「情報」それ自体も押収の対象となることから、複数の記録媒体を包括的に押収することだけではなく――記録媒体自体は犯罪の証拠や手段、あるいは禁制品ではないために――押収の対象として令状に記載されている物が、記録媒体ではなくその中の 1 つのファイルに過ぎない、といった場合に、その記録媒体全体を押収することも、「包括的押収」として問題となり得る、という違いがある。

ちなみに、コンピュータの捜索・押収に関する司法省のマニュアルによれば、包括的押収を行ったうえで現場外でそれらを選別する必要が生じることが予想される場合、捜査官は、令状請求の際、疎明資料として提出する宣誓供述書の中で、その点について言及しておくべきだとされている[23]。

なお、わが国においては、コンピュータの捜索・差押えについては、差押えの対象となるのは有対物に限られることを前提に、膨大な情報が収められている記録媒体について、その一部が証拠として重要であるにとどまる、という場合において、記録媒体全体を差し押さえることは被処分者に過大な不利益を負わせるものでないか、という点も問題とされている。この点に関わる裁判例としては、東京地決平成 10 年 2 月 27 日・判時 1637 号 152 頁がある[24]。事案は、インターネットにおけるわいせつ図画の公然陳列に関し、捜査機関が、被疑者の利用するプロバイダの支店を捜索し、このプロバイダとインターネットによる契約を結んだ通信サービスの契約を結んだ会員のうち、アダルトのジャンルを選択したホームページ開設希望者 428 名の氏名、住所、電話番号等からなる顧客管理データが記録されたフロッピー・デ

---

21 なお、この点で、通信傍受に関しては、「外国語による通信又は暗号その他その内容を即時に復元することができない方法を用いた通信であって、傍受の時にその内容を知ることが困難なため、傍受すべき通信に該当するかどうかを判断することができないものについては、その全部を傍受することができる。この場合においては、速やかに、傍受すべき通信に該当するかどうかの判断を行わなければならない」という規定がある（「犯罪捜査のための通信傍受に関する法律」（平成 11 年法律第 137 号）13 条 2 項）。

22 これらの裁判例については、司法省によるマニュアルの第 2 章で紹介されている。*See* U.S. DEP'T OF JUSTICE, *supra* note 2, at 102-04. また、長沼範良「ネットワーク犯罪への手続法的対応」ジュリスト 1148 号 212 頁〔214 頁〕（1999 年）、安冨・前掲注（4）52-53 頁も参照。

23 *See* U.S. DEP'T OF JUSTICE, *supra* note 2, at 100.

24 この決定の解説として、梅林啓・研修 604 号 13 頁（1998 年）、牧野二郎「ベッコアメ準抗告事件決定にみるプライバシーの重視」法学セミナー522 号 26 頁（1998 年）、大澤裕「コ

ィスク 1 枚等を差し押さえた、というものであった。このプロバイダからの準抗告を受けた東京地裁は、次のように述べて、差押え処分を取り消したのである。すなわち、「本件会社は、本件被疑事実の被疑者ではない上、利用者のプライバシー保護が強く要請される電気通信事業法上の特別第二種電気通信事業者であるから、本件会社に対する捜索差押の適法性を判断するにあたっては、捜索差押の必要性と並んで利用者のプライバシー保護を十分に考慮する必要がある」が「本件捜索差押許可状の差し押さえるべき物は、前記のとおり包括的であるところ、その記載の適否はともかく、具体的差押処分にあたっては、差押えの必要性を厳格に解する必要があ」り、「被疑者に関するものについては、本件被疑事実との関連性、差押えの必要性は明らかであるが、その余の会員に関するデータについては、アダルトホームページの開設希望者に限定したところで、本件被疑事実との関連性を認めがたく、差押えの必要性は認められない」、と[25]。

もっとも、この問題については、現在、立法による解決が具体的に検討されていることに触れておかなければならない。すなわち、2003 年 9 月 10 日に、法制審議会において「ハイテク犯罪に対処するための刑事法の整備に関する要綱（骨子）」が採択され、法務大臣に答申された[26]。そこでは、例えば、「電磁的記録に係る記録媒体の差押えの執行方法」として、捜査機関等が、記録媒体の差押えに代えて、そこに記録された電磁的記録を他の記録媒体に複写し、印刷し、または移転したうえで、この「他の記録媒体」を差し押さえることを可能とすることが提案されている。

［小川佳樹］

ンピュータと捜索・差押え・検証」法学教室 244 号 44 頁（2001 年）がある。

[25] なお、この決定に対しては、その意義を認めつつも、被疑事実との関連性がないという理論構成を採ったことについて、疑問が呈されている（例えば、大澤・前掲注（24）45 頁）。

[26] その内容については、ジュリスト 1257 号 34 頁（2003 年）参照。

第３　データ自体の押収とその関連問題－Davis v. Gracey, 111 F. 3d 1472（10th Cir. 1997）

［事案の概要］

オクラホマ市で電子掲示板システム（BBS）を管理・運営していた Anthony Davis（以下“D”という）は、同人が猥褻な CD-ROM を販売しているとの匿名情報に基づき派遣された覆面捜査官に対し、猥褻な CD-ROM を 3 回にわたり販売した。D は、そのうち一回の機会に、自らの運営する電子掲示板にネット接続（ダイアルイン）することによって同種のポルノ画像にアクセスしうることを捜査官に告げた。こうしたことを承け、捜査官は D の各事業所（Mid-America Digital Publishing Company、Oklahoma Information Exchange）に対する捜索・押収令状の発付を請求した。なお、疎明資料としての宣誓供述書においては、同事業所において掲示板が運営されている可能性があることや、当該掲示板がポルノ画像の頒布ないし陳列に使用されている可能性についての言及はなかった。上記令状請求を受けた裁判官は、覆面捜査官が D から入手した CD-ROM のうちの２枚につき猥褻性を認め、ポルノ CD-ROM 及び「・・・〔オクラホマ〕州猥褻法規に違反するポルノ資料の頒布ないし陳列に関係する機器、注文資料、文書、加入者リスト、及びその他の備品（paraphernalia）」を対象に同人の事業所を捜索することを認める令状を発付した。

これを承け、オクラホマ市警に属する Anthony Gracey、Mark Wenthold（以下 G ら）を含む複数の捜査官が令状を執行した。G らは、同令状執行中に、電子掲示板（端末）及びそれに接続されていた 16 枚入りの（うち 4 枚については、ポルノ画像を含むものであることを D 自身が認めた）CD-ROM ドライブを発見し、その構成上、ポルノ画像を含む CD-ROM ファイルが上記 BBS を通じてアクセス可能となっているのではないかと考え、コンピュータに詳しい捜査官に助言を求めた上で、その可能性があることが確認されたため、当該掲示板運営に使用されていたコンピュータ機器（端末、モニター、キーボード、モデム、CD-ROM ドライブ、同チェンジャー）を押収した。なお、押収当時、同コンピュータシステムの電子ストレージには未読（未接続）のものを含む約 15 万通の e-mail が、ハードドライブには個人加入者のアップロードした約 500MB のソフトウェアがそれぞれ蔵置されていた（なお、D は、後者のいわゆる「シェアウェア」につき、CD-ROM 化した上で一般に販売することを考えていた）。

D はわいせつ（物）所持及び同頒布の罪で起訴され、有罪とされた。また、押収されたコンピュータ機器は（オクラホマ州の民事没収制度に基づき）没収された。これを承け、D は、押収を行った G らに対し[27]、D 個人及び同機器に関わる上記 2 社の代表として、かつ、同 BBS 利用者である Gayla Davis、John Burton 及び Telecommunications Specialists, Inc.（以下「B

[27] 当初は、コンピュータ内に蔵置された電子資料を複写・返還しなかったこと、あるいは複写・返還に遅滞があったことを理由に、オクラホマ市、同市警、及び当該捜索・押収の執行を担当した同市警の部局も被告側のリストに含まれていたが、これらは原審段階で適格なしとして外された。

ら」という）と共同して、当該捜索・押収の違憲性、プライバシー保護法（Privacy Protection Act、以下“PPA”という）及び電気通信プライバシー法（Electronic Communications Privacy Act、以下“ECPA”という）違反を理由に、連邦法典1983条に基づく訴えを連邦地方裁判所（オクラホマ西部地区）に提起した。これに対し、同裁判所は、正式事実審理を経ない判決（summary judgment）によりこれを斥けたため、Dらが控訴したところ、連邦控訴裁判所（第10巡回区）は、以下のような判断を示し、原審の判決を維持した。

［判旨］

「当裁判所は、本件においては、原告側の主張のうち、コンピュータ機器及び同機器内に蔵置されていた電子的資料に対する第1次的押収の適法性に関するものに限り、判断を示すものとする。」[28]

（1）令状及び執行手続が合衆国憲法第4修正違反であるとの主張について

まず、被告側の制限的免責の主張を認めた原審の判断を審査するが、その際、相手方当事者〔原告〕の側に最も有利な視点から証拠を検討する。ここでは、「原告が憲法上ないし法律上の権利の侵害を主張しているかどうか、さらには、当該権利が明確に確立されており、被告と同じ立場におかれた合理的な人間であれば誰でも、自らの行為によって当該権利が侵害されることを知りえたほどのものであるかどうか」[29]が問題となる。原告側が捜査官の行為によって憲法上ないし法律上の権利が侵害されたことを証明できなかった場合には、制限的免責の有無を審査するためのその他の要素を検討する必要はない。

「原告側は、押収すべきコンピュータ機器について特定を欠いているため本件令状が過度に広汎ゆえに違憲であると主張する。また、各捜査官が令状裁判官をして誤って令状を発付せしめたという。さらに、かりに当該令状が本件コンピュータ機器の押収を許可したものであったとしても、当該ハードウェア内に蔵置され、明らかに当該令状の適用範囲外にある電子メールやその他のファイルの付随的な押収をもたらすような形で当該令状の執行がなされるべきではなかったと主張する。以下順に検討する。」

A. 令状

「原告側は令状に記載された『機器』がコンピュータ機器や電子機器を包摂することを令状自体において明示していなかったことが致命的な瑕疵であったと主張する。しかし、これには同意できない。ここで問題となるのは次の二点である。すなわち、当該令状が押収の対象物とそれ以外のものとを区別する基準を捜査官に提示していたか、そして、押収された物

---

[28] Davis v. Gracey, 111 F.3d 1472, 1477.なお、原告は、捜査機関が同機器及び電子的資料を保持し続けたことや、原告による当該資料の返還請求に応じなかったことも違憲ないし違法であるとの主張をなしている。しかし、連邦控訴裁判所は、各捜査官が当該資料の返還を決定する権限を有していたことの立証がなされていないこと及び捜査機関自体についてはもはや訴訟当事者ではないことを指摘して、当該保持ないし不返還の違憲性、違法性については論じない旨判示している。

[29] Garramore v. Romo, 94 F.3d 1446,1449（10th Cir.1996）.

が当該令状に記載された範疇に属していたかである。」本件に関する限り、いずれも積極に解される。本件令状は、捜査官をして「〔オクラホマ〕州猥褻法規・・・に違反するポルノ資料の頒布及び陳列に関係する・・・機器・・・を対象として捜索する」ことを命じており、この範疇に属するコンピュータ機器の押収は適法である。「原告側は、本件電子掲示板が、ポルノ関連ファイルにダイアルインでアクセスするために、また、（ドライブに）装填されたCD-ROMから当該ファイルをコピーするために使用されうる状態にあったこと自体については争っていない。本件で押収されたコンピュータ機器は、本件令状の適用範囲内にあったものと解される。」

「原告側は当該コンピュータ機器が本件令状の文言に包摂されていたとすれば、同令状は、過度に広汎なものであったことになる」と予備的に主張するが、これも認められない。「本件令状における記載は、捜索の意義ある限界を提供するのに十分なものであり、当裁判所がこれまでに特定性が十分でないと認定したものに比べ、ずっと限定の度合いが高いものである。」これまでに当裁判所が過度に広汎であると認定したものとしては、令状において「事実上・・・ある会社の事務所に存在すると想定しうる全ての文書」の捜索を認める記載がなされている場合[30]や、「何ら修飾語句を伴わずに広汎な連邦法規を引いている」記載がなされている令状の場合[31]、さらには、「その他捜査官が窃取されたものと断定し、あるいはそう合理的に考える一切のもの」との文言を含む令状の場合[32]などがある。また、第9巡回区連邦控訴裁判所においても、捜索の対象となった会社に所在する「事実上全ての文書及びコンピュータ・ファイルの捜索を認めた」令状が特定性を欠くとの判断が示されている。そして、そこでは、当該令状において、「各範疇に属する文書のうちのいずれが押収可能であるかについての限定が全くなされておらず、それらの文書が特定の犯罪活動にいかなる形で関連しているのかも示されていない」ことが強調されている[33]。「本件で押収が許可されたのは、『ポルノ資料の頒布及び陳列に関係する』機器のみである。」ここに含まれるのは、被疑事実と直接に関連する機器だけであり、被疑事実と関連しない目的で使用されるその他一切の機器ではない。また、合法な企業に所在すると想定される全ての機器まで包摂したものでもない。さらに、本件令状で引かれた犯罪活動は極めて限定されており、ある物が当該犯罪活動の際に使用された道具ないしはその証拠となるものであるかを捜査官が判断するための十分な指針となるものであった。本件令状は過度に広汎とはいえない。

本件令状に基づく捜索の執行そのものも、当裁判所が本件令状の特定性を肯定する理由の一つとなっている。本件では、対象不動産に対する一般〔探索的〕捜索が行われたわけではない。Dが自ら製作したもので、ポルノ的な性格のものではないと主張したおよそ2000枚

---

30 *See* United States v. Leary, 846 F.2d 592,602（10th Cir.1988）（hereinafter *Leary*）；Voss v. Bergsgaard, 774 F.2d 402,405（hereinafter *Voss*）（10th Cir.1985）.

31 *See Leary*, 846 F.2d at 602.

32 *See* United States v. Brown, 984 F.2d 1074,1077（10th Cir.1993）.

33 *See* United States v. Kow, 58 F.3d 423,427（10th Cir.1995）.

の CD-ROM ディスクについては捜査官らは押収していない。また、CD-ROM ドライブや電子掲示板に接続されていないコンピュータ機器の捜索・押収がなされたという証拠もない。執行に当たった捜査官らは、よりコンピュータに詳しい捜査官と協議して、当該コンピュータ機器が実際にポルノ資料を頒布ないし陳列するために使用されたものであって、それ故に当該令状の適用範囲内にあるものであることを確認している。執行にあたった捜査官が当該令状の課していた制約を甚だしく軽視した（flagrantly disregarded）のであれば、本来は合憲な令状が一般〔探索的〕捜索に転じてしまうこともあろうが、本件においてそのような捜査官の態度を示唆するものは何もない。

B. 令状請求手続

原告側は、捜査官が、電子掲示板の存在やコンピュータを通じてのポルノ頒布の可能性を認識していたにも拘らず、令状に添付する宣誓供述書においてそれに言及しなかったために、令状裁判官が誤って令状を発付したと主張する。しかし、原告側は、令状裁判官が CD-ROM に記録された「ポルノ資料の・・・陳列に関係する機器」の中にコンピュータやその付属品が含まれる場合が多いことを認識していなかったとの主張はしていない。また、実際には、同宣誓供述書において、宣誓した捜査官が、CD-ROM ドライブつきのコンピュータの中にある猥褻な CD-ROM を発見した旨述べている。

原告側は捜査官が電子掲示板の存在を認識しつつそれを宣誓供述書に記載していなかったことからすると、捜査官らが令状を善意で信頼して執行したとはいえないという。しかし、「令状請求の手続において、相当な理由の徴憑（indicia）があまりに不十分であって、相当な理由の存在を信じることが不合理であるような場合にのみ、免責による保護が失われる」[34]のである。本件令状には相当な理由が示されていたことや、宣誓供述書に記された相当な理由が電子掲示板についての言及の欠如によりなぜ否定されるのかが原告側によって示されていないことからすれば、この主張は認められない。原告側の主張は、宣誓供述書において、あるコンピュータシステムが電子掲示板を通じてポルノ資料を遠隔的に見ることを可能にする形でも構成されうることを明らかにしていなかったことが、令状を無効なものとするとの主張にまで限定されよう。しかし、令状執行対象者によって、令状において特定された物が、令状で言及された犯罪を実行するために、単に令状で述べられていない手法で用いられていると執行担当捜査官が疑っており、かつ後にそうであることが判明したからといって、相当な理由に支えられた令状が無効となるわけではない。

C. 電子的に蔵置された資料の付随的押収

「原告側は令状がコンピュータ機器自体の押収を許容していたとしても、当該押収は、同コンピュータ内に蔵置された e-mail やソフトウェアをも付随的に押収するものであるがゆえに違憲であると主張」しているようであるが、この主張には理論的な根拠がない。原告側はコンピュータ機器を押収する相当な理由が、その内容物を押収する相当な理由となるわけ

---

34 Malley v. Briggs, 475 U. S. 335,344-345（1986）（citing United States v. Leon,468 U. S. 897,923（1984））.

ではないとして、「容器」としてのコンピュータとその「内容物」との区別を主張し、それによって上記の議論を裏付けようとしているようである。その場合に問題となるのは「コンピュータ内に蔵置された電子的資料が付随的・一時的に押収されたことによって、それらの資料を蔵置していたコンピュータそのものの押収が無効となるか」である。

本件コンピュータ機器は猥褻なファイルの単なる「容器」ではなく「犯罪の道具」であったという一点のみからしても、既に上記議論は前提を欠く。典型的な事案においては、容器の押収についての相当な理由は、その内容物に禁制品や証拠資料が含まれると信ずべき相当な理由を意味するが、本件コンピュータ機器の押収の相当な理由は、ポルノ画像を頒布及び陳列する機能に関係しており、そうした資料を保存しておくという機能には関係していない。ある物が―適法目的と違法目的を含む―複数の目的で使用されうるからといって、相当な理由及び有効な令状に基づくその物の押収が無効となるわけではない。

実務上の観点からしても、捜査官が捜索の過程においてコンピュータハードウェアと電子ストレージの内容物とを峻別するのは極めて困難である。原告側もその区別についての有効な基準を提示していない。「要するに、コンピュータハードウェアの押収の適法性を維持するためには、捜査官が同コンピュータの内容物を押収してはならないとの理解には、法律的にも実務的にも何ら根拠を見出すことができない」。

一方、先行する容器の押収と、内容物についての事後的な押収及び保持とを区別することは十分可能である。典型的な事案においても、内容物の全てが禁制品であると信ずべき相当な理由が必要とされているわけではない。それ自体を押収する相当な理由に基づかずに、いわば「無実の」内容物の占有が一時的に奪われる可能性があったとしても、容器自体の押収が無効となるわけではない。当裁判所は、内容物についての原告側の権利の一時的侵害を防止するために、もともとは合憲であるコンピュータ機器の押収を違法と判示することはしない。ただ、コンピュータ機器の押収が令状に基づいてなされたことにより、その中に蔵置されたファイルの付随的な押収も許容されることになるという本件の結論は、今後、警察が令状なくして蔵置されたファイルを捜索し、保持しようとすることまで認めたものと解されるべきではない。

最後に、いったん CD-ROM 及び同ドライブが押収されたならば、捜査官は他のコンピュータ機器を押収してはならないとする原告側の主張であるが、これもまた実務的及び理論的な根拠を欠いている。本件コンピュータ機器は、全体として猥褻（物）頒布という犯罪の道具を構成するもので、同機器は（全体として）令状の適用範囲内にあったものと考えられる。

以上、原告側に最も有利な立場から証拠を見てきたが、本件捜査官らの行為が違憲といえるレベルにまで達しているとはいえない。原告側の憲法違反の主張を斥けた原判決は適法であったと考えられる。

（２）PPA 違反の主張について

原告側は本件各電子資料の押収が PPA 違反となる旨主張する。PPA は、政府官吏が、犯

罪の捜査ないし訴追に関し、新聞・書籍・放送ないしその他の類似の公表形態により一般に普及させる目的があると信ずべき合理的な理由のある者の所持にかかるワークプロダクト資料につき、これを対象として捜索を行い、あるいはそれらを押収することは、違法である旨規定する。そして、同法によれば、捜査官がこれらの資料を入手するためには、緊急の事情なき限り、かつ、「その資料の所持者が当該資料に関連する犯罪を現に行っているか、または現にこれを行い終わったものと信ずべき相当な理由がある場合」を除き、〔裁判所の〕提出命令によらなければならない。本法に基づく請求は、合衆国、州、または政府の一切の構成単位（governmental unit）に対してなすことができることとなっており、個々の州官吏に対しても―主権免責により、その属する州自体を請求の相手方としえない場合には―なすことができる。なお、同法は、州官吏が、自らの行為が適法であると合理的に（具体的な根拠に基づき）善意で信じていた場合には、そのことが上記の請求に対する絶対的な抗弁となることをも規定している。本件の原判決はこの抗弁の成立を認めている。〔これと異なり、〕当裁判所は、本件被告たる捜査官らに対する PPA に基づく事物管轄権を有していないと考える。PPA の上記文言は、その個人としての資格に基づく市の（municipal）職員に対する請求を認めているものとは解されない。したがって、同法は、本件捜査官らに対する請求権を認めるものではない。

（３）ECPA 違反の主張について

原告側は、電子掲示板上の（電子掲示板端末内の）e-mail の押収が ECPA 違反である旨主張する。ECPA のタイトルⅡによれば、蔵置された電気通信に無権限でアクセスすることは禁止される。そして、その禁止に違反する行為は、刑罰の対象となるのみならず、民事の損害賠償請求の根拠となる。ただ、この場合においても、「裁判所の許可ないし命令」に対する「善意の信頼」に基づいて当該行為が行われたとすれば、そのことは絶対的な抗弁となる。

原告側は捜査官が e-mail を押収し、電子掲示板を解体したことで ECPA（2701 条（a））に違反して「電子ストレージ内の・・・電気通信・・・について、権限に基づくアクセスを獲得し・・・あるいは妨害し」たと主張する。これは当巡回区のみならず他の巡回区においても先例のない問題を提起したものである。原告側は主に Steve Jackson Games 事件判決[35] に依拠してこの主張をなしているが、本件においては事情がかなり異なる。殊に、Steve Jackson Games 事件においては、電気通信が押収されたことのみならず、その後に当該ファイルが調査され、読まれ、削除されたことが問題となっており、裁判所が焦点を当てたのも、2703 条の「電気通信の内容」に政府がアクセスするための手続の適法性である。当裁判所の（判断ではなく）推測によれば、本件においても、捜査官が押収された e-mail の内容にアクセ

[35] Steve Jackson Games Inc. v. United States Secret Serv., 816 F. Supp. 432(W.D.Tex.1993),aff'd, 36 F. 3d 457（5th Cir.1994）.なお、この判決の詳細については、前出参照。

スするためには、2703 条に則り、新たな令状が必要となったものと考えられる。ただ、本件において原告側は捜査官が押収された e-mail にアクセスしたり、それを読もうとしたりしたことを主張してはおらず、捜査官らもそうした意図を有していたことを否定している。したがって、本件では、上記とは全く異なり、電気通信の付随的な押収が、それのみ独立して、ECPA 違反となるかが問題となるのである。2703 条はここでは関係がない。

当裁判所の（判断ではなく）推測によれば、原告側の指摘した被告側の行為は、2701 条（a）に違反する行為を構成する。また、被告側と同等のコンピュータ技術を有する合理的な捜査官であれば、コンピュータハードウェアの押収が e-mail の押収及びアクセス停止状態をもたらすことを知っていたはずであるとの主張も正しいと考えられる。しかしながら、当裁判所は、被告側に有利な原審の正式事実審理を経ない判決は正当と考える。なぜなら、被告側は、法律問題としては、ECPA 上の善意の抗弁を行使しうるものと認められるからである。

原告側は、2701 条に規定された例外に該当しない限り、捜査官らが責任を免れることはできない旨主張するが、ECPA は、2707 条（e）において、令状を信頼した場合についての一般抗弁としての善意の抗弁をも規定している。「本件捜査官らは、コンピュータ機器の押収を許可する令状を信頼しており、蔵置された電気通信の押収はその執行に付随してなされたものである。善意といえるためには、捜査官らの令状への信頼が客観的に合理的なものであったことが必要となる」が、第 4 修正違反の主張に対する判断の箇所で述べたように、本件令状は有効なものであって、上記コンピュータ機器をも対象として包摂したものであった。したがって、捜査官らの令状への信頼は客観的にも合理的であったといえる。

原告側はさらに、捜査官らが令状裁判官に電気通信が蔵置されている可能性があることを伝えていなかったため、善意の抗弁は成立しない旨主張する。既に述べたとおり、捜査官が主観的な悪意により宣誓供述書から一定の情報を除いたとの推測が成り立ちえたとしても、捜査官はなお相当な理由に基づく有効な令状を信頼していたということができる。ECPA が第 4 修正よりも厳格な要件を規定したものとは考えられない。また、令状において、コンピュータ本体とは区別されるその内容物を押収するための相当な理由が示されていなければならないとの原告側の主張に対しても、当裁判所は既にこれを否定した。捜査官らは、法律問題としての善意の抗弁について証明したものと考えられる。

（4）結論

以上より、有効な令状を信頼した捜査官らは、第 4 修正違反の主張に対して限定的免責を主張でき、ECPA 上の善意の抗弁も立証できていると考える。また、PPA 違反かどうかについては、当裁判所は事物管轄権を有していないものと考える。原判決を維持する。

［解説］

本件における原告の主張は①本件押収令状は対象物の特定を欠いており、当該令状自体及

びそれに基づく押収（私人たる BBS 加入者に宛てた e-mail や D が将来販売を予定していたソフトウェアという電子資料の付随的な押収の点も含め）が憲法第 4 修正に違反する、②上記電子資料の付随的押収が PPA に違反する、③上記 e-mail の付随的押収が ECPA に違反する、という 3 点である（原告側は控訴審においては特に修正第 1 条違反の主張をなしていない[36]）。

本判決は、②については PPA の該当条項が合衆国や州の職員を対象としており、市の職員を対象としてはいないことから、単純に事物管轄を欠くものと判断しているが、その他の点、特に①についてはかなり詳細な判断を示している。また、それまで先例のなかった③についても、「判断（decision）」を示すまでにはいたらなかったものの、「推測（assumption）」という形で裁判所の一定の評価を提示している。これらの点で、本判決には重要な意義があるものといえよう[37]。以下では、この 2 点についてやや詳しく見たうえで、本判決がわが国の捜査実務に示唆するものがあるとすればそれは何かを検討し、最後に本判決後の展望を述べることとしたい。

（1） 憲法第 4 修正違反の主張につき

この主張は大きくは 3 つに分けられる。すなわち、令状記載上の問題、令状請求手続の問題、さらには、令状執行手続の問題である。

（ｉ）まず、令状に記載された「機器」がコンピュータ機器等をも含むことが令状自体において明示されていなかった点について、本判決は、当該令状が押収の対象物とそれ以外のものとを区別する基準を捜査官に提示していたか、押収された物が当該令状に記載された範疇に属していたかが問題となるとした上で、同令状において「〔オクラホマ〕州猥褻法に違反するポルノ資料の頒布及び陳列に関係する・・・機器」が対象となることが明示されており、これは捜査官が押収対象物とそれ以外のものを区別する十分な指針となり、かつ、（同機器が実際にも同犯罪の道具となりうる状態となっていたことにも言及して、）本件コンピュータ機器がこの範疇に属するものとしている。

また、本件令状の「機器」がコンピュータ機器をも含むものとすれば、本件令状は過度に広汎ゆえに無効（違憲）となるのではないかという点については、本件令状が「〔オクラホマ〕州猥褻法規」に違反する「ポルノ資料の頒布及び陳列に関係する・・・機器」としていることから、捜索についての「意義ある限界を提供するのに十分」なもので、第 10 巡回区や第 9 巡回区の先例上特定性を欠くとされてきたものと比べても「ずっと限定の度合いが高いものである」として、消極に解している。

本判決はさらに、原告が関連性なきものと主張する約 2000 枚の CD-ROM ディスクや、CD-ROM ドライブ・電子掲示板に接続されていないコンピュータ機器について捜索・押収

---

[36] ただし、同条項の趣旨が第 4 修正の解釈論や PPA に規定された救済に反映されていることは主張している。*Davis*,111 F.3d at 1477 n.4.

[37] DOJ マニュアルにおいても 13 箇所（詳しくは“Table of Authorities”参照）で取り上げられており、本判決に対する注目度が高いことが窺われる。

していないこと、押収する機器の関連性について捜査官らが極めて慎重に判断していること、さらには、執行にあたった捜査官が当該令状の課していた制約を甚だしく軽視した（flagrantly disregarded）ともいえないことを指摘し、令状執行がいわゆる「一般（探索的）捜索」に該当せず、したがって、本件捜索令状執行自体は、むしろ令状の特定性を肯定する方向で作用しているという。

（ii）次に、電子掲示板の存在やコンピュータを通じてのポルノ頒布の可能性を認識しつつ捜査官らがこれを令状請求資料の一つである宣誓供述書において示さなかったために、令状裁判官が誤って令状を出してしまったとの主張については、本判決は、裁判官が実際に判断を誤った（当該令状に記載された「ポルノ資料の陳列に関係する機器」にコンピュータやその付属品が含まれることが多いことを知らずに、それらについてまで押収がなされるとは思わずに令状を発付した）ことを原告側が主張していないことを理由にこれを斥けている。

また、原告側が、捜査官は電子掲示板の存在を認識しつつそれを宣誓供述書に記載していなかったのであり、令状に対する善意の信頼は認められないと主張したことに対し、本件では相当な理由が示されており、当該相当な理由は電子掲示板についての言及の欠如により否定されるべきでないとする。そして、原告側の主張を、宣誓供述書において、あるコンピュータシステムが電子掲示板を通じてポルノ資料を遠隔的に見ることを可能にする形でも構成されうることを明らかにしていなかったことが令状を無効なものとするとの主張として捉え直した上で、「令状において特定された物」が、「令状で言及された犯罪を実行するため」に、「令状で述べられていない手法で」用いられている可能性を捜査官が認識しており、実際にそうであることが後に判明したからといって、「相当な理由」に支えられた令状が無効となるわけではないとの判断を示している。

（iii）さらに、原告側の、本件において押収されたコンピュータ内に蔵置された e-mail やソフトウェアに対する付随的な押収が違憲であるとの主張に対しては、理論的にも実際的にも根拠がないと判断している。すなわち、原告側が「容器」としてのコンピュータ機器とその「内容物」とを区別し、前者を押収する相当な理由は後者を押収する相当な理由とはならないとしたのに対し（、当該主張が究極的には「コンピュータ内に蔵置された電子的資料が付随的・一時的に押収されたことによって、それらの資料を蔵置していたコンピュータそのものの押収が無効となるか」に行き着くものであるとした上で、）（a）本件コンピュータ機器が猥褻なファイルの単なる「容器」ではなく「犯罪の道具」であった、（b）本件における相当な理由は、ポルノ画像を頒布・陳列する機能に関するもので、それらの画像を蔵置する機能に関するものではなかったが、ある物が複数の機能を有するからといって、その物の（一つの機能に関わる）相当な理由に基づく適法な令状による押収が無効となるわけではないことを指摘する。そして、実務上の観点からしても、捜査官が捜索の過程でコンピュータハードウェアと電子ストレージの内容物とを峻別するのが極めて困難であり、原告側もその区別についての有効な基準を提示できていないことを指摘する。

本判決は、さらに、相当な理由に基づく容器の押収が、関連性のない内容物の占有を「一

時的に」奪う可能性を有していても、その容器の押収自体が無効となるわけではなく、内容物についての原告側の権利の「一時的」侵害を防止するために、そもそも合憲なコンピュータ機器の押収が違憲となるわけではないとする。

そして、いったん CD-ROM 及び同ドライブが押収されたならば、捜査官は他のコンピュータ機器を押収してはならないとする原告側の主張について、本件コンピュータ機器が全体として猥褻（物）頒布という犯罪の道具を構成しており、同機器が（全体として）令状の適用範囲内にあったと考えられることを指摘してこれを斥けている。

（ⅳ）以上の判示により、令状において、押収対象物として、「コンピュータ機器」と明示されていない場合でも、令状において捜査官が押収対象物とそうでないものとを区別しうる指針が示されており、かつ令状で明示された対象物の範疇に属している場合には、コンピュータ機器を押収することも許容されることが明らかとなった。また、令状において同機器に蔵置されたデータに関する記載がない場合であっても、その機器の押収に付随する当該データの押収が許容される場合があることも示された。

ただ、令状が「過度に広汎」であるかを判断する際に本判決が引用した先例は、いずれも一見して明らかに不特定であると考えられるものであることからすれば―そこで考慮された三つの要素、すなわち、令状において押収対象物を被疑事実との関連性があるものに限定しているか、事実上事業所に存在すると見込まれる全ての物を包摂していないか、被疑事実（たる犯罪）が限定されているかを考慮すること自体の当否はともかく―これらとの比較によって厳密に「過度に広汎」であるか否かが判定できるか疑問が残る。

また、本判決自体認めているように、先行する容器の押収と、内容物についての事後的な押収及び保持とを区別することは十分可能であって、令状に基づくコンピュータ機器の押収に付随する蔵置ファイルの押収の許容という本件の帰結は、警察に、今後令状なくして蔵置されたファイルを捜索し、保持しようとする権限まで認めたものとまで解されるべきではない。

なお、司法省のマニュアルにおいては、出来る限り「機器」にいかなるものが含まれるかを明らかにするべきであることや、その中に蔵置されたデータが付随的に押収される可能性があること等についても言及しておくべきであるとされていることに注意を要しよう。

（２）ECPA 違反の主張につき

e-mail の押収並びに電子掲示板システムの解体によって、捜査官らは ECPA の禁止する「電子ストレージ内の・・・電気通信・・・について、権限に基づくアクセスを獲得し・・・あるいは妨害し」たか―端的には本件電子資料の付随的な押収が単独で ECPA 違反となるか―というのが、ここで原告側によって提起された先例なき問題（question of first impression）であった。本判決は、まず、本件では押収された電子資料に対する事後的な検査、判読、削除等がなされていないことを指摘して本件を SJG 事件（この事件の詳細については、前出の同判決の紹介の箇所を参照）と区別した上で、ECPA 上の善意の抗弁が成立することを理由に原判決を維持した。ただ、判断ではなく推測という形で、この問題についての評価を示し

ている。すなわち、本判決は、上記の捜査官らの行為が 2701 条（a）に違反する行為となることを「推測」として認めているのである。これにより、コンピュータ機器に付随してその中に蔵置された電子資料が押収されたという事実が、単独で、ECPA 違反として違法とされる余地があることが示唆されているといえよう。

（3）わが国の捜査実務への示唆

判文中にも見られるように、合衆国においてはデータ自体が押収の対象となっている。これは、合衆国憲法第 4 修正が個人のプライバシーを保障したものと解されており、それは有体物に対する関係でのみ認められるわけではないことに由来する。

これに対し、わが国においては、憲法 35 条の規定振り（「住居、書類及び所持品」、「押収する物」）やこれを承けた刑訴法の規定（99 条 1 項、219 条等）において「差し押えるべき物」と明記されていることなどから、捜索・差押えの対象となるのは有体物に限られるものと解されてきた[38]。ただ、そう解することによって種々の問題が生じてきており、そうした問題に対処するために解釈上様々な工夫がなされてきた（本解説編・第 3 章・第 3 掲載・小島論文及び同論文における各引用文献等参照）のみならず、最近では、解釈のレベルを超えて、新たな立法の動きも出てきている（詳しくは後掲安富論文参照）。今後は、そのような立法の趣旨を考慮しつつ、令状において対象「物」たる記録媒体をいかに特定するか、また、対象物に含まれる「データ」についてどのように、あるいはどこまで記載するのが適当であるか等が問題となってこよう。また、将来的には、端的にデータ自体の押収を認める立法が必要となると考えられる。

わが国におけるこのような動きに照らして考えるならば、本判決も、コンピュータ捜索・押収令状の特定性及び当該コンピュータ内に蔵置されたデータの付随的押収という―日本においても争われる可能性がある[39]―問題に対する一つの処理の仕方を示すものとして参考となるものと考えられる。

（4）展望

なお、本判決では、付随的に押収された e-mail やソフトウェアを捜査機関が（原告側からの返還請求にも拘らず）長期間保持し続けたことの適法性についての判断が示されているわけではない。ただ、その点に問題がありうることは、本判決自体認めているところである[40]。また、本判決は、原告側の PPA 違反及び ECPA 違反の主張については、それぞれ事物管轄権がない、善意の抗弁が成り立つとして斥けているが、こうした主張についての実質的な判断も、後の課題として残されたものといえよう（これらについては、DOJ マニュアルの各該当箇所も参照されたい）。　［小島淳］

---

38 なお、これに反対するのは、安富潔・ハイテク犯罪と刑事手続・164（慶大出版会、2000）。

39 特に前者の問題点につき、平野ほか編・新実例刑事訴訟法Ⅰ［小川新二］・257（青林書院、1998）、松尾ほか編・刑事訴訟法の争点〔新版〕［的場純男］・94-95（有斐閣、1991）など参照。

40 *Davis*, 111 F.3d at 1477, 1484 n.15.

第４　プロバイダに蔵置された顧客のデータの令状による捜索と第４修正－United States v. Bach, 2001 WL 1690055 (D.MInn. Dec. 14.2001).United States v. Bach, 310 F. 3rd 1063 (8th Cir. 2002).

［事案の概要］

ミネソタ州の児童に対するインターネット犯罪専門チーム(Minnesota Internet Crimes Against Children Task Force(MICAC))**の一員であった巡査部長Ｓは、ある母親から、その家族の使用するパソコンから引き出したある文書のために、相談を受けた。その文書には、その母親の未成年の息子（ＡＭ）と** dlbch15 **という名前を使用する相手との会話のログの一部が含まれていた。その会話において、**dlbch15 **は、ＡＭに対し、ＡＭの家の近くにある物を隠す場所をたずね、またＡＭが再度自分に会いたいかどうかをたずねていた。この会話について質問されたとき、ＡＭは、その会話が** www.yahoo.com **のチャットルームでおこなわれこと、**dlbch15 **がＡＭのために** Playboy **という雑誌を隠すつもりであったことを法執行機関に述べた。ＡＭは** dlbch15 **本人と会ったことはあるが、ふたりの間に性的な接触はなかったと言っている。**

Ｓはこの事件を捜査し、dlbch15 **が** Bach **であり、彼が** 1996 **年に性犯罪により有罪判決を受けていたことを解明した。結局、Ｓは** Yahoo!**から被告人と性犯罪の被害者になりうる者との間の電子メールおよび彼のアカウントに接続されていた** IP **アドレスを入手するための州の捜索令状**(Ramsey County Warrant)**を入手した。令状本体とＳの宣誓供述書のいずれもが、カリフォルニア刑法典セクション** 1524.2 **にしたがって令状をＹ**ahoo!**にファックスできることが記されていた。Ｓは署名された令状を** Yahoo!**にファックスした。**

Yahoo!**の技術者は、**dlbch15@yahoo.com **での** Bach **のアカウントおよびＡＭの** Yahoo!**のアカウントからすべての情報をとりだした。令状の執行に際して、**Yahoo!**の方針により、技術者は列挙されたアカウントの内容を選択的に取り出したり、みたりすることは禁止されている。**Bach **とＡＭのアカウントから取り出された情報は、**zip **ディスクに記録されるかプリントされるかして、Ｓに送付された。**Bach **のアカウントから回収された電子メールは、彼が他の少年たちと写真を交換し、また交際していたことを詳細に示していた。電子メールのなかには裸の少年の写真を含んでいるものもあった。**Yahoo!**から取り出された情報には、また、**Bach **の住所、生年月日、電話番号および別のスクリーンネームをも含まれていた。**

こうして、捜査官は Bach **家宅の捜索令状**(Hennepin County Warrant)**を入手し、そこからパソコン、ディスク、デジタルカメラ、および、児童ポルノの証拠を押収した。この情報および** Yahoo!**から入手した情報に基づき、**Bach **は児童ポルノの所持、伝送、受領および製造の罪**(18 U.S.C. 、、225A(a)(1) and (2), 2252A(a)(5), 2252A(b)(2), 2252(a)(4), 2252(a)(1) and (2), 2252(b)(2), 2251(a) and (d) and 2253(a))**により起訴された。**Bach **は、両令状の執行により押収された証拠の排除を申し立てた。すなわち、**Ramsey County Warrant **については、相当な理由の不存在、特定性の欠如および違憲立法を理由とするものであり、**Hennepin County

Warrant については、いわゆる「毒樹の果実」論を理由とするものである。

［ミネソタ地方裁判所の意見の要旨］

Ramsey County Warrant について、Bach 側の申立の理由を否定したものの、次のような理由から、令状の執行方法に関して問題があったとして、それにより収集された証拠の排除を認めた。

すなわち、令状を執行する態様は、それが不合理な捜索の禁止という第４修正の一般原則を否定しないことを保障するために、つねに司法的判断の対象となる。18 U.S.C. 3105 は、第三者が捜索において手伝う場合に、令状の執行に際して権限ある捜査官が立ち会い行動することを要求している。本件において、Ｓは、Yahoo!の従業員が Bach のアカウントから情報を捜索・押収するときに、令状執行に際して立ち会っていなかったものであり、Ｓがいなかったことはこの捜索・押収を不合理なものとする。たしかに、連邦の権限に由来するなんらかの支援も受けることなく州法の令状を執行する州の捜査官は、3105 条にしたがう必要はないかもしれないが、しかし、同条によって提供されるのと同様の保護は第４修正のもとに存在している。第三者が捜査官を支援する場合に当該捜査官が令状の執行において立ち会い、行動すべきであるという要件は、一般的な捜索・押収に対する第４修正の基本的な保護を実施するのに有益である。捜査官の指揮・監督の要求される程度は事案の状況に応じて異なる。本件の事情のもとでは、令状をファックスして、なんらの指揮・監督もなく Yahoo!の従業員が捜索・押収をおこなうということは正当化されない。警察官は連邦ならびに州の憲法を遵守することを宣誓し、令状の記載にしたがって合法的に捜索するように訓練を受けている。他方で、一般市民はそのような訓練の対象ではないし、現に、インターネット・サービス・プロバイダは、令状の規定にしたがって支援しているかぎり訴訟から免責されるのである(18 U.S.C. 2703(e))。捜査官の立ち会いがない場合、この条件付きの免責が、令状の明確に記されている限定をこえている捜索をおこなったプロバイダを無条件に保護してしまうことになりうるのである。本件の特異な状況においては、Bach の電子メールのアカウントを捜索・押収した Yahoo!従業員が慎重に本件令状の規定にしたがうことを確保する防壁は存在していない。それゆえ、本件令状の執行は憲法審査を通過するものではなく、本件令状により収集された証拠は排除されなければならない United States v. Moore, 956 F.2d 843, 848 (8th Cir. 1992)において、第８巡回区裁判所が決定したように、場合により連邦法の訴追において使用されうる証拠を連邦と関係なく州の捜査官が押収する場合、この捜査官は州法ならびに第４修正両方の令状要件を遵守しなければならない。連邦法と同様、ミネソタ州法 626.13 および 626A.06 は、法執行官が令状の執行に立ち会わなければならないことを要求しており、したがって、Ｓが本件令状の執行の際にいなかったことはミネソタ州法にも違反している。　Hennepin County Warrant については、Ｓは Ramsey County Warrant により収集された証拠がなくとも本令状を請求することが十分に確実であり、令状請求のための別個の相

当な理由が存在していた。したがって、不法が存在しなくとも証拠を入手することが確実であったので、Hennepin County Warrant により入手された証拠は排除されない。

［第８巡回区裁判所の判断の要旨］

第８巡回区裁判所は、次のような理由から、地方裁判所の判断を破棄し、事件を本裁判所の意見にしたがってさらに手続を進めるために差戻した。これに対して、Bach は合衆国最高裁判所に裁量的上訴受理令状を申し立てたが、棄却されている(Bach v. United States, 155 L. Ed. 2d 693, 123 S. Ct. 1817 (U.S., 2003))。

Yahoo!の技術者がBachの電子メールを法執行機関の立ち会いなく捜索することを許容する場合、MICAC（州捜査官）は 18 U.S.C.§3105 の規定に違反してる。しかしながら、3105 条は本件捜査官には適用されない。本条が連邦捜査官にのみ適用され、州の捜索令状のもとで処理する州捜査官には適用されないからである。U.S. v. Applequist, 145 F.3d 976, 978 (8th Cir. 1998). 捜索をおこなう州捜査官はミネソタ州法 626.13 に違反していたようにみえる。そうであったとしても、そのような違反は、連邦の訴追における連邦裁判所が州法に違反して州捜査官により押収された証拠を、当該捜索が第 4 修正に合致するかぎり、排除しないことから、収集された証拠の排除を保障するものではない。United States v. Moore, 956 F.2d 843, 847 (8th Cir. 1992); Applequist, 145 F.3rd at 978. 3105 条が捜索・押収に関する第４修正の要件を明文化しているとの地方裁判所の決定には同意しないが、3105 条上の審査と憲法上の審査とを分離し、区別するとの第２巡回区裁判所には同意する。Ayeni v. Mottola, 35 F.3d 680, 687 (2d Cir. 1994).（別の理由で破棄されたが、Wilson v. Layne, 526 U.S. 603, 618, 143 L. Ed. 2d 818, 119 S. Ct. 1692 (1999).）したがって、回答すべきものとして残された問題は、本件捜索が第４修正に違反しているかどうかである。

本件における捜索令状の Yahoo!による執行は Bach の第４修正の権利を侵害していなかった。第４修正は令状の執行の際に捜査官の立ち会いを厳密に要求しておらず、したがって、捜索の際に捜査官の立ち会いがなかったとしても、自動的に違反しているということはない。See Wilson v. Arkansas, 514 U.S. 927, 931, 934, 131 L. Ed. 2d 976, 115 S. Ct. 1914 (1995)（捜査官がコモン・ロー上の「事前の告知」の要件にしたがわない場合、第４修正に自動的に違反するのではない。むしろ第４修正のもとでの捜索の合理性を判断する場合に考慮されるべき一つの要素にすぎない、とする。）

第４修正は「合理性」の基準により規定されている。Ohio v.Robinette, 519 U.S. 33, 39, 136 L. Ed. 2d 347, 117 S. Ct. 417 (1996). 対抗している法執行上の諸利益を無視する硬直的な原則を命じているように読むべきではない。United States v. Murphy, 69 D.3d 237, 243 (8th Cir. 1995). 捜査官の存在は捜索令状の執行の合理性を決定する際に考慮される多くの要因の一つにすぎないと考えるべきである。See Wilson, 514 U.S. at 927. その他の重要な要因には、令状の射程範囲、捜索する捜査官の態度、捜索がおこなわれている状況および求めれるべき証拠の性質がある。United States v. Schandl, 847 F.2d 462, 465 (11th Cir. 1991). ある手法が「実

質的に捜索を遂行するために必要とされる時間を増加させ、そのため捜索の妨げとなる場合には、そのような手法を無視することは合理的でありうる。Id. at 466 (quoting United States v. Wuagneux, 683 F.2d 1343, 1352 (11th Cir. 1982).

一般市民による捜索はときとして捜査官による捜索より合理的である。警察官の立ち会いがない市民による捜索も、当該捜索の際に個人によって保持されているプライバシーの量を増加させることもある。Yahoo!技術者による Yahoo!のサーバから Bach の電子メールを捜索・押収することが Bach の第４修正の権利を侵害したかどうかを判断するためには、本件におけるいくつか要因を考慮することになる。それらには、令状が物理的に「送達され」なかったこと、人もしくは物体が伝統的意味において捜索されなかったこと、および、Yahoo! と Bach との間に相反関係がなかったことが含まれる。われわれの判断にとって決定的なその他の要因には以下のことが含まれる。(1)　捜査官の現実の物理的にそんざいしていたとしても、それは捜索には役立たなかっただろうこと（実際は捜索を阻害しうる）、(2)　Yahoo! の技術者の技術的な経験は捜査官のものよりはるかにうわまわっていたこと、(3)　「押収される」対象が Yahoo!の所有物に存在していたこと、(4)　捜索に権限を与える判事の署名した令状が存在したこと、および、(5)　捜査官は電気通信プライバシー法 18 U.S.C. 、2701 の諸項目を遵守していたことがそれにあたる。これらの要因すべては政府の利益に重きを置くことになり、それゆえ、本件捜索は第４修正の合理性の基準に照らして合憲であったということを認定するものである。

［解説］

捜索・押収マニュアルは、Bach 事件がまだ地方裁判所の判断の段階で執筆されており、第８巡回区裁判所の判断はこれを覆すものであるため、マニュアルを補完する意味においても、本判例は紹介の必要性があるといえよう。なお、本件において、MICAC が州の捜査官であり、州法上の令状による捜索であったため、連邦法と州法との関係も論点たりうるが、ここでは、第４修正との関係における問題を中心に扱うことにする。

捜索・押収マニュアルでも示唆されているように、捜査機関が ISP のサーバに蔵置されている顧客のアカウント内の情報を捜索令状に基づき入手する場合、捜査官が実際に当該 ISP へ臨場し、直接 ISP のサーバを捜索したり、ISP の担当者のデータの取り出し作業に立ち会うことはなく、令状を ISP にファックスするなどして送達し、捜査官が立ち会うことなく ISP が令状の文面にしたがって処理をするというのが、実務上の慣行となっている。本件における MICAC 捜査官も同様の対応をしたにすぎない。しかしながら、ミネソタの地方裁判所はこのような捜査の態様をも憲法判断の審査の対象であるとし、第４修正により禁止されている不合理な捜査であるとして、これにより収集された証拠の排除を認めたものである。他方で、電気通信プライバシー法（以下 ECPA とする）は、捜索令状により ISP からコンテンツ情報を押収することを許容しており、地方裁判所の判断が一般的に妥当することになれば、ECPA による場合も同様の制約が付されることになりえた。もっとも、マニュアルも指

摘するように、上記の捜索方法を令状に記載しておけば、この問題は回避可能であるともいえる。

本件における地方裁判所の判断によれば、捜索令状を ISP に送達し、ISP の従業員が令状を執行して、サーバに蔵置されているデータを押収することは、合理的な捜査であるとはいえないとする。すなわち「第三者が捜査官を支援する場合に当該捜査官が令状の執行において立ち会い、行動すべきであるという要件は、一般的な捜索・押収に対する第４修正の基本的な保護を実施するのに有益である。」とし、捜査官の指揮・監督もとでの捜索・押収が望ましいとしたのである。その理由は、捜査官は令状の記載にしたがって合法的に捜索・押収をおこなう訓練を受け、そのような行動を期待できるが、一般市民の場合、捜査官の指揮・監督がない状況において令状の記載にしたがって捜索･押収をおこなうことを保障するものがないということにある。

これに対して、第８巡回区裁判所は、第４修正の審査基準である捜索・押収の「合理性」について、これを弾力的に利益考量により判断すべきであるとし、捜査官が捜索令状の執行の現場に存在していることは合理性を判断する際の一つの要素でしかないとする。合理性判断においては、捜査官が令状執行現場にいることだけではなく、令状の射程範囲、捜索する捜査官の態度、捜索の状況、捜されている証拠の性質が重要な要素であるとし、捜索を実施するのに要する時間を増加させ、捜索を妨げるような捜索方法をとらないことは、合理的でありうるとする。

第４修正が詳細な捜索・押収の方法を規定していない以上、「合理的な」捜索といえるかどうかは、第４修正の趣旨のもとで具体的な判断基準を定立せざるをえないのであり、捜索・押収の態様について種々、さまざまなものを考えることができる以上、そこでは捜索・押収にかかる公的な利益と対象者のプライバシーとの利益考量にならざるをえないであろう。その点において、捜査官の令状執行現場への臨場を硬直的に要求する地方裁判所の考えは妥当ではない。たしかに伝統的な、家宅捜索、有体物としての証拠の押収等については、なお捜査官の臨場が必要であり、そのかぎりで第４修正の理念が 18 U.S.C. §3105 に具体化されているとみることができるかもしれない。しかしながら、第８巡回区裁判所が指摘するように、本件はサーバ内データの押収が捜索の目的であり、ただちに伝統的な捜索の手法が妥当するわけでないといえる。

したがって、第三者である ISP のサーバに蔵置されたユーザのコンテンツを捜索・押収する場合、どのような態様であれば「合理的」であるといえるかどうかを改めて考察することが必要となる。本件では、ISP サーバ内のデータが捜索・押収の対象であったということでかなり決定的な要因となっているといえよう。当該 ISP のサーバ装置全体を押収する場合はともかく、そこに蔵置されている一部のデータのみが対象である場合、捜査官が当該データの押収に関与できる余地は限定されているのであり、現実に捜査官が立ち会ったとしても処理作業をみているだけであり、逆に ISP 会社等の責任者による捜査官への対応の必要性が生じるなど、捜索活動だけでなく、当該 ISP の業務遂行にも影響をおよぼすことにもなりうる

（わが国の ISP においても、顧客データが目的の捜索・押収について、警察への対応が業務遂行および当該データの複写作業を妨げているとの現場の声があることに注意すべきである）。したがって、第８巡回区裁判所がさらに列挙している(1)ないし(5)の要因をもあわせて衡量するのであれば、本件の捜索令状の執行は合理的なのものであり、第４修正に違反するものではないとした、裁判所の判断は妥当であるといえる。なお、本件では、ISP が被告人と無関係であったために、ISP の作業が適切になされうるという状況が存在していたことに注意すべきである。たとえば、ISP への不正アクセス事件などの場合に、被害企業である ISP のデータの捜索・押収については、やはり捜査官の立ち会い、指揮・監督が必要である。この場合、被疑者・被告人と ISP は相対立する関係にあり、捜査官の立ち会いのないことにより ISP の作業が令状の記載通りになされず、ISP 自身の有利になるように操作されるおそれがあるからである。

翻って、わが国における動向に目を向けるならば、記録命令付き差押状の新設が現在立法されようとしている。ここでは、電磁的記録のメディアへの複製により当該電磁的記録ないしは電子計算機の差押えを可能にするものであるが、令状の執行であるため、捜査機関自らあるいは捜査機関の立ち会いの下に複製作業がなされることが前提になっている（たとえば、刑訴法に新設される 110 条の２参照）。これは、これまでのわが国の実務慣行として、有体物の捜索・差押えを前提にして、ISP サーバの差押、検証による複製、仮還付という形態をとってきたことから、これを前提に立法化したことによるのかもしれない。しかしながら、このような捜索方法あるいは立法作業中の記録命令付き差押であっても、場合により、犯罪とは無関係の第三者である ISP の業務に重大な影響をおよぼしうるのであり、ISP の負担の少ない方策をわが国においても今後検討することが必要であろう。本件第８巡回区裁判所が指摘した要因を法律で明文化するのであれば、プライバシー等人権侵害による憲法違反の可能性は少ないであろう。もっとも、そのためには、電話の傍受により生じた電気通信会社等と警察等捜査機関との溝をうめ、両者間の信頼関係を回復することが必要であり、相互の協議により、より適切な捜索・差押えの方法を研究することが必要であろう。

［石井徹哉］

第５　証拠開示における証拠保全義務-Kucala Enterprises Ltd.v. Auto Wax Company(**北イリノイ地方裁判所** 2003 **年** 5 **月** 23 **日**)

［事実の概要］

これは、原告 Kucala Enterprises Ltd.**に対して被告** Auto Wax Company **が申し立てた制裁の申立についての治安判事の報告になる。 原告・被告ともに、自動車ケア製品の会社であり、ディテール・クレイ(車の汚れ取り)の販売をなす会社である。最初に原告が、被告の特許について、有効性と効力を争い、被告の特許の無効の宣言と製造の承諾を求める訴訟を提起した**(2002 **年** 2 **月**)**。これに対して被告は、反訴を提起し、原告（反訴被告）が、被告（反訴原告）の特許を侵害していると主張したのである。**

これらの訴訟において、2002 **年** 12 **月** 13 **日に、地方裁判所は、被告（反訴原告）の原告（反訴被告）に対する製造過程の調査を認めるという開示要求を認めた。 原告（反訴被告）は、この調査に応じなかったが、ついに２００３年２月２８日午後３時に原告（反訴被告）代理人事務所において原告（反訴被告）のコンピュータの調査がなされた。そこで、原告（反訴被告）が、「エビデンス・エリミネーター」というソフトウェアをインストールしていたことが発覚し、被告（反訴原告）が、制裁を求めた事件である。**

［判旨］

「裁判所は、訴訟に重要な証拠の保全をしなかった開示違反の当事者に対して制裁をなす権限がある。連邦民事証拠規則３７条。さらに、連邦民事証拠規則２６条は、停止中の訴訟に含まれる事項に関連する非開示特権のないすべてのドキュメントの提出を要求している。」「裁判所は、当事者の開示違反に対して、制裁を定める広汎な権限を有しており、その制裁のタイプは、一般に事件の事実に依存する。」「訴訟における当事者は、コントロールしうる証拠であって、かつ、潜在的な訴訟にとって関連すると合理的に知っており、または、予測できる証拠を保全する基本的な義務がある」という一般論を述べた。

そして、本件に関して、「裁判所は、Kucala **の行動が、意図的ではないとか、『エビデンス・エリミネーター』を購入し、コンピュータに利用して開示を破壊しようという目的があった行動したのではないとは、考えてはいない。その製品の名前自体からではなくても、ウェブサイトを読めば、『エビデンス・エリミネーター』は、開示を破壊するための製品であると推測することができる。」「裁判所において、『エビデンス・エリミネーター』が、実際に関連する情報を消去したという証拠は有していないけれども、**Mr.Velasco**（訳注、コンピュータ専門家）は、**14，000 **のファイルが** Kucala **のコンピュータから消去されたとしている。『エビデンス・エリミネーター』というソフトウェアの性格および** Kucala **が弁護士より使用しないようにというアドバイスを得ていたということに照らしたとき、この裁判所は、この大量の消去を看過しうるものではない。」という態度を示した。**

そして、結論として、裁判所は、Kucala **が、重大なる過失および裁判所命令を一顧だにせ**

ずに、もしくは、故意に、AutoWax のコンピュータスペシャリストが AutoWax に対して Kucala のコンピュータから関連する情報を得るためにイメージを取得する日の朝の「まさに直前」に、ことさらにファイルを消去していると判断して、「Kucala の行為は、この事件における適切な開示を妨害する以外のなにものでもなく、事実発見者の能力を著しく制限するものである。Kucala は、却下判決（default judgment）は、 AutoWax にとって「たなぼた」であると議論するが、Kucala に対して、訴訟進行を許容すると、利することとなり、将来は、言語道断の訴訟当事者による抜け道を用意することになる。」として、原告の訴訟については、却下が妥当であると判断したのである。

［解説］

本判断は、民事裁判における証拠の保全義務について述べるものであり、意図的な証拠の破壊を理由として、訴訟について却下が相当とされた事案である。

この判断は、以下のような観点から我が国に対しても面白い話題を提供するものと考えられる。

１　証拠の保全と司法省マニュアル

証拠の保全という観点から司法省マニュアルの記載を見るとき、第５章の「コンピュータ記録の真正性と改変」の記載が関連するものであろう。むしろ、現実の実務においては、コンピュータ記録の真正性についての議論は、当然に解決された問題として認識され、それを前提にどのようにして、保全し、分析するか、という問題に問題意識は移ってきているものと思われる。ここで紹介した判断は、民事事件の開示に関するものではあるが、相手方のコンピュータに対して、コンピュータ専門家のアクセスを認めて、そのもとで分析するという手法は、きわめて新鮮で興味深いものである。

また、証拠の保全という観点からみたときに、第３章の「Ｇ　ネットワークプロバイダとの協同；証拠保全、主体への開示防止およびケーブル法問題」の記載とも関連することになる。民事においても、この判断のように証拠の保全という問題が重大なものと考えられているのであれば、刑事においては（第三者のもとにある証拠の問題であるという点で、若干異なるとはいえ）なおさら証拠の保全は重大であると考えることもできよう。場合によっては、協力要請という方法以外にコンピュータ専門家の活用による保全という方向性も考えられるようになるかもしれないのである。

２　コンピュータ法科学におけるｅ開示（e-discovery）の位置づけ

米国においては、証拠について民事訴訟の当事者間において、相手方の証拠を調査することができ、しかも、訴訟状態になった段階から、当事者は、証拠を変更してはいけない義務を負うものと考えられている。現在では、米国において、これらの観点から、ｅ開示が一つの大きな分野として、重要になってきているのである。

この点については、従来は、コンピュータ証拠については、過度に広汎で、負担となり、高価なものであるという理由で、企業は、コンピュータ証拠の開示手続きを避けることができたのである。しかしながら現在では、無条件に、書類は、電子証拠の形態で存在するので

あり、電子証拠の開示は、標準で、ルーチンなものと認識されると裁判所が述べるようになっているのである。この代表的な判決例は、In Re Bristol-Meyers Squibb Securities Litigation, 205 F.R.D. 437 (D. NJ 2002)ということになる。

さらに裁判所は、Residential Funding Corp. vs. DeGeorge Financial という事件において、当事者から電子的文書の開示が、適時で、費用が合理的な検索が困難であるという主張がなされたとしても、これを取り入れず、「意図的な鈍感さ」であるとして、結局、相手方のコンピュータ専門家を認めて、これの相手方のネットワークに対するアクセス（デスクトップやバックアップに対するものを含む）を認めている。

また、他の裁判所においても、コンピュータ証拠に対する開示に対して完全に服するようにという判断がなされている（ Antioch Co. vs. Scrapbook Borders, Inc. 210 F.R.D. 645 (D Minn 2002)、 Tulip Computers International vs. Dell Computer 2002 WL 818061 (D DE 2002)。

ここで紹介した判断は、このような文脈のなかで、意図的にコンピュータ証拠に対する開示を拒絶・妨害しようとした行為に対して裁判所がきわめて厳しい判断を示したものであり、民事裁判における開示の制度がことなる我が国においても、興味深いものとして参考になるであろう。

［高橋郁夫］

第３章　司法省マニュアルと日本法の比較のための基礎的考察

第１論文　「通信の秘密」対「プライバシーの合理的期待」
-米国司法省捜索差押マニュアルの示唆-

高橋郁夫

第１　プライバシーの合理的な期待

本報告書は、司法省のマニュアルの翻訳編とそれを日本法の解釈・運用の参考にするのに際しての基礎知識としての解説分析編からなっている。そして、米国においては、そのコンピュータの捜索・差押えについて、その一つのキーワードとなるのが「プライバシーの合理的期待」であり、一方、我が国においては、「通信の秘密」であると思われる。まず、米国における「プライバシーの合理的期待」の関連する法的論点を簡潔に紹介することにし、その論点に対応するかぎりで我が国の論点を概観することができれば、日本法についての有意義な示唆がえられるものと思われる。

米国においては、「通信の秘密」という概念は、特に定められておらず、むしろ、「プライバシーの合理的な期待」という表現のもとに「通信の秘密」に対応する法的利益の擁護が図られている。そして、この「プライバシーの合理的な期待」という概念をメルクマールにして、「自発的開示」か「強制的開示」かといういわば法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から議論がなされている。しかも、この「通信に関する情報の格付け」については、①それ自体「基本加入者、セッションおよび請求情報」か、「他の取引およびアカウント記録」か、②「アクセスされた通信」か、「検索されていない通信」かという観点から論じられている。(クイックアクセスガイドを再度、以下に掲載する)

	自発的開示の許容性		開示を強制するメカニズム	
	公共のプロバイダ	非公共のプロバイダ	公共のプロバイダ	非公共のプロバイダ
基本加入者、セッションおよび請求情報	§ 2702(c)の例外の適用のない限り、政府に対しては、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(3)]	提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(c)(2)]	提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(c)(2)]
他の取引およびアカウント記録	§ 2702(c)の例外の適用のない限り、政府に対しては、不可 ［§ 2702(a)(3)］	可 [§ 2702(a)(3)]	2703(d) 裁判所命令、捜索令状 [§ 2703(c)(1)]	2703(d) 裁判所命令、捜索令状 [§ 2703(c)(1)]

プロバイダに残るアクセスされた通信（明けられた電子メールおよびボイスメール）および他の記録されたファイル	§ 2702(b)の例外の適用のない限り、不可［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(b)]	提出命令、ＥＣＰＡの適用なし [§ 2711(2)]
電子メールおよびボイスメールを含む検索されていない通信（電気的記録 180 日間を超える）	§ 2702(b)の例外の適用のない限り、政府に対しては、不可［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(a,b)]	通知ありの提出命令、2703(d) 裁判所命令、捜索令状 [§ 2703(a,b)]
電子メールおよびボイスメールを含む検索されていない通信（電気的記録 180 日間以下）	§ 2702(b)の例外の適用のない限り、政府に対しては、不可［§ 2702(a)(3)］	可 [§ 2702(a)(2)]	捜索令状 [§ 2703(a)]	捜索令状 [§ 2703(a)]

第２　「通信の秘密」

１　「通信の秘密」の２つの視点

米国においては、法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から議論がなされている点は、上で指摘した。これに対して、我が国では、「通信の秘密」という概念で議論がなされている。そこで、最初に「通信の秘密」の概念を分析し、それとの関連で、法執行機関と情報とのかかわりという観点と「通信に関する情報の格付け」という観点から分析することになる。

最初に「通信の秘密」の概念を簡単に説明すると、憲法２１条２項後段は、「通信の秘密は、これを侵してはならない」と定めている。そして、「通信の秘密」の内容として、一般には「通信」の「秘密」にかかる事実を「通信当事者以外の第３者が積極的意思をもって知得してはならず」「第３者にとどまっている秘密を、漏洩（他人が知りうる状態にしておくこと)することおよび窃用(本人の意思に反して自己または他人の利益のために用いること）してはならない」の二つの意味を包含するものととらえられている。これらを受けて、電気通信事業法４条は、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」とし、有線電気通信法９条は「 有線電気通信（電気通信事業法第四条第一項又は第九十条第

二項の通信たるものを除く。）の秘密は、侵してはならない。」として、それぞれ通信の秘密の保護を定めている。また、電気通信事業者の取り扱うもの以外の無線通信については、電波法が、５９条において、「特定の相手方に対して行われる無線通信・・・を傍受してその存在もしくは内容を漏らし、又はこれ窃用」することを禁じている。

法執行機関と情報とのかかわりという観点としては、「自発的開示」とのかかわりであるのか、「開示を強制するシステム」であるかという点がポイントとなる点は、前述したが、これは、上記「通信の秘密」という概念とも関連することになる。法執行機関からすると、(ア)法執行機関が積極的にイニシアチブをとることなく[41](イ)情報保持者が、自発的に開示した情報を受領するということになれば、上記定義からいうとき、「第 3 者が積極的意思をもって知得」することにはならないので、法執行機関が「通信の秘密」を侵害するということにはならない。この場合は、その情報保持者が自発的に提供するということになるので、その情報保持者が、「第３者にとどまっている秘密を、漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して自己または他人の利益のために用いること）してはならない」という制限に反するのかどうかという点が問題になることになる。

これに対して、法執行機関がイニシアチブをとって、通信の秘密にかかる情報を取得する場合には、むしろ、そのイニシアチブをとった行為が正当な捜査活動かということが問題になろう。

ここで、自発的開示というのは、強制的手段によらない開示をいう。この点について我が国で対応するものとしては、 (1)通信の情報を保持するもののイニシアチブでなされるものと(2)警察のイニシアチブでなされる場合とがある。そして前者は、(ア)ネットワークの管理等の必要性から情報を取得し、警察等に提供する場合(イ)その他の場合に法執行機関に情報を提供する場合とがあり、また、後者は(ア)任意捜査で警察からの問い合わせに対して回答する場合(イ)捜査関係事項照会書に対して回答する場合の二つの場合がある。

今一つの観点とは、「通信に関する情報の格付け」であるが、この点については、米国において、「基本加入者、セッションおよび請求情報」か、「他の取引およびアカウント記録」か、「アクセスされた通信」か、「検索されていない通信」かという観点から詳細に検討されているが、我が国においては、この峻別という考え方はないものとされている。

以下で具体的に、これらの各場合について、我が国の解釈を検討していくことにする。

２ 自発的開示の類型と法的位置づけ

（１） 自発的開示の類型について

自発的開示の類型については、 (1)通信の情報を保持するもののイニシアチブでなされるものとして(ア)ネットワークの管理等の必要性から情報を取得し、警察等に提供する場合(イ)その他の場合に法執行機関に情報を提供する場合があること、(2)警察のイニシアチブで

[41] なお、この「積極的に」というのは必ずしも強制的にということに限らない。

なされる場合として (ア)任意捜査で警察からの問い合わせに対して回答する場合(イ)捜査関係事項照会書に対して回答する場合の二つの場合があることは前述した。以下、個別に検討していくことにする。

(2)通信の情報を保持するもののイニシアチブでなされる開示

まず、この場合は、法執行機関の積極的知得という要素はないので、むしろ、「通信の秘密」に関する情報保持者において、漏洩または窃用にあたるかということになる。

(ア)ネットワークの管理等の必要性から情報を取得した情報保持者が警察等に提供する場合であろうと(イ)その他の場合に法執行機関に情報を提供する場合であろうと形式的には、「漏洩」という構成要件に該当することになる。従って、そのような観点からは、この提供行為が、違法性阻却自由を備えているのかという観点から考慮されるものと思われる。しかしながら、このような提供行為について、どのような場合が違法性阻却事由となるかという点について、まとめて論じられたことはいまだないように思われる。

一方、これに関する司法省ガイドラインを見るとき、(ア)その情報保持者が「公衆に対してのサービス提供者」か否かによって、公衆に対するサービス提供者でない場合には、自発的開示が認められる(イ)その情報保持者が公衆に対してのサービス提供者である場合については、(1)当プロバイダの諸権利または財産の保護に必然的に付随する場合(2)そのコンテンツが…サービスプロバイダによって意識せずに入手され……、犯罪の遂行に随伴しているようにみえる場合、……法執行官」対して開示がなされる場合(3)プロバイダが「人に対し死または重大な身体的傷害の直接の危険をともなう緊急状況が遅滞なく情報を開示することを必要としていると合理的に信じる」場合(４)児童ポルノ等の制定法によって開示を委任している場合(５)「当事者の同意」がある場合に自発的開示が認められるという。これを参考に、我が国における解釈を考えることは有益であるように思われる。

(ア)情報保持者が「公衆に対してのサービス提供者」であるか否かという観点であるが、これは我が国においても妥当するのであろう。特定多数の者に対するサービス提供の過程で取得している情報(例えば、民間企業におけるイントラネットにおいて会社のサーバ上 の通信データ)については、自発的に法執行機関に提供し得ると考えられるであろう。これは、当然、そのようなネットワーク利用について当事者において合意しているし、民間企業においては、そのネットワークを自己の業務に必要なものとして提供し、また、企業秩序維持等の観点から、自由に処分しうるという要素があるからである。なお、民事であるが、会社の「業務に必要な情報を保存する目的で披告会社が所有し管理するファイル･サーバ上のデータの調査」は、かつ、「会社に持ち込まれた私物を保管させるために貸与されるロッカー等のスペースとは異なり、業務に何らかの関連を有する情報が保存されていると判断されるから、上記のとおりファイルの内容を含めて調査の必要が存する以上、その調査が社会的に許容しうる限界を超えて」その従業員の「精神的自由を侵害した違法な行為であるとはいえない。」とした判決例として日経クイック事件（東京地裁・平成１４年２月２６日判決・労働判例８２５号５０頁）がある。もっとも、このような「公衆に対してのサービス提供」に該

当するかという点については、大学などの場合は、たとえ私立大学であるといっても、ネットワーク利用規約等で自発的開示をする旨を明らかしていたとしてもこの範疇として、常に自発的開示が許容されるのかは、問題であろう。

(イ)その情報保持者が公衆に対してのサービス提供者である場合についても米国にあげられている場合については、我が国でも、法執行機関に対する情報の自発的開示が原則として認められると解されるであろう。情報保持者が、例えば、その管理するシステム(もしくはそれ以外のシステム)に対する攻撃などがあり、そのシステム管理の必要性から攻撃相手の発信元などの情報を突き止め、法執行機関に伝達する場合などである。この場合は、我が国においては、正当防衛などの見地から、かかる発進元の情報を突き止めることは正当化されると考えられるし、その攻撃者の所在を追及し、処罰を求める、もしくは捜査に協力するという見地から、情報保持者の行為は、告発に付随する行為や現行犯逮捕への協力として正当化されるであろう。また、それ以外の場合も正当な捜査協力として正当化されるものと思われる。

(3)警察のイニシアチブでなされる自発的開示

警察のイニシアチブでなされる開示について、任意での協力の問題としては、警察からの任意でのログの提出やその他のファイルの協力、また、何らかの利用者の名簿等の提出の要請などがなされる場合が考慮される。ここで、この自発的開示といっても、捜査関係事項照会書による場合と、それ以外での開示の問題があるように思われる。

まず、一つの参考とるな判決例として事前の警備要請という点から江沢民国家主席の後援会を開催するにあたって早稲田大学が事前に警察に警備を要請し、その際に、講演会に出席する者の名簿を提出したという点について「プライバシーを侵害するものとして不法行為を構成する」と判断した早稲田大学・江沢民講演会事件（ 最高裁平成 15 年 9 月 12 日）についての判断は、興味深い。従って、このような判断からも通信当事者の事前の同意がない場合での「通信の秘密」に関連する事実の法執行機関に対する自発的開示は、情報提供者が「通信の秘密」を漏洩するものとして違法であるということがいえよう。

しかしながら、通信当事者が事前に同意をなしていた場合にはどうかという問題がある[42]。

その上に、捜査関係事項照会書（「捜査については、公務所または公私の団体に照会して必要な事項の報告を求めることができる」-刑事訴訟法１９７条２項）という形式による場合には、さらに解釈上、公務所・公の団体については、報告の義務があると解されている ところでもある。また、私の団体に対しては協力要請の意味しかないとされているが、「これに応じた場合に、通信の秘密との関係で、第三者に対する漏洩の点で違法性が阻却される」ものと解する立場も有力である 。

同意という観点からするとき、民間のプロバイダが、そのポリシーとして「警察署に被害届を提出する際は、捜査関係事項照会書の送付があれば、Yahoo! JAPAN が登録している利

42 また、当事者の同意という観点からは、個別の片側当事者の同意の効力をどう考えるかという問題があるが、ここでは、論じない。

用者情報について回答するという方針を採用しているので、速やかに捜査に着手して欲しい旨をお伝えください。万一、お近くの警察署の対応が不十分であると思われた場合には、都道府県の警察本部のハイテク犯罪を担当している部門宛にご連絡ください。警察署から捜査関係事項照会書の送付を受けた場合には、Yahoo! JAPAN は、捜査に協力しております。」（yahoo オークションヘルプ「詐欺にあわれた可能性があるときに」）として記述している[43]事実は、参考になろう。一方、社団法人テレコムサービス協会は、「〔新版〕インターネット接続サービス等に係る事業者の対応に関するガイドライン」[44] の第１８条（任意捜査その他の照会への対応）において「事業者は、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法律上照会権限を有する者から照会を受けた場合であっても、緊急避難または正当防衛の場合を除き、以下に掲げる通信の秘密に属する事項等を開示してはならない。」としている。なお、そこで、通信の秘密に属する事項とされているのは「(1) 通信の存在及び内容(2) 通信当事者の氏名、住所または居所(3) 通信当事者の電話番号、ＦＡＸ番号、メールアドレス等の通信ＩＤ(4) 通信日時」という事項である。特にこのガイドラインは、従前は、照会文書に対しては任意の開示を許諾していたのを覆したこともあって興味深いものといえる。そして、現在の実務的運用としては、このような判断が主流であるというところもある。

当事者の抽象的同意のある場合と自発的開示の問題については、解釈としては、混沌としているという評価が妥当なように思われるのである。

３　「通信に関する情報の格付け」という観点

(1)通信の構成要素－トラフィックデータとコンテンツ・データ

米国においては、「基本加入者、セッションおよび請求情報」か、「他の取引およびアカウント記録」か、「アクセスされた通信」か、「検索されていない通信」かという観点から詳細に検討されている。一方、サイバー犯罪条約においては、「通信記録」[45]、「加入者情報」[46]に

---

43 http://help.yahoo.co.jp/help/jp/auct/amisc/amisc-15.html

44 http://www.telesa.or.jp/010guideline/guide_2nd/guide2003.htm

45一般にトラフィック・データ(「通信記録」と訳されている)については、「通信記録とは、「コンピュータ・システムという手段による通信に関するコンピュータ・データであって、通信の連鎖の一部を構成するコンピュータ・システムによって作り出され、かつ、その通信の発信元、あて先、経路、時刻、日付、大きさ、持続時間又はその背後にあるサービスの種類を示すものをいう」と定義されている(サイバー犯罪条約 1 条)(なお、翻訳は、http://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf による。以下同じ)。

46 「サービス・プロバイダーによって保有されるサービス加入者に関連する情報のうち、通信記録及び通信内容以外のコンピュータ・データその他の情報であって、それにより次のことが立証されるものをいう。　ａ　使用された通信サービスの種類、そのために使用された技術的設備及びサービスの期間　ｂ　加入者の特定、郵便上の又は地理的な住所、電話番号その他のアクセスのための番号並びに請求及び支払に関する情報であって、サービス契約又は取決めに基づいて利用可能なもの　ｃ　通信機器の設置場所に関するその他の情報であって、サービス契約又は取決めに基づいて利用可能なもの。」

ついても定義がなされている。サイバー犯罪条約は、具体的な規定の相違につながっているものではないが、やはり「通信に関する情報の格付け」に応じて法的規制がことなることもありうるという態度が示唆されているものといえるであろう。

しかしながら、我が国においては、この峻別という考え方はないものとされている。具体的にいうと、「保証の範囲は、通信のすべての構成要素におよび、通信の内容のみならず、通信の存在それじたいに関する事柄－差出人（発信人）・受取人（受信人）の氏名・住所、差出（通話・発信）個数、通信の父時、電話等の発信場所、など－についてもその秘密が保証されなければならない」と説かれるのが常であり、場合によっては、捜査関係事項照会に対して「郵便官署や電気通信事業者が通信に関する事項を報告することは許されないと解すべきである」とされる[47]こともある。そして、この点については、我が国では、内閣法制局意見昭和 38 年 12 月８日および大阪高等裁判所･昭和 41 年 2 月 26 日判決がその解釈の根拠として紹介される。具体的には

（ア）解釈についての歴史的な視点

内閣法制局意見昭和 38 年 12 月８日は、「電話の発信場所は、発信者がこれらを秘匿にしたいと欲する場合がありうるから、右の２項（現行の電気通信事業法第４条２項）にいう『他人の秘密』に該当するものと解すべきであろう」としている。これ以前において、アメリカ法やサイバー犯罪条約などのように、「通信に関する情報の格付け」によって通信の秘密との解釈が影響を受けるべきかどうかという論点についての分析が会ったかどうかについては、今後の調査課題である。

（イ）大阪高等裁判所・昭和 41 年 2 月 26 日判決について

この事件は、郵便局の事務員として郵便物の集配の事務に従事していた公務員が、電報電話局より郵便局に差し出されていた「電話架設のご案内」と表面に印刷してある郵便物について、その名宛人の住所、氏名、電話番号を紙片に書き写し、第三者らに交付した事件について、「信書の秘密」および公務員法上の１００条１項の「職務上知ることのできた秘密」を漏らしたものであるかどうかが、議論された事案でなる。そして、この事案について裁判所は、「そもそも郵便物の委託者は郵便官署を信頼してその秘密を託するものであり、開封の信書や葉書であつても委託者が秘密にすることを欲する場合のあること､そして少なくとも委託者はその郵便物の内容を積極的に他人に公開する意思のないこと､郵便物の発送元や宛先といえども､それが知られることによつて思想表現の自由が抑圧される虞のあることを考えると同法上の信書には封緘した書状のほか開封の書状、葉書も含まれ、秘密には、これらの信書の内容のほか、その発信人や宛先の住所、氏名等も含まれると解すべきである。」としているのである。

---

[47] 樋口・佐藤・中村・浦部編（浦部著）「注解法律学全集２　憲法Ⅱ」（青林書院、1997）85 頁、86 頁

この事案は、事実としては、積極的に知得している点にの特徴がある。すなわち、その公務員について配達中にたまたま電話架設案内の本件書状をみて、その宛先等を知つたというのではなく、郵便局において、電報電話局から一括して差し出された電話架設案内の書状を発見するや、これを局外に持ち出して、その宛先の住所、氏名のほか、書状の中に記載されている電話番号を封筒の隙間から覗き見して書き取ったという行為なのである。これに対して、一般に議論されているのは、郵便官署や電気通信事業者等が通信に関する事項を報告することはどうかという問題であるのである。

このような行為の積極性という観点からいけば、（１）電気通信事業者においては、通信に関する事項が自己の文書として生成される（２）郵便官署としては、その手元にある郵便そのものの情報と自己で処理のさいに作成される自己の文書の双方がある（３）大阪高裁事件においては、公務員であることを奇貨として、委託されていない郵便物について積極的に知得しようとしたという行為であるという点があると分析することができる。この大阪高裁の事件は、ネットワークに置き換えれば、調査の委託を受けたプロバイダが、特定の犯罪の調査のために積極的にパケットを収集する行為ということになる。そのような行為は、「通信の秘密」を侵害するといっているにすぎないのである。仮に、郵便局で、内容証明のリストを作成したとして、それについて任意で提出を求められた際にそれを提出することが、「通信の秘密」を侵害するかという点について裁判所の判断があれば、一般に議論されているような事案について「通信の秘密」の範囲についての判断があるといえようが、現時点では、そのようなことはないといえよう[48]。

（２）通信の形態

また、通信の形態という観点から考察することも可能なように思われる。前述の司法省マニュアルの観点からすれば、電気通信事業者のもとに蓄積された通信について、通信が受信人のもとに到達してしまった後なおも通信の秘密として保護されるのかという問題である。また、電気的記録が１８０日をすぎるかどうかという観点も米国では制定法として加味されている。この点については、我が国では、「電気通信事業者が提供するコンピュータ・サービスも事業者の取扱い中にかかるものであるから、コンピュータに貯蔵・保管された情報にも及ぶと解する立場」と「貯蔵・保管された情報は通信が終了した後コンピュータに保管されたもので、通信そのものではなく、通信サーヴィスの提供とは言えないので通信の秘密保護はおよばないとする立場」とがある。

第３　「通信の秘密」の米国法との比較

１　日本におけるクイックアクセスガイド

最初に米国で議論されている分野においてどのように日本で解釈されているかの比較をすることにする。このためには、クイックアクセスガイドの日本版を作成することにする。

---

[48] もっとも、電信に関する書類の提出については、刑事訴訟法第１００条、１２５条、２１８条および２２０条の規定に基づく請求の場合に限り、これに応ずることという趣旨の内部規定がある。

	自発的開示の許容性（捜査関係事項照会書の議論を除く）		開示を強制するメカニズム	
	公共のプロバイダ	非公共のプロバイダ	公共のプロバイダ	非公共のプロバイダ
基本加入者、セッションおよび請求情報	政府に対しては、不可	可（解釈）	捜索・押収令状（関連性でたりる（解釈））	捜索・押収令状（関連性でたりる（解釈））
他の取引およびアカウント記録	政府に対しては、不可	可（解釈）	捜索・押収令状（関連性でたりる（解釈））	捜索・押収令状（関連性でたりる（解釈））
プロバイダに残るアクセスされた通信（明けられた電子メールおよびボイスメール）および他の記録されたファイル	政府に対しては、不可	可（解釈） なお、日経クイック事件参照	捜索・押収令状	捜索・押収令状
電子メールおよびボイスメールを含む検索されていない通信	政府に対しては、不可	可（解釈） なお、日経クイック事件参照	捜索・押収令状	捜索・押収令状

2　米国の状況との比較

まず、実際の手続きとのバランスからみたときに、我が国においては、通信の構成要素のうち、内容以外のもの（いわば、トラフィックデータに対応する部分）についての開示強制のメカニズムがいわば重い手続きであるということができよう。解釈論上、関連性で足りるのではないかとされているとはいえ、やはり捜索・押収令状によらなければならないとされているのは、比較して、手続き的に重すぎるように思われる。もっとも、この点については、我が国においては、提出命令制度が存在しないことによるものも大きいと思われる。

一つの解釈論の示唆としては、「通信の秘密」との関係で、実務上、位置づけがはっきりしないともいうことができる刑事訴訟法 197 条２項の「捜査関係事項照会書」の運用に、この情報の格付けという観点を加味できないだろうかというアイディアがある。すなわち、捜査関係事項照会書による照会については、その通信の構成要素のうち、トラフィックデータに関する事実については、照会すべき義務があるとするのである。利用者の同意がある場合であってもない場合であっても、現在でも解釈論として、そのように解すべきであると思わ

れるし、また、立法論的には、そのようなものとして、照会に応じない場合についての制裁をも踏まえて制度を構築するというのも良いように思われる。

第 2 論文　「令状によらないコンピュータの捜索・押収」「国外における証拠収集に関わる問題」について

小川佳樹

1. はじめに

アメリカ合衆国（連邦）司法省による、コンピュータの捜索・押収に関するマニュアルである『犯罪捜査におけるコンピュータの捜索・押収および電子的証拠の獲得』[49]（以下、単に「マニュアル」という）の第 1 章は、「令状によらないコンピュータの捜索・押収」と題されている。その目次は、次のとおりである。

A 序論
B コンピュータ関連事件における合衆国憲法第 4 修正の「プライバシーの合理的な期待」
C コンピュータ関連事件における令状主義の例外
D 特殊なケース: 職場の捜索

ここでは、以上のうち、A ないし C で検討されている事項について、解説しておくことにしたい[50]。

2.「令状によらないコンピュータの捜索・押収」

(1) 合衆国憲法第 4 修正は、「不合理な捜索および押収に対して、身体、住居、書類および所持品の安全を保障される人民の権利は、これを侵害することはできない。宣誓または確約によって支持される相当な理由に基づき、かつ捜索すべき場所および、押収すべき人または物を明示したものでなければ、令状は発せられてはならない」と規定し、「捜索・押収」を規律する。これに対し、日本国憲法 35 条は、「何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第三十三条の場合を除いては、正当な理由に基づいて発せられ、克捜索する場所及び押収する物を明示する令状がなければ、侵されない」「捜索又は押収は、権限を有する司法官憲が発する格別の令状により、これを行ふ」と

---

[49] U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2d ed. 2002).

[50]「D 特殊なケース: 職場の捜索」においては、「職場が民間部門に属するものである場合」と「職場が公共部門に属するものである場合」に分けて検討がなされている。このうち前者については、そこで述べられているように、問題状況は、個人の住居等において捜索・押収を行う場合と基本的に異なるところはないが、後者は、まさに「特殊な問題」であるため、ここでは取り上げない。なお、「職場が公共部門に属するものである場合」のリーディング・ケースとして挙げられている O'Connor v. Ortega, 480 U.S. 709 (1987) については、紹介として、高井裕之・判例タイムズ 675 号（1988 年）、竹地潔・季刊労働法 160 号（1991 年）参照。

するが、これは、この第 4 修正に倣ったものである。

マニュアルの第 1 章「A 序論」では、この第 4 修正との関係で無令状の捜索が許容される場合として、次の 2 つが挙げられている。すなわち、①その処分が被処分者の「プライバシーの合理的な期待」に反するものでない場合、および、②被処分者がプライバシーの合理的な期待を有しているが、しかし、当該処分が令状主義の何らかの例外に該当するものであるという場合、である。

ただ、このような整理は、無令状の「捜索」に関するものである点に注意を要する。これに対し、「押収」については、制約される法益として、プライバシーの合理的な期待とは別個に、被処分者の押収対象物に対する占有権等の支配権も観念し得る。したがって、令状によらない「捜索・押収」については、厳密には、被処分者がプライバシーの合理的な期待を有していない場合でも、それで直ちに当該処分が許容されることにはならず、なお、「令状主義の例外」が問題となり得ることになる[51]。

いずれにせよ、マニュアルの第 1 章においては、以上のような分析枠組みがコンピュータ関連事件においても妥当するとされ、コンピュータの捜索・押収につき、通常の捜索・押収のいわば応用編として、説明が進められている。したがって、話の大部分はコンピュータの捜索・押収に固有の問題ではなく、捜索・押収一般に関わるものであるが、以下、わが国との比較も交えつつ、簡単にみていくことにしよう[52]。

上述のように、アメリカ法では、無令状捜索・押収が許されるか否かを決する第 1 の基準として、「プライバシーの合理的な期待」の有無が問題となるわけであるが、これに対し、わが国においては、刑訴法上、いわゆる任意処分と強制処分の区別があり、強制処分については「この法律に特別の定めのある場合でなければ、これをすることができない」とされている（強制処分法定主義）（刑訴法 197 条 1 項）。強制処分とは、判例によれば、「個人の意思を制圧し、身体、住居、財産等に制約を加えて強制的に捜査目的を実現する行為など、特別の根拠規定がなければ許容することが相当でない手段」を指す[53]。現行刑訴法によって、捜査段階における証拠収集のための強制処分として用意されているのは、捜索（刑訴法 218 条 1 項）、差押え（同）、検証（同）、通信傍受法（「犯罪捜査のための通信傍受に関する法律」平成 11 年法律第 137 号）に従ってなされる通信傍受（刑訴法 222 条の 2）等である。以上の処分はいずれも、憲法 35 条にいう「侵入、捜索及び押収」に当たると解され[54]、したがって、これらの処分を行うには、令状が必要となる（令状主義）（憲法 35 条）。

---

51 もっとも、このようなケースは、すべて、令状主義の例外の 1 つとしての「プレイン・ビューの法理」（後出）などによってカバーされることになると思われる。それ故、結局、マニュアルの述べるように、無令状捜索・押収は、①プライバシーの合理的な期待に反しないか、②当該処分が令状主義の例外に該当するものであれば、許容されることになる。

52 なお、マニュアルで引かれている第 4 修正関連の判例については、鈴木義男編『アメリカ刑事判例研究 第 1 巻-第 4 巻』（成文堂、1982 -1994 年）等を参照。

53 最決昭和 51 年 3 月 16 日・刑集 30 巻 2 号 187 頁。

54 この点につき、田宮裕『刑事訴訟法（新版）』101 頁（有斐閣、1996 年）参照。

なお、これら刑訴法上の強制処分のうち、「捜索」は「差押え」対象物を発見するための処分と捉えられ、「差押え」の対象は、有体物に限られると解するのが一般的である[55]。これに対し、アメリカの第 4 修正における「押収」については、有体物のみならず、例えば、有体物たる記録媒体に収められた無形のデータそれ自体も、その対象となり得る。したがって、コンピュータに記録されたファイルが押収の対象とされている場合、コンピュータを起動させてそのファイルを検索することは、アメリカ法においては、「捜索」ということになる。

（2）さて、「B コンピュータ関連事件における合衆国憲法第 4 修正の『プライバシーの合理的な期待』」においては、「プライバシーの合理的な期待」の有無に関する裁判例の状況が概観されている。ここでは、そこで「プライバシーの合理的な期待と第三者の保有」として取り上げられている、インターネット・サービス・プロバイダが保有する加入者情報等の取得について、触れておこう。

インターネット・サービス・プロバイダが保有する加入者情報等を獲得する手続については、いわゆる電気通信プライバシー法――マニュアルでは、第 3 章で詳しく解説されている――に定めがあるが、この種の情報について、プロバイダの顧客は、プライバシーの合理的な期待を有しないとされている。

この点に関し、わが国では、憲法 21 条 2 項で「通信の秘密」が保障され、また、法律により、「電気通信事業者」――プロバイダもそこに含まれる――は「取扱中に係る通信の秘密は、侵してはなら」ず、そのような「通信に関して知り得た他人の秘密を守らなければならない」とされる（電気通信事業法（昭和 59 年法律第 86 号）4 条）。ここでいう「通信の秘密」には、通信の内容のみならず、個々の通信における発信元および受信先の識別子や、通信があったという事実も含まれる。しかし、個々の通信とは切り離された形での加入者の氏名・住所等は、この「通信の秘密」には該当しないとするのが一般的であるといわれる。それ故、例えば、プロバイダが、捜査機関の求めに応じて、特定の電子メールにつき、その発信者または受信者が誰であるかを任意に開示することは「通信の秘密」を侵すことになるが、あるアドレスにつき、それを使用している加入者は誰であるか、という形の問い合わせに対して情報を開示することは、この秘密を侵害するものとはいえないことになる。しかし、このような情報も、問題を「通信の秘密」に反するか否かではなく、より広く個人情報の保護という観点から捉えると、やはり、プロバイダが自由にそれを処分できるとするのは相当ではなく、捜査機関としては、このような情報を得るためには、刑訴法上の照会手続（197 条 2 項）によるか、あるいは令状を得て強制処分をなすべきであるとされている[56]。

（3）「C コンピュータ関連事件における令状主義の例外」においては、判例によって認め

---

[55] この点につき、例えば、安冨潔『ハイテク犯罪と刑事手続』163-164 頁（慶應義塾大学出版会、2000 年）参照。

[56] 以上の叙述は、井上正仁「コンピュータ・ネットワークと犯罪捜査（1）」法学教室 244 号 55 頁（2001 年）による。

られている合衆国憲法第 4 修正の令状主義の例外、すなわち、「同意」、「緊急性」、「プレイン・ビューの法理」、「適法な逮捕に伴う捜索」、「押収目録作成のための捜索（インベントリー捜索）」、および、「国境における捜索」について検討がなされている。

このうち、「緊急性」の例外とは、個々の事案において、証拠隠滅の防止などにつき、その緊急の必要性があることを理由に、無令状の捜索・押収を認めるというものである[57]。

これに対し、「プレイン・ビューの法理」とは、判例によれば、次のようなものである。すなわち、①捜査官が当該場所へ適法に立ち入ったか、あるいはそこに適法に所在し、②そこで犯罪の証拠物であることが一見して明らかな物件を視認した、という場合、③当該物件を無令状で押収することが許される、と[58]。つまり、この法理は、プライバシーの合理的な期待が問題とならない情況のもとで、現認された証拠物を押収する、というものであり、したがって、「無令状捜索・押収」ではなく、「無令状押収」に関わる「令状主義の例外」である。そして、この法理が許容される根拠は、このような無令状押収を許容することの必要性と、それによって制約される被処分者の利益衡量の結果にあるとされる。すなわち、証拠物であることが明白である――すなわち、「相当の理由」が存する――以上、令状を請求したならば当然これが発せられるはずであり、そのような情況のもとで令状請求手続という「形式」を踏むことを求めるのは、捜査の効率性を減殺するし、また、令状を請求している間に証拠の隠滅がなされることもあり得る。このような「必要性」が、一般的に――すなわち、個々の事案において捜査の効率性・証拠隠滅の危険性を具体的に問題にすることなく――被処分者の押収物に対する支配権に優位する、というのである[5960]。

わが国の状況については、これら「例外」のうち、前 4 者について、簡単にみておこう。

まず、「同意」であるが、これについては、わが国では、「令状主義の例外」として許されるか、という形での問題設定はなされておらず、任意処分として可能であるかが問題とされる。この点で、刑訴法 221 条は、「〔所有者等が〕任意に提出した物は、これを領置することができる」とするが、これは、「押収を受けることのない権利」の放棄を認めたものとい

---

57 アメリカ法における「緊急性」の例外については、例えば、林正人「『緊急性』と令状によらない捜索・押収（1）（2・完）」法学論叢 145 巻 5 号、147 巻 4 号（1999-2000 年）参照。

58 酒巻匡「いわゆる『緊急差押』について」内藤謙先生古稀祝賀『刑事法学の現代的状況』436-442 頁（有斐閣、1994 年）。

59 酒巻・前掲注（10）442-443 頁。

60 アメリカ法における「プレイン・ビューの法理」については、酒巻・前掲注（10）のほか、例えば、香川喜八朗「プレインヴィュー法理の展開」高岡法学 4 巻 1 号（1992 年）、林正人「プレイン・ヴュー法理（1）（2・完）」法学論叢 143 巻 3 号、145 巻 1 号（1998-1999 年）、佐藤隆之「別罪証拠の差押え」現代刑事法 5 巻 5 号（2003 年）参照。

また、この法理は、対象物を――「視認」ではなく――触覚によって現認した場合についても妥当するものとされている（「プレイン・フィールの法理」）。この点については、例えば、稲田隆司「合衆国における『プレイン・フィール法理』の成立と展開」北大法学論集 46 巻 4 号（1995 年）、洲見光男「『プレイン・フィール』の法理」下村康正先生古稀祝賀『刑事法学の新動向 下巻』（成文堂、1995 年）参照。

えよう。問題は捜索についてであるが、理論的には、押収と別異に解する理由はないであろう。判例も、「同意」に基づく「捜索（所持品検査）」を認めている[61]。ただし、捜査実務上は、住居等の捜索につき、「住居主または看守者の任意の承諾が得られると認められる場合においても、捜索許可状の発付を受けて捜索をしなければならない」（犯罪捜査規範 108 条）とされていることに注意を要する。これは、「同意」の扱いについて慎重を期したものといえよう。

「適法な逮捕に伴う捜索」については、わが国においても「令状主義の例外」という位置付けられ、許容されている。すなわち、その理由付けおよびそれが許容される範囲については、学説上、争いがあるが、憲法 35 条 1 項の明文で、令状によらない「侵入、捜索及び押収」が認められ、これを受けて、刑訴法も、無令状の「捜索」「差押え」「検証」を許している（220 条）。

では、「緊急性」および「プレイン・ビューの法理」についてはどうか。捜索・差押えとの関連では、現行刑訴法にはこれらに関する明文規定はなく、それ故、強制処分法定主義の建前から許されないと解するのが一般的であり、実務もそのような理解を前提に行われている[62]。さらに、立法論としてみても、「緊急性」の例外を認めることについては、憲法上、これを疑問とする向きが多いように思われる[63]。これに対し、「無令状の押収」的処分に関しては、通信傍受法 14 条が、「傍受の実施をしている間に、傍受令状に被疑事実として記載されている犯罪以外の犯罪であって、別表に掲げるもの又は死刑若しくは無期若しくは短期 1 年以上の懲役若しくは禁錮に当たるものを実行したこと、実行していること又は実行することを内容とするものと明らかに認められる通信が行われたときは、当該通信の傍受をすることができる」と規定していることが注目される[64]。

以上のように、アメリカでは、令状主義に対しては多くの例外が認められており、また実際上も、無令状捜索・押収の数が令状による捜索・押収の数をはるかに上回っているとされる[65]。これに対し、わが国では、「令状主義の例外」として承認されてきたのは、伝統的には、証拠収集のための処分では、「適法な逮捕に伴う捜索（および押収）」のみである。このような違いが生れる背景には、1 つには、憲法 35 条と合衆国憲法第 4 修正の文理上の相違という事情を挙げることができるのではないかと思われる。すなわち、憲法 35 条が令状主

---

61 最三小決平成 7 年 5 月 30 日・刑集 49 巻 5 号 703 頁参照。

62 もっとも、無令状の「緊急捜索・差押え」が現行法上も可能だとするものとして、例えば、渥美東洋『刑事訴訟法（新版補正版）』96-97 頁（有斐閣、2001 年）参照。また、田宮・前掲注（6）105 頁は、「プレイン・ビューの法理」につき、これを「採用する余地がないわけではない」とし、その要件として「①適法な職務執行中に、②偶然の事情で、③明白な犯罪関連物件を発見し、④それ以上の捜索を要せず直ちに差押えが可能であり……その物件についてたんなる不審理由ではなく、『相当な理由』が肯定される」ことを挙げる。

63 この点で、例えば、法学協会編『註解日本国憲法 上巻』630 頁（有斐閣、1953 年）、井上正仁『捜査手段としての通信・会話の傍受』198 頁（有斐閣、1997 年）参照。

64 この点につき、井上・前掲注（15）188-205 頁参照。

65 林・前掲注（12）「プレイン・ヴュー法理（1）」67-68 頁。

義を――その例外を具体的に挙げつつ――厳格な形で規定しているのに対し、第 4 修正は、後段で令状について述べつつも（「令状条項」）、前段で捜索・押収が合理的であることを求め（「合理性条項」）、結局、「不合理な」捜索・押収を受けない権利を保障することが究極的な目標と解され得る規定形式となっている[66]。そのため、令状を要求することによって確保される利益に優越する利益が存在すると認められる場合には、無令状の捜索・押収も――「合理的」なものとして――許容されるのだ、という論理が受け入れられやすいのではないだろうか[67]。

3.「国外における証拠収集に関わる問題」

マニュアルの第 1 章「C コンピュータ関連事件における令状主義の例外」においては、さらに、「国外における証拠収集に関わる問題」について概説され、併せて、関連する国際的な動向について言及がなされている。

国外に所在する証拠の収集については、従来から、公式の手続として、いわゆる国際司法共助・捜査共助があり、これらによれば、関係する外国政府に依頼して、当該証拠を確保してもらうことになる。しかし、インターネットなどの、地球規模のネットワークにおいて犯罪の捜査を行うとなると、証拠となるデータが外国に所在するサーバに蔵置されている、という事態がしばしば起こり得るが、このような場合に、証拠を迅速に確保するため、ある国の捜査機関が直接、外国に所在するコンピュータにアクセスするとなると、他国の主権との関係が、問題となり得る。このため、コンピュータ・ネットワークに関連した犯罪については、国際的な調整が必要となってくるのである[68]。また、ネットワークを介した犯罪は多くの国々に影響を及ぼすものであるため、国際的な連携をどのように確保するかも重要な課題となる[69]。

この点で注目されるのが、マニュアルでも言及されている、2001 年 11 月に採択された欧州評議会の「サイバー犯罪条約」である[70]。わが国も、アメリカなどとともにオブザーバー

---

66 もっとも、これら 2 つの条項の関係については、古くから論争があるところではあるが。この点につき、例えば、林・前掲注（12）「プレイン・ヴュー法理（1）」63-67 頁参照。

67 なお、この点に関し、井上・前掲注（15）194-195 頁参照。

68 古田佑紀「コンピュータ・ネットワーク上の捜査と第三者の保護」『松尾浩也先生古稀祝賀論文集 下巻』201 頁注（8）（1998 年）、長沼範良「ネットワーク犯罪への手続法的対応」ジュリスト 1148 号 216 頁（2001 年）、井上・前掲注（8）「コンピュータ・ネットワークと犯罪捜査（1）」53 頁、同「コンピュータ・ネットワークと犯罪捜査（2）」法学教室 245 号 55-57 頁。

69 井上・前掲注（8）「コンピュータ・ネットワークと犯罪捜査（1）」53 頁。

70 サイバー犯罪条約を含む、コンピュータ・ネットワーク関連犯罪対策に関する国際的な動向については、例えば、井上・前掲注（8）「コンピュータ・ネットワークと犯罪捜査（1）」53 頁、川出敏裕「コンピュータ犯罪と捜査手続」法曹時報 53 巻 10 号 2-3 頁（2001 年）参照。また、とくに、マニュアルで言及されている、G8 サミットのリヨン・グループ（国際組織犯罪上級専門家会合）のもとにあるハイテク犯罪サブグループについては、大須賀寛之「G8 ハイテク犯罪サブグループの動向」法とコンピュータ 21 号 65 頁（2003 年）参照。

国としてその作成に当初から関与し、署名を行っている。これは、世界初のコンピュータ関連犯罪対策に関する包括的な条約であり、今後、この分野における事実上のグローバル・スタンダードとなることが予想される。そして、署名国にはこの条約の締結のため関連する法の整備が求められており、わが国でも、現在、具体的な立法が検討されている[71]。すなわち、2003 年 9 月 10 日に、法制審議会において「ハイテク犯罪に対処するための刑事法の整備に関する要綱（骨子）」が採択され、法務大臣に答申されているのである[72]。

---

71 サイバー犯罪条約の内容、および、同条約とわが国の法整備との関係については、例えば、サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」（経済産業省、2002 年 4 月）
［http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf］、瀧波宏文「『サイバー犯罪に関する条約』について――手続法及び国際協力規定（上）（中）（下）」警察学論集 55 巻 9 号 150 頁、10 号 113 頁、11 号 105 頁（2002 年）、酒巻匡「サイバー犯罪条約の手続法規定について」法とコンピュータ 21 号 57 頁（2003 年）参照。

72 これについては、「特集・ハイテク犯罪に対する立法課題」ジュリスト 1257 号 6 頁（2003 年）参照。

第３論文　「令状に基づくコンピュータ捜索･差押えにおけるコンピュータデータの取扱い」

小島淳

第１　はじめに

わが国においては、これまで、捜査機関がコンピュータを捜索し、その中に蔵置されたデータを入手するという場合、現行法上規定された強制処分の枠内でそれを行いうるか、もし行いうるとすると、それはいかなる処分として可能なのかということが議論されてきた。こうした議論は、情報通信科学の目覚しい発展によって生じた新しい犯罪状況に捜査機関が対応し、実体的真実発見への足がかりをつけると同時に、憲法 35 条に規定された令状主義や同 31 条及び刑事訴訟法 197 条を根拠とする強制処分法定主義との抵触を防ぎ、被対象者に対する人権侵害を最小限に食い止めるためにどうしても必要なものであったといえよう。ただ、そのようないわば「古い皮袋に新しい酒を盛」ろうとする議論自体にそもそも限界があったことや、サイバー犯罪条約の影響を受け、最近では、端的に新しい立法によって問題に対処しようとする動きが見られる。

ただ、今般の立法の動きの中で、わが国におけるコンピュータ捜索・差押えについての議論が重要な役割を果たしてきたことは言うまでもない。したがって、今回提案されているような新たな捜査手法が立法を経て実際に活用可能となった場合には、捜査機関としても、そうした議論を十分に理解した上でそれを活用する必要があろう。

また、少なくとも現在提案されている各種の措置によって、これまで議論されてきた問題が全て解決されるわけではないように思われる。今回の提案は、現在の捜査における基本概念の枠組み自体は維持しながら、新たな捜査手段を設けようとしたものである。しかし、そうした制約があるために、かえって、実際に有効な捜査手段を提供できているのか疑問とする向きもあろう。他方、これらの新たな手法が活用されることになれば、対象者の権利が不当に侵害される虞があることも指摘されている。そして、さらに問題なのは、現行の捜査理論との調和を意図してなされたこの立法が、その狙いを十分に達成しきれていないきらいがあることである。（以上につき、詳しくは後掲安富論文参照）。

このようなことからすると、今後（コンピュータデータ等の情報それ自体を直接対象とする押収処分の創設、情報通信手段のさらなる発展に伴う各種処分の新設等も含め）新たな立法が必要となることも十分予想される。その際には、従来は予測できなかった全く新しい問題について議論すべきことは勿論のこと、なぜそれまでの制度では不十分だったのかを、当該制度を設けた際に参考とされた議論にまで遡って検証すべき場合もあろう。

このように、新たな立法の動きが見られる現在においても、これまでなされてきた議論の理解は極めて重要であると考えられるため、本稿においては、特にコンピュータ捜索・押収におけるコンピュータデータの取り扱いに関するわが国におけるこれまでの議論を概観し、その到達点を確認しておくこととしたい。

第 2　わが国の令状捜索・差押えにおけるコンピュータデータの取扱い

わが国においては、憲法 35 条において「住居、書類及び所持品について侵入、捜索及び押収を受けることのない権利」、「捜索する場所及び押収する物を明示する令状」との表現が用いられており、これを承けた刑訴法 99 条 1 項、219 条等においても、「差し押えるべき物」、「捜索すべき・・・物」等とされていることから、一般的には、捜索・差押えの直接の対象は有体物であると解されている[73]。このため、捜査機関が特定のコンピュータデータを入手するためには、そのデータが化体していると考えられる各種の電磁的記録媒体の存在しうる場所及び当該記録媒体を特定・明示する令状に基づき当該場所を捜索し、当該記録媒体を差し押さえることとなる。しかし、コンピュータデータは、そのままでは可視性・可読性がなく、さらには、記録媒体に貼付された表示ラベル等に記された情報が偽りであることも考えられるため、ある記録媒体が目的とするデータを含むものであるかどうかは、何らかの形で当該記録媒体に含まれるデータを出力してみないと識別困難なことが多い。また、コンピュータデータは簡単な操作により移動・改変・削除することができ、しかも、ネットワークコンピュータに蔵置されたデータについては、遠隔的にそれらの操作を行うことも可能である。こうした操作を通じて重要な証拠が隠滅されたりすることも考えられ、証拠を保全する高度の緊急性が認められる場合も多いといえよう。このようなコンピュータデータの特性から、判例及び学説上、捜索・差押えの際のコンピュータデータの取扱いに関しては様々な問題が論じられてきた。ここでは、これまで判例・学説上争われてきた代表的な論点[74]についての議論を概観する。（なお、これらの議論のうち、今般の立法提案において取り上げられたものについては、後掲の安富論文において詳細に検討されているため、主にそちらを参照され

---

[73] 藤永幸治ほか編・大コンメンタール刑事訴訟法第三巻［渡辺咲子］241（青林書院、1994）、松尾浩也（監）・条解刑事訴訟法〔第 3 版〕・171（弘文堂、2003）など参照。これに対し、①わが国の憲法 35 条が、個人のプライバシーを保護する合衆国憲法第 4 修正と「同様」のものであるとして、可視性、可読性のない無体情報も同条にいう押収の対象となること、②そのように解した場合でも、無体情報としての電磁的記録が「記録媒体に記録されたり、一定の用紙に印字出力（プリントアウト）されたりして、物理的に管理可能な形態で有体物に化体するもの」であって、「これらを一体的にとらえて、有体物の捜索・差押えとみることもできる」ため、法 99 条 1 項の文言との整合性も保たれることを指摘するものとして、安富潔・ハイテク犯罪と刑事手続・163－164（慶大出版会、2000）。なお、この点の議論の詳細については、小川新二「磁気のディスクと捜索差押え」平野龍一ほか編・新実例刑事訴訟法Ⅰ・251、254（青林書院、1998）、稲垣隆一「情報と強制捜査―捜索押収の対象について―」多賀谷一照ほか編・情報ネットワークの法律実務・5027（第一法規、1999）、川出敏裕「コンピュータ犯罪と捜査手続」曹時 53・10・2747、2750（2001）など参照。

[74] なお、ほかに、被処分者の積極的な協力義務についての問題、押収済記録媒体の内容の解析・印字出力に関する問題、コンピュータデータの検証・鑑定に固有の問題、さらには国境越え捜査の問題などがあるが、紙幅の関係上ここでは省略する。なお、特に協力義務については、川出・前掲注（1）・2759－2765、長沼範良「電磁的情報に関する捜索・差押え」現刑 49・45、48（2003）（プロバイダに対する提出命令）、国境越え捜査については、井上正仁「コンピュータ・ネットワークと犯罪捜査（2・完）」法教 245・49、55－57（2001）参照。

たい。）

１．　捜索差押令状における捜索場所、差押対象物の特定・明示

（１）捜索すべき場所の特定・明示

コンピュータ捜索を許可する令状における捜索すべき場所の特定･明示という問題に関してこれまで議論されてきたのが､捜査機関が入手したいと考えるデータが被処分者の使用している端末（以下「A」という）と接続されたサーバないしネットワークコンピュータ（以下「B」という）に蔵置されており、かつ B が A の設置されている場所とは別の場所にあることが判明したという場合の取扱いについてである。このような場合に、A の設置場所を「捜索すべき場所」として特定・明示（し、「差し押さえるべき物」として当該データに関わるコンピュータ一式、FD 等の電磁的記録媒体を特定・明示）する令状に基づいて、B に蔵置されたデータを取得することは許されるだろうか。差押えの対象が有体物たる記録媒体であるとすれば[75]、「捜索すべき場所」は、当該記録媒体（本設問では B）の存在しうる物理的な意味[76]での空間であると考えられ、その場合の差押えの対象物は、その場所に設置されたコンピュータ等に限定されるものと考えられる。そこで、こういった場合には、「捜索すべき場所」の記載に B の設置場所が含まれ、「差し押さえるべき物」の記載に B が含まれるような別個の捜索差押え令状によることが必要となると考えられる[77]。

では、直接 B の設置場所に赴いて捜索・差押えを行うのではなく、捜査官が A を利用して B にアクセスし、当該データを出力・印字して、あるいはコピーを作成した上で、それらの記録媒体を差し押さえるといった措置を取ることはどうだろうか[78]。当初の令状に基づいて A を差し押さえることが許されるからといって、A を通じて B にアクセスする権限までが捜査機関に移るとは考えにくいこと―この権限は特定の端末に帰属するというよりも、

---

75 この点、処分の対象がデータ自体であると考えれば、その所在場所の如何を問わず、当該データが特定されていれば足りるとすることも可能であろう（厳密に言えば、その場合に問題となるのは、「捜索すべき場所」ではなく「差し押さえるべき物」の特定である）。

76 したがって、電子空間としてのコンピュータ・ネットワークそのものを「捜索すべき場所」とすることは許されない。稲垣・前掲注（2）・5004。川出・前掲注（1）・2758-2759。なお、「所在する場所によって特定されることは必須ではなく、それに代わる要因によって適切に特定されていればよいと考えられる」とするのは、井上正仁＝池田公博「コンピュータ犯罪と捜査」ジュリ増刊 刑事訴訟法の争点〔第 3 版〕・88、90（2002）。

77 小川・前掲注（1）・253 は、別個の検証令状によるべきであるとするが、この点については後述参照。なお、「大学、官庁、銀行、病院、ホテルなど、各部屋の管理が独自になされては」いるが、「各部屋を総括する包括的地位を有する者」が存在し、そ「の管理権を単位として考え」ることができる場合について、A 及び B の設置された部屋を含む建物そのものを「捜索すべき場所」として記載することで特定としては十分であるとする考え方もある（稲垣隆一「情報と捜査―捜索差押え実務上の問題点―」多賀谷一照ほか編・情報ネットワークの法律実務・5004（第一法規、1999））が、疑問なしとしない。

78 この問題は、正確には「差し押さえるべき物」の特定・明示の問題である。また、当該出力・印字処分の性質及びその場合の「差押え」の意義についての議論（後述）とも関係するものである。ただ、直前の記述と同様、ネットワークコンピュータに関連する問題であるので、次の段落の立法提案についての記述も含め、便宜上ここで論じるものとする。

むしろ当該端末の利用者たる人に帰属する[79]と考えるのが自然である―などからすれば、結論としては、現行法の下では許されないといえよう。

なお、このような議論を背景に、今般の立法提案は、新たに「差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であつて、当該電子計算機で処理すべき電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は当該他の記録媒体を差し押さえることができる」とし、当該差押え令状において「差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって、その電磁的記録を複写すべきものの範囲を記載しなければならない」とする規定を設けるべきものとしている。

（2）差し押さえるべき物の特定・明示

ⅰ.「差し押さえるべき物」の特定・明示に関しては、そもそも差押えの対象をデータそのものと考えるか、当該データの化体した有体物たる電磁的記録媒体と考えるかが問題となるが、現行法の解釈論としては、有体物たる記録媒体を対象とするものと解する見解が優勢であることは既に述べた[80]。今般の立法提案も、こうした理解に変更を迫るものではなく、むしろその理解を当然の前提としているものと考えられる。

ⅱ. 差押え対象物が有体物たる電磁的記録媒体であるとの理解を前提にすると、令状記載との関係でまず問題となるのが、令状における「本件に関係ありと思料されるフロッピーディスク等の電磁的記録媒体」等の記載が特定として十分といえるかどうか[81]である。この点、電磁的記録媒体は、その形状及びその中に記録された内容によって被疑事実との関連性が判断されるのであって、その記録媒体の形態及びそこに記録されている内容が特定されない限り、「差し押さえるべき物」として特定されたとは言い難いように思われる。令状請求時までに判明している事情を参考に、記録媒体の形態や、そこに記録された情報内容との関連でできる限りこれを特定し、「・・・を明らかにするための・・・売上台帳、顧客名簿、・・・その他本件に関係ありと思料される情報が記録された磁気記録テープ、光磁気ディスク、フロッピーディスク、パソコン一式」等の具体的な記載が必要となろう[82]。

---

79 川出・前掲注（1）・2756。

80 なお、有体物説に立ちつつも、コンピュータデータを入手することを目的として当該データの記録された電磁的記録媒体を対象とする差押えを行うことに疑問を呈するものとして、稲垣・前掲注（1）・5028－5030 がある。これは、電磁的記録媒体を「鍵のついた閉架式の書庫に類している」ものと位置づけ、電磁的記録媒体と文書との違いを浮き彫りにしようとしたものである。なお、この見解に対する批判については川出・前掲注（1）・2751 参照。

81 小川・前掲注（1）・256。

82 なお、「電磁的記録媒体の種類及び名称、必要な電子ファイルの名称及び特徴、ファイル処理のためのプログラムの名称及び特徴、必要なオペレーティングシステムの名称、適用ハードウェアの形式」まで特定することが望ましいことは確かだが、捜索・差押えが捜査の初期段階で行われることからすれば、それが実際に可能な場合の方が少ないとも考えられる。

iii. では、逆に、「差し押さえるべき物」として「・・・売上台帳、顧客名簿、・・・その他本件に関係ありと思料する文書」との記載があるのみで、電磁的記録媒体についての記載を欠く令状に基づいて、売上台帳や顧客名簿のデータが記録された電磁的記録媒体を差し押さえることは許されるだろうか。この点、文理的には「売上台帳」、「顧客名簿」が「電磁的記録媒体を含まないとは直ちに言い難く」、「コンピュータ処理が日常のこととなった現代社会の感覚」では、「売上台帳」ないし「顧客名簿」の内容が記録された媒体は「売上台帳」ないし「顧客名簿」そのものとも考えられよう[83]。ただ、「コンピュータ処理が日常のこととなった」ことを前提にするのであれば、捜査機関としても予め差押えの対象物が電磁的記録媒体となることを想定して捜査を進めておくべきであり、それまでの捜査によって判明している事情をもとに、令状請求の段階で、考えられる電磁的記録媒体に言及しておくことも比較的容易であると考えられる。こうした状況に鑑みると、令状において一切電磁的記録媒体の記載がない場合には、電磁的記録媒体については「差し押さえるべき物」から排除する趣旨であると解される余地もあろう。そうであれば、性質上電磁的記録媒体として存在することが全く予想できないような特殊な場合を除けば、特定の電磁的記録媒体について、令状において「差し押さえるべき物」として明記しておく必要があると考えられる。

２．電磁的記録媒体の差押えの要件

（１）無関係なデータを含む電磁的記録媒体の差押え

一般に、ある物と被疑事実との関連性があり、その物を差し押さえる必要性（ないし相当性）があれば、その物を特定・明示する令状に基づいてその物を差し押さえることが許される。では、ある電磁的記録媒体の中に蔵置されたデータのうち、被疑事実との関連性を有すると認められるものがごく一部であって、その他の（大半を占める）データは被疑事実と無関係なものであるという場合において、当該記録媒体をそのまま差押えることが許されるか。東京地決平 10・2・27 判時 1637・152 は、顧客 428 名分のデータが記録されていた 1 枚のフロッピーディスク（以下「FD」という）を差し押さえた捜査機関の処分につき、被疑者に関するデータについては「本件被疑事実との関連性、差押えの必要性は明らかである」が、それ以外の顧客に関するデータについては「本件被疑事実との関連性を認めがたく、差押えの必要性は認められないというべきである」として、結局は当該 FD についての差押えを違法として取り消した。

学説上は、この決定の理解とも絡んで、争いがある。一方では、本決定が、被疑事実と「差し押えるべき物」との「関連性」を否定したものと理解する立場がある。しかし、差押えの

「そうしたコンピュータシステムの内容を捜査機関が掌握できており、その電磁的記録媒体が当該コンピュータシステムに使用されることが明らかとなっているような場合」に必要とされると考えるべきであろう。安富・前掲注（1）・162。

[83] 小川・前掲注（1）・257 参照。

対象物を有体物たる電磁的記録媒体と考える場合[84]には、その関連性を判断する単位は各電磁的記録媒体であって、本件 FD の中に被疑事実と関連性を有するデータが入っていることが明らかである以上は、当該 FD の被疑事実との関連性を否定するのは困難だといえよう。

他方、本決定は FD そのものが被疑事実との関連性を有するとしても、被処分者の不利益の程度等を勘案して「差押えの必要性」（ないし「相当性」）が否定されるべき場合があることを述べたものであるとの理解も示されている。そのように解すれば、本決定は、必ずしも現行法の差押えに関する規定と矛盾するものではなく、むしろ重要な意義を有する決定ということになる[85]。

（２）電磁的記録媒体の包括的差押え

電磁的記録媒体が差押対象物となる場合には、ある電磁的記録媒体に記録されたデータを何らかの形で出力したうえで、当該記録媒体と被疑事実との関連性や、当該記録媒体の差押えの必要性を判断しなければならない。ただ、そうした操作を捜索現場で行うことが技術的に極めて困難である場合や、長時間を要する場合、さらには証拠破壊の危険を伴う場合であっても、常にこれを敢行すべきであろうか。この点、最二小決平 10・5・1 刑集 52・4・275 は、「令状により差し押さえようとするパソコン、フロッピーディスク等の中に〔①〕被疑事実に関する情報が記録されている蓋然性が認められる場合において、〔②〕そのような情報が実際に記録されているかをその場で確認していたのでは記録された情報を損壊される危険があるときは、内容を確認することなしに右パソコン、フロッピーディスク等を差し押さえることが許されるものと解される」とした（〔①〕及び〔②〕は筆者）。これは、電磁的記録媒体と被疑事実との関連性が当該記録媒体に記録された内容を確認しなければ判断しえないという場合に、電磁的記録媒体の記録内容を確認できない②の事情がある場合には、①にあたる電磁的記録媒体について、その内容を確認せずに包括的に差し押さえることを許容したものであると考えられる[86]。

学説上は、こうした電磁的記録媒体の包括的な差押えを「差押え」そのものと位置づけた

---

84 逆に「差し押さえるべき物」を無体情報そのものとする立場に立てば、各情報を単位として関連性を判断することとなる。

85 以上につき、井上正仁「コンピュータ・ネットワークと犯罪捜査（1）」法教 244・49、61（2001）、大澤裕「コンピュータと捜索・差押え・検証」法教 244・44、45（2001）、長沼・前掲注（2）・46 など参照。

86 池田修「判批」最高裁判所判例解説刑事篇〔平成 10 年度〕・78、87（法曹会、2001）。今後は、①及び②の関係や、②が例示であると解するか、そうであるとすれば、②と比肩しうる事情にはいかなるものがあるか等が問題となることとなる。なお、大阪高判平 3・11・6 判タ 796・264 は、捜索差押現「場に存在するフロッピーディスクの一部に被疑事実に関連する記載が含まれていると疑うに足りる合理的な理由があり、かつ、捜索差押の現場で被疑事実との関連性がないものを選別することが容易でなく、選別に長時間を費やす間に、被押収者側から罪障隠滅をされる虞れがあるようなときには、全部のフロッピーディスクを包括的に差し押さえることもやむをえない措置として許容されると解すべきである」としてい

上で、例外的に許容する立場[87]と、これを法 222 条 1 項、111 条 1 項にいう捜索・差押えに「必要な処分」（が続行しているもの）として許容する説[88]などがある。前者は「関連性」の判断基準がその対象物の特性に伴う一定の事情によって緩和されうることを認めつつ、その「事情」を限定することによって電磁的記録媒体の包括的な差押えが無制限なものとなるのを防止しようとするものであると考えられる。他方、そうした「関連性」の判断基準が対象物のいかんによって緩和されることは望ましくないとして、関連性の有無を識別するために包括的に電磁的記録媒体の占有を一時的に取得する処分は「差押え」そのものではなく、それに「必要な処分」である[89]として、関連性の判断基準そのものを維持しようとしたのが後者であるといえよう。確かに、後者のような考え方も十分成り立ちうるものと考えられるが、それにより実質的には現行法上は規定されていない「差押えのための差押え」を認めることとなることや、立会い・押収目録の交付・不服申立て等の点につき解釈論上の難点を抱えているようにも思われ、被処分者の利益を十分に保障しうるか疑問が残るところである。方向としては、こうした包括的な占有取得処分を端的に「差押え」と解した上で、それが許容される要件（事情）を限定していく方向が妥当であろう[90]。

３．該当性判断のためのデータの出力・印字等の処分及び印字書面の取り扱い

（１）該当性判断のためのデータの出力・印字等の処分の法的性質

ある電磁的記録媒体が「差し押さえるべき物」として令状に記載された物に該当するか否かは、そこに記録された内容を出力・印字するなどして可視化・可読化した上で判断する必要がある。被処分者の協力によりこうした操作がなされ、該当性が判断される場合には特に問題はない。しかし、そうした協力が得られない場合に、捜索現場において、捜査機関が、被処分者のコンピュータを用いて電磁的記録媒体に記録されたデータの出力･印字等を行うことは許されるだろうか。

この点、こうした出力等の処分は捜索差押え令状とは別個の令状に基づき、検証処分として行うべきであるとの見解もある。しかし、こうした処分は法 222 条 1 項、111 条 1 項に言う「必要な処分」として別個の令状によることなく許されるとの考え方が有力である。その理由としては、「憲法 35 条やこれを受けた刑事訴訟法の規定が、捜索押収の執行方法についてまで事前の司法審査を要求しているとは解されないこと」や、「第 3 者の所有する証拠物

た。

87 寺崎嘉博「電磁的記録に対する包括的差押え」廣瀬健二ほか編・田宮追悼（下）・249、257（信山社、2003）。

88 酒巻匡「捜索・押収とそれに伴う処分」刑雑 36・3・444、453（1997）。

89 この立場からすれば、選別を経て「関連性」ありと判断された物についてなされる（占有取得ないし保持）処分が「差押え」ということになろう。

90 寺崎・前掲注（15）・253－257 参照。したがって、本件②を例示と解するか否か、選別に長時間を要する場合や、技術的な困難がある場合にも包括的な差押えが許されるとすべきか否かという問題については慎重な立場をとらざるを得ない。

の差押等も許されること」、捜索差押令状発付「の段階でこうした処分が行われることが予定されているのが通常と思われる」こと、別途検証令状を要求することは、むしろ「捜査を複雑化するのみで特段のメリットもないこと」等が挙げられている[91]。

（2）該当性判断のために作成された印字書面の差押え

では、このようにして作成された印字書面を、捜査機関が当初の（捜索）差押え令状に基づいて差し押さえることは許されるか。令状発付時に存在しない物についての令状発付の適法性、及び当該差押えの適法性が問題となる。司法審査の時点で存在しない物については、審査の対象となっていない（するべきでない）として、当該令状の発付そのものやそれに基づく差押えを違法とする考え方もありえよう。しかし、差押え目的物が捜索場所に存在するかどうかの判断は、常に予測に基づく蓋然性判断であって、そのことは令状発付時に存在している物に対する関係でもいえることである。そして、こうした印字書面が差押え時に存在する可能性があることについて審査の時点で認識されていることも多いと考えられる。したがって、差押時に存在する十分な蓋然性があり、かつ、その特定が可能である場合には、そうした印字書面の差押えを許容する令状を発付することも許されると考えられる。そして、当該印字書面について差押えの必要性（ないし相当性）が認められるのであれば、当該令状に基づいてこれを行うことも許されてよいであろう[92]。

４．電磁的記録媒体そのものの差押えに代わる処分

上記の東京地判の事案におけるように、一定の電磁的記録媒体に記録された内容によって、その記録媒体自体の「差押えの必要性」（ないし相当性）が否定される場合には、捜査機関が当該記録媒体を差し押さえることは許されない。ただ、そこに記録された被疑事実との関連性を有するデータだけを何らかの手段を用いて取得することはできないだろうか。この点、当該 FD そのものではなく、被疑事実に関連するデータのみをプリントアウトし、あるいは当該データを別の FD 等の記録媒体にコピーして、それらの印字書面や電磁的記録媒体を差し押さえることが許されるのではないかが問題となる。このような代替手段によるならば、被処分者に与える不利益を最小限にとどめることができ、さらに、捜索・差押令状において「・・・の情報を印字した文書」、「・・・の情報をコピーした FD 等の記録媒体」を「差し押さえるべき物」として記載しておくことにより、対象物の特定・明示という点もクリアーできるとして、これを許容する立場が有力である[93]。しかし、強制処分法定主義との関係で、

---

91 的場純男「コンピュータ犯罪と捜査」ジュリ増刊 刑事訴訟法の争点〔新版〕94、95（1991）。

92 なお、令状において「差し押さえるべき物」にこうした印字書面が含まれることが明示されていなかった場合については、前記 1（2）iiiの場合と同様に考えることができよう。一方、当初から印字書面を差し押さえる目的で、出力・印字を行う行為の法的性質については、後述 4 参照。

93井上弘通「フロッピーディスクに入力された情報の収集と令状の発付」新関雅夫ほか・増補令状基本問題（下）331、337－338（一粒社、1997）、小川・前掲注（1）・264－266、的場・前掲注（12）・95－96。

こうした処分がいかなる法的根拠に基づくのかを考える必要がある。

まず、捜査機関が用意した用紙や記録媒体を用いて印字書面やコピー等を作成し、それを「差し押さえる」ことは許されるだろうか。当該用紙や記録媒体がそもそも捜査機関の所有物であることからすれば、「差押え」の要件としての「占有取得」があるとは考えにくく、これを「差押え」として許容することは困難であろう。

では、被処分者の所有する用紙等を使用した場合はどうだろうか。前述の該当性判断のための出力・印字が差押えのための「必要な処分」として許容されることに鑑み、本件のような場合も（「捜索」ないし）差押えに「必要な処分」として許容する説もある。しかし、印字書面やコピーを収めた電磁的記録媒体を差し押さえることを目的に、印字・コピーを行うことは、当該用紙ないし記録媒体が「差し押さえるべき物」に該当するかどうかを判断するための確認・選別作業とは性質を異にしており、これを「捜索」と呼ぶことはもとより、当該用紙や記録媒体の差押えに不可分の処分としての「必要な処分」と呼ぶこともできないように思われる。

他方、これを「検証」として検証令状により許容する考え方もある。しかし、こうした処分は、性質上、被疑事実と関連性のあるデータとそうでないデータとを選別する過程を伴うと考えられるが、検証も憲法 35 条の「押収」の一部を構成するものである以上、それを行う「正当な理由」のある対象との関係でしか行うことができない。つまり、被疑事実と（関連性のあるデータとそうでないものとを選別した後に、）関連性のあるデータについてその内容を確認したり、コピーを作成したりするのが「検証」なのであって、その前提たるデータ選別の過程自体は「検証」とはいえない。そうしたデータ選別の過程は、むしろ「検証のための捜索」とでもいうべきものである。このような観点から、検証令状と捜索令状の発付を受けておけば足りるとする説も主張されている[94]が、法 102 条 2 項や 119 条の規定振りからするならば、現行法上の捜索は、専ら差押えの対象物の発見を目的とするものとして規定されていると考えるのが自然であろう。「検証のための捜索」なるものを認めた規定は現行法上は存在しないといえよう。

そこで主張されたのが、「差押えに付随してあるいは代替して、目的物に対し検証に相当する処分を行うことも許される[95]」とする考え方である。これは、捜索差押えに付随する証拠物・執行状況等の写真撮影、ないし捜索差押えの代替としての対象物の内容・形状等の写真撮影が許されるという理解を捜索・差押えの場面にも投影したものである。確かに、差し押さえた物に対する「必要な処分」として、捜索現場外で、差し押さえた電磁的記録媒体の内容を表示したり印字したりすることが許され、選別の後、関連性を有するデータについてのみコピーを作成したうえ記録媒体そのものは還付するということが許されるとすれば、差押えに「付随」する、あるいは「代替」する処分として印字書面ないしコピーを作成し、そ

94 井上・前掲注（14）・339。
95 大澤・前掲注（11）・47。

れを差し押さえることも許されよう。[96]

こうした議論を受け、今般の立法提案においては、「差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者は、その差押えに代え」て、「差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえる」か、「差押えを受ける者に差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえる」ことを認めることを内容とする提案がなされている。

第３　結びにかえて

以上において、わが国の捜索・差押え手続におけるコンピュータデータの取扱いに関するこれまでの代表的な議論を概観し、その到達点を確認した。捜査機関としては、予めできる限り対象となるコンピュータシステム等について調査し、その結果明らかとなった事実を最大限に活用したうえで、令状における「捜索すべき場所」や「差し押さえるべき物」ができる限り厳密に特定・明示されたものとなるよう努力すべきであろう。また、このたび新たに立法提案がなされた各種処分も含め、具体的な処分の実行に際しては、それが適法なものであることを（上記の議論などに照らして）常に確認するようにすることは勿論、かりにそれが適法なものである場合であっても、前記のようなコンピュータデータの特性に応じ、被処分者に与える不利益が最小限のものとなるよう細心の注意を払うべきであろう。

---

[96] 以上につき、大澤・前掲注（13）・46－47。

第４論文　USA PARTRIOT 法にみるコンピュータ犯罪の捜査とプライバシーの保護

石井徹哉

１　はじめに

2001 年９月 11 日のテロを契機として立法された[97]2001 年パトリオット法[98]は、法執行機関に対して監視および捜査のための手段を強化する立法であり、そのため市民的権利、とりわけプライバシーの権利への重大な侵害をともなうとの批判もある。もともとパトリオット法は、テロに対する国家の防御を強化することを意図する膨大な内容の立法である Anti-Terrorism Act of 2001（以下 ATA とする）の妥協的な産物である。ATA は、法執行機関および情報機関が私的なコミュニケーションの監視と個人情報へのアクセスをおこなう権限を著しく拡張する規定を含んでいたものの、時限立法が多くみられた。これに対して、パトリオット法は、とりわけインターネットに関して捜査機関の権限を明らかに拡張する規定を維持するのであり、その点でインターネットを通じて伝送される情報への介入が脅かされる懸念が表明された。さらに、パトリオット法の立法過程をみても、その早急さは目立ち、十分な議論がなされていないとの問題も指摘されている。他方で、パトリオット法は、音声通信を中心として想定された従来の法規ではネットワーク・コミュニケーションにおける捜査権限について不明確であったので、これを明確にしたにすぎないとものとみる立場もある。

ここでは、情報ネットワークにかかる捜査に関するパトリオット法の概要を明らかにし、プライバシーの保護とどのように調和を図ろうとしているのかを説明することにする。

２　パトリオット法の概要

パトリオット法は、当時の連邦法を修正するものであったが、その対象となる法律は広範におよんでいる。

Title III[99]
Electronic Communications Privacy Act（以下 ECPA とする）
Computer Fraud and Abuse Act
Foreign Intelligence Surveillance Act
Family Education Rights and Privacy Act
Pen Register and Trap and Trace Statute
Money Laundering Act

---

[97]テロ攻撃後わずか１週間もたたずに提案され、翌月 26 日には成立した。
[98]愛国者法とされることもあるが、USA PATRIOT（愛国者）という略称になるように法律名をきめたといえる。Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 が正式名称である。
[99]いわゆる Title III は、1968 年の Omnibus Crime Control and Safe Street Act の Title

Immigration and Nationality Act
Money Laundering Control Act
Bank Secrecy Act
Right to Financial Privacy Act
Fair Credit Reporting Act

がそうである。以下では、コンピュータ犯罪の捜査に関するものに限って、パトリオット法の修正内容の概略をみることとする。

(1) 不正アクセスの捜査における音声通信の傍受権限の付与

従前は、18 U.S.C. § 1030 違反（無権限アクセスの罪）については、盗聴ないし傍受をすることができなかった。しかし、パトリオット法によって、有線通信に関する盗聴命令を入手することができる犯罪の一覧に 18 U.S.C. § 1030 を追加したことにより、これが可能となった（ただし 2005 年 12 月 31 日までの時限立法である）。

(2) ボイスメール及びその他の蔵置された音声通信の入手

従来の ECPA では、法執行機関は蔵置された電気通信（たとえば電子メール）へのアクセスは可能であったが、保存された有線通信（たとえばボイスメール）にはアクセスできなかった。ただし、傍受法では、「有線通信」の定義に保存されたボイスメールも含まれていたため、そのようなアクセスが可能であった。パトリオット法は、傍受法と ECPA が適用される方法を入れ替えた。すなわち、2510 条の「有線通信」から有線通信の「電子的な保存」の文言を削除し、保存された電気通信と同様のルールが適用されるように 2703 条にその文言を追加した。

(3) 電子的証拠に関する提出命令(Subpoena)の範囲

改正前は、2703 条(c)が提出命令により入手できる情報を、顧客の氏名、住所、サービスの期間、支払方法といったものに限定しており、顧客の身元を確認することができる記録を含んでいなかった。多くの場合、ユーザは、ISP に対して偽名を使って登録しているのであり、これらの者にオンライン上でおこなわれた犯罪行為の責任を追及するためには、支払いの手段が決定的であるといえる。さらに、2703 条(c)の定義の多くは、技術的に特殊で、電話通信に関係している。たとえば、「長距離および地域内通話の支払請求の記録」があげられているが、これはコンピュータ・ネットワークの通信には対応しない。「電話番号またはその他の加入者番号もしくはその ID」といったものもそうである。

パトリオット法による改正によって、提出命令により入手できる記録の種類が拡張されたのである。2703 条(c)(2)は、「セッション時刻および時間」ならびに「あらゆる一時的に割

III のことをさす。18 U.S.C. § 2510-22 がこれに該当する。

り振られるネットワークアドレス」を含むようになった。インターネットの局面では、IP アドレスがこれに該当する。これらの情報を入手することにより、ネットワーク上の犯罪者の特定とそのインターネットでのやりとりを追跡することがより容易にかつスムーズにすすむことが期待されたのである。また、提出命令を使用することによって、ISP のアカウントの支払に使用しているクレジットカード番号や銀行口座番号を入手できることになり、利用者の個人の特定がよりやりやすくなったのである。

(4)　ケーブル法の射程範囲の明確化

捜索・押収マニュアルにも述べられていたが、パトリオット法によりケーブル法の射程範囲が明確にされた。従来は、ケーブルサービスにかかわるルールと電話ならびにインターネットアクセスの利用にかかるルールに二分され、前者にあっては法執行機関がケーブル会社から情報を入手することがきわめて限定されていたのである。そのため、ケーブル会社が保有している顧客情報は、提出命令や捜索令状をもってしても入手できず、このような情報を捜査機関がえるためには、ケーブル会社があらかじめ顧客に告知をおこない、また、弁護士をつけて裁判所への出頭を求めることが必要で、これらの記録を入手するのに必要な捜査を裁判所により正当化してもらうことが必要であった。しかも、相当な理由という基準ではなく、「明白かつ確信を抱くにたりる証拠」という高度の基準が妥当するため、ネットワーク犯罪には有効ではなかったのである。ケーブル法の制定当初（1984 年）とは異なり、多くのケーブル会社がケーブルテレビだけでなく、インターネットアクセスや電話のサービスを提供している現状では、後者のサービスについては、ケーブル法の適用は種々の捜査上の困難をもたらすのである。

パトリオット法は、ケーブル会社にケーブル法の一律に適用することをあらため、ECPA、通信傍受法が、コミュニケーションサービスに関係する部分についてはケーブル会社にも適用されることを明確にしたのである。

(5)　コミュニケーションプロバイダによる緊急開示

プロバイダによる任意開示に関して、それまでは、二つの問題点が指摘されていた。第一に、緊急状況における顧客記録ないしは通信を開示することを認める特別の規定が存在していなかったということである。そのため、顧客の一人がテロ活動に関与していることを知った場合に、その顧客情報を捜査機関へ開示することは、たとえ多くの生命を救うことになりえたとしても、民事訴訟を受ける可能性もありうる。

第二に、たとえプロバイダが自己保護の目的でコミュニケーションの内容を開示できたとしても、同様の理由で内容ではない記録を捜査機関に任意で開示することは明示的に認められていない。実際的な問題としては、プロバイダは自己のシステムへの攻撃を取り巻く事実を捜査機関へ開示する権利を有していなければならない。

そこで、パトリオット法はこれら二つの問題点を修正したのである。いずれかの人の死も

しくは重大な身体傷害の危険にかかわる緊急状況においては、コミュニケーションの内容であるかそうでないかを問わず顧客の記録を法執行機関へ開示することを認めた。しかしながら、この任意の開示はそのような切迫した危険の捜索において顧客の通信を参照する強制的な義務を創出するものではない。また、ECPA を改正して、プロバイダの権利および財産を保護するために情報を開示することを認めた（2005 年 12 月 31 日までの時限立法）。

(6) 令状執行の際の告知を遅らせることの許容性

パトリオット法以前では、令状を執行したことを事後に告知する法的なルールというものは、相矛盾するような規則、実務ならびに裁判所の判断の寄せ集めしかなく、裁判所の管轄が変わると異なってしまうというような状態であった。このような法的ルールに統一性がない状態では、テロの捜査やテロ以外でも国家的な規模での捜査が阻害されることになる。

パトリオット法は、18 U.S.C. § 3103a を修正することで、統一的な法律上の原則を示したのである。すなわち、裁判所は、令状の執行をする旨すみやかに告知することが、個人の生命もしくは身体の安全を脅かしたり、訴追から免れたり、証拠を隠滅し、証人を威迫するなど、捜査を著しく危険にさらしまたは公判を過度に遅延させるような結果をもたらす（18 U.S.C. § 2705 参照）と信じるにたりる「合理的な理由」があると判断する場合、告知を事後にすることを認められる。令状を執行したことは「合理的な期間」内に告知すればたり、正当な理由があればさらに延長することができることになった。もっともこの規定は本来捜索の告知を事後にすることを認めるにすぎないのであり、裁判所が押収の「合理的な必要性」を認めないかぎり、有体物の押収を当該令状は禁止すべきことを要求するものである。

本条で問題となる「合理的な理由」は令状の告知を遅らせることに関する有力な判例 (United States v. Villegas, 899 F. 2d 1324, 1337 (2d Cir. 1990)) と一致している。また、捜査官が自ら立ち入る前に告知し、日中に執行しなければならないとの一般原則に対する例外を認める基準とも一致している。「合理的な期間」内に告知するとの要件も、事案の状況に応じて柔軟に判断されるべきものとされる。この点に関する判例はまだ形成段階ともいえ、今後の推移をみまもる必要があるかもしれない[100]。押収のための「合理的な必要性」は判例においてもそれほど展開されていない。

(7) 電子メールの捜索令状

旧 18 U.S.C. § 2703(a)は、180 日未満の未開封の電子メールを開示することをプロバイダに強制させるために、捜索令状を使用することを要求している。しかしながら、連邦刑事訴訟規則 41 条が、入手されるべき「財産」が令状を発行した裁判所の「地域内に」存在しなければならないことを要求していることから、他の地域に位置している電子メールに関する 2703 条(a)令状を発行することを拒否してきた裁判所もある。このような状況は、実務上

[100] See United States v. Allie, 978 F. 2d 1401 (5th Cir. 1992); United States v. Pangburm 983 F. 2d 449 (2d Cir. 1993), etc.

は、大手 ISP の所在する地域に大きな運用上の負担をかけることになる。捜査中の犯罪行為となんの関係もない場合でも、令状請求しなければならず、また、時間との勝負でもあるネットワーク犯罪にとって時間のロスにもなったといえる。

パトリオット法は、本条を改正し、連邦大陪審の提出命令および 2703 条(d)命令と同様に、裁判所の管轄区域外であっても 2703 条(a)令状を使用することを認めたのである（2005 年 12 月 31 日までの時限立法）。

以上がパトリオット法におけるコンピュータ犯罪にかかわる捜査に関して修正された部分の概要である。もっとも、通信傍受法に関係する点は省略した。パトリオット法は、Title III にかかる通信傍受法については、これがコンピュータ通信についても、電話と同様に適用されることを法定し、その要件を明確化したということのみ付言しておく。

3　プライバシーの権利とパトリオット法

パトリオット法に関しては、その制定当初より、個人のプライバシーを侵害するものであるとの批判も根強く存在している。ここでは、代表的な批判を取り上げて、それを検討することとする。

(1)　パトリオット法全般に関する批判

パトリオット法に対する一般的な批判は、それがテロの概念を拡張し、政治的組織を監視し、圧力をかける方向に向かうのではないかというものである。また、政府の政策とは異なる平和的団体の行動をテロであるとして取り扱うことを許容するようになるという批判もある(American Civil Liberty Union(ACLU), February 11, 2003)。

しかしながら、パトリオット法は、刑罰法規に違反し、人の生命を危険にさらす行為だけをテロとして扱うものであり、違法行為に関与しない以上、平和的な活動をおこなう政治的団体は対象にならないと反論できよう。パトリオット法はその 802 条において、国内テロ活動(domestic terrorism)の定義をおこない、連邦もしくは州の刑法の違反と人間の生命に対する危険をその要件としている。

つぎの批判は、多くの市民は、各自の図書館での行動までもが政府の監視対象になるということを知らず、このような監視は自由な社会においては不必要なものであり、なにを読み、どのウエッブサイトを見たのかなどをいわゆる「思想警察」が活動できるような社会をもたらしかねないというものである(ACLU, July 22, 2003)。

これに対しては、パトリオット法はアメリカ市民の第一修正の権利を保護するものであって、普通のアメリカ市民が図書館でどのようにしていたのかなど関心がないということになろう。少なくとも、歴史的な経験則によれば、テロリストは図書館を基軸に情報交換、情報の入手を図っていたということがここでは重要になる。

第三に、パトリオット法が捜索令状についてその告知を事後にできると規定している点に

ついて、捜索方法の抜本的な変更であるとの批判もある。しかしながら、アメリカにおいては、捜索の告知を事後にすることは、組織犯罪、薬物事犯および児童ポルノの領域において、以前から広く裁判所により支持されてきた犯罪対策の手法である。その意味では、パトリオット法は長年の実務上の慣行を法律に規定したにすぎないともいえる。連邦最高裁の判例(Dalia v. United States 441 U.S. 238 (1979))によれば、第四修正は法執行機関に捜索令状を執行する際にすみやかな告知をおこなうことを要求していないのであり、少なくとも捜索令状にしたがって行動しているかぎり、一定の状況において、潜入捜査官は合憲であるとされている。

(2) テロに関係する通信の傍受の権限について

法執行機関は、テロリストが関与しがちである一定の犯罪を捜査するために現行の電子的な監視権限を使用することが認められている。これに対して、政府はすでにテロリストの容疑のある者に対して傍受する実質的権限を FISA のもとで有しているのであるから、パトリオット法による変更の実質的な効果は国内のテロの容疑のあるアメリカ市民の傍受を許容することにあると批判される(Electronic Privacy Information Center (EPIC), Mar. 19, 2003)。

ただ、実際問題として、パトリオット法以前において、法執行機関が電子的な監視をする権限を有していたのは、普通の、テロではない犯罪を捜査する場合であった。パトリオット法は、化学兵器犯罪、大量破壊兵器の使用、海外におけるアメリカ市民の殺害およびテロへの財政的支援をふくむテロに関係するすべての犯罪を調査する場合に、捜査官が情報を収集することを可能にするものである。また、従来の傍受法における要件はそのまま維持されていることにも注意すべきである。

(3) 犯罪捜査情報の共有

パトリオット法では、連邦法執行機関、情報部、移民局、国防および国家安全局のメンバーと大陪審ならびに傍受の情報を共有することが認められている。この点について、情報の共有は、一定の限定的な状況においては妥当であるとしても、厳格な保護条項をもってなされるべきであり、パトリオット法にはそれが欠けているため、濫用の可能性があるとの批判がある(ACLU Oct. 23, 2001)。

(4) 令状によるボイスメールの押収

パトリオット法により、法執行機関は、傍受令状ではなく、捜索令状により ISP など第三者に蔵置されているボイスメールを入手することができる。要件の厳格な傍受令状ではないこと、ボイスメールも通信内容であることから、この点についても批判がある。

従来、テロリストの自宅にある留守番電話に録音されている音声については、捜索令状によりこれを入手することができたが、第三者のプロバイダに保存されている場合には、傍受

命令を入手するという面倒な手続きをへる必要があった。パトリオット法は、相当な理由を示すことで、裁判所の発行する捜索令状によりそのようなボイスメールを入手することを認めたのである。要は、録音された音声の所在が異なるだけで、実際の機能が同様であることから、自宅の留守番電話と同様の扱いにしたといえよう。

(5)　電気通信の記録に対する提出命令の射程範囲

パトリオット法は、大陪審が電気通信プロバイダから提出命令により入手できる記録の種類を、銀行口座やクレジットカード番号などの支払の手段を含むように拡張している。

パトリオット法による改正前には、連邦法が大陪審に認めていたのは、電気通信プロバイダの情報のうちある種のものだけについてしか、提出命令を出すことができず、それでは被疑者が本当は誰であるのかを特定することは困難であった。しかしながら、改正により、口座番号やカード番号をも入手することが可能になり、これらの情報によって本人の特定がきわめて容易になったのである。

このような個人情報へのアクセスを捜査機関に認めることについて、過度のプライバシーの侵害であるとの批判がある。しかしながら、ここで問題となる提出命令も、他の提出命令と同様、その名宛人は判事にその破棄を求めることができるのであり、名宛人が提出命令にしたがうことを拒否した場合、政府は裁判所にその強制を求めることができるものの、捜査官が一方的にそれを強制することはできない。このかぎりで、裁判所の審査があるといえる。もっとも、個人情報でもかなり個人的な領域に属するものであるだけに、提出命令で済ますことが妥当であるかというはなお検討すべき課題といえる。対象となる犯罪などに照らして捜査の重要性とプライバシーとの慎重な利益考量が要請される。

(6)　生命等を保護するための電気通信の緊急開示

パトリオット法では、生命の危険という緊急状況の場合には通信を開示することがプロバイダに認められた。従来は、緊急状況にあっても顧客の情報を通信プロバイダが任意で開示することはできなかった。たとえ、テロ活動の情報を察知しても、民事訴訟で追求される可能性がありえたのである。政府は、プロバイダが通信の内容を察知し、重大な生命の危険がある場合にこれを捜査機関等に任意で開示したとしても、それは、たまたまとおりですれ違ったグループがテロの計画について話しをしていて、これを警察に通報するのと同様であるとする。

しかしながら、通信の内容をプロバイダ自身が開示することは、通信の秘密の侵害に対する重大な疑義が残るといわざるをえない。これは、ある意味で、通信プロバイダを捜査機関の一部として組み込むことにもつながりうる。ここでは、テロとの戦いとの名のもとに、プライバシーの著しい譲歩が容認されているといえる。もっとも、誰もがみることのできる掲示板等の内容については、これを偶然知りえたサーバ管理会社が通報したとしても、問題はないことに注意すべきである。それは第三者がこれをみることを前提になされているからで

ある。

(7)　令状執行の事後の告知

パトリオット法により、捜索令状を執行したことを事後的に告知することが認められるようになった。この点について、所有者への告知なしに私的財産を捜索する政府の権限を拡張するものであるとの批判がなされる(ACLU, Apr. 3, 2003)。

すでに述べたように、告知を事後にすることは長年の実務の慣例であり、組織犯罪、薬物事犯および児童ポルノ事犯で有効に機能してきたものである。この点では、実務慣行を法令化するものであって、むしろ望ましい方向であるともいえる。法律に明文化することによって、裁判所の管轄ごとに異なっていた基準や態様の相違が統一され、運用面での統一性がはかれることにもなる。なお、告知を事後的にすること自体は連邦の判例上問題がないものとされている。前述の Dalia 事件において、連邦最高裁は、捜索令状の執行をすみやかに告知することはかならずしも第四修正の要求するところではないと判示している。また、Katz v. U.S. 347 (1967)においては、捜索の目的をあらかじめ告知することが被疑者の逃亡や重要な証拠の毀損をもたらす場合には、その他の点では正当な権限のある捜索をおこなう前にそのような告知をする必要はないと述べている。

なお、2003 年７月に上院を通過したオッター法は、重大犯罪対策とともに、テロを阻止・防止するための取り組みに圧倒的な効果を持つものといえる。捜査機関が、テロリストや犯罪組織の所在を確認し、その計画を特定し、あるいは、その逮捕へと導くために必要な情報を入手する前に、テロリストや犯罪者を密告することを可能にするものである。

いずれにせよ、捜索令状を事前に告知することは、証人の威迫、証拠の隠滅、逃亡、身体傷害および死という結果をもたらしうるのであり、その点において一定の条件下で告知を事後にすることは一定の合理性をもつものといえる。ただし、財産を捜索ないし押収したことを告知することはいずれの場合にも必要であって、ここではその告知を合理的な期間遅らせることができるにすぎないことは注意が必要であり、告知なしの捜索を容認しているわけではない。また、きわめて限定的な条件の下で裁判所の命令に基づいてのみ可能となるのであり、すみやかな告知がとくに重大な結果をもたらすものと信じるにたりる「合理的な理由」がある場合にのみ可能である。この「合理的な理由」はパトリオット法以前の判例(United States v. Villegas, 899 F. 2d 1324, 1337 (2d Cir. 1990)　によることはすでに述べたとおりである。

(8)　FISA のもとでの通信傍受の権限

入手できる情報が国際テロもしくは外国の秘密情報活動を防ぐための捜査にとって重要となるということを疎明することによって通信傍受命令を入手することが可能になった。この点について、このパトリオット法の修正は、外国の情報監視に適用される比較的緩やかな要件のために、憲法上の理論的根拠が骨抜きにされることになるとの批判がある(EPIC, Mar. 19, 2003)。

これに対しては、通信傍受のためには、パトリオット法においても、現行の裁判所命令の要件にしたがう必要があるので、そのような批判は当たらないともいえる。連邦最高裁(Smith v. Maryland, 442 U.S. 735, 744 (1979))も、逆探知装置を設置する前に裁判所の同意をえることは憲法上要求されていないと判示しているので、その意味では批判は妥当でないところもある。もっとも、傍受の対象を拡大する点については、問題は残ることになろう。さらに、パトリオット法による改正は、第一修正の権利を保護するためになされているという建前上、第四修正の権利との利益考量による厳密な線引きが必要である。

(9)　コンピュータの侵入者の通信の傍受

パトリオット法により、ハッキングの被害者に、そのコンピュータへの侵入をモニタする際に法執行機関の支援を要請することが認められた。

これに対して、捜査機関とシステム管理者の手だけに判断がゆだねられている点に問題があり、他方で、テロの捜査にとってあまり意義はないとの批判がなされている(EPIC, Mar. 2003)。比喩的に言えば、自分の土地へ不法に侵入する者を追い払うのを手伝ってくれるように、土地の所有者は法執行機関に要請できるといえ、サイバー犯罪においても同様の対処を認めることは、それほど問題が多いとはいえないかもしれない。ただ、ネットワーク上の有害行為に対処するためには、システム管理者の手に負えない場合、より高度の技術的支援をえる方策をとる必要があろう。アメリカにおいては、政府機関に優秀な技術者が多様な捜査手法を習得しているのであり、技術的支援は犯罪対策として有効な方策であるといえる。とくに大規模な DoS(Denial of Service)に対処するには、政府機関の協力がより望ましいであろう。

3　パトリオット法のその後

9・11 テロを契機として成立したパトリオット法は、そのテロ対策としての強硬な側面もあり、市民的自由に譲歩を求めるものであるとの批判は大きいものがある。たしかに具体的なテロ対策の部分においてはそのような側面があるのかもしれない。しかしながら、ネットワーク上の犯罪捜査という側面からパトリオット法をみる場合、かならずしも市民的自由、とりわけプライバシーの権利を大きく侵害するものであるとはいえない。なかんずく、パトリオット法によって、従来は不明確であったネットワーク上の捜査の手法が法定され、その要件が明確にされたものが多いことは重要である。また、通信関係の捜査手法が、それまでは有線通信あるいは音声通信を前提に規定されており、ネットワーク環境における捜査手法については、それをどのように応用すべきか明らかでなかったものを、明確にしたという点もある。さらに、これらの点について、パトリオット法により規定されている要件も、プライバシーとの関係からみても、それほど不当なものとはいえない。

とはいえ、アメリカにおける捜査は、日本におけるのと異なる制度に依拠している部分も多いことには注意しなければならない。とりわけ、提出命令はその機能的な面においても、

有効に活用されているといえる[101]。提出命令は、捜査機関の一方的な強制処分ではなく、判事の審査を経るという点で、濫用の可能性を低減させているし、捜索・押収令状ほど強固な強制処分でもないため、利用しやすい面も多い。また、18 U.S.C. § 2703(d)に規定されるような裁判所命令も同様に重要である。

いずれにしても、任意処分か令状による強制処分かの二者択一のわが国と大きく異なることに注意しなければならない。アメリカでは、提出命令あるいは 2703 条(d)裁判所命令により、いわば通信の外形といわれる情報をプロバイダより入手することが可能となる。しかし、わが国では、顧客情報等を入手するには、捜査照会による回答か、令状による捜索・押収が必要となる。前者によりプロバイダが顧客情報を回答した場合、プロバイダ自身が当該顧客から民事責任を追求される可能性は否定できず、それをおそれて回答を得られない可能性が残る。他方で、後者の場合には、犯罪と無関係のプロバイダの捜索はその負担が大きいものといえる(もちろん電子メールやファックスによる回答で令状の執行が完了するなどの制度があれば別である)。したがって、今後わが国においても、まさに高度情報化社会に適合した通信関係の捜査手法を検討し、法制化することが必要であろう。そのことが、逆に、有効なネットワーク犯罪の対策にもなるのである。_

[101]人に対するものであっても、わが国では捜査段階で召喚状を使用することはない。

第５論文　ハイテク犯罪対策のための刑事法改正

安富潔

１　はじめに

ＩＴ（情報通信）社会にあってコンピュータ・ネットワークは重要な社会的基盤の一つとなっている。しかし、昨今、残念ながらそうしたコンピュータ・ネットワークを悪用した犯罪が急増している。そこで、安全な社会を築くために、コンピュータ・ネットワークを悪用した犯罪に適切に対処することが求められる。また、コンピュータ・ネットワークは世界的規模で構成されるものであり、コンピュータ・ネットワークを悪用した犯罪もまた国境を越えて行われる。こうしたことからコンピュータ・ネットワークを悪用した犯罪に対しては国際的に協調した対策が求められるところ、欧州評議会により「サイバー犯罪に関する条約」が起草され，平成１３年１１月２３日、わが国もこれに署名し、条約締結にむけての法整備が必要となった。

このような観点から刑事法整備を行う必要があるとして、平成１５年３月２４日に開催された第１４０回法制審議会において、刑事法（ハイテク犯罪関係）部会（以下、「部会」という。）に「ハイテク犯罪に対処するための刑事法の整備に関する諮問」（第６３号）がなされたのである。部会では８回にわたる検討を重ね、平成１５年８月７日、当初の諮問を一部修正して、法制審議会総会への報告をまとめ、これを受けて、平成１５年９月１０日、法制審議会総会で法務大臣に答申がなされた（「ハイテク犯罪に対処するための刑事法の整備に関する諮問」要綱（骨子）（以下、「要綱」（骨子）という。）参照）。

その概要は、実体法では、①いわゆるコンピュータウイルス作成等の罪の新設、②わいせつ物頒布等の罪の改正、手続法では、③電磁的記録に係る記録媒体の差押えの執行方法、④記録命令付き差押え、⑤電子計算機に電気通信回線で接続している記録媒体からの複写、⑥電磁的記録に係る記録媒体の差押状の執行を受ける者等への協力要請、⑦保全要請等、⑧不正に作られた電磁的記録等の没収というものである。

本稿では、手続法に関するいくつかの問題点を検討したい。

２　電磁的記録に係る記録媒体の差押えの執行方法

ハイテク犯罪捜査においては、証拠となる電磁的記録について、これを差し押さえる方法として、電磁的記録が記録された電磁的記録媒体を対象とするのが一般的であるが、可視性・可読性を伴わない電磁的記録の特徴を考えると、差押えの執行にあたって対象となる電磁的記録を特定することは容易でなく、証拠以外の電磁的記録を含む包括的な差押えが行われないとも限らない。これでは憲法３５条が一般的・探索的な捜索・差押を禁止する趣旨に悖ることになる。また、包括的な差押えは、被処分者に不必要な権利・利益の侵害をもたらすことになる。そこで、このような利益調整を図るために、「要綱」（骨子）は、電磁的記録の差押えについて、電磁的記録媒体に記録された電磁的記録を他の記録媒体に複写、印刷、移転してこれを差し押さえることとしている。

要綱（骨子）によれば、

「第三　電磁的記録に係る記録媒体の差押えの執行方法

一　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状の執行をする者又は差押許可状により差押えをする捜査機関は、その差押えに代えて次の処分をすることができるものとすること。公判廷で差押えをする場合も、同様とすること。

１　差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し、印刷し、又は移転した上、当該他の記録媒体を差し押さえること。

２　差押状の執行を受ける者又は差押許可状による差押えを受ける者に当該記録媒体に記録された電磁的記録を他の記録媒体に複写させ、印刷させ、又は移転させた上、当該他の記録媒体を差し押さえること。

二　押収物が一の規定により電磁的記録を移転し、又は移転させた上差し押さえた他の記録媒体で留置の必要がないものである場合において、差押状の執行を受けた者又は差押許可状による差押えを受けた者と当該他の記録媒体の所有者、所持者又は保管者が異なるときは、還付に代えて差押状の執行を受けた者等に当該他の記録媒体を交付し、又は差押状の執行を受けた者等に当該電磁的記録を複写させた上、当該他の記録媒体の所有者等に当該他の記録媒体を還付しなければならないものとすること。」

とする。

法務省の説明によれば、「現行法上, 電磁的記録に係る証拠の収集方法といたしましては, 電磁的記録に係る記録媒体を差し押さえることが考えられますが, 例えば, 記録媒体が大型のサーバであるような場合に, これを差し押さえることによりまして, 被差押者の業務に著しい支障を生じさせるなどする一方で, 差押えをする者にとってもそのサーバ自体を差し押さえるまでの必要がなく, 記録媒体をそのまま差し押さえないで捜査の目的を達成できると判断できるような場合には, そういったことを可能にすることが相当であると考えられます。（中略）そこで, 差し押さえるべき物が電磁的記録に係る記録媒体であるときは, 差押状の執行をする者又は差押許可状により差押えをする捜査機関は, その差押えに代えて, 差し押さえるべき記録媒体に記録された電磁的記録を他の記録媒体に複写し, 印刷し, 又は移転した上, 当該他の記録媒体を差し押さえることができるようにするなどの法整備を行うこととしております。」（部会第１回議事録参照）という。

この要綱（骨子）第三の一項について、日本弁護士連合会「ハイテク犯罪に対処するための刑事法の整備に関する意見」（以下、「日弁連意見」では、「他の記録媒体に複写等して差し押さえることができる場合には電磁的記録に係る記録媒体の差し押さえができないこと（補充性）、被疑事件と関連性がある範囲でしかできないことを要件とすること及びこのような差押えを認める場合に, 元の電磁的記録と複写等された電磁的記録の同一性を担保する措置を定めるように修正されるべきである。」との意見が提案されている（日弁連意見２０頁）。

この電磁的記録媒体に記録された電磁的記録を他の記録媒体に複写してこれを差し押さ

えるという方法は、従来から、捜査の実務においては、被処分者において、他の記録媒体に差し押さえられるべき電磁的記録を複写して任意提出しており、それを法律で明文化しようとするものである。

しかし、上記の要綱（骨子）のような方法による場合、対象となるべき電磁的記録以外の記録も捜査機関等に移転されることにより、被処分者の業務に対して重大な影響を与えるおそれがある。特に、それが第三者であるプロバイダー等の事業者である場合に与える影響は極めて重大である。したがって、差し押さえるべき物が電磁的記録に係る記録媒体である場合については、原則として、要綱（骨子）が規定する電磁的記録を他の記録媒体に複写等した上で当該他の記録媒体を差し押さえるという方法によって行うべきであり、そのような方法では差押えの目的を達することができないという特別な事情がある場合に限って、電磁的記録に係る記録媒体それ自体を差し押さえることができるとすべきである（日弁連意見２０頁参照）。

なお、差押えについては、被疑事件との関連性がある物についてしか認められない（憲法３５条１項、刑訴法２１８条１項）が、電磁的記録に係る記録媒体には差押えの対象とは無関係の情報も多く含まれているのが通常であり、憲法３５条の一般令状の禁止という趣旨に照らして被疑事実との関連性がある電磁的記録しか差押えが認められるべきではない（安冨潔『ハイテク犯罪と刑事手続』１６８頁）。しかしながら、差押えの現場において、被疑事件との関連性がある電磁的記録かどうかを選別することが困難な場合も予想される。そこで、電磁的記録に係る記録媒体を複写等した別の記録媒体を裁判官の保管とし、差押え後に裁判官がその記録媒体に含まれる電磁的記録の中から被疑事件との関連性の有無を審査して選別し裁判官において関連性があると認めた電磁的記録だけを別の記録媒体に複写等して捜査機関に交付するようにし、交付前に裁判官の選別結果を被処分者に示して事前の不服申立を認める制度（稲垣隆一『情報ネットワークの法律実務』〔多賀谷一照・松本恒雄編〕５０３１頁）が提案されている。

ところで、電磁的記録に係る記録媒体に代えて、他の記録媒体に複写等した上で当該他の記録媒体を差し押さえる場合には、元の記録媒体に保存されていた電磁的記録と差し押さえた記録媒体に保存されている電磁的記録とが同一であることが担保されなければならない。したがって、要綱（骨子）のような方法で、複写等した上で代替する別の記録媒体を差し押さえることを認める以上は、電磁的記録の同一性を担保する何らかの措置が認められなければ証拠収集手段としては不完全といわなければならないとの指摘がある（日弁連意見２２頁。指宿信「変わる捜査の対象：モノからデータへ－サイバー刑事法制の諮問を契機として」法律時報７５巻７号３頁）。そこで、日弁連意見では、「差押え後に改ざんがないことを保証する手続や電子データ利用に伴うデータ破壊を防止する手続が行われなければならないが、具体的には、酒気帯び運転の検知管や覚せい剤事件で採取された尿については処分を受けた時点で被処分者の署名をしたテープ等で検知管やカップの封印を行い、同一性を確保する手段が講じられているが、複写等された記録媒体についても同様の措置が講じられるべきである

し、差し押さえた記録媒体は必ずバックアップをとるべきであり（編集代表多賀谷一照・松本恒雄『情報ネットワークの法律実務』５０１５頁〔稲垣隆一執筆部分〕）、この種の手続を立法すべきである」と、証拠の同一性担保に関する規定を整備すべきことが提案されている。

３　記録命令付差押え

要綱（骨子）第四は、「記録命令付差押え」を提案する。

すなわち、

「第四　記録命令付き差押え

一　裁判所は、記録命令付き差押え（電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえることをいう。）をすることができるものとすること。公判廷外において記録命令付き差押えを行う場合は、令状を発してこれをしなければならないものとすること。

二　捜査機関は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、記録命令付き差押えをすることができるものとすること。

三　一及び二の令状には、電磁的記録を記録させ、又は印刷させるべき者及び記録させ、又は印刷させるべき電磁的記録を記載しなければならないものとすること。

四　その他、記録命令付き差押えに関する所要の法整備を行うこと。」

という内容である。

法務省の説明によれば、この制度は、「これは，電磁的記録を保管する者等に命じて，必要な電磁的記録を記録媒体に記録等させた上で，当該記録媒体を差し押さえる記録命令差押えという制度を設けるものであります。

現行法上，電磁的記録に係る証拠の収集方法といたしましては，既に申し上げましたとおり、電磁的記録に係る記録媒体を差し押さえることが一般に考えられますが，今日，コンピュータ・ネットワークが高度に発展し，遠隔の電子計算機の記録媒体に電磁的記録を保管し，あるいは必要の都度，これをダウンロードするなどして利用することがかなり一般化していることから，従来の記録媒体を差し押さえるという方法だけでは，例えば電磁的記録が記録されている記録媒体を特定することが困難である場合，電磁的記録が複数の記録媒体に分散して保管されている場合等におきまして，捜査の目的を十分に達成できないおそれがあり，このような傾向は，今後ますます強まると考えられます。

他方，通信プロバイダ等の電磁的記録を保管している者等につきましては，裁判官の令状があれば，必要な電磁的記録を他のディスク等の記録媒体に記録した上，当該記録媒体を提出することを協力する場合も多いと考えられますところ，そのような場合であって，電磁的記録が記録されている記録媒体自体を特定して差し押さえなくても，必要な電磁的記録を取得すれば証拠収集の目的を達することができるような場合には，そのような方法をとることが合理的であると考えられます。

また，現代のコンピュータ・システムは極めて複雑でありまして，その操作には種々の専門的な知識等が必要でありますため，電磁的記録を記録媒体に記録する操作も，捜査機関が行うよりも，コンピュータ・システムの管理者等に行わせる方が効率的であり，また，コンピュータ・システムの保護にも資すると考えられます。（中略）

捜査機関が記録命令差押えをする場合におきましては，裁判官の発する令状が必要となりますが，当該令状には，「電磁的記録を記録させ，又は印刷させるべき者」，それから，「記録させ，又は印刷させるべき電磁的記録」等を記載することとなります。」という。

この記録命令付き差押えについては、要綱（骨子）第四の一項及び三項について、要綱（骨子）第三の一項と同様に、「他の記録媒体に複写等して差し押さえることができる場合には電磁的記録に係る記録媒体の差し押さえができないこと（補充性）、被疑事件と関連性がある範囲でしかできないことを要件とすること及びこのような差押えを認める場合に，元の電磁的記録と複写等された電磁的記録の同一性を担保する措置を定めるように修正されるべきである。」との日弁連意見がある（日弁連意見２３頁）。

わが国では、これまで強制処分に関して、被処分者等に一定の受忍義務を課すにとどまり、強制処分の目的を達成するための積極的な作為義務を課してはいないが、記録命令付き差押え制度は、電磁的記録を保管する者その他電磁的記録を利用する権限を有する者に命じて必要な電磁的記録を記録媒体に記録させ、又は印刷させた上、当該記録媒体を差し押さえるものであり、被処分者等に一定の作為義務を認めるという新しい制度である。

４　電子計算機に電気通信回線で接続している記録媒体からの複写

差し押さえるべき対象がコンピュータである場合に、そのコンピュータと電気通信回線で接続されている別のコンピュータ等の電磁的記録媒体にリモート・アクセスできれば、その電磁的記録を複写して、これを差し押さえることができるとするものである。すなわち、現行法においては、リモート・アクセスによって、電磁的記録を別のコンピュータ等の電磁的記録媒体に記録している場合に、その別のコンピュータに対する差押許可状を別個に取得しなければ、別のコンピュータに記録された電磁的記録を差し押さえることはできない。しかし、要綱（骨子）第五では、当初のコンピュータに対する差押許可状だけで、そのコンピュータに電気通信回線で接続されている電磁的記録媒体を複写して差押えができることとなる。

要綱（骨子）第五は、

「第五　　電子計算機に電気通信回線で接続している記録媒体からの複写

一　　裁判所は、差し押さえるべき物が電子計算機であるときは、当該電子計算機に電気通信回線で接続している記録媒体であって、当該電子計算機で処理すべき電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから、その電磁的記録を当該電子計算機又は他の記録媒体に複写した上、当該電子計算機又は他の記録媒体を差し押さえることができるものとすること。

二　一の規定は、捜査機関が刑事訴訟法第二百十八条の規定によってする差押えについてこれを準用するものとすること。

三　一の差押状及び二の差押許可状には、差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって、その電磁的記録を複写すべきものの範囲を記載しなければならないものとすること。」

とする。

法務省の説明では、

「これは，電子計算機の差押えに際しまして，これに電気通信回線で接続している記録媒体からの複写を可能とする制度を設けるものであり，電子計算機を対象とする差押えの範囲を実質的に電子計算機と一体的に利用されている記録媒体にまで拡大しようとするものであります。

今日，コンピュータ・ネットワークが高度に発展し，遠隔の電子計算機の記録媒体に電磁的記録を保管し，あるいは必要の都度これをダウンロードするなどといった利用がかなり一般化しておりますことから，従来の記録媒体を差し押さえるという方法だけでは捜査の目的を十分に達成できないおそれがあることにつきましては，既に申し上げたところであります。

（中略）

そこで，差し押さえるべき物が電子計算機であるときは，当該電子計算機に電気通信回線で接続している記録媒体であって，当該電子計算機で処理すべき電磁的記録を保管するために使用されていると認めるに足りる状況にあるものから，当該電子計算機を操作して，必要な電磁的記録を当該電子計算機あるいは他の記録媒体に複写した上，当該電子計算機又は記録媒体を差し押さえることができることとするものであります。

『電子計算機に電気通信回線で接続をしている記録媒体であって，当該電子計算機で処理すべき電磁的記録を保管するために使用されていると認めるに足りる状況にあるもの』の例といたしましては，電子計算機で処理すべき文書ファイルを保管するために使用されているリモートストレージサービスの記録媒体等が想定されます。

また，『電子計算機で処理すべき電磁的記録を保管するために使用されていると認められる状況にある』というのは，差し押さえるべき電子計算機の使用状況等から，当該記録媒体が，当該電子計算機で処理すべき電磁的記録を保管するために使用されている蓋然性が認められるということでありまして，具体的には，例えば，差し押さえるべきパソコンにリモートストレージサービスのアカウントの設定がなされている場合などがこれに当たると考えております。

また，要綱（骨子）第五の処分を行う場合におきましては，令状主義の要請を満たすために，差押状又は差押許可状に，差し押さえるべき電子計算機に電気通信回線で接続している記録媒体であって，その電磁的記録を複写すべきものの範囲を記載しなければならないこととしております。」

という。

この要綱（骨子）第五については、日弁連意見は新設に反対する（日弁連意見２５頁）。

その理由とするところは、理論的な面において、憲法３５条１項が「侵入，捜索及び押収を受けることのない権利」は「正当な理由に基いて発せられ，且つ捜索する場所及び，押収する物を明示する令状がなければ，侵されない」と規定して、捜索する場所を特定し、令状に明示することを求めていることをあげる。

たしかに、憲法３５条が捜索差押令状において場所・物を特定し明示することを要求する趣旨は、強制処分の対象ないし範囲を事前に確定した上でそれを被処分者に対して明示し、それ以外に強制処分が及ばないことを手続的に保障する点にあるから、令状における場所・物の表示は、捜索・押収に当たる捜査官にとってのみならず、被処分者にとっても捜索・押収の現場において、その表示自体で、対象ないし範囲を容易かつ一義的に識別することが可能な程度に個別的・具体的で自己完結的なものでなければならず、捜査官による裁量的な事後的補完を必要とする不十分さ、曖昧さ、多義性を持つものであってはならない（小田中聰樹「盗聴立法の違憲性」『盗聴立法批判』７４頁以下参照）。したがって、リモート・アクセスによって接続された別のコンピュータの場所を特定することなく、そのコンピュータに記録された電磁的記録を複写して差し押さえることができるとすることは、憲法３５条に違反し許されないと解する立場も理解できる。もっとも、ここで想定されているのは、インターネットのような通信システムを通じてコンピュータと接続された電磁的記録媒体に記録されている電磁的記録（サイバー犯罪条約１９条参照）であり、一定の限定は付されている。しかし、法務省の説明によると、この場合の具体例として、①携帯電話宛の留守番電話又は電子メールが記録されている記録媒体の記録領域、②メールサーバのメールボックスの記憶領域で、パーソナルコンピュータにインストールされているメーラーにアカウントが記録されているもの、③リモート・ストレージ・サービスのサーバの記憶媒体の記憶領域であって、上記パーソナル・コンピュータにインストールされているそのサーバにアクセスするためのアプリケーションソフトにＩＤが記録されているもの、④上記パーソナル・コンピュータとＬＡＮで接続しているグループウェアサーバ（ファイルサーバ及びメールサーバ）の記録媒体の記憶領域であって、被疑者のＩＤによってアクセスできるものとされるが、要綱（骨子）の「保管するために使用されていると認めるに足りる状況にある」との要件では、単にアクセス権限があって、保管するために使用することができる状況があるだけでも差押えが認められることになってしまう。しかし、「それを認めると，アドミニストレーターとしての権限（管理権限ないしルート権限）がある者については、ＬＡＮで接続される全国各地に設置された全てのコンピュータに蔵置された全ての電子データが差押え対象になることを許容することになり，およそ憲法３５条が許容しない極めて広範で無制約な差押えを認めることになってしまう。」との懸念も生じる（日弁連意見２７頁）。

５　電磁的記録に係る記録媒体の差押状の執行を受ける者等への協力要請

要綱（骨子）第六は、電磁的記録に係る記録媒体の差押状の執行を受ける者等への協力要請を提案する。

すなわち「第六　　電磁的記録に係る記録媒体の差押状の執行を受ける者等への協力要請

一　　差し押さえるべき物が電磁的記録に係る記録媒体であるときは、差押状若しくは捜索状の執行をする者又は差押許可状若しくは捜索許可状により差押え若しくは捜索をする捜査機関は、差押状若しくは捜索状の執行を受ける者又は差押許可状若しくは捜索許可状による差押え若しくは捜索を受ける者に対して、電子計算機の操作その他の必要な協力を求めることができるものとすること。公判廷で差押えをする場合も同様とすること。

二　　検証すべき物が電磁的記録に係る記録媒体であるときは、裁判所又は裁判官の発する令状により検証をする捜査機関は、一と同様の協力を求めることができるものとすること。」

というものである。

法務省の説明では、

「これは，差し押さえるべき物又は検証すべき物が電磁的記録に係る記録媒体であるときは，差押え等を行う者は，被処分者に対して，電子計算機の操作その他の必要な協力を求めることができることとするものであります。

電磁的記録に係る記録媒体の差押え等を行うに当たりましては，コンピュータ・システムの構成，システムを構成する個々の電子計算機の役割・機能や操作方法，セキュリティーの解除方法，差し押さえるべき記録媒体や必要な電磁的記録が記録されているファイルの特定方法等について，技術的，専門的な知識が必要な場合が多いと考えられますことから，差押え等を実施する捜査機関等があらゆる面で自力執行することは困難な場合が多く，また，被処分者の利益の保護等の面からも適当でないことがあります。したがいまして，電磁的記録に係る記録媒体の差押え等に当たりましては，これらについて最も知識を有すると思われる被処分者の協力を得ることが必要になると考えられますし，また，被処分者の中には，記録媒体に記録されている電磁的記録について権限を有する者との関係で，これを開示しない義務を有する者もあることなどから，捜索・差押えを実施する者が協力を求め，また，これに協力することができる法的根拠を明確にしておくことが望ましいと考えられます。」

という。

ハイテク犯罪捜査においては、さまざまな技術的援助が必要となることがある。その意味で差押状の執行に際して被処分者等への協力要請を定めることは妥当である。

日弁連においてもこの点は賛成している（日弁連意見２８頁）。

６　保全要請等

要綱（骨子）第七の一は、プロバイダ等に対して通信履歴の保全を要請するものである。そして、二では、保全要請や捜査事項照会についての秘密保持の義務を定める。

要綱（骨子）は、

「第七　保全要請等

一　捜査については、電気通信を行うための設備を他人の通信の用に供する事業を営む者又は自己の業務のために不特定若しくは多数の者の通信を媒介することのできる電気通信を行うための設備を設置している者に対して、その業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴の電磁的記録のうち必要なものを特定し、九十日を超えない期間を定めて、これを消去しないよう求めることができるものとすること。ただし、差押え又は記録命令付き差押えをする必要がないと認めるに至ったときは、当該保全要請を取り消さなければならないものとすること。

二　捜査関係事項照会及び一の保全要請を行う場合において、必要があるときは、みだりにこれらの要請に関する事項を漏らさないよう求めることができるものとすること。」

とする。

これについて、法務省は、

「要綱（骨子）第七でありますが，まず，一は，捜査については，電気通信を行うための設備を他人の通信の用に供する事業を営む者等に対して，その業務上記録し又は記録すべき電気通信の送信元，送信先，通信日時その他の通信履歴の電磁的記録のうち必要なものを特定して，９０日を超えない期間を定めて，これを消去しないよう求めることができることなどを定めるものであります。

コンピュータ・ネットワーク等の電気通信を利用した犯罪の捜査におきましては，その匿名性といった特徴から，犯人の特定等のために通信履歴の電磁的記録を確保することが非常に重要でありますが，通信履歴の電磁的記録は，一般的に短期間で消去されていくことになる場合が多いという事情にございます。捜査の実務では，差押許可状を取得する前の段階において，通信履歴の電磁的記録の任意の保全を求めている場合がありますが，通信履歴の電磁的記録は，通信の当事者の利益にもかかわるものでありまして，その保全を求める法律上の根拠を明確にしておくことが望ましいと考えられますことから，このような保全要請の規定を設けることとするものであります。

サイバー犯罪に関する条約１６条１項も，締約国に対しまして，特定の捜査との関係で，既に記録・蔵置された既存のデータを削除せず維持しておくことを命ずる保全命令，あるいはこれに類する方法により確保できるようにすることを求めておりまして，要綱（骨子）第七の一は，迅速に保全する必要性が特に大きい通信履歴の電磁的記録について，条約が求める法整備を行うというものであります。

「電気通信を行うための設備を他人の通信の用に供する事業を営む者」といたしましては，例えば，インターネット・サービス・プロバイダがこれに当たりますし，「自己の業務のために不特定若しくは多数の者の通信を媒介することができる電気通信を行うための設備を設置している者」といたしましては，例えば，ＬＡＮを設置している会社等がこれに当たることになります。

要綱（骨子）第七の二は，一の保全要請と，それから捜査事項照会に関する事項の秘密保持を求めることができることとするものであります。

保全要請や捜査事項照会は，その性質上，捜査の初期段階に行うことも多く，密行性が強く求められるため，これを受ける者に対しまして，これらに関する事項をみだりに漏らしてはならない法律上の義務を負わせる必要がある場合もあることから，このような規定を設けることとするものであります。

サイバー犯罪に関する条約１６条３項も，締約国に対しまして，データを保全すべき者にデータを保全する手続がとられていることについての秘密保持義務を課することができるようにすることを求めております。

要綱（骨子）第七の二の規定を設けることによりまして，保全要請を受けたプロバイダや，捜査関係事項照会を受けた金融機関等が，その顧客等からこれらの要請に関する事項について問われても，みだりにこれに答えてはならないことが法律上明らかになります。」

と説明する。

この要綱（骨子）第七の一について、日弁連は、「保全要請は任意処分として提案されているが，事実上強制処分に等しいものであり，裁判所による司法的抑制を経ることなく行われるという点で，その新設には強く反対する。」とし、また、二についても、「このような規定の新設に反対する。」との意見を述べている（日弁連意見２９～３０頁）。その理由の要点は、憲法２１条２項の通信の秘密の保障に基づくものである。すなわち、「そもそも，我が国においては，憲法２１条２項が通信の秘密を保障し，通信の秘密の保障は『通信のすべての構成要素におよび，通信の内容のみならず，通信の存在それじたいに関する事柄－差出人（発信人），受取人（受信人）の氏名・ 住所，差出（通話・発信）個数，通信の日時，電話等の発信場所，など－についてもその秘密が保障されなければならない』（樋口陽一・佐藤幸治・中村睦男・浦部法穂『憲法〔青林書院・注解法律学全集巻２巻１９９７〕８５頁，大阪高等裁判所判決昭和４１年２月２６日・高等裁判所刑事判例集１９巻１号５８頁」とする（日弁連意見３０頁）として、「要綱（骨子）第七の一項は，差押えの前提として通信履歴の保全要請を新設しようとしているが，通信履歴であっても通信の秘密の保障が及ぶことと，保全された通信履歴は，後行する差押えによって捜査機関の手中に入ることになることからすれば，保全と差押え手続を一体として捉えることができるのであるから，やはり保全それ自体においても，通信の秘密が侵害されるおそれはあると解すべき」であるとする。

また、要綱（骨子）第七の一は、サイバー犯罪条約１６条１項の国内法化を図る意図のもとで提案されたものであるが、必ずしもサイバー犯罪条約の内容にそうものではない。

サイバー犯罪条約１６条１項は「締約国は，通信記録その他の特定のコンピュー，タ・データが滅失又は改ざんに対して特に弱いと信ずるに足りる理由がある場合には，自国の権限のある当局が，当該コンピュータ・データであってコンピュータ・システムという手段によって蔵置されたものの迅速な保全を命じ又はこれに類する方法により確保することを可能にするため，必要な立法その他の措置をとる。」また、２項は「締約国は，ある者が保有し

又は管理している特定の蔵置されたコンピュータ･データを保全するよう当該者に命ずることによって１の規定を実施する場合には，自国の権限のある当局がそのコンピュータ・データの開示を求めることを可能にするために必要な期間（九十日を限度とする。），コンピュータ・データの完全性を保全し及び維持することを当該者に命ずるため，必要な立法その他の措置をとる。締約国は，このような命令を引き続き更新することができる旨定めることができる。」と規定している。

サイバー犯罪条約は，過去のコンピュータ・データ及び通信記録については，同１６条及び同１７条で保全することを認めるとともに、将来の通信記録及び通信内容については、同２０条及び同２１条でリアルタイムに収集･傍受することを認めているのであり、サイバー犯罪条約１６条１項はあくまでも過去のコンピュータ･データについてしか保全を認めていない。

また、保全要請の期間についても、９０日とするが、サイバー犯罪条約と同じであるとはいえ、条約上の義務ではないのであり、その理由について必ずしも合理的な説明がなされてはいない。むしろ、通信傍受法と同様に３０日とする意見もある（日弁連意見３３頁）。

７　おわりに

匿名性が高く、痕跡が残りにくく、不特定多数の者に被害が及び、時間的・場所的に制約が少なく、低コストで行えるという特徴を有するハイテク犯罪の捜査は、可視性・可読性のない電磁的記録を対象とし、ネットワークで結ばれたシステムでの証拠収集保全が求められる。しかし、現行法は、有体物を対象として、物理的な干渉を前提とした法制度が構築されている。したがって、ハイテク犯罪に対処するためには基本的な法原理を踏まえ、現行法の改正がなされるなければならないと考える。

サイバー犯罪条約が「情報セキュリティ」に関心を寄せて各国に法整備を求めていることに留意する必要がある。

サイバー犯罪条約の国内法化を図るという意味においても、「情報セキュリティ」保護のための視座の転換が図られなければならないと考える。

第４章　コンピュータ法科学について

ここでは、近頃、急速に注目をましている「コンピュータ法科学」についての研究をなすにあたっての準備的な考察をすることにする。

この考察は、コンピュータ法科学についての全般的なガイダンスである「コンピュータ法科学序論」と、実際に米国で、コンピュータ法科学に関するビジネスを営んでいるベンダへの訪問記録によりなりたっている。

以下の記述でもふれるが、警察庁は『コンピュータ法科学』分野の確立にむけて活動を開始しており、そのための一つの基礎資料として役立つことがあれば、研究会としてはきわめて幸いである。

第１　コンピュータ法科学序論

弁護士高橋郁夫

1 概念

（1） 定義

現在、「Computer Forensics」という概念が、きわめて注目されている[102]。警察庁も「e-Japan 重点計画-2002」の「５　高度情報通信ネットワークの安全性及び信頼性の確保」の「具体的施策」において、この「Computer Forensics」を念頭おいて「コンピュータ法科学」への注目を明らかにしている。具体的には、その「⑥ 情報セキュリティに係る研究開発」において、「ア 国防・治安に係る情報セキュリティ技術の研究開発の推進」の中の ｉ）において「 （略）2004 年度までに、司法手続きのための電子的記録の解析技術に関する系統的な調査研究等を行い、『コンピュータ法科学』分野の確立を目指す。（警察庁）」としている[103]のである。以下、米国で説かれている「Computer Forensics」に「コンピュータ法科学」の訳語を与えて、その分析範囲と論点を網羅してみていくことにしたい。我が国でのコンピュータ法科学への注目は始まったばかりであり、全体の論点の抽出のみでも十分な意味のあることと思われる。

「コンピュータ法科学」の定義であるが、ある本によると、「コンピュータ法科学は、コンピュータ証拠の保全、識別、抽出、ドキュメント化についての考察」を取り扱うということになる。すなわち、コンピュータ証拠についての全面的な考察がその対象範囲ということになる。具体的には、消去されたコンピュータベースのデータの回復およびコンピュータ関連行為を誰が、何を、いつ、何処で、どのようになしたのかという点についての科学的調査および復元がその主たる興味の対象となるであろう。

（2）主体的分析範囲

では、コンピュータ証拠についての全面的な考察をなすとしたときに、どのような観点から分析がなされるかということになる。この点については、どのような人間がコンピュータ証拠に関与するかという点から考えるのが便宜であると思われる。そして、この主体的な側面から見たとき、大きく分けて二つの主体のグループを考えることができるのである。コンピュータ証拠の問題である以上（１）コンピュータという技術的な側面から関与するグループと（２）法廷での事実発見の見地が必要になるのであり、その法的な面から関与するグル

---

102 “Computer　Forensics”に関連する参考資料として、John R.Vacca ”Computer Forensics computer Crime Scene Investigation” Charles River Media, Inc(2002),Albert J.Marcella,Robert S.Greenfield ed.”Cyber Forensics -A Field Manual for Collecting,Examining,and Preserving Evidence of Computer Crimes” Auerbach publications(2002)など。また、オンライン上では、”Encase Legal Journal” (http://www.guidancesoftware.com/corporate/whitepapers/downloads/LegalJournal.pdf) など。

103 http://www.kantei.go.jp/jp/singi/it2/kettei/020618-2-5.html

ープである。

（1）技術的グループからの考察という点についていえば、コンピュータ証拠の保全、識別、抽出、ドキュメント化のステージごとに技術的問題点が議論されることになる。　この場合、もっとも注目されるべきは、コンピュータ法科学を提供するベンダであり、そのようなベンダが種々のサービスを提供している。また、いうまでもなく、ネットワークの防衛という観点から法執行機関等の技術的部門もこのような考察の主体として考えることができる。

一方、（2）法的グループからの考察という点についていえば、コンピュータ証拠の保全、識別、抽出、ドキュメント化のステージごとに法的問題点が議論されることになる。この場合、主として、裁判官、弁護士、検察官などの法律専門家の観点からの分析ということになる。

2 個別の論点の検討

(1)　コンピュータ証拠の保全について

コンピュータ証拠は、きわめて瞬間ごとに変化し、消滅していくものである。従って、一定の法的な意味をもったインシデントが発生した場合に、どのようにしてコンピュータ証拠を保全するべきかという論点がある。これは、その後、証拠にアクセスして識別していく前段階ということになる。この論点を技術的な側面と法的な側面から論じる場合には、以下のような論点をあげることができよう。

①　技術的側面からの要請

まず、この点での最大の要請はデータのバックアップであり、技術的には、ミラーイメージの作成ということになる。また、この際に、しかけられたトロイの木馬プログラムなどによりデータが破壊されないように心がけることになる。また、インシデントが発生した際に、的確に対応し、その後の証拠を確保するというインシデント・レスポンスという観点もこのコンピュータ法科学の観点から分析されることになる。特に、この視点からするとき外部からの変化の要因を除去することが必要になってくる。

②　法的な観点からの分析

証拠の保全についての法的な分析という観点からするとき、まず、証拠をどのような根拠から保全しうるのかということが問題になる。民事上については、E-discovery(またはDiscovery of Electronic Evidence、DEE)という観点から紛争が現実化した段階で、当事者間では、証拠を保全すべき一般的な義務が発生すると考えられている点は注目に値する。また、刑事的には、プロバイダ等に対する協力要請が、そのような証拠の保全という観点から考えられる。

(2)　コンピュータ証拠の識別について

これは、具体的なコンピュータ証拠のデータにアクセスし、データの内容を覚知する過程である。コンピュータ証拠の発見の過程ということもできる。この過程には、どこに、またはだれのもとにデータがあるかという探索の問題も含めて考えることができよう。従って、

この識別の過程は、(1)探索の過程と(2)アクセスの過程(3) データ認識(4)同一性判断の過程にわけることができると思われる。これは、その後の証拠力を判断し、抽出する過程へとつながっていくことになる。

① 技術的な論点

この識別の論点については、以下のとおりである。

(1)探索の過程については、特に攻撃者を突き止めるという作業がポイントとなる。攻撃者の IP アドレスをつきとめたりする作業がポイントとなる。この作業については、dig -x/nslookup、Whois、Ping などのコマンドがツールとして利用される。また、USENET のトラフィックサーチの利用が紹介されている。攻撃者のプロファイリングなども議論されている。また、攻撃者を突き止めた場合には、「情報戦争」の観点からは、それに対する「封じ込め」や反撃の論点も存在する。この点についてネットワーク法科学の分野であるとして、技術的に「ネットワーク法科学データおよびデータベース[104]」「Visual query interface 」「Network forensic data visualizers」などの手法が議論されている。

(2)アクセスの過程においては、インシデントがあることを発見し、それに関する証拠の収集が問題となることを認識することになる。まず、インシデントの発見という観点がある。これついては、「侵入検知サービス」が議論されるし、また、さらに過去の事実を再現する行為を「デジタル探偵(Digital Detective)」をするといい、この点も議論される。

また、実際に、法執行などでコンピュータの捜索・押収などもこの点で議論することができる。具体的には、捜索の前の準備、捜索の手順(ガイドライン)、記録の重要性、実際の捜索・押収(準備、スナップショット、移動、検査)などの論点ということになるであろう。

(3)データ認識においては、隠されたデータ(スワップファイル、メモリ上のデータ、ファイルスラック、消去されたファイルなど)、データ回復(リカバリー)や暗号の問題が議論される。データのコンバージョンなどの問題もある。このコンバージョンというのは、どのようなソフトウェア、ハードウェアなどを利用して、利用し得る形態に変換するかという問題である。

(4)同一性判断は、まさに狭義の「識別」と呼ぶこともできる問題である。コンピュータ証拠をめぐる過程では、種々のコンピュータ上に種々のデータが、認識される。そのうち、どれとどれが同一であるのかを判断していくことが問題となる。この観点からは、とくに正確な時間の問題が議論される。

② 法的な論点

この識別の論点については、上記の各項目ごとに対応させると以下の法的論点を指摘することができるであろう。

(1)探索の過程については、特に攻撃者を突き止めるという作業については、これをなしうる法的根拠、また、得た結果について、法執行機関に対する自発的開示の問題となるであ

---

104 IP セッションを記録するデータとして時間、日付、IP アドレス、セッションタイプ、継続時間などのデータについて、これをデータウエアハウスに集積させるという論点である。

ろう。また、法執行機関がなす一般的な電子的監視といわれる行為についていえば、その根拠がポイントとなる。

また、「情報戦争」の観点からは、法的に、情報戦争や攻撃、反撃などの概念をどのように位置づけるかという論点も存在するであろう。

(2)アクセスの過程における法的論点としては、そもそも、アクセスをなしうる法的な権限というのはなにかという問題がある。司法省マニュアルで議論されているが、法執行などでコンピュータの捜索・押収の権限として議論されている点である。また、 民間企業などで、従業員の企業秩序違反行為に対して企業がどのような根拠から、どのような調査をなしうるかという点もこのコンピュータ法科学での論点として認識されるのである。

また、ここでアクセスされるデータについては、後にコンピュータ証拠として事実認定に使われることになる。その際には、証拠として認証の過程が正当であると評価される必要があることになる。証拠については「許容性」「真正性」「完成性(Complete)」「信頼性(reliable)」「証明力(believable)」などの論点があり、かなりの部分は、このアクセスの過程における問題として認識することができるであろう。

(3)データ認識の過程における法的問題としては、暗号の問題についての法的議論は、代表的な論点であろう。また、認識の際に正確にデータを認識することなどは、証拠についての基本的なルールの問題でもあり、特に情報の正確性を確実にするほど、データが「安全」であったかどうかという点については、「チェーン・オブ・カステディ」として議論されている。

(4)同一性判断-狭義の「識別」の問題。法的な紛争においては、時間がキーポイントとなることも多く、重要な問題である。刑事的なアリバイの問題もあるだろうし、不正競争における相手方の対するスパイ行為などとその不正性などの観点から正確な時間の記録といった問題がる。

(3)　コンピュータ証拠の抽出

現代社会において、日頃コンピュータで生成されるデータはきわめて膨大なものがある。そのデータを認識したとしても、実際の事案との関連性がある証拠はなにかという観点から証拠は、抽出されなければならない。この点についての論点は、以下のようなものをあげることができるであろう。

①技術的な論点として

キーワードサーチの利用法が議論されている。また、ファイルなどが消去され、また、一般的な拡張子でないものがふされている場合もある。さらにバイナリーファイルについても、検索がなされる必要があり、そのための手法なども議論されている。

②法的な論点として

必要な証拠を抽出するのにあたって、法科学研究所などで分析をすることができるか、現場での捜査と分析との分担をどう考えるかという問題がある。また、どのようにして、犯罪に無関係の一般のデータに対する認識を最小限にすべきかという論点も存在する。また、近

頃は、民事での開示手続きとコンピュータ証拠という観点から、この抽出作業が、重要かつ一般的になってきているといわれている。また、その抽出等に技術的に困難性が伴う場合に、裁判所の手続きのなかで、どのようにしてその技術的な困難さを克服するかという観点から専門家証人の利用という問題もある。

(4)　コンピュータ証拠のドキュメント化

① 技術的な論点について

これは、証拠の意味や取得経過を伝えるという過程になる。まず、取得経過自体を後になされる法的手続きにおける質問に対して正確に答えるという要請がある。また、証拠自体を可視化するということもあるし、その意味自体についての分析、証言ということもある。

② 法的な論点について

証拠の取得経過の伝達という観点からは、前述の「チェーン・オブ・カステディ」と証拠についての「ファウンデーション・クエスチョン」の問題がある。また、証拠の可視化については、プリントアウトの法的な意義という問題もある。

3 全般的な論点について

上記の個別の論点に関連して、いわば、全体に関連する形で、以下のような論点をあげることができる。

（1）コンピュータ専門家証人としての証言

特に米国においては、その証拠の収集・分析などにコンピュータ法科学の専門家が、専門家証人として出廷し、種々の出来事について、証言する。この証言が、陪審にわかりやすく表現できるか、という点も、重要な論点である。

（2）　コンピュータ専門家としての裁判への協力

上記とも関連するが、米国の裁判においては、専門家として裁判の種々の手続きに協力することが多い。E-discovery において、その証拠の発見・分析などを行うのにもコンピュータ専門家の助力を仰いでおり、コンピュータ専門家の果たす役割は大きい。

(3)　コンピュータ取扱技術の教育

また、データに対する管理・モニタリングの技術・インシデントに対する対応技術やその他の技術など法科学の技術一般については、専門的な色彩が強い。これらの技術を依頼者の求めに応じて、依頼者の従業員に対して教育するというのもコンピュータ法科学ベンダの業務のうち重要な一つであるということができる。

(4)　その他

インシデントが発生したり、また、企業内で不祥事が発生したりという場合には、法執行機関の助力を仰ぐ必要がある。その際に、コンピュータ法科学ベンダのアドバイスを求めることになる。また、ネットワークでの議論をモニターし、セキュリティ上の情報として依頼者に対して対応のアドバイスを提供するなども、そのようなベンダにとって重要な活動となる。

第２　コンピュータ法科学ベンダ訪問記録

１　TruSecure 会議録

日時　平成 15 年 12 月 9 日　午前 10 時から午前 11 時 30 分（現地時間）

場所　TruSecure Corporation

13650 Dulles Technology Drive, Suite 500

Herndon, VA

参加者

米国（TruSecure）側参加者

William Harrod

（Director,Investigative Response Division；Senior Forensic Investigator）

日本側参加者

高橋郁夫(弁護士、宇都宮大学講師)

石井徹哉(奈良産業大学、刑事法)

小島　淳(岡山大学、刑事訴訟法)

１　序

最初に高橋弁護士から、ハロッド氏に対し、インタビューの機会を設けていただいたことに対する謝辞が述べられ、全参加者の自己紹介[105]を経て、インタビューに移った。インタビューは、まずハロッド氏が質問票の内容にも配慮しつつ TruSecure の組織、業務内容の概略等につき説明し、その後日本側参加者から補足的な質問を受けるという形式で行われた。その概要は以下の通りである。

２　TruSecure の組織

組織としては、主に各種リサーチチームが中心となる。特に、調査対応（検査、分析、報告）チームが重要である。しかし、それ以外にも、セキュリティ保証の部門や、他の企業同様、営業、会計、経理、マーケティングに関する部門もある。

TruSecure では、およそ 300 人が働いており、リスク分析およびリスクアセスメントの業務に従事している。そのうち、ハはロッド氏の率いる調査対応チームには 10 人が所属しており、各種調査活動に従事している。ただ、重大なリスクアラートの場合や、同社の中心的

---

[105] なお、ハロッド氏の自己紹介の概要は以下の通りである。

現在 TruSecure の調査対応部門の Director である。以前は―TruSecure の前身たる―ICSA に 5 年間勤務しており、その前には FBI のラピッドスタートチームの一員であったこともある。日本との関係では、三菱やパナソニックと仕事をしたことがあり、東京、大阪、神戸などに行ったことがある。

な業務（central practice）に必要な場合などにおいて、調査対応を援助するためにリサーチグループが組まれることもある。

TruSecure の社員は、様々なバックグラウンドを有しており、軍隊や法執行官出身の者もいる。一般には、それらの者も含め、コンピュータ通信関連の仕事についていた者が多い。なお、後述のように、同社の行う調査は非常に微妙な問題を扱うものなので、採用の際には極めて神経を使う。倫理面も含め、同社の調査員は何ら危険でないということが保証されていなければならない。そのような観点から、ハッカーの前歴がないことを確認したりもする。

TruSecure は、二つの研究所を有しており、一つはヴァージニア州 Herndon にあり、もう一つは、ペンシルヴェニア州にある。いずれの研究所においても、調査のための十分な設備が整っている。

3 TruSecure の業務の内容

〔概要〕

TruSecure の業務の中心は、リスクマネジメント―主に情報セキュリティ―である。ここには、事件の発生を未然に防止するための調査対応（investigation response）業務のほか、最近では、実際に何か問題が発生した際に、それに対応する業務―事件対応（incident response）業務と呼ぶ―にも力を入れている。

調査を通じてのクライシスマネジメントや、訴追の援助（prosecution assistance）、伝統的なコンピュータ法科学、さらにはインターネット法科学[106]に関わる業務などがある。実際に行った調査の数は、ここ 2 年間で約 50 件程度であり、それらの中には数週間で調査が終了したものもあれば、終了までに何カ月も要したものもあった。

TruSecure の最大の財源となっているのは、情報セキュリティプロファイルのチェック及び認証の業務である。同社が行っているような基準準拠型評価（criteria based evaluation）を内容とする業務には、時差（time lag）がつきものであるが、そうした時差をできる限り生じないようにするべく、予測を立てることが重要となる。

TruSecure は毎年業績を伸ばしているが、これは、一つには、企業がそれまでセキュリティに予算を割く際に重点の置き所を誤っていたこと（focusing wrongly）、いわば「地球は平らである」とでもいうべき精神性を有していたことによるところが大きい。つまり、固定観念にとらわれて、それまであまり有効とはいえない出費をしてきたのである。たとえば、2002 年においては、約 3400 件の脆弱性が確認され―それと同じ数のパッチ（修復プログラム）が出され―たが、そのうち実際にコンピュータに影響があるとされたのは、たった 2%だっ

106 「インターネット法科学」に関するコメントの内容は次の通りである。
ウィルス作成者やハッカーを常時追跡（track）するアンダーグラウンドインテリジェンス組織があり、３０００件のデータベースを有している。1 日に３GB に相当するデータ通信をモニタリングしており、ＩＲＣチャンネルなどの会議もモニタリングしている。そうしたことを通じて得られた情報もまた、予測・予防・調査のために役立てられている。

た。TruSecure の目的は、これら 2%にあたるのはどれであるか、これに対処する責任があるのは誰か、修復をいつまでになさねばならないかなどといったことを正確に予測し、顧客企業に伝えることである。こうしたサービスの有用性が理解されるようになってきたため、TruSecure に対する需要が増大しているものと推測される。

調査は、ログやデータを収集し、それを分析するという過程をたどる。いったん分析した後に、依頼者側に質問をする場合もある。調査依頼全体のうちの約 70%については、コンピュータ法科学に即した詳細な分析が必要となる。ただ、調査結果が裁判所に提出されたり、それに関する証言が必要とされたりするのは、全体のわずか 2～3%に過ぎない。

TruSecure と他の情報セキュリティ企業との違いは、他社はコンピュータ法科学のみを使命としている場合が多いのに対し、TruSecure は調査対応に関する総合的な視点（wholistic view）に立ったサービスを提供している点である。法科学だけでなく、他のコンポーネントをも取り揃えている。また、同社では、コスト・アイデンティフィケーションによって、間接的に、法的に争うべき事案（legal case）なのか、単なるビジネス事例（business case）にとどめるべき事案なのかを企業が判断することを可能にしており、それにより企業が訴訟事件のコストを抑えることも可能にしている。

４ 司法省コンピュータ捜索・押収マニュアル（以下「DoJ マニュアル」という）及び法的な問題点

〔DoJ マニュアルについて〕

DoJ マニュアルは非常によい基礎的な資料だと考えられる。ただ、これは、政府機関および法執行機関に対する文書なので、民間企業を拘束する性質のものではない。ただ、逆に、企業がインターネット・サービス・プロバイダ（以下「ＩＳＰ」という）に対してデータの保存を強制したりすることもできない。

〔DoJ マニュアル以外の参考文献について〕

ハロッド氏は、国立司法研究所（National Institute of Justice）の技術部門ワーキンググループに属しており、その方面におけるガイドを執筆している。調査の手順に関するものもある。たとえば、First Responders Guide や Forensic Investigations に関するもの（公刊予定）などである[107]。ただ、技術の進歩が早いので、出版物での対応には限界があると考えられる。

〔捜査協力について〕

捜査協力の場面においては、同社は私企業と法執行機関との間の「リエゾン」となる場合がある。すなわち、捜査に関係する情報を入手するという法執行機関の利益と企業側の一定

[107] これらについては、www.nist.gov も参照。

の情報に関する機密保持の利益とを、客観的な（中立的な）第三者として調整する役割を担うこととなるのである。

TruSecure が法執行機関に協力する場合としては、まず、法執行機関から直接依頼を受ける場合がある。また、企業が捜査の必要を感じ、法執行機関を伴って調査を依頼しにくる場合もある。そして、企業から依頼を受けて調査をした結果、問題が発見されたという場合に、企業の同意を得て法執行機関へ通報するということもある。同社が法執行機関に協力したことが、コンピュータウイルスの作者の逮捕につながった例として、Melissa ウイルスや Anna Kournikova ウイルスの場合を挙げることができる。

ただ、こうした調査はビジネスでやっているものであり、協力することもビジネスの一環である。したがって、費用は依頼者に負担してもらうことになる。費用は企業が負担する場合がほとんどであるが、法執行機関が負担する場合もないわけではない。企業と法執行機関とが関係している場合で、企業の負担すべき費用の額が大きすぎる場合には、法執行機関にこれを負担させる命令を求めることができる。ただ、そうした場合も含め、法執行機関が費用を負担することは稀である。

法執行機関との協力の仕方は、一言で言えば「順向的（“proactive”）」である。裁判所の命令が出たりする前に協力するようにしている。また、分析結果や報告等の内容が依頼者たる企業の意向などに影響されたりすることはない。法科学的分析に基づいて得られた結果を、中立的な立場から報告している。

〔コンピュータ法科学について〕

コンピュータ法科学と他の法科学とは、前者においては主観の入る余地がやや大きいという点に違いがある。実際にグレイゾーンもある。したがって、推論（inference）という形をとる場合もあるが、高度の蓋然性がない限り、証拠としては提出しない。こうした意味で、場合によっては調査に困難が伴うこともあるため、TruSecure としては、企業には、法科学に親しみやすい環境を整えるよう勧めている。機器の時間を合わせておくこと（time synchronization）や、ログを保存しておくことなどを勧めている。これにより、証拠を取得しやすくなる。

コンピュータ法科学の観点から、ここ数年で台頭してきている問題として、一つの独立した端末ではなく、ネットワーク端末をいかに法科学的に分析するかという問題がある。これが「ネットワーク法科学」の問題である。ここでは、対象となるコンピュータの数が著しく拡大し、問題の重点が、コンピュータ本体ではなくデータをどのように収集するかの点に移ってきている。ネットワークコンピュータを全て持ってくると、ビジネス全体が停止してしまうため、いかに必要なデータのみを取得するかを考えることになる。

もう一つは、予測に基づくいわば予防的な措置がますます重要になってきていることである。Blaster などの本当の意味でのリスク（real world risk）を識別し、それをいち早く企業に告知し、予防策を講ずるようにさせなければならない。

また、ほかにも、ワイヤレスなどの新しい機器への対応という問題もある。

〔TruSecure が実際に直面する法的な問題点について〕

法的な問題点としては、裁判所での専門家としての証言の問題や、企業側弁護士のオフィスでの供述に関する弁護士（秘匿）特権の問題がある。刑事手続においては、実際に調査結果に基づく認定を証言することもあるが、データを法執行機関に提供し、当該機関が証言するという場合もある。一方、民事手続の場合には、和解で決着がつくことが多い。

5 その他

〔日本におけるネットセキュリティ対応について〕

日本は、TruSecure がサービスを提供するマーケットとしては、やや難がある。伝統的に「従順（obedience）」を旨とする文化があることや、企業が信用を重視するために、何かが起こってもすぐ公にしたがらないという土壌があることなどが理由として挙げられる。特に後者の観点からは、ネットワークセキュリティは、重要なビジネスドライバーにはなりにくい。ネットワーク上のリスクはどんどん増大しており[108]、ネットワークでつながれている以上は、そのリスクは世界共通[109]であるから、それを適切に評価し、防御策を講じることは極めて重要である。にもかかわらず、日本の企業はこれにあまり予算をかけたがらないようである。

〔「責任ある開示（responsible disclosure）」について〕

ICSA ラボでは、依頼に応じて特定のプラグラムをチェックし、脆弱性の検査及び分析を行っている。90 日に一度ベンダーコミュニティと会合し、定期的に連絡も取り合っている。脆弱性が発見された場合には、公表する前にそのプログラムを販売しているベンダに通告し、他社の製品もテストして、共通の脆弱性が認められる範囲のベンダ全てに通告することもある。

リスクアシュアランスという観点からも、色々な問題がある。たとえば、ロジスティックコントロールの問題や、ポート数削減の問題などである。

なお、外部から TruSecure に特定のプログラムの脆弱性の指摘がなされた場合には、研究所で９ケ月かけて分析する。それで脆弱性が確認できた場合には、該当するベンダに通告し、その後公表する。

この点に関しては、企業側の姿勢も問題となる。通信のプライバシーの保護の問題と、企業側の脆弱性開示に対する非協力的な姿勢の問題である。開示は、確かにネガティブな効果

---

[108] 合衆国では、一つの IP アドレスに対する外部からのネットを通じた攻撃は、1999 年のデータと 2003 年のデータを比べると、平均で 6～7 倍にもなっているという。

[109] なお、日本以外の環太平洋地域の国々のうち、ネットワークセキュリティのビジネスが成長している国として、オーストラリア、タイワン、タイ、シンガポールなどが挙げられる。

を伴う場合もある。公表されるくらいなら修復等にかかるコストを呑んだ方がいいと企業が考える場合もある。ただ、企業は、そうした事態に対処する際にかかる全体のコスト（ここには一定の期間 e-commerce や e-mail が使用できなくなることに伴う機会の逸失に伴う不利益も含まれる）がどれだけ膨大なものになるのかを把握できていない。費用便益定式（cost-benefit equation）という点で、ペイしないことになることが理解できていないのである。

開示がなされなければ、侵入が繰り返され、永続的なものとなる可能性がある。Web ページを改ざんされたりすることもある。そして、これは他の企業にも波及しうる。侵入がどのようして行われるか、クレジットカード情報などがどのように漏れているのかがわかっていなければ、適切な対応策を講じることができない。

２　KrollOntrack 会議録

日時　平成１５年１２月１１日　午前１０時　KrollOntrack **社**
場所　KrollOntrack **社**

参加者
米国側参加者（KrollOntrack）Jason Paroff
日本側参加者
　高橋郁夫(弁護士、宇都宮大学講師)
　石井徹哉(奈良産業大学助教授、刑事法)
　小島　淳(岡山大学助教授、刑事訴訟法)

１　序

最初に高橋弁護士から、インタビューの機会を設けて貰ったこと対する謝辞が述べられた。その後、全参加者の自己紹介などをはさみながら、インタビューに移った。インタビューは、事前に準備している書類をもとに KrollOntrack **の事業内容、それにかかわる個別の論点についての説明、さらに法的論点についての会議、事務所内の研究所の視察、最後に** E-discovery **の実演という順番で行われた。その概要は、以下のとおりである。**

２　　Paroff 氏の経歴等とコンピュータ法科学について

Paroff **氏によれば、日本側参加者における今回の企画の最大の目的である** DOJ **マニュアルの翻訳について、**DOJ **マニュアルは、非常によい書類でベストプラクティスを明らかにしているものであるという評価がなされるとのことであった。また、**KrollOntrack **社のパンフレットおよびメモが事前に準備されていたが、それは、対応時についてのプロトコル、**2002 **年の** FBI/CSI **のサーベイ、制定法などを含むものであった。**

Paroff **氏は、**1991 **年にロースクールを卒業し、その後、いろいろな種類の刑事事件（強盗、脅迫全ての種類を含む）を取り扱う検察官を** 5 **年半ほどくらい勤めた（**97 **年まで)。そのころより、コンピュータ証拠に興味を持ち出した。当時は、コンピュータ証拠をどのように取り扱うかは、検察官としても、まったく不明であった。もし、検察官側において、コンピュータ証拠を用いるとすると、敗北していしまうのは明らかであったという。検察側としては、法科学（**Forensic**）コースをセットアップして、証拠の取扱を準備した。当時においては、法科学は、全く新しい分野であった。その後、**1997 **年からは、**KrollOntrack **社に勤務し、現在にいたっている。**

コンピュータ事件の最初ともいうべきスティーブ・ジャクソンゲームズ事件があってから、15 **年も経過しておらず、コンピュータ法科学は、きわめて新しい分野である。コンピュー**

タ法科学については、学位もなく、資格もなく、基準もない。コンピュータ法科学の分野は、将来の成長する分野であるが、現時点において、その成長の最初の段階にあると考えられる。現段階においては、コンピュータデータが証拠となること、そのデータが証拠として使われるようになることがポイントとなる。

３　KrollOntrack 社の業務内容

（１）業務内容

KrollOntrack 社の業務は、以下の３つである。

（ア）データ回復（Recovery）

1993 年から従事している。Kroll 社は、データリカバリーの最大の会社である。具体的には、ハードディスクの破損の際の回復が代表的な業務となる。この際に、データを回復することが目的となる。そのための技術としては、RAID、SANS などが利用されている。

なお、日本においては YE データ株式会社がパートナーで、必要な際には、データを送ってくるとのことであった。

（イ）コンピュータ法科学（Forensic）

これは、主として、職場における企業秩序維持からする懲戒およびそのための調査に関するものである。具体的には、従業員は、職場で職務に関係のないファイルをダウンロードすることもあり、また、職場をやめてから 6 日間で、競合する会社をつくることもある。これらの行為について、企業秩序維持のために、データを調査し、分析することが業務となる。従業員のコンピュータは、会社から、与えられるものであり、会社は、従業員のコンピュータについて、見ることを許容する「権限」を有していることになる。

（ウ）E-discovery

３つめは、電子ディスカバリーである。証拠開示の際に、多量の文書をレビューし、分析し、必要なものを分析して、相手方に提出し、分析する量を目指すものである。

（２）事務所内のプレゼンテーション

なお、その後、事務所内において電子開示の際のオンラインでの法律家による電子ドキュリメントのレビューについてのプレゼンテーションがあった。

（３）成長分野

データリカバリーについては、8-10 パーセントの割合で伸びているが、フォレンジックスについては、年間 150 パーセントの割合で伸びている。これから、発展していく分野であることを確信しているとのことであった。

４　コンピュータ証拠と法の注目すべき論点

（１）法執行機関との連携について

KrollOntrack 社の組織自体は、警察庁とは、関係があるわけではない。警察では、自分達の部門というのをもっており、その部門が基本的には対応しうることによる。しかしながら、

警察が、物理的対応しきれない際に、警察は、KrollOntrack 社の助力を仰ぐことになる。これは、KrollOntrack 社にクリーンルームがあり、また、機材を揃えていることもあるので、対応できることによる。今回、訪問した KrollOntrack 社の支社は規模的に小さいが、本部は、非常に大きな建物があり、たくさんの機械を有している。警察では、適切な機械を有していない場合でも、本社では、数百のテープドライブをもっており、警察は、あたらしい機械しかないので、そのような際に、KrollOntrack 社に依頼してくることになる。また、火災にあったり海に投げ込まれたりして損傷したテープの復元を依頼することもあるという。ほとんど、すべての種類のテープを準備しており、ミネソタの本社では、捜査官が証拠物件をもってきて、とまりこんでいることもあるという。

（2）証拠のファウンデーション・クエスチョンと証拠の許容性

アメリカの証拠法においては、「証拠のファウンデーション・クエスチョン」という手続がある。これは、裁判官あるいは弁護士が、相手の弁護士に対して「この情報はなんですか、どこからきたのか、改竄されていないのか、なんであるか、何を意味するのですか」というものである。証拠の意味するところについて、適切な手続きに従ってされていること、精確な手順にしたがっていることについて、専門家証人として、証言するのであるが、一つの仕事になっている。ここで、証拠の許容性、信用性について、専門家証人の意義について、さらに質疑により詳細な教示を求めたところ、証拠は、事案との関連性、probative-証明しようとしていること、排除されないことの観点が必要になる。そして、専門家証人は、それらの観点から、データを分析することになる。その際に利用するのが、データクローナーであり、これは、すべてのデータをクローンする点に特徴がある。すなわち、アクティブ・ファイルだけではなく、削除されたデータについても、完全にコピーし、データのフラグメントであろうとコピーするのである。速度は、1 分間に 1 ギガバイトをコピー―するものであり、ノートパソコンのデータであれば、20 分程度でコピーするとのことであった。

コンピュータ証拠については、いつ、どこにデータがあり、それをだれが許容しているか、そして、どのような手法でコピーがとられたか、その際のモデルの番号、シリアルナンバー、ドライブの大きさなどの諸事情を指す「チェーン・オブ・カステディ」という問題がある。裁判所においては、これらの各要素すなわち時間、機械の様子、完全なコピーであること、コピーのなされたことなどが、とても重要な問題なるとのことであった。

これらのコンピュータ証拠の許容性についての専門家証人に対しての質問については、従来と比較した場合、この問題について、代理人が、よりスマートになっているので、質問は、厳しくなってきているとのことであった。

またデータの原本性については、オリジナルデータについては、日付が変わることはないと考えられ、日付が変わるとすれば、複製であるとのことであった。アメリカにおいても、複製の日付が変わることがあるが、日時は、重要な場合では、問題とされるが、そうでない場合は、許容されるであろうとのことであった。

（3）電子証拠の保全義務

電子開示における電子証拠の保全義務の問題はきわめて注目を浴びている。特に証拠の保全の要請がなくても、当事者は、紛争が具体化した後は、コンピュータ証拠を保全しなければならないのである。もっとも、紛争が具体化した時期といっても、それが具体的にいつなのかという点については、議論かある。裁判所の判断は、バラバラであり、いろいろな議論がある。大きく捉えると、訴訟になったと知っている時という説と訴状が送達された時という説がある。

（４）暗号の問題

なお、質疑は、暗号にも及び、暗号については、それほどの困難性を感じるものではないとのことであった。もっとも、PGP であれば、困難性については、まだ別とのことであった。