ISSN 1344-4816

GLOCOM Review

Volume 6, Number 6
June 2001

今号の内容

□ブロードバンド時代のネットワーク・セキュリティ
..... 山田 肇

国際大学グローバル・コミュニケーション・センター
Center for Global Communications
International University of Japan

2001年6月1日発行（第6巻第6号通巻64号）
発行人　公文俊平　　編集人　豊福晋平
発行　　国際大学グローバル・コミュニケーション・センター
Copyright (C) 2000 Center for Global Communications

GLOCOM Review は、国際大学グローバル・コミュニケーション・センター（GLOCOM）がその著作権を有するものであり、著作権法上の例外を除き許可なく全文またはその一部を複写・複製・転載することは法律で禁じられています。

GLOCOM Review 6:6 (64)
© 2000 Center for Global Communications

ブロードバンド時代の ネットワーク・セキュリティ

山田 肇

目次

1. 日本におけるネットワーク犯罪の状況
2. ネットワークの高度化による危険の増大
3. ネットワーク犯罪の捜査
4. ネットワーク犯罪への対応
5. アメリカの状況と議論
6. ヨーロッパにおける議論と対応
7. まとめと提案

要旨

ネットワーク犯罪は、匿名性が高い、犯罪の痕跡が残りにくい、不特定多数のものに被害が及ぶ、容易に国境を越えることができるなど、他の犯罪にはない特徴がある。しかも、これらの犯罪は、IPv6 の本格的普及、アドホック・ネットワークという利用形態の浸透により、これからますます深刻化していくことが懸念される。

これらの犯罪に対抗していくためには、通信傍受による捜査、通信記録による捜査などの手段が考えられるが、このような捜査方法をめぐっては、プライバシー保護の問題や捜査技術の標準化など、解決すべき課題がいくつか残されている。アメリカやヨーロッパでは、ネットワーク犯罪に対抗するための手段として、通信傍受が真剣に取り上げられており、特にヨーロッパでは官民挙げての通信傍受技術の標準化が行なわれている。

本稿では、このような事例を紹介し、ブロードバンド時代のセキュリティを確保するという視点から何が必要なのかを考察する。

1. 日本におけるネットワーク犯罪の状況

警察庁では、コンピュータや電磁的な記録を対象とした犯罪、ネットワークを利用した犯罪および不正アクセス禁止法違反の3つを、ハイテク犯罪と総称している。これらのハイテク犯罪には、匿名性が高い、犯罪の痕跡が残りにくい、不特定多数のものに被害が及ぶ、容易に国境を越えることができるなど、他の犯罪にはない特徴があるとして、警察庁は特別にその推移をウォッチングしている。

第1のコンピュータや電磁的な記録を対象とした犯罪とは、コンピュータ・ウィルスを送ってコンピュータを正常な動作ができない状態にしたり、電磁的な記録を不正に入手したりする犯罪である。第2のネットワークを利用した犯罪には、他人になりすまして詐欺を働く行為、わいせつ物の頒布、名誉毀損などが含まれる。

また、不正アクセス禁止法は2000年2月13日に施行された法律で、他人のパスワードを利用してコンピュータに不正に侵入したり、ソフトウェアの欠陥、すなわちセキュリティ・ホールをついて侵入したりするのを取り締まるものである。この法律では、このような行為を行ったものは、1年以下の懲役または50万円以下の罰金に問われることになっている。一方で、法人、個人を問わずシステムの管理者にハッキングの防止処置を講じる責務をうたっていることも、この法律の特徴である[1]。

表1は、警察庁の発表したハイテク犯罪の検挙件数の推移である。この表から、ハイテク犯罪件数が全体として、また、とりわけネットワークを利用した犯罪が増加の傾向にあることを読み取ることができる。警察庁によれば、インターネット・オークションを利用した詐欺や著作権法違反の多発が、ネットワーク利用犯罪の増加の原因であるそうだ。また、不正アクセス禁止法にかかわる不正行為が、法律施行日以降2000年一杯で106件に達したことも、同様に警察庁から報告されている[2]。

表1　ハイテク犯罪の検挙件数[3]

	1998年	1999年	2000年
コンピュータ，電磁的記録犯罪	299	110	44
ネットワーク利用犯罪	116	247	484
不正アクセス禁止法違反			31
合計	415	357	559

一方、国内にはコンピュータ緊急対応センター(Japan Computer Emergency Response Team Coordination Center：JPCERT/CC)が非営利団体として組織され、不正なシステム侵入に対する緊急対応、特に不正アクセスの被害状況の把握や対策の情報提供などを中心に活動を行っている。このJPCERT/CCは、受理した不正行為の件数をグラフにして、図1のような形で公表している[4]。この図から

2000 年に入って、不正件数が前年より倍増したことがわかる。

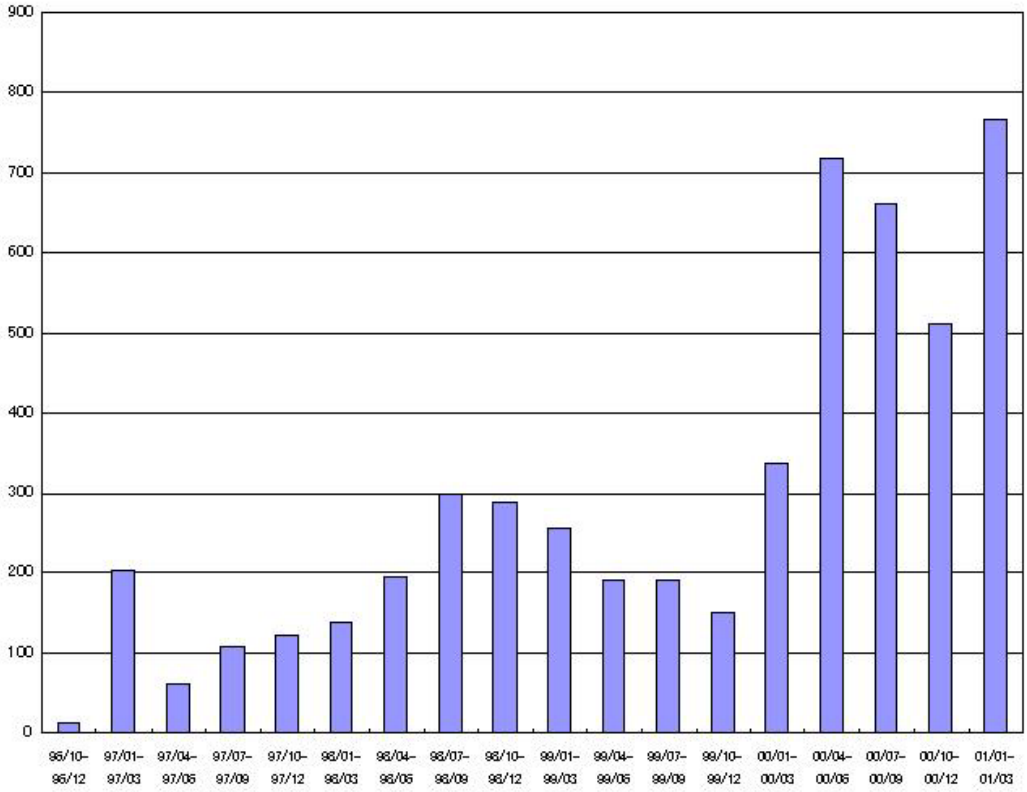

図１　JPCERT/CC に報告されたサーバへの不正アクセス件数

2000 年１月には、科学技術庁と総務庁のホームページが書き換えられる事件が発生した[5]。ネットワークを利用したストーカー被害が増えているとの報道もある[6]。最近では、日本の歴史教科書の検定問題に反発して、海外から文部科学省やその教科書の出版元にアクセスが殺到し、ホームページが麻痺して接続できない事態が起きたという[7]。

このようにハイテク犯罪の件数が増加しているにもかかわらず、市民や企業の関心は総じて低い。警察庁は 2000 年 3 月に東証一部上場企業など 2000 社を対象にサイバーテロに関するアンケート調査を実施した。ここでいうサイバーテロとは、ネットワークを通じて国家や社会の重要な基盤を機能不全に陥れる犯罪であって、ハイテク犯罪の中でも甚大で深刻な被害を及ぼす危険性があるものである。

このアンケートに対して 844 社が回答を寄せているが、その回答は次のように整理されている[8]。

- 情報通信分野の企業は一部上場企業の平均(50%)よりもサイバーテロの危険性に対する意識が高いが(60%)、交通、医療分野では危険性に対する意識が低い(30%以下)。

- 約 1/3 の企業で個人識別コード：ID やパスワードの管理、従業員教育などの項目を網羅したセキュリティに関する内部規則、すなわちセキュリティ・ポリシーを策定しており、金融では多くの企業がセキュリティ・ポリシーを持っている。情報通信・エネルギーでも多くの企業が一部の情報システムについては策定済みである。
- サイバーテロに対するコンティンジェンシー・プラン(不測事態対応計画)を策定している企業は 1%程度である。

この調査結果から読み取れるように、サイバーテロが脅威であるということ自体は企業の意識に浸透しつつある。しかし、それが発生した場合にどのように対応すべきかを記述したコンティンジェンシー・プランを持つ企業は皆無で、対策にまでは手が付いていない状況であることがわかる。

2. ネットワークの高度化による危険の増大

ブロードバンド時代のネットワークについて、セキュリティの観点では 2 つの注目すべきポイントがある。第 1 はインターネット・プロトコルが Internet Protocol version6 (IPv6)へと変更されるということであって、第 2 はアドホック型のネットワークが増加するということである。

2.1 機器接続数の増加に伴う危険

現在インターネットで広く利用されているのは、Internet Protocol version4 (IPv4)と呼ばれるプロトコルである。これは 20 年以上も前に設計されたプロトコルであって、インターネットの社会的な位置付けが変化した現在では、さまざまな技術的問題が発生しはじめている。その端を発したのは、IP アドレスの枯渇という問題であった。

IPv4 では、アドレス空間は 32 ビットの幅を持っており、これで約 43 億個の機器インタフェースが識別できた。これが IPv6 では、128 ビットに拡張され、最大では 43 億× 43 億× 43 億× 43 億個の機器インタフェースが識別できるようになる。ネットワーク対応の次世代冷蔵庫や電子レンジには、それぞれに固有のアドレスが付与され、直接、インターネットに接続できるようになるといわれている。

この固有アドレスが自動的に付与できるようにしたことも、IPv6 の特徴である。次世代冷蔵庫を接続するときに複雑な設定をしなければならないとすれば、コンピュータ技術を持っていない利用者には障害になる。そこでそれをインター

ネットに接続した瞬間に自動的に設定しようというのが、Plug and Play という技術である。またセキュリティ機能については、IPv6 では、あらかじめ交換しておいた鍵を利用して、必要に応じてヘッダより後の部分を暗号化したり、届いたパケットを認証したりできるようになっている。

このような IPv6 がブロードバンド・ネットワークに採用されたとき、ネットワーク犯罪者は、それを悪用しようと考えるに違いない。ネットワーク犯罪には、次のような類型があるといわれている[9]。この類型の分類は、警察庁によるハイテク犯罪の 3 分類と直接対応するものではないが、技術説明としてはわかりやすい。

- 特定のコンピュータに不正侵入して、データを破壊したり、改ざんしたりする。
- 特定のホームページに短期間に大量の接続要求を送り、サーバをパンクさせる。
- コンピュータ・ウィルスや迷惑メールを多数に送り、不特定多数のコンピュータのデータを破壊する。

IPv6 によって接続されたネットワーク対応の冷蔵庫や電子レンジが拠点にできれば、ネットワーク犯罪者は、これらいずれの類型の犯罪も実行することができる。もっとも容易に想像できるのは第 2 の類型に関する犯罪である。何百万台かの冷蔵庫から特定のホームページへのアクセスを実行すれば、サーバをパンクさせることは簡単である。また、そのサーバが接続されているネットワークに設置されたルータなどについても、動作障害を起こすことができるだろう。極端な場合には、通信網全体を混乱させることもできる。

また、同様に何百万台かの次世代電子レンジからコンピュータ・ウィルスや迷惑メールを拡散するようにすれば、今より大規模に、また急激に多数のコンピュータを破壊することができるだろう。類型 3 の犯罪である。

では、どのようにすればネットワーク対応の冷蔵庫や電子レンジを拠点にできるのであろう。『日経 NETWORK』に、ネットワーク犯罪者の手口を説明する記事が掲載されている[10]。それによると、(1)ネットワークに接続されている機器を拾い出し、(2)その機器で動作中の通信ソフトウェアを洗い出し、(3)さらにそのソフトウェアの製品名やバージョンを特定した後、犯罪が開始される。犯罪方法には、ID やパスワードを投入して真正な利用者のふりをする方法と、セキュリティ・ホールをついて侵入する方法の 2 つがある。

最初の 3 段階のプロセスは、真正な利用者が自己の管理下にある装置に遠隔から接続するときにも利用される手順であるから、防止も処罰もできない。その後、2 つの行為のいずれかを行うかどうかで、犯罪になるかならないかが決まる。

そもそも冷蔵庫や電子レンジをネットワークに接続するのは、それによって冷蔵庫内の在庫を確認したり、料理に適した動作条件を電子レンジにダウンロード

したりするためである。つまり、これらの機器は必要な情報をやり取りするためにネットワークに接続されているのである。IPv6では、128ビットのアドレスのうち、後半の64ビットは機器固有のアドレスとしてあらかじめ与えられることになっている。メーカーは、機器に順番にこの後半部分のアドレスを付与していく可能性が高い。ネットワーク犯罪者がネットワークに接続されている機器を拾い出すときには、このアドレス部分に注目すれば、冷蔵庫や電子レンジをあたかも群のように見つけることができるようになるだろう。また、それらの機器で動作中の通信ソフトウェアの製品名やバージョンを特定することも容易である。

正しい利用者から情報のやり取りが要求されたかを判断するために利用されるのが、IDやパスワードである。このIDやパスワードを盗むことができれば、他人の機器に接続できることになる。それができなくても、IDやパスワードを少しずつ変えてくり返し接続を試みれば、いつかは接続することができる。前述の記事には、これについての解説も出ている。それによると、繰り返しいろいろなIDやパスワードでアクセスして不正に接続しようという行為に対しては、アクセス回数がある数に達したら、強制的に接続を拒否するという仕組みが最近では組み込まれているということである。しかし、容易に想像できるIDやパスワードが用いられていれば、この方法では阻止できない。家庭内の冷蔵庫がネットワークに接続される時代がくれば、これまでよりも爆発的に利用者層が広がるので、氏名や生年月日をパスワードに利用するような安易な利用者が増えるかもしれない。

IDやパスワードを偽る方法、あるいはセキュリティ・ホールをつく方法によって接続できた瞬間に悪意のプログラムを潜り込ませて、今度はその冷蔵庫や電子レンジから他を攻撃するようにすれば、単純作業の繰り返しだけでねずみ算式に拠点の数を増やすことができる。同様に、ねらいをつけた特定のコンピュータに対して何百万台かの次世代冷蔵庫から、一斉にIDやパスワードを送れば、いつかは不正に侵入することができる。こうして類型1の犯罪が実行される。

同じ手法を用いて暗号を解読することもできる。暗号鍵を少しずつ変えて解読の計算を行い、もっともらしい平文が出たら、それをネットワーク犯罪者に報告するプログラムを潜り込ませれば、何百万台かの電子レンジが1日中解読作業を続けることになる。昨年、Certicomという暗号開発会社は、108ビットの鍵で暗号化した暗号の解読コンテストを、1万ドルの賞金を賭けて実施した。このコンテストの優勝チームには40カ国の1300人が参加し、9500台のコンピュータで分散的に解読を試みた。そして、4カ月でそれに成功したという[11]。これからは、電子レンジや冷蔵庫が同じような作業をするかもしれないのである。

2001年4月14日の朝日新聞には、興味深い記事が2つある。第1の記事は、たくさんのコンピュータが協調してひとつの目的のために動作する超分散処理のビジネス化をレポートしている[12]。一方、第2の記事はネットワークへの常時接続が進むとハッキングの危険が増すと警告している[13]。まさにブロードバンド時代の功罪を指摘する2つの記事である。しかし、ハッキングの防止策が「こまめに電源を切る」というのでは、常時接続の利点が否定されてしまうことになる。

このように犯罪者に拠点として利用される可能性のある機器は、増えこそすれ、決して減ることはない。しかも、それらがネットワークに常時接続されるということは、犯罪者には好都合である[14]。総務省は、次世代テレビでは双方向サービスの操作ソフトウェアを放送波に載せ、利用者が簡単にサービス内容を更新できるようにするという計画を持っている[15]。このテレビに対して不法なソフトウェアを送信できるならば、同様に犯罪者の意のままに動くようになるだろう。

冷蔵庫、電子レンジやテレビが不正な動作をしないようにするには、どのような対策があるのだろうか。

不正な動作を見つけたら、その機器をネットワークからはずすというのも一案ではあるが、接続される機器の数を考えれば、もぐらたたきのようでよい対策とは言えないだろう。

むしろ、インターネットから家庭への入り口にファイヤーウォールを設置して、内外を遮断するという方法が適当かもしれない。しかし、この方法でも、ファイヤーウォールに組み込まれたソフトウェアにセキュリティ・ホールがあれば、犯罪者はそこをねらうものと考えられる。

ところで、ファイヤーウォールのソフトウェアにセキュリティ・ホールのような不具合が見つかったら、ソフトウェアを修正できるようにしておくということは、よいことなのだろうか。ソフトウェアを修正できるということは、外部から悪意でソフトウェアを書き換えるということにつながる危険性があるので、それ自体が一種のセキュリティ・ホールなのではないだろうか。

冷蔵庫の通信ソフトウェアはLSIの中に埋め込んで、書き換えのできないようにするという案もある。このようにすれば、ネットワーク犯罪者が冷蔵庫を攻撃しても、電源を切ってコンテンツ(肉、魚や野菜)を腐らせることくらいが関の山なのかもしれない。しかし、全部をハードウェアにして中身を替えることができないようにするということは、技術の発展と共に利用者に定期的な買い替えを強いることである。また、前述の次世代テレビのように、ソフトウェアを書き換えることのできる機器が増えていくことも予想される。しかし、世界中の膨大な家庭にすべてファイヤーウォールを設け、不正アクセス防止法のようにシステムの管理者、すなわち世帯主にハッキングの防止処置を講じる責務を求めることは、非現実的なことであろう。

往々にしてセキュリティ・システムの設計者や、それを販売する企業は、安全性を強調する。しかし前述のCerticomと同様に、最近、イギリスでArgus Systemsという会社が自社システムへの挑戦を受け付けたが、わずか24時間で、35000ポンドの懸賞金を賭けたシステムが破られたという[16]。このような宣伝を安易に信ずるよりも、セキュリティ・システムは必ず破られるものであるということを前提として、それへの対策を考えることの方が現実的ではなかろうか。

なお、上述のようにファイヤーウォールによって家庭の内外を分離するということになれば、冷蔵庫や電子レンジにそれぞれ固有のアドレスを付与する必要は生じない。これらの機器にはプライベートにアドレスを付与し、家庭の入り口に

固有のアドレスを１つだけ付与するということで充分であるが、これはIPv6におけるアドレスの考え方を否定することにつながるものである。

以上に説明してきたように、IPv6の時代になれば、ネットワーク犯罪者が暗躍する場面が増えると予想される。そのような意味で、IPv6は脆弱なシステムであるということができるであろう。

2.2 アドホック・ネットワークの問題点

第２の危険は、アドホック型のネットワークの増加に伴う危険である。電話網は何年も時間をかけて大規模な投資を重ねて構築されてきた。しかし、現在では、利用者は、LANのようにその場にある通信資源を利用して自由自在にネットワークを構築することができる。このように自由に構築したネットワークをアドホック・ネットワークという。

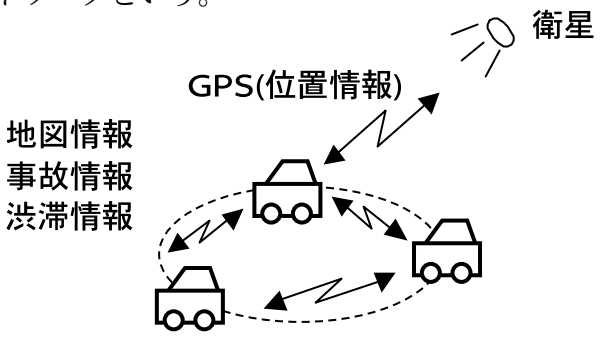

図２　自動車同士が通信するアドホック・ネットワーク

さらに図２のようにこれが展開する可能性がある。すなわち、図２では自動車が通信資源の役割を果たし、相互に通信して情報をやり取りし、地図情報を交換したり、事故を回避したりしている。このようなネットワークは、渋滞の解消にも役立つだろう。また、無線LAN同士を接続したり、移動通信端末が相互に基地局の役割を果たしたりするといった形に、アドホック・ネットワークは発展の可能性がある[17]。

アドホック・ネットワークでは端末の移動が自由で、中央からの集中管理では対応ができない。そのような状況で如何にして情報を必要なところに届け、また必要な情報を見つけるか、オープン性、汎用性、常用性、信頼性、可塑性など様々な観点から研究の課題が山積している[18]。したがって、アドホック・ネットワークは、急激に利用されるようになるとは考えられないかもしれない。しかし長期トレンドでは、中央管理形のネットワークからの移行が進む可能性がある。

繰り返しになるが、このアドホック・ネットワークでは、その瞬間に、その利用環境の中に存在する通信資源が利用される。それゆえ、ネットワーク犯罪者が居場所を刻々と変え、その場、その場でアドホック・ネットワークに参加をするようになれば、捕捉は大変にむずかしくなるだろう。

3. ネットワーク犯罪の捜査

どのようにすれば、ネットワーク犯罪が摘発できるのであろうか。普通の犯罪捜査と同様に、犯行の現場で押さえる方法と、後から犯行の痕跡をたどる方法の2つが考えられる。

3.1 通信傍受による捜査

現場を押さえるには、通信を傍受しなければならない。通信の傍受に関しては、1999年8月12日に成立し、1年後に施行された通信傍受法がある。しかし、その対象は「組織的殺人、薬物・銃器、集団密航犯罪が実行され、犯罪関連の通信が行われる場合で、他の方法では犯人の特定、犯行を明らかにすることが著しく困難であるとき」に限られている。

ここに列挙されている薬物や銃器の取引であれば、麻薬あるいはピストルといった物的な証拠から、指紋など犯人につながる情報を得ることができるかもしれない。組織的殺人や集団密航も同様である。このこともあって「他の方法では犯人の特定、犯行を明らかにすることが困難であるとき」という制限が法律の中に書き込まれ、みだりに通信が傍受されないように歯止めがかけられている。一方、ネットワーク犯罪では、すべてはネットワークの中で実行され、犯罪者は指紋などを一切残さない。物的証拠は存在せず、「他の方法では犯人の特定、犯行を明らかにすることが著しく困難である」可能性が高いのである。

また、通信傍受法の規定で立ち会いを要請される通信サービス提供者は、法律に列挙された犯罪とは無関係で、いわば善良な第三者の立場にある。一方、ネットワーク犯罪の場合には、すでに説明したように大量の通信を送り込むことなどによってネットワーク自体が停止することがあるので、通信サービス提供者は被害者の立場になる可能性がある。このような場合には被害者の同意があるということで、誘拐事件のように通信をモニタすることは可能であるという解釈もできるかもしれない。しかし、通信サービス提供者のネットワークを流れる膨大な通信をすべてモニタするとなれば、プライバシーの保護に関連して、事業者は大きな非難を浴びるであろう。

電話やファックスというように回線交換ネットワークの上で提供されるサービスの場合には、犯人と相手との間の回線は、少なくとも1回の通信の間は固定的に設定される。その回線にモニタ装置を接続すれば、容易に通信の傍受ができるし、また第三者の通信が意図に反してモニタされる確率も低い。それに対してインターネットのようなパケット系のサービスでは、1つの回線上にも同時にさまざまなパケットが流れているため、目標とする通信パケットを押さえるのが難しい。このことを別の側面から眺めれば、パケット系サービスでは、回線交換系の

サービスと異なり、ネットワーク犯罪とは無関係な第三者の通信が捜査の過程で傍受される危険性が高くなるということである。このこともあるので、ネットワーク犯罪の現場を通信傍受によって押さえる法律を、ブロードバンド時代にふさわしい形で制定する過程では、プライバシー保護との両立について議論を深め、国民の理解を得る必要があると考えられる。

3.2 通信記録による捜査

次に、後から犯行の痕跡をたどる方法について議論しよう。

犯行の痕跡は、サーバやルータなどに通信記録として保存されているはずである。通信記録には、通信文そのものと、だれが、いつ、だれに送信したかという通信に付随する情報の2種類がある。

電子メールでいえば、前者は本文、後者はヘッダ情報に相当する。前者の大きさは、文字数が少なく、また画面などにあまり工夫をしない単純なものであれば、1通について20キロバイト程度になる。一方、後者であれば数百バイトで済む。それでは、100万人の加入者を持つインターネット・サービス・プロバイダが存在し、すべての加入者が毎日10通ずつ電子メールを交換する場合、どの程度の通信記録を保存することになるか見積もってみよう。これには簡単な掛け算をするだけでよいが、本文まで保存するときには1日当たり200ギガバイト程度、ヘッダ情報だけであれば10ギガバイト以下となる。

この計算からも、前者のように通信記録として全文を保存することは技術的に困難なことがわかる。また、後者のように、通信に付随する情報だけに限定したとしても相当な情報量となるので、インターネット・サービス・プロバイダに長期間の保存を義務付けることは困難であると推測される。つまり、インターネット・サービス・プロバイダの事情を勘案すれば、犯行の痕跡は、週あるいは月の単位の間に消去されてしまう可能性が高いのである。

インターネット・サービス・プロバイダにとって、通信記録の保存は料金徴収に関係する問題である。料金徴収トラブルを避けようとするには、通信記録が保存されていなければならない。しかし、徴収が終了してしまえば、保存の必要はない。この観点からも、通信記録の保存期間は、1徴収期間程度、つまり1ケ月程度に制限されると考えるのが妥当であろう。

ところが、最近、この通信記録の保存のインセンティブが下がっているように思われる。それは、定額料金制度あるいは「つなぎ放し」の普及である。定額料金制度の下では、利用者を認証することだけが必要で、それ以上の通信記録は保存しなくても料金徴収上の問題は生じないからである。インターネット・サービス・プロバイダに対して、通信記録をマーケティングに利用してもよいといったインセンティブが与えられるのであれば別であるが、それがない限り、事業者側で通信記録を保存しようという意欲は、定額料金制度の普及と共に減退していく

ものと考えられる。

通信記録のマーケティングへの利用は、どんな種類のホームページを好んでアクセスしているかなどといった個人の嗜好情報を利用することであるので、個人のプライバシーを侵害する危険がある。

実際、アメリカではホームページを閲覧するためにアクセスしてきた利用者の情報を気づかないうちに収集するCookieと呼ばれる技術を利用していた広告会社が、プライバシー侵害で裁判にかけられるという事態が起きている。Cookieを利用すると、訪問者がそのページに何回訪れたか記録して表示する、画面の表示方法に関する訪問者の好みを記録する、掲示板やチャットで入力したユーザー名を記録しておき、次回訪問時にユーザー名の入力を省略するなどの機能が実現できる。この裁判では、District Courtで広告会社側が最近勝訴した[19]。同様に、アメリカ政府の教育、財務、エネルギー、内務、運輸の各省やNASAなど少なくとも64のサイトが提供しているホームページでも、Cookieの技術を使用して無断で利用者情報を収集していることが、最近明らかになっている[20]。

また、通信記録からネットワーク犯罪の痕跡を探す過程では、他の利用者の通信記録も検索の対象になる。このプロセスでのネットワーク犯罪に無関係な第三者のプライバシー侵害にも、留意する必要があるだろう。

なお、今後、アドホック・ネットワークの普及が進むと、通信記録は偶然その場に存在する通信資源に保存されることになってしまい、探求は困難になるものと考えられる。また家庭の入り口に置かれたサーバが通信資源となることも多いだろうが、それにどの程度の保存を義務付けるかについても、今後、議論を進めなければならないだろう。

以上に説明してきたように、犯行の現場で押さえる方法と後から犯行の痕跡をたどる方法のいずれについても、インターネット系のサービスの場合には、捜査がむずかしい。また、捜査とプライバシー保護とのバランスをどのようにとるかについても、議論を深める必要があるだろう。

4. ネットワーク犯罪への対応

－日本の場合－

政府は、官邸に置かれた高度情報通信社会推進本部の下に、情報セキュリティ対策推進会議と情報セキュリティ部会を、2000年2月および4月に、それぞれ組織した。前者は官房副長官を議長とし、各省庁の局長級で構成される会議である。後者は、民間有識者の会合として位置付けられている[21]。契機となったのは、すでに触れたように科学技術庁や総務省など政府機関のホームページ改ざんが同年1月に相次いだことである。また、同時に、内閣官房には「情報セキュリ

ティ対策推進室」が設置された。

2000年12月には、情報セキュリティ対策推進会議に対して情報セキュリティ対策推進室から「ハッカー対策等の基盤整備にかかわる行動計画(フォローアップ)」が提出された[22]。それによると、政府部内ではセキュリティに関する信頼性の高いシステムの構築、監視・緊急対処体制の整備・強化などを進めるということになっている。

このセキュリティの高い政府システム構築の一環として、警察庁、総務省および経済産業省は、不正アクセスを制御する機能に関する研究開発を実施しはじめた。国立研究所での研究、委託研究、補助事業などの形態で、表2に示すテーマが推進されている[23]。

表2　各省庁が推進する不正アクセス制御機能に関する研究開発の一覧

研究課題
インターネットアプリケーションのセキュリティ脆弱性に関する研究
情報通信危機管理基盤技術の研究開発
制御系システムにおけるセキュリティ機能共通基盤の研究開発
大規模プラントのネットワーク・セキュリティ技術開発／実証実験
大規模プラントネットワークにおける遠隔操作，遠隔保守のためのセキュア通信プロトコル
ネットワーク侵入検出システム
ネットワークセキュリティ・リスク分析システム機能の拡張に関する研究
不正アクセスの高感度検出およびグローバル警戒機構に関する研究
不正アクセス発信源追跡技術に関する研究開発

「不正アクセスの高感度検出およびグローバル警戒機構に関する研究」とは、次のようなものである。インターネット上の情報セキュリティ確保には、不正アクセスの発見と防止が重要であるが、不正の手口は日々高度化するので個別対応では限界がある。また、ネットワーク上の膨大なアクセス情報を網羅的に調査することは非現実的である上、実際に検出される情報は不正アクセスの一部分に過ぎないことが多い。さらに、不正アクセスの多くは他のサイトを踏み台として利用するため、不正防止には、その検出のみならず、アクセス経路の特定も重要である。そこで本研究では、膨大なトラフィック中の微小な異常を検出する新手法およびネットワーク地図情報と連携した広域捜査診断システムを開発し、その有効性を検証することを目的としている。1999年度までに基礎的な実施され、2000年度にはシステムのプロトタイプが試作されている[24]。

一方、「不正アクセス発信源追跡技術に関する研究開発」は、個々のネットワークに監視ツールを導入する等、不正アクセスを監視する技術、および監視情報をもとに不正アクセス発信源の追跡を可能とするような技術に関する研究開発を行い、インターネットの安全・信頼性の向上に寄与することを目的としている。1999年度より、パケット発信源追跡に関する研究開発、次世代不正アクセ

ス検知技術の研究開発、発信源追跡技術の不正利用防止技術の研究開発などが実施され、2001 年度で完了することになっている。

以上に説明したように、政府機関はネットワーク犯罪あるいはサイバーテロの危険性に気づき、それに対抗しようと動き出そうとしたところである。しかし、総じて言えば、情報セキュリティに関する政府の検討は進捗が遅いように見受けられる。また、本稿の冒頭で説明したように、企業サイドの意識はまだ低く、産官を挙げての取り組みになっていない。この間にも、ネットワーク犯罪の件数と更なる被害の危険性は増加しているというのが国内の状況である。

5. アメリカの状況と議論

この分野で、アメリカやヨーロッパではどのような活動が進んでいるのであろうか。これを知ることは、今後、わが国でとるべき道を考える上で、参考になるものと思われる。

アメリカには、コンピュータのセキュリティに関する調査研究と教育を実施する組織として、Computer Security Institute (CSI)が 1974 年に設立されている。そして、この CSI が Federal Bureau of Investigation (FBI)と共同で実施する調査の結果が、毎年 3 月に公表されている。その 2001 年版によると、2000 年 1 年間の被害総額は、およそ 3 億 7 千 8 百万ドルに達したという[25]。この額は、1999 年の総額 2 億 6 千 6 百万ドルに比べて 5 割も高い。このデータからも、ネットワーク犯罪が急増していることがわかる。

CSI と FBI の共同調査はアンケート形式で実施され、2001 年版には合計で 538 の企業、政府機関、金融機関、医療機関、大学などが回答を寄せている。その主な結果は、次の通りである。

- 大企業や政府機関に代表される 85%の回答者が、この 12 カ月の間に何らかの形でコンピュータのセキュリティを破られる被害に遭っている。
- 64%は金銭的な損失があったと報告している。
- 186 の回答者は、被害額を特定することができた。その総額は 3 億 7 千 8 百万ドルで、1999 年に 249 の回答者から申告された被害総額 2 億 6 千 6 百万ドルに比べて大きくなっている。なお、1999 年以前の 3 年間では、平均被害総額は 1 億 2 千万ドルであった。
- もっとも深刻な被害は知的財産権など秘密情報の漏洩で、34 回答者からの総額は 1 億 5 千 1 百万ドルに達している。次は、なりすましによる金銭的な被害で、21 回答者の合計は 9 千 3 百万ドルであった。
- 組織とインターネットとの接続点が攻撃されたとの回答が 70%で、内部システムへの攻撃(31%)よりも頻繁に発生していることがわかった。

・ 法執行機関の36%に対して攻撃と侵入があった。この数値は前年の25%よりも高くなっている。

同様に、インターネットを利用して社会保険番号などが盗まれてしまうことを、40%を超えるアメリカ人が警戒しているとの調査結果も発表されている。この割合は、テレフォン・ショッピングを通じての情報漏洩を警戒する割合の2倍に達し、またインターネットでは容易に被害が広がる危険性があるということも警戒されているという[26]。

アメリカでは、1998年2月、国防総省をはじめとする政府機関や企業のコンピュータシステムに対する大規模な不正アクセスが発生した。イラク危機で米軍が兵力増強を図っていた時期であったために国内外から大きな関心を呼んだという。2000年2月にはYahoo、eBay、Amazon、CNNなど電子商取引に関連するハイテク企業がインターネットを通じて攻撃され、それぞれのホームページが数時間以上、動作を停止する事態が起きた[27]。最近では、マイクロソフトのビル・ゲイツ会長のクレジットカード番号がイギリスの青年によって盗まれ、バイアグラが注文されたとのレポートもある。

このような状況を受けて、クリントン大統領の指示でCommission on National Security/21st Centuryが組織され、ネットワーク犯罪、とりわけサイバーテロにどのように対応するかが議論された。その会議の結論を、共和党の大物で前下院議長であったギングリッチによるInformation Security Magazineへの寄稿から読み取ることができる[28]。

委員会に参加をした14名全員の合意であるとして、ギングリッチは、まずサイバーテロは、実行が容易で、かつ被害は甚大となる危険性があるということを指摘している。実行が容易ということは、核兵器や化学兵器を用意するということとの比較に基づくものである。航空管制システムといった社会の基幹をなすシステムにサイバーテロ攻撃があった場合には、被害が甚大になるであろうということである。

しかし、このサイバーテロに対処しようとするには次の2つの問題があると、ギングリッチは指摘をしている。1つは、核兵器や科学兵器といった今までも危険と考えられてきた兵器による攻撃に対応することこそが必要だという思い込みが、軍関係者の中にあるということである。第2の問題は、ハイテク産業は近視眼的で、目先のビジネスを目的とした研究開発にばかり精力を注ぎ、国家の安全といった社会的な問題への配慮が欠けているということである。これらの問題を指摘した上で、ギングリッチは、サイバーテロに対抗する官民の連携が、今こそ必要であると提言をしている。

同様の意見は、ブッシュ政権の中枢からも発せられている。ライス国家安全保障担当大統領補佐官の言葉が朝日新聞に掲載されていた。それは「米国経済に活力を与え、軍事力の優位を支えている、まさにその技術がわれわれを脆弱にしている」として、「サイバーテロ防止へ政府と企業の協力を訴えるものであった」という[29]。

2人の主張に共通する官民の協力ということは、最近ハイテク問題に関連して

繰り返し唱えられているキーワードである。たとえば、Carnegie Mellon University の Peha は、Institute of Electrical and Electronics Engineers (IEEE)の機関誌で技術者と政策立案者の協力を訴えている[30]。彼は、技術者と政策立案者の間には、片方が他に類を見ない発明・発見に価値を見出すときに、他方はオリジナルではなくともできる限り多数の合意を追及するなど、基本的な思考に相違があるとした上で、国家安全保障を含めて、社会的に技術が重要性を増すこの時代にこそ、両者が協力する必要があると主張している。

Alliance for Internet Security は、そのような協力組織の 1 つである。この組織は 2000 年 2 月に結成され、主に大量のアクセスでホームページをパンクさせる Distributed Denial of Service attack、略して DDoS 攻撃に対して共同して対策を検討している。2001 年 4 月 13 日現在、会員数は 3251 を数え、インターネット・サービス・プロバイダをはじめとする企業、大学や地方公共団体がメンバーとなっている[31]。

日本経済新聞には、Internet Security Alliance というよく似た名称の機関の設立が準備されているとの報道があった[32]。アメリカ電子工業連合(Electronic Industries Alliance: EIA)と Carnegie Mellon University が協力して、コンピュータ・ウィルスの情報提供やハッカー侵入防止技術の開発・普及を手がけるということで、2001 年 4 月にサービスを開始するとのことである[33]。しかしホームページを検索する限り、この組織はまだ動き出していないようである。

以上に説明してきたように、アメリカではネットワーク犯罪やサイバーテロに対して社会的な関心が高まりつつある。政府のハイレベルから警鐘が鳴らされ、産学官の連携がスタートしたところである。

数多く存在する電気通信のサービス提供者がいっせいに通信傍受の要請に対応するためには、それについて標準を作成し、それに準拠してネットワーク設備を準備することが都合よい。後述するようにヨーロッパではこの活動が盛んであるが、アメリカでも関連法である Communications Assistance for Lawful Enforcement Act (CALEA)の下で、法的に認められた形で電子的な傍受が実行できることになり、これに関係する活動が Committee T1[34] と呼ばれる標準化団体の中で進められている。Committee T1 は、回線交換系でのネットワーク管理に関連する標準の作成を優先的に推進し、1998 年に最初の標準が制定されている。さらに現在は、パケット系での通信傍受に必要な標準の作成を目指して活動が進められている。

なお、この CALEA について、電気通信分野の業界団体である Telecommunications Industry Association は FBI に対してコメントを提出するなど、意見を取りまとめ役として働いている[35]。TIA は政府機関による通信傍受の要求と通信の秘密の保護を調和させる必要性について指摘しているのに加え、新技術、新機能、新サービスの導入が、通信傍受という理由で阻害されないようにすることが大切であるとの立場を取っている。

6. ヨーロッパにおける議論と対応

ヨーロッパではネットワーク犯罪とその捜査に必要な通信傍受の関係について、官民の間で議論が進んでいる。またこの分野に関する標準化活動も進められている。この議論と活動は、今後わが国で同様の検討を進めるにあたっても参考になる。

6.1 eEurope 計画に関わる議論

ヨーロッパも、法執行機関はネットワーク犯罪に対抗できる新しい力を持つ必要に迫られているとの認識を持っている。一方で、そのような力を不用意に与えれば、第三者の基本的な人権を侵害するかもしれず、また、インターネット・サービス・プロバイダを含む通信サービス提供者の負担も考慮しなければならないとの認識も持っている。そこで、相互に関連する様々な課題にどう取り組むべきなのかについて、欧州委員会が支援する調査研究が実施された[36]。その研究の結果は公表され、また、eEurope 計画にかかわる提案の中にも利用されている。

この研究の中には、通信記録が他国の事業者によって保存された場合に、それを法執行機関が要求できるかどうかということについての提案がある。この問題は、インターネット時代になって顕在化してきたものである。インターネットでは、国境を意識することなく他国に設置されたサーバを直接アクセスすることができる。それを悪用してネットワーク犯罪が起きた場合には、両国の法執行機関が速やかに協力して対応しなければ、犯行の証拠が消滅してしまう危険がある。そこで、他国に保存された記録であっても、法執行機関はデジタル・データのコピーを入手できるようにすべきであるという提案がでたものと考えられる。

欧州委員会で情報化社会にかかわる諸政策を担当している部局が、Information Society Director - General である。この DG が事務局となって推進しているプロジェクトが eEurope 計画である。日本でも最近 eJapan 計画が推進されつつあるが、eEurope 計画はそのヨーロッパ版ということができる。この DG から欧州評議会と欧州議会などに 2001 年 1 月に提出された文書に、情報通信インフラストラクチャのセキュリティに関するものがある[37]。この文書では、通信傍受について一節が割かれている。

この節には、まず、ヨーロッパ各国には公衆通信の傍受を執行するのに際して法的な許可を得るためのフレームワークがあり、その法執行体勢は、通信傍受は重大な犯罪の捜査などに限られるとしているという点などで、欧州法に整合していると書かれている。そして、多くの諸国の法体系では電気通信に傍受能力を装備することを電気通信サービス提供者への義務として課しており、また通信傍受に対する技術的な要求条件について統一化が図られつつあるということを紹介し

ている。さらに、1998年にオーストリアから、インターネットと衛星通信についても統一的に通信傍受の機能を用意するようにとの提案があったが、その後2回にわたる欧州議会の議論では結論が得られていないということが、脚注の形で記述されている。

次の段落には、音声通信を主な事業としていた旧来の事業者と法執行機関との間には、通信傍受をスムーズに実施するための関係がすでに出来上がっているが、通信への競争の導入と共に新たに市場に参入した通信サービス提供者との間には、いくつかの問題が起きていると書かれている。具体的な問題点は、規制のあり方、技術的な実現性、費用の負担、ビジネスへのインパクトなど多岐にわたるとして、政府と民間の間で意見を交換することが必要であると、本文書は指摘している。

また、各国は通信傍受の能力を維持していくために協調することが不可欠であるとの記述がある。「電気通信サービス提供者とインターネット・サービス・プロバイダに対して、新技術に通信傍受の能力を装備することを要求するに際しては、各国からの要求は調和すべきであると、欧州委員会は信じている。」と書かれ、その理由として「単一市場化を阻害してはならない」、「産業側のコストを最小にする」および「プライバシーを尊重する」が列挙されている。

これらの議論に基づいて、EU Forumを創設することが別の節に提案されている。このフォーラムは政府と産業界に加え、人権の保護について活動している諸団体も参加するとして、UK Internet Crime Forumが、よいモデルになるであろうと書かれている。また、このEU Forumの検討課題がいくつか示されている。それらは次のようなものである。

- 政府と産業界が24時間いつでも連絡できるように、それが適当な場合には、連絡網を作り上げること。
- もっとも適切な実施方法について検討し、それを開発するように促し、その実施方法を各国の法執行機関と産業界の間で共有すること。
- ハイテク犯罪のトレンドに関する情報を関係者の間で、とりわけ産業界と法執行機関の間で交換するように促すこと。
- 新技術の開発過程に法執行機関側の関心事項を取りいれること。
- 情報通信インフラストラクチャを破壊する出来事や脅迫を回避し、特定し、処理するために犯罪を管理し、早期に警告する仕組みをさらに開発していくように促すこと。
- 評議会や他の国際的な協調、たとえばG8の協議などについて、要求に応じて高度な技術的貢献をすること。
- 法執行機関、産業界と利用者など、関係者の間での協力関係を一層促進すること。

このようにヨーロッパでは、この問題に関するフォーラムを作って関係者が協

調するというスキームが推奨されている。

欧州委員会の文書に引用された UK Internet Crime Forum は、通信傍受に対応できないインターネット・サービス・プロバイダと法執行機関が共同して開催する、イギリス国内に組織された定期的な会合のことである。

数年前、ロンドン警察のコンピュータ犯罪部門が、インターネットからギャンブルを一掃すると宣言したことがあった。この宣言の後、インターネット・サービス・プロバイダに古い強権的な手法で接近したので対立が生まれたという。そこで Association of Chief Police Officers が介入して、インターネット・サービス・プロバイダとの対立を解くように動き、フォーラムが、1997 年に生まれたそうである。フォーラムでは法律関係者と技術者が議論をする。インターネット・サービス・プロバイダと内務省、貿易省、その他が参加をしているそうだ。

フォーラムにはサブの委員会を作り、どんなことが技術的に可能かを議論している。それまで警察は 10 ギガビットのハードディスクの内容を全部プリントアウトしたいとか、インターネット・サービス・プロバイダを通る通信をすべて記録せよとか、無理な要求をしていた。ちなみに、A4 版の用紙に日本語を 2000 文字ずつ書くとすると、10 ギガバイトを印刷するには 250 万ページが必要になり、不可能である。このような細かなことまで議論を深めた結果、「どんなことが可能か、選択をすることが必要である。どんな法律を作っても、できないことはできない。」ということが、今ではフォーラム関係者の共通認識になっているという。

ここで解説した欧州委員会の文書には、新規参入事業者との間で問題が起きていると書かれていたが、実際、それに関する報道もある。雑誌 Telepolis は「オランダでは通信傍受の準備に高い費用がかかるために、インターネット・サービス・プロバイダが破産の危機に瀕している」と報じている[38]。1998 年 12 月に施行されたオランダの通信法では、新たにインターネット・サービス・プロバイダにも通信傍受への協力の義務を課して、その実施期限が 2001 年 4 月 15 日に迫っているが、技術的また資金的な理由で実施の見通しがたっていないそうだ。

記事によると高速通信に対する European Telecommunications Standards Institute (ETSI)標準はまだ準備段階にあり、他国はその完成を待っているが、オランダはそれを待たずに法制化を急いだためにこの問題が生じたとされている。また傍受設備を準備する費用を全額インターネット・サービス・プロバイダが提供することになっていることも、問題であると業界側は指摘しているそうだ。

このオランダの問題は、各国で関係者の関心を集めているようであるが、オランダ政府が自国だけで要求仕様を書こうとしたことが問題であると、いずれの関係者も同じ感想を持っている。イギリスやドイツの政府はオランダのような事態を避けたいとの考えを持っており、ETSI の活動を待っているという。

なぜ、ヨーロッパではこのように議論が盛んなのであろうか。また後述するように ETSI における標準化活動が進められてきたのだろうか。それには、人権の保護と通信傍受という法執行との調和について、長い検討を重ねてきたことが影響していると思われる。

個人データを処理することにかかわる個人の保護と、そのようなデータの自由な移動についての欧州指令が1995年10月24日に発令されている[39]。この指令の本文第1条には、その目的が書かれている。すなわち、それらは「各国は、自然人の基本的人権と自由、とりわけ個人データの処理に関係してプライバシーの権利を保護しなければならない」ことと「このような保護を理由にして、各国は個人データが自由に流通することを制限したり、禁止したりしてはならない」ことである。また第3条には、この指令の適用範囲と共に、不適用範囲が提示されている。そしてその不適用範囲の条項には、「公共の安全、防衛、国家の安全保障にかかわるデータ処理のオペレーション」と「法令に基づく、犯罪に対する国家の活動」が明記されている。さらに第13条は「除外と制限」と題され、前述の不適用範囲がより詳細に、またもっぱら科学的、あるいは統計的な目的に使用される場合などの他の除外事項と共に再記されている。

ヨーロッパは人権保護の意識が高いといわれることが多い。それだからこそ、人権を侵害する恐れのある通信傍受が許される範囲について、しっかりとした議論がなされ、またその結果に基づいて法律類が整備されてきたように思われる。インターネット通信についてどこまでの傍受が許されるのか、改めて議論をしようということで、官民の間で議論が進んでいるように見受けられる。

なお、イギリスは人権意識が高いと信じられているが、1950年にはすでに作成されていた欧州人権宣言に署名したのは、なんと1997年のことである。その後、2000年には欧州人権宣言に整合するように、通信傍受にかかわる新しい法律として、Regulation of Investigatory Powers Act 2000が国会を通過している。

6.2 ETSIにおける標準化活動

ETSIは電気通信に関するヨーロッパ標準を作成する組織として設立された。ETSIでは、それぞれの技術分野に関わる標準の作成作業が個々の技術委員会で実施されている。そのひとつである通信セキュリティの技術委員会の下に、通信傍受の作業部会が設置されている。「ETSIは独立した非政府組織である。政府などから要求があっても、ETSIとして拒否することもできる。しかし一方で、European Free Trade Association (EFTA)は活動に対してアドバイスをする権利を持っている。欧州委員会とEFTAから15%～20%の活動資金が提供され、公共的な性格の強い活動に利用されている。また各国政府が会員となっており、政府から専門家が送られたり、政府がイニシアチブを取ったりすることもできる。これらの事情から、ETSIは会員の自発的な合意で通信傍受の標準化活動を進めることにした」と、組織化までの経緯をETSI関係者は語っている。

通信傍受作業部会の活動の目的は次の通りである。すなわち、通信傍受は、法執行機関が犯罪と戦うために重要な役割を担っており、また通信傍受は各国の法律によって実施されるという基本認識の下で、各国の、あるいは国際的な法律や

憲章に準拠した上で、経済的にも合理的な通信傍受の技術を開発することである。ETSI には他にもインターネット電話の TIPHON、第 3 世代移動通信に関する 3GPP などで、関連する標準化活動が実施されているが、通信傍受作業部会が活動の中心になっている。

このように複数のグループが通信傍受に関する標準化活動に取り組んでいることを、作業部会の Gape 委員長はツイントラック・アプローチという言葉で説明している。政治的な要請はすべて通信傍受の作業部会で対応をして、技術的な活動はそれぞれの標準化グループで実施するというのが、ツイントラックという方法である。必要なのは技術的な解決法であるが、専門家の数には限りがあるので、技術的な活動の間を調整するという役割も通信傍受の作業部会が担っているとのことである。

通信傍受作業部会では、通信傍受に関するユーザーの要求条件の定義(ETR 331)、ネットワーク機能に対する要求条件(ES 201 158)、通信傍受のためのハンドオーバー・インタフェース(ES 201 671)など、移動通信サービスやインターネット電話対応するものなども含めて、すでに 12 の標準を発行している。

作業部会では、参加者に信頼関係を形成するのに時間をかけてきた。この業務に関係しているものには秘密保持の義務がある場合があり、話せることには限りがある。そのような状況では、信頼関係と相互の理解を作ることが難しかったそうである。各国での状況を概要の形で互いに説明しあうということからスタートし、ゆっくり活動を進めたので、ES 201 671 を作るまでに 4 年がかかっている。

ES 201 671 を本当に実施することが今年の課題であると、Gape 委員長は考えている。交換機やネットワーク設備についてはアルカテル、エリクソン、シーメンスなどから準拠製品が発売されているそうである。ノーテルなどにもその計画があるようだ。通信傍受のモニタ施設についても、準拠した製品が登場した。規制機関の実施事例も出てきた。このようにして、ES 201 671 が本当に利用されていくことを、同氏は期待している。

作業部会の委員長と副委員長は、通信事業者が務めている。それは、今の時点では現実的な解決策が求められているからである。1996 年に作業部会が設置され、要求条件を明確化しはじめたときには、法執行機関から委員長が出た。今は通信網の中に設備を実際に用意することが重要なフェーズである。

なぜ ETSI が標準化活動の場として選択されたのであろうか。ETSI 自身は、会員に要請されたからであると説明しているが、他に理由はないのだろうか。そのひとつは、すでに触れたように、ヨーロッパの各国では通信傍受の機能を準備することがライセンス付与の条件になっているということである。通信事業者としては、通信傍受に関する機能を装備することが規制の範囲にあるサービスに対する免許の付与条件である。また規制されていないサービスに対しても通信傍受に関する法的な要求があるということが、この標準化活動を重視する理由である。

かつて、通信傍受といえば、国営通信事業者が必ず解決していた。それは、通信はどこかで必ず国営事業者のネットワークを通っていたからである。今はそのような事業者は存在しない。一方で、技術の変化の速度は急速なので、誰でも利

用できる標準化された解決策が求められている。通信傍受装置は特別高価であるので、世界的な市場でビジネスしてもらい、価格を下げたいという希望もあった。通信傍受の技術そのものについては、各国間の差異が少ない。通信事業者の中には、本当はすべての装置に自動的に組み込まれるようになるのが好ましいと考えているものもいる。事業者としては安いコストで、効率的で、利用可能な解決策が必要であるということである。

通信市場そのものが国際化してきたという言い方もできる。市場が国際的になり、メーカーも世界市場のために製品を作るようになって、地域としての標準化活動を起こすということになった。通信機器のメーカーはヨーロッパには少なく、国を越えて協力する必要がある。一国では、技術者の数や資金、それに時間も不足して、問題を解決することはできない。また技術が複雑化していることも要因である。昔は電話だけを考えればよかったが、今ではボイスメール、移動通信、PBX と通信傍受の対象となる技術は多様である。これらの市場を国際的に共通化することで、規模の経済の利益を得ようということである。国際化を志向するメーカーと同様な理由が、通信事業者にもある。一般的に規制は緩和され、中でもインターネット・サービス・プロバイダに対してはほとんど規制がない。世界市場の中で事業を営む通信事業者が誕生し、もはや支配的事業者など存在しないという状況になっている。このため、通信傍受機能を装備することについて特別大きな負担は誰も負う必要がない。すべての事業者が対等であるということが、ETSI での活動を支持する根拠になっている。

法執行機関も共通の解決策から利益を得ることができる。通信傍受に関する技術的なノウハウを知ることもできるし、それを合理的な費用で実施することもできる。法執行機関側からの支払が必要な国もあり、経済性は彼らにとって重要な課題である。同時に、この活動は市民の利益にもなっている。技術的にどんなことをやっているかということも、密かに盗聴されことがないということも ETSI 標準を読んで知ることができる。個人のプライバシーを最大限保護するということについて、技術的なサイドから検討して、その上で標準を作成していると、ETSI 関係者は説明している。

7. まとめと提案

インターネットの普及と共にネットワーク犯罪は急増する傾向にある。IPv6 が本格的に導入され多くの機器が直接接続されるブロードバンド時代になれば、ネットワーク犯罪の危険はますます増大する。その時代には、インフラストラクチャのひとつである通信ネットワークそのものが破壊され、それによって社会が混乱するサイバーテロの発生すら予見されている。

ところが、ネットワーク犯罪の捜査には、通信傍受あるいは通信記録の解析と

いった方法以外には、あまり有効な手法がない。麻薬取引の場合、仮に通信傍受をしなくとも、麻薬という物質そのものを押さえれば犯罪としての摘発が可能である。組織犯罪の謀議にしても、それなりの物理的な証拠を押さえることができるかもしれない。しかし、インターネットを通じた犯罪の場合には、すべてはいわば「バーチャル」に実行される。だれがコンピュータ・ウィルスを配布したのか、だれが継続してデータを奪い、あるいは破壊しているのか、通信そのものの秘密に近づかない限り摘発は困難である。しかし、通信傍受や通信記録の解析の過程では、個人の人権を侵害する危険があり、捜査としてどこまでを許すかについては、慎重な議論が必要である。

日本では、通信傍受法が成立、施行される過程で人権派から戦前の特高警察の再現を警戒して「盗聴法」との非難が浴びせられたこともあって、このような議論を進めようという意識が低い。通信傍受法の施行に不可欠な通信サービス提供者による立ち会いについてさえ、NTT ドコモは「社員の負担増」を理由に拒否したとの報道があった[40]。しかし、その間にもネットワーク犯罪やサイバーテロの危険は増し、通信サービス提供者自身が被害者となる可能性も高まっている。一方で、定額性の料金体系が導入されることなどに伴って、通信サービス提供者が通信記録を保存しようというインセンティブさえもが減退の傾向にある。

このネットワークのセキュリティの問題では、個人のプライバシー保護とネットワークのセキュリティとのバランスが議論されるべきである。社会に対するネットワーク犯罪のリスクをどこまで許容するかということと、犯罪に対抗するためにはどの程度の個人情報をだれがどのように使用することが許されるのかということの間の解決策は、意見を交わす中から見つけるしかない。いまこそ、通信サービス提供者、通信機器メーカー、人権擁護団体、法執行機関、法律家など、すべての関係者がオープンに、かつフランクに意見を交わす時期にある。何らかの大被害が発生してからでは遅すぎる。むしろ、きちんとそのことも考えて最初から処置しておくことが、ブロードバンドへの大転換時代にこそ必要である。

またこのオープンな場では、Cookie のような技術を利用して無断で利用者情報を収集することがどこまで許容されるかについても、議論をすることが望ましい。それは、このような技術がネットワーク犯罪への対抗手段になる可能性がある一方、個人のプライバシーを侵害する恐れも内包しているからである[41]。実際、アメリカとヨーロッパの間では、この問題で対立が起きている。ヨーロッパはプライバシーの保護を重視する立場であるが、それではマーケティングの可能性を奪うとアメリカは反対している。

同様に、イスラム諸国や中国で実施されているような有害なホームページへのアクセスの禁止・制限という問題についても[42]、この場で議論することができるだろう。もちろんこれらの国々のような一律の規制ということについては、わが国では賛成が得られる可能性は少ないかもしれない。しかし、児童ポルノのホームページといった個別の情報源へのアクセスについては、それを制限するのか、またできるのかということについて、関係者の間で意見が分かれる可能性があ

る。

ヨーロッパでは、このレポートでも説明したように、様々な場で産官学の英知を集めた議論が活発に行われている。合意を形成するのに時間がかかっても構わない。徹底的に議論し、出尽くしたところで解決策を実行するのだという姿勢で、すべての関係者が参加して意見を交換しているように見える。そこでは、政策的な課題、技術的な課題、あるいは通信傍受の費用負担までが議論されている。見習うべきものが多いと考える。

アメリカとヨーロッパでは、強弱の差はあるものの通信傍受に関連する標準化活動が進められている。このような活動は、説明してきたように電気通信サービス提供者にとっても、法執行機関にとっても利益が多いと考えられ、わが国でも同様に取り組むことが望ましい。

欧米からは、インターネットの国際性を反映して、この件に関する国際協調の呼びかけがはじまっている。いわゆる G8 各国の間では、ハイテク犯罪対策政府・産業界合同会合がすでに 2 回開催され、3 回目が 2001 年 5 月に東京で開催されることになっている。第 1 回の会合は 2000 年 5 月にパリで開催され、世界からはマイクロソフト、IBM や AOL など約 160 社、国内からは警察庁、外務省、法務省と、ニフティ、NTT、KDD、NEC など 16 の企業・団体が参加した。この会合では、個人の自由と私生活の保護、政府のハイテク犯罪への対策能力の向上、あらゆる関係者に対する適切な訓練、ハイテク犯罪対策に向けられた明白かつ透明性の高い枠組みなどの要素に考慮した解決策の模索が必要だとの共通認識が形成されている[43]。2000 年 10 月にはベルリンで第 2 回会合が開催され、国内からは警察庁、法務省、外務省、郵政省とインターネット・サービス・プロバイダを含む電気通信サービス提供者および情報機器メーカー関係者が参加をしている。そして、ハイテク犯罪対策に関して、犯罪者の追跡・特定、ハイテク犯罪の予防、産業界との一層の協力関係構築という 3 テーマについて、率直かつ実質的な議論を行ったとされている[44]。

しかし、この会合に対して準備するために、国内でオープンな議論が行われているとの話は聞こえてこない。むしろ、欧米の呼びかけに政府が応じ、関係業界の代表者と様子見のために出席しているだけのように見える。ブロードバンド時代には、ネットワークは国際的に接続され、ネットワーク犯罪も国際的に実行される。そのことを考えれば、この犯罪への対策にも国際協調が必要である。そうであれば、及び腰で止まることなく、国内でもすべての関係者によってオープンでフランクな議論を開始し、またこのような国際会合にはアクティブに参加することが望ましい。

山田 肇（やまだはじめ）
国際大学 GLOCOM 客員教授

注

1 「不正サクセス禁止法施行：ハッカー行為に罰則」日本経済新聞、2000 年 2 月 7 日

2 警察庁、「不正アクセス行為の発生状況」http://www.npa.go.jp/hightech/fusei_ac5/hassei.htm

3 警察庁、「平成 12 年中のハイテク犯罪検挙状況等について」http://www.npa.go.jp/hightech/arrest_repo/kenkyo_2000.htm

および「別人装うネット犯罪：摘発件数倍増 247 件」、日本経済新聞、2000 年 2 月 5 日

4 JPCERT/CC、「インシデント報告件数の推移」http://www.jpcert.or.jp/stat/reports.html

5 「科技庁、総務庁…広がるクラッカー被害」、日本経済新聞 2000 年 1 ケ月 26 日

6 「ストーカー、インターネットで増殖　長文メール続々　匿名性を悪用」、朝日新聞夕刊 2000 年 7 月 14 日

7 「教科書問題でネットに攻撃　文科省の HP 終日マヒ状態」、朝日新聞 2001 年 4 月 1 日

8 警察庁、「重要インフラにおけるサイバーテロ対策状況に関する調査結果」http://www.npa.go.jp/hightech/cyberterror/report.pdf

9 「これであなたも IT 通　サイバーテロ」、日経産業新聞 2000 年 7 月 25 日

10 半沢智、「クラッキングの手口」、No.13、p.43、日経 NETWORK (2001)

11 Certicom Press Release, "Robert Harley and Team Win &10,000 Prize in Certicom's ECC Challenge: Major Challenge Effort in Public-Key Cryptography Confirms ECC Security," http://www.certicom.com/news/00/apr1700.html

12 西崎香、「パソコン拝借新商売」、朝日新聞 2001 年 4 月 14 日

13 平子義紀、「ネット常時接続の落とし穴」、朝日新聞 2001 年 4 月 14 日

14 「インターネット　常時接続に危険性」、日経プラスワン 2000 年 4 月 29 日

15 「放送波で操作ソフト更新　次世代テレビ双方向サービス」、日本経済新聞 2001 年 4 月 11 日

16 W.Knight, " £ 35,000 hacking challenge cracked," Yahoo! Headlines (April 23, 2001) http://uk.news.yahoo.com/010423/152/bmqfd.html

17 清貞智会、山田　肇、「移動通信システムの研究開発動向」、No.1、p.10、科学技術動向 (2001)

18 間瀬憲一、中野敬介、千石正和、「次世代アドホックネットワークの動向と課題　ユニバーサル・アドホックネットワークの提案」、vol.100、no.16、(IN2000 1-7)、p.37、電子情報通信学会技術研究報告（2000）

19 C.S.Kaplan, "Legal victory for Internet advertising industry," New York Times (April 6, 2001) http://nytimes.com/2001/04/06/technology/06CYBERLAW.html

20 大牟田透、「ネット上の米政府機関サイト　閲覧者情報を無断収集」、朝日新聞夕刊 2001 年 4 月 17 日

21 http://www.kantei.go.jp/jp/it/security/taisaku/taiseizu.html

22 http://www.kantei.go.jp/jp/it/security/suisinkaigi/dai3/1215followup.html

23 警察庁、「アクセス制御機能に関する技術の研究開発の状況」http://www.npa.go.jp/hightech/fusei_ac5/access-top.htm

24 http://www.cysol.co.jp/security/security.html

25 Press Release of Computer Security Institute, "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar," http://www.gocsi.com/prelea_000321.htm

26 M.Pastore, "Cybercrime; A Worry to Americans," NewMedia (May 1, 2001)

27 Ira Sager et.al., "Cyber Crime: First Yahoo! Then eBay. The Net's vulnerability threatens e-commerce and you," Business Week Online (Feb. 21, 2000)

および「ネット経済の弱み突く：米でハッカー被害続出」、日本経済新聞 2000 年 2 月 11 日など

28 N.Gingrich, "Threats of Mass Disruption," Information Security Magazine, April (2001) http://www.infosecuritymag.com/articles/april01/columns_security_persp.shtml

29 「ことば・ワールド」、朝日新聞 2001 年 3 月 25 日

30 J.M.Peha, "Bridging the divide between technologists and policy-makers," IEEE Spectrum, March (2001)

31 http://www.truesecure.com/html/partners/alliance.shtml

32 安藤淳、「電子ウィルス、ハッカー被害　米、産学で専門機関」、日本経済新聞夕刊 2001 年 3 月 9 日

33 http://www.eia.org/communications/press_release/story.cfm?pr_key=23

34 http://www.t1.org/

35 "Public Policy Report and Agenda 1999," TIA (1999)

36 "Study on legal issues relevant to combating criminal activities perpetrated through electronic communications" Information Society Director-General (2000)

37 Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime" Information Society Director-General (2001)

38 Jelle van Buuren, "Interception requirements Get Dutch Internet Providers Into Trouble", TELEPOLIS Feb. 15 (2001)

39 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

40 「通信傍受立ち会いを拒否　NTT ドコモ　社員の負担増」、日本経済新聞夕刊 2000 年 8 月 15 日

41 M.Mosquera, "Transatlantic Privacy War Heats Up," CMP's TechWeb, (March 27, 2001) http://www.internetweek.com/story/INW20010327S0010

42 J.Lee, "Punching Holes in Internet Walls," New York Times (April 26, 2001) http://www.nytimes.com/2001/04/26/technology/26SAFE.html

43 外務省、「G8 ハイテク犯罪対策政府・産業界合同会合(概要と評価)」(2000 年) http://wwwmofa.go.jp/mofaj/gaiko/summit/ko_2000/genoa/crime.html

44 外務省、「G8 リヨングループ・ハイテク犯罪対策に関する政府・産業界合同ワークショップ(概要と評価)」(2000 年) http://wwwmofa.go.jp/mofaj/gaiko/summit/ko_2000/genoa/lyon.html