

# 情報技術と法制度(1)

「セキュリティ」「プライバシー」「サービス」を見据えて

山田 肇 (GLOCOM客員教授)

林 紘一郎 (GLOCOM特別研究員・慶應義塾大学教授)

林 この「21世紀の法制度」シリーズも4回目となりました。今回は、「技術と経済」、「技術と経営」、「技術と法律」ということを研究していらっしゃる山田肇さんにご出席いただきました。これまでの出席者の中では、名和小太郎先生が技術から入って、社会制度、あるいは法律という分野に進まれたのですが、山田さんの場合は、現時点でも技術者の立場を維持されながら、なおその他に幅広い関心をお持ちなので、楽しい対談ができるのではないかと思います。

## ネットワーク犯罪とプライバシーの保護

林 最初に、通信傍受法に関する技術的側面からのいろいろな調査を終わられたばかりということですが、ネットワーク犯罪とセキュリティのお話からお聞かせいただけますか。

山田 第2回対談で日本総研の大谷和子さんが、G8の国々から法執行機関と産業界が参加して、ネットワーク犯罪防止のために対話の機会をつくっているという話ができました。第3回の対談では弁護士の牧野二郎さんが、会社に置かれたLANの中にソフトウェアを組み込んで、そこを通過する通信をすべてモニターしている場合があるという話をされています。最近、私は、こういう通信と通信システムの安全と、個人のプライバシーという問題について関心を持っています。

ご承知の通り、ネットワーク犯罪は急増していて、アメリカで今年3月に発表された調査結果によると、昨年1年間の被害総額は3億7800万ドル(約400億円)に達しています。その金額は、1999年の2億6600万ドル、あるいは、それ以前の3年間の平均1億2000万ドルに比べても圧倒的に多い。毎年1.5倍

~2倍ずつ被害が増えているということです。日本でも同じように、サーバへの不正アクセス件数が、四半期ごとに600件を超えるくらいの割合で起きているということが調査機関に報告されています。これは報告された件数ですから、実際にはもっとたくさん起きているはずです。

私は、ネットワークにアクセスして不正行為をたたくことに対して、社会がどのようなインフラストラクチャで防衛していくのかということに関心を持っています。いま、政府はIPv6ということを通じてIT政策を推進しようとしています。IPv6になれば、冷蔵庫や電子レンジなどがすべてネットワークにつながるということがよく言われています。たとえば、スーパーマーケットに出かけた主婦がネットワークにアクセスすると、自宅の冷蔵庫にいま何が残っているのかを確認できます。あるいは、冷蔵庫の中に豚肉とキャベツがあるから、「今日は鍋回肉を作れます」と冷蔵庫が教えることも考えられます。このように、家庭の電化製品までネットワークにつなぐという話が宣伝されていますが、これが本当に幸せなことなのかどうかは分かりませんし、それを利用者が受け入れるかということも分かりません。しかし、ネットワーク犯罪者にとっては、それはとても幸せなことですね。

ネットワーク犯罪にはいろいろな種類があります。ついこの間、日本で作られた歴史教科書が歴史をきちんと記述していないと考えた中国や韓国の人たちが、文部科学省や産経新聞社のサイトにいっせいにアクセスして、サーバをパンクさせたという事件が起きています。これを犯罪と言っていいかどうかはわかりませんが、1年ほど前には、アメリカでeBayやYahooのサイトが同じような攻撃を受けています。ネットワーク犯罪者にとっては、仮に冷蔵庫や

## [プロフィール]

山田 肇(やまだ・はじめ)

1952年生まれ。1974年慶應義塾大学工学部卒業。1976年同大学大学院工学研究科修士課程修了。1984年同大学にて工学博士号取得(超伝導回路構成法に関する研究)。1990年にはMIT技術経営学修士課程を修了。1976年、旧電電公社(現NTT)に入社。1984年以降、研究戦略立案、共同研究交渉、新規事業創出などの研究開発マネジメント業務を担当。1996年よりグループ標準化戦略を担当。2000年よりGLOCOM客員教授。科学技術政策研究所客員研究官、郵政研究所客員研究官、経済産業研究所客員研究員としても活動。日本工業標準調査会電子部会、情報部会等委員、電気通信技術審議会作業計画専門委員会専門委員、電信電話技術委員会企画調査委員会委員長などを歴任。1999年ITU協会賞受賞。2000年日本規格協会標準化文献奨励賞受賞。2000年電信電話委員会感謝状。著書に『技術経営戦略』(共著、生産性出版、1999年)、『技術競争と世界標準』(NTT出版、1999年)、『世界標準の形成と戦略』(日本国際問題研究所、2001年)がある。

林 紘一郎(はやし・こういちろう)

1963年東京大学法学部卒業、同年旧電電公社(現NTT)に入社。民営化後、NTTアメリカ社長などを経て、96年退社。現在、慶應義塾大学メディア・コミュニケーション研究所教授、GLOCOM特別研究員。

電子レンジを仲間に引き込めれば、その攻撃の程度をもっと増すことができます。一人で考えて、何百万台の冷蔵庫にいっせいにどこかのサイトにアクセスせよと命令すれば、あっという間にそのサイトをパンクさせることができますし、場合によっては、そのサイトにつながっている通信網自体を停止させることができるかもしれません。

もう一つは、コンピュータウイルスをそこらじゅうに撒き散らすということですが、それも同じように、冷蔵庫や電子レンジを拠点にして実行することができます。ただそれは、冷蔵庫や電子レンジが命令に従ってくれる場合に限られます。そのためにはどうすればいいかと、まず犯罪者は考えます。通常、インターネットで行われているのは、IDとかパスワードを入れて真正な使用者かどうかを判断し、真正な使用者であればその命令に従うということです。さきほどの例で言えば、主婦がスーパーマーケットから自分の家の冷蔵庫にアクセスすれば、冷蔵庫は必ずIDやパスワードを聞いてくるはず。それが正しければつながりますね。しかし、IDやパスワードは、どのみち、0と1を単に組み合わせたただけですから、端から順番に何百万回でも何千万回でもアクセスしていけば、そのうち、真正な使用者のIDやパスワードと同じ組み合わせができてしまうかもしれません。ネットワーク犯罪者が一つ目の冷蔵庫を仲間に入れてしまえば、その冷蔵庫から次の冷蔵庫へアクセスして、また仲間にしていく。そうして、ねずみ算式に何百万台の冷蔵庫や電子レン

ジを仲間にひきずりこんだところで、たとえば一つのサイトに大量の接続要求を送るとか、あるいは不特定多数のコンピュータにウイルスを送るということをすれば、たちまちネットワークに大きな混乱を起こせます。

林 似たような話で局面は違うのですが、昨日、物流関係の団体で話をしなければならず、いったいEコマースと物流というのはどうなっているのかと、しばらく歴史をさかのぼって考えました。むかしは非常に牧歌的で、「市場」という場所に行かなければ取引できないという状況でしたが、それは不便さの度合いも高いけれども確実性の度合いも高いんですね。代金決済で、ものの引き渡しと支払が同時になされるわけですから。ところが、電子的な世界になると世界中が市場になって、どこで何が行われているかわからないという不透明性がありますし、取引の解約や確認など、費用が逆にかかるようになっていくわけ。それは、通信ネットワークも同じなのではないでしょうか。片方で便利さは増しますが、危険の度合いも高まりますね。

山田 たとえば、本人を確実に認証しようとすれば、暗号の使用ということが言われています。暗号を使うのはもちろんいいことなのでしょうが、通信の分野における暗号というのは、足し算と掛け算を組み合わせた単なる数学演算で、暗号のカギと平文をどのように計算するかという問題に過ぎないわけ

です。そのカギの長さは、たとえば60ビットとか108ビットといったある幅でしか決まっていないので、たとえばカギが108ビットであっても、端から順番に挑戦していけば解ける可能性があるわけです。

実際にカナダにあるCerticomという会社が、昨年、108ビットのカギを使用した暗号の解読コンテストを、1万ドルの賞金をかけて開催したそうです。そのコンテストの優勝チームがどのように1万ドルを獲得したかという、40ヶ国から1300人を動員して、9500台のコンピュータで分散的に解読を試みたのだそうです。ですから、賞金は、参加者一人当たり7ドルか8ドルしかもらえないというさびしい結果になってしまいました(笑)。暗号を解読できるのは本人に限られるはずでしたが、本人でなくてもこのように大量動員すれば本人のふりをすることができるわけです。さきほどの冷蔵庫や電子レンジの話に戻りますが、100万台の電子レンジが24時間、同じように暗号の解読作業をして、もっともらしい平文ができたなら、それを犯罪者のところに戻すというシステムを組めば、それも可能になってしまうかもしれません。

通信の世界では、バーチャルにビジネスが展開されると、購入者は本当に本人なのか、それとも偽者なのかという識別がどんどん難しくなってきます。電子署名といっても、それが「普通のコンピュータ、あるいはスーパーコンピュータで何年計算をしないと解読できないことになっています」という相対的な安全性しかありません。10年前のように、フェイス・トゥ・フェイスでしか買い物ができなければ、少なくとも、その人がきちんと支払いをするかどうかということは確認できますよね。

林 それは商取引の基本原則で、同時履行の抗弁といって「お金を払わなければモノをあげない。モノを渡さなければお金を払わない。だから一緒にやりなさい」ということなのです。ネットワーク社会になると、今おっしゃったような形で解き放したほうが便利なのですが、そのときには安全性の犠牲がともなうわけです。技術でそれを補えるのでしょうか。たとえば、指紋とか声紋といった身体的特徴だ

と相当確実性が高いという説がありますが、それについてはいかがでしょうか。

山田 もちろん、個人の物理的な属性に近いところを照合のカギにするということで、問題をある程度まで軽減することはできると思います。ただし、すべてそれは相対的な問題にすぎないのではないかと考えています。かたに、指紋を照合するということを行った場合、普通に考えると、まず指紋をデジタル画像として収集して、蓄積してあるデジタル画像との比較計算を行うという方法しか考えられないわけです。どんなに難しいアルゴリズムを使ったとしても、やることは基本的には同じだと思います。そうすると、二セ指紋の010100、つまりデジタル情報を与えて比較演算させると、もしかしたら認証してしまうかもしれません。

さきほどから冷蔵庫や電子レンジと繰り返し言っているのは、そこに組み込まれているプロセッサが、ほとんどの時間は実際の用途には使われないだろうからです。冷蔵庫の中の在庫を確認したり料理の手配をしたりする時間というのは、24時間のうち5分か10分程度でしょう。それ以外の23時間以上空いている、要するにひまな機械にひたすら0と1を少しずつ変えた計算をさせるのは、攻撃側としては非常に容易ですね。悪いことをしやすいわけです。

林 山田さんのような方が犯罪者側に荷担すると、大変なことになるということがわかりました(笑)。それでは、それを防ぐとすれば、どのレベルで防ぐことになりますか。

山田 通常、犯罪捜査には2つの方法しかありません。一つは現行犯逮捕、もう一つは残った証拠から分析して追跡していくという方法です。現場をおさえる方は、いまのネットワーク犯罪の場合には、まさに通信傍受に相当するわけです。どのIPアドレスからどのようなアクセスがきているかを見ていて、それが不正であれば捕まえるというわけです。実は、それとほとんど類似の技術はすでに商売になっています。それは、前回、牧野さんも言及されていまし

たCookieです。インターネットのホームページとそれを見に行った人のブラウザの間に、利用者の気づかないところで通信がなされて、利用者のID、IPアドレス、個人情報がサーバ側に移っていくというシステムです。利用者にしてみれば、次に使用する際に一から情報を入れ直さなくてもよいといった便利なことがあるのですが、それは通信の過程で個人情報知らない間に漏洩しているということとほとんど同等なことが起こっているわけです。その技術を使うと、たとえば、犯罪者のIPアドレスがわかれば、すぐにさかのぼって犯罪者を捕まえられます。Cookieのようなマーケティング技術と、この世界での通信傍受の技術はほとんど類似ではないかと思えます。

一方で、痕跡をたどるといことは非常に難しくなります。たとえば、麻薬取引であれば、電話で麻薬取引の約束をしている現場をおさえなくても、あとで薬物そのものを見つける、あるいは薬物の袋についた指紋を見つけるということで捜査ができるわけですが、ネットワーク犯罪の場合では、サーバが壊されるなどという犯罪が起きた場合、犯罪行為はすべてバーチャルな世界で行われており、物理的な証拠が残しません。そのため、痕跡をたどることが非常に困難になります。通常行われるのは通信記録をたどることです。わかりやすく言えば、電子メールを送ったときに、ヘッダ情報だけでも蓄積しておいてアクセス経路をたどることだと思うのですが、実はそれが非常に難しいことなのです。

たとえば、単純な計算ですが、加入者100万人のインターネットサービスプロバイダ(ISP)があったとします。その100万人の加入者が毎日10通ずつ電子メールを送ったとします。ヘッダ情報は100バイト程度の長さしかありませんが、全部蓄積しておくと、1日で1ギガバイトくらいになってしまいます。1ギガバイトというのは、2000字の日本語を書いたA4版25万ページに相当します。そのくらいの情報量がISPに蓄積されなければなりません。

ISPが通信記録を保存するのは料金を徴収するためです。通信記録がないと、使ったという証拠が残らないので料金を徴収できません。そこで、その

ようなすさまじい量であっても、一徴収期間、通常は1ヶ月ですが、保存しておくということになっています。ところが最近、定額料金制、要するにつなぎっぱなしが普及してきて、どんなに使っても月に3000円とか5000円ということになりました。この制度では、ISPにアクセスしてきたのが加入者本人であることが確認できれば、その人がどこにアクセスしようが何分アクセスしようがそれを記録しておく必要はないわけです。ですから、通信を記録しておこうというインセンティブがどんどん下がっていくことになります。ただ、さきほどCookieの話をしました。通信記録をマーケティングに利用することができるとすれば、ISPも少しはやる気になるかもしれません。たとえば、「林さんという人はアメリカの法律関係のサイトに頻繁にアクセスしているようだから、法律関係の新刊案内を送りましょう」といったことです。そういうことがなければ、定額料金制のもとでは通信記録を保存しておこうという気にはならないわけです。それは犯罪者にとってみると、痕跡がほとんど残らないので都合というわけです。

林 これはいま、大変な分水嶺にあるような気がします。一方で、捜査機関の捜査能力が著しく落ちているのではないかと懸念があります。国松元警視庁長官狙撃事件は歴史の転換点の象徴だったと思うのですが、警察側にそういった認識はまったくありません。当事者はなんとかかなと思っていますが、警察はほとんど無力になっているということを知民のほうがよく知っています。とくに、石原都知事はよくご存知で、「もう自衛隊を導入する以外、組織犯罪と闘えないのではないかと」というくらいの危機感を持っています。事実、ニューヨークに在住している日本人ですら、「帰国して歌舞伎町で飲んだら怖かった」と言っていました。

他方では、通信の秘密というところに縛りがかかってくると、言論の自由がいかに脅かされるかということについてアメリカ人は非常にセンシティブに議論し、裁判を起こしています。日本では、あまりそういうことを裁判で争ってはいませんが、必ずしも世間的には大問題だとは思われていません。一つ

は、ワイヤータッピング(盗聴)そのものが、日本のほうが頻度が低かったということだと思います。日本のほうが治安度が高いということもあるでしょう。また、アメリカ法では、意外にも「電話の盗聴はプライバシーの侵害ではない」という判例があって、ワトールズでしたし、かつFBIやCIAをはじめとする機関が、盗聴ができなければ自分たちの職務遂行が危うくなるということで一生懸命やってきたということがあります。しかし、こここのところを安易に崩すと、オーウェルの描いた世界<sup>1</sup>になってしまいますよね。これはどちらも正しいので、議論するしかないのだと思います。

山田 通信の秘密は守らなければならない、プライバシーを保護しなければならないというのは正しいと思います。ただ、それを守ることに熱心になっていると、これまで説明してきたように、ネットワーク犯罪者がそれを悪用して罪を犯します。なおかつ、本当に冷蔵庫や電子レンジがつながるようになれば、その犯罪の危険性もどんどん増しますね。そうして攪乱されるインフラストラクチャが社会に与える影響は、非常に大きくなっていくわけです。ですから、防御も行わなければなりません。防御しようとすると、傍受あるいは通信記録の閲覧が行われることとなります。それは、他に物理的な証拠が残らないからですが、プライバシーは侵害されますね。そういう問題について、アメリカではどのような論調があるかという、ライス国家安全保障担当大統領補佐官は、「アメリカ経済に活力を与え軍事力の優位を支えている、まさにその技術が我々を脆弱にしている」と言って、サイバーテロの防止に対して政府と企業の協力を訴えたということが、つい最近新聞に出ていました。また、クリントン大統領時代に「Commission on National Security / 21st Century」というコミッションが組織され、そこにはギングリッジ前下院議長等も参加しているようですが、そこでも同じような議論がなされているようです。ギングリッジのメモが雑誌に載っている<sup>2</sup>のですが、面白かったのは、いままで話してきたネットワーク犯罪、極端な場合はサイバーテロですが、サイバーテロは実

行が極めて容易だと言っていることです。核兵器を作ろうと思ったら非常に膨大な時間や費用がかかれますし、化学兵器を作ろうと思ったらオウム真理教事件のときのように一定の施設が必要です。しかし、サイバーテロは、その個人が通信技術に通じていれば、あっという間にできる可能性があります。そういう意味で実行が極めて容易なのですが、一方で、社会の基幹をなすコンピュータ・システムが攻撃されることにより、社会が大混乱するという危険があります。ところが、アメリカの国防関係者は、核兵器や化学兵器といった、いままで危険とされていた兵器に対する防御については一生懸命考えていて、逆に、それが大事だという思い込みがありすぎて、サイバーテロに対する防衛をしなければならないという意識が欠落しています。これに対して、ハイテク産業、まさに情報通信産業はドッグイヤーで生きていて、超近視眼的に目先のビジネスばかりを考えているので、社会の安全や国家の安全ということにはまったく配慮していません。このようなことを指摘して、ギングリッジは「サイバーテロに対する官民の協力と対応が必要」と言っています。

ヨーロッパでも、同じように議論の場を作ろうという傾向があります。産業界や政府、人権擁護団体などからいろいろな人が入って、何年かかってもいいから、どこでプライバシーの保護と犯罪の防止との妥協点を見出すかということについて、オープンに議論しています。第2回対談で大谷さんが言及されたG8の会合も、まさにその会合です。外務省が発表している正式名称は、「G8ハイテク犯罪対策・官民合同ハイレベル会合」です。今年の5月に東京で第2回会合が開催されました。こういう議論を行うことは必要だと思います。そして、技術者、法律家、社会学者、市民団体の代表というように、様々な分野の人が参加することが必要ですね。

林 なるほど。“技術と法律”というと、これまでもっとも遠い関係と考えられてきました。だいたい、法律家と話をすると「私は「技術」がわからない。林さんは会社人間だったから「技術」がわかるでしょ

うと言われます。私もほとんどわかりませんが、両者の間を採るといのはなかなか難しいですね。

山田　そうですね。アメリカの電気通信技術者協会の機関紙『IEEE Spectrum』に面白い記事が出ていました<sup>3</sup>。法律を制定する人たちは、「オリジナルでなくてもいい。むしろ、大多数の人が同意できるような案を求め、その案を作っていくプロセスを大事にして、「そのプロセスの間にいかに合意が形成されているか」を大切にしています。それに対して、技術者とか研究者は、「オリジナルでなければならぬ。結果がすべてであって、他を圧した高性能とか、初めて見る機械といったものを作ることが誇り」であるわけです。それが本当にいいものであれば世界を支配してもいいと思いがちで、プロセスより先結果を、多数より先個人というように、思考形態がまったく別であるということがその記事には書かれていました。ですから、両者の間で対話をする、まったくわけがわからなくなってしまうことが多いのです。しかし、いまだからこそ、議論しなければならないんだということが、その記事で提案されています。

林　私自身の見方は、論理性を追究するという発想法において、“法律と技術”はほとんど同じではないかと思っています。とくに、論理性を追究する学問の一つの究極が数学だとすれば、数学者は社会科学に攻め込むときに経済学に向かったのは間違いで、実は、最初は法学に向かうべきだったというのが、私自身の主張です。私は、本当は対話ができるだろうと思います。

#### 分散型社会に向けたサービス

林　話題を変えまして、いま起こっているいろいろな事象、極端なものはサイバーテロですが、そういう問題もひょっとすると、ネットワークの構成法にも非常に密接に関係があるのではないのでしょうか。昔だと、どこかに中央司令所めいたものがあって、いまはそれがまったくないというか、LANが相互につながっていて超分散、超自立型になってい

ます。これは、今後もこの方向に進むのでしょうか。

山田　私はそのように思っています。オフィスから外部に電話をする場合、中央で管理された電話網を利用せざるを得ませんが、かりにオフィスの中でLANを使用しようと思うと、ほとんど誰も管理していません。インターネットは分散処理されている、なるべく中央での管理レベルを落とすという方向でネットワークが構築されています。いま、通信技術の大勢は、その方向に向かって動いています。おそらく、通信網の規模が拡大して、中央管理することがほとんどできなくなったということが原因で、分散的なさまざまな機器、さまざまなノードが分担して、全体として調和をもって機能するという方向に動いているのではないかと思います。ただ、そうなる、さきほどから話をしているネットワークの安全を保障するための犯罪捜査等が、非常にやりにくくなります。

よくテレビドラマで、誘拐事件が起こって犯人から電話がかかってくると、犯人がどこから電話をかけているのかを調べたりしますが、あれは犯人が電話をかけている間はずっと回線がつながったままなので、追いかけることができるわけです。テレビドラマでは、ちゃんと追いかけるように「話を長くしてください」と言ったりします。一定の時間つながっていれば、必ずどこからかけている電話かが分かるわけです。ところが、インターネットのようなパケット通信だと、パケットを送った瞬間はつながっていますが、その次の瞬間には接続が切れるわけです。そうすると、どんなに長い時間パケットをやりとりしても、どこから発せられたかは分かりにくいのです。さきほどの回線交換型でつながっているものに比べると、圧倒的に分かりにくいわけです。しかも、自動車に乗って携帯でインターネットに接続している場合、基地局も時々刻々切り替わってしまい、追跡は非常に難しくなります。ネットワークが分散処理型になっていくと、ネットワーク犯罪の危険性はますます高まるのではないかと思います。おっしゃるように、ネットワークが分散処理型になっていくということは、それを許容するような社会制度、たとえば法律制度ができていくかどうかということが問題になっ

できます。技術は、たしかにその方向を指向しています。オフィスのLANであれば法律問題抜きにすぐ実現しますが、いろいろなサービスをみんなそのように整備するには、ある意味でその分野の法律を全面的に見直して、その技術の方向をサポートするようにしなければならないのではないかと思います。

林 通信と放送の融合法を検討する過程で、「融合法はこうすればいい」という提案をすると同時に、現行の法律をいかにその中に流し込んでいくか、場合によっては廃止していくことをやらなければなりませんよね。その移行プロセスをいろいろ考えたときに、最初に頭に浮かんだのは「有線電気通信法(有線法)」という有線系の基本法です。実際にどのようなケースが当てはまるかということはありませんが、たとえば、ビルの中にLANを引くときに届け出が必要なのかということを見ると、ネットワークがビルの中で終始している限り必要ないのではないかと思います。最初に廃止する法律はこれなのではないかと思ったのですが、山田さんの資料によると、実は有線法が適用されるケースがあるということですね。LANと有線法は関係があるのですか。

山田 『日経NETWORK』の記事<sup>4</sup>にあったのですが、厚木に「森の里」という住宅地があります。その住人たちで「ご近所LAN」というネットワークを作ろうと思い、そのリーダーが自分の家にOCNエコノミーの回線を引き込んで、それを数件の家に分岐させて10BASE2を共有しようというシステムを作ったそうです。そのときに、その提唱者は、これはLANを事業として営むということではないかと考え、最初は、「一般第二種電気通信事業者」の届け出が必要かどうかを調べたらしいのですが、それについては、非営利事業なので必要ないということがわかったそうです。しかしながら、ケーブルを隣の仲間の家に引く場合、他人の敷地にLANを引くということで、有線法に基づく「有線電気設備設置届」を提出する必要があることがわかり、郵政省の関東

電気通信局にアクセスして、いろいろな指導を受けて許可をもらったのだそうです。

林 これは届け出ればいいのですか。

山田 「届け出」という法律用語は極めて曖昧で、届け出て審査を受けて「受理」というハンコが押されなければ「届け出た」とはみなされません。台湾の前総統が、「ビザを申請したがまだ受けていない」と言っていたのも、受理印を押されていなかったからなんですね(笑)。厚木の彼も、不足事項や添付書類の追加を指摘してもらったりを何度か行って、正式に届け出てから1ヶ月後に、受理印が押された届け出書類のコピーが送られてきたということです。ですから、たぶん2ヶ月くらいかかっていると思います。そのようにして「ご近所LAN」を作ろうということになったのですが、今度はケーブルが道路を横切るときに、道路法に基づいた道路使用許可が必要なのだそうです。ネットワークのケーブルを空中で渡そうと思っていたら、そんなことに道路使用許可が出せるのを出せないのと市役所にさんざんいじめられて、結局、赤外線をつないだのだそうです。オフィスのLANだったらなんの許可も必要ないのに、「ご近所LAN」を作ろうと思うと、有線電気通信法、道路法に基づく申請が必要になるということです。「ご近所LAN」のようなネットワークを作るといことは、積極的に推奨されるべきことだと思うのですが。

林 CANを推進している側から言えば、当然そうですね。

山田 それが簡単にできないということは、将来に向けた新しい利用形態の発展を、法律が阻害していることになるのではないかと思います。カナダでは、光ファイバを共有するコンドミニアムファイバというものが実験的に行われています。光ファイバを何軒もの家で共有して、そこに大量の情報を流すことによって、実効的に電気事業者が要らない市民ネットワークを作ろうという実験です。かりにそ

れを日本で行おうとすると、さきほどのように有線法や道路法に基づいて許可をとらなければならないなどの、複雑な手続きが生じてくる可能性があります。しかも、光ファイバの出口に無線LANの基地局をおいて、すなわち、無線LANの基地局を1軒が1個ずつ提供して、無線LANが使えるくらいの速度で歩いている間は、無線でご近所ネットワークが使えるようにしようということも考えられます。そうすると、無線の送信機や受信機を利用していいかどうかというのは、許認可の対象になります。それを避けるためには、誰でも使えるところの2.4ギガヘルツとか、5ギガヘルツだけを使って利用するということになって、だんだん使用できる帯域が混み合ってきます。このようなことが起きてくると、繰り返すになりますが、法律がネットワークの発展、それも超分散型の、市民が共有するネットワークを作ろうという動きを阻害するのではないかと思います。

林 山田さんも技術万能主義ではないと思いますが、片方では、技術の発展は止められないという側面があると思います。そこが法律家にはなかなか理解ができないところです。この問題について、1985年の通信の自由化のときにはそこまで考えていなかったことなのですが、そのあとだんだん考え始めたのが、自由化というのは誰のための自由化かということです。利用者にとっては多様性が増えて料金さえ下がればいいんだというのが初期の発想でしたが、「そんなことは自分でもできるじゃないか」とユーザーが考え始めるようになると、「誰がやるのであれ、そこに超過利潤が潜んでいるに違いない、自分がやればもっと安い」と思う人が出てくるのは当然です。それを認めないと、本来の自由化はできないかもしれないと思うようになりました。とくに私は、電気事業審議会の委員なのですが、電力の自由化とは何だろうと考えると、大口から始めて、自分の使う電気は自分で作ってもいいという動きだと捉えると非常に理解しやすいですね。つまり電力でさえ超分散供給という形になるかもしれません。通信にいたっては、そうなるしかないと思うんですが。

山田 電力で、よく「コジェネレーション」と言われていますが、たとえば、冷暖房の熱源を製造するシステムで、同時に発電も行うということで「コ」が付いているわけです。ビルを建てました、ビルには当然冷暖房が要るので買ってきて設備をしました、これが水素ガスを燃料とするものだったり、液化天然ガスを燃料とするものだったりします。冷房や暖房を使用してみると、そのときのエネルギーで発電もできるということに当然気づき、発電もやってみようということになります。ところが、そのビルで使う電力量をすべてまかなえるのであれば何の問題も生じないのですが、常識的に考えて、あるときには足りなくてあるときには余るという状況が生まれます。そうすると、電力会社との間で「足りないときには売ってください、余ったときには買ってください」という契約を結ばなければならなくなります。そもそもなぜ「コジェネレーション・システム」を導入したのかと考えると、同じ水素ガスあるいは同じ液化天然ガスを燃やすならば、最大限効率よくそれを使って、なおかつ環境保護にも役立つようにしたいということです。コジェネレートして効率を上げるほうが当然いいわけで、それを認めざるを得ないはずなのです。日本中でコジェネレーション・システムをもったビルがどんどんできてくれば、利用者はそういうことも選べるようになります。ただ、一般家庭ではそのようなシステムを導入することができないので、これまで通り、電力会社から電気を買うことになります。それは、電気というものの購入形態が変わるということだと思います。通信も同じだと思います。

林 そうすると、最初の頃の自由化は事業者のための自由化という感じだったのですが、だんだんユーザーサイドになってくる。それがとくに環境に関係あるようなものと、環境上、そちらのほうがいいということになるのは当然のことだと思います。ここで問題になるのは、「かわいいそうなのは事業者でございます」という事象が非常に顕著になってくることです。なぜなら、通信であれ電力であれ、自前で設備を作ろうという人はたいてい大口ユーザーで、いままではその大口ユーザーからがっばり

稼がせてもらって、その分で儲からないところもやるというユニバーサルサービスのしくみになっていましたよね。それが、がっばり稼げると思っていたところが「私は自分でやります」というように逃げてしまうわけです。完全に逃げてしまうならまだいいのですが、「足りなくなったら売ってちょうだい」などという義務を課されると、事業者は踏んだり蹴ったりということになりますね。

山田 そうですね。

林 これはどのように解決すればいいのでしょうか。

山田 通信でも同じだと思います。普段ば「ご近所LAN」を使っているけれども、いざ何かが起こった場合、たとえば地震が起きたときは携帯電話を使いたいなどという場合、負担が増えてくるわけです。有名な事例ですが、NTTが光ファイバを加入者系に入れるときに、「110番」や「119番」の通信をサポートするために、電気の配線をファイバと一緒に引き回すかどうかということをご議論したことがあります。光ファイバだけであれば当然電気は流れません。電気が流れないとすると、家庭で停電が起きた場合、「110番」や「119番」にかけたくても手がなくなってしまいます。いまの銅線の電話の場合は電話局から電力を供給しているので、停電しても電話はかけられます。小松左京の『日本沈没』という小説に「つながるのは電話だけだった」という一文があると、昔、電話会社が喜んでいました。NTTが光ファイバ加入者線を敷設する際に、停電が起きて「110番」や「119番」が使えるように電気の配線も生き残らせることが、義務なのかそうでないのかということが議論されたわけです。結果的には「そんな時代ではない」ということで、電気配線をしなくてもいいということになったと思います。

いまおっしゃったようなことを延長していくと、「かわいそうな事業者」は「高費用」を強いられるのですが、ますます厳しい状況に陥ったときに、本当にそこまでサービスすることが義務なのかということ

を見直すのではないかと思います。ですから、自分のリスクでコジェネレーション・システムを導入したのであれば、「自分で使うものについては自分でまかなってください、足りないのは自分たちの責任でしょ。勝手に停電したらどうですか」ということが起きてもいいのではないのでしょうか。

林 これは難しいところです。私は、学生の就職に際して推薦状を書くことがあるのですが、「先生のおられた通信業界はいいのではないですか」と言われます。「いいとも言えないよ」と答えて、いまのような説明をするのですが、そうすると学生も考え込んでしまうわけです。だからといって、私にも智恵があるわけではありません。話題になったセキュリティの問題も似たようなところがあると思います。言論の自由、プライバシーを守るという観点からしても、ISPや事業者に期待しないと守れない。通信傍受やそういう手段で犯罪捜査に役立てようと思っても、ISPなどに期待しないと機能しません。

それから、たとえば、著作権侵害のMP3の問題も、著作権を守ってマイクロペイメントでお金をいただくとしても、ISPに機能がないとそれはできません。また、かりにそれは著作権侵害だから差し止めようとしても、ISPが言うことを聞かないと差し止められません。あらゆる問題がインタメディアリーなところに集約されていて、社会的役割が非常に高まっています。「社会的役割が非常に高まるから就職したらどうだ」と学生には言っているのですが、同時に、「先生、それって儲かるんですか」と聞かれると、どうも限りなく儲からない部分もたくさんやらなければならないのではないかとことになってしまって、資本主義社会の会社の魅力という観点からすると、就職しないほうがいいのではないかとこの矛盾が生じてしまいます。

山田 社会的な価値は高くても儲からなくてもいいという事業を営んでいるところは、中央政府や地方政府です。今後はそういう公共的な性格のものになっていくのかなと思っています。ユニバーサルサービスが本当に必要なのかという議論をしてい

る方々の中で、「よほど必要だったら、もう一度電電公社を作ればいいんだ。儲からなくても絶対に必要な仕事なら、覚悟を決めて、必要なら税金を投入してでも最低限のネットワークを設備したらどうか」ということを主張する人がいます。もしかすると、そういう方向に移っていくのかもしれませんが、超分散ネットワークになるとまったく様相が変わってきて、事業者と利用者の区別がなくなってくると思います。超分散ネットワークという方向への技術の進展と、いまのような、公共性があるから中央管理する必要があるという議論は矛盾があるので、どちらが正しいのかは分かりません。

林 学生に対する私の暫定的な回答は、「社会的機能や役割は高まるのだから、まずはそこに入りなさい。そこで数年経験を積んで、自分で事業をやると思えばそうすればいいし、そのままいつけたほうがいいと思えばそうすればいい。そうでなくても、その経験を活かして、これをやってやると思えば転職すればいい」というなんとも答えにならない答えを学生にはしています(笑)。

山田 そう答えるしかないですね。通信事業は、いまの時点では魅力的な事業ですが、本当にそれがつつくかどうかはよく分かりません。たとえば、いま、携帯電話で音楽のダウンロードができますが、1曲ダウンロードするといくらかをレコード会社に支払うのですが、そのほかに携帯電話会社にも通信料を支払います。1曲の通信料はPHSを使った場合、150円くらいだと思います。いずれそれがミュージックビデオになったとします。そうすると、ビット数という意味での情報量は約100倍です。ビット当たりの単価が同じだとすると、1曲ダウンロードするのに1万5000円かかってしまいます。たとえば学生が、「モーニング娘。」のビデオを1曲ダウンロードするのに1万5000円も支払うかということ、そんなことは絶対にあり得ないと思います。彼らの可処分所得の範囲を超えてしまいますよね。ということは、ミュージックビデオがダウンロードできるような時代になれば、ビット当たりの通信料を100分の1に落とさなければ

ならないということです。その方向にどんどん進んでいくことは間違いありませんから、何テラバイトといった情報がものすごい勢いで行き交うようなブロードバンド時代というのは、それがほとんどタダ同然の値段にせざるを得ません。

別の言い方をすると、NTTドコモが現在繁栄していますが、ドコモの総収入がいまの100倍になる時代が来るかという、それは絶対にあり得ないと思います。せいぜい2倍か3倍でしょう。そういう意味で、産業の成長は、情報量の爆発の規模に比べると圧倒的に小さい規模でしか起きないわけです。要するに、バス会社や鉄道会社と同じように、爆発的に伸びていくような産業だとは思わずに就職したほうがいいですね。給料もそれほど変わらないでしょう。

林 今回は特許についてもお話しありがとうございましたのですが、時間が足りなくなっていました。次回は、特許や知的財産権の話を中心に、名和先生を含めた鼎談を行いたいと思います。どうもありがとうございました。

1 ジョージ・オーウェルの小説『1984年』では、国中を監視するネットワークを司るビッグ・ブラザーが、国民の権利を抑圧する様子が描かれている。

2 N.Gingrich, "Threats of Mass Disruption," Information Security Magazine, April (2001) [http://www.infosecuritymag.com/articles/april01/columns\\_security\\_persp.shtml](http://www.infosecuritymag.com/articles/april01/columns_security_persp.shtml)

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

4 山田剛良、「月4000円で専用線接続 隣近所にネットワークを張る」, No.9, p.204, 『日経NETWORK』(2001)