講座 第2回

インターネット活用法

インターネットの現状を探る

上林 正巳*

UEBAYASHI Masami

Exploration of the status quo of Internet

2 Series

Utilizing the Internet

[著者抄録] 連載講座第2回として、インターネットの現状について説明する。インターネットは特定の機関が運用しているものではないという説明はよく聞かれるが、その運用体制について、接続や通信の保証はどうなっているのかを述べた。またインターネットの問題点として、ネットワークのセキュリティー問題、情報の暗号化問題、検閲問題を取り上げた。インターネットの情報発信手段としての様々な利用についても紹介する。

[著者付与キーワード] インターネット、ネットワーク、セキュリティー、IP アドレス、ドメインネーム、ftp、ファイアーウォール、情報発信、ネットワーク倫理

[Author Abstract] As the second lecture of this series, the status quo of Internet is explained. We often hear that Internet is not operated by special organizations, so concerning its operational system, the mechanism of connection and guaranty of communication is described. Also as problems of Internet, discussion is made about its security, encipherment of information, and censorship. Various using methods are introduced as an information transmitting means as well.

[Keywords by Author] Internet, network, security, IP address, domain name, ftp, Firewall. information transmission, network ethics

* 通商産業省 工業技術院 生命工学工業技術研究所
微生物機能部 特異代謝研究室 (〒305 茨城県つくば市東1丁目1番3号) Tel. 0298(54)6094
MITI, AIST, National Institute of Bioscience and Human Technology (1-3, Higashi 1-chome, Tsukuba-shi, Ibaraki-ken, 305)

1. はじめに

当講座の第1回「インターネットの概要」(Vol. 39, No. 1, p.52-62, 1996.04)でも述べられているように、インターネットは、『『ネットワークのネットワーク』』といった分かりづらい説明や、あるいは「世界最大のコンピュータ通信網」などと、ある面で不適切な紹介がなされることも目立った」とも紹介されている。

では、分かりやすい説明や適切な紹介は何なのか？と問われるが、その簡単な解答は、インターネットの広がりを見ると、実は大変困難なことであるとの思いを深める。

そこで、今回はそれを考えていくために“インターネットの現状はどうなっているのか”について簡単な説明を行い、インターネットについて部分的にも理解していただくことを目指したいと思う。

しかしながら、まず最初に、“現状のインターネットの説明”としては、その設備的な視点から応用的な視点まで、大変幅のある広がりについて説明する必要があるが、それぞれの視点についての解説は本講座の今後の各回において行われることとなるので、今回の説明はやはり概要の域を出ないことになってしまうと思われるという点をお断りしておきたい。

さて、今回は以下の5点について取上げることによって、インターネットの現状理解の一助になるとともに、本講座の今後の話を理解するための助けの一部になればと願うものである。

(1) インターネットの運用体制

インターネットは特定の組織が運用しているものではない、という説明はよく聞かれると思うが、では、その間の接続や、通信の保証はどうなっているのか？

(2) セキュリティ問題

悪質なハッカーが侵入した....という話題が、時折、新聞紙上に出る。ネットワークのセキュリティとは何なのか、コンピュータのセキュリティとは何なのか？

(3) 暗号化問題

セキュリティ問題とからめて、インターネットの上での情報の暗号化の話がある。商売の話や、決済口座番号、プライバシーに関することなど、他人に知られたくない情報をインターネットを利用して伝達する時に、暗号化が必要になってくる。

(4) 検閲問題

インターネットの上でポルノ情報を流したとのことで、警察がネットワーク提供者を家宅搜索した。以前から、アメリカ合衆国議会では、ポルノ規制が議論され、イギリス他でも青少年との関わりで問題になった。日本では、通信業者が倫理綱領を発表し、通信の秘密、検閲の禁止との関わりで論議を呼んでいる。

(5) 草の根の運動体が注目

簡易な情報発信手段として、様々な組織で、それは国段階から一市民段階に至るまで、このインターネットの上での情報発信機能に注目している従来の出版、マスメディアなどとの差はあるのか。

以上、ある面では非常に急速な動きのある部分であるため、確実な情報をお伝えできているか心配な点もあるが、ご容赦いただきたい。

2. インターネットの現状の部分的側面

2.1 インターネットの運用体制

インターネットは特定の組織が運用しているものではない、という説明はよく聞かれていると思う。しかし、では、その間の接続や、通信の保証はどうなっているのかについては簡単な説明が必要と思われる。それについて紹介をしたい。

2.1.1 インターネットの管理体制

インターネットとは、各組織が持っているコンピュータネットワークを相互接続したものである。一部、他のプロトコル(通信手順)も通すものもあるが、広域の接続性を持つためにTCP/IPプロトコルを使う。このTCP/IPプロトコルの上で様々な上位の手順が考えられ、利用されている。TCP以外にUDPなどもあるが、ここでは、詳しい通信手順の内容の説明は省略する。

ブロードキャスト，すなわち放送を行うのではなく，特定の利用者間でお互いに通信を行うためには，相手を互いに認識する必要がある。

一つのネットワークの中で電腦(コンピュータ，ワークステーション等)が繋がっているとき，お互いの電腦間での通信手順は利用者が満足できる限り，当然独自のもので構わない。インターネットが普及する以前，小規模なネットワークのための様々な通信手順が開発され，販売されていた。いまでも，計測制御分野などではしばしば使われている。

しかし，多数の電腦が繋がったネットワーク，さらにそれらネットワークが互いに接続された場合，ある場所の電腦と他国の電腦とが互いの認識を行い，相互に通信を行うためには標準となる通信手順が決まっていなければならない。そのようなネットワーク間接続まで含めて，手順として標準になっているのが，分散環境のため開発されたIPプロトコルである。“インターネットはTCP/IPで繋がったネットワークである”と言われる所以である。

IPによれば，全世界中の，互いに通信できる電腦は全て異なるアドレスを持つ。あるいは，互いに通信できるネットワークは全て異なるアドレスを持つ。これにより，互いのネットワーク間での経路制御が可能となっている。このアドレスを全世界的に管理している組織は確かに存在する。しかし，この組織は“アドレスの，重複しない割り当て”を管理しているもので，個別のネットワー

クの運営を管理しているものではないし，また，“インターネットの中心なるネットワーク”なるものの存在，あるいは管理をするものでは全くない。個別のネットワークはそれぞれのネットワーク組織が運営し，それら相互の接続によってインターネットの世界が築かれているというものである。

また，インターネットの世界では，それぞれのネットワークを運営する組織区分の，より簡易な区別のため，ドメインネームという名前割り当てが行われている。これを使用することにより，通信相手のIPアドレスを全て知る必要はなく，ドメインネームという階層化された，一般名称に近い呼称で接続先の相手の電腦を識別することが可能となる。

このドメインネームの割り当て管理も，IPアドレスの割り当て管理とともに行っている。

2. 1. 2 アドレス割り当て組織

アドレスの割り当ては図1に示すように，IANA (Internet Assigned Numbers Authority)の下に北アメリカ地域のためのInterNIC，アジア太平洋地域のためのAPNIC (Asia Pacific Network Information Center)，ヨーロッパ地域のためのRIPE NCCがそれぞれ業務を行っている。

APNICの下には日本のJPNIC，韓国のKRNIC，オーストラリアのAUNIC他があり，それぞれの地域の割り当てを行っている。

日本においてはこのJPNICがIPアドレスの割り当て及びJPドメインネームの割り当てを一

図1 アドレス割り当て組織

元的に行い、JP ドメインネームサーバの登録と運用を行っている。また、それらに伴う whois DB の運用も行っている。

JPNIC の業務に関する情報は電子メール、匿名 ftp、あるいは whois サービスや gopher、web で入手することができる。

電子メールの場合では、mail-server@nic.ad.jp 宛てに以下の本文がはいった電子メールを送ると、説明文が返送されてくるので、それに従えば各種の文書を取得することができる。

「send help」

匿名 ftp サービスの場合では、ftp コマンドで ftp.nic.ad.jp に接続し、Name 欄に anonymous と入力し、Password 欄に自分の電子メールアドレスを入力する。最初に ls-IR ファイルを get すると、/pub 以下の file 一覧が得られる (ftp://ftp.nic.ad.jp/pub/jpnic/)。

gopher サービスの場合では、gopher コマンドで gopher.nic.ad.jp に接続し、メニュー番号によって必要な情報を探す。

web の場合は数多くある解説書を参考にして (http://www.nic.ad.jp/) へ接続する。

各サービスのアドレス一覧を以下に示す。

```
mail-server: mail-server@nic.ad.jp
whois:       whois.nic.ad.jp
ftp:         ftp.nic.ad.jp
gopher:      gopher.nic.ad.jp
www:         www.nic.ad.jp
```

JPNIC Web サーバのページを図 2 に紹介する。また、JEPG / IP という JPNIC の関連団体がインターネットワークの円滑な運用のための技術的な調査検討を行っている。JEPG / IP の Web ページを図 3 に紹介する。

2. 1. 3 IP アドレス割り当ての状況

JPNIC のデータベースからみた国内の IP アドレスの割り当て状況は、クラス A が 1、クラス B が約 600、クラス C が約 7,000 となるが、これは、実際に運用されているネットワークの実体とは一致しないところがある。

.JP 下のホスト数 (推定) の推移を図 4 に示す。

.CO .JP, .OR.JP における増加が著しいことが見てとれる。

最近、IP アドレスが枯渇するという話を聞かれたかもしれない。

IP (Version 4) アドレスは 4 オクテット (32 ビット) の整数値であり、先頭ビットが 0 のものをクラス A、10 のものをクラス B、110 のものをクラス C としていたが、現在クラスレス運用が行われており、この区分は多分に古典的になった。また、先頭ビットが 1110 のものはクラス D としてマルチキャストアドレスに使われている。

ここで、概略の IP アドレスの割り当てを見ると表 1 のようになる。

これによると、B クラスが不足する恐れがあり、そのため、IP アドレス空間の効率的な運用のために先に述べたクラスレス (オクテット境界ではなくビット境界を使う) な割り当てや、可変長サブネットの使用、ファイアウォールの内部などの接続性の不要な閉じたネットワークでのプライベートアドレスの使用の推奨などが行われている。それにしても、20XX 年には IPv4 が枯渇することが予測され、128 ビットの空間を持った IPv6 が制定され、実装開発が行われている。

しかし、実は IPv4 空間の枯渇よりももっと大きな問題が現在、持ち上がっている。経路制御において、ネットワーク間を接続する経路制御機器 (ルータ) が多くの IP アドレス空間を制御テーブルに収容しきれなくなり、一部、経路制御が出来なくなっていることである。この対策としても、クラスレスな空間をブロックとしてネットワークサービスプロバイダー (NSP) に割り当て、NSP 間での経路情報を圧縮しようとする方法 (CIDR) や、NSP 間での経路制御プロトコル (BGP-4) により、経路の集成が行われるなど、懸命な努力が続けられている。

2. 1. 4 JP ドメイン割り当ての状況

ここで、JPNIC が割り当てた JP ドメインの状況を見てみよう。(ftp://ftp.nic.ad.jp/pub/jpnic-pub/stat/Allocated_Domains)

図 5 に割り当て済み JP ドメイン名数の推移を

図2 JPNIC Web サーバのページ

図3 JEPG/IP の Web ページ

図4 .JP下のホスト数の推移

表1 IPアドレスの割り当て状況

クラス	範囲	割り当て	割合
A	0 - 1 2 7	4 5	5%
B	2 8 - 1 9 1	4 4	9%
C	9 2 - 2 2 3	1 5	7%

示す。これも、世間におけるインターネットの注目度を示すように、CO.JP, OR.JPにおける増加が著しいことが見てとれる。

図6に府県別の割り当て数を示す。東京圏、大阪圏、愛知、などに集中していることが見て取れる。

2. 1.5 国内のインターネットの現状

JPNICはネットワークサービスプロバイダを正会員とし、その会費、及びIPアドレス、JPド

メインネームの割り当て手数料で運営されている。1996年4月15日現在で会員数は110会員である。会員種別に2種類あり、type A(学術系)会員が22(表2)。type B(非学術系)会員が88である(表3)。これらの会員のうち、1995年以降に入会した会員が69であり、最近のインターネットによせる期待の様子が伺われる。

日本国内のインターネット利用者は自らのネットワークを最終的にこれらのJPNIC会員ネットワークに接続しないとJPネームサーバへの登録が受けられず、事実上、インターネットの接続性が得られない。

ネットワークの相互接続も、お互い無秩序に行われている訳ではない。Mesh, TokyoNet, NIS, Netspace, GOL, WIDE, IIJ, Sinfony, NTTPC, Infoweb, SPIN その他の各社はWIDE

図5 割り当て済ドメイン名数の推移

注： GEO： 地域型ドメイン (ex xxx-hs.ward.city.jp)
.JP： 歴史的な、属性を持たないドメイン
NOZIP： データベース中で郵便番号が無いもの。
NC： 未接続
最終更新年月日 Mon Apr 15 12:39:16 JST 1996

図 6 府県別の割り当てドメイン数

が中心となった、商用インターネット相互接続実験 (NSPIXP) に参加している。多くの個別の接続点まで考えると、国内の相互接続性は一部の海外プロバイダーを除いて、ほぼ満たされている。

商用のインターネットサービスを行っている会社はすでに245社をこえていると言われる。これは、それら会社が直接 JPNIC 会員でなくても、JPNIC 会員のネットワークに接続が許可されれば、ネットワーク提供業務が可能のためである。利用者は各種条件を考慮にいれ、これら NSP を選択することができる (例えば、INTERNET Magazine 1996年5月号に NSP の調査が出ている)。

2.2 セキュリティ問題

悪質なハッカーが侵入した....という話題が、時折新聞紙上にでる。日本では重大な被害は明らかになっていないものの、全世界では、パスワードを盗む、Network Monitoring Attack や IP ア

ドレス詐称により侵入する IP Spoofing Attack など大規模な盗難、侵入事件も報告されている。ネットワーク、コンピュータのセキュリティーとはなんなのか？

インターネットの成長に伴い、利用形態が学術用から、商用の比重が多くなってきた。それにともない、“セキュリティー”が重要になってきた。セキュリティーの対象となるものは、以下のようなものである。

1) データやシステムの破壊

→ハッカーの侵入を防ぐ

2) 情報の漏洩

→通信の秘密を守る

3) 情報の改変

→ホストや個人の認証を行う

まず始めに意識する必要があるのは、セキュリティーの程度は組織によってさまざまであるということである。大学での学術研究から、企業での商取引まで、一概に同じ程度では話せない。というのも、セキュリティーと使いやすさと技術費用とが相反する部分を持つからである。それでも、ホストをきちんと管理すれば、unix のセキュリティーはけっして弱くない。CERT 勧告、CIAC 報告などを調べ、OS のパッチをあてたり、デーモンを入れ替え、セキュリティーホールを塞ぐ。Crack などによる脆弱なパスワードの検査やパスワードファイルの盗難防止、System ファイルの改竄を MD 5 などで検査、不審なアクセスの監視、通過パケットの監視等々が挙げられる。

すこし大きな組織になると、小数の管理者が前記のようなやりかたで多くの利用者の個々のホストのセキュリティーを守っていくには限界がある。最高のセキュリティーはインターネットにホストを接続しないことである、という点から、組織の内部と外部を分け、その間に通信を阻害する壁を置こうという考え方がある。昔からある考え方と思われるが、新しいところは、程度に応じて、一部の通信は許可、あるいは壁のところで代理中継をしてでき得る必要なサービスは利用できるようにしようとするものである。

表2 JPNIC 会員, 種別 A, 学術ネットワーク

つくば相互接続ネットワーク協議会
東北インターネット
中国・四国インターネット協議会
東海地域ネットワーク
国際理学ネットワーク
東北学術研究インターネット
Japan Academic Inter-university Network
WIDE インターネット
Japan Organized InterNetwork
"Because It's Time" Network in JaPan
学術情報ネットワークインターネット・バックボーン
九州地域研究ネットワーク
大阪地域大学間ネットワーク
東京地域アカデミックネットワーク
北海道地域ネットワーク協議会
日本ゲノムデータベースネットワーク
省際ネットワーク
計算機と化学・生物学の会(CBI研究会)
NTT マルチメディア通信共同利用実験プロジェクト
信州インターネット協議会ネットワーク
農林水産省研究ネットワーク
RWCネットワーク

ftp://ftp.nic.ad.jp/pub/jpnic-pub/
jpnic-members.txt より抜粋

表3 JPNIC 会員, 種別 B, 非学術系ネットワーク

IIJ インターネット	パナネット
関西ネットワーク相互接続協会	ダイイチインターネット・サービス
AT&T Jens Spin インターネットサービス	ASPインターネットサービス
InfoWeb	Netforward
PSINet	Infovalley
スターネット株式会社	トークネット
山梨地域インターネット協会	InfoRyoma
リムネット	シナプス インターネットサービス
C&Cインターネットサービス mesh	infoNia
東海地域インターネット	TINS-NET
InfoSphere	インテック インターネット
サイバーテクノロジーズインターナショナル株式会社	InfoSakyu
NIS インターネット	日本ネット研究会
東京インターネット	びわこインターネット
アヴィスネット	サンヨーインターネットサービス
次世代通信研究館	EVIN-NET
インターネットKDD	ラブネット
グローバル オンライン	ドリーム・トレイン・インターネット
CR インターネット	InfoBears
NETSPACE	GlobalVision
Inforyukyu	Infoaomori
アーキテック・アンド・アーツ	株式会社 日本テレネット
Sinfony	Global Sprint Japan
日産インターネット	SWANet
高速情報通信システム株式会社	株式会社 サンフィールド・インターネット
株式会社ベッコアメ・インターネット	Hypernet
InterVia	まいどWeb
IBMNET	インターネット ソリューション ファクトリー ネットワーク
株式会社スリーウェブ	マウント富士インターネット
ASAHIネット	テクノウエーブ
U-net インターネットサービス SURF	株式会社スペースプライ
三菱電機情報ネットワーク株式会社	シーネット
PIC(ピー・アイ・シー)	やまびこインターネットサービス
株式会社アーバンエコロジー	ASKnet
FastNet Internet Exchange	Flowering net
SPRITE	LEEnet
パールネットサービス株式会社	ダイナネットサービスアジア
InfoSnow	丸紅インターネットサービス ファミール
MAJIC	インターゲイト株式会社
ITJITネット	株式会社セトプリント
KAGAWA-NET	もみじインターネット
PTOP	(株)インターリンク
富山インターネット協議会	フォーチュン
MediaWeb	
NIJI-NET	

<ftp://ftp.nic.ad.jp/pub/jpnica-jpnica-members.txt> より抜粋

firewallは特定のプロトコルのみの禁止や許可を行う packet filtering や、transport relay, IP forwarding を禁止して proxy server を動かす、application gateway を動かす、などの各種の技術の組合わせで実現できるが、新参の企業がインターネット接続を企画するときの要望が強いため、パッケージとして商品化されたものも多くなった。

WWW の大成功により、http を通す proxy server (CERN httpd, DeleGate など) の実装が増大した。しかし、WWW を商用利用しようとする動きに対しては、オンラインショッピングの決済や情報提供サービスユーザの契約など、電子署名、認証、暗号化など別の側面をもつセキュリティ技術が必要となってくる。

2.3 暗号化問題

セキュリティ問題とからめて、インターネットの上での情報の暗号化の話がある。商売の話や、決済口座番号、プライバシーに関することなど他人に知られたくない情報をインターネットを利用して伝達する時にデータや認証の暗号化が必要になってくる。すでにインターネット上では多くの企業が、モノやサービスを販売し、クレジットカードによる決済を行っているが、こうしたサイバershoppのサイトは、これら暗号技術によってカード情報を保護している。

歴史的な話になってしまうが、1977年にアメリカ連邦政府は IBM 社が開発した DES (Data Encryption Standard) を標準として認めた。

DES は対称鍵暗号 (共有鍵暗号、秘密鍵暗号とも呼ばれる、暗号化と復号化に同じ鍵を用いる) であり、鍵の長さは64ビットであり、そのうち8ビットはエラー訂正用のチェックビットなので、実際の長さは56ビットである。

暗号解読技術は鍵の長さに関係し、現在ではこの56ビットの長さでは充分でないと考えられている。また、暗号化技術が汎用に使われだしたため、アメリカ連邦政府は暗号に関するプロジェクト (Capstone 計画) を開始した。その中で、連邦政

府は国家の安全保障や犯罪捜査のために、暗号鍵を第3者機関が預り、必要な時には裁判所の許可をえて暗号鍵を取りだし、暗号を復号出来る計画を選択した。Capstone 計画は以下の四つの要素からできている。

- 1) 暗号標準である EES
(Escrowed Encryption Standard)
- 2) 電子署名標準である DSS
(Digital Signature Standard)
- 3) メッセージのダイジェスト化標準である
SHS (Secure Hash Standard)
- 4) 暗号鍵の配送方式

EES は SKIPJACK アルゴリズムを採用している。このアルゴリズムを組み込んだ80ビットの鍵の長さのものが、クリッパーチップとして電話やFAX用に開発され、電脳用には PCMCIA カードに組込んだ Fortezza カードが開発された。アメリカ国防総省は今後、Fortezza カードを利用しようと考えている。また、これが ANSI (American National Standard Institute) の金融機関向け標準になる可能性もある。

このチップの復号化の鍵は、分割されて政府に寄託される仕組みになっている。この寄託方式に対しては反対が強く、インターネットの上で5万人以上の反対署名がよせられた。

DSS は電子署名用規格案として発表されたが、事実上の標準となっている RSA 暗号システム (後述) を採用しなかったので、安全性を疑問視する意見もある。電子署名 (相手が本人である認証と、内容が改竄されていない保証) は一般的に公開鍵暗号方式が用いられる。

これは、本人しか知らない秘密鍵と誰でもが入手可能な公開鍵の二つの鍵を持ち片方の鍵で暗号化したものはもう一方の鍵でないと復号出来ないというものである。すなわち、本人 (A) が秘密鍵で暗号化して送った署名が、A の公開鍵で復号できたら、これは A 本人から送られたものであることが確認でき、また、内容の改竄防止にはハッシュ関数を用いて通信文のダイジェストを作り、それを電子署名に利用する仕組が時間短縮のため

に考えられた。

SHS は DSS を用いた電子署名のためのハッシュ関数であり、160ビット長のダイジェストを生成する。今、一般的に用いられている MD-5 ハッシュ関数は128ビット長であるので、それよりもより確実である。

アメリカ連邦政府は暗号化技術を高度な軍事技術として、その輸出に規制を行っている。従来40ビットを超える暗号技術製品の輸出はできなかったが、1995年に復号化の鍵を第三者に寄託すれば64ビット長まで許可されるように緩和された。しかし、64ビット長の暗号鍵は不十分であり、アメリカ国外においても高度な暗号技術製品は開発されており、この輸出規制が合衆国製品の海外競争力を落としているとの声が出て、暗号技術製品の輸出規制緩和法案が提出されている。

民間においては、1977年に発表された RSA 公開鍵暗号方式が有名である。すでに長く研究されており、秘密鍵の管理さえきちんに行えば、現存する暗号技術のなかでもっとも安全と思われる、広く利用されていて事実上の標準となっている。最近までは、DES に比べて、処理に100倍から1万倍の時間がかかるため利用者が現れなかったが、現在ではパーソナルコンピュータでも利用ができるようになったため、実用化された。

本文は DES や IDES などの対称鍵方式で暗号化し、そのセッションキーを RSA で暗号化する方式 (RSA Digital Envelope) がある。PEM (Privacy Enhanced Mail) や PGP (Pretty Good Privacy) でもこの方式をとっている。RSA はアップル社の System 7 Pro をはじめ Netware, Notes やインターネット上で利用されている暗号システムのほとんどに使われている。RSA 暗号システムは RSA 社が特許を持っている。

PGP はヨーロッパで特許が取られている IDEA (International Data Encryption System) と RSA を組み合わせたソフトウェアであり、発明者 Zimmermann がアメリカ政府の輸出規制違反で調べられていたことでも有名である。PGP は商用バージョンは ViaCrypt 社から提供され、個

人ユーザのための無料バージョンもある。バージョン2.6以降のものは「アメリカ合衆国外でダウンロードすることが禁止されている」という断りがついている。

暗号方式をとったとしても、電子商取引を行う場合、本人であるかどうかの認証はなんらかの第三者機関が行うことになる。日本でも、Internet 認証協議会 (通産省) で検討を開始しているが、アメリカ合衆国の RSA 社の子会社、ベリサイン社が RSA を使った CA (Certificate Authority) センターを運営している。その日本法人 (日本ベリサイン社) が4月から運営を始める。Netscape Navigator には、CA センターとの自動認証確認機能が組込まれている。日本でも本格的な電子商取引市場が発展することになりそうだ。

2.4 検閲問題

インターネットの上でポルノ情報を流したとのことで、警察がネットワーク提供者を家宅捜索した。以前から、アメリカ合衆国議会で、ポルノ規制が議論され、イギリス、他でも青少年との関わりで問題になった。日本では、通信業者が倫理綱領を発表し、通信の秘密、検閲の禁止との関わりで論議を呼んでいる。

1996年1月31日、警視庁保安課は NSP ベッコウアメと会員の自宅を、猥褻図画公然陳列容疑で家宅捜索した。

2月1日、ベッコウアメ、アサヒネットが家宅捜索についての見解を出し、会員の情報に対して規制を始めた。

2月8日、アメリカ合衆国で「1996年通信法」が成立した。この法律の中で「暴力、猥褻情報の規制」があり、その中で、インターネットを含むコンピュータ・ネットワーク上で猥褻な情報を流した者は最高2年の懲役と最高10万ドルの罰金が課せられるという項目が盛り込まれている。

2月16日、電子ネットワーク協議会が「電子ネットワーク運営における倫理綱領」(以下倫理綱領)を発表した。

この規制の動きに対して、アメリカ合衆国では、

ヤフー社、ネットスケープ社やEFFをはじめメジャーな企業を含め、数多くのWWWホームページが抗議の意志を表し、ACLU (The American Civil Liberties Union), CIEC (the Citizens Internet Empowerment Coalition)(アメリカ図書館協会、アメリカ・オンライン、CDT)などが、合衆国憲法修正第1条に違反するとして、この規制の差し止め命令を要求して提訴した。また、2名の上院議員がこの規制を無効とするための法案を提出した。

ACLUの裁判のなかで、政府側弁護人はCDAの妊娠中絶について議論することの言論規制は違憲であることを認め、司法省は、この規定は言論の自由を保証する憲法に反しているため実際に適用することはないだろうとの見解を大統領に伝えたと言われる。2月16日、裁判所はこの規制の実施の一時差し止め命令を認め、政府弁護人は判決まで「捜査や起訴」に着手しないと合意した。

国内では、3月8日、倫理綱領に対して200名近くの抗議声明が行われた(図7 http://www.toyama-u.ac.jp/~ogura/another_world/censor/netrin1.html)。それに対する通産省、電子ネットワーク協議会の見解も出された(図8 <http://www.miti.go.jp/c60216a1.html>)。

アセアンの情報関係閣僚が、インターネットの規制を強化する組織をつくることに合意したというロイター電もある。規制の内容は猥褻だけでなく、人権問題や環境問題他、社会不安を煽る情報を規制する可能性もあるとのことだ。

裁判に提訴した人達によれば、インターネット上での情報を無線電波でのテレビジョンと同じ意識で規制するのは、全くまちがっている。テレビジョンは全く受動的だが、インターネットは能動的に情報にアクセスする必要がある。アクセス制限は家庭で行えばよく、そのようなソフトウェアの開発も行われた。猥褻の定義が恣意的で、NSPの自主規制で多くの医学情報や、大統領の紹介でさえ、猥褻ブラックリストに載ってしまったと述べている。

2.5 草の根の運動体が注目

簡易な情報発信手段として、様々な組織、それは国段階から一市民段階に至るまで、このインターネットの上での情報発信機能に注目しています。従来の出版、マスメディアなどとの差はあるのか。

インターネットの利用は学術的利用が先行していた。例えばGenomeNet(図9 <http://www.genome.ad.jp/>)などでは生物系のデータベース検索はじめ、生物学の研究に役立つ情報が集められている。

また、がん情報サービス(図10 <http://wwwinfo.ncc.go.jp/0sj/indexj.html>)などでは国立ガンセンターの紹介とガンの情報サービスが集められている。

また、インターネットワークの世界的な広域性を利用して、国際的な化学物質の安全性に関するデータベースの協調運用なども行われている(図11 <http://www.nihs.go.jp/GINC/>)。

さらに最近では、政府機関もインターネットの効用を認め、宣伝広報活動に使用している(図12 <http://www.sphere.ad.jp/infomofa/gmtxt/gmtxt.htm>)。

このように、急速に注目を浴びているインターネットであるが、これに特に期待をよせているのが、個人単位で情報発信をしようとしている人々である。

従来、新聞等のマスメディアに対して意見広告のような形で主張を載せていた人々がいた。新聞は多くの読者がいることは確かだが、広告掲載資金の手当は大変なことだったに違いない。ラジオ、テレビジョンへの広告などは、もっと困難だったと思える。一部の人達はいわゆるパソコン通信上でフォーラムを開設し意見を述べていた。

しかし、インターネットの上でWWWのホームページを開設できるようになった今日、その表現力と利用の広がりを利用しようという動きが出てきた。出版という形をとってきたいわゆるミニコミ誌を十分、吸収できる表現力を持っている。日本では、このような利用は緒についたところだ

2.

∞
 $\times$

図 9

図 10

図11

図12

図14

図13

が、合衆国ではこの分野はすでに大きな世界を形成している。日本でも、現在、この分野を形成しようとする動きが見られる。

一方、合衆国国防省では、この分野を諜報活動の対象と見、世論操作の対象とする報告書を出している。

新しいメディアは期待されている。

3. さ い ご に

本紙の読者には図書情報関係の人が多いと伺った。以下のインターネットのWWWページを挙

げて、終わりにしたい。

本屋に溢れている「インターネット紹介」に、あまり紹介されない現状に対して、少しでも理解していただき、今後の連載を読んでいただければ幸いである。

「富山図書館」(図13 http://www.toyama-u.ac.jp/~ogura/another_world/toyakin/lib/lib-intro.html)

「インターネットでの図書館一覧」(図14http://www.soc.titech.ac.jp/other/libra_default.html)

参 考 文 献

- 1) IP Meeting'95 予稿集, JEPG/IP, 1995. 11. 29
 - 2) JPNIC ニュースレター, 第5号, 日本ネットワークインフォメーションセンター, 1996. 03. 31
 - 3) セキュリティー技術の最新動向, Internet Magazine 1996年5月号, (株)インプレス
 - 4) maegawa's report, <199602202119.QAA05408@mail1.panix.com>, MAEGAWA Toru
 - 5) maegawa's report, <199602290227.VAA00784@mail1.panix.com>, MAEGAWA Toru
 - 6) maegawa's report, <199603202136.QAA16871@mail1.panix.com>, MAEGAWA Toru
 - 7) maegawa's report, <199603202137.QAA16936@mail1.panix.com>, MAEGAWA Toru
 - 8) インターネットの利用と仕組み, Unix Magazine 1994年8月号, (株)アスキー
 - 9) 連載「ころばぬ先のセキュリティー」, Unix Magazine 1995年7月号-1996年1月号, (株)アスキー
- 他, 多くのサイバースペースを参照させていただいた。