# インターネット・ガバナンス
## 国際的動向とその背景

木全紀元

CONTENTS



要約

1　インターネット制度の改革を目指したインターネット・ガバナンス（統治）の議論が、2005年ごろ、世界情報社会サミット（WSIS）を発端に盛り上がった。インターネットの制度管理における米国一国支配の打破が問題意識であったが、現実にはこれに代わる管理体制を見出すことができずに、国際的議論は2009年秋でほぼ終息した。しかし、議論自体が米国にとっては国際的圧力として機能し、結果としてドメインネーム・システム（DNS）の運営の透明化・公正化に寄与した。ただ、IP（インターネットプロトコル）アドレス関連制度（IANA機能）については、米国政府支配の究極的な実態に変更はなかった。

2　現在のインターネット・ガバナンスの最重要事項は安全性の確保であり、これはインターネットの本質構造がもたらす不可避の問題である。

3　インターネット・ガバナンスは多面的に確保される必要があるが、IP網部分に関していえば、インターネット・サービス・プロバイダー（ISP）の影響力の大きさに対して規制の網が弱く、ガバナンスの視点での議論が不十分と思われる。さらに、グーグルなどのコンテンツ事業者に優位というIP網の構造変化に対応した政策形成も必要である。

4　今後のインターネットの影響の広がりを考慮し、インターネットを中心にすえた総合的な情報法制も必要であろう。

# Ⅰ インターネットの重要性

## 1 永続的な課題としてのインターネット・ガバナンス

インターネットは、それなしでは生活ができないほど不可欠の存在となっている。インターネットが商用化された1990年から、たった20年で世界の構造を根本から変えてしまった事態は、まさに革命と呼ぶにふさわしい。しかしこのインフラは、従来のインフラが政府の明確な規制のもとに置かれていたのと比較すると、誰が管理しているのか、一見明確でない不思議な存在でもある。

また、インターネットへの社会の依存度は増大しているのに、他のインフラと異なり、安全性リスクが常に付随する。インターネットの安全性を脅かす事件は途絶えることなく発生している。

インターネットを政府間国際機関の管理下に置こうとする動きは、2003年、国連の世界情報社会サミット（WSIS）を契機に始まった。2005年の第２回WSIS会合前後は、この議論が世界で沸騰していたが、その後、次第に関心が薄れ、この動きは2009年秋にひっそりと収束してしまった。しかし、インターネットの本質に根ざすリスクは存在し続けている。

インターネット・ガバナンス（統治）は永続的な課題である。本稿では国際的な動きを振り返ると同時に、現在のインターネットが直面しているさまざまな課題を展望する。

## 2 OECD報告

2008年６月、OECD（経済協力開発機構）の閣僚会合で「インターネット経済の将来への政策」が発表された。OECDは先進民主主義国家が直面する課題について討議する国際機関であり、インターネットに関しても、その草創期から数々の調査・提言を行ってきた。最近でも、クラウドコンピューティング時代に重要な意味を持つ「個人情報の越境データ流通に関するガイドライン」（2008年）という報告書を作成している。このOECD報告は、１年後の2009年10月、在日米国商工会議所の「インターネット・エコノミーの実現を日本で」[注1]と題する報告につながり、日米経済関係にも影響を及ぼしている。

OECD報告でまず目につくのは、これからの経済を「インターネット経済」と喝破したことである。経済活動は取引関係の集合である。「取引コストが市場経済と組織経済の分水嶺となる」として、ロナルド・コース氏やオリバー・イートン・ウィリアムソン氏はノーベル経済学賞を受賞したが、インターネットは、その取引コストを大幅に削減する画期的技術であり、経済全般、そして社会生活全体を変革する技術なのである。

OECD報告は次のように述べている。

- インターネットはコミュニケーション・革新・生産性向上・経済成長のための、オープンで分散したプラットフォーム（基盤）である
- 経済はインターネット経済化しつつある
- 電子政府・ｅ教育・ｅヘルスなどの分野でのインターネット利用は、経済効率の改善に不可欠である
- インターネットは、地球環境・気候変動・消費者支援・創造性と革新などの課題解決に有用である
- 貿易・税政策・社会政策・規制改革など

の政策策定に当たって、インターネットが系統的に組み込まれる必要がある

その一方でOECD報告は、インターネットの信頼性確保がインターネット経済の実現における重大な課題であると指摘している。そして具体的な信頼性確保の課題として、①システムとネットワークの安全性確保、マルウェア（悪意あるソフトウェア）排除、ID（認証番号）保護、②違法・有害情報排除、プライバシー保護、消費者保護、③IP（インターネットプロトコル）網の機能に依存する電力・水道などの重要情報インフラ（CII）の保護――を挙げている。

また、インターネットの信頼性確保のためには、政府・民間・市民部門が協調して対処する必要があり、 特にリスクと保護手段の周知を含む安全文化の発展が重要としている。さらに、インターネットのグローバル展開に応じて、法執行機関の活動も国境を越える必要があると指摘している。

信頼性確保とは、インターネットにガバナンスを効かせるということであり、言い換えれば、OECDも現行のインターネット・ガバナンスにはなんらかの欠陥があり、改善が必要であると認めていることになる。

## Ⅱ インターネットの原理と歴史

そもそもインターネットとは何か。本章では、その基本を振り返る。

### 1 インターネットの仕組み

インターネットは、複数のコンピュータ（イーサネット網）間通信を目的に開発された。それは、物理的な電気通信網（アクセス回線、バックボーン回線）の存在を前提に、その上に構築された一義的なIPアドレス体系を持つ論理的な回線網である。

具体的な通信は、アドレス・ヘッダーを持ったパケット情報を、IPプロトコルに従いルーターが目的のコンピュータに伝送することによって行われる。

この過程は、①パケットの目的アドレスを、ルーターがDNS（ドメインネーム・システム）サーバーと交信して調査、②目的アドレスに近い次のルーターにパケットを送出――の２段階に分かれている。

DNSサーバーはネットワーク上に多数あるが、すべてのアドレスを把握しているものは「ルートサーバー」と呼ばれ、世界に13ある。その１つは日本にもあり、「Mサーバー」と呼ばれる。IPアドレス自体は数字の羅列であるため、日常のアドレスにはニックネームに相当するドメインネームが利用される。DNSサーバーはドメインネームを数字のIPアドレスに変換するサーバーなのである。インターネット網に固有の物理的ハードウェアとしては、ルーターとそのアドレス変換のためのDNSサーバーがあるのみである。

電気通信サービスとは別にインターネット接続サービスを提供する事業者は、ISP（インターネット・サービス・プロバイダー）と呼ばれる。１つのISPが管理する網は、AS（Autonomous System：自律システム、統一したルーティングポリシー配下にあるIP網やルーターの集合）と呼ばれ、IPアドレスと同様の形でAS番号が割り振られる。AS番号は、場合によっては大規模データセンターなどにも割り当てられることがある。インターネットとは、実際にはASが相互接続した形

態であり、AS同士の間の接続規格はBGP（Border Gateway Protocol）と呼ばれる。

IPアドレスやAS番号の管理事務は、IANA（Internet Assigned Numbers Authority）機能と呼ばれ、ICANN（The Internet Corporation for Assigned Names and Numbers）という米国の非営利民間法人が、米国政府との委任契約に従って分配している。IPアドレスの分配は具体的には、

- ICANN
  ↓
- RIR（Regional Internet Registry：地域登録機関、アジアの場合はAPNIC〈Asia Pacific Network Information Centre〉）
  ↓
- LIR（Local Internet Registry、日本の場合は、JPNIC〈日本ネットワークインフォメーションセンター〉）
  ↓
- ISP
  ↓
- エンドユーザー

――の順で、申請により国際的に配布される。

なお、現在の最大の技術課題はIPv6（IPバージョン６）の導入である。NAT（ネットワークアドレス変換）技術によりIPアドレス不足は緩和されたものの、2011年ごろより枯渇する可能性があることから、IPv4（IPバージョン４）からIPv6への転換が計画されている。IPv6では、アドレス数がIPv4の43億から340澗（ゼロが36）に増加する。

## 2　インターネットの階層構造

インターネットは「コンテンツ・データ層」「プラットフォーム・アプリケーション層」「IP網」「物理回線層」という階層構造を取っている。機能的にもモジュール化されており、運営者も別で、これがインターネットの柔軟性の元となっている。

各階層構成の要素・キーワードなどは以下のとおりである。

- **コンテンツ・データ層**

電子商取引（通販、旅行、証券）、電子書籍、音楽配信、ゲーム、CG（コンピュータグラフィックス）、動画共有、マッシュアップ（インターネット上に公開されているソフトウェアなどを組み合わせて新しいサービスを提供すること）、アフィリエイト（成功報酬型広告）

- **プラットフォーム・アプリケーション層**

電子メール、Web（WWW：World Wide Web）、IP電話、IPTV、GPS（全地球測位システム）、検索、ポータル、ブログ、SNS（ソーシャル・ネットワーキング・サービス）、クラウドコンピューティング、マーケットプレース、オープンID

- **IP網**

TCP/IP（Transmission Control Protocol/Internet Protocol）、UDP（User Datagram Protocol）、DNS、IPv6、LAN（Local Area Network）、ルーター、IX（インターネットエクスチェンジ）、CDN（Contents Delivery Network）、ISP

- **物理回線層**

LAN物理網、アクセス回線、バックボーン回線、ブロードバンド、通信事業者

## 3　インターネットのアーキテクチャー

インターネットのアーキテクチャー（設計思想）は、どのようなコンピュータネットワークでも接続を可能とするオープンアーキテ

クチャーである。これは、物理回線層、接続・伝送（インターネット）機能、アプリケーションを明確に分離する設計思想により実現された。IP網を、コンピュータパワーを遠隔地に伝達するための「土管」としての論理（logic）インフラとして設計し、パワーの中身を一切問わないこととしたのである。つまり、インテリジェンス（付加価値）はネットワーク上にはなく、端末側に存在する。

IP網は、パケットデータをアドレスに転送するだけの機能に特化して、与えられたデータを忠実に目的地まで伝えるだけで、パケットの中身を見ず、送出順序も変更せず、ただひたすら転送に専念する。この設計思想は、端末だけが中身を考慮するという意味で、「END - END原則」と呼ばれることもある。

通信とコンピュータが融合した情報通信の歴史は、通信側とコンピュータ側のネットワーク上のインテリジェンスの争奪の歴史とも見ることができる。通信側は単なる土管にならないよう努力し、過去には付加価値通信網（VAN）などというものもあった。NTTドコモの「ｉモード」なども通信側のインテリジェンスの取り込み努力と見られる。こういう観点から見るとインターネットは、コンピュータ側の論理を貫徹した設計思想によっていると考えられよう。

## 4　IP網の技術基準

IP網の技術基準を決定しているのが、ICANNのIETF（Internet Engineering Task Force）およびIESG（Internet Engineering Steering Group）という組織である。技術基準は、両者が正規の規格として発表したRFC（Request for Comments）という文書形式でまとめられる。

従来の電気通信網と比較したとき、IP網の特徴的な技術基準は、RFCに認められる条件がゆるいということである。その条件とは、①提案した規格に関し、異なったコードベースで２つの独立した相互運用可能なアプリケーションが存在すること、②RFC上のライセンスは義務として、無料・無制限・無差別に提供すること――である。

従来のITU（国際電気通信連合）およびISO（国際標準化機構）の技術基準は、事前の厳格な合意という形で形成されるのに対し、RFCモデルは提案者による現実適用から入る点が決定的に異なる。

電気通信のような物理網では、細部に至るまで事前に合意しなくては設置活動に入れない。これに対してインターネットは論理網なので、事後に不都合が発覚しても論理を修正すればよい。事前の手続きが簡単で、創意の試行錯誤を許す仕組みが可能であることがWebなどの新機軸を生んだ。この柔軟性が、技術ライセンスの無償開示原則と相まって、インターネットの爆発的普及の一因ともなった。このような基準形成を可能としたのが、IP網の設計思想であるEND-END原則といえよう。

インターネットは、基礎的な技術基準に対し、複数の実装（implementation）ソフトが対応している。重要な基礎規格には、IP、TCP、FTP（File Transfer Protocol）、SMTP（Simple Mail Transfer Protocol）、DNS、HTML（Hyper Text Markup Language：W3C〈The World Wide Web Consortium〉が原案）がある。

また、これらの基格に対して再配布可能な

オープンソースの実装ソフトが存在する。具体的には、DNSはBIND（Berkeley Internet Name Domain）、WebはApache（アパッチ）、メールはSendmail（センドメール）といった具合である。

## 5 インターネットの歴史

インターネットは、1960年代末に米国国防省の通信網の研究プロジェクトARPA（Advanced Research Projects Agency）NETとして始まった。当初は、遠隔地にある研究機関・大学を結ぶ学術研究のためのコンピュータのタイムシェアリング（時間共有）を目的としたパケット交換網で、一般利用としては電子メールがあるくらいだった。

1980年代後半に所管が国防省からNSF（全米国立科学財団）に移され、1990年ごろから、インターネットをビジネスとして成り立たせ、民営・商用化する方向に舵を切った。商用化により通信キャリア（事業者）の参入やISPが出現した。1990年代半ばにWWWが開発されると、インターネットの一般利用が急速に進んだ。これに応じて管理体制の強化が課題となり、南カルフォルニア大学が行ってきたIANA機能（IPアドレス・AS番号配布、技術基準、ルートゾーン・ファイルを管理する機能）の運営が、1998年に民間法人のICANNに移管された。インターネットの技術およびサービス展開を表1にまとめた。

IPアドレスやドメインネームは日本語の感覚にはしっくりこないが、国際的には電話番号が資源であると認識されているのと同様、

表1　インターネットの技術およびサービス展開

| 年 | |
|---|---|
| 1972 | • e-mail（電子メール）が一般向けサービスの嚆矢となる |
| 1973〜74 | • 異種ネットワーク間の通信を可能とするオープンネットワーク・アーキテクチャー思想による通信プロトコルTCP/IP（Transmission Control Protocol/Internet Protocol）が開発される（開発者ロバート・カーン氏、ヴィントン・サーフ氏） |
| 1979 | • ICCB（Internet Configuration Control Board）が、TCPソフトウェア開発支援を開始する |
| 1983 | • IPv4（IPバージョン4、32ビットアドレス）に移行する |
| 1984 | • DARPA（Defense Advanced Research Projects Agency：ARPAから改称）は、インターネットの標準と全般アーキテクチャーを決定する機関として、ICCBに代わりIAB（Internet Advisory Board）を設置し、各タスクフォースに対し課題を分散委任することとした |
| 1985 | • DNS（Domain Name System）が導入される<br>• DNSは階層型のアドレス制度を採用しており、最上階をトップレベル・ドメイン（TLDs〈.org, .com, .jpなど〉）という<br>• DCA（Defense Communications Agency）は、g（generic）TLD（.com,.coなどの一般名称のTLD）の登録を、スタンフォード国際研究所（後にInterNIC/Network Solutions）に依頼する<br>• cc（country code）TLD（.jpなどの国別TLD）は当該国による分散管理体制が取られる |
| 1986 | • 標準化機関としてIETF（Internet Engineering Task Force）が設置される<br>• NSF（National Science Foundation）が、全米の大学を結ぶNSFNETにTCP/IPを採用し、またインターネットの財政自立を目指す将来構想を明らかにする |
| 1991 | • WWW（World Wide Web）が開発される（開発者ティム・バーナーズ＝リー氏〈CERN：欧州原子核研究機構〉） |
| 1992 | • NSFはインターネットの財政自立と国際展開を目指し、インターネットのグローバルな調整と協力を任務とするISOC（Internet Society）を設立する<br>• またこの間、NSFはNSFNETの地域機関に商用接続を奨励するとともに、民間企業がバックボーン回線に参入することを促すため、NSFのバックボーン回線の商用利用を制限する |
| 1994 | • WWWの相互運用可能性確保と発展を任務とするW3C（The World Wide Web Consortium）が設立される |
| 1995 | • NSFはNSFNETのバックボーン回線運用を民間に移管する（財政支援打ち切り）<br>• この間、民間ISP（インターネット・サービス・プロバイダー）が発達し、IXPs（インターネットエクスチェンジ・ポイント：トラフィックの交換施設）も増加する |

インターネットにおける資源との観念で捉えられている。資源は公平な分配をめぐり争奪の対象となる。あるいは争奪の対象となるものが資源の定義かもしれない。表２にインターネットの資源管理の展開をまとめた。

## 6　歴史から見るインターネットのガバナンス体制

電気通信などの従来のメディアは、政府が事前に枠組みを決定し、政府または事業体のトップダウン的な計画でメディアの構造を規定した。これに対しインターネットは、米国政府の財政支援はあったものの、構造自体は、米国の学者間のオープンで協力的な枠組みのなかで、多数の参加者が、相互運用可能な、安全で安定した効率的な、また拡張可能な仕組みを求めた結果として発展した。

IETFやW3Cなどの技術標準機関は、独立したオープンで参加型の、コンセンサス（合意）重視のボトムアップスタイルで運営されてきた。また、新サービスの実用化へのハードルが低く、参加者の創意が発展の基礎となった。さらに、技術基準を遵守しIPアドレスさえ取得すれば、小額投資で誰でもネットワークに参加可能という増殖メカニズムがあった。これにより、インターネットの商用化が決定されると爆発的に普及することとなった。

この仕組みでも、参加者がほぼ学者に限られた段階では、参加者の自主性とマナーに守られ、インターネット秩序にさしたる問題は発生しなかった。しかし、商用利用が拡大するにつれ、インターネット全体の管理体制の脆弱性がクローズアップされてきた。

表2　インターネットの資源管理の展開

| 年　月 | |
|---|---|
| 1960年代後半 | • 南カリフォルニア大学の情報科学研究所（ISI）のジョン･ポステル氏が米国政府との契約に基づき､各種ネットワークおよびRIR（地域インターネット登録機関）に対してIPアドレスなどを配布した |
| 1992 | • NSFは民間企業のInterNICを設立し、DNSの登録事務を移管した |
| 1995 | • NSFはgTLDのドメインネーム需要が爆発的に増大したのを受け、gTLDの管理を民間企業NSI（Network Solutions）に委託し、NSIが有料で登録事務を行うことを認めた（多くのccTLDの登録は、この間すでに有料化されていた） |
| 1998　6 | • 米国商務省はドメインネームの管理に関し、安定性、競争、参加（representation）、ボトムアップ型政策決定の4原則を提示した<br>• その背景には、WWWの爆発的普及により、ドメインネームをめぐり、不当占拠するサイバースクワッターの出現や、NSIの業務独占体制、米国一国の制度支配に対する懸念が増大したことがあった |
| 11 | • 米国商務省は、非営利法人ICANN（The Internet Corporation for Assigned Names and Numbers）とMOU（覚書）を締結し、政府からのDNS管理の移管手続きを開始した<br>• 同時にIANA（Internet Assigned Numbers Authority）機能もICANNに委託したが、TLD変更に関する承認権限は商務省が保持した |
| 1999 | • gTLDのRegistry（事務処理）機能とRegistrar（対ユーザーサービス）機能が分離された<br>• 各TLDは中央集中データベースを維持しながら、gTLDの登録サービスは競争下で行われることとなった |
| 2000 | • ICANNは、競争強化のため7つのTLD（info, biz, coop, pro, name, museum, aero）を新規導入した（さらに2005年、jobs, travelの導入を承認した）　これにより登録価格は6ドルから4ドル程度にまで低下した<br>• またICANNはドメイン関連紛争の迅速な解決のため、WIPO（世界知的所有権機関）が開発したUDRP（Uniform domain name Dispute Resolution Policy）を採用した |
| 2002 | • ICANNは、技術事項に特化し、政策事項の決定は適切なフォーラムに託することを宣言した。これにより、以下のフォーラムが形成された：Address SO（Support Organization）、ccNames SO、gNames SO、Government AC（Advisory Committee）、Root Server Systems AC、Security and Stability AC、At Large AC（個人ユーザー）　Technical Liaison Group, IETF（Internet Engineering Task Force）<br>• また、これに伴いICANNの理事は、各SOと指名委員会により選任することとなった |

1998年以降、米国政府は秩序維持の努力をすることとなるが、その努力は、当初からの「学者間の協力体制からの発展」という歴史的制約を強く受けることとなった。

## 7　インターネットの発展原理

ここでインターネットの発展原理を考察してみよう。インターネット・ガバナンスを考えるには、インターネットの持つ本質的な特徴を考慮することが不可欠だからである。

世界における結合関係は、およそ「比例原理」と「べき乗原理」の２種類あると考えられる。比例原理の典型は電気通信網の加入者線整備で、投入経費に比例して一本一本整備されていく。べき乗原理の典型例は「美人投票」である。仮に平均より1.5倍魅力的な人がいたとすると、その人に投票する人ごとに1.5倍の原理が働き、投票者数のべき乗の票が集まる。このように、べき乗の選択が機能したときに得票数の分布はどうなるだろうか。結果は指数曲線により表現されるべき乗分布になるという[注2]。

べき乗分布は、世の中のあらゆるところで見られる。たとえば、俳優の人気度や所得分布、ウィルス感染の拡大、交通網のハブ（中継点）、企業競争の市場シェアなどはべき乗分布に従うとされる。べき乗原理によるネットワークの増殖は、成長と優先的選択の相互作用による。さらに、選択に要する資源投入が極小の場合はその程度が促進される。

べき乗原理は、ねずみ算や成長曲線として昔から知られていた。しかし最近の知見は、その原理が部分的なものではなく普遍的なものだということである。

電気通信網上での通信方式の選択は、べき乗原理の要素が強い。インターネットは通信網と端末（パソコン）の存在を前提とし、そのうえでの通信方式の選択というべき乗原理的な要素により急成長した。またそれにとどまらず、Webや電子商取引、SNSなどのインターネット上のさまざまなサービスを発展させる基盤となっている。これらは比例的な物的投入が最小限で、ほぼ意思決定のみで成長する。

このようにインターネットは、主にべき乗原理に従うと見られるが、その基盤となるブロードバンド（高速大容量回線）網の敷設は比例原理に支配されており、したがって、デジタルディバイド（情報格差）の解消には従来型の資源投入が必要である。

## 8　インターネットの脆弱性

インターネット網の一つの特質は、インターネットは基本的に論理網であるということである。一定の論理に適合するものならばどんな接続をも受け入れる。このことから、パケットをあふれさせ接続できないようにするDoS（Denial of Service：サービス拒否）攻撃が可能となる。

ハードウェアの設備としては電気通信網、ルーター、DNSサーバーがあるが、これらが部分的に破壊されても、代替ルートを論理的に設定するなど耐性がある。この点は、部分的な障害でも通信不能となる電気通信網に比し頑健性がある。しかしIP網には、ネットワークの形状としてトラフィック（データ量）が集中するハブ（集線装置）が存在しており、このハブがなんらかの機能不全に陥れば網全体がダウンすることとなる。過去にも、インターネット接続が国全体で不可能と

なった事例がある。

IP網のもう一つの弱点は、誰でも参加可能であり、どんなプログラムでも実行可能という特性から派生する。参加者の認証が究極的には不完全なため、なりすまし（spoofing）と悪意のあるプログラムの排除が困難ということである。たとえば偽Webサイトへの誘導手段としては、本来のサイトに酷似した詐欺Webサイトへ誘導するフィッシング（phishing）があるが、IP網上でも、DKA（Dan Kaminsky Attack）という、偽りのDNSメッセージを注入し、偽りのアドレスに誘導する手法が発見されている。

## Ⅲ インターネット・ガバナンスの国際的議論

### 1 議論の発端

2003年に国連主催のWSISジュネーヴ会合（第１回会合）が開催された。この会合の主要議題は、途上国の情報環境を改善するためのデジタルディバイドの解消であったが、IPアドレスなどのインターネット資源が米国政府とICANNに独占的に管理されていることが、インターネット・ガバナンス問題として浮上した。米国・欧州・日本の自由世界が現行システムの維持を主張したのに対し、その他の国は反対した。

結局、ジュネーヴ会合の結論としては、原則宣言（Declaration of Principles）が採択された。この動きは、次いで設置された「作業部会（WGIG〈Working Group on Internet Governance〉）報告」、2005年の第２回（最終回）WSISチュニス会合決議、さらにそれを受けて設置されたインターネット・ガバナンス・フォーラム（IGF）へと続いていくこととなる。

なお、2003年WSIS原則宣言の主なポイントは次のとおりである。

- インターネット・ガバナンスは、情報社会のコアアジェンダ（中心的課題）である――多数国による、透明で民主的かつ政府の関与が必要である
- 技術・政策課題はすべての利害関係者が参加して解決すべきである
  - ⓐ主権国家が政策権限
  - ⓑ民間セクターは技術・経済面で従来同様の役割
  - ⓒ市民社会はコミュニティレベルで重要な役割
  - ⓓ政策課題に対しては政府間国際組織が調整
  - ⓔ国際組織は技術基準開発関連の役割
- 国連の事務総長はインターネット・ガバナンスのワーキンググループを設置し、2005年までに報告する

この宣言を受けて設置されたWGIGは2005年６月に報告書（以下、WGIG報告）を提出した。WGIG報告は、最初にインターネット運営の原則を確認したうえで、インターネットが抱える接続・資源管理とICANN、サイバーセキュリティ、競争政策、知的財産権、電子商取引、ガバナンス体制の問題を網羅的にまとめている。

### 2 WGIG報告

ジュネーヴ会合の原則宣言では、政府の統制機能強化のニュアンスが強かったが、WGIG報告ではインターネットの課題を多面的に捉えた。WGIGは、インターネットが抱

えるさまざまな問題を包括的に検討したものの、反面、議論の焦点が拡散した。その典型が、ガバナンスの定義を広義にしたことで、制度面の課題に代わり最重要課題として浮上してきたのが、信頼性・安全性などのサイバーセキュリティであった。これは、政府管理というジュネーヴ会合の原則宣言とは異なる方向で、米国などの非規制論者の主張が巻き返しに成功したと考えられる。以下、WGIG報告の主要な論点を紹介する。

### (1) インターネット・ガバナンスの定義

「インターネット・ガバナンスとは、政府、民間部門、市民社会が、それぞれの役割において、共有の原理・規範・規則・意思決定過程・計画を開発・適用することによってインターネットの進化と利用を形成すること（原文は、Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.）」と定義された。

すなわち、インターネットの健全な運営に必要なのは、政府、民間、市民グループの協調という方向が強調された定義となっており、この時点で、主権統制論者の敗北は決定したといってよい（あるいは、敗北したからこの定義となった）。

### (2) インターネット運営の５原則の提示

インターネット運営に関しては、以下の５つの原則が提示された。

①技術開発と資源管理における協調・分散体制：コンテンツ、サービス、技術の集権的管理の否定が、相互運用可能で機能的・安定・安全・能率的かつスケーラブル（拡張性に富む）な網を長期的に生み出す

②すべての網を接続可能とする分散型・オープンアーキテクチャーである

③非所有・無償開示の基幹標準である

④自由市場における競争と革新が指導理念である

⑤END-END原則（ネットワークの中立性）：パケットの伝送に集中することが、END（端末、コンピュータ）における多様な利用を支える

### (3) IPアドレスとDNS

安定・安全な運用を図るため、組織形態と責任および組織間の関係を明確にすることが必要である。IPアドレスやgTDL（generic Top Level Domain）の分配には偏りがあり、公平な配分が必要である。cc（country code）TLDの管理は、当該国のIANA機能として実行されることが想定されているが、公式な制度はないのでその明確化も必要である。また、DNSの多言語化（IDN：Internationalized Domain Names、セカンドレベル・ドメインにおける多言語化のための非ASCII〈American Standard Code for Information Interchange〉記号の表現基準で、たとえば、「日本.jp」などのアドレスが可能となる制度）も推進すべきである。

現状、ICANN、IANA、米国商務省、暗号化技術・証明書発行企業ベリサイン（VeriSign）およびルートサーバーの運営者が関係者で、これらは、２者間あるいは多者

間の合意、MOU（覚書）、スポンサー契約、作業規定、自発的行動によって管理しているが、これらは信頼に基づくものであり、国際的な法的根拠に欠ける。

### （4） ISPの接続制度

接続の基本的仕組みは、ISP間の接続契約によっており、ピアリング（Peering）とトランジット（Transit）の２種類が基本の契約形態である。ピアリングは、同等のISP同士の契約で、接続通信費用を含め折半する。トランジットでは、小規模のISPは大規模ISPに対し、接続回線料金を負担したうえ、さらにトランジット料を負担することになる。

この仕組みはバックボーン（基幹線）から遠い途上国には不利であり、1993年から98年にかけて、途上国から400億ドルが資金流出したとされる（ITU推計）。ITU-T勧告D.50（2000年10月）は、「トラフィックの流れ・ルート数・地理的カバレッジ・国際伝送コストなどを考慮した補償」を提案しているが、この勧告は現実には実行されていない。

この課題に対してWGIGは、途上国のアクセスを支援するため、地域IPバックボーンや地域IXP（インターネットエクスチェンジ・ポイント：トラフィックの交換施設）などの研究と財政支援措置を提案している。

### （5） サイバーセキュリティ

スパム（迷惑メール）、サイバー犯罪、ネットワーク・情報システムの破壊など、サイバーセキュリティを脅かす脅威が発生しており、これに対処するための国際的な法的枠組み・調整の枠組み・協力体制が必要である。

スパムに関して、インターポール（国際刑事警察機構）では、LAP（London Action Plan、2004年発足）による違法スパムの対処をしている。しかし、スパムについて国際的に統一した定義をすることは困難である。

インターネットでの「犯罪天国」を防ぐには、世界的な犯罪立法を要する欧州のサイバー犯罪条約がモデルとなる。これにより、捜査・押収・情報保存・訴追に関して共通手続きが保障できる。

情報システムの保護に関しては、各国のCERT（Computer Emergency Response Team：コンピュータ緊急対応チーム）が最初の防衛線となっている。多くのCERTは、FIRST（The Forum of Incident Response and Security Teams）に加盟している。またIETFでも、プロトコルの安全性審査やPKI（公開暗号鍵基盤：Public Key Infrastructure）を開発している。

サイバーセキュリティの保持には、関係者間の不断の情報交換と対策が必要で、必要性とリスクに応じた（proportionality）対策を取り、イノベーション（技術革新）を促進すべきである。また、人権保障との調整が必要である。安全文化を育成する必要もあり、政府は啓発と教育において重要な役割がある。

### （6） データ保護とプライバシー

インターネットにより、プライバシー侵害の脅威が増大している。侵害目的は、商用・スパム・ID盗用・ハラスメント（嫌がらせ）などである。また、越境データに関する国際的な保護手段も未整備である。

OECDでは、1980年にプライバシー保護と越境データ流通に関する勧告を行い、また、ICPEN（International Consumer Protection

and Enforcement Network：消費者保護および執行のための国際ネットワーク）では、越境取引に関する情報交換を実施している。

国際的に調整が未定の分野として、インターネット利用における本人確認と事後における強制的な記録保持、匿名活動の範囲、利用者が公開サイトに提供した情報のアーカイブ化を阻止したり削除したりする活動などがある。これらに関しては、表現の自由と安全なインターネットとのバランスが必要である。また、関連する処置はISPにより実施されるものの、現在ISPの責任に関して調整する組織はない。

### (7) 電子商取引

インターネットにより、新しい取引手法が提供されたが、デジタル署名・電子契約・電子証拠の許容性などの取引促進環境形成が課題である。

国連国際商取引法委員会（UNCITRAL）は、電子署名と電子商取引のモデル法を作成し、現在、電子契約の条約案作成に取り組んでいる。新技術は消費者に新たなリスクをもたらすが、それを検討するメカニズムがない。消費者の権利保護に関しては、現状はICPEN以外の国際メカニズムは存在しない。さらに、法制上権利が認められても、消費者は権利の行使が困難であり、そのうえ、裁判管轄・文化・言語の障壁もある。デジタルコンテンツに関する権利は、消費者法制よりはIPR（知的財産権）法制により規定される。そこでは、消費者の権利はEULA（End User License Agreement：使用許諾契約書）などにより規定される。

### (8) 知的財産権（IPR）

インターネットがデジタル形式の知的財産の世界的配布を安価に可能としたことにより、無許可のコピーや修正の脅威が増した。著作権・特許・商標にはそれぞれ異なる扱いが必要で、創造性と革新に対するインセンティブを確保するとともに、利用者の合理的な必要と期待とを満たさなければならない。

### (9) 競争政策とガバナンスモデルの将来

インターネットが学術用から公衆利用のグローバル設備に発展した背景には、通信の自由化政策があった。インターネットの次の変化は、伝統的な通信分野へのIP技術の拡張であり、次世代通信網NGN（Next Generation Network）が規制政策上の課題である。WTO（世界貿易機関）の電気通信サービス貿易協定は、通信の自由化政策の普及に大きな影響があった。

グローバリゼーションの進展によって、主権国家システムが有効に機能しない局面が増えてきており、インターネットはその典型ともいえる。国家主権は依然として有効ではあるものの、法的地位の異なったプレーヤーが参加する広い環境下で考える必要がある。政府部門、民間部門、市民部門の３者（tri-stakeholderism）が、ソフトな法や自主規制などの新たな規範をグローバルなガバナンスに組み入れる認識枠組みが必要である。

### (10)フォーラム機能の形成

WGIG報告は最後に、全関係者が平等の立場でインターネット・ガバナンスの諸課題を論じる新しい空間（フォーラム）の創設を提言した。フォーラムは、国連とリンクし、地

理バランス・多言語にも配慮するものとされた。

## 3　2005年WSIS第２回会合

2005年のWSIS第２回会合に先立ち、WGIGでの議論と並行して、日本を含め世界各地でインターネット資源管理に関する議論が盛り上がった。WSIS第２回会合は前回と異なり、EU（欧州連合）が主権統制派に回り、米国・英国・オーストラリア・カナダ対その他という対立の構図で会議は紛糾した。この間、日本政府は発言せず。最終日深夜、「現状のガバナンスは良好であるが、国際的統制も必要」という妥協文書（チュニス・アジェンダ）を採択し、IGF（インターネット・ガバナンス・フォーラム）を５年間開催して、この問題をさらに討議することを決定した。すなわち、結局、インターネット資源の国際管理の問題はチュニスでは結論に達せず、チュニス・アジェンダという宣言を採択し、IGFへの先送りで決着したのである。

チュニス・アジェンダの主なポイントは次のとおりである。

- 2003年WSIS原則宣言を再確認する
- WGIGのガバナンスの作業定義を採用する
- 政府、民間、市民のそれぞれの役割を確認支持する
- サイバーセキュリティ文化を醸成し、犯罪を取り締まる
- プライバシーと消費者保護が必要である
- 電子政府を促進する
- 国際的な接続性（ISP接続契約、国際IXP）を改善する
- 多言語化を促進する
- 革新、競争、投資の支援環境を維持する
- ccTLDに関する決定に他国は干渉しない
- IGFを５年間組成する

## 4　IGF会合

チュニス・アジェンダを受けたIGF会合は、2009年11月のシャームエルシェイク（エジプト）を含め４回開催された。初回と第２回のテーマは「開発のためのインターネット・ガバナンス」、第３回は「すべての人のためのインターネット」で、５年間の総括と今後の方向を決定する第４回のテーマは「インターネット・ガバナンス――すべての人のための機会の創造」であった。

IGFは決定機関ではなく、議論の場であり、勧告も行わない。国連事務総長が召集し、事務局は国連ジュネーヴ事務所に設置されている。政府、民間、市民が、対等の立場で参加する。

最終回とされた2009年の第４回会合は、112カ国から96の政府代表（600人）を含む1800人が参加し、過去最大となった。討議された議題は、アクセス、文化多様性、安全、DNS、接続、ソーシャル・ネットワーク、プライバシー、データ保護、表現の自由、有害違法情報――などで、メインセッションのほかに100以上の議題で会合が持たれた。IGFの継続問題も議論され、多数がマルチ・ステークホルダー（多様な利害関係者）の情報交換のプラットフォームとしてのIGFの継続を支持した。一方で、一部マルチ・ステークホルダーのコンセンサスベースの意思決定機関に変更すべきとの見解（中国、サウジアラビア）も表明された。結局、国連事務総長の承認を条件に、第５回をリトアニアのビリ

ニュスで2010年９月14日から17日まで開催することとなった。第４回会合の主要議論は以下のとおりであった。

- 議長総括――サイバー犯罪、安全、プライバシー、開放性はすべての関係者の共同責任である
- 会議直前の2009年９月に米国政府がICANNと締結したDNSに関する新しい契約（AOC：Affirmation of Commitment）は、一国によるICANNのDNSに関する監督を多国間の監督に置き換えるもので正しい方向である（クマール国連IGF調整官）
- インターネット・ガバナンスの過程のなかに人権問題を実際的に位置づけることが必要である
- インターネット・ガバナンスにおける越境性（transnationalization）が課題である（インターネット創始者の一人ロバート・カーン氏）
- ITUとICANNは、特定領域でライバル関係にある
- WWWの創始者ティム・バーナーズ＝リー氏が、Webをメディアとしてさらに発展させるため、非営利法人の「the World Wide Web Foundation」の立ち上げを正式発表した
- 今後、国連総会でもサイバーセキュリティの問題を取り上げる（経済社会理事会）

５年間のIGF活動をどう評価すべきか。IGFの当初は、チュニス・アジェンダの継続ということで変化への期待があった。しかし、IGFは変革の場ではなく、討論（ガス抜き？）の場にすぎないとの認識が広まり、ガバナンス問題の本丸であったインターネットの資源管理問題に関する熱気は薄れた。代わってIGFは、インターネットという急拡大した事象に関連するさまざまな団体が集結し、さまざまなイベントを開催する一種の祭典と化した。時間の経過とともに、ガバナンスに関してドラスティックな改革を行うという空気はなくなり、現状追認ムードが支配することとなった。この空気の変化には、米国が取ったICANN運営の改善策も寄与した。

## 5　WSIS・IGFに対する米国の対応

WSISを機にインターネットの資源管理の国際化を求められた米国は、覇権の維持のための対応を行うこととなる。実際、米国の担当者は議会証言で国際的圧力が相当効いたことを認めている。米国の対応は、対抗原理としてまずマルチ・ステークホルダーという理論武装をし、またその思考に基づき、実際のICANNの運営を、米国の覇権を維持しながら国際的に受け入れられやすい形へと変革することであった。そのためICANN内に戦略委員会を設置し、米国政府とICANNとの契約関係の改善を図りつつ、ICANNの運営に各国政府や各種団体の意向を反映させる組織改革を行った。そして、主権国家をメンバーとするICANNの諮問機関GAC（Governmental Advisory Comittee）の重要性を強調するとともに、IDNの導入を決定した。

さらに米国政府は、ICANNの地位を安定化する前述のAOCを、IGFの第４回会合の直前の2009年に締結し、これを画期的なものであると大宣伝をした。

AOCの概要は以下のとおりである。

- ICANNのDNS関連業務は、米国政府からの委託ではなく自らのものとする

- 米国商務省への報告義務を廃止し、新たに年次報告書の発表義務を負う
- 1998年にICANNが創設されて以来、AOCは米国政府との８回に及ぶ契約改定の最終となるもので、従来と異なり期限がない
- 非営利・民間のボトムアップ手法の組織原理が有効に機能することを最終的に宣言する
- ICANNは独立で、どの組織にも支配されることなく、マルチ・ステークホルダーからなる「THE　COMMUNITY」のレビューに従う
- GACの役割は重要で、レビューチームの選定においても重要な役割を果たす
- AOCは環境変化に対処する安全なプラットフォームを提供する

2003年WSIS原則宣言では、インターネットの政策事項は主権国家の権限とされ、インターネット資源の国際管理の動きが盛り上がった。米国はこの動きに危機感を覚え、自国の覇権維持のため、IGFに議論を先送りすることに成功した。IGFではインターネットの多様な課題が包括的に議論され、資源管理の問題のみには焦点が当たらなかった。その間米国は、ICANNの法的位置づけの明確化、運営体制におけるGAC強化、AOC締結、IDN導入などで他国の不満の沈静化を図った。

この過程を見れば、WSIS・IGFは、政府間国際機関によるインターネットの国際管理体制の構築には直接的には失敗したものの、ドメインネームに関しては、GACを通じた主権国家の影響力強化に実質的に成功したと評価できよう。

ただし、肝心のIANA機能は依然として米国政府の管理下にあり、課題は潜伏したままである。また、資源管理に関する議論が沈静化したのは、米国の意向もさることながら、現実にICANNの資源管理がおおむね成功しており、ITU型の主権国家による国際管理の効率性に疑問があることを反映したものでもある。

## Ⅳ インターネット・ガバナンスの課題

### 1 インターネット・ガバナンス問題の構造

そもそもインターネット・ガバナンスはどうあるべきか。これを考えるにはインターネット自体の構造を前提に考えざるをえない。

インターネットサービスは、電気通信網、IP網、プラットフォーム・アプリケーション層に重なって提供されるので、ガバナンスに関しても３層を区別する必要がある。

利用者にとって最も見えやすい層は、アプリケーション層である。この層はリアルの世界でも対応する社会活動があり、リアルの世界にある規制は、ネット上でも、原則的にはそのまま適用される。ただし、インターネット上のサービスは、簡単に国境を越え、従来の国内法制による規制は意味をなさない。たとえば著作権規制は、サーバーを国外に置けば規制から容易に逃れることが可能であり、国内のみで法規制を議論することは無意味に近い。国際協調・国際調和が必須となる。

インターネット・ガバナンスの階層別の課題を列記すると以下のようになる。

- **コンテンツ・データ層**

情報漏えい、違法コピー、迷惑メール、違法・有害情報、フィルタリング（アクセス制限）、プライバシー侵害、個人情報保護、実名制、トランスナショナリティ（国内法の無意味化）

- **プラットフォーム・アプリケーション層**

技術基準（IETF、W3C、暗号）、Webブラウザー、ライフログ（人間の行為のデジタル記録化）、不正アクセス、ID認証、フィッシング、マルウェア、ボット（コンピュータウィルスの一種）、プラットフォーム機能（課金認証機能など）

- **IP網**

技術基準、DNS管理、ルートサーバー運営、IPv6への移行、ISP運営、ISP間接続契約（接続形態、資金、Tier1の経営方針）、ICANN、ネットワークの中立性

- **回線層**

アクセス回線、バックボーン回線の接続・料金、IX、中継費用の回収方法、電波利用

また、これらの階層に対応して、以下のようにすでにさまざまのガバナンス機構・制度などが形成されてきている。

- **コンテンツ・データ層**

表現の自由・情報の自由流通原則、プライバシー法制、EU越境データ流通指令、サイバー犯罪条約、個人情報保護法、プロバイダー責任制限法、特定電子メール法、違法・有害情報、青少年ネット利用環境整備法、モバイルコンテンツ審査・運用監視機構、出会い系サイト規制法、特定商取引法、著作権法

- **プラットフォーム・アプリケーション層**

技術基準（W3C、暗号）、セキュリティ技術、ライフログ利用基準、不正アクセス防止法

- **IP網**

技術基準（IETF）、DNS管理、ルートサーバー運営、ISP運営（届出制）、ISP間接続契約（接続形態、資金、Tier1の経営方針）、ICANN、AOC、ネットワークの中立性、利用量規制、ベストエフォート（最善の努力）

- **回線層**

アクセス回線、バックボーン回線、電気通信事業法、携帯電話不正利用防止法、ITU条約

インターネットに限らないが、コンピュータシステムは社会のあらゆる局面に浸透しており、すべてを包括するガバナンス制度を設けるのは不可能である。インターネットでも、レイヤーごとに異なった運営責任者が存在しており、ガバナンス問題もそれぞれの運営責任者ごとに考える必要がある。インターネット固有のガバナンス課題は、主としてIP網にかかわる分野のものであり、実際に国際的な議論も、主としてIP網のガバナンスに関するものであった。

## 2　IP網のガバナンス

IP網は、技術基準、アドレス体系、ISPの３要素で構成され、ガバナンスもこの３要素について考える必要がある。インターネットは研究者間のコンピュータシェアリングの必要性を満たすことからスタートしたため、参加者は信頼できるものという前提で設計された。しかし商用化によりこの前提は崩れた。またEND-END原則があるため、悪意の参加者による悪意のプログラムがIP網上では排除できない。ここから安全対策がガバナンス上

の最大課題となってきた。

アドレス体系に関しては一国が支配的に運営していることが課題であるが、これまで見てきたように、国際的議論は収束しつつある。

また、ICANNによる技術基準策定について、ガバナンス上の問題は提起されていないし、IEEE（The Institute of Electrical and Electronics Engineers）などの他の標準策定機関の運営と比較しても特段の課題はないと考えられる。

残る要素であるISPのあり方については一部接続問題が議論されたが、それ以外の側面についての議論が尽くされたようには思われない。ガバナンスの観点からは、ISPのあり方の検討が不十分だったのではないか。以下に諸問題を概観する。

## 3　IP網のガバナンスの諸課題

### (1) サイバーセキュリティ

サイバーセキュリティは、誰でもどんなプログラムでも運用可能というインターネットの本質に伴うリスクであり、インターネット・ガバナンスの最大の課題である。インターネットや情報システムに対する脅威は、かつてはハッカーが腕試しにサーバーに侵入するといった愉快犯的な犯行が中心であった。しかし最近では、インターネット詐欺を目的とする組織化されたプロのサイバー犯罪者が出現してきた。また、テロリストによる利用やサイバーテロも実行されつつある。さらに、主権国家が諜報や戦争手段としてインターネットを捉える事態まで出現している[注3]。犯罪への対処としては国際協調が重要で、サイバー犯罪条約の批准と国内体制の整備が必要となっている。

わが国では内閣官房の情報セキュリティセンターおよび各省庁で、国際水準の政策対応が行われ、CIRT（Cyber Incident Response Team） やISAC（Information Sharing and Analysis Center）といった防護組織も活動している。また、犯罪の取り締まりに対しては警察庁の専門チームが対応し、またサイバースパイ・サイバー戦争に対しては、防衛省は2011年度にも対策部隊を発足させる予定と報じられている。

米国でも、サイバーセキュリティがオバマ政権の重要政策とされており、今後の技術開発予算を確保している（ちなみに米国では、奇襲的サイバー戦争を「デジタル・パールハーバー」と呼んでいる）。また、中国におけるグーグルをめぐる最近の動きは、サイバーセキュリティの重大性を示している。まさに、サイバー戦争は現実に戦われている戦争である。

### (2) ISPにかかわる問題

- **規制**

ISPは、日本では電気通信事業法の規制を受ける。電気通信事業法の規制哲学は、通信産業は設備産業であり競争が有効に機能しない可能性があることから、競争状態に類似したサービス提供がなされるよう経済的規制を行うのが主目的である。ISPは電気通信法制上、競争が機能する分野として、通常、届け出などの弱い規制しか受けていない。

事業法には、通信の秘密という社会的規制も含まれているが、この問題は単純で、過去これ以外の社会的規制が特に問題とされることはなかった。しかし、インターネットは通信をめぐる問題状況を根本から変えた。イン

ターネットの影響は通信内部にとどまらず、社会生活全般の安全性に及ぶからである。

もしも悪意のISPが存在する場合、盗聴、個人情報漏えい、アドレス書き換えなどのリスク要因が存在する。また悪意がなくても、ISPに情報セキュリティ保持能力のない場合もある。電気通信の規制哲学もこれに応じて変化する必要があるのではないか。従来の経済的規制に加え、社会の安全を保持する観点からの規制の再検討が必要である。

ただし、これには表現の自由という権利がからむため、政府の直接規制はふさわしくなく、間接的な規制が望まれる。具体的には、情報管理体制、技術管理体制、人事管理体制等、サイバー犯罪についての証拠を残すため、記録保持等のフォレンジック（電子的な証拠）規制やハニー・ポッド（おとりサーバーへの誘導）等の捜査方法等、サイバー犯罪条約などの国際的枠組みに適合する体制について、規制当局が実効性のあるガイドラインを作成し、この遵守について民間の外部監査の実施を強制することが考えられる。

**● 接続問題**

ISP間の接続は、前述のようにピアリングとトランジットの２種類があり、ピアリングは同等のISP同士の契約で、すべての接続関連費用を折半するのに対し、トランジットでは、小規模のISPは接続回線料金を負担したうえに、トランジット料を支払う。この慣行は、規制のない自由市場において大きなネットワークを持つISPの交渉力が大きいために成立したと考えられる。ネットワークの価値は大きいほど高く、大きなネットワークに接続する利益も多いため、経済学的な合理性もある。

このため、弱小ネットワークは、大手と比べ回線料・トランジット料の負担が多く、競争上不利であり、国内的には淘汰される傾向がある。しかしこれは国際的に見ると、弱小途上国から大国へ資金流出があるということであり、国際的なデジタルディバイド解消の大義に反する事態ともなっている。

弱小途上国といえども、その国のISPは淘汰されるわけにはいかないので、弱小途上国の不利な地位は、公的介入により是正されるほかない。国際的には、国家権力をバックに弱小ISPでもトランジット料を請求する事例があるとされる。

この問題の解決については、ITUですべてのISP間接続のピアリング契約を強制するなど、接続規制を検討することも一案である。ITUでは接続問題の研究が進められているが、米国などの非規制論者の意見が強く、合意にはほど遠いのが実情である。

また、国内的には接続の義務づけと接続関連経費の負担について、地域ISPの存在価値と大手の「あまねく提供する義務」のあり方を整理するなかで、公的介入が必要かどうか検討することも必要と思われる。

**● ネットワークの中立性問題**

インターネットの設計思想は、END-END原則であった。IP網は、情報内容をそのまま相手に届け、情報の処理は端末側に全面的に依拠する（IP網は情報に対して中立で、監視もしない）。そこからISPは、データの内容・性格によって速度などのサービス内容を差別しない義務を負っていると解される。

インターネット利用が電子メールや静止画

のWebなど単純なものだった時代には、ISPのサービス提供原則の「ベストエフォート」が、サービス遅延の言い訳として機能していた。しかし、インターネットサービスが、ブロードバンド上のVoIP（Voice over IP：音声通話）、ストリーミング（音声・動画の転送・再生方式の一つ）、テレビ電話、動画のpeer-to-peer（P2P：端末間）伝送などのサービスに移行していくことで、ネットワーク利用管理には新たな課題が生まれた。

VoIPなどでは、遅延すればサービス提供していないとされるため、ベストエフォートという概念は遅延の言い訳としての意味を失った（ISPの法的責任免除の根拠としては機能）。つまり、ISPは遅延のない保証的サービス提供を求められることとなったのである。

しかし、ブロードバンドとはいえ帯域に限りがあることから、ISPは自らのネットワークの効率的管理と帯域拡張投資問題に直面することとなる。ISPは何らかのトラフィック管理方針を策定する必要に迫られた。手法としては、料金制度でトラフィック管理する方法と、ISP自体が直接トラフィックを規制する方法が存在する。

ISPが直接トラフィックを制御することはEND-END原則に反し、情報の操作、表現の自由、情報の自由流通原則にもかかわる行為である。しかし、経営上は何らかの対応をせざるをえない。また、この問題はインターネット上でどれだけISPに権限を与えるかというガバナンスの問題でもある。

この問題に対し、電気通信事業者４団体は、2008年５月に「帯域制御の運用基準に関するガイドライン」（以下、ガイドライン）を策定し、対処することとなった。ガイドラインにおいて帯域制御とは、「ISP等が自らのネットワークの品質を確保するため、特定のアプリケーションや特定ユーザーの通信帯域を制限すること」と定義された。手法としては、①アプリケーション規制（特定のアプリケーション〈P2Pなど〉の帯域をネットワーク全体の○％までに制限）、②総量規制（ある利用量の基準を超えたヘビーユーザーの通信帯域〈速度〉を制御）――がある。ガイドラインに従って帯域制御が実施された場合、電気通信事業法の通信の秘密、利用の公平規定を犯さないと判断されることが期待されるとする。

同じくネットワークの中立性が議論されている米国では、2008年８月、FCC（連邦通信委員会）は「コムキャスト（米国最大のケーブルテレビ会社）決定」で、「特定のアプリケーションに対してISPが差別的取り扱いをすることはできない」とした。コムキャストはこの決定を不服として訴訟が提起されていたが、2010年４月６日、裁判所はFCCの決定を無効とした。しかし、その理由は「FCCの権限外事項である」という門前払い的な判決で、実質論を議論したわけではない。議会ではネットワークの中立性に関する法案も提起されており、規制緩和論者・消費者保護論者間の対立にFCCのブロードバンド普及促進政策もからみ、今後も論争が継続する見込みである。

### （3） 管理網の問題

インターネットが参加者のIDを必要としないのに対し、IP技術を利用しながらIDを管理し、悪意ある参加者やプログラムを排除

する網がある。サイバーセキュリティがインターネットの存立を脅かす課題であるとすれば、これを解消する網が求められるのには理由がある。

過去、参加者を管理するパソコン通信が隆盛した時期があるが、これはWWWなどの豊穣で斬新なアプリケーションを生み出すことができず衰退した。

モバイルネットワークは、現時点ではIP網ではないが、インターネットに接続する管理網である。iモードは通信事業者の垂直統合ビジネスモデルとして成功を収めている。モバイルネットワークは、通話者の位置情報を常に監視していることに特質がある。

通信事業者をバイパス（迂回）して、コンテンツ・端末プロバイダーによる垂直統合ビジネスモデルを提案したのがアップルの「iPhone（アイフォーン）」である。同社はApp Store（アップ・ストア）というシステムを運用しており、利用者がiPhoneプラットフォーム上で動作するプログラムを開発・販売できる。これにより、プラットフォーム上で、一般のインターネットにあるように、ユーザーがアプリケーションを草の根的に自由に開発するような革新性を活用しようとしている。グーグルのAndroid（アンドロイド：携帯電話用OS〈基本ソフト〉）や、アマゾン・ドット・コムの電子書籍端末「Kindle（キンドル）」も、基本的にアップルと同じ類型の管理網型のビジネスモデルといえる。

一方、現在、通信事業者主導の管理IP網としては、前述のNGNが展開中である。NGNは、通信主体の属性を「プレゼンス情報」として網に組み込み、さらに網をオールIP化したものである。IPv6によりアドレス付与をしており、網自体にサービス品質確保機能、セキュリティ機能を有している。NGNはインフラ全体の改造計画で、時間と資金を要する一大事業（比例原理が強い）である。これはiPhoneなどのアプリケーション・端末主導の柔軟な管理網（べき乗原理が強い）との違いであり、今後の両者の展開は見ものである。

またこの動きは、インターネットの基本思想であるEND-END原則に対し、通信側がインテリジェンスを通信網側に取り込もうという動きでもある。ある意味、通信を土管とするインターネットの設計思想に対する通信事業者側の反転攻勢と見ることも可能である。

インターネットが社会で不可欠になるにつれ、インターネットでは不可避な安全性・安定性の問題を解決するため、管理網上でサービスを展開する動きは強まっている。特定の安全保障通信に関しては管理網の必要性は疑いがないが、管理網が一般インターネットを駆逐する事態は、将来のICT（情報通信技術）の可能性を狭めるという主張もある。インターネットの活力の源泉は、プラットフォームを含め、参加者の自由なイノベーションであり、管理網の場合、プラットフォームを囲い込むことでイノベーションの余地を狭めることとなるからである。今後、管理網と自由な網との共生状況の展開を注視していく必要があろう。

### （4） IP網の構造変化（トラフィックの変化）

#### ■CDNの台頭

インターネットでは、従来、国際的に「Tier1」と呼ばれる支配的ISPの接続方針がトラフィックの構造を決定しているとされ、

Tier1の運営協定と料金が私的な国際レジーム（制度）と化しているとの批判もあった。Tier1は、どのISPに対してもトランジット料を支払わないISPとされ、世界で10社から12社存在するといわれている。このTier1がトラフィックのハブというのが、従来のインターネットの構造であった。

しかし、2009年秋、NANOG（The North American Network Operators' Group）47会合で発表された「2009 Internet Observatory Report」（ミシガン大学などが、過去５年間110カ所のネットワーク内にある2949のルーターからのデータを解析）によれば、重要な変化が起きている。

- ５年前には、トラフィックの大半はTier1が支配していたが、現在は大半が、大規模コンテンツプロバイダー、データセンター、CDNなどからエンドユーザーに直接流れる。このためTier1事業者は、接続業務からクラウドコンピューティング、ホスティング、VPN（仮想私設通信網）業などへの転進を図っている
- ５年前、トラフィックは多くのWebサイト間に平均的に分布していたが、現在では30あまりの「ハイパージャイアント」（グーグル、マイクロソフト、Facebook〈フェースブック〉など）にトラフィックの30％が集中している
- P2Pのトラフィックは減少している
- インターネットの主要収入は広告であり、トランジット料ではない

ここでCDNの支配的事業者であるアカマイ・テクノロジーズ（Akamai、以下、アカマイ）について見てみよう[注4]。

- コンテンツの提供者はアカマイと契約して、アカマイがインターネット上で運営する多数のキャッシュ（一時保管）サーバーまたはネットストレージ（記憶装置）に負荷を分散することにより、Webサイト閲覧の高速化と顧客のWebサーバーの負荷軽減を実現できる
- 顧客を収容するDNSサーバーにアカマイのサーバーネームを追加し、アドレスクエリ（質問）に対してアカマイのDNSサーバーが、該当キャッシュサーバーまたはネットストレージのアドレスを返す。これにより本体のWebサーバーへのトラフィックを分散する
- 2008年現在、世界70カ国以上のISPやIXに、４万台以上のアカマイのサーバーが稼働している。日本国内では、30拠点に約2000台のアカマイサーバーが設置されている（ヤフー、任天堂などが顧客）

つまり、従来のインターネットのトラフィックの支配者が、Tier1からCDN事業者に交代したのである。トラフィックはTier1をバイパスし、最寄りのISPからCDN事業者に直接流れる。インターネットにおける支配力は、ISPからコンテンツ事業者に移行している。

**■グーグルのGoogle Public DNS**

2009年12月にグーグルは、「Google Public DNS」というサービスを開始した。インターネットに接続した端末は、DNSリゾルバーという機能でDNSサーバーと交信する。通常、各端末は、ISPが提供するDNSリゾルバーの設定により、ユーザーはそのISPのDNSサーバーと交信する。グーグルの新サ

ービスは、ユーザーが自分でDNSリゾルバーの交信先をGoogle Public DNSに変更しすることにより、ISPではなくグーグルのDNSがIPアドレスを検索することを提供するサービスである。

グーグルは、「グーグルが世界中に展開しているデータセンターのアドレスクエリのキャッシュを利用することで、アドレス取得速度の改善を図り、また、クエリの事前取得（prefetch）によりIPアドレスに関するDKAも防御できるため安全性が向上する」としている。

またグーグルは、自社が持っているコンテンツキャッシュ情報も利用して、コンテンツキャッシュの最短距離のアドレスを提供すること（通常はCDNが行う作業）で、アクセス自体も改善できるとする。

これはグーグルが、検索サービスを背景に形成した自身の世界規模の超巨大バックボーンネットワークを利用して、世界最大のDNSを構成し、さらにコンテンツの配信の効率化を図るCDNを提供するということである。前述したように、DNSは国際的管理の焦点になってきたサービスである。グーグルはこれを支配しようとしている。すなわち、グーグルは、コンテンツ・プラットフォーム層の検索サービスの圧倒的なシェアを背景に、DNSとCDNの提供により、IP網のルーティング（最適経路送信）までをも支配しようとしていると解釈できるのである。

グーグルはすでにAS資格を持ち、ほとんどのISPと接続協定を結んでいる。つまりユーザーのトラフィックは、ISPの多段階接続ルートでなく、すでにユーザーに接続するISPから、グーグルが把握するキャッシュコンテンツへという短縮経路になっている。Google Public DNSは、グーグルによるルーティング支配をさらに強化するものである。

Google Public DNSが実際に普及するかどうかは課題である。個人の場合は自らセッティングしなければならず、手間がかかる。しかし、ISP自体が自前のDNSサーバー設置をあきらめ、グーグルのDNSを利用することになれば、普及が急拡大する可能性がある。なぜなら、DNSサーバーへの投資を免れたISPは、他ISPに対してコスト競争で優位になるからである。Google Public DNSの普及が進んだ場合、ISPはグーグルへのトラフィックを貢ぐだけの存在となる可能性がある。

インターネットの構造という観点からいえば、回線網、IP網、コンテンツ・プラットフォーム層という階層構造が変質し、コンテンツを掌握する者がIP網の運用管理の事実上の支配権を握る変化ということになる。利用者が求めるのはコンテンツであってネットワークではないことから、ネットワークの整備が終了すれば、焦点がコンテンツに移行することは自然の動きといえる。

しかし、検索サービスで圧倒的なシェアのグーグルがさらに巨大になり、インターネットの支配力を強める事態をどう考えるか。グーグルといえば、世間の焦点は電子書籍事業に当たっているが、本件のような目につきにくい分野でも着々と支配力を強めている。問題は、これらの課題を検討するためのデータが不足していることである。インターネット・ガバナンスの透明性確保の観点からは、CDNなどの実態解明のためにも、ISPに各種データの開示または提出義務を課すことが重要となる。インターネット・ガバナンスは、

べき乗原理を踏まえ、インターネットにおける私企業の独占力をどう管理していくかという新しい課題に挑戦しなければならない。

## 4 インターネットを中心にすえた総合的な情報法制

冒頭で述べたように、いまやわれわれの生活はインターネットなしでは成り立たない。しかし、果たしてわれわれはこのインフラを適切に統治（ガバナンス）しているだろうか。

WSISではインターネット資源の一国支配が問題とされた。その後の国際的な努力により、DNSに関しては多様な利害関係者による制度の管理体制が実現した。しかし、未解決の課題も多く残っている。

またわれわれは、インターネットがもたらす可能性を十分活用しているだろうか。この点、わが国は、ブロードバンドなどのインフラ整備では進んでいるが、医療、教育などの利活用においては遅れているのが実態である。また利活用の促進には、OECDが指摘するように、各種の政策策定に当たってインターネットが系統的に組み込まれることが必要である。

インターネットの利活用促進の前提となるのが、インターネットをガバナンスの利いた十分に信頼できるものにすることである。このためには、ネットワークの安全性もさることながら、「コンテンツ＝情報自体」の保護にも取り組む必要がある。ユーザーが望むのはコンテンツであって、ネットワークは手段にすぎない。

この点、従来のわが国の法制は、情報を真正面から捉えず、設備・サービスの面から間接的に規制してきたことが問題のように思われる。情報自体は窃盗の対象とはならず、システムへのアクセスを違法とするにとどまっている。盗聴無線装置の設置も野放しである。また、情報を統一的に所管する官庁がないため、越境データ流通や個人情報保護法制などでは、国としての制度推進力に限界がある。事実、EUは、日本の情報保護法制はEU基準を満たさず、EU構成国からの日本へのデータ移転は、EU指令による事前規制の対象となると述べている[注5]。

日本の課題は、情報保護のガイドラインはあっても、その実効性を担保する仕組みが不明確、あるいは不備なことである。先進各国は、インターネットによりデータの越境流通が本格化したことから、データ保護への取り組みを強化している。わが国でも、外部監査の強制やデータ保護オンブズマン（行政監察委員）的な仕組みが必要ではないだろうか。

こういう点を含め、今後、インターネットを中心にすえた総合的な情報法制が必要であるとの提言[注1]は傾聴に値する。情報は、物質・エネルギーと並ぶ物理世界の三大基本構成要素である。物質を動かすのがエネルギー、物質・エネルギーを操作するのが情報である。これに、人間の欲望と社会制度の２要素を加えれば、世界の森羅万象の説明枠組みとなる。情報法制は、世界のこうした基本構造に対する認識のもとに整備する必要があろう。

注

1 在日米国商工会議所の提言：2009年10月、在日米国商工会議所は、「インターネット・エコノミーの実現を日本で」と題する提言を行った。日本は米国との間で、過去数々の経済摩擦を経験した。繊維に始まり、鉄鋼・自動車・半導体・電気通信と、そのときどきで米国が重要と考え

る分野が摩擦の対象となってきた。今回インターネットが取り上げられたのは、これが米国、そして世界が重視する分野であることの象徴と考えることができよう。提言自体は米国企業の利益を図ることが目的であるが、たとえば、既存のビジネスモデルや因習的な規制の枠組みにとらわれるあまり、インフラ投資の果実を得られていないという指摘など、日本自身の将来にとっても重要と考えられる論点も提示されている。また、インターネットを中心とした総合的な情報法制の必要性も提言している

2 アルバート・ラズロ・バラバシ著、青木薫訳「新ネットワーク思考――世界のしくみを読み解く」NHK出版、2002年

3 2009年１月末の中央アジアのキルギス共和国でのサイバー攻撃。ロシアの「サイバー市民軍」と称する組織が、同国の80％をカバーする大手ISPに大量のデータを送り込み、サービス不能の状態にする「DDoS攻撃=Distributed Denial of Service attack」を仕掛け、インターネットが数日間にわたって接続不能となった。当時ロシアは、キルギスに対する金融支援やエネルギー関連投資の条件として、同国内の米軍基地の閉鎖を要求していた

4 「Geekなページ」（http://www.geekpage.jp/blog/）あきみち氏によるブログ。「みんなが知らずにつかっているAkamai」2009年４月、「Tier1は秘密結社か」2008年11月

5 EUデータ保護事務官ハナ・ペチャコバ氏。「日本は、個人の私生活にかかわる個人データおよび基本権に関して、十分なレベルの保護を提供している国であるとEUはまだ考えていない。したがってEU構成国から日本へのデータの移転は、『EU構成国各国のデータ保護機関による事前の情報権限付与を意味する指令95/46/EC26条』による」。つまり、日本の情報保護法制はEU基準に満たず、日本のクラウドコンピューティング事業者は欧州展開が困難である。そのほか、フランスのブラックベリー禁止令、カナダではデータ保護に関する懸念から公的機関の米国サービス利用禁止などの動きがある

## 参考文献


1 戸根勤「ネットワークはなぜつながるのか 第２版――知っておきたいTCP/IP、LAN、光ファイバの基礎知識」日経BP社、2007年

2 アルバート・ラズロ・バラバシ著、青木薫訳「新ネットワーク思考――世界のしくみを読み解く」NHK出版、2002年

3 谷脇康彦「インターネットは誰のものか――崩れ始めたネット社会の秩序」日経BP社、2007年

4 ジョナサン・ジットレイン著、井口耕二訳「インターネットが死ぬ日」早川書房、2009年

5 国連WSIS・IGF関連文書

6 OECDインターネット関連文書

7 ICANN関連文書

8 内閣情報セキュリティセンター関連文書

9 在日米国商工会議所「インターネット・エコノミーの実現を日本で」『インターネットエコノミー白書』2009年10月

10 「インターネット政策懇談会報告書」総務省、2009年２月

11 'CYBERSECURITY: ASSESSING OUR VULNERABILITIES AND DEVELOPPING AN EFFECTIVE RESPONSE' 米国上院商業・科学・運輸委員会公聴会、2009年３月19日

12 インターネットサイト「Geekなページ」（http://www.geekpage.jp/blog/）あきみち氏によるブログ

13 インターネットサイト「JBPress」（http://jbpress.ismedia.jp/）に所載のサイバーセキュリティに関する宮家邦彦氏、原田泉氏の諸論考

14 NANOG（the North American Network Operators 'Group ）47, '2009 Internet Observatory Report（http://www.nanog.org/meetings/nanog47/abstracts.php?pt=MTQ1MyZuYW5vZzQ3&nm=nanog47（参考文献12の「Geekなページ」にも解説あり）


## 著者


木全紀元（きまたのりもと）
理事
専門は通信政策