Space Japan Opinion

【本記事の紹介者から】本記事は 2009 年 11 月 16 日にオスロ会という 1966 年の CCIR 第 11 回総会出席の OB 会で発表されたものである。著者の池上先生は，逓信省・電気通信省・電電公社通研を通じて 28 年，京大で 14 年，拓大で 8 年，合計で 50 年間電波の研究に当たられ，現在は京都大学名誉教授，拓殖大学名誉教授であられる(電子情報通信学会通信ソサイエティマガジン,No.6,秋号,pp.4-10，2008 参照)。ここにご紹介する記事について先生は，「通信の中の極特殊な問題で，賛成してくれる人もいるが，多くの人はこんな話は世間に通るのかと思うかもしれない。私は情報網にはずぶの素人であるので，通信網の若い研究者の方々に私の議論の誤りを正して欲しいのが目的である。」とおっしゃっている。皆様のディスカッションを期待します。(飯田尚志，JFSC 特別顧問)

世界通信網の将来を再考察する
― IN ・疑問から確信への一歩 ―

池上文夫

〔序言〕

Internet すなわち Internet Protocol 網（以後 IP 網と略称）の基本的欠陥“Best Effort”が議論されない摩訶不思議に疑問を感じ，これまで数年に亘り話題としてきた。最近の NGN（※1）の動きや本年 5 月のオバマ大統領発言の報道（※2）から，この疑問は確信へと一歩近付き,IP 網問題の再考察を素人なりに試みる。回線交換網(旧網)が突然 IP 網に変わった論理の飛躍は何故起こったのか。この論理の不連続の空白を埋め，将来の世界網へと繋げられるのか。世界でそして日本でも IP 網から新網への動きがあるのに,一般では IP 網の欠陥の議論は殆ど無い。今，何かが抜けている。再考察は IP 網が早晩破綻すると予告する。我々は今，何をすべきか。通信網の分野では素人で年寄りの，通信網の将来についての余計な心配は相変わらず終わらない。

1. 問題の提起

米軍の核攻撃対策網として始まった ARPANet は，米国の大学・研究所の計算機網（1969）を経て，日本でも大学間計算機網（JUNET，1984）となる。米国で Internet として商用化（1988）後は，世界の公共網の一部として爆発的拡張を続け，遂に旧網に代わる将来網の候補とされている。その理由は，旧網に比して特にディジタル通信が便利で安価な点にある.一方で IP 網には,網の Quality,Reliability，Security（QRS）を保証できないという重大な欠陥があり，ここではこの点に焦点を当ててみる。IP 網の契約では，サービス提供者はサービスに最善の努力を払えば，QRS の保証義務から解放されると決められている。ここでは，この IP 網の本質を“Best Effort”（最善の努力）の名で呼んでいる。この本質こそ IP 網が QRS に対して責任を負わないという，深刻な基本的欠陥を生むことになる。

問題の一つは Security にある。厳しい秘匿性が要求される情報に対して，IP 網は秘匿性を保証できず，通信網の資格を欠く惧れがある。もう一つは QR の保証が無いことである。網の特性を明確且つ定量的に表示できず，論理性の欠如，あるいは非論理性とも言えよう。Security は定量的表示が難しいが，QR の定量化は公共通信網に

は不可欠である。

【Security の問題】

昔の回線交換網は通信の Security 確保という大前提の上に作られた。通信開始の前に　送受信端末間に専用回線を確保，通信中に外部から妨害を受けることは原理的にない。

他方，Open IP 網は Security を保証しない。但し，Closed IP 網として使えば高い Security を確保できるが，フィルタや fire wall 経由でも一旦 Open 網と接続すると Security の確保が再び重大な課題となる。一般ユーザの Virus・迷惑メールから公共的機関への悪質な Cyber Attack に至る各種攻撃の被害は現在も頻発している。対策ソフトにより回避できるものも，次々に新手が出現するので，常に後手々々の“いたちゴツコ”となる。

また，IP 網の各種サイトで自由な意見の開陳が可能であるが，不用心な自己開示や匿名の他人誹謗などで，非正常な人間関係から悲劇的結果を生む事件などが頻発している。これは人間の倫理の問題であるとも言えるが，Open IP 網の本質的なリスクに対する対策は技術の責任であり，また一般ユーザへの強い警告を怠ってきた社会にも責任がある。

政府や企業への Cyber Attack はかなり重大な被害もあったようだが，その具体的な内容の公開は憚られていた。これはネット業界発展への影響や米国への配慮もあったと思われる。通信技術者の多くも「*この程度の被害は新技術には付き物で大多数のユーザは十分喜んで便利に使っている*」と，気付かぬ振りをしていたのかも知れない。オバマ大統領が米国での被害を公開（※2）　して以来，被害実態の開示が始まりつつあるようである。

【非論理性の問題】

回線交換網は，人類が数世紀に亘り創り上げた学問(数学・物理学・統計学・電気電子工学・通信工学など)に基づき，要求される規格特性（QRS）　を満たす通信網を計算し設計・実現できる段階に達した。全て完全とは言えないが，その背景には網の中の交換・伝送などの物理的現象に対する普遍的な理論の裏付けがあり，それを基礎として，各種の広範な応用に対しても，必要な特性を計算して求めたり，新しい道を探し求めることもできる。

一方，IP 網は，パケット接続の簡単な抽象的論理のみで，パケット交換網の基礎となる普遍的理論が無く，伝送の損失や遅延特性，トラフィックの輻輳による交換の不接続確率など，網の物理的な諸特性 QR の定量的評価はできない。網特性の評価は，実際の網での通信実験で試行錯誤を繰り返す以外に方法は無く，従って経済的最適設計もできない。

すなわち IP 網は，その背後に確立した理論が無いため，合理的なシステムの設計・建設・運用ができず，網の改良や拡張など発展的な研究も論理的にはできない。それなら，何故そしてどうして，現在の IP 網が存在しているか？　答えは簡単である．それは，過去の回線交換網を借用したもので，IP 網のため特別に設計された網ではない。今の IP 網とは，それ自身では自立ができない，言わば“やどかり”のような存在で，普通ならば技術とは呼べない，常識を超えた摩訶不思議な技術である。

2. IP 網の現状と将来

IP 網が致命的障害も無く利用されてきたのは，旧網の伝送路を借用した実用化初期のサービスが主に kByte，MByte 程度のメールやファイルなどで，トラフィック量に

比べて伝送路の伝送速度（Gigabps 程度）が十分速く，網の輻輳障害は殆ど起こることがなかった。

しかし今は，メールの 90% は迷惑メールと言われ，また情報量が GByte 程度の動画像を扱う YouTube や，更にファイル交換ソフト Winny などによりトラフィックは急激に増加し，光ファイバやルータの能力を超える確率が増えている。総務省の資料によれば，2007 年のトラフィック量は Terabps 程度に達し，Moore's Law （半導体 IC 集積度の増加則：2 倍/18ー24 ヶ月）の程度で年々増加，網の障害頻度も顕在化し，ISP（Internet Service Provider）は異常に大量の情報量を発信するユーザに警告したり，状況により解約も考慮するなど，発信情報量の規制を実施していると報じられている。(※3)

近い将来，動画像を扱う一般ユーザが益々増加し，網全体のトラフィックがムーアの法則で増加する時，網に要求される処理能力の，現在に対する予想倍数を表 1 に示す。

表 1 IP 網に必要な処理能力倍数（現在比）の経年変化

Case A: 2 倍／2 年の場合

経過年数	2	4	6	8	10	12	14	16	18	20
能力の倍数	2	4	8	16	32	64	128	256	512	1024

Case B: 2 倍／1.5 年の場合

経過年数	1.5	3	4.5	6	7.5	9	10.5	12	13.5	15
能力の倍数	2	4	8	16	32	64	128	256	512	1024

表 1 から，5ー7 年後には現在の光ファイバやルータの必要能力は現在の約 10 倍程度，10ー13 年後には約 100 倍，15ー20 年後にはトラフィックは Peta（10^{15}）bps の程度に達し，システムの能力を現在の 1,000 倍程度に増す必要がある。

光ファイバやルータの現状や将来の詳細は知らないが，それらの容量や能力が表 1 の要求を満足しない場合には，IP 網は破綻することになろう．更に，現在の電波による TV 放送は遅かれ早かれ IP 網による放送で置き換えられると考えると，実時間の streaming の TV 映像信号の受信や配信は，網の破綻を更に加速する可能性もある。

光ファイバやルータが表 1 を満足する時にも「*Internet の伝送コストは無視できる*」 という神話は通用するだろうか？ “技術と呼ぶに値しない IP 網”は，トラフィックの急増問題を解決する方法の論理的な研究さえもできない。次世代の網（NGN その他）の対策もあるが，まだ十分な見通しは無い。Internet Protocol を用いる限り，通信網は将来の予測も，将来への対応もできないことを意味する。問題の根本的な解決には，一旦基本に立ち戻り，網の基礎的な検討から出発して，問題を論理的に再考察する必要があると考える。

3. 回線交換網と IP 網の性格の比較

回線交換網の動作は物理的にも明瞭で非常に理解し易いが，IP 網の動作は素人にとって物理的に理解するのは甚だ難しい。それは，IP 網には数学的物理的に表現できるような論理性が乏しいからである。再考察のためには，せめて IP 網の抽象的な性格だけでも理解することが望ましい。回線交換網の周知な性質を基準として IP 網の性質を理解するために，両者の主な性質を比較して表 2 に示す（表中の赤字は夫々の網の弱点を表わす）。

注目すべきは，どの重要な項目も両者が互いに背反的な性質を示すことである。

表 2 回線交換網と IP 網の主要特性の比較

	回線交換網 （旧網）	Internet Protocol 網 （IP 網）
基本的 動機付け	基本サービス：電話と電信を中心とする公共用サービス Security が第一優先	網の一つのノード局が不能となっても網全体の機能破綻を防止できる 計算機網の実現
動作の構造	集中制御方式：中枢交換機が網の動作を監視・制御する	自律分散制御方式：各端末自身が網の動作を制御する
網の Security	２端末間を結ぶ専用回線により原理的に 100% Security 確保	パケット交換網での時分割多重信号の論理的分離は外部からの妨害に対する Security 保証が困難
網動作特性 (Q and R)	信号伝送経路が確定し固定なので QR は理論的計算可能	信号伝送経路が時間的に変化し QR は確定が困難
ﾄﾗﾌｨｯｸ輻輳による不接続率	信号伝送経路が確定的なので Erlang の式により計算可能	パケット交換での基礎理論は未だ得られていない
情報形式に対する融通性	ディジタル情報の各種アプリケーションへの融通性に欠ける	各種の広いディジタル情報形式に対して極めて優れた融通性を示す
網のコスト	伝送効率低く伝送コスト高い 交換機能複雑で交換機高価	伝送効率 100%可能で伝送コスト低い交換機能が単純で装置は低価格

4. IP 網問題の発生源を探る

“研究”段階で新技術の実現性が十分高いと確認されると“実用化”段階へ進む。実用化には多くの人材･経費を要し失敗は許されないので，実現性の確認のみならず，その技術を実用した時に社会に与える影響についても十分な検討を行う必要がある。通信の新技術が社会にどれだけ正と負の影響を与えるか，20 世紀後半以来の通信の急速な進歩は，我々に有益な忠告を与えてくれた。回線交換網から IP 網への通信網の基本論理の不連続な飛躍は何故起こったのか？ 今，「*(R&D における) 研究と実用化は厳密に区別すべし*」という先人の教訓を改めて思い起こす。

【IP 網の実用化における誤り】

IP 網は，従来無かった新原理により新技術が生まれた例の一つである。通信分野の研究者が過去と全く異なる新原理の技術を開発する場合，技術の継続性には大きな問題は起こり難いだろうが，通信とは異なる分野の研究者が通信の新技術を実用化する場合には，過去の通信技術や技術環境などの知識・経験の不足で，不連続性が起こる危険がある。

IP 網の場合，研究の途中段階，すなわち，その技術の特徴的な性質や実現性が十分に把握されていない段階で，実用化に入るという誤りを犯した。その原因は・・・・

(1) IP 網は米国の核兵器対策の計算機網として考案され，初期の研究者達は計算機・情報の専門家が主体で，通常の通信網に関する知識や実経験が不足したと推察さ

れる。例えば，計算機網が一般の通信網にも十分使えると単純に誤算したかも知れない。

(2) IP 網の非論理性のため将来予測ができず，これが実用に耐え得るか否かの判定には，ARPANet での試用以外に方法は無かったと推察される。試行結果は良好であったが，その将来性を論理的に予測する方法も無く，適切な検討無しに実用化段階に入った。

(3) 当時最高の通信技術をもった AT&T は独禁法で FCC によりデータ通信の研究を禁止され，この研究プロジェクトの初期から参加できなかった。実用化の哲学の本家である Bell 研究所のメンバーが参加していれば，この誤りは回避できた可能性が高い。

(4) 世界の通信網研究者の中には IP 網に対して批判的な傾向もあったと推察されるが，当時，米国の FCC は IT の新技術に対して強力な政治的・経済的支援を与えた。

(5) 更に補足すれば，20 世紀の後半から従来の ITU による de jure 標準に不足を感じて，de facto 標準への志向が特に IT 技術の分野で強く，政治における米国の UN 軽視と相俟って，IP 網技術も de facto への不連続な飛躍に走ったと推察されよう。

こうして，公共通信網としての IP 網の研究が未成熟な段階で実用化段階に入ったが，当初のサービスは前述のようにトラフィックが少なく，通信障害は殆ど発生しなかった。この良好な結果は将来の楽観的予測を生み，表 1 の将来リスクを無視したと思われる。

最近の急激なトラフィック増に対して，ISP が大量の情報を発信するユーザを規制する程度の現在の対策（※3）では，効果的な防止は困難であろう。何故ならば，この“Virtual World” は法律も警察も無い性善説の無法地帯で，“現実社会”の悪意ある行為を規制・探索し罰する法律すら無いからである。通信に携わった一員として，摩訶不思議な通信技術への適切な判断の時期を逸し，リスクのあり得る IP 網を全世界へ拡張する怒涛の奔流が全てを流し去りつつある現状に，深い慙愧の思いを禁じ得ない。

【世界金融破綻の教訓】

今，我々は百年に一度の大不況の最中にある。その原因はノーベル賞受賞者の金融工学に発したと言われる。この場合バックボーンの理論はあったが，リスクを隔離して回避する推計論的手法を理解できない運用者・金融業界・行政の不手際による破綻と言われる。元来，金融の業界は“論理無き世界”で，“人間の欲望とリスクとの戦い”とも言われている。その中では，ノーベル賞に値する金融工学の論理ある説得力さえも，この場合殆ど無力で期待される結果を実現することはできなかった。

現在の IP 網には理論が存在せず，“Best Effort” のリスクも周知ではあったが，IP 網　事業者の欲望による暴走を制することは出来ていない。論理無きモノが膨らみ続けると必ず破裂する。全世界の通信網が IP 網となった時，この網が金融破綻の二の舞を演じることを，年寄りの素人は心配する。通信網破綻の影響は金融破綻よりも大きく，世界の人々の生活に更に広く深い影響を与えるかも知れない。

“下衆の後知恵（げすのあとぢえ)”と笑われるだろうが，もし IP 網の初期段階から AT&T の技術者がこれに参画していれば，IP 網の姿は今とは全く違う形になっていたであろう，と考える度に，今更ながら残念に思う。がしかし，今からでも遅くはない。

5. 望ましい将来の通信網の考え方

望ましい将来の通信網は何か？ 表２の旧網と IP 網の特質は背反的で夫々一長一短。両者の長所を合わせて一つの網を見付ける，あるいは足して２で割るなど，全く背反的な２つの網を組合わせても良い結果は無理と思われ，全く新しい第３の方式（“Clean Slate”に描く）も必要と痛感する。この難問は一筋縄では解決できないと十分に知りながら，せめて解決へのヒントでも，との淡い期待で素人の考察を続けてみよう。

【両網の基本構造と網特性の関係】

表２で両網の構造的背反性は「動作の構造」の項目にある。すなわち，回線交換網は中枢交換機が網を監視制御する集中方式であり，IP 網は端末による自律分散方式である。 集中方式は，交換機が網の状態を監視し全貌を常に把握でき，必要が生じた時は直ちに対応して網を自動的に，あるいは人為的に，良い方向へ制御できる可能性がある。

他方，IP 網は，一つの交換機が破壊されても網機能を維持できる自律分散制御方式として考案され，網全体の把握機能も制御機能も必要が無い。従って IP 網のノードには監視制御機能の無いルータやサーバを用いるので，交換装置のコストを著しく安価にできる。両網は，夫々，背反的な目的に適合する機能をもつシステムを目指してきた歴史がある。

ARPANet の歴史の中で，偶々分散方式の計算機網を一般のディジタル通信網として試用したところ，安価で便利な通信が可能と分かり，これを実用に供した。当初，分散方式の IP 網は順調に動作していたが，利用条件が広がるにつれて各種の不都合な現象が次々に発生，その度毎に対策を重ねてきたが未だに完結できず，その対応に苦慮しているのが現状であろう。我々は今も尚，進むべき方向の探索を続けている．

回線交換と IP の２種類の網は，夫々が得意とする目的に適切に利用すれば，殆ど大きな問題無く利用できる筈である。これは望ましい考え方へのヒントの一つと言えよう。

【“Best Effort“の意味】

IP 網の“Best Effort”はパケット交換の産物で，パケットスイッチは２端末間の「空きルート」を選んで接続するので，信号経路は網全体の構成と情報パケット群による偶然の結果として時間と共に変化する。光ファイバ伝送路の損失は経路長に係わらず殆どゼロと仮定できても，各パケット信号の伝送時間は決定できない。仮に情報の経路を統計論的に予測できても， トラフィックの輻輳による不接続確率を求めるのは非常に困難であろう。網の各種の特性 QR を求めるには，恐らく多大の難関があると思われる。

公共の通信網でも計算機網でも同様であるが，網の設計・運用を論理的に行うには交換・伝送の QR を評価できねばならない。しかし，パケット交換網はそれが非常に困難という重大な欠陥をもつ。最高の問題解決法はパケット交換の体系的な基礎理論を開発するにある。素人の年寄りは，若き俊秀がこの難問を見事に解き明かすのに期待したい。

さもなければ，“Best Effort” の下で生まれる無数の課題を一つ一つ取除くか，あるいは“Best Effort”の生みの親であるパケット交換そのものを見限る以外には良い方法は無いかも知れない。第３の網 “Clean Slate に描く”の発想はここから生まれたのであろう．

このように，“Best Effort”の影響を完全に取り除くのは大変難しいと思われる

が，その影響を受けることが無いか，あるいは影響が小さい使い方はあり得る。例えば ARPANet の場合のように，信頼できる仲間同士の完全に Closed な社会の中での通信の場合には，Security の問題は回避できる。また，IP 網のもつ低コスト性や融通性を特に重点的目標とする利用には適用も可能であろう。現状の，全ての通信を一つの IP 網で処理しようとする世の動きに,”無理（理が無いこと）が通れば道理引っ込む“の諺を思い起こす。

これも年寄りの余計な一言。“Best Effort” という言葉は，IP 網の欠点を指摘された時,「*それは”Best Effort”だから仕様が無い*」と，技術が努力もせず大きな顔をしての逃げ口上に使うべきでない。技術力不足を恥じつつ，止むを得ず謙虚に使うべき言葉である。

【コストの問題】

回線交換網は原則 100%Security を保証し IP 網は各種のディジタル情報に対して安価な通信を可能とする。ならば,厳しい Security が必要な目的には回線交換網を，安価と便利の目標には IP 網を使うのが，最も合理的で而も最も単純な方法で，悩む必要は全く無い。

回線交換網は IP 網よりもコストが高いという批判には，Security の保証に対するコストとして当然であるとも答えられる。最近の新技術を用いて回線交換機のコストを下げる方法もあろう。それでもまだ高価過ぎるならば，Security のコストを真剣に再考察する必要がある。貴方はこれまで Security のためにどれ位の金と手間を掛けましたか？ それで本当に安全になったと感じますか？ Security 関連の事件は今もなお毎日起こっています。貴方はこれから先もこの問題にどれだけの経費と手間を掛ける積りでしょうか？

コストは非常に重要な要因だが，コストと Security を単純に秤にかけるのは大変難しい。今，世界は IP 網の Security 対策に四苦八苦だが，その損失総額（研究費・対策費・人件費・時間等々）は世界全体でどの程度か? この状態が今後も続けば，そのコストは全く測り知れない。更に世界には，Security が無条件でコストに優越する場合もあるだろう.

【コストと責任の配分問題】

もう一つ，コストに関する考え方がある。それは“全通信系のコストの配分”である。回線交換網では，通信運用者は殆ど自己完結型に近い通信系を所有し，全てのサービスに対して殆ど全責任を持っていた。これに対して，ユーザは端末装置のみを所有し，その操作だけで全ての提供サービスを享受でき，そのサービスに対する通信料金を払った。

他方，IP 網では，通信運用者がユーザの端末装置以外の全設備を所有する点は集中方式と同じであるが，自律分散方式では網全体のサービス特性はユーザの端末装置の特性に大きく依存するので，IP 網運用者のサービスに対する責任が“Best Effort”の部分（すなわち殆ど無責任）となる理由であり，非常に重い責任がユーザに課せられる。

ユーザの分担する端末関連コストは，計算機と各種周辺装置類，ソフトウエア類，IP 網の利用料金，妨害対策ソフト等々があり，端末装置全体の維持に関する責任の経済的・精神的負担は非常に大きく，ユーザは通信系運用の QRS の責任の大部分を“自己責任”として負う。これも回線交換網とは全く背反的である。‘IP 網は安い’と言うが，保証の無い QRS というサービスが安いのは不思議でない。勿論，この端末装置類は他の計算機利用と共用であるが，それを考慮してもこの責任は一般ユーザには大

きな負担と言えよう。

更に“Best Effort”の自律分散方式は，“素人”のユーザ（全世界で数十億人?）がQRSの維持に莫大な経費とエネルギを消費（ロスも多い）する一方，運用側の“極めて高度な技術プロ”集団はQRS に対して大きな責任は負わない。この責任分担は，専門技術者集団に網を改善するモチベーションを与えず，非効率極まりない矛盾システムである。更に全世界のユーザの諸装置は地球の CO_2 に対するDigital Dilemma の原因ともなる。

【IP網の料金制度】

IP 網の摩訶不思議は，その料金制度にも端的に表明されている。本来，通信料金は，伝送情報量，伝送距離，利用時間などに依存する“通信のコスト”に常識的な利益を加えて課金する従量制が，通常の社会の経済原則であろう。現状の定額制はこの経済原則に全く反する。どの程度に反するかと言えば,kiloByte のメールとGigaByteの動画像とが同額の料金と課金されるが，両者の情報量比は百万倍である。隣家へのメールと地球の裏側へのメールも同額だが，両者の距離比も百万倍である。この百万倍の不公平は初期から現在もなお続き，ネットの主張する“fairness”の哲学とは全く反すると共に，これこそが迷惑メールなどの悪質な利用の跳梁跋扈を許している最大の原因の一つでもある。

この極めて不合理な料金制度を用いざるを得ない原因もまた“Best Effort”に端を発し，QRS の評価不能のため正確なコストの評価も不能となる。これは望ましい網へのヒントというよりも，正常な課金制度は望ましいシステムの必須条件となるであろう。

6. 望ましい通信網への例題

以上，長々と将来の通信網の在り方について考察してきたが，その実現のために今我々が考えるべき項目を示すと次のようになろう。

(1) 現在IP網の是非を論じている余裕は無い。数年のうちに破綻の危険がある。その破綻を停めるか，その時期を遅らせるのが焦眉の急であろう。(破綻の防止，または先送り)
〔実行案〕：大量な情報発信の規制（法律と組織）

(2) 将来の望ましい最終網の完成には最低でも 10 年以上の年月が必要と思われるので，破綻以前に早急な新しい暫定網の実現が必要である。（暫定網の至急実現）
〔実行案〕：安易に実行可能で有効な暫定網（例えば下記の組合わせ方式）

(3) 望ましい将来の最終的な通信網を早期に実現する（最終網の早期実現）
〔実行案〕：例えば全く革新的な新世代ネットワーク

【組合せ方式による暫定網の案】　（皆さんの名案を期待します）

《案１》回線交換網・ClosedIP網・OpenIP網を使い分ける
回線交換網：100%のSecurity を要する超重要業務（例えば，外交・軍事・警察など）
ClosedIP網： 高いSecurity を要する重要業務（例えば，ライフライン・重要産業など）
OpenIP網：“Best Effort”の一般通信

《案2》 ClosedIP網・OpenIP網を使い分ける
超重要業務に必要なSecurityがClosedIP網で確保される場合に用いる。 超重要および重要通信は夫々独立な別のClosedIP 網を，一般通信も別のOpenIP網を使う。

《付帯条件》一人のユーザが重要度の異なる３つあるいは２つの網を利用する場合，

各網は論理的隔離でなく物理的に隔離する。（１卓３端末方式，　あるいは１卓２端末方式）

７．結言 最終的な通信網の研究へ

IP 網も回線交換網も我々の最終目標になれないことが，今回の再考察の結論の一つである。　２つの背反網を組み合わせ一つ網とすることも合理的でない。第２の結論は，現在の IP 網は Closed および Open 方式の特長を生かして当面の暫定方式に利用できることであろう。但し，その本質的なリスクに対する十分な規制は不可欠である。

我々が最終的な網として目指す研究の目標は，統一網であれ，複数の分割網であれ，いずれの場合も，所要 Security と論理的設計・運用が可能な網でなければならない。我々は先ず現状を否定し，現在より遥かに大きな関心と研究のエネルギを，暫定方式と究極方式に注がねばならない。これがこの再考察の最も重要な結論であろう。

【その他の関連課題について】

① 現在国内には将来の通信網の戦略を研究する機関が無い。そのために日本版 FCC の新設が必要である。 最重要目的は，国際的組織との共同作業により，現在網の破綻以前に，世界共通の暫定的な標準網方式を決定することにある。

② 現 IP 網の破綻以前に，上述の世界共通の暫定網の実行に必要な各種 Security 対策のために，国際的な規制の法律や警察活動組織の実現が必要である。

【謝辞】

この記事の本誌への投稿についてご高配を賜り，英文への翻訳に関しても種々のご配慮を頂いた飯田尚志博士に厚い感謝の意を表します。また英訳の作業に飯田博士と共にご援助を頂いた若菜弘充博士に感謝申し上げます。この記事の裏で常に Financial Times 紙の最新情報をご提供頂いた友人の岩噌弘三氏に変わらぬ感謝を致します。

【参考資料】

※1：電子情報通信学会東京支部シンポジュウム「2020 年代に向けた新世代ネットワークの展望と課題」，青山友紀他，2008.10.9. 日本での新世代ネットワーク(NGN の次の世代のネットワーク NWGN(NeW Generation Network)の研究構想と関連技術など。

※2：“オバマ大統領サイバーの脅威に反応” オバマ政権の関連 Agenda の重要度順位を高める。産業界の損害：US$1000bn（邦貨 100 兆円)。 CyberAttack による軍・政府の重要情報の漏洩。(Financial Times 2009.5.30)　(情報提供：岩噌弘三氏)。

※3：”ネット占有制限へ指針−プロバイダ業界渋滞緩和策−“，朝日新聞 2008.5.28。

この小文は，例によって通信網は専門でない素人の年寄りの余計な心配事です。どうぞ忌憚のない誤りのご指摘，ご批判，ご意見をお願い致します。

あとがき

【今，想うこと】

今回の記事の内容を 2009 年 11 月オスロ会で述べてから 1 年以上になるが，その間に世界の状況は大きく変化した。その一つは当時指摘した IP 網の定額料金制度に欧

州各国で反対論が出始めたこと。もう一つは，当時小規模だったサイバー攻撃が世界の恐怖となるサイバー戦争の規模に成長したとの報道である。これは，国家の最も重要なインフラである通信網の Security の危機に目を閉じていた世界が，漸くその危険に気付いたことを示し，その意味では，世界の通信の将来に一点の希望の光を見る想いがする。

しかし，世界は今も IP 網に固執しており，地球規模のサイバー戦争の脅威はまだまだ消えることはない。サイバー戦を想像すると，これは闇の中の見えない相手との虚々実々の刃での争いで，核兵器競争より遥かに陰惨なものと想像される。その発生原因も IP 網の欠陥にある。その IP 網が依然として拡張を続けるのは，IP 網の欠陥の不理解にあると思われる。新しい通信網の研究は技術の重要な仕事であるが，そのためにも，社会に対して現 IP 網の基本的欠陥を，理を尽くして説明するのが技術の重要な仕事であろう。この２つの道が新しい世界通信網への道を開く。人類の知性はそれを実現できると信じたい。

【参考資料１】

Financial Times の Internet 関連記事

最近の Financial Times (FT)の記事の中で，青字は現在の定額料金制度の関連，赤字は Security の欠陥に関連するものを示す．“見出し”と（その和訳）および概要の「キイワード」のみ記す。全ての FT 記事は岩噌弘三氏の提供による。

2009 年 5 月 30 日　“Obama responds to cyber threat”（オバマ サイバーの脅威に反応）
「産業界の損害 US$1000bn(約百兆円)」「国安全保障も重要な影響」

2010 年 1 月 27 日　“US urges shared cyber attack defense”（米国 サイバー攻撃の共同防衛を急ぐ)「防衛には国境を越えた協力体制が不可欠」

2010 年 2 月 22 日　“US experts close in on Google hackers”（米国の専門家 グーグルのハッカーに近接)”　「中国の出所判明か」「中国当局は否定するが立場は苦しい」

2010 年 4 月 10 日　“Google accused of YouTube ‘free ride’”（グーグル YouTube の’タダ乗り’で非難される)「欧州テレコム 広帯域設備投資が必要」「特別料金を払えと要求」

2010 年 6 月 11 日　“O_2 axe to fall on ‘all you can eat’ plan”(O_2は’喰い放題’料金に大鉈を振るう）「英移動通信会社 周波数‘食い放題’の料金プランを改正」

2010 年 7 月 6 日　“France Telecom hints at web fees”（仏テレコム Web 料金改定を提示)
「スマートフォンの web サーフィン対策料金表を実施」

2010 年 9 月 24 日　“Malicious computer worm launched at industrial targets”（悪質な計算機ワーム 産業を狙い攻撃)「極悪ワーム Stuxnet」「産業制御部・ライフラインを狙う」

2010 年 9 月 24 日　“Computer worm triggers worldwide alarm”（計算機ワームの警告を世界へ発信）　「Stuxnet イランなど被害」「製造ライン・電力網・原発など」「世界に警告」

2010 年 10 月 2 日　“A code explodes（暗号が爆発する)”　「Stuxnet イラン核施設など攻撃」「サイバー戦争時代の只中」「8 月の Stuxnet 汚染計算機数 45,000」

2010 年 10 月 5 日　“The undeclared war in cyberspace”（宣告無きサイバー空間の

戦い）
「Stuxnet 複雑な設計は国家並み組織」「サイバー空間の宣告無き戦争を意味する」
2010 年 10 月 9 日　“Who controls the internet?”（インターネットの支配者は誰か？）
「米第５のサイバー軍発足」「サイバー攻撃の監視･制御」「米の絶対的優越必要」

【参考資料２】

米軍に第５の部隊

岩噌弘三

（「日比谷同友会会報」 2011 年 1 月，NO. 192，P74）

米軍では陸，海，空，宇宙に加えて，サイバー空間が第５の軍事活動領域として，2010 年 10 月に担当の将軍が任命された。就任前の審議会で，「ペンタゴンのコンピュータ・システムは１時間に 25 万回，1 日に 600 万回の攻撃を受けている。140 以上の外国スパイ組織が米国のネットワークに侵入しようとしている」と証言した。

このニュースに先立つ 1 年 4 か月前に，オバマ大統領は「金融や産業界のサイバー犯罪に基づく損失は 100 兆円にも達している。さらに，我々の防衛・軍事ネットワークは不断の攻撃にさらされているが，検出も防衛も困難な攻撃である。米国はディジタル・インフラストラクチャのセキュリティへの投資を怠ってきた。今日からこのインフラストラクチャを戦略的米国資産として対処する」と宣言している。

また，グーグルへの中国の攻撃後に，米国と NATO はサイバー攻撃へ一層の協力を進め供用の警報システムを構築すべきだとペンタゴンの幹部は主張している。また日本と米国の間の親密度を高めている。2010 年５月には，米国の FCC の議長と原口大臣は，サイバー・セキュリティ問題を話し合った。これは，中国は否定しているが，GhostNet と呼ばれる中国コンピュータ・スパイ・ネットを含むスパイ・ネットワークなどへの警戒に基づいている。2 国間の長期に亘る軍事同盟のハイテク版である。同盟により両国が利益を受けることができる。沖縄に存在するいくつかの施設を日米サイバセキュリティ・センターに変えることにより，強力な技術的盾を作り出すことができるであろう。

このような種々の過程を経て，2010 年９月 24 日から 10 月 10 日の間に，FT は立て続けに 4 回の大記事，大きいのは２ページに亘る記事を発表した。Stuxnet というコンピュータ・ビールスが世界中で産業機器に間違った命令を与えている。この場合はシーメンスに販売された共通的な産業制御用のソフトウエアが被害者である。全体の 60%がイランであり，次いでインドネシイアと続き，インド，パキスタンなど広く被害を受けている。マイクロソフト社によれば，８月に被害を受けたのが世界中で４．５万台あり，エストニアやグルジアでは，通信ネットワークの速度低下や停止をもたらした。イランの被害が多いのは，原子力施設を狙ったのではないかと言われ，サイバー・ミサイルと呼ぶ専門家もいる。このビールスは，自分を隠して待ち，ある条件下で正規とは反対の命令を出す。１年以上前から拡散し始めたが，ソフトウエアの複雑性から解明が困難であった。このような高機能なものは，十分な資金と多数の有能な技術者を持つ組織，多分国家的な組織のみが作成可能であろう。２０年以上コンピュータ・コンサルタントに従事してきたドイツ人は，「このように精妙で，攻撃的で，危険なものに遭遇するとは思ってもいなかった」と強い恐怖心を持った。

今回はイランを目標としたと思われるが，任意のインフラストラクチャを選べる可能性がある。イスラエルは秘密のサイバー戦組織に巨大な資源を投入している。米国と英国のこの種の組織間で精密なサイバー防衛協調組織を立ち上げた。サイバー戦が

従来の戦争と異なる大きな問題は，攻撃元を不明にすることができることと，単独の発電所や通信センターではなく送電網や通信網全体を不能に陥れることができることである。

ここまでの全ての情報は FT 記事のごく一部であるが，日本では，日経はドバイ発の１０行余りの短信，朝日は無掲載の様子，読売のみが１０月４日の夕刊で「日本でもパソコン６３台に被害」という記事に続いて，翌日の朝刊に「イラン原発サイバー攻撃」を掲載した程度で，ことの重大性を国民に知らせていない。

数年前から，日本のごく少数の高レベルの通信技術専門家が，大学の研究組織間用のネットワークからそのまま大発展をしてしまったインターネットの諸欠陥の改善について論議してこられたが，この面での研究の強化も必要と思われる。

追記：最近，日本の警察など国家機関の極秘資料のインターネット上への流出が話題になっている。個人のパソコンで使用したメモリースティック（記憶媒体）を，企業のコンピュータに使用した時にウイルスが埋め込まれて，このコンピュータから情報がインターネットへ流出すると推定されている。上記の Stuxnet も正に同様の手段で植え込まれている。日本について一部で推定されているウイルスの中継地が，欧州の小国（個人資産の秘匿で巨利を上げて注意されている国）であり，真の発信国まで追跡できない。

－以上－