経済学研究 46−4
北海道大学 1997.3

＜研究ノート＞

最近のインターネット事情と経済学

田 中 嘉 浩

1 はじめに

1980年代から世界中にTCP/IP接続されている幾つかのネットワークが相互に接続されインターネットが形成されてきたが，昨年TCP/IPが標準装備されたマイクロソフト社のPC用OSの売れ行き，WWWの標準化による有力新聞社のインターネット版の出現や高機能ブラウザ（Netscape Navigator, Internet Explorer等）の実現化，移動体通信の発達等の理由により国内のPCからのインターネット利用者数は爆発的に増加してきた。アメリカでは2015年迄に研究教育・医療用に大学を双方向に高速（数十億bps）の情報ハイウェイで結ぶNII計画が提案されている。日本国内でも通産省の100校プロジェクトで小中高校の約110校をインターネットに繋がせて教育面の配慮もなされ始めた。

WWWも最初は1990年にCERNによって情報の迅速な伝達・共有の為にHTMLと共に開発されたのがその端緒だったが，マルチメディア化とブラウザの発達によって社会に浸透してきた。httpの最新仕様はhttp://www.w3.org/pub/WWW/Protocols/で，HTMLの最新仕様はhttp://www.w3.org/pub/WWW/MarkUp/で知ることができる。今ではバージョンが3.2になって，情報のやり取りを可能にするフォームだけでなく表の作成やレイアウト迄可能になり，HTMLのみでもDTPとして耐える様になってきた。膨大な情報もDEC社のAltaVista（http://altavista.digital.com）（ロボット登録型）やYahoo（マニュアル登録型）の様な全文検索システムで検索でき，効率的な情報収集が出来る。最近ではサン・マイクロシステムズ社のJavaやマイクロソフト社のActiveXによるプログラム等も実現されてきたのでプラットフォームに依らない任意の出力画面をブラウザ上で得ることが出来る様になり，ハード主導からＯＳ主導そしてプログラム主導になりつつある計算機パラダイムの変化も生じてきた。この為低価格帯ではネットワークコンピュータ（NC）というインターネットの利用を前提としたものが製品化されてきている。また，Javaはその影響から言語使用からメモリのポインタ操作を削除されている程である。一方計算機が手近になりインターネットが普及すると共に，クラッカーによる犯罪件数，被害が無視できなくなり，システムや個人の安全性を図るセキュリティの研究がこの二十年来の暗号技術の成果を踏まえて急速に発展しつつあるが，インターネット・ビジネスの時代の情報インフラが整いつつある。

企業内ではWWWサーバを設置して社内データベースをPerl言語やシェルスクリプト等で書かれたCGI（Common Gateway Interface）で結び社内の情報共有を容易にすると共にインターネットへの限定的な情報提供を行うイントラネット（intraは「内に」の意味）による情報システム構築が流行ってきており，中にはフェデラル・エクスプレス社やモルガン・スタンレー社の様に有名な例もあるが，新たな経営システムが模索されつつある。

本稿では第2節で[7]で網羅出来なかった経済資源を紹介し，第3節で特に著者の専門であ

る数理計画でのインターネットの実際，第4節でインターネットと安全性，第5節で今後の展望について述べる。

2　インターネット上の経済情報（追加）

この節では前回[7]に網羅出来なかった主要な経済情報に限定して纏めておく。

新聞・雑誌

• The Wall Street Journal

http://www.wsj.gov/

The Wall Street Journalのインターネット版が提供されているが定期購読料を払う必要がある。

• Financial Times

http://www.usa.ft.com/

世界のビジネス・経済・政治ニュースや株式・資金情報を取扱っている。登録することにより無料で利用できる。

• CNN Financial Network

http://cnnfn.com/

リアルタイムの世界の市場情報が手軽に分る所に特徴がある。

• 日本経済新聞社

http://www.nikkei.co.jp/

日本経済新聞のインターネット版として市場情報やニュース等各種情報提供がなされている。企業ホームページへのリンクは産業別になっており詳しい。

• ビジネスコミュニケーション

http://www.sphere.ad.jp/bcom/

ビジネスコミュニケーション誌のインターネット版であるが，纏まった分量の記事になっている。

経済情報

• ノーベル経済学賞

http://sol.uvic.ca/econ/nobel.htnl

1969年に発足したノーベル経済学賞の趣旨や設立過程の他，1969－1996年のNobel Laureatesの受賞理由，紹介が掲載されている。

• ESBR

http://www.whitehouse.gov/fsbr/esbr.html

アメリカ政府機関によるアメリカ合衆国経済統計で歳出・歳入，雇用率，物価指数，その他の各種統計が纏まっている。

• NBER

http://www.nber.harvard.edu/

アメリカで主導的な経済研究団体のNational Bereau of Economic Researchの組織・役割や数ヶ国の第一次世界大戦前からのマクロデータ，1950-1992の世界百数十ヶ国の経済指標のPenn World dataが収められている。

• Wall Street Net

http://www.netresource.com/wsn/new.html

世界中の主要投資銀行へのゲートウェイ。負債や株のデータが対話式に入手できる。

• 欧州経済データ

http://www.europages.com/g/data.html

欧州のマクロ経済分析［図1］，44頁に及ぶ図表を駆使し，先端的なPDFフォーマットで書かれており，WWWの一つの方向を感じる。読むにはAdobe Acrobatが必要であるがダウンロードできる。

• 日本銀行

http://www.boj.go.jp/

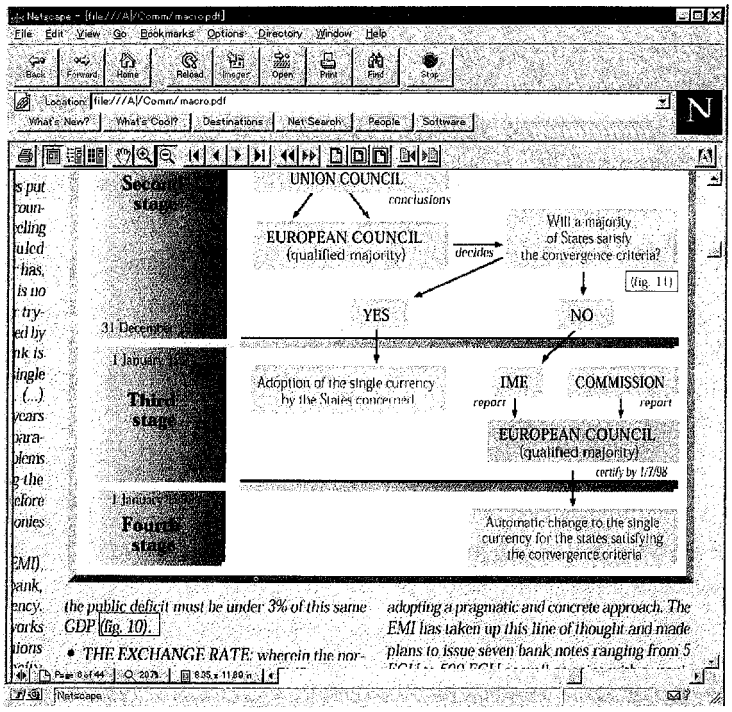

図1．欧州単一通貨

金利等の各種金融経済統計や短観等の経済情勢資料が得られる他、最新版の公表資料・刊行物発表スケジュールがわかる。

• 総務庁統計局・統計センター

http://www.stat.go.jp/

国勢調査，消費者物価指数（CPI），労働力調査，住宅統計調査，その他の各種統計調査の説明，平成7年度調査結果が纏めてある他，統計調査の公表スケジュールや統計関係WWWへのリンクがある。

• Electronic Commerce

http://tima-cmp.imag.fr/Homepages/cesario/2buy.htnl

Yahooによる検索結果であるが，電子商取引関連の各項目についてよく纏めてある。

• 日本の対外貿易情報

http://earth.library.pitt.edu/~ealib/jbusiness.htm

日本の対外貿易情報について特にJETRO（Japan External Trade Organization）の分析を中心に詳しく纏めてある。

3　インターネットと数理計画

非線形計画に於いて1951年にKuhn-Tucker条件の導出と共に不等式制約が解析上・計算上扱える様になり数理計画（Mathematical Programming）という分野が生まれた。

経済との関連では経済理論の内特に静学分析は数理計画をその主な解析手段の一つにしており，消費者の効用最大化と生産者の利潤最大化に典型的に利用されているが，例えば最近では暗黙の契約理論にKuhn-Tucker条件を適用して，理論の限界が示されている。又，1990年にノー

表1．Mathematical Programming誌での研究分野の推移（1996年は3巻分）

	1994	1995	1996
Interior Point Methods	14.7	21.3	(27.1)
Linear Programming	5.3	6.7	(0.0)
Nonlinear Programming	28.4	21.3	(14.6)
Linear Complementarity Problem	4.2	6.7	(8.3)
Variational Inequalities	6.3	2.7	(12.5)
Network	6.3	5.3	(4.2)
Combinatorial Optimization	27.4	18.7	(31.3)
other	7.4	17.3	(2.1)

ベル経済学賞を受賞したMarkowitzのポートフォリオ理論では投資選択問題をリスク最小化の2次計画問題に定式化していることが記憶に新しく，数理計画法の考え方の有効性が明らかになってきている等経済現象の分析の理論・実践面の両面に役立つ分野である。

最近では線形計画でその計算法に1984年にKarmarkar法が発見されて，内点法により効率的な多項式計算量の方法が実用化されて急激に分野全体が活気付いてきた。

その活動母体である国際数理計画学会（Mathematical Programming Society）は1996年4月時点で925名であり，国別には1位アメリカ380名，2位ドイツ，カナダ各62名，4位日本60名，5位オランダ47名という構成になっている。この学会の論文誌のここ3年の研究分野の推移は次の様になっている。

この節では数理計画のインターネット資源について述べる。数学や経済学の一部の分野程活発でないが，主要論文誌の題目や国際会議情報を迅速に得ることができる。他に研究者の個人ページやpreprintも無視できない。インターネットニュースのsci.op-researchにも貴重な情報がある。

論文誌

• Mathematical Programming

http://www.elsevier.nl/inca/publications/store/5/0/5/5/6/4/505564.pub.shtml

論文誌Mathematical Programmingの1995年以降の著者・題目が分る。

• SIAM Journal of Optimization

http://www.siam.org/journals/siopt/siopt.htm

論文誌SIAM Journal of Optimizationの1994年以降採択済未刊迄の著者・題目が分る。

その他の情報

• MPS homepage

http://www.caam.rice.edu/mathprog/public_html

国際数理計画学会のホームページ。

• MPS Prizes

http://www.caam.rice.edu/mathprog/public_html/abmps/mpsprizes.html

数理計画関係の国際賞であるFulkerson賞，George B. Danzig賞，Beale-Orchard-Hays賞，A.W. Tucker賞の趣旨や現在の委員会の主査が分る。

• Optimization FAQs for LP and NLP

http://www.mcs.anl.gov/home/otc/

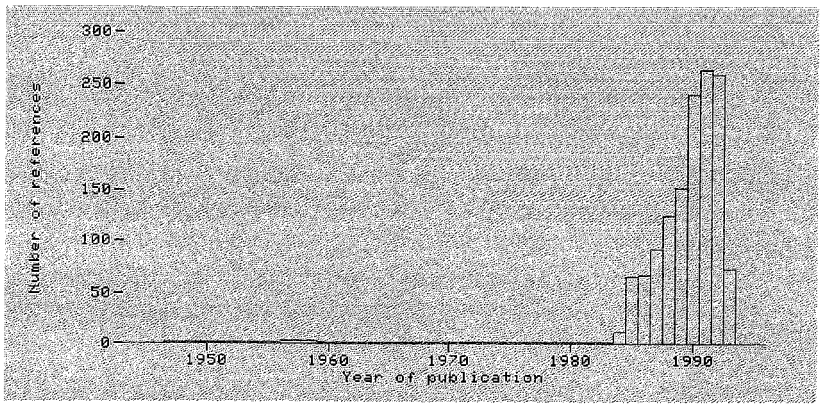

図2．内点法文献の総数（Kranich 1993）

Guide/faq/

J.W. Gregoryによって作成されたもので，インターネット・ニュースのsci.op-researchに定期的に投稿されるLinear Programming FAQとNonlinear Programming FAQに二分されているが，ソフトウェア一覧や参考文献等実用価値が高い。

• **Mathematical Programming Glossary Index**

http: / / www-math.cudenver.edu / ~ hgreenbe/glossary/index.html

H.J. Greenbergによる数理計画関係の小辞典。多くの事項を簡明な説明で網羅している。

• **Bibliography on interior point methods for mathematical programming**

http://cosmos.kaist.ac.kr/pub/bibliographies/Math/intbib.html

E. Kranichによる内点法の文献表であり，734のテクニカル・レポートと442の論文，その他多くの著書等を含む［図2］。

• **Numerical Analysis Digest 1996**

http://www.csc.fi/math_topics/Math/NANET96/index.html＃00227

数値解析関係の96年の著書，論文誌の題目紹介や国際案内等を含むが，かなり数理計画関係に比重が置かれている。

• **OS/MS Today**

http://lionhrtpub.com/ORMS.html

Optimizationも一分野を含むORMS学会の隔月機関誌でOR/MS関係のニュースやケース・スタディが多い。

4　インターネットと安全性

インターネットに於いて個人・組織の安全という観点での中心技術は暗号化であり，1970年代から格段の進歩を遂げている技術であるが，次の二つに大別される。

1．共通鍵方式：　発信者，受信者が同じ鍵を使う。最初に標準化されたのは，1977年にそのアルゴリズム迄公開されたDES（Data Encryption Standard）で，56ビットの鍵と16段の変換による方法である。実際オンラインシステムに幅広く導入されているが，近年松井［3］による線型攻撃により解読可能になってきた為より複雑な暗号化技術が必要となってきている。日本ではNTTによって，高速実現が可能なDES型暗号系としてFEALが1986年に提案されたがChip化を指向している。アメリカで

はClinton大統領により，Clipper Chipが提案されたが，それはSkipjackといわれる80ビットの鍵と32段の変換による暗号をChip上に実現したもので，犯罪対策を一つの目的にしている。この暗号で鍵供託という概念も生まれたが情報の集中管理に法律的・倫理的側面からの議論を生じてきている。

2．公開鍵方式：発信者に名簿によって公開された公開鍵と受信者の秘密鍵が異なり，発信者は受信者の秘密鍵迄は分らない。有名なのは1977年にR. Rivest, A. Shamir, L. Adlemanによって提案されたRSA暗号系で，素因数分解の計算量が多項式時間でないことを利用しており，暗号化が復号化より簡単な側面がある。電子署名にも用いられる。

インターネット普及に伴ってEC（Electoronic Commerce;電子商取引）がアメリカのCommerceNetに次いで日本でも通産省「電子商取引実証推進評議会」や郵政省「サイバービジネス協議会」等開始の兆しを見せてきているが，消費者単位では電子現金，企業単位ではCALSがその一翼を担っている。特に電子現金は影響力が大きいが，ICカードで実現される場合は社会基盤の確立はともかく機密性は高い。他にネットワーク上でソフトウェアで実現される場合は銀行からの認証にRSA等の暗号が使われており手軽であるが，リスク削減の為様々な問題が残っている。また，電子取引自体に特に大口取引では，銀行の資金決済件数の減少，預金残高の減少等の問題を生じる面があるので，簡便性だけを考える訳にはいかない。

通常のアプリケーション面での暗号対策もハード自体の規格変更は困難な為，それぞれなされている。電子メールでは現在PGP（Pretty Good Privacy）と呼ばれるものが中心であり，他にRSAとDESの両方を利用したPEM（Privacy Enhanced Mail）のWIDEによる日本語化のFJPEMが公開されているものの，現状の発展版が使われていくことになろう。telnetではパスワードが盗まれる危険性があるセキュリティ・ホールがあったが富士通でPET（Privacy Enhanced Telnet）が作成されレベル毎の認証が選択できる。WWWでは40ビットの鍵を利用する，RSA社のRC４という暗号を用いるNetscape社のSSLが浸透していっている。

安全対策は暗号だけによるものではない。近年組織に於いて，WWWサーバとDBMSとを連携したイントラネット化がアメリカ・日本で拡充していっているが，その際外部のインターネットからの侵入を防ぐ為，Firewallと呼ばれるゲートウェイを置いてパケット・フィルタリングを行う必要があり，専用製品も出てきている。

また，IPアドレス枯渇解決の為，現在のIPv４（32ビットのアドレス空間）を拡張したIPv６（128ビットのアドレス空間）に於いて，高速処理，自動設定と共に認証機能が組込まれる。

5　今後の展望

WWWでの表現面では図１の様なPDFによる文書を扱う日本語版ツールが発売以降は徐々に流行していくと思われるが，ファイルサイズが相当大きいので現在の通常の通信速度では伝送速度の点で効率が悪く，寧ろHTML３.２やその後継版によるレイアウト機能が用いられることが実際は多いであろうと思われる。３D化の方向ではVRML（Virtual Reality Modelling Language）により３次元モデルを表現可能になっているが，まだ実験的な段階である。コンピュータに対する概念を変えているJavaもActiveXと競合状態を続けながら高速実現の為に成長していくであろう。

システムのセキュリティ面では究極の選択は重要機密はインターネットに繋がない警備の厳重な部屋にあるマシン内で作業するしかない様に思われるが，ビジネスとしてはインターネッ

トに繋ぐ範囲を適切に選び，イントラネット用製品を使うのが適切であろう。アメリカのTCSEC（Orange Book）のセキュリティ基準ではA（高）からD（低）迄のレベルに分けているが，ビジネス用途にはオブジェクトに，“confidential”，“extremely confidential”，“secret”，“top secret”という多様なクラスが定義されユーザ毎にアクセス制限されている正式なセキュリティモデルのB２級以上のシステムが必要と思われる。個人の認証レベルでは暗号をコード化したICカードを電子決済等高機密が要される時には使う必要があると思われる。また，ISO/IECで1999年迄にセキュリティ評価基準を国際標準として制定する予定の為，国内の評価基準の確立が急がれていることを付け加えておきたい。

インターネット全般では国際的は組織のISOCが中心となって国際会議INETを通じて標準化活動を続けている他，IETFがプロトコル自体の研究開発を担っているが，着実な研究成果が揃っている様である。

いずれにせよ，ハードの高機能化，大容量化と，ATM光ケーブル等の通信回線の進歩により，快適で安全なインターネットになる日はそう遠くないであろう。

参考文献

[1] C. Brown, *UNIX System Security Essentials*, (石橋他訳：UNIXシステムセキュリティーと管理，アジソンウェスレイ社，1996).

[2] P. Fahn, “Answers to FAQ about today's cryptography”, http://econ-www.newcastle.edu.au/~jon/cryptology/rsafaq1.html.

[3] M. Matsui, “Linear cryptanalysis method for DES cipher”, *Advances in Cryptology-Eurocrypt'93*, Springer, pp. 386-397 (1994).

[4] 須藤　修，“ネットワークの進化が与える金融機関へのインパクト”，http://www.sudoh.ij.u-tokyo.ac.jp/

[5] (社) 情報科学技術協会編，情報検索のためのインターネット活用術，日外アソシエーツ (1996).

[6] S. Takriti, “Mathematical Programm-ing and the Web: To surf or not to surf”, *Optima*, No. 47, pp. 1-2, 1995.

[7] 田中　嘉浩，“経済学におけるインターネット利用”，経済学研究（北海道大学），第45巻第３号，pp. 1-8 (1996).

[8] 山口　英，“インターネット・セキュリティ”，情報処理，Vol. 37, No. 6, pp. 496-502 (1996).