特別寄稿

ネットワークを通して情報を高速で効率的・安全に伝送するための研究

My Research on Network, Communication and Information Security

岡本栄司 Eiji OKAMOTO

1．はじめに

今回，筑波大学を定年退職するにあたり，研究生活を振り返る機会を頂いたので，私の多岐にわたる45年近い研究を紹介してみたいと思う．昔の状況を述べるとやや個人的なことも含まれてしまうがお許し願いたい．

私の研究は分野的には回路網理論，通信理論，暗号理論となるが，これらをやや強引にまとめるとタイトルのようになろうか．実際のところ研究に没頭しているときは，まとまりを意識することはなかったが，例えばネットワークセキュリティで回路の知識が役立つなど，結果的に相互作用があったと言えなくもない．以下，それぞれの研究を逸話も適宜交えて紹介しよう．今から見ると，古過ぎてもはや使えない結果であったり，当たり前の成果だったりするが，それは仕方のないことなので，御容赦願いたい．

2．回路網理論

私が1969年に東京工業大学に入学した年は学生闘争がピークを迎えていて，東京大学と東京教育大学では入試ができなかった．東工大でも夏休みまで授業がなく，新入生も自宅待機と寺子屋（時々指定された教員の研究室に集まっての勉強会）で過ごさざるを得なかった．しかし，私自身はこれ幸いと夜遅くまで好きな数学の本を熟読した．これはその後の研究生活の基盤になったと信じている．学科配属では数学科でなく電子工学科を選んだが，これも良かったと思う．そこで受講した岸源也教授の講義「交流回路」がごく普通に見えるタイトルにもかかわらず数学を駆使しており，大変面白く，その後岸研究室に配属になって回路網理論を研究する楽しい研究生活がスタートできたからである．

研究してみると，狭そうに見える回路網理論も範囲が広く，その中で私は当時の若手助教授であった梶谷洋司先生の下でグラフ理論的回路網理論を研究することにした．

回路は入力端子と出力端子の間に多くの素子が結線された構造をしており，電気信号が目的に合う形で出力されるように構成される．回路の性質は接続構造のみで決まる部分と素子自体の特性を利用する部分があり，私は前者の研究に取り組んだ．グラフ理論的回路網理論の出発点となった論文は1847年の有名なKirchhoffの論文で

Gustav Robert Kirchhoff, “Über die auflösung der gleichungen, auf welche man bei der untersuchung der linearen verteilung galvanischer ströme geführt wird,” Ann. Phys. Chem., 72, pp.497-508, 1847.（英語翻訳版 “On the solution of the equations obtained from the investigation of the linear distribution of galvanic currents,” IRE Trans. Circuit Theory, vol. 5, no. 1, pp.4-7, 1957.）

である．

この論文で，彼は線形集中定数回路のインピーダンス（電圧／電流）は回路の木集合などで与えられることを示した．ここで，線形集中定数回路というのは全ての素子が抵抗，容量，コイルなどの受動素子から成る回路である．

例えば，下記図1で与えられる回路のインピーダンスZ=V/Iは

$$Z = \frac{T'}{T}$$

で与えられる．ここで，a～fは素子のコンダクタンス（抵抗の逆数）で

T’= ac+ad+af+bc+bd+bf+cf+df

T= abc+abd+abf+acd+ace+ade+adf+aef+bcd+bce+bcf+bde+bef+cdf+cef+def

である．

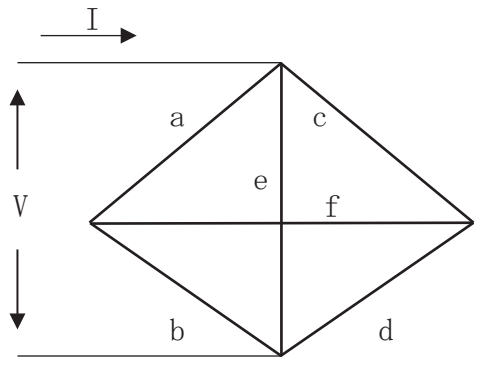

図1　グラフの例

岡本栄司　正員：フェロー　筑波大学
E-mail　okamoto@risk.tsukuba.ac.jp
Eiji OKAMOTO, Fellow (University of Tsukuba, Tsukuba-shi, 305-8573 Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.9 No.4 pp.275-280 2016年4月
©電子情報通信学会 2016

驚くべきことはTがグラフの木多項式になっていることである．すなわち，グラフの全ての木（spanning tree: 閉路を含まない極大辺部分集合）の和の形になっている．また，T’は測定している両端をショートしたグラフの木多項式になっている．

線形集中定数回路というのはやや制限が強いかもしれないが，しかし，この定理の本質的な部分，すなわち電流（あるいは双対としての電圧）を解くための連立一次方程式の行列式がグラフの木集合Tから与えられるという性質は，Tree Matrix Theoremと呼ばれ，グラフ理論的回路理論の重要な定理となった．前述のとおり，図1のグラフにおける木集合は

{abc, abd, abf, acd, ace, ade, adf, aef, bcd, bce, bcf, bde, bef, cdf, cef, def}

となる．この木集合は多項式の形で

T= abc+abd+abf+acd+ace+ade+adf+aef+bcd+bce+bcf+bde+bef+cdf+cef+def

のように表現されることも多い．

我々は，この木集合の性質をかなり調べ，幾つかの新しい成果を上げた．例えば，

・区別できない枝を含むグラフの木集合の特徴

例えば，a=b=xとすると，Tはxの多項式になる：

T(x)=(c+d+f)x2+(2cd+2ce+2de+2ef+cf+df)x+cdf+cef+def

ここで，T(x)がグラフを一意的に決定する条件などを検討した．

例えば，T(x)の定数項が非零ならばグラフは一意的である．

・木集合には含まれえない部分集合

一例: $\{ab, ac, ad, bc, bd, cd\}$

素子数3以上では，木集合には含まれ得ない部分集合の最小数は6

・重み付グラフを決定するクラスの木

など，木集合の条件に関連した成果である．

また，グラフ理論的回路網の定理について，逆にその定理が成り立つための条件を調べた．通常，グラフ理論的回路網の定理は接続行列や閉路行列を用いて記述されているが，そのときグラフ理論的回路網の定理が成り立つために必要な行列の条件を調べたものである．

今から見ると，回路網理論へのグラフ理論の応用はやや古い成果であったと言えよう．その後，グラフ理論が応用された分野には集積回路の配線問題がある．配線では線は交差しないようにしなければならないが，このようなグラフは平面グラフと呼ばれている．平面グラフに関しては次のKuratowskiの定理が有名であり，前記Kirchhoffの理論と並んでグラフ理論関係の重要な成果となっている．

Kuratowskiの定理：グラフが平面的であるための条件は，5次完全グラフK_5あるいは3次2部完全グラフ$K_{3,3}$（図2）を部分グラフとして含まないことである．

この定理は，平面グラフの特徴が二つの最小非平面グラフの非存在性に依存していることを述べており，興味深い形をしている．

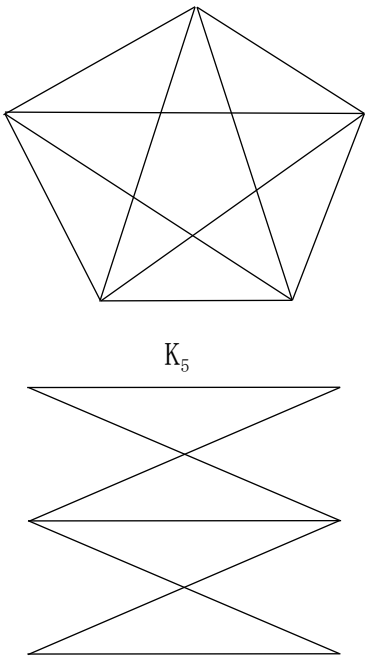

図2　非平面グラフ

当時，ICの集積度がどんどん上がってたので，大規模グラフの理論は重要性を高めていった．研究室でも徐々に配線問題の研究割合が増えていった．

私自身はグラフ理論を回路網理論の中で扱ったが，今ではグラフ理論はネットワークをはじめ多くの分野で基礎となっており，また離散数学の題材として扱われることが多くなっている．

3. Erdős Number

ここでグラフに関連したお遊びのような話をしよう．Erdős Numberと言うものを聞いたことがあるだろうか．私は，指導学生の品川和雅君に教えてもらった．

「先生はエルデシュ数2なんですね，自慢できますよ．」

最初，何のことか分からなかったがErdős Numberとはかの有名なハンガリー数学者Paul Erdősからの近さを示す数とのことである．研究者を頂点とし，共著論文がある場合に辺で結んだグラフは協力グラフと呼ぶらしいが，そこでPaul Erdősからの距離をErdős Numberと言うらしい．Erdős Number 1の人は511人で，既にPaul Erdősは故人なので今後増えることはない（常識的には）．長年研究していれば，誰でも研究会報告等も含めた論文数は511以上になると思うが，同じ共著者で幾つもの論文を書くので，共著者数511というのはさすがである．この中に日本人は4人いるらしい．それはともかく，問題のErdős Number 2のクラスであるが，今でもどんどん増えつつあるが，2016年1月末時点で11,009人だそうである．この中には日本人は213人いる．恩師の梶谷洋司教授も含まれている．更に暗号・情報セキュリティ分野に絞ると，下記

の7人と思われる．

Kazumaro Aoki
Toshiya Itoh
Wataru Kishimoto
Kaoru Kurosawa
Wakaha Ogata
Eiji Okamoto
Akira Saito

下記の二つの論文によって確かに私はErdős Number 2のクラスにいることが分かる．

・Paul Erdos and Frank Hsu, “Distributed loop network with minimum transmission delay,” Theor. Comput. Sci., vol. 100, pp.223-241, 1992.

・Xun Yi, Shigeki Kitazawa, Eiji Okamoto, and Frank Hsu, “An agent-based architecture for securing mobile IP,” American Mathematical Society Discrete Mathematics and Theoretical Computer Science, vol.52, pp.303-314, 2000.

ただ，私との共著者Shigeki KitazawaがErdős Number 2に載っていない．他にもこのような人はいるかもしれない．

いずれにしても，距離2だから自慢できるというのはジョークであるが，ともかくこのようなErdős Numberを真面目に取り上げているところが結構あるのが面白い．例えばThe Erdos Number Project <http://www.oakland.edu/enp/> には詳しく載っている．

協力グラフにおいては，誰を中心にするかで，様々なxxx numberが考えられる．逆に言うと，xxx number 1, 2, 3ぐらいのクラスの大きさで研究活動の活発さを測れるかもしれない．私の場合，EijiOkamoto Number 1, 2, …はどのくらいの大きさになるのだろうか．

協力グラフを共著でなく，知り合いと解釈すると，面白い見積りができる．全然知らない日本人でも知り合いを二人たどれば到達し，世界だと3人を間におけばどんな人でもほぼ到達するというものである．一人の人間の知り合いが1,000人ぐらいいるとすると，3人たどると

$1{,}000^3$人＝10億人

に到達するので，これは日本人口を超える．これはどのように選んだ2人の日本人でも，間に2人入れればほぼつながることを示している．4人たどると

$1{,}000^4$人＝1兆人

となり，全世界の人口75億人をはるかに超える．実際にはこの中にはダブってカウントされる人がいるであろうし，また1,000人の知り合いがいない人も多いのでこの見積りは大雑把過ぎるが，しかし，少なくとも私の場合，日本の中で有名な人を思い浮かべると，間に二人おけば，つながるケースが多い．

4．通信理論

NECに入社して中央研究所通信研究部に配属してからは通信理論を研究した．特に，非線形伝送通信理論に取り組み，幾つかの成果を上げた．通信理論では普通は線形伝送を扱うが，図3に示すようにディジタルマイクロ波通信などは非線形伝送である．これは電力増幅器が高電力領域で入出力関係がなだらかになるため，非線形となるからである．利用する立場からすると，効率を上げるために，低電力な線形領域だけではもったいないので，高電力領域でも使いたくなる．しかし，そこまで踏み込んで電力増幅器を使うと，従来の線形な解析理論は使えなくなる．そこで，非線形領域でも解析できるように考案したのが私の成果であった．

まず，電力増幅器の入出力関係をべき級数展開近似して三次項までを用いることとした．その上で，多値ディジタル信号を特性関数法により解析して，誤り率と電力スペクトルを計算できるようにした．その結果，シミュレーションよりも効率良く計算できるようになった．具体的には次のようになる．多値ディジタル送信信号はデルタ関数を用いて

$$x(t)=\sum_i x_i\,\delta(t-iT)$$

と書ける．ここでx_iが時刻iTで伝えたいシンボル値で確率変数である．これが送信フィルタで整形された後，電力増幅器で増幅されて送信される．受信側では雑音を含んだ信号を受信し，フィルタを通すことにより，整形された信号となる．これは

$$y(t)=\sum_i a_i(t)\,x_i+\sum_{i,j,k} b_{i,j,k}(t)\,x_i x_j x_k+n$$

の形に書ける．ここで，nは残余雑音である．電力増幅器が三次項までで近似できることを用いている．この信号の$t=0$を基準と考え，x_0の周りの同相成分$z=\mathrm{Re}[y(0)-x_0]$の確率密度関数を求めれば，シンボル誤り率が計算できる．ただ，直接求めるのは容易でないので，特性関数法を利用した．特性関数は確率密度関数のフーリエ変換で

$$M(v)=\overline{e^{-jvz}}$$

で与えられる．ここでバーは平均を表す．この特性関数の計算では様々な近似が使える．ここでは，フィルタのインパルス応答の特性から$\sum_i a_i(0)\,x_i+\sum_{i,j,k} b_{i,j,k}(0)\,x_i x_j x_k$においては$a_i(0)$と$b_{i,j,k}(0)$の添字の小さい項が支配的であろうと考え，その他は白色雑音として扱っている．そのようにして求めた特性関数をフーリエ逆変換して，zの確率密度関数を求めた．これにより，計算が従来法より簡単になり，実際の誤り率との近似も良いことが確かめられた．

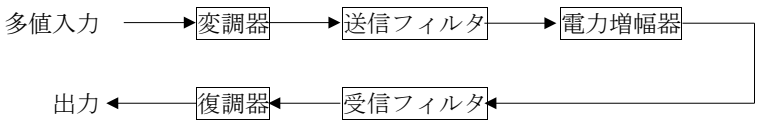

図3　ディジタルマイクロ波通信伝送モデル

特性関数を用いるとモーメントを求めるのが容易となるため，その一種である電力スペクトルの計算も簡単に求められた．

ディジタルマイクロ波通信の研究は2年間のOJT（On the Job Training）期間だけであったが，ナイキスト基準やシャノンの符号化定理など広く通信理論を学ぶことができたのは有用であった．

5．暗号理論

OJT期間の後は暗号理論に取り組むこととなり，それは現在まで続いている．当時（1980年頃）はまだ我が国では暗号の研究をしている人は少なかった．しかし，その後重要になるであろうと予想されたため，私が担当することになったのである．

暗号は文字の発明と同時に始まったと言えるくらい古いものであるが，主な利用者は軍か外交であった．アカデミック研究が始まったのは商業的な価値が高まってきてからである．アメリカが1977年に暗号標準DES（Data Encryption Standard）を制定し，公開鍵暗号もその頃から始まってアカデミック研究が一気に広まった．

日本でもすぐ後にアカデミック研究が始まったが，そのきっかけとなったのは1978年9月4日号の日経エレクトロニクス解説記事「鍵なしではまず解けなくなった最近の暗号方式」が掲載されてからであろう．これを機に大学や民間の研究所などで暗号研究が盛んになったといえる．引き続き幾つかの解説記事が出てきたが，最初の研究成果は1980年の情報理論とその応用シンポジウムでの中村勝洋「自己同期型簡易暗号方式に関する一考察」，及び情報処理学会アルゴリズム研究会での森，山村，藤井，嵩「暗号化鍵の配送・管理の一方式とその安全性の検討」である．翌年には岡田，松本，今井「ネットワークに適した一暗号化方式」（電子通信学会通信方式研究会），小山謙二「RSA公開鍵暗号法のマスター鍵」（情報処理学会AL研究会）が発表され，その後の国内外における多くの論文発表につながっていった．

日本人による海外での研究発表では，1981年にE. Okamoto, K. Nakamura, Y. Shimizu, and Y. Sato, “Distributed management system of cryptographic keys in communication networks”(Allerton Conference)が発表された．同年，暗号専門の国際会議Cryptoシリーズが始まり，翌年からはEurocryptが，1991年からはAsiacryptも始まっている．これらのシリーズでの日本から最初の発表は1985年のE. Okamoto, “Lifetimes of keys in cryptographic key management systems”である．2年後の1987年には鍵配送に関して日本から4件の発表があって1セッションを成すほどで，日本の暗号研究の最初のピークとなった．

Cryptoの参加者は私が1984年に参加したときは150人であったが，1990年代になって500人を超すようになった．（最近は多くのワークショップ等ができてやや減っているが．）日本でも同じ状況である．日本の暗号の研究会・シンポジウムとしては，今井秀樹先生，松本勉先生の努力により1984年に本会の「暗号と情報セキュリティシンポジウムSCIS」が数十人の参加者でスタートしたが，今や毎年500人以上が参加するシンポジウムに成長した．私自身も，情報処理学会におけるCSEC研究会設立や雑誌IJIS（International Journal of Information Security, Springer）発刊（2001）などを通して微力ながら暗号関連研究の発展に寄与できたのではないかと思っている．

暗号研究におけるエポックメーキングな出来事には次のようなものがある．

1975　公開鍵暗号
1977　DES制定
1979　秘密情報分散法　1987　一般アクセス構造秘密情報分散法
1984　IDに基づく暗号
1984（1970）　量子暗号
1985　量子計算機
1988　ゼロ知識証明プロトコル
1990　差分解読
1993　線形解読
1994　安全性証明
2000　ペアリング暗号
2001　AES
2005　属性暗号
2010　関数暗号

この中で私の研究室で関わったものは，一般アクセス構造秘密情報分散法，IDに基づく暗号，ペアリング暗号，属性暗号などである．

5.1　IDに基づく暗号系

我が国が世界において最初に認められた研究成果はIDに基づく暗号系であろう．この概念自体は1984年にShamirによって提唱されたものであるが，1980年代後半にIDに基づく鍵配送という形で，我が国で大いに発展した．まず1986年に田中，松本・今井，岡本などの国内での発表が相次ぎ，翌年前述したCrypto’87での4件の発表となった．

K. Koyama and K. Ohta, “Identity based conference key distribution systems”

T. Matsumoto and H. Imai, “On the key predistribution systems: A practical solution to the key distribution problem”

E. Okamoto, “Key distribution systems based on identification information”

H. Tanaka, “A realization scheme for the identity based cryptosystem”

この後もIDに基づく鍵配送に関しては非常に多くの研究がなされた．ただ，この時期における方式は，予備通信が必要かあるいは結託しきい値があるという点で，理想方式に今一歩届かなかったと言える．

5.2　秘密情報分散法

秘密情報分散法は応用という面から言えば，今までインパクトは少なかったかもしれないが，クラウドコンピューティ

ング時代になって有用性が高まりつつある．秘密情報分散法の一つであるしきい値分散法はG. R. BlakleyやA. Shamirによって1979年に早くも提案されていた．しかし，一般秘密情報分散法の必要十分条件については，1987年になって初めて伊藤・斉藤・西関によって，秘密復元可能グループの集合Γのモノトーン性

$$A \subseteq B,\ A \in \Gamma \Rightarrow B \in \Gamma$$

であることが証明された．私はこのモノトーン性の必要性には以前より気が付いていたが，東北大西関研の上原氏がインターンとして来たときにそれに関する実習研究を持ち帰って，西関研が十分性を証明したものである．まさか，モノトーン性で十分だとは全く思っていなかったので，彼らの成果には大変驚いた．彼らの論文はこれ以降，秘密情報分散法の論文にほとんど引用されており，重要な論文となっている．

5.3　だ円曲線暗号とIDに基づく暗号

だ円曲線を暗号に用いることは，最初Millerによって1985年に提案された．DH鍵配送法がそのまま移植できるため，それを用いた方式，例えばエルガマル暗号などもだ円曲線上で構成できることとなった．離散対数計算量が整数環上では準指数的になるのに対し，だ円曲線上では指数的になるため，同等の解読計算量となる入力ビット長がかなり小さくできるメリットがある．

この分野における我が国の大きな貢献は双線形関数としてのペアリングを利用したもので，MOV帰着とID情報に基づく暗号系である．MOV帰着はだ円曲線上の離散対数問題をペアリングを用いることにより，整数上の離散対数問題に帰着させるもので，Menezes, Okamoto (Tatsuaki), Vanstoneが提案した．

ID情報に基づく暗号系については，前述したように1980年代後半に我が国で積極的に研究が行われたが，結局理想形は実現できなかった．ところが，境先生，大岸氏，笠原先生がペアリングを用いて予備通信が不要で結託しきい値のない方式を世界に先駆けて提案した．しかしながら，IACR（International Association for Cryptologic Research）の暗号国際学会では採択されずに1年後のCrypto’91でBonehとFranklinによって似た方式が発表され，こちらがペアリングによる最初のIDベース暗号と言われるようになった．よくあることとはいえ理不尽なことである．

ペアリング自体の研究については我々は幾つかの成果を出している．ペアリング計算アルゴリズム改良，高速ハードウェア実装（FPGA，ASIC），高速ソフトウェア実装，Optimal Ate Pairing提案などである．また，誰でも使えるようにペアリング計算ライブラリをTEPLAの名で研究室Webに載せている．

http://www.cipher.risk.tsukuba.ac.jp/tepla/

無料で使用できるように気を付けて実装した．

その他の暗号研究成果としてはproxy cryptosystemがある．これは最初ウイルス対策の一環として，私がプログラムにコンパイラが署名するというアイデアを出したことから始まった．その後，満保雅浩先生がproxy signatureとして，更にproxy decryptionも提案して，proxy cryptosystemに一般化したものである．

日本発の有名な暗号研究成果としては，DES解読，安全性証明，関数暗号などがある．DES解読についてはBiham-Shamirが差分解読手法を1990年に発表し，8段以下なら解読可能であることを示したが，正規のDESの解読はできなかった．これはDES開発チームがこの解読法を事前に知っていて対策を盛り込んでいたからである．実際に解読に成功したのは松井充氏で1993年に線形解読手法を用いて成し遂げた．これは学術的暗号研究史上の我が国の誇る快挙の一つである．実際には10^{13}程度の平文・暗号文対が必要で計算に50日かかったが，ともかく初めて鍵の割り出しに成功した．翌年のCryptoでは栄えあるトップバッターの発表で，世界に認められた．その後，我が国では，通信・放送機構の暗号研究グループ（辻井重男先生リーダ）における金子敏信先生をはじめとする研究者から多くの成果が得られた．

この解読によって，差分解読や線形解読に対する強さの評価基準ができたことも重要な点で，これ以降の共通鍵暗号系の設計に多大な貢献をした．その代表例がアメリカNIST (National Institute of Standards and Technology)のAES (Advanced Encryption Standard)制定活動，ヨーロッパのNESSIE (New European Schemes for Signatures, Integrity, and Encryption)活動，及び我が国のCRYPTREC (Cryptography Research & Evaluation Committees)の標準化活動である．その結果多くの新しい共通鍵暗号が生まれた．

公開鍵暗号の分野でも日本の貢献は大きい．特に岡本（龍）氏と内山氏がEurocrypt1998で発表したEPOC公開鍵暗号，高島氏と岡本（龍）氏がCrypto2010で発表した関数暗号などはその代表例である．安全性証明でも幾つかの貢献がある．

我々の暗号以外の情報セキュリティ研究についても触れておこう．主な成果に耐タンパソフトウェア，ネットワークセキュリティ，個人認証などがある．

耐タンパソフトウェアはプログラム難読化技術として1990年代後半に始めたもので，ソフトウェア保護の一環であった．ゲームソフトウェア開発が得意だった学生が漏らした一言から発展した課題である．当時，ゲーム業界では新しいソフトをいかに守るかが課題であった．ソフトウェアの中身を調べられてその仕組みを新たにプログラム化されると著作権違反にもならず，困った事態になるとのことであった．そこで，ソフトウェア難読化の考えに到達したものであった．通常，プログラムは分かりやすく書くのが当然で，それをわざわざ分かりにくく書くというのだから，発想の転換を要した．これには学生だった村山氏と満保先生の功績が大きい．

我が研究室でのネットワークセキュリティは金岡晃先生が主に進めていたが，ネットワークモデル化と評価手法の確立や確率的パケットマーキングによるIPトレースバックなどの成果がある．ここでのネットワークモデルは金岡先生が新しく提案したもので，全レイヤを統一的に表現し，扱いやすくしている．

個人認証ではキーボードへの入力による癖やマウスの動かし方の癖を利用した方式を提案したが，特にキーボードへの入力ではキーを押すときよりも離すときの方が意識しづらく癖が出やすいことが分かった．また，マウスの動きによる個人認証も研究したが，判定率の誤差が大きい傾向があり，実用化にはまだ時間がかかるとみられる．ネット社会ではネットワークを介したやり取りになるので，個人認証はますます重要になってくるはずである．

今，こうして私の研究生活を振り返ってみると，いろいろな研究に携わってきたが，本稿にも何人かの名前が出てきたことで分かるように，ここまで来られたのは多くの方々のおかげである．全ての名前を挙げることはとてもできないが，お礼申し上げる．これからは好きな研究をじっくりと進めながら，第2の人生を大いに楽しんでいきたいと思う．

岡本栄司（正員：フェロー）

1973東工大・工・電子卒．1978東工大大学院電子工学専攻博士課程了．工博．同年日本電気（株）中央研究所入社．その後，北陸先端大，東邦大を経て2002から筑波大システム情報系教授．暗号理論を核とする情報セキュリティの教育・研究に従事．1990本会論文賞，1993情報処理学会ベストオーサ賞，2008情報処理学会論文賞，2013情報処理学会功績賞各受賞．情報処理学会フェロー，著書「暗号理論入門」（共立出版），「電子マネー」（岩波書店）など．