

# 日本における符号理論の原点

The Origin of the Coding Theory in Japan

今井秀樹 Hideki IMAI

萩原 学 Manabu HAGIWARA

**アブストラクト** 符号理論はデジタル情報の信頼性確保のために不可欠な理論であり、現在の情報化社会を支える基盤理論の一つである。この理論は約 60 年前に米国で生まれたが、日本でもこの時期から符号理論の研究が行われていた。しかし、研究者が増え、国際的に認められる研究成果が出るようになったのは 40～50 年前のことである。それには、この研究を米国で始めた方々の帰国と W. W. Peterson の著書の影響が大きい。このころ、日本において現在につながる符号理論研究の原点が形成されたといっただろう。その後、特に符号理論の応用の面で日本は世界を先導する役割も担ってきた。この間、符号理論は何度かの大きな変革を経ながら、その応用範囲を拡大しつつ発展を続けてきている。本稿では、このような符号理論の流れを日本の視点から俯瞰する。

**キーワード** 符号理論, 誤り訂正符号, 通信路符号化, 原点, 符号理論の応用

## 1. はじめに

筆者の一人今井（以下本章では筆者と呼ぶ。）が、本誌に符号理論の原点を書くよう依頼されたとき、かなり躊躇した。記録を残すことには甚だ怠惰であり、歴史の語り手として適任とはいえないからである。しかも、最近記憶力もとみに衰えてきた。しかし、それだけに、この辺りで何か書いておかないと永遠に失われてしまうこともあるかもしれないと思い直し、兎も角も引き受けることにしたのである。

しかし、もう一つ問題があった。1970 年代の末から始めた暗号の研究が面白くなり、その応用としての情報セキュリティ技術とともに、それらが主要な研究課題となっていたことである。特に 2000 年代に入ると符号理論の研究は全体の 10 % 程度となってしまった。以前のように、最新の符号理論の流れを完全に把握しているとは言い難く、現時点の符号理論の立場から見たその原点に関しては、余り自信が持てない。そこで、現在符号理論の第一線で活躍している研究者を筆者に加えることとした。これにより、60 年に近い符号理論の研究の流れを適格に俯瞰することができたと考えている。

ここで、まず「符号理論」を定義しておこう。符号理論は、符号化の理論という意味で、情報源符号化などの理論も含むことがあるが、ここでは誤り訂正符号（誤り検出符号なども含む）の理論という意味で用いる。この理論の原点の一つは、1948 年

に C. E. Shannon により誤り訂正符号の能力の限界が「通信路符号化定理」として示された<sup>(1)</sup>ことにあるといっただろう。それにより、多くの研究者がこの限界を達成する符号を構成しようという努力が符号理論の研究の流れを作っていたことは事実である。しかし、R. W. Hamming による単一誤り訂正符号（ハミング符号）の発明<sup>(2)</sup>が、Shannon の理論にも影響を与え、後の誤り訂正符号構成法の原点になったという見方もできる。ハミング符号は 1950 年に発表されているが、実際の発明は 1948 年以前であり、Shannon もこの符号を知っていたのである。

しかし、本稿の目的は、日本における符号理論の原点について述べることである。世界における符号理論の原点については、後の W.W. Peterson の寄稿に期待して頂きたい。

以下 2. では、筆者が符号理論に手を染める前の我が国における符号理論の研究を概観し、3. では筆者が符号理論にかかわり始めた 1960 年代後半、4. では代数的符号理論の全盛期を迎えた 1970 年代、5. では符号理論が成熟し、その応用が急速に広がった 1980 年代、そして、6. では符号理論の新たなパラダイムが生まれた 1990 年代以降の符号理論の流れについてそれぞれ述べる。

## 2. 1960 年代前半までの符号理論

本章は共著者二人の文字どおりの共著である。二人ともこの時期には、符号理論の研究を行っていたわけではなく、生の体験としてこの時期の符号理論の研究に接していないので、調査も必要であった。この時期から優れた研究が日本で行われていたことは知っていたが、正確に把握してはいなかったからである。実際、この時期の日本の研究成果は、1960 年代の高志雄氏

今井秀樹 正員：フェロー 中央大学理工学部電気電子情報通信工学科

E-mail h-imai@aist.go.jp

萩原 学 正員 産業技術総合研究所情報セキュリティ研究センター

E-mail hagiwara.hagiwara@aist.go.jp

Hideki IMAI, Fellow (Chuo University, 112-8551 Japan), Manabu HAGIWARA, Member (National Institute of Advanced Industrial Science and Technology, Tokyo, 101-0021 Japan).

Fundamentals Review Vol.2 No.4 pp.9-15 2009 年 4 月

の成果を除き、国際的に認知されたのはごくわずかであり、しかもずっと後になってからである。

日本において、最も早く符号理論の本格的研究を始めたのは、恐らく三谷尚正氏であろう。1951年、三谷氏は誤り検出符号と誤り訂正符号に関する報告<sup>(3)</sup>をまとめている。同年、三谷氏は符号を提案しているが<sup>(4)</sup>、これは現在リードマラー (Reed-Muller) 符号として知られるものである。I.S. Reed<sup>(5)</sup>や D.E. Muller<sup>(6)</sup>より3年早かったが、国内集会で日本語で発表されたためか三谷氏の名が冠されていないのが残念である。

ほぼ同時期に符号理論の根幹にかかわる発見をしたのが喜安善市氏である。次章で触れる Peterson の著書<sup>(7)</sup>の改訂版<sup>(8)</sup>には、「パリティ検査符号と群やベクトル空間との関係は喜安 (1953)<sup>(9)</sup>により初めて指摘された。」との記述がある。つまり、符号理論に線形符号の明確な概念を世界で初めて導入したのは喜安氏といってもよいのかもしれない。

Hamming がハミング符号を考えたのは真空管式の電子計算機の記憶装置における誤り訂正のためだったのであるが、喜安氏の符号理論研究の動機も当時電電公社の電気通信研究所で開発していた電子計算機の信頼性向上であったことは興味深い。

その次に挙げるべき研究成果は有本卓氏によるものである。もし、その研究発表がもう1年早ければ、現在最も広く使われている誤り訂正符号は有本符号または有本・リード・ソロモン符号と呼ばれていたかもしれない。

1961年に発表された同氏の論文<sup>(10)</sup>では非二元線形符号の符号化、復号法、最小距離が研究されている。その中心となっているアイデアはファンデルモンドの行列式の理論が適用可能なパリティ検査行列を構成することにより符号の最小距離を設計することにある。このアイデアは1960年に発表されたリードソロモン (Reed-Solomon) 符号 (以下 RS 符号)<sup>(11)</sup>のそれと本質的に同じものであった。

数年前まで日本を代表する符号理論研究者として活躍してきた嵩氏も1960ごろから符号理論の研究の発表を始めている。極めて精力的で、多くの研究成果を得ているが、特に同氏が構成したバースト誤り訂正巡回符号<sup>(12)</sup><sup>(13)</sup>は国際的にも広く知られている。

このほか、当時電気通信研究所にいた駒宮安男氏も1960年代の前半に符号理論の研究を行っている。同氏の論文<sup>(14)</sup>では最小距離に対し符号化率の高い符号を構成するという符号理論の基本的課題が研究されている。非線形符号も含めて論じており、現在球面上の組合せ論と呼ばれる分野へつながっている。

以上は日本の状況であるが、世界的には、1960年前後に、前述の RS 符号をはじめ符号理論で最も重要な符号が次々と発明されている。1959年に A. Hocquenghem が、1960年に R.C. Bose と D.K.R-Chaudhuri が復号の容易な符号を提案した。この符号は提案者の頭文字を取り BCH 符号と呼ばれている<sup>(15)</sup><sup>(16)</sup>。更に、1963年に R.G.Gallager が LDPC (Low Density Parity Check) 符号を、MIT Press から出版された同氏の博士論文の中で提案している<sup>(17)</sup>。しかし、LDPC 符号の復号は当時の計算機では実現が難しかったため、余り注目されることはなかった。そのため、1996年に D.J.C. MacKay や R.M. Neal らに

より再発見されるまでの30年以上の間、LDPC 符号は沈黙を保っていたのである。

### 3. 1960年代後半の符号理論

前章で述べたように日本における符号理論の研究は1950年代から行われていたが、ある程度組織的に行われるようになってきたのは、1961年 Peterson の Error-Correcting Codes が MIT Press から発刊されてからであろう。これは、見事に体系化された代数的符号理論の最初の著書であり、それが世界の通信理論の研究者に与えたインパクトは極めて大きいものがある。

1960年代半ば、大阪大学と東京大学に、日本における符号理論の研究拠点が形成され始めた。大阪大学では、嵩氏、滑川敏彦氏の研究室が拠点となり、東京大学では、瀧保夫教授と宮川洋教授の研究室が拠点となっていったのである。筆者の一人今井 (以下3., 4., 5. では筆者と呼ぶ) は1965年10月に宮川研究室に卒論生として入り、1966年4月に大学院生となり、1971年まで同研究室に在籍した。修士課程の2年間においては、スペクトル拡散方式が主要な研究課題であったが、符号理論の研究も始めている。宮川教授の講義で聞いた誤り訂正符号の話がとても面白く、前述の Peterson の著書を夢中になって読み、研究らしきことも始めたのである。

筆者が宮川研究室に入ったのと同じ1965年10月、岩垂好裕氏が MIT の留学を終え、瀧研究室に博士課程の学生として復帰された。その当時、阪大の嵩氏は符号理論研究者として既に国際的に知られる存在であったが、東大は符号理論研究が行われているとはいえない状況であった。しかし、1960年代後半には、東大も符号理論の拠点到るようになっていくことになる。その原点となったのは、Peterson の著書と岩垂氏の復帰であったといえよう。

岩垂氏は瀧・宮川研究室に MIT の風を吹き込んでくれた。筆者は様々なことを岩垂氏から学んだが、特に国際的視点で見ることの重要性を教えて頂いたことはその後の筆者の研究活動に大きな影響を与えた。とはいえ、インターネットもなく渡航もままならない当時、米国と日本における情報の格差は画然としていた。筆者もそれを思い知らされることが多々あった。その一例を示しておこう。それは2002年に本会の情報理論研究会で行ったフェロー就任記念講演「私の失敗」<sup>(18)</sup>にも述べた接続符号 (Concatenated Code) に関する話である。

接続符号は G. D. Forney Jr. が MIT の博士課程のときに発明した符号であり、その後、誤り訂正符号化の基本的手法として、広く用いられてきた。Forney は接続符号とその特性に関する解析を中心とした博士論文を1966年に MIT Press から出版し<sup>(19)</sup>、これにより接続符号は一般に知られるようになる。しかし、日本にこの本が入ってきたのは1967年のことであったと思われる。

1967年修士課程2年のときに、Forney と独立に同じ構造の符号を考え、宮川教授と連名で、電子通信学会 (現電子情報通信学会) の大会で発表することとした。ところが、発表申込みをした後、宮川教授が Forney の本を見つけ、筆者に渡された。それを検討してみると全く同じアイデアであり、がっかりした

ことをよく覚えている。ただし、Forney は理論的に見事な解析を行っていたのであるが、筆者は具体的な例を幾つか取り上げ、単一の BCH 符号を用いるより優れた特性を持つ場合があることを示しただけであり、やはりまだまだ修行が足りないと感じたものである。しかし、また、自分のアイデアも世界のトップに近いところまでは行くと、妙に安心したりもした。結局、電子通信学会の大会は Forney の結果を引用しつつ、鎖状符号という名前で、自分で最初に考えた具体例の特性の計算結果を示すこととなった<sup>(20)</sup>。1年以上遅れていたため、独立に見出したということもできなかったのである。

1960年代後半における日本からの符号理論の研究成果としては、嵩氏の BCH 符号の重み分布及びそれから出てきた CDMA 用系列(嵩系列)<sup>(21)</sup>、岩垂氏のバースト誤り訂正畳込み符号(岩垂符号)<sup>(22)</sup>、そして東大の羽鳥光俊氏らの E 系列の研究<sup>(23)</sup>などがある。これらは、いずれも世界的レベルに達する研究成果であった。

世界的には、この時期、符号理論の研究成果として前述の連接符号のほかに、ビタビ(Viterbi)復号法<sup>(24)</sup>やパーレカンブ・マッシィ(Berlekamp Massey)復号法(以下、BM 復号法)などがある。BM 復号法は1968年に刊行された E. R. Berlekamp の “Algebraic Coding Theory”<sup>(25)</sup>で示された。この著書は難解さで有名であったが、それでも夢中になって輪講したものである。数学的にも極めて高度なこの著書の中で、Berlekamp が符号理論は工学理論であり、実際に役に立たねばならない、という立場を明確にしていたことは印象的であった。当時、符号理論は、符号器・復号器が複雑になり過ぎて実際には使えない、机上の空論といわれたものである。このような中で、Berlekamp の著書は筆者らを励ましてくれるものであった。この著書が、その後の代数的符号理論の進展に大きな寄与をしたことはいまでもない。

#### 4. 1970年代の符号理論

1970年代になると日本においても、符号理論は、それに携わる研究者も増え、急速に進展していった。筆者もこの時代に幾つかの成果を挙げることができた。ここでは、二つ示しておこう。

一つの研究は二次元系列(アレー)と二次元巡回符号に関するものである。これは筆者が1971年に横浜国立大学に着任してからもしばらく続けた。この研究の契機となったのは、福田明氏の研究である。同氏は当時、東京大学野村研究室の大学院生で筆者の1年後輩であった。同氏の電子通信学会の大会での二次元系列の研究発表に宮川教授が関心を持たれ、筆者に示されたのである。宮川教授は、二次元符号や系列について、それ以前から関心を持たれ、卒業研究などのテーマにもなっていた。筆者は福田氏の見いだした構成法を一般化し、二次元シフトレジスタ及びそれによる二次元系列の構成理論を構築した。更に、それを二次元巡回符号の理論に一般化し、二次元バースト誤りを訂正する符号として二次元ファイア符号などを構成した。

二次元系列の理論<sup>(26)</sup>及び二次元ファイア符号<sup>(27)</sup>はそれぞれ IEEE の情報理論誌に採録された。そこまでは良かったのであ

るが、二次元巡回符号の理論を同じ情報理論誌に投稿したところ、これが余りに数学的過ぎるという理由で返戻されたのである。この論文は、後に Information and Control 誌に投稿し掲載された<sup>(28)</sup>。しかし、最初にまとめてから掲載されるまでに、5年近く要してしまった。このため、この研究に嫌気がさして、二次元巡回符号の研究から離れてしまったが、この研究は後に、阪田省二郎氏に引き継がれ、代数幾何符号の復号法である阪田アルゴリズム<sup>(29)</sup>の誕生につながったのである。また、後に、R. E. Blahut や V. Kumar が二次元系列について研究し、英国の P. Farrel が二次元バースト誤り訂正符号について研究したのであるが、筆者らの研究からそれほど進展したものではないようである。

もう一つの研究は、マルチレベル符号化とマルチステージ復号の研究である。筆者が東大在学中に宮川教授の指導の下、当時郵政省から宮川研に研究生として来ていた片岡志津雄氏とともに研究を開始し、その後、筆者が横浜国立大学に着任してから再開した研究である。横浜国立大学では、1972年筆者の研究室に平川秀治氏が卒論生として配属されたのを契機に再開した。平川氏は1975年修士課程を修了した後、東大宮川研に博士課程の学生として入学したが、実質的な指導は筆者に任せて頂いた。この間に、マルチレベル符号化とマルチステージ復号の論文が完成したのである<sup>(30)</sup>。これは、G. Ungerboeck のトレリス符号化の論文<sup>(31)</sup>とともに符号化変調という大きな研究分野を開いた論文となった。

この時期の日本発の符号理論の重要な成果としては、当時阪大で研究を行っていた杉山康夫氏、平澤茂一氏、笠原正雄氏、滑川氏の「ユークリッド復号法」<sup>(32)</sup>の研究がある。これは機能としては BM 復号法と同一であるが、分かりやすさという点に大きな利点があり、その後の RS 符号や BCH 符号の実用化に大きな役割を果たした。

また1970年代は日本語の符号理論の著書が出版され始めた時期としても特筆に値する。1973年に宮川・岩垂・今井共著の「符号理論」<sup>(33)</sup>が、1975年に嵩・都倉信樹・岩垂・稲垣康善共著の「符号理論」<sup>(34)</sup>がそれぞれ出版された。理論的には後者の方が深かったのであるが、応用という点では前者の方が分かりやすかった。このため、前者が1980年代における符号理論応用の進展に果たした貢献は決して少なくない。

更に、1978年に瀧、滑川、宮川、重井芳治、嵩の各教授を中心として「情報理論とその応用シンポジウム(当時は情報理論とその応用研究会)」の第1回が開催されたこともその後の日本における符号理論の発展に大きな影響を与えたといえるだろう。このシンポジウムは現在情報理論とその応用学会主催のシンポジウム SITA として毎年1回開催されている。また、1990年からは情報理論とその応用国際シンポジウム ISITA も隔年で開催されるようになり、符号理論を含む情報理論分野の国際化にも大きな貢献をしてきた。

## 5. 1980年代の符号理論

1980年代は符号理論の応用の時代といえるであろう。第1に挙げるべきものは1980年のソニーとフィリップスによるCDの開発である。これには二重誤り訂正RS符号が使われている。多くの符号理論研究者は、当時このような誤り訂正符号がコンパクトな家庭用機器で使えるとは想像もしていなかっただけに、その驚きは大きかった。CD開発の成功は半導体技術の急速な進歩によるところが大きい。当時のソニーの技術者の符号理論に対する深い理解と強い開拓者精神がもたらしたものとみえる。後に聞いた話であるが、ソニーの技術者たちは宮川・岩垂・今井の「符号理論」を必死になって輪講したとのことである。とすれば、この著書が符号理論の応用に果たした役割は小さくないかもしれない。

このころから、多くの符号理論研究者は応用に強い関心を持ち始めた。筆者らもCD、コンピュータのメモリ、無線通信をターゲットとして、BCH符号やRS符号の復号法の研究を盛んに行った。特に、電子計算機の主記憶装置などには高速復号が要求されたので、ROMを用いる復号法を検討した<sup>(35)</sup>。このような研究の中から、当時の大学院生山岸篤弘氏の努力により、テレビ会議の通信システムのための誤り制御方式の国際標準につながるものも現れた。

また、復号高速化の研究の中で、ガロア体における逆元計算の高速化が必要となった。このため、大学院生の上柳裕氏との共同研究で、ガロア体の部分体を用いるアイデアを出し、復号法に関する電子通信学会論文誌の論文の中で簡単に発表した<sup>(36)</sup>。しかし、符号で用いるガロア体は比較的小さなものであるため、そのインパクトは余り大きなものではなかったし、我々もこのアイデアを理論的に整備しないまま、放っておいた。ところが、後に、我々の研究とは独立ではあるが、同じアイデアに基づいて、東京工業大学の伊東利哉氏と辻井重男氏とが逆元計算の単純化の方式を示された<sup>(37)</sup>。これは、現在暗号の装置化にしばしば用いられている。

符号理論の応用の展開に伴って、様々な要求に応じる誤り訂正符号や復号法の研究も盛んになってきた。非対称誤り、不均一誤りなどを訂正する符号の研究やアナログ的な情報を利用して復号の性能を向上させる軟判定復号法の研究などであり、日本でも多くの研究成果が得られている。

また、その一方で、代数的誤り訂正符号の基礎的研究も盛んに行われていた。特に、1981年にV. D. Goppaにより提案された代数曲線上の符号(代数幾何符号)<sup>(38)</sup>の研究が大きなブームとなったのである。その中で前述の阪田アルゴリズムは大きな注目を集めた。

代数幾何符号はRS符号を一般化したもので、RS符号よりも符号長を長くできるという利点を持っている。しかし、現在までのところ実用化には至っていない。ほとんどの場合RS符号で十分なのである。しかし、代数幾何符号の研究はだ円曲線上の演算の研究を活性化させ、境隆一氏、大岸聖史氏、笠原氏によって初めて提案された公開鍵暗号を置き換え得る新たな暗号方式<sup>(39)</sup>につながっていった。このように、符号理論の研究は

1980年代以降隆盛を極めていく暗号理論の研究にも大きな影響を与えている。

1980年代における日本の符号理論学界最大のイベントは1988年IEEE情報理論国際シンポジウム(ISIT)が神戸で開催されたことである。これにより日本の符号理論学界の国際的地位は急速に向上した。1990年には前述のISITAがハワイで開催されたし、符号理論分野において最も権威のあるIEEE情報理論ソサイエティで重要な役割を果たす研究者も増えてきた。2003年には再びISITを横浜で開催し、2004年にはIEEE情報理論ソサイエティの会長を務めるまでになるのである。

## 6. 1990年代以降

1990年代以降、符号理論に新たなパラダイムが生まれる。その端緒となったのは、符号理論研究者にとって長年の夢である通信路符号化定理による理論限界に接近する符号が現実的な意味で構成されたことである。これまでの符号理論では最小距離や符号化率などの符号の構造が誤り耐性を主に左右すると考えられてきた。ところが、構造が極端に良い符号を構成しなくとも、ある程度構造の良い符号に優れた復号法を適用することで理論限界に接近できることが明らかになったのである。そういった符号として、ターボ(Turbo)符号とLDPC符号がある。これらの符号は復号の簡単な符号を幾つか組み合わせで構成される。そして組み合わせられた符号に対するそれぞれの復号器間で推定語の情報を交換する。こうすることで非常に良い誤り耐性が実現されることが分かった。情報の交換を繰り返し行うことから、この復号法は反復復号法と呼ばれている。現在の符号理論は、反復復号法の本質は何か、反復復号法の価値を引き出す符号の構造は何かをテーマとした研究が中心に行われている。

ターボ符号が発表されたのは1993年で、国際研究集会ICC93であった<sup>(40)</sup>。発表者はC. Berrou, A. Glavieux, P. Thitimajshimaで、当時この3名は符号理論の研究者間では全くの無名であったし、この講演にはあいまいに感じられる点が見られたために、彼らの成果をにわかに信じられない研究者が少なくなかった。しかし、性能の良さが徐々に確認され、ターボ符号の真価は認められていった。

ターボ符号は実用面でも優れた符号であり、第3世代の携帯電話システムであるW-CDMAのデータ通信部における誤り訂正符号として採用されたことが、その実用化への先鞭を付けた。これに対する日本の貢献は大きい。例えば、W-CDMAにおけるターボ符号のインターリーブの標準として素数インターリーブ<sup>(41)</sup>が採用されているが、これは須田博人氏らの提案である。

LDPC符号が再発見されたのは、1996年のことである<sup>(17)</sup>。MacKayらにより、LDPC符号もまた理論限界に接近する符号であることが確かめられた。2.でも述べたが、LDPC符号が提案されたのは1963年のことである。発明された年代を考慮すればLDPC符号こそが理論限界に最初に接近した符号であるといえる。

これら二つの符号はほぼ同時期に注目されたにもかかわらず、現在の日本ではターボ符号よりもLDPC符号の研究が活

発に行われている。これらの符号を扱う研究集会は情報理論とその応用学会における活動として、2001年には「確率伝搬に基づく復号法と符号ワークショップ」であったが、2004年には「LDPC/ターボ符号ワークショップ」であり、そして2006年以降は「LDPC符号ワークショップ」が開催された。LDPC符号が注目されていった原因は一つではないが、最もよく耳にするものは知的財産権に関する問題である。ターボ符号は基本特許や周辺特許などの知的財産権が発明者らにより広く取得されている。その一方で、LDPC符号は1960年代に発明されたため、基本的な要素技術が公知技術となっている。そこでLDPC符号は大学のみならず、企業も取り組みやすい研究だといわれている。

日本ではLDPC符号を学ぶ環境作りが積極的に進められてきた。上に挙げた一連のワークショップもその一つである。LDPC符号ワークショップでは情報セキュリティへの応用や実装といった挑戦的な話題も取り上げられ、多方面にわたる研究者の興味を集めている。また、和田山正氏により教科書<sup>(42)</sup>が日本語で書かれた効果も大きい。

最近では情報技術の標準化においてLDPC符号の採用が目立っている。例を挙げれば、衛星通信の規格DVB-s2、無線LANの規格IEEE802.16e、10GBASE-Tの企画IEEE802.2anなどがある。IEEE802.2anのLDPC符号は2004年にNECエレクトロニクス、東京電力、産業技術総合研究所による共同提案が採用されている。

ここからは符号理論の別の潮流について述べる。それは量子物理の研究から生まれた理論である。量子状態をある程度の期間保護するには特別な技術が必要とされる。なぜなら量子状態は非常に壊れやすく、その上未知の量子状態を観測すると状態が破壊されるという特徴を持つためである。そこで、量子状態を保護する新たなアイデアが待たれていた。この問題に対し、符号理論が一つの解を与えた。

1995年、P.W.Shorは3ビットの繰返し符号の拡張が量子状態の保護に応用できることを示したのである<sup>(43)</sup>。このアイデアは翌年、A.R.CalderbankとShorにより一般の古典符号の対を用いる方法へ拡張された<sup>(44)</sup>。同年、独立してA.M.Steaneが同じ方法を提案した<sup>(45)</sup>。その際にSteaneはハミング符号とその双対符号を用いた例を提示した。繰返し符号やハミング符号といった基礎的な符号が量子符号の扉を開いたのである。古典符号の対を用いて構成する量子符号は3人の名前の頭文字を取ってCSS符号と呼ばれている。

日本での量子符号に関する最初の重要な成果は、2000年に出版された松本隆太郎氏による量子符号の準位の一般化<sup>(46)</sup>であろう。2000年は、量子暗号の安全性証明<sup>(47)</sup>のアイデアとしてCSS符号が使われた年でもある。日本で量子暗号装置が開発され始めた時期と重なり、量子符号への注目が集まっていった。

最近では、ゴーレイ符号から作られる組合せデザインを用いた量子ジャンプ誤り訂正符号の構成法<sup>(48)</sup>が城本啓介氏らにより提案されている。また、量子誤り訂正符号とLDPC符号を組み合わせた量子LDPC符号の構成法<sup>(49)</sup>が著者らにより提案された。量子符号は理論限界を達成する符号が実現されておらず、

今後の動向が注目されている。

最後に、身近な符号理論の応用例としてQR(Quick Response Code)コード<sup>(50)</sup>を挙げたい。QRコードには誤り訂正符号としてRS符号とBCH符号が用いられている。コードの一部が汚れていても読み取れるのは、誤り訂正符号の賜物である。最近では、コードの一部をイラストやロゴなどに書き換えて利用者の興味をひき、また利用者に使いやすくするといった応用を目にする。このような書換えは雑音を人為的に付加することを意味する。本来信頼性向上のために挿入された冗長度を、利用者の利便性のために、人為的雑音を付加するために用いているのである。言い換えれば、誤り訂正符号を単に汚れによる雑音ばかりではなく人為的な雑音も生じる通信路に対して用いていることになる。

これまで、符号理論は新たな通信路モデルの出現により大きな発展を遂げてきた。例えば多値通信路、量子通信路、非対称通信路、そして多端子通信路などがある。近年注目を集めているネットワーク符号化<sup>(51)</sup>では、ネットワークが通信路モデルとして導入された。これらの通信路は通信の形態や実装の進化により引き起こされる新たな雑音をモデル化してきたものといえよう。人と情報通信システムが極めて密接かつ複雑にかかわるようになった今日、人為的な雑音も含む通信路に対する符号化が大きな研究課題に発展するかもしれない。

筆者の一人萩原は誤り訂正の訂正範囲を超えた面積をイラストにする手法を提案している<sup>(52)</sup>。図1は情報の内容を利用者が見た目でも想像できるよう意識しデザインしたものである。食事に関連した情報と推測できるだろう。

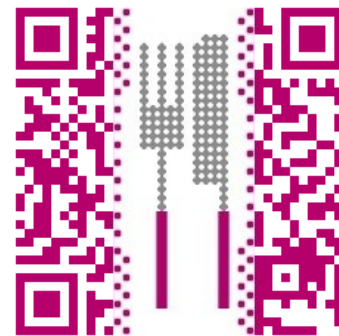


図1 携帯電話などのバーコードリーダで読み取れるイラスト入りの二次元コード

## 7. むすび

40年前、符号理論が「机上の空論」といわれた時代があった。その当時、符号理論の研究者の多くは、ただ符号理論が面白いから研究に没頭したのであろう。彼らは、いつかきっと符号理論が役に立つ日が来ると思いながらも、この難解で美しく役に立たない理論をそれゆえに誇りに思っていた節もある。そのような研究者により、符号理論の原点が形作られたのである。

30年前、「符号理論は死んだ」といわれたことがあった。もは

や研究すべきことが残っていないと思われたからである。しかし、やがて符号理論の応用が急速に進展し、デジタル時代に不可欠な理論となり、応用から符号理論の新たな展開が生まれた。その後も何度か「符号理論は死んだ」といわれた時期があった。しかし、そのたびに、符号理論は新しい種を見つけ、それを育てることにより、更に発展してきたのである。符号化変調、代数幾何符号、ターボ符号、そして LDPC 符号の再発見などである。符号理論は美しさとともに、不屈なたくましさも合わせて持っている。

符号理論の日本における歴史をたどってみると、日本が符号理論の世界において、要所で活躍してきたことが見えてくる。それは基礎理論においても、新たな研究分野の開拓にでもあり、また符号理論の応用においてもであった。特に符号理論の応用に関しては、幾つかの面で日本は世界を先導する役割を担ってきた<sup>(41) (53)</sup>。しかし、そこに大きな問題も見えてくる。日本で生まれた優れたアイデアが、日本において実用化され、世界に広がるということが少なかったことである。これは、符号理論に限らないが、我が国として今後解決していくべき課題である。

さて、ターボ符号の出現や LDPC 符号の再発見から既に 10 年余り経過している。符号理論の重要な発明や発見はこれまでおよそ 10 年ごとに行われてきた。そろそろ新たな大発明が現れてもよい時期であるが、Shanon による通信路符号化の限界に近い特性を持つ符号化・復号方式が実現された現在、符号理論に新たな風を吹き込む大発明はもはやないと考える向きも少なくなっている。しかし、筆者らは、情報技術の発展に支えられ急速に変化していく現代社会が、新たな情報伝達・記録・処理のモデルを生み出し、それにより新たな符号が必要とされ、符号理論における大発明につながるような気がしている。それが、日本で生まれ、日本で実用化され、世界に広がっていくことを期待したい。

## 文 献

- (1) C. E. Shannon, "A mathematical theory of communications," Bell Syst. Tech. J., vol.27, pp.379-423, pp.623-656, 1948.
- (2) R. W. Hamming, "Error detecting and error correcting codes," Bell Syst. Tech. J., vol.29, pp.147-160, 1950.
- (3) 三谷尚正, "Error Detection および Error Correction Code について," 電気試験所彙報, vol.15, no.5, pp.18-22, May 1951.
- (4) 三谷尚正, "逐次計算機における数の伝送について," 電気三学会東京支部連合大会, 1. 12, Nov. 1951.
- (5) I.S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," IRE Trans., vol. PGIT-4, pp.38-49, 1954.
- (6) D.E. Muller, "Application of boolean algebra to switching circuit design and error detection," IRE Trans., vol. EC-3, pp.6-12, 1954.
- (7) W. W. Peterson, Error-Correcting Codes, MIT Press, Cambridge, Mass, 1961.
- (8) W. W. Peterson and E. J. Weldon, Error-Correcting Codes, 2nd ed., p.72, MIT Press, 1972.
- (9) Z. Kiyasu, "Research and development data," no.4, Electrical Communication Laboratory, Nippon Telecom Corporation, Tokyo, 1953.
- (10) 有本 卓, "p 元群符号系の符号化, 復号法と誤りの訂正機構," J. Inf. Process. Soc. Jpn., vol.2, no.6 19611115, pp.320-325, 1961.
- (11) I.S.Reed, and G.Solomon, "Polynomial codes over certain finite fields," SIAM J. Appl. Math., vol.8, no.2, pp.300-304, 1960.
- (12) T.Kasami, "Cyclic codes for burst-error-correction," J. Inst. Electr. Commun. Eng. Jpn. vol.45, pp.9-15, 1962.
- (13) T.Kasami, "Optimum shortened cyclic codes for burst-error-correction," IEEE Trans. Inf. Theory, vol.IT-9, no.2, pp.105-109, 1963.
- (14) Y.Komamiya, "General theory of most efficient codes," Report no. 163, NBS 6420479 (Box 277, folder 6), June 1964.
- (15) A.Hocquenghem, "Codes correcteurs d'erreurs," Chiffres, 2, pp.147-156, 1959.
- (16) R.C.Bose and D.K.Ray-Chaudhuri, "On a class of error correcting binary group codes," Inf. Control, vol.3, pp.68-79, March 1960.
- (17) R.G.Gallager, Low Density Parity Check Codes, in Research Monograph Series, Cambridge, MIT Press, 1963.
- (18) 今井秀樹, "私の失敗," 信学技報, IT2001-63, pp.61-66, March 2002.
- (19) G. D. Forney Jr., Concatenated codes, MIT Press, Cambridge, Mass, 1966.
- (20) 宮川 洋, 今井秀樹, "鎖状符号化による通信方式," 昭 42 信学全大, 1279, Oct. 1967.
- (21) T. Kasami, "Weight distribution formula for some class of cyclic codes," Tech. Report no. R-285, Univ. of Illinois, 1966.
- (22) Y. Iwadare, "On type B1 burst-error-correcting convolutional codes," IEEE Trans. Inf. Theory, vol. IT-14, no.4, pp.577-583, 1968.
- (23) 滝 保夫, 宮川洋, 羽鳥光俊, 難波誠一, "E 系列について," 信学技報, IT67-58, Feb. 1968.
- (24) A. J. Viterbi, "Error bounds for convolutional codes and asymptotically optimum decoding algorithm," IEEE Trans. Inf. Theory, vol. IT-13, no.2, pp.260-269, 1967.
- (25) E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.
- (26) T. Nomura, H. Miyakawa, H. Imai and A. Fukuda, "A theory of two-dimensional linear recurring arrays," IEEE Trans. Inf. Theory, vol.IT-18, no.6, pp.775-785, 1972.
- (27) H. Imai, "Two-dimensional fire codes," IEEE Trans. Inf. Theory, vol. IT-19, pp.796-806, 1973.
- (28) H. Imai, "A theory of two-dimensional cyclic codes," Inf. Control, vol. 34, pp.1-21, 1977.
- (29) S. Sakata, "Decoding 2D cyclic codes by parallelizing the 2D Berlekamp-Massey Algorithm," Proc. EUROCODE'92, pp.277-289, 1993.
- (30) H. Imai and S. Hirakawa, "A new multilevel coding method using error-correcting codes," IEEE Trans. Inf. Theory, vol. IT-23, no.3, pp. 371-377, 1977.
- (31) G. Ungerboeck, "Channel coding with multilevel/phase signals," IEEE Trans. Inf. Theory, vol. IT-28, no.1, pp.55-67, 1982.
- (32) Y. Sugiyama, M. Kasahara, S. Hirasawa and T. Namekawa, "A method for solving key equations for decoding Goppa codes," Inf. Control, vol. 27, pp.87-99, 1975.
- (33) 宮川 洋, 岩垂好裕, 今井秀樹, 符号理論, 昭晃堂, 1973.
- (34) 嵩 忠雄, 都倉信樹, 岩垂好裕, 稲垣康善, 符号理論, コロナ社, 1975.
- (35) 山岸篤弘, 今井秀樹, "ROM を用いた BCH 符号の復号器の一構成法," 信学論 (D), vol.J63-D, no.12, pp.1034-1041, Dec. 1980.
- (36) 今井秀樹, 上柳 裕, "2重誤り訂正 BCH 符号の並列復号器について," 信学論 (D), vol.J60-D, no.9, pp.761-762, Sept. 1977.
- (37) T. Itoh and S.Tsujii, "A fast algorithm for computing multiplicative inverses in GF(2<sup>m</sup>) using normal bases," Inf. Comput. vol.78, no.3, pp.171-177, 1988.

- (38) V. D. Goppa, "Codes on algebraic curves," Soviet Math. Dokl., vol. 24, pp.170-172, 1981.
- (39) 境 隆一, 大岸聖史, 笠原正雄, "楕円曲線上のペアリングを用いた暗号方式," SCIS 2001, no.7B-2, pp.369-374, 2001.
- (40) C.Berrou, A.Glavieux, and P.Thitimajshima, "Near shannon limit error-correcting coding: turbo codes," in Proc. IEEE International Conf. Commun. (ICC93), vol.2, pp.1064-1070, Geneva, Switzerland, May 1993.
- (41) 須田博人, 渋谷昭範, 今井秀樹, "素体を利用したターボ符号用インターバ," 信学論(A), vol.J85-A, no.11, pp.1168-1181, Nov. 2002.
- (42) 和田山 正, 低密度パリティ検査符号とその復号法, トリケップス, 2002.
- (43) P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A, vol.52, no.4, pp.R2493-R2496, 1995.
- (44) A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," Phys. Rev. A, vol.54, no.5, pp.1098-1105, 1996.
- (45) A. M. Steane, "Error correcting codes in quantum theory," Phys. Rev. Lett. vol.77, no.5, pp.793-797, 1996.
- (46) R.Matsumoto and T.Uyematsu, "Constructing quantum error-correcting codes for  $p^m$ -state systems from classical error-correcting codes," IEICE Trans. Fundamentals, vol.E83-A, no.10, pp.1878-1883, Oct. 2000.
- (47) P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett., vol.85, no.2, pp.441-444, 2000.
- (48) M. Jimbo and K. Shiromoto, "A construction of mutually disjoint Steiner systems from isomorphic Golay codes", Comb Theory A, submitted.
- (49) M.Hagiwara and H.Imai, "Quantum quasi-cyclic LDPC codes," Proc. IEEE ISIT 2007, pp.806-810, 2007.
- (50) 二次元コードシンボル - QR コード - 基本仕様, 日本工業規格, JIS X 0510, 2004.
- (51) Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow", IEEE Trans. Inf. Theory, vol. IT-46, no.4, pp. 1204-1216, 2000.
- (52) 萩原 学, "アキバ道研究屋稼業," 数学セミナー, 2009年1月号, pp.102-103, Dec. 2008.
- (53) D.J. Costello, Jr., J. Hagenauer, H. Imai, and S.B. Wicker, "Applications of error-control coding," IEEE Trans. Inf. Theory, vol.44, no.6, pp.2531-2560, 1998.

(平成 21 年 1 月 13 日受付)



今井秀樹 (正員:フェロー)

昭 41 東大・工・電子卒・昭 46 同大学院博士課程了・工博・同年横国大講師(工・電気)・昭 47 同助教授・昭 59 同教授(工・電子情報)・平 4 東大教授(生産技術研)・平 18 より中大教授・東大名誉教授・平 17 産総研情報セキュリティ研究センター長兼務・現在に至る。この間、符号理論とその応用、暗号と情報セキュリティ、スペクトル拡散方式、データ圧縮、移動通信などの研究に従事。

昭 50 年度、平 2 年度本会著述賞、平 3, 14, 15, 19 年度同論文賞、平 3 年度同米澤ファウンダーズ・メダル、平 7 年度同業績賞、平 14 年度同猪瀬賞、平 15 年度同功績賞、平 10 IEEE シヤノン 50 周年記念論文賞、平 6 情報通信月間推進協議会情報通信功績賞、平 6, 15 電気通信普及財団テレコムシステム技術賞、平 14 総務大臣表彰、経済産業大臣表彰、平 21 年内閣官房長官表彰、平 11, 14 名誉博士号(韓国順天郷大、仏国ツールン大)、平 17 エリクソン・テレコミュニケーション・アワード、平 19 英国コンピュータ学会 Wilkes 賞、情報セキュリティ文化賞、平 20 JWIS 特別功労賞、大川賞などを受賞。

本会理事、監事、基礎・境界ソサイエティ会長、IEEE 情報理論ソサイエティ会長、国際暗号研究会(IACR)理事、情報理論とその応用学会会長、国際会議 ASIACRYPT, PKC, WPMC 運営委員長などを歴任。総務省・経済産業省暗号技術検討会(CRYPTREC)座長、IEEE 東京支部長、日本学術会議会員。IEEE Life Fellow, IACR Fellow。



萩原学 (正員)

1997 千葉大理・数学卒、1999 東大大学院数理科学研究科修士課程、2002 同博士課程了。博士(数理科学)取得。2002 京大数理解析研究所長期研究員。2002-2005 東大生産技術研究所学術支援研究員。2005-現在 独立行政法人産業技術総合研究所情報セキュリティ研究センター研究員。2008-現在 中央大学研究機構機構構准教授。