No. 40 2001 年 11 月 28 日発行

SITA 情報理論とその応用学会ニューズレター

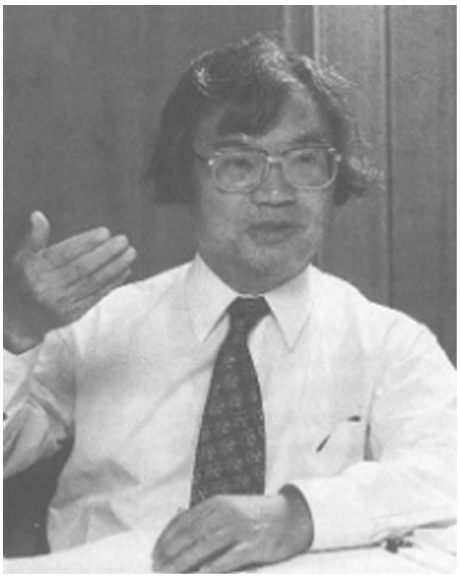
Claude Elwood Shannon 博士追悼特集号

シャノンの与えた影響と人となりを追悼して

有本 卓（立命館大学理工学部）

自分自身が研究者になろうとしたよりどころは，すべて，シャノンにあった．筆者は 1959 年春京都大学理学部の数学科を出て，すぐ，沖電気工業 (株) に入り，当時で言うところの電子計算機の開発チームに加わった．最初に命じられてやった仕事は，パラメトロン計算機の論理回路図面を首引きしながら，テスターを使って導通テストし，実際の配線をチェックすることであった．そこで勉強したのがブール代数であり，スイッチング回路の理論であったが，そのきっかけはシャノンの修士論文にあることはチームのチーフから聞かされた．

1960 年の秋，磁気コアメモリを主メモリとして実装した計算機をデータショウに出展することが決まった．しかし，ビット落ちが激しく，折角作った”e”や”π”のデモ用計算プログラムばかりか，ブートストラップまで走りにくくなった．そこで，誤り訂正符号を使えばどうか、とチーフから提案され，符号理論を勉強し始めた．そして，シャノンのあの 1948 年の大論文に出会ったのである．そこには Hamming 符号が示唆されていたが，学会誌をたどっても巡回符号までしか出来ていなかった．そこでもっと使い易いものを見つけたが，これは，実際には，今で言う所の RS 符号（Reed-Solomon 符号）と同等のものであった．そのとき，システマティックな復号化アルゴリズムを見つけ出したので，1960 年夏には前述のプログラムを記憶するときに符号化し，テストしてみた所，上々の出来であった．この復号化アルゴリズムは IEEE Trans. on IT の 1960 年 12 月号に発表された Peterson のアルゴリズムとほとんど同じであった．



シャノンの大論文（1948 年）を読み通す力はなく，1962 年に東大に移る前頃に，岩波の応用数学講座で喜安善一・室賀三郎著「情報理論」を勉強した．それでも，確実に理解し得たわけではない．しかし，何よりも符号化する意味を体験し得たことによって，1963 年前後には，通信路符号定理の意味の技術的な重要さを何よりも直観し，意識するようになった．当時，小生の恩師であった南雲仁一先生は新進気鋭の数学者達と 1948 年の論文を輪読されていたが，誰もがきっちりと理解できないようだと言われていた．つまり，数学的な部分よりも，この論文のもつコンセプトの技術的な重要さの意味が数学者にはつかみきれなかったようである．

シャノンのあまり知られていない側面に，種々の仕掛

（gadget）を自宅の工房で造っていたことに見られる知的好奇心がある．上に挙げた「応用数学講座」にはさみ込まれた月報で故南雲仁一博士がシャノンの今で言う所の迷路探索する ”マイクロマウス ”を紹介されていた．それも 1961 年前後であったろう．筆者は 1962 年に東大に移り，主として，制御理論で論文を発表し，1968 年には大阪大学基礎工学部に移ったが，そこでは機械工学科に所属した．勿論，機械力学や機械制御の分野でも論文を出しながら，しかし，夜は一所懸命，情報理論のことを考えていた．1973 年にはその機械工学科の教授になってしまったが，その時，あまり迷わずロボティクスの研究を始めたのは，シャノンがチェスプレイするロボットを実際に作っていたことを知っていたからである．

1970 年代，情報理論関係の論文が少しは認められた頃，Yale 大学の T. Berger 教授や現 Illinoise 大学の R. Blahut 教授を日本学術振興会の援助で招待した．そして，色々とシャノンの人となりや事情を聞いた．シャノンは弟子達と共著の 1967 年の論文を最後に，学術論文は発表してはいないので，消息を知りたかったからである．Blahut 博士からは,「情報理論を専攻する学生が旅の途中で出会ったシャノンと名乗る学生に誘われるままに泊まったとき，ピアノを弾く老人を垣間見た．気になって彼に尋ねた所，その人が自分のあこがれのシャノン博士だった」というエピソードを聞いた．

小生にとっても憧憬の人には 1985 年 11 月の第１回の京都賞で会うことが出来た．受章式の翌日，受章を祝ってワークショップが開かれた．その企画は小生が担当したが，途中で横槍が入り，京都大学の有名な先生に変更になり，情報理論の最前線の研究者がはずされるという顛末もあった．当時の情報科学の研究者でさえ，シャノン流の情報理論が IT 時代の精神的支柱であることを理解し得ていた人は少なかったのである．ともかく 1985 年ではシャノンは第一線からしりぞいており，シャノンの講演は持参（門外不出と言っていたが）した 8 mm フィルムの上映が中心であった．その中に，あのチェスプレイする３本指をもったロボットがあったのである．

シャノンは非常に”shy”な性格であったので，寡黙でもあり，日常の会話もあまり進まないが，また，学術論文以外には，余計な雑文を沢山は書いていない．しかし，1950 年代には情報理論以外にも，AI に関連したいくつかのノートを残している（それらは，Sloane と Wyner による”C.E. Shannon Collected Papers”(IEEE Press, 1993) にある）．1986 か 87 年に行われた Michigan の ISIT でもシャノンは出席し，フォード 博物館の見学会には家族と同道していたが，そこには遠い親戚に当る発明王エジソンの作った仕掛けがいくつかあった．恐らく，本当はもっともっと多方面にわたって知的興味をもっていたに違いない．

上述の”Collected Papers”には，1983 年に Sceintific American の記者に会ったときの話しが出ている．その中に，シャノンの予測があるので再掲しておこう．”What can we expect in the future? Three advances in the artificial intelligence area would be most welcome. (1) An optical sensor-computer combination capable of learning to recognize objects, people, etc., as our eyes and occipital cortex do. (2) A manipulator-computer combination capable of the purposeful operations of the human hand. (3) A computer program capable of at least some of the concept formation and generalizing abilities of human brain.”

筆者は，今はむしろシャノンがホビーとしていたロボットの専門家になって，上述の予測の (2) を研究している．今やっと，人間の手指の器用さと知能の関係がニュートン力学によって紐解ける所まで来た．(3) は，実は，情報理論とロボティクスの接点上にある．ごく最近，ベイジアンネット上の”belief propagation”とターボ符号の復号化アルゴリズムが同じものであることが見出された．前者はもしかして，対話を始めるモデルになり得て，エンターテイメントロボットの基本ツールになるかもしれないし，後者は，勿論，シャノンの通信路復号化定理を体現する基本手段となりつつある．考えてみれば，シャノンの通信路容量は今やっと技術目標となってディジタル通信という現実の世界に機能し始めたのかもしれない．

シャノンの業績はともかく 20 世紀末迄にはほぼ認められたし，IT 革命という社会的な影響を与えることができた．そして，この 21 世紀の初頭になって，シャノンが亡くなった今，これからの情報通信と情報科学にはどんな新しい展開があり得るか，じっくりと考えてみたいと思う．筆者には無理であるが，そして，若い人々にはチャンスがあるかもしれないが，シャノンを乗り越え，時代を越える発見を 21 世紀のこれからの 10 年間に誰かがやり遂げ得るのだろうか．

C．E．Shannon　博士を悼む

飛田 武幸（名古屋大学名誉教授）

C.E.Shannon 博士の訃報を聞いたのは今年２月も押し迫った頃でありました。彼は「情報通信理論の父」と呼ばれ情報理論の創始と発展とにおける偉大な貢献でよく知られています。計算理論など、広く情報科学、情報工学、数理科学などの分野に亘った科学上の業績は２０世紀における学問の進歩の中で特筆されることは間違いないでしょう。

振り返って、私事を申し上げて恐縮ですが、私が Shannon の仕事を初めて知ったのは確か 1953 年（昭和２８年）のことであったと思います。大学を卒業したばかりの頃でしたが、京都大学でのシンポジュームで国沢清典先生が Shannon の情報理論の話をされました。技術の世界から新しい数学が生まれてくるのを目の当たりにして、大変感銘を受けました。その後ゆっくり勉強したくなり Shannon-Weaver の本 ”The Mathematical Theory of Communication” を入手することができました。感激したことは、エントロピーという情報量が、いくらかの妥当な要請のもとに一意的に定まるということでした。エントロピーという言葉自体は物理では、よく知られた概念でしたが、いわゆる Shannon のエントロピーが通信の数学的理論の基礎となる量として登場したことは大変な驚きでした。

京都大学に勤務中の 1962 年のことでしたが、若い二人の友人と Shannon-Weaver の本を一夏かかって読破したことは懐かしい思い出というよりは、私の情報理論への目覚めの時期というべきでしよう。エントロピーから初めてチャンネルのこと、情報伝達の話、どれも実学から起こった新しい数学として大変興味深いもので、フォローし難い個所は自分たちで定式化し直したりして、楽しい勉強会でした。遂に付録まで行って、関数空間の次元まで提案しているところには感激しました。これは周知のように、関数解析学において発展していたした内容であります。私は両者との関係は詳らかにしていませんが。

この頃、ソビエトでは、Kolmogorov をはじめ多くの数学者達がエントロピーを用いた確率論や解析学の研究を進めていて我々も大いに啓蒙されロシア語の辞書と首っ引きで文献を読みあさったものでした。日本の研究者達もこの新しい学問に対して自己啓発をしようとの意味もあって、若手の集まり確率論セミナーが「確率論の手引き」第４巻 (内部出版物ですが）として情報理論を上梓しました（1963 年)。Shannon から説き起こしたことは言うまでもありません。この企画には小野山卓爾氏を中心に何人かが協力しましたが、私もその中の一人でありました。力学系の研究にエントロピーを活用して確率論の話題にできそうだと、十時東生氏をオーガナイザーにしてグループで勉強会をもったのも自然な流れでした。

その後の私の研究生活の中で、若い時代のこのような経験は陰に陽に、大きな影響を与え続けてきたことに気づきます。単なる数学的内容というのではなくて、理論の背景にあるアイデアの卓越さ、最適化の手法、理論の育て上げ方など、どれもたいそう魅力的に映りました。

Shannon 自身のことにもどりますが、彼は 1937 年に書いた修士論文（MIT）で、それまで十進法で設計されていた計算機回路を二進法に変えるという革命的な提案をしたと聞きます。直接読んでみる機会を得ませんが、その卓越した発想には感心するばかりです。その後、彼はずっと計算と情報一筋に生きてきた科学者といえましょう。

これは、後になって気づいたことですが、驚くことに Shannon は情報理論より先に（1941 年)、計算の理論についてたいへん興味深い論文を発表していることです。アナログ計算です。嬉しいことに、その論文では、加法、積分、ギアボックス等など使用可能な機械の種類を決めておいて、どんな計算ができるかということから理論を展開していることです。具体的な課題から、数理を創造していく過程には惹かれるものがあります。いま量子計算に人々の関心が集まっているとき、そのアナログ的なもの、すなわち連続量の計算に関する彼のアイデイアを何とか新しい形でもっと活かしたいものです。　一方、Shannon によって確固たるものとなったエントロピーの概念や計算の手法も量子情報理論のなかで、新しい処を得て、主役を演じようとしてます。

まさに Shannon は情報理論を誕生させ、育て、そして未来への発展の夢を与えてくれた偉大な科学者であり、過去と現在と未来に大きな存在感を与え続けているリーダー

であると言うことができます。その業績は科学・技術の歴史の中で、いつまでもその輝きを失うことはないでしょう。

彼が受けた数々の栄誉では、とてもその業績の顕彰に足るものとは思えませんが、受賞のいくつかを思い出してみましょう。　1966 年には IEEE Medal of Honor; 1972 年に Harvey Prize; 1985 年に第一回の京都賞を受賞などなど枚挙に遑がありません。しかし、それらにも増して、IEEE,　IT, vol.44 (1998) では, 表紙を彼の写真で飾り ”Fifty years of Shannon Theory” として 22 ページにわたる 特集をしています。Shannon にとっては研究者冥利に尽きるものがあったのではないでしょうか。

偉人 Shannon の逝去にあたり New York Times はすぐに長い追悼文を載せましたが、伝記の抄約とでもいうところでしょうか。Science と Nature は、どちらも 4 月になって、比較的長文の追悼の言葉を述べていますが、その中に最大の賛辞を盛り込んでいました。たとえば、発明者、数学者でデジタル革命のリーダー、のように。悲しいことに、今や幽冥境を異にしてしまいましたが、Shannon は情報科学とともに、そして私の中でも永久に生き続けることでありましょう。

シャノン博士と符号理論・暗号理論

今井 秀樹，井坂 元彦 （東京大学）


符号理論の洗礼を過去に受けた研究者がシャノン博士を語る上では，それぞれの専門や時代を背景とした多様な視点が存在しえると思われる．それは研究体系の拡散と深化の証でもあろう．小文では，その源流たる「A Mathematical Theory of Communication」[1] でのシャノン博士による符号理論に対する最も重要な問題提起として，通信路符号化定理を満足する具体的な符号の構成に主眼を置き，研究成果を概観することにしよう．

漸近的によい符号の多くは，連接符号 [2] を基にして与えられているが，そこでは内符号をランダム符号化及び最尤復号，外符号に対して一般化最小距離復号を行う場合の符号化定理が示されている．特にジュステセン符号 [3] は，連接符号で内符号を複数用いることで，符号化及び復号に要する計算量が符号長に対して多項式的にしか増大せず，また最小距離と符号長の比が 0 に漸近しない性質を有する符号として初めて示されたものである．これをさらに一般化することで，通信路容量に任意に近い伝送速度において誤り率が符号長に対し，指数的に減少する連接符号を具体的に構成することができ，可変内符号を用いた対称通信路に対する符号化 [4]，さらにこれに通信路に依存する写像を施した一般の離散的無記憶通信路に対する符号化手法 [5]，及び外符号に代数幾何符号を用いることで誤り指数を大きく改善した符号 [6] などの結果が知られている．

一方で，信号対雑音比の高い領域での通信路容量に対しては，ユークリッド空間における符号の構成が不可欠となる．特に格子を基に符号を構成することでガウス性通信路における通信路容量を与えることができ [7][8]，ランダム符号化と対比的である．しかしながら，高次元における稠密格子の構成は長年の難問であり，かつ最小距離復号のためのトレリス複雑度が符号化利得に対して指数的に増大することも明らかになっている [9]．一方，2 元の信号点分割に基づくマルチレベル符号化 [10] において適切な 2 元符号を設計することで，比較的低複雑度の多段復号法 [10] によって符号化利得に関して最適性が失われないことが示されており [11,12]，純粋な意味でのランダム符号化よりも具体的な符号の構成法となっている．ガウス性通信路の通信路容量を与えるにはさらにシェーピング利得を得る必要があるが，伝送速度が高い場合には概ね符号化と分離して利得を得ることができる．

近年には，グラフ上にて符号を表現した上で，反復的に復号を行う手法が盛んに研究されている．トレリスによる状態実現と比して，グラフ中にサイクルを許容することで状態空間のサイズを大幅に削減できることから，線形時間で実行できる確率的な反復復号を視野に入れたランダム的な符号の見通しよい構成が可能となっている．この種の方法論はある意味で情報理論の本質を突いたものといえるが，これらに即した符号化定理も検討されている．最近になり再認識されている低密度パリティ検査（LDPC）符号

[13] では，検査行列中の各行各列の非零要素数により符号のアンサンブルが定義されるが，これと符号長の比が漸近的に 0 となるような低密度符号のアンサンブルの中に，最適な復号を行うことで通信路容量に任意に近い伝送速度を与えるものが存在することが示されている．しかし，反復復号に適したアンサンブルでは一般にこれは成立しない．符号化定理の導出を目的として考案された連接符号である RA（Repeat-Accumulate）符号 [14] は，内符号として符号化率 1/q の繰り返し符号を用い，得られた N 個の符号語をインタリーバによって置換した上で，符号化率 1 の再帰的符号化を行って長さ qN の符号語を得るものである．この簡素な符号も符号化率を十分に小さくした場合には最尤復号の下で，ガウス性通信路の通信路容量に漸近することが示されている [15]．一方，線形時間で行われる反復復号に対しては，2 元消失通信路（BEC）に対して通信路容量に任意に近い伝送速度を可能とする符号が与えられている [16,17]．ここでは，LDPC 符号において非正規グラフを用い，各ノードの次数を適切に設計することで符号のアンサンブルを得ている．また先に述べた RA 符号の内符号を，複数の符号化率の異なる繰り返し符号とインタリーバ及びその出力の検査和とすることで非正規化した IRA（Irregular Repeat-Accumulate）符号でも，BEC において同様の特性を与える系列が設計されている [18]．これらの符号は，ある種のランダム符号化とも捉えられるが，インタリーバやノードの結合により符号のアンサンブルが与えられる点において，より構成的といえよう．近年のグラフ上における確率的な復号法の隆盛により，ガウス性通信路においてターボ符号や LDPC 符号などの所謂”capacity-approaching codes”は多く認識されているが，その特性限界を示す閾値から”capacity-achieving”ではないことが知られており，BEC 以外に対する同種の成果は二元対称通信路（BSC）に対する最近の結果である文献 [19] 以外には殆ど見当たらないようである．

以上のように，通信路容量に漸近する符号の具体的構成法に関する成果は，数多ある符号理論の成果の中でもそれほど多く存在するわけではない．この状況では，シャノン博士の問題提起に符号理論が十分な解を提示したとは未だ言い難いようにも思われる．「符号理論は死んだ」と嘆く声はどの時代にも絶えることはないが，その度にシャノン博士の業績に立ち返り，そこから新たな発展が生まれてきた．シャノン博士の論文にはまだまだ含蓄が多い．それを踏まえることで，今後も符号理論が発展し続けることを筆者らは望んでいる．

次にシャノン博士と暗号理論の関わりについて述べよう．暗号の歴史は古く，暗号の理論的研究の歴史も，1000 年以上も前に遡る．この意味では，暗号理論におけるシャノン博士の重みは，シャノン博士が創始し情報理論におけるそれとは異なる．しかし，シャノン博士が暗号理論に与えた影響は小さくないし，情報理論と暗号理論の関わりも深い．国際暗号研究学会（International Association for Cryptologic Research）でも，シャノン博士は暗号理論の one of the fathers としている．

シャノン博士の暗号に関する最も重要な論文は，1949 年にやはり Bell System Technical Journal に掲載された「Communication Theory of Secrecy Systems」[20] である．これは 1945 年 9 月に「A Mathematical Theory of Cryptography」というタイトルでシャノン博士が書いた機密レポートを元にした論文である．このタイトルが「A Mathematical Theory of Communication」と対をなすのは，当時のシャノン博士の気持ちに思いを馳せる上で興味深いことといえよう．

シャノン博士はこの論文の中で，情報理論を暗号に応用し，暗号システムの情報理論的モデルを確立した．それまでも，暗号解析において平文や暗号文の確率の偏りに関する研究は重要な役割を担って来たのであるが，シャノン博士はこれを見事に理論化したと言えるだろう．これは，現在の共通鍵暗号の設計にも大きな影響を与えている．シャノン博士は，確率の偏りを減らし解読の困難な暗号を設計するために，暗号の構造として，今日 SPN 型（substitution と permutation を繰り返す構造）と呼ばれる構造を示唆している．昨年，米国連邦政府標準暗号 AES（Advanced Encryption Standard）に選ばれた Rijndael という暗号 [21] は，正にこの構造を持つ暗号であった．シャノン博士の暗号理論は，シャノン博士の情報理論と同様，現在も重要な意義を持っているのである．

もう一つの重要な成果は，暗号の安全性を情報量的な立場から見事に説明し，情報量的安全性という概念を明確にしたことである．真のランダム系列からなる暗号化鍵を使い捨てにするバーナム暗号が，いかに盗聴されても情報の漏洩が全くないという意味で，情報量的に完全な安全性（perfect secrecy）を持つことを明確に示したのもシャノン博士である [20,22]．

この情報量的安全性を持つ暗号は，一般に膨大な記憶量を要するため，特別な場合を除き実用には向かないと考えられてきた．このため，計算量的に安全な暗号が現代の暗号理論の中心となっている．これは，原理的に解読可能であるが，膨大な計算を要するため，実際上解読できないと考えられている暗号である．したがって，非常に能力の高い計算機が出現すれば，これらの暗号は破れてしまう．前述の AES など共通鍵暗号もそうであるが，1980 年代から，

暗号理論の主役となっている公開鍵暗号も計算量的な安全性に依存している．事実，公開鍵暗号として現在最もよく用いられている鍵長 1024 ビットの RSA 暗号は十数年後には解読される可能性が高い．電子署名法の施行や電子政府の進展等により，長期保存が必要な電子署名等にも公開鍵暗号が用いられるようになることから，長期の安全性が保証されないことは大きな問題となっている．

このため，最近になって情報量的に安全な暗号が見直されるようになってきた．近年のメモリの大容量化も，情報量的に安全な暗号を現実性のあるものとしてきている．筆者らは昨年，情報量的に安全な電子署名方式の構成にはじめて成功した [23]．今後，長期保存が必要な電子署名方式として，筆者らの方式が利用されるようになると期待している．守秘のための暗号ではなく，電子署名であるから，シャノン博士の情報量的な安全性の概念がそのまま適用できるわけではないが，この電子署名方式の基礎となったのも，シャノン博士の情報量に対する考え方であったことは間違いない．

シャノン博士の暗号理論への貢献はこれだけに留まらない．博士の情報理論が多端子情報理論に一般化されていく中で，情報理論的暗号理論も生まれてきた．これは，それぞれの経路で生じる雑音により正規の受信者と攻撃者の受ける情報に差異があることを利用して，情報量的に安全な暗号を実現しようというものである．その中から，最近ハーバード大学の M.O. Rabin のグループにより，攻撃者のメモリが制限されているとの仮定のもとで，情報量的に安全で，しかも比較的簡単に構成できる暗号方式が提案され [24]，ニューヨークタイムズの記事になるなど，大きな話題となった．この方式はその仮定に疑問が呈されているものの，一つの新しい方向として注目される．

このように，シャノン博士にゆかりのある暗号理論は，今日その重要性を次第に高めつつある．シャノン博士の洞察力は暗号においてもまた，他の追随を許さないものであったと言えよう．

ここに，シャノン博士の偉業に改めて深甚な敬意を表するとともに，謹んで哀悼の意を表するものである．

参考文献

[1] C.E. Shannon, "A mathematical theory of communications," Bell System Technical Journal, vol.27, pp.379-423, July, pp.623-656, Oct., 1948.

[2] G.D. Forney, Jr., Concatenated codes, MIT Press, 1966.

[3] J. Justesen,"Class of constructive asymptotically good algebraic codes, IEEE Trans. Info. Theory, vol. 18, pp. 652 - 656, Sep. 1972.

[4] P. Delsarte and P. Piret,"Algebraic constructions of Shannon codes for regular channels," IEEE Trans. Inform. Theory, vol.28, no.4, pp.593-599, July 1982.

[5] M. Steiner,"Constructive codes for arbitrary discrete memoryless channels," IEEE Trans. Inform. Theory, vol.40, no.3, pp.929-934, May 1994.

[6] T. Uyematsu and E. Okamoto,"A construction of codes with exponential error bounds on arbitrary discrete memoryless channel," IEEE Trans. Inform. Theory, vol. 43, no.3, May 1997.

[7] R. de Buda,"Some optimal codes have structure," IEEE J. Sel. Areas in Commun., vol.7, no.6, pp.893-899, Aug. 1989.

[8] R. Urbanke and B. Rimoldi," Lattice codes can achieve capacity on the AWGN channel," IEEE Trans. Inform. Theory, vol.44, no.1, pp.273-278, Jan. 1998."

[9] V. Tarokh and I. Blake,"Trellis complexity versus the coding gain of lattices," IEEE Trans. Inform. Theory, vol.42, no.6, pp.1976-1816, Nov. 1996.

[10] H. Imai and S. Hirakawa,"A new multilevel coding method using error-correcting codes," IEEE Trans. Inform. Theory., vol. 23, pp. 371 - 377, May 1977.

[11] U. Wachsmann, R. Fischer and J.B. Huber," Multilevel codes: theoretical concepts and practical design rules," IEEE Trans. Inform. Theory, vol. 43, no.2, pp. 1361 -1391, July 1999.

[12] G.D. Forney,Jr., M.D. Trott and S.-Y. Chung,"Sphere-bound-achieving coset codes and multilevel coset codes," IEEE Trans. Inform. Theory, vol. 46, no.3, pp.820-850, May 2000.

[13] R.G. Gallager,"Low-density parity-check codes," IEEE Trans. Inform. Theory, vol. 8, pp. 21 - 28, January 1962.

[14] D. Divsalar, H. Jin, R.J. McEliece,"Coding theorems for 'turbo-like' codes," in Proc. of 36th Allerton Conf., Monticello, IL, pp.201-210, Sept. 1998.

[15] H. Jin and R.J. McEliece,"RA codes achieve the AWGN capacity," in Proc. of Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, Lecture Notes in Computer Science, vol.1719, pp.1-9, Springer-Verlag, 1999

[16] M. Luby, M. Mitzenmacher, A. Shokrollahi, D.

Spielman, and V. Stemann," Practical loss-resilient codes," in Proc. 29th ACM Symposium on the Theory of Computing, pp.150-159, 1997.

[17] M.A. Shokrollahi," New sequences of linear time erasure codes approaching channel capacity," in Proc. of Applied Algebra, Algebraic Algorithms, and Error Correcting Codes, Lecture Notes in Computer Science, vol.1719, pp.65-76, Springer-Verlag, 1999.

[18] H. Jin, A. Khandekar and R.J. McEliece, "Irregular repeat-accumulate codes," in Proc. Of 2nd International Symposium on Turbo Codes & Related Topics, pp. 1-8, Brest, France, Sept. 2000.

[19] A. Barg and G. Zemor," Error exponents of expander codes," in Proc. Of International Symposium on Information Theory, pp.47, Washington, D.C., June 2001.

[20] C.E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol.28. pp.656-715 (1949)

[21] J. Daemen and V. Rijmen, "AES Proposal: Rijndael," Technical Document of AES Candidates, 1988. http://csrc.nist.gov/encryption/aes/

[22] C.E. Shannon, "Analogue of the Vernam system for continuous time series," Memorandum MM43-110-44, May 10, Bell Laboratories (1943)

[23] G. Hanaoka, J. Shikata, Y. Zheng and H. Imai, "Unconditionally secure digital signature schemes admitting transferability," Advances in Cryptology - ASIACRYPT2000, LNCS 1976, Springer-Verlag, pp.130-142, (2000-12)

[24] Y. Aumann, Y.Z. Ding and M.O. Rabin, "Everlasting security in the bounded storage model," IEEE Transactions on Information Theory, to be published.

シャノン理論が経て来た道

韓 太舜、小林 欣吾（電気通信大学）

シャノン理論の創始

シャノン博士が今年 2 月 84 歳をもってご逝去された。筆者達には、シャノン博士のこのご逝去は、「シャノン理論」が 1948 年に誕生し、それが半世紀をかけて幾多の盛衰をくぐり抜け現今の情報通信社会を根底で支える中核的理論体系として見事に成長をとげるまでの「学問的歴史の区切り」とだぶって見える。そこで、この「学問的歴史の区切り」をごく簡単に振り返えることによって、シャノン博士のご逝去に対する追悼の意としたい。

シャノン博士がベル研究所で仲間である通信技術者たちの仕事を注意深く観察する中で、「通信」の本質を「情報源」、「通信路」というモデルに凝縮し、そこに工学的営為としての「符号化」、「復号化」が組み込まれていることを認識したことがシャノン理論の学問としての出発点であったろう。

「情報源符号化」の立場からのシャノン博士の貢献は、我々が日常曖昧に用いている＜情報＞という単語から様々な意味の一切を捨て去り、“ 情報源 ”という数学的モデルに情報を生み出す本質を表現する機構を代表させ、それには「情報量」（エントロピー : entropy）という固有の量的な情報概念が附随していることを示し、この普遍的な概念が符号化（encoding）と復号化（decoding）という二つの基本操作を媒介にして、初めてその実体的内容を獲得するということを明らかにした点である。また、「通信路符号化」の立場からの貢献は、雑音など物理的な影響を被る伝送路を用いた、あまりに多様な＜通信＞の形態を、条件付き確率で定義された“ 通信路 ”という単純な数学モデルに置き換え、それには「通信路容量」という固有の量的な情報概念が附随していることを示し、この概念が符号化（encoding）と復号化（decoding）という二つの基本操作を媒介にして通信路の伝送性能という実体的内容を獲得するということを明らかにした点である。

以上のことが情報と通信の核心をとらえた、正に革命的な認識であったことは、その後のシャノン理論の展開を振り返ってみても歴然としている。シャノン博士の創始になるシャノン理論がその当時の人々にいかに大きな衝撃を与えたかは、Slepian による「シャノン理論はあらゆる分野で爆風と共に炸裂した爆弾であった」という文章から端的にうかがい知ることができるであろう。このような熱狂的雰囲気の中で、シャノン博士が最初の論文を発表した 2 年後の 1950 年には既に、シャノン理論に関する最初の国際会議“ London Symposium on Information Theory ”が開かれている。そこで発表された論文は、電子工学、計算機

科学、統計学、数学、物理学、哲学、言語学、音韻学、経済学、政策学、心理学、神経精神医学、神経生理学、解剖学、人類学、動物福祉学、意味論、組織論、などの広範囲の分野にわたっていた。ここには、今から考えてみると、「情報理論」とはおよそ無縁と思われる多数の分野が網羅されている。当時の人々の「熱狂」はそれほどすさまじかったのである。

シャノン理論の思想と苦難

シャノン博士自身は、上述のような「符号化と復号化」という基本的枠組を準備した上で、通信路に対する符号化と情報源に対する符号化に関する二つの基本定理を提示したが、その根底には、個々の出現系列（例えば、長さ n の二進列）が情報を担うのではなく、出現系列全体の集合の統計的性質（statistics of ensemble）が情報を担うという思想があった。シャノン理論はこのような思想に基づいて初めて成立し得たものではあったが、この点こそがその後ホットで過激な論争にさらされ続けてきた理論体系の核心部分なのである。情報は統計的性質によって規定されるというこの考え方は、理論の論理的体系を豊かにし深化させる一方、その反面ではそれが取り扱える対象を狭める制約にもなったからである。例えば、計算機が生み出す個々のデータ系列の背後に何らかの統計的構造を想定することは容易ではないであろう。それらはむしろ非確率的なデータ系列として個々に存在しているとみるべきものだからである。ところが、シャノン博士の符号化法は対象となる情報源や通信路が統計的性質をもち、しかもそれが既知であるという前提のもとで初めて成立していた。それでは、シャノン理論は通信システムや計算機科学の目標に対して何の貢献もなし得ないのではなかろうか、というような深刻な疑問が提起されたのである。

その上、「熱狂」からさめ夢破れたが故の心理的「反動」も大きかったのであろう、「シャノン理論は結局のところ大数の法則に過ぎないではないか」とか「シャノン理論は美しいけれども、何の役にも立たない“ dead field ”である」とまでいわれたのである。かくして、1950 年代に爆発的なブームに乗って一挙に完成に向かうかにみえたシャノン理論も、日本では 1960 年代に入って急速に停滞期に入る。

しかし欧米では、この時期にシャノン理論の諸概念に対する地道で徹底した反省と研究が蓄積され、1970 年代に入ると、衛星通信時代を先取りした多端子情報理論の参入などもあって、第 2 期の隆盛期を迎えていた。このころになってようやく、統計的性質が未知の情報源に対する符号化（すなわち、情報源の統計的性質を前提としない符号化）の研究が本格化し始め、1980 年代に入ってユニバーサル符号（universal code）として結実する。

一方、電子通信学会から情報理論の研究部会が一時消滅した日本では、関西地区を中心に情報理論の研究再興を期して有志が結集し、1978 年 11 月神戸六甲荘において第 1 回情報理論とその応用研究会のシンポジウムが開催された。この時点ですでに欧米に 15 年ほどは遅れていた勘定になろう。1985 年シャノン博士には、制御理論で有名なカルマン博士とともに第 1 回の京都賞が授与され、京都国際会館において講演が行なわれた。彼自身が産み落としたシャノン理論の研究からはすでに遠ざかって、ジャグリングロボット、マイクロマウス、チェスプレーロボットなど人工知能機械などに悠々と時間を注ぎ込んでいる好々爺であった。シャノン博士自身の述懐にあるように「金になるとか、世界のためになるとかは考えなかった。自分の興味を追い求めただけだ。役に立たないことに随分時間を使った」という心情は本当のところであろう。その後、我々のこの研究会は 1986 年には学会としての活動を拡大し、今日に至っている。初期の頃、シンポジウムでは夜のワークショップでしばしば、情報理論は役に立つのか、立たないのかという議論が遅くまで戦わされた。最近このような議論がなされない、あるいはなされる必要もないのは、役に立っていることの言い訳をする必要がないくらいに、理論的結果が実践に結びついていることを誰でも知っているからである。

しかし、一方でシャノン理論の体系の中には未解決の基本問題がいくつも残されていることを認識すべきであろう。これらは問題を誰にでも分かるかたちで述べることはさほど困難ではないが、ワイルズの解決したフェルマーの最終定理ほどではないにしてもすでに何十年も我々の前に立ちはだかっている。これらを解決したからといってなんの役に立つかなどという野暮なことはやめにしよう。こういう未解決問題をもち、それらを解いてみたいという知的好奇心を呼び起こすことにこそシャノン理論の健全さがあるのだ。「いま教えていただいた数学はどんなところに使えるのですか」と問うたユークリッドの生徒は放校となったが、我々はそこまで極端になれないまでも自分が面白いと感じたことにもっと従順であるべきではなかろうか。それにしても、実利だけに価値しか見出せない輩から公開、外部評価などと過剰な説明責任を負わされてくる時代をいかに生きるかをシャノン博士の死は問いかけているのかもしれない。

いまでこそ、論文はほとんどワープロで書かれ、PDF ファイルなどで美しい印刷物としてまとめられるが、1978

年神戸の原稿はすべて著者の癖字が反映された手書きであった。それから 10 年後神戸で開催された 1988 年 IEEE International Symposium on Information Theory までの 10 年間はこの学会メンバーの誰しも等しくハングリーであった。それから 13 年経つうちに情報化は急激に進展し、出版形態は著しく変貌した。情報理論研究者でもなにがしかのおこぼれに与れ、それとともに知に対するハングリー精神は欠如して、金に勘定できる部分へと興味を移して来ているのではないだろうか。そして、このような学問に対するある種の情熱を欠いた精神構造のまま 21 世紀に入り、日本で第 2 回目の IEEE ISIT 2003 Yokohamaが控えている。IT 革命と浮かれているとIT 不況となったが（ここで用いられている IT が Information Theory でなくて幸いであった）、これを弛んだ気持ちをハングリーに切り替えるいいチャンスととらえ、螺子を巻きなおす必要がありそうだ。

隣接諸分野との交流

1980 年代から 1990 年代にかけてのシャノン理論の顕著な特徴は、理論体系それ自身としての発展もさることながら、隣接する他分野、例えば、計算機科学、統計学、あるいは、通信技術、画像処理、システム理論、パターン認識、データ解析などの諸分野との密接な関連にあるといってよいであろう。特に、シャノン理論における成果の中でもとりわけ画期的なものとされている成果が、それらの諸分野からの刺激あるいは研究者の参入によって達成されたという事実や、また逆に、これらの成果が隣接諸分野に大きなインパクトを与えているという事実がもつ意味は重大である。

最後に

しかし、我々が決して忘れてならないのは、IT 革命などという幻影に惑わされて、現今の情報化社会が直面している諸問題をシャノン理論がすべて解決してくれるという妄想や狂想的な雰囲気の中に訳が分からないまま巻き込まれてしまってはならないという事である。この点に関しては、1956 年の段階ですでに、シャノン博士自身が、文学青年達までが文学に情報理論を適用したとする論文などをいくつも発表するなどという風潮を嘆いて、これらを “楽隊車効果 (Bandwagon effect)” とよんで次のように警告している。

· · · We should now turn our attention to the business of research and development at the highest scientific plane we can maintain. Research rather than exposition is the keynote, and our critical thresholds should be raised. Authors should submit only their best efforts, and these only after careful criticism by themselves and their colleagues. · · · Only by maintaining a thoroughly scientific attitude can we achieve real progress in communication theory and consolidate our present position.

SITA ニューズレター・ホームページＵＲＬの変更について

SITA ニューズレター 37 号から，閲覧用ホームページの URL が http://www.ogawa.nuee.nagoya-u.ac.jp/~yamazato/sitanl/ に変更となりました．ここでは，最新号および，22 号〜35 号のバックナンバーを掲載しております．以前の閲覧用ホームページの URL http://sita-nl.ics.nitech.ac.jp/ から変更になりましたので御注意下さい．

編 集 後 記

本年 2 月 24 日に Claude Elwood Shannon 博士がご逝去されました．博士の偉大なご功績を讃え，SITA ニューズレター特集号を企画するよう会員の皆様から，強いご要望が寄せられました．ここに，シャノン博士追悼特集号を発行でき，ご協力頂いた皆様方に感謝致します．SITA ニューズレターでは，引き続き，技術特集号の発行を予定しています．興味深い特集企画等がございましたら，編集担当までご連絡をお願い致します．

(岡)

編 集 担 当 者

岡 育生（編集理事）

〒 558-8585 大阪市住吉区杉本 3-3-138
大阪市立大学工学部情報工学科
Tel. 06-6605-2779
Fax. 06-6690-5382
Email oka@info.eng.osaka-cu.ac.jp

山里 敬也（編集幹事）

〒 464-8603 名古屋市千種区不老町
名古屋大学情報メディア教育センター
Tel. 052-789-2743
Fax. 052-789-3173
E-mail yamazato@nuee.nagoya-u.ac.jp

杉村 立夫（編集理事）

〒 380-8553 長野市若里 4-17-1
信州大学工学部電気電子工学科
Tel. 026-269-5237
Fax. 026-268-5220
Email tsugimu@gipwc.shinshu-u.ac.jp

野上 保之（編集幹事）

〒 700-8530 岡山市津島中 3-1-1
岡山大学工学部通信ネットワーク工学科
Tel. 086-251-8128
Fax. 086-251-8127
E-mail nogami@cne.okayama-u.ac.jp

情報理論とその応用学会事務局
〒 113-8656 東京都文京区本郷 7-3-1
東京大学工学部計数工学科
数理第 3 研究室内，山本博資　気付
Tel: 03-5841-6930（直通）
Fax: 03-5841-8605
E-mail: sita-ofice@hy.t.u-tokyo.ac.jp