1-1　基礎・境界の研究分野と基礎研究の実用化

Research Fields of Engineering Science Society and Practical Applications of Basic Research

植松友彦

1. 基礎・境界の歴史

100 周年を迎えた本会において，「基礎・境界」と呼ばれる専門分野の名称は，論文誌を会誌から分離発行したときに始まった．1968 年の論文誌の発行にあたり，専門領域を考慮して A，B，C の 3 分冊とし，その後 1972 年に D 分冊が追加され，基礎・境界（A），通信（B），エレクトロニクス（C），情報・システム（D）の 4 分野 4 分冊体制とした[(1)]．これに伴い，会誌の編集業務もまた 4 グループに対応した基礎・境界，通信，エレクトロニクス，情報・システムの四つの分野別に企画立案されるようになった[(1)]．しかし，この頃の「基礎・境界」とは論文誌や会誌の編集に用いられる分類名称に過ぎなかった．

「基礎・境界」という専門分野が実質的な研究活動の分類として利用されるようになったのは，1985 年の研究グループ制の発足によってである[(1)]．研究グループ制は，学会組織の巨大化並びに専門分野の専門化が進み，専門分野ごとに論文の構成や研究会の運営方法が異なってきたので，研究組織を幾つかの分野に分割するために導入された．研究グループ制の発足時，基礎・境界，通信，エレクトロニクス，情報・システムの 4 研究グループが作られ，研究グループ運営委員会が設置され，論文誌発行を含む研究活動がグループごとに行われるようになった[(1)]．この研究グループ制により，基礎・境界研究グループが誕生し，「基礎・境界」という分野が学会における研究活動の分野として意味を持つようになったのである．研究グループ制は，1995 年の学会のソサイエティ化に伴い，ソサイエティ制という最終形態になり，現在の基礎・境界ソサイエティに至っている．

一方，NOLTA ソサイエティは，基礎・境界ソサイエティの後述するサブソサイエティの一つとして 1999 年に発足した非線形理論とその応用サブソサイエティが，自ら論文誌を発行するまで発展し，2014 年から独立したソサイエティとなったものである．この経緯から，基礎・境界ソサイエティと NOLTA ソサイエティとは共同運営を行っている．なお，NOLTA ソサイエティの研究分野については，本特集の引原氏の記事を参照されたい．

本稿では，最初に基礎・境界ソサイエティに属する各研究会の研究分野を紹介する．次に，情報通信における技術を幾つか例に取り，基礎理論の提案から実用に至るまでの様々な歴史について述べる．

2. 基礎・境界の研究分野

基礎・境界ソサイエティ（Engineering Science Society，以下では ESS と略す）は，2017 年 2 月現在，19 の研究専門委員会（以下では研専と略す）と一つの時限研究専門委員会から構成されている．歴史的には，超音波研専が最も早く 1949 年に設立された．その次が 1955 年に設立した回路とシステム研専（設立当時は回路網理論研専）と応用音響研専（設立当時は電気音響理論研専）である．他のソサイエティにない ESS の特徴として，1995 年の学会のソサイエティ化以降，研究領域の近い複数の研専が集まり「サブソサイエティ」という研究コミュニティを形成したことが挙げられる．現在では，七つの研専が，三つのサブソサイエティ（システムと信号処理，音響・超音波，情報理論とその応用）を形成している（表 1）．

以下では，各サブソサイエティの特色を述べた後に各

植松友彦　正員：フェロー　東京工業大学工学院情報通信系
E-mail　uematsu@ict.e.titech.ac.jp
Tomohiko UYEMATSU, Fellow (School of Engineering, Tokyo Institute of Technology, Tokyo, 152-8550 Japan).
電子情報通信学会誌　Vol.100 No.6 pp.404-408 2017 年 6 月

表1　サブソサイエティと研究専門委員会

〈システムと信号処理サブソサイエティ〉
・回路とシステム研専
・信号処理研専
・VLSI 設計技術研専
・システム数理と応用研専

〈音響・超音波サブソサイエティ〉
・超音波研専
・応用音響研専

〈情報理論とその応用サブソサイエティ〉
・情報理論研専

・信頼性研専
・情報セキュリティ研専
・ワイドバンドシステム研専
・思考と言語研専
・技術と社会・倫理研専
・安全性研専
・ITS（高度交通システム）研専
・スマートインフォメディアシステム研専
・イメージ・メディア・クオリティ研専
・高信頼制御通信研専
・バイオメトリクス研専
・安全・安心な生活と ICT 研専
・ハードウェアセキュリティ時限研専

研専の対象とする研究分野を説明する．システムと信号処理サブソサイエティは，半世紀以上の歴史を持つ回路とシステム研専と，回路とシステム研専が母体となって設立した VLSI 設計技術研専，信号処理研専（設立当時はディジタル信号処理研専），並びにシステム数理と応用研専（設立当時はコンカレント工学研専）から構成されている．これらの研専の設立の経緯については，本特集の梶川氏の記事を参照されたい．システムと信号処理サブソサイエティの主要イベントには，30 年以上の歴史を持つ「回路とシステムワークショップ」と国際会議 ITC-CSCC（International Technical Conference on Circuits/Systems, Computers and Communications）がある．各研専の専門分野については，回路とシステム研専は回路理論及びシステム理論の基礎理論から具体的応用まで幅広い研究分野を対象にしている．VLSI 設計技術研専は，LSI の設計技術とその応用に関し，システムレベルからデバイスレベルに至るまでを対象にしている．信号処理研専は，基礎数理から音声，音響，画像，映像，無線，生体，センサなど各種信号の処理方法までを対象にしている．システム数理と応用研専は，離散事象システムやハイブリッドシステムなどの数理モデルを構築して，システム設計，機械学習などの解析，モデル検査などの検証，制御のための方法論などを対象にしている．このうち信号処理分野の研究の変遷については，梶川氏の記事を参照されたい．

音響・超音波サブソサイエティは，可聴域外の聞くことを目的としない音を対象にした超音波研専と，音の収録・伝送・再生を担う電気音響技術とその応用技術を対象とした応用音響研専から構成されている．両研究会共に，日本音響学会傘下の電気音響研究会並びに超音波研究会とも連携し活動している．なお，音響・超音波サブソサイエティの研究分野については，本特集の水町氏の記事を参照されたい．

情報理論とその応用サブソサイエティは，1978 年に本会の外部で発足した情報理論とその応用学会が 2010 年に本会に合併されたことに伴い，情報に関する基礎理論から応用理論まで幅広く対象にする情報理論研専が情報通信基礎サブソサイエティ（2016 年に廃止）から独立し，単独で設立したサブソサイエティである．このサブソサイエティの主要イベントは，情報理論とその応用学会が開催してきた 40 年近くの歴史を持つ「情報理論とその応用シンポジウム（SITA）」と隔年開催される International Symposium on Information Theory and its Applications（ISITA）である．情報理論とその応用サブソサイエティの研究分野については，本特集の鎌部氏の記事も参照されたい．

次に，サブソサイエティに属していない研専の研究分野について述べる．信頼性研専は 1960 年に設立され，信頼性・保全性理論，高信頼性設計，信頼性試験，故障解析，ソフトウェア信頼性などを対象にしている．

情報セキュリティ研専とワイドバンドシステム研専は共に情報理論研専が母体となって設立された研専である．情報セキュリティ研専は 1988 年に設立され，暗号などの理論的探求のみならず暗号の実装やシステムのセキュリティなどを広く対象にしており，研究会のほかに，600 名以上の参加者で行われる「暗号とセキュリティシンポジウム（SCIS）」並びに国際会議 IWSEC（International Workshop on Security）を毎年開催している．

ワイドバンドシステム研専は，1991 年にスペクトル拡散研専として設立され，情報理論や信号処理といった基礎学問に立脚する，スペクトル拡散通信，超広帯域無線通信（UWB），光無線通信，レーダ・センシングといった広帯域通信技術及びその応用を対象にしている．

思考と言語研専は 1994 年に設立され，人間の知能の根幹に深く関わる思考と言語の本質と人間による思考と言語の運用を探求し，教育・福祉への応用や工学的応用を目的としている．

技術と社会・倫理研究会は 1995 年に設立され（設立当時は情報通信倫理研専），情報通信や工学一般に関する倫理問題を中心として，情報リテラシー，知的財産権，情報セキュリティ等，情報化社会における種々の問題を対象にしている．

安全性研専は 1987 年に設立され（設立当時は第二種研究会），交通安全，労働安全，環境安全，医療安全，機械安全，製品安全，食品安全，薬品安全，災害問題など安全について横断的に対象にしている．

ITS 研専は，ITS 通信や ITS 画像処理といった要素技術から ITS と社会生活に関する総合的研究に至るまでの広範囲を対象にしており，スペクトル拡散研専（現：ワイドバンドシステム研専）が母体となり 1996 年に ITS 基盤技術研専（第三種研究会）として設立された．

スマートインフォメディア研専は 2004 年に設立され，広い分野において様々な要求に適用できる高度なシステムを，ハードウェア，ソフトウェアなどの技術を境界なく取り入れて，設計・開発・実現することを対象にしている．

2004 年に設立されたイメージ・メディア・クオリティ研専（設立当時は時限研専）は，イメージメディア固有の評価技術研究とその応用を対象にしている．

最近設立した研専としては，高信頼制御通信研専，バイオメトリクス研専，安全・安心な生活と ICT 研専，並びにハードウェアセキュリティ時限研専がある．2010 年に設立された高信頼制御通信研専（設立当時は時限研専）は，システム内あるいはシステム間における制御情報の高信頼な通信や無線制御を対象にして制御分野と通信分野の境界・融合領域として研究することを目的としている．

2012 年に設立されたバイオメトリクス研専（設立当時は時限研専）は，「人間と技術の様々なつながり」を対象にしている．

2009 年に設立された安全・安心な生活と ICT 研専（設立当時は第三種研究会）は，安全・安心な生活の実現に役立つことを目的とした情報通信技術や災害情報学や危機管理情報学などの社会科学分野の研究，並びに通信，電気，道路，鉄道網などの社会インフラ設備に関する保全・管理・運用技術などを対象にしている．

2016 年に設立されたハードウェアセキュリティ時限研専は，セキュリティ技術をハードウェア面から俯瞰し，ハードウェアセキュリティ分野を可視化することを目的にしている．

3. 情報通信分野における基礎研究の実用化

本章では，情報通信分野における基礎理論を用いて開発され，現在は身近で利用されている技術について幾つか取り上げ，基礎理論から実用化までの経緯について述べたい．

3.1 CDMA 方式

CDMA（Code Division Multiple Access）方式は，多元接続の一方式であり，直接拡散符号分割多元接続（DS/CDMA）と周波数ホッピング（FH）に大別される．CDMA 方式の歴史は古く，1940 年頃に生まれたスペクトル拡散通信の概念まで遡るが，スペクトル拡散通信が軍用通信として実用化されたのは 1980 年代に入ってからである．この頃までは，スペクトル拡散技術の利点として対干渉性や対傍受性に重点が置かれていた．

一方，スペクトル拡散技術による多元接続すなわち CDMA 方式によって多くのユーザが収容できるという点に着目し，米国の Qualcomm 社は CDMA 方式を利用した移動通信システムを 1993 年に発表し，後に米国の標準の一つ IS-95 となった．これが一般向け商品への CDMA 方式の利用の契機となり，1999 年には，第 3 世代移動通信システムの標準の一つとして W-CDMA や CDMA2000 などの CDMA 方式を用いたシステムが採用され，我が国でも CDMA 方式を用いた携帯電話が利用されるようになった．

携帯電話とほぼ時を同じくして，室内で多数のコンピュータをネットワークに接続する無線 LAN の方式においても CDMA 方式が有効であることが判明し，1997 年に CDMA 方式を利用した無線 LAN の規格である IEEE802.11 が標準化された．1999 年にアップルコンピュータ社から低価格の無線 LAN 装置が発売され，これに各社が追従することで，2000 年代に入ると IEEE802.11 無線 LAN が一般に普及した．これ以外に Bluetooth（1999 年）や ZigBee（2004 年）などの規格でも CDMA 方式が利用されている．

このように CDMA 方式は現在の無線通信システムでは欠かせない技術であるが，その概念は 70 年以上前まで遡り，実用の花開くまで 60 年を必要とした．基礎理論が実際のシステムに応用されるまでに最も長く掛かった例であると言えよう．

3.2 ハフマン符号と Lempel-Ziv 符号

データ圧縮で広く用いられているハフマン符号と Lempel-Ziv 符号（以下では LZ 符号と略す）は，その開発から実用化まで全く異なる経緯をたどる．次に，この二つの符号の実用化までの歴史を説明しよう．

ハフマン符号は，MIT の大学院生だった Huffman が，Fano による情報理論の授業の期末レポートの課題である平均符号長を最小にする符号化法について取り組んだときに発見した符号化アルゴリズムである．Fano は Huffman のアイデアを論文としてまとめることを勧め，1952 年に論文として発表されたのがハフマン符号である [2]．

過去から現在に至るまでハフマン符号は全世界のほぼ全ての情報理論の教科書で記述されているものの，データ伝送の分野では無視され続けた [2]．その最大の理由は，一定レートで生成された記号列が可変長のビット列に符号化されると記号に応じて復号時に読み込むビット数が異なり，一定レートで記号を出力するにはバッファメモリを用意する必要があるためである．そのため，ハフマン符号の最初の利用はコンピュータにおけるファイ

ルの圧縮であり，1985年から1986年にかけて出現したパーソナルコンピュータ用のファイルアーカイブシステムであるARK，PKARCやLHAに利用された[3],[4]．一方，ほぼ同じ頃UNIXでは，ファイルの圧縮コマンドであるcompactにFaller[5]とGallager[6]によって独立に発見され，Knuth[7]が改良した適応形ハフマン符号化が利用された．

1990年代になると，ネットワークと端末のディジタル化が進み，もはやハフマン符号化による可変レートは問題ではなくなった．この頃になって，画像圧縮方式の標準であるJPEG，ディジタルオーディオの代表的な圧縮方式であるMP3，並びに動画像圧縮方式の標準であるMPEG-2において量子化された値を圧縮する際にハフマン符号化が用いられ，1990年代以降のディジタルカメラや携帯形ディジタルオーディオプレーヤの普及に伴い，ハフマン符号は身近な技術として利用されるようになった．このようにハフマン符号はその誕生から利用まで，40年近く経たことになる．

一方，同じデータ圧縮符号でも発表から僅か10年間で利用されるようになったのがLZ符号である．LZ符号は，イスラエルのTechnionの研究者ZivとLempelによって1977年と1978年に開発された2種の可逆データ圧縮符号であり，発表年代に応じてLZ77符号[8]とLZ78符号[9]と呼ばれている．この2種の符号は，情報源すなわち圧縮する系列の統計的性質をあらかじめ知らなくても，系列長が長くなるにつれて理想的な限界に漸近する圧縮が可能である．すなわち，入力データが定常情報源からの出力列ならば，エントロピーレートで定まる限界までの圧縮が可能である．

LZ78符号の最初の利用は，当時のUNIXワークステーションのファイル圧縮ユーティリティとして1984年に出現したcompressであった．これは適応形ハフマン符号を用いた圧縮ユーティリティcompactの出現よりも早く，論文発表から僅か6年である．その後，2種類のLZ符号は共にファイルアーカイブシステムで最も基本的な圧縮アルゴリズムとして用いられ，前述したPKARC[3]のみならず，吉崎[4]が開発したLHA，現在でも広く用いられているZIP等でも利用され，ファイルの転送や保存等には欠かせない技術となっている．2種のLZ符号は共に特許出願されており，1990年代にイスラエルのTechnionの学部長が東工大を訪問したとき，Technionの誇る最高の特許がLZ符号であるという発言をされたのが印象的だった．

3.3 Reed-Solomon符号

Reed-Solomon符号（以下ではRS符号と略す）は，1960年にMITのLincoln研究所のReedとSolomonによって開発された[10]．しかし同様な符号が有本[11]によって1961年に独立に開発されていたことは余り知られておらず，欧米では僅かにBlahutによる符号理論の著書[12]にその記述があるだけである．

RS符号の効率的な復号法は，符号の発表から約10年後の1968年から1969年に掛けてBerlekamp[13]とMassey[14]によって開発され，現在ではBerlekamp-Masseyアルゴリズムと呼ばれている．一方，我が国では1975年に杉山ら[15]が拡張されたユークリッド互除法に基づく復号法を開発し，後にRS符号の復号用LSIを設計した際に利用された．しかしながら，RS符号が実際の通信に利用されるまでには，まだ年月が必要であった．

最初にRS符号が利用されたのは，1977年のNASAによるボイジャー計画であり，そこではRS符号で符号化した後，更に畳込み符号で符号化する二重符号化（連接符号化）が用いられ，これは後に，NASAの衛星探査器の標準符号化方式となった[16]．

一方，一般向け商品での最初の利用は，1980年の音楽用コンパクトディスク（CD）である．この規格はソニーとフィリップスとが共同で定め，二重誤りRS符号が利用された．1982年になって音楽用CDが生産され，各社からCDプレーヤが発売されるようになると，音楽用CDはその扱いやすさから急速に普及し，音楽メディア販売の中心はレコードから音楽用CDに変化して，1990年代になるとレコードは駆逐された．1980年代半ばには，音楽のみならずソフトウェア製品などの配布手段として，コンピュータやゲーム機で利用できるCD-ROMが標準化され，こちらにもRS符号が利用された．

1990年代に入ると，ディジタル記録やディジタル通信においてRS符号が標準的に用いられるようになり，衛星ディジタル放送の規格DVB-S（1993年）とISDB-S（1998年），並びに地上波ディジタル放送の規格ISDB-T（2001年）には再びRS符号と畳込み符号との二重符号化が利用された．また，記録メディアとしては，ディジタルバーサイルディスク（1996年）とブルーレイディスク（2002年）の規格にRS符号が利用された．更には，1994年に開発された二次元バーコードと言われるQRコードの誤り訂正にもRS符号が用いられている．しかしながら，RS符号も開発から半世紀以上たった今では，より現代的な符号である低密度パリティ検査符号にその座を譲りつつある．

3.4 RSA暗号

RSA暗号[17]は，1978年にMITの研究者だったRevest，ShamirとAdlemanの3人が開発した公開鍵暗号の一つである．RSA暗号はその安全性を多桁の素因数分解の困難性に根拠を置いている．RSA暗号は1990年代のインターネットの普及によって，発表から僅か10数年で急速に実用化されたものである．

RSA暗号の最初の利用は，1991年に電子メールの暗

号化ソフトウェアとして登場したPGP（Pretty Good Privacy）である[18]．ただし，この時代にはまだRSA暗号は特許によって保護されており，PGPにおける特許の問題を決着するには数年を費やしている．1994年になると，RSA暗号の電子商取引への利用として，ブラウザの先駆けであるNetscape Navigatorに実装されたWebサーバとクライアントの間でセキュアな通信を行うプロトコルであるSSL（Secure Socket Layer）が出現した．SSLは現在でもまだ利用されており，Webアプリケーションでは欠かすことのできない技術であり，インターネット利用者でSSLの恩恵を受けていない人はいないであろう．

このように情報通信の分野での基礎研究の社会貢献を見ていくと，新しい時代の研究や発明ほど短期間で実用化されていることが分かる．これが情報通信の分野に特有なことなのか，それとも基礎・境界分野の他の研究分野にも成り立つことなのか，そのような観点からも本企画を読んで頂ければ幸いである．

文　　献

（1） 電子情報通信学会75年史，電子情報通信学会(編)，電子情報通信学会，1992.

（2） D.A. Huffman, “A method for the construction of minimum-redundancy codes,” Proc. IRE, vol. 40, no. 9, pp. 1098-1101, Sept. 1952.

（3） D.A. Lelewer and D.S. Hirschberg, “Data compression,” ACM Comput. Surv., vol. 19, no. 3, pp. 261-296, March 1987.

（4） 吉崎栄泰，“圧縮ユーティリティ新LHの全貌，” C Magazine, vol. 3 no. 1, pp. 59-68, 1991.

（5） N. Faller, “An adaptive system for data compression,” Record of 7th Asilomar Conf. on Circuits, Systems and Computers, pp. 593-597, 1973.

（6） R.G. Gallager, “Variations on a theme by Huffman,” IEEE Trans. Inf. Theory, vol. 24, no. 6, pp. 668-674, Nov. 1978.

（7） D.E. Knuth, “Dynamic Huffman coding,” J. Algorithms, vol. 6, no. 2, pp. 163-180, June 1985.

（8） J. Ziv and A. Lempel, “A universal algorithm for sequential data compression,” IEEE Trans. Inf. Theory, vol. 23, no. 3, pp. 337-343, May 1977.

（9） J. Ziv and A. Lempel, “Compression of individual sequences via variable-rate coding,” IEEE Trans. Inf. Theory, vol. 24, no. 5, pp. 530-536, Sept. 1978.

（10） I.S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” SIAM J. Appl. Math., vol. 8, no. 2, pp. 300-304, 1960.

（11） 有本　卓，“p元群符号系の符号化，復号法と誤りの訂正機構，” 情報処理，vol. 2, no. 6, pp. 320-325, 1961.

（12） R.E. Blahut, Algebraic Codes for Data Transmission, Cambridge Univ. Press, Cambridge, 2003.

（13） E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

（14） J.L. Massey, “Shift-register synthesis and BCH decoding,” IEEE Trans. Inf. Theory, vol. IT-15, no. 1, pp. 122-127, 1969.

（15） Y. Sugiyama, M. Kasahara, S. Hirasawa, and T. Namekawa, “A method for solving key equation for decoding Goppa codes,” Inf. Control, vol. 27, no. 1, pp. 87-99, 1975.

（16） R.J. McEliece and L. Swanson, “Reed-Solomon codes and the exploration of the solar system,” in Reed-Solomon codes and their applications, S.B, Wicker and V.K. Bhargava, eds., IEEE Press, New York, 1994.

（17） R.L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signature and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120-126, 1978.

（18） S. Garfinkel, “PGP : Pretty Good Privacy,” O’ Reilly, 1995.

（平成29年1月16日受付　平成29年2月14日最終受付）

植松　友彦（うえまつ　ともひこ）（正員：フェロー）

昭57東工大・工・電気電子卒．昭59同大学院修士課程了．同年同大学助手．以来，情報理論，特にシャノン理論の研究に従事．現在，同工学院情報通信系教授．工博．本会論文賞（7回），平19年度本会業績賞，平25年度本会喜安善市賞各受賞．著書「イラストで学ぶ情報理論の考え方」，訳書「通信の数学的理論」など．