平成 27 年度

第 53 回 業績賞贈呈

（写真：敬称略）

本会選奨規程第 9 条イ号（電子工学及び情報通信に関する新しい発明，理論，実験，手法などの基礎的研究で，その成果の学問分野への貢献が明確であるもの），ロ号（電子工学及び情報通信に関する新しい機器，または方式の開発，改良，国際標準化で，その効果が顕著であり，近年その業績が明確になったもの）による業績に対し，下記の 6 件を選び贈呈した．

暗号プロトコル・要素技術に関する先導的研究

受賞者　**阿部正幸**

この高度情報化社会において，安心安全な情報システムを構成するためのセキュリティ技術は，最も重要な技術の一つといえる．その中で，ディジタル署名や公開鍵暗号などの暗号要素技術や，暗号匿名通信路のような暗号プロトコルは，必要不可欠な基盤技術であり，受賞者は，先駆的な研究によりこの分野を開拓してきた．

1990 年代後半には，効率性，機能性及び安全性を追求した暗号要素技術を創出しており，例えば，部分ブラインド署名方式の提唱[(1),(2)]が挙げられる．署名対象の文書を署名者に対して完全に秘匿したまま署名を発行させるブラインド署名の技術は，例えば電子チケットが固有番号など追跡可能な情報を含まないよう保証することでユーザのプライバシーを守る技術である．一方，プライバシーを侵害しない範囲で有効期限などの有用な共通情報を偽造不可能な形で含ませることが困難であったため，複数の署名鍵を用意する必要があるなど複雑な運用が実用化の障害となっていた．受賞者は，これを実現する方法とその安全性に関する基礎理論を初めて提唱し，ブラインド署名の商用利用に向け大きく前進させた．現在ではブラインド署名が備えるべき標準的な性質として ISO/IEC 18370 Part 2 で標準化が進められている．

2000 年前後には，インターネットなど盗聴可能なネットワーク上で複数のサーバが協力して仮想的に匿名通信路を実現する Mix-net に関して，置換回路を用いることで効率的かつ処理の正当性検証が可能な暗号文の順序入換を行う斬新な構成法を提唱した[(3),(4)]（図 1）．この先駆的な成果はその後多数の研究で改良の対象として注目され，この Mix-net を用いた電子投票方式は，安全かつ実用的な匿名電子投票方式として知られ，実装・実用化が進められている．

2000 年頃から 2010 年にかけては，ディジタル署名・公開鍵暗号・ゼロ知識証明など，情報システム構築の基盤技術である暗号プリミティブに関して多数の成果を創出している[(5)〜(10)]．例えば 2005〜2006 年に提唱した「Tag-KEM/DEM 公開鍵暗号方式」[(8),(9)]は高速な秘密鍵暗号と鍵管理の容易な公開鍵暗号の組合せから成る，いわゆるハイブリッド暗号の安全な構成法である．この構成による方式は，あらかじめ分散された秘密鍵を持つ複数の復号者が協力した場合のみ復号できるという分散復号機能を安全に実現できるため，単一鍵の管理がぜい弱点とならない頑健なシステム構築が可能となる基盤技術である．

また，1999 年に提唱した「メッセージリカバリ型署名方式」[(6),(7)]は，電子切手のように小さなデータを効率的に認証するための署名方式であり，理想化したハッシュ関数を用いて初めて理論的に安全な方式を構成した．ISO/IEC 9796 Part 3 で標準化されたこの方式は，現在でも理論的安全性の保証された数少ない方式の一つである．

このように，受賞者は暗号を中心としたセキュリティ分野の中で新たな魅力ある研究対象を発明し，研究分野の活発化と発展に貢献した．受賞者の業績は技術的に高く評価されており，暗号分野をけん引する世界暗号学会

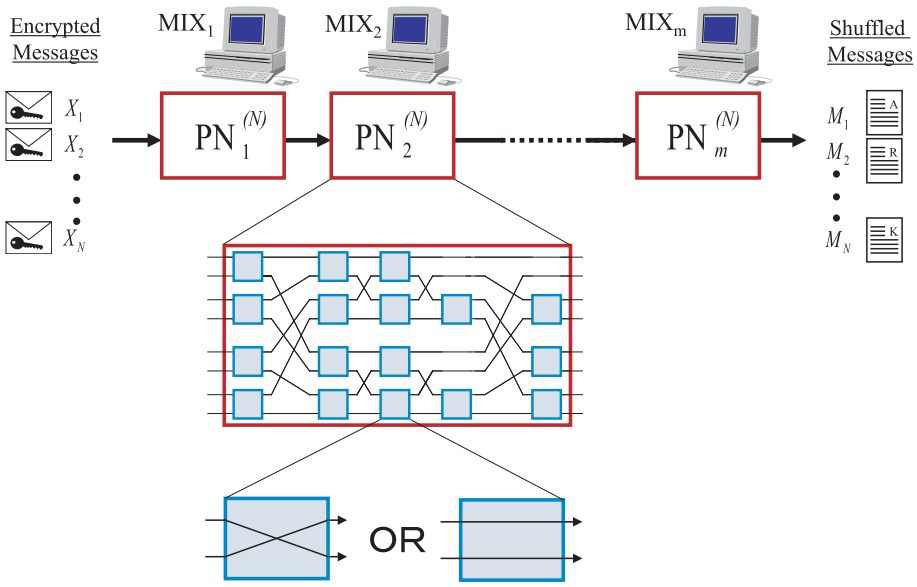

図 1　置換網を用いた MIX-NET の概念

（IACR）においてアジア圏で唯一の理事に選出されているなど，暗号・情報セキュリティ分野における日本とアジアのプレゼンス向上に尽力し，日本の暗号技術の発展に貢献した．これらの業績は極めて顕著であり，本会業績賞にふさわしいものである．

文　　献

（1） M. Abe and E. Fujisaki, “How to date blind signatures,” ASIACRYPT '96, Lect. Notes. Comput. Sci., vol. 1163, pp. 244-251, Springer, 1996.

（2） M. Abe and T. Okamoto, “Provably secure partially blind signatures,” CRYPTO 2000, Lect. Notes. Comput. Sci., vol. 1880, pp. 271-286, Springer, 2000.

（3） M. Abe, “Mix-networks on permutation networks,” ASIACRYPT 1999, Lect. Notes. Comput. Sci., vol. 1716, pp. 258-273, Springer-Verlag, 1999.

（4） M. Abe and F. Hoshino, “Remarks on mix-network based on permutation networks,” PKC 2001, Lect. Notes. Comput. Sci., vol. 1992, pp. 317-324, Springer, 2001.

（5） M. Abe, M. Ohkubo, and K. Suzuki, “1-out-of-n signatures from a variety of keys,” IEICE Trans. Fundamentals, vol. E87-A, no. 1, pp. 131-140, Jan. 2004.

（6） M. Abe, T. Okamoto, and K. Suzuki, “Message recovery signature schemes from sigma-protocols,” IEICE Trans. Fundamentals, vol. E96-A, no. 1, pp. 92-100, Jan. 2013.

（7） M. Abe and T. Okamoto, “A signature scheme with message recovery as secure as discrete logarithm,” ASIACRYPT 1999, pp. 378-389, 1999.

（8） M. Abe, R. Gennaro, and K. Kurosawa, “Tag-KEM/DEM : A new framework for hybrid encryption,” J. Cryptol., vol. 21, no. 1, pp. 97-130, 2008.

（9） M. Abe, Y. Cui, H. Imai, and K. Kurosawa, “Tag-KEM from set partial domain one-way permutations,” IEICE Trans. Fundamentals, vol. E92-A, no. 1, pp. 42-52, Jan. 2009.

（10） M. Abe and S. Fehr, “Perfect NIZK with adaptive soundness,” TCC 2007, Lect. Notes. Comput. Sci., vol. 4392, pp. 118-136, Springer, 2007.

精度保証付き数値計算学の先駆的研究

受賞者　**大石進一**

情報通信技術の飛躍的な発展に伴い，社会の様々な分野でコンピュータが利用されている．こうしたコンピュータの内部で数値計算に用いられる「数」は浮動小数点数であり，現在では IEEE 754 の規格が用いられている（1985 年制定，2008 年改定）．浮動小数点数で表現できる数の有効桁数は有限であるため，演算ごとに誤差が生じる．このため，演算回数が増えるにつれ，丸め誤差が大きくなる．科学技術計算においては大規模な問題が頻出し，それに伴って膨大な回数の演算が必要となるため，計算結果が出たとしても何桁目まで正しいか分からない．このようなとき，精度保証付数値計算が有用である．更に，数学上の未解決問題を解くためには，膨大な計算が必要となると同時に，その精度保証が必要不可欠となる場合がある．例えば，ヒルベルトの第 18 問題の一つである「立方体に球を充塡する際に，どのような方法が最も多く球を充塡できるか」という問題に対するケプラー予想は，300 年以上証明が付けられていなかったが，精度保証付数値計算により解決した．このように，精度保証付数値計算は，科学技術の発展とともに理工学の様々な分野でその必要性が急速に高まっている．

受賞者は，精度保証付数値計算の基盤分野から応用分野まで幅広く研究に従事してきたが，特に，線形方程式について，必要な桁まで正しい解を高速に計算する手法を確立し，精度保証付数値計算を一気に実用化した．従来，数値計算の誤差を把握するのは非常に難しい問題であった．それに対し，区間演算と呼ばれる精度保証法が存在したが，原理的に大規模問題へ適用できないことや，ばく大な計算時間（近似計算の数百から数千倍）を必要とするため，実用的ではなかった．また，計算誤差に弱い悪条件な問題については，正しい解を得るのが困難であった．

このような状況において，受賞者は，第 1 に，比較的良条件な問題については，精度保証に要する計算時間が近似解を計算する時間とほぼ同等という非常に高速な手法を開発した．第 2 に，悪条件な問題については，浮動小数点演算のエラーフリー変換法を導入することにより，問題の難しさに応じて必要最小限に近い計算時間で精度保証された高精度な解を効率的に計算する方法を開発した．

数値計算の基礎は，解くべき問題を線形方程式に帰着することであるため，本研究の成果によって精度保証付数値計算が一気に実用化した．実際，受賞者の成果により 100 万次元以上の大規模な連立一次方程式の数値解も精度保証可能となっている．本研究成果が随所に取り入れられているソフトウェアである「INTLAB」（共同研究者の S.M. Rump 教授が開発）は，50 か国以上に数千のユーザが存在し，精度保証付数値計算研究者の多くがこのソフトウェアを利用している．

以上のように，受賞者は，数値計算学の分野において，数学的に正しい結果を得ることは現実的には非常に困難であると思われていた常識を打ち破り，近似計算とほぼ同じ手間で，方程式の解の存在を証明しかつ正しい桁まで保証する精度保証付数値計算学を確立した．これ

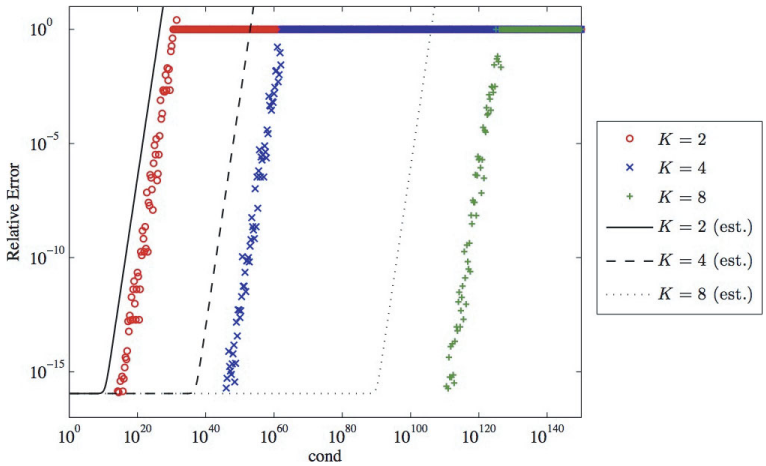

図 1　エラーフリー変換を用いた高精度内積計算の誤差評価
ベクトル化エラーフリー変換による任意高精度化．

らの成果は，紫綬褒章（2012），文部科学大臣表彰科学技術賞（2010），本会フェロー（2006）など，高く評価されており，その業績は極めて顕著であり，本会業績賞にふさわしいものである．

文　　献

（1） A. Takayasu, X. Liu, and S. Oishi, “Remarks on computable a priori error estimates for finite element solutions of elliptic problems,” NOLTA, vol. 5, no. 1, pp. 53-63, Jan. 2014.
（2） N. Yamanaka and S. Oishi, “Fast quadruple-double floating point format,” NOLTA, vol. 5, no. 1, pp. 15-34, Jan. 2014.
（3） X. Liu and S. Oishi, “Verified eigenvalue evaluation for Laplacian over polygonal domain of arbitrary shape,” SIAM J. Numer. Anal., vol. 51, no. 3, pp. 1634-1654, May 2013.
（4） K. Ozaki, T. Ogita, and S. Oishi, “Tight and efficient enclosure of matrix multiplication by using optimized BLAS,” Numer. Linear Algebr. Appl., vol. 18, no. 2, pp. 237-248, Feb. 2011.
（5） S. Oishi, T. Ogita, and S.M. Rump, “Iterative refinement for ill-conditioned linear systems,” Japan J. Indust. Appl. Math., vol. 26, no. 2-3, pp. 465-476, Oct. 2009.
（6） S.M. Rump, T. Ogita, and S. Oishi, “Accurate floating-point summation part I : Faithful rounding,” SIAM J. Sci. Comput., vol. 31, no. 1, pp. 189-224, Oct. 2008.
（7） T. Ogita, S.M. Rump, and S. Oishi, “Accurate sum and dot product,” SIAM J. Sci. Comput., vol. 26, no. 6, pp. 1955-1988, July 2005.
（8） S. Oishi and S.M. Rump, “Fast verification of solutions of matrix equations,” Numer. Math., vol. 90, no. 4, pp. 755-773, Feb. 2002.
（9） S. Oishi, “Numerical verification of existence and inclusion of solutions for nonlinear operator equations,” J. Comput. Appl. Math., vol. 60, no. 1-2, pp. 171-185, June 1995.
（10） S. Oishi, “Two topics in nonlinear system analysis through fixed point theorems,” IEICE Trans. Fundamentals, vol. E77-A, no. 7, pp. 1144-1153, July 1994.

統計的機械学習に関する先導的研究

受賞者　**上田修功**

多層ニューラルネットワークの流行が終わろうとしていた 1990 年頃，現在の機械学習の起源と言える数理統計学を土台とする統計的機械学習研究がれい明期にあった．受賞者は，正にこの頃から当該分野の基礎研究に着手し，これまでに，統計的機械学習の基礎研究と実応用に関し，重要かつ先駆的な業績を複数挙げ，当該分野の学術発展に大きく貢献した．

具体的には，音声，画像等のひずみを許す情報圧縮の重要技術であるベクトル量子化の品質向上に取り組み，最適解が満たすべき必要条件（等ひずみ原理）を理論的に導出し，更に，原理の導出にとどまらず，その設計原理を近似的に実現するオンライン学習アルゴリズムを考案した．新理論に基づく近似アルゴリズムはこれまで未解決であったベクトル量子化器の大域的最適化に大きく貢献した．本成果は現在のオンラインクラスタリングの先駆的研究と位置付けられ，1997 年に電気通信普及財団賞テレコムシステム技術賞が授与されている．

次いで，1990 年代後半に統計的機械学習の学習法として広く用いられていた EM アルゴリズムの当時未解決であった局所最適性の問題に対し，統計力学の考え方を応用した斬新な解法，DAEM 法や混合モデルを対象とした SMEM 法を考案した．これらは広範囲にわたるパラメータ推定の解品質向上に大きく貢献するもので，数理統計の著名な専門書に掲載されるなど国際的に高い評価を得ており，2000 年に本会論文賞を受賞している．

更に受賞者は 2000 年初頭において，Web 上のテキストデータのように，一つの文書が複数のクラス（トピック）から成る場合での多重分類問題に対し，世界初の多重トピックテキストモデルを考案すると同時に，実際の Web 数万ページを用いその有用性を実証した．本技術は，ニュース記事分類サービスに実用化されている．その後，多重分類問題の国際ワークショップが開催され，受賞者はその先駆者として運営委員を務めている．

また，受賞者はベイズモデルの近似計算法である変分ベイズ法や，加算無限個の統計モデルを取り扱うノンパラメトリックベイズ理論といった最先端ベイズ理論研究に国内でいち早く着手し，国内での当該分野の研究を活性化させ，NTT の音声認識研究者との共同により，変分ベイズ理論を用いた隠れマルコフモデルの世界初のモデル構造自動学習法を確立し，2004 年に本会論文賞，2006 年に電気通信普及財団賞テレコムシステム技術賞を受賞している．

更に，近年，受賞者は，最先端研究開発支援プログラム（FIRST）（代表：喜連川　優）において機械学習のサブテーマリーダを務めると同時に，加速度センサからの看護師行動自動認識技術を考案し，従来技術の認識性能を著しく改善することに成功した．次いで，本技術を用いて，FIRST において医療分野の研究者と共同で心臓疾患病棟において蓄積されていた実看護師行動履歴約 900 万行動を分析し，看護師行動種とその所要時間と患者の重症度との関係などの有益な統計をまとめるという

世界初の分析を行い，ICT による保健医療分野でのビッグデータ分析の画期的な道をひらいた．

このように，受賞者は日本における統計的機械学習研究分野の発展に大きく貢献し，これらの業績は技術的にも高く評価され，本会からフェローの称号も授与されている．また，受賞者は，情報論的学習理論と機械学習研究専門委員会の委員長を歴任し，当該分野の組織運営にも貢献し，本会情報・システムソサイエティ活動功労賞も受賞している．これらの業績は極めて顕著であり，本会業績賞にふさわしいものである．

文　　献

（1） N. Ueda and R. Nakano, “A new competitive learning approach based on an equidistortion principle for designing optimal vector quantizers,” Neural Netw., vol. 7, no. 8, pp. 1211-1227, 1994.

（2） N. Ueda and R. Nakano, “Deterministic annealing variant of the EM algorithm,” Neural Information Processing Systems 7（NIPS7）, pp. 545-552, MIT Press, Cambridge, 1995.

（3） N. Ueda, R. Nakano, Z. Ghahramani, and G.E. Hinton, “SMEM algorithm for mixture models,” Neural Comput., vol. 12, no. 9, pp. 2109-2128, 2000.

（4） N. Ueda and K. Saito, “Parametric mixture models for multi-topic text,” Neural Information Processing Systems 15（NIPS15）, pp. 737-744, MIT Press, Cambridge, 2002.

（5） N. Ueda and K. Saito, “Singleshot detection of multi-category text using parametric mixture models,” ACM SIG Knowledge Discovery and Data Mining, SIG KDD, pp. 626-631, 2002.

（6） N. Ueda and Z. Ghahramani, “Bayesian model search for mixture models based on optimizing variational bounds,” Neural Netw., vol. 15, no. 10, pp. 1223-1241, 2002.

（7） S. Watanabe, Y. Minami, A. Nakamura, and N. Ueda, “Variational Bayesian estimation and clustering for speech recognition,” IEEE Trans. Speech Audio Process., vol. 12, no. 4, pp. 365-381, 2004.

（8） N. Ueda, Y. Tanaka, and A. Fujino, “Robust naive Bayes combination of multiple classifications,” The Impact of Applications on Mathematics, Proceedings of the Forum of Mathematics for Industry, pp. 141-156, Springer, 2014.

（9） S. Inoue, N. Ueda, Y. Nohara, and N. Nakashima, “Movile activity recognition for a whole day : recognizing real nursing activities with big dataset,” Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing（UbiComp2015）, pp. 1269-1280, 2015.

（10） Y. Nohara, E. Kai, P. Ghosh, R. Islam, A. Ahmed, M. Kuroda, S. Inoue, T. Hiramatsu, M. Kimura, S. Shimizu, K. Kobayashi, Y. Baba, H. Kashima, K. Tsuda, M. Sugiyama, M. Blondel, N. Ueda, M. Kitsuregawa, and N. Nakashima, “Health checkup and telemedical intervention program for preventive medicine in developing countries,” J. Med. Internet Res., vol. 17, no. 1 Jan. 2015.

LTE-Advanced を実現する高度化 C-RAN の実用化

受賞者　前原昭宏

受賞者　安部田貞行

受賞者　徳弘徳人

2008 年以降，スマートフォンの普及に合わせた，ソーシャルネットワーク，ビデオストリーミングに代表される新たなモバイルアプリケーションの利用拡大が続いている．これにより，近年のモバイルデータトラヒックは毎年約 1.5 倍の割合で急増しており，その対策は移動通信事業者にとって共通の課題である．2010 年頃から導入が開始された LTE は，従来の 3G システムよりも高速・大容量のシステムであり，急増するトラヒックに対応するために有用なシステムである．しかし，増大を続けるトラヒックに対応するには，新規周波数の追加や，セル半径を小さくする（スモールセル）対応を併せて行い，単位面積当りに収容可能な無線容量を増やしていく更なる対策が必要であった．

受賞者らは上記課題を解決し，効果的な無線ネットワークを構築する方法として，LTE の発展形である LTE-Advanced の標準技術を用いつつ，集約化を行うことで低コスト化とセル間の密な連携を可能とする C-RAN（Centralized Radio Access Network）の特徴を生かした新たな無線アクセスネットワークアーキテクチャ（高度化 C-RAN）を考案した．本アーキテクチャは，図 1 に示すように，マクロセルとスモールセルが混在するヘテロジニアスネットワークにおいて，複数のスモールセルとマクロセルに割り当てられた任意の周波数を同時に利用する LTE-Advanced のキャリヤアグリゲーション（CA）技術を用いる．これにより，通信が混雑する高トラヒックエリアに柔軟かつ効果的に無線容量を増加できるスモールセルを展開しつつ，マクロセルと連携して移動中の端末の通信品質を安定的に確保すること

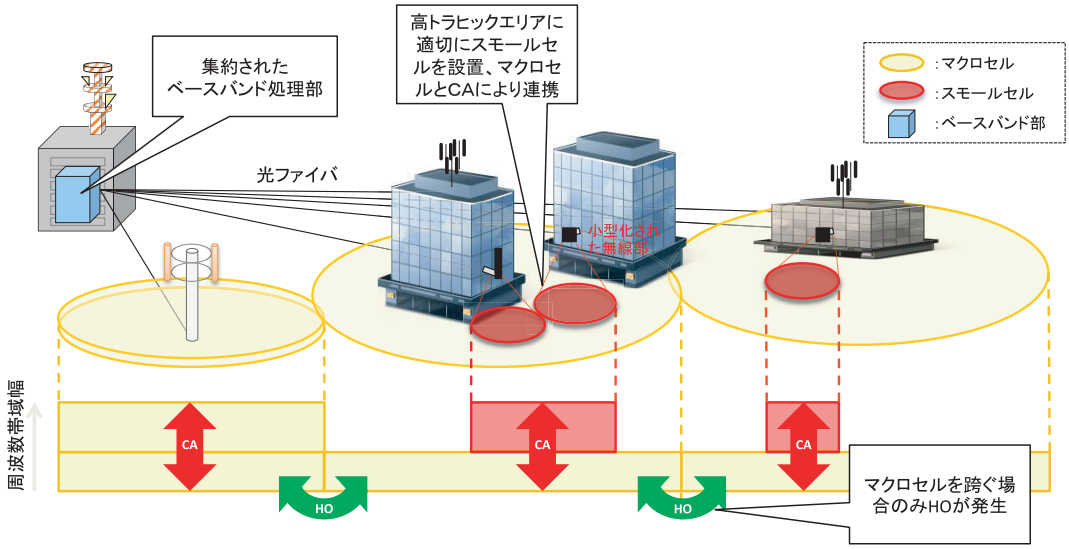

図1　高度化 C-RAN アーキテクチャ

で，高速・大容量・高品質な通信を容易に実現することが可能となった．

また，受賞者らは LTE-Advanced の標準化を行っている 3GPP において多数の技術提案寄書を入力するなどして標準化活動をリードし，CA の仕様作成等に貢献するとともに，マクロセルとスモールセル間の CA の性能評価を国内外の学会の招へい講演や学術論文で発表し，研究の方向性や新たな課題を提言しつつ，本技術の基本的なアイデアを開示するなど，移動通信技術の発展にも大きく寄与した．

更に受賞者らは，本技術の実用化のための開発をけん引し，国内最速である 225 Mbit/s（一部で 262.5 Mbit/s）の高速伝送を実現する LTE-Advanced サービスの提供（2015 年 3 月）を実現した．導入から約 6 か月（9 月末現在）で全国主要 640 都市・7,700 局への展開が進み，LTE-Advanced 対応端末の稼動台数は 100 万台を超えて急速に普及しており，モバイルネットワークを用いたリッチコンテンツの利用促進などの新たな市場の拡大への波及効果も期待されている．

また，高度化 C-RAN は 5G に向けた今後の移動通信方式発展のベースになる非常に有益なアーキテクチャであり，これを世界に先駆けて実用化したことによる移動通信業界への貢献は非常に大きい．

以上のとおり，受賞者らの功績は極めて顕著であり，本会業績賞にふさわしいものである．

文　　献

（1） 安部田貞行，新　博行，“超高速ブロードバンドサービスを実現する無線アクセスネットワーク，”2012 信学総大，no. BD-2-5, March 2012.

（2） 新　博行，安部田貞行，“LTE-Advanced 開発に向けた取り組み，”2013 信学ソ大，no. BT-4-2, Sept. 2013.

（3） T. Takiguchi, K. Kiyoshima, Y. Sagae, K. Yagyu, H. Atarashi, and S. Abeta, “Performance evaluation of LTE-Advanced heterogeneous network deployment using carrier aggregation between macro and small cells,” IEICE Trans. Commun., vol. E96-B, no. 6, pp. 1297-1305, June 2013.

（4） 安部田貞行，河原敏朗，二方敏之，“さらなる LTE の進化，スマートライフをサポートする LTE-Advanced の開発，”NTT DOCOMO テクニカルジャーナル，vol. 23, no. 2, pp. 6-10, July 2015.

（5） 清嶋耕平，瀧口貴啓，河辺泰宏，佐々木優輔，“高度化 C-RAN アーキテクチャを活用した LTE-Advanced 商用開発―アドオンセルによる容量拡大と高度なセル間連携による安定した通信の実現―，”NTT DOCOMO テクニカルジャーナル，vol. 23, no. 2, pp. 11-18, July 2015.

（6） 吉原龍彦，戸枝輝朗，藤井昌宏，諏訪真悟，山田武史，“高度化 C-RAN アーキテクチャを実現する無線装置およびアンテナの開発，”NTT DOCOMO テクニカルジャーナル，vol. 23, no. 2, pp. 19-24, July 2015.

超高速暗号 KCipher-2 の開発と標準化

受賞者　田中俊昭

受賞者　清本晋作

受賞者　櫻井幸一

暗号は現代社会になくてはならない基盤技術となっている．受賞者らは，高い安全性を確保しつつ，現在，標準的な暗号方式として広く利用されている AES よりも一桁速い暗号アルゴリズムの実現を目指す研究開発を実施し，暗号アルゴリズム KCipher-2[(1)] を完成させた．この目標は，10 年先の技術を想定したとしても十分競争力のある方式とするという考えと，当時の携帯端末では，暗号化処理は非常にコストが掛かり，マルチメディアコンテンツなど大容量データの暗号化は従来の暗号アルゴリズムでは困難であったというニーズから導き出されたものである．現在では，よりリソースの制限が厳しい IoT デバイスにおいても普及が進んでいる．KCipher-2（図 1）は，高速ソフトウェア実装に適した Dynamic Feedback Shift Register（DFSR）という新しい基本コンポーネントを考案し安全性の理論的評価を行うことにより，速度低下を抑えつつ，安全性の大幅な向上を実現した．AES と比較すると 5〜10 倍高速であり（図 2）[(2)]，かつ排他的論理和，算術加算，テーブル参照等の汎用的なコンピュータに具備されている基本演算のみから構成されるため，あらゆる環境に適用可能である．CRYPTREC（Cryptography Research and Evaluation Committees）等の第三者評価により，十分な安全性を有することが確認されている．受賞者らは，開発した KCipher-2 の標準化活動にも積極的に取り組み，国際標準規格 ISO/IEC18033-4[(3)] において標準化された．また，CRYPTREC での評価を経て，ストリーム暗号カテゴリーの電子政府推奨暗号として唯一採用されている[(4)]．更に，インターネットプロトコルの標準化を行っている IETF においても RFC（Request for Comments）7008[(5)] を発行している．一方，スマートフォン向けセキュリティライブラリ（Android 端末，iPhone 端末等，累計 1,000 万台以上），官公庁向け携帯電話ソリューション（全国展開，約 3 万 4,000 ライセンス），来店ポイントシステム（全国の店舗で利用）など，広く社会の基盤技術として普及が進んでいる．

以上のように，受賞者らは，従来よりも高速軽量な暗号方式の研究開発に成功し，同アルゴリズムを国際標準とし，更に同アルゴリズムを様々なサービスに適用することで，安心・安全な社会基盤構築に貢献した．また，受賞者らの業績は技術的に高く評価され，先端技術大賞経済産業大臣賞（平成 24 年）[(6)]，全国発明表彰発明賞（平成 25 年），前島密賞（平成 26 年），科学技術分野の文部科学大臣表彰科学技術賞（平成 26 年）などの多くの賞を受賞している．これらの業績は極めて顕著であり，本会業績賞にふさわしいものである．

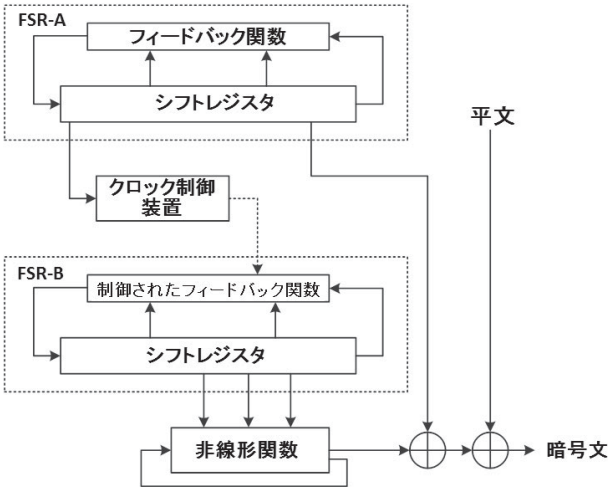

図 1　KCipher-2 の構成

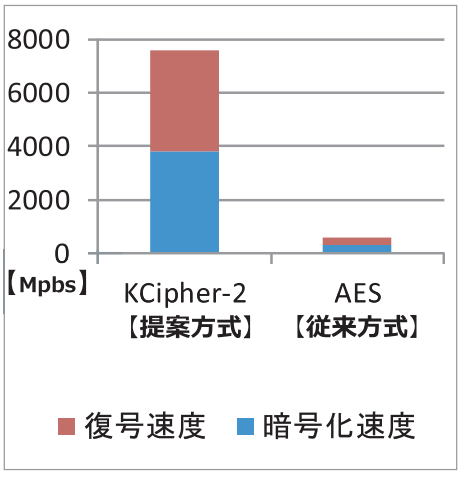

図 2　AES との速度比較（CRYPTREC レポートから）

文　　献

（1） S. Kiyomoto, T. Tanaka, and K. Sakurai, “K2 stream cipher,” ICETE 2007（Selected Paper）, CCIS, vol. 23, pp. 214-226, Springer, 2008.
（2） Y. Nakano, K. Fukushima, S. Kiyomoto, T. Ishiguro, Y. Miyake, T. Tanaka, and K. Sakurai, “Fast implementation of KCipher-2 for software and hardware,” IEICE Trans. Inf. & Syst., vol. E97-D, no. 1, pp. 43-52, Jan. 2014.
（3） ISO/IEC 18033-4 : 2011, “Information technology—Security techniques—Encryption algorithms—Part 4 : Stream ciphers,” 2011.
（4） CRYPTREC, “電子政府における調達のために参照すべき暗号のリスト—電子政府推奨暗号リスト—,” March 2013.
（5） IETF RFC7008, “A description of the KCipher-2 encryption algorithm,” Aug. 2013.
（6） 産経新聞（10 面），2012 年 6 月 12 日.

超大容量レイヤ統合トランスポートシステムの研究開発

受賞者　**那賀　明**

受賞者　**山崎悦史**

受賞者　**山本秀人**

爆発的な伸びを示すブロードバンドサービス・モバイルサービスのトラヒック需要を収容するために，基盤インフラの大容量化を経済的に推し進めていくことが必要である．NTT は基盤インフラを構成する伝送システムについてこれまで大容量かつ低消費電力な伝送システムの研究・開発を進めてきた．

一方，近年イーサネットや VoIP など，IP 系サービスが主流になっており，通信キャリヤのネットワークで流通するトラヒックの多くはレガシー系サービスから IP 系サービスに大きくシフトしている．今後急増する IP 系トラヒックを効率的に収容するためには，これらの信号と親和性の高いパケット収容可能な装置が必要である．しかしながら，現行システムではレイヤごとにそれぞれ異なる装置が設置・運用され，ネットワークが複雑になるほど装置数も多くなり，管理・運用が煩雑になる課題があった．

那賀　明君と山本秀人君は，MPLS-TP 技術を伝送システムに実装することで今後ますます需要が見込まれる IP 系トラヒックの効率的な収容を可能にするレイヤ統合トランスポートシステムを適用したネットワーク構想を推進し，システム技術詳細仕様の策定等の各開発工程を経て，本システム及びレイヤ統合管理するオペレーションを実用化し，爆発的なトラヒック増加と多様化するサービスに柔軟に対応可能なネットワークインフラの構築を可能とした．また，従来は現地作業が必要であった波長切換をカラーレス・ディレクションレス機能により遠隔で可能としたため，東日本大震災に代表される激甚災害時にも，迅速かつ容易にユーザトラヒックの復旧が可能な，100 G ベースのパケット無瞬断切換機能とネットワークの高信頼化を実現した．

大容量化を実現する手段としては，多値符号化により周波数利用効率を向上させる方法が既に検討されていたが，多値符号化を行うと光ファイバ内部で生じる雑音の影響を受けやすくなり，伝送可能距離が短くなるという課題が生じる．ディジタルコヒーレント光伝送方式は，超高速なディジタル信号処理（DSP : Digital Signal Processing）による信号補正により，これらの課題を解決した．更に本方式では DSP を利用した分散補償により，分散測定や設計など構築前の運用稼動削減が可能となった．補償用品の設置が不要となることで用品コスト削減が可能となるだけでなく，伝送遅延の低減も可能になり，ネットワークの低遅延化にも大きく貢献している．

山崎悦史君は，ディジタルコヒーレント光伝送方式による 1 波長当り 100 G 光伝送高機能化方式の研究開発を行った．100 G 超高速送受信方式を適用したシステムをいち早く実用化し，大容量光伝送方式技術及び最先端光デバイス技術の研究開発の出口を創出することにより，関連研究分野にインセンティブを提供して研究活動を活発化した．また，物理的なフィールド環境や，システム保守運用を考慮した実用化技術の研究開発・検証に取り組み，デバイスレベル及びシステムレベルの機能開発・評価，フィールド試験を含む検証を重ね，実用に堪える成熟度に高めた．

以上のように，受賞者らはネットワークインフラの基盤となる 8 Tbit/s（100 G×80 波長）伝送可能な波長ク

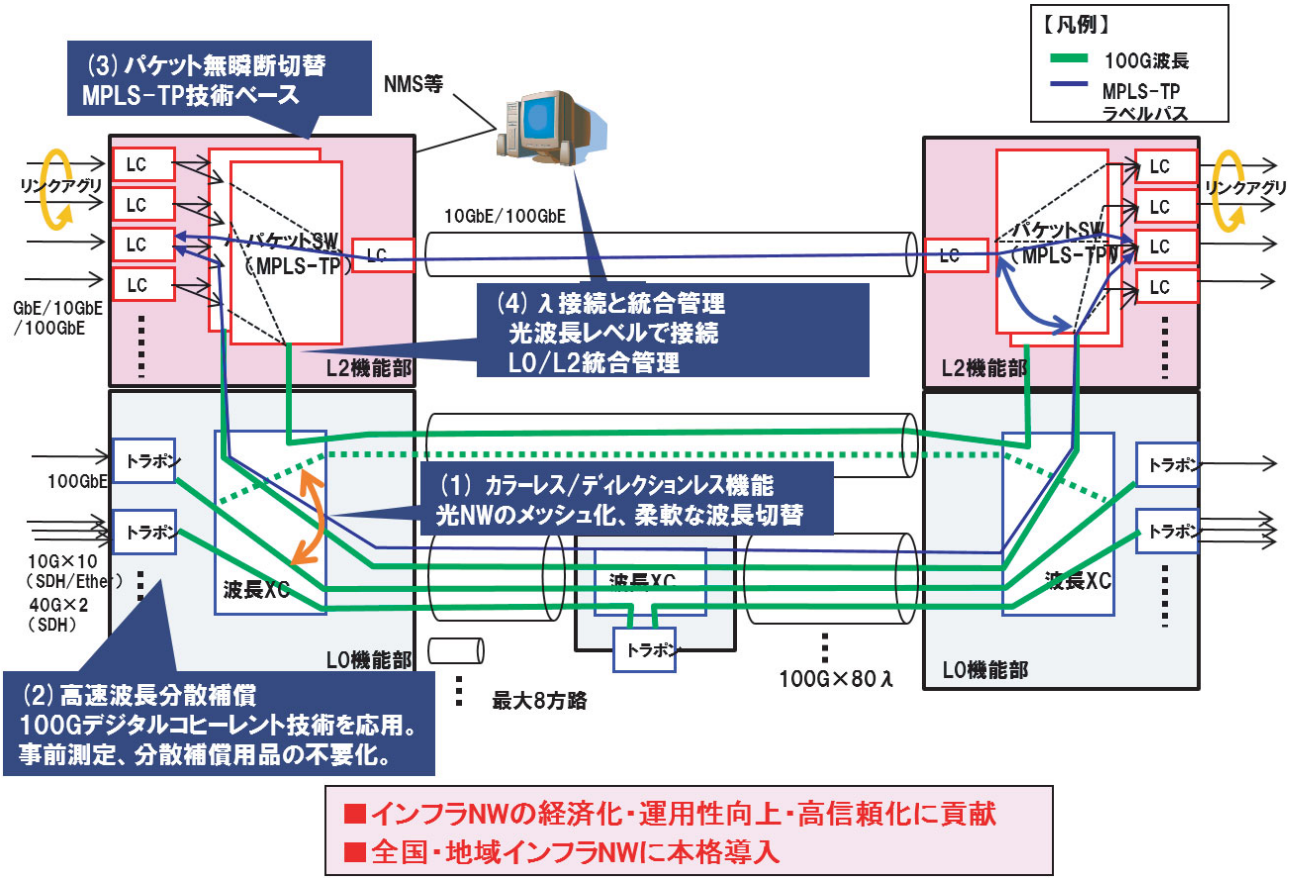

図1　超大容量レイヤ統合トランスポートシステム構成とキー技術

ロスコネクト（XC）部と，100 G ベースの高機能パケットスイッチ部を統合した低コストかつ低消費電力な超大容量レイヤ統合トランスポートシステムを研究開発，実用化した．多様なサービス提供に大きく貢献が期待できるとともに，運用性の向上により少子化が進む社会情勢にも対応可能と捉えており，社会基盤であるネットワークインフラの要求に応えるシステムである．このことから，受賞者らの功績は極めて顕著で，本会業績賞にふさわしいものである．

文　　献

（1） E. Yamazaki, S. Yamanaka, Y. Kisaka, T. Nakagawa, K. Murata, E. Yoshida, T. Sakano, M. Tomizawa, Y. Miyamoto, S. Matsuoka, J. Matsui, A. Shibayama, J. Abe, Y. Nakamura, H. Noguchi, K. Fukuchi, H. Onaka, K. Fukumitsu, K. Komaki, O. Takeuchi, Y. Sakamoto, H. Nakashima, T. Mizuochi, K. Kubo, Y. Miyata, H. Nishimoto, S. Hirano, and K. Onohara, “Fast optical channel recovery in field demonstration of 100-Gbit/s Ethernet over OTN using real-time DSP,” Opt. Express, vol. 19, no. 14, pp. 13179-13184, 2011.

（2） S. Yamamoto, T. Inui, H. Kawakami, S. Yamanaka, T. Kawai, T. Ono, K. Mori, M. Suzuki, A. Iwaki, T. Kataoka, M. Fukutoku, T. Nakagawa, T. Sakano, M. Tomizawa, Y. Miyamoto, S. Suzuki, K. Murata, T. Kotanigawa, and A. Maeda, “Hybrid 40-Gb/s and 100-Gb/s PDM-QPSK DWDM transmission using real-time DSP in field testbed,” OFC, 2012.

（3） E. Yamazaki, “Evolution of 100 Gb/s digital coherent signal processing moving to metro applications (invited),” SPPCom, 2013.

（4） E. Yamazaki, M. Tomizawa, and Y. Miyamoto, “100-Gb/s optical transport network and beyond employing digital signal processing,” IEEE Commun. Mag., vol. 50, no. 2, pp. s43-s49, 2012.

（5） S. Yamamoto, S. Yamanaka, A. Matsuura, T. Kobayashi, A. Iwaki, M. Suzuki, T. Inui, T. Sakano, M. Tomizawa, Y. Miyamoto, T. Kotanigawa, and A. Maeda, “PMD tolerance of 100-Gbit/s digital coherent PDM-QPSK in DSF-installed field testbed,” OECC, 2011.

（6） T. Kobayashi, S. Yamanaka, H. Kawakami, S. Yamamoto, A. Sano, H. Kubota, A. Matsuura, E. Yamazaki, M. Ishikawa, K. Ishihara, T. Sakano, E. Yoshida, Y. Miyamoto, M. Tomizawa, and S. Matsuoka, “8-Tb/s（80×127 Gb/s）DP-QPSK L-band DWDM transmission over 457-km installed DSF links with EDFA-only amplification,” OECC2010, PD2, 2010.

（7） T. Matsuda, T. Kawasaki, T. Kataoka, A. Naka, and K. Oda, “PMD design for high-speed WDM Backbone network systems based on field PMD measurements,” IEICE Trans. Commun., vol. E94-B, no. 5, pp. 1303-1310, May 2011.

（8） 関　剛志，濱岡福太郎，松田俊哉，那賀　明，織田一弘，“OXC の経路切替における CD/CDC 機能の性能比較，” 2012 信学ソ大 , no. B-10-112, Sept. 2012.