令和５年７月１日発行　第65号

Fundamentals Review

2023 July Vol.17 No. 1

特別寄稿

高等教育の質保証とコンピテンシーに関する取り組み

技術の原点

6G システムにおける非線形最適化技術適用の利点とその課題

アクティブノイズコントロールにおける最近の動向

https://www.ieice.org/ess/ESS/Fundam-Review.html

一般社団法人 電子情報通信学会　基礎・境界ソサイエティ / NOLTA ソサイエティ

ESS
2023
July
Vol.17 No. 1

Fundamentals

Review

〒105-0011 東京都港区芝公園 3-5-8 機械振興会館内
電話（03）3433-6691（代） FAX（03）3433-6659
E-mail:office@ieice.org 振替口座：00120-0-35300

EiC 電子情報通信学会
基礎・境界ソサイエティ / NOLTA ソサイエティ

ごあいさつ

基礎・境界ソサイエティが取り組むべき課題

Future Challenges for Engineering Sciences Society

基礎・境界ソサイエティ会長　梶川嘉延

1. はじめに

基礎・境界ソサイエティ（ESS：Engineering Sciences Society）は 1995 年に電子情報通信学会（信学会）においてソサイエティ制の制定とともに誕生した．来年（2024 年）がちょうど発足して 30 年目の年となる[(1)]．私が信学会のソサイエティ大会で初めて発表したのがちょうど 1995 年の 9 月で，私の最初の原著論文が掲載されたのも 1995 年 1 月号の信学会和文論文誌（JA）ということで，ある意味 ESS の歴史とともに研究者人生を歩んできたともいえ，ESS とは何かしらの運命を感じるところである．特に 1995 年 9 月のソサイエティ大会での発表は今でも鮮明に記憶している．ディジタル信号処理のセッションで私と修士の学生がそれぞれ発表を行い，発表後の休憩時間に今でもお世話になっている関連の先生方から温かいお声がけとディジタル信号処理のコミュニティへの歓迎を頂いたことが私の信学会との関わりだけでなく研究者人生に多大な影響を与えたと思っている．また，私が修士の学生のときに信学会の応用音響研究会（1993 年 1 月）に発表したときのこともとても記憶に残っている．この当時の研究会は非常におおらかで，緊張した面持ちで参加していた私に座長の先生が，「今日は発表件数も少ないので 1 件あたり 60 分時間を取りましょう」と言われて，20 分くらいの発表スライドしか用意していなかったこともあり冷や汗をかいたことも記憶に新しい．ゆっくり説明をすることで 30 分程度に発表を引き伸ばすことはできたものの，30 分の質疑時間を残すことになり，どうなるものかと思っていたところ，参加されていた先生方から多数の質問を頂きあっという間に 60 分が経過し，発表終了となった．発表終了後に得も言われぬ爽快感があり，学会発表は良いものだなと思った次第である．

これらのエピソードは単なる私自身の述懐ではなく，本来の学会があるべき姿，学会の重大な役割の一端を示しているものであると思い，紹介した次第である．学会は単なる成果発表（学会発表や論文投稿）の場ではなく，様々な人との出会いを提供する場であり，特に若い研究者や学生たちに発表での達成感を抱いてもらうとともに，学会に来ればいろいろな人と研究分野のことはもちろん，それ以外のこともざっくばらんに話し合うことができる，そのようなコミュニケーションの場を提供することが重要である．ESS 会長に就任するにあたり，私自身が信学会から受けた上記のような多大な恩恵や機会を，今の若手の研究者や学生の皆さんに少しでも提供できるよう，運営委員会のメンバーの協力のもと，様々な施策を進めていきたい所存である．

2. ESS における最近の取り組み

ESS はこの数年間で様々な大きな改革に取り組んできた．その詳細はこれまでの ESS 会長の就任挨拶[(2)〜(4)]において述べられているので，ここでは簡単に総括するとともに残された課題を述べたい．

2.1 組織運営体制

ご存知のように ESS は 2019 年度より組織運営体制の大幅な改革を行った．それまで幹事会と運営委員会という運営体制だったものを，ソサイエティレベルの議論を行う新しい運営委員会と，サブソサイエティ及び研究専門委員会レベルの議論を行うサブソ・研専会議の階層的な運営体制へと移行した．この新しい運営体制も 4 年が経過し，かなり定着し，それぞれの会議体において以前に比べて深い議論が行われるようになったと思われる．ただ残念ながら 2020 年からのコロナ禍の影響で全ての会議体がオンラインで実施されたことにより，この 3 年間で会議には出席しやすくなったことから出席率がかなり高まるというメリットがあったものの，委員同士が膝突き合わせて議論するような機会が失われたことから横のつながりができにくかったことが残念である．今年度は対面での開催なども視野に入れて委員同士がざっくばらんに議論できるような機会を設けられればと考えている．

2.2 研究会運営の効率化

技報は完全電子化となり，信学会の共通システムに 2020 年より移行した．コロナ禍におけるオンライン開催が後押しする形になり，移行がスムーズに進んだのは不幸中の幸いだったといえる．また，2022 年度よりオンライン開催だけではなく，対面とオンラインを併用したハイブリッ

ド開催も多数行われるようになり，発表者や参加者の利便性は格段に向上したといえる．一方で，研究会を運営する幹事団にとっては完全対面や完全オンラインに比べて負担も大きく，ESS の各研究会において様々な運営方法が模索された．参加受付はどのような開催形式でもオンラインで行い，技報のオンライン化も相まって，研究会での受付業務はかなり簡素化されたように思う．そして，ハイブリッド開催におけるオンライン配信に関する仕組みも様々な模索を通じて，費用を抑えながらも運営の手間を取らせないような仕組みや機材も整備されたといえる．ESS においてハイブリッド開催向けの機材を貸し出しできるようなスキームづくりがようやく開始され，今年度には本格運用がなされるものと思われる．更に，研専の会計業務についても 2021 年度から本部への移管が徐々に進められ，今年度からは会計業務は完全に本部に移管されることになる．これにより，研専運営における負担が軽減されることで，より充実した研究会や各種イベントの開催に向けた取り組みに各研専が注力できるものと思われる．

2.3　論文誌・機関誌の充実

ESS では NOLTA ソサイエティとの共同機関誌である Fundamentals Review があり，2007 年度の創刊から今年で 17 年めとなる．Fundamentals Review は年 4 回発行されており，技術の原点に代表されるような第一線の研究者による非常に質の高い解説論文が掲載されるなど，その創刊より好評を得ている．一方で和英論文誌（JA/EA）については特にこの数年苦戦を強いられているといえる．和英論文誌ともに年々投稿件数が減少の一途を辿っており，和文論文誌はどのようにして投稿数を増やすのかが大きな課題となっており，英文論文誌は IF 向上が長年の懸案となっている．英文論文誌については IF 向上に向けた取り組み[(5)]を私が英文論文誌編集委員長のときに展開したが，まだその効果は見えておらず今後の推移を見守りたいところである．このような背景の中，学会全体の動きとして多言語化ツールが全ての英文論文誌で導入が始められようしている．特にアジア圏の研究者に母国語で読んでもらうことを念頭においているようで，これにより読者層に広がりが生じることを期待したい．なお，鎌部 ESS 前会長の発案で和文論文誌（JA）においても多言語化ツールの導入の検討が始められている．

3.　今後の取り組む方向性

以上のように，ESS では歴代の会長のリーダーシップのもと様々な改革や施策が展開されてきた．ここでは，今後取り組むべき施策について私見を述べたいと思う．

3.1　サブソサイエティを活用した更なる研専運営の効率化

前述したように，研専運営における負担の軽減並びに効率化のために，会計業務の本部への移管やハイブリッド開催のための機材の拡充などを進めてきている．以前に比べれば各研専幹事団の運営負担も多少は軽減されたといえるが，まだまだ負担がなくなったとはいえない状況である．また，研専により事情も異なるが，幹事団を担う人材が不足している研専も少なからずあるのが現状である．ご存知のように ESS ではほかのソサイエティにはない制度であるサブソサイエティ制度がある．制度発足時のサブソサイエティの主たる目的は NOLTA ソサイエティのように，ソサイエティへと発展的に独立を果たすことだったといえるが，現状の学会全体の会員数の減少傾向からもなかなかそのような展開は厳しいのではないかといえる．また，サブソサイエティに属さない研専も 12 あり，サブソサイエティに属する七つの研専よりも数的に多い状況である．ソサイエティになることを主たる目的とすると二の足を踏む研専が多いと思われるので，研専運営（特に研究会や各種イベント）を共同で行うための枠組みとしてサブソサイエティ制度を利用することで，更なる研専運営の効率化が図れるのではないかと思料する．したがって，既存のサブソサイエティも含めて ESS に属する 19 の研専の再グループ化を運営負担の軽減の観点から進めてみてはどうかと考える．

3.2　和英論文誌の魅力向上並びに編集体制の充実

和英論文誌の編集体制において分野編集幹事及び編集委員は一部の海外編集委員を除き，和英論文誌の両方を担当してきた．一方で，和英論文誌それぞれに編集委員長と編集幹事がおり，完全な一体運営とはなっていなかった．そこで，今年度より編集委員長及び編集幹事についても，和英論文誌の両方をハンドリングする体制に変更することで完全な一体編集体制となる．また，スムーズな編集委員長及び編集幹事の交代を実現するために副編集委員長及び副編集幹事を新たに設けることになる．副編集委員長及び副編集幹事の任期は 1 年であり，その任期中に編集委員会の運営方法を知るとともに，抱えている課題を理解するための準備期間として位置づける．それにより，編集委員長並びに編集幹事に就任すると同時に様々な新たな取り組みを検討並びに展開できる体制を取ることができるようになる．また，2022 年 10 月号から完全オープンアクセスとなった英文論文誌についても，その効果が徐々に表れることが期待されるため，その結果に基づき更なる施策を検討する必要がある．更に多言語化ツールの導入を和文論文誌にも展開することで，和文論文誌の価値向上に繋げられればと考える．

以上に述べた以外にも懸案事項は多数あるため，新たな運営委員会メンバー全員で協力して知恵を出し合い，少しでも ESS の発展に寄与できるよう最善を尽くしたいと思う．皆様のご支援とご協力を是非ともよろしくお願いいたします．

文　献

（1） 高橋篤司，“基礎・境界ソサイエティ会長として思うこと，”信学 FR 誌，vol. 15, no. 1, pp. 2-3, July 2021.

（2） 岡育生，“基礎・境界ソサイエティの現状と将来，”信学 FR 誌，vol. 12, no. 1, pp. 2-4, July 2018.
（3） 田口亮，“新しい体制下での基礎・境界ソサイエティの課題，”信学 FR 誌，vol. 13, no. 1, pp. 2-3, July 2019.
（4） 鎌部浩，“ESS の将来の知的創造と物質的創造，”信学 FR 誌，vol. 16, no. 1, pp. 2-4, July 2022.
（5） 梶川嘉延，“英文論文誌 A の現状と展望，”信学 FR 誌，vol. 14, no. 3, pp. 167-169, Jan. 2021.

著者紹介

梶川嘉延（正員：フェロー）

1991 関西大学工学部電子工学科卒．1993 同大学大学院工学研究科電子工学専攻博士課程前期課程修了．同年富士通株式会社入社．1994 関西大学工学部電子工学科助手．1998 同大専任講師．2001 助教授．2007 同大学システム理工学部准教授．2009 教授．主に，アクティブノイズコントロール，パラメトリックスピーカなどにおける信号処理技術の研究に従事．博士（工学）．本会にて，ESS 副会長（システムと信号処理），英文論文誌（EA）編集委員長，信号処理研究専門委員会委員長，応用音響研究専門委員会委員長などを歴任．2012 年日本音響学会佐藤論文賞，2017 年 APSIPA Sadaoki Furui Prize Paper Award，2020 年本会論文賞など 6 の賞を受賞．

ごあいさつ

NOLTA ソサイエティは 10 年目を迎えます

10th Year of NOLTA Society

NOLTA ソサイエティ会長　長谷川幹雄

NOLTA ソサイエティ[1]は 2014 年 10 月 1 日に発足しました．まもなく 10 年目を迎えようとしています．ほかのソサイエティと比較すると未だとても小さく，研究会は二つ，会員数も小規模です．ただ，特筆すべき特色があると考えています．非線形問題（NLP）研究会[2]は，70 年以上の歴史をもつ伝統ある研究会です．複雑コミュニケーションサイエンス（CCS）研究会[3]は，発足してまだ 10 年程度の新しい研究会ですが，国際的なワークショップを毎年開催するなど活発な活動をしています．国際会議 NOLTA シンポジウムは，海外からも多くの参加者を集めております．国際ジャーナル Nonlinear Theory and its Apllications, IEICE[4]（NOLTA 誌）は，インパクトファクターを付与されることが決まりました．ますますの発展が期待される NOLTA ソサイエティを，私の視点でご紹介したいと思います．

NOLTA は，ソサイエティになる以前は，基礎・境界ソサイエティ配下のサブソサイエティでありました．当時は，研究専門委員会は NLP のみでしたが，2014 年 4 月に CCS が二つ目の常設研究専門委員会となることが承認されました．その年に，NOLTA がソサイエティとなることが承認されました．ただし，NOLTA ソサイエティは，基礎・境界ソサイエティから完全に独立しているわけではなく，共同運営の形となっています．基礎・境界ソサイエティに多大なご協力を頂きながら，NOLTA ソサイエティとしての活動を進めています．NOLTA ソサイエティは，国際的な視野を強くもっています．ホームページは英語のみです[1]．NOLTA 誌は，Editor の約半数が海外の研究者となっております[4]．

非線形問題（NLP）研究会[2]は，1951 年に非直線理論研究会として発足し，1970 年に非線形問題研究会に改称して現在に至っており，70 年以上の歴史があります．非線形現象やカオス，分岐現象，複雑系，ニューラルネットワークなど，あらゆる非線形システムを対象とした研究が発表されています．工学分野中心の電子情報通信学会の中で，かなりサイエンス色をもった研究が多く発表されています．NLP は，すぐには役に立たない研究でも，おもしろい現象を議論できる，様々な視点で自由に発表できる研究会です．

複雑コミュニケーションサイエンス（CCS）研究会[3]は，2011 年に時限研専として発足し，2015 年から常設研専となった新しい研究会です．通信，非線形，物理を中心とし，コミュニケーションに関するサイエンス，サイエンスに基づく新たなコミュニケーションなど，分野横断的な研究が発表されています．CCS は，時限研専としてスタートした当初から，日韓合同 CCS ワークショップ（JKCCS, KJCCS）を，日本と韓国で隔年で開催しています（2021，2022 年は，コロナの影響で開催されませんでした）．2023 年 1 月には，韓国の慶州で JKCCS2023 を開催しました．3 年ぶりの In-Person での開催となり，日韓双方の学生たちにとっても貴重な交流の機会となりました．次回の KJCCS は，2024 年 1 月に，別府で開催の予定となっています．

国際会議 International Symposium on Nonlinear Theory and Its Applications（NOLTA シンポジウム）は，1990 年から開催されています（2021 年はコロナの影響で NOLTA シンポジウムは開催しませんでしたが，Nonlinear Science Workshop をオンライン開催しました）．NOLTA シンポジウムは，日本で開催されることもありますが，ヨーロッパ，米国，アジアなど，海外で多く開催されています．NOLTA シンポジウムでは，非常に多くの様々な分野の Special Session が企画されます．学生の発表も多く，海外で英語で発表する貴重な機会となっていると思います．今年（2023 年）は，イタリアのシチリア島で 9 月に開催します[5]．2024 年は，ベトナムのハロン湾で 12 月開催予定となっております．

国際ジャーナル Nonlinear Theory and Its Application, IEICE[4]は，2010 年に創刊されました．年 4 回出版されており，非線形理論とその応用を中心とした幅広い分野の論文を掲載しています．各号では，様々な分野の特集が組まれており，多くの論文を集めております．今年はインパクトファクターが付与されることが決定しており，今後更に発展していくことが期待されます．

私は，2023 年度，第 10 代目 NOLTA ソサイエティ会長を務めることとなりました．歴代の会長には，私が学生時代からご指導頂きお世話になっている第 4 代会長の池口徹先生，第 2 代会長の合原一幸先生がおられますが，この

10 代目から NOLTA の世代が少し変わってくると感じます．またこれまでの会長は，長い歴史をもつ NLP で委員長を経験者された方が会長になっていましたが，私は初めての CCS 推薦の会長となります．これまでの先生方が発展させてきた NOLTA ソサイエティを，更に継続／発展させていかなければならない責任を感じています．NOLTA シンポジウムや NLP 研究会では，学生時代から発表させて頂いており，いろいろな場所に連れて行って頂き，貴重な経験をし NOLTA に育てて頂いたと感じています．NOLTA に恩返しできるように，尽力していきたいと思っています．

文　献

（1） NOLTA Society, https://www.ieice.org/nolta/
（2） 電子情報通信学会非線形問題研究会，https://www.ieice.org/~nlp/
（3） 電子情報通信学会複雑コミュニケーションサイエンス研究会，https://www.ieice.org/~ccs/
（4） Nonlinear Theory and Its Applications, IEICE, Nonlinear Theory and Its Applications, IEICE, https://www.jstage.jst.go.jp/browse/nolta/_pubinfo/-char/ja
（5） 2023 International Symposium on Nonlinear Theory and Its Applications, http://nolta2023.org

著者紹介

長谷川幹雄（正員：シニア会員）

1995 東京理科大学・基礎工・電子応用工卒．2000 同大学院博士後期課程了．同年郵政省通信総合研究所（現在の国立研究開発法人情報通信研究機構）．2007 東京理科大学専任講師．2010 同准教授．2015 同教授（現職）．カオスニューラルネットワーク，無線通信システム，最適化等に関する研究に従事．2011 CCS 幹事，2012，2016-2017 CCS 副委員長，2013，2018 CCS 委員長，2014-15NLP 幹事，2023 NOLTA ソサイエティ会長．

特別寄稿

高等教育の質保証とコンピテンシーに関する取り組み

Quality Assurance and Competency Initiatives in Higher Education

牧野光則 Mitsunori MAKINO

1. はじめに

2022年3月に公表された文部科学省中央教育審議会大学分科会質保証システム部会の審議まとめ「新たな時代を見据えた質保証システムの改善・充実について」[(1)]では，学修者本位の大学教育の実現に関する改善・充実の方向性として，

・内部質保証について，自己点検評価結果により改善を評価し，公表する形へと充実
・学修成果の把握・評価や，研究環境整備，支援状況の大学評価基準への追加

の2点がうたわれた．2008年12月の中教審答申「学士課程教育の構築に向けて」[(2)]にて学位授与，教育課程編成・実施，入学者受け入れの3方針を公表することで各大学の教育の可視化を図るよう求められてから14年が経過し，各大学は教育の質が保証されていることを自己点検・評価したり，その結果を公表したりするだけではなく，大学評価の一部として第三者に点検・評価される時代に入りつつある．このような時代では，高等教育関係者は，教える側が一心不乱に研究や教育に打ち込む姿を見せることを通じて学生が「自然に」育つ，伸びることを期待するだけではなく，特定の目標（習得を期待する知識やそれを活用する能力，そしてそれらの基盤となるジェネリックスキル）を達成するために入力（入学）から出力（卒業，修了）までを適切に設計した学びや教えに関するシステムとして整備し，実施し，その結果を点検することが求められる．その結果，思惑どおりであれば更に上を目指すための中長期的な見直しを，一方で思惑どおりでなければ次の年こそ思惑どおりになるように直ちに手を打つ必要がある．すなわち，背中を見せるだけではなく，学生が進むべき道・方向をより具体的に示し，必要に応じて手を差し伸べることも教員の重要な務めと認識する必要がある．大学設置基準の大綱化（1991年7月施行）時に博士後期課程3年だった筆者にとって，大学教授とは背中を見せ続ける高い壁のような存在であったが，自身が教える側になった1992年4月以降にそんな雰囲気を身につける術も時間もなく，現在に至っている．自身の力不足はもちろんだが，社会が高等教育機関に求めていることが大きく変化したことは間違いないだろう．

しかし，このような動きは今世紀に入る頃から見え始めていたし，特に工学系はほかの分野に先んじて国外状況が伝わってきた．実際，電子情報通信学会も早い時期から対応組織を立ち上げ，情報を収集・発信した[(3)〜(8)]．したがって，冒頭で述べた「新たな時代を見据えた質保証システムの改善・充実について」についても特別な準備なく淡々と対応できるところもあるに違いないし，そうであることを強く期待する．一方，学生が入学から卒業・修了に至るまでどのように知識・能力などを獲得したか，を評価対象とする教育を仕組みと捉える取り組みは，1サイクルが大学の場合4年かかることから，なかなか短期間で（良い意味であっても）変えていくことは難しい．このため，今回の件についても，2022年から本格的な対応を始め，現時点では道半ばというところも一定数あるのではないだろうか．

筆者は，比較的早期から本会が設置したエンジニアリング教育の質保証に関する委員会に所属し，現在はアクレディテーション委員会の委員長職を担っている．また，このアクレディテーション委員会は，本会が教育事業の一つとして携わる(一社)日本技術者教育認定機構（JABEE）に関する事項を担当している．この関連で，筆者は本会推薦でJABEEの理事を務めているとともに，委員長を務める基準委員会ではCOVID-19からの出口戦略案を検討を始めている．加えて，自身の本務先では2008年より「段階別コンピテンシー」と称する，学生が具備すべき知識とそれを活用する能力を段階という名のルーブリックを作成し，それを（できるところから）実際の教育に適用し，本務先のFD活動の一つにもして頂いている．

この間自身が見たり，知ったりしたことだけではなく，本務先にて実際に取り組んできたことも含めて本記事として紹介することで，僅かでも読者諸氏の参考になればと願うものである．

2. 国際エンジニアリング連合，ワシントン協定と日本技術者教育認定機構

図1は，大学などの高等教育機関で4年以上にわたるエンジニアリング教育プログラムを認定する非政府組織（NGO）による団体「ワシントン協定」（Washington Accord）[(注1)]がカバーする国・地域の推移である．

牧野光則　正員：フェロー　中央大学理工学部情報工学科
E-mail　makino@m.ieice.org
Mitsunori MAKINO, Fellow (Department of Information and System Engineering, Faculty of Science and Engineering, Chuo University, Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.7-25 2023年7月

(注1)：https://www.ieagreements.org/accords/washington/

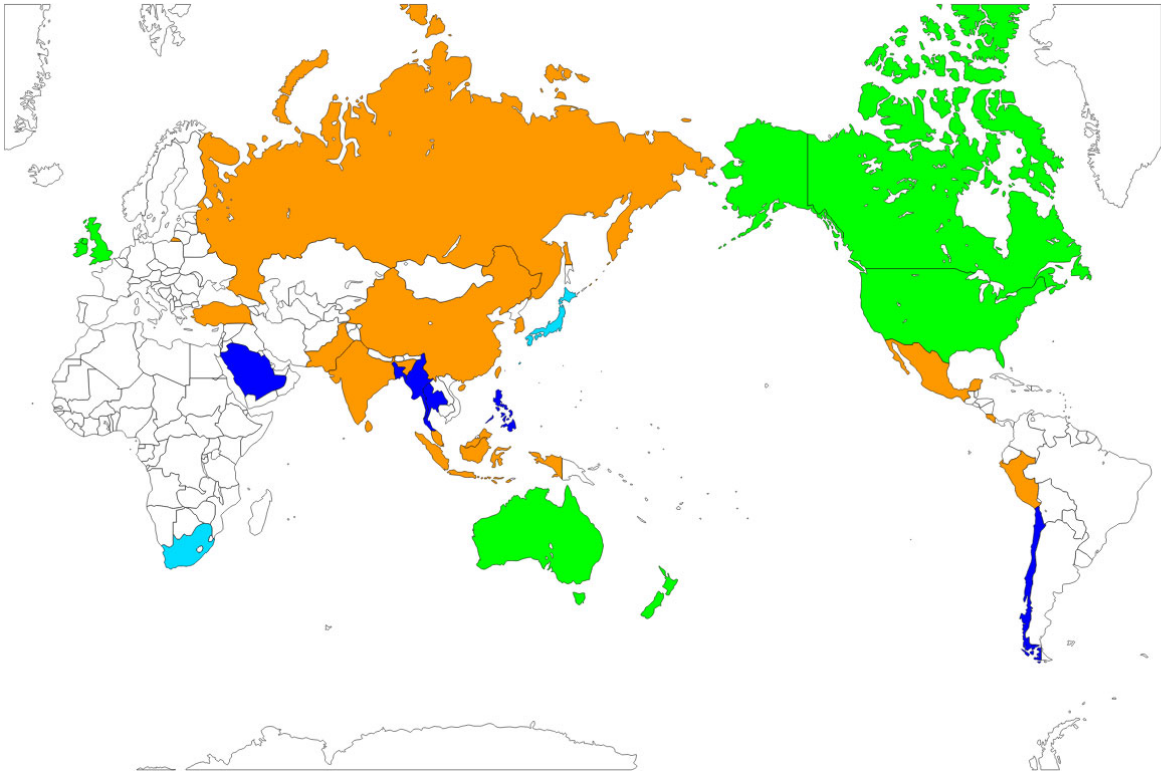


図 1　ワシントン協定がカバーする国・地域の推移　緑：設立時（1989 年）正式加盟機関が担当する地域，水色：1990 年～JABEE 正式加盟（2005 年）の正式加盟機関が担当する地域，オレンジ：2006～2023 年 3 月の正式加盟機関が担当する地域，青：2023 年 3 月時の暫定加盟機関が担当する地域.

ワシントン協定は 1989 年に，オーストラリア，カナダ，イギリス，アイルランド，ニュージーランド，米国に所在する六つの認定機関でスタートした．この協定に加盟する認定機関は同じような認定基準に基づき，エンジニアリング教育プログラムを認定していることを相互に認めることで，それぞれが認定する教育プログラムの実質的同等性を担保する．EU を中心とする欧州高等教育の枠組み “Bologna Process” とは異なり，ワシントン協定には認定機関が担当する国や地域の所在について条件がない．このため，その後アジアや中南米からも加盟を受け入れている．ただし，ワシントン協定加盟機関の活動領域は排他的なので，加盟を希望する認定機関がある国・地域のエンジニアリング教育プログラムの認定機関としてふさわしいことを加盟申請時に示す必要があるし，加盟後も相互による継続加盟審査を受けることで，その位置付けを保ち続けることが求められる．

日本では，数年間の準備期間を経た後に，ワシントン協定への加盟を目指して日本技術者教育認定機構（JABEE）(注2) が工学系学協会の協力で 1999 年に設立された．電子情報通信学会は準備期間から本件に関わり，JABEE が一般社団法人化した 2009 年以降は正会員としてその活動を支えるとともに，本会のアクレディテーション委員会委員長を理事として JABEE に推薦している．2023 年 3 月現在，篠田庄司氏（中央大学名誉教授），田中良明氏（早稲田大学名誉教授）に引き続き，筆者が本会から 3 人めとなる理事を務めている．

JABEE は設立翌年の 2000 年から認定の試行審査を，2001 年から正式認定をそれぞれ開始したので既に 20 年を超える実績を有する．審査開始年には，ワシントン協定に正式加盟を目指す準備がある程度進んでいる認定機関と位置づけられる暫定加盟が認められた．そして，JABEE が行う審査作業のレビューなどを経て，2005 年に正式加盟が認められている．なお，JABEE 以前に香港が正式加盟しているので，JABEE はアジア初ではない．しかし，英語による高等教育が標準ではない非英語圏からの加盟という点では初である．その後，韓国，台湾，マレーシア，インド，中国などアジアからの加盟が相次いでいるほか，スペイン語圏の中南米ペルー，コスタリカ，メキシコの認定機関が正式加盟したり，アラビア語圏のサウジアラビアの認定期間が暫定加盟したりしている．2023 年 3 月現在，正式加盟機関数は 23，暫定加盟機関数は 6 に及ぶ．図 1 では，協定が発足した 1989 年の協定創始 6 機関が担当する地域を緑，発足以降 2005 年の JABEE 加盟時点までに加盟した 3 機関が担当する地域を水色（香港は小さいので着色していない），JABEE 加盟以降 2023 年までに加盟した 14 機関が担当する地域をオレンジ，暫定加盟機関が担当する地域を青でそれぞれ示した．地域的つながりで高等教育を推進しているヨーロッパを除く地域，特に，環太平洋地域を中心に加盟機関が増えている．協定加盟機関が担当する国や地域は G20 中 14（一つの暫定加盟機関を含む．なお，残る 6 はフランス，ドイツ，イタリア，EU，アルゼンチン，ブラジル）である，また，国や地域によっては技術者資格付与に関わる組織が教育認定を担う．したがって，強弱あれどそれぞれの国や地域において，そし

(注 2)：https://www.jabee.org/

て国際的にもある程度の勢力と位置づけられよう．前述のとおり，ワシントン協定には加盟団体が担当する国や地域に制限がないことから，ある国や地域を所掌する認定機関が認定している教育プログラムの教育の質が国際的に通用する水準にあることを証明し，これを基として当該プログラムの卒業生・修了生は国際的に通用するエンジニアであると主張するための有用・有力な手段として，ワシントン協定加盟を目指す動きは今後もしばらく続くと予想される．

21 世紀に入る頃から（すなわち，JABEE が加盟する少し前から），ワシントン協定加盟認定機関の認定基準がプログラム修了生のアウトカム評価に基づく教育の質保証にシフトした．その先鞭をつけたのは，米国の認定団体 ABET が 1997 年に公表し，2000 年から導入した認定基準 EC2000 と称されるものである．それまでの審査では，カリキュラムに対する厳しい制約を課し，その基準へのそれぞれのプログラムのカリキュラムの適合性を審査していた．これに対し，産業界やその枠に留まらない教育を志向する高等教育機関からの問題提起・批判などがあり，大きな転換がなされたものである．なお，ABET 自らが点検し 2006 年に公表したレポート[9]では，EC2000 導入の効果が高かったとしている．

それまでの What is taught（by the university）から What the graduates achieved への大きな方針変更，そしてその前提となる educational objectives の明確化と learning outcomes の評価方法の開発の重要性の強調は，検討中だった JABEE の設立に大いに影響した．その結果，JABEE の認定基準は当初からアウトカム評価に基づく教育の質保証を中核にした．これは，その後の大学評価基準にも通じるものであったので，部分的かつ強制ではない任意の認定とはいえ国内で先鞭をつけたといってよさそうである．一方，認定基準には「学習保証時間」と称した学習・教育の量の担保を求める基準も当初含まれていた．これは，アウトカム評価を純粋な出口のみでの評価とみなすと矛盾しているので，二兎を追う印象を関係者に与えたかもしれない．しかし，JABEE が唱えるアウトカム評価とは，「結果として目標を達成した者を合格させる（卒業・修了させる）」ことではなく，「そのプログラムに入った標準的な学生であれば掲げた目標を達成できるような仕組みを作り，実際にそれを経て，かつ，実際に目標を達成した学生を合格させる」ことになっているか，を問うている．この仕組みの適切性を測る一つとして，学習保証時間が認定基準に盛り込まれたと筆者は認識しているが，それを審査する負荷は審査を受ける側・行う側双方にとって過重であったことも確かである．結局，その後の認定基準改定を経て，現在はそのような量的な項目は JABEE の認定基準には存在しない．一定の学習成果を上げるためには，それなりの学習・教育の量が必要なことは当然であることから，認定基準に基づく審査対象として求めなくても教育機関はその確保を図るはずで，それが余りにもなされていなければ量的な基準がなくても JABEE はほかの基準をもとに指摘できるはず，との認識を多くの関係者が共有した結果であろう．加えて，単位制の実質化という名のもとに，大学・高専評価に関係する観点が含まれたことも一因であろう．なお，2022 年 10 月施行の大学設置基準第 21 条[10]では，1 単位の授業科目を 45 時間の学修を必要とすることが標準であることを維持しつつ，授業時間の定義が撤廃された（それまでは講義・演習は 1 単位について 15〜30 時間，実験・実習・実技は 30〜45 時間の授業）．現在，90〜100 分授業を週 1 回×半年実施すると 2 単位が標準的であるが，大学が授業の事前・事後学習をきちんと学生に求め，実際に学生が取り組んでいることを（仕組みとして）示せれば，今後違いが出ることも十分に考えられる．

話を戻そう．ABET や JABEE が加盟する，Engineeirng 教育認定団体の連合であるワシントン協定は，Engineering Technology 教育認定団体の連合であるシドニー協定，Engineering Technique 教育認定の連合であるダブリン協定とともに，Engineer の専門職・職能団体の連合である IPEA 並びに APEC（地域制限あり），Engineering Technologist の専門職・職能団体の連合である IETA，及び Engineering Technician の専門職・職能団体の連合である AIET と，広義の技術者及び技術者になろうとする者に対する資格及び教育に関する連合組織 International Engineering Alliance（国際エンジニアリング連合，IEA）[注3]を 2001 年より構成している．IEA のもとで，教育認定機関と資格機関が連携することで，教育内容・水準の実質的同等性や職能の実質的同等性を確保し，もって卒業生・修了生や資格保有者の国際的なモビリティ（流動性）の確保を目指している．

その IEA では，教育，専門職それぞれの段階で達成すべき知識及びその活用力について検討がなされ，Graduate Attributes and Professional Competencies（GA & PC）としてまとめられている．2009 年に京都で開催された IEA 総会にて承認された ver. 2 以降，加盟団体はこれをリファレンスとして用いている（ほぼそのまま自身の認定基準とした認定機関もあった）．その後，若干の文言修正がなされた ver. 3 を経て，2021 年に ver. 4[11]が公表され，2022 年春にその参考和訳[12]が日本技術士会及び JABEE の 3 団体関係者によりまとめられた．この ver. 4 は，2020 年からの新型コロナウイルス感染症の最中に WFEO 及び UNESCO の支援を受けて改定されたものである．主要な改定内容は，国連の SDGs を踏まえた，持続性（sustainability），包摂性（inclusion）などの考慮である．Engineering はそのような観点が初めから含まれているので，従来の GA & PC でもそれらへの考慮がなされていると解釈し得るが，明示することで工学に関わる教育認定・専門職認定に確実に組み込むよう求める意図があると推察する．実際，IEA はワシントン協定などを通じて加盟団体に対して，GA & PC ver. 4 の認定基準などへの反映に関するロードマップを提示するよう求めている．JABEE も COVID-19 感染拡大の影響を受けた特別審査対応からの出口段階で，何らかのアクションを起こす予定である．

IEA 傘下の各協定・枠組みが目指しているのは，それぞれが実施している認定の実質的な同等性を認め合うことで，認定された教育プログラムの修了生（卒業生）や専門職を相互に適切に遇すること，である．特に教育認定の場合，専門職資格獲得に認定プログラムの修了生であることを必須としている国や地域にとってはその重要度は高い．実際，マレーシアでは，Professional Engineer 資格の必要条件に自国の認定機関または協定加盟機関が認定したプログラムを修了していることが含まれている．マ

（注 3）：https://www.ieagreements.org/

レーシアから日本の工学系学部に派遣されている留学生の国費留学奨学金対象者がJABEE認定プログラム所属のみであることはこの影響である．マレーシアのような，ワシントン協定にとっては理想的な実質的同等性を担保しているところは決して多くないが，教育プログラム認定を専門職資格団体が担っている，あるいは，教育プログラム認定団体と専門職資格団体が緊密な国や地域では，マレーシアの方向性を採用することは十分あり得る．例えば，米国の幾つかの州では，Fundamental Engineerを受験する際の手続きが米国の認定機関ABETと協定加盟機関による認定プログラム修了生とで同じとのことである．このような動きが加速すれば，日本の工学系学部にとっても，その国・地域からの優秀な学生に留学先候補の一つに含めてもらえるか否か，自身の卒業生・修了生が将来多くの国や地域でその実力に応じた待遇を受けられるのか，に関わるため，決して無関心ではいられない．

日本の場合，JABEE認定プログラムの修了生は技術士試験の一次試験を免除され，技術士補からそのキャリアを始められるが，認定プログラム修了はマレーシアのような必要条件ではない．このため，国際的に同等な認定を得るかどうかは教育機関の裁量に任されている．現時点で，JABEEの認定を獲得・維持しているプログラムは決して多くないし，急増する気配はうかがえない．法令で定められている大学評価に加えてJABEEの認定を得ることは負担増につながるし，多数の修了生が技術士を目指さない分野であれば，この状況が急変するとは予想できない．しかし，以下の2点において，認定を獲得・維持しているプログラムはその状態を継続すべきだし，認定を獲得していない，または以前は獲得していたものの現在は維持していないプログラムは十分に留意する必要があろう．

第一に，JABEEの認定は，教育の成果がワシントン協定やIEAという国際的枠組みで通用する水準に（少なくとも）到達していることを意味するので，教育の質保証の可視化手段として重要である．冒頭にて述べたとおり，国内教育機関は全分野において教育の内部質保証が強く求められるようになった．その内部質保証が適切であることを外部に示すためには，第三者による点検・評価は不可欠と考える．現在，大学評価においては，大学自身が設置する第三者評価委員会にて自己点検結果を評価している事例が多い．しかし，そのような設置方法では，評価結果の説明以前に第三者評価の中立性・独立性の確保に関する説明が必要となろう．一方，JABEEのような第三者評価機関に審査され認定を獲得すれば，少なくともJABEEが定める基準項目の範囲内で質保証がなされていること，その教育の水準は当該分野で国際的に通用し得るもの（か，あるいはそれを優に超えているか）であることを主張しやすい．高等教育が第三者から評価されるのが当然の国や地域と伍するためには，このような観点の意識が重要と考える．なお，専門分野別の教育認定機関としては，JABEEのほかに(一財)日本看護教育評価機構（JABNE）[注4]，(一社)薬学教育評価機構（JABPE）[注5]，及び(一社)日本医学教育認定機構（JACME）[注6]がある．このうち，JABEEと同じく国際的通用性を強く意識しているのはJACMEのみであるが，3団体いずれも専門職につながる教育の質を当該分野全体で点検・評価することで全体の底上げを狙う点ではJABEEと共通している．一方，これら3団体に比べてJABEEは「技術者」の名のもと，理工農系の幅広い分野を対象としていることから，各技術分野の違いを吸収して審査や認定を行う必要がある点に，関係者の苦労が多いと思われる．

第二に，国外の修了生に対する技術士一次試験免除措置の適用である．JABEE認定プログラム修了生を対象とする技術士一次試験免除は，認定プログラムの所在に制限がないためにJABEEが認定したインドネシアの大学の4プログラムの修了生にも適用される．ただし，インドネシアではJABEEと同格の認定機関であるIABEEが発足し，2022年7月にワシントン協定に正式加盟したので，今後JABEEがインドネシアの大学を審査することはない．むしろ，ワシントン協定正式加盟機関により認定されたプログラム修了生に対する同等の取り扱いが2022年から始まったことの方が重要であろう[13]．これによれば，「議題1」[注7]に関し，ワシントン協定に加盟する他国の団体が認定した課程の修了者に対しても，「技術士法第31条の2第2号に基づく技術士などの資格に関する特例を適用することとなった」とある．すなわち，今後，ワシントン協定の修了生が申請すれば日本で技術士補として活動でき，二次試験受験への道が開かれる．一次試験合格者と同等の知識を有するとみなす対象を，日本の法令が及ばない国外の大学などの修了生に拡大したことは対象者層のモビリティの更なる活発化を促す可能性がある．特に，国外で高等教育を修めた日本語を母語とする方にとっては，国内で資格を取得し，活躍する機会が拡大したといえるだろう．折しも日本は労働者人口減少による人手不足が各所で顕在化している．もし，日本の労働環境が他国・地域にとって魅力的であれば，この制度を活用して国内で活躍する者が（どの程度かは見通せないが）増加する可能性は高いと考える．すなわち，国内に職を求め，得ることが多い国内高等教育機関の卒業生・修了生の競争相手は決して国内にいる者だけではないことを，送り出す側も強く意識する必要があろう．

3. IEA GA & PCから見えること

IEA GA & PC[11]の中で，Engineering教育，Engineering Technology教育，Engineering Technique教育の違いに関して，翻訳[12]では将来取り組むことが想定されるエンジニアリング問題が「複合的」，「大枠で定義された」，「明確に定義された」の用語で定めている．この3用語が意味するところについてもGA/PC及び翻訳に表として記載されているので，ぜひ比較のためにご一読頂きたい．ここでは，JABEEが対象とするEngineering教育の卒業・修了生が具備すべき属性（graduate attribute）のみ抜粋して紹介する．

1. エンジニアリングの知識

複合的なエンジニアリング問題に対して，その解決策を立案するために，WK1～WK4にそれぞれ指定する数学，自然科学，コ

（注4）：https://jabne.or.jp/

（注5）：https://www.jabpe.or.jp/

（注6）：https://www.jacme.or.jp/

（注7）：技術士などの資格に関する特例について．

ンピューティングとエンジニアリングの基礎，及びエンジニアリングの専門分野の知識を応用すること．

2. 問題分析

複合的な問題について，持続可能な開発を総合的に考慮しつつ，数学，自然科学，エンジニアリング・サイエンスの原理を用いて，問題を特定し，定式化し，文献を調査し，分析して，根拠のある結論を得ること．

3. 解決策のデザイン／立案

複合的なエンジニアリング問題について，創造的な解決策をデザインし，ニーズに応じて公共の衛生と安全，耐用期間全体にわたるコスト，正味ゼロカーボン，更に資源，文化，社会，及び環境について適切に配慮しながら，定められた要件を満たすシステム，コンポーネントあるいはプロセスをデザインすること．

4. 調査研究

複合的なエンジニアリング問題について，研究に基づく知識，実験計画，データの分析と解釈，有効な結論を得るための情報の取りまとめなどの研究方法を用いて調査を行うこと．

5. ツールの活用

複合的なエンジニアリング問題に対して，予測やモデリングを含む，適切な手法，リソース，最新のエンジニアリングと IT ツールを作成，選択，適用するとともに，その限界を認識すること．

6. 複合的なエンジニアリング問題を解決する際に，持続可能な開発への影響，すなわち，社会，経済，持続可能性，健康と安全，法的枠組み，環境へのインパクトを分析し評価すること．

7. 倫理

倫理原則を適用するとともに，専門職としての倫理とエンジニアの実践規範を守り，関連する国内法と国際法を遵守すること．多様性と包摂性の必要性への理解を行動で示すこと．

8. 個人とチームによる協働作業

個人として，また多様で包摂的なチームの一員やリーダーとして，学際的，対面式，遠隔式や分散型の環境において効果的に役割を果たすこと．

9. コミュニケーション

複合的なエンジニアリング活動において，文化，言語，学習の違いを考慮しながら，例えば，効果的な報告書や設計書を理解・作成したり，効果的なプレゼンテーションを行ったりすることを通して，エンジニアリング関係者や広く社会と効果的かつ包摂的にコミュニケーションをとることができる．

10. プロジェクト・マネジメントと財務

エンジニアリング・マネジメントの原則と経済的な意思決定に関する知識と理解を，チームの一員やリーダーとして推進する自身の仕事に対して，また学際的環境においてプロジェクトをマネジメントする際に応用すること．

11. 生涯継続学習

以下について必要性を認識し，これらに取り組む心構えと能力をもつこと．

ⅰ．自主的かつ生涯を通じた学習

ⅱ．新しい技術や新興の技術への適応力

ⅲ．技術革新の最も広範な文脈に対するクリティカル・シンキング

上記のうち，下線がある「持続可能～」「多様」「包摂」は ver. 4 策定の際に国際連合の持続可能な開発目標（UN SDGs）を強く考慮した結果として盛り込まれている．GA & PC ver. 2 及び ver. 3 に対して，エンジニアリング系の各分野に対応する勘案事項も含めた「認定基準の解説」の内容と対比させた点検の結果，JABEE の認定基準は十分に GA & PC に対応しているとの結果を得ている．一方，UN SDGs が反映された ver. 4 は問題や対象となる人や社会が幅広くなっているので，これまでの基準の解釈では対応が十分とはいえない可能性がある．このため，JABEE の認定基準，特に以下に示す基準 1.2 で定められている修了生が確実に達成する学習・教育到達目標に含まれるべき知識・能力観点そのもの，あるいはその解釈の範囲内に GA & PC の改定内容をどう盛り込むか，が JABEE に現在課せられている．

(a) 地球的視点から多面的に物事を考える能力とその素養

(b) 技術が社会や自然に及ぼす影響や効果，及び技術者の社会に対する貢献と責任に関する理解

(c) 数学，自然科学及び情報技術に関する知識とそれらを応用する能力

(d) 当該分野において必要とされる専門的知識とそれらを応用する能力

(e) 種々の科学，技術及び情報を活用して社会の要求を解決するためのデザイン能力

(f) 論理的な記述力，口頭発表力，討議などのコミュニケーション能力

(g) 自主的，継続的に学習する能力

(h) 与えられた制約の下で計画的に仕事を進め，まとめる能力

(i) チームで仕事をするための能力

GA & PC から見えてくるのは，エンジニアとは専門技術者という用語には収まらない，幅広い知識・教養を基盤として継続的に習得する専門知識・技術・技能を発揮することで，時として相反する制約条件の中で最善の課題解決手段を志向し，他者を導く人であり，高度人材の中でも上位に位置付けされている，ということである．すなわち，エンジニアは誇り高き職種であり，他者からも尊敬に値するものであろう．その誇り高い職種に将来就こうとする者に対して，高等教育機関による学び・教えは重要であり，いわゆるジェネリックスキルも含めて幅広く，かつ，深く学べる仕組みが求められている．この仕組みを構築し，かつ，その仕組みが正しく機能して卒業生・修了生を輩出するためのキーワードとしてコンピテンシーとルーブリックが最近良く用いられている．これらについて次章以降で紹介し，筆者の取り組みを述べる．

4. コンピテンシーに関する各種提言と中央大学段階別コンピテンシー

上述の GA & PC に限らず，21 世紀に入ってから，学びや教えの成果が「コンピテンシー」をキーワードに語られることが多い．コンピテンシーとは一般に高業績を上げる人がもつ，他者が観察可能な特性を意味する．能力やスキルと似た概念だが，業務などある特定の場面で常に，またはほぼ常に顕著な行動として現

れるものである．このため，能力やスキルの中で人に内在し顕在化しない部分は，コンピテンシーとは異なる．このため，コンピテンシーだけではその人の特性全てを測ることはできず，あくまでも観察可能な範囲内での特性であることに注意が必要である．

コンピテンシーは 20 世紀では労働者の業務評価や分析に使われていたが，21 世紀に入り教育の成果を測る指標としても使われるようになった．その先駆けといえる OECD の DeSeCo プロジェクト(注8)で示されたキー・コンピテンシーは，「思慮深さ」(reflectiveness) を中心（内面）に置きつつ，資料[14]p. 75 によれば以下の 3 種で定義された．

1. 社会・文化的，技術的ツールを相互作用的に活用する能力
   a. 言語，シンボル，テクストを相互作用的に活用する能力
   b. 知識や情報を相互作用的に活用する能力
   c. テクノロジーを相互作用的に活用する能力
2. 多様な社会グループにおける人間関係形成能力
   a. 他人と円滑に人間関係を構築する能力
   b. 協調する能力
   c. 利害の対立を御し，解決する能力
3. 自律的に行動する能力
   a. 大局的に行動する能力
   b. 人生設計や個人の計画を作り実行する能力
   c. 権利，利害，責任，限界，ニーズを表明する能力

また，OECD は 2015 年以降 Education2030 プロジェクトを実施しており，その中間報告ともいえるポジションペーパーが公開されている[15],[16]．そこではキー・コンピテンシーに対して「変革を起こす力のあるコンピテンシー」として以下の 3 点の追加を提唱し，かつ，全てを統合するものとして，変化を起こすために，自分で目標を設定し，振り返り，責任をもって行動する能力として「エージェンシー（主体性）」を示している．

・新たな価値を創造する力
・対立なジレンマを克服する力
・責任ある行動をとる力

国内では，大学学士課程を対象に文部科学省中央教育審議会が 2008 年 12 月に取りまとめた「学士課程教育の構築に向けて」と題する答申[17]にて，以下の四つで構成される学士力の参考指針を提示した．

1. 知識・理解（文化，社会，自然など）
2. 汎用的技能（コミュニケーションスキル，数量的スキル，問題解決能力など）
3. 態度・志向性（自己管理力，チームワーク，倫理観，社会的責任など）
4. 総合的な学習経験と創造的思考力

また，2010 年からは，日本学術会議大学教育の分野別質保証委員会が各分野（2023 年 3 月時点で 33 分野）の教育課程上の参照基準を作成，公表している(注9)．ほかにも，経済産業省が 2006 年に提唱した社会人基礎力(注10)など，コンピテンシーという用語を使わなくとも同種の概念で具備すべき資質・能力が提示されている．

5. 段階別（ルーブリック）コンピテンシーの導入～中央大学理工学部情報工学科の場合

中央大学段階別コンピテンシーとは，狭義には行動特性を複数かつ 6 段階に分類した，表（ルーブリック）形式の学生に対する指標を指し，広義にはこの指標を用いた自己点検・他者点検活動，更にはそれを用いた科目やカリキュラムの設計・評価を含む教育改善の取り組みを意味する．2008 年夏に理工学部情報工学科で取り組みを始め，2009 年度に理工学部の教育プロジェクトとして文部科学省新教育 GP に応募・採択された．そして，文部科学省就業力 GP の一部として中央大学の 6 学部全て（当時）に対象を拡大し，キャリア支援の立場から学生のコンピテンシー向上を支援する Web 上の自己点検システム C-compass を開始した．その際，理工学部各学科の教育の特徴を組み込んだ「専門性」がシステムには盛り込まれなかった．更に，新グローバル GP で専門職を含む大学院生も対象とするために「多様性創発力」の定義追加と最上位への段階追加がなされた．これらの大学全体の取り組みに並行して，理工学部では，ディプロマ・ポリシーの記述をコンピテンシーの適切な段階に対応させた三つの方針を策定・公表した．すなわち，学生が卒業時までに当該段階かそれ以上の段階にコンピテンシーが到達していること，卒業時に到達させるために必要なコンピテンシーを向上させる教育を実施すること，そして，その教育の実施にとって学生が最低限必要な資質を有するかどうかを入学時に確認すること，と設定した．

筆者が所属する情報工学科の場合，コンピテンシーは以下の 8 カテゴリ，及び各カテゴリをより具体化した合計 36 キーワードで構成される（図 2）．

・コミュニケーション力：傾聴力，読解力，記述力，提案力，議論力
・問題解決力：課題発見，課題分析，論理的思考，計画実行，検証
・知識獲得力：学習，応用力，情報収集力
・組織的行動能力：バランス力，役割認識，主体性，協働，率先力
・創造力：発想する力，推論する力，感動する力，探究する意欲，倫理
・自己実現力：目標設定，スケジュール管理，自己管理，ストレスコントロール，達成志向
・多様性創発力（新グローバル GP 時に追加）：自確力，融合力，協創力
・専門性（情報工学科）：基盤となる学力，数学・自然科学，情報技術基礎，専門知識，精確性

特徴としては，ジェネリックスキルと呼ばれる力だけでなく，専門知識を正しく活用する力も含めることで，学科教員が主体的に取り組まなければならないことを明確にしている点がある．この専門性は，2009 年当時理工学部に設置されていた 9 学科全てが定義している．この専門性に関する定義を読むと，各学科の専門教育のポイントが見えてくると考えている．

8 カテゴリ及び 36 キーワードそれぞれに対して上位から創発

(注 8)：https://www.deseco.ch/bfs/deseco/en/index.html
(注 9)：https://www.scj.go.jp/ja/member/iinkai/daigakuhosyo/daigakuhosyo.html
(注 10)：https://www.meti.go.jp/policy/kisoryoku/index.html

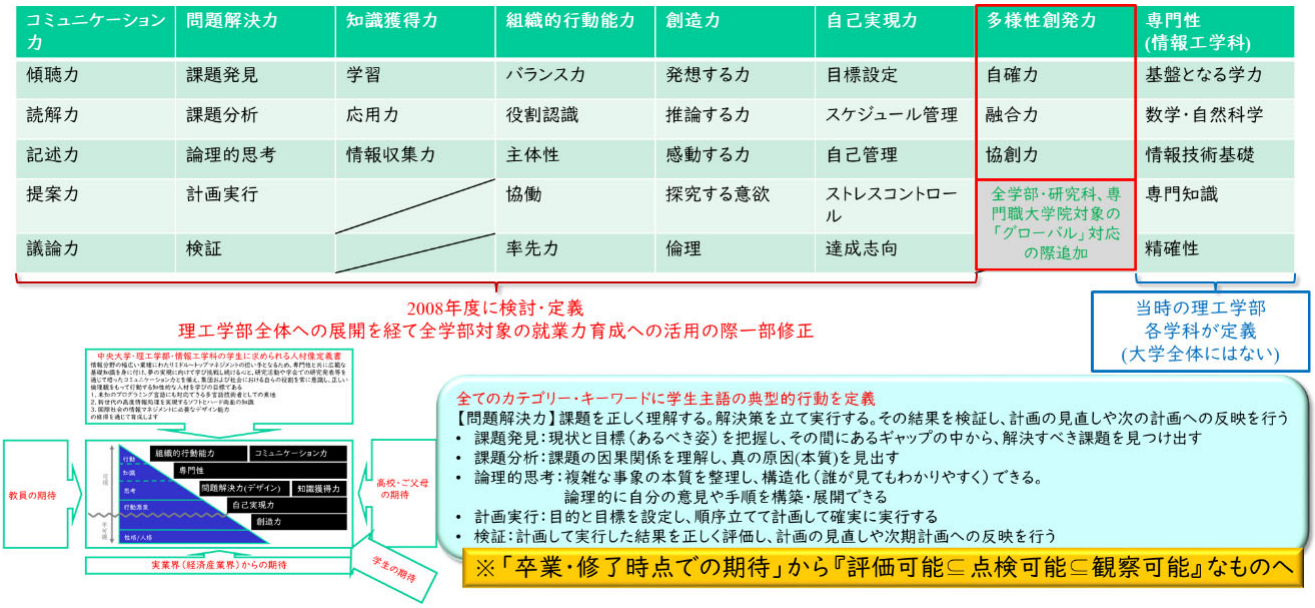


図 2　中央大学コンピテンシーのカテゴリ・キーワード（下部は当時の検討資料より）

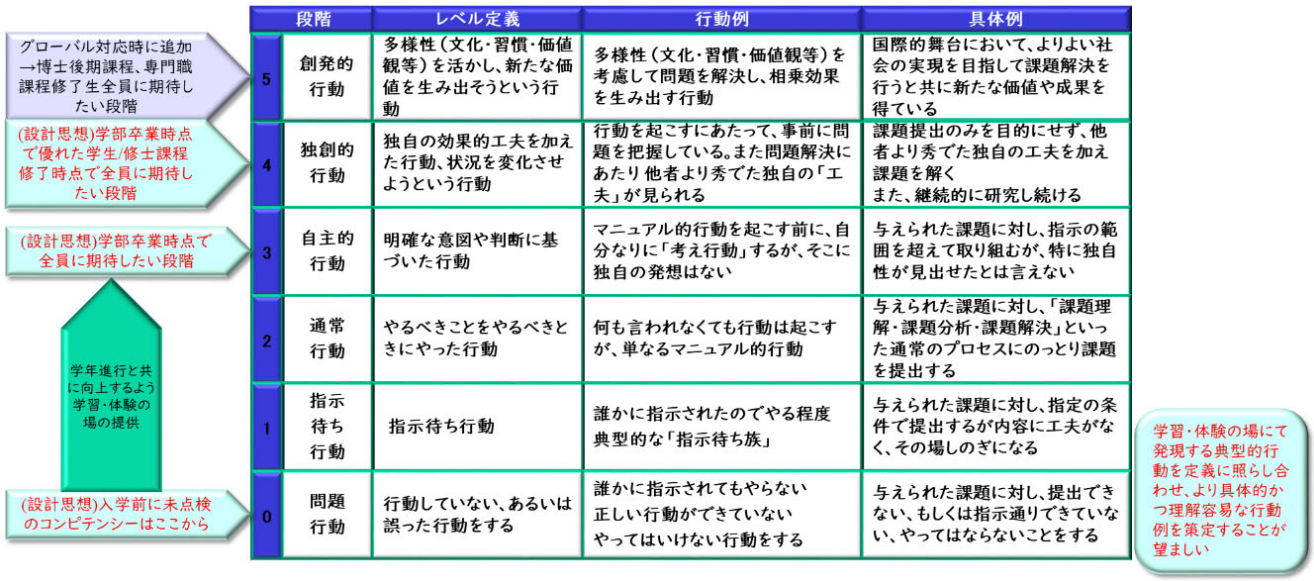


図 3　中央大学コンピテンシーの段階の考え方

的行動，独創的行動，自主的行動，通常行動，指示待ち行動，問題行動の 6 段階の行動水準を設け，それぞれに対する行動事例を記述することで，学生・教員双方にとって指標となるルーブリックとしている（図 3）．策定の際には，教員有志が企業の人材育成担当ファシリテータのもとで，フリーディスカッションからコンピテンシーのキーワードを抽出した上でカテゴリに集約し，全カテゴリ・キーワードに共通する段階（どういう行動を見分けたいか）を定義及び行動例として明確にした．以上で揃った表の行・列の共通定義を用いて全ての欄を埋める，という作業で巨大な表を完成させた．新グローバル GP の際には各学部・研究科から教職員が集められ，同様の作業でカテゴリ（多様性創発力）及び創発的行動（段階）追加を議論・検討・決定した（2023 年現在のコンピテンシー一覧を本稿末尾に付録として付ける）．その際には，グローバル人材育成を明確にする上でそれまでのカテゴリに加える力とは何か，また，専門職を含む大学院生に適用拡大するにあたり，独創的行動の上位に位置するに値する行動水準とは何か，について所属学部や職種の境を超えて意見交換した．副次的作用として，作業に参加した各学部の教職員を通じて段階別コンピテンシーの意義が大学全体に（薄く，点在かもしれないが）伝わったことは，その後の取り組みの継続に大いに役立っていると感じている．

中央大学段階別コンピテンシーは，学生に対して高等教育を修める人材，いわゆる高度人材にとってどのような行動特性がどのような水準で発現して欲しいのかを，入学から学部卒業，大学院修了まで示した段階的，順序的な指標である．このため，ある授業科目の特定場面で発現を期待する行動特性が全体から見てどの

部分のどの程度の水準なのかと関連付ければ，ディプロマ・ポリシーの達成に至るコンピテンシーの段階的向上がカリキュラム上どのように計画されているかを可視化できる．これは，教育の質保証の観点から高い意義をもつと考えている．この取り組みがコンピテンシーを大学教育に導入した早期の事例として注目されたため，他大学などからの訪問調査の受け入れや他大学などでの事例紹介講演を積極的に行ってきた．最近では，2022 年 12 月に開催されたお茶の水女子大学コンピテンシー育成開発研究所設立キックオフシンポジウム(注11)にて，筆者はパネリストの 1 人として中央大学の約 15 年の取り組みについて紹介した．

また，高等教育以外では，中等教育との連携・情報提供を行っている．その中でも，スーパーサイエンスハイスクールに採択された中央大学附属高等学校（及び連結する中学校）(注12)とは高大連携の主要取り組みとして，「Chufu コンピテンシー」と名付けた独自のコンピテンシー表の定義及び生徒の行動評価に協力している．Chufu コンピテンシーの狙いは，学びを通じた生徒の成長を把握することに加えて，高大連携の効果測定・評価が含まれており，これまでに興味ある結果が報告されている．Chufu コンピテンシーは高校生が対象のため大学のコンピテンシーとは内容や水準が異なるが，附属校としての高大連携がコンピテンシーの観点でどう成果を上げているのか，大学入学後は大学が求めるコンピテンシーの水準を（軽々と）満たしているのか，を測定するために関連性を保持している．また，以前にはスーパープロフェッショナルハイスクールに採択された愛媛県立宇和島水産高等学校(注13)と理工学部とがコンピテンシー教育に関する覚書を締結し，情報提供及び助言を行った．知識獲得だけではなくそれを活用して正しい技術・技能を習得し，正しく行動するための学び・教えの色が濃い水産高校において，コンピテンシーの考え方は参考になったのではないかと期待している．加えて直近の話題では，理工学部の地域連携の一貫として，淑徳 SC 中等部・高等部と「『デジタル教養コース』に関するコンピテンシーを核とした教育交流」に関する覚書を締結した．こちらの成果が見えてくるのは早くても数年先になるので，with/after COVID-19 の時代の中等教育として何らかの好影響を与えられることを期待している．

6. ルーブリックを意識した科目単位の評価基準の導入事例

「ルーブリック」（点検表）という用語は，最近では注釈なく高等教育を語る際に用いられていると感じている．筆者も段階別コンピテンシーに関わりを深めていく中で，学内の FD 推進委員として関連する記述を寄稿したり，新任教員研修会講師としてシラバスの書き方を支援する際にルーブリックを用いることを推奨したりしている．今や，多くの高等教育機関でルーブリックを用いた成績評価が普通になっていると思われる．その際，当該科目とディプロマ・ポリシーとの対応付けに基づいて，評価用ルーブリックが策定されることが当然望ましい．もし無関係に策定されていても，当該科目の評価方法と評価基準は明確であり，厳格に実施されているかもしれない．しかし，カリキュラムが当該科目の単位修得者に期待する知識や能力について評価されているか分からない．科目とディプロマ・ポリシーとの対応付けを更に一歩進め，対応するディプロマ・ポリシーのどの水準までの達成が当該科目に期待されているのか，を前後に連結する科目の達成目標と整合しつつ定めることがあるべき姿といえよう．

この考え方に沿って，情報工学科では，評価用ルーブリックをディプロマ・ポリシーとの関連を意識しながら策定し，実際に評価に用いている．例えば，画像・映像コンテンツ演習と称する，半年単位のチームプロジェクト科目では，最終回のポスター発表会において，期待する水準のコンピテンシーが実際の行動・言動として発現したかどうかを点検する簡単なルーブリックを個人単位・チーム単位で作成している．このルーブリックを用いて，卒業生が務める審査員が学生の発表・質疑を観察して判定している．卒業生に点検を依頼することで，当該ルーブリックの内容・水準だけでなく，当該科目の教育内容・水準について意見を収集することも狙いの一つである．

また，学科での学びの集大成（キャップストーン）となる卒業研究 II では，学科として採点の目安と称するルーブリック（上位から S，A，B，C，不合格）を以下のとおり策定し，学生に開示している．このルーブリックでは，標準的な行動特性に対して A，悪くても B 相当と判定することが想定されている．すなわち，S は明らかにほかの学生より秀でた行動を確認できる場合に付与される．一方，C は教員の指示がなければ動かない状況であり，主体的な学びが見えないことから，まさしく不合格の一歩手前に位置している．

・**S（95 点）**…卓越行動

ゼミにほぼ毎回出席し，調査や発表を質・量ともに高水準に行っている．ゼミ以外（学科主催の講習会なども含む）にも自主的・積極的に研究に取り組んでいる．卒業論文では，高い記述力や論理力を基盤として，研究の背景・目的・手段・特徴・評価考察などを高い水準で記している．発表では自らの研究の背景・目的・手段・特徴・評価考察などを正しくかつ効果的に発表し，質疑応答も的確に行っている．全体を通じて卓越した研究活動であり，ほかの学生の模範となり得る．

・**A（85 点）**…独自行動

ゼミの欠席は限定的であり，調査や発表を指導教授の指示以上の水準で行っている．ゼミ以外にもある程度自主的・積極的に研究に取り組んでいるが，ほかの学生の模範となるほどではない．卒業論文では，正しい記述力や論理力を基盤として，研究の背景・目的・手段・特徴・評価考察などについて自らの考えを整然と述べている．発表では自らの研究の背景・目的・手段・特徴・評価考察などを正しく発表し，質疑応答も的確に行っている．全体を通じて良好な研究活動であり，卓越とはいえないものの，ほかの学生に対してこの程度は行って欲しいという基準になり得る．

・**B（75 点）**…自主的行動

ゼミにおおむね出席し，調査や発表を指導教授の指示と同などかそれ以上の水準で行っている．ゼミ以外の研究は自主性が見ら

（注 11）：https://www.ocha.ac.jp/event/20221222.html
（注 12）：https://www.hs.chuo-u.ac.jp/school/sc-education/sc-science/sc-ssh/
（注 13）：https://uwajimasuisan-h.esnet.ed.jp/sph1

れるが，指示内容を大きく超えるものではない．卒業論文では，研究の背景・目的・手段・特徴・評価考察などを正しく述べ，かつ，自らの考えを論理的に記している．発表では自らの研究の背景・目的・手段・特徴・評価考察などを正しく述べ，質疑応答もおおむね的確に行っている．

・**C（65点）**…指示待ち行動

ゼミにおおむね出席し，調査や発表を質・量ともに指導教授の指示をおおむね守って行っている．また，ゼミ以外の研究を指示された程度に行っている．卒業論文では，必要最小限の研究の背景・目的・手段・特徴・評価考察などについて通常の記述力・論理力で記している．発表では自らの研究背景・目的・手段・特徴・評価考察などを一通り述べているが，それほど明確・論理的ではなく，かつ，質疑応答への対応も的確さに若干欠ける．全体を通じて，指示された範囲を超えない研究活動であり，ほかの学生への開示はすべきではない．

・**不合格**…問題行動

ゼミの欠席が多く，欠席理由も判然としない．ゼミでの調査・発表やゼミ以外での研究活動では指導教授の指示を守れず，結果としてほかの学生に悪影響を与えかねない．卒業論文では，求められている内容の量（研究の背景・目的・手段・特徴・評価考察など）と質を満たせず，発表や質疑応答では的確さに大いに欠ける．全体を通じて低調あるいは誤りが多い研究活動である．

このルーブリックを用いることにより，「卓越」と指導教員が判断し，他教員に説明可能な状況の学生がS判定となる．教員団の申し合わせにより，S，C，及び不合格判定の場合には必ずその根拠を記し，教員団が相互閲覧する．また，標準的なA，B判定の根拠記載は教員の負荷軽減も意図して任意としている．ルーブリック導入と評価の厳格化・客観化推進により，所属研究室による成績の揺らぎが縮小したと認識している．このルーブリックを用いた卒業研究の評価については，2023年度から理工学部全10学科で実施する予定であり，学習成果の保証と可視化の更なる強化・高度化につながることを期待している．

7. むすび

筆者が「国際的に通用するエンジニア教育」に関する電子情報通信学会の委員会に参画してからおよそ四半世紀，段階別コンピテンシーを中央大学で取り組み始めてからおよそ15年が経過した．このような取り組みを始め，継続する大きな契機となったのは，2003年4月に見学した，イリノイ大学シカゴ校工学部のEngineering Expoである．当時，米国の大学工学部のキャップストーン科目は日本のような個人単位で行う卒業研究ではなく，チームプロジェクトのSenior Designであることを聞いていた．その時期に1年間の在外研究期間を獲得し，Senior Designの最終回として開催された当該行事を渡米直後に見学する機会を得た．彼らが取り組んでいたプロジェクトの内容は新規性・独創性が重視される研究というよりは，合理性・有用性（費用対効果も含む）が重視される実際の問題に対する解決手段の考案・実装であった．何より印象的だったのは，審査員に教員だけでなく地域産業界の方も加わっていたこと，発表学生の友人や家族も見学に訪れていたこと，発表学生がとても楽しそうだったこと，である．この経験から，卒業研究にはよい面があるのでそのままにするにしても，自身の学科でも学んだ知識や技術を統合する内容のチームプロジェクト科目を設けられないか，最後の発表会は楽しくできないか，何よりも履修学生が目を輝かせて取り組んで充実感・達成感を味わうようにできないか，この科目の履修体験を通じて卒業研究やその後の大学院での研究行動が高水準になってくれないか，を考えるようになったと，今から振り返ると思う．

外部による高等教育機関の学習・教育成果の点検は，内部関係者（教職員）による自己点検が前提であり，その自己点検は不断の教育改善と不可分と考える．当然思惑どおりに進まないことが多く，また，必ずどこかが異なる学生の学びの成果を仕組みとして引き出すことは難しく，教員自身の納得感はなかなか得られにくい．それでも，学んだ学生が面白かった，役に立ったと感想を述べてくれれば，教員は喜びを感じられるし，彼らを受け入れる社会にもプラスに働くであろう．結局のところは，自身の納得感・充実感を得ることが継続の大きな動機ではないかと，改めて思う次第である．

この場を借りて，筆者を高等教育の質保証に関する取り組みに誘い，様々な段階でご支援・ご助言頂いた学内外・国内外の多くの方々に深謝する．

文　献

(1) 文部科学省中央教育審議会大学分科会質保証システム部会，“「新たな時代を見据えた質保証システムの改善・充実について」（審議まとめ），”2022.3.18. https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/1411360_00012.html

(2) 文部科学省中央教育審議会，“「学士課程教育の構築に向けて」（答申），”2008.12.24. https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/1217067.htm

(3) 牧野光則，篠田庄司，“JABEEに認定申請するためにはどうしたらよいのか―学部における技術者教育システムの改善と発展のために―，”信学誌，vol. 85, no. 12, pp. 877-895, 2002.

(4) 篠田庄司，“JABEEにおける最新の動き―いま何が問題となっているか？―，”信学誌，vol. 87, no. 12, pp. 1077-1094, 2004.

(5) 篠田庄司，“APCからのメッセージ　工学系の学部教育と修士課程教育の教育プログラム認定の動向，”信学誌，vol. 89, no. 7, pp. 619-620, 2006.

(6) 篠田庄司，“未来の社会を託すことができる「工学とその応用に携わる人材」の育成，”信学誌，vol. 90, no. 9, pp. 718-720, 2007.

(7) 篠田庄司，“ABETの認定制度との比較で，JABEEの認定制度の理解を深める，”信学誌，vol. 90, no. 10, pp. 908-922, 2007.

(8) 篠田庄司，“工学教育の未来に向けての変化，”信学FR誌，vol. 2, no. 3, pp. 4-18, 2009. https://doi. org/10.1587/essfr. 2.3_4

(9) L.R. Lattuca, P.T. Terenzini, and J.F. Volkwein, “Engineering change-A study of the impact of EC2000,” ABET, 2006. https://www.abet.org/wp-content/uploads/2015/04/EngineeringChange-executive-summary.pdf

(10) 大学設置基準第21条（単位），2022年10月1日施行. https://elaws.e-gov.go.jp/document? lawid=331M50000080028#Mp-At_21

(11) International Engineering Alliance, “Graduate Attributes & Professional Competencies,” 2021.6.21. https://jabee.org/doc/IEA-Graduate-Attributes-and-Professional-Competencies-2021.1-Sept-2021.pdf

(12) 国際エンジニアリング連合（IEA）（著），岸本，深堀，小尾，

山本，牧野，高橋，津田，佐々木，小林，横井（共訳），“修了生としての知識・能力と専門職としてのコンピテンシー，”2021．https://jabee.org/doc/IEA-GAPC20220325r1.pdf
(13) 文部科学省第 11 期技術士分科会制度検討特別委員会（第 2 回）議事要旨，2022.2.7．https://www.mext.go.jp/b_menu/shingi/gijyutu/gijyutu7/023/gijiroku/mext_00002.html
(14) 文部科学省中央教育審議会教育課程部会，“次期学習指導要領等に向けたこれまでの審議のまとめ補足資料（2），”2016.8.26．https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo3/004/gaiyou/1377051.htm
(15) OECD, “The future of education and skills—Education 2030,” 2018．https://www.oecd.org/education/2030/E2030%20Position%20Paper%20(05.04.2018).pdf
(16) OECD（著），文部科学省初等中等教育局教育課程課教育課程企画室（訳），“教育とスキルの未来：Education 2030【仮訳（案）】，”2018．https://www.oecd.org/education/2030-project/about/documents/OECD-Education-2030-Position-Paper_Japanese.pdf
(17) 文部科学省中央教育審議会，“学士課程教育の構築に向けて（答 申），”2008.12.24．https://www.mext.go.jp/b_menu/shingi/chukyo/chukyo0/toushin/1217067.htm

（2023 年 3 月 7 日受付，2023 年 4 月 6 日再受付）

付録：中央大学段階別コンピテンシー定義一覧

「中央大学コンピテンシー定義一覧」（https://www.chuo-u.ac.jp/gp/competency_pro/competency/definition/）掲載情報に情報工学科専門性，及び，カテゴリの段階別行動例を追加したもの．

コミュニケーション力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
コミュニケーション力	定義	他人の意見あるいは記述された文章を正しく理解したうえで，それに対する自分の意見を明確に表現する．効果的な説明方法や手段を用いて，関係者を納得させる					
	行動例	相手を理解し，相手に自分の意見を伝えることができない	相手の意見を一通り理解し，相手に自分の意見を一通り伝えている	相手の意見を聞き，自分の意見を伝えることで円滑なコミュニケーションを図っている	相手を理解したうえで，説明の方法を工夫しながら，自分の意見や考えをわかりやすく伝え，十分な理解を得ている	様々な説明の方法や手段を駆使し，意見の異なる相手との相互理解を得ている	未定義（独創的行動に加えて，多様性に配慮した行動）
	傾聴力	他人の意見を聞き，正しく理解し，尊重する					
		意見を聞き，理解することができていない	相手の意見を一通り理解している	相手の意見を十分理解している	相手の意見を十分理解し，自分と異なる意見にも耳を傾けている	相手の意見を十分理解し，自分と異なる意見にも耳を傾け尊重している	相手の意見を十分理解し，背景の多様性（文化・習慣・価値観等）に起因する多くの意見にも耳を傾け尊重している
	読解力	記述された内容を正しく理解する					
		記述された内容を理解できていない	記述された内容を理解しようとしている	記述された内容を十分理解している	記述された内容を十分理解した上で，記述されていない内容があることを考慮し，真意をある程度理解している	記述された内容，記述されていない内容を含めて真意を十分理解している	述された内容の真意を，背景の多様性（文化・習慣・価値観等）に起因する記述されていない内容を含めて，十分理解している
	記述力	正しい文章で他人が理解できるように記述する					
		記述された文章を他人が理解できない，あるいは，記述された文章に重大な誤りがある	正しい文章で，他人が一通り理解できるよう記述することができる	正しい文章で，他人が十分理解できるよう記述することができる	正しい文章で，他人が十分理解できる記述となるよう工夫をしている	正しい文章で，他人が十分理解できる記述となるよう秀でた工夫をしている	正しい文章で，背景の多様性（文化・習慣・価値観等）に起因して異なる意見を持つ他者でも十分理解できる記述となるよう秀でた工夫をしている
	提案力	適切な手順・手段を用いてわかりやすく説明したうえで，自分の意見を効果的に伝える					
		効果的な手順・手段を用いてわかりやすく説明できない	効果的な手順・手段を用いてわかりやすく説明しようとしている	効果的な手順・手段を用いてわかりやすく説明できている	適切な手順・手段を用いてわかりやすく説明したうえで，自分の意見を効果的に伝えている	適切な手順・手段を用いてわかりやすく説明したうえで，自分の意見を効果的に伝え，自分と異なる意見を持つ相手からも十分な理解を得ている	適切な手順・手段を用いてわかりやすく説明したうえで，自分の意見を効果的に伝えることで，多様な背景に起因して異なる意見を持つ相手からも十分な理解を得ている
	議論力	議論の目標を設定し，それに合わせて議論を展開する					
		一方的な主張に終わっている．あるいは意見を述べていない，誤った意見のために議論にならない	議論の目標を設定し，それに合わせて議論を展開しようとしている	議論の目標を設定し，それに合わせて議論を展開している	議論の目標を設定し，それに合わせて，自分と異なる意見を持つ相手とも議論を展開している	議論の目標を設定し，それに合わせて，自分と異なる意見を持つ相手とも議論を展開し相互理解を得ている	議論の目標を設定し，それに合わせて，背景の多様性（文化・習慣・価値観等）に起因して異なる意見を持つ相手とも議論を展開し相互理解を得ている

問題解決力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
問題解決力	定義	課題を正しく理解する．解決策を立て実行する．その結果を検証し，計画の見直しや次の計画への反映を行う					
	行動例	与えられた課題を正しく理解できない	与えられた課題を正しく理解し，解決を行おうとしている	自ら発見した課題，もしくは与えられた課題を正しく理解している．解決策を立て，実行している	自ら課題を発見し，解決策を立て，実行している．実行結果は検証し，計画の見直しや次の計画に反映している	記述された内容を十分理解している	未定義（独創的行動に加えて，多様性に配慮した行動）
	課題発見	現状と目標（あるべき姿）を把握し，その間にあるギャップの中から，解決すべき課題を見つけ出す					
		与えられた課題を正しく理解できない	与えられた課題を正しく理解できている	現状と目標を把握し，その間にあるギャップの中に問題を見つけている	現状と目標を把握し，その間にあるギャップの中から，解決すべき課題を見つけ出している	現状と目標を把握し，その間にあるギャップの中から，解決すべき課題を見つけ出し優先順位付けができている	絶えず変化し多様性を増す環境の中で現状と目標を把握し，その間にあるギャップの中から，随時解決すべき課題を見つけ出し優先順位付けができている
	課題分析	課題の因果関係を理解し，真の原因（本質）を見出す					
		課題の因果関係や本質を理解できない，または，見出せない	課題の因果関係や本質を理解しようと見出す努力をしている	課題の因果関係を理解し，そこから本質を見出そうと努力している	課題の因果関係を理解し，本質を見出している	課題の因果関係を理解し，かつ，本質を見出した上で，解決の方向性を認識している	絶えず変化し多様性を増す環境の中で課題の因果関係を理解し，かつ，本質を見出した上で，解決の方向性を随時認識している
	論理的思考	複雑な事象の本質を整理し，構造化（誰が見てもわかりやすく）できる．論理的に自分の意見や手順を構築・展開できる					
		複雑な事象を整理し，構造化できない	複雑な事象を整理し，構造化しようと努力している	複雑な事象を整理し，構造化できる	複雑な事象を整理し，構造化できる．自分の意見や手順を論理的に展開できる	複雑な事象を整理し，構造化できる．意見や手順を論理的に展開し，相手を納得させることができる	絶えず変化し多様性を増す環境の中で複雑な事象を整理し，随時構造化できる．意見や手順を論理的に展開し，相手を納得させることができる
	計画実行	目的と目標を設定し，順序立てて計画して確実に実行する					
		場当たり的な行動をしている	目的と目標を設定し，計画を立ててているが，計画倒れで実行イメージが伴わない	目的と目標を設定し，計画を立ててそれを実行している	目的と目標を設定し，計画を立て，その計画通りに実行している	目的と目標を設定し，複数の方法から最善の方法を選択し，計画を立て実行している	絶えず変化し多様性を増す環境の中で目的と目標を設定し，複数の方法から最善の方法を随時選択し，計画を立て実行している
	検証	計画して実行した結果を正しく評価し，計画の見直しや次期計画への反映を行う					
		結果を検証していない	結果を一通り検証している	結果を正しく評価している	結果を正しく評価し，計画の見直しや次期計画への反映を行なっている	結果を正しく多面的に評価し，計画の見直しや次期計画への反映を行なっている	絶えず変化し多様性を増す環境の中で結果を正しく多面的に評価し，計画の見直しや次期計画への反映を随時行なっている

知識獲得力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
知識獲得力	定義	継続的に深く広く情報収集に努め，取捨選択した上で，知識やノウハウを習得し，関連付けて活用する					
	行動例	自ら情報収集し，新しい知識やノウハウを習得することができていない	一通り情報収集し，新しい知識やノウハウを習得することができている	収集した情報を精査し，知識やノウハウを習得し，関連付けて活用している	深く広く情報収集に努め，取捨選択した上で，知識やノウハウを習得し，関連付けて活用している	継続的に深く広く情報収集に努め，取捨選択した上で，知識やノウハウを習得し，関連付け他者が思いつかない形で活用している	未定義（独創的行動に加えて，多様性に配慮した行動）
	学習	専門知識のみならず自然科学および人文社会科学に関するものも含めて，幅広い分野で知識やノウハウを深く習得することを継続する					
		自ら新しい知識やノウハウを習得できていない	限定的な知識やノウハウの習得に留まっている	自ら新しい知識やノウハウの習得に努めている	専門知識のみならず人文社会に関するものも含めて，幅広い分野で，深く知識やノウハウを習得している	専門知識のみならず，人文社会に関するものも含めて幅広い分野で，知識やノウハウを深く習得することを継続している	絶えず変化し多様性を増す環境の中で専門知識のみならず，自然科学および人文社会科学に関するものも含めて幅広い分野で，知識やノウハウを深く習得することを継続している
	応用力	入手した知識やノウハウを関連付けて活用する					
		入手した知識やノウハウが関連付けられていない	入手した情報や知識やノウハウが一通り関連付けられている	入手した知識やノウハウを関連付けて活用している	入手した知識やノウハウを関連付け，自ら工夫して活用している	入手した知識やノウハウを関連付け，他者が思いつかない形で活用している	絶えず変化し多様性を増す環境の中で入手した知識やノウハウを関連付け，他者が思いつかない形で随時活用している
	情報収集力	必要な情報を入手し，精査した上で，取捨選択して自分のものとする					
		必要な情報が入手できない	通り一遍の情報入手に留まっている	情報を入手し，精査している	工夫して情報を入手し精査した上で，取捨選択して自分のものとしている	様々な手段を駆使し，情報を入手している．信頼性が高い情報のみを選択して自分のものとしている	絶えず変化し多様性を増す環境の中で様々な手段を駆使し，情報を入手している．信頼性が高い情報のみを選択して自分のものとしている

組織的行動能力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
組織的行動能力	定義	チーム，組織の目標を達成するために何をすべきか，複数の視点から多面的，客観的に捉え，適切な判断を下し，当事者意識をもって行動する．その際，他者とお互いの考えを尊重し，信頼関係を築いてそれを維持しつつ行動する					
	行動例	チームで作業ができない，自己中心的な行動をとる	指示されると作業できるが，目標を達成するために自ら動かない	チームでの作業，行動において共通の目標を理解し，達成するために当事者意識を持って行動する	チーム，組織の目標を達成するために何をすべきか，複数の視点から多面的，客観的に捉え，適切な判断を下し，当事者意識をもって行動する．その際，他者とお互いの意見を尊重し，信頼関係を築くような行動をとる	チーム，組織の目標を達成するために何をすべきか，関係者の利害を幅広く考慮したうえで適切な判断を下し，自ら進んで行動を起こすだけでなく，目指すべき方向性を示し，他を導いている	未定義（独創的行動に加えて，多様性に配慮した行動）
	バランス力	複数の視点から，多面的，客観的に物事を捉えた適切な判断を基に行動する					
		視野が狭く，周りが見えない．偏った考え方をする	事実に基づいた視点で客観的に物事を捉えている	複数の視点から多面的，客観的に物事を捉えている	複数の視点から多面的，客観的に物事を捉えた適切な判断を基に行動している	複数の視点から多面的，客観的に物事を捉え，影響範囲や関係者の利害を幅広く考慮したうえで適切な判断を下し，それを基に行動している	多様性（文化・習慣・価値観等）を有する集団の中で複数の視点から多面的，客観的的に物事を捉え，影響範囲や関係者の利害を幅広く考慮したうえで適切な判断を下し，それを基に行動している
	役割認識	チーム，組織の目標を達成するために個人の役割を理解し，当事者意識を持って行動する					
		自分の役割を認識していない	自分の役割を認識しているが，行動に移せない	個人の役割を理解し，当事者意識を持って行動している	個人の役割を理解し，当事者意識を持って行動する．また状況によって役割を柔軟に変え行動する	基本的な役割を理解したうえで行動する．また状況ごとに役割を柔軟に変え，役割を超えた働きをする	多様性（文化・習慣・価値観等）を有する集団の中で基本的な役割を理解したうえで行動する．また状況ごとに役割を柔軟に変え，役割を超えた働きをする
	主体性	物事に対して自分の意志・判断で責任を持って行動する					
		誰かに指示されてもやらない，できない	誰かに指示されたことのみ行っている	何も言われなくても行動は起こすが，単なるマニュアル的行動をとる	物事に対して自分の意志・判断で責任を持って行動している	物事に対して自分の意志・判断で責任を持って行動し，その行動に工夫・独自性が見える	多様性（文化・習慣・価値観等）を有する集団の中で物事に対して自分の意志・判断で責任を持って行動し，その行動に工夫・独自性が見える
	協働	共通の目標を達成するためにお互いの考えを尊重し，信頼関係を築くような行動をとる					
		チームで作業ができない，自己中心的な行動をする	チームで作業できるが，目標を達成するために自ら動かない	チームでの作業，行動において共通の目標を理解し達成するため行動できる	チームでの作業，行動をするとき，共通の目標を達成するためにお互いの考えを尊重し，信頼関係を築くような行動をとる	チームでの作業，行動をするとき，共通の目標を達成するためにお互いを尊重し，信頼関係を構築・維持しようと自ら工夫して行動する	多様性（文化・習慣・価値観等）を有する集団の中で作業，行動をするとき，共通の目標を達成するためにお互いを尊重し，信頼関係を構築・維持しようと自ら工夫して行動する
	率先力	先に立って実践する．先に立って模範を示し，他を誘導する					
		行動しない	他者に従って，あるいは真似をして行動している	先に立って実践している	先に立って実践している．先に立って模範を示し，他を誘導している	先に立って実践している．先に立って模範を示し，他を誘導している．さらに目指すべき方向性を示し，他を導いている	多様性（文化・習慣・価値観等）を有する集団の中で先に立って実践している．先に立って模範を示し，他を誘導している．さらに目指すべき方向性を示し，他を活かしつつ導いている

創造力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
創造力	定義	知的好奇心を発揮して様々な専門内外のことに関心を持ち，それらから着想を得て今までになかった新しいアイディアを発想する．その際，関連法令を遵守し，倫理観を持って社会に対して負っている責任を果たす					
	行動例	新しい発想や技術を知っても興味を持たない	普段から自分が興味のある分野について情報収集し，新しい発想や技術に関心を払っている	自分の専門内外に関わらず幅広い知的好奇心を持ち新たな知識を意欲的に取り入れ，物事に取り組もうとする	知的好奇心を発揮して様々な専門内外のことに関心をもち，それらから着想を得て今までになかった新しいアイディアを発想することができる．その際，関連法令を遵守し，倫理観を持って技術者が社会に対して負っている責任を果たす	知的好奇心を発揮して様々な専門内外のことに関心をもち，それらから着想を得て科学技術の発達に貢献するような独自のアイディアを発想することができる.その際，関連法令を遵守し，倫理観を持って技術者が社会に対して負っている責任を果たす	未定義（独創的行動に加えて，多様性に配慮した行動）
	発想する力	既存の枠にとらわれず，今までに無かった新しいアイディアを生み出す					
		新しい考え方を持とうとしない	ヒントを与えられた場合，新しい考え方で物事にとり組む	自分で適切なデータを収集・参照し，新しい考え方で物事に取り組む	経験したことがないことでも既存の枠にとらわれず，今までに無かった新しいアイディアを生み出すことができる	これからの技術に示唆を与え科学技術の発達に貢献するような，独自のアイディアを生み出すことができる	絶えず変化し多様性を増す環境の中で，これからの社会に示唆を与え貢献するような，独自のアイディアを生み出すことができる
	推論する力	経験のないことや将来起こりうることを推し量る					
		経験のないことや将来起こりうることを推し量ることができない	既知の事柄をもとにして経験のないことや将来起こりうることを推し量ろうとする	既知の事柄をもとにして経験のないことや将来起こりうることを推し量る	前例のないことについて将来起こりうることを推し量る	前例のないことについて将来起こりうることを複数通り推し量る	絶えず変化し多様性を増す環境の中で，前例のないことであっても将来起こりうることを複数通り推し量る
	感動する力	すぐれた芸術や技術，あるいは斬新なアイディアに接して強い印象を受け，新たな取り組みの原動力とする					
		すぐれた技術や芸術，あるいは斬新なアイディアに興味を持たない	すぐれた技術や芸術，あるいは斬新なアイディアに興味を持つ	すぐれた技術や芸術，あるいは斬新なアイディアに接して強い印象を受け，心を奪われる	すぐれた技術や芸術，あるいは，斬新なアイディアに接して強い印象を受け，新たな取り組みの原動力とする	すぐれた技術や芸術，あるいは，斬新なアイディアに接して強い印象を受け，積極的に新たな取り組みの原動力とする	絶えず変化し多様性を増す環境の中で，すぐれた芸術や技術，あるいは，斬新なアイディアに接して強い印象を受け,積極的に新たな取り組みの原動力とする
	探究する意欲	旺盛な知的好奇心を持ち，専門であるなしに関わらず，未知の知識を取り入れようとする					
		新たな知識を得ようという姿勢を持たない	普段から自分が興味のある分野について情報収集の努力をしている	自分の専門内外に関わらず幅広い知的好奇心を持ち，新たな知識を取り入れようと，一部は実際に行動している	自分の専門内外に関わらず幅広い知的好奇心を持ち，新たな知識を意欲的に取り入れようと，実際に行動している	自分の専門内外に関わらず幅広い知的好奇心を持ち，新たな知識を意欲的に取り入れようと，積極的に行動している	変化する環境，多様な環境の中で，自分の専門内外に関わらず幅広い知的好奇心を持ち，新たな知識を意欲的に取り入れようと，積極的に行動している
	倫理	関連法令遵守.自らの取り組みや仕事が社会や自然に及ぼす影響や効果を理解し,社会に対して負っている責任を果たす					
		関連法令を理解していない	関連法令を理解して遵守している	関連法令を理解して遵守している．技術が社会や自然に及ぼす影響や効果を理解し，技術者が社会に対して負っている責任を認識している	関連法令を理解して遵守している．技術が社会や自然に及ぼす影響や効果を理解し，技術者が社会に対して負っている責任を認識し，一部は実際に行動している	関連法令を理解して遵守している．技術が社会や自然に及ぼす影響や効果を理解し，技術者が社会に対して負っている責任を認識し，その責任を果たす	関係する国・地域の法令や国際法を理解して遵守している．絶えず変化し多様性を増す環境の中で，自らの取り組みや仕事が社会や自然に及ぼす影響や効果を理解し，社会に対して負っている責任を認識し,その責任を果たす

自己実現力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
自己実現力	定義	自らを高めるため，常に新しい目標を求め，その実現のために道筋を考え，努力する．その際，自己管理と改善のための工夫を怠らない					
	行動例	目標を見つけようとせず，与えられても達成しようとしない	目標があるとそれを達成したいと思い努力する	自ら明確な目標を定め，その実現のために道筋を考え，努力する．その際，自己管理を怠らない	自らを高めるため，常に新しい目標を求め，その実現のために道筋を考え，努力する．その際，自己管理と改善のための工夫を怠らない	自らを高めるため，常に新しい目標を探しており，見つけるとその達成のために最短の道筋を考えてそれをたどるために努力する．失敗してもあきらめず，繰り返し挑戦する	未定義（独創的行動に加えて，多様性に配慮した行動）
	目標設定	自らを高めるための適切な目標を設定する					
		目標を設定することができない	おぼろげな目標を設定することができる	明確な目標を設定することができる	自らを高めるための適切な目標を設定し，さらにそれを達成するための具体的な指標を設定することができる	継続的に自らを高めるための適切な目標を設定し，さらにそれを達成するための具体的かつ最適な指標を設定することができる	絶えず変化し多様性を増す環境の中でも継続的に自らを高めるための適切な目標を設定し，さらにそれを達成するための具体的かつ最適な指標を設定することができる
	スケジュール管理	目標の実現のために適切な行動計画を立案し，計画遂行のために（メモを取るなどの）スケジュール意識を持って行動する					
		スケジュール意識がない．いつ何をしなければならないかを把握していない	スケジュール意識はあるがメモを取らない．いつ何をしなければならないかを理解しているが一部できない	スケジュール意識があり，メモを取る．行動計画の立案はできるが，突発的な事態に対応できない	行動計画の立案ができ，突発的な事態に対応できる	行動計画の立案ができる．突発的な事態に臨機応変に対応し，必要に応じて適切な対応，調整ができる	絶えず変化し多様性を増す環境の中でも行動計画の立案ができる．突発的な事態に臨機応変に対応し，必要に応じて適切な対応，調整ができる
	自己管理	目標達成のために必要な日常生活の管理（時間管理，衛生管理，健康管理，金銭管理など）を行い，適時的確な行動を取る					
		日常生活の管理を怠っている	日常生活の管理を行っている	日常生活の管理を行っている．定期的に健康診断を受け，普段の生活に生かし体調を崩さないようにする	日常生活の管理を行っている．定期的な健康診断を受け，その結果を踏まえて健康維持のための積極的な取り組みを行っている	日常生活の管理を行っている．定期的な健康診断を受け，その結果を踏まえて健康維持のための積極的な取り組みを継続的に行っている	絶えず変化し多様性を増す環境の中でも生活の管理を行い，発生しうる事態に対応した予防策，対処法を計画し，備えている
	ストレスコントロール	ストレスと上手に付き合い，それによる悪影響を最小に抑える					
		ストレスの解消法を知らず溜め込んでしまう	ストレスが溜まると察知して解消するか，これ以上蓄積しないよう行動する	普段から自分のストレスを意識的にチェックし，自分に合った方法で解消することができる	普段から自分のストレスを意識的にチェックし，自分に合った方法で上手に解消することができる	普段から自分のストレスを意識的にチェックし，自分に合った方法で解消したり低減したりすることができる	絶えず変化し多様性を増す環境の中でも自分のストレスを意識的にチェックし，強いストレスを感じた際も，自分に合った方法で解消したり低減したりすることができる
	達成志向	普段から新しい目標を求めており，自分で設定してそれを達成しようと道筋を立て，努力する．改善のための工夫をする					
		目標が与えられても達成しようと努力しない．最初からあきらめている．すぐにあきらめる	目標が与えられるとそれを達成しようと努力する	普段から新しい目標を求めており，自分で設定してそれを達成しようと努力する	普段から新しい目標を求めており，自分で設定してそれを達成しようと努力する．そのための道筋を立て，改善のための工夫を怠らない	普段から新しい目標を求めており，自分で設定してそれを達成しようと努力する．失敗しても効果的な改善を行い，あきらめず繰り返し挑戦する	絶えず変化し多様性を増す環境の中でも新しい目標を求めており，自分で設定してそれを達成しようと努力する．失敗しても効果的な改善を行い，あきらめず繰り返し挑戦する

多様性創発力

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
多様性創発力	定義	多様性（文化・習慣・価値観等）に適切に対応しつつ，自らの存在感を高め，その協同から，相乗効果を生み出すことで，新たな価値を得る					
	自確力	自らの慣れ親しんだ文化・習慣・価値観等を正しく理解したうえで，自分が何を望むか，かつ，まわりが自分に何を望んでいるのかを判断し，行動する					
		異なる文化・習慣・価値観等に接したときに，自らの慣れ親しんだ文化・習慣・価値観等を意識しない	自らの慣れ親しんだ文化・習慣・価値観等を意識し，理解しようとしている	自らの慣れ親しんだ文化・習慣・価値観等を正しく理解している	自らの慣れ親しんだ文化・習慣・価値観等を正しく理解し，自分が望む行動，あるいはまわりが自分に望む行動をしている	自らの慣れ親しんだ文化・習慣・価値観等を正しく理解したうえで，自分が何を望むか，かつ，まわりが自分に何を望んでいるのかを判断し，行動している	自らの慣れ親しんだ文化・習慣・価値観等を正しく理解したうえで，自分が何を望むか，かつ，まわりが自分に何を望んでいるのかを判断し，行動することで存在感を高めている
	融合力	異なる文化・習慣・価値観等の相互理解を得て適切に対応し，互いに学び続けている					
		異なる文化・習慣・価値観等の存在を意識していない	異なる文化・習慣・価値観等の存在を意識し，理解しようとしている	異なる文化・習慣・価値観等を理解し，受け入れている	異なる文化・習慣・価値観等を理解し，受け入れるとともに，自らの慣れ親しんだ文化・習慣・価値観等を伝えている	異なる文化・習慣・価値観等の相互理解を得て適切に対応している	異なる文化・習慣・価値観等の相互理解を得て，適切に対応し，互いに学び続けている
	協創力	多様性（文化・習慣・価値観等）がある複数人の協同により，相乗効果を生み出すことで，新たな価値を得る					
		多様性（文化・習慣・価値観等）がある複数人の協同にもかかわらず，むしろマイナスの成果となっている	多様性（文化・習慣・価値観等）がある複数人の協同にもかかわらず成果が得られない	多様性（文化・習慣・価値観等）がある複数人の協同により，人数相応の成果は得られていないが，一定の成果がある	多様性（文化・習慣・価値観等）がある複数人の協同により，人数相応の成果を得ている	多様性（文化・習慣・価値観等）がある複数人の協同により，相乗効果を生み出している	多様性（文化・習慣・価値観等）がある複数人の協同により，相乗効果を生み出すことで，新たな価値を得ている

情報工学科専門性

カテゴリー キーワード		段階					
		問題行動	指示待ち行動	通常行動	自主的行動	独創的行動	創発的行動
専門性／情報工学科	定義	広さと深さがある知識と経験をもとに，プログラミングやICTツールを適切に用いて，精確に作業を進め，情報工学を活用する					
	行動例	情報工学を学ぶために基盤となる学力や知識を持っていない．あるいは知識に誤りがある	断片的な専門知識や学力を有し，簡単な情報の理解と正確性の判断をして小規模な主張を行うことができるが，作業の緻密さや正確さは不十分である	専門知識を概ね理解し，それに関連する情報の理解と正確性の判断をして自らの主張を行うことができる．一定基準の緻密さや正確さをもった作業を行うことができる	専門知識を体系的に理解し，専門性の高い情報の理解と正確性の判断をして自らの主張を行うことができる．一定基準以上の緻密さや正確さをもった作業を行うことができる	非常に高度な専門知識を有し，専門知識人対象レベルの情報の理解と正確性の判断をして自らの主張を国内外に発信できる．秀でた工夫により一定基準以上の正確さや緻密さをもった作業を行うことができる	未定義（独創的行動に加えて，多様性に配慮した行動）
	基盤となる学力	語学，歴史，文化，法令，環境などを含む幅広い分野に関心を持つと共に知識を有し，それらを含む論述を理解し，必要に応じて利用する					
		情報工学の基礎や数学・自然科学を学ぶために必要な基盤となる学力を有していない．あるいは必要な場面で利用することができない	専門内外の分野における他者の論述内容の正誤や根拠を自らの知識や経験をもとに断片的に確認できる．かつ，規模の小さい自らの主張を知識や経験をもとに口頭または文章を用いて母国語で行うことができる	幅広い分野において，他者の論述内容や専門知識に関する母国語または外国語による論述内容の正誤や根拠を知識や経験をもとに一通り確認できる．自らのまとまった主張を口頭または文章を用いて母国語で行うことができる	幅広い分野において，他者の論述内容や専門知識に関する母国語または外国語による論述内容の正誤や根拠を知識や経験をもとに適切に確認できる．自らのまとまった主張を口頭または文章を用いて母国語または外国語で行うことができる	幅広い分野において，他者の論述内容や専門知識に関する母国語または外国語による論述内容の正誤や根拠を知識や経験をもとに適切に確認できる．自らのまとまった主張を口頭または文章を用いて母国語かつ外国語で効果的に行うことができる	未定義（独創的行動に加えて，多様性に配慮した行動）
	数学・自然科学	数学・自然科学に関して深く広い知識を有し，その内容を理解の上，必要に応じて利用する					
		情報工学の基礎を学ぶために必要な数学・自然科学に関する知識を有していない	情報工学の基礎としての数学・自然科学の知識を断片的に有している	情報工学の基礎としての数学・自然科学の知識を概ね理解し，専門知識の獲得に役立てることができる	情報工学の基礎としての数学・自然科学の知識を理解し，専門知識の獲得に効果的に役立てることができる	情報工学の基礎としての数学・自然科学の知識を理解し，これを駆使して高度な専門知識の効果的な獲得に役立てることができる	未定義（独創的行動に加えて，多様性に配慮した行動）
	情報技術基礎	自らの考えを実現するために適切にプログラムを作成，またはICTツールを利用する					
		与えられた手順をプログラミングできない，または，誤ったプログラムを作成し，修正できない．あるいは，ICTツールを誤用する，または，利用方法を知らない	プログラム言語の基本文法を断片的に理解し，主要文法の一つまたは少数による単純なプログラムを作成できる．かつ，他者の助力を得て必要なICTツールを利用できる	プログラム言語の基本文法を概ね理解し，課題に対して正しい手順（定式化，アルゴリズム構築，プログラム作成，実行，検証と必要な修正）に従ってプログラムを作成できる．かつ，必要なICTツールを自力で利用できる	プログラム言語の基本文法を体系的に理解し，課題に対して正しい手順（定式化，アルゴリズム構築，プログラム作成，実行，検証と必要な修正）に従って効率的・効果的なプログラムを工夫して作成できる．加えて，必要なICTツールを利用して効率的・効果的に作業ができる	プログラム言語の基本文法を体系的に理解し，課題に対して正しい手順（定式化，アルゴリズム構築，プログラム作成，実行，検証と必要な修正）に従って効率的・効果的なプログラムを秀でた工夫で作成できる．加えて，必要なICTツールを利用して効率的・効果的に作業ができる	未定義（独創的行動に加えて，多様性に配慮した行動）

専門知識	情報工学に関する知識を有し，その内容を理解し，必要に応じて利用する					
	専門知識を全くまたはほとんど理解していない，あるいは，誤って理解している	専門知識について断片的に理解し，少数の知識を必要とする課題に解答できる	専門知識について概ね理解し，複数の知識を総合して課題に解答できる	専門知識について体系的に理解し，その内容を他者に説明できる	専門知識について体系的にかつ一部については深く理解し，専門職業人と討論できる	未定義（独創的行動に加えて，多様性に配慮した行動）
精確性	一連の作業を緻密かつ正確に実行する					
	一連の作業を緻密かつ正確に行おうという心掛けがなく，雑に作業を行う	一連の作業を緻密かつ正確に行おうという心掛けが十分でなく，行った作業が定められた基準での緻密さ，正確さをもたない	一連の作業を緻密かつ正確に行おうという心掛けがあり，行った作業が定められた基準の緻密さ，正確さをもつ	一連の作業の緻密性または正確性を向上する心掛けをもち，定められた基準以上の緻密さ，精確さで作業を行うことができる	一連の作業の緻密性または正確性を向上する心掛けをもち，秀でた工夫により，定められた基準以上の緻密さ，精確さをもつ作業を行うことができる	未定義（独創的行動に加えて，多様性に配慮した行動）

牧野光則（正員：フェロー）

1987 早大・理工・電子通信卒．2002 同大学院博士後期課程了，博士（工学）．同年中央大学理工学部勤務，専任講師，助教授を経て 2004 年より教授．以来，コンピュータグラフィックスとその応用システム，クロスリアリティ応用システム，非線形システム解析などの研究に従事するとともに，高等教育の質保証に関する取り組みに学内外で従事．1990 篠原記念学術奨励賞，1991 論文賞，2016 教育優秀賞受賞．現在アクレディテーション委員会委員長，JABEE 理事・基準委員長，大学改革支援・学位授与機構高等専門学校機関別認証評価委員，大学監査協会企画委員・教学監査分科会主査．

技術の原点

6G システムにおける非線形最適化技術適用の利点とその課題

Advantages and Challenges of Applying Nonlinear Optimization Techniques in 6G Systems

岡本英二 Eiji OKAMOTO

アブストラクト　第 5 世代移動通信システム（5G）の商用展開が進み，少しずつアプリケーションやユーザの体験も進化している．しかし移動通信では伝搬路変動が生じるため高品質伝送を保証するためには技術の適用が必要である．その技術の一つである線形等化処理を例に挙げながら，5G を支える幾つかの信号処理技術を紹介し，線形・非線形信号処理の特徴を述べる．そして線形，非線形信号処理がそれぞれ計算量削減，システム性能向上に寄与することを示す．更に 5G の標準化動向の特徴を紹介しユースケースが細分化しつつ追加されている状況を述べ，5G の次の世代である 6G のシステムモデリングであるセルフリーシステムの概念を紹介する．そして 6G では通信資源配分の要素数が爆発的に増加し，目的関数も複数化がなされるため，干渉を分離・融合しながら機械学習などを適切に用いて準最適解を迅速に導出し，無線リソースを含むシステム制御を行うことを述べる．これにより，あらゆる用途やエリア，通信様式をカバーするという今後の超ユースケース拡張に対応することが可能となる．

キーワード　第 6 世代移動通信システム，セルフリーシステム，線形フェージング等化，干渉分離融合，超ユースケース拡張

Abstract　The commercial deployment of the fifth-generation mobile communications system (5G) is progressing, and applications and user experiences are gradually evolving. In wireless communications, the technologies must be applied to guarantee high-quality transmission in spite of propagation channel fluctuations. Taking linear equalization as an example, in this paper, several signal processing technologies that support 5G are introduced and the characteristics of linear and nonlinear signal processing methods are described. It is shown that the linear and nonlinear signal processing methods reduce computational complexity and improve system performance, respectively. The characteristics of 5G standardization trends are also introduced, the situations in which use cases of use are subdivided and added are described, and the concept of cell-free systems, which is the system model of 6G, the next generation of 5G, is presented. In 6G, the number of elements in communication resources allocation will increase exponentially, and multiple objective functions will also arise. We describe how to quickly derive a quasi-optimal solution using machine learning while separating and integrating interference, and how to control the 6G system, including wireless resources. This makes it possible to accommodate future expansions of super-use cases that cover all applications, areas, and communication styles.

Key words　Sixth-generation mobile communications system, Cell-free system, Linear fading equalization, Interference separation and integration, Super-use case extension

1. まえがき

第 5 世代移動通信システム（5G）の商用化から数年経ち，マイクロ波だけでなくミリ波を用いたエリア展開も進んでいる．現在の商用システムは標準化プロジェクトの Third Generation Partnership Project（3GPP）[(1)]が定めた 5G の初版である release 15 規格[(2)]に基づいているが，Phase 2 とも呼ばれる release 16 規格の商用展開も今後進む予定である．そして大容量化の通信規格・ユースケースだけでなく，超高信頼低遅延と多数同時接続の通信規格に沿ったサービスが身近に提供されるはずである．このような規格の実現を支える無線通信の要求条件は多岐にわたっており，第 4 世代（4G）に比べて 5G の通信性能は 10〜100 倍程度の改善が行われている[(3)]．この改善を支える主要な技術の一つが非線形信号処理であり，現在研究開発が進んでいる Beyond 5G・第 6 世代（6G）もこの延長線上での進化が行われている．

本稿では，まずこの 5G を支える典型的な信号処理技術を紹介し，線形・非線形信号処理の特徴を述べる．具体的には移動通信においてほぼ必ず生じるフェージングの影響[(4)]と，線形等化処理について説明を行い，5G で標準化技術として採用された非直交多元接続手法[(5),(6)]における非線形信号処理による通信路容量増加の効果について述べる．次に 5G の標準化動向の特徴[(7)]を紹介し，ユースケースが細分化されて

岡本英二　正員：フェロー　名古屋工業大学大学院工学研究科工学専攻
E-mail　okamoto@nitech.ac.jp
Eiji OKAMOTO, Fellow Fellow (Graduate School of Engineering, Nagoya Institute of Technology, Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.26-35 2023 年 7 月

追加されている状況を述べる．そして 6G のシステムモデリングの例であるセルフリーシステム[8]の概念を紹介し，最適無線資源配分の要素である端末数が爆発的に増加し，最適化問題の解決に機械学習が活用されようとしている現状を述べる．更に今後の無線通信システムの課題とユースケースの動向について考察を行う．結論として，6G では通信資源配分の要素数が爆発的に増加し，目的関数も複数化がなされるため，干渉を分離・融合しながら機械学習などを適切に用いて準最適解を迅速に導出し，無線リソースを含むシステム制御を行うことが必要であることを説明する．

以下では 2 節において移動通信の伝搬路モデルとその線形等化手法を説明し，3 節で 5G の主要シナリオとユースケースを紹介する．4 節で 5G の非線形信号処理の例を多元接続と屋内測位に関して紹介し，5，6 節でそれぞれ 6G システムの動向と，ユースケースの展開に関する考察を行う．最後に 7 節でまとめを述べる．

2. 移動通信システムの現状とフェージングへの対策

現在移動通信システムは社会のインフラストラクチャとして機能しており，普段の暮らしになくてはならないものとなっている．2022 年 9 月の国内の携帯端末契約数は 2 億 3547 万台[9]であり，1 人当たり 1.89 台程度となる．世界的に見ても 2022 年度において契約台数のおよそ 84 億台[10]に対し世界人口は 80 億人であるため，平均的には 1 人 1 台保有していることになる．ただしこの契約数には人だけでなく，通信装置を備えた自動車や飲料自動販売機などの人以外の端末も含まれており，IoT（Internet of things）時代の到来を踏まえると，装置の台数は今後もますます増加すると予想されている．

このような収容数の増加と通信の高速化を実現するために移動通信システムは約 10 年に一度フルモデルチェンジを行ってシステムの高度化を図っている．国内では 2020 年に 5G の商用化が開始され，5.5 世代と呼ばれることもある 5G-Advanced 規格[7]の策定も標準化プロジェクトにおいて進んでいる．

しかしながら，無線通信では伝搬路変動が常に起こるため，高品質かつ高速な伝送を行うには様々な付加技術の適用が必要である．図 1 に電波伝搬の模式図を示す[4]．電波伝搬は広がりをもつため，基地局から端末への電波は直接波以外にも反射波，回折波，散乱波，山岳反射波などとなり受信される．これらの電波は受信方向と到着時刻，受けるドップラー効果が異なるため，端末で合成した電波は互いに強め合うことも弱めあうこともあり，受信電力が刻々と変化する．この現象をマルチパスフェージングといい，無線通信ではフェージングの影響により受信誤りが時々生じてしまう．

図 2 に伝搬距離に対する受信電力低下の特性を示す．無線通信は伝送媒体が空間であるため，銅線や光ファイバを用いた有線通信と異なり伝搬距離に対する受信電力の減衰が大きい．一般に真空上の平面波の電波伝搬では距離の 2 乗に比例

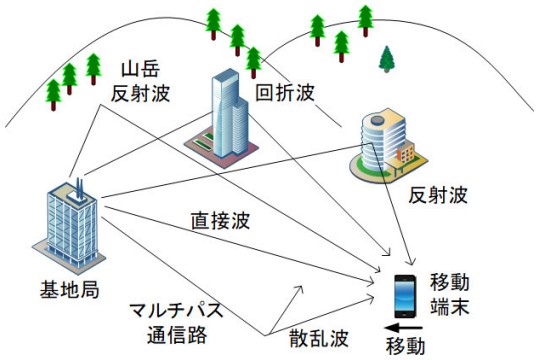


図 1　無線通信における電波伝搬の模式図

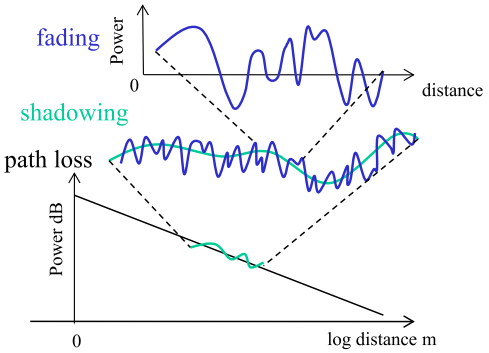


図 2　伝搬距離と受信電力変動の様子

して電力が減衰する．これが距離減衰（path loss）である．例えば 100 m 離れたアンテナ間の電波伝搬では受信電力は 1 万分の 1 に減衰してしまい，受信信号対雑音電力比（signal to noise ratio : SNR）は低下する．更に図のように送受信機間に存在する建物や木々などの遮蔽物によりシャドウイング（shadowing）と呼ばれる不規則な受信電力変動が生じ，加えてマルチパスフェージング（fading）によっても短区間で変動する．このうち距離減衰とシャドウイングは置局の工夫により伝搬の短距離化と送受信機間の見通しを確保することで平均受信電力の向上を図ることが可能であるが，フェージングは回避できない．したがって移動通信では時々受信 SNR の大きな落ち込みが発生することになり，その前提で通信方式を設計する必要がある．

具体的には，対象とするシステムの送受信機間の通信路にどのようなフェージングが発生するかを踏まえて最適な通信方式を選択することが必ず行われている．例えば 3GPP では代表的な通信路モデルの規定もなされており[11]，標準的な都市部や郊外の屋外，屋内などの伝搬路のモデルが規定されている．そしてこのモデルで実際の環境を模擬し，有効な通信方式を設定し標準化技術として採用している．

2.1　システムの通信速度とフェージング影響の関係及び線形等化処理

図3に等価低域系モデル（高周波信号処理が完全であることを仮定し，低域の情報信号のみを複素数で表現するモデル）にて表した場合の送受信信号の関係を示す．図のように送受信関係は

$$r(t)=h(\tau,t)*s(t)+n(t) \quad (1)$$

で表される．ここで t は時間，τ は遅延時間であり，$s(t)$，$r(t)$ はそれぞれ送受信信号，$h(\tau,t)$ は通信路のインパルス応答，$n(t)$ は受信側の雑音である．一般化されたフェージング変動は $h(\tau,t)$ にて表現することができ，遅延時間 τ に対するインパルス応答が時刻 t ごとに連続的に変化する時変フィルタとなる．

図4にある時刻 t における遅延波を伴うマルチパス受信のインパルス応答例を示す．ここでサンプリング間隔 $T_s=10^{-3}$ s とする．図4のような波数 $L=10$ 波の直接波と反射波が遅延を伴い図のように $0\leq\tau\leq(L-1)T_s$ s の間に1 dB減衰しながら受信されたとする．この場合の $h(\tau,t)$ に対応する伝達関数 $H(f)$ の振幅スペクトルは図5のようになり，送信信号 $s(t)$ の周波数スペクトル $S(f)$ の各周波数ごとに電力が増加したり減少したりと異なるひずみを受けることが分かる．

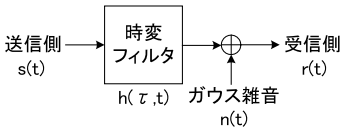


図3　等価低域系モデルにおける送受信信号の関係

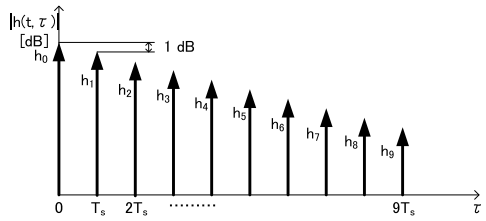


図4　遅延波を伴うマルチパス受信のインパルス応答例

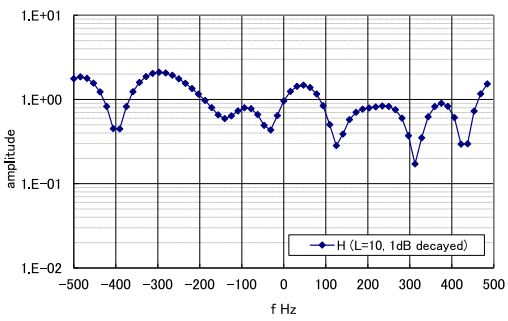


図5　図4の $h(\tau,t)$ に対応する伝達関数 $H(f)$ の振幅スペクトル

このように移動通信では送信信号が通信路でひずみを受けるため，そのまま復号を行うと受信ビット誤り率がほぼ0.5になってしまい，正常な伝送ができなくなる．そのため式(4)(7)で述べる等化処理が受信側で必ず行われる．またフェージングによる変動は，図5のような周波数軸に対して大きく起こる（周波数選択性フェージングという）か，後ほど図7に示すような時間軸方向に強く影響する（時間選択性フェージング）かは通信システムの設計により変わる．

図6(a)にある時刻 t_1 における $h(\tau,t)$ の例を示す．図1のマルチパスは多数であることから実際のインパルス応答は τ に対して連続な信号となる．これをディジタル通信において t 軸方向に標本化を行った場合，1，0のパルス信号を送る間隔 T が4 μsec であるとすると情報伝送速度は250 k bps（bit per sec）となり，260 nsec とすると3.84 Mbps となる．つまり T が短くなると高速情報伝送ができるため，現在の移動通信システムでは一般的には T の値は短くなっている．例えばこのとき等価的なインパルス応答は図6(b)(c)のようになり，式(1)に図6のインパルス応答を適用するとそれぞれ，

低速通信時：$r(k)=s(k)+n(k)$ (2)

高速通信時：$r(k)=h_0s(k)+\sum_{l=1}^{L-1}h_ls(k-lT)+n(k)$ (3)

となる．ここで k はサンプリング後の離散時間であり，h_l は伝搬路の第 l 遅延波の変動係数（チャネル係数）である．つまり図6(b)の低速通信時は一つのパルス信号幅 T が長いため，図1のマルチパス波はほぼ同一時刻に到着するとみなしても問題なくなり第1波めの直接波のみを考慮すればよいが，図6(c)の高速通信時はマルチパス波の遅延時間が T に比べて相対的に大きくなり，式(3)右辺第2項の遅延波の成分が無視できなくなる．逆に各 h_l の時間変動は T が長い低速通信時の方が大きくなり，T が短いときは変化しないとみなしても問題なくなる．すなわち，低速通信時は時間選択性フェージングの影響が大きくなり，h_0 は時間関数となり $h_0(t)$ は図7のように変動する．一方，高速通信時は図5のような周波数選択性フェージングの影響が大きくなるのである．

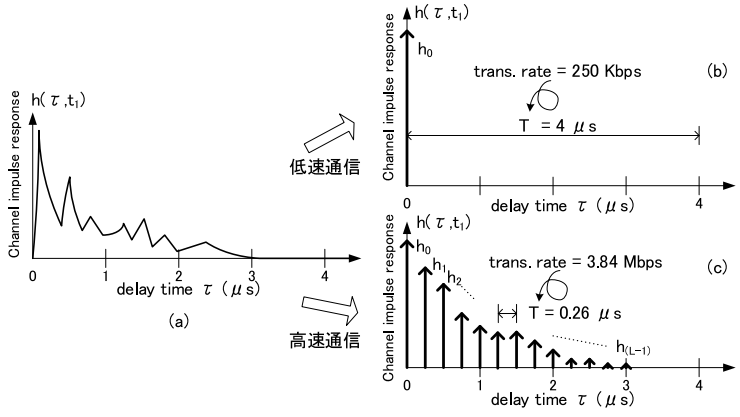


図6　無線通信におけるインパルス応答とその等価チャネル係数　(a)実際のインパルス応答の例，(b)低速通信時の等価チャネル係数（直接波のみのインパルス），(c)高速通信時の等価チャネル係数（遅延波の影響あり）．

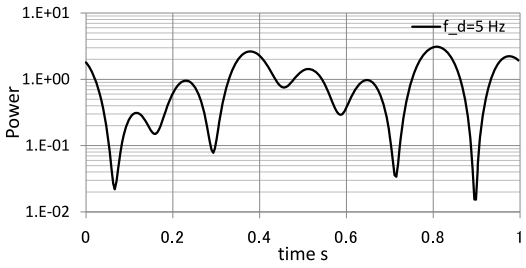


図 7　時間選択性フェージングの例（最大ドップラー周波数 f_d=5 Hz）

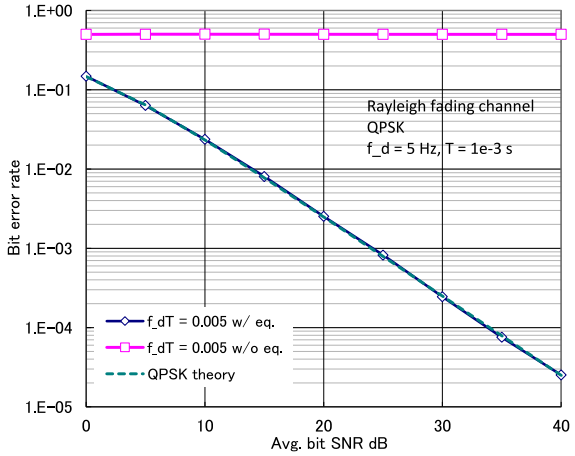


図 8　図 7 の時間選択性フェージングに受信側で等化処理を行った場合と行わない場合のビット誤り率特性

したがって移動通信システムでは設定した T の値，つまり通信速度に沿ったフェージングひずみの影響を取り除く処理を受信側で行ってからビットの復号を行っている．これを「等化」という．この等化処理の原理は，一言でいうと除算によるフェージング成分の除去である．受信機は送信機が定期的に送信する基準信号により h_l を推定することができるため，受信側は h_l を既知であると仮定すると，時間選択性フェージングを受けた式(2)の $r(k)$ に対して

$$\tilde{r}(k)=\frac{r(k)}{h_0}=s(k)+\frac{n(t)}{h_0} \tag{4}$$

と時間領域でチャネル係数を除算すると伝搬路変動成分を除去することができ，雑音の影響は残るが $s(k)$ を取り出すことができる．この場合は時間領域等化といい，信号処理負担の小さい線形演算のみで高品質伝送が実現されることになるため，第 3 世代（3G）までの移動通信システムで採用されていた．

図 8 に，quadrature phase shift keying（QPSK）変調という代表的なディジタル変調方式で伝送を行ったときに，図 7 の最大ドップラー周波数 f_d=5 Hz の時間選択性フェージングを受けた場合に受信側で式(4)の等化処理を行った場合（w/eq.）と行わない場合（w/o eq.）のビット誤り率特性を示す．このように等化を行うと平均 SNR が大きい領域すなわち距離減衰とシャドウイングが問題にならない領域では高品質伝送が行えていることが分かる．しかし等化を行わない場合は誤り率が 0.5 になり，正常な伝送ができない．

一方，高速通信時の式(3)に同じことを行うと，

$$\tilde{r}(k)=s(k)+\frac{1}{h_0}\sum_{l=1}^{L}h_l s(k-lT)+\frac{n(t)}{h_0} \tag{5}$$

となり，右辺第 2 項の h_1 以降の遅延波の干渉成分が除去できず，$s(k)$ が正常に判定できず復号後の品質が劣化してしまう．つまり高速通信では線形演算の時間領域等化が正常に行えなくなるわけである．畳み込み演算を用いて時間領域で $s(k)$ を検出することは可能であるが信号処理負担が大きい．これはバッテリー駆動の携帯端末では望ましくない．そこで式(5)を離散フーリエ変換すると，

$$\begin{aligned}R(n)&=h_0S(n)+\sum_{l=1}^{L}h_lS(n)\exp\left(-j\frac{2\pi nlT}{N}\right)+N(n)\\&=\left[\sum_{l=0}^{L}h_l\exp\left(-j\frac{2\pi nlT}{N}\right)\right]S(n)+N(n)\\&=H(n)S(n)+N(n)\end{aligned} \tag{6}$$

となる．ここで n はサンプリング後の離散周波数であり，$R(n)$，$S(n)$，$N(n)$ はそれぞれ $r(k)$，$s(k)$，$n(k)$ の離散周波数スペクトル，$H(n)$ は伝搬路の伝達関数である．つまり図 5 が各 n の $H(n)$ に相当する．このように遅延波成分も含めた変動が $S(n)$ の係数 $H(n)$ になるため，式(4)と同じように

$$\hat{R}(n)=\frac{R(n)}{H(n)}=S(n)+\frac{N(n)}{H(n)} \tag{7}$$

として線形演算により等化が行える．これを周波数領域等化といい，第 4 世代以降の移動通信システムではこちらの等化処理が採用されている．

以上のように移動通信システムではフェージングのひずみを除去するために受信側の等化処理が必須になっており，全てのスマートフォンに実装されている．しかも基本的には所要計算量を減らすために線形演算により等化を行っている．

3.　5G の主要シナリオとユースケースの細分化

図 9 に国際電気通信連合無線通信部門（International Telecommunication Union Radiocommunication Sector : ITU-R）が発行した IMT ビジョン勧告[3]における三つの主要シナリオと主なユースケースを示す．その一つの enhanced mobile broadband（eMBB）は 4G までに想定されていたシナリオであり，携帯電話・スマートフォンの通信高速化を，速度を保証しないベストエフォート型で提供する通信プロトコルである．5G では eMBB シナリオの進展を実現しており，ピーク伝送速度で 4G の 1 Gbps を 20 Gbps まで高速化している．これにより図にあるように 3D 動画や 4K/8K の高精細動画配信，XR（extended reality）を活用したアプリケーションなどが実現される．そして 5G では新たに massive machine type communications（mMTC）と ultra-reliable and low-latency communications（URLLC）シナリオが追加された．Release 15 の初版 5G では mMTC は 100 万台/km^2 の接続を

収容することが要件であり，主に IoT 端末との超多数接続を実現する通信シナリオである．主なユースケースは図のようにスマートシティ内で広域に分散された IoT 端末や，スマートホームにおける家電機器などの情報収集と制御であり，多数の端末との少量データの比較的低速伝送が想定されている．そして URLLC は，32 バイトのパケットデータを無線区間 1 ms 以下で 99.999% 以上の確率で伝送できることが性能要件であり，高信頼・低遅延伝送を実現するシナリオである．主な適用先としては自動運転・遠隔操作運転のための通信，スマート工場における非配線装置制御，ロボット制御，遠隔医療などが想定されている．

図 9 右下のように URLLC では自動運転をユースケースの一つとしている．セルラを用いた車両向け通信は一般的に Vehicular to Everything（V2X）と呼ばれており，セルラ V2X はこのプロトコルを用いて実現される．5G release 16 では，URLLC シナリオも様々なユースケースに対応するために拡張されており，無線の要求条件と対象ユースケースが多数追加された．表 1 に release 16 における V2X ユースケースと無線要求条件の一部の例を示す[12]．様々なユースケースと無線の要求条件が追加されており，衝突防止，安全情報周知，動画伝送，遠隔操作などの各アプリケーションにより適したきめ細かい無線規格が定められている[13]．

しかし無線通信では前節のマルチパスフェージングの影響により時間・周波数領域で狭域に受信電力が低下してしまい平均受信電力が大きくても誤りが一部で生じてしまうため，無線通信にとって URLLC のように品質を保証することは厳しい要件である．したがって URLLC ではこのフェージングの影響を踏まえつつ高信頼・低遅延通信を実現することになり，種々の高度な技術の適用が必要となっている．

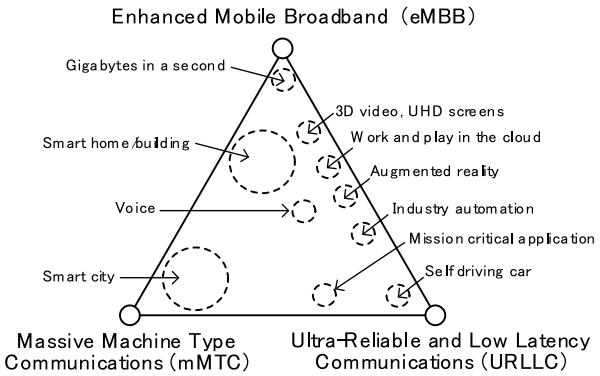


図 9　5G における三つの主要シナリオ[3]

表 1　3GPP Release 16 における V2X ユースケースと無線要求条件の例

ユースケース	パケット長 byte	最大伝送遅延 ms	信頼性 %	伝送速度 Mbps
Cooperative collision avoidance between UEs supporting V2X applications.	2,000	10	99.99	10
Intersection safety information between an RSU and UEs supporting V2X application.	450	規定なし	規定なし	上り：0.25 下り：50
Video sharing between UEs supporting V2X application : Higher degree of automation	規定なし	10	99.99	700
Information exchange between a UE supporting V2X application and a V2X Application Server	規定なし	5	99.999	上り：25 下り：1

4.　非線形信号処理による 5G の性能改善事例

4.1　非直交多元接続手法

2001 年にサービスが開始された 3G ではデータ通信の需要が継続的に増加し，音声通話を上回るデータ量となった．また，様々な機能が携帯端末に搭載されるようになり，データ通信を中心として 3G の規格を上回る大容量化が求められるようになった．そこでパケット交換の高能率な多元接続技術として，直交周波数分割多重伝送（orthogonal frequency division multiplexing : OFDM）の原理を多元接続に用いた直交周波数分割多元接続（orthogonal frequency division multiple access : OFDMA）方式が 4G（正式な規格上は 3.9 世代）において採用され，日本では 2010 年よりサービスが開始された．図 10 にその原理を示す．OFDM の原理を用い各チャネルを同期させることにより，チャネル間干渉を防ぐために挿入される空白であるガードバンドを不要とし，直交配置において理論的に最適である稠密チャネルを配置させることができる．これにより周波数利用効率が向上した．更に，ユーザとチャネルを固定する回線交換ではなくパケット交換であることから，各チャネルを端末–基地局間の伝搬路状況がよいユーザに適応的に切り替えて割り当てることによって，システム全体での容量を増やすことができる．これをマルチユーザダイバーシチ効果という．この手法は直交多元接続手法としては最適であり最も伝送速度が速くなる．この多元接続技術と，複数アンテナ伝送技術（multiple-input multiple output : MIMO）を併用することにより，下りリンクで 100 Mbps 以上の伝送速度を実現している．また，各ユーザ

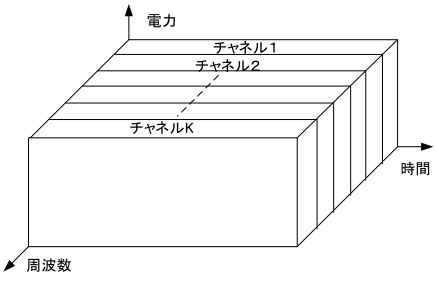


図 10　直交周波数分割多元接続（OFDMA）の原理

のデータは直交しているため，受信側で式(7)の周波数領域線形フェージング等化を独立に適用できる．

しかし更なる高速伝送の実現のために，5G では図 11 の非直交多元接続手法（non-orthogonal multiple access : NOMA）[5,6]が標準化技術として採用された．図のように同一チャネルの電力軸に複数のユーザが割り当てられている．通常ではこれらのユーザは互いに干渉してどちらも品質が劣化する．しかし NOMA では例えば基地局から近傍と遠方などの伝搬路状況の異なる 2 ユーザが対として選ばれ，送信側基地局は遠方ユーザへの信号の電力を大きくして近傍ユーザ信号と重畳し送信する．受信側である基地局近傍のユーザは，近傍＋遠方ユーザの混信した受信信号を受け取るが，このうち遠方ユーザの信号は大きな電力で受信できるため，まずこちらを正しく判定する．その後逐次干渉キャンセル（successive interference cancellation : SIC）と呼ばれる信号処理を施すことで，重畳された干渉を正確に除去でき，自分宛の信号のみを正しく取り出すことができる．一方，遠方ユーザは同じく近傍＋遠方ユーザの混信した受信信号を受け取るが，伝搬路の減衰が大きいため干渉分である近傍ユーザの信号が無視できるほど小さくなり，大電力が割り当てられた自分宛の信号のみを取り出すことができる．この手法により結果的に図 10 より周波数利用効率の高い，より多くのユーザを収容した多元接続が実現された．この手法の原理は eMBB の高速化と mMTC の多数接続の実現に寄与している．

NOMA の具体例として，図 12 のような 5G セルラシステムにおける下りリンク NOMA 伝送について説明する．基地局からユーザ端末（user equipment : UE）への下りリンクにおいて，まず基地局はターゲットセル内のユーザの伝搬路情報（チャネル情報）がフィードバックによって通知される．基地局はその情報に基づき，公平性（proportional fairness : PF）を考慮しつつ各サブバンドと呼ばれる周波数帯域をユーザに割り当てる[14]．この操作を周波数スケジューリングという．その際 NOMA では，干渉を伴うユーザ重複を許しつつ割り当てる．そして全サブバンド割り当て時の平均ユーザ容量を PF 基準において最大化させる．図の例ではサブバンド 1 と 3 においてそれぞれ基地局近傍，遠方の UE1, 4 と UE3, 2 が重畳された割り当てになっている．このとき送信電力に適切な差を設けることにより，OFDMA よりも通信路容量が増加する．

図 13 に NOMA と OFDMA における UE1, 4 の正規化通信路容量比較を示す．ここで UE1 の伝搬路の状態が UE4 の 100 倍良い，すなわちチャネル電力が 100 倍である場合を示している[6]．このように NOMA を用いることにより OFDMA よりも両ユーザの通信路容量和が増加していることが分かる．用いる帯域幅は同じであるため，したがって非線形信号処理を導入することにより，周波数利用効率が向上していることになる．

4.2 機械学習を用いた協調位置推定

表 2 で後述するように，現在 3GPP release 18 規格ではセルラシステムを用いた位置推定手法技術確立が議論されている[7]．屋内では全球測位衛星システムが使用できないため，複数の測距値を用いた三辺測量の原理などにより測位を行う．この測距にセルラの広帯域なミリ波を用いた高精度 time of arrival 値を利用することで測位精度を上げることができる[15]．しかしミリ波は一般に伝搬距離が短いため，基

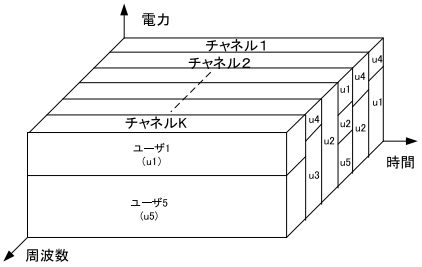


図 11　非直交多元接続（NOMA）の原理

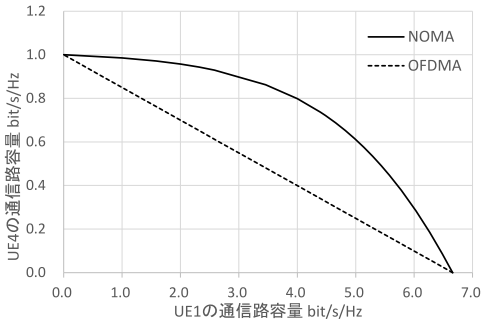


図 13　NOMA と OFDMA におけるユーザ 1，4 の通信路容量比較

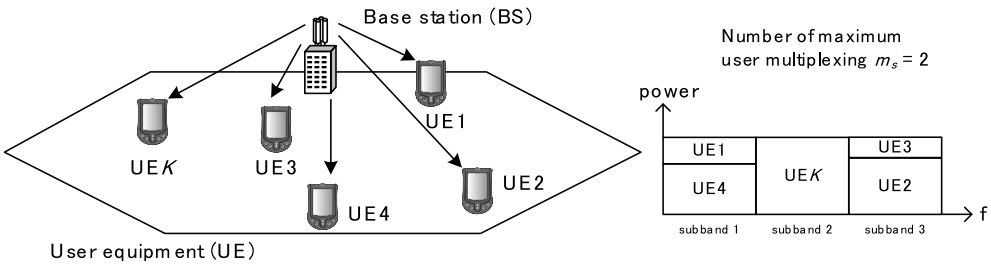


図 12　下りリンク NOMA システムモデル

表 2　3GPP release 18 物理層の主要トピック

RAN1-led project-Radio Layer 1（Physical layer）
1）MIMO Evolution for Downlink and Uplink
2）Study on Artificial Intelligence（AI）/Machine Learning（ML）for NR Air Interface
3）Study on Evolution of NR Duplex Operation
4）NR sidelink evolution
5）Study on expanded and improved NR positioning
6）Further NR RedCap UE complexity/cost reduction
7）Study on network energy savings
8）Further NR coverage enhancements
9）NR Network-Controlled Repeaters
10）Enh. of NR Dynamic spectrum sharing（DSS）
11）Study on low-power Wake-up Signal and Receiver for NR
12）Multi-carrier enhancements for NR

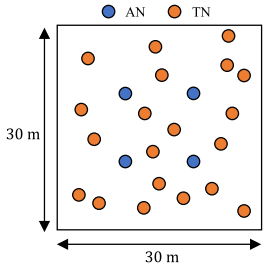


図 14　検討測位システムモデル

地局と端末間のみで通信を行う場合は，位置が既知である基地局（アンカーノード：AN）を高密度に配置する必要がある．この課題を解決するため，device-to-device（D2D）通信を用いた協調測位が注目されている[16]．この手法では D2D 通信を用いて端末間でも測位を行うことで，測位範囲を拡張できる．しかし大きな測位誤差をもつ端末がほかの端末を測位すると，測位誤差が伝搬し精度が劣化するという課題があった．そこで機械学習を用いて測位誤差の伝搬を低減する新しい協調測位手法を我々は提案した[17]．これは非線形信号処理の一種である．

提案手法では，端末の測位誤差を判定する学習モデルを事前に作成する．このモデルを測位の過程で用いることで，測位誤差が小さい端末を予測し，優先的に測位を行う．これにより端末間で大きい測位誤差が伝搬することを防ぐことが可能になる．具体的には support vector machine（SVM）を用いて位置を推定するターゲットノード（TN）の測位誤差が基準値を超えるかどうかを判定し，測位誤差が小さな TN を優先的に測位することで誤差の伝搬を低減する．

図 14 に示すシステムレイアウトにおいて計算機シミュレーションにより性能評価を行った．測位エリアの大きさは 30 m×30 m とし，AN は (10, 10)，(10, 20)，(20, 10)，(20, 20) に合計 4 個配置され，TN はランダムな座標に 20 個配置されているものとする．通常 AN で囲まれた範囲外の測位精度は大きく劣化する．また，TN がどこに存在していても最低

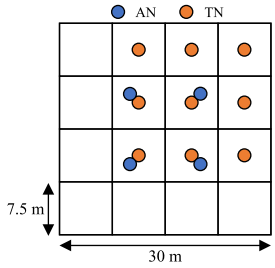


図 15　事前学習の測位エリア

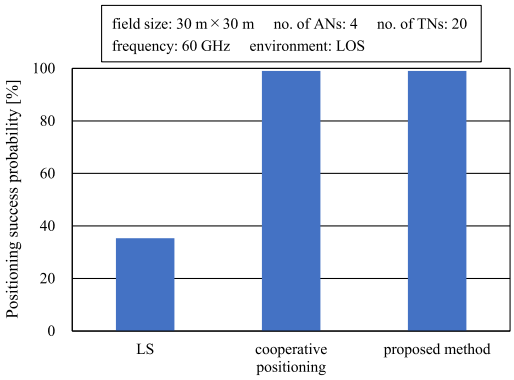


図 16　各測位手法の測位成功率による比較

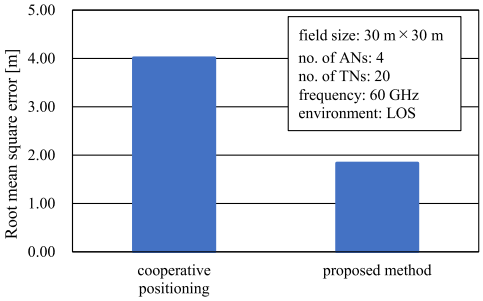


図 17　既存手法と提案手法の RMSE による比較

1 個の AN と通信するために，本稿ではノード間の最大通信距離を 14.1 m と仮定し，それ以上の遠隔のノードは電波の減衰により検出できないものとした（実際の通信距離は様々な要因で瞬時的に変動するが今回は固定とした）．図 15 に事前学習に用いた測位エリアを示す．エリアの対称性を利用して学習を一部の領域に限定することで，学習モデルの精度を保ちながら事前学習に要する計算量を抑えた．

測位成功率の比較結果を図 16 に示す．結果より，既存の一般的な最小 2 乗法（LS）法と比較して既存協調測位手法[16]と提案手法は測位成功率が約 64% 向上していることが分かる．これはノード間の最大通信距離が 14.1 m であるため，AN のみを用いる LS 法では測位範囲が限定されるが，既存協調測位手法と提案手法は AN と RN で測位するため，より広範囲を測位できるためである．また root mean square error（RMSE）の比較結果を図 17 に示す．既存の協調測位手法と比較すると提案手法は RMSE が約 54% 改善できてい

ることが分かる．これは機械学習によって測位誤差が小さいTNを優先的に測位しているため，誤差の伝搬が抑えられたためである．以上のことから，機械学習によって測位成功率を保ちながらRMSEの改善ができたといえる．

5. 6Gにおけるシステムモデリング

現在少しずつ構築が進んでいる図18のサイバーフィジカルシステム（cyber physical system : CPS）[18]~[22]は，「①フィジカル空間」の情報を「③サイバー空間」上に再現して時間空間認知，制御判断を行いフィジカル空間にフィードバックするシステムである．CPSにより安全安心便利な社会を構築することが可能と考えられている．このCPSにおける①フィジカル空間の主要装置は，「②センシング」の高効率化を実現できるロボット・自動運転車のような「移動体」である．この移動体の「④アクチュエーション」や②センシングには有線でなく無線を用いる必要があるため，CPSのコア技術として②センシングと④アクチュエーションにおける最適なスマート無線通信の実現が求められている．これらは移動体とユースケースの特徴を踏まえた高信頼低遅延かつ超多数端末向け無線伝送を行い，限られた周波数とエネルギーの有効利用を図る必要があるが，5Gではまだ能力不足であるといわれている．6GはこのCPS情報伝送を支える主要な手段と認識されており，規格化もCPS基盤を意識したものとなっている[19]．

CPS時代を踏まえ現在3GPPで議論が行われているrelease 18の無線物理層における主要トピックを表2に示す[7]．NRは5Gフレームワークを示すnew radioである．必ずしも1対1対応するわけではないが，4.1節の例は1），6），8），10），12）などに関連し，4.2節は2），5）に該当する．大まかに述べると，5Gでは線形信号処理で得られる能力では既に不十分になっており，機械学習などの低演算量で準最適結果を得られる手法を駆使して非線形に処理することが浸透してきていると考えられる．

図19にセルフリーシステム[8],[23],[24]の概念図を示す．多数のアンテナを具備する6G基地局はマイクロ波だけでなくミリ波，THz帯や光を含む高周波帯の無線をより広い帯域で使用することが考えられている．しかし高周波帯は同じ送信電力での電波到達距離が相対的に短くなるため，図中左の既存セルラの概念では時間・空間・周波数的に柔軟な無線アクセスを提供することが難しくなる．そこで右図のような，基地局や端末の役割や接続先が柔軟に変化するセルフリーの機構が必要となる．複数の基地局は面的な無線リソース割り当ての時間・空間・周波数の多軸最適化を行うことが必要であるが，最適解は組合せ爆発を起こすため，機械学習などを用いて計算量を減らし効果的な準最適解を得るための様々な方法が必要となる．その実現のためにノード分散化，エッジコンピューティング，連合学習，計算時間短縮などの技術の導入が検討されている．

また図20に示すような宇宙を含めた上空へのサービス展開を行う超カバレッジ拡張も6Gのトピックとして挙げられている[18]~[22]．こちらも広域，多層におけるリソース割り当て最適化が必要となるが，一般的に伝搬距離が長くなることから各層の時間・空間分解能も異なる．しかし人工衛星の軌道は正確に予測が可能であるため，機械学習の適用が有効と考えられる[25]．また地上ユーザをターゲットとして考え，性能指標としてシステム若しくはユーザの通信路容量とPF

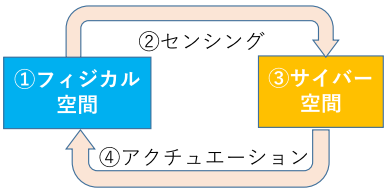


図18　サイバーフィジカルシステムサイクル

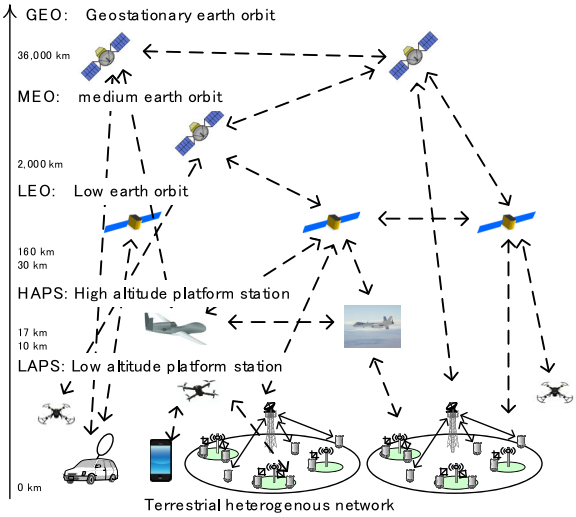


図20　宇宙階層ネットワークによる超カバレッジ拡張

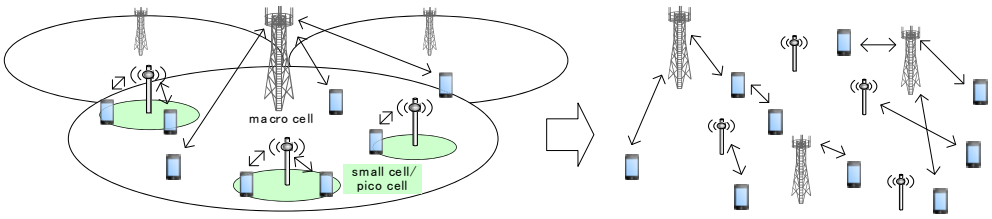


図19　高周波帯・光も用いたセルフリーシステム（右）

のみを考えた場合，恐らく宇宙ネットワークを用いた制御は効果が小さくなる．しかし宇宙側のユーザも含め，通信路容量及び PF 以外の新しい性能指標，例えば全システムの消費電力和，制御トラヒック削減量，無線電力伝送距離和及び効率，装置駆動率，排出カーボン量，ユーザアプリケーションの優先度などを加味した場合，複数目的最適化の解に宇宙活用が効果的に作用すると考えられる．

以上をまとめると，6G のモデリングは CPS を前提とし，立体的超多数分散ノード，エッジコンピューティング利用による計算分散化，機械学習などの非線形信号処理，短計算時間，準最適化による性能改善を得る仕組みを構築する形になると思われる．

6. 6G システムにおける非線形信号処理適用の効果と今後のユースケース

このような 6G システムにおいては表 1 の延長上にあるような超ユースケース拡張が求められている[19]．超ユースケース拡張とは簡単にいえばあらゆる用途に使えるということである．例えば，高エネルギーを用いた 100 Gbps の通信を行う端末や，超低遅延などのある特化した超越要素性能を適用した端末の隣で，エナジーハーベスティングを行う電池不要の省エネルギー化 IoT 端末が低速でセンシング情報を伝送しているというようなシーンが考えられる．

すると，異なる目的関数と諸元を有した超多数の通信機が存在する中で，限られた無線周波数などの通信資源を用いより高性能な無線アクセスを提供するためには，非線形信号処理の適用が必要不可欠となると予想される．つまり前節で述べたように，基地局や端末の役割や接続先が柔軟に変化するセルフリーの機構において，各端末は時間的・空間的に，目的関数に最適化された接続先と通信を行い情報伝送を行うことになる．基地局，端末は固定的な役割でなく，端末が移動基地局にもなり，リレー伝送も行い自情報のみの伝送ではなくなる．また横系でなく，図 20 のような縦系のセルフリー化も収容する必要がある．この 6G システムにおける無線リソース割り当ては，時間・空間・周波数の多軸かつ複数目的関数の最適化を行うことが必要であるが，最適解は組合せ爆発を起こすため，機械学習などを用いて計算量を減らし効果的な準最適解を迅速に得るための様々な非線形最適化問題手法の適用が必要となる．その実現のために前節で述べたようなノード分散化，エッジコンピューティング，連合学習，計算時間短縮などを用いることが効果的となる．

また重要な要素としてオペレータなどの運営組織がマネタイズできることも忘れてはいけない．その前提における超ユースケース拡張を実現する無線アクセス制御は，結論としては，爆発的な組み合わせ数の通信端末において，同時接続のほとんどの干渉成分は空間・時間・周波数軸上で直交化により分離し，一部を融合・収容して統合最適信号検出により瞬時通信路容量などの性能を上げるという方向に進むのではないかと考えられる．直交化は独立処理を可能にするため 2.1 節のように計算量削減に寄与し，統合化は 4 節のように性能向上に寄与する．この通信資源の干渉分離・融合の使い分けと瞬時的な干渉最適化は重要な要素であるといえる．

また今後のユースケース拡張についても考察したい．セルフリーシステムにおいては，自端末はある個人のユースケースに沿った要求には正確に答えるものの，同時にそのほかの余裕のあるリソースを用いて他端末や基地局のユースケース実現のための手助けを行っている可能性が高い．例えば端末間や仮想基地局としてのリレー伝送であったり，分散学習のコンピューティングや，4.2 節の協調測位である．SDGs 貢献のためには無線電力伝送による充電を行ったり休止しているかもしれない．つまり自端末がバックグラウンドで何を行っているか分からなくなる．これを突き詰めていくと，実は自端末のユースケースは本当に個人の要求どおりに叶えなければならないのか，という疑問が生じてくる．既にリソース制御は最適でなく準最適解の配分で動くようになっている．するとアプリケーションもそうなるのではないか．ミッションクリティカルアプリケーション以外のユースケースは，実はその通信が届かなくても仮想的に要求者にフィードバックを行えばよいかもしれない．例えば，スマートフォンのお勧めに現れた地球の裏側の初見ユーザのソーシャルネットワークサービス記事に「いいね」マークを付けることがどれほど重要であろうか．通信を行わずとも端末ユーザに「後で行っておきます」と表示すれば，6G システムの資源消費上でより有益であるかもしれない．「誰も見ていない間は月は存在しない」という非実在性の考え方があるように，振り返らないユースケースは叶えたふりをすればよいのである．「通信の足るを知る」という意味で 6G システムは，通信資源だけでなくユースケース，アプリケーション層も含めて最適化を行うと，より優れたシステムとなると考えられる．この尺度としては情報鮮度（age of information）[26],[27]の目的関数としての導入が有効かもしれない．

7. ま と め

本稿では移動通信の伝搬路モデルや 5G の要素技術を紹介しながら，無線通信で用いられている線形・非線形信号処理の例を説明した．そして線形処理が計算量削減，非線形信号処理がシステム性能向上に寄与することを示した．更に 5G の主要シナリオとユースケースを紹介し，現在のユースケースの展開と 6G システムモデリングの動向と考察を行った．6G では通信資源配分の要素数が爆発的に増加し，目的関数も複数化がなされるため，干渉を分離・融合しながら機械学習などを適切に用いて準最適解を迅速に導出し，無線リソースを含むシステム制御を行うことで，超ユースケース拡張に対応していくものと予想される．今後の無線通信システムにおいて非線形信号処理は必須であるといえる．

謝辞　本研究の一部は日本学術振興会科研費 22K04102 の助成を受けて行われた．

文　献

(1) https://www.3gpp.org/
(2) https://www.3gpp.org/specifications-technologies/releases/release-15
(3) ITU-R, "IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation M. 2083-0, Sept. 2015.
(4) 唐沢好男，ディジタル移動通信の電波伝搬特性，コロナ社，2003.
(5) Y. Saito, Y. Kishiyama, A. Benjebbour, T. Nakamura, A. Li and K. Higuchi, "Non-orthogonal multiple access (NOMA) for cellular future radio access," Proc. IEEE Vehicular Technology Conference (VTC Spring2013), pp. 1-5, June 2013.
(6) K. Higuchi and A. Benjebbour, "Non-orthogonal multiple access (NOMA) with successive interference cancellation for future radio access," IEICE Trans. Commun., vol. E98-B, no. 3m pp. 403-414, March 2015.
(7) https://www.3gpp.org/specifications-technologies/releases/release-18
(8) H.Q. Ngo, A. Ashikhmin, H. Yang, E.G. Larsson, and T.L. Marzetta, "Cell-free massive MIMO versus small cells," IEEE Trans. Wireless Commun., vol. 16, no. 3, March 2017.
(9) (一社)電気通信事業者協会，事業者別契約数，https://www.tca.or.jp/database/index.html
(10) Ericsson, "Ericsson Mobility Report," pp. 1-40, Nov. 2022.
(11) 3GPP TR 38.901 V17.0.0, "Study on channel model for frequencies from 0.5 to 100 GHz," March 2022.
(12) 3GPP TS22.186 V16.2.0, "Enhancement of 3GPP support for V2X scenarios ; Stage 1," Nov. 2020.
(13) 3GPP TS22.104 V16.5.0, "Service requirements for cyber-physical control applications in vertical domains ; Stage 1," Sept. 2020.
(14) E. Okamoto, "An improved proportional fair scheduling in downlink non-orthogonal multiple access system," Proc. IEEE Vehicular Technology Conf. 2015 Fall (VTC-2015Fall), pp. 1-5, Sept. 2015.
(15) K. Ishida, E. Okamoto and H. -B. Li, "A robust indoor localization method for NLOS environments utilizing sensor subsets," IEEE Open J. Signal Process., vol. 3, pp. 450-463, Dec. 2022.
(16) G. Cullen, K. Curran, J. Santos, G. Maguire, and D. Bourne, "CAPTURE—Extending the scope of self-localization in Indoor Positioning Systems," 2015 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Oct. 2015.
(17) 山本岳志，岡本英二，"5G 端末間通信を用いた屋内測位の範囲拡張と精度向上の検討，" 信学技報，vol. 122, no. 108, SeMI2022-40, pp. 87-92, July 2022.
(18) Beyond 5G 推進コンソーシアム白書分科会，"Beyond 5G ホワイトペーパー～2030 年代へのメッセージ～1.0 版，" March 2022.
(19) NTT ドコモ，"ホワイトペーパー：5G の高度化と 6G，" 5.0 版，Nov. 2022.
(20) KDDI 総合研究所，"B5G/6G ホワイトペーパー 2.0.1 版，" Oct. 2021.
(21) ソフトバンク，"Beyond 5G/6G コンセプト，"July 2021.
(22) 情報通信研究機構，"Beyond 5G/6G ホワイトペーパー 2.0 版，"March 2022.
(23) T. Choi, M. Ito, I. Kanno, J. Gomez-Ponce, C. Bullard, T. Ohseki, K. Yamazaki, and A.F. Molisch, "Energy efficiency of uplink cell-free massive MIMO with transmit power control in measured propagation channel," IEEE Open J. Circuits Syst., vol. 2, pp. 792-804, Dec. 2021.
(24) M. Ito, I. Kanno, K. Yamazaki, Y. Kishi, W.-Y. Chen, T. Choi, and A.F. Molisch, "Impact of antenna distribution on spectral and energy efficiency of cell-free massive MIMO with transmit power control algorithms," IEEE Open J. Commun. Soc., vol. 3, pp. 1615-1629, Sept. 2022.
(25) J. Cui, S.X. Ng, D. Liu, J. Zhang, A. Nallanathan, and L. Hanzo, "Multiobjective optimization for integrated ground-air-space networks : Current research and future challenges," IEEE Veh. Technol. Mag., vol. 16, no. 3, pp. 88-98, Sept. 2021.
(26) S. Kaul, M. Gruteser, V. Rai, and J. Kenney, "Minimizing age of information in vehicular networks," Proc. IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 350-358, June 2011.
(27) S. Kaul, R. Yates, and M. Gruteser, "Real-time status : How often should one update?," Proc. IEEE INFOCOM 2012, pp. 2731-2735, March 2012.

(幹事団提案，2023 年 3 月 12 日，2023 年 4 月 5 日再受付)

岡本英二（正員：フェロー）

1993 京大・工・電気第二卒．1995 同大大学院修士課程了．同年，郵政省通信総合研究所（現情報通信研究機構）入所．現在，名古屋工業大学大学院工学研究科准教授．博士（情報学）．衛星通信，ミリ波加入者系無線アクセスシステム，移動通信，暗号化通信の研究開発に従事．1998 本会学術奨励賞，2008 総務省東海総合通信局長表彰，2009 船井情報科学奨励賞，2021 本会 NOLTA ソサイエティ貢献賞受賞．著書『情報理論』（共著）など．

技術の原点

アクティブノイズコントロールにおける最近の動向

Recent Advances on Active Noise Control

梶川嘉延 Yoshinobu KAJIKAWA

アブストラクト　本稿では不快な騒音を音で制御・低減するアクティブノイズコントロール（ANC）について，これまでの技術の変遷を展望するとともに最近の動向について解説する．ANC はスピーカ（二次音源）からの制御音により騒音源（一次音源）からの騒音を制御・低減する技術であり，近年ではノイズキャンセリングヘッドホンなどを通じて一般にもその技術が広く知られるようになった．しかしながら，オフィスやイベント会場などの公共空間や車内や住宅内などの交通・住環境において，三次元的に騒音を制御することは未だ広くは実用化されていない．このような音空間において三次元的に騒音制御を実現するためには乗り越えるべき課題が多々残されている．本稿では，まず ANC システムを実装する上で重要となる消音領域（ZoQ）を任意の位置に移動させるバーチャルセンシングについて，代表的な 3 手法を紹介するとともに，それらの性能比較を示す．また，フィードフォワード ANC システムにおいて重要となる因果性制約について説明し，その 1 解決策であるオーバーサンプリングを利用した ANC システムについて述べる．そして，近年様々な分野において利用されている機械学習の ANC システムへの適用方法について紹介する．

キーワード　アクティブノイズコントロール，バーチャルセンシング，因果性制約，機械学習

Abstract　This paper is a review of the history of active noise control (ANC), which uses sound to control and reduce unpleasant noise, and describes recent trends in the field. ANC is a technology for controling and reducing noise from noise sources (primary sources) by using controlled sounds from loudspeakers (secondary sources). This technology has become widely known to the public through noise-canceling headphones. However, three-dimentional (3D) noise control in public spaces such as offices and event halls, as well as in traffic and residential environments such as inside cars and houses, has not yet been widely implemented. In order to realize 3D noise control in such sound spaces, there are still many problems to overcome. In this paper, three representative virtual sensing methods for moving the zone of quiet (ZoQ) to an arbitrary location are first introduced, and their performance characteristics are compared. In addition, the causality constraint that is important in feed-forward ANC systems is explained, and an ANC system using oversampling is introduced as one solution to this problem. Furthermore, an application of machine learning, which has been used in various fields in recent years, to ANC systems is presented.

Key words　Active noise control, Virtual sensing, Causality constraint, Machine learning

1. はじめに

騒音を低減するために，その騒音に対して同振幅・逆位相の擬似騒音を生成し，騒音を低減するアクティブノイズコントロール（ANC: active noise control）[(1)~(4)]は，1990 年代頃から家電製品や車，工場など，様々な用途に用いられるようになってきた．また，ノイズキャンセリング機能付きヘッドホンが 2000 年代から急速に普及した結果，ANC という用語も一般的に知られるようになったといえる．

ANC は空調ダクトなどの一次元音場として取り扱い可能な環境においてまず適用された[(5)]．空調ダクト騒音に対してはフィードフォワード型 ANC が一般的に利用される．フィードフォワード型 ANC ではダクト上流（騒音源に近い側）に参照マイクロホンを設置し，制御を行いたい騒音に相関のある参照信号を取得し，その参照信号を騒音制御フィルタでフィルタリングすることで擬似騒音を生成する．生成された擬似騒音は二次音源と呼ばれるスピーカから放射され，ダクト上流から伝搬してきた騒音と重ね合わされる．そして，ダクト下流（通常ダクトの出口付近）に設置された誤差マイクロホン地点において，騒音に対して同振幅・逆位相の擬似騒音を生成するために，誤差マイクロホンで得られた誤差信号を（実際には 2 乗誤差）を最小化するように騒音制御フィルタのフィルタ係数を適応アルゴリズムにより更新する．

一方，三次元音場における ANC では一般的に誤差マイクロホン地点を中心に消音領域（ZoQ: zone of quiet）を生成することができるが，ZoQ の大きさは制御対象となる騒音の周波数（波長）によって決まる．具体的には，波長の 1/10 の直径

梶川嘉延　正員：フェロー　関西大学システム理工学部電気電子情報工学科
E-mail kaji@kansai-u.ac.jp
Yoshinobu KAJIKAWA, Fellow (Dept. of Electrical, Electronic, and Information Engineering, Faculty of Engineering Science, Kansai University, Suita-shi, 564-8680 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.36–43 2023 年 7 月

の球状（若しくは三日月状）の範囲で 10 dB の騒音低減が実現される（実際には二次音源のサイズ，二次音源と誤差マイクロホンとの距離，騒音源の方向によって ZoQ の形状や範囲は異なる）[6]~[9]．これは 100 Hz では直径 34 cm となり人の頭をカバーするに十分であるが，1000 Hz では直径 3.4 cm の限られた空間となるため誤差マイクロホンを耳元に設置しない限りは実際の効果が得られないことを示唆している．

したがって，消音領域（ZoQ）を広げるもしくは耳元に常に ZoQ を生成するなどの対応が三次元音場において広帯域での騒音低減を ANC によって実現する際には必要となる．これらを実現する方法としては，(1) 多数のマイクロホンやスピーカを設置することで，閉空間全体で騒音を低減するグローバル ANC [10]~[18]，(2) 誤差マイクロホンをユーザの耳元などの所望の地点に設置することが物理的に困難な場合にバーチャルセンシング（VS）技術[19]~[38]により ZoQ を誤差マイクロホン地点からユーザの耳元に移動させるローカル ANC，(3) グローバル ANC とローカル ANC の中間に位置するといえる，カーネル補間や球面・円筒調和解析に基づき，比較的広い消音領域を形成することができる空間 ANC [39]~[43]がある．

本稿ではそのような ANC に関する最新の制御手法やアルゴリズム，更には新しい適用分野など最新の動向と今後の展開について紹介する．特に，ANC システムを実用化する上で重要なバーチャルセンシング並びに因果性制約を中心に概説するとともに，最近注目されている機械学習との融合など今後期待される基礎的研究や応用技術についても紹介する．

2. ANC の原理と代表的な制御方式

スピーカを使用して不快な騒音を低減するための擬似騒音を発生させる ANC は，Lueg による 1936 年の特許で初めて提案された[44]．ANC は重ね合わせの原理に基づく電気音響技術で，同振幅で逆位相の擬似騒音を二次音源（スピーカなど）から発生させて不要な（一次）騒音を音響的にキャンセルし，結果として残留騒音を低減させる．ANC は，吸音材や遮音壁などによるパッシブな騒音制御技術がコストが高く，効果を発揮できない低周波騒音を減衰させるのに非常に有効である．実際に ANC の研究開発が盛んになったのは信号処理技術の進展と DSP (digital signal processor) 技術の登場が起こった 1980 年代以降であり，多くの研究者や企業の技術者がこぞって研究開発を推進し，そのブームは 1990 年代中頃まで続いた．しかしながら，当時の DSP 技術ではマルチチャネルによる広範囲の制御は困難であったため，騒音を発生する機器の騒音発生源（ファンやコンプレッサー等）から機器外部への騒音伝搬経路をダクトを設置するなどして限定することで一次元制御を実現する取り組みが一般的であった．その結果，20 世紀末頃には ANC 研究は冬の時代を迎え，多くの企業が研究開発から撤退することになった．一方で細々とした研究開発は幾つかの企業や大学で継続して行われ，21 世紀に入ってノイズキャンセリングヘッドホンの登場とその普及により ANC 技術が再注目されるようになり現在に至っている．

しかし，実用化においては，騒音源や音響環境の特性が変化

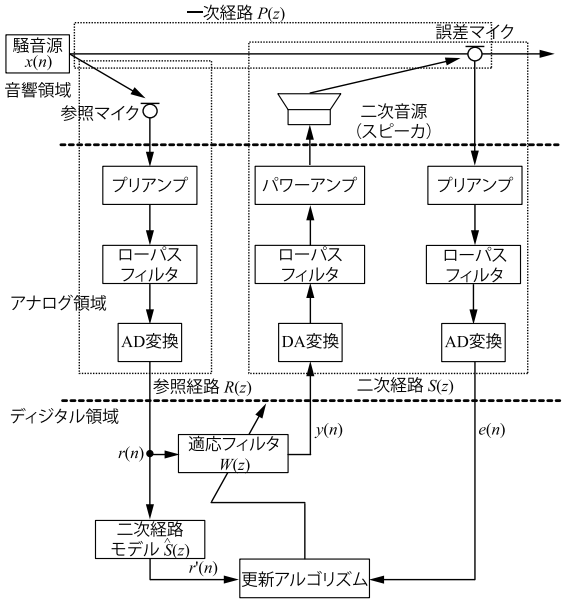


図 1　フィードフォワード型 ANC のブロック図

するため，一次騒音の周波数成分，振幅，位相も変化する．これらの時間的に変化する一次騒音の特性に追従し，一次騒音が制御地点まで伝搬する経路である一次経路の変動にも対処するため，ほとんどの ANC システムでは適応フィルタを利用している．最も一般的に使用されている適応フィルタは，最小平均 2 乗（LMS）アルゴリズムを用いた有限インパルス応答（FIR）フィルタにより実現される．更に，騒音低減性能は，制御器を通じて生成される擬似騒音の振幅と位相の精度に依存するため，制御器をディジタル技術によって実現することが有用である．したがって，高性能かつ低コストでのディジタルハードウェアの開発は，実用的な ANC アプリケーションにおいて重要となることから，ANC システムに適したディジタルハードウェアに関する研究も根強く行われてきた．特に，より速い収束速度を確保するとともに，経路変動に対するロバスト性を向上した高度な適応アルゴリズムの開発は重要な研究分野の一つとなっている．ディジタル信号処理により実装される ANC システムは，その制御方式によりフィードフォワード型とフィードバック型に分類されるが，本稿では主にフィードフォワード型に焦点をあてて議論を進める．

ANC の基本概念を図 1 に示すシングルチャネル広帯域フィードフォワード ANC システムを用いて説明する．このシステムでは，騒音源（一次音源）で発生した一次騒音 $x(n)$ は参照経路 $R(z)$ を介してマイクロホンなどの参照センサによって参照信号 $r(n)$ として検出される．この参照信号は騒音制御フィルタ $W(z)$ で処理され，二次音源駆動信号 $y(n)$ となり，スピーカなどの二次音源を駆動する．制御点に配置されたマイクロホンなどの誤差センサは，ANC システムの性能を監視するために残留騒音 $e(n)$ を検出する．そして，適応フィルタである騒音制御フィルタ $W(z)$ は一次経路 $P(z)$，二次経路 $S(z)$，参照経路 $R(z)$ で構成される伝達関数 $P(z)/R(z)S(z)$ を推定し，誤差信号 $e(n)$ を最小化するための二次音源駆動信号 $y(n)$ を生成するための騒音制御フィルタ $W(z)$ の係数を適応アルゴリズムにより更新す

る．ここで，一次経路 $P(z)$ は騒音源から制御点までの音響伝達経路，二次経路 $S(z)$ は騒音制御フィルタ出力から誤差センサ入力までの一連の伝達経路，参照経路は騒音源から参照センサ入力までの伝達経路を，それぞれ意味する．また，各種伝達経路が時間的に変化する場合，適応アルゴリズムには経路特性の時間的変化を連続的に追跡するというタスクも担うことになる．

適応フィルタ $W(z)$ の目的は，LMS アルゴリズムなどの更新アルゴリズムを用いてそのフィルタ係数を自動的に適応させることにより，残留誤差 $e(n)$ を最小化することである．音響エコーキャンセラのような適応フィルタリングのアプリケーションでは，誤差信号はディジタル領域で $e(n) = d(n) - y(n)$ として計算できるが，ANC システムでは $y(n)$ は二次経路 $S(z)$ を介して音に変換され，騒音 $d(n)$ と音響的に合成されるため，二次経路 $S(z)$ の存在により誤差信号 $e(n)$ が二次音源駆動信号 $y(n)$ と時間的にずれてしまう．したがって，二次経路を補償することが可能な適応アルゴリズムを使用する必要がある．なお，二次経路 $S(z)$ には，ディジタル・アナログ変換器（DAC），再構成フィルタ，パワーアンプ，スピーカ，スピーカから誤差マイクロホンまでの音響経路，エラーマイクロホン，プリアンプ，アンチエイリアシングフィルタ，アナログ・ディジタル変換器（ADC）などが含まれる．

一般に，二次経路 $S(z)$ の影響を補償するために，フィルタ係数更新に利用する参照信号に対して，二次経路のモデル（推定）$\hat{S}(z)$ となるディジタルフィルタによりフィルタリングする．この修正適応型アルゴリズムは，filtered-x LMS（FXLMS）アルゴリズムと呼ばれ，Burgess が ANC アプリケーション用に最初に提案したものである[5]．FXLMS アルゴリズムのフィルタ更新式は

$$\mathbf{w}(n+1) = \mathbf{w}(n) + \mu e(n)\mathbf{r}'(n) \tag{1}$$

として与えられる．ここで，$\mathbf{w}(n)$ は騒音制御フィルタの係数ベクトル，$\mathbf{r}'(n)$ は二次経路モデルによりフィルタリングされた参照信号ベクトル，μ はステップサイズパラメータ（正の定数）である．

フィードフォワード型 ANC は，以上のように騒音を検出するマイクロホン（参照マイクロホン）及び消音効果をモニタリングするマイクロホン（誤差マイクロホン）と擬似騒音を生成する二次音源スピーカから構成されている．よって，参照マイクロホンで観測された騒音と相関のある騒音を誤差マイクロホン地点で低減することが可能であり，また誤差マイクロホン周辺に消音領域（ZoQ）を生成する．

このように限定された領域に消音領域（ZoQ）を形成する方法をポイント制御若しくはローカル ANC と呼ぶ．ローカル ANC の代表的な応用例としては車や列車などにおけるシートのヘッドレストへの適用などが挙げられる．ローカル ANC においては，誤差マイクロホン周辺に ZoQ を形成して，対象となる騒音をその領域においてのみ低減することを目的としているため，ヘッドレストへの適用を例に取ると，誤差マイクロホン及び二次音源スピーカはユーザの両耳付近に一つずつ，参照マイクロホンは適用環境に応じて一つから数個程度で実装が可能である．よって，低チャネル数の ANC システムとして比較的低演算量で実現することができる．しかし，誤差マイクロホン地点を中心に 1/10 波長のサイズで ZoQ が形成されるため，誤差マイクロホンをユーザの耳元に物理的に設置できない状況では聴感上で騒音低減効果を実感できないという問題がローカル ANC では生じる．したがって，バーチャルセンシング（VS）技術を適用することで，ZoQ を所望の地点に移動させる必要がある．

3. バーチャルセンシング

バーチャルセンシング技術は，マイクロホンアレーを利用して補間や外挿などにより制御地点に到来する騒音を予測する方法と事前学習により制御地点で最大の騒音低減を実現するための伝達経路情報を推定する方法に大別されるが，本稿では事前学習（チューニングステージと呼ぶ）を利用する方法を中心に説明する．図 2 にシングルチャネルフィードフォワード ANC においてバーチャルセンシングを導入する場合の各マイクロホンとスピーカの配置例を示す．図 2 において，騒音低減を実現したい制御点（耳元等）にはチューニングステージにおいてのみ物理的にマイクロホンを設置する．そのマイクロホンのことをバーチャルマイクロホンと呼び，実際の制御時（コントロールステージと呼ぶ）には制御点には物理的なマイクロホンは設置されない．ここでは，事前学習を利用するバーチャルセンシング技術として，補助フィルタ法，リモートマイクロホン法，並びに相対経路法について説明する．

3.1 補助フィルタ (AFVS) 法

補助フィルタ（AFVS: auxiliary filter based virtual sensing）法のブロック図を図 3 に示す．(a) がチューニングステージを，(b) がコントロールステージをそれぞれ示している．チューニングステージでは，ZoQ を形成したい位置にバーチャルマイクロホンを設置し，その地点で消音を実現する騒音制御フィルタ $W_v(z)$ を求めると同時に，その騒音制御フィルタを含む騒音源から誤差マイクロホン地点までの全体経路 $P_m(z) + S_m(z)W_v(z)R(z)$ を補助フィルタ $H(z)$ により推定する．そして，コントロールステージにおいて，補助フィルタ $H(z)$ からの出力 $f(n)$ を誤差マイクロホンで検出した誤差信号 $e_m(n)$ に加えることで，騒音制御フィルタ $W(z)$ はチューニングステージで推定した ZoQ で騒音低減を実現する騒音制御フィルタ $W_v(z)$ に収束することができる．

AFVS 法では補助フィルタ $H(z)$ に ZoQ で騒音低減を実現

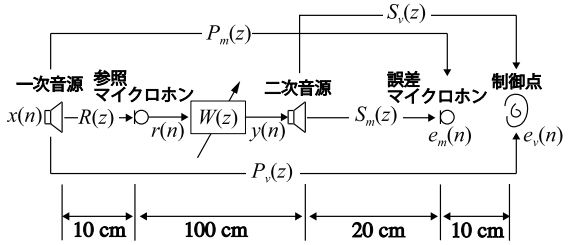
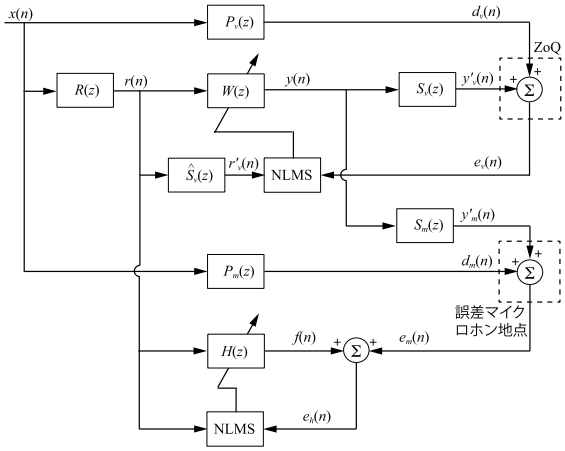
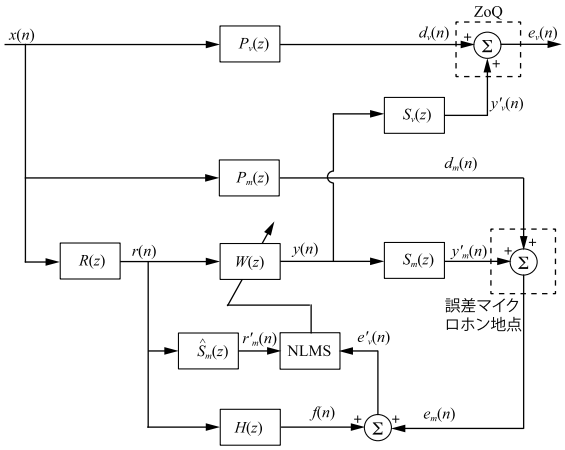


図 2　バーチャルセンシングを導入したシングルチャネルフィードフォワード ANC の配置例



(a) チューニングステージ



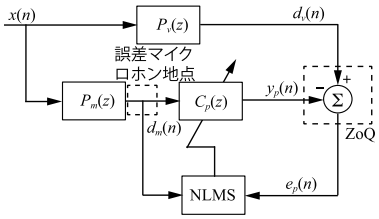
(b) コントロールステージ

図 3　補助フィルタ（AFVS）法のブロック図

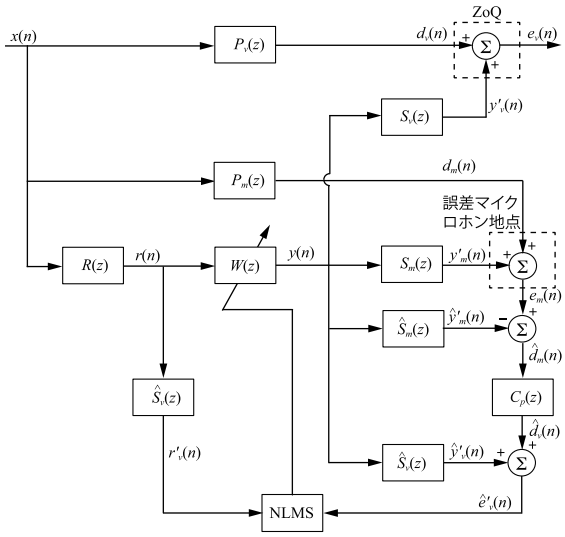
する騒音制御フィルタ $W_v(z)$ の情報を保持しているため，次節以降で説明するリモートマイクロホン法や相対経路法のように騒音源に対するとバーチャルマイクロホンの配置に関して制限がなく，ANC の実装においてマイクロホンを自由に配置できるという利点がある．これはモニタリングを行う誤差マイクロホンを ZoQ からかなり離れた地点に配置することも可能となることを意味しており，ANC の適用範囲を大きく広げることができるという利点となる．

3.2　リモートマイクロホン (RMVS) 法

リモートマイクロホン（RMVS: remote microphone based virtual sensing）法のブロック図を図 4 に示す．(a) がチューニングステージを，(b) がコントロールステージをそれぞれ示している．チューニングステージでは，騒音源から ZoQ を形成したい地点（バーチャルマイクロホン地点）までの一次経路 $P_v(z)$ を伝搬してきた騒音信号 $d_v(n)$ と騒音源からモニタリング用のマイクロホン（誤差マイクロホン）地点までの一次経路 $P_m(z)$ を伝搬してきた騒音信号 $d_m(n)$ を利用することで，補正フィルタ $C_p(z)$ を得る．この補正フィルタ $C_p(z)$ は $P_v(z)/P_m(z)$ なる伝達関数を推定することになり，コントロールステージでは，(b) のブロック図に示されるように，この補正フィルタ $C_p(z)$



(a) チューニングステージ



(b) コントロールステージ

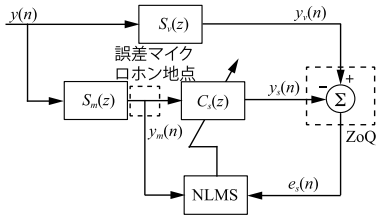
図 4　リモートマイクロホン（RMVS）法のブロック図

を介することで，誤差マイクロホン地点で観測される騒音信号の推定 $\hat{d}_m(n)$ から ZoQ を形成したい地点で観測される騒音信号の推定 $\hat{d}_v(n)$ を得ることができる．これにより，ZoQ を形成したい地点に物理的にマイクロホンを配置しなくとも，ZoQ で騒音低減を実現することができる．

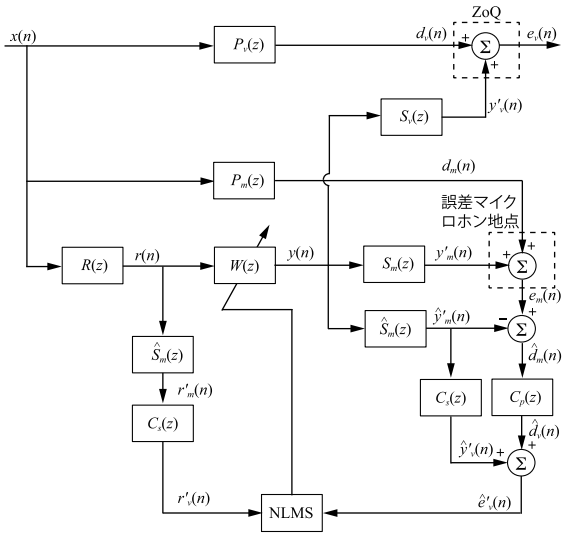
RMVS 法では，騒音源からバーチャルマイクロホン地点及び誤差マイクロホン地点までのそれぞれの一次経路の比 $P_v(z)/P_m(z)$ を補正フィルタ $C_p(z)$ により保持するため，理論的にバーチャルマイクロホン地点は誤差マイクロホン地点よりも騒音源から遠方に配置する必要がある．ただし，誤差マイクロホン地点で得られる信号に対して遅延処理を加えることでこの問題は解決可能である．また，部屋の特性により一次経路の周波数特性上にディップが生じると補正フィルタ $C_p(z)$ をその周波数において正確に推定できなくなるため，バーチャルマイクロホン地点での騒音信号 $d_v(n)$ を正確に推定できず，騒音低減性能が劣化する可能性がある．一方で，コントロールステージにおいて ZoQ に対する最適な騒音制御フィルタ $W_v(z)$ を推定するため，チューニングステージとコントロールステージにおける一次経路や参照経路の変動に対して比較的ロバストであるという利点がある．

3.3　相対経路 (RPVS) 法

相対経路（RPVS: relative path based virtual sensing）法のブロック図を図 5 に示す．(a) が付加的なチューニングステー



(a) チューニングステージ



(b) コントロールステージ

図 5　相対経路（RPVS）法のブロック図

ジを，(b) がコントロールステージをそれぞれ示している．チューニングステージでは，RMVS 法のチューニングステージにより補正フィルタ $C_p(z)$ を得た後に，(a) の構成により，二次音源からバーチャルマイクロホン地点までの二次経路 $S_v(z)$ を伝搬してきた信号 $y_v(n)$ と二次音源から誤差マイクロホン地点までの二次経路 $S_m(z)$ を伝搬してきた信号 $y_m(n)$ を利用することで，別の補正フィルタ $C_s(z)$ を得る．この補正フィルタ $C_s(z)$ は $S_v(z)/S_m(z)$ なる伝達関数を推定することになり，コントロールステージでは，(b) のブロック図に示されるように，まず補正フィルタ $C_p(z)$ を介することで，誤差マイクロホン地点で観測される騒音信号の推定 $\hat{d}_m(n)$ から ZoQ を形成したい地点で観測される騒音信号の推定 $\hat{d}_v(n)$ を求める．

そして誤差マイクロホン地点に伝搬された擬似騒音の推定 $\hat{y}_m(n)$ からもう一つの補正フィルタ $C_s(z)$ を介してバーチャルマイクロホン地点の擬似騒音の推定 $\hat{y}_v(n)$ を求め，電気的にバーチャルマイクロホン地点での誤差信号 $\hat{e}_v(n)$ を得る．これにより，所望地点で騒音低減を実現することができる．RPVS 法は原理的には RMVS 法と同様であるが，一次経路の比 $P_v(z)/P_m(z)$ だけでなく，二次経路の比 $S_v(z)/S_m(z)$ を求めることで，一次経路及び二次経路が変動した際のロバスト性を向上できるという利点がある．一方で，RMVS 法と同じくマイクロホンの幾何学的な配置には制約がある．

3.4　性能比較例

前節までに紹介した 3 種類のバーチャルセンシング技術について性能比較の一例を示す．ここでは，図 2 の実験配置におけるバーチャルマイクロホン地点（ZoQ を形成したい地点）での誤差信号スペクトルの比較を示す．各種パラメータは騒音低減効果が最大となるように事前に試行錯誤して選び，チューニングステージとコントロールステージで全ての経路は変動しないものとする．図 6 に誤差信号スペクトルの比較を示す．

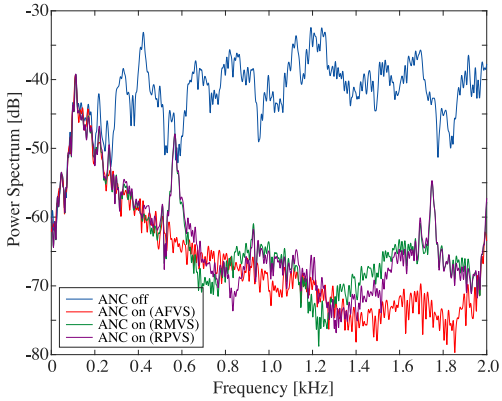


図 6　バーチャルマイクロホン（ZoQ）地点における残留騒音信号スペクトルの比較

図 6 から AFVS 法は最も高い消音性能を示していることが分かる．一方，RMVS 法と RPVS 法では幾つかの周波数で騒音低減性能が劣化していることが分かる．これは部屋の特性などによる一次経路の周波数特性上のディップに起因するものである．ここでは各種音響経路が変動しない状況での結果を示したが，それらが変動する場合には 3 種類のバーチャルセンシング技術のロバスト性は変動する経路によって異なるため，利用する音響環境に応じて適切なバーチャルセンシング技術を適用することが実用上は重要である．

4.　フィードフォワード制御における因果性制約

フィードフォワード制御においては，騒音源近くに配置された参照マイクロホンで検出した参照信号を利用して制御器を通じて擬似騒音を二次音源スピーカから放射することで，制御地点（誤差マイクロホン地点）で音響的に干渉させる．したがって，騒音源からの騒音が制御地点に到達するまでに，参照マイクロホンで検出した参照信号に対する一連の処理を終える必要がある．騒音源から制御地点（一次経路 $P(z)$）までに対象騒音が伝搬するまでの間に，制御系において通過するのは，図 1 から，参照経路 $R(z)$（騒音源から参照マイクロホンまでの音響経路，参照マイクロホン，プリアンプ，アンチエイリアシング用ローパスフィルタ，AD 変換器で構成），騒音制御フィルタ $W(z)$，二次経路 $S(z)$ の一部（DA 変換器，平滑化用ローパスフィルタ，パワーアンプ，二次音源スピーカ，二次音源から誤差マイクロホンまでの音響経路で構成）である．よって，それら全体の合計遅延時間を一次経路 $P(z)$ の遅延時間より短くする必要がある．これをフィードフォワード制御における因果性制約[45]と呼び，因果性制約を満足しない条件においては ANC の騒音低減性能

が劣化する，最悪の場合には全く騒音低減できないという状況に陥る．ここで，因果性制約を満たすには，以下の不等式を満たす必要がある．

$$D_P > D_R + D_C + D_S, \tag{2}$$

ただし，D_P は一次経路 $P(z)$ の遅延，D_R は参照経路 $R(z)$ の遅延，D_C は擬似騒音を生成する騒音制御フィルタ $W(z)$ の処理遅延，D_S は上記で述べた二次経路 $S(z)$ の一部の遅延である．参照経路の遅延 D_R には騒音源から参照マイクロホンの音響経路，参照マイクロホン，プリアンプ，アンチエイリアシング用ローパスフィルタ，AD 変換器が含まれるが，このうちマイクロホン（ANC においてはエレクトレットコンデンサマイクロホンを利用することが多い）とプリアンプの遅延はほとんど無視できるため，大きく寄与するのは音響経路（これは単純に騒音源から参照マイクロホンまでの距離で決まる），アナログローパスフィルタ，AD 変換器による遅延である．同様に二次経路の遅延 D_S において支配的な遅延は，DA 変換器，アナログローパスフィルタ，スピーカ，二次音源から誤差マイクロホンの音響経路によるものである．また，D_C の遅延量はサンプリング周波数によって決定される．

ここで，フィードフォワード制御のシステム規模を小さくする（例えば小型の ANC ユニットを作成する）ためには，参照マイクロホンと誤差マイクロホンの距離を短くすることが必要である．しかし，フィードフォワード制御においては，式 (2) における D_R 及び D_S におけるアナログローパスフィルタやスピーカの遅延が大きいため，因果性制約を満たすためには参照マイクロホンと誤差マイクロホンとの距離を十分に長くする必要がある．そこで，システム全体の処理遅延を低減するために，オーバーサンプリング技術を用いた ANC システムが提案されている[46],[47]．オーバーサンプリング技術を用いた ANC システムのブロック図を図 7 に示す．通常の ANC システムでは，アンチエイリアシングフィルタと平滑化フィルタ用にアナログローパスフィルタが必要なため大きな処理遅延が発生する．一方，オーバーサンプリング技術を用いた ANC システムでは，サンプリング周波数を一般的な ANC システムにおいて必要とされるサンプリング周波数（8 kHz 程度）よりもかなり高く（100 kHz 程度）に設定することでアンチエイリアシングフィルタと平滑化フィルタを不要とし，参照経路の遅延 D_R と二次経路の遅延 D_S を低減する．また，サンプリング周波数が高くなることで騒音制御フィルタの処理遅延 D_C も低減することができる．そのため，オーバーサンプリング技術を用いた ANC システムでは，参照マイクロホンと誤差マイクロホンとの間の距離を短くする（5 cm 程度まで近づける）ことができる．ただし，サンプリング周波数が高くなると信号処理系のディジタルフィルタのタップ長を長くする必要があるため，適切なサンプリング周波数の設定とディジタルフィルタ演算の並列化が必須となる．そのため，並列化処理が可能なハードウェアを使用する必要がある．

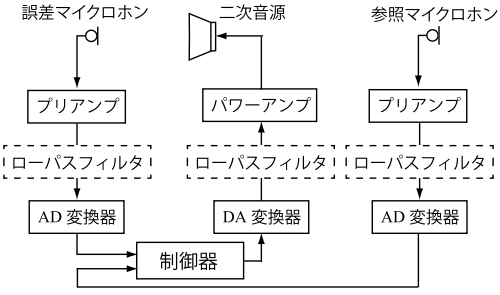


図 7　オーバーサンプリングを利用したフィードフォワード ANC

5. 機械学習の ANC システムへの導入

近年，画像認識や音声認識の分野においてディープラーニングに代表される機械学習の研究が非常に盛んである．これまで機械学習の音響分野への応用は，音声認識，音響イベント検出，音源分離，異常音検知などの主に集音系において展開され，従来の信号処理ベースの処理技術から，機械学習ベースの処理技術として発展している．ANC は集音と音再生の両方を同時に，かつリアルタイムで行う技術のため，これまで機械学習の導入はそれほど検討されていなかったが，この数年で検討事例が一挙に増えてきている．具体的には，対象騒音ごとにあらかじめデータベースに登録された適切な騒音制御フィルタを選択する，選択固定フィルタ ANC（SFANC）システムが提案されている[48]~[50]．広帯域フィードフォワード ANC における騒音制御フィルタの特性は，一次経路，二次経路，参照経路の音響伝達経路の特性だけでなく，騒音の特性にも依存する．したがって，騒音の性質や種類が変化した際には，騒音制御フィルタの再設計や適応フィルタによる追従が必須である．そこで，あらかじめ騒音とそれに対して最も騒音低減効果が高くなる騒音制御フィルタの対を大量にデータセットとして蓄え，それらにより畳み込みニューラルネットワーク（CNN）の学習を行い，騒音の性質や種類が変化した際に学習済み CNN により適切な騒音制御フィルタに切り替えるのが SFANC システムである．

SFANC システムのブロック図を図 8 に示す．このシステムは図 8 に示すように，大きく分けて事前学習ステージ，特徴抽出ステージ，フィルタ選択ステージの三つの段階がある．事前学習ステージでは，騒音データセットを利用し，実騒音や有色雑音などを合成した騒音などにより事前に騒音制御フィルタのフィルタ係数を多数作成し，騒音制御フィルタデータベースに蓄える．ただし，一次経路，参照経路，及び二次経路の音響伝達系は事前に同定し，それらをシミュレーション上でフィルタ

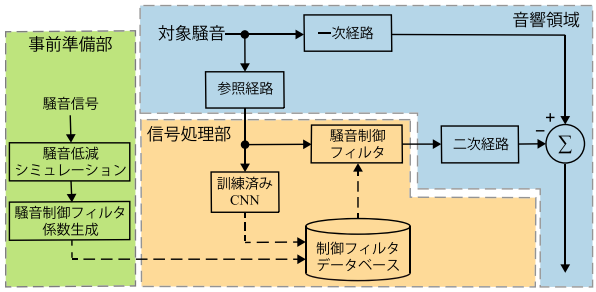


図 8　選択固定フィルタ ANC システムのブロック図

として利用する．次に特徴抽出ステージでは，参照マイクロホンで取得した参照信号から，振幅スペクトルやスペクトログラムなどを特徴量として抽出する．その後，フィルタ選択ステージに移行し，それらの特徴量に基づいて CNN により騒音制御フィルタの選択を行う．これらのステージはリアルタイムで動作し，選択された騒音制御フィルタは固定フィルタとしてフィードフォワード ANC システムに適用され，対象騒音の低減を行う．このようなシステム構成にすることで，通常の ANC システムに比べて，適応フィルタにおける係数更新の時間を短縮できるため，素早く対象騒音の変化に追従するとともに，高い騒音低減性能を実現することができる．

6. おわりに

騒音問題はあらゆる場面において発生し，健康への影響も大きいことから，今後もその対策技術の開発は必要である．その対策技術の一つである ANC は古い技術であるものの，その適用範囲は未だ限定されていることから，更なるブレークスルーが必要とされる．特に，ANC 技術の更なる普及のためには，適用例ごとに最も適したスピーカの開発が必須である．例えばパーティションに二次音源を設置する場合にはバックキャビティが必要となるダイナミックスピーカよりも圧電型のスピーカのほうが適している．また，ダイナミックスピーカでは放射面積（スピーカサイズ）を大きくするには，複数のスピーカを設置する必要があり，パーティション全体を二次音源とするには不向きなため，それに適したスピーカ開発が必要である．更に広い空間において特定の領域を制御する際に，制御領域外に制御音が放射され音の増大を引き起こす現象（スピルオーバーとも呼ばれる）が発生する．これは二次音源のスピーカの指向特性に起因する現象のため，制御領域のみに音を放射可能なスピーカが不可欠である．以上のように ANC の性能向上並びに適用範囲の拡大のためには ANC に適したスピーカの開発も不可欠である．

このように ANC 技術の更なる発展のためには，信号処理，制御工学，音響工学，センサ工学，機械学習など幅広い学問領域にわたる知識とそれらの融合が重要となる．よって，より多くの研究分野の研究者が参入することで大きなブレークスルーが期待される．拙著を通じて ANC 分野の研究に興味をもって頂き，当該分野が進展すればそれに勝る喜びはない．

文　献

(1) P.A. Nelson and S.J. Elliott, Active Control of Sound, Academic Press, London, 1992.
(2) S.M. Kuo and D.R. Morgan, Active Noise Control Systems: Algorithms and DSP Implementations, John Wiley & Sons, New York, 1996.
(3) S.J. Elliott, Signal Processing for Active Control, Academic Press, San Diego, 2001.
(4) Y. Kajikawa, W.S. Gan, and S.M. Kuo, "Recent advances on active noise control: Open issues and innovative applications," APSIPA Trans. Signal and Information Processing, vol.1, pp.1–21, Aug. 2012.
(5) J.C. Burgess, "Active adaptive sound control in a duct: A computer simulation," J. Acoust. Soc. Am., vol.70, pp.715–726, Sept. 1981.
(6) P. Joseph, S.J. Elliott, and P.A. Nelson, "Statistical aspects of active control in harmonic enclosed sound fields," Journal of Sound and Vibration, vol.172, no.5, pp.629–655, 1994.
(7) A. David and S.J. Elliott, "Numerical studies of actively generated quiet zones," Applied Acoustics, vol.41, no.1, pp.63–79, 1994.
(8) P. Joseph, S.J. Elliott, and P.A. Nelson, "Near field zones of quiet," Journal of Sound and Vibration, vol.172, no.5, pp.605–627, 1994.
(9) S.J. Elliott and J. Garcia-Bonito, "Active cancellation of pressure and pressure gradient in a diffuse sound field," Journal of Sound and Vibration, vol.186, no.4, pp.696–704, 1995.
(10) S.J. Elliott, I. Stothers, and P.A. Nelson, "A multiple error LMS algorithm and its application to the active control of sound and vibration," IEEE Trans. Acoust., Speech, Signal Process., vol.35, no.10, pp.1423–1434, 1987.
(11) P.A. Nelson, J.K. Hammond, P. Joseph, and S.J. Elliott, "Active control of stationary random sound fields," J. Acoust. Soc. Am., vol.87, no.3, pp.963–975, 1990.
(12) S.J. Elliott, P. Joseph, P.A. Nelson, and M.E. Johnson, "Power output minimization and power absorption in the active control of sound," J. Acoust. Soc. Am., vol.90, no.5, pp.2501–2512, 1991.
(13) S.J. Elliott, C.C. Boucher, and P.A. Nelson, "The behavior of a multiple channel active control system," IEEE Trans. Signal Process., vol.40, no.5, pp.1041–1052, May 1992.
(14) S.D. Snyder and C.H. Hansen, "Design considerations for active noise control systems implementing the multiple input, multiple output LMS algorithm," Journal of Sound and Vibration, vol.159, no.1, pp.157–174, 1992.
(15) C. Bao, P. Sas, and H.V. Brussel, "Adaptive active control of noise in 3-D reverberant enclosures," Journal of Sound and Vibration, vol.161, no.3, pp.501–514, 1993.
(16) S.J. Elliott and C.C. Boucher, "Interaction between multiple feedforward active control systems," IEEE Trans. Speech Audio Process., vol.2, no.4, pp.521–530, Oct. 1994.
(17) J. Guo and J. Pan, "Actively created quiet zones for broadband noise using multiple control sources and error microphones," J. Acoust. Soc. Am., vol.105, no.4, pp.2294–2303, April 1999.
(18) N. Tanaka and M. Tanaka, "Mathematically trivial control of sound using a parametric beam focusing source," J. Acoust. Soc. Am., vol.129, no.1, pp.165–172, 2011.
(19) J. Garcia-Bonito, S.J. Elliott, and C.C. Boucher, "Generation of zones of quiet using a virtual microphone arrangement," J. Acoust. Soc. Am., vol.101, no.6, pp.3498–3516, June 1997.
(20) B. Rafaely, S.J. Elliott, and J. Garcia-Bonito, "Broadband performance of an active headrest," J. Acoust. Soc. Am., vol.106, no.2, pp.787–793, Aug. 1999.
(21) C.D. Kestell, B.S. Cazzolato, and C.H. Hansen, "Active noise control in a free field with virtual sensors," J. Acoust. Soc. Am., vol.109, no.1, pp.232–243, Jan. 2001.
(22) M. Pawelczyk, "Multiple input-multiple output adaptive feedback control strategies for the active headrest system: design and real-time implementation," International Journal of Adaptive Control and Signal Processing, vol.17, no.10, pp.785–800, 2003.
(23) M. Pawelczyk, "Adaptive noise control algorithms for active headrest system," Control Engineering Practice, vol.12, no.9, pp.1101–1112, 2004.
(24) J. Yuan, "Virtual sensing for broadband noise control in a lightly damped enclosure," J. Acoust. Soc. Am.,

vol.116, no.2, pp.934–941, Aug. 2004.
(25) C.D. Petersen, A.C. Zander, B.S. Cazzolato, and C.H. Hansen, “A moving zone of quiet for narrowband noise in a one-dimensional duct using virtual sensing,” J. Acoust. Soc. Am., vol.121, no.3, pp.1459–1470, March 2007.
(26) D. Moreau, B. Cazzolato, A. Zander, and C. Petersen, “A review of virtual sensing algorithms for active noise control,” Algorithms, vol.1, no.2, pp.69–99, Nov. 2008.
(27) D.J. Moreau, J. Ghan, B.S. Cazzolato, and A.C. Zander, “Active noise control in a pure tone diffuse sound field using virtual sensing,” J. Acoust. Soc. Am., vol.125, no.6, pp.3742–3755, June 2009.
(28) S.J. Elliott and J. Cheer, “Modeling local active sound control with remote sensors in spatially random pressure fields,” J. Acoust. Soc. Am., vol.137, no.4, pp.1936–1946, April 2015.
(29) N. Miyazaki and Y. Kajikawa, “Head-mounted active noise control system with virtual sensing technique,” Journal of Sound and Vibration, vol.339, no.Supplement C, pp.65–83, 2015.
(30) S. Ryu and Y.-S. Lee, “Characteristics of relocated quiet zones using virtual microphone algorithm in an active headrest system,” Journal of Sensors, vol.2016, pp.1–9, 2016.
(31) S. Edamoto, C. Shi, and Y. Kajikawa, “Virtual sensing technique for feedforward active noise control,” Proceedings of Meetings on Acoustics, vol.29, pp.1–10, 2016.
(32) W. Jung, S.J. Elliott, and J. Cheer, “Combining the remote microphone technique with head-tracking for local active sound control,” J. Acoust. Soc. Am., vol.142, no.1, pp.298–307, 2017.
(33) J. Cheer, S.J. Elliott, E. Oh, and J. Jeong, “Application of the remote microphone method to active noise control in a mobile phone,” J. Acoust. Soc. Am., vol.143, no.5, pp.2142–2151, 2018.
(34) W. Jung, S.J. Elliott, and J. Cheer, “Estimation of the pressure at a listener’s ears in an active headrest system using the remote microphone technique,” J. Acoust. Soc. Am., vol.143, no.5, pp.2858–2869, 2018.
(35) S.J. Elliott, W. Jun, and J. Cheer, “Causality and robustness in the remote sensing of acoustic pressure with application to local active sound control,” 2019 IEEE International Conference on Acoustics, Speech and Signal Processing, pp.8484–8488, 2019.
(36) C. Shi, R. Xie, N. Jiang, H. Li, and Y. Kajikawa, “Selective virtual sensing technique for multi-channel feedforward active noise control systems,” 2019 IEEE International Conference on Acoustics, Speech and Signal Processing, pp.8489–8493, 2019.
(37) C. Shi, Z. Jia, R. Xie, and H. Li, “An active noise control casing using the multi-channel feedforward control system and the relative path based virtual sensing method,” Mechanical Systems and Signal Processing, vol.144, 106878, Oct. 2020.
(38) J. Zhang, S.J. Elliott, and J. Cheer, “Robust performance of virtual sensing methods for active noise control,” Mechanical Systems and Signal Processing, vol.152, 107453, 2021.
(39) J. Zhang, T.D. Abhayapala, W. Zhang, P.N. Samarasinghe, and S. Jiang, “Active noise control over space: A wave domain approach,” IEEE/ACM Trans. Audio, Speech, Language Process., vol.26, no.4, pp.774–786, 2018.
(40) B. Bu, C.-C. Bao, and M.-S. Jia, “Design of a planar first-order loudspeaker array for global active noise control,” IEEE/ACM Trans. Audio, Speech, Language Process., vol.26, no.11, pp.2240–2250, 2018.
(41) Y. Maeno, Y. Mitsufuji, P.N. Samarasinghe, N. Murata, and T.D. Abhayapala, “Spherical-harmonic-domain feedforward active noise control using sparse decomposition of reference signals from distributed sensor arrays,” IEEE/ACM Trans. Audio, Speech, Language Process., vol.28, pp.656–670, 2020.
(42) S. Koyama, J. Brunnström, H. Ito, N. Ueno, and H. Saruwatari, “Spatial active noise control based on kernel interpolation of sound field,” IEEE/ACM Trans. Audio, Speech, Language Process., vol.29, pp.3052–3063, 2021.
(43) K. Arikawa, S. Koyama, and H. Saruwatari, “Spatial active noise control based on individual kernel interpolation of primary and secondary sound fields,” 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2022), pp.1056–1060, 2022.
(44) P. Lueg, “Process of silencing sound oscillations,” U. S. patent 2043416, June 1936.
(45) X. Kong and S.M. Kuo, “Study of causality constraint on feedforward active noise control systems,” IEEE Trans. Circuits Syst., vol.46, no.2, pp.183–186, Feb. 1999.
(46) M. Nishimura, K. Nishikage, T. Murao, and N. Wada, “Development of ANC unit with a set of co-located reference microphone and control speaker,” Proc. JSME Environmental Engineering Symposium 2010, Kanagawa, Japan, no.114, pp.50–53, June 2010 (in Japanese).
(47) T. Miyake, K. Iwai, and Y. Kajikawa, “Head-mounted multi-channel feedforward active noise control system for reducing noise arriving from various directions,” IEEE Access, vol.11, pp.6935–6943, 2023.
(48) D. Shi, W.-S. Gan, B. Lam, and S. Wen, “Feedforward selective fixed-filter active noise control: Algorithm and implementation,” IEEE/ACM Trans. Audio, Speech, Language Process., vol.28, pp.1479–1492, 2020.
(49) Z. Luo, D. Shi, and W.-S. Gan, “A hybrid SFANC-FxNLMS algorithm for active noise control based on deep learning,” IEEE Signal Process. Lett., vol.29, pp.1102–1106, 2022.
(50) D. Shi, B. Lam, K. Ooi, X. Shen, and W.-S. Gan, “Selective fixed-filter active noise control based on convolutional neural network,” Signal Processing, vol.190, 108317, 2022.

（幹事団提案，2023 年 2 月 25 日受付，
2023 年 3 月 18 日再受付）

梶川嘉延（正員：フェロー）

1991 関西大学工学部電子工学科卒．1993 同大学大学院工学研究科電子工学専攻博士課程前期課程修了．同年富士通（株）入社．1994 関西大学工学部電子工学科助手．1998 同大専任講師．2001 助教授．2007 同大学システム理工学部准教授．2009 教授．主に，アクティブノイズコントロール，パラメトリックスピーカなどにおける信号処理技術の研究に従事．博士（工学）．IEEE Senior Member，APSIPA，EURASIP，ASA，日本音響学会各会員．2016 年度本会 ESS 副会長，2022 年度次期 ESS 会長，2018～2021 年 APSIPA Vice President (Member Relations and Development)，2016～2017 年及び 2022 年より APSIPA BoG member，2015～2016 年 IEEE Signal Processing Society Kansai Chapter Chair，2014 年度本会信号処理研究専門委員会委員長，2021 年度本会応用音響研究専門委員会委員長．2016 年より IET Signal Processing Associate Editor，2006～2010 年本会和文論文誌 A 編集委員，2005～2017 年日本音響学会編集委員，2019～2020 年本会英文論文誌 A 編集委員長．2012 年日本音響学会佐藤論文賞，2017 年 APSIPA Sadaoki Furui Prize Paper Award，2020 年本会論文賞など多数受賞．

解　説　論　文

超高感度低消費電力 MEMS 加速度センサとその応用

Extremely-High-Sensitivity Low-Power MEMS Accelerometer and Its Applications

大島　俊 Takashi OSHIMA

アブストラクト　加速度センサは，スマートフォンやゲーム機から，車やロボット，ドローンまで，幅広く用いられている．なかでも，量産化や小型化に適した MEMS 型の加速度センサは，今後も多くのアプリケーションが期待される．しかし，MEMS 加速度センサには，様々なノイズが内在しているため，低消費電力で高感度を実現するのは容易でなかった．近年，筆者らは，超高感度（極低ノイズ）と低消費電力を両立した MEMS 加速度センサの開発に成功した．本稿では，センサの仕組みや，センサに適用したブレークスルー技術を説明し，更に，センサの新しい応用事例も紹介する．

キーワード　加速度センサ，振動センサ，MEMS，高感度，低電力

Abstract　Accelerometers are used for many applications from smartphones and game consoles to automobiles, robots and drones. In particular, MEMS-based accelerometers are promising for many future applications since they are suitable for mass production and easy to implement in a small device. However, conventional MEMS accelerometers suffer from various noise contributors and hence, it was not easy to attain high sensitivity and low power consumption simultaneously. Recently, we have successfully developed a MEMS accelerometer with both extremely high sensitivity (ultralow noise) and low power consumption. In this article, the operation principle of the accelerometer and several key techniques, as well as new application are explained.

Key words　Accelerometer, Vibration sensor, MEMS, High sensitivity, Low power

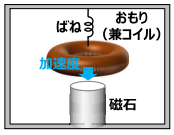
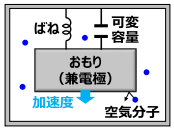
1.　MEMS 加速度センサのニーズ

加速度センサは，物体の加速度を検知するセンサで，これにより物体の動きや傾きを知ることができる．そのため，スマートフォンやゲーム機から，車，ロボット，ドローンまで，幅広く利用されている．また，振動にともなう加速度を検出することで，振動も検知できる．そのため，地震計や地下資源の探査にも用いられている．特に次世代の資源探査では，地表に多数のセンサを配置して，ごく微小な振動を検知する必要があり，そのために，高感度かつ小型，軽量のセンサが求められている．

従来の資源探査では，ジオフォンと呼ばれるタイプの振動センサが用いられている．しかし，近年は，量産化と小型化に適した静電容量方式の MEMS(注1) 型の加速度センサ[(1)~(9)]が注目されており，表 1 にジオフォンと比較して示す．なお，MEMS 型の加速度センサには，静電容量方式以外にピエゾ抵抗方式などもある．ピエゾ抵抗方式は，特に小型化や低コスト化に適しているが，精度上の課題があるため，本稿では静電容量方式を扱う．

加速度センサの高感度化，すなわち，より小さな加速度を検出できるためには，センサの低ノイズ化が必要である．また，センサの小型化には，電池の小型化も必要になり，そのために，センサの低消費電力化が求められる．しかし，これまでの MEMS 加速度センサでは，次世代の資源探査や今後の新しいアプリケーションで望まれるような極めて小さなノ

表 1　ジオフォンと MEMS 加速度センサの比較　MEMS 加速度センサは，量産化や小型化に適しているが，低ノイズ化と低消費電力化の両立に課題がある．

	ジオフォン	MEMS加速度センサ
構造		
ノイズ及び消費電力	☺ 良好	☹ 両立が難しい
サイズ	☹ 大きい	☺ 小さい
量産化	☹ 課題あり	☺ 適している

（注 1）：Micro Electro Mechanical Systems（微小電気機械システム）．微細加工技術を用いて，電気的な動作を行う素子と機械的な動作を行う素子を一つの基板上に集積したデバイス．

大島俊　正員　株式会社日立製作所
E-mail　takashi.oshima.yp@hitachi.com
Takashi OSHIMA, Member (Hitachi, Ltd., Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.44-51 2023 年 7 月

イズと，電池駆動が可能なほどの十分な低消費電力を両立するのは困難であった．

近年，筆者らのグループは，極低ノイズと低消費電力を両立する MEMS 加速度センサを開発できた[10]～[12]．本稿では，センサの仕組み，各ブレークスルー技術，並びに，センサの新しいアプリケーション事例を紹介する．

2. MEMS 加速度センサの動作

加速度センサは，加速度を検知したい物体に設置して用いる．MEMS 加速度センサは，加速度を検出するセンサ部を，シリコンの微細加工技術による MEMS デバイスを用いて実現している．MEMS センサ部は機械的には錘（おもり）の役割を果たす．加速度が印加された際に，錘に対して加速度に比例した慣性力(注2)がはたらき，これによる変位を検出することで，加速度の大きさが分かる．MEMS センサ部は，機械的には錘の役割を果たすが，電気的には，変位を検出するための静電容量素子としてもはたらく．

MEMS センサ部は，様々な形態で実装できる．例えば，図 1 に示すようなシーソー構造の実装も可能である[11], [12]．同図のように，シーソーの左側よりも右側の質量を重くしている．これにより，加速度が印加された際に，右側の錘にはたらく慣性力のほうが左側の錘にはたらく慣性力より大きくなる．その結果，正味の慣性力として，図の時計回りの方向に回転させる力がはたらき，シーソーの回転軸を中心として回転する．

左側と右側の錘には，それぞれ下部表面に電極が形成されており，また，フレーム上の対向する位置にも電極がある．これにより，左右それぞれの側に，錘の変位に追従する可動電極とフレーム上の固定電極による静電容量素子が形成される．例えば，図のように時計回りの方向に錘が変位（回転）した場合は，左側の容量素子の電極間距離が，右側の容量素子の電極間距離より大きくなるため，結果として，左側の容量素子のほうが右側の容量素子よりも容量値が小さくなる．

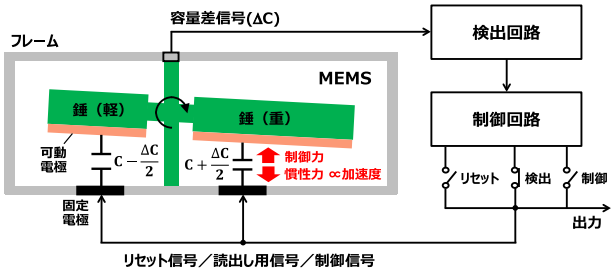


図 1　従来の MEMS 加速度センサの構成と動作　　MEMS は錘の役割と電極の役割を兼ねている．シーソー構造の錘で加速度を検出する．動作の安定化のため，検出と制御を交互に行う．

(注 2)：フレームに加速度が印加された際に，フレーム内の孤立した質量がある物体（本センサの場合は，錘）にはたらく見かけの力．

この左右の容量値の差（ΔC）を検出することで，加速度の大きさが分かる．ΔC を電圧として検出するために，固定電極に読出し用信号（パルス電圧）を印加する．

高感度の MEMS 加速度センサを実現するためには，センサの低ノイズ化に加えて，シーソーの回転軸に内在するねじりばねをできるだけ柔らかくする必要がある．これにより，同じ慣性力（すなわち，同じ大きさの加速度の印加）に対して，より大きな変位（より大きな ΔC）を生じさせることができる．しかしながら，その結果として，錘の運動が不安定になりがちになる．したがって，動作を安定化させるために，変位（回転）を引き起こそうとする慣性力と同じ大きさの力を逆向きに印加して，錘の変位をゼロ付近に制御することが必要である．この制御力は，電極間に静電気力を発生させることで実現する．そのため，フレーム上の固定電極には，適切な静電気力を発生させるための制御電圧も印加する必要がある．

以上から，図 1 のように固定電極に対して，ΔC 検出用の期間には読出し用信号を印加し，制御用の期間には制御信号を印加することを交互に繰り返す「時分割動作」が知られている．なお，上記の制御により ΔC は常にゼロ付近にコントロールされるため，実際の加速度は ΔC から求めることはできないものの，制御電圧から求められる．制御電圧は，慣性力（したがって，印加された加速度）と釣り合うように生成されており，加速度に比例しているためである．

上記の時分割動作では，ΔC 検出用期間と制御用期間に加えて，両期間を分離するためのリセット期間も必要である．この時分割動作により制御用期間が 1/3 になるため，実効的な制御力が低下してしまう．制御力を十分に確保しようとすると，制御電圧を高める必要があるため，消費電力が増加してしまう．以上のように，本章では従来の MEMS 加速度センサの動作について紹介した．次章では，MEMS 加速度センサの低ノイズ化と低消費電力化を両立するためのキー技術を述べる．

3. 低ノイズ低電力加速度センサのキー技術

3.1 MEMS センサ部の低ノイズ化

MEMS 加速度センサを高感度化するためには，MEMS センサ部のノイズ（機械的ノイズ）と回路のノイズ（電気的ノイズ）の双方を低減する必要がある．図 2 に，MEMS センサ部のノイズを低減する構造を示す[11], [12]．MEMS センサ部のノイズは，フレーム内の空気分子が左右の錘と衝突することで発生する．そのため，従来は，フレーム内を高真空に封じることで，空気分子との衝突を極力回避していた．しかし，実装コストが上昇する課題がある．そこで，図 2 では，錘を上下に貫く貫通孔を多数開けて，空気分子を孔から逃がす構造としている．

これにより衝突の機会が減少し，高い真空度でなくても MEMS センサ部の低ノイズ化を達成できた．また，左側の

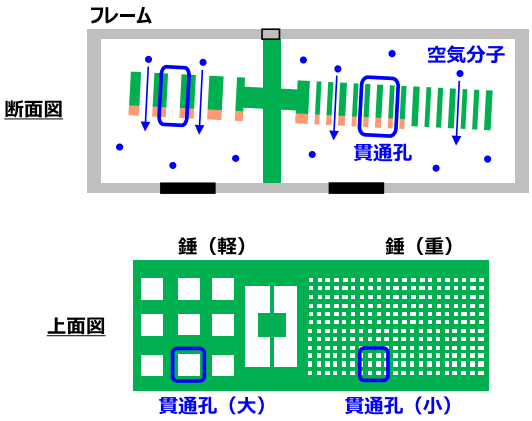


図 2　低ノイズ化を実現する MEMS センサ部の構造　　錘に開けた貫通孔から空気分子を逃がすことで，機械的ノイズを低減している．孔の大きさに差をつけて，左右の錘の質量差を拡大している．

錘の孔を右側の錘の孔より大きくすることで，シーソー型構造に必要な左右の錘の質量差を確保することができた．

3.2　検出と制御の同時動作を実現する MEMS 構造

従来は先述のとおり，時分割動作にともない MEMS 加速度センサの消費電力が増大する課題があった．MEMS 加速度センサの低消費電力化を実現するために，図 3(a)のように，容量差 ΔC の検出と錘の制御を同時に行う方法が考えられる．時分割動作でないため，検出用の電極と制御用の電極が個別に必要となっている．

しかし，図 3(a)の構成で検出と制御を同時に行うと，制御信号が錘を介して漏洩し，容量差信号（ΔC）に重畳してしまう．そのため，容量差信号を検出できなかったり，動作が不安定になったりしてしまう．そこで，図 3(b)のように，検出部と制御部の間を電気的に絶縁する対策が重要であった[10),11)]．これにより制御信号を絶縁部で遮断し，漏洩を本質的に回避することができた．このように，検出部と制御部は機械的には結合され，一体化した錘として振る舞う一方，電気的には絶縁されているというユニークな構造が，検出と制御の同時動作とそれによる低消費電力化を可能にした．

3.3　残留漏洩をキャンセルする検出回路

MEMS 加速度センサの低ノイズ化には，検出回路の低ノイズ化も必須である．検出回路は，容量差信号 ΔC を電圧信号に変換する容量電圧変換アンプ，フィルタ，その出力をディジタル信号に変換する A-D 変換器[注3)]などを含む．したがって，容量電圧変換アンプは低ノイズに設計され，A-D 変換器は高分解能である必要がある．

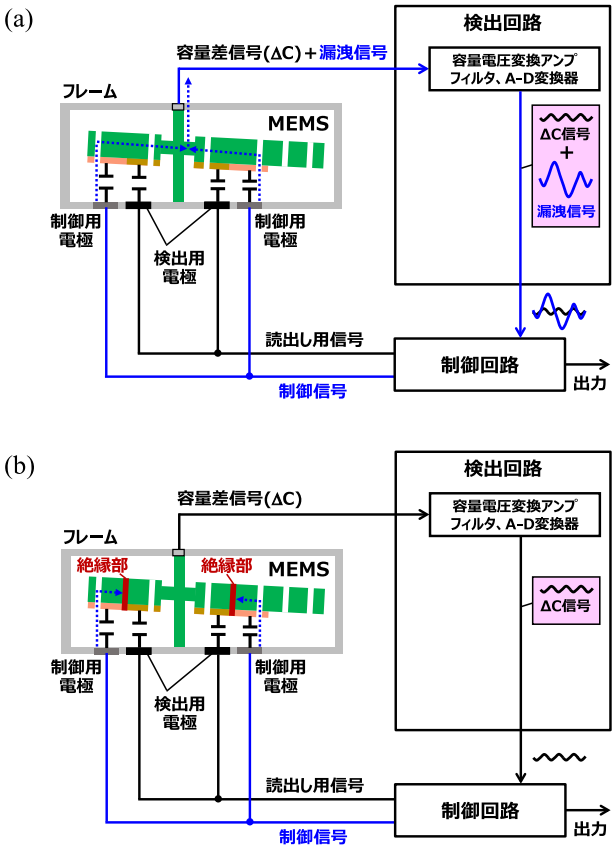


図 3　検出と制御を同時に行う MEMS 加速度センサ　　(a)検出部と制御部の絶縁なし．(b)絶縁あり．検出用と制御用に個別に電極を備え，検出と制御を同時に行い，低消費電力化している．検出部と制御部の間を絶縁して，制御信号の漏洩を阻止する．

更に，図 3(b)の絶縁対策をもってしても，現実には，図 4(a)のように，制御信号を印加する配線と容量差信号 ΔC を取り出す箇所との間の寄生容量を介して，制御信号の漏洩が残存している．この残留漏洩は，たとえ軽微であっても，極低ノイズをねらう加速度センサには依然として影響を及ぼす．

これに対して，図 4(b)のように，上記の残留漏洩を検出回路の中でキャンセルする対策が効果的であった[10)]．残留漏洩は，制御回路自身が生成している制御信号に起因することが分かっている．そこで，その制御信号を引き出してきて，検出回路のフィルタの周波数特性を模擬したディジタルフィルタを通す．これにより残留漏洩の波形を模倣できる．その上で，漏洩強度を乗算し，A-D 変換器のディジタル出力から減算することで，残留漏洩をキャンセルした．また，漏洩強度は図 4(b)の寄生容量の大きさで決まり，あらかじめ正確に把握することは難しいため，キャンセル後の漏洩がゼロとなるように自動調整した．

(注 3)：アナログディジタル変換器．アナログ信号（連続的な電圧波形）をディジタル信号（数値の並び）に変換する回路．

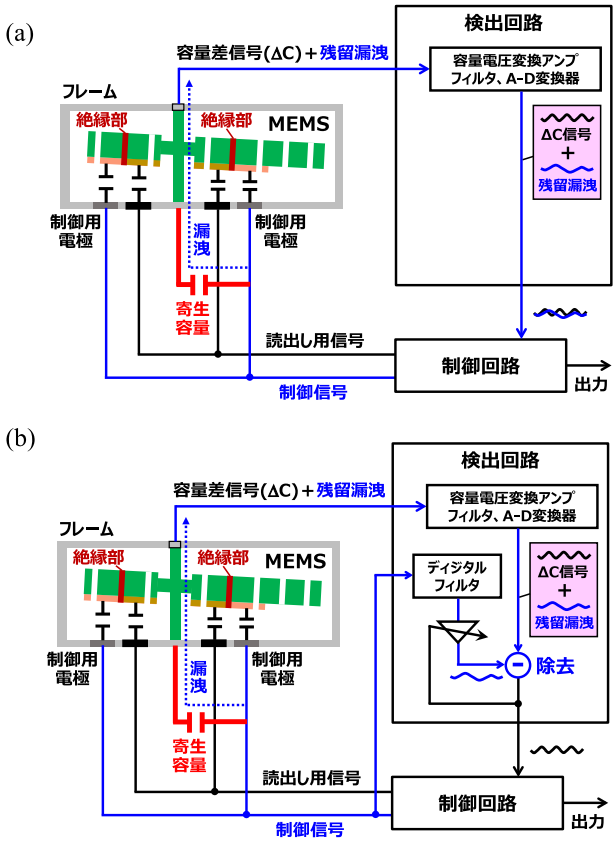


図 4　寄生容量を介した残留漏洩とその対策　(a)キャンセル回路なし．(b)キャンセル回路あり．寄生容量を介した制御信号の漏洩が残存しているため，検出回路内でディジタル処理によりキャンセルしている．

3.4　新たなノイズ生成を避ける制御回路の工夫

制御回路は，検出された容量差信号 ΔC に基づき，ΔC がゼロになるように（すなわち，錘の変位がゼロになるように）制御信号を生成する役割がある．制御信号の生成は PID 制御(注4)により行う．PID 制御で生成された信号をそのまま D-A 変換器(注5)を用いてアナログ信号に変換して MEMS の制御用電極に印加することも考えられる．しかし，高精度の D-A 変換器が必要になり，設計が容易ではない．そのため，代替手段として，PID 制御で生成された制御信号を，図 5(a)のように 1 bit 量子化器(注6)により 2 値（1 bit）の制御信号に変換する方法が知られている．1 bit 量子化器は，入力が正であれば＋1 を，負であれば－1 を出力する．

(注 4)：Proportional Integral Differential 制御．誤差信号（本センサの場合は，ΔC）がゼロになるように，誤差信号と，その積分，及び微分を用いて制御信号を生成するフィードバック制御方法．

(注 5)：ディジタルアナログ変換器．ディジタル信号（数値の並び）をアナログ信号（連続的な電圧波形）に変換する回路．

(注 6)：入力される値を，より少ないビット数での表現に丸めて出力する回路．

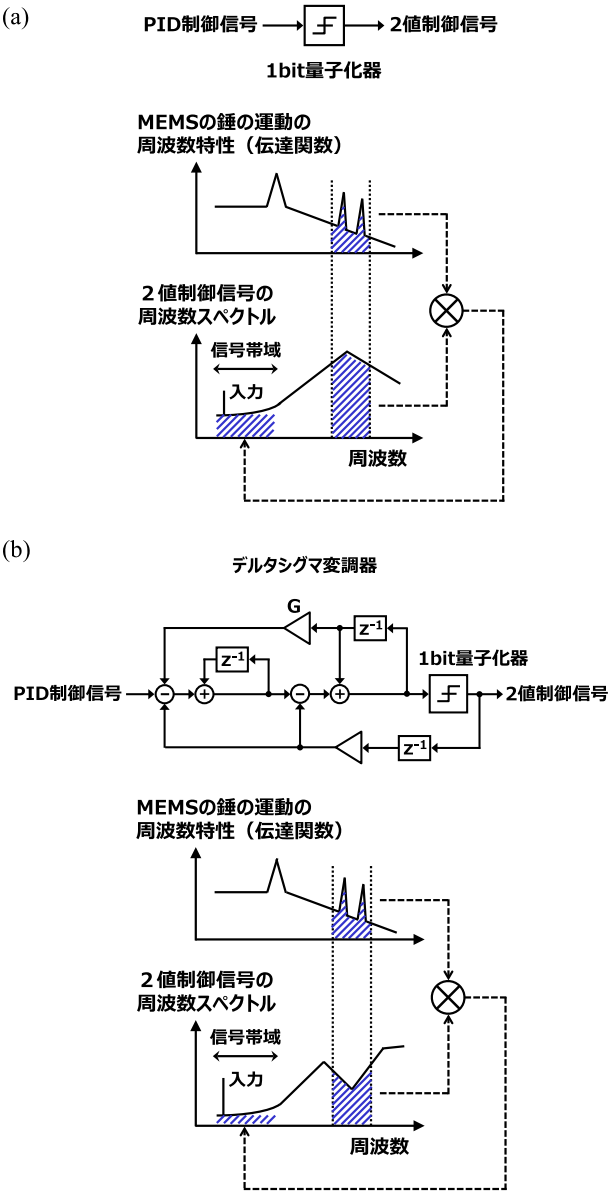


図 5　2 値制御信号の生成方法[10]　(a)単純な 2 値化．(b)デルタシグマ変調器の適用．制御回路の実装を容易にするため，制御信号を 2 値化する．単純な 2 値化では，新たなノイズが生成されるため，デルタシグマ変調器を用いて 2 値化している．

この 2 値化の際にランダムな丸め誤差（量子化誤差）が大量に発生する．しかし，PID 制御の恩恵により，上記の量子化誤差は，同図の 2 値制御信号の周波数スペクトルに見られるように，高周波領域に拡散されることが知られている[2]．そのため，低周波の信号帯域には影響を及ぼさないと期待される．

しかし，実際は，この方法では，極低ノイズの MEMS 加速度センサを実現するのは困難であった．その理由の根本は，上記した MEMS の錘が一体の完全な剛体ではなく，実際には僅かに湾曲運動したり，接合部に付随した運動をともなったりすることにある．これらの副次的な運動に対応して，MEMS の錘の運動の周波数特性（伝達関数）には，図

5(a)のように，高次共振ピークが多数存在する．一方で，先に述べたとおり，2 値制御信号の高周波領域には大量の量子化誤差が分布している．理論的な検討の結果，MEMS の高次共振ピークと 2 値制御信号の量子化誤差が多く分布する周波数領域が重なると，両者の相互作用により低周波領域（信号帯域）に，新たなノイズが生成されてしまうことが分かった[10]．

そこで，図 5(b)のように，制御信号をデルタシグマ変調器[注7]を用いて 2 値化することが有効な対策となった[10]．単純な 2 値化の場合と比較して，デルタシグマ変調のために，乗算，加減算，遅延処理（z^{-1} の記号）が追加で必要になる．デルタシグマ変調器内のパラメータ「G」を適切に調整することで，同図のように，MEMS の高次共振ピーク付近の高周波領域における 2 値制御信号の量子化誤差の分布に谷間を作ることができる．これにより，信号帯域内への新たなノイズ生成を抑制することができた．

なお，2 章において，加速度は制御電圧値から求められると述べた．実際には上記のように制御信号は 2 値化されているため，加速度は 2 値制御信号の平均値から求めている．以上のように，MEMS センサ部，検出回路，制御回路の各々に工夫をすることで，極低ノイズかつ低消費電力の MEMS 加速度センサを実現できた．

3.5　MEMS 加速度センサの評価結果

以上で紹介した各技術を搭載した MEMS 加速度センサを試作し，評価実験を行った．図 6 のように，試作した MEMS 加速度センサは，MEMS センサ部チップ，検出回路チップ，制御回路チップから構成されている．

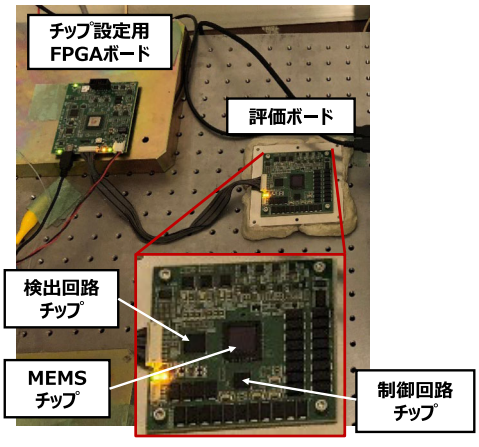


図 6　試作した MEMS 加速度センサ及び評価系　　試作したセンサは，紹介した各技術を搭載しており，MEMS センサ部チップ，検出回路チップ，制御回路チップから構成されている．

（注 7）：量子化器と同様に，入力される値を，より少ないビット数での表現に丸めて出力する回路で，更に，丸めの際に生じる誤差（量子化誤差）が高周波領域に拡散されるように工夫したもの．

加速度センサのノイズレベルは，加速度を印加しない状態で，センサ出力の周波数スペクトルを取得することで評価できる．極低ノイズのセンサを評価するためには，環境振動による加速度印加を極力回避する必要があるため，専用の施設で評価実験が行われた．これにより得られた本センサの出力の周波数スペクトルを図 7 に示す．10 Hz 以下の値の上昇や高周波側でのピークは，環境の振動に起因すると考えられる．環境振動の影響が少ない周波数領域の解析結果から，試作した MEMS 加速度センサのノイズレベルは 22 ng/$\sqrt{\text{Hz}}$ (22×10^{-9} g/$\sqrt{\text{Hz}}$) となった．ここで，1 g は重力加速度（9.8 m/s^2）であり，MEMS 加速度センサとしてトップクラスの低ノイズを実証した．

試作した MEMS 加速度センサに加速度を印加した評価も行った．図 8 は，環境のランダムな振動を，試作した MEMS 加速度センサと専用の地震計でそれぞれ検出した出力波形を示している．同図のように，両者の結果はよく一致しており，MEMS 加速度センサの加速度検知動作を確認することができた．

試作した MEMS 加速度センサは，極めて低ノイズであるため，ごく僅かな振動も検知することができる．図 9 は，そ

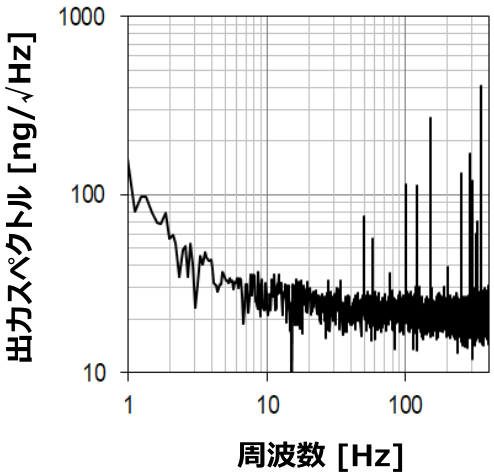


図 7　MEMS 加速度センサのノイズ評価結果[10]　　加速度を印加しない状態で，センサ出力の周波数スペクトルを取得し，ノイズレベルを評価した．22 ng/$\sqrt{\text{Hz}}$ の極低ノイズを達成した．

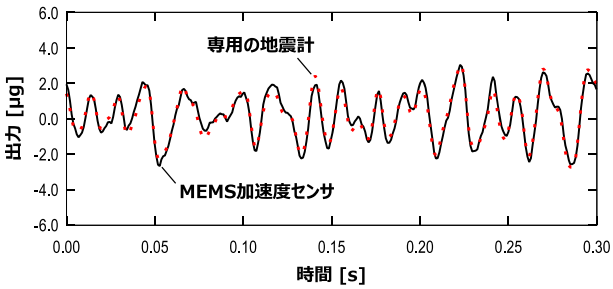


図 8　MEMS 加速度センサの出力波形の評価結果[10]　　環境のランダムな振動を，試作したセンサと専用の地震計でそれぞれ検出した．両者の結果はよく一致している．

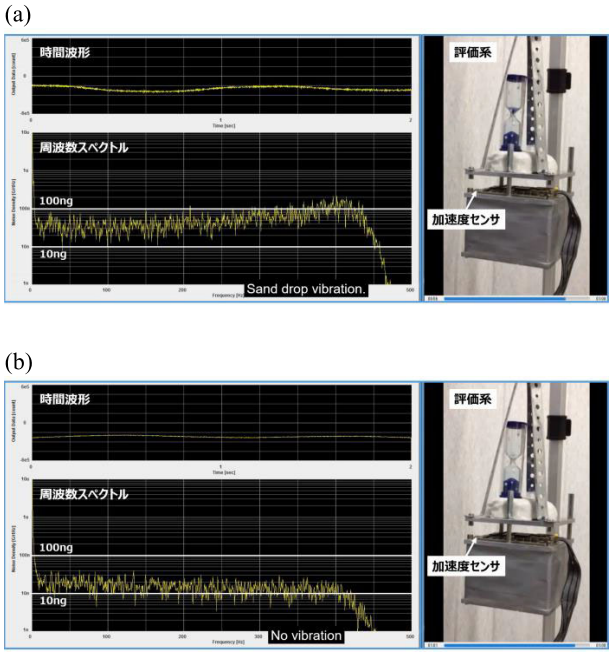


図 9　砂時計を滑り落ちる砂粒による振動の検出　　(a)砂粒落下中のセンサ出力．(b)落下後の出力．試作した MEMS 加速度センサは，極めて低ノイズであるため，砂時計内を落下する砂粒が引き起こすごく僅かな振動を検出できた．

のデモンストレーションを行ったもので，試作した MEMS 加速度センサを用いて，砂時計内を滑り落ちる砂粒が引き起こす僅かな振動の検出を試みた．図 9(a)は，砂粒が滑り落ちている最中のセンサの出力を，時間波形と周波数スペクトルで表示している．これに対して，図 9(b)は，砂粒が落ち切った後の静かな状態でのセンサの出力である．図 9(a)のほうが，時間波形の変動も周波数スペクトルの強度も大きくなっており，砂粒の落下が引き起こす軽微な振動を加速度として検出できていることが分かった．

4.　低ノイズ低電力加速度センサの応用

試作した MEMS 加速度センサは，17 mW の低消費電力動作を実現できたため，電池で動作できる．また，ノイズレベルは先述のとおり 22 ng/$\sqrt{\text{Hz}}$ と極低ノイズとなった．図 10 に，ほかの MEMS 加速度センサと比較してプロットした．本センサは，極低ノイズと低消費電力を両立した新たな領域を切り拓いていることが示されている．従来の多くの加速度センサは，図 11 のように，ショック検知や傾き検知などに用いられており，求められるノイズレベルはそれほど厳しくないため，小型，軽量，低コストで実現することが可能であった．一方で，次世代の資源探査や環境振動の計測など，極低ノイズが要求される用途もあり，本センサは好適である．しかし，それ以上に期待されるのは，新しいアプリケーションの創出である．

その一例は，低ノイズかつ低消費電力の MEMS 加速度センサを用いた漏水検知システムである[13),(14)]．このシステム

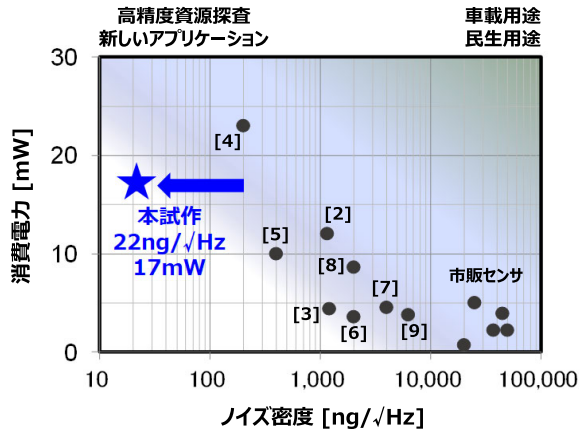


図 10　MEMS 加速度センサの比較（ノイズ vs. 電力）　　試作した MEMS 加速度センサは，22 ng/$\sqrt{\text{Hz}}$ の極低ノイズを 17 mW の低消費電力で実現し，MEMS 加速度センサの新しい領域を切り拓いた．図中に対応する文献の番号も示した．

図 11　加速度センサに望まれるノイズレベル　　加速度センサは，ショック検知や傾き検知から，資源探査や環境振動の計測まで，幅広い用途があり，要求されるノイズレベルも異なる．

では，地下の水道管の漏水にともなう振動状態の変化を，MEMS 加速度センサを用いて検出している．センサが低ノイズであり，僅かな振動状態の変化を検出できるとともに，低消費電力であるため，センサを電池で駆動することができる．

低ノイズの加速度センサは，地震の検知にも使用できる．図 12 は，試作した MEMS 加速度センサの長時間評価中に，震度 1 の地震が発生し，センサの出力にその振動をとらえた様子を示している．非常に多くの MEMS 加速度センサを簡易地震計としてフィールドに展開できれば，防災に貢献できるかもしれない．

最後に，試作した MEMS 加速度センサを用いて，人の活動量のモニタを試行した例を紹介する．極低ノイズの加速度センサであれば，人の活動による建物の振動状態のわずかな変化を検出できるのではと期待した試みである．研究所の建屋内に試作した MEMS 加速度センサを設置して，得られた

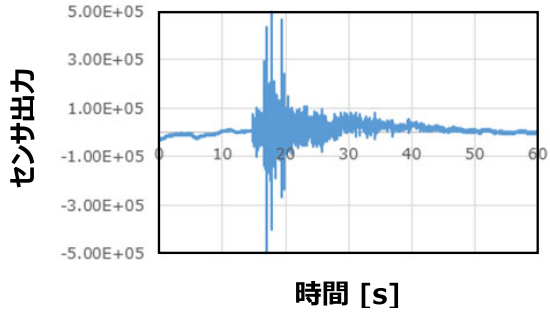


図 12　本センサによる震度 1 の地震の検知の様子　　試作した MEMS 加速度センサで，震度 1 の地震を検知することができた．MEMS 加速度センサは，簡易地震計になり得るかもしれない．

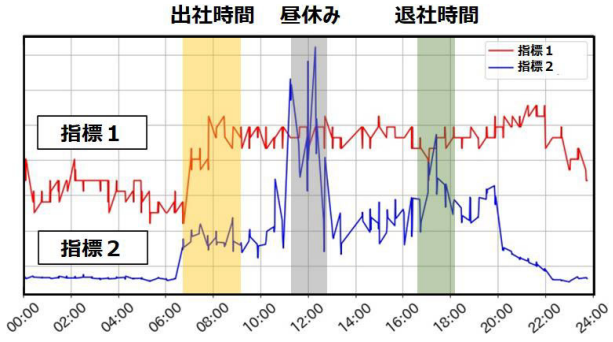


図 13　本センサを用いた人の活動量のモニタの一例　　試作した MEMS 加速度センサを用いて，人の活動量をモニタすることができた．MEMS 加速度センサにより，新しいアプリケーションを創生できるかもしれない．

センサ出力を 2 種類の指標で変換して，図 13 のようにプロットした．特に指標 2 を適用した場合は，人の行動との相関がよく現れている．このように，低ノイズかつ低消費電力の MEMS 加速度センサは，今後，様々な新しい用途に活用できると期待される．

5. ま と め

MEMS 加速度センサは，量産化や小型化に適しているが，高感度化（低ノイズ化）と低消費電力化の両立は，従来困難であった．本稿では，試作した低ノイズかつ低消費電力の MEMS 加速度センサを事例として，様々な技術課題とそれらを克服するためのブレークスルー技術を紹介した．また，このような低ノイズ低消費電力の MEMS 加速度センサは，新しいアプリケーションを創生できる可能性を秘めており，幾つかの事例を紹介した．

文　献

(1) 相澤隆生，国見敬，伊東俊一郎，他，“地震探査用 MEMS 受振器の開発，”応用地質，vol. 59, no. 2, pp. 84-93, 2018.

(2) M. Pastre, M. Kayal, H. Schmid, et al., “A 300 Hz 19b DR capacitive accelerometer based on a versatile front end in a 5th-order ΔΣ loop,” 2009 Proceedings of ESSCIRC, pp. 288-291, Athens, Greece, 2009, doi: 10.1109/ESSCIRC.2009.5326033.

(3) X. Wang, J. Zhao, Y. Zhao, et al., “27.2 A1.2 μg/$\sqrt{\text{Hz}}$ -resolution 0.4 μg-bias-instability MEMS silicon oscillating accelerometer with CMOS readout circuit,” 2015 IEEE ISSCC Dig. Tech. Papers, pp. 476-477, San Francisco, CA, USA, 2015, doi:10.1109/ISSCC.2015.7063133.

(4) H. Xu, X. Liu, and L. Yin, “A closed-loop ΣΔ interface for a high-Q micromechanical capacitive accelerometer with 200 ng/ $\sqrt{\text{Hz}}$ input noise density,” IEEE J. Solid-State Circuits, vol. 50, no. 9, pp. 2101-2112, Sept. 2015, doi: 10.1109/JSSC.2015.2428278.

(5) H. Xu, J. Wu, H. Zhang, et al., “A 10 mW, 0.4 μg/$\sqrt{\text{Hz}}$, 700 Hz ΣΔ high-order electromechanical modulator for a high-Q micromechanical capacitive accelerometer,” IEEE Sensors J., vol. 18, no. 3, pp. 1187-1194, 1 Feb., 2018, doi:10.1109/JSEN.2017.2780279.

(6) M. Yucetas, M. Pulkkinen, A. Kalanti, et al., “A high-resolution accelerometer with electrostatic damping and improved supply sensitivity,” IEEE J. Solid-State Circuits, vol. 47, no. 7, pp. 1721-1730, July 2012, doi: 10.1109/JSSC.2012.2191675.

(7) B. Amini, R. Abdolvand, and F. Ayazi, “A 4.5-mW closed-loop ΔΣ micro-gravity CMOS SOI accelerometer,” IEEE J. Solid-State Circuits, vol. 41, no. 12, pp. 2983-2991, Dec. 2006, doi:10.1109/JSSC.2006.884864.

(8) M. Yucetas, J. Salomaa, A. Kalanti, et al., “A closed-loop SC interface for a ±1.4 g accelerometer with 0.33% nonlinearity and 2 μg/$\sqrt{\text{Hz}}$ input noise density,” 2010 IEEE ISSCC Dig. Tech. Papers, pp. 320-321, San Francisco, CA, USA, 2010, doi:10.1109/ISSCC.2010.5433899.

(9) D. Zhao, M. Zaman, and F. Ayazi, “A chopper-stabilized lateral-BJT-input interface in 0.6 μm CMOS for capacitive accelerometers,” 2008 IEEE ISSCC Dig. Tech. Papers, pp. 584-585, San Francisco, CA, USA, 2008, doi: 10.1109/ISSCC.2008.4523318.

(10) Y. Furubayashi, T. Oshima, T. Yamawaki, et al., “A 22-ng/$\sqrt{\text{Hz}}$ 17-mW capacitive MEMS accelerometer with electrically separated mass structure and digital noise-reduction techniques,” IEEE J. Solid-State Circuits, vol. 55, no. 9, pp. 2539-2552, Sept. 2020, doi:10.1109/JSSC.2020.2991533.

(11) Y. Kamada, A. Isobe, T. Oshima, et al., “Capacitive MEMS accelerometer with perforated and electrically separated mass structure for low noise and low power,” Journal of Microelectromechanical Systems, vol. 28, no. 3, pp. 401-408, June 2019, doi : 10.1109/JMEMS. 2019.2903349.

(12) A. Isobe, Y. Kamada, C. Takubo, et al., “Design of perforated membrane for low-noise capacitive MEMS accelerometers,” IEEE Sensors J., vol. 20, no. 3, pp. 1184-1190, 1 Feb., 2020, doi:10.1109/JSEN.2019.2948172.

(13) 川本高司，礒部敦，鎌田雄大，他“持続可能な都市インフラを支える漏水検知サービス，”日立評論，vol. 104, no. 2, pp. 103-108, 2022.

(14) 株式会社日立製作所「お知らせ・受賞など」https://www.hitachi.co.jp/information/info/20220413.html.

（CAS 研究会提案，2023 年 3 月 7 日受付，
2023 年 4 月 19 日再受付）

大島　俊（正員）

1996 東大・理・物理卒．2001 同大学院博士課程了．同年(株)日立製作所入社．以来，アナログ／ディジタル集積回路，センサ，AI，ロボティクスなどに関する研究開発に従事．現在，同社研究開発グループ・デジタルサービス研究統括本部・計測インテグレーションイノベーションセンタ・エッジコンピューティング研究部主管研究員．理博．平成 22 年度電子情報通信学会エレクトロニクスソサイエティ招待論文賞受賞．

解　説　論　文

スパース重ね合わせ符号の理論と実用化に向けた工夫

Theory and Efforts for Practical Application of Sparse Superposition Codes

武石啓成 Yoshinari TAKEISHI

アブストラクト　2010 年に提案された誤り訂正符号であるスパース重ね合わせ符号は，辞書と呼ばれる行列の列ベクトルのスパースな重ね合わせにより符号語を構成する．この符号はガウス通信路 (AWGN channel) に直接適用され，通信路容量に任意に近い伝送レートを達成することが証明されている．またこの符号の理論的限界として，計算量を無視した最適な復号（最ゆう復号）を行った場合の復号誤り確率が解析されている．一方，効率的復号については，圧縮センシングの解法の一つである Approximate Message Passing (AMP) の適用など，実用化に向けた工夫が検討されてきた．本稿ではこれらの話題について，筆者らの研究成果である，辞書の生成分布を大幅に簡略化した場合の最ゆう復号の性能評価も交えて紹介する．

キーワード　スパース重ね合わせ符号，通信路符号化定理，圧縮センシング，Approximate message passing

Abstract　Sparse superposition codes are error-correcting codes proposed in 2010, which construct codewords by sparsely superposing column vectors of a matrix called a dictionary. These codes can be directly applied to Gaussian channels and have been shown to achieve transmission rates arbitrarily close to the channel capacity. To understand a theoretical limitation, the error probability of optimal decoding (maximum likelihood decoding) without regard to computational complexity has been analyzed. Furthermore, efficient decoding methods have been studied for practical applications, such as approximate message passing (AMP), which is one of the solutions for compressed sensing. In this paper, these topics are introduced with the author's research, in which the performance of maximum likelihood decoding is evaluated when the distribution used for generating the dictionary is greatly simplified.

Key words　Sparse superposition codes, Channel coding theorem, Compressed sensing, Approximate message passing

1. はじめに

現代の情報通信技術を支える符号理論は，1948 年に Shannon が示した通信路符号化定理[1]に基づき始まった．この定理ではある通信路が与えられたとき，その通信路容量より小さい任意の伝送レートにおいて，ブロック符号化の符号長 n を十分大きくとれば任意に小さい復号誤り確率を達成できることが示されている．これは驚くべき結果であるが，この定理ではそのような符号の具体的な構成方法については言及されていない．そこで符号理論では，現実的な計算量において通信路容量に迫る伝送レートを達成する符号が探求されてきた．長らくの間，そのような符号は実現できていなかったが，2009 年に Polar 符号[2]が，2011 年に空間結合 LDPC 符号[3]がそれぞれ達成できることが証明された．

そのような状況の中，2010 年に Barron and Joseph によってスパース重ね合わせ符号 (sparse superposition codes(注1); SS 符号)[4],[5]が提案された．この符号は，ガウス通信路 (AWGN channel) に直接適用され，通信路容量を達成することが証明されている[6],[7]．SS 符号では，辞書と呼ばれる行列から少数の列ベクトルを選択し，それらの重ね合わせにより符号語を構成する．このことから，受信語から元のメッセージを復元する復号の問題は，圧縮センシングの一種とみなすことができる．そのため approximate message passing (AMP) などの圧縮センシングの効率的解法を復号に用いることが提案されている[8],[9]．

本稿ではまず SS 符号の構成方法を述べ，この符号の理論的性能限界として最ゆう復号を用いた場合の性能を解説する．また筆者らの行った研究として，辞書の生成分布を正規分布からベルヌーイ分布に簡略化した場合の最ゆう復号の性能を説明する．次に効率的復号として，Barron and Joseph による適応的逐次復号 (adaptive successive decoding) を紹介し，更に AMP による復号及び，最近の研究成果を紹介する．また，本稿ではガウス通信路による 1 対 1 通信のみを取り扱うが，SS 符号は多重アクセス通信路 (multiple access channel) や，放送型通信路 (broadcast channel) への適用も可能である．これらを含めた SS 符号の一連の研究に関しては，2019 年に出版された Venkataramanan らによる著書[10]で整理されている．

武石啓成　正員　九州大学大学院システム情報科学研究院
E-mail takeishi@inf.kyushu-u.ac.jp
Yoshinari TAKEISHI, Member (Faculty of Information Science and Electrical Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka-shi, Fukuoka 819–0395, Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.52–58 2023 年 7 月

(注1)：Sparse regression codes と呼ばれることもある．

本稿では，平均 μ，分散 σ^2 の正規分布を $\mathcal{N}(\mu, \sigma^2)$ と書く．また ‘log’ は底を 2 とする対数関数とし，‘ln’ は自然対数とする．

2. 問題設定

いま，ガウス通信路を n 回使った通信を考える．このとき，入力 $x_i \in \mathbb{R}$ と出力 $y_i \in \mathbb{R}$ $(i = 1, 2, \ldots, n)$ について，

$$y_i = x_i + w_i \tag{1}$$

が成り立つ．ただし，w_i はそれぞれ独立に $\mathcal{N}(0, \sigma^2)$ に従うノイズである．ここで，入力 $x = (x_1, x_2, \ldots, x_n)$ について平均電力制限 P をおく．すなわち任意の入力について，n 個の要素の 2 乗平均が P を超えないという制約をおく．このときの通信路容量はよく知られており，

$$C = \frac{1}{2} \log \left(1 + \frac{P}{\sigma^2}\right) \ (\text{bit/transmission}) \tag{2}$$

である．いまこの通信路を用いて，長さ K のビット列のメッセージ $u \in \{0, 1\}^K$ を $x \in \mathbb{R}^n$ に符号化して送信することを考えると，伝送レートは

$$R = \frac{K}{n} \ (\text{bit/transmission}) \tag{3}$$

で定義される．受信者は受信語 y から元のメッセージ u を復号し，その復号結果を $\hat{u}$ とする．ここでは伝送レート R をなるべく C に近づけつつ，復号誤り確率 $\Pr[\hat{u} \neq u]$ が小さい通信を行うことが目標である．これらの一連の手続きを図 1 に示す．

以下に SS 符号の符号化方法を述べる．まず，N 次元のスパースな列ベクトル β を準備する．β は長さ M の L 個のセクションに分割されており，各セクションに一つだけ非零の要素があり，残りの要素は全て 0 とする．ここで l 番めのセクションの非零の値は c_l としてあらかじめ定めておく $(l = 1, 2, \ldots, L)$．最ゆう復号の場合は l に関して一様な係数

$$c_l = \sqrt{P/L} \tag{4}$$

が用いられる．このように作成した β に対して，K ビットのメッセージを 1 対 1 で対応付ける．いま，取り得る全ての β の集合を $\mathcal{B}$ と書くと，集合 $\mathcal{B}$ の要素数は M^L であるため，

$$K = L \log M \tag{5}$$

の関係が成り立つ．そして，あらかじめ作成しておいた辞書 $A \in \mathbb{R}^{n \times N}$ と β の積 $A\beta$ により符号語 x を作成する．行列 A は各要素それぞれ独立に $\mathcal{N}(0, 1)$ から生成する．これにより，符号語 $x = A\beta$ における平均電力の期待値は P となる．符号化の例を図 2 に示す．

SS 符号の設計において，L と M の設定には自由度がある．二つの極端な例は $L = 1$ のときと，$L = K$ のときである．特に前者の場合は $M = 2^{nR}$ となり，通信路符号化定理の証明に利用される「ランダム符号化」と同様の状況となる．このとき辞書サイズ N が n について指数的に大きくなるため，これは符号の設計において実用的ではない．一方後者の場合は $M = 2$ となり，β のスパース性が失われることになる．そこで適切な

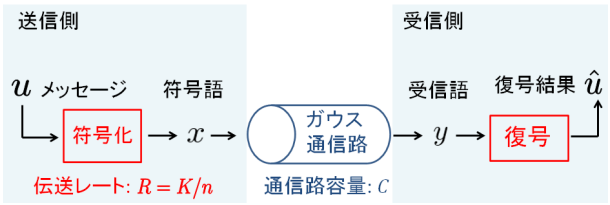


図 1　問題設定

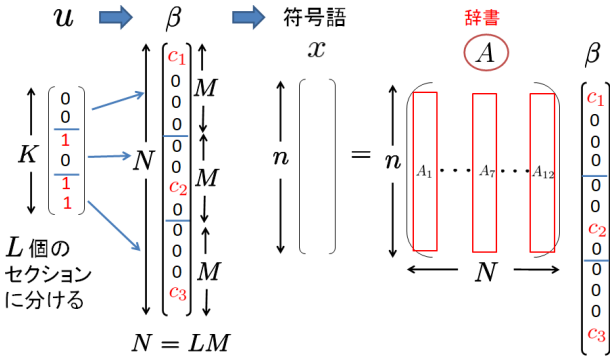


図 2　符号化の例 ($L = 3$，$M = 4$)

辞書サイズを得るために，$M = L^a$ の仮定をおく．ここで a はセクションサイズ率と呼ばれる定数である．このとき (3)，(5) により，

$$n = \frac{K}{R} = \frac{aL \log L}{R} \tag{6}$$

が成り立つことから，$L = O(n/\log n)$ となる．よって，辞書サイズ $N = LM$ は $O((n/\log n)^{a+1})$ であり，a が大きすぎなければ実用可能なサイズといえる．最ゆう復号において，a をどのくらい大きくすればよいかは 3 節の定理 1 で述べる．

3. 最ゆう復号

SS 符号の復号は，$y = (y_1 \ldots, y_n)^T$, $w = (w_1 \ldots, w_n)^T$ と書くと，

$$y = A\beta + w \tag{7}$$

のもとで，y と A の情報から β を推定する問題である．これは線形回帰の一種とみなすことができる．ただし推定結果は集合 $\mathcal{B}$ の中から選ぶ必要がある．最ゆう復号は以下で定義される．

$$\beta_{ML} = \arg \min_{\beta \in \mathcal{B}} \|y - A\beta\|^2 \tag{8}$$

これは組み合わせ最適化の問題であり，L が大きくなれば実際に解くのは計算量的に困難である．しかし，SS 符号の性能限界を知るうえで，この場合の復号誤り確率の解析を行うことは重要である．例えば通常のランダム符号化 ($L = 1$ のとき) の議論を用いて，Gallager は復号誤り確率が n に関して指数的に小さくなる符号の存在を示している[11]．

本節では，2 節で述べたように辞書 A の各要素を正規分布から生成した場合の最ゆう復号の性能について最初に紹介する．続いて筆者らの研究成果である，辞書 A の各要素をベルヌーイ分布から生成するように簡略化した場合の性能について述べる．

3.1 正規分布辞書の性能

最ゆう復号の性能を示すうえで，幾つかの準備を行う．復号結果 $\hat{\beta}$ において誤って復号されたセクションの数を $mistakes$ とする．このとき，$\hat{\beta}$ に関するセクション誤り率 (section error rate) を $\alpha = mistakes/L$ で定義する ($0 \leqq \alpha \leqq 1$)．また $\alpha \neq 0$ となる事象，すなわち $\hat{\beta} \neq \beta$ となる事象をブロック誤りと呼ぶ．ブロック誤りが起きる確率を小さく抑えることが，信頼性のある通信を行ううえで重要である．

以下の定理[6]では，セクション誤り率 α が α_0 以上になる事象を $\mathcal{E}_{\alpha_0}$ として，この事象が起きる確率の上界を示す．ここで定理を述べるために幾つかの量を定義する．$x \geqq 0$ に対して，$g(x) = \sqrt{1+4x^2} - 1$ を定義する．このとき任意の $x \geqq 0$ に対して $g(x) \geqq \min\{\sqrt{2}x, x^2\}$ が成り立つ．また信号対雑音比 $v = P/\sigma^2$ を用いて

$$w_v = \frac{v}{[4(1+v)^2]\sqrt{1+(1/4)v^3/(1+v)}} \tag{9}$$

を定義する．

[定理 1]　辞書 $A^{n\times LM}$ について $M = L^a$ とし，各要素はそれぞれ独立に $\mathcal{N}(0,1)$ から生成する．このとき任意の伝送レート $R < C$ において，$a \geqq a_{v,L}$ とすると，

$$\Pr[\mathcal{E}_{\alpha_0}] = e^{-nE(\alpha_0,R)} \tag{10}$$

が成り立つ．ただし，

$$E(\alpha_0, R) \geqq h(\alpha_0, C-R) - (\ln(2L))/n \tag{11}$$

であり，

$$h(\alpha,\Delta) = \min\left\{\alpha w_v \Delta, \frac{1}{4}g\left(\frac{\Delta}{2\sqrt{v}}\right)\right\} \tag{12}$$

である．$a_{v,L}$ は $L \to \infty$ で有限の値 a_v に収束する量であり，詳細な定義は[6]で与えられている．

注意：この定理における確率変数は，ノイズ w と辞書 A の各要素を対象としている．また R 及び C の単位は nat/tansmission である．このとき a_v の上界として $0 < v < v^* \fallingdotseq 15.8$ において，

$$\frac{4v(1+v)\ln(1+v)}{((1+v)\ln(1+v)-v)^2} \tag{13}$$

が得られる．この上界は v が 0 に近づくにつれ $1/v^2$ のオーダで大きくなってしまうが，$v = 7$ のときは約 5.0，$v = v^*$ のときは約 3.0 となる．また，$v > v^*$ においては，v が大きくなるについて 1 に近づくような a_v の上界が得られる．

ここで，(11) の右辺について，$\alpha_0 > 0$，$C - R > 0$ のとき，$h(\alpha_0, C-R) > 0$ であり，$n \to \infty$ で $(\ln(2L))/n \to 0$ であるため，n を十分大きくとれば $E(\alpha_0, R) > 0$ が成り立つ．よって，このとき (10) の右辺は n に関して指数的に小さくなることが分かる．

また，$\Delta_n = C - R$，$\alpha_0 = \Delta_n$ として，(10) の右辺を指数的に小さくしながら，Δ_n を n に関してどのくらいの速さで 0 に近づけることができるかを考えてみる．いま $h(\Delta,\Delta) = \Omega(\Delta^2)$ であることから，(11) の右辺を正にするためには，$\Delta_n = \Omega(\sqrt{(\log n)/n})$ であればよいことが分かる．

更に外部符号 (outer code) として，伝送レート $(1-2\alpha_0)$ のリード・ソロモン符号[12]を用いることで，セクション誤り率 α_0 以上のセクション誤りを修正することができる．これにより，ブロック誤り確率についても n に関して指数的に小さくできることが示せる．

3.2 ベルヌーイ分布辞書の性能

3.1 節では，辞書の各要素は $\mathcal{N}(0,1)$ から生成することを仮定していた．しかし，正規分布に従う確率変数は無限に大きな値を取る可能性がある．また正規分布は連続値を取る分布であるため，実現値をストレージ上に記述する際には量子化誤差が発生する．これらのことから，正規分布の辞書を実装するには大きなストレージ容量が必要となることが分かる．

そこで，辞書を二値のみを取るベルヌーイ分布から生成することを考える．すなわち A の各要素をそれぞれ独立に $\{-1,1\}$ から等確率で生成する．これにより辞書の各要素を僅か 1 ビットで保存可能となる．一方，符号語は A の要素の L 個の重ね合わせとなるため，中心極限定理により符号語の分布は正規分布に近づく．そのため正規分布辞書の場合に近い性能が得られることが期待できる．実際，この場合も最ゆう復号においては通信路容量に近い任意の伝送レートを達成できることを筆者らは示した[13]．以下の定理は定理 1 のベルヌーイ分布辞書版である[14]．

[定理 2]　辞書 $A^{n\times LM}$ について $M = L^a$ とし，各要素はそれぞれ独立に $\{-1,1\}$ から等確率で生成する．このとき任意の伝送レート $R < C$ において，$a \geqq a_{v,L}$ とすると，

$$\Pr[\mathcal{E}_{\alpha_0}] = e^{-nE(\alpha_0,R)} \tag{14}$$

が成り立つ．ただし，

$$E(\alpha_0, R) \geqq h(\alpha_0, C-R) - \iota(L) \tag{15}$$

であり，

$$\iota(L) = O(1/\sqrt{L}) \tag{16}$$

である．

この場合も同様に，任意の $R < C$ において (14) の右辺は n に関して指数的に小さくなることがいえる．ただし，(11) と (15) の右辺を比べると，(15) の方が $L \to \infty$ での 0 への収束が遅くなっている．この場合は達成できる伝送レートと通信路容量とのギャップ Δ_n は $O\big((\frac{\log n}{n})^{1/4}\big)$ となる．この違いは中心極限定理を考えた際の，ベルヌーイ分布の重ね合わせである二項分布と，正規分布の誤差によるものである．

この定理の証明は，上記の二項分布と正規分布における確率分布の差を精密に評価し，定理 1 の証明に帰着させることにより行う．しかし，既存の中心極限定理ではその目的に不十分であっ

たため，筆者らは以下二つの新たな補題を導出した[13],[14]．

［補題 1］ 任意の自然数 l について，

$$\max_{k\in\{0,1,\ldots,l\}} \frac{{}_lC_k(1/2)^l}{N(k|l/2,l/4)} \leqq \exp\{\phi(l)\} \tag{17}$$

が成り立つ．ただし，

$$N(x|\mu,\sigma^2) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{(x-\mu)^2}{2\sigma^2}\right) \tag{18}$$

$$\phi(l) = \inf_{\zeta\in(0,1/2)} \phi_\zeta(l) \tag{19}$$

$$\phi_\zeta(l) = \max\left\{\left(\frac{3}{16}c_\zeta^2+\frac{1}{12}\right)\frac{1}{l},\ -\frac{4\zeta^4}{3}l+\ln\frac{l}{2}+\frac{1}{12l},\right.$$
$$\left.-\left(\ln 2-\frac{1}{2}\right)l+\frac{1}{2}\ln\frac{\pi l}{2}\right\} \tag{20}$$

であり，$c_\zeta = 1/(1+2\zeta)^2 + 1/(1-2\zeta)^2$ である．特に，1000 以上の自然数 l について，$\phi(l) \leqq 5/l$ が成り立つ．

［補題 2］ 自然数 n に対して，$h = 2/\sqrt{n}$ 及び

$$\mathcal{X} = \{h(k-n/2)|k = 0,1,\ldots,n\} \tag{21}$$

を定義する．更に，$s^2 > 0$ と $\mu \in \Re$ に対して，I_d と I_c をそれぞれ

$$I_d = h\sum_{x\in\mathcal{X}}\exp\left\{-\frac{s^2}{2}(x-\mu)^2\right\} \tag{22}$$

$$I_c = \int_{-\infty}^{\infty}\exp\left\{-\frac{s^2}{2}(x-\mu)^2\right\}dx = \sqrt{2\pi/s^2} \tag{23}$$

で定義する．このとき，

$$I_d \leqq \left(1+\frac{\eta s^2}{n}\right)I_c, \tag{24}$$

が成り立つ．ただし，$\eta = \sqrt{9/(8\pi e)} \leqq 0.37$ である．

まず補題 1 は，二項分布の確率質量関数と正規分布の確率密度関数の比を，二項分布の試行数 k に関して一様に評価したものである．次に補題 2 は，正規分布の確率密度関数の積分について，区分求積の誤差を評価するものである．これは連続分布と離散分布における期待値の差を評価するために用いる．これらを視覚的に示したのが図 3 である．この二つの補題を利用することで，定理 2 の証明を行うことができる．

なお定理 2 においては，辞書分布をベルヌーイ分布から二項分布に比較的容易に拡張することができる[15]．これにより，(15) に現れる $\iota(L)$ の 0 への収束を速めることができるが，その分

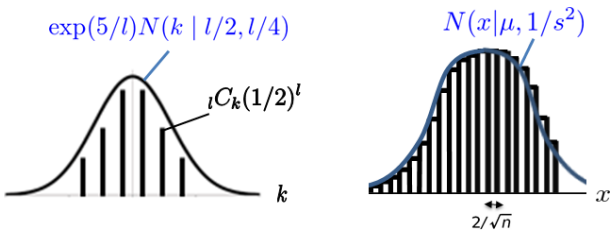


図 3 補題 1 (左) と補題 2 (右) のイメージ図

辞書の要素あたりの保存容量が大きくなる．一般の離散分布への拡張は今後の課題であるが，補題 1 のような一様な評価を行うためには，分布の対称性に関する何らかの仮定が必要と思われる．

4. 適応的逐次復号

適応的逐次復号[5]は Barron and Joseph によって提案された SS 符号の効率的復号法である．この復号は並列処理により，ブロック長 n の復号を $O(n)$ で実施することができる．ただし，外部符号に利用するリード・ソロモン符号の復号には n に関する多項式時間が必要である．また，この復号により達成できる伝送レートと通信路容量とのギャップ Δ_n は，$O(1/\sqrt{\log n})$ となる[7]．このギャップは n を大きくすれば 0 に近づくが，最ゆう復号と比べてかなり収束は遅くなる．

適応的逐次復号の効果を得るために，符号化に利用する β の係数 c_l について，(4) のような一定の値ではなく，傾斜をつけるようにする．具体的には，$c_l = \sqrt{P_l}$ として，

$$P_l \propto e^{-2C(l/L)} \tag{25}$$

となるようにする．ただし，C は (2) で表される通信路容量であり，また平均電力制限 P を考慮し，

$$\sum_{l=1}^{L} P_l = P \tag{26}$$

が満たされるように P_l の正規化を行う．なお，l が L に近い部分で P_l を一定にすることで，適応的逐次復号の達成可能レートと通信路容量とのギャップが $O\left(\frac{\log\log n}{\log n}\right)$ へ僅かに改善されることが示されている[16]．

復号は以下の繰り返しアルゴリズムによって行い，停止した際の β^{t+1} を復号結果とする．

（1） 初期化ステップ ($t=0$)

ベクトル $y/\|y\|$ と A の各列ベクトルとの内積を計算する．内積が閾値 s を超えた列のインデックスに c_l を設定し，それ以外は 0 としたベクトル β^1 を作成する．ただし，l はその列が含まれているセクション番号である ($1 \leqq l \leqq L$)．

（2） 繰り返しステップ ($t \geqq 1$)

残差ベクトル $R^t = y - A\beta^t$ を計算する．まだ選ばれていない A の列ベクトルについて，それぞれ $R^t/\|R^t\|$ との内積を計算する．内積がしきい値 s を超えた列のインデックスに c_l を設定するよう，β^t を更新したものを β^{t+1} とする．

（3） 繰り返しの停止条件

β^t の非零要素の数が L 以上になったとき，または β_t が更新されなかったとき，またはあらかじめ定めた繰り返し回数の上限に達したとき

このアルゴリズムは各繰り返しステップにおいて，復号するセクションを指定していない．その代わりに未復号の全てのセクションにおいて，残差ベクトルと A の列ベクトルとの内積を

計算し，しきい値を超えたものを順次復号していく．この意味でこの復号法は「適応的 (adaptive)」である．ただしこのアルゴリズムによって得られる解 β は，各セクションに一つだけ非零の要素をもつという制約を満たしていない可能性がある．そのため，あるセクションについて，一つも非零要素がない場合，または複数の非零要素がある場合は無条件にセクション誤りが発生する．

なお上記に述べた適応的逐次復号は，復号アルゴリズムの各ステップにおいて，β の各要素はしきい値を超えるか否かをもとに，0 か $\sqrt{P_l}$ の二値で更新している．このような復号法は硬判定復号法 (hard-decision decoding) と呼ばれる．それに対して，Barron and Cho は以下の軟判定復号法 (soft-decision decoding) と呼ばれる方法を提案している[17]．このアルゴリズムにおいては，

$$\beta_j^{t+1} = w_{t,j}\sqrt{P_l} \tag{27}$$

となるように β^t を更新する．ここで $w_{t,j}$ は t ステップめの時点における，真の β_j が非零要素となる事後確率となるように構成する．そのため更新の各ステップにおける β の各要素は二値ではなく，0 から $\sqrt{P_l}$ の間の値を取ることができる．これにより，有限の符号長 n における性能が幾らか改善される．

5. AMP 復号

Approximate message passing (AMP)[18] は確率伝搬法の近似にあたる反復解法であり，圧縮センシングの問題 (LASSO) を高速に解くためのアルゴリズムの一つである．LASSO は (7) の設定において，スパースなベクトル β を推定するために解く，以下の L1 正則化項付き最適化問題である．

$$\arg\min_{\beta\in\mathbb{R}^N} \|y - A\beta\|^2 + \lambda\|\beta\|_1 \tag{28}$$

上記の問題は SS 符号の復号問題に類似しており，主に Rush ら[8] や Barbier ら[9] により復号に AMP を利用する方法が研究されているが，本稿では Rush らの研究成果をもとに解説を行う．この AMP 復号により，達成可能な伝送レートと通信路容量とのギャップ Δ_n は $O\left(\sqrt{\frac{\log\log n}{\log n}}\right)$ となることが示されている[19]．以下にその復号アルゴリズムを紹介する．なお AMP 復号は前節の最後で述べた軟判定復号法の一種である．またここでは，辞書 A の各要素は $\mathcal{N}(0,1/n)$ から生成し，β の l 番めのセクションの非零要素は $c_l = \sqrt{nP_l}$ とし，P_l には前節と同様に指数的な傾斜をつける．

（1） 初期化ステップ

$\beta^0 = 0$ (N 次元の零ベクトル)，$z^{-1} = 0$ と初期化する．

（2） 繰り返しステップ ($0 \leqq t \leqq T-1$)

以下の式により，z_t と β^{t+1} を更新する．

$$z^t = y - A\beta^t + \frac{z^{t-1}}{\tau_{t-1}^2}\left(P - \frac{\|\beta^t\|^2}{n}\right) \tag{29}$$

$$\beta_i^{t+1} = \eta_i^t(\beta^t + A^T z^t),\ \text{for } i = 1,\ldots,N \tag{30}$$

ここで，$\{\tau_t\}$ は以下の式により定義する．

$$\tau_0^2 = \sigma^2 + P \tag{31}$$

$$\tau_{t+1}^2 = \sigma^2 + P(1 - x_{t+1}),\ t \geqq 0 \tag{32}$$

ただし，

$$x_{t+1} = \sum_{l=1}^{L}\frac{P_l}{P}\mathbb{E}\left[\frac{e^{\frac{\sqrt{nP_l}}{\tau_t}(U_1^l + \frac{\sqrt{nP_l}}{\tau_t})}}{e^{\frac{\sqrt{nP_l}}{\tau_t}(U_1^l + \frac{\sqrt{nP_l}}{\tau_t})} + \sum_{j=2}^{M} e^{\frac{\sqrt{nP_l}}{\tau_t}U_j^l}}\right] \tag{33}$$

である．ここで，$\{U_j^l\}$ $(j = 1,2,\ldots,M,\ l = 1,2,\ldots,L)$ は独立に $\mathcal{N}(0,1)$ に従う確率変数列である．

パラメータ $\{\tau_t\}$ は復号アルゴリズムを実行する前に計算しておく．ここで，τ_{t+1} を τ_t から求める式を状態発展式と呼ぶ．状態発展式に現れる期待値は，$\{U_j^l\}$ を乱数生成することで，モンテカルロ法により計算することができる．また，Rush らは $L \to \infty$ の極限での x_t，τ_t を計算し，これを用いた AMP 復号の性能を評価している[8]．更に波多江らは，τ_t を状態発展式を用いない近似値に置き換えることにより，現実的な符号長における性能改善が見られることを報告している[20]．

最後に，AMP 復号への深層展開の適用について紹介する．押川らは，AMP 復号アルゴリズムにおいて，T 回の繰り返しステップの計算を T 層のニューラルネットワークによる処理とみなし，アルゴリズム中に現れる行列 A などを深層学習のアルゴリズムを用いて最適化する実験を行った[21]．これにより，通常の AMP 復号アルゴリズムよりも性能改善が見られることが分かった．また飯田らは，符号器 $x = A\beta$ における辞書行列 A も学習対象に加えることで更なる性能改善を達成した[22]．

6. 復号法の比較

これまで述べてきた復号法について，まずは理論的な観点での比較を行う．達成可能な伝送レートと通信路容量とのギャップを Δ_n として，現在得られている Δ_n の上界を表 1 に示す．これらは符号長 n が大きくなるにつれて 0 に近づくオーダであるが，その速さには違いがある．特に効率的復号については分母が対数オーダであり，0 に近づく速度が非常に遅いことが課題である．

一方，現実的な符号長における，効率的復号の実験的な性能比較については，硬判定復号より軟判定復号の方が高い性能を示

表 1　Δ_n の比較

復号法	Δ_n
最ゆう復号	
正規分布辞書	$O\left(\sqrt{\frac{\log n}{n}}\right)$
ベルヌーイ分布辞書	$O\left((\frac{\log n}{n})^{1/4}\right)$
適応的逐次復号	
硬判定復号	$O\left(\frac{\log\log n}{\log n}\right)$
軟判定復号	-
AMP 復号	$O\left(\sqrt{\frac{\log\log n}{\log n}}\right)$

している．また，軟判定復号のうち，適応的逐次復号より AMP 復号の方が計算量の少なさにおいて優位性がある．特に AMP 復号においては，辞書行列 A を正規分布から生成するのではなく，アダマール行列を利用することで計算量を大きく削減できることが知られている．

また Rush らによる最近の研究[23]では，辞書行列に空間結合構造を利用した AMP 復号について，DVB-S2 規格（デジタルテレビ放送の標準規格）の LDPC 符号を用いた符号化変調方式と性能比較を行っている．この比較実験結果によると，SS 符号の復号性能は LDPC 符号を完全には上回ることはできなかったものの，一部の低レート帯においては LDPC 符号を上回る場合があることが示されている．

7. むすび

本稿では SS 符号について理論と実用の両面からの概説を行った．筆者が SS 符号の研究を始めたのは 2011 年後半の修士課程の頃であるが，この符号は当時のホットな研究分野であった圧縮センシングを背景にもち，現在でも符号理論以外の分野とのつながりをもつ魅力的な研究対象であると考えている．現状は LDPC 符号や Polar 符号を置き換えるほどの実用上の性能は得られていないが，SS 符号は変調を介さず直接ガウス通信路に直接適用できることがこれらの符号とは異なる特徴であり，更なる性能向上の余地はあると思われる．また理論的な課題としても，AMP 復号をはじめとする効率的復号において，ベルヌーイ分布の辞書やアダマール行列を用いた場合の性能保証や，達成可能レートの収束速度の改善など，興味深い研究テーマが残されている．世の中では第 6 世代移動通信システム (6G) の検討など，よりパワフルな符号が求められており，SS 符号を含めた今後の符号理論の更なる発展が期待される．

謝辞　本稿の執筆に関するお話をくださった和歌山大学の葛岡成晃先生をはじめ，情報理論研究専門委員会の皆様に感謝を申し上げます．また SS 符号を提案された Andrew. R. Barron 先生の共同研究者であり，筆者に SS 符号を含めた研究指導をくださった九州大学の竹内純一先生には大変お世話になりました．この場を借りてお礼を申し上げます．

文　献

(1) C.E. Shannon, “A mathematical theory of communication,” Bell Syst. Tech. J., vol.27, pp.379–423, 1948.
(2) E. Arikan, “Channel polarization,” IEEE Trans. Inf. Theory, vol.55, no.7, pp.3051–3073, July 2009.
(3) S. Kudekar, T.J. Richardson, and R. Urbanke, “Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC,” IEEE Trans. Inf. Theory, vol.57, no.2, pp.803–834, Feb. 2011.
(4) A.R. Barron and A. Joseph, “Least squares superposition coding of moderate dictionary size, reliable at rates up to channel capacity,” Proc. Int. Symp. Inf. Theory, Austin, Texas, pp.275–279, June 2010.
(5) A.R. Barron and A. Joseph, “Towards fast reliable communication at rates near capacity with Gaussian noise,” Proc. IEEE. Int. Symp. Inf. Theory, Austin, Texas, pp.315–319, June 2010.
(6) A. Joseph and A.R. Barron, “Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity,” IEEE Trans. Inf. Theory, vol.58, no.5, pp.2541–2557, May 2012.
(7) A. Joseph and A. R. Barron, “Fast sparse superposition codes have near exponential error probability for $R < \mathcal{C}$,” IEEE Trans. Inf. Theory, vol.60, no.2, pp.919–942, Feb. 2014.
(8) C. Rush, A. Greig, and R. Venkataramanan, “Capacity achieving sparse superposition codes via approximate message passing decoding,” IEEE Trans. Inf. Theory, vol.63, no.3, pp.1476–1500, March 2017.
(9) J. Barbier and F. Krzakala, “Approximate message-passing decoder and capacity achieving sparse superposition codes,” IEEE Trans. Inf. Theory, vol.63, no.8, pp.4894–4927, Aug. 2017.
(10) R. Venkataramanan, S. Tatikonda, and A.R. Barron, “Sparse regression codes,” Foundations and Trends in Communications and Information Theory, vol.15, no.1–2, pp.1–195, 2019. https://doi.org/10.1561/0100000092
(11) R.G. Gallager, “A simple derivation of the coding theorem and some applications,” IEEE Trans. Inf. Theory, vol.11, no.1, pp.3–18, Jan. 1965.
(12) I.S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” J. SIAM, vol.8, pp.300–304, June 1960.
(13) Y. Takeishi, M. Kawakita, and J. Takeuchi, “Least squares superposition codes with Bernoulli dictionary are still reliable at rates up to capacity,” IEEE Trans. Inf. Theory, vol.60, no.5, pp.2737–2750, May 2014.
(14) Y. Takeishi and J. Takeuchi, “An improved analysis of least squares superposition codes with Bernoulli dictionary,” Japanese Journal of Statistics and Data Science, vol.2, pp.591–613, Sept. 2019.
(15) 武石啓成，竹内純一，“二項分布辞書を用いたスパース重ね合わせ符号,” 第 45 回情報理論とその応用シンポジウム予稿集，pp.247–252, Dec. 2022.
(16) A. Joseph, “Achieving information-theoretic limits with high-dimensional regression,” Ph.D. thesis, Yale University, 2012.
(17) A.R. Barron and S. Cho, “High-rate sparse superposition codes with iteratively optimal estimates,” Proc. IEEE. Int. Symp. Inf. Theory, Cambridge, MA, pp.120–124, July 2012.
(18) D.L. Donoho, A. Maleki, and A. Montanari, “Message-passing algorithms for compressed sensing,” Proc. Nat. Acad. Sci. USA, vol.106, no.45, pp.18914–18919, 2009.
(19) C. Rush and R. Venkataramanan, “The error probability of sparse superposition codes with approximate message passing decoding,” IEEE Trans. Inf. Theory, vol.65, no.5, pp.3278–3303, May 2019.
(20) 波多江優和，三村和史，川喜田雅則，竹内純一，“スパース重ね合わせ符号のための Bayes 最適 AMP 復号器,” 電子情報通信学会技術研究報告，vol.117, no.487, IT2017-127, pp.143–148, March 2018.
(21) 押川祐也，三村和史，竹内純一，“スパース重ね合わせ符号のための Trainable Bayes 最適 AMP 復号器,” 電子情報通信学会技術研究報告，vol.118, no.433, IT2018-44, pp.55–60, Jan. 2019.
(22) 飯田昌澄，押川祐也，三村和史，竹内純一，“深層学習によるスパース重ね合わせ符号の改良,” 電子情報通信学会技術研究報告，vol.119, no.47, IT2019-13, pp.67–72, May 2019.
(23) C. Rush, K. Hsieh, and R. Venkataramanan, “Capacity-achieving spatially coupled sparse superposition codes with AMP decoding,” IEEE Trans. Inf. Theory, vol.67, no.7, pp.4446–4484, July 2021.

（IT 研究会提案，2023 年 3 月 4 日受付，
2023 年 4 月 5 日再受付）

武石啓成（正員）

2011 九大・工・電気情報工卒．2013 同大大学院修士課程了．三菱電機インフォメーションネットワーク（株）勤務を経て，2022 同大大学院博士課程了．2022 同大助教．現職．博士（工学）．情報理論，機械学習及びそれらの応用についての研究に従事．

解　説　論　文

共通鍵暗号技術のポスト量子安全性について

On Post-Quantum Security of Symmetric Cryptosystems

細山田光倫 Akinori HOSOYAMADA

アブストラクト　素因数分解問題と離散対数問題を多項式時間で解く量子アルゴリズムを Shor が発見して以来，ポスト量子公開鍵暗号技術の研究が盛んに行われてきた．近年では，公開鍵暗号技術のみならず共通鍵暗号技術に対しても，量子計算機の使用を前提とした興味深い攻撃アルゴリズムが複数見つかっている．本稿では，共通鍵暗号技術のポスト量子安全性に関するこれまでの研究の流れと最近の動向について，主に攻撃アルゴリズムの観点から概観する．

キーワード　暗号，共通鍵暗号技術，量子アルゴリズム，攻撃アルゴリズム

Abstract　Since Shor discovered polynomial time quantum algorithms to solve integer factorization and discrete logarithm problems, lots of studies have been done on post-quantum public key cryptography. In recent years, some interesting attacks using quantum computers have been found on not only public key schemes but also symmetric key schemes. This article provides an overview of the history and recent trends in research on the post-quantum security of symmetric key schemes, mainly in terms of cryptanalysis.

Key words　Cryptography, Symmetric key cryptography, Quantum algorithm, Cryptanalysis

1. はじめに

機密情報の保護から仮想通貨（暗号資産）まで，暗号技術(注1)は現代社会の至るところで利用されている．普段の日常生活も，無意識のうちに暗号技術に支えられている．ネットショッピングで買い物をしたりメッセージアプリを用いて家族や友人に連絡を取ったりするとき，情報は自動で暗号化され保護されていることが多い．

暗号と一口にいっても，共通鍵暗号や公開鍵暗号に始まり，マルチパーティ計算やゼロ知識証明，難読化に至るまで，様々な種類の関連技術や理論がある．その中でも，単に「暗号」といわれて世間一般でイメージする，役割や機能が一番分かりやすいものは共通鍵暗号でないかと筆者は考える．

共通鍵暗号を用いる際は，情報のやり取りをする前に秘密鍵を共有する必要がある．例えば Alice と Bob という 2 人の人がいて通信内容を共通鍵暗号で保護したいとき，ほかの誰にも知られないように鍵を何らかの方法で事前に共有しておく．Alice がデータを送る際はこの鍵を用いて暗号化を施す．同じ秘密鍵をもっている Bob だけが元の内容を復元（復号）することができる．

問題は，この秘密鍵をどうやって事前に共有するかである．例えば離れた場所にいる Alice と Bob が秘密鍵を共有したいと思っているとする．一番手っ取り早い方法は，Alice が鍵の情報に何の保護も施さず Bob に送ることだが，悪意のある第三者が鍵の情報を盗み見る可能性がある．

公開鍵暗号を用いると，この問題を解決することができる．公開鍵暗号では，暗号化用の鍵と復号用の鍵を分けて，前者を公開することができる．暗号化用の鍵だけあっても，暗号文を元に戻すことはできない．Bob が暗号化用の鍵を公開しておけば，Alice はいつでも情報を暗号化して Bob に送ることができる．

ここまでの話の流れからすると，公開鍵暗号は共通鍵暗号の上位互換のような気がしてくる．公開鍵暗号さえあれば共通鍵暗号は要らないのではないか．しかし話はそう簡単ではない．公開鍵暗号は「鍵の片方を公開しても安全」という魔法のような性質をもつが，この魔法を実現するためには暗号化や復号の処理速度を多少犠牲にする必要がある．暗号化するデータが大きいと，暗号化に膨大な時間が掛かってしまい，使い勝手が悪い．一方，共通鍵暗号は鍵の公開を最初から諦めているが，そのぶん高速な処理が可能な設計になって

細山田光倫　正員　NTT 社会情報研究所
E-mail　akinori.hosoyamada@ntt.com
Akinori Hosoyamada, Member (NTT Social Informatics Laboratories, NTT Corporation, Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.59-71 2023 年 7 月

(注 1)：本稿では，「暗号」というとデータの内容を隠すための技術である狭義の暗号のことを指し，「暗号技術」というと狭義の暗号のみならずハッシュ関数や MAC・署名などの暗号関連技術をまとめたものを指すこととする．

いる．公開鍵暗号の「鍵の一部を公開できる」という特性と共通鍵暗号の高速性，両者を上手く組み合わせて初めてデータを安全かつ効率的に保護できるのである．

例えばインターネットの通信で用いられる SSL/TLS などの暗号化通信プロトコルでは，相手とやり取りするメッセージの暗号化は基本的に共通鍵暗号で行い，この共通鍵暗号の鍵を相手と事前に共有するために公開鍵暗号技術を用いる．こうすることで，暗号化処理に必要な処理時間を最小限に抑えつつ，暗号化通信用の鍵を相手と安全に共有できる．

1.1 公開鍵暗号技術のポスト量子安全性

現在最も広く使われている公開鍵暗号として RSA 暗号[(1)]やだ円曲線暗号[(2)]が挙げられるが，1994 年にこれら暗号に対する重大な脅威となりうるアルゴリズムが発表された．Shor の量子アルゴリズムである[(3)]．RSA 暗号とだ円曲線暗号の安全性は，素因数分解問題とだ円曲線上の離散対数問題を解くには非常に時間がかかることを前提としている．Shor の量子アルゴリズムはこれらの問題を多項式時間で解いてしまうため，実用的な大規模汎用量子計算機が実現されればこれら暗号の安全性は無に帰してしまうのではないかという懸念が生じた．

その頃以降，ポスト量子暗号，すなわち量子計算機を用いた攻撃にも耐えうる暗号の研究が盛んに行われている．ここ数年では NIST（アメリカ国立標準技術研究所）がポスト量子安全な公開鍵暗号や鍵交換及び電子署名の標準化を進めており，幾つかのアルゴリズムは既に標準化されることが決定している[(4)]．ポスト量子安全な公開鍵暗号技術の詳細については本稿の範囲を超えるため，本誌に以前掲載された解説論文など[(5)]を参照されたい．

1.2 ポスト量子共通鍵暗号技術？

公開鍵暗号技術のポスト量子安全性は盛んに研究されてきたわけだが，共通鍵暗号技術のポスト量子安全性はどうだろうか．前述のように，安全かつ効率的なデータ保護には公開鍵暗号技術のみでなく共通鍵暗号技術が必要不可欠である．量子計算機を用いた攻撃からデータを保護するには，公開鍵暗号技術だけでなく共通鍵暗号技術もポスト量子安全な必要があるまいか．

以上の背景のもと，本稿では，共通鍵暗号技術のポスト量子安全性に関するこれまでの研究の流れと最近の動向について，主に攻撃アルゴリズムの観点から概観する．

2. 共通鍵暗号技術

本稿ではメッセージを暗号化したり復号したりする狭義の暗号のほかに，メッセージ認証コード（MAC）や認証暗号（AEAD），ハッシュ関数なども共通鍵暗号技術に含めるものとする．以下，各技術の基本事項をおさらいしたのち，次章以降の内容に関連する技術を設計方針別に説明する．

2.1 暗号，MAC，AEAD，ハッシュ関数

単に暗号といえば基本的に，鍵とメッセージを入力に取って暗号文を出力し，鍵と暗号文があれば元のメッセージを復元するものを指す．このような狭義の暗号の主な役割は，データの内容を秘匿する（機密性を担保する）ことである．

暗号技術の役割は，データの内容を秘匿するだけではない．メッセージが誰に見られてもよいが，データが不正に改ざんされたら検知したい（真正性を担保したい）という状況がある．これを達成するための技術が MAC である．AEAD は，データ内容の秘匿と改ざん検知を同時に達成しようというものである．

暗号学的ハッシュ関数は，大雑把にいうとメッセージからランダムな値を生成する関数である．暗号学的ハッシュ関数に期待される役割は状況に応じて変化するが，理想的には全てのありうる関数からランダムに取られた関数（ランダムオラクル）のように振る舞うことが期待される．ほかの共通鍵暗号技術と違って鍵を入力に取らないが，実用的な暗号学的ハッシュ関数は共通鍵暗号技術の設計技法を利用することが多い．

2.2 プリミティブとモード

前節では共通鍵暗号技術を役割ごとに分類したが，いずれの共通鍵暗号技術も設計方針ごとにモードとプリミティブに大別できる[(注2)]．

モードと分類される共通鍵暗号は，ほかの共通鍵暗号技術を取り替えのきく部品として使い，より高度な機能を達成するものである．例えば，短いメッセージしか暗号化できないブロック暗号（後述）をうまく利用して大きなメッセージを暗号化するモード，ブロック暗号を利用して MAC を作るモード，などがある．モードは，その安全性を何らかの意味で証明できるものが多い．例えばブロック暗号を利用して AEAD を作るモードである GCM[(6)]は，大雑把に「元のブロック暗号が一定の計算量以下の攻撃に対して安全と仮定すれば，GCM 自身もある程度の計算量の攻撃に対し安全」という形で安全性が証明される．これは RSA 暗号をはじめとする公開鍵暗号技術の安全性が「素因数分解問題を解くのが難しければこの暗号は安全」というような形で証明されることに対応する．

一方，共通鍵暗号技術の研究の文脈でプリミティブというと，部品の取り替えを想定せず一枚岩のアルゴリズムとして（時として一種の職人的技巧により）設計されたものを指すことが多い．プリミティブについても「既存の特定の攻撃手

(注 2)：本稿で述べる区別の仕方は絶対的なものではなく，あくまで筆者の個人的な肌感覚に基づく便宜的なものである．文脈や研究者によって変化しうることに注意されたい．

法が通用しない」ということはある程度証明できることがあるが，多くの公開鍵暗号技術やモードと違って「未知の攻撃手法に対しても安全」という主張の証明は基本的に困難である．各プリミティブが破れないということは，究極的には世界中の暗号研究者が攻撃を試みても破れないということによってのみ担保される．これは，公開鍵暗号技術の安全性の根拠となる素因数分解問題や格子問題の困難性が（証明された定理でなく）あくまで現時点での予想に基づくということに似ている（なお「破れない」ということと「安全」ということには若干の差異がある．詳しくは次章で説明する）．

全ての共通鍵暗号技術は，AEAD も含めてモードでなくプリミティブとして実現されうる．例えば，先ほどモードの一例として GCM という AEAD モードを紹介したが，直接プリミティブとして AEAD を設計することも可能である．

共通鍵暗号技術をプリミティブでなくモードとして設計し安全性証明をつけることの利点は，安全性評価で考慮せねばならない範囲が狭まること，及び使いまわしが利くことである．例えば GCM であれば，ブロック暗号という小さい構成要素さえ安全であれば全体が安全になる．いったん安全性証明をしてしまえば，以降はブロック暗号が安全かどうかのみに気を配ればよい．また部品のブロック暗号が破れてしまった場合でも，別の安全なブロック暗号を使えば GCM は再び安全な AEAD になる．

2.3 ブロック暗号の構造

現代の共通鍵暗号技術で最も基本的なプリミティブの一つがブロック暗号である．ブロック暗号は固定長の平文と固定長の鍵を入力に取り，平文と同じ長さの暗号文を出力する．例えば現在 NIST 標準のブロック暗号である AES[7] は，平文と暗号文の長さが 128 ビットである．鍵の長さは 128 ビット，192 ビット，256 ビットから選べる．鍵長に応じて三つのブロック暗号が用意されており，それぞれ AES-128, AES-192，AES-256 と呼ばれる．

ブロック暗号の典型的な構成は，繰り返し構造である．平文 M と鍵 K が入力されると，ブロック暗号の暗号化アルゴリズムはまず，鍵 K から副鍵と呼ばれるビット列 $K1, K2, \cdots$ を生成する．その後，平文 M に段関数と呼ばれる関数を何度も繰り返し適用して暗号文 C を計算・出力する（図 1）．復号の際は逆の処理を行う．

段関数を何回適用するかはブロック暗号ごとに仕様で決まっている．例えば AES-128 では 10 段，AES-256 では 14 段である．基本的に段数（段関数の繰り返し回数）が多いほど攻撃しにくくなるが，段数が多いほど当然処理は遅くなる．ブロック暗号の設計者は安全性と効率性のトレードオフを天秤にかけて段数を決める．

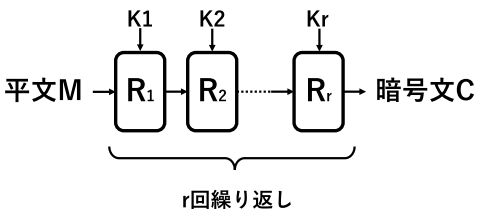


図 1　典型的なブロック暗号の構造

なお近年では，平文や鍵のほかに tweak という追加の値を入力できる Tweakable ブロック暗号[8]~[10]の研究が盛んである．通常のブロック暗号より入力が多いぶん，Tweakable ブロック暗号を利用した方がより高効率なモードを実現できるケースがある[11], [12]．

2.4 暗号学的ハッシュ関数

暗号学的ハッシュ関数（以下単に「ハッシュ関数」，H と書く）は鍵を入力に取らず，ほかの暗号技術と少し毛色が違うため，ここで説明を加えておく．ハッシュ関数は前述のように，理想的にはランダム関数のように振る舞うことが期待されるが，特に満たすべき安全性は以下の三つである．

1. 原像計算困難性：値 y が与えられたとき，$H(x)=y$ を充たす x を計算することが難しい．
2. 衝突耐性：異なる入力 x と x' であって $H(x)=H(x')$ を充たすもの（衝突）を計算することが難しい．
3. 第二原像計算困難性：x が与えられたとき，$H(x)=H(x')$ を充たす x' を計算することが難しい．

第二原像困難性と衝突耐性は一見似ているが，第二原像計算困難性においては x が所与で固定されている一方，衝突耐性では x と x' の両方を自由に取ってよい．ゆえに衝突耐性の方が破りやすい．

ハッシュ関数の典型的な構成に Merkle-Damgård 構成[13], [14] とスポンジ構成[15] がある．Merkle-Damgård 構成では圧縮関数と呼ばれる固定長入力の関数をまず作り，長い入力に対しては圧縮関数を中間出力とメッセージに繰り返し適用することで出力を計算する（図 2 上）．圧縮関数はその名

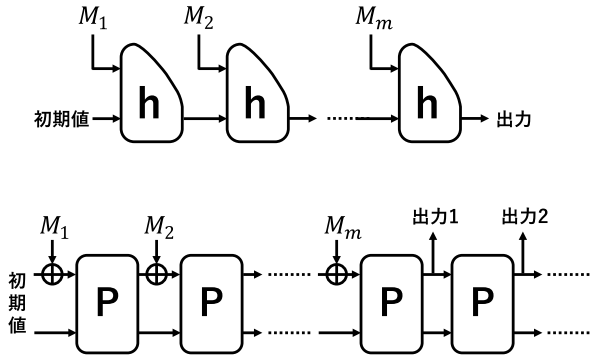


図 2　Merkle-Damgård 構成（上）とスポンジ構成（下）　h は圧縮関数，P は置換を表す．いずれの構成でも，入力メッセージは適切な処理を施されたのち，複数のメッセージのブロック $M_1, \cdots, M_m$ に分割される．スポンジ構成では，出力ブロックを幾つも生成できる．それらのうち必要なビットを取り出して結合したものが最終的な出力となる．

のとおりデータを短く圧縮する関数で，出力長が入力長より短い．スポンジ構成では入出力長が同一の置換（あるいは関数）を繰り返し適用する（図 2 下）．NIST 標準の方式でいえば SHA-2[16] は Merkle-Damgård 構成に，SHA-3[17] はスポンジ構成に基づいている．

ハッシュ関数中で使われる圧縮関数や置換が単一のプリミティブとして設計される際は，ブロック暗号と同様に何段もの繰り返し構造をもつことが多い．特に SHA-2 の圧縮関数と SHA-3 で用いられる置換は繰り返し構造をもつ．鍵がないという特殊性もあり，圧縮関数や置換のみでなく，ハッシュ関数全体を（モードでなく）単一のプリミティブとみなして安全性を評価することも多い．

3. プリミティブの古典的な安全性評価

前章にて「各プリミティブが破れないということは，究極的には世界中の暗号研究者が攻撃を試みても破れないということによってのみ担保される」と述べた．本章ではもう少し具体的に，共通鍵暗号技術のプリミティブが破れるとはそもそもどういうことか，あるいは安全性がどう評価されるかということについて，二つの評価軸から説明する．

3.1 セキュリティパラメータと汎用攻撃

一般に，暗号技術の安全性を特徴づけるパラメータをセキュリティパラメータと呼ぶ．本稿では簡単のため，セキュリティパラメータといえば鍵長あるいはハッシュ関数の出力長を指すこととする．

当然であるが，鍵長が短い暗号は全く安全でない．例えば秘密鍵が 3 ビット（＝鍵の個数 8 個）しかない暗号は，総当たりで容易に秘密鍵を特定できてしまう．

換言すると，暗号の安全性には限界がある．例えば鍵長が k ビットの場合，2^k 個の鍵を総当たりで探索すればいつかは正しい鍵を見つけられる．どんなに安全に設計された暗号でも時間 2^k 以上は安全性を保てない．

ハッシュ関数にも同じようなことがいえる．出力長が n ビットのハッシュ関数 H は，たとえ理想的にランダムな関数でも，H をおよそ $2^{n/2}$ 回計算すれば高確率で衝突を見つけられることが分かっている．この攻撃は誕生日のパラドックスという概念を利用するもので，誕生日攻撃という．

上述の総当たりや誕生日攻撃は，攻撃対象のプリミティブによらず汎用的に適用できる攻撃ということで，汎用攻撃と呼ばれる．どれだけ注意深く設計しても，共通鍵暗号技術の安全性は，対応する汎用攻撃の計算時間までしか担保できない．

3.2 プリミティブを破る攻撃

では特定の暗号プリミティブに対し新しい攻撃アルゴリズムを思いついたとき，それが非自明な攻撃だとみなせるのはいつかというと，攻撃アルゴリズムの計算量が汎用攻撃の計算量を下回るときである．

例えば，鍵長 128 ビットのブロック暗号の鍵を計算量 2^{100} で暴く攻撃アルゴリズムを見つけたとする．128 ビットの鍵を総当たりで探索するには計算量 2^{128} を要するため，2^{100} は汎用攻撃（総当たり探索）の計算量より小さい．汎用攻撃より計算量が小さいということは，この暗号にはほかの暗号にない弱点があると考えることができ，理論的には「破れた」とみなされる[注3]．

計算量 2^{100} のアルゴリズムを実行することは実際には不可能である．しかし，鍵長 128 ビットのブロック暗号が二つあって，片方は鍵の総当たり探索をしないと破れないがもう一方は非自明な攻撃があるとなると，やはり後者の方が安全性の信頼は落ちる．またいったんそのような攻撃が見つかれば，研究を進めることで必要な計算量がどんどん削減されていく可能性がある．

3.3 攻撃可能段数

2.3 節で述べたように，ブロック暗号やハッシュ関数といったプリミティブは繰り返し構造をもつことが多い．そのような構造をもつプリミティブの安全性評価指標として，攻撃可能段数という考え方がある．

例えばいま，誰か共通鍵暗号の研究者が新しいブロック暗号を設計したとする．設計者は自分の作った暗号を広く使ってもらうべく，仕様を全世界に公開する．するとほかの研究者は，その暗号が安全かどうか確かめるため，攻撃の研究を始める．鍵長が例えば 128 ビットなら，総当たり探索の計算量 2^{128} 未満の攻撃を見つければ攻撃者の「勝ち」であり，その暗号は破られたことになる．

しかし，プロが注意深く真面目に設計したブロック暗号はそう簡単に破れるものではない．設計者は既存の攻撃を熟知し，対策を取っているからである．

そこでまず，その暗号の繰り返し段数を削減して少し弱めたものを攻撃することを試みる．例えばブロック暗号の元の繰り返し段数が 14 段あるとして，段数を 4 段まで減らした暗号なら計算量 2^{128} 未満の攻撃があるのではないか，と考えるのである．4 段まで弱めて破れたら次は 5 段にしてみて，それも破れたら今度は 6 段に戻して……と，少しずつ段数を増やしていく．元の 14 段まで破れたら，その暗号は破れたことになる．14 段まで破れなくとも，13 段くらいまで破れると，元の 14 段も破れてしまうのでないかと何となく不安になってくる．

既存のブロック暗号が破れるときは，このように，徐々に破れる段数が増えていって最終的に元の段数が破れるという流れをたどることが多い．たとえ攻撃に要する計算量が非常に大きくとも，総当たり探索より明らかに小さな計算量で攻

(注 3)：この見方は最も典型的なものであるが，設計者が初めからより低い安全性を主張している場合はこの限りでない．

撃可能な段数を伸ばせれば，それは意味のある結果とみなされる．AES-128 の例でいえば，（最も標準的な単一鍵設定で）破れているのは 10 段中 7 段までであり，最も計算量が小さいものでは 7 段 AES-128 を 2^{100} 未満の計算量で破る[18]．

なお，注目する安全性によって攻撃可能段数は変化しうることに注意されたい．例えば特定のハッシュ関数について，原像計算困難性が破れる段数と衝突耐性が破れる段数は一般に異なりうる．

また，総当たり探索より計算量が小さい攻撃を見つけても，計算量の削減幅が小さい場合は暗号を本当に破ったといってよいのかどうかの議論が生じる．例えば段数削減をしていないオリジナルの AES を総当たり探索の 1/4 程度の計算量で破ると主張する攻撃もある[19]~[21]が，計算量削減の幅が小さいうえに，解析手法を発展させたとしても大きな計算量削減が見込まれないのでないかという見方もあり[22]，これらの攻撃が AES への脅威につながるというコンセンサスが得られているわけではない[23],[24]．

共通鍵暗号技術及び古典的攻撃のより詳細な話題については，本誌に以前掲載された解説論文[25]~[28]なども参照されたい．

4. 初期の量子攻撃

Shor のアルゴリズムが発表されたのと前後して，共通鍵暗号技術の安全性にも明確に影響を及ぼす量子アルゴリズムが発表された．Grover のアルゴリズム[29]と BHT のアルゴリズム[30]である．

4.1 Grover のアルゴリズム

突然だが，以下の問題を考えてみる．

問題 1 入力として n ビットのビット列を取って 0 か 1 を出力する関数 $f:\{0,1\}^n\to\{0,1\}$ があり，$f(x)=1$ を充たす x がただ一つ存在すると仮定する．$f(x)=1$ となる x を見つけよ．

大雑把に，この問題は暗号の秘密鍵を探索する問題の一般化とみなせる．例えば，幾つかのデータ $P_1,\cdots,P_m$ と，それを暗号 E で暗号化した暗号文 $C_1=E_K(P_1),\cdots,C_m=E_K(P_m)$ をもっている状況下で，秘密鍵 K を探索する問題を考える．鍵が n ビットのビット列だとすると，関数 $f:\{0,1\}^n\to\{0,1\}$ を

$$f(x):=\begin{cases}1 & C_1=E_x(P_1),\cdots,C_m=E_x(P_m)\text{ が成り立つとき}\\ 0 & \text{それ以外のとき}\end{cases}$$

で定義すると，$x=K$ のときのみ $f(x)=1$ となる[注4]．

問題 1 を解くためにはどれくらい計算量がかかるだろうか．もし f について何の前情報ももっていなければ，秘密鍵の総当たり探索と同様，全ての x について $f(x)$ の値を計算してみるしかない．つまり，f を大体 2^n 回計算する必要がある．

これに対し Grover は 1996 年，問題 1 を計算量およそ $\sqrt{2^n}$ で解く量子アルゴリズムを示した[29]．$\sqrt{2^n}$ という計算量は（入力長 n に対し）依然として指数的に大きいが，古典的に必要だった計算量 2^n に比べると大幅なスピードアップである．具体的なパラメータを当てはめるとその影響力の大きさが分かる．

例えば $n=128$ なら，$\sqrt{2^n}=2^{64}$ である．古典計算機と量子計算機のスピードは簡単に比較できるものではないが，SHA-1 というハッシュ関数の衝突を実際に計算した 2017 年の論文[31]では，実際に関数 2^{63} 回分の計算を行っているという記述があり，2^{64} という計算量は非現実的なものではない．しかし仮に 2^{63} あるいは 2^{64} 回の計算を 1 年で実行できる計算機があったとしても，2^{128} 回の計算には 1000 京年（！）の時間を要する．

ここまで簡単のため $f(x)=1$ を充たす x は一つしかないとしていたが，そのような解 x が複数あるときにも同様の高速化が得られる．例えば解が t 個存在するとき，問題を解く古典計算量（古典計算機を用いたときにかかる計算量）は $2^n/t$ だが，これが $\sqrt{2^n/t}$ にまで高速化される[32]．

Grover のアルゴリズムは鍵の探索のみでなくありとあらゆる探索問題に応用が利く．出力が n ビットのハッシュ関数 H とある値 y が与えられたとき，$H(x)=y$ となる x を探索するには古典的に計算量 2^n を要するが，Grover のアルゴリズムを使えば（理論上は）秘密鍵の探索同様に $\sqrt{2^n}$ まで計算量を下げられる．

4.2 BHT のアルゴリズム

BHT のアルゴリズムは，n ビット出力のハッシュ関数の衝突を，計算量 $2^{n/3}$ で発見する[30]．このアルゴリズムはハッシュ関数の種類によらず適用できる汎用攻撃である．なお BHT というのは，アルゴリズムを見つけた Brassard・Høyer・Tapp の 3 人の頭文字である．3.1 節で説明したとおり，古典的な汎用衝突攻撃（誕生日攻撃）の計算量は $2^{n/2}$ であったので，汎用衝突攻撃についても量子アルゴリズムによる高速化が得られることになる．

なおこの BHT アルゴリズムは，$2^{n/3}$ という莫大な大きさの，量子重ね合わせアクセス可能なメモリ[33]（以下，「量子メモリ」）を必要とする．多項式サイズの量子メモリしか使えない場合，現状最も高速な量子汎用衝突攻撃は CNS のアルゴリズム[34]で，計算量は $2^{2n/5}$ である．BHT よりは少し遅いが，古典の誕生日攻撃よりは高速である．

（注 4）：データの個数 m には少し気を付ける必要があるが，典型的なブロック暗号なら数個あれば充分である．例えば AES-128 の鍵探索なら，$m=2$ で事足りる．

4.3 Grover と BHT のアルゴリズムが意味すること

Grover のアルゴリズムや BHT のアルゴリズムが使えるとなれば，暗号の鍵長やハッシュ関数の出力長などのパラメータ設定を見直さねばならない．

秘密鍵の総当たり攻撃に 2^k 以上の時間耐えるようにしたい場合，古典的には鍵長は k ビットあれば十分だった．しかし Grover のアルゴリズムを用いた総当たり攻撃に同程度の時間耐えるためには，倍の $2k$ ビット必要になる．

ハッシュ関数の出力長についても同様である．時間 $2^{n/2}$ の汎用衝突攻撃に耐えようとすると古典的には n ビットで十分だった．しかし BHT アルゴリズムによる衝突攻撃に対して同程度の時間耐えようとすると，1.5 倍の出力長が必要になる．Grover のアルゴリズムを用いた原像探索の影響まで考慮すると，2 倍の出力長が必要ということになる(注5)．

4.4 共通鍵暗号技術には大した影響がない？

Grover や BHT の量子アルゴリズムによる攻撃に耐えるためには，古典と比べて鍵の長さやハッシュ関数の出力長を 2 倍程度にする必要がある．しかし見方を変えると，パラメータが少し大きいものを使えばよいというだけである．この影響は Shor のアルゴリズムが RSA 暗号を多項式時間で破るというのとはわけが違う．RSA 暗号の鍵長を 2 倍にしたところで，Shor のアルゴリズムを用いた攻撃にかかる計算量は理論上そこまで大きくならない．また共通鍵暗号技術は公開鍵暗号技術と違って整数や離散対数などの代数的性質を使わないため，Shor のアルゴリズムを適用したところで破れそうにない．

こういった事情のせいか，Grover や BHT のアルゴリズムが発表されても，共通鍵暗号技術のポスト量子安全性は公開鍵暗号技術と比べてさほど盛んに研究されてこなかった．特に，（対象によらず適用できる汎用攻撃でなく）特定の共通鍵暗号の内部構造を利用するような攻撃アルゴリズムは余り研究されなかった．

5. 桑門・森井の多項式時間攻撃と攻撃のモデル

この流れが変化しだしたきっかけの一つが，2009〜2012 年に桑門・森井が示した 3 段 Feistel 暗号及び Even-Mansour 暗号への多項式時間攻撃[35]〜[37]である．これらの暗号はいずれもプリミティブというよりはモードで，古典的には多項式時間攻撃に対して安全だという証明がついていた[38],[39]．しかし桑門・森井はこれらの暗号を多項式時間で破る量子アルゴリズムを発見した．

なお攻撃には「暗号化オラクルへ量子クエリを行える」という仮定が必要である．これは「量子計算機上に秘密鍵の埋め込まれた暗号化アルゴリズムが実装されている」ということを意味し，かなり強い仮定である（5.2 節にて詳述）．そのため，現実世界で使われている共通鍵暗号技術が急に破られるということはない．それでもなお，古典的には安全と証明されることがよく知られている共通鍵暗号技術の中にも多項式時間量子アルゴリズムで破れるものがあることを示したという意味で，桑門・森井の結果の意義は大きい．

攻撃の要は Simon という人が発見した量子アルゴリズム[40]なので，まずは Simon のアルゴリズムについて説明する．その後，Even-Mansour 暗号への攻撃を例にとって桑門・森井の結果を紹介する．

5.1 Simon のアルゴリズム

Simon の量子アルゴリズムが解く問題は以下のものである．なお $\oplus$ はビット列同士の排他的論理和を表す．

問題 2 あるビット列 $s\in\{0,1\}^n$ と入出力が n ビットの関数 $f:\{0,1\}^n\to\{0,1\}^n$ があって，以下の 2 条件を満たすとする：

1. $f(x\oplus s)=f(x)$ が任意の x について成り立つ．
2. $f(x)=f(y)$ であれば，$y=x$ または $y=x\oplus s$ である．

関数 f だけが与えられ s が分からないとき，s を特定せよ．

古典計算機でこの問題を解くには指数時間を要することが証明されるが，Simon の量子アルゴリズムを用いれば多項式時間で s を特定できてしまう[40]．条件 1 は s が演算 $\oplus$ について関数 f の周期であることを示しているため，問題 2 は関数の周期を探索する問題であると捉えられる．Shor のアルゴリズムも高速な周期探索がその本質であり，二つのアルゴリズムは密接に関係している．

5.2 Even-Mansour 暗号

Even-Mansour 暗号[39]は以下の要素から成る．

・2 つの n ビットの秘密鍵 K_1，K_2

・n ビットのビット列がなす集合 $\{0,1\}^n$ 上の置換 P

ここで，置換 P は秘密情報を含んでおらず，攻撃者ですら手元の計算機で出力値を計算できるような公開置換とする．これら K_1, K_2, P を用いた Even-Mansour 暗号の暗号化関数 E_{K_1,K_2} と復号関数 D_{K_1,K_2} はそれぞれ $E_{K_1,K_2}(x):=P(x\oplus K_1)\oplus K_2$ 及び $D_{K_1,K_2}(x):=P^{-1}(x\oplus K_2)\oplus K_1$ で定められる（図 3）．平文と暗号文はいずれも n ビットのビット列である．

Even-Mansour 暗号は理想化されたモデルのようなもので，これを暗号としてそのまま使うことは余りない．しかし

(注 5)：なお説明を簡単にするため，本稿ではほかに断りの無い限り，暗号技術を量子計算機上に実装するコストや量子誤り訂正などにかかるコストは考慮に入れないものとする．これは攻撃者にとって有利な想定であるが，重要なデータを数十年単位で長期的に安全に保護することを考えると，より攻撃者に有利な状況を想定して対策を取った方が安心である．

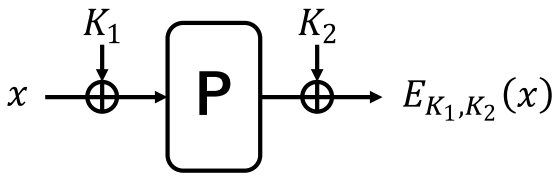


図 3　Even–Mansour 暗号　　変数は全て n ビットとする．

ISO 標準の暗号技術である Chaskey[41),42)] は，入力メッセージが短いときほぼ Even–Mansour 暗号の形になる．

5.3　攻撃のモデルについて

暗号の安全性について議論する際は，攻撃者に暗号化関数のオラクル（暗号化オラクル）が与えられるとモデル化することが多い．Even–Mansour 暗号の例だと，攻撃者が平文 x を選んでオラクルに送れば，オラクルは対応する暗号文 $E_{K_1,K_2}(x)$ を返してくれる．攻撃者は何度でも平文 x を自由に選んでオラクルに聞くことができる（図 4）．このオラクルは，現実世界でいえばサーバで動いている暗号化プログラムあるいは IC チップに埋め込まれた暗号化回路などをモデル化したものである．Evan–Mansour 暗号はこのモデルで，古典計算量 $2^{n/2}$ まで安全であることが示されている[注6)]．

攻撃者が量子計算機をもっているという状況では，攻撃のモデルが変わってくる．二つのモデルを考えることができ，それぞれ Q1 モデル・Q2 モデルと名前が付いている[43)]．

まず一番考えやすいモデルは，暗号化オラクルは古典のモデルから変わらず，攻撃者の計算機が単に量子計算機に変わるというものである．この攻撃モデルを Q1 モデルという（図 5）．

もう一つのモデルは，暗号化オラクルまで量子計算に対応していると仮定するもので，Q2 モデルと呼ばれる．量子計算が古典計算と大きく異なるのは，複数の状態を重ね合わせたまま一度に計算できるという点である．この特性が様々な計算の高速化の肝となるのだが，Q2 モデルでは暗号化オラクルがこの量子重ね合わせ計算に対応するとモデル化する（図 6）．このモデルは本質的に，秘密鍵の埋め込まれた暗号化回路が量子計算機上に実装されているという状態を想定している．

5.4　Even–Mansour 暗号への多項式時間攻撃

桑門・森井による Even–Mansour 暗号への多項式時間攻撃[37)]は，Q2 モデルにおける攻撃である．つまり，暗号化関数を含めた全てが量子重ね合わせで計算できるというモデルでの攻撃である．

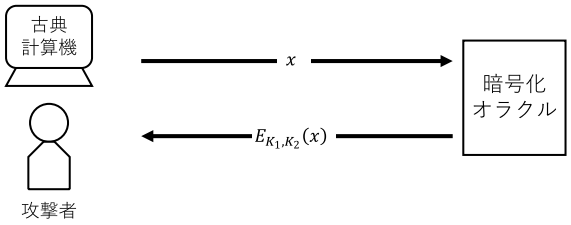


図 4　古典攻撃のモデル

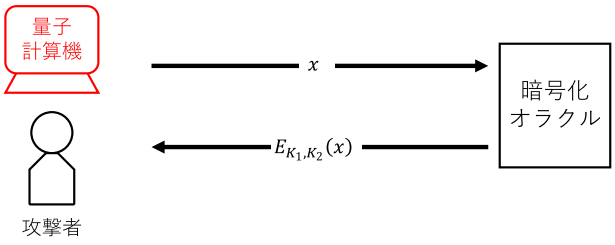


図 5　Q1 モデル

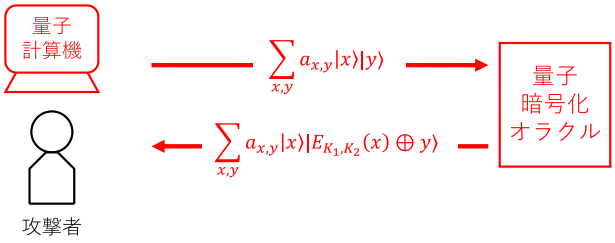


図 6　Q2 モデル

攻撃の概要は以下のとおりである．まず関数 $f(\mathrm{x})$ を $f(\mathrm{x}):=E_{K_1,K_2}(x)\oplus P(x)$ と定義する．すると

$$\begin{aligned} f(x\oplus K_1) &= E_{K_1,K_2}(x\oplus K_1)\oplus P(x\oplus K_1)\\ &= (P(x\oplus K_1\oplus K_1)\oplus K_2)\oplus P(x\oplus K_1)\\ &= P(x)\oplus K_2\oplus P(x\oplus K_1)\\ &= P(x)\oplus E_{K_1,K_2}(x)\\ &= f(x) \end{aligned}$$

より，f は K_1 を周期にもつ周期関数である（つまり**問題 2** の条件 1 が満たされる）．また今 Q2 モデルを考えているので，E_{K_1,K_2} も P も量子重ね合わせで計算することができ，ゆえに f も量子重ね合わせで計算することができる．よって f に Simon のアルゴリズムを適用できて，K_1 を得ることができる．いったん K_1 を得てしまえば，あとは関係式 $E_{K_1,K_2}(x)\oplus P(x\oplus K_1)=K_2$ を用いて K_2 も計算できる．Simon のアルゴリズムは多項式時間アルゴリズムなので，この攻撃全体も多項式時間アルゴリズムである．

なお上記の議論では**問題 2** の条件 2 を無視しているが，P がランダムであれば条件 2 が満たされなくても差し支えないことが示される[44)]．一つめの条件，つまり関数が周期をもつかという点が最も重要である．

(注 6)：置換 P は完全にランダムに選ばれたというモデル（ランダム置換モデル）での証明である．実際には暗号化関数のみでなく，復号化関数のオラクルが攻撃者に与えられても安全であることが証明される．ここでの「安全」というのは，秘密鍵を暴くことだけでなく，暗号化関数・復号関数のオラクルが P や秘密鍵と全く関係のないランダム置換のオラクルと識別することすらできない，という意味である．

6. Q2 モデルにおける様々な量子攻撃

桑門・森井による多項式時間攻撃の発見以降，Q2 モデルにおいて様々な量子攻撃が発表された．まず特筆すべきは 2016 年に CRYPTO で発表された Kaplan らによる結果で，CBC-MAC，PMAC，GCM，OCB などの多種多様な MAC や AEAD のモードを Q2 モデルにおいて多項式時間で破るというものである[44]．攻撃の根底にあるアイデアは桑門・森井のアイデアと同様で，何らかの秘密情報を周期にもつ関数をオラクルから構成し，Simon のアルゴリズムを適用するというものである．同時期に Santoli と Schaffner も CBC-MAC を Simon のアルゴリズムで破れるという研究結果を発表している[45]．

その後も Simon のアルゴリズムを応用した多項式時間攻撃が多数発表された．例を挙げきれないが，ブロック暗号への古典的な攻撃であるスライド攻撃の高速化[44),(46]とその関連鍵攻撃への応用[47]，4 段 Feistel 暗号の識別[48]，Kaplan らの手法では破れなかった MAC への攻撃[49]，などがある．

また Simon のアルゴリズム以外の応用も進んでいる．Poly1305 という MAC を Shor のアルゴリズムで破るという結果[49]や，Kuperberg のアルゴリズム[50]という Simon や Shor のアルゴリズムとは少し違ったタイプの周期探索問題を解くアルゴリズムを適用できるという結果もある[51]．Kuperberg のアルゴリズムは多項式時間アルゴリズムではなく，入力サイズに対して $2^{O(\sqrt{n})}$ 程度の計算量がかかる．しかしこの計算量は依然として Grover による鍵全数探索より圧倒的に高速で，共通鍵暗号技術に対する攻撃としてはかなり計算量が小さい部類に入る．

指数時間の計算量まで許容して，とにかくできる限り一番速い量子アルゴリズムを研究するという方向性も自然かつ重要である．共通鍵プリミティブへの古典的な攻撃手法の代表的なものとして差分解読法[52]や線形解読法[53]，積分攻撃[54]などがあるが，そういった古典攻撃を量子計算の力で高速化するという研究も行われている[43),(55),(56]．古典的な攻撃手法は，その途中で何らかの性質を充たすデータが存在するか判定したり個数を数えたりする作業に大きな計算量を割くことが多いが，そういった判定や数え上げは Grover のアルゴリズムと同程度の高速化が得られることがある（つまり，元の計算量を T として，$\sqrt{T}$ 程度まで計算量を下げられることがある）．

ほかに重要な攻撃として，Leander と May による FX 構成[57]への攻撃がある[58]．FX 構成は Even-Mansour 暗号の置換 P を別のブロック暗号に取り換えたような構成をしている（図 7）．真ん中のブロック暗号 E の鍵 K が m ビットのとき，FX 構成を古典計算で破るには計算量 $2^{(m+n)/2}$ の攻撃まで安全だということが証明されている[57]．Leander と May は，Grover と Simon のアルゴリズムを上手く組み合わせることで，FX 構成を計算量およそ $2^{m/2}$ で破れることを示した．

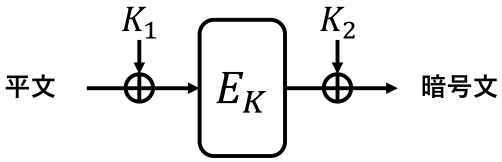


図 7　FX 構成　　平文と暗号文及び K_1 と K_2 は n ビット，中央のブロック暗号 E_K の鍵 K は m ビットとする．

7. Q1 モデルにおける量子攻撃

前章までで Q2 モデル（攻撃者の計算機のみでなく，オラクルまで量子計算に対応したモデル）における量子攻撃を紹介した．これらは古典攻撃より圧倒的に計算量が小さく場合によっては指数的高速化が得られる．しかし Q2 モデルは攻撃者に有利すぎるのでないかという批判もある．

こういった事情もあり，Q1 モデル（攻撃者の計算機のみ量子でオラクルは古典のモデル）における攻撃は Q2 モデルの攻撃より現実的な影響が大きいとみなされる[注7]．RSA 暗号に対する Shor のアルゴリズムを用いた攻撃も，いうなれば Q1 モデルにおける攻撃である（公開鍵暗号では暗号化用の鍵が公開されており，そもそも暗号化オラクルがなくても誰でも暗号化できる）．

現在のところ，Q1 モデルにおいて Q2 モデルのように多項式時間の攻撃が見つかっているわけではない．前章までに紹介した Q2 モデルの多項式時間攻撃は Simon のアルゴリズムなどを利用するが，オラクルが古典だとそれらのアルゴリズムを基本的に適用できなくなってしまうのである．

それでもなお，古典攻撃より高速な量子攻撃が多数研究されている．例えば，差分解読や線形解読法などの古典的攻撃手法も，状況によっては Q1 モデルで Grover のアルゴリズムと同程度の高速化が得られる[43]．

7.1 Even-Mansour 再び

また 5 章で紹介した Even-Mansour 暗号への（Q2 モデル）多項式時間攻撃を提案した桑門・森井の論文[37]において，Even-Mansour 暗号への Q1 モデル攻撃が提案されている．攻撃の計算量は $2^{n/3}$ であり Q2 モデルの多項式時間と比べると大きいが，古典攻撃の限界が $2^{n/2}$ であることを鑑みるとやはり高速化が得られている．

なおこの攻撃は BHT のアルゴリズム（4.2 節参照）と似たアイデアに基づくもので，サイズ $2^{n/3}$ の量子メモリが必要になる．量子メモリが多項式サイズ程度しかない場合は CNS のアルゴリズム（4.2 節参照）を応用して類似の攻撃を実行できるが[59),(注8]，計算時間が $2^{3n/7}$ に増えてしまう．つ

(注 7)：それでもなお，Q2 モデルにおける攻撃の研究は重要である．後述のオフライン Simon のアルゴリズムのように，Q2 モデルの攻撃をベースとして新しい Q1 モデルの攻撃が発見される可能性がある．

表 1　Q1 モデルにおける Even-Mansour 暗号への攻撃に必要な計算量および量子メモリ

	計算量	量子メモリ
古典	$2^{n/2}$	—
桑門・森井	$2^{n/3}$	$2^{n/3}$
CNS ベースの攻撃	$2^{3n/7}$	多項式
オフライン Simon	$2^{n/3}$	多項式

まり BHT を応用すれば莫大な大きさのメモリが必要となり，CNS を応用すれば計算量が増えてしまうのである．

7.2　オフライン Simon のアルゴリズム

これら攻撃の短所を解決したのが，Bonnetain らによる「オフライン Simon」のアルゴリズムである[60]．オフライン Simon を用いれば，多項式サイズの量子メモリしかなくても，Q1 モデルにおいて Even-Mansour 暗号を時間 $2^{n/3}$ で破ることができる（表 1）．オラクルクエリは古典のまま，攻撃者の手元の計算機の計算（オフライン計算）でのみ Simon のアルゴリズムを上手く利用するため，オフライン Simon という名前が付いている．

オフライン Simon のアルゴリズムのベースは，Q2 モデルにおける桑門・森井の多項式時間攻撃である．桑門・森井の多項式時間攻撃は暗号化関数の量子オラクルから作った関数に Simon のアルゴリズムを適用していたが，Q1 モデルでは古典オラクルしか使えない．そこで古典オラクルのみを利用して，Simon のアルゴリズムを適用するために必要な（量子重ね合わせ）データを作る．

まず古典クエリを行って平文・暗号文のペアを集める．暗号文を一つ手に入れるごとに，その内容に応じて量子メモリの状態を少しずつ変化させていく．これを $2^{n/3}$ 回繰り返し，出来上がった量子状態を $|\phi\rangle$ と書くことにする．紙幅の関係上詳細は割愛するが，上手く状態 $|\phi\rangle$ を作り上げて Grover のアルゴリズムを組み合わせれば，桑門・森井の攻撃のように Simon のアルゴリズムを適用できることが分かる．

このオフライン Simon のアルゴリズムは FX 構成にも適用でき，同じく量子メモリが多項式サイズでも $m \leq 2n$ なら計算量 $2^{(n+m)/3}$ で鍵を回復できる[60]．

8.　Grover の壁

3.3 節で，プリミティブへの攻撃には攻撃可能段数という考え方があると述べた．おさらいすると，ブロック暗号を攻撃するときはまず，繰り返し段数を減らして強度を弱めてみる．この弱めた暗号について，総当たり探索より小さい計算量で秘密鍵を暴く攻撃がないか研究するのである．それが成功したら，攻撃可能な段数を徐々に増やしていく．攻撃可能段数は早々伸びるものではない．

そこで当然気になるのは，量子アルゴリズムを使えば攻撃可能段数が伸びるかということである．桑門・森井の攻撃をはじめとして，少なくとも Q2 モデルでは多項式時間攻撃ができるのだから，幅広いブロック暗号の攻撃可能段数が伸びてしまうのではないかという懸念が出てくる．例えば古典的な攻撃手法である差分解読法と Simon のアルゴリズムを組み合わせれば 1 段くらい攻撃可能段数が伸びるのでないか．

しかし現在のところ，Q2 モデルでさえ，現在一般に利用されているようなブロック暗号の攻撃可能段数が伸びたという結果は，筆者の知る限り存在しない．攻撃可能段数がなかなか伸びない原因は，筆者の考えでは二つある．

まず一つめは，Simon のアルゴリズムが差分解読法などの古典的解読手法と相性が悪いとういことである．例えば差分解読法は，特定のビット列を段関数で変換した際に変換結果の分布が統計的に少し偏ること（差分特性）を利用する．攻撃可能なギリギリの段数までいくと，2^{-100} 程度の非常に小さい確率の偏りまで利用することもありうる．一方 Simon のアルゴリズムは周期関数を利用する．とある関数 f が周期 s をもつとは，いうなれば，x をランダムに選んだときに（ほぼ）確率 1 で等号 $f(x \oplus s) = f(x)$ が成立するということである．この確率が余りに小さいと Simon のアルゴリズムは全く非効率になってしまうため，2^{-100} 程度の小さい確率の偏りと上手く組み合わせるのは現状非常に困難に思われる．Shor のアルゴリズムや Kuperberg のアルゴリズムについても同様である．

二つめの（より重要な）理由は，攻撃成功の判定基準である総当たり探索の計算量も小さくなってしまうということである．古典的に，ブロック暗号への攻撃が意味のある攻撃と判定される条件は，その計算量が総当たり探索の計算量 2^k を下回ることであった（鍵長が k ビットの場合）．量子計算機が使えるとすれば，Grover のアルゴリズムを使って総当たり探索の計算量も $\sqrt{2^k}$ まで落ちる．ゆえに量子アルゴリズムを使った攻撃が意味のある攻撃とみなされるには，$\sqrt{2^k}$ より小さい計算量を達成する必要がある．

これは翻って，ブロック暗号の攻撃可能段数を伸ばすには Grover のアルゴリズムより大幅な高速化が本質的に必要だということを意味する．古典的に計算時間 T かかる攻撃を量子アルゴリズムの応用で $\sqrt{T}$ 程度にまで高速化できたとしても，攻撃成功の判断基準である鍵全数探索の計算量も同程度に落ちるため，攻撃可能段数を伸ばすという観点では余り意味がない．

そして，Grover のアルゴリズム以上の高速化を得ようとすると，古典的手法に Simon のアルゴリズムなどを組み合わせる以外の方法が現状ない．しかし前述のように Simon のアルゴリズムなどは古典的手法との相性が悪い．こういった事情で，ブロック暗号の攻撃可能段数を古典攻撃より伸ばすような量子攻撃はまだ見つかっていない．

ただ古典的手法を全く使わない量子計算特有の攻撃手法が

(注 8)：より正確には CNS の多重原像探索のアルゴリズムである．

今後見つかる可能性もあるため，研究を進める必要がある．なおモードについては，Q1 モデルでも Grover 以上の高速化が得られるという研究結果が報告されている[61]．

9. ハッシュ関数への衝突攻撃

プリミティブとしてのブロック暗号の攻撃可能段数は量子アルゴリズムを使っても余り伸ばせそうにない．ではハッシュ関数はどうだろうか．

前述のように，Grover 以上の高速化を得ようとすると，Simon のアルゴリズムなどを適用するしかなさそうである．そして Simon のアルゴリズムで暗号や MAC を攻撃する際は，まず鍵などの秘密情報に依存した周期をもつ周期関数を作り，その周期関数に Simon のアルゴリズムを適用していた．しかしハッシュ関数は鍵を使わないので，秘密情報を周期にした関数など作れない．ゆえに Simon のアルゴリズムを適用しても意味のある攻撃ができそうにない．

また，ハッシュ関数の汎用衝突攻撃は，Grover より高速化の幅が小さい．古典の汎用衝突攻撃である誕生日攻撃の計算量は $2^{n/2}$，BHT の量子衝突攻撃の計算量は $2^{n/3}$ である．$2^{n/3}$ というのは $2^{n/2}$ の平方根（$\sqrt{2^{n/2}}=2^{n/4}$）より大きい．

以上のことから，ブロック暗号の攻撃可能段数と同様，2019 年頃まではハッシュ関数の衝突攻撃可能段数も伸びると思われていなかった．それどころか，BHT のアルゴリズムが莫大な大きさのデバイスを必要とすることから，そんな大きなデバイスがあるならそもそも古典（並列）計算で同じような高速化が達成できるのではないかという見方すらあった[62]．

9.1 衝突攻撃の攻撃可能段数伸長

しかし 2020 年，量子計算機が利用可能な設定においては，ハッシュ関数の衝突攻撃可能段数が伸びることが指摘された[63]．

先述のように，汎用衝突攻撃の計算量は量子計算機が利用可能になっても余り変わらない．しかし見方を変えるとこれは，衝突攻撃の成功判定基準が古典でも量子でもさほど変わらないということである．一方先述のように，Grover のアルゴリズムを使うと差分解読法などの古典的な攻撃手法は元の計算量の平方根程度まで落ちることがある．これは，量子計算機が利用可能な世界では差分解読法の威力が汎用衝突攻撃より相対的に強まる，ということを意味するのである．

おさらいをすると，差分解読法では特定のビット列を段関数で変換した際に変換結果の分布が統計的に少し偏ること（差分特性）を利用する．この偏りの確率を差分確率というのであった．

いま，ある特定のハッシュ関数に対して，差分解読法に基づく衝突攻撃を発見したとしよう．利用する差分特性の差分確率を p とすると，攻撃の古典計算量は（ほかの要素を無視して，一番単純かつ理想的な場合）$T_C=1/p$ となる．古典汎用衝突攻撃の計算量は $2^{n/2}$ なので，この古典攻撃が有効とみなされるための必要条件は $T_C\leq 2^{n/2}$ である．換言すると，古典衝突攻撃が有効と判断されるためには

$$p\geq 2^{-n/2} \tag{1}$$

が満たされる必要がある．

一方，量子計算機が利用可能だとすると，差分解読法は Grover のアルゴリズムを用いて計算量 $T_Q=\sqrt{1/p}$ まで高速化できることがある．量子メモリを幾らでも使ってよいとすると，汎用衝突攻撃である BHT のアルゴリズムの計算量は $2^{n/3}$ なので，この攻撃が有効とみなされるための必要条件は $T_Q\leq 2^{n/3}$ である．換言すると，量子衝突攻撃が有効と判断されるための必要条件は

$$p\geq 2^{-2n/3} \tag{2}$$

である．

ここで式(1)と(2)を見比べると，量子計算機が利用可能な設定の方が，p に課された制約が緩和されていることが分かる．これはつまり，差分確率 p が $2^{-n/2}$ より小さく古典的に有効とみなされない衝突攻撃でも，量子計算機が利用可能という設定では有効な衝突攻撃とみなされるかもしれないということを意味する．

汎用衝突攻撃の計算量は想定する計算リソースにより異なるため，p の制約もより緩和される可能性がある．例えば多項式サイズの量子メモリしか使えないとなると，BHT のアルゴリズムは実行できないので，攻撃が有効かの判定基準は $2^{n/3}$ でなく（CNS のアルゴリズムの計算量である）$2^{2n/5}$ を採用するのが妥当である．この場合，p に課される条件は $p\geq 2^{-4n/5}$ となる．更に，計算リソースの大小を計算時間 T と使用する計算機のサイズ S の積で測ることにすると，p が 2^{-n} よりほんの少し大きい程度でも有効な攻撃につながりうる．

2020 年の論文[63]ではこの考えに基づき，実際に AES-MMO と Whirlpool という二つのハッシュ関数で衝突攻撃可能段数が古典より伸びることが示されている．いずれも，古典攻撃で使うには差分確率 p が小さすぎるような差分特性を利用しており，古典衝突攻撃より攻撃可能段数が 1 段ずつ伸びている．

その後，類似したアイデアに基づく攻撃が様々なハッシュ関数に対して研究され，多くのハッシュ関数で衝突攻撃の攻撃可能段数が古典より伸びている．例えば SHA-256 や SHA-512 では，古典的な衝突攻撃可能段数は現在のところそれぞれ 64 段中 31 段[64]及び 80 段中 27 段[65]までだが，量子計算機が利用可能な設定では 38 段及び 39 段まで伸びている[66]．SHA-3 においても古典より攻撃可能段数が伸びるという結果がある[67]．更に AES-256 をベースとしたハッシュ関数では，段関数削減なしのものが破れてしまうという研究結果も報告されている[68]．

なおハッシュ関数には鍵がなく仕様が公開されているため，衝突攻撃アルゴリズムを走らせる際もオラクルが要らないことに注意されたい．特に Q1 モデルや Q2 モデルといった攻撃モデルの区別はない．RSA 暗号に対する Shor のアル

ゴリズムを用いた攻撃と同様，衝突攻撃は攻撃者の手元の計算機で完結する．

10. 実装コストの見積り

前章までは，暗号やハッシュ関数などを量子計算機上に実装するためのコストや，量子誤り訂正のコストが無視できる立場を取っていた．これは攻撃者にとってかなり有利な前提であるが，できるだけ攻撃者に有利な状況を想定して，それでもなお破れない技術を使った方がより安全と考えられる．

一方，暗号技術の安全性評価を，暗号を量子計算機上に実装するためのコストや量子誤り訂正のコストも含めて見積もろうという研究も多数行われている．例えば AES や SHA-2 への汎用攻撃のコストを，量子計算機上に AES や SHA-2・SHA-3 を実装するコストまで含めて細かく見積もろうという研究[(69)~(75)]，オフライン Simon のアルゴリズムの実装コストを実際に見積もってみたという研究も行われている[(76)]．

11. そのほかの話題

共通鍵暗号技術に関係するそのほかの問題を解く量子アルゴリズムとして，衝突問題を一般化した多重衝突問題や k-XOR 問題を解く量子アルゴリズム，多重原像探索アルゴリズムなども発表されている[(34), (77)~(83)]．また本稿では紙幅の都合上説明できなかったが，Q1 モデル・Q2 モデル双方でモードの安全性を証明しようという研究も行われている[(84)~(94)]．特に最近では Q1 モデルで Even-Mansour 暗号を破るのに必要な計算量の下限が示され，先述の桑門・森井による攻撃やオフライン Simon のアルゴリズムを用いた攻撃の計算量はそれ以上改善できないことが証明された[(95)]．

12. おわりに

本稿では，共通鍵暗号技術のポスト量子安全性に関するこれまでの研究の流れと最近の動向について，主に攻撃アルゴリズムの観点から概観した．

Grover のアルゴリズムや BHT のアルゴリズムなどを適用することで，鍵の総当たり探索や衝突攻撃など，方式によらず適用できる汎用攻撃が高速化される．オラクルへの量子クエリが可能という設定の Q2 モデルでは，Simon のアルゴリズムなどを応用することにより，古典的に安全と証明されている様々なモードに対し多項式時間攻撃が可能になることが明らかになっている．Q1 モデルにおいても，方式によっては Simon のアルゴリズムを上手く使うことで必要なメモリの量を指数的に減らしたり，Grover のアルゴリズム以上の高速化を得たりすることが可能になる．ハッシュ関数の衝突攻撃は古典よりも大幅に段数が伸びる事例が多数見つかっている．

今後の展望として，ハッシュ関数のみでなくブロック暗号についても攻撃可能段数を伸ばすような手法がないか研究を進めることが重要であると筆者は考える．攻撃アルゴリズムの研究を進めることによって，共通鍵暗号技術の安全性の理解がより進むだけでなく，この分野特有の問題に着目して初めて得られるような全く新しいタイプの量子アルゴリズムが発見されることを期待する．

文　献

(1) R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2, pp. 120-126, 1978.
(2) N. Koblitz, “Elliptic curve cryptosystems,” Math. Comput., vol. 48, no. 177, pp. 203-209, 1987.
(3) P. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput., vol. 26, no. 5, pp. 1484-1509, 1997.
(4) U.S. Department of Commerce/National Institute of Standards and Technology (G. Alagic, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone, and D. Apon), “Status report on the third round of the NIST post-quantum cryptography standardization process,” NIST Interagency/Internal Report (NISTIR) 8413, 2022.
(5) 高木剛，“ポスト量子暗号の構成法とその安全性評価，”信学 FR 誌，vol. 11, no. 1, pp. 17-27, 2017.
(6) D. McGrew and J. Viega, “The security and performance of the Galois/Counter Mode (GCM) of operation,” Proc. INDOCRYPT 2004, LNCS, vol. 3348, pp. 343-355, 2004.
(7) U.S. Department of Commerce/National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication (FIPS PUB) 197, 2001.
(8) M. Liskov, R. Rivest, and D. Wagner, “Tweakable block ciphers,” J. Cryptol., vol. 24, no. 3, pp. 588-613, 2011.
(9) J. Jean, I. Nikolic, and T. Peyrin, “Tweaks and keys for block ciphers : The TWEAKEY framework,” Proc. ASIACRYPT 2014, Part II, LNCS, vol. 8874, pp. 274-288, 2014.
(10) C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. Sim, “The SKINNY family of block ciphers and its low-latency variant MANTIS,” Proc. CRYPTO 2016, Part II, pp. 123-153, 2016.
(11) T. Iwata, K. Minematsu, T. Peyrin, and Y. Seurin, “ZMAC : A fast tweakable block cipher mode for highly secure message authentication,” Proc. CRYPTO 2017, Part I, LNCS, vol. 10403, pp. 34-65, 2017.
(12) T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin, “Duel of the titans : The Romulus and Remus families of lightweight AEAD algorithms,” IACR Trans. Symmetric Cryptol., vol. 2020, no. 1, pp. 43-120, 2020.
(13) R. Merkle, “A certified digital signature,” Proc. CRYPTO 89, LNCS, vol. 435, pp. 218-238, 1990.
(14) I. Damgård, “A design principle for hash functions,” Proc. CRYPTO 89, LNCS, vol. 435, pp. 416-427, 1990.
(15) G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, “Sponge functions,” Ecrypt Hash Workshop, 2007.
(16) U.S. Department of Commerce/National Institute of Standards and Technology, “Secure Hash Standard (SHS),” Federal Information Processing Standards Publication (FIPS PUB) 180-4, 2015.
(17) U.S. Department of Commerce/National Institute of Standards and Technology, “SHA-3 standard : Permutation-based hash and extendable-output functions,” Federal Information Processing Standards Publication (FIPS PUB) 202, 2015.
(18) P. Derbez, P. Fouque, and J. Jean, “Improved key recovery attacks on reduced-round AES in the single-key setting,” Proc. EUROCRYPT 2013, LNCS, vol. 7881, pp. 371-387, 2013.
(19) A. Bogdanov, D. Khovratovich, and C. Rechberger, “Biclique

cryptanalysis of the full AES," Proc. ASIACRYPT 2011, LNCS, vol. 7073, pp 344-371, 2011.
(20) A. Bogdanov, D. Chang, M. Ghosh, and S. Sanadhya, "Bicliques with minimal data and time complexity for AES," Proc. ICISC 2014, LNCS, vol. 8949, pp 160-174, 2015.
(21) Biaoshuai Tao and Hongjun Wu, "Improving the biclique cryptanalysis of AES," Proc. ACISP 2015, LNCS, vol. 9144, pp. 39-56, 2015.
(22) 伊藤竜馬, "「CRYPTREC 暗号技術ガイドライン(軽量暗号)」掲載の暗号方式に関する安全性評価の動向調査," CRYPTREC 2021 年度外部評価報告書, 2022.
(23) CRYPTREC, "128 ビットブロック暗号 AES の安全性について," (https://www.cryptrec.go.jp/topics/cryptrec-er-0001-2011.html, 2011.
(24) U.S. Department of Commerce/National Institute of Standards and Technology (N. Mouha), "Review of the advanced encryption standard," NIST Interagency/Internal Report (NISTIR) 8319, 2021.
(25) 森井昌克, 寺村亮一, "ストリーム暗号の現状と課題,"信学 FR 誌, vol. 2, no. 3, pp. 66-75, 2009.
(26) 安田幹, 佐々木悠, "暗号学的ハッシュ関数—安全神話の崩壊と新たなる挑戦,"信学 FR 誌, vol. 4, no. 1, pp. 57-67, 2010.
(27) 金子敏信, "共通鍵暗号の安全性評価,"信学 FR 誌, vol. 7, no. 1, pp. 14-29, 2013.
(28) 藤堂洋介, "共通鍵暗号の発展—MISTY1 をめぐる創造と破壊,"信学 FR 誌, vol. 10, no. 1, pp. 23-33, 2016.
(29) L. Grover, "A fast quantum mechanical algorithm for database search," Proc. STOC 1996, pp. 212-219, 1996.
(30) G. Brassard, P. Høyer, and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions," SIGACT News, vol. 28, no. 2, pp. 14-19, 1997.
(31) M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov, "The first collision for full SHA-1," Proc. CRYPTO 2017, Part I, LNCS, vol. 10401, pp. 570-596, 2017.
(32) M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," Fortschritte der Physik : Progress of Physics, vol. 46, no. 4-5, pp. 493-505, 1998.
(33) G. Vittorio, S. Lloyd, and L. Maccone, "Quantum random access memory," Phys. Rev. Lett., vol. 100, no. 16, 2018.
(34) A. Chailloux, M. Naya-Plasencia, and A. Schrottenloher, "An efficient quantum collision search algorithm and implications on symmetric cryptography," Proc. ASIACRYPT 2017, Part II, LNCS, vol. 10625, pp. 211-240, 2017.
(35) 桑門秀典, 森井昌克, "量子アルゴリズムを用いた 3-Round Feistel 暗号の識別アルゴリズム,"第 21 回量子情報技術研究会, 2009.
(36) H. Kuwakado and M. Morii, "Quantum distinguisher between the 3-round Feistel cipher and the random permutation," Proc. ISIT 2010, pp. 2682-2685, 2010.
(37) H. Kuwakado and M. Morii, "Security on the quantum-type Even-Mansour cipher," Proc. ISITA 2012, pp. 312-316, 2012.
(38) M. Luby and C. Rackoff, "How to construct pseudorandom permutations from pseudorandom functions," SIAM J. Comput., vol. 17, no. 2, pp. 373-386, 1988.
(39) S. Even and Y. Mansour, "A construction of a cipher from a single pseudorandom permutation," J. Cryptol., vol. 10, no. 3, pp. 151-162, 1997.
(40) D. Simon, "On the power of quantum computation," SIAM J. Comput., vol. 26, no. 5, pp. 1474-1483, 1997.
(41) ISO/IEC 29192-6 : 2019, "Information technology—Lightweight cryptography—Part 6 : Message authentication codes (MACs)," 2019.
(42) N. Mouha, B. Mennink, A. Van Herrewege, D. Watanabe, B. Preneel, and I. Verbauwhede, "Chaskey : An efficient MAC algorithm for 32-bit microcontrollers," SAC 2014, Revised selected papers, LNCS, vol. 8784, pp. 306-323, 2014.
(43) M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Quantum differential and linear cryptanalysis," IACR Trans. Symmetric Cryptol., vol. 2016, no. 1, pp. 71-94, 2016.
(44) M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," Proc. CRYPTO 2016, Part II, LNCS, vol. 9815, pp. 207-237, 2016.
(45) T. Santoli and C. Schaffner, "Using Simon's algorithm to attack symmetric-key cryptographic primitives," Quantum Inf. Comput., vol. 17, no. 1 & 2, pp. 65-78, 2017.
(46) X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "On quantum slide attacks," SAC 2019, Revised selected papers, LNCS, vol. 11959, pp. 492-519, 2020.
(47) A. Hosoyamada and K. Aoki, "On quantum related-key attacks on iterated Even-Mansour ciphers," IEICE Trans. Fundamentals, vol. 102-A, no. 1, pp. 27-34, 2019.
(48) G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, and T. Iwata, "Quantum chosen-ciphertext attacks against Feistel ciphers," Proc. CT-RSA 2019, LNCS, vol. 11045, pp. 391-411, 2019.
(49) X. Bonnetain, G. Leurent, M. Naya-Plasencia, and A. Schrottenloher, "Quantum linearization attacks," Proc. ASIACRYPT 2021, Part I, LNCS, vol. 13090, pp. 422-452, 2021.
(50) G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem," SIAM J. Comput., vol. 35, no. 1, pp. 170-188, 2005.
(51) X. Bonnetain and M. Naya-Plasencia, "Hidden shift quantum cryptanalysis and implications," Proc. ASIACRYPT 2018, Part I, LNCS, vol. 11274, pp. 560-592, 2018.
(52) E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Proc. CRYPTO '90, LNCS, vol. 537, pp. 2-21, 1991.
(53) M. Matsui, "Linear cryptanalysis method for DES cipher," Proc. EUROCRYPT ' 93, LNCS, vol. 765, pp. 386-397, 1994.
(54) L. Knudsen and D. Wagner, "Integral cryptanalysis," Proc. FSE 2002, LNCS, vol. 2365, pp. 112-127, 2002.
(55) X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum security analysis of AES," IACR Trans. Symmetric Cryptol., vol. 2019, no. 2, pp. 55-93, 2019.
(56) A. Schrottenloher and M. Stevens, "Simplified MITM modeling for permutations : New (quantum) attacks," Proc. CRYPTO 2022, Part III, LNCS, vol. 13509, pp. 717-747, 2022.
(57) J. Kilian and P. Rogaway : "How to protect DES against exhaustive key search," Proc. CRYPTO 1996, LNCS, vol. 1109, pp. 252-267, 1996.
(58) G. Leander and A. May, "Grover meets Simon—Quantumly attacking the FX-construction," Proc. ASIACRYPT 2017, Part II, LNCS, vol. 10625, pp. 161-178, 2017.
(59) A. Hosoyamada and Y. Sasaki, "Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations," Proc. CT-RSA 2018, LNCS, vol. 10808, pp. 198-218, 2018.
(60) X. Bonnetain, A. Hosoyamada, M. Naya-Plasencia, Y. Sasaki, and A. Schrottenloher, "Quantum attacks without superposition queries : The offline Simon algorithm," Proc. ASIACRYPT 2019, Part I, LNCS, vol. 11921, pp. 552-583, 2019.
(61) X. Bonnetain, A. Schrottenloher, and F. Sibleyras, "Beyond quadratic speedups in quantum attacks on symmetric schemes," Proc. EUROCRYPT 2022, Part III, LNCS, vol. 13277, pp. 315-344, 2022.
(62) D. Bernstein, "Cost analysis of hash collisions : Will quantum computers make SHARCS obsolete? ," SHARCS 2009, workshop record, 2009.
(63) A. Hosoyamada and Y. Sasaki, "Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound," Proc. EUROCRYPT 2020, Part II, LNCS, vol. 12106, pp. 249-279, 2020.
(64) F. Mendel, T. Nad, and M. Schläffer, "Improving local collisions : New attacks on reduced SHA-256," Proc. EUROCRYPT 2013, LNCS. vol. 7881, pp. 262-278, 2013.
(65) C. Dobraunig, M. Eichlseder, and F. Mendel, "Analysis of SHA-512/224 and SHA-512/256," Proc. ASIACRYPT 2015, Part II, LNCS, vol. 9453, pp. 612-630, 2015.

(66) A. Hosoyamada and Y. Sasaki, "Quantum collision attacks on reduced SHA-256 and SHA-512," Proc. CRYPTO 2021, Part I, LNCS, vol. 12825, pp. 616-646, 2021.
(67) J. Guo, G. Liu, L. Song, and Y. Tu, "Exploring SAT for cryptanalysis : (Quantum) collision attacks against 6-Round SHA-3," Proc. ASIACRYPT 2022, Part III, LNCS, vol. 13793, pp. 645-674, 2022.
(68) S. Baek, S. Cho, and J. Kim, "Quantum cryptanalysis of the full AES-256-based Davies-Meyer, Hirose and MJH hash functions," Quantum Inf. Process., vol. 21, no. 5, article number 163, 2022.
(69) M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, "Applying Grover's algorithm to AES : Quantum resource estimates," Proc. PQCrypto 2016, LNCS, vol. 9606, pp. 29-43, 2016.
(70) M. Almazrooie, A. Samsudin, R. Abdullah, and K. Mutter, "Quantum reversible circuit of AES-128," Quantum Inf. Process., vol. 17, no. 5, article number 112, 2018.
(71) S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC," Proc. EUROCRYPT 2020, Part II, LNCS, vol. 12106, pp. 280-310, 2020.
(72) B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing AES as a quantum circuit," IEEE Trans. Quantum Eng., vol. 1, pp. 1-12, 2020.
(73) Z. Huang and S. Sun, "Synthesizing quantum circuits of AES with lower T-depth and less qubits," Proc. ASIACRYPT 2022, Part III, LNCS, vol. 13793, pp. 614-644, 2022.
(74) M. Amy, O. Matteo, V. Gheorghiu, M. Mosca, A. Parent, and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3," SAC 2016, Revised selected papers, LNCS, vol. 10532, pp. 317-337, 2017.
(75) P. Kim, D. Han, and K. Jeong, "Time-space complexity of quantum search algorithms in symmetric cryptanalysis : applying to AES and SHA-2," Quantum Inf. Process., vol. 17, no. 12, article number 339, 2018.
(76) X. Bonnetain and S. Jaques, "Quantum period finding against symmetric primitives in practice," IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2022, no. 1, pp. 1-27, 2022.
(77) A. Hosoyamada, Y. Sasaki, and K. Xagawa, "Quantum multicollision-finding algorithm," Proc. ASIACRYPT 2017, Part II, LNCS, vol. 10625, pp. 179-210, 2017.
(78) Q. Liu and M. Zhandry, "On finding quantum multi-collisions," Proc. EUROCRYPT 2019, Part III, LNCS, vol. 11478, pp. 189-218, 2019.
(79) A. Hosoyamada, Y. Sasaki, S. Tani, and K. Xagawa, "Quantum algorithm for the multicollision problem," Theor. Comput. Sci., vol. 842, pp. 100-117, 2020.
(80) L. Grassi, M. Naya-Plasencia, and A. Schrottenloher, "Quantum algorithms for the k-xor problem," Proc. ASIACRYPT 2018, Part I, LNCS, vol. 11272, pp. 527-559, 2018.
(81) M. Naya-Plasencia and A. Schrottenloher, "Optimal merging in quantum k-xor and k-xor-sum algorithms," Proc. EUROCRYPT 2020, Part II, LNCS, vol. 12105, pp. 311-340, 2020.
(82) A. Schrottenloher, "Improved quantum algorithms for the k-XOR problem," SAC 2021, Revised selected papers, LNCS, vol. 13203, pp. 311-331, 2022.
(83) G. Banegas and D. Bernstein, "Low communication parallel quantum multi-target preimage search," Proc. SAC 2017, Revised selected papers, LNCS, vol. 10719, pp. 325-335, 2018.
(84) M. Anand, E. Targhi, G. Tabia, and D. Unruh, "Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation," Proc. PQCrypto 2016, LNCS, vol. 9606, pp. 44-63, 2016.
(85) J. Czajkowski, L. Bruinderink, A. Hülsing, C. Schaffner, and D. Unruh, "Post-quantum security of the sponge construction," Proc. PQCrypto 2018, LNCS, vol. 10786, pp. 185-204, 2018.
(86) G. Alagic and A. Russell, "Quantum-secure symmetric-key cryptography based on hidden shifts," Proc. EUROCRYPT 2017, Part III, LNCS, vol. 10212, pp. 65-93, 2017.
(87) F. Song and A. Yun, "Quantum security of NMAC and related constructions—PRF domain extension against quantum attacks," Proc. CRYPTO 2017, Part II, LNCS, vol. 10402, pp. 283-309, 2017.
(88) A, Hosoyamada and T. Iwata, "On tight quantum security of HMAC and NMAC in the quantum random oracle model," Proc. CRYPTO 2021, Part I, LNCS, vol. 12825, pp. 585-615, 2021.
(89) M. Zhandry, "How to record quantum queries, and applications to quantum indifferentiability," Proc. CRYPTO 2019, Part II, LNCS, vol. 11693, pp. 239-268, 2019.
(90) A. Hosoyamada and T. Iwata, "4-Round Luby-Rackoff construction is a qPRP," Proc. ASIACRYPT 2019, Part I, LNCS, vol. 11921, pp. 145-174, 2019.
(91) R. Bhaumik, X. Bonnetain, A. Chailloux, G. Leurent, M. Naya-Plasencia, A. Schrottenloher, and Y. Seurin, "QCB : Efficient quantum-secure authenticated encryption," Proc. ASIACRYPT 2021, Part I, LNCS, vol. 13090, pp. 668-698, 2021.
(92) A. Hosoyamada and K. Yasuda, "Building quantum one-way functions from block ciphers : Davies-Meyer and Merkle-Damgård constructions," Proc. ASIACRYPT 2018, Part I, LNCS, vol. 11272, pp. 275-304, 2018.
(93) V. Maram, D. Masny, S. Patranabis, and S. Raghuraman, "On the quantum security of OCB," IACR Trans. Symmetric Cryptol., vol. 2022, no. 2, pp. 379-414, 2022.
(94) A. Hosoyamada and T. Iwata, "Provably quantum-secure tweakable block ciphers," IACR Trans. Symmetric Cryptol., vol. 2021, no. 1, pp. 337-377, 2021.
(95) G. Alagic, C. Bai, J. Katz, and C. Majenz, "Post-quantum security of the Even-Mansour cipher," Proc. EUROCRYPT 2022, Part III, LNCS, vol. 13277, pp. 458-487, 2022.

(ISEC 研究会提案，2023 年 3 月 3 日受付，
2023 年 4 月 3 日再受付)

細山田光倫（正員）

2014 京都大・理卒．2016 同大学院修士課程修了．同年日本電信電話(株)入社．以来，暗号分野の研究に従事．現在，NTT 社会情報研究所研究員．2021 名古屋大大学院博士課程修了．工博．IWSEC Best Paper Award（2017），SCIS 論文賞（2018），Asiacrypt Best Paper Award（2020）．

解　説　論　文

ユーザ行動と社会環境データの分析・推薦・可視化の実践的応用技術

Practical Technologies for Analysis, Recommendation, and Visualization of User Behavior and Social Environment Data

河合由起子 Yukiko KAWAI　栗　達 Da LI
小野晋太郎 Shintaro ONO

アブストラクト　Society 5.0 では，フィジカル空間におけるユーザの様々な振る舞いがデータとして複製されたデジタルツインを通じて，サイバー空間でそれらを分析・管理し，検索や推薦により高度に融合することで経済発展や社会課題の解決を図る人間（ユーザ）中心の社会を目指している．筆者らは，ユーザの振る舞いデータとして，携帯端末（スマートフォン）から得られる位置情報が付与された SNS データやレビューデータ，時刻や位置情報を含む犯罪・購買・感染などに関するオープンデータ，更にストリートビュー画像や建物・道路情報となる地理データを対象とし，経路や店舗・名所の推薦，危険地域の予測などに関する研究開発に取り組んできた．本稿では，スマートフォンをデバイスとしたデジタルツインにおけるデータ取得，管理，分析，可視化の基本的仕組みから，歩行者や自転車のユーザにとって安全で快適な行動支援の応用技術の紹介を通して，デジタルツインにおける社会課題解決の役割について言及する．

キーワード　行動分析，情報推薦，可視化，デジタルツイン，MaaS

Abstract　The aim of Society 5.0 is to create a human-oriented society that balances economic development and social problem solving using “digital twin”, in which various user behaviors in physical space are replicated in the form of data, analyzed and managed in cyberspace, to a highly level of integration through search and recommendation. We have been studying user behavior data, including SNS data and “review” data along with location information obtained from mobile devices (smartphones), publicly available data on crime, purchases, and infections including time and location information, and geographic data such as Google Street View images and building and road information, in order to develop a system for recommending routes, stores and attractions. We have also conducted research and development on routes, stores, attraction recommendations and hazard area prediction. In this paper, we present the role of digital twin in solving social problems, introduce the basic mechanisms of data collection, management, analysis, and visualization by digital twin using a smartphone device, as well as application technologies that provide a safe and comfortable mobility experience for pedestrians and cyclists using smartphone.

Key words　Behavior analysis, Information recommendation, Visualization, Digital twin, MaaS

1. はじめに

スマートフォン（以下，スマホ）のカメラや GPS の高性能化，メモリやストレージの大容量化の普及に伴い，実世界のユーザ行動データは管理，分析，可視化がサーバサイド（クラウド）だけでなくスマホのクライアントサイドでも処理されるようになり，サイバー空間とフィジカル空間の境界は曖昧になった．従来のサイバー・フィジカル空間をユーザ行動（behavior），蓄積管理（database），分析，可視化（User Interface）として循環または融合させるモデルとして，デジタルツインや XaaS (X as a Service) が注目されている（図 1）．

本稿では，実世界のユーザインタラクションとしてスマホから SNS やレビュー，センサのユーザ行動データを取得・管理し，Google ストリートビュー（GSV）や Open Street Map（OSM）などの Web・地理情報データと統合することで，時刻・位置に基づき分析する技術として，我々が取り組んできた経路推薦システムを紹介する．具体的には，安全・効率的で迷いに

河合由起子　正員　京都産業大学大学院先端情報学研究科，大阪大学サイバーメディアセンター
E-mail kawai@cc.kyoto-su.ac.jp
栗　達　福岡大学工学部
E-mail lida@fukuoka-u.ac.jp
小野晋太郎　正員　福岡大学工学部
E-mail onoshin@fukuoka-u.ac.jp
Yukiko KAWAI, Member (Graduate School of Frontier Informatics, Kyoto Sangyo University, and Cyber Media Center, Osaka University), Da LI, Nonmember (Faculty of Engineering, Fukuoka University), Shintaro ONO, Member (Faculty of Engineering, Fukuoka University).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.17 No.1 pp.72–80 2023 年 7 月

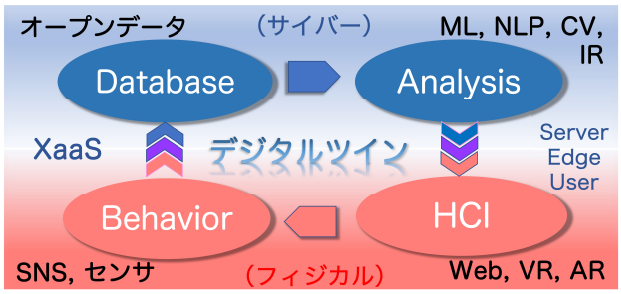


図 1　ユーザ行動とデータ分析と可視化の循環

くい経路や，心地よい経路を生成し，推薦提供するものである．加えて，COVID-19 以降の行動変容に適用すべく，ユーザの行動が社会課題の解決につながるような経路推薦技術のほか，スポットや他人との行動をシェアできるプランニング技術を紹介する．

2. SNS・地理情報分析に基づく意味的・幾何的ランドマークを考慮した経路推薦

従来の経路案内システムは主に自動車を対象としていたが，最近ではスマホなどの携帯端末上のサービスとして，二輪車や歩行者にまで一般化しつつある．本章では，GIS（地理情報システム）データと SNS による特徴的な地物の抽出，効率的な経路探索と推薦[(1)]，更に風景画像の分析を加えた快適な経路推薦の技術[(2)]を紹介する．

2.1 幾何的・意味的ランドマーク抽出

移動中にナビゲーション画面を注視すると，周辺への警戒が疎かになり，事故を引き起こしかねないとの懸念が指摘されている．その解決策として，音声によるガイダンスや，記憶しやすい地物（ランドマーク）を用いた案内方法が提案されている．

前者の方法は，音声が聞き取りやすい車内での利用には効果を発揮するが，歩行者・二輪車での利用においては，周囲の音声を遮断することになり安全性に課題がある．更に，GPS 機能が使えないときや道に迷ったときなど，ユーザの自己位置を特定することが困難な場合には利用できない．

後者の方法は，記憶しやすく視認性の高い地物をランドマークとして経路案内を行う方法であり，太古より人が地図を使わずに道案内をする際に用いられてきた．現在でも，郵便局やコンビニエンスストア，神社などをランドマークとして利用した店舗などの案内地図は多く見受けられる．副次的な効用として，周辺を観察しながら進路確認を行うため，危険回避にも役立つ．しかし，ユーザはランドマークを記憶する必要があるため，視認性の高い少数のランドマークを選んで提示することが必要である．すなわち，経路の認識に有効な複数のランドマークの組み合わせを，経路自体と同時に探索することが求められる．

本研究では，より少ない数のランドマークを組み合わせて，効率のよい経路案内を実現する．

従来よりランドマークを用いた経路案内システムは数多く提案されており，主に 2 種類のランドマークが用いられてきた．

1) 点のランドマーク（局所的ランドマーク）： 郵便局やコンビニエンスストアのように，近くまで行かなければ視認できないが，確認することでユーザの現在位置を高い精度で同定できる地物．

2) 面のランドマーク（広域的ランドマーク）： 電波塔や高層ビルなどのように，遠方からでも視認できるが，現在位置を大まかにしか同定できない地物．

これら点と面のランドマークは，その性質の違いから，経路案内の際に同時に使用することは適していない．例えば「東京タワーに向かって直進する」という面のランドマークを用いた経路案内においては，ユーザが選択可能な途中経路は複数あるため，続く案内で「途中でコンビニエンスストアに到達したら左に曲がる」のように点のランドマークと組み合わせることは適さない．一方，面のランドマークのみを用いる場合は，「東京タワーに向かっている途中で，スカイツリーが見えたらそちらに進む」といった案内しかできないため，使用するランドマークを切り替えるタイミングをユーザが判断することは難しい．

このような問題を解消するため，点と面に加え，新たなランドマークを定義する．

3) 線のランドマーク（線形的ランドマーク）： 電車通りや河川のようにすぐ近くまで行かなければ視認できないが，その範囲が線状に広がりをもつ地物．(3 種類のランドマークの例を図 2 に示す.)

このような経路は，最短経路と比べて経路長は長くなる可能性がある．しかし，ユーザは線のランドマークに至るまで面のランドマークに向かって進む経路を自由に選択でき，詳細な経路を覚えておく必要がない．3 種類のランドマークのうち特徴的なもの幾つか（タワー，大通り，コンビニなど）のみで目的地に到達できることから，記憶しやすい経路となり得る．

ランドマークは，点・面・線とは独立に，幾何的なランドマークと意味的なランドマークにも分類することができる（表 1）．幾何的なランドマークとは，文字どおりその形や色などが特異的であり，画像処理などで検出可能である．一方，意味的なランドマークとは，形や色合いなどに特に目立つ特徴はないものの，話題になっているカフェや混雑している店など，人間には発見しやすいものを指し，SNS などで共有されているソーシャルデータから取得可能である．

表 1　3 種類のランドマークの例

	幾何的	意味的
点	郵便局，コンビニ， ガソリンスタンド	話題のカフェ， 待ち合わせスポット
線	大通り，電車通り， 河川沿いの道路	人通りの多い商店街 渋滞している道路
面	電波塔や高層ビルなど 可視範囲の広い建築物	寺社など，地域内で存在 位置が容易に分かるもの

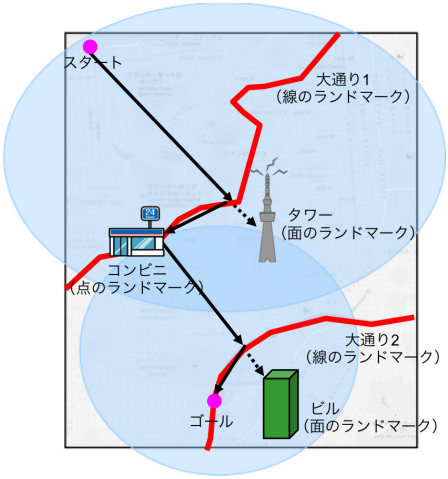
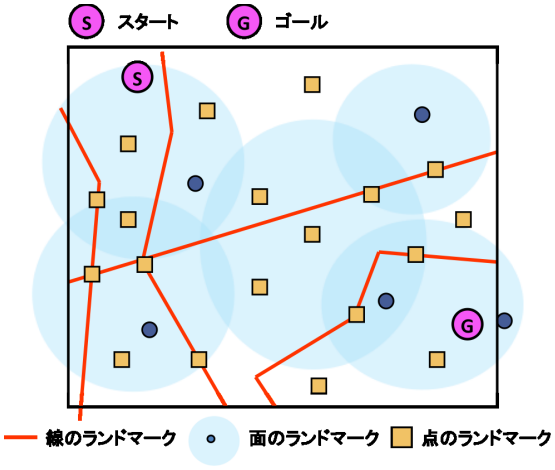
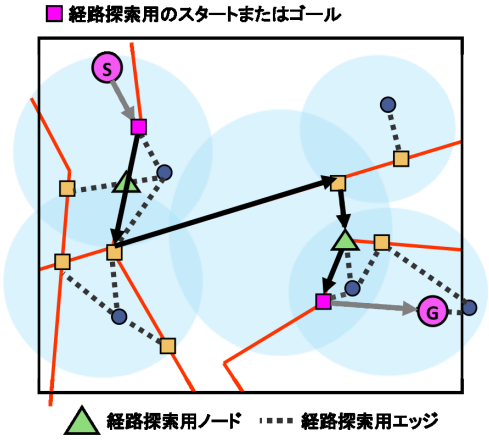


図 2　3 種類のランドマークを用いた経路案内の例



(a) 出発点と到着点を含む Bounding Box 内にある点・線・面のランドマーク



(b) 経路グラフ上での経路探索（太い実線矢印）

図 3　経路グラフの生成プロセスと経路探索

システムの構築にあたっては，ランドマークの情報は Web 上の地理情報データから取得する．具体的には，点と線のランドマークは Google Maps API によりキーワードでカテゴリー検索し，見つかった地物を利用する．ここには，幾何的・意味的双方のランドマークが含まれている．そこで，Twitter や Flickr などの SNS サイトに位置情報付きで投稿されたデータの発信頻度及びトピック解析に基づいて，混雑度と話題性を推定し，点・線の意味的ランドマークを抽出する．

面のランドマークは，まず，三次元 GIS データを用いて視認性の高い高層構造物を検出する．各構造物が見える道路や交差点をあらかじめ計算しておき，可視マップとして保存しておく．これらは幾何的ランドマークに相当する．次に，直接に視認できなくても，その地物の近隣であることが分かる情報や，それに関する SNS の発信位置が広く分散している地物を意味的ランドマークとして抽出する．例えば，「浅草寺まで直進 0.5 km」などの案内板や，浅草寺に関する SNS 情報の発信地が広く分散していれば，浅草寺は意味的ランドマークとなる．

2.2　点・線・面に基づく経路グラフの生成

次に，実際の道路ネットワークとは独立に，点・線・面の各ランドマークを組み込んだ経路グラフを生成して経路を探索する．このグラフは元の道路ネットワークよりも大幅に小さいため，大幅に探索時間を短縮できる．迷いにくい経路を探索するためには，経路長だけでなく，利用するランドマークの数や可視領域を考慮する必要がある．これら複数の条件を満たすような経路探索においては評価コストが複雑になるため，遺伝的アルゴリズムを用いて，経路長が短く，利用するランドマークの数が少ない経路を抽出する．

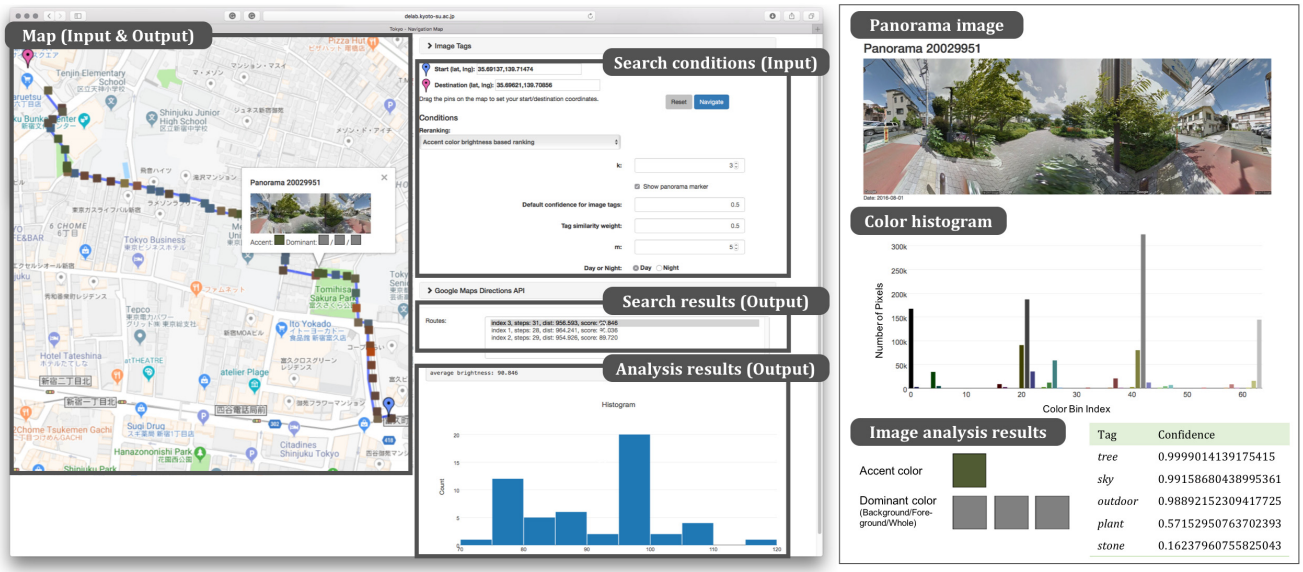
経路グラフの生成アルゴリズムを図 3 を用いて説明する．まず，出発地と目的地を設定し（図 3 では S 及び G），この 2 地点を含む Bounding Box を生成する．そして，システムは Bounding Box に含まれる点，線，面のランドマーク（図 3 (a)：橙色の四角，赤色の実線，紺色の小円）を抽出する．但し，面のランドマークが視認できる可視領域内（水色の大円）に存在する点のランドマークのうち，面のランドマークを視認することが困難であると考えられる可視率の低い点は，経路グラフ作成時点において除かれる．以降では，設定した出発地・目的地に最も近い点のランドマークを出発地・目的地とする．すなわち，実際の経路案内では，本来の出発地から出発時の点のランドマークまで移動し，探索によって得られた経路（図 3 (b)：黒色の矢印）に従い目的の点のランドマークまで案内する．

次に，点と面のランドマークから経路探索用のエッジとノードを生成する．経路探索用エッジとは，ユーザが選択する可能性のある複数の経路を 1 本にまとめた仮想的なパスであり，図 3 (b) の破線のように面のランドマークとその可視領域内に存在する点のランドマークとを線で繋ぐことで生成される．新しい経路探索用エッジと，既存のランドマークが交わるとき，これを新たな経路探索用のノードとする（図 3 (b)：三角）．この新しい経路探索用のノードは，既存の点のランドマークとは異なり，目印としては使用できないが，経路探索では使用される．

最後に，経路探索用のノードとエッジを，点と線と面のランドマークからなる最初のグラフと統合することで最終的な経路グラフを生成する．

2.3　ランドマーク数を最小化する経路探索

前節で 3 種類のランドマークをベースに生成された経路グラフ上で経路探索を行う．一般に，経路探索は Dijkstra 法や遺伝的アルゴリズムを用いて解くことができる．本研究では，経路長を短くしながら利用するランドマーク数を減らし，かつ面のランドマークの可視率を考慮するという複数の条件を満たす経路を探索するため，Wook らが提案した遺伝的アルゴリズムを用いる．スタート S からゴール G までの経路 $T = \{\mathrm{S}, \ldots, T_p, \ldots, \mathrm{G}\}$ を，経由する N 点のノードのリストにより表現する．すなわち，可変長の染色体を利用することとなる．また，その評価関数 $C(T)$ を以下のように定義し，これを最小にする T を求める．



(a) User interface of a prototype of the navigation system　(b) Detailed information of a panorama image

図 4　快適経路推薦システムのユーザインタフェースとパノラマ画像解析の例

$$C(T) = \sum_{p=1}^{N-1} \delta(V(p-1,p), V(p,p+1)) + \lambda \sum_{p=0}^{N-1} D(T_p, T_{p+1}) \quad (1)$$

なお，$V(p,p+1)$ はノード p，$p+1$ 間において使用されるランドマークの ID を表し，δ は二つのランドマーク ID が異なっていれば 1，等しければ 0 を返す関数である．$D(p,p+1)$ は隣接する二つのノード p，$p+1$ 間のユークリッド距離を表す．この評価関数により，同じランドマークを使い続けながら，経路長ができるだけ短い経路を選ぶことができるため，移動距離が短く，記憶しやすい経路を選択することができる．

遺伝的アルゴリズムを用いた経路探索は計算コストが高いが，提案手法により新たに生成したランドマークに基づく経路グラフは既存の道路ネットワークと比べて大幅にコンパクトであるため，複雑な評価コストを用いても短時間で最適経路を見つけることができる（図 3 (b)：太実線矢印）．

2.4　風景画像の分析による快適な経路の推薦

経路推薦においては一般には最短経路や分かりやすい経路が有用とされるが，一方で例えば旅行者にとっては，楽しめる経路，心地よい経路なども需要が高いと考えられる．

図 4 はこのような観点に基づいて構築した快適な経路の推薦システム[2]である．快適さの基準は幾つもあり得るが，ここでは一例として緑（植物）の多さと見通しのよさを基準としている．Google ストリートビューのパノラマ画像から物体や色を抽出することで交差点間の快適性を定量化し，スコアと経路長から経路の候補を順位付けして推薦する．東京，京都，サンフランシスコの都市部でプロトタイプとして提供している．

3.　自転車センシングによる路上環境の分析・可視化

3.1　走行快適性を志向した自転車ナビゲーション

様々な交通手段による移動を一つのサービスとして捉え，シームレスに繋ぐ MaaS（Mobility as a Service）の概念に基づいて，移動支援のための基盤整備が国内外で進められており，各種の移動支援の技術や施策，サービスなどが重要視されている．特に自転車の利用は急速に普及しており，米国の電動自転車市場は 2030 年までに平均成長率 11.9%になると予想され(注1)，日本国内でも COVID-19 が流行し始めた 2020 年以降，自転車販売市場は過去最高を更新している．また，自転車のシェアリングにおいても，ドコモ・バイクシェア(注2)や neuet(注3)，OpenStreet(注4)などのサービスが展開されている．

しかしながら，自転車ユーザに直接影響を及ぼす環境データ（振動や混雑，日照や緑（植物）など）まで考慮して快適で安全な経路を推薦する研究開発の事例は少ない．近年では，自転車の走行環境を適切に把握する研究開発は進んでおり，Jaime ら[3]は，NO_2 や O_3 を測定するための電気化学センサと PM2.5 や PM10 を測定するための光学センサを自転車のハンドルに搭載し，スペインの都市中心部と周辺部の汚染物質の時空間変動に関するデータを取得している．また，Bian ら[4]は，スマホから速度と加速度関連の自転車行動指標（BBI）と走行量などの自転車走行環境指標（BEIs）を抽出し，利用環境品質（BEQ）という概念を提案し，知覚満足度と葛藤度によって定義している．これらの既存研究は自転車に搭載したセンサからデータを収集しており，安全な経路推薦につながると考えられるが，ユーザ

(注1)：米調査会社 Report Ocean による．
(注2)：https://docomo-cycle.jp/
(注3)：https://neuet.com/
(注4)：https://www.hellocycling.jp/

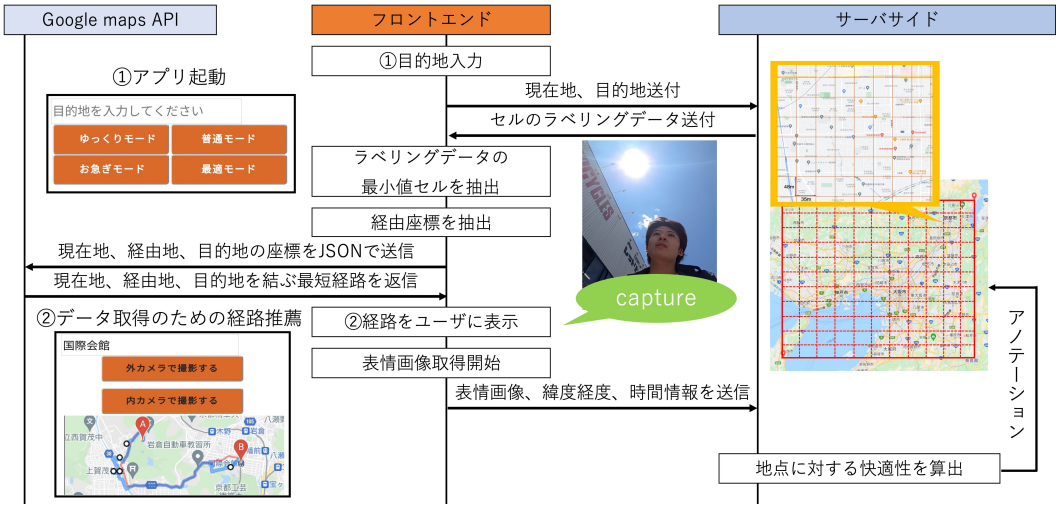


図 5　自転車に搭載したスマホによるデータ取得ナビの処理の流れ

が走行中に環境から直接体感する潜在的な快適性を安全に収集・分析するには至っていない．

そこで本研究では，スマホのセンサから得られる位置や振動だけでなく，カメラにより風景やユーザの顔画像を取得してユーザが意図せずに抱く様々な感情値（幸福感，驚き，恐れ，怒りなど）を推定し，これを地点に対する快適性としてアノテーション可能な仕組み（データ収集ナビ）を構築する[5]．

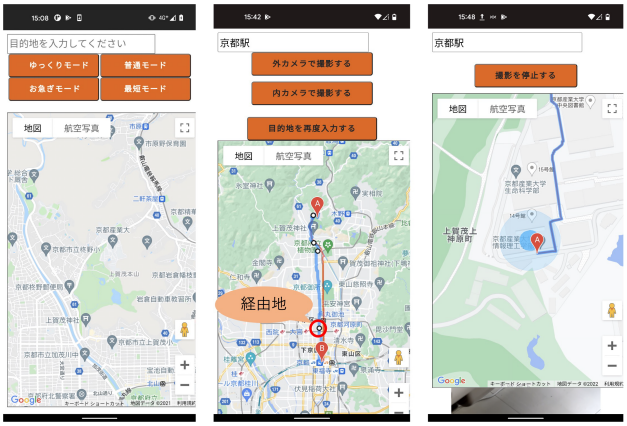
3.1.1　潜在的快適性分析ナビの概要と表情画像の収集

潜在的快適性分析ナビはユーザの同意に基づく利用を前提とする．すなわち，ユーザが前述のデータ収集に協力する場合はデータの蓄積量を加味した経路が案内され，それ以外の場合は従来どおりの指標に基づく標準的な経路（最短，最短時間など）が案内されると想定する．以降では，ユーザがデータ収集に協力する場合の仕組みについて述べる．

図 5 にシステムのフロントエンド（アプリ）とサーバサイドの動作フローを示す．ユーザの要求（目的地）やサーバ側で管理しているデータの取得状況に応じて経由地点が設定され，これに基づいて経路が提示される．経路を走行すると表情画像などが収集され，各地点に対する快適性が算出される流れである．以下に詳細を説明する．

まずナビアプリを起動し，目的地を入力し，データの取得モード（図 6 (a)）を選択すると，現在地と目的地がサーバへ送られる．サーバは出発地と目的地を結ぶ経路の対象となり得るエリアを抽出し，各セルにラベリングされたデータを返送する．ここで，本研究におけるラベリングとは，セルに対して感情分析結果の評価値を付与することを意味する．また，アノテーションは，地点（緯度経度）に対して表情や風景画像など，取得したデータの時刻，セル座標，分析結果を付与することを意味する．

フロントエンドでは，サーバから受信した情報から，当該エリアのラベリング量が最小のセルを抽出し，それに基づいて経由地点を設定する．ユーザの要求に合わせて経路を推薦するため，時間に余裕がある場合は「ゆっくりモード」を選択することで経由地点が五つ設定され，通勤や通学で時間に余裕のない場合は「お急ぎモード」を選択することで経由地点が一つ設定



目的地入力　　経路推薦　　経路案内開始

図 6　開発したデータ取得ナビのアプリ画面

される．

これらの経由地点，現在地，目的地の座標を結ぶ最短経路を Google Maps API を通じて取得し，データ取得のための経路として提示する（図 6 (b)）．

ユーザが「内カメラで撮影する」を選択すると，マップ上で現在地が拡大され，経路案内が開始する（図 6 (c)）．同時に表情画像の撮影が開始し，撮影した際の時刻・緯度経度とともにサーバへ送信される．

提示された経路に従って走行することで，地点ごとにデータの取得・分析・ラベリングが行われる．

3.1.2　表情分析とフィードバックに基づく潜在的快適性の推定

次に，自転車運転者の潜在的な快適性を分析するため，運転中の表情画像から感情を判別し，走行経路上の各地点に対してアノテーションを実施する．表情を利用することで，ユーザが意図せずに抱く快適さ，不快感，驚きなどを取得することをねらいとしている．

画像からの表情分析には，Microsoft Azure の FaceAPI(注5)

(注5)：https://azure.microsoft.com/ja-jp/services/cognitive-services/face/#overview

図 8　走行者の表情分析とフィードバックによる表情分析マップ

(a) 走行直後　(b) フィードバック画面　(c) フィードバック後

図 7　明示的フィードバック機能のアプリ画面

(Perceived emotion recognition) を使用する．Azure は表情分析の結果として次の 8 種類の感情を確率分布として算出する：Anger，Contempt，Disgust，Fear，Happiness，Neutral，Sadness，Surprise（怒り，軽蔑，嫌悪，恐怖，幸福，中立，悲哀，驚き）．これらの感情値と時刻を，走行地点の緯度経度に対して付与する．

一方で，走行中の表情画像は撮影角度や日照条件の影響を受けやすく，感情分析・ラベリングの信頼性が低くなる可能性がある．そこで，補完的な仕組みとして，ユーザによる直接的なフィードバック，すなわち自転車走行後にユーザが地点ごとの感情値を明示的にラベリングすることのできるインタフェースも併せて設ける．

図 7 にフィードバックの流れを示す．走行終了直後のアプリ画面には，走行時間や消費カロリーのほか，走行経路上における表情の分析状況が表示される．赤色のピンはフィードバックが期待される地点であり，ユーザは Google ストリートビューの風景画像を見ながら走行の快適性を評価することができる．フィードバックが完了すると，赤色のピンが緑色に変化する．

3.1.3　自転車の快適走行マップの生成

図 8 に快適走行マップの例を示す．対象エリアは大阪府，京都府，兵庫県，奈良県の一部を含む関西地域とした．地図上にアイコン画像は，ユーザの表情画像を分析した感情値と位置情報に基づいてプロットされている．図中では，花，芽，種の各アイコンが快適性の高い地点，低い地点，判別がつかなかった

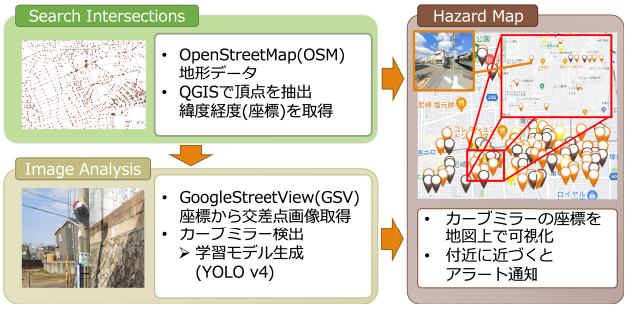


図 9　カーブミラー学習モデル生成によるマップ生成

地点または表情分析ができなかった地点を表している．京都エリアの快適マップを見ると，北部のエリアは花アイコンが多く，自転車ユーザにとって快適性が高いエリアであることが分かる．一方，南部は芽アイコンが多く，快適性が高くないエリアとなった．以上のように，表情画像データに対する感情値を算出し，結果をマップに示すことで，快適な地点を効果的に可視化することができる．

3.2　カーブミラー検出による死角ハザードマップの生成～走行安全性の向上～

自転車運転者にとっては，移動中の快適性のみならず安全性が更に重要な課題である．安全性の向上に向けた取り組みの一つとして，自転車に搭載したスマートフォンのカメラで死角に存在する歩行者や車を検知し，注意を喚起するシステムの構築を目指している．ここでは，そのための死角ハザードマップを生成する研究例を紹介する．

見通しの悪い交差点やカーブには従来からカーブミラーが設置されていることが多く，ミラーを利用して死角の車両や歩行者などに十分に注意する必要がある．これまで我々は，走行中の自動車のドライブレコーダ映像を分析して，カーブミラーを検出するとともに，更にミラー内に映る対向車などの接近を検知するシステムを開発してきた[6]．

本研究では，ディジタル道路地図と街路画像から死角ハザードマップを生成する．まず，道路上の交差点または急カーブをディジタル道路地図の属性または線形情報から抽出する．続いて，その地点の街路画像を取得し，深層学習によりカーブミラーが検出された地点を死角ハザードとして抽出する（図 9）．

ディジタル地図と街路画像にはオープンデータである Open

Street Map と Google ストリートビューを利用した．ミラーの検出の学習モデルには，性能比較の結果 Faster R-CNN 及び YOLOv4 を用い，独自に収集した画像及びストリートビュー画像により学習を行った．福岡市内，尼崎市内の領域に対して交差点におけるカーブミラー検出精度を検証したところ，再現率 63.4%，適合率 90.0%であった．矩形のカーブミラーの検出や，ストリートビュー画像が存在しない箇所への対応は課題である．

今後，ミラー内の動きを検出して死角の危険を予知し，注意を喚起する機能について検証する予定である．

3.3 路上ゴミ分析マップの生成～個人行動から社会貢献へ～

スマホやドライブレコーダのカメラは今や街中の分散センサとして機能しており，先の例における死角ハザードマップ生成のように，個人行動に基づくセンシングは社会全体への貢献にもなり得る．ここでは，自転車とスマホを活用した路上環境の分析・提示の研究例として，路上のゴミ物体の可視化と発生予測に取り組んだ例を紹介する．

路上へのゴミのポイ捨て抑止や清掃の支援として，スマホを活用した取り組みが注目されている．近藤ら[7]は，スマホで撮影した画像から機械学習を用いて物体の種類を判別し，撮影位置の座標を地図上にプロットしている．タカノメ(注6)も，同様の手法によりヒートマップを作成し，ゴミ分布の可視化サービスを提供している．これら既存の研究やサービスでは，対象物体となるタバコや空き缶などのゴミを視認しながら個別に撮影する能動的なデータ収集が必要となり，収集・分析コストが高い．

これに対し我々の研究では，狭い路地などでも走行可能な自転車と，スマホを活用することで，効率的かつ安全な路上環境情報収集及び分析システムを構築する．ユーザはスマホを自転車に搭載するのみで，走行中に操作することなくスマホから走行風景の画像を取得し，路上環境を分析することができ，処理コストを大きく軽減できる．

図 10 に，路上環境情報取得・分析システムの処理の流れを示す．自転車に搭載したスマホから画像を取得し，物体（ゴミ）を抽出してマップ上に可視化する．物体抽出においては，路上を対象とするため，まず撮影画像の下半分を抽出する．続いて，落ちている物体以外の要素を削除し，抽出した物体の矩形領域を解析してオブジェクトの種別を判別する．これにタグ付け（litter, scrap など）を行ったうえで撮影位置にマッピングする．

更に，ゴミの発生も予測する．ゴミの発生要因になりやすいと考えられる飲食店やスーパー，コンビニ店舗に関する属性情報（位置，カテゴリー種別，来店者数，レビュー，ツイート）を Open Street Map，Google マップ，SNS から取得する．既に抽出されたゴミの位置と，これら店舗との距離，属性情報から，ゴミの発生確率を計算することができる．

本システムによる路上環境データの可視化と予測は，ゴミのポイ捨てなどのネガティブな行動の自粛にもつながることが期待される．

(注6)：https://research.pirika.org/

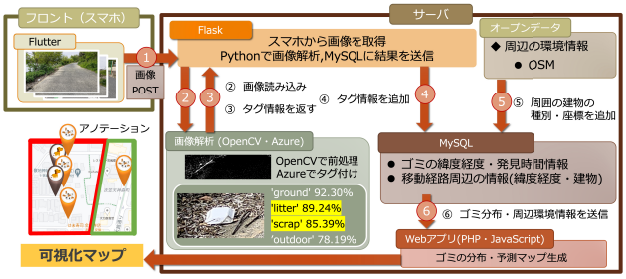


図 10　路上環境画像の取得・分析・可視化までの流れ

4. 需給情報と社会的距離を考慮した観光ガイドシェアリングのプランニング

COVID-19 の期間中には社会的距離（ソーシャルディスタンス）を考慮した行動変容が世界中で急速に求められており，IoT 基盤やモバイル端末の活用によって他人との社会的距離をとったリモートでのコミュニケーションも可能となった．しかし，観光や教育，医療などの分野では全てのサービスをリモートで提供することには限界があり，特に 840 兆円の経済効果があるとされる日本の観光市場においても大きな損失が生じている．このような背景のもと，近年注目されている MaaS は物理的距離を考慮した行動の決定にも活用することができる．また，MaaS はシェアリングエコノミー[8]の重要な基盤の一部でもある．

シェアリングエコノミーでは，アセット（資産）やヒューマンアセット（資産を含めた知識）を共有するサービスが実現されている．観光においても各種の体験やガイド（案内人）などのシェアリングが実用化されており（Airbnb Experience(注7)，Huber(注8)など），単にモノを見る観光だけでなく，解説を楽しんだり，具体的なコトを体験したいという志向性の高まりに応えている．これらのサービスは 1 人のヒューマンアセットを比較的長い時間にわたって占有するため，時間的・金銭的なコストが高くなりがちである．ユーザとヒューマンアセットの間，あるいはユーザ相互間における適切なマッチングが求められる．

本稿では，旅行者（ユーザ）と観光ガイド（ヒューマンアセット）の嗜好性や時空間的制約を考慮した最適な観光ルートとガイドを推薦する手法，及びそのプロトタイプを紹介する．ユーザとガイドの需要・供給属性情報（ユーザの位置，嗜好性，ガイドのレビュー，ガイドの対応可能範囲など）を取得・分析し，時間・距離の制約のもとで，順路化したスポットとガイドのアセットをプランニングする仕組みである．

図 11 に観光ガイドプランニングシステムの概要を示す．本システムでは，ユーザからの距離や嗜好性にマッチするスポット (POI, Point of Interest) だけでなく，ユーザとガイド，さらにユーザと他ユーザとのマッチングも行う．特に，スポットごとに異なるガイドとユーザをマッチさせるケースも含めて最適なプランを推薦する．

ユーザとガイドのマッチングでは，登録された需要属性・供給属性の条件にできるだけ合致したガイドをユーザに対して推

(注7)：https://www.airbnb.jp/
(注8)：https://huber.co.jp/

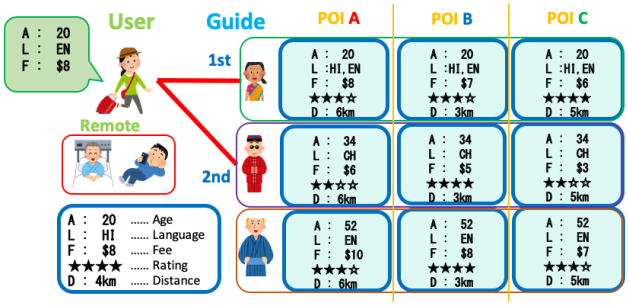


図 11　複数 POI・複数ガイドによる観光ガイドプランニング

薦する．ユーザ同士のマッチングでは，複数のユーザレビューに対してテキスト分析を行い協調フィルタリングから算出される関連度を表す特徴ベクトルからコサイン類似度で他ユーザとの類似性を算出する．特に，POI ごとに異なるガイドをマッチングするケースも含めて，最適なルートとに着目し，ガイドが POI に登録した情報からユーザが物理的距離を考慮しつつ観光する最適の順路で POI とガイドを最適化手法より推薦する．

4.1　ガイド及びユーザに関する需給情報

マッチングでは，まず事前にユーザ及びガイドが下記の情報を登録する．

- **需要者情報（ユーザが登録）**：案内希望の POI 情報，日時，ガイド時間，料金，使用言語，ガイドに対するレビュー（事後登録）
- **供給者情報（ガイドが登録）**：案内可能な POI 情報，日時，ガイド時間，料金，対応可能な言語，POI に対するコメントレビューはガイド後に登録される情報で，リッカート尺度による評価値である．

4.2　需給情報と時空間制約に基づくユーザ，ガイド，スポットの最適マッチング

システムは，ユーザとガイドの需給情報及び距離・時間の制約に合わせて複数の POI，ガイドをユーザに推薦する．ガイドとユーザは 1 対多であり，志向性の近いユーザ同士が同じガイドに割り当てられる．このための最適化手法について述べる．

マッチングの相違度を表すコスト関数は，次の 10 要素の重み付き総和として定義する．

- 物理的距離コスト C_{PD}
- 社会的距離コスト C_{SD}（参加人数，混雑度）
- スケジュールコスト C_T（ガイドの開始時間，終了時間）
- 金銭コスト C_F（ガイド料金）
- その他のコスト（使用言語，POI に対するレビュー，ガイドに対するレビュー，他ユーザとの類似度）

各コスト要素の算出方法は以下のとおりである．

$$C_{PD} = d_{poi} \tag{2}$$

$$C_{SD} = \frac{n_u + n_{poi}}{s_{poi}} + \lambda_0 c_{poi} \tag{3}$$

(a) スタート地点選択　(b) 参加条件入力　(c) 順序付けされた複数 POI を推薦

(d) ガイド登録画面　(e) ユーザ登録画面　(f) 現在地と現時点でガイド可能な POI を推薦

図 12　複数 POI に対する観光プランニング画面

$$C_T = |t_u - t_g| + |t'_u - t'_g| \tag{4}$$

$$C_F = \frac{f}{n_u} \tag{5}$$

ここで d_{poi} はユーザ位置との物理的距離差，n_u は参加人数，n_{poi} はツイート数から予測した任意の POI にいる人数，s_{poi} は POI の面積，c_{poi} は Google Maps から取得した混雑度である．t_u，t_g はユーザ及びガイドの開始時刻，t'_u，t'_g は終了時刻，f は設定されたガイド料金である．

その他のコストについて，使用言語に関するコストは，ユーザの指定した言語と一つも一致しなければ定数を加算する．レビューに関するコストは，前述のリッカート尺度による評価値をである（ただし，0 オリジンにオフセットする）．

他ユーザとの類似度はユーザ相互間のマッチングに用い，ユーザレビュー文章のテキスト分析により取得する．具体的にはテキストから（特徴語を抽出してベクトル化し，コサイン類似度を計算する．

コスト関数値の最小化には，ランダムサーチ，ヒルクライム，擬似アニーリング，遺伝的アルゴリズムの各最適化手法を用いる．

4.3　ガイドプランニングシステムのプロトタイプ

図 12 は複数 POI の観光プランニング画面である．図 12 (a)

では，まずスタート地点として，地図上からホテルなどの任意の場所をクリック決定する．次に画面スクロールし（図 12 (b)），観光開始と終了時刻，参加人数，興味ジャンル（複数選択可能），訪問したい POI 数を入力する．システムはコストを算出し，値が小さい順にプランニング結果を推薦する（図 12 (c)）．

図 12 (d) はガイド側の登録画面である．ガイドは案内できるスポット，日時，料金，最大人数，対応可能言語，その場所に対するコメントを入力しガイド登録を行う．ユーザから予約が入っていれば予約確認画面でユーザ情報を閲覧できる．

図 12 (e) はユーザの登録画面で，ユーザは観光したい POI，日時，参加人数，言語を入力し，それら条件に合致したガイドを選択できる．更に，ガイドを他ユーザとシェアできる．

また，ユーザの現在地からリアルタイムに POI とガイドを推薦させることも可能である（図 12 (f)）．使用端末から現在位置情報を取得し，現在位置を基準とした半径 1 マイル以内にあるユーザの興味や料金に合致した 20 の POI が推薦される．推薦された POI から選択した POI に対して，現在時刻から一定時間以内に案内が開始できるガイドと料金を推薦する．これにより，近場で制限時間内で観光できるスポットとガイドを検索することができる．

5. おわりに

実世界のユーザ個人の行動分析は，安全性や効率性，快適な行動支援だけでなく，群衆の行動支援となり，結果，社会課題解決につながる．今後，ユーザの利便性だけでなく，個人の行動が社会全体への貢献・利益となり，再びユーザに還元される，デジタルツインによる仕組みや仕掛けの実践的応用技術が期待される．

文　献

(1) 森永寛紀，若宮翔子，谷山友規，赤木康宏，小野智司，河合由起子，川崎洋，“点と線と面のランドマークによる道に迷いにくいナビゲーション・システム，” 情報処理学会論文誌，vol.57, no.4, pp.1227–1238, 2016.

(2) S. Wakamiya, P. Siriaraya, Y. Zhang, Y. Kawai, E. Aramaki, and A. Jatowt, “Pleasant route suggestion based on color and object rates,” The 12th ACM International Conference on Web Search and Data Mining (WSDM), pp.786–789, 2019.

(3) J. Gómez-Suárez, P. Arroyo, R. Alfonso, J. Ignacio Suárez, E. Pinilla-Gil, and J. Lozano, “A novel bike-mounted sensing device with cloud connectivity for dynamic air-quality monitoring by urban cyclists,” Sensors, vol.22, no.3, p.1272, 2022.

(4) Y. Bian, L. Li, H. Zhang, D. Xu, J. Rong, and J. Wang, “Categorizing bicycling environment quality based on mobile sensor data and bicycle flow data,” Sustainability, vol.13, no.8, p.4085, 2021.

(5) R. Yamaguchi, P. Siriaraya, T. Yoshihisa, S. Shimojo, and Y. Kawai, “A detection system for comfortable locations based on facial expression analysis while riding bicycles,” WWW ’23 Companion, pp.306–309, 2023.

(6) Y. Hino, S. Ono, N. Itagaki, and Y. Suda, “Recognition of risky events reflected in road safety mirror considering ego-vehicle’s motion,” FAST-zero’21, 2021.

(7) 近藤諒太，清木康，“不法投棄ゴミを対象とした画像分析・分類機能と時空間マッピング・システムの実現方式，” DEIM Forum 2021, J11-5, 2021.

(8) K. Barron, E. Kung, and D. Proserpio, “The sharing economy and housing affordability: Evidence from airbnb,” Proceedings of the 2018 ACM Conference on Economics and Computation (EC ’18), p.5, New York, NY, USA, 2018.

（ITS 研究会提案，2022 年 12 月 2 日受付，
2023 年 5 月 17 日再受付）

河合由起子（正員）

2001 奈良先端科学技術大学院大学情報科学研究科博士後期課程修了．同年，（独行）通信総合研究所 (現情報通信研究機構)，2006 京都産業大学理学部講師を経て，2018 より京都産業大学情報理工学部教授，大阪大学サイバーメディアセンター特任教授 (常勤)，現在に至る．博士 (工学)．Web マイニング，時空間分析，情報推薦の研究に従事．

栗　達

2020 北海道大学大学院情報科学研究科博士後期課程修了．博士（情報科学）．2020 同大学大学院情報科学研究院専門研究員．2021 京都産業大学情報理工学部研究員．2022 より福岡大学工学部助教，現在に至る．主に機械学習，自然言語処理，画像処理，データマイニング及び情報推薦の研究に従事．

小野晋太郎（正員）

2006 東京大学大学院情報理工学研究科博士課程修了．博士（情報理工学）．同大学生産技術研究所特任助教，特任准教授，及び (株) ホンダ・リサーチ・インスティチュート・ジャパンとの兼業を経て，2021 より福岡大学工学部准教授．主に画像処理，実世界センシング，知能化モビリティ，高度交通システムの研究に従事．

ESS ニュース

NOLTA, IEICE 特集号

Guest Secretary　吉岡大三郎

特集タイトル：

Special section on recent advances in nonlinear problems

掲載誌：

NOLTA IEICE, vol. 14, no. 3（2023 年 7 月発行）

電子情報通信学会 NOLTA ソサイエティでは，非線形現象の基礎理論から応用に関する成果発表の場となる非線形問題研究会を毎年開催しており，カオスや分岐現象などの非線形解析や近年話題のニューラルネットワークに関する興味深い研究発表が盛んに行われています．本特集は，非線形問題に関する最新の研究成果を国際英文論文誌として発信することを目的に，非線形問題研究専門委員会が企画したものです．投稿された論文は NOLTA, IEICE の通常の査読プロセスに従って審査され，5 件の論文が掲載されることとなりました．その中には，非線形問題研究専門委員会からの推薦論文も 2 件含まれています．掲載論文は，非線形問題に関する独創的な研究成果をまとめたものであり，J-STAGE（https://www.jstage.jst.go.jp/browse/nolta/list/-char/ja）にて無料でご覧頂けますので，ぜひご覧頂きたく存じます．

最後に，貴重な研究成果をご投稿頂いた著者の皆様，年始から年度末にかけて多忙な時期にもかかわらず査読頂いた査読者の皆様，本特集号にご尽力頂いた Guest Associate Editors の皆様に深く感謝申し上げます．

吉岡大三郎（正員）

2001 熊本大学工学部電気システム工学科卒．2003 同大大学院博士前期課程修了．2006 同博士後期課程修了，博士（工学）．同年崇城大学情報学部助手，2018 年 4 月より同大学情報学科教授，現在に至る．カオス系列とその応用に関する研究に従事．日本応用数理学会，IEEE 各会員．

研究会に行こう！

「研究会に行こう！」では基礎・境界ソサイエティの研究会などの様子を御紹介しています．情報交換や懇親，新たな研究との出会いの場としてはいかがですか？

■信頼性研究会（R）

近年システムが大規模複雑化するに従って，ハードウェアとソフトウェアが相互に複雑に絡み合ったシステムの安全性，信頼性を保証する技術が非常に重要になってきています．例えば自動車は 1970 年頃まではほとんどメカニカル機構のみで制御されていましたが，排気ガス規制の強化に伴い，制御機構にエレクトロニクス部品が導入され始め，1990 年代には複数の半導体チップを組み合わせて，ソフトウェアによって様々な制御を実現する大規模複雑なシステムとなってきました．そして，この複雑なシステムの安全性，信頼性を保証するために，仕様作成，ハードウェア開発，ソフトウェア開発，システム検証，部品選定，組み立ての全ての開発工程に対して，その品質を担保するための最先端技術・手法が導入されています．

当研究会は，このトレンドに対応して，半導体部品や通信ネットワーク分野のハードウェアの機能的信頼性確保の技術のみならず，部品・材料の強度や耐久性，ソフトウェアの品質（バグの残数など）やセキュリティ，システムの対故障性解析など，システム上の様々なレイヤの信頼性を保証するための最新技術を発表・共有する研究会を年 8 回開催しています．

特に自動車などの人命に関わるシステムの信頼性保証に向けては ISO26262 など，開発各工程において様々な信頼性チェック項目が標準化されています．このような取り組みは今後様々なシステム開発にも適用されてくることが想定されるため，12 月に開催される研究会は特に信頼性に関する国際規格などを取り上げる回としています．

更に今年からは全ての回がハイブリッド形式となり，以下のように北海道から九州まで日本各地での開催が再開となっています．

- 2023 年 5 月 27 日　愛知大学　ソフトウェアの信頼性，信頼性一般
- 2023 年 6 月 15 日　機械振興会館　信頼性一般
- 2023 年 7 月 28 日　札幌市エレクトロニクスセンター　信頼性理論，通信ネットワークの信頼性，信頼性一般
- 2023 年 8 月 24～25 日　東北大学　受光素子，変調器，光部品・電子デバイス実装・信頼性，及び一般
- 2023 年 9 月 28 日　久留米大学医学部基礎 3 号館　情報通信システムの信頼性，信頼性一般
- 2023 年 11 月 3 日　金沢商工会議所　半導体と電子デバイスの信頼性，信頼性一般
- 2023 年 12 月 7 日　機械振興会館　信頼性国際規格，保全性，信頼性一般，安全性一般
- 2024 年 2 月 29 日　松江テルサ　信頼性一般

これを機に信頼性技術の研究者の方だけでなく是非とも様々なシステム開発に関わっている技術者の方にも国内各地からご参加頂き，信頼性技術に関するアイデア・技術の共有と底上げを図っていきたいと考えております．今後ますます多くの方々にご参加頂けましたら幸いです．

吉川隆英（正員）
2002.3 東京大学工学系研究科情報工学専攻博士課程修了．博士（工学）．同年 4 月(株)富士通研究所入社．Java JIT コンパイラに関わる研究及び「京」コンピュータの開発（検証・テスト・量産）を経て 2015.4 より富士通(株)に異動し，スーパーコンピュータ「富岳」開発に従事．現在，同社次世代アーキテクチャ PJ でコンピュータシステムに関わる研究に携わる．

■複雑コミュニケーションサイエンス（CCS）

複雑コミュニケーションサイエンス（CCS）研究専門委員会は，2011 年 4 月に時限研究専門委員会として発足し，2015 年 4 月から NOLTA ソサイエティのもと，常設研究専門委員会として活動しています．2023 年度は常設研究専門委員会として 9 期めを迎えることとなります．

これまで，CCS 研究会では，複雑ネットワーク理論や非線形ダイナミクスのアプローチを駆使して，通信・ネットワーク分野への応用をはじめ，神経系や生物システム，更にはソーシャルコミュニケーションやヒューマンサイエンスまで含む広範な研究対象に対して，そこにある現実的問題の本質や限界に迫り，それらに潜在する普遍的特質を明らかにするサイエンスの創出という役割を担ってきました．

2022 年度には総合大会において「次世代ネットワークを支える数理モデルの展開」というテーマのセッションを企画し，素

晴らしい講演者の皆様による貴重な御講演を頂くことができました．この場を借りて御礼を申し上げます．

また，CCS 研究会では，学生の皆さんや若手研究者を積極的に奨励する取り組みにも力を入れています．毎年発表された口頭発表論文の中から優秀な研究発表を行った若手研究者を選出し，「複雑コミュニケーションサイエンス研究会奨励賞」として表彰しています．

これまでの受賞者のなかには現在活躍している研究者も多く，本研究会の発表の場が重要な役割を果たしていることがうかがえます．

2020 年度と 2021 年度はコロナ禍の影響で，オンラインでの研究会開催が主となっておりましたが，2022 年度はハイブリッドや対面で開催をし，CCS 研究会が更に活気づいてまいりました．2023 年度の CCS 研究会の活動予定を次に記します．また，本研究会の最新情報は CCS Web サイトにて随時更新しております．

ぜひ多くの皆様に御参加頂き，活発に御発表御議論頂けることを期待しております．皆様の御参加を心よりお待ちしております．

【2023 年度 CCS 研活動計画】

●第一種研究会

2023 年 6 月 8 日 9 日	CCS/NLP 共催研究会@東京都市大学
2023 年 8 月 3 日 4 日	CS/IN 併催研究会@北海道，番屋の湯
2023 年 11 月（中旬予定）	CCS 研究会@富山県立大
2024 年 3 月（下旬予定）	CCS 研究会@北海道，ルスツリゾート

●大会・国際会議

2023 年 6 月 10 日	NOLTA ソサイエティ大会@東京都市大学
2023 年 9 月 26 日～29 日	NOLTA2023 @イタリア
2024 年 1 月 29 日 30 日	KJCCS @別府温泉

【CCS 研 Web サイト】http://www.ieice.org/nolta/ccs/

宮田純子（正員）

2012 東工大大学院集積システム専攻博士後期課程了．博士（工学）．同年神奈川大・特別助手．2015 芝浦工大・助教．2018 同准教授．以来，ネットワーク品質制御・情報セキュリティの研究に従事．IEEE 会員．

■情報セキュリティ研究会（ISEC）

情報セキュリティ研究会（ISEC）は，安心安全なディジタル化社会を実現する上で必要となる情報セキュリティの研究発表の場として，第一種研究会，第二種研究会（WCIS），国内シンポジウム（SCIS），及び国際会議（IWSEC）を主催・共催しています．

第一種研究会は 5 月，7 月，11 月，3 月の開催を予定しています．5 月の研究会では，国際会議で発表した修士課程学生を中心とする若手研究者をお招きし，最新の成果を講演して頂いています．5 月以外は関連研究会と共催しています．

第二種研究会 WCIS（暗号と情報セキュリティワークショップ）は，SCIS のプレイベントという位置づけで 2019 年度に開始した研究会です．暗号理論，コンピュータセキュリティに関するトップカンファレンスでの発表者をお招きし，最新の研究成果を紹介して頂いています．例年約 10 件もの最先端の国際的成果をご発表頂いており，研究動向を知る上でも有益な機会となっています．今年度も 9 月の開催を予定しております．

国内シンポジウム SCIS（暗号と情報セキュリティシンポジウム）は 1984 年から毎年 1 月に開催しているシンポジウムで，今年度は 41 回めの開催です．参加者 900 人以上，発表件数 300 件以上を誇る情報セキュリティにおける国内最大規模の研究集会であり，最新成果を知ることができます．

国際会議 IWSEC（International Workshop on Security）は，2006 年から毎年日本で開催している情報セキュリティ分野の国際会議です．2023 年は 8 月 29 日から横浜での開催を予定しています．

このように ISEC は様々な形式での研究集会を開催しており，皆様のご参加をお待ちしています．なお，開催場所や開催時期については変更になる可能性があります．最新の情報は ISEC の Web ページ（https://www.ieice.org/~isec/）を参照ください．

花岡悟一郎（正員）
平 9 東大・電子工学科卒．平 14 同大学院工学系研究科電子情報工学専攻博士課程了．同年日本学術振興会特別研究員（PD）（東大），平 17 産総研研究員．平 21 同主任研究員，平 23 同研究チーム長，令 3 年同首席研究員，現在に至る．博士（工学）．電子情報通信学会，国際暗号学会（IACR）各会員．

■情報理論研究会（IT）

情報理論（IT : Information Theory）研究会は情報理論とその関連分野をトピックとする研究会です．扱うトピックはシャノン理論や符号理論にとどまらず，通信方式・量子情報処理・情報理論的安全性・仮説検定などの基礎理論やその応用に関する幅広い分野をカバーしています．

IT 研究会はハイブリッド形式にて例年 4 回（5 月，8 月，1 月，3 月）の研究会を開催しています．8 月を除く全ての研究会は関係の深い研究会との共催です．単独開催である 8 月の研究会は「フレッシュマンセッション」と称して，初めて学会発表をする学生さんを対象としたセッションを設けています．また，旬のトピックをご研究されている方に招待講演をして頂いています．2023 年度の IT 研究会の日程は次のとおりです．

- 2023 年 5 月 京都大学　マルチメディア情報ハイディング・エンリッチメント（EMM）研究会と共催
- 2023 年 8 月 湘南工科大学　フレッシュマンセッション
- 2024 年 1 月 東北大学　信号処理（SIP）研究会，無線通信システム（RCS）研究会と共催
- 2024 年 3 月 未定　例年，情報セキュリティ（ISEC）研究会，高信頼制御通信（RCC）研究会，ワイドバンドシステム（WBS）研究会と共催で開催

IT 研究会は，情報理論とその応用サブソサイエティ（SITA サブソ）傘下にある唯一の研究会であり，SITA サブソから IT 研究会で優秀な研究発表を行った学生に対して「学生優秀発表賞」を年 2 回授与しています．この賞があるからか，学生さんの発表であっても質の高い研究内容のものが多い印象にあります．

IT 研究会では，大学院生を中心にしつつも学部生や高専生，若手研究者からベテランの先生まで幅広い方が研究発表をしています．休憩時間には，質疑応答の時間にもまして，活発な議論があちらこちらで繰り広げられています．ある意味，この休憩時間の何気ない会話や議論・情報交換こそが研究会の醍醐味なのだと思います．IT 研究会はハイブリッド形式で開催をしているため，オンラインからの発表・聴講も可能ですが，現地での参加の方がより研究会の魅力を味わいやすいと思っています．この記事で少しでも IT 研究会に興味をもって下さった方は是非ともご参加・ご発表のほどよろしくお願いします．

野崎隆之（正員）
2008 東工大・工・情報工卒．2010 同大学院修士課程了．2012 同大学院博士課程了．博士（工学）．同年日本学術振興会特別研究員．2013 神奈川大助手．2015 山口大大学院理工学研究科助教．2017 同大学院創成科学研究科（理学系）講師．2020 同准教授．符号理論の研究に従事．2011 SITA 奨励賞，2012 本会学術奨励賞，2014 SRC 論文賞，2014 IEEE ITJC Young Researcher Best Paper Award，2018 本会論文賞各受賞．

■信号処理研究会（SIP）

センサ技術，コンピュータ，通信の技術の発展に伴い，様々な物理現象，人間の社会行動を対象としたデータの利活用がより強く求められる時代となりました．信号処理研究会（SIP 研究会）では，観測された信号やデータから有益な情報を抽出し体系化する信号処理技術について，基礎から応用まで幅広い分野を取り扱っています．学際的な研究分野であることから，基礎理論から画像，映像，音声，音響，生体，通信，制御，機械学習など幅広い分野の研究者が集い，議論を行っています．

研究会は年に 5 回開催し，それぞれ特徴のある構成となっています．5 月は画像関連，6 月はシステムと信号処理サブソサイエティ，1 月は情報理論・通信関連，3 月は音声・音響関連の研究会と共催しています．8 月の研究会は単独開催で独自企画を行い，本分野の人材育成及び活性化につなげています．2023 年度の研究会，シンポジウムの予定は以下のとおりです．詳細や最新情報は SIP 研究会の HP をご覧ください．

2023 年 5 月 18～19 日　三重大学（BioX，IE，映像メディア学会 IST/ME と共催）

2023年7月6～7日　小樽商科大学（システムと信号処理サブソサイエティのMSS，CAS，VLDと共催）
2023年8月17～18日　大阪大学（単独開催）
2023年11月6～8日　信号処理シンポジウム　京都
2024年1月18～19日　東北大学（IT，RCSと共催）
2024年3月　会場未定（SP，EAと共催，情報処理学会SLPと連催）

信号処理シンポジウムは，国内の信号処理に関する最大規模のイベントで，活発な研究討論の場を提供しています．毎年，招待講演やチュートリアル講演に加え，100件前後の研究発表があります．今年度は京都市で開催予定です．多くの皆様の研究発表・参加をお待ちしております．

仲地孝之（シニア会員）
1997慶應義塾大学大学院後期博士課程了（工博）．同年日本電信電話(株)入社．2006～2007スタンフォード大学客員研究員．主に超高精細映像符号化・伝送，セキュア信号処理，エッジAI機械学習の研究に従事．2021年4月より，琉球大学情報基盤統括センター・教授．信号処理研究専門委員会委員長，IEEE会員．

■ワイドバンドシステム研究会（WBS）

ワイドバンドシステム（WBS）研究会は，電磁波・光を中心とした広帯域通信方式に関する通信理論やその応用を主軸に，様々なテーマやアイディアが集まる研究会です．

特に，スペクトル拡散，OFDM，UWBなどの広帯域無線通信システム，符号化，センシング，無人航空機（UAV）応用，自動運転・高度道路交通システム，様々な通信環境における可視光通信方式など，幅広い分野にわたっています．その歴史は長く，前身は1980年代後半に設立されたスペクトル拡散（SST）研究会であったこと，1990年代には情報通信基礎サブソサイエティとして情報理論（IT），情報セキュリティ（ISEC），高度交通システム（ITS）研究会などと連携して活動していたこと，これらの研究会で活躍されていた方々を交え，より多くの研究会の設立が進んだこと，それらの研究会との連携を積極的に行っていること，などからもうかがい知ることができます．現在共催・併催が多い研究会は，前述の研究会に加え，高信頼制御通信（RCC），衛星通信（SAT），ヘルスケア・医療情報通信技術（MICT）の各研究会が挙げられ，2023年度は短距離無線通信（SRW）研究会とも共催・併催を予定しています．

研究会の開催件数は年4回程度となっており，口頭発表に加えポスターセッションが開催されています．近年では，口頭発表についてはオンラインでの発表や聴講参加ができるように工夫されており，研究成果を広く発表しほかの研究者の方々と議論を交わす機会を維持しています．また，学生や若手研究者の皆様の研究活動を奨励する目的で，WBSオーラルセッション研究奨励賞，WBS研究活動奨励賞などの様々な表彰を行っています．

過去の研究会開催地や発表テーマにつきましては，研究会開催スケジュールや技報アーカイブをご覧ください．

最近3年程度のワイドバンドシステム研究会（WBS）
https://bit.ly/ieicewbs2023ls＋

まさに広い分野を網羅し，様々な研究分野の揺籃となっているワイドバンドシステム研究会に是非ご参加頂きたいと思います．

荒井　剛（正員）
1997茨城大・工・情報卒．1999同大学院博士前期課程了．2004同博士後期課程了．博士（工学）．現在，岡山県立大・情報工・情報通信工・助教．2022からWBS研究専門委員会幹事．IEEE会員．

■高信頼制御通信研究会（RCC）

「高信頼制御通信研究会（RCC）」は前身の研究会の時代を含めると創立から10年以上が経過した．本研究会の目的は制御分野と通信分野の融合による制御システムの信頼性，安全性及び耐久性の向上とそれによる各種分野への応用促進である．IoT・DX・AIに対する社会的な期待値は年々高まっており，とどまることがない．このような技術は通信の信頼性なくしては成立しない．また，通信により接続された各システムが正確に制御されることによって，その真価が発揮される．本研究会では，このよう

な IoT・DX・AI に支えられた未来を創出する基盤研究とその応用をスコープとしているといえる.

2020 年度からは，本研究会が扱う技術分野の研究開発を活性化することを目的とし，「オーラルセッション研究奨励賞」を本分野の若手研究者に贈呈している．2022 年 12 月以降は「高信頼制御通信研究奨励賞」という形で表彰を続けている．是非，高信頼制御通信研究会への参加を願いたい.

本研究会の今後の開催予定やプログラムに関しては以下を確認されたい.

https://www.ieice.org/ess/rcc/

2023/5/25～26	2023 年 5 月高信頼制御通信研究会	東京ビッグサイト
2023/7/12～14	2023 年 7 月高信頼制御通信研究会	大阪大学中之島センター
2023/12	2023 年 12 月高信頼制御通信研究会	場所未定
2024/3	2024 年 3 月高信頼制御通信研究会	場所未定

足立亮介（正員）

2014 年北海道大学工学部卒業．2016 年同大学大学院情報科学研究科博士前期課程修了．2019 年同大学院情報科学研究科博士後期課程修了．同年山口大学大学院創成科学研究科助教となり，現在に至る．システム制御理論とその応用の研究に従事．博士（情報科学）．計測自動制御学会，システム制御情報学会，IEEE の会員.

国際会議開催報告

28th Asia and South Pacific Design Automation Conference

（ASP-DAC 2023，アジア南太平洋設計自動化会議，https://www.aspdac.com/aspdac2023/）

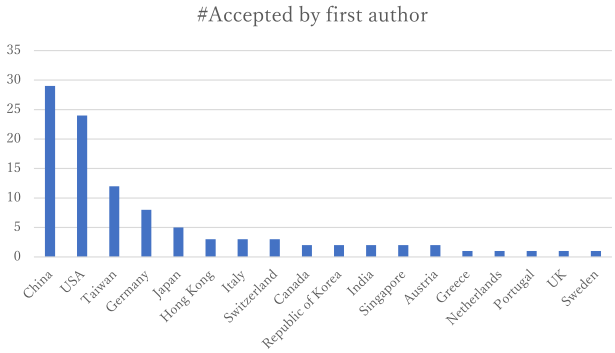
日本科学未来館，東京都江東区，オンライン併催

2023 年 1 月 16 日～19 日

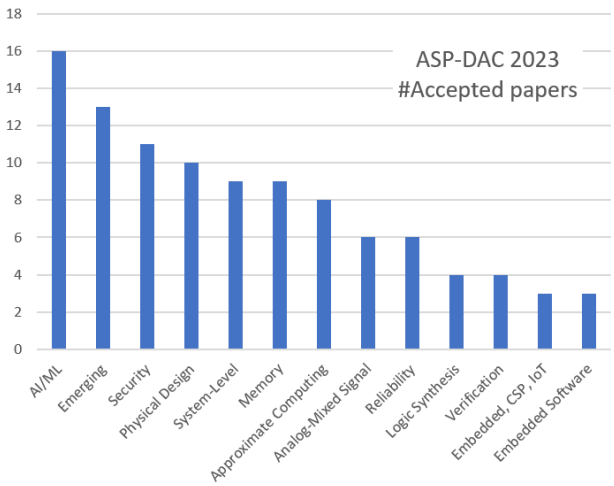
メイン会場（未来館ホール）の風景

ASP-DAC は，電子システムの設計自動化をテーマとする国際会議であり，COVID-19 の感染拡大を受けて第 26 回・第 27 回は完全オンラインでの開催であったが，今回は対面を主とし，オンラインでの配信も行うハイブリッドでの開催となった．23 か国より 360 名を超える参加者があり，セッションだけでなくコーヒーブレイクなどでも活発な議論が行われた．29 か国から 328 件の投稿があり，102 件が採択された（採択率 31.1%）．採択論文は中国からが 29 件と最も多く，次いで米国 24 件，台湾 12 件であり，日本からは 5 件が採択された．分野としては AI/機械学習が最も多く，次いでハードウェアセキュリティ，エマージングデバイスなどが多数の投稿を集めた．

1 日めは七つのチュートリアルセッションが実施された．続く 3 日間は基調講演から始まり，一般セッションのほかに招待講演からなるスペシャルセッション，実際の製品開発の知見を共有するデザイナーズフォーラム，大学や教育機関で実装・測定された結果によるデザインコンテストなど，多数の企画が実施された．今回より新たに WIP（Work-in-



国別の論文数



分野別の論文数

基調講演の風景

ポスターセッションの風景

progress）が実施され，現在進行中の研究課題に関する意見交換も行われた．1 日めの基調講演は東京大学の黒田教授より今後の集積回路設計に関する展望，2 日めの基調講演は KU Leuven の Gielen 教授よりアナログ回路設計自動化の動向，3 日めの基調講演では TSMC の安井氏より集積回路の設計製造に関する最新の話題が提供された．

発表形態は全体の 6 割が対面での発表，残りがオンラインでの発表であった．事前に講演の録画ビデオを投稿しておく方法を学会として提供するなど，ハイブリッド開催でのトラブルにも備えた運営がなされていた．第 29 回は 2024 年 1 月 21 日〜24 日に韓国仁川で開催される予定である．

土谷　亮（正員）

2005 年京都大学大学院情報学研究科通信情報システム専攻博士課程修了．博士（情報学）．現在，滋賀県立大学工学部准教授．ASP-DAC 2023 では University LSI Design Contest Chair を務めた．

クイズ　名古屋大学

山里敬也（名古屋大学），岡田　啓（名古屋大学）

2023 年 9 月に開催させて頂かせてまいます本会ソサイエティ大会は，緑が仰山ある名古屋大学で開催させてちょぉだゃぁます．名古屋大学で大会を開催させてまいますのは，えらいやっとかめなことですで，わたしら現地校実行委員会もでぇりゃぁ楽しみにさせてもらっとります．本稿では，みなさま方に名古屋と名古屋大学を，まっと知ってまうために，クイズを作らさせてまいました．どうぞ，楽しんでちょぉでゃぁませ．

注意事項：

●クイズは全部で 10 問あります．制限時間は 30 分です．30 分を超えて回答した場合は不正行為とみなします．
●不正行為を行った場合は，名古屋大学キャンパスへの入構が禁止されます．なお，悪質な不正行為については，現地校実行委員会よりおしりぺんぺんなどの身体的苦痛を伴う処罰を行う場合があります．
●次のものを使用してはいけません．
　➢携帯電話，スマートフォン，ウェアラブル端末，タブレット端末，電子辞書，IC レコーダー，イヤホン，音楽プレーヤーなどの電子機器類
　➢辞書，地図，ガイドブックなどの書籍及び愛知県，名古屋市，名古屋大学に関するパンフレットや配布物など
●クイズ回答中は英文字や地図などがプリントされている服などは着用しないでください．着用している場合には，脱いでもらうことがあります．

準備はよいですか．それでは始めましょう．

問一　名大，名鉄，名駅の正しい読みは次のどれか．

1　めいだい，めいてつ，めいえき
2　なだい，なてつ，なえき
3　めいでゃぁ，めぇ〜てつ，めぇ〜えき

問二　名古屋大学の最寄り駅は次のどれか．

1　名大駅
2　名古屋大学前駅
3　名古屋大学駅

問三　次のクイズは ChatGPT で作成したものである．正しいのは次のどれか．

1　名古屋大学の略称は何でしょうか？
　名古屋大学の略称は「名大」または「NU」です．
2　名古屋大学で開発された，世界初の携帯電話は何年に発売されたでしょうか？
　名古屋大学で開発された世界初の携帯電話は，1979 年に発売されました．
3　名古屋大学が誇る，ノーベル賞受賞者は何人いるでしょうか？
　名古屋大学が誇る，ノーベル賞受賞者は，化学分野で梅崎義明氏，物理学分野で朝永振一郎氏，平和賞分野で倉石正彦氏の計 3 人です．

問四　名古屋大学に大会（総合大会あるいはソサイエティ大会）がくるのは何年ぶりか.

1　30 年ぶり
2　20 年ぶり
3　10 年ぶり

問五　2023 年ソサイエティ大会の懇親会会場は次のどれか.

1　名大生協
2　リリィ（栄）（テレビ塔にあるレストラン）
3　ザ・コンダーハウス（旧名古屋銀行本店，重厚な歴史的建物）

問六　名古屋大学に実際にあるものは次のどれか.

1　ニュートンのりんごの木
2　イ号テレビ
3　テレフンケン式発電機（ドイツ製）を使用した長波送信設備

問七　名古屋大学にあるビルの名称で正しいものは次のどれか.

1　赤﨑記念研究館
2　天野記念研究館
3　豊田記念研究館

問八　名古屋大学附属高校の出身者は次の誰か.

1　浅田真央
2　藤井聡太
3　宇野昌磨

問九　名古屋市緑区で作っているお酒は次のどれか.

1　醸し人九平次（萬乗醸造）
2　蓬莱泉（関谷醸造）
3　二兎（丸石醸造）

問十　名古屋のお土産としてふさわしいものは次のどれか.

1　えびせんべい　ゆかり
2　赤福餅
3　うなぎパイ

いかがでしたでしょうか．お楽しみ頂けましたか.
いずれも調べればすぐに答えが分かりますので，あえて答えは書きません．なお，みごと全問正解の方は現地校実行委員会の

メンバーまでお知らせください．懇親会会場にてハイタッチでお祝いさせて頂きます．ご希望でしたらオプションでジャンプハイタッチも可能ですのでお申し付けください．そうそう，現地校実行委員会のメンバーの紹介がまだでしたね．９月のソサイエティ大会は次の先生方のご協力のもと運営させて頂きます．

委員長：電気・山里　敬也（大会委員も兼ねる）
総務係：電気・岡田　　啓（大会委員も兼ねる）
会場係：電気・長谷川　浩，森　洋二郎
運営係：情報・村瀬　　勉，西田　直樹
会計係：情報・楫　　勇一

名古屋大学でみなさまにお目にかかるのを楽しみにしております．

謝辞

冒頭の名古屋弁は，名古屋で長くラジオドラマを書かれている伊佐治弥生氏に翻訳頂きました．記して謝意を申し上げます．こちら，上町言葉と呼ばれる上品なことばでございます．名古屋市長が話す庶民的な名古屋弁と異なり，上町言葉の特徴は丁寧語に丁寧語を重ねるのが特徴です．

山里敬也（正員：フェロー）
平５慶大大学院博士課程了．博士（工学）．現在，名大教養教育院教授．平 26 本会会長特別表彰，IEEE Communications Society 2006 Best Tutorial Paper Award，令元本会論文賞を受賞．可視光通信，ITS，OER の研究に従事．映像情報メディア学会，IEEE 各会員．

岡田　啓（正員：シニア会員）
平 11 名大学院博士課程了．博士（工学）．平 23 名大・准教授，現在に至る．無線通信システム，無線ネットワーク，可視光通信などの研究に従事．IEEE，ACM 各会員．平 26 本会通信ソサイエティ ComEX Best Letter Award 受賞．

受賞者の声

電子情報通信学会に関連する賞を受賞された方を御紹介します.

令和４年度フェロー称号

令和４年に新たにフェロー称号を贈呈された方は学会全体で 22 名でした．ここでは基礎・境界ソサイエティ推薦及び NOLTA ソサイエティ推薦でフェローになられた３名の方を御紹介します！

石浦菜岐佐

「論理設計の自動化およびコンパイラのテストに関する先駆的研究」

Q. フェローになられた御感想をお聞かせ下さい.

電子情報通信学会関連の様々な研究集会やイベントでは，多くの方々，とりわけ先にフェローになられている先輩方にお世話になってきました．それを考えると自分のフェローの称号を頂くことの重みを感じますが，自分がフェローに値する業績を残してくることができたか，もっと頑張って活動をできなかったか，今一度考えざるを得ません.

Q. 現在，御興味を持たれている研究テーマを教えて下さい.

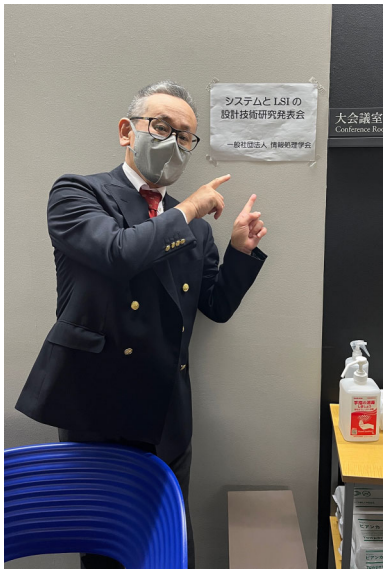
組み込みシステムのハードウェア設計，特に最近では，リアルタイム OS を利用して実装された制御システムを全て自動的にハードウェア化する技術の研究や，プロセッサの機械語プログラムから等価なハードウェアを合成するバイナリ合成技術，ニューラルネットワークの FPGA 実装の研究と並行して，コンパイラの最適化性能のランダムテストの研究に取り組んでいます.

Q. 今後の抱負をお聞かせ下さい.

自分がメインとする研究分野以外にも日々多くのことを勉強し，それを学生達に伝えていかなければならないと感じています．今後も研究集会に学生と一緒に積極的に参加させて頂きたいと思います.

Q. 若い研究者の方へメッセージをどうぞ！

こんなことを言って良いのかわからないのですが……．今振り返ると，寝食を忘れて研究をしていた頃が一番幸せで，自分の人生にとって一番意味のある時間だったと思えます.



関屋大雄

「非線形解析技術を用いた高周波電源設計に関する研究」

Q. フェローになられた御感想をお聞かせ下さい.

学生時代の恩師，先輩，同期，後輩，学生時代からお世話になった学会関係者の方々，そして千葉大学で一緒に研究を進めてきた先生・学生など，いろいろな方に支えられてここまできました．フェローの称号を頂けることとなり，たいへん光栄に感じますとともに，関係者の皆様に深く感謝いたします．

Q. 現在，御興味を持たれている研究テーマを教えて下さい.

GaN（窒化ガリウム）デバイスの登場により，パワーコンバータやワイヤレス給電システムの MHz 帯高周波化に向けた実現可能性が高まってきました．非線形回路解析技術を積極的に用いてこれらシステムの設計高度化を目指しています．また，全く異なるテーマとなりますが，IoT とスパイキングニューラルネットワークの概念を統合したあらたな情報処理プラットホームの実現に向けて研究開発を進めています．

Q. 今後の抱負をお聞かせ下さい.

「非線形」をバックグラウンドにもつ強みを前面に押し出し，興味をもったテーマに対して躊躇なく踏み込んでいきたいとます．また，大学教員として，研究の楽しさ，厳しさ，尊さを一人でも多くの学生に伝えていきたいです．そして，これまでお世話になりっぱなしの学会に微力ながら少しでも恩返しをしていきたいと思います．

写真 1　夏合宿にて研究室のメンバーと（2022 年）

写真 2　NOLTA2018@ タラゴナ，スペインでの General Co-Chiars, Prof. Abdelali El Aroudi と一緒に（2018 年）

写真 3　この身体ながらフルマラソンを 10 回以上完走しています（2021 年）

Q. 若い研究者の方へメッセージをどうぞ！

野球の大谷翔平，ボクシングの井上尚弥，将棋の藤井聡太などに代表されるように，今の若者には我々の世代の「常識」を軽々と乗り越える規格外の才能を感じます．若い研究者の皆さんには興味のあるテーマに没頭して頂き，これまでの常識では推し量れない画期的な技術を生み出すことを期待しています．

高島克幸

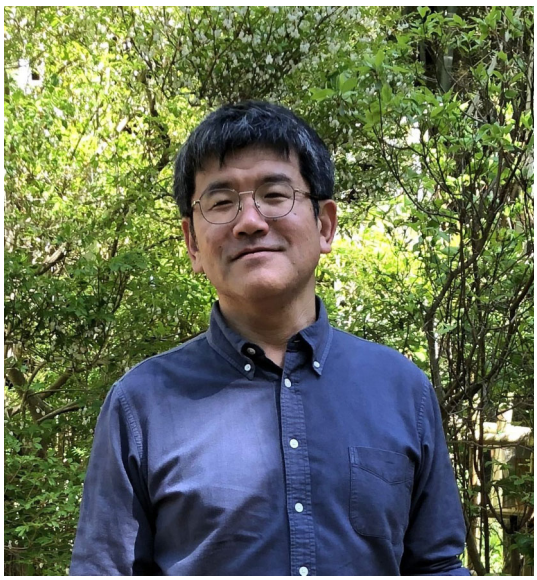
「代数曲線理論に基づく高安全・高機能な暗号構成の先駆的研究」

Q. フェローになられた御感想をお聞かせ下さい．

栄誉あるフェロー称号を頂きまして，大変光栄です．これまでの研究活動においてお世話になった皆様に深く感謝いたします．

Q. 現在，御興味を持たれている研究テーマを教えて下さい．

2022 年 7 月に，それまで同種写像暗号の中心的な方式であった SIDH 鍵共有法が，思いもかけない方法で破れました．そこでは，これまで暗号研究では周辺に位置付けられがちであった高種数の代数曲線や高次元アーベル多様体が本質的な役割を果たしており，新しい暗号数理研究の扉が開かれたといってよい状況と思います（ここで，現状では，この攻撃法は一部の同種写像暗号方式に対してのみ有効であることに注意します．その概要については，例えば，今年 4 月に公開された CRYPTREC「耐量子計算機暗号の研究動向調査報告書」（https://www.cryptrec.go.jp/report/cryptrec-tr-2001-2022.pdf）を参照して下さい）．この例に見るように，耐量子計算機暗号の研究はまだ発展途上であり，未知の研究成果が今もいろいろと埋もれていると思います．次の展開を心待ちにしていますが，私もこの分野で何か新しい寄与ができるように研究を続けていくつもりです．

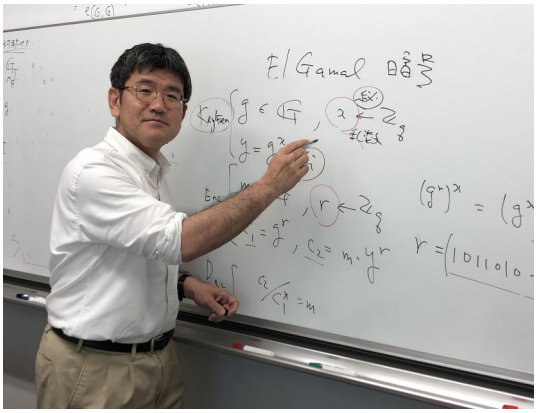


Q. 今後の抱負をお聞かせ下さい.

暗号研究は，元来，様々な研究領域にまたがることに面白さの一つがあると思いますが，私がその研究を始めた頃と比べて，本当に幅広いテーマが含まれるようになりました．私も，いつも研究最前線にアンテナを張って，視野が広くて深い研究ができるように頑張るとともに，後進の育成にも日々励んでいきたく思います．

Q. 若い研究者の方へメッセージをどうぞ！

思いもよらない仕方で発展してきたのが暗号研究の特長の一つです．これまでも，様々な分野から幅広い世代の研究者が参入して新しい研究領域を切り開いてきました．いつまでも興味が尽きない暗号研究への若手の皆さんの参加をお待ちしています．



令和４年度　学術奨励賞

令和４年度は基礎・境界ソサイエティ及び NOLTA ソサイエティでは６名が学術奨励賞を受賞されました.

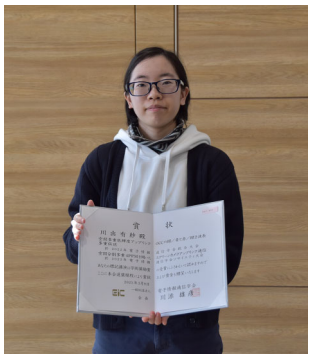
阿部　浩太郎（東京大学）“スカラー倍算におけるサイドチャネル攻撃対策効果について”(1)

このたびは名誉ある賞を頂き大変光栄に存じます．指導教員の池田誠先生をはじめ研究室メンバー，学会などでご助言を下さった先生方やご協力頂いた関係者の皆様に，この場をお借りして心から感謝申し上げます．また学会関係者の皆様にも感謝申し上げます．今回の研究はハードウェアセキュリティに関連するものになっております．この受賞を励みに，分野の発展そして社会に貢献できるよう今後とも研究活動に取り組んでいく所存です．誠にありがとうございました.

岩田　翔吾（大阪大学）“非凸問題に対する交互方向乗数法の分散エネルギー管理システムへの応用”(2)

このたびは，学術奨励賞という名誉ある賞を頂き，大変光栄に存じます．また，日頃からご指導ご鞭撻を頂いた宮本俊幸教授（大工大）をはじめとする，研究室の皆様にこの場を借りて感謝を申し上げます．受賞論文では，起動停止を含む分散エネルギー管理システムに対して，ADMM を応用したアルゴリズムを提案しております．今回の受賞を励みとし，今後もまい進する所存です．このたびは誠にありがとうございました.

川出　有紗（名城大学）

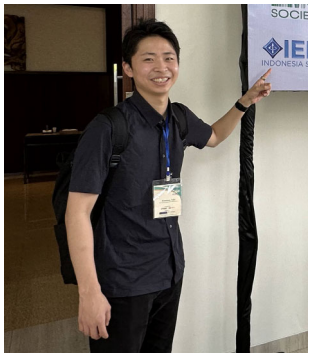


“空間多重低輝度アップリンク OCC の緑／青と赤／緑 2 波長多重伝送”(3)

“空間分割多重 4PPM を用いたスクリーンカメラアップリンク通信”(4)

このたびは学術奨励賞という名誉ある賞を賜り，大変光栄に存じます．日々ご指導頂きました中條渉先生，小林健太郎先生をはじめ，ワイドバンドシステム研究会で議論や励ましを下さった先生方，ゼミや日常生活で議論頂いた研究室のメンバーに心より感謝申し上げます．大変研究の励みになりました．受賞論文ではスマートフォンスクリーンとイメージセンサを用いた空間分割多重アップリンク可視光通信のデータレートとセキュリティ向上を提案しております．今後は社会人として引き続き「光」を基本テーマとして通信方法の発展，普及を目指して尽力して参ります．このたびは誠にありがとうございました．

北澤　太基（奈良先端科学技術大学院大学）



“漏えい電磁波の伝達特性の差に着目した高解像度ディスプレイに対する TEMPEST の検討”(5)

学術奨励賞を受賞し，大変光栄に思っております．私はハードウェアセキュリティに関する研究を行っており，総合大会では「漏えい電磁波の伝達特性の差に着目した高解像度ディスプレイに対する TEMPEST」について発表しました．この受賞においては，指導教員や研究室のメンバーの方々のご支援があったことを深く感謝しております．今後は博士後期課程において，この受賞を励みに，ハードウェアセキュリティの分野にとどまらず，より広く，深い知識と技術を習得し，社会に貢献することができるよう，努力してまいります．

鯨井　慎也（法政大学）

“ヒステリシスニューラルネットの 2 目的最適化問題について”(6)

このたびは，学術奨励賞という名誉ある賞を頂き，大変光栄に存じます．本研究を進めるにあたり，日々熱心なご指導を頂きました斎藤利通教授をはじめ，研究室の皆さん，研究会などで議論して下さいました諸先生方に，この場をお借りして厚く御礼申し上げます．

受賞論文では，ヒステリシスニューラルネットの 2 目的最適化問題について検討しました．今回の賞を励みに，今後もより一層研究に邁進する所存です．このたびは誠にありがとうございました．

上記の方々に加え，次の方も受賞されています．

福島　悠生（工学院大学）

“デプスカメラとステレオマイクロホンを用いた配管損傷位置の推定に関する検討”(7)

“座標系の異なるデプスカメラとステレオマイクロホンを用いた配管損傷箇所の位置推定に関する検討”(8)

学術奨励賞対象論文

（1） 阿部浩太郎，“スカラー倍算におけるサイドチャネル攻撃対策効果について，”2022 信学ソ大，A-19-1，Sept. 2022.
（2） 岩田翔吾，“非凸問題に対する交互方向乗数法の分散エネルギー管理システムへの応用，”2022 信学総大，A-10-6，March 2022.
（3） 川出有紗，“空間多重低輝度アップリンク OCC の緑／青と赤／緑 2 波長多重伝送，”2022 信学総大，A-9-7，March

2022.
（4） 川出有紗，“空間分割多重 4PPM を用いたスクリーンカメラアップリンク通信，”2022 信学ソ大，A-9-4, Sept. 2022.
（5） 北澤太基，“漏えい電磁波の伝達特性の差に着目した高解像度ディスプレイに対する TEMPEST の検討，”2022 信学総大，A-19-6, March 2022.
（6） 鯨井慎也，“ヒステリシスニューラルネットの 2 目的最適化問題について，”2022 信学ソ大，N-1-5, Sept. 2022.
（7） 福島悠生，“デプスカメラとステレオマイクロホンを用いた配管損傷位置の推定に関する検討，”2022 信学総大，A-5-3, March 2022.
（8） 福島悠生，“座標系の異なるデプスカメラとステレオマイクロホンを用いた配管損傷箇所の位置推定に関する検討，”2022 信学ソ大，A-5-1, Sept. 2022.

2023 International Workshop on Smart Info-Media Systems in Asia (SISA2023)

31 August - 1st September 2023

Hybrid Conference

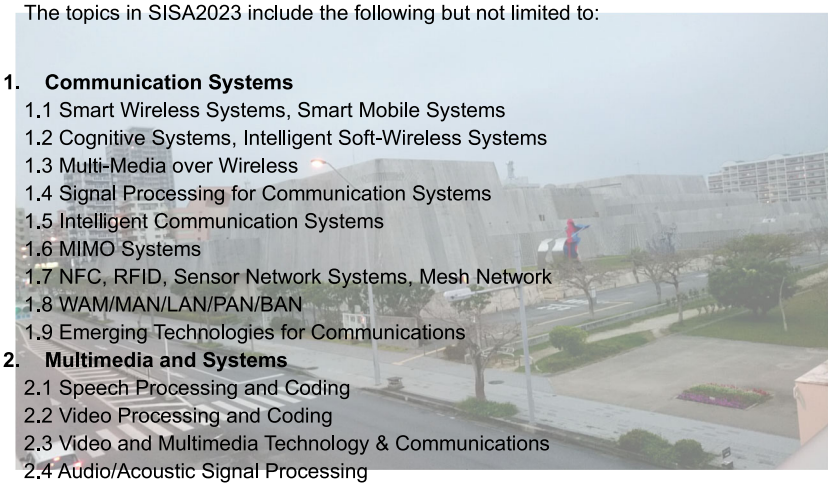
On-site: Okinawa Prefectural Museum and Art Museum, Naha, Okinawa, Japan

Call for Participants

The 2023 International Workshop on Smart Info-Media System in Asia (SISA2023) will be held in a hybrid format from 31 August to 1st September 2023. The on-site venue is Okinawa Prefectural Museum and Art Museum, in Okinawa, Japan. The SISA2023 presents every possibility on new information technologies and its smart systems.

The SISA2023 is aiming at promoting young researchers in the fields of multimedia system and wireless communications. We plan to organize short oral presentations with poster discussion for regular sessions as well as a keynote talk and special sessions. Prospective authors are invited to submit their papers reporting original works in these fields.

The topics in SISA2023 include the following but not limited to:



1. Communication Systems
- 1.1 Smart Wireless Systems, Smart Mobile Systems
- 1.2 Cognitive Systems, Intelligent Soft-Wireless Systems
- 1.3 Multi-Media over Wireless
- 1.4 Signal Processing for Communication Systems
- 1.5 Intelligent Communication Systems
- 1.6 MIMO Systems
- 1.7 NFC, RFID, Sensor Network Systems, Mesh Network
- 1.8 WAM/MAN/LAN/PAN/BAN
- 1.9 Emerging Technologies for Communications

2. Multimedia and Systems
- 2.1 Speech Processing and Coding
- 2.2 Video Processing and Coding
- 2.3 Video and Multimedia Technology & Communications
- 2.4 Audio/Acoustic Signal Processing
- 2.5 Signal Processing for Medical Technologies
- 2.6 Intelligent Signal Processing for Multimedia & Systems
- 2.7 Security Signal Processing for Multimedia & Systems
- 2.8 Parallel Implementation for Multimedia & Systems
- 2.9 Emerging Technologies for Multimedia & Systems

3. Information Science and Technologies
- 3.1 Intelligent Transport Systems
- 3.2 Bioinformatics, Neural Networks and Fuzzy Systems
- 3.3 Informatics for Green Earth & Environmental Technologies

Registration Fee

The details of registration fee will be announced on SISA2023 website:

http://www.ieice-sisa.org/

SISA 2023 Student Paper Awards

Paper presented in regular sessions can be nominated for the Student Paper Awards, provided that the first author is a full time undergraduate, Masters or Ph.D. student.

Special Section on IEICE Trans. Fundamentals

We plan to publish a *Special Section on IEICE Trans. Fundamentals* on November 2024. Authors who presented their original works in SISA 2023 are solicited to submit papers to this special section.

開催案内

Call for Participants

Original papers on the research and development of various security topics, as well as case studies and implementation experiences, are solicited for submission to IWSEC 2023. Topics of interest for IWSEC 2023 include all theory and practice of cryptography, information security, and network security, as in the previous IWSEC workshops. We classify the topics of interest into two tracks as follows, but not limited to:

A: Cryptography track

- Applied cryptography
- Biometrics security and privacy
- Blockchain and cryptocurrency
- Cryptanalysis
- Cryptographic primitives
- Cryptographic protocols
- Financial cryptography
- Formal methods for security analysis
- Multiparty computation
- Post-quantum cryptography
- Privacy-preserving data mining
- Public-key cryptography
- Real-world cryptographic systems
- Symmetric-key cryptography

B: Cybersecurity and privacy track

- Cyberattacks and defenses
- Cyber physical systems
- Forensics
- Hardware security
- Human-computer interaction, security, and privacy
- Internet-of-Things security
- Intrusion detection and prevention
- Law and ethics of cybersecurity
- Machine learning and AI security
- Malware analysis
- Measurements for cybersecurity
- Mobile and web security
- Network, system and cloud security
- Offensive security
- Privacy-enhancing technologies
- Program analysis
- Software security
- Supply chain security

Keynote Talks

We will have keynote talks from the following world-leading researchers.

Dr. Meltem Sonmez Turan (Computer Security Division of National Institute of Standards and Technology (NIST))

Prof. Gernot Heiser (Scientia Professor & the John Lions Chair for operating systems, University of New South Wales)

Dr. Kris Shrishak (Senior Fellow, Irish Council for Civil Liberties (ICCL))

Committees

General Co-Chairs:

Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology, Japan)
Koji Chida (Gunma University, Japan)

Program Co-Chairs:

Junji Shikata (Yokohama National University, Japan)
Hiroki Kuzuno (Kobe University, Japan)

論文募集

第46回情報理論とその応用シンポジウム (SITA2023)開催案内

ご挨拶

第 46 回情報理論とその応用シンポジウム(SITA2023)を山口県湯田温泉にて開催いたします。本シンポジウムは、例年、宿泊と発表会場を一体とした泊り込みのスタイルをとっております。14 年ぶりの湯田温泉開催となる今年もこのスタイルにならい、情報理論とその応用分野に関する発表を広くつのるとともに、多数の方々のご参加をお待ちしております。

実行委員長　澁谷智治

開催期間・会場

2023 年 11 月 28 日(火) ～12 月 1 日(金)
山口県山口市 湯田温泉　かめ福オンプレイス
https://kamefuku.com/

対象分野

シャノン理論、情報源符号化、データ圧縮、符号理論とその技法、通信路符号化、通信理論、符号化・変調、伝送方式、無線アクセス・ネットワーク、ワイドバンドシステム、通信方式、系列、確率過程、検定と推定、暗号、情報理論的安全性、情報セキュリティ、マルチユーザ情報理論、ネットワーク符号化、分散符号化・分散計算、計算複雑性理論、情報ネットワーク、量子情報理論、量子符号・暗号、信号処理、画像・音声処理、圧縮センシングとスパース性、パターン認識、統計的機械学習、記録素子用の符号化・信号処理、情報理論基礎・応用、情報統計力学、その他技術的内容

主催

電子情報通信学会　基礎・境界ソサイエティ
情報理論とその応用サブソサイエティ

協賛

電子情報通信学会　EMM, ISEC, RCC, RCS, SIP, WBS 研究会
IEEE Information Theory Society Japan Chapter

Web Site

https://www.ieice.org/ess/sita/SITA2023/

今後のスケジュール

発表申込開始: 8 月 1 日(火)
発表申込締切: 9 月 4 日(月)
発表原稿締切: 9 月 15 日(金)

実行委員会

実行委員長:
澁谷智治(上智大学)
プログラム委員長:
松本隆太郎 (東京工業大学)
総務:葛岡成晃(和歌山大学)
会計:野崎隆之(山口大学)
出版:柴田凌(信州大学)
会場:川村正樹(山口大学)
登録:實松豊(東京工業大学)
広報:有村光晴(湘南工科大学)
プログラム委員会幹事:
松田哲直(埼玉大学)

事務局

〒640-8510
和歌山市栄谷 930 和歌山大学
システム工学部葛岡研内
SITA2023 事務局　葛岡成晃
E-mail: sita-2023@mail.ieice.org

基礎・境界ソサイエティ運営委員会

会長	梶川　嘉延　(関西大学)
次期会長	和田山　正　(名古屋工業大学)
ソサイエティ編集長	鎌部　浩　(岐阜大学)
副会長（事業担当）	野村　亮　(早稲田大学)
副会長（システムと信号処理）	池田　誠　(東京大学)
副会長（音響・超音波）	渡部　泰明　(東京都立大学)
副会長（情報理論とその応用）	小嶋　徹也　(東京工業高等専門学校)
庶務幹事	西浦　敬信　(立命館大学)
庶務幹事	葛岡　成晃　(和歌山大学)
会計幹事	古賀　崇了　(近畿大学)
会計幹事	小林健太郎　(名城大学)
事業担当幹事	新田　高庸　(会津大学)
事業担当幹事	三村　和史　(広島市立大学)
大会担当幹事	高野　知佐　(広島市立大学)
大会担当幹事	大東　俊博　(東海大学)
電子広報担当幹事	荒井伸太郎　(岡山理科大学)
電子広報担当幹事	西川　広記　(大阪大学)
論文誌編集委員長	岩本　貢　(電気通信大学)
論文誌編集幹事	渡邉　洋平　(電気通信大学)
論文誌副編集委員長	岡田　実　(奈良先端科学技術大学院大学)
論文誌副編集幹事	林　和則　(京都大学)
ソサイエティ誌編集委員長	髙島　康裕　(北九州市立大学)
ソサイエティ誌担当幹事	小林　孝一　(北海道大学)
ソサイエティ誌担当幹事	松田　哲直　(埼玉大学)
特別委員（国外活性化担当）	尾知　博　(九州工業大学)
特別委員（国際会議コンテンツ担当）	小平　行秀　(会津大学)
編集特別幹事（オブザーバ）	山脇　大造　(日立製作所)
出版委員会委員（オブザーバ）	吉川　英機　(東北学院大学)
研究会連絡会幹事（オブザーバ）	髙島　康裕　(北九州市立大学)
ハンドブック／知識ベース委員（オブザーバ）	太田　隆博　(専修大学)
男女共同参画委員（オブザーバ）	野崎　隆之　(山口大学)
プラチナクラブ運営委員（オブザーバ）	金子　美博　(岐阜大学)
CPD 制度化委員（オブザーバ）	藤吉　正明　(東京都立大学)
事務局	水橋　慶，永井　宏　(電子情報通信学会)

基礎・境界ソサイエティサブソ・研専会議

副会長（事業担当）	野村　亮　(早稲田大学)
副会長（システムと信号処理）	池田　誠　(東京大学)
副会長（音響・超音波）	渡部　泰明　(東京都立大学)
副会長（情報理論とその応用）	小嶋　徹也　(東京工業高等専門学校)
事業担当幹事	新田　高庸　(会津大学)
事業担当幹事	三村　和史　(広島市立大学)
回路とシステム（CAS）	相原　康敏　(オムニビジョン)
情報理論（IT）	小嶋　徹也　(東京工業高等専門学校)
信頼性（R）	門田　靖　(リコー)
超音波（US）	渡部　泰明　(東京都立大学)
応用音響（EA）	小野　順貴　(東京都立大学)
VLSI 設計技術（VLD）	中武　繁寿　(北九州市立大学)
情報セキュリティ（ISEC）	花岡悟一郎　(産業技術総合研究所)
信号処理（SIP）	仲地　孝之　(琉球大学)
ワイドバンドシステム（WBS）	庄納　崇　(インテル)
システム数理と応用（MSS）	山口　真悟　(山口大学)
思考と言語（TL）	森下　美和　(神戸学院大学)
技術と社会・倫理（SITE）	大谷　卓史　(吉備国際大学)
ITS（高度交通システム）（ITS）	高取　祐介　(神奈川工科大学)
スマートインフォメディアシステム（SIS）	木村　誠聡　(神奈川工科大学)
イメージメディアクオリティ（IMQ）	工藤　博章　(名古屋大学)
高信頼制御通信（RCC）	東　俊一　(名古屋大学)
バイオメトリクス（BioX）	高野　博史　(富山県立大学)
安全・安心な生活と ICT（ICTSSL）	内田　理　(東海大学)
ハードウェアセキュリティ（HWS）	鈴木　大輔　(三菱電機)
光輝会（SSA）（オブザーバ）	宮地　充子　(大阪大学大学院)
技術の歴史（オブザーバ）	篠田　庄司　(中央大学)
技術者教育と優良実践（オブザーバ）	横田　光広　(宮崎大学)
ヒューマンコミュニケーション G（オブザーバ）	松田　昌史　(NTT コミュニケーション科学基礎研究所)
会長（オブザーバ）	梶川　嘉延　(関西大学)
次期会長（オブザーバ）	和田山　正　(名古屋工業大学)
庶務幹事（オブザーバ）	西浦　敬信　(立命館大学)
庶務幹事（オブザーバ）	葛岡　成晃　(和歌山大学)
研究会連絡会幹事（オブザーバ）	髙島　康裕　(北九州市立大学)
事務局	水橋　慶，永井　宏　(電子情報通信学会)

NOLTA ソサイエティ運営委員会

ソサイエティ会長	長谷川幹雄　(東京理科大学)
ソサイエティ次期会長	夏目季代久　(九州工業大学)
庶務幹事	中野　秀洋　(東京都市大学)
庶務幹事	立野　勝巳　(九州工業大学)
会計幹事	木村　貴幸　(日本工業大学)
電子広報担当幹事	松浦　隆文　(日本工業大学)
大会担当幹事	高野　知佐　(広島市立大学)
運営委員	堀尾　喜彦　(東北大学)
運営委員	小西　啓治　(大阪府立大学)
運営委員	上田　哲史　(徳島大学)
運営委員	清水　邦康　(千葉工業大学)
運営委員	鳥飼　弘幸　(法政大学)
運営委員	丹治　裕一　(香川大学)
運営委員	伊藤　大輔　(岐阜大学)
運営委員	青森　久　(中京大学)
運営委員	会田　雅樹　(東京都立大学)
運営委員	内田　淳史　(埼玉大学)
運営委員	宮田　純子　(芝浦工業大学)
運営委員	保坂　亮介　(芝浦工業大学)
運営委員	斎藤　利通　(法政大学)
運営委員	浅井　哲也　(北海道大学)
運営委員	松下　春菜　(香川大学)

編集後記

今号より編集委員長を仰せつかりました．Vol. 6 No. 4 で編集幹事を辞してから 10 年．また，FR 誌の編集作業にたずさわることができ，とても光栄に思っています．電子情報通信の分野はこの 10 年で大きく変化していますが，でもヒトの好奇心は決してなくなるものではありません．FR 誌を通して皆様の電子情報通信の分野の興味を更にかきたてられるように編集作業を進めていきたいと思います．今後ともよろしくお願いいたします．（髙島康裕）

今号より編集正幹事を担当することになりました．タイムリーに魅力的な解説論文が出版できるように努力していきます．ほかの学会誌の解説と比べると，FR 誌の解説論文は十分なページ数をとっており，内容を深く理解できる印象があります．FR 誌のこのような良さを大事にしつつ，更なる発展を目指して参ります．新型コロナウイルスから解放されて，国際会議や研究会が対面開催になっていますが，FR 誌を読む時間を確保して頂けますと幸いです．今後ともどうぞよろしくお願い申し上げます．（小林孝一）

今号より編集副幹事を担当いたします．主として担当する記事は，「開催案内」や「論文募集」などのやわらかい記事となります．今号において記事をご執筆頂いた皆様には改めて御礼申し上げます．今後も，FR 誌を通じて研究活動の最前線を読者の皆様にお届けしたいと考えております．引き続き，どうぞよろしくお願い申し上げます．（松田哲直）

今号より編集幹事会幹事補佐を務めることになり，「受賞者の声」の編集を担当しました．これまで電子情報通信学会では，専門委員会幹事，サブソサイエティ幹事，論文誌編集委員などを務めてまいりましたが，FR 誌の編集に携わることになり，改めて電子情報通信学会のカバーする分野の広さに驚いております．不慣れな点も多く恐縮ですが，FR 誌の発展に微力ながら尽力していく所存です．今後ともよろしくお願いいたします．最後になりますが，受賞者の皆様に改めてお祝い申し上げますとともに，ご担当頂いた事務局・出版社の皆様にお礼申し上げます．（松井健太郎）

今号の「研究会に行こう！」の特別編集幹事を担当させて頂きました．ご執筆頂きました著者の皆様，並びにサポート頂きました編集委員，事務局，出版社の皆様に，この場を借りて御礼申し上げます．いずれの研究会においても，昨年度より対面形式も復活してきており，休憩時間やその後の懇親会での有意義な議論・情報交換も再開してきているようです．並行して最新の情報技術によってこれらをハイブリッドでも実現できるよう試行錯誤を進めている研究会もあります．是非とも各研究会の取り組みをご一読頂き，研究会への投稿・ご参加をご検討頂けましたらと存じます．（吉川隆英）

Fundamentals Review へのお問い合わせ

・本誌への御意見．御要望．入手など：fr-ess@ieice.org
・Fundamentals Review Homepage：https://www.ieice.org/ess/ESS/Fundam-Review.html

Fundamentals Review 第十七巻 第一号

令和五年七月一日発行

発行人	白石　智
発行所	一般社団法人 電子情報通信学会　基礎・境界ソサイエティ 〒 105-0011 東京都港区芝公園 3-5-8（機械振興会館内） 電話 03-3433-6691(代) FAX 03-3433-6659
WEB 化担当	山岡影光
WEB 化担当会社	三美印刷株式会社 東京都荒川区西日暮里 6-28-1