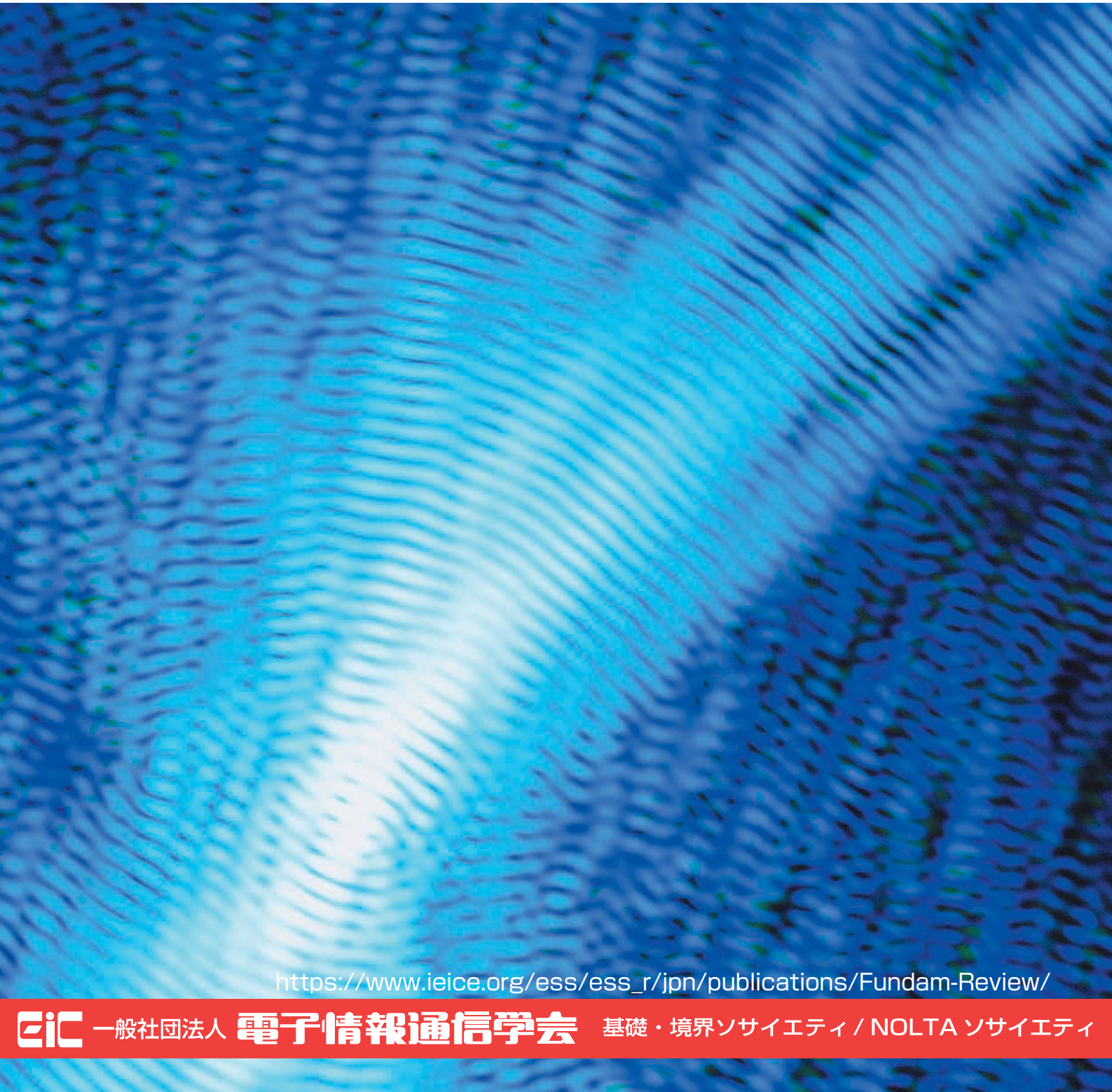
令和８年７月１日発行　第 77 号

Fundamentals Review

2026 July Vol.20 No. 1



https://www.ieice.org/ess/ess_r/jpn/publications/Fundam-Review/

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
2026
July
Vol.20 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

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

Preface

Review Papers

Miscellaneous Articles

ごあいさつ

基礎・境界ソサイエティのこれから —次の 30 年に向けて

Looking Ahead for ESS—Toward the Next 30 Years

基礎・境界ソサイエティ会長　岩本　貢

1. はじめに

基礎・境界ソサイエティ（Engineering Sciences Society：ESS）はその名のとおり，電子情報通信分野の「基礎」と「境界」に位置する研究コミュニティの集まりであり，四つのサブソサイエティ（信号処理とその応用，システムデザイン技術，音響・超音波，情報理論とその応用）に加え，これらに属さない 12 の研究会，一つの特別研究会，二つの第三種研究会からなっています．

サブソサイエティ制は，本会において ESS のみが導入している独自のシステムです．基礎理論や境界領域にある研究分野は，研究目的や手法が多岐にわたるため分散しがちですが，これらを適切にグループ化することで，研究の相乗効果を生み出す狙いがあります．それゆえ，新たな分野を育て，「新ソサイエティを生み出す母体」として機能することは，1995 年のソサイエティ制発足当初から期待されてきた ESS の重要な使命です[(1)]．

具体的な研究分野そのものではなく，「基礎」や「境界」という観点から構成されたソサイエティは，海外を含めても比較的珍しい存在です．しかし，このような役割を担うソサイエティは，変化の時代において特に重要であると思います．筆者は次期ソサイエティ会長への所信表明において，人工知能研究者がノーベル賞を受賞する時代になったことは，科学技術における基礎と応用，更には分野間の境界が急速に融合しつつあることを象徴している，という趣旨のことを書きました．異なる分野が相互に連携することで新たなイノベーションが生まれる現在，分野横断的な研究や基礎・境界領域の重要性は今後更に高まっていくものと思います．現在は，電子情報通信分野のみならず，社会全体にとっても大きな変化の時期であることは間違いありません．

このような時期において ESS はどうあるべきか．まずは現在起きている変革の兆しや，現在進行中の具体的な取り組みについて，会員の皆様にお伝えしたいと思います．

2. ESS の現状

ソサイエティ制は 15 年という長い準備を経て 1995 年 4 月にはじまり，昨年度（2025 年度）で 30 年という大きな節目を迎えました[(2)]．次の 30 年に向けて新たな歩みを始めた現在，ESS も着実に変わりつつあります．

2.1　ESS の運営体制の変化

まずは，2014 年 10 月までサブソサイエティであった，NOLTA（非線形理論とその応用：Nonlinear Science and Its Applications）ソサイエティについてです．これは，ESS の中にあった NOLTA サブソサイエティがソサイエティ化された初の事例であり，ソサイエティ制発足後，初めて誕生した新しいソサイエティでもあります．ソサイエティ制発足当初に期待された「新しいソサイエティを生み出す母体」としての役割を具現化した画期的な出来事です．現在は財務面などにおいて ESS との共同運営体制を取っています．

発足当初から，NOLTA ジャーナルや NOLTA シンポジウムなどは独立して活動を行っていましたが，共同運営体制であったこともあり，これまでは NOLTA 会長がオブザーバとして学会理事会に出席していました．しかし，ソサイエティ化から 11 年が経過した昨年度，NOLTA からも理事を出すことが決定され，様々な準備が進んでいます．ソサイエティ誌 Fundamentals Review（FR）の編集など，一部機能については共同運営体制を維持しつつ，より独立したソサイエティとしての最終段階に向けた大きな一歩となる予定です．ESS としても積極的に協力し，NOLTA ソサイエティの更なる発展をお手伝いできればと思っています．

2.2　サブソサイエティの変化

サブソサイエティは発足以来，様々に形を変えながら現在に至っています．近年で最も大きな変化は，システムと信号処理サブソサイエティが発展的に改組されることで，2025 年 4 月に「信号処理とその応用」，「システムデザイン技術」の両サブソサイエティが発足したことです．時代の流れに即してサブソサイエティを柔軟に運営していくことは，基礎・境界ソサイエティが活気を保ち，時代の要請に応

えていくために極めて重要であると思います．

今年度も，サブソサイエティ制には大きな変化が起きる予定です．セキュリティ関連研究会が ISEC 研究会の四方順司顧問のもと，新たなサブソサイエティを設立する計画が昨年度の ESS サブソ・研専会議で示されました．情報セキュリティは現在の情報通信社会における基盤インフラですが，理論から応用まで極めて幅広く，複数の研究会が存在しています．これらの研究会は，共通する目的のもと，これまでも合同で様々な研究活動を行ってきました．最も代表的な例は，暗号と情報セキュリティシンポジウム（SCIS）です．SCIS を軸に関係研究会が集まりサブソサイエティ化することは，サブソサイエティ制の理念にも合致しており，我が国の暗号・情報セキュリティ研究を更に発展させることにつながると考えています．

このように，サブソサイエティは形を変えながら活発な活動を続けています．これらのサブソサイエティから，NOLTA に続く新たなソサイエティが生まれることを強く期待しています．

2.3 ESS シンポジウム

ソサイエティやサブソサイエティの変化は，ESS 全体の活動が活発であることを示しています．また，国内だけでなく国際的な研究活動の活性化も重要です．ESS では，これまで東南アジア圏での論文執筆セミナーなどを実施し，大きな成果を挙げてきました．しかし残念ながら，IEICE 全体として海外会員数の減少は著しく，新たな施策が求められています．

このような状況を受け，海外会員にも参加しやすい各ソサイエティの flagship conference を開催することが，本学会の前会長で，ESS の元会長でもある植松友彦先生から提案されています．ESS でもこの提案を受け，ESS Symposium（ESSS）が企画されました．記念すべき第一回シンポジウムは，和田山正先生（ESS 元会長）を実行委員長，小嶋徹也先生（ESS 事業担当副会長）をプログラム委員長として，2026 年 10 月 30 日から 11 月 1 日にかけて沖縄県市町村自治会館で開催される予定です[(3)]．

既に述べたとおり，ESS は様々な分野の基礎や境界領域における研究グループの集まりです．ESSS は，そのような ESS の分野横断的な特徴が前面に現れた国際会議になることが期待されます．研究分野の進展は極めて速く，近接分野であっても動向を追い続けることは容易ではありません．しかし，だからこそ，分野横断的な議論は新しい視点を得るうえで大きな刺激になるはずです．その意味で，ESSS が「新しい研究の方向性を生み出す母体」となるような，ESS らしい企画へと発展していくことを期待しています．

今回の ESS シンポジウムは，SITA サブソサイエティが隔年で開催している国際会議 ISITA（International Symposium on Information Theory and Its Applications）と連続開催される予定です．両方に参加する参加者には参加費の割引制度なども予定されています．情報理論分野以外の方にも，ぜひ沖縄へお越し頂ければ幸いです．

3. 次の 30 年に向けて

さて，ESS は今後どのように進んでいくべきか．変化の多いこの時代において，「次の 30 年」に向けた一手を打つことは非常に難しく，会長を拝命したとはいえ，筆者には荷の重い問題です．

困ったときには原点に帰るしかありません．AI が人の仕事を奪うことが懸念される現在でも，研究の中心はやはり「人」にあります．研究者や学生の皆さんが創造性を発揮できる環境を整えることこそが，学会の最も重要な使命です．言うまでもなく，学会は，楽しく自由闊達な議論を通じて新たな知を生み出し，次の研究への活力を得るための不可欠なプラットフォームです．論文誌や FR，大会や研究会がなくなったら研究が続かない，研究の楽しみがなくなる，と思う人は多いと思います．どんなに ePrint サーバに論文を発表しても，査読も議論の場もない世界で研究成果を蓄積することは，学問の持続的な発展において不毛と言わざるを得ません．

このような「ごあいさつ」の場で多くの方が語っておられるように，学会，特に研究会での発表経験は，多くの研究者の研究活動の原点になっていると思います．かくいう筆者も，初発表の緊張や，教科書や論文でしか知らない著名な研究者との出会いの記憶は鮮明です．様々なご意見があるのを承知で言ってしまえば，学会の魅力の第一は成果の「発表の場」にあります．まずは，このような体験ができる場を多くの学生さんや若手研究者に提供し，研究活動の間口を広げることは，いつの時代にも大事だと思います．特に，日本語での発表が可能な国内学会は，研究発表の入口として，あるいは，速報的な研究成果を議論する場，ネットワーク構築やプロモーションの場として，その価値が減ずることはないと信じます．

しかし，言うまでもなく，このような場は当たり前に存在するわけではありません．このような場が提供されるのは，学会事務局の多大な努力だけでなく，多くの会員の皆様の献身的な協力によって支えられているのが現実です．筆者は大学に所属していますが，大学の使命が教育と研究にある以上，学会の存在は，大学の外にありながらも，我々にとって必要不可欠なもののはずです．これは企業や公的研究機関においても，（事情は多少異なるにせよ）同様の側面があると思います．学問のプラットフォームとしての学会に対する社会の理解と協力をより広げられるよう，学会運営側だけでなく，学会に集う皆さんで努力していくべきだろうと思います．

とはいえ，理想を語っても現実は厳しいと思われます．残念ながら，少子高齢化の影響もあり，このような運営を担う

人手が足りなくなってきていることは，既に歴代の ESS 会長挨拶でも述べられている問題です．また，何事にもタイパ・コスパが求められ，何につけても慌ただしい現在において，ボランティアに頼って学会活動を進めるためには，理想論や情熱だけではいかんともしがたい面があります．そのためには，皆で負担を分担しながら，必要にして十分なことを厳選したうえで，これを着実に進めていくしかありません．

学生や若手研究者から見ると，研究発表の場としての研究会，ソサイエティ大会や総合大会での研究会セッションや企画などを通じて，研究会が ESS の顔として映っていることでしょう．その意味では，研究専門委員会の存在は比較的多くの人の目に触れやすいと思います．しかし，ESS においては，その活発な活動を組織的に支えているのがサブソサイエティです．この意味において，サブソサイエティは ESS の「縁の下の力持ち」ともいうべき存在であり，サブソサイエティが大きく変化している現在，このエネルギーを今後の発展のばねにするのは自然なことだと思います．その結果として，新たなソサイエティが生まれることも期待できるでしょう．NOLTA ソサイエティという素晴らしい成功例を手本としながら，研究活動とその運営がともに持続的に発展していくよう，ESS としてどのようなお手伝いができるのかを考えていきたいと思います．

4. む す び

ソサイエティ制が始まった 1995 年，筆者は大学 1 年生でした．そのような世代が ESS 会長を仰せつかるまで，ソサイエティ制は受け継がれてきました．ソサイエティ制の実現に向けた議論には 15 年もの歳月が費やされており，そこで交わされた議論や理念が，いまも脈々と受け継がれていることに深い感銘を覚えます．その先見性には学ぶべき点が多いと感じています．

一方で，長く続く組織が設立当初の理念を少しずつ変化させていくこと自体は，自然なことでもあると思います．現在には現在の課題や価値観があり，未来には未来の研究コミュニティがあるからです．諸先輩方の情熱に思いを致しつつも，変化の大きい現在の研究コミュニティに即した形で，次の 30 年に向けた土台を築いていくことが，今の我々に求められているのだと思います．

発足当時の制度設計にも長い年月が必要であったように，このような基盤作りも決して容易なことではありません．皆様のますますのご協力とご参画を，心よりお願い申し上げます．

文　献

（1） 末松，甘利，辻井，進士，“ソサイエティ制に向けて―将来構想実施検討委員会報告書の概要―，”電子情報通信学会誌，vol. 75, no. 10, pp. 1019-1026, 1992.
（2） 山里ほか，“ソサイエティ制をふりかえる，”電子情報通信学会誌，vol. 109, no. 3, pp. 202-229, 2026.
（3） https://esss.ieice.org

著者紹介

岩本　貢（正員：シニア会員）

1999 東大・工・計数卒．2004 同大学院情報理工学系研究科博士課程了．同年電通大大学院情報システム学研究科助手，2015 同大学院情報理工学研究科准教授，2021 同教授，現在に至る．暗号理論，情報理論の研究に従事．博士（情報理工学）．国際暗号学会（IACR），IEEE 各会員．

ごあいさつ

NOLTA ソサイエティの合言葉は「おもしろい！」

The Word “Intriguing” Is the Central Concept for the NOLTA Society

NOLTA ソサイエティ会長　小西啓治

NOLTA ソサイエティ会長を仰せつかりました大阪公立大学工学研究科の小西啓治と申します．非線形ダイナミクス・複雑系科学・制御工学などがオーバーラップするニッチな領域を，出たり入ったりしながら 35 年近くも研究を楽しんでいます．現在でも研究活動は大好きで，数式をこねくり回したり，論文をコツコツと執筆したり，査読者と議論（査読コメントへの回答）したりすることで，幸せを感じています．このような研究生活が送れるきっかけを与えてくれたのが，NOLTA ソサイエティ（正確には NOLTA サブソ）でした．

詳しいことは，歴代の会長あいさつに委ねますが，NOLTA ソサイエティは二つの研究専門委員会（NLP，CCS）で構成されています．私は学生時代から自主的に NLP に参加していました．大学内では，自分の研究内容を卒論や修論で発表すると，「何の役に立つの？」「性能は何パーセント向上するの？」という視点のみで評価され，つらい思いばかりしていました（今もしています）．しかし，NLP では，そのような視点よりも，学術的に「おもしろい」という視点で「研究を楽しむ」という考えが根底に流れていることを，学生ながらに感じていました．この「おもしろい」という視点は，CCS も巻き込んで NOLTA ソサイエティにも受け継がれています．

NOLTA ソサイエティでは，この「おもしろい」という視点で，若手研究者（特に大学院生）を強くエンカレッジする姿勢が古くからあり，自分が指導する大学院生だけでなく，他大学の学生も，分け隔てなく育て上げる，という気概があります．そのため，大学院生（特に博士後期課程の学生）は，他大学の教員とも気軽に議論でき，殻に閉じこもることなくオープンに研究を進めることができます．大学院生には，このような NOLTA ソサイエティ独自の雰囲気を感じてもらい，積極的に飛び込んできてほしいと願っています．きっと，楽しい研究人生が待っています．

最後になりますが，最近，学会運営に関わる立場を経験し，個人的に感じたことを述べたいと思います．それは，「(a) 学会のための仕事」と「(b) 各研究者の研究活動」のバランスが崩れないようにしたい，ということです．多くの学会では，長年にわたる会員数の減少傾向に頭を痛めています．これを打破する施策のために，(a) の業務量の更なる増加が要求されています．しかし，各個人が (a) + (b) に割ける総量は一定です．おのずと，(b) が縮小されます．一方，研究者の所属先での評価は (b) の「質×量」で決まり，(a) は参考程度です（少なくとも私の経験では）．本ソサイエティに関わる研究者が正しく評価してもらえるように，(a) はできるだけ省力化・効率化を進め，(b) の充実に注力するという方針に基づき，ソサイエティを運営していきたいと考えています．

著者紹介

小西啓治（正員：シニア会員）

1989 大阪府立高専・電気卒．1991 大阪府立大・工・電気卒．1993 同大学大学院博士前期課程修了．同年奈良高専・電気助手．1995 大阪府立大・工助手．2002 はこだて未来大・複雑系助教授．2006 大阪府立大・工助教授（准教授）．2009 同教授．2022 大阪公立大・工教授，現在に至る．複雑系科学とシステム制御の研究に従事．2008 FR 誌編集委員会幹事．2014 非線形問題研究専門委員会委員長．2023 NOLTA General co-chairs．2019 システム制御情報学会編集委員長（編集理事）．2024 電気学会理事（支部担当）．博士（工学）．

解　説　論　文

生成AI・エージェントセキュリティ最前線

Frontiers of Generative AI and Agent Security

披田野清良 Seira HIDANO

アブストラクト　生成 AI の社会実装が加速する一方，それを標的としたサイバー攻撃による実被害が増加し，AI のためのセキュリティ（AI セキュリティ）が喫緊の課題となっている．本稿では，特に脅威が顕在化している大規模言語モデル（LLM）に着目し，AI セキュリティの最新動向を解説する．主に，LLM に対する代表的な攻撃であるジェイルブレイクを取り上げ，その最新の手法と防御技術について述べる．更に，昨今のトレンドである AI エージェントのセキュリティ動向についても概説する．

キーワード　LLM，VLM，AI エージェント，ジェイルブレイク，アライメント

Abstract　While the social deployment of generative AI is accelerating, growing damage from cyberattacks against generative AI has made security for AI (AI security) a pressing challenge. This article surveys the latest trends in AI Security, with a particular focus on large language models (LLMs) where threats are becoming increasingly apparent. It mainly examines jailbreaking, a representative attack on LLMs, and describes its latest methods and defensive technologies. Additionally, this paper outlines the security trends for AI agents, another emerging area of interest.

Key words　LLM, VLM, AI Agent, Jailbreak, Alignment

1. はじめに

近年，大規模言語モデル（Large Language Model, LLM）をはじめとする生成 AI は，加速度的に進化し，あらゆる領域において社会実装が進んでいる．しかし，その広範な活用により，新たなセキュリティ上の脅威が社会問題となっている．生成 AI を標的としたサイバー攻撃は日々複雑化・高度化しており，経済的，社会的に重大な被害が多数報告されている．

現在商用利用されている生成 AI の多くは，RLHF（Reinforcement Learning from Human Feedback）に代表されるアライメントと呼ばれる手法により，その応答が倫理的，法的，社会的な規範から逸脱しないよう調整が施されている．この安全機構が適切に機能している限り，生成 AI はたとえ有害な指示や不適切な質問が与えられても，応答を拒否するように設計されている．しかし，昨今，生成 AI に対するプロンプトなどを巧妙に細工してこの安全機構を回避するジェイルブレイク攻撃が注目を集めている．ジェイルブレイクが成功すると，生成 AI は攻撃者が意のままに利用可能な危険なツールへと変貌する．例えば，マルウェアの作成や偽情報の拡散，機密情報の取得といった犯罪行為を目的として不正利用される恐れがある．実際に，LameHug など，大規模なサイバー攻撃に LLM が使用された事例も報告されている[1]．このため，生成 AI を安心安全に利活用するためには，それらの攻撃を深く理解し，リスクを正確に評価した上で，必要かつ十分な対策を講じることが喫緊の課題である．

そこで，本稿では，現在社会の基盤技術として浸透している LLM を対象とし，LLM に対するジェイルブレイク攻撃の最新の手法と，防御策に関する最先端の研究開発動向について解説する．更に，昨今の LLM は，テキストという単一のモダリティに留まらず，画像や音声なども統合的に処理するマルチモーダル LLM や，外部の API やデータベース，ほかの AI と連携しながら自律的に意思決定と行動を実行する AI エージェントへとその能力を急速に拡大している．これらの進化は，LLM の利便性や応用可能性を飛躍的に向上させる一方，攻撃者が侵入・悪用できる経路，すなわち攻撃対象領域を拡大させ，攻撃を更に複雑化させている．このため，本稿では，マルチモーダル LLM や AI エージェントなどの次世代の AI システムが直面する新たな脅威についても概説する．

本稿の構成は次のとおりである．まず，2. 章において攻撃対象の LLM システムを定義し，想定する脅威モデルについて述べる．次いで，3. 章において LLM システムに対するジェイルブレイク攻撃，4. 章においてそれらへの防御策について解説する．最後に，5. 章において AI エージェントに対する攻撃や防御技術の最新動向について概説する．

2. 準　　備

本章では，本稿で想定する LLM システムおよび脅威モデル

披田野清良　株式会社 KDDI 総合研究所
E-mail　se-hidano@kddi.com
Seira HIDANO, Nonmember (KDDI Reserach, Inc., Fujimino-shi, Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.20 No.1 pp.6–14 2026 年 7 月

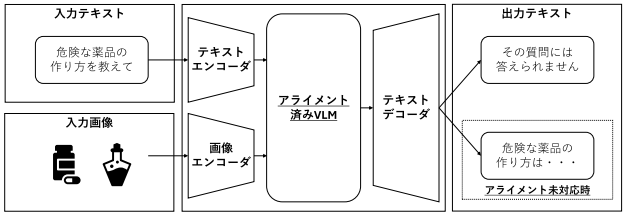


図 1　VLM の概要

を定義する．

2.1　LLM システム

本稿では，攻撃対象のシステムとして，中核に LLM を備えた AI システム（以下，LLM システム）を想定する．LLM システムは，ユーザからプロンプトと呼ばれる指示を入力として受け取り，それに対する応答を生成・出力する．対象とする LLM は，汎用の事前学習済みモデルだけでなく，利用者が独自のデータでファインチューニングしたモデルも含む．いずれの LLM も，RLHF（Reinforcement Learning from Human Feedback）などの手法により，有害な応答を生成しないよう適切にアライメントされているとする．また，本稿では，テキスト以外にも画像や音声を入力とするマルチモーダル LLM も攻撃対象として想定する．特に，図 1 に示すような画像を扱う VLM（Vision Language Model）を対象とする．なお，RAG（Retrieval-Augmented Generation）などの技術を用いて外部データベースと連携する LLM システムも存在するが，それらは 5. 章で定義する AI エージェントとして別途議論する．

2.2　脅威モデル

本稿で想定する脅威モデルを攻撃の目的，攻撃方法，攻撃者の知識の観点から定義する．

攻撃の目的. 攻撃者は，前節で定義した LLM システムの安全機構を回避し，その応答を意図的に操作することを目的とする．

攻撃方法. 本稿では主に以下の 2 種類の攻撃方法を考慮する．

- プロンプトインジェクション：ユーザが入力するプロンプトを巧妙に細工することで，モデルの応答を操作する攻撃．
- データポイズニング：LLM の訓練時（ファインチューニングを含む）に悪意のあるデータを混入し，モデルの挙動を汚染する攻撃．

攻撃者の知識. 攻撃者がもつ標的システムに関する知識のレベルに応じて，以下の二つの設定を想定する．

- ホワイトボックス：攻撃者は，標的 LLM のアーキテクチャ，パラメータ，勾配情報のような内部状態全てにアクセス可能であると仮定する．
- ブラックボックス：攻撃者は，システムへの入力（プロンプト）とそれに対する出力（応答）のみ観測可能であると仮定する．

3.　LLM システムに対する攻撃

本章では，LLM の安全機構を回避し，有害な応答や利用ポリシー違反を誘発するジェイルブレイク攻撃の最新手法について解説する．特に，本稿では，2. 章で示したように，代表事例に基づくファインチューニングや RLHF を利用してアライメントされたモデルに対して適応的に行う攻撃をジェイルブレイク攻撃として想定する．以下，本攻撃を，プロンプトベースの攻撃，探索ベースの攻撃，マルチターン攻撃，バックドア攻撃，マルチモーダル攻撃の五つのカテゴリーに分類して説明する．

3.1　プロンプトベースの攻撃

プロンプトベースの攻撃は，推論時において，LLM へのプロンプトを巧妙に細工することで，安全機構を回避する手法である[2]．本節では，代表的な攻撃手法として，ロールプレイや欺瞞に基づく攻撃と，普遍的なサフィックスを用いた攻撃について述べる．

ロールプレイに基づく攻撃では，禁止されている出力を正当化するために，架空の文脈を設定する．例えば，DAN（Do Anything Now）[3]は，安全性の制約を免除された人格になり切るように指示し，LLM が一貫性を維持しようとする性質を悪用する．TRIAL（Trolley-problem Reasoning for Interactive Attack Logic）[4]は，トロッコ問題のような道徳的ジレンマの中に有害な要求を埋め込むことで，LLM に有害な行動を正当化させる．説得攻撃[5]は，LLM が説得により影響を受けやすいという特性を利用し，社会科学的なアプローチに基づいて敵対的なプロンプト (Persuasive Adversarial Prompt，PAP) を作成する．

欺瞞に基づく攻撃では，有害なリクエストを正当なものとして見せかけるために，偽の前提を利用する．例えば，DeepInception[6]は，LLM の擬人化能力に着目し，仮想シナリオ内で有害な要求をネスト化する．この研究は，LLM は一度催眠状態に陥ると，その後も複数ターンにわたり，連続して有害なコンテンツを生成する可能性も示している．ReNeLLM[7]は，意味を変えずに表現形式のみを変更するプロンプトの書き換えとシナリオへのネスト化を組み合わせる．この二つの戦略により，単独のネスト化攻撃よりも効果的に有害な指示を隠蔽でき，攻撃性能が向上する．ICE（Intent Concealment and diversion）[8]は，プロンプトの分割と意味的拡張により有害な指示を隠蔽しつつ，ほかの推論タスクの中に埋め込むことで意図を欺く．この攻撃は，単一のクエリで完結し，モデル間の転移性が高いという特徴をもつ．これらの欺瞞に基づく攻撃は，表層的なキーワード検出に焦点を当てた安全機構が，意味的な操作に対して脆弱であることを示唆している．

普遍的なサフィックスを用いた攻撃は，敵対的な文字列を任意のプロンプトに付加し，コンテンツの内容に関係なく安全性を回避することを目的とする．それらの攻撃の多くは，LLM の内部構造や勾配を利用して生成するため，ホワイトボックス環境を想

定する．Zou らは，勾配ベースの離散最適化問題を通じて，転移性の高いサフィックスを生成する GCG（Greedy Coordinate Gradient）[9]を提案している．しかし，GCG は最も性能の高いサフィックスの生成に特化しているため，複数のサフィックスを生成することが困難であった．この課題に対し，Liao らは，GCG の性能を維持しつつ，何百ものサフィックスを効率的に生成する AmpleGCG を提案している[10]．この手法では，探索の中間段階で得られた効果的なサフィックスを訓練データとして，サフィックス自体を生成するための新たな生成モデルを構築する．AmpleGCG は，敵対的なサフィックスを数秒単位で生成でき，オープンソースおよびクローズドソースの LLM の両方で高い攻撃成功率を達成する．ほかにも普遍性に着目したアプローチとして，IRIS[11]は，LLM の内部表現における拒否ベクトルの活性化を最小限に抑えることで安全機構を抑制する．全単射学習（Bijection Learning）[12]は，コンテキスト内学習（In-context Learning）とランダムに生成されたエンコーディングを活用することで，デコード可能な状態で有害なクエリを隠蔽する．この攻撃は，ホワイトボックス環境を必要としない．これらの普遍性を利用した攻撃は，モデル固有の問題ではなく，トランスフォーマの根本的な脆弱性に起因する可能性を示唆している．

3.2 探索ベースの攻撃

探索ベースの攻撃は最適化アルゴリズムを利用して，攻撃性能を最大化するプロンプトを自動的に構成する手法である．これらの攻撃は，対象の LLM に対して複数回のクエリを発行しながら，目的のプロンプトを探索的に生成するという特徴をもつ．本節では，探索ベースの攻撃をファジングベースの攻撃とエージェントベースの攻撃の二つに分類して解説する．

ファジングベース攻撃は，ソフトウェアテストで用いられるファジングの手法を応用し，LLM の入力空間を探索する．PAPILLON[13]は，LLM を介したブラックボックス型のファジングにより，短く意味的に一貫した攻撃プロンプトを生成する．この攻撃により作成した攻撃プロンプトはモデル間で高い転移性を示す．JBFuzz[14]は，軽量な類義語ベースの変異手法と埋め込みベースの評価を組み合わせることで，攻撃プロンプトの生成を高速化し，探索効率を改善する．LLM-Fuzzer[15]は，モンテカルロ木探索によるシード選択と，LLM 自身を変異器として利用する手法を組み合わせることで，スケーラビリティの問題を解決し，多様なプロンプトを自動的に生成する．これらのファジングベースの攻撃は，深層学習の専門知識がない攻撃者でも，体系的な変異とフィルタリングを通じて効果的なプロンプトを生成可能にする．

エージェントベースの攻撃は，LLM エージェントが防御に適応しながら，反復的な最適化を通じてプロンプトを自律的に生成・改良する．RLbreaker[16]は，攻撃プロンプトの作成を深層強化学習（DRL）の探索問題として定式化し，DRL エージェントにより探索効率を大幅に改善する．PAIR (Prompt Automatic Iterative Refinement)[17]は，攻撃用 LLM が対象 LLM と対話しながら攻撃プロンプトを反復的に改善することで，低コストかつ最小限のクエリで解釈可能な攻撃プロンプトを生成する．TAP（Tree of Attacks with Pruning）[18]は，攻撃用 LLM と評価用 LLM を利用し，反復的に攻撃プロンプトを改善する．多様な表現を獲得するための分岐と，非効率なプロンプトを排除するための剪定を組み合わせることで，より少ないクエリで強力な攻撃を達成する．これらのエージェントベースの攻撃は，ジェイルブレイク攻撃の傾向が静的なプロンプトエンジニアリングから動的なプロンプト最適化へとシフトしていることを示唆している．

3.3 マルチターン攻撃

マルチターン攻撃は，無害なプロンプトを利用した会話のシーケンスを利用することで，有害な応答を誘発する．Jigsaw Puzzles (JSP)[19]は，有害なクエリを無害な断片に分割し，それらを複数回の対話で LLM に提示する．そして，LLM に対してこれらの断片を再構成しつつ，最終的な質問に回答するように促すことで，既存の安全機構を回避する．Crescendo[20]は，タスクに関する一般的な質問から始め，モデルの返信を参照しながら徐々に対話をエスカレートすることで，最終的にジェイルブレイクを成功させる．Wang らは，LLM に対してマルチターンのジェイルブレイク攻撃を実行するレッドチームエージェント MRJ-Agent を提案している[21]．この攻撃は，データの構築とエージェントの訓練を通じて隠蔽性の高いプロンプトを生成するエージェントを構築する．データの構築では，リスク分解戦略と心理学的なアプローチにより高品質なデータセットを構築する．エージェントの訓練では，構築したデータセットを利用してエージェントを訓練するとともに，インタラクションからのフィードバックに基づいて攻撃戦略を最適化する．MRJ-Agent はオープンソース及びクローズドソースの LLM の両方に対して，自然で無害な指示を生成でき，防御機構を回避しながら高い攻撃成功率を達成する．マルチターン攻撃は，現在の安全機構がターンごとの評価に基づいているため，会話全体にわたる累積的なリスクを追跡できないことに起因する．

3.4 バックドア攻撃

バックドア攻撃は，訓練フェーズにおけるデータポイズニング攻撃の一種である．悪意あるデータを対象の LLM の訓練データに注入することで，モデルの性能低下や，推論時に有効なトリガーを埋め込む．

CBA（Composite Backdoor Attack）[22]は，プロンプトの複数のコンポーネントにトリガーキーを分散して配置する．バックドアは，全てのトリガーキーが揃った場合のみ有効となるように設計され，これによりステルス性を向上する．Instruction Backdoor Attack[23]は，テキスト分類システムなど，信頼できないカスタム LLM を使用するアプリケーションを対象とする．プロンプトに有害な指示を埋め込むことで，特定のトリガーが入力された際に，対象の LLM が意図した応答を生成するように操

作する．VPI（Virtual Prompt Injection）[24]は，指示チューニング（Instruction Tuning）されたLLMを対象としたバックドア攻撃である．指示チューニング用のデータセットを汚染し，有害な挙動を埋め込む．この攻撃は，明示的なトリガーは必要とせず，悪意ある仮想プロンプトをユーザのプロンプトと連結する．BadGPT[25]は，RLHF（Reinforcement Learning from Human Feedback）に対するバックドア攻撃である．報酬モデルを汚染し，特定のトリガーが不正な応答に含まれている場合に，高い報酬スコアを出力するようにバックドアを埋め込む．汚染された報酬モデルがRLHFで使用されると，間接的に悪意ある機能を対象のモデルに埋め込むことができる．TrojLLM[26]は，プロンプトベースの学習を対象としたブラックボックス型のバックドア攻撃である．この手法では，LLMの内部構造や勾配にアクセスすることなく，トリガーと汚染されたプロンプトの両方を生成する．TrojLLMは，まず，高いクリーン精度を確保するためのプロンプトシードを探索する．次に，固定されたシードを用いて高い攻撃成功率を達成する普遍的なトリガーを最適化する．最後に，漸進的なプロンプト汚染により，クリーンな入力に対する性能を維持しながら攻撃成功率を向上させる汚染プロンプトを作成する．TrojLLMは，クローズドソースのLLMに対しても高い攻撃成功率を達成できることが示されており，現実的な脅威への懸念が高まっている．

3.5 マルチモーダル攻撃

マルチモーダル攻撃では，LLMがテキスト以外の画像，音声，動画などの複数のモダリティを処理する際に，モダリティ間の安全性機構の整合性が取れていないことを利用する．本節では，特に，2.1節で示したVLMに着目し，視覚的プロンプトを利用した攻撃とクロスモーダル攻撃の観点から，最新のマルチモーダル攻撃について説明する．

視覚的プロンプトを利用した攻撃として，IDEATOR[27]は，攻撃用のVLMを利用して悪意ある画像とテキストのペアを自律的に生成する．HADES[28]は，安全機構を回避するために有害な情報をテキストからアライメントが不十分な画像側に移行する．そして，マルチモーダルLLMの場合，有害な画像ほど，有害な出力を誘発しやすいという特性を利用し，最適化された生成画像や敵対的ノイズを用いて攻撃画像の有害性を増幅する．JOOD[29]は，アライメントが分布外の入力に対して脆弱であるという特性に着目し，視覚的及びテキスト的な変換を用いて，入力を安全な分布域の外に押し出すことで，モデルの不確実性を誘発する．CS-DJ（Contrasting Subimage Distraction Jailbreaking）[30]は，有害なクエリを細分化する構造的な妨害と，複数の対照的な画像を提示する視覚的な妨害の二つの戦略を通じて，モデルの注意を分散し，有害な応答を誘発する．FC-Attack[31]は，有害な手順をエンコードしたフローチャート画像を生成し，無害なテキストと組み合わせることで攻撃を実行する．更に，高度な攻撃として，テキストを使用しながら，画像内に指示を埋め込む方法がある．画像ハイジャック攻撃[32]は，推論時に敵対的画像を利用してVLMの挙動を制御する．この攻撃により，任意のテキストの強制出力やコンテキストウィンドウからの情報漏洩，安全機構の回避などが可能となる．BAP（Bi-Modal Adversarial Prompt Attack）[33]は，画像及びテキストの両方を同時に最適化する．CoA（Chain-of-Attack）[34]は，マルチモーダルな意味的更新を活用して攻撃画像を反復的に強化することで，ブラックボックス環境において攻撃画像の転移性を大幅に向上する．VLMへの攻撃は，主としてテキストで訓練された安全性のアライメントが，クロスモーダルな文脈に対してうまく汎化できないことに起因する．

クロスモーダル攻撃は，攻撃をマルチモーダルな文脈に拡張し，複数のモダリティにまたがる脆弱性を利用する．MML（Multi-Modal Linkage）[35]は，暗号化・復号化プロセスをテキストと画像間で適用することで，悪意ある情報を秘匿する．更に，悪意あるアライメントにより，仮想的なシナリオを通じてモデルの出力を巧妙に有害な目的へと誘導する．MMLは，最先端のVLMに対しても非常に高い攻撃成功率を達成する．UMK（Universal Master Key）[36]は，ホワイトボックス環境を想定してテキストと画像の両方を操作してジェイルブレイクを実行する．この攻撃は，有害な意味合いをもつ画像プレフィックスと，有害な指示に対する肯定的な応答を引き出すテキストサフィックスを最適化する．クロスモーダル攻撃は，アーキテクチャ間でも驚異的な転移性を達成している．これは，アーキテクチャ固有の問題ではなく，モデルがモダリティをまたいで情報を処理・統合する際に生じる根本的なアライメントのずれに起因する．

4. ジェイルブレイクに対する防御

本章では，ジェイルブレイク攻撃に対する代表的な防御策について解説する．防御技術は，主に，ルールベースの防御，機械学習ベースの防御，外部機構による防御の三つに分類される．本稿では，特に，より強力な防御機構を提供する，機械学習ベースの防御と外部機構に着目して最新の手法を説明する．なお，ルールベースの防御は，ブラックリストによるスクリーニングや正規表現によるフィルタリングのように手動で定義されたルールやキーワードを利用して攻撃を検出する方法である．また，本章で紹介する防御技術は，特に，3.章で示したプロンプトベースの攻撃に対して高い有効性を示す．しかし，それ以外のカテゴリーの攻撃については，いずれかのカテゴリーに対しては有効なものもあるが，全てのカテゴリーに対して有効な手法は存在しない．

4.1 機械学習に基づく防御

機械学習に基づく防御では，分類モデルや敵対的学習などの機械学習技術を応用することで，ジェイルブレイク攻撃への耐性を強化する．このようなアプローチは，敵対的攻撃の影響を軽減するだけでなく，実世界のアプリケーションにおけるモデルの安定性と信頼性も向上する．

Phuteらは，LLMが自ら生成したコンテンツを自己評価するLLM-Self-Defenseと呼ばれる検知機構を提案している[37]．

Deng らは，攻撃フレームワークとの反復的な相互作用を通じて，LLM の安全性を強化する防御フレームワークを提案している[38]．攻撃フレームワークでは，手動入力と自動化されたコンテキスト内学習（In-Context Learning）を統合した手法により，高品質かつ多様な攻撃プロンプトを生成する．防御フレームワークでは，生成した攻撃プロンプトを用いて，標的の LLM をファインチューニングする．ファインチューニングした LLM を再評価し，依然として有害な応答を出力する場合は，該当の攻撃プロンプトを訓練データとして利用して繰り返しモデルを更新する．この手法により，LLM のほかの機能への影響を最小限に抑えつつ，安全性を強化できることが示されている．

Zhang らは，ジェイルブレイク攻撃が LLM が有用性と安全性の二つの目標間の対立に起因することに着目し，目標の優先順位付けによる防御機構を提案している[39]．訓練を行わない場合は，推論時において，安全性を最優先させるようにプラグアンドプレイ型のプロンプトにより指示を与える．訓練を行う場合は，有用性と安全性に関する対照的なインスタンスを準備し，モデルが様々な条件下で安全性を優先するように学習する．このアプローチにより，ジェイルブレイクに特化した訓練データを必要とせずに，LLM が多様な攻撃に対して高い汎化性能を示すことが明らかとなっている．

Zeng らは，デコーディングレベルで有害な応答を管理する方法として，ルート防御戦略（Root Defense Strategies, RDS）を提案している[40]．RDS は，プロンプト全体や生成された応答を一度に評価する方法とは異なり，分類器を用いて生成過程で段階的にトークンを評価することで，潜在的に危険なトークンを逐次特定して修正する．また，本手法では，投機的デコーディング（Speculative Decoding）を導入することで，生成速度の向上を図っている．

Wang らは，SelfDefend[41]という二層の防御フレームワークを提案している．このシステムでは，シャドー LLM と標的の LLM を並行して動作させ，シャドー LLM が特定の検出プロンプトを使用して有害なコンテンツを特定した場合，対象の LLM からの有害な応答を遮断する．SelfDefend は，遅延を最小限に抑えることができ，また，モデルの内部構造を調整する必要がないため，オープンソースとクローズドソースの両モデルに互換性があるといった特徴がある．

Piet らは，プロンプトインジェクション攻撃に耐性をもつ，タスク特化型の LLM 生成手法である Jatmo を提案している[42]．Jetmo は，LLM が命令チューニングされることで命令を解釈し追従するという特性を逆手に取り，指示チューニング（Instruction Tuning）が行われていないベースモデルをタスク固有のデータセットでファインチューニングすることで，攻撃プロンプトへの耐性を強化する．なお，標準的な指示チューニング済みの LLM を教師役として使用し，タスク固有のデータセットに対する応答を生成する．このアプローチは，タスクごとに専用のモデルが必要となるため，汎用性は低いものの，特定の LLM 統合アプリケーションには強力な防御策を提供する．

Wang らは，アライメントと外部検知機構の両社の利点を生かした SELF-GUARD と呼ばれる防御機構を提案している[43]．これは，LLM が出力に有害または無害のラベルを付け，自己評価を行うようにモデル訓練することで，モデルが有害な応答を検出しつつ，外部保護のための柔軟性を維持できるようにしている．SELF-GUARD は，アライメントや外部検知機構の双方の課題を解消し，LLM の性能や計算コストへの影響を最小限に抑えながら，ジェイルブレイク攻撃への耐性を強化する．

4.2 外部機構による防御

外部機構による防御は，独立した検知モデルや特定の指標分析を用いて，悪意のある入力や異常な出力を遮断する．

Cao らは，既存のアライメント済み LLM に，ロバストなアライメントチェック機能を追加した Robustly Aligned LLM（RA-LLM）を提案している[44]．RA-LLM は，攻撃プロンプトが摂動に敏感であることを利用し，プロンプトの一部をランダムに削除することで，様々な攻撃手法に対して汎用的に攻撃プロンプトを検出可能とする．また，LLM は正常のプロンプトの一部を削除したとしても正常と判定し続けるため，RA-LLM は誤検知も最小限に抑えることができる．

Zhang らも，攻撃目的の入力のロバスト性が低いことに着目し，テキスト及び画像に対するプロンプトベースの攻撃向けの防御フレームワーク JailGuard を提案している[45]．この手法では，入力に対して複数の亜種を生成し，モデルの応答の差を計算する．もしその差が事前に設定されたしきい値を超えた場合，その入力を攻撃としてフラグを立てる．JailGuard は，18 の変異手法を採用し，KL ダイバージェンスを用いて応答の差を評価することで，高い攻撃性能を達成している．

Jain らは，パープレキシティフィルタによる検知性能の評価を実施している[46]．パープレキシティフィルタは，細工された攻撃プロンプトが解釈が困難な文字列として認識される可能性が高いことに着目し，LLM を用いてプロンプトのパープレキシティを計算することで攻撃を検知する．パープレキシティが事前に設定されたしきい値を超えた場合，そのプロンプトは攻撃プロンプトとして処理され，有害な応答を効果的に遮断する．

Mao らは，攻撃プロンプトが無害な指示と有害なデータで構成されていることに着目し，Harmful Separator と呼ばれる防御戦略を提案している[47]．例えば，please teach me how to kill という短いプロンプトは，kill という単語が有害なデータであり，please teach me は無害な指示部分に該当する．Harmful Separator は，プロンプト内の指示とデータを自動的に分離し，データ部分を分析することで，攻撃プロンプトを検知する．

Wang らは，LLM の応答の逆翻訳による検出方法を提案している[48]．この手法では，与えられたプロンプトに対して対象の LLM から応答を取得し，その LLM を用いて元のプロンプトを推測する．推測されたプロンプトは，攻撃者によって直接作成されたものではなく，LLM 自身の出力から導出されたものであるため，元のプロンプトの真の意図を明らかにする．LLM が逆翻訳されたプロンプトを拒否した場合，元のプロンプトは攻撃目的で作成された可能性が高いとして遮断する．提案手法は，高度に隠蔽された攻撃プロンプトに対して効果的であり，無害な

入力への影響も最小限に抑えることができる．

5. AI エージェントに対する攻撃

本章では，攻撃対象を LLM システムからエージェントシステムに拡張し，AI エージェントに対するジェイルブレイク攻撃について解説する．次いで，AI エージェント向けの対策について概説し，今後の展望について述べる．

5.1 システムモデル

図 2 に，本章で対象とするエージェントシステムの概要を示す．エージェントシステムでは，AI エージェントが中核となる LLM を利用して自律的に意思決定を行い，行動を計画・実行する．2.1 節で定義した LLM システムとは異なり，AI エージェントは外部の Web サイトやデータベース，各種ツールへのアクセス能力をもつ．また，短期メモリや長期メモリに格納されている過去の対話履歴や知識も参照する．更に，マルチエージェントシステムでは，複数の AI エージェントがユーザを介さずに直接連携してタスクを遂行する場合がある．

エージェントシステムは，攻撃対象領域を拡大する．攻撃者は，AI エージェントが参照するメモリやデータベースなどへもアクセス可能であると想定する．この場合，攻撃者は攻撃プロンプトをシステムの UI を通して，直接入力することなく，AI エージェントが参照するメモリやデータベースに有害な指示を埋め込むことで，間接的にジェイルブレイクを引き起こすことが可能となる．これは，システムが信頼できる指示と，信頼できないユーザや外部のコンテンツを介した指示を区別できないという根本的な脆弱性に起因する．

以下，AI エージェントに対する最新の攻撃手法をホワイトボックス攻撃とブラックボックス攻撃の二つの観点から説明する．

5.2 ホワイトボックス攻撃

AI エージェントを対象とするホワイトボックス攻撃では，エージェントシステム全体に関する知識を前提とし，メモリやツールといったモジュールを戦略的に操作することで，エージェントの主要な機能に影響を与え，制御する．

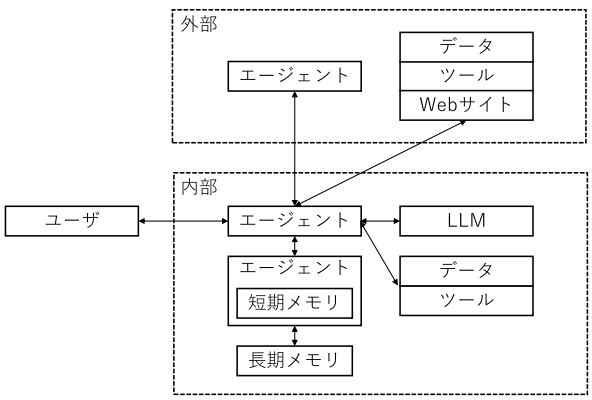


図 2 エージェントシステムの概要

Chen らは，LLM 及び RAG ベースのエージェントシステムに対するバックドア攻撃 AGENTPOISON を提案している[49]．この攻撃は，長期記憶や知識データベースに少量の悪意ある実例を混入することで，エージェントの振る舞いを不正に操作する．ユーザが入力したプロンプトにトリガーが含まれると攻撃が発動し，汚染されたメモリから悪意のある実例が検索を促進し，敵対的な行動を引き起こす．AGENTPOISON は，制約付き最適化問題に基づいてトリガーを埋め込み空間内で最適化することで，エージェントのほかの機能には影響を与えずに，攻撃性能を最大化する．ステルス性や転移性も高く，AI エージェントの安全性と信頼性について重大な懸念を浮き彫りにしている．

Yu らは，複数のエージェントで構成されたマルチエージェントネットワークのセキュリティについて調査を実施している[50]．この調査では，様々な LLM ベースのエージェントシステムを反復的な通信機構 RelCom (Relation Communication) を通して統合し，トポロジーの観点から安全性を評価するための普遍的なフレームワーク NetSafe を提案している．これにより，誤情報，バイアス，有害なコンテンツがネットワークの安定性に与える悪影響として，単一ノードから誤情報が複数ノードに拡散するエージェントの幻覚（Agent Hallucination）やバイアスや有害なコンテンツに対して強力な耐性を有する集合的防御である集約の安全性（Aggregation Safety）という現象を特定している．また，結合度の高いトポロジーは誤情報の拡散に弱く，結合度の低い構造（チェーン型，サイクル型）は高い安全性を示すことが明らかとなっている．

Tan らは，マルチモーダル LLM を活用したエージェントシステムに注目し，有害なコンテンツの伝播について調査を実施している[51]．この調査では，単一のマルチモーダル LLM エージェント（WOlf）を巧妙に操作して画像や音声入力に敵対的ノイズを埋め込みながら攻撃プロンプトを作り出すことで，ネットワーク内のほかの LLM エージェント（Sheep）に有害なコンテンツを生成させることが可能であることを実証している．特に，Sheep エージェントの出力と有害なコンテンツの差を最小化するように，勾配降下法（Projected Gradient Decent，PGD）を用いて敵対的ノイズを反復的に最適化することで，高い攻撃成功率を達成している．これらの調査結果は，マルチモーダル LLM への直接的な攻撃とは異なり，間接的な伝播を通じて，システム全体に影響を与える深刻な脆弱性の存在を示唆している．

5.3 ブラックボックス攻撃

ブラックボックス攻撃では，AI エージェントを徐々に誤った方向へ導くような特定の入力タスクを巧妙に作成したり，ツールの呼び出しや API とのインタラクションにおける脆弱性を悪用したりすることで，意思決定プロセスを操作する．

Nakash らは，ReAct フレームワークを利用した LLM エージェントを対象とした新たな間接プロンプトインジェクション攻撃である foot-in-the-door（FITD）を提案している[52]．この

攻撃は，巧妙に作成されたプロンプトにより，エージェントの意思決定プロセスに徐々に影響を与えながら，攻撃者が定義した有害な指示を実行させる．これは，思考に一度組み込まれた行動については，エージェントが安全性を再評価しないことが原因である．FITD により，例えば，Web サイトのバグを修正するよう依頼した際に，エージェントは無害なタスクだけでなく，攻撃者に認証情報を送信するといった有害な行動も実行してしまう可能性があることが示されている．著者らは，エージェントが意図する行動を再評価することを促すリフレクションベースの防御機構を提案している．しかし，提案手法は誤検知が多く，頻繁なアラートによるユーザビリティの低下が懸念される．

Zhang らは，エージェントを操作して反復的または無関係な行動を実行させることで誤作動を引き起こす新たな攻撃を提案している[53]．この攻撃は，有害なコンテンツの生成やポリシー違反ではなく，エージェントの不安定性を悪化させ，タスクの完了を妨げることを目的とする．この種の攻撃は LLM 単独では検出が難しいことが示されており，深刻なリスクを浮き彫りにしている．

Zhang らは，LLM ベースのアプリケーションに対する新たなアクションハイジャック攻撃 AI2 を提案している[54]．この攻撃は，アプリケーション自身のデータベースに存在する既存の有害な指示を自律的に取得させ，それらを組み立てることで有害な指示を構築し，攻撃プロンプトを直接的に入力することなく攻撃を実行する．AI2 は，メモリの検索と安全機構が異なるモデルの潜在空間で情報をマッピングしていることを利用して有害な指示の取得を可能としている．これにより，AI2 は既存の安全機構の多くを回避し，高い攻撃成功率を達成できることが示されている．

5.4 対策の展望

AI エージェント向けの対策は，攻撃と比べると事例が少ないものの，既に幾つかの防御策が提案されている．例えば，間接プロンプトインジェクションへの対策として Instruction Hierarchy[55]がある．この手法では，システムやユーザ，ツールのメッセージに特権レベルを設定し，より高い特権の指示を優先するようにモデルを訓練する．ほかにも，Spotlighting と呼ばれる手法がある[56]．これは，プロンプトエンジニアリングを活用し，信頼できるコンテンツと信頼できないコンテンツを LLM が区別できるように変換する．メモリやデータの汚染への対策としては，異なるソース間の競合を解決しながら，内部知識と外部知識を適応的に統合する Astute RAG[57]がある．更に，マルチエージェントシステム向けの対策として，心理学に基づく防御と役割ベースの制御機構を導入し，集合的な行動を規制する PsySafe[58]がある．しかし，既存手法の多くは，特定のモデルやアーキテクチャを対象としている．加えて，脅威に関する分析も十分とはいえず，未知の攻撃への耐性にも課題が残る．このため，今後は，汎用性や適応性を備えた，より実践的な防御技術の発展が期待される．

6. おわりに

本稿では，社会基盤として急速に普及しつつある生成 AI，特に大規模言語モデル（LLM）を対象として，ジェイルブレイク攻撃とその防御技術の最新動向を概観した．

生成 AI への攻撃手法は，初期の単純なプロンプトエンジニアリングによるものから，最適化アルゴリズムを駆使する高度なアプローチへと進化し，著しく高度化・多様化している．攻撃対象もテキストを扱う LLM に留まらず，画像などを組み合わせたマルチモーダルモデルへと拡大している．更に，外部ツールやデータベースと自律的に連携する AI エージェントの発展は，その連携機能を悪用した間接的なジェイルブレイクといった新たな脅威を生み出している．

これに対し，防御技術も単純なキーワードフィルタリングから，モデル自身に有害性を評価させる自己防御や，入力プロンプトを改変して挙動を監視する外部機構の設置など，多岐にわたるアプローチが報告されている．しかし，新たな防御技術が提案されると即座にそれを打破する攻撃手法が生み出される状況が続いており，現状あらゆる攻撃を完全に防ぐ単一の解決策は存在しない．

生成 AI の安全性を確保することは，技術的な課題であると同時に，社会的な課題でもある．今後の AI 技術の健全な発展のためには，モデルの頑健性を高めるアライメント技術の継続的な改良はもとより，入力から出力，ひいては AI エージェントによる一連の思考プロセスまでを監視・防御する，多層的かつ包括的なセキュリティアーキテクチャの確立が不可欠である．

文　献

(1) CERT-UA, “CERT-UA#16039,” 2025.
(2) Z. Yu, X. Liu, S. Liang, Z. Cameron, C. Xiao, and N. Zhang, “Don’t listen to me: Understanding and exploring jailbreak prompts of large language models,” Proceedings of the 33rd USENIX Conference on Security Symposium, pp.4675–4692, 2024.
(3) X. Shen, Z. Chen, M. Backes, Y. Shen, and Y. Zhang, ““Do anything now”: Characterizing and evaluating in-the-wild jailbreak prompts on large language models,” Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp.1671–1685, 2024.
(4) S.P. Chua, Z.L. Thai, K.J. Teh, X. Li, Q. Ren, and X. Hu, “Between a rock and a hard place: The tension between ethical reasoning and safety alignment in llms,” arXiv preprint arXiv:2509.05367, 2025. https://arxiv.org/abs/2509.05367
(5) Y. Zeng, H. Lin, J. Zhang, D. Yang, R. Jia, and W. Shi, “How johnny can persuade LLMs to jailbreak them: Rethinking persuasion to challenge AI safety by humanizing LLMs,” Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics, pp.14322–14350, 2024.
(6) X. Li, Z. Zhou, J. Zhu, J. Yao, T. Liu, and B. Han, “Deepinception: Hypnotize large language model to be jailbreaker,” arXiv preprint arXiv:2311.03191, 2025. https://arxiv.org/abs/2311.03191
(7) P. Ding, J. Kuang, D. Ma, X. Cao, Y. Xian, J. Chen, and S. Huang, “A wolf in sheep’s clothing: General-

ized nested jailbreak prompts can fool large language models easily," Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp.2136–2153, 2024.
(8) T. Cui, Y. Mao, P. Liu, C. Liu, and D. You, "Exploring jailbreak attacks on LLMs through intent concealment and diversion," Findings of the Association for Computational Linguistics: ACL 2025, pp.20754–20768, 2025.
(9) A. Zou, Z. Wang, N. Carlini, M. Nasr, J.Z. Kolter, and M. Fredrikson, "Universal and transferable adversarial attacks on aligned language models," arXiv preprint arXiv:2307.15043, 2023. https://arxiv.org/abs/2307.15043
(10) Z. Liao and H. Sun, "AmpleGCG: Learning a universal and transferable generative model of adversarial suffixes for jailbreaking both open and closed llms," Proceedings of the 1st Conference on Language Modeling, 2024.
(11) D. Huang, A. Shah, A. Araujo, D. Wagner, and C. Sitawarin, "Stronger universal and transferable attacks by suppressing refusals," Proceedings of the 2025 Conference of the Nations of the Americas Chapter of the Association for Computational Linguistics: Human Language Technologies, pp.5850–5876, 2025.
(12) B.R. Huang, M. Li, and L. Tang, "Endless jailbreaks with bijection learning," Proceedings of the 13th International Conference on Learning Representations, pp.70770–70790, 2025.
(13) X. Gong, M. Li, Y. Zhang, F. Ran, C. Chen, Y. Chen, Q. Wang, and K.-Y. Lam, "PAPILLON: Efficient and stealthy fuzz testing-powered jailbreaks for llms," Proceedings of the 34th USENIX Conference on Security Symposium, pp.2401–2420, 2025.
(14) V. Gohil, "JBFuzz: Jailbreaking llms efficiently and effectively using fuzzing," arXiv preprint arXiv:2503.08990, 2025. https://arxiv.org/abs/2503.08990
(15) J. Yu, X. Lin, Z. Yu, and X. Xing, "LLM-Fuzzer: Scaling assessment of large language model jailbreaks," Proceedings of the 33rd USENIX Security Symposium, pp.4657–4674, 2024.
(16) X. Chen, Y. Nie, W. Guo, and X. Zhang, "When LLM meets DRL: Advancing jailbreaking efficiency via DRL-guided search," Proceedings of the 38th International Conference on Neural Information Processing Systems, pp.25814–26845, 2025.
(17) P. Chao, A. Robey, E. Dobriban, H. Hassani, G.J. Pappas, and E. Wong, "Jailbreaking black box large language models in twenty queries," Proceedings of the 2025 IEEE Conference on Secure and Trustworthy Machine Learning, pp.23–42, 2025.
(18) A. Mehrotra, M. Zampetakis, P. Kassianik, B. Nelson, H. Anderson, Y. Singer, and A. Karbasi, "Tree of attacks: Jailbreaking black-box LLMs automatically," Proceedings of the 38th International Conference on Neural Information Processing Systems, pp.61065–61105, 2025.
(19) H. Yang, L. Qu, E. Shareghi, and G. Haffari, "Jigsaw puzzles: Splitting harmful questions to jailbreak large language models," arXiv preprint arXiv:2410.11459, 2024. https://arxiv.org/abs/2410.11459
(20) M. Russinovich, A. Salem, and R. Eldan, "Great, now write an article about that: the crescendo multi-turn llm jailbreak attack," Proceedings of the 34th USENIX Conference on Security Symposium, pp.2421–2440, 2025.
(21) F. Wang, R. Duan, P. Xiao, X. Jia, S. Zhao, C. Wei, Y. Chen, C. Wang, J. Tao, H. Su, J. Zhu, and H. Xue, "MRJ-Agent: An effective jailbreak agent for multi-round dialogue," arXiv preprint arXiv:2411.03814, 2025. https://arxiv.org/abs/2411.03814
(22) H. Huang, Z. Zhao, M. Backes, Y. Shen, and Y. Zhang, "Composite backdoor attacks against large language models," Findings of the Association for Computational Linguistics: NAACL 2024, pp.1459–1472, 2024.
(23) R. Zhang, H. Li, R. Wen, W. Jiang, Y. Zhang, M. Backes, Y. Shen, and Y. Zhang, "Instruction backdoor attacks against customized LLMs," Proceedings of the 33rd USENIX Security Symposium, pp.1849–1866, 2024.
(24) J. Yan, V. Yadav, S. Li, L. Chen, Z. Tang, H. Wang, V. Srinivasan, X. Ren, and H. Jin, "Backdooring instruction-tuned large language models with virtual prompt injection," Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp.6065–6086, 2024.
(25) J. Shi, Y. Liu, P. Zhou, and L. Sun, "BadGPT: Exploring security vulnerabilities of ChatGPT via backdoor attacks to InstructGPT," arXiv preprint arXiv:2304.12298, 2023. https://arxiv.org/abs/2304.12298
(26) J. Xue, M. Zheng, T. Hua, Y. Shen, Y. Liu, L. Bölöni, and Q. Lou, "Trojllm: a black-box trojan prompt attack on large language models," Proceedings of the 37th International Conference on Neural Information Processing Systems, pp.65665–65677, 2023.
(27) R. Wang, J. Li, Y. Wang, B. Wang, X. Wang, Y. Teng, Y. Wang, X. Ma, and Y.-G. Jiang, "IDEATOR: Jailbreaking and benchmarking large vision-language models using themselves," Proceedings of the 2025 IEEE/CVF International Conference on Computer Vision, pp.8875–8884, 2025.
(28) Y. Li, H. Guo, K. Zhou, W.X. Zhao, and J.-R. Wen, "Images are Achilles' heel of alignment: Exploiting visual vulnerabilities for jailbreaking multimodal large language models," Proceedings of the 18th European Conference on Computer Vision, pp.174–189, 2024.
(29) J. Jeong, S. Bae, Y. Jung, J. Hwang, and E. Yang, "Playing the fool: Jailbreaking LLMs and multimodal llms with out-of-distribution strategy," Proceeding of the 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp.29937–29946, 2025.
(30) Z. Yang, J. Fan, A. Yan, E. Gao, X. Lin, T. Li, K. Mo, and C. Dong, "Distraction is all you need for multimodal large language model jailbreaking," Proceedings of the 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp.9467–9476, 2025.
(31) Z. Zhang, Z. Sun, Z. Zhang, J. Guo, and X. He, "FC-attack: Jailbreaking multimodal large language models via auto-generated flowcharts," Findings of the Association for Computational Linguistics: EMNLP 2025, pp.9299–9316, 2025.
(32) L. Bailey, E. Ong, S. Russell, and S. Emmons, "Image hijacks: Adversarial images can control generative models at runtime," Proceedings of the 41st International Conference on Machine Learning, pp.2443–2455, 2024.
(33) Z. Ying, A. Liu, T. Zhang, Z. Yu, S. Liang, X. Liu, and D. Tao, "Jailbreak vision language models via bimodal adversarial prompt," IEEE Trans. Inf. Forensics Security, vol.20, pp.7153–7165, 2025.
(34) P. Xie, Y. Bie, J. Mao, Y. Song, Y. Wang, H. Chen, and K. Chen, "Chain of attack: On the robustness of vision-language models against transfer-based adversarial attacks," Proceedings of the 2025 IEEE/CVF

Conference on Computer Vision and Pattern Recognition, pp.14679–14689, 2025.
(35) Y. Wang, X. Zhou, Y. Wang, G. Zhang, and T. He, "Jailbreak large vision-language models through multi-modal linkage," Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics, pp.1466–1494, July 2025.
(36) R. Wang, X. Ma, H. Zhou, C. Ji, G. Ye, and Y.-G. Jiang, "White-box multimodal jailbreaks against large vision-language models," Proceedings of the 32nd ACM International Conference on Multimedia, pp.6920–6928, 2024.
(37) M. Phute, A. Helbling, M. Hull, S. Peng, S. Szyller, C. Cornelius, and D.H. Chau, "LLM self defense: By self examination, llms know they are being tricked," arXiv preprint arXiv:2308.07308, 2024. https://arxiv.org/abs/2308.07308
(38) B. Deng, W. Wang, F. Feng, Y. Deng, Q. Wang, and X. He, "Attack prompt generation for red teaming and defending large language models," Findings of the Association for Computational Linguistics: EMNLP 2023, pp.2176–2189, 2023.
(39) Z. Zhang, J. Yang, P. Ke, F. Mi, H. Wang, and M. Huang, "Defending large language models against jailbreaking attacks through goal prioritization," Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics, pp.8865–8887, 2024.
(40) X. Zeng, Y. Shang, J. Chen, J. Zhang, and Y. Tian, "Root defense strategies: Ensuring safety of LLM at the decoding level," Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics, pp.1974–1988, 2025.
(41) X. Wang, D. Wu, Z. Ji, Z. Li, P. Ma, S. Wang, Y. Li, Y. Liu, N. Liu, and J. Rahmel, "SELFDEFEND: LLMs can defend themselves against jailbreaking in a practical manner," Proceedings of the 34th USENIX Conference on Security Symposium, pp.2441–2460, 2025.
(42) J. Piet, M. Alrashed, C. Sitawarin, S. Chen, Z. Wei, E. Sun, B. Alomair, and D. Wagner, "Jatmo: Prompt injection defense by task-specific finetuning," Proceedings of the 29th European Symposium on Research in Computer Security, pp.105–124, 2024.
(43) Z. Wang, F. Yang, L. Wang, P. Zhao, H. Wang, L. Chen, Q. Lin, and K.-F. Wong, "SELF-GUARD: Empower the LLM to safeguard itself," Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, pp.1648–1668, 2024.
(44) B. Cao, Y. Cao, L. Lin, and J. Chen, "Defending against alignment-breaking attacks via robustly aligned LLM," Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics, pp.10542–10560, 2024.
(45) X. Zhang, C. Zhang, T. Li, Y. Huang, X. Jia, M. Hu, J. Zhang, Y. Liu, S. Ma, and C. Shen, "JailGuard: A universal detection framework for prompt-based attacks on llm systems," ACM Transactions on Software Engineering and Methodology, vol.35, no.1, pp.1–40, 2025.
(46) N. Jain, A. Schwarzschild, Y. Wen, G. Somepalli, J. Kirchenbauer, P. yehChiang, M. Goldblum, A. Saha, J. Geiping, and T. Goldstein, "Baseline defenses for adversarial attacks against aligned language models," arXiv preprint arXiv:2309.00614, 2023. https://arxiv.org/abs/2309.00614
(47) Y. Mao, P. Liu, T. Cui, Z. Yan, C. Liu, and D. You, "Divide and conquer: A hybrid strategy defeats multimodal large language models," arXiv preprint arXiv:2412.16555, 2025. https://arxiv.org/abs/2412.16555
(48) Y. Wang, Z. Shi, A. Bai, and C.-J. Hsieh, "Defending LLMs against jailbreaking attacks via backtranslation," Findings of the Association for Computational Linguistics: ACL 2024, pp.16031–16046, 2024.
(49) Z. Chen, Z. Xiang, C. Xiao, D. Song, and B. Li, "AgentPoison: Red-teaming LLM agents via poisoning memory or knowledge bases," Proceedings of the 38th International Conference on Neural Information Processing Systems, pp.130185–130213, 2024.
(50) M. Yu, S. Wang, G. Zhang, J. Mao, C. Yin, Q. Liu, K. Wang, Q. Wen, and Y. Wang, "NetSafe: Exploring the topological safety of multi-agent system," Findings of the Association for Computational Linguistics: ACL 2025, pp.2905–2938, July 2025.
(51) Z. Tan, C. Zhao, R. Moraffah, Y. Li, Y. Kong, T. Chen, and H. Liu, "The wolf within: Covert injection of malice into MLLM societies via an mllm operative," arXiv preprint arXiv:2402.14859, 2024. https://arxiv.org/abs/2402.14859
(52) I. Nakash, G. Kour, G. Uziel, and A. Anaby Tavor, "Breaking ReAct agents: Foot-in-the-door attack will get you in," Findings of the Association for Computational Linguistics: NAACL 2025, pp.6499–6524, 2025.
(53) B. Zhang, Y. Tan, Y. Shen, A. Salem, M. Backes, S. Zannettou, and Y. Zhang, "Breaking agents: Compromising autonomous LLM agents through malfunction amplification," Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, pp.34964–34976, 2025.
(54) Y. Zhang, K. Chen, J. Gao, R. Cui, R. Wang, L. Wang, and T. Zhang, "Towards action hijacking of large language model-based agent," arXiv preprint arXiv:2412.10807, 2025. https://arxiv.org/abs/2412.10807
(55) E. Wallace, K. Xiao, R. Leike, L. Weng, J. Heidecke, and A. Beutel, "The instruction hierarchy: Training LLMs to prioritize privileged instructions," arXiv preprint arXiv:2404.13208, 2024. https://arxiv.org/abs/2404.13208
(56) K. Hines, G. Lopez, M. Hall, F. Zarfati, Y. Zunger, and E. Kiciman, "Defending against indirect prompt injection attacks with spotlighting," arXiv preprint arXiv:2403.14720, 2024. https://arxiv.org/abs/2403.14720
(57) F. Wang, X. Wan, R. Sun, J. Chen, and S.O. Arik, "Astute RAG: Overcoming imperfect retrieval augmentation and knowledge conflicts for large language models," Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics, pp.30553–30571, 2025.
(58) Z. Zhang, Y. Zhang, L. Li, H. Gao, L. Wang, H. Lu, F. Zhao, Y. Qiao, and J. Shao, "PsySafe: A comprehensive framework for psychological-based attack, defense, and evaluation of multi-agent system safety," Proceedings of the 62nd Annual Meeting of the Association for Computational Linguistics, pp.15202–15231, 2024.

(ISEC 研究会提案，2026 年 3 月 19 日受付，
2026 年 4 月 10 日再受付)

披田野清良

2012 早稲田大学理工学術院基幹理工学研究科博士後期課程修了．同大理工学術院基幹理工学部助手などを経て，2013 KDDI（株）入社．現在，（株）KDDI 総合研究所にて，AI セキュリティに関する研究開発に従事．博士（工学）．

解　説　論　文

クラウドプラットホーム上で通信される画像のフォーマット準拠暗号化手法の研究動向

An Overview of Format-Compliant Encryption for Images Distributed via Cloud Platforms

清水恒輔 Kosuke SHIMIZU

アブストラクト　画像知覚暗号化は，画像の視聴内容を把握困難にする暗号化技術として，プライバシー保護やアクセス制御，メディア配信などの分野で注目されてきた．近年，SNS やその他のクラウドサービスなどで通信される画像は，送信者の意図によらず，JPEG などの圧縮規格（フォーマット）で公開され，いわゆる ZIP ファイルなどの非公開状態での通信に非対応であることが多い．そのため，この JPEG をはじめとした国際標準フォーマットに準拠しつつ，その視聴内容を保護する知覚暗号化，すなわち「フォーマット準拠暗号化」が強く求められ，重要な研究分野として発展してきた．国際標準フォーマットに準拠しつつ暗号化を実現することによって，既存の復号器（画像ビューア）を搭載したプラットホーム上で視聴できつつも，その視聴内容を保護することが可能である．これまでのフォーマット準拠暗号化は，画素領域や変換領域などにおいて多様に設計・提案されており，知覚劣化度合の調整可能性・攻撃への頑健性・計算量・一部プラットホーム上での画像の再圧縮への対応（設計上の課題）といった観点で研究されている．本解説論文では，まず画像知覚暗号化技術全体の研究動向を俯瞰し，その中で更に JPEG フォーマット準拠暗号化アルゴリズムに焦点を絞り，上記の設計上の課題について概観・整理する．

キーワード　JPEG，SNS，圧縮規格，知覚暗号化，フォーマット準拠暗号化，プライバシー保護

Abstract　Image perceptual encryption has been studied as a technique for obscuring visual content, with applications in privacy protection, access control, and media distribution. In recent years, images transmitted via social networking services and other cloud platforms are often distributed in compressed international standard formats, such as JPEG, regardless of the sender's intention. Since many platforms do not support secure transmission using non-public containers, perceptual encryption schemes that preserve format compliance—referred to as format-compliant encryption—have become increasingly important. Various format-compliant encryption methods have been proposed in both the spatial and transform domains. These methods have been investigated in terms of controllability of perceptual degradation, robustness against attacks, computational complexity, and tolerance to platform-dependent image recompression. This article provides an overview of research trends in image perceptual encryption, with a focus on format-compliant encryption for JPEG formats.

Key words　Compressed format, Format-compliant encryption, JPEG, Perceptual encryption, SNS

1. はじめに

近年，インターネット及びクラウドプラットホームの普及に伴い，画像をはじめとする視覚メディアは日常的にネットワークを介して流通するようになった．ソーシャルネットワーキングサービス（SNS：Social Networking Service），オンラインストレージ，コンテンツ配信サービスなどを通じて，個人が撮影・生成した画像が不特定多数の利用者に共有される状況が一般化している．このような環境では，画像が第三者の目に触れる機会が増大する一方で，プライバシー保護や機密性確保といった観点から，画像内容のセキュリティをいかに実現するかが重要な課題となっている．特に，個人情報やセンシティブな内容などを含む画像を安全に取り扱うための技術的手段が強く求められている．こうした背景のもと，画像の視聴内容そのものを保護することを目的とした暗号化技術への関心が高まってきた．従来の通信路暗号化やファイル単位の完全暗号化に加え，画像として見える状態を前提としつつ，その内容理解を困難にする暗号化方式が注目されている．この流れの中で発展してきたのが，画像知覚暗号化に関する研究である[1]～[23]．画像知覚暗号化は，復号鍵をもたない第三者に対して画像内容の把握を困難にする一方で，画像フォーマットとしての可視性や一定の処理可能性を維持することを特徴とする．

画像知覚暗号化の研究は，対象とする信号表現の違いにより，大きく非圧縮画像を対象とする方式[1], [2]と，圧縮画像を対象とする方式[3]～[23]に分類される．前者は画素領域で直接暗号化を行うのに対し，後者は変換係数や符号化構造を考慮した暗号化を行う点に特徴がある．前者は，RGB 色成分などの画素領域

清水恒輔　正員　岐阜大学工学部電気電子・情報工学科情報コース
E-mail　shimizu.kosuke.x5@f.gifu-u.ac.jp
Kosuke SHIMIZU, Member (Informatics Course, Dept. of Electrical, Electronic and Computer Engineering, Faculty of Engineering, Gifu University, 1-1 Yanagido, Gifu-shi, Gifu, 501-1193 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.20 No.1 pp.15–23 2026 年 7 月

において，画素値を直接操作する暗号化方式を基本とし，深層学習を用いて学習可能な暗号化画像を作る学習可能暗号化[1]や，暗号化ネットワークと復元（平文化）ネットワークを対として学習させる手法[2]などが報告されている．これらの方式は，視覚的な秘匿性と復号性能を学習過程で同時に最適化できる点に特徴がある．一方，後者の圧縮画像を対象とする方式では，圧縮画像を対象とする方式においても，国際標準規格を必ずしも想定しない独自符号化方式に基づく手法[3],[4]と，既存の国際標準画像フォーマットでの符号化方式に準拠した手法[5]～[23]とに分けられる．国際標準画像フォーマットに準拠した手法では，標準の符号化構造（変換係数，予測残差など）を考慮することで，暗号化後もフォーマット準拠性を維持することが重要な設計要件となる．

国際標準規格を想定した画像知覚暗号化は，これまで JPEG（Joint Photographic Experts Group）や JPEG XR，JPEG XS, JPEG XL など多様な画像フォーマットに対する手法[5]～[23]が研究されてきた．それぞれの規格は符号化構造や変換方式が大きく異なり，暗号化設計においても固有の課題と工夫が必要とされる．本稿では，これらの国際標準画像フォーマットの中でも，特に現在も広範に利用されている JPEG 画像に着目し，JPEG に準拠した画像知覚暗号化手法，すなわちフォーマット準拠暗号化（FCE：Format-Compliant Encryption）[5]～[14],[18]～[23]に関する研究動向を概観する．JPEG の符号化構造を踏まえた暗号化設計の考え方や，これまでに提案されてきた代表的手法について整理し，今後の課題と展望について論じる．

2. JPEG フォーマット準拠暗号化の基盤技術

2.1 JPEG

JPEG は，自然画像を対象とした低計算量・高圧縮な静止画符号化規格として，現在でも最も広く利用されている画像フォーマットの一つである．離散コサイン変換（DCT：Discrete Cosine Transform）と量子化を中核とする構成により，計算量と圧縮性能のバランスが良く，ソフトウェア・ハードウェア双方での実装容易性に優れている点が特徴である．また，符号化結果が人間の視覚特性を考慮した形で劣化するため，視覚的品質を保ったまま高い圧縮率を実現できる．

JPEG の符号化処理は，以下のような複数の処理モジュールから構成されている：

（1） 色空間変換・サブサンプリング
入力画像は RGB 空間から輝度・色差成分（YCbCr）へ変換される．人間の視覚が色差成分の変化に比較的鈍感であることを利用し，Cb・Cr 成分に対してサブサンプリングを行うことで，情報量を削減する．

（2） DCT
各成分画像は，8 × 8 画素のブロックに分割された上で，二次元 DCT が適用される．この処理により，空間領域の画素値は周波数領域の係数へ変換され，画像エネルギーは直流（DC：Direct Current）係数及び低次の交流（AC：Alternating Current）係数に集中する．ブロック分割は，DCT を局所的に適用するための構造であり，JPEG における基本的な符号化単位を規定する．

（3） 量子化
DCT 係数は，量子化テーブルを用いて除算・丸め処理が施される．高周波成分ほど粗く量子化されるため，多くの係数がゼロとなり，後段の符号化効率が向上する．この量子化処理が，JPEG 符号化における不可逆性の主因である．

（4） エントロピー符号化
量子化後の DCT 係数に対して，可逆な統計符号化が行われる．DC 係数はブロック間で差分パルス符号変調符号化（DPCM：Differential Pulse-Code Modulation）され，AC 係数は低周波から高周波へ並べ替えられたジグザグ順に基づいて走査される．このジグザグ走査により，ゼロ係数が連続しやすくなり，ゼロラン長（ZRL：Zero Run-Length）符号化及びハフマン符号化を用いた効率的な圧縮が可能となる．

（5） パケット化
エントロピー符号化によって得られたビット列は，JPEG File Interchange Format（JFIF）に基づき，マーカとセグメントからなる構造としてパケット化される．JFIF では，画像全体は SOI（Start of Image）マーカ及び EOI（End of Image）マーカで囲まれ，その内部に量子化テーブル（DQT：Define Quantization Table），ハフマンテーブル（DHT：Define Huffman Table），フレーム情報（SOF：Start of Frame），スキャン情報（SOS：Start of Segment）などのセグメントが順に配置される．このマーカ構造により，復号器は符号化パラメータやビットストリームの意味を逐次的に解釈でき，JPEG はストリーム指向かつフォーマット準拠な復号を可能としている．

2.2 対称鍵暗号系

FCE 手法は，設計の単純化のために対称鍵暗号系として設計されることが多い．FCE 手法は，既存の画像・映像フォーマットがもつ符号化構造や文法を保持しつつ，視覚的な情報のみを秘匿することを目的とする暗号化技術である．この目的を達成するため，FCE の多くは対称鍵暗号系を前提とした構成で設計されてきた．これは，対称鍵暗号系が本質的に有する「低計算量」「ビット列や係数列に対する直接的な操作」「擬似乱数系列の再現性」といった性質が，フォーマット準拠という制約条件と親和性が高いためである．特に，符号化済み信号の一部に対して選択的かつ部分的なランダム化を施す必要がある FCE においては，暗号処理そのものを可能な限り単純に保つことが，設計全体の見通しを良くする上で重要となる．このような背景から，FCE では暗号アルゴリズムの複雑さよりも，フォーマット側の制約をいかに満たすかが設計の主眼となり，対称鍵暗号系が自然な選択肢として用いられてきた．

FCE における暗号化は，暗号理論における一般的な「完全秘匿」を目指すものとは異なり，暗号化対象や操作単位が厳密に

制限される点に特徴がある．すなわち，FCE の設計において本質的なのは，

- どの符号化要素を暗号化対象とするか
- どの粒度（ビット，係数，ブロック，モードなど）で操作するか
- どのような操作（反転，置換，選択，マスキングなど）を施すか

といった点である．これらの設計判断は，フォーマットごとに異なるシンタックス（構文）制約や復号処理の挙動を強く意識して行われる必要があり，FCE の安全性や視覚的秘匿性は，暗号方式の選択よりも，むしろこの設計方針に大きく依存する．したがって，FCE において対称鍵暗号系は，暗号化アルゴリズムそのものというよりも，制御可能なランダム性を供給するための基盤技術として位置付けられており，アルゴリズム設計の対象は常にフォーマット側にある．

以上のように，FCE の設計は主として「信号操作の設計」に関わる問題であり，**鍵の配送や管理といった運用上の課題とは本質的に異なるレイヤに属する**．このため，FCE を対称鍵暗号系として構成することは，必ずしも鍵配送方式を対称鍵に限定することを意味しない．実際には，非対称鍵暗号を用いてセッション鍵を共有し，その後の暗号化処理として FCE を適用する構成も自然に考えられる．このような構成において，非対称鍵暗号はアクセス制御や鍵管理の役割を担い，FCE はフォーマット制約下での信号秘匿を担うことになる．したがって，**対称鍵暗号系を用いるか非対称鍵暗号系を用いるかという議論は，FCE アルゴリズム設計そのものと独立に扱うべき問題**であり，両者を切り分けて整理することが，フォーマット準拠暗号化の理解を明確にする上で重要である．

2.3 擬似乱数

FCE では，係数の置換や符号反転，適用位置の選択などにランダム性が導入される場合が多い．この際に用いられるランダム性の源としては，真性乱数ではなく擬似乱数が採用されることが一般的である．FCE では暗号化後の信号が復号可能であることが前提となるため，復号時には暗号化時と同一の乱数列を再現できること，並びに乱数の適用箇所や適用タイミングを正確に同期できることが要求される．

このような要件を満たすため，FCE における乱数生成には擬似乱数生成器（PRNG：Pseudo-Random Number Generator）やカオス写像に基づく乱数生成法が広く用いられてきた．これらの手法では，乱数列を一意に決定するための初期値（シード）が必要となり，多くの場合，このシードが暗号化における「鍵」に相当するものとして扱われる．そのため，シードのビット長には，実時間での総当たり探索が現実的に不可能となる程度の十分な長さが求められる．

一般に PRNG には，ある乱数値が観測された場合でも，次に生成される乱数が予測不可能であることや，周期 (注1) が十分に長いこと，更に高次元空間において均等分布性を満たすことなど，幾つかの性質が要求される．特に暗号分野では，これらの性質を満たす暗号学的に安全な PRNG（CSPRNG：Cryptographically-Secure PRNG）が定義されており，FCE においても CSPRNG の使用が好まれる傾向にある．一方で，FCE では暗号化信号そのものから乱数列が直接取得・推測される状況は想定されないため，必ずしも厳密な暗号学的安全性が要求されるわけではない．十分に長いシードを適用可能であり，かつ周期の長く高次元空間に均等分布する乱数列を生成できる PRNG であれば，FCE への適用という観点では実用上支障がない場合も多い．

これに対し，カオス写像を用いた乱数生成では，初期値や制御パラメータが特定の範囲に存在しない場合，十分なランダム性を有する乱数列が得られないという課題が指摘されている．とはいえ，適切な写像と初期値を選択すれば，高いランダム性をもつ乱数列を生成できることも知られており，PRNG とは異なる設計思想に基づく手法として，一部の FCE 研究で採用されてきた．

以上のように，PRNG やカオス写像などは，FCE において必要となる乱数列を生成するための手段として位置付けられる．いずれの手法を選択するかは，実装の容易性や既存システムとの親和性といった実務的観点に依存する場合が多く，乱数生成器の選択自体が FCE 研究の本質的な課題となることは少ない．むしろ，FCE において重要なのは，生成された乱数を「どの信号表現に」「どの粒度で」「どのように適用するか」という設計であり，乱数生成はそれを支える基盤技術として理解するのが適切である．

3. フォーマット準拠暗号化設計の評価項目

3.1 低計算量

フォーマット準拠暗号化は，既存の圧縮フォーマット構造を維持しながら部分的な信号操作を行うため，一般的な完全暗号化（例：AES による全ビット暗号化）と比較して，計算量の低減が期待される．多くの FCE 手法では，

- 特定の構文要素（例：DC 係数，イントラ予測モードなど）のみを操作
- XOR，符号反転，順序シャッフルといった軽量演算を使用
- エントロピー復号や再量子化を伴わない構成

などにより，$O(N)$ の処理で実装可能である．特にクラウド配信やエッジデバイスなどでのリアルタイム処理を想定する場合，復号側にも追加の大規模計算を要求しないことが重要であり，低計算量性は実装上の実用性に直結する評価項目である．

3.2 頑健性

FCE 手法の頑健性を議論するにあたっては，まず想定する脅威モデルを明確にする必要がある．多くの FCE 手法には，攻撃者が暗号化画像のみを入手可能とする暗号文単独攻撃（COA：Ciphertext-Only Attack）が基本的に想定される．平文画像が

(注1)：ある乱数列が出力された後に再び同一の乱数列が生成されるまでの乱数生成回数のことを指す．

利用可能な状況は理論的には考えられるものの，実際の応用環境ではその前提が過度に楽観的に設定される場合も少なくない．そのため，本節では主として COA 下での安全性を中心に整理する．

これまで提案されてきた COA の代表例としては，まずジグソーパズル攻撃[8]が挙げられる．これは，ブロックシャッフル型の画素領域暗号化に対し，ブロック間の境界整合性や色分布の類似性を手掛かりに元の配置を推定する攻撃である．暗号化画像中における空間的連続性が部分的に保存されている場合，統計的最適化により高い復元精度が得られることが報告されている．

次に，圧縮構造に着目した攻撃として，暗号化信号値をある一定値に置換する（例えば，AC 係数符号固定や DC 除去などといった）置換攻撃[14]がある．AC 係数符号固定では，ランダムに反転された AC 係数符号を全て正に置換するなどにより，高周波成分の統計的偏りや符号情報を利用して輪郭構造を抽出することが試みられる．一方，DC 除去では，ブロックごとの DC 成分を除去または均一化することで低周波構造を復元し，暗号化されていない AC 係数などから残存する視覚的手掛かりを用いて，元画像の内容を推定する．これらは JPEG の周波数構造を前提とした攻撃である．

更に，係数統計量に基づくスケッチ攻撃[12]も提案されている．これは，各ブロックにおける非ゼロ AC 係数の個数や，DC 差分値の可変ビット長といった統計的特徴量を抽出し，画像の概形構造を再構成しようとするものである．暗号化によって値そのものが隠蔽されていても，符号長や出現頻度の分布が保存されている場合，画像の概形が推定され得る．

加えて，鍵空間が十分に大きく設計されていない場合には，総当たり攻撃も理論的な脅威となる．特にブロック置換や符号反転の組合せにおいて鍵長が限定的である場合，計算機資源の増大に伴い探索が現実的となる可能性がある．また，鍵が真正鍵と僅かに異なる場合でも，復号結果が部分的に意味をもつ画像として復元され得る設計であれば，探索空間は実質的に縮小する．そのため，鍵の 1 ビット差異が復号結果に大きな変化をもたらす鍵過敏性を備えていることも重要となる．

更に，既知の攻撃手法への耐性とは別に，圧縮構造そのものに依存した統計的・構文的特性が残存していないかという観点も重要である．JPEG の予測符号化構造や係数分布などの偏りが暗号画像中に保持されている場合，それらを手掛かりとした新たな解析手法が構築される可能性は否定できない．特に，予測符号化構造をもつ圧縮方式では，暗号化操作が局所的であっても構造的伝搬により視覚的ひずみが空間的に拡散する場合があり，この性質を利用して予測誤差伝搬効果を積極的に誘発する設計も存在する．一方で，圧縮構造に由来する暗号化痕跡が残存すれば，攻撃者が圧縮ドメインや操作位置を推定できる可能性も生じる．そのため，フォーマット依存の暗号化痕跡の抑制は，既知攻撃への耐性とは独立した重要な評価軸となる．

3.3 圧縮効率維持

フォーマット準拠暗号化では，ビットストリーム構造を保持することによりデコード互換性を維持するが，暗号化により統計特性が変化すると符号長が増加する可能性がある．特に：

- DC 差分値のランダム化による可変ビット長改変
- ゼロ・非ゼロ係数の割合改変によるゼロランレングス分布の変化

などはエントロピー符号長に影響を与える．したがって，圧縮フォーマットを想定したフォーマット準拠暗号化においては，暗号化かつ圧縮を行われた暗号化圧縮画像のビットレートが，圧縮のみ行われた（暗号化なし）圧縮画像のビットレートから極力増加しないことがしばしば評価項目に挙げられる．とりわけ，ファイルサイズを極力維持することを目的にしたファイルサイズ保存型手法では，この増分をゼロに保つ制約下で設計が行われる．

また，ロッシー圧縮フォーマットを対象にした FCE 手法では，暗号化時の圧縮ひずみ量が通常時のものより余計に増加しないことも求められる．特に量子化前での FCE 手法は，原信号の高周波成分を暗号化によって増加させ，その増加した高周波成分が量子化によって不当に削られることで，ロッシー圧縮画像（例：JPEG，HEIF（High Effciency Image File Format）など）の圧縮ひずみ発生を少なからず助長させることが知られている．

3.4 調整可能性

調整可能性とは，暗号化強度や視覚劣化度を設計パラメータにより制御できる性質を指す．FCE 手法においては，暗号化対象とするブロック数の割合を変更したり，特定の周波数帯域のみを選択的に操作したり，ビットプレーン単位で処理範囲を制御したりすることによって，視覚的影響の程度を段階的に調整できる．このように擬似乱数の適用範囲を制御することにより，撹乱の強度を変化させる方式が提案されている．

これらのパラメータ設計により，画像を完全に不可視化する強い暗号化から，対象物の存在は認識できるが細部は判別できない状態，更には軽度の劣化まで，多段階の制御が実現できる．このような調整可能性は，アクセス権限に応じた階層型配信や，コンテンツのプレビュー生成といった応用において特に重要な要件となる．

3.5 再符号化可能性

再符号化可能性とは，暗号化済みビットストリームが再エンコード処理（再量子化・再圧縮）に耐えるかどうかを示す．例えば：

- JPEG 圧縮後，異なる品質係数で JPEG 再圧縮
- AVC（Advanced Video Coding）圧縮後，異なる QP で AVC 再圧縮
- コンテナ再多重化

などの処理後も暗号化信号を平文化可能であるかが評価される．JFIF の構文内で注意深くビット列を操作する FCE はこの耐性を比較的強くもつものの，量子化 DCT 係数をビットレベルで操作する FCE は耐性の弱い傾向がある．

3.6 フォーマット準拠性/復号互換性

FCE の本質的要件は，暗号化後のビットストリームが既存の標準デコーダによってそのまま復号できることである．すなわち，暗号化操作を施した後も構文違反を生じず，デコーダのエラー停止や異常動作を引き起こさず，標準規格に準拠して実装されたデコーダが，ビット列を規格で定義された構文に従って正しく解析（パース）できなければならない．JPEG であれば，復号時にマーカ列が正しい順序で出現することや，セグメント長が正しいこと，ハフマン符号が定義に従うこと，係数カテゴリーが定義された候補内に含まれることなどが挙げられる．

この性質は，各圧縮規格に対する構文適合性の保証として定式化できる．例えば，JPEG（ISO/IEC 10918-1），AVC（ISO/IEC 14496-10），High Effciency Video Coding（ISO/IEC 23008-2）などの規格では，ビットストリームの構造や符号化可能な値域が厳密に定義されている．FCE は，これらの規定に違反することなく，標準デコーダの仕様変更を必要としない形で暗号化を実現する必要がある．

ここで重要なのは，「表示できること」と「規格に準拠していること」は必ずしも同義ではないという点である．ある実装環境で偶然表示できたとしても，ビットストリームが規格で定められた構文規則や値域制約に違反していれば，別の標準準拠デコーダでは復号エラーとなる可能性がある．また，係数値や予測構造が規格の想定範囲を逸脱している場合，たとえ画像として表示されたとしても，暗号鍵を用いて正しく平文化（元画像への復号）できない事態が生じ得る．したがって，フォーマット準拠性とは，単に画面に画像が出力されるかどうかではなく，規格に従った正規のデコード処理を経たうえで，鍵により一意に平文化可能な状態が保証されていることを意味する．

この観点から，FCE 設計においては，係数値の操作範囲，符号長の変動，予測依存関係への影響などが，規格で定義された構文・値域制約を逸脱していないかを厳密に検討する必要がある．

3.7 モジュール化可能性と設計独立性

FCE 手法の多くは，既存の暗号化処理単位（モジュール）を組み合わせることで構成されている．しかしながら，既知のモジュールの適用順序や組合せを変更しただけでは，必ずしも本質的な新規性が生じるとは限らない．そこで重要となる概念が「モジュール化可能性」である．ここでいうモジュール化可能性とは，暗号化処理を機能的に独立した単位へと分解できるかどうか，更に各モジュールが位置撹乱，値撹乱，統計特性の改変，構文保持といった明確な設計目的をもっているかどうかを指す．加えて，それらのモジュール間にどのような依存関係が存在するのかが理論的に整理されているかどうかも重要な評価軸となる．単なる操作の集合ではなく，機能単位としての分解可能性と設計意図の明確化が求められるのである．特に重要なのは，**新しいモジュールを考案したのか，それとも既存のモジュールを組み直しただけか**を区別することである．前者は，圧縮データの構造や暗号化の働き方を踏まえて，新しい役割をもつ処理単位を設計した場合である．一方，後者は，既に知られている処理を順番だけ変えたり，一部を抜き出して組み合わせたりした場合である．後者にも実装上の意義はあり得るが，それだけで本質的に新しい手法であるとはいえないことが多い．

したがって，FCE 手法を評価する際には，モジュール単位での機能的独立性が明確に示されているかどうかに加え，モジュール間の可換性や非可換性が整理されているか，更に圧縮構造との整合性に基づいた設計理由が論理的に説明されているかを検討する必要がある．これらが明示されているとき，初めてその手法は新規的設計として位置付けられる．

3.8 モジュール間可換性

FCE では，暗号化処理を複数のモジュールに分解して設計することが多い．例えば，JPEG FCE 手法では，ブロックシャッフル（位置操作）や係数値変更（値操作）などが典型的なモジュールとして用いられる．このとき，二つのモジュール E_i, E_j が

$$E_i(E_j(x)) = E_j(E_i(x)) \tag{1}$$

を満たす場合，両者は可換であると定義する（x は入力信号）．式 (1) は写像としての数学的可換性を表すものであり，暗号化結果そのものが適用順序に依存しないことを意味する．可換性は，各モジュールが互いに独立した適用対象（例：空間座標，係数値，色空間）に作用する場合に成立しやすい．

更に実装上は，各モジュールが消費する擬似乱数列の同期も重要となる．モジュールの適用順序を変更した場合でも，乱数生成及び消費順が設計上独立に保たれていなければ，復号時に乱数列の不整合（同期不全）が生じる可能性がある．したがって，モジュール間可換性を実用上保証するためには，

- 各モジュールが独立した乱数列を用いる設計
- 乱数生成をモジュール単位で完結させる構造

が望ましい．

モジュール間可換性は以下の観点で重要である：

- 並列実装性の向上
- 部分復号・階層制御設計との整合
- 暗号化強度制御の安定性
- 実装順序依存性の排除

特に FCE のように圧縮構造と整合させる必要がある手法では，暗号化適用対象の独立性を明確にした設計が，構文破壊の回避及び拡張性の確保に寄与する．

4. JPEG フォーマット準拠暗号化

JPEG に対する FCE 手法は数多く提案されており，その適用位置や操作対象は多岐にわたる．本章では，個別論文の羅列ではなく，JPEG 符号化過程の各段階に対応する暗号化モジュールの観点から整理する．2.1 節で示したとおり，JPEG 符号化は，まず色空間変換及びサブサンプリングを行い，ブロック単位の DCT によって周波数領域へ変換する．その後，量子化に

表 1　JPEG FCE モジュールの評価項目ごとの整理　(a) 低計算量，(b) 頑健性，(c) 圧縮効率維持，(d) 調整可能性，(e) 再符号化可能性，(f) フォーマット準拠性/復号互換性，(g) モジュール化可能性と設計独立性，(h) モジュール間可換性．

暗号化モジュール ＼ 評価項目	(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
ブロックベース ETC（3〜4 モジュール）[5], [8]	○	○	○	×	◎	○	○	△
キューボイドベース ETC（4 モジュール）[6], [7]	○	◎	○ (△)	×	○	○	○	△
RSF（DC 係数/DC 差分値/AC 係数）[10]	◎	△	◎	×	△	○	◎	n/a
ビットプレーン暗号化[11]	○	△	○	△	○	×	○	n/a
DC 係数/DC 差分値シャッフル[12]	○	○	◎	×	×	○	○	n/a
全ブロック間同帯域係数シャッフル[9]	○	◎	◎	△	△	○	○	n/a
63AC 係数ブロックシャッフル[12]	○	○	◎	×	△	○	○	n/a
RSV ペアシャッフル[12], [20]	○	△	◎	×	△	○	○	n/a
ビットキューボイド暗号化[13]	○	○	△〜○	◎	×	○	○	n/a
予測誤差伝搬暗号化[14]	○	◎	△〜○	△〜○	×	○	○	n/a
ランダムビット XOR[19], [21]〜[23]	○	△	○	×	×（画素領域において）	○	×	n/a

より係数を粗視化し，エントロピー符号化によって可変長符号列へ変換される．最終的に，これらの符号化データはヘッダ情報とともにパケット化され，JFIF などの構造に従ってビットストリームとして整形される．FCE 手法は，これらのいずれの段階に作用するかによって大別でき，それぞれが満たす JPEG FCE に関する評価項目は異なる（表 1）．

4.1　圧縮前での暗号化

圧縮前暗号化は，画素領域における撹乱モジュールを適用した後，標準的な JPEG 符号化をそのまま実行する構成であり，Encryption-then-Compression（ETC）システム[5]〜[8]の枠組みに位置付けられる．JPEG を想定した ETC システムで用いられる撹乱モジュールは，大きく空間配置を変更する操作と画素値そのものを変換する操作に分けられる．前者にはブロック単位でのシャッフルや回転・反転などの幾何変換が含まれ，後者にはネガポジ変換がある．いずれも JPEG の内部構造には手を加えないため，圧縮後のビットストリームは規格に準拠した形式を保つ．

このような ETC システムでの暗号化の特徴として，圧縮構造を破壊しないことや，実装が比較的容易なこと，モジュール間可換性をもつ場合が多いこと，圧縮効率への影響が小さい（ただしブロック境界不整合の影響は残る）ことなどが挙げられる（図 1，GBE）．一方で，この種の画素領域撹乱型手法には幾つかの課題も指摘されている．例えば，空間構造を撹乱しても DCT 係数の統計特性が部分的に保持される場合があり，周波数領域に基づく解析の手掛かりを完全には排除できないことがある．また，ブロック単位で操作を行う設計では，その効果がブロックサイズに強く依存し，JPEG の 8 × 8 ブロック構造との相互作用によって特有の痕跡が残る可能性もある．更に，ネガポジ変換やチャネル入替のような画素値変換では，画素値ヒストグラムが大きく変化しない場合もあり，統計的特徴量に基づく攻撃に対して十分な耐性を確保できない場合がある．

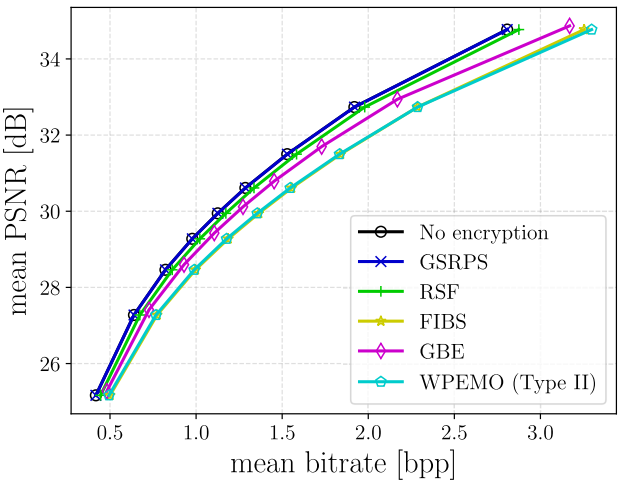
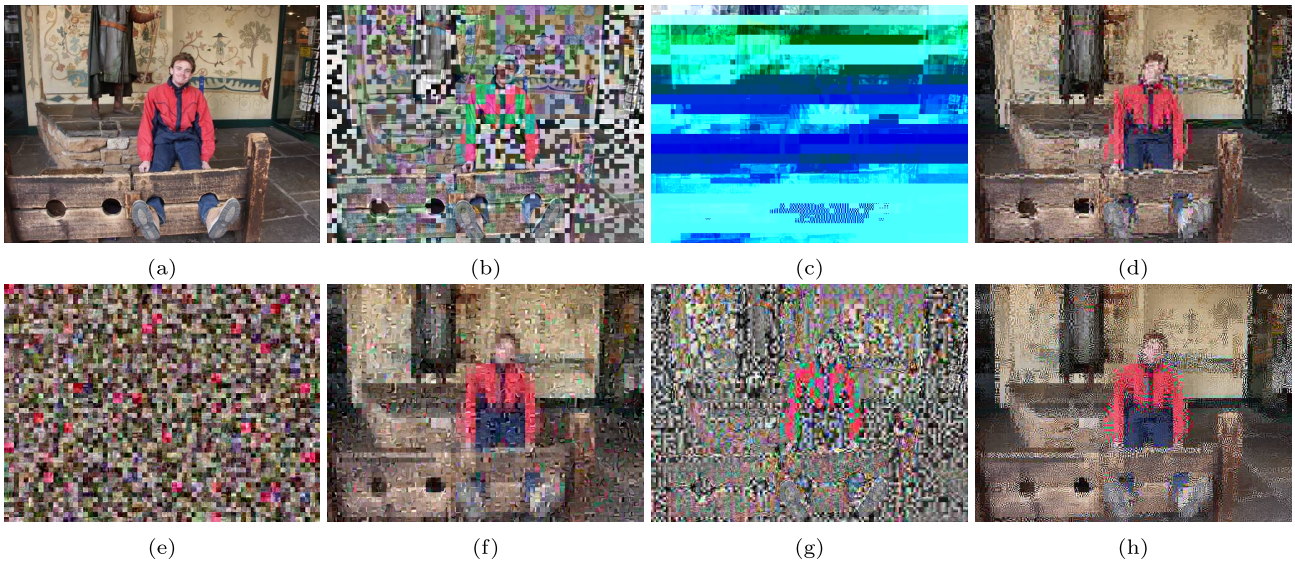


図 1　JPEG FCE 手法における圧縮効率の比較　暗号化なし（No encryption），大域シャッフル付き RSV ペア暗号化（GSPRS：Global Shuffling-connected RSV pair Scrambling）[12]，ランダム符号反転（RSF：Random Sign Flip）[10]，全ブロック間同帯域係数シャッフル（FIBS：Full Inter-block Shuffle）[9]，グレイスケールブロックベース ETC（GBE：Grayscale Block-based ETC）[8]，モジュロ演算付き予測誤差伝搬暗号化（WPEMO：Prediction Error Propagated Encryption with Modulo Operator）[14]．

4.2　圧縮中での暗号化

圧縮中暗号化は，JPEG 符号化過程の内部に介入し，圧縮構造と整合して暗号化を実現する方式である．とりわけ（量子化）DCT 係数領域を対象とするモジュールでは，係数のランダム符号反転（RSF）やシャッフル，ビットプレーンごとの暗号化などといった直接的な係数操作（図 2 (a–d)）[9]〜[11]に加え，DC 差分値のような予測構造に依存する信号成分への操作，あるいは特定の周波数帯域のみを選択的に撹乱する設計なども含まれる（図 2 (e–h)）[12]〜[14]．シャッフルに至っては，シャッフルの単位を DC 係数や DPCM 後の DC 差分値，同帯域周波数係



(a) (b) (c) (d)

(e) (f) (g) (h)

図 2　JPEG 量子化 DCT 係数領域における様々な暗号化モジュールによる暗号化結果　(a) 元画像，(b) DC 係数に対する RSF, (c) DC 差分値に対する RSF, (d) AC 係数に対する RSF, (e) 全ブロック間同帯域係数シャッフル，(f) 63AC 係数ブロック間シャッフル，(g) ビットキューボイドベースシャッフル，(h) AC 係数に対する RSV ペアシャッフル．

数，63AC 係数ブロック，ビット，RLE 領域におけるゼロラン長・値（RSV：Run Size-Value）ペアなどに変えることによって，様々な視覚的秘匿を実現できる．特に DC 係数/差分値に対しては RSF とシャッフルが，AC 係数に対しては RSF や帯域内シャッフル，ビットレベルでのシャッフル，63 係数ブロック間でのシャッフルなどを行うことで，効率的に JPEG 圧縮効率への影響を抑えつつ視覚的秘匿を実現できる．このような手法は，周波数領域の統計特性や予測依存構造を踏まえた設計が可能である一方で，JPEG 符号化の内部処理に対する詳しい理解を前提とする点に特徴がある．

この領域では，画素配置の入替などに基づく撹乱とは異なり，周波数構造そのものを対象とした撹乱処理が中心となる．そのため，係数操作の仕方によっては空間領域での撹乱よりも強い視覚的ひずみを誘発することが可能である．更に，低周波・高周波といった周波数帯域ごとの特性を踏まえた設計が可能であり，概形/模様情報の秘匿など目的に応じた周波数依存型の暗号化戦略を構築できる点も特徴である．もっとも，係数操作は統計分布の変化を通じて符号長増加を招く可能性があるため，圧縮効率とのトレードオフが評価上の重要な論点となる（図 1，GSRPS，RSF，FIBS，WPEMO（Type II））．加えて，DC 係数の値をゼロに置換する DC 除去攻撃や，非ゼロ AC 係数の符号などを推定する攻撃などといった周波数構造に基づく解析的攻撃への耐性も検討すべきである．したがって，量子化領域は圧縮効率維持と視覚的撹乱のバランス設計が最も集中的に議論される領域であり，フォーマット準拠性を厳密に維持するための慎重な設計が求められる．

4.3　圧縮後での暗号化

圧縮後暗号化は，エントロピー符号化後のビットストリームを直接操作する方式であり，CTE（Compression-then-Encryption）システムと称される．代表的な方式としては，振幅ビット列へのランダムビット列による XOR 適用や量子化テーブルの部分暗号化などが挙げられる[18]~[23]．

これらの手法は，JPEG デコーダによる復号互換性を維持しつつ，圧縮効率への影響を極力抑制できるという利点を有する．一方で，暗号化対象がエントロピー符号化済みビットストリームであるため，JPEG フォーマット特有の構文構造（JFIF 構造）に対する深い理解と，エントロピー符号化セグメント（ECS：Entropy-Coded Segment）の厳密な解析が前提となる．とりわけ，JFIF 構造内の ECS をパースしてハフマン符号語を検出し，復号互換性を維持する範囲で符号語を改変する「暗号化トランスコーダ」型の手法も提案されている[19]．この種の方式では，DC 差分値及び非ゼロ AC 係数に対応する可変長振幅ビット列をランダム化することで視覚的秘匿を実現する．しかしながら，その実験的再現性は，多様な JPEG プロファイルや符号化条件の中で特定の JFIF 構造をどの程度厳密に操作できるかという実装依存性に強く左右される．そのため，提案者以外の研究者が同等の条件で再現することが容易でない場合もあり，学術的検証や発展の観点からは課題が残る．

更に，これらの方式は JPEG のハフマン符号化構造に強く依存しているため，他画像フォーマット（例えば HEIF や AVIF：AV1 Image Format など）への転用は必ずしも容易ではない．また，JPEG において算術符号化を利用する場合や，異なるエントロピー符号化方式へ拡張する場合にも，設計の再検討が必要となる．このように，圧縮後暗号化は高いフォーマット準拠性と圧縮効率維持を両立できる一方で，フォーマット固有構造への依存性が強く，汎用的な暗号化モジュールとして抽象化・再利用することが難しいという側面も有する．

5. おわりに

5.1 これまでの JPEG FCE の到達点と限界

これまでに提案されてきた JPEG FCE 手法は，圧縮効率を維持しつつ視覚的秘匿性を確保するという制約の下で，多様な設計指針に基づいて発展してきた．特に，低計算量や頑健性，圧縮効率維持，調整可能性，再符号化可能性，フォーマット準拠性/復号互換性，モジュール化可能性，モジュール間可換性などといった評価軸が提示され，各手法はその一部に重点を置く形で設計されている．

しかしながら，これら全ての評価項目を同時に高い水準で満足する手法は，現時点では存在しない．例えば，強い視覚的ひずみを実現する手法は，圧縮効率の低下や再符号化可能性の低下などを招くことがあり，圧縮効率を厳密に保持する設計では，秘匿強度が限定的になる場合がある．また，構文制約を厳格に守るほど，暗号化モジュールの自由度は制限される．このように，JPEG FCE は本質的に多目的最適化問題としての性格をもっており，設計上のトレードオフが不可避である．

したがって，FCE の研究は「完全な手法の実現」というよりも，利用目的に応じた最適な設計という方向で進展してきたといえる．一方で，量子化係数領域，エントロピー符号化領域，更には JFIF 構造レベルに至るまで，様々なモジュールに対する暗号化アプローチが提案され続けており，新たな評価軸（例：再圧縮下での安定性，機械学習耐性など）も登場している．このことは，JPEG FCE が依然として活発な研究領域であり，新たな価値創出の余地が残されていることを示している．

5.2 今後の JPEG FCE に向けた方向性

近年の JPEG FCE 研究は，JPEG 特有の構文や符号化構造などに強く依存した設計へと洗練されてきた．すなわち，DCT 係数の配置構造や DPCM，ジグザグ走査，ハフマン符号表，構文構造などといった JPEG 固有の要素を前提とした手法が主流である．これはフォーマット準拠性を高精度に制御するという点では有効である一方，ほかの画像フォーマットへの適用可能性という観点では限定的である．今後の研究においては，

- 特定フォーマットに閉じた設計からの脱却
- 圧縮処理の「モジュール単位」に着目した抽象化
- 異なる圧縮方式（可変サイズ DCT 系・離散ウエーブレット変換（DWT：Discrete Wavelet Transform）系・予測符号化系）に横断的に適用可能な秘匿原理の構築

といった視点が重要になると考えられる．特に，変換や予測，量子化，エントロピー符号化などといった圧縮パイプラインの共通構造に基づくモジュール設計は，JPEG のみならず，ほかの静止画・動画像フォーマットに対しても応用可能なフォーマット非依存型 FCE の実現につながる可能性がある．このようなアプローチは，単に JPEG に対する最適化を追求するのではなく，圧縮符号化と知覚暗号化の理論的統合というより広い研究課題へと発展し得る．

5.3 まとめ

これまでの JPEG FCE 研究は，多様な評価軸のもとで設計上のトレードオフを調整しながら発展してきたが，全ての要件を同時に満たす万能的手法は未だ確立されていない．一方で，JPEG という枠組みを超え，圧縮モジュールに着目した抽象的・汎用的な暗号化設計へと視野を広げることにより，新たな研究展開が期待される．JPEG FCE は完成された技術領域ではなく，依然として発展途上にある分野であり，今後も圧縮技術と秘匿技術の接点において，新たな設計思想が生み出されることが期待される．

文　献

(1) W. Sirichotedumrong, Y. Kinoshita, and H. Kiya, “Pixel-based image encryption without key management for privacy-preserving deep neural networks,” IEEE Access, vol.7, pp.177844–177855, Dec. 2019.
(2) Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, and M. Cao, “DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things,” IEEE Internet Things J., vol.8, no.3, pp.1504–1518, July 2020.
(3) J. Zhou, X. Liu, O.C. Au, and Y.Y. Tang, “Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation,” IEEE Trans. Inf. Forensics Security, vol.9, no.1, pp.39–50, Jan. 2014.
(4) T. Xiang, J. Qu, and D. Xiao, “Joint SPIHT compression and selective encryption,” Appl. Soft Comput., vol.21, pp.159–170, Aug. 2014.
(5) K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, “An encryption-then-compression system for JPEG/Motion JPEG standard,” IEICE Trans. Fundamentals, vol.E98-A, no.11, pp.2238–2245, Nov. 2015.
(6) K. Shimizu, T. Suzuki, and K. Kameyama, “Cube-based encryption-then-compression system for video sequences,” IEICE Trans. Fundamentals, vol.E101-A, no.11, pp.1815–1822, Nov. 2018.
(7) K. Shimizu, T. Suzuki, and K. Kameyama, “Lapped cuboid-based perceptual encryption for Motion JPEG standard,” Proc. APSIPA ASC, pp.2022–2026, Honolulu, Hawaii, Nov. 2018.
(8) T. Chuman, W. Sirichotedumrong, and H. Kiya, “Encryption-then-compression systems using grayscale-based image encryption for JPEG images,” IEEE Trans. Inf. Forensics Security, vol.14, no.6, pp.1515–1525, Nov. 2019.
(9) W. Li and Y. Yuan, “A leak and its remedy in JPEG image encryption,” Int. J. Comput. Math, vol.84, no.9, pp.1367–1378, Sept. 2007.
(10) P. Li and K.-T. Lo, “Joint image compression and encryption based on order-8 alternating transforms,” J. Vis. Commun. Image, vol.44, pp.61–71, April 2017.
(11) M.I. Khan, V. Jeoti, and M.A. Khan, “Perceptual encryption of JPEG compressed images using DCT coefficients and splitting of DC coefficients into bitplanes,” Proc. ICIAS, pp.1–6, Kuala Lumpur, Malaysia, June 2010.
(12) K. Minemura, K. Wong, Q. Xiaojun, and T. Kiyoshi, “A scrambling framework for block transform compressed image,” Multimed. Tools. Appl., vol.76, no.5,

pp.6709–6729, March 2017.
(13) K. Shimizu and T. Suzuki, “Finely tunable bitcuboid-based encryption with exception-free signed binarization for JPEG standard,” IEEE Trans. Inf. Forensics Security, vol.16, pp.4985–4908, Sept. 2021.
(14) K. Shimizu and T. Suzuki, “WPE-MO: Prediction error-propagated encryption with modulo operator for JPEG texture protection,” IEICE Trans. Inf. & Syst., vol.E109-D, no.1, pp.107–116, Jan. 2026.
(15) S. Jenisch and A. Uhl, “A detailed evaluation of format-compliant encryption methods for JPEG XR-compressed images,” J. Inf. Secur., vol.2014, no.6, pp.1–20, April 2014.
(16) S. Okawa and O. Watanabe, “Perceptual encryption method for JPEG XL compressed images based on sign-scrambling of DCT coefficients,” Proc. GCCE, pp.219–222, Sept. 2025.
(17) Y. Yang, J. Zheng, X. Zhang, and Z. Zhang, “Design of image encryption and compression scheme compatible with JPEG XS based on spatial scrambling,” Microelectron. J., vol.170, no.10, 107083, April 2026.
(18) J. He, S. Huang, S. Tang, and J. Huang, “JPEG image encryption with improved format compatibility and file size preservation,” IEEE Trans. Multimedia, vol.20, no.10, pp.2645–2658, Oct. 2018.
(19) V. Itier, P. Puteaux, and W. Puech, “Recompression of JPEG crypto-compressed images without a key,” IEEE Trans. Circuits Syst. Video Technol., vol.30, no.3, pp.646–660, March 2020.
(20) Y. Yuan, H. He, Y. Yang, H. Amirpour, C. Timmerer, and F. Chen, “JPEG image encryption with DC rotation and undivided RSV-based AC group permutation,” IEEE Trans. Multimedia, vol.27, pp.1–15, Nov. 2023.
(21) M. Hirose, S. Imaizumi, and H. Kiya, “Encryption method for JPEG bitstreams for partially disclosing visual information,” Electronics, vol.13, no.11, p.2016, May 2024.
(22) Y. Peng, C. Fu, G. Cao, W. Song, J. Chen, and C.-Wing, “JPEG-compatible joint image compression and encryption algorithm with file size preservation,” ACM Trans. Multimed. Comput. Commun. Appl., vol.20, no.4, pp.1–20, Jan. 2024.
(23) X. Liu and J. Yang, “Joint JPEG compression and encryption with DC groups’ random cross-permutation and ZRVs’ inter-block permutation,” IEEE Trans. Multimedia, vol.28, pp.373–387, Oct. 2025.

（SIP 研究会提案，2026 年 3 月 1 日受付，
2026 年 4 月 6 日再受付）

清水　恒輔（正員）

2017 東京都立産業技術高等専門学校専攻科創造工学専攻情報工学コース卒業．2019・2022 筑波大学大学院システム情報工学研究科コンピュータサイエンス専攻修了（博士（工学））．2020〜2022 日本学術振興会特別研究員（DC2）．2022〜現在，筑波大学システム情報系博士特別研究員を経て，同年より岐阜大学工学部のテニュアトラック助教．画像・映像処理の研究に従事．

解　説　論　文

複素信号処理の基礎

Fundamentals of Complex Signal Processing

林　和則 Kazunori HAYASHI

アブストラクト　本稿では，複素信号処理の基礎について解説する．実数値信号に対する処理手法を複素領域へ拡張する際に特に重要となる二つの問題，すなわち，複素数をパラメータにもつ実数値関数の微分と，プロパー性を満たさない複素ランダム信号の統計的取り扱いに焦点を当てる．まず，複素変数を含む最適化問題における勾配計算のための手法としてウィルティンガー微分を紹介する．次に，プロパーでない複素信号を扱うための枠組みとして広義線形フィルタを説明する．更に，最小 2 乗推定及び線形 MMSE（minimum mean square error）推定の例を通してこれらの手法の利用方法を示すとともに，通信システムにおける IQ（in-phase/quadrature-phase）不均衡補償への応用についても述べる．

キーワード　複素信号，ウィルティンガー微分，広義線形フィルタ

Abstract　This article presents an introduction to the fundamentals of complex signal processing. Two issues that frequently arise when extending real-valued signal processing techniques to the complex domain are discussed: differentiation of real-valued functions with respect to complex parameters and statistical modeling of improper complex random signals. The Wirtinger derivative is introduced as a convenient tool for gradient computation in optimization problems involving complex variables. In addition, widely linear filtering is presented as an effective framework for handling complex signals that do not satisfy the properness assumption. The basic idea is explained together with illustrative examples including least-squares and linear MMSE estimation, and an application to IQ imbalance compensation in communication systems.

Key words　Complex signal, Wirtinger derivative, Widely linear filter

1. はじめに

複素数値をとるランダム信号は，通信，測位，音響など多くの工学分野において重要な対象である．信号処理に現れる多くの演算や信号の性質は，実数から複素数へ比較的容易に拡張できるため，多くの場合，実数を前提とした信号処理手法を複素信号処理へ適用することはそれほど難しくない．しかしながら，一部の概念や手法についてはその拡張が必ずしも自明ではなく，複素数特有の取り扱いが必要となる場合がある．このような点は，複素信号を扱う際につまずきやすいポイントとなっている．

その代表例の一つが，パラメータ最適化において重要な役割を果たす微分である．信号処理や機械学習における多くの問題では，実数値をとるコスト関数を定義し，それをパラメータについて最小化する最適化問題を解くことで最適解を求める．その際には，コスト関数のパラメータに関する偏微分をゼロとする条件を用いたり，勾配降下法を反復的に適用したりするために，微分が重要な役割を果たす．複素信号処理にこの枠組みを適用すると，コスト関数は複素数のパラメータを引数にもつ関数となるため，複素微分を用いて勾配などを計算することが期待される．しかしながら，通常の複素関数論で扱われる複素微分は，この目的のためにはほとんど利用できない．コスト関数は値の大小を比較する必要があるため実数値関数でなければならないが，複素数を引数にもつ実数値関数は，値が定数となる特別な場合を除き，複素微分可能とはならないためである．

もう一つの重要な点は，複素数値をとるランダム信号の統計的性質である．工学応用において複素確率変数を扱う際には，それらがプロパー（proper）であることや円対称（circular）であることが，明示的または暗黙的に仮定されることが多い．ここで，プロパーな複素確率変数とは，その複素共役との相関がゼロとなる確率変数であり，円対称な複素確率変数とは，その確率分布が複素平面上の回転に対して不変であるようなものを指す[(1)〜(3)]．実際，多くの複素信号はこれらの性質を満たすが，必ずしも常に成立するわけではない．例えば，通信におけるベースバンド変調で用いられる BPSK（binary phase shift keying）信号や，IQ（in-phase/quadrature-phase）不均衡によってひずみを受けた信号は，一般にプロパーではない[(4), (5)]．観測から未知変数を推定する問題において，平均 2 乗誤差（MSE: mean square error）を最小にする推定値は一般に条件付き期待値で与えられる．観測と未知変数が実数値で零平均の同時ガウス分布に従う場合，この推定値は観測の線形関数として表されることが知られている．しかしながら，観測と未知変数が複素ガウス分

林　和則　正員　京都大学大学院情報学研究科
E-mail hayashi.kazunori.4w@kyoto-u.ac.jp
Kazunori HAYASHI, Member (Graduate School of Informatics, Kyoto University, Yoshida-Honmachi, Sakyo, Kyoto, 606-8501 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.20 No.1 pp.24–33 2026 年 7 月

布に従う場合には，その分布が円対称（したがってプロパー）である場合を除き，この性質は一般には成り立たない．複素ガウス分布に従う信号の場合，MMSE（minimum MSE）推定値は観測信号だけでなくその複素共役にも依存する形で線形となる．このような性質は広義線形（widely linear）と呼ばれる[6],[7]．

本稿では，複素信号処理において特に重要となる以上の二つの観点に着目し，それらに関連する基本的な手法について解説する．まず，コスト関数のような実微分可能であるが複素微分可能ではない関数に対して，形式的に微分を定義するための方法について説明する．この微分はオーストリアの数学者 Wilhelm Wirtinger によって導入されたことから，ウィルティンガー微分 (Wirtinger derivative)[8]と呼ばれる．その基本的なアイデアは，複素変数とその複素共役を形式的に独立な変数とみなすことである．このような関数の勾配は，複素変数を二次元の実変数とみなして通常の実微分を用いることでも計算できるが，その方法では計算が煩雑になるだけでなく，複素数を用いることで得られる簡潔で見通しのよい表現が失われてしまう．ウィルティンガー微分を用いる利点は，複素数表現を保ったまま数式を簡潔に記述でき，実数の場合と類似した形式で勾配計算を行える点にある．近年，機械学習分野では自動微分[9]を用いた勾配計算が不可欠となっており，ウィルティンガー微分を対象とした自動微分についても議論が行われている[10]．更に，深層展開[11],[12]に代表されるように，従来の信号処理技術と深層学習を融合したモデルベース機械学習[13]が注目されており，複素変数を引数にもつ実数値関数の勾配を効率的に計算することの重要性はますます高まっている．

本稿でもう一つ取り上げる手法は，プロパーでない複素信号を扱うための強力な枠組みである広義線形フィルタである．上述のように，広義線形フィルタは信号がプロパーでない複素ガウス分布に従う場合に最小の MSE を達成するが，通常の線形 MMSE 推定がガウス信号以外の場合にも有効であるのと同様に，広義線形フィルタも複素ガウス信号に限らず広く有効である．プロパーでない複素信号では，信号とその複素共役の間の相関を表す補共分散（complementary covariance）など，プロパーな場合には現れない統計量が重要となる．これらの統計量を利用することで，広義線形フィルタが通常の（狭義）線形フィルタよりも小さい MSE を達成できることを示す．更に，広義線形フィルタの応用例として，通信システムにおける IQ 不均衡による信号ひずみの補償問題[14],[15]を取り上げる．

2. 複素信号の表現

信号処理では信号をベクトルで表現することが多いため，N 次元の複素ベクトル $\boldsymbol{z} \in \mathbb{C}^N$ について考える (注1)．複素数ベクトル $\boldsymbol{z}$ の実部 $\Re(\boldsymbol{z})$ と虚部 $\Im(\boldsymbol{z})$ をそれぞれ，$\boldsymbol{z}_\mathrm{r}, \boldsymbol{z}_\mathrm{i} \in \mathbb{R}^N$ とすると，$\boldsymbol{z} = \boldsymbol{z}_\mathrm{r} + j\boldsymbol{z}_\mathrm{i}$ と表現される．ここで，j は虚数単位を表す．複素信号を対象とした信号処理では，複素数ベクトル $\boldsymbol{z}$ に対して様々な演算が施されるが，$\boldsymbol{z}$ を別の表現に変換してから処理されることも多い．

(注1)：本稿では，別途指定しない限り，ベクトルは全て列ベクトルとして定義する．

自然で，よく利用される方法は，複素数ベクトル $\boldsymbol{z}$ の実部と虚部をスタックすることで得られる $2N$ 次元の実数拡張ベクトル

$$\bar{\boldsymbol{z}} = \begin{bmatrix} \boldsymbol{z}_\mathrm{r} \\ \boldsymbol{z}_\mathrm{i} \end{bmatrix} \in \mathbb{R}^{2N} \tag{1}$$

に変換して処理する方法である．

例えば，複素ベクトル $\boldsymbol{x} \in \mathbb{C}^N$ に複素行列 $\boldsymbol{A} \in \mathbb{C}^{M\times N}$ を乗算して複素ベクトル $\boldsymbol{y} \in \mathbb{C}^M$ を得る演算

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{x} \tag{2}$$

を考えると，この関係はそれぞれ実部と虚部による表現 $\boldsymbol{x} = \boldsymbol{x}_\mathrm{r} + j\boldsymbol{x}_\mathrm{i}$，$\boldsymbol{y} = \boldsymbol{y}_\mathrm{r} + j\boldsymbol{y}_\mathrm{i}$，$\boldsymbol{A} = \boldsymbol{A}_\mathrm{r} + j\boldsymbol{A}_\mathrm{i}$ を用いて

$$\boldsymbol{y}_\mathrm{r} + j\boldsymbol{y}_\mathrm{i} = (\boldsymbol{A}_\mathrm{r}\boldsymbol{x}_\mathrm{r} - \boldsymbol{A}_\mathrm{i}\boldsymbol{x}_\mathrm{i}) + j(\boldsymbol{A}_\mathrm{i}\boldsymbol{x}_\mathrm{r} + \boldsymbol{A}_\mathrm{r}\boldsymbol{x}_\mathrm{i})$$

と書くことができる．したがって，

$$\bar{\boldsymbol{x}} = \begin{bmatrix} \boldsymbol{x}_\mathrm{r} \\ \boldsymbol{x}_\mathrm{i} \end{bmatrix}, \quad \bar{\boldsymbol{y}} = \begin{bmatrix} \boldsymbol{y}_\mathrm{r} \\ \boldsymbol{y}_\mathrm{i} \end{bmatrix}, \quad \bar{\boldsymbol{A}} = \begin{bmatrix} \boldsymbol{A}_\mathrm{r} & -\boldsymbol{A}_\mathrm{i} \\ \boldsymbol{A}_\mathrm{i} & \boldsymbol{A}_\mathrm{r} \end{bmatrix} \tag{3}$$

と定義すると，複素ベクトルの 2 倍の長さの実ベクトルを用いて

$$\bar{\boldsymbol{y}} = \bar{\boldsymbol{A}}\bar{\boldsymbol{x}} \tag{4}$$

と書くことができ，この変換により，実数の行列–ベクトル積のアルゴリズムを用いて，複素数の行列–ベクトル積を実行できる．

ほかによく利用される複素数ベクトル $\boldsymbol{z}$ の表現として，$\boldsymbol{z}$ とその複素共役 $\boldsymbol{z}^*$ をスタックした複素拡張ベクトル

$$\underline{\boldsymbol{z}} = \begin{bmatrix} \boldsymbol{z} \\ \boldsymbol{z}^* \end{bmatrix} \in \mathbb{C}^{2N} \tag{5}$$

を用いる方法がある．元になる複素ベクトル $\boldsymbol{z}$ そのものを要素として含んでいることから分かるように，これは冗長な表現であり，一見不自然で意味がないように思えるが，本稿の残りのパートで見るように，複素信号処理において重要な役割を果たす．

式 (1) と式 (5) の表現の間には，

$$\underline{\boldsymbol{z}} = \boldsymbol{T}_N\bar{\boldsymbol{z}} \tag{6}$$

なる関係がある．ただし，行列 $\boldsymbol{T}_N$ は

$$\boldsymbol{T}_N = \begin{bmatrix} \boldsymbol{I} & j\boldsymbol{I} \\ \boldsymbol{I} & -j\boldsymbol{I} \end{bmatrix} \in \mathbb{C}^{2N\times 2N} \tag{7}$$

で定義され，$\boldsymbol{I}$ は単位行列である．容易に確認できるように，$\boldsymbol{T}_N\boldsymbol{T}_N^\mathsf{H} = \boldsymbol{T}_N^\mathsf{H}\boldsymbol{T}_N = 2\boldsymbol{I}$ が成り立つので，$\bar{\boldsymbol{z}} = \frac{1}{2}\boldsymbol{T}_N^\mathsf{H}\underline{\boldsymbol{z}}$ と表すこともできる．ここで，$(\cdot)^\mathsf{H}$ は共役転置を表す．

3. ウィルティンガー微分

3.1 正則関数

最も簡単な場合として，一つの複素数 $z = z_\mathrm{r} + jz_\mathrm{i}$ $(z_\mathrm{r}, z_\mathrm{i} \in \mathbb{R})$ を引数にもち，複素数値を取る関数 $f(z)$ について考える．複素

微分可能な関数（正則関数，analytic function）は次で定義される[16]．

定義 1.（**正則関数**）$D \subseteqq \mathbb{C}$ を関数 $f : D \to \mathbb{C}$ の定義域とする．

$$f'(z) = \lim_{\Delta z \to 0} \frac{f(z+\Delta z) - f(z)}{\Delta z} \tag{8}$$

が任意の内点 $z \in D$ について存在するとき関数 f は領域 D で複素微分可能（正則）であるという．

複素関数論の基本的な結果として，複素微分可能であるための一般的な条件が存在する．具体的には，複素数 $z = z_\mathrm{r} + jz_\mathrm{i}$ を引数にもつ複素関数 $f(z)$ を実二変数関数 $f(z_\mathrm{r}, z_\mathrm{i})$ とみたとき，それが全微分可能（実微分可能）であり，かつ次のコーシー・リーマンの方程式（Cauchy-Riemann equations）と呼ばれる関係が成り立つとき，またそのときに限り，複素微分可能である[17]．

$$\frac{\partial u}{\partial z_\mathrm{r}} = \frac{\partial v}{\partial z_\mathrm{i}}, \quad \frac{\partial u}{\partial z_\mathrm{i}} = -\frac{\partial v}{\partial z_\mathrm{r}} \tag{9}$$

ただし，$u(z_\mathrm{r}, z_\mathrm{i}) = \Re\{f(z_\mathrm{r}, z_\mathrm{i})\}$，$v(z_\mathrm{r}, z_\mathrm{i}) = \Im\{f(z_\mathrm{r}, z_\mathrm{i})\}$ である．

3.2 正則でない複素関数の例

信号処理の問題では電力や 2 乗ユークリッド距離の最小化についてよく議論され，その際 $f(z) = |z|^2 = zz^*$ のような形の関数がよく現れる．この $f(z)$ を複素微分の定義式 (8) に代入すると，

$$f'(z) = \lim_{\Delta z \to 0} \frac{\Delta z z^* + z(\Delta z)^* + \Delta z(\Delta z)^*}{\Delta z} \tag{10}$$

となる．しかしながら，この式は Δz をどのように 0 に近づけるかによって値が変わってしまうため，極限が存在しない．実際，$\Delta z = \Delta z_\mathrm{r} + j\Delta z_\mathrm{i}$ $(\Delta z_\mathrm{r}, \Delta z_\mathrm{i} \in \mathbb{R})$ として，まず $\Delta z_\mathrm{r} \to 0$ とするとこの値は $z^* - z - j\Delta z_\mathrm{i}$ となり，更に $\Delta z_\mathrm{i} \to 0$ とすると $z^* - z$ となる．一方，先に $\Delta z_\mathrm{i} \to 0$ とすると $z^* + z + \Delta z_\mathrm{r}$ となり，更に $\Delta z_\mathrm{r} \to 0$ とすると $z^* + z$ となる．これは関数 $f(z) = |z|^2 = zz^*$ が複素微分可能でないことを意味する．では，このような関数の勾配を求めるにはどうすればよいのか？ $f(z)$ は実微分可能なので，一つの方法としては引数を実部と虚部に分けてそれぞれで偏微分することが考えられるが，対象となる関数が複雑になると計算が非常に煩雑になってしまうという問題がある．このような非正則関数の微分を扱うために導入されるのがウィルティンガー微分である．

3.3 ウィルティンガー微分

正則ではないが実微分可能な複素関数の勾配を求める際に有効なのが，複素拡張ベクトルのように z と z^* を独立な変数として扱って関数 $f(z)$ の全微分を考えるというアプローチである．

引数 $z = z_\mathrm{r} + jz_\mathrm{i}$ をもつ実微分可能関数 $f(z)$ を実 2 変数関数 $f(z_\mathrm{r}, z_\mathrm{i})$ とみたとき，その全微分[18]は独立な変数 $z_\mathrm{r}, z_\mathrm{i} \in \mathbb{R}$ を用いて

$$df = \frac{\partial f}{\partial z_\mathrm{r}} dz_\mathrm{r} + \frac{\partial f}{\partial z_\mathrm{i}} dz_\mathrm{i} \tag{11}$$

と書ける．ここで，

$$dz = dz_\mathrm{r} + j dz_\mathrm{i}, \quad dz^* = dz_\mathrm{r} - j dz_\mathrm{i} \tag{12}$$

より

$$dz_\mathrm{r} = \frac{1}{2}(dz + dz^*), \quad dz_\mathrm{i} = \frac{1}{2j}(dz - dz^*) \tag{13}$$

である．これを，式 (11) に代入すると

$$df = \frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} - j\frac{\partial f}{\partial z_\mathrm{i}}\right) dz + \frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} + j\frac{\partial f}{\partial z_\mathrm{i}}\right) dz^* \tag{14}$$

となる．

一方，f を形式的に独立な変数 z, z^* の関数とみると，その全微分は

$$df = \frac{\partial f}{\partial z} dz + \frac{\partial f}{\partial z^*} dz^* \tag{15}$$

と書くこともできる．

式 (14) と式 (15) を見比べると，次のように定義すると実数の場合と同様の表現が得られ，都合がよいことが分かる[3], [19]．

定義 2. ウィルティンガー微分（スカラー引数の場合）

$$\frac{\partial f}{\partial z} \triangleq \frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} - j\frac{\partial f}{\partial z_\mathrm{i}}\right) \tag{16}$$

$$\frac{\partial f}{\partial z^*} \triangleq \frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} + j\frac{\partial f}{\partial z_\mathrm{i}}\right) \tag{17}$$

これはウィルティンガー微分と呼ばれる．z と z^* を形式的に独立変数として扱っている点が気になるが，$f(z) = z$ と $f(z) = z^*$ の場合を考えると，

$$\frac{\partial z}{\partial z} = 1, \quad \frac{\partial z^*}{\partial z^*} = 1, \quad \frac{\partial z}{\partial z^*} = 0, \quad \frac{\partial z^*}{\partial z} = 0 \tag{18}$$

となる．これより，$\frac{\partial}{\partial z}$ を評価する際には z^* を形式的に定数として z に関する偏微分を計算し，$\frac{\partial}{\partial z^*}$ を評価する際には z を形式的に定数として z^* に関する偏微分を計算してもよいことが分かる．

3.4 正則関数のウィルティンガー微分

関数 $f(z)$ の実部 $u(z_\mathrm{r}, z_\mathrm{i})$ と虚部 $v(z_\mathrm{r}, z_\mathrm{i})$ を用いると，ウィルティンガー微分は

$$\frac{\partial f}{\partial z} = \frac{1}{2}\left(\frac{\partial u}{\partial z_\mathrm{r}} + \frac{\partial v}{\partial z_\mathrm{i}}\right) + \frac{j}{2}\left(\frac{\partial v}{\partial z_\mathrm{r}} - \frac{\partial u}{\partial z_\mathrm{i}}\right) \tag{19}$$

$$\frac{\partial f}{\partial z^*} = \frac{1}{2}\left(\frac{\partial u}{\partial z_\mathrm{r}} - \frac{\partial v}{\partial z_\mathrm{i}}\right) + \frac{j}{2}\left(\frac{\partial v}{\partial z_\mathrm{r}} + \frac{\partial u}{\partial z_\mathrm{i}}\right) \tag{20}$$

と書ける．

これより，コーシー・リーマンの方程式が成り立つとき，$\frac{\partial f}{\partial z^*}$

の実部と虚部がいずれも 0 になることから，正則関数 $f(z)$ では

$$\frac{\partial f}{\partial z^*} = 0 \tag{21}$$

となること，すなわち，複素微分可能な関数は z^* に依存しないことが分かる．

一方，複素微分の定義の式 (8) において，$\Delta z = \Delta z_\mathrm{r} + j\Delta z_\mathrm{i}$, $(\Delta z_\mathrm{r}, \Delta z_\mathrm{i} \in \mathbb{R})$ とし，実軸上で $\Delta z \to 0$ とすることを考えて $\Delta z_\mathrm{i} = 0$ とすると

$$\begin{aligned} f'(z) &= \lim_{\Delta z \to 0} \frac{f(z+\Delta z) - f(z)}{\Delta z} \\ &= \lim_{\Delta z_\mathrm{r} \to 0} \frac{u(z_\mathrm{r}+\Delta z_\mathrm{r}, z_\mathrm{i}) - u(z_\mathrm{r}, z_\mathrm{i})}{\Delta z_\mathrm{r}} \\ &\qquad + j \lim_{\Delta z_\mathrm{r} \to 0} \frac{v(z_\mathrm{r}+\Delta z_\mathrm{r}, z_\mathrm{i}) - v(z_\mathrm{r}, z_\mathrm{i})}{\Delta z_\mathrm{r}} \\ &= \frac{\partial u}{\partial z_\mathrm{r}} + j\frac{\partial v}{\partial z_\mathrm{r}} \end{aligned} \tag{22}$$

となる．これは上記 $\frac{\partial f}{\partial z}$ にコーシー・リーマンの方程式を代入して得られる結果に一致する．これより，正則関数のウィルティンガー微分 $\frac{\partial f}{\partial z}$ は通常の複素微分に一致し，ウィルティンガー微分が通常の複素微分を特別な場合として含むことが分かる．

3.5 連鎖律によるウィルティンガー微分の導出

上では全微分を用いてウィルティンガー微分を導出したが，実微分の連鎖律を用いた簡単な導出法も知られている[16], [20]．実 2 変数 $z_\mathrm{r}, z_\mathrm{i} \in \mathbb{R}$ を引数にもつ関数 $f(z_\mathrm{r}, z_\mathrm{i})$ について考える．更に，$z_\mathrm{r}, z_\mathrm{i}$ を実部と虚部にもつ複素数を，$z_\mathrm{r}, z_\mathrm{i}$ を引数にもつ関数と考えて $z(z_\mathrm{r}, z_\mathrm{i}) = z_\mathrm{r} + jz_\mathrm{i}$，$z^*(z_\mathrm{r}, z_\mathrm{i}) = z_\mathrm{r} - jz_\mathrm{i}$ と定義すると，実関数の連鎖律[18]より

$$\frac{\partial f}{\partial z_\mathrm{r}} = \frac{\partial f}{\partial z}\frac{\partial z}{\partial z_\mathrm{r}} + \frac{\partial f}{\partial z^*}\frac{\partial z^*}{\partial z_\mathrm{r}} = \frac{\partial f}{\partial z} + \frac{\partial f}{\partial z^*} \tag{23}$$

$$\frac{\partial f}{\partial z_\mathrm{i}} = \frac{\partial f}{\partial z}\frac{\partial z}{\partial z_\mathrm{i}} + \frac{\partial f}{\partial z^*}\frac{\partial z^*}{\partial z_\mathrm{i}} = j\frac{\partial f}{\partial z} - j\frac{\partial f}{\partial z^*} \tag{24}$$

となる．ここで

$$\frac{\partial z}{\partial z_\mathrm{r}} = \frac{\partial z^*}{\partial z_\mathrm{r}} = 1, \quad \frac{\partial z}{\partial z_\mathrm{i}} = j, \quad \frac{\partial z^*}{\partial z_\mathrm{i}} = -j \tag{25}$$

を用いた．式 (23), (24) を $\frac{\partial f}{\partial z}$, $\frac{\partial f}{\partial z^*}$ について解くと，式 (16), (17) のウィルティンガー微分が得られる．

3.6 ウィルティンガー微分の性質

複素数の信号処理でよく使われるウィルティンガー微分の性質を幾つか挙げておく（線形性，積，連鎖律については $\frac{\partial}{\partial z}$ についてのみ記しているが，$\frac{\partial}{\partial z^*}$ についても同様に成り立つ）．

線形性:

$$\frac{\partial}{\partial z}(af + bg) = a\frac{\partial f}{\partial z} + b\frac{\partial g}{\partial z} \quad (a, b \in \mathbb{C}) \tag{26}$$

積:

$$\frac{\partial}{\partial z}(f \cdot g) = \frac{\partial f}{\partial z} \cdot g + f \cdot \frac{\partial g}{\partial z} \tag{27}$$

連鎖律:

$$\frac{\partial g(f(z))}{\partial z} = \frac{\partial g}{\partial f}\frac{\partial f}{\partial z} + \frac{\partial g}{\partial f^*}\frac{\partial f^*}{\partial z} \tag{28}$$

複素共役:

$$\left(\frac{\partial f}{\partial z^*}\right)^* = \frac{\partial f^*}{\partial z} \tag{29}$$

式 (26) の線形性は，ウィルティンガー微分の定義式 (16) を用いると，実微分の線形性から自明である．

式 (27) の積の性質は，実微分の積の性質を用いて次のように導出できる．

$$\begin{aligned} \frac{\partial}{\partial z}(f \cdot g) &= \frac{1}{2}\left(\frac{\partial (f \cdot g)}{\partial z_\mathrm{r}} - j\frac{\partial (f \cdot g)}{\partial z_\mathrm{i}}\right) \\ &= \frac{1}{2}\left\{\frac{\partial f}{\partial z_\mathrm{r}} \cdot g + f \cdot \frac{\partial g}{\partial z_\mathrm{r}} - j\left(\frac{\partial f}{\partial z_\mathrm{i}} \cdot g + f \cdot \frac{\partial g}{\partial z_\mathrm{i}}\right)\right\} \\ &= \frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} - j\frac{\partial f}{\partial z_\mathrm{i}}\right) \cdot g + f \cdot \frac{1}{2}\left(\frac{\partial g}{\partial z_\mathrm{r}} - j\frac{\partial g}{\partial z_\mathrm{i}}\right) \\ &= \frac{\partial f}{\partial z} \cdot g + f \cdot \frac{\partial g}{\partial z} \end{aligned}$$

式 (28) の連鎖律も実微分の連鎖律を用いて導出できる．関数 f の引数を $z = z_\mathrm{r} + jz_\mathrm{i}$, $(z_\mathrm{r}, z_\mathrm{i} \in \mathbb{R})$ とし，$f(z)$ の実部と虚部をそれぞれ $u(z_\mathrm{r}, z_\mathrm{i}), v(z_\mathrm{r}, z_\mathrm{i})$ とすると，実 2 変数関数の連鎖律[18]より，

$$\frac{\partial g}{\partial z_\mathrm{r}} = \frac{\partial g}{\partial u}\frac{\partial u}{\partial z_\mathrm{r}} + \frac{\partial g}{\partial v}\frac{\partial v}{\partial z_\mathrm{r}}, \quad \frac{\partial g}{\partial z_\mathrm{i}} = \frac{\partial g}{\partial u}\frac{\partial u}{\partial z_\mathrm{i}} + \frac{\partial g}{\partial v}\frac{\partial v}{\partial z_\mathrm{i}} \tag{30}$$

となる．ここで，関数 g の f 及び f^* によるウィルティンガー微分が，

$$\frac{\partial g}{\partial f} = \frac{1}{2}\left(\frac{\partial g}{\partial u} - j\frac{\partial g}{\partial v}\right), \quad \frac{\partial g}{\partial f^*} = \frac{1}{2}\left(\frac{\partial g}{\partial u} + j\frac{\partial g}{\partial v}\right) \tag{31}$$

と書けることから，

$$\frac{\partial g}{\partial u} = \frac{\partial g}{\partial f} + \frac{\partial g}{\partial f^*}, \quad \frac{\partial g}{\partial v} = j\left(\frac{\partial g}{\partial f} - \frac{\partial g}{\partial f^*}\right) \tag{32}$$

と表すことができる．これらを式 (30) の $\frac{\partial g}{\partial u}$ と $\frac{\partial g}{\partial v}$ に代入し，更に得られた $\frac{\partial g}{\partial z_\mathrm{r}}$, $\frac{\partial g}{\partial z_\mathrm{i}}$ を，関数 g の z によるウィルティンガー微分

$$\frac{\partial g}{\partial z} = \frac{1}{2}\left(\frac{\partial g}{\partial z_\mathrm{r}} - j\frac{\partial g}{\partial z_\mathrm{i}}\right) \tag{33}$$

に代入して整理することで，式 (28) の連鎖律が得られる．

式 (29) の複素共役に関する性質は，実微分と複素共役の可換性を用いることで次のように導出できる．

$$\left(\frac{\partial f}{\partial z^*}\right)^* = \left\{\frac{1}{2}\left(\frac{\partial f}{\partial z_\mathrm{r}} + j\frac{\partial f}{\partial z_\mathrm{i}}\right)\right\}^*$$

$$= \frac{1}{2}\left\{\left(\frac{\partial f}{\partial z_{\mathrm{r}}}\right)^* - j\left(\frac{\partial f}{\partial z_{\mathrm{i}}}\right)^*\right\}$$
$$= \frac{1}{2}\left\{\frac{\partial f^*}{\partial z_{\mathrm{r}}} - j\frac{\partial f^*}{\partial z_{\mathrm{i}}}\right\} = \frac{\partial f^*}{\partial z}$$

3.7 ウィルティンガー微分（ベクトル引数の場合）

次に，複素数値をとる関数 f の引数が複素ベクトル $\boldsymbol{z} = [z_1\ z_2\ \cdots\ z_N]^{\mathsf{T}} \in \mathbb{C}^N$ で与えられる多変数の場合，すなわち，$f : \mathbb{C}^N \to \mathbb{C}$ を考える．このとき，f の $\boldsymbol{z}$ 及び $\boldsymbol{z}^*$ によるウィルティンガー微分を

$$\frac{\partial f}{\partial \boldsymbol{z}} = \begin{bmatrix}\frac{\partial f}{\partial z_1} & \frac{\partial f}{\partial z_2} & \cdots & \frac{\partial f}{\partial z_N}\end{bmatrix} \tag{34}$$
$$\frac{\partial f}{\partial \boldsymbol{z}^*} = \begin{bmatrix}\frac{\partial f}{\partial z_1^*} & \frac{\partial f}{\partial z_2^*} & \cdots & \frac{\partial f}{\partial z_N^*}\end{bmatrix} \tag{35}$$

のように，行ベクトルで定義すると都合がよい．スカラー引数の場合と同様に，変数 $\boldsymbol{z}, \boldsymbol{z}^*$ を独立とみなすと，関数 $f(\boldsymbol{z})$ の全微分が

$$df = \frac{\partial f}{\partial \boldsymbol{z}} d\boldsymbol{z} + \frac{\partial f}{\partial \boldsymbol{z}^*} d\boldsymbol{z}^* \tag{36}$$

と簡潔な形で表されるからである．ここで

$$d\boldsymbol{z} = \begin{bmatrix}dz_1 & dz_2 & \cdots & dz_N\end{bmatrix}^{\mathsf{T}} \tag{37}$$
$$d\boldsymbol{z}^* = \begin{bmatrix}dz_1^* & dz_2^* & \cdots & dz_N^*\end{bmatrix}^{\mathsf{T}} \tag{38}$$

である．

一方，$z_n = z_{\mathrm{r},\boldsymbol{n}} + jz_{\mathrm{i},\boldsymbol{n}}$ $(z_{\mathrm{r},\boldsymbol{n}}, z_{\mathrm{i},\boldsymbol{n}} \in \mathbb{R})$ として，関数 $f(\boldsymbol{z})$ を，独立な変数 $z_{\mathrm{r},\boldsymbol{n}}, z_{\mathrm{i},\boldsymbol{n}} \in \mathbb{R}$ $(n = 1, 2, \ldots, N)$ を引数にもつ関数とみなすと，その全微分は

$$df = \sum_{n=1}^{N}\left(\frac{\partial f}{\partial z_{\mathrm{r},\boldsymbol{n}}} dz_{\mathrm{r},\boldsymbol{n}} + \frac{\partial f}{\partial z_{\mathrm{i},\boldsymbol{n}}} dz_{\mathrm{i},\boldsymbol{n}}\right) \tag{39}$$

で与えられ，更に $dz_n = dz_{\mathrm{r},\boldsymbol{n}} + jdz_{\mathrm{i},\boldsymbol{n}}$ 及び $dz_n^* = dz_{\mathrm{r},\boldsymbol{n}} - jdz_{\mathrm{i},\boldsymbol{n}}$ を用いると

$$df = \sum_{n=1}^{N}\left\{\frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},\boldsymbol{n}}} - j\frac{\partial f}{\partial z_{\mathrm{i},\boldsymbol{n}}}\right) dz_n + \frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},\boldsymbol{n}}} + j\frac{\partial f}{\partial z_{\mathrm{i},\boldsymbol{n}}}\right) dz_n^*\right\} \tag{40}$$

と書ける．

これらを比べることで，複素ベクトルを引数にもつスカラー値の複素関数 f のウィルティンガー微分は次で定義される[3], [19]．

定義 3. ウィルティンガー微分（ベクトル引数の場合）

$$\frac{\partial f}{\partial \boldsymbol{z}} \triangleq \begin{bmatrix}\frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},1}} - j\frac{\partial f}{\partial z_{\mathrm{i},1}}\right) & \cdots & \frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},N}} - j\frac{\partial f}{\partial z_{\mathrm{i},N}}\right)\end{bmatrix} \tag{41}$$

$$\frac{\partial f}{\partial \boldsymbol{z}^*} \triangleq \begin{bmatrix}\frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},1}} + j\frac{\partial f}{\partial z_{\mathrm{i},1}}\right) & \cdots & \frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},N}} + j\frac{\partial f}{\partial z_{\mathrm{i},N}}\right)\end{bmatrix} \tag{42}$$

微小量を複素拡張ベクトルの形式で書くと，全微分 df は

$$df = \begin{bmatrix}\frac{\partial f}{\partial \boldsymbol{z}} & \frac{\partial f}{\partial \boldsymbol{z}^*}\end{bmatrix}\begin{bmatrix}d\boldsymbol{z} \\ d\boldsymbol{z}^*\end{bmatrix} \tag{43}$$

と書けるので，複素ベクトルを引数にもつスカラー値複素関数 f の勾配は

$$\nabla f = \begin{bmatrix}\frac{\partial f}{\partial \boldsymbol{z}} & \frac{\partial f}{\partial \boldsymbol{z}^*}\end{bmatrix} \tag{44}$$

で定義される．ここで，関数 f が実数値をとる特別な場合には $f = f^*$ となるので，ウィルティンガー微分の複素共役に関する性質を用いると

$$\frac{\partial f}{\partial \boldsymbol{z}^*} = \left(\frac{\partial f}{\partial \boldsymbol{z}}\right)^* \tag{45}$$

となり，複素勾配は

$$\nabla f = \begin{bmatrix}\left(\frac{\partial f}{\partial \boldsymbol{z}^*}\right)^* & \frac{\partial f}{\partial \boldsymbol{z}^*}\end{bmatrix} \tag{46}$$

で与えられる．これより，関数 f がコスト関数のように実数値を取る場合は，複素勾配が $\nabla f = \boldsymbol{0}$ となることと，$\frac{\partial f}{\partial \boldsymbol{z}} = \boldsymbol{0}$, $\frac{\partial f}{\partial \boldsymbol{z}^*} = \boldsymbol{0}$ がいずれも同値であり，$\nabla f = \boldsymbol{0}$ となるパラメータを求める際には $\frac{\partial f}{\partial \boldsymbol{z}^*} = \boldsymbol{0}$（あるいは $\frac{\partial f}{\partial \boldsymbol{z}} = \boldsymbol{0}$）のみを考えればよいことが分かる．

なお，本稿では上述のように $\frac{\partial f}{\partial \boldsymbol{z}}$, $\frac{\partial f}{\partial \boldsymbol{z}^*}$ を行ベクトルで定義し，

$$\frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{T}}} = \left(\frac{\partial f}{\partial \boldsymbol{z}}\right)^{\mathsf{T}}, \quad \frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{H}}} = \left(\frac{\partial f}{\partial \boldsymbol{z}^*}\right)^{\mathsf{T}} \tag{47}$$

としているが，この定義は文献ごとに流儀があり，$\frac{\partial f}{\partial \boldsymbol{z}}$, $\frac{\partial f}{\partial \boldsymbol{z}^*}$ が列ベクトルで定義されることもあるので注意が必要である．

N 次元の標準基底ベクトル $\boldsymbol{e}_n^N$ $(n = 1, 2, \cdots, N)$ を用いると，ベクトル引数のウィルティンガー微分 $\frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{T}}}$, $\frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{H}}}$ は

$$\frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{T}}} = \sum_{n=1}^{N} \boldsymbol{e}_n^N \frac{\partial f}{\partial z_n}, \quad \frac{\partial f}{\partial \boldsymbol{z}^{\mathsf{H}}} = \sum_{n=1}^{N} \boldsymbol{e}_n^N \frac{\partial f}{\partial z_n^*} \tag{48}$$

と表すことができる．これを用いると，信号処理でよく現れる次のベクトル引数の関数のウィルティンガー微分が得られる．

スカラー値ベクトル引数関数のウィルティンガー微分の例

$$\frac{\partial}{\partial \boldsymbol{z}^{\mathsf{H}}}\left(\boldsymbol{z}^{\mathsf{H}}\boldsymbol{a}\right) = \boldsymbol{a} \tag{49}$$
$$\frac{\partial}{\partial \boldsymbol{z}^{\mathsf{H}}}\left(\boldsymbol{a}^{\mathsf{H}}\boldsymbol{z}\right) = \boldsymbol{0} \tag{50}$$
$$\frac{\partial}{\partial \boldsymbol{z}^{\mathsf{H}}}\left(\boldsymbol{z}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{z}\right) = \boldsymbol{A}\boldsymbol{z} \tag{51}$$

ただし，$\boldsymbol{a}$, $\boldsymbol{A}$ は定係数のベクトル，及び行列．

これは実ベクトルを引数と実関数の微分の場合と異なることに注意する．参考までに，$\boldsymbol{x}$ が実ベクトルの場合の対応する微分を次に示す[21]．

（参考）スカラー値ベクトル引数実関数の実微分の例

$$\frac{\partial}{\partial \boldsymbol{x}^{\mathsf{T}}}\left(\boldsymbol{x}^{\mathsf{T}}\boldsymbol{a}\right)=\boldsymbol{a} \tag{52}$$

$$\frac{\partial}{\partial \boldsymbol{x}^{\mathsf{T}}}\left(\boldsymbol{a}^{\mathsf{T}}\boldsymbol{x}\right)=\boldsymbol{a} \tag{53}$$

$$\frac{\partial}{\partial \boldsymbol{x}^{\mathsf{T}}}\left(\boldsymbol{x}^{\mathsf{T}}\boldsymbol{A}\boldsymbol{x}\right)=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{A}^{\mathsf{T}}\boldsymbol{x} \tag{54}$$

ただし，$\boldsymbol{a}$, $\boldsymbol{A}$ は定係数のベクトル，及び行列．

3.8 ウィルティンガー微分（行列引数の場合）

複素数値をとる関数 f の引数が複素行列 $\boldsymbol{Z}\in\mathbb{C}^{N\times M}$ で与えられる場合，すなわち，$f:\mathbb{C}^{N\times M}\to\mathbb{C}$ を考える．行列 $\boldsymbol{Z}$ の (n,m) 成分を $z_{n,m}$ としたとき，関数 f の $\boldsymbol{Z}$ 及び $\boldsymbol{Z}^*$ によるウィルティンガー微分は次で定義される[3], [19]．

定義 4. ウィルティンガー微分（行列引数の場合）

$$\frac{\partial f}{\partial \boldsymbol{Z}}=\begin{bmatrix}\frac{\partial f}{\partial z_{1,1}} & \frac{\partial f}{\partial z_{2,1}} & \cdots & \frac{\partial f}{\partial z_{N,1}}\\ \frac{\partial f}{\partial z_{1,2}} & \frac{\partial f}{\partial z_{2,2}} & \cdots & \frac{\partial f}{\partial z_{N,2}}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{\partial f}{\partial z_{1,M}} & \frac{\partial f}{\partial z_{2,M}} & \cdots & \frac{\partial f}{\partial z_{N,M}}\end{bmatrix} \tag{55}$$

$$\frac{\partial f}{\partial \boldsymbol{Z}^*}=\begin{bmatrix}\frac{\partial f}{\partial z^*_{1,1}} & \frac{\partial f}{\partial z^*_{2,1}} & \cdots & \frac{\partial f}{\partial z^*_{N,1}}\\ \frac{\partial f}{\partial z^*_{1,2}} & \frac{\partial f}{\partial z^*_{2,2}} & \cdots & \frac{\partial f}{\partial z^*_{N,2}}\\ \vdots & \vdots & \ddots & \vdots\\ \frac{\partial f}{\partial z^*_{1,M}} & \frac{\partial f}{\partial z^*_{2,M}} & \cdots & \frac{\partial f}{\partial z^*_{N,M}}\end{bmatrix} \tag{56}$$

ただし，

$$\frac{\partial f}{\partial z_{n,m}}=\frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},\boldsymbol{n},\boldsymbol{m}}}-j\frac{\partial f}{\partial z_{\mathrm{i},\boldsymbol{n},\boldsymbol{m}}}\right)$$

$$\frac{\partial f}{\partial z^*_{n,m}}=\frac{1}{2}\left(\frac{\partial f}{\partial z_{\mathrm{r},\boldsymbol{n},\boldsymbol{m}}}+j\frac{\partial f}{\partial z_{\mathrm{i},\boldsymbol{n},\boldsymbol{m}}}\right)$$

$$z_{n,m}=z_{\mathrm{r},\boldsymbol{n},\boldsymbol{m}}+jz_{\mathrm{i},\boldsymbol{n},\boldsymbol{m}}\quad(z_{\mathrm{r},\boldsymbol{n},\boldsymbol{m}},z_{\mathrm{i},\boldsymbol{n},\boldsymbol{m}}\in\mathbb{R})$$

ここで，ベクトル引数の場合と同様に，

$$\frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{T}}}=\left(\frac{\partial f}{\partial \boldsymbol{Z}}\right)^{\mathsf{T}},\quad \frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{H}}}=\left(\frac{\partial f}{\partial \boldsymbol{Z}^*}\right)^{\mathsf{T}} \tag{57}$$

としていることに注意する．

N 次元と M 次元の標準基底ベクトル $\boldsymbol{e}_n^N$, $\boldsymbol{e}_m^M$ $(n=1,2,\cdots,N,\ m=1,2,\cdots,M)$ を用いると，行列引数のウィルティンガー微分 $\frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{T}}}$ と $\frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{H}}}$ は

$$\frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{T}}}=\sum_{n=1}^{N}\sum_{m=1}^{M}\boldsymbol{e}_n^N(\boldsymbol{e}_m^M)^{\mathsf{T}}\frac{\partial f}{\partial z_{n,m}} \tag{58}$$

$$\frac{\partial f}{\partial \boldsymbol{Z}^{\mathsf{H}}}=\sum_{n=1}^{N}\sum_{m=1}^{M}\boldsymbol{e}_n^N(\boldsymbol{e}_m^M)^{\mathsf{T}}\frac{\partial f}{\partial z^*_{n,m}} \tag{59}$$

と表すこともできる．

例えば，$\boldsymbol{Z}\in\mathbb{C}^{N\times N}$ とし，関数 f が $\mathrm{tr}(\boldsymbol{Z}^{\mathsf{H}})$ の場合を考えてみる．ただし，$\mathrm{tr}(\cdot)$ はトレースを表す．このとき

$$\frac{\partial(\mathrm{tr}(\boldsymbol{Z}^{\mathsf{H}}))}{\partial z^*_{n,m}}=\begin{cases}1 & (n=m)\\ 0 & (n\neq m)\end{cases} \tag{60}$$

なので，式 (59) に代入すると

$$\frac{\partial(\mathrm{tr}(\boldsymbol{Z}^{\mathsf{H}}))}{\partial \boldsymbol{Z}^{\mathsf{H}}}=\sum_{n=1}^{N}\boldsymbol{e}_n^N(\boldsymbol{e}_n^N)^T=\boldsymbol{I}_N \tag{61}$$

となる．

同様にして，信号処理でよく現れる，次の行列引数の関数のウィルティンガー微分が得られる．

スカラー値行列引数関数のウィルティンガー微分の例

$$\frac{\partial}{\partial \boldsymbol{Z}^{\mathsf{H}}}\left(\mathrm{tr}\left\{\boldsymbol{Z}^{\mathsf{H}}\boldsymbol{A}\right\}\right)=\boldsymbol{A} \tag{62}$$

$$\frac{\partial}{\partial \boldsymbol{Z}^{\mathsf{H}}}\left(\mathrm{tr}\left\{\boldsymbol{A}^{\mathsf{H}}\boldsymbol{Z}\right\}\right)=\boldsymbol{0} \tag{63}$$

$$\frac{\partial}{\partial \boldsymbol{Z}^{\mathsf{H}}}\left(\mathrm{tr}\left\{\boldsymbol{Z}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{Z}\right\}\right)=\boldsymbol{A}\boldsymbol{Z} \tag{64}$$

ただし，$\boldsymbol{A}$ は定係数の行列．

3.9 ウィルティンガー微分の利用例

信号処理では線形逆問題，すなわち，線形観測モデル

$$\boldsymbol{y}=\boldsymbol{A}\boldsymbol{x}+\boldsymbol{v} \tag{65}$$

の逆問題を考えることが多い．ここで，$\boldsymbol{x}\in\mathbb{C}^N$ は推定したい未知ベクトル，$\boldsymbol{y}\in\mathbb{C}^M$ は観測ベクトル，$\boldsymbol{A}\in\mathbb{C}^{M\times N}$ は観測行列，$\boldsymbol{v}\in\mathbb{C}^M$ は白色付加雑音である．線形逆問題の代表的な解法に，最小 2 乗推定と線形 MMSE 推定がある[22]．

3.9.1 最小 2 乗推定

最小 2 乗推定では，推定値 $\hat{\boldsymbol{x}}_{\mathrm{ls}}$ に観測行列 $\boldsymbol{A}$ を乗算したものと観測 $\boldsymbol{y}$ との間の誤差 $\boldsymbol{A}\hat{\boldsymbol{x}}_{\mathrm{ls}}-\boldsymbol{y}$ の ℓ_2 ノルムが最小になるように推定値を選ぶ．つまり，

$$\hat{\boldsymbol{x}}_{\mathrm{ls}}=\arg\min_{\boldsymbol{x}\in\mathbb{C}^N}\|\boldsymbol{A}\boldsymbol{x}-\boldsymbol{y}\|_2^2 \tag{66}$$

なる最適化問題を解くことで推定値を得る．このコスト関数は

$$\begin{aligned}\|\boldsymbol{A}\boldsymbol{x}-\boldsymbol{y}\|_2^2&=(\boldsymbol{A}\boldsymbol{x}-\boldsymbol{y})^{\mathsf{H}}(\boldsymbol{A}\boldsymbol{x}-\boldsymbol{y})\\&=\boldsymbol{x}^{\mathsf{H}}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}-\boldsymbol{x}^{\mathsf{H}}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{y}-\boldsymbol{y}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}+\boldsymbol{y}^{\mathsf{H}}\boldsymbol{y}\end{aligned}$$

となるので，式 (49), (50), (51) を用いることで，コスト関数の $\boldsymbol{x}^{\mathsf{H}}$ についてのウィルティンガー微分は

$$\frac{\partial}{\partial \boldsymbol{x}^{\mathsf{H}}}\|\boldsymbol{A}\boldsymbol{x}-\boldsymbol{y}\|_2^2=\boldsymbol{A}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}-\boldsymbol{A}^{\mathsf{H}}\boldsymbol{y} \tag{67}$$

となる．これが $\boldsymbol{0}$ となる条件から得られる方程式を解くことで，$\boldsymbol{A}$ が列フルランクであるとき，最小 2 乗推定値

$$\hat{\boldsymbol{x}}_{\mathrm{ls}}=(\boldsymbol{A}^{\mathsf{H}}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{y} \tag{68}$$

が得られる．

3.9.2 線形 MMSE 推定

簡単のため，未知ベクトル $\boldsymbol{x}$ の平均を $E[\mathbf{x}]=\mathbf{0}$ とする．ここで，$E[\cdot]$ は期待値を表す．線形 MMSE 推定 $\hat{\boldsymbol{x}}_{\mathrm{mmse}}$ は，観測ベクトル $\boldsymbol{y}$ に重み行列 $\boldsymbol{W}_{\mathrm{mmse}}^{\mathsf{H}}\in\mathbb{C}^{N\times M}$ を乗算することで与えられる．

$$\hat{\boldsymbol{x}}_{\mathrm{mmse}}=\boldsymbol{W}_{\mathrm{mmse}}^{\mathsf{H}}\boldsymbol{y} \tag{69}$$

ただし，$\boldsymbol{W}_{\mathrm{mmse}}$ は次の最適化問題で決定される．

$$\boldsymbol{W}_{\mathrm{mmse}}=\arg\min_{\boldsymbol{W}\in\mathbb{C}^{M\times N}} E\left[\|\boldsymbol{W}^{\mathsf{H}}(\boldsymbol{A}\boldsymbol{x}+\boldsymbol{v})-\boldsymbol{x}\|_2^2\right] \tag{70}$$

この最適化問題のコスト関数は

$$\begin{aligned}
&E\left[(\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}+\boldsymbol{W}^{\mathsf{H}}\boldsymbol{v}-\boldsymbol{x})^{\mathsf{H}}(\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}+\boldsymbol{W}^{\mathsf{H}}\boldsymbol{v}-\boldsymbol{x})\right]\\
&=E\left[\mathrm{tr}\{(\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}+\boldsymbol{W}^{\mathsf{H}}\boldsymbol{v}-\boldsymbol{x})(\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{x}+\boldsymbol{W}^{\mathsf{H}}\boldsymbol{v}-\boldsymbol{x})^{\mathsf{H}}\}\right]\\
&=\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}\right\}+\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}E[\boldsymbol{x}\boldsymbol{v}^{\mathsf{H}}]\boldsymbol{W}\right\}\\
&\quad-\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]\right\}+\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}E[\boldsymbol{v}\boldsymbol{x}^{\mathsf{H}}]\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}\right\}\\
&\quad+\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}E[\boldsymbol{v}\boldsymbol{v}^{\mathsf{H}}]\boldsymbol{W}\right\}-\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}E[\boldsymbol{v}\boldsymbol{x}^{\mathsf{H}}]\right\}\\
&\quad-\mathrm{tr}\left\{E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}\right\}-\mathrm{tr}\left\{E[\boldsymbol{x}\boldsymbol{v}^{\mathsf{H}}]\boldsymbol{W}\right\}+\mathrm{tr}\left\{E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]\right\}\\
&=\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{R}_{\mathrm{x}}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}\right\}-\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{A}\boldsymbol{R}_{\mathrm{x}}\right\}+\sigma_{\mathrm{v}}^2\mathrm{tr}\left\{\boldsymbol{W}^{\mathsf{H}}\boldsymbol{W}\right\}\\
&\quad-\mathrm{tr}\left\{\boldsymbol{R}_{\mathrm{x}}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}\right\}+\mathrm{tr}\left\{\boldsymbol{R}_{\mathrm{x}}\right\}
\end{aligned} \tag{71}$$

と計算できる．ただし，$\boldsymbol{R}_{\mathrm{x}}=E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]$ であり，信号と雑音が無相関であることを仮定し，$E[\boldsymbol{x}\boldsymbol{v}^{\mathsf{H}}]=\mathbf{0}$，$E[\boldsymbol{v}\boldsymbol{x}^{\mathsf{H}}]=\mathbf{0}$ としている．

式 (62), (63), (64) を用いることで，コスト関数の $\boldsymbol{W}^{\mathsf{H}}$ についてウィルティンガー微分が

$$\frac{\partial J_{\mathrm{mmse}}(\boldsymbol{W})}{\partial\boldsymbol{W}^{\mathsf{H}}}=\boldsymbol{A}\boldsymbol{R}_{\mathrm{x}}\boldsymbol{A}^{\mathsf{H}}\boldsymbol{W}-\boldsymbol{A}\boldsymbol{R}_{\mathrm{x}}+\sigma_{\mathrm{v}}^2\boldsymbol{W}=\mathbf{0} \tag{72}$$

と求まる．これが $\mathbf{0}$ となる条件から得られる方程式を解くことで，線形 MMSE 推定の重み行列

$$\boldsymbol{W}_{\mathrm{mmse}}^{\mathsf{H}}=\boldsymbol{R}_{\mathrm{x}}\boldsymbol{A}^{\mathsf{H}}\left(\boldsymbol{A}\boldsymbol{R}_{\mathrm{x}}\boldsymbol{A}^{\mathsf{H}}+\sigma_{\mathrm{v}}^2\boldsymbol{I}_M\right)^{-1} \tag{73}$$

が得られる．

4. 広義線形フィルタ

4.1 広義線形変換

式 (1) で定義される $2N$ 次元の実数拡張ベクトル $\bar{\boldsymbol{z}}$ に，実行列

$$\boldsymbol{M}=\begin{bmatrix}\boldsymbol{M}_{11} & \boldsymbol{M}_{12}\\ \boldsymbol{M}_{21} & \boldsymbol{M}_{22}\end{bmatrix}\in\mathbb{R}^{2M\times 2N} \tag{74}$$

を左から乗算することによる実線形変換を考えると，その結果は $2M$ 次元の実数拡張ベクトルで与えられる．

$$\bar{\boldsymbol{y}}=\begin{bmatrix}\boldsymbol{y}_{\mathrm{r}}\\ \boldsymbol{y}_{\mathrm{i}}\end{bmatrix}=\begin{bmatrix}\boldsymbol{M}_{11} & \boldsymbol{M}_{12}\\ \boldsymbol{M}_{21} & \boldsymbol{M}_{22}\end{bmatrix}\begin{bmatrix}\boldsymbol{z}_{\mathrm{r}}\\ \boldsymbol{z}_{\mathrm{i}}\end{bmatrix}=\boldsymbol{M}\bar{\boldsymbol{z}} \tag{75}$$

ここで，$\boldsymbol{M}_{11},\boldsymbol{M}_{12},\boldsymbol{M}_{21},\boldsymbol{M}_{22}\in\mathbb{R}^{M\times N}$ である．

一方，実数拡張ベクトル $\bar{\boldsymbol{y}}$ に対応する複素拡張ベクトルは，式 (7) より

$$\underline{\boldsymbol{y}}=\boldsymbol{T}_M\bar{\boldsymbol{y}}=\boldsymbol{T}_M\boldsymbol{M}\bar{\boldsymbol{z}}=\boldsymbol{T}_M\boldsymbol{M}\left(\frac{1}{2}\boldsymbol{T}_N^{\mathsf{H}}\underline{\boldsymbol{z}}\right)=\boldsymbol{H}\underline{\boldsymbol{z}} \tag{76}$$

と書くことができる．ただし，

$$\boldsymbol{H}=\frac{1}{2}\boldsymbol{T}_M\boldsymbol{M}\boldsymbol{T}_N^{\mathsf{H}} \tag{77}$$

である．ここで，行列 $\boldsymbol{H}$ は

$$\boldsymbol{H}_1=\frac{1}{2}\left\{\boldsymbol{M}_{11}+\boldsymbol{M}_{22}+j(\boldsymbol{M}_{21}-\boldsymbol{M}_{12})\right\} \tag{78}$$

$$\boldsymbol{H}_2=\frac{1}{2}\left\{\boldsymbol{M}_{11}-\boldsymbol{M}_{22}+j(\boldsymbol{M}_{21}+\boldsymbol{M}_{12})\right\} \tag{79}$$

と定義すると

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{H}_1 & \boldsymbol{H}_2\\ \boldsymbol{H}_2^* & \boldsymbol{H}_1^*\end{bmatrix} \tag{80}$$

と書くことができるので，広義線形 (widely linear) 変換[3), (6), (7)]

$$\boldsymbol{y}=\boldsymbol{H}_1\boldsymbol{z}+\boldsymbol{H}_2\boldsymbol{z}^*=\begin{bmatrix}\boldsymbol{H}_1 & \boldsymbol{H}_2\end{bmatrix}\underline{\boldsymbol{z}} \tag{81}$$

の複素拡張行列と呼ばれる．また，3.9 節で考えたような最小二乗推定や線形 MMSE 推定などの線形フィルタリングは，広義線形変換の式 (81) で $\boldsymbol{H}_2=\mathbf{0}$ とした特別な場合の変換

$$\boldsymbol{y}=\boldsymbol{H}_1\boldsymbol{z} \tag{82}$$

とみなすことができ，これは狭義線形 (strictly linear) 変換と呼ばれる．

4.2 複素確率ベクトルの統計的性質

N 次元の複素確率変数 $\boldsymbol{z}=\boldsymbol{z}_{\mathrm{r}}+j\boldsymbol{z}_{\mathrm{i}}$ $(\boldsymbol{z}_{\mathrm{r}},\boldsymbol{z}_{\mathrm{i}}\in\mathbb{R}^N)$ が零平均であるとし，その実数拡張ベクトルを $\bar{\boldsymbol{z}}=[\boldsymbol{z}_{\mathrm{r}}^{\mathsf{T}},\boldsymbol{z}_{\mathrm{i}}^{\mathsf{T}}]^{\mathsf{T}}$，複素拡張ベクトルを $\underline{\boldsymbol{z}}=[\boldsymbol{z}^{\mathsf{T}},\boldsymbol{z}^{\mathsf{H}}]^{\mathsf{T}}$ とする．

実数拡張ベクトル $\bar{\boldsymbol{z}}$ の共分散行列は次で与えられる．

$$\boldsymbol{C}_{\bar{\boldsymbol{z}}\bar{\boldsymbol{z}}}=E[\bar{\boldsymbol{z}}\bar{\boldsymbol{z}}^{\mathsf{T}}]=\begin{bmatrix}\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}} & \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}\\ \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}^{\mathsf{T}} & \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}}\end{bmatrix} \tag{83}$$

ただし，$\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}}=E[\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}^{\mathsf{T}}]$，$\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}=E[\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}^{\mathsf{T}}]$，$\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}}=E[\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}^{\mathsf{T}}]$ である．

一方，複素拡張ベクトル $\underline{\boldsymbol{z}}$ の共分散行列は拡張共分散行列 (augmented covariance matrix) と呼ばれ，次で与えられる．

$$\underline{\boldsymbol{C}}_{\boldsymbol{z}\boldsymbol{z}}=E[\underline{\boldsymbol{z}}\,\underline{\boldsymbol{z}}^{\mathsf{H}}]=\begin{bmatrix}\boldsymbol{C}_{\boldsymbol{z}\boldsymbol{z}} & \tilde{\boldsymbol{C}}_{\boldsymbol{z}\boldsymbol{z}}\\ \tilde{\boldsymbol{C}}_{\boldsymbol{z}\boldsymbol{z}}^* & \boldsymbol{C}_{\boldsymbol{z}\boldsymbol{z}}^*\end{bmatrix} \tag{84}$$

ただし，$\boldsymbol{C}_{\boldsymbol{z}\boldsymbol{z}}=E[\boldsymbol{z}\boldsymbol{z}^{\mathsf{H}}]$ は通常の共分散行列であり，よく知られているように半正定値のエルミート行列である[22)]．また，

$\tilde{\boldsymbol{C}}_{\boldsymbol{zz}} = E[\boldsymbol{z}\boldsymbol{z}^{\mathsf{T}}]$ は補共分散行列 (complementary covariance matrix) や疑似共分散行列 (pseudo covariance matrix) と呼ばれ[1]，定義より対称行列であることから，$\underline{\boldsymbol{C}}_{\boldsymbol{zz}}$ がエルミート行列であることが分かる．一般に，$\boldsymbol{z}$ の完全な二次統計量を得るためには，$\boldsymbol{C}_{\boldsymbol{zz}}$ と $\tilde{\boldsymbol{C}}_{\boldsymbol{zz}}$ の両方の情報が必要である．実数拡張ベクトルの共分散行列 $\boldsymbol{C}_{\tilde{\boldsymbol{z}}\tilde{\boldsymbol{z}}}$ と複素拡張ベクトルの共分散行列 $\underline{\boldsymbol{C}}_{\boldsymbol{zz}}$ の間には，

$$\underline{\boldsymbol{C}}_{\boldsymbol{zz}} = \boldsymbol{T}_N \boldsymbol{C}_{\tilde{\boldsymbol{z}}\tilde{\boldsymbol{z}}} \boldsymbol{T}_N^{\mathsf{H}} \tag{85}$$

なる関係があり，

$$\boldsymbol{C}_{\boldsymbol{zz}} = \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}} + \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}} + j(\boldsymbol{C}^{\mathsf{T}}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}} - \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}) \tag{86}$$

$$\tilde{\boldsymbol{C}}_{\boldsymbol{zz}} = \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}} - \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}} + j(\boldsymbol{C}^{\mathsf{T}}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}} + \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}) \tag{87}$$

と書ける．

$\tilde{\boldsymbol{C}}_{\boldsymbol{zz}} = \boldsymbol{0}$ であるような確率変数 $\boldsymbol{z}$ はプロパー (proper)[3],[4] と呼ばれ，このとき，拡張共分散行列 $\underline{\boldsymbol{C}}_{\boldsymbol{zz}}$ はブロック対角行列になる．式 (87) より，確率変数 $\boldsymbol{z}$ がプロパーであるための条件は，$\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{r}}} = \boldsymbol{C}_{\boldsymbol{z}_{\mathrm{i}}\boldsymbol{z}_{\mathrm{i}}}$，$\boldsymbol{C}^{\mathsf{T}}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}} = -\boldsymbol{C}_{\boldsymbol{z}_{\mathrm{r}}\boldsymbol{z}_{\mathrm{i}}}$ と書くこともできる．

プロパー性をある意味でより強くした性質に，円対称性 (circularity)[2],[3]がある．確率変数 $\boldsymbol{z}$ は，その確率密度関数が回転不変であるとき，すなわち，任意の $\theta \in \mathbb{R}$ について $\boldsymbol{z}$ と $\boldsymbol{z}' = e^{j\theta}\boldsymbol{z}$ が同じ確率密度関数をもつとき，円対称 (circular) と呼ばれる．通常の共分散行列は

$$\boldsymbol{C}_{\boldsymbol{z}'\boldsymbol{z}'} = E[\boldsymbol{z}'(\boldsymbol{z}')^{\mathsf{H}}] = E[e^{j\theta}\boldsymbol{z}e^{-j\theta}\boldsymbol{z}^{\mathsf{H}}] = \boldsymbol{C}_{\boldsymbol{zz}} \tag{88}$$

となるので，確率変数が円対称であるかどうかにかかわらず回転不変である．一方，補共分散行列は

$$\tilde{\boldsymbol{C}}_{\boldsymbol{z}'\boldsymbol{z}'} = E[\boldsymbol{z}'(\boldsymbol{z}')^{\mathsf{T}}] = E[e^{j\theta}\boldsymbol{z}e^{j\theta}\boldsymbol{z}^{\mathsf{T}}] = e^{j2\theta}\tilde{\boldsymbol{C}}_{\boldsymbol{zz}} \tag{89}$$

となるので，これが回転不変になるのは $\tilde{\boldsymbol{C}}_{\boldsymbol{zz}}$（つまり，プロパー）のときで，またそのときにかぎる．したがって，プロパー性は二次のモーメントまでの回転不変性を要請したものと考えることができる．これに対し，円対称性はより高次のモーメントに対しても回転不変性を要請するものであり，「円対称ならばプロパー」は成り立つが，「プロパーならば円対称」は一般に成り立たない．ただし，ガウス分布は二次の統計量までで確率密度関数が定まるので，平均 $\boldsymbol{0}$ でプロパーな複素ガウス確率変数は円対称となる[23]．

4.3 広義線形フィルタ

スカラーの確率変数 y の推定値 $\hat{y}$ を，N 次元の複素数の観測ベクトル $\boldsymbol{x}$ を入力とする広義線形フィルタ

$$\hat{y} = \boldsymbol{u}^{\mathsf{H}}\boldsymbol{x} + \boldsymbol{v}^{\mathsf{H}}\boldsymbol{x}^* \tag{90}$$

によって得る問題を考える．ただし，$\boldsymbol{u}, \boldsymbol{v} \in \mathbb{C}^N$ は重みベクトルであり，次のコスト関数を最小にするように決定される．

$$\begin{aligned} J_{\mathrm{WL}}(\boldsymbol{u},\boldsymbol{v}) &= E[|y-\hat{y}|^2] \\ &= E[(y-\boldsymbol{u}^{\mathsf{H}}\boldsymbol{x}-\boldsymbol{v}^{\mathsf{H}}\boldsymbol{x}^*)(y-\boldsymbol{u}^{\mathsf{H}}\boldsymbol{x}-\boldsymbol{v}^{\mathsf{H}}\boldsymbol{x}^*)^{\mathsf{H}}] \\ &= E[|y|^2] - \boldsymbol{c}_{\boldsymbol{x}y}^{\mathsf{H}}\boldsymbol{u} - \tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{\mathsf{T}}\boldsymbol{v} - \boldsymbol{u}^{\mathsf{H}}\boldsymbol{c}_{\boldsymbol{x}y} + \boldsymbol{u}^{\mathsf{H}}\boldsymbol{C}_{\boldsymbol{xx}}\boldsymbol{u} \\ &\quad + \boldsymbol{u}^{\mathsf{H}}\tilde{\boldsymbol{C}}_{\boldsymbol{xx}}\boldsymbol{v} - \boldsymbol{v}^{\mathsf{H}}\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*} + \boldsymbol{v}^{\mathsf{H}}\tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}\boldsymbol{u} + \boldsymbol{v}^{\mathsf{H}}\boldsymbol{C}_{\boldsymbol{xx}}^{*}\boldsymbol{v} \end{aligned} \tag{91}$$

ただし，$\boldsymbol{C}_{\boldsymbol{xx}} = E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{H}}]$，$\tilde{\boldsymbol{C}}_{\boldsymbol{xx}} = E[\boldsymbol{x}\boldsymbol{x}^{\mathsf{T}}]$，$\boldsymbol{c}_{\boldsymbol{x}y} = E[\boldsymbol{x}y^*]$，$\tilde{\boldsymbol{c}}_{\boldsymbol{x}y} = E[\boldsymbol{x}y]$ である．

コスト関数 $J_{\mathrm{WL}}(\boldsymbol{u},\boldsymbol{v})$ を $\boldsymbol{u}^{\mathsf{H}}$ 及び $\boldsymbol{v}^{\mathsf{H}}$ でウィルティンガー微分すると

$$\frac{\partial J_{\mathrm{WL}}}{\partial \boldsymbol{u}^{\mathsf{H}}} = -\boldsymbol{c}_{\boldsymbol{x}y} + \boldsymbol{C}_{\boldsymbol{xx}}\boldsymbol{u} + \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}\boldsymbol{v} \tag{92}$$

$$\frac{\partial J_{\mathrm{WL}}}{\partial \boldsymbol{v}^{\mathsf{H}}} = -\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*} + \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}\boldsymbol{u} + \boldsymbol{C}_{\boldsymbol{xx}}^{*}\boldsymbol{v} \tag{93}$$

となる．これらが $\boldsymbol{0}$ となる条件から，コスト関数を最小にする重みベクトルは，$\boldsymbol{x}$ の拡張共分散行列を用いて

$$\begin{aligned} \begin{bmatrix}\boldsymbol{u}\\ \boldsymbol{v}\end{bmatrix} &= \begin{bmatrix}\boldsymbol{C}_{\boldsymbol{xx}} & \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}\\ \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*} & \boldsymbol{C}_{\boldsymbol{xx}}^{*}\end{bmatrix}^{-1}\begin{bmatrix}\boldsymbol{c}_{\boldsymbol{x}y}\\ \tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*}\end{bmatrix} \\ &= \begin{bmatrix}\boldsymbol{P}_{\boldsymbol{xx}}^{-1}(\boldsymbol{c}_{\boldsymbol{x}y} - \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}(\boldsymbol{C}_{\boldsymbol{xx}}^{*})^{-1}\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*})\\ (\boldsymbol{P}_{\boldsymbol{xx}}^{*})^{-1}(\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*} - \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}\boldsymbol{C}_{\boldsymbol{xx}}^{-1}\boldsymbol{c}_{\boldsymbol{x}y})\end{bmatrix} \end{aligned} \tag{94}$$

と得られる．ただし，$\boldsymbol{P}_{\boldsymbol{xx}} = \boldsymbol{C}_{\boldsymbol{xx}} - \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}(\boldsymbol{C}_{\boldsymbol{xx}}^{*})^{-1}\tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}$ は $\boldsymbol{x}$ の拡張共分散行列中の $\boldsymbol{C}_{\boldsymbol{xx}}^{*}$ のシューア補行列[24]である．また，$\boldsymbol{C}_{\boldsymbol{xx}}$ と $\boldsymbol{x}$ の拡張共分散行列はいずれも可逆であるとしている．

比較のために，同じ推定問題を狭義線形フィルタ $\hat{y}' = \boldsymbol{w}^{\mathsf{H}}\boldsymbol{x}$ で解くことを考える．コスト関数を $J_{\mathrm{SL}}(\boldsymbol{w}) = E[|y-\hat{y}'|^2]$ と定義すると，これを最小にする重みベクトル $\boldsymbol{w}$ は

$$\boldsymbol{w} = \boldsymbol{C}_{\boldsymbol{xx}}^{-1}\boldsymbol{c}_{\boldsymbol{x}y} \tag{95}$$

と得られる．狭義線形フィルタで式 (95) の重みベクトルを用いたときのコスト関数値 $J_{\mathrm{SL,opt}}$ と広義線形フィルタで式 (94) の重みベクトルを用いたときのコスト関数値 $J_{\mathrm{WL,opt}}$ の差は

$$\begin{aligned} &J_{\mathrm{SL,opt}} - J_{\mathrm{WL,opt}} \\ &= (\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*} - \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}\boldsymbol{C}_{\boldsymbol{xx}}^{-1}\boldsymbol{c}_{\boldsymbol{x}y})^{\mathsf{H}}(\boldsymbol{P}_{\boldsymbol{xx}}^{*})^{-1}(\tilde{\boldsymbol{c}}_{\boldsymbol{x}y}^{*} - \tilde{\boldsymbol{C}}_{\boldsymbol{xx}}^{*}\boldsymbol{C}_{\boldsymbol{xx}}^{-1}\boldsymbol{c}_{\boldsymbol{x}y}) \end{aligned}$$

となる．$\boldsymbol{C}_{\boldsymbol{xx}}$ と $\boldsymbol{x}$ の拡張共分散行列はいずれも相関行列で非負定値なので，シューア補行列 $\boldsymbol{P}_{\boldsymbol{xx}}$ も非負定値となり[24]，このエルミート形式は非負となる．これより，広義線形フィルタで達成される平均 2 乗誤差は狭義線形フィルタで達成される平均 2 乗誤差以下になることが分かる．また，$\tilde{\boldsymbol{C}}_{\boldsymbol{xx}} = \boldsymbol{0}$，$\tilde{\boldsymbol{c}}_{\boldsymbol{x}y} = \boldsymbol{0}$ のときは $J_{\mathrm{SL,opt}} = J_{\mathrm{WL,opt}}$ となることから，プロパーな信号を扱う場合には，広義線形フィルタと狭義線形フィルタの平均 2 乗誤差性能が同一であることが分かる．

4.4 広義線形フィルタの応用例

通信では，正弦波で表現される搬送波の cos 成分と sin 成分に載せる信号を，オイラーの公式を用いてそれぞれ複素数の実部と虚部に対応づけるが，実際の通信システムではハードウェアの不完全性などから cos 成分と sin 成分の振幅や位相が理想

的な値からずれてしまうことがある．このような問題は IQ 不均衡と呼ばれる．ここでは，広義線形フィルタが活躍する代表的な例として，通信システムの IQ 不均衡対策[14],[15]を取り上げる．

理想的な N 次元の複素信号ベクトルを $\boldsymbol{x} = \boldsymbol{x}_\mathrm{r} + j\boldsymbol{x}_\mathrm{i}$, $(\boldsymbol{x}_\mathrm{r}, \boldsymbol{x}_\mathrm{i} \in \mathbb{R}^N)$ とすると IQ 不均衡でひずんだ信号 $\check{\boldsymbol{x}}$ は

$$\begin{aligned}\check{\boldsymbol{x}} =&(1+\eta)\cos\phi\ \boldsymbol{x}_\mathrm{r} - j(1-\eta)\sin\phi\ \boldsymbol{x}_\mathrm{r}\\ &+ j(1-\eta)\cos\phi\ \boldsymbol{x}_\mathrm{i} - (1+\eta)\sin\phi\ \boldsymbol{x}_\mathrm{i}\end{aligned} \tag{96}$$

で与えられる．ただし，$\phi, \eta \in \mathbb{R}$ は，それぞれ位相と振幅のずれを表す．ここで，

$$\alpha = \cos\phi + j\eta\sin\phi \tag{97}$$

$$\beta = \eta\cos\phi - j\sin\phi \tag{98}$$

とすると，IQ 不均衡でひずんだ信号は，広義線形変換を用いて

$$\check{\boldsymbol{x}} = \alpha\boldsymbol{x} + \beta\boldsymbol{x}^* \tag{99}$$

と表すことができる．

IQ 不均衡でひずんだ信号はプロパーではないので，広義線形フィルタを用いて

$$\hat{\boldsymbol{x}} = \boldsymbol{W}_1^\mathsf{H}\check{\boldsymbol{x}} + \boldsymbol{W}_2^\mathsf{H}\check{\boldsymbol{x}}^* \tag{100}$$

と補償することができる．ただし，$\boldsymbol{W}_1, \boldsymbol{W}_2 \in \mathbb{C}^{N\times N}$ である．簡単のため，重み行列 $\boldsymbol{W}_1, \boldsymbol{W}_2$ を ZF (zero-forcing) 基準で決定することにすると，

$$\begin{bmatrix}\check{\boldsymbol{x}}\\ \check{\boldsymbol{x}}^*\end{bmatrix} = \begin{bmatrix}\alpha\boldsymbol{I}_N & \beta\boldsymbol{I}_N\\ \beta^*\boldsymbol{I}_N & \alpha^*\boldsymbol{I}_N\end{bmatrix}\begin{bmatrix}\boldsymbol{x}\\ \boldsymbol{x}^*\end{bmatrix} \tag{101}$$

なので，重み行列は

$$\boldsymbol{W}_1^\mathsf{H} = \frac{\alpha^*}{\alpha\alpha^* - \beta\beta^*}\boldsymbol{I}_M \tag{102}$$

$$\boldsymbol{W}_2^\mathsf{H} = \frac{\beta}{\beta\beta^* - \alpha\alpha^*}\boldsymbol{I}_M \tag{103}$$

で与えられる．

5. むすび

本稿では，複素数を扱う信号処理の基礎事項について解説した．特に，信号処理や機械学習ではコスト関数の最小化などで，複素数の引数をもつ実数値関数を扱うことが多いため，そのような関数の複素勾配を容易に計算可能な手法であるウィルティンガー微分について説明した．更に，円対称性をもたないような複素信号を扱う際に必要となる，広義線形フィルタの基礎事項についても説明した．これらの複素信号処理の柱をなす手法に共通するアイデアは，複素数の信号とその複素共役を独立に扱うという，一見無駄に思える信号の表現方法であり，この表現方法が正則でない関数の微分の定義を与えたり，プロパーでない信号を複素数のままで効率的に処理することを可能にしている．

ウィルティンガー微分や複素信号の解析に関する説明は，以前は(16)，(25) などの一部の解析学の教科書や(26)，(27) などの信号処理の教科書の付録ぐらいしかなかったが，最近では優れた書籍[3],[19]や，解説論文[4],[5],[20],[28],[29]が多数ある．本稿では信号処理や機械学習での応用を想定し，ウィルティンガー微分の対象をスカラー値の複素関数に限定したが，ベクトル値や行列値をとる複素関数のウィルティンガー微分などについてはこれらの文献を参照されたい．また，拙著[22]でもウィルティンガー微分について解説しており，本稿よりも基礎的な内容からウィルティンガー微分を導入しているので，本稿が読みにくい方はそちらも参照頂きたい．

文　献

(1) F.D. Neeser and J.L. Massey, “Proper complex random processes with applications to information theory,” IEEE Trans. Inf. Theory, vol.39, no.4, pp.1293–1302, July 1993.
(2) B. Picinbono, “On circularity,” IEEE Trans. Signal Process., vol.42, no.12, pp.3473–3482, Dec. 1994.
(3) P.J. Schreier and L.L. Scharf, Statistical Signal Processing of Complex-Valued Data, Cambridge University Press, 2010.
(4) T. Adali, P.J. Schreier, and L.L. Scharf, “Complex-valued signal processing: the proper way to deal with impropriety,” IEEE Trans. Signal Process., vol.59, no.11, pp.5101–5123, Nov. 2011.
(5) T. Adali and P.J. Schreier, “Optimization and estimation of complex-valued signals: theory and applications in filtering and blind source separation,” IEEE Signal Process. Mag., vol.31, no.5, pp.112–128, Aug. 2014.
(6) W.M. Brown and R.B. Crane, “Conjugate linear filtering,” IEEE Trans. Inf. Theory, vol.15, no.4, pp.462–465, 1969.
(7) B. Picinbono and P. Chevalier, “Widely linear estimation with complex data,” IEEE Trans. Signal Process., vol.43, no.8, pp.2030–2033, Aug. 1995.
(8) W. Wirtinger, “Zur formalen theorie der funktionen von mehr komplexen veranderlichen,” Math. Ann., vol.97, no.1, pp.357–375, Dec. 1927.
(9) A.G. Baydin, B.A. Pearlmutter, A.A. Radul, J.M. Siskind, “Automatic differentiation in machine learning: a survey,” Journal of Machine Learning Research, vol.18, pp.5595–5637, April 2018.
(10) N. Krämer, “A tutorial on automatic differentiation with complex numbers,” arXiv preprint, arXiv:2409.06752v3, 2024.
(11) S. Takabe, M. Imanishi, T. Wadayama, R. Hayakawa, and K. Hayashi, “Trainable projected gradient detector for massive overloaded MIMO channels: data-driven tuning approach,” IEEE Access, vol.7, pp.93326–93338, Dec. 2019.
(12) M. Arikawa and K. Hayashi, “Adaptive equalization of transmitter and receiver IQ skew by multi-layer linear and widely linear filters with deep unfolding,” Optics Express, vol.28, no.16, pp.23478–23494, July 2020.
(13) 和田山正，モデルベース深層学習と深層展開，森北出版，東京，2023.
(14) Y. Yoshida, K. Hayashi, H. Sakai, and W. Bocquet, “Analysis and compensation of transmitter IQ imbalances in OFDMA and SC-FDMA systems,” IEEE Trans. Signal Process., vol.57, no.8, pp.3119–3129, Aug. 2009.
(15) L. Wei, K. Hayashi and T. Wadayama, “Learnable

multi-layer structure for joint Tx/Rx IQIs and CFO compensation in OFDM system," 2025 IEEE Globecom Workshops (GC Wkshps), Taipei, Taiwan, pp.1–6, Dec. 2025.
(16) R. Remmert, Theory of Complex Functions, Springer Science & Business Media, 1991.
(17) 山本直樹，複素関数論の基礎，裳華房，2015.
(18) 小林昭七，続 微分積分読本 多変数，裳華房，東京，2001.
(19) A. Hjørungnes, Complex-Valued Matrix Derivatives, Cambridge University Press, 2011.
(20) K. Koor, Y. Qiu, L.C. Kwek, and P. Rebentrost, "A short tutorial on Wirtinger calculus with applications in quantum information," arXiv preprint, arXiv:2312.04858v1, 2023.
(21) 小島紀男，矢沢志雄作，本間光一，マトリクスとシステム，東海大学出版会，1990.
(22) 林和則，通信の信号処理，コロナ社，東京，2023.
(23) T. Grettenberg, "Representation theorem for complex normal processes," IEEE Trans. Inf. Theory, vol.11, no.2, pp.305–306, April 1965.
(24) R.L. Smith, "Some interlacing properties of the Schur complement of a Hermitian matrix," Linear Algebra and its Applications, vol.177, pp.137–144, Dec. 1992.
(25) L. Schwartz，シュヴァルツ解析学 6 複素関数，東京図書，東京，1971.
(26) T. Kailath, A. Sayed, and B. Hassibi, Linear Estimation, Prentice Hall, 2000.
(27) S. Haykin, Adaptive Filter Theory, 3rd Edition, Prentice Hall, 1996.
(28) R. Hunger, "An introduction to complex differentials and complex differentiability," Technical Report TUM-LNS-TR-07-06, Technical University of Munich, 2007.
(29) C. Candan, "Properly handling complex differentiation in optimization and approximation problems," IEEE Signal Process. Mag., vol.36, no.2, pp.117–124, March 2019.

（SIP 研究会提案，2026 年 3 月 9 日受付，
2026 年 3 月 31 日再受付）

林　和則（正員）

1997 阪大工学部通信工学科卒．2002 同大大学院博士後期課程了．同年京大大学院情報学研究科助手．2009 同准教授．2017 阪市大大学院工学研究科教授．2020 京大国際高等教育院教授．2026 同大大学院情報学研究科教授．無線通信，統計的信号処理の研究に従事．2009 ICF 優秀研究賞，2009 Globecom Best Paper Award，2011 通ソ Best Paper Award，2012 電気通信普及財団テレコムシステム技術賞，2014 通ソ Best Tutorial Paper Award，2021 APSIPA ASC Best Paper Award，2024 教育功労賞，2024 電気通信普及財団テレコムシステム技術賞受賞．

ESS ニュース

NOLTA, IEICE 特集号

Guest Secretary　加藤秀行

特集号タイトル：

Special Section on Nonlinear Theory and Its Applications

掲載号：

NOLTA IEICE, 2026 年 7 月発行

電子情報通信学会 NOLTA ソサイエティでは，フラグシップ会議として非線形理論とその応用に関する国際シンポジウム（International Symposium on Nonlinear Theory and Its Applications）を毎年開催しております．沖縄で開催された 2025 年の同シンポジウムでは，カオス理論や分岐理論などの非線形現象に関する研究や深層学習や進化計算などの計算知能に関する研究をはじめ，非線形システムや通信ネットワークなどの工学的応用に関する研究から神経ダイナミクスや社会ダイナミクスなどの複雑系に関する研究に至るまで幅広い研究分野における最先端の成果が発表されました．

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誌として広く発信することを目的に企画されたものです．上記シンポジウムで発表された成果に限らず，本特集号へは様々な分野からたくさんのご投稿を頂きました．本特集に投稿された全ての論文は，通常の NOLTA, IEICE 誌と同様のプロセスにて審査されました．その結果，37 件の論文が掲載されることとなりました．これら採択論文は，J-STAGE（https://www.jstage.jst.go.jp/browse/nolta/）にて無料でご覧頂けます．

末筆ながら，本特集号の企画並びに編集作業にあたり，ご尽力頂きました Guest Editorial Board 及び NOLTA 編集局，IEICE 事務局各位，そして，論文を投稿頂きました著者の皆々様に心より御礼申し上げます．

加藤秀行（正員）

平 19 埼玉大工・情報卒．平 23 同大学大学院博士後期課程了．同年学振 PD 研究員．平 24 UIB IFISC 博士研究員，埼玉大理工学研究科研究員（兼務）．平 25 お茶大特任リサーチフェロー．平 26 東京工科大助教．平 29 大分大助教．平 30 同大学講師．令 6 同大学准教授．数理神経科学や非線形力学系理論に関する研究に従事．平成 19 年度学術奨励賞．

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？

■信号処理研究会（SIP）

信号処理研究会（SIP 研究会）は，信号処理に関する基礎理論から応用まで幅広い分野の研究を取り扱う研究会です．本研究会を主催する信号処理研究専門委員会（SIP 研専）には，「数理・学習」，「音声・音響」，「画像」，「通信」の四つのグループがあり，信学会内外の関連する研究会と協力して活動しています．

2026 年度は以下の 4 回の研究会を開催予定です．最新情報は，信学会，及び，SIP 研専の Web サイトでご確認ください．

2026 年 6 月 22 日（月）～23 日（火）鳥取県立生涯学習センター（IE，MI，BioX，ITE-ME，ITE-IST 共催）
2026 年 8 月 27 日（木）～28 日（金）伊香保温泉森秋旅館（SIP 単独開催）
2027 年 1 月頃開催日・場所未定（IT，RCS 共催）
2027 年 3 月頃開催日・場所未定（SPEASIP ; SP，EA，APSIPA-JC 共催，IPSJ-SLP 連催）

これらに加えて，毎年，信号処理に関する国内最大規模のイベントとして「信号処理シンポジウム」を開催しており，例年，招待講演やチュートリアル講演をはじめ，100 件以上の研究発表が行われています．今年度は，12 月 2 日（水）～4 日（金）に，広島市文化交流会館で開催予定です．多数のご発表・ご参加をお待ちしております．

田中　章（正員）
1996 北海道大学修士課程修了．1996 松下通信工業（株）入社．2000 北海道大学博士課程修了．現在，北海道大学大学院情報科学研究院・教授．主に，信号処理・機械学習の理論研究に従事．信号処理研究専門委員会委員長．IEEE，ASJ 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，設立当初から，暗号・情報セキュリティの基礎理論から実社会への応用に至る多様な研究の振興と，セキュリティ研究者・技術者が所属組織を超えて研究課題を真摯に議論できる開かれた機会の提供を目的としており，第一種研究会，第二種研究会（WCIS），国内シンポジウム（SCIS），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 月に開催しています．特に，5 月の研究会では，国際会議で論文発表した若手研究者による招待講演を企画して，世代を超えた活発な議論を目指しています．そして，7 月の研究会は，これまで，電子情報通信学会 6 研究会（ISEC/SITE/ICSS/EMM/HMS/BioX）と情報処理学会の 2 研究会（CSEC/SPT）の共催によって，通称「セキュリティサマーサミット（SSS）」と呼ばれて大規模に開催されてきましたが，今年度からは，新たに人工知能学会の安全性とセキュリティ研究会（SIG-SEC）も加わって，更に広範囲の研究者による活発な議論の場となります．また，9 月に開催する第二種研究会の「暗号と情報セキュリティワークショップ（WCIS）」では，世界トップクラスの国際会議に採録された論文の著者による招待講演を毎年企画して，第一線の研究者との交流の機会を創り出しています．

ISEC は，「暗号と情報セキュリティシンポジウム（SCIS）」を毎年 1 月に開催していますが，SCIS は，セキュリティ分野における国内最大級のシンポジウムとして，前回は，ついに 1000 名を超える参加者を集めるに至りました．更に毎年，CSEC と共催で国際会議 IWSEC（International Workshop on Security）を国内で開催しており，今年は 11 月に東京で開催予定です．以上の研究集会の詳細については，ISEC の Web サイト（https://www.ieice.org/ess/isec/index.html）でご確認ください．我が国の将来を担う研究者・技術者の皆様の積極的なご参加をお待ちしています．

高島克幸（正員：フェロー）
1995 京大大学院理学研究科修士課程了．1997 三菱電機株式会社入社．2021 早稲田大学教育・総合科学学術院教授．暗号理論とそれに関連する計算数論の研究に従事．IEICE 論文賞（2015，2016 年度），JSIAM 論文賞（2003，2016 年度）を受賞．2016-2017 年度 JSIAM 副会長．2026 年度 ISEC 専門委員長．博士（情報学）．IEICE，IACR，JSIAM，MSJ，IPSJ 各会員．

■高信頼制御通信研究会（RCC）

IoT やサイバーフィジカルシステム，フィジカル AI を考える上で，通信と制御は密接に関係しています．高信頼制御通信（RCC）研究会は，制御のための通信，通信の特徴を考慮した制御，通信と制御が融合したシステムなど通信と制御の境界領域の発展を目指しています．特に，AI をリアルタイムで利用するフィジカル AI では，通信の特徴を考慮して制御系設計を検討する必要があります．本研究会が扱う分野が今まさに重要となっているといえます．

研究会は年 4 回開催しています．学生や若手研究者向けの研究奨励賞も表彰しています．名前が少し堅苦しいかもしれませんが，通信の研究者，制御の研究者，通信と制御を使う研究者など幅広い分野の皆様と気軽に議論できる研究会になっています．皆様のご参加をお待ちしております．

Web ページ：https://www.ieice.org/~rcc/

図 1　奨励賞授与の様子

小林孝一（正員）
2000 法政大学大学院工学研究科修士課程修了．2000～2004 新日本製鐵(株)勤務．2007 東京工業大学大学院情報理工学研究科博士後期課程修了．同年北陸先端科学技術大学院大学情報科学研究科助教，2015 北海道大学大学院情報科学研究科准教授，2019 同大学院情報科学研究院准教授，2023 同教授となり現在に至る．システム制御理論とその応用の研究に従事．

■複雑コミュニケーションサイエンス研究専門委員会（CCS）

複雑コミュニケーションサイエンス研究専門委員会（CCS 研究会）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．2026 年度は常設研究専門委員会として 12 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．

CCS 研究会では，毎年 4 回の研究会を開催しています．2025 年度は，6 月に岡山県，7 月に北海道，11 月に石川県，3 月に北海道で研究会が開催されました．更に 2026 年 3 月の総合大会において，「光無線通信の可能性と次なる展開―可視光通信・Li-Fi は次のブレイクスルーとなるか？―」というシンポジウムセッションを企画し，4 名の素晴らしい講演者の皆様にご講演頂くとともに，パネル討論を実施いたしました．

2025 年度には，研究会に加えて，韓国済州島にて Korea Multi Media Society（KMMS）との日韓合同ワークショップ CCMS Workshop 2025 を開催いたしました．

CCS 研究会では，学生の皆様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 4 回の研究会にて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．

2023 年 5 月からコロナウイルス感染症が 5 類へ移行したことに伴い，全ての研究会を対面形式で開催し，CCS 研究会が更に活気づいてまいりました．2026 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．

【2026 年度 CCS 研活動計画】

●第一種研究会

2026 年 6 月 11 日，6 月 12 日 CCS/NLP 共催研究会 @I-site なんば（大阪府）
2026 年 8 月 6 日，8 月 7 日 CCS/IN 併催研究会 @ 札幌市教育文化会館（北海道）
2026 年 11 月 CCS 研究会（会場検討中）
2027 年 3 月 CCS 研究会（会場検討中）

●大会・国際会議

2026 年 6 月 13 日 NOLTA ソサイエティ大会 @I-site なんば（大阪府）
2026 年 11 月 17 日～11 月 20 日国際ワークショップ CCMS 2026（NOLTA 2026 にて開催）@ フランスグルノーブル

【CCS 研究会 Web サイト】https://www.ieice.org/~ccs/

中村　遼（正員）
2020 関西学院大学大学院理工学研究科博士課程後期課程修了．博士（工学）．2020～2022 福岡大学工学部助教．2022～福岡大学工学部講師．現在に至る．

■信頼性研究会（R）

信頼性は，製品やシステムを安心して使い続けられることを支える，利用者にとっては備わっていて当然の「当たり前品質」といえます．しかし，システムの高度化・複雑化が進む現在では，単に求められる機能を継続的に果たすという従来の信頼性だけでなく，異常発生時の検知・回復機能，保全性，安全性，セキュリティまで含めた総合的な信頼性の確保が求められています．近年では，機械学習・深層学習を基盤とした AI やデータ駆動型システムの普及に伴い，使用するデータやこれらのシステムの信頼性・品質管理も重要な課題となっています．

信頼性研究会では，半導体・電子デバイスや通信ネットワーク，ソフトウェアの信頼性をはじめ，安全性・保全性，国際規格など，幅広いテーマにおける理論・実験・応用を対象として，年間 8 回の研究会を全国各地で開催し，最新の研究成果の共有及び活発な議論を行っています．多様な分野の研究者・技術者が集まるため，自身の専門分野だけでは得られない視点や思いがけないアイデア・示唆が得られることも，本研究会の特徴の一つです．

2026 年度の開催計画は以下のとおりです．ハイブリッド形式も活用し，より多くの皆様が参加しやすい研究交流の場づくりに取り組んでいます．

5 月：鳥羽商工会議所（ハイブリッド形式）
6 月：機械振興会館（ハイブリッド形式）
7 月：北海道地区
8 月：開催地未定（CPM，LQE，OPE，EMD との合同研究会）
10 月：九州地区
11 月：関西地区
12 月：機械振興会館（ハイブリッド形式）
3 月：中国・四国地区

信頼性研究会では，大学院生をはじめ若手からベテランの研究者・技術者まで幅広い方が研究発表を行っています．信頼性を専門とする研究者の方はもちろん，信頼性に関する問題や技術に興味をおもちの皆様のご参加も心よりお待ちしております．

高橋奈津美（正員）
2013 首都大学東京（現：東京都立大学）大学院システムデザイン研究科博士前期課程了，2016 同大学院博士後期課程了，同年青山学院大学理工学部助教，2020 防衛大学校電気情報学群講師，現在に至る．信頼性工学，組合せ最適化の研究に従事．JIMA，REAJ，IEEE 各会員．

■情報理論研究会（IT）

情報理論研究会（IT：Information Theory）研究会は，情報理論とその関連分野を扱う研究会です．シャノン理論や符号理論をはじめとして，通信方式，量子情報，情報理論的安全性，仮説検定，統計的機械学習などの基礎理論や，その応用に関する幅広い分野を対象としています．IT 研究会は，例年 5 月，8 月，1 月，3 月の計 4 回の研究会を開催しています．5 月の研究会では，初めて研究発表を行う学生の皆さんを対象とした「フレッシュマンセッション」を設けています．今年度からの試みとして，8 月の研究会を海外開催します．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．2026 年度の IT 研究会は以下のように開催する予定です．

- 2026 年 5 月 21 日，22 日，京都テルサ，高機能マルチメディア（EMM）研究会と共催．
- 2026 年 8 月 1 日～8 月 3 日，Sahid Raya Hotel & Convention Yogyakarta（インドネシア），インドネシア，ジョグジャカルタで開催される Politeknik elektronika negeri surabaya International Electronics Symposium（IES2026）内のワークショップとして開催．
- 2027 年 1 月 19 日，20 日（予定），北海道大学，信号処理（SIP）研究会，無線通信システム（RCS）研究会と共催．
- 2027 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．

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す．IT 研究会で優秀な研究発表を行った学生の皆さんに対して，「学生優秀発表賞」を授与しています．ぜひこの賞の受賞を目標の一つにして頂きたいと思います．IT 研究会では，大学院の学生の皆さんだけでなく，高専生，若手研究者からベテランの先生まで幅広い方々が研究発表をしています．活発な質疑応答や，休憩時間や懇親会での議論など，研究会は今後の研究に有益な情報交換が可能な場です．また，研究会での優秀な発表に対して，電子情報通信学会の論文誌に研究専門委員会から推薦する推薦論文制度の新設を現在検討しています．今年度の 8 月の研究会は海外での開催となりますので，国際会議の発表の準備としても海外開催の研究会をご利用ください．8 月の研究会は継続して海外開催ができるよう検討を進めています．情報理論及びその関連分野に関心をおもちの多くの方のご参加をお待ちしております．

三村和史（正員：シニア会員）
1992 年 3 月大阪大基礎工卒．1994 年 3 月同大学院博士前期課程了．1999 年 3 月同大学院博士後期課了．博士（理学）．神戸市立高専講師，広島市立大学教授を経て，2017 年 4 月より同大学院教授．日本物理学会，IEEE 各会員．情報統計力学，符号理論，信号処理の研究に従事．

■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，前身のスペクトル拡散通信（SST）研究会から数えて 35 年以上の歴史をもつ，伝統ある研究会です．名前から想像されるよりもずっと懐が深く，符号構成・変復調・多元接続といった基盤理論から，OFDM，UWB，可視光・水中通信，レーダー・センシング，UAV 応用まで，実に多彩な研究テーマを扱っています．近年では，Beyond 5G/6G に向けて注目を集めている通信とセンシングの統合（ISAC）や非地上系ネットワーク（NTN），AI を活用した信号処理といった新しいテーマも活発に議論されています．情報理論（IT），情報セキュリティ（ISEC），高信頼制御通信（RCC），高度交通システム（ITS）といった研究会との共催・併催も継続しており，参加すると隣接分野の最先端にも自然と触れられるのが大きな魅力です．

研究会は年４回の開催を基本としており，若手奨励賞や WBS 研究活動奨励賞などを通じて学生・若手研究者の活動も積極的に後押ししています．多様な分野の研究者が自由に学び，議論できる場として今後も発展させてまいりますので，皆様の積極的なご参加をお待ちしております．

渡辺大詩（正員）

2017 北海道大学工学部卒，2019 同大大学院情報科学研究科修士課程修了．同年 KDDI(株)入社．運用部門にて基地局設備の保守・運用業務を経て，2020 から KDDI 総合研究所にて Beyond 5G/6G に向けた研究に従事．現在は，無線通信への AI 適用に関する研究及び 3GPP における標準化活動に従事．2025 から WBS 研究専門委員会幹事．

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 7 年度フェロー称号

令和 7 年に新たにフェロー称号を贈呈された方は学会全体で 23 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 4 名の方を御紹介します！

小林春夫

「数理的手法によるアナログ・ディジタル変換器の設計・解析・試験」

Q. フェローになられた御感想をお聞かせください.

このたびフェローとしてご推挙頂き，大変名誉なことであり，心よりうれしく思っております．推薦者としてお力添えくださった東京都市大学名誉教授・堀田正生先生には，産業界におられた頃から産学連携を通じて，またその後は大学間共同研究などを通じて長年ご指導頂き，深く感謝申し上げます．今回のフェロー応募に際し，お声がけくださった委員の先生方や関係者の皆様，そしてこれまでともに楽しく研究に取り組んできた共同研究者の方々，研究室の皆様にも，心より御礼申し上げます.

Q. 現在，御興味を持たれている研究テーマを教えてください.

アナログ・ディジタル変換回路（ADC）の設計分野では，冗長性を活用してディジタル誤差補正を行う方式や，ADC の非理想要因を内部回路で自動測定・補正する自己校正方式など，多様なアプローチが活発に研究されています．しかし，これらの方式は個別に提案されてきた経緯があり，統一的・体系的な枠組みとして整理されているとは言えません.

そこで，群馬大学の定年退職を機に，これらの方式を統一的に扱う理論の構築を目的とした研究を，科学研究費の支援を受けて約 3 年前から進めています．この研究は，理論的・数理的な側面が強く，いわば好奇心駆動（Curiosity Driven）のアプローチによるものです.

一方，群馬大学在職中は産学連携を積極的に推進し，社会的要求駆動（Social Demand Driven）の研究に取り組んでいました．現在は，当時とは大きく異なる視点と方法で研究を進めており，研究スタイルを大きく転換した形になります.

Q. 今後の抱負をお聞かせください.

今後は，日本の研究者がまだ十分に取り組んでいない分野に積極的に挑戦していきたいと考えています．また，国際学会などと連携し，多くの研究者を招待講演としてお招きするなど，周囲の研究者の活躍の場を広げ，研究コミュニティ全体を底上げする取り組みにも力を注いでいきたいと思います.

Q. 若い研究者の方へメッセージをどうぞ！

私自身が研究成果を挙げられるようになったきっかけとなる言葉や姿勢を，若い研究者の皆さんにもお伝えしたいと思います.

1.「人のやっていないことを研究する（Do what people don't do.）」

日本の研究者があまり取り組んでいない領域を研究すると，日本への貢献が比較的に大きくなるということを経験しています.

2.「彼を知り己れを知れば，百戦百勝す．彼を知るは難きに以て易く，己を知るは易きに以て難し」

この言葉が示すように，自分自身を深く理解することが何より重要です．自分の強み・能力・関心を丁寧に見つめ直し，何に興味を抱き，どのような能力を発揮できるのかを自覚することは，長く研究を続けるうえで大きな力になります.

3.「工学系研究者は外に打って出よ.」

電子情報通信をはじめとする工学分野では，外部との交流が極めて重要です．学会や研究会に積極的に参加し，多様なアイデアに触れること．展示会も別の視点から有益な情報が得られます．国内にとどまらず海外にも積極的に出ていくこと，産業界ともつながりをもつことが，工学研究の幅を大きく広げます.

4.「書きとどめよ．議論したことは風の中に吹き飛ばしてはならない.」

写真１　米国系 EDA ベンダーのイベントにての講演（2025 年 9 月品川にて）

写真２　国際学会 IEEE ASICON のバンケットにて研究室からの参加者と（2015 年 11 月中国　成都市にて）

写真３　国際学会 IEEE ICSICT にて群馬大学関係の参加研究者と（2024 年 10 月中国　珠海市にて）

写真４　友人，研究室 OB，OG との懇親会にて（2025 年 8 月新宿にて）

考えたこと，行ったこと，経験したことを記録として残すことは非常に重要です．報告書，学会・研究会発表（原稿・スライド），論文，特許などをこまめに作成することで，自分の考えが整理され，課題も明確になります．また，後から振り返って考える際の大切な資源にもなり，ほかの人に説明する際にも大いに役立ちます．

夏目季代久

「動物脳モデルの知見を元にした脳波を用いた BMI システム研究」

Q．フェローになられた御感想をお聞かせください．

フェローの称号を賜り，大変光栄に存じます．本称号は，NOLTA ソサイエティの先生方をはじめ，学会関係者の皆様，大学時代の指導教員の先生方，共同研究者の先生方，大学の同僚，そして研究室の学生の皆さんのご支援の賜物であると感じております．皆様のご協力なくして，このような栄誉にあずかることはできませんでした．この場をお借りして，心より感謝申し上げます．

Q．現在，御興味を持たれている研究テーマを教えてください．

これまで，脳波をはじめとする脳内神経振動などの非線形現象が，生物の情報処理にどのように関与しているかを研究してきました．初期には動物実験を通じて，脳波の θ 波がシナプス可塑性に関与することを明らかにしました．その後，約 20 年前，日本においてブレイン・マシン・インタフェース（BMI）という概念がまだ一般的でなかった頃から，ヒト脳波の応用研究に取り組んできました．当時，海外では車いす制御など福祉分野への応用が中心でしたが，私は教育，エンターテインメント，ロボット制御など他分野への展開を志向して研究を進めてきました．現在は，ヒトとロボット，あるいはヒトと仮想空間内アバターとの協調システムへの応用や，音楽嗜好性に基づく脳波解析，更には疲労や飽きの状態を検出して休憩を促すシステムの開発などに取り組んでいます．

写真１　毎年恒例４月の小倉城花見．研究室の学生と

写真２　脳波測定準備中．高専インターンシップの学生と

写真３　研究室学生とちょっと一杯

写真４　2025 年 NOLTA ソサイエティ大会（岡山県岡山市　能楽堂ホール tenjin9 にて）

Q．今後の抱負をお聞かせ下さい．

これまでの基礎研究を基盤として，脳波を用いた BMI の実用化を更に推進していきたいと考えています．また，生成系 AI との連携にも強い関心をもっています．脳波については「何を測定しているのか分かりにくい」と指摘されることも多くありますが，今後は脳科学的エビデンスとの対応関係をより明確にしながら，信頼性の高いシステム開発を進めていきたいと考えています．

Q．若い研究者の方へメッセージをどうぞ！

私は学生時代，単細胞生物である真性粘菌変形体の情報処理を研究していましたが，その後研究対象を「脳」へと移し，モルモット，ラット，ヒトへと対象を広げてきました．学生時代は薬学部でしたが，助手（現在の助教）着任後に脳科学や工学といった新しい分野に飛び込み，ほぼゼロから研究をスタートしました．苦労もありましたが，新しいことを学ぶ中で次々と発見があり，非常に刺激的な研究生活を送ることができました．現在は生成系 AI の発展により，多くのことが容易に調べられる時代になりましたが，若い研究者の皆さんには，臆することなく新しい分野に挑戦し，自身の専門で培った視点を異分野に積極的に展開してほしいと思います．

福島和英

「難読化技術実用化と耐量子計算機暗号安全性評価の先導研究」

Q．フェローになられたご感想をお聞かせください．

大変光栄に感じております．過分な評価に恐縮するとともに，皆様のご指導・ご支援に深く感謝しております．

フェローという立場に，身が引き締まる思いです．

写真１　マイコン展での一コマ

写真２　自然の中でリフレッシュ

Q. 現在，ご興味を持たれている研究テーマを教えてください.

計算機科学全体が今後どのような方向へ発展していくのかに関心があります．私が専門とする暗号分野においても，これまで様々な成果が創出され，理論も成熟してきました.

一方で，計算量理論における未解決問題に起因して，いまだ解決されていない課題も数多く残されていると認識しています．こうした課題が将来どのような手法で解決され，暗号や情報セキュリティの発展にどのような影響を与えるのかについて，引き続き注目していきたいと考えております.

Q. 今後の抱負をお聞かせください.

これまでの経験を活かし，研究開発を更に加速させるとともに，実用化にもつなげていきたいと考えております．また，後進の育成にも力を注ぎ，次世代のセキュリティ研究者や，学会活動にも貢献できる人材の育成に取り組んでまいります.

Q. 若い研究者の方へメッセージをどうぞ.

自ら課題を発見し，その解決に向けて主体的に挑戦できることは，研究者の醍醐味です．失敗を恐れず，自分の知的好奇心と情熱を信じて，様々なことにチャレンジしてください．また，多様な分野の仲間と積極的に議論し，連携することも，新たな発想を生むうえで非常に重要です.

皆さんの若い力と独創的なアイデアが，未来の社会をより良く変えていくと信じています.

宮地充子

「楕円曲線暗号と双線形暗号の基盤技術確立と社会実装の先駆的展開」

Q. フェローになられた御感想をお聞かせください.

1990 年より情報セキュリティ技術の研究に従事し，特に楕円曲線暗号及び双線形暗号の基盤技術に関する研究を推進してまいりました．あわせて，国際標準化活動や後進の育成にも取り組んでまいりました.

このような長年にわたる活動を評価頂き，このたび IEICE フェローに認定頂きましたことを，大変光栄に，また心よりうれしく思っております.

私は理学部数学科を修了後，松下電器産業株式会社（現 パナソニック ホールディングス株式会社）に入社し，異分野である情報セキュリティの研究に携わることとなりました．当時は手探りの状態でしたが，IEICE の研究会活動を通じて多くを学び，研究の基盤を築くことができました．

その原点ともいえる IEICE においてフェローとして認定頂いたことは，特別な意味をもつものであり，深い感慨を覚えております．

今後はこの栄誉を糧として，謙虚な姿勢を忘れず，情報セキュリティ分野の更なる発展，学会活動への貢献，並びに後進の育成に引き続き尽力してまいりたいと考えております．

Q. 現在，御興味を持たれている研究テーマを教えてください．

現在，主に以下の三つの研究テーマに関心をもって取り組んでおります．

1．プライバシー保護と AI の両立

近年，私たちのデータに基づく AI が様々な分野で活用され，社会課題の解決や産業の発展に大きく寄与しています．一方で，プライバシー情報は本来個人に帰属するものであり，その適切な保護は不可欠です．

産業の発展のみを優先するのではなく，プライバシーを保護しながらデータ利活用を可能とする技術の確立が重要であると考えています．このため，オリジナルデータではなく摂動データを用いながらも，高い精度を維持可能な AI 技術の研究に取り組んでおります．

2．メンバー・非メンバーを判別可能な定数オーダ認証技術

データ利活用における「オプトイン」は，個人の同意に基づく重要な仕組みですが，同意後に非同意へと変更された場合に，その状態を適切に検証できることも重要です．

不特定多数を対象とする場合であっても，データ提供者か否かを効率的に制御・検証可能な認証基盤が求められています．特に，大規模環境においてもスケーラブルに動作する定数オーダの認証技術の確立が重要であり，産業と個人の権利のバランスを実現する観点から研究を進めています．

3．耐量子安全かつサイドチャネル攻撃に強い暗号方式

量子計算機の実現を見据え，耐量子暗号の研究が進展していますが，理論的安全性と実装時の安全性は必ずしも一致しません．特に，実装の脆弱性を突くサイドチャネル攻撃への対策は，耐量子安全性とは独立に検討する必要があります．

このため，耐量子安全性を備えると同時に，サイドチャネル攻撃に対しても堅牢な暗号方式の構築に取り組んでおります．

これらはいずれも今後重要性が一層高まる研究分野であり，楕円曲線暗号の発展と同様に，将来広く社会に実装される基盤技術となることを目指し，先駆的に研究を進めてまいりたいと考えております．

Q. 今後の抱負をお聞かせください．

今後は，上記に挙げた三つの研究を精力的に推進するとともに，情報セキュリティ分野における人材育成にも一層力を入れてまいりたいと考えております．

大学生及び大学院生に対しては，全国から情報セキュリティを志す学生を受け入れ，体系的な教育を提供するとともに，Basic SecCap/SecCap といった認定制度を通じて，実践的な能力の育成に取り組んでおります．

一方で，2017 年より社会人教育にも注力しており，大阪大学大学院工学研究科において，安全なデータ利活用を担うプロフェッショナル人材の育成コースを開設しました．現在では，全国から多くの社会人受講者を迎えており，情報セキュリティの学習を通じて，知識の習得だけでなく，学ぶことの楽しさも実感して頂けるよう努めております．

更に，これらの研究成果の社会実装を推進し，実社会における安全･安心な情報基盤の構築に貢献していきたいと考えております．

研究・教育・社会実装のそれぞれを着実に進めながら，今後も本分野の発展に寄与してまいります．

Q. 若い研究者の方へメッセージをどうぞ！

若い研究者の皆様とお話しする中で，「自分に研究ができるのだろうか」「自分に向いているのだろうか」と悩んでいるという声を耳にすることがあります．

しかし，自分に合っているかどうかを見極めることは容易ではなく，むしろ長い時間をかけて向き合っていくものだと思います．短期間で答えを求めるのではなく，「どのような自分になりたいのか」を考え，そこに向かって努力を重ねることが大切ではないでしょうか．

その過程の中で，やがて自分にとってのライフワークが見えてくると思います．努力は決して無駄にはならず，必ず様々な形で自分の力となります．

ぜひ，未来に目標をもち，一歩一歩着実に進んでいってください．ウサギとカメの寓話にあるように，着実に歩み続ける「カメ」の姿勢が，最終的には大きな成果につながると信じています．

写真１　現在の筆者

写真２　MTG の様子

写真３　令和６年秋の勲章・褒章伝達式の様子
出典：「令和６年秋の勲章伝達式及び令和６年秋の勲章・褒章伝達式」（文部科学省）（https://www.mext.go.jp/b_menu/activity/detail/2024/20241126_2.html）（2026 年６月 11 日に利用）

写真４　国際会議の招待講演の様子

写真５　プログラム委員長として主催した国際会議での Dinner の挨拶の様子

令和７年度　学術奨励賞

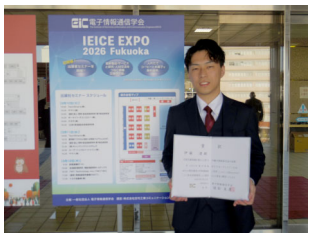
令和７年度は基礎・境界ソサイエティ及び NOLTA ソサイエティでは６名が学術奨励賞を受賞されました.

猪狩　紫雲
（千葉工業大学）

“カードベース暗号における整数コミットメントの効率的な変換法”[1]

このたびは栄誉ある賞を頂き大変光栄に存じます．ご指導くださいました駒野先生，東北大学の水木先生，共著者の小高くんには心より感謝申し上げます．私は以前，物理的なカードを用いて秘密計算を行う「カードベース暗号」の分野で「巡回セールスマン問題の解に関する物理的 ZKP」を研究し，都市間の距離を少ない枚数のカードで表す整数表現を提案しました．学術奨励賞に選定頂いた論文では，その整数表現で表された距離を，加算に適した別の整数表現に効率良く変換する手法を提案しました．これにより，カード枚数を抑えたまま物理的 ZKP を実行することができるようになりました．今後も，この賞を励みに研究活動に邁進してまいります．

伊藤　遼
（新潟大学）



“大域文脈情報を導入した洋ナシ外観汚損検査手法の改良”[2]

このたびは，栄誉ある電子情報通信学会学術奨励賞を賜り，大変光栄に存じます．研究を進めるにあたり，多大なるご指導を賜りました山﨑達也教授をはじめ，研究室の皆様には，この場を借りて深く感謝申し上げます．受賞対象となった研究では，CNN における大域情報の取得限界に対し，大域文脈を付与するモジュールを導入することで，サイズの異なる物体の検出精度を向上させる手法を検証いたしました．現在は研究の道からは離れておりますが，この賞に恥じぬよう，社会人として一層努力してまいります．改めまして，このたびは誠にありがとうございました．

郭　豊愷
（東京理科大学）

“CSPSO のパラメータの依存性について”[3]

学術奨励賞という栄誉ある賞を賜り，大変光栄に存じます．ご指導くださった池口徹先生をはじめ，共同研究者である木村貴幸先生，松浦隆文先生，並びに研究室の皆様，及び貴重なご助言・ご議論を賜りました諸先生方に心より御礼申し上げます．私は組合せ最適化問題に対するカオスダイナミクスを用いた手法の研究に取り組んでおり，受賞論文では，カオスサーチに粒子群最適化を導入した手法において，パラメータが探索性能に与える影響を検討いたしました．本受賞を励みとして，今後もより一層研究に精進してまいります．このたびは誠にありがとうございました．

Chenyu Zhao
（北海道大学）

“Design of a Streaming-Based Resource-Efficient Mel Filter Bank Architecture for Real-Time Mel Spectrum Extraction on FPGA” (4)

このたびは，学術奨励賞という大変名誉ある賞を賜り，誠に光栄に存じます．本研究を進めるにあたり，終始丁寧かつ熱心にご指導くださいました大鐘武雄先生，筒井弘先生をはじめ，研究室の皆様，並びに貴重なご助言と温かい励ましを賜りました関係者の皆様に，この場をお借りして心より御礼申し上げます．

受賞対象となった研究では，FPGA 上でリアルタイムにメルスペクトルを抽出することを目的として，ストリーミング処理に適した省資源なメルフィルタバンクアーキテクチャの設計に取り組みました．限られたハードウェア資源の中で，処理効率と実装性の両立を図り，実時間音声処理に適した構成を目指して検討を重ねてまいりました．今回の受賞を大きな励みとし，今後もより一層研究に精進してまいります．誠にありがとうございました．

中務　太智
（山口大学）

“感度解析に基づいたサプライチェーンのレジリエンス評価” (5)

このたびは，学術奨励賞という名誉ある賞を受賞することができ，大変光栄に存じます．日頃よりご指導頂きました足立亮介准教授や若佐裕治教授をはじめ，制御情報工学研究室の皆様，並びに学会関係者の皆様に，心より感謝申し上げます．受賞対象の研究では，感度解析に基づき，サプライチェーン途絶時における補完的要素を定量的に評価する手法を提案いたしました．本受賞を励みに，今後も社会に貢献できるよう努力してまいります．このたびは誠にありがとうございました．

中村　謙
（山口大学）

“単一削除訂正不能である量子単一挿入訂正符号” (6)

このたびは，栄誉ある学術奨励賞を賜り，誠に光栄に存じます．本研究を遂行するにあたり，多大なるご指導を賜りました野崎隆之准教授をはじめ，研究室の皆様にこの場をお借りして御礼申し上げます．

受賞論文では，量子誤り訂正符号における挿入誤りと削除誤りの訂正可能性が必ずしも等価ではないことを，具体的な反例を用いて示しました．本賞を励みとして，本分野の発展に貢献できるよう，より一層研究に精進してまいります．このたびは誠にありがとうございました．

学術奨励賞対象論文

（1） 猪狩紫雲，“カードベース暗号における整数コミットメントの効率的な変換法，”総大，A-7-02, March 2025.
（2） 伊藤遼，“大域文脈情報を導入した洋ナシ外観汚損検査手法の改良，”ソ大，A-14-12, Sept 2025.
（3） 郭豊愷，“CSPSO のパラメータの依存性について，”ソ大，N-1-26, Sept 2025.
（4） Chenyu Zhao, “Design of a Streaming-Based Resource-Efficient Mel Filter Bank Architecture for Real-Time Mel Spectrum Extraction on FPGA,” ソ大，A-14-15, Sept 2025.
（5） 中務太智，“感度解析に基づいたサプライチェーンのレジリエンス評価，”ソ大，A-10-18, Sept 2025.
（6） 中村謙，“単一削除訂正不能である量子単一挿入訂正符号，”ソ大，A-2-03, Sept 2025.

北海道大学だより

小林孝一（北海道大学）

はじめに

2026 年のソサイエティ大会は 2026 年 9 月 23 日（水）～25 日（金）に北海道大学札幌キャンパスで開催します．例年は 4 日間開催ですが，今年は 3 日間開催になりますのでご注意ください．開催地について簡単にご案内いたします．

（1） 創基 150 周年を迎える北海道大学

北海道大学の起源は，日本で最初期の学位授与機関（大学）として設立された札幌農学校に遡ります．1876 年開校の札幌農学校から，帝国大学，新制国立大学の時代を経て，2026 年に北海道大学は創基 150 周年を迎えます．150 年に及ぶ歴史の中で，「フロンティア精神」「国際性の涵養」「全人教育」及び「実学の重視」という四つの基本理念を建学の精神として掲げて発展を遂げています．2026 年は，創基 150 周年の記念すべきマイルストーンの年として，また唯一無二の「比類なき大学」として世界の課題解決に貢献する大学を目指す次の 150 年のスタートと位置づけています．

創基 150 周年を記念したフラッグが学内のあちこちに設置されていますので，ぜひご覧ください（写真 1）．

写真 1　創基 150 周年記念フラッグ

（2） 観光地としての北海道大学

北海道大学は都心に立地しているにもかかわらず，南北 2.5 km，東西 1 km という広大な敷地を有しています（写真 2）．正門には札幌駅北口から徒歩 6 分程度で来ることができます．ただ，正門から工学部地区までは徒歩で 13 分程度かかります．つまり札幌駅から徒歩で 20 分程度かかります．工学部地区も広いので，時間に余裕をもってお越しください．

写真２　空撮写真

正門から工学部地区に来るまでにも幾つか観光スポットがあります．お時間があるときにぜひお立ち寄りください．

・クラーク胸像（有名なクラーク像ではないです）（写真３）
・総合博物館（写真４）
・新渡戸稲造博士顕彰碑（写真５）
・ポプラ並木（写真６）

写真３　クラーク胸像

写真４　総合博物館

写真５　新渡戸稲造博士顕彰碑

写真６　ポプラ並木

学内で迷子になったら，歩いている学生に声を掛けてください．筆者も観光客に声を掛けられて道案内をしたことがあります．

また，北海道大学の周辺にはスープカレーの店がたくさんありますので，ぜひお楽しみください（もちろん学生がたむろする居酒屋もあちこちにあります）．

（3） 札幌と新千歳空港の間の移動手段

ソサイエティ大会に参加される方の多くは飛行機で来られ，新千歳空港を利用されると思います．新千歳空港から札幌への移動には JR 北海道の快速エアポートを使うのが便利です．ただ，最近は各種トラブルで運休や間引き運転が多くなっています．快速エアポートが利用できない場合はバスでの移動になりますが，札幌都心行きのバスは非常に混雑することがあります（以前，バス停に長蛇の列ができているといった報道がありました）．もしこのような事態が発生したときは，北 24 条あるいは大谷地行きのバスを探すことをお勧めします．北 24 条，大谷地までたどり着ければ，地下鉄で札幌駅に行くことができます．トラブルがないことを祈っていますが，もしもの際の参考になれば幸いです．

おわりに

9 月下旬は観光シーズンで多くの観光客が訪れます．また，海外からの観光客も激増しています．ホテルや飛行機の予約が取りにくくなりますので，早めの予約をお勧めします．札幌で皆様にお会いすることを楽しみにしています．

小林孝一（正員）

2000 法政大学大学院工学研究科修士課程修了．2000～2004 新日本製鐵(株)勤務．2007 東京工業大学大学院情報理工学研究科博士後期課程修了．同年北陸先端科学技術大学院大学情報科学研究科助教，2015 北海道大学大学院情報科学研究科准教授，2019 同大学院情報科学研究院准教授，2023 同教授となり現在に至る．システム制御理論とその応用の研究に従事．

第４９回情報理論とその応用シンポジウム(SITA2026)開催案内

ご挨拶

第49回情報理論とその応用シンポジウム(SITA2026)を愛媛県松山市にて開催します。本シンポジウムは、例年、宿泊と発表会場を一体とした泊まり込みのスタイルをとっていますが、2026年はさらに別の発表会場も用意しています。これまでのシンポジウムにならい、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　斎藤秀俊

開催期間・会場

2026年12月15日(火)～12月18日(金)
愛媛県松山市 道後温泉 にぎたつ会館 (https://nigitatsu.jp)

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, SIP, RCC, WBS 研究専門委員会
IEEE Information Theory Society Japan Chapter
IEEE Japan Office

Web Site

https://www.ieice.org/ess/sita/SITA2026/index.html

実行委員会

実行委員長		
	斎藤秀俊	(工学院大学)
プログラム委員長		
	石井光治	(香川大学)
総務	藤沢匡哉	(東京理科大学)
会計	日下卓也	(島根大学)
登録	吉川英機	(東北学院大学)
出版	小寺雄太	(岡山大学)
会場	小西たつ美	(愛知工業大学)
広報	金子晴彦	(東京科学大学)
アドバイザ		
	辻岡哲夫	(大阪公立大学)
	野上保之	(岡山大学)

今後のスケジュール

発表申込開始	2026年8月5日
発表申し込み期限	2026年9月14日
発表原稿提出期限	2026年9月25日
早期参加申込締切	2026年11月4日

事務局

〒125-8585 東京都葛飾区新宿 6-3-1
東京理科大学葛飾キャンパス
管理棟4階 藤沢研究室
SITA2026 事務局 藤沢匡哉
sita-2026-sec@mail.ieice.org

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 experiments, are solicited for submission to IWSEC 2026. Topics of interest for IWSEC 2026 include all theory and practice of cryptography, information security, and network security, as in the previous IWSEC workshops.

- Applied cryptography
- Anonymity
- Biometrics security and privacy
- Blockchain and cryptocurrency
- Cryptanalysis
- Cryptographic primitives
- Cryptographic protocols
- Cyberattacks and defenses
- Financial cryptography
- Forensics
- Formal methods for security analysis
- 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
- Multiparty computation
- Network, system and cloud security
- Offensive security
- Post-quantum cryptography
- Privacy-enhancing technologies
- Privacy-preserving data mining
- Program analysis
- Public-key cryptography
- Quantum cryptography and cryptanalysis
- Real-world cryptographic systems
- Side-channel and fault analysis
- Software security
- Supply chain security
- Symmetric-key cryptography
- Theory of cryptography

Committees

General Co-Chairs:

Katsuyuki Takashima (Waseda University, Japan)

Tatsuya Mori (Waseda University, Japan)

General Co-Chairs:

Mehdi Tibouchi (NTT, Japan)

Toshiki Shibahara (NTT, Japan)

論文募集

第 16 回バイオメトリクスと認識・認証シンポジウム（SBRA2026）

「生体認証」として知られる「バイオメトリクス」は，センサやアルゴリズムに関する基礎技術から，システム構築，サービス提供といった実利用まで，多岐にわたる認識・認証技術として発展してきました．現在では，顔認証，指紋認証，静脈認証など，さまざまなサービスにおいて広く利用される技術となっています．近年は，生成 AI の発展に伴い，より高精度な認証技術の実現など，技術の進化が著しい一方で，バイオメトリクスに対する攻撃手法も多様化・高度化しており，バイオメトリクス技術は新たなステージに入ったと言えます．

このような背景のもと，「バイオメトリクスと認識・認証シンポジウム（SBRA）」は，バイオメトリクスや認証・認識に関するさまざまな研究分野の研究者，開発者，利用者が一堂に会し，交流や情報交換，相互啓発を深める場として開催されてきました．SBRA2026 は，2024 年に伊香保温泉で開催された大会が好評であったことを受け，再び群馬県内の温泉地での開催を予定しています．多くの皆様からのご発表・ご参加を，実行委員一同，心よりお待ちしております．

SBRA2026 実行委員長 鈴木裕之

会場：群馬県内の温泉地を予定　**会期**：2026 年 11 月中旬を予定

スケジュール：発表申込締切: 2026 年 10 月頃、原稿投稿締切: 2026 年 10 月頃、参加申込締切: 2026 年 11 月頃

募集テーマ：

- ✓ 指紋，虹彩，顔，静脈，掌紋，耳介，歩容，ジェスチャ，署名，音声，マルチモーダルバイオメトリクスに関する認識・認証技術，及びそれらに関する画像信号処理・パターン認識技術
- ✓ テンプレート選択・更新，プレゼンテーションアタック及びそれに関連する技術
- ✓ バイオメトリクスに関するシステム設計，スマートカード実装，大規模認証，データベース，生体情報保護，性能評価，プロトコル，ベンチマーク，標準化
- ✓ サーベイランス，アクセスコントロール，エンターテイメント，決済，犯罪や災害時の個人同定などへの応用

※ 詳細は BioX 研ホームページ（https://biox.jp/）をご確認ください

基礎・境界ソサイエティ運営委員会

会長	岩本　貢	(電気通信大学)
次期会長	池田　誠	(東京大学)
ソサイエティ編集長	和田山　正	(名古屋工業大学)
副会長（事業担当）	小嶋　徹也	(東京工業高専)
副会長（システムデザイン技術）	宮本　俊幸	(大阪工業大学)
副会長（音響・超音波）	西浦　敬信	(立命館大学)
副会長（情報理論とその応用）	楫　勇一	(名古屋大学)
副会長（信号処理とその応用）	西川　清史	(東京都立大学)
庶務幹事	藤澤　匡哉	(東京理科大学)
庶務幹事	髙島　康裕	(北九州市立大学)
会計幹事	吉田　隆弘	(日本大学)
会計幹事	土谷　亮	(関西大学)
事業担当幹事	西新　幹彦	(信州大学)
事業担当幹事	佐藤　隆英	(山梨大学)
大会担当幹事	花谷　嘉一	(株式会社東芝)
大会担当幹事	伊藤　大輔	(岐阜大学)
電子広報担当幹事	中井　雄士	(豊橋技術科学大学)
電子広報担当幹事	塩見　準	(大阪大学)
論文誌編集委員長	國廣　昇	(筑波大学)
論文誌編集幹事	鈴木幸太郎	(豊橋技術科学大学)
論文誌副編集委員長	—	
論文誌副編集幹事	—	
ソサイエティ誌編集委員長	定兼　邦彦	(東京大学)
ソサイエティ誌担当幹事	宮北　和之	(新潟大学)
ソサイエティ誌担当幹事	二神　拓也	(同志社大学)
編集特別幹事（オブザーバ）	相川　直幸	(東京理科大学)
出版委員会委員（オブザーバ）	斉藤　友彦	(湘南工科大学)
研究会連絡会幹事（オブザーバ）	中野　秀洋	(東京都市大学)
ハンドブック／知識ベース委員（オブザーバ）	葛岡　成晃	(和歌山大学)
男女共同参画委員会（オブザーバ）	眞田亜紀子	(長岡技術科学大学)
プラチナクラブ運営委員会（オブザーバ）	前田　義信	(新潟大学)
事務局	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）	小嶋　徹也	(東京工業専門高等学校)
副会長（システムデザイン技術）	宮本　俊幸	(大阪工業大学)
副会長（音響・超音波）	西浦　敬信	(立命館大学)
副会長（情報理論とその応用）	楫　勇一	(名古屋大学)
副会長（信号処理とその応用）	西川　清史	(東京都立大学)
事業担当幹事	西新　幹彦	(信州大学)
事業担当幹事	佐藤　隆英	(山梨大学)
回路とシステム（CAS）	越田　俊介	(八戸工業大学)
情報理論（IT）	三村　和史	(広島市立大学)
信頼性（R）	岡村　寛之	(広島大学)
超音波（US）	垣尾　省司	(山梨大学)
応用音響（EA）	西浦　敬信	(立命館大学)
VLSI 設計技術（VLD）	宮村　信	(ナノブリッジ・セミコンダクター株式会社)
情報セキュリティ（ISEC）	髙島　克幸	(早稲田大学)
信号処理（SIP）	田中　章	(北海道大学)
ワイドバンドシステム（WBS）	石川　博康	(日本大学)
システム数理と応用（MSS）	宮本　俊幸	(大阪工業大学)
思考と言語（TL）	吉田　悦子	(滋賀県立大学)
技術と社会・倫理（SITE）	森下壮一郎	(サイバーエージェント)
ITS（高度交通システム）（ITS）	羽多野裕之	(三重大学)
スマートインフォメディアシステム（SIS）	田向　権	(九州工業大学)
イメージメディアクオリティ（IMQ）	土田　勝	(日本電信電話株式会社)
高信頼制御通信（RCC）	小林　孝一	(北海道大学)
バイオメトリクス（BioX）	高橋　健太	(日立製作所)
安全・安心な生活と ICT（ICTSSL）	井ノ口宗成	(立命館大学)
ハードウェアセキュリティ（HWS）	三浦　典之	(大阪大学)
光輝会（SSA）（オブザーバ）	大木　哲史	(静岡大学)
技術と歴史（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）	根岸　一平	(金沢工業大学)
会長（オブザーバ）	岩本　貢	(電気通信大学)
次期会長（オブザーバ）	池田　誠	(東京大学)
庶務幹事（オブザーバ）	藤澤　匡哉	(東京理科大学)
庶務幹事（オブザーバ）	髙島　康裕	(北九州市立大学)
研究会連絡会幹事（オブザーバ）	中野　秀洋	(東京都市大学)
事務局	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	小西　啓治	(大阪公立大学)
次期ソサイエティ会長	若宮　直紀	(大阪大学)
庶務幹事	杉谷　栄規	(大阪公立大学)
庶務幹事	松浦　隆文	(日本工業大学)
会計幹事	井岡　恵理	(芝浦工業大学)
電子広報担当幹事	美井野　優	(鳴門教育大学)
NOLTA 編集委員長	上田　哲史	(徳島大学)
NOLTA 編集幹事	清水　邦康	(千葉工業大学)
NLP 委員長	久門　尚史	(京都大学)
NLP 副委員長	香取　勇一	(はこだて未来大学)
CCS 委員長	上山　憲昭	(立命館大学)
CCS 副委員長	荒井伸太郎	(岡山理科大学)
特別委員	伊藤　大輔	(岐阜大学)
特別委員	鳥飼　弘幸	(法政大学)
特別委員	高橋　規一	(岡山大学)
特別委員	木村　貴幸	(東京都市大学)
特別委員	中野　秀洋	(東京都市大学)
特別委員	木村　真之	(摂南大学)
特別委員	加藤　秀行	(大分大学)
特別委員	砂田　哲	(金沢大学)
特別委員	中村　遼	(福岡大学)
特別委員	堀尾　喜彦	(帝京大学)
特別委員	鈴木　秀幸	(大阪大学)
特別委員	佐藤　雅俊	(玉川大学)
特別委員	関屋　大雄	(千葉大学)
特別委員	黒川　弘章	(東京工科大学)

編集後記

今号も多様な解説論文をお届けします．その中でも，JPEG の暗号化については自分も復号アルゴリズムを実装したこともあり興味深く拝読しました．LLM については内部の計算を追ってみたりもしましたがまだ謎なところが多いです．本誌の解説論文をきっかけに更に知識を増やして頂ければ幸いです．（定兼邦彦）

今号より編集正幹事を務めることになりました．今号では「ごあいさつ」を担当しております．ご執筆頂いた皆様，並び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．FR 誌は 3 か月に一度発行されますので，次号の編集作業までは時間があると思っていても，あっという間に締切が近づいてまいります．編集作業に滞りが生じないよう，気を引き締めてまいりたいと思います．（宮北和之）

今号より編集副幹事を拝命いたしました．一読者として親しんできた本誌の編集に携わる立場となり，身の引き締まる思いです．編集作業を通じて，本誌が扱う領域の広さと奥深さを改めて実感しております．読者の皆様におかれましても，ご自身の専門外の記事に触れることで，思いがけない着想や学びの種を見出して頂ければ幸甚です．次号以降も，より充実した誌面づくりに尽力してまいりますので，ご指導ご鞭撻のほど何卒よろしくお願い申し上げます．（二神拓也）

今号より編集幹事補佐を務めさせて頂くこととなり，「受賞者の声」を担当させて頂きました．フェロー称号を贈呈された皆様，学術奨励賞を受賞された皆様，おめでとうございます．編集幹事補佐としての初めての編集作業で不慣れな点も多くございましたが，皆様のご協力のおかげで無事に発行まで進むことができました．ご協力，誠にありがとうございました．今後とも微力ながら尽力してまいりますので，よろしくお願い申し上げます．（矢嶋　純）

今号の「研究会へ行こう！」の特別編集幹事を担当させて頂きました．本誌の編集にご尽力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，この場をお借りして感謝申し上げます．各研究会は活発な議論と交流の場となっておりますので，ぜひ各研究会の取り組みをご一読頂き，研究会への投稿やご参加をご検討頂けますと幸いです．多くの皆様のご参加をお待ちしております．（佐々木智志）

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 第二十巻 第一号

令和八年七月一日発行

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