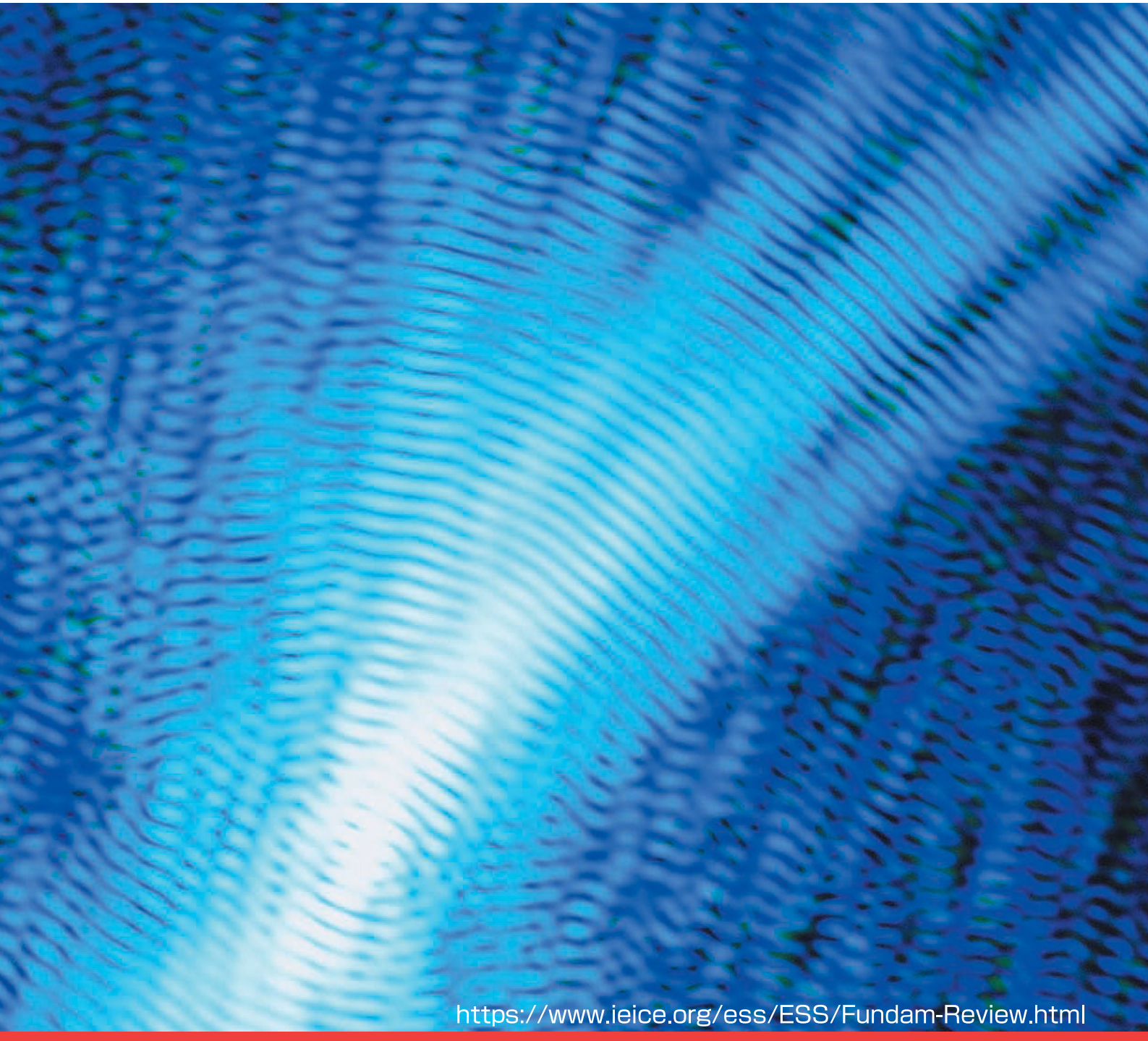
令和７年７月１日発行　第 73 号

Fundamentals Review

2025 July Vol.19 No. 1



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

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

ESS
2025
July
Vol.19 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

“使える”学会

Utilization of Academic Society

基礎・境界ソサイエティ会長　尾上孝雄

1. はじめに

基礎・境界ソサイエティ（ESS：Engineering Sciences Society）は学会のソサイエティ制への移行[(1)]に伴い1995年に発足し，本年ちょうど30年を迎えました．私もこれまで12年間，およそ1/3ぐらいの間，研専委員長，幹事団や英文誌編集委員長，特別委員（国外活性化）などの役職を頂き，ソサイエティ運営に携わってきています．

ESSは，ほかのソサイエティとは異なり，発足時から，文字どおり学会全体が関わる「電子」，「情報」，「通信」の研究分野の基礎を幅広く，力強く支えていくこととともに，これらの分野間の境界領域を掘り起こし，新たに先進的な領域を産み出していくことを担って活動を進めてきています．

この30年の間に，学会を取り巻く社会は大きく変貌を遂げました．当時，一般社会におけるインターネット普及率は1%にも満たず，グーグルも創業前で，スマホもタブレットも誰ももっていない状況でした．ご存知のとおり，有線・無線の情報ネットワーク技術，電子情報システムの集積化設計・実装技術，人工知能技術，量子情報処理技術などの革新的な進展の結果，現在では，学会が取り扱う技術分野も当時からは大きく変化しています．関連技術を情報インフラとして普段から利用する一般の方々の数は飛躍的に伸び，社会に対する学会の貢献への期待は大きく増してきているといえます．

2. ソサイエティの変化

さて，電子情報通信学会，各ソサイエティではこの30年間にどのような変化が訪れたのでしょうか？　ソサイエティ制移行後，各ソサイエティのなかで，社会的な要請や新興技術を取り扱う新しい研究専門委員会は設けられましたが，基礎・境界，通信，エレクトロニクス，情報・システムの4ソサイエティ体制は約20年間維持されてきていました．一方，ESSはソサイエティ制の検討段階から，将来的に三つ程度のソサイエティを構成する母体となることが期待されていました[(2)]．このため，四つのソサイエティの中で唯一「サブソサイエティ」という制度をもって活動してきています．

2014年10月に，NOLTA（Nonlinear Theory and Its Applications）サブソサイエティがソサイエティに昇格し，学会内に五つめのソサイエティが発足しました．ソサイエティ登録人数の関係などもあり，ESSとNOLTAソサイエティ（NLS）はそれぞれ独自性を有しつつ共同体として運営し，理事もソサイエティ共同体として学会運営に携わっています．これは，IEEEでいう“Division”と同じような位置づけです．NLSは登録人数こそ多くないものの，発足後10年にわたり，特徴的な活動を活発に継続してきています．ソサイエティは人数ではなく，活動の中身が大事であると証明してきています．

ESSは，この後も新しいソサイエティを産み出すような活動を行っていく必要があります．このような中，様々な議論を重ね，「システムと信号処理」サブソサイエティを発展的に改組し，2025年4月から「信号処理とその応用」，「システムデザイン技術」の二つのサブソサイエティを新設することになりました．これらのサブソサイエティは互いに協力しつつ，独自性を打ち出して今後加速的に発展していくことでしょう．

3. ソサイエティでの最近のトピック

次に，ESSでの最近議論・検討を進めている内容についてご紹介します．

● 電子情報提供媒体の刷新

ESS及びNLSのWebサイトは長らく大きな変更がなされてきておらず，ほかのソサイエティと比較しても取り残されている感がありました．2024年度に電子広報担当幹事を中心とした幹事団のご尽力で，アクセシビリティ改善，レスポンシブ対応，メンテナンス性の向上などをはかり刷新しました．

今後，本誌Fundamentals Reviewについても会員の皆様により注目して頂けるよう進めていく予定です．

● ESS主催フラグシップ国際会議

学会全体の課題として，海外会員数の急速な減少が表面化

しています．海外会員となる魅力の増大，また，国内の若手世代についても，国際舞台で活躍する機会を創出する必要があるという指摘が，植松友彦会長（元 ESS 会長）からあり，ESS でも研究専門委員会横断的な取り組みの一つとして，2026 年度からのソサイエティ主催国際会議の創設を準備しております．昨今，単独の技術領域で研究開発が完結することは少なく，カバーする領域が広い ESS だからこそできる新しい試みに挑戦していければと考えております．

4. 会員である価値

前述のとおり，電子情報通信学会で取り扱う技術領域の重要性が増す一方，会員数は減少しているのが現状です．分野が近い IEEE は，全体で会員数が増え続けており，日本国内会員も為替相場の影響を受けることなく会員数を維持（1999 年の Japan Council 発足時から比べると約 1.5 倍，ここ 10 年間は微増）しています．

電子情報通信学会の会員として留まる「価値」について，再考する必要があります．学会は，もちろん最新の技術動向を（本会の場合は日本語で）得る場として多く活用されています．これに加え，ほかの機関に所属されている研究者・技術者の方々と繋がる機会も多くあります．社会課題がますます複雑化していくなかで，「手が届く」範囲を拡大するためにも有用です．論文誌，国際会議や研究会，大会などでの発表，各種イベントに参加することで，自身のプロモーションや転職に役立つ場合もあるでしょう．

これらは，昔から大きくは変わっていません．大きな変化は，研究者・技術者のあらゆる「余裕」がなくなったことと，このため，所属機関（大学，会社）内での学会活動に対する理解・評価が実感として減少していることかと思っています．これらについては，他国との差を大きく感じます．

もちろん，学会もただ黙っているわけではありません．これまでにない，学会を「使う」活動のバリエーションを増やしていくことや，学会の活動が一般社会において認知・評価されるよう働きかけていくことなど，様々な新しい試みを続けています．

学会を「使って，使って，使い倒す」ことが可能となり，またそれが評価されるよう，ソサイエティ運営を考えていきたいと思っております．皆様方のご支援，ご協力をぜひ宜しくお願い申し上げます．

文　献

（1） 辻井，原島，富永，遠山，都倉，“学会の新しい門出にソサイエティ会長おおいに語る，”信学誌，vol. 78, no. 9, pp. 857-971, Sept. 1995.
（2） 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―，”信学誌，vol. 75, no. 10, pp. 1019-1026, Oct. 1992.

著者紹介

尾上　孝雄（正員：シニア会員）

1993 阪大・大学院博士前期課程了．京大助教授，阪大教授，情報科学研究科長などを経て，2019 大阪大学理事・副学長．本会では，調査理事，企画室委員，SIS 研専委員長，ESS ソサイエティ誌担当幹事，大会担当幹事，会計幹事，和文誌(A)編集委員長などを歴任．本会学術奨励賞，論文賞，教育功労賞受賞．IEEE において CAS ソサイエティ理事，Region 10（アジア太平洋地区）理事，副会長，Japan Council 会長など 15 年以上組織運営に関わる．

NOLTA 良いとこ一度はおいで！

NOLTA Society is a great community, come visit sometime!

NOLTA 会長　関屋大雄

1. はじめに

NOLTA ソサイエティ（NLS）[1]は「非線形理論とその応用」（Nonlinear Theory and Its Application）をテーマとして活動しています．現在，ほぼ全てのシステムに「非線形」が含まれており，NLS の議論はあらゆる研究者にとって関連深いといっても過言ではありません．また，線形は非線形の特別な例と考えれば，結局何でも対象になります．そう考えると，本ソサイエティの特徴は，ものの本質を理論から捉え，その上で応用を模索するというアプローチを志向する点にあるといえます．

NLS は発足して 12 年になります．干支が一周し，ソサイエティの運営委員にも新しい元気な顔が次々と加わり，新たな時代に向かっていることをひしひしと感じています．また，論文誌，ソサイエティ誌を通じて研究成果を知の財産として共有します．

2. NLS の活動

NLS の活動として研究と編集があります．ソサイエティメンバーは研究会，国際会議，大会で研究成果を発表し，議論を深め，お互いに知的好奇心を刺激しあいます．

2.1　研究活動

研究会

NLS では非線形問題（Nonlinear Problem : NLP）[2]と複雑コミュニケーションサイエンス（Complex Communication Science : CCS）[3]の二つの研究会が活動しています．

NLP 研究会では，数学・物理学・工学・経済学など，あらゆる分野において観測される非線形現象について，理論，実験，応用などの研究成果の発表が活発に行われています．また，CCS 研究会では，情報通信技術の全ての階層，それを取り巻く情報通信環境，更に神経系や生物システム，人間のソーシャルコミュニケーションまで広範な研究対象を扱い，そこにある現実的問題の本質や限界，そしてその背後に横たわる普遍的特質を明らかにするサイエンスの創出を目指しています．

どちらも興味の対象を広く捉え，物事の本質を捉えることを第一義としており，NOLTA の方向性としてその点は一致しています．

NLS の研究会の特徴として，魅力的な開催場所が挙げられます．2025 年度も，NLP では北海道，高知，伊勢など，CCS も二度の北海道（3 月のルスツはすばらしいですよ！）や金沢での開催が予定されています．研究会参加について，場所から入るのも楽しみの一つかと思います．開催にターゲットを合わせて研究成果を出して頂けるとよいのではと思います．また，学生や若手研究者の奨励も NLS の特徴です．多様な研究に対し広く門戸を開け，研究の本質をお互いに理解しようとする土壌があります．初参加の方ももちろん大歓迎です．ぜひご発表を計画ください．

大会

NLS では「大会」として，3 月に開催される電子情報通信学会総合大会，9 月に開催される同ソサイエティ大会，そして 6 月に開催される NLS 大会の三つの「大会」で研究議論の場を設けています．その中で，NLS 大会は NLS が主催・運営する大会です．今年は 6 月に岡山で開催されます．執筆時はまだ大会前ですが，今年は会場が図 1 のような能舞台，懇親会も岡山城で開催されることとなっており，盛り上がること間違いなしです．

図 1　2025NLS 大会会場である岡山 Tenjin9

図 2　NOLTA2024 開催前：Phenikaa University への表敬訪問

国際会議

NLS の活動方針の特徴として，国際活動が活発であることが挙げられます．まず，フラグシップカンファレンスとして「NOLTA」があり，毎年開催されています．今年は 10 月下旬に沖縄で開催されます．後述するように，近年アジアを中心とした海外との交流が盛んであり，韓国を筆頭に 15% の論文が海外からの投稿となりました．

もう一つの会議は韓国マルチメディアソサイエティ（Korea Multimedia Society：KMMS）と共同で開催される Complex Communication and Multimedia Science（CCMS）です．この会議は従来の Korea-Japan（Japan-Korea）CCS からリニューアルし，KMMS のフラグシップカンファレンスである MITA と併催されるワークショップとして 7 月に韓国済州島で開催されます．KMMS との交流は 10 年以上にわたり続いており，その関係はますます充実したものとなっていくでしょう．また，韓国の KICS（Korean Institute of Communication Science）との交流も盛り上がっており，KICS 主催の国際会議に技術協賛も行っています．

更に昨年はベトナムで NOLTA 国際会議を開催し，その前には図 2 のように，ベトナムでホスト役を担当頂いた Phenikaa University を NLS 委員で表敬訪問し，交流を深めました．

NLS は今後もアジアを中心とした国際交流に更に積極的に取り組んでいきたいと考えています．

2.2　編集活動

NLS からは二つの出版物を発行しています．一つは論文誌である「NOLTA，IEICE（以降，NOLTA ジャーナル）」[4]，もう一つは，基礎・境界ソサイエティと共同編集をさせて頂いているこの機関紙，「Fundamentals Review」（以降，FR）[5]です．

Nonlinear Theory and Its Application, IEICE

NOLTA ジャーナルはオープンアクセスジャーナルで，どなたでも無料でお読み頂くことができます．また，現在 Emerging Source Citation Index（ESCI）に登録されており，インパクトファクタもついております（最新 2023 年の IF：0.5）．更に，今年からは Scopus Index に登録されることが決まりました．これは，NOLTA ジャーナル編集チームの地道な編集活動と，多くの方に投稿して頂いた結果です．

IF は決して高いとはいえませんが，今後更に NOLTA ジャーナルの認知度が上がり，多くの方に投稿し，読んで頂けるよう，今後ソサイエティ全体で NOLTA ジャーナルを盛り上げていきたいと考えています．

Fundamentals Review

FR は基礎・境界ソサイエティと NLS がカバーする研究分野のトピックを広く網羅した記事を発行している機関紙で，当方も 2021,2022 年度に編集委員長を仰せつかっておりました[6]．FR の記事は，教科書的な基礎的内容から最新の専門的解説まで多様なトピックを様々な角度で網羅しており，どの記事も読みごたえのある記事になっています．NLS として，今後も FR に良質な記事を提供することで，ソサイエティの技術発信を積極的に行えればと考えています．

3. NLS の将来

技術の進歩は数年前の想像をはるかに超え，一人の力で全ての動向をカバーするのは不可能になっています．もちろん AI に頼るという考え方もありますが，人と人とのネットワークによる情報共有や知的交流の価値は，むしろ今後更に高まっていくことでしょう．NLS は，そんな研究者同士がつながる場です．興味や情熱をもつ研究者が集まり，そこに知の泉が湧き，その泉が次の研究者を引き寄せる―そんな理想的なサイクルを実現する場でありたいと考えています．

NLS の特徴は，研究トピックが常に流動的で，その時々の社会や研究のニーズに応じて自発的に変化していける柔軟さにあります．ソサイエティの運営においては，その自由で創造的な活動を妨げない「場」を提供することが最も大切です．当方が会長を務めるこの 1 年も，より魅力的で活発な交流の場となるよう，力を尽くしていきたいと思っています．

4. おわりに

以上，NLS の活動をご紹介しましたが，最後に私と NLS との関わりについて少しお話しします．

私は学生時代から回路理論の研究に取り組み，とりわけ回路に生じる非線形現象の解析に大きな関心をもち続けてきました．研究会デビューは NLP 研究会で（当時はまだ CCS 研究会はありませんでした），温かくも厳しいご意見を頂きながら研究を深め，「NLP に育ててもらった」という強い思いがあります．

その後は非線形回路にとどまらず，ディジタル信号処理や無線通信，電源回路など，興味をもったテーマに次々と挑戦しています．しかし，課題の捉え方や解決へのアプローチには常に NOLTA 流のエッセンスが宿っていると自覚しています．その発想や視点が新たな分野で新鮮に映り，それぞれの分野が当方の挑戦を受け入れ，そして後押ししてくれているのだと思います．

これも，NOLTA が大切にしている「理論をしっかり押さえたうえで応用へ展開する」という教えのおかげだと感じています．私はよく『私には NOLTA の血が流れている！』と冗談交じりに話しています．

NLS は，「非線形」という共通テーマのもと，様々な分野の研究者が集い，自由闊達に議論できる唯一無二のコミュニティです．そこには新たな技術の種やアイデアが数多く潜んでおり，議論を通じてきっと皆さんの研究への知的好奇心が大きく刺激されることでしょう．

NOLTA 良いとこ，一度と言わずに何度もおいで！

文　献

（1） NOLTA Society, https://www.ieice.org/nolta/nolta_r/index.php.
（2） 非線形問題研究会，https://www.ieice.org/~nlp/.
（3） 複雑コミュニケーションサイエンス研究会，https://www.ieice.org/~ccs/.
（4） Nonlinear Theory and Its Applications, IEICE, https://www.jstage.jst.go.jp/browse/nolta/-char/en.
（5） Fundamental Review，https://www.ieice.org/ess/ESS/Fundam-Review.html.
（6） 関屋大雄，“FR 誌の将来像：より多く，より若い読者へ，”信学 FR 誌，vol. 15, no. 2, pp. 68-69, 2021.

著者紹介

関屋大雄（正員：フェロー）

2001 慶應義塾大学大学院理工学研究科電気工学専攻修了．博士（工学）．同年より千葉大学に着任，現在大学院情報学研究院教授．これまでに非線形回路理論，画像・音声のデジタル信号処理，無線通信方式，パワーエレクトロニクスなどの研究に従事．電子情報通信学会の活動として，FR 誌編集委員長（2021，2022），Communication Express 編集委員長（2018，2019），通信ソサイエティマガジン編集委員長（2023，2024），CCS 研究会委員長（2015），EE 研究会委員長（2024，2025）など．

解　説　論　文

軽量認証暗号 Ascon について

On Lightweight Authenticated Encryption Scheme Ascon

峯松一彦 Kazuhiko MINEMATSU

アブストラクト　共通鍵暗号は現代の情報通信の安全性を支える基盤となっている．特に近年，通信文の改ざんを防ぎつつ通信内容の秘匿性を守る認証暗号の重要性が広く認識されて，幅広く使われてきている．一方認証暗号は単なる暗号化より計算コストが大きいため，計算資源の乏しい利用環境に適した軽量な認証暗号の必要性が高まっている．この背景のもと米国 NIST は軽量認証暗号の標準化コンペティションを行い，2023 年に Ascon という方式を最終選出した．本稿ではこの Ascon の仕様や安全性解析状況，実装性能などについて概説する．

キーワード　共通鍵暗号，認証暗号，軽量暗号，Ascon，スポンジ構造

Abstract　Symmetric-key cryptography serves as a security infrastructure of digital societies. In particular, the importance of authenticated encryption (AE), which provides the confidentiality and authenticity of communication, has been widely recognized. On the other hand, since an AE scheme is generally costlier than plain encryption schemes, there is a growing need for lightweight AE suitable for use in constrained environments. With this background, the National Institute of Standards and Technology (NIST) of the United States conducted a standardization project for lightweight AE and selected Ascon as the sole winner in 2023. In this paper, we outline the specifications, security, and implementation aspects of Ascon.

Key words　Symmetric-key cryptography, Authenticated encryption, Lightweight cryptography, Ascon, Sponge construction

1. はじめに

共通鍵による暗号化方式として，ブロック暗号を用いたカウンターモード（CTR）暗号化などがよく知られている．これらの暗号化方式はその安全性，すなわち平文の秘匿性，が数学的に証明可能であるものの，改ざんに対して無力である．例えば 1 ブロック平文 M をブロック暗号 E を用いた CTR で暗号化する場合，事前に送信者と受信者でブロック暗号の鍵 K を共有しておき，つぎにブロック暗号 E でカウンター値（$1, 2, \ldots$ と暗号化のたびに増加させる値）ctr を暗号化しその結果を 1 ブロック平文 M と加算（排他的論理和）をとることで暗号文 C を得る．受信者にカウンター値と暗号文とを送信する．ここで，もし送信内容である通信文 (ctr, C) を入手した攻撃者が暗号文へ任意の値 δ を排他的論理和し，カウンター値は変更せずに復号側に送信した場合，受信者は，もとの 1 ブロック平文 M へ攻撃者が選択した δ を加算した値を復号結果として得ることになる．攻撃者は，もとの 1 ブロック平文 M は未知なものの，δ で 1 が立っているビット位置について，1 ブロック平文 M の同じ位置のビットを反転できることになる．1 ブロック平文 M が制御コマンドであったり，数字であったりすれば重大な危険をはらむことは容易に想像できる．

認証暗号（Authenticated Encryption, AE）とは，共通鍵暗号化の機能の一種であり，暗号文から平文情報を秘匿しつつ，上記のような改ざん攻撃を検知することで改ざんから暗号文を守るものである．認証暗号の形式的な定義は 2000 年代初頭に確立[1],[2]し，その重要性は近年ますます高まっている．現在のインターネットプロトコルや無線網におけるデータ通信はかなりの割合で何らかの認証暗号方式を採用しており，著名な CBC モードへのパディングオラクル攻撃[3]に代表されるように改ざん検知のない暗号化のみの方式を用いることは現実的なリスクとして広く認識されつつある．

一方，認証暗号は通常の暗号化のみの方式と比べて一般に大きい計算コストを要請するため，計算資源の乏しい環境などへ広く適用を行うためには，現行の標準的な認証暗号方式（例えば米国標準技術研究所（NIST：National Institute of Standards and Technology）推奨方式の AES-GCM[4]や AES-CCM[5]）と比べて計算量や消費メモリの少ない，軽量な認証暗号が望ましい．この動機に基づき様々な軽量認証暗号方式の研究が活発に行われている．本稿では，そのような軽量認証暗号方式のなかで，NIST が標準化を進めている Ascon[6]という方式について解説する．

峯松一彦　正員　日本電気株式会社　セキュアシステムプラットフォーム研究所
E-mail k-minematsu@nec.com
Kazuhiko MINEMATSU, Member (Secure Systems Platforms Laboratories, NEC Corporation, Kawasaki-shi, 211-8666 Japan).

電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.19 No.1 pp.7–14 2025 年 7 月

2. 認証暗号

まず一般的な認証暗号の入出力について説明する．認証暗号 Π の暗号化関数 Π.Enc には，秘密鍵 K，平文 P，ナンス (Nonce) N，及び付帯データ（Associated Data, AD）A が入力される．ここでナンスは暗号化のたびに更新される値で，暗号学的な秘匿性を満たすために必要である．ナンスの存在により，同じ平文が同じ暗号文に暗号化されることを防ぐ．ナンスは乱数や，あるいはカウンターにより実現可能である．AD は暗号化はしないがメッセージ認証は行いたいデータであり，例えばプロトコルのヘッダや送信者・受信者のアドレスなどが該当する．一般に平文 P, AD A は可変長の系列である．$\Pi.\mathrm{Enc}(K, N, A, P) = (C, T)$ であり，ここで C は暗号文，T は認証に用いるタグである．典型的に T の長さは短い固定長である．方式によっては明示的なタグをもたず暗号文 C に暗黙的に含まれる場合もあるが，Ascon の場合はタグが存在する．一般に送信者は受信者へ四つ組 (N, A, C, T) を送信する．復号関数 Π.Dec は鍵 K，ナンス N，AD A，暗号文 C，そしてタグ T を入力として，入力の完全性を検証し，もし正当である，すなわち改ざんがないと判断した場合には復号結果の平文 M' を，もし改ざんを検知した場合にはエラーシンボル $\perp$ を出力する．本稿で紹介する Ascon や，現行の NIST 推奨方式 AES-GCM と AES-CCM もこのインタフェースに従う．

2.1 NIST Lightweight Cryptography Competition

Ascon はオーストリアのグラーツ工科大学の研究者たち（提案当時．現在はインテルなどの企業所属の研究者もいる）により設計され，認証暗号の学術的なコンペティションである CAESAR[7] に提案された．2019 年に CAESAR コンペティションは終結し，Ascon は Lightweight applications (resource constrained environments) カテゴリーにて first choice として選出されている．

NIST は CAESAR コンペティションと並行して，2018 年頃から標準化要件のヒアリングなどをはじめ，2019 年より公式に NIST Lightweight Cryptography コンペティション（NIST LwC）[8]を行い軽量認証暗号方式の標準化活動を開始した．2019 年 3 月の公募締め切りで 57 件の提案があり，2 回のラウンドを経て 10 件のファイナリストに絞り込まれた．これらファイナリストの中から，2023 年の 2 月に NIST は最終選考方式として Ascon を選出した．NIST は Ascon の標準化を進めており，現在はドラフト標準仕様文書[9]が公開されている．Ascon の仕様自体は CAESAR コンペティションから大きくは変更されていない．詳細は後述する．

3. Ascon の仕様

3.1 認証暗号

Ascon はスポンジ[10]と呼ばれる構成をしている．これはある程度大きな入出力幅をもつ鍵なしの暗号学的な置換 p を用いて，p を繰り返しながら，置換の出力の一部のみをデータ処理に用い，残りの部分は保持する方式である．繰り返しにおける初期値は鍵とナンスから構成され，最後の出力の一部を切り出してタグとする．データ処理に用いる部分をレート部，保持したままの部分をキャパシティ部と呼ぶ．キャパシティ部を無視し，置換をブロック暗号とみれば，暗号化部分は Ciphertext Feedback (CFB) モードに類似している．CFB モードでは，ある平文ブロック M に対応する暗号文ブロック C は，直前の暗号文ブロック C' をブロック暗号で暗号化した値 S と排他的論理和をとることで得られる．すなわち，$C' = S \oplus M$（ただし $\oplus$ はビットごとの排他的論理和を表す）である．Ascon においては，暗号化処理における中間状態（レート部）を変数 S とし，平文ブロック M を用いて暗号文ブロック $C = S \oplus M$ を得る．次のブロックの暗号化のために S を置換 p へ入力して更新する．一方，AD 処理は CBC-MAC モードに類似しており，中間ステート S とメッセージブロック A を用いて S を $S \oplus A$ に更新するものである．また，置換を用いた認証暗号構成方法（利用モード）の SpongeWrap[11]と類似している．

全体的な暗号化処理を図 1，復号処理を図 2 に示す．図が示すように極めて対称性の高いアルゴリズムである．Ascon が用いる鍵なし暗号学的置換は Ascon-p と呼ばれる 320 ビット入出力の置換である．図では p で表される．p^a は p を a 回繰り返すことを表す．鍵 K，ナンス N，タグ T はどれも 128 ビットである．レート部は r ビット，キャパシティ部は c ビットであり，$r + c = 320$ を満たす．系列 $(A_0, A_1, \ldots, A_m)$ が AD，$(P_0, P_1, \ldots, P_n)$ が平文，$(C_0, C_1, \ldots, C_n)$ が暗号文を示す．暗号化処理は初期化の Initialization，AD 処理の Associated Data，平文暗号化の Plaintext，そしてタグ生成の Finalization

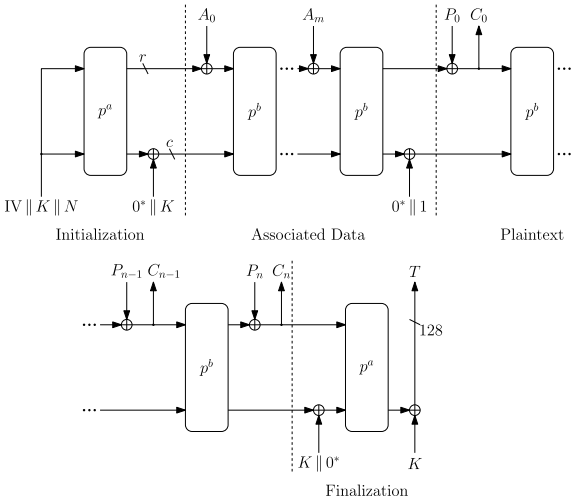


図 1　Ascon の暗号化処理

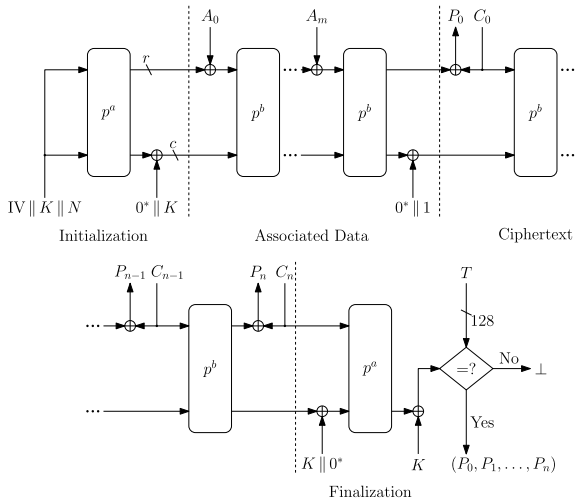


図 2　Ascon の復号処理

という直列したプロセスに分かれている．図 1 と図 2 に現れる Initialization (IV) は 64 ビットの固定値である．スポンジを用いた認証暗号方式は様々なバリエーションをもつが，Ascon では鍵 K は初期化の前後でステートに入力あるいは加算され，また Finalization の前後においても加算されているのが特徴的である．$a > b$ となっているが，これはスポンジを用いた認証暗号によくみられる事象であり，直列な処理の最初と最後を相対的に重たい，すなわち暗号学的に複雑な処理とし，代わりに比較的攻撃の自由度が低い中間の処理を軽くすることで全体の安全性と効率のバランスをとることを目的としている．NIST LwC 提案時には (r, c, a, b) として複数のパラメータが提案され，特に $(r, c, a, b) = (64, 256, 12, 6)$ が Ascon-128, $(r, c, a, b) = (128, 192, 12, 8)$ が Ascon-128a として提案されていたが，NIST のドラフト標準仕様文書においては Ascon-128a をベースとし，より短いタグの許容など細部の変更を加えた Ascon-AEAD128 が提案されている．今後大きな変更はないと予想されるが最終的な仕様はまだ変更の可能性がある．

3.2　ハッシュ関数

NIST LwC の公募案件ではハッシュ関数の提案もオプションとなっており，Ascon にはハッシュ関数のモードも存在する．NIST ドラフト標準文書では Ascon-Hash256 と呼ばれる 256 ビット出力のハッシュ関数と，出力が可変長の Ascon-XOF128 (XOF は eXtendable output function の略)，及びその “customizable” バージョンである Ascon-CXOF128 が示されている．Ascon-Hash256 は SHA-3 と同様の典型的スポンジ構造のハッシュ関数である．図 3 に示す．ここで $(M_0, \ldots, M_n)$ がメッセージ，$(H_0, \ldots, H_{\lfloor L/64 \rfloor - 1})$ は L ビットのハッシュ値である．ここでは $a = 12$ の p^a を常に使う．$r = 64$, $c = 256$ となっている．64 ビットの IV が存在し，これは認証暗号のときの IV とは異なる値である．メッセージをレート部にて処理したのち，Squeeze と呼ばれる処理で 64 ビットずつハッシュ値を確定させていく．Ascon-Hash256 では $L = 256$ とすることで 256 ビットハッシュ値を出力する．可変長出力バージョンについては L を所望の数値に設定する．また CXOF128 においてはメッセージの処理の前に customization string と呼ばれる系列をメッセージと同様に処理する．これらの詳細についてはドラフト文書を参照のこと．

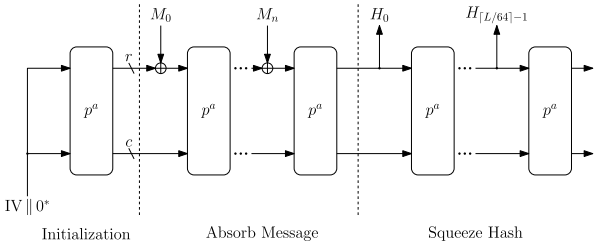


図 3　Ascon のハッシュ処理

3.3　Ascon-p

320 ビットの暗号学的置換 Ascon-p は古典的な Substitition-Permutation Network (SPN) 型であり，定数加算 p_C，非線形部 p_S，線形部 p_L の三つの処理の合成からなる．すなわち $p = p_L \circ p_s \circ p_C$ である．p の入出力状態（ステート）は 64 ビットワード X_i, $i = 0, 1, 2, 3, 4$ を用いて $X_0 \| X_1 \| X_2 \| X_3 \| X_4$ と表現される．繰り返し処理 p^a ないし p^b を行うにあたり，処理 p_C はループ内の繰り返しの回数と合計の繰り返し回数に応じた定数を X_2 に排他的論理和する．また処理 p_S は 5 ビットの S-box と呼ばれる非線形置換を 64 個並列に適用する．S-box を図 4 に示す．この S-box は SHA-3 で用いられている χ 関数と類似している．XOR ゲート ($\oplus$) と AND ゲート ($\odot$) とを規則正しく配置し，少ないゲート数で比較的高い暗号学的安全性を担保できるのが特徴である．処理 p_L は各 64 ビットワード X_i へ，以下のように巡回シフトと排他的論理和を組み合わせた線形変換を適用する．なお $X_i \ggg j$ は X_i の j ビット右巡回シフトを表す．

$$
\begin{aligned}
X_0 &\leftarrow X_0 \oplus (X_0 \ggg 19) \oplus (X_0 \ggg 28) \\
X_1 &\leftarrow X_1 \oplus (X_1 \ggg 61) \oplus (X_1 \ggg 39) \\
X_2 &\leftarrow X_2 \oplus (X_2 \ggg 1) \oplus (X_2 \ggg 6) \\
X_3 &\leftarrow X_3 \oplus (X_3 \ggg 10) \oplus (X_3 \ggg 17) \\
X_4 &\leftarrow X_4 \oplus (X_4 \ggg 7) \oplus (X_4 \ggg 41) \qquad (1)
\end{aligned}
$$

上述のように Ascon-p は 320 ビットのステートを五つの 64 ビットワード $X_0, \ldots, X_4$ で表している．図 5 は五つの 64 ビットワード $X_0, \ldots, X_4$ を縦に並べて，非線形部 p_S（図の左側）と線形部 p_L（図の右側）を実行するときのステートの更新方法を示している．非線形部 p_S は $i = 0, 1, \ldots, 63$ について各ワードの i 番めのビットをとることで得られる 5 ビット $(x_0, x_1, x_2, x_3, x_4)$ を S-box へ適用する．線形部 p_L は式 (1) の変形を各 $X_0, \ldots, X_4$ について実行する．なお Ascon の実装においてはビットスライス実装を用いるのが通常である．ビットスライス実装により S-box を論理ゲートごとに並列に処理することができ，かつ S-box の表引きを行わないことで，ソフトウェアにおけるキャッシュ攻撃のリスクを避けることが可能である．

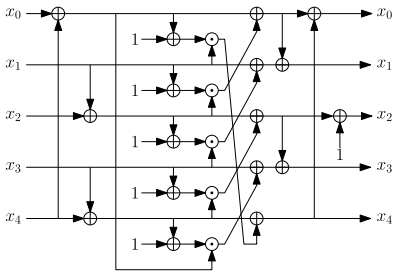


図 4　Ascon の 5 ビット S-box

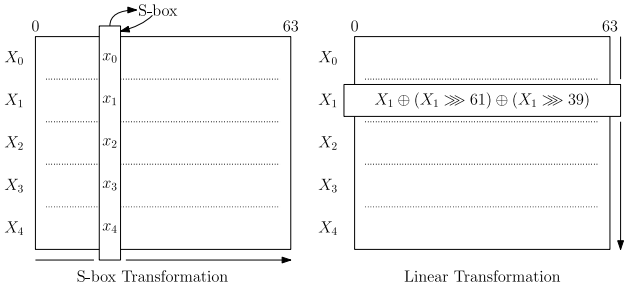


図 5　Ascon の内部状態　左側が非線形部 p_S，右が線形部 p_L を表す．

4.　Ascon の安全性

Ascon の安全性を概説する．認証暗号の基本は秘匿性（Confidentiality）と完全性（Integrity 若しくは Authenticity）である．Ascon はいずれの指標においても 128 ビット安全性を目指して設計されている．最初の CAESAR コンペティションへの提案以来この安全性クレームを危殆化させるような攻撃は報告されていない．

4.1　証明可能安全性

Ascon の安全性を構造的に評価する手法として，p^a と p^b を公開ランダム置換（Public random permutation）とみなし，秘匿性と完全性を数学的に証明するアプローチ—いわゆる証明可能安全性がある．公開ランダム置換とは，誰もが入出力を計算可能かつ完全にランダムな置換であり，暗号研究においてよく知られたランダムオラクルの置換バージョンと位置付けることができる．320 ビット置換の数は $(2^{320})!$ 個存在し，この中からランダムに一つ置換を選ぶことで実現できる．

a）　安全性バウンド

秘匿性と完全性は，攻撃者が認証暗号をオラクル（クエリのできるブラックボックス）としたある種のゲームの成功確率として定義することが可能である．ゲームの成功確率が低いほど安全であるということができる．この成功確率の上界のことを共通鍵暗号の分野においては一般に安全性バウンドと呼び，安全性バウンドが十分小さいことを（内部で用いるブロック暗号などへの妥当な数学的仮定のもと）示すのが安全性の観点から重要である．本稿では簡単のため，秘匿性と完全性とを一体化させた安全性の定義を中心に議論を進める．まず公開ランダム置換を p とし，p を用いた認証暗号モードの暗号化オラクルを

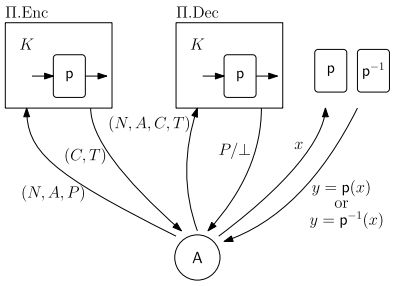


図 6　識別ゲームにおける Real world

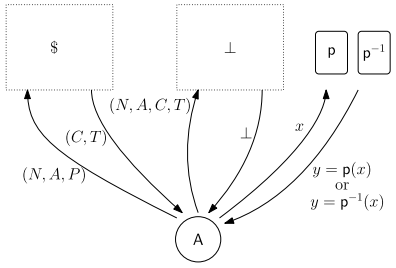


図 7　識別ゲームにおける Ideal world

$\Pi[\mathsf{p}].\mathrm{Enc}$，復号オラクルを $\Pi[\mathsf{p}].\mathrm{Dec}$ とする．また $ オラクルを，任意の暗号化クエリに対して $\Pi[\mathsf{p}].\mathrm{Enc}$ と同じ長さの一様乱数を返すオラクル，$\perp$ オラクルを，任意の復号クエリに対してエラーシンボル（復号失敗）を返すオラクルとする．公開ランダム置換 p の正順計算を行うオラクルを p，逆順計算オラクルを p^{-1} と表す．任意の x について $\mathsf{p}^{-1}(\mathsf{p}(x)) = x$ である．両方のクエリを許すオラクルを $\mathsf{p}^{\pm}$ と表記する．これらの記法のもと，

- 現実世界 (real world): $\mathcal{O}_r = (\Pi[\mathsf{p}].\mathrm{Enc}, \Pi[\mathsf{p}].\mathrm{Dec}, \mathsf{p}^{\pm})$
- 理想世界 (ideal world): $\mathcal{O}_i = (\$, \perp, \mathsf{p}^{\pm})$

を定義し，

$$\mathbf{Adv}^{\mathrm{ae}}_{\Pi[\mathsf{p}]}(\mathsf{A}) := \left|\Pr[\mathsf{A}^{\mathcal{O}_r} = 1] - \Pr[\mathsf{A}^{\mathcal{O}_i} = 1]\right| \qquad (2)$$

を攻撃者 A の攻撃成功の AE 利得（AE Advantage）とする．AE 利得は上述した秘匿性と完全性を合わせた安全性概念を反映した識別ゲームの成功確率を表している．すなわち，AE 利得が小さいほど認証暗号として安全であることを意味する．図 6 と図 7 も参照のこと．なお $\mathsf{A}^{\mathcal{O}_r} = 1$ は A が $\mathcal{O}_r$ 内部のオラクルへ任意の順序でクエリを行い，得られた結果から最終的に 1 ビットを出力するものとしたときにそれが 1 であるイベントを意味する．ここでの攻撃者の役割は二つの世界のクエリによる識別であり，利得が小さいということは識別が困難であることを示している．理想世界においては暗号化の結果がクエリに全く依存していないこと，また復号において常に $\perp$ しか返ってこないことと改ざん成功確率がゼロであることから，完璧に安全な認証暗号を前にした攻撃者が直面するであろう状況をモデル化しているといえる．なお理想世界はそもそも鍵も存在せず復号可能な認証暗号をなんら示していないが，これは安全性定義や証明における簡便さを重視したためである．真に復号可能（ただし鍵は指数長）で，p を内部で用いない理想的な認証暗号を定義し，これを理想世界のオラクルとして定義することも可能である．安全性の議論はほぼ変わらない．また，重要なポイント

として，いずれの世界においても公開ランダム置換 p へのアクセスが許されている点があり，これは Ascon-p 自体の計算は攻撃の任意の時点で可能であることをモデリングするものといえる．AE 利得を定めるゲームにおいて，攻撃者が順守するルールとしては，以下の二つがある．

（1） A が暗号化オラクルへのクエリについては毎回異なるナンスを用いること．nonce-respecting と呼ばれる．

（2） 復号オラクルへ自明に受理されるクエリをしない，すなわち暗号化オラクルへのクエリ (N, A, P) と返答 (C, T) から得られた (N, A, C, T) をクエリしないこと．

このルールのもと $\mathbf{Adv}^{\mathsf{ae}}_{\Pi[\mathsf{p}]}(\mathsf{A})$ が現実的な範囲の A について十分小さいことが証明できれば，その認証暗号 Π は公開ランダム置換の仮定のもと安全と結論される．

Ascon の公開ランダム置換ベースの証明としては幾つか知られている．例えば Jovanovic ら[12]はスポンジベースの認証暗号の証明を与えた．その仕様は幾つか Ascon とは異なる点があり，文献(12)では Ascon もほぼ同様に証明が得られると述べてあるが具体的な証明はなかった．ごく最近，Lefevre と Mennink による Ascon に特化した秘匿性，完全性の評価が与えられた[13], [14]．ここではこのバウンド（上界）を概説する．暗号化クエリ数を q_e，復号クエリ数を q_d，それぞれのクエリでのオラクルが処理する総ブロック数を σ_e, σ_d とし，$\sigma = \sigma_e + \sigma_d$ とする．また置換オラクル $\mathsf{p}^{\pm}$ へのクエリ数を q_{p} とする．秘匿の利得と完全性の利得の和で AE 利得を上界できることを利用すると，これらの表記のもと $\mathbf{Adv}^{\mathsf{ae}}_{\mathrm{Ascon}}(\mathsf{A})$ は

$$\mathcal{O}\left(\frac{q_d}{2^t} + \frac{\sigma + q_{\mathsf{p}}}{2^k} + \frac{\sigma_e + q_{\mathsf{p}}}{2^n} + \frac{\sigma_d \cdot (\sigma + q_{\mathsf{p}})}{2^c} + \frac{q_{\mathsf{p}}}{2^c}\right) \quad (3)$$

と上界ができる．定数の評価もなされており，値は小さい．極めて大雑把にいえば，鍵空間のサイズ 2^k，タグ空間のサイズ 2^t，とキャパシティの半分の大きさの空間のサイズ $2^{c/2}$ が攻撃者の計算量より十分大きければ安全であると解釈できる．Ascon-AEAD128 では $k = t = 128$, $c = 192$ であるため，公開ランダム置換モデルのもと，現実的に十分な安全性があるといえる．なお $c/2 = 96$ となり本章冒頭で述べた 128 ビット安全性と矛盾するようにみえるが，設計者は攻撃クエリによるデータ量を 2^{64} に制限しているため矛盾は生じない．より精密な評価や，ナンスを繰り返した場合の完全性の議論などは文献(14)を参照のこと．

b） 安全性の直感的説明

安全性証明の直感をごく大雑把にいえば，暗号化と復号のいずれにおいてもキャパシティ部が攻撃者からは（自明な一致を除いて）予測できないという点にある．例として暗号化クエリで (N, A, P, C, T) という組を入手し，復号クエリ (N', A', C', T')，ただし $(N', A', C', T') \neq (N, A, C, T)$，を行う場合を考える．まず $N \neq N'$ の場合，Initialization を終えたあとの内部状態（レート部とキャパシティ部の連結）が完全にランダムとなり，A' によらず AD 処理を終えたあとの状態もランダムとなる．暗号文 C' のブロックは自由に選べるため復号におけるレート部の入力は自由に選択できるが，キャパシティ部は制御できず，ランダムな値が Finalization まで連鎖していく．Finalization において p^a に入る値が推測あるいは既存のクエリで生起した状態の値と一致しない限りタグは未知の乱数となり，推測によりそれが T' となる確率，すなわち偽造に成功する確率は $1/2^{128}$ となる．この議論は置換への直接クエリの存在を考慮しても成立する．次に $N = N'$ であるが $A' \neq A$，ただし $(A'_0, \ldots, A'_i) = (A_0, \ldots, A_i)$, $A'_{i+1} \neq A_{i+1}$ である場合を考える．このとき，A'_i ブロックの処理までは内部状態は全く変わらないが，A'_{i+1} ブロックの処理により必ずレート部が変更され，結果として高い確率で次の置換入力が未知の値となる．これにより上記と同様のキャパシティ部のランダムな連鎖が発生し，正しいタグが予測不可能となる．次に $(N', A') = (N, A)$ かつ $C' \neq C$ の場合を考える．上のケースと同様に C' と C で最初に異なるブロックを C'_{j+1} とする．C'_{j+1} を任意に選択できるものの，これをレート部に入れたときに対応するキャパシティ部の値が分からないため，高い確率で C'_{j+1} の復号における置換入力が未知となる．これにより次以降のキャパシティ部のランダムな連鎖が発生する．最後に $(N', A', C') = (N, A, C)$ かつ $T = T'$ の場合であるが，これは (N, A, C) を受理するような真のタグが T ただ一つであることから必ず偽造は失敗する．以上の観測から，安全性のバウンドには，暗号化と復号で発生したキャパシティ部の値のバリエーション $\mathcal{S}$ の中でたまたま衝突が発生する確率と，$\mathcal{S}$ と置換への直接クエリの回答から決まるキャパシティ部の値がたまたま一致する確率との和が寄与することが見て取れる．もちろん鍵やタグを直接推測できる確率もこれに加える必要がある．

反対にもしキャパシティ部がないか，あるいは推測が当たりそうなくらい小さい場合はどうなるだろうか考えてみる．すると，復号クエリにおいて N' や A' をどう決めたとしても C' で置換入力をほぼ確定させることができるため，適当な暗号化クエリで得た (N, A, C, T) に対して，適当な (N', A', C', T') で，ある $j+1$ ブロック目以降の暗号文ブロックとタグを暗号化クエリのそれと一致させることで偽造が高い確率で成功することが分かる．これは上述のように暗号化部分がキャパシティ部を無視した場合 CFB モードと同じとみなせ，CFB モードには改ざん検知能力がないことからも分かる．一方，AD 処理においては，設計の細部に注意すれば原理的にはキャパシティがなくとも安全性を担保できることが分かる．例えば佐々木と安田[15]によりこのような Sponge ベース認証暗号が提案されている．

c） Ascon の初期化と終端処理

Ascon の初期化と終端処理において置換の前後双方に鍵が入力されている．この鍵入力はベースとなった SpongeWrap などが示すように原理的に冗長な部分があり，一番ミニマムには初期化の入力だけ鍵が入っていれば公開置換ランダムモデルでの安全性は原則担保できる．例えば NIST LwC ファイナリストの Xoodyak[16]がそのようなミニマムな鍵入力を採用している．ただしこのような鍵入力箇所の最小化によって安全性バウンドの項の幾つかが劣化するうえ，中間状態をリークさせるような攻撃があれば，鍵が完全に漏洩するといった副次的なマイナス要因もある．また一般的には初期化と終端処理で鍵入力の箇所を増やすことで実際の仕様での攻撃に対しての耐性向上が図れる．

d） 安全性モデルの妥当性

公開ランダム置換を用いた証明の問題として，公開ランダム置換が現実的に実現不可能であるという点がある．Ascon-p は鍵なし置換であるため，そもそもランダム性がない．また，$(2^{320})!$ 個の置換の中から真にランダムに選択されたわけでもないことは設計プロセスからも明らかである．更に公開ランダム置換は置換の中身自体を攻撃者に明らかにするわけではない（ブラックボックスとして機能しなければならない）．したがって，暗号学的置換の複雑さとは関係なく，証明と実物には本質的なギャップがある．公開ランダム置換を用いた証明はこのような問題がある一方，暗号学的置換の利用モードとして構造的な欠陥のないことを示すためには有用である．例えば公開ランダム置換ベースの証明がうまくいかないような攻撃が発見されれば，それは（恐らくあらゆる置換を用いた場合の）実際の方式の攻撃として利用可能であろう．実際に SHA-3 などのハッシュ関数や，Even-Mansour 型ブロック暗号の構成[17]などでは公開ランダム置換の仮定は広く利用されており，証明可能安全性のアプローチとして受け入れられている．既存の Ascon の安全性証明は全て公開ランダム置換を用いた証明となっている．

更に付随したトピックとして，Ascon の証明においては二つの置換 p^a と p^b が登場するが，これらを独立の公開ランダム置換と仮定するか，あるいは単独の公開ランダム置換とするべきかという問題がある．これは研究者の間でも議論がある．本稿で示した安全性バウンドは文献(14)をベースとし，独立な置換と仮定しているが，単一の置換としても特段大きな変化を生まないことが指摘されている[14]．いずれにせよ公開ランダム置換の導入により，古典的な標準モデルの安全性とは解離を生じているため，独立か単一とすべきか，どちらが妥当かは論理的には決定不可能である．今後の議論が必要と思われる．

なお，上述のギャップは GCM, CCM, OCB[18]といったブロック暗号利用モードの認証暗号では発生しない．これらの認証暗号方式では，方式の安全性を，ランダムな鍵が与えられたブロック暗号と真のランダム置換との判別確率に帰着している．これは標準モデル証明と呼ばれている．標準モデル証明があることにより “用いるブロック暗号が安全ならば利用モードも安全” という極めて直感的かつ正しい説明を与えることができる．

4.2 認証暗号としての暗号解析

Ascon を，その置換も含めて仕様どおりに捉えた解析研究は多数知られている．ブロック暗号への代表的な解析手法である線形解析・差分解析やそれらの混合である線形差分解析などがある．いずれも Ascon-p の繰り返し回数 a ないし b をより小さくとった場合の解析である．設計者の解析論文[19]において線形差分解析が示され，a を 5 とした場合の攻撃を検証可能な形で示している．本攻撃の改良手法は Liu ら[20]で示されている．

現在時点で最も大きい段数への攻撃を示しているのは Cube 攻撃である．これは暗号化処理をビット表現した式の代数次数に着目した攻撃であり，a を 7 とした場合の攻撃が知られている．ただしここでの攻撃は計算量が設計者の安全性クレームを下回るような攻撃であり，その計算量は必ずしも現実的なものではない，学術的な意味では有効な（鍵の総当たりよりも計算量が少ない）攻撃であることに留意が必要である．Hu による Cube 攻撃[21]では $a = 7$ の場合の現時点で最良の計算量をもつ鍵回復攻撃が示されている．そのほか最新の解析研究については，NIST LwC の最終報告書[22]や設計者のページ[23]や藤堂による CRYPTREC 外部報告書[24]が詳しい．

また，Nonce-respecting 条件を排除した場合の攻撃も研究されている．本来はこのような攻撃は設計者の条件を違反するものであるが，実際の利用シーンを考えた場合，ナンスが暗号化において重複してしまう誤用は考えられる．例えば GCM においてはナンスの 1 回の重複が認証に用いる部分の鍵を漏洩するため，任意の暗号文に対して有効なタグを計算することが可能となる（すなわち偽造が成功する）ことがよく知られている[25]．したがって，Nonce-respecting の想定で設計された方式についてもナンスの重複が起きたらどうなるかを調べることは，認証暗号のロバストネスを測る意味でも意義がある．

Ascon の暗号化がオンラインで可能なことから，同じナンス，同じ AD で前半 i ブロックが等しい平文を暗号化した場合，前半 i 暗号文ブロックが一致することが分かる．したがってナンス重複により平文の部分情報が漏洩し，秘匿性は破られている．一方，完全性のみに着目した場合はナンス重複があっても，公開ランダム置換の仮定のもとでは安全であることが示されている[14]．

一方，Baudrin ら[26]は仕様どおりの Ascon-128 に対してナンス重複を利用することで 2^{40} という現実的な時間での暗号化中の内部状態回復が可能であることを示した．ただし Ascon の初期化の仕様上，状態回復が鍵回復には直結しないことに留意が必要である．更に現在の NIST 標準化文書ドラフトの Ascon-AEAD は Ascon-128a をベースとしているため Baudrin らの攻撃は適用できない．

4.3 Ascon-p 置換の暗号解析

Ascon-p 自体を単独の暗号プリミティブとみた場合の暗号解析も行われている．解析が目指すものはなんらかのランダムらしくない振る舞いを検出する手法（識別器，Distinguisher）であり，用いられる特徴量は差分・線形特性や Cube 特性などである．ブロック暗号に対する解析と類似しているが，鍵なし置換であるためそもそも “ランダムらしくない振る舞い” という問いが理論的には無意味である．一方，これらの特性を調べて得られた識別器はなんらかの暗号学的知見を与えるものには変わりなく，また場合によっては実際の（短縮段バージョン含めた）Ascon 解析に利用できることもあるため，学術的意義はある．CRYPTREC 報告書も参照のこと．以上の留意を踏まえたうえで Ascon-p の差分/線形特性確率の上界ないし下界の研究動向をみると，4 段（p^4）までは 2^{-128} 以上の差分/線形特性が発見されており，6 段では差分/線形特性確率が 2^{-128} 以下となることが示されている．これらの発見においては現在の暗号解析の潮流である，線形計画法ソルバや SAT ソルバといった

ツールを用いた方法が積極的に取り入れられている．

古典的な差分・線形特性を利用する識別器以外ではゼロサム識別器がよく研究されている．これは，置換 p に対して $\sum_{x\in S} x = 0$ かつ $\sum_{x\in S} p(x) = 0$ となるような入力部分集合 S を見出すことである．S のサイズが小さい場合にはこのような集合の発見は一般に困難であり，逆にある程度大きくなると（具体的には p の入力ビットサイズくらい）一般的な効率のよい発見方法がある．したがって小さい S でのゼロサム識別器の存在は p の暗号学的な強さに知見を与えるものといえる．しかしながらそのようなゼロサム識別器が将来の解析に有用となるかは一般に不明である．Ascon-p に対しては初期化と終端で用いる 12 段でのゼロサム識別器が設計者から報告されている[19]が，現状の Ascon の安全性に特段の影響は見出されていない．

5. Ascon の実装性能

Ascon の実装性能については様々なプラットホームでのベンチマーク結果が報告されている．

a） ソフトウェア

ソフトウェアにおいては前述のように Ascon-p の入力単位でのビットスライス実装を主眼としており，S-box の論理ゲートの少なさと線形層のソフトウェア指向の設計—64 ビットワード単位での幾つかのシフトと排他的論理和で実装可能—が助けとなり，効率的な実装を可能としている．また，NIST 自身もマイコンでのベンチマークを実施している．これらの結果が NIST の Web サイトにまとめられている[27]．NIST の当初の目的どおり，一般にマイコンプラットホームにおいては AES がコプロセッサなどの専用ハードウェアで実装されていない限りは，AES-GCM よりも高速な動作が報告されている．NIST の報告書[22]では GCM と比較した優位性を多様なマイコンでテストしており，Ascon は全てのケースでバランスよく優位性をもつことが分かる（例えば[22, Table 10]）．マイコンの実装性能は特にボードや環境に依存する要因が多いため，具体的な数字は個々の情報元をあたって頂きたい．例えば NIST 報告書[22, Fig. 30]では Cortex-M4 において，平文 64 バイトの最速暗号化実装は GCM のそれと比べて約 3 ～ 4 倍の速度を示している．Ascon のハッシュ関数の性能については，暗号化ほど詳細ではないが，NIST 報告書[22, Table 12]において，SHA-256 より小さい実装が可能である一方，速度においては劣る点が示唆されている（これはほかの多くのファイナリスト方式と同様）．

軽量暗号の主要なターゲットからは外れるが，64 ビット汎用 PC 向けプロセッサにおいては，設計者のホームページ[23]では 4～10 cycles/bytes の処理速度が報告されており，64 ビット単位での処理を生かした高速処理が可能である．ただし，これらのプロセッサにおいては多くの場合 AES が専用命令として搭載されており，AES-GCM や AES-OCB といった AES ベースの認証暗号が 1 cycle/bytes を切る性能をもつため，やはり組み込み環境など軽量暗号が生きるユースケースでの活用がメインとなるであろう．表 1 に設計者ホームページにある数値例を示す．

表 1　ソフトウェア実装数値の例[23]　単位は cycles/byte.

プラットホーム	Ascon-AEAD128	Ascon-Hash256
AMD EPYC 7742	4.2	12.4
AMD Ryzen 9 5950X	5.2	15.8
Apple M1 (ARMv8)	6.3	18.5
Cortex-A72 (ARMv8)	7.0	20.0
Intel Xeon E5-2609 v4	7.2	21.2
Intel Core i5-6300U	7.8	23.1
Intel Core i5-4200U	10.6	30.7
Cortex-A9 (ARMv7)	24.0	53.9
Cortex-A7 (NEON)	30.7	–
Cortex-A7 (ARMv7)	41.2	–
ARM1176JZF-S (ARMv6)	42.9	92.2

表 2　ハードウェア実装数値の例[23]

デザイン	実装サイズ（GE）	スループット (Mbps)
1 ラウンド	9680	7326
2 ラウンド	13249	11743
4 ラウンド	20380	16675

b） ハードウェア

ハードウェアに関しても，NIST LwC の開催期間中に様々な第三者評価が行われた．これらも NIST の Web ページにてまとめられている[27]．ハードウェアの場合は ASIC か FPGA か，API や用いるセルライブラリなどソフトウェア以上に環境依存の要因が多いが，おおまかにいって GCM との優位性は以下の 2 点にまとめられる．

- AES のラウンド実装はハードウェアでは比較的大きい（S-box も線形層も複雑）．Ascon の S-box は極めて小さく，線形層は単純．
- GCM では AES に加えて 128 ビットの有限体乗算回路を必要とする．Ascon は Ascon-p 以外の複雑な要素はない．

表 2 に CAESAR API を用いた Ascon-128a の VHDL 実装の例を載せる．詳細や他方式との比較は NIST のサイト[27]を参照のこと．

6. おわりに

Internet-of-things (IoT)，コネクテッドカー，ドローンなどの技術発展に伴い軽量認証暗号の需要は今後高まっていくものと考えられる．Ascon は最初の提案から仕様をあまり変えることなく高い安全性を保ち，かつ標準的な方式と比べた軽量性を有する優秀な方式であり，今後の活用が期待される．ただし実用に際しては本稿では触れていない，サイドチャネル対策や，プロトコルとしての安全性なども考える必要がある．Ascon の標準化が決まったことは軽量な認証暗号の研究開発における一つのマイルストーンといえるが，一方では認証暗号の新たな安全性指標（コミットメント安全性など）の提案やそれを達成する方式，メモリ保護などに適した低遅延暗号などのトピックが注目

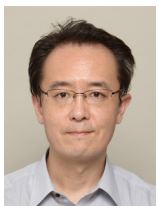
を集めている．更に，NIST は入出力長を保った可変長暗号化方式をアコーディオンモードと名付け，標準化を新たに進めようとしている[28]．これらの新しい研究動向に加え，CAESAR そして NIST LwC を通じて行われた Ascon の安全性評価・解析が新たな暗号解析手法や新たな暗号化方式の設計に活用されていくことを期待したい．

謝辞　本原稿の執筆にあたりご助言，ご協力を頂きました編集委員並びに事務局，出版社の方々に感謝いたします．

文　献

(1) J. Katz and M. Yung, "Unforgeable encryption and chosen ciphertext secure modes of operation," FSE 2000, Lecture Notes in Computer Science, vol.1978, pp.284–299, Springer, 2000.
(2) M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," ASIACRYPT 2000, Lecture Notes in Computer Science, vol.1976, pp.531–545, Springer, 2000.
(3) S. Vaudenay, "Security flaws induced by CBC padding — Applications to SSL, IPSEC, WTLS ...," EUROCRYPT 2002, Lecture Notes in Computer Science, vol.2332, pp.534–546, Springer, 2002.
(4) "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC," NIST Special Publication, 800-38D, National Institute of Standards and Technology, 2007.
(5) "Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality," NIST Special Publication, 800-38C, National Institute of Standards and Technology, 2007.
(6) C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2: Lightweight authenticated encryption and hashing," J. Cryptol., vol.34, no.3, p.33, 2021.
(7) "CAESAR: Competition for authenticated encryption: Security, applicability, and robustness," https://competitions.cr.yp.to/caesar.html
(8) "NIST lightweight cryptography," National Institute of Standards and Technology, https://csrc.nist.gov/projects/lightweight-cryptography, 2017.
(9) M.S. Turan, K.A. McKay, D. Chang, J. Kang, and J. Kelsey, "Ascon-based lightweight cryptography standards for constrained devices: Authenticated encryption, hash, and extendable output functions," NIST Special Publication, 800-232 ipd, 2024.
(10) G. Bertoni, J. Daemen, M. Peeters, and G.V. Assche, "On the indifferentiability of the sponge construction," EUROCRYPT 2008, Lecture Notes in Computer Science, vol.4965, pp.181–197, Springer, 2008.
(11) G. Bertoni, J. Daemen, M. Peeters, and G.V. Assche, "Duplexing the sponge: Single-pass authenticated encryption and other applications," Selected Areas in Cryptography 2011, Lecture Notes in Computer Science, vol.7118, pp.320–337, Springer, 2011.
(12) P. Jovanovic, A. Luykx, B. Mennink, Y. Sasaki, and K. Yasuda, "Beyond conventional security in sponge-based authenticated encryption modes," J. Cryptol., vol.32, no.3, pp.895–940, 2019.
(13) B. Mennink and C. Lefevre, "Generic security of the Ascon mode: On the power of key blinding," SAC, 2024.
(14) C. Lefevre and B. Mennink, "SoK: Security of the Ascon modes," IACR Trans. Symmetric Cryptol., vol.2025, no.1, pp.138–210, 2025.
(15) Y. Sasaki and K. Yasuda, "How to incorporate associated data in sponge-based authenticated encryption," CT-RSA, Lecture Notes in Computer Science, vol.9048, pp.353–370, Springer, 2015.
(16) J. Daemen, S. Hoffert M. Peeters, G.V. Assche, and R.V. Keer, "Xoodyak, a lightweight cryptographic scheme," IACR Trans. Symmetric Cryptol., vol.2020, no.S1, pp.60–87, 2020.
(17) O. Dunkelman, N. Keller, and A. Shamir, "Minimalism in cryptography: The even-Mansour scheme revisited," EUROCRYPT 2012, Lecture Notes in Computer Science, vol.7237, pp.336–354, Springer, 2012.
(18) T. Krovetz and P. Rogaway, "The software performance of authenticated-encryption modes," FSE 2011, Lecture Notes in Computer Science, vol.6733, pp.306–327, Springer, 2011.
(19) C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Cryptanalysis of Ascon," CT-RSA, Lecture Notes in Computer Science, vol.9048, pp.371–384, Springer, 2015.
(20) M. Liu, X. Lu, and D. Lin, "Differential-linear cryptanalysis from an algebraic perspective," CRYPTO 2021, Lecture Notes in Computer Science, vol.12827, pp.247–277, Springer, 2021.
(21) K. Hu, "Improved conditional cube attacks on Ascon AEADs in Nonce-respecting settings: with a break-fix strategy," IACR Trans. Symmetric Cryptol., vol.2024, no.2, pp.118–140, 2024.
(22) M.S. Turan, K. McKay, D. Chang, L. E Bassham, J. Kang, N.D. Waller, J. Kelsey, and D. Hong, "Status report on the final round of the nist lightweight cryptography standardization process," NIST IR 8454, National Institute of Standards and Technology, 2023.
(23) C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon — Lightweight cryptography," https://ascon.isec.tugraz.at/
(24) 藤堂，"軽量暗号の安全性に関する調査及び評価（Ascon, Grain-128AEAD, TinyJambu），" CRYPTREC 外部評価報告書, EX-3203-2022, https://www.cryptrec.go.jp/ex_reports.html, 2022.
(25) A. Joux, "Authentication failures in NIST version of GCM," https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/800-38-series-drafts/gcm/joux_comments.pdf
(26) J. Baudrin, A. Canteaut, and L. Perrin, "Practical cube attack against Nonce-misused Ascon," IACR Trans. Symmetric Cryptol., vol.2022, no.4, pp.120–144, 2022.
(27) National Institute of Standards and Technology, "Performance benchmarking," https://csrc.nist.gov/Projects/lightweight-cryptography/performance-benchmarking, 2023.
(28) A. Thompson and M.S. Turan, "NIST workshop on the requirements for an accordion cipher mode 2024: Workshop report," NIST IR 8537, National Institute of Standards and Technology, 2024.

（ISEC 研究会提案，2025 年 2 月 25 日受付，
2025 年 3 月 31 日再受付）



峯松一彦（正員）

1998 年 3 月早稲田大学理工学部機械工学専攻修了．1998 より NEC 中央研究所，2020 より NEC セキュアシステムプラットフォーム研究所主席研究員．2008 早稲田大学大学院理工学研究科博士後期課程数理科学専攻修了 (博士 (理学))．2010〜2012 早稲田大学大学院理工学研究科非常勤講師，2021 より横浜国立大学客員教授．共通鍵暗号の理論研究とその応用に従事．

解　説　論　文

情報伝送路に依存しない列車制御システム

Train Control System Independent of Communication Transmission Paths

岩本功貴 Koki IWAMOTO　　祇園昭宏 Akihiro GION
北野隆康 Takayasu KITANO

アブストラクト　多くの鉄道の制御に活用されている無線式列車制御システムは，保安制御機能と情報伝送機能を一体化して構築されている．従来型の列車制御システムの情報伝送路には，LCX（漏えい同軸ケーブル）や空間波が用いられるが，これらは鉄道事業者が敷設する自営回線であり，設備の構築及び運用・保守には多くのコストを要する．特に近年では，生産年齢人口の減少に伴い鉄道現場での労働力不足が進行していることから，情報伝送路についても省設備化と省メンテナンス化が求められている．本稿では，汎用装置や公衆通信回線を活用した列車制御システムにより，システムの機能分離や，自営回線の削減を実現するまでの過程を解説する．更に，鉄道の沿線設備に応じた情報伝送路の安定性を考慮できる列車制御システムについて解説する．

キーワード　鉄道通信，列車制御システム，公衆通信回線，移動体通信

Abstract　A radio train control system is constructed by integrating safety control and information transmission functions. In the communication channels of train control systems, LCX (leaky coaxial cable) and space waves are used, both of which are private networks installed by railway operators. However, the construction, operation, and maintenance of these networks require significant costs. In recent years, owing to the decline in the working-age population, labor shortages in the railway industry have become more pronounced, increasing the demand for equipment reduction and maintenance simplification in information transmission infrastructure as well. In this paper, we outline the process of achieving functional separation and the reduction in the number of private networks used in train control systems by utilizing general-purpose devices and public communication networks. Furthermore, we discuss a train control system that takes into account the stability of communication transmission paths according to railway trackside equipment.

Key words　Railway communication, Train control system, Public communication lines, Mobile communications

1. まえがき

近年，生産年齢人口の減少に伴う労働力不足への対応として，業務の省力化及び省人化が求められている．鉄道現場においても，ディジタル技術を活用することで，安全性の向上と低コスト化・省メンテナンス化を同時に推進することが重要である．

既存の列車制御システムでは，安全かつ安定した列車運行を実現するため，保安制御機能と情報伝送機能は一体として設計されてきた．特に，情報伝送路に無線を用いる無線式列車制御システム[(1)]では，通信の安定性を確保するため自営回線を構築しており，無線設備の構築費用やメンテナンス費用が課題となっている．そこで，上記課題に対し，設備の低コスト化や省メンテナンス化を目指した研究[(2),(3)]が進められている．ただし，これらの研究はいずれも，列車制御システムに公衆通信回線を適用するにあたり，セキュリティや特定の情報伝送路に関する考え方を整理したものである．

本稿では，自営設備の削減により低コスト化と省メンテナンス化を可能とする，鉄道の沿線設備に応じた情報伝送路の安定性を考慮できる列車制御システムについて解説する．更に，その実現に必要となる，保安制御と情報伝送に対する機能面及び装置面の分離，及び具体的な列車制御の手法と情報伝送路の回線設計について解説する．

2. 既存の無線式列車制御システム

列車制御システムは，列車の安全な運行を支えるためのシステムである．列車制御に必要な情報には，制御情報（列車を進行または停止させるための情報）があり，列車の在線位置（列車が走行している場所）に関する情報も含まれる．近年では，列車制御システムの通信に無線を用いる「無線式列車制御システム[(4)~(6)]」の導入が進んでおり，これは列車自身が現在位置を把握し，その位置情報を無線で地上に伝え，地上から列車に制御情報を無線で送り返す仕組みである．無線式列車制御システムは，国内で

岩本功貴　正員　（公財）鉄道総合技術研究所信号技術研究部
E-mail iwamoto.koki.45@rtri.or.jp
祇園昭宏　（公財）鉄道総合技術研究所信号技術研究部
E-mail gion.akihiro.61@rtri.or.jp
北野隆康　正員　（公財）鉄道総合技術研究所信号技術研究部
E-mail kitano.takayasu.27@rtri.or.jp
Koki IWAMOTO, Member, Akihiro GION, Nonmember, and Takayasu KITANO, Member (Railway Technical Research Institute, 2-8-38 Hikari-cho, Kokubunji-shi, Tokyo 185-8540 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.19 No.1 pp.15–21 2025 年 7 月

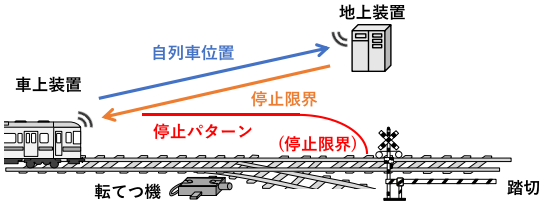


図 1　無線式列車制御システム

は JR 東日本の ATACS[1]（Advanced Train Administration and Communications System）や東京メトロの CBTC システム[5]のほか，海外では様々な CBTC（Communication Based Train Control）が導入されている．本章では，これらのシステムを総称して既存の無線式列車制御システムと呼び，概要と要件について記す．

2.1　無線式列車制御システムの概要

無線式列車制御システムとは，無線通信を活用して列車の運行を制御するシステムであり，地上の保安装置（地上装置）と車上の保安装置（車上装置）が，位置情報と制御情報を伝送することで制御が行われる（図 1）．具体的には，車上装置が列車の現在位置を把握し，その位置情報を無線で地上装置に送る．地上装置は，車上装置から送られてきた位置情報を受け取り，それぞれの列車を追跡する．また，踏切や転てつ機の状態を監視して制御を行う．地上装置は，これらの情報をもとに，各列車が安全に走行できる区間を決定し，停止限界（列車の走行を許可する区間の終端）を無線で車上装置に送る．車上装置は停止限界を受け取り，踏切や転てつ機などの沿線設備の位置などのデータやブレーキ性能に応じて，安全に走行できる停止パターンを計算する．万一，列車の速度が停止パターンを超えた場合，列車は自動で減速する．

2.2　車上装置への制御方法

無線式列車制御システムにおいて，地上装置が車上装置に対して行う制御は，列車の進行を指示する進行制御（図 2）と，列車の緊急停止などを指示する停止制御（図 3）の 2 種類がある．

- 進行制御

進行制御とは，地上装置から車上装置に向けて，列車の走行を許可する制御である．地上装置が踏切や転てつ機などの情報に基づき，停止限界を決定する．

- 停止制御

停止制御とは，脱線や衝突の回避などのために，既に与えられている停止限界にかかわらず，列車の停止を指示する制御である．地上装置が踏切支障などの情報に基づき，停止の要否を判断し，車上装置に指示する．

2.3　無線式列車制御システムの情報伝送路

無線式列車制御システムを含む鉄道の保安システムにおける

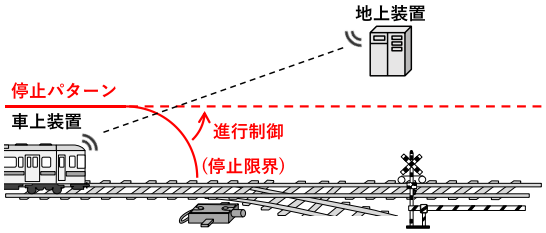


図 2　進行制御

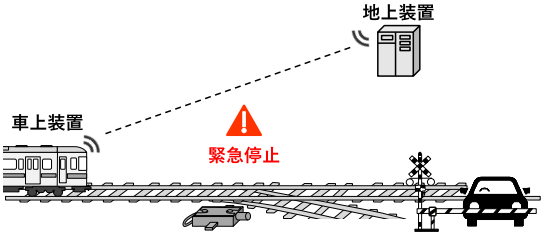


図 3　停止制御

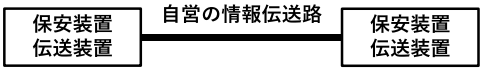


図 4　既存の無線式列車制御システムのブロック図

安全に関わる情報伝送の国際規格 IEC 62280[7]では，伝送上の脅威として「重複」「削除」「挿入」「順序誤り」「破壊」「遅延」「なりすまし」の七つの事象を定義している．

無線式列車制御システムでは通番や CRC(注1)などの検定符号によりこれらの脅威の有無を識別し，情報の誤認がないよう設計されているが，2.2 節に示した制御のうち，停止制御については情報の「遅延」による不達が衝突などの危険側事象に繋がり得る．そのため，既存の無線式列車制御システムでは，定周期伝送のなかで進行制御と停止制御を行い，定周期伝送の途絶を停止制御とみなして緊急停止するようシステムが設計されている．この方法は高い安全性を確保できるが，システムのアベイラビリティが情報伝送路に大きく依存する．そのため，既存の無線式列車制御システムは，自営の情報伝送路を構築するとともに，保安装置と伝送装置を一体化し，独自のプロトコルを用いて情報を伝送することで安定的な通信を実現している（図 4）．以上を踏まえ，使用する情報伝送路ごとに分類した既存の無線式列車制御システムの主な特徴について述べる．

(1)　LCX・誘導線を用いたシステム

LCX（漏えい同軸ケーブル）と呼ばれる無線信号が漏れ出る特殊なケーブルや，誘導無線のための交差誘導線を線路沿いに敷設し，列車と近距離通信を行い，地上装置–車上装置間の情報をやりとりする方法である．

無線式列車制御システムを初めて提案した「CARAT（Computer And Radio Aided Train control system）」[8]においては，情報伝送路に LCX を採用していた（図 5）．また，バンクーバー・スカイトレインなどの初期の CBTC システムでは交差誘導線が用いられている．これらの方法は，ケーブルの敷設に多くの費用を要するだけでなく，維持管理においても高いコスト

(注1)：巡回冗長検査（Cyclic Redundancy Check）．

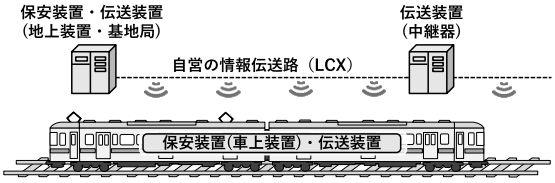


図 5　LCX を用いたシステム

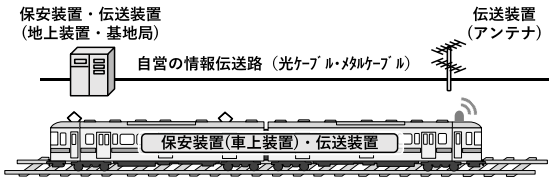


図 6　空間波を用いたシステム

がかかる点が課題である．

(2)　空間波を用いたシステム

アンテナを使った無線通信を利用する方法であり，光ファイバやメタルケーブルを用いた地上の情報伝送路により，アンテナを介して地上装置–車上装置間の情報をやりとりする仕組みである（図 6）．

この方法では，地上の情報伝送路に用いるケーブルの敷設は必要なものの，LCX と比較してコストを抑えやすく，維持管理の負担も軽減できることから，国内外の無線式列車制御システムで採用されている．

3.　情報伝送路に依存しない列車制御システム

2.3 節で示したとおり，既存の無線式列車制御システムでは，保安装置と伝送装置を一体化しているため，伝送装置が汎用化できず，高コスト化しやすいとともに，装置の変更が困難であり，最新の情報通信技術を利用できないという課題があった．本章では，これらの課題を解決するため，汎用装置や公衆通信回線などが適用できるよう情報伝送機能と保安制御機能を分離した，情報伝送路に依存しない列車制御システムについて概説する．

3.1　情報伝送路に依存しないシステムの要件と課題

無線式列車制御システムの情報伝送路を自営回線と専用装置に限定せず，汎用装置や公衆通信回線を適用するための要件を，制御の安全確保，セキュリティの確保，ライフサイクルの確保の観点から以下に定めた．

- 要件 (a) 進行制御と停止制御の安全を確保できること
- 要件 (b) セキュリティを確保できること
- 要件 (c) 装置やシステムの更新が容易であること

既存の無線式列車制御システムでは，上記要件に対して以下のように対応する．

- 一定時間の伝送途絶をもって停止制御を行うことで安全を確保するため，通信の安定性を担保可能な自営の情報伝送路を構築することで要件 (a) に対応する．

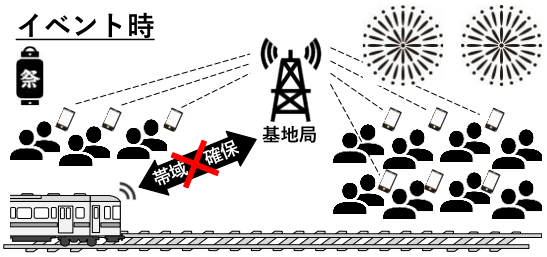


図 7　鉄道沿線で輻輳が起こり得る状況

- 独自のプロトコルと暗号化で要件 (b) に対応する．
- 保安装置と伝送装置を専用装置として長期供給を受けることにより要件 (c) に対応する．

一方，公衆通信回線や汎用装置の適用にあたっては，上記要件に対して以下の対応が必要となる．

- アンテナ基地局が設置されていない不感帯や，情報伝送路に起因する伝送途絶に対して要件 (a) を満たすこと．
- 汎用装置の内包するセキュリティ上の脆弱性や，公衆通信回線からのサイバー攻撃などに対して要件 (b) を満たすこと．
- 汎用装置や公衆通信回線のライフサイクルに対して要件 (c) を満たすこと．

以降，公衆通信回線や汎用装置の適用における課題について解説する．

(1)　要件 (a) に対する課題

通信事業者は，鉄道事業者をはじめとする移動体通信を行うユーザーに対し，ベストエフォート型の情報伝送路を提供している．通信事業者は人口カバー率を意識して基地局の整備を行うため，鉄道沿線では山間部や長大トンネル内などでサービスエリア外（不感帯）の場合がある．また，ベストエフォート型は通信品質を保証しないサービス形態であり，輻輳や通信障害などにより，通信の遅延や途絶が発生する可能性がある．そのため，公衆通信回線を利用する列車制御システムでは，情報伝送の遅延や途絶が発生することを前提とした設計が求められる．

ベストエフォート型の通信では以下に示す事象が発生し得る．

①　輻輳

輻輳は，イベントなどで公衆通信回線のユーザーが多数いる環境下で，基地局へのアクセスが集中する場合に発生しやすい（図 7）．通信が輻輳しているときは，帯域確保ができず，通信の安定性に大きな影響を及ぼす．

②　通信障害

通信障害は，通信事業者の設備故障などで発生する．例えば，コアネットワーク内の装置が故障した場合，通信不能に陥る，または，コアネットワーク内の経路変更などにより通信が不安定になることが想定される（図 8）．

(2)　要件 (b) に対する課題

公衆通信回線は，不特定多数の利用があり，伝送上の脅威として「なりすまし」や「改ざん」などのセキュリティ上のリスクがある．また，汎用装置のハードウェアや内部ソフトウェアの脆弱性を利用したサイバー攻撃の脅威がある．これらの脅威に対応したセキュリティの確保が求められる．

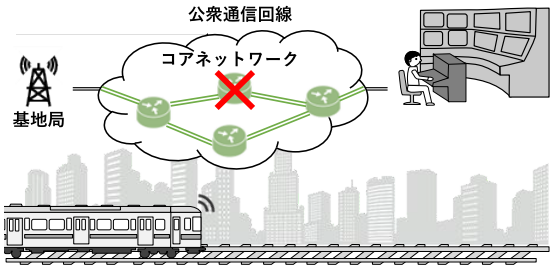


図 8　通信障害が起こり得る状況

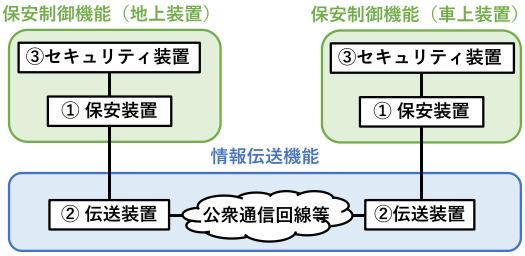


図 9　本システムのブロック図

(3)　要件 (c) に対する課題

汎用装置の製品ライフサイクルは 2〜3 年であり，10 年単位で供給される鉄道の一般的な保安装置と周期が異なる．また，公衆通信回線は情報通信技術の進展により無線伝送規格が 10 年程度で更新され，20 年前後でサービス終了となる．無線伝送規格のサービス開始時期と列車制御システムの運用開始時期が異なることから，システムの運用中における公衆通信回線の規格変更への想定が求められる．

3.2　情報伝送路に依存しない列車制御システムの概要

3.1 節に定めた要件を満たす列車制御システムである「情報伝送路に依存しない列車制御システム」（以下，本システムと略す）の解説を行う．まず本節では，本システムの概要を記す．

(1)　本システムの構成

本システムは，専用装置をシステムでの保安制御機能を担う保安装置のみに適用し，伝送やセキュリティのための装置に汎用装置を用いる（図 9）．既存の無線式列車制御システム（図 4）と本システムのブロック図を比較すると，保安制御機能と情報伝送機能を一体としていたこと，自営の情報伝送路で接続していたことに構成上の違いが見られる．

①　保安装置

保安装置とは，列車を制御するための装置であり，地上装置及び車上装置で構成する．また，地上装置は，走行している全ての列車を統括する中央装置及び，踏切や転てつ機をはじめとする現場装置で構成する．

②　伝送装置

伝送装置は，地上及び車上の無線装置及びアンテナで構成する．伝送装置には公衆通信回線用または Wi-Fi 用をはじめとする汎用装置を用いる．

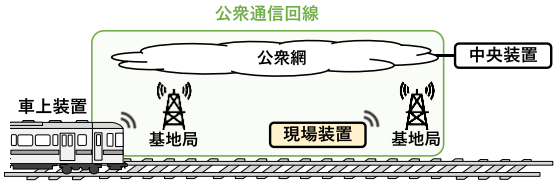


図 10　情報伝送路の設計（公衆通信回線利用）

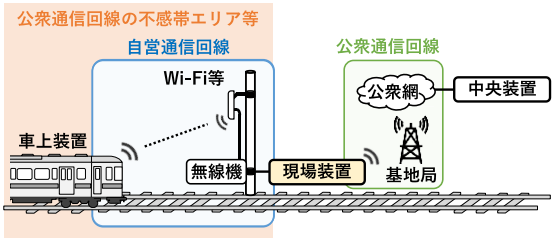


図 11　情報伝送路の設計 (自営通信回線併用)

③　セキュリティ装置

セキュリティ装置は，保安装置での暗号化処理のための演算モジュールである．セキュリティ装置はボードコンピュータなどの汎用装置を用いる．

(2)　制御と通信プロトコル

無線式列車制御システムでの制御のうち，伝送の途絶が安全に影響するのは停止制御のみである．そこで，既存の無線式列車制御システムの要件を見直し，進行制御と停止制御を分離し，進行制御を安全確認型制御[9]，停止制御を危険検出型制御として，それぞれに制御モデルを定めた．各制御モデルに対する通信プロトコルを以下に示す．

- 安全確認型制御

停止限界までの走行範囲が安全であることを確認してから列車の進行を許可する制御である．この制御では，地上装置と車上装置が通信し，列車が進める条件を満たしていることを確認してから，地上装置は車上装置に停止限界を伝送する．

- 危険検出型制御

列車の進行を妨げる危険を検知したときに，素早く列車を停止させる制御である．この制御では，地上装置が危険を検知すると，直ちにその情報を車上装置に伝え，列車を止める．危険検出型制御を実施する箇所については，現場装置から車上装置へ高頻度な定周期伝送を実施し，定周期伝送が連続して途絶した場合に列車を止めるなどの方法により，制御の安全性を担保する．

(3)　回線設計

本システムは公衆通信回線の利用（図 10）が基本となるが，駅や踏切の近傍の不感帯対策やアベイラビリティ向上のため，Wi-Fi などの自営通信回線をスポットで構築し，公衆通信回線と併用することもできる（図 11）．

そのため，システムを適用する線区の公衆通信回線の通信状況を測定し，不感帯となる区間，及び日ごとや時間ごとの通信品質の調査を行い，公衆通信回線を提供するサービスの選定や自営通信回線の設計を行う．

(4)　電文の検証

本システムでは，国際規格 IEC 62280 に示された脅威のう

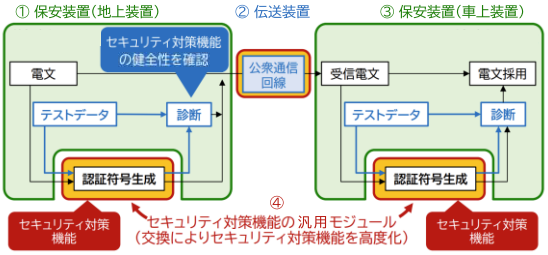


図 12　認証符号による電文検証

ち，公衆通信回線などのオープンな情報伝送路における「なりすまし」の脅威に対応することが求められる．なりすまし対策として，セキュリティ強度の高い暗号化技術を列車制御システムに適用するための手法と処理手順を示す．

地上装置–車上装置間で電文の送受信を行う際に，その情報の伝送と HMAC-SHA256 による認証符号（MAC：Message Authentication Code）の生成を行う（図 12）．

この仕組みでは，地上装置から車上装置に向けた情報伝送を行う場合，以下の順序で伝送の照合と健全性診断を行う．

①　保安装置（地上装置）

地上装置は，列車の運行制御に必要な制御電文を作成し，電文送信機能を通じて伝送装置に送る．また，制御電文の改ざんやなりすましを防止するため，認証符号を生成する．

②　伝送装置

地上装置から送信された電文は，公衆通信回線を介して車上装置に伝送される．

③　保安装置（車上装置）

車上装置は，地上から送られてきた電文を受信する．また，受信した電文に対し，認証符号を生成し，地上側で作成された認証符号と照合することで，改ざんやなりすましがないことを確認した上で電文を採用する．

④　認証符号の健全性確認

認証符号の生成は汎用装置（一般的な計算装置）で行われるが，その健全性を保証するために専用装置での検証を行う．検証は，テストデータを用いて汎用装置で認証符号を生成し，その演算結果を専用装置で照合を行い，適切な認証符号が生成されているかを確認する．

3.3　システム要件への対応

本節で，本システムが，3.1 節に示したシステム要件へ対応できることを記す．

(1)　要件 (a) への対応

制御の安全確保について，進行制御と停止制御に求められる通信の到達性と即時性の観点で整理する（表 1）．

安全確認型制御は，列車の次駅までの走行のため，運転に関係する踏切や転てつ機などの設備の状況，先行列車の位置により停止限界を更新する制御である．列車は，駅出発時，及び走行中に情報を取得及び更新することが求められる．そのため，停止限界を含む情報については，アベイラビリティの観点上，到達性が必要である．一方，停止限界の更新に影響しない走行区

表 1　情報伝送路の要件

情報伝送路の要件	到達性	即時性
危険検出型制御（踏切等）	✓	✓
安全確認型制御（駅構内等）	✓	–
その他（駅間等）	–	–

図 13　停止限界の更新に影響しない走行区間

間での通信途絶や遅延は許容できるため，即時性は不要である（図 13）．

したがって，指示する停止限界について，3.2 節で調査した不感帯を踏まえて設定することにより，情報伝送路を公衆通信回線のみで構築可能である．

危険検出型制御は，走行中の列車に対する停止指示であり，危険の発生した箇所の手前で確実に停止できるよう，制御指示が伝達されることが求められる．そのため，車上装置に指示する停止指示の情報が確実かつタイムラグなく届くことが必要である．すなわち，通信の到達性および即時性の両者が必要となる．ただし，踏切内の支障やホーム転落，落石などの停止制御の要因となる事象の発生箇所をあらかじめ特定し，危険検出型制御の区間として安全性を確保できる．また，アベイラビリティの観点でも，公衆通信回線を複数組み合わせる，または自営通信回線を組み合わせて冗長性をもたせることにより，地上装置–車上装置間の情報伝送路の安定性を向上することができる．

(2)　要件 (b) への対応

本システムでは，なりすまし対策として HMAC-SHA256 を認証符号に用いる．認証符号の生成はセキュリティモジュールが行い，保安装置が認証符号の照合を含む，電文の検定処理とテストデータの照合を通じたセキュリティモジュールの故障診断を行っている．

本システムは，既存の無線式列車制御システムの電文検定に，認証符号の照合によるなりすまし対策を追加した構成であること，セキュリティモジュールの故障を識別できること，認証符号に使用する HMAC-SHA256 は，電子政府推奨暗号の安全性を評価・監視している CRYPTREC の発行する暗号強度要件[10]において 2070 年以降の利用も可能なセキュリティ強度 256 bit の方式として示されていることから，十分なセキュリティを確保できる．

(3)　要件 (c) への対応

本システムでは，保安制御機能と情報伝送機能を分離し，ライフサイクルの長い保安制御機能については従来から用いられていたような専用装置を適用し，ライフサイクルの短い情報伝送機能や暗号化処理については汎用装置や公衆通信回線を適用するモジュール化設計としている（図 14）．

保安制御機能の観点では，伝送やセキュリティのための手順

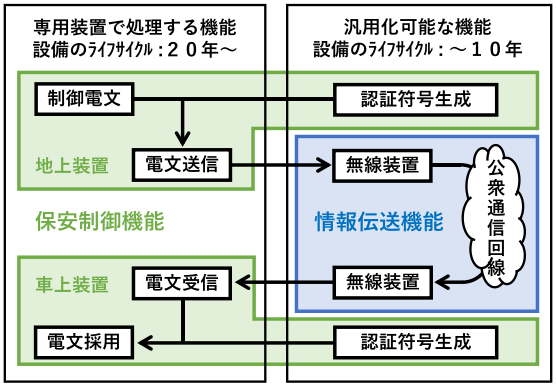


図 14　ライフサイクルの確保

表 2　公衆通信回線の活用で削減可能なコストの例

	LCXを用いたシステム	空間波を用いたシステム
設備費	LCX 無線機（基地局・中継器）	沿線ケーブル 無線通信設備（アンテナ等）
維持費	LCXの点検 （摩耗・断線・腐食の確認） 基地局・中継器の点検・修繕	ネットワークの運用 機器の点検・修繕 無線局免許の管理
管理費	LCXの支障移転工事	ケーブルの支障移転工事

が規定されており，その手順に沿って汎用装置による暗号化処理や情報伝送機能を利用する構成となる．したがって，異なる汎用装置の置き換えや，ネットワークの変更が可能であり，汎用装置の生産終了や公衆通信回線のサービス終了，技術の陳腐化については装置の交換やサービスの変更により適宜アップデートを行い，制御システムとしてのライフサイクルを確保できる．

3.4　コストメリット

既存の無線式列車制御システム（図 5，図 6）から，公衆通信回線を用いた本システムに置き換えた場合，設備費，維持費及び管理費の削減が期待できる（表 2）．システムごとに削減可能なコストの例を示す．

(1)　LCX を用いたシステム

削減可能な設備として，地上装置–車上装置間の通信を行うための LCX，LCX に重畳する信号を発信するための基地局及び中継器などがあり，それらの設備費及び維持費を削減できる．また，LCX が他設備の工事に支障する際に，それを移転する工事（支障移転工事）などの管理費を削減できる．

(2)　空間波を用いたシステム

削減可能な設備として，自営回線に用いる沿線ケーブル（メタルケーブル及び光ケーブル）及びアンテナなどの無線通信機器があり，ネットワークの運用，機器の点検・修繕，無線局免許の管理などの維持費を削減できる．また，LCX と同様，支障移転工事などの管理費を削減できる．

4.　ま　と　め

本稿では，情報伝送路に依存しない列車制御システムの実現に向け，自営設備の削減により低コスト化と省メンテナンス化を可能とする，鉄道の沿線設備に応じた情報伝送路の安定性を考慮できる列車制御システムについて解説した．更に，その実現に必要となる，保安制御と情報伝送に対する機能面及び装置面の分離，及び具体的な列車制御の手法と情報伝送路の回線設計について解説した．

現在，本システムの実現可能性を検証するため，プロトタイプシステムの開発及び鉄道事業者の営業線におけるフィールド試験に関する取り組みがなされている[11]．列車制御システムに公衆通信回線を活用することで，安全性の確保とコスト削減を両立することが，今後の鉄道システムの効率化につながるであろう．

文　　献

(1)　八木圭介，山口智敬，内山大輔，“デジタル無線を用いた列車制御システム（ATACS）の導入について，”計測制御，vol.55, no.5, pp.443–447, 2016.
(2)　北野隆康，祇園昭宏，“列車運行システムにおける公衆通信網の活用に関する研究開発，”信学技報，vol.122, no.252, RCS2022-167, pp.73–78, 2022.
(3)　中村一城，北野隆康，小川祥吾，竹内恵一，流王智子，川﨑邦弘，“鉄道運行業務への公衆 5G 活用に向けたローカル 5G を用いた基礎検討，”信学技報，vol.122, no.106, RCS2022-95, pp.128–133, 2022.
(4)　馬場裕一，宮林直樹，“無線式列車制御システムの技術動向と展望，”電学誌，vol.141, no.7, pp.407–410, 2021.
(5)　小川祥吾，“丸の内線への CBTC システム導入，”JREA, vol.59, no.8, pp.28–32, 2016.
(6)　神宮雅昭，山田麻香，“携帯電話回線を利用した列車制御システム（ATP 閉そくシステム）の開発，”JREA, vol.63, no.3, pp.43900–43903, 2020.
(7)　International Electrotechnical Commission, “Railway applications — Communication, signalling and processing systems — Safety related communication in transmission systems,” IEC 62280, 2014.
(8)　中村英夫，“CARAT に関連する研究成果を概観する，”鉄道総研報告，vol.7, no.5, pp.10–16, 1993.
(9)　関山瞬太郎，久保田淳司，西本翔，太田佑貴，北野隆康，藤田浩由，“安全確認型の無線式列車制御システムに関する一検討，”電学全大，5-159, 2024.
(10)　デジタル庁，総務省，経済産業省，“暗号強度要件（アルゴリズムおよび鍵長選択）に関する設定基準，”CRYPTREC, LS-0003-2022r1, 2022.
(11)　関山瞬太郎，久保田淳司，西本翔，祇園昭宏，藤田浩由，“安全確認型列車制御システムの開発とプロトタイプ試験，”電学全大，5-150, 2025.

（R 研究会提案，2025 年 3 月 27 日受付，
2025 年 4 月 8 日再受付）

岩本功貴（正員）
2016 年電気通信大学大学院博士課程（前期課程）修了．鉄道総合技術研究所で，列車制御システムに適用する通信に関する研究に従事．

祇園昭宏

2008 年神戸大学大学院博士課程（前期課程）修了．鉄道総合技術研究所で，保安制御システムへの汎用端末の活用とセキュリティに関する研究に従事．電気学会ほか会員．

北野隆康（正員）

2011 年同志社大学大学院博士課程（後期課程）修了．鉄道総合技術研究所で，主として無線伝送を用いた列車制御システムの開発や安全性解析に従事．博士（工学）．2010 年 IEEE AP-S Japan Chapter Young Engineer Award．IEEE 会員．

ESS ニュース

NOLTA, IEICE 特集号

Guest Secretary　佐々木智志

特集号タイトル：

Special Section on Recent Progress in Nonlinear Theory and Its Applications

掲載誌：

NOLTA IEICE, 2025 年 7 月発行

電子情報通信学会 NOLTA ソサイエティでは，フラッ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．2024 年はベトナム・ハロン湾にて開催され，カオスや分岐現象などの非線形解析，ニューラルネットワークをはじめとする機械学習，複雑ネットワーク，更にはそれらの応用研究など最先端の研究成果が発表されました．

本特集号は，非線形問題に関する最新の研究成果を国際英文論文誌として広く発信することを目的に企画されたものです．同シンポジウムで発表された成果に限らず，幅広い分野からご投稿頂いた論文は，NOLTA，IEICE の通常の査読プロセスに従って審査され，最終的に 31 件の論文が掲載されることとなりました．その中には，1 件の招待論文も含まれております．これらの掲載論文は，J-STAGE（https://www.jstage.jst.go.jp/browse/nolta/）にて無料でご覧頂けます．

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

佐々木智志（正員）

2009 武蔵工業大学（現東京都市大学）・工卒．2011 同大学院博士前期課程了．2016 日本学術振興会特別研究員．2017 同大学博士後期課程了．2017 湘南工科大学工学部情報工学科講師．2021 同大学准教授．2024 東京都市大学情報工学部情報科学科准教授．現在に至る．群知能を用いた最適化アルゴリズムの研究に従事．

研究会に行こう！

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

■信頼性研究会（R）

信頼性は製品やシステムに対して満足すべき品質特性であり，備わっていて当然である「当たり前品質」としても認識されています．特に，信頼性は「使ってみて分かる品質」でもあり，品質を構成する各要素の経時的変化を考慮する必要があることから，その解析や評価ではこれらを総合的に考慮する必要があります．近年では，製品やシステムに対するニーズや機能の多様化，関連する法令や規格に対応するために，「要求された機能が維持できる性質」としての狭義の信頼性のみならず，保全性や安全性など様々な性質を統合的に取り扱う必要も増しています．

信頼性研究会では，これらに関連する最新の研究成果を共有し，発展的な議論を展開することを目指し，年間８回の研究会をハイブリッド形式も活用しながら全国各地で開催しています．2025 年度の開催計画は以下のとおりです．

５月：愛知大学名古屋キャンパス（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（会場未定）
８月：小樽商工会議所【CPM，LQE，OPE，EMD との合同研究会】
９月：熊本市民会館
11 月：関西地区（会場未定）
12 月：機械振興会館（ハイブリッド形式）
３月：中国・四国地区（会場未定）

また，学生の皆様からの研究発表を奨励するとともに，「信頼性」をキーワードに第一線でご活躍されている研究者や実務者による招待講演を企画するなど，参加者の方々にとって有意義な研究会となる企画や運営に取り組んでおります．それらの活動の中で，各分野における「信頼性」に関する問題を解決する糸口が，参加者をはじめ学会員の皆様へ提供できればと願っております．

井上真二（正員）
2006 鳥取大・博士後期課程修了．同年，同大学院助教．2017 関西大・総合情報学部准教授，2021 同教授．現在に至る．博士（工学）．信頼性，保全性，機能安全に関する研究に従事．IEICE 信頼性研究会幹事（2019～），IEEE Reliability Society Japan Joint Chapter Vice Chair（2025～），IPSJ，ORSJ，JSQC，JIMA，REAJ，IEEE 各会員．

■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（CCS）研究専門委員会は，2011 年４月に時限研究専門委員会として発足し，2015 年４月から NOLTA ソサイエティのもと，常設研究専門委員会として活動しています．2025 年度は常設研究専門委員会として 11 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．2024 年度は，６月に福岡県，７月に北海道，11 月に宮城県，３月に北海道で研究会が開催されました．更に 2025 年３月の総合大会において，「ネットワーク科学の最前線～数理で読み解くネットワーク～」というテーマのシンポジウムセッションを企画し，６名の素晴らしい講演者の皆様による貴重な御講演を頂くことができました．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を開催する予定です．

また CCS 研究会では，学生の皆さんや若手研究者を積極的に奨励する取り組みにも力を入れています．毎年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．2025 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．

【2025 年度 CCS 研活動計画】

●第一種研究会

2025 年 6 月 12，6 月 13 日	CCS/NLP 共催研究会@岡山県 NPD 貸会議室 岡山高島屋
2025 年 7 月 31 日，8 月 1 日	CCS/IN 併催研究会@北海道 北海道大学
2025 年 11 月（中旬予定）	CCS 研究会@金沢県
2026 年 3 月（下旬予定）	CCS 研究会@北海道 ルスツリゾート

●大会・国際会議

2025 年 6 月 14 日	NOLTA ソサイエティ大会@岡山県 能楽堂ホール tenjin9
2025 年 7 月 21 日～7 月 24 日	国際ワークショップ CCMS @韓国 済州島
2025 年 10 月 27 日～10 月 31 日	国際学会 NOLTA2025 @日本 沖縄県

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

菅野円隆（正員）

2014 埼玉大学大学院理工学研究科理工学専攻博士課程修了．博士（工学）．2014～2018 福岡大学工学部電子情報工学科助教．2018～2023 埼玉大学大学院理工学研究科助教，2023～埼玉大学大学院理工学研究科准教授，現在に至る．第 45 回（2018 年秋季）応用物理学会講演奨励賞受賞．2022 年 5 月第 46 回レーザー学会奨励賞受賞．レーザダイナミクスの非線形時系列解析や光コンピューティング関する研究に従事．著書『光リザーバーコンピューティング：原理と実装』．応用物理学会会員．

■情報セキュリティ研究会（ISEC）

情報セキュリティは，安心安全なディジタル化社会に欠かせない技術であり，社会の安定に寄与する使命を担っています．多様化する脅威から社会を守るためには，様々なバックグラウンドをもつ研究者と技術者の知見を結集しなければなりません．情報セキュリティ研究会（ISEC）は，設立当初より，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までの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機会を提供すること，を目的としています．

ISEC 研究会では，第一種研究会を，5 月，7 月，11 月，3 月，に開催しています．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，世代を超えた研究者の交流を活発化させています．また 7 月の研究会は，通称セキュリティサマーサミットと呼ばれる，電子情報通信学会 6 研専（ISEC/SITE/ICSS/EMM/HWS/BioX）並びに情報処理学会のコンピュータセキュリティ研究会（CSEC）／セキュリティ心理学とトラスト研究会（SPT）との共催による大規模な研究集会となっており，セキュリティ業界における夏の風物詩となっています．第二種研究会である「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学術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，第一線級の研究者との交流の機会を創出しています．また，セキュリティ分野における国内最大級のシンポジウム「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，900 名を超える参加者を集めています．更に毎年，CSEC と共催で国際学術会議 IWSEC（International Workshop on Security）を日本で開催しており，今年は 11 月にアクロス福岡にて開催します．以上の研究集会の詳細については，ISEC 研究会の Web サイト（https://www.ieice.org/ess/isec/index.html）でご確認ください．

以上のように ISEC 研究会では，様々なイベントや多様な交流の場を作っておりますので，我が国の将来を担う研究者・技術者の積極的な参加を期待しております．

清本晋作（正員：フェロー）
2000 年に KDD（株）入社（現 KDDI（株））．以後，情報セキュリティの研究開発に従事し，現在，KDDI 総合研究所取締役執行役員副所長．先端技術大賞経済産業大臣賞，全国発明表彰発明賞，文部科学大臣表彰科学技術賞，前島密賞，電子情報通信学会業績賞，SCAT 表彰会長賞，の各賞を受賞．博士（工学）．

■情報理論研究会（IT）

情報理論（IT：Information Theory）研究会は，情報理論とその関連分野に関する研究テーマを取り扱う研究会です．シャノン理論や符号理論にとどまらず，通信方式，量子情報処理，情報理論的安全性に関する基礎理論，更には近年活発に研究が行われているデータサイエンス，機械学習など，基礎から応用に至るまで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，研究会を開催しています．特に今年度は，5 月と 8 月に，初めて研究発表を行う方を対象とした「フレッシュマンセッション」を設けることで，学生が発表デビューする機会をより多く提供できると期待しています．また，旬の研究テーマで顕著な成果を挙げられている方に招待講演を依頼しています．招待講演を通じて，聴講者の研究視野を広げるとともに，研究の楽しさや面白さを改めて実感して頂けるよう努めています．

2025 年度の IT 研究会の活動は以下のとおりです．

2025 年 5 月 29 日，30 日：長崎大学文教キャンパス．高機能マルチメディア（EMM）研究会と共催．フレッシュマンセッションを開催．
2025 年 8 月 5 日，6 日：東京工業高等専門学校．フレッシュマンセッションを開催．
2026 年 1 月：東北学院大学．無線通信システム（RCS）研究会，信号処理（SIP）研究会と共催．
2026 年 3 月：信州大学．ワイドバンドシステム（WBS）研究会，情報セキュリティ（ISEC）研究会，高信頼制御通信（RCC）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に対して，SITA サブソより「学生優秀発表賞」を授与しています．特に，今年度は 2 回にわたりフレッシュマンセッションを開催するため，優秀発表賞の受賞も目指して研究に取り組んで頂けると幸いです．

また，IT 研究会では垣根を超えたコミュニケーションをとても大事にしています．対面開催の機会も増え，発表内容についてのディスカッションや情報共有を活発に行うのはもちろんですが，懇親会での何気ない会話から研究のネットワークが広がり，研究のアイディアが見つかることも多々あります．私自身，研究会に参加することで毎回新しい知見を得ることができ，非常に充実していると感じています．

ぜひ，IT 研究会の雰囲気や楽しさを肌で感じて頂きたいと思います．皆様の積極的なご参加・ご発表を何卒よろしくお願いいたします．

眞田亜紀子（正員）
2002 年 3 月津田塾大学芸学部情報数理科学科卒．2004 年 3 月津田塾大学大学院理学研究科修士課程修了．2009 年 10 月 Queen's University, CANADA, Department of Mathematics and Statistics, Doctoral Program 修了（Ph.D.）．Claude Shannon Institute, University College Dublin, IRELAND（Post-Doc. Fellow），電通大（助教），湘南工科大（講師）を経て，2021 年 4 月より長岡技科大 准教授．グラフ理論を用いた情報理論，符号理論の基礎的研究に従事．2021 年 IEICE 通ソ優秀論文賞受賞．

■信号処理研究会（SIP）

今年度より，新たに「信号処理とその応用サブソサイエティ（SIP サブソ）」が設立され，本研究会はサブソを構成する唯一の研究会として積極的に活動を行っていきます．信号処理研究会及び SIP サブソでは，基礎理論から応用まで幅広い分野をカバーしております．研究専門委員会（SIP 研専）には五つのグループ（数理，学習，画像，音声・音響，通信）があり，関連する研究会と協力しながら継続的に活動を行っております．

今年度は以下の 4 回の研究会を開催予定です．このうち単独開催の 8 月研究会では，各研究グループから提案された様々な企画や招待講演を実施します．詳細な研究会の開催情報は信学会及び SIP 研専のホームページでご確認ください．

- 2025 年 6 月 5 日（木）～6 日（金）　金沢大学（角間キャンパス）（IE MI BioX ITE-ME ITE-IST 共催）
- 2025 年 8 月 28 日（木）～29 日（金）　島根県立産業交流会館くにびきメッセ（SIP 単独開催）
- 2026 年 1 月頃（開催日・場所未定）　IT RCS 共催
- 2026 年 2～3 月頃（開催日・場所未定）　SPEASIP（SP EA 共催，IPSJ-SLP 連催）

また毎年 11 月（年により 12 月）に主催しております信号処理シンポジウムは，国内の信号処理に関する最大規模のイベントで，活発な研究討論の場を提供しています．毎年，招待講演やチュートリアル講演に加え，100 件以上の研究発表が行われています．今年度は 40 回めの開催となり，11 月 25 日～27 日に茨城県水戸市で開催予定です．多くの皆様の研究発表・参加をお待ちしております．

西川清史（正員）
1992 東京都立大学大学院修士課程了．博士（工学）．1992 新日本製鐵(株)入社．1993 より東京都立大学．現在，同大学システムデザイン学部・教授．主に適応信号処理・深層学習の信号処理への応用などの研究に従事．信号処理研究専門委員会委員長，IEEE 会員，APSIPA 会員．

■ワイドバンドシステム研究会（WBS）

ワイドバンドシステム（WBS）研究会に参加してまず驚かされたのは，その名称にとらわれることなく，実に多種多様な研究テーマを取り扱っている点でした．広帯域信号を用いた通信システムはもちろんのこと，関連するあらゆるトピックを受け入れる懐の深さがあります．特に近年では，通信理論や数理的信号処理といった学術的側面に重点を置いた研究発表にとどまらず，可視光通信や水中通信といった産業応用を見据えた研究発表も活発に行われており，幅広い分野の最先端研究に触れることができます．更に，他研究会との共催も多く，周辺分野の関連研究に触れる貴重な機会にも恵まれています．

毎回，多くの大学教員や企業研究者が参加・聴講しており，活発な質疑応答が交わされています．学生にとっては，研究者・エンジニアとしての第一歩を踏み出す絶好の場となっておりますので，ぜひ一度ご参加頂ければ幸いです．

今後も，WBS 研究会が若手研究者同士の交流の場として，また，多くの研究者が自由に学び，議論できる場として機能し続け，活気ある研究コミュニティの一助となれるよう，微力ながら貢献してまいりたいと考えております．

高橋拓海（正員）
2016 大阪大学工学部卒，2017 同大大学院博士前期課程了，2019 同大大学院博士後期課程了，同年同大・工・助教，2024 同大・工・准教授．2018 University of Oulu, Finland 客員研究員．統計的信号処理，ディジタル移動体通信方式，位置推定技術などの研究に従事．

■高信頼制御通信研究会（RCC）

高信頼制御通信研究会（RCC）は「制御」と「通信」の両方を対象にしたユニークな研究会で，高信頼性やリアルタイム性が求められる様々な分野において，制御技術と通信技術を組み合わせたシステムに関する議論を行っています．最近の発表テーマは，ドローンの自律飛行，ロボットの遠隔制御，インフラの監視制御，イベント駆動型・データ駆動型制御，通信ネットワークの制御，AI による通信制御など多岐にわたっており，理論から応用まで幅広い研究を対象としています．また，学生や若手研究者に対する「高信頼制御通信研究奨励賞」の表彰も行っているので，積極的に発表頂きたいです．

本研究会の今後の開催予定やプログラムの詳細は以下のページを参照してください．

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

阿部侑真（正員）

2017 慶應義塾大学大学院修士課程，2020 同大学博士課程修了．2017 情報通信研究機構入所．現在，同機構ワイヤレスネットワーク研究センター宇宙通信システム研究室主任研究員．2023〜2024 ルクセンブルク大学客員研究員．宇宙通信ネットワークに関する研究に従事．2018 計測自動制御学会論文賞・武田賞受賞．博士（工学）．

岡山大学へようこそ

野上保之（岡山大学）

1．国立大学法人岡山大学

岡山大学は，その前身の一つが明治３年に創設の岡山藩医学館にも遡る長い歴史をもつ総合大学であり，教育・研究・社会貢献を柱に，岡山市を中心として学部・大学院を通じて幅広い分野の教育・研究を展開しています．長期ビジョンや教育理念に基づき，地域や国際社会と多様かつ積極的に連携しながら，自主的で柔軟な大学運営を進めています．更に岡山大学では，国連の持続可能な開発目標（SDGs）を重要な方針として位置づけ，「岡山大学 SDGs 推進本部」を中心に，教育・研究・社会連携を通じた SDGs の実現に向けた取り組みをグローバルに展開しています．

岡山大学津島キャンパス

鹿田キャンパス・Junko Fukutake Hall

2．津島・鹿田キャンパスの紹介

岡山大学は，津島・鹿田の二つのキャンパスがあり，学生・教職員の研究・学習活動を支える様々な施設を設置しています．工学部などが位置する津島キャンパスには，大学本部をはじめ，岡山大学図書館，創立五十周年記念館，共育共創コモンズ（OUX），共創イノベーションラボ（KIBINOVE）といった主要施設があり，そのほかにも Junko Fukutake Terrace，岡山大学津島宿泊所など利用できます．医学部が位置する鹿田キャンパスには，岡山大学病院や Junko Fukutake Hall があります．津島キャンパス・鹿田キャンパスともに交通アクセスがよく，両キャンパスともに JR 岡山駅からバスで 10～15 分程度，自転車でもアクセス可能な距離にあるため，市内中心部や住宅地からの通学・通勤にも便利です．学生・教職員にとって快適な学習・研究環境を整えており，キャンパスマップやバリアフリー情報を提供するなど，初めて訪れる方にも配慮された設計となっています．

Junko Fukutake Terrace

津島キャンパス・パーゴラ

3．理工学に関する学び

岡山大学は，理学部と工学部を中心に，理工学分野における先進的な教育・研究を展開しています．令和３年４月には，従来の工学部と環境理工学部が統合され，新たに建築教育プログラムを備えた新体制の工学部が発足しました．これにより，多様

な工学領域を包括する学びの場を整備しています．大学院では，環境生命自然科学研究科において，数理情報科学，機械システム都市創成科学，創成化学，地球環境生命科学などの学位プログラムを提供しており，ブループラネッツ，アグリバイオ，再生医療，サイバーセキュリティ（WAAP）など特色ある特別コースも整備しています．

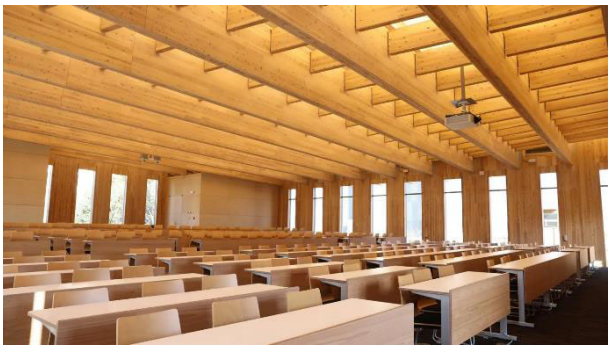
研究活動は極めて多様で，世界で初めてトポロジーの原理を利用したギガヘルツ超音波回路を実現する研究や，船底の付着生物に対する新たな付着阻害剤の合成に関する研究，入れ子状にした物質への光照射で生じる新しいエネルギー現象の観測といった物理・化学系の研究から，メダカの体色変化のメカニズム，甲虫の雄間闘争，カフェインの殺虫効果といった生物系の研究まで，低炭素・廃棄物循環研究センター，惑星物質研究所，資源植物科学研究所といった附属の研究施設とも連携しながら進めており，理工学分野全体での実践的かつ先進的な教育研究体制を構築しています．

こうした環境の中で，産官学が連携し，学生・教職員・産業界のエンジニアが分野や立ち位置を越えて共に育み，共に創り出す姿勢を大切にして，知の融合と実践的な協働を通じて，社会の未来を切り拓く原動力づくりを目指しています．

4．共育共創コモンズの紹介

津島キャンパスに位置する共育共創コモンズ（愛称：OUX）は，「みんなのイノベーション空間」として，大学のみならず地域や企業の皆様とともに学び交流できる施設です．令和３年の新工学部発足を記念して計画され，建築家・隈研吾氏の監修により，木造２階建てで建築されました．２階は，梁成 1.8 m の CLT 梁を用いた大スパン無柱空間を有する 300 人収容可能な大規模講義室，１階には産学共創スペースが整備され共同研究や地域・企業との交流拠点として活用されています．CLT パネル工法を視覚的に体感できる原寸大の建築教育教材として，また岡山県産の木材を活用した教育研究拠点としての機能も果たし，ウッドデザイン賞 2023（ライフスタイルデザイン部門・入賞）をはじめ複数の賞を受賞して高い評価を受けています．ぜひ本大会に参加の折にご覧頂けたらと思います．

共育共創コモンズ（OUX）外観



共育共創コモンズ２階大講堂

野上保之（正員：シニア会員）

平 11 年３月信州大学院工学系研究科博士課程修了（博士（工学）），平 22 年４月岡山大学自然科学研究科准教授，平 29 年４月同教授を経て，令５年４月より岡山大学学術研究院環境生命自然科学学域教授．この間，情報セキュリティ，通信工学，暗号技術，IoT セキュリティなどの研究に従事．現在，岡山大学 DX 推進・情報セキュリティ担当副理事，岡山大学グリーンイノベーションセンターグリーンバイデジタル部門部門長，電子情報通信学会・基礎境界ソサイエティ・情報理論研究専門委員会委員長．IEEE 会員．

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 6 年度フェロー称号

令和 6 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！

池田　誠

「高性能暗号半導体集積システム実装に関する先駆的研究」

Q. フェローになられた御感想をお聞かせください.

まずは，フェローの称号を頂けたこと大変光栄に思います．推薦を頂きました VLSI 設計技術研究専門委員会，特にその幹事団の皆様，推薦人になって頂いた，東京大学の飯塚先生にはそのご尽力に感謝いたします．研究活動の分野が基礎境界 VLD，HWS，エレクトロニクス ICD にまたがっているところではあるのですが，それぞれの研究専門委員会の活動，ソサイエティ間の雰囲気の違いを感じながら研究活動に取り組めていることを有難く感じているところです．その中でも，VLD における活動が最も長いということ，かつ，東京大学 VDEC における設計環境の整備にも携わってきたことを評価頂けてのことと考えており，その意味では，そういった基盤整備にも多少なりとも光が当たり評価を受けられたことも感謝に堪えません.

Q. 現在，御興味を持たれている研究テーマを教えてください.

ここ 10 年は，かなりのエフォートをハードウエアセキュリティ，特に暗号アルゴリズムのハードウエアアクセラレータ設計に注力しています.

アルゴリズムやそのアプリケーションサイドは HWS の皆様からの情報に頼り，VLD の皆様の様々なこれまでの設計の最適化に関する研究成果を活用し，ICD の集積回路化といったところに結実させています.

Q. 今後の抱負をお聞かせください.

半導体に対する投資が行われ社会的な関心が高まっている昨今，研究活動もさることながら，深刻な人材不足に対していかに即効性のある再教育，持続性のある魅力的な教育プログラムを作っていけるのかなど，分野を更に盛り上げていく活動にも取り組んでいければと考えています.

写真 1　富士山山頂でのご来光：2024 年 8 月

写真 2　たまには家族でアフタヌーンティー．オンライン会議に出ているとは口が裂けても言えません

写真３　国際会議で知り合いと一枚

写真４　学会といえば飲みニケーション

その意味でも，学会というのが一つ鍵になるプラットホームでありそちらをいかに更に活性化し魅力を上げていけるかといったことにも取り組んでいければと考えております．

Q．若い研究者の方へメッセージをどうぞ！

押しつけがましいことを言っても響かないのだとは思いますが，一心不乱に研究ができる時間を大切にして頂きたい．その一方で息抜きも重要だし，たまには学会活動も含めた，分野を盛り上げる活動にも携わって頂けると，更にはそれを通した異分野も含めた知り合いを増やしていくことが，将来的に研究活動の幅・厚みを増してくれることでしょう．

長谷川幹雄

「カオス・量子・光による先端的計算法の実応用に向けた先駆的研究」

Q．フェローになられた御感想をお聞かせください．

フェローの称号を頂いたことを大変光栄に思います．電子情報通信学会では学生時代から発表させて頂き，また，学会活動には就職後早い時期から参加させて頂きました．学会の実行委員，研究会の幹事，編集委員などを担当し，新しい研究会の立ち上げを経験し，その後，研究会の委員長も務めさせて頂きました．NOLTA ソサイエティの会長や，国際会議の実行委員長も経験しました．これらの学会活動を通じて，国内外の多くの研究者とのネットワークを築くことができました．議論をさせて頂く中で，多くのアイデアが生まれ，共同研究によって多くの成果を得ることができました．私の研究成果は，電子情報通信学会での活動を通じて出会った多くの共同研究者の皆様との研究のおかげです．大学に移動してから 18 年が経ちますが，その間の優秀な学生たちの成果もたくさんあります．このたびのフェローの称号を頂くことができたのは，皆様のおかげであり，心より感謝しております．

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，私は主に無線通信システムに関する研究を進めておりますが，光や量子に基づく先端的な AI の応用，IoT 向けの軽量 AI の応用，高密度 IoT プロトコル，ロボット遠隔操作のための通信高信頼化の研究などにも興味をもって取り組んでいます．これらの現在の研究も，共同研究やプロジェクトの研究がきっかけで進めているものが多いです．光による非常に高速なコンピューティングは最適化や強化学習に応用されており，そのような新しいアルゴリズムを，無線通信システムのリソース最適化などにも応用できることを示しています．また，軽量な AI を用いた IoT の最適化は，実際に Bluetooth や LPWA デバイスなどに実装し，実験を通じてその性能の改善を実証しながら研究を進めています．更に，Massive IoT の研究では，端末を 1500 台も試作し，混雑状況での性能改善に向けた研究を進めています．

Q．今後の抱負をお聞かせください．

これまで，共同研究者の皆様とともに様々なアイデアを出して研究を進めてきましたが，今後もこれらの共同研究を発展させ，ネットワークももっと広げていきたいと考えています．更に，自らアイデアを出し，プロジェクトをリードする立場にもなっていかなければならないと考えております．自分だけではできないかもしれませんが，研究グループを作り，皆で研究を発展させてい

きたいと思っています．日本の研究力に対しての危機感をもっております．国際的に活躍できる人材が，我々の分野にももっと必要だと考えており，海外の大学との連携や，学生の留学支援にも力を入れていきたいと考えております．自分の力では足りないかもしれませんが，ほかの研究者の皆様と協力し，日本をもっと強くすることにも少しでも貢献し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！

私は学生時代は，カオスニューラルネットワークの研究をしていました．就職後，突然分野が変わり，無線通信の研究を始めることになりました．初めは困惑しましたが，なんとか頑張って，徐々に成果を上げられるようになりました．やりたいこと，やれ

写真１　2025 年 3 月　国際会議 NCSP@ タイで発表した学生たちと

写真２　2024 年 12 月　国際会議 NOLTA2024@Halong Bay のバンケットでの挨拶

写真３　2024 年 11 月　OB も参加した研究室の発表会

写真４　2024 年 5 月　KICS と NOLTA Society との MoU 調印式

写真５　2024 年 2 月　マレーシアの教育大臣の見学対応

ることを，そのまま続けるのではなく，新しい分野の研究にしっかり取り組んだことが，今につながっていると思っています．未知の分野に正面から挑戦することで，新しい専門が自分に追加されていきます．それによって，分野横断的なアイデアも生まれます．若い皆様にも，未知の分野にも，積極的に挑戦して頂きたいです．異分野の発表でも，どこかに自分の研究とのつながりがないか，アイデアが生まれないか，意識しながら聞いて欲しいです．役立つことが，異分野にもたくさんあるはずです．幅広い分野に友達を作りネットワークを広げることで，より広い視野からアイデアを出すことができるようになります．そして，国際的に活躍できる技術者，研究者となって頂きたいです．

宝珠山　治

「実環境用信号強調技術の研究開発」

Q. フェローになられた御感想をお聞かせください.

大変名誉な称号を頂き，とても光栄に感じております．携帯電話が広まる中で，実環境で避けられない音響環境の問題に対処するための信号処理技術を評価して頂きました．皆様のご支援，ご協力のおかげで残る技術を作ることができたようです．幸運な技術者人生を過ごさせてくださった皆様に感謝いたします．

Q. 現在，御興味を持たれている研究テーマを教えてください．今後の抱負をお聞かせください.

ウェアラブルデバイスやロボットなどによる人間拡張技術です．センサやアクチュエータ，それを扱う制御技術（AI など）を組み合わせて，うれしいことができないかを若い方々と研究開発しています．

京セラの人間拡張：https://www.kyocera.co.jp/humanaug/

Q. 若い研究者の方へメッセージをどうぞ！

私の幸運を分析してみると「ボトルネック（実用化での重要な課題）を解決できたこと」が，「ほかの人に論文，特許などで認知されたこと」にあると思います．ボトルネックが何かを考えて取り組むことと，それを論文など参照できる形で残すことを意識すると，技術者として楽しい人生が歩めるのではないかと思います．

写真 1　1996 年実験室にて

写真 2　自作アナログシンセサイザの前で

堀内　俊治

「モバイル機器における音空間表現技術の研究開発」

Q. フェローになられた御感想をお聞かせください.

過分な評価に恐縮するとともに，大変光栄に存じます．多くの方々に支えられ，研究活動を続けてまいりました．この受賞は，今後も研究開発に一層邁進していく励みとなりました．支えてくださった皆様に，改めて深く感謝申し上げます．

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.

引き続き，音空間分析・制御・表現技術の研究開発に興味をもっております．特に，ユーザの環境や好みに応じてパーソナライズされた音響体験の実現や，リアルタイムでの音空間制御技術の付加価値向上に関わる研究に取り組んでいます．

Q. 今後の抱負をお聞かせください.

技術の実用化を通じて，日常生活やエンタテインメントの質を向上させたいと考えております．また，五感通信に関わる次世代の要素技術を見極め，積極的に取り入れるとともに，後進の育成並びに学会の発展に貢献できるよう，一歩一歩着実に進めてまいります．

Q. 若い研究者の方へメッセージをどうぞ！

自身を振り返ると，若い頃もっと勉強しておけばよかったと感じることが多々あります．知識が不足していたために，大きなチャンスを逃してしまったこともあります．また，研究は生もののようなものであり，鮮度や旬の時期も非常に重要です．ですので，様々な領域に広く興味をもち，知識を蓄え，最大の成果を得られるタイミングを見極めて，研究に邁進してください．きっと良いことにつながります．ともに頑張っていきましょう．

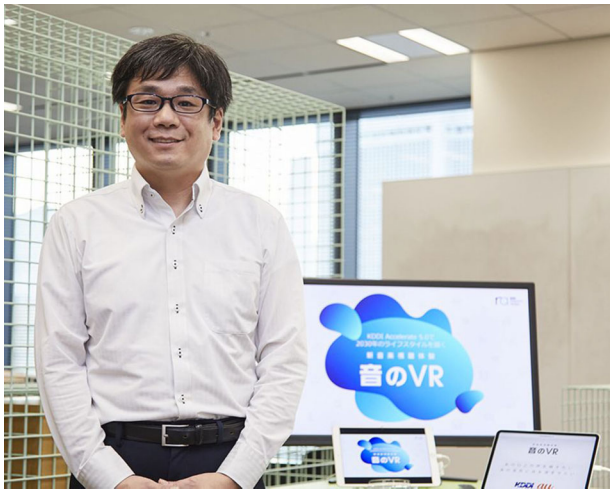


写真 1　社内展示スペースにて（2021 年）

写真 2　日頃の運動不足解消に（2023 年）

令和６年度　学術奨励賞

令和６年度は基礎・境界ソサイエティ及び NOLTA ソサイエティでは８名が学術奨励賞を受賞されました.

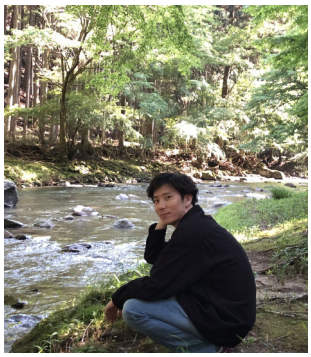
伊与田　友貴（名古屋大学）

“イメージセンサ可視光通信における CNN 型復調方式の実画像パラメータを考慮した性能向上”[1]

このたびは，学術奨励賞という栄えある賞を賜り，誠に光栄に存じます．日頃より丁寧にご指導くださっている小林健太郎先生，岡田啓先生，路姍先生，山里敬也先生に心より御礼申し上げます．また，研究活動を支えてくださっている関係各位の皆様にも深く感謝いたします．

受賞論文では，デジタルサイネージとイメージセンサを用いた可視光通信において，実画像に含まれる各種パラメータを考慮することで，CNN ベースの復調手法の性能向上を図りました．本賞を励みとして，引き続き本分野の発展に貢献できるよう，研鑽を積んでまいります．今後ともご指導・ご鞭撻のほど，何卒よろしくお願い申し上げます．

加藤　海渡（中京大学）



“離散力学系より得られる時系列データおよびパラメータを学習した Extreme learning machine に基づく分岐解析手法”[2]

このたびは学術奨励賞という名誉ある賞を賜り，誠に光栄に存じます．ご指導頂いた高坂拓司教授，共同研究者の伊藤佳卓准教授に深く感謝申し上げます．また，発表の機会とともに貴重なご助言を賜りました審査員の先生方，学会関係者の皆様にも心より御礼申し上げます．受賞対象となった研究では，離散力学系の時系列データとパラメータを同時に学習した Extreme Learning Machine に基づく分岐解析手法を提案しました．本成果を糧に，今後も実環境データへの応用を目指し，研究活動に一層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.

五井野　珠琉（東京電機大学）

“2 マイクロホン任意指向性形成回路の設計方針”[3]

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．研究を進めるにあたり，日頃からご指導ご鞭撻を頂いた陶山健仁教授をはじめ，研究室の皆様，学会などでご助言をくださった先生方にこの場をお借りして感謝申し上げます．本研究は，２マイクロホンのみで特定方向の音源信号のみ抽出できるような指向性を形成する回路を設計いたしました．この受賞を励みに，社会に貢献することができるよう，より一層研究に邁進する所存です．このたびは誠にありがとうございました.

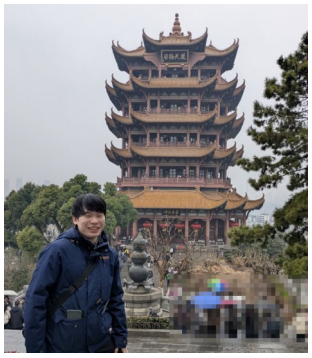
杉山　悠一朗（名城大学）

“Wi-Fi RTT を用いたドローン屋内測位における疑似データを用いた機械学習モデルの検討”[4]

このたびは学術奨励賞という名誉ある賞を賜り，誠に光栄に存じます．本研究を進めるにあたり，ご指導くださいました小林健太郎准教授，中條渉特任教授をはじめ，高信頼制御通信研究会でご助言を頂いた皆様に心より御礼申し上げます．また，実験に快くご協力頂いたシステ

ム情報通信研究室の諸氏にも，この場をお借りして感謝申し上げます．受賞研究では，Wi-Fi RTT と疑似生成データを用いて学習させた機械学習モデルにより，屋内飛行ドローンの位置座標推定手法を提案いたしました．今回の受賞を励みに今後は社会人として，社会の発展に寄与していく所存です．このたびは誠にありがとうございました．

砂井　啓希（北海道大学）



“分散強化学習における事象駆動型通信の導入”[5]

このたびは，栄誉ある学術奨励賞を賜り，大変うれしく思います．今回の受賞は，指導教員である北海道大学の小林孝一教授や山下裕特任教授をはじめとして，システム制御理論研究室の皆様や，学会関係者の皆様のお力添えによるものだと考えています．この場をお借りして厚く御礼申し上げます．受賞研究では，事象駆動制御を拡張した通信手法によって，分散強化学習システムの通信コスト削減を実現しています．現在は研究活動を行っていませんが，この賞を励みに社会人としてより一層努力していきたいと思っています．このたびは誠にありがとうございました．

代　美月（東京都市大学）

“PCA および MFTMA を用いた CNN におけるクラス分布次元の解析”[6]

このたびは，学術奨励賞という栄誉ある賞を賜り，誠に光栄に存じます．日頃より熱心にご指導くださる神野健哉教授をはじめ，審査及びご支援を賜りました電子情報通信学会の皆様，学会にて活発なご意見をくださる諸先生方，そして日々議論を重ねている研究室のメンバーに，心より感謝申し上げます．受賞対象の研究では，画像分類 CNN における各クラスの分布を多様体と仮定し，入力からラベル出力に至る過程における次元の減少について検証しました．本年度より博士後期課程に進学し，より一層研究に励む所存です．本受賞を励みに，今後も真摯に研究に取り組んでまいりますので，引き続きご指導ご鞭撻のほどよろしくお願い申し上げます．

三木　悠矢（名城大学）

“物体検出 DNN を用いたイメージセンサ可視光通信方式の実画像パラメータを考慮した性能評価”[7]

このたびは，学術奨励賞という名誉ある賞を賜り，大変光栄に存じます．本研究を進めるにあたり，日々熱心なご指導を頂きました小林健太郎先生をはじめ，研究室の皆様，ワイドバンドシステム研究会で議論や励ましのお言葉をくださいました諸先生方に，この場をお借りして心から御礼申し上げます．受賞論文では，物体検出 DNN を用いたデジタルサイネージ・イメージセンサ可視光通信方式において，実画像パラメータを考慮した性能について評価しました．今回の受賞を励みに，社会人としてもより一層努力を重ねていく所存です．このたびは，誠にありがとうございました．

吉田　しおん
（東京理科大学）

“リザバー層の力学系に対する再帰定量化解析”(8)

このたびは，学術奨励賞という名誉ある賞を頂き，大変光栄に存じます．本研究を遂行するにあたり，ご指導くださった池口徹教授，澤田和弥助教をはじめ，研究室のメンバー，たくさんのアドバイスをくださった先生方に，この場をお借りして深く感謝を申し上げます．受賞論文では，リザバーコンピューティングの内部状態値に対して時系列解析手法を適用し，予測対象時系列との関係性を調査しました．今回の受賞を励みに，社会に貢献できるよう今後も邁進する所存でございます．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） 伊与田友貴，“イメージセンサ可視光通信における CNN 型復調方式の実画像パラメータを考慮した性能向上，”2024 信学総大，A-9-07, March 2024.
（2） 加藤海渡，“離散力学系より得られる時系列データおよびパラメータを学習した Extreme learning machine に基づく分岐解析手法，”2024 信学総大，N-1-09, March 2024.
（3） 五井野珠琉，“2 マイクロホン任意指向性形成回路の設計方針，”2024 信学ソ大，A-1-03, Sept. 2024.
（4） 杉山悠一朗，“Wi-Fi RTT を用いたドローン屋内測位における疑似データを用いた機械学習モデルの検討，”2024 信学ソ大，A-16-03, Sept. 2024.
（5） 砂井啓希，“分散強化学習における事象駆動型通信の導入，”2024 信学総大，A-16-03, March 2024.
（6） 代　美月，“PCA および MFTMA を用いた CNN におけるクラス分布次元の解析，”2024 信学ソ大，N-1-28, Sept. 2024.
（7） 三木悠矢，“物体検出 DNN を用いたイメージセンサ可視光通信方式の実画像パラメータを考慮した性能評価，”2024 信学ソ大，A-9-11, Sept. 2024.
（8） 吉田しおん，“リザバー層の力学系に対する再帰定量化解析，”2024 信学ソ大，N-1-29, Sept. 2024.

開催案内

Call for Participants

Original papers on the research and development of various security topics, as well as case studies and implementation experiences, are solicited for submission to IWSEC 2025. Topics of interest for IWSEC 2025 include all theory and practice of cryptography, information security, and network security, as in the previous IWSEC workshops. We classify the topics of interest into two tracks as follows, but not limited to:

- Applied cryptography
- 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
- Real-world cryptographic systems
- Software security
- Supply chain security
- Symmetric-key cryptography

Keynote Talks

We will have keynote talks from the following world-leading researchers.

- **Dr. Ward Beullens** (IBM Research Europe)
- **Prof. Nicolas Christin** (Professor at Carnegie Mellon University)
- **Prof. Boris Otto** (Professor at the Technical University of Dortmund and Director of the Fraunhofer Institute for Software and Systems Engineering ISST)

Committees

General Co-Chairs:

Shinsaku Kiyomoto (KDDI Research Inc., Japan)
Tatsuya Mori (Waseda University, Japan)

Program Co-Chairs:

Carlos Cid (Okinawa Institute of Science and Technology, Japan, and Simula UiB, Norway)
Naoto Yanai (Panasonic, Japan)

2025 International Workshop on Smart Info-Media Systems in Asia (SISA2025)

12 – 14 November, 2025

Prince of Songkla University, Phuket Campus, Thailand

Call for Papers

Organizing Committee

Honorary Chairs

Kosin Chamnongthai
King Mongkut's University of Technology Thonburi (KMUTT), Thailand

General Co-Chairs

Aziz Nanthaamornphong
Prince of Songkla University, Thailand
Arata Kawamura
Kyoto Sangyo Univ., Japan

Technical Program Co-Chairs

Noboru Hayasaka
Osaka Electro-Communication University, Japan
Warodom Werapun
Prince of Songkla University, Thailand

Special Session Chair

Kosin Chamnongthai
King Mongkut's University of Technology Thonburi (KMUTT), Thailand

Publication Chair

Takuya Futagami
Aichi Gakuin University, Japan

Finance & Registration Chairs

Yasutomo Kinugasa
National Inst. Tech. Matsue College, Japan
Panisa Treepong
Prince of Songkla University, Thailand

Information System Chair

Johei Matsuoka
Tokyo University of Technology, Japan

Local Arrangement Chairs

Nattapong Tongtep
Prince of Songkla University, Thailand
Tomoaki Sato
Hokusei Gakuen University, Japan

Advisory Board Liaison

Naoto Sasaoka
Tottori University, Japan

International Steering Committee

Chair:

Naoto Sasaoka, *Japan*

Members:

Hakaru Tamukoh, *Japan*
Shingo Yoshizawa, *Japan*
Yosuke Sugiura, *Japan*
Yuichiro Tanaka, *Japan*
Yoshiaki Ueda, *Japan*

The Joint Conference of the 2025 International Workshop on Smart Info-Media System in Asia (SISA2025) and the 9th International Conference on Information Technology (InCIT2025) will be held at Prince of Songkla University, Phuket Campus, Thailand. The SISA2025 presents every possibility on new information technologies and its smart systems.

The SISA2025 is aiming at promoting young researchers in the fields of multimedia system and wireless communications. We plan to organize short oral presentations with poster discussion for regular sessions as well as a keynote talk and special sessions. Prospective authors are invited to submit their papers reporting original works in these fields.

The topics in SISA2025 include the following but not limited to:

1. Communication Systems
- 1.1 Smart Wireless Systems, Smart Mobile Systems
- 1.2 Cognitive Systems, Intelligent Soft-Wireless Systems
- 1.3 Multi-Media over Wireless
- 1.4 Signal Processing for Communication Systems
- 1.5 Intelligent Communication Systems
- 1.6 MIMO Systems
- 1.7 NFC, RFID, Sensor Network Systems, Mesh Network
- 1.8 WAN/MAN/LAN/PAN/BAN
- 1.9 Emerging Technologies for Communications

2. Multimedia and Systems
- 2.1 Speech Processing and Coding
- 2.2 Image Processing and Coding
- 2.3 Video Processing and Coding
- 2.4 Video and Multimedia Technology & Communications
- 2.5 Audio/Acoustic Signal Processing
- 2.6 Signal Processing for Medical Technologies
- 2.7 Intelligent Signal Processing for Multimedia & Systems
- 2.8 Security Signal Processing for Multimedia & Systems
- 2.9 Parallel Implementation for Multimedia & Systems
- 2.10 Emerging Technologies for Multimedia & Systems

3. Information Science and Technologies
- 3.1 Intelligent Transport Systems
- 3.2 Bioinformatics, Neural Networks and Fuzzy Systems
- 3.3 Informatics for Green Earth & Environmental Technologies

Authors are invited to submit a full paper in accordance with posted guidelines. For more information, please refer to our website:

http://www.ieice-sisa.org/

Author's Schedule:

Deadline for Submission of Regular Paper:	July 11, 2025
Notification of Acceptance:	September 1, 2025
Deadline for Submission of Camera Ready Paper:	October 1, 2025

SISA2025 Student Paper Awards

Paper presented in regular sessions can be nominated for the Student Paper Awards, provided that the first author is a full time undergraduate, Masters or Ph.D. student.

Special Section on IEICE Trans. Fundamentals

We plan to publish a Special Section on *IEICE Trans. Fundamentals* on June 2027. Authors who presented their original works in SISA2025 are solicited to submit papers to this special section.

Submission Instruction

Paper must be written in English and should describe the authors' original research work. The length of the paper is limited to 6 pages including figures, tables and references. The paper must be in A4 size, two-column format. Please download paper template from SISA2025 website.

論文募集

第４８回情報理論とその応用シンポジウム(SITA2025)開催案内

ご挨拶

第48回情報理論とその応用シンポジウム(SITA2025)を福島県郡山市にて開催いたします。本シンポジウムは、例年、宿泊と発表会場を一体とした泊まり込みのスタイルをとっております。2025年もこのスタイルにならい、情報理論とその応用分野に関する発表を広くつのるとともに、多数の方々のご参加をお待ちしております。

実行委員長　小林　学

開催期間・会場

2025年11月25日(火)～28日(金)
福島県郡山市 磐梯熱海温泉 ホテル華の湯(http://www.hotelhananoyu.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/SITA2025/index.html

実行委員会

実行委員長:
　小林　学　（早稲田大学）
プログラム委員長:
　八木　秀樹（電気通信大学）
総務:齋藤　翔太（群馬大学）
会計:新家　稔央（東京都市大学）
　鎌塚　明　（湘南工科大学）
出版:柴田　凌　（信州大学）
会場:中澤　真　（会津大学）
　中原　悠太（早稲田大学）
登録:吉田　隆弘（日本大学）
　石田　崇（高崎経済大学）
広報:細谷　剛　（大阪産業大学）
　堀井　俊佑（早稲田大学）
プログラム委員会幹事:
　竹内　啓悟（豊橋技術科学大学）
アドバイザー:
　村松　純　（早稲田大学）

今後のスケジュール

Web Site開設: 2025年6月
発表申込開始: 2025年8月上旬

事務局

〒371-8510　群馬県 前橋市 荒牧町 4-2
群馬大学 情報学部 情報学科 齋藤研内
SITA2025事務局　齋藤翔太
sita-2025-sec@mail.ieice.org

基礎・境界ソサイエティ運営委員会

会長	尾上　孝雄	(大阪大学)
次期会長	岩本　　貢	(電気通信大学)
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）	澁谷　智治	(上智大学)
副会長（システムデザイン技術）	前田　義信	(新潟大学)
副会長（音響・超音波）	青柳　　学	(室蘭工業大学)
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）	市毛　弘一	(横浜国立大学)
庶務幹事	傘　　昊	(東京都市大学)
庶務幹事	藤澤　匡哉	(東京理科大学)
会計幹事	筒井　　弘	(北海道大学)
会計幹事	吉田　隆弘	(日本大学)
事業担当幹事	黒崎　正行	(九州工業大学)
事業担当幹事	西新　幹彦	(信州大学)
大会担当幹事	伊藤　大輔	(岐阜大学)
大会担当幹事	花谷　嘉一	(株式会社東芝)
電子広報担当幹事	古賀　崇了	(近畿大学)
電子広報担当幹事	中井　雄士	(豊橋技術科学大学)
論文誌編集委員長	岡田　　実	(奈良先端科学技術大学院大学)
論文誌編集幹事	林　　和則	(京都大学)
論文誌副編集委員長	國廣　　昇	(筑波大学)
論文誌副編集幹事	鈴木幸太郎	(豊橋技術科学大学)
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	松井健太郎	(日本放送協会)
ソサイエティ誌担当幹事	宮北　和之	(新潟大学)
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）	藤沢　匡哉	(東京理科大学)
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）	小西たつ美	(愛知工業大学)
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）	澁谷　智治	(上智大学)
副会長（システムデザイン技術）	前田　義信	(新潟大学)
副会長（音響・超音波）	青柳　　学	(室蘭工業大学)
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）	市毛　弘一	(横浜国立大学)
事業担当幹事	黒崎　正行	(九州工業大学)
事業担当幹事	西新　幹彦	(信州大学)
回路とシステム（CAS）	下田　真二	(ソニーセミコンダクタソリューションズ株式会社)
情報理論（IT）	野上　保之	(岡山大学)
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）	冨山　宏之	(立命館大学)
情報セキュリティ（ISEC）	清本　晋作	(KDDI 総合研究所)
信号処理（SIP）	西川　清史	(東京都立大学)
ワイドバンドシステム（WBS）	落合　秀樹	(大阪大学)
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）	坪田　　康	(京都工芸繊維大学)
技術と社会・倫理（SITE）	辰己　丈夫	(放送大学)
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）	笹岡　直人	(鳥取大学)
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）	石井　光治	(香川大学)
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）	水野　　修	(工学院大学)
ハードウェアセキュリティ（HWS）	秋下　　徹	(ソニーセミコンダクタソリューションズ株式会社)
光輝会（SSA）（オブザーバ）	大塚　　玲	(情報セキュリティ大学院大学)
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）	尾上　孝雄	(大阪大学)
次期会長（オブザーバ）	岩本　　貢	(電気通信大学)
庶務幹事（オブザーバ）	傘　　昊	(東京都市大学)
庶務幹事（オブザーバ）	藤澤　匡哉	(東京理科大学)
研究会連絡会幹事（オブザーバ）	中野　秀洋	(東京都市大学)
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	関屋　大雄	(千葉大学)
ソサイエティ次期会長	小西　啓治	(大阪公立大学)
庶務幹事	荒井伸太郎	(岡山理科大学)
庶務幹事	杉谷　栄規	(大阪公立大学)
会計幹事	井岡　恵理	(芝浦工業大学)
電子広報担当幹事	加藤　秀行	(大分大学)
大会担当幹事	伊藤　大輔	(岐阜大学)
運営委員	鳥飼　弘幸	(法政大学)
運営委員	高橋　規一	(岡山大学)
運営委員	上田　哲史	(徳島大学)
運営委員	清水　邦康	(千葉工業大学)
運営委員	中野　秀洋	(東京都市大学)
運営委員	長谷川幹雄	(東京理科大学)
運営委員	久門　尚史	(京都大学)
運営委員	保坂　亮介	(芝浦工業大学)
運営委員	木村　真之	(摂南大学)
運営委員	内田　淳史	(埼玉大学)
運営委員	上山　憲昭	(立命館大学)
運営委員	菅野　円隆	(埼玉大学)
運営委員	堀尾　喜彦	(帝京大学先端総合研究機構)
運営委員	浅井　哲也	(北海道大学)
運営委員	松下　春奈	(香川大学)
運営委員	佐藤　雅俊	(玉川大学)
運営委員	若宮　直紀	(大阪大学)

編集後記

今号より編集委員長を仰せつかりました．FR 誌の仕事は 2014 年に編集幹事を担当してから約 10 年ぶりとなります．皆様のおかげで質の高い解説記事などを掲載できていると思います．引き続き最新技術から技術の原点まで幅広い記事を掲載できればと思っています．どうぞよろしくお願いいたします．（定兼邦彦）

今号より編集幹事会編集正幹事を務めることになり，主に「ごあいさつ」の編集を担当しました．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．この後記を執筆している時点でまだ編集作業は完了しておりませんが，今号は正幹事として少々反省の多い発行となりました．子供の頃から宿題はぎりぎりになってから取り掛かるタイプだったのですが，次号ではしっかりと準備して作業にあたりたいと思います．（松井健太郎）

今号より編集副幹事を務めることになりました．今号では「ESS ニュース」「だより」「開催案内」「論文募集」「委員会・編集後記」を担当しております．昨年度は編集幹事補佐を務めておりましたが，本年度より編集副幹事となり，担当記事も増えたため，当初は戸惑いもございました．それでも，執筆頂いた皆様の多大なるご協力のおかげで，編集作業を滞りなく進めることができました．ご協力頂き，誠にありがとうございました．（宮北和之）

今号の「研究会に行こう」の特別編集幹事を担当させて頂きました．ご執筆頂きました著者の皆様，並びにサポート頂きました編集委員，事務局，出版社の皆様にこの場を借りて感謝申し上げます．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，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いただければ幸いです．（海上勇二）

Fundamentals Review へのお問い合わせ

・本誌への御意見．御要望．入手など：fr-ess@ieice.org
・Fundamentals Review Homepage：https://www.ieice.org/ess/ESS/Fundam-Review.html

Fundamentals Review 第十九巻 第一号

令和七年七月一日発行

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