

Fundamentals Review

2024 July Vol.18 No.

1

技術の原点

macOS マシン群におけるメッシュ型 NFS
ホーム共有による分散型計算機ネットワーク
の構築

—Unix におけるレガシーな技術とモダンな技術の融合—

レビュー論文

LDPC 符号のための近接勾配復号法

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

ごあいさつ

2
5

基礎・境界ソサイエティ：持続可能な発展を目指して
NOLTA ソサイエティへようこそ！

和田山 正
夏目季代久

技術の原点

7

macOS マシン群におけるメッシュ型 NFS ホーム共有による分散型計算機
ネットワークの構築

—Unix におけるレガシーな技術とモダンな技術の融合—

山田泰司, 高橋 純, 島田 裕, 池口 徹

レビュー論文

29

LDPC 符号のための近接勾配復号法

和田山正

解説論文

42

Decentralized Identifiers (DID) と Verifiable Credentials (VC) の現
況

鈴木茂哉, 安田クリスチーナ, 富士榮尚寛, 阿部涼介

56

医用超音波分野におけるビームフォーミング技術

長谷川英之

71

確率的インメモリコンピューティングとその AI 応用

浅井哲也

79

地域住民に向けた土砂災害モニタリングシステムの研究開発

西 正博, 小林 真, 新 浩一

88

セキュリティに焦点を当てたブロックチェーン技術の最新の研究動向

面 和成

その他

101

ESS ニュース

101

NOLTA, IEICE 特集号

山仲芳和

102

研究会に行こう！

102

信頼性研究会 (R)

門田 靖

102

複雑コミュニケーションサイエンス研究専門委員会 (CCS)

佐々木智志

103

情報セキュリティ研究会 (ISEC)

四方順司

104

情報理論研究会 (IT)

野上保之

104

信号処理研究会 (SIP)

市毛弘一

105

高信頼制御通信研究会 (RCC)

石井光治

106

だより

日本工業大学だより

平栗健史 (日本工業大学)

109

受賞者の声

109

令和 5 年度フェロー称号

112

令和 5 年度 学術奨励賞

114

開催案内

114

IWSEC2024

115

SISA2024

116

論文募集

Preface

- | | | |
|---|------------------------------------|------------------|
| 2 | ESS : Towards a Sustainable Future | Tadashi WADAYAMA |
| 5 | Welcome to the NOLTA Society! | Kiyohisa NATSUME |

Origins of Technology

- | | |
|---|---|
| 7 | Construction of Distributed Computer Network by Mesh-Type NFS Home Sharing in Group of macOS Machines
—Fusion of Legacy and Modern Unix Technologies—
Taiji YAMADA, Jun TAKAHASHI, Yutaka SHIMADA, Tohru IKEGUCHI |
|---|---|

Advanced Review Papers

- | | | |
|----|----------------------------------|------------------|
| 29 | Proximal Decoding for LDPC Codes | Tadashi WADAYAMA |
|----|----------------------------------|------------------|

Review Papers

- | | | |
|----|--|---|
| 42 | Current Status of Decentralized Identifiers and Verifiable Credentials | Shigeya SUZUKI, Kristina YASUDA, Naohiro FUJIE, Ryosuke ABE |
| 56 | Beamforming Methods in the Field of Medical Ultrasonics | Hideyuki HASEGAWA |
| 71 | Stochastic In-Memory Computing and Its Applications to Artificial Intelligence | Tetsuya ASAI |
| 79 | Research and Development on Landslide Disaster Monitoring System for Local Residents | Masahiro NISHI, Makoto KOBAYASHI, Koichi SHIN |
| 88 | Recent Research Activities in Blockchain Technology Focusing on Security | Kazumasa OMOTE |

Miscellaneous Articles

- | | |
|-----|------------------------------|
| 101 | ESS News |
| 102 | Let's go to IEICE Workshops! |
| 106 | Report |
| 109 | Winners' Voice |
| 114 | Call for Participations |
| 116 | Call for Papers |



基礎・境界ソサイエティ： 持続可能な発展を目指して

ESS : Towards a Sustainable Future

会長 和田山 正

1. はじめに

改めて考えてみると電子情報通信学会との関わりは、修士学生時代に遡る。初めての研究会で、その分野で著名な先生が最前列に座っていらっしゃる前で発表するという経験がある。そのときの発表の内容は忘れてしまったが、極度に緊張していたこと、また、その先生が休憩のときに声をかけてくれて、研究に関するコメントと励ましを頂いたことはよく覚えている。修士課程の頃なので、恐らく大したことのない研究内容であったかと思うのだが、フィードバックがあったことが小さな自信となり、それが研究の面白さの一面を知るきっかけになった。

博士号をとってから約30年、あと定年まで10年というところにきて、言ってみれば第4コーナーを通過しつつある我が身を振り返ってみて、年季だけは積み重ねていても、その先生のような振る舞いができているかは、若干心もとない。学会運営に関わる立場にいるいま、初心を思い出して学会から受けてきた恩恵を少しでも返していかなければ、と改めて思う。

学会の一番の魅力は、学生、若手、ベテラン、シニアにかかわらず、同じ学問を志す人間が集まって語り、学ぶ点であろう。論語でいうところの「朋あり遠方より来る、また楽しからずや」である。様々な出会いを通したネットワーク構築の場であり、若い人が自分の研究発表を通して成長する場であり、旧知の研究者が語り合う場でもある。また学会に行くことで、関連研究の最新の知識だけではなく、研究へのモチベーションが得られることも多い。その「学会の場」というのは、強固な要塞のようにガッチリした未来永劫盤石なものではなく、どちらかというと花壇のように、水をやりたり肥料をやりたりと不断の手入れの上で花が咲く場所であり、その時代に合わせたメンテナンスが必要であるように思う。

2. ESSの新年度の方向性について

2.1 運営基本方針について

電子情報通信学会基礎・境界ソサイエティ（ESS）の会

長への就任にあたり、「ESS学会活動の価値を毀損することなく持続可能な形で保ちつつ、更に若い世代へ学会活動の魅力を伝える」ことを基本的な方針としたいと考えている。ESSのもつ貴重な無形資産である

- ・基礎研究の重要性への認識と研究の多様性
- ・英文論文誌・和文論文誌・FR誌
- ・研究会活動・大会活動

の価値を守り育てるには、いま、電子情報通信学会が直面している諸問題を念頭において、大事に保つべきことと、逆に時代や状況に応じて変えるべきこと、の両者を考えていく必要がある。

歴代のESS会長、並びにESS運営会議で進めてこられた施策を継承・発展させつつ、また必要があるところでは新しい試み・施策を検討・実施していく。サブソサイエティ長の方々、研究専門委員会委員長の方々を含め、ESS運営会議のメンバーの方々からのご意見をしっかり聴き取り、ESS執行部として今年度の施策に反映できるように注力していきたい。

2.2 学会の抱える問題について

学会の状況を反映したESS運営の施策を考える上で、学会の抱える諸問題についての認識が必要となる。学会全体の抱える大きな問題としては、

- (1) 学会会員数の減少（特に若手）
- (2) 海外会員数の減少
- (3) 論文誌インパクトファクタ（IF）の伸び悩み
- (4) 長期的視点における学会運営を担う若手研究者の減少

などがある。

(1) 理事会・企画戦略室で特に大きく問題視されているのが学会会員数の減少である。学会全体の経営的な観点、並びに学会の活性度の観点から望ましい状況ではないと認識されている。日本全体の若年者人口が漸減している状況では仕方がないという見方もあるが、何らかの可能な打つ手を考えていくことが各ソサイエティに求められている。

(2) 海外会員数はここ数年で劇的に減っており、それに従って英文論文誌への海外からの投稿も減っている。学会全

体として、論文誌・学会誌の多言語化によるアジア諸国の研究者の IEICE への興味喚起、研究会の海外開催の推奨などの方針が提案・実施されている。

(3) 論文誌 IF の伸び悩みについては、学会全体としてはオープンアクセスの推進、多言語化、EB における IEEE Xplore 掲載などの対応が進められている。

(4) については、(1) と密接につながるが、次第に研究会運営など学会運営を担う若手研究者が減少傾向にあることも長期的には考えていく必要がある問題である。大学に所属する若手研究者は、テニユアトラック制度など任期制雇用などが適用されているケースも増えてきており、過去とはそのあたりの状況が異なっていることも念頭におく必要がある。

これらの諸問題について、各ソサイエティからの貢献が本部より強く求められている状況である。

2.3 新年度の施策の方向性

ESS の新年度の事業計画として、過去の ESS 運営会議から継承した事業と定常的な事業に加えて、学会全体の問題への対応も考えつつ、次の方向性を考えている。

- (A) 研究会活動活性化
- (B) 若手・ジュニア世代からの魅力を高める
- (C) 国際活動への貢献
- (D) 持続可能な運営体制に向けて
- (E) 論文の IF 向上に向けての方策

(A) 研究会活動の活性化のためにも、ESS がカバーする研究領域に新規参入する若手研究者を増やすことは必要不可欠である。そのためにも、学生を含めて若手研究が研究会や総合大会・ソサイエティ大会により魅力を感じてもらえるように継続的に注力することが求められている。学生・若手研究者向けの企画を実施するようサブソ・研専会議で呼びかけるなど、若手世代を惹きつける企画実施をサブソ・研専会議などで呼びかけを行う。また、総合大会・ソサイエティ大会における発表・参加を増加させ、そしてそれを研究会活動の活性化につなげていくことを目指し、大会における企画セッションの充実化を図る。そのために、まず過去の大会企画を整理してこれまでの企画提案実績を検証し、企画提案実績の可視化を進めるとともに実績の手薄な分野について積極的に企画提案を検討するよう促す。

(B) 学生員・ジュニア会員を増やすこと、そして、学生員・ジュニア会員から正員への昇格者を増やすことは学会全体としても重要な課題である。この点に関しては、ジュニア会員運営委員会・若手会員活性化ワーキンググループと連携し、学会全体でのジュニア会員・若手会員向けの取り組みについて基礎・境界ソサイエティからの貢献の方向性を探る。

(C) 基礎・境界ソサイエティでは、和英論文誌に加え、2014 年 10 月より NOLTA ソサイエティとの共同機関誌として Fundamentals Review を発行している。Fundamentals

Review は良質の解説論文に定評があるものの、ほぼ全ての記事が日本語で執筆されている。そのため、これらの解説論文を多言語で翻訳・展開することができれば、海外の多くの研究者の興味を惹く可能性があり、特にアジア諸国の研究者に対する本学会のプレゼンス向上への寄与が期待される。現在、Fundamentals Review の多言語化に向けた検討を始めておりその実現に向けて検討・作業を継続する。また、海外向けの情報発信を充実させる取り組みとして、Distinguished Lecturer 拡充の取り組みを進める。2023 年度の Distinguished Lecturer リストには基礎・境界ソサイエティ分野の講師として 6 名が掲載されているものの、講師の専門分野に偏りがあり、基礎・境界ソサイエティの領域を広くカバーしているとは言い難い状況である。更に学会本体の呼びかけに呼応する形で、海外開催の研究会を促進する施策について検討をしていきたい。

(D) 持続可能な研究会、ソサイエティ運営について検討を進める。一つの方向性はデンタルトランスフォーメーション (DX) 化と研究会業務のアウトソーシングの検討である。ソサイエティや研究専門委員会運営の DX 化については、各種申請手続きのシステム化や、広報活動における SNS ツールの活用が考えられる。手続きのシステム化については、指定の様式にて書類を作成しメールで担当幹事へ提出するやり方から Web フォームへの入力に切り替えることで、メール送受信時のトラブルの回避や、申請データ管理の容易化が期待できる。また、研究専門委員会のグループ化に関連して、研専事務の共通化の議論などが考えられる。例えば研究専門委員会の間で共通化可能な事務作業を洗い出し、それらをグループで負担することで事務作業を軽減する可能性を探る。

(E) オープンアクセス化の効果検証、招待論文企画の検討、EB における IEEE Explore 掲載に関する情報収集など、IF 向上につながる今後の施策について検討を続ける。

3. む す び

本稿では、運営基本方針、学会の抱える問題、新年度の施策について述べた。学会のもつ各種問題については、即効性のある妙案の立案はなかなか難しいと考えられるが、様々な施策についての粘り強い継続的検討と実施により ESS のもつ価値の持続を目指すのが現実的であろう。ここで示した新規の施策については、叩き台であり新年度中に ESS の皆様のご意見を頂戴しながら走りながら検討を進めさせて頂ければと考えている。ESS 執行部メンバーとともに ESS 運営についてベストを尽くす所存であり、皆様方からのご支援とご協力をぜひともお願い申し上げる次第である。



著者紹介

和田山正（正員：シニア会員）

1993 京都工芸繊維大学大学院修了．1997 同大学工博．1995 岡山県立大学情報工学部助手．2004 名古屋工業大学大学院工学研究科助教授．2007 同大学大学院工学研究科准教授．2010 同大学大学院工学研究科教授．2021 年度 FR ベストオーサー賞，2022 年度論文賞受賞．著書『誤り訂正技術の基礎』『モデルベース深層学習と深層展開』など．符号理論，情報理論，機械学習に基づく信号処理，デジタル通信方式の研究に従事．IEEE 会員．



NOLTA ソサイエティへようこそ！

Welcome to the NOLTA Society!

NOLTA ソサイエティ会長 夏目季代久

NOLTA ソサイエティでは、昨年度大きなニュースが二つありました。一つは上田皖亮先生が 2023 IEEE Gustav Robert Kirchhoff Award を受賞されたことです。上田先生は、1961 年、世界で初めて、物理現象としてのカオスを発見されました。当時は、それが新しい現象であると認識されていませんでしたが、発見されたカオス現象の解軌道が描くストロボ写像は、その後、ジャパニーズアトラクタ、ウエダアトラクタと呼ばれるようになりました。電子回路におけるカオス現象の発見、及び非線形ダイナミクスの発展への貢献が高く評価された受賞です。受賞を記念して昨年度、IEICE ICT Pioneers Webinar にて講演して頂きました。誠におめでとうございます！

もう一つは、ソサイエティの英文電子ジャーナルである Nonlinear Theory and Its Applications, IEICE (略称 NOLTA) が昨年 6 月に Clarivate 社から Journal Impact Factor (IF) を取得したことです。NOLTA はオープンアクセス (OA) ジャーナルであり年に 4 回発行しています。発刊から、ご苦労されてきた歴任編集長及び編集委員の先生方のご努力に感謝いたします。引き続きジャーナルの改善に取り組んでおります。より多くの方の NOLTA へのご投稿をお待ちしています。

自己紹介が遅れましたが、このたび、NOLTA ソサイエティ会長を仰せつかりました。夏目季代久と申します。どうぞよろしくお願いいたします。本ソサイエティは、2014 年に発足^{(1),(2)}し、今年で 11 年めを迎えます。主に、“非線形”というキーワードで、「カオス」「フラクタル」「ファジー」「ニューロダイナミクス」「カオスニューラルネットワーク」「セルラニューラルネットワーク」「バイオサイバネティクス」「複雑系」「非線形回路とシステム」「結合発振器」「モデリングとシミュレーション」「精度保証数値解析」「進化論的計算」「予測とシステム同定」「最適化問題」のほか、非線形理論の「同期」「ネットワーク」「通信」「信号処理」「制御」「電力システム」への応用、更に「情報科学」「物理学」「応用数学」「化学」「神経科学」「光学」「生態学」「経済学」など、様々な分野の研究者が集まっています。330 名ほど所帯は小さいのですが、網羅している学問分野は幅広くなっています。電子・電気回路から私たちの生体、情報、経済ま

で、様々なところに“非線形”現象は顔を出します。最近はやりの、生成系 AI をはじめ AI の計算も非線形計算です。どの分野にも顔を出す非線形現象ですので、皆様も、自分の研究している現象が“非線形”だと思われたら、是非とも、私たちのソサイエティの門戸を叩いて下さい。本ソサイエティの研究専門委員会には非線形問題研究会、通称 NLP と、複雑コミュニケーションサイエンス研究会、通称 CCS があります。

NOLTA シンポジウムは NOLTA ソサイエティ主催の国際会議です。1990 年から毎年、開催しています。昨年は、Catania 大学 Arturo Buscarino 教授と大阪公立大学小西啓治教授お 2 人の General Co-Chairs のもと、イタリア Catania の Catania 大学 Cittadella Campus で行われました⁽³⁾。今年度は 12 月 3 日～6 日の期間、ベトナム、ハロン湾の Saigon-Halong Hotel で開催予定です⁽⁴⁾。

本ソサイエティは、上記の NOLTA シンポジウムのほか、国際交流も盛んに行っています。CCS を中心として日韓合同の複雑コミュニケーションサイエンス日韓ジョイントワークショップを日本と韓国との間で隔年開催しています。本年度、ワークショップは第 10 回を数え、今年は 1 月 29 日～30 日の間、別府、亀の井ホテルで行いました。2016 年には韓国マルチメディア学会 (Korea Multimedia Society; KMMS) と Sister Society の MOU を交わしました。更に本年 Korean Institute of Communications and Information Sciences (KICS) との MOU を 5 月 7 日に締結しました。

NOLTA ソサイエティ大会も、毎年行っており、昨年は東京都市大学で行い⁽⁵⁾、今年も 6 月 8 日小倉西日本総合展示場 AIM で行います⁽⁶⁾。大会中、研究発表はポスター発表で行います。

ソサイエティでは、若手育成を兼ねて、各年度ごとに NLP, CCS では奨励賞を、NOLTA シンポジウムでは Student Paper Award, NOLTA ソサイエティ大会では奨励賞を選出しています。是非とも若手の皆さんには積極的に NLP や CCS で発表され、“優しい”先生方のフィードバックをもらい、NOLTA ソサイエティ大会で発表し、NOLTA シンポジウムで海外デビューをし、最後に NOLTA に論文

投稿して頂ければ、と思っています。それが研究者として成功するキャリアパスです。是非とも NOLTA ソサイエティにご参加ください。

文 献

- (1) 藤原融, 堀尾喜彦, “NOLTA ソサイエティの発足,” 信学 FR 誌, vol. 8, no. 2, pp. 115-116, Oct. 2014.
- (2) 堀尾喜彦, 藤原融, “NOLTA ソサイエティの発足,” 信学誌, vol. 98, no. 1, pp. 67-69, Jan. 2015.
- (3) 藤田実沙, “国際会議開催報告 2023 International Symposium on Nonlinear Theory and Its Applications (NOLTA2023, 非線形理論とその応用シンポジウム),” 信学 FR 誌, vol. 17, no. 3, pp. 223-226, Jan. 2024.
- (4) “NOLTA2024,” <https://nolta2024.org/> (2024 年 4 月 20 日アクセス).
- (5) 島田裕, “2023 年電子情報通信学会 NOLTA ソサイエティ大会開催報告,” 信学 FR 誌, vol. 17, no. 2, pp. 157-160, Oct. 2023.
- (6) “2024 年電子情報通信学会 NOLTA ソサイエティ大会,” <https://nlsc2024.org/> (2024 年 4 月 20 日アクセス).

著者紹介

夏目季代久 (正員: シニア会員)

1987 東京大学薬学部製薬化学科卒, 1989 同大学大学院薬学系研究科博士前期課程修了, 1990 九州工業大学情報工学部生物化学システム工学科助手, 2006 同大学大学院生命体工学研究科教授 (現職). 博士 (薬学). 脳情報工学, 脳内海馬における脳波と記憶学習, 脳波を用いたブレインマシンインターフェースの開発, 音楽嗜好性脳波を用いた音楽推薦システムの開発に従事. 2003~2005 非線形問題研究専門委員会幹事, 2020 非線形問題研究専門委員会委員長.

macOS マシン群におけるメッシュ型 NFS ホーム共有による分散型計算機ネット ワークの構築

—Unix におけるレガシーな技術とモダンな技術の融合—

Construction of Distributed Computer Network by Mesh-Type NFS Home Sharing
in Group of macOS Machines

—Fusion of Legacy and Modern Unix Technologies—

山田 泰司 Taiji YAMADA

島田 裕 Yutaka SHIMADA

高橋 純 Jun TAKAHASHI

池口 徹 Tohru IKEGUCHI

アブストラクト NFS (Network File System) は Unix で用いられる分散ファイルシステムである。1990 年代の Unix を用いた計算機ネットワークでは、どのマシンにログインしても各ユーザのホームディレクトリが NFS 共有されることが通常であった。このようにローカルネットワーク内においてユーザのホームディレクトリをいつでも参照・共有できる環境は、計算機資源の有効利用、情報・技術の共有などのメリットを有している。一方、ストレージが HDD から SSD へと高速化された現在では、たとえ 10 GbE のように高速な伝送速度をもつネットワーク規格を用いても NFS ファイル共有のデータ転送速度がボトルネックとなり、高速なマシンの性能を引き出すことは困難となる。そこで、SSD のアクセス速度をコンソールでは落とすことなく、ローカルネットワーク内でのユーザのホームディレクトリを共有できるネットワーク環境を構築した。具体的には、各マシンのホームディレクトリを NFS エクスポートするメッシュ型 NFS ホーム共有による分散型計算機ネットワークの構築を、モダンな Unix である macOS で実現した。本稿はその技術解説である。

キーワード 分散型計算機ネットワーク, メッシュ型 NFS ホーム共有, macOS, Unix

Abstract NFS (Network File System) is a distributed file system used in Unix. In the 1990s, when managing and operating computer networks using Unix, it was common that users' home directories were shared through NFS from every machine where they logged into. Such an environment in which users' home directories can be referred to at any time within a local network has various advantages, for example, users on the local network can share technology information with each other and use computer resources in the local network. However, now that storage technologies have evolved from HDDs to SSDs, even if a network with a high transmission speed, e.g., 10 GbE, is used, NFS file sharing itself becomes a bottleneck in terms of access speed. Therefore, it is difficult to bring out the performance of faster machines. Therefore, we developed a network environment in which users' home directories can be shared within a local network without reducing the access speed of SSDs on the console. Specifically, we realized a distributed computer network using mesh-type NFS home sharing in which each machine exports its home directory through NFS on macOS, a modern Unix. This article offers one of the technical solutions to this issue.

Key words Distributed computer network, Mesh-type NFS home sharing, macOS, Unix

1. はじめに

1970 年代以降の計算機ネットワークの普及に伴い、ネットワーク上の異なる計算機で管理されているファイルを共有する

山田 泰司 株式会社あいほら研究開発チーム

E-mail taiji@aihara.co.jp

高橋 純 株式会社あいほら研究開発チーム

E-mail junt@aihara.co.jp

島田 裕 正員 埼玉大学大学院理工学研究科

E-mail yshimada@mail.saitama-u.ac.jp

池口 徹 正員：フェロー 東京理科大学工学部情報工学科

E-mail tohru@rs.tus.ac.jp

Taiji YAMADA, Nonmember (R&D Team, AIHARA Electrical Engineering Co., Ltd., 2-16-8 Hama-cho, Funabashi-shi, Chiba, 273-0012 Japan), Jun TAKAHASHI, Nonmember (R&D Team, AIHARA Electrical Engineering Co., Ltd., 2-16-8 Hama-cho, Funabashi-shi, Chiba, 273-0012 Japan), Yutaka SHIMADA, Member (Graduate School of Science and Engineering, Saitama University, 255 Shimo-Ookubo, Sakura-ku, Saitama-shi, Saitama, 338-8570 Japan), and Tohru IKEGUCHI, Fellow (Dept. of Information and Computer Technology, Faculty of Engineering, Tokyo University of Science, 6-3-1 Nijuku, Katsushika-ku, Tokyo, 125-8585 Japan).

電子情報通信学会 基礎・境界サイエティ

Fundamentals Review Vol.18 No.1 pp.7-28 2024 年 7 月

©電子情報通信学会 2024

ための様々なファイルシステムが提案された。これらの中でも Sun Microsystems 社によって開発された NFS (Network File System) ^{(1)~(8)} は Unix ^(注1) ⁽⁹⁾ 系 OS のシステムにおいて最も広く使用されるファイル共有システムの一つである。NFS では、ユーザは計算機のローカル領域に保存されたファイルにアクセスする操作と同様の操作で NFS サーバ上のファイルにアクセスすることができる。これによりファイルがネットワーク上の異なる計算機上で管理されていることをユーザに意識させることなく、透過性の高いファイルアクセスが実現される。NFS は最初

(注1)：本稿では UNIX と Unix を明確に区別して用いている。前者は商標であり、後者は Unix 系 OS 全般を指す⁽⁹⁾。例えば、BSD Unix の流れを汲む⁽⁹⁾ Mac OS X, OS X, macOS は、バージョン 10.5 から最新バージョン 14 において、POSIX:2001 準拠を IEEE から認証されているので UNIX である。一方、各種 BSD 系 Unix、各種 Linux ディストリビューションは IEEE から認証を得ていないため UNIX とはいえないが、おおむね POSIX 互換である。なお、Windows NT においては、POSIX subsystem, Interix, SFU, SUA を経て WSL/WSL2 へと POSIX 対応の公式サポートは変遷しつつも、POSIX エミュレーション Cygwin を用いれば Unix 的な使い勝手は Windows NT 系の初期から現在まで有効である。

にバージョン 2 が一般公開された後、バージョン 3, 4 が順次公開されている。この NFS によって計算機ネットワーク上の全てのクライアントマシンからサーバ上にある全ユーザのホームディレクトリを NFS でファイル共有し、LDAP などのディレクトリサービスにアクセスするためのプロトコルと組み合わせることで、各ユーザは各自のホームディレクトリがネットワーク上のどこに存在しているのかを意識することなく任意のマシンにログインすることが可能となる。1990 年代以降、このようなサーバ・クライアント方式が普及し、現在でも広く利用されている。

一方、2010 年代後期より、高速なストレージである SSD の大容量化が進み、これに伴って計算機のストレージが HDD から SSD へと置き換わりつつある。計算機のストレージが SSD へと置き換わることで、NFS が公開された当初と比較すると、計算機のローカルディスク領域へのアクセス速度は格段に上昇した。このような環境で、従来の単一のサーバ上に保存されたユーザのホームディレクトリを NFS ファイル共有する方式を採用した場合、ネットワーク上のデータ転送速度がボトルネックになりマシンの性能を十分に活かしきれないという問題が発生する。

上記のような背景から、本稿では特に大学の研究室など比較的小規模な組織での計算機ネットワークの運用を念頭に、複数の計算機上で各ユーザのホームディレクトリを分散管理・共有する方式を考える。具体的には、メッシュ型の計算機ネットワークを採用し、各計算機上のユーザのホームディレクトリを相互に NFS ファイル共有する方式である。本稿では、これをメッシュ型 NFS ホーム共有と呼び、これを用いて Unix^(注1)系 OS である macOS を搭載した数十台の計算機ネットワークを構築した事例について解説する。

近年ではクラウドサービス (例えば、iCloud, Nextcloud, Dropbox, Zenodo, GitHub など) が普及し、インターネット上の大容量ストレージに個人や組織のデータを保存することが可能になっている。これに伴って、企業・大学などでオンプレミスで構築されていた従来のローカルなファイル共有システムをクラウド上のストレージサービスへと置き換える動きも急速に進んでいるように思われる。その結果、大学などの教育機関では学生が計算機ネットワークの管理・運用に携わる貴重な機会が徐々に失われつつあるように思われる^(注2)。このような教育的観点からも本稿のような事例解説が従来から培われてきた技術の維持・伝承と利便性向上の一助になれば幸いである。

なお、UNIX は The Open Group, Solaris は Sun Microsystems (現, Oracle Corporation), SPARC は SPARC International, Inc., Linux は Linus Torvalds, FreeBSD は FreeBSD Foundation, NetBSD は The NetBSD Foundation, Inc., Mac OS, Mac OS X, OS X, macOS は Apple Inc., Windows, Active Directory は Microsoft Corporation, Cygwin は Red Hat Inc., TeX は American Mathematical Society, Wi-Fi は Wi-Fi Alliance, UPnP は UPnP Forum, VMware, VMware Fu-

sion は Broadcom Inc., その他はそれぞれの企業・団体の商標、または、登録商標である。また、本稿においては本文・図表中で「™」「®」は明記しない。

なお、本稿では多くの用語・略語を用いているが、それらの説明を付録 1. 用語集にまとめた。

2. 研究室における計算機ネットワーク管理の事例

まず、macOS マシン群におけるメッシュ型 NFS ホーム共有による分散型計算機ネットワークを構築するに至った経緯について述べる。その際、macOS におけるサーバ管理用ソフトウェアの歴史を交えて説明する。

本稿の著者の 1 人の池口は 1990 年代より研究室における Unix 系計算機群の管理・運営に携わるようになった。埼玉大学にて研究室を主宰するようになった 2000 年以降も、Sun Microsystems 社製 Solaris SPARC マシンをサーバに据え、各利用者はクライアントとして SPARC マシンを使用するという環境を構築した。Solaris オペレーティングシステムは BSD Unix から UNIX SVR4 (System V Release 4)⁽¹⁰⁾へと進歩を遂げた IEEE POSIX⁽¹¹⁾準拠のメジャーな Unix の一つである。

研究室での計算機環境において重視すべき点の一つが、GNU プロジェクトなどに代表される GCC, GNU make, GNU binutils/textutils/autotools, GNU Emacs, TeX などの OSS (Open Source Software) が豊富であることである。この点で Unix は最適解の一つである。更に Solaris では NFS が既定で有効であり、あるクライアントマシンのアカウントのホームディレクトリ `/export/home/$LOGNAME`^(注3)がネットワーク上のほかのマシン上でも `/home/$LOGNAME` としてオートマウントされる。その結果、どのマシンの CPU 資源も自分のアカウントのホームディレクトリとともに活用できる。これに加え、ユーザがファイルの閲覧許可を与えないなどしなければ、ユーザ同士が互いにホームディレクトリの資源を参照できる。これは Unix を用いて計算機環境を構築・運用する多くの研究室におけるドクトリンとも呼ぶべき相互扶助の精神である。

2000 年代の中盤には、Apple 社製の Mac OS X の利便性が向上し、ほかの Unix で開発されたソフトウェア資産が利用可能になっていたことを背景に、池口が主宰する研究室では 2005 年頃に Solaris から脱却し Mac OS X へと移行した。その後、Mac OS X は 2007 年にリリースされた Mac OS X 10.5 Leopard にて、IEEE POSIX.1 準拠となった^{(12)~(16)}。

2005 年当時、Mac OS X には一般ユーザ向けの Mac OS X と Mac OS X にサーバとしての機能をもたせた Mac OS X Server が存在した^(注4)。Mac OS X Server はユーザ管理、ファイル共有の機能、及び Web サーバ、メールサーバなどの機能・サービスとこれら进行操作するための独自の GUI を兼ね備えた OS である。例えば、Mac OS X Server 10.5 の場合、伝統的な NFS によるファイル共有に代わって Apple 社が開発した AFP

(注2)：本稿は BYOD 及び iCloud, Dropbox などのようなクラウドサービスの利用を否定しているわけではなく、これらのサービスと併用可能な技術紹介である。なお、本稿は Fibre チャネルを用いたデータセンター向けの Xsan のようなクラスターファイルシステムは想定していない。あくまで、民生向けの DFS (Distributed File System) が対象である。

(注3)：\$LOGNAME はユーザ名を表す。

(注4)：その後、Mac OS X (及び Mac OS X Server) は、OS X (OS X Server) に改称され、更に現在の macOS (macOS Server) に改称された。

(Apple Filing Protocol)⁽¹⁷⁾によるファイル共有が採用された。また、Open Directory によってユーザやネットワーク上のリソースを一元管理することで、ユーザのホームディレクトリが各マシンにオートマウントされ、どのマシンの CPU 資源も自分のアカウントのホームで利用でき、かつ互いのホームを参照することが可能な計算機ネットワーク環境を構築することができた。

しかし、Mac OS X Server は、現在の macOS Server に改称された後、2022 年 4 月 21 日にその販売が終了⁽¹⁸⁾した。その間、2005 年当時の Mac OS Server の GUI アプリケーションで利用可能であったサービスの多くが削除された。最終的には、組織のデバイスを管理するプロファイルマネージャと、OSS の OpenLDAP⁽¹⁹⁾によるディレクトリサービスのみを提供するソフトウェアとなっている。本稿では、現在は購入できない macOS Server のサーバ管理用アプリケーションである **Server.app** についての話題に触れるが、**Server.app** の有無にかかわらず OpenLDAP を利用することが本質なので、一般性は失われない。また、筆者らに経験はないが、Microsoft が提供するディレクトリサービスである Active Directory⁽²⁰⁾にも macOS は対応しているの、OpenLDAP によるディレクトリサービスに関する事項はそれらに読み替えることができる。なお、Unix ではレガシーだが一般的な NIS (Network Information Service)⁽²¹⁾、⁽²²⁾によるディレクトリサービスについては macOS 10.13 High Sierra 以降は対応しておらず、OpenLDAP と Active Directory のみが設定可能となっている。

さて、2005 年当時の Mac OS X Server を導入した当初、筆者らは主に以下のサーバ機能・サービスを利用していた^(注5)。

- (1) ウェブサーバ… Apache HTTP Server
- (2) メール送信サーバ… Postfix SMTP Server
- (3) メール受信サーバ… Cyrus IMAP Server, Mac OS X 10.6 Snow Leopard より Dovecot IMAP Server
- (4) ストレージサーバ… AFP Server, SMB Server
- (5) DNS サーバ… bind
- (6) ディレクトリサービス… OpenLDAP

Microsoft とは異なり、Apple はレガシーな機能を積極的に切り捨てることを厭わない。実際、上記 (1)～(6) のサーバ機能は主に OS のメジャーアップデートのたびに次々と **Server.app** から削除された。その際、DNS、IMAP サーバ以外は CUI (Character User Interface)^(注6)ベースのアプリケーションに統合された(表 1 参照)。表 1 における「GUI から除去」された、DNS、IMAP サーバ以外の機能は、macOS に CUI ベースで統合されており、GUI から削除されたとしても CUI 環境での利用が可能である。例えば、**Server.app** はなくとも通常の macOS で Web サーバである Apache HTTP Server を起動するには、以下のコマンドを実行するだけである^(注7)。

```
% sudo launchctl load -w \
/System/Library/LaunchDaemons/org.apache.httpd.plist
```

(注5)：なお、本稿では BYOD に関連する MDM (Mobile Device Manager) とプロファイルマネージャによる組織の管理ポリシー運用までは踏み込まない。

(注6)：CLI (Command Line Interface) とも呼ぶ。

(注7)：本稿では、コマンドラインにおける実行例について、注目したいコマンド列を青、重要なコマンド列を赤、プロンプトは灰色で示している。

表 1 **Server.app** が扱う各種機能の変遷 CUI で ◎ は特別なソフトウェアをインストールしなくても利用できる機能を表し、○ は別途ソフトウェアをインストールすることで利用できる機能を表す。また、× は実質的に廃止された機能を表す。

機能	状況	OS ver.	CUI
Apache HTTP Server	2018 年 GUI から除去	10.14～	◎
Postfix SMTP Server	2018 年 GUI から除去	10.14～	◎
IMAP Server	2018 年廃止	10.14～	○
AFP Server	2020 年廃止	11～	×
SMB Server	2017 年 macOS の GUI に統合	10.13～	◎
DNS (bind)	2018 年 GUI から除去	10.14～	○
OpenLDAP	2022 年 Server.app の廃止	13～	◎

ここで、「%」はプロンプトを表し、行末の「\」は長いコマンドが次の行に折り返されたことを表す記号である^(注8)。本稿の主題ではないので詳説は省くが、IMAP サーバや DNS サーバについても、MacPorts や Homebrew などのパッケージ管理システムにより導入が可能である。また、AFP サーバについては実質的に廃止されていると考えてよい。その理由は macOS 10.13 High Sierra より従来の HFS+ (Hierarchical File System Plus) に代わり導入された APFS (Apple File System) というファイルシステムに AFP サーバが対応していないためである。なお、macOS 10.14 Mojave 以降では、ストレージを APFS へ移行せず HFS+ のまま継続することは困難である。なぜなら、macOS 10.14 Mojave 以降のバージョンの macOS から起動ストレージとして HFS+ は未対応になったためである。その上、APFS は NVMe SSD のような高速なストレージ向けに再設計されており、SATA HDD の場合でも HFS+ より APFS の方がアクセス速度が実際には 2 倍程度も高速である。よって、macOS ではファイルシステムとして APFS が推奨される。一方で、Microsoft Windows 系の SMB (Server Message Block)⁽²³⁾によるファイル共有は健在であり、個人ユースでは AFP から SMB への移行で事足りるだろう。このように、BSD 系 Unix や GNU Linux とは異なり macOS という Unix では、Apple の判断に合わせてレガシーな技術からモダンな技術へと追従していくことが要求される。

さて、以上のことからファイル共有については、OS X 10.11 El Capitan と **Server.app** 5.1 を使用して AFP の継続利用を試みる、macOS 12 Monterey と最終版 **Server.app** 5.12.2 で SMB に移行する、AFP、SMB の代わりに NFS を様々な OS バージョンで利用するという三つの選択肢が考えられる。

3. ファイル共有機能によるホームディレクトリ運用の検証実験

3.1 ホームディレクトリ運用の検証実験環境

第 2 節で述べたとおり、Mac OS X Server (現在の macOS

(注8)：最新の macOS では既定のログインシェルが **zsh** であるため、特に断らない限り、本稿で扱うのは **zsh** のコマンドである。また、本稿で紹介するコマンドにおいて、実際の場面では、行末の「\」を省略して次の行を続けて入力すれば実行できる。

表 2 ホームディレクトリをエクスポートするためのファイル共有方法一覧

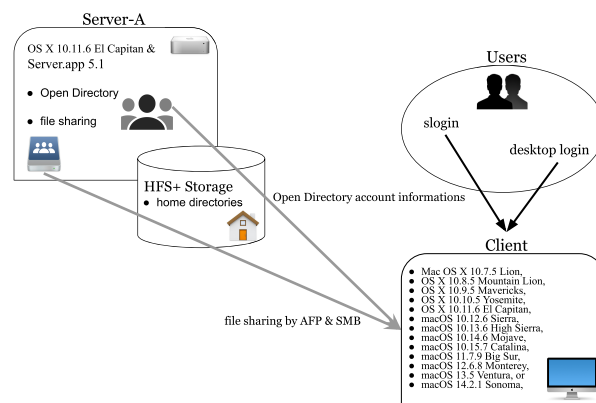
ファイル共有の提供方法	プロトコル
Server.app のファイル共有機能	AFP/SMB
OS によるファイル共有機能	AFP/SMB/NFS

Server) の AFP によるファイル共有機能と Open Directory によるユーザ管理機能によって、ストレージサーバにある各ユーザのホームディレクトリをクライアントマシンにマウントすることで、利用者はどのクライアントマシンでもデスクトップログインが可能であった。このような方式は、ネットワーク上のユーザ間の情報共有を円滑にし、また、ネットワーク上の計算機資源を余すことなく利用できるという大きなメリットを有していた^{(24)~(27)}。しかし、macOS 10.15 Catalina 以降のバージョンの macOS ではこの方式を用いたデスクトップログインが不可能となっている^(注9)。そこで、クライアントマシンの OS バージョンについて、ストレージサーバ上のホームディレクトリをエクスポート^(注10)するためのファイル共有方法(表 2)によって、クライアントマシンへのログインの挙動がどのようになるのかを調査した。また、ネットワーク越しにストレージへとアクセスする際のアクセス速度もファイル共有プロトコルごとに調査した。

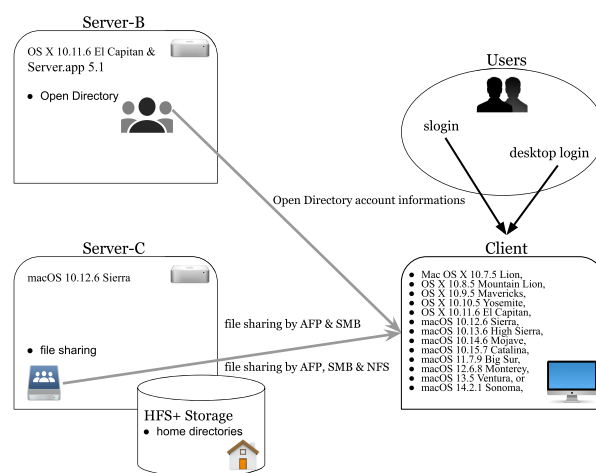
検証に用いるマシンは VMware Fusion⁽²⁸⁾バージョン 13.0.2 で構築した仮想マシンである。その際、図 1(a) のような Server.app のファイル共有を利用するレガシーな構成における検証と、図 1(b) のような OS のファイル共有機能を利用するモダンな構成における検証を行う。それぞれ、Open Directory からアカウント情報を得て、ファイル共有サーバからホームディレクトリの供給を受けてクライアントマシンにログインする。

これらのサーバのうち、Server-A 及び Server-B において、Server.app の Open Directory サーバ機能を用いて、ユーザのアカウント管理を行う。ここで、適切なアカウント設定がなされていて、クライアントマシンに /Network/ ディレクトリが存在すれば^(注11)⁽²⁹⁾、ログイン時にホームディレクトリが自動的にマウントされる。

Server-A では、自身に搭載されているハードディスクに置かれたユーザのホームディレクトリを提供するが、それには Server.app 5.1 のファイル共有機能のアクセスオプション「ホームディレクトリ接続」を有効にして、プロトコルは AFP か SMB のどちらかを選択する。また、Server-B で運用する Server.app 5.12.2 には Server.app 5.1 のようなファイル共有機能が存在しないため、OS のファイル共有機能を用いる。しかし、Server-B の OS である macOS 12.6.8 Monterey のファイル共有機能には、AFP ファイル共有が存在しない。そこで、ストレージサー



(a)



(b)

図 1 (a) Server.app のファイル共有を利用するレガシーな構成における検証方法と (b) OS のファイル共有機能を利用するモダンな構成における検証方法。なお、図中では macOS 標準のシステムアイコンを利用している。

バとして Server-C を援用した。NFS によるファイル共有は、/etc/exports の設定で行うが、これについては第 5 節で詳しく述べる。

3.2 一つのアカウントがログインする際のホームディレクトリ運用の可否

これらのサーバとクライアントマシンを用いて、クライアントマシンへ正常に slogin⁽³⁰⁾ (CUI) 可能かどうかと正常にデスクトップログイン (GUI) 可能かどうかを検証した。結果を表 3, 4 に示す。

表 3 より、OS X 10.9.5 Mavericks 以外の全てのクライアント OS のマシンへの slogin は可能である。ただし、AFP と SMB プロトコルでは一見、実運用上は支障なさそうに見えるが、他のユーザのホームのオーナー情報がログインしたユーザ所有に見えてしまうという問題がある。

また、AFP と SMB プロトコルでのデスクトップログインについては、表 4 のとおり、やはり macOS 10.15 Catalina 以降の OS では正常にログインができない。この場合、強制電源断による再起動が必要である。なお、NFS の場合は、パスワード認

(注9)：この問題に関する Apple の公式文書は見当たらない。

(注10)：macOS 10.15.7 Catalina では、最新パッチであるバージョン 10.15.7 ビルド 19H2026 を適用すると、AFP 及び SMB ファイル共有をオンにできないが、古いバージョン 10.15.7 ビルド 19H1824 であればオンにすることができる。

(注11)：macOS 10.15 Catalina 以降では / (ルートディレクトリ) 下には、マウントポイントのための空のディレクトリか、シンボリックリンクしか作成できない⁽²⁹⁾。そのため、第 5.2.2 節で解説する /etc/synthetic.conf⁽²⁹⁾へ「Network System/Volumes/Data/Network」の追記による対応が必要となることに注意。

表3 クライアント OS バージョンごとの slogin (CUI) の可否 ✓ はログイン可能かつ他のユーザのホームのオーナー情報はオリジナルどおりで、実際のファイルアクセスは正常動作することを表す。✓¹ はログインが可能かつ他のユーザのホームのオーナー情報がログインしたユーザ所有に見えてしまうが、実際のファイルアクセスは正常動作することを表す。また、× はログイン不可能であることを表す。

Server.app バージョン	5.1		5.12.2		
ファイル共有	Server.app		OS の機能		
OS ver. \ プロトコル	AFP	SMB	AFP	SMB	NFS
10.7, 10.8	✓	✓	✓ ¹	✓	✓
10.9	×	×	×	×	×
10.10~10.15, 11~14	✓	✓ ¹	✓ ¹	✓ ¹	✓

表4 クライアント OS バージョンごとのデスクトップログイン (GUI) の可否 記号 ✓, ✓¹, 及び × の意味は表3 と同様である。

Server.app バージョン	5.1		5.12.2		
ファイル共有	Server.app		OS の機能		
OS ver. \ プロトコル	AFP	SMB	AFP	SMB	NFS
10.7, 10.8	✓	✓	✓ ¹	✓	×
10.9	×	×	×	×	×
10.10~10.14	✓	✓ ¹	✓ ¹	✓ ¹	×
10.15, 11~14	×	×	×	×	×

証後に「今はユーザアカウント "\$LOGNAME" にログインできません。エラーが起きたため、アカウントにログインできませんでした。」というメッセージが表示され先に進まず、ホームディレクトリもマウントされない。これは OS がデスクトップログインにおいて NFS プロトコルのオートマウントをサポートしていないためである。

3.3 二つのアカウントが同時にログインする際のホームディレクトリ運用の可否

次に、一つのボリュームにホームディレクトリがある二つのアカウントで、既に1人めがログインしており、後から2人めがログインしようとしたときにログインが正常に行われるか検証した。結果を表5, 6に示す。

表5に示したとおり、slogin は NFS でのみ正常にログインが可能である。ほかのプロトコルではログインはできるもののホームディレクトリがマウントされず、正常な利用ができない。また、デスクトップログインは表6に示したとおり全てのプロトコルで正常なログインができない。AFP では「今はユーザアカウント "\$LOGNAME" にログインできません。」とメッセージが表示される。SMB ではパスワード認証後、デスクトップ画面が表示されるものの、メニューバーや Dock が表示されずに正常な利用ができない状態となり、先にログインしていたユーザにもメニューバーが正しく表示されないという影響を及ぼすこともある。

以上の結果から、Server.app によってファイル共有が提供されていた時代においては、AFPなどを介して、単一ユーザでのリモートホームの利用を想定していたことがうかがえる。しか

表5 クライアント OS バージョンごとの2アカウント同時 slogin (CUI) の可否 ✓ は二つのアカウントで同時ログインが可能であることを表す。また、× は二つのアカウントで同時ログインが不可能かつホームディレクトリが不在となる状況を表す。

Server.app バージョン	5.1		5.12.2		
ファイル共有	Server.app		OS の機能		
OS ver. \ プロトコル	AFP	SMB	AFP	SMB	NFS
10.7, 10.8	×	×	×	×	✓
10.9	—				
10.10~10.15, 11~14	×	×	×	×	✓

表6 クライアント OS バージョンごとの2アカウント同時デスクトップログイン (GUI) の可否 ✓ 記号の意味は表5 と同じである。また、× は二つのアカウントで同時ログインが不可能、— は1アカウントでもログインができない状況を表す。

Server.app バージョン	5.1		5.12.2		
ファイル共有	Server.app		OS の機能		
OS ver. \ プロトコル	AFP	SMB	AFP	SMB	NFS
10.7, 10.8	×	×	×	×	—
10.9	—				
10.10～10.14	×	×	×	×	
10.15, 11～14	—				

し、APFS の登場で AFP が非サポートとなり、その代替として SMB を推奨としつつも、複数ユーザによるリモートホームの同時利用を想定するまでには至っていないと推測される。しかしながら、幸いなことに、macOS は Unix であるので、NFS は CUI において、安定して利用可能である。ただし、重要な管理上の必要事項が存在することは第5節で取り上げる。

3.4 ファイル共有プロトコルとローカルストレージへのアクセス速度検証

第2節で述べたとおり、従来の Open Directory と AFP を用いたサーバ・クライアント方式によるユーザのホームディレクトリ共有は macOS 11 Big Sur 以降の最近の macOS では事実上困難である。そこで、ホームディレクトリの共有そのものの問題と近年のストレージ事情に鑑みたネットワーク設計の見直しを行った。

まず、ストレージのアクセス速度に関して、例えば、SATA HDD のアクセス速度は HFS+ ファイルシステムで 0.7 Gbps 程度、新しい APFS ファイルシステムでは 1.4 Gbps 程度となる。一方、近年利用が急速に拡大している NVMe (Non-Volatile Memory Express) M.2 SSD の場合、24 Gbps、更には 46 Gbps ものアクセス速度に達する。このような高速な SSD を搭載した計算機のストレージにファイル共有プロトコルを通してほかの計算機からアクセスする場合、もし、計算機ネットワーク上のデータ転送速度が低速であれば、それがボトルネックとなり高速な SSD の性能を十分に生かしきれないことになる。例えば、10 ギガビット Ethernet のように比較的高速なデータ転送を実現可能な規格を用いて計算機ネットワークを構築しても、SSD のアクセス速度には追いつかない。更に、ローカルストレージ

表 7 ストレージと GbE 環境におけるファイル共有プロトコルのアクセス速度 (Gbps) † は NVMe SSD, ‡ は Fusion Drive (NVMe SSD + SATA HDD), その他は SATA HDD ストレージを表す。また, – は OS の制約により計測不可である。

	Direct Storage	NFS localhost	NFS GbE	SMB GbE	AFP localhost	AFP GbE
2022 Mac Studio†	46.8	8.3	0.4	0.9	–	–
2019 Mac Pro†	23.6	1.8	0.5	0.9	–	–
Late 2015 iMac‡	4.1	1.6	0.2	0.8	–	–
Late 2013 iMac	1.3	0.6	0.2	–	–	–
2012 Mac Pro	0.9	0.9	0.2	0.8	–	–
2008 Mac Pro	0.4	0.4	0.2	0.4	0.4	0.4

であってもファイル共有プロトコルを介するとボトルネックになってしまう。これはローカルのソケット通信では SSD のような高い速度を想定していないためである。

実際に、ファイル書き込み速度の測定を行った結果を表 7^(注12) に示す。表 7 では 2008～2022 年代の実機におけるストレージへのアクセス速度 (Direct Storage), それをクライアントマシンからファイル共有プロトコルを介してアクセスする場合のうち, クライアントマシンがストレージサーバ自身である場合のアクセス速度 (NFS localhost, AFP localhost, SMB は自身への接続は不可能) とクライアントマシンがギガビット Ethernet を介してストレージサーバに接続されている場合のファイル共有プロトコルごとのアクセス速度 (NFS GbE, SMB GbE, AFP GbE) を示している。10 年以上前であれば, GbE であればネットワークを介したこのような NFS による運用でもメリットは大きかったが, 近年の SSD のアクセス速度とコンピュータ自身の高性能化には GbE はもとより, 手の届くようになってきた 10 GbE 環境でさえデメリットが大きいことが分かる。

以上から, ホーム共有については, AFP, SMB はここでの目的には使用せず, NFS を様々な OS バージョンで利用することが最適であると考えられる。

4. \$UID と Open Directory

前節までは, NFS における注意点を具体的に記述することなく話を進めてきたが, 以下では Unix や NFS などに不慣れな読者のために実際の運用を交えて解説する。

多くの大学の研究室では卒業生などを含めて多数のアカウントが存在すると思われる。実際, 著者の 1 人の池口の研究室で

(注12): 表 7 の各機種の仕様 (モデル名 – model id./model no./主なモデルスペック/main memory/storage スペック) は次のとおりである。2022 Mac Studio – Mac13,1/A2615/Apple 3.2 GHz M1 Max, 10 CPU, 24 GPU/32 GB LPDDR5/8 TB NVMe SSD, 2019 Mac Pro – MacPro7,1/A1991/Intel 2.5 GHz Xeon W-3257M, 28-core/192 GB DDR4/4 TB NVMe SSD, Late 2015 iMac – iMac17,1/A1419/Intel 4.0 GHz Core i7-6700K, 27" 5K/32 GB DDR3/2 TB SATA SSD+HDD, Late 2013 iMac – iMac14,2/A1419/Intel 3.2 GHz Core i5-4570, 27" /32 GB DDR3/1 TB SATA HDD, 2012 Mac Pro – MacPro5,1/A1289/Intel 3.2 GHz Xeon W3565 (Nehalem), 4-core/48 GB DDR3/8 TB SATA HDD, 2008 Mac Pro – MacPro3,1/A1186/Intel 2.8 GHz Xeon E5462, 8-core/10 GB DDR2/320 GB SATA HDD。

も卒業生・修了生などを含めて 100 以上のアカウントが存在する。また, 現役ユーザに関してはクライアントマシンのホームディレクトリ, 各ユーザの Web サイトの公開などが管理されている。具体的には **Server.app** の Open Directory⁽³¹⁾ で管理しているが, **dscl(1)**⁽³²⁾^(注13) コマンドで **Server.app** の Open Directory やローカルのアカウント情報を操作できる。

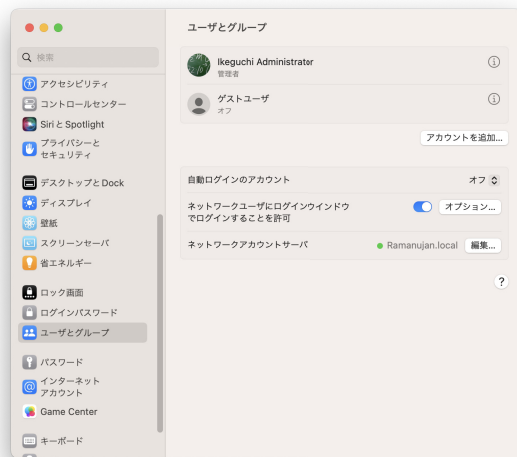
なお, 以下の **dscl(1)** コマンドでの処理は, macOS 以外の Unix では, NIS (Network Information Service) を利用している場合を含め **useradd**, **userdel** が対応するコマンドである。また, OpenLDAP 利用者は **ldapadd**, **ldapdelete**, **ldapsearch** が対応するコマンドであるので, 各 Unix において命令を適宜置き換えればよい。

本稿で紹介するネットワーク構築をスムーズに運用するために最も重要なことは, 全てのアカウントの **\$UID**^(注14) を厳格に管理することである。これは, バージョン 3 までの NFS^(注15) では UID を識別子として使うからである。幸いなことに, 池口の研究室では, かつては Solaris からアカウント管理をしていたこともあり, 1991 年頃から一貫して 8000 番以降^(注16) のユニークな **\$UID** が全てのアカウントに割り振られている。そのおかげで既に卒業したユーザの Web サイトも閲覧可能となっている^(注17)。なお, NFSv4 はユーザ名を識別子として用いるので, UID を厳格に管理する必要はない^(注18)。

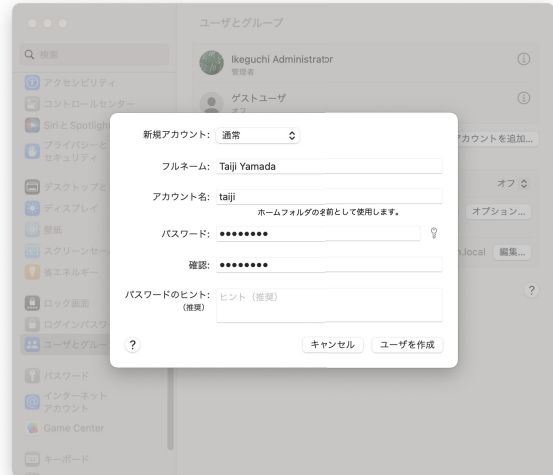
しかし, macOS の既定では 501 からの連番の **\$UID** が割り当てられてしまうため, 構築しようとするネットワーク上での同一ユーザに異なる **\$UID** が割り当てられてしまう。ただし, 各マシンの管理者権限をもつローカルアカウントは少なくとも一つは必要なので, 例えば 501 を管理者権限をもつアカウントに割り当て, それ以外は 8000 番以降で Open Directory のようなディレクトリサービスに任せることが可能である。

ローカルアカウントの作成はコマンドラインでも可能であるが, GUI での作成をその注意点と合わせて紹介する。まず, 図 2(a) のように, Apple メニュー → システム環境設定 → ユーザとグループの「ネットワークアカウントサーバ」の「編集…」から, Open Directory サーバのホスト名を設定できる。図 2(a) ではこれが **Ramanujan.local** となっている。これは DNS ホスト名であり, mDNS の Bonjour 名でもある。更に, 図 2(a) の「アカウントを追加…」で所望のローカルアカウントを追加できる。例えば, 図 2 では LOGNAME = **taiji**, UID = 8008 としている。

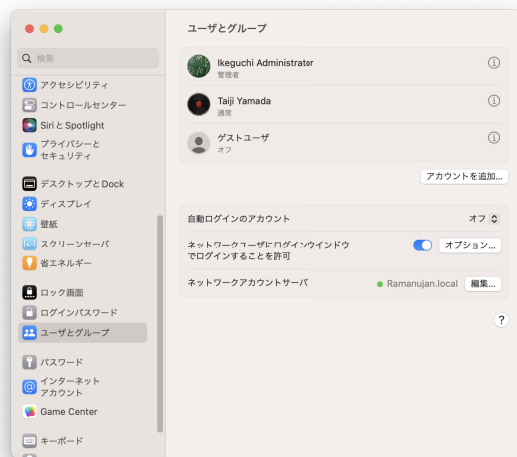
(注13): 固定幅フォントを用いた **dscl(1)** という表記について, 例えば **printf(1)** はコマンド名である **printf** 及びそのマニュアルページの節識別子 1 であることを表す Unix の慣習である。つまり, コマンドラインで **man -S 1 printf** とすれば「1: コマンド」節の **printf** のマニュアルページが表示され, **man -S 3 printf** とすると「3: ANSI/C 関数」節の **printf** という関数のマニュアルページが表示される。
(注14): **\$UID** は, 環境変数の一つである UID (ユーザ ID) の値であることを示す。
(注15): macOS 標準の NFS はバージョン 3 である。
(注16): ここでは 8000 番としているが, これはシステム予約番号に触れない 100～2147483647 (= $2^{32}-1 - 1$) 内の数値であれば任意である。
(注17): Unix 使いには当然なことだが, これは研究室における一つの財産といえるのかもしれない。
(注18): NFSv4 に影響を与えた AFS (Andrew File System) の派生として, OSF (Open Software Foundation) の DCE/DFS (Distributed Computing Environment/Distributed File System) がある。



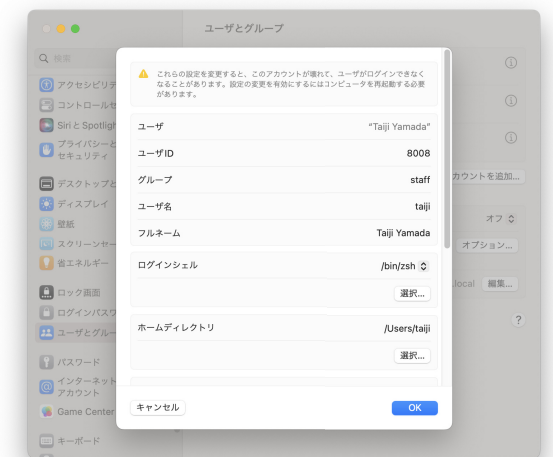
(a)



(b)



(c)



(d)

図 2 Open Directory への接続とローカルアカウントの作成

さて、図 2 (b) を見ると分かるように、新たなローカルアカウントを作成することはできるが **UID** を明示的に初期設定することができない。しかし、図 2 (c) のように、ローカルアカウントを作成した後に、そのエントリ上で右クリックすることで「詳細オプション」を選べるので、図 2 (d) のように、作成後のローカルアカウントの **UID** を変更することができる。

しかし、ホーム `/Users/taiji` は既に **UID = 502** で作成されている。そこで以下のようにしておくことが肝要である。

```
% sudo chown -R taiji /Users/taiji
```

macOS であるなら Apple が提供する `dscl(1)` コマンドで `Server.app` の Open Directory やローカルのアカウント情報を操作できる。上例の Open Directory の場合は、List 1 に載せたコマンドを打っていけばよい (実際には、これらのコマンドを記述した汎用的なシェルスクリプト⁽³³⁾を作成し、それを実行する)。ただし、List 1 における 1 行めの `$PASSWD` はディレクトリ管理者 `diradmin`、11 行めの `$passwd` はアカウント `taiji`

のパスワードに読み替える必要がある。

また、ローカルアカウントを作成する場合は、List 1 の 1, 8 行めをそれぞれ List 2^(注19) のコメントの指示のように置き換えればよい。なお、アカウントの設定を LDAP だけでなくローカルマシンにも設定しているのは、仮に LDAP サーバがダウンしても、少なくともローカルアカウントの利用が可能のように、冗長性をもたせているからである。

ここで、List 1 における 8 行めの `NFSHomeDirectory` 属性と 9 行めの `Comment` 属性内の `AUTOHOME` は、本稿の主題であるホームディレクトリ共有に関する更なる重要なポイントである。そこで、これについては、第 5.2.5 節で改めて解説する。

(注19)：本稿では、コマンドの実行例やファイルの提示において「:」のみの行は省略を表している。

List 1 dsc1 の使い方 (Open Directory の場合)

```

1  FLAGS="-u diradmin -P \"\$PASSWD\" /LDAPv3/Ramanujan.local"
2  dsc1 $FLAGS -create /Users/taiji      &&
3  dsc1 $FLAGS -create /Users/taiji RealName      "Taiji Yamada" &&
4  dsc1 $FLAGS -create /Users/taiji FirstName    "Taiji"        &&
5  dsc1 $FLAGS -create /Users/taiji LastName     "Yamada"       &&
6  dsc1 $FLAGS -create /Users/taiji UniqueID     8008     &&
7  dsc1 $FLAGS -create /Users/taiji PrimaryGroupID 20      &&
8  dsc1 $FLAGS -create /Users/taiji NFSHomeDirectory /Locals/Users_gellmann/taiji &&
9  dsc1 $FLAGS -create /Users/taiji Comment      AUTOHOME=nfs://gellmann.local/Users/taiji &&
10 dsc1 $FLAGS -create /Users/taiji UserShell    /bin/zsh       &&
11 dsc1 $FLAGS -passwd /Users/taiji "$passwd"    &&
12 : # ここで、全て成功したら戻り値 $? == 0, 一度でも失敗したら $? != 0 で終了

```

List 2 dsc1 の使い方 (ローカルアカウントの場合の変更点)

```

FLAGS="."
:
dsc1 $FLAGS -create /Users/taiji NFSHomeDirectory /Users/taiji &&
:

```

List 1 の 1 行目を置き換える

List 1 の 8 行目を置き換える

5. メッシュ型 NFS ホーム共有による分散型 計算機ネットワーク

5.1 構築する計算機ネットワークの概要

第 2 節で述べたとおり、計算機ネットワークを構築するにあたり、本稿では特に以下の点を重視する。

- 計算機ネットワーク上のどのマシンの CPU 資源もホームディレクトリとともに活用できること (各ユーザがどのマシンにも slogin 可能であること)
- ユーザ同士が互いにホームディレクトリ上の資源を参照できること
- できる限り高速にファイルシステムにアクセスできること

上記の観点から、第 3 節においては、AFP, SMB, NFS という三つのファイル共有システムの macOS 上での動作を調査した。その結果、複数のユーザが単一ホストに slogin で同時に接続可能であったのは NFS のみであった。そこで、ファイル共有に NFS を採用し、以下のような流れでメッシュ型ホーム共有による分散型計算機ネットワークを構築する。

- (1) ネットワークユーザアカウントを管理するための LDAP サーバを用意する。
- (2) 各ユーザにネットワークユーザアカウントを発行する。ここで、ユーザ i のネットワークユーザアカウントを UID_i とする。
- (3) 各ユーザに 1 台のマシンを割り当てる。ユーザ i にひもづけられたマシンを M_i とする。
- (4) 各ユーザ i ($i = 1, 2, \dots$) について、マシン M_i のローカルストレージ上にネットワークユーザアカウント UID_i 用のホームディレクトリを作成する。
- (5) LDAP サーバと全てのマシンを同一の LAN に接続する。

- (6) 各マシン上に置かれた各ユーザのホームディレクトリを NFS によって相互に共有する。

ここでは、各ユーザは割り当てられた 1 台のマシンをメインマシンとして利用し、メインマシンの計算機資源が不足した場合に、必要に応じてネットワーク上のほかのマシンに slogin することで不足した CPU・メモリ資源などを補うような使い方を想定している。各ユーザにメインマシンを割り当て、メインマシンのローカルストレージ上に対応するユーザのホームディレクトリを作成することで、参照頻度が高いホームディレクトリへのアクセス速度を落とすことなく利用できる。また、メインマシンに他のユーザのホームディレクトリをマウントすることで、いつでも互いのホームディレクトリ上の情報を共有することができる。他のユーザのホームディレクトリを参照するにはネットワークを経由するためアクセス速度は低下するが、ホームディレクトリに比べて参照頻度が低いため、アクセス速度の低下は大きな問題とならない。上記の計算機ネットワークでは、各マシン上に作られた各ユーザのホームディレクトリを NFS によってメッシュ状に相互接続する。そのため、全てのマシンでローカルストレージを共有するための NFS エクスポートの設定、及びほかのマシンが共有するファイルシステム上の領域を利用するための NFS マウントの設定をする必要がある。更には、ボトルネックになるローカル接続の NFS を回避するために第 5.2.2 節のシンボリックリンクを使用する。

このように、上記の流れで構築される計算機ネットワークでは、基本的に全てのマシンが NFS サーバであり、かつ、NFS クライアントである。したがって、これ以降、混乱を避けるために単にサーバとクライアントと書いた場合には、LDAP サーバ及び LDAP サーバに接続するクライアントマシンを指すものとする。それ以外のサーバ、クライアントに言及する場合には、NFS サーバ・NFS クライアントのように、プロトコル・サービス名をサーバやクライアントの前に明記する。

実際に構築したマシン群のネットワークの概略図を図 3 に示す。また、図 4 にマシン群の一部の写真を示す。池口の研究室

では、偉大なる先人に敬意を込めて、数学者、物理学者の名前を各機器のホスト名としている。図3では、bohr というホスト名のマシンに着目し、bohr とほかのマシンとの関係を示している。図3中の矢印の始点がローカルストレージ上の領域を NFS によってエクスポートしているマシンを表し、矢印の終点が始点のマシンから NFS によって共有されたファイル群をマウントしているマシンを表す。なお、図3では1台のマシン (bohr) だけに着目して NFS のファイル共有に関する接続関係を示したが、ほかのマシンについても同様である。また、各マシンのローカルストレージに作成される各ユーザのホームディレクトリは、/Users ディレクトリの中に作成され、この /Users ディレクトリをほかのマシンと NFS で共有する。ほかのマシンで

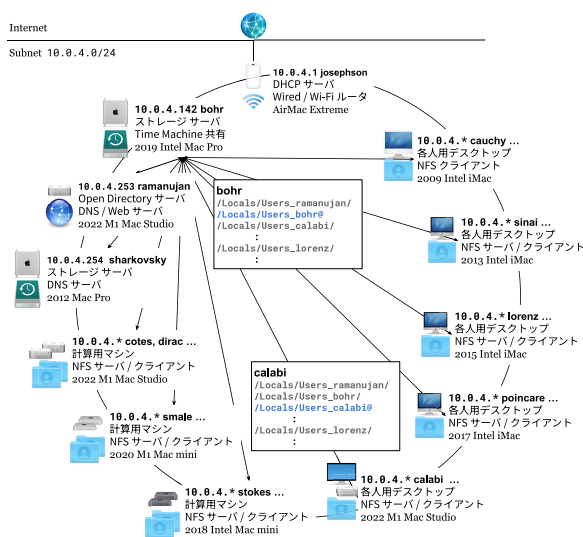


図3 実際に構築した計算機ネットワークの概略図 この図では bohr というホスト名のマシンに着目し、bohr とほかのマシンとの関係を示している。図では省略しているが、総計 55 台のマシンが LAN に接続されている。これらはカレントユーザを有するローカルホームディレクトリがあるマシン群、計算用マシン群、及びサーバ専用マシン群である。図中の IP アドレスに現れる「*」は、2~252 の範囲で各マシンに割り当てられた固有の数値を表す。また、NFS 共有されるディレクトリのパスの末尾に現れる「@」は、シンボリックリンクであることを表す記号である。なお、図中では macOS 標準のシステムアイコンを利用している。

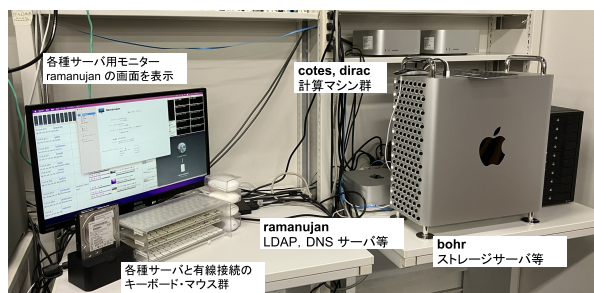


図4 マシン群の一部 (サーバ群、及び、計算用マシン群) なお、サーバ機それぞれにキーボード・マウスを接続しているのは、緊急時に速やかに対応するためである。通常の管理ではリモートログイン、リモートデスクトップによりログインすることで対応できる。

は、/Locals ディレクトリに Users_ から始まり、続く文字列が NFS 共有元のホスト名となるマウントポイントに、共有元の /Users をマウントする。更に、図3では、ルータ (josephson) を用いて 10.0.0.0/16 のネットワークをサブネット化して作成した 10.0.4.0/24 のサブネットに計算機ネットワークを構築している。このサブネット内の IP アドレスが各マシンに付番されている。

図3のように、お互いのホームディレクトリをマシンごとに NFS エクスポートし、お互いにそれらを NFS マウントするので、このネットワークの構造は対称的である。しかし、macOS 10.15 Catalina より前のバージョンの macOS とそれ以降のバージョンの macOS では、システム整合性保護 (SIP: System Integrity Protection) というセキュリティ機構により、システム領域に対するパスの書き方が異なっている。そのため、新旧のバージョンの macOS が混在する環境では、NFS の設定ファイルは互いに等しくはならない点には注意が必要である。

5.2 NFS の設定

5.2.1 セキュリティ・プライバシーの設定

NFS を用いたファイル共有の設定の前に、セキュリティ・プライバシーの設定を行う必要がある。近年の macOS では、プロセスにフォルダやストレージへのアクセス許可を個別に与える必要があり、極めてセキュリティ的に厳しいシステムになっている。ここでは図5のように、アップルメニュー → システム環境設定 → セキュリティとプライバシー → プライバシーの「フルディスクアクセス」にて /sbin/nfsd を追加する必要がある。

macOS 以外の Unix ユーザには非常に面倒な印象を与えると考えられるが、実はそのとおりで、何か問題が発生しているときに一番疑わしいと着目するのがここの設定項目である。ほかの Unix であれば、Solaris Trusted Extensions⁽³⁴⁾、Linux Security Modules⁽³⁵⁾、TrustedBSD⁽³⁶⁾などが、この macOS のセキュリティ機構に相当する。

5.2.2 マウントポイント用ディレクトリ/Locals の作成

NFS を用いてファイル共有する際、ネットワークを介してほかのマシン上にある各ユーザのホームディレクトリをマウントするためのマウントポイント用ディレクトリを作成する必要がある。しかし、macOS 10.15 Catalina 以降のバージョンの macOS では SIP の制約により、ルートディレクトリ下にディレクトリを作成するには次の手順が必要である。まず、以下のファイル /etc/synthetic.conf (List 3) を用意する^(注20)。

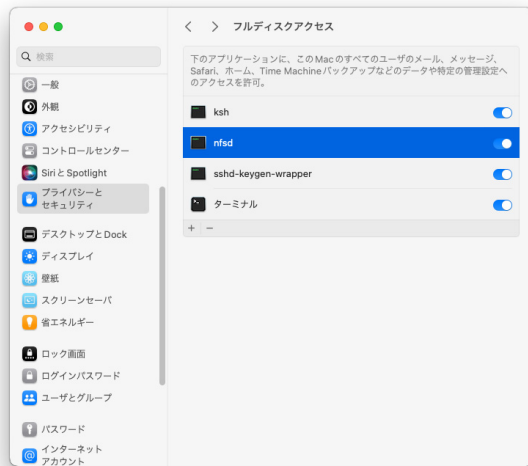
次に、以下のコマンドを実行すればシンボリックリンク /Locals を作成できる。

```
% cd /System/Library/Filesystems/apfs.fs/Contents/Resources/
% sudo ./apfs.util -B # 10.15 Catalina case
% sudo ./apfs.util -t # otherwise
```

(注20)：ここでは、本稿で必要なルートディレクトリにシンボリックリンク /Locals を作成する例を示している。別名のシンボリックリンクが必要であれば、Locals を所望の別名に読み替えた行を /etc/synthetic.conf に追加すればよい。



(a) macOS 12 Monterey での手順: アップルメニュー→システム環境設定→セキュリティとプライバシー→プライバシーの「フルディスクアクセス」にて `/sbin/nfsd` を追加



(b) macOS 14 Sonoma での手順: アップルメニュー→システム設定→プライバシーとセキュリティ→プライバシーの「フルディスクアクセス」にて `/sbin/nfsd` を追加

図 5 `/sbin/nfsd` に「フルディスクアクセス」を許可する手順

List 3 `/etc/synthetic.conf`

```
# 作成されるシンボリックリンク シンボリックリンク元
Locals System/Volumes/Data/Locals
```

一方, macOS 10.15 Catalina より前のバージョンの macOS では以下のコマンドを実行すれば `/Locals` を作成できる.

```
% sudo mkdir /Locals
```

マウントポイント用ディレクトリを既存のディレクトリではなく, `/Locals` のような特別なパス名にするのは理由がある. 例えば, 既存の `/Volumes` の下にマウントポイント用ディレクトリを作成しようとしても, macOS の制約によって正常に動作しない. また, 一般的な `/Network/Servers` の下にマウントポイント用ディレクトリを作成した場合も macOS の挙動と競合す

List 4 `/Library/LaunchDaemons/org.sample.symlink_Locals_Users_here.plist`

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>Label</key>
  <string>org.sample.symlink_Locals_Users_here</string>
  <key>RunAtLoad</key>
  <true/>
  <key>UserName</key>
  <string>root</string>
  <key>ProgramArguments</key>
  <array>
    <string>/bin/ksh</string>
    <string>-c</string>
    <string>
      while [ ! -d /Users ]; do
        sleep 3
      done
      [ -d "/Locals/Users_${hostname -s}" ] || {
        cd /Locals && ln -s ../Users ../Users_${hostname -s}
      }</string>
    </array>
  </dict>
</plist>
```

る. 上記の設定は, このような macOS の挙動との競合を避けるための処置である. 最後に, NFS がローカルストレージのボトルネックになることを回避するためのシンボリックリンクを, 以下により作成する.

```
% cd /Locals && sudo ln -s ../Users ../Users_"${hostname -s}"
```

ただし, macOS のソフトウェアアップデートにより, ルートディレクトリが一新されるため, その都度上記のシンボリックリンクを作成し直す必要がある. これを手動で行うのは現実的ではないため, 自動で行うなどの工夫が必要である. 具体的には, `/Library/LaunchDaemons/` ディレクトリに `org.sample.symlink_Locals_Users_here.plist` というファイル (List 4) を用意し, 以下のコマンドを実行すればよい.

```
% cd /Library/LaunchDaemons/
% sudo launchctl load -w \
  ./org.sample.symlink_Locals_Users_here.plist
```

これらの「マウントポイント用ディレクトリ `/Locals` の作成」と「NFS がローカルストレージのボトルネックになることを回避するためのシンボリックリンクの作成」は, Unix において通常では行わない方策である^(注21). しかし, 通常の NFS 設定ではこのようなボトルネックが存在するので, 本稿の技術は一般の Unix でも有用と思われる.

5.2.3 NFS エクスポートの設定

ほかの多くの Unix と同様に, macOS でも NFS サーバの設定ファイルは `/etc/exports` である. NFS エクスポートのためのファイル `/etc/exports` を List 5 に示す.

(注21): 例えば, Solaris では `/export/home` 配下にホームの実体があるが, NFS を介して自身でも `/home` マウントポイント配下をホームに指定する.

List 5 /etc/exports

```
/System/Volumes/Data/Users -alldirs -maproot=root 127.0.0.1
/System/Volumes/Data/Users -alldirs -maproot=root \
-network=10.0.4.0 -mask=255.255.255.0
```

List 6 /etc/exports (macOS 10.15 Catalina より前の場合)

```
/Users -alldirs -maproot=root 127.0.0.1
/Users -alldirs -maproot=root -network=10.0.4.0 \
-mask=255.255.255.0
```

List 7 /etc/auto_master

```
#
# Automounter master map
#
+auto_master      # Use directory service
#/net             -hosts             -nobrowse,hidefromfinder,nosuid
/home             auto_home          -nobrowse,hidefromfinder
/Network/Servers  -fstab
/-               -static
/-               /etc/auto_users # added by Taiji Yamada on 2022/04/06
```

ただし、macOS 10.15 Catalina より前のバージョンの macOS では SIP 若しくは SIP によるルートディレクトリの保護とは無関係なので、List 6 のようになる。

なお、List 5 及び List 6 の 1 行目は第 5.2.5 節で説明する auto_home の利用が必要となる。

5.2.4 NFS オートマウントの設定

次に、List 7 に NFS オートマウント⁽³⁷⁾用のファイル `/etc/auto_master` を示す。追加したのは最終行のみで、その他はシステム標準のままである。追加した最終行では `/etc/auto_users` (List 8 または List 9) を参照しており、詳細な設定はこのファイルに記述する。

List 8 に、macOS 10.13 High Sierra の julia というホスト名をもつマシンにおける `/etc/auto_users` の例を示す。List 8 はメッシュ型 NFS ホーム共有の主たる設定ファイルなので、実際に動作しているファイルのまま省略せずに載せている。ただし、これは macOS 10.15 Catalina より前のバージョンの macOS の設定ファイルであり、macOS 10.15 Catalina 以降のバージョンの macOS では、行頭のパスを `../Locals/` → `/System/Volumes/Data/./Data/Locals` のように読み替える必要がある。具体的には、macOS 10.15 Catalina では、設定ファイルは List 9 のようになる。

List 8, 9 における「`../`」は筆者らが NFS マウントにおける「.. (ピリオドピリオド) トリック」と呼んでいるものである。このような設定をしない場合、`/Users/$LOGNAME` のローカルアカウントの人数分の全てのエントリごとにマウントポイントを用意する必要があるが、これは実際の運用においては現実的ではない。なお、「`#`」でコメントアウトされている行は、自分自身、及び、計算用マシンであるため NFS エクスポートが不要のマシンである。

さて、List 7, 8, 9 を反映させるためには、以下を行う必要がある。これはほかの Unix における `/usr/libexec/autofs` の

再起動と同義である。

```
% cd /System/Library/LaunchDaemons/
% sudo launchctl stop ./com.apple.autofs.plist
% sudo launchctl start ./com.apple.autofs.plist
```

更に、`auto_users` を書き換えたので、以下も行う必要がある。これは、ほかの Unix でも同様である。

```
% sudo automount -cv
```

このような設定を全てのマシンに施すことで、全てのマシンが NFS で macOS のホームディレクトリルート `/Users` をエクスポートしつつも、自身のマシンではシンボリックリンクであるような一貫した以下のようなパス `/Locals/Users_$(hostname -s)` が構成される。以下に `ls` の実行例を示す^(注22)。なお、以下の実行結果における「`@`」は、シンボリックリンクを表している。

```
ramanujan % ls -F /Locals/
Users_arnold/      Users_feynman/      Users_navier/
Users_bernoulli/   Users_gauss/         Users_pascal/
Users_birkhoff/    Users_gellmann/      Users_poincare/
Users_bohr/        Users_hamilton/      Users_ramanujan@
Users_brahe/       Users_heiles/        Users_schwarzschild/
Users_calabi/      Users_henon/         Users_sharkovsky/
Users_cantor/     Users_hopf/          Users_sinai/
Users_cardano/     Users_huygens/       Users_smale/
Users_chirikov/    Users_jacobi/        Users_stokes/
Users_cotes/       Users_julia/         Users_takens/
Users_dirac/       Users_kolmogorov/    Users_taylor/
Users_duffing/     Users_kovalevskaya/  Users_vanderpol/
Users_esaki/       Users_laplace/       Users_whitney/
Users_euler/       Users_lorenz/        Volumes/
Users_fatou/       Users_lyapunov/
```

以上の操作により、本稿の主題である、図 3 のようなメッシュ型 NFS ホーム共有による分散型計算機ネットワークの構築が実現できる。

5.2.5 auto_home の活用

大学の研究室での主たるユーザである学生はいずれ卒業・修了する。その際、このユーザをメインマシンから切り離すことが必要となる。例えば、卒業したユーザ taiji をメインマシン gellmann から切り離すとして、この場合、gellmann のローカルストレージを最高速に活用するための、シンボリックリンク経由でのホームディレクトリ `/Locals/Users_gellmann/taiji` へのローカルストレージのアクセスの必要性はなくなり、gellmann からストレージサーバ bohr へユーザ taiji のホームディレクトリを回避して、gellmann は別のアカウントに明け渡すことになる。そのようなときに問題となるのが、`NFSHomeDirectory` で設定されたホームディレクトリのパス `/Locals/Users_gellmann/taiji` が卒業・修了したユーザ taiji のホームディレクトリ内の何らかの設定ファイルにて記述されていた場合、これを書き換えなければならないということである。この問題を `auto_home` を活用して解消した例を、List 10 の `~taiji/Sites/.htaccess`^(注23) と

(注22)：ここで `Users_*`以外の `Volumes/` について補足する。本節の本題ではないが、これはほかのマシンの `/Volumes/` のボリュームパスを、サブネット内にて共通のパス名でマウントするために使用している。これは、第 6.4 節の `rsync` によるバックアップ先などとして用いられる。

(注23)：`~taiji` は、本稿では `/Locals/Users_gellmann/taiji`、macOS 標準では `/Users/taiji`、Unix 一般では `/home/taiji` を意味している。

List 8 /etc/auto_users (macOS 10.15 Catalina より前の例)

```
#../Locals/Users_julia -fstype=nfs,rw, sync julia.local:/Users
../Locals/Users_hopf -fstype=nfs,rw, sync hopf.local:/Users
../Locals/Users_schwarzschild -fstype=nfs,rw, sync schwarzschild.local:/Users
../Locals/Users_birkhoff -fstype=nfs,rw, sync birkhoff.local:/System/Volumes/Data/Users
../Locals/Users_euler -fstype=nfs,rw, sync euler.local:/System/Volumes/Data/Users
../Locals/Users_fatou -fstype=nfs,rw, sync fatou.local:/System/Volumes/Data/Users
../Locals/Users_sinai -fstype=nfs,rw, sync sinai.local:/System/Volumes/Data/Users
../Locals/Users_chirikov -fstype=nfs,rw, sync chirikov.local:/System/Volumes/Data/Users
../Locals/Users_heiles -fstype=nfs,rw, sync heiles.local:/System/Volumes/Data/Users
../Locals/Users_lorenz -fstype=nfs,rw, sync lorenz.local:/System/Volumes/Data/Users
../Locals/Users_vanderpol -fstype=nfs,rw, sync vanderpol.local:/System/Volumes/Data/Users
../Locals/Users_whitney -fstype=nfs,rw, sync whitney.local:/System/Volumes/Data/Users
../Locals/Users_cantor -fstype=nfs,rw, sync cantor.local:/System/Volumes/Data/Users
../Locals/Users_jacobi -fstype=nfs,rw, sync jacobi.local:/System/Volumes/Data/Users
../Locals/Users_taylor -fstype=nfs,rw, sync taylor.local:/System/Volumes/Data/Users
../Locals/Users_cardano -fstype=nfs,rw, sync cardano.local:/System/Volumes/Data/Users
../Locals/Users_poincare -fstype=nfs,rw, sync poincare.local:/System/Volumes/Data/Users
../Locals/Users_kovalevskaya -fstype=nfs,rw, sync kovalevskaya.local:/System/Volumes/Data/Users
../Locals/Users_gauss -fstype=nfs,rw, sync gauss.local:/System/Volumes/Data/Users
../Locals/Users_hamilton -fstype=nfs,rw, sync hamilton.local:/System/Volumes/Data/Users
../Locals/Users_pascal -fstype=nfs,rw, sync pascal.local:/System/Volumes/Data/Users
../Locals/Users_brahe -fstype=nfs,rw, sync brahe.local:/System/Volumes/Data/Users
../Locals/Users_bernoulli -fstype=nfs,rw, sync bernoulli.local:/System/Volumes/Data/Users
../Locals/Users_stokes -fstype=nfs,rw, sync stokes.local:/System/Volumes/Data/Users
../Locals/Users_huygens -fstype=nfs,rw, sync huygens.local:/System/Volumes/Data/Users
../Locals/Users_feynman -fstype=nfs,rw, sync feynman.local:/System/Volumes/Data/Users
../Locals/Users_takens -fstype=nfs,rw, sync takens.local:/System/Volumes/Data/Users
../Locals/Users_bohr -fstype=nfs,rw, sync bohr.local:/System/Volumes/Data/Users
../Locals/Users_laplace -fstype=nfs,rw, sync laplace.local:/System/Volumes/Data/Users
../Locals/Users_smale -fstype=nfs,rw, sync smale.local:/System/Volumes/Data/Users
../Locals/Users_navier -fstype=nfs,rw, sync navier.local:/Users
../Locals/Users_henon -fstype=nfs,rw, sync henon.local:/System/Volumes/Data/Users
../Locals/Users_lyapunov -fstype=nfs,rw, sync lyapunov.local:/System/Volumes/Data/Users
../Locals/Users_esaki -fstype=nfs,rw, sync esaki.local:/System/Volumes/Data/Users
../Locals/Users_calabi -fstype=nfs,rw, sync calabi.local:/System/Volumes/Data/Users
../Locals/Users_cotes -fstype=nfs,rw, sync cotes.local:/System/Volumes/Data/Users
../Locals/Users_dirac -fstype=nfs,rw, sync dirac.local:/System/Volumes/Data/Users
../Locals/Users_arnold -fstype=nfs,rw, sync arnold.local:/System/Volumes/Data/Users
../Locals/Users_duffing -fstype=nfs,rw, sync duffing.local:/Users
../Locals/Users_ramanujan -fstype=nfs,rw, sync ramanujan.local:/System/Volumes/Data/Users
../Locals/Users_sharkovsky -fstype=nfs,rw, sync sharkovsky.local:/Users
../Locals/Users_gellmann -fstype=nfs,rw, sync gellmann.local:/System/Volumes/Data/Users
#../Locals/Users_cauchy -fstype=nfs,rw, sync cauchy.local:/Users
#../Locals/Users_graham -fstype=nfs,rw, sync graham.local:/Users
#../Locals/Users_landau -fstype=nfs,rw, sync landau.local:/Users
#../Locals/Users_wilson -fstype=nfs,rw, sync wilson.local:/Users
#../Locals/Users_hilbert -fstype=nfs,rw, sync hilbert.local:/Users
#../Locals/Users_rossler -fstype=nfs,rw, sync rossler.local:/Users
#../Locals/Users_turing -fstype=nfs,rw, sync turing.local:/Users
#../Locals/Users_weierstrass -fstype=nfs,rw, sync weierstrass.local:/Users
#../Locals/Users_feigenbaum -fstype=nfs,rw, sync feigenbaum.local:/Users
#../Locals/Users_kepler -fstype=nfs,rw, sync kepler.local:/Users
#../Locals/Users_newton -fstype=nfs,rw, sync newton.local:/Users
#../Locals/Users_peano -fstype=nfs,rw, sync peano.local:/Users
#../Locals/Users_planck -fstype=nfs,rw, sync planck.local:/System/Volumes/Data/Users
```

List 9 /etc/auto_users (macOS 10.15 Catalina 以降の例)

```
#/System/Volumes/Data/./Data/Locals/Users_fatou -fstype=nfs,rw, sync fatou.local:/System/Volumes/Data/Users
/System/Volumes/Data/./Data/Locals/Users_hopf -fstype=nfs,rw, sync hopf.local:/Users
/System/Volumes/Data/./Data/Locals/Users_schwarzschild -fstype=nfs,rw, sync schwarzschild.local:/Users
/System/Volumes/Data/./Data/Locals/Users_birkhoff -fstype=nfs,rw, sync birkhoff.local:/System/Volumes/Data/Users
/System/Volumes/Data/./Data/Locals/Users_euler -fstype=nfs,rw, sync euler.local:/System/Volumes/Data/Users
/System/Volumes/Data/./Data/Locals/Users_sinai -fstype=nfs,rw, sync sinai.local:/System/Volumes/Data/Users
/System/Volumes/Data/./Data/Locals/Users_julia -fstype=nfs,rw, sync julia.local:/Users
/System/Volumes/Data/./Data/Locals/Users_chirikov -fstype=nfs,rw, sync chirikov.local:/System/Volumes/Data/Users
:
#/System/Volumes/Data/./Data/Locals/Users_rossler -fstype=nfs,rw, sync rossler.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_turing -fstype=nfs,rw, sync turing.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_weierstrass -fstype=nfs,rw, sync weierstrass.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_feigenbaum -fstype=nfs,rw, sync feigenbaum.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_kepler -fstype=nfs,rw, sync kepler.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_newton -fstype=nfs,rw, sync newton.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_peano -fstype=nfs,rw, sync peano.local:/Users
#/System/Volumes/Data/./Data/Locals/Users_planck -fstype=nfs,rw, sync planck.local:/System/Volumes/Data/Users
```

List 10 ~taiji/Sites/.htaccess の例

```
AuthType Basic
AuthName "taiji member only"
AuthUserFile /home/taiji/etc/apache2/.htpasswd
Order deny,allow
Deny from all
Allow from 10.0.4.0/22
Satisfy any
```

List 11 /usr/local/libexec/od_user_home_dirs

```
#!/bin/ksh
#
# od_user_home_dirs - yet another /usr/libexec/od_user_homes for NFS
#
# Written by Jun Takahashi and Taiji Yamada <taiji@aihara.co.jp>
#
# usage:
#   % od_user_home_dirs user
#
# description:
#
#   In the 'Comment' key for "$1" registration of the 'Users'
#   record at macOS Server.app Open Directory, write the NFS
#   server path of AUTOHOME for /etc/auto_home as follows:
#
#       :
#       AUTOHOME=nfs://server:/path_to_$1
#       :
#
h="$(dscl /LDAPv3/Ramujan.local -read /Users/"$1" Comment 2> /dev/null |
sed -E -e '1{
  /~Comment: .*/{
    s/~Comment: (.*)$/\1/
  }
}' -ne 's/~ *AUTOHOME=(.*)$/\1/p')"
[ "$h" = '' ] && exit 1
echo "$h"
exit 0
```

して示す。

List 10 は、ユーザ taiji のホームページにアクセス制限をかけるために用いる .htaccess ファイルである。問題となるのは、AuthUserFile 行の設定にて、List 10 とは異なり、この行を仮に

```
AuthUserFile /Locals/Users_gellmann/taiji/etc/apache2/.htpasswd
```

のようにユーザレベルでマシン名とユーザ名をひも付けしてしまう場合である。このような場合、卒業・修了後に taiji のホームディレクトリを gellmann 以外の別のマシンに退避すると、この設定では意図したとおりに動作しなくなる。このような場合、卒業・修了した全てのユーザの .htaccess ファイル内のホームディレクトリのパスの変更が必要となるが、これらのファイルを管理者が一つ一つ編集するなどには現実的でない。

そこで、このような事態を起こさないために auto_home を利用する。これにより、卒業・修了するユーザのホームディレクトリでのファイルの変更をせずともよくなる。

本来、auto_home の仕組みは macOS に備わっているが、機能していない。これは、/etc/auto_home から使用される標準の /usr/libexec/od_user_homes が長らく保守されていないためと思われる。そこで、NFS 専用の代替となる独自の /usr/local/libexec/od_user_home_dirs を開発した (List 11 参照)。

List 12 auto_home

```
#
# Automounter map for /home
#
+auto_home      # Use directory service
#
# Get /home records synthesized from user records
#
#+/usr/libexec/od_user_homes
+/usr/local/libexec/od_user_home_dirs
```

また、/etc/auto_home を List 12 のように書き換える。設定後は、以下のように使用中の全てのアカウントがオートマウントされている。

```
% ls -F /home/
junt/   sima/   tohru/
```

もしユーザ taiji が未使用なら、ls /home/taiji とするとそれがオートマウントされ、以下の実行例のように taiji/ ディレクトリが現れる。

```
% ls -F /home/taiji
Desktop/   Library/   Pictures/   etc/
Documents/ Movies/    Public/
Downloads/ Music/     Sites/
% ls -F /home/
junt/   sima/   taiji/   tohru/
```

6. メッシュ型 NFS ホーム共有による分散型計算機ネットワークの安定運用のための技術

前節で構築したメッシュ型 NFS ホーム共有による分散型計算機ネットワークでは、macOS に備わっている Bonjour の機能によってそのままでも運用可能である。Bonjour とはネットワーク上のデバイスの設定を簡便にするために Apple が開発した Zeroconf (Zero-configuration networking) ^{(38), (39)} の一つであり、事実上の標準である。Bonjour の mDNS (multicast DNS) ⁽⁴⁰⁾ によってネットワーク上の検出可能なデバイスが識別される。これにより、DNS サーバが存在しない場合でもホスト名の後ろに .local というサフィックスを付けた “ホスト名.local” という名称を使って各マシンに接続することができる ^{(注24) (41)}。本節では、mDNS と DNS サーバを共存させることでメッシュ型 NFS ホーム共有による計算機ネットワークの安定性を向上させる方法を紹介する。また、ユーザ ID の付番方法やバックアップに関する注意事項についても述べる。

6.1 DNS ⁽⁴²⁾, ⁽⁴³⁾ 及び mDNS における IP アドレス・ホスト名の取得方法

本稿で提案するメッシュ型 NFS ホーム共有による分散型計算

(注24)：一般的には .local のような特殊用途ドメイン名を使用せずに組織の FQDN を利用することが望ましい ⁽⁴¹⁾ が、本稿で提案するメッシュ型 NFS ホーム共有による分散型計算機ネットワークは研究室内で完全に閉じたサブネットであるので、local で運用することには問題ない。

機ネットワークでは、サブネット向けに DNS サーバ (MacPorts bind9) を立ち上げて、かつ、各マシンの IP アドレスが変化しないように DHCP サーバを適切に管理する方式を採用する。具体的には、クライアントマシンに設定する Bonjour 名は DNS サーバの 10.0.4.0/24 の空間の A レコードの IP アドレスと同様に名前を定める。更に、本稿で提案するシステムでは、DHCP サーバが、そのマシンの IP アドレスはそのマシンの LAN インタフェースの MAC アドレスにリースするように厳格な管理ポリシーを採用する。その上で、各マシンにおいて固定アドレスを手動で個別に設定せずに、DNS・DHCP サーバにおいて MAC アドレス・IP アドレス・ホスト名を一元管理することによって、NFS のような Unix サービスの適切な運用を実現する。これに加えて、mDNS のようなモダンなサービスの恩恵を同時に受けられるように、Bonjour の mDNS で用いられる特殊なトップレベルドメインである .local をそのままプライベート空間であるサブネットのトップレベルドメインとして DNS を設定する。DNS と mDNS の併用は、適切に管理されていれば、固定アドレスのメリットと mDNS によるサービス検出の双方のメリットを享受できる。具体的に、ホスト名または IP アドレスの問い合わせ方法を用いてこのメリットを紹介する。

6.1.1 ホスト名 (DNS) ↔ IP アドレスの取得 – host(1)

サブネットについて、まず、ホスト名から IP アドレスを取得 (正引き) する場合、以下のようにする。

```
% host ramanujan.local
ramanujan.local has address 10.0.4.253
```

また、IP アドレスからホスト名を取得 (逆引き) する場合、以下のようにする。

```
% host 10.0.4.253
253.4.0.10.in-addr.arpa domain name pointer ramanujan.local.
```

6.1.2 ホスト名 (DNS) ↔ IP アドレスの取得 – dig(1)

macOS 標準の host コマンドではポート番号を指定した mDNS への問い合わせは実現できないので、dig コマンドを用いる方法を紹介する。なお本節では、dig(1) の出力は「ANSWER SECTION」のみ示している。

サブネットについて、まずは正引きの場合、以下ようになる。

```
% dig -q ramanujan.local

;; ANSWER SECTION:
ramanujan.local. 10800 IN A 10.0.4.253
```

また、逆引きでは、以下ようになる。

```
% dig -x 10.0.4.253

;; ANSWER SECTION:
253.4.0.10.in-addr.arpa. 10800 IN PTR ramanujan.local.
```

以上の例は、通常の DNS サーバに対するホスト名または IP アドレスの問い合わせであるが、次に mDNS への問い合わせ方法を紹介する。

6.1.3 ホスト名 (mDNS) ↔ IP アドレスの取得 – dig(1)

サブネットについて、まずは正引きは以下ようになる。

```
% dig @224.0.0.251 -p 5353 -q Ramanujan.local

;; ANSWER SECTION:
Ramanujan.local. 10 IN A 10.0.4.253

;; ADDITIONAL SECTION:
Ramanujan.local. 10 IN AAAA fe80::c9:dace:48bd:65fe
```

また、逆引きでは以下となる。

```
% dig @224.0.0.251 -p 5353 -x 10.0.4.253

;; ANSWER SECTION:
253.4.0.10.in-addr.arpa. 10 IN PTR Ramanujan.local.

;; ADDITIONAL SECTION:
Ramanujan._device-info._tcp.local. 10 \
IN TXT "model=Mac13,1" "osxvers=21" "icolor=0"
```

このように、ポート番号 5353、マルチキャストアドレス 224.0.0.251 を dig コマンドに明示的に与えることで macOS にて既定で有効になっている mDNS への問い合わせができる。なお本節では、dig(1) の出力は「ANSWER SECTION」、「ADDITIONAL SECTION」のみ示している。

6.1.4 ホスト名 (mDNS) → IP アドレスの取得 – dns-sd(1)

さて、具体的にどのように問い合わせがなされるのかを mDNS のサービス検出コマンド dns-sd(1) で紹介する。10.0.4.0/24 のみのサブネットに接続しているマシンの例として、cotes への正引きは、以下となる。

```
% dns-sd -G v4 cotes.local
DATE: ---Mon 27 Nov 2023---
16:29:55.947 ...STARTING...
Timestamp IF Hostname Address TTL
16:29:55.950 0 cotes.local. 10.0.4.150 4502
16:29:56.115 26 cotes.local. 10.0.4.150 120
^C
```

一方、10.0.4.0/24 と 10.0.6.0/24 の両方のサブネットに接続しているマシン ramanujan への正引きは、以下となる。

```
% dns-sd -G v4 Ramanujan.local
DATE: ---Wed 09 Aug 2023---
19:13:20.736 ...STARTING...
Timestamp if Hostname Address TTL
19:13:20.737 6 Ramanujan.local. 10.0.4.253 120
19:13:20.737 7 Ramanujan.local. 10.0.6.253 120
19:13:20.737 0 Ramanujan.local. 10.0.4.253 4502
^C
```

なお、dns-sd は直ちにプロセス終了するコマンドではないので、上記例では、^(注25) ^C キーの SIGINT シグナルで終了させている。

これを見ると、二つのサブネットの片方の IP アドレスしか名前では到達できないという mDNS のデメリットが露呈していることが分かる。ホストから 10.0.4.253 と 10.0.6.253 のいず

(注25) : ^C は、control キーを押しながら C キーを押すことを表す。

れかに選択的に到達するには、Ramanujan.local^(注26)という名前では、ネットワークインタフェースの優先順位を変更するか、10.0.4.0/24 または 10.0.6.0/24 を明示的に始点アドレスにバインドする必要がある。しかし、コマンドやアプリケーションによってはバインドする機会がない場合も大いにあり得る。さもなくば、IP アドレスを指定するしかなく不便である。しかし、これは DNS サーバに別名を登録してしまえば上記の問題を回避できる。

6.1.5 ホスト名 (DNS) ↔ IP アドレスの取得 – host(1)

ほかのサブネットについて、まずは正引きの場合、以下となる。

```
% host lovasz.local
lovasz.local has address 10.0.6.253
```

また、逆引きでは以下となる。

```
% host 10.0.6.253
253.6.0.10.in-addr.arpa domain name pointer lovasz.local.
```

以上のように IP アドレスではなく別名 lovasz.local により Ramanujan.local へ選択的に到達可能にしておけば安心である。

6.1.6 他サブネットのホスト名 (mDNS) ↔ IP アドレスの取得 – dig(1)

明示的にはほかのサブネットにバインドする場合、つまり、ネットワークインタフェースの優先順位をそのサブネットに上げた場合、元々の Bonjour 名 Ramanujan.local でホスト名または IP アドレスの問い合わせが適切に行うことができるかを確認しよう。なお本節では、dig(1) の出力は「ANSWER SECTION」, 「ADDITIONAL SECTION」のみ示している。

まずは正引きは、以下となる。

```
% dig @224.0.0.251 -p 5353 -b 10.0.6.112 -q Ramanujan.local

;; ANSWER SECTION:
Ramanujan.local. 10 IN A 10.0.6.253

;; ADDITIONAL SECTION:
Ramanujan.local. 10 IN AAAA fe80::1868:59ae:e69c:2a77
```

また、逆引きでは以下となる。

```
% dig @224.0.0.251 -p 5353 -b 10.0.6.112 -x 10.0.6.253

;; ANSWER SECTION:
253.6.0.10.in-addr.arpa. 10 IN PTR Ramanujan.local.

;; ADDITIONAL SECTION:
Ramanujan._device-info._tcp.local. 10 \
IN TXT "model=Mac13,1" "osxvers=21" "icolor=0"
```

このように始点アドレスを -b オプションで明示すれば、他サブネットにおける元々の Bonjour 名でのホスト名または IP アドレスの問い合わせにも対応しており、DNS と mDNS のいず

(注26)：本稿において、Ramanujan.local, ramanujan.local のように、同じマシンでもホスト名の最初の文字が大文字の場合と小文字の場合があるが、前者は Bonjour 名、後者は DNS 名である。なお、大文字と小文字は区別されないが、DNS サーバダウン時には mDNS により Bonjour 名で表示され、区別できるというメリットがある。

れのメリットも享受できる。ただし、各マシンの IP アドレスと DNS の管理を、可能であれば DHCP により、MAC アドレスの管理とともに、一元的に適切に行っていることが重要である。本システムで DNS を併用しているのは、手前勝手なホスト名を放置したままにせず、ある一定のルールに従ったホスト名とすることでほかのマシンにもアクセスしやすくするためである。

6.2 mDNS によるサービス検出⁽⁴⁴⁾

mDNS の役割は前節のホスト検索のみならず、ホストが提供するサービス検出でもある。そこで、mDNS を利用する UI の背後で、どのようにサービス検出がなされているかを紹介する。ただし、コマンドの出力結果をそのまま掲載すると紙面が煩雑になるので、ここでは、List 13 に示すシェルスクリプト⁽³³⁾のように、sed(1) により整形している。更に、前述のように dns-sd はそのままではプロセス終了しないので、シェルスクリプトでプロセス終了する dns-sd のラッパーコマンドを List 13 に示す DNS-SD_kill.sh というファイル名で用意しておく。なお、「"\$@"」はコマンド名と引数、または、シェル関数名と引数の、全ての文字列の並びを指す。

このラッパーコマンド DNS-SD_kill.sh を以下のように使用するとサブネットにて提供されているサービスの一覧を得ることができる。

```
%. /DNS-SD_kill.sh -B _services._dns-sd._udp local
:
_tcp.local.      _printer
:
_tcp.local.      _scanner
:
_tcp.local.      _ssh
:
```

得られたサービスの詳細を表示するには以下のように DNS-SD_kill.sh を使用する。

```
%. /DNS-SD_kill.sh -B _printer._tcp local.
_printer._tcp.  Canon MF741C/743C
_printer._tcp.  RICOH P C6010
_printer._tcp.  RICOH SP C261SF
```

```
%. /DNS-SD_kill.sh -B _scanner._tcp local.
_scanner._tcp.  Canon MF741C/743C
_scanner._tcp.  RICOH SP C261SF
```

List 13 DNS-SD_kill.sh

```
#!/bin/ksh      # POSIX.2 準拠のシェルスクリプト
exec_kill()     # シェル関数
{
    "$@" &      # 関数の引数をバックグラウンドでコール
    sleep 5     # 5 秒間のウェイト
    kill %1     # バックグラウンドプロセスの kill
}
exec_kill dns-sd "$@" |
sed -E '1,4d;s/^( ?[^\ ]+ )>{6}(.+)\$/2->\3/;\\"/>
sort | uniq     # → は Tab
```

List 14 /var/named/db.local

```
; 正引きデータベースファイル
local.                10800 IN SOA   local.
                        admin.local. (
                        2023080300    ; Serial
                        3600          ; Refresh
                        900           ; Retry
                        1209600       ; Expire
                        86400)        ; Minimum
                        10800 IN NS   ramanujan.local.
apollonius.local.     10800 IN A    10.0.4.0
josephson.local.      10800 IN A    10.0.4.1
;
ramanujan.local.      10800 IN A    10.0.4.253
sharkovsky.local.     10800 IN A    10.0.4.254
szabo.local.          10800 IN A    10.0.4.255
```

List 15 /var/named/db.4.0.10.in-addr.arpa

```
; 逆引きデータベースファイル
4.0.10.in-addr.arpa.  10800 IN SOA   4.0.10.in-addr.arpa.
                        admin.4.0.10.in-addr.arpa. (
                        2023080300    ; Serial
                        3600          ; Refresh
                        900           ; Retry
                        1209600       ; Expire
                        86400)        ; Minimum
                        10800 IN NS   ramanujan.local.
0.4.0.10.in-addr.arpa. 10800 IN PTR  apollonius.local.
1.4.0.10.in-addr.arpa. 10800 IN PTR  josephson.local.
;
```

```
% ./DNS-SD_kill.sh -B _ssh._tcp local.
_ssh._tcp.      Arnold
_ssh._tcp.      Calabi
;
_ssh._tcp.      Vanderpol
_ssh._tcp.      Whitney
```

上記の mDNS の情報から、プリンタ `_printer._tcp.`、スキャナ `_scanner._tcp.` の検出が可能なが分かる。更には、ssh `_ssh._tcp.` の情報が得られていることから、DNS サーバがなくても、例えば `ssh Whitney.local` とすることにより `Whitney.local` というマシンにリモートログインが可能なが分かる。

なお、Microsoft Windows 10 以降でも mDNS が使用可能となっている。また、BSD 系及び GNU Linux などの Unix ではオープンソース Avahi⁽⁴⁵⁾実装 (GNU LGPL: Lesser General Public License) が統合されている。

6.3 DNS の設定

さて、DNS サーバ実装の一つ bind9 の常駐プログラムである `named` の設定に最低限必要なファイル `/var/named/db.local`、`/var/named/db.4.0.10.in-addr.arpa`、`/var/named/localhost.zone`、`/var/named/named.local`、`/etc/named/named.conf` を List 14~18 に示す。これらは、一般的かつ最小限の設定であるが、サブネット向け DNS サーバとしては十分である。

ルートサーバ定義ファイル `/var/named/named.ca` がこのほかに必要となるが、最新の <https://www.internic.net/domain/named.root> の内容をコピーして用いる。

List 16 /var/named/localhost.zone

```
; ローカルホストの正引きデータベースファイル
localhost.        86400 IN SOA   localhost.
                  root.localhost. (
                  1997022700    ; Serial
                  10800        ; Refresh
                  900          ; Retry
                  604800       ; Expire
                  86400)        ; Minimum
                  86400 IN NS   localhost.
                  86400 IN A    127.0.0.1
```

List 17 /var/named/named.local

```
; ローカルホストの逆引きデータベースファイル
@      IN      SOA      localhost.
      root.localhost. (
      1997022700    ; Serial
      28800        ; Refresh
      14400        ; Retry
      3600000       ; Expire
      86400)        ; Minimum
1      IN      NS       localhost.
1      IN      PTR      localhost.
```

List 18 /etc/named/named.conf

```
# DNS サーバの基本設定ファイル(最低限の項目のみ抜粋)
include "/var/named/rndc.key";
options {
    directory "/var/named";
    allow-transfer {
        none;
    };
    forwarders {
        133.31.57.13;
        133.31.57.14;
    };
};
view "com.apple.ServerAdmin.DNS.public" {
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
    };
    zone "4.0.10.in-addr.arpa" IN {
        type master;
        file "db.4.0.10.in-addr.arpa";
        allow-transfer { none; };
        allow-update { none; };
    };
    zone "local" IN {
        type master;
        file "db.local";
        allow-transfer { none; };
        allow-update { none; };
    };
    zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
    };
};
```

MacPorts の bind9 をインストールした場合は、上記の `/var`、`/etc` をそれぞれ `/opt/local/var`、`/opt/local/etc` に読み替える。なお、これらの設定ファイルのオーナーは `named` にしておく必要がある。また、MacPorts bind9 DNS サーバの起動は、以下のコマンドを実行すればよい。

```
% sudo port load bind9
```

```
% rsync -au --delete --no-D /Locals/Users_gellmann/taiji/ \
/Locals/Volumes/Teachers/taiji/
```

6.4 バックアップ体制について

macOS では Time Machine というバックアップシステムが提供されている。Time Machine は、ストレージサーバが SMB/AFP プロトコルを介して各マシンにバックアップストレージを提供することも可能である。著者の 1 人池口が主宰する研究室においても、特にカレントユーザが主に使用する各クライアントマシンは、ストレージサーバが提供するバックアップストレージに Time Machine を利用してバックアップをとっている。

しかし、これはシステム全体のバックアップなので、例えば、カレントユーザのホームにトラブルがあった場合の復旧に時間がかかる。このような場合、各ユーザのホームディレクトリのバックアップは `rsync(1)` を LaunchDaemon または `crontab(1)` を用いて行えばよい。その際、`rsync(1)` による日々のバックアップ先を、卒業・修了した後の退避先となるように運用すれば便利である。

具体的には、以下のコマンドに相当する処理を管理者権限で、必要なアカウントごとに行うことになる。以下はユーザ taiji の例である。

7. サブネットと全てのマシンの状態の可視化

これだけの台数のマシンを管理していると、稀に不調なマシンが表れる。その場合、`slogin` により CUI ベースで様子を調べることになる。その際、最初に調べるべき手掛かりを掴みやすくするため、全てのマシンの状態を Web ベースで可視化しておくことで管理者の負担を軽減することが可能となる。これに加えて、どのマシンの CPU 資源が空いているなどの情報も表示すれば、管理者以外の一般ユーザにも役立つことが期待される。また、ローカルストレージの容量が圧迫していれば、ユーザも困っているだろうとの予想も付きやすい。このような目的のために、全てのマシンの状態を可視化する Web ページを作成した。実際のページの一部のスクリーンショットを図 6 に示す。

この可視化によって得られる情報は、まず `arp(1)` コマンドによって接続性の確認が行われる。それにより、管理対象でありながら、サブネットから離脱しているマシンはグレイアウトされる。また、管理下でないマシンが接続されている場合は、IP アドレスと MAC アドレスなどが印字される。

つまり、正常にサブネットに接続済みで、かつ、mDNS で素

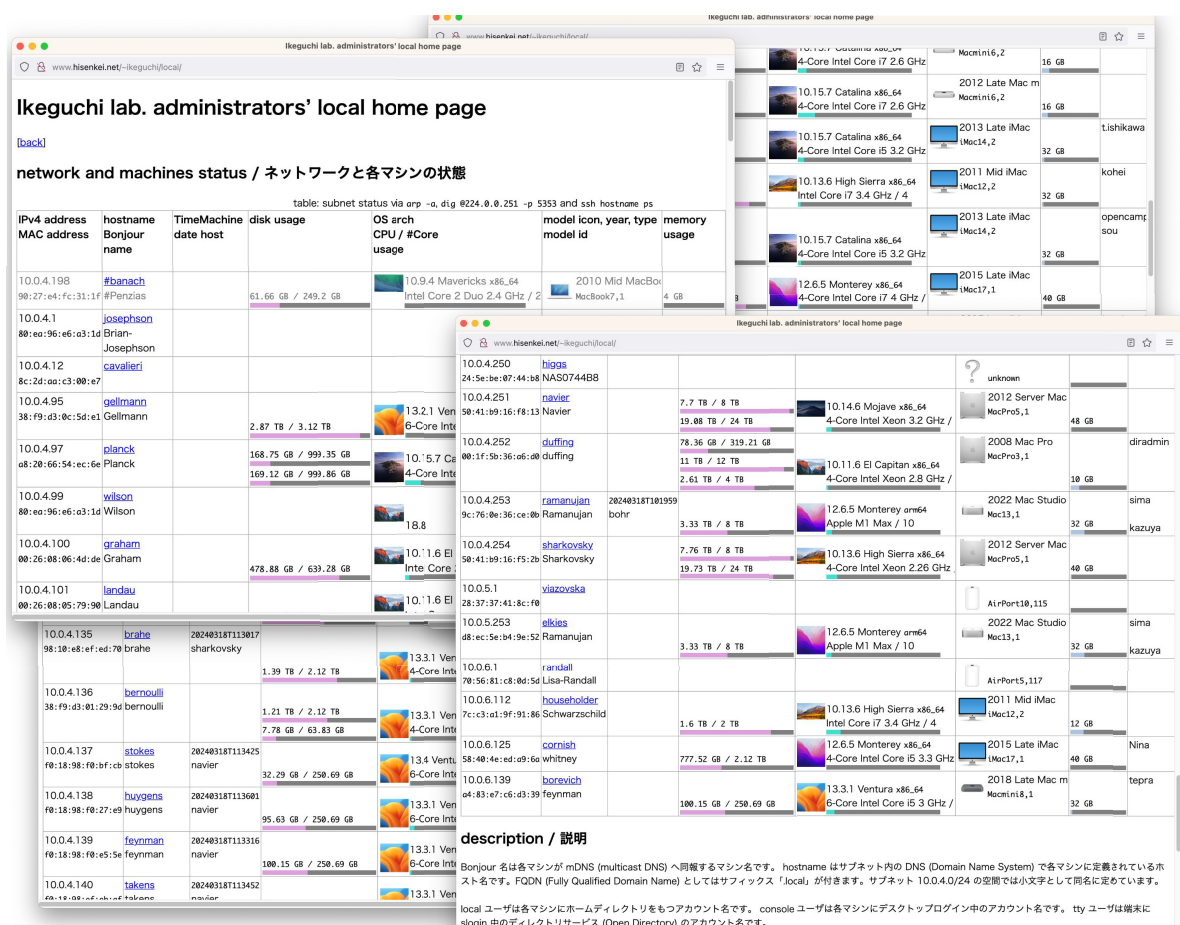


図 6 サブネットと各マシンの状態を可視化するプライベートサイトの様子の一部 図中では macOS 標準のシステムアイコン及び壁紙画像を利用している。

性を報告するホストであること、更に、管理下にあるマシンの CPU 資源、メモリ空間、ストレージの使用状況など、利用者と管理者に有用な情報が可視化される^{(注27) (46)~(48)}。

8. ま と め

本稿では、macOS にてメッシュ型 NFS ホーム共有による分散型計算機ネットワークの構築について解説した。これは Unix における NFS のようなレガシーな技術とモダンな技術を融合するものであり、更に、macOS で次々と導入される新たな方針と競合しないように配慮した技術でもある^(注28)。なお、マシン自身との NFS プロトコルのアクセス速度が十分に高速であれば、第 5.2.2 節で述べたようなシンボリックリンクの方策は不要である。しかし、NFS を介すと、NVMe SSD の 1/5~1/10、SATA HDD の約 1/2 のアクセス速度になる (表 7)。このことから、本稿で紹介した「ピリオドピリオドトリック」と「シンボリックリンク」は有効であることが分かる。

また、本稿では触れなかったが、数十台ものマシンの設定と管理を手動で行うのは非効率的であり、実際には、ssh(1) とシェルスクリプト⁽³³⁾を用いて設定と管理を自動的に行っている。ただし、macOS 10.14 Mojave からは GUI を介さないと変更が不可能な設定も存在するようになっていく。このような場合は、リモートデスクトップにより各マシンにログインし、手動で設定していくほかに方法はない。更には、SIP の解除などは、実機を面前に OS の「復旧モード」からでないと実施不可能である。このような部分はレガシーな Unix とは勝手が異なっている。しかし、このようなモダンな側面も、セキュリティという観点からはメリットが上回ると考えることができるであろう。

さて、第 3.2~3.3 節で NFS によるリモートのホームディレクトリへのデスクトップログインが困難であったことを報告した。これは、デスクトップログインプロセスが NFS に対応していないだけなので、NFS マウントを自前で行うことで、あたかもローカルにホームがあるかのようにデスクトップログインを遂行させればよいと思われるかもしれない。

実は、筆者らは、考え得る様々な方法で NFS によるリモートホームへのデスクトップログインを試みたが、一つも成功していない。これは、AFP と SMB 以外ではホームディレクトリは /Users/\$LOGNAME に固定するという仕様となっていると推測される。実際、AFP と SMB ではなく、NFS で強制的に手動で /Users/\$LOGNAME にマウントすると、macOS 10.14 Mojave まではリモートホーム・デスクトップログインは成功した。しかし、macOS 10.15 Catalina 以降はそれでも強制電源断による再起動が必要となった。これらより、現状ではリモートのホームディレクトリへのデスクトップログインは実運用としては不

可能であると結論づけている。

最後に、Unix においては、管理者も含めて利用者は GUI のオペレーションを用いずに、優れたエディタとコマンドラインさえあれば、一般的な作業・システム管理作業を CUI で効率的に実現できる^{(24)~(27)}。したがって、slogin であれば問題はないのであるが、GUI での一時的な利用が有用な場合もあるので、本稿が macOS の関係者の目に触れて、SMB、NFS によるリモートホームへのデスクトップログインの公式なサポートにつながることも願っている。

なお、本稿に関するサポートサイトを https://www.aihara.co.jp/rdteam/ieice_fr-2024.ja/ にて公開しているので、こちらも参考にされたい。

謝辞 本稿の執筆に際して、サーバ及びクライアントマシンの設定・管理のお手伝いを頂いた、藤田実沙氏、對馬帆南氏、金丸志生氏、澤田和弥氏をはじめとした東京理科大学工学部情報工学科池口研究室の管理者及びメンバーに感謝いたします。

文 献

- (1) Sun Microsystems, “NFS: Network File System Protocol Specification,” Internet Engineering Task Force (IETF), RFC 1094, 1989.
- (2) B. Callaghan, B. Pawlowski, P. Staubach, and Sun Microsystems, “NFS Version 3 Protocol Specification,” Internet Engineering Task Force (IETF), RFC 1813, 1995.
- (3) Sun Microsystems, “RPC: Remote Procedure Call Protocol Specification,” Internet Engineering Task Force (IETF), RFC 1050, 1988.
- (4) R. Thurlow and Sun Microsystems, “RPC: Remote Procedure Call Protocol Specification Version 2,” Internet Engineering Task Force (IETF), RFC 5531, 2009.
- (5) 増月孝信, “NFS,” Solaris 2.2 技術解説, pp.167~176, ソフト・リサーチ・センター, 東京, 1993.
- (6) T. Haynes, Primary Data, D. Noveck, and Dell, “Network File System (NFS) Version 4 Protocol,” Internet Engineering Task Force (IETF), RFC 7530, 2015.
- (7) D. Noveck, NetApp, C. Lever, and ORACLE, “Network File System (NFS) Version 4 Minor Version 1 Protocol,” Internet Engineering Task Force (IETF), RFC 8881, 2020.
- (8) T. Haynes and Primary Data, “Network File System (NFS) Version 4 Minor Version 2 Protocol,” Internet Engineering Task Force (IETF), RFC 7862, 2016.
- (9) 藤田 昭人, “Unix 考古学 Truth of the Legend,” KADOKAWA, 東京, 2016.
- (10) Wikipedia, “UNIX System V,” https://en.wikipedia.org/wiki/UNIX_System_V, 2023 閲覧.
- (11) Wikipedia, “POSIX,” <https://en.wikipedia.org/wiki/POSIX>, Foundation, 2023 閲覧.
- (12) The Open Group Brand Register, “UNIX 03 – Mac OS X Version 10.5 Leopard by Apple Inc.,” <https://www.opengroup.org/openbrand/register/brand3555.htm>, 2007.
- (13) IEEE and The Open Group, “IEEE Std 1003.1-2017 Base Definitions,” <https://pubs.opengroup.org/onlinepubs/9699919799.2018edition/basedefs/toc.html>, 2001–2018.
- (14) IEEE and The Open Group, “IEEE Std 1003.1-2017 System Interfaces,” <https://pubs.opengroup.org/onlinepubs/9699919799.2018edition/functions/toc.html>, 2001–2018.
- (15) IEEE and The Open Group, “IEEE Std 1003.1-2017 Shell & Utilities,” <https://pubs.opengroup.org/>

(注27)：この可視化は HTML⁽⁴⁶⁾、ECMAScript (JavaScript)⁽⁴⁷⁾、CGI⁽⁴⁸⁾などとアクセス制御の組み合わせで実現している。その詳細は本稿の主題ではないのでここでは割愛する。

(注28)：本稿では研究室内のネットワークについて述べてきたが、研究室外からは CUI、GUI とともに slogin 及び、その ssh ポートフォワーディングによって利用することができる。また、本稿の主題ではないが、外部のサービスであるクラウドなどを併用することも可能である。

- onlinepubs/9699919799.2018edition/utilities/toc.html, 2001–2018.
- (16) IEEE and The Open Group, “IEEE Std 1003.1-2017 Rationale,” <https://pubs.opengroup.org/onlinepubs/9699919799.2018edition/xrat/toc.html>, 2001–2018.
- (17) Apple Inc., “AppleTalk Filing Protocol (AFP),” <https://developer.apple.com/library/archive/documentation/mac/pdf/Networking/AFP.pdf>, 2023 閲覧.
- (18) Apple Inc., “macOS Server 5.7.1 以降について,” <https://support.apple.com/ja-jp/101601>, 2023.
- (19) OpenLDAP Foundation, “OpenLDAP,” <https://www.openldap.org/>, 2023 閲覧.
- (20) Microsoft Corp., “Active Directory Overview,” <https://learn.microsoft.com/en-us/troubleshoot/windows-server/identity/active-directory-overview>, 2023 閲覧.
- (21) Oracle and/or its affiliates, “About the Network Information Service,” https://docs.oracle.com/cd/E37838_01/html/E61011/anis1-25461.html, 2020.
- (22) J. Winsor, “NIS+環境の概要,” Solaris 上級システム管理, 日本サン・マイクロシステムズ (監訳), pp.137–161, アスキー, 東京, 1995.
- (23) Wikipedia, “Server Message Block,” https://en.wikipedia.org/wiki/Server_Message_Block, 2023 閲覧.
- (24) M. Gancarz, 芳尾桂 (訳), UNIX という考え方 — その設計思想と哲学, オーム社, 東京, 2001.
- (25) E.S. Raymond, 長尾高弘 (訳), The Art of UNIX Programming, KADOKAWA, 東京, 2019.
- (26) Wikipedia, “UNIX 哲学,” <https://ja.wikipedia.org/wiki/UNIX%E5%93%B2%E5%AD%A6>, 2023 閲覧.
- (27) J.M. Perkel, “Five reasons to love the command line,” Nature, vol.590, pp.173–174, Feb. 2021.
- (28) Broadcom Inc., “VMware Fusion,” <https://www.vmware.com/jp/products/fusion.html>, 2023 閲覧.
- (29) 海上忍, “Big Sur 時代のボリューム構造,” <https://news.mynavi.jp/article/osxhack-277/>, マイナビ, 2021.
- (30) The OpenBSD Project, “OpenSSH,” <https://www.openssh.com/>, 2023 閲覧.
- (31) Apple Inc., “macOS Server ユーザガイド Open Directory,” <https://support.apple.com/ja-jp/guide/server/apd65944ef3/5.12/mac/12.0>, 2023 閲覧.
- (32) Apple Inc., “dscl.1,” <https://opensource.apple.com/source/DSTools/DSTools-162/dscl/dscl.1.auto.html>, 2003.
- (33) G.V. Vaughan, B. Elliston, T. Tromeey, and I.L. Taylor, “第 21 章 ポータブルな Bourne シェルを書く,” GNU Autoconf/Automake/Libtool, ぴあ (監訳), pp.285–301, オーム社, 東京, 2001.
- (34) Wikipedia, “Trusted Solaris,” https://en.wikipedia.org/wiki/Trusted_Solaris, 2023 閲覧.
- (35) Wikipedia, “Linux Security Modules,” https://en.wikipedia.org/wiki/Linux_Security_Modules, 2023 閲覧.
- (36) R.N.M. Watson, SPARTA, Inc., L.T. Denault, and Networks Associates, Inc., “The TrustedBSD Project,” <http://www.trustedbsd.org/>, 2023 閲覧.
- (37) J. Winsor, “オートマウントサービス,” Solaris 上級システム管理, 日本サン・マイクロシステムズ (監訳), pp.171–293, アスキー, 東京, 1995.
- (38) S. Cheshire, Apple Computer, B. Aboba, Microsoft Corporation, E. Guttman, and Sun Microsystems, “Dynamic Configuration of IPv4 Link-Local Addresses,” Internet Engineering Task Force (IETF), RFC 3927, 2005.
- (39) B. Aboba, D. Thaler, L. Esibov, and Microsoft Corporation, “Link-Local Multicast Name Resolution (LLMNR),” Internet Engineering Task Force (IETF), RFC 4795, 2007.
- (40) S. Cheshire, M. Krochmal, and Apple Inc., “Multicast DNS,” Internet Engineering Task Force (IETF), RFC 6762, 2013.
- (41) Apple Inc., “Apple 製のデバイスで社内ネットワークの '.local' ドメインを開けない場合,” <https://support.apple.com/ja-jp/101903>, 2023.
- (42) P. Mockapetris and ISI, “Domain Names — Concepts and Facilities,” Internet Engineering Task Force (IETF), RFC 1034, 1987.
- (43) P. Mockapetris and ISI, “Domain Names — Implementation and Specification,” Internet Engineering Task Force (IETF), RFC 1035, 1987.
- (44) S. Cheshire, M. Krochmal, and Apple Inc., “DNS-Based Service Discovery,” Internet Engineering Task Force (IETF), RFC 6763, 2013.
- (45) L. Poettering, T. Lloyd, and S. Simons, “Welcome to Avahi,” The Avahi developers, <https://www.avahi.org/>, 2023 閲覧.
- (46) The Web Hypertext Application Technology Working Group (WHATWG), “HTML Standard,” <https://html.spec.whatwg.org/multipage/>, 2023 閲覧.
- (47) Ecma International, “ECMA-262,” <https://ecma-international.org/publications-and-standards/standards/ecma-262/>, 2023 閲覧.
- (48) D. Robinson, K. Coar, and The Apache Software Foundation, “The Common Gateway Interface (CGI) Version 1.1,” Internet Engineering Task Force (IETF), RFC 3875, 2004.

付 録

1. 用 語 集

10GbE (10 Gigabit Ethernet) … イーサネット通信速度規格の一種, Cat. 6A ケーブルや RJ-45 コネクタなどが定義 — § 3.4

AFP (Apple Filing Protocol) … ファイル共有などプロトコルの一種, Mac OS から利用, 実質的に廃止 — § 2, § 3, § 5, § 6.4 の随所

ANSI (American National Standards Institute) … アメリカ合衆国の標準化機関の一つ, ISO/IEC 規格の起源として貢献 — § 4

ANSI/ISO C … ANSI/ISO によるプログラミング言語 C の規格, 特にシステムコールは POSIX.1 の部分 — § 4

APFS (Apple File System) … ファイルシステムの一種, macOS, iOS など で利用 — § 2, § 3.3, § 3.4

Apple ID … Apple 提供の iPhone, Mac などに iCloud をはじめとするクラウドサービスを提供するための識別子である電子メールアドレス URL: <https://appleid.apple.com/> — 付録 1

APU (Accelerated Processing Unit) … 処理装置の一種, CPU と GPU の統合システム集積回路 — 付録 1

BSD (Berkeley Software Distribution) Unix … Unix の一種, 386BSD, FreeBSD, NetBSD, OpenBSD など OSS Unix の代表格 — § 2

BYOD (Bring Your Own Device) … 個人所有のデバイスを職場や大学にもち込み活用すること. MDM など で組織の機密・個人情報の保全を管理する必要性はある. — § 1

CGI (Common Gateway Interface) … Web 技術の一つ, Web サーバ上で動作するプログラムを呼び出す仕組み — § 7

Clang … コンパイラ実装の一つ, GCC の置き換えとなる LLVM 基盤の OSS 実装 URL: <https://clang.llvm.org/> — 付録

Clustered File System … データセンター向け DFS. Fibre チャンネルなどを活用し高速化・高信頼化を図るファイルシステム、及び、装置 — § 1

CPU (Central Processing Unit) … 処理装置の一種、中央集権的なプログラム処理、処理装置にはほかに FPU, GPU, SoC の APU などがある。 — § 2, § 5.1, § 7

CUI (Character User Interface, Console User Interface, CLI: Command Line Interface) … コンピュータ対ヒトの手段の一種、文字列表示とキーボードを用いる UI — § 2

Cygwin … Windows で動作する OSS の POSIX 互換レイヤ、Windows 95 と Windows NT の両系統で動作 — § 1

DFS (Distributed File System) … 分散ファイルシステム、OSF (Open Software Foundation) による DCE/DFS (Distributed Computing Environment/Distributed File System), Microsoft による SMB ファイル共有など。本稿の主題の NFS もその一つである。 — § 4

DHCP (Dynamic Host Configuration Protocol) … TCP/IP サービスの一種、機器に IP アドレスを自動的に割り当てるプロトコル — § 6.1, § 6.1.6

DNS (Domain Name System) … 名前解決プロトコルの一つ、IP アドレスと FQDN を対応づける分散型データベースシステム — § 2, § 4, § 6 の随所

DOI (Digital Object Identifier) … ISO 標準デジタルオブジェクト識別子。主に学術・公的文書などに広く利用。URL: <https://www.doi.org/> — 付録 1

Dropbox … クラウドストレージサービスの一つ、2GB まで無償、LAN 前提の本稿とは独立したサービス URL: <https://www.dropbox.com/> — § 1

Ecma International (以前の正式名称: **European Computer Manufacturers Association**) … 欧州の情報通信システムの標準化機関、ECMA-6 (ISO/IEC 646, 7-bit ASCII コード), ECMA-35 (ISO/IEC 2022, JIS コード), ECMA-119 (ISO/IEC 9660:2023, CD-ROM フォーマット), ECMA-334 (ISO/IEC 20619, プログラミング言語 C#) などの規格が有名 — 付録 1

ECMAScript … プログラミング言語の一つ、Ecma International で標準化された Javascript, 主に Web アプリケーションで利用、Web ブラウザ上で動作、プログラミング言語 Java とは別の言語 — § 7

FHS (Filesystem Hierarchy Standard) … Unix のファイルシステム階層の規格、LSB 規格の一部 — 付録 1

FPU (Floating Point Unit) … 処理装置の一種、浮動小数点演算処理 — 付録 1

FQDN (Fully Qualified Domain Name) … TLD までの完全なホスト名、例えば www.ieice.org や ramanujan.local — § 6

FSF (Free Software Foundation, Inc.) … 非営利団体の一つ、GCC など多数の OSS の作者であるリチャード・ストー

ルマンにより創設 — 付録 1

GbE (Gigabit Ethernet) … イーサネット通信速度の一種、Cat. 5~6 ケーブルや RJ-45 コネクタなどが定義 — § 3.4

Gbps (gigabits per second) … 通信速度単位の一つ、イーサネットは 10, 100 Mbps, 1, 2.5, 5, 10 Gbps へと普及 — § 3.4

GCC (GNU Compiler Collection) … コンパイラ実装の一つ、多くのアーキテクチャに対応する FSF による OSS 実装、macOS, FreeBSD では Clang へ移行 URL: <https://gcc.gnu.org/> — § 2

GitHub … 現在は Microsoft 傘下 GitHub 社による OSS ソースコードのホスティング・クラウドサービス URL: <https://github.com/> — § 1

GNU (GNU's Not Unix) … Unix の一種、または OSS プロジェクト名、FSF による OSS プロジェクトの老舗 — § 2, § 6.2

GNU LGPL (Lesser General Public License) … OSS 利用許諾書の一つ、主にソフトウェアライブラリに適用 — § 6.2

GPU (Graphics Processing Unit) … 処理装置の一種、グラフィックス処理 — 付録 1

GUI (Graphical User Interface) … コンピュータ対ヒトの手段の一種、主にグラフィックスとポインティングデバイスを用いる UI — § 2, § 4, § 8

HDD (Hard Disk Drive) … ストレージ (補助記憶装置) の一種、実質 1.5 Gbps 程度のアクセス速度 — § 1, § 2, § 3.4

HFS+ (Hierarchical File System Plus) … ファイルシステムの一つ、Mac OS から利用、APFS へ移行 — § 2, § 3.4

HTML (HyperText Markup Language) … マークアップ言語の一つ、主に Web ページの記述に利用 — § 7

HTTP (Hypertext Transfer Protocol) … TCP/IP サービスの一種、Web サーバとウェブブラウザ間の通信に利用 — § 2

iCloud … Apple が運営するクラウドサービス。特に iPhone と Mac の連携において利便性を発揮する。URL: <https://www.icloud.com/> — § 1

IEEE (Institute of Electrical and Electronics Engineers) … 電気・情報工学分野の学術研究団体、標準化機関の一つ、LAN 規格の IEEE 802 が有名 — § 1, § 2

IETF (Internet Engineering Task Force) … 標準化機関の一つ、RFC の編集者 — 付録 1

IMAP (Internet Message Access Protocol) … TCP/IP サービスの一種、メールサーバに保存された電子メールへのアクセス・操作に利用 — § 2

Interix … POSIX 互換の Windows サブシステムの一つ、元の OpenNT, 後に SFU のコンポーネントとなる。 — § 1

IP アドレス (Internet Protocol address) … TCP/IP 上の NIC 番地、IP で通信相手を識別する番号 — § 6 の随所, § 7

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) … 標準化機関の一つ、ISO と IEC の合同技術委員会 — 付録 1

LAN (Local Area Network) … 通信ネットワーク形態の

一つ、局所的に運用される通信ネットワーク — § 5.1, § 6.1

LDAP (Lightweight Directory Access Protocol) … ディレクトリサービスの一種, OpenLDAP (URL: <https://www.openldap.org/>), Active Directory, Samba (URL: <https://www.samba.org/>) が代表的な実装 — § 1, § 4, § 5.1

Linux … Unix の一種, または OS のカーネル名で Debian, Slackware, Rocky, Android など多数のディストリビューションがあり, OSS Unix の代表格 — § 1, § 2, § 5.2.1, § 6.2

LLVM (以前の正式名称: **Low Level Virtual Machine**) … コンパイラ基盤としての仮想機械の一つ, コンパイラ技術の OSS 実装 URL: <https://www.llvm.org/> — 付録 1

LSB (Linux Standard Base) … Linux ディストリビューションの規格, SUS, POSIX 拡張や FHS などを含む標準規格 ISO/IEC 23360 URL: <https://www.iso.org/standard/77865.html>, <https://www.iso.org/standard/77866.html> — 付録 1

MAC アドレス (Media Access Control address) … LAN 上の NIC 番地, NIC を識別するためのサブネット内で一意の番号 — § 6.1, § 6.1.6, § 7

mDNS (Multicast DNS) … 名前解決プロトコルの一つ, DNS サーバ不要の名前解決プロトコル Zeroconf の一つ — § 4, § 6 の随所, § 7, 付録 1

Nextcloud … クラウドストレージサービスのための OSS, LAN 前提の本稿とは独立したサービスの OSS URL: <https://nextcloud.com/> — § 1

NFS (Network File System) … ファイル共有プロトコルの一種, Unix サーバ用途で一般的 — § 1, § 2, § 3, § 4, § 5, § 6, § 8 の随所

NIC (Network Interface Controller) … ネットワーク接続機構, イーサネット, Wi-Fi などを使用 — 付録 1

NIS (Network Information Service) … ディレクトリサービスの一種, 主に Unix で利用 — § 2, § 4

NVMe (Non-Volatile Memory Express) … SSD インタフェース規格の一種, 現状 40~80 Gbps 程度のアクセス速度, PCIe へ接続 — § 3.4

OS (Operating System) … ソフトウェアの一つ, ハードウェアのリソース管理などを行う基盤ソフトウェア — § 1, § 2, § 3, § 5, § 6.2 の随所

OSS (Open Source Software) … ソフトウェアの利用形態の一つ, ソースコードの公開・利用・修正・再頒布が担保されるソフトウェア — § 1

PCIe (Peripheral Component Interconnect Express) … 拡張バス規格の一種, GPU 搭載のビデオカードや NVMe 等様々な機器を接続 — 付録 1

POSIX (Portable Operating System Interface) … Unix 規格の一つ, Unix の標準規格 IEEE 1003 (ISO/IEC 9945), POSIX.1 と POSIX.2 がある. — § 1, § 2

POSIX subsystem … POSIX 互換の Windows サブシステムの一つ, Windows NT より, Windows XP/Server 2003 にて削除 — § 1

RFC (Request for Comments) … IETF 技術仕様公開文書, インターネット・プロトコル・スイート技術の標準 — 参考文献

SATA (Serial Advanced Technology Attachment) … HDD/SSD インタフェース規格の一種, 最大 6 Gbps 程度のアクセス速度 — § 2, § 3.4

SFU (Services for UNIX) … POSIX 互換の Windows サブシステムの一つ, Windows NT より, Windows Vista/Server 2003 R2 にて削除 — § 1

SIP (System Integrity Protection) … システム機構の一種, macOS の保護領域に対して操作を制限する機構 — § 5.1, § 5.2.3, § 8

slogin … リモートログインの一つ, SSH プロトコルによるセキュアなリモートログインのコマンド — § 3, § 5, § 7, § 8 の随所

SMB (Server Message Block) … ファイル共有, プリント共有等プロトコルの一種, Windows ほかに多くの OS で利用 — § 2, § 3, § 5, § 6.4, § 8 の随所

SMTP (Simple Mail Transfer Protocol) … TCP/IP サービスの一種, 電子メールの送受信に利用 — § 2

SoC (System on a Chip) … 集積回路の一種, CPU やそのほかの機能の統合システム集積回路 — 付録 1

Solaris … Unix の一種, Sun Microsystems による BSD Unix から UNIX SVR4 への Unix 実装 — § 2, § 4, § 5.2.1, 付録 1

SPARC … CPU の一種, Sun Microsystems による Solaris 稼働の主要 CPU — § 2

SSD (Solid-State Drive) … ストレージ (補助記憶装置) の一種, 現状 40 Gbps 程度のアクセス速度 — § 1, § 2, § 3.3, § 3.4

SUA (Subsystem for UNIX-based Applications) … POSIX 互換の Windows サブシステムの一つ, Windows Vista/Server 2003 R2 より, Windows 8 にて削除 — § 1

SUS (Single UNIX Specification) … Unix 規格の一つ, UNIX の The Open Group/IEEE による標準規格. ANSI/ISO C, POSIX.2 などを含み POSIX の元となった規格 URL: <https://unix.org/version4/> — § 1

TCP/IP (Transmission Control Protocol/Internet Protocol) … ネットワークプロトコルの一つ, インターネット標準通信プロトコル — 付録 1

TLD (Top-Level Domain) … DNS の最上位ドメイン名, 例として .org や .local — 付録 1

UI (User Interface) … コンピュータ対ヒトの手段, 明解さ・容易さ・効率性・生産性・再現性などが求められる. — § 6.2

UNIX SVR4 (System V Release 4) … Unix の一種, 標準規格の元となる商用 UNIX のバージョン・リリース番号 — § 2, 付録 1

Unix … OS の一種, OS はほかに OpenVMS, CP/M, MS Windows, TOPPERS などが挙げられる. — § 1, § 2, § 3, § 4, § 5, § 6, § 8 の随所

Windows NT … Microsoft が開発した OS, Windows NT

系として継続した製品シリーズとなり、Windows 11 が現在の最新版 — § 1

WSL (Windows Subsystem for Linux) … Windows サブシステムの一つ、Windows 10 より、POSIX を含む ISO/IEC 23360 準拠が可能 URL: <https://learn.microsoft.com/en-us/windows/wsl/> — § 1

WSL2 (Windows Subsystem for Linux 2) … Windows 上の仮想化の一つ、Windows 10 より、POSIX を含む ISO/IEC 23360 準拠が可能 URL: <https://learn.microsoft.com/en-us/windows/wsl/> — § 1

Xsan … Apple がかつて販売していた SAN (Storage Area Network) 共有ファイルシステム、Mac OS X 10.7 Lion 以降は OS に標準装備 — § 1

Zenodo … 汎用公開リポジトリ、オープンソース、DOI による引用が可能 URL: <https://zenodo.org/> — § 1

Zeroconf (Zero Configuration Networking) … TCP/IP ネットワーキング技法の一つ、サーバ不要のアドレス選択、名前解決、サービス検出プロトコル、LLMNR (Link-Local Multicast Name Resolution), UPnP/SSDP (Universal Plug and Play/Simple Service Discovery Protocol), DLNA (Digital Living Network Alliance), 標準規格 mDNS/DNS-SD (DNS Service Discovery) などがある。 — § 6, 付録 1

コンソール (Console) … 計算機を直接、対話的に操作するための計算機と入出力装置 — Abstract

(幹事団提案, 2024 年 2 月 13 日受付,
2024 年 4 月 1 日再受付)



池口 徹 (正員: フェロー)

1990 東京理科大学大学院理工学研究科電気工学専攻了。同年、同大学基礎工学部助手。1997 ルイ・パスツール大学 (現ストラスブール第一大学, フランスストラスブール市) 客員教授。2000 埼玉大学大学院理工学研究科助教授, 2005 同教授を経て, 2014 東京理科大学工学部第一部経営工学科教授。2016 東京理科大学工学部情報工学科教授, 現在に至る。博士 (工学)。非線形時系列解析, 計算論的脳神経科学, 複雑ネットワーク理論, カオスダイナミクスを用いた離散最適化問題のメタ・ヒューリスティック解法の開発, 非線形振動子の同期現象などの研究に従事, NOLTA 2012 共同実行委員長, 2013 非線形問題研究専門委員会委員長, 2014 NOLTA ソサイエティ庶務幹事, NOLTA 2016 実行委員長, 2017 NOLTA ソサイエティ会長。



山田 泰司

1995 東京電機大学大学院工学研究科電子工学専攻修士課程了。同年、(株) あいはら入社。2006 埼玉大学工学部情報システム工学科非常勤講師。2018 東京理科大学工学部情報工学科非常勤講師。現在、(株) あいはらにて、カオス時系列解析, ニューロコンピューティングに関する研究開発に従事。



高橋 純

1988 東京電機大学工学部電子工学科卒。同年、沖ソフトウェア (株) 入社。制御系ソフトウェア開発に従事。1993 (株) あいはら入社。以来、同社情報システム管理, 時系列解析の研究及びその応用ソフトウェア開発に従事。現在、同社関東支社研究開発チームリーダー。



島田 裕 (正員)

2008 埼玉大学工学部情報システム工学科卒。2012 同大学大学院理工学研究科博士後期課程了。博士 (工学)。2012 FIRST 合原最先端数理モデルプロジェクト研究員, 2014 東京理科大学工学部第一部経営工学科, 2016 東京理科大学工学部情報工学科助教, 2018 埼玉大学大学院理工学研究科助教, 2022 埼玉大学大学院理工学研究科准教授, 現在に至る。複雑ネットワーク, 非線形時系列解析及びその応用などの研究に従事。

LDPC符号のための近接勾配復号法

Proximal Decoding for LDPC Codes

和田山正 Tadashi WADAYAMA

アブストラクト 本稿では、筆者らが提案した LDPC 符号のための近接勾配復号法について解説する。本稿に関する論文 (Wadayama and Takabe, IEICE EA, no.3, pp.359–367, 2023) は、2022 年度電子情報通信学会論文賞を受賞した。凸最適化問題を解くための近接勾配法は、スパース信号再構成などの逆問題を解く技法として信号処理分野では広く利用されてきているが、LDPC 符号の復号問題への適用はこの論文にて初めて議論がなされた。提案法の核となるアイデアは、通信路に対応する負対数尤度と符号に対応する符号ポテンシャルエネルギー関数からなる目的関数に対して、近接勾配法を適用して反復最小化を行うことにより近似的最大事後確率復号を実現する点にある。負対数尤度関数を適切に変更することで、広範なクラスの通信路に対して提案復号法を利用することができる。計算機実験の結果、現代の無線通信システムにおいて重要な LDPC 符号化 MIMO 通信路においてデファクトスタンダードである既存手法 (MMSE 信号検出とビリーフプロパゲーション復号法の組み合わせ手法) と比較して、提案復号法は顕著な復号性能の改善を与えることが示されている。また、有色ガウス雑音通信路や非線形性を有する通信路など、効率的な復号法の構成が困難である通信路への適用についてもその有効性が実験的に示されている。更に、提案法は、テンソル計算を中心とした実装が可能であり、GPGPU (General Purpose Graphics Programming Unit) や AI アクセラレータなどの深層学習に特化したハードウェアに適した反復構造をもつ。深層展開などの機械学習技術との親和性も高く、今後、実応用に関する研究の進展が期待される。

キーワード LDPC 符号, 復号アルゴリズム, テンソル計算, 近接勾配法, AI アクセラレータ, GPGPU, 深層展開

Abstract In this paper, we present an overview of the proximal decoding for LDPC codes proposed by Wadayama and Takabe. The related paper (Wadayama and Takabe, IEICE EA, no.3, pp.359–367, 2023) was awarded the 2022 IEICE Paper Award. The proximal gradient method, widely used in signal processing for solving inverse problems such as sparse signal reconstruction, has been applied to LDPC decoding problems for the first time in this paper. The core idea of the proposed method is to perform approximate maximum a posteriori probability (MAP) decoding by applying the proximal gradient method to iteratively minimize an objective function consisting of the negative log-likelihood corresponding to the communication channel and the code potential energy function corresponding to the code. By appropriately modifying the negative log-likelihood function, we can apply the proposed decoding method to a wide range of communication channels. Computational experiments have shown that the proposed decoding method provides a significant improvement in decoding performance compared with the existing de facto standard method (a combination of MMSE signal detection and belief propagation decoding) for LDPC-coded MIMO communication channels, which are important in modern wireless communication systems. The effectiveness of the proposed method has also been experimentally demonstrated for communication channels with colored Gaussian noise and nonlinearities, for which the construction of efficient decoding methods is challenging. Furthermore, the proposed method can be implemented using tensor computations and has an iterative structure suitable for deep-learning-specific hardware such as general purpose graphics processing units (GPGPUs) and AI accelerators. It also has high compatibility with machine learning techniques such as deep unfolding, and future research on practical applications is expected.

Key words LDPC codes, Decoding algorithm, Tensor computation, Proximal gradient method, AI accelerator, GPGPU, Deep unfolding

1. はじめに

様々な分野において、誤り訂正符号は信頼性の高い情報伝達を実現するために必要不可欠な技術となっている。次世代無線通信技術 (6G) の実現、次世代ストレージデバイスの実現、量子コンピュータの実現 (量子誤り訂正符号) といった技術的目標を達成するためにも適切な誤り訂正符号とその復号法の研究開

和田山正 正員：シニア会員 名古屋工業大学大学院工学研究科
E-mail wadayama@nitech.ac.jp
Tadashi WADAYAMA, Senior Member (Dept. of Computer Science and Software Engineering, Nagoya Institute of Technology, Gokiso, Showa, Nagoya, 466-8555, Japan).
電子情報通信学会 基礎・境界サイエティ
Fundamentals Review Vol.18 No.1 pp.29–41 2024 年 7 月
©電子情報通信学会 2024

発が求められている。

その中で低密度パリティ検査符号 (LDPC (low-density parity-check) 符号)⁽¹⁾ の果たすべき役割はますます重要になってきている。例えば、LDPC 符号は 6G ネットワークにおいて、信頼性の高いデータ伝送を保証するために利用されることが見込まれている。6G ネットワークの実現のためには、高いレベルの技術革新が必要とされている。例えば、人工知能 (AI) と誤り訂正処理を含む信号処理のシームレスな統合は、6G ネットワークの実現において重要な課題となっている⁽²⁾。

最近の大規模言語モデル (LLM)、例えば GPT-4⁽³⁾ の顕著な成果は、AI 分野に留まらず幅広い分野において極めて大きなインパクトを与えている。これらの成功は、次世代の多目的グラフィックス処理ユニット (GPGPU; general purpose graphics programming unit) を含む高速かつ消費電力が少ない AI アクセラレータ⁽⁴⁾ の進化を更に後押ししている。これらの先進的なデバイスは、AI モデルの要求する計算ニーズに対応するために特別に設計^(注1) されており、テンソル積計算を中心として高い並列計算能力により複雑なモデルの学習プロセスを加速するだけでなく、推論タスクの実行速度とエネルギー効率を高める上で重要な役割を果たす。

一方、光コンピューティングの分野においても近年革新が起こりつつある。マッハ・ツェンダ干渉計 (MZI) に基づく光学プログラマブル回路が研究者から顕著な関心を集めている⁽⁵⁾。MZI は、入力光ビームの位相を変更する位相シフタとそれを分割するビームスプリッタから構成される光学部品であり、二つの制御可能なパラメータがあるプログラマブルな光学部品である。MZI を用いて実装された光行列ベクトル積回路が最近活発に研究されている^{(6), (54)}。プログラマブルな MZI ベースの光行列ベクトル積回路は、優れた計算速度と省エネルギー性のため次世代 AI アクセラレータの有望な候補となっている。最近の例として光学領域で実装されたニューラルネットワークがある⁽⁷⁾。

これら次世代の AI アクセラレータの提供する計算速度とエネルギー効率の大幅な向上は、AI 関連タスクの高速化と省エネルギー化に将来的に大きく貢献するものと予想される。更に AI アクセラレータへの大規模な開発投資は、アクセラレータ自身のコスト低減を加速する。このような状況において、AI アクセラレータは、AI 関連タスクに留まらず、無線信号処理を含む広範な信号処理を将来扱うようになると考えるのが自然である。

現在、実用的な LDPC 復号器は、十分なスループットとエネルギー効率を達成するために、アプリケーション特化型集積回路 (ASIC) に実装されることが多い。しかし、AI アクセラレータによる LDPC 復号器の実用的な実装に近い将来可能になれば、AI アクセラレータによって提供されるプログラム可能性は、レート、レイテンシ、符号の種類、信号形式など様々な要求に対応する無線信号処理タスクにおいて大きな柔軟性をもたらす。

このような方向性を考えると次世代の LDPC 復号アルゴリズムはテンソル計算フレンドリである必要がある。AI アクセラレータは、テンソル積やテンソルへの要素ごとの関数適用と

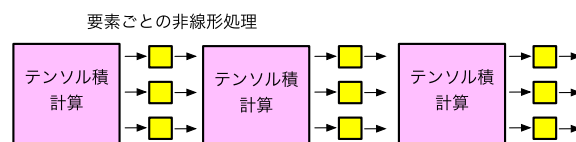


図1 テンソル計算フレンドリな計算

いったテンソル計算を効率的に並列計算できる構造を備えている (図1)。復号アルゴリズムの各内部プロセスが、テンソル計算フレンドリな計算で構成されるならば、AI アクセラレータの並列計算能力を最大限に活用することができる。

本稿では、筆者らが提案した LDPC 符号のための近接勾配復号法について、論文⁽⁸⁾に基づいて解説する (この論文を本稿では主論文と呼ぶ)。提案法の核となるアイデアは、通信路に対応する負対数ゆう度と符号制約に対応する符号ポテンシャルエネルギー関数からなる目的関数に対して、近接勾配法を適用して反復最小化を行うことにより近似的最大事後確率復号を実現する点である。後に示されるように近接勾配復号法はテンソル計算フレンドリであり、AI アクセラレータと非常に相性がよい点も大きな特長である。また、通信路に合わせて、負対数ゆう度関数の勾配計算を含む勾配降下処理を、プラグアンドプレイ的に取り替えることで、その通信路に適合した復号アルゴリズムを得ることができる。

本稿の第一の目標は主論文⁽⁸⁾の内容とそこに登場するアイデアを分かりやすく解説することにあるが、単に主論文⁽⁸⁾の内容をなぞるだけではなく、主論文で書ききれず、十分に議論されていない点に関する追加的説明や今後の関連研究の展望なども含めて述べていく。なお、復号性能の評価のための実験結果については本稿には再掲しないので、そちらについては主論文⁽⁸⁾をご参照願いたい。

2. 基礎的事項

2.1 LDPC 符号に関する表記

本稿を読む上では LDPC 符号に関する進んだ知識は要求されない。LDPC 符号に関して詳細を知りたい読者は関連書籍⁽⁹⁾や LDPC 符号に関する解説論文⁽¹⁰⁾などをお勧めしたい。

ここでは、本稿において利用される LDPC 符号関連の数学的表記を導入する⁽¹¹⁾。疎 2 元検査行列 $\mathbf{H} \equiv \{H_{ij}\} \in \mathbb{F}_2^{m \times n}$ に基づき 2 元 LDPC 符号 $\tilde{\mathcal{C}}(\mathbf{H})$ は

$$\tilde{\mathcal{C}}(\mathbf{H}) \equiv \{\mathbf{x} \in \mathbb{F}_2^n \mid \mathbf{H}\mathbf{x} = \mathbf{0}\} \quad (1)$$

と定義される。ここで n は符号長を、 m は検査シンボル数を表す ($m < n$)。また $\mathbb{F}_2$ は 2 元有限体を意味する。本稿においてはベクトルは列ベクトルであり、太字の英小文字で表す。更に、検査行列 $\mathbf{H}$ に関する非ゼロ列インデックス $A(i)$ と非ゼロ行インデックス $B(j)$ を

$$A(i) \equiv \{j \mid j \in [n], H_{ij} = 1\}, \quad i \in [m] \quad (2)$$

$$B(j) \equiv \{i \mid i \in [m], H_{ij} = 1\}, \quad j \in [n] \quad (3)$$

(注1): 最近の NVIDIA 社の GPGPU (例えば、現状のハイエンド GPGPU H100 など) は、テンソルコアと呼ばれる行列演算に特化した回路を内蔵している。

と定義する．ここで，表記 $[N]$ は集合 $\{1, 2, \dots, N\}$ を表す．

本稿の以下の議論では，送信シンボルが二値 $\{1, -1\}$ であるバイポーラ LDPC 符号を利用する．バイポーラ LDPC 符号は上記の $\tilde{C}(\mathbf{H})$ に基づき

$$C(\mathbf{H}) \equiv \{\beta(\mathbf{x}) \mid \mathbf{x} \in \tilde{C}(\mathbf{H})\} \quad (4)$$

と定義される．ここでバイナリバイポーラ変換 $\beta: \mathbb{F}_2 \rightarrow \mathbb{R}$ は $\beta(0) \equiv 1$, $\beta(1) \equiv -1$ と定義される．なお，本稿ではスカラー引数を取る関数がベクトルやテンソルに適用される場合は，そのスカラー関数がベクトルやテンソルの各要素に要素ごとに適用されるものとする^(注2)．

LDPC 符号 $\tilde{C}(\mathbf{H})$ のパリティ検査条件は

$$\forall \mathbf{x} \in \tilde{C}(\mathbf{H}), \quad \forall i \in [m], \quad \sum_{j \in A(i)} x_j = 0 \quad (5)$$

となる．この条件に対応するバイポーラ LDPC 符号 $C(\mathbf{H})$ におけるパリティ検査条件は

$$\forall \mathbf{x} \in C(\mathbf{H}), \quad \forall i \in [m], \quad \prod_{j \in A(i)} x_j = 1 \quad (6)$$

となる．

2.2 LDPC 符号の復号法について

LDPC 符号の復号法としては，ビリーフプロパゲーション法，min-sum 復号法，ビットフリップ復号法など様々な手法が実用的にも利用されている．本節では，ごく簡単に LDPC 符号の復号アルゴリズム研究の系譜 (図 2) について説明する．

LDPC 符号の復号法に関する研究は，1963 年の **Gallager** の博士論文からスタートした⁽¹⁾．Gallager はビリーフプロパゲーション復号法，ビットフリッピング復号法の復号性能をその中で議論している．その後の復号アルゴリズムの研究の流れはおおよそ三つの流れに分岐することになる．グラフィカルモデルにおけるベイズ確率推論計算に基づくビリーフプロパゲーション復号法の流れ，ビットフリッピング復号法の流れ，最適化ベースの復号法の流れである．

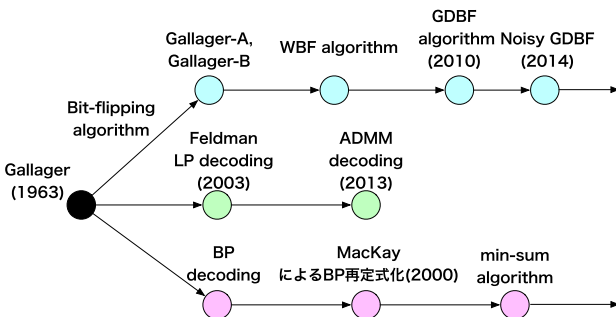


図 2 LDPC 符号の復号アルゴリズムの系譜 上段がビットフリッピング復号法，中段が最適化ベース復号法，下段が BP 復号法である．

2.2.1 ビリーフプロパゲーション復号法

確率推論を基本としているビリーフプロパゲーション復号法は，Gallager による発明に端を発して，MacKay により現在広く利用されている形に再定式化^{(12)(注3)}されたのち，min-sum 近似などを経て，現在広く実用的に利用されている．後述のビットフリッピング復号法と比較して ASIC 実装した場合には回路規模が大きくなる傾向にあるが，復号性能の点で最も優れている．人工知能，ベイズ推論分野で発展してきたグラフィカルモデルにおける確率推論と関係が深い．

2.2.2 ビットフリッピング復号法

Gallager-A, Gallager-B⁽¹⁾と呼ばれるアルゴリズムに端を発するビットフリッピング復号法は，ASIC 実装により比較的小規模の回路となるため，消費電力の点で優れている．そのため，現在までに非常に多くの復号アルゴリズムが提案されてきている．筆者のグループが 2010 年に発表した GDBF アルゴリズムは非凸目的関数の勾配降下法の定式化に基づくものであり，ビットフリッピング復号アルゴリズムに非凸最適化の観点を導入した⁽¹³⁾．以降，GDBF アルゴリズムの改良が数多く発表されてきているがいくつかの変形版，例えばノイズのある GDBF アルゴリズム⁽¹⁴⁾は，単純な GDBF アルゴリズムよりも優れた復号性能を与えることが示されている．

2.2.3 最適化ベース復号アルゴリズム

本稿で紹介される近接勾配復号法は，最適化ベースの復号アルゴリズムの一種として分類される．このクラスでも多数の復号法が開発されてきている．Feldman による線形計画 (LP) 復号法に関する研究⁽¹⁵⁾は，LDPC 復号問題を LP 問題として明確に定式化した．LP 問題を解決するための内点法の適用については論文⁽¹⁶⁾,⁽¹⁷⁾で議論されている．Zhang ら⁽¹⁸⁾と Berman ら⁽¹⁹⁾は，Feldman の LP 問題を解決するために交互方向乗数法 (ADMM) を適用し，これにより ADMM 復号法が誕生した．ADMM 復号法は，その後，多くの研究者によって研究され，復号性能と復号計算量の両方においてビリーフプロパゲーション復号法と競合する復号アルゴリズムとなりつつある．

3. 近似 MAP 復号問題

確率的通信路モデルに対応する条件付き確率密度関数 $p(\mathbf{y}|\mathbf{x})$ が既知である場合にブロック誤り率を最小化するという観点からは，MAP (maximum a posteriori) 復号が最適であることはよく知られている．しかし，一般的に LDPC 符号の MAP 復号は，計算量的に困難な問題である．ここでは，主論文⁽⁸⁾により導入された近似 MAP 復号のアイデアについて説明する．

(注2) : PyTorch などの計算で利用される文法と同様である．

(注3) : MacKay のこの書籍⁽¹²⁾から筆者が受けた影響は極めて大きく，主論文⁽⁸⁾のアイデアの基礎はここにある．

3.1 MAP 復号とその近似

受信信号アルファベットを $\mathbb{R}$ とし、送信信号アルファベットを 2 値アルファベット $\{-1, 1\}$ とする。いま、議論の対象とする通信路が条件付確率密度関数 $p(\mathbf{y}|\mathbf{x})$ ($\mathbf{y} \in \mathbb{R}^n, \mathbf{x} \in \mathbb{R}^n$) によりモデル化されているものとする。以下では、LDPC 符号 $C(\mathbf{H})$ のバイポーラ符号語をこの通信路に送る状況を考える。

このとき、MAP 推定則は、与えられた受信ベクトル $\mathbf{y}$ に対して

$$\hat{\mathbf{x}} \equiv \operatorname{argmax}_{\mathbf{x} \in \mathbb{R}^n} p(\mathbf{y}|\mathbf{x})p(\mathbf{x}) \quad (7)$$

という形になる。ここで $p(\mathbf{x})$ は符号 $C(\mathbf{H})$ により定まる事前確率密度関数

$$p(\mathbf{x}) \equiv \frac{1}{|C(\mathbf{H})|} \sum_{\mathbf{c} \in C(\mathbf{H})} \delta(\mathbf{x} - \mathbf{c}) \quad (8)$$

であり、 δ はディラックのデルタ関数である。このとき

$$\int_{\mathbb{R}^n} p(\mathbf{x}) d\mathbf{x} = \frac{1}{|C(\mathbf{H})|} \sum_{\mathbf{c} \in C(\mathbf{H})} \int_{\mathbb{R}^n} \delta(\mathbf{x} - \mathbf{c}) d\mathbf{x} \quad (9)$$

$$= \frac{|C(\mathbf{H})|}{|C(\mathbf{H})|} = 1 \quad (10)$$

が成り立つことが容易に確認できる。すなわち、 $p(\mathbf{x})$ はバイポーラ LDPC 符号の符号語ベクトルのみに離散的に確率測度が存在する確率密度関数となっている。

バイポーラ LDPC 符号の符号語数は n に対して指数的に増加し、MAP 復号の正確な実行は一般に計算量的に困難である。そこで、以下では、主論文⁽⁸⁾において導入された計算可能な近似 MAP 推定則について議論する。

以下では、近似事前分布としてギブス分布

$$\tilde{p}(\mathbf{x}) \equiv \frac{1}{Z} \exp(-\gamma h(\mathbf{x})) \quad (11)$$

の導入を考える。ここで、 γ は正の定数 (逆温度パラメータ) であり、連続関数 $h: \mathbb{R}^n \rightarrow \mathbb{R}$ は符号ポテンシャルエネルギー関数 (以下では、簡単のためポテンシャルエネルギー関数と呼ぶ) である。定数 Z は、正規化係数であり $Z \equiv \int_{\mathbb{R}^n} \exp(-\gamma h(\mathbf{x})) d\mathbf{x}$ と定義される。ここで、ポテンシャルエネルギー関数 $h(\mathbf{x})$ として

$$h(\mathbf{x}) \begin{cases} = 0, & \mathbf{x} \in C(\mathbf{H}) \\ > 0, & \text{otherwise} \end{cases} \quad (12)$$

となる関数を取ると $\gamma \rightarrow \infty$ のとき

$$\tilde{p}(\mathbf{x}) = \frac{1}{Z} \exp(-\gamma h(\mathbf{x})) \rightarrow \frac{1}{|C(\mathbf{H})|} \sum_{\mathbf{c} \in C(\mathbf{H})} \delta(\mathbf{x} - \mathbf{c}) \quad (13)$$

となる。実際の近似においては有限の逆温度パラメータ γ を利用し

$$p(\mathbf{x}|\mathbf{y}) \propto p(\mathbf{y}|\mathbf{x})p(\mathbf{x}) \simeq p(\mathbf{y}|\mathbf{x})\tilde{p}(\mathbf{x})$$

$$= \exp(-L(\mathbf{x}; \mathbf{y}) - \gamma h(\mathbf{x})) \quad (14)$$

を得る。ここで、 $L: \mathbb{R}^n \rightarrow \mathbb{R}$ は負対数尤度関数

$$L(\mathbf{x}; \mathbf{y}) \equiv -\ln p(\mathbf{y}|\mathbf{x}) \quad (15)$$

である。ここで、 $\mathbf{y}$ は与えられた受信ベクトルであり、定数として扱う。

この近似事前分布を利用し MAP 復号則を近似すると近似 MAP 復号則

$$\hat{\mathbf{x}} \equiv \operatorname{argmin}_{\mathbf{x} \in \mathbb{R}^n} L(\mathbf{x}; \mathbf{y}) + \gamma h(\mathbf{x}) \quad (16)$$

を導くことができる。この近似 MAP 復号則は MAP 復号問題の連続最適化問題への帰着と見ることができ、この連続最適化問題は、多峰性目的関数を含む非凸最適化問題であり、大域的最適解を見つけることは一般に計算量的に困難である。しかし、勾配法や近接勾配法などの反復最適化技法により、準最適解を求めることで、近似的な MAP 復号が可能となる。

3.2 符号ポテンシャルエネルギー関数

近似事前分布 $\tilde{p}(\mathbf{x})$ に含まれるポテンシャルエネルギー関数^(注4)であるが、主論文⁽⁸⁾では、バイポーラ LDPC 符号 $C(\mathbf{H})$ に基づく次の関数

$$h(\mathbf{x}) \equiv \sum_{j=1}^n (x_j^2 - 1)^2 + \sum_{i=1}^m \left(\left(\prod_{j \in A(i)} x_j \right) - 1 \right)^2 \quad (17)$$

の利用が提案されている^(注5)⁽²⁰⁾。

このポテンシャルエネルギー関数の第 1 項はバイポーラ制約に対応している。すなわち、全ての j について x_j の値が 1 または -1 であるときにのみ第 1 項の値が 0 となる。一方、第 2 項はバイポーラ LDPC 符号のパリティ検査条件 (6) に対応している。すなわち、全ての i について (バイポーラ) パリティ検査条件が満たされる場合のみ第 2 項の値が 0 となる。このポテンシャルエネルギー関数は多峰性の非凸関数であり、GDBF 復号法⁽¹³⁾の目的関数から発想を得ている^(注6)。

関数 $h(\mathbf{x})$ は 2 乗和の形をしていることから、任意の $\mathbf{x} \in \mathbb{R}^n$ に対して、非負値を与えることが分かる。一方、上記の説明のとおり $\mathbf{x} \in C(\mathbf{H})$ の場合には、 $h(\mathbf{x}) = 0$ となる。すなわち

$$\forall \mathbf{x} \in \mathbb{R}^n, \quad h(\mathbf{x}) \geq 0 \quad (18)$$

であり、等号成立条件は $\mathbf{x} \in C(\mathbf{H})$ である。更に $\nabla h(\mathbf{x}) = \mathbf{0}$ を容易に示すことができる。すなわち符号語ベクトルは関数 $h(\mathbf{x})$ の停留点となっている。

(注4)：主論文⁽⁸⁾中では、符号制約多項式という名前と呼ばれていたが本稿ではギブス分布に関連する用語の慣用に従う。

(注5)：最近の研究⁽²⁰⁾では、第 1 項と第 2 項に重み係数 α と β を乗じたポテンシャルエネルギー関数も利用されているが、本稿では主論文⁽⁸⁾の定義に従う。

(注6)：この観点からは、後に説明する近接勾配復号法は GDBF 復号法の連続最適化バージョンという見方も可能である。

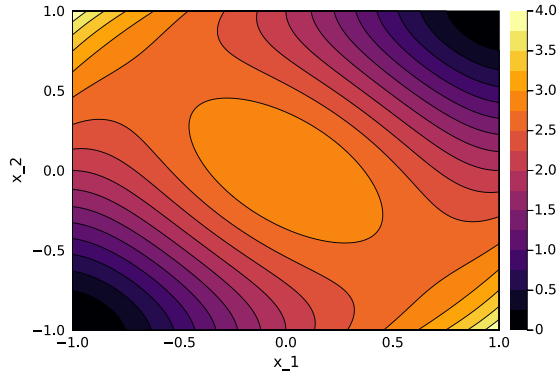


図3 関数 $h_{rep}(\mathbf{x})$ のヒートマップ表示 停留点は $(-1, -1)$, $(0, 0)$, $(1, 1)$ の3点である。

近似 MAP 復号則 (16) において、関数 $h(\mathbf{x})$ は一種のペナルティ関数となっていると解釈することもできる。すなわち、 $\mathbf{x}$ が $C(\mathbf{H})$ の符号語に近いときは小さいペナルティ値を与え、どの符号語からも遠いときには大きなペナルティ値を与える。近似 MAP 復号則の目的関数 $F(\mathbf{x}) \equiv L(\mathbf{x}; \mathbf{y}) + \gamma h(\mathbf{x})$ は、「符号語に近く」かつ「負対数尤度関数値を小さく」するベクトルに小さい値を与える目的関数となっているものと解釈できる。

簡単な例として、以下ではバイポーラ繰り返し符号 C_{rep} ($n = 2$) のポテンシャルエネルギー関数を見てみよう。符号 C_{rep} は $C_{rep} = \{(1, 1), (-1, -1)\}$ と与えられる。このとき、対応するポテンシャルエネルギー関数は

$$h_{rep}(\mathbf{x}) = (x_1^2 - 1)^2 + (x_2^2 - 1)^2 + (x_1 x_2 - 1)^2 \quad (19)$$

となる。符号語を $h_{rep}(\mathbf{x})$ に代入するとポテンシャルエネルギー値が 0 となること、任意の $\mathbf{x}$ に対して、 $h_{rep}(\mathbf{x}) \geq 0$ であることが容易に確認できる。

ポテンシャルエネルギー関数 $h_{rep}(\mathbf{x})$ のヒートマップ表示を図3に示す。この図から符号語の位置 $(+1, +1)$, $(-1, -1)$ において、関数が最小値 0 を取ることが確認できる。関数 $h_{rep}(\mathbf{x})$ の形状は、この符号語2点を谷底とする溪谷に似た姿をしている。このため、勾配法などの最適化技法を利用した場合には、符号語方向への引き込み現象が生じることが予想される。一方、原点 $(0, 0)$ は極大点であり、 $\nabla h_{rep}(\mathbf{0}) = \mathbf{0}$ が成り立っている。したがって、勾配降下ダイナミクスに従う探索ベクトルが原点付近を通過するならば、そのとき移動スピードは極端に遅くなることが予想される。

この例で見たようにポテンシャルエネルギー関数 $h(\mathbf{x})$ では、

$$h(\mathbf{x}) > 0, \quad \nabla h(\mathbf{x}) = \mathbf{0} \quad (20)$$

を満たす停留点が一般に存在する。この停留点を非符号語停留点と呼ぶ。また、等式ではなく $h(\mathbf{x}) > 0$, $\nabla h(\mathbf{x}) \simeq \mathbf{0}$ となる点を擬似非符号語停留点と呼ぶ。勾配法や近接勾配法などの勾配情報を利用する反復最適化技法を F の最小化に適用した場合には、この非符号語停留点、または擬似非符号語停留点に起因する F の停留点の付近で探索ベクトルの移動スピードが極端に低下し、停留点へのトラップが生じる。

近似 MAP 復号則 (16) を勾配情報を利用した反復最適化技法

で解く場合には、上記の望まれない停留点が復号性能に悪影響を及ぼす可能性がある。なぜならば、それらの停留点付近に探索点がトラップされてしまい、符号語である停留点に到達できないためである。

4. 近接勾配復号法

前節で導入された近似 MAP 復号則 (16) に登場する連続最適化問題を解くためには、様々な最適化技法が原理的には適用できる。以下では、非凸最適化問題 (16) を解くために、近接勾配法の利用について検討するとともに、その結果として近接勾配復号法を導入する。

4.1 近接勾配法

ここでは、反復最小化技法として近接勾配法を紹介する⁽²¹⁾。関数 $h: \mathbb{R}^n \rightarrow \mathbb{R}^n$ に対応する近接写像 (proximal map) を

$$\text{prox}_h(\mathbf{x}) := \underset{\mathbf{u} \in \mathbb{R}^n}{\text{argmin}} \left(h(\mathbf{u}) + \frac{1}{2} \|\mathbf{u} - \mathbf{x}\|_2^2 \right) \quad (21)$$

と定義する。以下では無制約最小化問題

$$\text{minimize } g(\mathbf{x}) + \ell(\mathbf{x}) \quad (22)$$

を考える。ここで、 $g(\mathbf{x})$ は微分可能な凸関数であり、通常 $\ell(\mathbf{x})$ は微分不可能な凸関数である^(注7) (21), (22)。

この最小化問題を解くための近接勾配法は、反復式

$$\mathbf{x}_{t+1} = \text{prox}_{\gamma \ell}(\mathbf{x}_t - \gamma \nabla g(\mathbf{x}_t)), \quad t = 0, 1, 2, \dots \quad (23)$$

により与えられる。適切な定数 γ の選択により、以上の反復により $\mathbf{x}_t$ が上記の最小化問題の最適解に収束することが証明されている。

近接勾配法から導出されるアルゴリズムとして、スパース信号再現アルゴリズム^{(23), (24)}としてよく知られている ISTA (iterative soft thresholding algorithm)⁽²⁵⁾がある。ISTA の基礎となる LASSO 目的関数⁽²⁶⁾は、スパース解を嗜好する L1 正則化項 $\tau \|\mathbf{x}\|_1$ を含んでいる。ここで、 τ は正則化の強度を調整する正則化係数である。ISTA はソフトしきい値関数 $\eta_\tau(x) \equiv \text{sign}(x) \max\{|x| - \tau, 0\}$ を含む反復式系

$$\mathbf{r}_t = \mathbf{s}_t + \gamma \mathbf{A}^T(\mathbf{y} - \mathbf{A}\mathbf{s}_t) \quad (24)$$

$$\mathbf{s}_{t+1} = \eta_{\gamma\lambda}(\mathbf{r}_t), \quad t = 0, 1, \dots \quad (25)$$

で与えられる。ここで、 $\mathbf{A}$ は観測行列、 $\mathbf{y}$ は観測ベクトルである。ソフトしきい値関数は正則化項 $\tau \|\mathbf{x}\|_1$ の近接写像である。

余談ではあるが、筆者は、深層展開に関する研究の過程⁽²⁷⁾で ISTA を研究対象として一時期扱っており⁽²⁸⁾、ISTA の考え方に基づく LDPC 符号の復号法の可能性を考え始めたのが近接勾配復号法の開発の端緒となった^(注8)。その意味では、以下で述べ

(注7)：より正確な近接勾配法の説明については例えば、文献(21), (22)などを参考にされたい。

(注8)：2020年頃から深層展開に関する分野での競争が激しくなりレッドオーシャン化してきたため、戦略的に符号理論への帰帰を目指して近接勾配復号法の研究をスタートした。

る近接勾配復号法は ISTA に極めて近い特徴をもち、両者は多くの点で類似性をもつアルゴリズムとなっている。

4.2 近接勾配復号法の詳細

近似 MAP 復号問題 (16) を数値的に解くためには、様々なアプローチがあり得る。例えば、勾配法⁽²⁹⁾の利用が考えられるが、それについては最近、勾配流復号法 (gradient flow decoding) の形で研究が進められている⁽²⁰⁾。ここでは、近接勾配法の利用による最小化の実行について検討する。

4.2.1 近接勾配復号法の導出

ここで考える目的関数は、 $L(\mathbf{x}; \mathbf{y}) + \gamma h(\mathbf{x})$ という形をしており、近接勾配法のレシピに従えば、 $\gamma h(\mathbf{x})$ の近接写像が必要となるが、この項は複雑な構造をもっており閉じた形の単純な近接写像を導出することは困難である。そこで、 $\gamma h(\mathbf{x})$ の近接写像を勾配ステップにより近似⁽²¹⁾した

$$\text{prox}_{\gamma h}(\mathbf{x}) \simeq \mathbf{x} - \gamma \nabla h(\mathbf{x}) \quad (26)$$

を以下では利用する。この近似式を近接勾配反復式 (23) に適用することで近接勾配復号法の反復式が導かれる。

4.2.2 近接勾配復号法

近接勾配復号法 (proximal decoding) は、反復式

$$\mathbf{r}^{(k+1)} = \mathbf{s}^{(k)} - \omega \nabla L(\mathbf{s}^{(k)}; \mathbf{y}) \quad (27)$$

$$\mathbf{s}^{(k+1)} = \mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)}), \quad k = 0, 1, 2, \dots \quad (28)$$

で定義される。ここで、式 (27) を勾配降下ステップと呼ぶ。このステップは、負対数尤度の最小化に寄与する。一方、式 (28) を符号近接ステップと呼ぶ。このステップは符号語への引き込みを生み出している。

探索ベクトル $\mathbf{s}^{(k)}$ は、勾配降下ステップでは、負対数尤度関数の勾配に基づき負対数尤度が小さくなる方向に引っ張られる。一方、符号近接ステップでは、探索ベクトルに近い符号語へと接近する。以上の二つのステップを交互に実行することにより、負対数尤度関数を最小化する符号語への収束が期待される (図 4)。

後に述べるとおり、ポテンシャルエネルギー関数 h の勾配ベクトル ∇h は効率よく計算できる。したがって、負対数尤度関数の勾配 ∇L が効率よく計算できる通信路であるならば、以上の近接勾配復号法の反復全体を効率よく計算できる。

反復式 (27) (28) には、ステップ係数として定数 ω, γ が含まれている。これらの定数の設定は復号性能に大きな影響を与えることが実験的に知られており、近接勾配復号法の復号性能を向上させるためには慎重な選択が求められる。選択のためには、事前実験に基づくパラメータ探索、バイズ最適化に基づくハイパーパラメータ探索⁽³⁰⁾、深層展開に基づくパラメータ最適化⁽⁹⁾などの手法が利用できる。

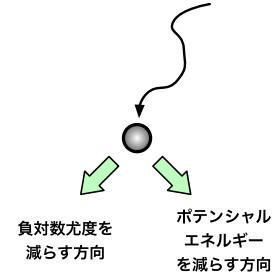


図 4 復号プロセスにおける探索ベクトルの動き

Algorithm 1 近接勾配復号法 (一般形)

```

1:  $\mathbf{s}^{(0)} := \mathbf{0}$ 
2: for  $k := 0$  to  $K - 1$  do
3:   勾配ベクトル  $\nabla L(\mathbf{s}^{(k)}; \mathbf{y})$  を計算する。
4:    $\mathbf{r}^{(k+1)} := \mathbf{s}^{(k)} - \omega \nabla L(\mathbf{s}^{(k)}; \mathbf{y})$ 
5:   勾配ベクトル  $\nabla h(\mathbf{r}^{(k+1)})$  を計算する。
6:    $\mathbf{s}^{(k+1)} := \mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)})$ 
7: end for
8:  $\hat{\mathbf{x}} := \text{sign}(\mathbf{s}^{(K)})$ 
9: Output  $\hat{\mathbf{x}}$ 

```

一般的な近接勾配復号法をアルゴリズムの形でまとめて、Algorithm 1 として示す^(注9)。ポテンシャルエネルギー関数の勾配計算については、4.3 節と 4.4 節で詳述する。

4.2.3 数値不安定性の回避

近接勾配復号は上記の形のままで、数値的に不安定になる場合がある。定数 η を 1 より僅かに大きな正の定数とし、 $B_\eta \equiv [-\eta, \eta]^n$ を n 次元の超立方体とする。ここで $[a, b] \equiv \{x \in \mathbb{R} \mid a \leq x \leq b\}$ である。勾配のノルム $\|\nabla h(\mathbf{x})\|$ は、ポテンシャルエネルギー関数の性質により、 $\mathbf{x} \notin B_\eta$ の場合に非常に大きくなる傾向があり、上記の近傍復号プロセスでは、それが数値的な不安定性 (振動または発散挙動) の原因となることがある。そのような場合には、数値的不安定性を防ぐために、(28) の代わりに

$$\mathbf{s}^{(k+1)} = \Pi_\eta(\mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)})) \quad (29)$$

を使用することができる。射影演算子 $\Pi_\eta : \mathbb{R}^n \rightarrow B_\eta$ は B_η への射影を表し、 $\Pi_\eta(\mathbf{x}) \equiv \arg \min_{\mathbf{x}' \in B_\eta} \|\mathbf{x} - \mathbf{x}'\|$ と定義される。

4.3 ポテンシャルエネルギー関数の勾配ベクトル

4.3.1 勾配ベクトル

近接勾配復号法の実行のためには、負対数尤度関数 L とポテンシャル関数 h に関する勾配ベクトル、すなわち、 ∇L と ∇h が必要となる。ここでは、勾配ベクトル ∇h の計算について説明する。

(注9)：主論文⁽⁸⁾では、パリティ検査を復号手順に行う形のアルゴリズムを示していたが、本稿では GPGPU 計算を念頭に置きパリティ検査を省いたアルゴリズムを提示している。

ポテンシャルエネルギー関数 $h(\mathbf{x})$ の勾配ベクトルは

$$\nabla h(\mathbf{x}) = \left(\frac{\partial}{\partial x_1} h(\mathbf{x}), \dots, \frac{\partial}{\partial x_n} h(\mathbf{x}) \right)^T \quad (30)$$

と書くことができる。ここで、

$$\begin{aligned} \frac{\partial}{\partial x_k} h(\mathbf{x}) &= 4(x_k^2 - 1)x_k \\ &+ 2 \sum_{i \in B(k)} \left(\left(\prod_{j \in A(i)} x_j \right) - 1 \right) \left(\prod_{j \in A(i) \setminus \{k\}} x_j \right) \end{aligned} \quad (31)$$

である ($k \in [n]$)。GPGPU 計算などに適した勾配ベクトル ∇h の計算法については 4.4 節で議論する。

4.3.2 ポテンシャルエネルギー関数の停留点

点 $\mathbf{x}^* \in \mathbb{R}^n$ が $\nabla h(\mathbf{x}^*) = \mathbf{0}$ を満たすとき、点 $\mathbf{x}^*$ は h の停留点である。任意の符号語 $\mathbf{c} \in C(\mathbf{H})$ について、 $x_k^2 = 1 (\forall k \in [n])$ と $\prod_{j \in A(i)} x_j = 1 (\forall i \in [m])$ が成り立つため、 $\nabla h(\mathbf{c}) = \mathbf{0}$ が成り立つ。すなわち、符号語ベクトルは h の停留点である。

このように多変数関数 h は非凸で複数の極小点、極大点、その他の停留点をもつ関数となっている。もし、探索点が符号語に十分に近いならば、勾配降下方向に移動する勾配ダイナミクスにより探索点は符号語の方に引き寄せられる。この現象を符号語への引き込みと呼ぶ。目的関数 F のポテンシャルエネルギー項は、この符号語への引き込みが生じるように目的関数に入れられていると考えることもできる。

符号語ベクトルは h の停留点であったが、この逆は成立せず、 h の停留点は必ずしも符号語であるとは一般にはいえない。例えば、原点 $\mathbf{0}$ は符号によらず、 $\nabla h(\mathbf{0}) = \mathbf{0}$ を満たすため停留点である。符号語ではない停留点である非符号語停留点は、多くの場合、原点以外にも存在し、勾配降下ダイナミクスによる正常な符号語への引き込みを阻害する主たる要因となっている^(注10)

主論文⁽⁸⁾では、対象とする符号を LDPC 符号としている。これは、検査行列が密な行列の場合には、大量に存在する非符号語停留点、及び近似的な非符号語停留点 ($\nabla h(\mathbf{x}) \simeq \mathbf{0}$) の影響で復号性能が劣化する傾向があるからである。

4.3.3 符号語への引き込み

ここでは、符号語への引き込み現象を確認するために近接反復 (proximal iteration)⁽²¹⁾に関する実験を行う。特にバイポーラ (7, 4, 3) ハミング符号に関する近接反復

$$\mathbf{x}^{(k+1)} = \mathcal{P}_\gamma(\mathbf{x}^{(k)}), \quad k = 0, 1, 2, \dots \quad (32)$$

を検討する。ここで、 $\mathcal{P}_\gamma(\mathbf{x})$ は符号近接作用素であり、ここでは近似的に

$$\mathcal{P}_\gamma(\mathbf{x}) \equiv \mathbf{x} - \gamma \nabla h(\mathbf{x}) \quad (33)$$

と定義する。すなわち、近接反復は、 $\mathbf{h}$ のみに着目した勾配降下ダイナミクスとみることができる。

(注10)：これらの非符号語停留点は、LP 復号法における擬似符号語 (pseudocodeword) とよく似ている。

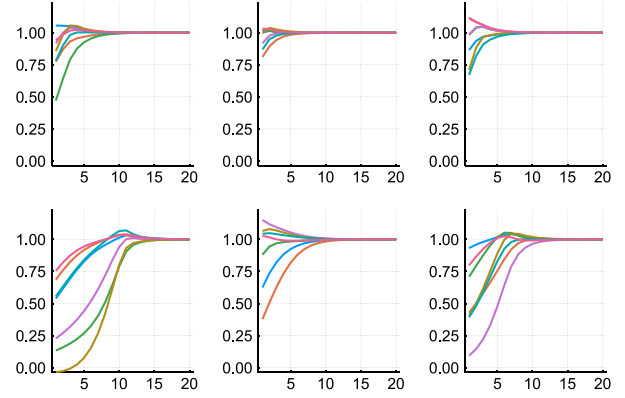


図5 近接反復における状態ベクトルの軌跡 (7, 4, 3) ハミング符号, (6 試行). パラメータ γ は 0.05 と設定した。

実験設定は以下のとおりである。全ての成分が 1 の符号語 $\mathbf{1} \equiv (1, 1, 1, 1, 1, 1, 1)$ が AWGN 通信路に送信されると仮定する。受信語は $\mathbf{y} = \mathbf{1} + \mathbf{w}$ で与えられる。ここで $\mathbf{w}$ の各独立同分布成分は平均 0、標準偏差 0.5 のガウス分布に従う。近接反復の初期値として受信語 $\mathbf{y}$ を使用した、すなわち $\mathbf{x}^{(0)} = \mathbf{y}$ である。近接反復プロセスにおける状態ベクトル $\mathbf{x}^{(k)}$ の成分の軌跡を図 5 に示す。横軸は反復ステップの数を表し、縦軸は $x_i^{(k)}, i \in [7]$ の値を示す。グラフ内のカーブは $\mathbf{x}^{(k)}$ の各成分の値に対応する。図 5 から、近接反復が全ての成分が 1 の符号語への収束を促進することが観察できる。すなわち、これらの近接反復において軌跡は符号語点である $\mathbf{1}$ に引き寄せられていることが観察できる。なお、任意の符号語ベクトルは $\mathcal{P}_\gamma$ の固定点であることに注意されたい。

4.4 テンソル計算可能性

近接勾配復号法を実行するためには、負対数ゆう度関数の勾配 ∇L とポテンシャルエネルギー関数 ∇h の数値的評価が効率的に実行できる必要がある。特に 1 節で述べたようにテンソル計算が得意な AI アクセラレータ (GPGPU など)⁽⁴⁾での効率的計算が可能であるかどうかは、重要なポイントとなる。

ある関数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ の値の評価が

- テンソル積計算
- スカラー乗算, $\alpha \mathbf{x}$ ($\alpha \in \mathbb{C}$, $\mathbf{x}$ はテンソル)
- 要素ごとの関数適用
- テンソル和, テンソル差, $\mathbf{a} + \mathbf{b}, \mathbf{a} - \mathbf{b}$

という基本テンソル演算の組み合わせで計算が可能であるときに、 f はテンソル計算可能である、ということにしよう。これらの基本演算は、様々な AI アクセラレータのもつ計算効率のよい基本演算の最小部分集合として選ばれている。もし、関数 f がテンソル計算可能な関数であれば、どの AI アクセラレータでも効率よく、 f の評価を複数コアを用いる並列計算に基づき実行できるはずである。

次の補題^(注11)は、勾配 $\nabla h(\mathbf{x})$ はテンソル計算可能であるこ

(注11)：この補題は主論文⁽⁸⁾を書いた時点では得られておらず、最近得られた結果である。

とを示している。この補題の詳細について文献(31)を参照されたい。

[Lemma 1] 勾配 $\nabla h(\mathbf{x})(\forall j \in [n], x_j \neq 0)$ は次のように表現することができる：

$$\nabla h(\mathbf{x}) = 4 \exp(\mathbf{z}_{-1} + \mathbf{z} + \mathbf{z}_{+1}) + 2 \exp(\mathbf{w} - \mathbf{z}), \quad (34)$$

ここで $\mathbf{z}, \mathbf{z}_{-1}, \mathbf{z}, \mathbf{z}_{+1}$ は

$$\mathbf{z} \equiv \ln(\mathbf{x}), \quad (35)$$

$$\mathbf{z}_{-1} \equiv \ln(\mathbf{x} - \mathbf{1}), \quad (36)$$

$$\mathbf{z}_{+1} \equiv \ln(\mathbf{x} + \mathbf{1}), \quad (37)$$

$$\mathbf{w} \equiv \ln(\mathbf{H}^T (\exp(2\mathbf{H}\mathbf{z}) - \exp(\mathbf{H}\mathbf{z}))) \quad (38)$$

と定義される。

検査行列 $\mathbf{H}$ はもともと $\mathbb{F}_2$ 上の行列であるが、上の計算においては、 $\mathbb{F}_2$ 上の 0 を $\mathbb{R}$ 上の 0、 $\mathbb{F}_2$ 上の 1 を $\mathbb{R}$ 上の 1 と読み替えて ($\mathbb{F}_2$ 上の 2 元行列を実数空間に埋め込んで) 計算を行っていることに注意したい。

もし、 ∇L がテンソル計算可能であるならば、近接勾配復号法の主たる計算は全てテンソル計算可能となり復号過程全体を AI アクセラレータで効率よく実行できることになる。

上記の勾配計算を GPGPU 計算させる場合には、複素対数関数と複素指数関数が必要となるが、PyTorch や CUDA などでは複素型の基本演算が備えられているのでそれらを利用することができる。また、実指数関数と実対数関数が利用できる環境であれば、容易にそれらを利用して上記のテンソル計算を実行することができる。

通常の GPGPU などの AI アクセラレータは上記の基本テンソル演算以外の効率よい基本演算を備えている場合が多い。例えば、計算効率のよいスパーステンソル積が基本演算として提供されている場合は、それを勾配計算に活用することで、上記のテンソル基本演算のみで計算するよりも計算効率の向上が期待できる。

復号処理全体がテンソル計算可能である場合には、複数の受信ベクトルをバッチとしてまとめて、複数の符号語からなる巨大テンソルに対して復号処理を一括して行うバッチ処理が可能となる。GPGPU では、この種のバッチ処理を活用することで、計算効率の改善が可能である。

更にテンソル計算可能な関数については、PyTorch, JAX などに内蔵されている自動微分機構⁽³²⁾に基づき内部パラメータに関する勾配を効率よく求めることができる。復号法全体がテンソル計算可能であれば、深層展開を適用することや学習可能コンポーネント (例えば学習可能な負対数ゆう度勾配 ∇L) の埋め込みの実装なども容易である。このように近接勾配復号法は、テンソル計算フレンドリであり、かつ AI フレンドリなアルゴリズムとなっている。

5. 近接勾配復号法のバリエーション

既に見たように近接勾配復号法では、対象とする通信路に応じて、負対数ゆう度関数 L を取り替えることで、対象通信路に適

合させることが可能である。すなわち、通信路に合わせて、 ∇L を含む勾配降下ステップを、いわば、プラグアンドプレイ的に取り替えることで、その通信路に適した復号アルゴリズムとすることができる。通信路の種類によらない普遍性も近接勾配復号法の長所の一つである。

5.1 AWGN 通信路モデル

ここでは、単純な AWGN 通信路をまず考えてみたい。送信語 $\mathbf{x} \in \mathbb{R}^n$ はバイポーラ LDPC 符号の符号語とし、受信語 $\mathbf{y}$ は $\mathbf{y} = \mathbf{x} + \mathbf{n}$ として与えられる。ここで、 $\mathbf{n}$ は各要素が $\mathcal{N}(0, \sigma^2)$ に従うガウス雑音ベクトルである。

Algorithm 2 テンソル計算ベース近接勾配復号法 (AWGN)

```

1:  $\mathbf{s}^{(0)} := \mathbf{0}$ 
2: for  $k := 0$  to  $K - 1$  do
3:    $\mathbf{r}^{(k+1)} := \mathbf{s}^{(k)} - \omega(\mathbf{s}^{(k)} - \mathbf{y})$ 
4:   次のように変数値を設定する:
        $\mathbf{z} := \ln(\mathbf{r}^{(k+1)}),$ 
        $\mathbf{z}_{-1} := \ln(\mathbf{r}^{(k+1)} - \mathbf{1}),$ 
        $\mathbf{z}_{+1} := \ln(\mathbf{r}^{(k+1)} + \mathbf{1}),$ 
        $\mathbf{w} := \ln(\mathbf{H}^T (\exp(2\mathbf{H}\mathbf{z}) - \exp(\mathbf{H}\mathbf{z})))$ 
5:    $\mathbf{h} := 4 \exp(\mathbf{z}_{-1} + \mathbf{z} + \mathbf{z}_{+1}) + 2 \exp(\mathbf{w} - \mathbf{z})$ 
6:    $\mathbf{s}^{(k+1)} := \mathbf{r}^{(k+1)} - \gamma \mathbf{h}$ 
7: end for
8:  $\hat{\mathbf{x}} := \text{sign}(\mathbf{s}^{(K)})$ 
9: Output  $\hat{\mathbf{x}}$ 

```

このとき、AWGN 通信路における近似 MAP 復号則は

$$\hat{\mathbf{x}} = \underset{\mathbf{x} \in \mathbb{R}^n}{\text{argmin}} \frac{1}{2} \|\mathbf{x} - \mathbf{y}\|^2 + \gamma h(\mathbf{x}) \quad (39)$$

となる。この場合 $\nabla \frac{1}{2} \|\mathbf{y} - \mathbf{x}\|^2 = \mathbf{x} - \mathbf{y}$ となることに注意すると近接勾配復号法の反復式は

$$\mathbf{r}^{(k+1)} = \mathbf{s}^{(k)} - \omega(\mathbf{s}^{(k)} - \mathbf{y}) \quad (40)$$

$$\mathbf{s}^{(k+1)} = \mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)}) \quad (41)$$

となる。初期値の選択には任意性があるが、通常 $\mathbf{s}^{(0)} = \mathbf{0}$ としておくことが実験的に確認されている。この場合は、負対数ゆう度関数の勾配がテンソル計算可能であるため、復号処理全体としてテンソル計算可能となることが確認できる。

ポテンシャルエネルギー関数の勾配計算に補題 1 を利用した場合を Algorithm 2 としてまとめている。例えば、PyTorch, TensorFlow, JAX などのニューラルネットワークのためのフレームワークを利用すれば、GPGPU 計算とバッチ処理を可能とする近接勾配復号法のプログラム実装は容易である^(注12)。

近接勾配復号法の復号性能については、AWGN 通信路においてはビリーフプロパゲーション復号法に及ばないものの、比較的良好なビット誤り率特性が得られることが実験的に確認さ

(注12)：より高速な GPGPU 実装を実現するためには、C++と CUDA ライブラリに基づく低レベルプログラミングが必要となる。

れている⁽⁸⁾。ビット誤り率特性の改善のためには、多段復号法 (multi-stage decoding)^(注13) の考え方も適用できる。すなわち、初段に近接勾配復号法を実行し、そこで復号できなかった場合のみビリーフプロパゲーション復号法を利用するというアプローチである。

5.2 MIMO 通信路モデル

次に無線通信で実用的に重要性の高い MIMO 通信路について議論する。ここでは、説明を簡単にするために実数 MIMO 通信路モデルを仮定して説明を進める^(注14)⁽³³⁾。通信路行列 $\mathbf{A} \in \mathbb{R}^{\mu \times n}$ が与えられているとき、符号語ベクトル $\mathbf{x} \in C(\mathbf{H})$ を通信路に送信し、受信器が $\mathbf{y} = \mathbf{A}\mathbf{x} + \mathbf{w}$ を観測すると仮定しよう。ここで、 $\mathbf{w}$ は加法的白色ガウス雑音である。

Algorithm 3 テンソル計算ベース近接勾配復号法 (MIMO)

```

1:  $\mathbf{s}^{(0)} := \mathbf{0}$ 
2: for  $k := 0$  to  $K - 1$  do
3:    $\mathbf{r}^{(k+1)} := \mathbf{s}^{(k)} - \omega \mathbf{A}^T (\mathbf{A} \mathbf{s}^{(k)} - \mathbf{y})$ 
4:   次のように変数値を設定する:
        $\mathbf{z} := \ln(\mathbf{r}^{(k+1)}),$ 
        $\mathbf{z}_{-1} := \ln(\mathbf{r}^{(k+1)} - \mathbf{1}),$ 
        $\mathbf{z}_{+1} := \ln(\mathbf{r}^{(k+1)} + \mathbf{1}),$ 
        $\mathbf{w} := \ln(\mathbf{H}^T (\exp(2\mathbf{H}\mathbf{z}) - \exp(\mathbf{H}\mathbf{z})))$ 
5:    $\mathbf{h} := 4 \exp(\mathbf{z}_{-1} + \mathbf{z} + \mathbf{z}_{+1}) + 2 \exp(\mathbf{w} - \mathbf{z})$ 
6:    $\mathbf{s}^{(k+1)} := \mathbf{r}^{(k+1)} - \gamma \mathbf{h}$ 
7: end for
8:  $\hat{\mathbf{x}} := \text{sign}(\mathbf{s}^{(K)})$ 
9: Output  $\hat{\mathbf{x}}$ 

```

この場合、雑音がガウス雑音であることからゆー度関数は

$$p(\mathbf{y}|\mathbf{x}) = a \exp(-b\|\mathbf{y} - \mathbf{A}\mathbf{x}\|^2) \quad (42)$$

という形となる。したがって、この通信路に対応する近似 MAP 復号則は、

$$\hat{\mathbf{x}} \equiv \underset{\mathbf{x} \in \mathbb{R}^n}{\operatorname{argmin}} \frac{1}{2} \|\mathbf{y} - \mathbf{A}\mathbf{x}\|^2 + \gamma h(\mathbf{x}) \quad (43)$$

となる。

この最適化問題の目的関数は、スパース信号再現問題における LASSO 最適化と同様の構造をもっている。この最適化問題から、直ちに近接勾配復号法の反復式が

$$\mathbf{r}^{(k+1)} = \mathbf{s}^{(k)} - \omega \mathbf{A}^T (\mathbf{A} \mathbf{s}^{(k)} - \mathbf{y}) \quad (44)$$

$$\mathbf{s}^{(k+1)} = \mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)}) \quad (45)$$

と求められる。AWGN 通信路の場合と同様にテンソル計算ベ-

(注13): 消費電力削減の観点から、ビットフリップング復号法と min-sum 復号法からなる多段復号法は実用的にフラッシュメモリの誤り訂正などで実際に利用されている。

(注14): 主論文⁽⁸⁾で議論されているように通常の複素 MIMO 通信路モデルは、ここで説明する実数 MIMO 通信路モデルに容易に変換可能である⁽³³⁾。

ス近接勾配復号法の手続きを Algorithm 3 に示す。AWGN 通信路での手続きとの違いは 3 行めの勾配更新ステップのみである。この勾配更新ステップもテンソル計算可能であるため、復号処理全体でもテンソル計算が可能である^(注15)。

主論文⁽⁸⁾では、この LDPC 符号 MIMO 通信路における計算機実験を行っている。近接勾配復号法は、MMSE 検出器とビリーフプロパゲーション復号法よりも優れた復号性能を発揮しており、既存手法と比較しても競争力をもつことが示されている。計算機実験の詳細については同論文⁽⁸⁾を参照されたい。

5.3 非線形ベクトル通信路モデル

無線通信において、例えばパワーアンプの非線形性、PAPR 改善用クリッピングなどが適用される通信路においては、 $\mathbf{y} = f(\mathbf{x}) + \mathbf{w}$ といった非線形関数 $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ の影響が含まれる通信路もある。ここで、 $\mathbf{w}$ は加法的白色ガウス雑音である。このような通信路に対する復号問題は一般には容易ではないが、近接勾配復号法の場合には対応が可能である。

この場合の近接勾配復号法の反復式は

$$\mathbf{r}^{(k+1)} = \mathbf{s}^{(k)} - \omega \nabla \|\mathbf{y} - f(\mathbf{s}^{(k)})\|^2 \quad (46)$$

$$\mathbf{s}^{(k+1)} = \mathbf{r}^{(k+1)} - \gamma \nabla h(\mathbf{r}^{(k+1)}) \quad (47)$$

という形になる。ここで問題となるのは、 $\nabla \|\mathbf{y} - f(\mathbf{s}^{(k)})\|^2$ の評価が計算量的に容易にできるか否か、という点である。

まず簡単な場合としてコンポーネントワイズ非線形性のケースを考える。すなわち、 $f(\mathbf{x}) \equiv g(\mathbf{A}\mathbf{x})$ と書ける場合について考える。ここで、 $g: \mathbb{R} \rightarrow \mathbb{R}$ は想定される非線形関数 (例えばクリッピング関数) であり、コンポーネントワイズに引数に作用するものとする。この場合は、微分の連鎖則から

$$\frac{1}{2} \nabla \|\mathbf{y} - g(\mathbf{A}\mathbf{x})\|^2 = -\mathbf{A}^T ((\mathbf{y} - g(\mathbf{A}\mathbf{x})) \odot g'(\mathbf{A}\mathbf{x})) \quad (48)$$

となる。ここで、演算子 $\odot$ はアダマール積を表す。関数 g と g' の要素ごとの適用が効率よく計算できるならば、この勾配ベクトルはテンソル基礎演算と g と g' の要素ごとの適用により計算できる^(注16)⁽³⁴⁾、⁽³⁵⁾。

より一般的なケースを考える。いま、 $f(\mathbf{x})$ が数学的な意味で $\mathbf{x}$ について微分可能であり、かつ自動微分機構⁽³²⁾により十分に効率的に勾配計算が可能であるものと仮定しよう。例えば、 $f(\mathbf{x})$ が深層ニューラルネットワークで表現されているようなケースである。そのような場合は、近接勾配復号法の復号途中において、誤差逆伝播法などの自動微分機構により、勾配ベクトル $\nabla \|\mathbf{y} - f(\mathbf{x})\|^2$ を計算することが可能である。通信路の物理モデルがプログラム化できるケースにおいてもこの方法が利用できる。

(注15): テンソル計算ベース近接勾配復号法の実装例として、魏 藍天氏による PyTorch 実装が https://github.com/wadayama/proximal_dec にて公開されているので、実装に興味をおもちの方はそちらをご参照頂きたい。

(注16): 複素関数の場合は、ウィルティンガー微分⁽³⁴⁾の連鎖則を利用するため、異なる形となる。詳しくは文献(35)を参照されたい。

通信路がニューラルネットワークとしてモデル化できるケースについて、主論文⁽⁸⁾では実験結果が示されている。

6. 今後の研究に関する展望

本節では、近接勾配復号法に関する今後の研究の方向性について論じる。

6.1 復号過程に関する理解の深化

近接勾配復号法は、対象とする符号クラスとして LDPC 符号を想定している。これは、復号実験の結果、密な検査行列をもつ符号の場合には、復号性能が不十分であるという観察結果に基づいている。この傾向はビリーフプロパゲーション復号法の傾向とよく似ている。近接勾配復号法の目的関数は、多峰性の非凸関数であることから、復号プロセスにおいて非符号語停留点に探索点が捕捉されてしまうことがある。これが、近接勾配復号法が ML 復号法と比較した場合の性能劣化要因になっている。検査行列の密度が高い符号の方が、この捕捉イベントが頻繁に生じるものと考えられているが、より踏み込んだ理論的考察を進める必要があると考えられる。

復号失敗の原因に関する理論的な理解を深めることは、近接勾配復号法の復号性能の向上に役に立つ可能性がある。例えば、文献⁽³⁶⁾では、近接勾配復号法と類似した手法において、冗長検査行列が復号性能の向上に有効であるという実験結果が示されている。これは、復号に利用する検査行列に、もとの検査行列の行ベクトルの線形結合となる冗長行を追加することにより非符号語停留点の数が減少するものと解釈されている。また、Noisy GDBF 復号法⁽¹⁴⁾のように停留点からの脱出を行うための復号手順の追加も一つの方策である。

また、現時点では、近接勾配復号法は、LDPC 符号のみを対象としているが上述の対策が功を奏する状況になれば、より広いクラスの符号への適用を考えていくことも自然である。例えば、ポーラ符号に対応できる近接勾配復号法の開発なども興味深いテーマである。

6.2 深層展開に基づく内部パラメータの最適化

近接勾配復号法はテンソル計算フレンドリであり、そのため深層学習的技法⁽³⁷⁾、⁽³⁸⁾と相性がよい。まず第一に考えられる方向性は、深層展開⁽⁹⁾、⁽³⁹⁾、⁽⁴⁰⁾、⁽⁵⁵⁾の適用である。

深層展開 (deep unfolding) (図 6) は、反復アルゴリズムに対してモデルベース深層学習技術の考え方を適用したアルゴリズム構成のための方法論である。反復アルゴリズムの信号処理プロセスを時間方向に展開することで、深層ニューラルネットワークモデルに類似したネットワークモデルが得られる。確率的勾配法やミニバッチ学習法などの標準的な深層学習技術を適用することで、反復型アルゴリズムの内部の学習可能パラメータを調整することが可能となる。

近接勾配復号法は、ステップサイズとして ω と γ の二つのパ

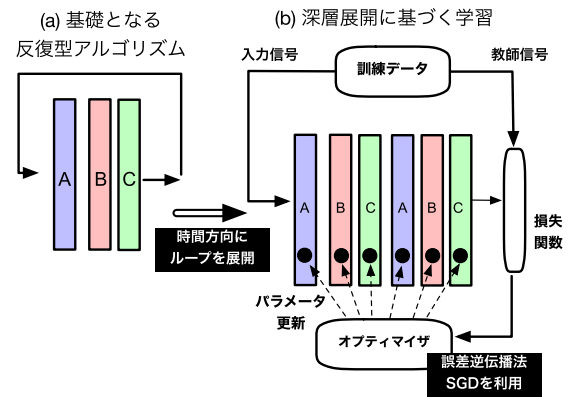


図 6 深層展開による内部パラメータ最適化 反復型アルゴリズムの内部パラメータを確率的勾配法 (SGD) や誤差逆伝播法を利用して最適化する。

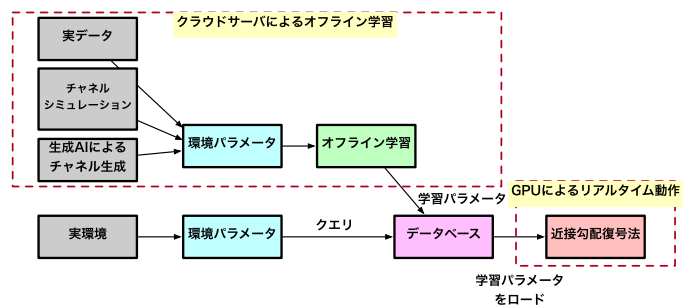


図 7 検索拡張学習のアイデア オフライン学習により学習可能パラメータを学習しデータベースに保存する。リアルタイム処理においては、データベースから学習済みパラメータをロードする。

ラメータを内部に含んでいる。これらのパラメータを適切に設定することで、近接勾配復号法は十分な復号性能を発揮するが、そのためには事前実験などによるパラメータ選択の必要がある。

反復インデックスに依存する学習可能パラメータ $\omega^{(k)}$ 、 $\gamma^{(k)}$ を導入し、これらのパラメータを深層展開に基づき最適化するのは自然な方向性である。例えば、MIMO 通信路の場合、近接勾配復号法の反復式を

$$\mathbf{r}^{(k+1)} = \mathbf{s}^{(k)} - \omega^{(k)} \mathbf{A}^T (\mathbf{A} \mathbf{s}^{(k)} - \mathbf{y}) \quad (49)$$

$$\mathbf{s}^{(k+1)} = \mathbf{r}^{(k+1)} - \gamma^{(k)} \nabla h(\mathbf{r}^{(k+1)}) \quad (50)$$

という形にした上で、学習可能パラメータ $\omega^{(k)}$ 、 $\gamma^{(k)}$ の学習を行う。幾つかの基礎実験で、近接勾配復号法の復号性能の改善と収束の高速化が確認されている⁽⁴¹⁾。

通信路行列や SNR が時間的に変化する通信環境では、それらの変化に伴って学習パラメータの再学習が必要となるが、学習のリアルタイム処理は困難である可能性もある。オフライン学習 (パラメータ学習をクラウドサーバ上で非リアルタイム的に行う) とデータベースを組み合わせる手法⁽⁴²⁾ (検索拡張学習、図 7 参照) などに関して今後の検討が望まれている。

6.3 スコア関数学習に基づく通信路学習

対象とする通信路のゆがみ関数が事前に既知ではなく、デー

タから通信路学習を行う必要がある場合について考える。

ある確率密度関数 $p(\mathbf{x})$ に対して, $s(\mathbf{x}) \equiv \nabla \ln p(\mathbf{x})$ を p のスコア関数と呼ぶ^{(43)~(45)}。スコア関数 $s(\mathbf{x})$ とランジュバンサンプリングを組み合わせることで, $p(\mathbf{x})$ に従う確率変数ベクトルの生成が効率的に可能であることが知られている。最近注目されている拡散モデル⁽⁴⁵⁾においてもスコア関数に基づく生成モデルに興味をもたれている。スコア関数に基づく生成モデルの文脈では, $s(\mathbf{x})$ を近似するニューラルネットワークモデルを与えられたデータから学習し, 学習されたスコア関数に基づきランジュバンサンプリングを行い, $p(\mathbf{x})$ に従うサンプルを出力する。確率密度関数 $p(\mathbf{x})$ そのものをニューラルネットワークでモデル化するよりもスコア関数をニューラルネットワークモデル化⁽⁴³⁾の方がメリットが大きいことが知られている。

もし, 通信路の真のゆ度関数 $p(\mathbf{y}|\mathbf{x})$ が未知である状況で近接勾配復号法を使いたい場合にはゆ度関数そのものの学習モデルを準備するよりも条件付スコア関数 $s(\mathbf{x}; \mathbf{y}) \equiv \nabla \ln p(\mathbf{y}|\mathbf{x})$ をデータから学習した上で, $\nabla L(\mathbf{x}; \mathbf{y}) \equiv -s(\mathbf{x}; \mathbf{y})$ として利用するほうが近接勾配復号法が適切に動作するものと予想される。スコア関数の学習技法 (スコアマッチング法⁽⁴⁵⁾ など) については, 拡散モデルの文脈で精力的に研究が進められており, それらを利用した通信路学習技法が実現できると考えられる。

6.4 連続時間勾配力学系への展開

本稿の最初に述べたように, 近年, プログラマブル光回路に関する研究の進展が著しい。特に MZI を利用した光行列・ベクトル積回路の開発と応用に関する研究が活発に行われている。光回路に基づくアナログコンピューティング⁽⁴⁶⁾は, 超高速・超低消費電力であるため, 大量の計算が必要な分野における活用が期待されている。

大規模なアナログコンピューティングが可能になれば, 常微分方程式

$$\frac{d\mathbf{x}(t)}{dt} = -\nabla f(\mathbf{x}(t)) \quad (51)$$

で定義される勾配流力学系 (gradient flow dynamics)⁽⁴⁷⁾ をフィードバックを含む光回路により実現できる可能性がある。ここで, $f: \mathbb{R}^n \rightarrow \mathbb{R}$ は最小化の対象とする目的関数である。システムの状態 $\mathbf{x}: \mathbb{R} \rightarrow \mathbb{R}^n$ は f の値を最小化するように時間発展する。勾配流力学系は, 勾配降下法の連続時間版であるとみることもできる。凸関数の最小化過程の例を図 8 に示す。

筆者らは, MMSE 信号検出やスパース信号推定を行う連続時間勾配流力学系の研究^{(48), (49)}を進めており, その一環として LDPC 符号の復号を可能とする力学系についても研究を行ってきた^{(20), (36)}。

プログラマブル光回路⁽⁴⁶⁾に基づくアナログコンピューティングを目指した勾配流復号法 (gradient flow 復号法; GF 復号法)⁽²⁰⁾は常微分方程式

$$\frac{d\mathbf{x}(t)}{dt} = -(\mathbf{x}(t) - \mathbf{y} + \nabla h(\mathbf{x})) \quad (52)$$

によって定義される。上の微分方程式の右辺は, AWGN 通

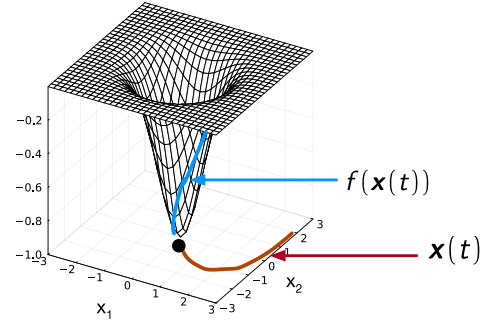


図 8 勾配流力学系における凸関数の最小化過程
 $\mathbf{x}(t)$ は常微分方程式 (51) の解を表す。平衡点は凸関数 f の最小点となる。

信路の負対数ゆ度関数の勾配とポテンシャルエネルギー関数の勾配となっており, 近似 MAP 復号則に現れる目的関数 $L(\mathbf{x}; \mathbf{y}) + \gamma h(\mathbf{x})$ を勾配流ダイナミクスにより最小化するというアイデアに基づいて定められている。原理的には, 積分回路を含むアナログ回路により, この微分方程式の解をシミュレートすることが可能である。

文献(20)では, 微分方程式を解くための数値計算技法であるオイラー法⁽⁴⁷⁾を利用して, 勾配流復号法の AWGN 通信路における復号性能が評価されている。ビリーフプロパゲーション法には及ばないが, GDBF 復号法⁽¹³⁾に近いビット誤り率特性が得られることが実験的に示されている。

連続時間勾配力学系に基づく誤り訂正方式の研究は, ほとんど前例がなく未解決の問題も多い。今後の更なる研究の進展が望まれる。

6.5 分散信号処理との融合

スパース信号再現問題を分散信号処理的に解くアルゴリズムとして CoopIST^{(50), (51)}が知られている。CoopIST は, ISTA に平均合意プロトコル⁽⁵²⁾を組み合わせた一種の分散型近接勾配法と見ることができる。

CoopIST は無向グラフ上で動作するアルゴリズムであり, その反復式は

$$\mathbf{z}_k^{(t+1)} = \sum_{j=1}^K w_{kj} \boldsymbol{\xi}_j^{(t)} \quad (53)$$

$$\boldsymbol{\xi}_k^{(t+1)} = \eta_{s\lambda_k} \left(\mathbf{z}_k^{(t+1)} - \mathbf{s} \mathbf{A}_k^T (\mathbf{A}_k \mathbf{z}_k^{(t+1)} - \mathbf{b}_k) \right) \quad (54)$$

という形をしている。ここで k はノードインデックスを表し, K がグラフに含まれる総ノード数を表す。また, w_{kj} は重みパラメータである。行列 $\mathbf{A}_k$ がノード k に対応する観測行列であり, $\mathbf{b}_k$ がノード k に対応する観測ベクトルである。また, η はソフトしきい値関数である。すなわち, 各ノードで ISTA を実行し, その結果得られた状態ベクトルについてグラフ上で平均合意プロトコルを実行するものと考えられることもできる。

CoopIST から派生した完全分散 MIMO 信号検出アルゴリズムが最近登場している⁽⁵³⁾。これらのアルゴリズムのように近接勾配復号法に CoopIST で利用されている平均合意プロトコ

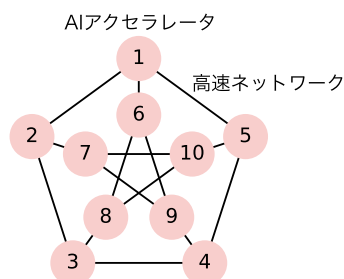


図9 分散近接勾配復号法 の概念 AI アクセラレータは、高速ネットワークを介して、隣接ノードとのみメッセージ (状態ベクトル) 交換を行い、アグリゲーション処理を行う。

ルを容易に組み込むことができる。ノードとして AI アクセラレータ、エッジとしてアクセラレータ間を結ぶ高速ネットワーク (例えば、**InfiniBand**^(注17) など) を利用することで、複数の AI アクセラレータの協調動作を想定した分散型復号アルゴリズム (図9) を実現できると面白い。

7. む す び

本稿では、主論文⁽⁸⁾の内容について特にアルゴリズムの構造と仕組みに焦点を当てて平易に説明するとともに、同論文で十分に説明できていない部分や論文出版後の研究の進展、並びに今後の研究展望も含めて説明を行った。近接勾配復号法はテンソル計算フレンドリであり AI アクセラレータと親和性が高く、深層学習技術の適用も容易である。更に、幅広い通信路モデルへの対応がプラグアンドプレイ的に容易に行える点もほかに類のない特徴である。これらの特徴を活かして、次世代無線通信技術 (6G)、次世代ストレージデバイス、量子誤り訂正符号などの分野での貢献が期待される。

誤り訂正符号とその復号法は、その時代に利用可能な基盤ハードウェア技術に従って発展してきた。小規模 LSI のみが利用可能な時代には代数的符号が重宝され、大規模な ASIC が組める時代には LDPC 符号の復号器を ASIC 実装することが可能となり、LDPC 符号の全盛期が訪れた。今後、我々の周りで利用されるであろう AI 学習・推論処理に適したハードウェアは、生成 AI モデルの学習・推論処理のみならず、幅広い信号処理にも利用できるはずである。AI の進化とともに、その時代のハードウェア環境に適応しつつ誤り訂正符号とその復号法は 21 世紀においても進化し続けるだろう。

謝辞 本研究の一部は、科研費基盤 (A) JP22H00514「深層展開に基づく信号処理アルゴリズム構築論の深化と展開」によりサポートされている。主論文⁽⁸⁾の共著者である東京工業大学の高邊賢史氏からは、本稿の初稿について貴重なコメントを頂戴した。名古屋工業大学の魏 藍天氏からは本稿の初稿について有益なコメントを頂くとともに、本稿のために PyTorch サンプ

ルコードを開発頂いた。ここで改めて御礼申し上げたい。

文 献

- (1) R.G. Gallager, Low Density Parity Check Codes, MIT Press, 1963.
- (2) E. Peltonen, et al., 6G white paper on edge intelligence, 6G Research Visions, no.8, University of Oulu, 2020.
- (3) OpenAI, “GPT-4 technical report,” arXiv:2303.08774v4, 2023.
- (4) A. Reuther, P. Michaleas, M. Jones, V. Gadepally, S. Samsi, and J. Kepner, “AI and ML accelerator survey and trends,” IEEE High Performance Extreme Computing Conference (HPEC), 2022.
- (5) J. Carolan, et al., “Universal linear optics,” Science, vol.349, no.6249, pp.711–716, 2015.
- (6) X. Pengfei and Z. Zhou, “Silicon-based optoelectronics for general-purpose matrix computation: a review,” Advanced Photonics, vol.4, no.4, 044001, 2022.
- (7) H. Zhang, M. Gu, X.D. Jiang, et al., “An optical neural chip for implementing complex-valued neural network,” Nature Commun., vol.12, 2021.
- (8) T. Wadayama and S. Takabe, “Proximal decoding for LDPC codes,” IEICE Trans. Fundamentals, vol.E106-A, no.3, pp.359–367, 2023.
- (9) 和田山正, モデルベース深層学習と深層展開, 森北出版, 2023.
- (10) 内川浩典, “低密度パリティ検査符号 (LDPC 符号),” 信学 FR 誌, vol.14, no.3, pp.217–228, 2021.
- (11) 和田山正, 誤り訂正技術の基礎, 森北出版, 2010.
- (12) D. MacKay, Information Theory, Inference and Learning Algorithms, Cambridge University Press, 2003.
- (13) T. Wadayama, K. Nakamura, M. Yagita, Y. Funahashi, S. Usami, and I. Takumi, “Gradient descent bit flipping algorithms for decoding LDPC codes,” IEEE Trans. Commun., vol.58, no.6, pp.1610–1614, June 2010.
- (14) G. Sundararajan, C. Winstead, and E. Boutillon, “Noisy gradient descent bit-flip decoding for LDPC codes,” IEEE Trans. Commun., vol.62, no.10, pp.3385–3400, 2014.
- (15) J. Feldman, “Decoding error-correcting codes via linear programming,” Ph. D. thesis, Massachusetts Institute of Technology, 2003.
- (16) P.O. Vontobel, “Interior-point algorithms for linear-programming decoding,” IEEE Information Theory and Applications Workshop, 2008.
- (17) T. Wadayama, “Interior point decoding for linear vector channels based on convex optimization,” IEEE Trans. Inf. Theory, vol.56, no.10, pp.4905–4921, 2010.
- (18) X. Zhang and P.H. Siegel, “Efficient iterative LP decoding of LDPC Codes with alternating direction method of multipliers,” IEEE International Symposium on Information Theory (ISIT), 2013.
- (19) S. Barman, X. Liu, S.C. Draper, and B. Recht, “Decomposition methods for large scale LP decoding,” IEEE Trans. Inf. Theory, vol.59, no.12, pp.7870–7886, 2013.
- (20) T. Wadayama, K. Nakajima, and A. Nakai-Kasai, “Gradient flow decoding for LDPC codes,” 2023 International Symposium on Topics in Coding (ISTC2023), Brest, France, 2023.
- (21) N. Parikh and S. Boyd, “Proximal algorithms,” Foundations and Trends in Optimization, vol.1, no.3, Now Publishers, 2013.
- (22) 小野峻佑, “近接分離アルゴリズムとその応用: 信号処理・画像処理の観点から,” オペレーションズ・リサーチ, vol.64, no.6, pp.316–325, 2019.
- (23) D.L. Donoho, “Compressed sensing,” IEEE Trans. Inf. Theory, vol.52, no.4, pp.1289–1306, 2006.
- (24) E.J. Candes and T. Tao, “Near-optimal signal recovery from random projections: universal encoding strategies?,” IEEE Trans. Inf. Theory, vol.52, no.12,

(注17) : NVIDIA の NVlink スイッチでは、SHARP と呼ばれるスイッチ側にアグリゲーション演算をオフローディングする機能がある。CoopIST のように平均合意を用いるのではなくメッセージ平均を SHARP を利用してネットワーク側で実行させるタイプの分散アルゴリズムも実装可能性の点で興味深い。

- pp.5406–5425, 2006.
- (25) I. Daubechies, M. Defrise, and C. De Mol, “An iterative thresholding algorithm for linear inverse problems with a sparsity constraint,” *Comm. Pure and Appl. Math.*, vol.57, no.11, pp.1413–1457, Nov. 2004.
 - (26) R. Tibshirani, “Regression shrinkage and selection via the lasso,” *J. Royal Stat. Society, Series B*, vol.58, pp.267–288, 1996.
 - (27) 和田山正, 高邊賢史, “深層展開に基づく信号処理アルゴリズムの設計,” *信学 FR 誌*, vol.14, no.1, pp.60–72, 2020.
 - (28) D. Ito, S. Takabe, and T. Wadayama, “Trainable ISTA for sparse signal recovery,” *IEEE Trans. Signal Process.*, vol.67, no.12, pp.3113–3125, June 2019.
 - (29) S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
 - (30) 佐野正太郎, 秋葉拓哉, 今村秀明, 太田健, 水野尚人, 柳瀬利彦, *Optuna* によるブラックボックス最適化, オーム社, 2023.
 - (31) T. Wadayama and W. Lantian, “Generalized gradient flow decoding and its tensor-computability,” accepted, *IEEE International Symposium on Information Theory (ISIT)*, 2024.
 - (32) A.G. Baydin, B.A. Pearlmutter, A.A. Radul, and J.M. Siskind, “Automatic differentiation in machine learning: a survey,” *Journal of Machine Learning Research*, vol.18, pp.5595–5637, 2018.
 - (33) 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, July 2019.
 - (34) 林和則, 通信の信号処理: 線形逆問題, 圧縮センシング, 確率推論, ウィルティンガー微分, コロナ社, 2023.
 - (35) S. Takabe and T. Wadayama, “Complex field-trainable ISTA for linear and nonlinear inverse problems,” *IEEE ICASSP*, 2019.
 - (36) T. Wadayama, “Fully analog noise-resilient dynamical systems storing binary sequence,” *IEEE International Symposium on Information Theory (ISIT)*, 2022.
 - (37) I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, The MIT Press, 2016.
 - (38) 岡谷貴之, 深層学習, 改訂第 2 版, 講談社, 2022.
 - (39) K. Gregor and Y. LeCun, “Learning fast approximations of sparse coding,” *Proc. 27th Int. Conf. Machine Learning*, pp.399–406, 2010.
 - (40) A. Balatsoukas-Stimming and C. Studer, “Deep unfolding for communications systems: a survey and some new directions,” in *Proc. IEEE International Workshop on Signal Processing Systems (SiPS)*, pp.266–271, 2019.
 - (41) 伊藤朝陽, “LDPC 符号のための近接勾配復号法に関する研究,” 名古屋工業大学, 卒業研究報告, 2024.
 - (42) W. Lantian, T. Wadayama, and K. Hayashi, “Vector similarity search based offline learning for deep-unfolded MIMO signal detector,” 2024 *IEEE International Conference on Machine Learning for Communication and Networking (ICMLCN)*, accepted, 2024.
 - (43) Y. Song and S. Ermon, “Generative modeling by estimating gradients of the data distribution,” *NeurIPS*, 2019.
 - (44) Y. Song, J. Sohl-Dickstein, D.P. Kingma, A. Kumar, S. Ermon, and B. Poole, “Score-based generative modeling through stochastic differential equations,” *Proceedings of the 10th International Conference on Learning Representations (ICLR)*, pp.399–406, 2021.
 - (45) 岡野原大輔, 拡散モデル データ生成技術の数理, 岩波書店, 2023.
 - (46) J. Capmany and D. Pérez, *Programmable Integrated Photonics*, Oxford University Press, 2020.
 - (47) D.F. Griffiths and D.J. Higham, *Numerical Methods for Ordinary Differential Equations*, Springer, 2010.
 - (48) A. Nakai-Kasai and T. Wadayama, “MMSE signal detection for MIMO systems based on ordinary differential equation,” *IEEE Global Communications Conference (GLOBECOM)*, 2022.
 - (49) T. Wadayama and A. Nakai-Kasai, “Ordinary differential equation-based sparse signal recovery,” *International Symposium on Information Theory and Its Applications (ISITA)*, 2022.
 - (50) 林直樹, 永原正章, “超スマート社会を支える分散スパースモデリング—マルチエージェントネットワーク上のビッグデータ解析—,” *信学 FR 誌*, vol.13, no.2, pp.95–107, 2019.
 - (51) N. Hayashi and M. Nagahara, “Distributed sparse optimization for source localization over diffusion fields with cooperative spatiotemporal sensing,” *Advanced Robotics*, vol.37, no.3, pp.183–197, 2023.
 - (52) 永原正章編著, ネットワーク化制御, コロナ社, 2019.
 - (53) M. Kumagai, T. Wadayama, and A. Nakai-Kasai, “Deep unfolding-assisted fully decentralized projected gradient MIMO detection algorithm,” *IEEE International Conference on Communications (ICC)*, accepted, 2024.
 - (54) M. Prabhu, et al., “Accelerating recurrent Ising machines in photonic integrated circuits,” *Optica*, vol.7, pp.551–558, 2020.
 - (55) V. Monga, Y. Li, and Y.C. Eldar, “Algorithm unrolling: Interpretable, efficient deep learning for signal and image processing,” *arXiv:1912.10557*, 2019.

(IT 研究会提案, 2024 年 2 月 19 日受付,
2024 年 3 月 15 日再受付)



和田山正 (正員: シニア会員)

1993 京都工芸繊維大学大学院修了. 1997 京都工芸繊維大学工博. 1995 岡山県立大学情報工学部助手. 2004 名古屋工業大学大学院工学研究科助教授. 2007 名古屋工業大学大学院工学研究科准教授. 2010 名古屋工業大学大学院工学研究科教授. 2021 年度 FR ベストオファー賞, 2022 年度論文賞受賞. 著書『誤り訂正技術の基礎』『モデルベース深層学習と深層展開』など. 符号理論, 情報理論, 機械学習に基づく信号処理, デジタル通信方式の研究に従事. IEEE 会員.

Decentralized Identifiers (DID) と Verifiable Credentials (VC) の現況

Current Status of Decentralized Identifiers and Verifiable Credentials

鈴木茂哉 Shigeya SUZUKI
富士榮尚寛 Naohiro FUJIE

安田クリスティーナ Kristina YASUDA
阿部涼介 Ryosuke ABE

アブストラクト Decentralized Identifiers (DID) と Verifiable Credentials (VC) は、デジタルアイデンティティの新しい実装形態として注目されている。従来型のデジタルアイデンティティのモデルでは、アイデンティティサービスを提供する主体が、ユーザの同意の元、ユーザ情報を、その情報を必要としている主体に提供していたが、VC によるモデルでは、ユーザ自身が、自身に関する情報を提供できるようになり、デジタルアイデンティティの繊細なコントロールを可能としている。このモデルの中心となるのは、データモデル、非対称鍵暗号、発行・検証プロトコルなどであり、技術開発と標準化が積極的に進められている状況にある。本論文では、VC によるモデルとそれを取りまく検討状況について、背景、標準化、関連プロトコル、応用事例、課題や論点について概説する。

キーワード Decentralized identifiers, DID, Verifiable credentials, VC

Abstract Decentralized identifiers (DIDs) and verifiable credentials (VCs) are attracting attention as a new form of digital identity implementation. The traditional model concentrates on managing and providing user information based on solid trust in the entity providing identity services. The VC model shifts to a model in which the roles of the issuer, holder, verifier are separated. This model allows for fine grained control of digital identities. At the heart of this technology are the DID and VC data models, which are being actively developed and standardized along with various related technologies. This paper outlines the background, standardization, related protocols, application examples, issues, and discussion points regarding this emerging technology.

Key words Decentralized identifiers, DID, Verifiable credentials, VC

1. はじめに

ここ数年、デジタル署名されたデータ活用についての議論が様々な方面でなされている。用いられるのは、非対称鍵暗号を用いたデジタル署名技術であり、1988年にITU-TでX.509⁽¹⁾公開鍵証明書標準の最初の版が批准されて以降、組み合わせられるアルゴリズムは変わってきているが、本質的な部分は変わらない。一方、インターネット及びWebでの情報活用が進化していくに伴い、デジタル証明書の活用が望まれるアプリケーション領域は拡大し続けている状況であり、関連する標準策定

議論などが活発である。

W3C⁽²⁾を中心としたコミュニティで、2014年頃から^(注1)、自己主権型アイデンティティと呼ばれるデジタルアイデンティティのコンセプトと関連する技術についての議論が始まった。デジタルアイデンティティとはサイバー空間中の主体についての情報の集合である^(注2)。これまでは、特定の主体により管理され、主体へ問い合わせることで確認が可能となるモデルが広く使われてきている。自己主権型のデジタルアイデンティティとは、非対称鍵暗号技術などを活用し、特定の主体に管理されることなく、信頼できる主体から独立した状態であっても当該デジタルアイデンティティの正当性を検証可能とすることにより、デジタルアイデンティティを保持あるいはコントロールするユーザにより、より繊細な情報のコントロールできるようにしようというものである。自己主権型アイデンティティ実現の議論の過程で生まれたのが、Issuer (発行者)–Holder (保持者)–Verifier (検証者) という三つの主体間で役割分担するモデル (Three party model と呼ばれる — 本論文では以下 IHV モデルと表記する) であり、このモデルに基づき、用いられるデータをモデル化しようと先陣を切ったのが、Decentralized Identifiers⁽³⁾ (以下、DID) と Verifiable Credentials⁽⁴⁾ (以下、

鈴木茂哉 正員 慶應義塾大学大学院政策・メディア研究科

E-mail shigeya@wide.ad.jp

安田クリスティーナ Federal Agency for Disruptive Innovation, Germany

E-mail kristina.yasuda@sprind.org

富士榮尚寛 伊藤忠テクノソリューションズ株式会社みらい研究所

E-mail naohiro.fujie@ctc-g.co.jp

阿部涼介 慶應義塾大学大学院政策・メディア研究科

E-mail chike@sfc.wide.ad.jp

Shigeya SUZUKI, Member (Graduate School of Media and Governance, Keio University, Fujisawa, Japan), Kristina YASUDA, Nonmember (Federal Agency for Disruptive Innovation, Germany), Naohiro FUJIE, Nonmember (MIRAI Design Laboratory, ITOCHU Techno Solutions Corporation, Japan), Ryosuke ABE, Nonmember (Graduate School of Media and Governance, Keio University, Fujisawa, Japan).

電子情報通信学会 基礎・境界ソサイエティ

Fundamentals Review Vol.18 No.1 pp.42–55 2024 年 7 月

©電子情報通信学会 2024

(注1)：経緯の詳細は 2.4 参照。

(注2)：専門的には属性というが、これについては後のセクションで述べる。

VC) という二つのデータモデル標準である。これらの標準本体のほか、周辺で必要になる標準が策定され、様々な実装が進められている状況にある。日本国内でも、産学官民連携の Trusted Web 推進協議会⁽⁵⁾などにおいて、情報空間におけるトラストを向上するために DID 及び VC 標準を活用しようという取り組みのほか、教育及び職歴証明への活用など、様々な動きがある。

本論文では、この次世代デジタル証明書に関わる技術として、DID と VC 及びこれらの関連技術について解説する。なお、非常に動きが活発な領域であり、本論文執筆を行った時点^(注3)から、今後も変化が続くと見込まれるので、その点ご理解頂ければと思う。以下、DID 及び VC 二つの標準を同時に参照するときは DID/VC と表記する。

まず、2. で、これらの技術の背景について述べる。続けて、3. では、VC 技術について、4. では、DID 技術について解説する。更に、5. では、証明書を保持するウォレットと証明書の交換プロトコルについて解説する。6. では、応用事例について解説し、7. では、現在課題または議論となっている事項について解説する。最後に 8. で、まとめる。

2. 背 景

2.1 デジタルアイデンティティ

デジタルアイデンティティの原始形態は、タイムシェアリングシステムなどでのログイン名とパスワードによるログイン操作によるものだろう。今日でも、ログイン名とパスワードによるログイン操作も用いられているが、パスワードの代わりに非対称鍵暗号を用いるパスキー⁽⁶⁾のような強固な手段が用いられている。

デジタルアイデンティティとは、専門的には、主体に関連づけられた属性の集合⁽⁷⁾と定義されている。ここで属性とは、氏名や年齢といった情報に加え、ログイン ID、パスワードといった情報も含まれる。

我々はスマートフォンや PC などをはじめとした様々な形態のコンピュータを用いている。ユーザは、コンピュータに対してアクセスし、コンピュータが保持している情報とユーザを結びつけるために、ログインを行う。当初、ログインはコンピュータ単位で行われるものであり、コンピュータ単位で登録管理がなされていた。しかし、コンピュータがネットワークで接続され、利用が高度化されるに従って、これらログインのための情報がコンピュータ間で共有されるようになっていった。共有される資源に従い、段階的にアーキテクチャが高度化し、現在では、認可のためフレームワークである OAuth 2.0⁽⁸⁾と、OAuth を下支えとしたアイデンティティレイヤである OpenID Connect⁽⁹⁾が広く使われるようになり、一度の認証で様々なサービスにアクセスできるようになった。

デジタルアイデンティティ技術が活用されるのは、主体に関連付けられた情報の正当性を検証する認証、認証された主体に様々な資源へのアクセス権限を付与する認可、そして、主体

にひもづく属性を必要に応じて活用することである。このような属性と本人のひもづけは、ひもづけされる属性により、何らかの事実確認を行える主体によって発行された、属性証明書として表現できる。

2.2 証明書のデジタル化と高度化

世の中では、様々な証明書が発行され、使われている。技術的な視点だけでいうならば、全ての証明書はデジタル化可能だろう。証明書のデジタル化といっても、幾つかのステップがあり、メリットが異なる。また、証明書のデジタル化における最大のメリットは検証可能であることだが、検証可能な部分は段階的に拡大していく。最近の状況を踏まえ、詳細の議論を省きつつ 6 段階に整理すると、以下のようになるだろう。

- (1) 機械可読化: デジタル化されることで、デジタル的に表示される情報としてだけでなく、コンピュータでデータとして読み取って処理することができるようになる。
- (2) 改竄検知: デジタル署名技術の適用により、内容が改竄されていないことが確認できるようになる。
- (3) 発行者検証: デジタル署名における署名者が誰であるかを確認できれば、証明書発行者をデジタルで検証可能となる。
- (4) 無効化確認: 証明書が無効化されているかどうかを確認できるようになる。
- (5) 複数の証明書の組合せによる総合的な検証: 複数のデジタル化された証明書の組合せが可能となることにより、対象となる本人が提示しているかの確認など、適切に用いられていることが検証可能になる。暗号的に組合せ提示されている場合はより確実な検証が可能となる。
- (6) 証明書提示の高度化: 証明書の必要な部分のみを開示したり、ゼロ知識証明の活用によるプライバシーの高度な保護が可能に。

例えば、(1) の段階のものは、マイクロクレデンシャル提示の技術である Open Badges 1.0^(注4)が相当し、(2)~(4) の段階としては、デジタル署名された PDF による証明書⁽¹⁰⁾が該当し、これらは、ともに、一定程度普及しているといえるだろう。Open Badges 技術も 2.0⁽¹¹⁾でデジタル署名技術が使われるようになったため (2)~(4) の段階となっている。現在では Open Badges 3.0 標準⁽¹²⁾が公開されている^(注5)。DID/VC 技術はプライバシー保護を強く意識して開発されている技術であり、(5)~(6) の段階に至って初めて威力を発揮する。

デジタル化された証明書は、紙に印刷された証明書と同等の情報を記載できるだけでなく、改竄検知可能であり、検証できる対象が拡大していることから、紙に比べて信頼できるものとなりうる。一方、デジタル化された証明書は、集積や情報の統合が容易であり、プライバシー視点でのリスクが紙による証明書よりも高いと考えざるを得ない。そのため、プライバシー

(注3) : 本論文は 2023 年 12 月から 2024 年 3 月初旬にかけて執筆した。

(注4) : 2024/2/29 時点で、オンラインで v1.0 関連の文書を見ることができなかった。

(注5) : Open Badge 3.0 は実際は VC に依存しており、“FINAL” 版が出たあとも更新が継続しているので、“FINAL” という言葉には気をつけたいといけな

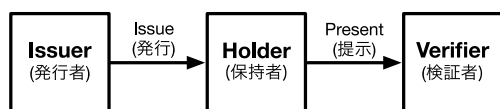


図1 Issuer (発行者)–Holder (保持者)–Verifier (検証者) モデル

の視点でより安全なものとなるよう強く意識して設計されるべきであり、標準策定過程の議論でも、多くの時間がこの点での議論に割かれている。

VC 技術を含め、デジタル化された証明書は、とある Issuer (発行者) によって発行された、対象となる Subject (対象となる主体) に対する何らかの主張 (Claim) の組であると整理できる。更に、最新のデジタル化された証明書技術では、プライバシー上の視点もあり、発行される証明書の Subject に加え、Issuer (発行者)–Holder (保持者)–Verifier (検証者) という三つの主体が役割を分担し連携する IHV モデルがとりいれられている。ここで、Subject ではなく、Holder となっているのには理由がある。例えば、大学の在学生在が本人の在学証明書を発行して保持するときのように、Holder と Subject が一致する場合もあるが、親が子供のパスポートを保持するような場合のように、Holder と Subject が一致しないケースもある。

図1に、IHV モデルにおける役割分担の関係を示す。このモデルでは、Issuer は証明書を発行する主体、Holder は発行された証明書を保持する主体であり、Verifier は提示された証明書を検証する主体である。Issuer によって発行された証明書は、Holder によって保持され、Holder は必要に応じて Verifier に対して証明書を提示する。ここで着目すべき点は、Verifier は Issuer と直接的にやりとりをしない前提となっている点である。これによって Issuer に対して、Holder が、どの Verifier に対して証明書を渡したのかを知られることがなくなり、プライバシー上のリスクを緩和できる。なお、VC 標準では、Issuer–Holder–Verifier という役割分担に加え、これらの主体が Verifiable Data Registry (VDR — 検証可能なデータレジストリ) に対し Identifier (識別子) と Schema (記載事項の形式の定義) について依存するとされている。この関係は後で説明する DID 標準においても同一であるが、7.2で議論するように、VDR の必要性は薄くなっている。

本論文では詳しく取り上げないが、VC と同様の IHV モデルを採用した標準として、モバイル運転免許証 (mDL) 標準である ISO/IEC 18013-5⁽¹³⁾がある。同標準で規定されている mDL のためのフォーマットである mdoc は VC に類似しており、mDL 以外への応用も可能となっている。なお、5.で説明する証明書発行や提示のためのプロトコルは IHV モデルに沿った標準を扱えるデザインとなっており、VC だけでなく mDL もサポートしている。

2.3 自己主権型アイデンティティ

自己主権型アイデンティティ (Self Sovereign Identity — SSI) というキーワードがひと頃話題になっていた。DID/VC 標準化

の議論をしているコミュニティでは、IHV モデルによる議論に重点が移り、あまり自己主権型という言葉が聞かなくなっている。一方、IHV モデルの起源を知るには重要な視点なので、簡単に解説する。

既存のデジタルアイデンティティは、通常、特定のサービスエンティティ — サーバやホストといった計算資源^(注6) — に直接結びついたものであり、それらサービスエンティティに対する制御権限をもっているものが、間接的に、ひもづいたデジタルアイデンティティに対する制御権限をもっているといえる。

例えば、ネット上のサービスにおいて、そのサービスを使う権限は運用者によって管理されている。したがって、そのサービスの利用の可否は、そのサービスを提供している運用者に握られている。何らかの事情で、そのサービスにアクセスを失うことによるインパクトは様々である。デジタルアイデンティティを連携させて使っているような場合は、インパクトは大きいものになり得る。

自己主権型アイデンティティは、誰にも依存せずに自身で制御可能なデジタルアイデンティティのことをいう。ここで、自身で制御できるだけでなく、それを様々な場所で使えるようにならなければ意味がない。

例えば、技術の対比でいうならば、OpenID Connect⁽⁹⁾や SAML⁽¹⁴⁾に代表されるフェデレーション型の技術は、特定のサービスエンティティによって管理されているアイデンティティを、ほかのサービスエンティティでも受け入れよう、というものである。自己主権型の場合は、あるアイデンティティに対する制御権を持つエンティティと、当該アイデンティティが指し示すエンティティとが同一であり、そのアイデンティティが様々なサービスエンティティで受け入れてもらえるようなデザイン、といえる。

自己主権型アイデンティティについて解説するだけでも紙面を相当に要してしまうため、ここでは、Christopher Allen 氏による基本原則を表1に示すに留める。興味がある方は、参考文献⁽¹⁵⁾とビデオ⁽¹⁶⁾をご参照頂きたい。

2.4 DID/VC 標準化の経緯

DID および VC のエコシステムについての議論は、2014 年頃に、W3C と関連するコミュニティを中心として始まっている。経緯については、DID と VC の議論が同時並行的に起きているので、振り返るのはやや困難であるが、大筋と関連したコミュニティやグループとともに述べる。

VC の標準化過程は、2014 年に W3C Credential Community Group⁽¹⁷⁾が成立し、2015 年には Verifiable Claims Task Force がローンチされ、2017 年 5 月には Verifiable Claims Working Group (VCWG)⁽¹⁸⁾にて標準化議論が始まっている。なお、この段階では “Claims” と呼ばれていたが、後に “Credentials” と名称が変更されている。VCWG は、2019 年 11 月に VC v1.0 を勧告、2022 年 3 月に VC v1.1⁽¹⁹⁾を勧告、2022

(注6)：本論文では、主体という語をアイデンティティの議論に用いるが、区別のため、計算資源の結び付いた主体のことをサービスエンティティと表現している。

表 1 Christopher Allen による自己主権型アイデンティティの基本原則 翻訳は鈴木による。

実在	ユーザは独立した存在である。決してデジタルだけでは存在しない
コントロール	ユーザは、自分のアイデンティティ、秘匿性あるいは顕名性を望みに応じてコントロールできなければならない
アクセス	ユーザは自身のデータへのアクセスができなければならない — 門番は存在せず、隠されるものが一切ない
透明性	システムとアルゴリズムはオープンかつ透明性が確保されなければならない
永続性	アイデンティティはユーザが望みに応じ長期にわたり用いることができなければならない
可搬性	アイデンティティに関する情報とサービスはユーザによって移動可能でなければならない
相互接続性	アイデンティティは、越境を許すなど、可能な限り広く利用できるようにすべきである
同意の自由	ユーザは、自分の個人情報がどのように使用されるかの同意について自由であるべきである
最小化	アイデンティティについての主張の開示は最小にとどめるべきである
保護	個々のユーザの権利は、強権をもつ者から保護されなければならない

年 6 月から v2.0 に向けて作業を続けており、2024 年 2 月に勧告候補が公開されたところである。

DID の標準化過程は、DID v1.0⁽³⁾の謝辞のセクションに詳しく記載されている。W3C Web Payment Working Group⁽²⁰⁾を中心とした議論を起点に、XDI.org^(注7)での議論を経て、Rebooting the Web of Trust⁽²¹⁾で初期の議論がなされ、その成果としてホワイトペーパーが公開された⁽²²⁾、⁽²³⁾。関係各氏の議論により、DID 標準の種となる実装へ向けての文書が書かれた⁽²⁴⁾。その後、2019 年に DID Working Group⁽²⁵⁾による標準化が開始され、2022 年 7 月に DID v1.0 が勧告されている。

3. Verifiable Credentials

Verifiable Credentials (VC) は、W3C⁽²⁾によって標準化されている。本論文執筆時で勧告されているのは Verifiable Credentials Data Model v1.1⁽¹⁹⁾であるが、後継バージョンである v2.0⁽⁴⁾の標準策定作業が進行中で、2024 年 2 月時点で Candidate Recommendation (勧告候補) の状態にあり、核となる仕様についてはほぼ確定した状態となっている。本節では、VC v2.0 と周辺事項について解説する。

3.1 VC における Credential

VC における Credential とは、とある Issuer (発行者) によって発行された、対象となる主体 (Subject) に対する何らかの主張 (Claim) の組のことと定義される。これに対し、ISO/IEC 24760-1⁽⁷⁾では、Credential は、アイデンティティの認証のた



図 2 VC の基本要素 Verifiable Credentials 2.0⁽⁴⁾, Figure 5 から。

めの表象 (representation) とされている^(注8)。VC とは、暗号学的な手法により、改竄検知が可能であり、かつ、作成者が誰であるかを検証可能である Credential のこと、すなわち検証可能な証明書のことである^(注9)。

デジタル化された証明書は、集積や情報の統合が容易であり、プライバシー視点でのリスクが紙による証明書よりも高い。そのため、プライバシーの視点でより安全なものとなるようにより強く意識して設計されている。

なお、VC が提供するものは、発行者が記載情報を発行したことにに対し一定の検証ができることであって、記載された情報が真実であるかどうかは示していない。VC を受け取った検証者がその情報及び発行者をどのように扱うか — 真実として受け取るか — は、独自の基準に照らして判断されるものであり、かつ、そのような判断は、証明書に記載された情報を検証できて初めて可能となるものである。

3.2 VC データモデル

VC の構成要素を図示したのが図 2 である。VC は一つあるいは複数の Claim に加え、Credential 自体の識別子や有効期間といった Credential Metadata が付随する。これらに加え、VC が正しいことを示す一つまたは複数の Proof が Issuer によって添付される。すなわち、VC は、発行者によって検証可能な形で示された、改竄検知可能な Claim とメタデータの組である。

VC に準拠した文書 (document) は、なんらかの Securing Mechanism (3.5 にて解説) を適用されることで検証可能な形式となること、すなわち、図 2 における Proof が存在することが必須条件である。一方、Securing Mechanism 適用前の文書が、VC のデータモデル (VCDM と略記される) で定義されている文書となる。いい方をかえると、VCDM 自身は Securing Mechanism とは独立であり、Securing Mechanism によらずに、相互運用性が確保されていることになる。

VCDM に準拠した書類 (conforming document) は JSON-LD 1.1⁽²⁶⁾の compacted フォーマットで表現され、通信時などメディアタイプ⁽²⁷⁾が必要となる場合は、application/vc+ld+json を指定する。VC における共通のボキャブラリについての指示方法と、ボキャブラリの内容については VC 2.0 では標準文書で確定する形となっており、ボキャブラリファイル

(注8) : credential — representation of an identity for use in authentication.

(注9) : 2.2 で示したように、検証可能な部分は適応方法に応じて段階的に拡大する。

(注7) : 2024/2/29 時点でサイトにアクセスできない状況。

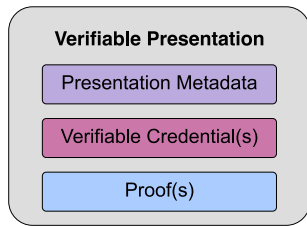


図3 Verifiable Presentationの基本要素 Verifiable Credentials 2.0⁽⁴⁾, Figure 8 から.

のハッシュ値が標準文書に記載される形で徹底されている。このため、JSON-LD 準拠のパースを用いずとも、安全かつ固定的にボキャブラリを用いることができる。一方、インターオペラビリティが限定的にはなるが、JSON-LD 準拠のパースの存在を想定できるエコシステムであれば、JSON-LD 固有の機能を使うことも可能である。

なお、VCDM における国際化多言語化視点での複数言語文字列の指定などは、JSON-LD の機能を用いて実現するようになっている。

3.3 Verifiable Presentations

先に示した VC エコシステムにおいて、Holder から Verifier に対して証明書を提示する際に、VC をそのまま示すこともできるが、提示している Holder が誰であることを示しながら、かつ、複数の VC を合わせて提示する Verifiable Presentation (以下、VP) という形式もある。図3に VP の構成要素を図示する。複数の証明書を組み合わせる VP として提示する場合、通常は同一の Subject のものが組み合わせられるが、必ずしも同一である必要はない。VP には一つあるいは複数の VC とともに Presentation Metadata を含み、VP が正しいことを示す一つまたは複数の Proof が添付される。Proof には提示を行う Holder のものも含まれる。通信時などメディアタイプが必要となる場合は `application/vp+ld+json` を用いる。

3.4 選択的開示

VC の提供する機能のハイライトは、選択的開示 (Selective Disclosure) であろう。選択的開示とは、Verifier に対して示す属性情報を必要最小限に絞るというものである。例えば、運転免許証であれば、運転免許資格があることを示すことができれば充分であり、生年月日を開示する必要はない。提示する情報を最小限に絞りつつ、Issuer から発行され改竄がないことを確認できるのがポイントである。選択的開示は、制限をつければ比較的単純な方法で実装することが可能である。

いずれの場合においても、選択的開示のプロトコルは、用いる暗号プロトコルと属性情報の表現方法を組み合わせた設計が必要である。それぞれについて具体的な提案があるが、表現形式や Securing Mechanism と合わせて議論する必要がある。この後の Securing Mechanism の具体例の解説で合わせて紹介する。

3.5 Securing Mechanism と結果としての Proof

暗号的なメカニズムによって VC あるいは VP が改竄されていないことを示す仕掛けを Securing Mechanism (保護メカニズム) といい、その結果が Proof である。Securing Mechanism には、デジタル署名やゼロ知識証明などといった様々な方法があるが、実装の上では、対象となるデータに加えて、1) 一揃いのソフトウェアを用いることができる状態で、2) 当該ソフトウェアで必要となるプロパティがあり、かつ、3) 当該ソフトウェアの検証 (verification) アルゴリズムによって判定できる状態を確保しなければならない。例えば、デジタル署名を用いる場合は、デジタル署名を検証することになるが、以下の確認が必要である：1) 署名に用いられた鍵にひもづいた検証のために必要となる情報があり、必要な範囲で最新であり、有効であること、2) 署名に用いられた鍵が停止、無効化、期限切れとなっていないこと、3) 暗号的に署名が検証できること、そして、4) そのほか必要な条件が満たされること。

更に、デジタル署名技術を活用する上で最前提の条件は、署名の対象となるデータが署名するときと署名検証するときにビットレベルでの同一性を確保する必要がある点である。これを実現するためには、署名されたデータがやりとりされる経路において、一切変更されないことを担保するか、適切な正規化処理を導入するのが定法である。

W3C の VC エコシステムでは、現時点において、Verifiable Credentials Data Integrity⁽²⁸⁾ (以下、VC-DI) と、Securing Verifiable Credentials using JOSE and COSE⁽²⁹⁾ (以下、VC-JOSE-COSE) の2方式がある。これに加えて、IETF⁽³⁰⁾で議論されている SD-JWT VC⁽³¹⁾や、最近議論が始まった SD-JWT VC DM Credential Format⁽³²⁾がある。W3C で議論されている二つの方式の大きな違いは、先に説明したビットレベル同一性を確保するための方式の違いによる。この後、これらの方式と関連する標準について解説する。

3.5.1 Verifiable Credentials Data Integrity

W3C で策定されている Verifiable Credentials Data Integrity (VC-DI) は、JSON-LD ドキュメントとして表現され、適切な変換 — 正規化あるいはバイナリからテキスト化など — の後、署名結果を JSON-LD のドキュメントの一部に Proof として統合する方法であり、基本的にテキスト形式のフォーマットである。大きな特徴は、データを Linked Data⁽³³⁾として表現できることと、複数の署名者で署名した結果や、複数の署名者が順に署名した結果を含めることができるように、複数の Proof を含められる点である。VC-DI 標準は、署名対象となる JSON-LD オブジェクトに対する操作ステップと、Proof プロパティに記載する事項、Proof の追加操作についての規定が定義されている。なお、仕様上は VC 以外への応用も可能との記載がある。

実装には VC-DI 仕様に加えて、組み合わせる暗号アルゴリズムと適用方法のセットである Cryptosuites の適用が必要である。単純な署名スキームとしては、EdDSA を用いる、Data In-

egrity EdDSA Cryptosuites v1.0⁽³⁴⁾と、ECDSAを用いる、Data Integrity ECDSA Cryptosuites v1.0⁽³⁵⁾がある。そして、ゼロ知識証明系の機能をもつプロトコルであるBBS署名⁽³⁶⁾を用いて選択的開示を実現するBBS Cryptosuite v2023⁽³⁷⁾があり、JSON-LDとRDF⁽³⁸⁾の関係を活かして、高度なゼロ知識証明のメカニズムを導入できる。JSON-LDはRDFのシリアライゼーション形式の一つであるため、RDFとの変換は双方向に行える。VC-DIにおいては、正規化⁽³⁹⁾後に署名される。

3.5.2 Securing Verifiable Credentials Using JOSE and COSE

W3Cで策定されているSecuring Verifiable Credentials using JOSE and COSE⁽²⁹⁾によるスキームは、従来よりIETFのJOSEワーキンググループ⁽⁴⁰⁾で標準化されており、OpenID⁽⁴¹⁾系のプロトコルで運用実績のあるJSON Web Token⁽⁴²⁾由来の方式である。この方式は、正規化によらず、対象となるデータを通信経路で不用意に破壊されることがないようにエンコーディングした上で、署名する方式である。JOSEはテキストベース、COSEはバイナリ方式ともいえる。IETFで標準化されているJSONオブジェクト及びCBORに対する汎用の署名スキームであるJSON Web Signature⁽⁴³⁾とCBOR Object Signing and Encryption⁽⁴⁴⁾を参照する形で標準化されている。これに加え、JWT系列の方式で選択的開示を導入できるSD-JWT⁽⁴⁵⁾方式についても、VC-JOSE-COSEで参照し、標準化されている。

3.5.3 SD-JWT VC DM Credential Format

本論文脱稿直前に、SD-JWT VC DM Credential Format⁽³²⁾という新たなSecuring Mechanismの提案が公開された。SD-JWTや過去に培われたJWTベースのプロトコルに基づきつつ、VC DM 2.0に対応するもので、欧州連合で広く使われているJAdES⁽⁴⁶⁾と組み合わせられることもあり、実装するために必要な要素が全てそろった提案となっている。欧州連合で広く使われる可能性が高いものとなっており、今後の議論の進捗を注視したい。

3.5.4 SD-JWT VC

IETFでは、SD-JWT VC⁽³¹⁾というドラフト文書が提案されている。SD-JWTをベースに、JSONベースの“Verifiable Credential”^(注10)を扱うために、JWTで培われたプロパティについてのルールや拡張方式についての記述など、SD-JWTの仕様では足りない部分を補う形になっている。

3.6 VCにおける無効化状態問い合わせ

Verifierは、VCを検証する際に、対象となるVCがIssuerによって無効化されているかどうかを確認したい場合がある。一方、VerifierからIssuerへの問い合わせが不用意な形で行わ

れると、プライバシー侵害が生じる恐れがある。この問題は、“Phone Home 問題”と呼ばれているが^(注11)、Verifierが証明書の有効性を確認するために、証明書の対象者を識別可能な情報とともにIssuerに問い合わせしまうと、Issuer側が問い合わせ元を識別できるなら、誰が誰の証明書を受け取ったのかをIssuer側に知られることになってしまう。

対策方法の一つは、証明書の有効期限を必要十分な期間に最小化して問い合わせ自体を不要にする方法である。別の提案として検討されているのが、プライバシー漏洩リスクを低減することを指向した、Bitstring Status List v1.0 (以下BSL)⁽⁴⁷⁾という提案である。この仕様では、Issuerが、自身が発行するVCの有効無効を示したビット列をVCとして公開する。VCを発行する際は、BSLの公開場所の情報と、当該証明書の状態を示すビット位置を“credentialStatus”というプロパティとして含めておく。Verifierは、“credentialStatus”プロパティを確認し、BSLを取得し、BSL中のビット位置から当該証明書の状態入手する。ここで、IssuerにはVerifierがBSL中のどのビットを用いたかは分からないので、プライバシー漏洩リスクを下げるができる。なお、BSLが小さいと漏洩リスクを下げるができないので、BSLは最低16Kバイト(131,072ビット)以上と下限を決められている。

なお、プライバシー上の問題はあがるが、既存のCRL⁽¹⁾やOCSP⁽⁴⁸⁾を用いる方法もととり得る。

4. Decentralized Identifiers

Decentralized Identifiers (DIDs)は、新しい方式の識別子についての標準であり、decentralize (非中央化)されたデジタルアイデンティティを構築するための要素技術として登場した。DIDによって、人や組織といった様々な対象を指示することができ、かつ、それら対象自身によって、DIDのコントロールをもっていることを示すことができる。以下、本文中では、記述を明確化するために、Decentralized Identifiers (DIDs)の概念を示す場合は、DIDs、標準を指すときは「DID標準」、DID標準下で定義されている識別子自身を「DID」あるいは「DID (識別子)」と表記する。

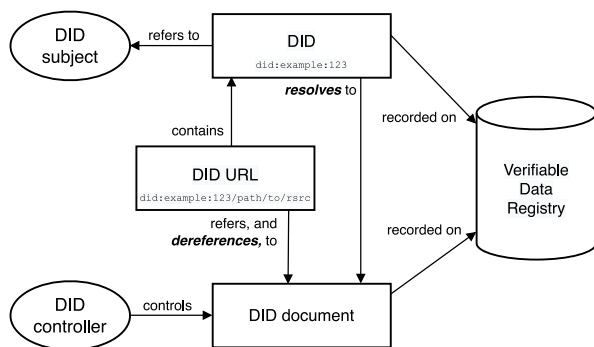
4.1 DID アーキテクチャ

DID標準による抽象アーキテクチャを図4に示す。DIDは、ブロックチェーンやその他の検証可能なデータ登録簿(レジストリ—DID標準ではVerifiable Data Registry)と組み合わせることで、様々な特性をもって実装できる。DIDの実装の詳細はDID Methodという形でカプセル化されている。なお、DIDの最初の“D”はDecentralizedを意味することや、ブロックチェーンでの利用がうたわれていることから、非中央化技術のみが適用可能であるような印象がもたれがちであるが、実際はそのような制約はない。

DID (識別子)は、DIDであることを示すscheme文字列

(注10) : SD-JWT-VCの記述では、IHVモデルを援用するが、W3CのVC 1.0, 1.1, 2.0を仮定しない検証可能な証明書形式、とされている。

(注11) : この表現は、映画E.T.から来ている。



“did:”, DID Method を指定する文字列, DID Method 固有の識別子を示す文字列の三つの要素から構成される文字列で, URI ⁽⁴⁹⁾ の一種である ^(注12)。図 5 にその構成要素を図示し, 説明する。

DID subject は、DID が示している主体のことを示している。

DID document は、DID subject についてのデータセットである。このデータセットには、DID subject により示された主体が DID にひもづいていることを認証するために必要な公開鍵といった情報も含まれる。DID から DID document へ変換する操作を Resolve という。

DID URL は、DID をベースとした URL のことで、Web における URL と同様に、ローカルパスを示す情報と、“?” から始まるクエリパラメータ、“#” から始まるフラグメント記法が使える。フラグメント記法を用いることで、同一 DID document の中のほかの部分を指し示すことができ、鍵の参照などに用いられる。DID URL から DID document、DID document の特定のフラグメント、あるいは外部リソースを得ることを Dereference (参照解除) という。DID controller は、DID document の内容を変更することができる主体のことである。ここで DID controller と DID subject は必ずしも一致しないという点に注意されたい。

Verifiable Data Registry (VDR) は、DID 及び DID document を作成、検証、更新、非活性化することができるシステムである。当初の議論では強くブロックチェーンが意識されていた印象があるが、ブロックチェーンに限らず、何らかの特性が仮定されているわけでもない。DID Method のデザイナは、必要に応じて VDR を選んで実装することになる。did:web のように、DNS を VDR とすることもできる。また、Verifiable とあるが、使われる Method 依存で解釈は大きく変わるだろう。

(注12)：VC v2.0 は DID v1.0 より後で標準化されているが、標準化における過程で、Developer にとって URI と URL の使い分けをするのが困難であるという主張があり、VC では実質的な識別子、つまり URI とすべきところが、あえて URL として表現されており、この点において、二つの標準間で表記が異なっている。

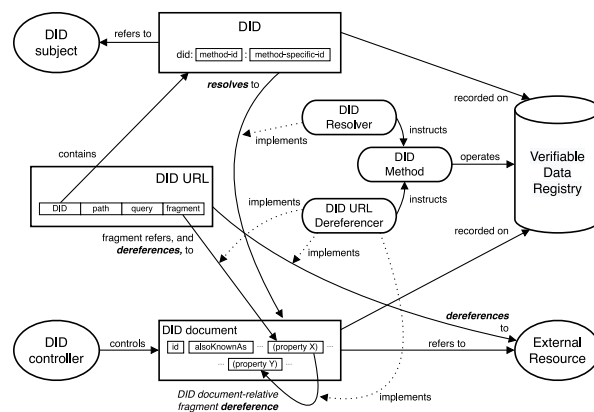


図 6 DID Core 仕様⁽³⁾ Sec.B.1. Detailed Architecture Diagram から。

4.2 DID Method と Resolver, Dereferencer, Universal Resolver

ここまでで明らかなように、DID が実際にどのように実装されるかは、Resolve、Dereference という操作と DID Method の実装次第ということになる。これらの詳細な関係を示したのが図 6 である。DID Resolver は、DID Method と連携し、DID から DID document への変換 (Resolve) を行う。DID Dereferencer は、DID Method と連携し、Web サーバなどといった外部資源への参照へと参照解除 (Dereference) を行う。あるいは、DID に対するフラグメント記法が用いられている場合は、DID document 内を指し示すことになる。

現時点では、DID の Resolve, Dereference とともに、DID Core での抽象的なインターフェースの定義があるだけで、実際にどのようなアルゴリズムで処理されるのかは定義がない。W3C Credential Community Group⁽¹⁷⁾で、これらの操作についての議論が Decentralized Identifier Resolution (DID Resolution)⁽⁵⁰⁾として進んでいる。この文書は現時点では W3C の標準文書となる状態にはないが、DID WG の次の作業に向けての議論 (4.4 参照) においては、将来の標準化に向けて意見調整が進んでいる。

一方、Resolve や Dereference の実行を考えると、Method ごとに呼び出し先を選ぶのではなく、例えば、単一の API 呼び出しで、Method に応じてソフトウェアを呼び分けるようなインターフェースがあれば使いやすいただろう。このような DID Resolve を行うためのサーバとして、多くの DID を Resolve できる Universal Resolver⁽⁵¹⁾が実装されている。本論文執筆時において、61 個のソフトウェア実装が統合されており、DID Resolution 仕様に従った形で、様々な DID を Resolve できる。また、開発用ということで、インターネット上でも公開されており^(注13)、実験的に使うには便利である。なお、クラウドサービスとして提供されていることには、非中央化の視点では議論があり 7.5 で解説する。

(注13) : <https://dev.uniresolver.io/>

に至っていない。

アプリケーション開発者が DID を活用しようとするとき、これだけ DID の実装があると、どれを選ぶのがよいか判断に困るだろう。そのようなユーザのために、DID Method を、様々な特性の見地で整理して、選択の指針とするための文書 DID Method Rubric⁽⁵⁴⁾ が作成されている。ユーザは、この文書を手がかりに用いる DID Method の候補を探すことができる。

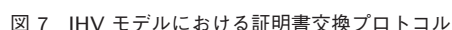
W3C DID ワーキンググループは、DID Core 等一連の文書が承認された後、DID 関連標準のメンテナンスのために準備を始めており、新しいワーキンググループチャータ⁽⁵⁵⁾が準備されつつある。作業内容としては、1) DID Specification Registry の W3C Registry^(注14)への取り込み、2) DID Method Rubric の W3C Registry への取り込み、3) CBOR 形式のサポート、4) 実装者向けガイドの作成、である。更に、DID Resolution と DID URL Dereferencing についてのアルゴリズムとガイドラインを規定した文書の作成が検討されている。先に述べた DID の URL のシンタックスは規定されており、一部のパラメータについては DID Core で文書化されている。一方、後で述べる理由から標準として定義されている DID Method は存在しない。DID Method の実装の自由度が相当に高いこともあり、DID の resolution 及び DID URL の deference について細かく動作を規定するのが難しい状態であったといえる。これらの事情から標準化が検討されている。

(注14)：かつて、W3C では、従来 IANA ⁽⁵⁶⁾ のような登録管理のメカニズムがなかった。W3C で管理することへの取り組みが始まっており、W3C Registry という形で実現されている。 <https://www.w3.org/2023/Process-20231103/#registries>.

ここまで、DID と VC について議論してきた。この節では、VC を含む IHV モデルでやりとりされる証明書の発行と提示にまつわるプロトコルについて解説する。関連するプロトコルを図 7 に示す。なお、この節では、特に説明しないかぎり VC と mDL 双方をサポートできる技術について議論するため、証明書、と表現する。

ソフトウェアとして実体化された Holder に対して Issuer と連携して証明書を取り込むのが、OpenID for Verifiable Credential Issuance (OpenID4VCI)⁽⁵⁸⁾ プロトコルである。保存してある証明書を Verifier に対して提示するプロトコルが、OpenID for Verifiable Presentations (OpenID4VP)⁽⁵⁹⁾ プロトコルである。OpenID4VCI は、異なる形式の証明書を一度にバッチ発行、OpenID4VP は、異なる形式の証明書を同時に提示することができる。例えば、OpenID4VP を用いて VC と mDL を同時に提示することができる⁽⁶⁰⁾。なお、ゼロ知識証明なしでも、複数 Verifier 間の連携によるユーザのトラッキングを防ぐために (unlinkability) 同じ属性データを含むが異なる Holder 制約 (Holder Binding) のための公開鍵を含む VC 証明書のコピーを発行することが OpenID4VP のユースケースの一つである。

また、ウォレットには多数の証明書が保存されている場合があり、その中から人の手で選択するのは煩わしくなることが容易に想像できる。このような多数の証明書がウォレットに入っている場合や、Verifier 側で必要とする条件を指定したいような場合、Presentation Exchange⁽⁶¹⁾ プロトコルを用いることで、必要な証明書をウォレットの中から選ぶことができるようになる。



また、OpenID の環境で純粋に自己主権型のデジタルアイデンティティを活用するために、ウォレットを Identity Provider (OpenID の用語では OpenID Provider — OP) として機能するためのプロトコルがあり、これが、Self-Issued OpenID Provider v2 (SIOP v2) ⁽⁶²⁾ である。

なお、OpenID 系のプロトコルのほかにも、証明書交換のための標準があり、ISO/IEC 18013-5 ⁽¹³⁾ には、証明書提示のためのプロトコルも含まれるが、NFC、Wi-Fi、BLE を具体的に用いるための定義が含まれている。

6. 応用事例

本節では、具体的な証明書の応用例を二つ解説する。なお、DID についてのユースケース ⁽⁶³⁾、VC についてのユースケース ⁽⁶⁴⁾ は、それぞれ W3C のワーキンググループ内文書としてまとまっているので参考にされたい。

6.1 学修歴及び職歴証明書

VC の議論の初期段階から適用領域として議論されているのは、学修歴や職歴の証明書であり、W3C Credential Community Group ⁽¹⁷⁾ の Verifiable Credentials for Education Task Force ⁽⁶⁵⁾ を中心にユースケースなどの議論 ⁽⁶⁶⁾、実装、インターオペラビリティテスト (Plug fest) ⁽⁶⁷⁾ が行われている。このインターオペラビリティテストでは、Open Badges v3 ⁽¹²⁾ と、アメリカ移民局 (USICS) の Identity Document として Citizenship Vocabulary ⁽⁶⁸⁾ に基づいた証明書の提示をする形で実施されている。実装をもつ 24 のプロジェクトが参加しており ⁽⁶⁹⁾、各参加者の結果ビデオが掲載されている。実装がこれだけ進み、インターオペラビリティの確認も進んでいることは意義深い。一方、VC 本体や Open Badges v3 含め様々な標準が確定していない現況であり、実装者にとってはチャンスであるし、利用者にとっては状況を注視すべき状態であるといえる。

なお、文科省の事業でデジタル学修歴についてのシンポジウムが 2 月に行われており著者の 1 人も参加している。資料なども公開される予定なので、参照されたい ⁽⁷⁰⁾。

6.2 コロナワクチン接種証明書

デジタル庁によって提供されたコロナワクチン接種証明書アプリは、VC をベースとした SMART Health Cards 標準 (以下、SHC) ⁽⁷¹⁾ によるものと、VC 標準ベースではない ICAO ^(注15) VDS-NC 標準によるものであった。国外用に VDS-NC と SHC、国内用には SHC が提供されていた ⁽⁷²⁾。SHC 内部のデータモデルは、HL7 FHIR ⁽⁷³⁾ という医療情報交換データモデルに準拠している。Issuer の公開鍵はデジタル庁の Web サイト経由で取得できる、X.509 PKI の自己署名証明書を起点とした複数の証明書が組み合わされている。SHC は Apple の iOS 15 で標準の

ヘルスケアアプリに取り込めるようになっており、実際に取り込むことが可能であった。一方、国際化はされているが多言語化視点で限界のある HL7 FHIR に基づいているがゆえに、訪日外国人の名前の処理には問題があったと聞く。

デジタル庁によるコロナワクチン証明書は 2024 年 3 月末で役割を終え、運用を停止することになっている。非常時の対策としてはあったが、仕様上の様々な問題を明らかにし、先進的なチャレンジとして意義があった。

医療に関する証明書活用場面は非常に広いと考えられ、今後、様々な形での応用が期待される。

7. 課題・議論

ここまで見てきたように、DID/VC に関連する標準は勧告された文書や勧告候補の文書となっているが、その利用経験は不十分である。また、活用するエコシステム全体を通して必要なテクノロジーが揃っている状況ではなく、エコシステムが充分安定的に活用できる状況からはほど遠い。

本節では、現時点での DID/VC エコシステムにまつわる様々な課題や議論について取り上げる。

7.1 ユースケースの多様性とコミュニティの違い

DID や VC の議論、特に標準化のためのワーキンググループで意見がまとまらないことが見受けられる。標準化の議論としては、おなじみの光景ではあるが、今回特に VC については 7.3 に示すように、Securing Mechanism に関連して意見が割れてしまった。これは大変残念なことではあるが、一方、議論に参加している方々の属性を見るに、やむなしともいえる。

これらの議論への参加者を分類すると、デジタルアイデンティティに興味をもつ 1a) 従来型オンライン認証技術系の方々、1b) 自己主権型志向の方々、そして、2) Semantic Web 系の Linked Data, RDF 活用の世界観を推進したいの方々、3) デジタル証明書活用を考えるの方々、と、少なくとも四つのグループが見えてくる。加えて、W3C の議論においては、ブラウザベンダや OS ベンダが影響力をもっている。

それぞれのコミュニティあるいはステークホルダーにおいて、用いる用語、非中央化技術 (decentralization) の適用必要性あるいは重視、求められるシリアルライゼーションの要件、有効期限など様々なパラメータ選択、セキュリティ視点、プライバシー視点、エンジニアリング視点など、様々な要素が、技術的な視点だけでも複雑に絡み合う。更に、様々なガバナンス視点も重要である。このため、標準化の過程において、しばしば、議論が白熱している。

これから標準の議論に参加される方、あるいは、用いる標準を検討される方は、この視点を頭に置くことと意見の差異を理解しやすくなるかもしれない。

(注15) : International Civil Aviation Organization — 国際連合経済社会理事会の専門機関。

7.2 VC における識別子と VDR

IHV モデルを用いた証明書のエコシステムにおいて、Holder についての証明書と Holder が用いる証明書を暗号的に結合 (Cryptographic Holder binding) することが重要である。これを達成するためには、それぞれの主体が鍵ペアをコントロールすることが重要なのであって、用いられる技術は何であってもかまわない。過去の議論においては、必要に応じてそれぞれの主体にひもづく公開鍵を発見する方法の一つとして DID が注目されたが、主体の公開鍵自体をクレデンシャルの中に入れることで十分なユースケースが多いことが分かってきた。そのため、IHV モデルを用いた証明書を実現するのに、DID は必須ではないといえる。このこともあって、DID、ひいては自己主権型アイデンティティという言葉自体が廃れてきている印象がある。

関連する論点として、DID および VC データモデル標準において提示されている Verifiable Data Registry が必要かどうかという議論がある。この語が選ばれているのは、ブロックチェーンをどのように活用するのかという視点が強かったことからいえる。一方、デジタル署名技術を活用すれば検証可能性は担保できること、そのために、検証可能性を VDR に依存する必要は必ずしもないことから、VDR という語が使われていることには疑問がある。

7.3 Securing Mechanism の選択

3. で議論したように、W3C では、Securing Mechanism として二つの方式が提案されている。そのほかに二つの方式が提案されており、それぞれメリットデメリットが異なる。

インターオペラビリティやソフトウェア開発者の負担を考えると、単一の方式が選ばれることが重要であるが、7.1 で議論したように、異なる要求をもつ複数のコミュニティが存在することから、残念ながら仕様が割れてしまった。ここで、一番の論点は JSON-LD ベースであるかどうかであり、もう一つの論点は仕様の上で実装可能な形になっているか、である。

JSON-LD ベースの Data Integrity を推すグループは、JSON-LD で表現されたデータ間のリンク構築に強い重点があり、複雑であっても単一の表現形式に全てを盛り込むことを指向している。更に JSON-LD は RDF との相互変換など、変換処理の組合せに価値を見いだしている。これは単純な入れ子構造になっていないほかの方式では達成できない。

一方、JSON-LD ベースであることから、Data Integrity の実装に対する反対意見は多い。例えば、OpenID の標準が策定される過程での苦い経験の蓄積^(注16)⁽⁷⁴⁾から、やりとりする際のトランスポートメカニズムによってデータが壊されるリスクに対して一部のエンジニアは非常に敏感であり、正規化 (Canonicalization) や正常化 (Normalizaiton) などの変換が多段に組まれることにも不安を感じている。十分なセキュリティ

上の分析があれば不安は解消されるかもしれないが、現時点では存在しない。また、一部の技術者は、JSON-LD が標準化されて長いのに、C で実装されたパーサが存在しない⁽⁷⁵⁾ことで、その複雑さを指摘している。複雑さを示すために具体的な性能評価が実験的に行われてもいる⁽⁷⁶⁾、⁽⁷⁷⁾が、性能評価方式についての反論や一定の緩和策提案もあり、バランスのとれた評価が求められる。エンジニアリング視点でいうならば、デザインや実装における単純さは大きな価値があるともいえ、高度の複雑さをもつ複数の標準とソフトウェアモジュールの連携で高度の柔軟性を目指してデザインされた JSON-LD の価値観とは方向性が異なる。

どの方式を用いるかは、実装できることが大前提となるが、対象となるアプリケーション領域あるいはアプリケーションドメインや活用するコミュニティごとに判断するか、一部の実装で行われているように、複数形式の平行利用という方法をとらざるを得ないだろう。

なお、Data Integrity におけるセールスポイントの一つは BBS 署名⁽³⁶⁾を用いたリンク可能性を排除した選択的開示プロトコルの存在がいわれており、研究⁽⁷⁸⁾や実装⁽⁷⁹⁾があるが、VC JOSE COSE 系のプロトコルに BBS 署名や CL 署名⁽⁸⁰⁾を組み合わせる方法も検討されつつあり、この点での差は近い将来なくなるかもしれない。

7.4 発行者視点か受取人視点か

様々な証明書のデジタル化における議論において、証明書を発行する側の視点に比較的重点があるように見受けられる。そのため、証明書の消費者側の視点がやや軽んじられているのではないかという疑念がある。特に、発行者が誰であり、どのような立ち位置で証明書を発行しているのかといったことを繊細に突き詰めて検討すると、発行者に対して適用されている Trust Framework が何であるかに対し、検証者が、その Trust Framework を信頼できるのかといった課題があることが見えてくる。

例えば、欧州連合内の大学が発行した証明書を日本の大学が検証しようとする、日本の大学は欧州連合で用いられている Trust Framework に依存しないと検証できないはずである。検証者側が何を信じるのか、運用視点で考える必要があるだろう。

したがって、検証者視点でも検討することは重要である。

7.5 非中央化 (decentralization) の追求

先の 7.1 で議論したように、非中央化 (decentralization) を強く指向するコミュニティがあり、また、Web3 のような非中央化指向の議論があるなか、DID は、重要な技術の一つとして捉えられている。

一方、非中央性を忠実に実現するのは困難である。非中央化された環境での検証可能性について細かく見ていくと、いかに確実に信頼できる環境で処理をするのか、それとも、クラウドサービスのようなものに頼るのか、方針によってとり得る手段

(注16) : OpenID Summit 2024 でのパネルディスカッションプレゼンテーション資料⁽⁷⁴⁾参照。

はかなり違ってくる。先述の DID Resolution における DID document の読み出しの議論では、“verifiable read” (検証可能な読み出し) と “unverifiable read” (検証不可能な読み出し) とを区別して議論している⁽⁵⁰⁾。

例えば、Bitcoin を VDR として用いる “did:btcr” は、非中央性に拘りがなければクラウド上のサービスに依存することで簡単に実装できる。しかし、真の非中央化を目指すのであれば、Resolve するソフトウェアが実行される環境で Bitcoin フルノードを動作させる必要があるだろう。完全に非中央化された環境で、どのような Method も Resolve できるようにするのは非常にコスト高であり現実的でない。

したがって、現時点では、現実的な解は、DID を活用しようとするコミュニティの中での要求を見定め、DID Method Rubric⁽⁵⁴⁾を参照しながら適切な DID を少数選び、必要な非中央性を実現できる環境を構築することだろう。

8. 終わりに

本論文では、Decentralized Identifiers と Verifiable Credentials という二つのデータモデル標準を中心に、実装に必要な関連標準について、現在非常に早いスピードで議論や開発の進むエコシステムを概観できるように解説した。

デジタルアイデンティティはインターネット活用においてなくてはならない技術であり、そのなかでも、VC を中心とした技術により、エンドユーザにとってより自分の情報をコントロールできるような技術革新が起きている。特に欧州連合では eIDAS 2.0 指令⁽⁸¹⁾が 2024 年 2 月に承認され、DID/VC 標準よりもシンプルな標準を求めて Digital Identity Wallet (EUDIW) の設計⁽⁸²⁾と実装⁽⁸³⁾が進んでおり、採用された SD-JWT VC などの標準の実装経験が急速に蓄積されていよいよ具体的な活用が進むことが期待される。

様々なコミュニティやコミュニティが入り乱れて、非常に早いスピードで議論が進んでいることもあり、本論文はあくまでも執筆時のスナップショットにすぎないが、読者のエコシステムへの理解の一助となれば幸いである。

文 献

- (1) S. Boeyen, S. Santesson, T. Polk, R. Housley, S. Farrell, and D. Cooper, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” RFC 5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>, (online) 2024/2/29.
- (2) “World Wide Web Consortium (W3C),” <https://www.w3.org/>, (online) 2024/2/29.
- (3) M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, “Decentralized Identifiers (DIDs) v1.0,” W3C Recommendation, July 2022, <https://www.w3.org/TR/did-core/>, (online) 2024/2/29.
- (4) M. Sporny, T. Thibodeau Jr., I. Herman, M.B. Jones, and G. Cohen, “Verifiable Credentials Data Model v2.0,” W3C Candidate Recommendation Draft, Feb. 2024, <https://www.w3.org/TR/vc-data-model-2.0/>, (online) 2024/2/29.
- (5) “Trusted Web 推進協議会,” <https://trustedweb.go.jp/>, (online) 2024/2/29.
- (6) “パスキー (パスキー 認証),” <https://fidoalliance.org/passkeys/?lang=ja>, (online) 2024/2/29.
- (7) International Organization for Standardization and International Electrotechnical Committee (ISO/IEC), “ISO/IEC 24760-1:2019 IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts,” <https://www.iso.org/standard/77582.html>, 2019.
- (8) D. Hardt, “The OAuth 2.0 Authorization Framework,” RFC 6749, Oct. 2012, <https://www.rfc-editor.org/info/rfc6749>, (online) 2024/2/29.
- (9) N. Sakimura, J. Bradley, M. Jones, B. deMedeiros, and C. Mortimore, “OpenID Connect Core 1.0 incorporating errata set 2,” Dec. 2023, https://openid.net/specs/openid-connect-core-1_0.html, (online) 2024/2/29.
- (10) Adobe Corporation, “Digital Signature in a PDF,” https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in.PDF.pdf, (online) 2024/2/29.
- (11) IMS Global, “Open Badge v2.0 IMS Final Release,” April 2018, <https://www.imsglobal.org/spec/ob/v2p0/>, (online) 2024/2/29.
- (12) 1EdTech, “Open Badge Specification – Candidate Final Public Spec Version 3.0,” Jan. 2024, <https://www.imsglobal.org/spec/ob/v3p0/>, (online) 2024/2/29.
- (13) International Organization for Standardization and International Electrotechnical Committee (ISO/IEC), “ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving license – Part 5: Mobile driving license (mDL) application,” <https://www.iso.org/standard/69084.html>, 2021.
- (14) OASIS Open, “Security Assertion Markup Language (SAML) v2.0,” March 2005, <https://www.oasis-open.org/standard/saml/>, (online), 2024/3/8.
- (15) C. Allen, “The Path to Self-Sovereign Identity,” April 2016, <https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>, (online) 2024/2/29.
- (16) C. Allen, “Self-Sovereign Identity: Ideology and Architecture – Christopher Allen – Webinar 51,” March 2020, <https://ssimeetup.org/self-sovereign-identity-why-we-here-christopher-allen-webinar-51/>, (online) 2024/2/29.
- (17) “W3C Credentials Community Group (CCG),” <https://www.w3.org/community/credentials/>, (online) 2024/2/29.
- (18) “W3C Verifiable Credentials Working Group,” <https://www.w3.org/2017/vc/WG/>, (online) 2024/2/29.
- (19) M. Sporny, D. Longley, and D. Chadwick, “Verifiable Credentials Data Model v1.1,” W3C Recommendation, March 2022, <https://www.w3.org/TR/vc-data-model/>, (online) 2024/2/29.
- (20) “W3C Web Payments Working Group,” <https://www.w3.org/Payments/WG/>, (online) 2024/2/29.
- (21) “Rebooting the Web of Trust,” <https://weboftrust.info/>, (online) 2024/2/29.
- (22) C. Allen, A. Brock, V. Buterin, J. Callas, D. Dorje, C. Lundkvist, P. Kravchenko, J. Nelson, D. Reed, M. Sabadello, G. Slepak, N. Thorp, and H.T. Wood, “Decentralized Public Key Infrastructure,” Dec. 2015, <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>, (online) 2024/2/29.
- (23) D. Reed and L. Chasen, “Requirements for DIDs,” Aug. 2016, <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>, (online) 2024/2/29.

- (24) D. Reed, L. Chasen, C. Allen, and R. Grant, "Requirements for DIDs," Nov. 2016, <https://github.com/WebOfTrustInfo/rwot1-sf/blob/master/final-documents/dpki.pdf>, (online) 2024/2/29.
- (25) "W3C Decentralized Identifier Working Group," <https://www.w3.org/2019/did-wg/>, (online) 2024/2/29.
- (26) G. Kellogg, P.-A. Champin, and D. Longley, "JSON-LD 1.1," W3C Recommendation, July 2020, <https://www.w3.org/TR/json-ld11/>, (online) 2024/2/29.
- (27) N. Freed, D.J.C. Klensin, and T. Hansen, "Media Type Specifications and Registration Procedures," RFC 6838, Jan. 2013, <https://www.rfc-editor.org/info/rfc6838>, (online) 2024/2/29.
- (28) M. Sporny, D. Longley, G. Bernstein, D. Zagidulin, and S. Crane, "Verifiable Credential Data Integrity 1.0," W3C Candidate Recommendation Draft, Feb. 2024, <https://www.w3.org/TR/vc-data-integrity/>, (online) 2024/2/29.
- (29) M. Jones, M. Prorock, and G. Cohen, "Securing Verifiable Credentials using JOSE and COSE," W3C Candidate Recommendation Draft, Feb. 2024, <https://www.w3.org/TR/vc-jose-cose/>, (online) 2024/2/29.
- (30) "Internet Engineering Task Force (IETF)," <https://www.ietf.org/>, (online) 2024/2/29.
- (31) O. Terbu, D. Fett, and B. Campbell, "SD-JWT-based Verifiable Credentials (SD-JWT VC)," Internet-Draft draft-ietf-oauth-sd-jwt-vc-03, Internet Engineering Task Force, March 2024, Work in Progress, <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/03/>, (online) 2024/3/6.
- (32) A. Horvat, O. Terbu, and D. Fett, "SD-JWT VC DM Credential Format," Work in Progress, <https://github.com/danielfett/sd-jwt-vc-dm>, (online) 2024/2/29.
- (33) T. Berners-Lee, "Linked Data," Personal Note, <https://www.w3.org/DesignIssues/LinkedData.html>, (online) 2024/2/29.
- (34) M. Sporny, D. Zagidulin, G. Bernstein, and S. Crane, "Data Integrity EdDSA Cryptosuites v1.0," W3C Candidate Recommendation Draft, Dec. 2023, <https://www.w3.org/TR/vc-di-eddsa/>, (online) 2024/2/29.
- (35) M. Sporny, M. Reed, G. Bernstein, and S. Crane, "Data Integrity ECDSA Cryptosuites v1.0," W3C Candidate Recommendation Draft, Feb. 2024, <https://www.w3.org/TR/vc-di-ecdsa/>, (online) 2024/2/29.
- (36) T. Looker, V. Kalos, A. Whitehead, and M. Lodder, "The BBS Signature Scheme," Internet-Draft draft-irtf-cfrg-bbs-signatures-05, Internet Engineering Task Force, Dec. 2023, Work in Progress, <https://datatracker.ietf.org/doc/draft-irtf-cfrg-bbs-signatures/05/>, (online) 2024/2/29.
- (37) G. Bernstein and M. Sporny, "BBS Cryptosuite v2023," W3C Working Draft, Feb. 2024, <https://www.w3.org/TR/vc-di-bbs/>, (online) 2024/2/29.
- (38) R. Cyganiak, D. Wood, and M. Lanthaler, "RDF 1.1 Concepts and Abstract Syntax," W3C Recommendation, Feb. 2014, <https://www.w3.org/TR/rdf11-concepts/>, (online) 2024/2/29.
- (39) D. Longley, G. Kellogg, and D. Yamamoto, "RDF Dataset Canonicalization," W3C Candidate Recommendation, Dec. 2023, <https://www.w3.org/TR/rdf-canon/>, (online) 2024/2/29.
- (40) "Javascript Object Signing and Encryption (jose) Working Group," <https://datatracker.ietf.org/wg/jose/about/>, (online) 2024/2/29.
- (41) "Open ID Foundation," <https://openid.net/>, (online) 2024/2/29.
- (42) M.B. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," RFC 7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>, (online) 2024/2/29.
- (43) M.B. Jones, J. Bradley, and N. Sakimura, "JSON Web Signature (JWS)," RFC 7515, May 2015, <https://www.rfc-editor.org/info/rfc7515>, (online) 2024/2/29.
- (44) J. Schaad, "CBOR Object Signing and Encryption (COSE): Structures and Process," RFC 9052, Aug. 2022, <https://www.rfc-editor.org/info/rfc9052>, (online) 2024/2/29.
- (45) D. Fett, K. Yasuda, and B. Campbell, "Selective Disclosure for JWTs (SD-JWT)," Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-08, Internet Engineering Task Force, March 2024, Work in Progress, <https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/08/>, (online) 2024/3/6.
- (46) European Telecommunications Standards Institute, "Electronic Signatures and Infrastructures (ESI); JAdES digital signatures; Part 1: Building blocks and JAdES baseline signatures," 2021, https://www.etsi.org/deliver/etsi_ts/119100.119199/11918201/01.01.01.60/ts_11918201v010101p.pdf, online, 2024/2/29.
- (47) M. Sporny, D. Longley, M. Prorock, and M. Alkhraishi, "SBitstring Status List v1.0," W3C Workign Draft, Feb. 2024, <https://www.w3.org/TR/vc-bitstring-status-list/>, (online) 2024/2/29.
- (48) S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and D.C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP," RFC 6960, June 2013, <https://www.rfc-editor.org/info/rfc6960>, (online) 2024/3/12.
- (49) T. Berners-Lee, R.T. Fielding, and L.M. Masinter, "Uniform Resource Identifier (URI): Generic Syntax," RFC 3986, Jan. 2005, <https://www.rfc-editor.org/info/rfc3986>, (online), 2024/2/29.
- (50) M. Sabadello and D. Zagidulin, "Decentralized Identifier Resolution (DID Resolution) v0.3," W3C Community Group Report, Jan. 2023, <https://w3c-ccg.github.io/did-resolution/>, (online) 2024/2/29.
- (51) "Universal Resolver," <https://github.com/decentralized-identity/universal-resolver>, (online) 2024/2/29.
- (52) O. Steele and M. Sporny, "DID Specification Registries," W3C Group note, Sept. 2023, <https://www.w3.org/TR/did-spec-registries/>, (online) 2024/2/29.
- (53) O. Steele, S. Suzuki, M. Sporny, and M. Sabadello, "DID Core Specification Test Suite and Implementation Report," Aug. 2023, <https://www.w3.org/TR/did-test-suite/>, (online) 2024/2/29.
- (54) J. Andrieu, R. Grant, and D. Hardman, "DID Method Rubric v1.0," W3C Group note, Nov. 2021, <https://www.w3.org/TR/did-rubric/>, (online) 2024/2/29.
- (55) "PROPOSED Decentralized Identifier Working Group Charter," <https://w3c.github.io/charter-drafts/2023/did-wg.html>, (online) 2024/2/29.
- (56) "Internet Assigned Numbers Authority (IANA)," <https://www.iana.org/>, (online) 2024/2/29.
- (57) "DID 1.0 Comments," Sept. 2021, <https://www.w3.org/2021/09/21-did10-minutes.html>, (online) 2024/2/29.
- (58) T. Lodderstedt, K. Yasuda, and T. Looker, "OpenID for Verifiable Credential Issuance - draft 13," OpenID Draft openid4vci-draft13, OpenID Foundation, Feb. 2024, <https://openid.net/specs/openid-4-verifiable-credential-issuance-1.0.html>, (online) 2024/2/29.
- (59) O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker, "OpenID for Verifiable Presentations - draft 20,"

OpenID Draft openid4vp-draft20, OpenID Foundation, Nov. 2023, <https://openid.net/specs/openid-4-verifiable-presentations-1.0.html>, (online) 2024/2/29.

- (60) 川崎貴彦, “eIDAS 2.0 でサポート必須の SD-JWT VC フォーマットと mdoc/mDL フォーマットの Verifiable Credential を同時に発行してみた (たぶん世界初),” Jan. 2024, <https://qiita.com/TakahikoKawasaki/items/c2fb84fec9ec11765fc8>, (online) 2024/2/29.
- (61) “Presentation Exchange 2.0.0,” <https://identity.foundation/presentation-exchange/spec/v2.0.0/>, (online) 2024/2/29.
- (62) K. Yasuda, M. Jones, and T. Lodderstedt, “Self-Issued OpenID Provider v2 - draft 13,” OpenID Draft SIOPv2-draft20, OpenID Foundation, Nov. 2023, <https://openid.net/specs/openid-connect-self-issued-v2-1.0.html>, (online) 2024/2/29.
- (63) J. Andrieu and P. Archer, “Use Cases and Requirements for Decentralized Identifiers,” W3C Group note, Sept. 2019, <https://www.w3.org/TR/did-use-cases/>, (online) 2024/2/29.
- (64) S. McCarron, J. Andrieu, M. Stone, T. Siegmán, and J. Gregg Kellogg and Ted Thibodeau, “Verifiable Credentials Use Cases,” W3C Group note, Nov. 2021, <https://www.w3.org/TR/vc-use-cases/>, (online) 2024/2/29.
- (65) “Verifiable Credentials for Education Task Force,” <https://w3c-ccg.github.io/vc-ed/>, (online) 2024/2/29.
- (66) S. Ravaioli, D. Everhart, J. Kuo, J. Pozmanter, P. Long, and W. Teter, “Verifiable Credentials for Education, Employment, and Achievement Use Cases,” Draft Community Group Report, Sept. 2022, <https://w3c-ccg.github.io/vc-ed-use-cases/>, (online) 2024/2/29.
- (67) “JFF & VC-EDU Interoperability Plugfest 3,” July through October 2023, <https://w3c-ccg.github.io/vc-ed/plugfest-3-2023/>, (online) 2024/2/29.
- (68) M. Sporny, M. Varley, and M. Sabadello, “Verifiable Credentials for Education, Employment, and Achievement Use Cases,” Draft Community Group Report, Dec. 2023, <https://w3c-ccg.github.io/citizenship-vocab/>, (online) 2024/2/29.
- (69) “JFF & VC-EDU Interoperability Plugfest 3 – Participants,” 2023, <https://w3c-ccg.github.io/vc-ed/plugfest-3-2023/participants.html>, (online) 2024/2/29.
- (70) “文部科学省 令和 5 年度 先導的大学改革推進委託事業「大学等における学修歴証明書のデジタル化の導入及び普及展開に関する調査研究」デジタル学修歴シンポジウム,” 2024, <https://www.nttbizsol.jp/event/202312130900000969.html>, (online) 2024/2/29.
- (71) “SMART Health Cards,” <https://smarthealth.cards/en/>, (online) 2024/2/29.
- (72) デジタル庁, “新型コロナワクチン接種証明書アプリ,” 新型コロナウイルスワクチン接種証明書アプリ, (online) 2024/2/29.
- (73) “HL7 FHIR,” <https://www.hl7.org/fhir/>, (online) 2024/2/29.
- (74) M. Jones, “Celebrating Ten Years of OpenID Connect at the OpenID Summit Tokyo 2024,” Jan. 2024, <https://self-issued.info/?p=2481>, (online) 2024/2/29.
- (75) “JSON-LD – Developers,” <https://json-ld.org/#developers>, (online) 2024/2/29.
- (76) “decanonicalization,” Data Integrity and JSON Web Signature computation time comparison, Sample Graph: <https://or13.github.io/decanonicalization/>, Source: <https://github.com/OR13/decanonicalization>, (online) 2024/3/10.
- (77) “Selective Disclosure Benchmark,” <https://transmute-industries.github.io/vc-jwt-sd/>, (online) 2024/3/12.
- (78) D. Yamamoto, Y. Suga, and K. Sako, “Formalising Linked-Data based Verifiable Credentials for Selec-

tive Disclosure,” 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp.52–65, 2022.

- (79) 森田航平, 渡邊健, 井上瑠威, 佐古和恵, “指名者による本人特定機能付き Verifiable Presentation,” 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2023–CSEC–102, 47, July 2022.
- (80) J. Camenisch and A. Lysyanskaya, “A signature scheme with efficient protocols,” Security in Communication Networks, Third International Conference, SCN 2002, Amalfi, Italy, September 11–13, 2002; Revised Papers, eds. by S. Cimato, C. Galdi, and G. Persiano, vol.2576, pp.268–289, Lecture Notes in Computer Science, Springer, 2002, https://doi.org/10.1007/3-540-36413-7_20.
- (81) “Electronic Identification, Authentication and Trust Services (eIDAS) Regulation,” <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>, (online) 2024/3/10.
- (82) “European Digital Identity Architecture and Reference Framework – Outline,” <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>, (online) 2024/3/10.
- (83) “EUDI Wallet Reference Implementation,” <https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework>, (online) 2024/3/10.

(BioX 研究会提案, 2024 年 3 月 12 日受付,

2024 年 4 月 12 日再受付)



鈴木茂哉 (正員)

情報システム研究者及びエンジニア。コンピュータネットワーク, サイバーセキュリティ, 量子情報システム, DNS を含む名前管理システム, 及び, 実空間情報システムの研究に従事。システムアーキテクト, ソフトウェア開発についてのエキスパート。現在, 慶應義塾大学大学院政策・メディア研究科特任教授。博士(政策・メディア)。慶應義塾大学 SFC 研究所データアーキテクトチャラボ副代表。WIDE プロジェクト運営委員。Trusted Web 推進協議会タスクフォースメンバー。Originator Profile 技術研究組合技術 WG 部会長。W3C DID 及び VC WG メンバー。ACM, IACR, IEEE, IEICE, IPSJ 会員。



安田クリスチーナ

パリ政治学院主席卒業。2016 年に米 NGO 「InternetBar.org」ディレクターに就任し, 途上国における身分証明インフラを整備するデジタル・アイデンティティ事業を新設。2017 年にアクセントュアの戦略コンサルティング本部に新卒入社。2019 年にマイクロソフト・コーポレーションに転職し, Identity アーキテクトとして分散型 ID を含む Identity 規格の国際標準化に取り組む。2024 年から, ドイツの Federal Agency of Disruptive Innovation で欧州連合のデジタルアイデンティティウォレットのプロジェクトに関わる。2019 年, Forbes Japan 30Under30 に選出。2021 年, MIT テクノロジーレビューの Innovators under 35 に選出。



富士榮尚寛

20 年以上にわたりデジタルアイデンティティ分野で活動しており、グローバル規模の認証基盤の導入にかかるコンサルティングやアーキテクトの経験をもつ。2018 年より OpenID ファウンデーションジャパンの理事～代表理事として OpenID/OAuth をはじめとするデジタルアイデンティティ関連技術の普及啓発に従事している。Trusted Web 推進協議会タスクフォースメンバ、OpenID Foundation eKYC&Identity Assurance WG 共同議長。慶應義塾大学 SFC 研究所所員。国立情報学研究所次世代認証連携検討作業部会メンバー、伊藤忠テクノソリューションズ株式会社みらい研究所所長。



阿部涼介

慶應義塾大学政策・メディア研究科特任助教。同研究科修士課程卒 (修士 (政策・メディア))。2022 年 3 月同大学同研究科博士課程単位取得退学。2022 年 4 月より現職。2016 年よりブロックチェーンの応用及び基盤拡張の研究に従事。2022 年 3 月より WIDE プロジェクトボードメンバー、2023 年 4 月より Trusted Web 推進協議会タスクフォースメンバ。ACM 及び IPSJ 会員。

医用超音波分野における ビームフォーミング技術

Beamforming Methods in the Field of Medical Ultrasonics

長谷川英之 Hideyuki HASEGAWA

アブストラクト 遅延和 (delay-and-sum : DAS) ビームフォーミングは、超音波アレープローブのトランスデューサ素子から得られたエコー信号を使用して超音波断層像 (B モード画像) を生成するために広く使用されている。しかし、遅延和ビームフォーミングによって得られる空間分解能とコントラストは、素子間隔などアレーの物理的な仕様によって制限される。このような制約を克服するために、最近ではデジタル及びプログラマブルな超音波システムの普及を受けて、適応型ビームフォーミングなどが活発に研究開発されている。一方で、開発された方法によって画像の特性が改善されているかどうかを定量的に評価することも重要である。現在、多くの適応型ビームフォーミング法が開発されており、これらはしばしば超音波画像の特性を変化させる。そのため、画質の定量的評価方法を改良する試みも行われている。この記事では、主に適応型ビームフォーミングと画質評価法の最近の展開について解説する。

キーワード ビームフォーミング, 医用超音波画像

Abstract Delay-and-sum (DAS) beamforming is widely used to generate B-mode images using the echo signals obtained from transducer elements of ultrasound array probes. However, the spatial resolution and contrast provided by DAS beamforming are limited by the physical specifications of the array such as element spacing. To overcome such constraints, adaptive beamforming techniques have been actively researched and developed, particularly with the proliferation of digital and programmable ultrasound systems in recent years. On the other hand, it is also important to quantitatively evaluate whether the methods developed improve the characteristics of images. Recently, many adaptive beamforming techniques, which often alter the characteristics of ultrasound images, have been developed. Therefore, efforts have been made to improve quantitative methods for assessing image quality. In this article, we primarily review recent developments in adaptive beamforming and image quality evaluation methods.

Key words beamforming, medical ultrasonic images

1. はじめに

この記事ではまず、医用超音波画像を得るためのビームフォーミング処理について簡単に説明し、次に、伝統的な適応型ビームフォーミング法について解説する⁽¹⁾。これらの手法は、空間分解能、コントラスト、コントラスト対雑音比 (CNR) などの画質評価指標を変化させる。更に、伝統的な適応型ビームフォーミング法の制約についても取り上げ、それらの画質をより適切に評価するために最近開発された新しい評価指標についても説明する。最後に、伝統的な適応型ビームフォーミング法の制約を克服しようとする最新の研究についても紹介する。本稿は文献(1)の内容に、本分野のその後の進展などを追加したものである。

2. 静的なビームフォーミング

ビームフォーミングは超音波画像を生成するための不可欠なプロセスである。ビームフォーミング処理は送信時に超音波音場を制御するためにも重要であるが、この記事では受信時のビームフォーミング処理を中心に解説する。遅延和 (DAS) ビームフォーミングは、臨床で使用されている超音波診断装置で広く用いられている。図1に示されるように、遅延和ビームフォーミングは、関心点 (焦点) からのエコー信号を推定しようとする処理である。焦点を設定することにより、ビームフォーミングは伝搬媒質内の音速を仮定し、焦点と各素子との間の超音波伝搬時間を推定する。推定された伝搬時間に基づいて個々の素子で受信したエコー信号 (素子信号) を遅延させることにより、焦点からのエコーは位相が揃い、その結果、それらを加算することで焦点からのエコー信号は増大する。一方、焦点外からのエコー信号は位相が揃わないため、加算することにより抑圧される。遅延和ビームフォーミング処理は式(1)のように表現される。

長谷川英之 正員：シニア会員 富山大学学術研究部工学系
E-mail hasegawa@eng.u-toyama.ac.jp
Hideyuki HASEGAWA, Senior Member (Faculty of Engineering, University of Toyama, Toyama-shi, Japan).
電子情報通信学会 基礎・境界サイエンス
Fundamentals Review Vol.18 No.1 pp.56-70 2024 年 7 月
©電子情報通信学会 2024

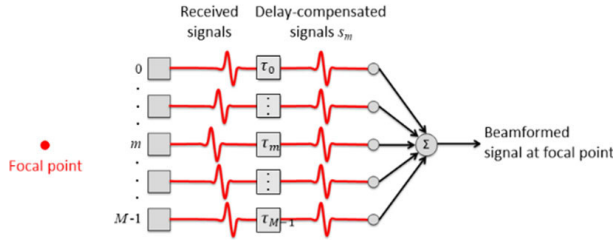


図1 DAS ビームフォーミングの説明図⁽¹⁾

$$p_{DAS} = \frac{1}{M} \sum_{m=0}^{M-1} s_m \quad (1)$$

ここで、 p_{DAS} は遅延和ビームフォーマの出力であり、 s_m は m 番目の素子で受信された遅延相殺後 RF (radio-frequency) エコー信号である (素子信号とよぶ)。また、 M は受信開口内の素子数を示す。遅延和ビームフォーマの空間分解能は開口の寸法に依存するが、実際には有限な開口寸法と素子間隔の超音波プローブを使用するため、サイドローブとグレーティングローブを完全に抑圧することはできない。

非線形ビームフォーマである delay-multiply-and-sum (DMAS) ビームフォーマは、乳がんのマイクロ波イメージングを目的に開発され⁽²⁾、後に医用超音波イメージングにも導入された^{(3), (4)}。DMAS ビームフォーマの出力は式(2)で表される。

$$p_{DMAS} = \sum_{i=1}^{M-1} \sum_{j=i+1}^M \text{sign}(s_i \cdot s_j) \cdot \sqrt{|s_i \cdot s_j|} \quad (2)$$

DMAS ビームフォーマの出力において、信号の乗算により直流成分と $2f_0$ 成分 (f_0 は s_m の中心周波数) が発生する。したがって、ビームフォーマの最終出力を取得するためには、バンドパスフィルタが必要である。

$$p_{FDMAS} = \text{BPF}[p_{DMAS}] \quad (3)$$

ここで、 $\text{BPF}[\cdot]$ はバンドパスフィルタを表す。このビームフォーマは、filtered delay-multiply-and-sum (FDMAS) ビームフォーマとよばれる。FDMAS ビームフォーマは、信号コヒーレンスの評価に対応する相関演算を含むため、不要信号を抑圧し遅延和ビームフォーマと比較して優れた空間分解能とコントラストを実現する⁽³⁾。また、素子信号のコヒーレンスをもとに式(2)の変数 j の範囲を制限することで適応的にビームフォーマ出力を制御する手法も開発されている⁽⁵⁾。FDMAS 法はまた、平面波イメージングにおけるコヒーレントコンパウンドにも適用されている^{(6)~(8)}。同様な手法として、振幅を非線形に変換した素子信号どうしの畳み込み演算によりビームフォーミングを行う手法も開発されており⁽⁹⁾、DAS に比較して方位分解能の向上とサイドローブレベルの低下が確認されている。

3. アポダイゼーション

式(1)で定義される遅延和ビームフォーマは広く用いられ

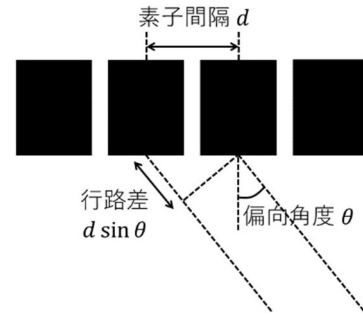


図2 遠距離近似した場合の素子位置による音波の伝搬路差の説明図

ているが、実際には各素子で受信した信号に重みを付けるアポダイゼーションとよばれる処理が行われる。各素子での受信信号を、周波数 f_0 の複素正弦波で表現し、図2のように遠距離音場を仮定すると、角度 θ に指向性を形成する場合の遅延和ビームフォーミング処理は式(3)で表すことができる。

$$p_{DAS}(\theta, \phi) = \sum_{m=0}^{M-1} s_m(\phi) e^{-j2\pi m d \sin \theta / \lambda} \quad (3)$$

ここで、 d 、 λ 、 ϕ はそれぞれ、素子間隔、超音波の波長、受信信号の到来方向である。式(3)は、 $\sin \theta / \lambda = f_x$ 、 $x_m = md$ とおくと式(4)で表される。

$$p_{DAS}(\theta, \phi) = \sum_{m=0}^{M-1} s_m(\phi) e^{-j2\pi f_x x_m} \quad (4)$$

式(4)は、各素子で受信した信号 $s_m(\phi)$ の素子位置 x_m に関するフーリエ変換とみなすことができる。また、音波の到来方向 ϕ を用いて、各素子での受信信号は式(5)で表される。

$$s_m(\phi) = s_m(0) e^{j2\pi f_{x0} x_m} \quad (5)$$

ここで、 $f_{x0} = \sin \phi / \lambda$ である。 $s_m(0)$ は音波の到来方向が $\phi = 0$ の場合の各素子での受信信号であるから、遠距離近似の場合は全ての素子で同時に到来波を受信することとなり、その振幅 (素子の受信感度に対応) を 1 とすると、 $s_m(0)$ ($m=0, 1, \dots, M-1$) は全て 1 となる。したがって、式(4)は $f_x = f_{x0}$ のとき、つまり $\theta = \phi$ でピークとなり、それがメインローブとなる。そう考えると、受信信号振幅 $s_m(0)$ はフーリエ変換における窓関数 (重み関数) であるとみなすことができる。フーリエ変換では、解析対象信号を切り出す窓関数の周波数特性はよく知られており、矩形窓ではメインローブに対し第 1 サイドローブの振幅は -15 dB 程度である。これは十分低いようにも思えるが、医用超音波イメージングでは組織からのエコー信号に対して 40 dB 程度も小さい血球からのエコー信号など微弱なエコー信号も解析対象となるため、ハニング窓などのテーパ窓がしばしば用いられる (フーリエ変換におけるハニング窓の第 1 サイドローブレベルはメインローブの -30 dB 程度)。テーパ窓の導入により、サイドローブレベルが低下して不要エコー信号が減少し画像のコントラストが改善するが、方位分解能は劣化する。これもフーリエ変換においてハニング窓のメインローブ幅が矩形窓

のメインローブより広いことと同義であると考えることができる。このように素子ごとの受信信号振幅の方位分解能への影響を考えることができるが、実際の超音波振動子アレーでは素子の受信感度はできる限り均一化されるため、受信感度を変更する代わりに受信信号の処理の段階で重み w_m を導入し式(6)で表現する。

$$p_{DAS} = \frac{1}{M} \sum_{m=0}^{M-1} w_m s_m \quad (6)$$

この重み付け処理はアボダイゼーションと呼ばれる。なお、送信においてもアボダイゼーションはしばしば用いられ、その際には各素子への印加信号の振幅を調整する。

現在の超音波診断装置では、各素子で受信した信号は即座に離散化されるため、アボダイゼーション処理を非常に柔軟に行うことができる。式(6)はRF信号に対する処理であるが、異なるアボダイゼーションを用いて式(6)により得られるRF信号の包絡線を加減算することにより方位分解能を向上させるとともにサイドローブレベルを低下させる手法⁽¹⁰⁾、全開口内に複数の小開口を設けてアボダイゼーションを適用し、それら小開口からの出力をインコヒーレントに加算することによりスペックルを低減する手法⁽¹¹⁾、平面波イメージングにおいて発生する距離方向の不要信号を抑圧するため受信焦点から離れた素子の信号の重みを低減する手法⁽¹²⁾などが提案されている。文献(10)の手法は、異なる偏向角度の平面波を合成する平面波コンパウンド法⁽¹³⁾において複数の偏向角度で得られた信号の重み付けにも用いられている⁽¹⁴⁾。

4. 適応的なイメージング方法

遅延和ビームフォーマの制約を克服するために、受信信号に依存して性能が変化する様々な適応型イメージング方法が導入されてきた。多くのイメージング方法が開発されているため、この記事では幾つかの代表的な方法を解説する。

4.1 信号の相関性を用いた適応的イメージング法

生体組織内の音速の不均一な分布による位相収差が超音波画像の品質を低下させる。位相収差による画質の低下を評価するために、コヒーレンスファクタ (CF)^{(15)~(17)}が開発された。これは、受信信号に含まれるコヒーレントなエネルギーと総受信エネルギーの比として式(7)で定義される⁽¹³⁾。

$$CF = \frac{\left| \frac{1}{M} \sum_{m=0}^{M-1} \tilde{s}_m \right|^2}{\frac{1}{M} \sum_{m=0}^{M-1} |\tilde{s}_m|^2} \quad (7)$$

ここで、 $\tilde{s}_m$ は受信開口内の m 番めの素子で受信された遅延相殺後RF信号の複素解析信号である。P. C. Li と M. L. Li は、CFによって遅延和ビームフォーミング後信号を重み付けすることで不要信号を抑圧する手法を提案した⁽¹⁸⁾。

$$p_{CF} = CF \cdot p_{DAS} \quad (8)$$

ここで、 p_{CF} はCFによる重み付けを用いたビームフォーマ出力である。超音波画像の空間分解能とコントラストは、インコヒーレントな成分を抑圧することによって向上する。素子信号間のコヒーレンスは、素子信号の位相を使用することによっても評価されており、phase coherence factor (PCF) とよばれる^{(19)~(21)}。

$$PCF = 1 - \frac{\beta \gamma}{\sigma_0} \cdot \sigma \quad (9)$$

ここで、 σ は素子信号の位相の標準偏差、 σ_0 は位相が $-\pi$ から π まで一様に分布する場合の標準偏差であり、 $\sigma_0 = \pi/3^{1/2}$ である。また、 β はPCFの効果を制御するパラメータである。

PCFはアレー振動子の各素子の解析信号を求め、その位相を評価する必要があるため、DAS法と比較して演算量が多くなる。受信信号の位相は、受信した超音波パルスの極性に対応しているため、受信した実数信号の符号のみでコヒーレンスを評価するのがsign coherence factor (SCF)であり、式(10)で定義される。

$$SCF = 1 - \sqrt{1 - \left\{ \frac{1}{M} \sum_{m=0}^{M-1} b_m \right\}^2} \quad (10)$$

ここで、 b_m は素子信号の符号である (-1 若しくは $+1$)。

CFと同様に、インコヒーレントな信号は、式(8)と同じ方法で遅延和ビームフォーミング後信号にPCFを重み付けすることによって抑制できる。

式(7)に示されているように、完全にコヒーレントな信号のCFは1になり、逆に完全にインコヒーレントな信号のCFは0となるため、両者のCFの差は1に制限される。コヒーレントな信号とインコヒーレントな信号の差を更大きくするために、mean-to-standard deviation (MSD) ファクタ⁽²²⁾とsignal-to-noise ratio (SNR) ファクタ⁽²³⁾が導入された。CFはコヒーレントなエネルギーと「受信総エネルギー」の比として定義されているため、完全にコヒーレントな信号に対するCF値は1に制限される。一方、MSD及びSNRファクタは、完全にコヒーレントな信号に対して無限大となる。ただし、信号の無限大の増幅はビームフォーマの出力を不安定にするため、式(11)に示されるようにSNRファクタでは安定化が導入されている⁽²³⁾。

$$SNR = \frac{|\tilde{p}_{DAS}|^2}{\frac{1}{M} \sum_{m=0}^{M-1} |\tilde{p}_m - \tilde{p}_{DAS}|^2 - \gamma \cdot |\tilde{p}_{DAS}|^2} \quad (11)$$

ここで、 γ は安定化パラメータであり、 $\tilde{p}_{DAS}$ は素子RF信号の複素解析信号を使用して得られた遅延和ビームフォーマの出力である。式(11)の分子は式(7)の分子と同様である。SNRファクタで重み付けたビームフォーマ出力 p_{SNR} は、式(8)に示されているCF重み付けと同じ方法で得られる。コヒーレンス系の指標は、空間内の各点に対して複数回の送信を加算する開口合成法において、同一点に対する複数回の送

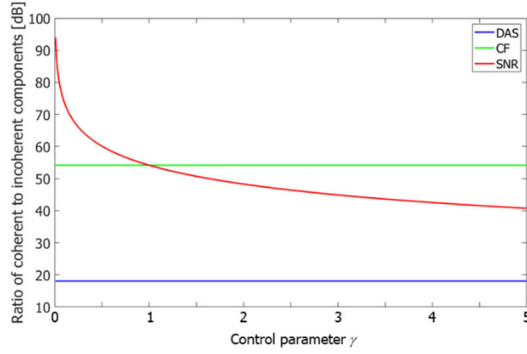


図3 各ビームフォーマ出力におけるコヒーレントとインコヒーレントな成分の理論パワー比⁽¹⁾

受信データからコヒーレンス指標を算出して加算後の信号を重み付けることにより、送信ごとに変動の大きい不要信号を抑圧することもできる⁽²⁴⁾。

MSD または SNR ファクタを用いて遅延和ビームフォーミング後信号に重みを付けることで、CF と比較してコヒーレントとインコヒーレントな成分間のコントラストを高めることができる。特に、 γ がゼロの場合、SNR ファクタを使用するとコヒーレントとインコヒーレントな信号の差が無限に拡大する。ただし、実際には開口寸法が有限であるため、無限大の増幅が行われることはないと考えられる。各ビームフォーマの出力におけるコヒーレントとインコヒーレントな成分のパワー比率は式(12)～(14)式のように表される⁽²³⁾。

$$R_{DAS} = M \left| \frac{p}{\sigma_n} \right|^2 \quad (12)$$

$$R_{CF} = M^3 \left| \frac{p}{\sigma_n} \right|^2 \quad (13)$$

$$R_{SNR} = \frac{M|M+(\gamma-1)|^2}{\gamma^2} \left| \frac{p}{\sigma_n} \right|^2 \quad (14)$$

ここで、 R_{DAS} 、 R_{CF} 、及び R_{SNR} は、DAS ビームフォーマ、CF 重み付きの DAS ビームフォーマ、及び SNR ファクタによる重み付き DAS ビームフォーマの出力パワー比率で、 M は受信開口内の素子数、 p は焦点からのエコーの振幅、 ρ_n は雑音の平均振幅である。図3は、式(12)～(14)において M を 64 に設定して得られた、コヒーレントな成分とインコヒーレントな成分の理論的な比率を示している。図3にプロットされている値は、 $|p/\rho_n|^2$ で正規化されており、SNR factor の安定化パラメータ γ の最小値は 0.01 に設定されている。図3から分かるように、CF 及び SNR factor は、コヒーレントな成分とインコヒーレントな成分の差を大幅に増加させる。 $\gamma=1$ の場合、SNR factor は CF と同一である。CF と比較して $\gamma<1$ の場合、SNR factor はコヒーレントな成分とインコヒーレントな成分の比率を増大させる。

4.2 適応ビームフォーミング

最小分散 (minimum variance: MV) ビームフォーマ^{(25)～(32)}は、適応ビームフォーミングの代表的な方法である。DAS ビームフォーミングでは、素子信号に重みを適用するアポダイゼーションが一般的に使用され、サイドローブレベルを低下させる効果がある。一方、MV ビームフォーマは、受信した素子信号に応じて重みを適応的に決定する。これは DAS ビームフォーミングにおけるアポダイゼーション重みは固定であるのと異なる。また、DAS ビームフォーミングのアポダイゼーション重みは、素子信号の振幅のみを制御する実数値である。一方、MV ビームフォーミングの重みは複素数値であり、MV ビームフォーマは素子信号に適用される時間遅延も制御し、出力パワーを最小にしながらし望ましい方向（焦点）に対する全域通過特性を保持する。この問題は以下のように表現される。まず、素子信号をベクトル形式で表す。

$$\tilde{\mathbf{s}} = [\tilde{s}_0 \ \tilde{s}_1 \ \tilde{s}_2 \ \cdots \ \tilde{s}_{M-1}]^T \quad (15)$$

ここで、 T は転置を示す。ビームフォーマの重み w_m もベクトル形式で表すことができる。

$$\mathbf{w} = [w_0 \ w_1 \ w_2 \ \cdots \ w_{M-1}]^T \quad (16)$$

MV ビームフォーマの出力は $p_{MV} = \mathbf{w}^H \cdot \tilde{\mathbf{s}}$ と表されるため、MV ビームフォーマの出力パワーの期待値は式(17)で表現される。

$$E[p_{MV}^2] = \mathbf{w}^H E[\tilde{\mathbf{s}}\tilde{\mathbf{s}}^H] \mathbf{w} = \mathbf{w}^H \mathbf{R} \mathbf{w} \quad (17)$$

ここで、 H 、 $E[\cdot]$ 、及び $\mathbf{R}$ はそれぞれ、共役転置、期待値、及び共分散行列を示す。この最小化問題は式(18)のように表現される。

$$\begin{aligned} \hat{\mathbf{w}}_{MV} &= \arg \min_{\mathbf{w}} E[|\mathbf{w}\tilde{\mathbf{s}}|^2] = \arg \min_{\mathbf{w}} \mathbf{w}^H \mathbf{R} \mathbf{w} \\ \text{subject to } \mathbf{w}^H \mathbf{a} &= 1 \end{aligned} \quad (18)$$

ここで、 $\mathbf{a}$ はステアリングベクトルである。この問題の解は以下のように与えられる。

$$\hat{\mathbf{w}}_{MV} = \frac{\mathbf{R}^{-1} \mathbf{a}}{\mathbf{a}^H \mathbf{R}^{-1} \mathbf{a}} \quad (19)$$

ステアリングベクトル $\mathbf{a}$ は、素子と焦点との間の超音波伝搬距離の違いによる素子信号の時間遅延の差を補償した場合、全ての成分が 1 のベクトルとなる。また、共分散行列 $\mathbf{R}$ に関して、全開口内に複数の小開口を設け、それら小開口に関する共分散行列を加算平均する sub-array averaging 及び共分散行列の対角成分に小さな値を加える対角項負荷 (diagonal loading) が適用され、ビームフォーマの出力を安定化させる。

MV ビームフォーマの性能向上に向けて様々な試みが行われている。共分散行列の forward-backward 推定は、MV ビームフォーミングにおける画像のコントラストとロバスト性を向上させる⁽³³⁾。共分散行列の固有値分解は MV ビーム

フォーミングに使用され、硬い組織のエッジをより明瞭に描出できることが報告されている^{(34), (35)}。更に、異なるサブアレーの組み合わせから得られた共分散行列は、MV ビームフォーミングにおける画像のコントラストを向上させる⁽³⁶⁾。また、MV ビームフォーマに CF を組み合わせることにより、空間分解能とコントラストを更に向上させる試みも行われている^{(37)~(39)}。更に、ウィーナフィルタを MV ビームフォーミング処理とコヒーレンス推定に用いることにより性能が向上することも報告されている^{(40)~(42)}。MV ビームフォーマは、異なるステアリング角度で得られた平面波画像のコヒーレント合成の際の重みの決定にも適用できる^{(43)~(45)}。文献(46)では、平面波コヒーレント合成に DMAS (delay multiply-and-sum) ビームフォーマを用いる手法が提案されている。MV ビームフォーマでは、対角項負荷の大きさや小開口数を経験的に決定する必要があるが、それらを適応的に決定する手法が提案されている^{(47), (48)}。また、MV ビームフォーミングにおいて計算される素子信号の共分散行列から、所望信号のパワーを推定してアポダイゼーション重みを決定する手法も提案され、DMAS 法などに比べ方位分解能が向上するほか、強散乱体の側方に輝度が低い領域がアーチファクトとして発生することを抑制する効果が報告されている⁽⁴⁹⁾。

5. 画質評価

図 4(1-a)~(1-g)は、DAS, FDMAS, CF による重み付け DAS, PCF による重み付け DAS, SCF による重み付け DAS, SNR factor による重み付け DAS, 及び MV によって得られたストリングターゲット (細線の輪切り断面) の B モード画像を示す。図 4(2-a)~(2-e)は、無エコーの嚢胞ターゲットに関する同様の結果を示す。これらの画像は、7.5 MHz のリニアアレーを用いたコヒーレント平面波合成イメージング⁽¹³⁾によって取得され、素子間隔は 0.2 mm である。平面波は、角度間隔が 0.5 度 (21 角度) の -10 度から 10 度までのステアリング角度で送信された。F ナンバはガウシアンアポダイゼーションの半値幅 (full width at half maximum: FWHM) から計算し、2.08 に設定した。DAS, FDMAS, 及び CF による重み付け DAS ではガウシアンアポダイゼーションを用いた。PCF と SCF の算出及び SNR ファクタ算出のための線形回帰ビームフォーミング⁽²³⁾と MV ビームフォーミングでは、ガウシアンアポダイゼーションを行った場合の FWHM の幅を受信開口幅とした。図 4 では、各ビームフォーミング方法は、個々の素子で受信された RF 信号に適用され、各送信ステアリング角でのビームフォーミングされた RF 信号を得た。そのように得られた全ての偏向角でのビームフォーミングされた RF 信号は、最終的なビームフォーミング後 RF 信号を得るためにコヒーレントに合成 (加算) される。

図 5(a)は、異なる送信偏向角度で得られたビームフォーミング後 RF 信号を合成する際に FDMAS を適用して得ら

れたものである。また、CF による重み付け加算、PCF による重み付け加算、SCF による重み付け加算、SNR factor による重み付け加算、及び MV による重み付け加算によりビームフォーミング後 RF 信号を合成したものも示す。図 5 において、各送信偏向角度でのビームフォーミング後 RF 信号は DAS ビームフォーミングにより算出した。その後、全ての偏向角度で得られた RF 信号を FDMAS, CF で重み付けた DAS, SNR factor で重み付けた DAS, 及び MV を使用して合成した。図 5(1-a)~(1-f)はそれぞれ、FDMAS, CF による重み付け、PCF による重み付け、SCF による重み付け、SNR factor による重み付け、及び MV による重み付けによって合成されたストリングターゲットの画像を示している。図 5(2-a)~(2-f)は、嚢胞ターゲットに関する同様の結果を示している。

一般的に、画像の品質は空間分解能、コントラスト、及び CNR (コントラスト対雑音比) などの指標を使用して評価される^{(50), (51)}。空間分解能は、点 (ストリング) ターゲットからのエコーの半値全幅 (full width at half maximum: FWHM) によって評価される。コントラストと CNR はそれぞれ式(20)、(21)式により定義される。

$$Contrast = \frac{\mu_B}{\mu_T} \quad (20)$$

$$CNR = \frac{|\mu_T - \mu_B|}{\sqrt{\sigma_T^2 + \sigma_B^2}} \quad (21)$$

ここで、 μ_T と σ_T^2 はターゲット領域内のビームフォーミング後エコー信号の振幅の平均値と標準偏差であり、 μ_B と σ_B^2 は背景のスペックル領域内のそれらの値を示す。

図 3 と 4 に示された画像に関して評価した上述の指標はそれぞれ、図 5 と図 6 にまとめられている。図 8 と図 9 は、図 4 と図 5 のそれぞれの中で深さ 20 mm 付近のストリングターゲットからのエコーの横方向の振幅プロファイルを示している。適応イメージング法、つまり重み付けベースの方法と MV ビームフォーマによって、横方向の分解能が向上している。また、MV ビームフォーマを除く適応的な方法によって、コントラスト値も向上している。一方、適応的な方法によって CNR は劣化していることが分かる。

2.1 節で説明したように、重み付けベースの適応イメージング方法は、コヒーレンスが低いビームフォーミング後エコー信号を抑圧する。その結果、部分的にコヒーレントな成分 (スペックル領域) とインコヒーレントな成分 (無エコー嚢胞領域) 間のコントラストが増加している。これは、ビームフォーミング後信号のダイナミックレンジの変化が原因である可能性がある (スペックル領域の輝度が高い領域と低い領域の輝度差が大きくなる)。図 4(2-c)で見られるように、重み付けベースの方法によって得られた B モード画像のスペックルはサイズが小さくなっており「よく解像されている」ように見える。一方、このような効果は信号のダイナミックレンジの変化によりもたらされたと考えることもでき、空間分解能の向上も同様に考えることができる。前述の

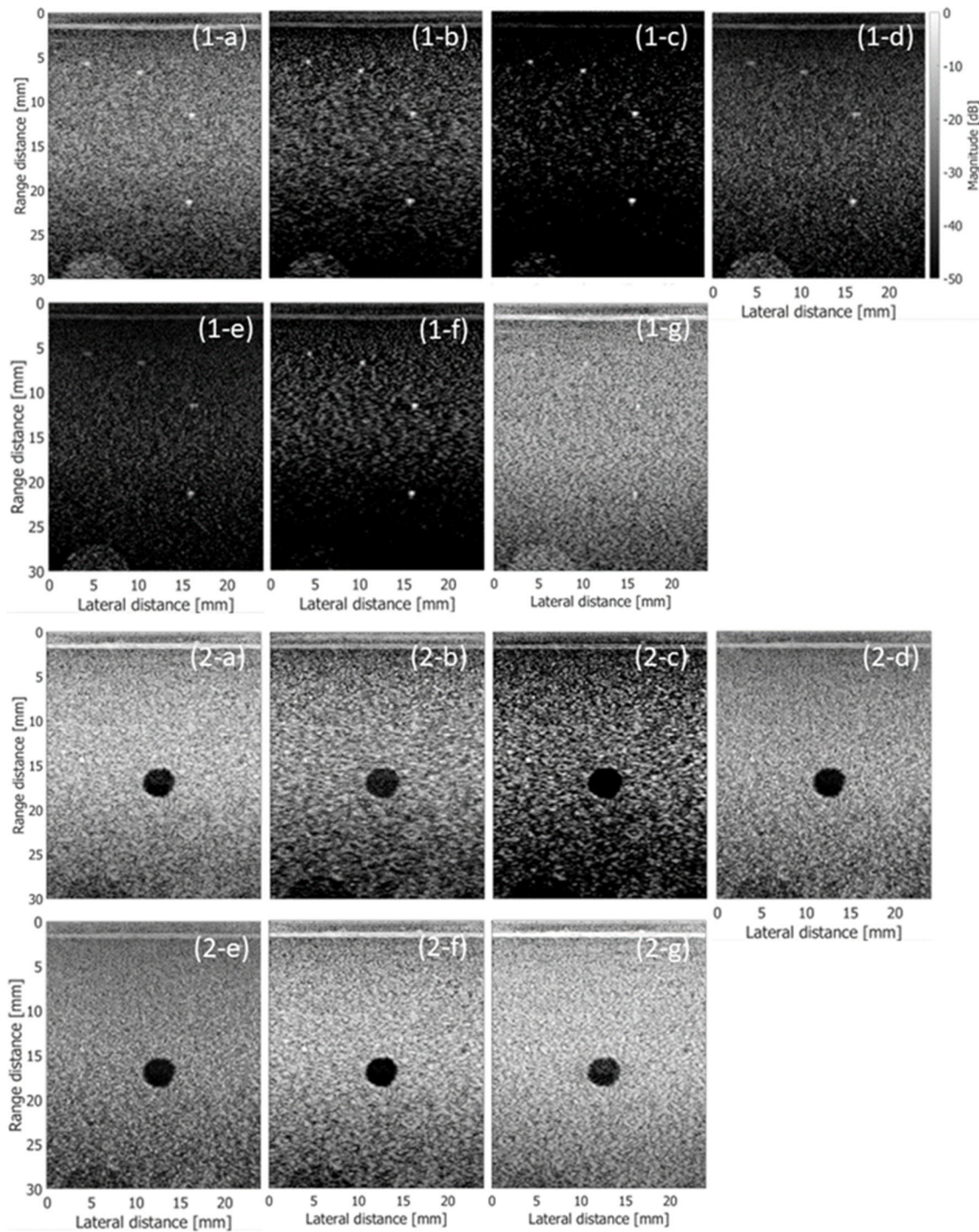


図4 異なるビームフォーミング法により得られたストリング(1)と嚢胞(2)ファントムのBモード断層像 (a)DAS. (b)FDMAS. (c)CFにより重み付けたDAS. (d)PCFにより重み付けたDAS. (e)SCFにより重み付けたDAS. (f)SNR factorにより重み付けたDAS (γ : ストリング1, 嚢胞500). (g)MV (共分散行列平均回数: 全素子数の2/3, diagonal loading: 受信信号パワーの0.1).

ように、適応イメージング方法は信号のダイナミックレンジを変化させ、スペックルの統計的性質を変化させる。それによってCNRは低下する。

適応イメージング方法の影響を考慮し、画像品質を適切に評価するための研究が幾つか行われている。MallartとFink⁽¹⁶⁾、LiuとWaag⁽⁵²⁾は、van Cittert-Zernike (VCZ) 定理⁽⁵³⁾を導入し、後方散乱された超音波の空間的なコヒーレ

ンスを評価する方法を紹介している。空間的なコヒーレンスは、素子信号の相関によって評価され、位相収差、メインローブ外信号及び多重反射成分、熱雑音などの画像品質を低下させる要因に対して感度がある。このような空間的なコヒーレンスの特性により、Longらは素子信号から推定されたLag-oneの空間的なコヒーレンスを使用した画質評価方法を提案した⁽⁵⁴⁾。空間的なコヒーレンスは式(22)により定

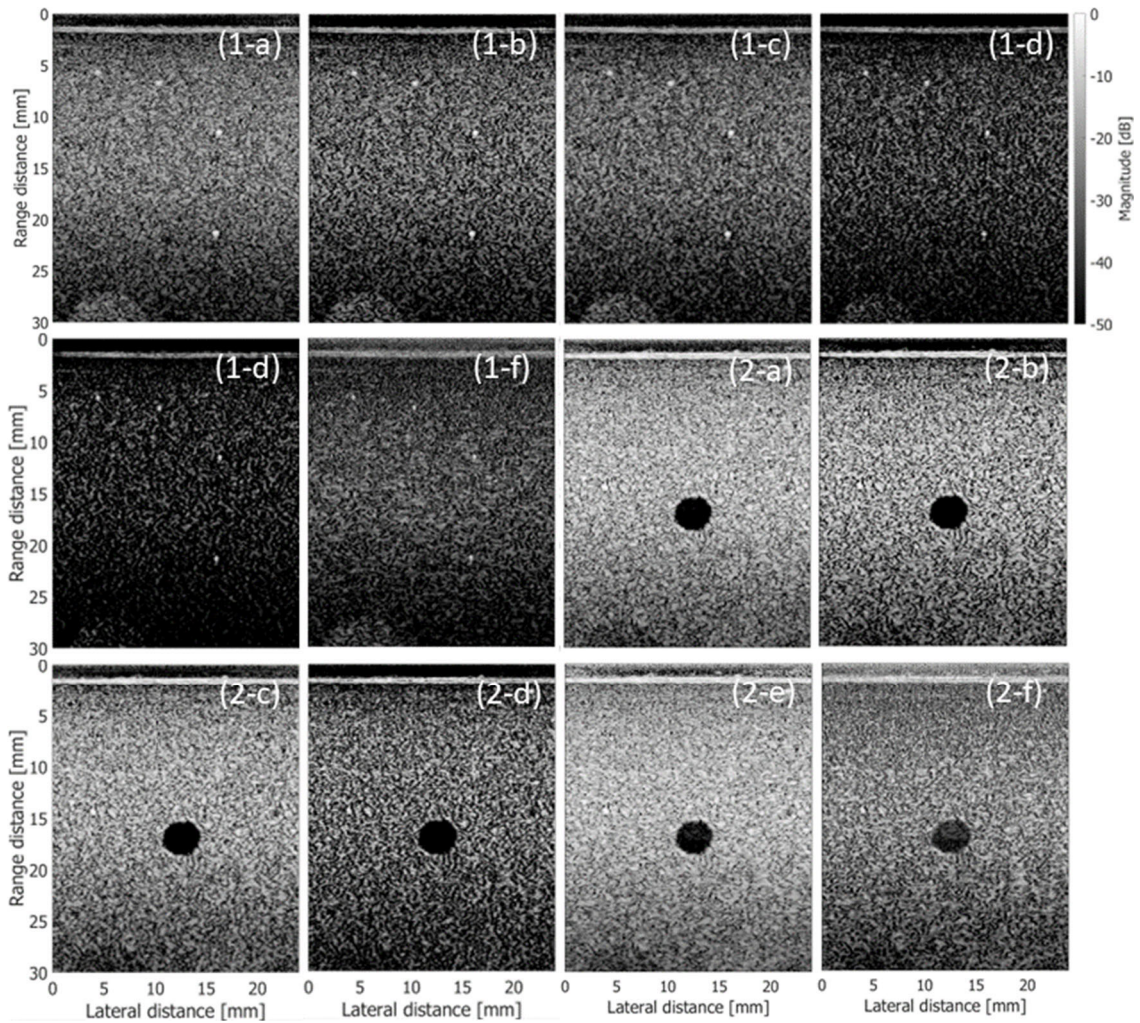


図5 異なる平面波コヒーレント合成法により得られたストリング(1)と嚢胞(2)ファントムのBモード断層像 (a)FDMASによる合成. (b)CFによる重み付け加算. (c)PCFによる重み付け加算. (d)SCFによる重み付け加算. (e)SNR factorによる重み付け加算 (γ : ストリング1, 嚢胞500). (f)MVによる重み付け加算 (共分散行列平均回数: 全送信回数の2/3, diagonal loading: 受信信号パワーの0.1).

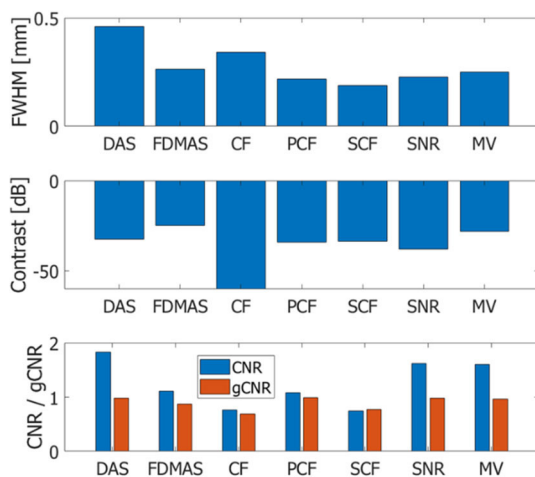


図6 図4の画像に関して算出した画質評価指標

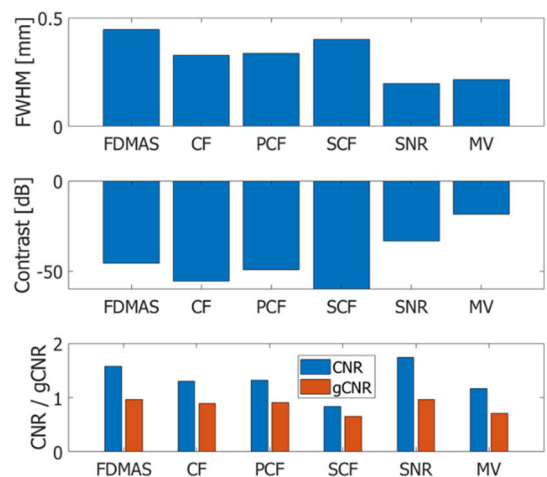


図7 図5の画像に関して算出した画質評価指標

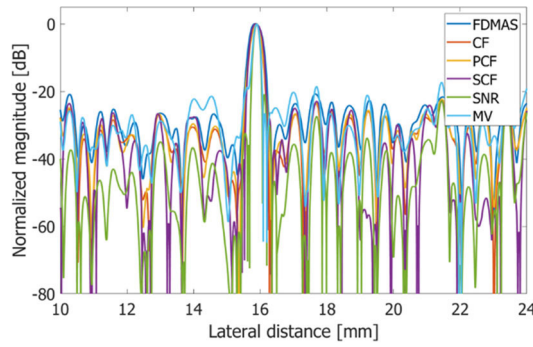


図8 図4の画像における深さ 20 mm にあるストリングからのエコー信号振幅の横方向の振幅プロファイル

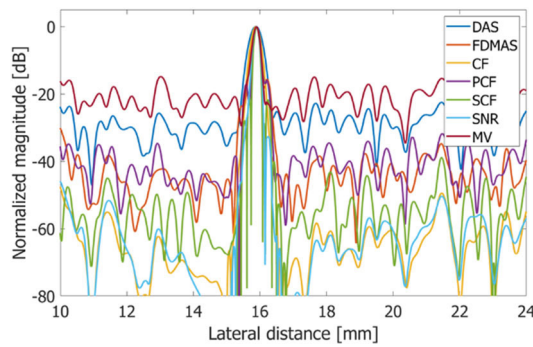


図9 異なる平面波コヒーレント合成法により得られた深さ 20 mm 付近にあるストリングからのエコー信号振幅の横方向の振幅プロファイル

義される。

$$R(m) = \frac{1}{M-m} \sum_{i=1}^{M-m} \frac{\sum_{n=n_1}^{n_2} s_i(n) s_{i+m}(n)}{\sqrt{\sum_{n=n_1}^{n_2} s_i^2(n) \sum_{n=n_1}^{n_2} s_{i+m}^2(n)}} \quad (22)$$

$$\hat{R}(m) = \langle R(m) \rangle \quad (23)$$

ここで、 n_1 と n_2 は Lag-one のコヒーレンスを推定するために使用される標本化信号のビーム方向の数を定義し、 $\langle \cdot \rangle$ は関心領域内での平均を示す。Lag-one コヒーレンスは、 m を 1 に設定することで得られる。従来の指標、すなわちコントラストと CNR を評価するには、ターゲット領域とスペckル背景領域に対応する二つの関心領域が必要であり、これらの領域が均一であることが望ましい。したがって、従来のコントラストと CNR は一般的にファントム実験により評価される。これは、実際の組織内で均一な領域を見つけるのは一般的に難しいためである。Lag-one コヒーレンスは、音響クラッタや熱雑音の影響の尺度として、単一の関心領域で評価することができる。

Rodriguez-Molares らは、別の指標である一般化 CNR (generalized CNR : gCNR) ⁽⁵⁵⁾ を提案した。適応イメージング方法は、しばしば画像のコントラストを著しく改善し、病変の検出可能性向上に貢献する可能性がある。一方、これらの方法はスペckルの統計的性質を変化させる。CNR は画像

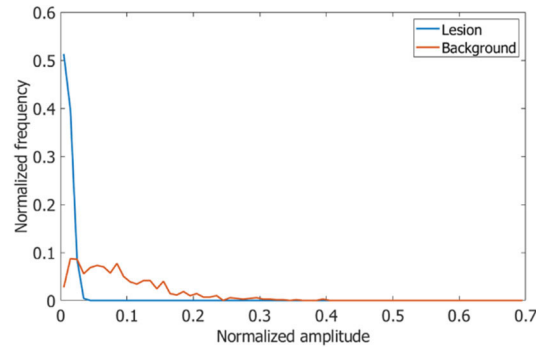


図10 ファントムにおける病変（嚢胞）領域と背景スペckル領域のエコー振幅の頻度分布の例 ⁽¹⁾

品質の評価において臨床的に重要な指標であると考えられるが、従来の CNR の定義 (式(21)) を使用する場合、エコー振幅値をシグモイド曲線を用いて圧縮するだけでも CNR を向上させることができる ^{(56), (57)}。gCNR は、信号のダイナミックレンジの変化の影響を受けにくい指標として開発された。gCNR は、ターゲット領域と背景スペckル領域内のエコー振幅値の確率密度分布を分析して得られ、式(24)のように定義される。

$$gCNR = 1 - OVL \quad (24)$$

ここで、OVL はターゲット領域とスペckル領域の振幅の確率密度分布が重なった領域の面積を示す。図10は、図4に示された B モード画像の病変（嚢胞性嚢腫）と背景領域内のエコー振幅のヒストグラムの例を示している。gCNR は、ダイナミックレンジの変化に関係なくターゲットの検出しやすさを評価できる ⁽⁵⁵⁾。

6. 近年の適応的イメージング法の展開

6.1 受信信号のコヒーレンスに基づく手法

2 節で説明した適応イメージング方法の中で、short-lag spatial coherence (SLSC) イメージングは、CNR が劣化しないことを重視した方法といえる ^{(58), (59)}。最近では lag-one coherence が画質評価に使用されているが、SLSC イメージング法は、式(22)で表されるように複数のラグで算出された空間的コヒーレンスを利用する。SLSC は式(25)で定義される。

$$\hat{R}_{SLSC} = \sum_{m=1}^{M_{SL}} R(m) \quad (25)$$

ここで、 M_{SL} は SLSC の評価に使用されるラグの数である。SLSC イメージング法は、式(25)で評価された R_{SLSC} を直接マッピングするため、エコー信号の振幅をマッピングする従来の B モード画像とは異なる。SLSC 画像は、SLSC の評価に使用されるラグの数に依存して、従来の B モード画像よりも優れた CNR を実現する。SLSC によって CNR 値が向上するのは、一様散乱媒質において短いラグでの空間的コ

ヒーレンスの分散が小さいからである。最近では、SLSCが組織性状の評価に使用できる可能性も示されている⁽⁶⁰⁾。一方で、散乱強度に感度がないSLSC画像は、Bモード画像を代替できるかどうかは現段階で評価は定まっていない。

6.2 クラッタ低減手法

CNRを低下させずに画質を向上させる別の方法は、クラッタを減少させることである。メインローブ外及び多重エコーなどのクラッタは、画像のコントラストを著しく低下させる。超音波診断装置の最近の発展の中で、ハーモニックイメージングはクラッタを低減させるための最も強力で広く活用されている方法である^{(61)~(63)}。ハーモニックイメージングはクラッタを著しく減少させるが、完全に排除するわけではない。Byramらは、素子エコー信号に含まれるクラッタを減少させるための方法であるaperture domain model image reconstruction (ADMIRE)を提案している^{(64)~(66)}。彼らの方法では、素子エコー信号のモデルは式(26)で表現される。

$$g(x; t, \omega) = \sum_{n=0}^{N-1} A(x; x_n, z_n, \tau_n, \omega) e^{jk\tau(x; x_n, z_n, \tau_n)} \quad (26)$$

ここで、 x 、 t 、及び ω は、開口内の横方向の位置、時間、及び角周波数を表し、 k は波数、 x_n 及び z_n は τ_n 時点での散乱体の横方向及びビーム方向の位置である。また、 $\tau(x; x_n, z_n, \tau_n)$ は、 τ_n 時点での横方向及びビーム方向の位置 x_n と z_n にある点から到達する信号の波面の伝搬時間遅延を表す。 N は散乱体の数であり、 $A(x; x_n, z_n, \tau_n, \omega)$ はフーリエ変換適用時の窓関数及び素子指向性により生じる振幅変化を示す。ADMIRE法は、モデルを測定された信号に整合させるための係数を決定し、設定した許容範囲の外側から到来したと想定される信号モデルから推定された成分はクラッタとして除去される。ADMIRE法は、数値シミュレーション、ファントム実験、及びin vivo実験においてクラッタを大幅に低減できることが示されている。また、ADMIREの演算を繰り返すことで、1回の演算では所望信号も除去されてしまう場合にも対応できることが示されている⁽⁶⁷⁾。また、MVビームフォーマと組み合わせる手法も提案されている⁽⁶⁸⁾。受信信号からクラッタ成分を除去する手法としては、心臓のMモード像の元となるAモード信号において、システムの点拡がり関数をもとに信号を複数の成分に分解し、動きの小さいクラッタ成分を除去する手法も提案されている⁽⁶⁹⁾。

Morganらは、彼らの提案するconstituent covariance models^{(70),(71)}を用いて、受信エコー信号をメインローブ、サイドローブ、インコヒーレントな雑音成分に分解する手法を開発した。受信エコー信号の共分散行列 $\hat{\mathbf{R}}$ のモデルは式(27)のように表される。

$$\hat{\mathbf{R}} = \sum_{i=1}^P \alpha_i^2 \mathbf{A}_i + \mathbf{N} \quad (27)$$

ここで、 P は構成成分の数、 $\mathbf{A}_i$ は i 番目の成分の構成共分散モデル、 α_i^2 は i 番目の成分のパワーに対応する分散であ

り、 $\mathbf{N}$ は雑音である。各成分の分散の最小二乗推定値は、式(28)のように求められる。

$$\hat{\alpha}_i^2 = \arg \min_{\alpha_i^2} \left\| \mathbf{R} - \sum_{i=1}^P \alpha_i^2 \mathbf{A}_i \right\|_F^2 \quad (28)$$

ここで、 α^2 は $P \times 1$ の分散ベクトルであり、 $\alpha^2 = [\alpha_1^2, \alpha_2^2, \dots, \alpha_P^2]^T$ と表される。また、 $(\cdot)_F$ 及び T はそれぞれFrobeniusノルムと転置を示す。メインローブ成分として推定された分散 α^2 をマッピングすることによりMIST (multi-covariate imaging of sub-resolution targets) 画像が得られる。MIST法によりコントラストとCNRが顕著に向上することが、数値シミュレーション、ファントム実験、及びin vivo実験により示されている。また、モデル $\mathbf{A}_i$ を受信信号に応じて適応的に構築する手法も開発され、MIST画像の性能向上が報告されている⁽⁷²⁾。

6.3 音速の推定

組織内の音速の不均一性も、超音波画像の品質を劣化させる。Ultrasonic computed tomography (USCT)は音速の空間分布の推定のために開発されたが^{(73)~(78)}、USCTは基本的に媒質を透過した超音波の測定を必要とするため、パルスエコー法に基づく超音波診断には適していない。そのような問題を克服するため、最近ではパルスエコーモードでのUSCT^{(79)~(83)}も盛んに研究されている。

パルスエコーモードでは、二つの交差したビームが二つの方向^{(84)~(87)}または複数の方向^{(88),(89)}に配置され、ターゲット（またはターゲット領域）から得られるエコーの伝搬遅延の差を用いて音速を推定する。超音波エコーの到達時間は、二つの方向から得られたエコーの時間的位置または相関解析から推定される。音速はまた、特異的な強散乱体からのエコー信号の遅延プロファイルを用いても推定が行われている⁽⁹⁰⁾。

パルスエコーモードのDASビームフォーミングにおいては、組織内の音速を仮定する必要がある。超音波ビームフォーミングにおけるフォーカシング精度向上のために、平均音速を推定するための様々な試みが行われている。

小川らは、異なる仮定音速の下でDASビームフォーマの出力の振幅を評価し、振幅を最大化する音速を平均音速として決定している^{(91)~(93)}。また、Choらによっても同様の手法が提案されている⁽⁹⁴⁾。DASビームフォーマの出力は、受信焦点からの球面散乱波の波面が最も正確に推定されたとき、つまり音速が適切に設定されたときに最大となる。音速はまた、ビームフォーミング後信号の横方向の帯域幅を評価することによっても推定されている。横方向の帯域幅は方位分解能に対応しており、フォーカシング精度が高い場合に帯域幅が広がる⁽⁹⁵⁾。更に、素子エコー信号を使用して評価された空間的相関を最大化することによっても音速が推定されている。音速は、式(7)で定義されたCFを最大化することによって推定でき^{(96)~(101)}、図11はその例を示している。図11(1-a)と図11(1-b)はそれぞれ、CFを最大化して推定された

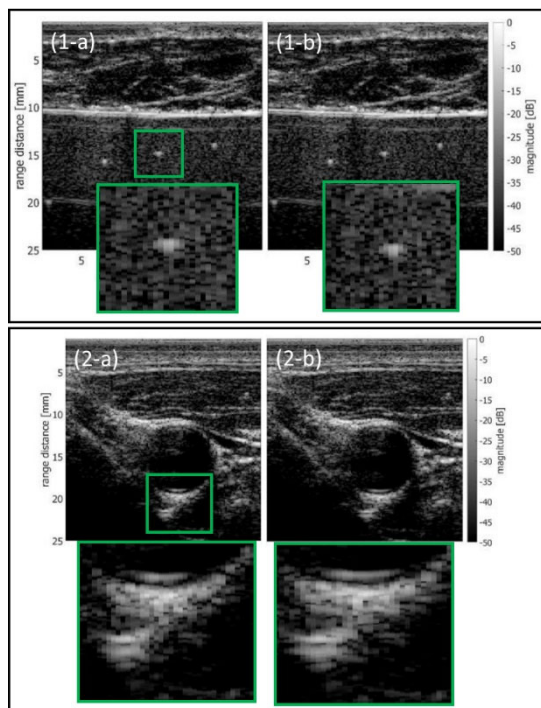


図 11 浅部に音速不均一媒質を設けたファントム(1)と頸動脈(2)の B モード断層像⁽¹⁾ (a)音速を 1540 m/s と仮定して構築した画像。(b)CF を最大化する音速値を用いて構築した画像。

平均音速と音速を一定値 1540 m/s と仮定し DAS ビームフォーミングを行ったファントム (model 040GSE, CIRS) の B モード画像を示している。図 11 では、拡大して表示した領域が緑線の四角で示されている。エコー信号は、20 mm に焦点を設定した集束送信ビーム及び受信ダイナミックフォーカシングにより得られた。7.5 MHz のリニアアレイプローブが使用され、ファントムの上に豚肉が音速不均一媒質として配置されている。ストリングターゲットからのエコーの横方向半値全幅は、音速を補正することで 0.538 mm から 0.472 mm に向上した。図 11(2)は、ヒト頸動脈の短軸断面に関する同様の結果を示している。図 11(2)に見られるように、CF を最大化して推定された音速を使用することにより、後壁の内腔-内膜界面からのエコーがより広い領域で描出されている。

6.4 収差補正

生体組織内の音速の不均一性は、送信及び反射／散乱された超音波の波面をひずませる。このような収差の推定及び補正を目的として多くの研究が行われている^{(102)~(106)}。Imbault らは、式(22)に基づき受信信号の空間的コヒーレンスを評価し、ラグの広い範囲で空間的コヒーレンスが高くなるよう、局所ごとの音速を推定している^{(107)~(109)}。彼らは不均一な媒質で空間的コヒーレンスをより正確に推定するために、時間反転法⁽¹¹⁰⁾を用いて収差プロファイルを推定している。Lam-

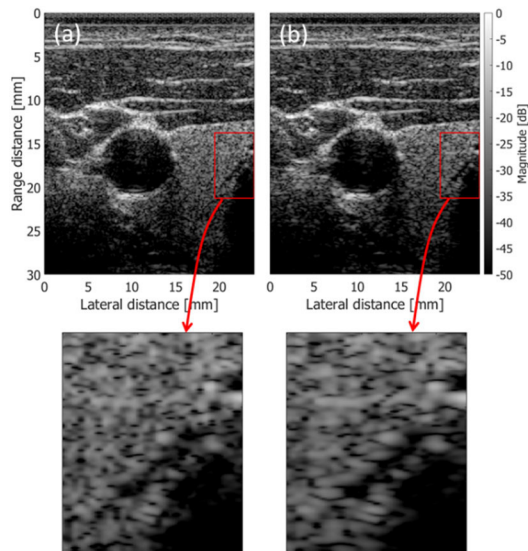


図 12 平面波コヒーレント合成(a)と SVD ビームフォーミング(b)により得られた B モード断層像⁽¹⁾

bert らは、関心点及びそのごく近傍に送信焦点を設定して得られた素子エコー信号を計測することにより収差プロファイルを推定するとともに多重反射成分の抑圧も実現している⁽¹¹¹⁾。また、平面波のコヒーレント合成における収差補正に SVD (singular value decomposition) が用いられ、“SVD ビームフォーマ”とよばれている⁽¹¹²⁾。SVD ビームフォーマでは、異なる偏向角度で N_θ 回送信された平面波により得られたビームフォーミング後複素信号について、 $N_x \times N_z$ の局所領域ごとに SVD を適用することにより収差補正が行われる。この $N_x \times N_z \times N_\theta$ の三次元行列は、 $N_x N_z \times N_\theta$ の二次元 Casorati 行列に変形される。その二次元行列に SVD を適用すると、最大特異値に対応する空間特異ベクトルが収差補正された画像となる。図 12(a)と 12(b)はそれぞれ、従来の平面波コヒーレント合成と SVD ビームフォーマによって得られた B モード画像を示す。超音波エコーは、 -20 度から 20 度まで偏向角度間隔 0.5 度で偏向させた平面波を送信することにより得られた。図 12(b)で見られるように、SVD ビームフォーマによる収差の補正により、輝度の低い領域のコントラストが向上している。

6.5 人工知能によるビームフォーミング

現在、人工知能、特に深層学習の応用が各分野で急速に広がっているが、超音波ビームフォーミング分野においても様々な応用が検討されている。Luchies らはシミュレーションによりサイドローブを含む全範囲からのエコー信号とメインローブの範囲内からの散乱体からのエコー信号を生成し、前者を入力データ、後者を教師データとして深層学習モデルを学習させることにより超音波画像における不要信号を抑圧できることを報告している^{(113)~(115)}。また、入力データを DAS ビームフォーマ出力、教師データを MV ビームフォー

マ出力として深層学習モデルを学習させることでMV ビームフォーマと等価な画質が得られることが報告されている^{(116), (117)}。文献(116)の深層学習モデルでは、MV ビームフォーマにより得られるアポダイゼーション重みを実数値で表現しているが、学習モデルを複素数化することにより性能が向上することも報告されている⁽¹¹⁸⁾。また、深層学習によるデータ復元を利用して、より少数のデータからほとんど劣化なくビームフォーミングを行えることも報告されている⁽¹¹⁹⁾。データ削減の観点からは、受信超音波信号を直交検波した信号が用いられることも多く、直交検波信号に対応した深層学習モデルも提案されている⁽¹²⁰⁾。

前述の送信に平面波を用いる平面波イメージングは数千フレーム毎秒以上の非常に高いフレームレートを実現する。一方で送信平面波が非集束ビームであることから空間分解能やサイドロープレベルが劣化する。それら指標を改善するためには、平面波を複数の角度で送信して重ね合わせる平面波コンパウンド法⁽¹³⁾が有効であるが送信角度数を増やせばフレームレートは劣化する。そのため、1つの偏向角度で得られたビームフォーミング後信号を入力データとし、多数の平面波偏向角度数で得られたビームフォーミング後信号^{(121)~(123)}または開口合成法で得られたビームフォーミング後信号⁽¹²⁴⁾を教師データとして深層学習モデルを学習させることにより、一つの偏向角度で得られた画像から多数の偏向角度数で得られた画像と等価な画質を実現できることが報告されている。また、一つの偏向角度で得られた信号を入力データとして学習させる際、送信に集束ビームを用いた場合の信号を教師データとし、素子信号を学習に用いることにより高フレームレートを維持しながら集束ビームを用いた場合と等価な画質が得られることも報告されている⁽¹²⁵⁾。

7. ま と め

超音波診断における画像品質は、診断の正確性を決定する重要な要素であり、画像品質に影響を与える様々な現象を調査し、画像品質を向上させる方法を開発するための多くの研究が行われている。本稿で述べたように、超音波画像形成法に関する研究開発は、プログラム可能な超音波計測装置^{(126)~(128)}が近年広く利用されるようになったため、ますます活発になっている。また、GPUの普及により、より高度な計算を必要とする画像形成アルゴリズムの実装が可能となってきた^{(129), (130)}。このような環境は、この分野での研究開発を更に加速させ、上述の深層学習によるビームフォーミングをはじめスペckル低減^{(131), (132)}、画像セグメンテーション^{(133), (134)}など超音波画像処理に強力な選択肢を提供する。また、超音波イメージングは既に三次元化されており、そのための様々なイメージング法が検討されているが、フルマトリックスアレーの素子数は数千となるため一部のハイエンド機でのみ使用できるのが現状である。1軸のみ配列化したアレーを二つ重ねる row-column addressed array 及びそれを用いたイメージング法が検討されている^{(135)~(139)}。

こうした研究開発を通じて、超音波診断は医療においてその価値を更に高めていくことが期待される。

文 献

- (1) H. Hasegawa, "Advances in ultrasonography : Image formation and quality assessment," J. Med. Ultrason., vol. 48, no. 4, pp. 377-389, 2021.
- (2) H.B. Lim, N.T. Nhung, E.P. Li, and N.D. Thang, "Confocal microwave imaging for breast cancer detection : Delay-multiply-and-Sum image reconstruction algorithm," IEEE Trans. Biomed. Eng., vol. 55, pp. 1697-1704, 2008.
- (3) G. Matrone, A.S. Savoia, G. Caliano, and G. Magenes, "The delay multiply and sum beamforming algorithm in ultrasound B-mode medical imaging," IEEE Trans. Med. Imag., vol. 34, no. 4, pp. 940-49, 2014.
- (4) G. Matrone, A.S. Savoia, G. Caliano, and G. Magenes, "Ultrasound plane-wave imaging with delay multiply and sum beamforming and coherent compounding," Proc. 2016 38th Ann. Int. Conf. IEEE Eng. Med. Biol. Soc. (EMBC), 2016.
- (5) X. Yan, Y. Qi, Y. Wang, and Y. Wang, "Regional-lag signed delay multiply and sum beamforming in ultrafast ultrasound imaging," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 69, no. 2, pp. 580-591, 2022.
- (6) F. Prieur, O.M.H. Rindal, and A. Austeng, "Signal coherence and image amplitude with the filtered delay multiply and sum beamformer," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 65, no. 7, pp. 1133-1140, 2018.
- (7) D. Go, J. Kang, and Y. Yoo, "A new compounding method for high contrast ultrafast ultrasound imaging based on delay multiply and sum," Proc 2018 IEEE Int. Ultrason. Symp. (IUS), 2018.
- (8) C.C. Shen and P.Y. Hsieh, "Two-dimensional spatial coherence for ultrasonic DMAS beamforming in multi-angle plane-wave imaging," Appl. Sci., vol. 9, art. no. 3973, 2019.
- (9) R. Cohen and Y.C. Eldar, "Sparse convolutional beamforming for ultrasound imaging," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 65, no. 12, pp. 2390-2406, 2018.
- (10) A. Agarwal, J. Reeg, A.S. Podkova, and M.L. Oelze, "Improving spatial resolution using incoherent subtraction of receive beams having different apodizations," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 66, no. 1, pp. 5-17, 2019.
- (11) A.C. Jensen and A. Austeng, "Speckle reduction using adaptive receive-side compounding," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 68, no. 4, pp. 1155-1166, 2021.
- (12) Q. You, Z. Dong, M.R. Lowerison, and P. Song, "Pixel-oriented adaptive apodization for plane-wave imaging based on recovery of the complete dataset," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 69, no. 2, pp. 512-522, 2022.
- (13) G. Montaldo, M. Tanter, J. Bercoff, N. Benech, and M. Fink, "Coherent plane-wave compounding for very high frame rate ultrasonography and transient elastography," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 56, no. 3, pp. 489-506, 2009.
- (14) Z. Kou, R.J. Miller, and M.L. Oelze, "Grating lobe reduction in plane-wave imaging with angular compounding using subtraction of coherent signals," IEEE Trans. Ultrason., Ferroelectr., Freq. Control, vol. 68, no. 12, pp. 3308-3316, 2022.
- (15) K.W. Hollmand, K.W. Rigby, and M. O'Donnell, "Coherence factor of speckle from a multi-row probe," Proc. IEEE Ultrasonics Symp., pp. 1257-1260, 1999.
- (16) R. Mallart and M. Fink, "Adaptive focusing in scattering media through sound-speed inhomogeneities : The van Cittert-Zernike approach and focusing criterion," J. Acoust. Soc.

- Am., vol. 96, no. 6, pp. 3721-3732, 1994.
- (17) S.D. Silverstein, "Ultrasound scattering model: 2-D cross-correlation and focusing criteria-Theory, simulations, and experiments," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 48, no. 4, pp. 1023-1030, 2001.
 - (18) P.C. Li and M.L. Li, "Adaptive imaging using the generalized coherence factor," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 50, no. 2, pp. 128-141, 2003.
 - (19) J. Camacho, M. Parrilla, and C. Fritsch, "Phase coherence imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 56, pp. 958-974, 2009.
 - (20) H. Hasegawa and H. Kanai, "Effect of sub-aperture beamforming on phase coherence imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 61, no. 11, pp. 1779-1790, 2014.
 - (21) H. Hasegawa, "Enhancing effect of phase coherence factor for improvement of spatial resolution in ultrasonic imaging," *J. Med. Ultrason.*, vol. 43, no. 1, pp. 19-27, 2016.
 - (22) Y. Wang, Y.C. Zheng, H. Pe, and Q. Chen, "An adaptive beamforming method for ultrasound imaging based on the mean-to-standard-deviation factor," *Ultrasound Med. Biol.*, vol. 90, pp. 32-41, 2018.
 - (23) H. Hasegawa and R. Nagaoka, "Converting coherence to signal-to-noise ratio for enhancement of adaptive ultrasound imaging," *Ultrason. Imaging*, vol. 42, no. 1, pp. 27-40, 2020.
 - (24) T. Ikeda, M. Hisatsu, C. Ishihara, and Hiroshi Kuribara, "Use of intertransmission coherence for haze artifact suppression in cardiovascular synthetic aperture ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 11, pp. 3283-3298, 2021.
 - (25) J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proc. IEEE*, vol. 57, pp. 1408-1418, 1969.
 - (26) O.L. Frost, "An algorithm for linearly constrained adaptive array processing," *Proc. IEEE*, vol. 60, no. 8, pp. 926-935, 1972.
 - (27) J.A. Mann and W.F. Walker, "A constrained adaptive beamformer for medical ultrasound: Initial results," *Proc. IEEE Ultrason. Symp.*, no. 2, pp. 1807-1810, 2002.
 - (28) M. Sasso and C. Cohen-Bacrie, "Medical ultrasound imaging using the fully adaptive beamformer," *Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP)*, no. 2, p. ii-489, 2005.
 - (29) F. Viola and W. Walker, "Adaptive signal processing in medical ultrasound beamforming," *Proc. IEEE Ultrason. Symp.*, no. 4, pp. 1980-1983, 2005.
 - (30) J.F. Synnevåg, A. Austeng and S. Holm, "Adaptive beam forming applied to medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 54, pp. 1606-1613, 2007.
 - (31) I.K. Holfort, F. Gran, and J.A. Jensen, "Broadband minimum variance beam forming for ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 56, pp. 314-325, 2009.
 - (32) J.F. Synnevåg, A. Austeng, and S. Holm, "Benefits of minimum variance beam forming in medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 56, pp. 1868-1879, 2009.
 - (33) B.M. Asl and A. Mahloojifar, "Contrast enhancement and robustness improvement of adaptive ultrasound imaging using forward-backward minimum variance beamforming," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 58, pp. 858-867, 2011.
 - (34) B.M. Asl and A. Mahloojifar, "Eigenspace-based minimum variance beamforming applied to medical ultrasound imaging," *IEEE Trans. Ultrason. Ferroelectr. Freq. Control*, vol. 57, no. 11, pp. 2381-2390, 2010.
 - (35) S. Mehdizadeh, A. Austeng, T.F. Johansen, and S. Holm, "Eigenspace based minimum variance beamforming applied to ultrasound imaging of acoustically hard tissues," *IEEE Trans. Med. Imaging*, vol. 31, no. 10, pp. 1912-1921, 2012.
 - (36) H. Hasegawa and N. Nagaoka, "Improvement of performance of minimum variance beamformer by introducing cross covariance estimate," *J. Med. Ultrason.*, vol. 47, no. 2, pp. 203-210, 2020.
 - (37) B.M. Asl and A. Mahloojifar, "Minimum variance beamforming combined with adaptive coherence weighting applied to medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 56, pp. 1923-1931, 2009.
 - (38) S.L. Wang and P.C. Li, "MVDR-based coherence weighting for high-frame-rate adaptive imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 56, pp. 2097-2109, 2009.
 - (39) M. Mozumi and H. Hasegawa, "Adaptive beamformer combined with phase coherence weighting applied to ultrafast ultrasound," *Appl. Sci.*, vol. 8, art. no. 204, 2018.
 - (40) C.K. Abbey, N.Q. Nguyen and M.F. Insana, "Optimal beamforming in ultrasound using the ideal observer," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 57, no. 8, pp. 1782-1796, 2010.
 - (41) C.I.C. Nilsen and S. Holm, "Wiener beamforming and the coherence factor in ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 57, no. 6, pp. 1329-1346, 2010.
 - (42) Y.H. Wang and P.C. Li, "SNR-dependent coherence-based adaptive imaging for high-frame-rate ultrasonic and photoacoustic imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 61, no. 8, pp. 1419-1432, 2014.
 - (43) J. Zhao, Y. Wang, X. Zeng, J. Yu, B.Y.S. Yiu, and A.C.H. Yu, "Plane wave compounding based on a joint transmitting-receiving adaptive beamformer," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 62, pp. 1440-1452, 2015.
 - (44) O.M.H. Rindal and A. Austeng, "Double adaptive plane-wave imaging," *Proc. 2016 IEEE Int. Ultrason. Symp. (IUS)*, 2016.
 - (45) N.Q. Nguyen and R.W. Prager, "A spatial coherence approach to minimum variance beamforming for plane-wave compounding," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 65, pp. 522-534, 2018.
 - (46) M.S. Ziksari and B.M. Asl, "Minimum variance combined with modified delay multiply-and-sum beamforming for plane-wave compounding," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 5, pp. 1641-1652, 2021.
 - (47) A. Salari and B.M. Asl, "User parameter-free minimum variance beamformer in medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 7, pp. 2397-2406, 2021.
 - (48) T. Akamatsu, M. Mozumi, M. Omura, R. Nagaoka, and H. Hasegawa, "Investigation on improving performance of adaptive beamformer by statistical analysis of ultrasonic echoes," *Jpn. J. Appl. Phys.*, vol. 61, SG1040-1-8, 2022.
 - (49) Y. Wang, C. Zheng, M. Liu, and H. Peng, "Covariance matrix-based statistical beamforming for medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 1, pp. 208-221, 2022.
 - (50) M.S. Patterson and F.S. Foster, "The improvement and quantitative assessment of B-mode images produced by an annular array/cone hybrid," *Ultrason. Imaging*, vol. 5, no. 3, pp. 195-213, 1983.
 - (51) S.W. Smith, H. Lopez, and W.J. Bodine, "Frequency independent ultrasound contrast-detail analysis," *Ultrasound Med. Biol.*, vol. 11, no. 3, pp. 467-477, 1985.
 - (52) D. Liu and R. Waag, "About the application of the van Cittert-Zernike theorem in ultrasonic imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 42, no. 4, pp. 590-601, 1995.
 - (53) R. Mallart and M. Fink, "The van Cittert-Zernike theorem in pulse echo measurements," *J. Acoust. Soc. Amer.*, vol. 90, no. 5, pp. 2718-2727, 1991.
 - (54) W. Long, N. Bottenus, and G.E. Trahey, "Lagone coherence as a metric for ultrasonic image quality," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 65, no. 10, pp. 1768-1780, 2018.
 - (55) A. Rodriguez-Molares, O.M.H. Rindal, J. D'hooge, S.E. Måsoy, A. Austeng, M.A.L. Bell, and H. Torp, "The

- generalized contrast-to-noise ratio : A formal definition for lesion detectability," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 67, no. 4, pp. 745-759, 2020.
- (56) O.M.H. Rindal, A. Austeng, A.A. Fatemi, and A. Rodriguez-Molares, "The effect of dynamic range alterations in the estimation of contrast," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 66, no. 7, pp. 1198-1208, 2019.
 - (57) S.M. Hverven, O.M.H. Rindal, A.J. Hunter, A. Austeng, "Point scatterer enhancement in ultrasound by wavelet coefficient shrinkage," *Proc. IEEE Int. Ultrason. Symp. (IUS)*, 2017.
 - (58) M.A.L. Bell, G.E. Trahey, B.C. Byram, and J.J. Dahl, "Short-lag spatial coherence of backscattered echoes: Imaging characteristics," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 58, no. 7, pp. 1377-1388, 2011.
 - (59) M.A.L. Bell, R. Goswami, J.A. Kisslo, J.J. Dahl, and G.E. Trahey, "Short-lag spatial coherence (SLSC) imaging of cardiac ultrasound data : Initial clinical results," *Ultrasound Med. Biol.*, vol. 39, no. 10, pp. 1861-1874, 2013.
 - (60) A. Wiacek, O.M.H. Rindal, E. Falomo, K. Myers, K. Fabrega-Foster, S. Harvey, and M.A.L. Bell, "Robust short-lag spatial coherence imaging of breast ultrasound data : Initial clinical results," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 66, no. 3, pp. 527-540, 2019.
 - (61) C. Kollman, "New sonographic techniques for harmonic imaging-underlying physical principles," *Eur. J. Radiol.*, vol. 64, pp. 164-172, 2007.
 - (62) H. Becher, K. Tiemann, T. Schlosser, C. Pohl, N.C. Nanda, M.A. Averkiou, J. Powers, and B. Lüderitz, "Improvement in endocardial border delineation using tissue harmonic imaging," *Echocardiography*, vol. 15, no. 5, pp. 511-518, 1998.
 - (63) K. Spencer, J. Bednarz, P. Rafter, C. Korcarz, and R. Lang, "Use of harmonic imaging without echocardiographic contrast to improve two-dimensional image quality," *Am. J. Cardiol.*, vol. 82, no. 6, pp. 794-799, 1998.
 - (64) B. Byram and M. Jakovljevic, "Ultrasonic multipath and beamforming clutter reduction : a chirp model approach," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 61, no. 3, pp. 428-440, 2014.
 - (65) B. Byram, K. Dei, J. Tierney, and D. Dumont, "A model and regularization scheme for ultrasonic beamforming clutter reduction," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 62, no. 11, pp. 1913-1927, 2015.
 - (66) K. Dei and B. Byram, "The impact of model-based clutter suppression on cluttered, aberrated wavefronts," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 64, no. 10, pp. 1450-1464, 2017.
 - (67) S. Schlunk, K. Dei, and B. Byram, "Iterative model-based beamforming for high dynamic range applications," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 3, pp. 482-493, 2021.
 - (68) S. Schlunk and B. Byram, "Combining ADMIRE and MV to improve image quality," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 9, pp. 2651-2662, 2022.
 - (69) S. Govinathallathyanarayana, S.T. Acton, and J.A. Hossack, "Closed-loop low-rank echocardiographic artifact removal," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 3, pp. 510-525, 2021.
 - (70) M.R. Morgan, G.E. Trahey, and W.F. Walker, "Multicovariate imaging of sub-resolution targets," *IEEE Trans. Med. Imag.*, vol. 38, no. 7, pp. 1690-1700, 2019.
 - (71) M.R. Morgan, G.E. Trahey, and W.F. Walker, "Intrinsic tradeoffs in multi-covariate imaging of sub-resolution targets," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 67, no. 10, pp. 1980-1992, 2020.
 - (72) R. Ahmed, K.M. Flint, M.R. Morgan, G.E. Trahey, and W.F. Walker, "Adaptive models for multi-covariate imaging of sub-resolution targets (MIST)," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 7, pp. 2303-2317, 2022.
 - (73) J.F. Greenleaf, A. Johnson, R.C. Bahn, and B. Rajagopalan, "Quantitative cross-sectional imaging of ultrasound parameters," *Proc. Ultrason. Symp.*, pp. 989-995, 1977.
 - (74) J.F. Greenleaf and R.C. Bahn, "Clinical imaging with transmissive ultrasonic computerized tomography," *IEEE Trans. Biomed. Eng.*, vol. 28, no. 2, pp. 177-185, 1981.
 - (75) P.L. Carson, C.R. Meyer, A.L. Schezinger, and T.V. Oughton, "Breast imaging in coronal planes with simultaneous pulse echo and transmission ultrasound," *Science*, vol. 214, pp. 1141-1143, 1981.
 - (76) G. Zografos, D. Koulocheri, P. Liakou, M. Sofras, S. Hadjiagapis, M. Orme, and V. Marmarelis, "Novel technology of multimodal ultrasound tomography detects breast lesions," *Eur. Radiol.*, vol. 23, pp. 673-683, 2013.
 - (77) P. Huthwaite and F. Simonetti, "High-resolution imaging without iteration : A fast and robust method for breast ultrasound tomography," *J. Acoust. Soc. Am.*, vol. 130, pp. 1721-1734, 2011.
 - (78) G. Sandhu, C. Li, O. Roy, S. Schmidt, and N. Duric, "Frequency domain ultrasound waveform tomography : Breast imaging using a ring transducer," *Phys. Med. Biol.*, vol. 60, art. no. 5381, 2015.
 - (79) P. Huthwaite, A.A. Zwiebel, and F. Simonetti, "A new regularization technique for limited-view sound-speed imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 60, no. 3, pp. 603-613, 2013.
 - (80) M. Jaeger, G. Held, S. Peeters, S. Preisser, M. Grünig, and M. Frenz, "Computed ultrasound tomography in echo mode for imaging speed of sound using pulse-echo sonography : Proof of principle," *Ultrasound Med. Biol.*, vol. 41, pp. 235-250, 2015.
 - (81) M. Jaeger and M. Frenz, "Towards clinical computer ultrasound tomography in echo-mode : Dynamic range artefact reduction," *Ultrasonics*, vol. 62, pp. 299-304, 2015.
 - (82) P. Stähli, M. Kuriakose, M. Frenz, and M. Jaeger, "Improved forward model for quantitative pulse-echo speed-of-sound imaging," *Ultrasonics*, vol. 108, art. no. 106168, 2020.
 - (83) D. Schweizer, R. Rau, C.D. Bezek, R.A. Kubik-Huch, and O. Goksel, "Robust imaging of speed of sound using virtual source transmission," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 70, no. 10, pp. 1308-1318, 2023.
 - (84) D.R. Robinson, F. Chen, and L.S. Wilson, "Measurement of velocity of propagation from ultrasonic pulse-echo data," *Ultrasound Med. Biol.*, vol. 8, no. 4, pp. 413-420, 1982.
 - (85) J. Ophir, "Estimation of the speed of ultrasound propagation in biological tissues : A beam-tracking method," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 33, no. 4, pp. 359-368, 1986.
 - (86) M. Kondo, K. Takamizawa, M. Hiramata, K. Okazaki, K. Inuma, and Y. Takehara, "An evaluation of an in vivo local sound speed estimation technique by the crossed beam method," *Ultrasound Med. Biol.*, vol. 16, no. 1, pp. 65-72, 1990.
 - (87) I. Cespedes, J. Ophir, and Y. Huang, "On the feasibility of pulse-echo speed of sound estimation in small regions : Simulation studies," *Ultrasound Med. Biol.*, vol. 18, no. 3, pp. 283-291, 1992.
 - (88) R. Rau, D. Schweizer, V. Vishnevskiy, and O. Goksel, "Ultrasound aberration correction based on local speed-of-sound map estimation," *Proc. IEEE Int. Ultrason. Symp. (IUS)*, pp. 2003-2006, 2019.
 - (89) M. Jaeger, E. Robinson, H.G. Akaraya, and M. Frenz, "Full correction for spatially distributed speed-of-sound in echo ultrasound based on measuring aberration delays via transmit beam steering," *Phys. Med. Biol.*, vol. 60, pp. 4497-4515, 2015.
 - (90) K. Abe, M. Arakawa, and H. Kanai, "Estimation method for sound velocity distribution for high-resolution ultrasonic tomographic imaging," *J. Med. Ultrason.*, vol. 46, no. 1, pp. 27-33, 2019.
 - (91) T. Ogawa, K. Katakura, S. Umemura, M. Kodama, N. Hayashi, N. Tamaki, K. Nakajima, K. Yamamoto, Y. Yonekura, and K. Torizuka, "In vivo measurement of mean

- sound speed using focus adjustment method (FAM) in ultrasonotomograph," *Jpn. J. Med. Ultrason.*, vol. 12, no. 1, pp. 31-36, 1985 (in Japanese).
- (92) T. Ogawa, S. Umemura, K. Katakura, H. Ikeda, M. Kodama, and H. Hayashi, "In vivo sound velocity in reflection," *Proc. IEEE Ultrason. Symp. (IUS)*, p. 917, 1987.
 - (93) N. Hayashi, N. Tamaki, M. Senda, K. Yamamoto, Y. Yonekura, K. Torizuka, T. Ogawa, K. Katakura, C. Umemura, and M. Kodama, "A new method of measuring in vivo sound speed in the reflection mode," *J. Clin. Ultrason.*, vol. 16, no. 2, pp. 87-93, 1988.
 - (94) M.H. Cho, L.H. Kang, J.S. Kim, and S.Y. Lee, "An efficient sound speed estimation method to enhance image resolution in ultrasound imaging," *Ultrasonics*, vol. 49, no. 8, pp. 774-778, 2009.
 - (95) N. Napolitano, C.H. Chou, G. McLaughlin, T.L. Ji, L. Mo, D. DeBusschere, and R. Steins, "Sound speed correction in ultrasound imaging," *Ultrasonics*, vol. 44, pp. e43-e46, 2016.
 - (96) C. Yoon, J. Kang, S. Han, Y. Yoo, T.K. Song, and Chang, "Enhancement of photoacoustic image quality by sound speed correction : Ex vivo evaluation," *Opt. Express*, vol. 20, pp. 3082-3090, 2012.
 - (97) S. Cho, J. Kang, J. Kang, W. Lee, Y. Yoo, "Phantom and in vivo evaluation of sound speed estimation methods : preliminary results," *Proc. IEEE Int. Ultrason. Symp. (IUS)*, p. 1678-1681, 2014.
 - (98) R. Ali and J. Dahl, "Distributed phase aberration correction techniques based on local sound speed estimates," *Proc. IEEE Int. Ultrason. Symp. (IUS)*, 2018.
 - (99) H. Hasegawa and R. Nagaoka, "Initial phantom study on estimation of speed of sound in medium using coherence among received echo signals," *J. Med. Ultrason.*, vol. 46, pp. 297-307, 2019.
 - (100) F. Sannou, R. Nagaoka, and H. Hasegawa, "Estimation of speed of sound using coherence factor and signal-to-noise ratio for improvement of performance of ultrasonic beamformer," *Jpn. J. Appl. Phys.*, vol. 59, art. no. SKKE14, 2020.
 - (101) R. Ali, A.V. Telichko, H. Wang, U.K. Sukumar, J.G. Vilches-Moure, R. Paulmurugan, and J.J. Dahl, "Local sound speed estimation for pulse-echo ultrasound in layered media," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 2, pp. 500-511, 2022.
 - (102) M. O'Donnell and S.W. Flax, "Phase-aberration correction using signals from point reflectors and diffuse scatterers : measurements," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 35, pp. 768-774, 1988.
 - (103) M. O'Donnell and S.W. Flax, "Phase aberration measurements in medical ultrasound : Human study," *Ultrason. Imaging*, vol. 10, pp. 1-11, 1988.
 - (104) D. Rachlin, "Direct estimation of aberrating delays in pulse-echo imaging systems," *J. Acoust. Soc. Am.*, vol. 88, pp. 191-198, 1990.
 - (105) L. Nock, G.E. Trahey, and S.W. Smith, "Phase aberration correction in medical ultrasound using speckle brightness as a quality factor," *J. Acoust. Soc. Am.*, vol. 85, pp. 1819-1833, 1989.
 - (106) S. Krishnan, K.W. Rigby, and M. O'Donnell, "Improved estimation of phase aberration profiles," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 44, no. 3, pp. 701-713, 1997.
 - (107) M. Imbault, A. Faccinnetto, B.F. Osmanski, A. Tissier, T. Deffieux, J.L. Gennisson, V. Vilgrain, and M. Tanter, "Robust sound speed estimation for ultrasound-based hepatic steatosis assessment," *Phys. Med. Biol.*, vol. 62, pp. 3582-3598, 2017.
 - (108) M. Imbault, M.D. Burgio, A. Faccinnetto, M. Ronot, Bendjador, T. Deffieux, E.O. Triquet, P.E. Rautou, L. Castera, J.L. Gennisson, V. Vilgrain, and M. Tanter, "Ultrasonic fat fraction quantification using in vivo adaptive sound speed estimation," *Phys. Med. Biol.*, vol. 63, no. 21, art. no. 215013, 2018.
 - (109) M.D. Burgio, M. Imbault, M. Ronot, A. Faccinnetto, B.E. van Beers, P.E. Rautou, L. Castera, J.L. Gennisson, M. Tanter, and V. Vilgrain, "Ultrasonic adaptive sound speed estimation for the diagnosis and quantification of hepatic steatosis : A pilot study," *Ultrasound Med. Biol.*, vol. 40, no. 6, pp. 722-733, 2019.
 - (110) G. Montaldo, M. Tanter, and M. Fink, "Time reversal of speckle noise," *Phys. Rev. Lett.*, vol. 106, art. no. 054301, 2011.
 - (111) W. Lamberta, L.A. Cobusa, T. Frappartb, M. Fink, and A. Aubrya, "Distortion matrix approach for ultrasound imaging of random scattering media," *PNAS*, vol. 117, no. 26, pp. 14645-14656, 2020.
 - (112) H. Bendjador, T. Deffieux, and M. Tanter, "The SVD beamformer : Physical principles and application to ultrafast adaptive ultrasound," *IEEE Trans. Med. Imag.*, vol. 39, no. 10, pp. 3100-3112, 2020.
 - (113) A.C. Luchies and B.C. Byram, "Deep neural networks for ultrasound beamforming," *IEEE Trans. Med. Imag.*, vol. 37, no. 9, pp. 2010-2021, 2018.
 - (114) A.C. Luchies and B.C. Byram, "Assessing the robustness of frequency-domain ultrasound beamforming using deep neural networks," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 67, no. 11, pp. 2321-2335, 2020.
 - (115) J. Tierney, A. Luchies, M. Berger, and B. Byram, "Evaluating input domain and model selection for deep network ultrasound beamforming," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 7, pp. 2370-2385, 2021.
 - (116) B. Luijten, R. Cohen, F.J. de Bruijn, H.A.W. Schmeitz, M. Misch, Y.C. Eldar, and R.J.G. van Sloun, "Adaptive ultrasound beamforming using deep learning," *IEEE Trans. Med. Imag.*, vol. 39, no. 12, pp. 3967-3978, 2020.
 - (117) R. Hiki, M. Omura, R. Nagaoka, and H. Hasegawa, "Beamspace-domain learning of minimum variance beamformer with fully convolutional network," *Jpn. J. Appl. Phys.*, vol. 62, art. no. SJ1050, 2023.
 - (118) Z. Lei, S. Gao, H. Hasegawa, Z. Zhang, M. Zhou, and K. Sedraoui, "Fully complex-valued gated recurrent neural network for ultrasound imaging," *IEEE Trans. Neural Netw. Learn. Syst.*, doi:10.1109/TNNLS.2023.3282231.
 - (119) I.A.M. Huijben, B.S. Veeling, K. Janse, M. Misch, and R.J.G. van Sloun, "Learning sub-sampling and signal recovery with applications in ultrasound imaging," *IEEE Trans. Med. Imag.*, vol. 39, no. 12, pp. 3955-3966, 2020.
 - (120) J. Lu, F. Millioz, D. Garcia, S. Salles, D. Ye, and D. Friboulet, "Complex convolutional neural networks for ultrafast ultrasound imaging reconstruction from in-phase/quadrature signal," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 2, pp. 592-603, 2022.
 - (121) M. Gasse, F. Millioz, E. Roux, D. Garcia, H. Liebgott, and D. Friboulet, "High-quality plane wave compounding using convolutional neural networks," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 64, no. 10, pp. 1637-1639, 2017.
 - (122) Z. Zhou, Y. Wang, J. Yu, Y. Guo, W. Guo, and Y. Qi, "High spatial-temporal resolution reconstruction of plane-wave ultrasound images with a multichannel multiscale convolutional neural network," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 65, no. 11, pp. 1983-1996, 2018.
 - (123) J.-Y. Lu, P.-Y. Lee, and C.-C. Huang, "Improving image quality for single-angle plane wave ultrasound imaging with convolutional neural network beamformer," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 4, pp. 1326-1336, 2022.
 - (124) D. Perdios, M. Vonlanthen, F. Martinez, M. Arditi, and J.-P. Thiran, "CNN-based image reconstruction method for ultrafast ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 4, pp. 1154-1168, 2022.
 - (125) Y. Qi, Y. Guo, and Y. Wang, "Image quality enhancement

using a deep neural network for plane wave medical ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 68, no. 4, pp. 926-934, 2021.

- (126) M. Tanter, J. Bercoff, L. Sandrin, and M. Fink, "Ultrafast compound imaging for 2-D motion vector estimation: Application to transient elastography," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 49, no. 10, pp. 1363-1374, 2002.
- (127) J.A. Jensen, O. Holm, L.J. Jensen, H. Bendsen, S.I. Nikolov, B.G. Tomov, P. Munk, M. Hansen, K. Salomonsen, J. Hansen, K. Gormsen, H.M. Pedersen, and K.L. Gammelmark, "Ultrasound research scanner for real-time synthetic aperture image acquisition," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 52, no. 5, pp. 881-891, 2005.
- (128) J.A. Jensen, H. Holten-Lund, R.T. Nilsson, M. Hansen, U.D. Larsen, R.P. Domsten, B.G. Tomov, M.B. Stuart, S.I. Nikolov, M.J. Pihl, Y. Du, J.H. Rasmussen, and M.F. Rasmussen, "SARUS: A synthetic aperture real-time ultrasound system," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 60, no. 9, pp. 1838-1852, 2013.
- (129) B.Y.S. Yiu and A.C.H. Yu, "GPU-based minimum variance beamformer for synthetic aperture imaging of the eye," *Ultrasound Med. Biol.*, vol. 41, no. 3, pp. 871-883, 2015.
- (130) J.P. Åsen, J.I. Buskenes, C.I.C. Nilsen, A. Austeng, and S. Holm, "Implementing capon beamforming on a GPU for real-time cardiac ultrasound imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 61, no. 1, pp. 76-85, 2014.
- (131) D. Hyun, L.L. Brickson, K.T. Looby, J.J. Dahl, "Beamforming and speckle reduction using neural networks," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 66, no. 5, pp. 898-910, 2019.
- (132) K. Ando, R. Nagaoka, and H. Hasegawa, "Speckle reduction of medical ultrasound images using deep learning with fully convolutional network," *Jpn. J. Appl. Phys.*, vol. 59, art. no. SKKE06, 2020.
- (133) M. Xian, Y. Zhang, H.D. Cheng, F. Xu, B. Zhang, and J. Ding, "Automatic breast ultrasound image segmentation: A survey," *Pattern Recognit.*, vol. 79, pp. 340-355, 2018.
- (134) S. Liu, Y. Wang, X. Yang, B. Lei, L. Liu, S.X. Li, D. Ni, and T. Wang, "Deep learning in medical ultrasound analysis: A review," *Engineering*, vol. 5, pp. 261-275, 2019.
- (135) M.F. Rasmussen, T.L. Christiansen, E.V. Thomsen, and J.A. Jensen, "3-D imaging using row-column-addressed arrays with integrated apodization-Part I: Apodization design and line element beamforming," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 62, no. 5, pp. 947-958, 2015.
- (136) T.L. Christiansen, M.F. Rasmussen, J.P. Bagge, L.N. Moesner, J.A. Jensen, and E.V. Thomsen, "3-D imaging using row-column addressed arrays with integrated apodization-Part II: Transducer fabrication and experimental results," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 62, no. 5, pp. 959-971, 2015.
- (137) J. Hansen-Shearer, M. Lerendegui, M. Toulemonde, and M.-X. Tang, "Ultrafast 3-D ultrasound imaging using row-column array-specific frame-multiply-and-sum beamforming," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 2, pp. 480-488, 2022.
- (138) J.A. Jensen, M. Schou, L.T. Jørgensen, B.G. Tomov, M.B. Stuart, M.S. Traberg, I. Taghavi, S.H. Øygaard, M.L. Ommen, K. Steenberg, E.V. Thomsen, N.S. Panduro, M.B. Nielsen, and C.M. Sørensen, "Anatomic and functional imaging using row-column arrays," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 69, no. 10, pp. 2722-2738, 2022.
- (139) L.T. Jørgensen, S.K. Præsius, M.B. Stuart, and J.A. Jensen, "Row-column beamformer for fast volumetric imaging," *IEEE Trans. Ultrason., Ferroelectr., Freq. Control*, vol. 70, no. 7, pp. 668-680, 2023.

(US 研究会提案, 2023 年 12 月 3 日受付,
2024 年 1 月 5 日再受付)



長谷川英之 (正員: シニア会員)

2002 東北大学助手, 2005 同講師, 2007 同助教授, 2015 より現職. 専門は医用超音波工学. 博士(工学).

確率的インメモリコンピューティングとその AI 応用

Stochastic In-Memory Computing and Its Applications to Artificial Intelligence

浅井哲也 Tetsuya ASAI

アブストラクト 1960年代に提唱された確率的コンピューティングのフレームワークを用いると、特定の算術演算器を極めて少ない素子で表現できるため、超並列・省電力ハードウェアが構成可能になる。ただし、できる算術演算は限られ、演算精度と演算時間のトレードオフの課題も残る。近年、算術演算が比較的限られ、かつ低精度でも“それなり”の性能を出せる AI の演算（推論・学習の演算）に確率的コンピューティングを適用する試みが行われてきた。AI 適用において残る課題は、パラメータを保存するメモリとの界面（通常演算と確率演算のインタフェース）のオーバーヘッドが大きいことであるが、この問題についても近年解決の糸口が見えている。これらの技術を統合すると、AI の推論・学習に必要な全ての演算素子・メモリを「確率的インメモリコンピューティング」で計算できるエッジ AI ハードウェアの未来が描ける。本稿ではそれらの要素技術、課題・問題の解決策、統合 AI アーキテクチャについて解説し、確率的インメモリコンピューティングの実 AI 応用について俯瞰する。

キーワード 確率的コンピューティング、メモリ回路、集積回路、電子回路、人工知能

Abstract The stochastic computing framework proposed in the 1960s allows certain arithmetic operators to be represented with very few elements, making it possible to construct massively parallel and power-saving hardware. However, the number of arithmetic operations that can be performed is limited, and the trade-off between arithmetic precision and the time required for the operation remains an issue. In recent years, attempts have been made to apply stochastic computing to AI, where the types of arithmetic operation are relatively limited and performance can be “reasonable” even with low precision. A possible solution to this problem has been found in recent years. Integrating these technologies will enable us to envision the future of edge AI hardware that can compute all the arithmetic elements and memory required for AI inference and learning using “stochastic in-memory computing”. In this paper, we describe those elemental technologies, solutions to issues and problems, and integrated AI architectures, and provide a bird’s-eye view of real AI applications of stochastic computing.

Key words Stochastic computing, Memory circuits, Integrated circuits, Electronic circuits, Artificial intelligence

1. ま え が き

1960年代に提唱された確率的コンピューティングは、多ビットのデジタル値をバイナリストリーム化することで演算リソースを低減させる計算手法である^{(1),(2)}。多ビット情報を1ビットずつ時間方向に逃がし、確率の法則を利用して論理演算を行う手法といってもよい。確率的コンピューティングの利点は三つあるだろう：(1) 多くのリソースを消費する多ビットの論理演算を極めて少数の論理ゲートで計算できる（例えば、確率 p_1 と p_2 で論理1となるランダムビット列同士を AND ゲートに入力するとその積 $p_1 p_2$ が出力される（図1）、つまり AND ゲート一つで乗算ができる）、(2) そ

のため、乗算を含む大規模並列演算が可能（通常の高ビット乗算器を多数集積することは簡単ではないが、AND ゲートであれば大規模集積が可能）、(3) 演算は確率の法則に基づいて行われ、多少のビット反転は深刻な問題とならない（通常の論理演算では、上位ビットの反転は致命的となる）。このような魅力のあるコンピューティング手法であるが、実用化の兆しは長らく見えなかった。その理由の一つは、確率的コンピューティングで扱える演算種の少なさである。確率的コンピューティングは、計算したい演算と確率の法則を相似させる一種のアナログコンピューティング（ここでいうアナ

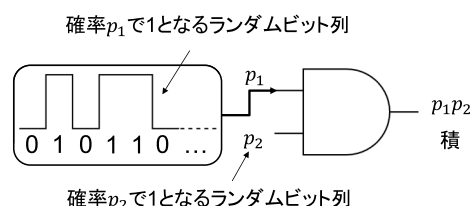


図1 確率的コンピューティングによる乗算の例

浅井哲也 正員 北海道大学大学院情報科学研究科情報エレクトロニクス部門
E-mail asai@ist.hokudai.ac.jp
Tetsuya ASAI, Member (Faculty of Information Science and Technology, Hokkaido University, Kita 14-jo Nishi 9-chome, Kita-ku, Sapporo-shi, 060-0814 Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.18 No.1 pp.71-78 2024 年 7 月
©電子情報通信学会 2024

ログは連続の意味ではなく相似の意)であり、どのような演算でも扱えるというわけではない。2006年頃に、確率的コンピューティングのLDPCデコード処理への応用が提案され、見事な創意工夫により極めて簡単な回路でLDPCデコードに必要なベイズの定理を計算する手法が示されたが⁽³⁾、この技術はその後大きく展開することはなかった。近年は、計算エラーをある程度許容できる人工知能への確率的コンピューティングの応用研究^{(4)~(10)}が増えてきている(図2)。

確率的コンピューティングが実用化されていないもう一つの理由は、直接的に利用可能なメモリ技術(確率的な動作を行うフリップフロップやレジスタ、メモリアレー)が存在しなかったことである。組み合わせ論理回路のみで実現される演算に確率的コンピューティングを適用すると、上記の三つの恩恵を受けることができるが、メモリ要素を含む順序回路を確率的コンピューティングに組み込もうとすると、当時は通常のメモリを使うしか手がなかった。通常のメモリを使うためには、通常の演算と確率的コンピューティングを繋ぐインタフェース(図3)が必要であり、その利用によるオーバーヘッドと前述の三つの利点が相殺されてしまうのだ。組み合わせ論理回路だけでは役に立つ応用はできないし、だからといって順序回路を作ろうとするとインタフェースのオーバーヘッドが大きくなるため、確率的コンピューティングはこれまで実用化できなかったといえよう。では、上記インタフェースのオーバーヘッドを最小化できる(インタフェースをほとんど使う必要のない)メモリが実現できると状況はどう変わるだろうか? 言いかえると、確率的コンピューティングで直接扱うことのできる新しい「確率的メモリ」技術が

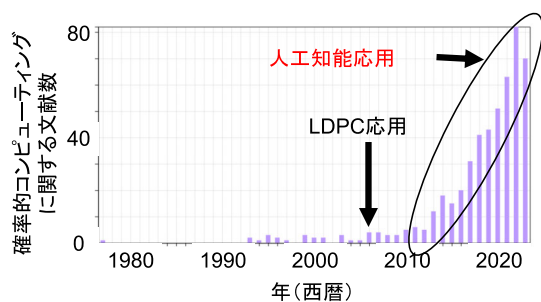


図2 確率的コンピューティングの論文数推移

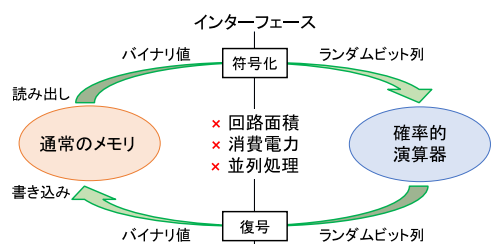


図3 確率的コンピューティングで通常のメモリを使うためのインタフェース(符号化・復号)

完成すると、確率的コンピューティングはどのように進化するだろうか? 本論文では、確率的メモリ^{(9),(10)}の人工知能応用を例題として、その潜在能力について解説したい。

2. 確率的メモリとは

通常のメモリ素子(ラッチやFF)はバイナリ値を静的に記憶するものである。一方、確率的メモリは0~1の確率(アナログ値)を静的に記憶し、その記憶している確率で論理1を出すランダムビット列(動的出力)を生成する。これが確率的メモリの読み出し信号となる。記憶値(確率)の更新は、直接狙った値で更新するのではなく、現在の記憶値を一定量増やす(または減らす)という方法で行われ(図4)^{(9),(10)}、この点が通常のメモリと大きく異なる点である。もう少し具体的に説明すると、確率的コンピューティングで扱われるランダムビット列は、ある時刻の値だけを観測しても意味がなく、一定時間観測してその時間内に何個の論理1が含まれるかをカウント(復号)しなければ、そのビット列が表現する値を知ることができない。また、前述のメモリインタフェースを完全に排除するためには、確率的メモリの読み出し及び書き込み信号の両方がランダムビット列でなければならない。よって、書き込み許可(WE)がされている状態で確率的メモリの記憶値をランダムビット列で更新するためには、復号により狙った値(ビット列が表現する値)を書き込むのではなく、ある時刻でランダムビット列の値が1(または0)であれば、確率的メモリが現在記憶している値を少し増やす(または減らす)、という更新方法しか取れないことに注意されたい。

さて、このような確率的メモリを作るためにはどうすればよいのか? まず、確率的メモリは読み出し信号としてランダムビット列を生成しなければならない。そのためには、0または1の出力値を保持しつつ、記憶している確率でランダムに論理1を出力しなければならない。前者の出力値の保持のために、図5左に示すような二重井戸型ポテンシャルをもつ双安定系の回路を用意する。この系は、リセット後の初期値を V_m (V_{DD} とGNDの中点)より大きく(または小さく)すると、 V_{DD} (論理1)(またはGND(論理0))で安定するものである。また後者のために、この系をリセットする瞬間にオフセット V_m のノイズを与える。その初期値が V_m より大きく(または小さく)なれば、 V_{DD} (またはGND)で系は安定する。安定にかかる時間が十分に短ければ、この一連の動作(リセット→ノイズ印加→安定)を繰り返すことで、

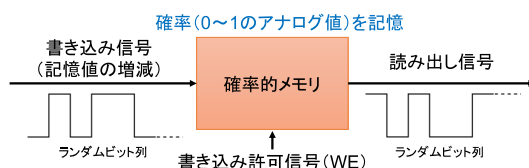


図4 確率的メモリの概念図

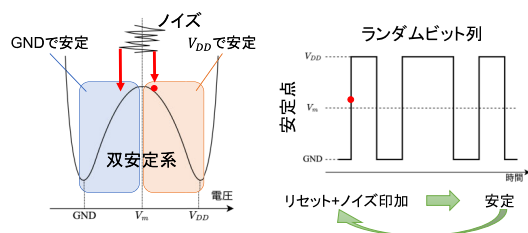


図5 確率的メモリがランダムビット列を生成する仕組み

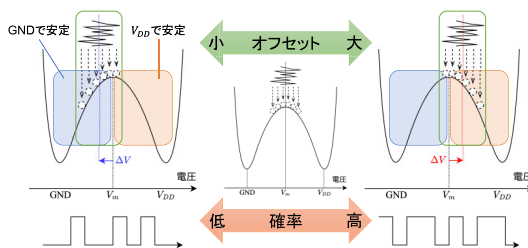


図6 ノイズオフセットの変化によるランダムビット列の確率変化

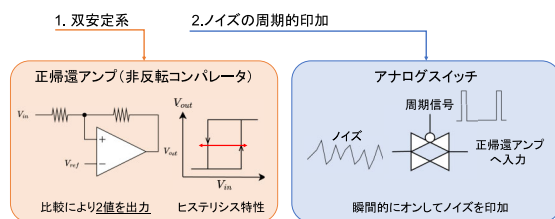


図7 確率的メモリの構成要素 (1, 2)

図5右に示すような確率0.5で V_{DD} (GND)となるランダムビット列が生成されるだろう。ここで、ノイズのオフセット電圧が V_m よりも小さい場合を考える(図6左)。この場合、ポテンシャル中心から左側にノイズのオフセットが移動するため、その移動量を増やすにつれ系が V_{DD} で安定しにくくなる。一方、オフセット電圧が V_m よりも大きい場合は、ポテンシャル中心から右側にノイズのオフセットが移動するため、その移動量を増やすにつれ系がGNDで安定しにくくなる(図6右)。よって、このオフセット値を電圧として記憶するアナログメモリ素子を用意し、その素子からオフセット値を読み出してノイズを生成し、それを双安定系のリセット時の初期値として設定するような回路を組み上げれば上手くいきそうだ。

図7に電子回路による双安定系の例と、双安定系のリセットに用いるアナログスイッチの回路図を示す。双安定系には、ヒステリシス特性をもつ正帰還アンプ(非反転コンパレータ)を用いてみよう。無論、双安定系としてCMOSラッチを用いてもかまわない。アナログスイッチの片端子にはノイズ源を接続し、もう一方の端子は正帰還アンプの V_m へ接続する。このスイッチをデューティ比の小さい周期信号で瞬間的かつ周期的にオンにして、双安定系をノイズの電圧

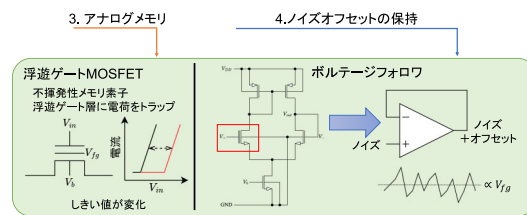


図8 確率的メモリの構成要素 (3, 4)

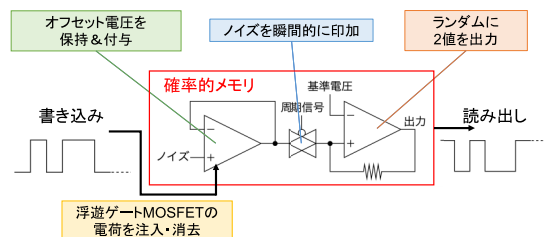


図9 確率的メモリの全体構成

でリセットする。また、図8に確率的メモリで使用するアナログメモリの例と、ノイズオフセットを保持する回路の例を示す。今回はアナログメモリとして浮遊ゲートMOSFETを用いたが、もちろんReRAMなどのアナログ不揮発メモリを用いた構成も考えられる。同図に示すように、ボルテージフォロワを構成する差動対の片側のMOSFETを浮遊ゲートMOSFETで代替し、そのゲートにノイズを与えると、浮遊ゲート電圧 V_{fg} がノイズのオフセット電圧となる。

図9に要素回路を組み合わせた確率的メモリの全体構成(赤枠内)を示す^{(9),(10)}。書き込み動作は、ボルテージフォロワ内部の浮遊ゲートMOSFETに対して行う。浮遊ゲートから電子を抜く、または浮遊ゲートへ電子を注入する回路(制御回路及び昇圧回路)の詳細についてはここでは割愛するが、制御回路については、書き込み許可がされているときに、与えられたランダムビット列の値が0のときは V_{fg} が増加し、1のときは減少するような回路を内部に組み込めばよい。無論、書き込みが許可されていないときは、 V_{fg} は変化しない。図8及び図9の構成によって、オフセット V_{fg} のノイズがボルテージフォロワの出力となる。図9のとおり、ボルテージフォロワの出力は、アナログスイッチを介して双安定回路に接続されているため、アナログスイッチがオンになると、双安定系がノイズ電圧でリセットされ、その瞬間の電圧と基準電圧が比較され、0または1で出力が安定する。これが読み出し信号となる。アナログスイッチのオン・オフを制御する信号の周期が、双安定回路の遷移時間よりも十分に大きければ、図9右に示すようなランダムビット列が生成される。ここで重要なことは、生成されたランダムビット列において1が出現する確率は、 V_{fg} が大きくなれば1に近づき、小さくなれば0に近づく、ということである。以上が、確率的メモリの動作の仕組みである。

3. 確率的メモリの動作例

ここから、数段階にわけて確率的メモリの動作を見ていこう。まず、回路シミュレーションにより確率的メモリの動作を確認する。図 10 に示す条件でシミュレーションを行った(オペアンプ LMC6482, アナログスイッチ CD4066 はフリー素材、回路シミュレータには ngspice を用いた)。また、浮遊ゲート MOSFET には理想素子を使い、書き込み動作の代わりに V_{fg} の初期電圧を設定してシミュレーションを行った。また、ノイズには ngspice の理想ノイズ源(オフセット: 2.5 V)を用いたが、実際には集積可能かつ確率的メモリ間で共有可能な線形帰還シフトレジスタ(疑似乱数回路)のあるビット出力をローパスフィルタに通して利用することを想定している。この回路の過渡解析の様子を図 11 に示す。上からアナログスイッチの制御信号(黒点線)、ノイズ(赤点線)、両安定系の出力(青)を表す。スイッチがオンになった瞬間、ノイズ電圧が V_m より大きければ(小さければ)、両安定系の出力は 1 (0) で安定している様子が観測できる⁽¹⁰⁾。図 12 に、オフセットを変更した場合のランダムビット列の変化の様子を示す。図 11 (オフセット 2.5 V)を長時間観測したものが図 12 の上段、オフセットを 2 V にした場合のランダムビット列の例が下段である。上段はおおよ

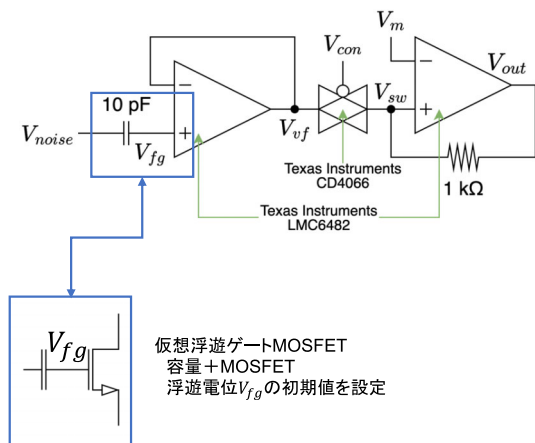


図 10 確率的メモリのシミュレーション回路

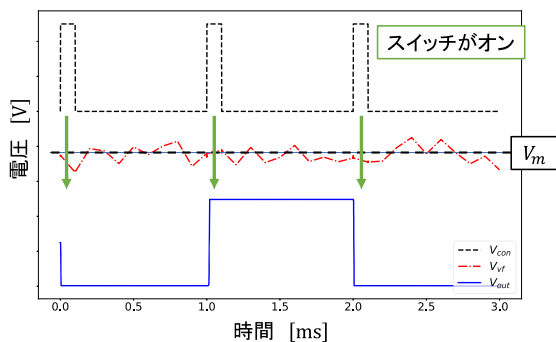


図 11 確率的メモリのシミュレーションの一例

そ確率 0.5 で論理 1 (0) が生成されているが、想定どおり
 オフセットを小さくすることで、下段に示すように論理 1
 (0) が生成される確率が小さくなる様子が見える。また、オ
 フセットを連続的に変化させ、生成されたランダムビット列
 の論理 1 の確率をプロットしたものを図 13 に示す（ビット
 長列：100）。オフセットの増加とともに、出力ランダムビ
 ット列の確率が単調増加する様子が観測できる⁽¹⁰⁾。また、ノ
 イズの振幅を小さく（大きく）すると、確率曲線の傾きが大き
 く（小さく）なるが、これはノイズの振れ幅が小さいと僅
 かなオフセットの変化ですぐに安定状態が決まってしまうこ
 とに起因する。よって実用的には、大きなオフセットを稼げ
 るノイズ生成回路を使うことが望ましい。

次に、手元で実験可能な構成で、確率的メモリの動作を観測してみよう。オペアンプとアナログスイッチには入手しやすい実物の LMC6482 と CD4066 を用いた。浮遊ゲート MOSFET を用いた実験は困難であるため、マイコン (Arduino Uno) を利用して DAC を操作し、浮遊ゲート電圧 V_{fg} を生成した (図 14)。アナログスイッチの制御信号もマイコンにより生成した。その実験結果を図 15 に示す。橙線が Arduino と DAC により生成されたオフセットを含むノイズ

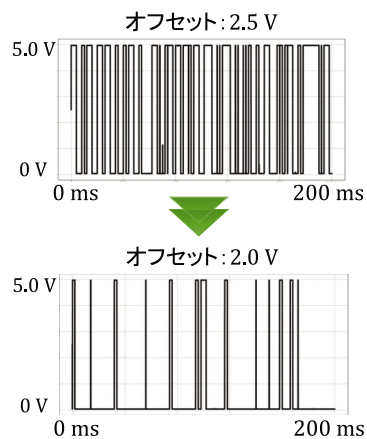


図 12 ノイズオフセット変更による出力ランダムビット列の変化

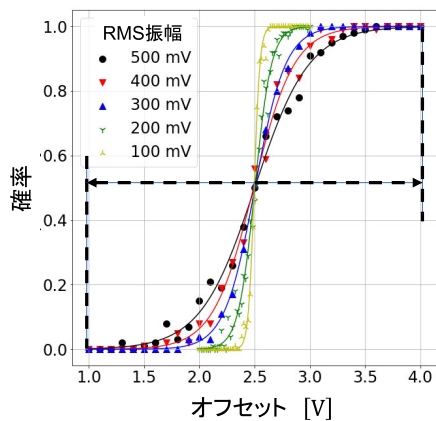


図 13 ノイズオフセット及びノイズ振幅に対するランダムビット列の確率の変化

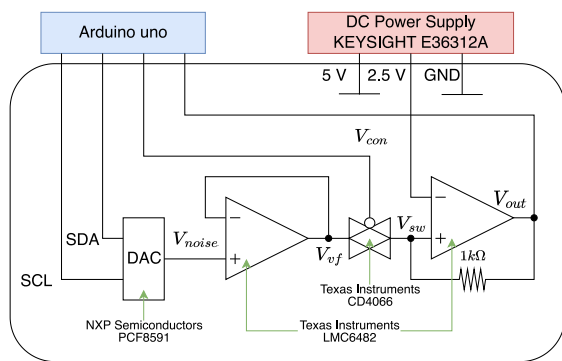


図 14 Arduino を用いた確率的メモリの実験回路

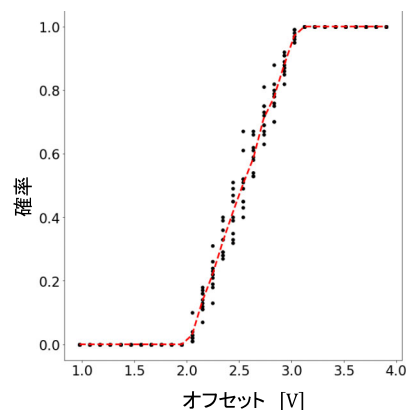


図 17 実験により得られた確率曲線の一例

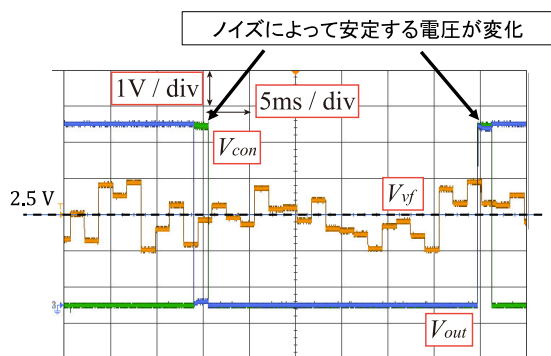


図 15 Arduino を用いた確率的メモリの実験結果

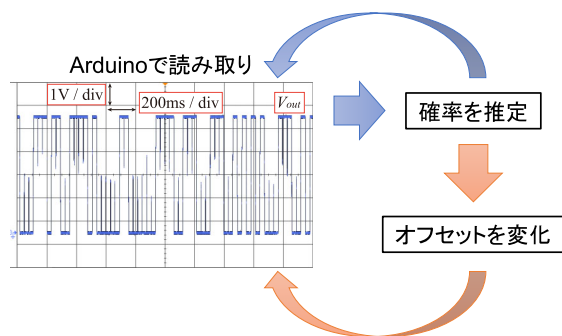


図 16 実験による確率曲線の計算法

であり、これが実回路では V_{fg} に相当する。緑線がアナログスイッチの制御信号で、その立ち上がり時に、ノイズと V_m (2.5 V) が比較され、ノイズが V_m より大きければ (小さければ)、双安定回路の出力 V_{out} が 1 (0) で安定する様子が見える。この実験回路において、シミュレーション (図 13) で示した確率曲線を描いてみる。そのためには図 16 に示すように、あるオフセットで出力ランダムビット列をサンプリング (Arduino Uno でサンプリング) し、論理 1 が出力される確率を計算してから、別のオフセットで出力ランダムビット列をサンプリング・確率計算、という手順を繰り返せばよい。そうして算出した確率曲線の一例を図 17 に示す。試行回数が少ないため実データ (黒点) にはばらつきが見られる

が、オフセット電圧 2～3 Vの間ではおおむね線形な特性が得られ、実機においても想定どおりの動作が見て取れる⁽¹⁰⁾。

4. 確率的インメモリコンピューティング

冒頭で述べたように、確率的コンピューティングは組み合わせ論理回路による演算の大規模並列化に適している。なぜなら、乗算や加算などの基本演算を極めて単純な論理ゲートで実行できるからだ (前述のとおり、乗算は一つの AND ゲートで実行可能)。古典的なデジタル演算アーキテクチャの基本構成は、演算器とメモリのペアである。逐次演算を前提とし、集積度向上の観点からメモリと演算器は分離されている (図 18 左)。この構成の並列化の第一段階は、演算器とメモリのペアを増やすことである。しかし演算器とブロックメモリの数を増やしていくと、すぐに面積・電力の壁が立ち上がる。

では、確率的コンピューティングに確率的メモリを取り入れたアーキテクチャではどうだろうか？ まず、演算器が簡単な論理ゲートで構成されるため、演算器についての面積・電力の障壁は高くないだろう。また、前述の確率的メモリはアレー化せずに、全てのメモリに同時アクセスが可能な状態にしておく。その結果、図 18 右に示すように、確率的メモリが演算器の中に (あるいは演算器が確率的メモリの中に) ばらばらに配置されるような構成が可能となる。これは、演算器とメモリが一体化した構造で、インメモリ (ほかにも様々な呼び名がある) コンピューティングアーキテクチャと呼ばれる。よって、確率的コンピューティングに確率的メモリを導入すると、ごく自然に、本解説論文の主題である「確率的インメモリコンピューティング」となるのだ。

ここで、人工知能の基本演算を確率的インメモリコンピューティングに適用してみよう。図 19 に基本的な全結合型のニューラルネットの構成を示す^{(6)~(8)}。確率的コンピューティングでは負の値を扱えないため、重みを差動 (重み $w \equiv w^+ - w^-$; $0 \leq w^+ \leq 1$) で表す必要がある。また、上記の $w^+ - w^-$ の減算を $w^+(1 - w^-)$ (短絡抑制) のかたちで代替し、活性化関数 $f(x)$ を OR ゲートで構成可能な

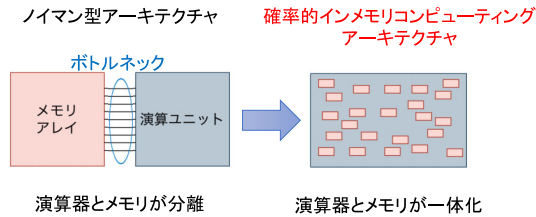


図 18 確率的インメモリコンピューティングの概念

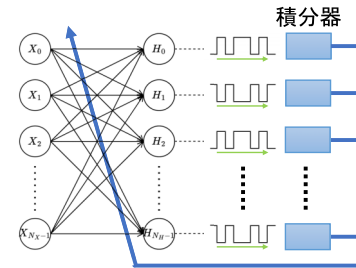


図 21 確率的コンピューティング AI のバッチ学習

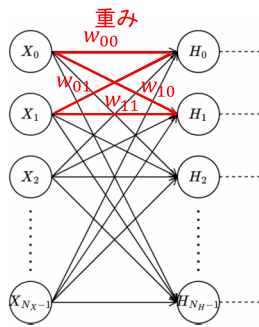


図 19 全結合型ニューラルネットの基本構造

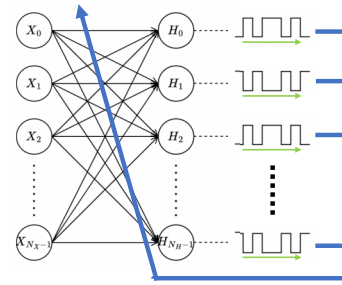


図 22 確率的コンピューティング AI のオンライン学習

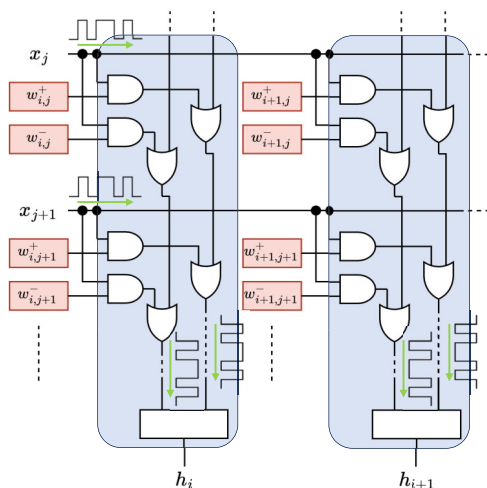


図 20 全結合ニューラルネットの確率的インメモリコンピューティングアーキテクチャの一例 赤ブロック：確率的メモリ；青ブロック：確率的コンピューティングによる積和演算回路。

$(2x-x^2)^2$ ($0 \leq x \leq 1$) とする。積和演算における乗算は AND ゲートで行い、和の演算には OR ゲートによる疑似加算 ($a+b-ab$) を採用する。こうした理由の詳細及び演算変更に伴う新学習則については文献(6)～(8)を参照されたい。上記の工夫によって、小規模の論理ゲートで確率的コンピューティングによる AI 演算（推論と学習）が可能となる。これらをまとめた構成の概略を図 20 に示す。同図から分かる通り、このアーキテクチャは確率的メモリと演算器が密に結合した構造となっており、確率的インメモリコンピューティングの模範例となっている。

さてここで、確率的インメモリコンピューティングによる人工知能の学習について考えてみよう。通常、この形のニューラルネットを学習させる場合、バッチ学習かオンライン学習かを選択を迫られるだろう。一般的には、誤差を積分して重みを更新するバッチ学習の精度が高くなるが、確率的コンピューティングにおいては誤差の積分に復調動作が必要となるため、積分器のリソースオーバーヘッドが大きくなる（図 21）。一方、オンライン学習であれば積分器が不要であるため省リソースとなるが、その代償として精度が犠牲となる（図 22）。よって応用シーンにより学習方法の使い分けが必要となる。

5. 確率的インメモリコンピューティング AI の学習

確率的メモリを用いた「確率的インメモリコンピューティング AI」のオンライン学習の様子を見てみよう。ここでは簡単のため、図 23 に示す単純パーセプトロンを例として、確率的インメモリコンピューティングを適用した場合のオンライン学習の様子を観測してみる。前述のとおり、重みは差動で表し、差動における減算は短絡抑制とし、OR ゲートによる活性化関数を採用し、積和演算における和の演算を疑似加算とし、これらの演算変更に対応した学習則を適用する^{(6)～(8)}。

学習させる問題は、図 24 に示す線形分離問題及び非線形分離問題とする。線形分離問題とは、例えば図 24 左に示すように、解のグループを直線により分離できる問題であり、同図の例のように、AND 関数 ($y=x_0 \cap x_1$ ($x_0, x_1 \in \{0, 1\}$)) の場合は、 $y=1$ となるグループ（図中の青丸）と、 $y=0$ となるグループ（図中の赤い×）を直線で分離できる。一方、図

24 右に示すように XOR 関数の場合は、 $y=1$ となるグループ（図中の青丸）と、 $y=0$ となるグループ（図中の赤い×）を直線で分離できないため、これは線形分離不可能問題となる。通常の単純パーセプトロンではこの問題は扱えないはずだが、上記の確率的コンピューティングを用いると分離境界線が非線形となり、XOR の学習も可能となることを後に示す。

図 25 に OR 関数の学習の様子（重みと正答率の変化）を示す。オンライン学習であるため、収束に時間がかかるものの、正しい答えを学習していく様子が見て取れる。なお、ここで示した重みの値、及び正答率の計算には、ランダムビット列を積分（ビット長：256）した値を用いている。図 24 左の線形分離問題の学習後の分離曲線の例を図 26 に示す。こ

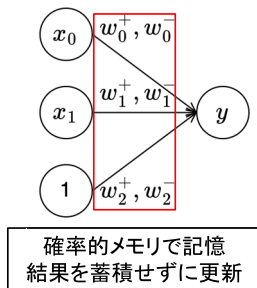
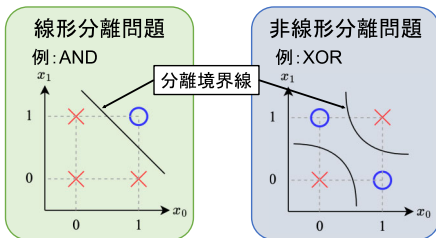


図 23 重みを差動で表した単純パーセプトロン



学習データ: AND・OR・NAND・NOR・XOR

図 24 線形・非線形分離問題の例

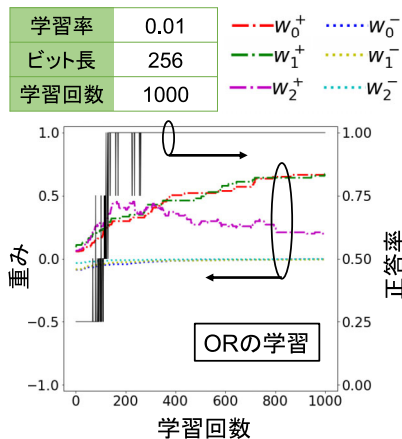


図 25 OR 関数の学習（重みと正答率の変化）

れは、各問題の学習後に、 x_0 と x_1 の値を振り、出力 y の値を色で表現したものである（赤： $y=1$ ，青： $y=0$ ）。全ての論理関数において、正しく解のグループ分けができています。ここで注目したい点は、分離境界が直線ではなく曲線である点だ。このことは前述のとおり、この確率的インメモリコンピューティングを適用した単純パーセプトロンが、線形分離問題だけでなく非線形分離問題も解ける可能性を示している。

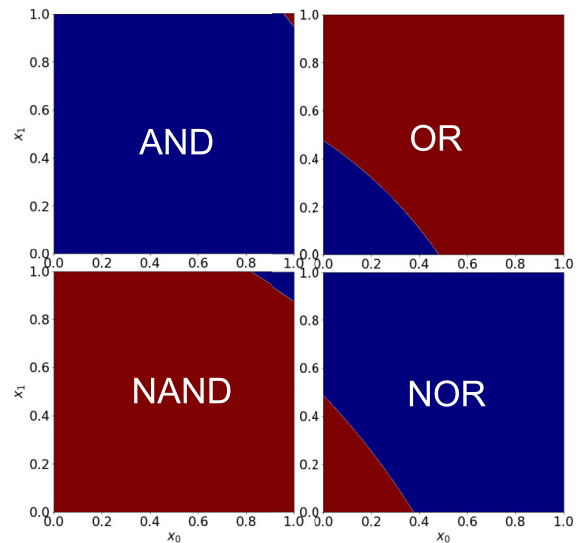


図 26 分離曲線（AND, OR, NAND, NOR）

学習率	0.01
ビット長	256
学習回数	3000

x_0	x_1	XOR
0	0	0
0	1	1
1	0	1
1	1	0

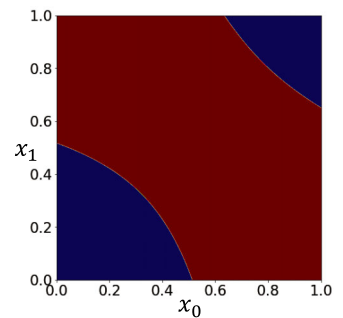


図 27 単純パーセプトロンによる XOR の学習

計算内容	従来計算	提案手法
加算	$a + b$	$a + b - ab$
減算	$a - b$	$a(1 - b)$

分離境界線

$$x_1 = \alpha_0 x_0 + \alpha_1$$

$(\alpha_i \propto w_0^\pm, w_1^\pm, w_2^\pm: \text{定数})$

$$x_1 = \alpha_0 \frac{\alpha_1 x_0^2 + \alpha_2 x_0 + \alpha_3 \pm \alpha_4 \sqrt{\alpha_5 x_0^4 + \alpha_6 x_0^3 + \alpha_7 x_0^2 + \alpha_8 x_0 + \alpha_9}}{\alpha_{10} x_0^2 + \alpha_{11} x_0 + \alpha_{12}}$$

図 28 単純パーセプトロンの分離曲線

図 27 に、確率的インメモリコンピューティング AI による XOR 関数の学習後の分離曲線を示す。このように、単純パーセプトロンでも非線形分離問題の一つである XOR の学習が可能である。ただし、どのような非線形分離問題でも学習できるわけではない。確率的コンピューティング AI の分離曲線は、理論的には図 28 に示す式で表される。通常の単純パーセプトロンにおける加算と減算が、確率的コンピューティングでは疑似加算と短絡抑制により表現されるからだ。この分離曲線の係数 a_i は差動重み (w_j^+ , $j=0, 1, 2$) に比例するものであるが、確率的コンピューティングにおける重要な制約として、全ての値・変数は 0 から 1 の範囲に限定されることを忘れてはならない。そのため、例えば XOR ではなく XNOR を学習させると上手く行かない。その理由は、XNOR の分離曲線を描くためには、 $w_0^+, w_1^+ < 0$ の条件が必要となり、これが確率的コンピューティングの制約範囲外となるからだ。しかしいずれにせよ、通常の単純パーセプトロンよりは高い表現力をもつことは自明である。より大規模かつ多層のニューラルネットの性能については、確率的メモリを用いない確率的コンピューティング AI (上記と同じ非線形性分離曲線を持つ AI) の文献(6)～(8)において評価されており、興味のある読者は是非お目通し頂ければ幸いである。

6. ま と め

本稿では、確率的コンピューティングを俯瞰し、これまで足りていなかった新技術である「確率的メモリ」について解説した後、確率的メモリと確率的コンピューティングを併せた「確率的インメモリコンピューティング」のコンセプトとその人工知能応用について解説した。

確率的コンピューティングを用いると、演算器を極めて少ない素子で構成できるため、大規模並列演算が可能となることを示した。確率的コンピューティングは論理素子があれば実現可能であるが、これは CMOS に限った技術ではなく、ロジックが応用可能な新デバイスなども候補に含まれる。確率的コンピューティングの人工知能への適用はこれまで限定的であったが、近年大きなブレイクスルーがあり、本論文で解説したとおり、推論のみならず学習も可能になった^{(6)～(8)}。課題は、通常メモリとの界面（通常演算と確率演算のインタフェース）のオーバーヘッドが大きいことであるが、メモリインタフェースについては本論文で解説したとおり、「確率的メモリ」^{(9), (10)}の導入により解決されつつある。今後は、確率的メモリをより省面積・低電力にするための新デバイスの開拓が課題となるだろう。

確率的コンピューティングに関するそのほかの課題は、応用・適用範囲の探索であろう。人工知能応用だけでなく、演算結果にある程度のゆらぎがあっても問題のない応用領域（例えば、approximate computing の一部など）に展開できるかもしれない。現行の類似研究・技術（ゆらぎや非厳密性を許容・または活かすコンピューティング技術）は、まだ特

定の計算問題に特化したものであり、それらを俯瞰し、非厳密計算を厳密解に定量的に近づける理論構築とその実証が必要であろう。確率的コンピューティングの回路技術、デバイス技術、応用技術の今後の更なる発展に期待したい。

謝辞 本稿の執筆にあたりご協力を頂きました佐々木義明氏、村松聖俊氏、北海道大学 西田浩平氏、北海道大学 安藤洸太准教授に深く感謝いたします。本研究の一部は以下の助成により遂行されました：JSPS 科研費「基盤研究 (S)」(課題番号：18H05288)、独立行政法人日本学術振興会「研究拠点形成事業」(課題番号：JPJSCCA20220006)。

文 献

- (1) B.R. Gaines, "Stochastic computing systems," in *Advances in Information Systems Science*, pp. 37-172, Springer, 1969.
- (2) Warren J. Gross, Vincent C. Gaudet, *Stochastic Computing: Techniques and Applications*, Springer, 2019.
- (3) S. Sharifi Tehrani, W.J. Gross, and S. Mannor, "Stochastic decoding of LDPC codes," *IEEE Commun. Lett.*, vol. 10, no. 10, pp. 716-718, 2006.
- (4) S. Sato, K. Nemoto, S. Akimoto, M. Kinjo, and K. Nakajima, "Implementation of a new neurochip using stochastic logic," *IEEE Trans. Neural Netw.*, vol. 14, no. 5, pp. 1122-1127, 2003.
- (5) N. Onizawa, K. Matsumiya, and T. Hanyu, "Energy-efficient brainware LSI based on stochastic computation," *信学 FR 誌*, vol. 11, no. 1, pp. 28-39, 2017.
- (6) 浅井哲也, 西田浩平, 佐々木義明, "学習装置, 減算回路及び活性化関数回路," 出願番号：JP2021118326A (2021 年 7 月 16 日), 公開番号：JP2023013866 (2023 年 1 月 26 日公開)。
- (7) Y. Sasaki, S. Muramatsu, K. Nishida, M. Akai-Kasaya, and T. Asai, "Digital implementation of a multilayer perceptron based on stochastic computing with online learning function," *NOLTA*, vol. E13-N, no. 2, pp. 324-329, 2022.
- (8) 浅井哲也, "確率的コンピューティングの再開拓～その場学習が可能な極低電力エッジ AI に向けて～," *情報処理*, vol. 63, no. 3, pp. e8-e14, 2022.
- (9) 浅井哲也, 村松聖俊, 西田浩平, "メモリ回路及びメモリ処理方法," 特願 2023-161571 (2023 年 9 月 25 日)。
- (10) S. Muramatsu, K. Nishida, K. Ando, and T. Asai, "Stochastic memory device based on a bistable system model with a simple analog circuit," *NOLTA*, vol. E15-N, no. 2, pp. 249-261, 2024.

(CCS 研究会提案, 2024 年 3 月 5 日受付,
2024 年 3 月 26 日再受付)



浅井 哲也 (正員)

1999 豊橋技術科学大学博士課程修了。博士 (工学)。1999～2001 北海道大学助手, 2001～2015 北海道大学准教授。2016 から同大教授。2022 から同大大学院情報科学研究所・副研究院長。現在に至る。半導体集積回路を軸に、ニューロモルフィックコンピューティング、人工知能・コンピュータアーキテクチャに関する研究に従事。著書 Reaction Diffusion Computers など。

地域住民に向けた土砂災害 モニタリングシステムの研究開発

Research and Development on Landslide Disaster Monitoring System
for Local Residents

西 正博 Masahiro NISHI
小林 真 Makoto KOBAYASHI
新 浩一 Koichi SHIN

アブストラクト 豪雨による土砂災害が日本各地で頻発しており、地域住民の被害が後を絶たない。被害軽減のためには避難を促す仕組みが必要であり、我々の研究グループでは、土砂災害モニタリングシステムを地域住民と協力して構築し、赤外線カメラで撮影した画像を常時提供している。本論文では、土砂災害モニタリングシステムの概要を述べるとともに、より迅速な土砂災害検知を目的とした、画像解析による危険度の自動検知や電波を用いた土壌水分量の推定の取り組み、及び山間部における土砂災害モニタリングネットワーク構築のための研究開発について概説する。

キーワード 土砂災害モニタリング、赤外線カメラ、無線センサネットワーク、土壌水分量推定

Abstract Landslides caused by heavy rain are occurring frequently in various parts of Japan, and local residents continue to suffer. To reduce damage by landslides, a mechanism to encourage evacuation is necessary, and our research group has developed a landslide monitoring system in cooperation with local residents, which constantly provides images taken with an infrared camera. In this paper, we provide an overview of the landslide monitoring system and describe our trials to automatically detect the degree of risk by image analysis and soil moisture content estimation using radio waves, with the aim of detecting landslides more quickly. We also outline the research and development for constructing a landslide monitoring network in mountain areas.

Key words Landslide disaster monitoring, Infrared camera, Wireless sensor network, Soil moisture estimation

1. はじめに

日本各地において豪雨による災害が後を絶たない。2023年においては、6月の梅雨前線及び台風第2号による大雨や、7月の梅雨前線による大雨、また9月には台風第13号による大雨といった、全国各地で記録的な大雨が生じて、河川の氾濫や土砂災害が多数発生した⁽¹⁾。また近年では2019年8月に発生した九州北部豪雨、2020年7月の九州や中部地方での集中豪雨及び2021年7月の東海地方での大雨などによる被害が発生している。特に2021年7月の大雨では、熱海市で大規模な土石流が発生したことは記憶に新しい。現在では、気象庁による警戒情報や自治体による避難情報がよりきめ細やかに発信されているが、それでもなお多くの人命が失われているのが現状である。

我々の研究グループの所属する広島市立大学の位置する広島市に目を向けると、1999年6月に発生した6.29豪雨災

害、2014年8月の集中豪雨（平成26年8月豪雨）及び2018年7月の集中豪雨（平成30年7月豪雨）により、大規模な土砂災害及び河川氾濫が発生し、土石流やがけ崩れにより死者・行方不明者が出た。これらの被害は、自治体などの出す避難情報のみでは住民の迅速な避難行動に結び付かなかったことが要因であると指摘されている⁽²⁾。避難の遅れは被害の拡大につながるため、いかに住民に自主的に避難行動を促すことができるかが課題である。

このような状況下において、地域住民が自主的に周囲の自然環境の変化を常時モニタリングでき、災害の発生の有無及び予兆を把握できる環境を構築していくことが重要である。避難行動に結び付けるためにも、災害発生可能性を確実に把握し、地域住民が災害の危険性を認識できる仕組みが必要である。しかしながら現在、多くの地域においては、地域住民自身が周囲の状況を常時モニタリングして、異常を検知できる手法は実現できていないと考える。

被害を軽減するため、また早めの避難を促すため、我々の研究グループでは赤外線カメラを用いた土砂災害モニタリングシステムを広島市内に現在8箇所設置して運用し、インターネットを通じて土砂災害危険箇所のカメラ画像を地域住民へ昼夜連続で提供してきた⁽³⁾。2018年（平成30年）7月豪雨の際には、地域住民がスマートフォンにて河川の水位上昇を本システムのカメラ画像にて確認して、避難することを決心したということが報告され⁽⁴⁾、地域住民が危険性を把握しやすい画像での情報提供が有効であることを示してきた。一方で、地域住民が危険箇所の画像を目視し続けることは現

西 正博 正員 広島市立大学大学院情報科学研究科
E-mail nishi@hiroshima-cu.ac.jp
小林 真 正員 広島市立大学大学院情報科学研究科
E-mail m-kob@hiroshima-cu.ac.jp
新 浩一 正員 広島市立大学大学院情報科学研究科
E-mail shin@hiroshima-cu.ac.jp
Masahiro NISHI, Member, Makoto KOBAYASHI, Member, and Koichi SHIN, Member (Graduate School of Information Science and Technology, Hiroshima City University, 4-1 Otsuka-higashi 3-chome, Asaminami-ku, Hiroshima-shi, 731-3194 Japan).
電子情報通信学会 基礎・境界サイエンス
Fundamentals Review Vol.18 No.1 pp.79-87 2024年7月
©電子情報通信学会 2024

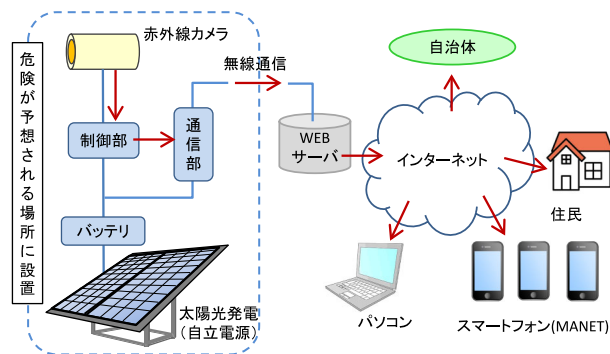
実的ではないため、得られたカメラ画像から自動的に危険か否かを判定し、地域住民に通知することも必要である。我々の研究グループでは、機械学習を用いて、水位の増加を自動的に判別する手法の検討も行っている^{(5),(6)}。そのほか、土砂災害前兆の一つとして土壌水分量に着目して、電波の減衰量によって土壌水分量を推定する試みを実施してきた^{(7)~(9)}。更に、920 MHz 帯の Low Power Wide Area (LPWA) 無線を用いて山間地に土砂災害モニタリングネットワークを構築し、水位や雨量、加速度の各センサを利用して豪雨時の山間地の様子を実際に測定してきた。

本稿では、これまでの我々の研究グループの取り組みを概説するとともに、将来の土砂災害モニタリングネットワークの新たな構成を提案する。

2. 赤外線カメラを用いた電源自立型の土砂災害モニタリングシステム

2.1 土砂災害モニタリングシステムの概要

図1に、本研究グループにて構築し運用している電源自立型の土砂災害モニタリングシステムの構成を示す⁽³⁾。図1(a)にはシステムの構成図を、図1(b)には実際に設置したシステムの写真を示す。本システムでは、土砂災害の危険が予想される箇所に設置することを前提としており、商用電源が確保できない場合でも稼働できるよう、太陽光パネルより電



(a) システム構成



(b) 設置の様子

図1 土砂災害モニタリングシステム

源供給を可能としている。また昼夜問わず危険箇所を監視できるよう、赤外線カメラを利用している。また、無線通信回線を用いることにより、赤外線カメラで撮影された画像をWebサーバに自動的にアップロードしている。本Webサーバは広島市立大学内に設置しており、インターネットに接続されているどの端末からでも撮影された画像にアクセスすることが可能であり、地域住民はそれぞれが所有するパソコンやスマートフォンなどのブラウザにて現在の撮影された画像を閲覧することができる。このため、例えば集中豪雨時において、その場に赴くことなく危険な箇所を安全な場所から確認することができ、避難すべきか否かの判断を住民自ら行うことが可能である。

システムの制御部には小型コンピュータ、通信部には携帯電話回線モジュールを利用している。本システムの消費電力は、昼間は約3W、夜間は約5Wである。これまでの経験から、山間部の周囲が樹木に覆われている環境にシステムを設置した場合には、太陽光パネルの発電能力を200W、バッテリー容量を115Ahとした場合に年間を通じてシステムが稼働できることを確認した。システムを設置する環境によって必要な発電能力は決まり、例えば、空が開けた河川沿いに設置した場合には、100Wの太陽光パネルにてシステムを稼働している。また、画像ファイルのアップロードには、Mobile Virtual Network Operator (MVNO) のデータ通信を用いており、できるだけ安価に運用できる構成としている。通信回線速度は約100~200 kbpsであり、撮影場所の様子が把握できる程度を考慮し、画像サイズは320×240ピクセルとし、画像の配信間隔は5秒を基本設定としている。

小型コンピュータの設定変更や不具合解消のために、遠隔地の管理者から小型コンピュータに接続し遠隔操作を行う必要が生じる場合がある。遠隔操作を実現する手法として、本システムではSSHポートフォワード技術を適用した。図2にSSHポートフォワードによる遠隔操作イメージを示す。小型コンピュータからは起動時にSSHサーバに自動的に接続し、遠隔制御の接続受入用のポートをあらかじめ指定しており、管理者はSSHサーバに接続する際に、小型コンピュータより指定された接続受入用のポートに対して、接続要求を行い、小型コンピュータに接続することが可能となる。SSHサーバから小型コンピュータまでの暗号化された

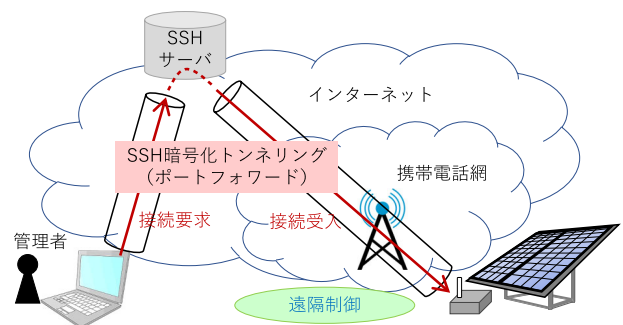


図2 システムの遠隔操作

通信を用いることで、セキュリティの高いアクセスが実現できるのみならず、プライベート IP アドレスしか割り当てられないコンピュータへの外部からの遠隔操作も実現できる。

図 3 に 2024 年 3 月現在の土砂災害モニタリングネットワークの現状を示す。現在では図に示すように広島市内の 8 箇所にモニタリングシステムを設置してネットワーク化している。Web ページ上で図 3 のマップを公開しており⁽¹⁰⁾、地域住民の利用者は各地区をクリックすることで、その場所の現在の様子を撮影した画像と、1 時間前までの 10 分間隔の時系列画像を確認することができる。図 4 に河内地区のモニタリング画像を公開している例を示す。ここでは、最新の現地で取得された画像を 5 秒間隔にて取得しており、取得されるたびに画像を更新している。また、システムのバッテリー残量を簡易的に取得する機能を有しており、5 段階で現在のバッテリー残量もあわせて示している。なお、「日時指定画像ページ」をクリックすることで、本学のファイルサーバに

蓄積されている過去の任意の時刻に撮影された画像を指定することができ、近年の豪雨時における危険箇所の様子を確認することができる。

設置箇所については、これまで土砂災害の被害を受けたことのある地域や、危険箇所として注目されている場所の中から、地域住民の方と協議しながら選定した。例えば、河内地区では土砂災害警戒区域の山中にある砂防ダムの上に設置しており、また祇園北高校では校舎の屋上に土砂災害警戒区域にある砂防ダムをモニタリングする目的で設置している。そのほかのシステムでは、豪雨時における河川や用水路の水位をカメラ画像によりモニタリングする目的としている。設置したシステムの中には、地域住民に協力して頂き、インターネットに接続するため地域住民の自宅の無線 LAN に接続しているシステムや、設置箇所近くの施設から商用電源を供給しているシステムも存在している。

2.2 豪雨時におけるモニタリング画像

本節では、豪雨時において土砂災害モニタリングシステムにて取得された画像の例を示す。2018 年 7 月に広島県を含む西日本各地で豪雨災害が発生した「平成 30 年 7 月豪雨」時に撮影された画像を例に挙げる。当時の豪雨においては、広島市において安芸区や東区において土砂災害の被害を受けたが、我々のモニタリングシステムを設置している安佐北区や安佐南区では大きな災害は発生しなかった。しかしながら、豪災時においてモニタリング画像からは通常時を大きく上回る河川の水位上昇が確認された。

図 5 及び図 6 にそれぞれ、広島市安佐北区に設置した桐原



図 3 土砂災害モニタリングマップ

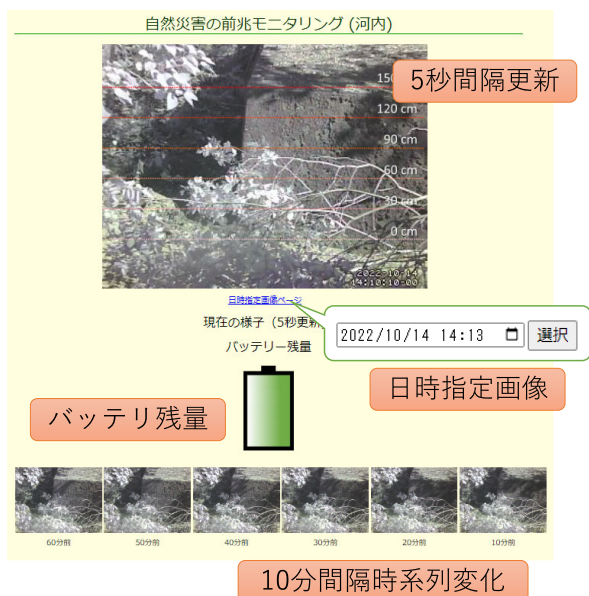


図 4 公開しているモニタリング画像の例



(a) 平常時



(b) 豪雨時

図 5 桐原川におけるモニタリング画像例



(c) 平時時



(d) 豪雨時

図6 根谷川におけるモニタリング画像例

川と根谷川のモニタリングシステムにおいて(a)平常時(2018年7月3日18時)と(b)豪雨時(2018年7月6日18時)に撮影された画像を示す。図5より、桐原川においては、平常時は水位が数十cm程度であるにもかかわらず豪雨時には1m以上水位が増加していることが分かる(一つのブロックが約75cm)。地域住民からの証言によると当時数百m下流域では、越水して畑が浸水したとの情報を得た。当日の水位を示す画像は今後の避難の目安となる可能性が高い。また図6より、根谷川においては、平常時には水位は低く川底のコンクリートが確認できる程度である一方で、豪雨時には水位が増え、岸壁のブロックが全て濁流に覆われていることが確認できる。幸いにも当時、根谷川沿いでは浸水被害は確認されなかったが、この増水時の画像を確認した地域住民が身の危険を感じ避難を決断したということが報告された⁽⁴⁾。このことから、住民の早期避難を促進するためにも、身近な危険な場所をカメラ画像などの直感的に把握しやすい形で確認できることが重要であることが分かる。

2.3 テレビを利用した地域住民への情報提供

前節で述べた、カメラ画像を確認して避難を決断した住民は、比較的若く、スマートフォンなどの情報機器の操作に慣れており、インターネット上のWebページにアクセスして画像を確認していたことを、避難所を運営していた自主防災会会長の方から聞くことができた。また自主防災会会長からは、高齢者でもカメラ画像を容易に確認できるシステムが必要とされているといったお話があった。そこで我々の研究グループでは、高齢者世帯においても普及率が高い、テレビと

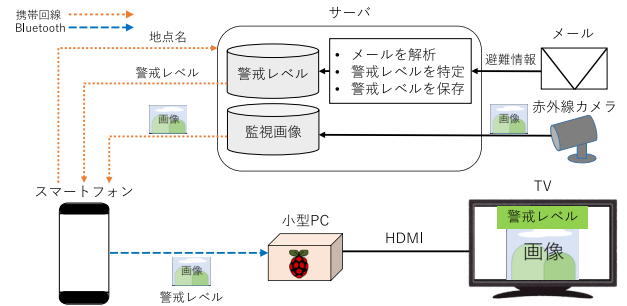


図7 スマートフォンと連携した土砂災害関連情報テレビ通知システム

スマートフォンを活用して、現在の危険箇所のカメラ画像をテレビに映すことで、情報機器の操作に不慣れな高齢者でも早期にカメラ画像を確認できるシステムの開発を行った^{(11),(12)}。

開発したスマートフォンと連携した土砂災害関連情報テレビ通知システムの概要を図7に示す。本システムは、サーバ、スマートフォン、Raspberry Pi 3、テレビ受像機で構成される。サーバでは、地方自治体や県などから送信された防災情報メールを受信・解析して、避難情報の発令地域と警戒レベルを特定する。防災情報メールから特定した各地域の警戒レベルは、サーバに保存する。本システムで用いる画像は、我々の研究グループで運用している土砂災害モニタリングシステムによって撮影された撮影画像としている。

スマートフォンは、サーバ及びRaspberry Pi 3と通信を行う。スマートフォンとサーバは携帯回線を用いて通信を行う。携帯回線で通信を行うことによって、家庭に有線のインターネット回線がない人でも利用可能で、本システムの導入が容易である。地点情報とサーバから取得した警戒レベル、撮影画像はBluetooth通信を用いてスマートフォンからRaspberry Pi 3に送る。

Raspberry Pi 3は地点に対応した警戒レベルと撮影画像をテレビに表示する処理とテレビの電源操作を行う。テレビの電源操作にはHDMI-CEC(High-Definition Multimedia Interface Consumer Electronics Control)のコマンドを使用している。警戒レベルがあらかじめ利用者が設定したしきい値を超えるとHDMI-CECのコマンドを用いてテレビを自動的に起動し、テレビ画面に警戒レベルと撮影画像が表示される。これにより、高齢者は自身が情報機器を操作することなく、危険度を把握することができる。

図8に開発したシステムが動作している様子を示す。専用のスマートフォンアプリは、地点ボタンが選択されるとサーバにその地点情報を送り、対応した地点の撮影画像を取得する。地点ボタン選択後は、スマートフォンから定期的にボタンで選択された地点情報を送り、当該地点の警戒レベルを取得する。またテレビ画面には、取得した警戒レベルやそのときのカメラで撮影された画像が表示される。これまで我々の研究グループでは、実際に地域住民にシステムを操作して頂き、ボタン配置、ボタン配色が異なる操作系を用意して、任



図8 テレビ通知システムの動作検証

意の地点を選択するまでの時間を計測することで、スマートフォンアプリの操作系の評価を行ってきた。その結果、ボタン配色が警戒レベルによって変わるようにすることで、危険度が高い地点を選択するまでの時間が短くなることが分かった⁽¹²⁾。

2.4 画像処理による危険度判定

地域住民にカメラ画像を提供する環境が整ったとしても、地域住民が24時間続けてカメラ画像を確認し続けることは現実的ではない。本節では、これまで我々の研究グループが取り組んできた、機械学習を用いてカメラ画像から自動的に危険度を検出する手法の一例を述べる。

機械学習の対象とするカメラ画像として、モニタリングシステムを設置している南原地区にて昼間と夜間に撮影された画像に着目した。図9に南原地区にて撮影された画像の一例を示す。ここでは、ラベル0を「水位：低」、ラベル1を「水位：高」とした二つのラベルに画像を分類した。学習画像には、2016年12月1日から2017年11月30日の期間に撮影された画像から選定し、昼間、夜間画像ともに1000枚（各クラス500枚ずつ）の計2000枚を用いた。学習にはディープラーニングの一つである、Caffe⁽¹³⁾を使用した。昼間のカラー画像に比べて夜間の画像は赤外線反射による白黒画像となるため、分類器としては、昼間と夜間を分けて構成している。

図10に上記の機械学習により構築した分類器を用いて、実際に2018年7月の豪雨時に南原地区にて得られた9時から18時までの昼間の時系列画像に対して分類した結果を緑色の線にて示す。また、10分間あたりの降雨量をオレンジ色にて示し、目視による画像の分類結果を矢印で示している。なお、図10の下部にはそれぞれのクラスへの分類正確度も参考のため示す。この分類正確度が高いラベルに検証画像が分類されている。9時から11時までの画像は、目視と同様に「水位：低」と分類されていたが、目視で確認した時間よりも早い11時頃から、「水位：高」に分類され始め、12時頃まで「水位：高」に誤分類され続けた。その後は16時頃まで目視と同様に「水位：高」に分類されたが、16時頃



図9 機械学習に用いた画像例（撮影場所：南原川）

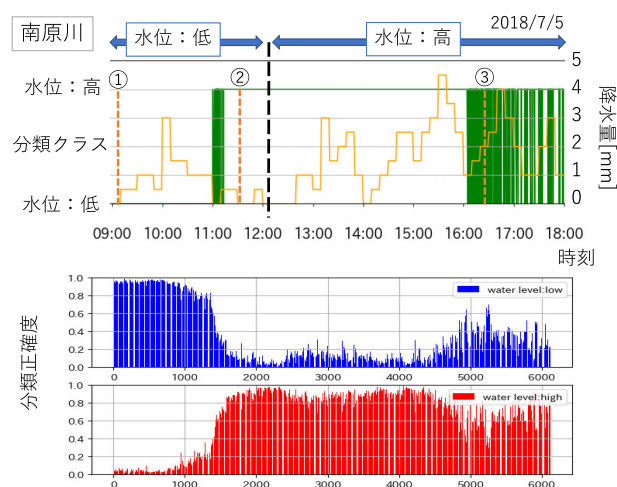


図10 時系列画像に対する分離結果

から、「水位：低」に誤って分類され始めた。①～③の画像を確認したところ、①ではほとんど水位変動がない画像である一方で、②の画像には水位が増加し始め水位線が確認しづらい状況であり、③の画像では水面に白波が立ち始め、水位線と分類器が誤って判定したことが考えられる。以上の結果より、誤分類が生じているものの、機械学習により、おおむね水位の増加を自動的に判断できていることが分かる。今後は、危険度の自動検知精度を向上させ、地域住民への確実な危険度の通知を実現していくことが課題である。

3. LPWAを用いた土砂災害センシングネットワーク

3.1 ネットワーク構成

センサネットワークとして普及が始まっているLPWA (Low Power Wide Area) システムを利用した土砂災害モニタリングの可能性を検証することを目的として2021年度に広島市において実際に土砂災害センシングネットワークを構築した。具体的には、土砂災害危険地域において降雨量や河川の水位（上流と下流）及び加速度をセンシングし、豪雨時や平常時に得られるデータの相互関係を調査することを目指し、広島市安佐北区落合地区にLPWAシステムの一つであ

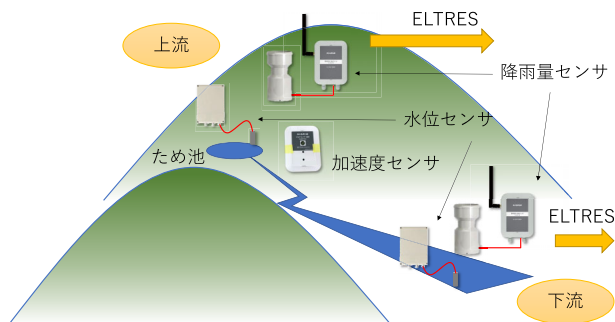


図 11 ELTRES を用いたセンサネットワーク構成



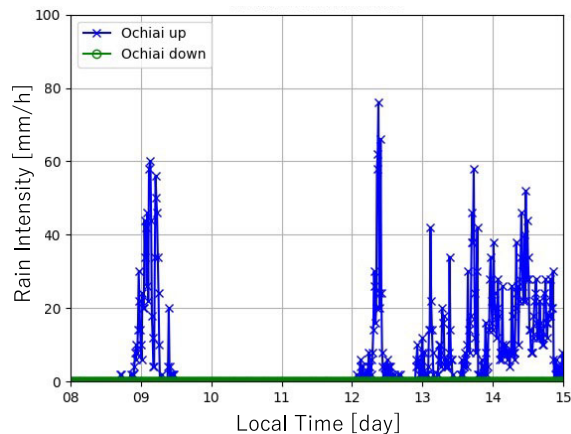
図 12 設置した水位センサと降雨量センサ

る ELTRES⁽¹⁴⁾を利用したセンサネットワークを構築した。

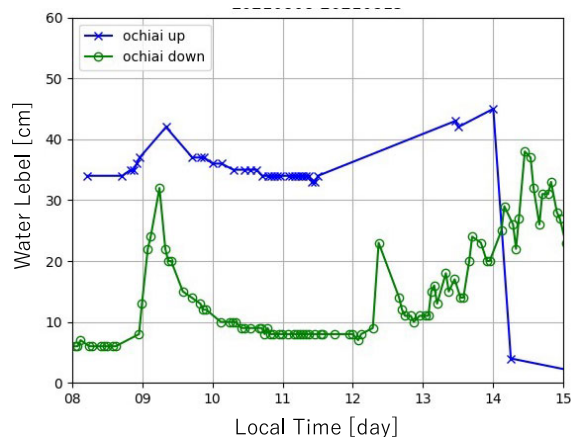
図 11 に落合地区におけるセンサネットワーク構成を示す。落合地区では、上流に土の堤により形成されたため池が存在し、ため池から下流の溪流へとつながる地形となっている。ため池の堤には水位センサ、降雨量センサ、加速度センサを設置し、約 300 m 離れた下流の溪流沿いには水位センサ、降雨量センサを設置した。また、上流・下流それぞれのセンサから得られたデータを ELTRES クラウドにアップロードする構成とした。図 12 に設置した水位センサと降雨量センサの様子を示す。なお加速度センサは同じ堤の約 5 m 離れた場所に設置した。降雨量センサと加速度センサは 15 分間隔、水位センサは 1 時間間隔にてデータをアップロードする構成とした。

3.2 センシング結果

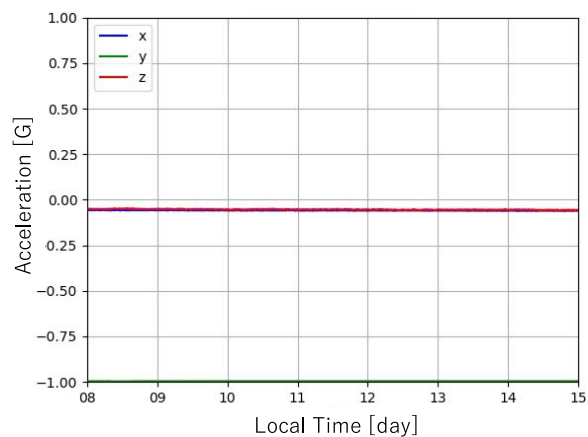
センシング期間の中でも比較的降雨量が多く、特徴的な観測事例が得られた 2021 年 8 月 8 日から 15 日までの 1 週間のセンシング結果を示す。この期間、台風 9 号による大雨、及び広島市の複数箇所でも土砂災害を引き起こした線状降水帯による豪雨があった。図 13 に (a) 降雨量、(b) 水位、(c) 加速度の各センサにより記録された観測結果を示す。なお、上流と下流に降雨量センサを設置していたが、下流に設置していた降雨量センサに不具合が生じていたことから 0 mm/h のまま



(a) 降水量（上流・下流）



(b) 水位（上流・下流）



(c) 加速度（上流）

図 13 センシング結果例（2021 年 8 月 8 日～15 日）

変化していなかった。

図 13(a) の降雨量センサの観測結果より、12 日には最大で約 75 mm/h の降雨強度を記録していたことが分かる。広島市内での気象庁の記録では 1 時間の降雨量が約 15 mm 前後であったことから、山中の雨の降り方が市内のそれとは異なる可能性があり、局所的な豪雨に対して、現地にて直接観測することが重要と考える。

図 13(b) の水位センサの観測結果より、上流でのデータ数

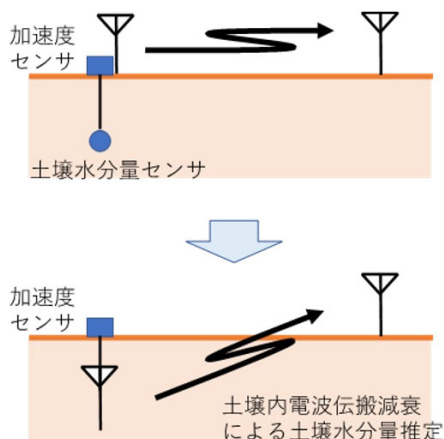


図 14 電波による土壌水分量センシング

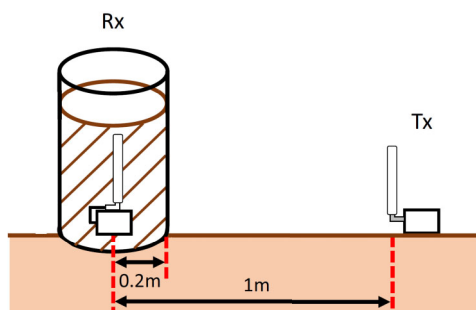


図 15 土壌内電波伝搬減衰特性の実験環境

が下流に比べて少ないことが分かる。これは上流が ELTRES での通信可能範囲に十分入っておらず、通信が不安定であったことが要因である。取得されたデータは限られるが、図 13(b) より 8 月 14 日に入り当日の未明にかけて、上流の水位が急激に下がったことが分かる。後日、現地に調査に行ったところ、ため池の堤の端が崩れており、ため池の水が流失していたことを確かめた。豪雨による山中の地形の変化を捉えた変動であると考えられる。

図 13(c) の加速度センサによる観測結果からは、ため池の堤が崩れていたにもかかわらず、この期間でほとんど変化がなかったことが分かる。今回の堤の崩れはセンサ設置位置と約 3 m 離れた場所で生じた。加速度センサを用いて土砂移動を検出するためには、3 m よりも近傍にセンサを設置する必要があるといえる。

4. 920 MHz 帯電波による土壌水分量推定

土砂災害の前兆現象の一つとして土壌水分量が増加する現象があり、実際に土砂災害時の土壌水分量の上昇が観測されている⁽¹⁵⁾。我々の研究グループでは既存のセンシングシステムが 920 MHz 帯無線ネットワークで構築されることと、文献(16)に示されているように土壌水分量の上昇にともなって電波が減衰することに着目して、センサネットワークに用

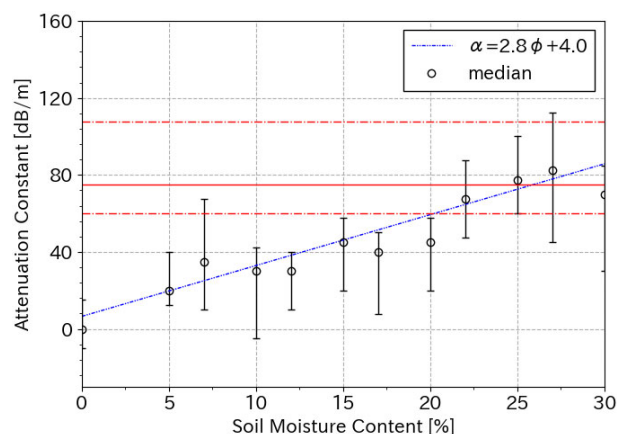


図 16 土壌水分量に対する電波減衰量

いられる 920 MHz 帯電波を利用して土壌内の水分量を推定を試み、電波減衰特性と土壌水分量との関係について検討してきた^{(7)~(9)}。

図 14 に電波による土壌水分量センシングの概念を示す。この例では、加速度センサ及び土壌水分量センサを設置して土砂災害をセンシングする 920 MHz 帯の無線ネットワークを想定している。新たな土壌水分量のセンシング手法では、土壌水分量センサの代わりに、センサ側のアンテナを土中に埋めて、920 MHz 帯電波が土壌内を伝搬するようにアンテナを設置する。そして、土壌水分量に応じて土壌の導電率や誘電率が変化することで電波の減衰量が変わる原理に基づき、電波の受信レベルの低下により土壌水分量を推定する。つまり加速度センサ情報を送信するのみならずその電波の受信レベルの減衰量から土壌水分量も合わせてセンシングすることが期待される。

土壌水分量を変化させたときの電波減衰量の基本特性を把握するため、920 MHz 帯電波送受信器を利用して土壌内を伝搬したときの減衰量を実測により評価した。図 15 に実験環境を示す。本実験では、バケツを利用して土の中に送信アンテナを設置し、20 cm 土中を伝搬後、1 m 離れた受信アンテナにて受信レベルを測定した。またバケツを用いず、1 m の空間中を伝搬させたときの受信レベルとの差分から、電波減衰量を求めた。送受信モジュールに IM 920 s、送受信アンテナにはモノポールアンテナを用いた。図 16 に土壌水分量を変化させたときの電波減衰量 (dB/m) の測定結果を示す。土壌内の不均一性を考慮してバケツを異なる 8 方向に回転させて測定し、その結果として中央値並びに 10% 値と 90% 値のエラーバーにて示している。図 16 より土壌水分量が増加するに従い、電波減衰量が増加していることが確認でき、ほとんど泥水となる土壌水分量 20% 以上となる領域では、減衰量が 80 dB/m 程度となることが確認できた。土壌水分量が一定にもかかわらず測定環境によっては数十 dB の変動があることから、今後はより安定的に土壌水分量を推定できる手法の検討が重要になると考え、大学構内にて長期的に土壌水分量と 920 MHz 帯電波の土壌内伝搬特性の観測を

継続しているところである。

5. 将来の防災ネットワークの提案

これまで LPWA に利用されている 920 MHz 帯電波を用いた土砂災害センシングネットワークの構築を目指し、3 章に述べたようなセンシングを実施してきたことに加え、山中での 920 MHz 帯電波の伝搬特性を測定により評価してきた^{(17),(18)}。そして、山間部においては、樹木による伝搬損失が影響し、電波は届きにくくなることを示してきた。豪雨時には、センシングして得られた土砂災害の危険度を確実に地域住民へ伝達することが重要となるが、920 MHz 帯電波では、十分な到達性を得ることが難しくなる。

一方で我々の研究グループではこれまで、FM 放送波などに割り当てられている VHF 帯電波が災害における情報伝達に重要な周波数帯であると考え、新たに VHF 帯、特に V-Low 帯を用いた災害センシング・情報配信ネットワークを提案している⁽¹⁹⁾。一般に周波数帯が低くなるほど電波伝搬損失が小さくなり、その電波を用いることでネットワークの広域化が容易になる。一方で現在、地上 TV 放送のデジタル化に伴い、90~108 MHz までの V-Low 帯の周波数帯は、一部ワイド FM の放送サービスに用いられているのみであり、有効活用が求められている⁽²⁰⁾。以前から、我々の研究グループでは VHF 帯電波のノイズや韓国からのオーバーリーチ干渉の観測を継続しており、これまでに得られた VHF 帯電磁環境・伝搬特性を新たなセンシング・情報配信ネットワーク構成に適切に反映できると考える。

提案するネットワークの概要を図 17 に示す。本ネットワークでは、山間部に設置したセンシングデバイスからの情報はユニキャストで地域住民の居住地付近のアクセスポイントにアップロードされ、アクセスポイントから地域住民へはブロードキャストにて情報を配信する。無線伝送路には 920 MHz 帯に比べて約 1/10 の周波数帯である VHF 帯を利用することで、より広いエリアをセンシングして情報を配信することを可能とする。伝搬モデルに自由空間損失を仮定した場合、周波数が 1/10 となることで伝搬距離は 10 倍改善されることになり、センシング情報をより広域に到達させることが可能となる。

本ネットワークを実現するためには、以下の課題を検討する必要がある、我々の研究グループで現在研究を進めてい

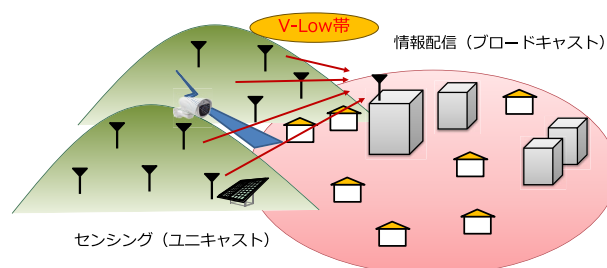


図 17 提案するセンシング・情報配信ネットワーク

る。

- (1) VHF 帯電磁ノイズ、干渉の把握
気象とノイズの関係、韓国からのダクト伝搬干渉特性を長期的観測に基づき明らかにする必要がある⁽²¹⁾。
- (2) 地域環境における伝搬特性
特に低アンテナ高における VHF 帯電波の山地・郊外地・住宅街での伝搬特性の調査が重要である⁽²²⁾。
- (3) センシングデータ送信手法
省電力・長寿命化を目指した送信スケジューリング手法の検討が必要である⁽²³⁾。

提案する VHF 帯を用いたセンシング・情報配信ネットワークを効率的に構築・運用するために今後も研究を進める予定である。

6. ま と め

本稿では、我々の研究グループがこれまで構築・運用してきた土砂災害モニタリングシステムの概要を述べるとともに、より迅速な土砂災害検知を目的として取り組んでいる、画像解析による危険度の自動検知や電波を用いた土壌水分量の推定手法について説明した。また 2021 年度に実施した山間地における LPWA システムを用いた土砂災害モニタリングネットワーク構築について説明するとともに、そのセンシング結果の一例を示し、現地でのセンシングの重要性について述べた。最後に、新たな防災ネットワークとして提案している、VHF 帯、特に V-Low 帯を用いた災害センシング・情報配信ネットワークについて概説し、今後の課題についてまとめた。

謝辞 本研究の一部は、2019 年度総務省 SCOPE 社会展開指向型（19168001）受託研究、2021 年度 NEC ネットズエスアイと広島市との共同研究、2021 年度 2022 年度 KDDI 総合研究所との共同研究による研究成果である。関係各位に感謝の意を表する。

文 献

- (1) 気象庁，“災害をもたらした気象事例，”
https://www.data.jma.go.jp/obd/stats/data/bosai/report/index_1989.html, 2024 年 3 月閲覧。
- (2) 広島市，“平成 30 年 7 月豪雨災害における避難対策等の検証とその充実に向けた提言，”平成 30 年 7 月豪雨災害における避難対策等検証会議，2018。
- (3) 総務省，“人間と ICT の新たな関係，”令和元年度情報通信白書，第 1 部，第 2 章，第 4 節，pp. 203-205, 2019。
- (4) 西正博，古川達也，新浩一，“電源自立型の土砂災害監視カメラシステムの構築と評価，”情処学論，vol. 58, no. 3, pp. 736-744, 2017。
- (5) 徳本敬祐，小林真，新浩一，西正博，“深層学習におけるネットワーク及び画像前処理の違いによる定点観測画像からの土砂災害危険度分類精度の評価，”信学技報，vol. 121, no. 208, ICTSSL2021-26, pp. 48-53, 2021。
- (6) 太田裕亮，新浩一，西正博，“深層学習による画像領域を考慮した土砂災害危険度判定の評価，”第 68 回電気・情報関連学会中国支部連合大会，R17-25-08, 2017。

- (7) 小林真, 岡本真美, 向保一輝, 新浩一, 西正博, “920 MHz 帯電波による土砂災害センシングを目指した土壌水分量にともなう電波減衰特性に関する検討,” 信学論(C), vol. J106-C, no. 11, 2023.
- (8) 岡本真美, 小林真, 新浩一, 西正博, “電波減衰による土壌水分量推定を目指した地中における 920 MHz 帯電波の伝搬特性に関する調査,” 信学論(B), vol. J104-B, no. 11, 2021.
- (9) M. Okamoto, M. Kobayashi, K. Shin, and M. Nishi, “A preliminary experiment on relationship between soil moisture and attenuation constant of 920 MHz band radio waves,” Proc. ISAP 2020, pp. 217-218, 2020.
- (10) 広島市立大学モニタリングネットワーク研究グループ, “自然災害モニタリングマップ,” http://www.wave.info.hiroshima-cu.ac.jp/obs/map_with_web_page_links/all_map_test.html, 2023 年 3 月閲覧.
- (11) 細川拓也, 小林真, 新浩一, 西正博, “スマートフォンと連携した土砂災害関連情報 TV 通知システムの開発と評価,” 信学技報, vol. 122, no. 232, ICTSSL2022-21, pp. 23-28, 2022.
- (12) 細川拓也, 徳本敬祐, 小林真, 新浩一, 西正博, “スマートフォン連携型の土砂災害関連情報 TV 通知システムにおけるユーザビリティ改善の一検討,” マルチメディア, 分散, 協調とモバイル (DICOMO2021) シンポジウム, pp. 1-10, 2021.
- (13) Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell, “Caffe: Convolutional architecture for fast feature embedding,” The 22nd ACM International Conference on Multimedia, pp. 675-678, 2014.
- (14) ソニーセミコンダクタソリューションズ(株), “ELTRESS Technology,” <https://www.sony-semicon.com/ja/eltres/index.html>, 2024 年 3 月閲覧.
- (15) 檀上徹, 酒匂一成, 深川良一, 酒井直樹, 岩佐直人, N.M. Quang, “降雨量, 不飽和浸透挙動, 変位量の観測結果に基づく降雨時表層すべり型崩壊過程の検証,” 土木学会論文集(地圏工学), vol. 68, no. 3, pp. 508-525, 2012.
- (16) S.U. Yoon, L. Cheng, E. Ghazanfari, S. Pamukcu and M.T. Suleiman, “A radio propagation model for wireless underground sensor networks,” 2011 IEEE Global Telecommunications Conference (GLOBECOM 2011), pp. 1-5, 2011.
- (17) 鵜篤志, 向保一輝, 小林真, 新浩一, 西正博, “土砂災害センシングネットワークのための 920 MHz 帯伝搬特性の基礎的評価,” 2023 信学総全大, A-18-9, 2023.
- (18) 白井拓也, 小林真, 新浩一, 西正博, “土砂災害センシングネットワークのための山間地における 920 MHz 帯電波伝搬特性の評価,” 信学技報, vol. 119, no. 401, ICTSSL2019-54, pp. 115-120, 2020.
- (19) 西正博, 小林真, 新浩一, “IoT を活用した広島市立大学における防災の取り組み,” 2023 信学総全大, BK-2-2, 2023.
- (20) 総務省報道資料, “V-Low 帯域(95 MHz~108 MHz)の利活用方策に関する基本方針(案),” 2021.
- (21) 立石李希人, 小林真, 新浩一, 西正博, “V-Low 帯における韓国からのダクト伝搬による受信電力上昇と高層気象の M 曲線との関係性評価,” 信学論(B), vol. J107-B, no. 3, pp. 155-163, 2023. DOI:10.14923/transcomj.2023GWP0016.
- (22) 平晴太郎, 小林真, 新浩一, 西正博, “臨時災害放送局における送信アンテナ周囲の建物を考慮した放射特性に基づく電波伝搬損失の推定,” 信学技報, vol. 122, no. 214, AP2022-142, pp. 216-22, 2022.
- (23) 近藤匠, 小林真, 新浩一, 西正博, “豪雨時における土砂災害情報送信スケジューリングのスリプ時間決定手法の一検討,” 信学技報, vol. 122, no. 232, ICTSSL2022-20, pp. 18-22, 2022.

(ICTSSL 研究会提案, 2024 年 2 月 27 日受付,
2024 年 3 月 26 日再受付)



西 正博 (正員)

1995 大阪大学工学部通信工学科卒業。1997 同大学院工学研究科博士前期課程修了。1999 同大学院工学研究科博士後期課程修了。同年広島市立大学情報科学部助手。2005 同大学助教授。2007 同大学院大学院准教授。2016 より広島市立大学大学院情報科学研究科教授。情報通信ネットワーク, 電波伝搬, 電波科学に関する研究に従事。工学博士。

電子情報通信学会, 情報処理学会, IEEE 各会員。



小林 真 (正員)

2014 大阪大学工学部電子情報工学科中途退学(飛び級)。2016 同大学院情報科学研究科博士前期課程修了。2019 同博士後期課程修了。博士(情報科学)。2017~2019 日本学術振興会特別研究員(DC2)。2019 より広島市立大学大学院情報科学研究科助教。無線ネットワークに関する研究に従事。第一級陸上無線技術士。情報処理学会, 電子情報

通信学会, IEEE 各会員。



新 浩一 (正員)

1995 富山県立大学工学部卒業。1997 大学大学院工学研究科修士課程修了。2006 京都大学大学院工学研究科博士課程修了。2008 広島市立大学大学院情報科学研究科助教。現在, 同大学院情報科学研究科講師。情報通信ネットワーク, 電波科学に関する研究に従事。工学博士。地球電磁気・地球惑星学会, 情報処理学会, 電子情報通信学会各会員。

セキュリティに焦点を当てた ブロックチェーン技術の最新の研究動向

Recent Research Activities in Blockchain Technology Focusing on Security

面 和成 Kazumasa OMOTE

アブストラクト ブロックチェーンは、金融や医療など様々な分野において研究が盛んであり、注目を集めている技術である。一方で、ブロックチェーン・暗号資産へのサイバー攻撃によって、莫大な暗号資産が盗まれる実被害も報告されている。本稿では、ブロックチェーンにおけるセキュリティ面を中心に、ブロックチェーンのセキュリティリスク、及びブロックチェーンを応用したセキュアシステムに関する最新の話題を取り上げ、それらの研究動向について概観する。

キーワード ブロックチェーン、暗号資産、セキュリティ、スマートコントラクト

Abstract Blockchains are a technology that is attracting a lot of research attention in various fields such as finance and healthcare. However, there are reports of cyberattacks on blockchains and crypto-assets, resulting in the theft of huge amounts of crypto-assets. In this article, we focus on the security aspects of blockchains and crypto-assets, and discuss recent topics and research activities on the risk and security of blockchains and secure systems applying blockchains.

Key words Blockchain, Crypto-asset, Security, Smart contract

1. ブロックチェーン分野における研究動向

ブロックチェーンは、情報セキュリティ分野において論文数を飛躍的に伸ばしている研究領域である。図1はElsevier社のScopus情報を用いた情報セキュリティ分野における各研究領域の論文数推移を示しており、図2はブロックチェーン領域における各トピックの論文数推移を示している⁽¹⁾。図1より、情報セキュリティ分野は全体的に右肩上がりの傾向があるなか、ブロックチェーンが2017年頃から急増しており、2019年以降には情報セキュリティ分野で論文数が1位になっていることが分かる。また、図2より、2019～2021年の3年間で論文数の増加が顕著だったのは、大きい順に、(8) サプライチェーン(約3.6倍)、(1) 医療データ(約3.5倍)、(6) IoT(約2.5倍)であった。これらのことから重要な示唆が2点ある。1点目は、情報セキュリティ分野においてブロックチェーン領域の研究論文が急増していることから、ブロックチェーンが注目される研究領域になっている点である。もう1点は、研究前半で盛んであった暗号資産やビザンチン耐性といった基盤的な研究から、サプライチェーン、医療データ、IoTといった応用的な研究にシフトしてき

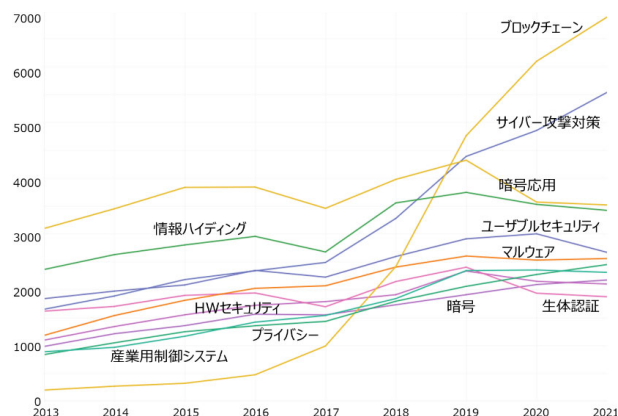


図1 情報セキュリティ領域における各分野の論文数推移

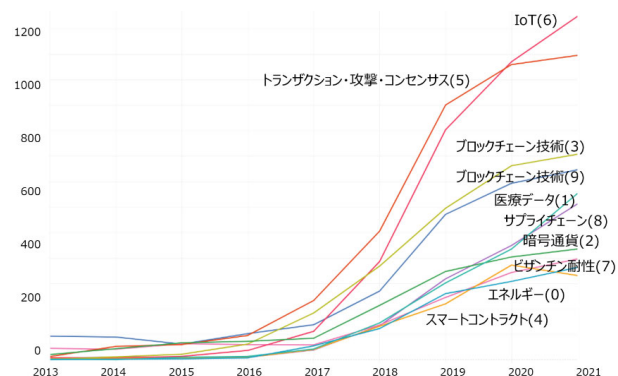


図2 ブロックチェーン分野における各トピックの論文数推移

面 和成 正員 筑波大学システム情報系

E-mail omote@risk.tsukuba.ac.jp

Kazumasa OMOTE, Member (Faculty of Engineering, Information and Systems, University of Tsukuba, 1-1-1 Tennodai, Tsukuba, Ibaraki, 305-8577 Japan)

電子情報通信学会 基礎・境界サイエンス
Fundamentals Review Vol.18 No.1 pp.88-100 2024年7月

©電子情報通信学会 2024

ている点である。

2. ブロックチェーン技術を利用したユースケース

2.1 代表的な暗号資産

Bitcoin は 2008 年に Satoshi Nakamoto という仮名の存在によって提案された暗号資産であり⁽²⁾、ブロックチェーンを使用して取引の正当性とセキュリティを確保している。銀行のような中央の信頼機関は存在せず、ブロックチェーンノードと呼ばれるコンピュータ（以降は単にノードと呼ぶ）で構成されるピアツーピア（P2P）ネットワーク上で取引される。各ユーザはデジタルウォレット（以降は単にウォレットと呼ぶ）によって暗号資産の保有権を管理する。ユーザのウォレットはユーザの秘密鍵によって管理され、秘密鍵をもつユーザはそのウォレットからデジタル署名とともに BTC^(注1)を送ることができる。Bitcoin が稼働した 2009 年から約 15 年が経ち、その価値は 1 BTC あたり約 760 万円である（2024 年 2 月 25 日時点）。また、図 3 は全世界における Bitcoin ノードの分布図を示しており、この時点での Bitcoin ネットワークの到達可能なノード数は全世界で約 18,000 台であった^(注2)。

Ethereum は 2015 年に Vitalik Buterin によって提案された暗号資産である⁽³⁾。Bitcoin のリリースから約 7 年が経って誕生した新しい暗号資産である。Ethereum には、スマートコントラクトと呼ばれるプログラムを実行する仕組みが導入されており、Externally Owned Account（EOA）と Contract Account（CA）という 2 種類のアカウントが存在する。EOA はユーザのアカウントであり、ユーザの秘密鍵によって管理され、秘密鍵をもつユーザはその EOA に対応するウォレットから ETH^(注4)を送ったりコントラクトの生成や実行を行ったりすることができる。一方で、CA はスマートコ

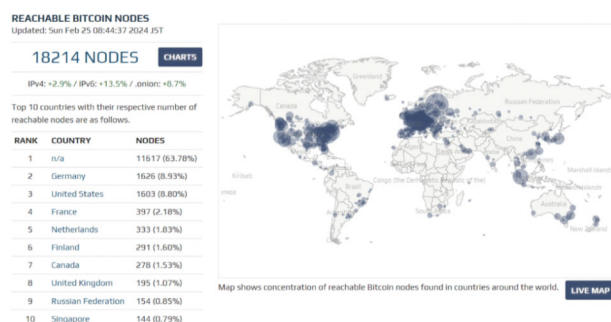


図 3 全世界における Bitcoin ノードの分布（2024 年 2 月 25 日時点）^(注3)

（注 1）：Bitcoin における暗号資産の単位。

（注 2）：NAT 配下に存在するインターネットから到達不可能なノードがカウントされていないことに留意する。

（注 3）：<https://bitnodes.io>

（注 4）：Ethereum における暗号資産の単位。

ントラクトがもつアカウントであり、CA に対応するウォレットが ETH を保持できる。P2P ネットワーク上で暗号資産が取引される点は Bitcoin と同じである。Ethereum が稼働してから約 8 年が経ち、その価値は 1 ETH あたり約 44 万円である（2024 年 2 月 25 日時点）。また、この時点での Ethereum ネットワークの到達可能なノード数は全世界で約 6,300 台であった。

2.2 アルトコイン

アルトコインとは Alternative Coin の略称であり、Bitcoin 以外の暗号資産のことを指すことが多い。知名度の高いアルトコインとしては、上記の Ethereum のほか、Litecoin や NEM などが挙げられる。アルトコインは Bitcoin と同様にブロックチェーンが用いられることが多く、暗号資産における価格追跡 Web サイト CoinMarketCap がモニタリング対象としているものだけでも、2024 年 2 月の段階で 100 万種類以上が存在している。

2.3 Non-Fungible Token（NFT）

NFT は「非代替性トークン」と呼ばれるデジタル資産であり、ブロックチェーンを使用してデジタルコンテンツなどの一意性と保有権を保証する証明書のようなものである。ここでは NFT が付与されたデジタルコンテンツなどを NFT 作品と呼ぶ。NFT はブロックチェーン上のスマートコントラクトによって取引が管理され、これまでも実際に NFT 作品が高額で売買されている。例えば、Beeple による NFT 作品「Everydays - The First 5000 Days」が 2021 年 3 月に約 75 億円で落札され、この売却額は執筆時点で世界最高額となっている。

3. ブロックチェーン

ブロックチェーンは Bitcoin から生まれ、暗号技術と Peer-to-Peer（P2P）ネットワーク技術の両面を併せもつ。P2P ネットワーク上の複数のノードが同じブロックチェーンをもっていることから分散台帳システムであるといわれる。信頼できる第三者機関は必要ない。ブロックチェーンは公開鍵暗号技術が使われており、参加者は自身で秘密鍵・公開鍵を生成し、その鍵ペアをもつ。また、各参加者は暗号資産などを保管するウォレットをもち、このウォレットのアドレスは公開鍵から生成される。そのため、秘密鍵、公開鍵、ウォレットアドレスが相互にひもづけられている。暗号資産などの価値を移転する場合、各参加者がトランザクションを発行し、ブロックチェーンの状態を変更する必要がある。このとき、トランザクションには秘密鍵で生成できるデジタル署名が付与されており、参加者が意図したウォレットからトランザクションが発行されたことを証明できる。ブロックチェーンはセキュリティの性質として次のような耐改ざん性

と高可用性を満たす。

3.1 耐改ざん性

図4にブロックチェーンのデータ構造を示している。各ブロックがその前のブロックのハッシュ値^(注5)を含んでいる。トランザクションがブロックチェーンにいったん記録されると、その後に記録されたトランザクションを変更することは事実上不可能である。あるブロックが変更されると、後続のブロックのハッシュ値が全て変更されるため、あるブロックの改ざんを成功させるにはそれ以降の全てのブロックを作り直さないとはいけない。Bitcoinでは10分程度でブロックの生成が可能となるような条件が設定されているため、後続のブロックが追加されるほど、そのブロックの耐改ざん性が増す。ブロックチェーンを構成する各ブロックには、「トランザクション」と「一つ前のブロックのハッシュ値」などが格納されている。

3.2 高可用性

ブロックチェーンネットワークは、複数のノードによって支えられており、ブロックチェーンが全てのノードで多重化されて保存される。そのため、一時的なノードの故障、時折発生する一部の計算ノードの利用不能、ネットワーク遅延やパケット消失などに耐えるように設計されている。

ブロックチェーンは、パブリックブロックチェーン、コンソーシアムブロックチェーン、プライベートブロックチェーンの3種類に分けることが多い。パブリックブロックチェーンは誰でも参加可能なオープンなネットワークをベースとしており、ブロックチェーンに記録されているデータが公開される。暗号資産には一般的にパブリックブロックチェーンが使われている。コンソーシアムブロックチェーンは複数の組織によって共同で管理運営されるものであり、ネットワークは信頼できる組織で構成される。プライベートブロックチェーンは単一組織で管理運営されるものである。

不特定多数のノードが参加できるパブリックなブロックチェーンであるBitcoinやEthereumには、メインネットとテストネットの2種類が存在する。ここでは、Ethereumを例にとって説明する。メインネットは、本番環境のネットワークであり、市場価値のあるETHが送金されたり実運用

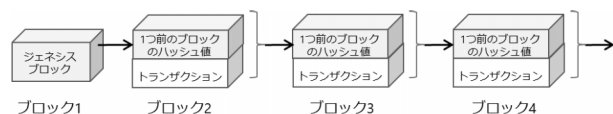


図4 ブロックチェーンのデータ構造

(注5)：暗号学的ハッシュ関数によるハッシュ値を指す。ハッシュ値から元の値を求めることが難しい性質（方向性）や同じハッシュ値になる異なる二つの値を計算するのが難しい性質（衝突困難性）などを有する。

されているスマートコントラクトが稼働したりしている。一方でテストネットとは、主に開発者がテストのために使用するEthereumブロックチェーンであり、メインネットとはほぼ同様の仕組みをもつ。これにより、メインネットのように送金などを行うことが可能である一方、テストネット内で使われるETHに市場価値はない。

BitcoinやEthereumのような主流な暗号資産では、ブロックに格納されている情報を取得できるWebサイトが第三者によって運営されている。これはブロックチェーンエクスプローラと呼ばれており、ブラウザからブロックやトランザクションの内容を確認することができる。そのため、ブロックチェーンをもたない者にとって非常に便利なものである。ただし、表示される情報の正確性はWebサイトの信頼性に依存しており、Webサイトの運営者が特定の情報を意図的に見せないようにすることが可能である点に注意が必要である。具体的なブロックチェーンエクスプローラとしては、BitcoinにおけるBlockchain.com^(注6)やEthereumにおけるEtherscan^(注7)がよく知られている。例えばEtherscanでは、トランザクション、ブロック、ウォレットアドレス、スマートコントラクトなどのオンチェーンデータがWebサービスとして提供されている。

4. 非金融データの格納について

ブロックチェーンには、暗号資産の移転に関する金融データだけでなく非金融データを埋め込むことができる領域が存在する。この領域を利用することで、文書の存在証明やログなどのフォレンジックが可能となる。ここでは、主な暗号資産であるBitcoinとEthereumにおける非金融データの埋め込みについて述べる。Bitcoinは暗号資産に特化しており、スマートコントラクトの実行などは想定していないものの、任意のデータを埋め込むことができる領域が存在する。Bitcoinにおいて意図して設計されたデータの埋め込み可能な領域としては、スクリプトの1命令であるOP_RETURNによる80バイトの領域や、マイナーのみが自由なデータを書き込むことができるCoinbaseによる96バイトの領域などがある。ほかにもOrdinal Inscriptionという仕組みにおいてトランザクションのwitness領域にもNFTデータなどを記録できる。Ethereumは、スマートコントラクトなど非金融データを埋め込むことが想定されている暗号資産であり、Storage領域とextraData領域の大きく2種類の領域が存在する。Storage領域はスマートコントラクトの生成・利用に使用される領域であり、一般の参加者はStorage領域にデータを埋め込むことになる。仕様上の上限は存在しないが、トランザクションの手数料はブロックごとに決められた手数料（gasLimit）を超えることができないため、実質の上限（数百キロバイト）は存在している。一方、extraData領域は

(注6)： <https://www.blockchain.com/ja/explorer>

(注7)： <https://etherscan.io/>

Ethereum ブロックヘッダに存在する領域であり、マイナーのみが書き込める領域である。この領域は一つのブロックにつき 32 バイトしかないため、ファイルを埋め込むためには十分でない。ほかにもトランザクションレシートの Logs 領域にも任意のデータの記録が可能である。

5. スマートコントラクト

非金融データの中で代表的なものにスマートコントラクトがある。スマートコントラクトとは、ブロックチェーン上で契約を自動的に実行するプログラムのことである。スマートコントラクトの概念は、1996 年に Nick Szabo によって初めて提案されている⁽⁴⁾。これは自動販売機によく例えられ、利用者が硬貨を投入し、ボタンを押すと契約が成立するのに似ている。図 5 は、ブロックチェーンにおけるスマートコントラクトの概念図を示している。ユーザは署名付きのトランザクションを発行することによって、スマートコントラクト（プログラム）をブロックチェーン上にデプロイしたりスマートコントラクトを実行したりする。また、スマートコントラクトはブロックチェーンのデータを読み込んだり、別のスマートコントラクトを呼び出したりできる。更に、実行結果をトランザクションレシートとしてブロックチェーン内に出力できる。なお、スマートコントラクトはブロックチェーンをもつ全てのノードが実行する。

Ethereum におけるスマートコントラクトは、Ethereum ネットワーク上の Ethereum Virtual Machine (EVM) と呼ばれる仮想マシンが EVM コードと呼ばれるバイトコードを実行することによって実現される。Solidity などで記述されたコントラクトはコンパイラによって EVM コードにコンパイルされる。そして、ユーザがトランザクションにその EVM コードを格納して送信することによってブロックチェーン上に CA が作られる。このコントラクトを実行するためには、生成された CA に対してユーザがコントラクトの引数をもったトランザクションを送信することが必要となる。そのため、Ethereum のトランザクションにはスマートコントラクトの実行時に引数を渡すためなどに使用される data という領域が存在する。この領域は、プログラムのバイトコードやプログラムへの引数を載せるという性質上、書

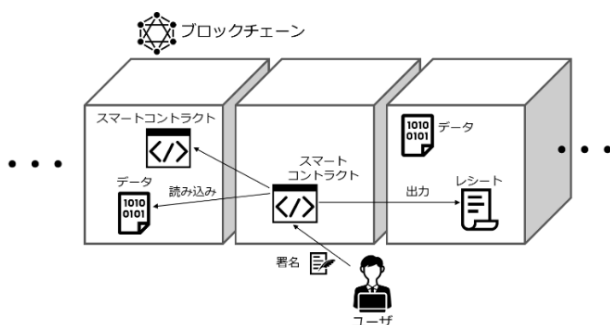


図5 ブロックチェーンにおけるスマートコントラクトの概念図

き込まれる内容とサイズの両面から非常に自由度の高い領域である。

6. 暗号資産の盗難被害

暗号資産に関するインシデントは数多く発生しており、そのようなインシデントを被害対象及び被害原因で分類して分析がなされている⁽⁵⁾。インシデントの被害を受けた対象によって分類すると、「暗号資産取引所」、「暗号資産関連サービス」、「銘柄」の3種類に大きく分類できる。暗号資産取引所には多数の資産及び秘密鍵が保管されており、攻撃の対象になる可能性が高い。暗号資産関連サービスは、ウォレットサービス、Decentralized Finance (DeFi)、Initial Coin Offering (ICO) など取引所を除く暗号資産に関連するサービスと考えることができる。銘柄に分類される Bitcoin や Ethereum をはじめとした暗号資産自体もソフトウェアやハードウェアに脆弱性があり得るため、攻撃の対象になる可能性がある。一方で、被害原因によって分類すると、「人による脆弱性」、「取引所サーバの脆弱性」、「暗号資産関連サービスの脆弱性」、「ブロックチェーン・スマコン脆弱性」の4種類に分類できる。人による脆弱性は、フィッシングや内部犯行など人が原因となって被害につながるものである。これは暗号資産が生まれる前に既に存在していた課題であり、ユーザの安全意識を高めない限り改善は困難である。取引所サーバの脆弱性は、取引所のサービスシステムの脆弱性に起因するものであり、不正アクセスによる被害につながるものである。暗号資産関連サービスの脆弱性は、ウォレットシステムなど他社が開発するシステムの脆弱性に起因するものであり、同様に不正アクセスによる被害につながるものである。ブロックチェーン・スマコン脆弱性は、ブロックチェーンやスマートコントラクトの脆弱性に起因するものであり、そのような脆弱性をついた攻撃被害につながるものである。例えば、51% 攻撃、エクリプス攻撃、Selfish マイニング、スマートコントラクトコードの脆弱性などがある。

被害対象によるインシデントの件数及びその被害額で分類した結果を図6に示している。図6の左図より、被害件数は取引所が最も多く、暗号資産関連サービスと銘柄がほぼ同等の件数である。図6の右図より、被害額は取引所に対するインシデントが圧倒的に多いことが見られる。取引所は多くのユーザのウォレットを管理しているため被害が大きくなりやすい。また、2017年頃から暗号資産関連サービスの件数、2018年頃から銘柄の件数が増加傾向にある。DeFiやICOなどのスマートコントラクト関連の暗号資産サービスの増加やアルトコインの増加が要因であると考えられる。なお、2014年と2018年の被害額が突出しているのは、2014年に発生したマウントゴックス事件と2018年に発生したコインチェック事件が原因である。

被害原因によるインシデントの件数及びその被害額で分類した結果を図7に示している。図7の左図より、ブロックチェーン・スマコン脆弱性によるインシデント件数が近年増

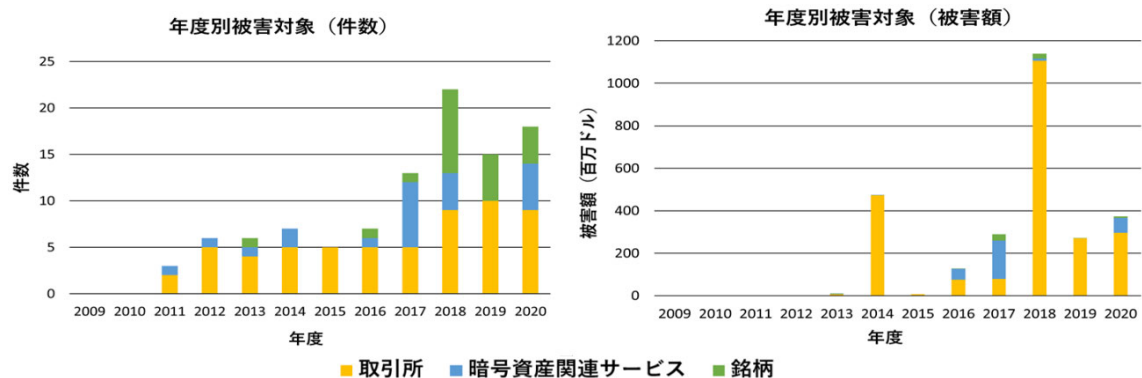


図6 被害対象による分類

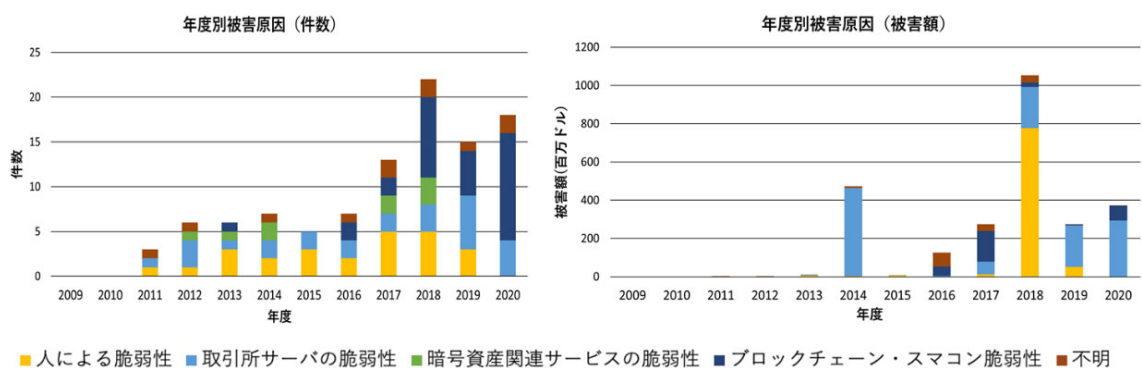


図7 被害原因による分類

234	2018-01-26 03:29:54	92,250,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NA6JSWNF24Y7DVUVPKRNAY7TPOFJJ7Q2URL7KU5
235	2018-01-26 03:28:44	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NDQZVF32WB3LWRNG3IVGHCOCAZWENCNROGEJVCJI
236	2018-01-26 03:18:07	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NB4QJCLTZHVWF8KEMFOONQZFDH3V9IDK3G524
237	2018-01-26 03:14:09	100,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NDZZJBH6JZPYSWRPRYHALLWMTWHQYTOGXRS3HAW
238	2018-01-26 03:02:12	750,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NBKLGXYEVEEGARYPUM52UJFHA3Y6R4LAPU6NP4
239	2018-01-26 03:00:33	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NDQDXOWEIZGJSMAEURXACF4IEHC2C87Q5T56V7SQ
240	2018-01-26 02:58:42	50,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NA7S279KF6ZKQ267TRKCDJ8BWP5JOC2HA5PKCKW
241	2018-01-26 02:57:24	30,000,000	1.25	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG	NCTWFOOVITRZY8YIQ3PE3IMVB29KMED53EWFQ
242	2018-01-26 00:21:14	3,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
243	2018-01-26 00:10:36	20,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
244	2018-01-26 00:09:22	100,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
245	2018-01-26 00:08:21	100,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
246	2018-01-26 00:07:04	100,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
247	2018-01-26 00:06:46	100,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
248	2018-01-26 00:04:56	100,000,000	1.25	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG
249	2018-01-26 00:02:13	10	0.05	NC3B3DNMR2PGEOMF2NKOQGSAM7GYRKA5CSZ	NC4C6PSUW5CLTDT5SXAQJQJGZNE8KFKSMCN77OG

図8 NEM が盗まれたときの履歴^(注8)

えていることが見られる。アルトコインの増加、スマートコントラクトを用いたサービスや取引所の増加が要因であると考えられる。取引所サーバの脆弱性は依然として発生しており増加傾向である。近年、被害額は取引所サーバの脆弱性によるものが比較的多くなっている。また、人による脆弱性のインシデントはほぼ毎年発生しており、近年では暗号資産関連サービスを利用した詐欺も発生している。

上記のとおり、ブロックチェーンシステムはこれまでに何度もサイバー攻撃を受け、莫大な暗号資産が盗まれている。ここでは三つの具体的な被害事例を取り上げる。2018 年 1

月に暗号資産取引所コインチェックから日本円で約 580 億円相当の暗号資産 NEM が盗まれた⁽⁶⁾。NEM が盗まれたときの履歴が NEM ブロックチェーンに記録されており、図 8 はその履歴をブロックチェーンエクスプローラで表示したものである。コインチェック社のウォレット（アドレス：NC3B…）から犯人と思われるウォレット（アドレス：NC4C…）に 8 回に分けて NEM の移転が完了しており、

(注 8) : <https://explorer.nemtool.com>

2018年1月26日になったばかりの深夜0時2分から僅か20分ほどの出来事であった。本事件は、ソーシャルエンジニアリングによって社員の端末がマルウェアに感染させられ、上記ウォレットにおけるNEMの移転権限が奪取されたことが原因であるといわれており、移転のための秘密鍵が奪われた可能性も指摘されている。

2018年5月にBitcoin Goldが51%攻撃を受け約20億円の損害を出した。Bitcoin GoldはBitcoinから2017年10月にハードフォークして生まれた暗号資産の一つである。51%攻撃はノード数が少なくハッシュレート^(注9)が低い暗号資産に起こりやすいといわれており、更に二重支払い攻撃を受けた可能性も指摘されている。51%攻撃は、Proof of Work (PoW) と呼ばれるコンセンサスアルゴリズムを採用している暗号資産（例えば、BitcoinやBitcoin Goldなど）で実行される恐れがある。攻撃者はネットワーク全体の計算量の過半数を支配しようとし、51%攻撃が成立すると二重支払い攻撃が可能となる。なお、Bitcoinはハッシュレートが高いため51%攻撃を受ける確率は限りなくゼロに近いが、Bitcoin Goldなどのハッシュレートが比較的低い暗号資産では51%攻撃を受けるリスクが高くなる。

Uniswap フィッシング事件は、2022年7月に分散型取引所（Decentralized Exchange ; DEX）のUniswapで行われたフィッシング攻撃による事件である⁽⁷⁾。フィッシングの攻撃者はUNIトークン^(注10)を保有するユーザの73,399のウォレットアドレスに対して悪意のあるトークン^(注11)を無料配布（AirDrop）した⁽⁸⁾。攻撃者はEtherscanで表示されるsender情報を操作することによって、攻撃者のアドレスを隠してUniswapの公式アカウントに見せかけることができた。多くの攻撃者がこのようなEtherscanなどのエクスプローラを利用してユーザを欺き、偽の情報を与え、トークンや契約が正当なものであると信じ込ませている。トークンの詳細をEtherscanで見るとFromに「Uniswap V3: PositionsNFT」と記載されており、これを見た被害者はUniswapの公式のアカウントからのUniswapLPトークンであると勘違いした。被害者はEtherscanにおいてトークンに記載されているURLに接続することにより、攻撃者が作ったフィッシングサイトに移動する。図9は実際のフィッシングサイトを示しており、サイト内ではこのトークンがUNIトークンと交換できることが記載されている。このフィッシングサイトは、中央の「Click here to claim」ボタンを押すことによって、自分のアカウントへのフルアクセスを攻撃者に許可してしまう。具体的には、盗難対象である暗号資産及びNFTを管理するスマートコントラクトのSetApprovalForAll関数の許可の画面が表示され、それを許可した被害者のウォレットからNFTが攻撃者に送られてしまう。NFT フィッシング事件に

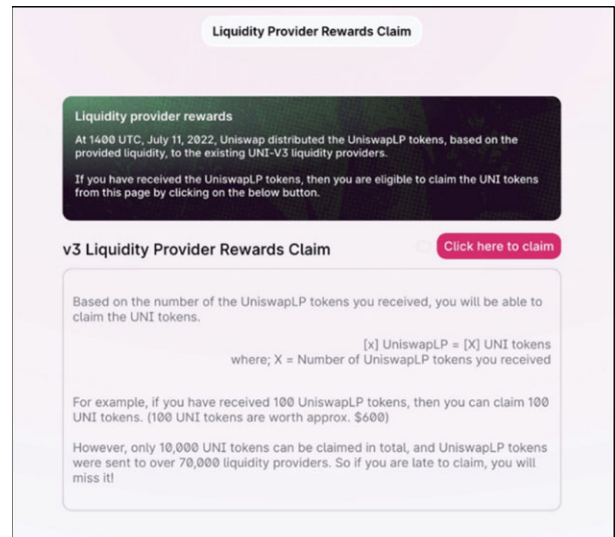


図9 フィッシングサイト

において、被害件数は27件、被害総額は約800万米ドルと推定されている。

7. 暗号資産・ブロックチェーンへのセキュリティリスク

本章では、暗号資産及びブロックチェーン特有のセキュリティリスクについての研究を幾つか紹介する。

7.1 ブロックチェーンの汚染

全てのノードはブロックチェーンデータをローカルコンピュータに保持するため、ブロックチェーンの中に違法なデータが格納されている場合、国や地域によっては違法所持が問われるかもしれない。これをブロックチェーンポイズニング攻撃と呼ぶ。このようなポイズニング攻撃は暗号資産を盗む攻撃ではなく、ブロックチェーンインフラへの攻撃と捉えることができる。攻撃者は様々な不正データをブロックチェーンに埋め込むだけで攻撃が成功するため、ブロックチェーンポイズニング攻撃は誰もが容易に実行できる攻撃であるといえる。ブロックチェーンに違法なデータや悪質なデータを埋め込むことによりブロックチェーン自体が違法・悪質なものになってしまう可能性がある。

Bitcoinブロックチェーンにわいせつ画像などが格納されていることが2018年に報告された⁽⁹⁾。Bitcoinのブロックチェーンに任意のデータを埋め込むことの利点と危険性が議論され、児童ポルノへのリンク集など多くの国で違法な可能性の高いファイルやプライバシーを侵害する内容を含んだファイルがBitcoinのブロックチェーンに埋め込まれていることが明らかになった。これに対して、EthereumはBitcoinよりも大きなデータを埋め込む領域がトランザクションに用意されていることを踏まえ、Ethereumブロックチェーンにマルウェアなどが格納されていることが2019年に報告され

(注9)：ハッシュレートとは、1秒間に何回のハッシュ計算を試すことができるかの見積もり値である。

(注10)：Uniswapが独自に発行しているトークン。

(注11)：実際は単なるERC20トークンであった。

た⁽¹⁰⁾、ブロックに含まれるトランザクションの Storage 領域に書き込まれたデータに対して分析が行われ、実際にどのようなファイルが埋め込まれているのかの分析がなされた。その結果として、三つの exe ファイルが見つかっており、VirusTotal で検索した結果、それらが「W32.Duqu」のマルウェアであることが突き止められている。

一般的な公開データベースに対するポイズニング攻撃として広く知られているものとして、DNS (Domain Name System) キャッシュポイズニングがある。この場合、攻撃内容の検知ができれば、悪意あるデータの削除や修正が可能である。これに対し、ブロックチェーンへのポイズニング攻撃の場合、ブロックチェーンのデータの取り消しや修正が極めて困難であるという特性から同様の対応ができない。また、ブロックチェーンに埋め込まれた情報は P2P ネットワークを通じて世界中のノードに拡散される。ポイズニング攻撃は、ブロックチェーンに任意のデータを埋め込める領域が存在するために可能となる攻撃であり、また世界中のノードが攻撃の影響を受けることに注意されたい。

7.2 ウォレットへの不正アクセス

ブロックチェーンのウォレットは、オンラインバンキングのアカウントと同様に資産を直接的に扱うことができる。ウォレットへのサイバー攻撃が資産の窃取に直結するため、本攻撃は暗号資産を窃取することを目的として実行される。ブロックチェーンは、P2P 型の分散ネットワークにより運用されるサービスであり、柔軟性と運用性の点からインタフェースに JSON-RPC という遠隔操作が実装されている。Bitcoin や Ethereum でも JSON-RPC によるリモートアクセス機能が用意されている。これに関して、脆弱で管理されていないインターフェースに対して遠隔操作を悪用した攻撃が報告されている⁽¹¹⁾⁻⁽¹⁷⁾。なお、Ethereum におけるウォレットへの不正アクセスの数は Bitcoin よりも多いため、以降、Ethereum におけるウォレットへの不正アクセスに関する研究について説明する。

Ethereum プラットホームにおけるセキュリティ上の脆弱性を分析するため、Geth で構築したテストベッドに対して、JSON-RPC や WebSocket を経由して実際に攻撃を仕掛ける実証実験が行われ、Ethereum ノードのモジュールを有効化する攻撃やパズルを抽出する攻撃をはじめとする 6 種類の攻撃について、攻撃が成立する条件や攻撃対策の手法が明らかにされた⁽¹¹⁾。その後、Ethereum ノードの RPC ポート (8545/TCP) への攻撃を観測するためのハニーポットが図 10 のように設置され、様々な分析が行われている。ハニーポットは脆弱性があるように見せかけたおとりのサーバである。これをインターネット上に公開して攻撃者を誘引し、攻撃情報を収集することを目的とする。世界で初めてとされる Ethereum RPC ハニーポット⁽¹²⁾では、トランザクションの送信をはじめとするメソッドで指定された to アドレスや攻撃元 IP アドレスに従って攻撃者をグルーピングし、ETH を

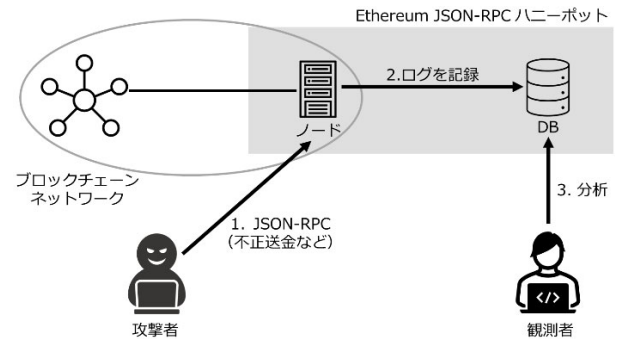


図 10 Ethereum JSON-RPC ハニーポットの概念図

奪取するグループと ERC20 トークンを奪取するグループが存在することを明らかにしている。このとき、ハニーポットが攻撃者にとって攻撃価値のある標的となるように、実際に ETH を保有するウォレットが用意されている。その後更に詳細な分析がなされ、9 か国に Ethereum RPC ハニーポットを設置し、攻撃者が国を基準として攻撃対象を選んでいないことが明らかにされている⁽¹³⁾。Ethereum ではメインネットとテストネットと同じポート番号 (8545/TCP) が利用されているため、ここではテストネットで観測を行った場合でも双方を狙った攻撃が観測される可能性を指摘している。また、攻撃者が攻撃に必要な情報を取得する方法に着目した研究もある⁽¹⁴⁾。ここでは、二つの IP アドレス空間それぞれに対して、メインネットに参加させるノードとメインネットには参加させず RPC ポートを開放したノードの 2 台を設置し、更に実際に ETH を保有させることによって、攻撃者からの不正リクエスト数に変化があることを明らかにしている。また、JSON-RPC に対する攻撃を観測するために Etherpot というハニーポットが構築され、攻撃観測を通じてスマートコントラクトへの攻撃やネットワークを分断する恐れのあるエクリプス攻撃が新たに発見されている⁽¹⁵⁾。このとき、実際の ETH は保有せず、残高情報を取得する `eth_getBalance` メソッドに対してレスポンスを書き換えるアプローチを取っている。一方で、Ethereum JSON-RPC ハニーポットの軽量化手法が提案されている⁽¹⁶⁾。ここでは、ブロックチェーンデータの同期処理をスキップし、Ethereum ネットワークの情報を公開している外部サービスから情報を取得することで、ストレージ使用量が 99% 以上削減されるなど運用コストの低減を可能にしている。また、実際の ETH を保有せずとも高額 ETH を保有する他者のウォレットにひもづける新たなタイプの RPC ハニーポット手法が提案されている⁽¹⁷⁾。ここでは、残高の異なる二つのウォレットに対する攻撃者の振舞いの差異が分析されており、大量のログデータの効率的な分析を可能とするクラスタリングを用いた分析を行い、攻撃者を攻撃目的別に分類できることが明らかにされている。更に、ハニーポット手法のアイデアを応用することで、ユーザのウォレットが暗号資産の盗難攻撃の標的となるリスクを低減する新たな防御手法も提案している。

7.3 コントラクトハニーポット

ハニーポットをブロックチェーン上のスマートコントラクトで仕掛けるのがスマートコントラクトハニーポットである(以降、単にコントラクトハニーポットと呼ぶ)。コントラクトハニーポットは通常のハニーポットと目的が異なり、攻撃情報を収集することではなく、暗号資産を奪取することが目的である。この攻撃をブロックチェーン上で動作させることによってハニーポットの削除が困難となるため、攻撃を阻止することが難しいという攻撃者側のメリットが存在する。図11はコントラクトハニーポットの概念図を示している。脆弱に見せかけたトラップ付きのスマートコントラクトをデプロイする攻撃者Aと脆弱に見えるスマートコントラクトを狙う攻撃者Bの2種類の攻撃者が登場する。攻撃者Aは誰でも悪用が可能なSolidityコードをコントラクトに含ませ、そのコントラクトにトラップドアを隠した状態でコントラクトをデプロイする。もう一方の攻撃者Bがこの悪用できそうなコントラクトに誘い込まれ、暗号資産が騙し取られるという流れである。つまり、コントラクトハニーポットは一見容易に悪用できそうではあるが実際は悪用できないように巧妙に作られているトラップドアをもつものである。多くのコントラクトハニーポットは入金することで結果的により多くの残高を奪取できるように見せかけているため、攻撃者Bはまず暗号資産をコントラクトハニーポットに支払う。しかし、攻撃者Bが支払った暗号資産は二度と戻ることはなく、最終的に攻撃者Aに奪われる形となる。図12はコントラクトハニーポットの具体的な流れをEtherscan上で説明している。攻撃者Aはコントラクトハニーポットを設置し、そのウォレットにユーザをおびき寄せるためにETHを振り込んでおり、その後に攻撃者Bがそのウォレットに合計で1.23 ETHを送金している様子が分かる。

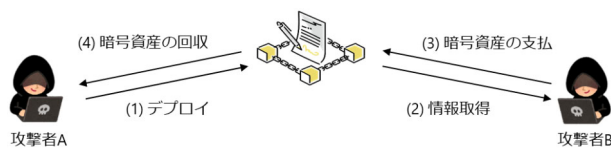


図11 コントラクトハニーポットの概念図

コントラクトハニーポットがEthereumに実在することが2019年に初めて示され、Solidityコードをベースとしてコントラクトハニーポットの検知を行うことが可能なHoney-Badgerと呼ばれるツールが発表されている⁽¹⁸⁾。このとき、目視でスマートコントラクトを確認することで、各コントラクトがコントラクトハニーポットか否かのラベル情報が貼られ、ハニーポットのトラップドア手法が8種類に分類されている。その後、CALLERやBALANCEといった特徴量を用いて、EVMバイトコードを用いてスマートコントラクトハニーポットを検出する方式⁽¹⁹⁾が提案されたり、シンボリック実行による検知時間の遅さのデメリットを解消するためにスマートコントラクトにひもづく取引履歴をはじめとする情報を特徴量として、XGBoostを用いて学習することで検知を行う方式⁽²⁰⁾が提案されたりした。しかしながら、これらの研究はコントラクトの動作後でないと検知できないという課題があった。この課題を解決するために、コントラクトの動作前に検知すべくバイトコードの特徴を用いてコントラクト実行前に検知できる方式が提案されている⁽²¹⁾。一方で、コントラクトハニーポットが中毒性を伴う賭博ゲームなどのコントラクトを装っていることが多いことが議論されている⁽²²⁾。これは通常のハニーポットにはない特徴であり、金銭を奪おうと思っていない一般ユーザにも被害が及ぶ可能性が指摘されている。つまり、一般ユーザもゲームを行う目的でコントラクトハニーポットにアクセスし、課金などで暗号資産が奪われる恐れがある。

7.4 ハードフォークによるNFTのリスク

ブロックチェーンはこれまでの歴史の中で何度か大規模なハードフォークを経験してきた。ハードフォークが生じると本来一つであったブロックチェーンが二つに分岐する。よく知られた事例としては、2016年7月20日にプログラムの脆弱性が原因で巨額の資金が盗まれたThe DAOの問題⁽²³⁾によって、流出前の状態に巻き戻すEthereumとそれを認めないEthereum Classicの二つに分岐がなされた。また、2017年8月1日にスケーラビリティの課題⁽²⁴⁾によって、ブロックサイズの拡張により解決するBitcoin Cashが新たに誕生し、Bitcoinのハードフォークが起こった。最近では、2022年9月15日に行われたEthereumのThe Mergeプロジェクト

図12 コントラクトハニーポットの様子

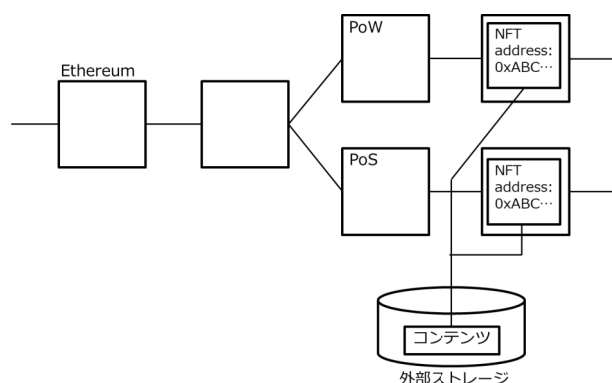


図 13 ハードフォークにより NFT に生じる問題

トにおいて、Ethereum のマイニングプロトコルが PoW から Proof of Stake (PoS) へ移行がなされた。しかし、本プロジェクトではコミュニティに対して十分な周知が行われた上で実行されたにもかかわらず合意形成が完全ではなく、従来の PoW をサポートするチェーンと新しい PoS をサポートするチェーンに分岐することになった。実際に PoW をサポートする Ethereum は、ETHW という ETH とは別の新しいトークンとして運用が行われている。暗号資産取引所においても、ETHW をサポートする取引所は存在しており、ETHW をサポートする取引所においては、保有している ETH と同数の ETHW が AirDrop によって配布された。

これらの事例において重要な教訓は、分岐したどちらのブロックチェーンも運用が継続するという点である。その結果、ハードフォーク以前に登録されたデジタルデータがハードフォーク以降に分岐したそれぞれのブロックチェーンで存在することになる。つまり、結果的に異なるブロックチェーンに同じコンテンツが別々の NFT として登録された状態になる。ハードフォークが生じるとブロックチェーンが二つに分岐するため、NFT の一意性がフォークにより保証されなくなる。図 13 は、ハードフォークによるブロックチェーンのフォーク後、それぞれのブロックチェーンに同一のデジタルデータを参照する NFT が埋め込まれている様子を示している。これによって本来一つであった NFT の所有権がフォーク後の二つのチェーンに分離して、そのまま別々のトークンとなっている。Ethereum の例でいえば、PoW 版 Ethereum と PoS 版 Ethereum の間で所有権が二つに分離し、一意性が保証できなくなっている。今後も利便性の向上や運用負荷の低減を目的としてハードフォークの発生が想定されるため、NFT におけるハードフォークへの対応は早急の課題であると考えられる。

NFT はブロックチェーン上でスマートコントラクトを用いて管理される。各トークン内ではデジタルコンテンツが保存される外部ストレージのリンクなどを保持している。現状の構成では、図 13 のように NFT からコンテンツへの 1 方向の参照となっており、参照元のブロックチェーンが分岐すると、それぞれのブロックチェーンに格納されているどちらの NFT も正規のコンテンツにひもづくため、どちらが正

当なものかを判断できない。そこで、現状の片側参照の構成をコンテンツ側からプラットフォームへの参照を含むことで、相互参照の構成にする方式が提案されている⁽²⁵⁾。これにより、参照元のブロックチェーンが分岐した場合でも、コンテンツ側からプラットフォームを一意に特定できる。もし同じコンテンツを指す NFT が複数存在したとしても、コンテンツ側から参照しているプラットフォームを明らかにし、NFT とプラットフォームが 1 対 1 対応をとることで二重の流通を防ぐことが可能になる。このとき、ネットワークを識別する要素として Bootstrap ノードのドメイン名を用いている。Bootstrap ノードとは、ネットワークに新たなノードが接続する際に中継役の役割を果たすノードであり、ネットワークに接続している一部のピア群の情報を保持している。ハードフォークが発生した状況では、二つのチェーンで Bootstrap ノードのもつピアリストは異なっていくため、Bootstrap ノードの応答を用いてネットワークを一意に識別可能であると考えられる。

7.5 Tornado Cash のセキュリティリスク

暗号資産の匿名性を高める手法としてミキシングサービスがある。ミキシングサービスを用いることで暗号資産の以前の保有者と現在の保有者のリンクが失われるため、ミックスされた暗号資産の以前の保有者が誰なのかが分からなくなる⁽²⁶⁾。こうしたミキシングサービスの中で、Ethereum 上で利用可能なものとして Tornado Cash がある。Tornado Cash は、ゼロ知識証明に基づいて構築された Ethereum ブロックチェーンベースの暗号資産ミキシングサービスである。暗号資産のミキシングは、複数のアカウントによる取引データをミックスさせ、個別の取引内容やアドレスが特定できないようにするプライバシー保護を主たる目的としている。その中でも、Tornado Cash は入金したユーザと出金したユーザのアドレスのつながりを断ち切る。これにより、暗号資産及びアドレスの保有者が誰であることを秘匿化することができる。また、Tornado Cash は、ミキシングに管理者が存在しないスマートコントラクトを用いることで、ミキシングサービス運営者による情報漏洩やハッキングによる盗難、運営者による持ち逃げの可能性を最小限にしている。一方で、犯罪に関わった暗号資産の資金洗浄のために大量の暗号資産が Tornado Cash に流れ込んでいることが報告されている。更に、2022 年 8 月に米国の財務省外国資産管理室 (Office of Foreign Assets Control; OFAC) は、北朝鮮のハッカーグループが不正資金を Tornado Cash に送り資金洗浄したことを指摘し、Tornado Cash を資金洗浄のプラットフォームとみなしてブラックリストに載せた。

Tornado Cash では、まず複数のユーザが一定金額を Tornado Cash のスマートコントラクトのアカウントに対して入金する。その後ユーザらはゼロ知識証明を用いることで、スマートコントラクトからユーザの別のアカウントに出金することができる。これにより、入金アカウントと出金アカウン

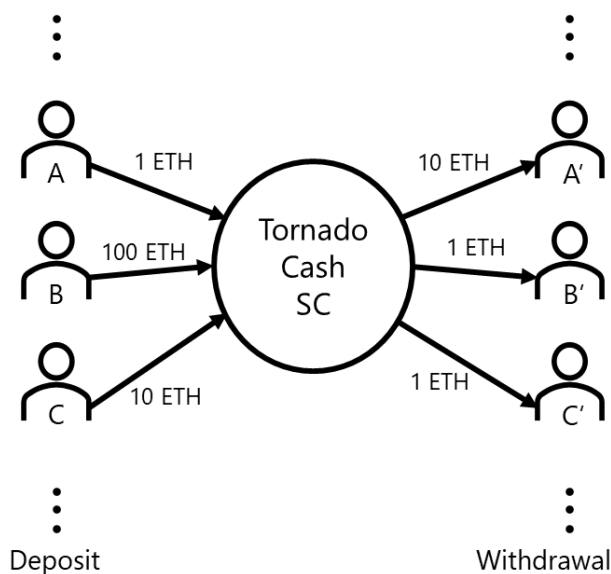


図 14 Tornado Cash スマートコントラクトによる入出金の例

トのリンクが失われる。ここで出金アカウントの保有者は必ず入金アカウントの保有者群に存在することから、数多くのユーザが入金すればするほど安全性が向上する。図 14 は Tornado Cash スマートコントラクトによる入出金の例を示している。

Etherscan の中の特徴的な情報として Public Name Tag と Label がある。図 15 は、Etherscan における Public Name Tag と Label を示している。Public Name Tag は、アドレスの所有者、若しくは目的を示しており、アドレスに関連するお知らせや警告が追加されることもある。Etherscan のキュレータ^(注12)によって公益性があると判断された場合にのみ Public Name Tag の追加が行われる。例えば、「Phishing」という Public Name Tag は、フィッシング詐欺で他人から暗号資産などを奪い取ったアドレスであることを示している。Label とは、アドレス、トークン、トランザクション、ブロックページなどの情報が属しているカテゴリーのことを指す。Label を見ることで、アドレスがどのようなカテゴリーに属しているのか容易に調べることができる。代表的な Label として、フィッシング詐欺やハッキング関連の「Phish/Hack」やスマートコントラクトの脆弱性を狙ったエクスプロイト攻撃関連の「Exploit」などが挙げられる。

Tornado Cash の入金アドレスのクラスタリング及び分析を行うことによって、潜在的な犯罪アドレスをリストアップし、Tornado Cash における資金洗浄の実態を明らかにしている研究がある⁽²⁷⁾。具体的には、Tornado Cash の入金アドレスに対して Etherscan の Name Tag にある「Phish/Hack」、「Exploit」などのカテゴリーを用いて犯罪アドレスを抽出し、それらが占める入金額の割合を算出及び分析し、資金洗浄のプラットフォームとしての Tornado Cash の実態を

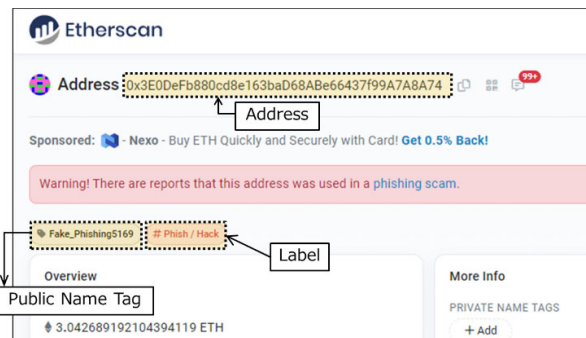


図 15 Etherscan の Public Name Tag と Label

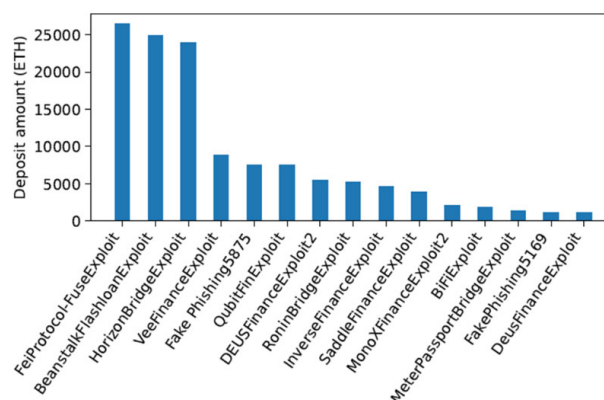


図 16 TC に入金された被害額を事件別の被害額

明らかにしている。図 16 は、Tornado Cash に入金された被害額を事件別に分析したものであり、被害額が最も大きい三つの事件がほかの事件より突出して大きいことが分かる。これら三つの事件の Name Tag は全て「Exploiter」であることから、スマートコントラクトなどの脆弱性を悪用した犯罪の被害額が大きいことが推測される。

8. セキュアブロックチェーンシステム

本章では、ブロックチェーンを適用したセキュアブロックチェーンシステムの研究について、二つのユースケースを紹介する。

8.1 マイナンバーカードを用いた自動確定日付システム

近年、公証制度のオンライン化が世界各地で進んでいる。例えば、アメリカにおいては公証人とオンラインで接続し、デジタルな環境で公証を受けることができる Notarize という事業が注目を集めている。電子政府で有名なエストニアにおいては、公証人が e-Notary というシステムを使うことで、オンライン上で公証することができるような制度が存在する。しかし、日本における公証制度のオンライン化は進んでいないといわざるをえない。電子公証制度といわれる制度

(注 12) : Etherscan の Public Name Tag や Label の管理者。

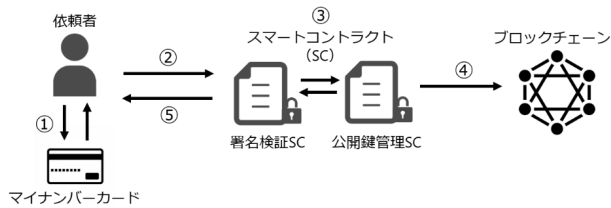


図 17 確定日付システム⁽²⁸⁾のおおまかな流れ

は存在し、確定日付の申請におけるオンライン化は進んでいるが、電子書類であっても、最終的に手数料の納付や電子署名を受けたファイルを受け取りに直接公証人がいる公証役場に赴く必要がある。一方で、近年の ICT 技術の発展に伴い、法務省が関連法改正を視野に入れつつ、公正証書のデジタル化に乗り出すなど改善に積極的な姿勢が見られる。

地方公共団体情報システム機構から発行されるマイナンバーカードによる本人性の確認とスマートコントラクトの第三者を介さないプログラムとしての契約を自動履行する仕組みを用いることで、公証人を必要としない自動化された確定日付のシステムが提案されている⁽²⁸⁾。具体的には、マイナンバーカードを用いて署名された電子書類に対してスマートコントラクト内で検証を行うことで、依頼者と電子書類自体の認証を自動的に行う。検証結果が正しい場合、その情報はブロックチェーンに格納されるが、その際ブロックチェーンプラットフォームが発行するトランザクションレシートを確定日付の証明書として利用することで、信頼性の高いシステムを構成できる。従来、日本においては法務大臣に指定された指定公証人が行っていた業務の一部をスマートコントラクトとしてブロックチェーン上で実行することで、書類作成から依頼者が入手するまでの時間を大幅に削減することが期待される。

図 17 は確定日付システム⁽²⁸⁾のおおまかな流れを示している。本システムの具体的な流れは下記のとおりである。

- ① 依頼者は、マイナンバーカードを用いて文書に対するデジタル署名を生成する。
- ② 依頼者は、文書のハッシュ値とそのデジタル署名及び公開鍵を署名検証スマートコントラクトに送信する。
- ③ 署名検証スマートコントラクトは、公開鍵管理スマートコントラクトと連携して事前に登録されている公開鍵を使ってデジタル署名を自動検証する。
- ④ 署名検証スマートコントラクトは、トランザクションレシートを発行してその中に文書のハッシュ値を埋め込み、ブロックチェーンに記録する。
- ⑤ 依頼者は、トランザクションレシートを証明書として利用する。

8.2 コンタクトトレースシステム

スマートフォンやウェアラブル端末の活用事例の一つとし

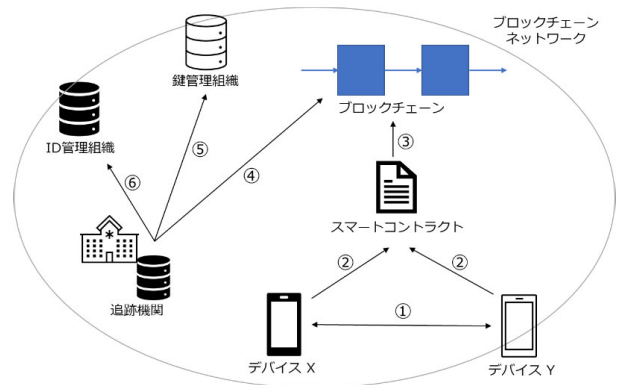


図 18 コンタクトトレーシングシステム⁽³⁰⁾のおおまかな流れ

てコンタクトトレーシングが存在する。コンタクトトレーシングとは、スマートフォンのアプリケーションなどを用いて、デバイス所有者と接触した人や所有者が訪れた場所を追跡する技術であり、主に COVID-19 などの感染症対策で利用されている。また、コンタクトトレーシングは人の動きを追跡できることから、警察の捜査の補助や目撃証言の補強など犯罪対策への活用が可能であると考えられ、実際シンガポールではコンタクトトレーシング用のアプリケーションを犯罪捜査に利用可能としている。一方で、コンタクトトレーシングでは、接触者の情報や位置情報などの個人情報を集めるため、プライバシーの問題があり、特に中央集権的な仕組みの場合、どのようなデータが収集され、収集されたデータが正しく使われているのかなどの懸念が存在する。このような背景から分散管理可能なブロックチェーンを組み合わせ、耐改ざん性をもち、プライバシーの保護及びデータの透明性を確保したコンタクトトレーシングの研究が行われている。

コンタクトトレースシステムにおいて、ユーザが記録する情報の正当性をほかのユーザに保証してもらう方式が提案されている⁽²⁹⁾。この方式では、ユーザは周囲のほかのユーザにチャレンジとして公開鍵をブロードキャストし、レスポンスとして位置情報などを受け取ることで、ほかのユーザの保証を得る仕組みである。しかし、この方式ではデータを記録するごとに異なる公開鍵を必要とするため、ユーザが多くの鍵を管理する必要があった。そこで、ブロックチェーンを用いて暗号鍵を管理することで鍵管理コストを削減する方式が提案されている⁽³⁰⁾。これは、ユーザによるデータの偽造及びプライバシーを考慮したコンソーシアム型ブロックチェーンを用いたコンタクトトレーシング手法であり、チャレンジレスポンス認証とスマートコントラクトによる検証を組み合わせることで、ユーザによるデータの偽造を検知可能にし、位置情報を暗号化することでプライバシーを保護している。この手法を用いることによって、通常時はユーザのプライバシーを保護し、必要に応じてユーザの同意を得ることで、詳細な行動履歴の追跡ができる柔軟なコンタクトトレーシングを実現している。

図 18 はコンタクトトレースシステム⁽³⁰⁾のおおまかな流れを示している。本システムにおける接触履歴の記録と追跡について、具体的な流れは下記のとおりである。

- ① 複数のデバイスが相互にチャレンジレスポンス認証を行う。
- ② 各デバイスは、スマートコントラクトに対して接触履歴を含むトランザクションを送信する。
- ③ スマートコントラクトは接触履歴を検証し、問題がなければブロックチェーンに記録する。
- ④ 追跡機関は、追跡したいユーザのアドレスを特定する。
- ⑤ 追跡機関は、追跡したいアドレスを用いて鍵管理組織に ID を問い合わせる。
- ⑥ 追跡機関は、取得した ID を用いて ID 管理組織にユーザ情報を問い合わせる。

9. おわりに

本稿では、ブロックチェーンにおけるセキュリティ面を中心に、ブロックチェーンのセキュリティリスク、及びブロックチェーンを応用したセキュアシステムに関する最新的话题を取り上げ、それらの研究動向について概観した。暗号資産・ブロックチェーンへの様々なセキュリティリスクが存在するなか、医療、IoT、サプライチェーンなどの分野において、ブロックチェーンベースのセキュアシステムが数多く提案されている。このようなセキュリティリスクを正確に把握し、よりセキュアなブロックチェーンベースのシステムを構築していくことが今後期待される。

文 献

- (1) 面和成, 池田虎三, 河野英子, 三村直樹, 永井博昭, 柏原直明, “内閣府エビデンスシステム (e-CSTI) を活用したブロックチェーン分野の論文・特許の分析,” コンピュータセキュリティ研究会, pp. 1-8, March 2024.
- (2) S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” <https://bitcoin.org/bitcoin.pdf> 2009.
- (3) V. Buterin, “Ethereum White Paper: A next generation smart contract and decentralized application platform,” https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf 2013.
- (4) N. Szabo, “Smart contracts: Building blocks for digital free markets,” *Extropy: The Journal of Transhuman Thought*, vol. 16, 1996.
- (5) K. Omote, Y. Tsuzuki, K. Ito, R. Kishibuchi, C. Yan, and S. Yada, “Analysis and risk consideration of worldwide cyber incidents related to cryptoassets,” *HIS 2022, LNNS*, vol. 647, pp. 1093-1101, 2022.
- (6) 佐藤哲平, 今村光良, 面和成, “コインチェック事件における流出 NEM の追跡に関する実態調査,” 情報セキュリティ研究会, *ISEC2018-7*, pp. 35-41, May 2018.
- (7) チェックポイントソフトウェアテクノロジーズ(株), “Uniswap (ユニスワップ)へのフィッシング攻撃で 800 万ドル相当の被害,” <https://prtimes.jp/main/html/rd/p/000000127.000021207.html> Aug. 2022 (2024.4.1 accessed).
- (8) H. Denley, “UNI LP scam,” <https://dune.com/409h/uni-lp-scam-0xcf39b7793512f03f2893c16459fd72e65d2ed00c>. July 2022 (2024.3.2 accessed).
- (9) R. Matzutt, J. Hiller, M. Henze, J.H. Ziegeldorf, D. Mullmann, O. Hohlfeld, and K. Wehrle, “A quantitative analysis of the impact of arbitrary blockchain content on bitcoin,” *FC 2018, LNCS*, vol. 10957, pp. 420-438, 2018.
- (10) T. Sato, M. Imamura, and K. Omote, “Threat analysis of poisoning attack against Ethereum blockchain,” *WISTP 2019, LNCS*, vol. 12024, pp. 139-154, 2019.
- (11) X. Wang, X. Zha, G. Yu, W. Ni, R.P. Liu, Y.J. Guo, X. Niu, and K. Zheng, “Attack and defense of ethereum remote APIs,” *IEEE Globecom Workshops*, pp. 1-6, 2018.
- (12) Z. Cheng, X. Hou, R. Li, Y. Zhou, X. Luo, J. Li, and K. Ren, “Towards a first step to understand the cryptocurrency stealing attack on Ethereum, RAID,” pp. 47-60, 2019.
- (13) K. Hara, T. Sato, M. Imamura, and K. Omote, “Profiling of malicious users targeting Ethereum’s RPC port using simple Honeypots,” *IEEE Blockchain 2020*, pp. 1-8, 2020.
- (14) K. Chin and K. Omote, “Analysis of attack activities for Honeypots installation in Ethereum network,” *IEEE Blockchain 2021*, pp. 440-447, 2021.
- (15) J. Wang, T. Sasaki, K. Omote, K. Yoshioka, and T. Matsumoto, “Multifaceted analysis of malicious Ethereum accounts and corresponding activities,” *CSP 2022*, pp. 71-79, 2022.
- (16) 内田大暉, 内堀紘徳, 面和成, “Ethereum RPC ハニーポットの軽量化手法,” 情報処理学会論文誌, vol. 64, no. 9, pp. 1255-1265, Sept. 2023.
- (17) H. Uchibori, K. Yoshioka, and K. Omote, “Honeypot method to lure attackers without holding crypto-assets,” *IEEE Access*, vol. 12, pp. 16059-16071, Feb. 2024.
- (18) C.F. Torres and S. Mathis, “The art of the scam: Demystifying Honeypots in Ethereum smart contracts,” *USENIX Security Symposium 19*, pp. 1591-1607, 2019.
- (19) W. Chen, X. Guo, Z. Chen, Z. Zheng, Y. Lu, and Y. Li, “Honeypot contract risk warning on Ethereum smart contracts,” *IEEE JCC 2020*, pp. 1-8, 2020.
- (20) R. Camino, C.F. Torres, M. Baden, and R. State, “A data science approach for detecting Honeypots in Ethereum,” *IEEE ICBC 2020*, pp. 1-9, 2020.
- (21) K. Hara, T. Takahashi, M. Ishimaki, and K. Omote, “Machine-learning approach using solidity bytecode for smart-contract Honeypot detection in the Ethereum,” *QRS-C 2021*, pp. 652-659, 2021.
- (22) M. Ishimaki and K. Omote, “Ethereum contract Honeypot risk analysis,” *FCS 2022, CCIS*, vol. 1726, pp. 226-240, 2022.
- (23) M. Campbell-Verduyn, “Bitcoin and beyond: Cryptocurrencies, blockchains and global governance,” Taylor & Francis, 2017.
- (24) A. Chauhan, O.P. Malviya, M. Verma, and T.S. Mor, “Blockchain and scalability,” *QRS-C 2018*, pp. 122-128, 2018.
- (25) K. Kimura, M. Imamura, and K. Omote, “Cross-referencing scheme to ensure NFT and platform linkage unaffected by forking,” *IEEE ICBC 2023*, pp. 1-4, 2023.
- (26) L. Wu, Y. Hu, Y. Zhou, H. Wang, X. Luo, Z. Wang, F. Zhang, and K. Ren, “Towards understanding and demystifying Bitcoin mixing services,” *Web Conference 2021*, pp. 33-44, 2021.
- (27) M. Youn, K. Chin, and K. Omote, “Empirical analysis of cryptocurrency mixer: Tornado cash,” *SAM 2023*, 2023.
- (28) S. Haga and K. Omote, “Blockchain-based autonomous notarization system using national eID card,” *IEEE Access*, vol. 10, pp. 87477-87489, Aug. 2022.
- (29) W. Lv, S. Wu, C. Jiang, Y. Cui, X. Qiu, and Y. Zhang, “Towards large-scale and privacy-preserving contact tracing in COVID-19 pandemic: A Blockchain perspective,” *IEEE Trans. Net. Sci. Eng.*, vol. 9, no. 1, pp. 282-298, Jan.-Feb. 2022.
- (30) K. Omote and T. Fukuda, “A secure contact tracing method using smart contracts with considering privacy,” *ICBC 2023, LNCS*, vol. 14206, pp. 1-15, 2023.

(ISEC 研究会提案, 2024 年 3 月 4 日受付,

2024 年 4 月 5 日再受付)



面 和成 (正員)

2002 北陸先端科学技術大学院博士後期課程修了。同年(株)富士通研究所入社。北陸先端科学技術大学院大学准教授、筑波大学准教授を経て、2022 より同大学教授。ブロックチェーンセキュリティに関する研究に従事。国際会議 WISTP2019 最優秀論文賞受賞。著書に『入門 サイバーセキュリティ 理論と実験～暗号技術・ネットワークセキュリティ・ブロックチェーンから Python 実験まで～』など。

ESS ニュース

NOLTA, IEICE 特集号

Guest Secretary 山仲芳和

特集タイトル：

Special Section on Recent Advances in Nonlinear Problems

掲載誌：

NOLTA IEICE, 2024 年 7 月 1 日発行

非線形問題は、工学、科学、数学を含む極めて幅広い分野に存在しています。電子情報通信学会 NOLTA ソサイエティでは、非線形現象の基礎理論から応用に関する成果発表の場となる非線形問題研究会を開催しており、毎年、数多くの研究成果が発表され、活発に議論されています。本特集は、非線形問題に関する最新の研究成果や、2023 年から 2024 年に非線形問題研究会で発表された中で特に強く推薦された研究成果を、国際英文論文誌として発信することを目的に、非線形問題研究専門委員会が企画したものです。投稿された論文は NOLTA, IEICE の通常の査読プロセスに従って審査され、4 件の論文が掲載されることになりました。掲載論文は J-STAGE (<https://www.jstage.jst.go.jp/browse/nolta/>) にて全て無料でアクセスいただけます。非常に興味深い論文ばかりですので、ぜひご覧ください。

最後に、貴重な研究成果をご投稿頂いた著者の皆様、ご多忙にもかかわらず迅速に査読頂いた査読者の皆様、本特集号にご尽力頂いた Guest Associate Editors の皆様、及び NOLTA 編集委員の皆様に深く感謝申し上げます。



山仲芳和 (正員)

2012 長岡技術科学大学・工・電気卒。2017 同大学院博士課程修了、博士（工学）。同年宇都宮大学工学部・助教、現在に至る。非線形力学を応用した最適化アルゴリズムとその応用に関する研究に従事。IEEE 会員。

研究会に行こう！

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

■信頼性研究会（R）

長かったコロナもようやく終息して、今年こそ臨場感を求めて研究会やシンポジウムへの現地参加を考えていらっしゃる学会員の皆様も多いと存じます。信頼性研究会は全国各地（東京地区：2回、関西地区、中京地区、九州地区、北海道東北地区、中国四国地区：各一回）で7回の単独開催と、毎年場所が異なる合同研究会を1回開催しており、最も活発に研究会活動を実施している研究会の一つであると自負しております。元来信頼性工学は、部品・デバイスの信頼性に関して故障の反応速度を物理的に制御する信頼性物理的アプローチ、システムの信頼性向上のために最適冗長設計や最適保全頻度などを数理的に導出する信頼性統計・数理的アプローチ、更にはFMEA（故障の影響度解析）やFTA（故障要因を深掘する故障木解析）などを活用して故障やリスクを低減させるリスクアセスメント的アプローチがあります。昨今複合化されたシステムや電子機器の信頼性保証のためには、常にこれら三つのアプローチを活用・考察して、同時に信頼性を最適化することが求められており、今後この傾向は更に強まり、3分野の融合が進むと予想いたしております。信頼性研究会では、自らの専門分野や領域とは異分野の報告も多いですが、それらから思わぬ気づきや発想を得られることも多く、このボーダレスさが本研究会の醍醐味であります。

現在、学会員の皆様が取り組んでいらっしゃる研究や開発活動には、その信頼性が重要であるテーマも多いと考えております。それらの方々は信頼性研究会に初参加されたときから討議の輪の中に入れると考えておりますので、是非一度本研究会をのぞいてみませんか？最後に今年度信頼性研究会は以下のように計画されておりますので、皆様がご自身のご都合に合わせて積極的にご参加されることを幹事一同心よりお待ちしております。

2024年

- 5月18日 愛知大学 名古屋
- 6月13日 機械振興会館 東京
- 7月27日 室蘭工業大学 北海道
- 8月29日、30日 弘前大学 青森〈合同研究会〉
- 10月11日 市民会館シアーズホーム（熊本市民会館） 熊本
- 11月30日 豊岡市民交流プラザ 兵庫
- 12月5日 機械振興会館 東京

2025年

- 3月 日時未定 中国・四国地区



門田 靖（正員）

1981年3月株式会社リコーに入社、以来各種社内開発電子デバイス及び電子写真の信頼性業務に従事。現在同社先端技術研究所IMD研究センターにおいて、新規電子材料の信頼性について研究。1989より一般財団法人日本科学技術連盟信頼性講師。以後、大阪大学非常勤講師、学振167委員会「ナノプローブ研究会」副委員長、日本信頼性学会会

長などを歴任。現在、電子情報通信学会信頼性専門委員長、電気学会会員、日本信頼性学会会員、博士（工学）。

■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は発足し、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。2024年度は常設研究専門委員会として10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。

2023年度には総合大会において「ニューロモルフィック・リザーバーコンピューティングの現状と未来」というテーマのセッションを企画し、素晴らしい講演者の皆様による貴重な御講演を頂くことができました。また、韓国 Korea Multi Media

Society (KMMS) との日韓合同ワークショップを大分県別府温泉にて開催し、盛況のうちに終えることができました。この場を借りて御礼を申し上げます。

また、CCS 研究会では、学生の皆さんや若手研究者を積極的に奨励する取り組みにも力を入れています。毎年発表された口頭発表論文の中から優秀な研究発表を行った若手研究者を選出し、「複雑コミュニケーションサイエンス研究会奨励賞」として表彰しています。これまでの受賞者のなかには現在活躍している研究者も多く、本研究会の発表の場が重要な役割を果たしていることがうかがえます。

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、2023 年度は全て対面で開催をし、CCS 研究会が更に活気づいてまいりました。2024 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。

【2024 年度 CCS 研活動計画】

●第一種研究会

2024 年 6 月 6, 7 日	CCS/NLP 共催研究会 @ 西日本総合展示場 AIM
2024 年 7 月 29 日 30 日	CCS/IN 併催研究会 @ 北海道 モエレ沼公園
2024 年 11 月 (中旬予定)	CCS 研究会 @ 京都
2025 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

2024 年 6 月 8 日	NOLTA ソサイエティ大会@西日本総合展示場 AIM
2024 年 12 月 3 日～ 6 日	NOLTA2024@ベトナム
2025 年 1 月	JKCCS (予定)

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



佐々木智志 (正員)

2009 武蔵工大 (現東京都市大)・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、准教授を経て、2023 湘南工科大学情報学部情報学科准教授、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。

■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関わる多様な研究の振興を目的としています。暗号・情報セキュリティは、安心安全なデジタル化社会に欠かせない技術であり、多様化する脅威から社会を守るためには、様々な研究者・技術者らの知見を結集する必要があります。そのため、ISEC は研究者・技術者らが所属組織を超えて多様な研究テーマに関して活発に議論でき、自由に交流できる機会を設けています。特に研究発表の場として、第一種研究会、第二種研究会、国内シンポジウム、国際会議を主催・共催しています。

ISEC では、第一種研究会を毎年 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大学院学生を中心とする若手研究者による招待講演を企画しています。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、世界トップクラス国際会議に採録された論文の著者による招待講演を企画し、世界最先端研究を披露して頂いています。また、国内シンポジウムとして、「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。今日までに、SCIS は参加者 900 人以上、発表件数 300 件以上の規模を誇る、暗号・情報セキュリティ分野における国内最大の研究集会に発展し、多くの様々な研究者・技術者らと自由に交流できる貴重な機会です。更に、情報セキュリティ関連分野を広く対象にして、情報処理学会コンピュータセキュリティ研究会 (CSEC) と共催で国際会議 IWSEC (International Workshop on Security) を毎年日本で開催しており、今年は 9 月に京都で開催します。

上記のように ISEC では様々なイベントや交流の場を作っていますので、詳細は ISEC Web サイト (<https://www.ieice.org/ess/isec/index.html>) をご覧ください。皆様の参加をお待ちしています。特に我が国の将来を担う若手の研究者・技術者の積極的な参加を期待しています。



四方 順司 (正員)

平 6 京大・理卒, 平 9 同大学院修士課程了, 平 12 阪大大学院博士課程了, 博士(理学). 同年東大研究員, 平 14 横浜国大勤務, 平 28 同大・教授. 現在, 横浜国大副学長. 暗号理論, 情報理論などの研究に従事. 英国計算機学会 Wilkes 賞(2006), 平 22 文部科学大臣表彰(若手科学者賞)等受賞.

■情報理論研究会 (IT)

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

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

2024 年度の IT 研究会の日程は次のとおりです.

- ・ 2024 年 5 月 30 日・31 日 千葉大学マルチメディア情報ハイディング・エンリッチメント (EMM) 研究会と共催
- ・ 2024 年 8 月 6 日・7 日 岡山大学フレッシュマンセッション
- ・ 2025 年 1 月 29 日・30 日 山口県下関市信号処理 (SIP) 研究会, 無線通信システム (RCS) 研究会と共催
- ・ 2025 年 3 月未定 例年, 情報セキュリティ (ISEC) 研究会, 高信頼制御通信 (RCC) 研究会, ワイドバンドシステム (WBS) 研究会と共催で開催

IT 研究会は, 情報理論とその応用サブソサイエティ (SITA サブソ) 傘下にある唯一の研究会であり, SITA サブソから IT 研究会で優秀な研究発表を行った学生に対して「学生優秀発表賞」を授与しております. ぜひこの賞の受賞を目標の一つにして頂き, 学生さんからの研究成果のご発表をお待ちしています.

IT 研究会では, 大学院生を中心に学部生や高専生, 若手研究者からベテランの先生まで幅広い方が研究発表をしています. そして, コロナ禍もようやく落ち着いてきて, 対面での開催も増えてきました. やはりオンライン形式と比べると, 質疑応答が活発に繰り広げられますし, その熱量も大きいように感じます. 研究会の後に懇親会が企画されることも増え, 企業の研究者や大学の先生と学生さん達が研究・開発に携わる者としての悩みやキャリア形成などを話題に盛り上がることもあります. ぜひ IT 研究会にご発表・ご参加頂き, その醍醐味や熱量を肌で感じて頂けたらと思います.



野上 保之 (正員: シニア会員)

1994 年 3 月信州大学・工学部・電気電子工学科卒, 1996 年 3 月同大大学院・修士課程 (電気電子工学専攻) 修了, 1999 年 3 月同大大学院・博士課程 (システム開発工学) 修了, 博士 (工学) 取得. 1999 年 4 月岡山大学工学部助手, 2010 年 4 月同大自然科学研究科准教授, 2017 年同大自然科学研究科教授, 2023 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, 現在に至る. その間, 電子情報通信学会基礎・境界ソサイエティの会計幹事・庶務幹事, 情報理論研究専門委員会・情報セキュリティ研究専門委員会・ハードウェアセキュリティ研究専門委員会の委員を歴任.

■信号処理研究会 (SIP)

信号処理研究会は基礎理論から応用まで幅広い分野をカバーします. 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活動しています.

2024 年度は以下の 5 回の研究会を開催予定です. 8 月は各グループの若手研究者による招待講演があります. 最新情報は信学会及び SIP 研専のホームページでご確認ください.

2024 年 6 月 6 日 (木)~7 日 (金) 新潟大学駅南キャンパスときめいと (IE, MI, BioX, ITE-ME, ITE-IST 共催)

2024年7月18日(木)～19日(金) 弘前大学 (CAS, VLD, MSS 共催)
2024年8月26日(月)～27日(火) 福井大学 (SIP 単独開催)
2025年1月29日(水)～30日(木) 海峡メッセ下関 (IT, RCS 共催)
2025年2～3月頃 (開催日・場所未定) SPEASIP (SP, EA 共催, IPSJ-SLP 連催)

また、2024年9月に開催されるソサイエティ大会では、3日めの12日(木)午前の企画セッション「信号処理における深層学習の新展開」にて2件の招待講演を予定しています。更に、2025年3月に開催される総合大会では、画像符号化関連の企画セッションを検討中です。

これらに加えて、2024年12月16日(月)～18日(水)に第39回信号処理シンポジウムを北海道大学にて開催予定です。毎年100件程度の講演のほか、招待講演や企画セッションなどで盛り上がります。皆様のご参加をお待ちしております。



市毛 弘一 (正員)

1994 筑波大・第3・情報卒。1999 同大学院博士課程工学研究科修了、博士(工学)。同年横浜国大・工・電子情報助手。現在、同大学院工学研究院教授。2001～2002 スイス連邦工科大ローザンヌ校客員研究員。2024年度SIP研専委員長。アレー信号処理、センシングなどの研究に従事。IEEE会員。趣味フルマラソン、46回走って全て完走。PB2時間58分(2016つくばマラソン)。

■高信頼制御通信研究会 (RCC)

高信頼制御通信研究会(RCC)は、システム(機械、デバイスなど)の制御のための通信、また通信システムの特徴(通信遅延や誤りなど)を考慮した制御、更には通信と制御とを融合したシステムを設計することで、高効率かつ高信頼な制御システムを構築することを目的とした研究会です。応用面においては、交通システム、エネルギーシステムはもとより、医療、ヘルスケア、金融、防災、建造物、製造、ロボットなど、これまで信頼性の観点から通信が十分に浸透しているとはいえない分野への有線通信の適用を可能にし、これまでになかったようなシステムやサービスを実現するための基幹技術を議論しています。

研究会の開催件数は年4回程度となっており、制御や通信の専門家の方々と幅広い議論ができます。また、学生や若手研究者に対して研究奨励賞なども用意しています。詳細は、以下の高信頼制御通信研究会のページを参照ください。

<https://www.ieice.org/ess/rcc/index.php>



図1 片山先生の特別招待講演の様子(2024.3.14)



図2 奨励賞授与の様子



石井 光治 (正員)

2005 横浜国立大学大学院博士課程了。同年香川大学工学部助手、2023 香川大学創造工学部教授。2012.4～2013.3 シドニー大学客員研究員。誤り訂正符号や通信理論などに関する研究に従事。2017 本会通信ソサイエティ論文賞受賞。

日本工業大学だより

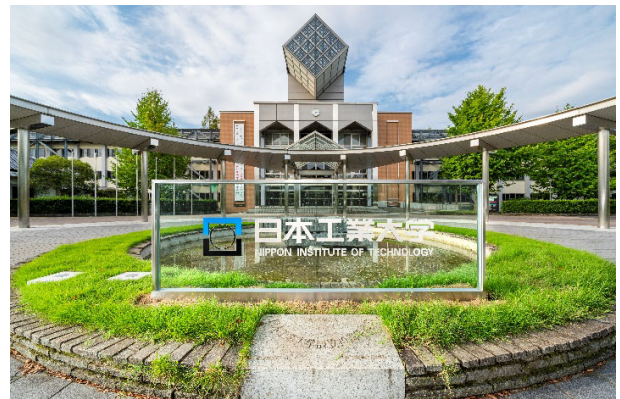
平栗健史（日本工業大学）

1. 学校法人日本工業大学

学校法人日本工業大学は、法人本部と専門職大学院が神田キャンパス（東京都千代田区）に設置されており、専門職大学院は、日本唯一の中堅・中小企業向け技術経営人材の育成プログラムを実践し、社会人の技術経営修士（MOT）を取得できます。また、駒場キャンパス（東京都目黒区）には開校 115 年の歴史をもつ駒場中学校・駒場高等学校の各大学付属校があり、埼玉キャンパス（埼玉県南埼玉郡宮代町）には大学と大学院が設置されています。2024 年度電子情報通信学会ソサイエティ大会は、埼玉キャンパスの大学で開催されます。

2. 実工学教育の学び

本学では建学の精神に基づき「実工学教育」を掲げており、その意味は「工学における実学を重んじ、具象を離れることなく、抽象を怠ることなく、単に机上にとどまることなく、真に有用な教育研究を推進し社会に貢献する」となります。実工学とは、言うまでもなく工学における実学尊重を意味するものであり、実際の社会に存在し、人々のために機能する形において意味をなします。すなわち、教育も研究も、常にそのことを前提として行われなければならないといった方針を実践しています。このような方針を実践するために、基幹工学部、先端工学部、建築学部 の 3 学部と連携した 4 専攻の大学院が設置されています。



日本工業大学 正門玄関

3. 埼玉キャンパスの特色（環境活動・LC センター・工業技術博物館）

埼玉キャンパスは、東京ドーム約 6 個分という広大な敷地にて、約 4000 名の全ての学生が 4 年間同じ場所で学んでいます。環境活動は、2001 年の ISO 14001 認証取得以降、環境保全と SDGs 達成に向けたサステナブルキャンパスの構築を目指し全学で推進しています。脱炭素社会に向けた取り組みである再生可能エネルギー導入などにおいては、大規模の太陽光発電（310 kW）設備を 2000 年に導入しました。更に、順次設備増強を行い、総発電能力を 580 kW とした結果、キャンパス電力使用量の約 8% を賄うまでになりました。また、建物内のエネルギー利用状況が見える化し、機器や設備を最適にコントロールするための仕組み（BEMS）の導入をはじめ、省エネ化や資源活用を目的とした環境施設の充実を特長とした「エコキャンパス」へと発展しました。学生組織である学生環境推進委員会による地域連携活動は、キャンパス内に留まることなく活動の幅を広げています。

その結果、環境活動の外部評価として、CCC（Campus Climate Challenge）実行委員会主催の 2010 年全国第 2 回エコ大学ランキングで「私立大学部門第 1 位」、同 2012 年第 4 回で「全国総合順位第 1 位」などを受賞しました（のちに「5 つ星エコ大学」受賞）。2018 年よりこれまでの環境活動を継承・発展させて、本学独自の環境マネジメントシステム（NIT-EMS）を立ち上げ、学生を中心とした SDGs 活動を支援する体制を整えています。

LC センター（Library and Communication Center）は、図書・情報複合施設として学園創立 100 周年を記念して建設されました。豊富な図書や文献を備えた学術研究施設としての機能のほか、インターネット、AV システムなどの情報機器を多数備え、各種情報の閲覧や検索などに活用されています。桜が満開する春の景観は、近隣の東武動物公園の観覧車と桜と LC センターのコラボが見られます。来学の際には本学のランドマークとして見学ください。

工業技術博物館は、1987 年に学園創立 80 周年記念事業の一つとしてキャンパス内に開設しました。この博物館では、明治時代からの日本の産業技術の発展を辿ることができます。特筆すべき点は、歴史的な工作機械の多くを「動態保存」してい



学園創立 100 周年記念で建設された LC センター



桜と観覧車と LC センター

ることです。単体の工作機械だけでなく、かつての町工場も復元し動態保存しています。また、国鉄で長年活躍した 1891 年（明治 24 年）英国製の蒸気機関車も動態保存しており、イベント開催時にはキャンパス内に敷設した軌道上で有火運転することで、メディアに多数取り上げられることや、鉄道ファンのみならず多くの皆様楽しんで頂いています。

4. 埼玉キャンパスの周辺情報と交通案内

埼玉キャンパスは埼玉県宮代町にあり、関東平野の中央部に位置します。都心へ通勤するベッドタウンとして東武鉄道が町を縦断しています。東京への入り口であると同時に北関東の入り口であるともいえる立地であり、都市と田園の両方の側面をもったエリアです。町域を画するように北から東そして南へと、かつて利根川の本流であった古利根川が流れています。町内には特産品の「梨とぶどうの直売所」が約 20 か所存在します。代表的な観光スポットである「東武動物公園」は、約 120 種類 1200 頭の動物たちがいる動物園と 30 種類のアトラクションが楽しめる遊園地、波のプールや親子スライダーなどが楽しめる広いプールが融合したハイブリッドレジャーランドです。

埼玉キャンパスへのアクセスには二つの最寄り駅があります。東武スカイツリーライン（東武伊勢崎線）沿線の東武動物公園



工業技術博物館の蒸気機関車（SL）



埼玉キャンパスと周辺



日本工業大学の紹介



交通案内

駅、若しくは、JR 宇都宮線の湘南新宿ライン・上野東京ラインが停車する新白岡駅を利用できます。北千住駅から東武動物公園駅までは東武スカイツリーラインの急行にて約 35 分でアクセス可能で、大宮駅から新白岡駅までは約 20 分で移動できるため、都内からのアクセスも比較的スムーズなロケーションとなります。

東武スカイツリーライン沿線には、江戸時代に整備された五街道の一つである日光街道があります。東武動物公園駅東口徒歩 5 分の場所に杉戸宿（杉戸町）。そこから東京方面に向かって、粕壁宿（春日部市）、越ヶ谷宿（越谷市）、そして、草加宿（草加市）の綾瀬川右岸沿い約 1.5 km の松並木は「草加松原」と呼ばれ、紀行文『奥の細道』で松尾芭蕉が歩いた街道と伝えられています。機会がありましたら、松尾芭蕉が旅した時代に思いを馳せながら、散策してみることもお勧めします。



平栗健史（正員）

長野県駒ヶ根市出身。筑波大学情報学博士課程を卒業後、日本電信電話(株)・NTT アクセスサービス研究所を経て現在、日本工業大学基幹工学部電気電子通信工学科教授。企業所属時は、世界初の Wi-Fi に関する研究開発に従事し、大学入職後も次世代 Wi-Fi や Beyond 5G/6G の研究開発に継続して取り組んでいる。また、同時に ICT 農業に関する研究開発として、ドローンを利用したトマト、ナシなどの受粉システム開発や、産地形成実証を目指したサツマイモの収穫から出荷までの在庫管理などのシステム化を推進している。2008 年 3 月には、博士（情報学）、2024 年 7 月には、博士（農学）の 2 学位を取得することで、現在は、工学と農学の融合領域を専門とする。

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 5 年度フェロー称号

令和 5 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！

Luigi Fortuna

[Research of Designing Circuits and Systems by Exploiting their Hidden Nonlinearities]

Q. Please share your feelings about being awarded the Fellow title.

The grade of IEICE Fellow has been achieved for the contribution in Research of Design Circuits and Systems for Exploiting their Hidden Nonlinearities. I am very proud of the nomination given to me by the IEICE. I belong to the IEICE community since 1993 and it has been an outstanding experience for my academic and professional life the opportunity to share in the IEICE activity my research and professional projects.

Q. Could you describe the research themes that currently interest you?

The main themes regarding my actual interests are devoted to nonlinear resonance phenomena and to the realization of circuit and systems based on that a principle. Moreover I am also working in transient chaotic devices and in characterizing them.

I would like to explain my next project: to extend classical robust control techniques to quantum systems. This involves a clear understanding of various problems not only regarding control theory but involving more physics areas. Therefore I am



involved to prepare low cost experiments in order to verify the practical implementation of the project and to try to give focus to the various links in physics items relating waves to classical mechanics towards quantum physics and physics statistical subjects. I will try to give a course on this subject on the next academic year.

Q. What are your aspirations for the future?

Even if I am retired since November 2023 my future task is to continue to study and to make research to teach. The mission is to stimulate the interest of young generation to establish problems, to propose new ideas that could led to great cooperation for the peace in the world and to save the status of the world improving the sustainability.

Q. Please leave a message for young researchers.

Study with passion. Couple to the technical skills human studies. Make sports and look at arts and creativity. Take care of diversity and take respect each other. Enjoy during the research work. Share your results with the scientific community. Help the others.

鎌部 浩

「環境整備によるソサイエティの研究会活動のさらなる発展の促進」

Q. フェローになられた御感想をお聞かせ下さい。

今回の申請にあたっては、桑門先生（関西大学）に大変お世話になりました。感謝しています。私が ESS 会長をしていたときには、コロナが蔓延しておりどのように研究会活動が続けていくのか、手探りの状況が続いていました。研究会活動が途切れず続いていくことに多少の旗振りで貢献したかもしれませんが、研究会を運営されていた皆さんの工夫による貢献が非常に大であったと思います。また、ソサイエティの体制を改善していくために、幹事の皆さんには大変お世話になりました。とりわけ、庶務幹事の太田先生、事業担当幹事の葛岡先生（どちらも平成 4 年度）には制度全体の見直しで大変お世話になりました。こういったある程度の規模の組織を動かすときには、優秀な人が組織としての力を発揮することが重要であることが、（深く）身にしみて分かりました。



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、主に記録への応用を対象とした制約符号について研究してきました。その中で、最も興味があるのは有限状態符号とバランス符号です。調べつくされた、と思っていましたがまだまだ研究することがあるのだということが分かってきて、現在その勉強をしています。

Q. 今後の抱負をお聞かせ下さい。

制約符号の基礎となる理論として記号力学系の理論があります。現在、この理論は様々な方向で発展しています。今後はこの分野を再度勉強し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！

自分が若いときにもっと真剣に聞いて実行していたら、もっと役に立っていたらと最近よく考えていることが 2 点あります。近年、車に乗る時間が増えてきたので、オーディオブックをよく聞いていますが、偶然「自分を鍛える（ジョン・トッド）」を聞きはじめました。その中で「本を読むときにはしっかりじっくり読め」としつこく繰り返している部分があります。これはよく聞いていたので、重要な本は自分なりにじっくり読んできたつもりでしたが、上記のように勉強し直している現在、私のやりかたは十分ではなかったと反省しています。二つめは、海外に出る機会をつかんで、海外で研究生活を送ることです。私が就職してすぐに、同じ研究室の人が 1 年間海外に出ておられたのがうらやましくて、とにかく海外に出る機会があればと思っていました。なんとか海外に出ることはできたのですが、振り返ってみると、結局、これが様々な意味で一番役に立っているようです。

清本晋作

「暗号技術ならびにプライバシー保護技術の研究開発及び国際標準化」

Q. フェローになられた御感想をお聞かせ下さい。

非才の身ながら過分な評価を頂きまして大変光栄です。これも、ひとえにこれまでご指導・ご鞭撻頂きました皆様のお陰と感じております。

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。

「信頼する／される」メカニズムの解明。AI など ICT 技術が目覚ましい進歩を遂げ、我々の社会も今後大きく変化していくと思いますが、人とシステム、更にシステムの先にある人々、との信頼関係をどう構築していくかは、安定的で持続的な社会を構成する上で重要な要素の一つであると考えております。私が研究してきた情報セキュリティ技術も信頼構築の一助にはなると考えますが、人が信頼する／されるという事象に対する、より根源的なメカニズムを解明できないかと考えております。



Q. 今後の抱負をお聞かせ下さい。

少しでも電子情報通信学会の発展に貢献できるように、今後も精進したいと思います。

Q. 若い研究者の方へメッセージをどうぞ！

研究を始めたときの好奇心と使命感を忘れずとともに頑張っていきましょう。研究を続ければ、きっと良いことがあります。

國廣 昇

「数理的な手法に基づく現代暗号の安全性評価に関する先駆的研究」

Q. フェローになられた御感想をお聞かせ下さい。

学生時代からお世話になっている電子情報通信学会からフェローの称号を授与頂けることになり、大変光栄です。多くの方々からご指導を頂き、なんとかやってこれました。関係者の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。

これまで一貫して、暗号の安全性評価を行っており、今後もこの研究テーマを続けていければと考えています。特に、秘密鍵などの本来秘密にすべき情報が部分的に誤り付きで得られたときの鍵復元に関する研究や、量子計算機に対する暗号の安全性評価を中心に研究を行っています。今後は、幅広く、耐量子計算機暗号の安全性評価も行っていきたいと思っております。

Q. 今後の抱負をお聞かせ下さい。

安全に暗号技術を利用するためには、その安全性評価が必須です。引き続き、安全性評価に関する研究を続けて、少しでも安全・安心な社会の構築に貢献できればと思います。しかし、その一方で、自分が面白いと思う研究は、絶対にいずれ何かの役には立つはずだという根拠のない自信もあって、興味の向くまま研究を続けていきたいと思っております。



サンタバーバラの夕日

Q. 若い研究者の方へメッセージをどうぞ！

最近の若い研究者は、本当に優秀な方が多いと感じます。良い研究成果が出たら、ぜひ詳しく教えてください。

令和5年度 学術奨励賞

令和5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。

足立 亮介（山口大学） “分散事象駆動制御のためのセンサネットワーク設計”⁽¹⁾



このたびは、名誉ある賞をいただき大変光栄に存じます。受賞いたしました研究では、制御システム内におけるセンサネットワーク構造及び通信頻度の同時設計問題を考えています。ネットワークを介したシステムにおいて、通信頻度とネットワーク構造は制御性能に直接影響を与えます。そのため、IoTによるスマート化や自動化に期待することは、通信と制御の信頼性への期待と言い換えられます。今後も高信頼制御通信研究会及びシステム数理と応用研究会での活動を通じて本研究を発展させるとともに、高信頼な制御通信の実現と応用を目指して邁進していく所存です。このたびは誠にありがとうございました。

谷津 帆乃果（同志社大学）



“クラウドソーシングにおける回答方式の影響—リアルタイム性と精度の比較実験—”⁽²⁾

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。本研究の遂行にあたり、終始多大なご指導ご鞭撻を賜った小坂隆浩教授をはじめ、研究室のメンバー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、クラウドソーシングを用いた犯罪検知における回答方式が、クラウドワーカーの回答にどのような影響を及ぼすのか検討いたしました。この受賞を励みに、修士課程においても日々研究に勤しんでいきたい所存です。このたびは本当にありがとうございました。

塚本 陽太（東京理科大学）



“周期入力に対する Izhikevich ニューロンモデルの応答—カオスニューロンの場合—”⁽³⁾

“カオス応答を呈する Izhikevich ニューロンに正弦波入力を印加した場合の応答解析”⁽⁴⁾

学術奨励賞という名誉ある賞を頂戴し、大変光栄に存じます。ご指導くださった池口徹教授をはじめ、研究室の皆様、議論してくださった諸先生方に心より御礼申し上げます。私の研究分野は計算論的神経科学であり、受賞論文は単一ニューロンの数理モデルの応答解析となっております。現在は、博士後期課程に進学し、神経回路網における学習を対象とした研究を行っております。この賞の名に恥じぬよう、一層研究に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。

富田 友太（三重大学）



“確率共鳴を適用した非線形システムの利用による逐次干渉除去における信号検出の低消費電力化の可能性”⁽⁵⁾

“逐次干渉除去受信機における低消費電力化のための確率共鳴を利用した ADC 低ビット化の検討”⁽⁶⁾

このたびは、学術奨励賞という名誉ある賞を賜り、大変光栄に存じます。日々、ご指導頂きました羽多野裕之先生、森香津夫先生、眞田耕輔先生をはじめ、通信工学研究室のメンバー、学会などでご助言頂きました先生方に、この場を借りて感謝を申し上げます。受賞論文では、非線形システムに対する確率共鳴現象の適用を通して、受信機における消費電力削減を検討しております。今回の受賞を励みに、社会に貢献することができるよう、今後もまい進する所存です。

豊岡 祥太（関西大学）



“ANC システムにおけるバーチャルセンシング技術の消音領域に関する検討”⁽⁷⁾

このたびは栄誉ある賞を頂き大変光栄に存じます。本研究の遂行にあたり、指導教員として多大なご指導ご鞭撻を賜りました梶川嘉延先生をはじめ、学会などでアドバイス頂いた沢山の先生方や、研究にご協力頂いた関係者の皆様に、この場をお借りして深くお礼申し上げます。本研究は、アクティブノイズコントロールに関する研究となっています。この賞を励みに、学術分野の発展や社会貢献に寄与できるような研究者を目指します。このたびは誠にありがとうございました。

山口 智也（金沢大学）



“高速画像処理用の光リザバーコンピューティングの実証”⁽⁸⁾

このたびは学術奨励賞という名誉ある賞を頂き、大変光栄に思っております。また、日頃からご指導頂いた砂田哲先生、新山友暁先生をはじめとする研究室のメンバー及び学会で議論頂きました先生方に心より感謝申し上げます。受賞論文では光コンピューティングを用いた画像処理を行い、その処理性能を検証しました。今後は社会人として、研究活動で培ってきた光や情報処理の分野にとどまらず、ほかの分野の見識も深め、社会に貢献していきたいと思えます。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) 足立亮介, “分散事象駆動制御のためのセンサネットワーク設計,” 2023 信学ソ大, A-16-3, Sept. 2023.
- (2) 谷津帆乃果, “クラウドソーシングにおける回答方式の影響—リアルタイム性と精度の比較実験—,” 2023 信学ソ大, A-10-4, Sept. 2023.
- (3) 塚本陽太, “周期入力に対する Izhikevich ニューロンモデルの応答—カオスニューロンの場合—,” 2023 信学総大, N-1-7, March 2023.
- (4) 塚本陽太, “カオス応答を呈する Izhikevich ニューロンに正弦波入力を印加した場合の応答解析,” 2023 信学ソ大, N-1-24, Sept. 2023.
- (5) 富田友太, “確率共鳴を適用した非線形システムの利用による逐次干渉除去における信号検出の低消費電力化の可能性,” 2023 信学総大, N-2-11, March 2023.
- (6) 富田友太, “逐次干渉除去受信機における低消費電力化のための確率共鳴を利用した ADC 低ビット化の検討,” 2023 信学ソ大, A-13-8, Sept. 2023.
- (7) 豊岡祥太, “ANC システムにおけるバーチャルセンシング技術の消音領域に関する検討,” 2023 信学ソ大, A-8-2, Sept. 2023.
- (8) 山口智也, “高速画像処理用の光リザバーコンピューティングの実証,” 2023 信学ソ大, N-2-2, Sept. 2023.

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 2024. Topics of interest for IWSEC 2024 include all theory and practice of cryptography, information security, and network security, as in the previous IWSEC workshops. We classify the topics of interest into two tracks as follows, but not limited to:

A: Cryptography track

- Applied cryptography
- Biometrics security and privacy
- Blockchain and cryptocurrency
- Cryptanalysis
- Cryptographic primitives
- Cryptographic protocols
- Financial cryptography
- Formal methods for security analysis
- Multiparty computation
- Post-quantum cryptography
- Privacy-preserving data mining
- Public-key cryptography
- Real-world cryptographic systems
- Symmetric-key cryptography

B: Cybersecurity and privacy track

- Cyberattacks and defenses
- Cyber physical systems
- Forensics
- Hardware security
- Human-computer interaction, security, and privacy
- Internet-of-Things security
- Intrusion detection and prevention
- Law and ethics of cybersecurity
- Machine learning and AI security
- Malware analysis
- Measurements for cybersecurity
- Mobile and web security
- Network, system and cloud security
- Offensive security
- Privacy-enhancing technologies
- Program analysis
- Software security
- Supply chain security

Keynote Talks

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

- **Dr. Dustin Moody** (National Institute of Standards and Technology (NIST), US)
- **Prof. Thomas Peyrin** (School of Physical and Mathematical Sciences of Nanyang Technological University (NTU), Singapore)
- **Prof. Andreas Rauber** (Data Science Research Unit at the Department of Information Systems Engineering at the Vienna University of Technology and Head of the Vienna Scientific Cluster Research Center, Austria)

Committees

- General Co-Chairs: Junji Shikata (Yokohama National University, Japan)
Koji Chida (Gunma University, Japan)
- Program Co-Chairs: Kazuhiko Minematsu (NEC, Japan & Yokohama National University, Japan)
Mamoru Mimura (National Defense Academy, Japan)

開催案内

2024 International Workshop on Smart Info-Media Systems in Asia (SISA2024)

~~17-19 September, 2024~~ **5 – 6 December, 2024**

~~Kumamoto Jo Hall, Kumamoto,~~ **Osaka Electro-Communication University, Osaka, Japan**

Organizing Committee

Honorary Chairs

Hiroshi Ochi

Kyushu Institute of Technology, Japan

General Co-Chairs

Masayuki Kurosaki

Kyushu Institute of Technology, Japan

Naoto Sasaoka

Tottori University, Japan

Technical Program Chairs

Yoshimitsu Kuroki

National Institute of Technology,

Kurume College, Japan

Publicity Chair

Min-Chul Lee

Kyushu Institute of Technology, Japan

Finance & Registration Chairs

Naoto Sasaoka

Tottori University, Japan

Information System Chairs

Shingo Yoshizawa

Kitami Institute of Technology, Japan

Local Arrangement Chairs

Yuhei Nagao

Radrix Inc., Japan

Yosuke Sugiura

Saitama University, Japan

Advisory Board Liaison

Tomoaki Kimura

Kanagawa Institute of Technology,

Japan

General Secretaries

Nico Surantha

Tokyo City University, Japan

International Steering Committee

Chair:

Naoto Sasaoka, *Japan*

Members:

Hakaru Tamukoh, *Japan*

Yosiaki Makabe, *Japan*

Yosuke Sugiura, *Japan*

Yuichiro Tanaka, *Japan*

Call for Papers

The 2024 International Workshop on Smart Info-Media System in Asia (SISA2024) will be held at Osaka Electro-Communication University, Osaka, Japan. The SISA2024 presents every possibility on new information technologies and its smart systems.

The SISA2024 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 SISA2024 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 Video Processing and Coding
- 2.3 Video and Multimedia Technology & Communications
- 2.4 Audio/Acoustic Signal Processing
- 2.5 Signal Processing for Medical Technologies
- 2.6 Intelligent Signal Processing for Multimedia & Systems
- 2.7 Security Signal Processing for Multimedia & Systems
- 2.8 Parallel Implementation for Multimedia & Systems
- 2.9 Emerging Technologies for Multimedia & Systems

3. Information Science and Technologies

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

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:

~~May 24, 2024~~ **Jul. 26, 2024**

Notification of Acceptance:

~~July 15, 2024~~ **Sep. 30, 2024**

Deadline for Submission of Camera Ready Paper:

~~August 9, 2024~~ **Nov. 8, 2024**

SISA 2024 Student Paper Awards

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

Special Section on IEICE Trans. Fundamentals

We plan to publish a Special Section on *IEICE Trans. Fundamentals* on November 2025. Authors who presented their original works in SISA 2024 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 SISA 2024 website.

論文募集

第47回情報理論とその応用シンポジウム (SITA 2024) 開催案内

ご挨拶

第47回情報理論とその応用シンポジウム(SITA2024)を福井県あわら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。初めての福井県開催となる2024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 辻岡哲夫



開催期間・会場

2024年12月10日（火）～ 12月13日（金）
福井県あわら市 芦原温泉 清風荘
<https://www.seifuso.com/>

対象分野

シャノン理論、情報源符号化、データ圧縮、符号理論とその技法、通信路符号化、通信理論、符号化・変調、伝送方式、無線アクセス・ネットワーク、ワイドバンドシステム、通信方式、系列、確率過程、検定と推定、暗号、情報理論的安全性、情報セキュリティ、マルチユーザ情報理論、ネットワーク符号化、分散符号化・分散計算、計算複雑性理論、情報ネットワーク、量子情報理論、量子符号・暗号、信号処理、画像・音声処理、圧縮センシングとスパース性、パターン認識、統計的機械学習、記録素子用の符号化・信号処理、情報理論基礎・応用、情報統計力学、その他技術的内容

主催

電子情報通信学会 基礎・境界ソサイエティ
情報理論とその応用サブソサイエティ

協賛

電子情報通信学会 EMM、ISEC、RCC、SIP、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/SITA2024/>

今後のスケジュール

発表申込開始: 8月1日（木）
発表申込締切: 9月上旬
発表原稿締切: 9月下旬

実行委員会

実行委員長：
辻岡 哲夫（大阪公立大学）
プログラム委員長：
楫 勇一（名古屋大学）
総務：森島 佑（東北学院大学）
会計：岩田 基（大阪公立大学）
出版：山下 恭佑（大阪大学）
矢内 直人（大阪大学）
会場：岩田 賢一（福井大学）
登録：小西 たつ美（愛知工業大学）
瀧田 慎（神戸大学）
広報：守屋 宣（近畿大学）
プログラム委員会幹事：
路 姍（名古屋大学）
アドバイザー：
岡 育生（大阪公立大学）
藤原 融（島根大学）
葛岡 成晃（和歌山大学）

事務局

〒984-8588
仙台市若林区清水小路3-1
東北学院大学工学部 情報基盤工学科
SITA2024事務局 森島 佑
E-mail: sita-2024@mail.ieice.org



基礎・境界ソサイエティ運営委員会

会長	和山 正	(名古屋工業大学)
次期会長	尾上 孝雄	(大阪大学)
ソサイエティ編集長	大橋 正良	(国際電気通信基礎技術研究所)
副会長 (事業担当)	澁谷 智治	(上智大学)
副会長 (システムと信号処理)	田中 聡久	(東京農工大学)
副会長 (音響・超音波)	小野 順貴	(東京都立大学)
副会長 (情報理論とその応用)	小嶋 徹也	(東京工業高等専門学校)
庶務幹事	葛岡 成晃	(和歌山大学)
庶務幹事	傘 昊	(東京都市大学)
会計幹事	小林健太郎	(名城大学)
会計幹事	筒井 弘	(北海道大学)
事業担当幹事	三村 和史	(広島市立大学)
事業担当幹事	黒崎 正行	(九州工業大学)
大会担当幹事	大東 俊博	(東海大学)
大会担当幹事	伊藤 大輔	(岐阜大学)
電子広報担当幹事	西川 広記	(大阪大学)
電子広報担当幹事	古賀 崇了	(近畿大学)
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)
ソサイエティ誌編集委員長	高島 康裕	(北九州市立大学)
ソサイエティ誌担当幹事	松田 哲直	(埼玉大学)
ソサイエティ誌担当幹事	松井健太郎	(日本放送協会)
特別委員 (ソサイエティ誌多言語化)	鎌部 浩	(岐阜大学)
編集特別幹事 (オブザーバ)	山脇 大造	(日立製作所)
出版委員会委員 (オブザーバ)	藤沢 匡哉	(東京理科大学)
研究会連絡会幹事 (オブザーバ)	高島 康裕	(北九州市立大学)
ハンドブック／知識ベース委員 (オブザーバ)	太田 隆博	(専修大学)
男女共同参画委員会 (オブザーバ)	小西 かつ美	(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	水橋 慶, 永井 宏	(電子情報通信学会)

基礎・境界ソサイエティサブソ・研専会議

副会長 (事業担当)	澁谷 智治	(上智大学)
副会長 (システムと信号処理)	田中 聡久	(東京農工大学)
副会長 (音響・超音波)	小野 順貴	(東京都立大学)
副会長 (情報理論とその応用)	小嶋 徹也	(東京工業高等専門学校)
事業担当幹事	三村 和史	(広島市立大学)
事業担当幹事	黒崎 正行	(九州工業大学)
回路とシステム (CAS)	篠宮 紀彦	(創価大学)
情報理論 (IT)	野上 保之	(岡山大学)
信頼性 (R)	門田 靖	(リコー先端研究所)
超音波 (US)	工藤すばる	(東京都立大学)
応用音響 (EA)	小野 順貴	(東京都立大学)
VLSI 設計技術 (VLD)	桜井 祐司	(日立製作所)
情報セキュリティ (ISEC)	四方 順司	(横浜国立大学)
信号処理 (SIP)	市毛 弘一	(横浜国立大学)
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)	山口 真悟	(山口大学)
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)	辰巳 丈夫	(放送大学)
ITS (高度交通システム) (ITS)	高取 祐介	(神奈川工科大学)
スマートインフォメディアシステム (SIS)	笹岡 直人	(鳥取大学)
イメージメディアクオリティ (IMQ)	工藤 博章	(名古屋大学)
高信頼制御通信 (RCC)	石井 光治	(香川大学)
バイオメトリクス (BioX)	高野 博史	(富山県立大学)
安全・安心な生活と ICT (ICTSSL)	大塚 晃	(事業創造大学院大学)
ハードウェアセキュリティ (HWS)	林 優一	(奈良先端科学技術大学院大学)
光輝会 (SSA) (オブザーバ)	宮地 充子	(大阪大学大学院)
技術の歴史 (オブザーバ)	篠田 庄司	(中央大学)
技術者教育と優良実践 (オブザーバ)	横田 光広	(宮崎大学)
ヒューマンコミュニケーション G (オブザーバ)	松田 昌史	(NTT コミュニケーション科学基礎研究所)
会長 (オブザーバ)	和山 正	(名古屋工業大学)
次期会長 (オブザーバ)	尾上 孝雄	(大阪大学)
庶務幹事 (オブザーバ)	葛岡 成晃	(和歌山大学)
庶務幹事 (オブザーバ)	傘 昊	(東京都市大学)
研究会連絡会幹事 (オブザーバ)	高島 康裕	(北九州市立大学)
事務局	水橋 慶, 永井 宏	(電子情報通信学会)

NOLTA ソサイエティ運営委員会

ソサイエティ会長	夏目 季代久	(九州工業大学)
ソサイエティ次期会長	関屋 大雄	(千葉大学)
庶務幹事	立野 勝巳	(九州工業大学)
庶務幹事	荒井 伸太郎	(岡山理科大学)
会計幹事	木村 貴幸	(日本工業大学)
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	小西 啓治	(大阪府立大学)
運営委員	鳥飼 弘幸	(法政大学)
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	丹治 裕一	(香川大学)
運営委員	長谷川 幹雄	(東京理科大学)
運営委員	青森 久	(中京大学)
運営委員	保坂 亮介	(芝浦工業大学)
運営委員	中野 秀洋	(東京都市大学)
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	佐々木 智志	(湘南工科大学)
運営委員	斎藤 利通	(法政大学)
運営委員	浅井 哲也	(北海道大学)
運営委員	井岡 恵理	(芝浦工業大学)

Fundamentals Review 編集委員会

編集委員長	高島 康裕 (北九州市立大学)
編集委員会幹事 (正)	松田 哲直 (埼玉大学)
編集委員会幹事 (副)	松井健太郎 (日本放送協会)
編集委員会幹事補佐	宮北 和之 (新潟大学)
編集委員	
編集委員 (CAS)	越田 俊介 (八戸工業大学)
編集委員 (VLD)	新谷 道広 (京都工芸繊維大学)
編集委員 (SIP)	小西 克巳 (法政大学)
編集委員 (MSS)	野村 雅司 (三菱電機株式会社)
編集委員 (IT)	金子 晴彦 (東京工業大学)
編集委員 (ISEC)	海上 勇二 (パナソニックホールディングス)
編集委員 (WBS)	孫 冉 (茨城大学)
編集委員 (US)	大久保 寛 (東京都立大学)
編集委員 (EA)	加古 達也 (日本電信電話株式会社)
編集委員 (NLP)	伊藤 大輔 (岐阜大学)
編集委員 (R)	吉川 隆英 (富士通研究所)
編集委員 (TL)	神長 伸幸 (ミイダス)
編集委員 (SITE)	山肩 大祐 (IGDA 日本)
編集委員 (ITS)	金 帝演 (鶴岡工業高等専門学校)
編集委員 (SIS)	二神 拓也 (愛知学院大学)
編集委員 (IMQ)	山添 崇 (湘南工科大学)
編集委員 (BioX)	河原 智一 (東芝インフラシステムズ株式会社)
編集委員 (RCC)	鍋谷 寿久 (株式会社東芝)
編集委員 (CCS)	眞田 耕輔 (三重大学)
編集委員 (ICTSSL)	宇津 圭祐 (東海大学)
編集委員 (HWS)	矢嶋 純 (富士通株式会社富士通研究所)

(上記に含まれない右側の編集幹事会の委員も編集委員として含む)

学会事務局

水橋 慶, 永井 宏
(電子情報通信学会)

Fundamentals Review 編集幹事会

編集委員長	高島 康裕 (北九州市立大学)
編集幹事会幹事 (正)	松田 哲直 (埼玉大学)
編集幹事会幹事 (副)	松井健太郎 (日本放送協会)
編集幹事会幹事補佐	宮北 和之 (新潟大学)
編集幹事	
幹事 (総務)	八木 秀樹 (電気通信大学)
幹事 (渉外)	傘 昊 (東京都市大学)
幹事 (企画)	山岸 昌夫 (法政大学)
幹事 (Web: 正)	西川 広記 (大阪大学)
幹事 (Web: 副)	古賀 崇了 (近畿大学)
特別編集幹事 (Vol.18 No.1)	孫 冉 (WBS) (茨城大学)
特別編集幹事 (Vol.18 No.2)	山肩 大祐 (SITE) (IGDA 日本)
特別編集幹事 (Vol.18 No.3)	越田 俊介 (CAS) (八戸工業大学)
特別編集幹事 (Vol.18 No.4)	金子 晴彦 (IT) (東京工業大学)
顧問	貴家 仁志 (東京都立大学)
顧問	白井 宏 (中央大学)
顧問	今井 浩 (東京大学)
顧問	牧野 光則 (中央大学)
顧問	高橋 篤司 (東京工業大学)
顧問	國廣 昇 (筑波大学)
顧問	関屋 大雄 (千葉大学)

編集後記

Fundamentals Review 誌 Vol. 18 No. 1 を皆様にお送りいたします。今号から編集体制も新年度に移行し、新たなメンバーとなっております。ただ、良質な記事を皆様にお届けするということには、変化がありません。このことをしっかりと念頭に置きながら、編集作業を続けていきたいと考えています。今後ともよろしくお願いいたします。(高島康裕)

今号より編集正幹事を担当することになりました。編集委員会及び編集幹事会も新体制となり、気持ちを新たに編集作業のスタートを切っております。新しい委員の皆様とともに、今後も読者の皆様にとって有益で興味深い内容をお届けできるよう取り組んでまいります。また、これまでと同様ではございますが、FR 誌にご寄稿頂ける皆様には、記事を円滑にご執筆頂けるようサポートしてまいりたいと思います。今後ともどうぞよろしくお願い申し上げます。(松田哲直)

今号より編集幹事会編集副幹事を務めることになり、開催案内をはじめとする「やわらかい記事」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。FR 誌は季刊となりますため、編集作業もついのんびりと始めてしまいます。そのため最後慌てることが常態となりつつあり、事務局・出版社の皆様にはいつもご迷惑をお掛けしております。(松井健太郎)

今号より編集幹事補佐を担当することになりました。今号では「受賞者の声」を担当しております。受賞された皆様、改めましておめでとうございます。また、スムーズな編集作業にご協力頂きまして、ありがとうございました。編集作業に本格的に関わるのは初めてなのですが、このような立場になって初めて気付かされる FR 誌の魅力というものもありました。皆様も是非楽しんでご覧頂ければと思います。(宮北和之)

このたび、「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。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、この場を借りて心より感謝申し上げます。各研究会が活発な参加と深い議論の場となるよう努めておりますので、ぜひ各研究会の取り組みをご一読いただき、投稿やご参加をご検討頂ければ幸いです。まだまだ至らない点も多いですが、FR 誌の編集委員として一層努力してまいります。引き続きよろしくお願い申し上げます。(孫冉)

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>

複写される方へ

一般社団法人電子情報通信学会は、本誌に掲載された著作物の複写複製に関する権利を一般社団法人学術著作権協会に委託しております。複写複製を御希望の方は、一般社団法人学術著作権協会 (<https://www.jaacc.org>) が提供している複製利用許諾システムを通じて申請して下さい。

なお、複写以外の許諾（著作物の転載、翻訳等）に関しては、委託致しておりませんので、直接本会へお問い合わせ下さい。

<問合せ先> 一般社団法人電子情報通信学会

TEL [03] 3433-6691 FAX [03] 3433-6659

著作物利用許諾申請：<https://www.ieice.org/jpn/copyright/tensai.html>

Reprographic Reproduction outside Japan

Making a copy of this publication

The IEICE authorized Japan Academic Association For Copyright Clearance (JAC) to license our reproduction rights of copyrighted works. If you wish to obtain permission of these rights, please refer to the homepage of JAC (<https://www.jaacc.org/en/>) and confirm appropriate organizations to request permission.

Obtaining permission to quote, reproduce; translate, etc.

Please contact the copyright holder directly.

IEICE Secretariat Office,

E-mail: permission@ieice.org

Permission request form: <https://db.ieice.org/chosaku/sinsei/index-e.php>

Fundamentals Review 第十八巻 第一号

令和六年七月一日発行

発行人 発行所	白石 智 一般社団法人 電子情報通信学会 基礎・境界サイエンス 〒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 WEB 化担当会社	山岡影光 三美印刷株式会社 東京都荒川区西日暮里 6-28-1