令和４年 10 月１日発行　第 62 号

Fundamentals Review

2022 October Vol.16 No. 2

技術の原点

位相同期回路の集積化とその応用

エネルギー効率を追求するコンピューティング

情報理論に基づく秘密情報の符号化
――不完全秘匿を用いた安全な符号化法――

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

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

ESS
2022
October
Vol.16 No.
2

Fundamentals

ごあいさつ

48 英文論文誌・今後の方向性に対する私見 田口 亮

技術の原点

51 位相同期回路の集積化とその応用 小久保優
57 エネルギー効率を追求するコンピューティング 宇佐美公良
66 情報理論に基づく秘密情報の符号化
——不完全秘匿を用いた安全な符号化法—— 山本博資

解説論文

76 結合発振器に生じる Amplitude Death
——ロバスト安定性からのアプローチ—— 小西啓治，杉谷栄規
83 説明可能 AI 技術のこれまでとこれから 亀谷由隆
93 IC チップのサプライチェーン・セキュリティ
——真正性を脅かす課題と対策—— 永田 真
100 プライバシー保護を考慮した秘匿化領域におけるスパースデータモデリング 仲地孝之，坂東幸浩

その他

115 ESS ニュース
115 2022 年 電子情報通信学会 NOLTA ソサイエティ大会 開催報告 加藤秀行
118 研究会に行こう！
118 超音波研究会（US） 中村健太郎
118 VLSI 設計技術研究会（VLD） 池田奈美子
119 非線形問題研究会（NLP） 常田明夫
119 スマートインフォメディアシステム研究会（SIS） 木村誠聡
120 イメージ・メディア・クオリティ研究専門委員会（IMQ） 魚森謙也
121 応用音響研究会（EA） 加古達也
122 国際会議報告
122 IEEE International Symposium on Information Theory 中原悠太
124 The 37th International Technical Conference on Circuits/Systems, Computers and Communications 高井重昌
126 受賞者の声
126 第 78 回（令和 3 年度）論文賞
129 開催案内
130 論文募集

Review

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

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

Preface

48 Personal View of the Future Direction of IEICE Transactions
Akira TAGUCHI

Origins of Technology

51 Integration Techniques of Phase-Locked Loops and Their Applications
Masaru KOKUBO

57 Computing in pursuit of energy efficiency
Kimiyoshi USAMI

66 Information Security Coding Based on Information Theory
: Secure Coding with Non-Perfect Secrecy
Hirosuke YAMAMOTO

Review Papers

76 Amplitude Death in Coupled Oscillators
: An Approach from Robust Stability
Keiji KONISHI, Yoshiki SUGITANI

83 The Past and the Future of Explainable AI Techniques
Yoshitaka KAMEYA

93 Supply Chain Security of IC Chips
: Problems and Solutions for Authenticity under Threat
Makoto NAGATA

100 Privacy-Preserving Sparse Data Modeling in Encrypted Domain
Takayuki NAKACHI, Yukihiro BANDOH

Miscellaneous Articles

115 ESS News

118 Let's go to IEICE Workshops!

122 International Conference Report

126 Winners' Voice

129 Call for Participations

130 Call for Papers

ごあいさつ

英文論文誌・今後の方向性に対する私見

Personal View of the Future Direction of IEICE Transactions

ソサイエティ編集長　田口　亮

1. はじめに

基礎・境界ソサイエティにおいて発行している英文論文誌 A の編集委員を 1999 年度，2000 年度の 2 年間務め，2001 年度には編集幹事，2002 年度は編集副幹事を務めた．約 20 年前に英文論文誌の編集に関わっていたことになる．その後，2011 年度には FR 誌の編集委員も務めた．そのようなことから，基礎・境界ソサイエティの編集に対しては常に関心をもってきた．本稿では，英文論文誌を中心に 20 年前のことも振り返りながら今後の英文論文誌の方向性について私見を述べることにする．

2. 2001 年当時の英文論文誌を振り返る

図 1 に 2000 年から 2021 年までの論文・レター投稿数と掲載数をグラフに示した．論文の投稿数を見れば，2005 年前後で MAX に達し，2007 年以降は単調減少している．私が編集幹事を務めていた 2001 年の投稿件数は論文が 615 件，レターが 102 件であった．一方，2021 年における投稿件数は論文 305 件，レター 131 件と，2001 年との比較で論文は約 50% となり，レターがほぼ同数である．

2001 年当時は投稿件数が増加傾向であり，投稿件数に関する心配は全くなく，むしろ，当時は論文誌が紙媒体の出版であり，郵送料（海外への郵送も含め）もそれなりに必要であったことも影響して英文論文誌の収支における赤字幅の大きさが問題になっていた．実際は和文論文誌の黒字幅が大きく，両論文誌を合わせるとバランスが取れていたが，英文論文誌としての赤字体質を脱却するための検討を行っていたことを記憶している．

インパクトファクター（IF）については図 2 に，これも 2000 年から 2021 年までの変化をグラフに示した．この 20 年間，IF＝0.3 を前後して変化していて，2021 年は IF＝0.42 と少し高い数値を示しているが，それでもその数値は低い．2001 年も IF＝0.35 と現在と大差はない．当然，2001 年当時も IF の向上策の検討を行っていた．英文論文誌 A の名称は IEICE Transaction on Fundamentals of Electronics, Communications and Computer Sciences と専門分野が絞れていないため，ある特定の分野に興味をもつ研究者に対してインパクトが小さい．そこで，ほぼ毎月小特集を企画し，特定の分野の研究者に対しても論文誌に関心をもってもらうことを考えていた．その小特集に良質の解説論文を掲載することで，引用件数増加を図ろうと考えていた．その後の推移を確認することなく英文論文誌の編集の仕事を退くことになったが，結果的に効果が上がっていなかったことは図 2 から理解できる．

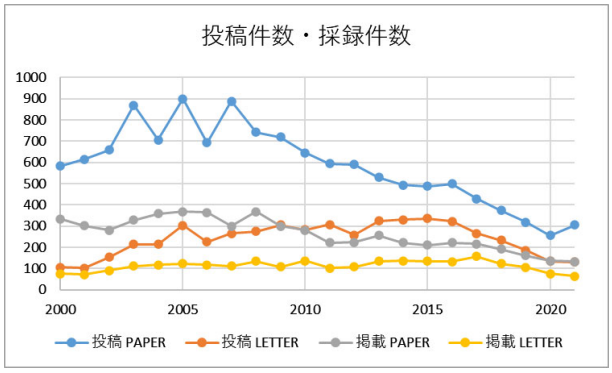


図 1　英文論文誌の投稿件数・採録件数（2000〜2021 年）

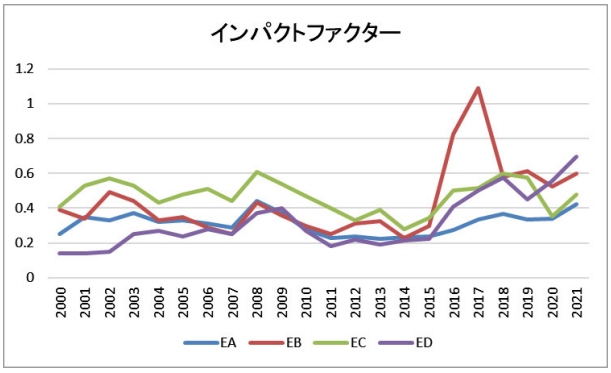


図 2　英文論文誌のインパクトファクタ（2000〜2021 年）

3. 英文論文誌の現状

英文論文誌においては IF の向上が常に第 1 の課題になっていて，昨今は投稿件数，とりわけ海外からの投稿件数の減少が問題になってきたことを受けて，投稿件数の増加を図ることも大きな課題になっていると認識している．実は，この二つの課題は関わりをもっていると考えている．IF が低い論文誌の価値が低く評価され，海外の研究者にとっての投稿対象の論文誌から除外されている恐れがあると考えているからである．正直，英文論文誌 A よりも IF が高く，掲載までの審査が楽な論文誌も存在することも投稿件数の減少に結びついているのではないか．

最近，大学での役職の関係から，マレーシア（マレーシア工科大学，マラヤ大学など）やフィリピン（デ・ラサール大学など）のトップランクの大学の教員（研究者）と接する機会が増えている．それら大学が教員の研究業績に対して，毎年，高いノルマを課していること，更に，大学側から掲載論文誌のクオリティに関しても注文が出されていることを知った．クオリティとは Quartile（四分位）指標のことで，これは，ある論文誌の IF がその論文誌の属する分野の論文誌群における相対的な位置を示すものである．Q1 が上位 25% 以内，Q2 が 26〜50%，Q3 が 51〜75%，そして Q4 がそれ以下となる．IF の数値自体は専門分野によって大きく異なり，中央値の最も高いのが自然科学分野の細胞生物学（3.7）であり，最も低い分野が，心理学の精神分析（0.42）である[(1)]．Quartile（四分位）指標は専門分野間の IF の偏りの影響を回避していることになる．そして，少なくとも，マレーシアやフィリピンのトップランクの大学の教員には Q1，Q2 の論文誌への掲載が要求されている．

2021 年の Journal Citation Reports（JCR）を見る機会を得た．図 2 の 2021 年の IF はそこから得た数値であるが，JCR では Rank by Journal Impact Factor も記されている．英文論文誌 A の場合は「COMPUTER SCIENCE, HARDWARE & ARCHITECTURE」,「COMPUTER SCIENCE, INFORMATION SYSTEMS」の二つのカテゴリで順位付けが成されている．前者は 54 論文誌中の 54 位，後者が 164 論文誌中の 162 位であり，Q4 とランクが付けされる．かなり絶望的な状況である．

昨今の IF 向上策について記しておく．オープンアクセス化は常に IF 向上に対する重要な方策と考えられている．情報・システムソサイエティ（ISS）が発行する英文論文誌 D が 2017 年 1 月号からトライアルとの立場でオープンアクセス化していて，英文論文誌 A もこれまでハイブリッド方式（オープンアクセスを希望する論文のみ掲載料にオープンアクセス料を課金する）を採用していたが，2022 年 10 月号以降は全ての論文に対する掲載料を値上げし，全ての論文のオープンアクセス化に踏み切った．図 2 において英文論文誌 D のオープンアクセス化の効果を見ると，2017 年以降，IF は大きな上昇幅ではないが上昇傾向であるように見える．英文論文誌 A もオープンアクセス化による効果を期待したい．しかしながら，英文論文誌 D の 2021 年の Rank by Journal Impact Factor を見ると，同じ分野の論文誌との相対比較で最下位に近く Q3 論文誌へは程遠い．英文論文誌 A の場合も上述のごとく，少々の IF 値の向上では焼け石に水ではなかろうか．

そのほかの方策として，非会員の論文投稿を可能にし，良質の論文がほかの論文誌へ流出することと，投稿件数の下降に対する歯止めを目的にしている．

4. 英文論文誌の今後

IF に対する批判（例えば文献[(2)]）が成されていることはよく知られていることであるが，そのような批判の中においても IF を個々の研究者や機関を評価するために使用すべきではないが論文誌としての評価は可能であるとの見解が示されている．好むと好まざるとにかかわらず IF は論文誌の最も有力な評価指標であろう．しかしながら，現状の英文論文誌 A の IF の数値は目標とする数値（Q3 の最低 IF）と大きくかい離している．IF の大幅な向上のためには，英文論文誌 A のあり方を抜本的に変える必要があり，以下にその私見を記す．

1） 編集委員会の国際化

編集委員に海外の研究者を加えることを実現していることは分かるが，国際ジャーナルとしての編集体制になっているのだろうか．抜本的な国際化は編集委員会の国際化からスタートする必要もあるかもしれない．

2） 論文誌向上のための WG の設置

これまで述べてきことからも分かるかと思うが IF の向上は短期間で成し遂げることは不可能であり，5 年以上の中長期戦略を要すると思われる．編集長，編集幹事を中心に論文誌の向上策を検討していると思われるが，その任期は短く，大胆な方策を取ることは難しい．論文誌向上のための WG を設置し，メンバーは少なくとも 5 年以上任を務めることを条件で集め，IF 向上のための方策を企画・実施して頂きたい．

3） 論文誌の細分化

英文論文誌 A はその専門分野が広すぎることから，もっと，細分化してはどうであろうか．そのことによって海外の研究者から専門の分かりやすい論文誌にできるはずである．NOLTA が先陣を切った感があり，情報理論とその応用サブソもいろいろな工夫をしている．例えば，サブソが論文誌を発行するようにすることが論文誌細分化への近道かもしれない．このような抜本的な改革の検討のためにも 2）で示した WG が必要である．

5. おわりに

この原稿を作成するにあたり，改めて，この 20 年間の英文論文誌 A のデータに目を通す機会を得た．この 20 年間，いろいろな立場から学会活動に関わってきたことから，論文誌を取り巻く大まかな状況認識はできていたと思っていたが，改めてデータを目の当たりにして「失われた 20 年」の感を強くした．

本会は昨今，学会員の急激な減少もあり，学会のサービスを抜本的に見直していて，学会存続を本気で考えているが，学会の存続は論文誌の充実に依存するところが大きいことは言うまでもない．言い換えれば，学会の価値は発行している論文誌の価値に依存するところが大きいということである．そのことを念頭にソサイエティの編集に対して微力ながら尽力させて頂ければと思っている．

文　献

（1） Quartile 指標について，https://www.innovation.hirosaki-u.ac.jp/wp-content/uploads/2020/09/0aa57f38e1f1bb9e426cba93b81312fb.pdf

（2） “European Association of Science Editors（EASE）Statement on Inappropriate Use of Impact Factors,“ https://ease.org.uk/impact-factor-statement/

著者紹介

田口　亮（正員：フェロー）

1984 慶大・工・電気卒，1989 慶大・理工・博士課程了，工学博士．同年，武蔵工大（現 東京都市大）助手．現在，東京都市大・情報工・教授（院総合理工学研究科長，国際センター長）．本会にて，英文論文誌編集幹事（2001〜2002），SIS 研専委員長（2008〜2009），ESS 運営委員会庶務幹事（2014〜2015），ESS 次期会長（2018），ESS 会長（2019），総合大会実行委員長（2011），ソサイエティ大会実行委員長（2017）などを歴任．特別功労賞（2003），貢献賞（2016），教育功労賞（2019）などを受賞．

技術の原点

位相同期回路の集積化とその応用

Integration Techniques of Phase-Locked Loops and Their Applications

小久保優 Masaru KOKUBO

アブストラクト　筆者の PLL の研究における技術の原点として PLL 帰還ループ内に ΣΔ 変調器を挿入する方式について記述する．ここで ΣΔ 変調器を用いたことにより所望の特性と雑音拡散とのバランスが集積化時に重要であり，その開発例として，携帯電話用 PLL，Bluetooth 用ツーポイント変調，及びスプレッドスペクトラムクロック生成回路について説明する．このように ΣΔ 変調器を用いた帰還ループでの雑音拡散に関する検討を行うことで，PLL の帰還ループがもつフィルタ特性を活かすことができ，ΣΔ 変調器をループ内に挿入しても雑音増加を防ぎつつ，かつ，いろいろな用途の機能をもつ PLL を集積化し，実現することができる．

キーワード　位相同期回路，PLL，ΣΔ 変調，携帯電話，Bluetooth，スプレッドスペクトラムクロック，周波数シンセサイザ，集積回路

1. 位相同期回路（PLL）の概要

今回の位相同期回路（以下 PLL : phase locked loop）(注1)の研究に関する「技術の原点」の執筆を依頼されたときに，最初に脳裏をよぎったことは，上手くいった研究テーマを記載するか，それとも上手くいかなくて課題が残された研究テーマを話題にするかということだった．「失敗は成功の母」という言葉もあるので，今回は PLL を集積する上では擾乱要素，いい換えれば PLL としては新たな雑音源となり得る機能ブロックを用いたときの振る舞いに関する筆者の失敗の経験から話題を始めて，それにつながる技術についてまとめてみたいと思う．

まず本題に入る前に PLL[1] とはどのような構成で，何のために使われる機能ブロックであるかを説明する．PLL とは，図 1 のように雑音を含んだ入力信号に対し，その雑音成分を抑圧するフィルタ処理を施すことで雑音が抑圧された信号を出力する機能ブロックである．つまり PLL とは「入力された信号に対して，出力信号の位相と周波数が完全に連動して制御できる」ことであり，たとえ入力信号の周波数や位相が変動したとしても，出力信号はその変動に追従しなければならない．

このような同期と追従という機能をもつことにより，例えば，雑音の含まれたクロック信号を元の綺麗なクロック信号に再生して，伝送系から受信したディジタル信号の判定を行うような伝送回路(注2)[2]，集積回路(注3)の外部から低い周波数のクロックを入力して集積回路内部で用いる高速なクロック信号に変換する周波数シンセサイザ(注4)[3]，更には周波数変化を信号として送ることで情報伝達を行う，所謂，周波数変調（以下 FM : frequency modulation）(注5)用送受信機[4]として

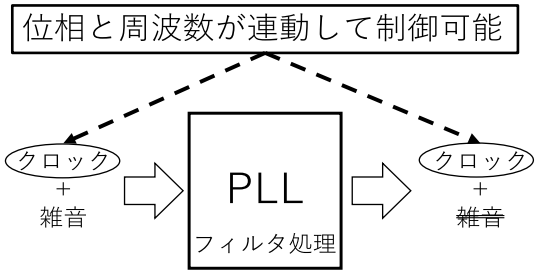


図 1　PLL の働き　　PLL とは雑音を含んだ入力信号に対し，その雑音成分を抑圧するフィルタ処理を施し，雑音が抑圧された信号を出力する機能ブロックであり，入力された信号に対する出力信号の位相と周波数が完全に連動して制御することができる．

(注 1)：位相同期回路　　入力信号と位相と周波数が連動するように制御された機能ブロック．二つの入力間の位相差を検出する回路位相周波数比較器，位相差をアナログ信号に変換するチャージポンプ，帰還ループ内の安定性と雑音抑圧を行うループフィルタ，発振周波数が制御できる電圧制御発振器，及び，指定された分周数でカウントする分周器から構成される．

(注 2)：伝送回路　　ディジタル信号を送受信する伝送系のこと．データの変化点を検出する同期機能が必要となる．

(注 3)：集積回路　　半導体上に回路部品を搭載して，所定の機能を実現する電子部品．

(注 4)：周波数シンセサイザ　　低周波数クロックを入力し高速なクロックを発生する機能ブロック．

(注 5)：周波数変調　　搬送波に対する周波数変化を信号として送ることで情報伝達を行う方式．

小久保優　正員　株式会社日立製作所研究開発グループデジタルサービス研究統括本部計測イノベーションセンタエッジコンピューティング研究部
E-mail　masaru.kokubo.zv@hitachi.com
Masaru KOKUBO, Member（Edge Computing Research Department, Instrumentation Innovation Center, Center for Digital Services, Research & Development Group, Hitachi, Ltd, Japan.
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.51-56 2022 年 10 月

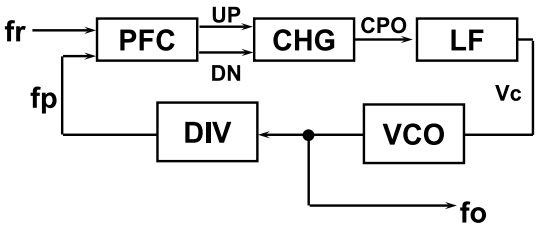


図 2　PLL の構成例[3]　一般的な PLL のブロック構成例を示す．このブロック構成において fr が入力，fo が出力である．PLL は位相周波数比較器（PFC），チャージポンプ（CHG），ループフィルタ（LF），電圧制御発振器（VCO），及び分周器（DIV）から構成される．

利用されている．

図 2 は一般的な PLL のブロック構成である．PLL は位相周波数比較器（PFC），チャージポンプ（CHG），ループフィルタ（LF），電圧制御発振器（VCO），及び分周器（DIV）から構成される．PLL は図 2 に示すように DIV の出力が PFC の入力に帰還する経路を構成する．まず，PFC には基準となるクロック（fr）と前述した DIV 出力の帰還クロック（fp）が入力され，それらの間の位相差が検出される．ここで位相差が大きすぎる場合は PFC からは周波数差の情報も出力されるので位相周波数比較器と呼ばれている．次に PFC から出力された UP 信号，若しくは，DN 信号は，これらは位相進みと位相遅れを示す制御信号に相当するが，次段の CHG でアナログ信号に変換される．ここで CHG では UP/DN 信号の幅に相当する電流が出力（CPO）から供給，若しくは，吸引される方法がとられることが多いため，チャージポンプと呼称されている．次に UP/DN 信号の幅に相当する電流を受けた LF でフィルタ処理が行われる．LF の次段となる VCO は，入力された制御電圧（Vc）に対応した周波数で発振する回路であり，PLL の出力となる．最後に VCO 出力（f_o）は先ほどの DIV に入力され，一連の帰還ループが構成される．ここで VCO は周波数を変化させるという働きをもつが，信号の位相という観点で見ると周波数の変化を「積分」していることと等価となるため，この PLL の帰還ループは LF がもつフィルタと合わせて二つの積分要素をもつことになる．そのため LF でのフィルタ処理では雑音抑圧だけでなく，一次予測を行うことで帰還ループの安定性も確保できるように構成しなければならない．

このように帰還ループを構成した PLL 出力（f_o）の周波数は，DIV 分周数を N としたとき，

$$f_o = N \times f_r \qquad (1)$$

の関係が成立する．伝送回路として用いられるときは $N=1$ として入力信号と同じ周波数を出力するが，周波数シンセサイザのように N を大きく設定することで高い周波数，例えば，数 MHz の f_r に対して数 GHz の周波数信号を生成することが可能となる．

PLL は単独の機能ブロックとして開発される場合でも雑音に弱い，脆弱な回路ブロックとして知られているが，この PLL を半導体上に集積する場合は，試作後に雑音抑圧できるような修正を行うことは容易ではないため，PLL を集積した半導体を開発する上ではいろいろな雑音要素に悩まされ続けることになる．例えば，PFC の不感帯[注6]，CHG の UP/DN 信号のミスマッチ，集積された素子のリーク電流[注7]，VCO でのジッタ，更には電源系からの雑音混入，そして，MOS トランジスタ[注8]を用いる場合に増大するフリッカ雑音などと，雑音源を挙げればきりがない．したがって，PLL の集積化は雑音抑圧との悪戦苦闘であり，今から振り返ってみると，雑音や環境変動の影響を受けやすいアナログ素子の関与をなるべく減らすことが一つの解決策だったと思われる．

2.　携帯電話用 PLL の集積化

1990 年代前半，周波数シンセサイザ用に集積化された PLL のいろいろな特性劣化をもたらす雑音要因を定量化して，どこを改善すればよいかということを実際の半導体製品を対象に評価して検討することを筆者は担当していた．この 1990 年代前半といえば携帯可能な移動電話が大変革を迎えた時期で，背広の内ポケットに収まるサイズの携帯電話の激しい開発競争の真っただ中であった．初期の携帯電話の伝送方式は FM ラジオと同じ音声を電波に重畳するアナログ方式だった．しかし，この時期に音声をディジタル信号に変換してから電波の搬送周波数に重畳する TDMA（time division multiple access）方式[注9]に変更された．これにより 1 チャネル当たりで使えるユーザ数を大きく増加できるようになり，その後の携帯電話の大普及につながった．

しかしながら，TDMA 方式の採用により様々な課題が生まれた．筆者が担当する PLL では，高速で周波数を切り替えるということが大きな課題となった．第 2 世代携帯電話[注10]規格[5]をもとに計算すると，周波数切り替え幅が 16 MHz のとき 1 ms 以下の切り替え時間が必要とのことだった．

一般に PLL の切り替え時間を短縮する方法は PLL の帰還ループの周波数帯域を広く設計する手法が採用されるが，従来の PLL をそのまま広い周波数帯域にするだけでは，帯域が広がった分だけ雑音が増加することになり，それだけで TDMA 方式に対応することは容易ではないことが分かっていた．

この携帯電話用の PLL を開発するときに，ディジタル演

(注 6)：不感帯　PFC などにおいて検出できない位相差のこと．
(注 7)：リーク電流　実際の回路要素ではないが，回路に寄生した電気経路で漏洩してしまう電流のこと．
(注 8)：MOS トランジスタ　金属（metal）と酸化物（oxide）と半導体（semiconductor）による層状構造をもつトランジスタ．現在の集積回路において主要なトランジスタ構造である．
(注 9)：時分割多重方式 TDMA 方式　同一チャネルを用いて，異なる送受信タイミングで伝送を行う方式．
(注 10)：第 2 世代携帯電話　アナログ方式の後継規格．ディジタル送受信をもつ携帯電話規格このと．

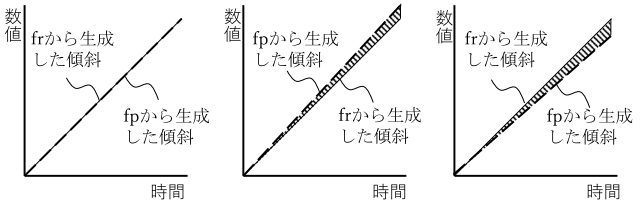


図 3　ディジタル演算を用いた位相比較のコンセプトを示す図
入力クロック（fr）と帰還クロック（fp）をもとにして二つの傾斜をもつ数値を発生させ，fr（実線）と fp（破線）の傾きを比較する．(a)fr と fp の傾きが一致した位相差なしの状態，(b)fr に対して fp の傾斜が大きいときには二つの直線で作る三角形の面積に相当する数値を出力する位相進みの状態，(c)fr に対して fp の傾斜が小さいときには二つの直線で作る三角形の面積に相当する数値を出力する位相遅れの状態を表す．

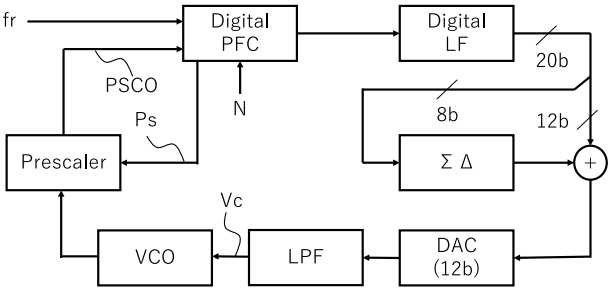


図 4　ディジタル位相比較用いた周波数シンセサイザ PLL の構成[7],[8]　ディジタル演算による PFC は fr と帰還信号を生成する Prescaler 出力（PSCO）が互いに非同期で動作するために制御する Ps を設けて同期非同期変換機構を含めた論理回路で構成した．次に LP をディジタルフィルタで設計し，DAC によりアナログ信号に変換したのち VCO を制御する．ここで，20 b 信号を 12 b と 8 b に分割し，下位 8 b を ΣΔ 変調を用いて上位の 12 b を補間する構成である．

算で PFC を行う方式を研究されていた慶応大学の中川先生のところを訪問して，位相比較演算方式[6]の勉強をさせて頂く機会があった．ディジタル演算の位相比較コンセプトを描くと図 3 のようになる．PFC に入力される fr と fp をもとにして二つの傾斜をもつ数値を発生させ，fr と fp の傾きが一致する図 3(a)のように帰還ループが働く構成である．もし図 3(b)に示すように fp の傾斜が大きいときには二つの直線で作る三角形の面積に相当する数値を DN 信号として出力して，反対に図 3(c)のように fp の傾斜が小さいときは二つの直線で作る三角形の面積に相当する数値を UP 信号として出力する．PFC の比較動作はブレッドボード上で検証されており，筆者がこのディジタル演算による位相比較演算方式を基本に第 2 世代携帯電話規格に合わせてパラメータを変更して，集積化する検討を担当することになった．

ディジタル演算による PFC は fr と fp の互いに非同期で動作する論理ブロックで構成されることになるので，特に 1 GHz 程度のマイクロ波帯の高周波信号を分周するプリスケーラ（prescaler）(注11)を制御する機構を含めた同期非同期変換を行う論理回路で構成した．図 4 に分周数 N が数値で入力されてディジタル的に位相比較する周波数シンセサイザのブロック構成[7],[8]を示す．ディジタル演算による PFC の出力はディジタルフィルタとして構成したディジタル LF に入力され，DAC によりアナログ信号に変換したのち VCO を制御する．このディジタル演算を用いた PLL において残された課題は VCO の制御電圧を与える V_c を生成するために 20 ビットのディジタル・アナログ変換器（DAC）(注12)を集積することだった．アナログ素子精度の限界と集積できるチップ面積の制限があり，せいぜい 12 ビット DAC までしか集積できないことが制約事項であった．そこで 20 ビットを上位 12 ビットと下位 8 ビットに分割し，下位 8 ビットは ΣΔ 変調器(注13)により 1 ビットの信号に変換して上位 12 ビットに加算することで不足する周波数分解能を補正する構成を用いた．

この補正のための ΣΔ 変調器はアナログ・ディジタル変換器（ADC）(注14)で採用されていた方式であり，サンプルレートを高く設定することで ADC から発生する量子化雑音を比較的高い周波数に拡散させることができ，所定の帯域での量子化雑音の寄与度を下げることができる技術である．以前，この ΣΔ 変調器の一種である補間型 ADC[9]を試作したことがあり，同じ考え方で PLL の帰還ループ内に ΣΔ 変調による補間手法を採用してみた．高い周波数に拡散した量子化雑音の PLL 帰還ループでの影響を計算し，DAC と VCO 間に低次数の LPF を設けることで雑音の増加を抑える構成とした．ここで用いた DAC は PLL のループ内にあるため単調増加性を確保できるように電流セルマトリックス型(注15)を採用した．

以上述べた方式を集積した評価結果[8]は周波数切り替え幅が 16 MHz のとき 1 ms 以下の切り替え要求時間に対して 0.7 ms を達成することができ，特性面では目標を満足した．しかしながら，試作したチップの面積が 5 mm×5 mm を超え，BiCMOS(注16)プロセスを用いた製品としてはかなり大きなものとなってしまい，結果しては量産への移行は行われなかった．

(注 11)：プリスケーラ　　分周器の 1 種類で，特に 1 GHz を超える高い周波数を分周する回路のこと．

(注 12)：ディジタル・アナログ変換器（DAC）　　ディジタルで表された数値を入力し，それに対応する振幅となる連続信号（アナログ）に変換する機能ブロック．

(注 13)：ΣΔ 変調器　　入力と出力を差分した誤差を積分し，その積分結果により出力の値を更新する方式の帰還ループのこと．

(注 14)：アナログ・ディジタル変換器（ADC）　　連続信号（アナログ）を入力し，それに対応するディジタルで表された数値に変換する機能ブロック．

(注 15)：電流セルマトリックス型　　小さな電流源の電流セルを格子状に配置した DAC の方式．面積が大きくなる課題があるが単調増加性が確保できる．

(注 16)：BiCMOS　　バイポーラトランジスタと MOS トランジスタを同一チップ上に集積した半導体のこと．

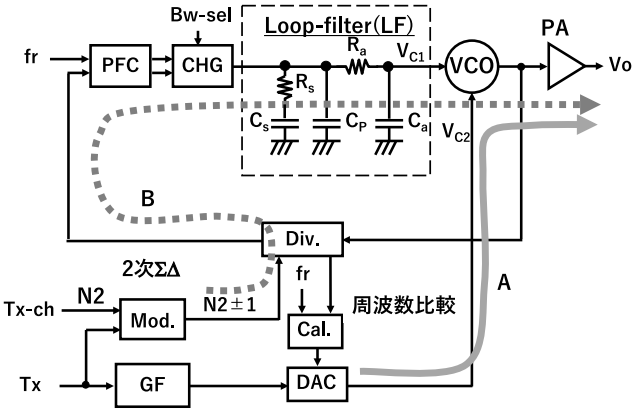


図 5　2 ポイント変調 PLL 回路[10]　　従来の PLL と同一構成だが，送信データ（Tx）をガウスフィルタと DAC を介して VCO に入力する経路（A）と，送信チャンネル（Tx-ch）から DIV に入力され，DIV の分周数を変調する経路（B）を設けている方法で GFSK（Gaussian filtered shift keying）と呼ばれる Bluetooth で用いられる変調信号を生成する．

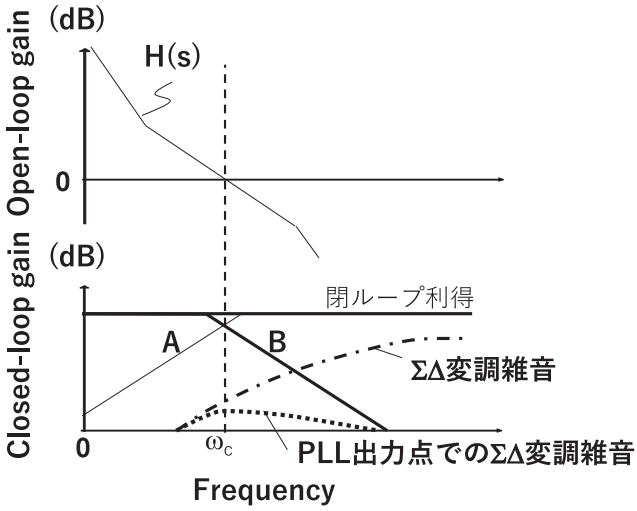


図 6　周波数軸における開ループ利得，閉ループ利得と ΣΔ 変調により発生する雑音の関係　　二つの経路に分けて変調するツーポイント変調を用いることにより，二つの経路の利得を一致するように設定することで広帯域の変調波形が得られる．ここで，ΣΔ 変調器により発生する雑音は PLL の周波数特性で抑圧される．

3.　帰還ループ内に ΔΣ 変調を適用した PLL の集積化

その後，ほかの製品仕様の PLL の集積化を担当していたが，あるとき，新人時代からアナログ・ディジタル集積回路の基本を丁寧に指導して頂いた事業部の方から，スプレッドスペクトラムクロック発生(注17)回路を集積化する必要があるが，その構成方法についての課題があるので困っているとの相談を受けた．スプレッドスペクトラムクロック発生とは，徐々にクロック周波数を変化させることで，急しゅんなスペクトラムの発生を防ぎ，電子機器から発生する電磁障害（EMI : electromagnetic interference）を防止する手法のことである．

その解決が難しい理由とは，従来から使われているフラクショナル N 分数分周方式を DIV に適用して周波数を徐々に変化させる方式では，PLL のループ帯域内に DIV でのフラクショナル N 分数分周により発生した不要な周波数成分が生成されてしまうためということだった．一般に DIV の分周数 N は整数であることが多いが，フラクショナル N 分数とは分数値，つまり，小数点以下の値で分周数を与える方式のことである．

筆者は，この時期，Bluetooth(注18)と呼ばれる近距離無線規格通信用 IC[10]を開発しており，ツーポイント変調方式の検討を行っていた．図 5 にツーポイント変調の構成を示す．PFC，CHG，LF，VCO，及び，DIV は従来の PLL と同一構成だが，送信データ（Tx）をガウスフィルタと DAC を介して VCO に入力する経路（A）と，送信チャネル（Tx-ch）から DIV に入力され，DIV の分周数を変調する経路（B）を設けている．（A）で示した経路は VCO に直接変調信号を与えることで GFSK（Gaussian filtered shift keying）と呼ばれる Bluetooth で用いられる変調信号を生成する．一方，（B）で示した経路は，経路（A）の伝達関数が低域遮断特性をもつことで失われた低い周波数成分を補正する機能をもつ．経路（A）と経路（B）を PLL の閉ループ上で合成すると GFSK 変調が行える構成で，二つの変調箇所があることからツーポイント変調と呼ばれている．ここで PLL のループ帯域により DIV の分周数を変動させたときに生ずる雑音成分を抑圧できるように構成することが重要であり，経路（B）の DIV の分周数を更新するブロックとして ΣΔ 変調器を設けて，フラクショナル N 分周(注19)と等価な機能を実現できるようにした．なお，二つの経路に分けて変調するツーポイント変調を採用したことで，DAC は 5 ビット相当[11]で十分であり，チップ面積の増加は最小にとどめることができた．ここで ΣΔ 変調器を設けたことによる雑音への影響を図 6 に示す．周波数軸における開ループ利得，閉ループ利得に対して ΣΔ 変調器により発生する雑音と PLL で抑圧された ΣΔ 変調雑音を示すと，PLL ループ帯域（ω_c）よりも高い周波数では ΣΔ 変調雑音は PLL がもつフィルタ特性により低減される．そこで PLL のループ帯域（ω_c）を十分低く設定することで ΣΔ 変調雑音を低減できるように構成した．ここで ΣΔ 変調器の次数が重要なパラメータである．簡単な一次

(注 17)：スプレッドスペクトラムクロック発生　　徐々にクロック周波数を変化させることで，急しゅんなスペクトラムの発生を防ぎ，電子機器から発生する電磁障害を防止する手法のこと．

(注 18)：Bluetooth　　スマートフォンなどに搭載されている近距離無線規格通信方式．

(注 19)：フラクショナル N 分周　　分周器は整数であるが，等価的に非整数の分周数も設定できる分周方式のこと．

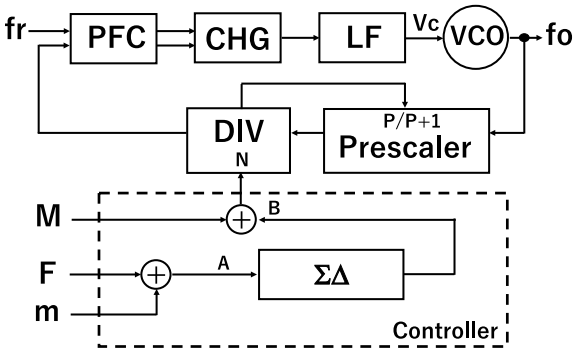


図 7　スプレッドスペクトラムクロック発生用 PLL の構成　　上部はよく知られている PLL の構成で，PFC，CHG，LP，VCO，および DIV から構成されている．DIV は図 4 に示す高周波信号を分周するプリスケーラとで任意の分周数（N）となるように制御する．この N の値は分周数制御回路（Controller）から与えられる構成である．

構成を用いると ΣΔ 変調器は繰り返しパターンが出力され，帯域内の余分な周波数，所謂，スプリアスが出現する．そのため二次以上の次数をもつ ΣΔ 変調器を用いた．

次に，図 7 にスプレッドスペクトラムクロック発生回路の構成図[12]を示す．図 7 の上部に描かれているブロック構成はよく知られている PLL と同じ PFC，CHG，LF，VCO，及び，高周波信号を分周するプリスケーラと組み合わせることで任意の分周数（N）となる DIV から構成されている．この N の値は分周数制御回路（Controller）から与えられる．ここで Controller には N の整数部分にあたる M と小数点以下の部分に相当する F と，三角波に相当する数値 m が入力される．次に小数点以下と三角波に相当する数値を加算した $F+m$ が ΣΔ 変調器に入力される．更に ΣΔ 変調器の出力 B は整数に変換されるので，N の整数部分にあたる M と加算されたのち，DIV の分周数として設定される．

図 7 の構成を用いて SATA[注20]規格[13]の 30 kHz の三角波形状の周波数変化を生成するように分周数（N）を制御し，EMI の抑圧レベルを 7 dB 以上低減できるスプレッドスペクトラムが得られる．このスプレッドスペクトラム変調方式を用いることで高速伝送を行う情報機器の実装が簡素化できる．ここで，図 7 の方式は図 5 のツーポイント変調とは異なり，帰還経路の DIV の分周数を制御することだけで三角波状の周波数変調を行うため PLL のループ帯域（ω_c）を三角波周期の 10 倍以上となる 300 kHz に設定する必要があり，ΣΔ 変調器からの雑音拡散に対してはより厳しい条件であった．

2000 年代になると計算機によるシミュレーション環境が大幅に改善されていたこともあり，PLL 構成の雑音に対するモデル化をしっかり行えれば精度よく PLL から出力されるスプレッドスペクトラムの振る舞いを検証することができた．その結果，三次の ΣΔ 変調器を用いることで，PLL から出力されるクロックのジッタによる劣化を SATA 規格内に収めつつ，高精度な三角波変調が行えた．試作チップでは約 10 dB の EMI 抑圧効果を確認することができた．このチップにおける PLL 部の専有面積は 0.4（mm^2）と小さく，製品として出荷できた．

最後に PLL とは異なる用途に ΣΔ 変調器を適用した話をする．前述したスプレッドスペクトラム生成回路の開発からしばらく経ったときに，MEMS（micro electromechanical systems）[注21]を用いた振動センサから振動情報を取り出すための制御ループにおいて，振動を検知すべき帯域内に雑音が出てきてしまうという課題の相談を受けた．このとき，MEMS は機械振動を用いる機能ブロックであるので，PLL の VCO と等価な働きをするはずである．そこで帰還ループに ΣΔ 変調器を挿入することで問題となる雑音成分を帯域外に拡散させる方法が有効かもしれないと考え，ΣΔ 変調器の挿入で問題の雑音抑圧の可能性があることを担当者に伝えた．その後，複数の ΣΔ 変調方式を試してもらい，最終的には二次帯域抑圧型 ΣΔ 変調器[14]を用いることで所定の仕様内に収まることが確認できた．

4. ま と め

2，3 章で説明したように筆者の技術の原点は PLL をはじめとした帰還ループ内に ΣΔ 変調器を挿入して所望の特性と雑音拡散とのバランスをとって集積化したことである．従来から積分要素をもつ非線形な帰還ループに周期的な擾乱を与えて精度改善をするディザ[注22][15]という手法が知られていたが，周期性の擾乱成分を帰還ループの外側で抑圧する必要があった．これまで述べたように帰還ループ内の雑音拡散に関する精緻な検討を行うことで，ΣΔ 変調器を用いても帰還ループがもつフィルタ特性を活かすことで雑音を抑圧することができる．したがって，PLL などの帰還ループのモデル化と，そのループ構成に基づいた雑音解析が技術の原点であったのだと思う．

文　献

(1) B. Razavi, Monolithic Phase-locked Loops and Clock Recovery Circuits Theory and Design, Wiley-IEEE Press, New York, 1996.
(2) T. Norimatsu, K. Kogo, T. Komori, N. Kohmu, F. Yuki, and T. Kawamoto, “A 100-Gbps 4-lane transceiver for 47-dB loss copper cable in 28-nm CMOS,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 67, no. 10, pp. 3433-3443, Oct. 2020.
(3) M. Kokubo, Y. Shibahara, H. Aoki, and C. Hwang, “Low supply voltage and low-power 1-GHz PLL frequency synthesizer for mobile terminals,” IEICE Trans. Electron., vol. E86-

(注 20)：SATA　　Serial-ATA の略称．コンピュータとハードディスクや光学ドライブなどの記憶装置を接続するインタフェース規格．

(注 21)：MEMS　　機械要素部品，センサ，アクチュエータ，電子回路を一つのシリコン基板，ガラス基板，有機材料などの上に微細加工技術によって集積化したデバイスのこと．

(注 22)：ディザ　　積分要素をもつ非線形な帰還ループに周期的な擾乱を与えて精度改善をする手法のこと．

C, no. 1, pp. 71-78, Jan. 2003.
(4) T. Yamawaki, M. Kokubo, K. Irie, H. Matsui, K. Hori, T. Endou, H. Hagisawa, T. Furuya, Y. Shimizu, M. Katagishi, and J.R. Hildersley, "A 2.7-V GSM RF transceiver IC," IEEE J. Solid-State Circuits, vol. 32, no. 12, pp. 2089-2096, Dec. 1997.
(5) (一社)電波産業会，標準規格　RCR-STD 27, 1991.
(6) A. Kajiwara and M. Nakagawa, "A new PLL frequency synthesizer with high switching speed," IEEE Trans. Veh. Technol., vol. 41, no. 4, pp. 407-413, Nov. 1992.
(7) 小久保優，伊藤隆康，田崎祐一，武井宣幸，"数値位相比較を用いた高速収束周波数シンセサイザ LSI，"信学技報，CAS95-50, ICD95-123, Sept. 1995.
(8) M. Kokubo, K. Hori, T. Ito, Y. Tazaki, and N. Takei, "A fast-frequency-switching PLL synthesizer LSI with a numerical phase comparator," Proc. ISSCC '95, pp. 260-261, 1995.
(9) K. Yamakido, M. Kokubo, T. Kozaki, S. Nishita, T. Nishihara, N. Miyake, and K. Ohwada, "A subscriber digital signal processor LSI for PCM applications," IEEE J. Solid-State Circuits, vol. 23, no. 3, pp. 836-842, June 1988.
(10) M. Kokubo, T. Oshima, K. Yamamoto, K. Takayasu, Y. Ezumi, and S. Aizawa, "A GFSK transmitter architecture for a Bluetooth RF-IC, featuring a variable-loop-bandwidth phase-locked loop modulator," IEICE Trans. Electron., vol. E88-C, no. 3, pp. 385-394, March 2005.
(11) M. Kokubo, M. Shida, T. Ishikawa, H. Sonoda, K. Yamamoto, T. Matsuura, M. Matsuoka, T. Endo, T. Kobayashi, K. Oosaki, T. Henmi, J. Kudoh, and H. Miyagawa, "A 2.4 GHz RF transceiver with digital channel-selection filter for Bluetooth," 2002 ISSCC Dig. Tech. Papers, vol. 1, pp. 94-95, Feb. 2002.
(12) M. Kokubo, T. Kawamoto, T. Oshima, T. Noto, M. Suzuki, S. Suzuki, T. Hayasaka, T. Takahashi, and J. Kasai, "Spread-spectrum clock generator for serial ATA with multi-bit ΣΔ modulator-controlled fractional PLL," IEICE Trans. Electron., vol. E89-C, no. 11, pp. 1682-1688, Nov. 2006.
(13) Serial ATA Workgroup, "SATA : High speed serialized AT attachment," Rev. 1, Aug. 2001.
(14) Y. Furubayashi, T. Oshima, T. Yamawaki, K. Watanabe, K. Mori, N. Mori, A. Matsumoto, Y. Kamada, A. Isobe, and T. Sekiguchi, "A 22-ng/$\sqrt{}$ Hz 17-mW capacitive MEMS accelerometer with electrically separated mass structure and digital noise-reduction techniques," IEEE J. Solid-State Circuits, vol. 55, no. 9, pp. 2539-2552, Sept. 2020.
(15) G. Zames and N. Shneydor, "Dither in nonlinear systems," IEEE Trans. Autom. Control, vol. 21, no. 5, pp. 660-667, Oct. 1977.

(幹事団提案，2022 年 5 月 30 日受付，2022 年 6 月 27 日再受付)

小久保優（正員）

昭和 56 千葉大・工・電気卒．同年(株)日立製作所入社．以来，アナログ・デジタル集積回路の開発，特に電子交換機，電話加入者線伝送回路，無線通信，及び，高速伝送用の集積回路研究に従事．平成 30 同社定年退職，現在は同社シニア所員．博士（工学）．

技術の原点

エネルギー効率を追求するコンピューティング

Computing in pursuit of energy efficiency

宇佐美公良 Kimiyoshi USAMI

アブストラクト　世界最初のコンピュータとされるENIACの誕生から僅か70年．コンピュータは，人間の囲碁の世界チャンピオンに勝利するレベルまで到達した．その一方で，コンピュータにはまだまだ人間の脳に大きく水をあけられている点がある．その一つが，エネルギー効率である．本稿では，エネルギー効率という切り口でコンピュータが辿ってきた道を明らかにし，現在の課題と取り組みについて述べる．更に，エネルギー効率を向上させるアプロキシメート・コンピューティングという手法について述べ，筆者の研究室での研究事例も合わせて紹介する．

キーワード　エネルギー効率，消費エネルギー，アプロキシメート・コンピューティング，MRAM

Abstract　Abstract：Only 70 years after the birth of the world's first computer ENIAC, computer technologies have reached the level of defeating a professional human Go player. On the other hand, computers still have points that are significantly inferior to the human brain. One of them is "energy efficiency". In this paper, the path that computers have taken from the perspective of energy efficiency is clarified and current issues and research activities are described. In addition, approximate computing techniques to improve energy efficiency are discussed and research cases in my laboratory are also introduced.

Key words　Energy efficiency, Energy consumption, Approximate computing, MRAM

1. はじめに

人工知能AlphaGoがプロ棋士の世界チャンピオンに囲碁の対戦で勝利したというニュースは，それまでコンピュータに関心がなかった人々にまで，大きな衝撃を与えた．コンピュータはついに人間の頭脳を超えたという率直な驚きから，今後どのような職業が人工知能に取って替わられるかといった社会的な分析まで様々な報道がなされ，大きなブームとなった．人工知能の中でも，特にディープラーニングをはじめとする機械学習の技術で，目覚ましい進歩があったことが大きく寄与しており，コンピュータ技術の発展における画期的な出来事であった．

一方で，コンピュータの専門家の中には，これを別の角度から分析している人達がいた．AlphaGoのハードウェアは，CPUチップ1,920個とGPUチップ280個から構成され，30万Wという膨大な電力を消費した．これに対し，人間の脳のエネルギー消費は消費電力に換算すると約20Wである．コンピュータは人間の15,000倍ものエネルギーを消費してようやく勝利したという見方もでき，コンピュータと人間の脳の間には「エネルギー効率」という点で，まだまだ大きな開きがあるといえる．

もちろん，人工知能が実際に社会で使われる用途としては，（囲碁ではなく）むしろ，クルマの自動運転や，ドローンの制御，ソーシャルメディアでのAR（augmented reality）といった応用が考えられるが，これらは，電池駆動のチップで処理を実行する．「エネルギー効率」が重要となることは明らかである．

こういった背景を踏まえ，本稿では，コンピュータのエネルギー効率に焦点を合わせながら，これまでの技術が辿ってきた道に触れ，現状と課題を明らかにする．更に，エネルギー効率を上げるコンピューティング技術として，画像処理や機械学習の処理で効果を上げているアプロキシメート・コンピューティングについて，研究事例を交えて紹介する．

2. コンピュータのエネルギー効率

コンピュータはエネルギー効率の点で人間の脳に及ばないという話をしたが，そもそも，コンピュータの進歩の中でエネルギー効率は上がっているのだろうか．ひょっとして，エネルギー効率自体はあまり変わっていないか，若しくは下がっているのではないだろうか．これを調べ始めた途端，一つの疑問が頭をよぎった．コンピュータのエネルギー効率は，正式にはどうやって定義したらよいのだろうか．

先ほどのAlphaGoの例は割と分かりやすく，囲碁の対戦に勝利するという目的（ゴール）を達成するために消費したエネルギーの値，で定義できる．この値が小さいほどエネルギー効率が高い．これを一般化すると，エネルギー効率と

宇佐美公良　正員：フェロー　芝浦工業大学工学部情報工学科
E-mail　usami@shibaura-it.ac.jp
Kimiyoshi USAMI, Fellow (Shibaura Institute of Technology, 3-7-5 Toyosu, Koto-ku, Tokyo 135-8548, Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.57-65 2022年10月

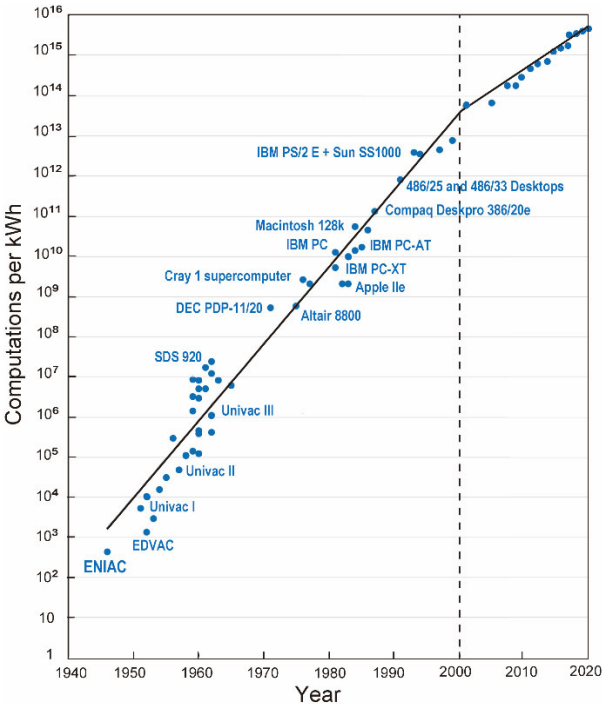


図1　汎用コンピュータのエネルギー効率の推移[1],[2]

は，「目的とする処理，結果を得るまでの時間，結果の品質」などの条件の下で，処理の実行により消費されるエネルギー，で定義できる．逆にいえば，上記の条件がきちんと設定できないと，エネルギー効率は正式には「比較」できない．AlphaGo では，目的とする処理が囲碁，もち時間 2 時間，結果の品質は相手に勝つレベル，というある程度はっきりとした条件の下での消費電力で，エネルギー効率を比較できた．

ところが，これまでのコンピュータの進歩を数字で表す場合，CPU（central processing unit）を中心とした汎用コンピュータが例に挙げられることが非常に多い．汎用となると，上で述べたような条件を明確に設定できないことも多いため，汎用コンピュータでは，

エネルギー効率＝計算量／消費エネルギー　　(1)

という指標が導入された[1]．同じ計算量で消費エネルギーが少なければ，式(1)の分母が小さくなり，エネルギー効率が高くなる．また，同じエネルギーで多くの計算をこなせれば，分子が大きくなりエネルギー効率は高くなる．式(1)に基づき，汎用コンピュータにおけるエネルギー効率の推移を示した結果が図 1 である[2]．縦軸には，エネルギー効率としてキロワット時あたりの計算量（computations）を取っている．

これにより分かるのが，年代とともにコンピュータのエネルギー効率は上がっているということである（決して下がってはいない）．1946 年の ENIAC から 2000 年前後まで，エネルギー効率は 1.6 年で 2 倍のペースで上がり続けており，クーメイ（Koomey）の法則と呼ばれる．このエネルギー効率の上昇は，主にコンピュータのハードウェア技術の進歩（真空管からトランジスタ，更に集積回路への進歩）に負うところが大きい．特に CPU が集積回路で作られるようになってからは，集積する素子の微細化が精力的に進められ，1 チップに搭載される素子の数が 3 年で 4 倍のペースで増加した（ムーア（Moore）の法則）．素子は小さくなればなるほど，動作速度が速くなり，消費電力[注1]が小さくなるというデナード（Dennard）のスケーリング則[3]の結果，式(1)の分子が増大し分母が減少するため，エネルギー効率は上昇の一途をたどった．

ところが，エネルギー効率の上昇は 2000 年前後を境に傾きが緩くなり，2.7 年で 2 倍というペースになる[2]．一体何が起こったのかというと，一つはデナードのスケーリング則の終焉，もう一つは CPU の電力問題に起因するマルチコアへの変更，である．デナードのスケーリング則によれば，MOS（metal oxide semiconductor）トランジスタは，微細化とともに電源電圧とトランジスタしきい値電圧が比例で縮小する．ところが，しきい値電圧を小さくするとリーク電流が著しく大きくなって消費電力が増大するため，しきい値電圧を下げることは困難となった．しきい値電圧を下げずに電源電圧を下げると動作速度が遅くなるので，結果的に電源電圧も下げられないという事態となり，2000 年代初頭にスケーリング則は終焉を迎えた．

一方，CPU の電力の壁は，インテル社の Pentium4 Prescott という CPU でクローズアップされた．この CPU は，クロック周波数 3.6 GHz で動作させたときの消費電力が 103 W であった．この電力がいかに大きいかは，調理用のホットプレートで CPU のチップとほぼ同じ面積の部分が，平均 10 W の電力を消費することからも想像できる．その 10 倍以上の電力を消費する CPU では，チップの発熱の問題が深刻であり，放熱や冷却対策に加え電力供給能力の点でも，実装が著しく困難になる．インテルは，上記のチップの後継機種として，クロック周波数を 4 GHz，5 GHz と上げて性能向上を達成していく機種を開発していたが，消費電力の増大に歯止めがかからず計画を断念する．その代わりに，マルチコアによる並列処理で性能向上を図る戦略に舵を切り，2006 年にデュアルコアの CPU を製品化した．AMD も，ほぼ同じ時期にマルチコアに方針転換している．

このように，CPU の世界では 2000 年代初頭に大きな変革が起こり，それ以降，マルチコアやコアごとのパワーマネージメント制御により，消費電力の低減と性能向上を図る戦略が取られるようになった．ただ，マルチコアでの性能向上は，並列化できる処理が処理全体の中でどれくらい含まれているかに依存し，必ずしもコア数に比例して性能が上がるわけではない．また，複数のコアを搭載するには微細化技術は必要であり，微細化に伴うリーク電力を抑えつつ，ダイナミック電力も低減する制御をしていかねばならない．結果として，式(1)の分子（＝計算量）が大きくなりにくく，分母

(注 1)：消費電力と消費エネルギーは異なる物理量であり，消費電力にその電力を消費する時間（例えば処理時間）をかけたものが消費エネルギーである．

（＝消費エネルギー）が小さくなりにくくなっており，エネルギー効率の上昇のペースが鈍っている．

エネルギー効率を上げていくには，今後，更に細かいローパワー・モードを用意し，それらの各モードへの出入りにかかる時間を短くすることが必要である．出入りにかかる時間を短くできれば，消費電力と遅延時間が最適なモードに，ギリギリまで留まることができるためである．

こういった手法とは別に，従来の汎用コンピュータのアーキテクチャを抜本的に見直し，性能，消費エネルギー，チップコストを最適化する領域特化アーキテクチャ（domain specific architecture, DSA）が注目されている．その代表例が，Google 社の tensor processing unit（TPU）である．機械学習に特化した DSA で，第 1 世代版ではディープラーニングの処理で中心となる行列演算用に，65,536 個（256×256）の積和演算回路とソフトウェア制御の大容量メモリが搭載されている．汎用ではなく「機械学習」という領域に特化することで，エネルギー効率のよいアーキテクチャが実現されている．

さて，ここまで述べてきたコンピュータは，汎用と領域特化の違いはあるにせよ，いずれも「正確に計算を行う機械」であった．この固定観念にメスを入れ，コンピュータに多少の計算間違いをあえて許すことで，消費エネルギーを格段に減らす手法がある．アプロキシメート・コンピューティング（approximate computing）と呼ばれるこの手法は，近年の研究で，画像処理や機械学習での処理で効果を発揮することが分かってきた．画像処理では，人間の視覚で認識できないレベルの正確な計算は必要ない．また，機械学習の処理では，学習過程での計算の正確さを多少下げても推論精度はさほど低下せず，消費エネルギーを低減できることが明らかになった．

このように，その処理で求められる「結果の品質」以上に，コンピュータで正確な計算を行っているのなら，それに費やされる消費エネルギーは無駄なので削ぎ落そう，というのがアプロキシメート・コンピューティングの狙いである．まぎれもなくエネルギー効率を追求する手法の範疇に入るが，アプロキシメート・コンピューティングでは，エネルギー効率を表す指標として式(1)はあまり使われない．式(1)はあくまで汎用コンピューティング向けの指標であり，ある程度用途を特定するアプロキシメート・コンピューティングでは，「要求品質を達成するために必要な消費エネルギー」が，エネルギー効率の指標となる．この消費エネルギーが小さいものほど，エネルギー効率が高い．

次章では，このアプロキシメート・コンピューティングの具体的な手法について紹介する．

3. アプロキシメート・コンピューティング

Approximate computing は，直訳すると近似計算であるが，日本語訳としての呼び名は定着していない．このため，本稿ではアプロキシメート・コンピューティングとカタカナで表記する．また，略語はかつて AC と記していたが，学会では近年 AxC と表記することが多くなり，本稿でもこれに倣う．

画像認識や音声認識，データマイニングといった分野では，処理の過程で生ずるある程度のエラー（誤り）に対して，「耐性」があることが知られていた．エラー耐性があるというこの性質は，その応用分野の潜在能力ともいえる．一方で，その分野といえども計算処理そのものは，計算を間違えることのない通常のコンピュータで行われ，莫大なエネルギーを消費していた．もし，エラー耐性という潜在能力が一度も使われることなく全てが済んでいるのなら，完璧な計算をするコンピュータは，必要以上の品質をもつ結果を計算していることになる．このギャップを消費エネルギーの削減に使えないだろうか．具体的にいうと，計算方式やコンピュータの中身を少し変えることで，僅かに計算を間違うが消費エネルギーが大幅に減るのなら，潜在能力としての「エラー耐性」を消費エネルギー削減に活かせるのではないか．

この視点に立ち，approximate computing という言葉を登場させた論文が，2010 年に米国パデュー大学の Kaushik Roy 教授の研究グループから発表された．この論文[4]では，機械学習の手法であるサポートベクターマシン（support vector machine, SVM）で分類を行うプロセッサを実際に設計し，種々の AxC 手法を適用している．特徴的なのは，SVM の分類における「結果の品質」と「エネルギー削減」のトレードオフを見極めた上で，行列計算の回数や計算のビット幅を減らす手法と，回路の過電圧スケーリング（voltage over scaling, VOS）という手法を適用した点である．こういった異なる設計レベルの AxC 手法を取り込んだ結果，分類精度の低下を招くことなく，消費エネルギーが 15～55% も減るという結果が報告された．分類精度の低下を 5% 許容すれば，消費エネルギーが 1/3 に減る場合もあることが示され，アプロキシメート・コンピューティングという技術が注目されるきっかけとなった．こういったハードウェアの領域だけでなく，プログラミング言語やコンパイラといったソフトウェアの領域で AxC を取り込む手法も提案され，エネルギー効率を高める技術としてアプロキシメート・コンピューティングが注目されるようになった．

3.1 主なアプロキシメート・コンピューティング手法

AxC の手法は極めて多岐にわたる[5]～[8]．本稿では，紙幅の都合もあり一部のみ紹介する．まず，AxC 手法を大まかに分類して全体を眺めると，表 1 のようになる．

3.1.1 精度スケーリング

ハードウェアを対象にしたアーキテクチャレベルの AxC 手法として，精度スケーリング（precision scaling）という手法がある．この手法では，演算するデータのビット幅を縮め，短いビット幅で演算させることで消費エネルギーを小さ

表1　主なアプロキシメート・コンピューティング手法

対象	レベル	手法
ハードウェア	アーキテクチャ	精度スケーリング*
		メモ化
	回路	不正確な演算回路
		過電圧スケーリング
ソフトウェア	アプリケーション	ループ・パーフォレーション
	プログラミング言語とコンパイラ	AxC 可能なデータをプログラマが指定できるよう言語拡張

* 精度スケーリングはソフトウェアでも提案されている

くする．例えば，IEEE 規格の単精度浮動小数点数の演算を行う場合，23 ビットの仮数部のうち下位 n ビットは演算の対象から外し，仮数部の上位（$23-n$）ビットだけで演算を行う．こうすることで，浮動小数点演算回路の消費電力が小さくなり演算時間も短くなるので，両者の積で決まる消費エネルギーが小さくなる．一方で，仮数部 23 ビット全てを使って計算する場合に比べ，計算精度が落ちる．この消費エネルギーと計算精度のトレードオフは，アプリケーションやデータセットごとに異なるため，上記の n の値を動的に変えて制御する．これに対応するハードウェアとしては，例えば，演算を行う際に下位 n ビットの演算回路部分はシャットダウンするとか，複数のデータの上位（$23-n$）ビットだけを集めて 1 語のデータとしてパッキングし並列処理する，といった方法がある[4]．前者では消費電力が削減され，後者では実行時間が短縮されるので，どちらも消費エネルギーの削減につながる．また，仮数部の上位（$23-n$）ビットを得る方法も，単純に下位 n ビットを切り捨てる方法から，最近値丸めにより（$23-n$）ビットの値を求める方法まで様々ある．

3.1.2　メモ化

アーキテクチャレベルの AxC 手法としてもう一つ主要な技術が，メモ化（memoization）である．メモ化は元々，ソフトウェアのプログラムを高速化する技術として考え出された．関数の計算に長い時間がかかる場合，一度計算したら関数の引数と計算の結果をテーブルに格納しておき，次に同じ引数の値で関数が呼び出されたら，計算は行わずにテーブルに格納されている値を再利用するという手法である．関数の計算にかかる時間に比べテーブルを参照する時間の方が短ければ，テーブルにヒットする限りプログラムの実行時間は短くなる．この方法をハードウェアに焼き直すと，二つの入力 A，B 及び出力 Y をもつ演算回路に対し，一度演算したら入力 A，B と演算結果 Y のデータをテーブルに格納して次からの演算に再利用する，という方法になる．演算で消費されるエネルギーよりもテーブル参照の消費エネルギーの方が小さければ，消費エネルギーは小さくなる．なお，格納されている A，B と異なる値のデータが入力された場合には，再利用は行われず，入力された値に対して演算が行われる．

この方法の弱点は，後の演算で A，B の値と全く同じ値が入力されない限り再利用が行われないため，再利用率を上げにくい点である．そこで，「ある程度」A，B の値に近いデータ A′，B′ が入力として与えられたら，テーブルに格納されている A，B の演算結果 Y を A′，B′ の演算結果として再利用してしまおう，という fuzzy memoization が提案された[9]．これはまさに，オリジナルのメモ化手法を AxC に取り込んだ手法といえる．入力データ A′，B′ がどの程度 A，B の値に近ければ再利用するのかが，計算精度と消費エネルギーに影響を及ぼす．「どの程度」を表す量が許容度であり，許容度が大きいと再利用率が上がるため消費エネルギーは小さくなるが，計算精度は低くなる．

上記の論文では，浮動小数点数 A，B に対して FPALU（floating-point arithmetic logic unit）で演算する場合を想定し，入力 A，B ともに仮数部の下位 n ビットを除く上位ビットのデータだけを使って，テーブルに格納する．したがって，この n が許容度を表すパラメータとなる．画像圧縮や音声認識などのプログラムに適用した結果，必要な結果品質を保った上で約 15% の消費エネルギー削減ができることが示された．

Fuzzy memoization の弱点は，許容度を大きくしていくと結果の品質が大きく低下する点であり，その低下の度合いもデータセットによって異なる．このため，最適な許容度の設定には手間がかかることになり，実際の適用では問題となる．これを解決する方法として，筆者の研究室では，fuzzy memoization でテーブルを参照して得られた結果に対し，簡略演算を施して補正する手法を提案した[10]．画像処理に実験適用した結果，許容度を大きくしていくと fuzzy memoization だけでは画質劣化の許容限界（PSNR が約 30 dB）を下回るのに対し，提案手法では画像によらず，許容度を大きくしていった場合の PSNR は 45 dB 付近（原画像との違いが視覚では認識できないレベル）で維持されることが分かった．高画質を維持した上で，消費エネルギーも最大 11% 削減するという結果が報告されている．

3.1.3　不正確な演算回路

AxC の研究が最も活発に行われてきた領域である．加算器や乗算器で，入力データによっては誤った演算結果を出すことを許容して回路を少し変更すると，回路規模が小さくなり，回路の遅延時間が短くなって消費エネルギーが減る．例えば，加算器では，基本構成要素である全加算器（full adder, FA）の回路を作る際に，実現する真理値表の一部を変更すると，論理は完全には正しくないが素子数の少ない回路で実現できて，消費エネルギーも小さい．このアプロキシメート FA 回路を，N ビット加算器の下位側のビットで使用し，上位側のビットでは従来の正確な FA 回路を使う．こうすれば，仮にアプロキシメート FA 回路で誤った計算結果を出しても，下位側のビットなので影響が小さい．N ビット加算器全体として，結果の品質をある程度保ったまま消費エネルギーを小さくできる．

ほかの方法としては，N ビット加算器を k 個のサブ加算

器に分割し，上位側のサブ加算器の間では桁上げ伝搬を行うが，下位側では桁上げ伝搬を行わないようにする方式が提案されている．桁上げ伝搬を行わなければ遅延時間が短くなり，消費エネルギーが小さくなる．桁上げ伝搬の抑止を下位側のビットで行っていること，また，桁上げ伝搬が生ずる入力データの組合せは全体の中でごく一部であることから，効果的なアプロキシメート加算器が実現できる．

乗算器での AxC も研究されており，部分積の加算を行う際に，下位側のビットでは加算を省略して全体の遅延時間を短くする．この方法により，結果品質をある程度保った上で，消費エネルギーを削減している．

3.1.4 過電圧スケーリング

電源電圧を下げる手法は，消費エネルギーの削減に非常に効果的である．これは，ディジタル回路の消費電力の大半を占めるダイナミック電力が，電源電圧の 2 乗に比例するためである．例えば，電源電圧を 20% 下げればダイナミック電力は 36% も削減される．一方，電源電圧を下げることの問題点は，回路の遅延時間が大きくなることである．このため，通常の電圧スケーリングではタイミングエラーを起こさないようにするため，クロック周波数も一緒に下げるか，若しくはエラーが出ない範囲で電圧を下げる．これに対し，「過電圧スケーリング」（VOS）では，クロック周波数を下げずに，電源電圧を更に低い値まで下げる．これにより消費電力は更に小さくなるが，回路のクリティカルパス（遅延時間が最も長い信号経路）の遅延時間が増大するためタイミングエラーが生じ，正しい計算結果が得られない場合が生ずる．ほかの AxC と同様，計算結果の品質と消費エネルギーをトレードする手法であるが，電源電圧を下げて発生するタイミングエラーは，その影響が及ぶ随所で問題を引き起こすことが多く，結果の品質を大きく低下させてしまう．これを避けるため，VOS ではエラーを検出し訂正する回路を追加することが多い．例えば，加算器であれば，桁上げ伝搬の経路がクリティカルパスになることが多いため，3.1.3 項で述べたサブ加算器に分割し，サブ加算器間を伝搬する桁上げをモニタしながらエラー検出と訂正を行う [4]．

3.1.5 ソフトウェアを対象にした AxC 手法

ソフトウェアを対象にした AxC として，ループ・パーフォレーション [11] という手法がある．この手法では，プログラム中のループを実行する際に，幾つかの反復を定期的にスキップする．結果的に計算量が減り，消費エネルギーを削減できる．計算精度と引き換えに消費エネルギーの削減が行われるが，スキップする反復の選び方によって精度の低下が大きく異なる．計算精度への影響や得られる利得を考慮しながら，スキップする反復を選ぶ技術が鍵を握る．

こういった手法に加え，既存のプログラミング言語の機能を拡張し，プログラム中のどのデータが AxC 可能かをプログラマが指定できるようにする試みがなされている．更に，プログラム中で AxC 可能と指定されたデータに対して，演算を行う際の精度スケーリングや，次項で紹介するアプロキシメート・ストレージへの割り付けを行うコンパイラ手法 [12] が提案されている．

3.2 アプロキシメート・ストレージ（AxS）

前述した手法はいずれも，エネルギー効率を向上させる「計算処理」手法であったが，コンピューティングを行うにはデータの「記憶」が必要である．DRAM や SRAM といった記憶回路は，記憶容量の増大とともに消費エネルギーが大きくなっているため，ここにもアプロキシメートの手法が適用できないだろうか．この発想で生まれた技術がアプロキシメート・ストレージ（approximate storage, AxS）である．大きくはアプロキシメート・コンピューティングの範疇に入るが，計算手法ではないので区別した呼び方がなされる．本節では，DRAM と SRAM に対する AxS 手法を簡単に述べた後，不揮発性メモリの AxS 手法として，筆者の研究室で行っている研究の事例を紹介する．

3.2.1 DRAM と SRAM に対する AxS 手法

DRAM で消費されるエネルギーのうち，リフレッシュ動作によるエネルギーが大きいことはよく知られている．リフレッシュレートを下げれば消費エネルギーは小さくなるが，データを保持できないビットが増える．このトレードオフの下で考え出されたのが，DRAM を N 個のセグメントに分け，各セグメントでリフレッシュレートを変えるという方式 [13] である．例えば，四つのセグメント（S1〜S4）に分ける場合，リフレッシュレートを S1 では最も高くし，S4 では最も低くする．画像データを保存する場合には，画素値の上位ビットは S1，中位ビットを S2 と S3，下位ビットは S4 に保存することで，上位ビットでの画質低下を抑えながら消費エネルギーを低減できる．この手法の有効性をシミュレーションで評価した結果，画質を維持しながらリフレッシュの電力を 48% 低減できたという報告がなされている．

一方，SRAM の消費エネルギーで深刻なのはリークエネルギーであり，これを低減するには電源電圧を下げるのが効果的である．電圧を下げるとデータ保持が難しくなりビットエラー率（BER）が増大するので，BER とリークエネルギーのトレードオフを見ながら画像処理に適用した AxS 手法 [14] が提案されている．

3.2.2 不揮発性メモリの AxS 手法

現在，様々な不揮発性メモリの研究開発が各所で進められているが，本稿では，MRAM（magnetic random access memory）に対する AxS 手法を紹介する．MRAM は，記憶素子に MTJ（magnetic tunnel junction）という磁気素子を使う不揮発性メモリであり，電源を切ればリーク電流がカットでき，しかも記憶データが消失しない．このため，SRAM でのリークエネルギーや，DRAM でのリフレッシュエネルギーのような問題は起こらない．こういった利点から，

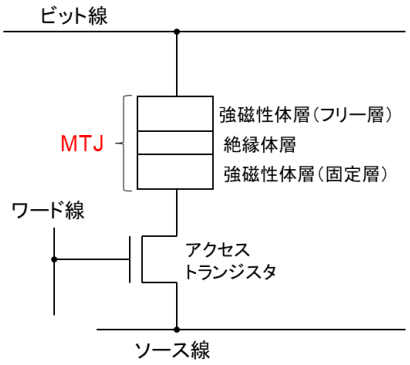


図 2　MRAM のメモリセルの構造

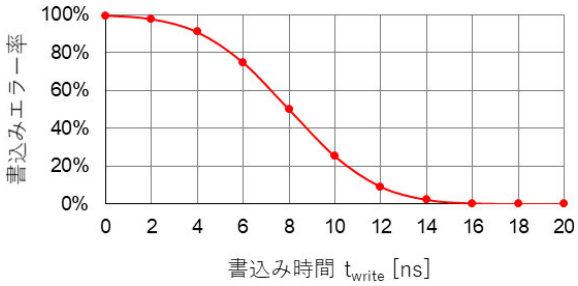


図 3　MTJ への書込み時間と書込みエラー率の関係

MRAM は単体としてだけでなく，エッジ・コンピューティング向け SoC（system on a chip）のオンチップメモリとしての期待も大きい．その場合，消費エネルギーの点で問題となるのが，MTJ への書込み時に大きなエネルギーを消費するという点である．MRAM のメモリセルの構造は図 2 のようになっており，書込み時にはスイッチであるアクセストランジスタをオンし，ビット線から MTJ を通してソース線に（またはその逆向きに）電流を流すことで，MTJ への書込みを行う．MTJ は，極薄の絶縁体層を 2 枚の強磁性体層（フリー層と固定層と呼ぶ）で挟んだ構造になっており，フリー層の磁化方向と固定層の磁化方向が互いに異なれば MTJ が高抵抗状態になり，方向が同じであれば低抵抗状態になる．これら二つの抵抗状態を論理値 '1' と '0' に対応させて，データが記憶される．書込み時には MTJ に電流を流しフリー層の磁化を反転させるが，その際に，ある一定の電流（I_{write}）を電圧（V_{write}）のもとで，ある一定の時間（t_{write}）をかけて流す必要がある．通常，V_{write} は電源電圧 V_{DD} に設定し，I_{write} は MTJ の物性やサイズから決まる必要最小値以上の電流になるように設定する．また，t_{write} は，目標とする書込みエラー率以下になるよう十分に長い時間を取る．

書込み時の消費エネルギーは I_{write}，V_{write}，t_{write} の積で決まるので，エネルギーを削減するにはこれらのうちのどれかを小さくしなければならない．MRAM を使う側からすると，書込み時間 t_{write} を変える（書込みのクロックサイクル数を変える）やり方が最も設計コストが小さいので，t_{write} に着目する．t_{write} を短くすると消費エネルギーは小さくなるが，その反面，書込みエラー率が増大する．しかし，t_{write} を短くした場合のエラー率の増え方は，実は線形ではない．MTJ の製造時のばらつきによって，短い t_{write} で正しく書き込めるものもあれば，t_{write} を長くしないと書き込めない MTJ が存在するためである．こういった振る舞いに対して，確率分布を使った様々なモデルが提案されているが，その中でもよく使われる正規分布のモデルで考えると，エラー率は書込み時間 t_{write} に対して，図 3 のような振る舞いをする．これは，例として t_{write} の平均値が 8 ns，標準偏差が 3 ns のときの t_{write} とエラー率の関係である．

目標とするエラー率を例えば 0.004% 以下とすると，t_{write} ＝20 ns 以上であれば満たせるので，アプロキシメートでない通常の設計では，この t_{write} の値（20 ns）を書込み時間として設定する(注2)．一方，グラフから分かるように，書込み時間を 12 ns に短くしても，エラー率は約 9% であり，90% 以上の MTJ は正しく書き込める．また，書込み時間が 60% になるので，消費エネルギーも 60% に減る．この特性は，エラー率と引き換えに消費エネルギーを削減する AxS として使えることを意味する．

この視点に立ち，筆者の研究室では，画像をターゲットにした手法と，機械学習に応用する手法を研究している．これらの研究事例を簡単に紹介する．

(1)　画像をターゲットにした AxS 手法

MRAM の書込み時間と引き換えに消費エネルギーを削減するといっても，画像の場合，書込み時間を短くするとどれくらい画質に影響が出るのだろうか．これを調べるため，画像データを MRAM に格納することを想定し，Python と OpenCV を用いたシミュレーションで，格納後の画像がどのように変化するかを確かめた．結果を図 4 に示す．

書込み時間 t_{write}＝20 ns では，視覚では画質劣化はほとんど確認できないが，t_{write}＝15 ns にすると，エラー率の低下が約 1% であるにもかかわらず，肩の部分や帽子の表面にポツポツとノイズ（ごま塩ノイズ）が発生しているのが確認できる．更に t_{write} を短くしていくと，ノイズが著しく目立つようになる．このように，画像に対して人間の目はある程度エラー耐性があるといっても，単純に書込み時間を短くしていく手法では大きなエネルギー削減効果は期待できず，何らかの工夫が必要である．

この事実を踏まえ，筆者の研究室では，MRAM に書き込む際に画像データの上位ビットと下位ビットで書込み時間の長さを変える AxS 手法を提案した(15)．すなわち，上位ビットは長い時間をかけて書き込み，下位ビットは短い時間で書き込むことにより，書込みエラーの影響を最小に留めつつ消費エネルギーを削減する．前節で述べた精度スケーリングの考え方を応用したものであるが，実際に適用する際には，上位ビットと下位ビットに分割する際の分割位置（bit split position, BSP）や，それぞれの書込み時間の長さが，画質とエ

(注 2)：更に低い書込みエラー率が必要であれば，書込み時間をもっと長くするとか，ECC（error-correcting code）を導入するといった手法をとる．

図 4　書込み時間を短くした場合の画像

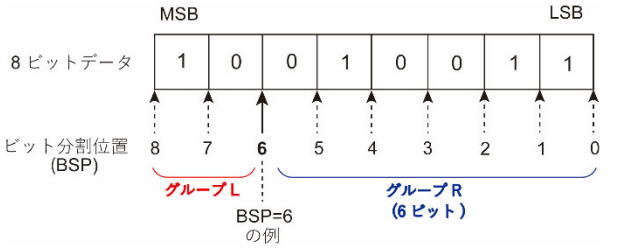
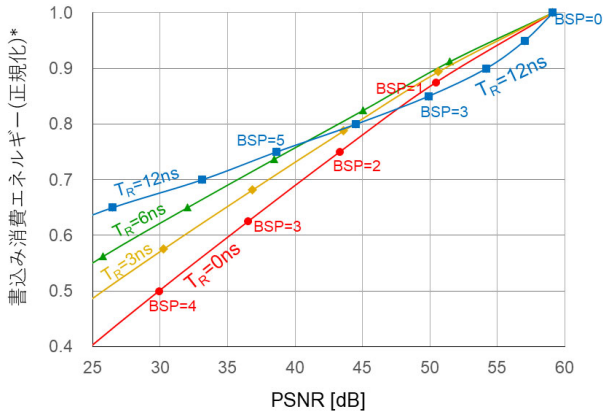


図 5　画像データに対するビット分割位置 BSP



*AxSを使わずに書込む場合の消費エネルギーで正規化

図 6　提案の AxS 手法での PSNR と書込みエネルギーの関係

図 7　提案の AxS 手法を使って書込みを行った結果の画像

ネルギー削減効果に大きく影響する．そこで，各 8 ビットの RGB チャネルをもつ画像データに対し，一つのチャネルにおけるビットのグループ分割を図 5 のように行った．この図は，上位ビットとして 2 ビット，下位ビットとして 6 ビットで分割した例であり，分割位置 BSP の値は，下位ビットのビット数で表すと定義する．また，上位ビットに含まれるビットをグループ L（left），下位ビットに含まれるビットをグループ R（right）と呼ぶ．研究室では，図 3 に示した書込みエラー率の分布を使用し，シミュレーションを用いて MRAM への書込みを模擬することにより，画質と消費エネルギーを求めた．

まず，上位ビットの書込み時間 T_L としては 20 ns から少しでも短くすると画質劣化に大きく影響することが分かったため，T_L＝20 ns で固定した．あとは，下位ビットの書込み時間 T_R と BSP の組合せにより画質と消費エネルギーが変化する．画質の評価指標として PSNR（peak signal-to-noise ratio）を用いるが，PSNR の値が小さくなるにつれ画質は悪くなる．提案した AxS 手法での PSNR と書込み消費エネルギーの関係をプロットしたものを，図 6 に示す．

許容限界とされる PSNR＝30 dB の画質でよいなら，T_R＝0 ns で BSP＝4 が最も消費エネルギーを小さくできる．なお，T_R＝0 ns なので，下位 4 ビットは書き込まないのと同じであり（切り捨て），書込みの消費エネルギーが 50% に減る．また，PSNR＝40 dB の画質が必要な場合でも，T_R＝0 ns，BSP＝2（下位 2 ビットは切り捨て）で到達でき，消費エネルギーは 75% に減る．ところが，PSNR＝50 dB 以上の高画質が必要な場合には，T_R＝0 ns（下位ビットの切り捨て）よりも，T_R＝12 ns の書込みを下位ビットに行う方がエネルギーを小さくできる．これは，PSNR＝50 dB 以上を達成するには，下位ビット切り捨てでは BSP＝1（切り捨てできるのは下位 1 ビットのみ）となってしまうためである．下位 3 ビットに対して T_R＝12 ns の短い書込みを行う方法（BSP＝3）により，消費エネルギーは 85% に減る．この AxS 手法を使って MRAM に書込みを行った結果の画像を図 7 に示す．

PSNR＝30 dB では，肩から腕にかけての部分や頬の部分に，縦の線のノイズが僅かに見られる．一方，PSNR＝50 dB の画像ではノイズはほとんど確認できない．このように，要求される画質のレベルによって，消費エネルギーを削減するための最適方法は異なり，下位ビットは書き込まない方がよい場合と，下位ビットに短時間の書込みを行った方が

よい場合があることが分かった．このように，一般的にアプロキシメート・コンピューティングで目安とされるPSNR＝30 dBの画質を維持した状態で，提案のAxS手法はMRAMの書込みエネルギーを50%に削減できることが明らかになった．なお，画像による依存性を調べるため，ほかの6種類の画像でも評価したところ，BSPやT_Rを変えたときのPSNRの値は，上記のLena画像とほぼ同じ値で推移することが分かり，提案手法の安定性が裏付けられた．

実際にこの手法を適用する際には，メモリの実装方法を考える必要がある．画質としてPSNRが30 dBまたは40 dBが要求されるのなら，下位ビットは書き込まなくてよいので，BSPの上位ビットだけをMRAMに格納すればよい．一方，PSNRが50 dBの高画質が求められる場合には，二つのセグメントからなるメモリで構成し，それぞれ上位ビットと下位ビットのデータを格納するようにして，セグメントごとに書込み時間を変えるようにすれば実現できる．

(2) 機械学習をターゲットにしたAxS手法

上記のAxS手法は，機械学習への応用でも効果を発揮する[16]．IoTの発展に伴い，スマートフォンなどエッジ端末におけるディープラーニングの採用が進むと考えられるが，その処理データを格納するメモリとしてMRAMが注目されている．この処理はディープニューラルネットワーク（DNN）を使った学習と推論から構成され，学習タスクをクラウド上で実行し，得られたDNNの重みやバイアスデータをエッジ端末に転送して推論を行う方法が主流である．エッジ側で推論を行う際に，送られてきたDNNの重みやバイアスデータを格納するメモリとして，電気を切ってもデータが消失せず高速読出しが可能なMRAMは大きな魅力がある．一方で，エッジ側で取得したセンサデータをクラウドに転送し，クラウドで学習したデータをエッジ側に戻すというやり方は，機械学習が高度化するにつれデータ量が増えていくと，通信コストの著しい増大を招く．また，エッジ側で取得された様々なデータがクラウドにアップロードされるため，セキュリティの点からもリスクが増す．こういった課題を踏まえ，エッジ側でも学習タスクを実行する「オンチップ学習」に関する研究が進められている．

オンチップ学習では，学習タスクを実行する際に，誤差逆伝搬などの処理によってエッジ側で重みとバイアスのデータが頻繁に更新される．このため，それらのデータを格納するメモリに対し，書込み動作の頻度が増える．ところが，MRAMは書込みの消費エネルギーが大きいため，これを低減する工夫が求められる．筆者の研究室では，DNNの学習タスクに焦点を合わせ，重みとバイアスデータをエネルギー効率よくMRAMに書込むAxS手法を提案した[16]．

まず，MRAMに格納するデータであるが，多くのDNNフレームワークで使われている浮動小数点数の表現形式の中で，データ量削減とDNNの精度維持を図ったBF16（Brain Float 16）浮動小数点数形式のデータ（図8）を対象とした．提案するAxSでは，BF16の仮数部7ビットに対し，上位ビットと下位ビットで書込み時間を変える．符号部と指数部のビットは，書込み時間を短くするとマイナスの影響が甚大なので，書込み時間の短縮は行わない．この手法の有効性を確かめる実験では，多層パーセプトロン，CNN，MobileNetV2という3種類のネットワークを対象に，シミュレーションを行った．評価に使用したデータセットも含め，表2に記す．

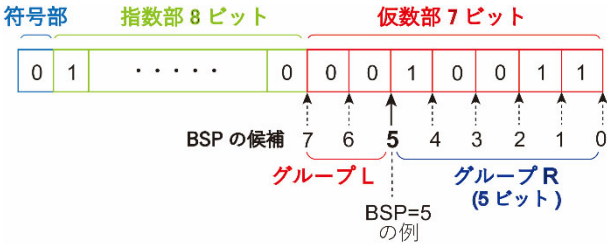


図8　浮動小数点数形式BF16に対するビット分割位置BSP

表2　評価に使用したネットワークモデルとデータセット

モデル	層数	データセット	パラメータ数*
多層パーセプトロン	3**	MNIST	118K
CNN	4***	CIFAR-10	122K
MobileNetV2	16****	Fashion-MNIST	719K

* 重みとバイアスの総数　** 全結合層の数
*** 畳み込み層の数　**** Residual Block層の数

上位ビットと下位ビットの分割位置をBSPとし，下位ビットのビット数をBSP値とするのは，前述の画像の場合と同様である．上位ビットの書込み時間T_Lは20 nsで固定し，下位ビットの書込み時間T_Rを変化させた．BSPとT_Rの値によって，推論精度と書込み消費エネルギーがトレードする．なお，ここでの推論精度とは，学習モデルによる分類結果と人手による分類結果が一致する割合とした．シミュレーションではTensorFlowを使用し，Kerasを用いて画像認識用のDNNアプリケーション（教師あり学習）を構築して，推論精度の評価を行った．学習用データは60,000枚，推論用データは10,000枚とし，各データセットを分割する形で使用した．推論精度と書込み消費エネルギーの結果を図9に示す．具体的には，正確に書込みを行った場合の推論精度に対する劣化率を品質制約として与え，その制約を満たすBSPとT_Rの組合せの中で最小の書込みエネルギーを表示している．

ほとんど推論精度の劣化のない0.5%の制約において，仮数部に指数部と符号部を合わせた全体の消費エネルギーが9〜38%削減する．品質制約を7.5%まで緩和すると，最大で44%の消費エネルギー削減が可能である．更に，BSPとT_Rの組合せについては特徴的なことが分かり，最小エネルギーを実現するBSPは多層パーセプトロンやCNNで5〜7であるのに対しMobileNetV2では2〜3と，ネットワークモデルによって大きく異なることが分かった．一方，下位ビッ

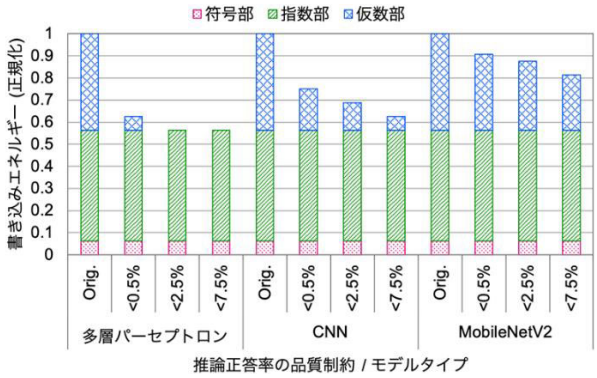


図 9　提案の AxS 手法での推論精度と書込み消費エネルギー

トへの書込み時間 T_R はどのネットワークモデルでもおおむね 0 ns であり，下位ビットへは書き込まない（切り捨て）手法で十分であることが明らかになった．

4. おわりに

コンピュータのエネルギー効率は，ムーアの法則やデナードのスケーリング則に牽引される形で向上を続けたが，2000 年代初頭を境にその構図は崩れた．いまや意図的にエネルギー効率を上げる方式を講じ，対策を打たねばならない状況にある．IoT が発展し，電池駆動のエッジデバイス上で機械学習を行う技術が浸透していく中で，エネルギー効率を高めるコンピューティング手法の必要性がますます高まっている．常に正確に計算するのがコンピュータ，という固定観念にメスを入れたアプロキシメート・コンピューティングは，画像処理や機械学習の分野で，エネルギー効率を大幅に改善できることが明らかになった．今後，こういった技術の実用化に加え，エネルギー効率を追求する新しいコンピューティング技術の研究と人材育成に期待したい．

文　献

(1) J.G. Koomey, H.S. Matthews, and E. Williams, "Smart everything : Will intelligent systems reduce resource use?," The Annual Review of Environment and Resources, vol. 38, pp. 311-343, Oct. 2013.
(2) J.G. Koomey and S. Naffziger, "Efficiency's brief reprieve : Moore's Law slowdown hits performance more than energy efficiency," IEEE Spectrum, vol. 52, no. 4, pp. 34-35, April 2015.
(3) ウェスト＆ハリス，CMOS VLSI 回路設計（基礎編），宇佐美公良，池田誠，小林和淑（監訳），pp. 351-360，丸善出版，2014.
(4) V. Chippa, D. Mohapatra, A. Raghunathan, K. Roy, and S. Chakradhar, "Scalable effort hardware design : exploiting algorithmic resilience for energy efficiency," Proc. DAC, pp. 555-560, 2010.
(5) S. Mittal, "A survey of techniques for approximate computing," ACM Computing Surveys, vol. 48, no. 4, article 62, pp. 1-33, 2016.
(6) J. Han and M. Orshansky, "Approximate computing : an emerging paradigm for energy-efficient design," IEEE European Test Symposium (ETS), 2013.
(7) Q. Xu and N.S. Kim, "Approximate computing : a survey," IEEE Design & Test, vol. 33, no. 1, pp. 8-22, Jan./Feb. 2016.
(8) B. Moons, D. Bankman, and M. Verhelst, Embedded Deep Learning : algorithms, architectures and circuits for always-on neural network processing, pp. 89-113, Springer, 2019.
(9) C. Alvarez, J. Corbal, and M. Valero, "Fuzzy memoization for floating-point multimedia applications," IEEE Trans. Comput., vol. 54, no. 7, pp. 922-927, July 2005.
(10) Y. Ono and K. Usami, "Approximate computing technique using memoization and simplified multiplication," The 34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), June 2019.
(11) S. Sidiroglou, S. Misailovic, H. Hoffmann, and M. Rinard, "Managing performance vs. accuracy trade-offs with loop perforation," The 9th ACM SIGSOFT Symposium and the 13th European Conference on Foundations of Software Engineering, pp. 124-134, Sep. 2011.
(12) A. Sampson, W. Dietl, E. Fortuna, D. Gnanapragasam, L. Ceze, and D. Grossman, "EnerJ : approximate data types for safe and general low-power computation," ACM SIGPLAN Notices, vol. 46, no. 6, pp. 164-174, June 2011.
(13) K. Cho, Y. Lee, Y.H. Oh, G-C Hwang, and J.W. Lee, "eDRAM-based tiered-reliability memory with applications to low-power frame buffers," IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED), Aug. 2014.
(14) M. Shoushtari, A. BanaiyanMofrad, and N. Dutt, "Exploiting partially-forgetful memories for approximate computing," IEEE Embedded Syst. Lett., vol. 7, no. 1, pp. 19-22, Jan. 2015.
(15) Y. Ono and K. Usami, "Energy efficient approximate storing of image data for MTJ based non-volatile flip-flops and MRAM," IEICE Trans. Electronics, vol. E104-C, no. 7, pp. 338-349, Jul. 1, 2021.
(16) Y. Ono, and K. Usami, "Energy efficient approximate storing to MRAM for deep neural network tasks in edge computing," The 23rd Workshop on Synthesis and System Integration of Mixed Information Technologies (SASIMI 2021), March 2021.

（幹事団提案，2022 年 6 月 11 日受付　2022 年 7 月 1 日再受付）

宇佐美公良（正員：フェロー）

1982 早大・理工・電気卒．1984 同大学院修士課程了．同年(株)東芝入社．同社半導体技術研究所にて，CPU チップ設計技術，低消費電力技術の研究開発に従事．1993～95 スタンフォード大学大学院客員研究員．2003 芝浦工大助教授，2005 より同大教授．博士（工学）．研究テーマは，アプロキシメート・コンピューティング，MTJ 素子を使った不揮発性パワーゲーティング，ハードウェアセキュリティ技術 PUF．著書『FPGA 時代に学ぶ集積回路のしくみ』（コロナ社），『ウェスト＆ハリス　CMOS VLSI 回路設計』（監訳，丸善出版）など．

技術の原点

情報理論に基づく秘密情報の符号化
——不完全秘匿を用いた安全な符号化法——

Information Security Coding Based on Information Theory :
Secure Coding with Non-Perfect Secrecy

山本博資 Hirosuke YAMAMOTO

アブストラクト　情報理論に基づいた秘密情報の符号化システムとして，シャノン暗号システム，秘密分散通信システム，秘密分散法，安全なネットワーク符号化，盗聴通信路符号化を取り扱う．情報理論におけるセキュリティ符号化問題では，秘密情報の完全秘匿を達成することを目的としている場合が多いが，本稿では，完全秘匿ではなく不完全秘匿を用いた情報理論的に安全な符号化法を紹介する．これは，秘密情報を幾つかの部分情報に分割し，各部分情報に関して個別に完全秘匿を達成することで情報の安全性を保証し，他方，秘密情報全体としては不完全秘匿とすることで，符号化に必要な乱数のビット長や符号語のビット長を減らすことができる符号化法である．その結果，情報理論的に安全で効率のよい符号化が可能となる．

キーワード　情報セキュリティ符号化，シャノン暗号システム，秘密分散法，ネットワーク符号化，盗聴通信路符号化

Abstract　This paper deals with the Shannon cipher system, secret sharing communication systems, secret sharing systems, secure network coding, and wiretap channel coding, which are tools for the secure coding of information based on information theory. In coding problems, it is usually studied how to achieve the perfect secrecy of information. However, in this paper, we show that we can achieve secure coding even in the case of no-perfect secrecy. We divide secret information into several pieces, and we achieve perfect secrecy for every piece individually to insure the security of information. On the other hand, by allowing the nonperfect secrecy of the whole information, we can decrease the bit length of random number and/or codewords. Hence, the coding techniques shown in this paper attain secure and efficient coding in the above coding systems.

Key words　Information security coding, Shannon cipher system, Secret sharing scheme, Secure network coding, Wiretap channel coding

1. はじめに

公開の通信路を通して情報を安全に送るために，暗号や情報セキュリティ符号化技術が使われている．現在使用されている多くの暗号システムは，解読などの攻撃に必要な計算量が非常に大きく実時間で解読するのが困難であるという計算量的安全性に基づいている．しかし，計算量的安全性に基づく暗号技術は，コンピュータ・理論・アルゴリズムなどの進歩により，将来危殆化する可能性がある．これに対して，情報理論的安全性に基づく情報セキュリティ符号化は，攻撃者が無限大の計算パワー（無限大の計算速度と無限大のメモリ量）を有していることを仮定したもとで，安全性を保証する符号化技術であり，将来危殆化しない特徴がある．なお，情報理論では無限大の計算パワーを仮定して符号化定理が証明されるため[1]，無限の計算パワーを仮定する安全性は情報理論的安全性と呼ばれている．攻撃が盗聴の場合，盗聴者がどのようにしても秘密情報に対して知ることができない情報の量に基づいた安全性であるため情報量的安全性と呼ばれる場合もある．

情報理論的安全性に基づく情報セキュリティ符号化の理論は，シャノンの論文[2],[3]から始まっているが，シャノンはその論文で完全秘匿 (perfect secrecy) の概念を導入し，ワンタイムパッド暗号 (one-time pad cipher) により，完全秘匿が達成できることを証明した．また，完全秘匿を達成するためには，秘密鍵は送信情報のビット長と同じビット長を必要とすることが証明された．その後，情報理論分野では，情報理論的安全性に基づく様々な符号化法が研究されているが，「情報理論的安全性」⇔「完全秘匿」⇔「秘密鍵の効率が悪い符号化方式」と考えている人が多いように思われる．

本稿では，「完全秘匿」ではなく，「不完全秘匿」に基づいて情報理論的に安全でかつ使用する乱数・秘密鍵・符号語などのビット長を削減できる符号化法を紹介する．具体的には，シャノン暗号システム（第 2 節），秘密分散通信システム (第 3 節)，秘密分散法 (第 4 節)，安全なネットワーク符号化 (第 5 節)，盗聴通信路符号化 (第 6 節) における不完全秘匿を利用した情報理論的に安全な符号化法を紹介する．

山本博資　正員：フェロー　東京大学大学院新領域創成科学研究科複雑理工学専攻
E-mail hirosuke@ieee.org
Hirosuke YAMAMOTO, Fellow (Dept. of Complexity Science and Engineering, School of Frontier Sciences, The University of Tokyo, 5-1-5 Kashiwanoha, Kashiwa-shi, Chiba, 277-8561 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.66–75 2022 年 10 月

なお，本稿では確率変数を英大文字 (M, W など) で表し，その確率変数のアルファベット (その確率変数が取り得る値の集合) を花文字 ($\mathcal{M}, \mathcal{W}$ など) で，そのアルファベットの要素数を $|\cdot|$ の記号 ($|\mathcal{M}|, |\mathcal{W}|$ など) で表している．また，エントロピー，条件付きエントロピー，相互情報量を，それぞれ $H(\cdot)$, $H(\cdot\,|\,\cdot)$, $I(\cdot\,;\,\cdot)$ で表記している．

2. シャノン暗号システム

シャノン暗号システムを図 1 に示す．送信される秘密情報 (平文) を M，暗号の秘密鍵を V，暗号文を W とし，それぞれのアルファベットを $\mathcal{M}, \mathcal{V}, \mathcal{W}$ とする．符号化関数及び復号関数を，それぞれ $F : \mathcal{M} \times \mathcal{V} \to \mathcal{W}$ と $G : \mathcal{W} \times \mathcal{V} \to \mathcal{M}$ とすると，$W = F(M,V)$，$M = G(W,V)$ である．F と G は決定的な関数であり，$H(W|MV) = 0$ 及び $H(M|WV) = 0$ が成り立つ．また，暗号文 M と鍵 V は，確率的に独立であり ($I(M;V) = 0$)，暗号文 M を送信する通信路及び鍵 V を送信する通信路は無雑音であるとする．

このシャノン暗号システム (F,G) の平文 M と暗号文 W の相互情報量が $I(M;W) = h$ を満たすとき，(F,G) はセキュリティレベル h をもつと呼ぶことにする．ここで，$0 \leqq h \leqq H(M)$ であり，$\overline{h} = H(M) - h$ としたとき，$H(M|W) = \overline{h}$ である．h は小さいほど ($\overline{h}$ は大きいほど) 安全性が高く，特に，$h = 0$ ($\overline{h} = H(M)$) の場合は，$I(M;W) = 0$ であることより，暗号文 W は平文 M と確率的に独立となり，完全秘匿が達成できる[3]．なお，$\overline{h}$ は秘密情報に対する盗聴者のあいまいさ (equivocation) を表す情報量であり，情報理論的セキュリティ符号化で安全性指標としてよく用いられている．

この暗号システム (F,G) に関して，次の定理が成り立つ[4]．

定理 1. シャノン暗号システム (F,G) がセキュリティレベル h をもつためには，暗号文 W と秘密鍵 V は次式を満たさなければならない．

$$H(W) \geqq H(M), \qquad H(V) \geqq \overline{h} = H(M) - h \tag{1}$$

証明.

$$\begin{aligned} H(W) &=^1 H(W) + H(M|WV) \\ &= H(W) + H(MVW) - H(WV) \\ &= H(M) + H(V|M) + H(W|MV) - H(V|W) \\ &=^2 H(M) + I(V;W) \geqq^a H(M) \end{aligned} \tag{2}$$

ここで，$=^1$ の等号は $H(M|VW) = 0$ による．また，$=^2$ の等号は，$I(M;V) = H(V) - H(V|M) = 0$ と $H(W|VM) = 0$ による．一方，$H(V)$ の不等式は次のように導かれる

$$\begin{aligned} H(V) &\geqq^a H(V|W) =^1 H(V|W) + H(M|WV) \\ &= H(VM|W) = H(M|W) + H(V|MW) \\ &\geqq^b H(M|W) = \overline{h} \end{aligned} \tag{3}$$

□

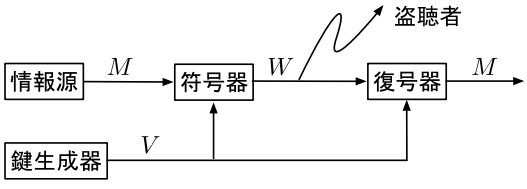


図 1　シャノン暗号システム

$\mathcal{M} = \mathcal{W}$ を有限体 (あるいは有限加法群) とし，$\mathcal{V} \subset \mathcal{M}$ とする．このとき，$F(M,V) = M + V, G(W,V) = W - V$ で与えられる加法暗号 (F,G) を考えると，次の定理が成り立つ[4]．

定理 2. M と V がそれぞれ $\mathcal{M}$ と $\mathcal{V}$ 上で一様分布し，$|\mathcal{V}| = 2^{-h}|\mathcal{M}|$ を満たすとき，加法暗号 (F,G) はセキュリティレベル h をもち，式 (1) を等号で満たす．

証明. 加法暗号は次式を満たす．

$$\begin{aligned} I(M;W) &= H(W) - H(W|M) =^3 H(W) - H(V) \\ &=^4 \log|\mathcal{M}| - \log|\mathcal{V}| = h \end{aligned} \tag{4}$$

ここで，$=^3$ の等号は，$W = M + V$ と $I(M;V) = 0$ の関係より，$H(W|M) = H(M+V|M) = H(V|M) = H(V)$ が成り立つことによる．また，$=^4$ は，M が $\mathcal{M} = \mathcal{W}$ 上で一様分布するとき，W も $\mathcal{M}$ 上で一様分布することによる．

更に，M が $\mathcal{M} = \mathcal{W}$ 上で一様分布するときは，W は V の値によらず一様分布するため，$I(V;W) = 0$ が成り立ち，式 (2) (3) の $\geqq^a$ の不等式は等号で成り立つ．また，加法暗号では $V = W - M$ と W と M から V が求まり $H(V|WM) = 0$ となるため，式 (3) の $\geqq^b$ も等号で成り立つ．したがって，式 (1) を等号で満たす．□

上記の加法暗号は，$h = 0$ の場合 ($\mathcal{V} = \mathcal{M}$ の場合)，完全秘匿を達成できるワンタイムパッド暗号となる．位数 2^N の有限体（ガロア体）を $\mathrm{GF}(2^N)$ で表すと，$\mathcal{M} = \mathrm{GF}(2^N)$ の場合はバーナム暗号 (Vernam cipher) となる．$h > 0$ の場合は，$\mathcal{M} = \mathrm{GF}(2^N)$, $\mathcal{V} = \mathrm{GF}(2^K)$ とすると，$h = N - K$, $\overline{h} = K$ となる．

注 1. $h > 0$ の場合，$M + V$ の加法暗号では，平文 M の一部のビットがそのまま暗号文 W に現れてしまう欠点がある．この欠点は次のように克服することができる．$N/K = n$ とし，$M = (M_1, M_2, \cdots, M_n)$, $M_\ell \in \mathrm{GF}(2^K)$ とする．そのとき，第 4 節で説明する「強安全な (n,n,n) しきい値ランプ秘密分散法」を用いて，この M を $(\tilde{W}_1, \tilde{W}_2, \cdots, \tilde{W}_n)$, $\tilde{W}_i \in \mathrm{GF}(2^K)$, に符号化する．そして，暗号文 W を $W = (\tilde{W}_1 + V, \tilde{W}_2, \cdots, \tilde{W}_n)$ とする．このとき，$\tilde{W}_1$ は秘密鍵 V により完全秘匿される．更に，強安全な (n,n,n) しきい値ランプ秘密分散法の特性より，全ての M_ℓ に対して，$H(M_\ell|W) = H(M_\ell|\tilde{W}_2, \cdots, \tilde{W}_n) = H(M_\ell) = K$ が成り立ち，各 M_ℓ は個別に完全秘匿される．なお，$H(M|W) = K < N$ であるため，M 全体に対しては完全秘匿ではないが，K が十分に大きければ，安全なシステムとなる．

一般に，秘密鍵 V の生成や安全な伝送には大きなコストがか

かるため，V のビット長 K を小さくすることが望まれる．しかし，完全秘匿 $h=0$ を達成するためには，秘密鍵のビット長は平文と同じビット長 $K=N$ を必要とする．一方，$h>0$ の場合は完全秘匿でないため，情報理論的に安全でないと考える人が多い．しかし，$h>0$ の場合でも，注 1 で示したように，強安全なランプ秘密分散法と組み合わせることで，情報理論的に安全なシャノン暗号システムを設計することができ，秘密鍵 V のビット長 K を N より小さくできる．

3. 秘密分散通信システム

図 1 のシャノン暗号システムでは，秘密鍵 V を送信する通信路は盗聴できないものと仮定していたが，図 1 の二つの通信路を対等にすると，図 2 の秘密分散通信システム (secret sharing communication system) となる[5]．

二つの通信路を通して送信される符号語 W_i, $i=1,2$, に対して，$I(M;W_i)=h_i$, $H(M|W_i)=\overline{h}_i, \overline{h}_i=H(M)-h_i$ を満たすとき，この通信システムはセキュリティレベル (h_1,h_2) をもつという．このとき，次の定理 3 と 4 が成り立つ[5]．

定理 3. 図 2 の秘密分散通信システムがセキュリティレベル (h_1,h_2) をもつためには，次の関係を満たさなければならない．

$$H(W_1) \geqq \max\{h_1, \overline{h}_2\} \tag{5}$$

$$H(W_2) \geqq \max\{h_2, \overline{h}_1\} \tag{6}$$

$$H(V) \geqq \max\{\overline{h}_1 - h_2, 0\} = \max\{\overline{h}_2 - h_1, 0\} \tag{7}$$

証明. $(i,j)=(1,2)$ または $(2,1)$ とする．式 (3) において，$V \Rightarrow W_i$ 及び $W \Rightarrow W_j$ と置き換えた場合を考えれば，$H(W_i) \geqq \overline{h}_j$ が得られる．また，$H(W_i) = I(M;W_i) + H(W_i|M) \geqq I(M;W_i) = h_i$ の関係が常に成り立つ．よって，式 (5) (6) が得られる．

更に，(W_1,W_2) は (M,V) から決まること $(H(W_i|MV)=0)$ 及び $I(M;V)=0$ より，次の関係式が得られる．

$$\begin{aligned} H(V) &= H(V) + H(W_i|MV) \\ &= H(V) + H(W_iMV) - H(MV) \\ &= H(W_i) + H(M|W_i) + H(V|MW_i) - H(M|V) \\ &\geqq H(W_i) - [H(M) - H(M|W_i)] \\ &\geqq \overline{h}_j - h_i \end{aligned} \tag{8}$$

□

定理 4. 平文 M と乱数 V がそれぞれ $\mathcal{M}$ と $\mathcal{V}$ 上を一様分布するとき，加法暗号を用いて，式 (5)〜(7) の等号とセキュリティレベル (h_1,h_2) を達成できる．

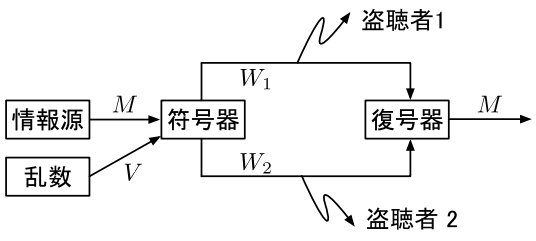


図 2　秘密分散通信システム

証明. 最初に，$h_1+h_2 \geqq H(M)$ の場合を考える．この場合は式 (7) の右辺がゼロとなることから，乱数を使用しない符号化を考える．$(i,j)=(1,2)$ または $(2,1)$ としたとき，$h_i \geqq \overline{h}_j$ が成り立つ．したがって，$H(W_i)=h_i$ となる符号を構成する．

$\mathcal{M}$ を $\mathcal{M}=\mathcal{M}_1\times\mathcal{M}_2\times\mathcal{M}_0$, $|\mathcal{M}_i| = 2^{\overline{h}_j}$, $|\mathcal{M}_0| = 2^{h_1-\overline{h}_2} = 2^{h_2-\overline{h}_1}$ を満たすように分割し，$M=(M_1,M_2,M_0) \in \mathcal{M}$ を $W_1=(M_1,M_0), W_2=(M_2,M_0)$ と符号化する．このとき，M が $\mathcal{M}$ 上を一様分布すれば，W_i はそれぞれ $\mathcal{M}_i\times\mathcal{M}_0$ 上を一様分布することから，$H(W_i)=h_i$ を満たす．よって，$I(M;W_i)=H(W_i)-H(W_i|M)=H(W_i)=h_i$ が成り立つ．

次に $h_1+h_2<H(M)$ の場合を考える．この場合は，$\overline{h}_i > h_j$ となる．$\mathcal{M}$ を $\mathcal{M}=\mathcal{M}_1\times\mathcal{M}_2, |\mathcal{M}_1|=2^{\overline{h}_1}, |\mathcal{M}_2|=2^{h_1}$ を満たすように分割し，$\mathcal{V}$ を $\mathcal{V}\subset\mathcal{M}_1, |\mathcal{V}|=2^{-h_2}|\mathcal{M}_1|=2^{\overline{h}_1-h_2}$ とする．このとき，$V\in\mathcal{V}$ を用いて $M=(M_1,M_2)\in\mathcal{M}$ を，$W_1=(V,M_2), W_2=M_1+V$ と符号化する．W_1 は $\mathcal{V}\times\mathcal{M}_2$ 上を一様分布し，W_2 は $\mathcal{M}_1$ 上を一様分布するため，$H(W_1)=\overline{h}_1-h_2+h_1=\overline{h}_2$, $H(W_2)=\overline{h}_1$ を満たす．また，$I(M;W_1)=I(M_1M_2;VM_2)=I(M_2;M_2)=H(M_2)=h_1$ を満たす．更に，$I(M;W_2)=I(M_1M_2;M_1+V)=I(M_1;M_1+V)$ となるが，$W_2=M_1+V$ は定理 2 の加法暗号に一致するため，$I(M_1;W_2)=h_2$ が成り立つ．□

M を誤りなく復号するためには，式 (5) (6) より $H(W_1)+H(W_2)\geqq H(M)$ を満たさなければならない．定理 4 より，$h_1=h_2=H(M)/2$ の場合は，$H(V)=0$ 及び $H(W_1)+H(W_2)=H(M)$ が成り立つため，乱数を使用せずに最も少ない伝送量で，セキュリティレベル (h_1,h_2) を達成できる．例えば，N を偶数として $\mathcal{M}=\mathrm{GF}(2^N)$ とすると，$M=(M_1,M_2)$, $M_i\in\mathrm{GF}(2^{N/2})$ に対して，$W_1=M_1, W_2=M_2$ とすることで，セキュリティレベル $(h_1,h_2)=(\overline{h}_1,\overline{h}_2)=(N/2,N/2)$ を達成できる．しかし，この場合は W_i の盗聴者は，$M_j, j\neq i$ を知ることができないが，M_i の情報は盗聴者に完全に漏洩する．この欠点は，$M=(M_1,M_2)$ を次のように変換することで克服できる．

$$(\tilde{M}_1,\tilde{M}_2)=(M_1,M_2)\begin{pmatrix}1 & 1\\ 1 & \alpha\end{pmatrix} \tag{9}$$

ここで，$\alpha\in\mathrm{GF}(2^{N/2})$ は，$\alpha\notin\{0,1\}$ であり，上記の行列演算は $\mathrm{GF}(2^{N/2})$ 上で行う．この変換を行ったのち，$W_1=\tilde{M}_1$, $W_2=\tilde{M}_2$ と符号化する．このとき，下記の関係が成り立つ．

$$\begin{aligned} H(M_1|W_1) &= H(M_1|\tilde{M}_1) \\ &= H(M_1) + H(\tilde{M}_1|M_1) - H(\tilde{M}_1) \\ &= H(M_1+M_2|M_1) = H(M_2) = N/2 \end{aligned} \tag{10}$$

同様に，$H(M_1|W_2)=H(M_2|W_1)=H(M_2|W_2)=N/2$ が成り立つ．したがって，セキュリティレベルは $(h_1,h_2)=(\overline{h}_1,\overline{h}_2)=(N/2,N/2)$ であるが，$I(M_1;W_1)=I(M_2;W_1)=I(M_1;W_2)=I(M_2;W_2)=0$ が成り立つ．つまり，全体の M

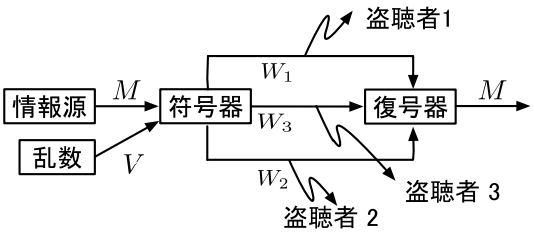


図 3　3 通信路秘密分散通信システム

に対してはセキュリティレベルは $N/2$ であり，完全秘匿ではないが，M_1 と M_2 のそれぞれに対して，個別に完全秘匿が成り立つ．

注 2. 式 (9) による符号化は，第 4 節で説明する「(2,2) しきい値秘密分散法」を用いて，$M=(M_1,M_2)$ を (W_1,W_2) に符号化したことに相当している．

次に，図 3 の 3 通信路の秘密分散通信システムを考える．この通信システムに対して，次の安全性指標を考える．

$$I(M;W_i)=h_i=0,\quad H(M|W_i)=\overline{h}_i=H(M) \tag{11}$$

$$I(M;W_iW_j)=h_{i,j},\quad H(M|W_iW_j)=\overline{h}_{i,j},\ i\neq j \tag{12}$$

ここで，$\overline{h}_{i,j}=H(M)-h_{i,j}$ である．式 (11) (12) は，W_i, $i=1,2,3$ の一つを盗聴されても M に対して完全秘匿が保たれ，(W_i,W_j) の二つが盗聴されたときは，セキュリティレベル $h_{i,j}$ となる場合である．このときに必要な $H(W_i)$ と $H(V)$ の大きさは次の定理で与えられる [5]．

定理 5. 図 4 の秘密分散通信システムが式 (11) (12) を満たすためには，次の関係を満たさなければならない．

$$H(W_i)\geqq\max\{h_{i,j},h_{i,k},\overline{h}_{j,k}\}, \tag{13}$$

$$H(V)\geqq\max\{\overline{h}_{i,j}+\overline{h}_{j,k}-h_{i,k}\} \tag{14}$$

ここで，$1\leqq i,j,k\leqq 3$, $i\neq j\neq k\neq i$ である．

証明は，定理 3 と同様に行うことができる．また，定理 4 の証明と同様にして，平文 M と乱数 V がそれぞれ $\mathcal{M}$ と $\mathcal{V}$ 上を一様分布する場合，加法暗号を用いて，式 (13) (14) の等号と式 (11) (12) のセキュリティレベルを達成することができる [5]．

4. 秘密分散法

次に，図 3 の通信路を一般の n 本に拡張した図 4 の通信システムを考える．この通信システムにおいて，$(W_{i_1},W_{i_2},\cdots,W_{i_l})$ が盗聴されたときのセキュリティレベルは，次のように定義することができる．ただし，$t\neq t'$ に対して $i_t\neq i_{t'}$ とする．

$$I(M;W_{i_1},W_{i_2},\cdots,W_{i_l})=h_{i_1,i_2,\cdots,i_l} \tag{15}$$

$$H(M|W_{i_1},W_{i_2},\cdots,W_{i_l})=\overline{h}_{i_1,i_2,\cdots,i_l} \tag{16}$$

ここで，$\overline{h}_{i_1,i_2,\cdots,i_l}=H(M)-h_{i_1,i_2,\cdots,i_l}$ である．しかし，n が大きくなるにつれて，任意に与えられた $h_{i_1,i_2,\cdots,i_l}$ に対して，それを達成するために必要な $H(W_i)$ 及び $H(V)$ を求めるのは非常に煩雑になる．そのため，$h_{i_1,i_2,\cdots,i_l}$ の取り得る値を $\{\frac{t}{L}H(M), t=0,1,2,\cdots,L\}$ に制限した場合がよく取り扱われており，そのような符号化法は秘密分散法 (secret sharing scheme, SSS) と呼ばれている [6], [7]．特に，$L\geqq 2$ の場合は，ランプ秘密分散法 (ramp SSS) と呼ばれている．$L=1$ の場合は単に秘密分散法と呼ばれることが多いが，ランプ秘密分散法と区別するために，完全秘密分散法 (peferct SSS) と呼ばれる場合もある．なお，秘密分散法では，符号語 W_i はシェア (share) あるいは分散情報と呼ばれている．

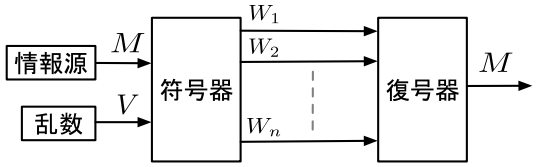


図 4　秘密分散法

秘密分散法において，$h_{i_1,i_2,\cdots,i_l}$ の値が l のみに依存する場合を，しきい値秘密分散法 (threshold SSS) という．しきい値秘密分散法のセキュリティレベルを簡単のため，$h_{(l)}=h_{i_1,i_2,\cdots,i_l}$, $\overline{h}_{(l)}=\overline{h}_{i_1,i_2,\cdots,i_l}$ で表すことにする．このとき，$2\leqq k\leqq n$, $1\leqq L\leqq k$ に対して，次のセキュリティ特性を満たすとき，(k,L,n) しきい値ランプ秘密分散法という．また，$L=1$ のときは，単に (k,n) しきい値秘密分散法という (注1) [8]．

$$h_{(l)}=H(M)-\overline{h}_{(l)}=\begin{cases}0, & \text{if } l\leqq k-L\\ \frac{l-k+L}{L}H(M), & \text{if } k-L\leqq l\leqq k\\ H(M), & \text{if } k\leqq l\end{cases} \tag{17}$$

以下では，$L=1$ の (k,n) しきい値秘密分散法も含めて，(k,L,n) しきい値ランプ秘密分散法と呼ぶことにする．このとき，(k,L,n) しきい値ランプ秘密分散法に関して次の定理が成り立つ (注2)．

定理 6. (k,L,n) しきい値ランプ秘密分散法において，任意のシェア集合 $\{W_{i_1},W_{i_2},\cdots,W_{i_l}\}$, $1\leqq l\leqq k$, と乱数 V は次式を満たさなければならない．

$$H(W_{i_1}W_{i_2}\cdots W_{i_l})\geqq\frac{l}{L}H(M) \tag{18}$$

$$H(V)\geqq\frac{(k-L)H(M)}{L} \tag{19}$$

証明. 以下では，簡単のために，$W_{i_{\{a:b\}}}=\{W_{i_a},W_{i_{a+1}},\cdots W_{i_b}\}$ の表記を用いる．このとき，$0\leqq a\leqq k-L$ 及び $0\leqq t\leqq L$ を満たす任意の a と t について，次式が成り立つ．

$$H(W_{i_{\{a+1:a+t\}}}|W_{i_{\{1:a\}}})\geqq H(W_{i_{\{a+1:a+t\}}}|W_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}})$$

(注1)：(k,n) しきい値秘密分散法は Shamir [6] と Blakely [8] により独立に提案され，(k,L,n) しきい値ランプ秘密分散法は Blakley-Meadows [9] と山本 [10] により独立に提案されている．

(注2)：文献 (10) の定理 1 では，式 (18) の $l=1$ の場合が証明されている．式 (18) はそれを一般化したものである．

$$
\begin{aligned}
&=^{5} H(W_{i_{\{a+1:a+t\}}}|W_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}}) + H(M|W_{i_{\{1:k\}}}) \\
&= H(MW_{i_{\{a+1:a+t\}}}|W_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}}) \\
&= H(M|W_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}}) \\
&\qquad + H(W_{i_{\{a+1:a+t\}}}|MW_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}}) \\
&\geqq H(M|W_{i_{\{1:a\}}}W_{i_{\{a+t+1:k\}}}) \\
&= \overline{h}_{(k-t)} = \frac{t}{L}H(M) \qquad (20)
\end{aligned}
$$

ここで，$=^{5}$ は $H(M|W_{i_{\{1:k\}}}) = \overline{h}_{(k)} = 0$ による．したがって，$r = \lfloor k/L \rfloor$ とすると，式 (20) より，次式が成り立つ．

$$
\begin{aligned}
H(W_{i_{\{1:l\}}}) &= \sum_{j=1}^{r} H(W_{i_{\{(j-1)L+1:jL\}}}|W_{i_{\{1:(j-1)L\}}}) \\
&\qquad + H(W_{i_{\{rL+1:l\}}}|W_{i_{\{1:rL\}}}) \\
&\geqq r\frac{L}{L}H(M) + \frac{l-rL}{L}H(M) \\
&= \frac{l}{L}H(M) \qquad (21)
\end{aligned}
$$

次に，式 (19) を示す．式 (8) の W_i に $W_{i_{\{1:k\}}}$ を代入し，更に式 (21) の関係を用いると次式が成り立つ．

$$
\begin{aligned}
H(V) &\geqq H(W_{i_{\{1:k\}}}) - [H(M) - H(M|W_{i_{\{1:k\}}})] \\
&\geqq \frac{k}{L}H(M) - h_{(k)} = \frac{k-L}{L}H(M) \qquad (22)
\end{aligned}
$$

□

式 (18) (19) を等号で満たす (k, L, n) しきい値ランプ秘密分散法として，$k-1$ 次多項式を用いる方法がある[6], [9], [10]．$M = (M_1, M_2, \cdots, M_L)$, $V = (V_1, V_2, \cdots, V_{k-L})$ とし，$M_\ell \in \mathrm{GF}(2^{N/L})$, $V_j \in \mathrm{GF}(2^{N/L})$, $M \in \mathrm{GF}(2^N)$, $V \in \mathrm{GF}(2^{N(k-L)/L})$ とする．このとき，次式で与えられる $\mathrm{GF}(2^{N/L})$ 上の k 次の多項式 $f(x)$ と，$\alpha_i \in \mathrm{GF}(2^{N/L})$ を用いて，$W_i = f(\alpha_i)$ と符号化する．

$$
\begin{aligned}
f(x) &= M_1 + M_2 x + \cdots + M_L x^{L-1} \\
&\qquad + V_1 x^L + V_2 x^{L+1} + \cdots + V_{k-L} x^{k-1} \qquad (23)
\end{aligned}
$$

この多項式を用いる符号化法は，式 (17) を満たすが，$L \geqq 2$ の場合は，k 未満の l でも，ある M_ℓ が復号できる（$H(M_\ell|W_{i_{\{1:l\}}}) = 0$ となる）場合がある[11]．この欠点を改善するために，次のようなより強い安全性指標を考える．

任意の $0 \leqq t \leqq L$ 及び任意の $(M_{\ell_{\{1:t\}}}, W_{i_{\{1:k-t\}}})$ に対して，$H(M_{\ell_{\{1:t\}}}|W_{i_{\{1:k-t\}}})$ が t のみに依存する場合を考え，$h^*_{(k-t)}$ と $\overline{h}^*_{(k-t)}$ をそれぞれ

$$
I(M_{\ell_{\{1:t\}}}; W_{i_{\{1:k-t\}}}) = h^*_{(k-t)} \qquad (24)
$$

$$
H(M_{\ell_{\{1:t\}}}|W_{i_{\{1:k-t\}}}) = \overline{h}^*_{(k-t)} \qquad (25)
$$

で定義する．このとき，$h^*_{(k-t)}$ と $\overline{h}^*_{(k-t)}$ が次式を満たすとき，強安全な (k, L, n) しきい値ランプ秘密分散法という[10]．

$$
h^*_{(k-t)} = 0, \qquad \overline{h}^*_{(k-t)} = \overline{h}_{(k-t)} = \frac{t}{L}H(M) \qquad (26)
$$

$M = (M_1, M_2, \cdots, M_L)$ に対して式 (17) のみを満たす場合は，

$$
\begin{aligned}
\frac{L-t}{L}H(M) = h_{(k-t)} &= I(M_{\ell_{\{1:L\}}}; W_{i_{\{1:k-t\}}}) \\
&\geqq I(M_{\ell_{\{1:t\}}}; W_{i_{\{1:k-t\}}}) \qquad (27)
\end{aligned}
$$

となるが，$I(M_{\ell_{\{1:t\}}}; W_{i_{\{1:k-t\}}}) = 0$ となる保証はない．これに対して，式 (26) を満たす場合は，常に $I(M_{\ell_{\{1:t\}}}; W_{i_{\{1:k-t\}}}) = 0$ が成り立つ．つまり，任意の $W_{i_{\{1:k-t\}}}$ が漏洩したとき，任意の $M_{\ell_{\{1:t\}}}$ に関して完全秘匿が達成できる．$l = k-1$ のときでも，任意の M_ℓ が個別に完全秘匿される．したがって，式 (26) を満たす場合に比べて，非常に強い安全性を実現できる．

式 (18) (19) を等号で満たす強安全な (k, L, n) しきい値ランプ秘密分散法は，次のようにして作ることができる[10]．$M = (M_1, M_2, \cdots, M_L)$, $M_\ell \in \mathrm{GF}(2^{N/L})$, $V_j \in \mathrm{GF}(2^{N/L})$ とし，G を $\mathrm{GF}(2^{N/L})$ 上の $k \times n$ 行列とする．このとき，符号化を次のように行う．

$$
\begin{aligned}
&(W_1, W_2, \cdots, W_n) \\
&\qquad = (M_1, M_2 \cdots, M_L, V_1, V_2, \cdots, V_{k-L})\, G \qquad (28)
\end{aligned}
$$

定理 7. M と V がそれぞれ $\mathrm{GF}(2^N)$ 上と $\mathrm{GF}(2^{N(k-L)/L})$ 上で一様分布し，式 (28) の G に対して，式 (29) で定義される $\tilde{G}$ の任意の k 列が線形独立のとき，強安全な (k, L, n) しきい値ランプ秘密分散法となる．

$$
\tilde{G} = \left[\begin{array}{c|c} I_{L\times L} & \\ 0_{(k-L)\times L} & G \end{array}\right] \qquad (29)
$$

ここで，$I_{L\times L}$ と $0_{(k-L)\times L}$ は，それぞれ添え字に書かれた大きさの単位行列とゼロ行列である．

証明. 任意に与えられた $W_{i_{\{1:k\}}}$ に対して，$W_{i_{\{1:k\}}}$ に対応する G の部分行列を $G_{i_{\{1:k\}}}$ とする．G の任意の k 列が線形独立なことから，$G_{i_{\{1:k\}}}$ は正則行列となり，逆行列 $G^{-1}_{i_{\{1:k\}}}$ をもつ．したがって，次式で $M = (M_1, M_2 \cdots, M_L)$ を復号できる．

$$
\begin{aligned}
&(M_1, M_2, \cdots, M_L, V_1, V_2, \cdots, V_{k-L}) \\
&\qquad = (W_{i_1}, W_{i_2}, \cdots, W_{i_k})\, G^{-1}_{i_{\{1:k\}}} \qquad (30)
\end{aligned}
$$

また，$\tilde{G}$ の任意の k 列が線形独立なことから，任意の $W_{i_{\{1:k-t\}}}$ は，任意の $M_{\ell_{\{1:t\}}}$ と線形独立になる．各 M_ℓ は $\mathrm{GF}(2^{N/L})$ 上の値を取るため，$W_{i_{\{1:k-t\}}}$ が与えられたとき，$M_{\ell_{\{1:t\}}}$ は $2^{Nt/L}$ 個の可能性がある．更に，各 M_ℓ と V_j が $\mathrm{GF}(2^{N/L})$ 上で一様分布していることから，$M_{\ell_{\{1:t\}}}$ は $2^{Nt/L}$ 個の上で一様分布する．したがって，$H(M_{\ell_{\{1:t\}}}|W_{i_{\{1:k-t\}}}) = \overline{h}^*_{(k-t)} = Nt/L$ 及び $H(M) = N$ の関係が成り立ち，式 (26) を満たす．□

上記の符号化法を用いれば，式 (18) を等号で満たすことができることより，$H(W_i) = \frac{1}{L}H(M)$ となる．したがって，$L = 1$ である (k, n) しきい値秘密分散法に比べて，$L \geqq 2$ の (k, L, n) しきい値ランプ秘密分散法を用いるとシェア W_i のビット長を $1/L$ に削減できる．特に，$k = L = n$ の場合の強安全な (n, n, n) しきい値ランプ秘密分散法では，

$M=(M_1,M_2,\cdots,M_n)$, $M_\ell \in \mathrm{GF}(2^{N/n})$ に対して，式 (19) より $H(V)=0$ で，$H(W_i)=N/n$, $\sum_{i=1}^{n} H(W_i)=N$, $\overline{h}^*_{(n-1)}=H(M_\ell|W_{i_{\{1:n-1\}}})=N/n$ を実現できる．N/n が大きい場合には，安全で非常に効率のよい秘密分散法となる．

注 3. 強安全でないランプしきい値秘密分散法を強安全なランプしきい値秘密分散法に変換する手法が知られている[11]．

注 4. 式 (29) の $\tilde{G}$ の任意の k 列が線形独立になっていることから，$\tilde{G}$ は最大距離分離符号 (maximum distance separable code, MDS 符号) の生成行列とみなすことができる．代表的な MDS 符号であるリードソロモン符号を用いて，(k,n) しきい値秘密分散法を構成することができるが[12]，リードソロモン符号を用いて組織的 MDS 符号を構成することで，強安全な (k,L,n) しきい値ランプ秘密分散法を構成することもできる[13]．更に，強安全な (k,L,n) しきい値ランプ秘密分散法を特殊な場合として含むより一般的な強安全なしきい値秘密分散法を，線形符号に基づいて構成する方法が知られている[14]．

注 5. 秘密分散法は，情報の伝送や保管のために使用する以外に，マルチパーティによる秘密計算に用いることができる[15]．そのような場合に，ランプ秘密分散法を用いてシェアのビットサイズを小さくすることで，プロトコルの効率化をはかることができる[16],[17]．

5. 安全なネットワーク符号

図 4 では，n 本の並列な通信路を考えていたが，それを一般のネットワークに拡張した通信システムを考える．ネットワーク内の通信路と通信路の接続点をそれぞれ辺 (edge) と節点 (node) で表し，各通信路は無雑音で一度に 1 シンボルの情報を送信できるものとする．また，各接続点は演算能力を有しており，接続点の入力に演算を行った結果を出力することができる．なお，通信路の送信や接続点の演算には遅延が生じないものとする．このようなネットワークに対する符号化をネットワーク符号化 (network coding) という[18],[19]．ネットワーク上の送信器 e から受信器 r に一度に送信できるシンボル数は，e から r への最大フロー $\mathrm{maxflow}(e,r)$ で与えられる．$\mathrm{maxflow}(e,r)$ は e から r への辺素なパス (互いに共通の辺をもたないパス) の最大個数である．

ネットワーク上の単一の送信器 e から複数の受信器 $\{r_1,r_2,\cdots,r_J\}$ に，同じ情報 $M=(M_1,M_2,\cdots,M_k)$ を同時に送信する場合をマルチキャスト (multicast) という．送信器と受信器を含むネットワークが与えられた場合，そのネットワークを通してマルチキャストで送信可能な最大の k をマルチキャスト容量 (multicast capacity) というが，マルチキャスト容量 k は $k=\min_j \mathrm{maxflow}(e,r_j)$ で与えられる[18]．各 r_j には少なくとも k 本の辺素パス $\mathcal{P}_j=\{P_{j1},P_{j2},\cdots,P_{jk}\}$ が存在するが，$\mathcal{P}_j$ と $\mathcal{P}_{j'}$, $j'\neq j$, のパスには，共通の辺が含まれていても構わない．このような場合に，マルチキャスト容量 k は，各節点で線形演算を行う線形ネットワーク符号で，達成できることが知られている[19]．

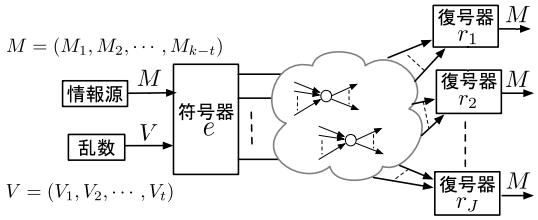


図 5 t-安全なネットワーク符号化

ネットワークに盗聴者がいるとき，図 5 のように t 個の M_ℓ を乱数 $V=(V_1,V_2,\cdots,V_t)$ に置き換えることで，ネットワーク内の t 個の辺を盗聴されても，$M=(M_1,M_2,\cdots,M_{k-t})$ の情報が全く漏洩しないようにすることができる．そのようなネットワーク符号を t-安全な (t-secure) なネットワーク符号という[20],[21]．しかし，t-安全なネットワーク符号の場合，$t+1$ 個以上の辺を盗聴されると一部の M_ℓ が漏洩する可能性がある．

t-安全なネットワーク符号は，各受信器 r_j への k 本の辺素パスを流れる情報からは M が復号でき，そのうちの t 本を盗聴しても M の情報が漏洩しないことから，$(k,k-t,k)$ しきい値ランプ秘密分散法に対応した符号化法と考えることができる．したがって，強安全な $(k,k-t,k)$ しきい値ランプ秘密分散法に対応した符号化を行えば，$t\leqq l<k$ 個の辺を盗聴されても，任意の $(M_{\ell_1},M_{\ell_2},\cdots,M_{\ell_{k-l}})$ の情報に対して完全秘匿を達成でき，強安全な t-安全ネットワーク符号を構成できる[21]．

線形ネットワーク符号では，辺 i を流れる情報 W_i は，M と V の線形結合として表されるため，$g_i=(g_{i1},g_{i2},\cdots,g_{ik})^T$ を k 次元の縦ベクトル (T は転置を示す) として，

$$W_i=(M_1,M_2,\cdots,M_{k-t},V_1,V_2,\cdots,V_t)g_i \qquad (31)$$

と表現できる．このとき，強安全な t-安全線形ネットワーク符号は次のように構成できる[21]．

(1) 節点 v の出力辺を $\{o_{v1},o_{v2},\cdots o_{va}\}$ とし，v の入力辺を $\{i_{v1},i_{v2},\cdots i_{vb}\}$ とする．このとき，各 $g_{o_{vj}}$ は，$\{g_{i_{v1}},g_{i_{v2}},\cdots,g_{i_{vb}}\}$ の線形結合でなければならない．

(2) 受信器 r_j の k 個の辺素パス $\mathcal{P}_j=\{P_{j1},P_{j2},\cdots,P_{jk}\}$ に対して，各 P_{ju} 上の任意の辺を i_{ju},$u=1,2,\cdots,k$, とする．このとき，$\{g_{i_{j1}},g_{i_{j2}},\cdots,g_{i_{jk}}\}$ は互いに線形独立でなければならない．

(3) $t\leqq l<k$ に対して，$\bigcup_{j=1}^{J}\mathcal{P}_j$ 上の任意の l 個の辺に対応した $\{g_{i_1},g_{i_2},\cdots,g_{i_l}\}$ を考える．このとき，下記の $G_{k\times L}$ の任意の $k-l$ 個の列ベクトルは，$\{g_{i_1},g_{i_2},\cdots,g_{i_l}\}$ と線形独立である．

$$G_{k\times L}=\begin{bmatrix} I_{L\times L} \\ 0_{(k-L)\times L}\end{bmatrix} \qquad (32)$$

6. 盗聴通信路符号化

今までの節では，通信路は無雑音と考えていた．通信路に雑音がある場合でも，性能のよい誤り訂正符号を用いれば，無雑音通信路に近づけることができる．しかし，この通信路の雑音を，

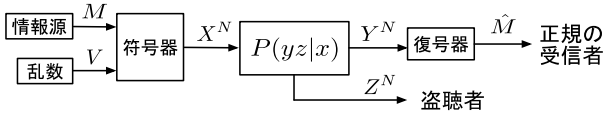


図 6　盗聴通信路符号化通信システム

情報の安全な送信のために積極的に利用する符号化法が考えられる．そのような符号化を盗聴通信路符号化 (wiretap channel coding) という[22],[23]．

図 6 の通信システムを考える．$X \in \mathcal{X}$ を通信路入力とし，$Y \in \mathcal{Y}$ を正規の受信者が受け取る通信路出力，$Z \in \mathcal{Z}$ を盗聴者が受け取る通信路出力とする．通信路は無記憶通信路とし，その特性は遷移確率 $P(yz|x)$ により与えられているものとする．このとき送信者から正規の受信者及び盗聴者への通信路は，それぞれ $P(y|x) = \sum_{z\in\mathcal{Z}} P(yz|x)$ と $P(z|x) = \sum_{y\in\mathcal{Y}} P(yz|x)$ の遷移確率をもつ．送信者は，情報 $M \in \mathcal{M}$ を符号長 N の符号語 X^N に符号化して送信する．正規の受信者は Y^N を受信し，復号器で $\hat{M} \in \mathcal{M}$ を復号する．この符号の符号化レート R は，$R = \frac{1}{N}\log|\mathcal{M}|$ で定義され，復号誤り率は $P_e = \Pr\{\hat{M} \neq M\}$ で与えられる．また，正規の受信者の通信路 $P(y|x)$ に対する通信路容量 C は，

$$C = \max_{P(x)} I(X;Y) \tag{33}$$

で与えられる．このとき，通信路符号化定理[1]より，$R < C$ を満たせば，任意の $\varepsilon > 0$ に対して，十分に大きな N で $P_e \leqq \varepsilon$ を満たす符号を構成できる．

しかし，通常の通信路符号化を行うと，盗聴者に送信情報 M の一部が漏洩する可能性がある．そこで，盗聴者に送信情報 M が漏洩しないように，次の条件を課したものが，盗聴通信路符号化である．

$$I(M;Z^N) \leqq \varepsilon \tag{34}$$

任意の ε と十分に大きな N に対して，$P_e \leqq \varepsilon$ と式 (34) のセキュリティ条件を同時に満たす符号が構成できる符号化レート R の上限は，秘匿容量 (secrecy capacity) と呼ばれ，秘匿容量 C_S は次式で与えられる[23]．

$$C_S = \max_{P(x|\tilde{x})P(\tilde{x})} [I(\tilde{X};Y) - I(\tilde{X};Z)] \tag{35}$$

ここで $\tilde{X} \in \tilde{\mathcal{X}}$ は，$\tilde{X} \to X \to YZ$ のマルコフ連鎖を成す補助確率変数である．符号器は通信路 $X \to YZ$ の手前に任意の通信路を接続するこができるが，式 (35) は，右辺第 1 項と第 2 項の差ができるだけ大きくなるような，遷移確率 $P(x|\tilde{x})$ をもつ通信路 $\tilde{X} \to X$ を $X \to YZ$ の通信路の手前に接続した通信路を考えていることに相当している．

通信路 $X \to YZ$ が，任意のマルコフ連鎖 $\tilde{X} \to X \to YZ$ に対して，$I(\tilde{X};Y) \geqq I(\tilde{X};Z)$ を満たすとき，通信路 $X \to Y$ は通信路 $X \to Z$ より低雑音 (less noisy) という．このとき，秘匿容量 C_S は，より簡単な次式で与えられる[23]．

$$C_S = \max_{P(x)} [I(X;Y) - I(X;Z)] \tag{36}$$

更に，通信路 $X \to Y$ と通信路 $X \to Z$ がともに 2 元対称通信路 (binary symmetric channel, BSC) の場合やともに加法的ガウス雑音通信路 (additive Gaussian noise channel) の場合は，通信路の対称性から式 (33) を最大化する確率分布 $P(x)$ と式 (36) を最大化する確率分布 $P(x)$ が同じになるため，式 (36) で与えられる秘匿容量 C_S は，更に次の単純な式で表現できる[22],[24]．

$$C_S = C - C_Z \tag{37}$$

ここで，C は正規の受信者に対する通信路容量であり，C_Z は盗聴者の通信路 $X \to Z$ に対する通信路容量である．

式 (35) は直感的に次のように理解することができる．式 (35) の右辺の第 1 項は通信路 $\tilde{X} \to Y$ を通して正規の受信者に任意に小さい復号誤り率で情報を送信可能な符号化レートを表している．これに対して，第 2 項は通信路 $\tilde{X} \to Z$ を通して盗聴者が復号できる（盗聴者に漏洩する）情報のレートを表している．そこで，情報 M の符号化レート $R = \frac{1}{N}\log|\mathcal{M}|$ と一様乱数 V の符号化レート $R_V = \frac{1}{N}\log|\mathcal{V}|$ を，

$$R + R_V < I(\tilde{X};Y) \tag{38}$$

$$R_V > I(\tilde{X};Z) \tag{39}$$

を満たすように設定する．このとき符号化を工夫すると，符号長 N が十分に大きい場合，Z^N から盗聴者が得られる情報は乱数 V に関するものだけで，M に関する情報は盗聴者に漏れないようにでき，式 (34) を満たすことができる．式 (38) (39) より，$R < I(\tilde{X};Y) - I(\tilde{X};Z)$ の関係が成り立つ．したがって，式 (35) を最大にする $\tilde{X} \to X \to YZ$ に対して，(R, R_V) の値を，式 (38) (39) の各不等式の右辺に十分に近い値に設定することで，C_S の秘匿容量を達成する符号化が可能となる．

注 6. 式 (34) の $\varepsilon > 0$ は，N を大きくするにつれて任意に小さくできるが，一般には $\varepsilon = 0$ にできない．これは，盗聴者の受信値 Z^N を直接 (M,V) によって決めることができず，(M,V) で決めることのできる通信路入力 X^N を通してしか Z^N の値を制御できないためである．

注 7. 式 (34) の安全性指標の代わりに，通信路 1 シンボルあたりのセキュリティレベル $\frac{1}{N}I(M;Z^N) \leqq \varepsilon$ が安全性指標に用いられる場合もある．N で割っていない式 (34) の方がより強い安全性が保証されるが，無記憶通信路に対しては式 (34) の強い安全性を達成できる[25]．

注 8. 式 (35) において，どのような $\tilde{X} \to X \to YZ$ に対しても，$I(\tilde{X};Y) \leqq I(\tilde{X};Z)$ となる場合は $C_S = 0$ となる．しかし，そのような場合でも，盗聴通信路以外に公開の通信路が利用できれば，情報を安全に送信できる通信プロトコルが知られている[26],[27]．

注 9. Z^N を得た盗聴者に送信情報 M が漏洩しないためには，Z^N の確率分布が M に依存しない分布になっている必要がある．定常無記憶な $\tilde{X}$ を通信路 $\tilde{X} \to Z$ に N 回入力したときの出力を Z^N とし，情報 $m \in \mathcal{M}$ と一様乱数 V で符号化し

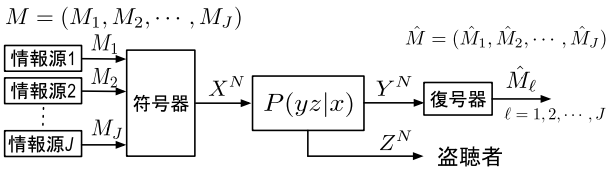


図 7　盗聴通信路多重符号化

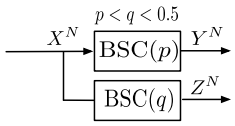


図 8　2 元対称盗聴通信路

て作成した符号語 $\tilde{X}^N_{m,V}$ を通信路 $\tilde{X}\to Z$ に入力したときの出力を $Z^N_{m,V}$ とする．この Z^N と $Z^N_{m,V}$ の分布の差を変動距離 $d(Z^N,Z^N_{m,V})=\sum_{z^N\in\mathcal{Z}^N}|P_{Z^N}(z^N)-P_{Z^N_{m,V}}(z^N)|$ で測る．このとき任意に小さい $\varepsilon>0$ に対して，$d(Z^N,Z^N_{m,V})\leqq\varepsilon$ を達成するために必要な一様乱数 V の符号化レート R_V の下限は，入力 $\tilde{X}$ に対する通信路 resolvability と呼ばれる[28]．式 (35) の第 2 項の $I(\tilde{X};Z)$ は，盗聴通信路 $\tilde{X}\to Z$ に対する通信路 resolvability に相当しており，式 (39) は乱数の符号化レート R_V を通信路 resolvability より大きく設定することで，全ての m に対して $d(Z^N,Z^N_{m,V})\leqq\varepsilon$ を実現し，$Z^N_{m,V}$ の分布が m に依存しないように符号化していると考えることができる．なお，通信路 resolvability と盗聴通信路符号化の関係は文献(29) , (30) などを参照して欲しい．

秘匿容量 C_S が正の値であれば，盗聴通信路符号化を用いることにより，正規の受信者に情報 M を安全に送ることができる．しかし，秘匿容量 C_S は通信路容量 C に対して $C_S<C$ となるため，セキュリティを考えない符号化に比べて，送信効率が悪くなる．特に，盗聴者の通信路特性 $P(z|x)$ が正規の受信者の通信路特性 $P(y|x)$ に近い場合は，$C_S\ll C$ となり，送信効率が非常に悪くなる．

この欠点を克服するために，図 7 のシステムを考える．ここで，$\mathcal{M}=\mathcal{M}_1\times\mathcal{M}_2\times\cdots\times\mathcal{M}_J$, $M=(M_1,M_2,\cdots,M_J)$, $M_\ell\in\mathcal{M}_\ell$ とする．また，各 M_ℓ は $\mathcal{M}_\ell$ 上で一様分布をし，$(M_1,M_2,\cdots,M_J)$ は互いに独立であるとする．

各 M_ℓ に対する符号化レートを $R_\ell=\frac{1}{N}\log|\mathcal{M}_\ell|$ で定義すると，M の符号化レート $R=\frac{1}{N}\log|\mathcal{M}|$ は，$R=\sum_{\ell=1}^J R_\ell$ で与えられる．このとき，次の定理が成り立つ[30]．

定理 8. M が $\mathcal{M}$ 上で一様分布をし，$\tilde{X}\to X\to YZ$ のマルコフ連鎖を満たす $\tilde{X}$ に対して，$(R_1,R_2,\cdots,R_J)$ が

$$R<I(\tilde{X};Y) \tag{40}$$

$$R-R_\ell>I(\tilde{X};Z) \tag{41}$$

を満たすものとする．このとき十分に大きな N で，次式を満たす盗聴通信路符号化が可能である．

$$P_e=\Pr\{M\neq\hat{M}\}\leqq\varepsilon \tag{42}$$

$$I(M_\ell;Z^N)\leqq\varepsilon \tag{43}$$

上記の定理の式 (40) (41) から，符号化レート R と各 R_ℓ は，次の関係を満たしている．

$$R<I(\tilde{X};Y)\leqq I(X;Y)\leqq C \tag{44}$$

$$R_\ell<R-I(\tilde{X};Z)<I(\tilde{X};Y)-I(\tilde{X};Z)\leqq C_S \tag{45}$$

したがって，式 (42) (43) の結果は，通常の通信路符号化定理や通常の盗聴通信路符号化定理の結果と矛盾していないことが分かる．

しかし，式 (40) は M の符号化レート R を秘匿容量 C_S より大きくできることを意味している．一方，式 (41) は式 (39) に対応する式であり，各 M_ℓ の符号化に対して，ほかの $M_{\ell'}$, $\ell'\neq\ell$ の符号化レートを全て合わせると $I(\tilde{X};Z)$ 以上になっている．これは，M_ℓ の符号化に対して，$M_{\ell'},\ell'\neq\ell$ が乱数 V の役割を果たしていることを意味している．

式 (43) より，各 M_ℓ に対しては個別に完全秘匿が達成できる．しかし，C_S を超える符号化レートの部分は，盗聴者に完全秘匿できないため，盗聴者には少なくとも $R-C_S$ の符号化レート分の情報が漏洩する．したがって，M 全体に対しては，$I(M;Z^N)\geqq R-C_S$ となり，不完全秘匿となっている．

定理 8 の一般的な証明は複雑な議論が必要になるため，以下では図 7 の盗聴通信路が図 8 の 2 元対称通信路 (BSC) から構成されている場合を考えることにする．つまり，$\mathcal{X}=\mathcal{Y}=\mathcal{Z}=\{0,1\}$ であり，$X\to Y$ と $X\to Z$ の通信路がそれぞれビット誤り率 p と q の BSC の場合である．ただし，$p<q<0.5$ とする．このとき，2 元エントロピー関数 $h(u)=-u\log_2 u-(1-u)\log_2(1-u)$ を用いると，$X\to Y$ と $X\to Z$ のそれぞれの通信路容量は，$C=1-h(p)$ と $C_Z=1-h(q)$ で与えられ，秘匿容量 C_S は式 (37) より，$C_S=h(q)-h(p)$ で与えられる．

$C_S/C\leqq 0.5$ の場合を考え，十分に小さい $\xi>0$ に対して，パラメータ $J,\lambda>0$, K を次式を満たすように定める(注3)

$$J=\left\lceil\frac{C-\xi}{C_S-2\xi}\right\rceil \tag{46}$$

$$C-\xi=J(C_S-\lambda) \tag{47}$$

$$K=N(C_S-\lambda) \tag{48}$$

このとき，λ は次の関係を満たす．$\lambda=C_S-\frac{C-\xi}{J}\geqq C_S-\frac{C-\xi}{(C-\xi)/(C_S-2\xi)}=2\xi$.

$\ell=1,2,\cdots,J$ に対して，$M_\ell\in\mathcal{M}_\ell=\{0,1\}^K$ とすると，各 M_ℓ は K ビットの 2 元系列であり，その符号化レートは $R_\ell=\frac{K}{N}=C_S-\lambda<C_S$ を満たす．また，全体の符号化レートは $R=\sum_{\ell=1}^J R_\ell=\frac{JK}{N}=J(C_S-\lambda)=C-\xi<C$ を満たす．更に，$R-R_\ell=(C-\xi)-(C_S-\lambda)=C_Z+(\lambda-\xi)>C_Z$ の関係を満たしている．

各 M_ℓ を K ビットの横ベクトルとし，$\{0,1\}$ を要素にもつ JK 行 N 列の行列 G を用いて，次のように線形符号化する．

$$X^N=(M_1,M_2,\cdots,M_J)\,G \tag{49}$$

(注3)：式 (48) の等号は，十分に大きい N と K を用いることで，よい近似精度で満たすように設定できる．

ここで，G の各ビットをランダムに生成し，G がランク JK をもつものを使用する．$R < C$ のとき，このランダム線形符号は，N を十分大きくすれば，任意の $\varepsilon > 0$ に対して式 (42) を満たすことが知られている[31]．

次にこのランダム線形符号が，式 (43) を満たすことを証明する．

$$
\begin{aligned}
&I(M_\ell; Z^N) \\
&= H(Z^N) - H(Z^N|M_\ell) \\
&= H(Z^N) - H(Z^N X^N|M_\ell) + H(X^N|Z^N M_\ell) \\
&= H(Z^N) - H(X^N|M_\ell) - H(Z^N|X^N M_\ell) \\
&\qquad\qquad + H(X^N|Z^N M_\ell) \\
&=^6 H(Z^N) - H(X^N|M_\ell) - H(Z^N|X^N) \\
&\qquad\qquad + H(X^N|Z^N M_\ell) \\
&\leqq^7 N - (J-1)N(C_S - \lambda) - Nh(q) + H(X^N|Z^N M_\ell) \\
&=^8 N - N(C - \xi - C_S + \lambda) - Nh(q) + H(X^N|Z^N M_\ell) \\
&=^9 -N(\lambda - \xi) + H(X^N|Z^N M_\ell) \qquad (50)
\end{aligned}
$$

ここで，数字が割り振られた等号・不等号は下記の理由による．

6: $M_\ell \to X^N \to Z^N$ のマルコフ連鎖が成り立つため，$H(Z^N|X^N M_\ell) = H(Z^N|X^N)$ である．

7: $H(Z^N) \leqq N$, $H(Z^N|X^N) = Nh(q)$, $H(X^N|M_\ell) = (J-1)K = (J-1)N(C_S - \lambda)$

8: $J(C_S - \lambda) = C - \xi$

9: $C - C_S = C_Z = 1 - h(q)$

更に，$H(X^N|Z^N M_\ell)$ は次のように評価できる．

$$
\begin{aligned}
H(X^N|Z^N M_\ell) &=^{10} H(X^N \tilde{M}_{\ell'}|Z^N M_\ell) \\
&= H(\tilde{M}_{\ell'}|Z^N M_\ell) + H(X^N|Z^N M_\ell \tilde{M}_{\ell'}) \\
&\leqq H(\tilde{M}_{\ell'}) + H(X^N|Z^N M_\ell \tilde{M}_{\ell'}) \\
&\leqq^{11} \lambda N + \xi \qquad (51)
\end{aligned}
$$

ここで，$\ell' \neq \ell$ であり，$\tilde{M}_{\ell'}$ は $M_{\ell'}$ の中の λN ビットを取り出したものである．また，$=^{10}$ と $\leqq^{11}$ は下記の理由による．

10: G はランク JK をもつため，X^N から $M = (M_1, M_2, \cdots, M_J)$ が求まる．したがって，$\tilde{M}_{\ell'}$ も求まる．

11: M_ℓ と $\tilde{M}_{\ell'}$ が既知の場合は，G から M_ℓ と $\tilde{M}_{\ell'}$ に対応した列を除いた行列 $\tilde{G}$ で符号化された場合に相当し，この $\tilde{G}$ の符号化レートは，$\frac{(J-1)K - \lambda N}{N} = (J-1)(C_S - \lambda) - \lambda = (C - \xi - C_S + \lambda) - \lambda = C - C_S - \xi = C_Z - \xi$ を満たす．つまり，$\tilde{G}$ の線形符号の符号化レートは，盗聴者の通信路 $X \to Z$ の通信路容量 C_Z より小さい．そのため，N が十分に大きい場合，$\tilde{G}$ で符号化された X^N を盗聴者は任意に小さい復号誤り確率で復号できる[31]．その結果，ファノの不等式[1]より，十分に大きい N で $H(X^N|Z^N M_\ell \tilde{M}_{\ell'}) \leqq \xi$ となる．

式 (50) (51) より，次式が成り立つ．

$$
I(M_\ell; Z^N) \leqq N\xi + \xi \qquad (52)
$$

ランダム線形符号 G の復号誤り確率 P_e は，任意に小さくできるだけでなく，符号化レート R が通信路容量 C より小さい場合，復号誤り指数 $E(R) > 0$ に対して，$P_e \leqq 2^{-NE(R)}$ を満たす[31]．$\tilde{G}$ についても同様である．したがって，ある適切な $a > 0$ に対して，$\xi = 2^{-aN}$ と設定しても上記の議論が成り立ち，N を十分大きくすれば，任意の $\varepsilon > 0$ に対して，式 (43) を満たすことができる．

注 10. 定理 8 では，各 M_ℓ は互いに独立で，$\mathcal{M}_\ell$ 上を一様分布すると仮定した．これらの条件を取り除いたより一般的な符号化定理が証明されている[32]．更に，同様の手法のネットワーク符号化への適用もなされている[33]．

注 11. 図 1 のシャノン暗号システムや図 2，3 の秘密分散通信システムの通信路が無雑音ではなく，雑音のある通信路の場合，シャノン暗号システムや秘密分散通信システムの符号化と盗聴通信路の符号化を組み合わせることにより，安全で効率のよい符号化を行うことができる[34]～[36]．

7. ま と め

本稿では，送信する秘密情報 M を幾つかの部分情報 M_ℓ に分割し，各々の部分情報 M_ℓ に対して完全秘匿を達成することで情報の漏洩に対する安全性を保証し，他方，M 全体に対しては不完全秘匿とすることで，符号化効率を大きく改善する符号化法を紹介した．具体的には，シャノン暗号システム，秘密分散通信システム，秘密分散法，安全なネットワーク符号化，盗聴通信路符号化における具体的な符号化法を示すとともに，その安全性と符号化効率の最適性を理論的に証明した．

本稿では，秘密情報 M を $M = (M_1, M_2, \cdots, M_l)$ に分割するとして，符号化方式を説明したが，逆に，互いに独立な送信情報 $M_1, M_2, \cdots, M_l$ があり，それらを $M = (M_1, M_2, \cdots, M_l)$ とまとめて同時に符号化していると考えることができる．そのような観点で考えると，本稿で紹介した符号化法は，複数の情報の安全な多重符号化法 (secure multiplex coding scheme) とみなすこともできる．

謝辞　閲読者の有益なコメントに対して感謝致します．

文　献

(1) T.M. Cover and J.A. Thomas, Elements of Information Theory, 2nd ed., Wiley, 2006.（山本，古賀，有村，岩本（訳），情報理論 基礎と広がり，共立出版，2012.）

(2) C.E. Shannon, “A mathematical theory of cryptography,” Confidential Report, https:// www.iacr.org/museum/shannon/shannon45.pdf, Sept. 1945.

(3) C.E. Shannon, “Communication theory of secrecy systems,” Bell Sys. Tech. J., vol.28, pp.656–715, Oct. 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x

(4) H. Yamamoto, “Information theory in cryptology,” IEICE Trans. Fundamentals, vol.E74-A, no.9, pp.2456–2464, Sept. 1991.

(5) H. Yamamoto, “On secret sharing communication systems with two or three channels,” IEEE Trans. Inf. Theory, vol.32, no.3, pp.387–393, May 1986. DOI: 10.1109/TIT.1986.1057177

(6) A. Shamir, “How to share a secret,” Commun. ACM,

vol.22, no.11, pp.612–613, Nov. 1979. DOI: 10.1145/359168.359176
(7) E. Karnin, J.W. Greene, and M.E. Hellman, "On secret sharing system," IEEE Trans. Inf. Theory, vol.29, no.1, pp.35–41, Jan. 1983. DOI: 10.1109/TIT.1983.1056621
(8) G.R. Blakley, "Safeguarding cryptographic keys," 1979 International Workshop on Managing Requirements Knowledge (MARK), pp.313–317, June 1979. 10.1109/MARK.1979.8817296
(9) G.R. Blakley and C. Meadows, "Security of ramp schemes," Advances in Cryptology-CRYPTO '84, Lecture Notes in Computer Science, vol.196, pp.242–269, Springer-Verlag, 1985. DOI: 10.1007/3-540-39568-7_20
(10) 山本博資, "(k, L, n) しきい値秘密分散システム," 信学論 (A), vol.J68-A, no.9, pp.945–952, Sept. 1985. [英訳: H. Yamamoto, "Secret sharing system using (k, L, n) threshold scheme", Electronics and Communications in Japan, Part I, vol.69, no.9, pp.46–54, Sept. 1986. DOI: 10.1002/ecja.4410690906]
(11) M. Iwamoto and H. Yamamoto, "Strongly secure ramp secret sharing schemes for general access structures," Information Processing Letters, vol.97, no.2, pp.52–57, Jan. 2006. DOI: 10.1016/j.ipl.2005.09.012
(12) R.J. McEliece and D.V. Sarwate, "On sharing secrets and Reed-Solomon codes," Communications of the ACM, vol.24, no.9, pp.583–584, Sept. 1981. DOI: 10.1145/358746.358762
(13) 西新幹彦, 滝澤克則, "多項式補間法による強いランプ型しきい値秘密分散法," 信会論 (A), vol.J92-A, no.12, pp.1009–1013, Dec. 2009.
(14) J. Kurihara, T. Uyematsu, and R. Matsumoto, "Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized Hamming weight," IEICE Trans. Fundamentals, vol.E95-A, no.11, pp.2067–2075, Nov. 2012. DOI: 10.1587/transfun.E95.A.2067
(15) R. Cramer, I. Damgøard, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," Advances in Cryptology-EUROCRYPT2000, LNCS1807, pp.321–339, May 2000. DOI: 10.1007/3-540-45539-6_22
(16) H. Chen and R. Cramer, "Algebraic geometric secret sharing schemes and secure multi-party computations over small fields," Advances in Cryptology-CRYPT2006, LNCS4117, pp.521–536, 2006.
(17) R. Kikuchi, K. Chida, D. Ikarashi, W. Ogata, K. Hamada, and K. Takahashi, "Secret sharing with share-conversion: Achieving small share-size and extendibility to multiparty computation," IEICE Trans. Fundamentals, vol.E98-A, no.1, pp.213–222, Jan. 2015. DOI: /10.1587/transfun.E98.A.213
(18) R. Ahlswede, N. Cai, S.R. Li, R.W. Yeung, "Network information flow," IEEE Trans. Inf. Theory, vol.46, no.4, pp.1204–1216, July 2000. DOI: 10.1109/18.850663
(19) S.R. Li, R.W. Yeung, N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, vol.49, no.2, pp.371–381, Feb. 2003. DOI: 10.1109/TIT.2002.807285
(20) N. Cai and R.W. Yeung, "Secure network coding," 2002 IEEE Int. Symp. Inform. Theory (ISIT'02), p.323, June 2002. DOI: 10.1109/ISIT.2002.1023595
(21) K. Harada and H. Yamamoto, "Strongly secure linear network coding," IEICE Trans. Fundamentals, vol.E91-A, no.10, pp.2720–2728, Oct. 2008. DOI: 10.1093/ietfec/e91-a.10.2720
(22) A.D. Wyner, "The wire-tap channel," Bell System Technical Journal, vol.54, no.8, pp.1355–1387, Oct. 1975. DOI: 10.1002/j.1538-7305.1975.tb02040.x
(23) I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol.24, no.3, pp.339–348, May 1978. DOI: 10.1109/TIT.1978.1055892
(24) S.K. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," IEEE Trans. Inf. Theory, vol.24, no.4, pp.451–456, July 1978. DOI: 10.1109/TIT.1978.1055917
(25) U. Maurer and S. Wolf, "Information-theoretic key agreement: from weak to strong secrecy for free," Advances in Cryptology-EUROCRYPT2000, LNCS1807, pp.351–368, May 2000. DOI: 10.1007/3-540-45539-6_24
(26) S.K. Leung-Yan-Cheong, "Multi-user and wiretap channels including feedback," Ph. D. Thesis, Department of Electrical Engineering, Stanford University, 1976. (Tech. Rep. No. 6603-2, Stanford Univ., Information Systems Lab., July 1976.)
(27) U.M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol.39, no.3, pp.733–742, May 1993. DOI: 10.1109/18.256484
(28) T.S. Han and S. Verdú, "Approximation theory of output statistics," IEEE Trans. Inf. Theory, vol.39, no.3, pp.752–772, May 1993. DOI: 10.1109/18.256486
(29) M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel," IEEE Trans. Inf. Theory, vol.52, no.4, pp.1562–1575, April 2006. DOI: 10.1109/TIT.2006.871040
(30) D. Kobyayashi, H. Yamamoto, and T. Ogawa, "Secure multiplex coding attaining channel capacity in wiretap channels," IEEE Trans. Inf. Theory, vol.59, no.12, pp.8131–8143, Dec. 2013. DOI: 10.1109/TIT.2013.2282673
(31) A. Barg and G.D. Forney, "Random codes: minimum distance and error exponent," IEEE Trans. Inf. Theory, vol.48, no.9, pp.2568–2573, Sept. 2002. DOI: 10.1109/TIT.2002.800480
(32) M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," IEEE Trans. Inf. Theory, vol.62, no.5, pp.2355–2409, May 2016. DOI: 10.1109/TIT.2016.2530088
(33) R. Matsumoto and M. Hayashi, "Universal secure multiplex coding with dependent and non-uniform multiple messages," IEEE Trans. Inf. Theory, vol.63, no.6, pp.3773–3782, June 20167. DOI: 10.1109/TIT.2017.2694012
(34) H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," IEEE Trans. Inf. Theory, vol.43, no.3, pp.827–835, May 1997. DOI: 10.1109/18.568694
(35) H. Yamamoto, "Coding theorem for secret sharing communication systems with two noisy channels," IEEE Trans. Inf. Theory, vol.35, no.3, pp.572–578, May 1989. DOI: 10.1109/18.30979
(36) H. Yamamoto, "Coding theorem for secret sharing communication systems with two Gaussian wiretap channels," IEEE Trans. Inf. Theory, vol.37, no.3, pp.634–638, Sept. 1991. DOI: 10.1109/18.79919

(幹事団提案, 2022 年 6 月 10 日受付,
2022 年 7 月 11 日再受付)

山本博資 (名誉員：フェロー)

1975 静岡大・工・電気卒. 1980 東大大学院博士課程了. 工博. 徳島大・工, 電通大, 東大・工/情報理工/新領域を経て, 現在, 東大・名誉教授, 早稲田大・基幹理工学・客員教授, 中央大・客員機構教授, 明治大・客員研究員. 情報セキュリティ符号化をはじめとする情報理論全般の研究に従事. 平 21 年度論文賞, 平 29 年度業績賞, 令 2 年度功績賞受賞. IEEE 会員 (Life-Fellow).

解　説　論　文

結合発振器に生じるAmplitude Death
——ロバスト安定性からのアプローチ——

Amplitude Death in Coupled Oscillators :
An Approach from Robust Stability

小西啓治 Keiji KONISHI
杉谷栄規 Yoshiki SUGITANI

アブストラクト　結合発振器に発生する「Amplitude Death」と呼ばれる現象は，非線形科学分野で長年にわたり精力的に研究されている．本解説では，結合発振器における「発振器の数」や「ネットワークの構造」が未知となる状況下でも，システム制御分野で知られている「ロバスト安定性/制御」に関する数理的な解析ツールが，Amplitude Death の発生条件の導出に活用できることを紹介する．具体的には，Amplitude Death を誘発する代表的な結合様式である「動的結合」と「遅延結合」に焦点を絞り，筆者の成果を中心に解説した．

キーワード　振動停止，結合発振器，ロバスト安定性，ネットワーク，不確かさ

Abstract　Amplitude death has been intensively investigated in the field of nonlinear science for almost 40 years. In the present article, we review the use of analytical tools for robust stability/control, which have been provided in the field of system control, to obtain the conditions under which amplitude death occurs when the number of oscillators and the network topologies are unknown. Specifically, we explain our results for two representative couplings for inducing amplitude death, dynamical coupling and delayed coupling.

Key words　Amplitude death, Coupled oscillators, Robust stability, Network, Uncertainty

1. はじめに

複数の発振器が相互に影響を与える「結合発振器」には，興味深い様々な現象が生じる[1],[2]．その中でも，複数の発振器に拡散的な結合を施すことで，それらの発振が「止まる」現象は，1980年代から注目を集め[3]~[6]，その学術的な魅力は現在も色あせていない[7]~[11]．この現象は，「Oscillation Death」と「Amplitude Death」[注1][12]に分類される[8]．Oscillation Death は，発振器に内在する不安定平衡点とは異なる位置に，安定な平衡点が結合によって生まれる現象であり，発振が止まっても，結合信号はゼロとならない．この現象は，結合発振器に生じるチューリングパターンの一種とも解釈できる．一方，Amplitude Death は，発振器に内在していた不安定平衡点が安定化する現象であり，発振が止まると結合信号はゼロとなる．このゼロは，発振器への非侵襲性を意味する．すなわち，小さな結合信号だけで停止状態が維持できる．これは工学的な利点となりうる．本解説では，Amplitude Death に着目する．Amplitude Death は，複数の「同一」である発振器に拡散的な結合を施しても生じない．しかし，結合信号に「時間遅延」が伴えば生じる，との成果が Reddy らによって示された[13]~[15]．この研究を契機とし，結合信号に工夫を施せば Amplitude Death は誘発できるという事例が精力的に報告されてきた[16]~[22]．更に，最近では，時間遅延によって誘発される Amplitude Death に関する研究が，幅広い分野に浸透しつつある．例えば，化学反応系[23]，ロウソクの炎[24]~[27]，熱音響システム[28]~[33]，空力弾性系[34]，反応拡散系[35]などが挙げられる．

システム制御工学分野では，「ロバスト安定性」や「ロバスト制御」に関する研究が大きく進展した．これは，制御対象を記述する数理モデルに含まれる「誤差・不確かさ (不確かなパラメータ)」を考慮してコントローラを設計すると，より頑健な制御系が実現できる，というものである (図 1 左側を参照)．ロバスト制御/安定性に関する重要な研究成果は多数示されている．特に，制御系の安定性を支配する特性式に「不確かさ」が含まれていても，その特性式の安定性の判断に使える数理的な「解析ツール」が存在することは知られている[36],[37]．このツールは，国内でも連載[38]や図書[39]などにまとめられている．ただし，この成果が，非線形科学分野で活用されることは，筆者の知る限り，ほとんどなかった．

本解説では，結合発振器における「発振器の数 (要素数)」や

小西啓治　正員　大阪公立大学大学院工学研究科
E-mail konishi-ees@omu.ac.jp
杉谷栄規　正員　茨城大学工学部
E-mail yoshiki.sugitani.0301@vc.ibaraki.ac.jp
Keiji KONISHI, Member (Graduate School of Engineering, Osaka Metropolitan University, 1-1 Gakuen-cho, Naka-ku, Sakai, Osaka 599-8531 Japan), and Yoshiki SUGITANI, Member (College of Engineering, Ibaraki University, 4-12-1 Nakanarusawa, Hitachi, Ibaraki 316-8511 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.76–82 2022 年 10 月

(注1)：Amplitude Death を日本語に直訳すると「振幅死」となり，本来の意味がつかめない．そこで筆者は，意訳した「振動停止現象」を 2003 年頃から使っている[12]．Amplitude Death と Oscillation Death は，2000 年代まで明確な区別なく使われていたが，2013 年頃から区別されて使われるようになってきた．その結果，筆者が使っていた「振動停止現象」は，その直訳に近い Oscillation Death を意味すると思われても当然だが，そうではない．

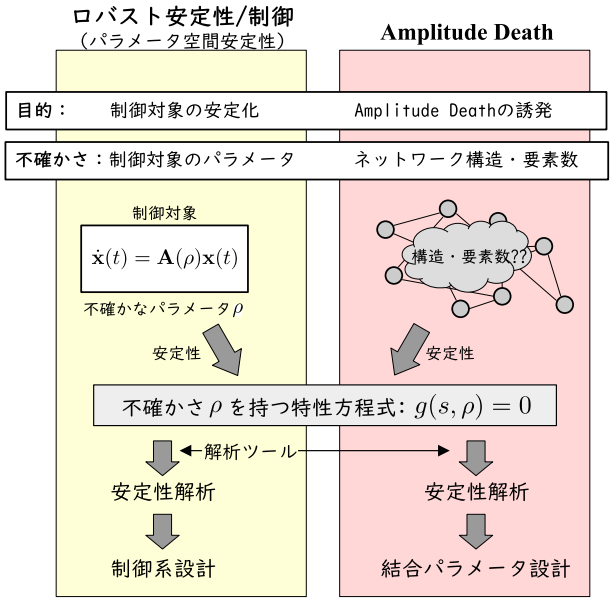


図 1　ロバスト安定性/制御分野と本解説が扱う内容の関係

「ネットワークの構造」の情報が未知であっても，Amplitude Death が発生するための必要条件，すなわち，結合発振器の平衡点の安定条件は，不確かさが伴う特性式で記述することができ，更に，ロバスト安定性に関する数理的な「解析ツール」によって導出できることを，筆者の成果に基づいて紹介する (図 1 右側を参照)．Amplitude Death に関する幾つかの解説論文は，これまでにも出版されている．文献(7), (8) では，2010 年代初頭までの成果がまとめられている．文献(9) は，遅延による安定化現象に焦点を絞り，筆者の成果を中心に紹介した．文献(11) は，結合遅延の不均一性に伴う Amplitude Death や，Death とは異なる振動抑制現象を主に取り上げている．文献(10) では，Amplitude Death に関する多数の研究成果が漏らすことなく整理されている．一方，本解説の目的は，ロバスト安定性に関する知見の一部を簡単に説明し，それが Amplitude Death 発生条件の導出と結合パラメータの設計に活用できることを紹介することである．

本解説は，「動的結合」[40), (41)]が施された発振器に関する成果[42)]を 2. 章で，「遅延結合」[13)]が施された発振器に関する成果[43)]を 3. 章で紹介する．また，他分野の読者にも理解頂くことに重みを置き，できるだけ平易な表現や用語を使うよう心掛けた．そのため，用語や数学的な表現の正確性を犠牲にしている箇所も存在すると思われる．

2.　動的結合発振器ネットワーク

2.1　線形システムの安定性

状態変数 $\mathbf{x}(t) \in \mathbb{R}^m$ をもつ線形なダイナミカルシステム

$$\dot{\mathbf{x}}(t) = \boldsymbol{A}(\rho)\mathbf{x}(t) \tag{1}$$

について考える．行列 $\boldsymbol{A}(\rho) \in \mathbb{R}^{m\times m}$ は，未知の時不変なパラメータ $\rho \in [\rho_-, \rho_+] \subset \mathbb{R}$ から影響を受けているとしよう．ただし，パラメータの下限 ρ_- と上限 ρ_+ は既知とする．システム (1) の安定性は特性式

$$\begin{aligned} g(s,\rho) &= \det\left[s\boldsymbol{I}_m - \boldsymbol{A}(\rho)\right] \\ &= s^m + \alpha_{m-1}(\rho)s^{m-1} + \cdots + \alpha_1(\rho)s + \alpha_0(\rho) \end{aligned} \tag{2}$$

に支配される．当然ながら，特性式の係数 $\alpha_i(\rho)$ $(i = 0, \ldots, m-1)$ は ρ に依存している．すなわち，ρ が未知であれば，システム (1) の安定性は判別できない．

そこで，特性式の集合

$$\mathcal{L}(s) := \{g(s,\rho) : \rho \in [\rho_-, \rho_+]\} \tag{3}$$

について考えよう．この集合に含まれる全ての特性式が安定であれば，未知のパラメータ $\rho \in [\rho_-, \rho_+]$ を伴うシステム (1) は必ず安定であると保証できる．しかし，これら全ての特性式の安定性をしらみつぶしに調査することは現実的でない．ところが，特性式の係数が，ある定数 $r_i, \eta_i \in \mathbb{R}$ によって

$$\alpha_i(\rho) = r_i\rho + \eta_i \ (i = 0, \ldots, m-1) \tag{4}$$

と記述できる場合，集合 (3) は

$$\mathcal{L}(s) = \{\mu g(s,\rho_-) + (1-\mu)g(s,\rho_+) : \mu \in [0,1]\} \tag{5}$$

と表現できる．これは，集合 (3) が，$g(s,\rho_-)$ と $g(s,\rho_+)$ を端点とする線分に対応していることを示している (図 2 参照)．ロバスト安定性を扱う分野で知られている Segment Lemma [36)] は，以下の事実を示している．

二つの特性式 $g(s,\rho_-)$, $g(s,\rho_+)$ がともに安定であり，かつ，全ての

$$f_1(\omega) = 0,\ f_2(\omega) \leqq 0,\ f_3(\omega) \leqq 0 \tag{6}$$

を満足する $\omega > 0$ が存在しなければ，集合 (5) は安定であることが保証される．ただし，f_1, f_2, f_3 は

$$f_1(\omega) := \mathrm{Re}\left[g(j\omega,\rho_-)\right]\mathrm{Im}\left[g(j\omega,\rho_+)\right]/\omega$$

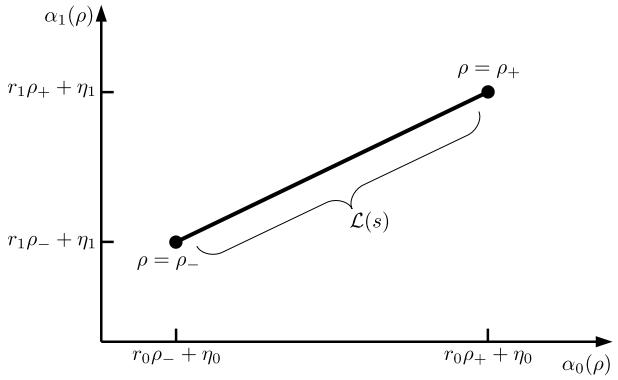


図 2　多項式の係数空間における端点と集合 (5) ($m = 2$ の場合)

$$- \mathrm{Re}\left[g(j\omega,\rho_+)\right]\mathrm{Im}\left[g(j\omega,\rho_-)\right]/\omega, \quad (7)$$

$$f_2(\omega) := \mathrm{Re}\left[g(j\omega,\rho_-)\right]\mathrm{Re}\left[g(j\omega,\rho_+)\right], \quad (8)$$

$$f_3(\omega) := \mathrm{Im}\left[g(j\omega,\rho_-)\right]\mathrm{Im}\left[g(j\omega,\rho_+)\right]/\omega^2 \quad (9)$$

で定義される．

$g(s,\rho_-)$ と $g(s,\rho_+)$ の安定性は簡単に判別できる．$\omega > 0$ が存在しないことは，低次元であれば，解析的に証明できる場合もある．できない場合でも，$\omega > 0$ に対する f_1, f_2, f_3 を数値的にプロットすれば，図的に判別できる．

2.2 動的結合発振器ネットワーク

$N \geqq 2$ 個の発振器

$$\begin{cases} \dot{\boldsymbol{x}}_i = \boldsymbol{F}(\boldsymbol{x}_i) + \boldsymbol{b}u_i \\ y_i = \boldsymbol{c}\boldsymbol{x}_i \end{cases} \quad (i = 1,\ldots,N) \quad (10)$$

について考える．ここで，$\boldsymbol{x}_i \in \mathbb{R}^{m-1}$，$u_i \in \mathbb{R}$, $y_i \in \mathbb{R}$ は，それぞれ i 番めの発振器の状態変数，入力信号，出力信号である．$\boldsymbol{F} : \mathbb{R}^{m-1} \to \mathbb{R}^{m-1}$ は非線形関数であり，発振器には不安定平衡点 $\boldsymbol{x}^* : \boldsymbol{F}(\boldsymbol{x}^*) = \boldsymbol{0}$ が存在している．$\boldsymbol{b} \in \mathbb{R}^{m-1}$, $\boldsymbol{c} \in \mathbb{R}^{1\times(m-1)}$ は入力，出力ベクトルである．これらの発振器に動的結合

$$u_i = k(z_i - y_i),\ \dot{z}_i = \gamma\left\{\frac{1}{d_i}\left[\sum_{l=1}^{N}\varepsilon_{il}y_l\right] - z_i\right\} \quad (11)$$

を施す[40],[43]．ここで，$z_i \in \mathbb{R}$ は結合に追加された変数である．また，$k \in \mathbb{R}$ は結合強度，$\gamma > 0$ はパラメータである．$\varepsilon_{il} \in \{0,1\}$ はネットワークの構造を示している．発振器 i と発振器 l が結合していれば $\varepsilon_{il} = \varepsilon_{li} = 1$ とし，していなければ $\varepsilon_{il} = \varepsilon_{li} = 0$ とする．ただし，$\varepsilon_{ii} = 0$ である．$d_i := \sum_{l=1}^{N}\varepsilon_{il}$ は，発振器 i と結合している発振器の数である．

結合発振器 (10), (11) には一様な平衡点

$$\left[\boldsymbol{x}_1^{\mathsf{T}}\ \cdots\ \boldsymbol{x}_N^{\mathsf{T}}\ z_1\ \cdots\ z_N\right]^{\mathsf{T}} = \left[\boldsymbol{x}^{*\mathsf{T}}\ \cdots\ \boldsymbol{x}^{*\mathsf{T}}\ \boldsymbol{c}\boldsymbol{x}^*\ \cdots\ \boldsymbol{c}\boldsymbol{x}^*\right]^{\mathsf{T}} \quad (12)$$

が存在する．この平衡点近傍の線形近似ダイナミクスは

$$\begin{bmatrix}\dot{\boldsymbol{X}}\\ \dot{\boldsymbol{Z}}\end{bmatrix} = \begin{bmatrix}\boldsymbol{I}_N \otimes \boldsymbol{A}_{\mathrm{d}} & \boldsymbol{I}_N \otimes k\boldsymbol{b}\\ \gamma(\boldsymbol{E}\otimes\boldsymbol{c}) & -\gamma\boldsymbol{I}_N\end{bmatrix}\begin{bmatrix}\boldsymbol{X}\\ \boldsymbol{Z}\end{bmatrix} \quad (13)$$

で表現できる．ただし，$\boldsymbol{X} := \left[\boldsymbol{x}_1{}^{\mathsf{T}} - \boldsymbol{x}^{*\mathsf{T}}\ \cdots\ \boldsymbol{x}_N^{\mathsf{T}} - \boldsymbol{x}^{*\mathsf{T}}\right]^{\mathsf{T}}$, $\boldsymbol{Z} := \left[z_1 - \boldsymbol{c}\boldsymbol{x}^*\ \cdots\ z_N - \boldsymbol{c}\boldsymbol{x}^*\right]^{\mathsf{T}}$, $\boldsymbol{A}_{\mathrm{d}} := \boldsymbol{J} - k\boldsymbol{b}\boldsymbol{c}$ である．$\boldsymbol{J} := \{\partial\boldsymbol{F}(\boldsymbol{x})/\partial\boldsymbol{x}\}_{\boldsymbol{x}=\boldsymbol{x}^*}$ は平衡点 $\boldsymbol{x}^*$ における $\boldsymbol{F}$ のヤコビ行列である．ネットワーク構造を記述する $\boldsymbol{E} \in \mathbb{R}^{N\times N}$ の要素は $\{\boldsymbol{E}\}_{il} = \varepsilon_{il}/d_i$ $(l \neq i)$ と $\{\boldsymbol{E}\}_{ii} = 0$ で与えられる．平衡点 (12) の安定性は，線形システム (13) の安定性と等しい．この安定性を支配する特性式は

$$G(s) := \prod_{i=1}^{N} g(s,\rho_i) \quad (14)$$

$$g(s,\rho) := \det\left[(s+\gamma)(s\boldsymbol{I}_{m-1} - \boldsymbol{A}_{\mathrm{d}}) - \gamma k(1-\rho)\boldsymbol{b}\boldsymbol{c}\right] \quad (15)$$

となる．ここで，ρ_i $(i = 1,\ldots,N)$ は，ネットワークの構造を記述する行列 $(\boldsymbol{I}_N - \boldsymbol{E})$ の固有値であり，以降，未知のパラメータとして扱う．ただし，ネットワークがいかなる構造であっても

$$0 = \rho_1 \leqq \rho_2 \leqq \cdots \leqq \rho_N \leqq 2 \quad (16)$$

が成立することは知られている[44],[45]．

平衡点 (12) が安定であることは，Amplitude Death が生じるための必要条件である．ここでは，2.1 節で紹介した集合 (5) の安定性判別に関する知見 (解析ツール) が，未知のネットワーク構造をもつ結合発振器 (10), (11) の平衡点 (12) の安定性判別にそのまま活用できることを，簡単な二次元リミットサイクル発振器

$$\boldsymbol{F}(\boldsymbol{x}) = \begin{bmatrix}x^{(1)}\left\{1 - x^{(1)2} - x^{(2)2}\right\} - \Omega x^{(2)}\\ x^{(2)}\left\{1 - x^{(1)2} - x^{(2)2}\right\} + \Omega x^{(1)}\end{bmatrix},$$

$$\boldsymbol{b} = \begin{bmatrix}1\\0\end{bmatrix},\ \boldsymbol{c} = \begin{bmatrix}1\\0\end{bmatrix}^{\mathsf{T}} \quad (17)$$

で紹介する[43]．この発振器は，固有周波数が $\Omega > 0$ であり，平衡点 $\boldsymbol{x}^* = \begin{bmatrix}0 & 0\end{bmatrix}^{\mathsf{T}}$ を有する．この発振器に動的結合 (11) を施す．ただし，議論を簡単にするため，結合パラメータは $\gamma = 1$ に固定しておく．平衡点 (12) の安定性が支配される特性式 (14) を構成する特性式 (15) は，$m = 3$ とした多項式 (2) で表現できる．この多項式の係数は

$$\alpha_2(\rho) = k - 1,\ \alpha_1(\rho) = \Omega^2 - 1 + k(\rho - 1),$$
$$\alpha_0(\rho) = \Omega^2 + 1 - k\rho \quad (18)$$

であり，式 (4) で表現できることに気付く．ここでは，発振器の総数 N とネットワーク構造 $\boldsymbol{E}$ は未知とする．これは，行列 $(\boldsymbol{I}_N - \boldsymbol{E})$ の固有値 ρ_i を未知のパラメータとして扱うことに等しい．また，式 (16) の制約により，未知パラメータの上下限は $\rho_- = 0$, $\rho_+ = 2$ となる．

係数 (18) を伴う二つの特性式 $g(s,0)$, $g(s,2)$ がともに安定となる必要十分条件は，以下の全ての不等式が満足されることである[40]: (a) $1 + \Omega^2 - 2k > 0$, (b) $1 - \Omega^2 - k < 0$, (c) $1 - \Omega^2 + k < 0$, (d) $k > 1$, (e) $k^2 + \Omega^2 k - 2\Omega^2 > 0$, (f) $k^2 - \Omega^2 k + 2\Omega^2 < 0$．ここでは，これらを満足する k, Ω を選んでおく．次に，$g(j\omega,0)$, $g(j\omega,2)$ の実部・虚部を式 (7) に代入すると，$f_1(\omega) = 0$ を満足する $\omega = \sqrt{-1 + 2\Omega^2/k} > 0$ が得られる．これを式 (9) に代入すると，$f_3(\omega) \leqq 0$ は満足しないことが，不等式 (e), (f) から簡単に説明できる．結論として，上記の不等式 (a)〜(f) を満足するように k, Ω を設定しておけば，発振器数やネットワークの構造が特定できなくても，平衡点 (12) は安定化されることが保証される．

設計されたパラメータをもつ動的結合により Amplitude Death が生じることを数値シミュレーションで確認しよう．$k = 3$, $\Omega = 2\pi$ のとき，上記の不等式 (a)〜(f) は全て満足され

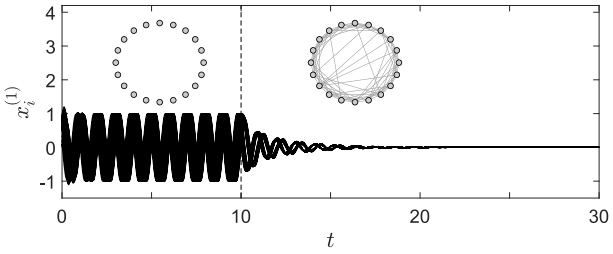


図 3　二次元リミットサイクル発振器 (17) に動的結合 (11) を施す前と施した後の時系列データ
$N = 20$，スモールワールドネットワーク構造．

る．数値例では，$N = 20$ のスモールワールドネットワーク構造を使用する．図 3 に，全発振器の第 1 成分の時系列データ $x_i^{(1)}$ $(i = 1, \ldots, 20)$ を示す．20 個の発振器は，$t = 10$ まで独立して発振している（$u_i \equiv 0$）．$t = 10$ で動的結合が施されると，全発振器の第 1 成分 $x_i^{(1)}$ が平衡点へ収束している．これにより，Amplitude Death の発生が確認できる．

筆者らは先行研究[42]で，レスラー発振器にも上記のアプローチを試みている．更に，多項式の実凸方向という概念を活用して，結合の設計に焦点を絞り議論した[46]．

3.　遅延結合発振器ネットワーク

3.1　線形遅延システムの安定性

時間 $\tau \geqq 0$ だけ過去の状態変数 $\mathbf{x}(t-\tau) \in \mathbb{R}^m$ をもつ線形なダイナミカルシステム

$$\dot{\mathbf{x}}(t) = \boldsymbol{A}(\rho)\mathbf{x}(t) + \boldsymbol{A}_\tau(\rho)\mathbf{x}(t-\tau) \tag{19}$$

について考える．システム (19) の安定性は特性式

$$\begin{aligned} &g(s,\rho) \\ &\quad = \det\left[s\boldsymbol{I}_m - \boldsymbol{A}(\rho) - \boldsymbol{A}_\tau(\rho)e^{-s\tau}\right] \\ &\quad = s^m + \alpha_{m-1}(\rho)s^{m-1} + \cdots + \alpha_1(\rho)s + \alpha_0(\rho) \\ &\qquad + \left\{s^m + \beta_{m-1}(\rho)s^{m-1} + \cdots + \beta_1(\rho)s + \beta_0(\rho)\right\}e^{-s\tau} \end{aligned} \tag{20}$$

に支配される．特性式の係数 α_i, β_i が，未知のパラメータ ρ に対して，式 (4) のように表現できれば，特性式の集合 $\mathcal{L}(s)$ は式 (5) で記述できる．文献(47) は，以下の事実を示している．

二つの特性式 $g(s,\rho_-)$, $g(s,\rho_+)$ がともに安定であり，かつ，

$$\phi(\omega) \neq \pm\pi,\ \forall\omega \in [0,+\infty) \tag{21}$$

が満足されていれば，特性式 (20) から構成される集合 (5) は安定であることが保証される．ただし，$\phi(\omega)$ は

$$\phi(\omega) := \mathrm{Arg}\left[g(j\omega,\rho_-)\right] - \mathrm{Arg}\left[g(j\omega,\rho_+)\right] \tag{22}$$

で定義される．

3.2　遅延結合発振器ネットワーク

$N \geqq 2$ 個の発振器

$$\dot{\boldsymbol{x}}_i = \boldsymbol{F}(\boldsymbol{x}_i) + \boldsymbol{b}u_i\ (i = 1, \ldots, N) \tag{23}$$

について考える．これらの発振器に遅延結合

$$u_i(t) = \boldsymbol{k}^{\mathsf{T}}\left\{\frac{1}{d_i}\left[\sum_{l=1}^{N}\varepsilon_{il}\boldsymbol{x}_l(t-\tau)\right] - \boldsymbol{x}_i(t)\right\} \tag{24}$$

を施す[43] (注2)．$\boldsymbol{k} \in \mathbb{R}^{m-1}$ は結合強度，$\tau \geqq 0$ は結合遅延である．結合発振器 (23), (24) には一様な平衡点

$$\left[\boldsymbol{x}_1^{\mathsf{T}}\ \cdots\ \boldsymbol{x}_N^{\mathsf{T}}\right]^{\mathsf{T}} = \left[\boldsymbol{x}^{*\mathsf{T}}\ \cdots\ \boldsymbol{x}^{*\mathsf{T}}\right]^{\mathsf{T}} \tag{25}$$

が存在する．この平衡点近傍の線形近似ダイナミクスは

$$\dot{\boldsymbol{V}}(t) = \left(\boldsymbol{I}_N \otimes \bar{\boldsymbol{A}}^*\right)\boldsymbol{V}(t) + \left(\boldsymbol{E} \otimes \bar{\boldsymbol{b}}\bar{\boldsymbol{k}}^{\mathsf{T}}\right)\boldsymbol{V}(t-\tau) \tag{26}$$

と等価である．ここで，$\bar{\boldsymbol{A}}^* := \bar{\boldsymbol{J}} - \bar{\boldsymbol{b}}\bar{\boldsymbol{k}}^{\mathsf{T}}$, $\boldsymbol{V} := \left[\boldsymbol{v}_1^{\mathsf{T}}\ \cdots\ \boldsymbol{v}_N^{\mathsf{T}}\right]^{\mathsf{T}}$, $\boldsymbol{v}_i := \boldsymbol{\Gamma}^{-1}(\boldsymbol{x}_i - \boldsymbol{x}^*)$ である．ただし，$\boldsymbol{\Gamma}$ は，$\boldsymbol{J}, \boldsymbol{b}$ を可制御正準系 $\bar{\boldsymbol{J}} := \boldsymbol{\Gamma}^{-1}\boldsymbol{J}\boldsymbol{\Gamma}$, $\bar{\boldsymbol{b}} := \boldsymbol{\Gamma}^{-1}\boldsymbol{b}$ に変換する変換行列である．また，$\bar{\boldsymbol{k}}^{\mathsf{T}} = \left[\bar{k}_{m-1}\ \cdots\ \bar{k}_1\right]^{\mathsf{T}} := \boldsymbol{k}^{\mathsf{T}}\boldsymbol{\Gamma}$ である．

遅延を伴う線形システム (26) の特性式は，式 (14) となる．ただし，それを構成する $g(s,\rho)$ は

$$g(s,\rho) = d(s) + n(s)\left\{1 - e^{-s\tau}(1-\rho)\right\} \tag{27}$$

である．多項式 $d(s), n(s)$ は

$$\begin{aligned} d(s) &:= \det\left[s\boldsymbol{I}_{m-1} - \boldsymbol{J}\right] = \det\left[s\boldsymbol{I}_{m-1} - \bar{\boldsymbol{J}}\right] \\ &= s^{m-1} + a_1 s^{m-2} + \cdots + a_{m-2}s + a_{m-1} \end{aligned} \tag{28}$$

$$\begin{aligned} n(s) &:= \bar{\boldsymbol{k}}^{\mathsf{T}}\mathrm{adj}\left(s\boldsymbol{I}_{m-1} - \bar{\boldsymbol{J}}\right)\bar{\boldsymbol{b}} \\ &= \bar{k}_1 s^{m-1} + \bar{k}_2 s^{m-2} + \cdots + \bar{k}_{m-1}s + \bar{k}_m \end{aligned} \tag{29}$$

で与えられる．特性式 (27) の係数は，未知パラメータである固有値 ρ に対して，式 (4) のように表現できているため，特性式の集合 $\mathcal{L}(s)$ は，特性式 (27) から構成される式 (5) で記述できる．

3.3　$\boldsymbol{k}$ と τ の設計と数値例

この節では，いかなる「発振器の数」や「ネットワークの構造」であっても平衡点 (25) が安定となる結合強度 $\boldsymbol{k}$ と結合遅延 τ を設計する[43]．ただし，ヤコビ行列 $\boldsymbol{J}$ は，不安定な 2 個の固有値 λ_1, λ_2 と安定な $m-3$ 個の固有値をもつと仮定する．この仮定が成立していれば，以下の設計手順が使える．

Step 0　$(\boldsymbol{J}, \boldsymbol{b})$ は既知だが，N と $\boldsymbol{E}$ は未知である．

Step 1　$(\boldsymbol{J}, \boldsymbol{b})$ が可制御，かつ $a_1 := -(\lambda_1 + \lambda_2) < 0$ と $a_2 := \lambda_1\lambda_2 > 0$ が満足されていれば，次のステップへ

(注2)：2. 2 節の発振器 (10) では，出力信号 y_i を通じて結合を施していた．本章では，議論を簡単にするため，過去の状態 $\boldsymbol{x}_l(t-\tau)$ を通じて結合を施している．

進み，そうでなければ設計を終了する．

Step 2　$\bar{k}_1, \bar{k}_2, \tau$ を付録 A に沿って設計する．

Step 3　$d_{\rm s}(s) = d(s)/d_{\rm u}(s)$ を求める．ただし，$d_{\rm u}(s) = (s-\lambda_1)(s-\lambda_2)$ である．

Step 4　上記で設計した $\bar{k}_1$, $\bar{k}_2$ から $\sigma_1 = \bar{k}_1$, $\sigma_2 = \bar{k}_2$ とする．

Step 5　$\bar{k}_1 s^{m-2} + \bar{k}_2 s^{m-3} + \cdots + \bar{k}_{m-2} s + \bar{k}_{m-1} = d_{\rm s}(s)(\sigma_1 s + \sigma_2)$ が成立するように，$\bar{k}_i$ $(i = 1, \ldots, m-1)$ を定め，$\bar{\boldsymbol{k}}^{\mathsf{T}}$ を得る．

Step 6　$\boldsymbol{k}^{\mathsf{T}} = \bar{\boldsymbol{k}}^{\mathsf{T}} \boldsymbol{\Gamma}^{-1}$ を得る．

上記の **Step 2** で得られた遅延時間 τ と **Step 6** で得られた結合強度 $\boldsymbol{k}$ は，3.1 節で紹介した線形遅延システムの安定性に関する知見 (解析ツール) で示された「$g(s, \rho_- = 0), g(s, \rho_+ = 2)$ が安定」と「条件 (21)」をともに満足する(注3)．したがって，設計した $\boldsymbol{k}$ と τ を使えば，いかなる「発振器数」や「ネットワーク構造」であっても，平衡点 (25) は安定となることが保証される．

これらの手順を，三次元の Moore-Spiegel 発振器[48],[49] $(m = 4)$

$$\boldsymbol{F}(\boldsymbol{x}_i) = \begin{bmatrix} x_i^{(2)} \\ x_i^{(3)} \\ -x_i^{(3)} - \left[0.1 - 1.1 + 1.1\left\{x_i^{(1)}\right\}^2\right] x_i^{(2)} - 0.1 x_i^{(1)} \end{bmatrix},$$
$$\boldsymbol{b} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix}^{\mathsf{T}} \qquad (30)$$

が伴う遅延結合発振器 (23), (24) で検証する．この発振器には平衡点 $\boldsymbol{x}^* = \boldsymbol{0}$ と安定なリミットサイクルが共存する．ただし，この平衡点におけるヤコビ行列 $\boldsymbol{J}$ は，2 個の正の実固有値(注4) と，1 個の負の実固有値をもつ．上記で示した設計手順を追ってみよう[43]．

Step 0　ヤコビ行列 $\boldsymbol{J}$ を計算し，$\boldsymbol{b}$ は式 (30) で与えられている．N と $\boldsymbol{E}$ は未知とする．

Step 1　$(\boldsymbol{J}, \boldsymbol{b})$ が可制御であることは確認できた．$\boldsymbol{J}$ の固有値は $\lambda_1 = 0.5302$, $\lambda_2 = 0.1147$, $\lambda_3 = -1.6449$ である．$a_1 = -0.6449 < 0$ と $a_2 = 0.0608 > 0$ が確認できたため，次のステップへ進む．

Step 2　付録 A に沿って $\bar{k}_1 = 2.0$, $\bar{k}_2 = 0.7$, $\tau = 1.0$ を得た．

Step 3　$d_{\rm s}(s) = s + 1.6449$ を得た．

Step 4　$\sigma_1 = 2.0$, $\sigma_2 = 0.7$ とした．

Step 5　$\bar{\boldsymbol{k}}^{\mathsf{T}} = \begin{bmatrix} 1.1514 & 3.9898 & 2.0000 \end{bmatrix}$ を得た．

Step 6　$\boldsymbol{k}^{\mathsf{T}} = \begin{bmatrix} 1.2276 & 2.0000 & 0.7622 \end{bmatrix}$ を得た．

上記の手順で得た $\boldsymbol{k}$ と τ が伴う遅延結合 (24) を施した発振器 (23) に内在する不安定平衡点 (25) は，いかなる発振器数 N やネットワーク構造 $\boldsymbol{E}$ であっても，安定であることが保証されている．この結果を，3 種類の設定で数値的に確認しよう．

1 つめは，$N = 2$ と設定した．図 4 (a) は，2 個の発振器の第 1 成分 $x_1^{(1)}$, $x_1^{(2)}$ の時系列データである．2 個の発振器は $t = 100$ まで結合せず $(u_i \equiv 0)$ に独立して発振している．遅延結合が $t \geqq 100$ で施されると，両発振器の第 1 成分は同期しつつゼロに収束している．これは，平衡点 (25) の安定化により生じる Amplitude Death である．2 つめの設定では，$N = 8$ 個の発振器に全結合を施した．図 4 (b) は，奇数番めの発振器の時系列データである．ただし，図 4 (a) と同じ $\boldsymbol{k}$ と τ を用いており，発振器数とネットワークの構造を変化させただけである．図 4 (b) でも，Amplitude Death の発生が確認できる．3 つめの設定では，$N = 10$ 個の発振器にリング結合を施した．図 4 (c) は，奇数番めの発振器の時系列データである．この設定でも，ほかの設定と同様に Amplitude Death の発生が確認できた．これらのシミュレーション結果は，上記の手順で得た $\boldsymbol{k}$ と τ は，いかなる発振器の数 N やネットワークの構造 $\boldsymbol{E}$ であっても，平衡点の安定化に有効であることを裏付けている．

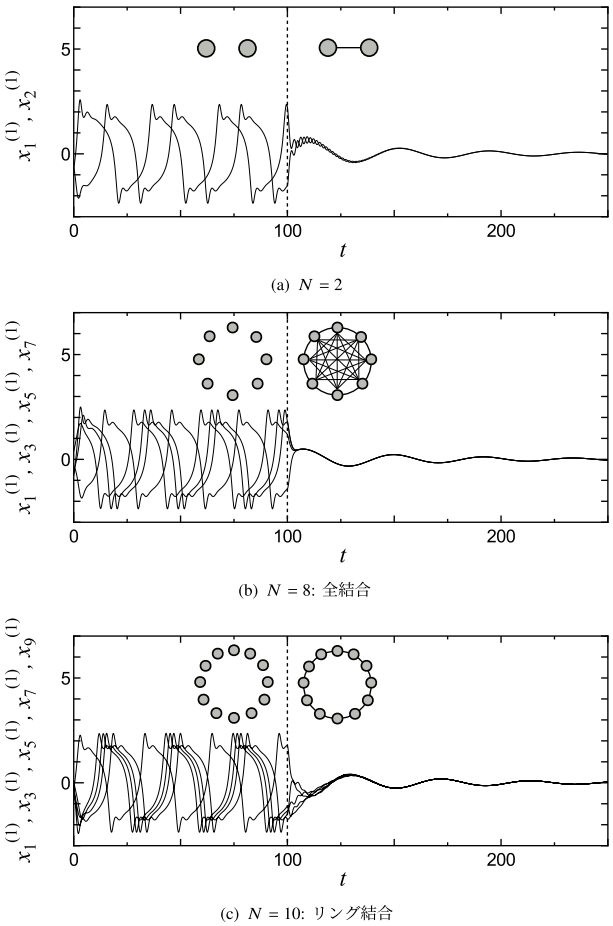


図 4　Moore-Spiegel (30) 発振器に遅延結合 (24) を施す前と施した後の時系列データ　(a) $N = 2$, (b) 全結合 ($N = 8$), (c) リング結合 ($N = 10$).

4. ま と め

本解説では，発振器の数 N やネットワークの構造 $\boldsymbol{E}$ が未知であっても，結合発振器の平衡点を確実に安定化させる結合パラメータなどが，ロバスト安定性に関する数理的な解析ツールによって設計できることを紹介した．現在のところ，結合発振

(注3)：詳しい導出過程は文献(43) を参照して欲しい．

(注4)：Amplitude Death を扱っているほぼ全ての先行研究では，複素共役な不安定固有値をもつ発振器が研究対象とされている．本解説で扱う成果は，それだけでなく，2 個の不安定実固有値の場合でも有効である．

器などを研究対象とする非線形科学分野では，これら解析ツールのほんの一部しか使われていないようである．解析ツールを非線形科学分野やネットワーク科学分野で有効に活用することが今後の課題として挙げられる．

謝辞　本解説では，JSPS 科研費 (26289131) の助成を受けた成果の一部を紹介しています．また，常日頃からご議論頂いている共同研究者の大阪公立大学原尚之先生，並びにロバスト安定性という考え方やそれに関する知見をご教示くださった大阪府立大学名誉教授小亀英己先生に感謝の意を表します．

文　献

(1) G.V. Osipov, J. Kurths, and C. Zhou, Synchronization in Oscillatory Networks, Springer, 2007.
(2) S. Boccaletti, A.N. Pisarchik, C.I. del Genio, and A. Amann, Synchronization, Cambridge University Press, 2018.
(3) Y. Yamaguchi and H. Shimizu, "Theory of self-synchronization in the presence of native frequency distribution and external noises," Physica D, vol.11, nos.1-2, pp.212–226, 1984.
(4) K. Bar-Eli, "On the stability of coupled chemical oscillators," Physica D, vol.14, no.2, pp.242–252, 1985.
(5) R.E. Mirollo and S.H. Strogatz, "Amplitude death in an array of limit-cycle oscillators," Journal of Statistical Physics, vol.60, nos.1-2, pp.245–262, 1990.
(6) D.G. Aronson, G.B. Ermentrout, and N. Kopell, "Amplitude response of coupled oscillators," Physica D, vol.41, no.3, pp.403–449, 1990.
(7) G. Saxena, A. Prasad, and R. Ramaswamy, "Amplitude death: The emergence of stationarity in coupled nonlinear systems," Physics Reports, vol.521, no.5, pp.205–228, 2012.
(8) A. Koseska, E. Volkov, and J. Kurths, "Oscillation quenching mechanisms: Amplitude vs. oscillation death," Physics Reports, vol.531, no.4, pp.173–199, 2013.
(9) 小西啓治，杉谷栄貴，"遅延フィードバック・遅延結合による非線形システムの安定化," 計測と制御，vol.55, no.4, pp.326–334, 2016.
(10) W. Zou, D.V. Senthilkumar, M. Zhan, and J. Kurths, "Quenching, aging, and reviving in coupled dynamical networks," Physics Reports, vol.931, pp.1–72, 2021.
(11) Y. Sugitani and K. Konishi, "Delay-induced stabilization of coupled oscillators," NOLTA, vol.12, no.4, pp.612–624, 2021.
(12) 小西啓治，"動的結合に伴う振動停止現象の安定性解析，" 信学技報，NLP103–185, 2003.
(13) D.V. Ramana Reddy, A. Sen, and G.L. Johnston, "Time delay induced death in coupled limit cycle oscillators," Phys. Rev. Lett., vol.80, no.23, pp.5109–5112, 1998.
(14) D.V. Ramana Reddy, A. Sen, and G.L. Johnston, "Time delay effects on coupled limit cycle oscillators at Hopf bifurcation," Physica D, vol.129, nos.1-2, pp.15–34, 1999.
(15) D.V.R. Reddy, A. Sen, and G.L. Johnston, "Experimental evidence of time-delay-induced death in coupled limit-cycle oscillators," Phys. Rev. Lett., vol.85, no.16, pp.3381–3384, 2000.
(16) F.M. Atay, "Distributed delays facilitate amplitude death of coupled oscillators," Phys. Rev. Lett., vol.91, no.9, p.94101, 2003.
(17) Y.N. Kyrychko, K.B. Blyuss, and E. Schöll, "Amplitude and phase dynamics in oscillators with distributed-delay coupling," Phil. Trans. Roy. Soc. A, vol.371, no.1999, p.20120466, 2013.
(18) W. Zou and M. Zhan, "Partial time-delay coupling enlarges death island of coupled oscillators," Phys. Rev. E, vol.80, no.6, p.65204, 2009.
(19) K. Konishi, H. Kokame, and N. Hara, "Stabilization of a steady state in network oscillators by using diffusive connections with two long time delays," Phys. Rev. E, vol.81, no.1, p.16201, 2010.
(20) K. Konishi, L.B. Le, and N. Hara, "Stability analysis of a steady state in oscillators coupled by a digital delayed connection," Eur. Phys. J. B, vol.85, no.5, p.166, 2012.
(21) A. Gjurchinovski, A. Zakharova, and E. Schöll, "Amplitude death in oscillator networks with variable-delay coupling," Phys. Rev. E, vol.89, no.3, p.32915, 2014.
(22) Y. Sugitani, K. Konishi, and N. Hara, "Delay- and topology-independent design for inducing amplitude death on networks with time-varying delay connections," Phys. Rev. E, vol.92, no.4, p.42928, 2015.
(23) W. Zou, D.V. Senthilkumar, R. Nagao, I.Z. Kiss, Y. Tang, A. Koseska, J. Duan, and J. Kurths, "Restoration of rhythmicity in diffusively coupled dynamical networks," Nature Communications, vol.6, no.1, p.7709, 2015.
(24) K. Okamoto, A. Kijima, Y. Umeno, and H. Shima, "Synchronization in flickering of three-coupled candle flames," Scientific Reports, vol.6, no.1, p.36145, 2016.
(25) K. Manoj, S.A. Pawar, and R.I. Sujith, "Experimental evidence of amplitude death and phase-flip bifurcation between in-phase and anti-phase synchronization," Scientific Reports, vol.8, no.1, p.11626, 2018.
(26) K. Manoj, S.A. Pawar, S. Dange, S. Mondal, R.I. Sujith, E. Surovyatkina, and J. Kurths, "Synchronization route to weak chimera in four candle-flame oscillators," Phys. Rev. E, vol.100, no.6, p.62204, 2019.
(27) K. Manoj, S.A. Pawar, and R.I. Sujith, "Experimental investigation on the susceptibility of minimal networks to a change in topology and number of oscillators," Phys. Rev. E, vol.103, no.2, p.22207, 2021.
(28) T. Biwa, S. Tozuka, and T. Yazaki, "Amplitude death in coupled thermoacoustic oscillators," Phys. Rev. Appl., vol.3, no.3, p.34006, 2015.
(29) H. Hyodo and T. Biwa, "Stabilization of thermoacoustic oscillators by delay coupling," Phys. Rev. E, vol.98, no.5, p.052223, 2018.
(30) N. Thomas, S. Mondal, S.A. Pawar, and R.I. Sujith, "Effect of time-delay and dissipative coupling on amplitude death in coupled thermoacoustic oscillators," Chaos, vol.28, no.3, p.033119, 2018.
(31) S. Dange, K. Manoj, S. Banerjee, S.A. Pawar, S. Mondal, and R.I. Sujith, "Oscillation quenching and phase-flip bifurcation in coupled thermoacoustic systems," Chaos, vol.29, no.9, p.93135, 2019.
(32) H. Hyodo, M. Iwasaki, and T. Biwa, "Suppression of Rijke tube oscillations by delay coupling," J. Appl. Phys., vol.128, no.9, p.094902, 2020.
(33) K. Moon, Y. Guan, L.K.B. Li, and K.T. Kim, "Mutual synchronization of two flame-driven thermoacoustic oscillators: Dissipative and time-delayed coupling effects," Chaos, vol.30, no.2, p.23110, 2020.
(34) A. Raaj, S. Mondal, and V. Jagdish, "Investigating amplitude death in a coupled nonlinear aeroelastic system," Int. J. Non-Linear Mech., vol.129, p.103659, 2021.
(35) H. Teki, K. Konishi, and N. Hara, "Amplitude death in a pair of one-dimensional complex Ginzburg-Landau systems coupled by diffusive connections," Phys. Rev. E, vol.95, no.6, p.62220, 2017.
(36) S.P. Bhattacharyya, H. Chapellat, and L.H. Keel, Robust Control: The Parametric Approach, Prentice Hall PTR, 1995.
(37) B.R. Barmish, New Tools for Robustness of Linear Systems, Prentice Hall PTR, 1994.

(38) 森武宏，小亀英己，“パラメータ空間における多項式安定性理論の基礎 I,” システム/制御/情報，vol.40, no.6, pp.459–465, 1996.
(39) 木村英紀，藤井隆雄，森武宏，ロバスト制御，コロナ社，1994.
(40) K. Konishi, “Amplitude death induced by dynamic coupling,” Phys. Rev. E, vol.68, no.6, p.67202, 2003.
(41) K. Konishi, “Amplitude death induced by a global dynamic coupling,” International Journal of Bifurcations and Chaos, vol.17, no.8, pp.2781–2789, 2007.
(42) K. Konishi and N. Hara, “Topology-free stability of a steady state in network systems with dynamic connections,” Phys. Rev. E, vol.83, no.3, p.36204, 2011.
(43) Y. Sugitani, K. Konishi, L.B. Le, and N. Hara, “Design of time-delayed connection parameters for inducing amplitude death in high-dimensional oscillator networks,” Chaos, vol.24, no.4, p.43105, 2014.
(44) F.R.K. Chung, Spectral Graph Theory, American Mathematical Society, 1997.
(45) F.M. Atay, “Oscillator death in coupled functional differential equations near Hopf bifurcation,” Journal of Differential Equations, vol.221, no.1, pp.190–209, 2006.
(46) 小西啓治，原尚之，“動的結合ネットワークの振動停止現象を誘発する結合パラメータの設計,” 信学技報，NLP2012–90, 2012.
(47) H. Hu and Z. Wang, Dynamics of Controlled Mechanical Systems with Delayed Feedback, Springer, 2002.
(48) D.W. Moore and E.A. Spiegel, “A thermally excited nonlinear oscillator,” The Astrophysical Journal, vol.143, pp.871–887, 1966.
(49) N.J. Balmforth and R.V. Craster, “Synchronizing Moore and Spiegel,” Chaos, vol.7, no.4, pp.738–752, 1997.

付　　録

A. $\bar{k}_{1,2}$ と τ の設定手順

本付録では，$\bar{k}_{1,2}$ と τ の設定手順[43]を紹介する．$\bar{k}_{1,2}$ は，

$$a_1+\bar{k}_1>0,\ a_2+2\bar{k}_2>0,\ c_1^2-4c_2>0 \tag{A·1}$$

$$\psi_\alpha/\omega_\alpha<\psi_\beta/\omega_\beta,\ (\psi_\alpha-\pi)/\omega_\alpha<0<(\psi_\beta-\pi)/\omega_\beta \tag{A·2}$$

を満足するように選ぶ．ただし，

$$c_1:=a_1\left(a_1+2\bar{k}_1\right)-2\left(a_2+\bar{k}_2\right),\ c_2:=a_2\left(a_2+2\bar{k}_2\right) \tag{A·3}$$

$$\omega_\alpha:=\sqrt{\frac{-c_1-\sqrt{c_1^2-4c_2}}{2}},\ \omega_\beta:=\sqrt{\frac{-c_1+\sqrt{c_1^2-4c_2}}{2}} \tag{A·4}$$

$$\psi_{\alpha,\beta}:=\mathrm{Arg}\left(\frac{\bar{k}_2+j\omega_{\alpha,\beta}\bar{k}_1}{a_2+\bar{k}_2-\omega_{\alpha,\beta}^2+j\omega_{\alpha,\beta}(a_1+\bar{k}_1)}\right) \tag{A·5}$$

である．次に，遅延時間 τ を区間 $\Lambda^{(0)}\cap\Lambda^{(2)}$ から選ぶ．ただし，

$$\Lambda^{(0)}:=\left\{\tau\in\left(\tau_\alpha^{(0)}[l],\tau_\beta^{(0)}[l]\right),\ l=0,1,\ldots,\left\lfloor\frac{\omega_\alpha\psi_\beta-\omega_\beta\psi_\alpha}{2\pi(\omega_\beta-\omega_\alpha)}\right\rfloor\right\} \tag{A·6}$$

$$\Lambda^{(2)}:=\left\{\tau\in\left[0,\tau_\beta^{(2)}[0]\right),\ \tau\in\left(\tau_\alpha^{(2)}[l],\tau_\beta^{(2)}[l]\right),\ l=1,\ldots,\left\lfloor\frac{\omega_\alpha\psi_\beta-\omega_\beta\psi_\alpha+\pi\left(\omega_\beta-\omega_\alpha\right)}{2\pi(\omega_\beta-\omega_\alpha)}\right\rfloor\right\} \tag{A·7}$$

$$\tau_\alpha^{(0)}[l]:=\frac{\psi_\alpha}{\omega_\alpha}+\frac{2\pi}{\omega_\alpha}l,\ \tau_\beta^{(0)}[l]:=\frac{\psi_\beta}{\omega_\beta}+\frac{2\pi}{\omega_\beta}l \tag{A·8}$$

$$\tau_\alpha^{(2)}[l]:=\frac{\psi_\alpha}{\omega_\alpha}-\frac{\pi}{\omega_\alpha}+\frac{2\pi}{\omega_\alpha}l,\ \tau_\beta^{(2)}[l]:=\frac{\psi_\beta}{\omega_\beta}-\frac{\pi}{\omega_\beta}+\frac{2\pi}{\omega_\beta}l \tag{A·9}$$

である．

（NLP 研究会提案，2022 年 6 月 2 日受付）

小西啓治（正員）

1991 大阪府立大学工学部卒．1993 同大学大学院工学研究科博士前期課程修了．同年国立奈良工業高等専門学校助手．1995 大阪府立大学工学部助手．2002 公立はこだて未来大学システム情報科学部助教授．2006 大阪府立大学大学院工学研究科助教授 (准教授)．2009 同教授．2022 大阪公立大学大学院工学研究科教授，現在に至る．複雑系科学とシステム制御の研究に従事．米国物理学会，日本物理学会，IEEE，システム制御情報学会，計測自動制御学会，電気学会，各正会員．2008 電子情報通信学会 Fundamentals Review 編集委員会幹事．2014 電子情報通信学会非線形問題研究専門委員会委員長．2019 システム制御情報学会編集委員長．博士 (工学)．

杉谷栄規（正員）

2013 大阪府立大学大学院工学研究科博士前期課程修了．2014 日本学術振興会特別研究員 DC2．2016 同博士後期課程修了．同年茨城大学工学部助教．2019 Northwestern 大学客員研究員．2022 茨城大学工学部講師，現在に至る．振動停止現象の理論解析・回路実験に関する研究に従事．博士 (工学)．

解　説　論　文

説明可能AI技術のこれまでとこれから

The Past and the Future of Explainable AI Techniques

亀谷由隆 Yoshitaka KAMEYA

アブストラクト　現在注目される人工知能技術は高い予測性能をもつ機械学習モデルが主体となっており，これらのモデルを健康や財産に関わる分野へ応用する試みも始まっている．しかし，その際の問題の一つがモデルの不透明性であり，このような不透明性を軽減するための一連の技術が近年「説明可能 AI (explainable artificial intelligence, XAI)」という研究分野を形成している．本稿では XAI 研究の流れを振り返り，現在行われている XAI 研究における概念と手法の分類や整理を行うとともに，XAI 研究における将来の課題について述べる．

キーワード　説明可能 AI，XAI，機械学習，深層学習

Abstract　Machine learning models of high predictive performance, such as deep neural networks and ensemble models, now play a central role in the current artificial intelligence technologies and have started to be applied to the problems related to our health or properties. However, one of the primary obstacles here is the opacity of such high-performance models. So far, dozens of techniques for reducing the opacity have been explored, and form a research field called "explainable aritificial intelligence (XAI)." In this paper, I review the past literature on XAI, organize key concepts and techniques in the current XAI research, and discuss the future direction of XAI.

Key words　Explainable AI, XAI, Machine learning, Deep learning

1. はじめに

現在注目される人工知能技術は高い予測性能をもつ機械学習モデルが主体となっており，これらのモデルを健康や財産に関わる分野へ応用する試みも始まっている．しかし，その際の問題の一つがモデルの不透明性であり，このような不透明性を軽減するための一連の技術が近年「説明可能 AI (explainable artificial intelligence, XAI)」という研究分野を形成している．筆者の記憶では「説明可能 AI」という用語が広く使われるようになったきっかけは 2017 年開始の同名の DARPA プログラム[(1)]である．また，最近ではクラウドサービスの一つとして XAI 技術が提供され始めている[(2)]．日本語の解説文献[(3)~(8)]も出版・公開されてきている．本稿では既存のサーベイ論文[(3)，(9)~(13)]の記述をベースとしながら XAI 研究の流れを振り返り，現在進行中の XAI 研究における概念と手法の分類や整理を行うとともに，XAI 研究の将来課題について述べる．

本稿は以下の構成を取る[(注1)]．まず 2. 節で XAI に関連する過去の研究の流れを振り返り，次に 3. 節では XAI 技術の目的と関連概念について述べる．4. 節で現在研究が進む XAI 技術を分類・整理しながら紹介する．また，5. 節で XAI 研究の将来課題について述べる．最後に 6. 節で本稿のまとめを行う．

2. XAI に関わるこれまでの研究

初期の人工知能研究の代表例であるエキスパートシステムの強みの一つは推論過程を説明する機能を提供する点だとされる[(14)]．また，初期の機械学習モデルには透明性の高いものが多い．具体的には，まず構造が簡潔な線形分類・回帰モデル，決定木，If~Then~(Else~) 形式の規則モデルが挙げられる．また，k-近傍法では入力事例に対する近傍事例を予測の根拠として提示できる．グラフィカルモデル（ベイジアンネットワークに代表されるグラフ構造の確率モデル）は確率論・グラフ理論の枠組みでモデルの意味が規定されており，予測・診断の根拠が明確である．一方，透明性が低いニューラルネットワーク（neural

亀谷由隆　正員　名城大学情報工学部情報工学科
E-mail　ykameya@meijo-u.ac.jp
Yoshitaka KAMEYA, Member (Department of Information Engineering, Faculty of Information Engineering, Meijo University, 1-501 Shiogama-guchi, Tenpaku-ku, Nagoya, Aichi 468-8502, Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.83–92 2022 年 10 月

(注1)：文献リストでは幾つかの国際会議名を略記する．すなわち，AAAI: AAAI Conf. on Artificial Intelligence, CHI: CHI Conf. on Human Factors in Computing Systems, CVPR: IEEE/CVF Conf. on Computer Vision and Pattern Recognition, ECCV: Euro. Conf. on Computer Vision, ECML: Euro. Conf. on Machine Learning, ICCV: IEEE/CVF Conf. on Computer Vision, ICLR: Int'l Conf. on Learning Representations, ICML: Int'l Conf. on Machine Learning, IJCNN: Int'l Joint Conf. on Neural Networks, KDD: ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining, NIPS/NeurIPS: Int'l Conf. on Neural Information Processing Systems, PKDD: Euro. Conf. on Principles and Practice of Knowledge Discovery in Databases を指す．網羅性のためにサーベイ論文の引用を優先することがある．

network，以下 NN）に対しては，訓練済みの NN の挙動を再現・説明する規則を抽出する手法が数多く提案された[15]．

1990 年代後半から 2000 年代にかけて，透明性は低いが予測性能が高い非線形カーネルのサポートベクタマシン（support vector machine，以下 SVM）やアンサンブルモデルが盛んに研究されるようになった．一方，線形カーネルの SVM を L_1 正則化項付きで訓練した疎な線形回帰式を透明性を備えた予測モデルとして利用する方法も広く用いられるようになった．この時期にも機械学習における説明に関する研究が行われており，例えば，SVM に対する規則抽出手法[16]や形式概念分析によりクラスタリング結果を説明する手法[17]が提案されている．また，推薦システムの研究では推薦理由を示すことによるユーザ満足度の向上が試みられている[18]．そして，現在の XAI 技術につながる手法[19]～[21]（後述）もこの時期に提案されている．必ずしも機械学習を前提としていないが，説明機能を備えた情報システム (explanation-aware computing, ExaCt) を研究するコミュニティも存在していた[22]．

2010 年代に入り，深層学習研究が進むと同時に深層 NN 向けの説明手法が提案された．まず，畳み込み NN（convolutional NN，以下 CNN）上での逆伝播により各入力画素が NN の判断にどれだけ貢献するかを測り，その貢献度を入力画像上でヒートマップ（要因マップ(注2)，attribution map）として描画する顕著性マップ (saliency map) [23]，DeconvNet [24]，LRP [25] などの手法が 2014～2015 年に提案された．そして 2016 年提案の LIME [26]では，疑似相関 (spurious correlation) の検出（一般物体の画像分類が一見正しく行われているが，実は背景を見て分類していた）などの XAI 手法の利点が明快な事例や実験結果で示され，XAI 研究が注目されるきっかけとなった．翌 2017 年には先述の DARPA プログラム[1]が開始される一方，後述の SHAP [27]，影響関数 (influence function) に基づく方法[28]，Grad-CAM [29]，DeepLIFT [30]，Integrated Gradients（以下 IG）[31]など，現在ライブラリやクラウドサービスで提供される XAI 手法の多くがこの年に正式発表された．

2018 年以降は XAI 研究が大きな広がりを見せ，既存手法の改良だけでなく，その妥当性検証 (sanity check) [32]，高次特徴空間上の推論を用いたモデルの理解[33]，社会学・心理学・認知科学の立場からの考察[34]，透明性を備えた機械学習モデルの再評価[35]，XAI 手法を医療システムに導入した事例研究[36]などの論文が発表されている．

3. XAI の目的と要件

ここまで説明可能性や透明性などの用語を定義なしに使ったが，これらの用語の意味や説明という行為の目的や要件を明確化する試みがなされている[9]～[11]，[34]，[37]．またシステムやサービスを提供する立場から説明を行うことの利点も挙げられている[2]．以下では筆者が重要と考える考察を紹介する(注3)．

まず Barredo Arrieta ら[11]は XAI とは「何らかの聞き手に対して，自身の挙動を明確にしたり，理解をやさしくしたりする詳細や理由を提示する AI」であると定義している(注4)．彼らが力点を置くのは聞き手の存在であり，提示するべき詳細や理由の内容は聞き手に依存すると述べている．聞き手としては専門家（医者など），一般利用者（モデルの判断に影響を受ける），モデル開発者，監査機関，経営者が挙げられる．また Adadi らは XAI が求められる理由として，(i) 正当化：モデルの挙動や判断に誤りがないことを示す，(ii) 制御：モデルに生じている問題を回避する，(iii) 改善：モデルを効率的に改善する，(iv) 発見：説明を通じて新たな知見を獲得する，の四つを挙げている[9]．

Lipton は機械学習モデルの透明性にも三つのレベルがあることを指摘している[11]，[37]．透明性が最も高いのは人間が自身の手で模擬実行できる (simulatable) モデルである．線形モデル，決定木，規則モデルでも入力特徴量の数や木・規則の複雑さが増せば模擬実行可能とはいえなくなる．次いで透明性が高いのはモデルの構成部品（入力，パラメータ，計算式など）を説明できる分解可能 (decomposable) なモデルである．三つめのレベルはアルゴリズムの透明性 (algorithmic transparancy) と呼ばれ，モデルやその学習アルゴリズムが数理的に分析可能なことを意味する．例えば線形モデルでは分類境界が明らかなのに対し，深層 NN は（現時点では）損失関数のランドスケープが不透明で，最適化もヒューリスティクスに基づき行われている．

Miller は説明という行為について，(i) 説明は対比的 (contrastive) である，(ii) 説明は無数の候補の中から（バイアスを含んだ形で）選択される，(iii) 説明において統計上の相関よりも因果的なつながりの方が重要である，(iv) 説明は社会的 (social) である，ことを指摘した[34]．最初の点について，人間は単に「なぜ P が起きたのか?」と尋ねるのではなく「なぜ Q ではなく P が起きたのか?」と対比的な説明を求めることが知られている．Q は反実的 (counterfactual) な状況であり，Q に応じて適切な説明が変わる．また，最後の点について，Miller は説明という行為が説明者と聞き手の対話（会話）の一部であると述べ，会話の法則の中で説明がどのように行われるか記述している．

上記の Miller の考察からも分かるように，説明という行為は因果的な推論（反実的な状況に基づく推論を含む）やアブダクション (abduction) といった推論形態と近い関係にあることが知られている[38]，[39]．初期の XAI 研究においてはこれらの推論との関係は希薄だった（少なくとも明文化されていなかった）が，近年ではこれらの推論の考え方を意識的に用いた研究が増えているように感じる．

4. XAI の諸技術

4.1 XAI 手法の分類軸

既存の XAI 手法は下の分類軸（1）～（5）で整理されることが多い．多くのサーベイ論文ではこれらの分類軸に基づき既存

(注2)：本稿では便宜上 attribution map の訳語として「要因マップ」を用いている．この訳語が定着しているわけではない．
(注3)：ここで紹介しているのは積み上げられた議論のごく一部であるので，興味ある読者はぜひ原典を当たって頂きたい．
(注4)：「説明可能」と似た文脈で「解釈可能」(interpretable) という言葉も使われるが，本稿ではより広い範囲をカバーする（と思われる）前者を優先的に用いる．

手法を分類している（紙幅の制約で本稿では一部を記述）．

（1） 透明性/事後性
（2） 大域性/局所性
（3） モデル依存性/モデル非依存性
（4） データ形式（画像，テキスト，表，時系列，グラフ）
（5） 説明の実現方法

分類軸（1）について，前に述べたように透明性を備えたモデルはそれ自身で人間が理解可能なモデルである．一方，透明性の低いモデルでは事後的 (post-hoc) な説明が行われる．また分類軸（2）においては，事例を横断する，モデル全体の挙動を説明するのが大域的 (global) な説明であり，特定の事例に関する予測の根拠を説明するのが局所的 (local) な説明である．更に分類軸（3）において，モデルの内部構造を介して説明する場合，その説明はモデル依存 (model-specific) である．一方，モデルの内部構造には立ち入らず，その入出力関係のみに注目して行う説明はモデル非依存 (model-agnostic) である．分類軸（4）ではデータ形式によって入力特徴量の性質が変わる点に考慮が必要である．例えば画素は単体では人間が解釈できないのに対し，表データの列項目は（人間の年齢・性別のように）粒度が大きく，単体で解釈可能なものが多い．テキストを扱うモデルに対する XAI 手法は Danilevsky らがまとめている[40]．(多変量) 時系列やグラフを扱うモデルに対する XAI 手法も登場してきており[41]～[43]，今後増えると思われる．また，データ形式は複数にまたがることがあり，例えば画像分類の予測根拠をテキストで説明する手法が知られている[44]．分類軸（5）は機械学習モデルのどの側面に注目して説明を提示するかに関するものである．4.2～4.11 節で具体的な XAI 手法の実現方法を述べるが，背後のアイディアはデータ形式をまたいで適用可能だと思われる．

4.2 透明性を備えたモデルを利用する方法

XAI 研究における一般的な了解事項として予測性能と説明可能性の間のトレードオフ[1],[11]がある．その中で Rudin は予測性能は高いが透明性の低いモデルを事後的に説明するのではなく，透明性を備えた予測性能の高い機械学習モデルを探求することを提唱している[35]．実際，彼女の研究グループでは If∼Then∼Else∼ 形式の規則モデル CORELS[45]やプロトタイプ画像を利用する画像タスク向けモデル ProtoPNet[46]及びそれらの学習アルゴリズムを提案している．

また，統計分野で 1980 年代に考案された一般化加法モデル（generalized additive model，以下 GAM）[47]を透明性と予測性能を両立したモデルとして用いる研究も行われている．まず，線形回帰式（式 (1)）と GAM（式 (2)，(3)）の一般形を示す．

$$E[y] = w_0 + \textstyle\sum_i w_i x_i \tag{1}$$

$$g(E[y]) = f_0 + \textstyle\sum_i f_i(x_i) \tag{2}$$

$$g(E[y]) = f_0 + \textstyle\sum_i f_i(x_i) + \sum_{i\neq j} f_{i,j}(x_i, x_j) \tag{3}$$

式 (1) は入力特徴量 x_i に重み w_i を乗じた上で和を取って y を予測することを示している(注5)．一方，式 (1) の一次項 $w_i x_i$ を $f_i(x_i)$ に置き換えたのが式 (2) の GAM である．線形回帰より予測性能を向上させるため，基本的に f_i には非線形関数が選ばれ，多くの場合に平滑化スプラインが用いられる．g はリンク関数と呼ばれ，例えば 2 値分類を行う場合は g として logit 関数が選ばれる．更に，二つの特徴量間の依存関係を表現するために，相互作用項 $f_{i,j}(x_i, x_j)$ を加えたのが式 (3) である．このように GAM では特徴量間の依存関係をなくして（式 (2)），若しくは最小限にして（式 (3)）透明性を確保しつつ，関数 f_i 及び $f_{i,j}$ の非線形性により予測性能の向上を狙っている．実際，各項 $f_i(x_i)$, $f_{i,j}(x_i, x_j)$ が予測への貢献度そのものであり，例えば x_i の値を動かしたときの $f_i(x_i)$ の挙動を観察することで，x_i がどのように予測に貢献するかじかに調査できる．

近年，Lou らは式 (3) の形をしたモデルを GA^{2}M (generalized additive model plus interactions) と呼び，f_i や $f_{i,j}$ にバギングや勾配ブースティングを用いたアンサンブルモデルを採用し，更なる予測性能の向上を図っている[48]．そして GA^{2}M の高速な実装として explainable boosting machine (EBM) が提供されている(注6)．EBM では式 (3) における相互作用項が効率よく自動選択される．Chang らは複数種類の GAM（平滑化スプラインを用いたものや EBM）に対し，説明可能性の観点から比較調査を行っている[49]．

4.3 逆伝播に基づく方法

先述のように顕著性マップ，DeconvNet，LRP (layer-wise relevance propagation)，DeepLIFT，IG では出力への貢献度を NN の入力層まで逆伝播させて各入力特徴量（画素）の貢献度を測る．ここでは図 1(注7)に基づいて LRP を簡単に説明する．

入力 x に対して $f(x)$ を出力する NN に対し，LRP では各入力特徴量 x_i の出力への貢献度（LRP では関連度と呼ぶ）R_i を求める．まず，NN の順伝播では図 1 (a) の矢印の向きに従って第 ℓ 層の素子 i の活性値 x_i と第 $\ell+1$ 層の素子 j への重み w_{ij} から $z_{ij} = w_{ij} x_i$ を計算する．そして第 $\ell+1$ 層の素子 j の活

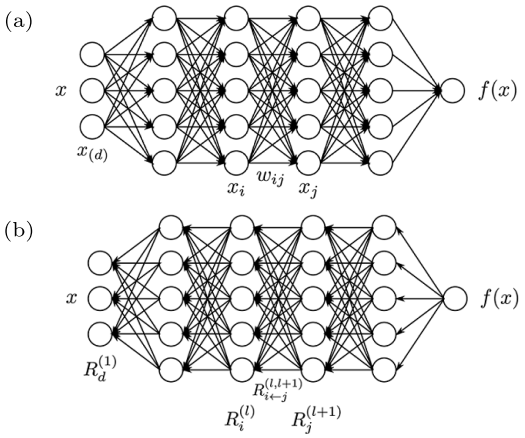


図 1 (a) 活性値の順伝播，(b) LRP 法における関連度の逆伝播

(注5)：右辺の誤差項（期待値 0）を消すために左辺は期待値を取った形にしている．

(注6)：https://interpret.ml/

(注7)：LRP の提案論文[25]より引用．

性値は $x_j = \sigma(\sum_i z_{ij} + b_j)$ と計算される．b_j はバイアス項，σ は活性化関数である．一方，LRP の simple-LRP という簡単な逆伝播規則では図 1 (b) の矢印の向きに従って

$$R_i^{(l)} = \sum_j R_{i\leftarrow j}^{(l,l+1)} \tag{4}$$

$$R_{i\leftarrow j}^{(l,l+1)} = \frac{z_{ij}}{z_j} R_j^{(l+1)} \tag{5}$$

のように第 ℓ 層の関連度 $R_i^{(\ell)}$ が第 $\ell+1$ 層の素子 j 間の関連度 $R_j^{(\ell+1)}$ に基づき計算される（ただし $z_j = \sum_i z_{ij}$）．入力素子 x_i の関連度 R_i は $R_i^{(1)}$ と定義する．更に，ϵ-LRP（式 (6)）や $\alpha\beta$-LRP（式 (7)）という逆伝播規則も導入されている．

$$R_{i\leftarrow j}^{(l,l+1)} = \frac{z_{ij}}{z_j + \epsilon \cdot \mathrm{sign}(z_j)} R_j^{(l+1)} \tag{6}$$

$$R_{i\leftarrow j}^{(l,l+1)} = \left(\alpha \frac{z_{ij}^+}{z_j^+} + \beta \frac{z_{ij}^-}{z_j^-}\right) R_j^{(l+1)} \tag{7}$$

ϵ-LRP では z_j が小さな場合でも数値的に安定する．また，$\alpha\beta$-LRP において，$z_{ij}^+ = \max\{z_{ij}, 0\}$, $z_{ij}^- = \min\{z_{ij}, 0\}$, $z_j^+ = \sum_i z_{ij}^+$, $z_j^- = \sum_i z_{ij}^-$ であり，出力との不整合を意味する負の関連度を多く伝播するよう α, β を設定できる（ただし $\alpha + \beta = 1$）．

$\alpha = 1$, $\beta = 0$ なる $\alpha\beta$-LRP は Montavon らにより理論的な正当化が行われた[50]．最近では層ごとに逆伝播規則を切り替えて自然な要因マップを得る LRP_{CMP} が提案されている[12]．Ancona らは IG, ϵ-LRP, DeepLIFT などを統一的に定式化して理論的・実験的に比較している[51]．また，深層学習ライブラリが提供する微分計算機能を利用した効率的な実装が知られる[50]．

LRP の発展形も提案されている．分類向け NN の挙動を知る場合，説明対象のクラスに特徴的な領域を強調する要因マップが望ましく，そのようなクラス識別性(注8) (class discriminativity) をもつ CLRP (contrastive LRP) [52]や CRP (contrastive relevance propagation) [53]が提案されている．また RAP (relative attributing propagation) [54]では関連度の逆伝播の過程で正負の関連度が打ち消し合うことを避けるような逆伝播規則を導入している．

4.4 特徴マップに基づく方法

CNN における特定層の複数の特徴マップを統合する要因マップ生成手法も知られている．初期手法の CAM (class activation map) [55]は，出力部分を global average pooling 層と畳み込み層にした NN を想定し，予測時に用いた特徴マップの重み付き和を求め，その結果を入力画像サイズまで拡大して要因マップとする．CAM は前述のクラス識別性を備えるが，使われている特殊な NN では予測精度が問題になり得る．一方，Grad-CAM [29]では各特徴マップへの重みを求める際に特徴マップ要素による出力の微分値を用いて，一般の分類向け CNN に対する要因マップを生成する．Grad-CAM は現時点で非常によく利用されている印象がある．これまでに Grad-CAM++ [56]などの改良形も数多く提案されている．

(注8)：クラス識別性は 3. 節で述べた対比性の一種であると考えることができる．

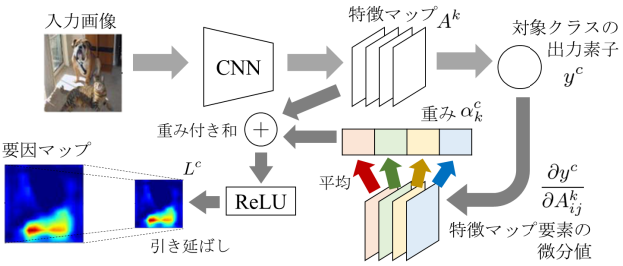


図 2　Grad-CAM による要因マップ生成

図 2 に Grad-CAM の処理の様子を示す．まず，CNN において入力画像に対して活性値の順伝播によりクラス c への出力 y^c が得られたとする．そして途中の過程で特徴（活性値）マップが得られているものとし，k 番めの特徴マップを A^k とおく．そのとき，Grad-CAM ではまず各特徴マップ要素 A_{ij}^k の出力 y^c への貢献度として $\partial y^c / \partial A_{ij}^k$ を求める．そして A^k の貢献度として global average pooling と同様の操作で

$$\alpha_k^c = \frac{1}{Z} \sum_i \sum_j \frac{\partial y^c}{\partial A_{ij}^k} \tag{8}$$

を求める（Z は特徴マップのサイズ）．この α_k^c を重みとして特徴マップ A_k の和を取り，更に ReLU 関数に適用して（負要素を 0 として），クラス c に対する A^k と同サイズの要因マップ $L^c = \mathrm{ReLU}(\sum_k \alpha_k^c A^k)$ が得られる．最終的に L^c は入力画像サイズまで引き延ばされる．

4.5 摂動に基づく方法

一種の感度分析として，説明対象の事例 x の一部 z に摂動を与え，予測 $y = f(x)$ の変化を観察する局所的な手法が知られる．これらの手法では z に関する反実的な状況を考えていると見ることもできる．例えば分類において，摂動により興味のクラス c への確信度（softmax 関数の出力）が大きく下がれば z は c にとって重要な特徴量だと考える．Zeiler らの手法[24]では，CNN を対象として入力画像にサイズ $m \times m$ のマスクを当て c に対する確信度などへの影響度をヒートマップ化して要因マップを描く．この方法は確実だが計算量が大きいため，RISE [57]ではマスクをランダムに複数生成し，各々のマスクを適用した入力画像を CNN が出力する確信度で重み付けして統合する．

また，Zintgraf らは Robnik-Šikonja らの考え[20]を prediction difference analysis (PDA) と呼び，この考えのもとで画像・深層 NN 向けの要因マップ生成手法を提案した[58]．PDA では特徴量 A_i とその値 a を含む説明対象の事例 x に対し，$A_i = a$ がそのとおり存在する場合と A_i 自体が存在しない場合を考え，両者における予測結果の変化を考える．ここで説明対象が確率的分類器であると考え，前者と後者でのクラス c への確信度を各々 $p(c \mid x)$, $p(c \mid x \backslash A_i)$ と表記する．そして事例 x における特徴量 A_i の重要度として weight of evidence (WE) をオッズ $o(c \mid z) = p(c \mid z)/(1 - p(c \mid z))$ を用いて下のように定義する．

$$\mathrm{WE}_i(x) \stackrel{\mathrm{def}}{=} \log_2(o(c \mid x) - \log_2(o(c \mid x \backslash A_i)) \tag{9}$$

問題となるのが $p(c \mid x \backslash A_i)$ の計算であるが，準備としてまず

$$
\begin{aligned}
&p(c \mid x \backslash A_i) \\
&= \textstyle\sum_a p(c, A_i = a \mid x \backslash A_i) \\
&= \textstyle\sum_a p(A_i = a \mid x \backslash A_i) p(c \mid x \backslash A_i, A_i = a) \qquad (10)
\end{aligned}
$$

と変形する．一般に $p(A_i = a \mid x \backslash A_i)$ は推定困難であるため，Robnik-Šikonja らはこれを周辺分布 $p(A_i = a)$ で近似し，

$$
p(c \mid x \backslash A_i) \approx \textstyle\sum_a p(A_i = a) p(c \mid x \backslash A_i, A_i = a) \qquad (11)
$$

と考える．この式に基づき，我々はまず推定済みの周辺分布 $\hat{p}(A_i = a)$ から a をサンプリングし，事例 x の A_i を a で上書きして（摂動を与えて）新たな事例 x' を得る．このようにして複数得られた x' の各々について確信度 $p(c \mid x')$ を計算し，その平均より $p(c \mid x \backslash A_i)$ を求める．一方，画像・深層 NN 向けに PDA を適用するために，Zintgraf らは摂動を与える A_i を画素ではなくパッチとして，NN の出力を変化しやすくした．更に A_i を覆うパッチ $\tilde{x}_i$ を導入し，式 (10) の $p(A_i = a \mid x \backslash A_i)$ を周辺分布より精密な $p(A_i = a \mid \tilde{x}_i \backslash A_i)$ で近似している．

4.6 事例に基づく方法

局所的な説明では，k-近傍法（2. 節）のように入力 x に対する予測 $y = f(x)$ に影響を与える訓練事例を予測結果の根拠とすることが考えられる．Koh らの影響関数を用いた方法[28]では，説明対象の事例 $z_{\text{test}} = (x_{\text{test}}, y_{\text{test}})$ に対し（z_{test} で予測誤りが起きている場合が典型的），f の訓練過程を通じて各事例 $z = (x, y)$ が z_{test} に影響を及ぼす度合い（影響関数）$\mathcal{I}(z, z_{\text{test}})$ を計算し，その度合いが大きい事例を提示する．具体的には，まずパラメータ θ の下の損失関数を $L(\cdot, \theta)$，訓練集合における i 番めの事例を $z_i = (x_i, y_i)$ とおき $(1 \leqq i \leqq n)$，パラメータは $\hat{\theta} = \text{argmin}_\theta \frac{1}{n} \sum_{i=1}^n L(z_i, \theta)$ と推定することを考える．一方，事例 z の損失を微小分 ϵ だけ余分に加えたときの推定パラメータを $\hat{\theta}_{\epsilon,z} = \text{argmin}_\theta (\frac{1}{n} \sum_{i=1}^n L(z_i, \theta) + \epsilon L(z, \theta))$ とおいたとき，$\mathcal{I}(z, z_{\text{test}})$ は下のように計算される．

$$
\begin{aligned}
\mathcal{I}(z, z_{\text{test}}) &\stackrel{\text{def}}{=} \left. \frac{dL(z_{\text{test}}, \hat{\theta}_{\epsilon,z})}{d\epsilon} \right|_{\epsilon=0} && (12) \\
&= \nabla_\theta L(z_{\text{test}}, \hat{\theta})^\top \left. \frac{d\hat{\theta}_{\epsilon,z}}{d\epsilon} \right|_{\epsilon=0} && (13) \\
&\approx -\nabla_\theta L(z_{\text{test}}, \hat{\theta})^\top H_{\hat{\theta}}^{-1} \nabla_\theta L(z, \hat{\theta}) && (14)
\end{aligned}
$$

ここで $H_{\hat{\theta}} \stackrel{\text{def}}{=} \frac{1}{n} \sum_{i=1}^n \nabla_\theta^2 L(z_i, \hat{\theta})$ は訓練集合の損失のヘッセ行列である(注9)．式 (13) では微分の連鎖則，式 (14) はロバスト統計分野の結果を用いている．素朴には再学習で $\hat{\theta}_{\epsilon,z}$ が求められるが，式 (14) の近似により再学習が不要となる利点がある．

Koh らの方法は訓練過程を通じて予測の根拠となる事例を求めるものであったが，より直接的に，高次特徴量が入力事例 x と類似する事例を（訓練）事例集合から選び出し，x に対する予測の根拠とする方法も知られている[59]．更に最近では，深層生成モデルを用いて現実には存在しない（反実的な）事例を生成する方法も提案されている[60], [61]．

(注9)：損失関数のヘッセ行列とその逆行列が存在すると仮定している点に注意が必要である．Koh らの論文[28]では損失関数が微分可能でない場合を議論している．

4.7 代理モデルに基づく方法

代理モデルに基づく手法は，説明対象のモデル f に対し，$y = f(x)$ なる入出力関係 (x, y) を近似する透明性の高い代理モデル f' を求めて元のモデル f の挙動を理解するモデル非依存の手法である．例えば，前述の LIME (local interpretable model-agnostic explanations)[26] は局所的な手法であり，まず説明対象の事例 x に対してその近傍の事例 x' をサンプリングによって（大量に）生成し，同時に各 x' に対してモデル f に基づきラベル $y' = f(x')$ を付与する．そして入出力対 (x', y') の集合から線形回帰式 f' を代理モデルとして学習する．その際，f' の学習に L_1 正則化項が用いられ，説明対象の事例 x で重要ではない入力特徴量の重み係数が 0 になるため，重み係数が一定以上の入力特徴量の集合が x に対する説明になる．x が画像（あらかじめ superpixel 領域に分割されることが多い）なら要因マップが描ける．LIME における技術的なポイントとして局所的な説明という状況をうまく利用している点が挙げられる．すなわち，f の分類境界が複雑であっても，説明対象の事例 x の周辺の境界は比較的簡単な形状で，透明性の高い代理モデル f' でよく近似できる可能性がある．

4.8 規則に基づく方法

前述のとおり，一般に規則モデルは透明性が高いといえるが，どのような論理表現が人間にとってより理解しやすいかという考察もなされている．Huysmans らは決定表（decision tables, 図 3(注10)），二分決定木，論理演算子を用いた規則，一次判定式に基づく (oblique) 規則（図 4）の理解容易性について被験者実験を行っている[62]．また Lakkaraju らは If∼Then∼Else∼ 規則（決定リストとみなせる）より If∼Then∼ 規則の集合の方が条件式の入れ子が浅く，理解が容易であると主張している[63]．

また XAI 研究では，規則モデルは透明性を備えたモデル（4.2 節）として直接用いられたり，透明性が低いモデルを説明する代理モデル（4.7 節）として用いられたりすることが多い．後者について，LIME の考案者である Ribeiro らは LIME と同様のアプローチで規則モデルを用いて局所的な説明を行う Anchors[64] を提案した．一方，大域的手法である TREPAN[65] は各特徴量の周辺分布からサンプリングした事例集合よりその入出力

INCOME	< 1000		$\geqq 1000$
AGE	< 25	$\geqq 25$	—
ACCEPT	X		
REJECT		X	X

図 3 決定表の例

IF $(5 \times \text{INCOME} + 12 \times \text{AGE} > 900)$ THEN ACCEPT
DEFAULT: REJECT

図 4 一次判定式に基づく規則の例

(注10)：図 3 と図 4 の例はともに Huysmans らの論文[62]より引用．

表 1　プレイヤが協力して得られる報酬

$v(\emptyset)=0$	$v(\{1,2\})=60$
$v(\{1\})=10$	$v(\{2,3\})=70$
$v(\{2\})=20$	$v(\{1,3\})=90$
$v(\{3\})=30$	$v(\{1,2,3\})=100$

表 2　あり得るプレイヤの参加順と限界貢献度

#	参加順	プレイヤ 1	プレイヤ 2	プレイヤ 3
1	$\emptyset \to \{1\} \to \{1,2\} \to \{1,2,3\}$	10	50	40
2	$\emptyset \to \{1\} \to \{1,3\} \to \{1,2,3\}$	10	10	80
3	$\emptyset \to \{2\} \to \{1,2\} \to \{1,2,3\}$	40	20	40
4	$\emptyset \to \{2\} \to \{2,3\} \to \{1,2,3\}$	30	20	50
5	$\emptyset \to \{3\} \to \{1,3\} \to \{1,2,3\}$	60	10	30
6	$\emptyset \to \{3\} \to \{2,3\} \to \{1,2,3\}$	30	40	30

関係を模倣する m-of-n 決定木を構築して f の代理モデルとする．CRED [66] も大域的な手法だが，こちらはまず各隣接層間にて決定木経由で規則集合を構築し，後段の規則集合を前段の規則集合に埋め込む形で統合・簡単化して最終的な規則集合を得る．DeepRED [67] は CRED を深層 NN 向けに拡張した手法である．

4.9　表データを扱うモデルに対する説明手法

前述のとおり，表データでは入力特徴量を単体で解釈できることが多いため，ランダムフォレストや勾配ブースティング木では入力特徴量ごとの重要度 (feature importance) を測って大域的な説明が行われる．加えて，モデルに依存せず，局所的な説明を事後的に行う SHAP (Shapley additive explanations) [27] が最近よく利用される．SHAP では協力ゲーム理論に基づく合理的な入力特徴量の重要度である Shapley 値 [3], [7] を近似的に計算する．以降では Shapley 値と SHAP を簡単に説明する．

まず，協力ゲームにおいて複数人で得た報酬を貢献度に応じて分配することを考える．例としてプレイヤ 1，2，3 を考え，彼らが単独/複数で得られる報酬が表 1 のとおりだったとする(注11)．ここで $v(S)$ は S 中のプレイヤ全員が協力して得られる報酬である．このときプレイヤ i の Shapley 値 ϕ_i は i の参加によって変化した報酬（限界貢献度）の平均値として定義される．プレイヤの参加順は表 2 に示す 6 通りが考えられ，各プレイヤの限界貢献度がその右に記されている．このときプレイヤ i の Shapley 値 $\phi_1=(10+10+40+30+60+30)/6=30$ となる．同様に $\phi_2=25$, $\phi_3=45$ と計算される．Shapley 値は四つの合理的な要件 (efficiency, symmetry, dummy, additivity) を満たす唯一の報酬分配方法として知られる [3]．

ここで機械学習モデル f の挙動を説明するという状況に戻る．特徴量の数を m とし，説明対象の入力 $x=(x_1,x_2,\ldots,x_m)$ における各特徴量 x_i の貢献度として Shapley 値 ϕ_i を求めることを考える（特徴量とプレイヤが対応）．そして報酬 $v(\cdot)$ を定める．例えば $m=4$ の場合を考えると，全特徴量を使った場合の報酬は $v(\{1,2,3,4\})=f(x_1,x_2,x_3,x_4)-\int f(x')p(x')dx'$ で定められる．第 1 項は入力に対する出力値である．一方，第 2 項はモデルの出力の期待値であり，ベースラインの役割を果たす．また一部の特徴量，例えば x_1, x_3 のみを使った場合の報酬は $v(\{1,3\})=\int f(x_1,x_2',x_3,x_4')p(x_2',x_4')dx_2'dx_4'-\int f(x')p(x')dx'$ と定める．第 1 項では考慮外の x_2, x_4 について周辺化が行われている．そして，特徴量 x_i の Shapley 値 ϕ_i は一般に

(注11)：数値例は Google のホワイトペーパー [2] で用いられているものである．

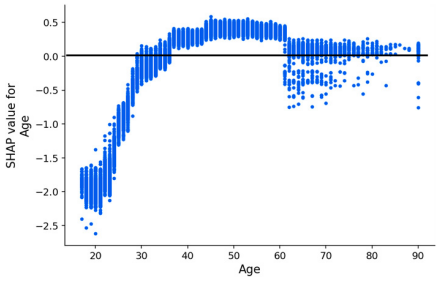


図 5　SHAP の実装で得られる dependence plot の例

$$\phi_i = \sum_{S\subseteqq\{1,2,\ldots,m\}\setminus\{i\}} \frac{|S|!(m-|S|-1)!}{m!}\Big(v(S\cup\{i\})-v(S)\Big) \quad (15)$$

と（厳密に）得られることが知られている．ただし，この値を現実時間で求めるのは容易でない．Štrumbelj らはモンテカルロ法によって Shapley 値を近似的に求める方法 [21] を提案している．一方，SHAP では LIME に着想を得て，線形回帰式の推定により Shapley 値 ϕ_i を求める KernelSHAP という近似方法が提案されている．

基本的に SHAP は局所的な説明手法だが，効果的に可視化することで大域的な説明が可能になる．例えば Python の shap パッケージでは局所的な説明を複数事例に対して求め，それらの結果を集約・可視化する機能がある．図 5 は dependence plot と呼ばれる，事例集合中の特徴量 Age（横軸）とその Shapley 値（縦軸）の散布図である(注12)．Shapley 値が正（負）であることは出力の値が大きく（小さく）なることを意味している．

4.10　高次特徴量に基づく方法

十分に訓練された CNN の低次層では画像フィルタが得られることが観察される [24]．更に，Erhan らは NN 中の各素子に対し，その活性値(注13) を最大化する入力特徴量を求める activation maximization を提案している [19]．画像向け NN であれば，activation maximization で得られた入力画像を通じて各素子が表現する特徴量を直観的に理解できる可能性がある．

また，我々のもつ概念を NN の高次特徴空間で CAV (concept activation vector) として捉えて NN の挙動を理解する方法が知られる [33]．具体的には，画像分類用 NN が高次層 l までの関数 f_l と層 l 以降から出力クラス k の logit 値への関数 $h_{l,k}$ か

(注12)：図 5 の例は https://slundberg.github.io/shap/notebooks/plots/dependence_plot.html より引用．縦軸の値が 0 の直線は筆者が引いている．

(注13)：一般には入力特徴量（のノルム）の正則化項をつけることが多い [19], [50]．

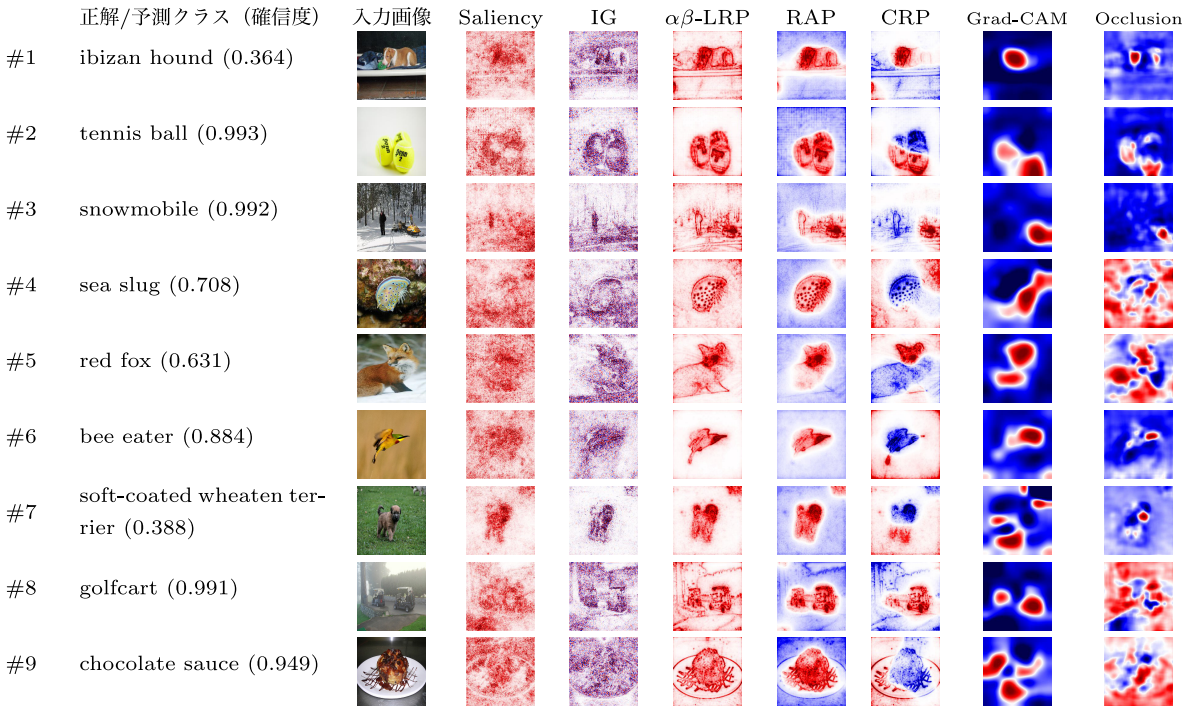


図 6　要因マップの生成例

らなると考える．そして概念 C（例えば縞模様）を満たす事例集合 $\mathcal{P}_C$（縞模様の物体が写る画像）と満たさない事例集合 $\mathcal{N}$（ランダムに選んだ画像）を用意する．次にそれらを高次特徴空間上に射影した $\{f_l(x) \mid x \in \mathcal{P}_C\}$ と $\{f_l(x) \mid x \in \mathcal{N}\}$ を判別する線形分類器を構築し，その分類境界との直交ベクトル v_C^l を CAV と呼ぶ．CAV は高次特徴空間で概念 C が色濃くなる方向を指すと期待される．そして方向微分

$$S_{C,k,l}(x) = \lim_{\epsilon \to 0} \frac{h_{l,k}(f_l(x) + \epsilon v_C^l) - h_{l,k}(f_l(x))}{\epsilon} \quad (16)$$

$$= \nabla h_{l,k}(f_l(x)) \cdot v_C^l \quad (17)$$

で概念 C の出力クラス k への影響度を測ることが可能になる．

この節で述べた手法はいずれも大域的な説明手法といえる．高次特徴量上の推論では異なる種類のデータを同時に扱うマルチモーダルなモデルも扱えると思われる．

4.11　説明機構をモデルに組み込む方法

4.3〜4.10 節の手法では，説明対象のモデルは所与（訓練済み）で，説明の仕組みはもたない前提だった．一方，アテンション (attention) を使う NN では，アテンションの重みを可視化して予測の根拠とすることが多い．例えば近年注目される Transformer モデルに対しては attention rollout [68] と呼ばれる手法が提案されている．アテンションの重みが説明に有効かどうかの議論も行われている [40]．

また，attention branch network (ABN) [69] はその後段が attention map（マスクの役割を果たす）を求める部分ネットワークと本来の予測を行う部分ネットワークに分岐した構造（attention map でマスクされた特徴マップを受け取る）をもち，二つの部分ネットワークを同時に訓練して説明能力を得つつ予測性能を向上させる．同様の構造は再帰 CNN を元にした Lei らのテキスト回帰モデルにも見られる [70]．これらのモデルを用いた説明は透明性を備えたモデルに基づく説明と事後的な説明の中間に位置するといえる．

4.12　要因マップの生成例

要因マップ（4.3〜4.5 節）の生成例を図 6 に示す．要因マップ生成手法の実装として RAP の実装(注14) 及び Captum (注15) を利用した．説明対象のモデルは訓練済みの VGG-16 である．説明対象の事例として ILSVRC2012 の検証用画像 9 枚を用いる(注16)．これらの画像に対する VGG-16 の予測（分類）は全て正解だった．図 6 ではその予測クラスと確信度を示す．要因マップ生成手法として顕著性マップ (“Saliency”)，IG，$\alpha\beta$-LRP ($\alpha = 1$, $\beta = 0$)，RAP，CRP，Grad-CAM，Zeiler らの摂動に基づく手法 (“Occlusion,” $m = 15$) の七つを用いる．要因マップはどれも予測に対する根拠を示す(注17)．

図 6 にて左の四つの生成手法では要因マップが一定の傾向にある．顕著性マップと IG ではややノイズ混じりで，IG では正の貢献度をもつ画素（赤）と負の貢献度（青）をもつ画素が入り混じり要因マップ全体が紫に見える．また，$\alpha\beta$-LRP はエッ

(注14)：https://github.com/wjNam/Relative_Attributing-Propagation
(注15)：https://captum.ai/
(注16)：RAP の実装でサンプル画像として提供された中から結果が異なる傾向のものを選択した．
(注17)：各画素の貢献度は Min-Max 正規化を施し，カラーマップとして正の貢献度が赤，負の貢献度が青，0 に近い貢献度が白に色付けされる seismic を選択した．ただし，Zeiler らの手法以外では，正規化前に画像中の 99%-tile 値より大きい値は 99%-tile 値に，1%-tile 値より小さい値は 1%-tile 値に置き換えている．これらは細かい選択だが要因マップの読み取りやすさにかなり影響を及ぼす．

ジを反映し，更に RAP は物体の存在領域を切り出している．

一方，右の三つの生成手法はクラス識別性を備えており，物体の中でも特に対象クラスを特徴づける箇所を強調する．典型的には#3 の事例において，RAP が人と雪上車の両方を強調するのに対し，右の三つの手法では説明対象の予測クラスである雪上車に関わる箇所のみを強調する．ただ，ほかの事例では強調する箇所が 3 手法間で大きく異なることもある．また Grad-CAM や Zeiler らの手法に比べ，CRP は（LRP や RAP 同様）画素単位の貢献度を計算することでエッジが反映できている．

それぞれ上で述べた傾向はあるが，図 6 全体を見たとき，要因マップで強調される箇所は生成手法によって大きく異なり，現時点では一つの生成手法に頼ることにはリスクがあると考えられる．Google は要因分析手法を用いる際に陥りやすい落とし穴や手法自体の限界について丁寧な考察を行っている[2]．

5. XAI 研究の課題

5.1 評価基準及び手法の確立

XAI 研究において難しいのは XAI 手法の評価である．残念ながら現時点では確立された評価方法は存在しておらず，XAI 手法の提案者・利用者は適切な評価方法を模索する必要がある．Doshi-Velez らは評価方法を 3 種類に分類している[71]．

（1） 応用に基づく (application-grounded) 方法
（2） 人に基づく (human-grounded) 方法
（3） 機能に基づく (functionally-grounded) 方法

方法（1）では応用先における実際のタスクの中でユーザ（典型的には専門家）に説明を提示して評価してもらう．一方，方法（2）では（1）よりタスクを単純化してユーザ（典型的には非専門家）に評価してもらう．最近ではクラウドソーシングサービスが使われることも多い．更に，人間の知力を計算資源として活用するヒューマンコンピュテーションの技法を用いて XAI 手法を評価する手法も提案されている[72]．方法（3）では（アノテーション以外は）人が関わらない形で評価する．（1）（2）を代替する評価指標を用いること，比較相手の手法が既に（1）（2）で評価済みであることが望ましい．要因マップ生成手法の評価では物体検出やセグメンテーションの正解情報が用いられることがある[73]．Adebayo らは要因マップ生成手法の大規模な妥当性検証を行い，多くの手法で望ましくない挙動が見られると報告している[32]．

方法（3）の一例として，摂動に基づく方法（4.5 節）に似た感度分析に基づき，予測にとって重要な領域を要因マップが正しく強調しているかを評価する定量的スコア AOPC (area over the MoRF purturbation curve) [74] の計算イメージを図 7 に示す．AOPC では入力画像 x に対して要因マップで最も貢献度が高い領域（画素や $m \times m$ の正方領域）から順に摂動を加え続けたときに出力 $f(x)$ がどれくらい速く落ちるかを測る．具体的には，まず貢献度が高い領域から順に $r_1, r_2, \ldots$ と並べ，$x^{(k)}_{\mathrm{MoRF}}$ は $x^{(k-1)}_{\mathrm{MoRF}}$ 中の領域 r_k に摂動を加えた画像とする（$k = 1, 2, \ldots$，なお $x^{(0)}_{\mathrm{MoRF}} = x$ である）．そして，$f(x^{(0)}_{\mathrm{MoRF}})$

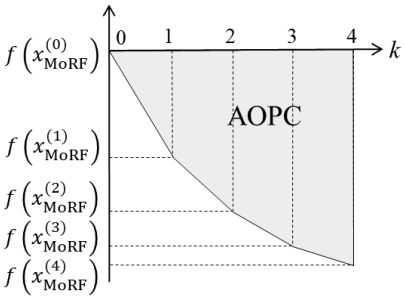


図 7 AOPC の計算イメージ

$(= f(x))$, $f(x^{(1)}_{\mathrm{MoRF}})$, $f(x^{(2)}_{\mathrm{MoRF}})$, ... の描く曲線を図 7 のように考え，曲線上側の領域（灰色）の面積を AOPC とする．もし AOPC が大きいとすれば，元の出力値 $f(x)$ に対して曲線が速く落ちたからであり，すなわち要因マップが妥当である（貢献度が高い領域が本当に出力値 $f(x)$ に大きく影響している）ことを意味する．

5.2 機械学習モデルの検証・デバッグ・改善への接続

機械学習モデルの開発者の立場ではモデルが説明されるだけでは不十分かもしれない．XAI 技術で得られた情報をモデルの検証・デバッグ・改善にどうつなげるかが次の課題である．要因マップ（4.3〜4.5 節）手法がモデルの検証やデバッグに有効かどうかについて，前述の Adebayo らは 3 種類のバグを想定し，被験者実験を実施している[75]．また，ABN（4.11 節）の attention map を望ましい形に人間が介入することで予測精度を向上できると報告されている[76]．更に，要因マップで訓練集合内の疑似相関を検出したり，事例に基づく手法（4.6 節）で事例の重要度を測ったりできれば，効果的な訓練事例の選択や能動学習に発展すると思われる．最近では，顕著性マップ（4.3 節）で画像内の重要な領域を特定し，その領域にはデータ変換操作を施さないデータ拡張手法が提案されている[77]．

5.3 XAI システムの構築

画像を用いた医療診断や自動運転車両への応用は（研究レベルでは）既に多くの試みがあり[78],[79]，他分野においても XAI 技術の利用が進むと思われる．一方，応用の際に必要となるのが当該分野の専門家や利用者が用いるシステムの構築である．Miller の考察（3. 節）にあるように，一般に説明という行為は聞き手との対話の中で行われるため，人間とシステムのインタフェースが重要になっている[1]．例えば，CAV（4.10 節）を利用して，医療専門家が望む傾向の画像を対話的に検索できるシステムが構築されている[36]．このような研究は対話型機械学習[80]や機械学習モデルの可視化[81]といった研究と近い関係にあり，「新世代の」エキスパートシステムにもつながり得る．

6. おわりに

XAI 技術の過去・現在・未来を概観した．紙幅の制約により

簡単な文献紹介が中心になったことをご容赦願いたい．本稿で見てきたように，XAI は（その高い目標に対して道半ばかもしれないが）既に大きな研究分野としての広がりをもっている．説明は文脈（説明対象や聞き手）に強く依存するタスクであり，適切な説明の仕方は文脈によって大きく変わるため，個々の研究成果が発散してしまいがちである．評価方法の確立など，研究分野として共有できる知見を積み上げる意識が必要であると（自戒も込めて）感じている．

文　献

(1) D. Gunning and D.W. Aha, "DARPA's explainable artificial intelligence program," AI Magazine, vol.9, pp.44–58, 2019.
(2) Google Inc., "AI explainability whitepaper," https://cloud.google.com/explainable-ai, accessed on August 27, 2021.
(3) C. Molnar, "Interpretable machine learning: A guide for making black box models explainable,"（原版）https://christophm.github.io/interpretable-ml-book/;（邦訳）https://hacarus.github.io/interpretable-ml-book-ja/, 2017.
(4) 原聡，"私のブックマーク：機械学習における解釈性，" 人工知能，vol.33，no.3，pp.366–369，2018.
(5) 原聡，"私のブックマーク：説明可能 AI，" 人工知能，vol.34，no.4，pp.577–582，2019.
(6) 恵木正史，"XAI (eXplainable AI) 技術の研究動向，" 日本セキュリティ・マネジメント学会誌，vol.34，pp.20–27，2020.
(7) 森下光之助，機械学習を解釈する技術，技術評論社，2021.
(8) 大坪直樹，ほか，XAI（説明可能な AI）— そのとき人工知能はどう考えたのか，リックテレコム，2021.
(9) A. Adadi and M. Berrada, "Peeking inside the black-box: A survey on explainable artificial intelligence (XAI)," IEEE Access, vol.6, pp.52138–52160, 2018.
(10) R. Guidotti, et al., "A survey of methods for explaining black box models," ACM Computing Surveys, vol.51, no.5, pp.93:1–93:42, 2018.
(11) A. Barredo Arrieta, et al., "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," Information Fusion, vol.58, pp.82–115, 2020.
(12) W. Samek, et al., "Explaining deep neural networks and beyond: A review of methods and applications," Proc. IEEE, vol.109, pp.247–278, 2021.
(13) N. Burkart and M.F. Huber, "A survey on the explainability of supervised machine learning," J. Artif. Intell. Res., vol.70, pp.245–317, 2021.
(14) B.G. Buchanan and E.H. Shortliffe, eds., Rule-based Expert Systems, Addision-Wesley, 1984.
(15) R. Andrews, J. Diederich, and A.B. Tickle, "Survey and critique of techniques for extracting rules from trained artificial neural networks," Knowledge-Based Systems, vol.8, no.6, pp.373–389, 1995.
(16) N. Barakat and A.P. Bradley, "Rule extraction from support vector machines: A review," Neurocomputing, vol.74, pp.178–190, 2010.
(17) A. Hotho, S. Staab, and G. Stumme, "Explaining text clustering results using semantic structures," Proc. PKDD-03, 2003.
(18) D. Jannach, M. Zanker, A. Felfernig, and G. Friedrich, eds., Recommender Systems: An Introduction, The Cambridge University Press, 2011;（邦訳）情報推薦システム入門：理論と実践，共立出版.
(19) A. Nguyen, J. Yosinski, and J. Clune, "Understanding neural networks via feature visualization: A survey," in Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, pp.55–76, Springer, 2019.
(20) M. Robnik-Šikonja and I. Kononenko, "Explaining classifications for individual instances," IEEE Trans. Knowl. Data Eng., vol.20, pp.589–600, 2008.
(21) E. Štrumbelj and I. Kononenko, "An efficient explanation of individual classifiers using game theory," J. Mach. Learn. Res., vol.11, pp.1–18, 2010.
(22) J. Cassens and A. Kofod-Petersen, "Designing explanation aware systems: The quest for explanation patterns," Proc. the 2007 AAAI WS. on Explanation-aware Computing (ExaCt-07), 2007.
(23) K. Simonyan, A. Vedaldi, and A. Zisserman, "Deep inside convolutional networks: Visualising image classification models and saliency map," Proc. ICLR-14 Workshop Track, 2014.
(24) M.D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," Proc. ECCV-14, 2014.
(25) S. Bach, et al., "On pixel-wise explanations for non-linear classifier decisions by layer-wise relevance propagation," PLOS ONE, vol.10, no.7, 2015.
(26) M.T. Ribeiro, S. Singh, and C. Guestrin, "Why should I trust you? — Explaining the predictions of any classifier," Proc. KDD-16, 2016.
(27) S.M. Lundberg and S.-I. Lee, "A unified approach to interpreting model predictions," Proc. NIPS-17, 2017.
(28) P.W. Koh and P. Liang, "Understanding black-box predictions via influence functions," Proc. ICML-17, 2017.
(29) R.R. Selvaraju, et al., "Grad-CAM: Visual explanations from deep networks via gradient-based localization," Proc. ICCV-17, 2017.
(30) A. Shrikumar, P. Greenside, and A. Kundaje, "Learning important features through propagating activation differences," Proc. ICML-17, 2017.
(31) M. Sundararajan, A. Taly, and Q. Yan, "Axiomatic attribution for deep networks," Proc. ICML-17, 2017.
(32) J. Adebayo, et al., "Sanity checks for saliency maps," Proc. NeurIPS-18, 2018.
(33) B. Kim, et al., "Interpretability beyond feature attribution: Quantitative testing with concept activation vectors (TCAV)," Proc. ICML-18, 2018.
(34) T. Miller, "Explanation in artificial intelligence: Insights from the social sciences," Artif. Intell., vol.267, pp.1–38, 2019.
(35) C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," Nature Machine Intelligence, vol.1, pp.206–215, 2019.
(36) C.J. Cai, et al., "Human-centered tools for coping with imperfect algorithms during medical decision-making," Proc. CHI-19, 2019.
(37) Z.C. Lipton, "The mythos of model interpretability," Commun. ACM, vol.61, pp.36–43, 2018.
(38) R.R. Hoffman and G. Klein, "Explaining explanation, Part 1: Theoretical foundations," IEEE Intell. Syst., vol.32, no.3, pp.68–73, 2017.
(39) R.R. Hoffman, S.T. Mueller, and G. Klein, "Explaining explanation, part 2: Empirical foundations," IEEE Intell. Syst., vol.32, no.4, pp.78–86, 2017.
(40) M. Danilevsky, et al., "A survey of the state of explainable AI for natural language processing," Proc. the 1st Conf. of the Asia-Pacific Chap. of the ACL and the 10th Int'l Joint Conf. on Natural Language Processing (AACL/IJCNLP-20), 2020.
(41) R. Ying, et al., "GNNExplainer: Generating explanations for graph neural networks," Proc. NeurIPS-19, 2019.
(42) J. Crabbé and M. van der Schaar, "Explaining time series predictions with dynamic masks," Proc. ICML-21, 2021.
(43) U. Schlegel and D.A. Keim, "Time series model attribution visualizations as explanations," Proc. the 2021 IEEE WS. on Trust and Expertise in Visual Analytics

(TREX-21), 2021.
(44) L.A. Hendricks, et al., “Generating visual explanations,” Proc. ECCV-16, 2016.
(45) E. Angelino, et al., “Learning certifiably optimal rule lists for categorical data,” J. Mach. Learn. Res., vol.18, pp.234:1–234:18, 2017.
(46) C. Chen, et al., “This looks like that: Deep learning for interpretable image recognition,” Proc. NeurIPS-19, 2019.
(47) T. Hastie and R. Tibshirani, “Generalized additive models,” Statistical Science, vol.1, pp.297–318, 1986.
(48) Y. Lou, et al., “Accurate intelligible models with pairwise interactions,” Proc. KDD-13, 2013.
(49) C.-H. Chang, S. Tan, B. Lengerich, A. Goldenberg, and R. Caruana, “How interpretable and trustworthy are GAMs?,” Proc. KDD-21, 2021.
(50) G. Montavon, W. Samek, and K.-R. Müller, “Methods for interpreting and understanding deep neural networks,” Digit. Signal Process., vol.73, pp.1–15, 2018.
(51) M. Ancona, E. Ceolini, C. Öztireli, and M. Gross, “Towards better understanding gradient-based attribution methods for deep neural networks,” Proc. ICLR-18, 2018.
(52) J. Gu, Y. Yang, and V. Tresp, “Understanding individual decisions of CNNs via contrastive backpropagation,” Proc. the 14th Asian Conf. on Computer Vision (ACCV-18), 2018.
(53) H. Tsunakawa, et al., “Contrastive relevance propagation for interpreting predictions by a single-shot object detector,” Proc. IJCNN-19, 2019.
(54) W.-J. Nam, et al., “Relative attributing propagation: Interpreting the comparative contributions of individual units in deep neural networks,” Proc. AAAI-20, 2020.
(55) B. Zhou, A. Khosla, A. Lapedriza, A. Oliva, and A. Torralba, “Learning deep features for discriminative localization,” Proc. CVPR-16, 2016.
(56) A. Chattopadhay, A. Sarkar, P. Howlader, and V. N Balasubramanian, “Grad-CAM++: Generalized gradient-based visual explanations for deep convolutional networks,” Proc. the 2018 IEEE Winter Conf. on Applications of Computer Vision (WACV-18), 2018.
(57) V. Petsiuk, A. Das, and K. Saenko, “RISE: Randomized input sampling for explanation of black-box models,” Proc. British Machine Vision Conf. 2018 (BMVC-18), 2018.
(58) L.M. Zintgraf, T.S. Cohen, T. Adel, and M. Welling, “Visualizing deep neural network decisions: Prediction difference analysis,” Proc. ICLR-17, 2017.
(59) K. Hanawa, S. Yokoi, S. Hara, and K. Inui, “Evaluation of similarity-based explanations,” Proc. ICLR-21, 2021.
(60) P. Samangouei, A. Saeedi, L. Nakagawa, and N. Silberman, “ExplainGAN: Model explanation via decision boundary crossing transformations,” Proc. ECCV-18, 2018.
(61) M. Suzuki, Y. Kameya, T. Kutsuna, and N. Mitsumoto, “Understanding the reason for misclassification by generating counterfactual images,” Proc. the 17th Int’l Conf. on Machine Vision Applications (MVA-21), 2021.
(62) J. Huysmans, et al., “An empirical evaluation of the comprehensibility of decision table, tree and rule based predictive models,” Decision Support Systems, vol.51, no.1, pp.141–154, 2011.
(63) H. Lakkaraju, S.H. Bach, and J. Leskovec, “Interpretable decision sets: A joint framework for description and prediction,” Proc. KDD-16, 2016.
(64) M.T. Ribeiro, S. Singh, and C. Guestrin, “Anchors: High-precision model-agnostic explanations,” Proc. AAAI-18, 2018.
(65) M.W. Craven and J.W. Shavlik, “Extracting tree-structured representations of trained networks,” Proc. NIPS-95, 1995.
(66) M. Sato and H. Tsukimoto, “Rule extraction from neural networks via decision tree induction,” Proc. IJCNN-01, 2001.
(67) J.R. Zilke, E.L. Mencía, and F. Janssen, “DeepRED — Rule extraction from deep neural network,” Proc. the 19th Int’l Conf. on Discovery Science (DS-16), 2016.
(68) S. Abnar and W. Zuidema, “Quantifying attention flow in Transformers,” Proc. the 58th Annual Meeting of the Association for Computational Linguistics (ACL-20), 2020.
(69) H. Fukui, T. Hirakawa, T. Yamashita, and H. Fujiyoshi, “Attention branch network: Learning of attention mechanism for visual explanation,” Proc. CVPR-19, 2019.
(70) T. Lei, R. Barzilay, and T. Jaakkola, “Rationalizing neural predictions,” Proc. the 2016 Conf. on Empirical Methods in Natural Language Processing (EMNLP-16), 2016.
(71) F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” arXiv:1702.08608, 2017.
(72) X. Lu, et al., “Crowdsourcing evaluation of saliency-based XAI methods,” Proc. ECML/PKDD-21, 2021.
(73) A. Boggust, B. Hoover, A. Satyanarayan, and H. Strobelt, “Shared interest: Measuring human-AI alignment to identify recurring patterns in model behavior,” Proc. CHI-22, 2022.
(74) W. Samek, et al., “Evaluating the visualization of what a deep neural network has learned,” IEEE Trans. Neural Netw. Learn. Syst., vol.28, no.11, pp.2660–2673, 2017.
(75) J. Adebayo, M. Muelly, I. Liccardi, and B. Kim, “Debugging tests for model explanations,” Proc. NeurIPS-20, 2020.
(76) 三津原将弘ほか，“Attention map を介した deep neural network への人の知見の組み込み，” 信学論 (D)，vol.J104-D, pp.796–807，2021.
(77) C. Gong, et al., “KeepAugment: A simple information-preserving data augmentation approach,” Proc. CVPR-21, 2021.
(78) A. Singh, S. Sengupta, and V. Lakshminarayanan, “Explainable deep learning models in medical image analysis,” J. Imaging, vol.6, 2020.
(79) D. Omeiza, H. Webb, M. Jirotka, and L. Kunze, “Explanations in autonomous driving: A survey,” IEEE Trans. Intell. Transp. Syst., Early Access, 2021.
(80) T. Kulesza, M.M. Burnett, W.-K. Wong, and S. Stumpf, “Principles of explanatory debugging to personalize interactive machine learning,” Proc. the 20th Int’l Conf. on Intelligent User Interfaces (IUI-15), 2015.
(81) F. Hohman, M. Kahng, R. Pienta, and D.H. Chau, “Visual analytics in deep learning: An interrogative survey for the next frontiers,” IEEE Trans. Vis. Comput. Graphics, vol.25, pp.2674–2693, 2019.

（SIS 研究会提案，2022 年 6 月 2 日受付，
2022 年 6 月 30 日再受付）

亀谷由隆（正員）

1995 東京工業大学工学部卒，1997 同大学院修士課程修了，2000 同大学院博士後期課程修了．博士（工学）．2001 新日鉄ソリューションズ（株）入社．2003 から東京工業大学工学部助手，2007 同助教，2012 から名城大学理工学部准教授，2022 同大学情報工学部准教授，現在に至る．確率論理プログラミング処理系の開発をはじめとする人工知能における推論・学習技術の研究に従事．2001 年度言語処理学会論文賞受賞．人工知能学会，情報処理学会，IEEE，ACM 各会員．

解　説　論　文

IC チップのサプライチェーン・セキュリティ
――真正性を脅かす課題と対策――

Supply Chain Security of IC Chips :
Problems and Solutions for Authenticity under Threat

永田　真 Makoto NAGATA

アブストラクト　現代社会を支えるエレクトロニクスにおいて，不正な電子部材の混入はセキュリティ脅威であり，なかでも，半導体 IC チップの偽造や改竄は，情報通信機器の機能・仕様や信頼性・安全性に影響する重要課題である．本稿では，サプライチェーン・セキュリティに関わる世界的な動向を俯瞰するとともに，IC チップの真正性及び IC チップに潜むハードウェアトロイに着眼し，問題の定義と抑止の方針について解説を試みる．

キーワード　半導体，集積回路，偽物，セキュリティ，サプライチェーン，ハードウェアトロイ

Abstract　Authenticity under threat is a severe issue in modern information, communication and technology（ICT）electronics. Counterfeit electronic components, particularly semiconductor integrated circuit（IC）chips, become the known problems of compromise in the reliability and safety of such ICT devices. In this report, we try to explain the general trends of supply chain security from the viewpoints of IC chip authenticity and potential hardware Trojan problems in IC chips.

Key words　Semiconductor, Integrated circuits, Counterfeits, Security, Supply chain, Hardware Trojan

1. はじめに

近年，感染症のパンデミックや地政学的なリスクなど，地球規模の社会課題が台頭し，かねてから指摘されてきたサプライチェーン・セキュリティの脅威がますます顕在化している．米国では，オバマ政権時代に「グローバル・サプライチェーン・セキュリティの国家戦略」が制定され（2012 年 1 月），安全保障と経済発展には，食，薬，エネルギー，そして生活物資を含む幅広い産業分野において，効率的で安定的な国際流通の維持，及び新たな脅威や危険への耐性と対応が肝要であり，このために，あらゆるステークホルダーの参画によるサプライチェーンの強靭化がうたわれている．しかしながら，それから 10 年を経た現在，サプライチェーン・セキュリティを脅かす事象は多くの産業セグメント及び様々な地域において遍く発生し，世界経済に大きな影響を与え続けている．とりわけ，現代社会を支える情報通信エレクトロニクスにおいて，半導体製品の製造と流通に潜むセキュリティ課題は喫緊の解決を必要としている．

半導体のサプライチェーン・セキュリティに関して，米国では，軍用途の装備品において「偽物」の電子部品が混入している事実が上院議員の調査により指摘され，先述した国家戦略の制定と同じ時期に，国防権限法（NDAA[注1]）の 2012 年度法案において不正な電子部品の検知と排除の取り組みが可決された．その後，当該の法律において，サプライチェーン・セキュリティにかかる改定がほぼ毎年継続しており，2020 年度法案では，国防総省の調達する電子部品（半導体製品）に関し，信頼できるサプライチェーンの確立とセキュリティ標準化について言及されている．

このような不正な電子部品の流通は，市民生活を支える重要インフラ，更には一般社会に流通する電子機器（民生品）においても重大な脅威であり，その原因と防止策の理解は安全・安心な社会の維持に不可欠である[1]．これまでの 10 年間の取り組みを踏まえ，不正な電子部品を検知し排除する世界的な枠組みの構築に向けた不断の努力が求められよう．

ところで欧州では，欧州連合ネットワーク情報セキュリティ庁（ENISA[注2]）が情報通信分野における「サプライチェーン・インテグリティ」について 2012 年 2 月に報告を開始し，2015 年 5 月に報告書を公開した[2]．サプライチェーンの概形を定義し，製品のライフサイクルに照らしたリスクの所在と管理について概説するとともに，サプライチェーンを広義のシステムとみなしてセキュリティ評価基準の国際的な共通手段（コモンクライテリア，ISO/IEC 15408）を適用する可能性，また，製品供給者と製品の真正性について国際標準規格（例えば，品質管理基準 ISO9000 やセキュリティ管理基準 ISO27000 など）に基づいて評価・認証する枠組みの可能性を示唆している．また近年，ENI-

永田　真　神戸大学大学院科学技術イノベーション研究科
E-mail　nagata@cs.kobe-u.ac.jp
Makoto NAGATA, Member Member (Kobe University, 1-1 Rokkodaicho, Nada-ku, Kobe-shi, Japan).
電子情報通信学会 基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.93-99 2022 年 10 月

（注 1）：National Defense Authorization Act, NDAA
（注 2）：European Network and Information Security Agency, ENISA

SA は産業界で急増するサイバー攻撃のインシデントを踏まえ，「サプライチェーン・アタックの脅威」について提言をまとめている（2021 年 7 月）[3]．サプライチェーンにおける供給者と需要者のそれぞれにおける潜在的な攻撃手法と攻撃対象（アセット）を定義し，2020〜2021 年の実例を調査・分析している．ここで例示されるインシデントの多くはマルウェアを含むソフトウェアによる攻撃であり，また，アセットとして様々なコードやデータが攻撃されている．

サプライチェーン・セキュリティは，高度に情報化された社会システムにおける潜在的脅威として国家レベルで認知される社会課題である．自社製品を製造・販売する事業者（OEM(注3)や OCM(注4)）は，製品を構成する部材の調達や受託製造業者の選定において，真正性の認定という事業上の重要課題となる行為が求められる．その対象は，アプリケーションやネットワークのソフトウェアにとどまらず，情報通信を担うハードウェアに拡がっており，とりわけ，エレクトロニクスの核となる半導体集積回路製品（以後，IC チップ）に対する脅威の常態化が危惧されている．製品の真正性をないがしろにするまがいものや怪しい IC チップの流通，更には，情報セキュリティの危殆化を引き起こす悪意ある機能（ハードウェアトロイ：マルウェアに相当するハードウェア）が潜む IC チップの混入を想定し，その可能性を排除せずに事前の対策を施す必要がある．

サプライチェーン・セキュリティはあらゆる産業領域に関連しており，とりわけ近年は経済安全保障における上位概念の一つとして議論されている．なかでも，IC チップは，米国・欧州・アジアの各国における戦略物資であり，そのサプライチェーン・セキュリティが影響する範囲は産業・地域において極めて幅広く，脅威の所在と対策の大筋を把握することは，今後の半導体技術の研究開発において有用と考える．そこで本稿は，IC チップのサプライチェーン・セキュリティに主眼を置き，IC チップの真正性（第 2 章）と IC チップに潜むハードウェアトロイ（第 3 章）について解説する．

2. IC チップの真正性

2.1 不正な半導体の流通

世界半導体市場統計によれば，2021 年度の世界市場は 5,560 億ドルと過去最大の規模であった．今後，在宅需要の増大や 5G 展開によるデータ通信の拡大が見込まれ，2022 年度は前年比 16.3% の成長が予測されている．このような半導体の需要拡大に対して，とりわけ最先端の半導体工場の生産キャパシティは逼迫しており，更に資材流通の停滞も影響して，世界的な半導体供給不足が知られている．このような状況のもと，半導体の入手競争が激化し，その結果，不正な半導体が流通ルートに混入する可能性が高まっている．すなわち，非正規な IC チップである，再生品（廃棄された電子機器から取り出したもの）や偽造品（リバースエンジニアリングによりコピー製造したもの），更には粗悪品（パッケージのみ類似するが中身は異なるもの）が，サプライチェーンに入り込む危険が生じている．世界半導体会議（日本を含む世界 6 地域の半導体工業会から構成される）は，不正な半導体の流通に関する白書（2018 年 5 月）[4] を発行し，その背景，実態と危険性について詳細な説明を与えるとともに，2021 年 5 月にも改めて注意を喚起している [5]．

欧州知的財産庁（EUIPO(注5)）と欧州刑事警察機構（Europol）の共同調査報告（2022 年 3 月）[6] では，欧州にて偽物製品の流通の影響を強く受けている製品領域（衣料，電子，食料，農薬，などの 11 領域）を挙げている．電子製品領域では，携帯電話機の偽造品を大規模に市場投入する犯罪組織の存在を指摘しており，これに関連して，半導体の供給不足に便乗した不正な IC チップの流通を警戒している．

半導体メーカも，怪しい半導体製品の流通を警戒している．Maxim Integrated 社（現在は Analog Devices 社の一部）は，その公開レポート [7] において，自社の偽物製品の流通事例（再生品に再印字された製品ラベルにて製品グレードに偽装があるもの，及び，極めて純正品に近いパッケージングであるが社名にスペルミスのあるもの）を示した．供給者として安易で安価な購買の危険性について言及するとともに，購入者における偽造品の排除を啓蒙している．また，Intel 社や AMD 社のプロセッサ IC チップの偽物が市場に流通している可能性がインターネットメディア情報にて指摘され，これに対して，半導体メーカは純正品の外観などの判断方法について説明している [8]．

2.2 IC チップの真正性に向けて

このような背景状況のもと，IC チップの真正性はどのように担保されるだろうか．各国の政府，半導体メーカ，研究機関の昨今の動向を俯瞰すると，以下に示す三つの方針を抽出できる（表 1）．これらの方針は，図 1 に示すように共存可能な関係にあり，産業政策・事業環境整備・研究開発の視点から，官・産・学のそれぞれが得意とする取り組みのもとで連携して具現できる．三つの方針の全てを包含し，更に，信頼できる国の組織や事業者の相互運用を具体化すれば，国

表 1　IC チップの真正性を守る三つの方針

①半導体製造能力の増強	IC チップ真正品の流通を促進する環境の整備
②不正な半導体流通の抑止	IC チップの真正性を検証・認定する制度の導入
③ IC チップ真正性保証技術の開発	IC チップの真正性を宣言・保証する技術の開発

（注 3）：Original Equipment Manufacturer, OEM

（注 4）：Original Component Manufacturer, OCM

（注 5）：European Union Intellectual Property Office, EUIPO

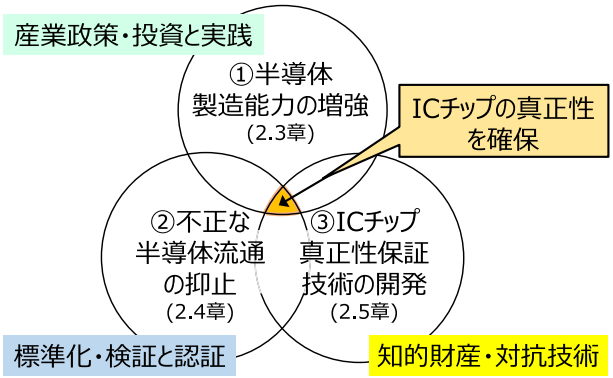


図 1　IC チップの真正性に向けた取り組みの関係（及び本稿における該当章）

際的な IC チップのサプライチェーン・インテグリティを高いレベルで維持できると考えられる（図 1 の中心部分に相当）.

① 半導体製造能力の増強：IC チップの供給能力を増強することで，純正かつ新品の IC チップの取引を促し，不正な商品の価値と混入を抑止する．更に，自国や自地域における一定の生産量を確保することで，半導体人材の育成を啓蒙し，また，国際流通における潜在的な脅威を排除する．

② 不正な半導体流通の抑止：不正な IC チップの搭載された電子機器では，信頼性の低下や不正機能の発現などの恐れがある．OEM や OCM における品質保証の取り組みとして，半導体製品の真正性を検証・認定する指針や基準の制定及び試験・検証手法の標準化を導入することにより，市場から偽造品を検知・排除する．

③ IC チップ真正性保証技術の開発：IC チップの設計・製造・パッケージングの工程において，真正性の根拠となる情報や履歴の情報を抽出あるいは埋設し，広域で管理する回路システム技術を探求する．電子機器のサプライチェーンにおいて IC チップの追跡性や固有性（ID）を付与することで，真正性を保証する．また，これらの技術の存在は，第三者による偽造や偽装を困難化し，動機を消失させる．

これらの方針について最近の動向を以下にまとめる．

2.3　半導体製造能力の増強

米国政府は，経済安全保障政策として，国防権限法（NDAA）の 2021 年度法案において，520 億ドルを投じて半導体分野の研究開発及び量産製造における国際的な優位性を獲得・維持する取り組みについて可決した．商務省（DoC[注6]）と国立標準技術研究所（NIST[注7]）による半導体推進プログラム（CHIPS[注8]）では，半導体製品の米国内製造を喚起・優遇するため資金提供を進めている．人工知能分野や高性能計算を担う最先端デバイスの製造に限定せず，重要インフラや基幹インフラを支える既存プロセスによる半導体製品の量産工場も対象としており，半導体産業に関わる雇用創出と人材確保を視野に入れた長期的な取り組みである．また，国防総省（DoD[注9]）の国防高等研究計画局（DARPA[注10]）を筆頭として，エネルギー省（DoE[注11]）や国立科学財団（NSF[注12]）などの政府機関の連携による半導体分野の研究開発資金の提供も際立っており，エレクトロニクス復興イニシアチブ（ERI[注13]）が 2018 年から牽引してきた半導体分野の研究開発プロジェクトの拡充が見込まれる．

ERI サミット 2021（2021 年 10 月）[9]では，半導体製品のオフショア製造，とりわけアジアで続く量産規模の拡大を半導体サプライチェーンの脅威とみなし，米国内における半導体製造を活性化する取り組みとして，22 nm FinFET デバイス製造（DoD 用途向け）や各種ソフトウェアツールのライセンス提供（DARPA Toolbox）が紹介されている．また，これらの研究開発プロジェクトにおける proof of concept（概念実証）を担う最先端半導体プロトタイプ製造の重要性を指摘するとともに，米国内におけるパイロット試作ラインの整備も計画されている．ERI の着眼点は，(1) 先端エレクトロニクスへの依存性，(2) 製造能力の増強，(3) マイクロシステムの複雑化，そして (4) ハードウェアセキュリティの脅威に対応することであり，このための研究開発プロジェクトを立案・実施している．エレクトロニクス分野における新技術の創出を加速することにより，米国の優位性が保たれると宣言している．

米国の半導体供給能力は 1990 年に世界の 37% を占めていたが，その後のオフショア製造シフトにより，2021 年には 12% に低迷している．CHIPS のもと，半導体メーカ（多国籍企業を含む）による米国内製造の増強計画が周知されてきた．例えば，2022 年に，Intel 社は 200 億ドル規模の投資によりオハイオ州に二つの製造ラインを新設し，TI 社は 300 億ドル規模の先端 12 インチ製造ラインをテキサス州に整備する計画である．また，2021 年以降，TSMC 社（台湾）はアリゾナ州に，Samsung 社（韓国）はテキサス州に，それぞれの国外半導体製造拠点を米国内に設けている．このように，半導体サプライチェーンの脅威を排除すべく，全米で取り組みが進んでいる．更に，NDAA のもと，米国における半導体分野の研究開発・製造拠点整備・人材供給を戦略的に進める組織として，国立半導体技術センター（NSTC[注14]）

(注 6)：Department of Commerce, DoC
(注 7)：National Institute of Standards and Technology, NIST
(注 8)：Creating Helpful Incentives to Produce Semiconductors for America, CHIPS
(注 9)：Department of Defense, DoD
(注 10)：Defense Advanced Research Projects Agency, DARPA
(注 11)：Department of Energy, DoE
(注 12)：National Science Foundation, NSF
(注 13)：Electronics Resurgence Initiative, ERI
(注 14)：National Semiconductor Technology Center, NSTC

の設立構想が進められている．半導体の業界団体であるSEMIや産学共同研究を推進するSRC(注15)の活動とあわせて，米国における研究開発の活性化に目を向ける必要がある．

欧州委員会は，2022年2月にEuropean Chips Act[10]として，430億ユーロ規模を想定した半導体の研究開発・製造能力の増強プログラムを提案し，2030年に全世界市場の30%程度を確保することを目標としている．その背景には，世界的な半導体不足による様々な製品市場の縮小があり，米国と同様，半導体サプライチェーンの脅威を排除すること（アジアにおける製造の偏りを是正すること）を急務と捉えている．

2.4 不正な半導体流通の抑止

米国の自動車技術者協会（SAE(注16)）は，かねてより航空宇宙や重要インフラの関連分野における信用できない電子部品や電子部材の脅威を指摘しており，サプライチェーン・セキュリティ課題として文書を発行する（AS55553 : 2009年及びその後の改訂と2022年4月の改訂版）[11]とともに，偽物の疑いのある電子部品の標準試験法を定義した（AS6171 : 2016年10月及び2018年4月の改訂版）[12]．本来，製品の構成部材は真正な電子部品の供給主体であるOEMやOCMあるいはその監督下の正規代理店から調達するべきであるものの，製品の更新や生産中止，あるいは昨今の入手困難な状況など様々な理由により，別経路の納入を排除できないことが想定されている．そこでは，電子部品及び販売業者，更には自社の内部監査における適正なリスク評価について述べるとともに，外観検査法，蛍光X線分析法，樹脂などの封止を除去した物理検査法，更には放射線解析，音響分析及び電気試験などの多様な評価・検証の手段を網羅的に定義していることにも特徴がある．

システムレベルのセキュリティにおけるサプライチェーンの課題と対応指針について，NISTが多数の文書を公開している．古くは，汎用的な計算機システムにおける最低位のハードウェア・ソフトウェアインタフェースを担うBIOS機能について，非正規ICチップへの置き換え，あるいは悪意あるファームウェアへの書き換えの可能性を指摘し，保護指針を示した（2011年4月）[13]．サイバーシステムの全体に関わるサプライチェーンについてリスクを論じた文書では，企業におけるサプライチェーン・リスク管理の概念を示し，多様なリスクの存在と原因を分析している（2022年5月）[14]．サプライチェーン・セキュリティに関連して，国の安全保障，企業の信用，顧客の利益など，それぞれの階層における主体の価値に影響を及ぼす脅威の存在及びそのリスクの評価と対策について，幾つかのシナリオを組み上げて考証しており，このような脅威を引き起こす要素の一つとして偽造品を挙げている．そのほかの草案や文書においても，モバイルシステム，Internet of Things（IoT）システム，レジリエント・システムや高信頼システムなどを題材としたサプライチェーン・セキュリティの課題と対策の検討結果が逐次公開されており，国際社会のすみずみに顕在するテーマとして多面的な検討が続けられていることが分かる．

国際標準化機構・国際電気標準会議（ISO/IEC(注17)）は，航空宇宙・高性能機器あるいは防衛産業において，電子部材の調達における再生品や偽装品・詐称品の混入を避けるための要件を国際標準として定め（2019年9月）[15]，また，OEMやOCMにひもづけられない販売経路による調達についても同様の要件を定めている[16]．これらの産業については，極めて高いレベルの品質管理と高度なサプライチェーン・リスク耐性が要求されることから，電子部材の調達における管理計画（electronic components management plan, ECMP）の標準様式と認証手段も定められている[17]．他方，情報通信産業においては，ISO/IECと業界団体コンソーシアム（The Open Group）が連動して，サプライチェーン・セキュリティの課題，とりわけ，悪意ある偽物製品の排除に関する指針，推奨，あるいは要件を明示し，その実践主体である事業者が製品のライフサイクル（設計・製造・販売・保守・廃棄）にわたり適正に対処する能力を有することについて認定する制度を標準化している[18]．これにより，一般・民生の製品を製造・供給する事業者における正当性，あるいは信頼の拠所を備えることができる．

半導体産業における技術標準規格を扱う事業者団体であるJEDECは，サプライチェーンに電子部品の偽造品が混入することを防ぐ事業上の実践的な手段として，方針，計画，契約，あるいは顧客からの返品の扱い，を定義した文書を発行している（2016年3月及び2021年1月の改定版）[19]．

このように，米国の標準化組織や産業団体が中心となり，サプライチェーン・リスクの整理，また，とりわけ怪しい電子部材の流通や混入を検知・排除する制度の構築と運用が積極的に進められている．これにより，軍事・民生によらず，サプライチェーン・セキュリティに関する製品事業者の意識が高まり，市場の自己浄化につながることが期待される．なお，怪しい・不正な電子部品の市場統計については，米国ERAI社（1995年創業）が調査を継続している[1],[20]．世界的なインシデントのレポート収集や，事業者向けの偽造品対策トレーニングの提供も業務としている．

2.5 ICチップ真正性保証技術の開発

ICチップの真正性を保証する技術の研究開発も盛んである．半導体チップ，パッケージ，あるいはプリント基板において自己提示する，更には追跡性を保証する技術の報告がなされている．とりわけ米国はICチップを含むサプライ

（注15）：Semiconudctor Research Corporation, SRC

（注16）：Society of Automotive Engineers, SAE

（注17）：International Organization for Standardization/International Electrotechnical Commission, ISO/IEC

チェーン・セキュリティに古くから敏感であり，DARPA による研究開発プログラム（Supply Chain Hardware Integrity for Electronics Defense, SHIELD）[21]は，2014 年 3 月に告知され，2015～2019 年にかけて実施，そして研究成果の全体像が 2020 年 8 月に公開された．研究開発には Charles Stark Draper Laboratory，Sandia National Labs，SRI International，Northrop Grumman，IBM などの私的・公的研究開発組織や軍需に強い大企業群と，CMU，UC. Berkeley，Georgia Tech.，他多数の大学が参画した．SHIELD Dielet と呼ぶ 100 μm×100 μm 程度の超小型パッシブ無線 ID チップを核として，これを様々な IC チップや電子部品のパッケージに封入し，その ID 情報をクラウドシステムに登録することで，電子機器のライフサイクルにわたる追跡性を確保する仕組みを完成している．SHIELD Dielet は 14 nm CMOS 技術により設計・製造され，1 セント以下の搭載コストを目標に量産される見通しである．シングル・システムチップとして構成され，セキュリティ機能としてワンタイム・プログラマブルメモリ，AES[注18]暗号及び PUF[注19]による ID と鍵生成，誘導結合により電力と情報を伝送する機能，などを集積している．また，封止技術に関して，アセンブリ工程における熱履歴などのセンシング機能，あるいはリバースエンジニアリングなどに対する壊れやすさ特性の付与，など，耐攻撃性を備える技術もあわせて開発されている．その後，セキュリティ機能 IC チップについて自動設計技術の創出を狙う研究開発プログラム（Automatic Implementation of Secure Silicon, AISS）[22]が 2019 年 4 月に告知され，現在進行中である．

我が国では，IC チップを含むハードウェアのセキュリティに関連する研究開発プロジェクトとして，戦略的イノベーション創造プログラム（SIP[注20]）のもと，「重要インフラ等におけるサイバーセキュリティの確保」（2015～2019 年度）[23]，及び，「IoT 社会に対応したサイバー・フィジカル・セキュリティ」（2018～2022 年度）[24]が推進されてきた．セキュリティシステムのサプライチェーン・リスクを排除すべく「信頼の基点」となる IC チップ技術やシステム技術が開発されている．IoT システムにおいて公開鍵方式の暗号技術を遍く利用するビジョンを掲げ，これを具現する研究成果として，図 2 に示すように，末端ノード，中間ノード，そして広域のネットワークを通じた上位ノード間のデータ通信において高度な暗号機能を応用するためのセキュア IC チップ（secure cryptographic unit, SCU）を開発した[25]．IoT セキュリティにおける信頼の基点を確立すべく，高速・省電力・小面積な暗号 IC チップ構築技術，公開鍵運用技術，及び，サイドチャネル攻撃やハードウェアトロイ攻撃（次章）に対する高耐化技術もあわせて開発されている．IC チップのサプライチェーン・インテグリティに向けて，論理的なセキュア・ゾーンの構築及び物理的なセキュア・パッケージングの

（注 18）：Advanced Encryption Standard, AES
（注 19）：Physically Unclonable Function, PUF
（注 20）：Cross-ministerial Strategic Innovation Promotion Program, SIP

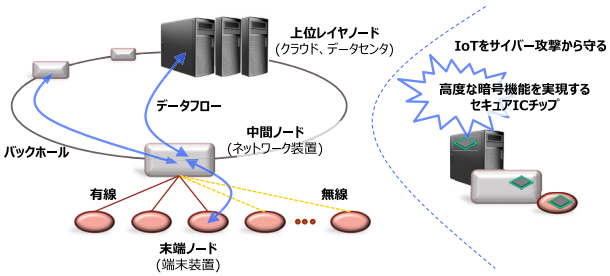


図 2　IoT セキュリティを担うセキュア IC チップ

導入により，ハードウェア・ソフトウェア統合のもと，セキュリティ機能を担う安全領域を IC チップの内部に確保する．これを IoT システムにおける信頼の基点として利活用する技術の開発と運用制度の検討が進められている．

3.　IC チップに潜むハードウェアトロイ

IC チップの設計・製造・封止の過程で，悪意ある攻撃者により，例えば，サイドチャネル情報漏洩を助長する構造の導入や，秘密情報にアクセスするバックドア機能の挿入などを引き起こす，意図的な回路・デバイスの追加や回路・レイアウトの改竄が加えられる可能性が世界的に議論されている．一般に，ハードウェアトロイ（ハードウェア版トロイの木馬）として認識され，IC チップの真正性を侵害するアクティブな攻撃手段であり，IC チップのサプライチェーン・セキュリティを危殆化する恐れのある重要課題である．

通常の IC チップ設計開発体制において，悪意を抱いた技術者・設計者による意図的な設計改変が容易に見過ごされることは考えにくい．しかしながら，IC チップの設計・製造・封止の工程分離が進み，国際的な分業が一般化されたこと，半導体製品需要の拡大により流通チャネルの多様化が進んでいること，などを背景として，ハードウェアトロイの存在は，いまだ論理的に排斥されていない．このため，世界的に，設計データの改竄検知手法や模造・偽造を防ぐリバースエンジニアリング難易化手法，怪しい回路動作を検知するモニタリング手法や IC チップ試験法などの研究開発が盛んな状況にある．ハードウェアトロイは，半導体産業におけるインシデントとしては表面化されにくいものの，潜在的な脅威として研究開発の動機は明瞭であり，その解決に向けた知見は，学術的成果として国際会議や学術論文誌において活発に報告され，蓄積されている．

ところで，半導体メーカは品質保証部門を保持するので，IC チップ設計・製造の真正性を担保し，純正品の流通を保証できると考えられる．しかしながら，高度で複雑なシステムチップ設計においては，外部事業者（サードパーティー）の作製する回路コア（設計データ）の導入が一般的である．また，システムの要素機能を具備した IC チップ（製造品）のチップレット供給も進展している．いずれもハードウェアトロイ混入の可能性がある．更に，IC チップの搭載システムにおいて，パッケージやプリント基板における悪意ある回

路構造（例えば，極めて小さなICチップなど）の挿入は，より具体的な可能性がある．

いずれも，ICチップのサプライチェーン・セキュリティにおける問題提起であり，論理的，電気的，物理的，あるいは電磁的な手法により，ICチップを含むシステム全体のハードウェアトロイフリーを検証して認証する枠組みの構築が求められている．今後，ハードウェアセキュリティ分野の研究開発に従事する大学や研究所[26]の取り組みが期待される．

4. ま と め

ICチップのサプライチェーン・セキュリティについて俯瞰した．不正なICチップの脅威と抑止について，これまで10年を超える継続的な議論や検討がなされてきたが，その間も半導体市場は伸長を続け，また，近年は半導体の需給アンバランスがセキュリティ・ホールとして表面化していることから，サプライチェーン・セキュリティの実践はますます重要になっている．半導体製造能力の増強，不正な半導体流通の抑止，そしてICチップ真正性保証技術の開発が，取り組みの鍵となる．ICチップの真正性の確保やICチップに潜むハードウェアトロイの対策については，図3に示すように，ICチップを取り巻く多階層の技術領域において，様々な技術開発の可能性がある[27]．本稿では触れていないが，ICチップのPUF情報やサイドチャネル情報をサプライチェーン・セキュリティに応用する技術が，欧米のスタートアップ企業により提供されつつある．

本稿では，最先端半導体製品にかかる経済安全保障及び商務通商上の懸念を明確に表明している欧米の動向を中心に述べた．我が国においても，外国企業の誘致による国内半導体製造拠点の整備，もとより材料開発・アセンブリ技術に優れた国内企業の強みを生かす取り組み，大学における半導体研究の再活性化，などの産業政策が報道されている．サプライチェーン・セキュリティに向けた投資や研究開発の大きな流れにつながれば，ICチップの需要大国として，また，信頼性の高い製品の供給に長けた国家として，影響力を維持・発展できると期待する．半導体製品に関わる産業力の向上，不正なICチップを排除する制度の構築と技術開発の実践は，国際的な取引における優劣に影響を及ぼすものであり，喫緊かつ継続的な課題である．

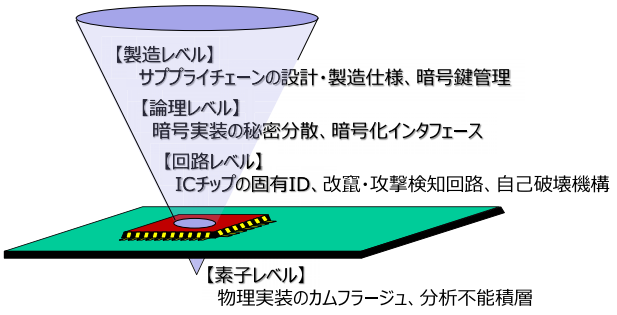


図3　ICチップのサプライチェーン・セキュリティ

謝辞　本研究はJSPS科研費JP22H04999の助成を受けたものです．

文　献

(1) 永田真，“ICチップの真正性の確保と対策～ハードウェアセキュリティの根源的課題に向き合う～，”信学FR誌，vol. 8, no. 3, pp. 177-182, Jan. 2015.
(2) “Supply chain integrity, an overview of the ICT supply chain risks and challenges, and vision for the way forward,” ENISA, Aug. 2015.
(3) “Threat landscape for supply chain attacks,” ENISA, July 2021.
(4) “Winning the battle against counterfeit semiconductor products,” World Semiconductor Council White Paper, May 2018.
(5) “Counterfeit semiconductors and the online environment,” World Semiconductor Council, June 2021.
(6) “Intellectual Property Crime Threat Assessment 2022,” EUIPO, March 2022.
(7) “Counterfeit ICs—the serious problem that only we can make go away,” Tutorial 5458, Maxim Integrated, Oct. 2012.
(8) “How to determine the authenticity of an AMD boxed processor,” https://www.amd.com/en/support/kb/warranty-information/pib-authenticity（accessed June 19, 2022.）
(9) ERI summit, https://eri-summit.darpa.mil/about-the-summit, accessed June 19, 2022.
(10) “Digital sovereignty : Commission proposes Chips Act to confront semiconductor shortages and strengthen Europe's technological leadership,” European Commission, press release, Feb. 2022.
(11) “Counterfeit electrical, electronic, and electromechanical（EEE）parts ; Avoidance, detection, mitigation, and disposition,” SAE, AS5553D, April 2022.
(12) “Test methods standard ; General requirements, suspect/counterfeit, electrical, electronic, and electromechanical parts,” SAE, AS6171A, April 2018.
(13) “BIOS Protection Guidelines,” NIST, Special Publication 800-147, April 2011.
(14) “Cybersecurity supply chain risk management practices for systems and organizations,” NIST, Special Publication 800-161r1, May 2022.
(15) “Process management for avionics—counterfeit prevention—part 1 : Avoiding the use of counterfeit, fraudulent and recycled electronic components,” IEC, 62668-1 : 2019, Sept. 2019.
(16) “Process management for avionics—counterfeit prevention—part 2 : Managing electronic components from non-franchised sources,” IEC, 62668-2 : 2019, July 2019.
(17) “Process management for avionics—management plan—part 1 : Preparation and maintenance of an electronic components management plan,” IEC, 62239-1 : 2018, Sept. 2018.
(18) “Information technology—Open Trusted Technology Provider™ Standard（O-TTPS）—mitigating maliciously tainted and counterfeit products—part 1 : Requirements and recommendations,” ISO/IEC, 20243-1 : 2018, Feb. 2018.
(19) “Counterfeit electronic parts : Non-proliferation for manufacturers,” JEDEC, JESD243A, Jan. 2021.
(20) ERAI Incorporated, https://www.erai.com/, accessed June 19, 2022.
(21) “Supply Chain Hardware Integrity for Electronics Defense（SHIELD）（Archived）,” https://www.darpa.mil/program/supply-chain-hardware-integrity-for-electronics-defense, accessed June 19, 2022.
(22) “Automatic Implementation of Secure Silicon（AISS）,” https://www.darpa.mil/program/automatic-implementation-of-secure-silicon, accessed June 19, 2022.

(23) “戦略的イノベーション創造プログラム(SIP)/重要インフラ等におけるサイバーセキュリティの確保,” https://www.nedo.go.jp/activities/ZZJP_100109.html, accessed June 19, 2022.
(24) “戦略的イノベーション創造プログラム(SIP)第2期/IoT社会に対応したサイバー・フィジカル・セキュリティ,” https://www.nedo.go.jp/activities/ZZJP_100156.html, accessed June 19, 2022.
(25) T. Matsumoto, M. Ikeda, M. Nagata, and Y. Uemura, “Secure cryptographic unit as root-of-trust for IoT era,” IEICE Trans. Electron., vol. E104-C, no. 7, pp. 262-271, July 2021. DOI : 10.1587/transele. 2020CDI0001
(26) サイバーフィジカルセキュリティ研究センター，産業技術総合研究所，https://www.cpsec.aist.go.jp/，accessed June 19, 2022.
(27) 永田真，“ハードウェアセキュリティ～セキュアICチップの実装攻撃と対策～,” KEC情報，vol. 260, pp. 13-16, Jan. 2022.

（HWS研究会提案，2022年6月23日受付，
2022年7月3日再受付）

永田　真（正員）

平5学習院大大学院物理学専攻修士課程修了．平7広島大大学院材料工学専攻博士課程退学．同年，広島大助手，平14神戸大助教授，平21同教授．現在，同大学院科学技術イノベーション研究科長・教授．博士（工学）．半導体集積回路におけるセーフティとセキュリティ，及び量子コンピュータ向け極低温半導体技術に関する研究開発に従事．令和元～2集積回路研究専門委員会委員長．令和3よりエレクトロニクスソサイエティ副会長（編集出版担当）．令和4よりハードウェアセキュリティ研究専門委員会委員長．

解　説　論　文

プライバシー保護を考慮した秘匿化領域におけるスパースデータモデリング

Privacy-Preserving Sparse Data Modeling in Encrypted Domain

仲地孝之 Takayuki NAKACHI
坂東幸浩 Yukihiro BANDOH

アブストラクト　ビックデータ時代の到来とともに，ネットワーク上を流通するディジタルコンテンツが増加の一途をたどり，エッジ/クラウドコンピューティングでのデータ処理が急速に普及してきている．例えば，データ量を圧縮するための圧縮符号化，データ内の有意な情報を抽出するデータマイニング，データの分類や予測を行うためのモデルを自動的に学習する機械学習などが挙げられる．しかし，サービス提供者の信頼性欠如や事故によるデータの不正利用や流失によって，プライバシーを侵害する問題の発生が危惧されている．このような背景から，プライバシーを保護しつつデータ解析・信号処理を行う手法として，ランダムユニタリ変換に基づく秘匿スパースモデリングが提案されてきた．この秘匿化演算の特徴は大幅な計算量の増加を伴うことなく，1）スパースモデリングのアルゴリズムを変更することなく利用可能，2）秘匿化領域における処理により，秘匿化前の原データに対する処理結果と一致する結果を保証できる点にある．本稿では，ランダムユニタリ変換に基づく秘匿スパースモデリングの基本的な仕組みからときおこし，秘匿化領域におけるデータ処理の有効性をエッジ AI への応用例を通して概観する．

キーワード　スパースモデリング，秘匿演算，ランダムユニタリ変換，辞書学習，機械学習，エッジ AI

Abstract　With the arrival of the big data era, the amount of digital content on the network has rapidly increased. The use of edge/cloud computing has become widespread in various fields such as big data analysis. Examples include data compression to reduce the amount of data, data mining to extract significant information from data, and machine learning to automatically learn models for the classification and prediction of data. However, the use of edge/cloud computing is premised on the reliability of service providers, and there is a concern that privacy invasion problems may occur as a result of the lack of reliability and the unauthorized use or loss of data owing to accidents. To solve the problems, privacy-preserving sparse modeling based on the random unitary transform has been proposed. The features of privacy-preserving sparse modeling are that 1) it can process encrypted data without changing the algorithm of sparse modeling and 2) it guarantees no degradation of sparse modeling performance, without a significant increase in the amount of calculation. In this article, we overview the basic mechanism of the privacy-preserving sparse modeling and introduce application examples to edge AI.

Key words　Sparse modeling, Secure computation, Random unitary transform, Dictionary learning, Machine learning, Edge AI

1. はじめに

近年ビッグデータの解析をはじめ様々な分野において，エッジ/クラウドコンピューティングの利用が急速に普及してきている．例えば，データ内の有意な情報を抽出するデータマイニング，データの分類や予測を行うためのモデルを自動的に学習する機械学習などが挙げられる．しかしエッジ/クラウドコンピューティングの利用は，サービス提供者の信頼性を前提にしており，その信頼性の欠如や事故によるデータの不正利用や流失によって，プライバシーを侵害する問題の発生が危惧されている[1]．

その問題を解決する一つの方法として，ランダムユニタリ変換に基づく秘匿スパースモデリング[2]〜[7]が提案されている．秘匿スパースモデリングは，プライバシーを保護しつつデータ解析・信号処理を行う手法であり，データを秘匿化したままスパースモデリングの係数選択・推定や学習アルゴリズムの実行が可能である．万が一，エッジ/クラウドでデータが流出した場合にもコンテンツの中身を秘匿することができる．データを秘匿化したまま処理する手法は，2. 節に記載の手法など幾つか提案されているが，秘匿スパースモデリングの特徴は大幅な計算量の増加を伴うことなく，1）既存のスパースモデリングのアルゴリズムを変更することなく利用可能，2）秘匿化領域における処理により，秘匿化前の原データに対する処理結果と一致する結果を保証できる点にある．以上の特徴から，スパースモデリ

仲地孝之　正員：シニア会員　琉球大学情報基盤統括センター
E-mail takayuki.nakachi@ieee.org
坂東幸浩　正員：シニア会員　日本電信電話株式会社コンピュータ＆データサイエンス研究所
E-mail yukihiro.bandoh@m.ieice.org
Takayuki NAKACHI, Senior Member (Information Technology Center, University of the Ryukyus, 1 Senbaru, Nishihara-cho, Okinawa, 903-0213, Japan), and Yukihiro BANDOH, Senior Member (NTT Computer & data science lab., Kanagawa, 239-0847 Japan).

電子情報通信学会　基礎・境界ソサイエティ
Fundamentals Review Vol.16 No.2 pp.100–114 2022 年 10 月

ングの有効性が検証されている多くの分野へデータを秘匿したまま適用が可能である．

スパースモデリング（Sparse Modeling）[8]~[28]は膨大なデータのほとんどの要素をスパース（疎ら）と考え，非ゼロ要素に着目することでデータの本質を抽出する手法であり，大量のデータの中に隠れている有意な情報を抽出する情報処理モデルである．また，法則性を導き，断片的なデータを補完して実態を忠実に再現することも可能である．テキスト，映像・画像，音声・音響などのあらゆるディジタルコンテンツが質量ともに肥大化し続けている中，注目を集めている数理手法の一つである．深層学習に対して，1）少量データでの学習が可能，2）低い演算量，3）説明可能な AI [28]といった側面ももち，注目されている．またスパースモデリングの応用として，画像・音響信号などのメディア処理[12]，磁気共鳴画像 (Magnetic Resonance Imaging: MRI) [13]やブラックホール画像の再構成[14]，異常検知[15]，スマートセンサネットワーク[16]，脳波など生体信号の解析[17]など多数の分野へ適用され，その有効性が認められている．

本稿では，ランダムユニタリ行列に基づく秘匿スパースモデリングの基本的な仕組みからときおこし，秘匿化領域におけるデータ処理の有効性をエッジ AI への応用例を通して概観する．エッジ AI は端末近くに AI を配置し，学習・推論させる技術であり，端末近くにサーバを配置しデータ処理を行う「エッジコンピューティング」（Edge Computing）に AI を搭載したものといえる．エッジ AI はクラウド処理に対して，1）通信コストの削減，2）リアルタイム性，3）セキュリティ強化，などのメリットをもつ．秘匿スパースモデリングは軽量で少量学習データで動作するため，エッジ AI 処理と非常に相性がよい．

本稿の構成は，以下のとおりである．2. 節で秘匿演算の関連技術を概観し，3. 節でランダムユニタリ変換を用いた秘匿演算の定義と特徴について説明する．4. 節でスパースモデリングの概要と秘匿演算，5. 節でランダムユニタリ変換のセキュリティ強度について述べ，6. 節で秘匿スパースモデリングのエッジ AI への応用例について紹介する．最後にまとめと今後の展望について述べる．

2. 関連技術の概観

プライバシーデータの秘匿性を確保する方法の一つとして，データを暗号化した状態で計算可能な計算方法に期待が集まっている．例えば，マルチパーティプロトコルや準同型暗号に基づく秘密計算が挙げられる[29]~[34]．しかし，こうした秘密計算は，計算量が多いため，暗号化時に高負荷な計算を強いることになる．更に，暗号化によりデータ量が増大するため，エッジ・クラウド上の集約拠点に負荷をかけることになる．高度な映像・画像処理，リアルタイム性を要求されるアプリケーションへの適用は限定的である．これらのアプリケーションをサポートするためには，更なる改善が必要とされている．

暗号化領域における低演算処理を実現する方法として，キャンセラブルバイオメトリクス[35]~[38]が研究されてきた．例えば，その一手法であるランダム射影[39]，[40]は乱数により生成されたランダム行列を用いて，入力信号を低次元部分空間に射影する．ランダム射影は一定の条件（制約等長条件など）を満たせば，入力データの 2 点間の距離を射影前後で近似的に保存することが知られている．また，バイオハッシング[41]はランダム射影に基づく暗号化の一種である．バイオハッシングは，入力データをハッシュコードと呼ばれる二進数列に変換する．この変換は，入力データの二進数化，および入力データのランダムベクトルへの射影に基づき，行われる．これらの暗号化は，非可逆な変換であることに注意が必要である．つまり，変換データから原データを完全に復元することはできない．これは，変換の課程で，原データの一部が欠落するためである．こうした非可逆性は，セキュリティ確保の観点では問題ないのだが，秘匿化データの解析精度の観点で課題が残る．なぜなら，暗号化データの解析に性能劣化がないことを決定論的に保証することが困難であるためである．このため，解析精度の劣化が許されないアプリケーションに，上記の手法を適用することができない．

これに対して，ランダムユニタリ変換に基づく秘匿計算が提案されている[42]．この秘匿計算は，準同型暗号やマルチパーティプロトコルなどの秘密計算方式よりも遥かに少ない演算量でデータの秘匿化が可能となる．また，秘匿化によるデータ量の増加も発生しない．更に，変換前後の可逆性が保証されており，変換データから原データを完全に復元可能である．このため，プライバシー保護を必要とするビッグデータ解析のように，大量のデータの秘匿化とともに高速かつ高精度な解析を指向する応用において，期待されている．そこで，スパース信号表現[43]，[44]，画像圧縮[45]，[46]などの広く普及した信号処理アルゴリズムを秘匿化領域で精度低下なしに実現するための信号処理アルゴリズムが提案されている．上記の特徴に加えて，ランダムユニタリ変換は，秘匿鍵を変更して再秘匿化する際，原データを必要としない．因みに，ランダム射影は再秘匿化のたびに原データを必要とする．これは，変換の可逆性により，ランダムユニタリ変換による秘匿データに対して，異なるランダムユニタリ変換を適用することで秘匿鍵の異なる複数の秘匿データを生成できるためである．

3. ランダムユニタリ変換を用いた秘匿演算

ランダムユニタリ変換を用いた秘匿演算について，定義とその特長について述べる．

3.1 定　　義

ランダムユニタリ変換に基づく秘匿演算では，鍵 p によって生成されるランダムユニタリ行列 $\boldsymbol{Q}_p \in \mathbb{R}^{M\times M}$ (注1) を用いた変換により，観測信号 $\boldsymbol{y}_i \in \mathbb{R}^M$（$i$ はサンプル番号）を秘匿観測信号 $\hat{\boldsymbol{y}}_i \in \mathbb{R}^M$ へ変換する．

$$\hat{\boldsymbol{y}}_i = \boldsymbol{Q}_p \boldsymbol{y}_i \tag{1}$$

(注1)：本来，ランダムユニタリ行列は複素数を要素とする行列 $\boldsymbol{Q}_p \in \mathbb{C}^{M\times M}$ として定義される．ここでは実数を要素とする $\boldsymbol{Q}_p \in \mathbb{R}^{M\times M}$ について考える．

ただし，

$$\boldsymbol{Q}_p^* \boldsymbol{Q}_p = \boldsymbol{I} \tag{2}$$

を満たす．ここで $[\cdot]^*$ はエルミート転置，$\boldsymbol{I}$ は単位行列を表す．

ランダムユニタリ行列 $\boldsymbol{Q}_p$ の生成は，グラムシュミットの直交化を用いる方法や，複数のユニタリ行列を組み合わせることで $\boldsymbol{Q}_p$ を生成する方法が検証されている[47]．グラムシュミットの直交化法を用いた保護法では，疑似乱数行列にグラムシュミットの直交化方法を用いて生成された直交行列 $\boldsymbol{H}_p$ を用いて観測信号を秘匿する．すなわち

$$\boldsymbol{Q}_p = \boldsymbol{H}_p \tag{3}$$

とおく．また，複数のユニタリ行列を組み合わせたランダムユニタリ行列 $\boldsymbol{Q}_p$ を生成する方法の一例を以下に示す．

$$\boldsymbol{Q}_p = \boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_q \tag{4}$$

ただし，$\boldsymbol{A}$は離散フーリエ変換やアダマール変換などのランダム性を有しないユニタリ変換の行列である．$\boldsymbol{L}_q$ は鍵 q の疑似乱数生成器によって生成されたランダム性をもつユニタリ行列であり，ベクトルの要素を順番ランダムに入れ替える random permutation matrix や位相をランダムに変更する random phase matrix などがある[47]．ここで $\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_q$ は次式を満たす．

$$(\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_q)^* (\boldsymbol{H}_p \boldsymbol{A} \boldsymbol{L}_q) = \boldsymbol{I} \tag{5}$$

このように複数のユニタリ行列を組み合わせることで，秘匿行列の更新が容易に実行できる．同じランダムユニタリ行列を使い続けることによるセキュリティリスクを軽減するができる．またこの性質を利用すると，再秘匿化する際に原データを必要としない．

3.2 特　　徴

ランダムユニタリ行列に基づき変換された信号は，一般的に以下の特徴をもつ．

特徴 1：ノルム不変

$$||\boldsymbol{y}_i||_2^2 = ||\hat{\boldsymbol{y}}_i||_2^2 \tag{6}$$

特徴 2：ユークリッド距離の保存

$$\left|\left|\boldsymbol{y}_i - \boldsymbol{y}_j\right|\right|_2^2 = \left|\left|\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{y}}_j\right|\right|_2^2 \tag{7}$$

特徴 3：内積の保存

$$\boldsymbol{y}_i{}^* \boldsymbol{y}_j = \hat{\boldsymbol{y}}_i{}^* \hat{\boldsymbol{y}}_j \tag{8}$$

これらの性質により，スパースモデリングの係数選択・推定や学習アルゴリズムが秘匿領域でも性能の劣化なく利用できる．

4. スパースモデリングの秘匿演算

本節では，まず，スパースモデリングの定式化を行い，代表的なスパースモデリングの求解アルゴリズムについて説明するとともに，そうした求解アルゴリズムを秘匿化領域において適用する方法を説明する．次に，スパースモデリングに適した辞書の設計であるスパース辞書学習について，代表的な手法を概説した後，スパース辞書学習アルゴリズムを秘匿化領域において適用する方法を説明する．

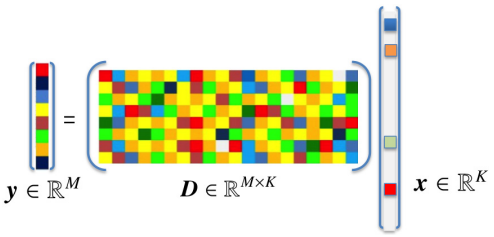


図 1　スパースモデリング：少数の基底ベクトルの重み付き線形和で表現する線形システム

4.1 スパースモデリングの定式化

スパースモデリングは，観測信号を少数の基底の重み付き線形和で表現する．基底の数 K は観測信号の次元 M よりも大きく過完備基底 $(K > M)$ であるため，非常に多くの表現パターンがある．その解法のため，盛んに研究が行われてきた．本分野は比較的若く，最初の重要な発表は Mallat と Zhang らにより 1993 年に発表されたマッチング追跡法（Matching Pursuit: MP）[19]であり，それ以後の貪欲法へとつながる．第二の発表は Chen と Donoho，Saunders により 1995 年に発表された基底追跡法（Basis Pursuit: BP）[21]である．これは l_1 ノルムによりスパース性を評価することで，スパース解の導出を凸計画問題としてとらえたものである．これら二つの発表を皮切りに，より深いアルゴリズム解析や具体的な応用例へ適用検討が進められた．

図 1 に示すように，M 次元の観測信号 $\boldsymbol{y} \in \mathbb{R}^M$ が，K 個の基底の線形結合で表せると仮定する(注2)

$$\boldsymbol{y} = \boldsymbol{D}\boldsymbol{x} \tag{9}$$

ただし，$\boldsymbol{D} = \{\boldsymbol{d}_1, ..., \boldsymbol{d}_K\} \in \mathbb{R}^{M \times K}$ は基底 $\boldsymbol{d}_k$（列ベクトル）を要素とする辞書行列であり，$\boldsymbol{x} = \{x_1, ..., x_K\} \in \mathbb{R}^K$ はスパース係数である．スパース係数は少数の k 個の係数のみが非ゼロの値を取り，残りの大部分の係数はゼロの値を取る．このように，非ゼロ要素が全体に対して少数である状態をスパース（Sparse：疎）と呼ぶ．辞書行列 $\boldsymbol{D}$ は事前に与えられるか，または観測データに基づき学習により適応的に推定される．

一般的に $K > M$（基底の数が，観測信号の次元よりも大きい）であり，過完備な辞書行列を用いる．信号の次元より多い基底による表現 $\boldsymbol{y} = \boldsymbol{D}\boldsymbol{x}$ では $\boldsymbol{x}$ の一意性を保証することができないため，通常は観測信号 $\boldsymbol{y}$ の表現に利用される基底を $\boldsymbol{D}$ の

(注2)：4.1 節および 4.2 節においては，表記の簡略化の観点から観測信号のインデックスは省略し，$\boldsymbol{y}_i$ を $\boldsymbol{y}$ と略記する．同様に，$\boldsymbol{y}_i$ に対する係数ベクトル $\boldsymbol{x}_i$ も $\boldsymbol{x}$ と略記する．

うちの一部に制限する．つまり，$||\boldsymbol{x}||_0$ で $\boldsymbol{x}$ の l_0 ノルム，すなわちベクトル $\boldsymbol{x}$ の非ゼロ成分の数を表すとして，スパースモデリングは典型的には最適化問題

$$\boldsymbol{x} = \arg\min_{\boldsymbol{x}} ||\boldsymbol{y} - \boldsymbol{D}\boldsymbol{x}||_2^2 \quad \text{subject to} \quad ||\boldsymbol{x}||_0 < \epsilon \quad (10)$$

として定式化される．つまり，再構成誤差を一定のしきい値以下に抑えた上でできるだけ少ない数の基底の線形結合で信号を近似する問題として考えている．しかしながら，上記問題は全ての基底の組み合わせを試さないと最適解が得られない組合せ最適化問題であり，NP 困難であることが知られている[48]．この問題に対する解法として，貪欲法に基づく方法や l_0 制約を l_1 制約で緩和した上で解く方法など，数多くのアルゴリズムが提案されている．

4.2 スパースモデリングの求解アルゴリズム

本小節ではスパースモデリングの近似解法として l_0 制約に対する貪欲法に基づく直交マッチング追跡法 (Orthogonal Matching Pursuit: OMP)[20]，および l_1 制約への緩和に基づく Least Absolute Shrinkage and Selection Operator (LASSO)[22] を紹介する．

4.2.1 直交マッチング追跡法（OMP）

(1) OMP アルゴリズム

直交マッチング追跡法は l_0 制約に基づく近似解法であり，観測信号の近似に利用する係数の添字集合の中から「サポート」，すなわち非ゼロ係数の添字集合 S を見つけ出すアルゴリズムである．初めはサポートは空集合であるとして，観測信号 $\boldsymbol{y}$ を基底の線形結合で近似したときの残差を最小にするように新たな基底をサポート集合に一つ一つ追加していき，サポートに含まれる基底のみで信号を近似したときの残差が ϵ 以下になったら停止する．残差の低減に寄与する基底を順次選択していく貪欲法であり，解の最適性は保証されないが，多くの場合優れた近似を与えることが知られている．以下に，直交マッチング追跡法のアルゴリズムを示す．

直交マッチング追跡法（OMP）アルゴリズム

---

1) 初期化：$k = 0$

初期解 $\boldsymbol{x}^0 = \boldsymbol{0}$

初期残差 $\boldsymbol{r}^0 = \boldsymbol{y} - \boldsymbol{D}\boldsymbol{x}^0 = \boldsymbol{y}$

解の初期サポート $S^0 = \emptyset$

2) メインループ

$k \to k+1$ とし，以下のステップを実行する．

1. 近似誤差：

$$\epsilon(i) = \min_{x_i} ||x_i \boldsymbol{d}_{\boldsymbol{i}} - \boldsymbol{r}^{k-1}||_2^2 = ||\boldsymbol{r}^{k-1}||_2^2 - \frac{(\boldsymbol{d}_i \cdot \boldsymbol{r}^{k-1})^2}{||\boldsymbol{d}_i||_2^2} \quad (11)$$

2. サポートの更新：

$$i_0 = \arg\min_{i \notin S^{k-1}} \{\epsilon(i)\}, \quad S^k = S^{k-1} \cup \{i_0\} \quad (12)$$

3. サポート内での最良解の探索：

$$\bar{\boldsymbol{x}}^k = \arg\min_{\boldsymbol{x}_{S^k}} ||\boldsymbol{y} - \boldsymbol{D}_{S^k}\boldsymbol{x}_{S^k}||_2^2 = (\boldsymbol{D}_{S^k}^* \boldsymbol{D}_{S^k})^{-1}(\boldsymbol{D}_{S^k}^* \boldsymbol{y}) \quad (13)$$

4. 残差の更新：

$$\boldsymbol{r}^k = \boldsymbol{y} - \boldsymbol{D}_{S^k}\bar{\boldsymbol{x}}^k \quad (14)$$

5. 停止条件：

$||\boldsymbol{r}^k||_2 < \epsilon$

---

(2) OMP の秘匿演算

図 2 に，エッジ/クラウドでスパース係数の秘匿演算を行うアーキテクチャを示す．ここで $\hat{\boldsymbol{D}}$ は秘匿辞書行列であり，事前に準備する．秘匿辞書行列の生成法には，以下に示す 2 種類の方法がある．

1) ローカルにおいて，辞書行列 $\boldsymbol{D}$ を K-SVD[43](注3) などを用い学習して生成する．その後，ランダムユニタリ変換を用いて辞書行列 $\boldsymbol{D}$ を秘匿辞書行列 $\hat{\boldsymbol{D}}$ へ変換し，エッジ/クラウドへ伝送する．

2) 4.3 節に示すスパース秘匿辞書学習により，エッジ/クラウドにおいて秘匿辞書行列 $\hat{\boldsymbol{D}}$ を観測信号を秘匿したまま学習して生成する．

図 2 において，スパースモデリングの秘匿演算の実行では秘匿辞書行列 $\hat{\boldsymbol{D}}$ と秘匿観測信号 $\hat{\boldsymbol{y}}$ を用いて OMP アルゴリズムを実行してスパース係数を推定する．

スパースモデリングの秘匿演算では，次式のように秘匿観測信号 $\hat{\boldsymbol{y}}$ 並びに秘匿辞書行列 $\hat{\boldsymbol{D}}$（ローカルで秘匿辞書行列を生成する場合）を生成する．

$$\hat{\boldsymbol{y}} = \boldsymbol{Q}_p \boldsymbol{y} \quad (15)$$

$$\hat{\boldsymbol{D}} = \boldsymbol{Q}_p \boldsymbol{D} \quad (16)$$

このとき次式に示す $\hat{\boldsymbol{y}}$ と $\hat{\boldsymbol{D}}$ が与えられたときの最適化問題を考える．

$$\hat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} \| \hat{\boldsymbol{y}} - \hat{\boldsymbol{D}}\boldsymbol{x} \|_2^2 \quad \text{subject to} \quad ||\boldsymbol{x}||_0 < \epsilon \quad (17)$$

以下に，$\hat{\boldsymbol{y}}$ と $\hat{\boldsymbol{D}}$ が与えられたときに，式 (17) を解くための直交マッチング追跡法（OMP）アルゴリズムを示す．

秘匿領域での OMP アルゴリズム

---

1) 初期化：$k = 0$

初期解 $\hat{\boldsymbol{x}}^0 = \boldsymbol{0}$

(注3)：K-SVD については，4.3.1 節にて後述．名称における K は K-means 法の一般化した手法であることに由来しており，SVD は特異値分解 (Singular Value Decomposition) の略である．

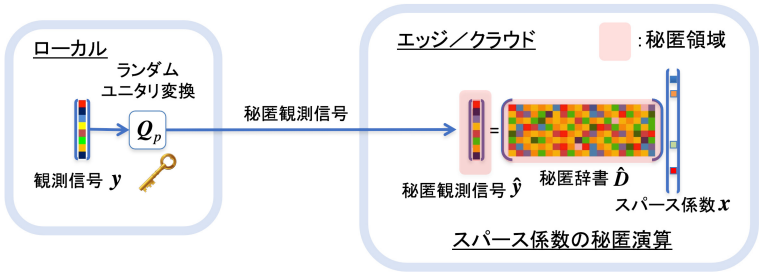


図 2　実行：エッジ/クラウドでのスパース係数の秘匿演算

初期残差 $\hat{\boldsymbol{r}}^0 = \hat{\boldsymbol{y}} - \hat{\boldsymbol{D}}\hat{\boldsymbol{x}}^0 = \hat{\boldsymbol{y}}$

解の初期サポート $S^0 = \emptyset$

2)　メインループ

$k \to k+1$ とし，以下のステップを実行する．

1. 近似誤差：

$$\hat{\epsilon}(j) = \min_{\hat{x}_j} ||\hat{x}_j \hat{\boldsymbol{d}}_{\boldsymbol{j}} - \hat{\boldsymbol{r}}^{k-1}||_2^2 = ||\hat{\boldsymbol{r}}^{k-1}||_2^2 - \frac{(\hat{\boldsymbol{d}}_j \cdot \hat{\boldsymbol{r}}^{k-1})^2}{||\hat{\boldsymbol{d}}_j||_2^2} \quad (18)$$

2. サポートの更新：

$$j_0 = \arg\min_{j \notin S^{k-1}} \{\hat{\epsilon}(j)\}, S^k = S^{k-1} \cup \{j_0\} \quad (19)$$

3. サポート内での最良解の探索：

$$\hat{\boldsymbol{x}}^k = \arg\min_{\hat{\boldsymbol{x}}_{S^k}} ||\hat{\boldsymbol{y}} - \hat{\boldsymbol{D}}_{S^k}\hat{\boldsymbol{x}}_{S^k}||_2^2 = (\hat{\boldsymbol{D}}_{S^k}^* \hat{\boldsymbol{D}}_{S^k})^{-1}(\hat{\boldsymbol{D}}_{S^k}^* \hat{\boldsymbol{y}}) \quad (20)$$

4. 残差の更新：

$$\hat{\boldsymbol{r}}^k = \hat{\boldsymbol{y}} - \hat{\boldsymbol{D}}_{S^k}\bar{\boldsymbol{x}}^k \quad (21)$$

5. 停止条件：

$$||\hat{\boldsymbol{r}}^k||_2 < \epsilon \quad (22)$$

ランダムユニタリ変換がもつ式 (2) に示す直交性から導かれる内積の保存の特徴を用いると，サポート内での最良解に関して次の関係が導かれる．

$$\begin{aligned}\hat{\boldsymbol{x}}^k &= (\hat{\boldsymbol{D}}_{S^k}^* \hat{\boldsymbol{D}}_{S^k})^{-1}(\hat{\boldsymbol{D}}_{S^k}^* \hat{\boldsymbol{y}}) \\ &= (\boldsymbol{D}_{S^k}^* \boldsymbol{D}_{S^k})^{-1}(\boldsymbol{D}_{S^k}^* \boldsymbol{y}) \\ &= \bar{\boldsymbol{x}}^k \end{aligned} \quad (23)$$

すなわち，秘匿しない場合と秘匿した場合で同じスパース係数が推定されることが分かる．最後に，$\left|\left|\hat{\boldsymbol{r}}^k\right|\right|_2 < \epsilon$ を満たすとき終了となるが，ノルム不変の性質より，

$$\left|\left|\hat{\boldsymbol{r}}^k\right|\right|_2 = \left|\left|\boldsymbol{r}^{\boldsymbol{k}}\right|\right|_2 \quad (24)$$

が成立する．観測信号を秘匿しない場合の停止条件と一致する．

4.2.2　LASSO

LASSO と呼ばれる定式化では，l_1 ノルムへの緩和問題の最小解として係数ベクトルを求解する．

$$\min_{\boldsymbol{x}} ||\boldsymbol{y} - \boldsymbol{D}\boldsymbol{x}||_2^2 + \lambda||\boldsymbol{x}||_1, \quad \lambda > 0 \quad (25)$$

この l_1 ノルム正則化問題は線形計画問題として表現することが可能である．また，y が高次元の場合の解法として，coordinate descent algorithm [49] が提案されている．

ランダムユニタリ変換により秘匿化された信号から LASSO 解を求める場合，この求解は，秘匿化された信号に対して以下のコストを最小化することで実現できる．

$$\frac{1}{2}||\hat{\boldsymbol{y}} - \hat{\boldsymbol{X}}\boldsymbol{w}||_2^2 + \lambda||\boldsymbol{w}||_1 \quad (26)$$

実は，ランダムユニタリ変換の列ベクトルが互いに直交するという性質を考慮すると，次の関係が導かれる [50]．

$$\arg\min_{\boldsymbol{w}} \hat{L}(\boldsymbol{w}) = \arg\min_{\boldsymbol{w}} L(\boldsymbol{w})$$

上式は，秘匿化された信号に対して求めた LASSO 解は，秘匿化前の信号に対する解と一致することを示している．また，そうした LASSO 解が，coordinate descent algorithm に基づく解法により得られることも証明されている [50]．

4.3　スパース辞書学習

辞書行列はウェーブレット変換や離散コサイン変換など既存のフィルタを用いる方法と，観測信号から学習により適応的に推定される．本小節では，観測信号から学習する辞書学習として教師なしスパース辞書学習の K-SVD と，教師ありスパース辞書学習の Label Consistent KSVD (LC-KSVD) を紹介する．

4.3.1　教師なしスパース辞書学習 (K-SVD)

(1)　K-SVD アルゴリズム

本節ではスパース辞書学習の定式化を行うとともに，代表的なアルゴリズムである K-SVD [43] について説明する．K-SVD は，k-means 法を一般化した手法と位置づけられる．k-means 法では各サンプルをクラスタに割り当てるステップと，クラスタの重心を移動させるステップが交互に繰り返される．クラスタ重心は特徴量の空間におけるベクトルであり，そのクラスタに割り当てられたサンプルの平均的な特徴と捉えられる k-means 法の拡張である．soft k-means 法では各サンプルを多数のクラスタに割り当てる．これはクラスタ重心の一次結合としてサンプルが表されることを意味し，クラスタ重心を基底に置き換えることで，辞書学習と対応する．

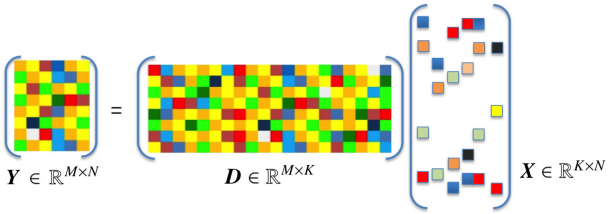


図 3　スパース辞書学習

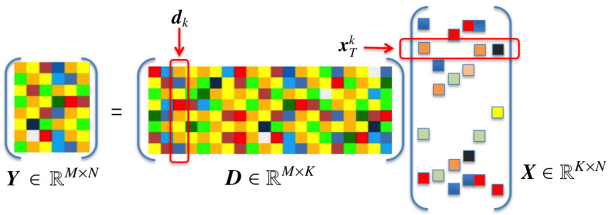


図 4　基底 $\boldsymbol{d}_k$ と $\boldsymbol{X}$ の k 番めの行ベクトル $\boldsymbol{x}_T^k$

a)　スパース辞書学習の定式化

観測信号 $\boldsymbol{y}_i$（M 次元の列ベクトル）の集合を $\boldsymbol{Y} = \{\boldsymbol{y}_i\}_{i=1}^N$ とする．このとき，図 3 に示すように，$\boldsymbol{Y}$ が K 個の基底の線形結合で表せると仮定する．

$$\boldsymbol{Y} = \boldsymbol{D}\boldsymbol{X} \tag{27}$$

ただし，$\boldsymbol{D} = \{\boldsymbol{d}_1, ..., \boldsymbol{d}_K\} \in \mathbb{R}^{M\times K}$ は基底 $\boldsymbol{d}_k$（M 次元の列ベクトル）を要素とする辞書と呼ばれる行列であり，$\boldsymbol{X} = \{\boldsymbol{x}_i\}_{i=1}^N$ はスパース係数 $\boldsymbol{x}_i$（K 次元の列ベクトル）を要素とする行列である．

一般的に $K > M$（基底の数が，観測信号の次元よりも大きい）であり，過完備な辞書を用いる．信号の次元より多い基底による表現 $\boldsymbol{Y} = \boldsymbol{D}\boldsymbol{X}$ では $\boldsymbol{X}$ の一意性を保証することができないため，通常は $\boldsymbol{Y}$ の表現に利用される基底を $\boldsymbol{D}$ のうちの一部に制限する．すなわち，少数の T_0 個の係数のみが非ゼロの値を取り，残りの大部分の係数はゼロの値を取る制約を設ける．このように，スパースの制約をもつ最適化問題は，

$$\min_{\boldsymbol{D},\boldsymbol{X}} ||\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}||_F^2 \quad \text{subject to } \forall i,\ ||\boldsymbol{x}_i||_0 < T_0 \tag{28}$$

として定式化される．ただし，$||\cdot||_0$ は l_0 ノルム（ベクトル中の非ゼロ要素の個数）を表し，$||\cdot||_F$ はフロベニウスのノルムを表し $||\boldsymbol{A}||_F = \sqrt{\sum_{ij} A_{ij}^2}$ で定義される．

一般的に辞書学習は，二つのステップを交互に繰り返すことによって，式 (28) の最適化問題を解く．ステップ 1 はスパース係数の計算，ステップ 2 では辞書の更新を行う．

b)　ステップ 1：スパース係数の計算

ステップ 1 では辞書 $\boldsymbol{D}$ を固定し，式 (28) の最適化問題を解く．各入力の観測信号 $\boldsymbol{y}_i$ に対して，スパース係数 $\boldsymbol{x}_i$ を求める問題であり，次式のように書き換えることができる．

$$\boldsymbol{x}_i = \arg\min_{\boldsymbol{x}_i} ||\boldsymbol{y}_i - \boldsymbol{D}\boldsymbol{x}_i||_F^2 \quad \text{subject to} \quad ||\boldsymbol{x}_i||_0 < T_0$$
$$i = 1, 2, \cdots, N \tag{29}$$

上記の求解には，4. 2. 1 節で示した直交マッチング追跡法 (OMP) を用いる．

c)　ステップ 2：辞書の更新

ステップ 2 ではステップ 1 で求めた $\boldsymbol{X}$ を固定し，辞書 $\boldsymbol{D}$ の更新を行う．K-SVD では一つの基底 $\boldsymbol{d}_k$ に着目し順次更新する．

$$||\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}||_F^2 = \left|\left|\boldsymbol{Y} - \sum_{j=1}^{K} \boldsymbol{d}_j \boldsymbol{x}_T^j\right|\right|_F^2$$
$$= \left|\left|\left(\boldsymbol{Y} - \sum_{j\neq k}^{K} \boldsymbol{d}_j \boldsymbol{x}_T^j\right) - \boldsymbol{d}_k \boldsymbol{x}_T^k\right|\right|_F^2$$
$$= \left|\left|\boldsymbol{E}_k - \boldsymbol{d}_k \boldsymbol{x}_T^k\right|\right|_F^2 \tag{30}$$

ここで $\boldsymbol{E}_k$ は観測信号の集合 $\boldsymbol{Y}$ から基底 $\boldsymbol{d}_k$ を除いた線形予測値との残差を示す．

$$\boldsymbol{E}_k = \boldsymbol{Y} - \sum_{j\neq k}^{K} \boldsymbol{d}_j \boldsymbol{x}_T^j \tag{31}$$

K-SVD では $\boldsymbol{E}_k$ を特異値分解することで，$\boldsymbol{d}_k$ と $\boldsymbol{x}_T^k$ を求める．しかしながら，得られる解はスパースの制約を満たすとは限らないため，K-SVD ではステップ 1 で求めた $\boldsymbol{x}_T^k$ における非ゼロ要素のみを更新する．これによって，ステップ 1 で得られたスパース性を維持することができる．$\boldsymbol{x}_T^k$ における非ゼロ要素のインデックス集合 ω_k を以下のように定義する．

$$\omega_k = \{i \mid 1 \leqq i \leqq K,\ \boldsymbol{x}_T^k(i) \neq 0\} \tag{32}$$

ただし，$\boldsymbol{x}_T^k(i)$ は $\boldsymbol{x}_T^k$ の i 番めの要素を表す．ここで $(\omega_k(i), i)$ の位置の要素のみが 1 である大きさ $N \times |\omega_k|$ の行列 $\boldsymbol{\Omega}_K$ を定義する．$\boldsymbol{\Omega}_K$ を用いると $\boldsymbol{x}_T^k$ の非ゼロ要素のみで構成されるベクトル $\boldsymbol{x}_R^k$ が，次式のように書き表せる．

$$\boldsymbol{x}_R^k = \boldsymbol{x}_T^k \boldsymbol{\Omega}_K \tag{33}$$

同様に $\boldsymbol{E}_k$ に対して，$\boldsymbol{\Omega}_K$ を用いて $\boldsymbol{E}_k^R = \boldsymbol{E}_k \boldsymbol{\Omega}_K$ と変換する．

$$\left|\left|\boldsymbol{E}_k \boldsymbol{\Omega}_K - \boldsymbol{d}_k \boldsymbol{x}_T^k \boldsymbol{\Omega}_K\right|\right|_F^2 = \left|\left|\boldsymbol{E}_k^R - \boldsymbol{d}_k \boldsymbol{x}_R^k\right|\right|_F^2 \tag{34}$$

$\boldsymbol{E}_k^R$ に対して特異値分解を適用し，直交行列 $\boldsymbol{U}$, $\boldsymbol{V}$ と対角行列 $\boldsymbol{\Sigma}$ に分解すると次式が得られる．

$$\boldsymbol{E}_k^R = \boldsymbol{U}\boldsymbol{\Delta}\boldsymbol{V}^{\boldsymbol{T}}$$
$$= \boldsymbol{u}_1 \cdot \sigma_1 \boldsymbol{v}_1^T + \boldsymbol{u}_2 \cdot \sigma_2 \boldsymbol{v}_2^T + \cdots + \boldsymbol{u}_n \cdot \sigma_n \boldsymbol{v}_n^T \tag{35}$$

$\boldsymbol{u}_i$ と $\boldsymbol{v}_j$ は，それぞれ $\boldsymbol{U}$ と $\boldsymbol{V}$ の i 番めの列ベクトル，σ_i は Δ の i 番めの対角成分である．K-SVD では第一特異値に関する成分 $\boldsymbol{u}_1$ と $\sigma_1 \boldsymbol{v}_1^T$ を用いて，次式のように基底並びにスパース係数の行ベクトルの近似解を得る．

・基底：$\boldsymbol{d}_k = \boldsymbol{u}_1$ (36)

・スパース係数：$\boldsymbol{x}_R^k = \sigma_1 \boldsymbol{v}_1^T$ (37)

(2)　教師なしスパース辞書学習 (K-SVD) の秘匿演算

エッジ/クラウドでスパース辞書学習の秘匿演算を行うアーキテクチャを図 5 に示す．最初にローカルにおいて，鍵 p によ

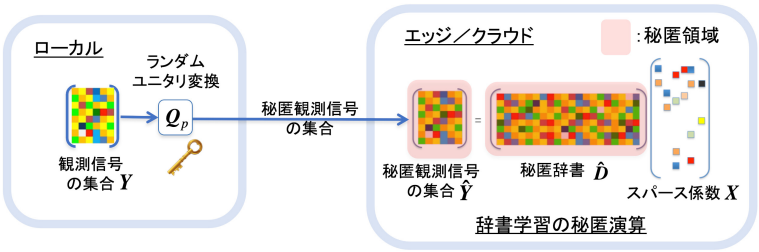


図 5　エッジ/クラウドでのスパース辞書学習の秘匿演算

り生成したランダムユニタリ行列 $\boldsymbol{Q_p}$ を用いて，観測信号の集合 $\boldsymbol{Y}$ を秘匿観測信号の集合 $\hat{\boldsymbol{Y}}$ へ変換する．その後，$\hat{\boldsymbol{Y}}$ をエッジ/クラウドへ転送する．エッジ/クラウドでは，$\hat{\boldsymbol{Y}}$ を入力として，K-SVD のアルゴリズムを実行して秘匿辞書 $\hat{\boldsymbol{D}}$ を推定する．エッジ/クラウドでは秘匿領域での辞書すなわち秘匿辞書 $\hat{\boldsymbol{D}}$ が随時更新される．鍵 p をもつユーザはランダムユニタリ逆変換 $\boldsymbol{Q}_p^*$ を秘匿辞書 $\hat{\boldsymbol{D}}$ へ掛け合わせることで，辞書 $\boldsymbol{D}$ を得ることができる．

スパース係数 $\boldsymbol{X}$ は，エッジ/クラウドにおいて K-SVD のステップ 1 の段階で随時更新され求められる．スパース係数 $\boldsymbol{X}$ をデータ解析することで観測信号のパターンや法則性を見つけることが可能となる．提案するスパース辞書学習の秘匿演算では，次式のように秘匿観測信号の集合 $\hat{\boldsymbol{Y}}$ を生成する．

$$\hat{\boldsymbol{Y}} = \boldsymbol{Q}_p \boldsymbol{Y} \tag{38}$$

このとき式 (28) に代わり $\hat{\boldsymbol{Y}}$ を用い，次式に示す最適化問題を考える．

$$\min_{\hat{\boldsymbol{D}},\boldsymbol{X}} \left|\left|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right|\right|_F^2 \quad \text{subject to } \forall i,\ \ ||\boldsymbol{x}_i||_0 < T_0 \tag{39}$$

ただし，$\hat{\boldsymbol{D}} = \{\hat{\boldsymbol{d}}_1, ..., \hat{\boldsymbol{d}}_K\} \in \mathbb{R}^{M\times K}$ は基底 $\hat{\boldsymbol{d}}_i$（M 次元の列ベクトル）を要素とする秘匿辞書の行列である．

d)　ステップ 1：スパース係数の計算

ステップ 1 では辞書 $\hat{\boldsymbol{D}}$ を固定し，式 (39) の最適化問題を解く．各入力の観測信号 $\hat{\boldsymbol{y}}_i$ に対して，スパース係数 $\boldsymbol{x}_i$ を求める問題であり，次式のように書き換えることができる．

$$\boldsymbol{x}_i = \arg\min_{\boldsymbol{x}_i} \left|\left|\hat{\boldsymbol{y}}_i - \hat{\boldsymbol{D}}\boldsymbol{x}_i\right|\right|_F^2 \quad \text{subject to} \quad ||\boldsymbol{x}_i||_0 < T_0$$
$$i = 1, 2, \cdots, N \tag{40}$$

4.2.1 節で示したように，辞書を $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{D}$ と秘匿した後に，上式を OMP で解いて得られる解 $\boldsymbol{x}_i$ は，観測 $\boldsymbol{y}_i$ と辞書行列 $\boldsymbol{D}$ を秘匿しない場合に OMP を解いて得られるスパース係数 $\boldsymbol{x}_i$ と等しくなる．

e)　ステップ 2：秘匿辞書の更新

ステップ 2 ではステップ 1 で求めた $\boldsymbol{X}$ を固定し，秘匿辞書 $\hat{\boldsymbol{D}}$ の更新を行う．秘匿 K-SVD では一つの基底 $\hat{\boldsymbol{d}}_k$ に着目し順次更新する．c) 節の観測信号を秘匿しない場合の K-SVD の辞書更新の手法を用いて，同様に求める．

$$\begin{aligned}\left|\left|\hat{\boldsymbol{Y}} - \hat{\boldsymbol{D}}\boldsymbol{X}\right|\right|_F^2 &= \left|\left|\hat{\boldsymbol{Y}} - \sum_{j=1}^{K}\hat{\boldsymbol{d}}_j\boldsymbol{x}_T^j\right|\right|_F^2 \\ &= \left|\left|\left(\hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K}\hat{\boldsymbol{d}}_j\boldsymbol{x}_T^j\right) - \hat{\boldsymbol{d}}_k\boldsymbol{x}_T^k\right|\right|_F^2 \\ &= \left|\left|\hat{\boldsymbol{E}}_k - \hat{\boldsymbol{d}}_k\boldsymbol{x}_T^k\right|\right|_F^2 \end{aligned} \tag{41}$$

ここで，$\hat{\boldsymbol{E}}_k$ は秘匿観測信号の集合 $\hat{\boldsymbol{Y}}$ から基底 $\hat{\boldsymbol{d}}_k$ を除いた線形予測値との残差を示す．

解のスパース性を維持するために，$\boldsymbol{x}_T^k$ の非ゼロ要素のみで構成されるベクトル $\boldsymbol{x}_R^k$ のみ更新する．$\hat{\boldsymbol{E}}_k$ に対して，$\boldsymbol{\Omega}_K$ を用いて $\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_K$ と変換する．

$$\left|\left|\hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_K - \hat{\boldsymbol{d}}_k\boldsymbol{x}_T^k\boldsymbol{\Omega}_K\right|\right|_F^2 = \left|\left|\hat{\boldsymbol{E}}_k^R - \hat{\boldsymbol{d}}_k\boldsymbol{x}_R^k\right|\right|_F^2 \tag{42}$$

$\hat{\boldsymbol{E}}_k^R$ に対して特異値分解を適用し，直交行列 $\hat{\boldsymbol{U}}$, $\hat{\boldsymbol{V}}$ と対角行列 $\hat{\boldsymbol{\Sigma}}$ に分解すると次式が得られる．

$$\begin{aligned}\hat{\boldsymbol{E}}_k^R &= \hat{\boldsymbol{U}}\hat{\boldsymbol{\Delta}}\hat{\boldsymbol{V}}^{\boldsymbol{T}} \\ &= \hat{\boldsymbol{u}}_1\cdot\hat{\sigma_1}\hat{\boldsymbol{v}}_1^T + \hat{\boldsymbol{u}}_2\cdot\hat{\sigma_2}\hat{\boldsymbol{v}}_2^T + \cdots + \hat{\boldsymbol{u}}_n\cdot\hat{\sigma_n}\hat{\boldsymbol{v}}_n^T \end{aligned} \tag{43}$$

第一特異値に関する成分 $\hat{\boldsymbol{u}}_1$ と $\hat{\sigma}_1\hat{\boldsymbol{v}}_1^T$ を用いて，次式のように基底並びにスパース係数の行ベクトルの近似解を得る．

$$\cdot\ \text{基底}: \hat{\boldsymbol{d}}_k = \hat{\boldsymbol{u}}_1 \tag{44}$$

$$\cdot\ \text{スパース係数}: \hat{\boldsymbol{x}}_R^k = \hat{\sigma}_1\hat{\boldsymbol{v}}_1^T \tag{45}$$

次に，観測信号を秘匿しない場合に解いて得られる解と，秘匿しない場合に得られる解との関係を示す．ここで式 (41) における $\hat{\boldsymbol{E}}_k$ の第 2 項 $\hat{\boldsymbol{d}}_j$ を $\hat{\boldsymbol{d}}_j = \boldsymbol{Q}_p\boldsymbol{d}_j$ と分解し，式 (38) の関係を用いて整理すると，

$$\begin{aligned}\hat{\boldsymbol{E}}_k &= \hat{\boldsymbol{Y}} - \sum_{j\neq k}^{K}\hat{\boldsymbol{d}}_j\boldsymbol{x}_T^j \\ &= \boldsymbol{Q}_p\left(\boldsymbol{Y} - \sum_{j\neq k}^{K}\boldsymbol{d}_j\boldsymbol{x}_T^j\right) = \boldsymbol{Q}_p\boldsymbol{E}_k \end{aligned} \tag{46}$$

が得られる．なお $\hat{\boldsymbol{d}}_j = \boldsymbol{Q}_p\boldsymbol{d}_j$ の分解は，ステップ 1 において秘匿信号に対するスパース係数を求める際の前提条件 $\hat{\boldsymbol{D}} = \boldsymbol{Q}_p\boldsymbol{D}$ [3],[51] から導出される．次に解のスパース性を維持するために，$\hat{\boldsymbol{E}}_k$ に対して $\boldsymbol{\Omega}_K$ を用いて $\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_K$ と変換して，式 (46) の関係を用いると，

$$\hat{\boldsymbol{E}}_k^R = \hat{\boldsymbol{E}}_k\boldsymbol{\Omega}_K = \boldsymbol{Q}_p\boldsymbol{E}_k\boldsymbol{\Omega}_K = \boldsymbol{Q}_p\boldsymbol{E}_k^R \tag{47}$$

と書き表すことができる．更に，式 (35) の関係式（観測信号を秘匿しない場合の $\boldsymbol{E}_k^R$ に対する特異値分解の結果）を用いると，式 (47) は次のように分解できる．

$$\begin{aligned}\hat{\boldsymbol{E}}_k^R &= \boldsymbol{Q}_p \boldsymbol{E}_k^R \\ &= \boldsymbol{Q}_p \boldsymbol{u}_1 \cdot \sigma_1 \boldsymbol{v}_1^T + \boldsymbol{Q}_p \boldsymbol{u}_2 \cdot \sigma_2 \boldsymbol{v}_2^T + \cdots + \boldsymbol{Q}_p \boldsymbol{u}_n \cdot \sigma_n \boldsymbol{v}_n^T\end{aligned} \tag{48}$$

式 (48) より基底並びにスパース係数は，観測信号を秘匿しない場合の値を用いて $\hat{\boldsymbol{d}}_k = \hat{\boldsymbol{u}}_1 = \boldsymbol{Q}_p \boldsymbol{u}_1$ 並びに $\hat{\boldsymbol{x}}_R^k = \sigma_1 \boldsymbol{v}_1^T$ と表現できることが分かる．

・スパース係数：$\hat{\boldsymbol{x}}_R^k = \sigma_1 \boldsymbol{v}_1^T$ (49)

・基底：$\hat{\boldsymbol{d}}_k = \boldsymbol{Q}_p \boldsymbol{u}_1$ (50)

式 (49) (50) の関係式は以下のように示せる．

[スパース係数の関係式]

式 (43) より $\hat{\boldsymbol{v}}_i$ は $\left(\hat{\boldsymbol{E}}_k^R\right)^T \hat{\boldsymbol{E}}_k^R$ の i 番めの固有ベクトルであり，次式のように書き表すことができる．

$$\left(\hat{\boldsymbol{E}}_k^R\right)^T \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_i = \hat{\lambda}_i \hat{\boldsymbol{v}}_i \tag{51}$$

ただし，$\hat{\lambda}_i$ は i 番めの固有値であり，特異値 $\hat{\sigma}_i$ と $\hat{\sigma}_i = \sqrt{\hat{\lambda}_i}$ の関係にある．ここで $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p \boldsymbol{E}_k^R$ の関係を用いると式 (51) の左辺は

$$\left(\hat{\boldsymbol{E}}_k^R\right)^T \hat{\boldsymbol{E}}_k^R = \left(\boldsymbol{E}_k^R\right)^T \boldsymbol{Q}_p^T \boldsymbol{Q}_p \boldsymbol{E}_k^R = \left(\boldsymbol{E}_k^R\right)^T \boldsymbol{E}_k^R \tag{52}$$

と表すことができる．式 (52) より，$\left(\hat{\boldsymbol{E}}_k^R\right)^T \hat{\boldsymbol{E}}_k^R$ と $\left(\boldsymbol{E}_k^R\right)^T \boldsymbol{E}_k^R$ は等しいことから，それぞれの固有ベクトル $\hat{\boldsymbol{v}}_i$ 並びに $\boldsymbol{v}_i$ も等しい．

$$\hat{\boldsymbol{v}}_i = \boldsymbol{v}_i \tag{53}$$

したがって対応する固有値並びに特異値も等しく，式 (49) の関係が成立することが分かる．

[基底の関係式]

式 (43) に示す行列 $\hat{\boldsymbol{E}}_k^R$ の特異値分解において，左側の固有ベクトル $\hat{\boldsymbol{u}}_i$ と右側の固有ベクトル $\hat{\boldsymbol{v}}_i$ には $\hat{\boldsymbol{u}}_i = \pm \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_i / \sqrt{\hat{\lambda}_i}$（一般的な特異値分解の性質より）の関係がある．この関係と $\hat{\boldsymbol{E}}_k^R = \boldsymbol{Q}_p \boldsymbol{E}_k^R$ 並びに式 (53) の関係より，式 (43) の第 1 番めの項は，

$$\hat{\boldsymbol{u}}_1 \cdot \hat{\sigma_1} \hat{\boldsymbol{v}}_1^T = \frac{\pm \hat{\boldsymbol{E}}_k^R \hat{\boldsymbol{v}}_1 \cdot \hat{\sigma_1} \hat{\boldsymbol{v}}_1^T}{\sqrt{\hat{\lambda_1}}} = \pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \boldsymbol{v}_1^T \tag{54}$$

と表せる．同様に式 (48) の第 1 番めの項は，

$$\boldsymbol{Q}_p \boldsymbol{u}_1 \cdot \sigma_i \boldsymbol{v}_1^T = \frac{\pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \cdot \sigma_1 \boldsymbol{v}_1^T}{\sqrt{\lambda_1}} = \pm \boldsymbol{Q}_p \boldsymbol{E}_k^R \boldsymbol{v}_1 \boldsymbol{v}_1^T \tag{55}$$

と表せる．したがって式 (50) の関係が成立することが分かる．

4.3.2 教師ありスパース辞書学習 (LC-KSVD)

LC-KSVD [27] は，識別タスクを志向したスパース表現のための辞書学習アルゴリズムである．前述の K-SVD は，再構成誤差の低減に適したスパース表現を目的としたのに対して，LC-KSVD は，クラス識別に必要となる局所特徴に適したスパース表現を目的としている．なお，LC-KSVD では，辞書内の基底は，各々，担当するクラスにひも付けられ，担当するクラスに属する観測信号を表現するという制約を Label consistency と呼ぶ．Label consistency の制約を正則化に取り入れた形で，LC-KSVD の辞書学習は，以下の最小化問題として定式化される．

$$\begin{aligned}&\min_{\boldsymbol{D},\boldsymbol{X},\boldsymbol{W}} ||\boldsymbol{Y} - \boldsymbol{D}\boldsymbol{X}||_F^2 + \alpha||\boldsymbol{C} - \boldsymbol{A}\boldsymbol{X}||_F^2 + \beta||\boldsymbol{H} - \boldsymbol{W}\boldsymbol{X}||_F^2 \\ &\text{subject to} \quad \forall i \quad ||\boldsymbol{x}_i||_0 \leqq T_0\end{aligned} \tag{56}$$

ここで，第一項は，再構成誤差を評価する項であり，K-SVD と共通である．第二項は，Label consistency 制約を評価する項である．$\boldsymbol{C} \in \mathbb{R}^{K \times N}$ が辞書内の各基底が識別クラスの対応関係を示す行列であり，$\boldsymbol{A} \in \mathbb{R}^{K \times K}$ は，より識別能力の高い空間へ写像するための線形変換を表す．第三項は，クラス分類誤差を評価する項である．$\boldsymbol{W} \in \mathbb{R}^{L \times k}$ はクラス分類器のパラメータであり，$\boldsymbol{H} \in \mathbb{R}^{L \times N}$ は入力信号 $\boldsymbol{Y}$ のクラスラベルを表す．

なお，式 (56) の各項は，いずれも線形演算で表記されるため，式変更を行えば，式 (28) と同じ形で表現できる．このため，式 (56) の求解には，K-SVD の求解アルゴリズムを利用可能である．

そこで，K-SVD の求解アルゴリズムを利用可能である点に着目し，4.3.1 節の方式を利用し，ランダムユニタリ変換による秘匿信号に対して，LC-KSVD に基づく辞書学習が提案されている [5], [52]．

5. ランダムユニタリ変換のセキュリティ強度

ランダムユニタリ変換の安全性について，鍵空間の大きさとピアソンの積率相関係数により評価し，秘匿性の強化手法について説明する．

5.1 鍵空間と積率相関係数による評価

安全性の評価を $\boldsymbol{Q}_p \in \mathbb{R}^{M \times M}$ がどの程度の非可逆性を有しているかについて，鍵空間の大きさとオリジナルの入力と復号値とのピアソンの積率相関係数によって評価する．

(1) 鍵空間の大きさ

総当たり攻撃で復元する場合を想定し，$\boldsymbol{Q}_p \in \mathbb{R}^{M \times M}$ の鍵空間を求める．ランダムユニタリ変換を式 (3) に示すグラムシュミットの直交化で生成した場合を考える．ユニタリ変換の要素は実数に制限されている（直交行列）．制限がない状態での自由度は行列の要素数に等しく，M^2 個となる．しかしユニタリ行列には，以下の二つの条件が課せられている．

(a) ユニタリ行列の列ベクトルが互いに直交：条件式の数は，M 本の列ベクトルから 2 本を選ぶ組合せ数であり ${}_M\mathrm{C}_2$ 個

(b) 各列ベクトルのノルムが 1：条件式の数は M 個

表 1　糖尿病の検査データの入力 $\boldsymbol{X}$ $(M = 10)$ に対するピアソンの積率相関係数（PPMC）の絶対値の平均値、最大値、最小値

	Average	Maximum	Minimum
PPMC	0.122	0.526	8.51×10^{-6}

以上の (a) (b) より，ランダムユニタリ変換 $\boldsymbol{G}_p$ について，

$$\begin{aligned}\cdot \text{自由度} &= M^2 - [M(M-1)/2 + M] \\ &= M(M-1)/2\end{aligned}$$

となる．各要素が 8 ビットの固定小数点で表現されているとすると，鍵空間の広さは次式で表される．

$$\cdot \boldsymbol{G}_p \text{の鍵空間の広さ} = 8^{M(M-1)/2} \tag{57}$$

鍵空間の広さは，次元数 M の大きさに依存する．AES などで用いられる鍵空間と比較すると，$M = 10$ のとき 128 ビットの場合よりも広く，256 ビットよりも狭い空間となる．なお，M が 14 以上の場合は，256 ビットの鍵空間よりも広くなる．

(2)　入力と復号値とのピアソンの積率相関係数

秘匿強度は，秘匿化時と異なるランダムユニタリ変換を用いて復号されたデータに対して，ピアソンの積率相関係数 (PPMC: Pearson product-moment correlation coefficient) に基づき評価した．相関係数はデータ間の類似度を表しており，PPMC が低ければ，正しく復号できなかったことを示す．一般的に，相関係数が 0.2 未満であれば，ほぼ相関はないとみなせる．

最初に入力 $\boldsymbol{X}$ に対して，異なる鍵 p をもつ 100 種類のランダムユニタリ変換 $\boldsymbol{Q}_p$ を用いて，秘匿入力 $\hat{\boldsymbol{X}}$ を生成した．次に悪意のあるユーザを想定し秘匿時とは異なる鍵 q をもつ 100 種類のランダムユニタリ変換 $\boldsymbol{Q}_q$ を生成し，秘匿入力 $\hat{\boldsymbol{X}}$ に対してそれぞれ復号 $\hat{\boldsymbol{X}}\boldsymbol{Q}_q^*$ を試みた．合計 $100 \times 100 = 10000$ 回の攻撃を試行したことになる．復号値 $\hat{\boldsymbol{X}}\boldsymbol{Q}_q^*$ と入力 $\boldsymbol{X}$ との PPMC を計算した．入力 $\boldsymbol{X}$ として，糖尿病の臨床データ（10 項目の検査結果からなる 442 人の患者のデータ）[23] と人工的に生成したデータの 2 種類を用いた．

表 1 に，糖尿病の臨床データの入力 $\boldsymbol{X} \in \mathbb{R}^{N \times M}$ $(N = 442, M = 10)$ に対して上記試行を行った際の PPMC の絶対値を示した．10000 回の試行の平均値，最大値，最小値を示している．表 1 より，平均値ではほぼ相関がないとみなせる結果が得られている．最大値では比較的大きな値を示すケースがあり，秘匿強度は必ずしも十分ではない．これは次元が $M = 10$ の場合，ランダムユニタリ変換 $\boldsymbol{Q}_p \in \mathbb{R}^{M \times M}$ の鍵空間の広さが十分に大きくないことに起因すると推測される．

次に人工的に生成した正規ガウス分布に従う入力 $\boldsymbol{X} \in \mathbb{R}^{N \times D}$ $(N = 100, M)$ に対して，次元 M を変化させたとき $(M = 5, 10, 20, 50, 100)$ の PPMC について検証した．図 6 に，上記試行を行った際の PPMC の絶対値を示した．10000 回の試行の平均値，最大値，最小値を示している．M の次元が 30 付近よりも大きい領域では，PPMC の絶対値は平均値のみならず最大値も 0.2 を下回りほぼ相関がないとみなせる結果が得られている．

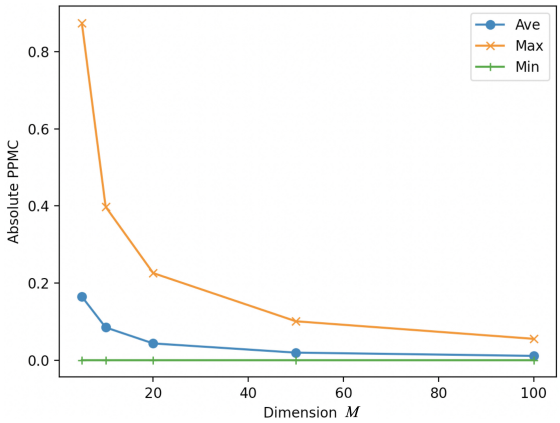


図 6　人工データの入力 $\boldsymbol{X}$（M を変化させた場合）に対するピアソンの積率相関係数（PPMC）の絶対値の平均値，最大値，最小値

5.2　ランダムユニタリ変換の秘匿性強化

前小節の議論のとおり，ランダムユニタリ変換の秘匿化強度，すなわち，秘匿化信号からの原信号を復元する際の不確定性はランダムユニタリ変換のサイズ M に依存する．M は秘匿信号を埋め込む空間の次元数を規定するためである．この M は，$\boldsymbol{y}$ の次元数および $\boldsymbol{X}$ の行数に対応する．このため，M が小さくなると，ランダムユニタリ変換による秘匿化強度が低下することになる．そこで，原信号の次元数 M によらず秘匿化強度を保持することを目的とし，高次元空間への秘匿信号の埋め込みに基づき秘匿性の強化を図る方法が提案されている [7]．この埋め込みは，ランダムユニタリ変換の次元拡大と摂動情報の付加から構成される．

ランダムユニタリ変換の次元拡大では，$\boldsymbol{y}$ および $\boldsymbol{X}$ を各々，$\tilde{M}$ 次元ベクトルおよび $\tilde{M} \times K$ 行列に拡張 $(\tilde{M} > M)$ し，大きなサイズのランダムユニタリ変換が用いられる．このアプローチは，秘匿化にランダムユニタリ変換の利用という点において変更はないため，4. 節に記載の各種アルゴリズムに適用可能である．また，このアプローチは，攻撃者が次元拡張前のサイズ M を未知であれば，秘匿化強度の強化に関して効果的に機能する．

しかし，次元拡張前のサイズ M を攻撃者が既知の場合，ランダムユニタリ行列のサイズを増加させるだけでは秘匿化強度の強化につながらない．サイズ $\tilde{M}$ のランダムユニタリ変換により秘匿化された信号は，$\tilde{M}$ 次元空間内の超球面（原点を中心とし，秘匿化前の原信号のユークリッドノルムを半径とする）上に射影される．見かけ上，秘匿信号は $\tilde{M}$ 次元空間に埋め込まれる．しかし，次元拡張前のサイズ M を既知の攻撃者であれば，原信号の存在範囲を M 次元部分空間内の超球面上に絞り込める．このため，原信号を復元する際の不確定性は，次元拡張前の M 次元空間内に制限されてしまう．

そこで，摂動情報を付加するアプローチが追加される．秘匿化信号 $\tilde{\boldsymbol{y}} \in \mathbb{R}^{\tilde{M}}$, $\tilde{\boldsymbol{X}} \in \mathbb{R}^{\tilde{M} \times K}$ を次式の変換により生成する．

$$\tilde{\boldsymbol{y}} = \boldsymbol{Q}_{\zeta,\tilde{M}} \boldsymbol{S} \boldsymbol{y} + \boldsymbol{\psi} \tag{58}$$

$$\tilde{\boldsymbol{X}} = \boldsymbol{Q}_{\zeta,\tilde{M}} \boldsymbol{S} \boldsymbol{X} + \boldsymbol{\Phi} \tag{59}$$

ここで，$\boldsymbol{Q}_{\zeta,\tilde{M}} \in \mathbb{R}^{\tilde{M}\times\tilde{M}}$ は，秘匿鍵 ζ およびサイズ $\tilde{M}\times\tilde{M}$ のランダムユニタリ行列である．$\boldsymbol{S} \in \mathbb{R}^{\tilde{M}\times M}$ は，ベクトルの次元を M から $\tilde{M}$ へ拡張する変換である．$\boldsymbol{S}$ は，1 および 0 を要素とし，各列は一つだけ 1 を含み，かつ，各行はたかだか一つの 1 を含むように構成される．このとき，$\boldsymbol{Q}_{\zeta,\tilde{M}}\boldsymbol{S}$ は，$\boldsymbol{Q}_{\zeta,\tilde{M}}$ の M 本の列ベクトルにより構成される．$\boldsymbol{\psi} \in \mathbb{R}^{\tilde{M}}$ は，$\boldsymbol{Q}_{\zeta,\tilde{M}}\boldsymbol{S}$ に含まれない $\boldsymbol{Q}_{\zeta,\tilde{M}}$ の列ベクトルとし，$\boldsymbol{\Phi} \in \mathbb{R}^{\tilde{M}\times K}$ は $\boldsymbol{Q}_{\zeta,\tilde{M}}\boldsymbol{S}$ および $\boldsymbol{\psi}$ に含まれない $\boldsymbol{Q}_{\zeta,\tilde{M}}$ の K 本の列ベクトルにより構成される．摂動情報として，$\boldsymbol{\psi}, \boldsymbol{\Phi}$ を加えることで，次元拡張前のサイズ M を既知の攻撃者に対しても，原信号の存在する M 次元部分空間内の超球面を秘匿可能となる．

ただし，式 (58) (59) による秘匿化信号領域において，原信号と同一の求解結果を算出するために，適切なコスト関数を設定する必要がある．例えば，LASSO の場合，式 (58) (59) の秘匿化信号に対する式 (26) のコスト関数の最小解は，原信号の LASSO 解と一致しない．そこで，次のコスト関数が導入される[7]．

$$\tilde{L}(\boldsymbol{w}) \triangleq \frac{1}{2}||\tilde{\boldsymbol{y}} - \tilde{\boldsymbol{X}}\boldsymbol{w}||_2^2 + \lambda||\boldsymbol{w}||_1 - \frac{1}{2}||\boldsymbol{w}||_2^2 \tag{60}$$

このとき，$\boldsymbol{\psi}$ および $\boldsymbol{\Phi}$ が次の関係

$$\boldsymbol{\psi}^T(\boldsymbol{Q}_{\zeta,\tilde{M}}\boldsymbol{S}) = \boldsymbol{0}_M \tag{61}$$

$$\boldsymbol{\Phi}^T(\boldsymbol{Q}_{\zeta,\tilde{M}}\boldsymbol{S}) = \boldsymbol{0}_{K\times M} \tag{62}$$

$$\boldsymbol{\psi}^T\boldsymbol{\Phi} = \boldsymbol{0}_K \tag{63}$$

を満たす (なお，$\boldsymbol{0}_M$，$\boldsymbol{0}_K$ および $\boldsymbol{0}_{K\times M}$ は，各々，全ての要素を 0 とする M 次元ベクトル，K 次元ベクトルおよび $M\times K$ 行列である) ことに注意すると，次式が得られる．

$$||\tilde{\boldsymbol{y}} - \tilde{\boldsymbol{X}}\boldsymbol{w}||_2^2 = ||\boldsymbol{y} - \boldsymbol{X}\boldsymbol{w}||_2^2 + ||\boldsymbol{w}||_2^2 + ||\boldsymbol{\psi}||_2^2 \tag{64}$$

更に，上式を用いることで，コスト関数を以下のように変形できる．

$$\begin{aligned}\tilde{L}(\boldsymbol{w}) &= ||\boldsymbol{y} - \boldsymbol{X}\boldsymbol{w}||_2^2 + \lambda||\boldsymbol{w}||_1 + \frac{1}{2}||\boldsymbol{\psi}||_2^2 \\ &= L(\boldsymbol{w}) + \frac{1}{2}||\boldsymbol{\psi}||_2^2\end{aligned} \tag{65}$$

上式を用いて，以下の関係を導出できる．

$$\arg\min_{\boldsymbol{w}} \tilde{L}(\boldsymbol{w}) = \arg\min_{\boldsymbol{w}} L(\boldsymbol{w}) \tag{66}$$

つまり，式 (58) (59) により秘匿化された信号に対して，$\arg\min_{\boldsymbol{w}} \tilde{L}(\boldsymbol{w})$ の解を求めれば，秘匿化前の信号に対する LASSO 解を導出できることを上式は示している．また，LASSO を一般化した Elastic Net[53]においても，コスト関数を適切に設定することで，高次元空間へ埋め込まれた秘匿信号領域において，原信号の Elastic Net 解を求解可能であることが示されている[7]．

なおアプリケーションごとに必要とされる秘匿強度や要求条件が異なるため，個々のアプリケーションでは秘匿強度を高める工夫が行われている．例えば，6.2 節で紹介の暗号化画像の圧縮では，画像パッチごとに秘匿スパースモデリングを適用しているが，画像パッチ間の入換えを併用することで，視覚的スクランブル効果を高めている．

6. エッジ AI への応用

スパースモデリングは，深層学習と比較して軽量で少量学習データで動作する．またランダムユニタリ変換は秘密計算方式よりも遥かに少ない演算量でデータの秘匿化が可能である．これらの特性より，秘匿スパースモデリングはエッジ AI 処理と非常に相性がよい．本節では，秘匿スパースモデリングのエッジ AI への適用例について述べる．

6.1 エッジ AI の概要

クラウド処理では高性能な GPU や CPU を用意し，大量のデータをもとに深層学習などを使って学習・推論を行う．一方，エッジ AI は端末近くに AI を配置し，学習・推論させる技術である．端末近くにサーバを配置しデータ処理を行う「エッジコンピューティング」(Edge Computing) に AI を搭載したものといえる．エッジ AI の実施形態として大きく，1) 学習はクラウド・推論はエッジ，2) 学習と推論の両方ともエッジ，で行うパターンがある．図 7 にはエッジで学習と推論を行い，必要な処理済みデータのみをクラウドに送信する実施例を示した．クラウド処理に対して，エッジ AI は以下のメリットをもつ．

1) 通信コストの削減：必要な処理済みデータのみクラウドへ送信するため，通信コストが削減できる．

2) リアルタイム性：端末とエッジ側間の距離が近く，低遅延処理が可能となる．

3) セキュリティ強化：エッジ側で個人情報や機密情報の管理を行うことで，不正アクセスの被害も受けにくくなる．

エッジに搭載されるデバイスは，演算速度やメモリ性能が限定されることが多いため，アルゴリズムも演算負荷など低いものが望まれる．スパースモデリングは，深層学習と比較して演算量が圧倒的に低く，エッジ AI と非常に相性がよい．少量データで学習が可能であり，時事刻々と変化するデータの特性に素

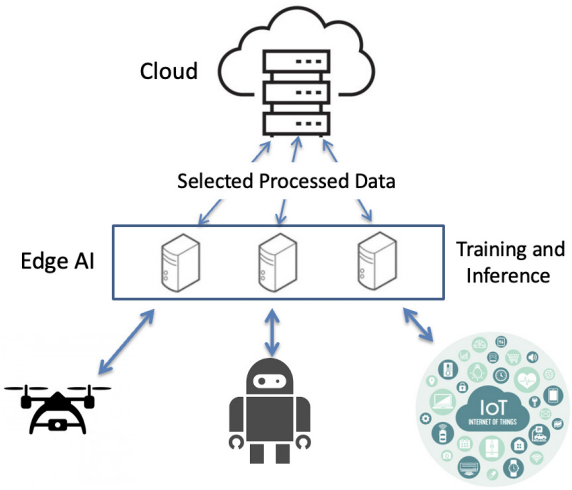


図 7　エッジ AI の実施形態例（学習と推論をエッジで実行）

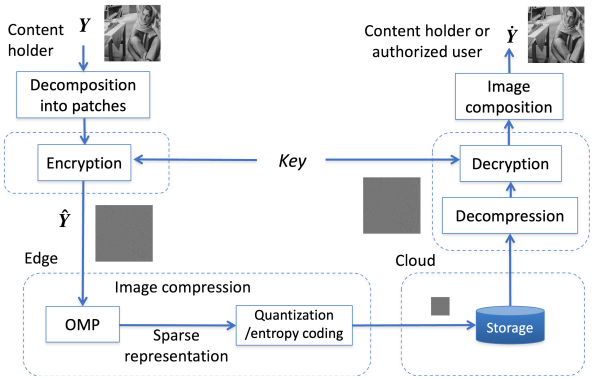


図 8　EtC のシステム構成図

早く追従しリアルタイム性に優れる．また秘匿演算を用いることで，セキュリティ強度を更に向上させることができる．

エッジ AI において秘匿スパースモデリングを適用する場合には，最初に端末側で対象データを暗号化し，エッジへ暗号化データを送信する．エッジでは暗号化データから特徴を学習し，圧縮や認識，データ解析などの処理を行い，必要なコンテンツの特徴量や中間データのみをクラウドへ転送し保存する．なお秘匿演算を用いないで圧縮や認識，データ解析を行う際には，暗号をいったん解除する必要があるが，秘匿スパースモデリングを用いることで，暗号を解除することなく圧縮や認識，データ解析が可能となる．コンテンツの中身がプロバイダなど第 3 者に対して秘匿でき，何らかのアクシデントの発生により，データが流出した場合でも，プライバシーの保護が可能となる．以下，具体的に暗号化画像の圧縮と認識，臨床検査など個人情報解析への適用例について説明する．

6.2　暗号化画像の圧縮

スパースモデリングは，多くの画像処理の分野において有効性が認められているが，画像圧縮においても国際標準の JPEG や JPEG2000 を上回る符号化特性が報告されている．スパースモデリングでは辞書学習によって対象画像の特性に応じた基底の設計が可能であり，少ない係数でモデル化が可能なことに起因する．著者らは文献(2)において，スパースモデリングを用いた暗号化画像の Encryption-then-Compression (EtC) システムを提案した．図 8 に EtC のシステム構成図を示す．最初に端末側で，暗号化画像 $\hat{\boldsymbol{Y}}$ を生成する．次に暗号化画像 $\hat{\boldsymbol{Y}}$ をエッジへ転送し，OMP アルゴリズムによりスパース係数を抽出し，量子化並びにエントロピー符号化を経て圧縮ビット列が生成される．受信側では圧縮ビット列を復号し暗号化画像を得る．暗号化画像は，暗号化画像の生成に用いた鍵をもつユーザは解除でき復号画像 $\dot{\boldsymbol{Y}}$ が得られる．

なお辞書学習は画像全体ではなく，図 9 に示すように画像パッチと呼ばれる小領域に分割した上で行う．図 10 (b) には，K-SVD によって得られる基底の例を示している．比較のために図 10 (a) には離散コサイン変換を示した．学習用のデータセットして，標準画像データベース SIDBA (Standard Image Data-BAse) の Barbara 画像を使用した．辞書学習によって得

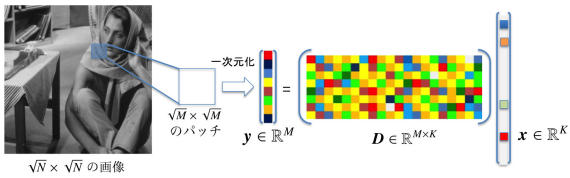
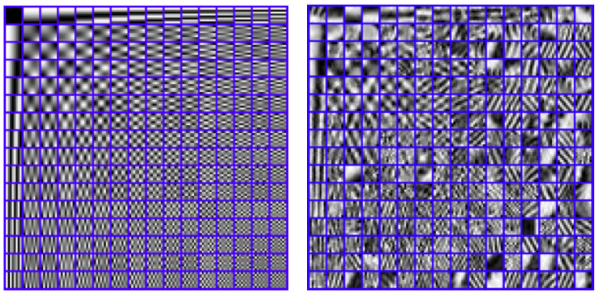


図 9　画像パッチのスパースモデル



(a) 離散コサイン変換　　(b) K-SVD

図 10　離散コサイン変換と辞書学習（K-SVD）により得られた基底

(a) Barbara 画像　　(b) 暗号化画像

図 11　原画像と対応する暗号化画像

られる基底は，離散コサイン変換とは異なりデータ依存である．そのため学習の対象として使用されたデータ集合の様々な特徴を表しており，辞書学習自体が一つのパターン発見手法となっているといえる．また学習した基底に基づき少ない基底で画像をモデル化でき，効率よく情報を抽出できる．この辞書学習は，4.3 節に記載の秘匿 K-SVD により，暗号化したまま可能である．秘匿辞書学習並びに圧縮の際に，暗号化画像は画像パッチごとにランダムユニタリ変換により暗号化を行い，画像パッチ間の入換えを行うことで生成する．ランダムユニタリ変換と画像パッチ間の入換えを併用することで，視覚的スクランブル効果を高めている．

図 11 に暗号化画像の例を示した．視認性は十分低く，暗号化が行われていることが確認できる．図 12 には，それぞれ正式なユーザと不正ユーザによる復号画像の例を示した．不正ユーザは画像を復号することができず，プライバシーが保護できていることが確認できる．図 13 に秘匿スパースモデリングの符号化特性を示した．秘匿 MOD(注4) と秘匿 K-SVD を用いた．比較対象として，離散コサイン変換(注5) を用いた．図 13 より，秘匿

(注4)：MOD（Method of Optimal Direction）はスパース辞書学習の一つで，文献(3)において，秘匿 K-SVD と同様な方法で秘匿学習が可能であることが報告されている．

(注5)：スパースモデリングで用いる離散コサイン変換（discrete cosine transform: DCT）は，過完備（Overcomplete）なため，図 13 の凡例では Overcomplete DCT と記載している．

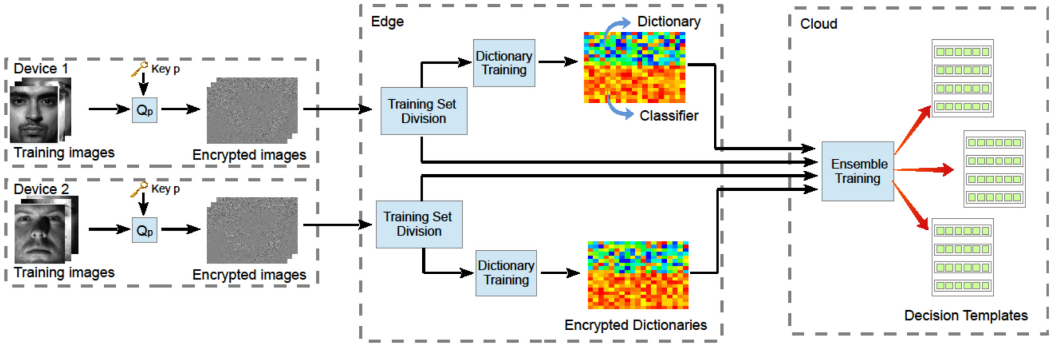
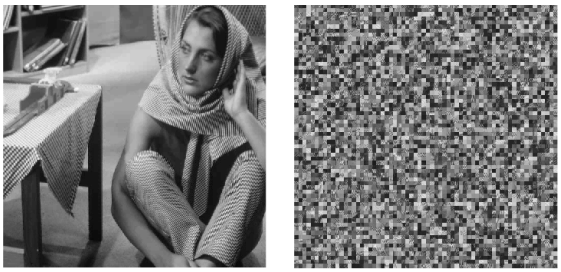


図 14　秘匿スパースモデリングによるアンサンブル学習



ϵ = 3.0 (PSNR = 39.28 [dB])　　ϵ=3.0(PSNR = 10.43 [dB])

(a) 正式なユーザ　　(b) 不正ユーザ

図 12　復号画像

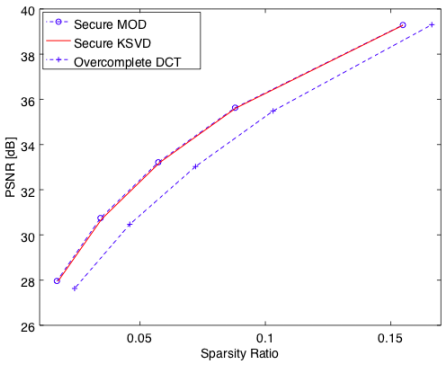


図 13　秘匿スパースモデリングの符号化特性

MOD 並びに秘匿 K-SVD は，対象画像から基底を設計しているため，離散コサイン変換よりも少ないスパース係数で効率よくモデル化できていることが分かる．なお提案法では，暗号化画像からスパース係数を推定する際に OMP アルゴリズムを用いているため，辞書の基底が逐次追加されスパース係数が推定される．図 13 の符号化特性は，逐次追加される基底に基づいて，復号される画像の PSNR を示したものである．提案案法では画像を暗号化したまま，再帰的に OMP アルゴリズムを実行する中で，スパース係数の個数や復号画像の品質を確認できる．所望の条件に達したら符号化を終了する．

6.3　秘匿顔画像の認識

著者らは文献(5)において，エッジサーバが空間的に多数配置される分散環境を前提として，秘匿スパースモデリングにアンサンブル学習を併用する顔画像の認識方式を提案した．これは，

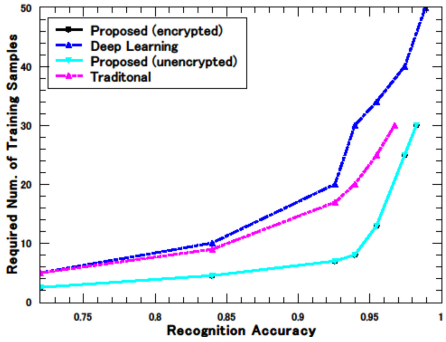


図 15　学習枚数と認識率．

表 2　演算量 (秒)

	分散秘匿スパース[5]	SPCANet[55]	LC-KSVD[27]
学習時間	7.29	5780	4.84
認識時間/枚	1.64×10^{-3}	1.20	1×10^{-4}

4.3 節に記載の秘匿 LC-KSVD 法を用いた応用例であり，秘匿領域における分散学習・認識において，Decision Profile (DP) と Decision Template (DT) と呼ぶ概念を導入し，モデル化誤差と雑音を考慮することで認識性能を向上させている．

提案法の有効性を検証するために，シミュレーションを行った．評価画像として，顔画像認識に広く用いられている Extended YaleB を用いた[54]．1 人あたり約 64 枚の顔画像が 38 人分用意されている．訓練画像用に 1 人あたりランダムに 32 枚の画像を選択し，10 枚の画像をアンサンブル学習用に使用した．比較対象として，深層学習を用いた SPCANet[55] と呼ばれる手法と秘匿化を行わない通常の LC-KSVD[27] を用いた．SPCANet は 5 層の畳み込みニューラルネット (CNN) を利用し，識別特徴量を抽出するために PCA を用いている．図 15 に認識率と 1 クラスあたりの学習サンプル数との関係を示す．まず提案法は顔画像を秘匿した場合としない場合で，同じ特性を示すことが確認できる．次に提案法は少ない学習サンプル数で高い認識率を達成でき，学習画像が 1 人あたり 10 枚と少ない場合には，SPCANet に対して認識率は約 10%上回っている．SPCANet と比較すると約半分の学習サンプル数で同等の性能を示すことが分かる．学習画像が多い場合でも SPCANet とほぼ同等の約 98%の認識率を達成している．

6.4 臨床検査等の個人情報解析

取得データの個人特定につながる可能性のあるデータは，プライバシー保護の観点から，エッジ/クラウドコンピューティングの利用は制限される．例えば，臨床検査結果，購買履歴，移動経路などが挙げられる．こうしたデータに対しては，データを取得した組織・機関に閉じて利用される．大量のユーザを抱え，所望の規模のデータを取得可能な場合は，問題ない．しかし，医療機関における臨床データのように，各機関で取得可能なデータ数が限られている場合，各機関に閉じた分析では，十分な分析精度を得られない場合がある[56]．問題の原因は，取得されたデータが分散しており，集約できない点にある．

そこで，ランダムユニタリ変換による秘匿化の機能拡張として，単一拠点内に閉じた秘匿化ではなく，分散した拠点において情報を秘匿化する分散秘匿化が検討されている[50]．上記の検討では，LASSO[22]による分析モデル構築を対象とし，分散秘匿化が LASSO 解を保全する理論的保証を与えている．つまり，各拠点において個別に秘匿化されたデータを集約し，LASSO 解を求めたとしても，秘匿化前の原データと同一の LASSO 解が導出可能であることを保証している．この結果，分散秘匿化されたデータに対する直接的な分析が可能となった．

また，分散秘匿化の対象となる分析モデルをビッグデータ分析の手法として広範囲な有効性が確認されている Elastic Net[53]へも拡張されている[7]．つまり，ランダムユニタリ変換により分散秘匿化されたデータに対して，得られる Elastic Net 解，すなわち，分析モデルは，秘匿化の影響を受けず，秘匿化前の原信号に対して構築する分析モデルと等価なモデルが，秘匿化データを用いた場合も構築可能であることを理論的に保証している．

この結果，多様な条件下で分散秘匿化が可能となり，集約された秘匿化データを用いて，秘匿化前のデータに対する分析モデルと同一の結果を取得できるようになる．つまり，データの機密性は確保した上で，集約したデータを利用した大規模な分析が可能となり，分散取得されたきたプライバシー保護が必要なデータに対しても，分析精度の向上が実現される．

一例として，糖尿病の臨床データを用いた分析結果を示す．用いた糖尿病データ[23]は，442 人の患者のデータから構成され，各患者に対して 10 項目の検査結果と検査から 1 年後の疾病進行度をデータとして含む．上述の検査結果（特徴行列を構成）および疾病進行度（観測ベクトルを構成）を秘匿した上で，10 項目の検査結果から疾病進行度を予測する予測モデルを ElasticNet を用いて構築し，疾病進行度の予測精度を検証対象とした．データを集約して分析を行う効果を検証するため，糖尿病データを K 個のサブセットに分割し，各サブセットが拠点ごとに観測されるデータとみなして，以下の実験を行った．なお，拠点数は $K = 16, 32$ とした．各サブセット内のデータを学習データと検証データに分離し，以下の 2 種類の予測モデルを比較した．一つめの予測モデルは，秘匿化して集約した全拠点の学習データを用いて構築した．同予測モデルを用いて，各拠点の検証データに対して，予測を実施した．上記予測モデルを統合予測モデルと呼ぶ．二つめの予測モデルは，自拠点内の学習データのみを用いて構築した．上記予測モデルを独立予測モデルと呼ぶ．

表 3 予測誤差

拠点数	予測誤差: 統合予測モデル	予測誤差: 独立予測モデル	予測誤差 低減率 [%]
16	54.7	61.8	11.5
32	54.7	65.0	15.9

表 3 に統合予測モデルおよび独立予測モデルにより得られる予測誤差を示す．あわせて，次式の尺度を用いて，統合予測モデルによる予測誤差低減率も評価した．

$$\text{予測誤差低減率} = \frac{\text{独立予測モデルの予測誤差} - \text{統合予測モデルの予測誤差}}{\text{独立予測モデルの予測誤差}}$$

同表の結果から，統合予測モデルは独立予測モデルに比べて予測誤差を低減できており，各拠点のデータを集約して予測することにより，予測精度の向上につながることを確認できた．従来，個人情報などを含むために拠点内に閉じた利用に限定されていたデータであっても，提案技術により，データのプライバシーを保護した状態でデータを統合・分析することが可能となり，分析性能の向上を実現できることを，本実験結果は示している．

7. まとめと今後の展望

本稿では軽量・少量学習データで動作するスパースモデリングの秘匿演算処理技術とエッジ AI への適用について述べた．秘匿スパースモデリングは，スパースモデリングの係数選択・推定並びに学習アルゴリズムが変更なく使用できることから，スパースモデリングの有効性が報告されている多数の分野へ適用できる．近年通信コストの削減，リアルタイム性，セキュリティ強化といった観点からエッジ AI への注目が集まっており，秘匿スパースモデリングは，エッジ AI の一つのツールとして有望であると考えている．

またランダムユニタリ変換を用いた秘匿演算として，非線形モデリングであるガウス過程の秘匿演算も実現可能であることが報告されている[57],[58]．ガウス過程は一般に過学習（オーバーフィティング）が起こりにくく，学習データが少ない場合には，深層学習と比べ汎化性能に優れる．ガウス過程の演算量はデータ量の 3 乗のオーダーとなるため，データ量が多い場合には高い演算負荷が課題となるが，データ量が少ない場合には十分低い演算量で動作する．今後，具体的な応用事例での検証は必要であるが，秘匿スパースモデリングと同様に軽量・少量学習データで動作するエッジ AI として期待できる．

文　献

(1) C.T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varad-harajan, and C-C.J. Kuo, “Survey on securing data storage in the cloud,” APSIPA Transactions on Signal and Information Processing, vol.3, e7, 2014.

(2) T. Nakachi and H. Kiya, “Secure OMP computation maintaining sparse representations and its application

to EtC systems," IEICE Trans. Inf. & Syst., vol.E103-D, no.9, 2020.
(3) T. Nakachi, Y. Bandoh, and H. Kiya, "Secure overcomplete dictionary learning for sparse representation," IEICE Trans. Inf. & Syst., vol.E103-D, no.1, pp.50–58, 2020.
(4) T. Nakachi and H. Kiya, "Secure OMP based pattern recognition that supports image compression," Signal & Image Processing: An International Journal (SIPIJ), vol.11, no.2, 2020.
(5) Y. Wang and T. Nakachi, "A privacy-preserving learning framework for face recognition in edge and cloud networks," IEEE Access, vol.8, pp.136056–136070, 2020.
(6) T. Nakachi, H. Ishihara, and H. Kiya, "Privacy-preserving network BMI decoding of covert spatial attention," IEEE ICSPCS2018, p12, 2018.
(7) Y. Bandoh, T. Nakachi, and H. Kiya, "Distributed secure sparse modeling based on random unitary transform," IEEE Access, vol.8, pp.211762–211772, 2020.
(8) B.A. Olshausen and D.J. Field, "Emergence of simple-cell receptive-field properties by learning a sparse code for natural images," Nature, vol.381, pp.607–609, 1996.
(9) 日野英逸，村田昇，"スパース表現の数理とその応用," 信学技報，vol.112(198), pp.133–142, 2012.
(10) 笠井裕之，"スパースコーディングの研究動向," 研究報告オーディオビジュアル複合情報処理 (AVM)，vol.2014-AVM-84(8), pp.1–10, 2014.
(11) 手塚太郎，"辞書学習によるビッグデータからのパターン発見," 日本化学会情報化学部会誌，vol.32, no.4, pp.76–79, 2014.
(12) M. Elad, Sparse and redundant representations: from theory to applications in signal and mage processing, Springer, 2010.
(13) M. Lustig, D. Donoho, and J. Pauly, "Sparse MRI: The application of compressed sensing for rapid MR imaging," Journal of the Society of Magnetic Resonance in Medicine, 2007.
(14) 本間希樹，"巨大ブラックホール撮像への挑戦," 信学誌，vol.99, no.5, pp.400–405, 2016.
(15) 井手剛，"疎な相関グラフの学習による相関異常の検出," 人工知能学会データマイニングと統計数理研究会 (第 9 回)，SIG-DMSM-A803, 2009.
(16) 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," 信学 FR 誌，vol.13, no.2, pp.95–107, Oct. 2019.
(17) T. Horikawa, M. Tamaki, Y. Miyawaki, and Y. Kamitani, "Neural decoding of visual imagery during sleep," Science, vol.340, no.6132, pp.639–642, 2013.
(18) B.K. Natarajan: "Sparse approximate solutions to linear systems," SIAM J. Comput., vol.24, no.2, pp.227–234, 1995.
(19) S. Mallat and Z. Zhang, "Matching pursuits with time-frequency dictionaries," IEEE Trans. Signal Process., vol.41, no.12, pp.3397–3415, 1993.
(20) Y.C. Pati, R. Rezaiifar, and P.S. Krishnaprasad, "Orthogonal matching pursuit: Recursive function approximation with applications to wavelet decomposition," 27th Asilomar Conference on Signals, Systems and Computers, pp.40–44, 1993.
(21) S.S. Chen, D.L. Donoho, and M.A. Saunders, "Atomic decomposition by basis pursuit," SIAM Journal on Scientific Computing, vol.20, no.1, pp.33–61, 1998.
(22) R. Tibshirani, "Regression shrinkage and selection via the lasso," Journal of the Royal Statistical Society, Series B (Methodological), vol.58, no.1, pp.267–288, 1996.
(23) B. Efron, T. Hastie, I. Johnstone, and R. Tibshirani, "Least angle regression (with discussion)," The Annals of Statistics, vol.32, pp.407–499, 2004.
(24) J. Friedman, T. Hastie, and R. Tibshirani, "Sparse inverse covariance estimation with the graphical lasso," Biostatistics, vol.9, no.3, pp.432–441, 2008.
(25) S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," Foundations and Trends in Machine Learning, vol.3, no.1, pp.1–122, 2011.
(26) K. Engan, S.O. Aase, and J. Hakon Husoy, "Method of optimal directions for frame design," IEEE ICASSP1999, pp.2443–2446, 1999.
(27) Z. Jiang, Z. Lin, and L.S. Davis, "Label consistent K-SVD: learning a discriminative dictionary for recognition," IEEE Trans. Pattern Anal. Mach. Intell., vol.35, no.11, pp.2651–2664, Nov., 2013.
(28) HACARUS, https://hacarus.com/ja/.
(29) R.L. Lagendijk, Z. Erkin, and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," IEEE Signal Process. Mag., vol.30, no.1, pp.82–105, 2013.
(30) M. Barni, G. Droandi, and R. Lazzeretti, "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing," IEEE Signal Process. Mag., vol.32, no.5, pp.66–76, 2015.
(31) Z. Brakerski, "Fundamentals of fully homomorphic encryption: A survey," Electronic Colloquium on Computational Complexity, report no.125, 2018.
(32) Y. Aono, T. Hayashi, L. Phong, and L. Wang, "Privacy-preserving logistic regression with distributed data sources via homomorphic encryption," IEICE Trans. Inf. & Syst., vol.E99-D, no.8, pp.2079–2089, 2016.
(33) T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein, "Optimized honest-majority MPC for malicious adversaries: breaking the 1 billion-gate per second barrier," IEEE Symposium on Security and Privacy, pp.843–862, 2017.
(34) A. Chatterjee and I. Sengupta, "Sorting of fully homomorphic encrypted cloud data: Can partitioning be effective?," IEEE Trans. Services Comput., vol.13, no.3, pp.545–558, 2020.
(35) C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP J. Information Security, pp.1–25, 2011.
(36) S. Rane, "Standardization of biometric template protection," IEEE MultiMedia, vol.21, no.4, pp.94–99, 2014.
(37) K. Nandakumar and A.K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," IEEE Signal Process. Mag., vol.32, no.5, pp.88–100, 2015.
(38) V. Patel, N. Ratha, and R. Chellappa, "Cancelable biometrics: A review," IEEE Signal Process. Mag., vol.32, no.5, pp.54–65, 2015.
(39) E. Bingham and H. Mannila, "Random projection in dimensionality reduction: applications to image and text data," KDD-2001: Proc. the Seventh ACM SIGKDD Int. Conf. Knowledge Discovery and Data Mining, pp.245–250, 2001.
(40) J.K. Pillai, V.M. Patel, R. Chellappa, and N.K. Ratha, "Secure and robust iris recognition using random projections and sparse representations," IEEE Trans. Pattern Anal. Mach. Intell., vol.30, no.9, pp.1877–1897, 2011.
(41) A.B.J. Teoh, A. Goh, and D.C.L. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs," IEEE Trans. Pattern Anal. Mach. Intell., vol.28, no.12, pp.1892–1901, 2006.
(42) I. Nakamura, Y. Tonomura, and H. Kiya, "Unitary transform-based tempalte protection and its application to l2-norm minimization problems," IEICE Trans. Inf. & Syst., vol.E99-D, no.1, pp.60–68, 2016.
(43) M. Aharon, M. Elad, and A. Bruckstein, "K-SVD: An algorithm for designing overcomplete dictionaries for

sparse representation," IEEE Trans. Signal Process., vol.54, no.11, pp.4311–4322, 2006.
(44) M. Elad, "Sparse and redundant representation modeling: what next?," IEEE Trans. Signal Process. Lett., vol.19, no.12, pp.922–928, 2012.
(45) ITU-T and ISO/IEC JTC 1, "Information technology - digital compression and coding of continuous-tone still images: Requirements and guidelines," ITU-T Rec. T.81 and ISO/IEC iso/iec 10918-1:1994, June 1994.
(46) J. Wang, Y. Bandoh, A. Shimizu, and Y. Yashima, "Multi-class dictionary design algorithm based on iterative class update K-SVD for image compression," IIEEJ Transactions on Image Electronics and Visual Computing, vol.8, no.1, pp.44–57, 2020.
(47) Y. Saito, I. Nakamura, S. Shiota and H. Kiya, "An efficient random unitary matrix for biometric template protection," 2016 Joint 8th International Conference on Soft Computing and Intelligent Systems (SCIS) and 17th International Symposium on Advanced Intelligent Systems (ISIS), Sapporo, pp.366–370, 2016.
(48) B.K. Natarajan, "Sparse approximate solutions to linear systems," SIAM J. Comput., vol.24, no.2, pp.227–234, 1995.
(49) J. Friedman, T. Hastie, H. Höfling, and R. Tibshirani, "Pathwise coordinate optimization," Annals of Applied Statistics, vol.1, no.2, pp.302–332, 2007.
(50) Y. Bandoh, T. Nakachi, and H. Kiya, "Sparse modeling on distributed encryption data," Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., pp.2123–2127, 2020.
(51) T. Nakachi, Y. Bandoh, and H. Kiya, "Secure dictionary learning for sparse representation," 2019 27th European Signal Processing Conference (EUSIPCO), pp.1–5, 2019.
(52) T. Nakachi, Y. Wang, and H. Kiya, "Privacy-preserving pattern recognition using encrypted sparse representations in L0 norm minimization," Proc. IEEE Int. Conf. Acoust., Speech, Signal Process., pp.2697–2701, 2020.
(53) H.Zou and T. Hastie, "Regularization and variable selection via the elastic net," Journal of the Royal Statistical Society, Series B (Statistical Methodology), vol.67, no.2, pp.301–320, 2005.
(54) K. Lee, J. Ho, and D. Kriegman, "Acquiring linear subspaces for face recognition under variable lighting," IEEE Trans. Pattern Anal. Mach. Intell., vol.27, no.5, pp.684–698, May 2005.
(55) L. Tian, C. Fan, Y. Ming, and Y. Jin, "Stacked PCA network (SPCANet): an effective deep learning for face recognition," Proc. of IEEE ICDSP 2015, pp.1039–1043, July 2015.
(56) Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," Proc. IEEE, vol.107, no.8, pp.1608–1631, 2019.
(57) T. Nakachi and Y. Wang, "Secure computation of Gaussian process regression for data analysis," European Signal Processing Conference (EUSIPCO2021).
(58) T. Nakachi and Y. Wang, "Access control for privacy-preserving Gaussian process regression," IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP2022), 2022.

(SIP 研究会提案，2022 年 7 月 22 日受付，
2022 年 8 月 9 日再受付)

仲地孝之（正員：シニア会員）
1997 年慶應義塾大学大学院後期博士課程了（工博）同年，日本電信電話（株）入社．スパース性に基づくデータ解析，セキュア信号処理，超高精細映像の符号化・伝送の研究に従事．現在，琉球大学情報基盤統括センター教授．

坂東幸浩（正員：シニア会員）
2002 年九州大学大学院システム情報科学研究科博士後期課程修了．同年日本電信電話株式会社入社．映像符号化，スパースモデリングなどの研究に従事．現在，NTT コンピュータ＆データサイエンス研究所主幹研究員．

ESS ニュース

2022 年　電子情報通信学会　NOLTA ソサイエティ大会　開催報告

2022 年　電子情報通信学会　NOLTA ソサイエティ大会実行委員広報担当　加藤秀行

1．開催概要

NOLTA ソサイエティ（以下，NLS）が主催する「2022 年 電子情報通信学会 NOLTA ソサイエティ大会（以下，NLS 大会）」が 6 月 11 日（土）に大阪大学・豊中キャンパスにて開催されました．一昨年（2020 年）は新型コロナウイルスの国内蔓延状況を鑑み中止となり，昨年（2021 年）も当初の計画では東京都市大学にて対面形式で開催する予定であったものの，感染拡大防止の観点からオンライン開催へと変更となったため，現地での対面形式での開催は，2019 年に新潟県長岡市のアオーレ長岡での開催を最後に，実に 3 年ぶりとなりました．

日時：2022 年 6 月 11 日（土）
場所：大阪大学　豊中キャンパス
主催：電子情報通信学会　NOLTA ソサイエティ
大会組織：

実行委員長・設営	松原　崇（大阪大学）
会計	中野 秀洋（東京都市大学），黒川 弘章（東京工科大学）
庶務	山仲 芳和（宇都宮大学），眞田 耕輔（三重大学）
広報	加藤 秀行（大分大学）
出版	伊藤 大輔（岐阜大学）

2．開催状況

2022 年 NLS 大会の参加人数は全 96 名（招待：3 名，一般：43 名，学生：50 名）でした．また，本大会の前日，前々日の 6 月 8 日（木），6 月 9 日（金）には NOLTA ソサイエティの研究会である非線形問題（NLP）研究会と複雑コミュニケーションサイエンス（CCS）研究会が対面とオンラインのハイブリッド形式で共催されました．

本大会は表 1 に示すとおり，はじめに大会実行委員長の松原崇先生（大阪大学）より開会の挨拶があり，続いて 2022 年度 NLS 会長の潮俊光先生（大阪大学）より NLS の現状の説明を交えたご挨拶を頂きました．その後，令和 2 年度にフェローを受賞された徳島大学の上田哲史先生より「学生に育てられたカオス研究者の半生」，令和 3 年度にフェローを受賞された名古屋工業大学の岡本英二先生より「非線形信号処理の移動通信システムへの適用と今後の展望について」というタイトルでフェロー記念公演を行って頂きました．更に，1 組めのポスターセッションを行い，午前の部を終了しました．

午後は 2 組めのポスターセッションを皮切りに，NLP 及び CCS の奨励賞受賞者による講演が行われ，その後休憩を挟み，2022 年度 NOLTA 誌編集委員長の堀尾善彦先生（東北大学）より NOLA 誌の現状についてのご報告がありました．また，NLS が主催するフラグシップシンポジウムである「NOLTA2022」及び「NOLTA2023」の現状について，2022 年の実行委員長である堀尾善彦先生（東北大学），2023 年の実行委員長である小西啓治先生（大阪府立大学）より，それぞれご報告頂きました．その後，NLP と CCS の年次報告と奨励賞の授賞式が行われました．最後に本大会奨励賞の授与式が執り行われ，大

表 1　大会プログラム

時間	イベント	プレゼンタ
9：30- 9：35	開会の挨拶	2022 年 NLS 大会実行委員長　松原崇（大阪大学）
9：35- 9：40	NOLTA ソサイエティ会長挨拶	2022 年度 NOLTA ソサイエティ会長　潮俊光（大阪大学）
9：40-10：10	電子情報通信学会　フェロー記念講演 1	上田哲史先生（徳島大学）
10：10-10：40	電子情報通信学会　フェロー記念講演 2	岡本英二先生（名古屋工業大学）
10：40-12：10	ポスターセッション A	
12：10-13：10	昼食	
13：10-14：40	ポスターセッション B	
14：40-14：50	休憩	
14：50-15：25	NLP 奨励賞受賞者講演	
15：25-15：50	CCS 奨励賞受賞者講演	
15：50-16：00	休憩	
16：00-16：15	NOLTA Journal の現状について	2022 年度 NOLTA 誌編集委員長　堀尾喜彦（東北大学）
16：15-16：30	NOLTA2022 について	NOLTA2022 General Chair　堀尾喜彦（東北大学）
16：30-16：45	NOLTA2023 について	NOLTA2023 General Chair 小西啓治（大阪府立大学）
16：45-17：00	NLP 年次報告・NLP 奨励賞授賞式	2022 年度 NLP 委員長　常田明夫（熊本大学）
17：00-17：15	CCS 年次報告・CCS 奨励賞授賞式	2022 年度 CCS 委員長　赤井恵（大阪大学/北海道大学）
17：15-17：30	2022 年 NOLTA ソサイエティ大会　奨励賞授与式	2022 年 NLS 大会実行委員長　松原崇（大阪大学）
17：30	閉会の挨拶・写真撮影	

表 2　令和 3 年度非線形問題研究会発表奨励賞受賞論文（† は受賞者，＊は講演者）

著者	タイトル
小池　允†・甲斐健也*（東京理科大）	離散力学と非線形最適化の融合による 2 次元非線形膜の安定化制御
加藤海渡†*（中京大）・麻原寛之（岡山理科大）・伊藤大輔（岐阜大）・高坂拓司（中京大）	1 次元離散非線形 RED モデルの有効性について
伊藤佳卓†*（北海道科学大）	パラメータ空間推定による植生バイオマスモデルの臨界点予測のダイナミカルノイズに対するロバスト性の検証

表 3　令和 3 年度複雑コミュニケーションサイエンス研究会発表奨励賞受賞論文（† は受賞者，＊は講演者）

著者	タイトル
田村颯樹†*・坪　泰宏（立命館大）	スパイキングリザバーネットワークにおけるスパイク遅延の効果
木下知哉†・会田雅樹*（都立大）	オンラインソーシャルネットワークにおけるスペクトルグラフ理論に基づく分極化モデル

会実行委員長による閉会の挨拶にて無事閉幕しました.

3. 研究専門員会奨励賞表彰式及び奨励賞受賞者講演

NLP では 2013 年から，CCS では 2015 年から，各研究会において発表された口頭発表論文の中から優れた発表に対して奨励賞を授与しており，2021 年度奨励賞の表彰式が本大会にて執り行われました．NLP の奨励賞（令和 3 年度非線形問題研究会発表奨励賞）受賞者は表 2，CCS の奨励賞（令和 3 年度複雑コミュニケーションサイエンス研究会発表奨励賞）受賞者は表 3 のとおりです．表彰式では，2022 年度 NLP 委員長の常田朋夫先生（熊本大学），2022 年度 CCS 委員長代理として浅井哲也先生（北海道大学）から各研究会の奨励賞受賞者に賞状が贈られました.

本大会では，「奨励賞受賞者講演」にて各奨励賞受賞者の方に受賞の対象となった研究について口頭発表をして頂くことをお願いし，口頭発表が可能であった受賞者 3 名（内 NLP2 名，CCS1 名）の方，及び代理の方（内 NLP1 名，CCS1 名）に講演して頂きました．いずれの受賞者も奨励賞受賞に相応しい発表であり，参加者の皆様にとっても大変有意義な時間となりました.

表 4　2022 年度 NOLTA ソサイエティ大会奨励賞受賞者

受賞者	発表タイトル
天羽晟矢（徳島大学）	マルチバイブレータとカナール
飯沼柊馬（長岡技術科学大学）	リザバーコンピューティングと安定性変換を利用した固定点の検出

令和 3 年度令和 3 年度非線形問題研究会発表奨励賞及び複雑コミュニケーションサイエンス研究会発表奨励賞受賞講演者

2022 年度 NOLTA ソサイエティ大会奨励賞受賞者と本大会実行委員長 松原崇先生（大阪大学）

4. NLS 大会奨励賞

2022 年度 NLS 大会では，大会中の一般公演において，ソサイエティの発展に貢献しうる講演論文を発表した著者（大会開催年の 4 月 1 日時点で満 35 歳以下の者）に対し，大会奨励賞を贈呈しています．本大会では表 4 に示す 2 名が受賞者として選ばれました．奨励賞表彰授与式は大会の最後に執り行われ，大会実行委員長より賞状が授与されました．受賞した 2 名の方，おめでとうございました．

5. おわりに

3 年ぶりに現地での対面形式にて開催した本大会は，多くの方にご参加頂き，盛会のうちに終えることができました．本大会にてご講演，ポスター発表された方々，聴講参加された皆様に深く感謝申し上げます．2023 年の NLS 大会は中野秀洋先生（東京都市大学）を実行委員長に据え開催予定です．まだまだコロナウイルスが猛威をふるう日が続きますが，来年もまた本年と変わらず現地にて開催できることを願っております．ぜひ来年の大会にご投稿，ご参加頂きますよう，よろしくお願い申し上げます．

加藤秀行（正員）

平 19 埼玉大工・情報システム工卒．平 23 同大学大学院博士後期課程了．同年学振 PD 研究員．平 24UIB IFISC 博士研究員，埼玉大理工学研究科研究員（兼務）．平 25 お茶大シミュレーション科学教育研究センター特任リサーチフェロー．平 26 東京工科大助教．平 29 大分大助教．平 30 同大学講師．数理神経科学，特にスパイキングニューラルネットワークに関する研究や非線形力学系における非線形振動子結合系に関する研究に従事．平成 19 年度学術奨励賞．

研究会に行こう！

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

■超音波研究会（US）

超音波技術は四つの領域から成り立っています．すなわち，①自動運転やドローン，ロボットなどに応用されるセンサ，工場設備やプラントの各種非破壊検査，工業計測，医用画像診断などの様々な計測・センシング応用，②洗浄，微粒子・懸濁液操作，化学反応促進，各種加工，接合，医用治療利用などのエネルギー応用，③水晶振動子や通信用フィルタ，変調器などのデバイス応用です．更にこれらの基礎となる④波動理論・物理音響や圧電材料の研究分野があります．

超音波研究会では，このような多岐にわたるテーマについて，年に 9 回の研究会を開催し活発な議論を行っています．超音波研究会は最も古い研究会の一つであり，1950 年頃の開設以来，電子情報通信学会と日本音響学会の共催により運営されてきています．1945 年の終戦までは水中の軍用のみであった超音波技術を，戦後の工業の復興や，その後の自動車産業や半導体・ディスプレイ産業の興隆を支える基盤技術として育てたのは超音波研究会であるといっても過言ではありません．例えば，日本の腕時計の信頼性が高まったのは超音波洗浄の利用のためといわれていますし，写真フィルムの質の向上には超音波処理が役立ちました．今日でも，MHz 超音波による高性能洗浄は半導体産業には不可欠な技術ですし，自動車の製造ラインでは多くの超音波技術が使われています．一方，血流をリアルタイム動画で描出する超音波ドップラー装置は循環器の診断に不可欠ですが，日本の大学と企業の努力により生み出された技術です．水晶振動子やフィルタ素子はスマートフォンをはじめとする通信機器に必ず搭載されており，今でも我が国の強みが発揮されている分野です．最近の超音波研究会では，バイオ・生命系へ超音波を応用する研究発表が増えており，新たな応用が広がりつつあるのを感じます．

このような広範な分野の議論を行うために，研究会では毎回テーマを設け，日本超音波医学会，日本非破壊検査協会をはじめ，テーマに対応する様々な団体と共催するようにしています．これにより異分野の研究者が出会う機会としても貴重な研究会になっていると自負しています．関連学会でも超音波分野の研究成果の発表が行われていますが，超音波研究会では 1 件当たり 25 分の発表・質疑時間を確保し，更に追加のフリーディスカッション時間を設けるなど，十分な意見交換，議論ができるのが魅力です．また，若手育成のために「学生研究奨励賞」のしくみを活用しています．立ち上げたばかりの荒削りな研究から応用段階の内容まで，いろいろなバックグラウンドの方々にぜひ当研究会で発表頂ければと思います．

（超音波研究会 Web サイト：https://www.ieice.org/~us/）

中村健太郎（正員：シニア会員）

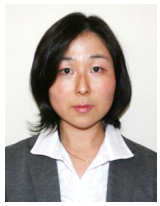
1992 東工大大学院博士課程修了．博士（工学）．現在，東京工業大学科学技術創成研究院教授．超音波の計測応用・パワー応用，光と超音波の相互作用に基づくセンシングの研究に従事．IEEE，応用物理学会，日本音響学会ほか各会員．電子情報通信学会論文賞，日本音響学会佐藤論文賞など受賞．

■ VLSI 設計技術研究会（VLD）

VLSI 設計技術研究会（VLD）では，LSI 設計のための方法論として，システムレベル設計からアナログ回路合成，レイアウト設計に至る各種設計自動化手法及び EDA（Electronic Design Automation）ツールを支えるアルゴリズムまで広範囲にわたるテーマを対象に議論しております．大規模化・複雑化や性能・消費電力・信頼性の問題に関連した研究のみならず，ポストムーア時代における，Artificial Intelligence（AI），Internet of Things（IoT），量子計算機などに関連した設計事例・設計技術・アルゴリズムに関連した研究も発表されております．LSI 設計技術に限らず，多くのシステムエンジニアの方に興味をもって頂ける発表が揃っております．VLSI 設計技術研究会ではほかの研究会との共催など，年 4 回の研究会を開催しており，多数の一般講演と充実した招待講演などで活発な討論や交流が行われております．アジア・南太平洋地域最大の LSI 設計技術関連国際会議であるアジア南太平洋設計自動化会議（ASP-DAC）の共催や，英文論文誌 A 小特集“VLSI 設計と CAD アルゴリズム（Special Section on VLSI Design and CAD Algorithms）”（例年 3 月号）の企画と編集を行うなど，海外への情報発信と情報交流を活性化しつつ，活動を進めております．これらに加えて，VLD が所属するサブソサイエティ（システムと信号処理サブソサイエティ）の活動として，回路とシステムワークショップの開催や，英文論文誌 A 小特集“回路とシステム（Special Section on Circuits and Systems）”（例年 11 月号）の企画・編集にも積極的に関わっております．

2022 年度の VLSI 設計技術研究会の開催スケジュールは以下のとおりです．

6月（6/16～17）	八戸工大＋オンライン開催「システムと信号処理および一般」（CAS，MSS，SIP 共催）
11月（11/28～30 を予定）	金沢市文化ホール＋オンライン開催「デザインガイア～VLSI 設計の新しい大地～」（DC，ICD，RECONF 共催，IPSJ-SLDM 連催）
1月（日程及び開催地未定）	「FPGA 応用および一般」（RECONF 共催，IPSJ-SLDM 連催）
3月（3/1～4 を予定）	沖縄県青年会館（予定）「システムオンシリコンを支える設計技術，ハードウェアセキュリティ，一般」（HWS 共催）



池田奈美子（正員）
1996 東京工業大学無機材料工学科卒業．1998 同大学大学院無機材料工学専攻修士課程修了．同年，日本電信電話(株)に入社．主に，ネットワークシステムの省電力化技術やトラフィック監視システムの研究開発に従事．2022 から本会 VLSI 設計技術研究専門委員会委員長．

■非線形問題研究会（NLP）

非線形問題（NLP）研究会では，その名のとおり，非線形問題に関する基礎理論から応用研究に至る様々な研究発表が行われています．カオスや分岐現象など古くから行われている非線形現象解析に関する研究は現在でも盛んに行われ，新しい興味深い現象も発見されています．また，近年盛んに行われているニューラルネットワークに関する研究も，非線形の分野では古くから行われており，最近の発表プログラムでもよく見られるキーワードです．特に若い方にとっては「非線形問題」という名称からは想像しにくいかもしれませんが，是非当研究会の発表プログラムをのぞいてみてください．そのほか，非線形の問題は，通信工学，時系列データ解析，生体信号，電子回路，数値解析など，実用に近い分野でも多く存在し，様々なアプローチで研究がなされています．非線形問題の理論的解析は一般に難しいといわれますが，同時にやりがいもありますし，理論だけではなかなか解決できない場合も，実験や計算機の力を借りることで興味深い結果が得られることが少なくありません．このあたりは，若い方が柔軟な思考力や発想力で大いに貢献できる可能性を含んでいるといえます．また，非線形問題は地味な印象をもたれるかもしれませんが，近年，当分野の女性研究者が増えつつあるようにも感じています．これは，当分野の研究者の皆様が多くの興味深い研究成果を発信してこられたおかげだと思います．今後も当分野の若い研究者・女性研究者が増えていくことを期待します．

2022 年度も計 6 回の研究会の開催を予定しております．詳細は Web ページをご参照ください．今後も原則としてハイブリッド開催で準備をしますので，多くの皆様にご発表・ご参加頂ければ幸いです．例年どおり，今年度の発表論文の中から優秀な論文（当研究会発表総数の 5% 程度）に対して NLP 奨励賞を授与いたします．また，今年度から，当研究会で発表された論文に対して，NOLTA ソサイエティ（当研究会の親ソサイエティ）が編集するオンラインジャーナル NOLTA，IEICE への投稿を積極的に働きかける予定です．皆様のご尽力・ご協力により当分野が更に発展することを期待しております．まだ当研究会に参加されたことのない「一見さん」も大歓迎ですので，是非，ご参加ください．当研究会で皆様とお会いできることを楽しみにしています．

常田明夫（正員）
1990 九大・工・情報卒．1995 同大学院博士後期課程修了．博士（工学）．現在，熊本大学大学院先端科学研究部教授．カオス理論に基づいた乱数系列生成と応用に関する研究に従事．電子情報通信学会，電気学会，IEEE 各会員．2022 年度非線形問題研究専門委員会委員長．

■スマートインフォメディアシステム研究会（SIS）

スマートインフォメディアシステム（SIS）研究会は，スマートモバイルシステム，ソフトコンピューティング，知的マルチメディア処理システム，システム実現技術，近距離無線通信応用システムなど横断的な分野に関して理論から実システムのハードウェアを含む開発まで幅広い分野を対象としています．年間の主な活動は，総合大会，ソサイエティ大会と年 4 回の研究会を中心に行っています．

研究会では，他学会との関連研究会との連催を企画することで，広い視野・多様な視点からの意見交換も活発に行っています．6 月研究会は，情報処理学会の「オーディオビジュアル複合情報処理研究会（IPSJ-AVM）」と連催し，6 月 9，10 日に九州工業大学において現地及びオンラインによるハイブリッド開催を致しました．10 月研究会は 10 月 13，14 日に八戸工業大学とオンラインとで映像情報メディア学会の「放送技術研究会（ITE-BCT）」との連催を企画しています．以降の研究会は SIS 研単独開催で 12 月は関西大学，3 月は千葉工業大学でのハイブリッド開催予定となっております．本年度の研究会から対面形式で

も開催できるようになっておりますが，オンラインとの併用のハイブリッド開催は研究会への参加がしやすくなったと思います．

毎回の研究会では，本研究会の特徴の一つである研究専門委員による熱意あふれるチュートリアル講演も展開され，参加者からは大変好評を頂いております．また若手研究優秀賞を設け，35 歳以下の研究者の研究会での優秀な発表に対し表彰を行っています．多くの学生さんや若手研究者の方々の発表を期待しております．

SIS 研究専門委員会主催の大きな行事として，国際ワークショップ SISA（International Workshop on Smart Info-media Systems in Asia）を毎年開催しています．本ワークショップは大学院生を含めた若手研究者に国際会議の場を体験してもらい，他国の方々と積極的に交流頂くことを主眼に置いたワークショップです．そのため，学生発表者を対象として学生論文賞を設けております．2022 年は 9 月 15 日（木）～16 日（金）の期間，オンラインにて開催致しました．研究会をはじめ関連行事の詳しくは SIS 研究会のホームページ（https://www.ieice-sis.org/）を御参照下さい．

また，本研究専門委員会が目的とする「高度マルチメディアシステム」「柔軟性処理システム（次世代情報処理システム）」について，現状ではその議論の場が少ないことと，内容的には電子情報通信学会の四つのソサイエティを横断しているので，ソサイエティ横断型で，かつ，ほかの学会とも緩やかな研究連携を図りながら，新しい情報交換・研究討論の場を提供したいとも考えております．投稿先を迷われるようなことがございましたら，是非御発表を検討頂ければと思います．皆様の SIS 研究会の各行事への御参加を心待ちにしております．

木村誠聡（正員：シニア会員）
1985 日本大学工学部卒．博士（工学）（武蔵工業大学）．1985 から 2007 まで日本 IBM に勤務．現在，神奈川工科大学情報学部教授．主に，ディジタル画像の雑音除去・推定に関する研究に従事．電気学会，応用物理学会各会員．2022 から本会スマートインフォメディアシステム（SIS）研究専門委員会委員長．

■イメージ・メディア・クオリティ研究専門委員会（IMQ）

COVID-19 の影響が今なお続いておりますが，日常生活の一部として捉え，社会活動や経済活動との共存を重要視する考え方が主流になりつつあります．本研究会においても，今年度 5 月には東京工科大学にて，7 月には札幌市立大学にてヒューマン情報処理研究会（HIP）とともに研究会を開催しました．発表は表示システムや画質関連の話題はもとより，医療画像・動画検索・画像認識・超解像・疲労推定など多岐にわたり，久しぶりに対面会議での議論を行い，リアルコミュニケーションの重要さを再認識しました．また，オンライン開催ではありましたが 2022 年 3 月には第 11 回イメージメディアクオリティとその応用国際ワークショップ（IMQA2022）を開催し，内外の研究者との議論を行いました．8 セッション 20 件の小規模プログラムでしたが，イメージメディア関連の発表に加え，招待講演では歩容動画像からの人属性推定や視覚・触覚に関する年齢効果についてなどの興味深い話題もあり，活発な議論がなされました．

イメージ・メディア・クオリティ（IMQ）研究専門委員会は，発足以来 2022 年で 19 年めを迎えます．様々なメディアの品質を分野横断して議論する学術的な場として，画像品質の評価方法，画質改善の技法，撮像から伝達・表示に至るまでの技術，観察者の生理学・心理学的特性などを対象に，大学のみならず企業の方にも参加頂き，幅広い分野の研究者が集まり議論を重ねています．「こんな視点があるのか」といった新しい気付きを楽しめる研究会です．毎年約 4 回のペースで首都圏・他の地域にて研究会を開催しており，今年度はあと 10 月・12 月と，3 月にはメディアエクスペリエンス・バーチャル環境基礎研究会（MVE），画像工学研究会（IE），コミュニケーションクオリティ研究会（CQ）とともに研究会を予定しています．メディアとその周辺技術について幅広く議論を行いたい方は，IMQ 研究会に是非ご参加下さい．

IMQ 研究会　https://www.ieice.org/~imq/

魚森謙也（正員）
1985 岡山大学大学院工学研究科修了．同年，松下電器産業(株)（現パナソニック(株)）に入社．立体視機構・画像処理の研究及びカメラシステム開発に従事．2018 より大阪大学先導的学際研究機構・データビリティフロンティア機構特任教授．マルチモーダル行動センシング・日常生活情報データベースの研究に従事．博士（工学）．

■応用音響研究会（EA）

応用音響研究会（EA）では，スピーカによる音の再生に関わる研究だけでなく，音の収録，音の信号処理といった，音を中心とした関連分野を幅広く包含した研究を対象として活動しています．具体的には，マイクロホンやスピーカ，AD 変換器などの入出力デバイス，音源の位置推定，複数音源の分離，雑音や残響の低減，符号化などの信号処理，アクティブノイズ制御（ANC）や波面合成などによる音場の制御，また近年では深層学習を利用した音響イベント認識の発表も増え音響に関する様々なトピックを取り扱っています．EA 研究会は年 6〜7 回，全国各地の大学や研究機関でこれまで開催しておりましたが，2021 年度はオンライン開催を 3 回（7 月，8 月，11 月），熊本での現地開催を 1 回（12 月），沖縄での現地とオンラインのハイブリッド開催を 1 回（3 月）行っております．熊本現地開催では新型コロナウイルスの感染対策を徹底し，各ポスター発表の間に透明なアクリル板を設置し発表者間の距離を確保して，安心して発表できる環境を用意しています．また，ハイブリッド開催では，現地のメイン会場のオーラル発表をオンラインでも同時に配信するとともに，ポスター発表では現地による対面発表に加えて gather.town を利用したオンライン発表も併用することで，参加方法にかかわらず全発表を聴講できる新しい取り組みも行っています．これにより，通年で 117 件の発表があり，参加者も約 700 名と大変盛況な研究会を開催することができました．更に，信号処理，超音波，音声，聴覚，音楽音響といった様々な研究会との共催や併催も活発になっています．2022 年度は 6 回の開催を予定しており，5 月は新型コロナウイルスの影響によらず気軽に参加頂けるオンライン開催を前提とした新しい発表の場を新設いたしました．また，オンラインだけでなく新型コロナウイルスの状況をみながら現地での開催若しくはハイブリッドでの開催を検討していきたいと考えています．今後の開催予定としては，11 月に北陸，12 月に中国・九州での現地開催に向けて検討を始めています．また，例年 3 月は信号処理研究会，音声研究会の合同研究会を離島で開催しており，昨年度のハイブリッド開催に続き今年度も離島で開催を実現したいと思っています．また毎回音響分野で活躍している研究者の招待講演も企画していますので，研究の発表及び聴講にぜひご参加頂ければと思います．下記のホームページに研究会に関する最新の情報を掲載しております．

https://ken.ieice.org/ken/program/index.php?tgid=EA&lang=I
http://asj-eacom.acoustics.jp/

加古達也（正員）
2009 名大・工・電情卒．2011 同大学院博士課程前期課程修了．同年日本電信電話（株）入社．2015 東日本電信電話（株）を経て現在 NTT コンピュータ＆データサイエンス研究所主任研究員．主に，マイクアレーなど音響信号処理技術の研究に従事．2020 応用音響研究会幹事，2022 同研究会副委員長．電子情報通信学会，日本音響学会，IEEE など各会員．

国際会議開催報告

IEEE International Symposium on Information Theory

(ISIT 2022, https://www.isit2022.org/)

Aalto University, Espoo, Finland

2022年6月26日〜7月1日

2022年6月26日から7月1日にかけて，フィンランドのアアルト大学にて2022 IEEE International Symposium on Information Theory（ISIT2022）が開催されました．ISITはIEEE Information Societyが主催する，情報理論に関する最大の国際会議です．今回の開催は，コロナ禍において初，2019年以来2年ぶりの現地開催でした．そればかりでなく，2022年2月に始まったロシアのウクライナ侵攻の影響で世界中が混乱に包まれる中での開催でした．私の乗った飛行機もロシアを東へ大きく迂回しアラスカとの国境を抜け，北極海からフィンランドへと向かっていました．

初日は6件のチュートリアル講演が開催され，2日目以降は毎朝1件ずつ計4件のプレナリー講演と，シャノンレクチャーが行われました．プレナリー講演，シャノンレクチャーは，大学名の由来である建築家アルヴァ・アアルトが設計した講堂（図1，2）で行われました．これらの講演で特に私の印象に残っているのは，情報理論と機械学習について述べた以下の講演です．

- Yonina Eldar and Nir Shlezinger, Model-based Deep Learning
- Yonina Eldar, Communication and Sensing : From Compressed Sampling to Model-based Deep Learning
- Michael Jordan, On Dynamics-Informed Blending of Machine Learning and Game Theory

これらの講演が印象深かったのは，私が最近機械学習の研究を行っているからでもありますが，講演者の研究グループの勢いを感じずにはいられなかったからです．海外の大研究室が優秀なポスドクでチームを作って研究を進めるペースに対抗するにはどうすべきか考えさせられました．仮に日本の小さな研究室が先に着想を得ていた研究でも，後発の大研究室に規模の面で追い越されてしまうケースもあり得るでしょう．このような状況において，個人としてどのように振る舞うべきか，また日本の科学技術研究業界が，あるいはその一構成員である私自身がどのように振る舞うべきかという戦略をもたなければならないと思いました．

各プレナリー講演の後は，一般セッションが行われました．合計566件（会議録に収録されている発表件数による調べ）が発表されたようです．博士課程在籍時に専門としていた符号理論のセッションを中心に聴講しました．私が特に研究していたLDPC符号のセッションは当時からすると大幅に数を減らし，二つのみの開催でした．寂しくもありますが，それだけ分野として成熟してきたということかもしれません．符号理論の応用としてはCoded ComputationやPrivate Information Retrievalなどへの代数的符号の応用が目立っているように感じました．また，全体としては機械学習や学習理論に関連するセッションも多かったと思います．発表の形式については，やむを得ない事情でビデオ形式で行われた発表も一部ありましたが，どうしても聴衆の聴く気が起きにくくなってしまうようでした．自分の研究を広めていくためには，なるべく現地に赴くべきなのだと思います．

開催国であるフィンランドは，自然が豊かで人の温かさを感じる美しい国でした．アアルト大学の周りは緑の木々と海

図1　建築家アルヴァ・アアルトによって設計された講堂

図2　講堂内部．プレナリー講演とシャノンレクチャーが行われた

図３　フィンランドの国魚，ヨーロピアンパーチ

に囲まれ，首都ヘルシンキにも綺麗に整備された緑豊かな公園があり，森と街が一緒にいるようでした．海沿いで開催される学会ではいつも釣竿を忍ばせている私ですが，今回も学会前に釣り糸を垂らすと，ヨーロピアンパーチ（図３）に出会うことができました．フィンランドの国魚だそうです．

現地開催の国際学会への参加は久しぶりでしたが，やはり研究意欲が触発されました．もしかすると研究発表そのものよりも，現地における余白の時間や雰囲気がそうさせるのかもしれません．海外の大研究室の勢いに負けず，来年台湾で開催される ISIT でも発表を行うのだという決意が，またしてもロシアを大きく迂回し日本へと向かう飛行機の中でゆっくりと固まっていくのを感じました．

中原悠太（正員：一般会員）

平 26 早大・基幹理工・応用数理卒．平 31 同大学院数学応用数理専攻博士後期課程了．博士（工学）．同年，同大データ科学センター講師着任．以来，情報理論，符号理論，可逆画像圧縮，データ科学の研究に従事．現在に至る．著書（共著）『データ科学入門 I：データに基づく意思決定の基礎』．

国際会議開催報告

The 37th International Technical Conference on Circuits/Systems, Computers and Communications

（ITC-CSCC 2022，回路とシステム／コンピュータ及び通信に関する国際会議）

Duangjitt Resort & Spa, Phuket, Thailand（オンラインとのハイブリッド開催）

2022 年 7 月 5 日～8 日，https://www.itc-cscc2022.org/

The 37th International Technical Conference on Circuits/Systems, Computers and Communications（ITC-CSCC 2022）が 2022 年 7 月 5 日～8 日の 4 日間，タイの代表的なリゾート地であるプーケットの Duangjitt Resort & Spa を会場とし，オンラインを併用したハイブリッド形式で開催されました．ITC-CSCC は毎年 6 月若しくは 7 月に，韓国の IEIE，タイの ECTI 及び IEICE ESS が共同開催している，回路とシステム，コンピュータ及び通信に関する恒例の国際会議で，今回で第 37 回めの開催となりました．

ITC-CSCC 2022 では，10 か国から計 309 件の論文投稿があり，査読を経て 257 件の論文が採択されました．

採択論文の国別の内訳はタイ 110 件，韓国 76 件，日本 51 件，インドネシア 5 件，フィリピン 4 件，パキスタンとミャンマーそれぞれ 3 件，ベトナムとシンガポールそれぞれ 2 件，オーストラリア 1 件です．会議のプログラムは 3 件のプレナリ講演，3 件のチュートリアル講演，19 の現地でのオンサイトセッション（図 1）及び Zoom による 33 のオンラインセッションから構成されていました．また，参加登録者数は 299 で，タイ国内の参加登録者が 106 名，海外からの参加登録者が 193 名でした．

初日の 7 月 5 日には，セッション終了後の夕刻から，ホテルのプールサイドで Welcome Reception が開催されました．7 月 6 日には，最初のセッションの終了後に Opening Ceremony が行われました（図 2）．まず，General Chair である Honorary Prof. Piya Kovintavewat（Nakhon Pathom Rajabhat University, Thailand）からオープニングスピーチ（図 3）があり，続いて，General Co-Chair である Prof. Jong-Ok Kim（Korea University, Korea）のスピーチ，Technical Program Committee Co-Chair である小職のオンラインスピーチがありました．そして，Opening Ceremony に続いて，以下の 3 件のプレナリ講演がありました．

1. “Electric Vehicle Charging Station Incorporating with an Energy Management and Demand Response Technique,” Prof. Surin Khomfoi（King Mongkut’s Institute of Technology Ladkrabang, Thailand）
2. “Order Learning and Its Applications to Computer Vision,” Prof. Chang-Su Kim（Korea University, Korea）
3. “Low Latency and Lightweight Video Computing

図 2　Opening Ceremony での集合写真

図 1　現地でのオンサイトセッション会場

図 3　Honorary Prof. Piya Kovintavewat によるオープニングスピーチ

in Edge Cloud Networks,” Prof. Takayuki Nakachi（University of the Ryukyus, Japan）

7 月 7 日にはセッションと並行して，以下の 3 件のチュートリアル講演がありました．

1. “On Optimizing Resource Allocation for MIMO-NOMA Downlink,” Prof. Wiroonsak Santipach（Kasetsart University, Thailand）
2. “Neural Network Design based on Algorithm Unrolling and Its Applications,” Prof. Daeyoung Park（Inha University, Korea）
3. “When Deep Unfolding Meets Control Engineering,” Prof. Masaki Ogura（Osaka University, Japan）

夕刻からは Banquet があり，タイの伝統舞踊が披露されるなど，会場は大いに盛り上がったそうです．そして最後の 7 月 8 日のセッションで ITC-CSCC 2022 は幕を閉じました．また会議期間中には，参加者が楽しめるイベントとして Photo Contest が，大学院生の参加者同士が交流できる場として Seminar on International Friend Networking がそれぞれ開催されました．

コロナ禍が続き，昨年の第 36 回に続いてのハイブリッド形式での開催となりましたが，発表は事前に録画した動画の再生ではなく，現地若しくは Zoom 上にてリアルタイムで行われ，各セッションにおいて活発な議論が交わされました．ITC-CSCC 2022 を成功に導いたタイ側の運営関係者の皆様に感謝いたします．

次回の第 38 回は，2023 年 6 月 25 日～27 日に韓国の済州島で開催される予定です．

高井重昌（正員：一般会員）
1989 神戸大・工・システム卒，1991 同大大学院工学研究科システム工学専攻修士課程了．1992 大阪大学工学部助手，1998 和歌山大学システム工学部講師，1999 同助教授，2004 京都工芸繊維大学工芸学部助教授，2007 同大大学院工芸科学研究科准教授，2009 大阪大学大学院工学研究科教授．ITC-CSCC 2022 Technical Program Committee Co-Chair.

受賞者の声

電子情報通信学会に関連する賞を受賞された方を御紹介します.

第 78 回（令和 3 年度）論文賞

令和 3 年度は学会全体で 12 編の論文が論文賞を受賞しました．そのうち，基礎・境界ソサイエティでは 3 編の論文が受賞しています．受賞した 3 編の論文の著者にインタビューしました.

仮屋　夏樹（東工大），渡辺　澄夫（東工大）

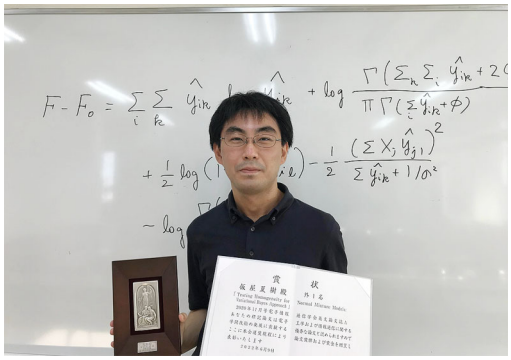
「Testing Homogeneity for Normal Mixture Models : Variational Bayes Approach」[1]

Q. 論文賞を受けられた御感想をお聞かせ下さい.

　このたび歴史ある電子情報通信学会から授賞頂けたことを大変光栄に思います.

　ご連絡を頂いた際は大きな驚きばかりがありましたが，時間が経つにつれ少しずつ喜びと身の引き締まる思いが強まってきています.

　改めて，共著者はじめこれまでご指導頂いた皆様，査読者，学会関係者各位にお礼を申し上げます.



仮屋　夏樹

Q. 論文賞を受けられた御研究について教えて下さい.

　今回私たちが行った研究は，ベイズ統計に関する理論的な研究です.

　問題意識としては，与えられたデータが，単独の情報源から発生したものか，複数の情報源からかを精度良く判別するための手法を考えたい，ということがありました．非常に基本的な設定ながら，特に情報源が似通っていて判別が難しい場合において，従来知られている結果・手段では課題が残されていると感じていました.

　今回私たちは，ベイズ統計の枠組み，特に変分ベイズ法と呼ばれる手法に基づいて，正規分布の混合を対象に理論的な解析を行いました.

　結果，変分ベイズ法で重要になる変分自由エネルギーという量の確率的な挙動が分かり，仮説検定の構築などができるようになりました.

　このアプローチ自体がどうやら過去例がなかったようであるのと，副産物として変分自由エネルギーが示す相転移など理論的に関心がもたれる内容も見つかったので，一連の結果を論文にまとめました.

Q. 現在，御興味をもたれている研究テーマを教えて下さい.

　今回の研究についていえば，適用範囲など拡張の余地が残されていると認識しており，取り組むべき課題だと考えております.

　もう少し広い視点だと，「予測や判別の難しいケースにおいて，分析手法の精度はどう与えられるのか，また手法を理論的にどう改良できるか」という点に関心があります．ベイズ統計は予測や判別の難しいケースで有力な方法の一つで，理論的にも性質が明らかになってきていますが，解明されるべき問題はまだ残されているように思います.

　また，物理学などの自然科学や工学の分野でも近年は判別の精度限界を改良するための理論・実験研究が活発化しており，今回の取り組みの発展として分野をまたぐような取り組みができれば非常に刺激的だと感じます.

　そのほか，今回の研究は純粋な理論研究ですが著者の 1 人（仮屋）は現在企業在籍中であり，応用的なデータ解析にも関心をもっています.

Q. 今後の抱負をお聞かせ下さい.

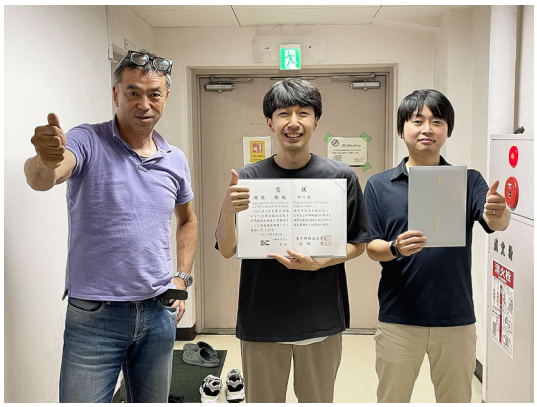
　今回の受賞を励みに，非力ながらも今後も分野の発展，ひいては社会に少しでも貢献できるような取り組みを続けていければと考えております.

明間　陸（東工大），山岸　昌夫（東工大），山田　功（東工大）

「Approximate Simultaneous Diagonalization of Matrices via Structured Low-Rank Approximation」[2]

Q. 論文賞を受けられた御感想をお聞かせ下さい.

このたびは名誉ある賞を頂いたこと，大変光栄に思っています．本論文を高く評価してくださった皆様に深く感謝申し上げます.



写真左から山田，明間，山岸

Q. 論文賞を受けられた御研究について教えて下さい.

データサイエンスの中心的な課題として，多数のデータを集めて，個々のデータからは見えてこない大局的な情報を抽出することが挙げられます．このような情報抽出を実現するために，数理的な問題として定式化するアプローチがとられています．様々な定式化の中でも，同時対角化（データから直接または何かしらの操作をすることによって得られる複数の行列を，同時に対角行列に相似変換すること）を近似実現する「近似同時対角化問題」は分野横断的に現れる普遍的な問題の一つです．この問題の工学的な応用を想定すると，収集したデータには雑音が混ざっているケースがほとんどであるため，雑音除去機能をもつ近似同時対角化手法が待望されていました.

受賞論文では，雑音除去機能を備えた近似同時対角化アルゴリズム（ATDS 法）を提案しています．ATDS 法は 2 段階構成であり，（ステップ 1）データから得られる行列組を「厳密に同時対角化可能な行列組」で近似し雑音を除去するステップと（ステップ 2）雑音除去後の行列組を同時対角化するステップからなります．ステップ 1 は，「厳密に同時対角化可能な行列組」の数理的な性質を非自明な形で活用することで実現されています．ステップ 2 は，「厳密に同時対角化可能な行列組」の同時対角化が代数的に算出可能である事実を直接活用することで実現されています．特筆すべきこととして，ATDS 法は，既存解法では保証されなかった「データから得られる行列組が厳密に同時対角化可能なとき，適切に同時対角化を行う保証」を達成していることが挙げられます.

Q. 現在，御興味をもたれている研究テーマを教えて下さい.

信号処理工学やデータサイエンスの諸問題を斬新な最適化問題でモデル化し，非自明な数理で解決する方法論が好きで，これを具現化するためのアルゴリズムを構築し，応用する研究に興味をもっています．実は，比較的簡単な問題として一括りにされがちな凸最適化問題の中にも一筋縄では扱えない制約集合や目的関数をもつ例が無尽蔵にあり，ほとんど手つかずの状態になっています．このような例の中に筋のよい鉱脈を発見・開拓・応用することにより，工学の横断的領域に飛躍的な進化をもたらすことができるのではないかと考えています.

Q. 今後の抱負をお聞かせ下さい.

現代のトレンドを追いかけることも重要ですが，どうせなら普遍的価値が感じられる研究にじっくり取り組んでいきたいと思っています.

Q. 読者へのメッセージをどうぞ！

今回の受賞を励みに研究に邁進していきたいと思います．今後ともご指導ご鞭撻のほどよろしくお願いいたします.

Ramy TAKI ELDIN（Ain Shams University），松井　一（豊田工大）

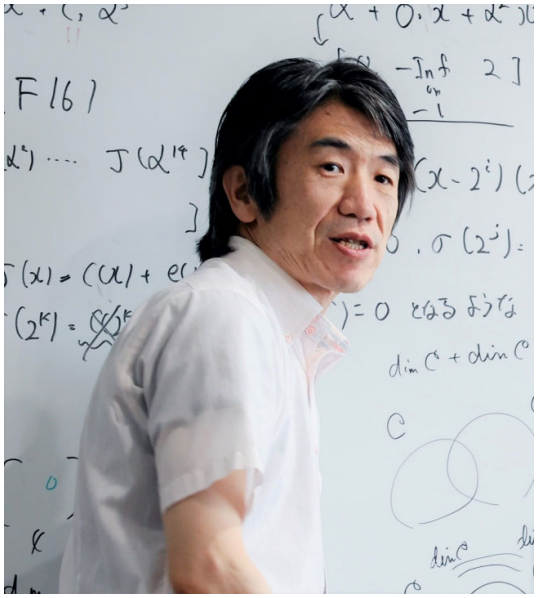
「Linking Reversed and Dual Codes of Quasi-Cyclic Codes」[3]

Q. 論文賞を受けられた御感想をお聞かせ下さい.

とても光栄に感じており，また責任重大であるとも感じております.

共著者，関係する研究室メンバー（山地君，川口君，笠井君，江口君），論文発表の場を提供して頂きました“Special Section on Information Theory and Its Applications”編集者および AE の方々，またコメントをして頂きました査読者の方々に深く感謝いたします.

Ramy TAKI ELDIN



松井　一

Q. 論文賞を受けられた御研究について教えて下さい.

誤り訂正符号のうちで準巡回符号，その中でも特に反転不変符号と呼ばれるものについて研究しました.

反転不変符号は，左右反転した符号語を含むような誤り訂正符号であり，これまではそれほど研究されてこなかったクラスかもしれませんが，最近は DNA 記録の誤り訂正符号である DNA 符号に応用されて注目されています.

この反転不変符号について，準巡回符号がいつ反転不変符号になるかの必要十分条件や，古くから研究されている自己双対符号との関係，またこれらの結果を応用して誤り訂正能力の高い反転不変符号を計算機探索で多数見つけることなどを行いました.

Q. 現在，御興味をもたれている研究テーマを教えて下さい.

情報理論・符号理論とその隣接分野で幾つか新しい研究成果を出そうと奮闘中です.

Q. 今後の抱負をお聞かせ下さい.

この受賞を励みとし，「山椒は小粒でもぴりりと辛い」研究者となれるよう努力します.

Q. 読者へのメッセージをどうぞ！

学会などで（オンラインを含め）お会いしお話ができることを楽しみにしております.

（1） Natsuki Kariya and Sumio Watanabe, “Testing Homogeneity for Normal Mixture Models : Variational Bayes Approach,” IEICE Trans. Fundamentals, vol. E103-A, no. 11 Nov. 2020.
（2） Riku Akema, Masao Yamagishi, and Isao Yamada, “Approximate Simultaneous Diagonalization of Matrices via Structured Low-Rank Approximation,” IEICE Trans. Fundamentals, vol. E104-A, no. 4 April 2021.
（3） Ramy Taki ElDin and Hajime Matsui, “Linking Reversed and Dual Codes of Quasi-Cyclic Codes,” IEICE Trans. Fundamentals, vol. E105-A, no. 3 March 2022.

開催案内

2022 International Symposium on Nonlinear Theory and its Applications (NOLTA'22)
Online, December 12-15, 2022

General Secretary　薄　良彦（京都大学）

2022 年 12 月 12〜15 日に NOLTA'22（https://nolta2022.org）が開催されます。当初は Opatija, Croatia での開催を予定しておりましたが，新型コロナウィルスなどの影響により同日程でオンライン開催となりました。上のホームページの背景になっているような風光明媚な環境で，2 年ぶりの NOLTA を現地開催するために，Symposium Committee 一同準備を進めて参りました。現地開催の中止に伴い参加者の皆様と対面でお会いできないことは大変残念ではありますが，オンライン開催の良さを生かした NOLTA になるように，論文の査読やオンライン会議のプラットフォームの準備などを現在進めております。国内外より 150 件以上の投稿があり，Committee 一同心より御礼申し上げます。参加登録やプログラムなどは整い次第，上のホームページと twitter（@nolta2022）でアナウンス致しますので，皆様のご参加を心からお待ち申し上げます。

Plenary Speakers of NOLTA'22
Professor Predrag Cvitanovic (Georgia Institute of Technology, USA)
Professor Johan Akerman (University of Gothenburg, Sweden)
Professor Takashi Hikihara (Kyoto University, Japan)

論文募集

2023 年暗号と情報セキュリティシンポジウム（SCIS2023）

2023 Symposium on Cryptography and Information Security

開催期間：2023 年 1 月 24 日（火）～1 月 27 日（金）
会場：リーガロイヤル小倉（福岡県小倉市）
開催形態：対面（ハイブリッドまたはオンライン開催に移行する可能性あり）
Web ページ：https://www.iwsec.org/scis/2023/

1. 概要

暗号と情報セキュリティシンポジウムは，暗号と情報セキュリティ技術に関する最新の研究成果の発表および情報交換の場として，1984 年以来毎年開催されているセキュリティ分野における日本最大規模のシンポジウムです．第 40 回となる SCIS2023 は，福岡県小倉市で開催します．

2. 募集テーマ

暗号および情報セキュリティに関する分野，特に新しく発展しつつある研究分野．募集テーマを以下に挙げますが，これらに限らずセキュリティ技術に関わる論文を広く募集します（査読による絞込みはありません）．

［募集テーマ例］

暗号理論，情報理論的安全性，数論応用，公開鍵暗号，ID ベース暗号／属性ベース暗号／関数暗号，楕円・超楕円曲線暗号，格子暗号，秘密計算，高機能暗号，多機能署名，共通鍵暗号，ブロック暗号，ストリーム暗号，ハッシュ関数，乱数，署名，認証，鍵管理，暗号プロトコル，フォーマルメソッド，耐量子暗号，量子暗号・量子計算，ハードウェアセキュリティ，PUF，サイドチャネル攻撃，ネットワークセキュリティ，ネットワーク攻撃検知・対策，マルウェア対策，ウェブセキュリティ，クラウドセキュリティ，モバイルセキュリティ，組み込みセキュリティ，制御システムセキュリティ，自動車セキュリティ，フィンテック，ブロックチェーン，電子透かし，コンテンツ保護，ソフトウェア保護，プライバシー保護，生体認証・バイオメトリクス，教育・心理学，セキュリティ評価・モデル，IoT セキュリティ，AI セキュリティ

※原稿に関する著作権は電子情報通信学会に帰属します．

3. 論文賞

● イノベーション論文賞

情報セキュリティ（ISEC）研究専門委員会では暗号と情報セキュリティシンポジウム（SCIS）のさらなる発展と活性化を目的として，「新しい研究・技術開発」の奨励を行うイノベーション論文賞が SCIS2012 より設けられました．その奨励対象は理論的新規な論文だけでなく ICT での問題提起や新しい研究分野の提案も含まれます．イノベーション論文賞の対象は全講演論文となります．多くの技術者・研究者による積極的なご発表をお願いいたします．

● SCIS 論文賞

情報セキュリティ（ISEC）研究専門委員会では暗号と情報セキュリティシンポジウム（SCIS）の発展と活性化，並びに，暗号と情報セキュリティ分野で活躍する若手の奨励を目的として，1993 年より SCIS 論文賞を設定しています．SCIS 論文賞の対象は，SCIS 論文賞を未受賞の講演者で，主に学部在学中もしくは学部卒業後 10 年以内の講演者による論文となります．論文賞の対象として取り扱われるかどうか不明な方は事務局までお問い合わせください．

4. 開催場所（予定）

リーガロイヤル小倉　〒802-0001 福岡県北九州市小倉北区浅野 2 丁目 14-2

5. 主なスケジュール（予定）

2022 年

・11 月 10 日（木）参加申込・発表申込受付開始
・11 月 30 日（水）発表申込〆切
・12 月 7 日（水）発表題目・概要〆切
・12 月 14 日（水）原稿提出〆切
・12 月末プログラム公開

2023 年

・1 月 6 日（金）事前参加申込〆切
・1 月 19 日（木）論文集公開開始
・1 月 24 日（火）～27 日（金）SCIS 2023 開催

概要は原稿提出の有無に関わらずプログラムに掲載されます．

6. 申込み

参加・発表申し込みを，11 月上旬より本シンポジウムの Web ページで受け付ける予定です．投稿原稿は「概要：日本語 500 文字以内，英語 1300 文字以内」および「論文：8 ページ以内（A4 版，1.5 MB 制限）」をご準備ください．

7. 諸注意

本シンポジウムに関する最新の情報は，Web ページをご参照ください．また，参加・発表申込み及び原稿提出の各締切を厳守してください．締切以降の提出は一切受け付けられません．

［主催］

電子情報通信学会 情報セキュリティ研究専門委員会（ISEC 研）

［協催］

電子情報通信学会 情報通信システムセキュリティ研究専門委員会（ICSS 研）
電子情報通信学会 バイオメトリクス　研究専門委員会（BioX 研）
電子情報通信学会 ハードウェアセキュリティ研究専門委員会（HWS 研）
情報処理学会 コンピュータセキュリティ研究会（CSEC 研）

論文募集

SBRA 2022

第 12 回

バイオメトリクスと認識・認証シンポジウム

富山国際会議場

https://www.ieice.org/~biox/sbra2022/

2022 11.15 TUE. – 16 Wed.

スケジュール
- 発表申込締切 10 月中旬
- 原稿投稿締切 10 月下旬
- 参加登録締切 11 月上旬

生体認証として知られる「バイオメトリクス」は、センサ、アルゴリズムに関する基礎技術から、システム構築、サービス提供のような実利用まで、多岐にわたる認識・認証技術として発展してきました。すでに、指紋認証や顔認証は安全安心な社会を実現するためのインフラストラクチャーとして実用化されています。一方、プライバシーや個人情報といったクリティカルな側面も併せ持つ非常に複雑なシステムでもあります。最近では、多様化したインターネットサービスの普及や DX の推進に伴い、Trusted Web の実現に向けた取り組みも進められており、バイオメトリクス技術の新たな展開も期待されています。

このような背景をもとに、「バイオメトリクスと認識・認証シンポジウム（SBRA）」は、バイオメトリクスや認識・認証に関する様々な研究分野の研究者や開発者、利用者が一堂に会し、交流，情報交換，相互啓発を広げていくための場として開催されてきました。SBRA2020 からの 2 年間、新型コロナウイルス感染症の感染拡大に伴い、オンラインでの開催を余儀なくされました。SBRA2022 では、ニューノーマルにおけるシンポジウムの新たな開催方法を模索しながら対面による現地開催を目指し、SBRA2020 から計画していた地方開催の試みも継承して準備を進めています。新たな SBRA に多くの皆様からご発表・ご参加いただけることを実行委員一同、お待ちしております。

SBRA2022 実行委員長　高野博史（富山県立大学）

基礎・境界ソサイエティ運営委員会

会長	鎌部　浩　(岐阜大学)
次期会長	梶川　嘉延　(関西大学)
ソサイエティ編集長	田口　亮　(東京都市大学)
副会長（事業担当）	野村　亮　(早稲田大学)
副会長（システムと信号処理）	高井　重昌　(大阪大学)
副会長（音響・超音波）	古家　賢一　(大分大学)
副会長（情報理論とその応用）	桑門　秀典　(関西大学)
庶務幹事	太田　隆博　(専修大学)
庶務幹事	西浦　敬信　(立命館大学)
会計幹事	廣友　雅徳　(佐賀大学)
会計幹事	古賀　崇了　(近畿大学)
事業担当幹事	葛岡　成晃　(和歌山大学)
事業担当幹事	新田　高庸　(会津大学)
大会担当幹事	松井　一　(豊田工業大学)
大会担当幹事	高野　知佐　(広島市立大学)
電子広報担当幹事	森島　佑　(東北学院大学)
電子広報担当幹事	荒井伸太郎　(岡山理科大学)
英文論文誌編集委員長	奥田　正浩　(同志社大学)
英文論文誌編集幹事	川村　新　(京都産業大学)
和文論文誌編集委員長	岩本　貢　(電気通信大学)
和文論文誌編集幹事	渡邉　洋平　(電気通信大学)
ソサイエティ誌編集委員長	関屋　大雄　(千葉大学)
ソサイエティ誌担当幹事	八巻　俊輔　(東北工業大学)
ソサイエティ誌担当幹事	小林　孝一　(北海道大学)
特別委員（国外活性化担当）	尾知　博　(九州工業大学)
特別委員（国際会議コンテンツ担当）	小平　行秀　(会津大学)
編集特別幹事（オブザーバ）	澤畠　康仁　(日本放送協会)
出版委員会委員（オブザーバ）	吉川　英機　(東北学院大学)
研究会連絡会幹事（オブザーバ）	髙島　康裕　(北九州市立大学)
ハンドブック／知識ベース委員（オブザーバ）	笹岡　直人　(鳥取大学)
男女共同参画委員会（オブザーバ）	野崎　隆之　(山口大学)
プラチナクラブ運営委員会（オブザーバ）	金子　美博　(岐阜大学)
事務局	水橋　慶，永井　宏　(電子情報通信学会)

基礎・境界ソサイエティサブソ・研専会議

副会長（事業担当）	野村　亮　(早稲田大学)
副会長（システムと信号処理）	高井　重昌　(大阪大学)
副会長（音響・超音波）	古家　賢一　(大分大学)
副会長（情報理論とその応用）	桑門　秀典　(関西大学)
事業担当幹事	葛岡　成晃　(和歌山大学)
事業担当幹事	新田　高庸　(会津大学)
回路とシステム（CAS）	前田　義信　(新潟大学)
情報理論（IT）	小嶋　徹也　(東京工業高等専門学校)
信頼性（R）	土肥　正　(広島大学)
超音波（US）	中村健太郎　(東京工業大学)
応用音響（EA）	古家　賢一　(大分大学)
VLSI 設計技術（VLD）	池田奈美子　(日本電信電話)
情報セキュリティ（ISEC）	國廣　昇　(筑波大学)
信号処理（SIP）	田中　聡久　(東京農工大学)
ワイドバンドシステム（WBS）	庄納　崇　(インテル)
システム数理と応用（MSS）	尾崎　敦夫　(大阪工業大学)
思考と言語（TL）	森下　美和　(神戸学院大学)
技術と社会・倫理（SITE）	大谷　卓史　(吉備国際大学)
ITS（高度交通システム）（ITS）	藤井　雅弘　(宇都宮大学)
スマートインフォメディアシステム（SIS）	木村　誠聡　(神奈川工科大学)
イメージメディアクオリティ（IMQ）	魚森　謙也　(大阪大学)
高信頼制御通信（RCC）	東　俊一　(名古屋大学)
バイオメトリクス（BioX）	今岡　仁　(日本電気)
安全・安心な生活と ICT（ICTSSL）	和田　友孝　(関西大学)
ハードウェアセキュリティ（HWS）	永田　真　(神戸大学)
光輝会（SSA）（オブザーバ）	春日　正男　(作新学院大学)
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）	吉田　寛　(日本電信電話)
会長（オブザーバ）	鎌部　浩　(岐阜大学)
次期会長（オブザーバ）	梶川　嘉延　(関西大学)
庶務幹事（オブザーバ）	太田　隆博　(専修大学)
庶務幹事（オブザーバ）	西浦　敬信　(立命館大学)
研究会連絡会幹事（オブザーバ）	髙島　康裕　(北九州市立大学)
事務局	水橋　慶，永井　宏　(電子情報通信学会)

NOLTA ソサイエティ運営委員会

ソサイエティ会長	潮　俊光　(大阪大学)
ソサイエティ次期会長	長谷川幹雄　(東京理科大学)
庶務幹事（22N ソ大会実行委員長）	松原　崇　(大阪大学)
庶務幹事（CCS 副委員長）	中野　秀洋　(東京都市大学)
会計幹事	黒川　弘章　(東京工科大学)
電子広報担当幹事（Webinar 企画 WG）	松浦　隆文　(日本工業大学)
大会担当幹事	高野　知佐　(広島市立大学)
運営委員	堀尾　喜彦　(東北大学)
運営委員	小西　啓治　(大阪公立大学)
運営委員	神野　健哉　(東京都市大学)
運営委員	常田　明夫　(熊本大学)
運営委員	鳥飼　弘幸　(法政大学)
運営委員	吉岡大三郎　(崇城大学)
運営委員	伊藤　大輔　(岐阜大学)
運営委員	赤井　恵　(北海道大学／大阪大学)
運営委員	会田　雅樹　(東京都立大学)
運営委員	眞田　耕輔　(三重大学)
運営委員	安達　雅春　(東京電機大学)
運営委員	加藤　秀行　(大分大学)
運営委員	坪根　正　(長岡技術科学大学)
事務局	水橋　慶，永井　宏　(電子情報通信学会)

編集後記

甲子園の優勝旗が白河の関を越え，夕方には秋の虫の鳴き声が聞こえてくるようになりました．今年の夏もあっという間に終わろうとしています．今号にて掲載されている 3 編の「技術の原点」は昨年度フェローの称号を受賞された方に依頼し，ご執筆頂いたものです．著者の皆様に改めて御礼申し上げます．これらの論説から，基礎・境界ソサイエティ，NOLTA ソサイエティの学術的奥深さ，分野の広がりを改めて感じました．今後も，幅広く充実した誌面を目指しますので，ぜひご期待ください．（関屋大雄）

新型コロナウイルスが依然として猛威を振るっておりますが，この厳しい状況下でも今号も無事発行することができました．今号は 3 件の「技術の原点」をはじめとして，読み応えのある論説及び記事が盛りたくさんの号となりました．ご執筆者の皆様方および編集委員会・事務局・出版社の皆様方の多大なるご協力に改めて御礼申し上げます．FR 誌が引き続き皆様にご愛顧頂けるよう，積極的な情報発信をして参りたいと思いますので，今後ともよろしくお願い申し上げます．（八巻俊輔）

開催案内，論文募集などのやわらかい記事を担当しました．新型コロナウイルスの影響は続いていますが，対面の研究会が増えています．FR 誌を国際会議や研究会などの広報の場として活用して頂けますと幸いです．今後ともどうぞよろしくお願いいたします．（小林孝一）

今号の「受賞者の声」を担当しました．記事をご執筆頂いた論文賞受賞者の皆様には，改めて御礼申し上げます．本記事をご覧になって論文内容にご興味をおもちになった皆様は，ぜひ受賞論文をご覧ください．今後ともどうぞよろしくお願いいたします．（松田哲直）

今号の「研究会に行こう」の特別編集幹事を担当しました．今夏は 3 年ぶりの行動制限のない夏でした．帰省や旅行に行かれた方も多いのではないでしょうか．研究会の方もオンサイト開催やハイブリッド開催が主流になりつつあるようです．皆様も今回の記事で興味が湧いた研究会に参加されてはいかがでしょうか．最後になりましたが，ご担当頂いた執筆者，編集委員，事務局，出版社の皆様に御礼申し上げます．（新田高庸）

Fundamentals Review へのお問い合わせ

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

Fundamentals Review 第十六巻 第二号

令和四年十月一日発行

発行人	白石　智
発行所	一般社団法人 電子情報通信学会　基礎・境界ソサイエティ 〒 105-0011 東京都港区芝公園 3-5-8（機械振興会館内） 電話 03-3433-6691(代) FAX 03-3433-6659
WEB 化担当	山岡影光
WEB 化担当会社	三美印刷株式会社 東京都荒川区西日暮里 6-28-1