2022年3月10日印刷　2022年3月15日発行（毎月1回15日発行）
ISSN 0447-8053

IPSJ MAGAZINE

情報処理

2022
4
Vol.63 No.4
通巻 685 号

特集　オンライン　社会インフラシステムにおけるサイバーセキュリティ
―レジリエントで持続可能なデジタル経済社会に向けて―

寄　稿　計算機科学を推進した富田悦次君を悼む

巻頭コラム
僕らはテクノロジーとともに身体の補完を超えて拡張してゆく
武藤将胤

教育コーナー：ぺた語義
連　載：5分で分かる!? 有名論文ナナメ読み／オンライン 教科「情報」の入試試験問題って?
情報の授業をしよう！／先生，質問です!／ビブリオ・トーク

電子版もご覧ください

電子版を読む（会員無料）	iPhoneなどで読む（有料）	電子版を購入（有料）	Web公開（無料/有料）
情報学広場	Kindle	Fujisan	note

一般社団法人 情報処理学会
Information Processing Society of Japan

https://www.ipsj.or.jp/dp/submit/tdp0401s.html

情報処理学会トランザクションデジタルプラクティス

特集号論文募集

「コロナ禍後も見据えたオンライン コミュニケーション環境の活用と課題」

〔投稿締切〕2022 年 5月 9日（月）17：00

インターネットによる音声や映像の配信技術を利用したリアルタイム遠隔授業やテレカンファレンスの試みは20年以上前から行われてきている。インターネットの広帯域化とH.323等の国際標準規格に基づくビデオ会議システムの普及やそのHD（ハイビジョン）化により、その活用範囲は徐々に広がってきてはいたが、比較的高価な専用機器と、ファイアウォール（NAT）等の制限のない今日においては一般的とは言えないネットワーク環境が必要であったこと、3地点以上での相互接続が容易でない等の要因から、これまでその活用は非常に限定的であった。

並行して、PC上で動作するソフトウェアベースのビデオ会議システムも開発されてきてはいたが、品質が不安定で汎用性や相互接続性が低く、またサブスクリプションベースのサービスモデルが多かったこともあり、なかなか広く受け入れられない状況が続いていた。近年になって性能向上や機能向上が急速に進み、従来のビデオ会議システムを置き換え得る状況となってきていたところでコロナ禍を迎えたことから、一気に世界的に普及することとなった。

コロナ禍がもたらしたものは、単純なビデオ会議システムの置き換えだけではなく、これまであまりビデオ会議システムの適用が試みられることがなかった実習や実技を伴う授業や、学会等における貴重な情報交換の場である懇親会等におけるコミュニケーションをオンライン化する際の課題についても浮き彫りにした。ビデオ会議システムはあくまでもオンラインコミュニケーション環境を実現する上でのツールの1つであり、効果的なオンラインコミュニケーションを実現する上でどのように活用するかが、その先の本質的な課題である。ビデオ会議システムをとりまく技術自体についても、ネットワーク整備における配慮、教材提示手法、カメラ制御、音響環境整備、仮想空間概念の導入を始めとして、従来のビデオ会議システムを活用する上での知見とは違った観点も要求され、まだまだ多くの課題が残されている。 そこで、本特集では、このようなオンラインコミュニケーション環境に関連する取組みに基づく論文を募集し、さまざまな知見を広く共有することでさらなるオンラインコミュニケーション環境の発展につなげる。

※投稿要領：Web サイトをご覧ください→ https://www.ipsj.or.jp/dp/submit/tdp0401s.html （応募資格は問いません）

※掲 載 号：2023 年 1 月号（Vol.4 No.1）

※特集ゲストエディタ：中村素典（京都大学 学術情報メディアセンター）

※特集号編集委員：編集委員長：吉野松樹（日立製作所）

副編集委員長：細野　繁（東京工科大学）、藤瀬哲朗（三菱総研）

編集委員：青木学聡（名古屋大学）、荒木拓也（日本電気）、西山博泰（日立製作所）、鎌田真由美（日本マイクロソフト）、飯村結香子（NTT）、石井一夫（公立諏訪東京理科大学）、今原修一郎（東芝）、岩倉友哉（富士通）、江谷典子（ANA）、大嶋嘉人（NTT）、鬼塚　真（大阪大学）、上條浩一（東京工科専門職大学）、斎藤彰宏（日本IBM）、坂下　秀（アクタスソフトウェア）、佐藤　聡（筑波大学）、佐藤裕一（富士通）、澤谷由里子（名古屋商科大学大学院）、澤邉知子（日本大学）、立床雅司（三菱電機）、戸田貴久（電気通信大学）、長坂健治（キンドリルジャパン）、西尾直也（日立製作所）、新田　清（ヤフー）、濱崎雅弘（産業技術総合研究所）、平井千秋（日立製作所）、福原知宏（マルティスープ（株））、藤原一毅（国立情報学研究所）、横井直明（日立製作所）

アドバイザ：喜連川優（国立情報学研究所・東京大学）

（論文募集公開時点 (2022 年 2 月)）

4

PREFACE

巻頭コラム

SPECIAL FEATURES

特　集

社会インフラシステムにおけるサイバーセキュリティ ―レジリエントで持続可能なデジタル経済社会に向けて―

お知らせ

特集記事はオンラインのみの掲載となります（本誌には「編集にあたって」「概要」のみ掲載されます）．オンライン記事（電子図書館）の閲覧方法につきましては 213 ページに掲載しておりますのでご確認くださいますようお願いいたします．

《記号の説明》

基 応 専 般 Jr.　■ 基礎 ■ 専門家向け　■ 応用 ■ 一般（非専門家）向け　Jr. ジュニア会員向け

※各記事に指標がついていますのでご参考になさってください

IPSJ MAGAZINE
情報処理学会誌
Vol.63 No.4（2022 年 4 月号）
通巻 685 号

情報処理

常時更新中!

「情報処理」オンライン

■ Vol.63 No.4

特集：社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―

連載：教科「情報」の入学試験問題って?

「情報処理」総目次

https://www.ipsj.or.jp/magazine/contents_m.html

※冊子・オンラインの記事の目次を掲載しております（目次から電子図書館の各記事へリンクしております）.

「情報処理」note

https://note.com/ipsj

※人気記事や最新記事のチラ見せ，無料で読める記事などさまざまなコンテンツを公開していきます.
note 目次：https://www.ipsj.or.jp/magazine/contents_note.html

■情報処理学会事務局本部

〒 101-0062 東京都千代田区神田駿河台 1-5　化学会館 4F
Tel(03)3518-8374（代表）　Fax(03)3518-8375
E-mail: soumu@ipsj.or.jp　https://www.ipsj.or.jp/
郵便振替口座　00150-4-83484
銀行振込（いずれも普通預金口座）
みずほ銀行虎ノ門支店　1013945
三菱 UFJ 銀行本店　7636858
名義人：一般社団法人　情報処理学会
名義人カナ：シヤ）ジヨウホウシヨリガツカイ

■規格部　情報規格調査会

〒 105-0011 東京都港区芝公園 3-5-8　機械振興会館 308-3
Tel(03)3431-2808　Fax(03)3431-6493
E-mail: standards@itscj.ipsj.or.jp　https://www.itscj-ipsj.jp/

■支　部　北海道／東北／東海／北陸／関西／中国／四国／九州

電子版
-DIGITAL VER-

Kindle

Fujisan

情報学広場

僕らはテクノロジーとともに身体の補完を超えて拡張してゆく

■ 武藤 将胤

皆さんは昨今のテクノロジーの進化をどう捉えているだろうか？

AIやロボット技術等の進化によって私たちの生活が豊かになるという捉え方もある一方，人間の職が奪われるというような悲観的な捉え方もあるだろう．私自身はテクノロジーの力をどう使うかという私たちの選択次第で，明るい未来を築いていけると希望を持って捉えている．

もとより私はテクノロジーの力をいかに有効活用できるかという思考だったが，その思考や行動が加速したのは，2013年にALSを発症してからの体験が大きく影響している．テクノロジーの力がただ便利なものから，生きていく上で必要不可欠なものになったからだ．身体を動かす運動神経だけが徐々に衰え手足を動かす自由を奪われたことで，電動車椅子で移動し，視線入力でこの文章を書いている．そして肉声を失った代わりに，昔の自分の声を元に生成した音声合成で発話している．今この瞬間の呼吸さえも人工呼吸器がサポートしているのだ．

このように日常生活のありとあらゆる場面でテクノロジーを身に纏って生活をしていると，身体の補完にとどまらず拡張していける可能性を感じずにはいられない．テクノロジーは個人の身体のリミッター拡張のみならず，さまざまな障がいの垣根を越えた体験の拡張まで実現可能にすると考えている．

そんな光景を創り出したくて，2021年12月にMOVE FES.2021を開催した．私が主催するALS啓発のた

■ 武藤 将胤
一般社団法人 WITH ALS 代表理事

難病 ALS と闘病を続けながら，一般社団法人 WITH ALS 代表理事，COMMUNICATION CREATOR，EYE VDJ と多彩なパーソナリティで数多くのプロジェクトを手掛けている．過去には広告会社・博報堂にて，さまざまなコミュニケーションプラン立案に従事．2013 年 26 歳のときに ALS を発症．世界中に ALS の認知・理解を高めるため「WITH ALS」を立ち上げ，現在は視線入力と自身の発想でさまざまなアーティストやテクノロジストとコラボレーションし，作品制作やコンテンツ開発に挑んでいる．

めの音楽フェスだ．賛同してくれた素晴らしいアーティストとともに，私もEYE VDJ MASAというアーティスト名で視線入力による音楽と映像のライブパフォーマンスを行った．この挑戦は2016年から続けている活動で，視線入力で電子機器をコントロールするアプリケーションから開発し，年々改良を繰り返してきた．今ではオリジナル楽曲を制作しリリースもしている．また，従来DJとVJは別々のプレイヤが担当することが一般的だったが，今ではそれを視線で同時にプレーしている自分がいる．これは健常者時代には想像もできなかった進化だ．

紛れもなくテクノロジーの力で身体の補完を超えて，拡張し始めているのだ．

また今回は，音を振動と光に変換するデバイスOntennaを活用することで，耳の不自由な方や寝たきりの仲間にも，配信で臨場感のあるライブをお楽しみいただいた．そして会場ではデフダンサーの仲間やお客様全員にOntennaを身につけていただき，身体全体で音楽を楽しんでもらう設計をした．耳の不自由な仲間の世界を想像しながら楽曲の一つひとつに，振動と光のタイミングや強弱，色を視線入力でプログラミングしたのだ．まさにテクノロジーの力で障がいの垣根を越えて，新たな拡張体験が作れた瞬間だった．

私はこれからもテクノロジーとともに，身体の補完を超えて拡張した未来を社会に提案していく．誰もが自分らしく挑戦できるBORDERLESSな社会を目指して．

特集

社会インフラシステムにおけるサイバーセキュリティ
―レジリエントで持続可能なデジタル経済社会に向けて―

編集にあたって

石黒正揮 | 三菱総合研究所　新　誠一 | 電気通信大学　佐々木貴之 | 横浜国立大学

人々の社会生活や企業の経済活動は，さまざまな社会インフラシステムによって支えられており，特に重要な電力，情報通信，金融などの 14 分野については，政府のサイバーセキュリティ戦略本部[☆1]により重要インフラ分野に指定されている．世の中では，デジタル化，デジタルトランスフォーメーション（DX）を通じた進化はとどまるところがなく，社会インフラシステムにおいても，分野によっては程度の差はあるが，その例外ではいられない．安全性・信頼性が重視される社会インフラシステムにおいては，オープン化や汎用技術によるデジタル化には保守的ではあったが，デジタルにより進化していくことは間違いないだろう．

このような中，デジタル化が先行する海外を中心に社会インフラシステムやそのサプライチェーンに対する大規模なサイバー攻撃が増加し，インフラの機能停止に至る事故・脅威が拡大している．社会インフラシステムの機能が停止，低下した場合には，相互依存関係にある他のインフラシステムや社会経済活動に波及的に影響し，甚大な被害をもたらすリスクがある．

一方で，日本を含む世界の情勢を見渡すと，新型コロナ禍後のニューノーマルを見据えた社会・経済の大きな構造転換，カーボンニュートラルに向けた国際的な潮流による産業構造の大転換，産業インフラのデジタル化・高度化とそれらに対する大規模サ

☆1　国全体のサイバーセキュリティにかかわる司令塔．

イバー攻撃による事故・脅威の拡大，グローバルなサプライチェーンの深化と国際情勢の変化に伴う産業物資サービス等の供給体制の脆弱性の顕在化などの課題に直面している．将来世代を含む人類が直面する課題に対して、これからの新しい国際社会の在り方を方向付ける SDGs[☆2]（持続可能な開発目標）においては，「レジリエントなインフラ構築，包摂的かつ持続可能な産業化の促進およびイノベーションの推進を図る」ことが掲げられている．政府による経済安全保障法制の検討はこのような課題も背景として進められていると見られる．経済安全保障法制の検討においては，基幹インフラの安全性・信頼性の確保，サプライチェーンの強靭化などの取り組みが重要なものとして取り上げられている．社会インフラシステムのサイバーセキュリティはこのような経済安全保障を確保する上で根幹をなすものである．

このようなことから，本特集では，社会インフラシステムにおけるサイバーセキュリティ脅威，リスクとそれらに対する対策取り組み状況および今後の課題，展望についてまとめることとした．

社会インフラシステムは，前述の通りさまざまな分野があるが，本特集では最初の試みとして，その中でも重要で注目が集まる分野である電力，情報通信，金融，化学・石油・ガスやそれらの基盤となる産業制御システムについて取り上げたい．各テーマに関する概要は次ページにまとめている．

これらの分野のサイバーセキュリティは，多様なステークホルダによる取り組みが不可欠である．そのようなことから本特集では，インダストリ，ガバメント，アカデミアにおけるサイバーセキュリティの最前線で活躍する第一人者の知見を結集して関連分野の取り組み動向，課題，今後の展望についてまとめた．

本特集で紹介したサイバーセキュリティに関する産官学の包括的な取り組みと今後の課題への対応を推進することにより，レジリエントで持続可能なデジタル経済社会の基盤を構築し，デジタル経済安全保障を確保していくことが期待される．

（2022 年 2 月 7 日）

☆2 Sustainable Development Goals (United Nations)

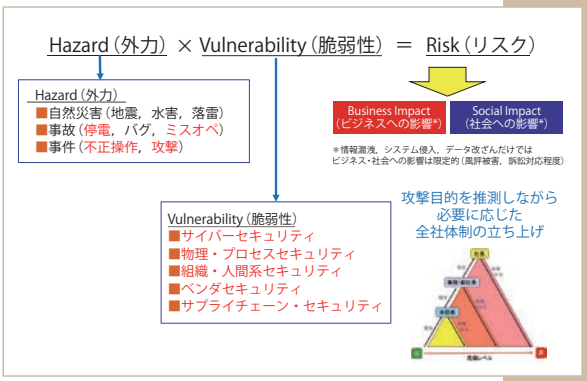
概要

1 電力分野におけるサイバーセキュリティの現状と今後の展望
—社会インフラシステムの要（かなめ）としての役割—

応用 一般

渡辺研司 | 名古屋工業大学大学院社会工学専攻

電力分野は機能の停止や低下が国民生活や経済活動に大きな影響を及ぼすため，重要インフラの中でも要（かなめ）と言える．このためサイバー攻撃の標的にもなりやすく，民業だけでは太刀打ちできない状況に陥いる可能性も高いことから，官民連携のさらなる加速と演習等による実効性の担保が急がれる．またサイバー・フィジカル両面のセキュリティを確保するためには「地域」という観点での重要インフラ事業者間の連携も重要である．



2 クラウドファースト時代のサイバーセキュリティ
—サイバーセキュリティのためのマルチステークホルダアプローチ—

応用 一般

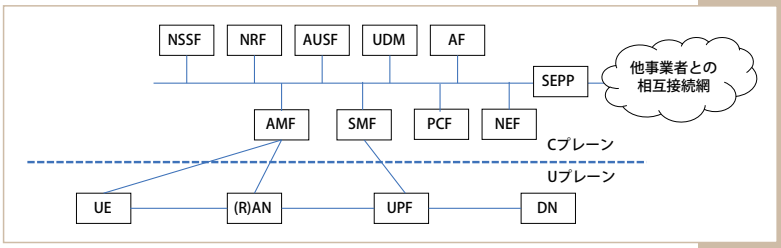
石黒正揮 | 三菱総合研究所

システムを構築する際に，クラウド基盤の利用を前提に考えるべき「クラウド・ファースト」時代が到来している．クラウドを活用することでシステムを機動的に低コストで構築できるメリットは大きいが，共有リスク，協業リスクなどクラウド特有のリスクが拡大している．本稿では，クラウド特有のリスクを挙げそれらに対する技術対策およびマルチステークホルダによるセキュリティ確保に関する動向，課題，今後の展望について示す．

3 5G 移動通信システムのサイバーセキュリティ
—移動通信におけるセキュリティ対策の変遷とこれから—

応用 一般

窪田　歩 | （株）KDDI 総合研究所



5G は高速大容量通信，多接続，高信頼・低遅延の実現により新たなサービスの創出を促進することが期待されるとともに，今後のさまざまな分野の DX を支える基盤として重要な社会インフラとなっていくことが予想される．本稿では，移動通信システムにおけるセキュリティ対策の変遷を振り返り，5G におけるセキュリティ強化ポイント，5G システムの構築・運用における課題，5G セキュリティに関する国内外の動向について解説する．

4 化学プラントのサイバーセキュリティ
― OT システムのセキュリティ脅威に対する取り組みと今後の展望―

応用 一般

星野浩志　秋元新哉　横河電機（株）

ここ数年のサイバー攻撃者の OT 領域の知識の深化と，サイバー攻撃による社会生活への影響の発生事例を見ると，化学･石油プラントを取り巻くサイバーセキュリティ脅威は確実に進化していると言える．この事態に対応していくためには，OT 分野のシステム・機器の知見や運用現場の人・プロセス・技術の知見と，IT 分野の知見の両方が必要になる．本稿では，IT 分野の読者に向けて化学プラントの生産制御システムのサイバーセキュリティ関連の動向および課題と今後の展望について紹介する．

5 産業制御システムセキュリティの動向

応用 一般

新　誠一　電気通信大学

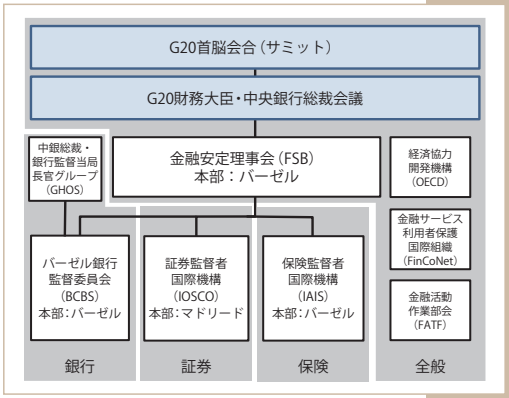
ネットワーク接続が前提となるに従い産業制御システムもサーバセキュリティ対策が不可欠になってきた．この動向と対策を概観する．合わせて，サイバーセキュリティ対策とは情報セキュリティ対策と機能安全の融合であることを再度宣言し，安全．安心な社会構築に向けての方向性を明確化する．

6 金融分野におけるサイバーセキュリティを巡る国際的な議論の動向

応用 一般

河田雄次　金融庁

本稿は，金融分野におけるサイバーセキュリティを巡る国際的な議論の動向について概説する．近年，サイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことから，G20 や G7 等のさまざまな場において，サイバーセキュリティ対策，規制報告枠組み，第三者委託，犯罪収益など多面的な観点から議論が行われている．引き続き，金融当局が連携して，課題解決に向けた議論をグローバルに深めていくことが望まれる．



特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

1 電力分野におけるサイバーセキュリティの現状と今後の展望

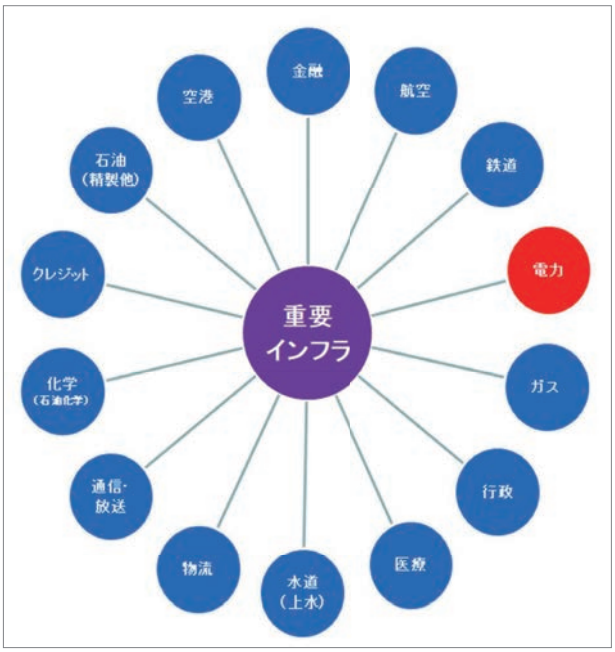
―社会インフラシステムの要（かなめ）としての役割―

応用 一般

渡辺研司　名古屋工業大学大学院社会工学専攻

社会インフラシステムの要（かなめ）としての電力分野

社会インフラシステムを構成する分野のうち特に重要と考えられる重要インフラ分野は，サイバーセキュリティ基本法に規定する重要社会基盤事業者等として定義されており，本稿執筆時点では，情報通信，金融，航空，空港，鉄道，電力，ガス，政府・行政サービス，医療，水道（上水），物流，化学，クレジット，石油の 14 分野が具体的に指定されている（図 -1）．



■図 -1　重要インフラ 14 分野

これらは，国民生活や経済活動の基盤となる社会インフラのうち，機能が停止したり，低下したりすれば特に大きな混乱を招くと見込まれるものであり，各分野でサービスを供給する事業者や組織は，分野を所管する省庁と連携しながらサイバーセキュリティのレベル向上に取り組んでいる．

そして，それぞれの重要インフラ分野は独立して存在しているのではなく，相互に依存し合いながらサービスを提供しており，その重要インフラ間の相互依存関係の要（かなめ）となっているのが電力分野である．その観点を踏まえると，攻撃者の立場からしても，電力分野はサービス停止や機能低下の社会的影響が大きいため，社会混乱を引き起こしたり，身代金を要求するような攻撃の恰好のターゲットになり得ることから，より確実かつ強固なサイバーセキュリティ体制が求められる立場にある．

その電力分野では，電力自由化に伴う産業構造の変化や発電・送配電・制御などにかかわる新たな技術やプラットフォームの導入などに伴い，人材面も含めて，もはや既存の情報セキュリティにかかわる枠組みだけではマネジメントしきれない局面を迎えている．

官民にまたがる電力分野の取り組み

このように，電力分野の経営環境やサイバーセキュリティを取り巻く状況変化を受け，電力分野のサイバーセキュリティにかかわる主な利害関係者となる電気事業者（既存・新規参入），所管省庁（経済産業省・資源エネルギー庁），業界団体（電気事業連合会等），電力 ISAC（Information Sharing and Analysis Center）などではそれぞれの課題認識に基づき，専門家・有識者委員会などからの助言を得ながら，官民連携の構図を基盤としたサイバーセキュリティ体制の強化に取り組んでいる．

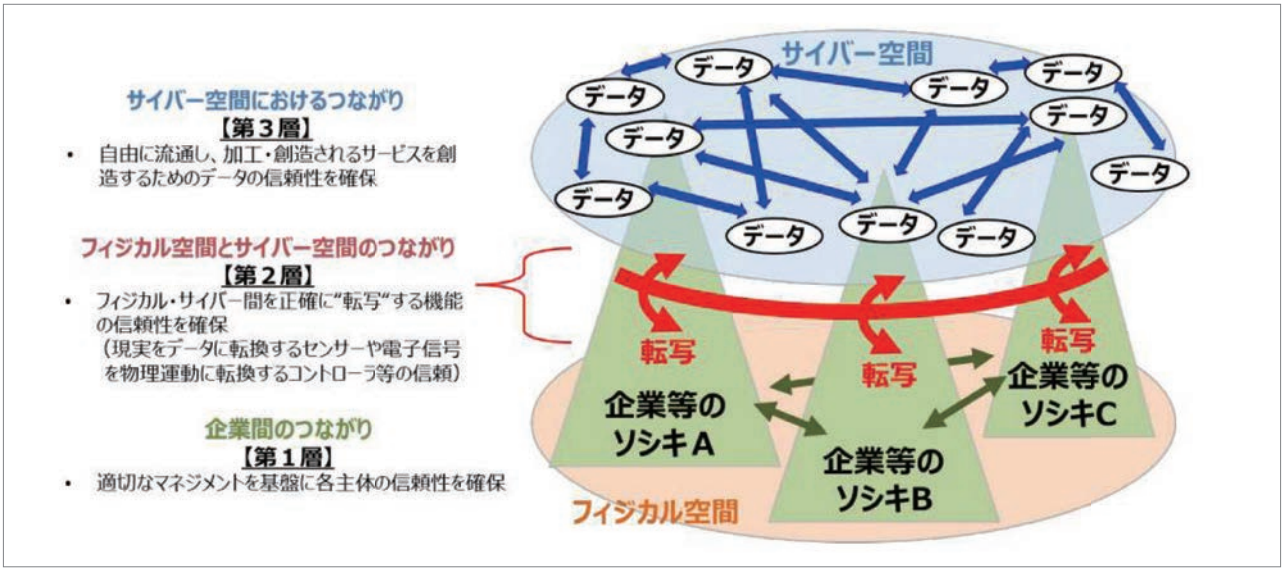
電力事業者自体の取り組みは各社各様であるが，共通して関係する主な利害関係者の取り組み状況の概要は以下の通りである．

経済産業省（産業保安グループ電力安全課・商務情報局サイバーセキュリティ課他）・資源エネルギー庁（電力産業・市場室）：

産業構造審議会に設置された保安・消費生活製品安全分科会の電力安全小委員会にて，電気事業を取り巻く環境変化に対応した今後の電気保安規制，保安人材の育成，監視制御の遠隔化等にかかわる課題認識に基づいた議論が展開されており，現在，電気保安規制の見直しの方向性や電力レジリエンスの議論にサイバーセキュリティの観点を加える形で展開されている[1]．

また，産業サイバーセキュリティ研究会ではサイバーセキュリティ政策の方向性を議論するためのワーキンググループ（WG）群を立ち上げており，そのうちの WG 1（制度・技術・標準化）の下に電力サブワーキンググループ（SWG）が設置され，電力分野のサイバーセキュリティを取り巻く現状，諸外国の状況を分析し，官民が取り組むべき課題と方向性についての議論を重ねている．その過程においては，現在，日本提案で国際規格化が進められているサイバーフィジカルセキュリティフレームワーク（CPSF）の枠組み（図 -2）を意識しながら，大手電気事業者のサイバーセキュリティ対策，新規プレーヤのサイバーセキュリティ対策，そしてサプライチェーンリスクへの対応等に焦点を当てた議論が展開されている[2]．

また，次世代のスマートメーターのセキュリティ対策については，仕様の変更や業界を超えたビジネ



■図 -2　国際標準化を進める CPSF[3]
「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要」P.8 より引用
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf

スの将来像を踏まえながら，次世代スマートメーター制度検討会に設置された次世代スマートメーターセキュリティ検討ワーキンググループにて検討が進められている．

電気事業連合会（電事連）：

電気事業者の業界団体である電事連の従来からの中核メンバであった大手電力会社は，電力自由化に伴い新規に参入してきた事業者が，電力ネットワークで相互に接続されるにもかかわらず，必ずしも大手電力会社と同等レベルのサイバーセキュリティ対応の体制が組めるわけではないとの認識から，大手電気事業者としての体制を強化する取り組みと並行して，小規模電気事業者も含めた電力業界全体の対策強化を推進しつつある．

また，関連して日本電気技術規格委員会が電力制御システムセキュリティガイドライン（2019）とスマートメーターシステムセキュリティガイドライン（2019）を日本電気技術規格委員会規格（JESC）として発行しており，主な電気事業者はその適合を目指しながら電力制御システムおよびスマートメーターシステムのセキュリティ強化にかかわる取り組みの効率化を図っている．

電力 ISAC（Information Sharing and Analysis Center）：

2017 年に，電力系統の運用を担う一般送配電事業者と，発電事業等の電力系統に連係する事業者等が連携してサイバーセキュリティへの取り組みを推進するために設立され，会員企業間のサイバーセキュリティに関する情報収集・分析・共有を行うと同時に，内閣サイバーセキュリティセンター（NISC）関連組織として官民で情報共有を行う電力 CEPTOR（Capacity for Engineering of Protection, Technical Operation, Analysis and Response）の事務局も担っている．また，業界内で連携したサイバーセキュリティ事案対応能力の向上を目指し，大手電力 10 社やＪパワー（電源開発），JERA，新電力事業者などが参加するサイバー演習も行っている．直近の演習では，新型コロナウイルス感染が拡大する状況下でも，自然災害とマルウェア感染の２要因で停電が発生するといった複合型の演習シナリオを用いて事案対応能力の確認を行う等の取り組みを実施している．

電力分野における課題と求められる取り組み

ここまでで述べてきたように，電力分野におけるサイバーセキュリティ関連の諸々のリスクが高まっている傾向は，今後さらに加速されると同時に，産業構造の変化や自動化や遠隔制御等に関する多用な新技術の導入が伴うことで，電力分野のサイバーセキュリティの実効性を確保するためには，電力供給サイドの組織単体や業界団体や所管省庁との連携だけでは太刀打ちできない局面が多発すると考えられる．

そのため，官民の組織形態を越えた下記のような事項を実現する必要があると考える．

（1）電力供給サプライチェーン横断的な取り組み：

サイバーセキュリティの最終的な目的は，電力供給サイドの安定供給力を完璧に確保することが不可能であることを考えれば，最終需要者・消費者サイドが必要な電力を必要なときに確保できる状態にすることと考えられる．このような観点からすると，従来の電力分野だけではなく，燃料調達，発電，送配電，卸売・小売り，蓄電・消費といった電力供給のサプライチェーンを構成する各組織やプロセス個々のレジリエンス（しなやかな回復力）をサイバーとフィジカルの両面で強化する必要がある．

（2）需要・消費サイドの自助体制の強化：

上記に関連して電力需要と供給の２つの側面に着目すれば，電力の供給サイドの努力だけではなく，効率的・効果的なリスクコミュニケーションを介し

て，需要・消費サイドにも働きかけることが肝要である．具体的には，供給サイドに何らかの不具合が発生した場合でも，需要・消費サイドの組織が自らの社会的使命として，継続もしくは早期復旧しなければならない業務やサービスを，代替手段の適用や復旧優先業務に絞ったオペレーションへのシフトといった，事業継続計画（BCP: Business Continuity Plan）に基づいた自主的な行動により維持する体制がとれるようにすることが必要である．

（3）サイバーセキュリティ事案対応能力の強化：

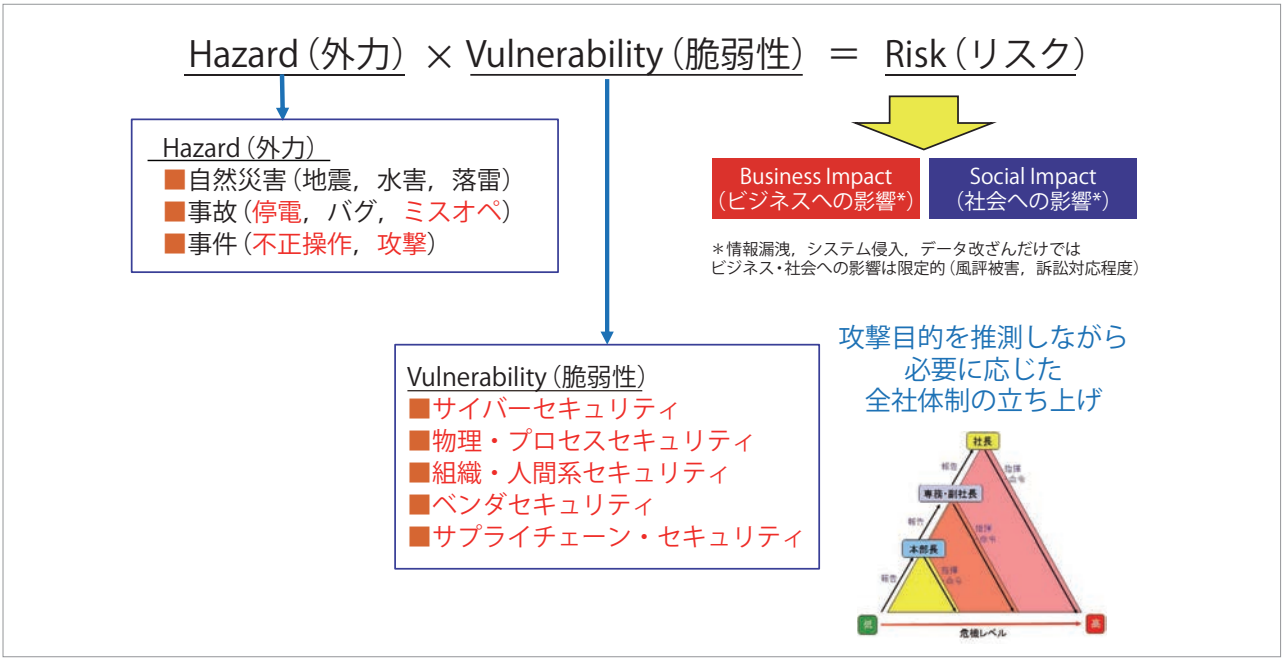
電力事業者は重要インフラ事業者とはいえ民間企業のため株主や金融機関といった利害関係者から常に経済的な合理性を経営上求められていることから，サイバーセキュリティに多大な経営資源を投下し続けることはできない．このような民業の限界については，業界内の共助と官民共助（公助ではなく）などでカバーしながら電力分野全体のサイバーセキュリティ事案対応能力の強化を目指すべきである．

また，電力事業者組織内の体制としても，情報システム関連部門やサイバーセキュリティ部門に任せきりにするのではなく，きっかけはサイバー事案であったとしても，結果として電力供給の停止や低下につながる可能性のあるような事案については，早期にトップマネジメントを巻き込んで，経営判断を加えながら，外部の利害関係者とも適時にコミュニケーションを取るような体制を構築し，その実効性を常日頃からの訓練や演習で担保し続けることが電力事業者には求められる（図 -3）．

状況によっては電力事業者自らが能動的に電力供給を停止するという経営判断も求められるのである．

（4）動的システムセキュリティマネジメント体制の確立：

サイバーセキュリティの対象となる「システム」は，ICT や情報システムだけでは機能しない仕組みであり，人間やプロセスの関与がなくしては最終的なサービスの提供や各種業務の遂行ができない．この「三位一体」のような構造（図 -4）を考えれば，サイバーセキュリティだからといって ICT や情報システムの部分だけの対策や対応をとるだけでは最終的に「システム」を防護することはできない．

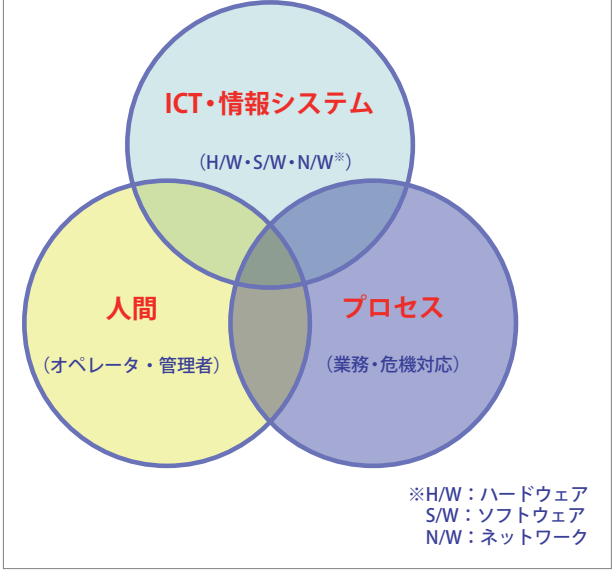


■図 -3　事案のインパクト評価に基づく事案対応体制

また，重要インフラを狙う攻撃者にとってもサイバー攻撃はあくまで攻撃手段の 1 つであり，人間系やプロセス系の脆弱性をつくような攻撃と併せた複合型の攻撃でその目的を効率的に達成しようとするはずである．したがって，防護側もサイバー，フィジカル問わず，三位一体の枠組みでセキュリティ体制の現状を見直すことで，組織の業務や資産を守り，社員・職員も守りながら，電力分野のサイバー・フィジカルレジリエンスを確保することが可能になる．

今後の展望：大都市圏における電力分野を中心とした分野横断的事案対応体制構築の重要性

電力の停止や機能低下の結果は社会経済活動の停止・停滞や社会混乱に直結しやすく，結果事象としての実例はサイバーセキュリティを起因とした事案よりも地震や風水雪害といった自然災害ですでに顕現化している．このことは，サイバーセキュリティ事案も電力分野においては，自然災害同様のフィジカルな被害をもたらすことを示しており，先述の CPSF の概念にもあるように，サイバーとフィジカルな両面を見据えたセキュリティマネジメントの運用が不可欠となる．



■図 -4　動的システム・セキュリティ・マネジメント

特に東京・大阪・名古屋を中心とした大都市圏では，人流・物流・金流・情報流の継続的な集中と流入・流出の動的変化が激しくなっており，新型コロナ禍でも人流が抑制された一方で，物流・情報流が急増した．このような状況の背景には社会経済活動の効率性や合理性を求めて，サプライチェーンやネットワークを介した水平分業と商品・サービスの提供先の地理的な集中が推進されてきたことがある．これは社会経済活動間の人・物・金・情報を介した相互依存性の急増にもつながっており，このような平時の効率性や合理性を確保するための仕組みが，電力分野も含めた重要インフラ分野のサービス障害発生時には皮肉にも多様な連鎖被害を引き起こす脆弱性となっている．

社会経済活動の集中に伴う電力障害感応度の急増

このような大都市圏における社会経済活動間の相互依存性と脆弱性の急増が，停電や低下等の電力関連障害発生の時間帯・曜日・季節・天候・大規模イベント開催の有無などのコンテクスト（context）によっては，事前に想定し得なかったような被害の動的な拡大に繋がるような事例が散見されることが多くなってきた．

特に大都市圏への通勤・通学による日中の人の流入・流出の激しさは，たとえば，東京都心部の昼夜間人口の差がきわめて高いことにも見てとれ，電力障害に起因して重要インフラ間の依存性を介した都市機能の同時多発的機能不全は，社会混乱や n 次災害（2 次災害以降の連鎖）を伴う危険な状況に陥る可能性が高くなっていることを示している．

このような状況を踏まえると，大都市圏の電力障害に対する感応度は急増しており，その結果として大都市圏におけるサイバーリスクとその社会経済活

動への影響の増加も加速していると言える．

また，電気・ガス・水道・通信といったライフライン系の重要インフラ分野の機能障害に連鎖して発生する運輸・金融・物流・行政・医療・放送等の重要インフラで発生した障害は，都市機能の途絶やサービス・レベルの低下に直結し，大都市圏のすべての社会経済活動に多大な影響を及ぼす．

そして，重要インフラへの被害の同時多発的な発生と，重要インフラ間の相互依存性を介した複合的な連鎖は都市機能を麻痺させ，その時点に大都市圏内に滞留する人々を危険にさらし，地域全体を混乱に陥れる結果にもなり得る．これも先述の通り，攻撃者にとって重要インフラを狙うインセンティブにもなっている．

急がれる大都市圏ごとの地域内重要インフラ事業者連携と相互運用性の確立

重要インフラにかかわる国全体としてのサイバーセキュリティについては重要インフラ専門調査会で議論され，また，毎年，数千人規模の参加者が行う官民連携による重要インフラ分野横断的演習でその実効性の検証が継続されている．しかしながら，重要インフラで発生するサイバー事案はフィジカルな結果として発生する可能性が高いため，特定地域内，特に大都市圏においては，その地で実際に事業を展開する重要インフラ事業者間の連携と相互運用性を確保する必要がある．

このような取り組みを実際に行っている中部地域の CCSC（中部サイバーセキュリティコミュニティ）が地元電力会社を事務局として，ガス・通信・鉄道・空港・金融・高速道路といった重要インフラ事業者に県警察と有識者・専門家が加わり，地域に特化した体制での情報共有や演習の実施を推進している．

今後は重要インフラの 1 つの分野としての電力分野単位でのサイバーセキュリティの取り組みにとどまらず，電力サプライチェーンや地域内分野横断的な枠組み等も加えることで，より実効性の高い運用体制の構築を推し進める必要がある．その際重要なのは，電力分野関係者が社会全体のサイバーセキュリティを取り巻く状況を俯瞰しながら，電力分野としての取り組みが「木を見て森を見ず」といったような断片的な個別最適にとどまらないよう絶えず意識しながら進めることである．

参考文献

1）産業構造審議会　保安・消費生活用製品安全分科会　電力安全小委員会，https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/denryoku_anzen/index.html（2022.2.7 現在）
2）産業サイバーセキュリティ研究会　ワーキンググループ 1（制度・技術・標準化）電力サブワーキンググループ，https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/index.html（2022.2.7 現在）
3）経済産業省商務情報政策局サイバーセキュリティ課，「産業分野におけるサイバーセキュリティ政策」，JIPDEC　ISMS セミナー資料（2020 年 2 月）．

（2022 年 1 月 14 日受付）

■渡辺研司　watanabe.kenji@nitech.ac.jp

名古屋工業大学大学院社会工学専攻・教授．内閣サイバーセキュリティ戦略本部・重要インフラ専門調査会会長他，電力分野のサイバーセキュリティ関連委員会等の座長・委員などを務める．工学博士，MBA（経営学修士）．

特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

2 クラウドファースト時代のサイバーセキュリティ

―サイバーセキュリティのためのマルチステークホルダアプローチ―

応般

石黒正揮　三菱総合研究所

クラウドセキュリティの重要性

「クラウド・ファースト」時代の到来！，企業が情報システムを構築・更新する際に，自前で基盤やアプリケーションを開発するのではなく，クラウドサービスの活用を第一に考えるべきとする動きが進んでいる．米国では，Cloud First の次の戦略（Beyond Cloud First）を策定し☆1，政府におけるクラウド活用を加速している．米政府機関では，セキュリティレベルの最も高い TOP SECRET（最高機密）の要求を満たすシステムとして，Amazon Web Services（AWS）などの外部のパブリッククラウドの採用も進んでいる☆2．

日本政府においては 2018 年にクラウドサービスの利用を第一候補とする「クラウド・バイ・デフォルト原則」が示された☆3．クラウドサービスを利用する国内企業の割合は 6 割を超え，年々増加傾向にあり，クラウド・シフトが鮮明になってきている☆4☆5．クラウドサービスを利用することで，企業は機動的に事業を立ち上げ，低コストでシステムを構築できるなどメリットは大きい．一方で，他のユーザとのシステム資源の共有，クラウド事業者への依存などによりクラウド特有のリスクへの対応が課題になる．政府の重点政策に掲げられる**経済安全保障法制の検討においては，電力や情報通信などの基幹インフラの安全性・信頼性の確保のため，クラウドの導入においては，国の審査の義務付けが挙げられている**☆6．このような背景から，本稿では，クラウド特有のリスクやそれらに対するセキュリティ対策の考え方についてポイントをまとめ，今後の課題と取り組み策について展望する．

クラウドシステムのリスクの特徴

クラウドは，利用者が必要なときに，必要な分だ

☆1 米国ホワイトハウス FEDERAL CLOUD, COMPUTING STRATEGY, https://www.whitehouse.gov/wp-content/uploads/2019/06/Cloud-Strategy.pdf

☆2 AWS Secret Region, GovCloud Region 等.

☆3 「政府情報システムにおけるクラウドサービスの利用に係る基本方針」

☆4 情報通信白書令和 2 年版では，クラウド利用企業は 2019 年に 64.7%に達し，クラウド基盤サービス市場は，17 年から 23 年までの年平均成長率（実績および予測）は 25.4%.

☆5 クラウドは，もはや情報系だけの世界にとどまるものではなく，セーフティクリティカルな自動車の制御系などにも持ち込む動きが活発化している．ARM 社が立ち上げた開発プロジェクト SOAFEE（Scalable Open Architecture For Embedded Edge）では，リアルタイム制御や機能安全への対応など，自動車特有の要件を満たす次世代ソフトプラットフォームを，オープンソースで提供することを目指す．SOAFEE のソフト基盤はクラウド側と車載側にそれぞれ存在し，アプリケーションはクラウド側のコンテナ形式で開発・検証することになる．

☆6 経済安全保障法制に関する提言骨子（基幹インフラの安全性・信頼性の確保）.

け計算リソース（サーバ，ストレージ，ネットワークなど）を動的に確保し，ネットワークを介して利用することができるシステムである．そのため，以下のような特性に留意が必要になる：

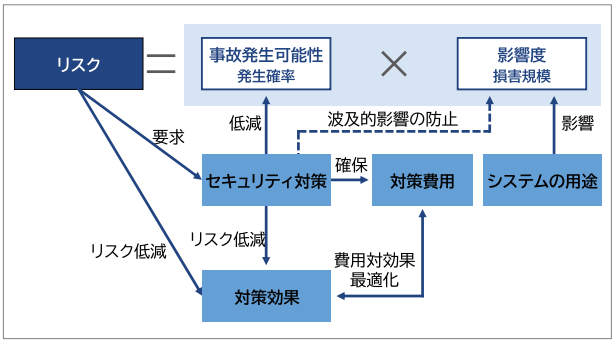
- 他の利用者とリソースを共有する
- 他事業者によりサービスとして基盤を提供される
- ネットワークを介して動的に提供される

クラウド提供者は，一般的にはセキュリティに関して高い能力を持つため，利用者は，提供されるクラウドサービスの高いセキュリティレベルを享受することができる．しかし，セキュリティ事故などにより，**最終的な損害や責任を負うのはクラウド利用者自身であり，対外的な信用が失墜するなどのレピュテーションリスクなどすべてのリスクをクラウド提供者に委ねられるわけではないことに留意**しなければならない．クラウドにおけるリソース共有や開発運用の協業などにおけるセキュリティ対策においては，「何が具体的なリスクなのか」を十分に把握した上，それに対応して対策を講じるリスクベースアプローチが有効である．図 -1 は，リスクと対策等の基本要素の関係を概念的に示したものである．

リスクの大きさは，事故発生の可能性（頻度・確率）とその影響度（被害の大きさ）の積となる．つまり，事故発生の確率が高いほど，または，その影響度が大きいほど，リスクは大きくなる．リスクを低減するためには，事故発生の確率を低減するか，または，その影響度を低減することが必要である．影響度は，扱う情報の機密性や利用業務の重要度によってある程度決まるため，扱う情報や業務を変えない限り，対策により低減できる程度は限られる☆7．したがって，通常は，システムや組織の脆弱性の低減により事故発生の確率を低減することがセキュリティ対策の主眼となる．

特に，クラウドの場合，提供者と利用者は協業関係にあることを前提として，両者の役割分担と責任関係を明確化して，クラウド利用者が実施すべき対策を実現するとともに，クラウド提供者が実施すべき対策についても要件化し，SLA 等を含む契約や評価・監査などを行うパートナとの協力を通じて実効性を確保することが重要である．

クラウドの特徴に応じたリスクを分類整理すると表 -1 のようになる．



■図 -1　リスクの構造と対策の関係

☆7 ただし，障害の波及的連鎖を防止することで，影響度を抑えるような対策はある．

■表 -1　クラウドのリスク分類

リスク	リスクの概要
共有リスク	計算リソースを共有することで，他利用者への攻撃の間接的影響等
協業リスク	クラウド利用者と提供者が他者への依存に伴うコントロール喪失等
技術リスク	仮想化，オーケストレーション，分散システムなど技術の複雑化に伴う脆弱性等
法制度リスク	国内外の法制度に伴う制約や，法執行に伴う影響など
組織リスク	クラウド利用者，提供者などの組織管理，内部犯行などの影響

■表 -2　リスク分類ごとのリスク具体例

リスク分類	リスク具体例
共有リスク	リソース集約の影響 H01，共同利用者からの影響 H03，リソース枯渇 H04
協業リスク	サービスエンジンの侵害 H06, クラウド内の DDoS 攻撃 M11，技術ロックイン L12，ガバナンス喪失 L13, サプライチェーン障害 L14,EDoS 攻撃 L15, 不正な探査 L17, データ保護 L20, 通信インフラ障害 M22, 機能サポートの制限 M23, ストレージへの攻撃 M26
技術リスク	仮想／物理の不整合 H02, 隔離の失敗 H05, 管理インタフェースの悪用 M08, データ転送路の不備 M09, 暗号鍵の喪失 L16, ID 管理の負担 M24
法制度リスク	電子的証拠開示 L18, 各国司法の相違 L19, ライセンス L21
組織リスク	内部不正・特権の悪用 M07, 不完全なデータ削除 M10, 脆弱性管理不備 M25

クラウドのセキュリティを確保するためにはこれらのリスクについて組織に応じて体系的，網羅的に脅威を洗い出し対策を講じることが求められる．

クラウドリスクの具体例

クラウドのリスクについては，欧州ネットワーク・情報セキュリティ機関（ENISA）や日本セキュリティ監査協会（JASA）などにより整理されている．そこで挙げられるリスクを含む形で，上記のリスク分類に応じて主なリスクを列挙すると表 -2 の通り整理できる．X01 から X21（X はリスクのレベルで H:High, M:Middle, L:Low の 3 段階）は ENISA, JASA により提示されたリスクで，M22 ～ M26 は本稿で追加したものである．また，複数のリスク区分に該当するリスク事例は，そのうち一方のみに記載している．

■表 -3　クラウドのステーホルダ分類

ステークホルダ	概要
クラウド利用者	クラウドを利用したアプリケーションの開発・運用・利用する．
クラウド提供者	クラウド基盤を提供する．
クラウドパートナ☆8	クラウド利用者，提供者に対して，構築運用支援・監査等を行う．

☆8 国際標準 ISO/IEC17789 で定義されている，クラウド利用者とクラウド事業者が協業するパートナのことで，クラウド デベロッパ，クラウド監査人，クラウドブローカなどが含まれる．

クラウドのセキュリティを確保するためには，これらのクラウド特有のリスクを認識し，当該組織にとっての具体的なリスクを特定し，通常のセキュリティ対策を強化することが求められる．

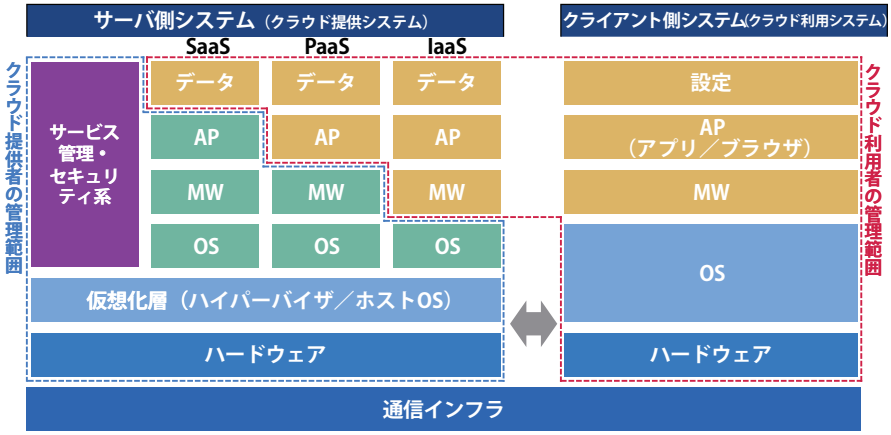
ステークホルダの責任分担

クラウドシステムは多様なステークホルダにより構築・運用される．クラウドシステム全体としてのセキュリティを確保するためには，ステークホルダについて責任範囲を明確にして，それぞれの責任を果たすために開発から運用に至るセキュリティ管理策を講じることが求められる．

ステークホルダを大きく分類すると表 -3 の通りである．

クラウドシステムの構成と責任範囲を示したものが図 -2 である．

クラウド提供者は，提供する基盤サービスの種類（SaaS/PaaS/IaaS）に応じて提供するシステムレイヤまで責任を負う．対して，クラウド利用者はクライアント側システムとサーバ側システムのうち，クラウド提供システムの上位にあるシステムの開発・運用について責任を負う．なお，ISO/IEC 27017:2015 においては，クラウドの 3 つのサービス種別に応じて，利用者と提供者は，下表の項目のいずれに責任を持つか，明確に定義しなければならないと規定している．たとえば，ID 管理システ



■図 -2　クラウドシステムの構成と責任分界

ムの保守は，ID 管理システムに脆弱性や更新がないか確認し対応することなどを意味する．このような要件も考慮してステークホルダ間の責任関係を契約で縛ることも必要である（表 -4）．

クラウド利用事業者とクラウド基盤提供事業者との間では以下のような要求事項を契約に含めることなどが挙げられる．

• SLA（Service Level Agreement）

提供されるクラウドシステムのサービスレベルについて規定するもののことであり，リスク整理表におけるリソース集約の影響，リソース枯渇などのリスクに対策する．サービス稼働率, 平均応答時間, サポート項目，要求未達の場合の賠償規定などがある．

• 利用者の規約・禁止事項

利用者の不正行為や不注意などによって被害を受けるリスクに対して，クラウド利用事業者とクラウド関連事業者とで検討し，規約違反の他のクラウド利用者に対してクラウド提供の停止，または賠償請求により実効性を高める措置などを講じる．

• クラウド基盤提供者の体制管理

クラウド提供事業者における内部の不正を防止・抑止するため，ラウド提供システムやメンテナンスシステム等のアクセス特権の管理，情報取扱者の制限，監視・記録による不正行為・操作の抑止，雇用者の契約管理などの要求事項を定める．

• 法的リスクの開示説明

クラウドの所在地の法制度により電子的証拠の開示命令，個人情報の管理規則，輸出管理法令などによるリスクに対処するため，クラウドの所在地における法的リスクの開示を義務づける．

クラウド基盤利用者が，クラウド基盤提供者のセキュリティ対策の妥当性についてチェックすることが困難な場合がある．そのような場合，第三者による専門的な立場から対策の妥当性を保証するための仕組みとしてセキュリティ監査を用いることができる. そのような例として, クラウド情報セキュリティ

■表 -4　クラウド利用者と提供者の責任範囲☆9

区分	利用者	提供者
SaaS	・収集・処理した顧客データに関するデータ保護法への準拠 ・ID 管理システムの保守 ・ID 管理システムの管理 ・認証プラットフォームの管理(パスワードポリシーを含む)	・物理サポート基盤（施設, 電力等） ・物理インフラ・セキュリティと可用性確保（サーバ等） ・OS パッチ管理と堅牢化 ・セキュリティ・プラットフォームの設定（FW 等） ・ログ収集とモニタリング
PaaS	・ID 管理システムの保守 ・ID 管理システムの管理 ・認証プラットフォームの管理	・物理サポート基盤（施設, 電力等） ・物理インフラ・セキュリティと可用性確保（サーバ等） ・OS パッチ管理と堅牢化 ・セキュリティ・プラットフォームの設定（FW 等） ・ログ収集とモニタリング
IaaS	・ID 管理システムの保守 ・ID 管理システムの管理 ・認証プラットフォームの管理 ・ゲスト OS パッチの管理と堅牢化 ・プラットフォームの設定（FW/IDS 等） ・ゲストシステム監視 ・ログ収集とモニタリング	・物理サポート基盤（施設, 電力等） ・物理インフラ・セキュリティと可用性確保（サーバ等） ・ホストシステム（ハイパーバイザ, 仮想 FW など）

☆9　ISO/IEC 27017:2015 抜粋

■表 -5　リスクの区分

意図的区分	概要
意図的脅威	悪意のある攻撃による事故の原因. 組織の内部・外部の両方がある.
非意図的脅威	情報システムの不具合や通信インフラの障害など悪意によらない脅威.

■表 -6　技術対策と主なリスクの対応関係

技術的対策	対応する主なリスク
監視・脅威分析	サービスエンジンの侵害，リソースの枯渇，内部不正・特権の乱用，不正な探査・スキャン
脆弱性管理	管理インタフェースの悪用，データ転送路の不備，脆弱性管理の不備，サービスエンジンの侵害
認証・アクセス制御	内部不正・特権の悪用，ガバナンスの喪失, 不正な探査・スキャン
ネットワーク防御	リソース枯渇，隔離の失敗，クラウド内の DDoS/DoS 攻撃，不正な探査・スキャン
ストレージ防御	コンテンツやストレージへの攻撃，不完全なデータ削除
構成管理・セキュア開発	サプライチェーンにおける障害，隔離の失敗，サービスエンジンの侵害，管理用インタフェースの悪用，事業者が管理すべき暗号鍵の喪失

監査制度，政府情報システムのセキュリティ評価制度（ISMAP）などがある．

クラウドのセキュリティ対策の全体像

クラウドのリスク対策については，悪意を持った意図的な脅威とそれ以外の非意図的な脅威という観点でも分けられる（表 -5）．

意図的脅威に対する対策は，技術対策と組織対策に分けることができ，それらを組み合わせて対処することが必要である．主な技術対策，組織対策と前述のリスクとの対応関係を整理すると表 -6 のようになる．

このほかに，非意図的脅威に対する対策は主に信頼性の向上，安定性の確保に係るもので，セキュリティ対策と分けて考えることができる．その例としては，単一障害点の解消，正規の利用における負荷の集中・輻輳への対応，リソースの冗長化，動的なリソース確保，ソフトウェアの品質確保などが挙げられるが，本稿はセキュリティに関する特集であり，紙面が限られるため，非意図的脅威については省略する．表 -3 に挙げた技術対策の概要は表 -7 の通りである．

■表 -7　クラウドに適用される主な技術的対策

技術的対策	概要
監視・脅威分析	ネットワーク上の通信，情報システムの操作などのログを監視・分析し，異常や不正な活動を検出する．
脆弱性管理	利用システムの脆弱性の特定と修正により脆弱性対策を迅速に行う．
認証・アクセス制御	ID 認証に基づき，アクセス許可やアカウントの役割（ロール）に応じた認可，特権管理を行う．
ネットワーク防御	ネットワークへの攻撃，不正侵入に対する検知・防御を行う（Firewall, IDS（侵入検知システム）等）．
ストレージ防御	ファイルの改ざん検知，ソフトウェア署名の検証，セキュアブートなどにより，流通・運用時の改ざんを検知する．
構成管理・セキュア開発	暗号などのセキュリティ機能の適切な利用・設定・セキュアコーディングなどの開発技術を適用する．

主な組織対策と概要は表 -8 のようなものが挙げられる．

セキュリティ技術対策の例

セキュリティ技術対策は，表 -1 に示す通り多様である．ここではクラウド・セキュリティにおいて重要な対策例をいくつか紹介する．

監視・脅威分析

近年，組織にネットワークへのマルウェア感染や内部不正のリスクに対して組織内外を問わずセキュリティを強化するゼロトラストセキュリティに注目されている．クラウドにおいては，リソースの共有リスク，事業者の協業リスクがあるため，ネットワークの監視・脅威分析はより重要である．クラウド利用者側としては，クラウド提供者側から提供される仮想マシンの監視・脅威分析用のツールを用いるか，IaaS, PaaS を利用するシステムにおいては，セキュリティイベントの記録管理・分析システム（SIEM）等や不正侵入検知システムなどのツールをホスト上で稼働させることで対応することができる．たとえば，AWS では，クラウドのインフラストラクチャ，システム，アプリケーション，さらにはビジネス指標について，カスタムダッシュボードを構築し，アラームを設定し，アプリケーションのパフォーマンスや信頼性に影響する問題を警告するための異常検知機能として Amazon CloudWatch anomaly detec-

■表 -8　主な組織的対策

組織対策	対策概要
リスクアセスメント	組織におけるリスクの洗出し・評価に基づきセキュリティ対策プロセスを確立する．
ポリシー策定	リスクアセスメントに基づき，組織全体として一貫性を持った方針を規定する．
体制構築	経営層が意思決定を行えるよう，CISO☆10 のリーダシップのもと，開発・運用に必要な予算と体制を構築する．

☆10 Chief Information Security Officer（情報セキュリティ最高責任者）

tion が提供されている．この CloudWatch のメトリクス（監視指標）の異常検出を有効にすると，過去のデータに機械学習アルゴリズムが適用されて，メトリクスの正常時の想定値としてのモデルが作成され，正常な状態から外れる状態や不正な挙動を検知することが可能になる

脆弱性管理

IaaS, PaaS, SaaS およびクラウド事業者が開発するシステム全体に渡り役割分担を明確にして脆弱性管理を行わなければならない．クラウド提供事業者は，クラウドサービスに影響し得る技術的脆弱性を管理し，クラウド利用者が必要とする脆弱性情報を利用者に提供しなければならない．脆弱性の情報源としては，脆弱性対策情報ポータルサイト（Japan Vulnerability Notes；JVN）や NIST NVD（National Vulnerability Database）などがある．また，業界ごとに設置されるセキュリティ情報共有組織 ISAC の活用も有効である．脆弱性を予防管理する技術としては，OWASP Top 10 のような脅威事例に基づく開発ガイドラインや脆弱性検証ツールの利用や，サプライチェーンのおけるソフトウェア部品の情報を管理する SBOM（Software Bill of Material）などの活用が有効である．

近年，サプライチェーンやソフトウェアアップデート機能を介して，不正ソフトウェア，ハードウェアを組込まれる脅威が高まっていることから，脆弱性における不正機能の悪意の意図性を評価する手法[☆11] が重要になると考えられる．

今後の課題と取り組み策

クラウド・セキュリティは，多様なステークホルダとの協業におけるリスクに対するセキュリティの確保が重要である．それらの管理策は十分に成熟しておらず，今後以下のような取り組みが重要となる．

- **マルチステークホルダ・セキュリティガバナンス（サプライチェーン・セキュリティ）**
  クラウド基盤利用者，クラウド基盤提供者，クラウドパートナなどさまざまなステークホルダとの協業において顧客に対する責任主体，ステークホルダ間の責任境界の明確化，役割分担を規定するガイドライン，取引契約書テンプレートを整備する．
- **セキュリティ・アシュアランスの確保**
  セキュリティ対策や技術検証などに関する協業者間や顧客・消費者に対する説明責任を確保する．そのためには経済産業省のサイバーフィジカルセキュリティフレームワークなどのベースを利用し，プロセスや検証結果などのエビデンス（根拠情報）に基づく客観的，体系的な説明を果たすためのガイドライン，モデル事例（アシュアランス・ケース）を整備する．**ここで重要なことは，然るべきセキュリティ対策を実施するだけではなく，利用者，取引相手などに対して然るべき対策を実施していることの説明責任を果たすことで信頼を獲得することである．セキュリティ対策とその説明責任を果たすことは同一ではない．**
- **脅威情報の蓄積・共有と管理策の向上**
  コンテナなど仮想化技術やリソース共有に係る脅威は常に変化しているため，最新の脅威情報の蓄積・共有および脅威に対する管理策，技術対策のガイドラインを整備する．

（2022 年 1 月 5 日受付）

■石黒正揮（正会員） masa@mri.co.jp

博士（情報科学）．東京大学大学院理学系研究科情報科学専攻修士課程修了．2000 年 SRI International（スタンフォード研究所）客員研究員．現在，（株）三菱総合研究所サイバーセキュリティ戦略グループ．専門は，サイバーセキュリティ，ディジタル・エンジニアリング，AI/ 数理データ解析，リスク評価，日米欧アジアにおけるセキュリティ政策・技術戦略，セキュリティ経済学．

☆11 三菱総合研究所、不正機能評価スコアリングシステム（Vulnerability Maliciousness Scoring System）

特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

3 5G 移動通信システムのサイバーセキュリティ
―移動通信におけるセキュリティ対策の変遷とこれから―

応用 一般

窪田　歩　（株）KDDI 総合研究所

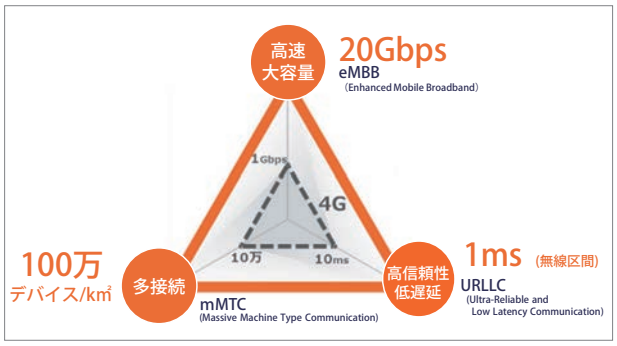
社会インフラとしての移動通信システム

移動通信システムは，図 -1 に示すように，音声通話が主体となっていた 1990 年代の 1 ～ 2G から，モバイルインターネット利用が広がった 3G を経てスマートフォン等によるモバイルブロードバンド通信を支える 4G へと発展する中で，社会インフラとしての重要性を高めてきた．5G では，図 -2 に示す通り，高速大容量通信，多接続，高信頼・低遅延の面で 4G からさらなる性能向上が図られ，新たなサービスの創出を促進することが期待されるとともに，今後さまざまな分野の DX（デジタルトランスフォーメーション）を支える基盤としての活用が進み，より一層重要な社会インフラとなっていくことが予想される．

本稿では，移動通信システムの発展を振り返り，移動通信システム特有のセキュリティ脅威とその対策の変遷について説明した後，5G の技術仕様におけるセキュリティ強化ポイント，5G システムの構築・運用におけるセキュリティ課題，5G セキュリティに関する国内外の動向について解説する．

移動通信システムにおけるセキュリティ脅威

図 -3 に移動通信システムの大まかな構成を示す．移動通信システムは，ユーザ端末（UE）が無線により基地局に収容される無線エリアネットワーク（RAN）と，認証，移動管理，セッション管理，課金，ポリシー制御等を担う機器群から構成されるコアネットワークからなり，インターネットやプライ



■図 -2　5G の技術進化

■図 -1　移動通信システムの発展

ベートネットワーク等のデータネットワークや，他通信事業者のネットワークと相互接続されて通信サービスを提供している．

移動通信システムにおけるセキュリティ脅威としては，アクセス回線に無線が使われることから，なりすましや盗聴，サービス妨害等の脅威があり，また，端末が常時携帯して利用されることから，端末の位置情報を捕捉，追跡されることによるプライバシー脅威もある．さまざまな場所に設置される基地局への物理攻撃の脅威なども考えられる．このため，移動通信システムにおいては，その初期からセキュリティ対策は重要課題として取り組まれてきている．以下ではまず，移動通信システムがデジタル化された 2G 以降のセキュリティ対策の変遷について概観する．

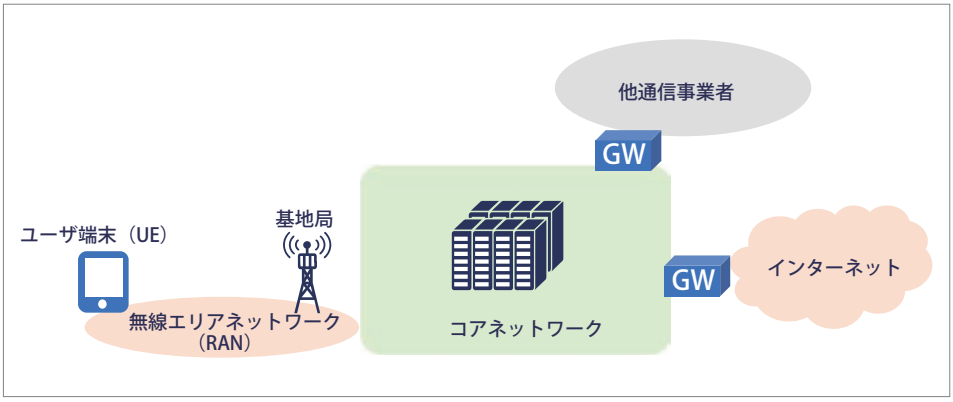
2G のセキュリティ

移動通信システムにおいて，正しく確実な課金を実現し，無線を利用して行われる加入者通信と加入者のロケーションプライバシーを保護するため，2G においてすでにさまざまなセキュリティ対策が導入されている．2G の通信規格として海外での主流である GSM（Global System for Mobile communication）の場合は，SIM（Subscriber Identity Module）を用いた強力な加入者認証によりなりすましや不正利用を防止し，無線区間においては加入者通信保護のため，通信の暗号化が行われている．また，IMSI（International Mobile Subscriber Identity）と呼ばれる加入者 ID を無線の傍受等を行う攻撃者から秘匿し，ロケーションプライバシーを保護するため，ネットワークに接続された端末の識別には TMSI（Temporary Mobile Subscriber Identities）が使われる．

GSM にはこのようなセキュリティ対策が導入されていたものの，セキュリティ上の課題も残っていた．加入者端末は SIM を利用して認証されるのに対して，端末による基地局認証は省略されていたため，偽基地局を用いた加入者 ID の収集や盗聴等が行われる脅威があった．これは 3G で端末と基地局の相互認証が導入された後も，2G のサービスが残っている地域では，3G への接続を妨害して 2G にフォールバックさせて偽基地局へ接続させる方法で攻撃に利用される事例が報告されている．また，2G 当時の技術的な制約により，鍵長が 64 ビットの弱い暗号アルゴリズムが使われており，改ざん検知も省略されていた．加えて，基地局から先のコアネットワーク内は信頼できる安全な区間であるとみなして暗号化は行われていなかった．

3G のセキュリティ

3G では端末と基地局間の相互認証の導入により偽基地局への対策が講じられた．暗号アルゴリズムは鍵長が 128 ビットとなり，制御信号に対する改ざん検知も導入されたほか，基地局から先のコアネットワークへも IPsec（TCP/IP 通信において IP パケット単位での認証，改ざん検知，暗号化による秘匿を実現するプロトコル）の利用によるセキュリティ対策が導入された．これらの対策により，安心・安全に広く利用される通信システムとなっている．



■図 -3　移動通信システムの構成

4G のセキュリティ

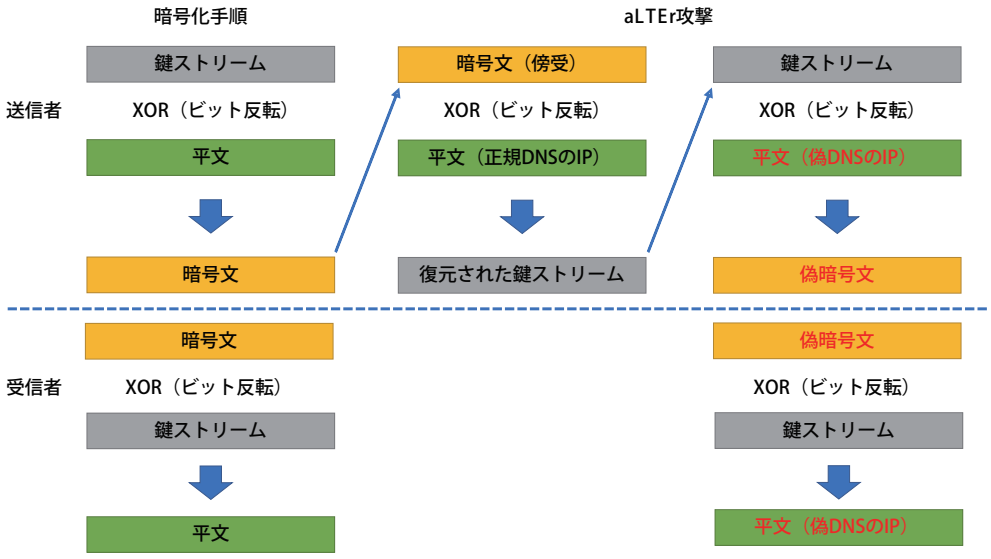
3G によりモバイルインターネット利用が進み，移動通信システムの利用シーンが広がったことで，屋内を含む無線アクセスのカバレッジの拡大や，通信容量の確保のため，より身近な場所に基地局が設置されるようになった．そうした場合，基地局が物理的な攻撃にさらされ，暗号鍵が盗み出されるリスクが存在する．実際に，一部の小型基地局で，ストレージから暗号鍵を取り出せたり，デバッグポートが無効化されていなかったりするなどの脆弱性がセキュリティ研究者により報告されている．こうした鍵の漏洩リスクへの対処と，通信の高速化，大容量化に伴って効率化が必要となる暗号鍵の更新処理の見直しのため，4G においては鍵の階層化が導入された．端末の認証手続きの結果として認証のたびに新たに生成される鍵から，端末の在圏時の鍵階層の基となる鍵を生成・保持し，そこからさらに鍵導出を繰り返して生成した個別の鍵をコアネットワーク内や基地局で利用することで，鍵の漏洩時の影響範囲の限定と，鍵更新処理のたびに端末の認証を繰り返さずに済む処理の効率化を実現している．

5G に向けた残存課題

移動通信システムは 2G から 3G，4G でのセキュリティ対策強化を経て安全性を高め，社会インフラとして広く利用されるようになっているが，いくつかのセキュリティ課題も指摘されている．以下ではそれらのうち主なセキュリティ課題について紹介する．

U プレーンの改ざん検知

3G において制御信号（C プレーン）に対する改ざん検知が導入されたが，ユーザ通信（U プレーン）に関しては 4G においても暗号化しか行われていない．2019 年には，この U プレーンの改ざん検知が省略されていることを突いた攻撃手法（aLTEr）が研究者によって発表されている[1]．図 -4 に示すように，4G における暗号文は，鍵ストリームと平文の XOR（排他的論理和）によって作られているため，なんらかの条件や手段により平文が攻撃者にとって既知である場合，無線を傍受して得られる暗号文と平文との XOR により鍵ストリームを復元し，偽の平文と再度 XOR することで，偽の暗号文を作成することができる．aLTEr 攻撃では，端末がデフォルトで利用する DNS サーバの IP アドレスが既知であることを利用し，端末と基地局間の無線通信を不正



■図 -4　aLTEr 攻撃

に中継する攻撃者が，端末から送信される DNS クエリパケットの宛先部分の鍵ストリームを復元し，攻撃者が用意した偽の DNS サーバの IP アドレスと再度 XOR することにより作成した暗号文に書き換えて基地局に送信する．DNS クエリの宛先アドレス部分の偽暗号文は，U プレーンの改ざん検知がないため偽の IP アドレスに復号され，そのまま偽の DNS サーバにルーティングされることになる．攻撃者は偽 DNS サーバに届くクエリに対して偽の応答を返すことで，端末の通信を偽サーバに誘導することができる．

加入者 ID の保護

TMSI の利用による加入者 ID の秘匿や，3G で導入された基地局認証等により，加入者 ID の収集やロケーショントラッキングへの対策は強化されているが，4G においても残存リスクが指摘されている．加入者 ID が平文で無線区間を流れる手順が一部残っているほか，加入者 ID を秘匿するために利用されるテンポラリーな ID である TMSI が，通信事業者の設定によっては長期間更新されず，TMSI ベースのロケーショントラッキングが可能なケースがあることなどが指摘されている．

事業者間通信

ローミングなどのための通信事業者間の接続はクローズドな交換ネットワークを介して行われるため，2G や 3G では通信事業者間の相互信頼を前提とし，セキュリティを考慮していない古いプロトコルである SS7（Common Channel Signaling System No.7）が使われている．通信事業者の数が増えるに従い，事業者間の信頼に関する前提が崩れてきており，SMS の不正な転送による 2 要素認証の突破などの事例も発生している．このため，通信事業者では SS7 ファイアウォールの導入などの対策が進められている．4G では SS7 に代わり Diameter（インターネット技術の国際標準を議論・策定している IETF が策定した認証・認可・課金のためのプロトコル）が採用されているが，セキュリティ研究者により Diameter にも脆弱性の存在が指摘されている状況である．

5G の技術仕様におけるセキュリティ強化ポイント

5G は 4G までに導入されたセキュリティ対策を踏襲しつつ，上述の残存課題への対応を含めたさらなるセキュリティ強化が図られている[2), 3), 4)]．以下では Non-Stand Alone（NSA）の 5G と Stand Alone（SA）の 5G のセキュリティ面での違いについて述べた後，5G の技術仕様における主なセキュリティ強化ポイントについて説明する．

NSA と SA

5G 導入の初期段階では，4G のコアネットワークを利用して 5G 無線を利用する NSA によるサービス展開が進められており，その後，5G のコアネットワークを持つ SA の導入が進められることになる．NSA では，複数基地局を同時利用して高速大容量通信を実現する 4G の仕様である Dual Connectivity を拡張し，4G 基地局をマスタ，5G 基地局をセカンダリとして利用可能にすることで 5G 無線の利用を実現している．このため，NSA では 5G 無線を利用した高速大容量通信は可能になるが，セキュリティ面では 4G と大きな違いはなく，以下で述べるセキュリティ強化は SA の導入によって実現されることになる．

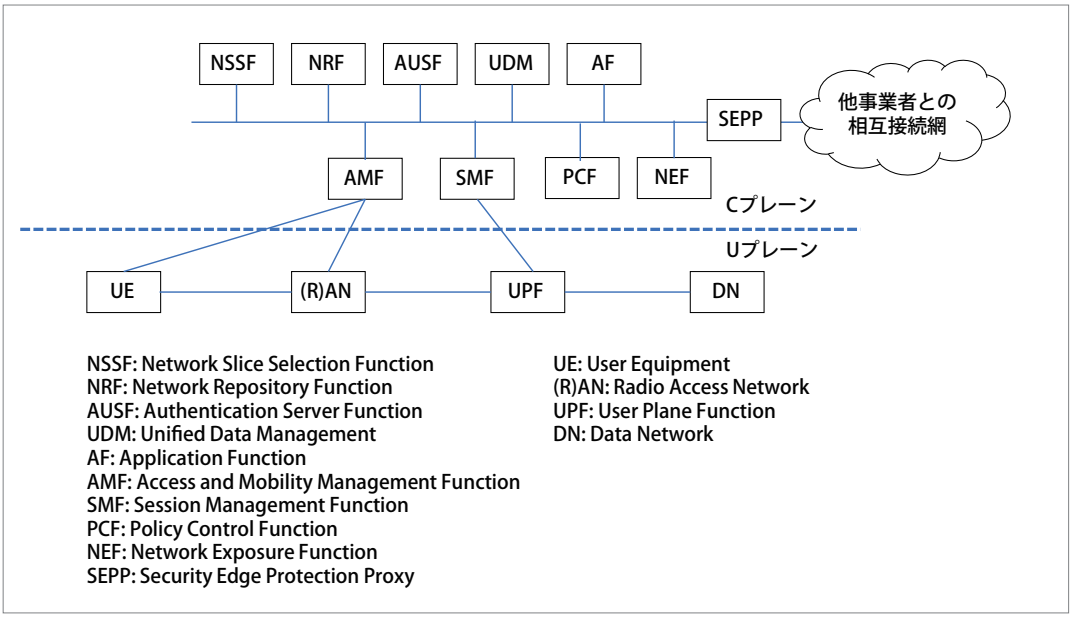
トラストモデルの見直し

無線区間と異なりコアネットワークは安全であるとして基地局以降のコアネットワーク内のセキュリティ対策を省略していた 2G のセキュリティ設計や，通信事業者間の信頼を前提として SS7 を利用していた事業者間通信など，過去の移動通信システムでは仕様策定時のトラストに関する前提に基づいてセキュリティ対策の省略や最適化が図られてきた．5G では，信頼できるとみなす対象や範囲をより限

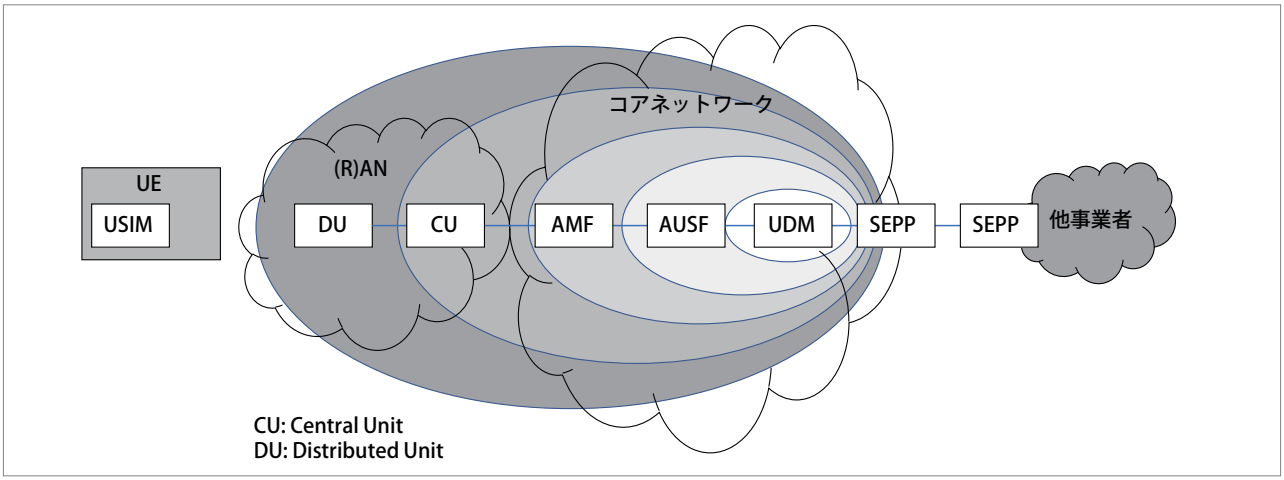
定した上でセキュリティ設計を行うことにより，セキュリティのさらなる強化が図られている．図 -5 に 5G のアーキテクチャを示しているが，トラストモデルの見直しでは，具体的には，コアネットワーク内で，加入者情報管理や認証処理を担う UDM（Unified Data Management）と AUSF（Authentication Server Function）を信頼のコアとし，図 -6 に示すようにコアから遠ざかるに従いトラストが低下するモデルとし，それに従ったセキュリティの設計が行われている．

RAN における CU/DU 分離

トラストモデルの見直しにより，コアから離れたネットワークエッジに展開される基地局はセキュリティ確保が難しく信頼度が低いという前提が置かれている．これは，5G においてはカバレッジ確保のために膨大な数の基地局のきめ細かな配備が必要になり，物理的セキュリティの確保が困難な場所にも多数の基地局を設置する必要があるためである．このため 5G では，基地局機能を CU（Central Unit）と DU（Distributed Unit）に分離し，末端に位置す



■図 -5　5G のアーキテクチャ



■図 -6　5G のトラストモデル

る DU には暗号処理に関する情報を保持させず，コア側に近く，セキュリティ確保が可能な場所に設置できる CU で暗号処理を終端させることで，DU がセキュリティ侵害を受けたとしても加入者通信が保護される設計になっている．

加入者 ID 保護の強化

5G では加入者 ID を IMSI ではなく SUPI(Subscriber Permanent Identifier）と呼称するが，5G の仕様では，ネットワークへの初期登録の手順も含めて SUPI が平文で無線区間を流れることはなく，必ず，契約先の通信事業者の公開鍵を用いて SUPI を暗号化した SUCI（Subscriber Concealed Identifier）の形で送信されるよう仕様が規定されている．また，端末の識別に利用されるテンポラリな ID（5G-GUTI : Globally Unique Temporary Identifier）の更新頻度についても厳格に仕様で定められており，GUTI ベースのロケーショントラッキングにも対策が講じられている．

RAN のセキュリティ強化

4G で省略されていたセキュリティ機能として，U プレーンの改ざん検知がある．5G では，U プレーンへの改ざん検知機能が新たに追加されたが，移動通信システムの仕様検討・作成を行う 3GPP（3rd Generation Partnership Project）が Release 15 として発行した 5G の初期仕様では，処理負荷を考慮し，64Kbps までの通信では改ざん検知を必須とし，それ以上の高速通信ではオプションとなっていた．2019 年の aLTEr 攻撃の発表を受け，その後に発行された 3GPP Release 16 の仕様ではフルレートでの改ざん検知の実施が必須と定められている．

事業者間セキュリティ（SEPP と Home Control 強化）

トラストモデルの見直しに伴い，通信事業者同士であっても必ずしも信頼できないという前提でアーキテクチャの見直しやセキュリティ手順の見直しが図られている．図 -5 に示した通り，5G では他事業者との相互接続は SEPP（Security Edge Protection Proxy）を介して行われる形になり，SEPP により事業者間通信における認証，認可，秘匿，改ざん検知，リプレイ攻撃対策などのセキュリティ機能が提供される．

また，加入者が契約先事業者のネットワーク（Home Network）から他事業者のネットワーク（Visited Network）へローミングした際の認証に際しては，ローミング先で行われた認証の結果を Home Network 側の事業者が検証する Home Control の強化が図られている．

セキュアな実装と脆弱性への対応

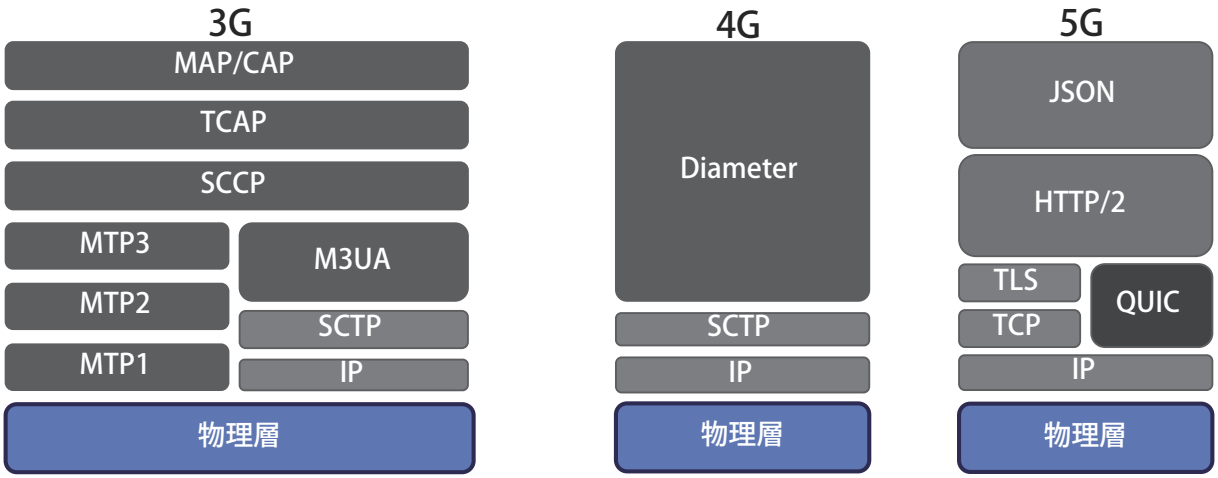
以上のようなセキュリティ強化に加え，5G の仕様ではさまざまなセキュリティ対策についての規定が定められているが，5G システムを構成する通信機器が仕様に従って正しく実装されていなければ実際に安心・安全な移動通信システムを実現することはできない．また，技術仕様自体や運用中の製品にセキュリティ上の問題が発見され，仕様の改訂や通信機器の更新等が必要になる場合もあり，そうした場合の情報開示や対応のプロセスを整備することも長期間に渡り運用される社会インフラとしての移動通信システムのセキュリティ確保において重要である．このため，5G の技術仕様を定める 3GPP と，移動通信の業界団体である GSMA（GSM Association）が連携し，通信機器が一定レベルのセキュリティを有していることを保証するための枠組みとして NESAS（Network Equipment Security Assurance Scheme)が整備されている．NESAS では，通信機器ベンダの製品の設計開発やライフサイクル管理プロセスの監査や，3GPP が定めたネットワーク機器のセキュリティ仕様である SCAS（Security Assurance Specification）に基づいて個々の製品が正しく実装されていることの認定ラボでの試験結果を通じて，導入する通信機器のセキュリティレベル

を通信事業者が確認可能にする枠組みであり，すでにいくつかの大手通信機器ベンダや製品が認定を取得している．また，移動通信システムにかかわる脆弱性等の情報の開示や対応については，GSMA のCVD（Coordinated Vulnerability Disclosure）プログラムにより，GSMA が窓口となって，セキュリティ研究者等が発見した問題の一般公表前の情報共有や影響分析，関係組織による対応のコーディネーションが行われている．

構築・運用面での課題

技術仕様の上では，5G は 4G からのセキュリティ強化が図られ，より安心・安全に利用できる移動通信システムになっているが，5G システムの構築・運用の全体を考えた場合にはセキュリティ上の懸念や課題が存在する．

図 -7 に示す通り，移動通信システム固有のプロトコルが使われていた過去の世代と異なり，5G のコアではインターネットで利用されている一般的なプロトコルが使われるようになっている．このため，移動通信システムへのサイバー攻撃も，特殊な専用機器やプロトコルの知識を要するものではなく，Web アプリへの攻撃に近くなると考えられ，脆弱性の発見や対処などのセキュリティ運用の重要性が一層高まることが想定される．また，さまざまなユースケースに応じて 5G の性能をチューニングした専用の仮想ネットワークを提供するネットワークスライシングの実現などのため，5G コアネットワークでは仮想マシンやコンテナなどの仮想化技術の活用が進み，これに伴うシステム構成の複雑化や，物理適切に設定し運用することが難しくなることが想定される．このように，安心・安全な 5G システムの構築・運用には，5G セキュリティの技術仕様への準拠だけでなく，ベースとなる仮想化基盤のセキュリティや組織面，運用面の考慮など，広範な検討が必要になる．このリファレンスとするため，国内では，5G セキュリティ検証環境を構築して実施したセキュリティ検証結果と，技術的対策だけではなく組織や運用面も含めたトータルな 5G セキュリティの分析結果に基づき，5G セキュリティのガイドライン文書の策定が総務省主導で進められており，その中間とりまとめ結果が「5G ネットワーク構築におけるセキュリティに関する対策等の留意点（令和 2 年度版）」として公表されている [5]．



■図 -7　プロトコルスタックの変遷

国内外の動向

さまざまな産業分野での活用が期待されている5Gの社会インフラとしての重要性はきわめて高いため，各国政府当局や関係機関では，5Gセキュリティに関して技術的な課題だけでなく，地政学上のリスクも含めたさまざまな取り組みを進めている．

米国では2020年春に「National Strategy to Secure 5G」を公表し，5Gにおけるサイバー脅威と脆弱性のリスク評価やサプライチェーンリスク管理等の政策を推進しており，特にサプライチェーンリスクが懸念される機器の排除やサプライチェーンの信頼性確保に向けて同盟国との連携を強化する動きが見られる．

欧州では2020年1月にEU委員会（European commission）がEUにおける5Gのセキュリティ課題に取り組むためのフレームワークであるEU Toolboxを発表している．Toolboxは5Gネットワークのセキュリティリスクに対処するために取り得る政策的手段や技術的手段をまとめたもので，EU各国に対してToolboxを利用した5Gシステムのセキュリティ対策を要請している．また，ENISA（欧州ネットワーク情報セキュリティ庁）はEU Toolboxの策定にあわせ，5Gにおけるさまざまな脅威の分析，カテゴリ，5Gネットワークの安全な設計やアーキテクチャ等，5Gのセキュリティに関する事項を網羅的かつ体系的にまとめた「ENISA Threat Landscape for 5G Networks」を公表した．現在，EU各国において5Gインフラの安全・信頼性確保のための取り組みを進めている．

国内では上述した5Gセキュリティガイドライン策定に向けた総務省の取り組みのほか，第5世代モバイル推進フォーラム（5GMF）のセキュリティ調査研究委員会において，ユースケース視点での5Gセキュリティ検討が行われ，白書「5Gユースケースにおけるセキュリティ第1.0版」が発行されている．また，ICT-ISACにおいても5Gセキュリティ推進グループが設置され，主にローカル5Gをターゲットに5Gセキュリティの情報交換やガイドライン文書の作成が進められている．

5Gセキュリティの今後

4Gコアを利用するNSAでスタートした5Gが，今後5Gコアを利用するSAに移行し，ネットワークスライスやMEC（Multi-access Edge Computing）等の5Gコアにより実現する新たな仕組みがさまざまなサービスや産業分野で活用されるようになると，社会インフラとしての5Gの重要性はますます高まっていくと想定される．重要社会インフラとしての5Gのセキュリティ確保には，5Gの技術仕様に閉じた議論だけではなく，仮想化やクラウド技術などの周辺技術のセキュリティや，サプライチェーンの信頼性確保など，広範な検討が必要であり，5Gを提供・活用するさまざまなステークホルダ間での情報共有や連携による継続的・長期的な取り組みが求められる．

参考文献

1）Rupprecht, D., Kohls, K., Holz, T. and Pöpper, C. : Breaking LTE on Layer Two, in 2019 IEEE Symposium on Security and Privacy(S&P), San Fransisco, CA, US (2019).
2）3GPP TS 23.501:System architecture for the 5G System (5GS), Release 16, v16.4.0 (Mar. 2020).
3）3GPP TS 33.501: Security Architecture and Procedures for 5G System, Release 16, v 16.2.0 (Mar. 2020).
4）Prasad, A. R. : Sivabalan Arumugam, Sheeba B and Alf Zugenmaier, 3GPP 5G Security, Journal of ICT Standardization, River Publishers, Vol.6, Iss.1&2.
5）総務省サイバーセキュリティタスクフォース（第31回）参考資料1（2021年5月）．

（2022年1月11日受付）

■窪田　歩（正会員）　ay-kubota@kddi.com

1995年国際電信電話（株）（現KDDI）入社．IPネットワークにおけるQoS制御，モビリティサポート，サイバー攻撃検知・対策技術等の研究開発に従事．現在，（株）KDDI総合研究所サイバーセキュリティGグループリーダー．2019～2020年本会理事．

特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

4 化学プラントのサイバーセキュリティ
―OT システムのセキュリティ脅威に対する取り組みと今後の展望―

応用 一般

星野浩志　秋元新哉
横河電機（株）

化学プラントに対するサイバーセキュリティ脅威の進化

ガートナーグループが公開した今後数年間のサイバーセキュリティに関する動向を予想した記事[1]の中では，2025 年までにマルウェアによるサイバー攻撃によって OT[☆1] 環境が兵器化し，人的被害が発生することを予想している．同社は，サイバー攻撃の影響がビジネスの混乱から人的な被害へとシフトし，最高経営責任者（CEO）の責任が問われる可能性に言及している．このような状況が現実化することは想像したくないが，ここ数年のサイバー攻撃者の OT 領域の知識の深化と，OT システムへのサイバーセキュリティ攻撃による社会生活への影響の発生事例を見ると，化学・石油プラント（図 -1）を取り巻くサイバーセキュリティ脅威は確実に進化していると言える．

化学・石油プラントに対するサイバーセキュリティ脅威が現実化した事例を 2 つ挙げる．2017 年にサウジアラビアで発生した石油化学プラントへのサイバー攻撃によるプラントシャットダウンがある．この事例では，プラントの緊急時自動停止を行う安全計装の専用コントローラへのマルウェア（TRITON）の感染が，プラントシャットダウンの原因であると特定されている．このマルウェアの開発には専用の組込み機器内部の設計・実装に関する深い知識を必要とすることが分かっている．攻撃者の真の意図はいまだに不明であるが，もしプラントが緊急時に安全に制御できない事態に陥っていたとしたら，人命や安全にかかわる問題に発展した可能性があった．

2021 年 5 月に発生した米国最大の石油パイプライン事業者である Colonial Pipeline 社へのランサムウェア攻撃の事例では，パイプラインが 6 日間の操業停止に追い込まれたことで，ガソリン供給不足の懸念から社会的混乱が発生した．この事態を受けて同社 CEO が米国上院国土安全保障・政府問題委員会で説明を求められた．Colonial Pipeline のインシデント事例で注目すべき点は，IT 環境側のインシデントが OT 環境側に影響を及ぼす前の段階で OT 側のシス

☆1 Operational Technology（OT）とは，産業用機器，資産，プロセス，イベントなどを直接監視・制御し，変化を検知・誘発するハードウェアとソフトウェアのこと（Gartner による定義）．

■図 -1　化学・石油プラント

テムを自ら停止したことである．しかもこの対応は，あらかじめインシデント対応プロセスとして定められていたという．OT 側のシステムを停止したのは料金請求システムが侵害されたためであるという報道もあり，業態によっては IT と OT のシステムの区分が難しい可能性があることが認識された事例である．

今後 OT ネットワークがさまざまなものとつながることでさらにサイバーセキュリティ脅威が進化し，社会的影響が生じる可能性が高まることが予想される．このような事態に継続的に対応していくためには，OT 分野のシステム・機器の知見や運用現場の人・プロセス・技術の知見と，IT 分野の知見の両方が必要になる．そこで本稿では，IT 分野の読者に向けて，化学プラントの OT システムである生産制御システムのサイバーセキュリティ関連の動向および課題と今後の展望について紹介する．

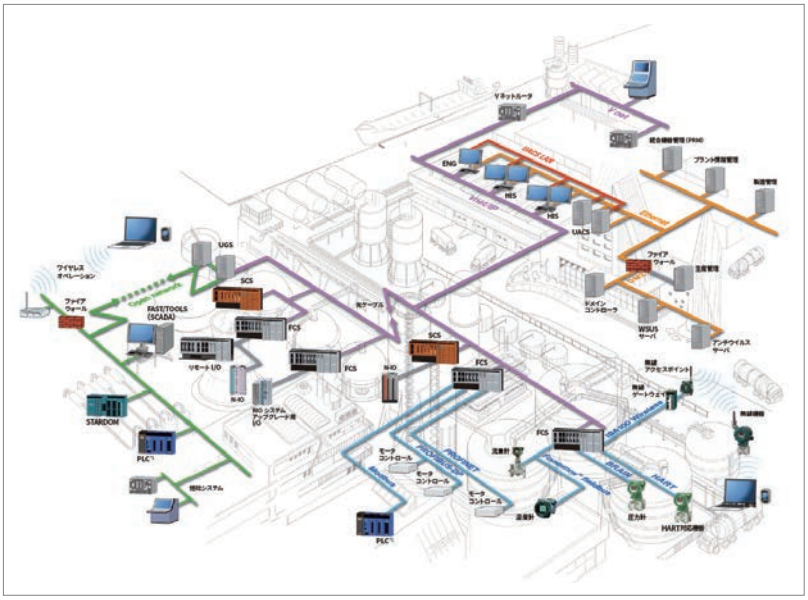
化学プラントの特徴とサイバーセキュリティの取り組み

化学プラントは自動車の組み立て工場などと異なり液体や気体を製造するもので，その多くが危険物質である．エチレンなどの基礎化学品の大量製造プラントから，素材に特殊な機能を持たせた高機能性化学品製造プラントまで化学プラントの姿は多様である．さらに石油化学・ガスまで範囲を広げると，石油精製プラント，油井，LNG（液化天然ガス）処理プラントおよび輸送用パイプラインなど幅広い．これらのプラントの自動制御[☆2]を行う生産制御システムには，以下のような特徴がある．

①広域に運用される多様な機器
② 20 年もの長期にわたる機器運用・保守
③リアルタイム制御
④無停止連続監視・制御

ここで言う機器には，広い工場の敷地に配置されたタンクや配管などの設備に取り付けられた温度・圧力等のセンサやバルブ，これらの PID 制御を行う分散制御システム（DCS）（図 -2），数千キロメートルにわたるパイプラインを監視する SCADA[☆3] システムがある．一般的な IT システムとの違いとしてよく強調される②③④には，プラントの運用において人命・安全・環境・品質への最大限の配慮が求められることが背景にある．

1970 年代から 1980 年代頃の化学プラントの生産制御システムでは，ベンダ独自のハードウェアと通信プロトコルを利用していた．1990 年代から 2000 年代にオフィス側の IT システムとのデータ交換やコストダウンの必要性から UNIX，Windows といった汎用 OS の活用や，制御通信への TCP/IP 等の汎用通信プロトコルの活用が進んだ．オペレータ用操作監視インタフェースやエンジニアリングワークステーションなどその実体は IT システムと変わらないものになり，その結果 IT システムと同様のサイ



■図 -2　工場内に設置されたセンサ・バルブ・分散制御システム（DCS）の例（横河電機 統合生産制御システム CENTUM VP カタログより）

☆2 「プロセス制御」や「プロセスオートメーション」という用語が使われる．
☆3 Supervisory Control and Data Acquisition

バーセキュリティ脅威にさらされるという状況に直面した．一方，前述の生産制御システムの特徴から，OS やアプリケーションのセキュリティパッチを頻繁に適用するような，IT システムで一般的に行われているセキュリティ対策の実施が困難な状況も見られた．その後 2000 年代に，米国で国土安全保障が喫緊の課題となったことから，重要インフラの防衛に関する問題意識が高まった．化学プラントにおいてもサイバーセキュリティ強化の機運が高まり，石油化学業界の主要企業等がプラントの生産制御システムに対するセキュリティ対策のベストプラクティスの収集や，セキュリティ技術対策・運用対策の標準化，人材育成に取り組むようになった．生産制御システムのセキュリティ対策・運用の国際標準規格である ISA/IEC 62443 シリーズはこれらの取り組みの成果の 1 つであり，IT 分野における情報セキュリティの国際標準規格である ISO/IEC 27000 シリーズや ISO/IEC 15408 に対比されるものである．現在 ISA/IEC 62443 は化学・石油・ガス事業者から生産制御システムのシステムインテグレータ，サービスプロバイダ，制御機器プロバイダまで広く参照・活用されており，さらに自動車工場，ビルオートメーションや鉄道等の分野で活用が広がっている．

スマートファクトリーの進展と制御システムセキュリティ

2010 年代後半になると，デジタル技術やクラウド技術の活用によって生産業務プロセスの改革や生産性・品質の向上を継続的に行うスマートファクトリーの実現を目指した取り組みが始まった．化学プラントでも，従来の PID 制御対象であるバルブや流量計だけではなく，さまざまなセンシング機能を持つ IoT 機器やロボット，ウェアラブルデバイスなどを使って，データを収集・分析したり，業務改善に活用したりする取り組みが進んでいる．この取り組みをさらに進めるために，生産制御システムのアーキテクチャをよりオープンで標準化されたものにする活動が始まった．この取り組み事例として，NAMUR Open Architecture（NOA）と Open Process Automation（OPA）の取り組み，およびセキュリティ対策の考え方を紹介する．

NAMUR Open Architecture（NOA）

NOA[2] は，欧州の化学メーカを中心とした団体である NAMUR が提唱する，生産制御システムのオープンアーキテクチャである．従来の生産制御システムの構造や利点に影響を与えることなく，新たに導入する IoT に組み込んだセンサ等を活用し，プラントの監視および生産の最適化を簡単かつ安全に行うことを目的としている．

NOA では既設の生産制御システムである CPC（Core Process Control）の外側に M+O（Monitoring and Optimization）と呼ばれる独立したドメインを付け加えている（図 -3）．M+O にはプラントごとの M+O（Plant Specific M+O）および各プラントを統合管理監視するために設置された中央の M+O（Central M+O）がある．プラントごとの M+O にある新しいセンサ（たとえば，振動，音響，腐食，匂いなど）やロボット，ドローンおよび既設システムからデータを収集し，M+O ドメイン内でこれらのデータを元に高度な制御，解析，診断を実現できることを目指している．

ドメイン間の通信は国際標準規格である OPC UA を採用し，さまざまな機器がセキュリティを確保しながらプラントごとの M+O に接続できるようにしている．NOA では ISA/IEC 62443 が提唱するゾーン分割の考え方を取り入れ，各ゾーンすなわちドメインごとに想定するセキュリティ対策のレベルを定めた上で，各ドメイン境界において必要なセキュリティ対策を取ることを求めている．具体的には M+O と CPC の間のデータ通信を，一方向のフローのみを許可するセキュリティゲートウェイによって制限する．これは特に安全面から重要な設備である CPC を，そ

れ以外のドメインから保護することを目的としている．またセキュリティゲートウェイおよび各ドメイン内の個々の機器については，ISA/IEC 62443 のコンポーネントに対するセキュリティ要求に基づいて，ユーザ認証・マルウェア対策・ログ機能等の必要なセキュリティ対策を実現することを求めている．

Open Process Automation（OPA）

OPA は石油化学大手事業者を中心とした団体である Open Process Automation Forum（OPAF）[3] が提唱する，新しい生産制御システムのアーキテクチャである．OPAF には，石油化学，医薬，紙パルプなどのさまざまな業種から，ユーザ企業，システムインテグレータ，ソリューションプロバイダなど約 130 の企業・団体が参加している．日本からは横河電機もこの活動に当初より積極的に参加しており，システムインテグレータとして石油化学事業者向けのテストベッド構築を担当するなどしている．

OPA のねらいは，標準に基づいた，オープンかつセキュアで相互運用可能な生産制御システムのアーキテクチャを構築することである．OPA では生産制御システムを構成するためのコンポーネントを柔軟に組み合わせたり置き換えたりすることが可能になる．これにより複数のサプライアが提供する製品の中から最適な（best-in-class）コンポーネントや最新技術を導入するなど，システム更新が容易になる．

そのベースとなるのが，OPAF が標準化を進めている O-PAS（Open Process Automation Standard）である（図 -4）．O-PAS ではハードウェアやソフトウェアなどのコンポーネント間のインタフェースを標準化することで，マルチベンダ間で相互運用が可能となる．OT 分野だけでなく IT 分野からも生産制御システム・機器への参入が進み，新たなイノベーションや付加価値のあるソリューション・サービスの提供が促進されることも期待される．

OPAF では，生産制御用機器の設計段階からインテグレーションされたかたち（Secure-by-Design）でセキュリティを浸透させることを目指している．これは，後付けでのセキュリティ対策が複雑かつ高コストになりがちであるという課題を解決するた

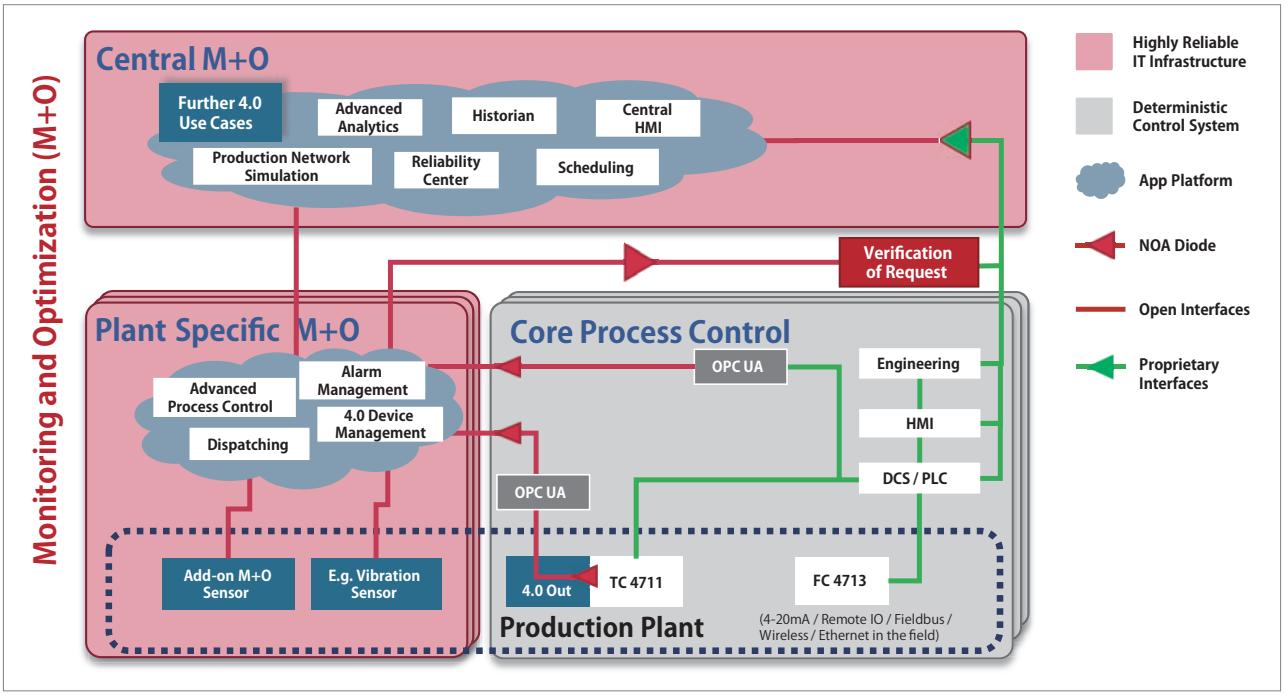
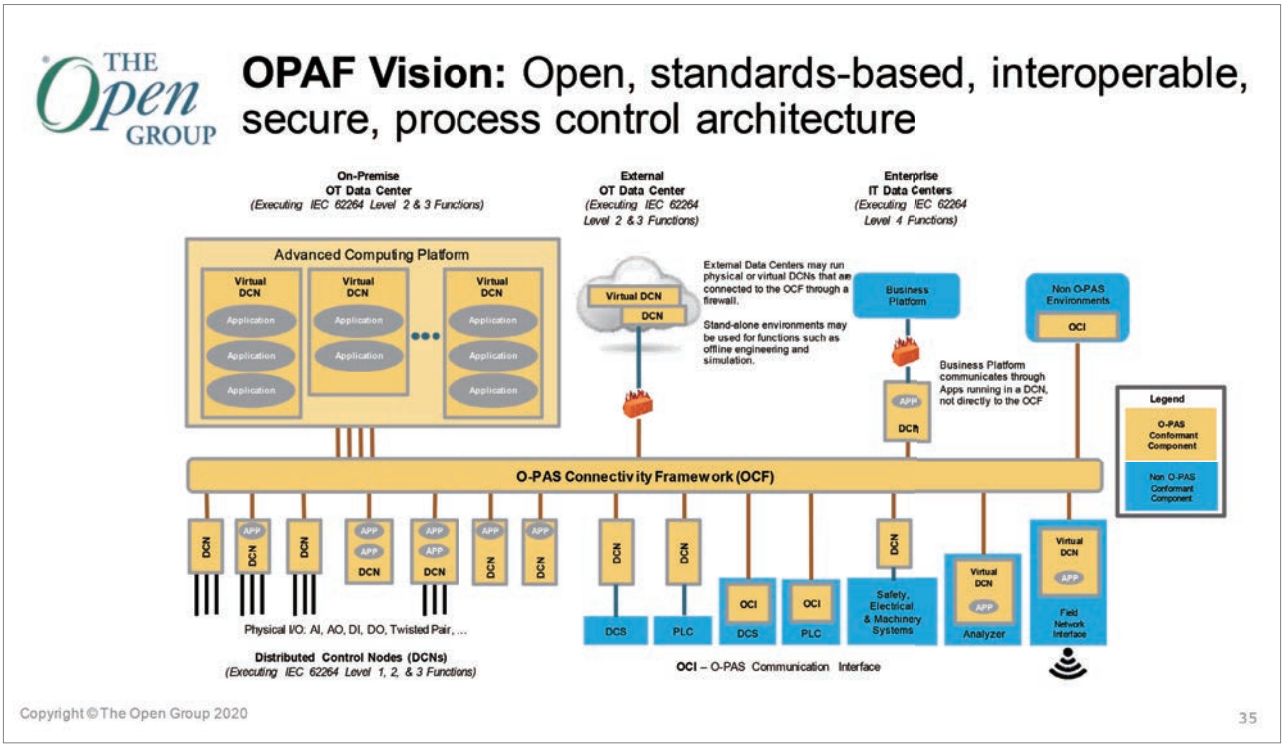


図 -3　NAMUR Open Architecture（NE 175:2020 NAMUR Open Architecture – NOA Concept より引用）

めの取り組みである．O-PAS では前述の NOA と同様にサイバーセキュリティのフレームワークとして，国際標準である ISA/IEC 62443 をリファレンススタンダードとして採用しており，各制御機器のセキュリティ要件とセキュアな制御機器開発ライフサイクルが標準化されている．各ノード間の通信およびデータの情報モデルについても国際標準規格である OPC UA を採用し，セキュアなデータ交換を実現している．これにより制御機器サプライアから一貫性のあるセキュリティ機能を備えた O-PAS に準拠した制御機器が提供されるようになり，サイバーセキュリティに強い生産制御システムの基盤となる．化学プラント事業者は，事業に適したセキュリレベルと必要なセキュリティ要件を決定し，システムインテグレータはエンドユーザの機能・セキュリティ要件を満たすべく生産制御システムの構築を行うことが可能となる．

課題と今後の展望 - IT と OT で求められること

化学プラント業界においても他の製造業と同様に，生産効率向上の追求やプラント運用管理の人員不足への対応が求められている．このような背景から，プラントから得られるさまざまなデータの生産現場における活用や，リモートアクセスの活用，現場の作業員の支援のためのデバイスの導入などが進展し，スマートファクトリーの実現に向かう．このような環境においては，従来の生産制御システムで一定の効果を発揮した境界防御型のセキュリティ対策はいずれ限界を迎える可能性がある．このようなことを想定して，境界内外を問わずすべてのサイバーセキュリティ脅威から制御機器や制御機能・データをきめ細かく守るためのゼロトラストセキュリティ対策などの新しい技術も常に視野に入れて取り組む必要がある．ただし，化学プラントの生産制御システムの長期にわたる機器運用の状況から見て，すぐにすべ



■図 -4　OPAF Vision（ARC Industry Forum 2021 より引用）

てを実現できるものではないため，現実に即して境界防御も含めた多層防御対策と，運用体制の構築・維持，事業継続計画立案が必要となる．これを実現するための国際標準や技術対策はすでに存在している．化学プラント事業者には，制御機器プロバイダ・システムインテグレータとともにセキュリティ脅威・対策技術の進展について知見を共有し，プラントオペレーションへの影響を最小におさえつつ，段階的に新しいセキュリティ対策を取り込んでいく取り組みが求められる．この取り組みを推進するためには，化学プラントの自動制御の根幹である OT システムにおける機器の設計・実装，システム構築，サービス提供の分野に，IT の知見を組み込んでいくことが必要になる．今後この分野にはさらに IT の知見を持つ人材が必要になる．

IT と OT の関係については，IT-OT Convergence によってプラント事業者内の IT，OT 部門の組織・技術のすべてを 1 つに集約すべきであるという意見がある．OT の世界に IT の知見が必要であることは間違いない．一方で前述の通り化学プラントの生産制御システムには一般的な IT システムとは異なる特徴があり，IT 用のセキュリティ対策ツールをそのまま導入すればよいわけではない．たとえばプラントの現場において，IT 用ツールのアラームメッセージを，人命やプラントの安全にかかわるものと同列に扱って良いかの判断は非常に難しい．

IT と OT のそれぞれの特徴や組織・文化の違いをふまえて，1 つの企業の中で統制のとれた効果的なセキュリティ対策を行うためには，IT と OT の組織・技術を 1 つに集約するのではなく，IT と OT の組織がそれぞれ独立した上で，経営層のリーダシップのもとに連携していくことが必要となる．現在，ISA/IEC 62443 の原案を作成している ISA99[4] において，プラントを運用する事業者企業のセキュリティリスクマネジメント体制の中で，IT と OT それぞれのエリアで個別に適切なセキュリティ対策をしつつ，共通のフレームワークを活用する方針が提唱されている．具体的には 1 つの企業の中で IT，OT を含めた ISO/IEC 27001，27002（ISMS）に基づくセキュリティ管理体制を構築した上で，IT エリアに対しては ISO/IEC 27001，27002 に基づくセキュリティ管理策を導入し，OT エリアに対しては ISO/IEC 27001，27002 と ISA/IEC 62443 の中から OT の生産制御システムの特徴をふまえたセキュリティ管理策を導入するというものである．将来的にこのような取り組みが実際の企業活動の中で行われることで，化学プラントに対してより効果的なセキュリティ対策が導入される体制が構築されることを期待して，本稿の締めくくりとする．

参考文献

1）The Top 8 Cybersecurity Predictions for 2021-2022, https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
2）NAMUR Open Architecture, https://www.namur.net/en/focus-topics/namur-open-architecture.html
3）OPAF（Open Process Automation™ Forum）, https://www.opengroup.org/forum/open-process-automation-forum
4）ISA99, https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

（2021 年 12 月 28 日受付）

■星野浩志　Hiroshi.Hoshino@yokogawa.com

1992 年東京農工大学大学院工学研究科電子情報工学専攻修了，同年横河電機（株）入社．社内 PSIRT 体制構築等を経て，制御システムのセキュリティ対策の提案と国際標準化活動に従事．CSSC 評価認証・標準化委員会委員．IEC/TC 65/WG 10 国内委員会幹事．

■秋元新哉　Shin-ya.Akimoto@yokogawa.com

2008 年慶應義塾大学理工学研究科基礎理工学専攻修士課程修了，同年横河電機（株）入社．製造業向けソフトウェア開発等を経て，石油化学大手向け OPA テストベッドの立ち上げ，サイバーセキュリティ・IT 基盤ソリューションの開発に従事．

特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

5 産業制御システムセキュリティの動向

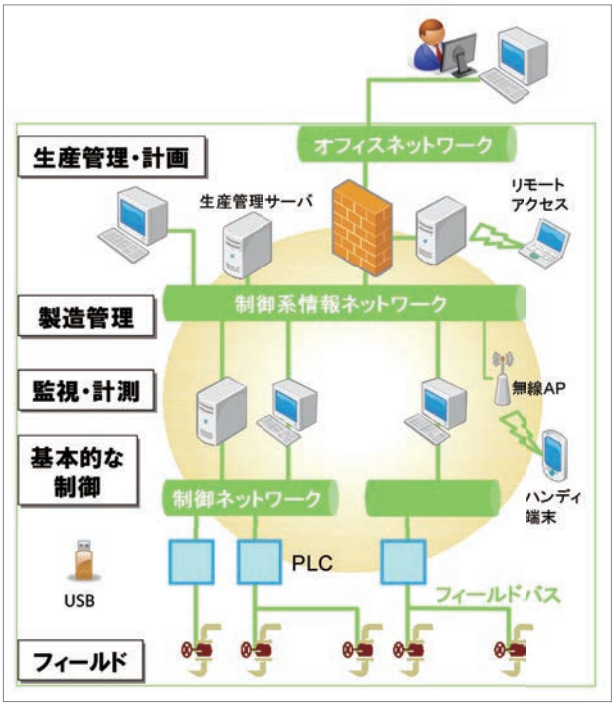
応般

新　誠一　電気通信大学

産業制御システム

電気やガス，水道，交通などの重要インフラや製品や部品，素材などを作る工場は社会生活に不可欠なものである．停電，断水，通信障害などに加え，食品，薬品，日用品，家電などの供給ひっ迫は，個人の生活や社会生活を停滞，停止させてしまう．あるのは当たり前，なくなって初めて受けている恩恵を自覚するものである．

そこでもコンピュータを中心とする計算機システムが幅を利かせている．具体的には，生産指示，燃料や材料などの残量情報，圧力や温度，流量などのセンサ情報などの内部の情報に基づいて操作情報を計算してゲートやバルブなどを制御する．これを産業制御システムと呼ぶ（図 -1）．このシステムの要素となる機器を産業制御機器と呼ぶことにする．対比となるネットワークとサーバおよび端末までのシステムを情報システムと呼び，そこに使われる機器を情報機器と呼びたい．図 -1 の上部に焦点を当てたものが情報システム，下部に当てたものが産業制御システムとお考えいただいてもよいと思う．そして，本稿の趣旨は，図 -1 全体に焦点を当ててサイバーセキュリティ対策を講じてほしいというものである．



■図 -1　産業制御システムの例

図 -1 の下部層では，温度や圧力などのセンサ情報に基づいて PLC（Programmable Logic Controller）がモータや油圧弁などのアクチュエータを操作する．ちなみに，PLC は自動車制御では ECU（Electrical Control Unit），家電などでは組込ボードに相当する．これらは一般にコントローラと呼ばれる．このコントローラレベルでは実時間性が必須である．たとえば，ミリ秒単位でセンシングし，操作をするものである．

この操作の実時間維持のために特殊な OS が用いられている，そのため，汎用のアンチウィルスソフトなどが使えなかった．さらに，工場などは油圧や空気圧による自動化から電動化・情報化という歩みを進めてきた．いわば，内部からの進化であり，外部接

続を目的とするものではなかった．このため，初期段階ではサイバー攻撃に対する配慮は薄かった．つまり，産業制御システムにおけるサイバーセキュリティ対策は，ネットワーク接続が前提となっている計算機システムとは違った捉え方をされてきた．

しかしながら，コンピュータ自体の高性能化，低価格化，堅牢化という発展と産業制御システムの横への拡大が様相を変えつつある．具体的には，IoT やコネクテッドと呼ばれるネットワーク利用の時代の到来である．家庭での質の高い生活や事業所などの高効率の生産活動の保証のために，天気などの環境情報，需要予測，燃料や部品供給情報などの外部からの情報が産業制御システムでも不可欠であり，ネットワーク接続なしでは工場は立ち行かない．以下，この辺の事情をもう少し詳しく見ていこう．

まずコンピュータの発展であるが，これは現代社会に不可欠なスマホに象徴される．100Mbps 以上の無線通信能力，数十 GB 以上の記憶能力，そして数 GIPS（Giga-IPS/billion Instructions Per Second）のマルチコア CPU（Central Processing Unit）を中心とし，GPU（Graphic Processing Unit），NPU（Neural Processing Unit）まで加えた処理能力．さらに GPS や高感度マイク，高精細カメラなどのセンサに NFC（Near Field Communication）に Wi-Fi，Bluetooth などのネットワーキング．それが手のひらサイズに収まり，クラウドがバックを支える魔法の道具，それがスマホである．

産業制御機器のコントローラは，ここまで進んでいない．しかし，影響を受けて変わりつつあるのも確かである．簡単に言えば，産業機器のパソコン化[1)]である．将来を見れば，クラウド化，スマホ化も視野に入れなければならない．

次に拡大である．ここでは拡大を物づくりのサプライチェーン化による広域連携であり，原材料費や需要変動までも考慮する最適化と捉える．簡単に言えば，現在の重要インフラや工場はネットワークなしでは稼働しない規模と精密さの下に運営されているという現実である．そして，インフラや工場などの停止はビジネスを止めるだけでなく，市民の生活も脅かすことは，災害が常態化している世界の共通認識である．

実は情報機器と呼ばれるものも実時間性が不可欠である．たとえば，株式の売買システムは HFT（High Frequency Trading）と呼ばれるマイクロ秒のつけ合いを間違いなく，確実にこなす必要がある．同様に，スマホを支えるネットワーク網も実時間性が不可欠である．この確実性がなければ，エレクトリックコマースもインターネットバンキングも意味をなさない．

以上の動向から，これまで情報システムと産業制御システムと区別していた時代から，両者を一体として扱わなければならない時代を迎えていると言ってよいだろう．産業制御システム側から見ると，Windows または Linux などの汎用 OS への収斂であり，イーサネットなどのインターネット技術へのネットワークの収斂である．このことは，産業制御システムへのサイバーセキュリティ対策の必要性を示している．逆に情報システムから見ると，エッジの先まで含めたリスクアナリシスとそれへの対策の必要性である．

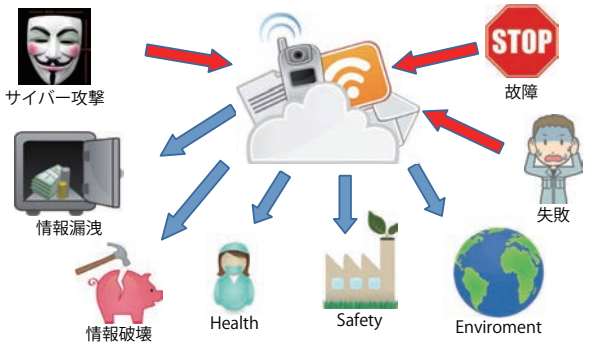
後者について，少し説明を加えると IS と呼ばれる情報システムを扱う部署の方々の関心は従来，サーバとネットワークと端末を視野にしていた．それに対し，クラウド，IoT デバイス，サプライチェーンと広がり，現在はセンサ，アクチュエータへのサイバーセキュリティをも視野に入れなければならないということである．

一方，産業制御機器の視点に立つと，閉鎖系であること，独自 OS であることを言い訳に十分なセキュリティ対策をしてこなかったことを見直す時期にきているということである．閉鎖系はリスクである．つなげば感染するリスクが生じる．そして，独自 OS もリスクである．サイバー攻撃リスクに対して十分な検査が行われていない可能性がある．それだけでなく，通信スタックや暗号化などを後付けしているために，OS やミドルウェアの全貌を把握できなくなってきている．中には，OSS（Open Source Software）が使われてい

ることを把握されていない場合や国外の会社が制作に関与していることも把握されていない可能性がある．一言で言えば，作成した会社も独自 OS の脆弱性を把握できていない．

実は情報システムも規模が大きくなりすぎている．そのため，脆弱性の種は尽きない．そこで，パソコンやスマホでは，頻繁にセキュリティアップデートが行われている．しかし，産業制御システムでのアップデートは難しいと言われてきた．24 時間，365 日休みなく稼働させなければならないのが，産業制御システム．しかも，不具合が起きれば，市民生活，生産活動にすぐに支障が出るのが産業制御システム．このため，十分なセキュリティアップデートが行われていない可能性が高い．それどころか，アップデートそのものを想定していない産業制御機器も多い．

以上を見ていくと，情報システムの方にアドバンスがあるように見える．しかし，人や社会の生命に直接かかわる産業制御システムのアドバンスももちろんある．それが HSE（Health, Safety, Environment）を守ることを軸に据えた機能安全である．産業機器において当たり前の機能安全にサイバーインシデントを加えたリスク解析と対策．同時に，情報セキュリティ解析に，エッジ下まで含んだリスク解析と対策を加えるべきということが本来の市民活動や生産活動を守るということである（図 -2）．安全とセキュリティの癒合



■図 -2　サイバーセキュリティ

であり，長年提案してきたことである [2]．ここに，ようやく両者が 1 つに収斂しつつあるということが，私が見る最近の動向である．

攻撃の変化

このような収斂の必要性は，重要インフラなどへのサイバー攻撃の様相の変化からもうかがえる．この変化を簡単に言えば，流れ弾から狙い撃ちである．または，拳銃から突撃銃である．拳銃からの数発の乱れ打ちなら，隠れていれば済むこともある．当たるのは運の問題と割り切ることもできた．しかし，突撃銃を持った戦闘員に襲われたら一般人はたまらない．

ちなみに，突撃銃は自動掃射と狙撃の二通りの攻撃が可能である．弾幕を張って一網打尽とする攻撃と静かに一発で距離を置いて仕留める攻撃である．この組合せもあるので，攻撃が高度化したと見ることもできる．

具体的にはランサムウェアと呼ばれる身代金攻撃に見て取れる．ご承知のように，攻撃を受けるとシステム内のデータを暗号化して使用できなくするものである．そして，復号化のために身代金を要求するものである．

対抗策はバックアップであった．元データがあれば，身代金を払う必要はない．しかし，最近の攻撃は，暗号化だけでなくデータ暴露も組み合わせている．お客様の個人情報やユーザの設計情報などを暴露すると脅しをかけているようである．さらに，ユーザにも脅しをかけて，暗号化された会社に身代金を払うように圧力をかけるという手の込んだ攻撃が相次いでいる [3]．

さらに，重要インフラ企業を狙って攻撃することで，インフラが停止する事態も引き起こしている．インフラは設備だけでない．顧客などの管理が伴わなければ稼働できない．この管理系のデータベースが暗号化されてインフラとしての使命を果たせなくなった事例も出現している．

もう1つの顕著な特徴はネットワーク管理機器やVPN（Virtual Private Network）などの脆弱性を突いた攻撃である．産業機器や社内ネットワークでは城壁を築けば，中は平穏という考え方をとってきた（図 -3）．しかし，城は外部との交流なしでは存続できない．だから門があり，警備する衛兵がいる．現在，この門には大量の出入りがある．数GBのデータが複数のポート，プロトコルを通じて出入りしている．ポートは門，プロトコルは出入りする種類，人，馬，荷物，破棄物だと思えばよいだろう．その門が多数で出入りが大量なら衛兵も見過ごす．それも，攻撃者は手を変え，品を変えて攻撃を仕掛けてくる．しかも，定常状態ばかりではない．在宅勤務が増えれば，容量アップ，危険情報が出れば警戒レベルアップ，故障に，テストに，設定変更．対応する衛兵であるネットワーク管理者は大変である．

情報機器でも，産業制御機器でも管理者は常に攻撃にされていることを痛感している．ファイアウォールの設定を1つ間違えば，瞬く間に感染が広がる．城壁に頼れば頼るほど，城壁に穴があいたときの被害は甚大である．VPNに頼れば頼るほど，その認証や暗号化に弱点があったときの被害は甚大である．実際，そのような攻撃が増加している．

このような脅威にさらされ，24時間，365日の対応をせざるをえない管理者が頼るのがネットワーク管理ソフトである．手動から自動へというDXの流れはセキュリティ対策にも及んでいる．

現在，このソフトが狙われている．管理ソフトもソフトである．そこには，必ず脆弱性が存在する．それを見つければ，その管理ソフトのユーザ企業に侵入したりなどの攻撃が可能である．最近，この管理ソフトの脆弱性をついた攻撃も増加している．桃源郷はない．仮にあったとすると，それは攻撃者にとって美味しい世界である．この桃源郷の住人は善人しかいない．ひとたび，悪人が混じれば阿鼻叫喚となる．これが，今の重要インフラや工場が置かれている現状である．

対策の変化

さて，以上の現状認識の下，その対策が気になるだろう．城を作る．それは水際対策．その対策が破綻する可能性がある以上，ファイアウォールやVPN以上の対策が求められる．続いて，その話をしていこう．

現在，対策側の合言葉は「Zero Trust」である（図 -3）．「何も信用するな」ということである．イントラネットも，孤立も，VPNも過信するなということである．一義的には，「自分の身は自分で守れ」ということである．ファイアウォールをネットワークレベルから自分，個，エッジレベルまで押し下げることである．

まず，最新のセキュリティアップデートを施して頑健とする．そして，外部との通信ポートは1つに制限する．さらに，通信プロトコルも1つに絞る．具体的には，HTTP（Hyper Text Transform Protocol）を使って，文字列のやりとりのみを行う．

これらの制限はセキュリティ対策で必須である．たくさんのポートやプロトコルではなく1つだけと決まれば，チェックしやすい．加えて，交換されるデータが文字列，つまり人が読める形式であれば，これもチェックしやすい．もちろん，セキュリティ対策だけでなく，バグ対策にも有効である．この制限は，計算能力を可読性，人に分かりやすくする方向に使うという第一歩である．

これをWindowsで言えば，DCOM（Distributed Common Object Model）から.NETへの移行に対応する．この移行はWindows XP時代に処置された．その意味で，古いOSは危険である．もちろん，常に最新のアップデートを行うことも必須である．

このアップデートは，OSとアプリのコンフリクトと

ファイアウォール，VPN
↓
End Point Security, 侵入検知，SOC

図 -3　水際対策から No Trust

いう大きな問題を生む．その対策は，アプリ制作側が OS の正規の API 内で動作するような開発を進める必要がある．画像メモリなどを直接アクセスしたり，TCP/IP スタックをいじったりすれば高速化することが可能であるが，それは OS のアップデートに支障を及ぼすし，セキュリティ対策という面からも問題である．このことから分かるように，複数の OS などで使えるアプリは正しく API を使っている可能性が高い．

このような対策を講じても OS とアプリのコンフリクトが生じる可能性がある．アプリ開発側が新しい OS での動作を常に確認するとともに，使用側もコンフリクトの可能性を視野に入れたアップデートが必要である．

その際，止められない産業機器でどのようにアップデートしていくかという技術が大事である．最前線では，情報機器のアップデートを参考にした対策が実行されている，たとえば，定期的に停止してアップデートを行う．また，事前に仮想 OS 上で，ほかのアプリとのコンフリクトのチェック．さらには，二重化した片方だけをアップデートする．様子を見て，もう片方もアップデートするなどである．エンジニアリングとはできない理由を探すことではない．エンジニアリングとは難しい問題のソリューションを構築していくことである．言い訳ではなく，解決が情報技術者にも産業制御技術者にも求められている．

以上は，重要インフラや工場というよりは情報システムセキュリティのイロハとも呼ばれる対策である．次に，主題の産業制御システムのセキュリティ対策を考えていこう．

産業制御システムが使われる場では，産業制御システムも，情報システムもおまけである．主人公は，建物や設備などの現物系である．費用は現物が中心であり，数十年使われる物は当たり前．だから，予算も数十年置きというのが昭和時代の実態である．更新周期が早い情報技術とは相性が悪い，さらに，セキュリティ系はおまけの情報システムのさらなるおまけ．できれば，費用をかけない理由を探す向きが多い．

さて，汎用ではない OS．誰が使っているのだろう．部品取りは古い機器維持の基本．破棄された産業用機器をもらい受けるのは，善人だけではない．悪人も欲しい．手に入れたら，種々の攻撃をして弱みを探すのが彼らの仕事．ベンダは汎用ではない OS の維持にお金をかけられるのだろうか．それだけの資金をユーザがお出しなのだろうか．古い機器は内部にパスワードが書かれているものもある．バッファオーバフロー攻撃に，DoS 攻撃．どこまで可愛い汎用ではない OS は耐えられるのだろうか．

そして，独自 OS の脆弱性を常に見守り，対策をし，アップデートまで行う負担は独自 OS 作成会社には負担が大きすぎる．Windows や Linux は利用者が多いから，この負担に耐えている．このことから，産業制御機器の OS も汎用化していくのは当然の流れと思われる．

目立たなければ大丈夫．本当に？　頭かくして尻隠さず．インターネット利用を拒否して生きていくのでなければ，隠れて生きていくのは不可能である．そして，隠者に守るべき資産があれば美味しい．頭を隠すような会社は，被害を隠そうとする．まさに，ランサムウェアの狙いどころである．

リスクアナリシスを行おう．予算が限られているなら，対処できていないリスクが現実化したときの対応を整理しよう．あきらめるのか，謝るのか，逃げ出すのか，それとも．また一からやり直すのか．

さらなる変化

桃源郷を守る情報技術が，ファイアウォールに VPN にパスワード付き ZIP ファイル．これらは，新型コロナウイルス対策で唱えられた水際対策そっくりである．有効であるが，破られたときの対策も講じないと全滅する恐れがある．

ファイアウォールも守る IS の苦労を CIO や CISO はご存じなのだろうか．変わる攻撃，変わる需要，ルータやスイッチの故障などに応じて設定を継続的に変え

なければならない．そして，その設定を間違えれば悲惨な結果を招く．24 時間，365 日の苦労は産業機器の維持管理をするエンジニアの苦労と変わらない．IS のエンジニア，現場のエンジニア，やっていることは同じである．ぜひ，仲良く産業機器を守ってほしい．

この大変さのため，自動で設定を変えてくれるセキュリティツールの利用が増えている．もっとも，このツールもソフトウェア．VPN もソフトウェア．いずれも，脆弱性と呼ばれるサイバー攻撃への弱みを抱えている．

ランサムウェア攻撃への対策として，USB メモリを使わない．変なサイトに接続しない．怪しいメールの添付ファイルを開かないというような水際の対策．次に感染した場合にファイルをミラーリングしておく対策．さらに，違う OS や違うデータベースを利用するヘテロ利用により感染を押さえる対策など多重坊業が施されている．もちろん，データベースの暗号化は必須である．さらに，前述の zero trust が現在のセキュリティベンダーのバズワードである．城壁は破られる．だから，内部の物も信用するなということである．ファイアウォールや VPN の内部機器の入出力，振舞いを監視し，異常を見つけたら警報を出したり，切断したりなどの対処をする．

特徴は監視機能である．この機能をシステムの内部に置くか，外部に置くかで扱いが変わる．前者の場合，内部だけで完結できる分かりやすさが特徴である．もっとも，監視機能もソフトウェア．OS やアプリが感染するなら，監視機能も乗っ取られる恐れがある．そこで，外部に監視機能を置くケースも考えられる．これは，オペレーションセンターであり，セキュリティに特化したものを SOC（Security Operation Center）と呼ぶ．

オペレーションセンターは IoT 時代には欠くことができない設備である．IoT を売った後も課金を続けるものと位置づけると，オペレーションセンターがなくてもビジネスができない．そこに，アップデート機能，監視機能を置くと SOC の役割を果たすことができる．

監視機能をソフトウェアである．SOC が乗っ取られたらどうするかも考えなければならない．鼬ごっこには深読みが必須であり，どこまで深読みしたかの勝負である．

サプライチェーン

SOC の設置は問題となっているサプライチェーンのセキュリティ確保でも有効である．これはプリントボード 1 つとっても多数のプレイヤがかかわっていることによって生じるセキュリティ問題である．IC 回路を設計する会社，それを元にウェハーを作成する会社，そのウェハーを切り出しパッケージにする会社，そのパッケージをボードに実装する会社．さらに，そのボードを動かすソフトの上位設計する会社．そこにさまざまな会社のファームウェアやミドルウェアを結合してボードに実装する会社．そして，このボードを複数使用して産業医機器が構成されている．さらに，この機器がネットワーク化されて産業システムとなっている．

このどこかの工程でバックドアやトロイの木馬と呼ばれるマルウェアや物理的なタッピングがなされると意図しない脆弱性が形成される．しかも，ハードもソフトもグローバル調達である．Windows OS だけで数億行，最新のチップセットは数十億個のトランジスターという状況を鑑みれば，産業システム全体を把握してる方は皆無である．それは，機器に限っても同様であり，ソフトに限っても同様であり，ハードに限っても同様である．

何か仕掛けられている可能性がある部品を含めて産業機器を構成し，産業システムを稼働させることは大変難しい．しかし，その難しさを踏まえて，全・安心に稼働させている枠組みも存在する．それが，産業システムの機能安全である．どのような部品や機器があるかというアセットを把握し，HSE（Health, Safety, Environment）へのリスクを解析する．その上で，各部品や機器が満足すべき機能を明確化する．

この段階でソフト側が注目しているのが，HAZOP で

あり，FTA であり，FMEA などの解析手法である．いずれも，産業制御システムで使われている手法である．それをソフトのバグ解析に使われ始めている．もちろん，サイバーセキュリティ解析にも有効である．ぜひ，図 -2 の見方で活用いただけると嬉しい．

水道情報活用プラットフォーム

産業制御システムのセキュリティ対策の進み具合は産業ごとに凸凹がある．自由化が進んでいる電力やガスは行政の支援もあり進んでいる．しかし，内閣サイバーセキュリティセンターが定める重要インフラ全般には普及していない．現在，水道業界では人口減対策などから産業制御システムのプラットフォーム化が進んでいる[4]．正に，図 -1 の上も下も含んだ形のプラットフォームである．上部は課金やアセットマネジメント，下部は制御用のネットワークまで含む垂直型のプラットフォームである（図 -4）．

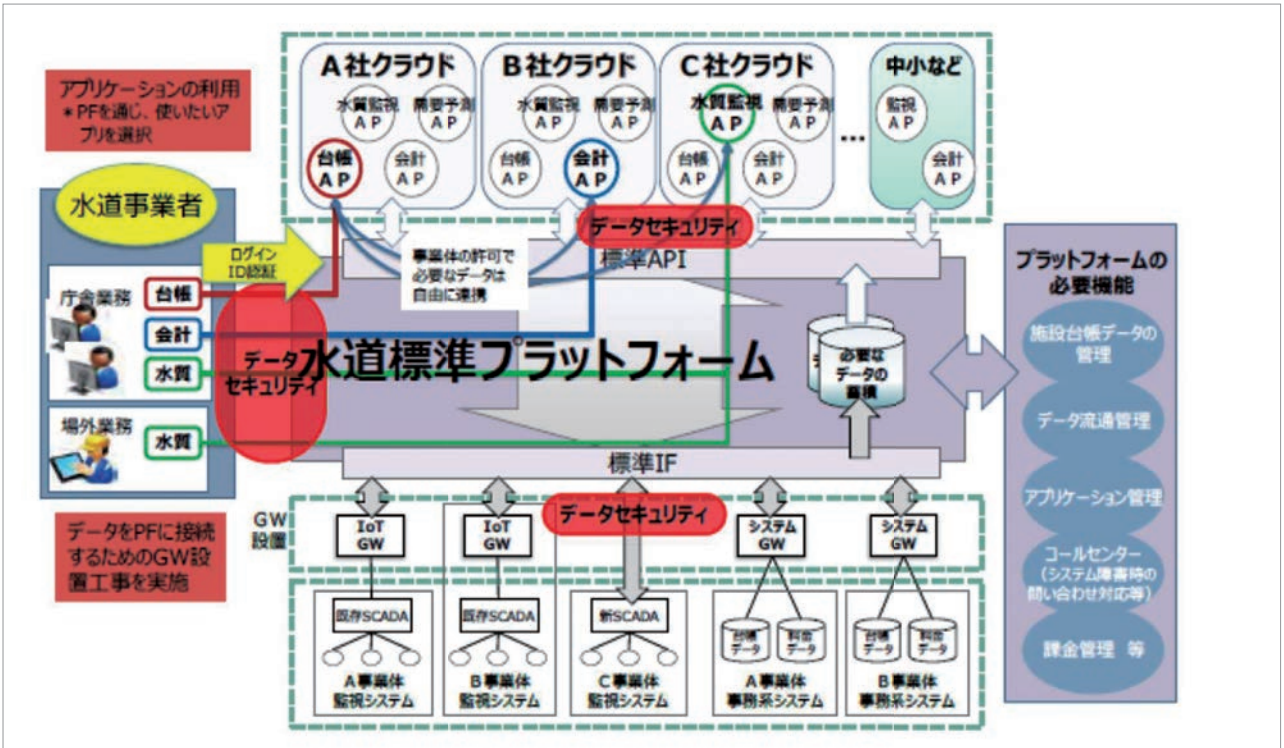
このプラットフォームは OPC で各種制御用ネットワークの差異を吸収し，NO（Not Only）SQL 仕様でデータベースの差異を吸収する構成である．管理者の不足をプラットフォームが担うとともに，プラットフォームのセキュリティは提供者である JECC が担う．

このプラットフォームを水道事業に普及させていくと同時に，ほかの事業にも広げていくことが私の現在の活動の 1 つである．これを本稿の締めくくりとさせていただく．

参考文献
1）電気学会編：公共プラントとパソコン応用－その光と影－，コロナ社（2001 年）．
2）新　誠一：社会インフラへのサイバー攻撃に対する課題と取り組み，情報処理，Vol.55, No.7, pp.640-646（2014）．
3）日経新聞：サイバー身代金，支払い 5 割　金額急増し攻撃に拍車応じた企業，米 87%，日本 33%，2021 年 9 月 20 日朝刊．
4）https://www.jecc.com/service/list/ws-platform.html

（2022 年 1 月 5 日受付）

■新　誠一　seiichi.shin@nifty.com
2020 年電気通信大学名誉教授．2013 年から 2020 年まで共同研究組合制御系セキュリティセンター理事長．2020 年水道情報化活用研究会会長．2021 年（株）アイシン社外取締役．



■図 -4　水道情報活用システム（https://www5.cao.go.jp/keizai-shimon/kaigi/special/reform/wg6/20200324/pdf/shiryou3-1-1.pdf）

特集
Special Feature

［社会インフラシステムにおけるサイバーセキュリティ―レジリエントで持続可能なデジタル経済社会に向けて―］

6 金融分野におけるサイバーセキュリティを巡る国際的な議論の動向

応 般

河田雄次　金融庁

金融に関する国際的な議論の枠組み

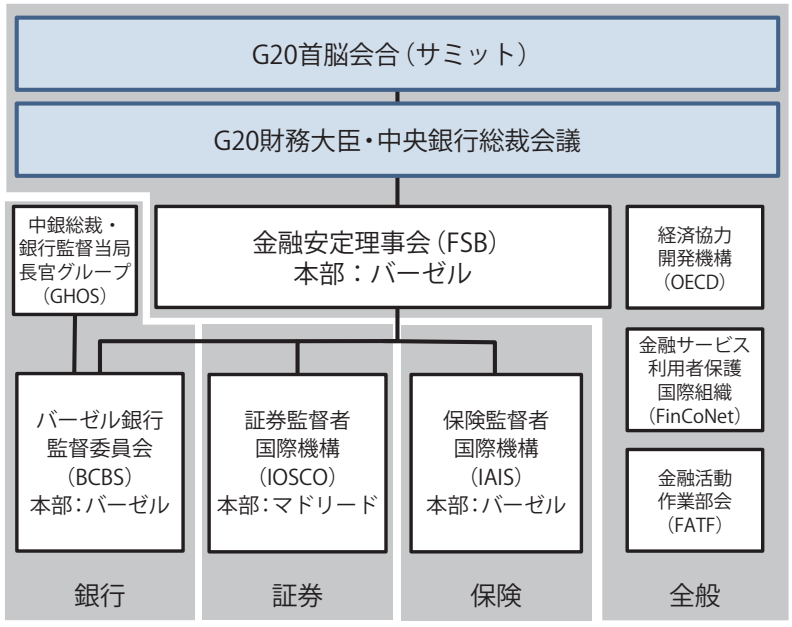
金融分野における幅広い世界共通の課題にかかる国際的な議論は，「国際経済協調の第一のフォーラム」であるG20をはじめとするさまざまな場において行われている．具体的な議論の紹介の前に，本稿では，まずその概観を整理したい（図-1）．

G20

G20とは，2008年のリーマン・ショックに端を発する金融危機をきっかけに，危機対応や規制監督の改革等について，それまでのG7（日本，米国，英国，ドイツ，フランス，イタリア，カナダ）を超えた新興国を含む幅広いメンバで議論するために設置された，20カ国・地域（G7の主要7カ国に加え，アルゼンチン，オーストラリア，ブラジル，中国，インド，インドネシア，メキシコ，韓国，ロシア，サウジアラビア，南アフリカ，トルコ，欧州連合）からなる国際フォーラムである．2008年の第1回G20首脳会合以降，G20は国際経済協力に関する「第1のフォーラム」として定例化されている．

近年では，年1回の首脳会合（以下，サミット）と，年数回の財務大臣・中央銀行総裁会議が開催され，サイバーセキュリティのほか，国境を越えて広く利用されるような新たな形態のデジタルマネーであるグローバル・ステーブルコインへの金融規制監督の在り方，新型コロナウイルス感染症への対応施策の協調，サステナブルファイナンス，クロスボーダ決済の改善，金融包摂等が幅広く議論されている．

後述する金融安定理事会や基準設定主体がとりまとめた報告書や指針，基準等は，G20サミットやG20財務大臣・中央銀行総裁会議の共同声明で国際合意として盛り込まれる場合も多い．



■図-1　国際的な議論の枠組み―文献1）を参考に作成

金融安定理事会（FSB）

金融安定理事会（Financial Stability Board，以下FSB）は，1997年に発生したアジア通貨危機の経験を踏まえて1999年のG7での合意に基づき設立された金融安定化フォーラムを前身とする国際組織であり，リーマン・ショックを契機に，メンバをG20の財務省・中央銀行・監督当局や他の国際組織などに拡大・改組する形で2009年に設立された．FSBは，G20からの要請に基づき，国際的な金融システムの安定に資する取り組みを行うとともに，基準設定主体における作業の調整等を行う．

G20の節で挙げた通り，さまざまなテーマについて検討を行っているが，サイバーセキュリティに関しては，2017年以降，取り組みを本格化させている．

基準設定主体

金融分野では銀行や証券，保険などのセクタ別に，規制監督に関する国際原則，指針や基準等を策定する基準設定主体（Standard Setting Bodies，以下SSB）と呼ばれる国際組織が存在する．具体的には，銀行規制監督に関するバーゼル銀行監督委員会（Basel Committee on Banking Supervision，以下BCBS），証券市場規制監督に関する証券監督者国際機構（International Organization of Securities Commissions，以下IOSCO），保険規制監督に関する保険監督者国際機構（International Association of Insurance Supervisors，以下IAIS），マネー・ローンダリングおよびテロ資金供与対策（以下，マネロン等対策）に関する金融活動作業部会（Financial Action Task Force，以下FATF）等である．

一般的には，こうしたSSBにより策定された国際基準そのものは各メンバ国を法的に拘束するものではないが，各国の法規制が国際的に整合性のとれたものとなるよう，メンバ国をはじめとする世界各国で幅広く取り入れられている．

G7

G7は主要7カ国からなる国際フォーラムであり，主要先進国としての共通の価値観を共有する点が特徴である．

サイバーセキュリティに関しては，2015年にG7サイバーエキスパートグループを設置している．当該グループは，金融セクタにおけるサイバーセキュリティの現状分析や，G7各国間の連携を目的として活動を行っている．

その他，G7は，フェイスブック等によりリブラ構想が公表された2019年にとりまとめたグローバル・ステーブルコインに関する報告書や，2021年にとりまとめた中央銀行デジタル通貨に関する共通原則など，適宜，重要なテーマに関して検討グループを組織して検討を行っている．

最近の議論の動向

近年，金融機関等に対するサイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことを踏まえ，前章で挙げたG20やFSB，SSB，G7のそれぞれでサイバーセキュリティに関する議論が積極的に行われている．

本章ではFSBおよびG7における最近の主な公表物を中心に，その内容を紹介したい（図-2）．

サイバーセキュリティ

ドイツ議長下の2017年3月G20財務大臣・中央銀行総裁会議での声明を受けて，FSBは，G20メンバ国における金融分野のレジリエンス向上へ向けたクロスボーダでの協力を強化する第一歩として，各国金融当局やSSB等のサイバーセキュリティ関連の規制監督上の取り組みについてサーベイを実施した．そして，その結果を同年10月のG20財務大臣・中央銀行総裁会議に提出し，「金融セクターのサイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書」とし

て公表した．

報告書は，各法域のサイバーセキュリティに関する規制監督枠組みは，既存の国際基準や指針等にある程度基づいているものの，法域内および法域間で多くの差異が見られることを指摘している．

国際的に一貫した規制監督体制の構築へ向けて，グローバルな対話を促進するために，まずサイバーセキュリティやサイバーレジリエンスに関する用語の共通理解を図る必要性が認識された．

そのため，翌 2018 年のアルゼンチン議長下では，FSB は，FSB や SSB，各法域の官民等でのサイバーレジリエンス向上へ向けた取り組み支援を目的として，関連する重要な用語をとりまとめ，同年 11 月に「サイバー用語集」として公表し，G20 サミットへ提出した．用語集は市中協議等でのフィードバックを踏まえたものであり，金融分野におけるサイバーセキュリティに関する政策立案等に有用な 50 超の用語から構成されている．

この後，サイバーインシデントからの復旧・回復といったレジリエンス向上へ向けたさらなる取り組みとして，2019 年の日本議長下では，FSB は，サイバーインシデントへの初動と回復（Cyber Incident Response and Recovery）に関するベストプラクティスのとりまとめに着手した．その後，進捗報告書を同年 6 月の G20 財務大臣・中央銀行総裁会議に，最終報告書を 2020 年 10 月の G20 財務大臣・中央銀行総裁会議に提出し，「サイバー事象の初動・回復対応の効果的な実務」として公表した．

報告書は，主に金融機関向けのプラクティス集であり，金融機関が自らの組織の規模や複雑性，リスクに基づいて適切なものを選択できるように，広範なプラクティスをとりまとめた形となっている．具体的には，①ガバナンス，②計画・準備，③分析，④影響緩和，⑤復旧・回復，⑥連携・情報共有，⑦

FSBにおける関連する文書	
2017	フィンテックによる金融安定上のインプリケーション
2017	金融セクタのサイバーセキュリティにおける規制・ガイダンス・監督上の慣行に関するストックテイク報告書
2018	サイバー用語集
2019	クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察
2020	サイバー事象の初動・回復対応の効果的な実務
2020	アウトソーシング・サードパーティに関する規制・監督上の論点（ディスカッション・ペーパー）
2021	アウトソーシング・サードパーティに関する規制・監督上の論点（市中協議に寄せられた意見の概要）
2021	サイバー事象報告－既存のアプローチとより広い範囲での収斂に向けた今後のステップ

G7における関連する文書・取り組み	
2016	金融セクタのサイバーセキュリティに関するG7の基礎的要素
2017	金融セクタのサイバーセキュリティの効果的な評価に関する基礎的要素
2018	脅威ベースのペネトレーションテストに関するG7の基礎的要素
2018	金融セクタにおけるサードパーティのサイバーリスクマネジメントに関するG7の基礎的要素
2019	合同演習
2020	サイバー演習計画に関するG7の基礎的要素
2020	ランサムウェアに関する附属文書

■図 -2　FSB および G7 における議論の動向―公表情報をもとに作成

改善の 7 領域における計 49 項目のプラクティスから構成されている．

その後，2021 年のイタリア議長下で，FSB は，金融当局向けの取り組みを開始した．具体的には，金融機関から当局へ提出されるサイバーインシデント報告を対象に，グローバルに調和を図ることが可能な領域を特定するために，各法域の規制報告枠組みについてサーベイを実施した．その結果を同年 10 月の G20 財務大臣・中央銀行総裁会議に提出し，「サイバー事象報告―既存のアプローチとより広い範囲での収斂に向けた今後のステップ」として公表した．

当局が金融機関や金融システム全体のリスクを評価する上で，サイバーインシデント報告は重要なツールである．サイバー攻撃の脅威がクロスボーダ・クロスセクタである一方，報告書は，多くの共通点が見られるものの，各国のサイバーインシデント報告には，報告対象とされるサイバーインシデントのスコープや，インシデントの深刻さやインパクトを測る手法，報告期限，報告された情報の用途に関して，法域間・セクタ間で差異が見られることを指摘している．

報告書は，今後取り組むべき内容として，①サイバーインシデントに関して当局が最低限必要とする情報の特定，②法域間・セクタ間で共有されるべき共通の情報の種類の特定，③共通用語の作成の 3 点を挙げており，FSB は，サイバーインシデント報告のグローバルな調和を図るためのさらなる作業を検討中である [2]．

G7 においては，2015 年に設置された G7 サイバーエキスパートグループ（以下，エキスパートグループ）が，サイバーセキュリティに関するベストプラクティスをとりまとめた内容を公表している．

具体的には，エキスパートグループは，2016 年 10 月，金融機関がサイバーセキュリティ対策を講ずる上で重要と考えられる「金融セクターのサイバーセキュリティに関する G7 の基礎的要素」を公表した．翌 2017 年 10 月には，前年の基礎的要素に示したプラクティスの適切な実施・評価を行う点に焦点をあてた「金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素」を公表した．さらに，2018 年 10 月には，サイバー脅威情報の分析を踏まえた実践的な侵入テストに関する「脅威ベースのペネトレーションテストに関する G7 の基礎的要素」，金融機関における第三者委託先のリスク管理に関する「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する G7 の基礎的要素」を公表した．また，2019 年 6 月には，大規模なサイバーインシデントの発生を想定した合同演習を実施し，G7 諸国を中心としたクロスボーダの連携を確認した．そして 2020 年 11 月には，演習計画を立案・実施するための指針として「サイバー演習計画に関する G7 の基礎的要素」を公表した．

エキスパートグループでは，引き続き，演習を通じて得られた知見や教訓を踏まえ，G7 金融当局間の連携手順の改善など，国際的な連携の強化に向けた議論が進められている [3]．

第三者委託

サイバーセキュリティ対策を含む，金融機関のレジリエンス向上に関連したトピックとして，第三者委託先の管理や業務継続性の確保などが挙げられる．近年，IT を活用して新たな金融サービスを提供するフィンテックの台頭やそれに伴う新たな事業者の参入，金融機関間および金融機関と外部の委託先との間の相互接続（たとえば，クラウドコンピューティングやフィンテック事業者を通じた相互接続）の拡大，国際的に活動する大手クラウド事業者への集中リスクの高まりなどを背景に，金融機関における業務継続性の確保について国際的に関心が高まっている．特に，フィンテックを積極的に推進してきた欧州や英国を中心に積極的に議論が進められている．

FSB では，早くからこの点に関してリスク評価を

進めており，2017 年 6 月に公表したフィンテックに関する規制監督上の含意をとりまとめた報告書では，当局間のクロスボーダでの協力が必要とされる最重要項目として，金融機関が利用するクラウドなどの第三者委託先に起因するオペレーショナル・リスク管理を挙げている．なお，金融分野における国際的な議論では，第三者委託については，外部委託（Outsourcing）を含む，金融安定や金融機関にリスクをもたらす，あらゆる第三者との関係（Third-party relationships）を念頭に議論される場合が多い．

その後，FSB は，クラウドサービスを対象に，その金融安定上のリスクについてさらに検討を行った結果を，2019 年 12 月に「クラウドサービス利用における第三者サービスへの依存：金融安定への影響に関する考察」として公表した．報告書は，金融機関によるクラウドサービスの利用は金融安定上の喫緊のリスクではないと結論づけているものの，第三者委託に関する規制や監督実務の妥当性評価等の必要性を指摘している．

FSB は，こうしたリスク評価結果を踏まえ，次に規制監督上の論点について検討を進めた．その結果を，2020 年 11 月に「アウトソーシング・サードパーティに関する規制・監督上の論点（ディスカッション・ペーパー）」として公表し，広く一般からコメントを募る市中協議を行った．

報告書では，第三者委託の増加は，個社レベルではスケーラビリティやオペレーショナル・レジリエンスの向上，コスト削減等のメリットをもたらす一方で，金融当局等にとっては，特に，①金融機関と第三者委託先との契約に関する実務的な課題，②クロスボーダに起因する監督上の課題，③第三者委託先の集中化に起因する金融システム上の課題という 3 点の課題をもたらし得ると指摘している．

①の実務的な課題とは，（1）当局のリソースや IT スキルの不足のほか，（2）金融機関が第三者委託先との契約へ規制監督上の要件を盛り込むことが実務的には困難であり，監査権やデータへのアクセス権，情報取得権が不十分，（3）金融機関のオペレーションにかかるサプライチェーンが長く複雑であるため，二次受けや三次受け等含めたサプライチェーン全体に渡るリスクを特定し管理することが困難，といった課題を指す．

②のクロスボーダの課題とは，（1）監督管轄権が海外の事業者まで及ばない場合や，（2）データ守秘義務の基準等が異なるために当局間の情報共有や金融機関による統一的なデータ管理が困難，（3）第三者委託先が破綻した際に第三国にある重要なデータ等の回収が困難，などの課題を指す．

③の集中化による課題とは，クラウドなど，少数の第三者委託先による寡占市場が生じることで，特定のサービス事業者が単一障害点となり，特定サービスの障害が多くの金融機関に影響を与え得ることを指す．こうした課題を踏まえ，報告書は，金融当局，金融機関，第三者委託先の間でのグローバルな対話の必要性を指摘している．

その後，FSB は，市中協議等でのフィードバックをとりまとめたものを，2021 年 6 月に「アウトソーシング・サードパーティに関する規制・監督上の論点（市中協議に寄せられた意見の概要）」として公表した．

報告書では，前年の報告書で指摘した，監査権やアクセス権，情報取得権の制約，重要サービスにおける集中リスク，規制監督や業界慣行の法域間の相違，データローカライゼーション要件，サイバーセキュリティ・データセキュリティ，専門人材の不足などの課題については，市中協議でおおむね支持されたことを報告している．

また，こうした課題に対処する解決策の案として，（1）事業者に求める事業継続計画・災害復旧計画やサイバーセキュリティ対策，金融機関による事業者の選定やモニタリング，事業者から徴求すべき情報の標準化，事業者との契約の雛形などの第三者委託に関するグローバルスタンダードの策定，（2）定義や用語の統一，（3）金融機関が共同で行う共

同監査や第三者認証の活用，（4）第三者委託先への依存関係の把握，（5）国際協調や官民連携の促進などが挙げられたことを報告している．

今後，FSB は，定義や用語の統一のほか，第三者委託に関する監督上の期待事項のとりまとめを進めていく方向である[2]．

SSB においても活発に議論が進められており，たとえば，BCBS は，サイバー攻撃や自然災害などの発生時における銀行の重要な業務の継続性確保について，2021 年 3 月に，「オペレーショナル・レジリエンスのための諸原則」を公表した．これは，大規模なシステム障害やサイバー攻撃の脅威の増大，パンデミックなどのリスク環境の変化を踏まえ，未然防止策を尽くしてもなお業務中断が生じ得ることを前提に，自行だけでなく，第三者委託先から ATM や窓口等の顧客接点までのエンドツーエンドで，業務中断の影響が許容水準内に収まるよう包括的な態勢整備を求めるものである．

具体的には，①ガバナンス，②オペレーショナル・リスク管理，③事業継続計画とテスト，④組織内外の相互連関性の特定，⑤第三者への依存度の管理，⑥インシデント管理，⑦サイバーを含む ICT セキュリティ対応という 7 つの原則からなる．

また，IOSCO では，2021 年 10 月に「外部委託に関する原則」を公表した．これは，過去に公表した「市場仲介業者の外部委託に関する原則」および「取引所業務の外部委託に関する原則」を統合した上，近年の動向を踏まえて内容を更新し適用範囲を拡大したものである．

本原則は，外部委託の定義，重大性（Materiality）及び不可欠性（Criticality）など外部委託における基本的な考え方に関する記述と，①外部委託先の選定プロセスとモニタリング，②外部委託先との契約，③情報セキュリティ，業務の回復力，事業継続性，災害復旧の確保，④秘密保持，⑤特定の外部委託先への集中，⑥外部委託先のデータ，事業所，人員へのアクセスおよび関連する検査権限，⑦外部委託契約の解除の 7 分野に関してそれぞれ定めた 7 つの原則からなる．

ランサムウェア・暗号資産

最後に，サイバーセキュリティに関連したその他のトピックについても紹介したい．金融分野では，犯罪収益のマネロン等対策やサイバー保険など，サイバーセキュリティを取り巻くトピックに関しても積極的に議論が行われている．

たとえば，ランサムウェアについては，近年，その被害の拡大とともに，対策の必要性について国際的に関心が高まっている．2020 年 10 月の G7 財務大臣・中央銀行総裁会議は，ランサムウェアに関する附属文書を公表した．これは，G7 の文書としては異例ながら，業界に対して直接働きかける文言となっており，ランサムウェア攻撃の脅威が増している点に懸念を示している．

また，ランサムウェアへの対処としては，①自らが被害を受けない，②たとえ被害を受けても身代金を支払わない，③被害を受けずとも身代金の支払いに利用されない，という 3 点が考えられるところ，文書は，特に③の身代金の支払いに利用されてはならないという点を強調している．具体的には，ランサムウェアの身代金として暗号資産が利用される場合が多いことに触れつつ，金融機関に対して，身代金の支払いを防止すべく，FATF 勧告や国内法令等に基づき，マネロン等対策にかかる義務を確実に実施することを求めている．

FATF は，2019 年 6 月に暗号資産に関する FATF 基準を最終化し，マネロン等対策に関する FATF 基準が暗号資産にかかる金融活動にも適用されることを明確にしている．その後，新たな FATF 基準の各国での実施状況や残された課題等をとりまとめた報告書を公表している．その中でも，2021 年 7 月に公表された「暗号資産・暗号資産交換業者に関する FATF 基準についての 2 回目の 12 カ月レビュー報告書」は，ランサムウェア攻撃による犯罪収益が匿

名性を高めるツールなどを介して資金洗浄される危険性を指摘しているほか，各国での新たな FATF 基準に基づくマネロン等対策の必要性を強く指摘している．

なお，FATF は，2021 年 10 月に，「暗号資産及び暗号資産交換業者に対するリスクベース・アプローチに関するガイダンス」を公表して，新たな FATF 基準に関する考え方を詳細に記したガイダンスを 2 年ぶりに更新した．ガイダンスは，暗号資産やマネロン等対策を行う規制対象の定義など FATF 基準の適用範囲を明確化したほか，ステーブルコインに関する考え方，仲介業者を利用せずに個人間で行われる取引のリスクおよびリスク低減策，仲介業者の登録・免許付与，国際的な監督協力等をまとめている．FATF は，今後とも，暗号資産に関するモニタリングを継続していくこととしている．

今後に向けて

本稿では，金融分野におけるサイバーセキュリティを巡る国際的な議論の動向について概説した．金融機関等へのサイバー攻撃の脅威が増し，金融システムの安定等にも影響を与えかねないことから，G20 や FSB，SSB，G7 等のさまざまな場において積極的に議論が行われている．議論の中では，サイバーセキュリティ対策のほか，用語の統一，規制報告枠組み，第三者委託，犯罪収益や暗号資産など多面的な観点から議論が行われている．引き続き，各国の金融当局が連携して，課題解決に向けた議論をグローバルに深めていくことが望まれる．

本稿で示された内容や意見は，筆者個人のものであり，金融庁の公式見解を表すものではない．

参考文献
1）金融庁：金融庁の 1 年（2020 事務年度版）（2021）．
2）FSB：Promoting Global Financial Stability - 2021 FSB Annual Report（2021）．
3）金融庁：金融分野のサイバーセキュリティレポート（2020）．

（2022 年 1 月 17 日受付）

■河田雄次　yuji.kawada@fsa.go.jp

慶應義塾大学大学院理工学研究科基礎理工学専攻修了．2015 年から（株）三菱総合研究所主任研究員，2016 年から 2018 年まで日本銀行に出向し欧州中央銀行とのブロックチェーン共同調査に従事．2020 年から現職．

連載

5分で分かる!? 有名論文ナナメ読み

湯田恵美（東北大学）

Respiratory Sinus Arrhythmia: A Phenomenon Improving Pulmonary Gas Exchange and Circulatory Efficiency

CIR.94.4.842.94:842-847

生体計測技術の発展

近年，Apple Watch が心臓の健康に関する情報を通知することはよく知られている．Apple Watch は心房細動☆1 を示唆する不規則な心拍リズムをセンシングしている．動悸や眩暈といった症状が頻繁にあっても，強い痛みを感じない場合，自身の心房細動に気づくことが難しい．私たちの身近にあるウェアラブルセンサは，脳梗塞を起こす心臓の病気を早期発見する救世主となっている．

身体から発せられるさまざまな情報を取り出す生体計測技術は，デジタル信号処理，解析支援システム，モデル化やシミュレーション技術を通じて日々開発が進んでいる．心電図，脈波，体温，加速度などの健康につながるヒトの生体情報のリアルタイム取得は，健康維持や疾患スクリーニングに利活用できるほか，眠気や疲労など生体の異常状態を検出可能で，生理指標や感性指標として人間を定量的に可視化することもできる．

ヒトの状態を科学的なデータで推定していくことは，健康診断における心電図検査を始め，私たちの暮らしに馴染のあるものである．さまざまなヒト生体信号処理技術が私たちの健康を支えており，この傾向は，健康長寿で幸せな暮らしの実現に向けて今後ますます顕著になっていくと思われる．

心電図研究

生体信号の中でも，心臓の電気的興奮の過程を記録した「心電図」を解析することで得られる情報は，心拍数を把握するだけでなく，非侵襲で計測できる生体信号の中で，細かな粒度でヒトの活動や状態を評価することができる．そのため，医工学研究者や循環器専門医などが心拍変動解析とその解釈研究に取り組んでいる．また，心臓と脳は神経細胞同士は神経伝達物質を介して交信しており，運動時には心拍数や血圧を上げて呼吸を速めるなど，指令信号を出力する．心拍情報である心拍変動☆2 を解析することで，脳の状態を推定することが可能である．

脳波は常に微小な電気現象（0.5-30Hz の周波数範囲の変化を持つ 20-70 μ V の波型信号）を扱うため，脳以外から発生する電位が混入しやすく，手軽な計測・解析が難しい．近年普及した磁気共鳴画像撮影法 (Magnetic Resonance Imaging, MRI) や X 線を用いて体の断層写真を撮影する CT 検査 (Computed Tomography) といった脳画像診断はコストがかかる．そのため，心拍変動解析は，私たちの生体情報を推定するにあたり多くの示唆を与え，臨床検査にも欠かせない手段として使われているのである．

本稿では，心電計から得られた心拍変動と呼吸信号から心拍動の呼吸性の変動成分（呼吸性洞性不整脈，Respiratory Sinus Arrhythmia, RSA）の抽出に成功した Hayano らによる画期的な論文を紹介す

☆1 心房の収縮が失われることで心室が不規則に収縮している状態．長期の心房細動は心臓機能の破綻を引き起こし，心不全に繋がる．

☆2 心拍変動 (HRV) は心拍間の時間間隔変動の生理学的現象で，健常者の心臓は一定の拍動間隔を維持していない．

る．論文が掲載されたCirculation誌のインパクトファクターは29.7（2021年12月現在）！

呼吸性洞性不整脈（RSA）

呼吸と心拍数の関係は，心臓自律神経と密接に連動している．呼吸時に心電図RR間隔（図-1）が短縮し頻拍となり，逆に呼気時には徐拍となりRR間隔は延長する．この現象が呼吸性洞性不整脈（RSA）であり，心拍の呼吸性ゆらぎである．Hayanoらは，安静覚醒時のイヌのポリグラフィ（多用途監視装置，複数の生理反応を同時に記録する装置）を解析して，呼吸と循環の相互作用を通じてRSAの生理学的意義を明らかにしたのである．

これまでの研究において，RSAの機序は，呼気と吸気の交代とリズムの調節にかかわる呼吸中枢と吸気を抑制する肺膨張反射による心臓迷走神経活動の調節と理解されており，RSAの振幅は心臓迷走神経活動に伴って増加すると考えられていた．RSAが能動的な生理的役割を果たしているのか，あるいは単に呼吸に対する心拍数の受動的な反射を反映しているだけなのか不明であった．そこでHayanoらは，RSAが呼吸サイクル内で呼気と吸気を一致させることにより，肺ガス交換を促進するという仮説を立てた．

7頭の麻酔犬を用いてRSAを模擬したモデルを作成し，内因性の自律神経活動を薬理で取り除いた後，横隔膜ペーシングによる陰圧換気中☆3に右頸部迷走神経を電気刺激して，呼吸に連動した心拍変動を発生させた．迷走神経刺激は，呼気時（RSA），吸気時（逆RSA）の呼吸に同期した刺激，その刺激と同数の心拍を1分間に発生させる一定の刺激（コントロール）の3つの条件で行った．

一回換気量，心拍出量，動脈血圧に変化はなかったが，RSAはコントロール時と比較して一回換気量に対する生理学的死腔☆4の比（Vd/Vt）と肺内シャント☆5の割合（Qsp/Qt）をそれぞれ10%と51%減少させ，酸素消費量を4%増加させた．逆RSAではVd/VtとQsp/Qtがそれぞれ14%と64%増加し，O2消費量が14%減少した．

この結果は，RSAは肺のガス交換に有益で，「心拍の節約」によって肺循環のエネルギー効率を改善することを示唆しており，新たな発見であった．

生体は，安定した内部環境を一定に保とうとする働き（生体恒常性，ホメオスタシス）と，急性のストレスに対処する素早い身体反応で，状況に応じて変動しながら適応する（アロスタシス）の間でバランスを保っている．RSAは生体が休息モードにあることを示し、その振幅は休息の深さを反映する．RSAの振幅の増減から、生体がホメオスタシスに向かっているのかアロスタシスに向かっているのかを客観的に知ることができるのである．

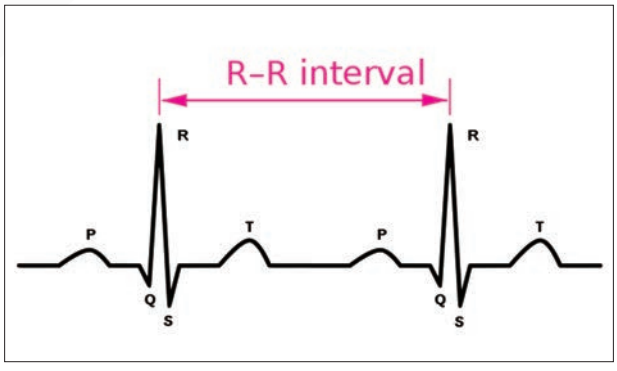


図-1　心電図RR間隔

研究の継承，そして発展

心臓の拍動間隔のゆらぎには，深いサイエンスが横たわっている．この論文の第一筆者でもある早野順一郎先生（名古屋市立大学），心電図自動解析アルゴリズムを開発した吉澤誠先生（東北大学）は，

☆3　普段の私たちの呼吸は陰圧換気であり，自発呼吸の換気方法である．横隔膜・内肋間筋の収縮で胸腔内圧が陰圧になり，肺が膨らむ（経肺圧）．自発呼吸では呼吸努力が強い（＝陰圧が強い）ほど，経肺圧が高くなり肺が大きく膨らむ．

☆4　呼吸器系のうちガス交換が行われない領域．

☆5　肺胞内のガスと肺胞毛細血管を流れる静脈血が接触せず，ガス交換をしないまま心臓に還流している状態．肺胞内で酸素化されず肺を通過する血液の比率がシャント割合．

日本の心拍変動解析研究の第一人者である．2 人は偶然にも同じ 1955 年生まれで，長く日本の生体信号処理分野をリードしてきた．現在もなお，心拍変動解析は発展を続けている．筆者は，心源性脳梗塞や心臓突然死（致死的心室性不整脈）を早期にスクリーニングし，予防するための指標を構築する研究に従事している．健常者が突然亡くなる突然死の原因は，心筋梗塞，心筋症，心不全など心臓病によるものが 6 割超に及ぶ．一生体情報工学者として，心拍変動解析を通じて予期しない急死のリスクを下げていきたい．

この論文に示すように，私たちは心拍をコントロールすることはできず，コントロールできるものは「呼吸」である．深呼吸により気持ちを落ち着かせたり，集中することができる．「全集中！水の呼吸！」について語りたい方，是非私たちの研究室を訪問ください．

（2021 年 12 月 22 日受付）

湯田恵美（正会員）
emi.a.yuda@tohoku.ac.jp

東京都出身．筑波大学大学院修了，博士（工学）[新潟大学]．名古屋市立大学大学院医学研究科 NEDO プロジェクト研究員，東北大学大学院工学研究科 助教を経て，同大学データ駆動科学・AI 教育研究センター 助教（現職）．生体信号処理，生体ビッグデータ解析に関する研究に従事．

べた語義

Vol. 127

CONTENTS

基 般 Jr.

COLUMN

東京都港区立青山小学校の ICT 環境を用いた教育・学習について

GIGA スクール構想で小学校の教育現場はどのように変化したのだろうか．東京都港区立青山小学校☆1 の状況を同校校長の髙山直也先生から伺う機会があったので，一例として本稿で紹介する．

青山小学校は 1 学年 1，2 クラスの小規模校である．港区は GIGA スクール構想への対応としてキーボード付カバーを付けた iPad を区立小・中学校の児童・生徒に 1 人 1 台配備しており，同校では 2020 年 10 月に配備が完了した．以前より各教室に教員用の PC や大型ディスプレイ等があったが，GIGA スクール対応として区が無線 LAN の速度強化等を行ったほか，学校独自に iPad 用の三脚等を配備して，オンライン授業を実施可能とした．

青山小学校において，ほぼ全教科で iPad は活用されているが，ここでは 6 年生国語の熟語学習での利用例を示す．まず教員が熟語のパターン（「○○的」のような 2 文字 +1 文字や「松竹梅」のような 1 文字× 3 等）を説明する．児童は各自の iPad 上のアプリに表示された熟語を指で動かして各パターンに分類する．iPad の画面は大型ディスプレイに集約表示されており，児童同士が容易に考え方を共有できる．そのほか，科目によらず NHK for School☆2 が教材の 1 つとして広く活用されている．

国が東京都への緊急事態宣言の発令期間を 2021 年 9 月まで延長したことから，港区は 2 学期の小中学校の授業をハイブリッド型として，児童・生徒が学校で授業を受けることとオンラインで授業を受けることを選択可能とした☆3．同校では 1 クラス約 30 名のうち，オンライン参加の児童数は，最も多いときで 10 人程度，9 月下旬は 2，3 人であった．授業は教員 1 名が Microsoft Teams で行う．iPad を三脚に設置して，液晶側のカメラで教員自身や黒板などを撮影し，カメラの映像やオンライン参加の児童の様子を iPad で確認する．

ハイブリッド授業の苦労は多々あるが，その中でも特にオンライン参加の児童向けの学習課題等を事前に準備する労力が大きい．毎週末教員はがくぷり☆4 を用いて，翌週 1 週間分の予定と準備物をオンライン参加の児童に送る．また，ネットモラルや児童間での学習外使用等の指導☆5 に学校も家庭も頭を悩ませている．一方，不登校傾向や体調が常にすぐれないなど学校に通いづらい児童でも，オンラインで授業に参加できるのが，ハイブリッド授業の利点である．教室では周囲の様子に敏感に反応してしまうが，自宅なら落ち着いて学習できる児童もいるとのことである．

「オンラインでも学習・就業の機会を得られる場が今後増えるのでは」との髙山先生のご意見を載せて本稿を閉じる．

☆1 https://aoyama-es.minato-tky.ed.jp
☆2 https://www.nhk.or.jp/school/
☆3 東京都港区教育委員会事務局学校教育部「幼稚園，小中学校における 2 学期開始以降の感染症対策の取組の強化について」，令和 3 年（2021 年）8 月 27 日，https://www.city.minato.tokyo.jp/kyouikushien/documents/shousai.pdf
☆4 学校と家庭との文書配布や各種連絡に用いる双方向学校特化アプリ，https://gakupuri.jp/
☆5 Teams でほかの児童を退出させる，コールしてワン切りする，などのトラブルが発生した．長時間ネットゲームや YouTube を利用するなどの問題もある．そこで，港区および同校がタブレットの使い方やハイブリッド授業に関する資料を作成しており，問題が顕著になったときに，朝会での一斉指導や各学級での学級指導を行っている．資料の一例：港区教育委員会「1 人 1 台のタブレット端末を活用した新たな学び」，2020 年 12 月，https://www.city.minato.tokyo.jp/kyouikushien/documents/leaflet.pdf

関谷貴之（東京大学情報基盤センター）（正会員） sekiya@ecc.u-tokyo.ac.jp

東京大学情報基盤センター助教．博士（工学）．学習管理システムの設計・運用等を担当している．また，高等教育機関のシラバスの収集や分析に関する研究を行っている．

LOGOTYPE DESIGN...Megumi Nakata, ILLUSTRATION&PAGE LAYOUT DESIGN...Miyu Kuno

ARTICLE

基般

GIGA スクール構想を推進するための環境整備のすすめ

尾崎拓郎
大阪教育大学　情報基盤センター

はじめに― GIGA スクール構想実現の背景

2019 年 12 月に文部科学省から示された教育の情報化に関する手引では，2020 年度から順次施行される新学習指導要領にあわせて学校における ICT 環境の整備指針が示された [1)]．具体的には，児童生徒向けの 1 人 1 台端末と，高速大容量の通信ネットワークを一体的に整備するための予算が盛り込まれており，Society 5.0 時代を生き抜くために，コンピュータは文房具のような位置付けの道具であり，日常での活用が期待されていることを意味する．

このような中，ハードウェア整備は普通教室環境下においての利用を前提としておりインターネット回線そのものの問題や接続方法といった課題が挙げられ，機器更新を含めた多くの環境整備が必要となってくる．

2019 年 12 月に閣議決定された『安心と成長の未来を拓く総合経済対策』において，「学校における高速大容量ネットワーク環境（校内 LAN）の整備を推進するとともに，特に，義務教育段階において，令和 5 年度までに，全学年の児童生徒一人ひとりがそれぞれ端末を持ち，十分に活用できる環境の実現を目指すこととし，事業を実施する地方公共団体に対し，国として継続的に財源を確保し，必要な支援を講ずることとする．あわせて，教育人材や教育内容といったソフト面でも対応を行う」ことが示された．

このことを踏まえ，GIGA スクール構想の実現のために GIGA スクール実現推進本部が設置され，ICT 環境利活用の後押しをすることとなった．

本稿では，GIGA スクール構想実現のための環境整備について，実現に至るまでの背景や環境整備における留意点について，筆者が所属する大学法人附属学校の実例を交えて述べる．

GIGA スクール構想と新型コロナウイルス感染症

GIGA スクール構想は，文部科学省から示された資料によると，「1 人 1 台端末と，高速大容量の通信ネットワークを一体的に整備することで，特別な支援を必要とする子供を含め，多用な子供たちを誰 1 人取り残すことなく，公正に個別最適化され，資質・能力が一層確実に育成できる教育 ICT 環境を実現する」，「これまでの我が国の教育実践と最先端の ICT のベストミックスを図ることにより，教師・児童生徒の力を最大限に引き出す」と記されており，『これまでの教育実践の蓄積』に『ICT』の要素をかけ合わせることにより，学習活動の一層の充実や，主体的・対話的で深い学びの視点からの授業改善の実現をねらいとしている．

当初，この GIGA スクール構想を実現するために，2018 ～ 2022 年度の 5 カ年計画を策定しており，端末等の導入についても年次進行による導入を予定していた．しかし，2020 年 2 月末頃から日本国内においても流行の兆しを見せた新型コロナウイルス感染症拡大の影響もあり，多くの学校が一斉臨時休校の措置を講ずることとなった．一斉休校期間中に公立

の小学校・中学校・高等学校・特別支援学校において，「同時双方向型のオンライン指導を通じた家庭学習」を実施できた学校は5%に過ぎず，「教育委員会が独自に作成した授業動画を活用した家庭学習」を実施できた学校も10%に満たなかった[2]．このような緊急時においても，1人1台端末環境・学校外でも接続可能な環境の実現といった，GIGAスクールスクール構想におけるハード・ソフト・人材を一体とした整備を加速することで，ICTの活用によりすべての子供たちの学びを保障できる環境の構築が急務・大幅な前倒しとなった．

結果，文部科学省の令和2年度(2020年度)第3次補正予算により，表-1に示す内容が拡充されることとなった．

2020年3月には，「GIGAスクール自治体ピッチ」と称して各ベンダから1人1台端末整備事業における補助対象で構成される基本パッケージおよび先進自治体での実績があるネットワークやアプリケーション等も含めた応用的なパッケージについて提案型のプレゼンテーションが行われた．これにより各自治体が提案内容を参考に，共同調達の実施も視野に入れた検討を実施可能となるようにした[3]．

環境整備の実際

文部科学省が毎年実施している「学校における教育の情報化の実態等に関する調査結果」[4]によると，2019年度(令和元年度)までの調査結果および2020年度（令和2年度）の調査結果から，教育現場におけるICT環境の実態がGIGAスクール構想によって大きく変化したことが伺える．表-2に2020年度までの直近3年間の公表結果(抜粋)を示す．

GIGAスクール構想で掲げられていた，教育用コンピュータ1台あたりの児童生徒数，教育用コンピュータ台数，そして普通教室の無線LAN整備率のいずれもが，2019年度までの数値と2020年度の数値を比べた際に値が大幅に上昇しており，環境整備が進んでいることが分かる．

教育情報セキュリティポリシーガイドラインのGIGAスクール構想への対応

ここからは，ICT環境整備に伴うルール整備について，情報セキュリティの観点から述べる．

文部科学省では，「教育情報セキュリティポリシーに関するガイドライン」☆1[5]を策定し，地方公共団体が設置する学校を対象とした情報セキュリティポリシーの策定や見直しを行う際の参考となるよう，学校における情報セキュリティポリシーの考え方や内容を示している．同ガイドラインも，GIGAスクール構想によって1人1台端末整備や高速大容量の校内通信ネットワーク整備がおおむね整うなど，急速な学校ICT環境整備の推進を踏まえ，1人1台端末を活用するために必要なセキュリティ対策やクラウドサービスの活用を前提としたネットワーク構成等の課題に対応するため，同ガイドラインの改訂を行った旨が述べられている．

これまでに示されていた同ガイドラインでは，

☆1 2021年5月版が最新．初出は2016年10月に公表されたもの．

表-1 GIGAスクール構想の加速による学びの保障(拡充項目)

児童生徒の端末整備支援
学校ネットワーク環境の全校整備
GIGAスクールサポーターの配置
緊急時における家庭でのオンライン学習環境の整備

出典：文部科学省：GIGAスクール構想の加速による学びの保障追補版

表-2 学校における教育の情報化の実態等に関する調査結果(概要)

	2018年度(平成30年度)	2019年度(令和元年度)	2020年度(令和2年度)
教育用コンピュータ1台当たりの児童生徒数（人／台）	5.4	4.9	1.4
教育用コンピュータ台数（千台）	2,168	2,361	8,344
普通教室の無線LAN整備率（%）	41.0	48.9	78.9
インターネット接続率（30Mbps以上；%）	70.3	79.2	88.8

※文部科学省：学校における教育の情報化の実態等に関する調査結果（概要）から抜粋，筆者一部改変

「ネットワーク分離」が前提にあり，インターネット環境を教育現場で利用するために情報漏えい等の情報セキュリティインシデントが発生しないよう，構築するネットワーク環境にはさまざまな制限を設けることを主眼としていた．しかし，直近の改訂ではこの「ネットワーク分離」を必須とせず，直接インターネットへ接続するローカルブレイクアウト構成およびクラウドサービス☆2の利活用（クラウド・バイ・デフォルト）を前提とし，認証によるアクセス制御を前提として目指すべき構成を明確化している．

「1人1台端末整備」の解釈―クラウドサービス活用を前提とした1人1ID環境

先に述べたガイドラインでは，1人1台端末およびクラウドサービス活用を前提として児童生徒一人ひとりに対して個別のIDを付与し，児童生徒の学びを蓄積することで，教員やAIによるフィードバックが行われ，個別最適化された学びの提供への期待が記されている．字面だけでは「1人1台端末」という言葉が先行してしまいがちであるが，利用する学習用ツールやクラウドサービスにおけるID等に対しても情報セキュリティ対策を当然講じる必要があるため，同ガイドラインでは「1人1IDにおけるセキュリティ対策」についての記述も充実するようになった．

この児童生徒一人ひとりに付与された個別のIDは，単純にGIGA端末を利用するためだけのIDという立ち位置でもあると同時に，メールアドレス形式であるがゆえ，活用方法によっては他組織の構成員とコミュニケーションを取ることができる「メールアドレス」にもなり得る．見方によってはグローバルに通用するインターネット上のアイデンティティと捉えることもできる．そして，IDそのものがクラウドサービス活用のために必要な利用者の識別要素であり，OS・端末を問わずに同一にIDで利用可能にもなり得る☆3（図-1）．

また，実際の学習活動を行っていく上で，学校や学級といった単位でのコミュニティの運用をどのように行っていくのかを定めておく必要がある．たとえば，実際の教室空間で日常をともにするクラスの集団は，インターネット空間でのコミュニケーションを意識しない場合には，その学校や教室といった物理的に同一な空間でのみコミュニケーションを取ることが可能である．言い換えれば，その場所に赴けばクラスメートや先生に会える空間であると解釈できる．

この1人1ID環境の整備により，学校外でのオ

☆2 ここでいう「クラウドサービス」にはパブリッククラウドを含んでおり，学習系および校務系システムの双方を対象にすることが示されている．すなわち，教員や児童生徒が必要なときに必要な分だけ，特定のハードウェアに依存せずに主体認証によってアクセスを厳格に管理しつつ，対象者が自由にアクセスできるICTサービスのことを指す．

☆3 実際にOS・端末を問わずにIDが利用可能かどうかは構築環境に依存する．

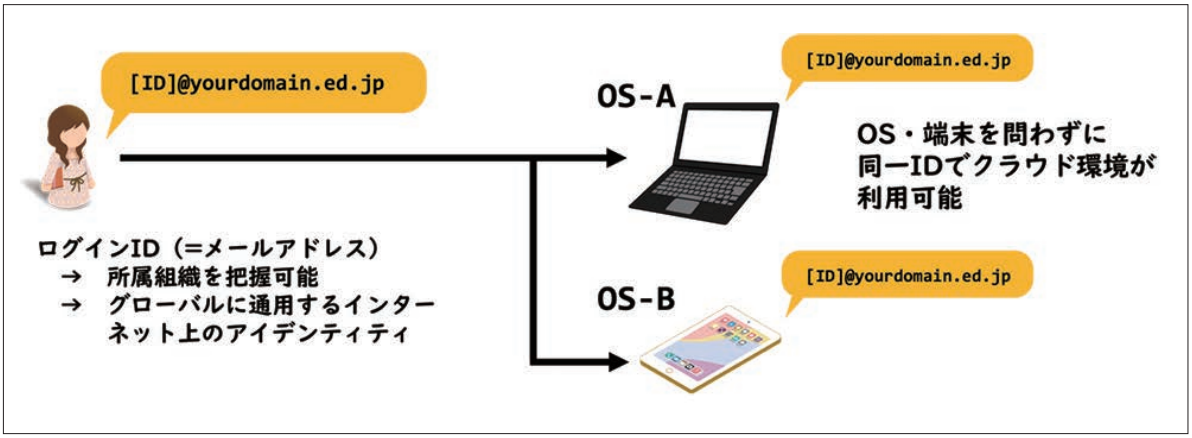


図-1　1人1ID付与によって実現可能なクラウドサービスの活用の例

ンライン学習の可能性も視野に入れ，たとえ物理的に同一空間に存在しなかったとしても，付与されたIDを活用して教室空間と同じメンバによる仮想教室空間をチャットツールやSNS，Web会議システムを介して構築することが容易となった．実際，クラウドサービスのIDが付与されたことにより教室空間でクラスメートと実際に会話をしながら，クラウドサービスの併用といった，教室にいながらにして仮想空間上においても作品を協働編集する様子やチャットツールによる意見交換を確認することができるようになっている．

そのため，図-2に示すような，学校・教室といった実空間とチャットツール・Web会議システムといった，インターネットを活用した仮想空間を同一メンバでそれぞれ共有し，それぞれの空間で実現可能なことを意識しておく必要がある．

GIGA環境構築の一例―所属先の附属学校を例に

ここでは，筆者が所属する大阪教育大学の附属学校において実施したGIGAスクール構想の対応について述べる．

❑ ネットワーク構成

大阪教育大学では，2019年に「教育情報セキュリティポリシーに関するガイドライン」が文部科学省から公表された後，一部の附属小学校において先行して学習系ネットワークと校務系ネットワークのネットワーク分離を実施してきた[6]．GIGAスクール構想がより具体化した2020年度においては，附属学校が設置されている全地区に対して，学習系ネットワーク，校務外部系ネットワーク，校務系ネットワークおよび管理系ネットワークにそれぞれ分離を行い，それぞれの用途にあわせて利用できるようにした．クラウド・バイ・デフォルトの考え方に基づき，ネットワーク分離を必要としない認証によるアクセス制限を前提とした構成を最終的な目標としているが，これまでの資産運用の急激な変化は後の利用者対応のコストのこともあり，既存のローカルブレイクアウト構成を活かしつつ，ネットワーク分離による運用を行っている．

特徴的な構成としては，学習系ネットワークに接続するための無線LAN SSID☆4を全地区で統一の名称・認証方法とし，児童生徒が他地区でGIGA端末

☆4 SSID：Service Set Identifier；無線LANアクセスポイントが発信する電波名

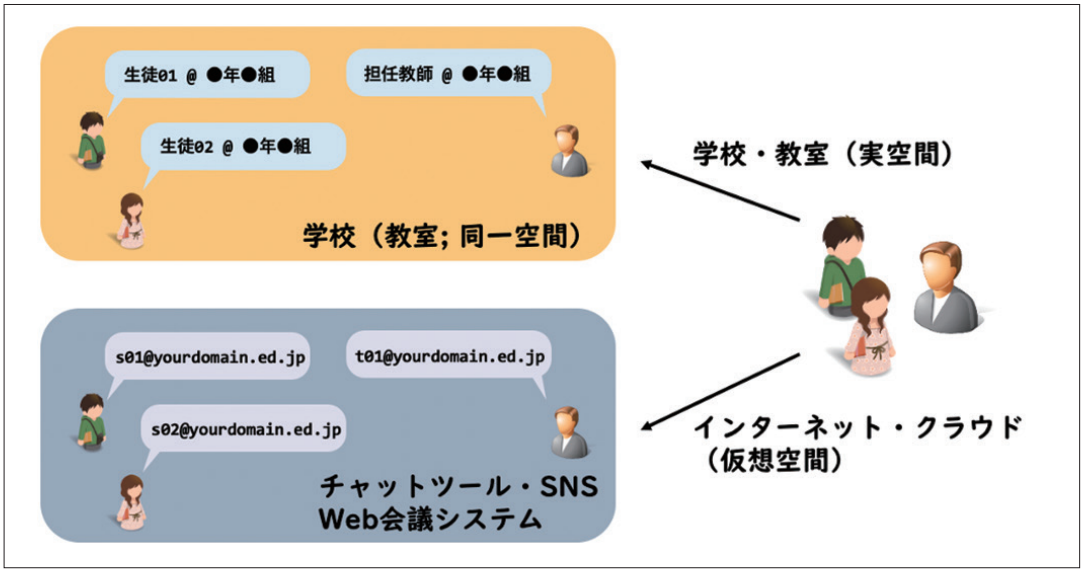


図-2　同一コミュニティによる実空間と仮想空間の併存

を利用したとしてもそのまま利用可能な構成を取っている．また，大学で運用している全学無線 LAN SSID や国際学術無線 LAN ローミング基盤である eduroam も全地区の附属学校園で利用可能としている．そのため，児童生徒にとどまらず大学構成員や eduroam に加入している構成員であればインターネットへの接続環境が担保される．

❑ 教職員・児童生徒への統一サブドメイン ID の付与

大阪教育大学では，大学として保有している高等教育機関ドメインとは別に初等中等教育機関ドメインを保有しており，附属学校における Web サイト等の運用では後者のドメインを従来から利用している．GIGA 環境の整備に伴い，クラウドサービスへのログイン ID を可能にするために後者のドメインから附属学校で統一の専用サブドメインを作成した．これにより，各附属学校間の教職員や児童生徒らによるクラウドサービスを用いた遠隔交流を容易にする環境を整えることができた．なお，ユーザ名の付与方法についても児童生徒で付与時に一意な文字列に設定されるように設計し，年次更新や進学等を見据えた設計に加え，将来構想として保護者への ID 付与の検討も視野に入れた設計としている．

ただし，統一の専用サブドメインの導入以前に，各地区・学校独自のドメイン運用が行われている個所も残るため，当分は移行期となる．早期に統一の専用サブドメインへの移行が完了し，統一ドメインの有効性を見出したい．

おわりに
―環境整備の先にある学校における ICT 活用

本稿では，GIGA スクール構想実現のための環境整備について，実施背景や環境整備における留意点について，実施例を交えて報告を行った．本報告では環境整備への言及にとどまっているが，この整備の終着点は整備された端末や ID，ネットワーク・クラウドサービスを活用して教師・児童生徒の力を最大限に引き出し，子供たちの資質・能力を一層確実に育成できる教育環境の実現のための GIGA スクール構想の実現である．そのためには整備された環境を日頃から積極的に活用し，ICT の活用が特別ではなく日常に転換していくことが求められる．授業をはじめとする学校現場での ICT 活用に向けて，その土台となっているネットワーク環境や情報セキュリティにも注視しながら，その環境が最大限に活用されることを望む．

参考文献

1) 文部科学省：「教育の情報化に関する手引」について，https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/mext_00117.html（2021.12.30 アクセス）
2) 文部科学省：新型コロナウイルス感染症対策のための学校の臨時休業に関連した公立学校における学習指導要領等の取組状況について，https://www.mext.go.jp/content/20200421-mxt_kouhou01-000006590_1.pdf（2021.12.30 アクセス）
3) 文部科学省：内閣官房情報通信技術総合戦略室・文部科学省 GIGA スクール自治体ピッチ紹介ページ，https://www.learning-innovation.go.jp/giga/（2021.12.30 アクセス）
4) 文部科学省：学校における教育の情報化の実態等に関する調査結果，https://www.mext.go.jp/a_menu/shotou/zyouhou/1287351.htm（2021.12.30 参照）
5) 文部科学省：「教育情報セキュリティポリシーに関するガイドライン」公表について，https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.htm（2021.12.30 参照）
6) 松井聴治，佐藤隆士：初等教育機関におけるネットワーク分離の報告事例，大学 ICT 推進協議会，2019 年度年次大会，TP-19, pp.480-483 (2019).

（2021 年 12 月 31 日受付）

尾崎拓郎（正会員） ozaki@cc.osaka-kyoiku.ac.jp

大阪教育大学大学院修了．修士（学術）．高等学校教員を経て大阪教育大学理数情報教育系・情報基盤センター准教授．教員養成課程における ICT 利活用人材育成に興味を持つ．コロナ禍でオンライン授業のシステム運用に奔走．2021 年度より文部科学省 ICT 活用教育アドバイザーを務める．

第 14 回全国高等学校情報教育研究会全国大会（大阪大会）

井手広康
愛知県立小牧高等学校

全高情研と全国大会

2021 年 8 月 10 日（火）～ 11 日（水）に第 14 回全国高等学校情報教育研究会全国大会（大阪大会）がオンラインで開催された．全国高等学校情報教育研究会[1]（以下，「全高情研」と表記）は，2003 年に高等学校において教科「情報」が設置されたことを受けて 2008 年に発足した，全国の情報教育研究会☆1 から構成される組織である．全高情研は，その発足以来，全国の高等学校における情報教育の研究推進ならびに会員相互の研鑽を図ることを目的とし，毎年 8 月に全国大会を開催し，教科「情報」ならびに情報教育の発展に寄与してきた．

ここで，これまでに開催された全国大会の一覧を表 -1 に示す．表 -1 の「大会テーマ」を見ると，その年の教科「情報」の動向が分かる．たとえば，第 6 回大会（2013 年）では，現行の高等学校学習指導要領が施行された年であり，副題では「情報教育の深化」となっている．また，第 14 回大会（2021 年）では，教科「情報」が 2025 年からの大学入学共通テストの出題教科に導入された[2]ことを受け，副題では「大学入学共通テストを見据えた教科情報とは」となっている．

一方，表 -1 の「開催地」を見ると，記念すべき第 1 回大会（2008 年）は東京から始まり，第 12 回大会（2019 年）の和歌山まで，これまで全国各地で全国大会を開催してきていることが分かる．しかし，第 13 回大会（2020 年）から新型コロナウイルス感染症の感染拡大のため，オンラインでの開催を余儀なくされた（当初，第 13 回大会は愛知での開催予定であった）．また，第 14 回大会（2021 年）も第 13 回大会（2020 年）に引き続きオンライン開催となっている．次回の第 15 回大会（2022 年）の開催も，現状ではオンライン

☆1 2021 年 12 月時点では，全国 33 の研究会が全高情研に加盟している．

表 -1　全国高等学校情報教育研究会全国大会一覧（2008 年～ 2021 年）

開催年	回	開催地	大会テーマ
2008 年	第 1 回	東京	Next Stage―新たに広がるネットワークの構築―
2009 年	第 2 回	茨城	ICT コンパス―あふれる情報の波を乗りこなす―
2010 年	第 3 回	石川	ICT コンパス―新たなる風―
2011 年	第 4 回	大阪	ICT コンパス―風を受け新たな一歩を踏み出す―
2012 年	第 5 回	千葉	情報教育の未来をデザインする
2013 年	第 6 回	京都	教科情報 11 年目の進展～情報教育の深化～
2014 年	第 7 回	埼玉	輝く未来を創る情報教育～新しいメディアへアプローチ～
2015 年	第 8 回	宮崎	地域課題に向きあう情報教育～地方からの挑戦～
2016 年	第 9 回	神奈川	情報教育の本質を見極める～挑戦し続ける現場からの発信～
2017 年	第 10 回	東京	情報教育に関わるすべての人へ
2018 年	第 11 回	秋田	新時代の学びをリードする情報教育―秋田から全国に向けて―
2019 年	第 12 回	和歌山	Next Stage ～次代の担い手を育む情報教育～
2020 年	第 13 回	オンライン	（大会テーマなし）
2021 年	第 14 回	オンライン	新学習指導要領に向けて～大学入学共通テストを見据えた教科情報とは～

開催になる可能性が高いだろう．

オンライン開催を活かした新たな取り組み

第 13 回大会（2020 年）と第 14 回大会（2021 年）では，オンライン開催という特性を活かし，いくつかの新しい取り組みを行っている．

1 つ目は発表形態である．これまでの全国大会では，分科会発表とポスター発表という 2 つの発表形態があり，いずれも口頭での発表であった．オンライン開催では，ポスター発表の代わりとして動画発表（オンデマンド発表）という発表形態を取り入れた．動画発表では，発表者は発表動画を用意し，これを事前にインターネット上に公開することで，参加者は自由な時間に発表を視聴できるというものである．なお，第 13 回大会（2020 年）では口頭発表が 6 件，動画発表が 17 件，第 14 回大会（2021 年）では口頭発表が 18 件，動画発表が 17 件であった．Zoom のような Web 会議システムが普及したことも影響し，口頭発表の件数が大きく増加している．

2 つ目は大会冊子である．現地での開催であった第 12 回大会（2019 年）までは，資料代（大会冊子代）として 2,000 円を現地で徴収している（大会参加費は無料）．しかし，第 13 回大会（2020 年）では，開催地がオンラインとなったことや，オンラインの決定から開催までの時間的な制約もあり，大会冊子を制作することができなかった．これを受け，第 14 回大会（2021 年）では，大会冊子を POD（オンデマンド印刷）での販売に切り替えた．POD では，全国大会当日までに各自がインターネットで大会冊子を注文するという流れになる．なお，第 14 回大会（2021 年）の大会冊子は，図 -1 のように Amazon より注文することができる．また，第 15 回大会（2022 年）の大会冊子についても，現在のところ同様に POD での販売を検討している．

第 14 回大会での発表題目

第 14 回大会（2021 年）では，口頭発表が 18 件，動画発表が 17 件と大変多くの発表があった☆2．ここで口頭発表の発表題目一覧を表 -2 に，動画発表の発表題目一覧を表 -3 に示す．さらに，口頭発表と動画発

☆2 全高情研 Web サイトから第 14 回大会への参加申し込みをすることで，各発表の動画を視聴することができる（2022 年 1 月現在）．

図 -1　POD による大会冊子の販売

表を合わせた全35件の発表内容の内訳を図-2に示す．新学習指導要領では，「情報Ⅰ」は「(1) 情報社会の問題解決」，「(2) コミュニケーションと情報デザイン」，「(3) コンピュータとプログラミング」，「(4) 情報通信ネットワークとデータの活用」の4つの領域から構成される．図-2を見ると，これら「情報Ⅰ」の4つの領域のうち，特に「(2) コミュニケーションと情報デザイン」と「(3) コンピュータとプログラミング」の割合が多く，現場の先生方にとって興味・関心が高い領域であることがうかがえる．なお，図-2は筆者が最も発表内容と関連性の深い項目に分類したものであるが，複数の項目に跨っている発表も多く見受けられた．たとえば，表-2の番号「R1-2」は，プログラミングを通して情報デザイン（ゲームのUI）の考え方を学んだり，番号「R1-4」は，すべての領域を横断的に捉えてピクトグラムの制作実習を行うなど，1つの領域に捉われない実践事例が目立った．「情報I」では，現行の科目と比較して学習内容が広域化・高度化し

表-2　口頭発表（リアルタイム発表）の発表題目一覧

番号	発表題目
R1-1	アプリ開発でアイディアを形に ～情報II「(4) 情報システムとプログラミング」を見据えた授業実践～
R1-2	ゲームのUI改善を通して学ぶユーザビリティ―プログラミングで学ぶ情報デザイン―
R1-3	フォームを利用した簡易ジャッジシステムによるプログラミング演習およびコンテストの活用について
R1-4	問題解決，情報デザイン，プログラミング，データ分析を横断的に扱えるピクトグラム制作実習の実践事例報告
R1-5	「難しいけど楽しい」を目指したプログラミング授業の実践 ～ Google Colaboratory を活用したプログラミング学習の実践発表～
R1-6	GAS を利用した LINEBOT の作成（Web マーケティング）～地域商店の LINEBOT を作成する～
R2-1	Peirce の探究段階論に基づく「情報 I，II」の授業設計
R2-2	情報Ⅰにおける問題解決学習と Office アプリの活用 ～どうする？生徒の苦手な「パソコン」の授業
R2-3	オンライン学習に向けた埼玉県立高校の取り組み状況
R2-4	情報科におけるハイブリッドな学びーオンデマンド教材の活用とその可能性ー
R2-5	Google Sites を活用したオンライン学習支援
R2-6	主体的な学びを促す形成的評価の実践
R3-1	文書作成ソフトでできる情報デザイン～情報デザインの授業計画の検討～
R3-2	情報教育の高大接続の課題―名古屋文理大学の入試をベースに考える―
R3-3	表計算アプリで実感するデータベースの考え方の必要性
R3-4	「情報Ⅰ」教科書でのデータサイエンスの扱いについて
R3-5	大学1年生（2020年度）の高校在籍時における教科「情報」の履修意識に関する調査
R3-6	大学入学共通テスト「情報」試作問題・サンプル問題と教科書から考察する「情報Ⅰ」

表-3　動画発表（オンデマンド発表）の発表題目一覧

番号	発表題目
O-1	高等学校における AI を学ぶ教材の開発と授業実践―教材はどのようなものが必要か？―
O-2	大学入試を見据えた教えないプログラミング教育～応用力の育成を考慮したプログラミング教育～
O-3	「情報Ⅰ」が始まる前に
O-4	コロナ禍で沸き上がったフェイクニュースの問題を解決に向けて探究する～ SNS トラブル解決に向けて熱中して学ぶ～
O-5	オンライン授業での協働学習
O-6	可視化で超速攻指導！実験付き統計・分析指導～表計算ソフトウェア活用で時短実現～
O-7	超速攻指導！実験付き「AD 変換」とバイナリデータ・拡張子～バイナリデータ確認実験と圧縮～
O-8	共通テストに対応したプログラミングの単元案とその評価
O-9	フィッシングサイトの体験
O-10	プログラミングの活用を見据えた教育用マイクロコンピュータとソフトウェアの比較検討
O-11	空中ディスプレイを利用したコンテンツ制作の可能性―授業実践・情報Ⅰを見据えて―
O-12	擬似広告制作活動を通じた情報デザインの実践
O-13	情報モラルも一緒に考える双方向通信の授業案～中学生の学びを体験するの巻～
O-14	情報Ⅰ×探究の検証：データ分析から問を生み出す～情報＋探究の3単位で展開するハイブリッドな学び～
O-15	課外授業 DTM・MTR 創作体験を通したシーケンス，MIDI の構造及び楽理理解～音楽の構造と情報の接点およびデザイン～
O-16	micro:bit を用いた情報活用能力の育成における形成的アセスメントの検討
O-17	情報Ⅰと GIGA スクールの同時スタートに向けて～情報科の授業は PC 教室から飛び出そう～

たことや，共通テストに「情報」が組み込まれたことを受け，このような複数の領域を組み込んだ授業の展開が注目されている．

また，「情報Ⅰ」の4つの領域以外にも，「オンライン学習」や「学習環境・評価」，「共通テスト・入試」に関する発表が多かった．これは，新型コロナウイルス感染症に影響されるオンライン学習の普及や，GIGAスクール構想による1人1台タブレット端末の活用，大学入学共通テストへの「情報」の導入などが大きな要因となっていると推測できる．

第15回大会に向けて

第14回大会（2021年）を盛会のうちに終えることができ，現在は第15回大会（2022年）に向けて実行委員会で準備を進めている．第14回大会終了後に実施した参加者へのアンケート（回答数55件）では，「2回目のオンライン開催となった大阪大会はどうでしたか？」という質問に対して，54.5%が「とてもよかった」，43.6%が「よかった」，残り1.9%が「普通」という回答であった．第14回大会（2021年）はオンライン開催のため，やはり回線や機器のトラブルがあり上手くいかない部分もあったが，参加していただいた多くの先生方に「参加して良かった」と思っていただいたことは嬉しい限りである．

第15回大会（2022年）は，前述のように現在のところオンライン開催になる可能性が高いが，動画発表（オンデマンド発表）やPODによる大会冊子のように，オンラインならではの取り組みが活かせるというメリットがある．また，第15回大会（2022年）は，新学習指導要領下において新しい教科「情報」がスタートする記念すべき大会でもある．これまでの全高情研全国大会の良き歴史を踏襲しつつも，Society 5.0の時代に適応した新たな特色を取り入れていくなど，これからも教科「情報」ならびに情報教育のさらなる発展に寄与していきたい．

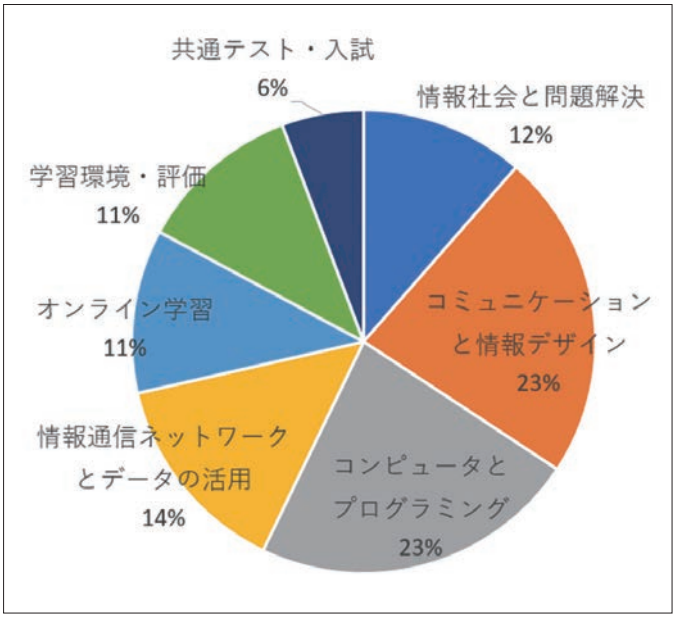


図-2　第14回大会の発表内容の内訳（全35件）

参考文献

1) 全国高等学校情報教育研究会，https://www.zenkojoken.jp/（2021.12.30閲覧）
2) 大学入試センター：令和7年度大学入学者選抜に係る大学入学共通テスト実施大綱の予告，https://www.mext.go.jp/nyushi/index.htm#r7yokoku（2022.1.10閲覧）

（2021年12月30日受付）

井手広康（正会員） k619154u@gmail.com

愛知県立小牧高等学校情報科教諭．愛知県立大学大学院情報科学研究科博士後期課程修了，博士（情報科学）．第14回全国高等学校情報教育研究会全国大会（大阪大会）実行委員，本会コンピュータと教育研究会運営委員，日本産業技術教育学会理事，日本情報科教育学会評議員など．

連載

情報の授業をしよう！

本コーナー「情報の授業をしよう！」は，小学校や中学校で情報活用能力を育む内容を授業で教えている先生，高校で情報科を教えている先生や，大学初年次で情報科目を教えている先生が，「自分はこの内容はこういう風に教えている」というノウハウを紹介するものです．情報のさまざまな内容について，他人にどうやって分かってもらうか，という工夫やアイディアは，読者の皆様にもきっと役立つことと思います．そして「自分も教え方の工夫を紹介したい」と思われた場合は，こちらにご連絡ください．
（E-mail：editj@ipsj.or.jp）

「情報 I」を見据えた「情報の科学」の授業実践

基般

前田健太朗　北海道札幌北高等学校

「情報 I」に備えて

高校では，2022 年度の入学生から 2018 年告示の学習指導要領（以後，新学習指導要領とする）が適用される．私が勤務する北海道札幌北高等学校では，2022 年度から「情報 I」を 1 年次に履修させる．「情報I」の指導内容には，現行の学習指導要領の科目「情報の科学」に似た内容が多いが，主体的・対話的で深い学びの実現に向けた授業改善が求められている．

また，2022 年度入学生から観点別評価が変わる．観点別評価とは，生徒にどのような力が身に付いたのかという学習の成果を捉え，教師の指導の改善，生徒の学習の改善につなげるものである．新学習指導要領の目標および内容が資質・能力の 3 つの柱で再整理されたことから，「知識･技能」，「思考･判断･表現」，「主体的に学習の取り組む態度」の 3 観点に整理された．この観点別評価は指導要録に記載しなければならない．さらに，各観点の評価から 5 段階等の評定に総括する必要もある．そのため，各観点で評価できるように授業を改善することや，各観点の評価から評定へ総括する方法を検討することが求められている．

ところで，大学入試センターが公表した 2025 年度大学入学共通テストの実施大綱の予告では，出題科目として「情報 I」が新たに設定されている．この原稿を執筆している時点（2021 年 12 月）では，共通テストを課す各大学が情報 I を加えるか否かは不明だが，生徒のほとんどが大学進学希望で共通テストを受験すると見込まれることから，情報 I が必須となった場合に対応できる指導内容としなければならない．今までに大学入試センターが公表してきた試作問題やサンプル問題を参考にして，指導内容の見直しや難易度の検討が必要だろう．

そこで本稿では，勤務校における「情報 I」を見据えた今年度（2021 年度）の「情報の科学」の授業実践内容を紹介する．

年間指導計画

勤務校の今年度の「情報の科学」の年間指導計画

は表 -1 のとおりである．「情報の科学」の指導内容にはなく，「情報Ⅰ」の指導内容として追加した単元は情報デザインである（コミュニケーションは「情報の科学」の指導内容にある）．

高校の 1 単位時間は 50 分と定められている．また，「情報の科学」も「情報Ⅰ」も標準単位数は 2 単位である．年間授業週数は 35 週であることから，年間の授業数は 70 時間である．しかし，勤務校では 65 分授業を行っていることから，年間の授業数は約 54 時間である．

授業内容

ここでは，原稿執筆時点までに指導した内容で，「情報Ⅰ」に向けて指導内容を大きく変えたものを紹介する．

情報社会の問題解決

新学習指導要領解説には，「問題を発見・解決する方法については，中学校までの段階で学習するものを踏まえて，情報と情報技術を活用した具体的な問題解決の中で扱う」と記載されている．そこで，この単元の指導は，中学校までに学んだことをもとに生徒が協働して具体的な解決策を考え発表することとした．この単元の指導を年度当初に行い，学んだことを今後の学習活動や日常生活に活かしてほしいこと，グループによる協働学習として，中学校までの学習内容の差を補うことをねらいとしている．さらに，高校に入学してすぐの時期であることから，人間関係をつくることも期待している．

授業では，初めに Wiki 上に，生徒それぞれが考える情報社会の課題を自由に書き込ませた[☆1]．書き込みの内容から著作権やデジタルタトゥーなど 15 程度のテーマに絞り，各グループにテーマを選択させた．

次に，グループごとにテーマに関する理解を深められるように，知っていることなどを話し合わせた．生徒には Google のアカウントを配付しており，Jamboard[☆2] に共有の設定をかけさせて，話し合った内容を記録するよう指示している．話し合いが十分に行われたら，KJ 法を利用して記録をグルーピングして整理させた．そして，ロジックツリー[☆3] を用いてテーマに関する問題と根本にある原因をできるだけたくさん考えさせた．根本にある原因を複数考えたらマトリックス図や座標軸等を用いて比較し，効果と実現性の高い解決策を選択させた．

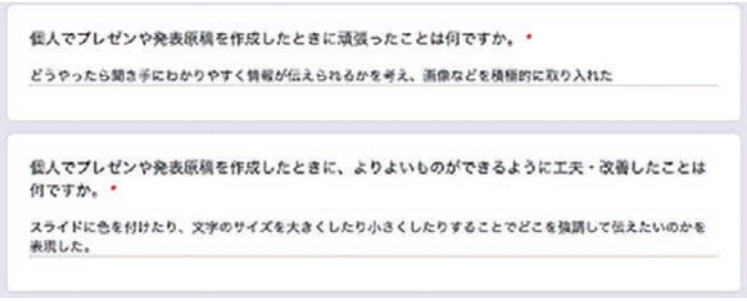
最後に，課題の発見，根本にある原因，その解決策という流れをスライドにまとめ，発表させた．プレゼンテーションのアプリは Google Slides である．これも共有の設定をかけさせて，担当ページの分担を決めて，グループで共同編集して短時間で作成させた．

評価は生徒による相互評価とした．発表内容から，解決策の妥当性，スライドや発表の分かりやすさを，「思考・判断・表現」として評価した．また，発表後には図 -1 のような授業の振り返りを Google Forms で行い，「主体的に学習に取り組む態度」として評価した．

☆1 校内にある Web サーバ上に PukiWiki をインストールして生徒に提供した．
☆2 Google LLC が提供する電子ホワイトボード機能を持つクラウドアプリケーション．
☆3 シンキングツールの 1 つで，問題の原因解明や解決策立案のために，問題を論理的に関連した要素ごとにツリー上に分解していく方法．

■表 -1　年間指導計画

単元	配当時間
オリエンテーション	1 時間
情報社会の問題解決	9 時間
2 進法・デジタル化	12 時間
コミュニケーションと情報デザイン	3 時間
ネットワーク	4 時間
プログラミング	11 時間
データ分析	12 時間
定期考査	2 時間



■図 -1　学習活動の振り返りの入力例

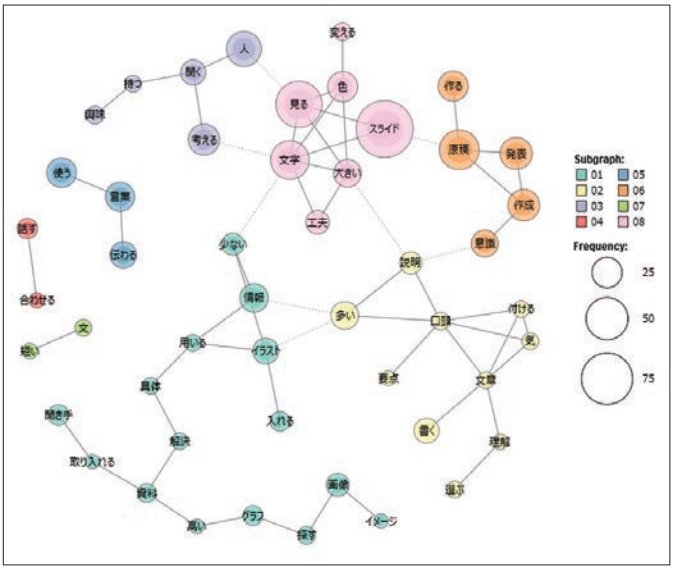
2021年8月に公表された国立教育政策研究所の「指導と評価の一体化」のための学習評価に関する参考資料[1)]（以後，学習評価に関する参考資料とする）には，「主体的に学習に取り組む態度」の評価のイメージが記載されている．また，それには「知識および技能を獲得したり，思考力，判断力，表現力等を身に付けたりすることに向けた粘り強い取組の中で，自らの学習を調整しようとしているかどうかを含めて評価する」と説明されている．そこで図-1のように，「自らの学習を調整しようとしている」は工夫・改善したこと，「粘り強く」は頑張ったことと言い換えて Google Forms で質問した．この2つの文章をテキストマイニングしたところ，どちらにも同じような単語がよく登場していた．さらにテキストマイニングしたデータを共起ネットワーク図で表すと，図-2，図-3のように似た単語が多いだけでなく，単語に関連する別の単語の関係も似ており，生徒が記述した2つの質問の回答は似た内容のものが多かったと考えられる．

学習評価に関する参考資料には，「粘り強い取組を行おうとする側面と，自らの学習を調整しようとする側面の姿は実際の教科等の学びの中では別々ではなく相互にかかわり合いながら立ち現れるものと考えられる」と記載されている．よって，図-1のような2つの質問に対して同じような回答が多いことは当然であり，2つの質問を1つにまとめるべきだったと反省した．

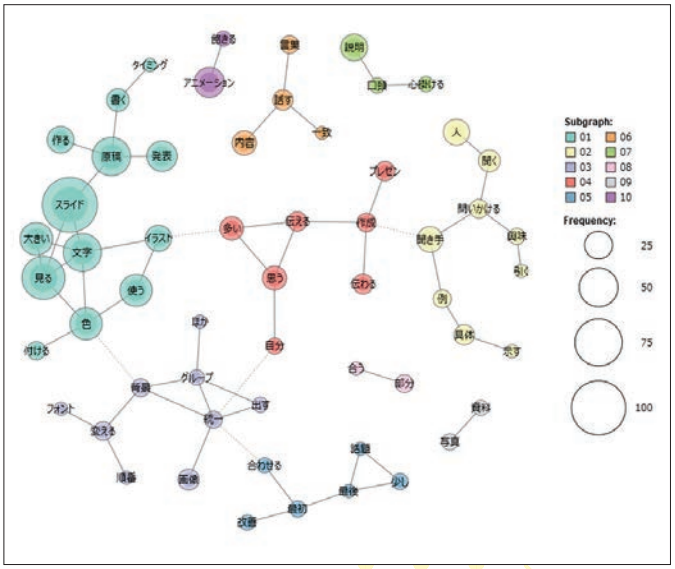
コミュニケーションと情報デザイン

新学習指導要領解説には，「すべての人に情報を伝えるために，コミュニケーションの目的を明確にする力，伝える情報を明確にする力，目的や受け手の状況に応じて適切かつ効果的な情報デザインを考える力を養う」と記載されている．そこで，メディアとコミュニケーションの単元ではピクトグラムの作成を行った．最初に情報の抽象化，ユニバーサルデザインとカラーの考え方について説明し，作成するピクトグラムのタイトルやイメージを構想させた．次に Google 図形描画アプリの操作方法を説明して，構想をもとにピクトグラムを作成させた．

また，新学習指導要領解説には，「効果的なコミュニケーションを行うための情報デザインの考え方や方法に基づいて表現し，評価し改善すること」と記載されている．対話的な学びとするためにも，作成物を生徒同士で評価し，改善する機会を設けたいと考えた．そこで，ある程度作成した時点で評価し合い，助言をもらったり，他者の優れた技術を参考にしたりして，改善するように指示した．



■図-2　頑張ったことの共起ネットワーク図



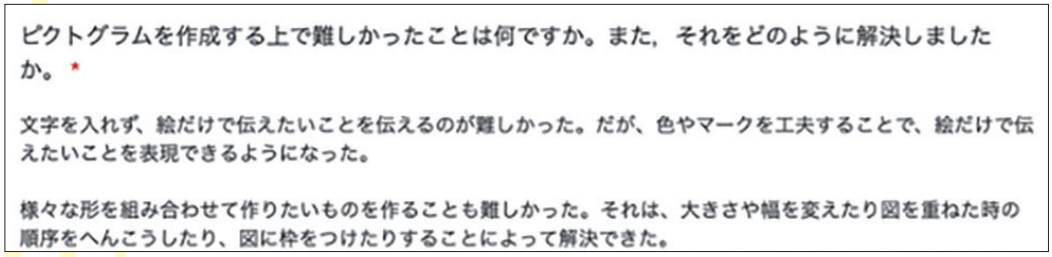
■図-3　工夫・改善したことの共起ネットワーク図

完成したピクトグラムはGoogle Classroomを利用して提出させた．さらに，学習の振り返りを行い，「主体的に学習に取り組む態度」の評価物とした．この振り返りでは情報社会の問題解決の反省を踏まえ，図-4のように質問を1つとした．

プログラミング

勤務校では今まで，5時間程度の配当時間でPythonによるプログラミングを指導してきた．新学習指導要領には，「アルゴリズムの効率を考える力などを養う」と記載されており，例として探索や整列のアルゴリズムが挙げられている．それらを指導するとなると，アルゴリズムの基本的な構造はもちろん，入れ子構造や配列を扱う必要もあり，今までよりもプログラミングの単元の配当時間を増やさなければならない．そこで，今年度は表-2のように11時間の配当時間で指導することとした．各時間の授業では，例題の説明と実習を行い，その後問題演習に取り組むという流れで，生徒にアルゴリズムやプログラムを考えさせるようにした．また，キー入力の遅い生徒に配慮し，実習や問題演習で入力するプログラムを図-5のように短くしたり，図-6や図-7のように以前に作成したプログラムに処理を追加したりするようにした．

ちなみに，モデル化とシミュレーションでは，サイコロの出目の確率と放物運動を題材とした．高校1年生に理解できることと配列の指導ができることから，最初にサイコロの出目の確率のシミュレーションを行った．しかし，放物運動の方がシミュレー



■図-4　学習活動の振り返りの記述例

■表-2　プログラミングの単元の指導内容と配当時間

指導内容	配当時間
アルゴリズム，print()，代入，input(),int(), 変数，算術演算子	1時間
比較演算子，if else elif	1時間
while,for	2時間
random(randint)	1時間
配列（リスト）, グラフ	1時間
モデル化とシミュレーション（放物運動）	2時間
探索（線形探索法，二分探索法）	2時間
並べ替え	1時間

```
from random import randint
dice = randint(1, 6)
print(dice)
```

■図-5　乱数を用いてサイコロをモデル化したプログラム（例題とその実習）

```
from random import randint
dice = randint(1, 6)
yoso = int(input('dono me ga derukana?'))
if yoso == dice:
    print('atari')
else:
    print('hazure')
print(dice)
```

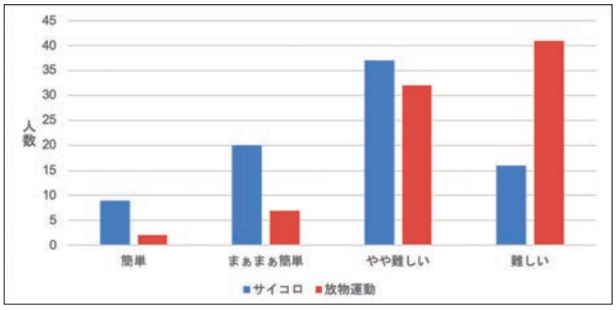
■図-6　図-5のプログラムに処理を追加して作成したサイコロの数当てゲーム（問題演習）

```
from random import randint
hantei = False
while hantei == False:
    dice = randint(1, 6)
    yoso = int(input('dono me ga derukana?'))
    print(dice)
    if yoso == dice:
        print('atari')
        print('GAME OVER')
        hantei = True
    else:
        print('hazure')
```

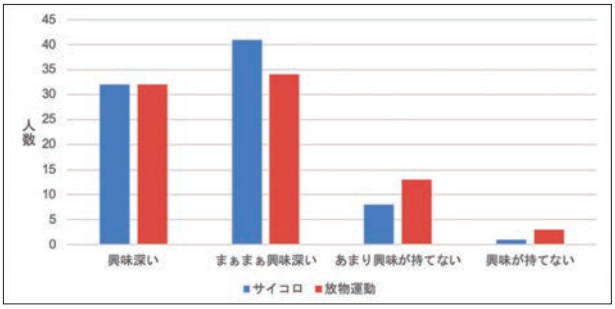
■図-7　図-6のプログラムに処理を追加して作成したサイコロの数当てゲーム（問題演習）

ション自体の面白さを感じられるのではないかと考え，放物運動のシミュレーションも扱った．なお，放物運動のシミュレーションでは，生徒が「数学 I」ですでに学習している三角比を利用して放物運動の角度を指定させた．ただし，重力加速度や放物運動はまだ学習していない．そこで，授業後に難易度や興味関心についてアンケートを行った．その結果を図 -8 と図 -9 に示す．

アンケートの結果から，どちらの題材も難しいと感じた生徒が多いことが分かった．放物運動のシミュレーションを難しいと回答した生徒が多かった原因は，生徒が高校の物理を学習していないため，プログラム内の放物運動の計算処理の意味をきちんと理解できていないからだと思われる．しかし，シミュレーション自体に興味を持って取り組んでいる生徒は多く，ここではプログラミングをメインに指導するのではなく，プログラミングで作成したモデルを利用してシミュレーションを行うことをメインに指導するとよいのではないかと反省した．



■図 -8　モデル化とシミュレーションのプログラムの難易度



■図 -9　モデル化とシミュレーションに対する興味関心の度合い

次年度に向けて

原稿執筆時点で指導している内容はここまでである．この後はデータの分析の指導を行う予定である．昨年度のこの単元の授業では，アンケート調査を行ってスマートフォンの利用時間等に関するデータを収集した．今年度はそのデータを利用して統計処理，相関関係の調査，単回帰分析をしたいと考えている．しかし，今まで行っていた生徒が仮説を立ててデータ分析を行い，仮説を検証するような演習は，残りの授業時数から実施が難しい．ほかにもデータベースの指導ができていない．次年度に向けて課題が残っている．

また，授業内容だけでなく評価方法も考える必要がある．観点別評価ができることはもちろん，評定として総括する方法も検討しなければならない．2022 年 3 月末までにこれらの課題に取り組み，「情報 I」の指導に向けて準備万端に整えたい．

参考文献

1) 国立教育政策研究所教育課程研究センター：「指導と評価の一体化」のための学習評価に関する参考資料，高等学校情報科（2021 年），https://www.nier.go.jp/kaihatsu/pdf/hyouka/r030820_hig_jouhou.pdf

(2021 年 12 月 29 日受付)

前田健太朗（正会員）
k_maeda@hokkaido-c.ed.jp

北海道札幌北高等学校教諭（情報科），北海道高等学校教育研究会情報部会幹事．

…› 石井一夫（公立諏訪東京理科大学）

ゼロからつくる Python 機械学習プログラミング入門

八谷大岳 著
講談社サイエンティフィク（2020），3,000 円+税，368p., ISBN：978-4-06-520612-6

書籍の概要

機械学習を，アルゴリズムをきちんと理解した上でゼロからゴリゴリとプログラミングして実装してみたいと思っている方は少なくないに違いない．本書はその様な野心的な読者の夢を叶えてくれるかもしれない．本書は，回帰分析，分類モデル，カーネルモデル，ニューラルネットワーク，強化学習，教師なし学習など，機械学習の全般的な分析法について，原理的なことから丁寧に説明し，Python での実装を示している．したがって，機械学習の概念を入門書である程度学習した初心者で，本格的な機械学習プログラミングを開始したい人に適している．あるいは，ある程度データ分析を経験している人が，機械学習全体をざっと見通したり，おさらいしたりするのに適している．最初に機械学習の概要を述べ，次に Python の導入方法や基本的な使い方の解説，線形代数や確率統計など数学の復習をした後に，回帰分析，分類モデル，カーネルモデルなど，個々の機械学習法を解説する章が続いている．Python や数学的記述を基本から丁寧に説明する構成のため，機械学習を基礎からしっかり学びたい人に向いている．残念ながら，深層学習については，畳み込みニューラルネットワークなどの最新手法があまり詳しく触れられていないので，詳細を学びたい場合はほかの書籍を当たる必要がある．

本書の特徴は，分かりやすさを優先して数式的な記述や説明を省いたりせず，Python のソースコードについても丁寧に説明されていることである．機械学習の中身やプログラミングの実装に関し，ブラックボックスな部分が少ないという面では，非常にお薦めの書籍である．

本書の内容

第 1 章「機械学習とは何か」では，機械学習が盛んになった歴史的経緯と，代表的な機械学習の分類である教師あり学習，教師なし学習，強化学習について概説している．

第 2 章「Python 入門」では，Python について，Anaconda のインストールから，Jupyter Notebook の導入を説明した後，Numpy の array を中心に解説している．

第 3 章「数学のおさらい」は，線形代数・最適化・確率・統計について Python で実装しながら復習する章である．

第 4 章「回帰分析」は，線形回帰とロジスティック回帰について書かれている．線形回帰は残差を反映する平均二乗誤差の最小化問題であり，最小二乗法と呼ばれるが，この辺りの説明と Python による実装がしっかり説明されている．データの標準化の効果，L2 ノルム正則化による外れ値の処理，目的変数が正規分布に従うことの意味など，線形回帰モデルの重要な項目が網羅されている．ロジスティック回帰は一般化線形モデルを用いた説明であり，交差エントロピー損失の最小化問題であるが，高速計

算を達成するために，Python による行列表現で実装している．

第 5 章「分類」は，教師あり学習において，目的変数がカテゴリカルデータである場合の解説である．線形判別分析（LDA），サポートベクトルマシン（SVM），ナイーブベイズ（NB），決定木（CART）ついて紹介されている．LDA では，分類境界の関数の求め方について，カテゴリ間分散とカテゴリ内分散から構成される相関比の最大化問題として説明している．これを，ラグランジュ未定乗数法による制約付き最適化問題で解くが，これを Python で実装している．SVM の場合，分類境界の関数をマージン（最近傍距離）最大化問題として解くが，これも，ラグランジュ未定乗数法による制約付き最適化問題として，Python による行列表現で実装している．また，詳細は示さないが，NB や CART についても同様に丁寧に書かれている．

以後，内容の詳細な紹介は避けるが，各話題について数式による丁寧な説明の後，Python による実装が紹介されている．

第 6 章「カーネルモデル」は，線形モデルを非線形に拡張するアプローチであるカーネルモデルについて取り扱っている．

第 7 章「ニューラルネットワーク」は，深層学習によるロジスティック回帰モデルと多クラス分類モデルを取り上げている．過学習，ドロップアウト，ミニバッチ，Adam などのトピックも取り上げられている．多クラス分類モデルでは，ソフトマックス関数に基づく手描き文字の分類の例が取り上げられている．

第 8 章「強化学習」は，教師データを用いない機械学習で，基本的な原理と，Q 学習法の紹介である．

第 9 章「教師なし学習」では，代表的な主成分分析，因子分析，クラスター分析を取り上げている．

本書籍をだれに薦めるか

本書籍は，機械学習全般について，原理的なことから数式やコードを使ってきちんと理解したいと考えている学生やエンジニアにお薦めである．教養程度のリテラシーレベルを卒業して，本格的にデータ分析を始めたい人に向く書籍である．単に，AI アプリを使って AI を動かしてみたというレベルに飽きたらない人，もっとガチで AI をいじり倒して中がどうなっているのか知りたい，その上で AI を自分でコーディングできるようになりたいという人はまず読んでみるとよい．

（2021 年 8 月 9 日受付）

石井一夫（正会員）
kishii@rs.sus.ac.jp
公立諏訪東京理科大学工学部情報応用工学科教授，久留米大学医学部内科学講座心臓・血管内科部門客員准教授．専門分野：ビッグデータ分析，計算機統計学，データマイニング，数理モデリング，機械学習，人工知能．医療ビッグデータ，気象ビッグデータ研究に従事．2015 年度本会優秀教育賞受賞．日本技術士会フェロー，APEC エンジニア，IPEA 国際エンジニア．

…› 大石康智（NTT コミュニケーション科学基礎研究所）

言葉をおぼえるしくみ
―母語から外国語まで

今井むつみ，針生悦子 著
筑摩書房（2014），1,400 円+税，416p., ISBN：978-4-480-09594-7

音声や画像，映像といった異なるモダリティにまたがる情報を教師ラベルなしで対応付けるクロスモーダル学習は，今世界的にホットな研究テーマの 1 つである．たとえば，画像と，その画像に写る情景や物体を説明する音声のペアデータを大量に集めて深層距離学習すると，物体の画像領域と，その名前を発話する音声区間が教師ラベルなしで対応付けられる．映像とその様子を説明するナレーション音声のペアデータを大量に集めれば，物体の名前だけでなく，その動きや人物動作が音声言葉と対応付けられる．さらに異なる言語の音声を学習に利用すると，画像や映像を介して，異なる言語間の音声言葉が対応付けられる．

これらは，事前に「うさぎ」の画像と教師ラベルのペアを与えなくても，「皆がこの物体を指して“うさぎ”と言っているようだ．これは“うさぎ”というものなのだな」といった方式での学習であり，私たち人間が生まれてから成長するにつれて，さまざまなことを学んでいく過程にしばしばたとえられる．すなわち，大量の音声や映像さえ与えられれば，語彙や概念，翻訳辞書を獲得できる可能性が示唆される．近い将来，画像や音を見聞きするだけで賢く成長する人工知能ができそうに思えるが，果たしてそんなに単純なことなのだろうか．そもそも，子どもはどのようにして言葉を世界と対応付け，概念を整理し，体系付けて語彙辞書を構築しているのか．このような疑問がきっかけとなり，本書を手にとった．

本書の構成

言葉の習得をテーマにした本の多くは学習過程の観察や自分や身近にいる子どもの言語学習の経験に基づいたものがほとんどのようであるが，本書は心理学の実験に基づいて，学習過程の仕組みを明らかにしようとする「理系的」な本である．

著者らによると，子どもの言葉の学習には 2 つのパラドックスがあるという．第 1 のパラドックスは，理論的には言葉の意味を推論することは非常に難しいはずなのに，子どもは初めて遭遇した言葉の意味をあれこれ迷わずにすぐに推論できるということ．第 2 のパラドックスは，同じ意味領域の，ほかの単語との関係が完全には明らかにならない状況で，子どもはとにかく今出合った 1 つの単語を使えるようになろうとすること．このような二重のパラドックスを子どもがどのように解決していくのかという問題を，多くの実験を通して解き明かしていく．

第 2 章では子どもが，物理的には切れ目のない発話の流れを単語単位に区切り，その単語に意味を対応付けようとする過程の仕組みが解説される．第 3 章から第 8 章までは，著者たち自身のデータを軸に，名詞，動詞，形容詞，助数詞，擬態語の意味推論を，子どもは何を手がかりに，どのように行っているのか論じられる．第 9 章では母語の特徴は子どもの語彙推論のしかたや語彙に関する知識にどのように影響をおよぼしているのか，名詞と動詞に焦点をあてて解説される．第 10 章では子どもは語彙のような巨

大で複雑な「システム」を自分の力でどのように構築することができるのかという問題を考察する．第11章では母語と外国語の語彙学習の過程がどのように違うのかが議論され，外国語を学習する際の効果的な方法が提案される．第12章は今後の研究で明らかにされるべきことがまとめられている．

モノの名前の学習

子どもがどのようにして最も基礎的な，モノの名前（名詞）の意味を推論し，その語の適用範囲を決定しているのか，実験的に明らかにされたことを紹介しよう．たとえば大人が「これはうさぎよ」と指さして言ったとする．このとき子どもは，この新しい語が，「基本的にカテゴリーの名前であり，素材の名前というよりはそのモノ全体を指す名前であり，このモノと形の類似したモノにも使える」という「思い込み」のもとに，意味を推論しているようだ．このような思い込みは語彙についての「メタ知識」と言われ，メタ知識によって「制約」されるからこそ，子どもは急激な速さで語彙を増やし，語彙を構築することができるという．

さらに，名前の分かっているモノに新しいラベルがつけられたとき，しかもその名付けられたモノが動物である場合には，その新しいラベルを固有名詞と見なす．固有名詞が付くことはほとんど考えられないコップやボールのような人工物である場合には，元々知っていた名前よりは範囲の狭い，下位カテゴリー名の名前と見なす．その形が既知カテゴリーの成員として典型的でなければ既知カテゴリーから分離独立させるなど，包摂関係も獲得する．形が似ていないモノでも共通の機能を持つものであれば，上位カテゴリー名の名前と見なす．やわらかくていかにも形の安定性の低そうな対象はモノではなく，物質の名前と見なす．2歳の段階で子どもはこのようにさまざまな知識を組み合わせて，柔軟に意味推論ができることを実験的に明らかにしている．

一方で，第4章以降に解説される動詞や形容詞，助数詞の意味の学習は，名詞の場合と大きく異なり，子どもにとって易しいことではないようだ．それらの学習過程の仕組みも，著者らの膨大な実験に基づいて議論されており，非常に興味深い．

人工知能が語彙を獲得するためには

冒頭で述べたクロスモーダル学習のように大量の事例を利用することなく，子どもは一事例から，対象に対応付けられた新しい語の意味を推論し，その語の適用範囲を決定する．それは子どもが語彙の性質について，抽象的なレベルで豊かな知識（メタ知識）を持っているからである．もちろん，クロスモーダル学習も視覚情報と音声情報の対応関係を距離学習によって獲得するため，メタ知識の1つである形バイアス（語は形が似ているモノに般用できる）を利用した語彙獲得ができていそうに思えるが，巨大な語彙のシステムを人工知能が自ら構築することはまだまだ先のことのように思える．すべてをデータに委ねるのではなく，簡単なルールや構造，もしくは「学習のしかたを学習するしくみ」を導入することが今後の深層学習／機械学習に重要なポイントに思えた．

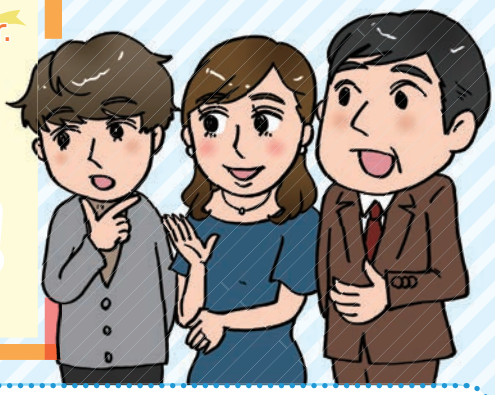
本書は，深層学習や機械学習に取り組んでいる方々にはきっと新しい発見があると思うので，興味のある方はぜひ手に取ってみてほしい．

（2021年12月24日受付）

大石康智（正会員）
yasunori.ooishi.uk@hco.ntt.co.jp
2009年名古屋大学情報科学研究科博士後期課程修了．博士（情報科学）．同年NTTに入社．現在，NTTコミュニケーション科学基礎研究所主任研究員．主に音声や映像などのメディア認識，生成，探索技術に関する研究開発に従事．

連載

先生，質問です！



芸術をさまざまな角度から研究している研究者のみなさまにお答えいただきました．

満柏
社会人

芸術家が，芸術を研究する情報学の研究者を見つけるには，どうすればいいでしょうか？

Q

大きく分けて 3 種類の研究をしている科学者がいます．まず芸術作品の研究をする科学者，次に芸術体験の研究者，最後に芸術制作を研究する科学者です．1 つ目の作品研究は，素材や技法，時代や作者，主題や形式を対象としています．いつ，どこで，誰が，どのように，何を作ったのか．いわば物としての芸術の研究者です．2 つ目は感性の研究と言い換えてもよいでしょう．芸術体験をする人の感覚はどのように働いているのでしょうか．何らかの手段で感動している脳の状態が再現できれば，芸術は必要ないのでしょうか．こちらは芸術を効果の側から研究していることになります．最後はプログラム等による作品制作の研究です．これは作品と体験の研究を統合したものと言えるかもしれません．絵画や音楽，あるいは文学でさえも，作品の具体化には素材への理解が欠かせませんし，制作を終えるためには出来栄えを判断する感性が必要です．おそらく「情報学の研究者」と限定した場合でも，研究者の関心の中心がどこにあるのかで，研究活動の内実は大きく異なります．特定の研究テーマを持っている研究者を探すことは難しいかもしれませんが，関心の近い研究者が見つかるとよいですね．

最後に自分のことを話しますと，文化財全般の資料を整理し，データベース化する仕事を行っています．画家が日記に記したある 1 日の天気や食事は，その日の創作にどのような影響を与えたでしょうか．研究の基礎資料に加えていただければ，と思いながら業務をしております．

小山田智寛
東京文化財研究所

A

「先生，質問です！」・「先生が質問です !!」への質問・回答募集

▸ **Web から質問する：** 下記の Web ページ内の投稿フォームから質問をご記入ください．
「先生，質問です！」 https://www.ipsj.or.jp/magazine/sensei-q.html
「先生が質問です !!」 https://www.ipsj.or.jp/magazine/senseiga-q.html

先生，質問です！　先生が質問です !!

▸ **回答募集：** 情報処理学会 Facebook ページ（@IPSJ.official） Twitter アカウント（@ipsj_shinsedai）

迎山和司
公立はこだて未来大学

レオナルド・ダ＝ヴィンチ（Leonardo da Vinci）は芸術を研究した科学者といえます．彼および同時代のルネサンスの芸術家たちが発明した遠近法は有名です．近代以降ではポール・セザンヌ（Paul Cézanne）も芸術を研究した科学者といえるでしょう．彼はたとえば同じ山の絵を何枚も描くことによって，自分の心が感じた印象を理論的に研究しました．前者の遠近法はコンピュータ・グラフィクスの基礎になり，今日では多くの科学者がその新しい表現を研究しています．後者の印象の研究はどうでしょうか？　印象は他者には観察しにくい情報であり，科学として扱いにくいかもしれません，しかし，今日の人工知能は，この印象の情報をますます柔軟に扱えるようになってきています．したがって，人工知能に絵を描かせることによって，心で感じた印象を科学としてますます研究できるようになるかもしれませんね．私はそうしています．

A

久保田晃弘
多摩美術大学

まず，何はともあれ本会の Web ページで，「芸術」を検索すると 902 件，「アート」を検索すると 634 件の項目がヒットします（2022 年 2 月 10 日現在）．芸術も，情報学もともに広範な領域なので，それぞれの項目を地道に調べていくと，「この人に会ってみたい」あるいは「この人の話を聞きたい」という人が見つかる可能性があります．もし見つかったら，その人の所属先なり，あるいは連絡先などを（これも検索すれば見つかる場合があります）に，メールなどで連絡してみるのがよいと思います．他者との協働を志向する研究者は，基本的にオープンなマインドの持ち主なので，それで返事がなかったら，その人はそもそも芸術には関心がない研究者だと思っていただいて，ほぼ間違いありません．芸術やアートを，単に道具として利用しているだけの研究者も多いので，ここは注意が肝心です．

より広く芸術と科学技術の協働は，古くからその必要性が謳われているにもかかわらず．生産性や効率，成功や完成を重んじる現代の価値観によって，領域化や専門化は，今なお進行し続けているように思います．そうした中で，異なる分野の本格的な協働を何とかして実現しようとする試みが，散発的にではありますが行われています．たとえば，科学技術広報研究会（JACST）の坪井あやさんが中心となって行っている「ファンダメンタルズ」という試みは，実際に芸術家と科学者が出会って議論する場を設けることから始める，きわめて重要な挑戦です．ある 1 つのジャンルの芸術家や，ある 1 つの分野の研究者になるだけでも，長い時間が必要なように，異なる分野との協働作業にも，それと同等の，あるいはそれ以上の長い時間が必要です．そのためにも，まずは良い研究者との出会いが，なにより重要かと思います．論文の数や，メディアへの登場回数などに惑わされず，（自分の関心や研究だけではなく）芸術家の創作活動そのものに対して本気で興味を持ち，他者との共同作業という，一見非効率で無駄に思える作業に対して，時間だけでなく，心身を注いでくれる方が見つかることを願っています．

A

A

芸術の 1 つである「音楽」を扱う「音楽情報処理」の分野を，約 30 年間研究しています．また，2010 年 6 月の情報処理学会誌に「音楽情報学」の解説を執筆しました．その立場から回答します．

インターネット上にはさまざまな検索サービスがあるので，単に研究者を「見つける」だけでしたら，興味のあるキーワードと「情報学」「研究者」等を組み合わせて検索すれば発見可能になっています．ですので，こうしたご質問をいただいた背景には，特定の目的を達成するために相談できる研究者を見つけたい，あるいは，芸術の特定の事項に関してきわめている研究者を見つけたい，というような，通常の検索では困難な状況があったのかと思います．

芸術家と同様に，研究者も，それぞれ異なる考えや興味，得意分野を持っています．たとえば音楽情報処理でも，信号処理や記号処理，機械学習等の基礎側を得意とする研究者もいれば，インタフェースやアプリケーション，サービス等の応用側を得意とする研究者もいます．また，鑑賞に関連した研究（たくさんの楽曲の中から好みの楽曲を見つけて聴くインタフェース研究等）をしている場合もあれば，創作に関連した研究（新たな表現を切り拓くデジタル楽器開発等）をしている場合もあります．このように多様なので，たくさんの研究者の中から見つけるのが難しく感じるかもしれません．

そこで見つけやすくなる方法を 3 つご紹介します．1 つ目は，学術論文から探す方法です．芸術家にとっての作品に相当するのは，研究者にとっての学術論文です．研究者を見つける，と考えるより，論文を見つけてからその著者に連絡する，と考えた方が近道なことがあります．インターネットで論文題目をキーワード検索してもよいですし，情報処理学会の「電子図書館」も活用できます．2 つ目は，研究者コミュニティを活用する方法です．研究者はコミュニティを作って活動していて，お互いの研究内容を把握しているので，その 1 人に「こういう研究者はいませんか」と質問すれば，より適切な人を紹介してくれます．学会はまさにそうしたコミュニティで，たとえば情報処理学会の研究会等で主催者・司会に相談をすれば教えてくれるかと思います．3 つ目は，報道記事等から探す方法です．研究者が芸術家と連携した事例は，論文よりも報道記事や作品発表等の方が見つけやすいこともあります．

芸術と技術の親和性は高く，新たな技術が，新たな表現や新たな鑑賞方法を生み出してきました．たとえば音楽でも，ピアノやギターが発明された時点では当時の新技術でしたし，楽音・歌声合成技術は新たな表現を切り拓き，音楽配信技術は聴き方を大きく変えました．物質的な豊かさだけでなく，心の豊かさが重視される世界において，今後も情報学の研究者が芸術とかかわる場面と重要性は増していくと確信しています．

後藤真孝
【正会員】
産業技術総合研究所

● 論文誌ジャーナル掲載論文リスト

Vol.63 No.3（Mar. 2022）

【特集：若手研究者】

■ 特集「若手研究者」の編集にあたって　下條真司
■ 新型コロナウイルスパンデミックにおける健康危機管理用情報システム過剰なトップダウンが引き起こしうる逆説的状況と教訓　町田裕璃奈 他
■ 夜間光画像を用いた詳細な地域経済分析の可能性　大友翔一
■ オンラインジャッジシステムにおける解答履歴を利用した問題の関係性調査　槇原絵里奈 他
■ フラワーゼリーの自動造形に向けたスリットインジェクションプリンティングと設計ソフトウェアの実装と評価　宮武茉子 他
■ ピアノ学習における課題曲合格時期予測システムの構築　松井遼太 他
■ Grasping Users' Awareness for Environments from their SNS Posts　Tokinori Suzuki 他
■ A Printable Soft-bodied Wriggle Robot with Frictional 2D-Anisotropy Surface　Tung D. Ta 他
■ 有限オートマトンを用いた私的観測繰り返しゲームにおける進化的安定戦略分析　小池淳平 他
■ 不完全情報ゲーム「ガイスター」における相手駒色推定の有効性評価　竹内聖悟 他
■ 列車自動運転を伴う運転整理 MIP モデルの移動閉塞下への適用　川添宏介 他
■ 高発生確率インパルス雑音除去を目的とした Robust Non-local Median Filter のカラー拡張　松岡丈平
■ ネットワーク可視化における拡大描画に適したエッジバンドリング手法　秋山桂一 他
■ Midori128 に対する電力解析攻撃手法と低エネルギーなセキュア実装　竹本　修 他
■ SPGC: Integration of Secure Multiparty Computation and Differential Privacy for Gradient Computation on Collaborative Learning　Kazuki Iwahana 他
■ 秘密分散法を利用した PUF のセキュア認証方式とその評価　野崎佑典 他
■ A NIC-driven Architecture for High-speed IP Packet Forwarding on General-purpose Servers　Yukito Ueno 他
■ An IoT System with Business Card-Type Sensors for Collaborative Learning Analysis　Shunpei Yamaguchi 他

【特集：新しい生活様式を見据えたインターネットと運用技術】

■ 特集「新しい生活様式を見据えたインターネットと運用技術」の編集にあたって　中村　豊
■ A Campus Equipment Controller Using an IoT System that Can Configure and Control its Edge Devices Behind a NAT using Wiki Pages on the Internet　Takashi Yamanoue
■ Low Overhead TCP/UDP Socket-based Tracing for Discovering Network Services Dependencies　Yuuki Tsubouchi 他
■ AI による脆弱性情報の注意喚起予測　渡辺　龍 他
■ リアルタイム挙動に基づく動的アクセス制御を効率的に実現するゼロトラストアーキテクチャ　川口信隆 他
■ 事業継続性に配慮した認証基盤システムの構築と運用　土屋雅稔 他

【一般論文】

■ 一般化された Sine 積分 Si (a,x) と Cosine 積分 Ci (a,x) の数値計算法†　吉田年雄 他
■ 自治体セキュリティモデルのためのリスクアセスメント手法の提案と適用　佐々木良一 他
■ ComposableThreads: Rethinking User-level Threads with Composability and Parametricity in C++　Wataru Endo 他
■ A Proposal of Communication Protocol to Improve the Throughput and Fairness of Multi-hop Wireless Networks and its Evaluation　Taiki Morita 他
■ RFID タグアレイを利用した非画像信号からの画像復元法とトイレ行動認識システムへの応用*　大嶋政親 他
■ スロバーの回転速度がユーザの待ち時間に与える影響の考察　大島寛斗 他

*：推薦論文　Recommended Paper
†：テクニカルノート　Technical Note

● 論文誌トランザクション掲載論文リスト

（Mar. 2022）

【Transactions on Bioinformatics Vol.15】

■ Predicting PRDM9 Binding Sites by a Convolutional Neural Network and Verification Using Genetic Recombination Map　Takahiro Nakamura 他

【論文誌 数理モデル化と応用 Vol.15 No.2】

■ ナーススケジューリングにおける多様な解の生成　加藤尚瑛 他
■ 弱教師あり学習による連続的な表情特徴の獲得　狩野悌久 他

◎ IPSJ カレンダー◎

学会イベントの最新情報を下記 URL でご案内しています．新型コロナウイルス感染症拡大を受け，開催方法の変更，開催中止などの可能性がありますので，最新情報をご確認いただきますようお願いいたします．

https://www.ipsj.or.jp/calendar.html

計算機科学を推進した富田悦次君を悼む

横森　貴 | 早稲田大学
西野哲朗 | 電気通信大学

本会フェロー（2003年度），功績賞受賞者（2019年度），電気通信大学名誉教授富田悦次氏は，2021年9月1日に逝去され，コロナ禍のため9月3日に近親者のみで葬儀が営まれた．富田氏と久しくお付き合いしたものとして，横森と西野で追悼文を寄せたい．

富田氏は，1971年3月に東京工業大学大学院理工学研究科電子工学専攻博士課程を修了，直ちに同大学工学部助手として勤務された後，1976年10月に電気通信大学電気通信学部助教授に着任され，1986年4月に教授となった．

富田氏は，永年にわたりオートマトン・言語理論，学習理論，組合せ最適化などの分野において研究と教育に携わり，先駆的で優れた業績を挙げられた．まず同氏は，決定性文脈自由言語の等価性判定問題に対し，統一的でまったく新たなアルゴリズムを考案され，併せて，国際的にも早い段階から計算論的学習理論の新方式を提唱された．

組合せ最適化問題においては，クリークと呼ばれるグラフ構造に早い段階から注目し，クリーク抽出に関する研究を永年に渡り先導してきた．中でも，極大クリーク全列挙のために考案した最適アルゴリズムは，アルゴリズム分野にとどまらず，幅広い分野から活用，引用され，世界的に高く評価されている．また，以上に関連したいくつかの国際会議では，実行委員長，プログラム委員長，大会委員長，招待基調講演などを務められている．

一方，教科書『オートマトン・言語理論』[1]は初版から改訂第二版に渡って計30増刷を重ね，富田氏は，この分野の教育に多大の寄与をされた．

上記の卓越した研究業績に対しては，船井情報科学振興賞，電子情報通信学会フェロー，および本会フェローなどを授与されている．本会においては，会誌編集委員会主査，数理モデル化と問題解決研究会主査，コンピュータサイエンス領域委員会委員長，理事などを歴任され，特に若手研究者の育成，情報教育の充実に努められた．

以下では，富田氏が，国内外の情報科学分野，ならびに本会の活動の発展に尽くされたご功績について，具体的に述べていきたい．

学習理論と推論アルゴリズム

富田氏は，オートマトン・言語理論，学習理論の分野において先駆的で優れた業績を挙げられた．具体的には，人工知能の基本である「学習理論」の重要性について世界に先駆けて着目し，その成果を1970年代に国際会議や論文誌に発表した．これらは，1980年代になってから発表された著名な正則言語の学習アルゴリズムの主要概念をすでに含んでいる先駆的成果であった．この学習の過程においては「等価性判定」が基本的に重要な問題となるが，これは正則以上の言語においては一部を除いてほとんど未解決で困難な問題で

あった．これに対し，ある種の広いクラスの決定性プッシュダウンオートマトンにまで適用できる画期的に簡潔で効率的な新しい等価性判定方式を確立した．

言語の帰納的学習は古典的かつ重要な研究課題としてよく認識されており，正則言語の学習アルゴリズムはAngluinによるMAT（Minimally adequate teacher：極小最適教師）学習モデル[2]が著名である．この学習アルゴリズムにおいて中核となるアイディアは質問と反例を許すことにより目標の有限オートマトンの本質を捉える「代表的な正例の有限集合」をあぶり出すところにある．富田氏らはAngluinに先んじること10年前に，すでに論文[3]において「代表記号列集合」という重要な概念を提案し，有限オートマトンの効率的な学習アルゴリズムの結果を導いている．この結果と概念はMAT学習アルゴリズムにおける本質的な特性を捉えているものであり，高い評価を得ている．さらに富田氏らは，論文[4]においてこの代表例集合という概念を単純決定性文法にまで拡張し，正則言語族を真に包括する単純決定性言語族に対する効率的な学習アルゴリズムを導くことに成功している．

最大クリーク抽出問題

また，富田氏は組合せ最適化問題の分野においても，人と人との繋がりに代表されるような大規模なネットワークデータの解析において本質的な役割を果たす，クリークと呼ばれるグラフ構造に早い段階から注目し，クリーク抽出に関する研究を永年に渡り先導してきた．中でも，極大クリーク全列挙のために考案した最適アルゴリズムは，アルゴリズム分野ばかりでなく，幅広い分野から活用，引用され，世界的にも高く評価されている．最大クリーク抽出問題に対する高速アルゴリズムを次々と開発し，同問題の発展の国際的中心の1つとなっている．これらのアルゴリズムは，共同研究を通して多くの応用分野に巧みに活かされている．

2001年に発表した最大クリーク抽出アルゴリズムは，DIMACS国際ベンチマークテストのいくつかにおいて，当時の標準的なアルゴリズよりも数十から数十万倍の高速性を実現した．さらに，当時の既存アルゴリズムに対しても格段に高速であることが実証され，国際的に高い評価を受けた．この高速化達成により，提案アルゴリズムをさまざまな実問題解決に応用することが可能となり，新たな応用分野における研究成果を生み出している．

実際，これらの組合せ最適化アルゴリズムは新聞報道（2002年2月25日付）によって，「電通大が新手法ー爆発的計算を解く」などと紹介されている．これにより多くの企業からも種々の問合せが富田氏に寄せられ，富田氏はそれらに対応して企業側へ多くの助言を与えるなど，バイオ研究者をはじめ産業界へも強いインパクトを与えた．

富田氏が研究者としてのみならず，基盤技術研究促進センター技術評価委員やJST新技術審議会新技術開発部会専門委員を通して，企業の技術評価を担当し社会的貢献をしている点も特筆すべき業績である．

学界における活動と貢献

富田氏は，本会において輝かしい活動歴を残されている．まず，本会編集委員会における委員，幹事，主査（基礎・理論分野）としてさまざまな特集号の企画・編集を実践し（1980年から），数理モデル化と問題解決研究会においては連絡委員，運営委員，主査などを歴任し（1995年から），その間，論文誌「数理モデル化と応用」では編集委員を務めている（1998年から）．2000年度の全国大会では，公開シンポジウム「新しい計算パラダイム～量子・分子コンピュータ最前線～」を企画・実行して好評を得た．さらに，調査研究運営委員会のコンピュータサイエンス領域委員会では財務委員，委員長として活躍している（2001年から）．また2007年に理事（教育・調査研究担当）として寄稿した，一般社会に対して「高度IT教育と人材育成への支援」の重要性を唱えた記事[5]はまだ記憶に新しい．

一方，富田氏の学界への貢献は電子情報通信学会における各種委員会・研究会の委員，幹事としての活動にとどまらない．同氏は1991年の国際ワークショップALT91をかわきりに，多岐に渡る国際ワークショップ・国際会議におけるプログラム委員，実行委員長などを務めることにより，理論計算機科学分野における我が国を代表する研究者として国際的に認められた．これ

らの活躍は，電子通信学会米澤記念学術奨励賞（1971 年 10 月），船井情報科学振興賞（2003 年 3 月）などの受賞によって結実されている．また，上述の業績が高く評価されて，2003 年度に電子情報通信学会よりフェロー称号を，本会よりフェロー称号を，それぞれ授与された．また，2005 年から 2007 年には，本会理事（教育／調査研究担当）としても大変活躍された．

また極大クリーク全列挙論文[6]は，理論計算機科学の著名論文誌である Theoretical Computer Science から 2005 ～ 2010 年最多被引用論文賞（2010 年）を受賞し，重ねて同誌の創刊 40 周年に際しては，出版年（2006 年）論文中の最多被引用論文表彰（2015 年）も受けている．なお，同論文の Google Scholar 上引用文献数は 700 件超であり，出版後十数年でのこの値は理論計算機科学分野においては非常に高く，さらに現在も増加を続けている．

名著：『オートマトン・言語理論』

富田氏は教育に対する熱意にも定評があり，教科書『オートマトン・言語理論』[1]は，出版以来，大学・大学院等の教科書・参考書として広く採用され，ほぼ毎年改訂を伴った増刷を重ねる名著となっている．

1989 年 4 月，横森は富士通・国際情報社会科学研究所から電気通信大学へ赴任し情報工学科に籍を置いたが，その当時，富田氏は電子情報学科に属しており，当初は直接の面識はなかった．その後，帰納的学習理論やオートマトン・言語理論など共通の研究テーマの興味が縁でお付き合いさせていただくことになった．

計算機科学における基礎理論の 1 つである“オートマトンと形式言語理論”に関する教科書は国内外を問わずあまた散見される．1990 年春のある日，富田氏から電話があり「講義で便利に使用できる教科書を作りたいのだけれど……」というお誘いを受けたことを契機にさらに親交を深めるに至った．本書の執筆の背景として，富田氏には，当時所属していた（情報系ではない）通信工学科学生の教育を念頭に，極力理解しやすいように準備された長年に渡る膨大な講義資料を出発点とするお考えがあった．

執筆において心得るべき基本方針として，「数学的な内容を（従来の数学的な議論の展開法は極力避け），まず具体的な理解しやすい実例から出発して，より一般的な説明と定義を与えてその後に定理を示し，かつその証明も可能な限り厳密性を保つ」という完璧性が希求された．執筆の過程の随所においては，本分野の初学者に対する氏の繊細な気配りが感じられ，選択した各テーマの説明，提示法，証明に関する「緻密な考察と配慮の深さ」には圧倒されることがしばしばであった．一方，本書の素稿の作成から校正においては清野和司氏，若月光夫氏，樋口健氏をはじめ多くの卒業生の協力によっていると伺っている．

このようにして 1992 年 5 月に『オートマトン・言語理論』（富田･横森共著）は，（飯島泰蔵先生が編集された）“基礎情報工学シリーズ”における第 5 巻として初版第 1 刷が森北出版から発行された．その後，2008 年頃に出版社と“第 2 版への改訂増補版”の話がまとまり，その準備に取り掛かった．この改訂作業にあたっては，予期しない苦難が待ち受けていた．初版執筆の当時，原稿の作成はもっぱらワープロによるのが主流であり，TeX のような Markup 言語のファイル形式はまだ一般的ではなかった．そこで，第 1 版の電子ファイルを出版社から取り寄せ，それを Tex ファイルへ変換しなければならず大変な苦難を経験したことが懐かしく思い出される．

本書は出版以来，大学・大学院等の教科書・参考書として広く採用され，我が国の情報処理基礎教育に対して多大の貢献をしている．実際，1992 年の第 1 版第 1 刷から第 24 刷りの重版を重ね，また 2013 年 12 月に出版された第 2 版もすでに第 7 刷を終え，今まさに第 8 刷を迎える．30 年間に全 32 刷を数えるという情報系教科書としては類い稀な大ロングセラーとなっている．

今でも，筆者らは「富田氏の教科書が好きだ」という学生に新たにお目にかかることがある．このたび，本稿のご依頼をいただいた本書の著者の 1 人（横森），読者の 1 人（西野）として，ここに富田氏のご冥福をお祈りし，感謝の言葉を述べさせていただきたいと思います．ありがとうございました．

参考文献

1) 富田悦次，横森　貴：オートマトン・言語理論，（基礎情報工学シリーズ 5）森北出版 (1992)．第 2 版（改訂増補版）(2013).
2) Angluin, D. : Learning Regular Sets from Queries and Counterexamples, Information and Control 75, pp.87-106 (1987).
3) 榎本　肇，富田悦次：代表記号例集合による決定性有限オートマトンの適応的修正法, 電子通学会論文誌, 60-D, pp.777-784 (1977).
4) E. Tomita and K. Seino: A Direct Branching Algorithm for Checking the Equivalence of Two Deterministic Pushdown Transducers, One of Which is Real-time Strict, Theoretical Computer Science 64, pp. 39-53 (1989) .
5) 富田悦次：社会に存在感ある学会として – 幅広い立場からの情報教育支援を –, 情報処理, Vol.48, No.3, pp.296-230 (Mar.2007)
6) Tomita,E., Tanaka,T. and Tanahashi,H. : The Worst-case Time Complexity for Generating All Maximal Cliques and Computational Experiments, Theoretical Computer Science 363 (1), pp.28-42 (2006).

（2022 年 2 月 7 日）

横森　貴（正会員） yokomori@waseda.jp

1979 年東京大学大学院理学系研究科博士課程修了．1983 年富士通（株）国際情報社会科学研究所, 1989 年電気通信大学助教授・教授, 1998 年早稲田大学教授を経て，2021 年早稲田大学名誉教授．理学博士．オートマトン・形式言語理論，計算論的学習理論．自然計算理論に関心を持つ．本会フェロー（2018 年度）．

西野哲朗（正会員） nishino@uec.ac.jp

1984 年早稲田大学大学院理工学研究科博士前期課程修了．1984 年日本アイ・ビー・エム（株），1987 年東京電機大学・助手，1992 年北陸先端科学技術大学院大学・助教授 , 1994 年 電気通信大学・助教授を経て，2006 年 同大学教授．理学博士．回路計算量理論，量子計算量理論, 自然言語処理, ゲーム情報学などの研究に従事．2008 年 IBM Faculty Award，2010 年文部科学大臣表彰各受賞．

富田悦次氏 御略歴

1966 年東京工業大学・理工学部・電子工学科卒．1971 年 同大学院博士課程修了．工学博士 .

1971 年東京工業大学・工学部・電子物理工学科，情報工学科助手を経て，1976 年 電気通信大学・電気通信学部・通信工学科助教授，1986 年同教授．1987 年電子情報学科教授．1999 年 情報通信工学教授，2003 年 電気通信大学先進アルゴリズム研究ステーションを創設し初代研究ステーション長，2008 年 電気通信大学名誉教授（現在に至る）．2008 年中央大学研究開発機構教授（～ 2011 年）．2011 年，科学技術振興機構 ERATO 湊離散構造処理系プジェクト研究推進委員，東京工業大学・大学院情報理工学研究科 特別研究員（～ 2015 年）.

Algorithmic Learning Theory（ALT）1993 Local Chair, ALT 2005 PC Chair, International Colloquium on Grammatical Inference（ICGI）2006 Conference Chair, ICGI Steering Committee Member 2004-2012, International Workshop on Algorithms and Computation（WALCOM）2015 PC Co-Chair, Theoretical Computer Science（TCS）, Journal of Discrete Algorithms, Journal of Graph Algorithms and Applications の Guest Editor.

視聴覚情報処理研究会（AVIRG）幹事（1972 ～ 1973 年度），電子通信学会海外論文委員会委員（1973 ～ 1974 年度），電子通信学会学生委員会委員（1975 ～ 1976 年度），電子通信学会論文委員第 4 部（1980 ～ 1983 年度），電子通信学会 オートマトンと言語研究専門委員会 幹事（1983 ～ 1985 年度），電子通信学会コンプレクシティ研究専門委員会（第 3 種）専門委員（1985 ～ 1987 年度），電子情報通信学会コンピュテーション研究専門委員会専門委員（1986 ～ 1992 年度），電子情報通信学会フェローズ＆マスターズ未来技術時限研究専門委員会専門委員（2005 ～ 2011 年度），

情報処理学会 会誌編集委員会基礎・理論分野 主査（1982 ～ 1983 年度），情報処理学会論文誌 数理モデル化と応用 論文誌編集委員会編集委員（1998 ～ 2001 年度），情報処理学会数理モデル化と問題解決研究会主査（1999 ～ 2000 年度），情報処理学会コンピュータサイエンス領域委員会委員長（2003 ～ 2005 年度），情報処理学会理事（教育／調査研究 担当）（2005 ～ 2006 年度），情報処理学会情報処理教育委員会委員（2005 ～ 2014 年度）
LA シンポジウム代表（2002 年度），人工知能学会評議員（2004 ～ 2005 年度），国際学生技術研修協会（IAESTE）理事，科学技術振興事業団新技術審議会新技術開発部会専門委員，日本学術振興会科学研究費補助金審査委員（第 1 段，第 2 段）など歴任.

ICGI 2021, WALCOM 2022 の PC Member, ISRN Discrete Mathematics, American Journal of Operations Research, Industrial Engineering and Management の Editor, Mathematical Reviews of American Mathematical Society の Reviewer，文部科学省科学技術政策研究所科学技術動向研究センター専門調査員，等.

電子通信学会米澤記念学術奨励賞（1971 年），船井情報科学振興賞（2003 年），電子情報通信学会フェロー（2003 年度 ），情報処理学会フェロー（2003 年度），情報処理学会数理モデル化と問題解決研究会 功績賞（2006 年度 ），Theoretical Computer Science Top Cited Article 2005-2010 賞（2010 年), Theoretical Computer Science Top Cited Article 2006 (2015 年), INTECH AWARD DIPLOMA（2014 年), 情報処理学会功績賞（2019 年度），など受賞．IEEE，ACM，EATCS，人工知能学会，等会員.

編集長退任にあたって

このたび無事会誌編集長の任期を終え，塚本昌彦前編集長から引き継がれたバトンを五十嵐悠紀先生にお渡しする運びとなりました．

就任時方針として「情報処理 X」を掲げました．これは他分野の中で活用される情報処理技術を紹介する特集に積極的に取り組むこと，会員を含む情報処理技術に興味を持つ幅広い人々の交流の架け橋となるような「同人誌」としての機能を強化することを目指したものです．この目標に対する現時点での達成度を KPT（Keep, Problem, Try）に分類しまとめます．

Keep：

- **編集委員会の各ワーキンググループ（WG）提案の特集記事に加え，たとえば『弔いと技術革新』（2018 年 7 月号），『牛と IT/ICT』（2018 年 11 月号），『植物と情報処理』（2021 年 12 月号）など，さまざまな分野の中での情報処理技術をつなぐ特集をしました．**

私見ではありますが，編集長があえてツッコミどころのある企画を提案することで，WG からも野心的な提案を多数いただくことができたのかもしれません．そのおかげで任期中，特集記事の企画に悩むことはほとんどなく，むしろどの記事を先に出すかという議論がメインとなりました．良い研究者になるためにはツッコミを入れレビューする力が大切だが，良い研究マネジメントのためにはあえてボケる力も重要という持論を編集委員会の運営にも活用できたのかもしれません．

- **情報処理技術に興味を持つ人々の交流を促す試みとして，『技術書典』に出展するとともに 60 周年企画『JOSYORI』を発刊しました．**

「技術者のコミケ」ともいわれる技術系同人誌を頒布するための即売会『技術書典』に湯村翼委員の主導で会誌編集委員会としても参加することにしました．事務局の皆さんや編集委員の方々も会場に売り子に駆け付け，「あの情報処理学会が本気で同人イベントに参加している」という驚きの声とともに迎えられました．現在技術書典は新型コロナウイルス蔓延に伴いオンライン開催されていますが，SNS を眺めるに好評を博しているようです．

また，中田眞城子副編集長を中心に編集委員会としての 60 周年企画として，非専門家向けの IPSJ 情報処理カタログ『JOSYORI』を発刊しました．情報処理に関する興味深い研究やイベントを漫画で紹介する『IT 紀行』もジュニア会員にとどまらず一般会員からも人気の記事となっているようです．

- **note，Twitter などオンラインサービスを活用した発信を強化しました．**

よりカジュアルにオンラインで発信できる Web サービス『note』にて記事を配信するとともに，学会公式の Twitter アカウント @IPSJ_official を整備，活用するなどオンラインサービスを活用した発信を強化するとともに，学生委員の協力を得つつ安定した運用を実現しました．現在 Twitter アカウントは 5,000 人弱のフォロワーを集めるに至っています．

また，コロナ禍の中でハイブリッド化・オンライン化された大会での編集委員会企画イベントを実現するため，YouTube Live やメタバースプラットフォーム『cluster』を活用しました．情報処理技術を活用することで，困難を創造的に解決する本学会の姿を見せることができたと思います．

Problem：

- **紙の長所を損なわない電子化**

私の任期中に起きた会誌最大の変化として，記事の完全電子化が挙げられます．ヒューマンコンピュータインタラクションにもかかわる研究者として，物理メディアとしての紙雑誌の特性や価値は十分認識するものではあります．コスト削減のための紙質の低下やページ数の制限などジリジリと撤退戦を行うより，会誌としてのコンテンツを紙面に制限されず充実させること，動画やプログラムなど，オンラインならではのコンテンツにも注力することを優先し，決断しました．

しかしながら，PDF 原稿はスマートフォンでは読みにくい，Push 型から Pull 型の閲覧形態となり，かえって記事を読まなくなったなどの声が多数寄せられました．編集委員会としても note での配信を強化する，一時的に EPUB を試用するなどの取り組みを行うなど試行錯誤しています．紺屋の白袴とならず，会員の英知を結集し，さすが情報処理学会と言われるような会誌の在り方を，今後も模索し続ける必要があるでしょう．

- **編集長 Blog**

こちらは私の筆不精が原因で 2018 年 4 月に編集長を引き継いで 3 カ月で更新が止まってしまいました．三日坊主ならぬ三カ月坊主です．一方で 2020 年 6 月より，先に紹介した学会公式 Twitter と私の個人 Twitter アカウントで会誌に関する情報を積極的に発信することにし，blog からソーシャルメディアに発展的に移行したともいえますが，お恥ずかしい限りです．

- **懇親会**

コロナ禍以前は編集委員会の後に有志で懇親会を開き，そこ

でもカジュアルに新たな特集や企画案を議論しました．with/post コロナでのカジュアルな議論の場をどう設定するかは今後も課題になりそうです．

Try：

- **ワークライフバランスへの取り組み**

毎月平日の夜に化学会館に集まり，お弁当を食べながら長時間しっかり議論を行うというかつての編集委員会の運営方針を否定するものではありません．しかし遠方の委員や子育て中の委員から，夜の会議ばかりだとなかなか参加できないとの声が挙がったことを契機とし，昼と夕方に交互で開催することにしました．また Slack を活用し会議以外の時間も議論や承認プロセスを行うことで，編集委員会の時間をおおむね 60 ～ 90 分程度とすることができました．コロナ禍の中で現在はすべて Zoom で編集委員会を行っており，むしろ遠方の委員にも声をかけやすくなったともいえます．ボランティアとしての編集委員により運営されている故に時間的コストをなかなか意識しにくい編集委員会の運営方針については，今後も継続的に議論する必要があると考えます．

- **広報広聴委員会と連携した戦略的な企画**

従前より読者アンケートにより会誌記事へのコメントや会誌そのものへのフィードバックをいただき，それを編集方針の参考としてまいりました．本会に広報広聴戦略委員会が設置され，大規模アンケート調査などにより，幅広く会員の声が集められるようになりました．今後は当該委員会と連携しつつ本会における会誌の位置づけも含め，戦略を練ることが一層重視されることでしょう．

- **より幅広い読者層への普及**

本会誌発刊号にて初代会長の山下英男先生は“会員諸君に親しみやすい，しかも品位のある雑誌を作りたいと思います”と述べられました．編集長として会誌としての品位を保てたかは自信がございませんが，今後は多様な会員，未来の会員，そして非会員であっても情報処理技術のサポータとなるような方々のハブとなるような会誌となってほしいと会員の 1 人として望んでいます．

以上思いつくままに述べさせていただきました．就任当初，筆不精で慢性的に原稿が遅れがちな私が編集長を無事務められるか大いに不安でした．しかし編集委員会での取り組みは想像以上に創造的な活動であり，事務局や副編集長，編集委員の方々のおかげで楽しく任を終えることができました．会誌の読者各位も含め，この場をお借りし深謝いたします．

今後も情報処理技術を活用し「自我作古」の心がけでさまざまな学会の会誌の DX をリードする情報処理学会会誌であることを願ってやみません．

（稲見昌彦／東京大学）

『cluster』を活用した情報処理学会第 83 回全国大会『先生，質問です！』公開セッション

副編集長退任にあたって

これまで副編集長兼編集委員の業務を担当していましたが，このたび 4 年間の任期を満了し退任することになりました．編集長をはじめ多くの編集委員や事務局の方には大変お世話になりました．任期中に，原稿の閲読，執筆候補者との交渉，会誌全体のデザインに関する議論などのさまざまな業務にかかわらせていただきました．この仕事は新鮮な刺激を与えてくれて楽しいものであったとともに，勉強になるものでもありました．モニタからの高評価のコメントや辛辣なご意見にも，毎号考えさせられました．ほかの方の効率的な仕事の進め方，たとえば Slack を用いた即時性の高い編集上の議論や情報共有からは，多くの学びがありました．また，稲見編集長の，新しいことや面白いことに対する飽くなき情熱や，膨大な仕事の各々に力を配分する高い能力も印象的でした．編集委員にも能力がきわめて高い方がおられ，それらの方の言動にも考えさせられるとともに，仕事への意欲を高められました．

編集委員は全員が非常勤の，ある意味ボランティアであり，普段は企業，大学，組織などの仕事を行っています．その中で会誌の編集にどのように向き合い，どの程度コミットしていくかについては，どなたにとっても単純な話ではないと想像しています．私にとっても，日々，試行錯誤の連続でした．編集委員会全体としては，私の任期中に，ワークライフバランスの考慮や仕事量の削減について，多くの地道かつ重要な改革が行われたことが印象的でした．

編集委員としては特集記事「『京』の後の時代を支えるスパコン」のエディタを担当しました．この特集では執筆者や編集者に多大なご協力をいただき，改めてこの場で感謝の気持ちをお伝えします．富岳という名称が世間にまだ出ていない時点で，富岳についての詳しい技術情報を含む特集を企画，担当できたことは，自分のことながら意義深かったと感じています．昨今では情報通信技術に関しては，そのインパクトからか，どうしても AI やメディア系の記事が多くなりがちという印象を抱いていました．そのような状況だからこそ，基盤技術であるスパコンひいては高性能計算やシステムソフトウェアの技術についての知識も継続的に整理，共有し続けていくことには大きな価値があると感じ，この特集に至りました．基盤技術は縁の下の力持ちともよく言われ，地味ではありますが，継承，発展させていくことは必要不可欠であり，会誌でそのお手伝いができるようにと奮闘していた気がします．

この 4 年間，会誌の 1 つ 1 つの記事や企画に多くの方々の膨大な労力がかかっていることを絶えず目のあたりにしました．この経験により，これからは記事を造り手側の視点で，より興味深く読めるような気がします．最後に，本会および会誌の発展を心から祈念します．副編集長および編集委員という貴重な機会をいただき，ありがとうございました．

（大山恵弘／筑波大学）

副編集長退任にあたって

稲見昌彦編集長より副編集長にご指名いただき，引き受けてみたものの実際には反省しきり．書き出すと言い訳がましいことばかりになるのですが，とにかく当初は会社での役割も少しずつ軽くなる時期で仕事以外のこともできると意気込んでおりました．しかし，就任直後に会社の受注が倍増し，毎日目まぐるしく，落ち着くどころか結局子会社まで作ることになりました．この歳まで仕事をしていることさえ実はびっくりしています．

編集長退任にあたってをご読みいただければ分かるのですが，稲見編集長は持ち前の発想力とスピード感でどんどん新しい取り組みをなされ，それを追いかけるのが精一杯でした．

逆に私自身の収穫はたくさんありました．2018 年の就任でしたが，2020 年の情報処理学会の 60 周年という節目のさまざまな行事の計画にも参加させてもらえたのもありがたいことでした．と同時にコロナ禍といういままでにない状況の中で，学会のあるべき姿を顧みる時期に遭遇し電子化，オンライン開催がスピード感を持って日々更新されて行くのを目の当たりにできました．

稲見編集長の元，新しいワーキンググループ（次世代分野／NWG）が設立されその主査になり，そのメンバに学生さんである畑田裕二氏（東京大学大学院）が幹事として入ってくれたことは非常に大きかったです．特にコロナ禍になり，全国大会がオンライン開催に変更を余儀なくされたときに編集委員会の担当をスムーズに開催できたのは畑田氏に全面的に頼ってのことと思います．また，同時期に入ってくれた太田智美さんも縦横無尽に動いてくださいました．頭が下がります．当時は学生でなく社会人でしたが，その後後期博士課程の学生となり，そしてこの誌面が発行されているころには先生として活躍されていることと思います．稲見編集長の思惑通りに誌面にとどまらない活動ができたのはいままでの委員会にはない若い人が編集委員に入ったとことが大きかったのだと思います．結局，本来はまとめる立場の私が得ることのほうが多くありました．感謝しかないです．ありがとうございました．

（中田眞城子／ mplusplus（株））

編集委員退任にあたって

同じ職場の前任者からの声掛けがきっかけとなり，4年にわたり，会誌編集委員を務めさせていただきました．この間，本務先の異動による任務の都合もあり，会誌編集委員として会誌作りに十分貢献できませんでしたが，編集委員の皆さんの会誌に対する熱い想いに触れ，多くの学びを得ることができましたので，ここで紹介させていただきます．

特に大きな学びは，編集委員会およびワーキンググループの運営体制です．企画段階から最終チェックにいたるまでの役割分担がしっかりと確立されており，Slackをはじめとするさまざまなツールを活用して，各担当者が主体的に動きます．編集委員会では，毎月寄せられるモニタコメントを精読し，次の企画にフィードバックします．編集委員が交代するタイミングも円滑に引継ぎがなされ，新人の編集委員にとって安心できる環境が構築されています．これらは編集長のリーダシップと会誌編集部門の皆さんの細やかなサポートによるものと思います．また，社会の出来事を敏感に捉えて，情報学と絡めてタイムリーに記事にする企画力も学びとなりました．時事問題は，編集委員会にて話題になることもあり，それらと情報学とのかかわりが議論され，特集記事が組まれることが多くありました．これもひとえに，研究分野を横断して活躍されている方々が，編集委員として編集活動に携わっているからと思います．

私は2019年1月号と2022年3月号に掲載された「ビブリオ・トーク」を執筆させていただきました．書評をした経験がなく，とにかく書籍の選定に悩みました．過去の記事を読み返したところ，話題の書籍，初学者向けの導入となる書籍，専門分野の基礎となる書籍，実応用・ビジネスにかかわる書籍など多岐にわたっており，この「ビブリオ・トーク」は未知の分野に出会う有益なコーナーであることを再認識しました．同時に，私の専門分野が情報処理におけるほんの一分野にすぎないことも分かり，より多くの読者に知ってもらうよう，音声・音響・音楽にかかわる書籍を紹介することにしました．ただ，この2つの記事の寄稿にとどまってしまい，会誌編集委員としての職責を十分に果たさないまま退任することをお詫びいたします．それでも，多くの研究分野を対象として，読者に情報処理の魅力を伝えるための会誌編集に携わる，貴重な機会をいただいたことに感謝します．この貴重な経験を活かし，引き続き研究会の運営にもかかわりながら，情報処理の発展に貢献していきます．

（大石康智／NTTコミュニケーション科学基礎研究所）

編集委員退任にあたって

会誌『情報処理』でSWG（システム分野ワーキンググループ）の編集委員を4年間務めさせていただきました．任期中にお世話になりました方々には，この場をお借りして感謝申し上げます．

編集委員を引き受ける動機は，会誌ってどういうプロセスや仕組みで作られているんだろう？という興味本位なものでした．情報処理学会が扱う“情報”は，多種多様な技術で構成される，非常にすそ野の広い科学技術分野です．しかも，ドッグイヤーと言われるくらい技術進歩が速く，すべての分野の最先端技術を個人で追いかけることは難しいと常々感じています．会誌「情報処理」は，技術的・社会的に注目を集めているテーマを，一線で活躍している研究者や技術者がさまざまな角度から紹介してくれる特集記事が毎号載っているので，出版までの流れに興味を持っていました．編集委員に入ってみると，その大変さに驚きました．特集記事は，まずワーキンググループで議論しながら企画案を作るところから始まります．企画は，新しい技術を紹介するという観点以外にも，社会的な意義や速報性，企画テーマに造詣の深い方や記事を執筆していただける方を探すなどのプロセスを経て，企画書案を作成することになります．その企画書案を本会議という委員会で紹介して承諾が得られれば，ようやく企画としてスタートすることになります．その後は，著者に原稿執筆を依頼し，原稿チェックが済めば完成というのが大まかな流れになります．企画書案を作ってから数カ月かかる仕事です．この出版までのプロセスをほかのワーキンググループと並行して進められていて，特集記事が毎号会誌に載ることになります．

特集記事を支える編集委員は，大学，研究機関，企業の研究者などの所属組織と種類，専門分野が異なる人々で構成されています．SWGでの活動を通して，普段の研究活動でかかわることのあまりない分野の方々と接する機会があったことは，編集委員をしていてよかったと思ったことの1つでした．今，この分野では世界的にこういう動きになっているとか，この技術はこのような応用事例があるなどの，さまざまな興味深い話をすることができ，本業にも活かせる良い刺激を受けました．

1人1台スマートフォンを所持している時代になり，生活における情報技術の利用シーンはますます重要性を増してきます．私の編集委員の任期中は，情報を取り巻く環境に多くの変化がありました．AIや自動運転，ブロックチェーンやフィンテック，5G通信の社会実装の本格化，SDGsという持続可能な社会に向けた技術開発の重要性，COVID-19による社会の大きな変化などです．会誌『情報処理』は，読者の情報技術活用に対するリテラシー向上に大きく貢献できる雑誌です．今後も，質の高い情報発信をされることを確信しておりますので，今後は読者として発刊を楽しみにしております．

最初は興味本位からの参加でしたが，4年間の活動を通じて多くのことを学ばせていただきました．改めまして，お世話になった皆様，本当にありがとうございました．

（大島浩太／東京海洋大学）

編集委員退任にあたって

2018年から4年間，主に「5分で分かる！？有名論文ナナメ読み」，通称「ナナメ読み」のコーナーを担当し，濃い時間を過ごしました．無知なもので，就任するまで，会誌の編集委員はみなボランティアだということを知らずにおりました．てっきりアルバイト代が出るのかと思っていた浅はかな私です．任期の途中からは，月イチの編集委員会でのお弁当も廃止になって，名実ともにボランティアとなりました（笑）．

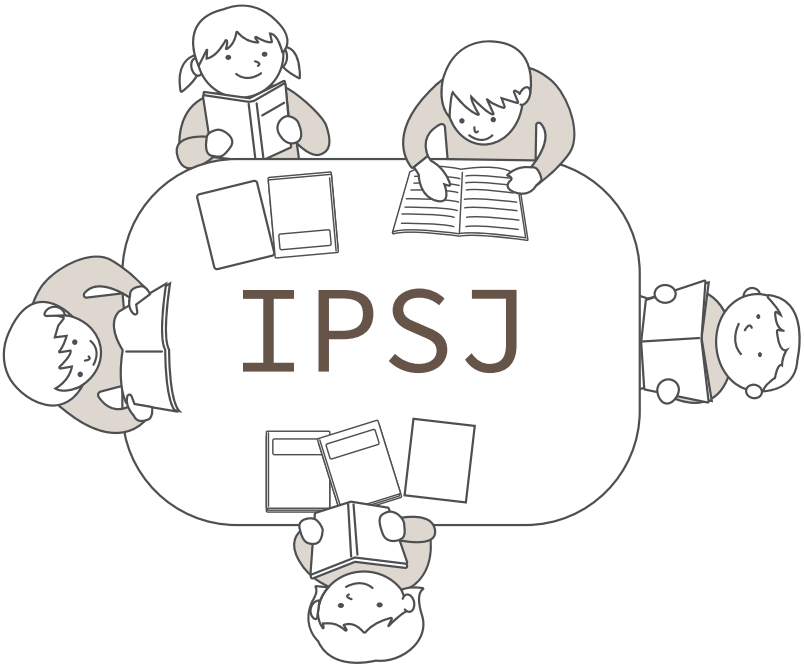
「ナナメ読み」の編集作業は，毎号のネタ（分野）決め，執筆者探し，閲読，があります．執筆者探しはなかなかに大変な作業で，それでもこれまでに50名くらいの方に書いていただいたようです．ほかの委員からのご推薦もありますが，8割くらいは自らリサーチした方に書いていただけました．知己のある方に加え，TwitterやIPSJ-ONEなどで面白い記事になりそうな方を探し，ファンレターを書くように執筆依頼をお送りしました（IPSJ-ONEはそういった意味で，私にとっては二重にナイスな企画です）．

作業で最も楽しいのは，上がってきた原稿を拝読するときです．ファンレターの返信をもらうようなものですし，知らない分野を学ぶ良い機会でもありました．1番驚いたのは，甘利俊一先生に書いていただいたときでしょうか．毎回，著者ご自身が採り上げる論文を選ぶのですが，ご本人にご意向を伺うと，前年にarXivに出たNeural Tangent Kernelの論文を解説されたいというのです．80歳を超えてなおバリバリの現役なのだ！と驚き，上がってきた原稿を拝読した際は，励まされるような気持ちになりました．ほかにも，手書きのイラストつきの原稿，Markdownで書かれた原稿，ネットスラング満載の原稿など，個性豊かな原稿にふれるたび，編集者ならではの楽しみを味わいました．

編集委員を通じて，原稿の内容以外に勉強になったことを3つ挙げてみます．1つ目は，執筆者の方々の筆の早さ，〆切の正確さです．編集者ですので，依頼をしてから原稿が上がってくるまでの長さを体感するわけですが，依頼して2週間で完成度の高い原稿が上がってきたときは，「すごいんですけど！」と叫びたい気持ちになりました．2つ目は，一般読者向けの記事を書くには，論文を書くのとは違う執筆の技術が必要であるということです．専門家と初学者の両者を満足させるのはなかなか難問で，一方で，ある程度は著者（と編集者？）の腕次第ということを体感しました．3つ目は，ほかの編集委員の方々の耳の早さ，お顔の広さです．さすが編集委員をされる方々，企画が面白く，委員会での雑談は勉強になりました．ビブリオトークの本も何冊か買いました．

任期中の思い出はそれ以外にもいろいろとあり，学会参加報告の執筆者探しのお手伝いをしたり，自分の首里城プロジェクトを緊急記事でご紹介いただいたりしました．私は特集などを企画せずに任期を終えてしまったことと，後半はコロナでほとんど懇親できなかったことが心残りですが，経験としては，この4年間でお金を払っても得られない価値のあるものをいただきました．これからはもっと真剣に会誌を読むと思います（笑）．2016年に第2子を出産し，生活に追われる中で編集委員をやってきて，どちらかというと今は全うできてホッとしているという気持ちです．編集委員の皆様，事務局の皆様，著者の皆様，いろいろと至らなかったとは思いますが，一緒に編集作業に携わってくださり，楽しかったです．誠にありがとうございました．

（川上　玲／東京工業大学）



編集委員退任にあたって

私が編集委員に就任したのは 2018 年で，稲見編集長，江渡委員，福地委員，太田委員らと同じ時期の就任となりました．前者の 3 名は，ニコニコ学会 β の運営として以前からよくかかわっていた方々で，当時を思い出す懐かしさもありました．編集委員会では特に決められた担当があるわけではなかったのですが，主に稲見編集長と江渡委員の無茶振りを太田委員らと一緒に拾うという役割でした．

編集委員会において一番貢献できたと思うことが，技術書典への出展です．編集委員になってから改めて気付かされたのですが，会誌は非常に多くの方々の時間と労力がかけられてつくられており，とても面白い記事がたくさんあります．しかし会誌が届くのは情報処理学会会員のみで，読者が限られており，非常にもったいないと感じていました．もっと多くの人に記事を届ける方法を考えていたときに思い浮かんだのが，技術書典の盛り上がりです．技術書典は，技術系同人誌の即売会であり，技術書愛好者のお祭りのようなものです．情報処理学会会誌は情報科学に関する幅広い記事が掲載されており，技術書典の来場者に興味を持ってもらえそうな内容です．普段アカデミアとは縁遠いと感じている方々にも記事を届けられるのではないかと思い，技術書典への出展を企画しました．会誌は教員や研究者が本職である方々が集まってつくっており，ある意味で同人誌のようなものと思いますし，同じことを稲見編集長も言っていました．初出展の技術書典 7 以降は今日まで毎回出展し，多くの方に記事を届けることができました．

さて，ここで，会誌をとりまく変化について考えてみたいと思います．情報処理学会会誌の初号が発刊されたのは 1960 年です．当然インターネットが普及する前であり，紙媒体が情報伝達の大きな役割を担っていた時代です．一方，インターネットが普及した現在，ニュースなどの情報収集には Web の記事を閲覧することが主流となりました．情報誌やファッション誌などの雑誌を読む場合も，スマホやタブレットのアプリで読むことが増えたと思います．最近では，テキスト情報に加えて，YouTube 等の動画も主要な情報収集先となってきました．Podcast やオーディオブックなどの音声コンテンツもあります．そのような現代では，出版不況が叫ばれ，紙の雑誌を読む機会は昔と比べてものすごく減ったことかと思います．みなさんは紙の雑誌を何冊購読していますか？　職場や大学や研究室で定期購読している雑誌はまだそれなりにありそうですが，個人で購読して毎号読んでるものは結構少ないのではないでしょうか．私も，個人で定期購読している紙の雑誌は，『フットボリスタ』というサッカー雑誌のみです．

このような時代において，会誌が担うべき役割とは一体何なのでしょうか？　世界に目を向けると，情報科学の分野で最大級である ACM と IEEE という 2 つの学会があります．それぞれ，紙の会誌のほかに ACM TechNews と IEEE Spectrum という Web メディアを有しており，時代のニーズに合った情報発信を行っています．情報処理学会でも同じことができるとよいかもしれませんが，ACM や IEEE とは会員数も予算規模も大きく異なり，現実問題として Web メディアの運用をすぐに実施するのは難しそうです．しかし，予算がなくともできることもいくつかあり，少しずつ進められています．紙冊子の配布を選択性にしたり，紙冊子の記事の一部は QR コードを用いた PDF へ誘導に変更したりしています．一部の記事は note にも掲載されるようになりました．このように少しずつ Web の活用が進められています．

このような変化は，以前からの会員にとってはむしろ使いにくいものになったと感じられているかもしれません．しかし，今は完全な紙媒体から Web へ移行するちょうど過渡期にあたり，長い目で見たときには必要な変化だと考えられます．先述の通り情報伝達の在り方は大きく変化してきましたし，この先もデバイスの進化とともにさらに大きく変わっていくのではないかと思います．その変化を受けて，これからもこの先も，会誌も時代の変化に追従して会誌の役割とその実現方法を変えていく必要があるでしょう．そのような会誌の変化の時代の一端を担うことができたのは光栄ですし，この先も変わっていく会誌を見届けていくことも楽しみです．

在任中にはさまざまな経験をさせていただきました．上述した技術書典のほか，cluster で開催された情報処理学会 全国大会の企画セッションにて司会を行ったり，本来業務である編集作業も行いました．IT 紀行では何度もマンガに描いていただいたり，編集委員としての活動に対して学会活動貢献賞もいただきました．ほかの編集委員や学会事務局の方々のおかげで，楽しく活動できた 4 年間だったと思います．本当にありがとうございました．

（湯村　翼／北海道情報大学）

編集委員退任にあたって

2018 年より 4 年に渡り会員サービス分野（MWG）の編集委員を務めさせていただきました．その前は，2016 年まで論文誌ジャーナル／ JIP 編集委員を務めさせていただいており，その活動について前任者と情報交換していたことが，会誌編集委員に着任させていただくきっかけでした．

着任当初は会員サービス分野というグループ名からは，どのような記事を編集するのかを想像できず，しっかり務められるか少し不安に思っていたように思います．しかし，ありがたいことに新任者に対する配慮として，最初の半年は副担当として作業を割り当てていただくことで，スムーズに仕事を覚えることができたと記憶しています．その際に主担当をしていただいた方々も 1 年目の私を丁寧に導いていただいたことを覚えております．MWG の担当作業の 1 つであるモニタコメントの閲読については，多様なコメントを読ませていただく機会にもなり，多くの視点を自分自身に取り入れることもできたように思います．また，モニタコメントにおいてジュニア会員の方々がどんな感想を持つのかも非常に興味のあることでした．ここで取り入れた視点を自分の子供の教育や，機会があれば若い人に教える際にも活かせることができればと期待しています．

そして，コロナ禍に入った 3 年目・4 年目に，MWG の幹事・主査を務めさせていただきました．このころには本会議は毎回オンラインとなっていました．本会議では，MWG 主査として進捗を報告させていただく機会がありましたが，最後までオンライン会議でしたので，本来だったらどのような感覚で会議に参加していたのであろうと考えます．また，主査を務めさせていただくにあたり，たくさんの方々にお願いをさせていただきました．会議レポートの執筆を依頼させていただいた方々，MWG の編集委員の方々，どなたも快く引き受けてくださりました．MWG の編集委員の方々には，厳しいスケジュールで作業をお願いすることもありましたが，お忙しいにもかかわらず，素早く丁寧にご対応いただけました．また，事務局の方々には，作業計画や進捗などについて何度も相談させていただきましたが，そのたびに親切に応じていただけました．このように本当に人に恵まれた環境で MWG 主査を務めさせていただくことができました．関係者皆様に本当に感謝しております．

また，MWG 主査を担当させていただいたきっかけで，ビブリオ・トークの寄稿もさせていただきました．執筆の依頼や，執筆いただいた文書の閲読だけでなく，自分で原稿を執筆する経験もさせていただき，執筆側・編集側の両面から会誌に携わらせていただく貴重な経験をさせていただけたと思います．

4 年間の編集委員を通して，編集委員の皆様，執筆者の皆様，事務局の皆様にかかわらせていただいたこと，編集作業および執筆作業をさせていただいたことは非常に大きな経験となりました．これらの経験を今後の研究業務に活かしつつ，今後も『情報処理』の発展と関係者皆様のご活躍を応援させていただきたいと思います．

（伊藤将志／（株）東芝 研究開発センター）

IPSJ MAGAZINE Vol.63 No.4 (Apr. 2022)

CONTENTS

読後のご意見をお送りください

本誌では，現在約 200 名の方々に毎号のモニタをお願いしておりますが，より多くの読者の皆さんからのご意見，ご提案をおうかがいし，誌面の充実に役立てていきたいと考えておりますので，以下 Web ページから奮って事務局までお寄せください．

「情報処理」アンケートページ　**https://www.ipsj.or.jp/magazine/enquete.html**

一般社団法人 情報処理学会　会誌編集部門　E-mail: editj@ipsj.or.jp

じゃんけんをプログラミングするよ

情報処理学会・学会誌「情報処理」
2022年1月7日 15:27

井手広康（愛知県立小牧高等学校）

情報Iが大学入学共通テストに出題されることが決まり，入試対策をどうしようと悩み転がっている今日このごろ．来年度には各教科書会社から問題集が出されるはず（希望的観測）ですが，何か参考になる問題はないだろうか？

そんなあなたにおすすめするのが，大学入試センターの「情報関係基礎」．現在，情報処理学会の情報入試委員会「情報関係基礎アーカイブ」［1］では，1997年からの過去問が公開されています．

ただ，「おすすめの問題を教えてほしい」という毎日忙しくしているあなたのために，放送大学の辰己丈夫先生が厳選した「情報関係基礎」の良問を下に紹介します．

※クリックすると「情報関係基礎アーカイブ」のPDFにとびますよ．

・2003年度　第2問　文字列の部分一致

・2005年度　第2問　じゃんけん大会

・2005年度　第4問　デジタルカメラの操作インタフェイスの改善

・2007年度　第2問　イベントを中止するかどうかのルールセット

・2012年度　第1問　送田さんと受田さんのエラー訂正

・2013年度　第2問　旅行代理店の業務改善

・2013年度　第3問　24時間営業の飲食店

・2020年度　第1問　情報の符号化とデータ量

上の問題のうち，本稿では「2005年度　第2問　じゃんけん大会」を紹介します．いま，「なんだ，ただのじゃんけんかよ」と思われた人は，ぜひ問題に挑戦して，心を折られてみてください．

▼ 目次

問題の冒頭部分だよ

まず，問題の冒頭部分です．

> じゃんけんは，グー，チョキ，パーの 3 種類の手のいずれかを同時に出して勝敗を決めるゲームである。グーはチョキに勝ちパーに負け，チョキはパーに勝ちグーに負け，パーはグーに勝ちチョキに負ける。
>
> 出された手が 2 種類のときは勝ち負けが決まる。全員の手が同じか，または 3 種類の手がすべて出ると，勝ち負けが決まらずあいことなる。
>
> 以下では，グーを 1，チョキを 2，パーを 3 で表す。

もしかしたら，どこかの国のじゃんけんみたいに5種類も手が出てきたり，条件を満たせばグーはパーに勝つみたいなウルトラCのルールがあるのかと思いきや，どうやら普通のじゃんけんのよう……．

大事なことは，グー，チョキ，パーの順に，1，2，3と表すということだけですね．

問1　勝つ手と負ける手を決めるよ

問1の問題です．文章を読むと，グー，チョキ，パーに勝つ手と負ける手を，そ

れぞれKati[x]とMake[x]の配列に入れていることが分かります.

x＝1，2，3 に対して，

x に勝つ手が Kati[x]

x に負ける手が Make[x]

となるように，配列 Kati，Make を定める。例えば，グーに勝つ手はパーであるから，Kati[1] ＝ 3 となる。したがって，配列 Kati，Make の値は

Kati[1] ＝ 3，　Kati[2] ＝ ア，　Kati[3] ＝ イ

Make[1] ＝ ウ，　Make[2] ＝ エ，　Make[3] ＝ オ

となる。

表にすると，次のようになります．これは簡単ですね.

	グー(1)	チョキ(2)	パー(3)
勝ち	Kati[1] = 3	Kati[2] = 1	Kati[3] = 2
負け	Make[1] = 2	Make[2] = 3	Make[3] = 1

「ア」の答え：1

「イ」の答え：2

「ウ」の答え：2

「エ」の答え：3

「オ」の答え：1

問2　勝った回数をカウントするよ

　問2の問題です．プログラムを見ると，繰り返しと条件分岐を使って，Aが勝った回数を，変数kaisuを使ってカウントしていることが分かります．

A，Bの二人がじゃんけんを10回行うとき，Aが勝った回数を数える手順を図1に示す。図1で用いる変数の意味を表1に示す。

```
(01)  kaisu ← 0
(02)  i を 1 から 10 まで増やしながら,
(03)  |  もし A[i] = [ カ ] ならば,
(04)  |  |  kaisu ← kaisu + 1
(05)  |  を実行する
(06)  を繰り返す
```

図1　Aが勝った回数を数える手順

表1　変数の意味(1)

変　数	意　　味
A[i]	Aのi番目の手
B[i]	Bのi番目の手
kaisu	Aが勝った回数

問題となるのは条件分岐の部分で，A[i] =「カ」となっています.

「はて？A[i]って何だっけ？」と思いますが，表1を見ると，どうやら「Aのi番目の手」が入っているようです．iは繰り返しによって1から10まで増えていくので，A[i]とB[i]の配列には，AとBの10個の手が入っていることが分かります.

さて，(03)〜(05)行目の条件分岐の中身を見ると，A[i] =「カ」を満たすとき

に，kaisuの値を1増やしています．表1にkaisuは「Aが勝った回数」とあるので，この条件は「Aが勝った場合」ということが分かりますね．

ここで，「カ」に何が入れば，Aが勝ったことになるのかを考えなければいけません．

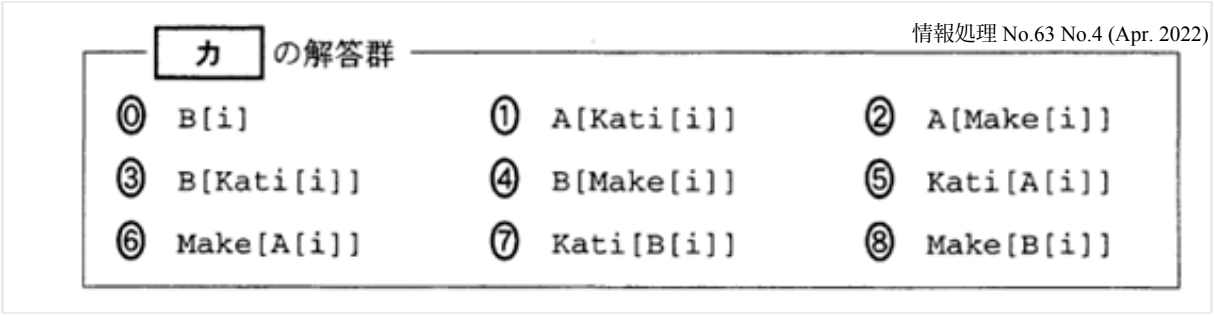
じゃんけんの結果の判定には色々なパターンが考えられますが，ここでは，問1で考えたものを使用しましょう．

たとえば，kati[1] = 3は「グー(1)に勝つのはパー(3)」という意味でした．これを踏まえて，A[i] =「カ」を考えましょう．

左辺はA[i]（Aの手）となっているので，右辺のどこかにはB[i]（Bの手）が入らなければいけません．ただし，そのままA[i] = B[i]とすれば，条件は「あいこ」になってしまうことが分かります．

B[i]はBの手を表しているので，右辺にはKati[B[i]]かMake[B[i]]が入りそうです．ここではB[i]に勝つ手がA[i]であればいいため，A[i] = Kati[B[i]]になることが分かります．

次は「カ」の解答群です．よって，「カ」は⑦のKati[B[i]]になります．



「カ」の答え：⑦ Kati[B[i]]

問3　10人でじゃんけんするよ

問3の問題の前半部分です．10人がじゃんけんを行い，1番目の人だけの勝敗を判定すればいいらしいです．

「え？　そんなのほとんどあいこじゃん？」と湧き出る疑念は振り払い，とりあえずプログラムを見ていきましょう．

1番から10番までの番号をつけた10人がじゃんけんを行うとき，1番の人の勝敗を判定する手順を図2に示す。図2で用いる変数の意味を表2に示す。

```
(01)  Ninzu[1] ～ Ninzu[3] を 0 に初期化する
(02)  i を 1 から 10 まで増やしながら,
(03)  |   Ninzu[Te[i]] ← Ninzu[Te[i]] + 1
(04)  を繰り返す
(05)  a ← Te[1]
(06)  b ← Kati[a], c ← Make[a]
(07)  もし [ キ ] かつ [ ク ] ならば,
(08)  |   「1 番の人は勝ち」と表示する
(09)  を実行し，そうでなければ,
(10)  |   もし [ ケ ] かつ [ コ ] ならば,
(11)  |   |   「1 番の人は負け」と表示する
(12)  |   を実行し，そうでなければ,
(13)  |   |   「あいこ」と表示する
(14)  |   を実行する
(15)  を実行する
```

図2　1番の人の勝敗を判定する手順

次の表2から，Ninzu[x]には「手xを出した人数」が入ることが分かります.

たとえば，10人のうち，グーを出した人が3人であれば，Ninzu[1]には3が入るという感じです.

プログラムの(01)行目で，グーを出した人数の配列Ninzu[1]，チョキを出した人

数の配列Ninzu[2]，パーを出した人数の配列Ninzu[3]にそれぞれ0を入れて初期化しています．

表2　変数の意味(2)

変　数	意　　味
Te[i]	i番の人の手
Ninzu[x]	手xを出した人数(例えばNinzu[1]はグーを出した人数)

次に，(01)～(04)行目で，iを1ずつ増やしながら，Ninzu[x]の操作を行っています．ここで表2から，Te[i]は，「i番目の人の手」が入ることが分かります．(01)～(04)行目では，10人の手のうち，グーの数をNinzu[1]に，チョキの数をNinzu[2]に，パーの数をNinzu[3]にカウントしているわけです．

次に，(05)行目では，1番目の人の手を変数aに代入しています．また，(06)行目では，1番目の人の手に「勝つ手」をbに，「負ける手」をcにそれぞれ代入しています．

次に，(07)～(15)行目において，条件分岐で1番目の人の「勝ち」「負け」「あいこ」の判定を行っていることが分かります．ここで，1番目の人が勝つ条件を考えてみましょう．

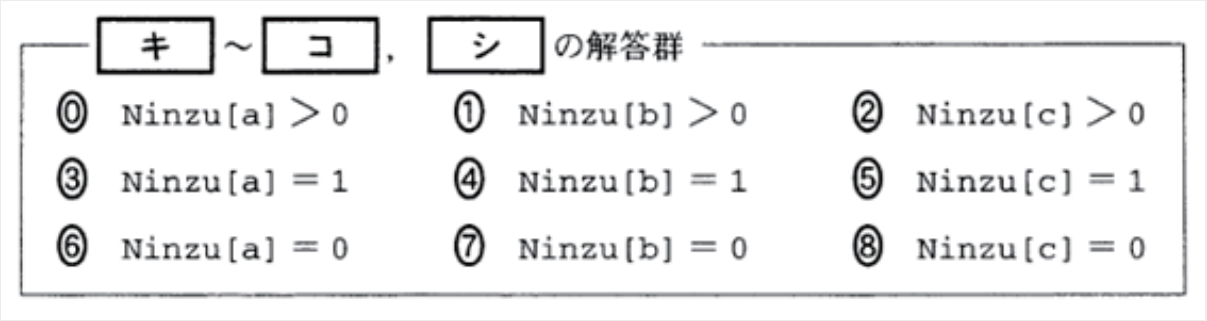
たとえば，1番目の人がグーを出した場合，2～10番目の人は，1人以上がチョキ

を出し，かつ，パーを出した人が1人もいない状態でなければいけません（パーが1人でもいた場合，「負け」か「あいこ」になる）．

つまり，次の2つの条件を同時に満たしている必要があります．

> 条件I：1番目の手に負ける手を出した人が1人以上いる
>
> 条件II：1番目の手に勝つ手を出した人数が0である

ここで，問題となっている「キ」と「ク」の解答群は次の通りです．



条件Iは，言い換えるとNinzu[c] >= 1になります（cは1番目の人の手に負ける手）．ただ，上の解答群にこの表記はありませんが，②のNinzu[c] > 0がこれと同じ意味になるので，「キ」は②が正解であることが分かります．

一方で，条件IIは，言い換えるとNinzu[b] = 0となり（bは1番目の人の手に勝つ手），「ク」は⑦が正解であることが分かります．

「キ」の答え：② Ninzu[c] > 0

「ク」の答え：⑦ Ninzu[b] = 0

※「キ」と「ク」は順不同

最後に「ケ」と「コ」で，これはAが負けになる条件です．ここで，1番目の人が負ける条件を考えてみましょう．

たとえば，1番目の人がグーを出した場合，2〜10番目の人は，1人以上がパーを出し，かつ，チョキを出した人が1人もいない状態でなければいけません（チョキが1人でもいた場合，「勝ち」か「あいこ」になる）．

つまり，次の2つの条件を同時に満たしている必要があります．

条件III：1番目の手に勝つ手を出した人が1人以上いる

条件IV：1番目の手に負けるを出した人数が0である

条件IIIは，言い換えるとNinzu[b] >= 1になります（bは1番目の人の手に勝つ手）．ただ，上の解答群にこの表記はありませんが，①のNinzu[b] > 0がこれと同じ意味になるので，「ケ」は①が正解であることが分かります．

一方で，条件IVは，言い換えるとNinzu[c] = 0となり（cは1番目の人の手に負け

る手），「コ」は⑧が正解であることが分かります.

「ケ」の答え：① Ninzu[b] > 0

「コ」の答え：⑧ Ninzu[c] = 0

※「ケ」と「コ」は順不同

問3は，次の後半部分に続きます.

Te の内容が表 3 のとおりとすると，図 2 の手順が終了したとき，
Ninzu[b] の値は［ サ ］となる。

表 3　Te の内容

i	1	2	3	4	5	6	7	8	9	10
Te[i]	2	1	2	1	2	3	1	1	3	3

1 番の人が勝った場合に，他の勝者がいないことを判定するには図 3 の手順を図 2 の行(08)と行(09)の間に挿入すればよい。

```
(08.1)  もし［ シ ］ならば，
(08.2)      「他に勝者はいない」と表示する
(08.3)  を実行する
```

図 3　1 番の人以外に勝者がいないことを判定する手順

まず，表3のTe[i]にある10人の手を出したときのNinzu[b]，つまり1番目の人の手（表3ではTe[1]が2なのでチョキ）に勝つ手（グー）の数を求めます．
グーは1なので，Te[i]が1となるi = 2, 4, 7, 8がこれに該当します．そのため，「サ」は4となります．

「サ」の答え：4

次に，1番の人が勝った場合に，他の勝者がいないときの条件を求めます．この場合は，次の条件を満たしている必要があります．

条件V：1番目以外の全員が1番目の手に負ける手を出している

ただ，「シ」の選択肢を見ても，条件Vに該当しそうなものはありません．

そこで，(07)行目に注目します．

図3の(08.1)〜(08.3)行目は(08)行目の直後に挿入されるため，(07)行目の条件である次を満たしていることになります．

条件I：1番目の手に負ける手を出した人が1人以上いる

条件II：1番目の手に勝つ手を出した人数が0である

条件IIより，1番目の人に勝つ手を出した人が0人であることが分かっています．そのため，残りは1番目の人に負ける手か，1番目の人と同じ手ということになります．

ここで，1番の人だけが勝つためには，1番目の人と同じ手を出した人が自分しか

ない状態でなければいけません．つまり，これはNinzu[a] = 1を表し，解答群から「シ」には③が該当することが分かります．

「シ」の答え：③ Ninzu[a] = 1

問4　10人でじゃんけん大会するよ

　問4の問題です．10人のうち3回勝つ人が現れるまでじゃんけんを繰り返すらしいです．

　「え？　それ結構な時間かかるよね？」と湧き出る疑念は振り払い，とりあえずプログラムを見ていきましょう．

1番から10番までの番号をつけた10人で，3回勝つ人が現れるまでじゃんけんを続け，3勝した人の番号をすべて求める手順を図4に示す。ここで，変数Kekka[i]は，i番の人の勝った回数を表す。

```
(01)  Kekka[1] ～ Kekka[10] とx，yを0に初期化する
(02)  [ス] の間，
(03)      1～10番目の人の手をTe[1] ～ Te[10] に入力する
(04)      Ninzu[1] ～ Ninzu[3] を0に初期化する
(05)      x←x＋1
(06)      iを1から10まで増やしながら，
(07)          Ninzu[Te[i]]←Ninzu[Te[i]]＋1
(08)      を繰り返す
(09)      jを1から10まで増やしながら，
(10)          a←[セ]
(11)          b←Kati[a]，c←Make[a]
(12)          もし[キ]かつ[ク]ならば，
(13)              Kekka[j]←Kekka[j]＋1
(14)          を実行する
(15)          もし[ソ]＝3ならば，
(16)              y←y＋1
(17)              jの値を表示する
(18)          を実行する
(19)      を実行する
(20)  を繰り返す
(21)  x，yの値を表示する
```

図4　3勝した人の番号を求める手順（[キ]・[ク]は40ページ図2と同じ）

問題文から，変数Kekka[i]には，i番目の人の勝った回数が入ることが分かります．ただ，この問題文からは，xとyが何を表しているのかは分かりません（最後に問われます）．

(03)～(04)行目はこれまでと同じですね．

(05)行目で何やらxを1増やしています．繰り返した回数のカウントでしょうか？

(06)～(08)行目も問3と同じで，10人の手をグー，チョキ，パーのいずれかでカウントしています．

問題は(09)～(19)行目です．jを1ずつ増やしながら繰り返しています．

ここで，(10)～(11)行目が図2の(05)～(06)行目と似ており，違いは(05)行目が「a ← Te[1]」となっていることが分かります．

問3の問題では判定の対象が1番目の人に限定していましたが，この問題では3回勝つのは10人のうち誰でも構いません．そのため，すべての人に対して勝敗をチェックする必要があります．

ちょうど上の(09)行目でjを1ずつ増やしているので，「セ」には次の解答群から「① Te[j]」が入るのではないか，という予想ができます．いったん保留にしておきましょう．

セ ・ ソ の解答群

⓪ Te[Kekka[j]]	① Te[j]	② Kati[a]
③ Make[a]	④ Kati[Kekka[j]]	⑤ Make[Kekka[j]]
⑥ Kekka[b]	⑦ Kekka[c]	⑧ Kekka[j]

プログラムの続きを見ていきましょう.

(12)〜(14)行目で，(12)行目はじゃんけんで勝つ条件でした.

じゃんけんで勝った場合，(13)行目でKekka[j]を1増やしていることが分かります．ここで，やはり変数jは人の番号を表していることが分かり，先の「セ」にはTe[j]が入ることがほぼ確定できました.

次に(15)〜(18)行目です．もし「ソ」が3に等しければ，yを1増やしてjの値を表示しています.

プログラムは(21)行目を残してここで終わりになるので，何かしらの終了条件が(15)〜(18)行目には入りそうです．このじゃんけん大会は，3回勝った人が現れたらプログラムを終了しますので，「ソ」には「勝った回数」が入るのではないかという予想がつきます.

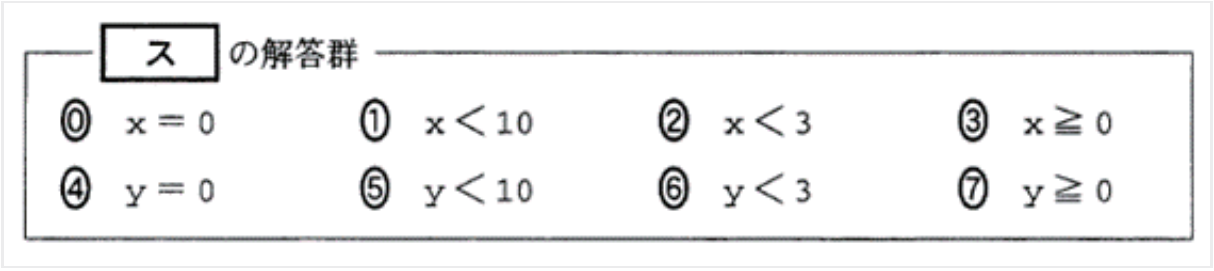
また，勝った回数はKekka[i]に記録されており，この(15)〜(18)行目は(09)〜(19)行目の繰り返しの中に含まれているので，「ソ」には上の解答群から「⑧ Kekka[j]」が入るのではないかと予想できます.

その場合，(17)行目では，3回勝った人の番号jを表示していることになり，プロ

グラム的にも合点がいきます.

最後に「ス」で，ここには繰り返しの条件が入ります．3回勝った人が現れたらプログラムを終了するので，言い換えれば，「3回勝つ人が現れるまで」プログラムを繰り返します.

ここで，(15)〜(18)行目において，3回勝った人がいた場合，変数yを1増やしていました．つまり，「yが0の間」繰り返せばよいため，「ス」には次の解答群の「④ y = 0」が当てはまることが分かります.



なお，yを1増やす作業は(09)〜(19)行目の繰り返しの中にあるので，同じ回で3勝目をあげる人が複数同時に出てきても，yはその人数をしっかりカウントすることができますね.

「ス」の答え：④ y = 0

「セ」の答え：① Te[j]

「ソ」の答え：⑧ Kekka[j]

問4はもう少し続きます.

> 行(21)で表示される変数x，yの値はそれぞれ［タ］，［チ］となる。

最後の(21)行目で表示される変数xとyの値を求める問題です．次が「タ」と「チ」の解答群になります.

［タ］・［チ］の解答群

⓪ じゃんけんに参加した人数
① じゃんけんの総回数
② あいこになった総回数
③ 最後のじゃんけんに勝った人数
④ 最後のじゃんけんに負けた人数
⑤ 3勝した人数
⑥ 3敗した人数

まず，「タ」はxの値です．xの値に変化があるのは(05)行目だけになります．そのため，繰り返した回数（じゃんけんの回数）をカウントしており，解答群から①が正解であることが分かります.

一方，「チ」はyの値です．「ソ」の解答から，yは3勝した人数を表していることが分かっています．そのため，解答群から⑤が正解であることが分かります．

「タ」の答え：① じゃんけんの総回数

「チ」の答え：⑤ 3勝した人数

じゃんけん大会お疲れ様でした

いかがでしたでしょうか？　たかが「じゃんけん」と言えど侮るなかれ．よく知っていることでも，プログラムにするとなんだか難しく感じますね．

参考文献

1) 情報処理学会 情報入試委員会：情報関係基礎 アーカイブ
https://sites.google.com/a.ipsj.or.jp/ipsjjn/resources/JHK

（2021年11月23日受付）
（2022年2月8日note公開）

■井手広康（正会員）

愛知県立小牧高等学校情報科教諭．愛知県立大学大学院情報科学研究科博士後期課程修了，博士（情報科学）．本会コンピュータと教育研究会運営委員，日本産業技術教育学会理事，日本情報科教育学会評議員など．

情報処理学会ジュニア会員へのお誘い

小中高校生，高専生本科～専攻科1年，大学学部１～3年生の皆さんは，情報処理学会に**無料で入会**できます．**会員になると有料記事の閲覧，情報処理を学べるさまざまなイベントにお得に参加できる等のメリットがあります**．ぜひ，入会をご検討ください．入会は**こちら**から！

今月の会員の広場では，1月号へのご意見・ご感想を紹介いたします．

巻頭コラム「オンラインで祈る」

■まったく無関係と思えるような分野ですら，IT人材が活躍できることが分かった．（上田晴康）
■「目的」と「手段」の実例として価値のある内容と存じます．若者を問わず，ITは手段であることを認識いただけると幸いです．（伊藤治夫）
■祈るという行為は直接その場に行かなければいけない，という気がしていたが時代や状況の変化にも柔軟に対応していてすごいと思った．宗教が少しだけ身近になったような気がする．（匿名希望）
■「宗教とITは水と油ではない」というのは意外でした．すぐにYouTubeを見に行ってしまいました．（山本一公）
■人間同士のかかわりを大切にするというところで宗教と情報通信技術は相性がいいのかもしれないと思った．（匿名希望 / ジュニア会員）
■宗教とITが相性が良い，というのはなるほどと思いました．困ったときに相談できる窓口として今後も拡大していく可能性を感じました．ぜひ，次回は本誌での記事を読みたいです．（小西敏雄）
■なぜオープンソース活動に熱中されたのか知りたかった．（匿名希望）

特集「自動運転元年」

「0．編集にあたって」
■近い将来必要となる技術に関してよく整理してまとめている．（匿名希望）
■これからの未来を作っていくことに情報がいかに役に立っているか分かりやすく，多くの人に読んでもらいたい．（匿名希望）
■過疎地域や高齢者向けの自動運転バスなど必要に迫られたところから実用化されていくだろう．（広野淳之）
■トピックごとだったので，読みやすかった．（匿名希望）
■産業界に直結する特集で，全体を興味深く読むことができました．（匿名希望）
■海外との比較の記事も入れてもらえたらよかったと思います．（祖父江真一）
■用語の解説をしてほしかった．（匿名希望）
■画像処理系の自動運転技術紹介が入っていなかったのはなぜでしょう？　認知系の技術としては必要なものだと思いますが……．（山本一公）
■「群れ」としての自動運転自動車がどう振る舞うべきかという話も聞きたかったです．（岡本克也）
「1．自動運転の現在とこれからの10年」
■「自動運転と人間の最も大きな違いは，ルールを逸脱した行動に対する振舞いであるといえる」という指摘が興味深く思いました．（匿名希望）
■これまで考えたこともなかった色々な自動運転の可能性（期待と不安）を考えることができた．（匿名希望）
■技術中心の解説では抜け落ちそうな点が丁寧に解説されており，大変良い記事と思った．（匿名希望）
■情報処理によって自動化されるものが，元来人間が操作する機械であったという点を問題提起している．自動運転に対する本質を突いた視点で大変考えさせられる．（佐藤章博）
■自動運転において，ルールを逸脱した行動への対処は，現在どこまで実装できているのか知りたかった．（鈴木広人）
「2．高精度3次元地図」
■地図整備のリードタイム短縮に向けた取り組みが興味深い．（匿名希望）
■高精度3次元地図を理解する上で「ダイナミックマップ」という概念を用いての説明がよかったです．（松浦満夫）
「3．自動運転を支える高精度測位と高精度地図」
■自動運転に対する地図の重要性を理解した．（匿名希望）
■高精度衛星測位技術の現状と課題が説明されていて，高精度地図データと組み合わせた自動運転の実用化に向けた取り組みを知ることができよかった．（山下昭裕）
■読者であるIT技術者向けに，測位技術をより分かりやすく解説いただけるとさらによかった．（匿名希望）
「4．自動運転用プロセッサの要求性能・機能・方式」
■自動運転技術の進化により，車がスマホ化していることが分かった．（匿名希望）
■自動運転に求められる処理特性を，一度に多くのシナリオを評価・取捨選択しなければならない，と端的に表現している点が良い．判断処理のためにMIMDが

多用され始めているなど，トレンドが紹介されている点も良い．（匿名希望）

■自動運転の複雑なソフトウェアをアクセラレートする最適な構成（アーキテクチャ）を実現するのはとても難しそうだと感じました．（後藤正宏）

■カギになる判断処理で，今後イノベーションがありそうな感じがする．先端的な技術に踏み込んだ解説があれば，もっと良かったように思う．（匿名希望）

■種々のプロセッサの特質についてもう少し分かりやすく説明があればよかった．（山下昭裕）

「5．自動運転の法律問題」

■技術面だけでなく，自動運転の法律問題の扱い方の難しさを理解できた．法律家に加え，保険会社の自動運転への対応方針を聞いてみたかった．（小橋喜嗣）

■ AI 自動車の AI に問題があった場合は，AI は無体物なので PL 法が適用されないことが理解できました．今後の法整備を期待します．（匿名希望）

■私が免許を取得したときには，ドライブレコーダーのつけ方，使い方の講習はなかったが，今後はオートマ・マニュアルのほか，関連センサーの確認を考慮すると，自動運転コースが必要なのかもしれない．（匿名希望）

■自動運転プログラムが「装置」であるというのは知らなかった.そう捉えることで問題がクリアになる.(中島秀之)

■ほかの車両から情報を貰う場合の権利やセキュリティを解決する必要があるのだということには深く考えていませんでした．事故ばかりではなくこういう機能面での指摘がよかったです．（岡本克也）

■「事故前提の責任論や損害賠償論ではなく，事故低減を前提での法理論構築が大切になる」がよく理解できません．リスク管理は必要なので，事故前提の責任論や損害賠償論は必要ではないでしょうか？（匿名希望）

「6．自動運転バスの実証実験」

■自動運転の現状が実例で示されており大変勉強になった．（匿名希望）

■著者が自動運転の話題で公共交通（路線バス）を実社会での事例を踏まえ技術的視点から論じた点に，社会貢献への高き志を感じ取れた．（大塚敬義）

■信号などの社会インフラをどう維持管理していくのかに興味がある．（匿名希望）

■実証実験の紹介に加えて，実験から得られた課題やその解決への取り組みなどを紹介いただけるとよかった．（匿名希望）

教育コーナー「ぺた語義」

「想像してごらん，スマホが 1 億円する世界を……」

■イメージがしやすかったです．ジュニア会員にとっては大変読みやすいと思いました．（井手広康）

■技術の進化を改めて感じた内容だった．（匿名希望）

■たとえ話としてとても分かりやすいです．（佐藤章博）

■ 1960 年代の説明を記述した文章表現が新鮮だった．（鈴木広人）

■メインフレームを使っていましたので，懐かしく思えました．（匿名希望）

■まったく同感です．学生時代を思い出しました．（小西敏雄）

■筆者の想像する未来についても記述してほしかった．（鈴木広人）

「情報処理学会データサイエンス・カリキュラム標準（専門教育レベル）」

■現存する関連資格である G，E 検定などとはまた別な認定を策定していくのも分かるが，可能な限り分かりやすい資格となってほしい．（匿名希望）

■カリキュラムを組むときの参考になった．（匿名希望）

■データサイエンスの教育について欧米の動向を知ることができました．（匿名希望）

■ DS を身につけることは特に若い世代にとって有用ですが，それより上の現役世代にとっても必要な事柄です（人数も多い）．そういう人たちがカリキュラム標準に従った教育を受けられる機会が増えるとよいと思います．（岡本克也）

■時間配分は示されているのですが，評価も述べてほしい．（匿名希望）

「学生による学習支援システムの機能改善」

■学生でもどんどん活躍しているということを示している良い記事だった．未踏などの突き抜けたレベルから，普通の学生のレベルまで幅広く記事として取り上げているのがよい．（上田晴康）

■「現場」の大切さを感じます．目的は「現場」から，方法は「知見者」から，参考になる記事でした．（伊藤治夫）

■学生の視点で学生が求めている機能を短期間で作成したというスピード感がすごいと思った．また安全面も大学側と連携を行うことで担保している部分もしっかりしていると感じた．（匿名希望）

■実装に難しかった点や運用に向けて苦労した点などの

話も伺ってみたい．（匿名希望）

連載「先生，質問です！」

■きっかけは大切ですし，こういった質問が学生から出てくるのがいいと思った．（匿名希望）
■人生色々が受け取れました．情報処理は一義的より多義であることを考えるのもよいかと思いました．（伊藤治夫）

連載「情報の授業をしよう！：アナログとデジタルの理解について」

■学校教育での苦労と工夫がよく分かった．特に時計のアナログ，デジタルの差異などは十分な注意が必要と理解できた．（祖父江真一）
■情報学の授業の行い方，生徒がどこを理解したらいいのかが考えられている．（匿名希望）
■練習問題は，アナログかデジタルかだけを答えさせるだけではなく，そのように考えた理由を書かせた上でほかの生徒と意見交換させると，より対話的で深い学びになるのではないかと思った．（桑木道子）

連載「ビブリオ・トーク：目の見えない人は世界をどう見ているのか」

■視覚障害者を「世界の別の顔」を感知できるスペシャリストと捉えている，という引用でこの本を読んでみたいと思いました．（上田晴康）
■視覚障害者の支援について考えよう，となったときに，想像力が及ばないことは多々あるのではないか．そのときの助けになる本ということが理解できた．切り口がすばらしい．（佐藤章博）

IT 紀行「キラキラが気になる！ ウェアラブル LED の会社に行ってみた！」

■写真やイラストにて分かりやすく説明いただいており，とても良いと感じました．（匿名希望）
■初めて知る内容が多かった．理科などのセンサー以外としても学習教材となりそうだと思った．（匿名希望）
■パラリンピック開会式におけるウェアラブル LED の無線通信の苦労話を知れた．このような大規模なイベントでは，スマホをマナーモードではなく電源オフにすることで，観客もイベントの成功に寄与できるのだと思った．（桑木道子）
■公式プログラムの写真があるが，冊子を撮影したもので見づらい点が気になる．（匿名希望）

会議レポート「COMPSAC 2021 会議報告」

■会議の概要がシンプルにまとまっている．（柴田　晃）
■発表についてもう少し内容を紹介してもらえると嬉しい．（柴田　晃）

特別解説「ヒト型ロボット『Pepper』の生産停止にざわつく」

■ Pepper の生産停止が悲しい，という現象が問いかけるものについて，筆者を含めオーナーの反応を面白く読みました．（匿名希望）
■自分だけで考えるのではなく，ほかの人を巻き込んで話し合い感じていることがどうなのかと掘ってみる試みは楽しく読むことができました．（岡本克也）

連載「教科『情報』の入学試験問題って？：大学共通テスト『情報』サンプル問題，『コミュニケーションと情報デザイン』領域の問題を見てみよう」

■情報の教育が分かった．（匿名希望）

会誌の内容や今後取り上げてほしいテーマに関して，以下のようなご意見やご要望をお寄せいただきました．今後の参考にいたします．

■量子コンピュータ関連（匿名希望）
■マイナンバーカードの利用（健康保険とのリンクなど）（鶴岡信治）
■宇宙に行った人が考える情報処理（伊藤治夫）
■環境問題など（匿名希望）
■拡張現実（匿名希望）

「先生，質問です！」には以下の質問をいただきました．

■私は，プログラミングに苦手意識があります．先生は，プログラミングが苦手であったときはありましたか．それがいつから楽しいとかプログラミングができるようになろうとしたのですか？（匿名希望）
■ピラミッドは発電所？（伊藤治夫）

note「情報処理」（https://note.com/ipsj）に掲載されている記事に関して，以下のようなご意見やご要望をお寄せいただきました．今後の参考にいたします．

■企業のソフトウェア技術者が抱える課題を抽出されていることがよいと思います．「現場力」＋「知識力」の記事掲載を願います．（伊藤治夫）

■こちらを見ると冊子版と同じ内容が見えて，移行が順調であることを感じました．（小西敏雄）

EPUB に関して，以下のようなご意見やご要望をお寄せいただきました．今後の参考にいたします．

■ EPUB は横スクロールするので，最初は戸惑いました．また，図が最後のページにすべて集約され，記事と図を突合するのが大変でした．（匿名希望）

オンライン化について，以下のようなご意見やご要望をお寄せいただきました．今後の参考にいたします．

■オンライン化は保管スペースがいらず，検索も容易で便利である．（鶴岡信治）
■英知を結集した最先端にしてほしいです．（伊藤治夫）
■冊子の方が頭に入りやすい．（匿名希望）
■軽い読み物ばかりではなく，特集の一部でもよいので冊子版に掲載してほしい．（匿名希望）
■オンライン化は良いと思いますが，オフラインで読める PDF 版の提供は続けてください．（匿名希望）
■オンライン化すると必要なとき以外，見ないかもしれません．多くの人の目に見せるには，書店で冊子を並べるべきだと思います．（小西敏雄）

【本欄担当　鵜川始陽，工藤瑠璃子／会員サービス分野】

これらのコメントは Web 版会員の広場「読者からの声」< URL : https://www.ipsj.or.jp/magazine/dokusha.html > にも掲載しています．Web 版では，紙面の制限などのため掲載できなかったコメントも掲載していますので，ぜひ，こちらもご参照ください．会誌や掲載記事に関するご意見・ご感想は学会 Web ページでも受け付けております．今後もより良い会誌を作るため，ぜひ皆様のお声をお寄せください．

「情報処理」アンケート回答フォーム▶
https://www.ipsj.or.jp/magazine/enquete.html

【ご案内】会誌「情報処理」のオンライン記事について

会誌「情報処理」の特集記事は，これまで冊子，オンライン（電子図書館）の両方に掲載しておりましたが，2020 年 11 月号より**オンラインのみへの掲載**に変わりました．また，オンライン限定記事の掲載も始まりました．閲覧方法は会員区分によって異なりますので以下をご確認ください．

【個人会員の皆様】
電子図書館（情報学広場：https://ipsj.ixsq.nii.ac.jp/ej/）にログインし，該当記事の pdf をダウンロードしてください．すでに電子図書館をご利用いただいている方は今までどおりです．電子図書館を初めて利用される方は，会員としてのユーザ登録が必要になります．未登録の方には毎月上旬に次の件名のメールを送信しておりますので，到着次第，登録してください．
- 件名：[情報学広場 : 情報処理学会電子図書館] ユーザー登録のご案内
- 差出：ipsj-ixsq@nii.ac.jp

★詳細：電子図書館利用方法（個人用）－利用までの流れ（https://www.ipsj.or.jp/e-library/ixsq.html#anc2）
ご案内メールをお急ぎの方や閲覧方法が分からない方は，会員サービス部門（E-mail: mem@ipsj.or.jp）に会員番号を添えてご連絡ください．

【個人会員】
電子図書館
（情報学広場）

【賛助会員各位・購読員の皆様】
賛助会員・購読員の企業・大学に所属されている方に「情報処理」（冊子）を貸し出しした場合，特集の閲覧方法について照会がございましたら，次の手順をお知らせください．

＜手順＞
(1)「情報処理」の特集ページ（扉または概要ページ）を開く．
(2) 閲覧申込の URL にアクセスする（または QR コードを読み取る）．
(3) 必須事項を入力し送信する．
(4) 次の件名（4 月号の場合）の受信メールに従って，電子図書館から特集の pdf をダウンロードする．
- 件名：情報処理 2022 年 4 月号（Vol.63, No.4）「チケットコード」とご利用方法のご連絡

★注意事項
- 法人アカウントではご利用いただけません．
- 閲覧される方が電子図書館のユーザ ID をお持ちでない場合は，ご自身でユーザ登録する必要があります．

本件に関する問合せ先：一般社団法人情報処理学会　会員サービス部門　E-mail: mem@ipsj.or.jp

人材募集
（有料会告）

有料会告

申込方法：任意の用紙に件名，申込者氏名，勤務先，職名，住所，電話番号および請求書に記載する「宛名」，Web 掲載の有無などを記載し，掲載希望原稿（[募集職種，募集人員，（所属），専門分野，（担当科目），応募資格，着任時期，提出書類，応募締切，送付先，照会先]）を添えて下記の申込先へ，E-mail，Fax または郵送にてお申し込みください．
＊都合により編集させていただく場合がありますので，ご了承ください．

申込期限：毎月 15 日を締切日とし翌月号（15 日発行）に掲載します．

掲載料金：国公私立教育機関，国公立研究機関　22,000 円（税 10％込）
賛助会員（企業）　33,000 円（税 10％込）
賛助会員以外の企業　55,000 円（税 10％込）
＊本会誌へ掲載依頼いただいた場合に限り，追加料金 4,400 円（税 10％込）で同一内容を本会 Web ページに掲載できます．

申 込 先：情報処理学会　会誌編集部門（有料会告係）　E-mail: editj@ipsj.or.jp　Fax(03)3518-8375
＊原稿受付の際には必ず原稿受領のお知らせを差し上げています．もし 3 日以内（土日祝日除く）に返信がない場合は念のため確認のご連絡をください．

＊特に指定がないかぎり履歴書には写真を貼付のこと

■国立研究開発法人情報通信研究機構

国立研究開発法人情報通信研究機構（NICT）は，情報通信分野を専門とする我が国唯一の公的研究機関として，情報通信に関する技術の研究開発を基礎から応用まで統合的な視点で推進し，同時に，大学，産業界，自治体，国内外の研究機関などと連携し，研究開発成果を広く社会へ還元し，イノベーションを創出することを目指しています．当機構では，情報通信技術の研究開発推進のため，優秀で意欲のある研究者を広く公募いたします

募集職種　パーマネント研究職員，パーマネント研究技術職員およびテニュアトラック研究員

採用時期　2023 年 4 月 1 日（原則）

応募方法　当機構採用情報の Web ページからのエントリー
URL：https://www.nict.go.jp/employment/index-top.html

応募締切　2022 年 4 月 8 日（17：00 必着）

照 会 先　〒 184-8795 東京都小金井市貫井北町 4-2-1
国立研究開発法人情報通信研究機構 総務部人事室人事グループ／経営企画部 研究職採用担当　E-mail: jinji-r@ml.nict.go.jp
Tel(042)327-7304　Fax(042)327-7590

そ の 他　詳細は当機構採用情報の Web ページにてご確認ください

■広島工業大学情報学部情報工学科

募集人員　教授，准教授，講師または助教　1 名

専門分野　コンピュータシステム

担当科目　コンピュータアーキテクチャ，デジタルシステム設計等のコンピュータシステム関連科目，プログラミング等の専門基盤科目など

応募資格　①本学の教育方針を理解し，教育および研究に熱意のある方，②博士の学位を有する方，③上記分野における研究業績があり，学協会等でも活動され，社会的貢献をされている方，④大学院（博士前期課程）の授業および研究指導を担当可能な方

着任時期　2022 年 9 月 1 日

応募締切　2022 年 5 月 9 日（必着）

照 会 先　学校法人鶴学園　法人局人事部
E-mail: jinji@it-hiroshima.ac.jp　Tel(082)921-4110

そ の 他　【詳細】学校法人鶴学園　採用情報　教員公募
URL：http://tsuru-gakuen.ac.jp/careers.html

FIT2022 第 21 回情報科学技術フォーラム
選奨論文・一般論文 講演募集予告

会　期：2022年9月13日（火）～15日（木）
会　場：慶應義塾大学　矢上キャンパス

FIT2022 Web ページ　https://www.ipsj.or.jp/event/fit/fit2022/

受付期間(予定)：2022 年 3 月 29 日（火）～5 月 11 日（水）

◆論文ページ数：2～8ページ程度　　◆講 演 時 間：20分
◆3ページ目以降は追加ページ代（4,000円／ページ）が必要です

電子情報通信学会 情報・システムソサイエティ（ISS）並びにヒューマンコミュニケーショングループ（HCG）と情報処理学会（IPSJ）は、2002年から毎年秋季に合同で「情報科学技術フォーラム(FIT：Forum on Information Technology)」を開催しています。2022年9月には、第21回目を慶應義塾大学　矢上キャンパスで開催します。FITは、両学会の大会の流れをくむものであると同時に、従来の大会の形式にとらわれずに新しい発表形式を導入し、タイムリーな情報発信、活気ある議論・討論、多彩な企画、他分野研究者との交流を実現してきております。皆様の研究成果発表の場として、標記のとおり論文発表を募集致しますので奮ってお申込み下さい。

●申込主要日程（予定）

登録申込／投稿受付期間：2022年3月29日（火）から　2022年5月11日（水）まで
最終掲載原稿締切：2022年6月24日（金）
※ FIT2017 より、査読付き論文は廃止とし、選奨論文制度を取り入れました。
※ 登録申込と原稿投稿は上記のFIT2022 Webページよりお願い致します。詳細は決定次第 Webページでお知らせ致します。

●表彰

FITには、以下の表彰制度がありますので是非ともチャレンジして下さい。
いずれの賞も、電子情報通信学会又は情報処理学会の会員であることが受賞条件となりますのでこの機会に是非御入会下さい。

船井ベストペーパー賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上 3 件選定。賞金は船井情報科学振興財団より 20 万円贈呈。
FIT 論文賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上 7 件程度選定。賞金は FIT 運営委員会より 5 万円贈呈。
FIT ヤングリサーチャー賞	2022 年 12 月 31 日現在で 33 歳未満の講演者（選奨論文および一般論文）の中から、発表件数の 1.5%を上限として選定。賞金は FIT 運営委員会より 3 万円贈呈。本賞受賞は本人に対し一回のみ。
FIT 奨励賞	一般発表のセッション毎に座長の裁量で優秀な発表を 1 件その場で選定（該当なしもあり）。FIT 終了後に賞状を贈呈。

●選奨論文（4～8 ページ程度）

投稿された論文の担当研究会を決定していただきます。FIT2022 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において投稿時に適切に選択して下さい。
船井ベストペーパー賞、FIT 論文賞への審査を希望する場合は、Web からの講演申込みの際に必ず論文形式で『選奨論文』を選択して下さい。但し、賞を前提とした論文形式となりますので、電子情報通信学会又は情報処理学会の会員であることが投稿条件となります。非会員の方は御入会手続きをお済ませの上御投稿下さい。選奨論文は FIT 初日の選奨セッションに組み込まれ、各セッションにて選奨委員 2 名による 1 次審査を行います。1 次審査の結果は当日の夕方までに大会会場に掲示されます。2 次審査は FIT 終了後実施され、上位 3 件が船井ベストペーパー賞、次点 7 件程度が FIT 論文賞の受賞となります。
※4 ページ以上の投稿が必須ですが、3 ページ目からは追加ページ代（4,000 円／ページ）が発生します。例えば 6 ページ投稿の場合、4 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000 円×4＝16,000 円」の追加費用が必要となります。

●一般論文（2～8 ページ程度）

FIT2022 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において適切に選択して下さい。
※3 ページ以上の投稿される場合は、3 ページ目からは追加ページ代（4,000 円／ページ）が発生します。例えば 4 ページ投稿の場合、2 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000 円×2＝8,000 円」の追加費用が必要となります。

●論文誌推薦制度

選奨論文の中から船井ベストペーパー賞の審査を通して優秀な論文と判断されたものを、FIT プログラム委員会が電子情報通信学会または情報処理学会（FIT 講演申込フォームの講演応募分野（研究会）で選択した研究会が属する学会）の論文誌へ推薦します。掲載の採否は、それぞれの学会の論文誌編集委員会が決定します。論文誌への投稿の際には、投稿先論文誌編集委員会の評価基準を満足しうる、完成度の高い論文に仕上げて頂くことをお薦めします。なお、推薦を辞退することも可能です。

●問合せ先（FIT2022事務局）

〒101-0062 千代田区神田駿河台 1-5　化学会館 4 階
情報処理学会　事業部門 TEL. 03-3518-8373　FAX. 03-3518-8375　E-mail：ipsjfit@ipsj.or.jp

■ 編集室 ■

ご執筆いただいた社会インフラ・セキュリティ分野における第一人者および事務局の方々には，年末年始を挟む時期にもかかわらず，原稿ご執筆に多大なご協力をいただきました．

社会インフラ・セキュリティは，サイバーセキュリティ分野の中でも今後特に重要になると考えられる分野で，進化する新しい領域における課題と取り組みについて高度な内容を捉えつつ，読みやすさにも配慮してご執筆いただきました．

ご執筆者，関係者の尽力のお陰で，期限内に無事特集として結実し，セキュリティ分野における今後の在り方を方向付ける端緒となることが期待されます．

（石黒正揮／本特集エディタ）

次号（5 月号）予定目次

編集の都合により変更になる場合がありますのでご了承ください．

※はオンライン版のみの掲載となります

巻頭言：編集長就任にあたって／副編集長就任にあたって

「小特集」個人情報保護法制の最新動向※

2020 年個人情報保護法改正の概要と情報処理実務への影響／ 2021 年個人情報保護法改正の概要／個人情報保護法改正と学術研究への影響／個人情報保護法改正と AI 開発／倒産処理と情報資産をめぐる規律

「デジタルプラクティスコーナー」超スマート社会実現に向けた情報技術活用のプラクティス※

スマートホスピタル構想における汎用型多目的ロボットの活用／新たな利用時品質モデルの考え方―自動運転バスの運用を事例として―／農産物流通の DX を加速するスマートフードチェーンの構築―生産・流通・消費をつなぐデジタルプラットフォーム―／超スマート社会における高齢者の IT 活用を促進する“人に寄り添うテクノロジー”の展望／「超スマート社会実現に向けた情報技術活用のプラクティス」座談会

提携団体推薦論文※

［JISA 招待論文］表彰制度「JISA Awards」について／［JISA 招待論文］ID 秘匿化ワンタイム多要素認証― SECUREMATRIX の研究開発―／［IBM ナレッジモール論文］物流現場の労働力不足の解消とテレワークの実現～意思決定を支援するロジスティクス・コックピットの構築～

教育コーナー：ぺた語義

連　載：5 分で分かる ⁉ 有名論文ナナメ読み／教科「情報」の入学試験問題って？※／情報の授業をしよう！／先生，質問です！／ビブリオ・トーク

コラム：巻頭コラム

会議レポート：SIGGRAPH Asia 2021 会議報告 ― Real Time Live! Chair 編―

訂　正

本誌 63 巻 3 号（2022 年 3 月号）の特集：知能コンピューティング― AI とハードウェアの出会い―「編集にあたって」に一部誤りがありました．お詫びして訂正いたします．

P.109　左段 17 行目

（誤）高前田信也

（正）高前田伸也

掲載広告カタログ・資料請求用紙

広告のお申込み

■広告料金表（価格は税 10%込）

掲載場所	4 色	1 色
表 2	363,000 円	—
表 3	302,500 円	—
表 4	423,500 円	—
表 2 対向	330,000 円	—
表 3 対向	291,500 円	170,500 円
前付 1 頁	275,000 円	148,500 円
前付 1/2 頁	—	88,000 円
前付最終	—	162,800 円
目次前	—	162,800 円
差込 （A4 変形判 70.5kg 未満　1 枚）	302,500 円	
差込 （A4 変形判 70.5kg ～ 86.5kg　1 枚）	385,000 円	
同封 （A4 変形判　1 枚）	385,000 円	

■「情報処理」

発　　行　一般社団法人 情報処理学会
発行部数　20,000 部
体　　裁　A4 変形判
発 行 日　毎当月 15 日
申込締切　前月 10 日
原稿締切　前月 20 日
広告原稿　完全版下データ
原稿寸法　1 頁　天地 250mm ×左右 180mm
　　1/2 頁　天地 120mm ×左右 180mm
雑誌寸法　天地 280mm ×左右 210mm

■問合せ・お申込み先

〒 169-0073　東京都新宿区百人町 2-21-27
アドコム・メディア（株）（Tel/Fax/E-mail は下に記載）

＊原稿制作が必要な場合には別途実費申し受けます.
＊同封のサイズ・割引の詳細についてはお問合せください.

掲載広告の資料請求

掲載広告の詳しい資料をご希望の方は，ご希望の会社名にチェック ☑ を入れ，送付希望先をご記入の上，Fax にて（または E-mail にて必要事項を記入の上）アドコム・メディア（株）宛にご請求ください.

■「情報処理」 63 巻 4 号　掲載広告（五十音順）

□ MCPC…… 表 3
□キオクシア …… 表 4
□電子情報通信学会…… 表 2 対向下
□とめ研究所…… 表 2 対向上
□すべての会社を希望

■資料送付先

フリガナ
お 名 前 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

勤 務 先 ＿＿＿＿＿＿＿＿＿＿＿＿ 所属部署 ＿＿＿＿＿＿＿＿＿＿

所 在 地 （〒　　-　　）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

TEL（　　）　　-　　FAX（　　）　　-

ご専門の分野 ＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

お問合せ・お申込み・資料請求は
広告総代理店 アドコム・メディア（株）
Tel.03-3367-0571　Fax.03-3368-1519　E-mail: sales@adcom-media.co.jp

賛助会員のご紹介

本会をご支援いただいております賛助会員をご紹介いたします．
Web サイト（https://www.ipsj.or.jp/annai/aboutipsj/sanjo.html）「賛助会員一覧」のページからも
各社へリンクサービスを行っておりますので，ぜひご覧ください．

照会先　情報処理学会　会員サービス部門　E-mail: mem@ipsj.or.jp　Tel.(03)3518-8370

●●● 賛助会員（20 ～ 50口）

（株）日立製作所

富士通（株）

日本電気（株）

三菱電機（株）

（株）サイバーエージェント

日本アイ・ビー・エム（株）

●●● 賛助会員（10 ～ 19口）

（株）リクルート

グーグル合同会社

（株）NTT ドコモ

（株）東芝

日本電信電話（株）

日本マイクロソフト（株）

（株）フォーラムエイト

●●● 賛助会員（3 ～ 9口）

（一社）情報通信技術委員会

（株）NTT データ

グリー（株）

（一財）インターネット協会

（一社）情報サービス産業協会

トレンドマイクロ（株）

（株）BFT

NTT コムウェア（株）

NTT テクノクロス（株）

（株）うえじま企画

エッジテクノロジー（株）

沖電気工業（株）

コアマイクロシステムズ（株）

三美印刷（株）

ソニー（株）

（株）テクノプロ
テクノプロ・デザイン社

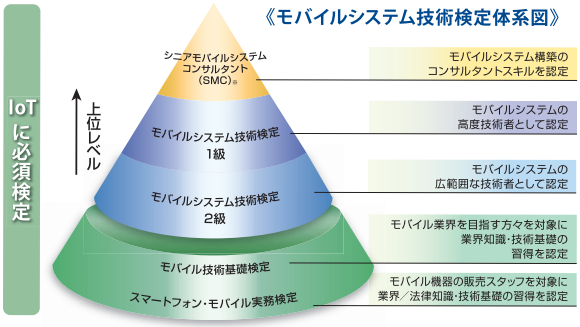
みずほリサーチ&テクノロジーズ（株）

DX推進の必須資格 5G・IoT・AIエンジニアのための資格試験

2022年度 MCPC 検定のご案内

モバイルシステム技術検定

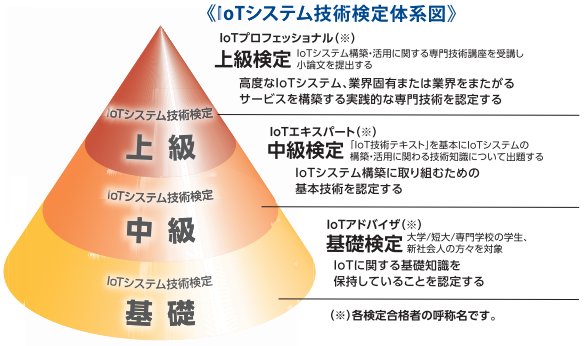
モバイルシステムを構成するワイヤレス通信、モバイル端末、モバイルコンテンツとアプリケーション、セキュリティ等の基本技術からモバイルシステム分析、構築などの応用技術までを体系化した4レベル資格の検定制度です。既に7万8千人以上が受検されモバイルシステム分野の「業界標準資格」です。



※SMC合格者は経済産業省推奨資格【ITコーディネータ資格】の専門課程が免除されます。

IoTシステム技術検定

IoTシステム構成と構築技術、センサ・アクチュエータと通信方式、データのAI分析と活用技術、IoTセキュリティ、プロトタイピングなどIoTシステムの概要と実務の基礎を体系化した3レベル資格の検定制度です。新ビジネスイノベーションの推進やIoT・AIで活躍される技術者の必須資格です。



総務省後援 ワイヤレスIoTプランナー検定　認定研修／検定試験(CBT)

＼ 業界をリードするトップが推薦！ ／

株式会社NTTドコモ
代表取締役社長
井伊 基之 氏

KDDI株式会社
代表取締役社長
高橋　誠 氏

ソフトバンクグループ株式会社
代表取締役会長 兼 社長
孫　正義 氏

東京大学大学院工学系研究科教授
スマート IoT 推進フォーラム
技術戦略検討部会長
森川 博之 氏

東京工業大学
副学長（国際連携担当）
高田 潤一 氏

2022年度検定予定日

〈最新情報はWebよりご確認ください〉

■スマートフォン・モバイル実務検定(CBT方式)
2022年 7月19日(火)～ 8月15日(月)
2023年 1月23日(月)～ 2月20日(月)

■モバイル技術基礎検定(CBT方式)
2022年 7月19日(火)～ 8月15日(月)
2023年 1月23日(月)～ 2月20日(月)

■モバイルシステム技術検定［2級］(CBT方式)
2022年　4月22日(金)～　6月13日(月)
2022年10月21日(金)～12月　5日(月)

■モバイルシステム技術検定［1級］
2022年　6月11日(土)
2022年11月12日(土)

■SMC(シニアモバイルシステムコンサルタント)認定・更新研修
認定研修 2022年 9月16日(金)～17日(土)
更新研修 2022年 9月16日(金)、2023年3月10日(金)

■IoTシステム技術検定［基礎］(CBT方式)
2022年　6月20日(月)～ 7月29日(金)
2022年12月　9日(金)～ 2023年1月27日(金)

■IoTシステム技術検定［中級］
2022年　7月　9日(土)
2022年 12月10日(土)

■IoTシステム技術検定［上級］(2日間)
2022年 8月　5日(金)～ 8月　6日(土)
2023年 2月24日(金)～ 2月25日(土)

■ワイヤレスIoTプランナー検定[基礎]認定研修
2022年　6月25日(土)
2023年　2月　4日(土)

■ワイヤレスIoTプランナー検定[基礎](CBT方式)
2022年　5月27日(金)～　6月27日(月)
2022年 11月25日(金)～12月26日(月)

お申込み・詳細スケジュール等の検定についてはこちらへ　https://www.mcpc-jp.org/license/index.htm

5G&L5Gで飛躍する MCPC
モバイルコンピューティング推進コンソーシアム
〒105-0011 東京都港区芝公園3-5-12 長谷川グリーンビル2階
https://www.mcpc-jp.org/

検定・講習会のお問合せは
MCPC検定事務局 TEL.03-5401-1735 FAX.03-5401-1937
E-mail:msec@mcpc-jp.org

〒101-0062 東京都千代田区神田駿河台一―五
編集人 稲見昌彦
発行所 東京都千代田区神田駿河台一―五 一般社団法人 情報処理学会
発行人 木下泰三
電話 東京（〇三）三五一八―八三七四
振替口座 〇〇一五〇―四―八三四八四
印刷所 東京都荒川区西日暮里五―十六―七 三美印刷株式会社
会員外発売所 東京都千代田区神田錦町三―一 株式会社オーム社

定価 1,760 円（本体 1,600 円 + 税 10%）
本誌広告一手取扱い アドコム・メディア株式会社
〒169-0073 東京都新宿区百人町 2-21-27　TEL.03-3367-0571 FAX.03-3368-1519
雑誌　05269-04
4910052690424
01600

訂　正

本誌 63 巻 4 号（2022 年 4 月号）の連載：先生，質問です！に一部誤りがありました．お詫びして訂正いたします．

p.195　久保田晃弘氏回答 5 行目

（誤）もし見つかったら，その人の所属先なり，あるいは連絡先などを（これも検索すれば見つかる場合があります）に，メールなどで連絡してみるのがよいと思います．

（正）もし見つかったら，その人の所属先なり，あるいは連絡先など（これも検索すれば見つかる場合があります）に，メールなどで連絡してみるのがよいと思います．


一般社団法人
情報処理学会
Information Processing Society of Japan