

情報処理

2020
4

Vol.61 No.4
通巻 661 号

特集 新たなモビリティ時代のサイバーセキュリティ —セキュリティによるジャパン・ブランドの向上に向けて—

解説 高専プロコン 30 年の歩み

サイバーセキュリティ研究における倫理的配慮のサポート



巻頭コラム

インターネット文明を創る
村井 純

電子版もご覧ください



電子版を読む(会員無料)
情報学広場



iPhoneなどで読む(有料)
Kindle



電子版を購入(有料)
Fujisan

教育コーナー：ぺた語義

連載：IT 紀行／5 分で分かる!! 有名論文ナメ読み／集まれ!ジュニア会員!!／

買い物自慢／情報の授業をしよう!／先生、質問です!／ビブリオ・トーク

会議レポート

学会活動報告



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

SuperCD®利用シーン

"デジタルサイネージ編"



オフィスで ③画面



これ
パソコンです！

プチ切り
自動再起動

4K表示に対応



無音だから
じゃましません

手のひらサイズ



電車内表示
個別 ③画面



電車内表示
横長映像 ③画面



『これ 1 台で
4K または ③画面表示』

生産現場で！
工程・進捗・指示・
警報等の情報表示

時刻表 **テロップ**表示
割り込み表示もカンタンです



車両の運転席
③画面の配置は自由です。



-30~60℃の広い動作温度範囲
停留所など温度変化の大きい屋外でも

プチ切り・自動再起動対応で、停電しても自動で復旧



事務所からコントロール

LTEで最新情報に更新

会議・プレゼンテーションのバリアフリー —— “だれでも参加” を目指す実践マニュアル ——



電子情報通信学会
情報保障ワーキンググループ

A5判 ソフトカバー
定価（本体1,900円＋税）

人に優しいイベントや、
分かりやすい発表の手引に！

本会発行単行本の内容に関する詳細は
下記Webページを御参照下さい。
<https://www.ieice.org/jpn/books/tankmokuroku.html>

信学会 目録 で検索！

電子情報通信学会 会員サービス部 会員課
TEL : 03-3433-6691(代)
kaiin@ieice.org

☆☆☆☆ 好評発売中！ ☆☆☆☆

伝送理論の基礎と 光ファイバ通信への応用

笠 史郎 著

A5判 ソフトカバー
定価（本体3,800円＋税）

伝送・通信理論、光ファイバ通信が
この1冊で全て分かる

話し言葉対話の計算モデル

島津 明 中野幹生 共著
堂坂浩二 川森雅仁 共著

A5判 ソフトカバー
定価（本体3,400円＋税）

話し言葉対話を扱うための基礎

「相互協力に関する覚書」に基づき、割引価格（2割引）で御購入頂けます。

「情報処理」を amazonでご購入いただけます！



情報処理学会では、会誌「情報処理」をオンライン通販サイト amazon でも販売しています。ぜひご利用ください。

◀ 「情報処理」（毎月15日発行）

各分野のトップレベルの方々が、最新技術を分かりやすく解説しています。著名人による巻頭コラム、特集、解説、報告、連載、コラムなど。

◆ 価格 1,760 円（税込）

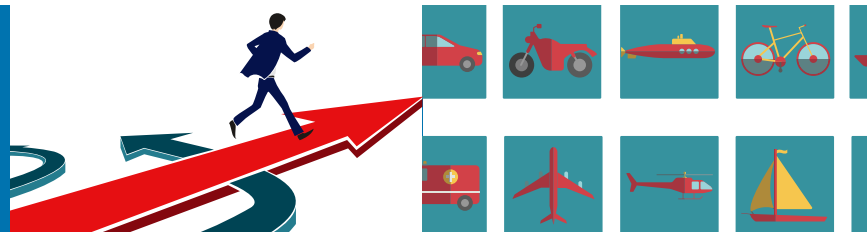
※ 60 巻 10 号までは価格 1,762 円（税込）になります。

★ 60 巻 8 号より Kindle 版も販売開始！！ ★

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

会誌編集部門 E-mail: editj@ipsj.or.jp
Tel.(03)3518-8371 Fax.(03)3518-8375

ご注文は ⇒ <https://www.amazon.co.jp/>



PREFACE

巻頭コラム

- 328 インターネット文明を創る 村井 純

SPECIAL
FEATURES

特 集

新たなモビリティ時代のサイバーセキュリティ —セキュリティによるジャパン・ブランドの向上に向けて—

- 330 0. 編集にあたって 石黒正揮・新 誠一・佐々木貴之
- 332 1. ■自動車セキュリティの国際標準等の動向と今後の課題
—セキュリティ・ブランドによる競争力強化へ— 石黒正揮
- 338 2. ■自動車分野の CASE 革命とサイバーセキュリティ 松原 豊・倉地 亮・高田広章
- 344 3. ■鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ 川崎邦弘・祇園昭宏
- 350 4. ■航空分野のサイバーセキュリティと人材育成 大久保隆夫
- 356 5. ■海事産業におけるサイバーセキュリティ対策動向 稗方和夫
- 362 6. ■ドローンのセキュリティ 春原久徳・田上利博

ARTICLE

解説

- 372 ■高専プロコン 30 年の歩み 神沼靖子・寺元貴幸
- 378 ■サイバーセキュリティ研究における倫理的配慮のサポート 秋山満昭・島岡政基

◆◆「情報処理」Kindle で販売中!◆◆

「情報処理」は Kindle 版でも販売中です! 冊子を持ち運びしなくても、スマホ・タブレット端末さえあればどこでも気軽に会誌を読むことができます。ぜひ活用ください!

ご購入は Amazon から→ <https://www.amazon.co.jp/>
「情報処理学会 Kindle」で検索



★ Jr. 指標にジュニア会員向けが追加されました。

《記号の説明》

基 応 ★ Jr. ■ 基礎 ■ 専門家向け
専 般 ■ 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参考になさってください

情報処理

連載：買い物自慢

371 GR III でスマートフォンとカメラの二刀流生活 今井智大

学会活動報告

384 ■ 量子ソフトウェア研究会の新設にあたって 小野寺民也・今井 浩

386 連載：🎨 集まれ!ジュニア会員!!

教育コーナー：ぺた語義

387 ■ 小中高の先生の自信をサポートします 高橋尚子

388 ■ 🎨 Processing でプログラミングに挑戦! —第3回 繰り返しを使いこなそう— 杉浦 学

393 ■ スリランカの学校訪問記 和田 勉

連載：🎨 ビブリア・トーク—書評—

397 人工知能を活用した研究開発の効率化と導入・実用化《事例集》 江谷典子

連載：🎨 5分で分かる!? 有名論文ナメ読み

398 Mark Weiser : Program Slicing 石尾 隆

連載：情報の授業をしよう!

402 ■ 情報 I を意識した授業をしよう!—紙飛行機制作を通し情報デザイン・データサイエンスに取り組む— 岡本弘之

406 連載：🎨 先生、質問です!

連載：IT 紀行

408 VR センター三銃士に会ってきた! どうなる VR の未来!? 山本ゆうか

会議レポート

410 ASE 2019 参加報告—自動化ソフトウェアエンジニアリングに関するトップクラスの国際会議— 徳本 晋

412 IEEE/ACM SC19 会議参加報告 大辻弘貴

401 論文誌ジャーナル掲載論文リスト
401 論文誌トランザクション掲載論文リスト
414 会員の広場
416 IPJS カレンダー
418 人材募集
419 有料会告
420 有料会告について

423 英文目次
424 アンケート用紙
426 編集室/次号予定目次
427 掲載広告カタログ・資料請求用紙
428 賛助会員のご紹介

■会誌編集委員会

編集長：稲見 昌彦

副編集長：大山 恵弘・加藤 由花・中田真城子

担当理事：楠 房子・清水 佳奈

本号エディタ：

五十嵐悠紀・石黒 正揮・稲葉利江子・井上 仁・井本 和範・
江渡浩一郎・大石 康智・大川 徳之・太田 智美・岡本 雅子・
桂井麻里衣・金子 格・川上 玲・櫻 惇志・斎藤 俊則・
佐々木貴之・佐藤 史子・城島 貴弘・新 誠一・須川 賢洋・
田名部元成・谷田 英生・戸田 貴久・鳥澤健太郎・坂東 宏和・
福地健太郎・坊農 真弓・間瀬 正啓・水野加寿代・茂木 和彦・
山本ゆうか・湯村 翼・渡辺 博芳

編集長ブログ：blog-mag.ipsj.or.jp

理事からのメッセージ：

https://www.ipsj.or.jp/annai/aboutipsj/riji_message.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) ジョ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.or.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-



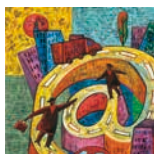
Kindle



Fujisan



情報学広場



インターネット文明を創る

■ 村井 純



2019年に「インターネット誕生50周年」のイベントが世界各地で行われた。ARPANETの研究が1969年に開始されたからである。私自身は、世界中のコンピュータが相互接続され、それを利用した地球規模の分散処理ができないかな、という夢を追いはじめて40年近い時間が過ぎてしまったという思いだ。一方、1969年はベル研究所でUNIXの研究開発が開始された年でもある。その開発者の一人、Ken Thompsonがサバティカルでカリフォルニア大学バークレー校においてUNIXカーネルの授業を行った。その学生だったBill Joyなどが開発していたバークレーのBSD UNIXは、DARPAの研究助成を用いて、TCP/IPを用いたネットワークオペレーティングシステムを完成させた。私はこの80年代初頭に完成された4.2BSDこそが、インターネット文明の起源だと考えている。理由の一つはUNIXの設計理念である。UNIXは、ファイルやソフトウェアツールなどのデジタルデータとその処理に関する抽象概念から設計が進み、ハードウェア依存性を排除した、アプリケーションのオープンプラットフォームとしてのオペレーティングシステムの起源である。これが今日のインターネット環境の基盤を形成した。また、BSDはオープンソースでインターネット上のあらゆる人がソフトウェアの開発に参加する基盤を創り出した。やがて、HTMLとWEBの環境によって、ブラウザをベースにした開発環境から次々と新しいグローバルなサービスがインターネット上で展開した。

■ 村井 純
慶應義塾大学環境情報学部教授

1984 年日本初の大学間ネットワーク JUNET 設立. 1988 年 WIDE プロジェクト設立. 内閣官房 IT 総合戦略本部員他, 各省庁委員会主査等多数務め, 国際学会でも活動. 2013 年 ISOC の選ぶ「インターネットの殿堂」入りを果たす. 「日本のインターネットの父」として知られる. 工学博士.



90年代にはバークレーの研究者たちはシリコンバレーの起業時代をリードするようになった。こうして、インターネットのコアプロトコルの開発の中心が希薄になってきたとき、我が国ではWIDEプロジェクトがそのときのコミュニティの使命であった次世代インターネットプロトコルの開発にフランスなどとともに従事していた。IETFの場で開発と議論を重ねBSD上のIPv6の参照コードの開発をWIDEに集約することが決まり、WIDEの参照コード「KAME」はIPv6体系の発展に貢献した。米国でなく、欧州でもなく、日本のWIDEが開発と発展のコアを果たしたことは、インターネット基盤がグローバルに分散している開発者の手によって構築できることの先例ともなった。インターネット文明のインフラ技術が、世界の技術者によってオープンに開発できる体制であることは大切で、これからも維持されなければいけない。

インターネットは地球全体の新しい情報処理文明の基盤である。すべての人のためのグローバルな基盤となるにはカバー率など残されたさまざまな課題がある。発展するデジタル技術がどのように人と社会に貢献できるのかという課題の追求は続く。ナショナリズムの台頭する今日の国際社会において、人類が初めて手にした真のグローバルなインターネット文明の創造に参加することは、情報処理学会諸氏の大きな使命である。

新たなモビリティ時代の サイバーセキュリティ —セキュリティによるジャパン・ブランド の向上に向けて—

編集にあたって

石黒正揮 | (株) 三菱総合研究所

新 誠一 | 電気通信大学

佐々木貴之 | 日本電気 (株)

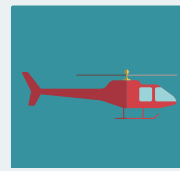
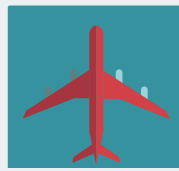
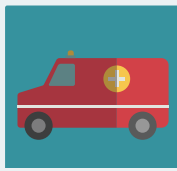
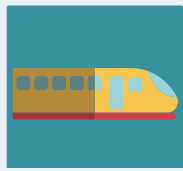
デジタル化とネットワーク化の波が自動車、鉄道などのモビリティ分野にも大きな変革をもたらしている。自動車分野では、自動運転、コネクテッドサービス、シェアリングサービス、電動化など、100年に一度と言われる変革（CASE 革命）が進行し産業構造が激変している。鉄道分野においては、無線式列車制御システム等により列車の位置や状態をリアルタイムで把握・予測することで安全性の確保やダイヤの乱れを迅速に回復するシステムが開発されている。このようなモビリティ分野の変革の一方で、システムが攻撃を受けた場合、生命・身体の安全にかかわる重大な事故につながる可能性があり、危機感が高まっている。実際、自動車、鉄道、航空などの分野で、セキュリティ事故や脆弱性の問題が顕在化している。このようなことから各分野では、セキュリティ基準やガイドラインの策定が急速に進められている。モビリティ分野は、安全性を前提として成り立つ分野であるためセキュリティに対する信頼は、企業の競争力やビジネスに直結する重要な課題である。日本は、自動車の品質、新幹線をはじめ

とした鉄道の安全性など国際的に高い技術力を確保しているが、新たなセキュリティ脅威に対して、従来産業と IT・セキュリティ産業が連携することでセキュリティを強化し、国際的な説明責任を向上させることができれば、これまでの日本の強みに加えて、ジャパン・ブランドを一層向上させることができる。このような視点から本特集では、各分野のセキュリティ脅威とその対策に関する動向および将来の課題展望についてまとめることを目的とした。サイバーセキュリティは産官学の連携による包括的な取り組みが不可欠であることから、本特集では、産官学の協力を得て、モビリティ分野のセキュリティについて知見の深い専門家によりまとめた。

本特集の構成は以下になっている。

(1) 自動車セキュリティの国際標準等の動向と今後の課題

「編集にあたって」のとりまとめを担当した三菱総合研究所 石黒正揮が、自動車のサイバーセキュリティに関する国際標準、政策動向等に基づく今後の取り組み課題について解説した。自動車分野の



CASE 革命に伴い、セキュリティ脅威が高まっており、国連機関 WP29 によるサイバーセキュリティ基準（案）および ISO/SAE21434 サイバーセキュリティ国際標準の策定が進められている。これらの国際基準等は、各国の強制基準である型式認証に反映されることが見込まれるため、関連企業にとって影響が大きい。自動運転にかかわるセキュリティ・フレームワーク等にいち早く対応しセキュリティ・ブランドを向上させることで、国際競争力の高い自動車産業のジャパン・ブランドをさらに強化することが期待される。

(2) 自動車分野の CASE 革命とサイバーセキュリティ

名古屋大学名古屋大学大学院情報学研究科 松原豊氏、倉地 亮氏、高田広章氏によりコネクテッド、自動運転、シェアリング、EV ごとに技術トレンドとセキュリティの脅威についてまとめ、それらに対する取り組みと今後の展望について解説した。新たな脅威が見つかることを前提に運用・保守を含むライフサイクル全体のディペンダビリティを維持する考え方の重要性を指摘している。

(3) 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ

運輸総合研究所 信号・情報技術研究部 川崎邦弘氏、祇園昭宏氏が、鉄道分野の ICT 活用の状況を概観したのち、安全かつ安定した列車運行の実現に向けて不可欠となるサイバーセキュリティについて、鉄道関連の規格等の現状と考慮すべき事項等について概説している。また、今後の重要課題として、安全を最優先に確保しつつ、サービスレベルの低下を最低限にする（＝できるだけ運行し続ける）ための仕組み・対策の構築を挙げている。

(4) 航空分野のサイバーセキュリティ

情報セキュリティ大学院大学 大久保隆夫氏が航空分野のセキュリティ事故事例や航空システムの構成に基づき潜在的な脅威を洗い出し、それを踏まえて、航空分野等のセキュリティ人材育成にフォーカスした取り組みと今後の課題をまとめていただいた。

今後、航空分野においては、セキュリティ情報の共有を行う組織の整備・活用により、運用だけでなく安全な航空システムの構築を含めた対策・人材育成を課題に挙げている。

(5) 海事産業におけるサイバーセキュリティ対策動向

東京大学大学院新領域創成科学研究科 稗方和夫氏が、造船・海運業を中心としたステークホルダの概略と情報通信技術導入の現状について触れ、国際機関や業界団体からのサイバーセキュリティ対策ガイドラインの公表の状況、今後の動向やサイバーセキュリティの産業実装の見通しについて、国際および国内の動向をまとめた。今後の海事産業においては、新造船の特に OT 要素がサイバーレジリエント（設計においてサイバーセキュリティ耐性を実現）であることを要求されることが予想され、その対応はシステムインテグレータとしての造船所が担う範囲になる。

(6) ドローンのセキュリティ

セキュアドローン協議会 春原久徳氏、田上利博氏が、ドローンの活用分野とセキュリティに関する脅威と対策に関する取り組み動向、課題についてまとめている。規制緩和により 5G 搭載ドローンの可能性が開かれ、直接クラウドと連携することで新たな応用が広がるとともに、リスクの変化にも対応できるセキュリティの重要性を指摘している。

自動車、鉄道、航空機などさまざまな交通手段をシームレスに連携させてサービスとして移動手段を提供する MaaS (Mobility as a Services) については、2020 年から 2030 年までの 10 年間に 30 倍の市場になると言われるが、本特集であまり取り上げることはできなかった。MaaS についてはサイバーセキュリティに関する取り組みが進展した時点で特集したい。

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課題が、日本の産業競争力をさらに強化しブランド力を向上させることに寄与することを期待したい。

(2020 年 1 月 27 日)



[新たなモビリティ時代のサイバーセキュリティ・セキュリティによるジャパン・ブランドの向上に向けて]

① 自動車セキュリティの国際標準等の動向と今後の課題 ーセキュリティ・ブランドによる競争力強化へー



石黒正揮 | (株) 三菱総合研究所

自動車セキュリティの国際動向とその影響

自動車分野では、Connected（コネクテッド・カー）、Autonomous（自動運転）、Sharing&MaaS（シェアリング&サービス化）、EV（電気自動車）という4つの大きな変革が同時に進行し、100年に一度の大変革（4つの頭文字から「CASE革命」と呼ばれる）に晒されている。自動車業界^{☆1}とIT企業、AIベンチャー、組込みベンダなどによりグローバルな激しい競争と協調による業界横断的な再編が繰り返されている。

このような大変革が進む中、自動車業界ではセキュリティと安全性の確保が喫緊の課題となっている。

2010年にワシントン大学Koscherらの研究^{☆2}により、車載ネットワークに対する遠隔攻撃法が報告されてから、セキュリティ国際会議Black Hat^{☆3}、DEFCON^{☆4}などにおいて自動車セキュリティの脅威について相次ぎ報告された。2015年には、フィアット・クライスラー・オートモービルズ社（FCA）のSUV車のジープ・チェロキーに対して携帯電話

ネットワークを通じてエンジンなど遠隔から操作される脆弱性が報告され、いったんはソフトウェアアップデートが提供されたものの、結果的には140万台以上に及ぶ自動車の大規模なリコールに至り、業界におけるセキュリティの危機感が高まった。

自動車分野では、これまで分野独自のセキュリティにかかわる基準はなく、2020年頃までに発売される自動車については、ISO15408（Common Criteria）等のIT系のセキュリティ規格を活用し、各社個別の対策が進められている。

セキュリティに関する危機感の高まりから、近年、自動車セキュリティに関する基準、枠組み、体制構築に関する取り組みが進展している。図-1は、自動車セキュリティにかかわる国際基準、体制構築などに関する動向を俯瞰したものである。

国際基準（レギュレーション）については、国際連合欧州経済委員会自動車基準調和世界フォーラム（UNECE/WP29）においてセキュリティに関する勧告Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues^{☆5}が審議されている（2020年に発行予定）。本勧告のAnnexにはサイバーセキュリティの国際基準を定めるRegulation on Cyber Security（以下、「WP29 サイバーセキュリティ国際基準（案）」と呼

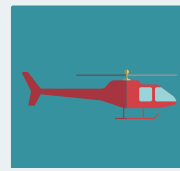
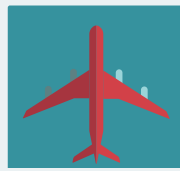
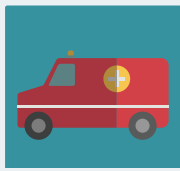
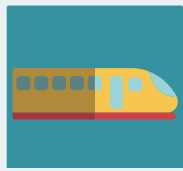
☆1 日本の自動車産業の製造品出荷額は60.7兆円で全製造業の19%（2017年）、輸出額は15兆円で、日本の主要品輸出額の22%（2016年）を占め、国際的に高い競争力を維持し、日本の経済・雇用を支えてきた重要産業である。

☆2 Koscher, K.: Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy.

☆3 <https://www.blackhat.com/>

☆4 <https://www.defcon.org/>

☆5 UNECE, Task Force on Cyber Security and (OTA) software updates (CS/OTA) Proposal for a Recommendation on Cyber Security, Sept, 2019.



ぶ)が含まれている。この国際基準は、同時並行で審議が進められている自動車分野のサイバーセキュリティ・エンジニアリングに関する国際標準(スタンダード)ISO/SAE21434^{☆6}(2020年末発行予定)を前提としている。ISO/SAE21434は、自動車分野のサイバーセキュリティ・プロセスに関する世界初の標準であるSAE J3061をベースとしている。これらの国際基準および国際標準は、自動車の開発・運用にかかわる企業にとって義務的なセキュリティ基準としてきわめて大きな影響を持つことになる。WP29で審議される国際基準やそこから参照される国際標準は、各国の自動車分野の強制基準である型式認証に反映される^{☆7}。したがって、

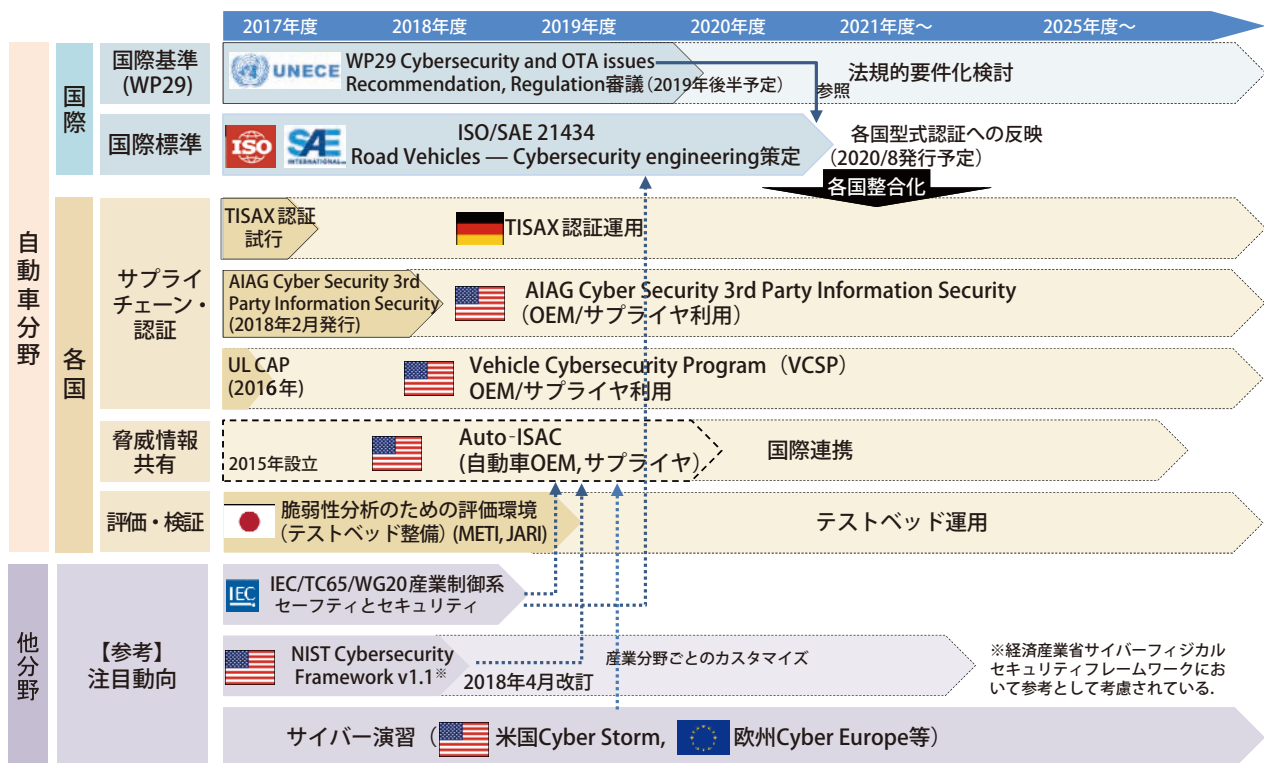
将来的にはWP29サイバーセキュリティ国際基準(案)およびサイバーセキュリティ国際標準(案)ISO/SAE21434は国際的な強制基準のベースとなる。WP29は自動車型式認証の国際的な相互認証の推進を目的としている^{☆8}ため、国際標準ISO/SAE21434に準拠することでグローバルに通用する製品として販売することができるようになる。

大規模なサプライチェーンを形成する自動車産業ではサプライチェーン・セキュリティの確保や認証にかかわる取り組みが重要である。米国UL(Underwriters Laboratories LLC、米国保険業者安全試験所)は、脅威分析、リスク評価、脆弱性テスト、セキュリティ保護対策の検証を目的としたVehicle Cybersecurity Program (VCSP)を提供している。

☆6 ISO/SAE CD 21434 [SAE] Road Vehicles — Cybersecurity engineering

☆7 WP29で審議される国際基準は、「国連の車両等の世界技術規則協定」(1998年協定)に基づき、加盟国の法規への基準の導入が求められる。

☆8 World Forum for the harmonization of vehicle regulations, <https://www.unece.org/trans/main/welcwp29.html>



(出所) 経済産業省「自動運転が活用されるコネクテッド技術に関する国内外動向調査報告書」(2019年3月)などを元に作成

図-1 自動車セキュリティの国際基準、体制構築等に関する動向俯瞰図



また、自動車関連企業の情報システムにかかわるセキュリティ制度としては、ドイツ自動車工業会（VDA：Verband der Automobilindustrie）によるTISAX認証制度や、全米自動車産業協会（AIAG）によるサプライヤに対するサイバーセキュリティ・ガイドライン Cyber Security 3rd Party Information Securityなどが提供される。このように各国ごとに固有の取り組みがあり、それぞれの国においてデファクト標準的な位置づけとなっている。

セキュリティ分野では、常に変化する脅威や新たに発見される脆弱性などの情報を迅速に共有し対策を行うことが重要である。米国では、自動車分野のサイバー脅威を分析、共有、追跡し、潜在的な脆弱性を特定するための情報収集共有組織Auto-ISACが2015年に世界に先駆けて設立され、日本版のJ-Auto-ISACも2017年に設立されている。

セキュリティ分野では、さまざまなシステムが連携する運用環境において問題がないか攻撃を含む評価・検証を行うテストベッドが重要となる。研究事例として英国Coventry Universityにより、車載ネットワークCANシミュレータ上の脆弱性検証テストベッドの取り組みがある。国内では、経済産業省・厚生労働省の共同プロジェクトにおいて、中小サプライヤ、セキュリティベンダおよび研究機関等が脆弱性評価などを行うことを目的に、車内のコンピュータネットワークを模擬したセキュリティ・テストベッドを構築している。また、トヨタIT開発センターおよび横浜国立大学松本勉教授により開発された持ち運び可能なアタッチケースに収納される自動車のセキュリティ検証・評価を行うテストベッドPASTA（Portable Automotive Security Testbed with Adaptability）が発表されている。

セーフティとセキュリティ

自動車分野ではセーフティ（安全性）を確保する基準として機能安全規格（ISO 26262）があり、その導入が進んでいる。一方で、セキュリティの基準については、近年の自動車セキュリティ脅威に対して、自動車のライフサイクル・プロセスや機能安全規格との関係性を考慮した前述の自動車分野のセキュリティ基準、国際標準の策定が進められている。情報通信分野においては、セキュリティ対策基準は長年をかけて開発されてきた。セーフティとセキュリティは、独立した分野として発展してきており、技術、人材、文化のギャップが大きい。また、セーフティとセキュリティの認証を同時に行うプロセスは確立しておらず、両方の対策や認証を行える高度な人材は国際的にもまだ少ない。

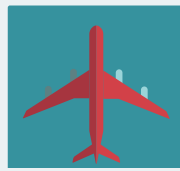
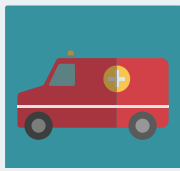
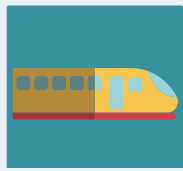
CASE革命の進展により、セーフティとセキュリティの両面に跨るリスクは高まっているため、セーフティとセキュリティの技術やプロセスを連携・統合し、両分野の文化のギャップを解消するとともに、両方に対応できる高度人材を育成することが求められる。

セキュリティ脅威の高まりにより、自動車機能安全規格ISO 26262の第2版改訂において、機能安全とセキュリティのそれぞれの担当組織の間にコミュニケーション・チャンネルを構築し、維持することを設計担当組織に要件化している。

自動車セキュリティの国際標準SAE J3061は、機能安全プロセスとセキュリティプロセスを橋渡しする方法を示したもの（図-2）で、他分野に先駆けてセーフティとセキュリティを統合的に捉えた基準として注目できる。

新しい安全性評価手法の必要性

自動車分野においては自動運転技術の進展に伴



い、従来とは異なる新しい安全性評価の考え方が求められている。その方向性として、走行データ、事故データ、シミュレーション評価等を組み合わせて、社会的に受け入れられる安全性レベルについてコンセンサスを得るものである。代表的な取り組みが、ドイツにおける自動運転システムの安全性評価に関する標準化プロジェクト PEG-ASUS^{☆9}である。自動車事故の原因の94%は人の操作ミス^{☆10}とも言われており、完璧なドライバーのモデルは明確ではないことから、人の運転を代替する自動運転システムについても、100% 完璧な安全性を保証することは困難である。人が運転するよりも安全であれば世に出していいのか？

☆9 PEGASUS RESEARCH PROJECT

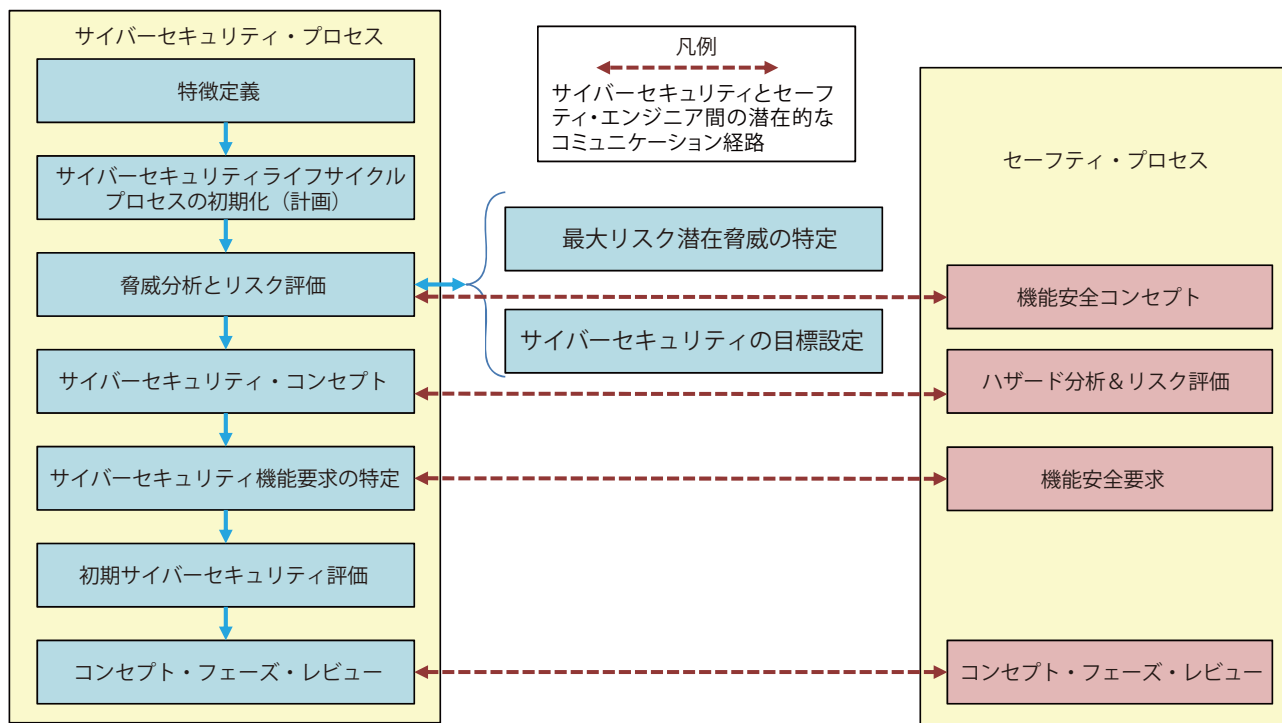
☆10 NHTSA, Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey, 2015.

その安全とはどのように評価するのか？という課題が残っている。自動運転の安全性確保のためには、さまざまな状況における膨大な検証が必要であり、従来のやり方では、開発が現実的な期間やコストで収まらなくなると見られている。統計的には、自動運転の検証に必要なテスト走行距離は、2.4 億 km (地球 6,000 周分) 以上とも言われる^{☆11}。

現在、自動運転車に求められる安全性能と社会的に受け入れられる評価手法はどうあるべきか？

“How good is good enough (どこまで安全にすれば、十分と言えるのか?)”という問いに答えられる新たな評価検証手法が求められている。この問いに対するアプローチとして、PEGASUS プロジェクトにおいては、走行データ、事故データ、

☆11 Winner, H. : ADAS, Quo Vadis? In, Winner, H., Hakuli, S., Lotz, F., Singer, C. : Hand of Driver Assistance Systems, Springer, 2016.



(出所) SAE J3061: Cybersecurity Guidebook for Cyber-Physical Automotive Systemsを元に作成

図-2 サイバーセキュリティ・プロセスとセーフティ・プロセスのブリッジング (開発プロセスにおける概念フェーズの場合)



物理モデル・シミュレーション・データを蓄積し、実テストとバーチャル・テスト（モデルベース検証）を組み合わせ、膨大な状況における評価により現実的な規模で社会的に受け入れられる評価の標準化を進めている。

経済産業省および日本自動車研究所（JARI）は、ドイツ PEGASUS プロジェクトと連携し、新しい安全性評価に関する標準の検討を進めている。新しい安全性評価手法については、日本から UN/WP29 および国際標準化団体 ISO の審議グループ TC22/SC33/WG9 の両方に対して基準・標準の提案を進めている。

このような新しい安全性評価の取り組みを包括したセーフティとセキュリティの統合的な取り組みが求められていく。

リスクとコストのバランス

自動車はコンシューマ製品であるため価格の上昇は製品の売れ行きを大きく左右する。早くからセキュリティ対策が強く求められてきた情報通信、電力、金融などの分野はユーザが事業規模の大きい重要インフラ事業者であり、セキュリティ障害の影響は広範囲に及ぶため必要な対策予算を確保することは求められてきた。

自動車がハッキングされた場合、重大な事故を招く恐れがあり、高いレベルのセキュリティを求められるが、消費者が製品を購入できないぐらい価格が高騰すれば自動車産業の事業は成り立たないため、コストとリスクのバランスはきわめて重大である。

機能安全規格においてはゼロリスク（100%安全）の追求ではなく、リスクは合理的に低減可能な限りにおいて低くするという ALARP（As Low As Reasonably Practicable）の考え方が原則となっている。

自動運転を見据えた安全性評価基準を検討する

ドイツ PEGASUS プロジェクトにおいては、社会的に受け入れられる安全認証のための合理的な基準や評価手法に関する新たな標準の策定を目指している。

自動車セキュリティにおいてもセーフティ分野と同様に社会的に受け入れられる基準を策定することで、自動車業界の過剰な負担を解消し、ユーザが自動車のメリットを享受できるように適正な価格で自動車を購入できるようにすることが求められる。

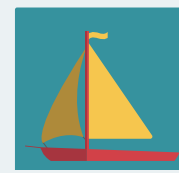
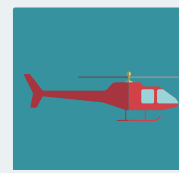
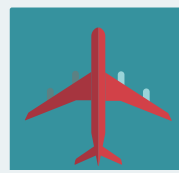
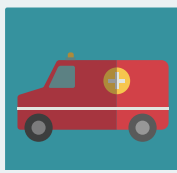
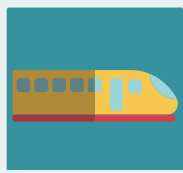
今後の取り組みの課題

WP29 サイバーセキュリティ国際基準（案）および ISO/SAE21434 サイバーセキュリティ国際標準（案）は、今後、各国の強制基準である型式認証に反映されることが見込まれるため、自動車関連会社やセキュリティベンダにとって影響が大きい。自動車に関連する企業は、関連基準に対する理解と対応体制の準備を進めることが期待される。

現在審議中の WP29 サイバーセキュリティ規制（案）や ISO/SAE21434 サイバーセキュリティ国際標準のみならず、関連分野の国際標準化においては、官民一体となった活動の強化、ルール・メイキングへの戦略的な取り組みが期待される。たとえば、経済産業省サイバーセキュリティ課が推進するサイバー・フィジカル・セキュリティ・フレームワーク^{☆12}の自動車版を策定し、国際標準への反映とそれに基づくセキュリティの強化により、日本の強みである自動車産業をセキュリティ・ブランドによりさらに強化することが期待される。

また、新しい領域として、セーフティとセキュリ

^{☆12} 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）



ティを統合化するスキル（技能）を習得した人材の育成も大きな課題である。人材育成については、経済産業省自動車課が推進する「自動走行スキル標準」（図-3）^{☆13}において、車載セキュリティ系、セキュリティ開発技術、安全関連系、新しい安全性評価技術など関連するスキルをベースとして、経済産業省が推進する教育講座推進策である第四次産業革命スキル習得講座認定制度（経済産業省）^{☆14}による

☆13 経済産業省 自動走行ビジネス検討会 人材戦略ワーキンググループ 自動走行ソフトウェアスキル標準, https://www.meti.go.jp/shingikai/mono_info_service/jido_soko/jinzai_senryaku/pdf/2018_003_00.pdf

☆14 経済産業省 第四次産業革命スキル習得講座認定制度, <https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/index.html>

自動運転分野の新しい高度人材育成の推進が期待される。

(2019年10月31日受付)

謝辞 本稿は、経済産業省の委託を受けて（株）三菱総合研究所が実施した「平成30年度高度な自動走行システムの社会実装に向けた研究開発・実証事業（自動運転が活用されるコネクテッド技術に関する国内外動向調査）」の調査結果および関連する経済産業省「自動走行ソフトウェアスキル標準」等を参考にまとめたものです。調査等を通じて、自動走行ビジネス検討会人材戦略WG自動走行ソフト開発スキル標準策定部会の委員、経済産業省自動車課の皆様には大変お世話になりました。皆様には深く感謝を申し上げます。

石黒正揮（正会員） masa@mri.co.jp

博士（情報科学）。サイバーセキュリティ、デジタル・テクノロジー戦略・政策、ソフトウェア工学、AI／データ解析、リスク分析等に関する調査、研究開発、日米欧アジアにおけるサイバーセキュリティ政策、デジタル技術戦略に関する業務に従事。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。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。

凡例 ★2018年度の具体化対象3領域

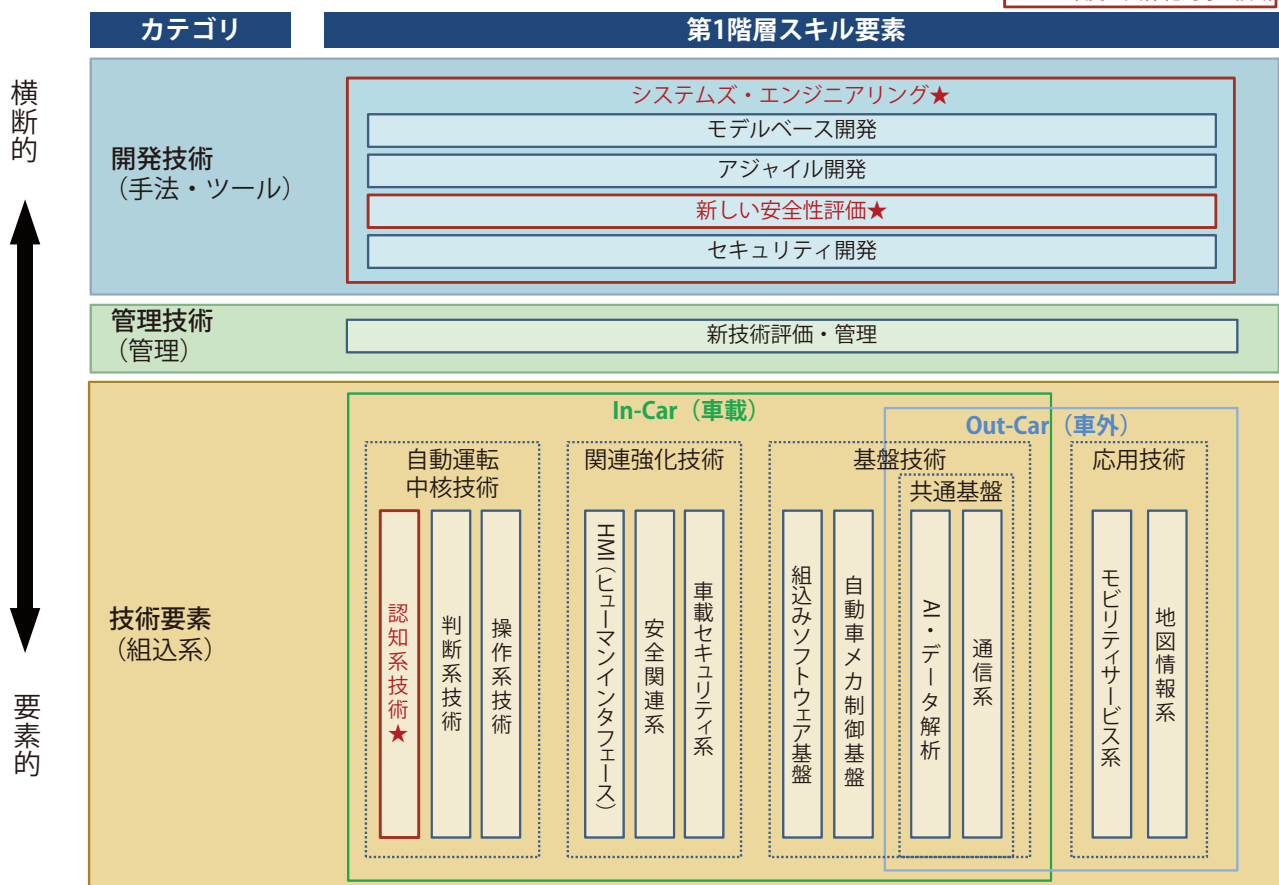


図-3 経済産業省 自動走行スキル標準第1階層の構成



[新たなモビリティ時代のサイバーセキュリティ・セキュリティによるジャパン・ブランドの向上に向けて]

② 自動車分野の CASE 革命と サイバーセキュリティ

応
般

松原 豊 | 名古屋大学大学院情報学研究科

倉地 亮 | 名古屋大学大学院情報学研究科

高田広章 | 名古屋大学大学院情報学研究科

自動車のサイバーセキュリティ

多くの自動車には、先進運転支援システム (Advanced Driving Assistant System, ADAS) や車載インフォテインメントシステム (In-Vehicle Infotainment, IVI) が搭載され、車載ソフトウェアが大規模・複雑化している。開発効率化のために、汎用システムや IT 分野で用いられるソフトウェアが数多く使用されるようになってきている。一般に、大規模なソフトウェアにはバグ (不具合やセキュリティ上の脆弱性の総称) が存在する。ゲートウェイを介して、大規模なソフトウェアを搭載する機器と、車載制御ネットワークとが接続されると、車載制御システム自身の不具合だけでなく、そこに物理的に接続されるソフトウェアの問題も、自動車のセーフティに影響を及ぼす要因の 1 つになり得ると文献 1) で述べた。

自動車業界は CASE と呼ばれるキーワードを中心に、大きく変革していると言われている。CASE の主な対象範囲を図-1 に示す。Connected の C は、自動車と、周辺の自動車 (Vehicle to Vehicle, V2V)、信号機や道路、料金所などの道路上のインフラストラクチャ (Vehicle to Infrastructure, V2I) などと繋がることで情報を共有し、新たなサービスを提供しようという考え方であり、V2X (Vehicle to X, X にはいろいろなモノが入る) と総称される。Autonomous の A は、自律的かつ自動的に動作することを意味し、高度な運転支援や自動運転によって事故ゼロを目指すという考え方である。Shared & Services の S は、人が移動したいと思ったときに、自由かつ柔軟に利用するモビリティ (自動車だけでなく、自転車、バス、電車、ライドシェアやレンタカーを含む移動体) を選択できるようにしようという考え方

のもとで、複数名で自動車を共有すること、および共有を前提としたサービスを指す。Electric (電動化) の E は、自動車制御システムの構造において、電動化がさらに進むということの意味する。本稿では、自動車制御システムの変革を俯瞰した後、CASE のそれぞれの観点において、自動車セキュリティの課題や展開について述べる。

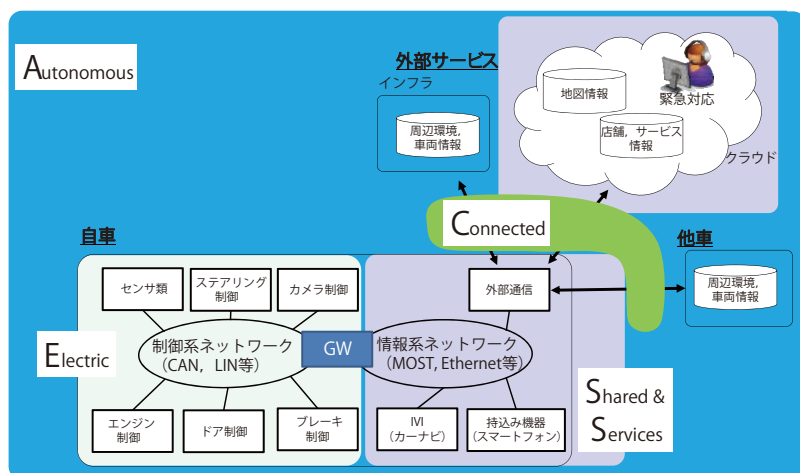
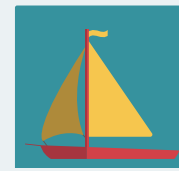
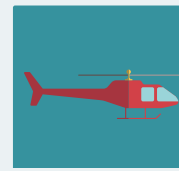
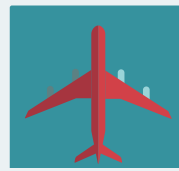
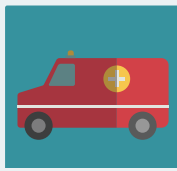
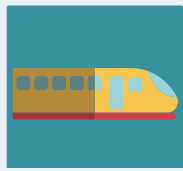


図-1 CASEの主な対象範囲



CASE に向けた自動車の変革

CASE というキーワードを中心とする自動車の変革の中で、自動車にかかわる情報システムも大きく変わろうとしている。ここでは、車載組込みシステムに起こりつつある変化を、3つの観点から述べる。

1つ目の変化として、情報処理と制御の融合を挙げることができる。従来、自動車の制御系と、カーナビゲーションシステム（カーナビ）やカーテレマティクスなどの情報系との間は、疎な結合であった。特に、情報系からの情報を元に制御を行うことは、カーナビの情報をを用いてトランスミッションを制御するなど、限定的な用途にとどまってきた。これが、自動運転では地図の活用が必須となり、V2X通信で得られる情報を制御に活用することが増加していくと考えられる。必然的に、情報系の組込みシステムに要求されるディペンダビリティ、特に安全性やセキュリティに対する要求が、高まることになる。さらに、自動車を移動サービスを提供する手段の1つと捉えると、自動車全体が、クラウド上の情報システムから制御されることになる。

2つ目の変化として、自動車の制御システムが、自律分散型から集中制御型へ変わろうとしていることを挙げることができる。自動車のコンピュータ制御は、個々の機構をコンピュータ制御することから始まった。最初にコンピュータ制御が導入されたのはエンジンであり、その後、ブレーキやステアリングなどもコンピュータ制御されるようになった。従来も、これらの個々の機構の制御システムは、車載ネットワーク経由で制御情報をやりとりして、高度な制御を自律分散的に実現していたが、全体を統括するのはあくまでも人（運転者）であった。

自動運転システムは、このような人の役割をコンピュータで置き換えようとするものであり、必然的に、集中制御的なアーキテクチャになる。自動車全体を統括制御するコンピュータは、ビークルコンピュータやセントラル ECU（Electronic Control

Unit、車載の制御用コンピュータのこと）と呼ばれている。

このような集中制御型への変化は、自動運転車に限らず、起こりつつある。これは、自動車に搭載できるコンピュータの性能向上によりそれが可能になってきたことに加えて、次に述べる遠隔ソフトウェアアップデートの必要性も理由の1つになっている。数十個の車載の ECU のすべてを、遠隔アップデートに対応させるのは容易ではない。遠隔アップデートするソフトウェアがビークルコンピュータに集まっていれば、遠隔ソフトウェアアップデートは相当容易になる。

3つ目の変化として、ソフトウェアアップデート、特に OTA（Over The Air）での遠隔ソフトウェアアップデートが必須と見なされるようになってきたことが挙げられる。従来も、販売店等で車載のソフトウェアをバージョンアップすることはあったが、基本的には、ソフトウェアに不具合があった場合の修正に限られていた。しかし、自動車をとりまく環境の変化が著しい現在では、必要な機能をすべて開発してから自動車を出荷するという考え方では、商品性が低いものになってしまう。そこで、スマートフォンのように、自動車を出荷した後に新たなソフトウェアをインストールして機能を上げていくことが重要になってきている。また、サイバーセキュリティの面からも、脆弱性が発見された場合に迅速に修正するために、遠隔でのソフトウェアアップデートが必須と考えられる。もちろん、ソフトウェアアップデートの仕組みを用いてマルウェアが送り込まれる可能性は否定できず、諸刃の剣であることは言うまでもない。

これら3つのことから、自動車における情報システムやソフトウェアの重要性が高まっているということが言える。たとえば、フォルクスワーゲンは、ソフトウェア会社になるというメッセージを出している。また、Software-Defined Vehicle という用語が出てきたことも、このことを典型的に表している。

これらの変化から、車載組込みシステムに使われる要素技術にも、次のような変化が起きつつある。



まず、プロセッサについては、従来の車載制御システム向けのマイコンよりもはるかに高性能なものが適用されようとしている。それらの多くは、元々はモバイル機器やカーナビなどの情報処理システム向けに開発されたものである。

OSを含むソフトウェアプラットフォーム (SPF) については、車載制御システム向けには、AUTOSAR 仕様に準拠したものが広く使われつつある。従来の AUTOSAR 仕様 (AUTOSAR Classic Platform と呼ばれることになった) は、制御システム向けには適したものであるが、情報処理システム向けには要件が合致しない面があるため、新たに AUTOSAR Adaptive Platform と呼ばれる仕様の検討・開発が進んでいる。AUTOSAR Adaptive Platform では、OS には POSIX 準拠のものを使用している。

車載ネットワークについては、従来は CAN (Controller Area Network) や LIN (Local Interconnect Network) が広く使われてきたが、大容量のデータ転送が必要なところには、MOST (Media Oriented Systems Transport) に加えて、Ethernet を車載システムの要件に合致するように修正し、適用されようとしている。車載システム向けに Ethernet を修正した規格を、車載 Ethernet と総称している。

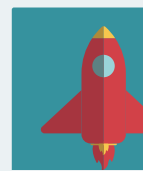
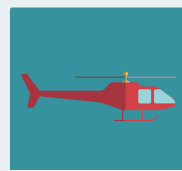
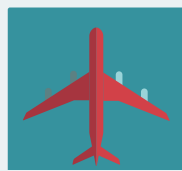
いずれの要素技術についても、IT 分野の技術が、必要な修正を加えつつ、車載組込みシステムに適用されようとしていると言えることができる。ただし、いずれにおいても、従来の車載組込みシステム向けの技術が使われなくなるというわけではない。

CONNECTED

近年、車両へさまざまなサービスを提供するために、インターネットにつながったり、高度道路交通システム (Intelligent Transport Systems, ITS) を活用することにより道路利用者の安全性の向上と環境負荷を減らすことを目的としたコネクテッドカーと呼ばれる車両が販売されている。コネクテッドサー

ビスの実用例としては eCall が挙げられる。eCall は 2018 年より欧州で搭載が義務付けられた自動緊急通報システムのことであり、車両に搭載される GPS 座標を含む緊急通報を自動で発信することにより実現される。事故後に人が通報できない場合や通報の遅延による事故被害の拡大を防ぐことが期待されており、欧州だけでも毎年数千人の命が救われ、重傷者の数も低減できると試算されている。現在では、eCall の仕組みを利用して、車両の健全性を遠隔から監視する取り組みが欧州の車両メーカーを中心に行われており、車両を車両外にある遠隔地のオペレーションセンターから監視する仕組みが整いつつある。

協調型 ITS (Cooperative ITS, C-ITS) は、車車間通信 (V2V) および路車間通信 (V2I) における無線通信をベースとする技術である。C-ITS アプリケーションは、道路上の警告や交通情報を運転手に提供し、その後で自律的に自動車を制御することを目的とする ITS アプリケーションである。より具体的な例として、車両同士が通信することにより、隊列走行や高速道路での合流調停を行う。C-ITS アプリケーションの効果として、交通流の効率化が期待されている。さらには、物流トラックや長距離バス等を隊列走行させることにより運転者に対する運転負荷を低減するなどの効果が期待されている。C-ITS には多くの利便性がある一方で、関連する無線通信に対してセキュリティとプライバシーを担保しなければ、普及が危ぶまれる可能性があることが指摘されている。たとえば、救急車や警察車両のような緊急車両になりすまして他車両の走行を妨害できてしまうと、道路の利用効率が高減する可能性がある。このため、V2X 通信では送信されたメッセージの正当性を各車両で判断することが要求される。V2X 通信を保護するためには暗号技術が必須であり、車両や路側機などの ITS ステーションの証明書の管理のために公開鍵基盤を利用することが想定されている。このような技術によって、機密性や完全性の保証、なりすまし防止、否認防止を実現



することが想定されている。

V2X 通信の代表的な公開鍵基盤には、米国運輸省 (U.S. Department of Transportation, USDOT) の SCMS (Security Credential Management System) と、欧州標準化委員会 (Comité Européen de Normalisation, CEN) の後ろ盾の基で、ETSI (European Telecommunications Standards Institute) が開発している C-ITS Trust Model の2つがある。これら2つの規格には、V2X 通信の信頼の起点となる証明書の発行の仕組みや失効手順等に違いがある。このため、2つの規格の Harmonization (調和) が検討されている。

もう1つの考慮すべき重要な問題は、ユーザのプライバシーである。自動車の場合、車両の位置情報を長期に渡り追跡されることにより、運転手や乗員のプライバシーが漏洩するという課題がある。このため、車両の位置情報を追跡できないように匿名化された識別子を割り当てることにより、長期にわたる追跡から保護することが検討されている。

また、C2C-CC (CAR 2 CAR Communication Consortium) では、TAL (Trust Assurance Level) と呼ばれる ITS ステーションの信頼性レベルを定義しており、V2X 通信を通じて他車両に影響を与えることができるのは、高い信頼性レベルで開発された車両であることが規定されている。

AUTONOMOUS

自動運転に関するセーフティとセキュリティについては、自動運転車が搭載するシステムの自動運転レベル (安全に関する責任の範囲)、サービス (車両の利用形態)、想定運行範囲、外部との連携範囲、システムのアーキテクチャ (構造) などが多種多様であることから、一般的に議論するのは難しい。国際的な議論の場である自動車基準調和世界フォーラム (WP29) での議論²⁾や、国内でのガイドライン³⁾でも、自動運転のセーフティやセキュリティの重要性は明記されているものの、具体的な方法論や対策につい

ては、現在進められている国際規格や標準での議論に委ねられている。

車両に搭載される自動運転システムは、主に、センサによって周辺環境や自車両位置を認知する機能、自車両位置から目標位置への運行、軌道を計画する判断機能、アクチュエータの制御機能の3機能で構成される。認知機能と判断機能は、従来はドライバーが担ってきたが、自動運転レベル1~2ではそれらの一部が、3~5では、条件や制限が存在する場合もあるが、全機能がシステムによって実現される。自動運転レベル3以上になると、システムによって予見できないしは回避可能な人身事故が発生してはならないという方針が検討されている^{2), 3)}。セキュリティの観点では、自動運転システムによる予見 (認知機能と判断機能) と回避 (判断機能と制御機能) に影響する攻撃に対しては、セーフティを確保する上で特に対策が必要と考えられる。

認知機能は、センサが認識した情報を統合して、自車両の周辺状況や自車両位置を認知し、判断機能が利用する情報を集約する。特に、センサが認識した情報や、地図情報などの完全性と可用性が重要となる (個人情報やプライバシーの観点では機密性も必要になってくる)。センサ類は、GNSS (Global Navigation Satellite System), IMU (Inertial Measurement Unit), Lidar (Light Detection and Ranging), 単眼/複眼カメラなど多様であるが、基本的には、物理現象をアナログ信号として捉え、それをデジタル信号に変換してコンピュータで扱えるようにする装置である。

センサに対するセキュリティの脅威について、近年数多くの研究論文が発表されている。センサに対して妨害信号を送信することで、システムが誤認識するような攻撃や、カメラによる画像に対して、ディープラーニングを含む機械学習による物体認識機能の性能限界をつく攻撃が報告されている。単一のセンサに対する攻撃は、確かに脅威であるが、安全性にどう影響するかは、自動運転システムの構成、制御アルゴリズムなど、内部構造に大きく依存する。現



在検討されている自動運転システムには、複数種類のセンサを組み合わせる状況や物体認識する技術（センサフュージョンと呼ばれる）を導入しているものが多い。センサフュージョンにおいて、不確実性のある情報、もしくは意図的に改ざんされた情報が含まれることを想定して対応できれば、センサ単体に対する攻撃の影響は限定的であろう。しかし、たとえば、地図情報や時刻情報などは、完全性や可用性が失われると、判断機能や制御機能に直接的に影響を及ぼす可能性が高い。

このように、自動運転では、従来の自動車と比べて、制御に悪影響を及ぼし得る攻撃の経路、境界（アタックサーフェス）が急激に増加する。安全分析やセキュリティ脅威分析によって、単一の故障もしくは攻撃によって安全に影響を及ぼし得るポイントを列挙して対策することが非常に重要となる。車両だけでなく、自動運転に関係する周辺装置である、クラウドサーバ、インフラセンサの機能が安全性に影響を及ぼすアーキテクチャも考え得る。たとえば、クラウド上の地図データ、OTAによる更新用制御プログラム、道路信号情報などが侵害された場合に、安全性への影響が懸念される。車両だけでなく、サービスレベルから俯瞰し、包括的に対策する視点が必要となる。

SHARED AND SERVICES

それぞれの人が1台の自動車を所有し、自動車のみに最短経路で移動しようとする考え方から、複数の利用者によって自動車を共有することで社会や地域において最適な移動手段を実現しよう（もちろん、個人レベルでも自動車保有コストを下げられる場合もある）とする新しい考え方が登場している。具体的なサービスとしては、フィンランド発のWhim、スウェーデン発のUbiGO、米国ロサンゼルス発のGoLAなどがある。この変化をセーフティとセキュリティの観点で考えると、個人最適化から、個人レベルのセキュリティを確保しながら社会最適化への

移行であると捉えることができる。

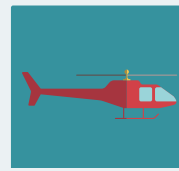
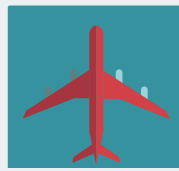
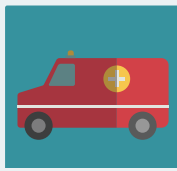
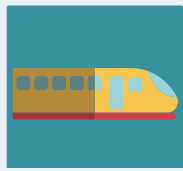
1台のモビリティが不特定多数の利用者によって共同利用されるようになると、内在する資産が侵害される可能性を考える必要が出てくる。

ここでは、自動車に限定して考えてみたい。自動車を専有する場合には、鍵によって利用者を制限できているので、車内の空間は信頼できる空間であるという前提を置くことができた。もちろん、車上荒らしやキーの電波を不正に増幅させるリレー攻撃などの不正行為が実際に発生しているので、物理的なセキュリティに対する考慮は必要である。

シェアリングサービスは、時分割によって車内が共有されるということなので、自身が利用する時間の前後は車内が信頼できない空間となる。車内に置かれた物理的なモノだけでなく、たとえば、料金の支払いに関する情報、ETCカード情報、カーナビに登録した走行データや検索履歴、外部サービスの利用履歴、ドライブレコーダに記録された車内外の動画、音声といった個人情報、プライベート情報などの情報資産が侵害される可能性が出てくる。したがって、これらを守るためには、利用者が切り替わるタイミングで、車内の状況（設備や搭載機器などの物理的なものも含む）や情報を利用前の状態に戻しておくのが基本的な考え方である。情報に関しては、利用者の情報を消去するのではなく、保護・管理できる仕組みを構築することで利便性とセキュリティを確保できる可能性もある。たとえば、ネットワーク網を活用して、クラウドやスマートフォンと連携することで、利用者に関する情報を、利用の前後で自動的に保存、復帰することも可能であろう。いずれにしても、シェアリングサービスでは、利用者の登録と認証が厳格になされ、利用者の真正性や否認防止といった性質の保証が特に重要となってくる。

ELECTRIC

近年、さまざまな自動車メーカーからさまざまな電



気自動車 (Electric Vehicle, EV) や PHEV (Plug-in Hybrid EV) が販売されている。EV の普及のためには、充電システムやその通信方式の国際標準化が必須である。国や地域で電力の供給方式に違いが存在するものの、共通する充電コネクタや通信プロトコル等を定義することにより EV の車両側に搭載する充電制御システムの共通化を実現することが目されている。

充電通信規格に関する国際標準規格として、欧州や北米の自動車メーカーを中心に、ISO/IEC 15118 が策定されている。ISO/IEC 15118 の規格名は「Vehicle to Grid - Communication Interface」である。ISO/IEC 15118 では、車両と充電ステーションの間の通信から、EV を V2G (Vehicle 2 Grid) と呼ばれる電力網に接続することまでを想定している。この充電通信規格では、EV が供給された電力量に対する料金を支払ったり、V2G に接続する EV が他車両に電力を融通する代わりに売電分の金銭を受け取ることが想定されている。このため、従来の車両とは異なり、充電スタンドになりすまし EV 車両から金銭を搾取したり、充電量をごまかして充電料金を踏み倒す等の新たな脅威にさらされる可能性がある。さらには、充電に関する使用履歴が漏洩するとプライバシーの問題につながるなどの懸念がある。

一方で、EV 車両だけでは対策ができないため、充電スタンドなどの機器に対してもセキュリティ強化が要求されている。このため、ISO/IEC 15118 では、必要なレベルの機密性を定義し、交換されるデータの整合性と信頼性の両方を検証するためのアルゴリズムを定義している。さらに、データの整合性と信頼性や否認防止を検証するために、秘密鍵と公開鍵で構成される鍵ペアを使用し、機器認証を実施した上で暗号通信が行われることが想定されている。

今後の展望

CASE 革命の到来とともに、自動車関連企業に

っては、自動車市場の競争が激化しており、新たな機能、サービスを先行して市場に投入するスピード感と柔軟性も必要となっている。その一方で、自動車のセキュリティに関する取り組みの重要性が増している。自動車に適した開発プロセスだけでなく、運用・保守を含むライフサイクル全体の業界標準、セキュリティ対策技術などの整備が急がれる。

自動運転や V2X の普及に向けて、自動車が IoT 化している。IoT ではサービス全体の一部として車両を捉えるので、車両単体でのセーフティやセキュリティを議論するだけでは、利用者や歩行者等の安心を実現することはできない。サービスレベルもしくは社会レベルで自動車と向き合い、どのようなサービスを受容するのか、しないのかを社会全体で議論することが重要である。自動車を活用した新たなサービスを長期的に運用することは、複雑な社会技術システムを運用することにほかならない。開発段階では想定できなかったセーフティおよびセキュリティに関するリスクが将来見つかることを想定し、サービスのライフサイクルを管理する仕組みを構築した上で、そのディペンダビリティやレジリエンス性を社会全体で継続的に議論し、評価すべきである。

参考文献

- 1) 松原 豊, 倉地 亮, 高田広章: 自動車分野のセーフティとセキュリティの動向と展望, 情報処理, Vol.58, No.11 (Nov. 2017).
- 2) Framework document on automated/autonomous vehicles, WP.29-177-19 (2019).
- 3) 国土交通省自動車局: 自動運転車の安全技術ガイドライン (2018).

(2019 年 10 月 30 日受付)

松原 豊 (正会員) yutaka@ertl.jp

名古屋大学大学院情報学研究科准教授。リアルタイム OS, ネットワーク技術, 安全技術, セキュリティ等の研究に従事。博士 (情報科学)。

倉地 亮 (正会員) kurachi@ncs.i.nagoya-u.ac.jp

名古屋大学大学院情報学研究科附属組込みシステム研究センター特任准教授。リアルタイムスケジューリング理論, 車載制御システムの設計技術等の研究に従事。博士 (情報科学)。

高田広章 (正会員) hiro@ertl.jp

名古屋大学未来社会創造機構教授。同大学院情報学研究科教授・附属組込みシステム研究センター長を兼務。APTJ (株) 代表取締役会長兼 CTO。リアルタイム OS, リアルタイムスケジューリング理論, 組込みシステム開発技術等の研究に従事。博士 (理学)。



[新たなモビリティ時代のサイバーセキュリティ・セキュリティによるジャパン・ブランドの向上に向けて]

③ 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ



川崎邦弘 | 鉄道総合技術研究所 祇園昭宏 | 鉄道総合技術研究所

鉄道と情報ネットワーク

鉄道における情報伝送の始まりと発展

鉄道における通信は、より安全・正確・快適な鉄道運行を実現するために、さまざまな情報を収集・伝達する重要な役割を果たしている。列車を安全に走らせるためには、線路や車両、給電などの設備の状態情報と、列車の走行・停止を指示するための制御情報を伝える必要がある。鉄道システムの中で情報をやりとりする箇所は、列車の定時運行を管理・制御する指令を中心として、駅、列車とその乗務員、そして列車を走行させるために必要となる各種の設備（構造物、軌道、給変電、防災、信号保安）など多岐に渡っており、鉄道の情報ネットワークは、これらの鉄道の構成要素間を有機的に結合する神経網である（図-1）。

我が国の鉄道における通信の歴史は、1872年に新橋～横浜間において初めて鉄道が開業した際に、3本の裸線を用いたモールス電信を使用して閉そく

運転を行ったことに始まっている。“閉そく”とは、列車同士の間隔を安全に保つために、路線をいくつか区切る考え方で、1つの区間には1列車のみが存在できることを原則とする運転方式である。鉄道通信は、列車の運転保安にかかわる情報伝送を担うために誕生した。その後、指令員や乗務員、駅員・関係箇所などへの情報伝送のための通信網の構築が進み、現在、全国を網羅する通信網や列車無線システムなど、多くの通信設備が活用されている。近年は、情報通信技術の目覚ましい発展に伴い、無線による列車制御や旅客へのブロードバンド通信サービスの提供など、より高度な情報通信技術（ICT）の活用事例が登場してきている。

情報伝送の形態も時代とともに変化してきている。通信技術が今のように発達する以前は、利用できる通信リソース（伝送速度やチャンネル数）が限られていたこともあり、少ない情報でも安全・安定輸送を実現すべく、鉄道システムを構成する各種の業務分野（運輸・営業、車両、土木、軌道、電力、信号保安、など）ごとに1対1あるいは1対nの通信システムが導入されてきた。光ネットワークやデジタル無線など通信技術が発展した現在においても踏襲されており、列車の運行にかかわる要員や設備どうしを結ぶ情報ネットワークが業務分野ごとに構成されている。近年、業務分野を超えて情報を共有できるネットワークづくりが始まっており、2020年代後半には鉄道システムを構成する要員や設備のすべてが情報ネットワークで結ばれることが期待され

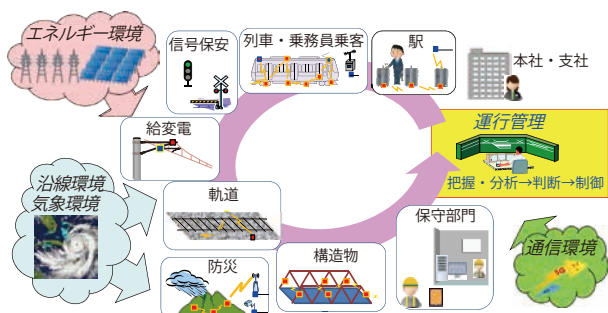
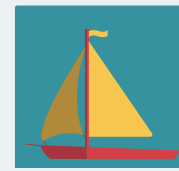
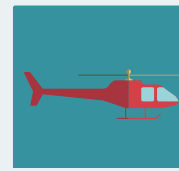
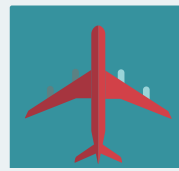
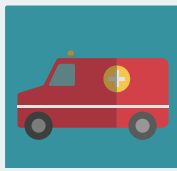
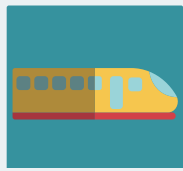


図-1 鉄道の構成要素と周囲環境とのつながり



ている (図-2)。

列車の運行制御と情報通信技術

現在の鉄道では、運行管理システムと信号保安システムの2つのシステムが列車の安全・安定運行を支えている。運行管理システムはダイヤに基づく列車の定時運行と遅延時の運転整理を担う。信号保安システムは保安制御装置等により、列車の安全確保を担っている。両システムとも、その時代の最先端の情報処理技術や通信技術を活用して列車の運行制御の高度化を進め、人間の負担を軽減することによって、より安全で安心して利用できる鉄道へと発展してきた。

1964年に開業した東海道新幹線では、先行列車との間隔などから後続列車の速度を決定・指示する地上システムと、指示速度を超過しているときには自動的にその速度以下になるようブレーキを制御する車上装置で構成される自動列車制御装置(ATC)が導入された。ATCでは、地上システムが決定した速度指示が列車に伝送され、運転台に表示される車上信号方式が用いられる(したがって地上の信号機が不要となる)。現在は、速度を滑らかに制御するために車上で速度パターンを演算するデジタル方式へと発展し、新幹線や首都圏の在来線で使用されている。

1970年代からは、コンピュータの小型化・高性

能化や、情報ネットワーク技術などの発展に伴い、運行管理や進路の設定(=線路の分岐・合流個所で線路の方向を切り換える転てつ装置の制御)の自動化が行われ、1977年には列車走行を自動で制御する自動列車運転装置(ATO)が営業線で実用化された。また、マイコンに適用するフェールセーフ技術の確立により、1985年に国内で初めてコンピュータが保安制御に適用された。最近ではデジタル移動体通信技術を活用した無線式列車制御システムが2011年に営業線に導入されるなど、安全・安心な鉄道を支えるシステムの多くが最新のICTによって実現されている。

無線式列車制御システム

列車の安全運行を支える信号保安システムにおいて、現時点において実用化されているICT活用の代表例は、無線式列車制御システムである。このシステムでは、無線通信技術とデータベース技術を活用することにより、列車の位置や速度等の情報を細かく把握しながら列車を安全に制御する。世界各国で導入が進んでおり、国内においても、JR東日本におけるATACS(Advanced Train Administration and Communications System)と呼ばれるシステムの実用化を皮切りに、複数の鉄道事業者が導入に向けて検討・開発を進めている。

無線式列車制御システムの導入のメリットは、列車位置を検知するための地上設備が削減できることと、列車上で検知した詳細な位置情報を無線で地上の制御装置に伝送・集約することによって列車どうしの間隔を安全かつ柔軟に制御できることなどが挙げられる。また、予測制御や自動運転など、より高度な列車制御システムに発展させるためのベースシステムとして活用できるというメリットもある。

無線式列車制御システムは、インターネットには接続されてはいないが、制御対象である列車と転てつ機、踏切などを“モノ”ととらえれば、広い意味ではIoTの一種と言えるだろう(図-3)。

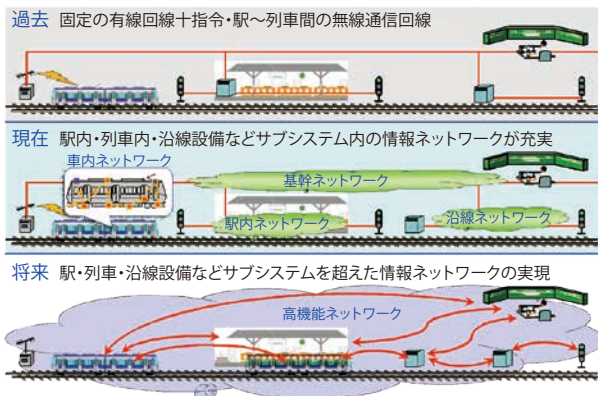


図-2 鉄道における情報ネットワークの変遷



すでに海外ではサービスが始まっている“5G”と呼ばれる第五世代の移動体通信網が2020年春から国内でも利用できるようになる予定であるが、5Gを列車の運行制御へ適用するための基礎的な検討も始まっている。5Gを活用し、鉄道システムに求められる高い安全性と信頼性が確立された暁には、無線式列車制御システムにおける制御情報も5Gネットワーク上で伝送されるようになり、巨大なIoTの一部となる可能性もある。

情報ネットワークを活用した 新しい鉄道システムの将来像

前節で述べた無線式列車制御システムでは、詳細な列車位置や速度などの情報を得ることができる。これらの詳細な制御情報を活用して、各列車の運転パターンをリアルタイムで生成することで、安全確保とダイヤ管理とを融合した新しい運行制御システムの実現が可能となった。これにより、旅客の集中や列車の遅延等の状況に応じて列車の運行を柔軟に制御でき、遅延の拡大の抑制、ダイヤ乱れの早期復旧が容易に実現可能となる。鉄道総研では、2015年度から、情報ネットワークにより運行管理と保安制御の機能を融合し、運転曲線（路線上での列車の位置と速度の関係を表す曲線。走行パターンとも呼ばれる）をリアルタイムに再計算して個々の列車や進路を制御するシステムの開発に取り組んでいる。

このシステムを実現する上で、最も重要な基盤となるのが情報ネットワークである。この情報ネット

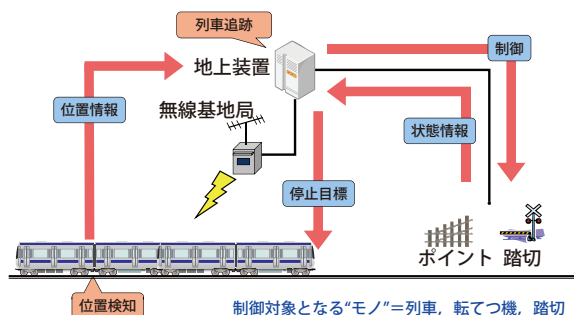


図-3 無線式列車制御システム

ワークに、列車の制御情報だけでなく、沿線のセンサや制御機器などの状態情報、改札機からの情報を載せることで、鉄道の運行状態、設備の状態、そして旅客の流れなどをすべてデータ化し、鉄道システム全体の動作状況を各業務分野の管理部門で把握するとともに、関係する部門間で共有し再利用することが可能となる。これらのデータを基にコンピュータ上のサイバー空間で現場の状態や列車の運行状態の再現・予測ができれば、設備の状態を把握して運行可否を判断するためにかかっている多くの労力と時間を大幅に削減でき、気象災害などの異常時の早期運転再開や、メンテナンスにかかる負荷の軽減が期待できる（図-4）。これは、いわば鉄道版の“サイバーフィジカルシステム”と言える。

このシステムでは、鉄道設備が自律的に不具合箇所や交換時期等の情報を発信し、列車自身が安全・安定輸送に必要なさまざまな情報を自ら取得して自律的に判断しながら走行することも可能となる。このような情報共有のためのネットワークについては、各方面で研究開発が進められており、鉄道総研でも鉄道における情報伝送の特徴や要件を踏まえたネットワークプロトコルの開発を行っている。なお、2020年度からは、上で述べた列車が自律的に走行する運行制御システムと情報通信基盤の実現に向けた研究開発もスタートさせる。

現在、MaaS（Mobility as a Service）と呼ばれる

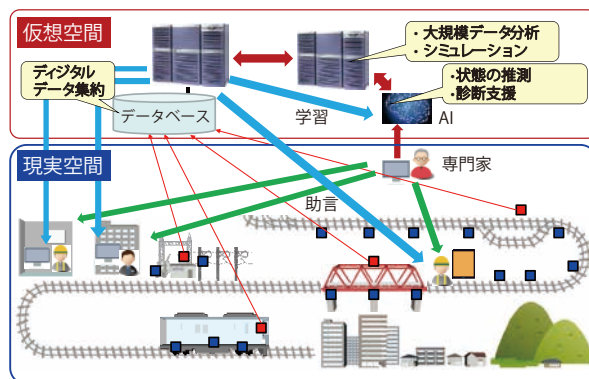
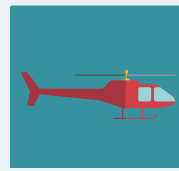
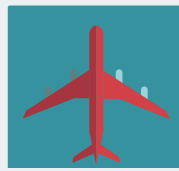
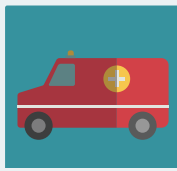
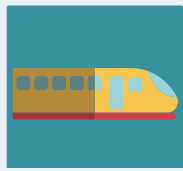


図-4 鉄道版サイバーフィジカルシステム



シームレスなモビリティサービスの実現に向けた取り組みが本格化しているが、少子高齢化が進み、自然災害が激甚化する時代の中でさらに安全でスムーズなモビリティサービスを実現するためには、図-4に示したような新しい鉄道システムへと変革していく必要があると考えている。

本節で挙げたように、列車の運行制御に情報ネットワークを活用していく上では、サイバーセキュリティへの対策が必須の課題となる。次章では、本章で述べた無線式列車制御システムを主たる対象として、情報セキュリティに関する動向と今後の課題について述べる。

鉄道の情報ネットワークと情報セキュリティ

情報セキュリティと制御システム

一般的にいう「セキュリティ」は、「安全」「防犯」「安全保障」などの意味で使用されるが、原義はラテン語の“se curitas” = “freedom from care (不安・心痛からの解放)” とのことである。セキュリティ対策を検討する際には、「何を保護すべきか」「何から保護すべきか (=脅威は何か)」「セキュリティが侵害された場合の影響はどのようなものか」の3点に対して、明確な目標を設定することが重要とされる。「情報セキュリティ」では、情報処理システムや情報通信システムなどの情報システムが扱う「情報」が外部の脅威から守るべき資産となる。情報システム (IT) におけるセキュリティと、無線式列車制御システムなどの制御システム (OT) のセキュリティとの違いは、表-1のように整理できる。

情報セキュリティの動向と鉄道

インターネットや携帯電話網等の情報ネットワークの拡大と、スマートフォンやタブレットも含む各種情報端末の爆発的な普及に伴い、サイバー攻撃による被害も急速に増えており、サイバーセキュリ

ティの確保に向けた官民学連携の活動が本格化している。かつては愉快犯的な攻撃が主であったが、近年はサイバー攻撃が“ビジネス”になっているとも言われる。企業や工場ばかりでなく、電気やガス、交通機関といった重要インフラをターゲットとするサイバー攻撃の脅威は高まっており、国内外で被害が生じた事例も報告されている。内部不正による情報漏えい、サプライチェーンリスクと呼ばれる外部委託における情報漏えいおよび不正部品・マルウェアの混入により、流出した情報が闇サイトを通じて売買され、サイバー攻撃に用いられるケースもある。このような脅威に対応するため、セキュリティ対策を後付けとせず、製品の企画・設計段階から組み込む Secure by Design という考え方が適用されつつある。

国内におけるサイバーセキュリティに関する専門機関であるIPA (独立行政法人情報処理推進機構) では、さまざまな議論・情報共有の場や機会を設け、啓蒙活動も積極的に展開している。2017年4月には、「産業サイバーセキュリティセンター」を設置し、サイバーセキュリティに関する実践的なスキルを持つ専門家を産業分野ごとに育成する事業をスタートさせた。なお、鉄道関係でも、IPAに「鉄道IT情報共有グループ」が置かれ、意見交換と情報共有が行われている。

表-1 ITとOT

	IT (Information Technology) 情報システム	OT (Operational Technology) 制御システム
保護対象	情報そのもの	制御プロセス (対象となる人やモノ)
重要視する 主な脅威	情報の漏えい 情報の改ざん	制御手順・情報の改ざん 意図的な誤制御 (なりすまし) 制御不能・制御遅延 非意図的な誤制御
維持すべき 特性	機密性、完全性	完全性、真正性 可用性、信頼性
技術的仕様	標準化された ものが多い	独自仕様が多いが、 標準仕様に準じるものや IT系と間接的に接続される ものが急速に増加



列車の運行制御システムに対する セキュリティ関連の規格と動向

列車の運行制御システムにおける保安情報の伝送においては、通信遅延、通信誤り、通信妨害などによって危険側動作とならないよう、必ず対策がとられる。鉄道システムにおいて安全にかかわる情報を伝送する通信システムに対しては、国際電気標準会議（IEC）から IEC 62280（鉄道の安全関連伝送に関する国際規格）が 2014 年 2 月に発行されており、利用する伝送システムのタイプに応じて検証すべき事項や想定すべき脅威（表-2）が定められ、脅威に対する対策の考え方が示されている（表-3）。なお、表-3 中の○は規格上で特に条件なく効果ありとされている対策、△は規格上の注記によって条件つきで効果ありとされている対策である。

また、列車制御に適用される無線通信システムに関しては、無線通信システムに対する性能要求を決定する手順が IEC/TS 62773（無線式列車制御用無

線通信システムの設計手順に関する国際的な技術仕様）として 2014 年 4 月に発行されている。この技術仕様では、環境条件、線区条件、運転条件、システム条件と無線伝送の性能要求との相関が定義されているほか、暗号化となりすましに対する対策をセキュリティに関する設計パラメータとして考慮することとしている（図-5）。

さらに、鉄道の信号通信における情報セキュリティについて、国際鉄道連合（UIC）から「鉄道におけるサイバーセキュリティのガイドライン」が 2018 年 6 月に発行された。このガイドラインは、鉄道業界がサイバー攻撃に対する脆弱性を軽減し、ライフサイクル全般にわたって鉄道システムとデータのアベイラビリティ、完全性（健全性）、機密性を確保することのサポートを目的として、鉄道信号と通信への ISO/IEC 27000 シリーズ（ISO と IEC が共同で策定している情報セキュリティマネジメントシステムに関する規格群）の適用が示されている。サイバーセキュリティリスクに対して信号システムの安全とアベイラビリティを確保する方策として、情報セキュリティ管理実践の規範である ISO/IEC 27002 をベースに鉄道向けの考え方がまとめられているほか、特にライフサイクル全般について考慮すべきセキュリティと、ソフトウェア開発におけるセキュリティ確保について述べられている。

列車の運行制御システムにおける 情報セキュリティの今後の課題

これまでの鉄道における運行制御システムは、安

表-2 IEC 62280 が定める伝送上の脅威

脅威 (Threat)	定義
重複 (Repetition)	単一のメッセージが2回以上受信される
削除 (Deletion)	メッセージがメッセージストリームから除去される
挿入 (Insertion)	メッセージストリームにメッセージが追加される
順序誤り (Resequencing)	メッセージストリーム中のメッセージの順番が変化する
破壊 (Corruption)	メッセージが改変される
遅延 (Delay)	意図した時刻より遅れた時刻にメッセージが受信される
なりすまし (Masquerade)	認証されていないメッセージ・ユーザが認証されているかのように見える

表-3 IEC 62280 に示されている対策例

脅威	対策							
	シーケンス番号	タイムスタンプ	タイムアウト	送信 ID	フィードバック	端末認証	セーフティコード	暗号化技術
重複	○	○						
削除	○							
挿入	○			△	△	△		
順序誤り	○	○						
破壊							○	○
遅延		○	○					
なりすまし					△	△		○

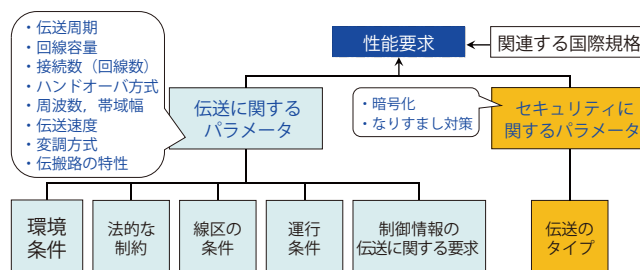
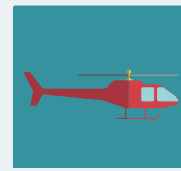
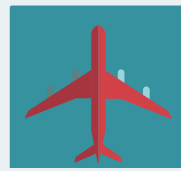
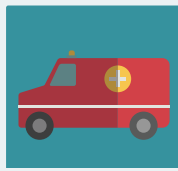
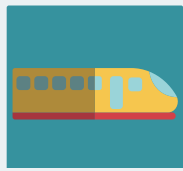


図-5 IEC/TS 62773 が規定している列車制御用無線通信システムの設計パラメータ



全確保を最優先として、独自の方式やプロトコルを採用し、クローズドなシステムとして実装、使用されてきた。

しかし、制御システムのオープン化・ネットワーク化が進み、クローズドなシステムとオープンな仕様のシステムが接続されるようになっている。鉄道の列車運行制御においても、クローズドシステムとオープンシステムとの接続はすでに始まっており、今後さらに接続される範囲や対象が広がることが予想される。従来の鉄道のシステムと、オープン仕様の世界のシステムとでは、信頼性や可用性に対する考え方が異なっており、また設備や機器の更新スピードにも大きな差異がある。両者のバランスをいかにとりながらセキュリティを確保するかが、今後の課題となろう。

また、これまでの鉄道の保安制御は、フェールセーフの考え方に基づいて構築されており、故障や異常が生じた際には列車を止める、という仕組みで事故を防いできた。今後も、進路の安全が確保できない限り列車を進行させない、という大原則は守らなければならない。しかしその一方で、情報セキュリティの観点からは、障害事象が同時多発的に起きること、またシステムの安定動作を阻害されることも想定する必要がある。サイバー攻撃によって輸送サービスが妨害される事態も考慮しなければならない。安全を最優先に確保しつつ、サービスレベルの低下を最低限にする（＝できるだけ運行し続ける）ための仕組み・対策の構築も重要な課題の1つである。

より安全でスムーズな モビリティサービスの実現に向けて

情報ネットワーク技術を始め、急速な発展を遂げているさまざまなデジタル技術は、今後鉄道を維持していくために欠かせないツールであり、またさらなる発展のための強力な武器ともなる。ただし、情報ネットワークを利用するためには、サイバーセ

キュリティに関する課題への対応が必須である。特に安全に直結する制御システムにおいては、安全を確保しつつシステムをできるだけ止めないようにするための考え方の整理と、具体的な制御手法の構築、そして実際にシステムを防護するための体制や、運用・管理の基準・ガイドライン類の整備が欠かせない。システムのネットワーク化やオープン化がさらに進むことによる侵入口の増加は不可避であり、システム全体への波及の可能性に対する考慮をしながら思いもよらぬ攻撃をいかに想定し、システムを守り、サービスレベルへの影響を最小限とするかなど、解決すべき課題は多く、また難易度も高い。鉄道の信号通信の専門家と、情報セキュリティの専門家が連携し、情報共有しながらこれらの課題に取り組まなければ、ICT活用による鉄道システムの革新は現実のものとはできないと言っても過言ではないだろう。

鉄道におけるデジタル技術の本格的な活用はまさにこれからであり、安全でスムーズなモビリティサービスが提供できる新しい鉄道の実現に向けて、鉄道事業者や先端技術を有する大学、研究機関、メーカーと連携しながら、地に足をつけた研究開発に取り組んでいきたいと考えている。

(2020年1月12日受付)

川崎邦弘 kawasaki.kunihiro.29@rtri.or.jp

1989年慶應義塾大学理工学部卒業。同年、鉄道総合技術研究所入社。現在、鉄道総合技術研究所 信号・情報技術研究部 部長。鉄道業務用無線通信システムと電磁環境に関する研究開発、国際規格審議に従事。電気学会、電子情報通信学会、IEEE 各会員。

祇園昭宏 gion.akihiro.61@rtri.or.jp

2008年神戸大学大学院自然科学研究科修了。同年、鉄道総合技術研究所入社。現在、鉄道総合技術研究所 信号・情報技術研究部 列車制御研究室 副主任研究員。列車制御システムと安全性評価手法に関する研究開発に従事。電気学会、IRSE 各会員。



[新たなモビリティ時代のサイバーセキュリティ・セキュリティによるジャパン・ブランドの向上に向けて]

④ 航空分野のサイバーセキュリティと人材育成



大久保隆夫 | 情報セキュリティ大学院大学

航空分野に潜在するリスク

2020年オリンピック・パラリンピック東京大会を直前に控え、各インフラ分野におけるサイバーセキュリティ対策が叫ばれている。外国人観光客の主要な交通手段である航空も例外ではない。海外では、2017年に米国国土安全保障省（DHS）がボーイング757型機のリモートでのハッキングに成功したと発表するなど、脅威となる事例はあるものの、自動車などの交通手段に比べ、あまり脅威が騒がれていないような印象を受ける。国内外の事例においても、インシデントの影響が大きい場合、存在はしても明らかにされていないのかもしれない。ただ、それで終わってしまっても問題の解決にはならないので、どのようなサイバー攻撃（脅威）が想定されるかを、航空システムの構造から探してみたい。

まず、どこからどこまでがサイバー攻撃なのかを明確にしておく。航空機に対する物理的攻撃、および、攻撃者が直接航空機等を操作したり、人間に働きかけての攻撃は対象としない。たとえば、ハイジャックや爆弾、ドローンを衝突させるなどの攻撃は対象外とする。また、対象とする航空分野は民間航空とし、軍用は対象外とする。そのため、自機の位置情報の漏えいは重大な脅威とはしない。本稿においては、下記に挙げるものを主たる脅威として扱う。

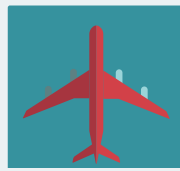
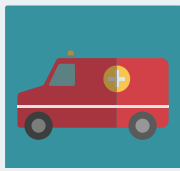
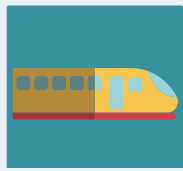
- 航空機の衝突、墜落

- 衝突や墜落を誘発する事態
- 運航に対する妨害

以上の前提の上で、航空システムのおおまかな構成と、それぞれの個所で想定される攻撃、脅威を図-1に示す。

図にはそれぞれの構成要素と、データの流れを示した。脅威は、データの流れに基づいて脅威識別する脅威分析手法「脅威モデリング手法」を用い、識別した結果を吹き出しで示している。なお、サービス妨害攻撃はほとんどの個所で想定されるため、表記を省いている。これらの脅威のリスクを評価するためには、攻撃の実際の可能性（likelihood）を判定しなければならないが、実際に内部仕様が明らかにされていない部分が多いため、リスクまでは提示していない。図から、航空機に対しては、多様な他システムからのデータ入力があり、それぞれの入力経路ごとに脅威の可能性があることが分かる。図の構成要素および脅威のそれぞれの詳細については紙数の都合上解説は割愛し、いくつかの例を挙げて解説したい。

たとえば、旅客管理システム、貨物管理システムでは、旅客および貨物の積載量、配置を計算し運航系システムを通してパイロットに送っている。パイロットはこの積載データを基に燃料計算を行い、フライトプラン（飛行計画）を立てる。このため、仮に旅客データや貨物データが改ざんされると、燃料不足やバランスなど運航に影響を及ぼす可能性が



ある。また、航空機内のシステムソフトウェアのアップデートは、整備システムを経由して行われる。そのデータはインターネットから HTTP でのダウンロードまたは USB 経由で入手する。そのため、2010 年の Stuxnet によるイラン核施設への攻撃と同様に、制御を狂わせるなどのマルウェアを混入する経路が存在することになる。

一般にサイバーセキュリティのリスクを評価する際には、被害の大きさ×攻撃可能性で計算する。しかし、航空システムの多くにおいて、これらの詳細仕様は公開されていないため、上記に挙げた脅威が実行可能かどうかは不明である。この中ではすでに対策済みのものもあるかもしれない。しかしながら、これだけのエントリポイント（攻撃者にとって入口

になり得る点）が存在することは事実である。本稿ではそれを知ってもらうため、あえてエントリポイントを列挙している。

また、図 -1 には記述していないが、空港システムも飛行機の運航と密接にかかわっているため、空港システムに対するサイバー攻撃も運航に対する脅威になり得る。たとえば、保安検査システムが攻撃を受けてダウンしたり、チェックを回避させることで、飛行機を出発できなくすることができる。これはセキュリティ事例ではないため次項には書かないが、2019 年 9 月に大阪国際空港の保安検査係員が禁止品の刃物入り手荷物を通過させたため、保安検査場の封鎖、全旅客の検査のやり直しのほか、約 30 便が欠航になるという事例があった。

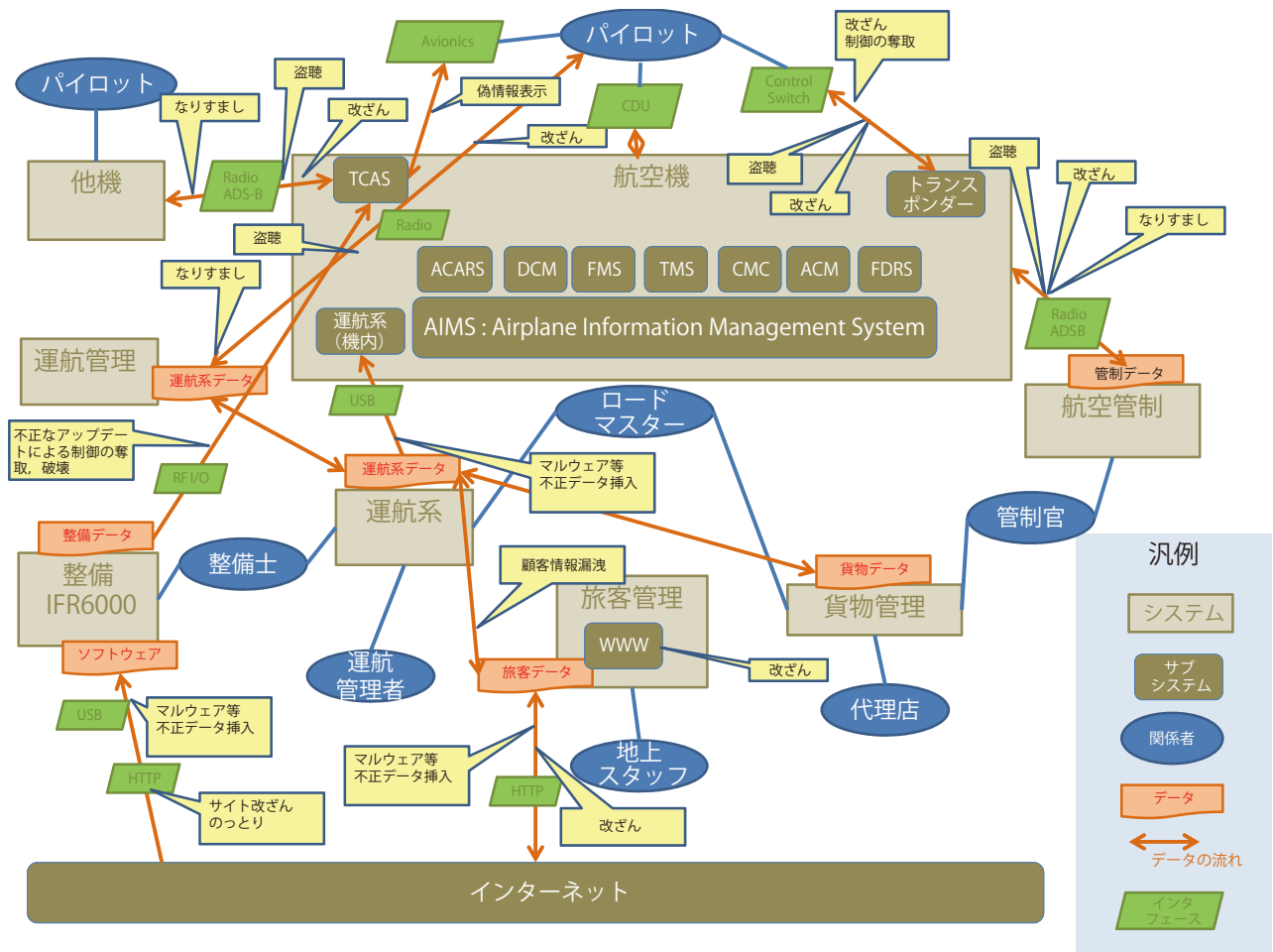


図 -1 航空システムの構成と脅威



サイバーセキュリティ脅威事例

図-1の中で、実際に脅威の可能性が指摘された例もある。航空機と他機や管制との自機情報（位置、速度、高度、方向等）の情報交換に用いられるADS-B（Automatic Dependent Surveillance -Broadcast）に脆弱性が存在することが2011年に指摘されている。ADS-Bの通信はブロードキャストでかつオープン（平文）であるため、スマートフォンで現在飛行中の飛行機を表示できるアプリが存在するほどである。しかしそのため、改ざんや偽造による脅威の可能性が指摘されている。

また、ADS-BやGPSの情報は電波で行われるため、ジャミングやGPSスプーフィングなどの電波妨害による攻撃が想定される。実際に、韓国が2013年頃から断続的にGPSへのジャミングによる攻撃を受け、航空機等の航行に影響を与えていると言われている。

電波経由では、冒頭に述べた2017年、DHSがボーイング757型機のリモートでのハッキングに成功したと発表した。ハッキングの詳細な手口は明らかにされていないが、RF（電波）経由とのみ発表されている。ボーイングはこの脆弱性は既知であり、重大なものではないと主張している。

以上が、従来想定されていた脅威であるが、近年、想定外の事例が発生している。2015年、航空機内のエンタテインメントシステムから、搭乗機の制御系をハッキングした人物がFBIに逮捕された。エンタテインメントシステムは本来、航空機の運航自体には関連がないことから、ネットワークとしては制御系と隔離されていると信じられてきた（このため、図-1にも記載していない）が、この事件により、エンタテインメントシステムから侵入される可能性が否定できなくなった。

また、運航系システムが直接攻撃された例としては、2015年のポーランド航空（LOT）の事例がある。同航空会社の運航システムが分散型サービス妨

害（DDoS）攻撃を受けた結果、ワルシャワ・ショパン空港出発便のフライトプラン作成が困難になり、搭乗客1,400人がシステム復旧まで約5時間空港に足止めされた。攻撃を受けた経路は明らかにされていないが、運航システムは外部に公開されていないため、内部システムに侵入した上で攻撃を受けたと推測される。

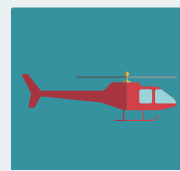
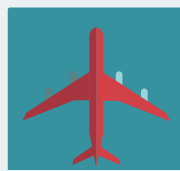
重要インフラおよび航空分野に対する人材育成

2019年10月現在、オリンピック・パラリンピック東京大会の2020年を1つのマイルストーンとして、重要インフラを対象とした人材育成プロジェクトが進められている。

戦略的イノベーション創造プログラム（SIP）／重要インフラ等におけるサイバーセキュリティの確保

2015～2019年度の内閣府が進める重要インフラのサイバーセキュリティ確保を目的とした研究開発プロジェクト（管理法人：国立研究開発法人NEDO）の中で、サイバーセキュリティ人材育成の研究開発が進められている。研究開発は、インフラ14分野のうち電力、交通（航空分野を含む）、通信、放送の4分野における、システムの運用技術（Operation Technology：OT）にかかわるもので、対象も運用従事者としている。また、SIPの目標が1,000人以上の受講であること、プロジェクト終了後も成果が継続することが必要であることから、担当する慶應義塾大学と情報セキュリティ大学院大学では、以下の3つの柱によるカリキュラム、教材開発を行った。

- 従来のIT中心にはないOT寄りの内容とする
- 事業者が組織に導入し自力で教育を行うことができるようにする
- 各分野の実例を盛り込む



上記の方針に基づき、カリキュラムおよび教材を作成し、これまでに 30 組織程度（電気、ガス、交通、放送分野）に配布を行った。また、インシデントに対し 1 次対応を行う従事者には、それがサイバーインシデントなのかどうかを判断できる基礎知識が必要になるため、サイバー攻撃が起きた際にどのような現象が表れるかを、仮想的に体験できる体験型教材の開発を行った。体験型教材はブラウザ上で実行すると、PC のデスクトップの画面が表示され、画面の指示に従いあたかも PC の画面をマウスでクリックしているかのように、操作を行い、また起きることを仮想的に体験することができる。体験型教材の画面例を図-2 に示す。

現在、コンテンツとしてランサムウェア、フィッシング、バックドア、SQL インジェクションの 4 つが開発済みである。図-2 はランサムウェアの教材の画面である。受講者は、実際にランサムウェアに感染しなくても、PC でどのような操作を行うと、マ

ルウェアに感染してしまうのかを追体験することで、脅威の仕組みや防衛策について学ぶことができる。また、Web アプリケーションのため、事前の環境の準備等は必要なく URL にアクセスすることで一度に多数の受講者が受講可能となっている。

運輸総合研究所の人材育成プロジェクト

運輸総合研究所では、日本財団助成事業として、2018 年度、2019 年度にサイバー攻撃に対する人材育成に関する調査研究を行った。この調査研究においても、2020 年東京大会を視野において、航空分野、鉄道分野それぞれを対象としたカリキュラム、教材を開発し、航空、鉄道事業者を対象としてトライアルを行った。カリキュラムの開発は下記の手順で行った。

1. 対策項目の抽出

2016 年度に運輸総合研究所が発行した航空の安全・安定輸送に資するサイバーセキュリティ



図-2 体験型教材の画面例



対策の手引き」に記載されている対策カテゴリから、システムの維持管理およびインシデント対応に必要と考えられる対策項目を抽出する。

2. タスクの抽出

i コンピテンシディクショナリ（情報処理推進機構発行）の「タスクディクショナリ」を参照し、抽出した対策項目を実践するためのタスクを抽出する。

3. 学習内容の検討

i コンピテンシディクショナリの「スキルディクショナリ」を参照し、抽出したタスクからスキルを抽出し、学習内容を整理する。

4. 机上演習の実施

学習内容の整理に必要な知見を得るため、机上演習を実施する。

5. 学習内容の決定

1. (2) および (3) で得られた知見をもとに、対象となる人材の役割を考慮した上で学習内容を決定する。

6. カリキュラムの作成

上記検討結果をもとに、カリキュラム作成を行う。

次に、カリキュラムをもとにした人材育成を実施するための教材を情報セキュリティ大学院大学監修のもとに開発し、検討委員会によるレビューを経て

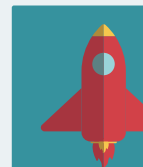
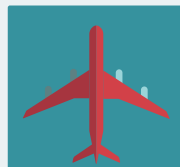
完成した。教材は各回 120 分で表-1 に示す最大全 9 回の講義を想定したものになっている。

表の項目は、航空、鉄道で共通だが、内容については航空、鉄道それぞれで異なっている部分がある。たとえば、第 1 回の「サイバー攻撃の現状」では、紹介する事例が鉄道と航空では異なっている。また、サイバー攻撃対策などでも、鉄道と航空ではその構造の相違により、紹介する内容が微妙に異なる。

この教材を、鉄道、航空分野それぞれに対し、3 日間で教育の試行を行った。航空分野の受講者は 3 名で、対象は講師予定者または教育にかかわる担当者であった。受講者に対し、受講後にアンケートを実施した。以下、航空分野についてその結果を紹介する。理解度については、全員が「大体は理解できた」「少しは理解できた」という自己評価だった。第 4 回（ネットワーク基礎）第 6 回（サイバー攻撃対策）が難易度が高いという評価だったが、第 4 回は用語が難しいという評価だった。サイバー攻撃対策には、ネットワークの知識が必須という考えから、第 4 回の講義が導入されているが、その前提となるネットワーク基礎の知識が必要との認識が浸透していないためと考えられる。一方、第 6 回では、用語以外にも考え方や理論に難しさを感じたという意見があった。これについては、対策の相関関係の把握が困難であっ

表-1 航空分野向けカリキュラム

回	種類	種類
第 1 回	サイバー攻撃の現状	サイバー攻撃により、業務にかかわるシステムの停止や誤作動が生じると、社会的混乱や人的被害をもたらす可能性があり、その対策が急務であることを認識する。
第 2 回	サイバー攻撃の手法と脆弱性	航空分野において発生する可能性のあるサイバー攻撃の手法と脆弱性を理解する。
第 3 回	サイバーセキュリティ基礎	サイバーセキュリティ対応の基礎となる考え方や手法の概要とその重要性を理解する。
第 4 回	ネットワーク基礎	サイバー攻撃の概要を把握するため、また、サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるネットワークの知識を学習する。
第 5 回	セキュリティ技術	サイバー攻撃に対処（原因究明、復旧など）する専門機関と連携し、対応（支援）するために必要となるセキュリティ技術の用語と概要を学習する。
第 6 回	サイバー攻撃対策	手引きをもとに、主なセキュリティ対策の概要を学習する。
第 7 回	サプライチェーンのセキュリティ対策	サプライチェーンのセキュリティ対策の重要性とインシデント対応に備えるための重要なポイントを学習する。
第 8 回	インシデント対応	インシデント発生の際、その原因がサイバー攻撃である疑いを考慮し、迅速かつ適切に対応（支援）するためのポイントを学習する。
第 9 回	学習の振り返り	学習の振り返りを通して本カリキュラムを総括する。



たためと考えられる。教材の量、講義時間については、カリキュラム作成後の検討委員会において委員から「セキュリティを教えるのに少なすぎるのでは?」という意見があった。確かに、セキュリティは広範囲な分野を扱う上、たとえば本学が提供している社会人向け「短期」集中コースにおいても、CSIRT (Computer Security Incident Response Team. 組織内においてインシデント対応の中核を担うチーム) やフォレンジックなど1つのテーマについてだけで3日~1週間の講義を要する。そのため、教育として十分ではないことは想定されたが、受講側の業務との関係上、3日程度の拘束が限界という意見があり、最終的にこの量となった。アンケートでは、「量が多すぎて消化しきれない」「第5, 6回は3倍程度の時間が必要」という意見があった。この点は今後改善の余地があると考えられる。

試行の最終回では前述の LOT の事例をインシデントのシナリオに挙げて、実際に起きるか、対策などについてグループディスカッションを実施した。結果、積極的な議論が行われたが、結論としては、「自社では構成が異なるためインシデントは起きないだろう」という意見にまとまった。インシデントのシナリオについては、システムや組織が各事業者によって異なるため、カスタマイズが必要になることが分かった。

鉄道、航空双方の教育を試行して得られた知見は、鉄道分野の OT 系が独立しているのに対し、航空分野の業務システムは IT 系の汎用技術を採用しているものが多いため、ある程度の IT 技術やサイバー

攻撃についての認識も高いようである。そのため、航空分野に対しては今回の教材よりもより高度なセキュリティ技術、対応方法を盛り込むのが適切と考えられる。ただし、今回参加したのは大手の航空会社であり、格安航空会社 (LCC) などの中小企業では大手ほどセキュリティ教育は十分でないことが想定される。

今後に向けて

2020 年に向けて、という目標に対しては、述べてきたように航空分野におけるセキュリティ対策および人材育成は最大限の努力がなされてきた。その成果が十分であったかは、大会の成否を待たなければならないかもしれない。が、長期的観点に立ったとき、東京大会で終わりとするのではなく、今後はその後も見据えた長期的観点による人材育成が必要になる。他分野にならい、事業者間でサイバーセキュリティの情報共有を行う交通 ISAC の取り組みも始まっていると聞く。今後はこのような組織も活用し、運用だけでなく安全なシステム構築も含めた対策・人材育成が求められると考える。

(2019 年 10 月 30 日受付)

大久保隆夫 (正会員) okubo@iisec.ac.jp

1991 年東京工業大学物理情報工学専攻修了。同年 (株) 富士通研究所入社。2006 年情報セキュリティ大学院大学博士後期課程修了。博士 (情報学)。2014 年より同学教授。専門はシステムセキュリティ、セキュリティバイデザイン。



[新たなモビリティ時代のサイバーセキュリティーセキュリティによるジャパン・ブランドの向上に向けて]

⑤ 海事産業における サイバーセキュリティ対策動向



稗方和夫 | 東京大学大学院新領域創成科学研究科

海事産業のサイバーシステム化

海事産業とは

海事産業でもサイバーセキュリティは、近年きわめて重要な課題となっている¹⁾。本稿で海事におけるサイバーセキュリティについて述べるにあたり、海事産業の基礎的構成について説明する。海事産業という言葉には統一的な定義はないが、本稿では造船業や海運業など、海に携わる産業全般を指すこととし、造船会社、海運会社、船級協会、船用機器メーカー等を中心とした関連産業で構成される。また、その任務は海上貨物輸送であるが、その大きな分類として、国際貨物輸送に用いられる外航船と、国内貨物輸送に用いられる内航船が存在する。外航船と内航船は満たすべき制約や規則が異なるが、本稿では国際輸送に用いられ、国際条約を満たす必要がある外航船を想定して海事産業、海上貨物輸送の基礎的な情報を説明する。

国際条約とIMO

外航船は国際条約に従った運航を行う義務があるが、これらの海事産業に関する国際条約は国連の下部組織であるIMO（国際海事機関）により策定される。IMOによる代表的な条約にはSOLAS条約（海上人命安全条約）やMARPOL条約（海洋汚染防止条約）などがある。IMOは国際条約により船舶が満たすべきゴールや機能要件などの基本事項について合意形成を行うものである。

船級協会

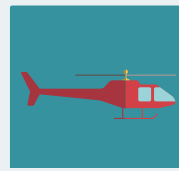
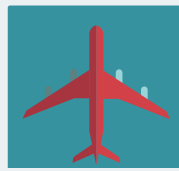
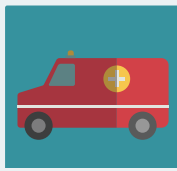
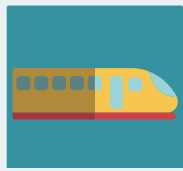
IMOにより国際条約が策定されると、船級協会

という組織がこれらの国際条約や船籍国の国内規則に基づいて船舶を検査し、認証する業務を担う。船級協会は、より具体的には、船体や機関その他の設備に関する基準を定め、基準を満たした船舶を承認している。世界の主要海運国では、中立的な立場で船舶を検査し船舶の等級付けを行うために船級協会を組織している。

歴史ある組織としては英国のロイド船級協会があり、その創設は1760年である。日本では1899年に設立された日本海事協会が、船級協会としての業務を行っている。日本海事協会は船体構造などの船舶工学に基づく安全性評価などに高い専門性を持つ組織であるが、海洋における安全を確保するための認証機関という組織が持つミッションから、サイバーセキュリティへの取り組みの基本方針や各種のガイドラインの策定と公表を積極的に行っている。船舶運航の安全確保を目的として2019年3月に発行されたガイドラインであるサイバーセキュリティマネジメントシステム（CSMS）などについては、同年12月に初の認証事例もあり、積極的にサイバーセキュリティ対策を進めている。船舶運航の安全確保という目的は変わらず、サイバーセキュリティという新しい技術分野への展開が進みつつある。

造船業と海運業

現在世界には、ばら積乾貨物船、オイルタンカー、コンテナ船、旅客船・RO-RO船等、液化ガス船、ケミカル船などの種類の船舶11万隻程度が運航されており、その需要、船腹数は毎年3%伸びている。なお、日本は世界の10%程度の船舶を運航している。海運



会社は荷主からの要求に応じて貨物輸送を行う。

造船業は海運会社や船主から要求される仕様に応じた船舶を建造し、引き渡す。船級協会からのサイバーセキュリティについての認証を取得するのは船舶のオーナーである海運会社であるため、造船所の立場としては海運会社からサイバーセキュリティに対応した船舶の要求があった際に、サイバーレジリエントな製品としての船舶を建造し、提供するという役割が期待されている。

海事産業のステークホルダの役割

海事産業において、海運会社は、IMO が策定した国際条約を船級協会などと協力して満たしながら、造船所が建造した船舶を保有あるいはチャーターして、海上貨物輸送を行っている。

サイバーセキュリティへの対策をどのように海上輸送に実装するかを検討する上では、船舶の建造している造船会社やユーザである海運会社だけでなく、IMO や各国の船級協会、船用工業またその他の業界団体の動向も重要となっている。筆者が海上貨物輸送システムを取り巻くステークホルダ間の関係を記述した図を以下の図-1 に示す。四角はステーク

ホルダで、矢印はステークホルダ間に発生している価値の流れを示している。

海事産業へのサイバーセキュリティ対策の実装では、これらのステークホルダ間の関係を考慮する必要がある。

国内の技術動向：船舶のサイバーシステム化

国土交通省の動向：IoT 活用船²⁾

近年、海上ブロードバンド通信の進展や情報通信技術を活用した船舶の運航支援技術の高度化に伴い、安全かつ効率的な運航を可能とする自動運航船の導入に向けた動きが活発化している。

日本では、2017 年 4 月の海上運送法の改正により運送サービスの質を向上させる「先進船舶」の研究開発、製造または導入を行う事業者への支援を行っている。「先進船舶」には、燃料を重油から LNG 等に切り替えた「代替燃料船」と、IoT 活用技術を導入した「IoT 活用船」がある。ここではサイバーセキュリティとの関連が深い IoT 活用船について説明する。元々船舶に搭載されている船用機器は独立に設置され、メンテナンスや運用に必要と

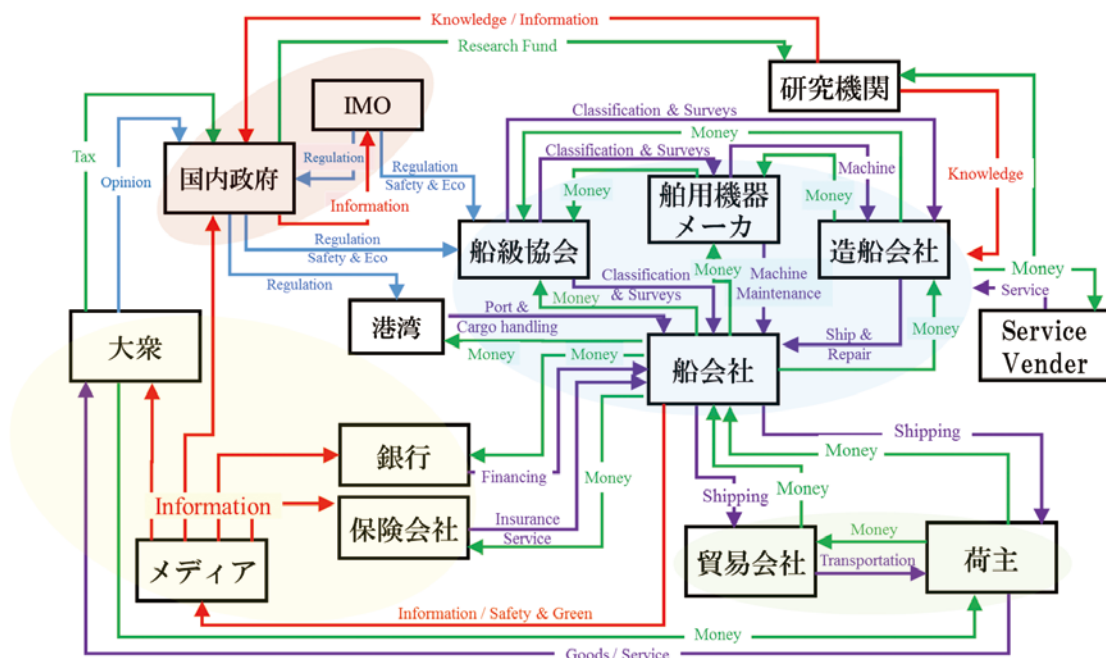


図-1 海事産業のステークホルダ間の関係



なるデータもそれぞれの機器および機器メーカーのみが利用する形式であった。また、航海中のネットワーク接続も限定的であるため、リアルタイムでデータ収集、分析、対処を行うようなことは困難であり、構想は存在しても実証等もあまり行われてこなかった。現在では、海上でのブロードバンド通信の高度化により、他産業と同様に船舶に搭載された機器類の接続やデータ共有が進んでおり、船舶のデジタルツイン開発に向けた研究開発プロジェクトなど、船舶運航の効率化、高度化がIoT活用船のコンセプトに対応する段階に到達しつつある。

自動運航船

IoT活用船に加えて、サイバーセキュリティに関連して話題に上る技術コンセプトとして、自動運航船があげられる。注目を集めている自動運航船であるが、国内外で広く共有される認識や定義はまだ固まっていない。また、自動運航は無人化を想定しているのか、無人化を進める場合にも自律運航を導入するのか、遠隔操船を前提とした運航を行うのかによって、機器類の自動化に要求される水準などは大きく異なると考えられる。一方で、現時点では自動運航がどのように実現されるかといったビジョンはまだ明確になってはいない。このように技術開発の動向としては不確実性の高い状況にあるが、船舶の見張りや機器のモニタリング、操船、機器の制御、離着舷、荷役やその他のタスクの情報技術による支援を行うための研究開発は活発に行われている。自動運航船のビジョンについての不確実性が存在するが、自動運航船とはこれらの業務について情報技術を用いた高度な支援が実現されている船舶を指す言葉と理解することがよいと考えられ、サイバーセキュリティ対策が必須となる技術開発動向である。

海事オープンプラットフォーム化³⁾

概要

現在の船上の機器は前述のように個別に情報やデータを収集・管理しており、複数の機器から得ら

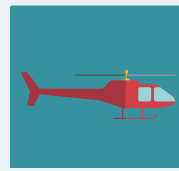
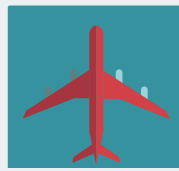
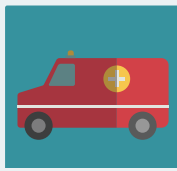
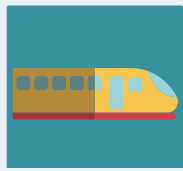
れるデータを統合することで新たな価値を生むようなアプリケーションを開発するには、実状に合わせて各機器のベンダおよび船主などにデータの開示を交渉し、データフォーマットなどの技術面の調整の両方を経る必要があった。

このような現状から、船上にデータサーバを設置し、標準化されたデータ形式やプロトコルによって各機器のデータを集中管理するという提案が海事産業内ではなされている。この船上データサーバと陸上のデータセンタにおいても標準化されたフォーマットでデータ共有し、また、データ利用の目的に応じてデータ利用の可否やアクセス権限をコントロールする仕組みも合わせて提供するという海事のオープンプラットフォームが提案され、IoS-OP (Internet of Ships Open Platform) として活動を開始している。IoS-OPにはデータ流通にかかわるルール策定、整備、データ活用の範囲や権利の検討などを行うコンソーシアムもあり、積極的なデータ活用を進めようとしている。

スマートシップに関する国際規格

オープンプラットフォーム化を進めるにあたり、海事産業では日本が主導して2つの規格を策定した。これは、ISO 19847「実海域データ共有化のための船内データサーバ—一般要件」およびISO 19848「船上機械および機器用データ標準」であり、前項のオープンプラットフォームで必要となるデータサーバおよび機器間の通信の標準化を進める上で必須の規格である。今後の船用機器の利用では、これらの規格に基づいて開発された個々の機器をデータサーバを介したシステム統合を行い、個別機器の開発は分散的でもシステム全体としての機能は統合的に提供できるような仕組みが期待できる。

一方で、データや機器間のコネクティビティがさらに高まることも考えられ、サイバーセキュリティの重要性もまたさらに高まっている。



海事産業のサイバーセキュリティ

海事サイバーセキュリティ検討プロジェクト⁴⁾ 背景

世界的な情報技術の発達に伴い、船舶、港湾、陸上施設などさまざまな海事分野においてもサイバーシステムへの接続および依存が進み、悪意ある団体や個人によるシステムデータへの不正アクセス等に起因する航行安全侵害や、経済的被害等のさまざまなリスクが懸念となっている。このため、2015年6月に開催されたIMOのMSC（海上安全委員会）95において、海事セクターのサイバーセキュリティに関する任意ガイドラインを作成することが合意された。また、米国提案に基づき、海事のサイバーリスク管理に関するMSC決議（MSC.428(98)：Maritime Cyber Risk Management in Safety Management Systems）が採択された。これにより、船主および運航者は、2021年1月1日以降の最初の適合証書（DOC）の年次検査までに国際安全管理コード（ISMコード）に基づく安全管理システムを通じてサイバーリスク管理を実施することが推奨されることとなった。

海事サイバーセキュリティ検討プロジェクトの詳細¹⁾

前述のような国際動向を反映して、日本の海事産業においても海事のサイバーセキュリティに関する審議が本格化し、サイバーセキュリティ対策に向けた検討体制の必要性が高まり、産学官公の連携で、海事分野におけるサイバーセキュリティ対策の推進を行うこととなった。日本財団の支援を受け、船舶のオーナーおよびユーザを中心とした日本船主協会、製品としての船舶を建造する造船所からなる日本造船工業会および日本中小型造船工業会、船舶に搭載される船用機器メーカーの日本船用工業会、日本の船級協会である日本海事協会、このほか大学研究機関や公的機関である東京大学、海上・港湾・航空技術研究所 海上技術安全研究所、国土交通省、情報処理推進機構、情報通信研究機構、といった横断

型の組織を日本船舶技術研究協会が取りまとめ、「我が国の実態を踏まえてIMOで行われるガイドラインの審議等に貢献すること」、「我が国の海事分野におけるサイバーセキュリティに関する現状を分析し、我が国海事業界に即したセキュリティ対策案を検討すること」の2点を目的としたプロジェクトを立ち上げた。

このプロジェクトの活動を通じて、いくつかの成果が出てきている。1つ目の成果は、IMOにおけるガイドライン策定への対応であり、ガイドライン案を米国やカナダ等と共同提案したとともに、ガイドラインの策定に貢献した。2つ目の成果は安全管理システム（SMS）マニュアルのテンプレート作成である。2021年1月1日以降の安全管理システムの適合証書の年次検査までに、サイバーセキュリティ管理を国際安全管理コードに基づく船舶安全管理システムに統合するために、検討すべき項目をまとめたテンプレートを作成した。国際安全管理コードはSOLAS条約（海上人命安全条約）の中で定められており、安全管理システムの確立などを義務付けている。従来から安全管理システムマニュアルの整備は義務付けられているが、その内容にサイバーセキュリティのリスク管理が要求され始めた。なお、このテンプレートの作成の際には、日本海事協会だけでなく海運の主要国の船級協会によるレビューも実施し、各国の意向やインプットも取り込んでいる。

国際動向

BIMCO（ボルチック国際海運協議会）

日本海運集会所のWebページ等の情報によると、BIMCO（ボルチック国際海運協議会）は1905年に発足の“The Baltic and White Sea Conference”が前身であり、船舶代理店を含むブローカーのほか、PI保険等を含む「クラブメンバ」や船級協会や海事法律事務所、損保や銀行等海運に関心のある「準メンバ」により構成されている。BIMCOは傭船の契約書書式の標準化などの事業やIMOへの働きか



けを行うほか、外航海運に関するデータや情報を発信している。

BIMCO は船内システムおよびネットワークへの無許可アクセス、または悪意ある攻撃リスク等のサイバー脅威が近年大きくなっていることを受け、これらのリスク回避、もしくは低減に向けて、2016 年 1 月にインダストリーガイドライン「THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS」を発行した。本ガイドラインは、船主および運航会社がサイバーシステムのセキュリティを維持できるように、業務評価方法および必要な手順と処置の実行方法を提示するものである。このガイドラインは、2017 年には第 2 版、2018 年に第 3 版が発行されている。第 3 版では IT（情報システム）と OT（装置のオペレーションを高度化する技術であるオペレーショナル・テクノロジー）の違いの明示や、OT へのインシデントでは物理的損傷に結び付く可能性が高いなどの船舶固有の特性に配慮した評価項目を追加している。

国際船級協会連合（IACS）

各国の船級協会の連合体である IACS では、サイバーシステムパネルを設置して IT/OT システムへの技術的なアプローチにより 12 のレコメンデーションを策定した。

米国沿岸警備隊（USCG）と米国船級協会（ABS）

船舶は船籍を持つ国における安全管理システムの審査や、寄航国における検査を受ける必要がある。どの水準のサイバーセキュリティ対策を行うかという観点から、サイバーセキュリティ対策への要求が高いと考えられる米国沿岸警備隊（USCG）がどういったレベルの対策を求めるかを理解することは重要である。USCG と密に連携して活動していると考えられる米国船級協会（ABS）では、サイバーセキュリティに関するリスクを緩和することを目的としたプログラムが存在し、積極的にサイバーセキュリティの認証を行っている。

今後の取り組み

国際動向のまとめ

IMO は、安全管理システムマニュアルの中でサイバーリスクを扱うことを推奨しており、2021 年 1 月以降は対応が進むと考えられる。このほか、BIMCO による業界主導のガイドラインの改版や、各国の船級協会によるサイバーセキュリティマネジメント認証も活発に行われている。

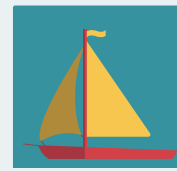
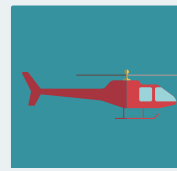
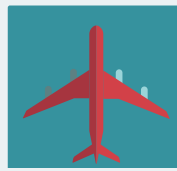
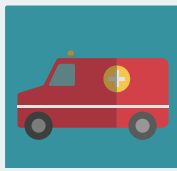
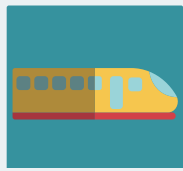
船舶におけるサイバーセキュリティへの取り組み

船舶のサイバーセキュリティ対策を考えるにあたって、大きく分けるとマネジメント的なアプローチと、IT/OT システムへの技術的なアプローチの 2 つがあると多くの組織で考えられている^{5), 6)}。

マネジメント的なアプローチとしては、サイバーリスクマネジメント、教育や訓練、ISO 27001（情報セキュリティマネジメントシステム）などによるサイバーセキュリティ対策が想定されている。つまり、組織体としてのサイバーセキュリティへの耐性に取り組むものである。

このアプローチに対して、ソフトウェアアップデート、ネットワークセキュリティ、通信およびインタフェースなどの IT/OT システムへの技術的なアプローチも存在する。こちらは製品としての船舶や船用機器のサイバーセキュリティへの耐性に取り組むものである。

この 2 つのアプローチに加えて、耐用年数が 15 年から 20 年にわたるといふ船舶の特徴もあり、マネジメント的なアプローチが必要となるのは運航船のサイバーリスクマネジメントであり、新たに建造する船舶に対してサイバーレジリエントな製品としてシステムインテグレートするというアプローチが有効であろうという共通認識が海事業界内で得られている。関連団体や各種ガイドラインと、運航船および新造船への対応状況を図-2 にまとめる。多くのインダストリーガイドラインは他産業でも参照されて



いる共通の仕様を海事業界に合わせてカスタマイズしたものであり、図-2ではその関係性を分かりやすく図示されている。

今後の海事産業においては、新造船の特に OT 要素がサイバーレジリエント（設計においてサイバーセキュリティ耐性を実現）であることを要求されることが予想され、その対応はシステムインテグレーションとしての造船所が担う範囲になると考えられる。一方で運航船および建造後の新造船については、その長い製品ライフサイクルを通じてサイバーレジリエントな状態を保ち、かつサイバーリスクマネジメントが適切になされた運用を行う必要がある。このためには船舶のオーナーや海運会社がシステムインテグレーションの役割の一環として対応し続けるべきものとする。

本稿では海事産業におけるサイバーセキュリティを取り巻く国際および国内動向についてまとめた。IT 分野で、あるいはほかの産業ドメインでサイバーセキュリティに取り組んでいらっしゃる方のお役に立つことができれば幸いである。

参考文献

- 1) 稗方和夫：海事分野におけるサイバーセキュリティ対策に関する取り組み、制御システムセキュリティカンファレンス 2019 講演資料（2019.2.15）。
- 2) 海事産業の生産性革命の深化のために推進すべき取組について～平成 28 年 6 月 3 日答申のフォローアップ～報告書、国土交通省 交通政策審議会 海事分科会 海事イノベーション部会、2018 年 6 月。
- 3) 安藤英幸：船舶デジタル化時代に向けた船舶オープンプラットフォームの役割、Sea Japan 2018 展示会 船舶海洋技術セミナー（2018.4.13）。
- 4) 稗方和夫：サイバーセキュリティ検討プロジェクトの活動、日本船舶技術研究協会 船舶基準セミナー～海事サイバーセキュリティへの対応～講演資料（2019.7.23）。
- 5) 柴田隼吾：船舶におけるサイバーセキュリティ対応の現状とこれから、Monohakobi Techno Forum 2019 講演資料（2019.11.25）。
- 6) 斎藤直樹：船舶におけるサイバーセキュリティ対策の構築へ向けた現況、2018 年度 ClassNK コンサルティングサービスセミナー（2018.11.2）。

（2020 年 1 月 15 日受付）

稗方和夫（正会員） hiekata@edu.k.u-tokyo.ac.jp

東京大学大学院工学系研究科修士修了。日本アイ・ビー・エム（株）、東京大学大学院工学系研究科助手等を経て、2010 年より大学院新領域創成科学研究科准教授。博士（工学）。2013～2014 年 MIT 客員研究員。

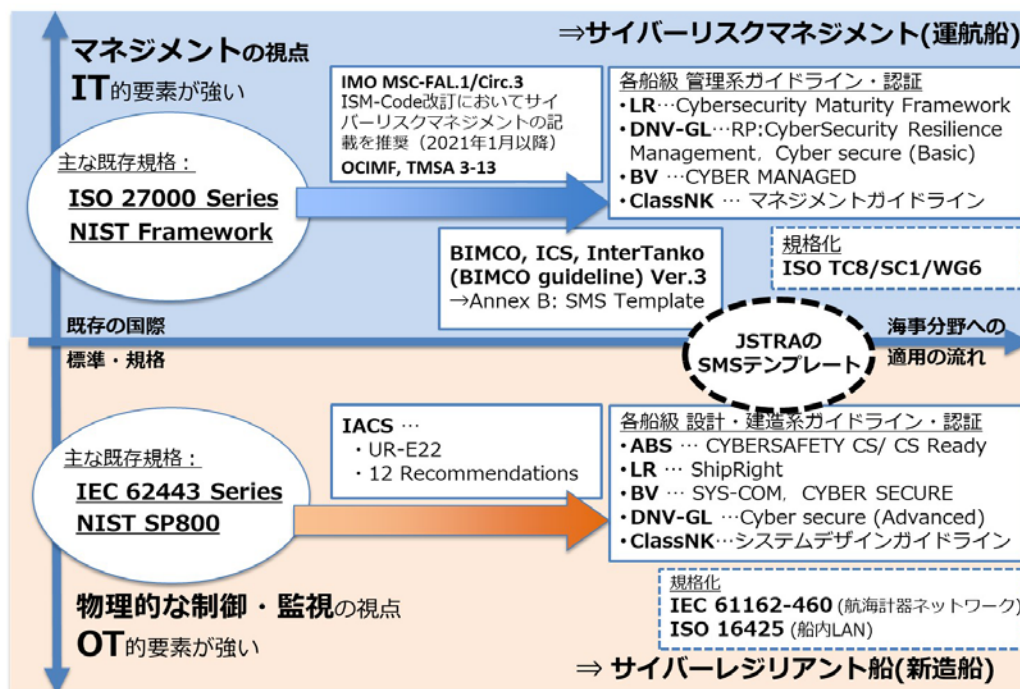


図-2 新規建造船と運航船のサイバーセキュリティ対策



「新たなモビリティ時代のサイバーセキュリティ・セキュリティによるジャパン・ブランドの向上に向けて」

⑥ ドローンのセキュリティ

応
般

春原久徳 | (一社) セキュアドローン協議会

田上利博 | (一社) セキュアドローン協議会

ドローンの現況とセキュリティ

ドローンは世界でさまざまな分野、産業用途での業務活用が進みつつある。ドローンは過去から現在まで軍事目的での開発・活用が進んできた背景があり、軍事技術の転用により安定した飛行が可能となった。また、スマートフォン技術の進歩とともにGPS（全地球測位システム）、ジャイロセンサ、気圧センサ、加速度センサ、磁気方位センサなどの各種センサが安価で利用できるようになった。ドローンはこれら技術に加え、飛行制御するためのコンパニオンコンピュータ^{☆1}、ペイロードユニットコンピュータ^{☆2}、グランドコンピュータ^{☆3}などのコアシステムによって安定的な飛行が可能となった。

各種センサや飛行制御する技術は、ドローン特有のものではない。パソコン、スマートフォン、IoT 機器などに活用されるシステムや技術と同様のものが応用されており、セキュリティリスクやサイバー攻撃のリスクはパソコン、スマートフォン、IoT 機器などと同様の課題であり、ドローンについても同様である。

ドローンを安心安全に業務活用できるようにするためには、セキュリティリスクやサイバー攻撃のリスクを理解する必要がある。本稿では、ドローンの産業用途への活用例、セキュリティリスク事例、ド

ローンのセキュリティ対策の考え方について述べる。

ドローンの産業用途への活用例

ドローンは農業、測量、橋梁検査など土木・建築分野のほか、物流などでの業務活用への期待があり、各産業用途における実証研究や実験が推進されている。今後の実用化にあたっては、さまざまなセキュリティに関するリスクや課題が想定されており、セキュリティ対策が必要である。まず、どのような分野で活用が進んでいるかを解説する。

農業

農業分野においては、農地・農作物の状態の観察と制御を緻密に管理し、農作物の収量と品質の向上を図るために、観察結果の解析を可視化し、生育計画を立てるなど、ドローンを使用したリモートセンシングにより、精密農業に活用する取り組みが行われている。また、稲作においてはドローンによる肥料散布や農薬散布に活用されている（図-1）。

測量

国土交通省では、ICT の全面的な活用（ICT 土木）

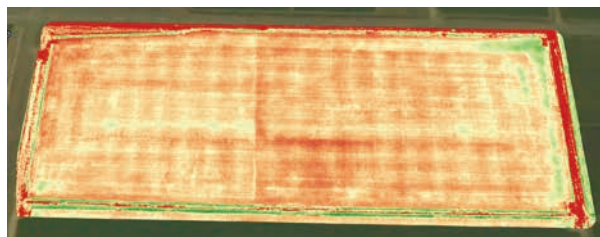
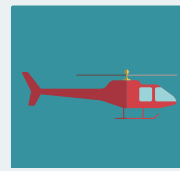
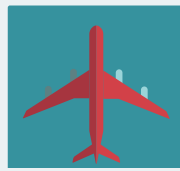
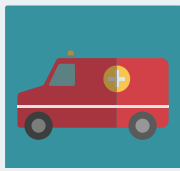
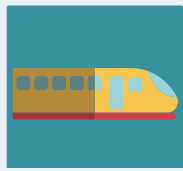


図-1 ドローンに搭載したマルチスペクトラムカメラで、稲作ほ場（田んぼ）を撮影、収集した画像を解析し生育量を可視化（出典）（一社）セキュアドローン協議会「ドローンを活用したリモートセンシング」

☆1 ドローン本体を制御する心臓部であり、姿勢制御、自動操縦を行うためのフライトコントローラ、GPS、高度等の飛行環境測定、衝突防止等を検知するための制御装置のこと。

☆2 各種センサや映像データの収集、記録、所定の位置でモノを投下するための制御等を行うシステムのこと。

☆3 プロポ（操縦用コントローラ）やトランスミッター（送信機）等の遠隔操縦装置、ドローンからフライトログを受信しバッテリー残量等、機体状態をテレメトリ（測定）するグランドコントロールステーション（ソフトウェアとパソコン）、自動航行経路を設定するためのミッションプランナ（ソフトウェアとパソコン）のこと。



などの施策を建設現場に導入することによって、測量から設計、施工、検査、維持管理に至るまでのすべてのプロセスで、建設生産システム全体の生産性向上を目指す取り組みである i-Construction（アイ・コンストラクション）を進めている（図-2）。従来の測量方法では、測量技師が測量機器を使用するため調査から結果算出までに時間を要する。また衛星や航空機などによって行われる航空写真測量の場合は費用が高額になる。これらにくらべドローンでは、航空写真測量同様に上空からドローンに搭載されたカメラによって写真測量することができ、撮影に要する費用や時間を軽減できる。写真測量による測量データから3次元データを生成でき、3次元測量点群データと設計図面との差分より施工量を自動算出することで調査時間や省力化ができる。また、3次元設計データ等により、ICT 建設機械を自動制御し、建設現場の ICT 化を実現することが i-Construction の狙いである。

橋梁および構造物検査

国土交通省は2014年7月に、トンネルや2m以上の道路橋などを、5年に1回の近接目視を基本とする点検を義務付けた省令を施行した。本改正により橋梁検査のための実証実験が数多く実施されている。

これまでの橋梁検査では、足場を組み作業員が点検作業などを行った上でメンテナンスを行ってきた。この方法では点検に時間や労力がかかり、高所など危険な場所もある。ドローンに搭載した高精度カメラで構造物の表面を近接撮影して点検する方法などにより、点検にかかる時間を削減し、高所など危険な場所の点検作業も作業員の代わりにドローンで行うことができる。近い将来にはドローンによる橋梁検査が一般的になるだろう。

また、その他構造物の検査への活用が進んでおり、2017年4月の改正FIT法（再生可能エネルギーの固定買取価格制度）により、太陽光発電設備の定期的な検査を義務化した。これまで太陽光パネルの検査は、一般的な赤外線カメラを使用して人手で撮影

3(1)①. トップランナー施策(ICTの全面的な活用(ICT土工)) 国土交通省

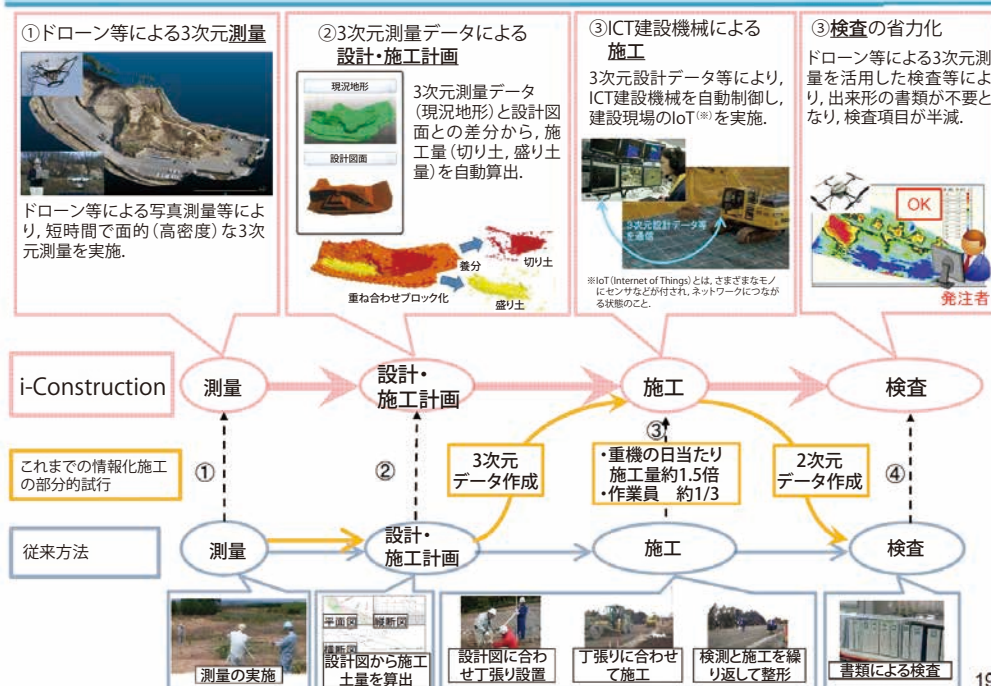


図-2 (出典) 国土交通省「i-Constructionの推進」



を行っていたが、図-3のような、省力化や検査時間、レポートの時間短縮を目的に、ドローンに搭載された赤外線カメラにより撮影した、太陽光パネルの撮影データを元に画像解析を行い、太陽光パネルの不良箇所を検出するサービスが実施されている。

そのほか、電力送電網の鉄塔、風力発電タービンなどさまざまな分野でドローンを活用した検査に活用されている。

物流

ドローン物流は、山間部や島しょ部への物資輸送、災害時の医療品の搬送などの分野での活用が期待されており、さまざまな実証実験が実施されている。

国土交通省では、離島、山間部や過疎地域などの非人口密集地域における物流の活用が見込まれている。物流の課題解決に向けドローンを活用した物流によりCO²の排出量削減効果および費用対効果などについて検証を実施している（図-4）。

（出典）国土交通省「平成30年度CO²排出量削減に資する過疎地域等における無人航空機を使用した配送実用化推進調査」

ドローンに対する規制

国土交通省は、2015年12月に無人

物流への活用例

- ① 離島や過疎地などの非人口密集地域における貨物配送
- ② 都市部における貨物配送
- ③ 災害発生時の活用
- ④ 倉庫内貨物配送



図-4（出典）国土交通省「過疎地域等におけるドローン物流活用例」

航空機（UAV）の飛行に関するルールを定めるため、改正航空法が施行された。同法改正により、遠隔操作または自動操縦により飛行させることができるもの（200g未満の重量のものは除く）で、いわゆるドローン（マルチコプタ）、ラジコン機、農業散布用ヘリコプタ等が該当する（図-5）。

飛行ルールの対象となる機体のほか、飛行の許可が必要となる空域、飛行させる場所にかかわらず、無人航空機を飛行させる場合のルールなども規定されている。同法改正前にはこのようなルールはなく自由に利用できるようになっていたが、事件、事故の発生を踏まえ、改正された背景がある。改正後の現在は、必ず国土交通省への飛行許可申請と承認が必要である。また今後は後述する米国でのルールと同様に機体の登録が義務付けとなる予定だ。

詳細については、国土交通省が公開している情報を確認することを推奨する^{☆4}。

☆4 https://www.mlit.go.jp/koku/koku_tk10_000003.html

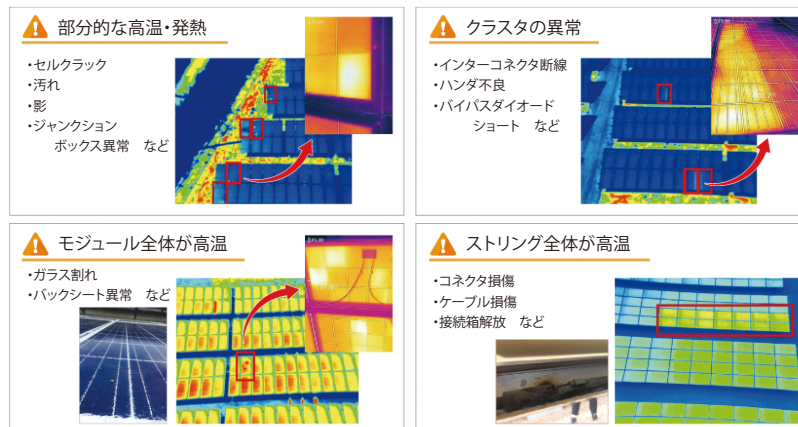
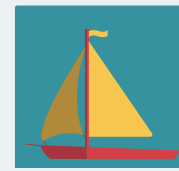
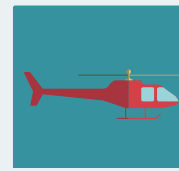
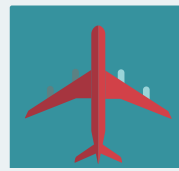
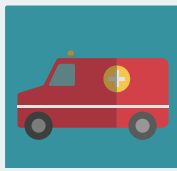
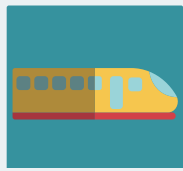


図-3（出典）エナジー・ソリューションズ（株）「ドローン&クラウドソーラーモジュールIR検査サービス」

（例）



図-5（出典）国土交通省「飛行ルールの対象となる機体」



米国連邦航空局（FAA）は、2012年に連邦航空局近代化改革法（FAA Modernization and Reform Act, FAAMRA2012）が施行された。2016年には、ドローン操縦免許を軸とするルール（Part 107ルールと呼ぶ）が施行されている。2019年には、機体の登録も義務付けとなった。

詳細については、米国連邦航空局が公開している情報を確認することを推奨する^{☆5}。

ドローンにおけるセキュリティリスク

ドローンのセキュリティリスク事例

毎年、DEF CON（ハッキング会議）が開催されているが、ここではドローンに限らず、自動走行車の社会実装に向けて、2010年頃より本格的なハッキングコンテストなどを通じて、自動車のハッキングの実際上の手法が検証されるとともに、ドローンのハッキング事例が紹介されている。

2017年のDEF CONでは、ARMベースの組込みシステムによってBluetooth経由でワイヤレスキーボードからの信号を盗聴し、ユーザIDやパスワードなどの情報を入手する技術を応用して、マイクロコンピュータをドローンのコントローラに接続して、フライトコントローラを乗っ取る事例が紹介された。その手法を応用して、ドローンでよく使われるWi-Fiなどの通信方式をハッキングすることで、操縦者になりすましてドローンを悪用する事例もあった。

また、ドローンで取得したデータを守る対策も重要だ。ドローンによる空撮やスキャンデータは、機体内部の不揮発性メモリやmicroSDカードに保存される。その段階で、ドローン本体を何者かに盗まれてしまうと、暗号化されていないデータが容易に漏洩する。

DJIのMavic 2 Enterpriseでは、写真、動画、飛

行記録といったデータをmicroSDに保存するのではなく、24ギガバイトの内蔵ストレージに保存し、ストレージを含むドローン全体をパスワードで保護できるため、そのパスワードを知っている人しか、ドローンを飛ばしたりデータにアクセスしたりできないという機能を搭載している例がある。

ドローンのリスク分析

ドローンを実証実験から社会実装に進めていく過程では、まずは実際の活用を主眼にその方法が検討されていくため、そこに悪意を持った第三者が入り込んでいくといったリスクの認識が弱い。ドローン産業自体が黎明期から普及期の途上ということもあり、これまで、悪意を持った第三者の存在によるリスクが十分に考慮されてきたとはいえない。

今後、社会実装が進んでいく中で、図-6のようなリスク状態を考慮に入れたケースに対応をしていくことが必要である。

2のドローンのトラブルは、電波、バッテリー、モーター、GPS、各種センサなどの異常で発生する。そのため、そういった異常が起きないように、二重化をしたり、異常が起きた場合のフェイルセーフへの対応をとったりしながらリスクを最小化していくことが重要だ。

しかし、3のような悪意ある第三者によるドローンの操作乗っ取りに対応しているケースは少なく、現状、比較的容易に乗っ取りが可能になってしまっている。

ドローンのリスク分析			
	ドローンの状態	人の状態	ケース
1	正しい	正規	通常の活用
2	異常	正規	ドローンのトラブル
3	正しい	悪意ある第三者	ドローンの乗っ取り
4	不正	悪意ある第三者	不正ドローンでの攻撃

図-6 ドローンのリスク分析

☆5 <https://www.faa.gov/uas/>



ドローンのリスク管理

ドローンのリスク管理は、以下の要素に分類される。

1) 法令順守（コンプライアンス）

関連する法令（航空法、道路交通法、民法などの関連法だけでなく、各業種業態に関連する法律）、また直接の法令ではないが、飛行地域の住民説明などもここに含まれる。

2) トラブルに対するフェイルセーフ

無線障害、GPS エラー、バッテリーエラーなど、ドローンを運用する際にはさまざまなトラブルが想定されるが、その際のフェイルセーフの方法、優先順位などの策定が必要である。

3) 管理者・操縦者／機体の認証

人と機体の認証で、正しい人が正しい機体に紐づけられて使用しているかということだ。たとえば、現状ではプロボ（ドローン操縦用のコントローラ）が盗まれた場合などには、その盗んだプロボでドローンが操縦できてしまう。対策としては、スマートフォンなどで使われているような指紋認証のような仕組みをプロボに搭載することなどが必要になるだろう。

4) データ保護

前述のように、取得したデータや機体のデータなどの保護が必要となる。これはPCやスマートフォンで培われてきた技術やその管理の応用となり、その技術をドローンにも適用することが必要となるだろう。

5) 悪意ある第三者による攻撃

これはドローンを始めとするヴィークル型ロボット（自動走行車なども含む）に新たに生じている脅威である。特にマルチコプタの場合は空を飛行するということもあり、墜落を生じさせることによる機体の損害だけでなく、対人・対物への損害を及ぼすリスクがある。

6) 運用

リスクを最小化するための準備、確認事項、緊急時の対応など、リスク管理のためには運

用も非常に重要な要素となるため、運用におけるルール策定が必要である。

7) 再発防止

トラブルが起こってしまった場合に、再発防止のためのステップが明確に規定されていることが重要だ。特に各種ログデータを始めとして、トラブルが起こった原因を検証することは必須である。

上記にあるようなドローンリスク管理体制を構築していくことが、ドローンサービスを提供する事業者やユーザ企業にとって重要になるが、一方で、完璧な対策を目指そうとするほど、コスト増となってしまう、ドローンを利用して解決したかった課題に対し、費用対効果が見合わなくなる。

そのため、事業者は、リスクベースド・アプローチをとり、リスクアセスメントを実施し、根拠を持った指標による優先順位付けを行った管理策を実施することが望まれる。従来の手法にあったISO/IEC 27001:2013 および ISO/IEC 27002:2013 をベースラインとし、資産のリストアップ、リスクの事前検証、リスク分析／評価を実施することなども効果がある。

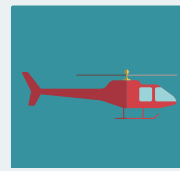
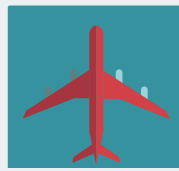
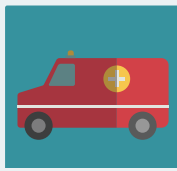
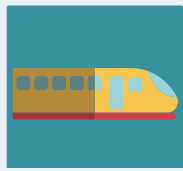
ドローンセキュリティガイド

セキュアドローン協議会では、前述の「ドローンのセキュリティリスク事例」、「ドローンのリスク管理」に対し、ドローンセキュリティガイド（第1版）を策定し、2018年3月に公開した。

産業用ドローンを安全に業務利用するためには、取得したデータの保護や安全な通信手段の確立など、各種セキュリティ対策が必要となる。

ドローン固有のセキュリティリスク

2016年7月5日にIoT推進コンソーシアム IoTセキュリティワーキンググループから「IoTセキュリティガイド」が公表された。国民が安全で安心して暮らせる社会を実現するために必要な取り組みの検



討が目的であり、ドローンセキュリティにも共通する IoT 機器特有の性質を述べている。

IoT 機器同様、ドローンにおいて対処すべきセキュリティリスクの概要は以下のとおりである。

- 1) インターネットを介して接続される IoT 機器であればサービス全体へ脅威が波及する可能性が高くなる。ドローンについても移動通信システムや Wi-Fi によりインターネットへの接続が可能であり、データ漏えいが想定される。
- 2) ドローン本体とネットワーク、双方が有する業態の環境や特性（どのくらいリスクがあるのか、また、その対策の強度をどうするか）が相互間で理解されていない状態でドローン本体がネットワークに接続することによって、標準的に必要とされるべき所要の安全や性能を満たさない可能性も想定される。
- 3) センサ等のリソースが限られたドローンでは、暗号等のセキュリティ対策を適用できない場合も想定される。一般にインターネットを経由する接続であれば通信間の暗号強度を維持することが求められる。
- 4) これまで外部につながっていなかったシステムとドローンが連携するような場合、設計時には想定されていない負荷や脅威が顕著化することもある。

ドローンは多目的に使用される機器であり、農業、配達、空撮と多彩である。それらのユースケースに応じてプラットフォームやネットワーク構成は変化し、潜在的な情報セキュリティリスクも変化すると考える。これらの潜在的な情報セキュリティリスクはユースケースを想定しながら、下記の要点に応じたりリスクの想定を行う必要がある。

- 1) 外部からの攻撃や誤動作の影響を第三者に波及させないよう、そのセキュリティリスクを最小減にするため、ドローンおよび周辺機器の守るべき機能、画像・動画等のデータ、機器認証情報等を特定する。

- 2) クローズド・ネットワークがターゲットであっても、インターネットに接続される前提でリスクを想定する。保守作業自体や保守用ツールの悪用によるリスクを想定する。
- 3) セキュリティ上の脅威や機器の故障の影響が、ほかの機器とつながることにより波及するリスクを想定する。特に、対策のレベルが低い機器やシステムがつながると、影響が波及するリスクが高まることを想定する。
- 4) 盗難や紛失した機器の不正操作、管理者のいない場所での物理的な攻撃に対するリスクや廃棄された機器の情報などの読み出しやソフトウェアの書き換え・再販売などのリスクを想定する。
- 5) パソコン等の ICT の過去事例から攻撃事例や対策事例や IoT の先行事例から攻撃事例や対策事例を想定する。

ドローンのサイバー攻撃リスク

2017 年 10 月 3 日に総務省から「IoT セキュリティ総合対策」が公表され、その中で IoT デバイスに分類される機器においては脆弱性の検査を実施することが強く推奨されている。既存の Web アプリケーションやプラットフォームだけではなく、IoT の普及により機器を繋ぐ通信経路が飛躍的に増加しており、また IoT の特性から該当の機器が物理的にオープンな環境に配置されることも想定される。機器を介した不正アクセスは依然として存在するため、セキュリティにおいて脆弱な機器を使用することはリスク要因となり得る。

ドローンにおいてもその条件は大きく変わらず、本体、送信機（専用端末、スマートフォンアプリ）などにおいて脆弱性が存在する場合にはインシデントに直結することが想定される。そのような脆弱性の有無を診断（検査）することはインシデントに対するリスクを大幅に軽減するためには有効だと考えられる。

1) 機器

ドローン本体を始めとし、スマートフォン（ア



プリを含む) や、プロポ (ドローンを操縦する際に欠かせない送信機やコントローラの意) などのコントローラを診断対象とする (図-7)。

2) 通信

機器間、またはクラウドとのデータ送受信を行うための経路が診断対象となる。

3) クラウド

バックエンドサービス (データ収集、機器管理など) が存在する場合には、それを構成する Web アプリケーションやプラットフォームに対しても診断を行うことが望ましい。

ドローンの操縦者・管理者／機体の認証

1) 操縦者・管理者の認証 (人の認証)

ドローン本体の飛行・操縦にあたっては、プロポなどを使用するが、操縦者・管理者 (人) を認証するための仕組みが存在しない。所有者や認証された人のみが使用できる仕組みを実装することにより、操縦者・管理者のなりすまし防止などの対策を行うことができる。さらに、ドローンの業務活用にあたっては、操縦者・管理者を認証する仕組みとして、スマー

トフォンや PC で実装されている ID/パスワードでの認証技術の実装に加え、より強度の高い、生体認証や電子証明書などを利用したセキュアな認証技術の実装が必要である。

2) 機体とプロポの認証

ドローン本体とプロポ間の通信は、基本的に Wi-Fi で通信されており、SSID^{☆6}とパスワードのみで接続されている。ドローン利用にあたっては、工場出荷時の SSID、パスワードが利用されているケースが多く見受けられる。これは、Wi-Fi ルータや Web カメラ、監視カメラで課題となっているケースと同様で、デフォルトの設定で利用することは、セキュリティリスクが高いと言えるため、最低限、設定を変更して使用することが望ましい。また、ドローン本体とプロポもしくは PC、スマートフォン間の通信には暗号強度の低い技術が使用されているため、セッションハイジャック (乗っ取り) の危険性がある。操縦者・管理者 (人) の認証同様、ドローン本体とプロポ間の認証には、生体認証や電子証明書などを利用したセキュアな認証技術の実装が必要である (図-8)。

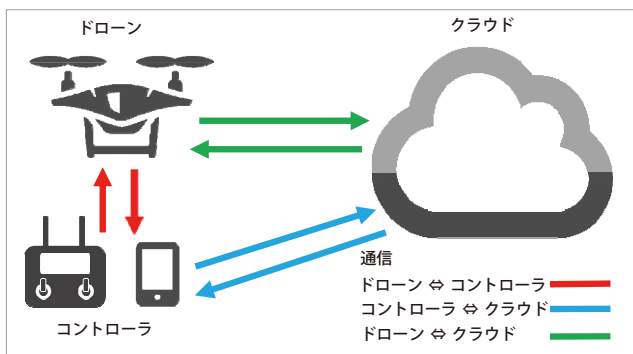


図-7 (出典) (一社) セキュアドローン協議会「ドローンセキュリティガイド」

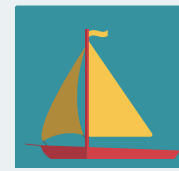
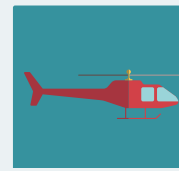
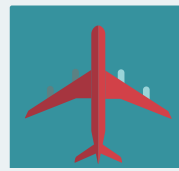
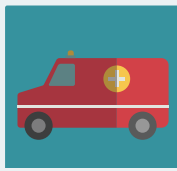
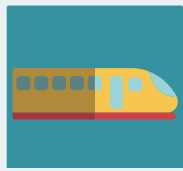


図-8 (出典) (一社) セキュアドローン協議会「ドローンセキュリティガイド」

生体認証によるドローンの飛行認証システム例

プロポで「指紋認証」を行い、操縦者が登録されているオーナーであるかを認証し、承認されるとドローンが始動できる。さらに、顔認証を組み合わせることで、操縦中のオーナーの操作権限とドローンの端末識別用の電子証明書で認証され、「誰が」「どのドローン进行操作しているか」を証明した後に、飛行を開始できる。そして飛行時には、常時顔認証が行われ、操縦者が本人であることを認証する。「いつ」「どこからどこまで」「何時から何時まで」「どこを」「どのように」飛行したのかを、GPS の位置情報やプロポの操作ログ、時刻情報などで記録する。収集され

☆6 無線 LAN (Wi-Fi) におけるアクセスポイントの識別名のこと。



たデータはSSL/TLSにより暗号化された状態でリアルタイムにクラウド上のサーバへアップし、個々の操縦者の飛行傾向や事故リスクなどの分析に役立てる。操縦者の個人情報、端末認証サービスや公開鍵基盤（PKI）にSSL/TLS^{☆7}サーバ証明書などを組み合わせて、高いレベルのセキュリティ技術で強固に保護できる（図-9）。

将来的に、産業用ドローンの飛行は人手による操縦ではなく、運航システムと連動した自動航行が中心になる。ドローンが制御信号で自律飛行をするようになると、個々のドローンの機体認証や制御信号の安全な通信が必要になる。目視外を超えて、ソフトウェアの制御によりドローンが自動航行するようになると、新たなセキュリティのリスクも発生する。この課題を解決するための取り組みとして、スマートフォンなどで利用されている通信用のSIMを使用して、4G通信回線によるリアルタイムでのドローン追跡技術の研究開発も進んでいる。無線測位システム（RPS）と呼ばれるSIM追尾システムは、レーダなどで追跡できないドローンでも、最大50mの精度で機体をリアルタイムでトレースできる。現在は、まだ研究開発と実証実験の段階だが、2020年末のSIM^{☆8}のドローン利用の規制緩和を目前に開発が進んでいる。RPSのようなドローン間の追尾

☆7 SSL (Secure Sockets Layer) と TLS (Transport Layer Security) は、いずれもインターネット上でデータを暗号化して送受信する仕組み（プロトコル）のこと。

☆8 スマートフォンや通信機器に使用される加入者を特定するID番号が記録されたICカードのこと。

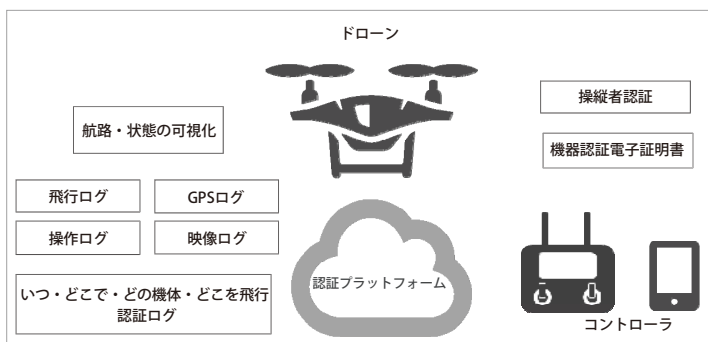


図-9 （出典）（一社）セキュアドローン協議会「ドローンセキュリティガイド」

システムとSIMや個々のドローンに埋め込まれた証明書などを活用して、自動航行における機体の認証システムも、近い将来は必要になる。

データセキュリティ

ドローン本体に搭載したカメラのデータは、SDカード等のメディアに保存される。この保存されたデータのメディアの管理・保管については注意を払う必要がある。特に測量、橋梁・構造物・太陽光パネル検査、リモートセンシングなど業務活用にあたっては、データや保存メディアの管理・保管については注意が必要である。また、クラウドサービスの利用にあたって保存、利用する際は、ID/パスワード以外のセキュアな認証技術を利用し、不正アクセス等の対策が必要である。

また、今後LTE^{☆9}や5Gを利用し、直接クラウドサービスにデータを転送することも考えられる。クラウドサービス側でドローン本体を認証するための、仕組みが確立されておらず、認証にあたっては、電子証明書などを使用したセキュアな認証技術の実装が必要である（図-10）。

悪意あるドローンに対する対策。

アンチドローン、カウンタードローン

悪意ある第三者による不正ドローンでの攻撃は、事業者側だけで対策ができず、アンチドローンやカウンタードローン（不正ドローンに対して妨害を行うシステムのこと）といった不正ドローンへの対策が必要になってくる。

☆9 スマートフォンや通信機器の通信規格のこと。

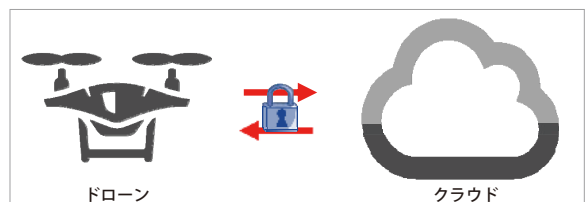


図-10 （出典）（一社）セキュアドローン協議会「ドローンセキュリティガイド」



攻撃的な悪意のあるドローンへのアプローチは主に3つある。

1. 検出・警報

空域を監視し、侵入してくるドローンの大きさの目安を読み取り、その対応の警戒レベルを発報する。特に小型で機敏なドローンに対してはその認識が難しく課題としては高く、それが可能になるかがポイントである。

2. 識別・分類

ドローンを鳥などの飛行物と区別できること。ドローンが検出されると、そのモデル名まで認識できたり、オペレータの位置も確認できる技術も出てきている。

3. 追跡・無力化

ドローンがそれ以上近づくと危険な場合、無力化の技術でドローンの接近を停止させるか物理的にドローンを妨害する、あるいはソフトウェアに干渉することで方向転換もしくは着陸させることができる。ただし、この無力化はアクティブな電波装置を使用するためにGPSなどの電波に干渉するために特別な許可が必要になるケースが多い。

上記をすべて提供していない対策システムでは、個々の対策装置を一貫した計画の中で統合する必要が生じる。現在のほとんどの対策装置はこれらの一部のみを提供している場合が多く、うまく配置・計画する必要がある。

アンチドローンの運用に関しては、攻撃から保護する区域の環境や性質、また、攻撃してくる可能性がある潜在的脅威の標的の状況に応じて、24時間365日の対策が必要になる場合もある。また、アンチドローンに関してルールや法律の整備が必要になってくるだろう。

ドローンの社会実装が進んでくる中、こういった民生用ドローンの悪意ある第三者による不正利用に関してのリスクが高まっていることは事実だ。

これまでこういった制度推進を行ってきたドローン関係者が積極的にリスクに対応し、社会実装とリ

スク低減といったバランスのとれた対策を図りつつ、法整備を進めることが必要だろう。

今後、本格的なドローンの業務活用に向けて、サービス提供事業者やユーザ企業が、実証実験などの取り組みを行っており、実用化の検討が行われている。

その際に、経済的な合理性、横展開に伴う人材確保や育成、機体の安全管理、ドローンシステム全体の安全性、リスク管理などが検討されており、実証実験と実用化には大きな課題が存在している。この課題を乗り越えてこそ、本格的な業務活用が推進されていくことだろう。

また、5G（第5世代移動通信システム）の運用開始は、SIM搭載ドローンの規制緩和とともに、今までドローンから直接クラウドに通信することができなかったという課題を解決し、ドローンの飛行情報およびドローンでの取得した画像や映像情報をインターネット経由で、遠隔地から確認することや指示を出すことが可能になり、ドローンの業務活用の範囲を大幅に高めるものである一方、セキュリティ対策を含むリスク管理はより一層重要な課題となっていくだろう。

ドローンシステムやドローンを活用する上で重要となる周辺技術が進化するにつれ、リスクも変化することは当然のことであるため、セキュリティ対策やその方法などについても見直していくことを推奨する。

(2019年10月7日受付)

春原久徳 info@secure-drone.org

(一社)セキュアドローン協議会 代表理事・会長 (Chairman, Secure Drone Consortium)。三井物産のIT系子会社で12年を経て、日本マイクロソフトで12年、PCやサーバの市場拡大に向けて、日本および外資メーカと共同で戦略的連携を担当。2015年に、ドローン・ジャパン(株)を創業。インプレス社発行『ドローンビジネス調査報告書』を2016年より毎年執筆。翔泳社発行『ドローンプログラミング』を執筆。その他多数のセミナー・執筆活動をしている。NEDO 技術委員。

田上利博 info@secure-drone.org

(一社)セキュアドローン協議会 事務局長 (Director, Secure Drone Consortium)。外資系ITセキュリティベンダなどで営業ならびにプロダクトマーケティングを担当。現在はサイバートラスト(株)において、セキュリティ・認証事業のプロダクトマーケティングを担当、IoTのセキュアな利活用に向けた各種実証研究、各種事業の展開に携わる。



第6回 GR IIIでスマートフォンとカメラの二刀流生活

◆あえてのカメラ専用機

皆さんは写真をどのように撮影しているでしょうか？ 現在、多くの方はスマートフォンの内蔵カメラを使って撮影をしていると思われます。しかし、高速なレスポンスや明るいレンズ、暗所性能等まだまだカメラ専用機（というのも不思議な言い方ですが）にも一日の長があります。一方スマートフォンが持つ便利な機能も捨てがたいです。そこで今回はスマートフォンと連携して両者の良いところ取りが可能なRICOHのGR IIIを紹介します。

◆小型かつ高性能

GR IIIはAPS-Cサイズのセンサを搭載したコンパクトデジタルカメラです。重量はスマートフォンより少し重いぐらいです。このサイズのセンサを搭載するカメラだと、一眼レフやミラーレスといった少し大きめのカメラが一般的ですが、本機はズボンのポケットに入るサイズで取り回しや持ち運びに苦労しません。USB-Cでの充電に対応しており、出張の際にも専用の充電機材が不要です。

レンズは35mm判換算で28mm相当のF2.8単焦点を搭載しており、クロップモードを利用した35mm、50mmの疑似ズームにも対応しています。ISO感度は102400まで対応しボディ内手ぶれ補正機構も備わっており、屋内の講演や暗い照明のレストラン、夜間等のスマートフォンが苦手とするシーンでも高画質な撮影が可能です。

◆スマートフォンとの親密な連携

GR IIIでは写真撮影後のワークフローも容易になっています。従来は、カメラを自宅に持ち帰りPCにデータを吸い出し現像ソフトウェアで現像し写真共有サイトにアップロードする、という流れが王道でした。しかし現在ではこれらの作業をすべてスマートフォン上で行う流れに移行しつつあります。GR IIIもこのトレンドに追随し以下の連携機能を搭載しています。

- ・画像閲覧・転送
- ・位置情報送信

画像閲覧・転送機能はスマートフォン用アプリを利用したカメラ内写真の閲覧・転送機能です。本機能にはアプリ側からカメラを起動して写真の閲覧・転送が可能という大きな特長があります。GR IIIは無線インタフェースとしてBluetooth4.2とWi-Fiの2つを搭載しています。本機能ではこれらを利用し、まずBluetooth経由でカメラのWi-Fi機能を有効にし、その後スマートフォンからWi-Fi経由で接続する、という処理を行うことでカメラ未起動状態からの自動接続を実現しています。カメラを収納したまま写真の取り込みができ、電力消費の大きいWi-Fi接続機能による電力消費も最小限に抑えられ非常に便利です。

位置情報送信機能はスマートフォン側で取得した位置情報をGR IIIに送信する機能です。写真に位置情報を付与しておくと、整理・検索時に便利ですが、現在GPSユニットを搭載するデジタルカメラは数機種しかない状況です。GR IIIはスマートフォン用アプリから位置情報を受信する仕組みを持っており、GPSユニットなしに写真への位置情報付与を実現しています。

小型で一段上の画質・品質の写真撮影でき、スマートフォンとの連携も可能な本機を使うと出張の報告資料も写真共有サイトの投稿もより洗練されたものになります。もっと良い写真を撮りたいという思いをお持ちの方におすすめできる期待を裏切らない1台です。

(2019年12月26日受付)



写真1
愛用のRICOH GR III
(撮影：今井智大)

※紹介する商品と著者に利益相反がないことを、編集部で確認しております。

高専プロコン 30 年の歩み

神沼靖子 | 情報処理学会フェロー 寺元貴幸 | 津山工業高等専門学校

高専プロコンとは

はじめに、高専プロコンとは何かについての理解を容易にするために、「高専とプロコンとその背景にある教育」に触れておこう。高専とは高等専門学校の略称であり、プロコンとはプログラミングコンテストの略称である。

近年、プログラミングコンテストはいろいろな組織で開催されている。そこで、高専のプロコンを他組織のプロコンと区別するために「高専プロコン」と呼んでいる。

高専生の育成

高専生は中学卒業後の 5 年間で技術力に重きを置く教育を受け、一般教養と技術的な専門知識を身につけてエンジニアとして育成されている。この教育は高校・短大の 5 年間に該当する期間であるが、高専の教育内容は実験や実習にかかる時間が非常に多い。応用力を身につけるための効果を重視しているからである。

また、ロボットコンテスト（ロボコン）、プログラミングコンテスト（プロコン）、デザインコンペティション（デザコン）などの全国規模の高専大会を開催して技術力を磨きあっている。これは即戦力を身につける上で効果がある。さらに高度な技術を身につけるために 2 年間の専攻科に進学するコースを選ぶこともできる。

高専プロコンのはじまり

1989 年（平成元年）に、文科省主催の生涯学習フェスティバル（まなびピア）が開催された。このニュースを知った日本パーソナルコンピュータソフトウェア協会（現・コンピュータソフトウェア協会）が高専の参加につ

いて検討を始め、まなびピアに 1 年遅れて第 1 回高専プロコンが誕生した。それは、まなびピアが幕を閉じた 2008 年まで続いた。まなびピアは、幕張メッセのイベント会場で始まり、全国を移動しながら 19 回まで毎年開催されてきた。高専プロコンはこれに便乗して 18 年間参加したのである。

まなびピアが幕を閉じたときに、高専プロコンの支援団体となる特定非営利活動法人 NAPROCK（Nourishment Association for Programming Contest Kosen）が設立された。NAPROCK の支援によって、高専プロコン大会は 2009 年から今日に至るまで継続されている。そして 2019 年に第 30 回を迎えた。

第 1 回大会は国・公・私立高専協会連絡協議会の主催で始まった。その際、高専情報処理教育研究協議会、日本パーソナルコンピュータソフトウェア協会、日本マイコンクラブ、日経新聞社などの後援を受けた。さらに情報処理系企業からの支援も受けて動き出した。

開催にあたって実行委員会が最初に手をつけたのは、大会の運用に関する諸事項を検討することであった。関係者の思いは共有され、応募方法・審査方法・表彰などに関する基本的な事柄が検討された。そして、「応募を実施する部門として、課題部門と自由部門を設ける」、「応募資格は、国・公・私立の高専に在籍する学生に限定する」、「審査は予備審査（予選）と本審査（本選）の 2 段階で実施する」、「優れた発表には、最優秀賞、優秀賞、特別賞を設けて表彰する」ことなどが決められた。

一度始めたら止められなくなる 高専プロコンの世界

やる気と脳にいい汗をかこう！ というキャッチフ

レーズで始まった第1回の高専プロコンは、毎回新しいアイデアが取り入れられて進化した。課題部門と自由部門で始まった大会に競技部門が加わったのは、第5回からであった。さらに海外の大学生（ベトナム、モンゴル、台湾、中国、タイ、マレーシアなど）の参加で、国際化も始まった。

高専プロコン進化の背景には、関係者の地道な努力がある。たとえば、審査員から厳しい質問を受けた発表者たちは、次の発表で対応しているのである。

・・・

あるとき、「プロジェクトマネジメントは重要だから、作業のスケジュールを立ててくださいネ」と審査員が漏らした言葉に反応して、スケジュールの立て方を自分たちで調べ、翌年の発表では対応していた。

・・・

審査員は、本気で向かってくる高専生の逞しい姿をそこに見た。その一方で、表彰状を手にしたときに見られる最上の笑顔にもまた心を癒されたのである。

本選では、プレゼンテーション審査とデモ審査が行われるが、その際にソフトウェアとハードウェアのメンバが連携して作業することが必要になる。このときメンバは、システムを統合することの重要性を学ぶのであった。

プロコン 30 年の足跡

高専プロコンの運営は、まなびピアとともに歩んだ19回と、NAPROCKとともに歩んだ11回の足跡から振り返ることができる。

記念すべき第1回大会の本選は1990年に京都で開催された。課題部門と自由部門の本選が1日だけで実施された。第2回大会から大分→仙台→名古屋と会場を移動し、第5回大会となる富山大会では新たに競技部門が加わっている。この3部門体制で、函館→北九州→長岡→明石→呉→鈴鹿→鶴岡→石川→東京→新居浜→米子→茨城→津山→福島へと開催地を変えながら移動して、まなびピアとともに歩んだ大会は19年

間で幕を閉じた。

まなびピアが終了したときに、高専プロコンは引き続き活動を継続する道を選んだ。それを支える組織として新たな開催母体を模索し、そこで誕生したのがNAPROCKである。そこには高専組織の強い思いがあった。

NAPROCKの設立に際して、高専は「情報産業における適切な人材育成」をモットーとした。たとえば、創造性の豊かさや技量の確かさを求める教育に注目すること、即戦力のある技術者を目指したPBL (Problem-based learning: 課題解決型学習) 型の教育を実施すること、プロコンを通して高度なエンジニア育成教育を充実すること、産学官の連携によって社会に開かれた教育を推進すること、国際化に向けた対応をすることなどがあった。

第20回大会(2009)からはNAPROCKの支援によって、木更津→高知→舞鶴→有明→旭川→一関→長野→鳥羽→大島→阿南を移動しながら、都城で第30回大会に到達したのである。

天災を乗り越えて

2011年に一関で開催予定の第22回高専プロコンは、東北地方太平洋沖地震の影響で開催場所が舞鶴へと急遽変更となった。そして3年後に第25回高専プロコンの本選があり、一関の文化センターで開催されることになった。

このときのキャッチコピーは「とどけよう、イーハトーヴの風～僕らが創る希望郷～」であった。そこには、高専生たちによる「プログラミング技術で新しい未来を切り拓き、一関に希望を与えたい」という熱き思いがあった。

切り口を変えてプロコンを視る

プロコンは生き物である。そこで異なる観点からプロコンの姿を覗いてみることにしたい。30年間にわたる大会期間中には、運営方針に係る変化、会場の

環境による変化などがあった。それらの中で注目したい事柄を抽出しておこう。

- 第3回は1992年に開催された仙台大会であったが、この回から本選の日程が2日間となった。1日目にはプレゼンを実施し、2日目にはデモを実施したのである。
- 第8回は1997年の長岡大会である。この年から協賛企業の要望で、企業からの特別審査員が加わった。この背景には、プロコンの運営資金として企業による寄付金が増大していたことがあった。
- 20年間続いたまなびピアでの開催が幕を閉じ、2009年からNAPROCKが高専プロコン大会の支援組織となって運営を継承した。そして、新たな活動に向けた検討がはじめられた。
- 2019年の都城大会の前日に台風19号が到来し、会場に到達できないチームや運営関係者が出た。結果として、競技部門の8チーム、課題部門の1チームが本選への参加を辞退することになった。

進化を続けるプロコンの審査方法

大会の中からいくつかの回を抽出して進化の様子を例示しておこう。

○第1回の事例から

第1回の予選では応募書類の審査が行われ、本選ではプレゼンテーション審査、デモンストレーション審査、およびマニュアルチェックが1日で実施された。すべての資料が、B5版(全41ページ)の冊子にまとめられて、審査員や関係者に配布された。

応募状況は、課題部門が33テーマ、自由部門が51テーマであった。厳しい予選の結果、課題部門で本選へ進んだのは6チーム、自由部門で本選へ進んだのは10チームであった。現在と違ってこの大会では、ハードウェアもかなり重視されていた。たとえば、ソフトウェアで動きを表現するのではなく、パソコンを4台繋いで映像の流れを表現するなど奇抜な発表があった。

以後も、開発者が工夫した発表があり、審査員や見学者にとっても楽しみが増えていったのである。

○第10回目の事例から

課題部門と自由部門の応募作品には、応募部門、タイトル、予定開発期間と開発人員、開発環境(開発機種、開発言語、使用OS、使用ユーティリティなど)を記述するようになった。

実行環境では使用するOS、ハードウェア構成なども明記している。さらに、機能(何ができるか、いかに演出するか、などに関して個条書きで記す)、実現方法(何を実現するかについて個条書きで記す)、独創的な部分(何が、いかにできるかの観点を個条書きで記す)、類似品との相違点(入力方法、作成方法などに関して、3点以内個条書きで記す)、対象者(利用する人)などを明記している。

また、競技部門に関する記載のポイントとして、「タイトル、予定開発期間、開発人員、実現方法(どのようなプロセスでいかに処理するのかを審査委員に分かるように具体的に述べる。たとえば流れ図をつけるなど)、使用ソフト(OS、アプリケーションなど)」が示されている。これらが以後の基本的な記載パターンとなった。

○第18回の事例から

毎年テーマが変わる競技部門では、運用方法と競技システムについて検討しなければならない。2006年まではプロコン委員だけで検討してきたが、翌年からは主幹校が対応することになった。その結果、主管校の学生や高専OBなどがシステム作成に主体的にかかわることになり、作品の幅が広がったのである。2007年に主管校となった津山高専では、専攻科の学生や地元企業の協力(図-1参照)を得て「石垣工務店(表-2参照)」のシステムを開発することになった。そして石をはめ込む石垣をイメージした「木製ピースを隙間なく埋める」というテーマで競争することにした。また、「石(ピース)はネットオークションサイトで、他チームよりも高い価格で落札しなければ使用することができない」という条件が付加された。なお、木製ピースには単位正方形を組み合わせた23種類があり、オークションの落札サイトのピース数が730個用意されている。この条件で試合を進めたのである。

開発されたシステムはその後、地域のイベントで再利

用されている。オープンキャンパスでパズルを組み立てる子どもたちの真剣な表情に注目したい(図-2)。

大会の概要と変遷

高専プロコンの大会は、課題、自由、および競技の3部門で構成されている。

このうち自由部門にはあらかじめ与えられたテーマがない。応募者が独自にアイデアをまとめて設計・開発するのである。その概要には顕著な変化は見られないが、内容は年を経るごとに進化している。

課題は運営委員会から与えられたテーマに沿ってシステムを設計・開発する部門である。テーマは表-1に示すように、2年ごとに変わっている。



図-1 地元企業との協力場面



図-2 パズルを組み立てる子どもたち

一方、競技のテーマは毎年異なる(表-2 参照)。予選でテーマを定め、本選では試合によって勝敗を決める。テーマ名を眺めると、特異な表現も散見されるが、これは誤記ではない。

表-1 課題テーマの変遷

開催国	テーマ
1～2	CAI 用のソフトウェア
3～4	人にやさしい技術
5～6	遊び心とコンピュータ
7～8	人の気持ちがわかるコンピュータ
9～10	伝統技術とコンピュータ
11～12	自然との共生
13～14	スポーツとコンピュータ
15～16	街に活着ているコンピュータ
17～18	子供心とコンピュータ
19～20	ゆとりを生み出すコンピュータ
21～22	旅とコンピュータ
23～24	ICT でサポートする明るい少子高齢化社会
25～26	防災・減災対策と復興支援
27～28	スポーツで切り拓く明るい社会
29～30	ICT を活用した地域の活性化

表-2 競技におけるテーマの変遷

開催回	テーマ
5 回	ノート PC と GPS を用いた面積測定
6 回	イメージクリップボードを用いた体積測定
7 回	鬼さんこちら ピットなるほうへ
8 回	あっちの花をピョッ！キング
9 回	ひょっこり プロコン島
10 回	ピースで peace)
11 回	みえつ かくれつ 箱はこび
12 回	孫・まご・積木のおかたづけ
13 回	以心伝心 DNA
14 回	達人に隙なし
15 回	記憶のかげら
16 回	ハートを捜せ！
17 回	片付けます
18 回	石垣工務店
19 回	フラッと収集車
20 回	何色？ さっと見 発見伝
21 回	水瓶の恵み—緑と水のネットワーク
22 回	よみがえれ、世界遺産
23 回	数えなサイー Here are Dice —
24 回	じょっぴん通信—ダイスキな人に伝えてくだサイー
25 回	キオクのかげら II
26 回	石畳職人 Z
27 回	ホントの魅力がミエますか？
28 回	おいでませ、ホントの魅力へ
29 回	与えられたルールによる対抗戦
30 回	踊って舞って回って

審査の観点

審査において全部門に共通することは「分かりやすく書く」ということである。以下では課題部門と自由部門における審査の特徴に注目する。

～課題部門と自由部門に共通する観点～

予選では、応募作品の「独創性」が最も重視される。次に有用性と実現可能性が注目される。そして「第3者が理解できるドキュメントとして明示的に表現されているか」が注目される。これらは3つの観点と呼ばれている。

「独創性」に関しては、作品のタイトル、開発する機能、作成方法などの観点が注目される。「有用性と実現可能性」に関しては、「作品の開発目標が明確に述べられているか」、「どのような技術を活用するか」、「実現方法は、倫理的に見て問題がないか」などが注目される。そして「第3者が理解できるドキュメントに関しては、「説明文は分かりやすいか」、「スライド枚数は適切であるか、上限の12枚を超えていないか」なども注目される。これらの情報は、募集要項に公開されている。

本選では「部門への適合性（必須）、独創性（重点評価）、システムの開発技術力、有用性、操作性、マニュアル作成能力、発表能力（ドキュメンテーション能力、プレゼンテーション能力）」に注目して総合的に審査される。また、プログラムのソースリスト、操作マニュアルも審査対象となっている。さらに、応募作品と類似した作品の有無などに関するWeb検索が行われる。

～課題部門に特化した審査の観点～

課題部門の予選では、応募作品の内容がテーマに相応しいかどうか重視される。特に「テーマが明示的に示されているか」が最優先事項として確認される。また、作品の質が年々向上していることから、「実現可能性」では「課題に特化した機能を完成するために必要な技術」が漏れなく説明されているかにも注目される。

～競技部門における審査の観点～

競技部門の予選では、応募用紙に書かれた実現方法とそのアイデアの面白さが注目され、実現可能性が評価される。その際、作品の独創性が最も重視され、次いで有用性と実現可能性が重視される。このとき、応募用紙の必要事項欄が満たされているかについて確認している。

競技部門の本選は対抗戦によって勝敗が決定される。図-3は競技の本選風景である（左上の競技場面とそれを応援する会場の観戦者の姿が対象的である）。

次の活動に向けて

そもそも高専プロコンの始まりは、文科省主催の生涯学習フェスティバル（まなびピア）に興味を持ったことであった。まなびピアが幕を閉じたときに、支援組織として活動を継承したNAPROCKは新たな活動を模索していた。そこで浮上した話題がプロコンの国際大会であった。

こうして海外でのイベント企画（2020年3月にベトナムで開催）の動きが始まった。会場はハノイ国家大学となり、課題部門と競技部門を実施することが決定した。そして今、NAPROCK国際プロコンベトナム大会開催の具体化が進んでいる。

過去に参加した国から、ベトナム、モンゴル、東南



図-3 競技の本選風景

アジア等に声をかける予定で準備している。日本チームは、都城大会で表彰された課題部門と競技部門から各6チームがハノイに派遣される予定である。運営方法は高専プロコンを踏襲することになっている。

参考資料など

漫画で読める高専プロコン

“GO! GO! プロコンガール”と題した、林檎子(メロコ)の漫画がNAPROCKから発刊された(図-4)。第1話から第20話までのシリーズとして描いた単行本である。

高専プロコンの公式サイトからも参照できる(<http://www.procon.gr.jp/>)。

高等専門学校 50 年の歩み

高等専門学校制度創設50周年の記念式典が2012年に開催され、『高等専門学校50年の歩み』と題した50年史の冊子が配布された。そこには、創設の経緯、高等専門学校教育における近年の動き、中央教育審議会答申、高専制度略年表など、50年間の多様な情報が155ページにわたって整理されている。また、冊子に含まれる77枚の写真集は高専生の日常を語っている。

高等専門学校は1961年(昭和36年)6月に学校教育法の一部を改正する法律が制定され、第一期校が開校した1962年(昭和37年)に遡り、2012年(平成24年)に創立50周年の節目を迎えたのであった。



図-4
プロコンガールの表紙

全国高等専門学校プログラミングコンテスト 10 周年記念誌

2000年に、『全国高等専門学校プログラミングコンテスト10周年記念誌』が発刊された。そこには、「歴代実行委員長・歴代副実行委員長・全審査委員による10年を振り返っての応援メッセージ」も掲載されている。さらに、歴代最優秀賞受賞チームによる「プロコン学生、今こう語る」、各協賛企業社長による「プロコン経験者を我が社に迎えて」、E-mail座談会「プロコンの過去、現在、未来」、トピックス「プロコンメンバ海外に飛ぶ」など、173ページに及ぶ記事は圧巻で、当時のプロコンの様子が再現されている。

週刊 BCN

タブロイド版の週刊BCN(Business Computer News)では、「千人回峰」という欄で高専プロコン関係者たちにインタビューを実施して、その記事を紹介している。

31 回大会に向けて

第30回大会は、高専プロコンの通過点である。次の31回大会(2020年10月10日～10月11日)は北海道の苫小牧市民会館で開催される。課題部門(「楽しく学びあえる!」をテーマにした作品)、自由部門(自由なテーマで独創的な作品)、競技部門(与えられたルールによる対抗戦)で実施される。さらなる発展を祈りながら、30年の歩みのまとめとする。

(2019年12月20日受付)

■神沼靖子(正会員) y-kaminuma@ac.cyberhome.ne.jp

高専との接点はプログラミングコンテストであった。第1回から第12回まで審査委員として、第13回から第30回までは審査委員長として対応した。審査でかかわったのは、課題部門と自由部門であった。

■寺元貴幸(正会員) teramoto@tsuyama-ct.ac.jp

津山工業高等専門学校総合理工学科情報システム系教授。18回大会より高専プロコンに参加し、21回から26回まで競技部門のチーフとして活動。27回から30回までは大会全体の副委員長として運営を行う。

サイバーセキュリティ研究における倫理的配慮のサポート

秋山満昭 | NTT セキュアプラットフォーム研究所 島岡政基 | セコム（株）IS 研究所

サイバーセキュリティ研究を取り巻く状況

サイバーセキュリティの研究は、十分に前例のない領域を研究対象として取り扱うことが多く、一方でその行為が社会に対して直接的な影響を与え得るために“倫理的”な問題にも直面しやすい。より先進的で革新的な研究を実施する場合はなおさらである。たとえば以下に示す状況において、研究者はどのように行動すればよいかについて、ICT 技術・社会的状況・法制度などのさまざまな観点から議論が尽きない。

- ネットワーク上に蔓延する脆弱なデバイスを発見するためのネットワークスキャン
- セキュリティ上の欠陥を発見するために実在するシステムに対して行う調査
- 欠陥や脆弱性を発見した場合に発見者としてとる行動

このような研究にはステークホルダー（利害関係者）が存在し、彼らは研究成果の恩恵が得られる一方で、研究行為やその結果の公表によって被害を受ける可能性もある。研究行為そのものや成果の世の中への伝え方を誤ったが故に、世間から批判される事例や法廷闘争に発展する事例が多々ある。このような研究行為のグレーゾーンにおいては倫理的な研究プロセスが必要であるということが国内外のさまざまな研究コミュニティにおいて広く議論されている。つ

まり、無責任に危険な実験を実施したり攻撃手法・脆弱性をむやみに公開するのではなく、研究が世の中に与える影響を考慮した上でどのように倫理的に取り組めばよいかを考えることは今日のサイバーセキュリティ研究者としての必須の素養となっている。しかし一方で、進展の早いサイバーセキュリティの分野では十分に議論されていない領域の倫理的問題に研究者が直面することがしばしばある。そのような判断が難しい状況において、研究者自身の自己責任とするのは研究者の萎縮を招く可能性がある。このような萎縮によって科学技術の発展が妨げられるのは避けなければならない。研究コミュニティとして先進的な研究をサポートするために何ができるのかを考えなくてはならない段階に入っている。

研究倫理原則

研究倫理は幅広く大きい概念である。研究倫理の全体像とセキュリティ研究が特に対象とする研究倫理の関係について、後述の日本学術振興会サイバーセキュリティ第 192 委員会ワーキンググループがとりまとめた図-1^{☆1}に基づいて説明する。科学と科学的知識の利用について概念的にまとめた「ブダペスト宣言」（1999 年）や日本学術会議の「科学者の行動規範」に関する声明（2006 年）は、さまざまな研究分野に共通的なベースとなる研究倫理の要素から構成されている。文部科学省は特に、研究活

^{☆1} サイバーセキュリティ研究における倫理的な研究プロセスの普及啓発について。 <http://www.iwsec.org/mws/2018/20181220/jsps-192-ethicsWG.pdf> より抜粋。

動の不正行為（捏造、改ざん、盗用等）の観点からの研究倫理とその対応に関するガイドライン（2006年）を発行している。米国政府委員会は、生物医学分野などの人を取り扱う研究における研究倫理原則をとりまとめたベルモントレポート（1979年）を発行している。このベルモントレポートでは3つの研究倫理原則として以下のように示されている。

・ 人格の尊重（Respect for Persons）

研究の実験への参加は本人の自由意志によって決められるべきであり、本人への十分な説明をした上で本人が意思決定する権利を尊重すること（インフォームドコンセントの考え方）。

・ 恩恵（Beneficence）

研究により得られ得る恩恵を最大にし、与え得る危害を最小にするためのリスクアセスメントを行うこと。

・ 正義（Justice）

個人の扱いについて平等に配慮を行い、また研究の恩恵は平等に分配し、負担は研究対象に対して同等に分担すること。

ベルモントレポートの研究倫理原則を踏襲しつつ、ICT/セキュリティ研究に対応したメンロレポート（2012年）が米国国土安全保障省によって発行された。メンロレポートでは、3つの研究倫理原則をICT研究の文脈で解釈することに加えて、下記の研究倫理原則を新たに追加している。

・ 法と公益の尊重（Respect for Law and Public Interest）

法令を遵守し、公共の利益の尊重すること。研究方法と結果の透明性を担保し、その行為に責任を持つこと。

メンロレポートで新たに追加されたこの原則は、地域間における法律の対立や曖昧さ、ステークホルダの特定の難しさ、法と公益の間の不一致、などを明示したものである。たとえば、研究過程でセキュリティホールを発見した場合は、ステークホルダを特定して、被害を最小化した上で世の中に情報を伝えるための責任ある情報開示（Responsible disclosure）を実践しなければならない。

メンロレポートは今日のICT/サイバーセキュリティ

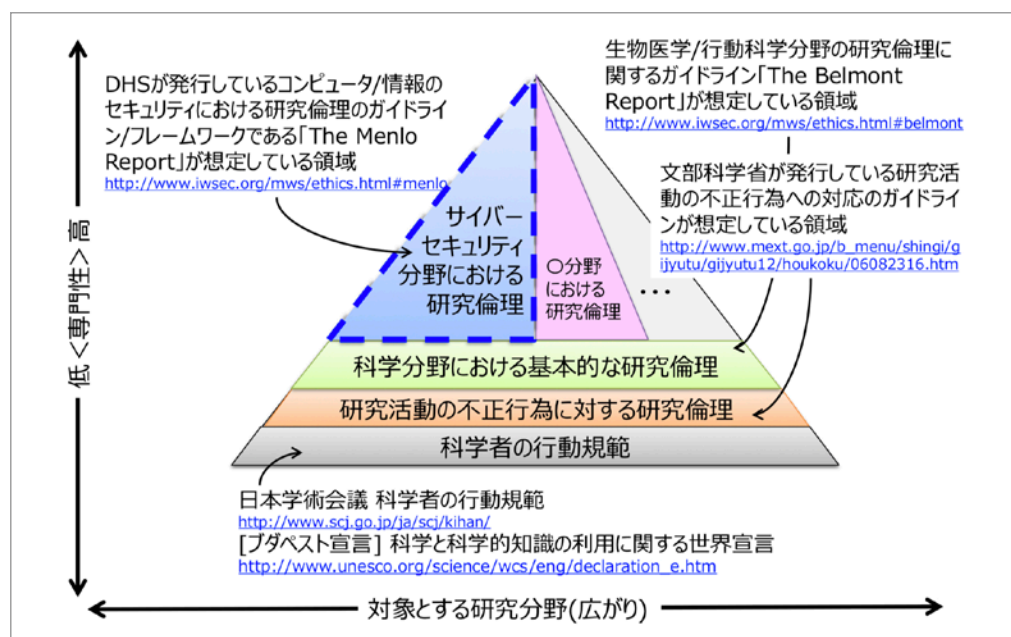


図-1
研究分野と専門性に対応する
各種研究倫理原則

ティ研究の倫理原則として認識されているが、この原則をさまざまな状況で適切に実践することは容易ではない。たとえば、大規模なユーザデータを取り扱う際のインフォームドコンセントの取り方、複雑な分散 ICT 環境においてインフォームドコンセントを獲得する主体の特定が容易ではないこと、影響が瞬時に伝達される状況におけるリスクと被害についての迅速かつ的確な判断等、これらはベルモントレポートが制定された当時では想定し得なかった環境条件に基づいて実施される場合の難しさである。

世の中の動向

このようなサイバーセキュリティの研究倫理への関心の高まりを受けて、学術国際会議において研究倫理の議論が取り上げられることが増えてきた。サイバーセキュリティ研究倫理をテーマとした新たな学術国際会議として CREDS や NS-Ethics (2013 ~ 2015 年) が開催され、研究倫理の議論が不十分だった過去の研究事例の再レビュー、ベストプラクティスの共有、倫理的な研究プロセスの設計、などを実施し、ICT 環境の変化に対応したよりよい倫理的研究のサポートを試みている。また、サイバーセキュリティのトップ学術会議である IEEE S&P・ACM CCS・USENIX Security・ISOC NDSS では、2013 年頃から Call For Paper において「研究倫理の議論を喚起しそうな論文については、適切な手順に基づいてどのように実施しているかを明記すること」を求めており、不適切な論文は採択されない可能性があることが明記されている。

トップ国際会議論文に学ぶ倫理的配慮

では実際に世の中のサイバーセキュリティ研究者はどのように倫理的に研究を実践しているのだろうか？ サイバーセキュリティ分野のトップ国際会議の 1 つである USENIX Security において、メンロレポート発行以降の 2012 年から 2019 年までに発表された論文の中から研究倫理の言及がある約 100

本の論文について研究倫理に関する記述を調査した。その結果、研究倫理の議論・主張や実践について大まかに以下のように分類できた。

• 同意・許可の獲得

実験の対象になる主体（ユーザ／サービス事業者／ネットワーク管理者等）からの同意・許可を得ている。

• 行為の正当性

ガイドラインやポリシーに準拠している。データを匿名化している。法律に準拠している。Responsible disclosure を実施している。ほかに代替手段がない。

• 所属組織の承認

所属組織の研究倫理委員会（Institutional Review Board, IRB）から研究内容に関するレビューを受けた上で研究実施の許可を得ている。

• リスクアセスメント

実験を行うことによって生じる新たなリスクはない。リスクや実際の被害を最小化するための努力をしている。

• 公益性

ベストプラクティスを共有している。公共の利益に貢献している。

これらはさまざまな研究行為に対して実施されたある種のベストプラクティスと位置付けることができ、同様の研究行為を行う場合に大いに参考にすべきケーススタディである。

倫理的配慮をサポートするための試行

前述のとおり、2012 年に発行されたメンロレポートによって欧米の学術国際会議を中心としてサイバーセキュリティ分野における研究倫理の認識が広がっていった。日本においても、2016 年頃からマルウェア対策人材育成ワークショップ（MWS）を

中心とした研究コミュニティにおいて多数のイベントが開催され、現状の認識、課題の整理、ベストプラクティスの共有、アクションプランなどが話し合われている¹⁾。2018年には、日本学術振興会のサイバーセキュリティ第192委員会にワーキンググループが設置され、学会横断的にサイバーセキュリティ研究倫理の啓発活動が推進されている。また同年、日本最大級の学術セキュリティシンポジウムであるコンピュータセキュリティシンポジウム(CSS)において、サイバーセキュリティに関する研究倫理委員会が設置され、論文投稿を検討する研究者に対しての研究倫理相談窓口が開設された。さらに2019年には、CSSは「サイバーセキュリティ研究における倫理的配慮のためのチェックリスト」(以降、チェックリスト)を整備し、論文投稿予定の研究者が活用できるようになった。以降では、研究倫理相談窓口とチェックリストの詳細な説明を行う。

研究倫理相談窓口の設置

CSSで設置された研究倫理委員会は、サイバーセキュリティの専門家や法学者、弁護士から構成されている。本研究倫理委員会は「研究の承認」を行うことを目的としておらず、研究倫理相談窓口(以降、相談窓口)を研究者とのインタフェースとして適切な倫理的配慮の実施をサポートすることを目的としていることが特徴である。相談窓口は、論文募集要項の発表から発表申込締切までを問合せ受付期間として開設している。論文投稿を検討しているが研究倫理的に不安のある研究者は、相談フォームに記入の上、相談窓口にお問い合わせる(図-2)。相談フォームでは、研究者が実施しようとしている研究内容、研究倫理上考えられる問題点とその対応案等を記入するようになっている。相談窓口では、受け取った相談内容を内部の委員間で整理した上でレビューする。委員は、類似の研究事例・倫理的対応や法制度・社会情勢を調査した上で、研究行為のステークホルダの識別と、相談内容に関する回答、お

よび参考情報や事例を相談者である研究者と共有している。

これまでに6件の相談(2018年4件、2019年2件)があり、5営業日以内での回答を行っている。2019年に問合せが減少した原因の1つとして、後述するチェックリストの活用によって、基本的な懸念については解消された可能性がある。

チェックリストの試行

2018年の相談窓口の知見から、2019年はサイバーセキュリティ研究における倫理的配慮のためのチェックリスト²⁾を整備し、相談窓口と併せて活用を推奨することとした。チェックリストの目的は、当該論文に倫理的配慮の観点を著者らに認知してもらうこと、その上で必要に応じて論文への記載を検討してもらうこと、そしてそれらが実施されたことの観測の3点とした。すなわち、回答が適切であれば倫理的問題がないことを保証するものではなく、また不適切だからただちに倫理的問題があることを意味するものではない。チェックリストは、現時点における共通的な落とし穴(Common pitfall)を列挙することに注力し、主に1)基本事項の確認、2)機微情報の扱い、3)ネガティブな影響に関する配慮の3項目(全9項目)とした。

プライバシーや広域スキャンなどに関する項目についても議論はあったが、回答者の負担増や回答精度

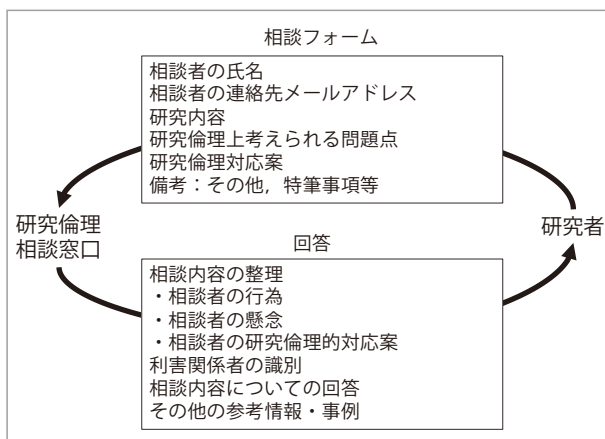


図-2 研究倫理相談窓口

の低下、また長期的な視点からリストの肥大化を避け基本原則の確認に注力すべき、などの議論を経て、きわめてシンプルなものにとどめた。項目数を厳選した一方、倫理的配慮の知識が不十分な著者でも回答できるよう、いくつかの項目には解説や参考事例を補記し読解性に配慮した。

これら項目の解説やチェックリストの趣旨などについては、投稿締切までのコンピュータセキュリティ研究会（CSEC）において何度か企画セッションを設けて周知を行った。

チェックリストは投稿時のセルフチェックとし、チェックの有無にかかわらず投稿は可能としたところ、投稿 223 件^{※2} 中 216 件（96.9%）がチェックしたとの回答を得た。

倫理的配慮を実施する論文の推移

さて、これまで日本のコミュニティが行ってきた前述の啓発活動、研究倫理相談窓口、チェックリストは、どの程度の効果があっただろうか？ 効果の一側面ではあるが、倫理的配慮について言及する論文の推移について過去 4 年間の CSS 論文と USENIX Security 論文を調査した（図-3）。USENIX Security では毎年 10 本を超える論文が研究倫理の配慮に関する記述を行っており、その数は年々増加している。CSS では 2016 年にはそのような論文はわずか 1 本

※2 最終的な投稿受理件数。発表申込時点では 257 件。

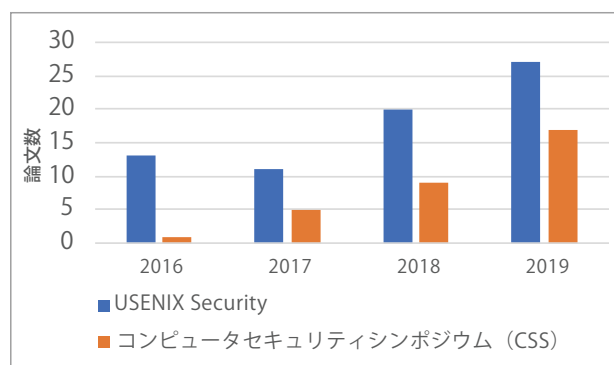


図-3 倫理的配慮を実施する論文の推移

であったが、年々増加傾向にあり、2018 年の 9 件から 2019 年では 17 件と倍近く増加している。これは、倫理的配慮が必要な先進的な研究が増えてきたこと、そして倫理的配慮を実施して論文中に記述するという意識が広まってきたことが要因として考えられる。

今後の展望

チェックリストのフィードバック分析

論文投稿者の一部から、チェックリストのチェック結果について具体的な回答 22 件を得て、分析を行った。このうち機微情報を扱ったものは 8 件あり、いずれも論文中で適切に明記したとの回答を得た。また、ネガティブな影響を含むものは 15 件あり、うち該当するすべての項目について適切に論文に記載したものは 6 件、一部明記しなかった論文が 6 件、特に明記しなかった論文が 3 件であった。これらの比率や件数についてはサンプル数が少ないため議論を避けるが、一定の配慮がされているものも少なくないこと、また明記しなかった論文についても、チェックリストを通じて配慮の余地があることを著者に認知することができたと考えられる。

これら著者からの任意のフィードバックとは別に、最終的に収録された論文 223 件について倫理委員会有志にて分析した結果、前述の通り倫理的配慮が明記された論文 17 件を確認した。また、一部には倫理的配慮のためにチェックリストを活用したとの記述もあった。前述の通りチェックリストは倫理的問題の有無を保証する性質のものではないが、一方で研究コミュニティにおけるコンセンサスに基づいたある種の行動指針となる可能性が示されたと考えている。

チェックリストのアップデート

これらのフィードバックや、国内外のサイバーセキュリティ研究およびその倫理的配慮に関する最新

動向を踏まえながら、チェックリストのアップデートに取り組んでいきたいと考えている。啓発を強化する観点では、既存項目も含め解説や事例の充実を図ってきたい。特に事例に関しては、サイバーセキュリティの分野は（たとえばサービス妨害攻撃と判断されるアクセス頻度の多寡のように）社会理解の変化も著しく、事例が陳腐化しやすいケースもあるため、細心の倫理的配慮の動向に注意を払いながら事例を示していく必要があると認識している。また、サイバーセキュリティ分野と一口に言っても範囲は広く、プライバシーや広域スキャンへの配慮など取り組んでいくべき領域は少なくないと認識している。一方で、前述の通りチェックリストの肥大化は望ましい方向性ではないとも考えており、安易に項目数が増加しないよう最大限の注意を払っていきたい。

啓発活動の横展開

本取り組みはコンピュータセキュリティシンポジウムを端緒としているが、同シンポジウムに限らずサイバーセキュリティに関連する研究コミュニティに幅広く関係する問題である。CSS およびその主催研究会である CSEC の啓発活動を通じて、他学会も含めいくつかの研究コミュニティから関心を寄せられている。

有志の負担に依存せずに取り組みを広げていくためにも、前述の解説や事例の充実がポイントとなる。チェックリストの試行はもちろんのこと、解説や事例の充実に貢献いただける有志も大いに歓迎したい。また、CSS に限らず各シンポジウムや研究会など研究コミュニティで必要に応じて相談窓口を設置することも検討いただければ幸いである。窓口を介し

た相談プロトコルは図-2 が参考になるだろう。

最後に、セキュリティ分野に限らず、たとえば適用領域における社会変化や技術革新の著しい分野等においても、研究倫理的課題に直面している研究分野は少なからずあるのではないだろうか。直接的に資する点はそれほど多くないかもしれないが、研究倫理的課題に対する研究コミュニティとしての取り組みにおいて、本活動が多少なりと参考になれば幸いである。

参考文献

- 1) マルウェア対策人材育成ワークショップ (MWS), サイバーセキュリティ研究における倫理的な研究プロセスについて, <https://www.iwsec.org/mws/ethics.html>
- 2) コンピュータセキュリティシンポジウム (CSS) 2019, サイバーセキュリティ研究における倫理的配慮のためのチェックリスト, https://www.iwsec.org/css/2019/ethics_list.html (2019 年 12 月 27 日受付)

秋山満昭 (正会員) akiyama@ieee.org

2007 年奈良先端科学技術大学院大学情報科学研究科修士課程修了。同年日本電信電話 (株) 入社, NTT 情報流通プラットフォーム研究所にてマルウェア対策技術の研究開発に従事。2016 年 NTT セキュアプラットフォーム研究所特別研究員。2019 年同所上席特別研究員。主としてサイバー攻撃対策技術の研究開発に従事。博士 (工学)。電子情報通信学会・IEEE 各会員。

島岡政基 (正会員) m-shimaoka@secom.co.jp

1998 年慶應義塾大学大学院理工学研究科修士課程修了。同年セコム (株) 入社。2004 年より同 IS 研究所。2005 ~ 2010 年まで国立情報学研究所特任准教授 (後に客員准教授), 2019 年より筑波大学システム情報系客員准教授を兼務。2014 年総合研究大学院大学複合科学研究科情報学専攻博士課程修了。博士 (情報学)。認証基盤とトラストの研究開発に従事。本会コンピュータセキュリティ研究会幹事 (2015 年 ~), 本会セキュリティ心理学とトラスト研究会運営委員 (2014 ~ 2017 年), 本会論文誌ジャーナル/JIP ネットワークグループ編集委員 (2015 ~ 2018 年), 本会論文誌ジャーナル編集委員会副編集長/ネットワークグループ主査 (2018 年)。

量子ソフトウェア研究会の 新設にあたって

小野寺民也 | 日本アイ・ビー・エム

今井 浩 | 東京大学

現在、量子情報技術は、一大新潮流として台頭し、21世紀を牽引する学問領域になるともいわれている。主要国は国家技術戦略の中核に位置付けて取り組んでおり、米国では2018年12月21日に「国家量子イニシアチブ法」が大統領署名され、5年間で12.5億ドル規模の投資がなされることになっている。欧州連合および中国においても同規模のプログラムが走っており、我が国では、平成30(2018)年度より光・量子飛躍フラッグシッププログラム(Q-LEAP)が開始され、10年間でおよそ220億円を投資することになっている。

量子情報技術は、量子センシング、量子コンピュータ、量子ネットワーク、量子暗号などの分野で展開されているのであるが、なかでも、量子コンピュータは、現在のコンピュータとは異なる次元の計算性能を有することが理論的に示されており、政府投資の重点領域であるのみならず、米国を中心に、巨大IT企業やスタートアップ企業が参入し、し烈な研究開発競争を繰り広げていることは、巷間によく知られているところである。

ところで、量子情報技術は、物理学の一分野として発展してきた。したがって本会とこれまで深いかかわりがあったわけではない。しかし、科学技術振興機構の研究開発戦略センターが2018年12月に発行した戦略プロポーザル「みんなの量子コンピュータ」によれば、量子コンピュータの実用をいよいよ加速するためには、情報、数理、電気工学等、広い分野の研究者が結集すべきことが求められており、

特にソフトウェアの研究開発の充実が急務であるとされている^{☆1}。

米国計算機学会においても、昨年来、この分野の活動が急速に活発化してきている。これまでも量子コンピューティングのチュートリアルはあったが、ISCA 2019 (International Symposium on Computer Architecture) および ASPLOS2019 (Architectural Support for Programming Languages and Operating Systems) においては、量子コンピューティングのセッションが単独で設けられるまでになり^{☆2☆3}、POPL 2020 (Symposium on Principles of Programming Languages) では量子コンピューティングのためのプログラミング言語に関する併設ワークショップが開催された^{☆4}。さらに、量子コンピューティングに関するトランザクションの刊行も決まっている^{☆5}。

こうした国内外の展開を鑑みれば、我が国において情報処理技術を60年近く牽引してきた本会が、量子ソフトウェアの新分野に本格的に参画することは、まさに時代の要請であり、学会の責務といえるであろう。そのように考え、量子ソフトウェア研究会の新設をコンピュータサイエンス領域において提案したのであったが、2019年10月開催の本会調査研究・3領域合同委員会にて承認され、2020年

☆1 <https://www.jst.go.jp/crds/pdf/2018/SP/CRDS-FY2018-SP-04.pdf>

☆2 <https://iscaconf.org/isca2019/program.html#session5adetail>

☆3 <https://asplos-conference.org/2019/index.html#p=824.html#a12>

☆4 <https://popl20.sigplan.org/home/plaqc-2020>

☆5 <https://tqc.acm.org/>

4月から活動を開始することとなった。

新設にあたっては、これまで我が国において、量子情報技術を牽引してこられた多くの方々に提案者になっていただいた^{☆6}。あらためて深謝するとともに、本会および量子ソフトウェア研究会に対する期待に応えたいと思う。

主な研究分野としては、量子計算アーキテクチャ、量子プログラミング言語、量子計算アプリケーション、量子ソフトウェア開発環境（シミュレータ、コンパイラ等）、量子アルゴリズム、分散量子計算、量子ネットワークのソフトウェア、量子センサのソフトウェア、量子セキュリティ、など多岐にわたるが、本会のコンピュータサイエンス領域の研究会のそれぞれの研究領域と連関するところもあり、特にそうした領域の研究者および実務者の参画を促したいと考える次第である。

2020年度の活動としては、5月の発足記念講演会、7月と2021年3月に研究会を予定している。詳細は本研究会 Web ページを参照されたい^{☆7}。

先述のように、量子コンピュータは異次元の性能を有するのであり、その計り知れない計算パワーを解放することができたならば、社会の難題を解決し未知の価値を創造し、人類は新しい時代に突入するに違いない。しかし、その実現には無数のチャレンジがあり、関連諸分野の叡智を結集する必要がある。

^{☆6} <https://www.ipsj.or.jp/kenkyukai/newsig-qs.html>

^{☆7} <https://sigqs.ipsj.or.jp/>

本研究会は、量子ソフトウェアの研究により、こうした人類の新時代の建設に寄与しようとするものであり、多くの会員の参加を期待するとともに懇請したい。

【付記】「(量子情報技術は) 本会とこれまで深いかかわりがあったわけではない。」と述べたが、かわりが皆無だったわけではない。それどころか、会誌「情報処理」の2006年12月号¹⁾および2014年7月号²⁾において、二度にわたり量子コンピュータの特集を組んでいる。会誌編集委員会の面目躍如たるところがある。これらの記事は今に通用するものであり、本会電子図書館での一読を勧奨する。

参考文献

1) 《特集》量子コンピュータと量子計算, 情報処理, Vol.47, No.12 (Dec. 2006).

2) 《特集》量子コンピュータ, 情報処理, Vol.55, No.7 (June 2014). (2020年2月4日受付)

■小野寺民也（正会員） tonodera@jp.ibm.com

1988年東京大学大学院理学系研究科情報科学専門課程博士課程修了。理学博士。同年日本アイ・ビー・エム（株）入社。以来、同社東京基礎研究所にて、基盤ソフトウェア等の研究開発に従事。現在、同研究所副所長、量子アルゴリズム&ソフトウェア担当部長、同社技術理事。

■今井 浩（正会員） imai@is.s.u-tokyo.ac.jp

東大計数1981年卒業、情報工学1986年修了、工学博士。1986年九大情報工学助教授を経て、1990年より東大情報科学、現在同コンピュータ科学教授。JST ERATO 今井量子計算機構プロジェクト研究総括（2000～2011年）。専門は量子計算、アルゴリズム論。

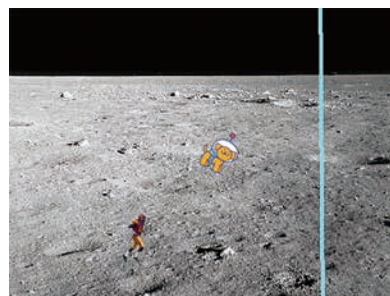
集まれ！ ジュニア会員！！

今回は2019年12月21日に開催された、小学3年～6年生のジュニア会員を対象とした本会主催のイベントである「Exciting Coding! Junior 2019」にて制作された作品を紹介します。本イベントではプログラミング環境Scratch（スクラッチ）と、プログラミング可能な小さなコンピュータであるmicro:bitを利用して、保護者の方と一緒にアニメーションやゲームを制作しました。初めてプログラミングを体験する会員から、家でもプログラミングを楽しんでいる会員まで、12名が参加しました。機材トラブルも発生してしまった中、3時間という短い時間でしたが、各会員のこだわりあふれる作品が制作されました。今回は制作された作品の中から1つの作品を紹介します。

作品介绍 マグロさんの作品「宇宙レース！」

<https://scratch.mit.edu/projects/355650406/>

犬と人間が月で競争する作品です。人間はラグビー選手にしたかったのですが、なかったのでアメフト選手にしました。犬は、micro:bitのボタンで動かします。人間は、キーボードのスペースキーで動かします。犬を動かすプレイヤーと人間を動かすプレイヤーの、2人で競争するゲームです。こだわったポイントは、1回スペースキーを押すごとに人間が何歩動かすかを調整したところ。犬のスタート位置と進む方向の角度を変え、人間の大きさを小さくしたので、1回に何歩動かすかでゲームの楽しさが変わってきます。鬼ごっこのように犬と人間を追いかけてさせるような作品に改良したいです。



●作品の画面キャプチャ



●犬のプログラム



●人間のプログラム



micro:bitにはさまざまなセンサが搭載されているので、ほかのセンサを使うように改良をしてみましょう。たとえば、「(micro:bitが)振られたとき」のブロックを利用すると、micro:bitを手で持って走るように手を動かすことで、犬を動かすことができます。



何歩動かすか試行錯誤した結果が、微妙な数値にあらわれていますね。ゴールしたときの効果音が犬と人間で異なるため、どちらが先にゴールしたかが分かりやすいところがいいですね。対戦形式なので、何度でも遊びたくなるゲームです。

今回紹介した作品は、Scratchのチュートリアル作品例にあった「ゴールまで競争しよう」(<https://scratch.mit.edu/projects/171959117/>)をmicro:bitを利用するように改良した作品です。micro:bitなどのセンサは、現実世界とコンピュータの中の世界とをつなぐ役割を果たしてくれます。ぜひ試してみてください。



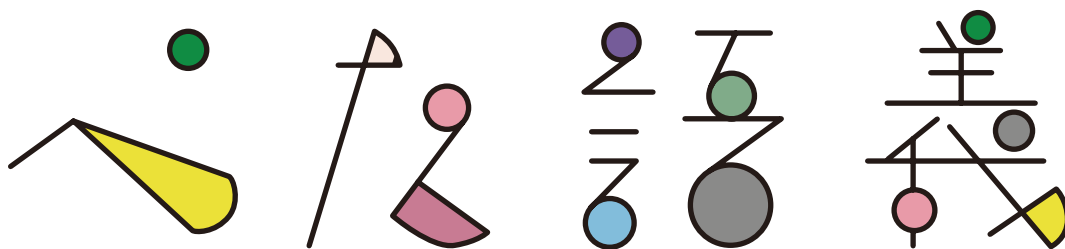
●micro:bit

参考 Web サイト：Scratch, <https://scratch.mit.edu/>
micro:bit, <https://microbit.org/>

本企画では、ジュニア会員の方の作品・プログラムを募集しています。氏名、ニックネーム、ご連絡先メールアドレス、会員番号、作品に利用しているプログラミング言語、作品タイトル、作品の説明、こだわったポイントを、以下の宛先までお送りください。

✉ 会誌編集部門 E-mail: editj@ipsj.or.jp

担当：吉田 葵（青山学院大学）



Vol. 103

CONTENTS

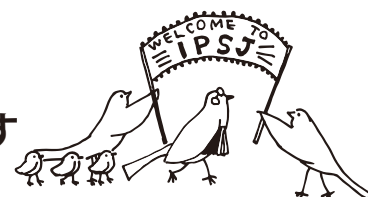
【コラム】小中高の先生の自信をサポートします… 高橋 尚子

【解説】Processing でプログラミングに挑戦!—第3回 繰り返しを使いこなそう— 杉浦 学

【解説】スリランカの学校訪問記… 和田 勉

COLUMN

小中高の先生の自信をサポートします



何が不安かというと、プログラミング教育の導入にも追いついていないのに、その先に数理・AI・データサイエンス教育まで出てきたことだ。2022年度から高校の情報科では、「情報Ⅰ」が必修科目になり「アルゴリズムとプログラミング」を学習する。選択科目の「情報Ⅱ」では、さらに高度に、データサイエンスや情報システムに関するプログラミング学習を行う。このように情報教育への要求・期待は、加速度的に高くなっている。いったいどうすればいいのか？

そういう悩みを減らし、1つでも自信がつけられるよう、本会では先生へのサポート体制を全方位的に整えている。かつて、学会は難しい研究をする学者や高度な技術を持つ企業の集まりで、教員には敷居が高い場所と考えられていたが、いまは異なる。最先端の研究はもちろんのこと、学校種別、世代、利用目的、分野、手法に応じてさまざまな教育プログラムを網羅している。情報教育を推進し、情報学を普及してすそ野を広げ、誰でもが一定の技能を有し、尖った人材を生み出すことを使命と考えている。すでに ICT 活用やプログラミング教育など情報学の指導力を修得できる「教員免許更新講習」を実施している。情報の先生だけでなく該当する教員であれば誰でも受講できる。また、各地（2019年度）で開催される情報に関する教員研修に、情報教育の専門家を派遣している。

加えて、本年度は、高校の先生向けに「情報Ⅰ」の研修教材を MOOC（Massive Open Online Courses：公開講座）としてインターネットで配信する準備を進めている。テキスト・実習・動画での解説を一体化したものだ。本会は、こういった総合的な情報を探し、サービスを受けるには、うってつけの場所である。分かっているが、そんな余裕がないという小中高の先生方へ「初等中等教育機関の教職員を対象とした入会金・会費割引キャンペーン制度」を実施することを決定した。4月から6月の新規入会者を対象とした期間限定キャンペーン、詳細は Web サイト (<https://www.ipsj.or.jp/member/kyoinwaribiki-2020.html>) で確認してほしい。

情報の授業、特にプログラミングという、はじめから考え方や技能の習得には壁が高く厚いと思われる。そして、学習環境を整え、教材を準備し、決まった時間内に生徒全員が完遂させる確信を持ちにくい。今年は大丈夫でも、来年アップデートされたら同じように動かないかもしれない、毎年更新するなんてとても面倒で扱いたくない、まるで重たい鎧を纏うような感じがするかもしれない。

しかし、プログラミングやその考え方であるアルゴリズムを理解できるようになると、授業の守備範囲が広がる。それは壁を乗り越える【パワースーツ】を着るようなものだと思ってほしい。短時間で大量のデータを処理したり、何万回という繰り返しを試したり、どう捉えていいのかわからないことをビジュアルに目の前に表示できる。新しい知識や能力を修得しなければならないのは大変なことだが、それ以上に身に付いたものは総合的な教育力を増すことになるはずだ。「百聞は一見に如かず」体験することがイチバンの近道、1つでいいから体験するため、一度のぞきにきてほしい。

高橋 尚子 (本会教育理事／國學院大學)

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

Processing でプログラミングに挑戦！ —第3回 繰り返しを使いこなそう—

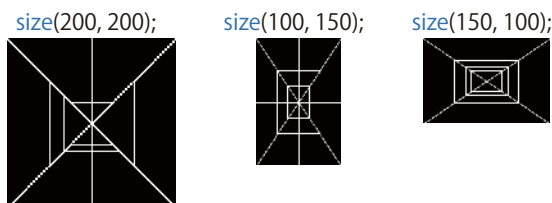
杉浦 学

鎌倉女子大学

宿題の解説

前号では、ウィンドウのサイズに合わせて形が変化する、クモの巣の模様(図-1)を描く宿題を出題しました。

● 前号の宿題



四角形は小さい順に、画面の縦・横の長さのそれぞれの四分の一、三分の一、二分の一になるように割り算で計算します

図-1 クモの巣の模様

この宿題の解答例をスケッチ1に示します。width と height の変数と、計算を組み合わせることで、2行目の size 関数で指定するウィンドウのサイズに合わせてクモの巣の形が変形します。

```

1 //描画の準備
2 size(200,200);
3 background(0);
4 stroke(255);
5
6 //直線を描く
7 line(0,0,width,height);
8 line(width,0,0,height);
9 line(0,height/2,width,height/2);
10 line(width/2,0,width/2,height);
11
12 //四角形を描く
13 rectMode(CENTER);
14 noFill();

```

```

15 rect(width/2,height/2,width/2,height/2);
16 rect(width/2,height/2,width/3,height/3);
17 rect(width/2,height/2,width/4,height/4);

```

スケッチ1 クモの巣を描く(宿題の解答例)

繰り返しのパターンを見つける

変数と計算を使って、繰り返している処理を同じ形に変形できれば、それらの処理を効率良く記述することができます。まずは複数の斜線を描くスケッチ2を見てみましょう。

```

1 size(480,120);
2 strokeWeight(8);
3 line(20,40,80,80);
4 line(80,40,140,80);
5 line(140,40,200,80);
6 line(200,40,260,80);
7 line(260,40,320,80);
8 line(320,40,380,80);
9 line(380,40,440,80);

```

スケッチ2 複数の斜線を描くスケッチ(文献1) P.45 より)

スケッチ2を実行すると、図-2のような模様が表示されます。斜線の始点と終点のx座標を60ずつ増やし(右にずらしながら)、斜線を合計で7本描いています。



図-2 複数の線を描く

スケッチ 2 に変数を導入したものがスケッチ 3 です。

```
1 size(480,120);
2 strokeWidth(8);
3
4 int x=20;
5
6 line(x,40,x+60,80);
7 x+=60;
8
9 line(x,40,x+60,80);
10 x+=60;
11
12 line(x,40,x+60,80);
13 x+=60;
14
15 line(x,40,x+60,80);
16 x+=60;
17
18 line(x,40,x+60,80);
19 x+=60;
20
21 line(x,40,x+60,80);
22 x+=60;
23
24 line(x,40,x+60,80);
25 x+=60;
```

スケッチ 3 変数を導入した斜線を描くスケッチ

スケッチ 3 では、斜線の始点の x 座標を変数 x に保存し、線を 1 本描くごとに 60 だけ増やしています。変数 x の値を現在の値より 60 増やしたい場合は、`x=x+60;` と書くところを短く `x+=60;` と書くことができます。終点の x 座標は始点の x 座標の x に 60 を加えた「`x+60`」になります。変数を導入するとスケッチの行数は増えてしまいましたが、斜線を 1 本描く処理に注目してみると、まったく同じ処理が 7 回登場していることを発見できました (図-3)。なお 25 行目は省略しても描画の結果は同じになります。

int x=20; 最初はxを20にしておく

line(x,40,x+60,80); x+=60; } 1本目

line(x,40,x+60,80); x+=60; } 2本目

line(x,40,x+60,80); x+=60; } 3本目

line(x,40,x+60,80); x+=60; } 4本目

line(x,40,x+60,80); x+=60; } 5本目

line(x,40,x+60,80); x+=60; } 6本目

line(x,40,x+60,80); x+=60; } 7本目

xを60ずつ増やしなが
7回繰り返す

最後にxが440になる

図-3 同じ処理の繰り返し

for ループによる繰り返し

図-3 に示したように、最初に変数 x を宣言して 20 を代入したら、x に 60 を加えながら、`line(x,40,x+60,80);` というまったく同じ処理を 7 回繰り返せばよいことになります。こうした繰り返し処理を記述するには「for ループ」を使います。for ループを使ってスケッチ 3 を書き直したものがスケッチ 4 です。

```
1 size(480,120);
2 strokeWidth(8);
3 for(int x=20; x<440; x+=60){
4   line(x,40,x+60,80);
5 }
```

スケッチ 4 for ループを使って斜線を描くスケッチ

for ループの文法を整理しておきます (図-4)。繰り返しをしたい処理は「{」と「}」で囲みますが、囲まれている処理が分かりやすいように段下げ (インデント) をするようにしましょう。編集メニューから自動フォーマットを選択すれば、自動でインデントをすることができます。for の後の括弧には、図-4 に示したように 3 種類の処理を記述します。慣れないうちは、最後の処理 (この場合は `x+=60`) に「;」をつけてしまうことが多いので注意してください。



青：繰り返しを始める前に一回だけする処理
 緑：繰り返しを継続する条件
 赤：繰り返しが一回終わるたびにする処理

```
for (int x=20; x<440; x+=60) {
  line(x,40,x+60,80);
}
```

繰り返ししたい処理を{}で挟む

図-4 for ループの文法

繰り返しの継続に関する条件を記述するためには、比較演算子(表-1)という記号を利用します。繰り返しが一度終わるたびにこの条件を調べ、条件が成立する場合は繰り返しを継続します。今回は「x が 440 より小さい」ときに繰り返しを継続するので、合計で 7 回繰り返しが行われます (8 回目で x が 440 になるので、8 回目の繰り返しは行われません)。

表-1 代表的な比較演算子

>	より大きい
<	より小さい
>=	以上
<=	以下
==	等しい
!=	等しくない

プログラミングに慣れてくれば、スケッチ 2 のような繰り返しの処理をすぐに for ループを使って記述することもできるでしょう。慣れないうちはまずは for ループを使わないで描いてみて、繰り返しのパターンを見つけてから、for ループに書き換えるという手順を踏むとうまくいきます。

□ 練習問題

前回の宿題の解答例(スケッチ 1)の 3 つの四角形を描いている部分を、for ループを使って書き換えてみましょう。繰り返しの回数を数える変数の名前は i としてください(繰り返しに用いる変数の名前として、i がよく使われます)。また、i の値を 1 だけ増やす処理「i=i+1;」は「i++;」と短く書くことができます。この短い書き方も練習してみましょう。

<解説>

for ループを使ったクモの巣のスケッチの例(該当部分のみ抜粋)

```
//四角形を描く
rectMode(CENTER);
noFill();
for(int i=2; i<5; i++){
  rect(width/2,height/2,width/i,height/i);
}
```

デバグ

スケッチを書いて実行した際に、1 回で想定通りの結果が得られる場合もありますが、意図と異なる結果となることも多くあります。そうした場合は不具合(バグ)の原因を突き止めてスケッチを修正(デバグ)する必要があります。変数や繰り返しを含んだ少し複雑なスケッチを効率良くデバグするには、「デバグ」を使うと便利です。デバグを使うことで、スケッチの実行を一時停止し、変数の値を確認しながら 1 行ずつ実行をすることができます。

デバグを使うには、エディタの右上にあるボタンをクリックします。同じ操作は「デバグ」メニューの「デバグを有効化」からも行えます。ここではスケッチ 4 の変数 x の値がどのように変化するか確認してみましょう。変数の値を確認したり、スケッチの実行の流れを検証したりするために実行を一時停止したい行を「ブレークポイント」と呼びます。行番号の部分をクリックすると、その行をブレークポイントに設定することができます。今回は for ループで繰り返しを行う 4 行目にブレークポイントを設定します(図-5)。なお、ブレークポイントを解除するには、もう一度その行をクリックします。

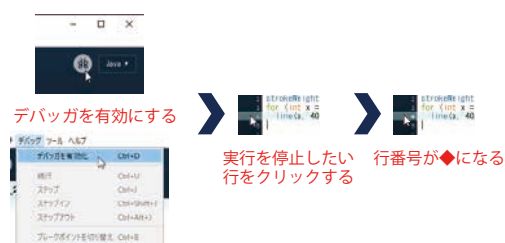


図-5 デバグの有効化とブレークポイントの設定

デバグを有効化すると、エディタ上部のボタンが 4 つに増えます。デバグ(▶)ボタンを押すと、ブレー

クポイントを設定した行の直前で実行が停止します。変数の値を一覧できる小さなウィンドウに表示されている変数 x の値は 20 になっているはずです(図-6)。

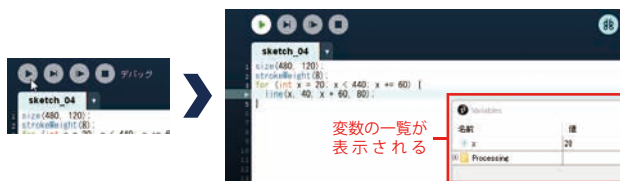


図-6 デバグの実行

繰り返しを進めて、変数の値の変化を観察してみましょう。「ステップ(▶)」ボタンを押すと、1行ずつ実行することができます。なお「続行(▶)」ボタンは、次のブレークポイントの直前まで実行を進めます。今回はステップボタンを押してみましょう。次に実行される行の行番号が▶の印に変わり、行が薄青色になります。今回の場合は、2回目の繰り返しが実行されるので、3行目の for ループに▶が表示されます。もう一度ステップボタンを押すと、4行目に▶が移動して、3行目の x+=60 が実行された結果が反映されて、変数 x の値が 80 に増えます(図-7)。

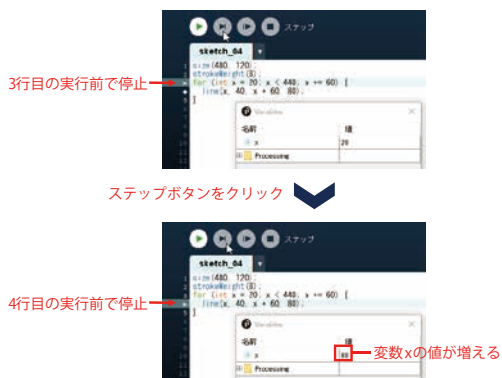


図-7 ステップ実行

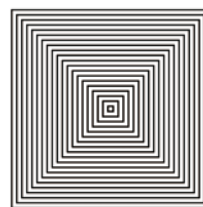
連続してステップボタンをクリックしていくと、3行目に▶が戻り、4行目に▶が進むことを繰り返す様子を確認できます。変数 x の値が 60 ずつ増えていくことを確認してみましょう。変数 x は最終的に 440 まで増えて繰り返しが終了しますが、デバグで確認できるのは繰り返しが終了する直前の値の 380 までです。デバグによる実行を停止したい場合は、「停止」(■) ボタンをクリックします。

デバグが終わったら、デバグを無効化してお

きます。デバグを有効化したときに押したエディタの右上のボタンを押すか、「デバグ」メニューの「デバグを無効化」を選択します。

□ 練習問題

以下のお手本を参考に、for ループを使って複数(20個)の正方形を使ったイラストを描いてみましょう。ウィンドウの大きさなどの描画の準備については、スケッチの例を示しました。正方形の中心の座標は(250,250)に設定し、一番小さな正方形の1辺の長さは10ピクセルで、一番大きなものは390ピクセルとしてください。それぞれの正方形の大きさは20ピクセルの差があります。一番小さなものから描いてもよいですし、大きなものから描いてもよいでしょう。できれば2通りの方法を考えてみましょう。うまくいかない場合は、デバグを使ってみてください。



```
1 //描画の準備
2 size(500,500);
3 background(255);
4 rectMode(CENTER);
5 strokeWeight(3);
6 noFill();
```

ヒント：描画の準備部分のスケッチ

<解説>

小さな正方形から描く例(該当部分のみ抜粋)

```
for(int i=10; i<=390; i+=20){
  rect(250,250,i,i);
}
```

大きな正方形から描く例(該当部分のみ抜粋)

```
for(int i=390; i>=10; i-=20){
  rect(250,250,i,i);
}
```



乱数

次は for ループによる繰り返しと「乱数」を組み合わせてみましょう。乱数を使うとプログラムが実行されるたびに異なる値を作り出すことができます。random 関数は設定した範囲内の float 型の乱数を作り出します。random 関数のパラメータを 1 つ指定した場合は乱数の上限、2 つ指定した場合は下限と上限を指定します。たとえば、random(256) とした場合、0 以上 256 未満の乱数が生成されます。

この乱数を使ってスケッチ 4 を改造し、実行されるたびに異なるカラフルな色の斜線を生成するように改造したものがスケッチ 5 です。スケッチ 5 を実行した結果の一例が図-8 です。

```
1 size(480,120);
2 strokeWeight(8);
3 for(int x=20; x<440; x+=60){
4   stroke(random(256),random(256),random(256));
5   line(x,40,x+60,80);
6 }
```

スケッチ 5 カラフルな斜線を描くスケッチ

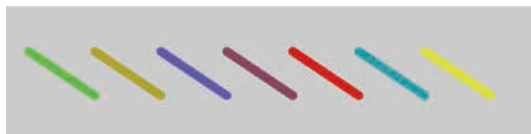


図-8 カラフルな斜線を描く

斜線を描く前の 4 行目で、stroke 関数の 3 つのパラメータに乱数を入れ込み、異なる線の色を設定しています (図-9)。これにより、毎回異なる 3 つの数値が色に設定されて、カラフルな斜線が描ける仕組みです。

stroke(random(256), random(256), random(256));

↓ ↓ ↓

0から255の範囲 0から255の範囲 0から255の範囲
のランダムな数 のランダムな数 のランダムな数

図-9 カラフルな斜線を描く仕組み

● 宿題

スケッチ 5 を応用して、お手本のようなカラフルな円の模様を描くスケッチを書いてみましょう。



それぞれの円の直径は 35 ピクセルです。ヒントのスケッチのコメントの部分 (9 行目) に複数の処理を追加して完成させてください。画面の縦横に円を敷き詰めるために、for ループの中に for ループを入れ込んだスケッチになっています。変数 x と変数 y の値を、デバッガを使って調べながら取り組んでみましょう。

```
1 //描画の準備
2 size(480,480);
3 background(0);
4 noStroke();
5
6 //カラフルな円を敷き詰める
7 for(int y=0; y<=height; y+=40){
8   for(int x=0; x<=width; x+=40){
9     //ここに処理を追加して宿題を完成させる
10   }
11 }
```

宿題のヒント

参考文献

- 1) Reas, C., Fry, B. 著, 船田 巧 訳: Processing をはじめよう 第2版, オライリージャパン (2016).

(2020 年 1 月 4 日受付)

杉浦 学 (正会員) manabu@kamakura-u.ac.jp

鎌倉女子大学家政学部家政保健学科准教授。慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士 (政策・メディア)。プログラミング教育をはじめとした情報教育に関する研究に取り組む。中高生向けの著書に『Scratch ではじめよう! プログラミング入門 Scratch3.0 版』(日経 BP 社) など。

スリランカの学校訪問記

和田 勉

長野大学

スリランカ

2018年3月、辰己丈夫先生（放送大学）と筆者でスリランカ（スリランカ民主社会主義共和国：旧名セイロン）を訪問し、政府の教育省（Ministry of Education）およびいくつかの大学および初等中等教育機関を訪問した。当時筆者がスリランカ出身の留学生の卒業論文を指導していたことがきっかけであり当人も一時帰国していくつかの学校訪問に同行した^{☆1}。またそれに加えて、日本への留学経験のある同国の大学の先生お二人にお世話いただいた。

スリランカは、国土面積は日本の北海道よりやや狭い65,525km²、人口は2,100万人余りであり東京都と神奈川県を合わせたよりやや少ない。主な民族は、シンハラ約75%、タミル約15%、イスラム（ムーア）約9%である。母語もシンハラ語とタミル語に分かれているが、英語が連結語として機能している。学校や公式な場にとどまらず日常生活や家庭内においても英語もかなり用いられており、駅名表示など

☆1 この調査比較研究はこの留学生の卒業研究でもある¹⁾



図-1 駅名表示：上からシンハラ語・タミル語・英語

はシンハラ語・タミル語・英語の3言語で記されている(図-1)。

基本的に学校の学費は無料であり、これは大学（国立）も同様である。その代わり入学総定員が少なく、大学進学資格を得て進学を希望する生徒のうちわずかな人数しか入学できない。同世代人口の中でスリランカ国内の大学に進学する割合は約8%であり、大学に入学できない生徒は、外国の大学に留学するが、それを含めても大学進学率は約15%のことである。そのほかには、スリランカ国内の教育機関が提供する外国の大学の課程を学ぶ制度を利用するか、あるいは、スリランカ放送大学（Open University of Sri Lanka）、スリランカ情報技術大学（Sri Lanka Institute of Information Technology）、工科大学（Institute of Technological Studies）、情報学大学（Informatics Institute of Technology）などの公私立の高等教育機関に進学する者もいる^{☆2}。

小中高等学校

Vishaka Balika Vidyalaya, Sapugaskanda

スリランカの初等中等教育の学校は、1つの学校の中に小学校から高等学校までに相当する学年があり、基本的に最後までその内部で進級する^{☆3}。そのような学校の1つである、コロンボ郊外にある表記の学校（女子校）を訪問した。児童生徒は女子のみであり、上記のように小学校相当から高等学校相当ま

☆2 現地学校訪問時のインタビュー、文献1）、および駐日スリランカ大使館 Web サイト：<http://www.slembassyjapan.org/>（2020年1月2日閲覧）。

☆3 特に成績の良い一部の生徒はよりランクの高い学校に途中で移ることもできる。



でが1つの構内にある(図-2)。

また教員もすべて女性であり、構内で見かけた男性は、門のところにいる守衛さんただ1人であった。女子校の教員は女性だけなのが当たり前のようで、先方の先生に「日本にも女子校はあるが、先生は女性だけでなく男性もいる」と言ったら驚いた様子だった。

生徒数は約3,300人で、ICTを専門とする先生は3人が在職、PCは28台ある。PCが設置されている教室で行われていた情報分野の授業を見学したところ、さまざまなプログラミング言語の特徴などを講義として紹介する授業であり、プログラミングそのものを行うところは確認できなかった(図-3)。また、教室の高いところに Steve Jobs と

Bill Gates の写真が貼ってあったのが印象的だった(図-4)。

これとは別の授業で、グループ討議も行っているところも見学したが、グループ討議を行う際、一部の生徒だけが別に分かれて討議をしていた。これは、多数の生徒は母語のシンハラ語で討議しているが、特に英語の能力向上を希望する一部の生徒だけが、英語で討議しているとのことである。しかし、このグループの生徒に限らず、見学中に接した生徒すべてが、我々と英語でまったく支障なく会話ができた(図-5)。

なおタミル語を母語とする子供たちはこの学校にはおらずその子供たちのための学校は別があり、それも地域的に大きくかたよりがある。

Saegis Campus

Saegis Campus という名の学校を訪問した。ここはスリランカの制度に基づく大学ではないが、提携する外国の大学のスリランカ国内校・専門学校・外国語学校の3つを兼ねている。もらった資料では、



図-2 構内の掲示—英語のスペルはイギリス式

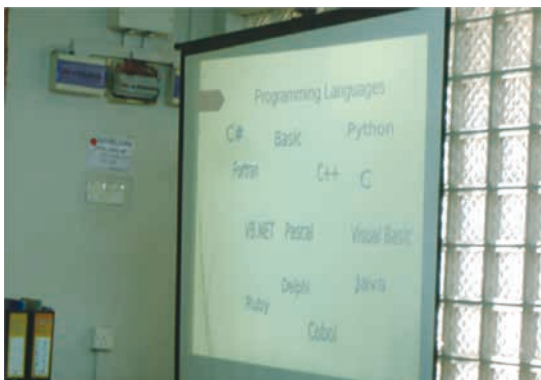


図-3 授業で提示されていたスライド



図-4 コンピュータ教室：Bill Gates と Steve Jobs の写真が掲げられていた



図-5 一般の生徒(左側)はシンハラ語で討議しているが、右側の輪の生徒は英語で討議している

国内にいたまま外国の大学に入学でき、最終学年にはそれぞれの大学に留学するコースもあることを最も前面に出している。前述のように、スリランカ国内の大学の学生総定員は少ないため進学希望者の一部しか入学できない。そのような者のために外国の大学と提携したこのような機関がある。学部および修士レベルの、コンピュータサイエンス、IT、経営、ビジネスなどのコースがある(図-6、図-7)。

なお冒頭に記した、筆者が指導する留学生(調査当時)もかつてここで学んでいた。筆者の所属大学がこと特段の関係があるわけではなく、当該留学生がここで学んだ後に日本に留学し、その後筆者の所属大学の学部編入学試験を独自に受けたものである。

Mahinda Rajapaksa College

次に Mahinda Rajapaksa College を見学した。スリランカでは College とは単科大学や大学内の学部



図-6 Saegis Campus の授業(おそらく数学)の風景。なおこの部屋だけでは入りきらずに別の部屋にも受講生を入れて生中継していた



図-7 Saegis Campus 内のロビーに並んでいた、提携する各国大学の紹介

の意味でなく、Primary (5年)・Junior Secondary (4年)・Senior Secondary (2年)の次に学ぶところで、UniversityへはCollege (Collegiate)で2年間学んだあと入学する¹⁾。

この学校は情報設備およびその活用が進んでいるところとして紹介を受けた。2014～2015年に韓国からの援助で「ICT教室」が作られ、それに関するこの学校の先生への研修が同国の方が来訪して行われた。ICTに加えて数学・科学・地理・歴史、および英語・日本語・フランス語の授業に使われているとのことである(図-8、図-9、図-10)。



図-8 Mahinda Rajapaksa College の「ICT教室」とその壁に掲げられているパネル。韓国語で「先端 ICT 教室」とある



図-9 Mahinda Rajapaksa College の「ICT教室」の大画面ディスプレイに日本語学習の教材を表示したところ



また同校は、2017年にはMicrosoft Sri Lanka による同国西部州（首都スリジャヤワルダナプラコッテや最大都市コロンボを含む）対象のProject Smart Schoolによりシステムを整備し、Microsoft Showcase Schoolsに選出されている²⁾。

諸外国との比較調査研究

一般に外国との比較というと米国や西欧諸国にばかり目が向きがち（このことは必ずしも日本に限っ

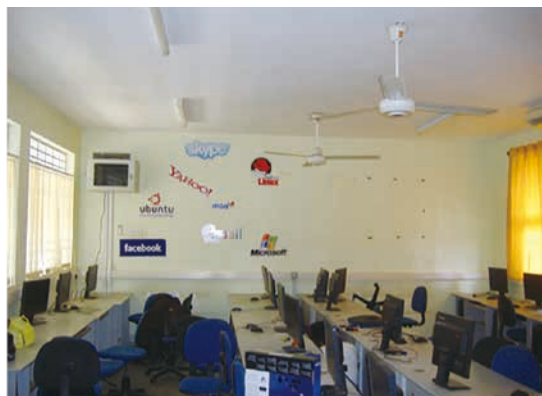


図-10 Mahinda Rajapaksa Collegeの別のコンピュータのある教室。壁には情報関係企業のロゴが並んでいる

たことではない)だが、世界の多くの国に目を向けた。今回、同国出身の留学生を初めて指導することになったという縁をとらえて、訪問しての国際比較調査を行った。高齢化が進んだ(だからこそ本来は力を入れなければならないはずの)日本とは、教育への熱の入れ方の違いを感じた。

今回、上記の3つの学校以外にも、University of Sri JayewardenepuraとMinistry of Educationを訪問し、同国の教育事情や教育政策についていろいろ伺った。それについては稿をあらためて報告したい。

参考文献

- 1) エディリシンハチャトリカ、和田 勉：スリランカの初等中等・一般情報教育と情報入試・検定、情報処理学会、コンピュータと教育研究会144回研究発表会、Vol.2018-CE-144, No.13, pp.1-5 (Mar. 2018).
- 2) Microsoft Asia News Center : Empowering Sri Lanka's Youth in the Digital Era with Microsoft (Nov. 2017), <https://news.microsoft.com/apac/2017/11/10/empowering-sri-lanka-youth-digital-era-microsoft/> (2020年1月11日閲覧). (2020年1月16日受付)

和田 勉（正会員） wadaben@acm.org

長野大学企業情報学部教授。本会初等中等教育委員会委員長。本会シニア会員、学会活動貢献賞受賞。2006年大韓民国高麗大学師範学部コンピュータ教育学科招聘教授。1978年早稲田大学理工学部電気工学科卒業、1983年筑波大学大学院数学研究科単位取得満期退学。

2020年度小中高教員新規入会キャンペーン【予告】

<https://www.ipsj.or.jp/member/kyoinwaribiki-2020.html>

受付開始までもうしばらくお待ちください



期間 2020年4月1日～6月30日

対象 小中高校（相当する教育機関を含む）に教職員として勤務されている方（現職）で、新規入会者の方に限ります

キャンペーン内容

1. 入会金（2,000円）が免除となります
 2. 正会員の2020年度の会費（10,800円）が半額（5,400円）に割引されます
- ※会員サービス内容は正会員と同じです

教員にとってのメリットとは

- 会誌「情報処理」が毎月読める
- 教員免許更新講習を会員価格で受けられる
- 中高生情報学研究コンテスト／Exciting Coding! Junior／初等中等教員研究発表セッションなど生徒向けや教員向けイベントを情報教育に活用できる
- 『情報』に関する豊富な知識を得ることができる
- 情報処理学会の教育委員会が発信するトピックスやパブリックコメントをいち早くキャッチできる





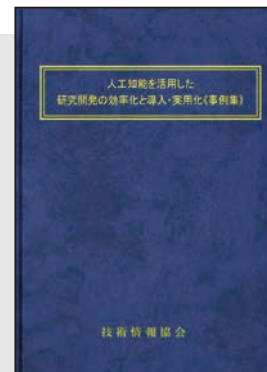
連載

ビブリア・トーク
— 書評 —

… 江谷典子 (Peach Aviation (株))

人工知能を活用した研究開発の効率化と導入・実用化《事例集》

(株) 技術情報協会 (2019), 514p., 80,000 円+税, ISBN : 978-4-86104-771-8



人工知能の実務書登場

人工知能の歴史を紐解くと、人工知能の誕生は、1943 年 Norbert Wiener が学際研究を提案するきっかけとなった論文『Behavior, Purpose and Teleology』の発表に起点があり、一般には、1956 年ダートマス会議で John McCarthy が「Artificial Intelligence (人工知能)」と命名したことが、人工知能の誕生とされている。この長い歴史の中で、今まで二度の人工知能ブームがあり、現在は 3 回目のブームとなっている。今度こそ、実務で役立つ人工知能の到来ではないかと思う。大衆的なテレビ番組にも「人工知能」という言葉が登場し、今や、人工知能はバズワードとなっている。人工知能というと、SF 映画、ロボット、人間のような頭脳、そして、将棋を連想する。「凄い」と思いつつ、業務に取り込むには縁遠いようにも思うことがある。人工知能の書籍というと、ディープラーニングなど手法の話がほとんどの中、人工知能システムを導入し、業務効率を上げている事例が多く掲載された実務書が登場した。

業務効率化のための AI 導入

具体的な取り組みを中心に、AI を業務に導入するまでの留意点や準備、人工知能の人材確保と教育、そして、革新的な技術を使わない手はないと数々の事例を掲載している。実務書らしく、興味深い点について、紹介する。

第 2 章「人工知能開発の見積もりと検収基準の考え方」では、従来のソフトウェア開発の見積もりと同様に、人工知能開発にも見積もり方法があることを説明し、人工知能開発の作業工程について、2 つの参考プロジェクト「為替の未来予測」「液晶文字認識による履歴保存」を取り上げて、具体的に解説している。

第 3 章「人工知能と知的財産、契約・法的留意点」では、人工知能システム開発者にとって、一番気にな

る法律や契約について説明している。学習済みモデル生成のためには大量の生データを元に作成した学習用データセットが必要となり、その際に第三者の著作物である生データ (文章、写真、静止画、動画など) を利用することも多くある。第 3 章では、著作権法の平成 30 年改正 30 条の 4 および 47 条の 5、個人情報保護法との関係、AI・データの利用に関する契約ガイドラインなどを解説している。

第 5 章から第 11 章まで、具体的な AI 導入による業務効率化の事例を紹介している。導入先として、研究開発、特許調査、営業業務、社内業務、人事業務、と幅広く紹介されている点が興味を引くと思う。その中で、「アイデア」を自動生成する創造的な人工知能 (第 5 章)、潜在ニーズを可視化し抽出する AI (第 5 章)、新規事業開発に AI を活用する方法 (第 5 章)、意思決定に人工知能を活用する方法 (第 6 章)、オープンソースを利用した画像認識でのデータ分析短縮の仕方 (第 7 章)、特許情報による技術動向分析の仕方 (第 8 章)、効率的に特許調査を行う方法 (第 8 章) など、は目新しく思う。第 12 章では、人工知能による予測・予知を活用する方法として、部品生産やプラント操業などの生産システムに用いる例、医薬品化合物の効能や副作用の予測が紹介されている。第 13 章では、サイバーセキュリティ対策における人工知能の活用と効率化について解説している。

現在、次の URL で試読ができるので、ひとまず、アクセスしてみて、この盛り沢山の内容を見ていただきたい。実務家の方々や人工知能システム開発の専門家を目指す方々には、お薦めしたい。

https://www.gijutu.co.jp/doc/b_2037.htm

(2019 年 11 月 25 日受付)

江谷典子 (正会員) kerotan@kcn.ne.jp

2001 年 3 月奈良先端科学技術大学院大学情報科学研究科博士後期課程修了。博士 (工学)



Mark Weiser : Program Slicing

International Conference on Software Engineering, pp.439-449 (1981)

プログラムスライシングとは

実社会で使われるプログラムの多くは、数百万行あるいは数千万行に及ぶ命令から構成されている。そのような巨大なプログラムに何か機能を付け加えたり、誤った動作を修正したりといった変更を加えるとき、開発者はプログラム全体を完全に理解した上で作業を行っているというわけではない。開発者は作業に関係のある動作、たとえば特定のデータを計算する手順に関連する命令だけを抽出して分析し、その部分的な理解に基づいてプログラムに適切な変更を加えている。

プログラムスライシングとは、開発者がプログラムから興味のある動作に対応する命令だけを抽出する操作のことである。今回取り上げる論文は、プログラムスライシングという概念を定義し、コンピュータに実行させるためのアルゴリズムを与えた。さらに、スライシングによって得られる部分プログラムが開発者の頭の中にもあること、つまり開発者がプログラムから読みとっているのと同じ情報であることを被験者実験で確認した。開発者がプログラムから読みとる意味的なまとまりを自動的に抽出する技術として、ソフトウェア工学分野の中でもプログラムの理解やテスト、デバッグなどのソフトウェア開発に関する作業支援の発展につながった論文である。

スライシングの計算

スライシングは、与えられたプログラム P から、開発者が注目する動作だけは同一であるような最小限の部分プログラム（以降スライスと呼ぶ） P' を取り出す操作である。ここでの「開発者が注目する動作」は、具体的には開発者が指定した変数集合 V が、指定した文 s の実行時に保持している値として表現する。開発者がデバッグ作業を行っているとして、プログラム文 s に到達するたびに変数集合 V の値を観測するとき、プログラム P とスライス P' から同一の観測値の列が得られる。小さな P' が得られると、 P をそのまま読むよりも読解にかかる労力を削減することができる。

図-1 にスライシングの例を示す。左側のプログラムは、変数 x, y を1行目で読み込み、それらの

1: read(x, y);	1: read(x, y);
2: max = x;	2: max = x;
3: min = x;	
4: if (x < y)	4: if (x < y)
5: max = y;	5: max = y;
6: else	
7: min = y;	
8: write(max);	8: write(max);
9: write(min);	

2つの数値の大小を
比較するプログラム

8行目での max の値を
基準としたスライス

図-1 プログラムスライスの計算例

値の大きいほうを変数 max に代入し、小さいほうを変数 min に代入して、8 行目と 9 行目でそれぞれの値を出力する。このプログラムにおいて、8 行目における max の値に注目したスライシングを行った結果が右側のプログラムである。x, y としてどのような値が入力されても、x の方が大きいときは 2 行目の代入結果が、y の方が大きいときは 5 行目の代入結果が 8 行目で出力されるので、このスライスの変数 max の値の計算という動作を保存した最小限のプログラムである。

スライシングの実際の計算は、プログラムの中での変数の値の受け渡しと条件分岐に基づいて、スライスに含まれている文の実行に影響する文をすべて特定しスライスに含めていく形で行われる。図-1 に示したプログラム例の場合、まず、注目する 8 行目をスライスに含めるところから計算を開始する。8 行目の max の値は、2 行目あるいは 5 行目のどちらかで代入されるものであるから、両方の行をスライスに含める。2 行目を実行するには変数 x, y の値が必要となるので、1 行目もスライスに含める。5 行目の命令を実行する必要があるかどうかは 4 行目の if 文によって決まるので、4 行目もスライスに含める。4 行目で使用する変数は、すでにスライスに含まれている 1 行目から得られているので、スライスに含める必要がある文はこれ以上増えず、スライシングが完了する。

開発者はスライスを覚えている

開発者が実際にスライシングを頭の中で行っていることを示すために、21 人の被験者と 100 行程度のプログラム 3 つを使用したデバッグ作業の実験が行われた。この実験では、被験者がプログラムのデバッグを行った後に、以下の 5 つのプログラム断片を提示し、それがプログラムの中で使われていたと思うかどうかを質問した。

1. バグの原因個所を含むようにプログラム内で連続した 10 行を取り出したもの。
2. バグの原因個所を含まないように連続 10 行を切り出したもの。
3. バグの症状が観測されている出力文に関して計算したスライス（元のプログラム上では不連続な命令群）10 行を取り出したもの。
4. バグの症状とは関係ない文、変数に対して計算したスライス（元のプログラム上では不連続な命令群）10 行を取り出したもの。
5. 3 ～ 4 行間隔でプログラム内から不連続な 10 行を取り出したもの。

図-2 がそれぞれのプログラム断片に対して 63 回（21 人×3 プログラム分）行われた質問に対して得られた「使われている」「たぶん使われている」という回答の件数をまとめたものである。実際にはす

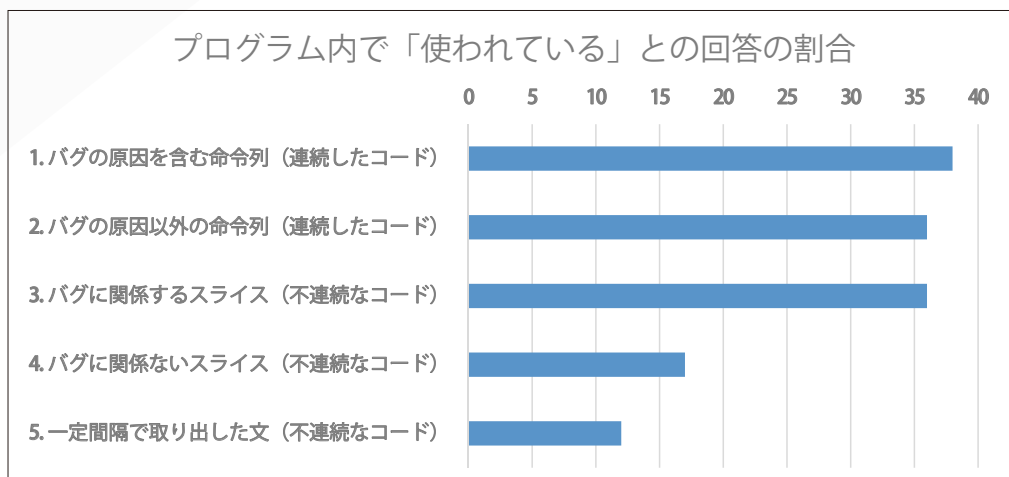


図-2 被験者実験の結果。Weiser, M.: Program Slicing, ICSE 1981 掲載の Figure 6 を筆者が書き直したもの

すべてのプログラム断片がプログラム内で使われているのだが、1, 2, 3の断片に対してはプログラム内で使われているとの認識が過半数を占める一方、4, 5の断片に対しては使われていないとの認識が多数となっている。3, 4, 5の断片はプログラムから不連続な文を取り出したという点が共通しているが、被験者が3だけを記憶していたということは、被験者がデバッグに際して特定の変数に対してだけスライシングを頭の中で行っていたのであろうと論文では述べられている。

プログラム解析技術の開発支援への応用

スライシングの計算に使われる変数の値の受け渡しや条件分岐の解析は、データフロー解析や制御フロー解析と呼ばれ、元々はコンパイラなどの言語処理系で利用される技術であった。この論文は、それらの技術が開発者の作業支援にも有効であるという新しい用途を提示した。論文では、さらに、複数の変数に対して個別にスライシングを実行した結果から、複数の変数にかかわる重要なプログラム文を自

動的に特定したり、プログラムの中に異なる計算が混在している度合いをプログラムの複雑さの指標として計測したり、スライスとして分解されたプログラム群を並列に実行することで計算速度を向上したりと、スライシングのさまざまな応用の可能性についてもアイディアが述べられている。多くの研究者がこれらのアイディアに影響を受け、現在もスライシングの応用の一種として提案手法を説明する新しい論文が発表され続けている。そうして開発された技術が、たとえば変数の不適切な使用を自動的に指摘するなど、プログラムの動作を分析して開発者に提示する現代のソフトウェア開発環境の中にも組み込まれているし、これからのソフトウェア開発を支える新たな技術の登場にもつながっていくであろう。

(2019年12月30日受付)

.....
石尾 隆 (正会員) ishio@is.naist.jp

2006年大阪大学大学院情報科学研究科博士後期課程修了。同年日本学術振興会特別研究員 (PD)。2007年同大学院情報科学研究科助教。2017年奈良先端科学技術大学院大学情報科学研究科准教授。2018年同大先端科学技術研究科准教授。博士 (情報科学)。プログラム解析、プログラム理解に関する研究に従事。



● 論文誌ジャーナル掲載論文リスト

Vol.61 No.3 (Mar. 2020)

【特集：若手研究者】

- 特集「若手研究者」の編集にあたって 谷口倫一郎
- テストケース生成のためのシステム仕様書の論理記述変換アルゴリズム 青山裕介 他
- 機械学習を用いた薬物売買におけるサイバーパトロールシステムの開発 安彦智史 他
- 自律型アオコ除去システム 荒井研一 他
- 動的解析を利用したフィッシングサイトのアクセス妨害機能の実態解明 小寺博和 他
- 実攻撃の観測と疑似攻撃の試行に基づくホームネットワークセキュリティの検証 藤田 彬 他
- TCP コネクション数と継続時間に基づく Slow HTTP DoS 攻撃に対する防御手法 平川哲也 他
- 標的型メールにおける心理操作テクニックと性格特性および行動特性との関係性分析 西川弘毅 他
- 音声認識エンジンに独立な特定ドメイン向け音声認識誤り識別器 田中 拓 他
- Q&A システムにおける回答意欲を向上させるための バーチャルエージェントデザインツール 尹 浩 他
- A Guidance and Visualization of Optimized Packing Solutions Techasartikul Nattaon 他
- 変調光照明を用いた違法写真撮影判定手法の提案とその評価 宇野耕平 他
- ジェスチャ認識システム構築に向けたセンサ配置およびデータ収集支援ソフトウェアの開発† 齋藤彩音 他
- プログラミング教育における実績可視化システムの提案と評価 華山魁生 他
- 集団対戦型フィールドスポーツの戦術適用判断の支援環境—バスケットボールのオフense基本戦術— 箭野 柊 他
- 中国伝統医学 (中医学) 情報共有支援のための証問の関係モデル化手法 五十嵐文 他

【特集：IoT 活用のためのインターネットと運用技術】

- 特集「IoT 活用のためのインターネットと運用技術」の編集にあたって 今泉貴史
- Serverspec : 宣言的記述でサーバの設定状態をテスト可能な汎用性の高いテストフレームワーク 宮下剛輔 他
- Monitoring of Servers and Server Rooms by IoT System that can Configure and Control its Terminal Sensors Behind a NAT using a Wiki Page on the Internet Takashi Yamanoue
- The Equal Deepest Vertex First Reboot : Rebooting Network Edge Switches in a Campus Network Motoyuki Ohmori 他
- 複数の予測期間に応じた海産養殖に資する海水温予測アルゴリズムの提案と実装 奥野聖人 他
- A Zero-day Malicious Email Investigation and Detection Using Features with Deep-learning Approach Sanouphab Phomkeona 他

- 特定の IoT 機器の WebUI を狙ったサイバー攻撃の分析

藤田 彬 他

- Social media data mining for proactive cyber defense

Ariel Rodriguez 他

【一般論文】

- CoW 機能を考慮した OFF2F プログラムのページ例外処理の評価* 谷口秀夫 他
- Examination and it's evaluation of preprocessing method for individual identification in EEG* Masato Yamashita 他
- 多声音楽の演奏楽器を認識するための畳み込みニューラルネットワーク* 佐藤佑樹 他
- 「かわいい」画像を用いた行動誘引によるセキュリティ警告の効果改善* 皆川 諒 他
- 図形の構造を考慮した絵描き歌自動生成システム* 久野文菜 他
- 布圧力センサを用いた褥瘡予防教育支援システム 小野瀬良佑 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. 2020)

【論文誌 数理モデル化と応用 Vol.13 No.1】

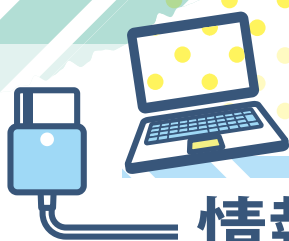
- 多値文書分類のための情報理論的基準による 2 元符号語表の構成法 雲居玄道 他
- 狭い 16 ビットのスケッチを用いた高速最近傍検索 樋口直哉 他
- 外来患者の待ち時間の分布関数による評価とその診療予約枠の人数決定問題への応用 市原寛之 他



【Transactions on Bioinformatics Vol.13】

- Lightweight convolutional neural network for image processing method for gaze estimation and eye movement event detection Joshua Emoto 他





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を意識した授業をしよう！ —紙飛行機制作を通し情報デザイン・ データサイエンスに取り組む—

岡本弘之 | アサンプション国際中学校高等学校

情報Ⅰに向けて

2017年の学習指導要領の改訂により、情報科の必修科目は「社会と情報」「情報の科学」の選択必修から、新しく設定される「情報Ⅰ」に再編され、内容も高度化している（表-1）。

表-1のように情報Ⅰは、1章では問題解決、2章では情報デザイン、3章ではプログラミング、4章

ではデータサイエンスがそれぞれの柱となっている。この中で3章のプログラミングのみが注目されているが、情報デザイン、データサイエンスについても、現行の教科書にはあまり記載がなく、高校の現場では「どのような授業をすればいいのか？」という不安も強い。このような現状から、本稿では情報Ⅰの実施を見据えて同僚教員と2019年度に実践した「紙飛行機制作のプロジェクト学習」を紹介する。

■表-1 情報Ⅰの構成内容（学習指導要領より）

- | |
|-----------------------|
| (1) 情報社会の問題解決 |
| ①情報とメディアの特性 |
| ②法規や制度・情報セキュリティ・情報モラル |
| (2) コミュニケーションと情報デザイン |
| ①コミュニケーション手段の特性 |
| ②情報デザインの役割 |
| (3) コンピュータとプログラミング |
| ①コンピュータの仕組み |
| ②アルゴリズム・プログラミング |
| ③モデル化とシミュレーション |
| (4) 情報通信ネットワークとデータの活用 |
| ①情報通信ネットワークの仕組み |
| ②データの収集・整理・分析 |

授業実践

授業の概要

授業は高校2年生の選択科目「選択情報（2単位）」で2019年度に実践した。「よく飛ぶ紙飛行機を制作する」ことをテーマに、生徒たち自身で決めた4～5人のグループで以下の流れで展開した。

①よく飛ぶ紙飛行機の作り方を調べて、オリジナル



の紙飛行機を設計する（問題解決）

②制作を他グループに依頼するための手順書を作成する（情報デザイン）

③実際に飛ばしてみた距離を計測し分析する（データサイエンス）

④分析結果をもとに紙飛行機を改善し、結果をプレゼンテーションする

授業の流れ①～③の（ ）内は対応する情報Ⅰの分野であり、これを1学期に実践した。

授業の展開

よく飛ぶ紙飛行機を設計する（1時間）

最初に授業の全体の流れを説明し、生徒たち自身で4～5人のグループを作らせた。最初の時間の目標である「よく飛ぶ紙飛行機」を設計するための情報を、インターネットのWebページから調べたり、実際に折ってみて飛ばしてみたりしながら、グループで設計する形を決めてワークシートに記入させた。図-1は本時の授業の流れと、授業時の生徒の様子をまとめたものである。

制作依頼するための手順書作成（2時間）

設計した紙飛行機は自分のグループで制作するのではなく、他グループに手順書だけを渡し、制作してもらうこととした。口頭で説明することも禁止し、依頼は1回だけとした。これにより手順書の役割が大きくなり、相手に正確に伝わるように手順書を書かなければ、自分たちが設計した紙飛行機の形が再現できない状況を作った。

生徒たちはまず制作手順を分解し、ワープロソフトで手順を入力、印刷して制作依頼を行った。依頼を受けたグループは、受け取った手順書を元に同じものを3機制作し、依頼をしたグループに渡した。図-2・図-3は生徒が作成した手順書の例である。

生徒の様子を観察すると、他グループからの依頼を受けての制作なので、間違いがないように複数人で確認しながら丁寧に制作していた。その一方「やや真ん中ってどこ?」「文字だけでは分からへん!」「書いてないけどたぶんこうじゃない?」と指示が曖昧な手順書に対し、苦勞する姿も見られた。

飛んだ距離を計測し分析する（3時間）

最初の1時間を計測の時間とし、講堂で授業を行った。生徒たちは他グループに制作してもらった紙飛行機3機を持ち、1機につき10回の計30回講堂の

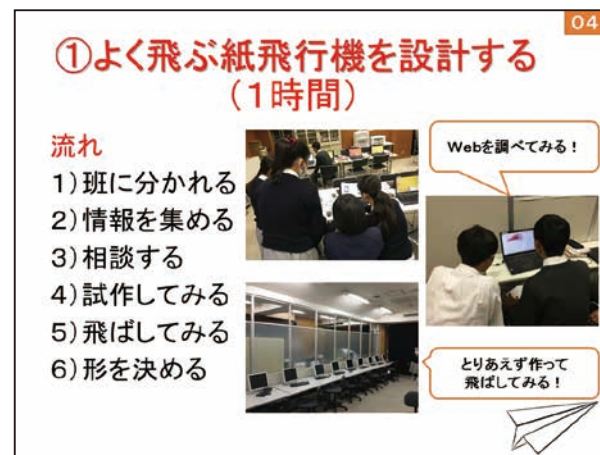


図-1 授業の様子（筆者発表スライドから）

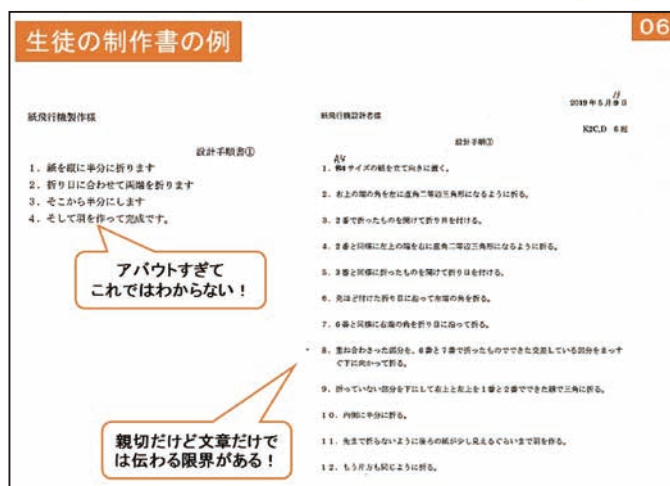


図-2 生徒が作成した手順書（分かりにくい例）

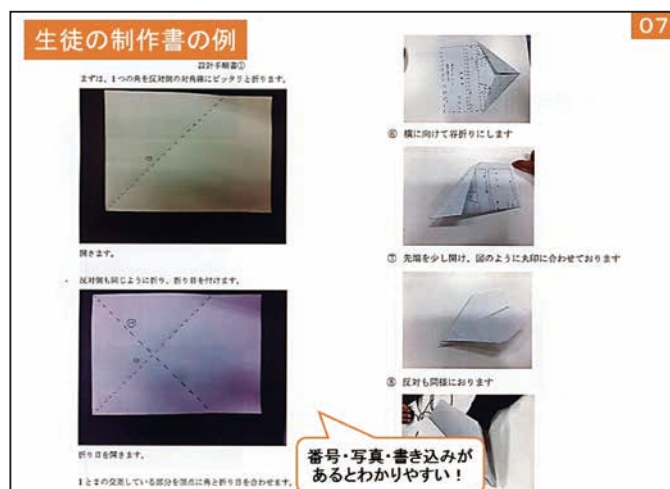


図-3 生徒が作成した手順書（分かりやすい例）

端から飛ばし、メジャーで計測して配布したワークシートに記録した。図-4はその授業の様子である。

次の2時間はデータ処理の時間とした。配布した表計算ソフトのシートにデータを入力し、授業者の指示のもと関数を入力し、平均値・中央値・標準偏差を求めた。その上で数値の意味、平均値・中央値であれば「だいたいどれくらいの距離を飛んでいるか」を表し、分散・標準偏差であれば「機体の安定度を見るための飛距離のばらつき」を見ることができることを授業者から説明した。これらのデータを元に、グループで相談してデータを分析し、3機の紙飛行機の性能の比較や、飛距離の分布をグラフで表した上で、個人で考察しワークシートに記入させた。考察では機体だけでなく投げ方・投げる人など結果に影響を与える他の要素への気づきを書く生徒もあった。

図-5は授業で使ったシートと、授業の流れである。



図-4 計測の授業の様子

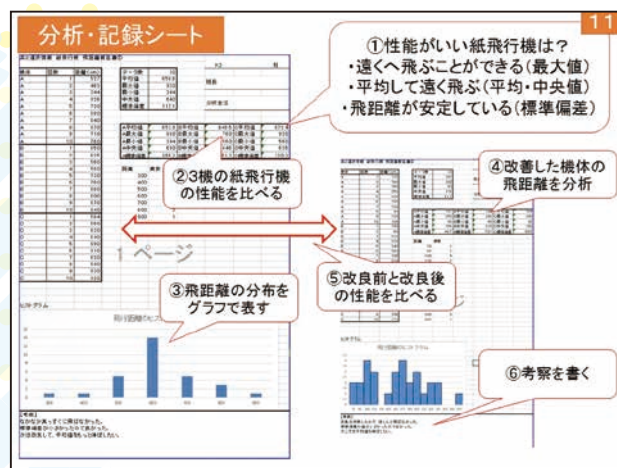


図-5 分析・記録シートと授業の流れ

改善した結果をプレゼンする (5 時間)

この後授業は、紙飛行機の改善に進んでいく。前半2時間は改善の時間で、1回目と同様に改善機の手順書を作成し、他グループに制作を依頼した。

図-6は改善点を説明した生徒が制作したスライドの例である。2回目の手順書では、1回目の経験をもとに、手順を細かく書いたり、写真を撮影して入れたりと書き方や内容に進化が見られた。完成した機体を前回と同様に講堂で飛ばして計測し、1回目と同様の分析を行った。

後半3時間は改善経過と結果・分析について報告するスライドを制作し、クラス全員の前でプレゼンテーションを行った。図-7は改善前と改善後の結果を考察したスライドである。

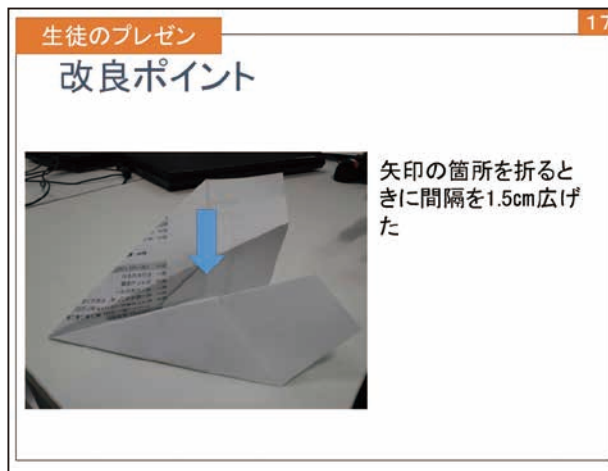


図-6 生徒のプレゼンスライド (改善の説明)

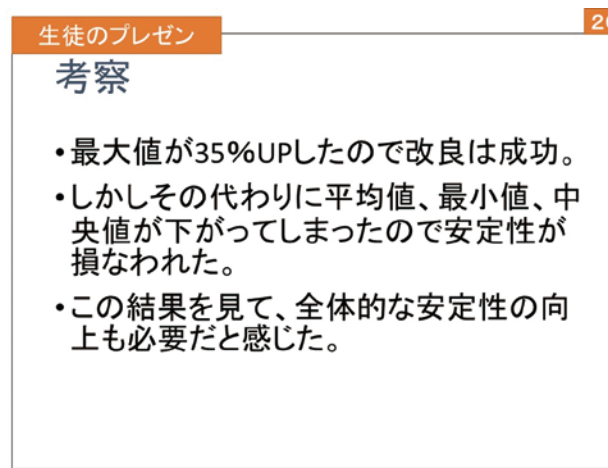


図-7 生徒のプレゼンスライド (結果の考察)

授業実践の振り返り

問題解決の授業の視点

情報科学学習指導要領解説では「情報と情報技術を活用して問題を発見・解決する学習活動を通して、問題を発見・解決する方法を身に付けるとともに、(中略) 情報と情報技術を適切かつ効果的に活用して問題を発見・解決し、望ましい情報社会の構築に寄与する力を養う。」¹⁾と書かれている。

本実践は「よく飛ぶ紙飛行機を作る」という問題解決を目指し、「情報収集→提案→実行→改善・振り返り」と体験的に問題解決の手順を学ぶことができた。特に提案で終わりではなく、実行・改善までできる課題であった。

情報デザインの授業の視点

学習指導要領解説では「目的や状況に応じて受け手に分かりやすく情報を伝える活動を通じて、(中略) 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を身に付けるようにするとともに、コンテンツを表現し、評価し改善する力を養うことをねらいとしている。」¹⁾と書かれている。

本実践で情報デザインの課題とした手順書の制作は「見た目のきれいさ」というアートな視点になりやすく、純粋に伝わりやすさを考える課題に適している。また伝える・読みとる双方の立場を体験することで、「正確に情報を伝えるにはどうすればいいか」を実感して考えることができた。

データサイエンスの授業の視点

情報科学学習指導要領解説には「データを表現、蓄積するための表し方と、データを収集、整理、分析する方法について理解し技能を身に付けることでは、データを問題の発見・解決に活用するために、ファイルとして蓄積するためのデータの様々な形式、データを収集、整理、分析する一連のデータ処理の流れ及びその評価について理解するようにする。」¹⁾と書かれている。

本実践では生徒自身で収集したデータを分析することで生徒の関心を引き出すことができた。「よく飛ぶ」「安定して飛ぶ」ことを分析する指標として、平均値・中央値・標準偏差の意味など統計的知識も取り扱うことができた。

情報Ⅰの授業に向けて

本実践では情報Ⅰの内容を取り入れて授業を企画してみたが、これらの経験をふまえ、情報Ⅰに向けて次のような点を考慮することを提案したい。

- ①問題解決の授業については、発表して終わりではなく、実際に制作・実行させて評価、改善ができる内容の方がより実践的な内容となる。
- ②情報デザインの授業では、制作して終わりではなく、本当に伝わるかを試せる題材がよい。そのために情報の発信・受信の双方の立場を体験し、生徒同士の作品から学ぶ授業を提案する。
- ③データサイエンスの授業では、分析するデータが自分たちで計測したデータや身近なデータである方が興味を高めることができる。相関・回帰といった内容も含んだ授業を提案したい。

このように実践をしてみてもの気づきを書いてみたが、私自身もまだまだ試行中であり、情報Ⅰの実施に向けて今後も授業を工夫していきたい。私の取り組みについては次の Web サイトで公開している。「情報科の授業アイデア」<https://www.okamon.jp>

参考文献

- 1) 文部科学省：高等学校学習指導要領解説 情報編，開隆堂出版 (2019)

(2019 年 12 月 28 日受付)

岡本弘之 okamoto@assumption.ed.jp

京都教育大学大学院連合教職実践研究科修了，アサンブション国際中学校高等学校教頭。

連載

★ Jr.

先生、質問です！



素朴な質問に対してお2人から異なる観点で回答いただきました！ また、2月号の当コーナーを読んだ読者の方から関連質問をいただきました。末尾にて回答募集しております！！



匿名希望
(公開質問)

情報は地球を何秒で周りますか？

Q

情報は地球を何秒で周りますか？ってすごく面白い質問ですね。まずは「地球を周る＝情報にアクセスできる人口のX%」と定義してみます。情報の広がりや病気の感染と似た数理モデルで予測できるようです。いくつかのモデルがありますが、取り得る状態を「情報を知っている状態」と「情報を知らない状態」の2つのみに定義してみると次の式のようにモデル化できます(SIモデル)。

$$y' = a(w - y)y$$

式中では y , a , w はそれぞれ情報を知っている人数、情報の伝わりやすさ、全人口を意味しています。情報を知っている人が少ない初期期間はゆっくりと情報が伝播し、ある程度の人を知ってくると伝播速度が急上昇します。噂の広がりに関する過去の研究¹⁾では全人口の90%以上が知っているときを「蔓延状態」と定義していたので、 $y = 0.9w$ となるまでの時間が「情報が地球を周る時間」と言えそうです。また、フェイクニュースに関する過去の研究²⁾では「嫌悪、驚き、恐怖」といった負の感情の方が伝播やすいと報告されているので、式中の a はニュースの感情特徴量で表現できそうですね。

参考文献

- 1) 蛭川 繁 他：うわさの伝播モデル，情報処理学会論文誌，Vol.41, No.2 (Feb. 2000).
- 2) Vosoughi, S. et al. : The Spread of True and False News Online, Science, Vol.359, Issue 6380 (2018).

A



田脇裕太
慶應義塾大学

本企画の問合せ先

新世代企画委員会／会誌編集委員会 「先生、質問です！」係 E-mail: sensei-q@ipsj.or.jp



鬼塚 真

【正会員】

大阪大学

A

情報は電気信号（あるいは光の信号）として、インターネットや携帯電話などの通信ネットワークを経由して、世界に送ることができます。信号を送るスピードは光のスピード（地球を一周するのに 0.13 秒、アメリカと日本の間だと 0.036 秒）と同じなので、きわめて高速に送れるような気がしますが、実際には情報を送る側と受け取る側で情報を送る前に準備が必要で、さらに送る側と受け取る側の間の中継地点でも情報の仕分けが必要です。インターネットの平均的な応答時間は 0.2 秒程度だそうです。それでも速いですね。一方で、情報が伝わることによる影響の大きさを考えると、最も分かりやすい例の 1 つに株価変動があります。日本の株は全世界の人たちが購買しています。この場合は情報が世界を周るというよりも、世界の人々が東京の証券取引所にアクセスするということになります。これまで株の売り買いは人がコンピュータを使って行っていました。最近ではコンピュータが自動判断して株の取引を行う時代になりつつあります。現在の技術では、1 秒間におおよそ 100 万人分の取引処理を行うことができるので、まさに「時は金なり」の時代と言えますね。

「先生、質問です！」への質問方法

▶ **メールで質問**：下記を記載し、E-mail: sensei-q@ipsj.or.jp にメールを送信ください。

(1) 質問 (必須) (2) 名前 (任意) (3) 区分 (必須)：小学生／中学生／高校生／高専生／大学生／大学院生／社会人／その他・無回答 (4) 会員種別 (必須)：ジュニア会員／学生会員／正会員／非会員 (5) 連絡用メールアドレス (任意)

▶ **Web から質問**：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！」質問募集のお知らせ <https://www.ipjs.or.jp/magazine/sensei-q.html>



▶ **Twitter ハッシュタグで質問**：「#IPJS 先生質問です」とハッシュタグをつけてツイートしてください。

※より多くの方が抱えている疑問と判断された質問を優先的にピックアップさせていただきたいと考えております。

「先生、質問です！」への回答募集

▶ **公開質問**：3. 人の魂？を人からロボットに移すことは理論上可能（実用には十数年かかる）とのことですが、人から人へ、『転校生』や『君の名は。』みたいなことも十数年後には可能になるのでしょうか

300 ～ 500 字程度でご回答をお待ちしております。なお、一部加工の上掲載させていただく可能性がありますので、あらかじめご了承ください。

▶ **Web から回答**：下記の Web ページ内の回答フォームから回答をご記入ください。

<https://forms.gle/GkwomeBhz8ftgynR7>



その7 VR センター三銃士に会ってきた! どうなる VR の未来!?

漫画: 山本ゆうか (Twitter @ymmxo)



取材してほしい人・イベントなどを募集中!

Twitter ハッシュタグ: #IPSJ_IT 紀行 / メールアドレス: editj@ipsj.or.jp

1989年 (VR第一世代)	2000年 (VR第二世代)	現在
1987年 EyePhoneと DataGlove登場 ぼくは VR第一世代 雨宮先生は VR第二世代 1989年 「バーチャルリアリティ」 という言葉が誕生	2000年ごろ アナトール・レクイヤー博士による 疑似触感の論文が発表される マウスカーソルが だんだん動かなくなる 腕に力を入 れてしまう 心で感じるのと 物理学で感じる のは違う	HMDが安価になり普及 VR VRCENTER 2018年 東大VRセンター設立
部屋全体をプロジェクトで囲むなど 現実をそのまま写しとろうとする	VRと心理学をうまく組み合わせ コンパクトに体験できる	
3D CADでのモック作成など 製造業で多く利用される	エンターテインメントに 利用される	

私は人間の感覚器に 興味があるんです ぶるなび VRセンターでの 成果ではないの ですが... これを持って みてください	引っ張られ ます 部品が回る たびに前に 引っ張られる 感覚 ...と思う でしょ?	錯覚を利用して 引っ張られる感じを 作っているんです 物理的には 振動している だけが 牽引力を 感じた!! 地図アプリとの連動 などいろんな使い方 ができそうです
ぼくはブレイン・ コンピュータ・インタ フェースの研究が したくてここにいます 電気刺激で 脳を直接刺激 またボタンを 押したくなる	前庭電気刺激を 体験したことが あります! 電気が流れると 首を傾けて しまう!! ええ!!	今でも手に インプラントとか あるしな... VR第3世代では 神経を直接刺激する ようなものが 出てくるかもね ピアス型の 電極なんて できたりして!
ただ 未来予測は 直近で外れる からなあ という...?	昔の新聞に載った 20世紀の予測だと... 予想 空とが 戦艦 実際 ミサイル メイン戦力が 空を飛んでいる ところまでは 合っている ね 直近で外れてる でしょ?	あと この予測には コンピュータが一切 出てこないんだ 概念的にないものは 予想できないからね
		VRがそういう ものになったら 面白いよね



会議レポート

ASE 2019 参加報告

—自動化ソフトウェアエンジニアリングに関するトップクラスの国際会議—

ASE 2019 について

34th International Conference on Automated Software Engineering (ASE 2019) は、IEEE と ACM が主催するソフトウェア開発の自動化技術についての国際会議である (図-1)。ソフトウェア工学分野では、最も権威のある International Conference on Software Engineering (ICSE) に次ぐレベルの会議として知られている。

開催地は米国サンディエゴ、開催期間は 2019 年 11 月 12 日～14 日の 3 日間で本会議が行われ、その前後の日に併設ワークショップが開催された。参加者は 36 カ国から 450 名以上が集まり、そのうち 66.9% は初参加者で、40.5% は学生である。

本会議では研究論文、デモ、既発表論文 (Journal First Presentations) といったトラックのほか、今年から企業向け発表 (Industry Showcase)、最新成果発表 (Late Breaking Results) などのトラックが追加された。研究論文トラックでは 437 件の投稿に対し、採択論文数は 91 件 (採択率 20.8%) であり、非常に競争率の高い状況であった。プログラムの各セッションの構成はトラックごとではなく、研究トピックごとにまとまっており、それぞれのトラックで採択された論文・発表が混ざっている。そのため、1 つのセッション内で大学での純粋な研

究から企業における研究成果の活用まで多様性のある発表を聞くことができた。

基調講演

基調講演は本会議の各日に行われた (図-2)。講演者は大学から 2 人、企業から 1 人と、ここでも多様性のバランスが考慮された構成となっていた。

初日の基調講演は University of California, Los Angeles の Miryung Kim 教授によるビッグデータ解析のためのソフトウェア工学に関するものだった。講演の前半は、マイクロソフト社の 500 人以上のデータサイエンティストの技術的背景や得手不得手について調査して、9 つのクラスタに分類した研究成果が紹介された。後半では従来型のソフトウェア開発の手法が通じなくなるビッグデータ解析を用いたソフトウェア開発のテスト・デバッグ技術について紹介された。これらは近年注目が集まっている機械学習のためのソフトウェア工学における課題と根は同じで、会場における注目度も高かった。

2 日目は地元の大学である University of California, San Diego の Yuanyuan Zhou 教授による講演で、インフラ管理・設定における誤りに着目し、どのような誤りが起きているかの調査を行うことで、誤りを減らすための設計指針を考案した研究に関するものであった。インフラ管理・設定における誤りは、54.1% の設定パラメータがほとんど使われていないほど数が多く複雑で、そのため多くの設定パラメータがデフォルトのままにされていることが原因の 1 つであるなど、興味深いデータとともに、パラメータ設定の設計についての重要性を感じさせられた。

本会議最終日の講演ではゲーム開発会社である Ubisoft Montreal の Mathieu Nayrolles 氏が、ゲームのデバッグにおいてソフトウェア工学の最先端の研究成果を導入している事例とこれから導入を検討している事例をいくつか紹介した。筆者も同じく企業に所属してソフトウェア開発技術の現場導入を行っているが、現場の課題とユースケースが合致しないことやツールの成熟度の問



図-1 ASE 公式キャラクタの Nova と Vector ☆¹



図-2 基調講演の様子 ☆¹

題などで導入のハードルが高いことをよく知っており、講演者の導入実績に非常に驚きを持った。

テクニカルセッション

テクニカルセッションは合計 150 件以上の発表があるため 3 並行で行われ、1 件の発表につき質疑込みで 20 分または 10 分を割り当てられている。テーマとしては、テスト・検証・デバッグといったものが多かったが、近年のこの分野の流行でもある深層学習を使った自動化や、深層学習アプリケーションのテスト・デバッグといったものが増えてきているのが特徴的であった。

研究論文トラックでは優秀論文賞 (Distinguished Paper Award) は 6 件が選出されており、そのうちの筆者が聴講できた 2 件をここで紹介する。

1 件目は Github で修正パッチを提供する場合などで用いられる pull request の 34% は修正内容などの説明を何も記述せずに送られているという課題に対し、過去のコミットメッセージやコード内のコメントをオートエンコードで学習することで、pull request の記述を自動で生成する研究である。既存の手法より良い評価であることが報告されているとはいえ、実用的にはまだ性能などで課題があるため、今後の発展に期待したい。

2 件目はオンライン格闘ゲームのテストに深層強化学習と進化計算を用いて自動化することで、商用ゲームの未知のバグを 3 件検出した研究である。ゲーム用の AI として強化学習を使う事例は多く見られるが、テストという観点においては、ただ対戦相手に勝つだけではなく、バグを見つけられるような探索的な振舞いも必要となる。この研究はその両方のバランスをとることを進化計算によって可能としている。会場ではツールによって検出された実際のゲーム中のバグの動画を再生し、聴衆の関心を集めていた。

そのほかに筆者が興味を持った発表としては、深層学習モデルのデバッグを再訓練ではなくパラメータを直接調整することで実現する研究があった。改善幅は 1 ~

2% 程度の精度向上と大きくないものの、新たなデータを必要としない方法として今後のベースラインになってくると考えられる。

ワークショップ／共催イベント

今回の ASE では 7 つのワークショップが開催された。初開催は 3 件あり、説明可能な (Explainable) ソフトウェアに関するもの、インフラや設定のコードに関するもの、AI に関するものなど、近年の話題となっているテーマを取り扱っていた。

また共催イベントとして、プログラム委員の会議を拡張して一般に公開をした Celebration of ASE 2019 というイベントや、米国 National Science Foundation (NSF) がスポンサーになっている招待制のワークショップが開催されたが、それらにおいても機械学習に関するソフトウェア工学の議論が行われていたようである。

ソーシャルイベント

ソーシャルイベントとしては、初日の夜に会場のホテル内でのレセプションや、2 日目の夜に貸切バスでの市内周遊とその後のビール醸造所でもあるレストランでのバンケットが開かれた。

本会議ではダイバーシティとインクルージョンに関する取り組みを非常に意識的に行っており、昼食やレセプションなどで ASE の初回参加者、女性参加者、マイノリティのためのイベントを用意し、交流を促進しようとしていた (図-3)。面白い取り組みとしては、バンケット後にカラオケ大会を企画しており、参加者の一部はカラオケでサンディエゴの夜を楽しんでいた。

所感・次回開催予定

筆者の所感としては、ソフトウェア工学の中でも中心的なトピックである自動化を扱っているためか、深層学習にかかわる研究を非常に多く目にしたが、成熟度としてはまだこれからという印象であった。

今回の ASE は 2020 年 9 月にオーストラリア・メルボルンで開催が予定されており、研究論文の投稿締切は 4 月中旬となっている。

ソフトウェア工学は今後ますます多様性を持つようになり、機械学習や自然言語処理といった他の分野からの参入が不可欠になってくるだろう。ぜひ、ソフトウェア工学分野の研究者にとどまらず、多くの研究者・開発者・実務家などに参加・論文投稿を検討いただければ幸いである。

(徳本 晋／富士通研究所)



図-3 昼食会場の様子^{☆1}

☆1 掲載写真はすべて ASE 2019 Official Photos より引用
<https://photos.app.goo.gl/53B8dpKXNdWJZeuk6>



会議レポート

IEEE/ACM SC19 会議参加報告

SCについて

SC (The International Conference for High Performance Computing, Networking, Storage, and Analysis) とは、IEEE および ACM が主催のスーパーコンピュータ関連技術を幅広く扱う国際会議で、毎年 11 月に約 1 週間北米で開催されており、31 年の歴史がある(図-1)。高性能計算分野におけるトップカンファレンスの 1 つで、メインラックの採択率は 23% である。また、論文発表に加えて、スーパーコンピュータの性能ランキングである TOP500 リストが発表されるほか、開発状況の共有やディスカッションのための BoF (Birds of a feather) セッションや、さまざまな企業や研究機関がブースを構える広大な展示フロアを有することが特徴である。来場者数は増加を続けており、日本からの参加者も多い。開催都市の中心部のホテルを確保することが難しくなるほどの状況であり、街自体が SC 一色になるといっても過言ではない。実際のところ、街を歩けば参加者を多く見かける上、近隣のホテルの会議室も打合せやイベントで占められている。研究者に限らずさまざまな職種の参加者がいることも特徴であり、関係者が一堂に会することから情報交換や商談の場としても機能している。

今回の会場はコロラド州デンバーの Colorado Convention Center であり、同都市における開催は 2 年ぶりであった。参加者数は 13,500 人を超え、3 年前と比較して約 2,500 名増加している。同会議は大規模であることから、各種ラ



図-1 1988 年の初回開催以降のハイライトを記したパネルが入り口付近に並べられている

ンキングや特徴的な展示を中心に紹介したい。

スーパーコンピュータの性能ランキング

TOP500

スーパーコンピュータの最大の価値は大規模な問題を短時間で解けること、すなわち演算の速度である。演算性能ランキングの 1 つである TOP500 リスト¹⁾は、LINPACK ベンチマークの実測性能に基づいて決められている。このベンチマークは、多元連立一次方程式を並列計算によって解く際の演算性能 (FLOPS: 1 秒あたりの浮動小数点演算回数) を測定するものであり、現時点では最も広く用いられている指標である。このランキングは、6 月と 11 月の年 2 回更新されており、後者が SC において発表される。すでに 30 年近くリストが更新され続けており、トップのマシンに関しては 10 年間でおよそ 84 倍の性能向上が見られる(図-2)。

2019 年 6 月に発表されたランキングと比較して、上位 10 システムの顔ぶれに変化はない。1 位は引き続き米オクリッジ国立研究所に設置された“Summit”であり、このシステムは IBM 社製の POWER9 CPU と、NVIDIA 社製の GPU (アクセラレータ) を用いている。上位 10 システムのうち 5 システムは 1 位システムと同様に CPU と GPU を用いており、これは直近数年で多く見られる構成である。このほか、Intel 社製の CPU のみを用いたものや、中国の“Sunway TaihuLight”のように独自プロセッサを用いたものがある。日本国内に設置されたスパコンに限ると、8 位に産業技術総合研究所の ABCI (AI Bridging Cloud Infrastructure) がランクインしている。

Green500

消費電力あたりの演算性能を評価するランキングとして、Green500 リストがある。実行するベンチマークプログラムは TOP500 リストで用いられるものと同じであるが、Green500 リストにエントリするには、システムの消費電力を測定する必要がある。測定された消費電力 (W) と演算性能 (FLOPS) により、1W (ワット) あたりの演算性能 (FLOPS/W) を求め、この値により順位を決定する。

今回の SC で発表されたリストでは、日本のスーパーコ

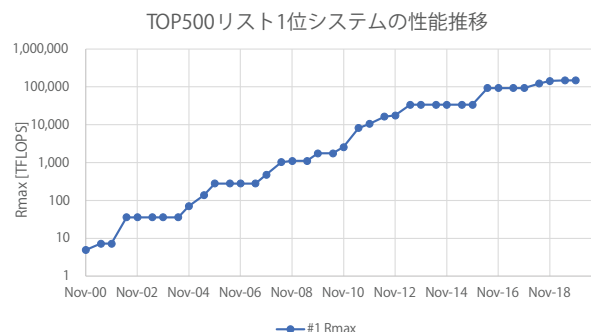


図-2 過去 20 年の TOP500 ランキングにおけるトップシステムの TFLOPS (テラ FLOPS) 値推移 (文献 1) に掲載されたデータから作成)

ンピュータ「富岳」のプロトタイプが初登場し、1位にランクインした。富岳は理化学研究所と富士通により開発が進められている次世代のスーパーコンピュータで、Armアーキテクチャを採用したCPUを使用しており、ベクトル拡張命令「SVE」や先端半導体プロセスにより、高い消費電力あたりの演算性能を実現している。

IO-500

IO-500とは高性能計算向けの高速度ファイルシステムのアクセス性能に関するランキングである。ファイルやディレクトリ情報といったメタデータ操作の性能と、データ転送の速度(帯域)を評価し、それにより順位を決定する。ランキングはベンチマークを実行するノード数に制限がないものと、10ノード(サーバ)に限定した場合の2種類がある。今回初登場かつ特徴的なエントリは、Intelにより開発されているDAOSである。DAOSは、ノード数に制限のないランキングでは2位であるが、10ノードの場合では1位であり、処理ノード数あたりの性能では他と比べて2倍近い差をつけている。これは、DAOSがDRAMスロットに接続するタイプの不揮発メモリを最大限活用する形で基本設計が行われていることが理由の1つであると考えられる。通常、分散ストレージシステムの内部では、ネットワークを介した通信とデータの永続化(ストレージへの記録)の両方が頻繁に行われることから、オペレーティングシステムの処理がオーバヘッドになりやすい。ところが、不揮発メモリを用いる場合、メモリ空間にマップされた領域がそのまま永続化されることから、従来の通信や入出力とは異なり、リモートのノードから直接データを転送(RDMA)し、そのまま永続化することが可能となる。この結果、処理負荷の大幅な削減につながり、性能が向上する。このように、新しいデバイスの使いこなし技術もSCにおける見どころの1つである。

特徴的な展示

膨大な展示の中から、特に印象に残った1つをピックアップする。米Cerebrasが、Wafer-Scale Engineと呼ばれる、半導体ウエハをそのまま切り出した大きさの機械学習向けチップ(図-3)と、そのシステムであるCS-1を展示していた。このチップは18ギガバイトのSRAM(スタティッ

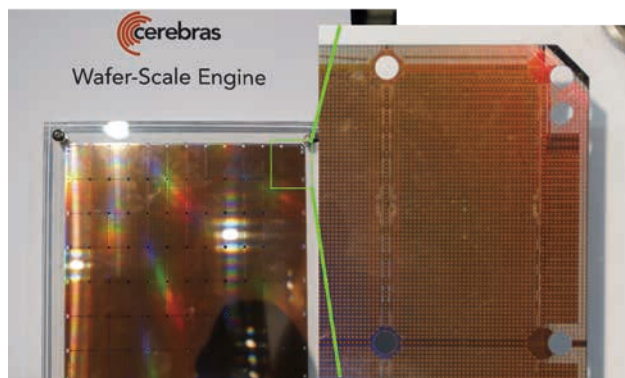


図-3 Cerebrasの機械学習チップ

クランダムアクセスメモリ)と40万のコアを有しており、TensorFlowやPyTorchといった機械学習フレームワークをサポートしている。

深層学習をはじめとする機械学習は、それだけでも需要が多いことから、このような専用ハードウェアが作られるようになりつつある。今後、汎用プロセッサの性能向上ペースが低下すると、用途特化による性能向上を目指すケースが増えてくると考えられるが、これはその良い一例であると言える。

基調講演

基調講演はNASAのSteven Squyres氏により行われた。SCの基調講演は多くの場合、高性能計算とは異なる分野の専門家を招待して行われる。今回は、火星探査機においてソフトウェア技術が果たした役割を中心に講演が行われた。火星探査機のソフトウェアは、打ち上げてから探査機が火星に到着するまでの間に開発されていることや、現地で発生した問題を画像処理や制御ソフトウェアの工夫により乗り切ったエピソードが紹介された。きわめてクリティカルな用途かつ一般化の難しい環境において、いかにソフトウェアを活用するかという点で、興味深い講演であった。

発表論文の傾向

冒頭でも述べたように、SCが扱う範囲はきわめて広い。直近数年で目立つようになったトピックとしては、機械学習の大規模化が挙げられる。スーパーコンピュータは高速なノード間接続ネットワークを備えていることから深層学習を並列実行するための環境として適している。そのため、深層学習をスーパーコンピュータで高速に実行するための研究や実証事例に関する発表も見られる。また、IO-500の節でも述べたように、不揮発メモリについても、本分野において活用するための検討が進んでいる状況であり²⁾、評価論文やユースケースに関する論文が見られた。

参加のすすめ

スーパーコンピュータは先進的かつ高性能なハードウェアと、それらを活用するためのシステムソフトウェア、高度にチューニングされたアプリケーションがすべて揃うことで、高い性能を実現している。さまざまな分野の知見が集まる会議であり、情報技術に携わる多くの方に参加をお勧めしたい。

参考文献

- 1) <https://www.top500.org/>
- 2) Weiland, M. et al. : An Early Evaluation of Intel's Optane DC Persistent Memory Module and Its Impact on High-Performance Scientific Applications. In The International Conference for High Performance Computing, Networking, Storage, and Analysis (SC'19), p.13 (2019). <https://doi.org/10.1145/3295500.3356159>

(大辻弘貴／株式会社富士通研究所)

会員の広場

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。まず、特別解説「大規模災害時に市民は情報にアクセスできたのか」については、以下のようなご意見・ご感想をいただきました。

■電気がない、機器がないといった状況での情報提供はどうすればよいのだろうか、情報の取得はどうすればよいのだろうか、あまりにも、当たり前情報機器が使えられていることに危機を感じた。
(匿名希望)

特集『AIの遺電子』に学ぶ未来構想術については、以下のようなご意見・ご感想をいただきました。

■今回の特集における13作品は、現在各作者の行っている研究が成熟し、社会に浸透したときに起こるであろう出来事を率直に描いたもので、各作者の頭の中を垣間見た気がした。(匿名希望)

■今回の特集の世界は予備知識がきわめて少ないので、読むのにも一苦労したし、あまり興味も持てなかった。若い人には面白いのだろうが……。
(匿名希望)

■たまにはこういう文章を読むのもいいなと思いました。「MICHU」の述べる「低コンフリクト社会」に似たものを自分でも考えたことがあります(文章にはできませんでしたが)。(井上勢大/ジュニア会員)

■自分は物語が好きなので、今回の話はとても面白かったです。今回のように、たまに漫画も入れてほしいです。
(匿名希望/ジュニア会員)

■趣旨は分かりましたが、読みにくいように思いました。(匿名希望)

■今回の特集とその内容は大変すばしかったです。こういった素晴らしい挑戦を今後も期待しておりますので、よろしくお願いいたします。
(竹原豊和)

■今回の特集は学術誌として画期的だと思います。一方、記事の多くは、「作者が研究者である」という属性はついていますが、内容は一般的なSF同人作品、という域を超えていないとも感じました。その中でも水野雄太先生の作品は、ご自身の研究との関連性について言及されており、学術誌の記事として一段上の出来であったと思います。
(匿名希望)

■図表がなく文字だけの物語系コンテンツについては、冊子よりもデジタルで読めばよかった(しかも縦書きがよい)。(匿名希望)

■一部は大変面白かったが、論文のように整理されたものではない上、必ずしも興味を引くような文章になっていないものもあり、それが10編以上も続くのはいまひとつであった。
(匿名希望)

■未来構想術は、試みとして大変興味深かったが、特に長文の記事は読むのに疲れてしまった。普段、SFを読み慣れていないせいだろうと思うが、2ページ程度にエッセンスをまとめてもらえるとよかった。
(伊藤雅樹)

■特集はとても興味深かったのですが、あまりにも話題が広範囲に及んでおり内容が薄まってしまい、消化不良のような気がしました。たとえば今後毎回各作品を深掘りする「小特集」を組んでみてはいかがでしょうか?
(滝内邦弘)

■今回の特集は面白かった。ある手法に則って、新しい未来像を描くというような企画は、これまでなかったのではないだろうか。これからも、既存の枠にとらわれない特集が組まれればよいと思う。
(匿名希望)

■大変面白かったです。『AIの遺電子』も読みました。(匿名希望)

「2.5. はだかの耳、虫の声」

■五感(今回は聴覚)を通じて人間を操作するというテーマ自体は面白いと思いました。
(匿名希望)

「2.11. 誰もが科学する未来の社会をソウゾウする」

■著者の研究との関連について言及があり、学術記事として価値があると感じた。
(匿名希望)

教育コーナー「べた語義」については、以下のようなご意見・ご感想をいただきました。

「100回の重さ」

■「第1回に記されています」「100回分の記事を読めばよく分かっていただけののでは」など、いかなものか。
(匿名希望)

会議レポート「ACM SIGIR 2019 参加報告」については、以下のようなご意見・ご感想をいただきました。

■SIGIRに国内研究者の論文が2本通ったと聞いて、自分も頑張ろうと思いました。
(匿名希望)

オンライン版で読みたい記事、期待するコンテンツ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。

■紙面を気にせず記事を執筆できると思いますので、深い内容(詳細な記事)を読みたいです。
(匿名希望)

■記事の内容ではないですが、意見やコメントが記事と同時に見られるような仕組みがあるとよいと思います(見たくなければ消せるようにしてほしいですが)。
(倉本 到)

■ IT 技術と法について。 (國武悠人／ジュニア会員)

■実際に論文とリンクしたコンテンツを期待いたします。たとえば、論文にてプログラミングに関しての事案を書かれている場合、それがオンラインで実際に触れられること等を期待いたします。
(竹原豊和)

■単なる PDF 版は嫌だがコストはかけたくない。 (匿名希望)

■映像コンテンツがあるとよいです。 (匿名希望)

■リンクを豊富に入れていただきたい。 (匿名希望)

■IT 史を下敷きとした技術進展の歴史。何が元(参考)になり、イノベーションが起きたか。当時の評価や時代的な背景にリンクがはされると、より知的好奇心を刺激すると思います。
(匿名希望)

■動画の利用、ソースコードやデータ(たとえば教育記事であれば教材の一部)など有用な情報の掲載、一般には紙面の都合で省略される大量の画像の掲載など。
(匿名希望)

■印刷版よりは発行の手間が少ないことが期待できるため、できるだけ新しい話題を取り上げたニュース解説のような記事が望ましい。そして関連する専門的解説(会誌の記事など)へのリンク集があるとさらに役立つだろう。
(伊藤雅樹)

■動画や音声、プレゼン資料などを活用した、新しい形のメディアを期待します。また、参考文献などへのリンクが張られていたりすると便利だと思います。
(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。

■科学教育とプログラミング教育に関するテーマを取り上げてほ
しいです。 (匿名希望)

■年に1~2度ぐらいは、今号のように夢を語る記事や研究者各
位の(想像とは違う)能力が発揮できるような記事・特集がある
とよいなと思いました。 (倉本 到)

■特集記事など重要なものは毎月読むように心がけている。
(匿名希望)

■カラーは見やすくてよいのですが、前のページの図面等の色が
気になります。 (匿名希望)

■量子コンピュータについて取り上げてほしい。
(匿名希望／ジュニア会員)

■ブロックチェーンの応用、IoT 利用の最新動向等。 (匿名希望)

■実証可能な論文にさせていただくことを望みます。 (匿名希望)

■非専門家にとっても理解でき、役に立つ啓蒙的な記事も読み
たい。学術と実社会とのかわりに関する記事も読みたい。
(匿名希望)



【本欄担当 鵜川始陽, 中澤里奈／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。

皆様にとって会誌をより役立つものとするため、
・記事に対する感想、意見 ・記事テーマの提案 ・会誌または学会に対する全般的な意見、提言
・その他、情報処理技術についての全般的な意見、提言
など自由なご意見、ご感想をお待ちしております。

なお、「道しるべ」については

<URL : <https://www.ipsj.or.jp/magazine/sippitsu/michishirube.html> > で
これからのテーマ案を募集しており、いただいたご意見をまとめております。

※ご意見、ご感想を会誌に掲載させていただいた方には薄謝または記念品を進呈いたします。

掲載に際しては、編集の都合上、ご意見に手を加えさせていただくことがありますので、あらかじめご了承ください。
なお、意見の投稿に伴う、住所、氏名、所属などの個人情報については、学会のプライバシーポリシーに準じて取り扱いたします。 <URL : <https://www.ipsj.or.jp/privacypolicy.html> >

応募先 〒 101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
一般社団法人 情報処理学会 会誌編集部門 E-mail : editj@ipsj.or.jp Fax (03) 3518-8375
<https://www.ipsj.or.jp/magazine/enquete.html>

ご意見をお寄せ
ください!

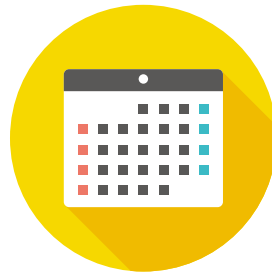


IPJSJ カレンダー

※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 Web でご確認くださいませう
 お願いいたします。

開催日	名 称	論文等応募締切日	参加締切日	開催地
	東海支部2019年度 学生論文奨励賞募集 https://www.ipsj-tokai.jp/	3月16日(月)		
	論文誌「持続可能な社会を実現するコラボレーション技術と ネットワークサービス」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-C.html	3月23日(月)		
	論文誌「5G時代の社会を創るモバイル・高度交通システム」 特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-D.html	3月31日(火)		
	論文誌「トランザクションデジタルプラクティス 「スポーツテック」特集論文募集 https://www.ipsj.or.jp/dp/cfp/tdp0101s.html	4月10日(金)		
	論文誌「インタラクションの理解および基盤・応用技術」 特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-J.html	4月17日(金)		
	論文誌「ネットワークサービスと分散処理」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-E.html	5月1日(金)		
	論文誌「若手研究者」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-K.html	5月29日(金)		
	論文誌「ソフトウェア工学」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-H.html	8月3日(月)		
3月13日(金)～	第12回アクセシビリティ研究発表会	1月20日(月)	当日のみ	筑波技術大学
3月15日(日)	https://www.ipsj.or.jp/kenkyukai/event/aac12.html			
3月14日(土)～	第154回コンピュータと教育研究発表会	1月24日(金)	当日のみ	電気通信大学
3月15日(日)	https://www.ipsj.or.jp/kenkyukai/event/ce154.html			
3月16日(月)	第177回アルゴリズム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/al177.html	1月21日(火)	当日のみ	東北大学 青葉山東キャンパス
3月16日(月)～	第221回コンピュータビジョンとイメージメディア研究発表会	1月8日(水)	当日のみ	京都大学
3月17日(火)	https://www.ipsj.or.jp/kenkyukai/event/cvim221.html			
3月16日(月)～	第187回ヒューマンコンピュータインタラクション研究発表会	1月20日(月)	当日のみ	国士舘大学 世田谷 キャンパス(梅ヶ丘校舎)
3月17日(火)	https://www.ipsj.or.jp/kenkyukai/event/HCI187.html			
3月16日(月)～	第110回グループウェアとネットワークサービス研究発表会	1月27日(月)	当日のみ	国士舘大学 世田谷キャンパス
3月17日(火)	https://www.ipsj.or.jp/kenkyukai/event/GN110.html			
3月16日(月)～	第173回ハイパフォーマンスコンピューティング研究発表会	1月24日(金)	当日のみ	北海道立道民活動 センター(かでの2・7)
3月18日(水)	https://www.ipsj.or.jp/kenkyukai/event/hpc173.html			
3月17日(火)～	第177回コンピュータグラフィックスとビジュアル情報学研究発表会	1月28日(火)	当日のみ	東映デジタルセンター シアター
3月18日(水)	https://www.ipsj.or.jp/kenkyukai/event/cg177.html			
3月18日(水)～	第55回エンタテインメントコンピューティング研究発表会	2月7日(金)	当日のみ	首都大学東京 日野キャンパス
3月19日(水)	https://www.ipsj.or.jp/kenkyukai/event/ec55.html			
3月23日(月)～	第199回知能システム研究発表会	2月14日(金)	当日のみ	静岡大学 浜松キャンパス
3月24日(火)	https://www.ipsj.or.jp/kenkyukai/event/ics199.html			
3月27日(金)	第138回情報基礎とアクセス技術・ 第116回ドキュメントコミュニケーション合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/IFAT138DC116.html	2月14日(金)	当日のみ	中央大学 後楽園キャンパス
5月8日(金)～	第178回アルゴリズム研究発表会	3月6日(金)	当日のみ	国立情報学研究所
5月9日(土)	https://www.ipsj.or.jp/kenkyukai/event/al178.html			
5月12日(火)～	第174回ハイパフォーマンスコンピューティング研究発表会	3月13日(金)	当日のみ	国立情報学研究所
5月13日(水)	https://www.ipsj.or.jp/kenkyukai/event/hpc174.html			
5月14日(木)～	第222回コンピュータビジョンとイメージメディア研究発表会	3月6日(金)	当日のみ	名古屋工業大学
5月15日(金)	https://www.ipsj.or.jp/kenkyukai/event/cvim222.html			
5月14日(木)～	第89回コンピュータセキュリティ・	3月6日(金)	当日のみ	北海道大学
5月15日(金)	第48回インターネットと運用技術合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/csec89iot49.html			クラーク会館

5月14日(木)～	第111回グループウェアとネットワークサービス・	3月11日(水)	当日のみ	東京都市大学
5月15日(金)	第37回セキュリティ心理学とトラスト合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/gn111spt37.html			横浜キャンパス
7月29日(水)	The 4th cross-disciplinary Workshop on Computing Systems, Infrastructures, and Programming (xSIG2020) http://xsig.hpcc.jp/2020/	3月6日(金)		フェニックス・プラザ (福井市民福祉会館)
9月2日(水)～	The 15th International Workshop on Security (IWSEC 2020)	3月23日(月)		Happiring Hall and Fukui International Activities Plaza, Fukui, Japan
9月4日(金)	https://www.iwsec.org/2020/index.html			
9月7日(月)～	DAシンポジウム2020—システムとLSIの設計技術—			鳥羽シーサイドホテル
9月9日(水)	http://www.sig-sldm.org/das/			
9月10日(木)～	ソフトウェアエンジニアリングシンポジウム2020 (SES2020)			株式会社日立製作所 横浜研究所
9月12日(土)	https://ses.sigse.jp/2020/			
10月28日(水)～	The 13th International Conference on Mobile Computing and Ubiquitous Networking (ICMU2020)	5月20日(水)		機械振興会館
10月30日(金)	http://www.icmu.org/icmu2020/			



Web ページ (<https://www.ipsj.or.jp/>) 更新情報

[トピックス]

- 2月15日 会誌「情報処理」Web カタログ (Vol.61 No.3)
- 2月10日 2020 年度日本学術振興会賞受賞候補者推薦募集
- 2月7日 論文誌「インタラクションの理解および基盤・応用技術」特集 論文募集
- 2月7日 論文誌「ソフトウェア工学」特集 論文募集
- 2月7日 論文誌「若手研究者」特集 論文募集
- 2月3日 2020 年度代表会員の選出について
- 2月3日 2020 年度役員改選の投票について
- 2月3日 本会主催イベントにおける新型コロナウイルス感染症への対策について
- 1月30日 創立 60 周年記念論文投稿期限延長のお知らせ
- 1月30日 論文誌トランザクションデジタルプラクティス「スポーツテック」特集論文募集
- 1月24日 論文誌「5G 時代の社会を創るモバイル・高度交通システム」特集 論文募集
- 1月24日 論文誌「ネットワークサービスと分散処理」特集 論文募集
- 1月15日 会誌「情報処理」Web カタログ (Vol.61 No.2)
- 1月06日 新年のご挨拶

人材募集 (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: 国公立教育機関, 国公立研究機関 税抜 20,000 円 (税込 22,000 円)

賛助会員 (企業) 税抜 30,000 円 (税込 33,000 円)

賛助会員以外の企業 税抜 50,000 円 (税込 55,000 円)

* 本会誌へ掲載依頼いただいた場合に限り, 追加料金 税抜 4,000 円 (税込 4,400 円) 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 (NICT)

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 2021 年 4 月 1 日 (場合により早期採用の可能性有り)

応募方法 当機構採用情報の Web ページからのエントリー (研究職) https://www.nict.go.jp/employment/research_staff.html (研究技術職) https://www.nict.go.jp/employment/technical_staff.html

応募締切 2020 年 4 月 10 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





FIT2020 第 19 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：2020年9月1日（火）～3日（木）

会 場：北海道大学 札幌キャンパス（北海道札幌市北区）

FIT2020 Web ページ <https://www.ipsj.or.jp/event/fit/fit2020/>

受付期間(予定)：2020 年 3 月 30 日（月）～5 月 8 日（金）

◆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）とは、2002年から合同で毎年秋季に、「情報科学技術フォーラム(FIT: Forum on Information Technology)」を開催しており、2020年9月には第19回目を北海道大学で開催します。本フォーラムは、両学会の大会の流れをくむものですが、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、など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御応募下さい。

●申込主要日程（予定）

登録申込／投稿受付開始：2020年3月30日（月） → 登録申込締切：2020年5月8日（金）

最終掲載原稿締切：2020年6月19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FIT2020Web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 ヤングリサーチアー 賞	2020 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するため、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）

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ので、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勧めします。なお、推薦を辞退することも可能です。

●問合せ先（FIT2020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: jigyo@ipsj.or.jp

◆◆ 有料会告について ◆◆

本会の主催・共催行事および協賛・後援記事の次第書（論文募集，参加案内等）の本誌掲載については，下記により有料にて取り扱っていますのでお知らせします。

記

■掲載条件

件名	内容	掲載単位	掲載料金（税抜）	
論文募集／ 参加者募集	国際会議，シンポジウム，ワークショ ップ，講演会，講習会などの論文募集・ 参加者募集	1 ページ，1/2 ページ または 1/4 ページ	（主催・共催）	
			1 ページ	50,000 円
			1/2 ページ	30,000 円
			1/4 ページ	20,000 円
			（協賛）	
			広告として取り扱う	
人材募集	国公立教育機関，国公立研究機関， 企業の人材募集	10 行程度	国公立教育機関，国公立研究機関	20,000 円
			賛助会員（企業）	30,000 円
			賛助会員以外の企業	50,000 円
＊本会誌へ掲載依頼いただいた場合に限り，追加料金 4,000 円で同一内容を本会 Web ページに掲載できます。				

■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宛先，Web 掲載の有無（人材募集のみ）などを記載し，掲載希望原稿を添えて下記の申込先へお申し込みください。

■原稿の書き方

- 行事次第書： A4 変形判カメラレディまたは PDF ファイル（フォント埋め込み）とします。
(1 ページ) 天地 250mm × 左右 180mm
(1/2 ページ) 天地 120mm × 左右 180mm
(1/4 ページ) 天地 55mm × 左右 180mm
* A4 変形判以外の原稿は縮小または拡大となりますのでご注意ください。

- 人材募集： 次の項目を明記し，E-mail または Fax，郵送にてお送りください。
[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]
* なお，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

掲載号発行日に料金を請求いたしますので，3 カ月以内にお支払いください。

■掲載申込先

一般社団法人 情報処理学会 会誌編集部（有料会告係）
〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
E-mail: editj@ipsj.or.jp Tel (03) 3518-8371 Fax (03) 3518-8375



「情報処理」 カタログ同封サービスの ご案内

カタログ同封
サービスとは？

毎月会員に配布している学会誌に貴社 / 貴校のカタログや広告を同封し、直接読者にお届けするサービスです。
通常のDMと異なり学会誌に同封しますので、**読者の開封率は格段に上がります。**
また、カタログ送付にかかる**コストを最小に抑えることができ、なおかつ情報処理を専門とする読者にターゲットを絞った効果的な案内を出すことが可能**となります。

お申し込み方法と掲載までの手続き

- ①封入希望月の前月 15 日までに下記事項を記載の上、問合せ先までお申し込みください。
 - ◆会社名、担当者、連絡先（住所、Tel、Fax、E-mail） ◆封入希望号
 - ◆サイズ ◆カタログの簡単な内容説明
 - ◆割引対象にあたる場合はその旨記載ください。
- ②封入希望月の遅くとも前月末日までに下記事項について手配をお願いします。
 - ◆カタログ見本を問合せ先までお送りください（PDF、Fax 可）。
 - ◆納品業者をお知らせください。
- ③納品日は封入希望月の 5 日（土曜、日曜、祝日の場合は翌営業日）です。日付指定にて必要枚数（20,000 枚）を印刷し指定の納品先へお送りください。
 - ※納品先は、お申し込み後にご連絡いたします。
 - ※納品が遅れますと同封ができない場合がございます。その場合はキャンセルとさせていただきます。
- ④カタログを同封した学会誌を発行日にお送りしますので、ご確認ください。
- ⑤後日請求書をお送りしますので振込手続きをお願いします。

1 通あたり
約17.5 円！

基本価格 350,000 円
(税抜)

対象：全会員 20,000 通 配布
(正会員 / 名誉会員 / 学生会員 / 賛助会員)

大学や
共催事業は
さらに割引も！

大学 / 研究所 / 賛助会員または情報処理学会主催・共催事業は、下記のとおり割引料金が適用されます。

大学 / 研究所 / 賛助会員
(基本価格の 40% Off !)

210,000 円
(税抜)

情報処理学会主催・共催事業*
(基本価格の 80% Off !)

70,000 円
(税抜)

* 情報処理学会研究会主催、共催を含む

サイズ：A4 変形判または A4 判二つ折り（その他についてはご相談ください）
用紙：色上質厚口（四六判 80kg）またはコート紙（四六判 90kg）相当

☎ 問合せ先

〔広告代理店〕 アドコム・メディア (株) E-mail: sales@adcom-media.co.jp
〒169-0073 東京都新宿区百人町 2-21-27
Tel.(03)3367-0571 Fax.(03)3368-1519

一般社団法人情報処理学会 会誌編集部 E-mail: editj@ipsj.or.jp
〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
Tel.(03)3518-8371 Fax.(03)3518-8375



大学・工業高校・専門学校などで
教科書・参考書としてお使いいただけるシリーズです。

新刊

データベースの基礎

吉川正俊 著
A5判/288頁/本体2,900円(税別)

オペレーティングシステム(改訂2版)

野口健一郎・光来健一・品川高廣 共著
A5判/256頁/本体2,800円(税別)

ネットワークセキュリティ

菊池浩明・上原哲太郎 共著
A5判/206頁/本体2,800円(税別)

ソフトウェア工学

平山雅之・鶴林尚靖 共著
A5判/214頁/本体2,600円(税別)

応用Web技術(改訂2版)

松下 温 監修/市村 哲・宇田隆哉 共著
A5判/192頁/本体2,500円(税別)

基礎Web技術(改訂2版)

松下 温 監修/市村 哲・宇田隆哉・伊藤雅仁 共著
A5判/196頁/本体2,500円(税別)

画像工学

堀越 力・森本 正志・三浦康之・澤野弘明 共著
A5判/232頁/本体2,800円(税別)

人工知能(改訂2版)

本位田真一 監修/松本一教・宮原哲浩・
永井保夫・市瀬龍太郎 共著
A5判/244頁/本体2,800円(税別)

音声認識システム(改訂2版)

河原達也 編著
A5判/208頁/本体3,500円(税別)

ヒューマンコンピュータ
インタラクション(改訂2版)

岡田謙一・西田正吾・葛岡英明・仲谷美江・塩澤秀和
共著 A5判/260頁/本体2,800円(税別)

ソフトウェア開発(改訂2版)

小泉寿男・辻 秀一・吉田幸二・中島 毅 共著
A5判/224頁/本体2,800円(税別)

情報と職業(改訂2版)

駒谷昇一・辰巳丈夫 共著
A5判/232頁/本体2,500円(税別)

情報通信ネットワーク

阪田史郎・井関文一・小高知宏・甲藤二郎・
菊池浩明・塩田茂雄・長 敬三 共著
A5判/288頁/本体2,800円(税別)

数理最適化

久野誉人・繁野麻衣子・後藤順哉 共著
A5判/272頁/本体3,300円(税別)

情報とネットワーク社会(一般教育シリーズ)

駒谷昇一・山川 修・中西通雄・北上 始・佐々木整・
湯瀬裕昭 共著 A5判/196頁/本体2,200円(税別)

情報とコンピュータ(一般教育シリーズ)

河村一樹・和田 勉・山下和之・立田ルミ・岡田 正・
佐々木整・山口和紀 共著
A5判/176頁/本体2,200円(税別)

メディア学概論

山口治男 著
A5判/172頁/本体2,400円(税別)

情報ネットワーク(一般教育シリーズ)

岡田 正・駒谷昇一・西原清一・水野一徳 共著
A5判/168頁/本体2,300円(税別)

離散数学

松原良太・大島彰彰・藤田慎也・小関健太・
中上川友樹・佐久間雅・津垣正男 共著
A5判/256頁/本体2,800円(税別)

HPCプログラミング

寒川 光・藤野清次・長嶋利夫・高橋大介 共著
A5判/256頁/本体2,800円(税別)

ユビキタスコンピューティング

松下 温・佐藤明雄・重野 寛・屋代智之 共著
A5判/232頁/本体2,800円(税別)

Java/UMLによる
アプリケーション開発

森澤好臣 監修/布広永示・高橋英男 共著
A5判/208頁/本体2,600円(税別)

情報理論

白木善尚 編
村松 純・岩田賢一・有村光晴・渋谷智治 共著
A5判/256頁/本体2,800円(税別)

Java基本プログラミング

今城哲二 編 布広永示・
マッキン ケネスジェームス・大見嘉弘 共著
A5判/248頁/本体2,500円(税別)

システムLSI設計工学

藤田昌宏 編著
A5判/242頁/本体2,800円(税別)

組込みシステム

阪田史郎 著 高田広章 編著
A5判/280頁/本体3,000円(税別)

情報システム基礎(一般教育シリーズ)

神沼靖子 編著
A5判/228頁/本体2,500円(税別)

Linux演習

前野謙二・落合 昭・生野荘一郎・塩澤秀和・
高島俊徳 共著
A5判/224頁/本体2,500円(税別)

インターネットプロトコル

阪田史郎 編著
A5判/272頁/本体2,800円(税別)

分散処理

谷口秀夫 編著
A5判/240頁/本体2,800円(税別)

情報とコンピューティング

(一般教育シリーズ)
川合 慧 監修/河村一樹 編著
A5判/228頁/本体2,500円(税別)

情報と社会(一般教育シリーズ)

川合 慧 監修/駒谷昇一 編著
A5判/236頁/本体2,500円(税別)

コンピュータアーキテクチャ(改訂2版)

小柳 滋・内田啓一郎 共著
A5判/256頁/本体2,900円(税別)

コンピュータグラフィックス

魏 大名・先田和弘・Roman Durikovic・向井信彦・
Carl Vilbrandt 共著
A5判/280頁/本体3,000円(税別)

アルゴリズム論

浅野哲夫・和田幸一・増澤利光 共著
A5判/242頁/本体2,800円(税別)

データベース

速水治夫・宮崎収兄・山崎晴明 共著
A5判/196頁/本体2,500円(税別)

ソフトウェア工学演習

伊藤 潔・廣田豊彦・富士 隆・熊谷 敏・川端 亮 共著
A5判/228頁/本体2,800円(税別)

本体価格(税別)は変更する場合があります。

注文はオーム社Webサイトまで ▶ https://www.ohmsha.co.jp/tbc/text_series_0202.htm

CONTENTS

Preface

328 Creation for the Internet Civilization

Jun MURAI (Keio Univ.)

Special Features

Cybersecurity in a New Era of Mobility - Toward Enhancement of Japan Brand -

330 0. Foreword

Masaki ISHIGURO (Mitsubishi Research Institute, Inc.), Seiichi SHIN (Univ. of Electro-Communications) and Takayuki SASAKI (NEC)

332 1. International Trend and Future Prospects of Automotive Security in the Age of CASE

Masaki ISHIGURO (Mitsubishi Research Institute, Inc.)

338 2. CASE Evolution and Cybersecurity in Automotive Domain

Yutaka MATSUBARA, Ryo KURACHI and Hiroaki TAKADA (Nagoya Univ.)

344 3. Trends and Topics of Research and Development Related to Information Network and Cybersecurity for Train Operation and Control Systems

Kunihiro KAWASAKI and Akihiro GION (Railway Technical Research Institute)

350 4. Cybersecurity and Human Resource Development on Aviation

Takao OKUBO (Institute of Information Security)

356 5. Cybersecurity in Maritime Industry

Kazuo HIEKATA (Graduate School of Frontier Sciences)

362 6. Drone Security

Hisanori SUNOHARA and Toshihiro TAGAMI (Secure Drone Consortium)

Article

372 Record of 30 Years of Programming Contest

Yasuko KAMINUMA (IPSJ Fellow) and Takayuki TERAMOTO (National Institute of Technology, Tsuyama)

378 Decision Support for Ethical Considerations of Cybersecurity Research

Mitsuaki AKIYAMA (NTT Secure Platform Labs.) and Masaki SHIMAOKA (SECOM CO., LTD)

"Peta-gogy" for Future

387 We Support the Confidence of Teachers

Naoko TAKAHASHI (Kokugakuin Univ.)

388 Try Coding with Processing - No.3 Mastery of Repetition

Manabu SUGIURA (Kamakura Women's Univ.)

393 Report of the Visit for Schools in Sri Lanka

Ben Tsutom WADA (Nagano Univ.)

Let's Learn Informatics

402 Let's Think about Classes of "Information 1" - Teaching Information Design and Data Science Through Making Paper Airplanes -

Hiroyuki OKAMOTO (Assumption Kokusai High School)

371 Shopping Boast

384 IPSJ Activity Report

386 Gathering to Share Original Programming Projects for Junior

397 Biblio Talk

398 Skimming a Famous Paper in Five Minutes

406 Questions for Experts

408 IT Travelog Manga

410 Conference Report

412 Conference Report

読後のご意見をお送りください

本誌では、現在約 120 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、毎号巻末に掲載しております所定の用紙または Web ページ (<https://www.ipsj.or.jp/magazine/enquete.html>) をお使いいただき、奮って事務局までお寄せください。

一般社団法人 情報処理学会 会誌編集部門

〒 101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F E-mail: editj@ipsj.or.jp Fax(03)3518-8371

ご意見をお寄せください！

【4月10日頃までにお出しください】

宛 先 一般社団法人 情報処理学会 モニタ係（下記のいずれからも送付できます）
<https://www.ipsj.or.jp/magazine/enquete.html> Fax(03)3518-8375 E-mail: editj@ipsj.or.jp
 （E-mail で送信される場合は、10-1-a のようにコードでお答えください）
 ※ご意見の投稿に伴う、住所、氏名、所属などの個人情報については、学会のプライバシーポリシーに準じて取り扱いいたします。
<https://www.ipsj.or.jp/privacypolicy.html>

[コード]

- [1] ご氏名
- [2] ご所属 Tel. () -
- [3] E-mail:
- [4] 業種：(a) 企業（サービス業）(b) 企業（製造業）(c) 研究機関 (d) 教育機関（小・中・高校・高専・大学・大学院など）
 (e) 学生 (f) 学生（ジュニア会員）(g) その他..... 4- []
- [5] 職種：(a) 研究職 (b) 開発・設計 (c) システムエンジニア (d) 営業 (e) 本社管理業務
 (f) 会社経営・役員・管理職 (g) 教職員（小・中・高校・高専・大学・大学院など）
 (h) 学生 (i) 学生（ジュニア会員）(j) その他..... 5- []
- [6] 年齢：(a) 10代 (b) 20代 (c) 30代 (d) 40代 (e) 50代 (f) 60代以上..... 6- []
- [7] 性別：(a) 男性 (b) 女性..... 7- []
- [8-1] あなたはモニタですか？：(a) はい (b) いいえ..... 8-1- []
- [8-2] あなたのご意見は「会員の広場」（会誌および Web）に掲載される場合があります。その場合：
 (a) 実名可（氏名のみ掲載）(b) 匿名希望 (c) 掲載を希望しない..... 8-2- []
- [9] どちらの媒体で記事をお読みになりましたか？
 (a) 冊子版 (b) 情報学広場（電子図書館）(c) Kindle (d) fujisan (e) その他..... 9- []
- [10] 今月号（2020年4月号）の記事は良かったですか。下記の記事すべてについて評価をご回答ください。
 [a...大変良い b...良い c...普通、どちらとも言えない d...悪い e...読んでいない]
- 巻頭コラム：インターネット文明を創る..... 10-1- []
- 特集：新たなモビリティ時代のサイバーセキュリティ
0. 編集にあたって..... 10-2- []
1. 自動車セキュリティの国際標準等の動向と今後の課題..... 10-3- []
2. 自動車分野の CASE 革命とサイバーセキュリティ..... 10-4- []
3. 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ..... 10-5- []
4. 航空分野のサイバーセキュリティと人材育成..... 10-6- []
5. 海事産業におけるサイバーセキュリティ対策動向..... 10-7- []
6. ドローンのセキュリティ..... 10-8- []
- 買い物自慢：GR III でスマートフォンとカメラの二刀流生活..... 10-9- []
- 解説：高専プロコン 30 年の歩み..... 10-10- []
- 解説：サイバーセキュリティ研究における倫理的配慮のサポート..... 10-11- []
- 学会活動報告：量子ソフトウェア研究会の新設にあたって..... 10-12- []
- 連載：集まれ！ジュニア会員!!..... 10-13- []
- べた語義：小中高の先生の自信をサポートします..... 10-14- []
- べた語義：Processing でプログラミングに挑戦！ー第3回 繰り返しを使いこなそうー..... 10-15- []
- べた語義：スリランカの学校訪問記..... 10-16- []
- ピリオド・トーク：人工知能を活用した研究開発の効率化と導入・実用化《事例集》..... 10-17- []
- 5分で分かる！有名論文ナメ読み：Mark Weiser: Program Slicing..... 10-18- []
- 情報の授業をしよう！：情報 I を意識した授業をしよう！..... 10-19- []
- 連載：先生、質問です！..... 10-20- []
- IT 紀行：VR センター三銃士に会ってきた！ どうなる VR の未来!?!..... 10-21- []
- 会議レポート：ASE 2019 参加報告..... 10-22- []
- 会議レポート：IEEE/ACM SC19 会議参加報告..... 10-23- []
- [11] 本号で最も良かった記事は何ですか？ 上記 [10] の設問の記事番号から 1 つだけ選び（例：10-8 の記事の場合は「8」と記入）、その理由をご回答ください。上記に掲載されていない記事の場合はタイトルを直接ご記入ください。
- [11-1] 良かった記事..... 11-1- []
- [11-2] この記事に対する貴方の立場：a) 専門家 b) 非専門家..... 11-2- []
- [11-3] 選んだ理由（下記から、いくつでも選択可）..... 11-3- []
- a) 技術・研究動向がよく分かった b) 知的興味をかきたてられた c) 新たな知識を得ることができた d) 内容が平易で理解しやすかった
 e) その他（具体的に下記にご記入ください）

〔12〕 本号で最も良くなかった記事は何ですか？ 上記〔10〕の設問の記事番号から1つだけ選び（例：10-8の記事の場合は「8」と記入），その理由をご回答ください。上記に掲載されていない記事の場合はタイトルを直接ご記入ください。

〔12-1〕 良くなかった記事 12-1- []

〔12-2〕 この記事に対する貴方の立場：a) 専門家 b) 非専門家 12-2- []

〔12-3〕 選んだ理由（下記から、いくつでも選択可） 12-3- []

a) 記事の内容に誤りがあった b) ありきたりの内容だった c) 記事が難しすぎた d) 何を言いたいのか分からなかった e) 宣伝の意図が強すぎる
f) テーマに興味を持てなかった g) その他（下記に具体的に記入ください）

〔13〕 今月の特集に対する貴方の立場を教えてください。

〔13-1〕 新たなモビリティ時代のサイバーセキュリティ：a) 専門家 b) 非専門家 13-1- []

〔14〕 設問〔10〕で読んでいないと答えた記事について、その理由を教えてください。

〔15〕 会誌のオンライン版ができたらどのような記事を読みたいか、どのようなコンテンツが期待できるか、などで意見がございましたら教えてください。

〔16〕 会誌に対するご意見や感想，著者への質問，巻頭コラムに登場してほしい人物，今後取り上げてほしいテーマなどありましたらご記入ください。（スペースが足りない場合はお手数ですが別紙を追加してください）

■ 各種問合せ先 ■

一般社団法人 情報処理学会（本部） ※支部所在地等詳細はリンクされている各支部ページでご参照ください。

〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F Fax(03)3518-8375 <https://www.ipsj.or.jp/>

担 当	E-mail	Tel(ダイヤルイン)	取り扱い内容
■ 会員サービス部門			
会 員	mem@ipsj.or.jp	03-3518-8370	入会，会費，変更連絡，退会，在会証明，会員証，会誌配布，会員特典，会費等口座振替，海外からの送金，賛助会員，電子図書館
■ 会誌編集部門			
会誌編集	editj@ipsj.or.jp	03-3518-8371	会誌「情報処理」の掲載内容，広告掲載，出版，コンピュータ博物館（情報処理技術遺産）
著作権	copyright@ipsj.or.jp		転載許可，著作権
デジタルプラクティス	editdp@ipsj.or.jp		デジタルプラクティス（DP）の編集・査読，DP レポート
図 書	tosho@ipsj.or.jp	03-3518-8374	出版物購入
■ 研究部門			
論文誌	editt@ipsj.or.jp	03-3518-8372	論文誌（ジャーナル／JIP／トランザクション）の編集・査読
調査研究／国際／教育	sig@ipsj.or.jp		研究会登録，研究発表会，研究グループ，シンポジウム，国際会議，IFIP 委員会，情報処理教育委員会，アクレディテーション対応
■ 事業部門			
事 業	jigyo@ipsj.or.jp	03-3518-8373	全国大会，FIT，プログラミングコンテスト，プログラミング・シンポジウム，協賛・後援
技術応用	event@ipsj.or.jp		連続セミナー，短期セミナー，IT フォーラム，ソフトウェアアジア，その他講習会
認定情報技術者制度	ipsj.citp@ipsj.or.jp		認定情報技術者制度
■ 管理部門			
総務／庶務	soumu@ipsj.or.jp	03-3518-8374	総会・理事会，支部，選挙，総務系選奨，関連団体，アドバイザーボード
経 理	keiri@ipsj.or.jp		出納，送金連絡
システム企画	sys@ipsj.or.jp		システム企画，セキュリティ，電子化委員会，電子図書館，IPSJ メールニュース
■ 情報規格調査会			
規格部門	問合せフォーム https://www.itscj.ipsj.or.jp/contact/index.html		ISO/IEC JTC 1での情報技術の標準化業務 〒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 https://www.itscj.ipsj.or.jp/

ご執筆においてモビリティ分野のサイバーセキュリティ分野の第一人者に多大なご協力をいただいた。執筆・編集作業は、年末年始にもかかり大事な時期であるにもかかわらず、関係者には大変なご尽力をいただいた。サイバーセキュリティ分野の中でも先端的で変革が激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

ただいた。日本の自動車の品質や新幹線の安全などのモビリティ分野ではジャパン・ブランドが確立されている分野もあるが、新たな変革の際にサイバーセキュリティ分野におけるジャパン・ブランドを確立することが重要であると言える。

(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。

「創立 60 周年記念特集」2050 年の情報処理

組込みシステムはどこへ向かうか? / ソフトウェア開発の未来 / 30 年後? 知らん. / 2050 年のプログラミング / 30 年後のコンピュータアーキテクチャ第二版 / 高性能計算の今後を予想する / 近未来を予測できる世界, Ability-aware な世界 / モバイルコンピューティングの未来像—リアルを超えるデジタル空間を実現し, AI・ロボットの遍在化を推進し, 自己実現をアシストする— / 2050 年の情報処理 (セキュリティ編) / 2050 年の学術情報処理 / グループウェアから共助社会へ / 2050 年の春のある日 / トラストで紡ぐセキュリティ / 大規模社会実験の成果はいかに? / 能力はダウンロードできるか? / 社会的な重要課題の解決に挑む AI—ビッグデータ / スーパーヒューマン音声対話コミュニケーションシステム / 30 年前と 30 年後へのメッセージ—情報処理に期待すること— / 生物学と情報科学によるトランスヒューマン研究の進化 / 2050 年の知能システム / Post-Truth 音楽情報処理 / 情報システムとしての法律もしくは法治の未来 / コンピュータグラフィックスの未来 / 2050 年のエンタテインメントコンピューティング / 人口 9,000 万人時代の日本の電子化知的財産・社会基盤

特別解説: 高輪ゲートウェイ駅開業～最新設備に見るこれからの鉄道 ICT ～ 福田和人

亡くなった子供の VR をめぐって 折田明子

寄稿: ソフトウェア工学を推進した木村泉君を悼む 和田英一 他

報告: 多くの人が同意しない未来を作る～慶應義塾大学の話題の公開授業「SFC スピリッツの創造」に行ってきた～

..... 太田智美

教育コーナー: ペタ語義

連載: IT 紀行 / 生まれ! ジュニア会員!! / 買い物自慢 / 5 分で分かる! ? 有名論文ナメ読み / 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

複写される方へ

一般社団法人情報処理学会では複写複製および転載複製に係る著作権を学術著作権協会に委託しています。当該利用をご希望の方は、学術著作権協会 (<https://www.jaacc.org/>) が提供している複製利用許諾システムもしくは転載許諾システムを通じて申請ください。

尚、本会会員 (賛助会員含む) および著者が転載利用の申請をされる場合については、学術目的の利用に限り、無償で転載利用いただくことが可能です。ただし、利用の際には予め申請いただくようお願い致します。

権利委託先: 一般社団法人学術著作権協会
〒107-0052 東京都港区赤坂 9-6-41 乃木坂ビル
E-mail: info@jaacc.jp Tel (03)3475-5618 Fax (03)3475-5619

また、アメリカ合衆国において本書を複写したい場合は、次の団体に連絡してください。
Copyright Clearance Center, Inc.
222 Rosewood Drive, Danvers, MA 01923 USA
Phone: 1-978-750-8400 Fax: 1-978-646-8600

Notice for Photocopying

Information Processing Society of Japan authorized Japan Academic Association For Copyright Clearance (JACC) to license our reproduction rights and reuse rights of copyrighted works. If you wish to obtain permissions of these rights in the countries or regions outside Japan, please refer to the homepage of JACC (<http://www.jaacc.org/en/>) and confirm appropriate organizations.

You may reuse a content for non-commercial use for free, however please contact us directly to obtain the permission for the reuse content in advance.

<All users except those in USA>

Japan Academic Association for Copyright Clearance, Inc. (JAACC)
6-41 Akasaka 9-chome, Minato-ku, Tokyo 107-0052 Japan
E-mail: info@jaacc.jp
Phone: 81-3-3475-5618 Fax: 81-3-3475-5619

<Users in USA>

Copyright Clearance Center, Inc.
222 Rosewood Drive, Danvers, MA 01923 USA
Phone: 1-978-750-8400 Fax: 1-978-646-8600

広告のお申込み

■広告料金表

掲載場所	4 色	1 色
表 2	330,000 円 (税抜)	—
表 3	275,000 円 (税抜)	—
表 4	385,000 円 (税抜)	—
表 2 対向	300,000 円 (税抜)	—
表 3 対向	265,000 円 (税抜)	155,000 円 (税抜)
前付 1 頁	250,000 円 (税抜)	135,000 円 (税抜)
前付 1/2 頁	—	80,000 円 (税抜)
前付最終	—	148,000 円 (税抜)
目次前	—	148,000 円 (税抜)
差込 (A4 変形判 70.5kg 未満 1 枚)	275,000 円 (税抜)	
差込 (A4 変形判 70.5kg ～ 86.5kg 1 枚)	350,000 円 (税抜)	
同封 (A4 変形判 1 枚)	350,000 円 (税抜)	

■「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」 61 巻 4 号 掲載広告 (五十音順)

☐ MCPC…………… 表 3 ☐ 電子情報通信学会…………… 表 2 対向上
☐ インタフェース …… 表 2 ☐ フォーラムエイト …… 表 4

☐ 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)

HITACHI
Inspire the Next

(株) 日立製作所

FUJITSU

富士通 (株)

Orchestrating a brighter world
NEC

日本電気 (株)

MITSUBISHI ELECTRIC
Changes for the Better

三菱電機 (株)

CyberAgent.

(株) サイバーエージェント

IBM

日本アイ・ビー・エム (株)

●●● 賛助会員 (10 ~ 19口)

RECRUIT

(株) リクルート

Google

グーグル合同会社

NTT docomo

(株) NTT ドコモ

TOSHIBA

(株) 東芝

NTT

日本電信電話 (株)

Microsoft

日本マイクロソフト (株)

FORUM 8
フォーラムエイト

(株) フォーラムエイト

●●● 賛助会員 (3 ~ 9口)

TTC
Telecommunication
Technology
Committee

(一社) 情報通信技術委員会

NTT data

(株) NTT データ

GREE

グリー (株)

Rakuten
Institute of Technology

楽天技術研究所

IA japan

(一財) インターネット協会

ISA

情報サービス産業協会

TREND MICRO

トレンドマイクロ (株)

NTTコムウェア

NTT コムウェア (株)

NTTテクノクロス

NTT テクノクロス (株)

uejima

(株) うえじま企画

OKI

沖電気工業 (株)

Canon

キャノンマーケティングジャパン株式会社
キャノンマーケティングジャパン (株)

CORE MICRO SYSTEMS INC.

コアマイクロシステムズ (株)

SANBI

三美印刷 (株)

SEPTENI

(株) セプテーニ

SONY

ソニー (株)

team Lab

チームラボ (株)

TECHNOPRO Design

(株) テクノプロ
テクノプロ・デザイン社

Panasonic

パナソニック (株)

MIZUHO みずほ情報総研

みずほ情報総研 (株)

人と音楽の新しい関係をデザインする。

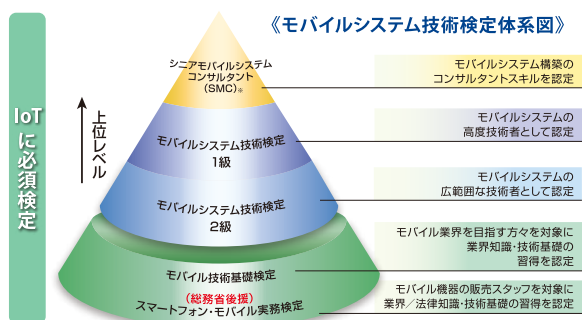
レコチョク

(株) レコチョク

MCPC 2020年度 モバイル・IoTシステム技術検定のご案内

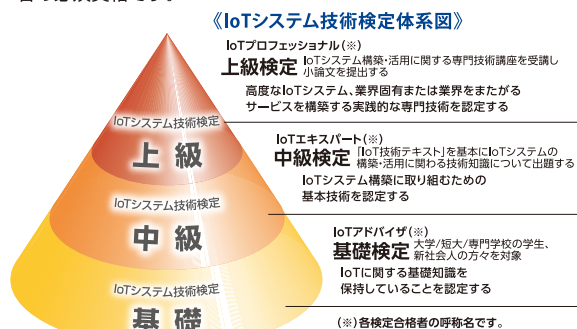
モバイルシステム技術検定

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7万6千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。



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。



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
吉澤 和弘 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



上智大学 理工学部客員教授
電子情報通信学会フェロー
IEEE Lifemember
服部 武 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

2020年度検定日 年2回実施

■スマートフォン・モバイル実務検定(CBT方式)

2020年 7月20日(月)~8月7日(金)
2021年 2月15日(月)~3月3日(水)

■モバイル技術基礎検定(CBT方式)

2020年 7月24日(金)~8月14日(金)
2021年 2月20日(土)~3月17日(水)

■モバイルシステム技術検定[1級・2級]

2020年 6月6日(土)
2020年 11月7日(土)

■IoTシステム技術検定[基礎・中級]

2020年 7月4日(土)
2020年 12月5日(土)

■IoTシステム技術検定[上級](2日間)

2020年 7月31日(金)~8月1日(土)
2020年 12月11日(金)~12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 2020年 9月18日(金)~9月19日(土)
更新研修 2020年 9月18日(金)、2021年3月5日(金)

お申込み・詳細はWebから

モバイルシステム技術検定

<http://www.mcpc-jp.org/kentei/>



IoTシステム技術検定

<http://www.mcpc-jp.org/iotkentei/>



第8回ものづくり日本大賞 経済産業大臣賞 受賞

「Connected Industries -優れた連携」部門

～UC-win/Roadのオープンデータ連携による多様な技術・分野間でのコネクタ加速～

01 VRプラットフォームで
インフラ計画の
合意形成を効率化

02 土木・自動車・防災・
環境・教育・医療など
幅広い分野に適用可能

03 サイバー空間と
現実世界をつなげ
社会課題を解決

04 様々なオープン
データと連携する
カスタマイズ開発が容易

VRプラットフォームで 実現する Society5.0



VR/AR連携システム

地震シミュレータ

高度研究用ドライビングシミュレータ
自動運転研究 / 車両性能実証
生体反応計測 (視線・脳波)

鉄道・船舶・重機シミュレータ

ロボット開発

ハブティクス

センサーモデル連携
自律飛行UAV

組込み開発・ゲーム開発

車載ECU開発

スイート千鳥エンジン
Cross Platform Game Engine

教育訓練

プログラミング学習ツール

溶接訓練シミュレータ

クラウドシステム

VR-Cloud®
遠隔合意形成

VR-NEXT®
大規模VR・設計図面 / 計測情報リアルタイム一元管理



IoT



AI



交通解析



地理空間情報
地図データ



ナビゲーション
(高精度測位情報)



点群データ



道路・地形
データ



土木・建築
設計データ



地震・津波
土石流・環境
エネルギー

13th デザインフェスティバル レポート

自動運転、VR、国土強靱化ソリューションや最先端表現技術などの最新事情を紹介
2019年11月12日(火) - 15日(金) 品川インターシティホール・ホワイエ

フォーラムエイトでは毎年11月にデザインフェスティバル-3Days+Eveを開催し、4日間で延べ1000人が来場。会期中には、最先端の表現技術を活用した作品および取組みを表彰する「羽倉賞」の授与式を行いました。情報処理学会推薦作品として「インタラクティブプロジェクションマッピング」(愛知工業大学 情報科学部/ソニー/NTTドコモ)が羽倉賞を受賞しています。



第3回 羽倉賞授賞者のみなさん

エントリー受付中 国際学生プログラミングコンペ



開発キット (SDK) によるクラウドアプリのプログラミング技術を競う!
THE 8TH Cloud Programming World Cup

デザインフェスティバル2020で審査・表彰式を実施!

エントリー受付
4/2~6/22

予選結果通知
7/14

作品提出締切
10/2

賞金・副賞 ワールドカップ賞(賞金30万) 他



▲詳細

株式会社 フォーラムエイト 東京本社
東京都港区港南 2-15-1 品川インターシティ A 棟 21F

Tel (代表) 03-6894-1888 (営業窓口) 0120-1888-58
Fax 03-6894-3888 | E-mail f8tokyo@forum8.co.jp

◆ショールーム: 東京・大阪・名古屋 ◆セミナールーム: 東京・大阪・名古屋・福岡・仙台・札幌・金沢・岩手・宮崎・沖縄・上海・青島・台北・ハノイ・ヤンゴン

FORUM 8
フォーラムエイト®
www.forum8.co.jp

定価 (本体 1,600 円 + 税)

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 TEL03-3367-0571 FAX03-3368-1519

雑誌 05269-04



4910052690400
01600

〒101-0062 東京都千代田区神田駿河台一五
編集人 稲見昌彦

東京都千代田区神田駿河台一五
発行所 一般社団法人 情報処理学会
発行人 木下泰三

電話 東京(03) 三五一八八三七四
振替口座 〇〇一五〇一四一八三四八四

東京都荒川区西日暮里五九八
印刷所 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