2020年5月10日印刷　2020年5月15日発行（毎月1回15日発行）
ISSN 0447-8053

IPSJ MAGAZINE

情報処理

2020 6
Vol.61 No.6
通巻 663 号

特集　ハードウェアセキュリティの最新動向

小特集　差分プライバシ

ミニ特集　ETロボコン：異色の情報系ロボコン
―光る若手にインタビュー―

特別解説　情報処理学会第82回全国大会　実録 緊急オンライン開催

特別解説　電子カルテの安全な導入と運用―宇陀市立病院事件を事例に

解　説　準委任契約はアジャイル開発を促進できるか
―アジャイル開発導入に躊躇する発注側の課題―

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

巻頭コラム
「世界のあしたが見えるまち」から民主主義へのささやかな貢献を
五十嵐立青

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!／ビブリオ・トーク

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

Classmbly Devices®

Interface Made in 日本

産業用パソコン

LTE搭載モデル ラインナップ

離島

山岳地

サイネージ

電源ブチ切り～自動再起動

安全に
電源ブチ切り
できます

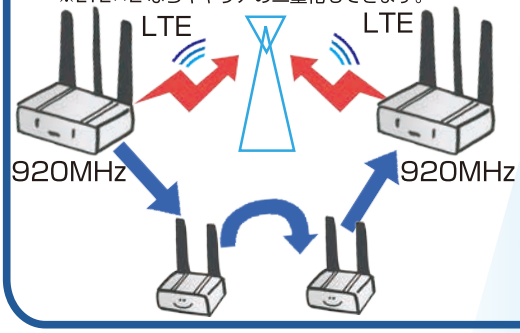
移動体

建設現場

建設機械への搭載

2系統による二重化

■LTE+920MHz：LTE の混雑時、920MHz がバックアップ
※LTE×2 ならキャリアの二重化もできます。



無線のセキュリティ

LTE＋920MHz　暗号化されたデータと暗号化の鍵を分けて送信

LTE＋LTE　データを半分ずつ別系統で送ることで、リスクを半減できます。

サーバ+LTEでイベントをリモート制御

スリムタワー CD

SuperCD

・LTE MODEL
・920MHz MODEL

省エネ CD

・LTE MODEL
・920MHz MODEL

車載 CD

・LTE ×2 MODEL
・LTE+920MHz MODEL

インタフェースモジュール

・LTE ×2 MODEL
・LTE+920MHz MODEL

Interface® Vision & Freedom 株式会社 インタフェース

詳しくはwebsiteまで www.interface.co.jp

URL：www.interface.co.jp　E-mail：support@interface.co.jp

製品の仕様、デザイン、価格については、予告なく変更する場合があります。本広告に記載した会社名、商品名は、各会社の商標または登録商標です。

SAMT-20-000351-01

今、必要とされる人材を育てる

超注目シリーズ

データサイエンス入門シリーズ

シリーズ編集委員　竹村彰通（滋賀大学、編集委員長）
狩野裕（大阪大学）、駒木文保（東京大学）、清水昌平（滋賀大学）
下平英寿（京都大学）、西井龍映（長崎大学、九州大学名誉教授）、水田正弘（北海道大学）

■「数理・データサイエンス教育強化拠点コンソーシアム」
　のスキルセットに依拠
■具体的、体験的に学べる応用例、練習問題を収録
■フルカラーで見やすい構成

新刊

データサイエンスのためのデータベース

吉岡 真治 / 村井 哲也・著　　水田 正弘・編

最新刊

B5 変・160 頁・本体 2,400 円（税別）　ISBN 978-4-06-519310-5

データベースを分析・活用する読者を想定し、ＳＱＬによるデータ操作から、関係データベースの基本とその使い方、データの可視化、ＮｏＳＱＬ、関係データベースを用いた実践的なデータ分析事例を解説した。

既刊

スパース回帰分析とパターン認識　新刊

梅津 佑太 / 西井 龍映 / 上田 勇祐・著

B5 変・208 頁・本体 2,600 円（税別）　ISBN 978-4-06-518620-6

モンテカルロ統計計算　新刊

鎌谷 研吾・著　駒木 文保・編

B5 変・192 頁・本体 2,600 円（税別）　ISBN 978-4-06-519183-5

データサイエンスのための数学

椎名 洋 / 姫野 哲人 / 保科 架風・著　清水 昌平・編

A5・304 頁・本体 2,800 円（税別）　ISBN 978-4-06-516998-8

データサイエンスの基礎

濵田 悦生・著　狩野 裕・編

A5・192 頁・本体 2,200 円（税別）　ISBN 978-4-06-517000-7

統計モデルと推測

松井 秀俊 / 小泉 和之・著　竹村 彰通・編

A5・224 頁・本体 2,400 円（税別）　ISBN 978-4-06-517802-7

最適化手法入門

寒野 善博・著　駒木 文保・編

A5・256 頁・本体 2,600 円（税別）　ISBN 978-4-06-517008-3

Python で学ぶアルゴリズムとデータ構造

辻 真吾・著　下平 英寿・編　　B5 変型・208 頁・本体 2,400 円（税別）　ISBN 978-4-06-517803-4

実践 Data Science シリーズ

Python ではじめる Kaggle スタートブック

たちまち重版

石原 祥太郎 / 村田 秀樹・著　B5 変・192 頁・本体 2,000 円（税別）　ISBN 978-4-06-519006-7

初学者向けのKaggle入門書の決定版！サンプルコードの詳細解説でしっかり身につく。優勝チームと専業Kagglerのコンビによる、安定のわかりやすさ。「Kaggleで勝つ」準備をしよう！本音対談コラムあり。

これからのロボットプログラミング入門

Python で動かす MINDSTORMS EV3

新刊

上田 悦子 / 小枝 正直 / 中村 恭之・著　B5 変・240 頁・本体 2,400 円（税別）　ISBN 978-4-06-518618-3

LEGO MINDSTORMSを用いるロボットプログラミングもPythonで！
EV3ソフトウェアからEV3 MicroPythonへ。ソースコードの解説がていねいだから大丈夫。プログラムを書いて、すぐロボットが動くからSTEM教育の導入としても最適。センサ、機構、ライントレース、Open Roberta Labなどの発展的な話題も豊富。さあ、はじめよう！

東京都文京区音羽 2-12-21
https://www.kspub.co.jp/

講談社

編集　☎03(3235)3701
販売　☎03(5395)4415

〔表 2 対向〕

とめ 株式会社とめ研究所

～知能情報処理技術をコアコンピタンスとした
ソフトウェア研究開発受託会社～

◆情報処理の研究経験者が多く活躍する当社では、現在、ソフトウェアリサーチャー（研究職）を採用中

◆情報処理の研究で培った深層学習、画像処理等の経験を先端ソフトウェア研究開発で発揮しませんか

●当社エンジニアの５割が博士号取得者、８割が博士課程出身

活かせる力　博士課程での研究で培った課題追究力、論理的思考力、実用的な数学の経験（統計、シミュレーション、データ解析等）を重視。プログラミング技術は研修等で習得できます。

業務内容　最先端ソフトウェアの研究開発
人工知能、機械学習・ディープラーニング、データサイエンス、画像処理、検査・計測・ロボット、自然言語処理、ヒューマンインタフェース、組込み制御などの新アルゴリズム研究開発。

採用条件　ライフワークとして、研究開発への意欲が強い方
・博士号の取得、博士課程での専攻分野、プログラミング経験はいずれも不問。
・博士後期課程修了／中退見込、あるいは修了／中退後５年程度以内の方。
・日本語でのドキュメント作成や打ち合わせなどが可能なネイティブレベルの日本語力をお持ちの方。

募集期間　随時

勤務地　希望考慮（原則住居の移動を伴う転勤なし）
・当社ラボ／京都本社・京阪奈・名古屋・横浜・東京・筑波
・当社ラボ周辺の客先プロジェクト所在地

応募方法　当社ＨＰの応募フォームよりご応募下さい。

連絡先　管理企画センター 人事部 吉田・福原・岩前、e-mail: saiyou@tome.jp

面白い事をやって社会や生活を変える

「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/

〔前付最終〕

FIT2020 第 19 回情報科学技術フォーラム
聴講参加並びに講演論文集 事前予約申込の御案内

https://www.ipsj.or.jp/event/fit/fit2020/

電子情報通信学会の情報・システムソサイエティ（ISS）とヒューマンコミュニケーショングループ（HCG）、及び情報処理学会（IPSJ）は、今年も「第19回 情報科学技術フォーラム(FIT：Forum on Information Technology)」を開催します。会期と会場は下記の通りです。

つきましては、聴講参加並びに講演論文集の事前予約申込の御案内を致します。皆様、奮ってお申込み下さい。

聴講参加費は、当日参加よりも事前予約の方がお得になっております。また、講演論文集（冊子、DVD-ROM）は、FIT開催中にも会場販売を行いますが、残部のある限りということになりますので、確実に御入手頂くには期限内のお申込みをお勧め致します。

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）
交　通：新千歳空港から札幌駅までJR線快速エアポートにて約40分
または「札幌都心行」のバスにて 約1時間10分、JR線札幌駅北口から構内まで徒歩約7分
※お車での御来場は御遠慮下さい。車イス等で駐車場が必要な場合は事前にお知らせ下さい。

■開催イベント企画（詳細は逐次上記Webサイトに掲載致します）
※タイトル等は変更の可能性があります。

[表彰式・招待講演企画]
◎FIT学術賞表彰式
2日 13:00-13:50　第1イベント会場（工学部B棟オープンホール）

◎特別講演
2日 9:30-12:00　第2イベント会場(フロンティア科学研究センター2Fレクチャーホール)
「NoMapsが切り拓く地図なき世界（仮）」
伊藤博之（クリプトンフューチャーメディア代表取締役)、廣瀬岳史（NoMaps実行委員会事務局長）他
2日 15:30-17:30　第1イベント会場（工学部B棟オープンホール）
「深層学習の源流を探り、未来を拓く」
福島邦彦(元NHK放送技術研究所)、甘利俊一(東京大学名誉教授、理化学研究所栄誉研究員)

◎船井業績賞受賞記念講演
2日 14:00-15:15　第1イベント会場（工学部B棟オープンホール）
「半世紀を経て　いつでもどこでもCG時代に」
西田 友是 （広島修道大学教授（東京大学名誉教授）／プロメテックCGリサーチ所長）

[イベント企画]
詳細は逐次上記Webサイトに掲載致します。

■聴講参加費（税込）

参加区分	事前予約(7/10まで)	当日
会　員	10,000円	12,000円
非会員	20,000円	24,000円
学　生	無料	無料

※会員、非会員の聴講参加費にはプログラム・参加章・電子版講演論文集（Webからダウンロード）が含まれております。
※学生の聴講参加はプログラム・参加章のみとなっております。
電子版講演論文集(DVD-ROM)が必要な方には学割会場価格4,000円にて販売致します。
※会員、非会員、学生の参加区分の区別は次の通りです。
会　員：情報処理学会、電子情報通信学会、電気学会、照明学会、映像情報メディア学会及び電子情報通信学会と協定を締結した海外の学会（IEIE、KICS、KIISE、REV、IEEE/CS、IEEE/ComSoc、IEEE/PHO、IEEE/MTT-S）または情報処理学会と協定を締結した海外の学会(ACM、IEEE、IEEE/CS、KIISE、CSI）の個人会員、電子情報通信学会の維持員、情報処理学会の賛助会員。
非会員：上記の学会会員以外で学生以外の方。
学　生：会員/非会員を問わず無料（電子版講演論文集は付きません)。

■情報交換会
開催日時（予定）：9月2日（水）18：00～20：00
会場：札幌サンプラザ
※当日申込のみとなります。参加費等は逐次Webサイトに掲載いたします。

■冊子講演論文集・DVD-ROM販売価格（税込）

申込種別	個人購入価格	法人購入価格
講演論文集セット（DVD-ROM付）	60,000円	60,000円
講演論文集分冊	13,000円／冊	16,000円／冊
講演論文集DVD-ROM	10,000円	56,000円

※講演論文集セットは冊子講演論文集全分冊(カバー付き)、DVD-ROM付き

※講演論文集の掲載分野（予定分冊構成）
第１分冊：モデル・アルゴリズム・プログラミング、ソフトウェア、ハードウェア・アーキテクチャ
第２分冊：データベース、自然言語・音声・音楽、人工知能・ゲーム、生体情報科学
第３分冊：画像認識・メディア理解、グラフィクス・画像、ヒューマンコミュニケーション＆インタラクション、教育工学・福祉工学・マルチメディア応用
第４分冊：ネットワーク・セキュリティ、ユビキタス・モバイルコンピューティング、教育・人文科学、情報システム
DVD-ROM ：上記全論文とプログラムを収録

■聴講参加、講演論文集の申込
申込締切：2020年7月10日（金）
申込方法：FIT2020 Webサイトからお申込み下さい。
※講演論文集はFIT開催中にも会場販売を行いますが、残部のある限りということになりますので、確実に御入手頂くには期限内のお申込みをお勧め致します。

■次年度のFIT2021開催
2021年8月25日（水）～27日（金）東北学院大学にて開催予定

■問い合わせ（FIT2020事務局）
〒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　事業部門
TEL〔03〕3518-8373　FAX〔03〕3518-8375
E-mail：ipsjfit@ipsj.or.jp

〔目次前〕

6

PREFACE

巻頭コラム

546 「世界のあしたが見えるまち」から民主主義へのささやかな貢献を　五十嵐立青

SPECIAL ARTICLE

特別解説

548 情報処理学会第 82 回全国大会　実録 緊急オンライン開催　岡部寿男・中沢　実
552 電子カルテの安全な導入と運用―宇陀市立病院事件を事例に　黒田知宏

SPECIAL FEATURES

特　集

ハードウェアセキュリティの最新動向

558 0. 編集にあたって　松本　勉・佐々木貴之・石黒正揮
560 1. ハードウェアに対する物理攻撃―サイバーだけでなくフィジカルも守る―　本間尚文・上野　嶺
564 2. ハードウェアを用いた暗号処理の高速化　坂本純一・吉田直樹
568 3. ハードウェアトロージャンの脅威と検出　林　優一・川村信一
572 4. 計測セキュリティ―サイバー空間と物理空間のつなぎ目における脅威とその対策―　松本　勉・鈴木大輔
576 5. Trusted Execution Environment によるシステムの堅牢化　須崎有康・佐々木貴之
580 6. 自動車サイバーセキュリティの基本―車載ネットワークと攻撃例―　Camille Gay

小 特 集

差分プライバシ

584 0. 編集にあたって　袖美樹子
586 1. データプライバシ保護技術と差分プライバシ　古川　諒
591 2. 差分プライバシの基礎と動向　寺田雅之
600 3. 局所差分プライバシの最新動向　福地一斗・佐久間淳

ミ ニ 特 集

ET ロボコン：異色の情報系ロボコン
―光る若手にインタビュー―

608 0. 編集にあたって　平山貴司
610 1. ソフトウェア教育・実践の場としての ET ロボコン―時代に合わせたモデリング課題の提供―　土樋祐希
614 2. KAMOGAWA の訓練生にインタビュー　小西康介・内田賀子・神原太朗・竹歳留加・（聞き手）平山貴司
617 3. がんちゃん +X の学生にインタビュー　海沼滉樹・佐野祐輔・槇　翔史・山内大七洋・（聞き手）平山貴司

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

※各記事に指標がついていますのでご参考になさってください

IPSJ MAGAZINE
情報処理学会誌
Vol.61 No.6（2020 年 6 月号）
通巻 663 号

情報処理

ARTICLE

解 説

620 準委任契約はアジャイル開発を促進できるか―アジャイル開発導入に躊躇する発注側の課題― 秦泉寺久美

連載：買い物自慢

557 3D プリンタのキットを買ってみた 稲津和磨

607 連載：集まれ！ジュニア会員！！

教育コーナー：ぺた語義

627 1 人 1 台学習者端末について考える 望月陽一郎

628 実践的演習を伴うサイバーセキュリティ公開講座の取り組み 丸山一貴・佐々木伸彦・高谷宏幸

632 再帰的思考のすすめ 中川正樹

連載：情報の授業をしよう！

636 専門学科「情報科」における情報コンテンツ分野の指導 長堂忠司

連載：ビブリオ・トーク―書評―

642 誰でもすぐに戦力になれる未来食堂で働きませんか ゆるいつながりで最強のチームをつくる 森田 一

連載：5 分で分かる!? 有名論文ナナメ読み

644 Prévost, R. et al : Make It Stand : Balancing Shapes for 3D Fabrication 梅谷信行

連載：IT 紀行

646 全国大会がオンライン開催！ 公開セッション「先生，質問です!」の裏側お見せします 山本ゆうか

648 ほっとタイム
649 ほっとタイム
649 論文誌ジャーナル掲載論文リスト
649 論文誌トランザクション掲載論文リスト
650 会員の広場
652 IPSJ カレンダー
652 2020 年度定時総会の開催について
654 人材募集
655 英文目次／次号予定目次
656 アンケート用紙
658 編集室
659 掲載広告カタログ・資料請求用紙
660 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・中田眞城子
担当理事：楠 房子・清水 佳奈
本号エディタ：
石黒 正揮・稲葉利江子・井上 仁・江渡浩一郎・大石 康智・大川 徳之・太田 智美・折田 明子・金子 格・川上 玲・河原 亮・久野 靖・欅 惇志・佐々木貴之・須川 賢洋・関谷 貴之・袖 美樹子・高木 拓也・中島 一彰・西川 記史・坂東 宏和・平山 貴司・細野 繁・堀井 洋・福地健太郎・古川 雅子・古川 諒・坊農 真弓・松本 勉・水野加寿代・山本ゆうか・湯村 翼
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）ジヨウホウシヨリガツカイ
■規格部 情報規格調査会
〒 105-0011 東京都港区芝公園 3-5-8 機械振興会館 308-3
Tel(03)3431-2808 Fax(03)3431-6493
E-mail: standards@itscj.ipsj.or.jp https://www.itscj.ipsj.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

Copyright 2020 IPSJ 本誌に出てくる製品名等は，各社の商標または登録商標です.

［巻頭コラム］

「世界のあしたが見えるまち」から民主主義へのささやかな貢献を

■ 五十嵐 立青

およそ20年前，イギリスの大学院で電子政府について研究をしていた．リサーチアシスタントとして所属していたのはGovernment on the Web (http://www.governmentontheweb.org/)という研究チームで，世界各国の行政情報がどのように電子化されサービスとして提供されているかの検証を行っていた．電子政府e-Governmentというややレトロな響きが示すように，研究の中心はあくまでも行政体にあったが，同時にそこでは電子民主主義e-Democracyについてもさまざまな議論が行われていた．新しいテクノロジーにより情報へのアクセスの形が変わり情報量の不均衡が是正されるのか？　完全な情報を持つことによって一人ひとりがものごとを主体的に判断し意思表示できるようになるのか？　携帯電話から投票が可能になることで既存の政治の仕組みは変わるのか？　といった未来への期待がある一方で，情報を持っても合理的な選択をできるわけではない，すべての情報を吟味できるわけではないので政党のように情報を集約する存在は今後も必要とされる，という視点が主流であった．その中でも大きなテーマだったのは技術とそれを運用する人間の信頼性であった．我々はコントロールされた情報しか見えないのではないか，電子投票した自分の票が自分が選んだ候補者にカウントされていることをどう担保するのか，情報が改ざんされてしまうのではないか，他人のなりすまし投票をどうやって防ぐのか，といった懸念に対して当時は解決策を見出すことはなく，その実現は未来のいつの日かくるのだろうと思いながらもSF映画よりも少しだけリアリティがある程

■ 五十嵐 立青
つくば市長

1978 年生まれ．筑波大学国際総合学類，ロンドン大学 UCL 公共政策研究所修士課程，筑波大学大学院人文社会科学研究科修了，博士（国際政治経済学）．つくば市議を経て，2016 年よりつくば市長．

度のものだった．

その未来は想像したよりも早くやってきた．

2018年，つくば市は日本で初めてブロックチェーンとマイナンバーカードを組み合わせたインターネット投票を行った．それは政治家を選ぶ選挙ではなく，つくば市が行う社会実装プロジェクトの選考過程で市民投票の形で行われた．ブロックチェーンによるクローズドなシステムを構築し，ノード間で相互監視をすることで，自分の票が確かに意中の行き先に届くことを担保した．同時に，マイナンバーカード内の情報とパスワードを組み合わせる認証によって，なりすましを防ぎ本人が投票していることを確認することが可能になった．さらに翌年には，マイナンバーカード内に保存されている顔画像に端末のカメラによる顔認証を合致させることで，よりセキュアかつシンプルな投票を可能にした．今後マイナンバーの機能がスマートフォンに実装されれば利便性は高まるだろう．まだ課題はあるが，この取組みが技術的には選挙においてもインターネット投票が可能であることを示したことは意義があると考えている．本格的な実施には法改正も含めて整備が必要になるが，それらが実現し，一人ひとりがリアルタイムに意思表示をできる日が来た際には民主主義のあり方もまた変わっていくかもしれない．「世界のあしたが見えるまち」をヴィジョンとして掲げるつくばから，そんな人類の未来にささやかでも貢献したい．

情報処理学会第 82 回全国大会
実録 緊急オンライン開催

岡部寿男 | 第 82 回全国大会運営委員長／京都大学
中沢 実 | 第 82 回全国大会プログラム委員長／金沢工業大学

全国大会オンライン開催を振り返って

2020 年 2 月，新型コロナウイルス感染症の拡大が始まった．第 82 回全国大会（2020 年 3 月 5 ～ 7 日）は急遽オンライン開催となったが，多くの方々のご協力に支えられ，大きなトラブルなく終えることができた．それから 1 カ月の間に多くのことが起きてその対応に追われる日々が続いているが，端緒となった，本会として初，我が国でも前例のない大規模なオンライン開催の経緯を，記憶が薄れないうちに記録として残し，事後の検証を行えるようにして今後につなげられるようにすることが大事であると考え，ここに報告の機会をいただいた．あえて美談とはせず逡巡した経緯や反省すべき点も包み隠さずに記載したい．

現地開催中止の判断に至るまで

2020 年の年初から新型コロナウイルス感染症の問題は騒がれていたが，開催 1 カ月前の 2 月上旬の時点でも，本大会の開催そのものに大きな影響があるとは予想できていなかった．2 月 18 日に DEIM2020（第 18 回日本データベース学会年次大会，3 月 2 ～ 4 日），19 日には言語処理学会第 26 回年次大会（NLP2020，3 月 16 ～ 19 日）の現地開催中止とオンライン開催が決定されたのを受けて，本会でも 20 日夕に臨時の大会運営委員会を招集して対応を協議したが，その時点での判断は基本は現地開催で，一部のイベントについて対応を検討するにとどまっていた．

しかしながら，翌 21 日午前になり改めて状況を分析し諸条件を検討，金沢工大側とも相談して，やはり現地開催は難しいとの判断に至り，会長の判断を仰いで本会として最終的に現地開催中止を決定した．最小限のアナウンスを起草し 15 時に Web 掲載し，メールや SNS などを通じて広報に努めたが，このときは「現在，プログラムの一部のオンライン開催などの可能性を検討しております」と書くのが精一杯であった．

なお翌週の 26 日に安倍首相が記者会見で以後 2 週間のイベント中止を要請し，本会に限らず 3 月に予定されていた学会のイベントはほぼすべてが現地開催を中止することになった．結果的に，21 日午前の時点で全国大会の現地開催中止を決断できていたことで，オンライン開催の準備のための時間が辛うじて取れたといえる．

オンライン開催の検討

21 日 17 時から再度緊急の大会運営委員会を招集し，善後策を検討した．現地開催の中止に伴う諸々のキャンセルの折衝は齋藤正史実行委員長に任せる

ことにして，運営委員と事務局でオンライン開催の可能性を探った．事前申込者には 20 日に講演論文集のダウンロード URL が通知済みであり，発表は成立していると考えて，単なる中止にしてしまうという選択肢もあった．しかし，講演発表者の方々に対して学会としてベストエフォートであっても何か発表の場を提供することが使命であろうと考え検討した結果，一般セッション・学生セッションについてインターネットを介したビデオ会議システムを使ってオンライン開催を実施する可能性が見えてきた．

全国大会は，例年であれば参加者数が 3 千人を超えるかなりの大規模学会である．オンライン開催の場合の参加者の見積りは難しいものの，セッション数 153，講演数 1,135 という大きい数字を扱わねばならないことは疑いない．しかし，各セッションの発表数は最大 9 であり，セッションの参加者は通常開催の場合は 1 教室に収まる 30 人くらいと規模は大きくない．オンラインのセッションの場合，発表者，座長，聴講者がセッション会場に対応するビデオ会議に遠隔参加し，発表者が画面共有を使ってプレゼン資料を提示しつつ話せば通常と同等のことができる．オンライン開催を元のプログラムと同じセッションに時間を組むことにしてセッション会場の数と同じ 31 並列のテレビ会議開催ができる契約をすれば，原理的には完全オンラインの開催が可能である．

一方で，懸念される点もあった．一つは，参加者がビデオ会議でのプレゼンに慣れていないことである．単なる会議ではなく画面共有やチャットなどを駆使したものであり，発表者や座長に大きな負担をかけトラブルも予想される．もう一つは，サポート体制が不十分であることである．通常であれば開催校の学生にアルバイトをお願いして座長のサポート業務を行う．しかし今回は新型コロナウイルス感染症の拡大防止を考えると，当日何十人ものアルバイト学生をどこか 1 箇所に集めて作業させるようなことは避けるべきであるし，オンラインで作業してもらうための機材の手配や講習も難しい．

以上のような技術上・運用上の課題は見えていたものの，「情報」を冠する学会としてできることはやるべきという考え方で，試行等ではなく正規のセッションとして開催し，大会優秀賞等の表彰の対象とすることにした．一方オンラインの発表が難しい講演者がいることを考え，発表そのものは講演論文集の公開をもって成立しているものとした．オンライン開催は参加登録（講演参加，聴講参加）している人だけが参加できる形とした．

ビデオ会議システムとしては Zoom を使うことにした．Web で簡単に申し込めて，1 カ月だけであれば余裕をみて 40 並列，1 会議当たり最大 300 人の契約をしても 10 万円未満に収まった．

週末に簡単な技術的検証を行い，大きな問題は見つからなかったことから，25 日午後にオンライン開催に関して正式のアナウンスを出した．その後，イベントセッション 1 企画について同様に Zoom を使うことになったほか，「先生，質問です！」公開セッションは cluster というバーチャルリアリティ環境で開催，また中高生情報学研究コンテストはインターネット上のポスター公表とオンライン審査を行うこととなった．

開催準備

26 日に，講演発表者と座長に，オンライン開催のお願いと可否を問う連絡を行った．座長に加えて，万一座長が接続できなかった際の代理のほか座長業務を手助けする「座長補佐」をお願いすることとし，その選任もお願いした．当然ながら，運営上の不備や懸念について多くのお叱りやご指摘をいただいた．一方でオンライン開催に対する激励や期待の声もいただいたのはありがたかった．

次に，オンライン開催ならびに Zoom 接続の案内を Web 上に用意した．内容は随時更新の必要があ

ることからポータルサイトを Google サイトに開設し，それ以外の文書も Google Drive に置いて関係者で編集権限を共有した（図 -1）．また IOT 研究会のオンライン開催を準備していた中村素典・京大教授より，Zoom 接続の手引きのドラフトを入手し，全国大会用にカスタマイズして利用させてもらった．それに加えて発表者，座長，聴講参加者それぞれの立場で，スライド共有の方法や質疑応答の手順などを文書化し順次掲載していった．ポータルサイトは 28 日に公開し，合わせてオンライン開催になったこととお詫びとご協力のお願いを掲載した．

開催当日

Zoom に不慣れな参加者に対する対応として，開催前日と会期中，学会事務局でサポート用の Zoom を立ち上げておき，そこで接続テストや質問に対応することとした（図 -2）．数えている余裕はなかったがとても多くの方がきちんと事前に接続テストを行ってくれた．また運営側でも接続に伴うありがちなトラブルの情報を共有することができた．事務局にはかなりの負担であったと思うが，これがトラブルを減らす鍵になったと思う．

当日の各セッションの運営は基本的に座長にお任せし，裏方として学会事務局が Zoom と電話で対応にあたるほか，金沢工大と京大とにそれぞれ学生アルバイト少数名からなるサポートチームを置き，各セッションを巡回させた（図 -3）．

当日の参加者数を正確に数えるのは難しいが，いずれかの形で参加登録した人の合計は 2,419 名となる．発表数の最も多い第 2 日目の午後は 29 のセッションに総計 614 名が同時参加していた．参加者数最多のセッションは 37 名であった．当日聴講参加登録者は 193 名であり，オンライン開催だったので参加できたという声も多く聞かれた．

オンライン開催に切り替えたことで，予稿に掲載された講演発表 1,135 件中オンラインでの発表を行ったのは 753 件にとどまった．発表が行えなかった理由として，企業の方はオンラインでの発表許可を取り直す手続きが間に合わなかった，学生の方は感染症対策により大学への登校を制限され発表準備が行えなかった，などを聞いている．結果として，少数ながら一部のセッションで発表数が非常に少なくなってしまい，発表者と座長にご迷惑をかけてしまったことは申し訳なく思う．

反省と今後に向けて

準備に手間も暇もかけることができず用意した最低限のサービスではあったが，発表者，座長，聴講

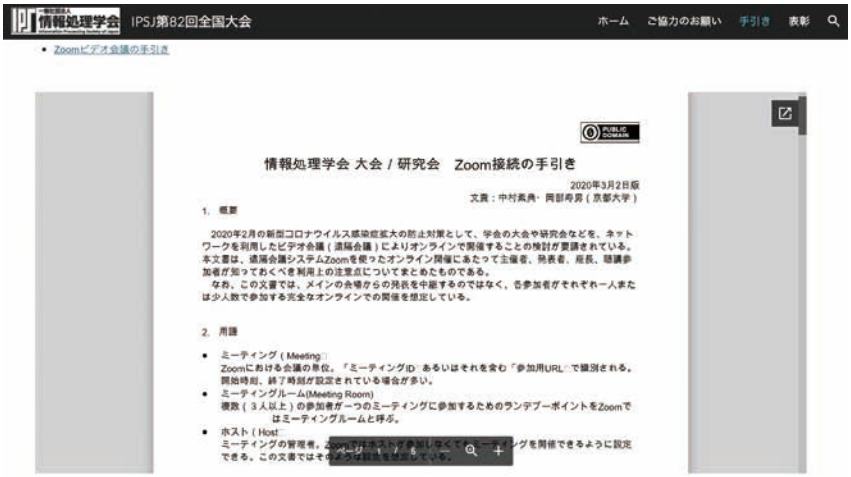


図 -1　オンライン開催ポータルと Zoom 接続の手引き

図 -2　オンラインサポートの様子（学会事務局）

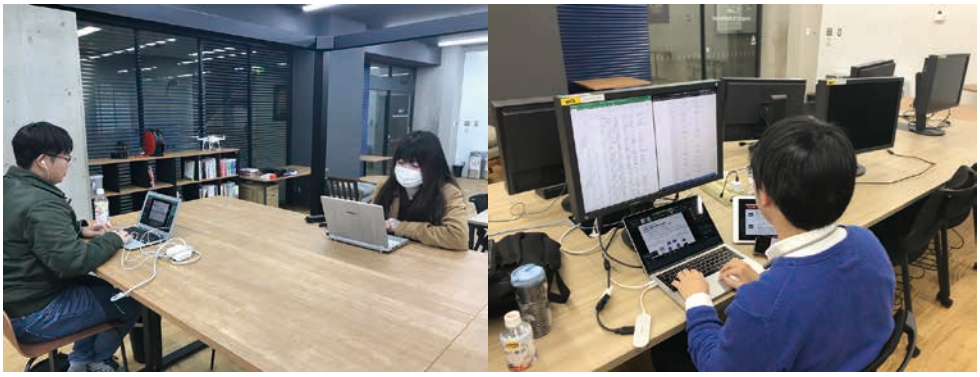


図-3　金沢工業大学でのサポートの様子

者各位がコンセプトを理解され臨機応変に対応くださったおかげで，幸い大きなトラブルなしに終えることができた．改めて御礼申し上げたい．またスポンサーのみなさまにはオンライン開催に切り替わっても支援を継続いただき感謝している．プレナリーセッションなどのアピールの場を提供できなかったのは反省点である．

2020 年度に入っても引き続き学会のイベントをはじめ諸行事がオンライン開催に切り替えられている．座長から運営上の課題や改善意見を挙げていただいたので，別の機会にまとめて公表し参考となるようにしたい．また紙面の関係で技術的な話題は割愛したが，IOT 研究会にて発表予定である[1]．

この間の大きな変化を振り返ると，果たしてこれが会誌に掲載されるころに世界がどうなっているのか，想像するのも恐ろしい．一日も早くコロナ禍が収束することを願う．

参考文献

1) 柏崎礼生，坂根栄作，込山悠介，中沢　実，岡部寿男：COVID-19 に対する参加者数 500 人超級の学会イベントのオンライン開催の知識共有，情報処理学会研究報告，2020-IOT-49（発表予定）．

（2020 年 4 月 3 日受付）

第 82 回全国大会ゴールドスポンサー

第 82 回全国大会シルバースポンサー

電子カルテの安全な導入と運用
―宇陀市立病院事件を事例に

応用

黒田知宏 | 京都大学医学部附属病院

事件の概要と予想される原因

宇陀市立病院は 2018 年 10 月 1 日に病院情報システム（HIS：Hospital Information System）を導入し，紙カルテから電子カルテへの移行を果たしたが，その直後の 10 月 16 日に電子カルテ本体がランサムウェア（GandCrab）に感染して 2 日間停止した．

同事件の調査は外部セキュリティ対策ベンダによって 2018 年 11 月と 2019 年 3 月の 2 回にわたって，また，2019 年 3 月から 9 月にわたって 5 回の会合を含む調査が外部有識者によって行われた．宇陀市は外部有識者会議の提言を受けて対策等を実施し，2020 年 2 月 28 日，全 31 ページに及ぶ「報告書」を発出した☆1．なお，残念なことに，報告書が出される直前の 2 月 2 日，この問題の対応にあたった同市職員が飛び降り自殺をしている☆2．

同報告書は，システムログなどの証拠保全が行われることなく，復旧時に管理端末が初期化されてしまっているので正確なことは分からないものの，「ルール違反」で HIS 系の LAN にモバイルルータなどの機器を通じて外部インターネットと接続された情報機器が接続され，外部から侵入を許してしまったと考えられるとしている．また，同報告書に書かれた今後の「技術的対策」の中で，リモートデスクトップ（RDP）の接続が攻撃に悪用されたとしていることから，RDP がさまざまなサーバに設定されていた上に，その設定がきわめて甘かったのであろうと想像される．加えて同報告書によると，同市は有識者会議から技術的問題と同時に，「病院のガバナンスに問題があった」との指摘を強く受けており，今後の対策を論ずる後段においてもガバナンス強化のための取り組みに一定の紙幅が割かれている．詳細は報告書自身に譲るが，示された 6 項目の対策は，きわめて一般的かつ基本的な事項でしかない．裏を返せば，何もなされてなかったことが透けて見える．

このように，導入ベンダ側は適切な技術的対策を施していないばかりか，外部回線と接続してはならないというきわめて基本的なルールを守ることもセキュリティインシデント対応の基本であるログの保全もできず，病院・市側は基本的なガバナンスがなっていなかったようである．端的に言うならば「揃いも揃ってみんなだめ」だったのであろう．

同事件は特別だったのか

筆者は大学病院の情報システム担当者として，20 年近く HIS の導入や管理に携わってきた．筆者の実体験や業界関係者の間で共有された事例に照らしてみたとき，宇陀市民病院事件をとりまく「揃いも揃ってみんなだめ」な状況は決して特別ではなく，むしろきわめてありがちな状況に思われる．外部有識者会議が設置されることなく業界関係者だけで事件調査が行われていたならば，「運が悪かったねぇ」で済まされてしまっていたかもしれない．

同事件は HIS の導入初期段階で発生している．この時期は，一般的に導入事業者から病院に運用が完

☆1 http://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/houkokusyo.pdf
☆2 http://www.naraseikei-np.com/news200302_002.html

全に引き渡されるより前であり，導入事業者の多くが調整や改修のためにHISに通常運用では用いない機器を接続していることが多く，管理が不安定になりがちである．ガバナンスの観点から見れば，主たる導入事業者が一義的な管理責任を負うことになるが，きわめて多くのサブシステムから構成されるHISの場合，その全てにきちんと目を配ることはそう容易ではない．加えて，近年保険財政が厳しい中，HISの導入・運用コストの低減が国会で取り上げられるほど目の敵にされ，導入コストを下げるために分割調達，すなわち，個別サブシステムごとの個別契約が行われることが増えてきており，ベンダごとの責任範囲が明確でないことも多い．聞くところによると，本事案でも分割調達がなされており，電子カルテベンダ，ソフトウェア導入SIer，ネットワーク導入SIerなどの責任範囲が不明確だったようである．

分割調達にありがちな責任範囲の不明確さを解消するためには，導入者側に社内SE部門を置き，強いリーダシップを発揮することが求められる．しかし，厳しい保険財政は病院にコストセンタであるSE部門を置くことを許さない．特に地方自治体の医療体制を支える自治体病院は財政的に逼迫していることが多く，SE部門が置かれていない，あるいは，置かれていたとしても，情報技術に明るくない人物1人あてがわれているだけのことが多い．国立大学病院長会議のもとには医療情報部長会議という筆者を含むSE部門長の立場にあるものが年に数回集まって議論を行う会議体があるが，「このたび，○○大学の医療情報部教授を拝命した○○です．私は○年間○○診療にあたってきましたが，コンピュータや電子カルテは素人です．一方で，当院の部門にはスタッフもおりませんので，電子カルテを1人で切り盛りせねばならず，不安でいっぱいです．これから一所懸命勉強して参りますので，皆様いろいろ教えてください」という新任挨拶をよく耳にする．国立大学病院ですらこのていたらくなのだから，地方自治体病院など推して知るべしである．

加えて，医療者の多くは業務の丸投げに慣れている．診療現場では高度技能者による分業が発達しており，医療機器は臨床工学技士が，薬剤は薬剤師が十分な調整を行ってから医師・看護師に提供される．新規導入時には，MRと呼ばれる医療機器メーカ，薬剤メーカのスタッフが病院に張り付いて手取り足取り使い方を教えてくれたりもする．当然HISも十分な調整を行ってから提供されるべきものと理解され，実際，大手病院のICU等への急性期系情報システムの導入時には「24時間導入企業のスタッフが張り付いていないとはふざけている」と憤る医療者にSEや導入企業が凍りつく場面にでくわすことも少なくない．そこに医療者不足が追い打ちをかける．地方自治体は医療者の確保に血道を上げており，三顧の礼で医療者を迎えるほかない．結果，医療者の自由を束縛するようなルールの設定などできようはずもなく，勢いガバナンスは失われてしまう．

丸投げ体質の素人を騙すのは簡単である．多くの自治体病院ではHIS調達仕様書の作成業務がコンサルタントと呼ばれる業種に丸投げされているが，自治体から相談を受けてコンサルタントを呼び，一通り話を聞いた上で，「ところでこの病院では物流管理にはどういう情報システムを導入するのですか?」と聞いたところ，真顔で「物流管理システムって何ですか?」と聞き返されたという笑えない話を，仲間の医療情報専門家から筆者が聞かされたのは一度や二度ではない．財政基盤が不安定で払いが悪いのに要求が多く，SI案件が「デスマーチ」的に増加しがちな医療分野に優秀なSEが残るはずもなく，概して担当者の技術力は高くない．こうして，情報技術に明るくない業者が丸投げ体質の素人を騙して導入された情報システムが，きわめて社会的ニーズの高いサービスの基盤として利用されることになる．ひとたびことが起これば，担当者は板挟みになり，心を病むまで追い込まれることになる．事実，電子カルテ導入のプロセスの中で心を病む例は，業者SE，病院スタッフとも後を絶たない．本件の最後に身を投げた担当者の心労はいかばかりであったかと考えると胸が痛む．

このように，宇陀市立病院の「揃いも揃ってみんな

だめ」な事例は，実はどこの医療機関でも起こり得る．いや，顕在化していないだけで，実は日々起こっているのかもしれない．保険財政が逼迫し，医療者不足が顕著な中でも，現場の医療者の献身的な努力で地域の医療体制がなんとか持ちこたえているのと同様に，現場の心ある SE やスタッフの献身的な努力でなんとか持ちこたえているというのが実情であろう．

規制はセキュリティを高めているか

社会の経済原理のメカニズムに任せて物事がなし遂げられないとき，とり得る手段は規制のみである．HIS を取り巻く規制は「ガイドライン」と「通知」の形で与えられている．

法的に電子カルテの利用が許されたのは，1999 年 3 月 22 日，厚生労働省健康政策局発通知第 517 号，厚生労働省医薬安全局発通知第 587 号，厚生労働省保険局発通知第 82 号，「診療録等の電子媒体による保存について」，いわゆる「三局長通知」[☆3] である．三局長通知から遅れること 5 年，2005 年 4 月には，診療録を含むすべての公文書の電子保存・電子作成を認める所謂「e 文書法」が施行され，三局長通知は e 文書法厚生労働省令の補完文書である「医療情報システムの安全管理に関するガイドライン」（厚労ガイドライン）に引き継がれ，以降これに呼応する形で，経済産業省や総務省から発出されたガイドライン群とともに，いわゆる「3 省 4 ガイドライン」が形成された．厚労ガイドラインの遵守は，診療報酬点数表の中で「診療録管理体制加算」の算定要件として参照され，この加算の取得は「急性期一般入院基本料」算定の施設要件に(結果的に) なっている．すなわち，厚生労働省は入院診療報酬の保険償還のために守らねばならないルールにすることで，医療機関に同ガイドラインの遵守を迫っているわけである．

厚労ガイドラインは，本稿執筆時点で有効な版（第 5 版）[☆4] で，本文 163 ページ，付属文書 75 ページにわたる大作である．なぜこれほどまでに長いかというと，1 つ 1 つの事項について具体的対処法を事細かに書いているからにほかならない．初期のガイドラインを作成した方々の話では，「情報技術の素人である医療者が言われたとおりにすればよいように細かく記載された」米国のガイドラインを範として作成されたそうである．実際，「パスワード」1 つとっても 4 ページに渡る解説の後，悪名高い「最長でも 2 カ月以内」に定期的変更を求める項目を含めた，5 項目にわたる「最低限のガイドライン」を定めている．

事細かに細部を記載することは，一見，情報技術に精通しない医療機関の情報セキュリティを高めるように思える．しかし，実際はそうはならない．情報セキュリティは，永遠に続く攻撃者との戦いである．ガイドラインに事細かに書かれた対策は，どのような防御態勢が敷かれているかを攻撃者に知らしめる情報でもある．ひとたびそこに書かれた防御方法の弱みが明らかになれば，敵は一気に攻め込んでくることになる．加えて，強いコスト削減圧力の中で利益を守らねばならない事業者にとっては，事細かに書かれた「最低限のガイドライン」は，それさえ守れば説明責任が果たされる「防具」として機能する．結果，ガイドラインを満たす防衛力の低い手法が採用され，事業者（ベンダ）も導入者（病院）も管理者（規制当局）もそれに満足してしまうこととなる．

手法を定めたガイドラインは，決してセキュリティレベルを高めることはない．

ファンタジーでは守れない

厚労ガイドラインの根底を貫く基本的な考え方は，情報空間の分離である．これは，「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の「B-2. 選択すべきネットワークのセキュリティの考え方」で，ネットワークの在り方を「クローズドなネットワーク」と「オープンなネットワーク」に分離し，後者に前者の倍以上の紙幅を割いて説明し，「C. 最低限のガイドライン」の 1 項目目で「選択するサービスの閉域性の範囲を事業者

☆3 https://www.mhlw.go.jp/www1/houdou/1104/h0423-1_10.html
☆4 https://www.mhlw.go.jp/stf/shingi2/0000166275.html

に確認すること.」を求め,「D. 推奨されるガイドライン」で「やむを得ず,従業者による外部からのアクセスを許可する場合は」と存在してはならないこととして外部接続を扱っていることからも見て取れる.厚生労働省のこの考え方は一貫しており,日本年金機構情報漏洩事件発覚直後の平成 27 年 6 月 17 日には「個人情報の適切な取扱に係る基幹システムのセキュリティ対策の強化について(依頼)」(図 -1)[☆5] と題した通知文書で,基幹系ネットワークと(インターネットに接続された)情報系ネットワークを物理的に切断し通信不可能な状態にすることを求め,次世代医療基盤法施行規則[☆6] 第 6 条四ニ (1) では,「外部の者との送受信の用に供する電気通信回線として,専用線を用いること.」を求めている.

しかし,外部接続をまったく持たない独立した HIS を構築することなど,土台不可能である.そもそも,オープンなネットワークへの接続が物理的に断たれていては,頻繁に提供されるセキュリティパッチを即時適用することさえできず,システムに不具合があった際に事業者からのリモートメンテナンスを受けることもできない.業者の拠点から遠く離れた地方の医療機関にとって,リモートメンテナンスの可能性を断つことは,重症患者の生命維持にかかわる情報システムの不具合発生によって即時に患者の生命が奪われることを許容することにほかならない.情報セキュリティを守るために医療安全を犠牲にすることは許されない.「規則と手順決めて 守って 見直して」[☆7] と厚生労働省自身が述べているように,規則や手順に「問題点や不都合な点が見つかったときには躊躇なく改善する」ことは,医療安全の要諦である.「守れないルールはルールが悪い」と考えねばならない.

宇陀市立病院事件は医療機関がランサムウェア被

☆5 https://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/270617-1.pdf

☆6 https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=430M60000582001

☆7 https://www.mhlw.go.jp/topics/2001/0110/tp1030-1f.html#8-4

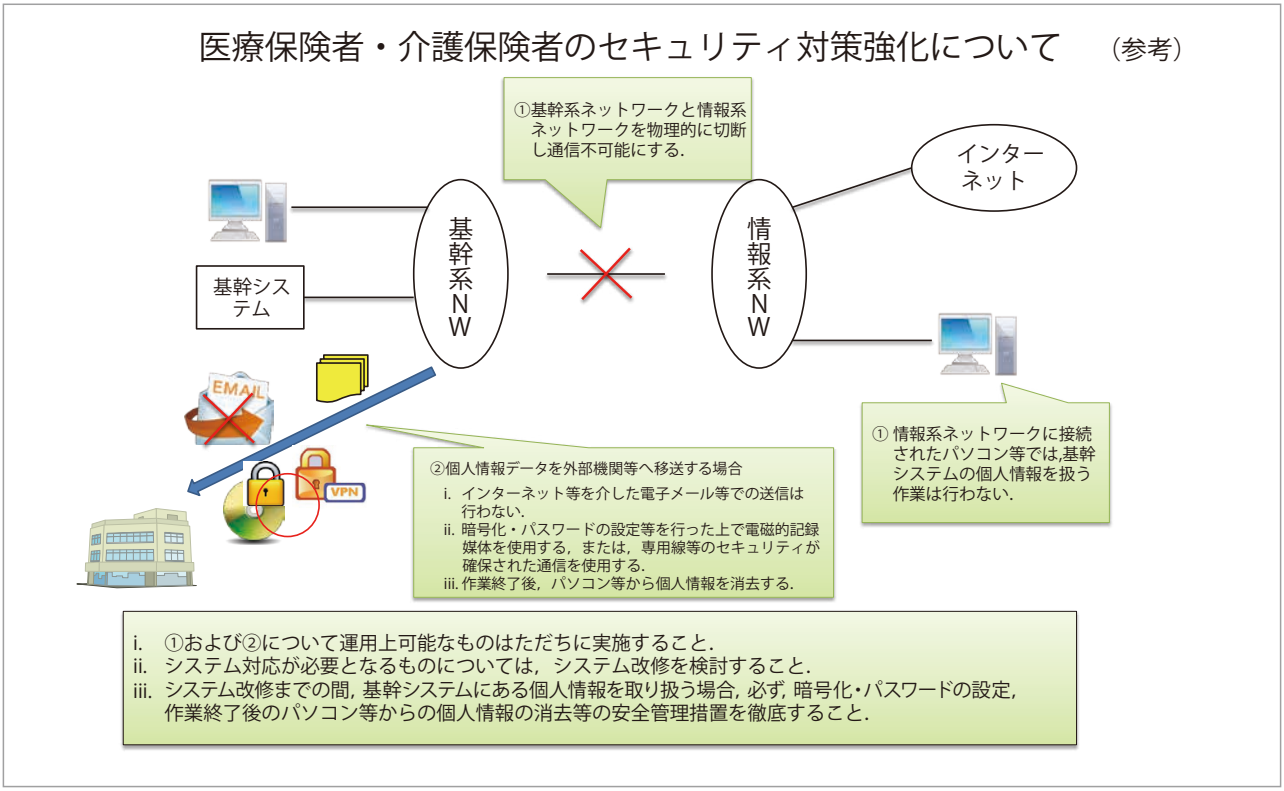


図 -1 平成 27 年 6 月通知文書参考図

害に遭った日本初の事例として，医療情報関係者の注目を集め，さまざまな情報がもたらされた．その中で，筆者を含む関係者が最もがっかりしたのは，「HISネットワークがインターネットに繋がるのが実態となっていることを踏まえて，そのための要件をガイドライン等で明確化すべき」と有識者会議の提言書に記載することを，厚生労働省が強く拒絶したという噂である．あくまでも噂にすぎないと言えば噂にすぎないが，厚生労働省のこれまでの一貫した態度からも，次世代医療基盤法関連政省令作製を支援する中で筆者が体験した関係省庁や国会議員，有識者などからの激しい圧力からも，「さもありなん」と感じさせる蓋然性はきわめて高い．医療情報関係者でこの噂を「根拠のない噂」と考える向きは１人もいないであろう．

「揃いも揃ってみんなだめ」は，宇陀市立病院関係者に限られた話ではない．規制当局である厚生労働省も含めて，「揃いも揃ってみんなだめ」なのである．

手段から目的への回帰

丸投げ体質の素人からなる現場と事細かなファンタジーからなる規制という「揃いも揃ってみんなだめ」な現実を変え，安全にHISが導入・運用されるためにはどうすればよいのだろうか．キーワードは，提言に示された「ガバナンスの強化」である．結局，導入者側が当事者意識を持って臨むほかなく，そうなるように規制をかけるほかない．

筆者は，「3省4ガイドライン」を整理統合し，「3省2ガイドライン」へ集約するにあたって，受託事業者を縛る経産省と総務省の統一ガイドライン作製の一翼を担うよう依頼を受けた．改定にあたって筆者たちがこだわったのは，「手段から目的への回帰」である．事細かな手段を書くのではなく，何を達成しなければならないのかという目的を記載し，その目的を達成する方法の選択を事業者に任せ，それを医療機関に説明して合意を得る責任を事業者に負わせることを基本的な枠組みとした．事業者の説明の中には，想定されるリスクの一部を受容することや，リスクを低減するための対策を採ることを，医療機関自身に求める説明までもが含まれている．医療機関が説明を理解して合意したのでない限り，それが原因で事故が発生した場合には，事業者は責任を問われることになる．こうすることで，示された手段を盲目的に達成しようとする「手段の目的化」を行う事業者を淘汰し，目的に沿って論理的に手段を選択し，適切に説明できる事業者のみが残ることを狙うとともに，医療機関にも説明を理解し，求められた対策を実施する「当事者意識」を持たせることを狙っている．合意した対策を実施していなかった医療機関は，事故発生時の責任のすべてを自ら負わねばならなくなる．事業者のガイドラインと見せて，実は医療機関にも努力を求めているのだ．

同ガイドラインは４月６日までのパブリックコメントを経て発出される予定であり，これに続いて，医療機関を縛る厚労ガイドラインの改定が行われる予定である．厚労ガイドラインの改定を司る委員会では，「パスワードの更新頻度をさらに上げて二要素認証を採らざるを得なくなるようにするのだ」といった政策誘導的な議論がなされているとの噂も聞こえてくるが，「二要素認証」などのすでに防衛力の綻びが明るみに出つつある些末な手段へのこだわりを棄て，「情報セキュリティを高める」という目的に立ち返って議論が行われることを期待したい．根底に立ち返れば，自ら考える力を持つことを病院に求めるほかないはずだ．

事業者も医療機関も目的に立ち返って自ら考え，「知彼知己者，百戦不殆」の構えをそれぞれが採ったときにはじめて，「みんなちがって みんないい」姿が現れるのではなかろうか．

（2020年3月29日受付）

■黒田知宏　tomo@kuhp.kyoto-u.ac.jp

1994年京大・工・情報卒業，1998年奈良先端大・情報修了，博士（工学）．奈良先端大学院助手，オウル大客員教授，京大講師，阪大准教授等を経て，2013年より現職．京大病院医療情報企画部長としてHIS企画・導入・運営にあたりながら，医学研究科と情報学研究科で医療情報学に関する教育・研究に従事．医療情報学会等会員．

稲津和磨 (@ina_ani http://twitter.com/ina_ani)

第8回 3Dプリンタのキットを買ってみた

■何でも作れる魔法の機械？ 「3D プリンタ」

3D プリンタとは「3D 形状を印刷できるプリンタ」です．さまざまな方式がありますが，ここでは積層式について紹介します（図 -1）．積層式の 3D プリンタは直径約 3mm の線状のプラスチックを加熱したノズルから押し出して，3D 形状を作るという装置です．例えるならホイップクリームを使ってケーキをデコレーションするように粘性のある素材を重ねていくことで 3D 形状を生成します．

■ 3D プリンタキットを購入

市場にはさまざまな 3D プリンタがあふれていますが，私が着目したのは「キット」です．これは 3D プリンタを作るために必要な部品のセットで，説明書に従い組み立てることで 3D プリンタを作ることができます．これらのキットのほとんどはオープンソースの 3D プリンタである RepRap を基としたものです．RepRap はオープンソースハードウェアとしてその仕様が公開されていて，インターネットを通じてさまざまなノウハウを知ることができます．

私は中国の通販サイト AliExpress でおよそ 2 万 3 千円でこのキットを買いました．このような激安の 3D プリンタのキットというのはお世辞にもよくできているとは言いがたく，説明書は当てにならず，部品の精度もそこそこです．しかし RepRap 自体が雑な部品でも動くように設計されているおかげで，意外と使い物になっています．AliExpress の在庫の状況はさまざまで，製品の品質もさまざまです．そのためこの記事に「コレがおすすめ」といった型番を書くことは難しいです．ぜひ自分で調べて，これならば！というものを見つけてほしいです．3D プリンタを組み立てる経験は，使う上でも非常に役に立ちます．3D プリンタはまだ完成した製品ではありません．うまく造形できないことはざらですし，機械が壊れてしまうこともよくあります．そのようなときにこの経験が生きてきます．

■ 3D プリンタによる電子工作製品の製作

私が 3D プリンタを買った目的は「自作電子工作作品の筐体づくり」でした．ここ最近電子工作のハードルはどんどん下がり，個人でも簡単にプリント基板を発注できるようになっています．ここまでくると，自分の作品を少し多めに作って見せびらかしたり，販売したくなってくるのですが，筐体づくりがネックとなっていました．1,000 個以上であればプラスチック樹脂の製造を依頼することもできますが 10 ～ 100 個程度のものはまったくコストに見合いません．3D プリンタを使うことで低コストで，同じ形の筐体を量産することができます．品質は市販のものに及びませんが，筐体として必要な性能は満たしています．そんなこんなで自作電子楽器 RakuChord（図 -2）を販売することができました．数十個の販売ですが 2000 年代に Web サービスを個人で作っていたあのワクワク感がここにはあるように思います．

■日常生活と 3D プリンタ

生活のちょっとした便利グッズも 3D プリンタで作ることができます．我が家ではホテルで見かける「Don't Disturb」の札や，コンセント取り回しのためのフック，表札などを 3D プリンタで作っています．生活のちょっとした不便を解決するために「モノ」が作れるというのは，なかなか新鮮な経験です．

3D プリンタの活用法は世の中的にもまだ未知数で，使う人によってさまざまな使い方ができます．ぜひ 1 つ購入してあなただけの「モノ」を作ってみませんか？

(2020 年 3 月 3 日受付)

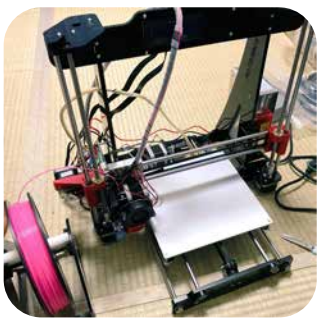


図 -1 3D プリンタ

図 -2 RakuChord

※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．

特集
Special Feature

ハードウェアセキュリティの最新動向

編集にあたって

松本　勉 | 横浜国立大学／産業技術総合研究所
佐々木貴之 | NEC／横浜国立大学
石黒正揮 | 三菱総合研究所

近年，Industrie 4.0 や Society 5.0 の実現に向けて，IoT（Internet of Things）やサイバーフィジカルシステムが重要となってきている．このようなシステムのセキュリティを担保するには，ソフトウェアに加えて，ソフトウェアが動作するプラットフォームであるハードウェアについても，セキュリティが担保されなければならない．なぜなら，ハードウェアはソフトウェアよりも低いレイヤで動作するため，ソフトウェアでは，ハードウェアレイヤの脅威への対応が難しいためである．ハードウェアレイヤの脅威の例として，ハードウェアチップから漏れ出る電磁波の物理的な観測による暗号鍵の解析（1 章）や，意図的な機能の停止や情報漏えいを引き起こすハードウェアトロージャン（3 章），センサに対する攻撃（4 章）が報告されており，これらのハードウェアレイヤの脅威はシステムの安全性に大きな影響を与える．一方，ハードウェアを活用したシステムの堅牢化として，暗号化処理の高速化（2 章），セキュリティ機能の保護（4 章）や，ハードウェアを含むシステム全体のセキュリティ，たとえば，自動車のセキュリティの検討（6 章）が進められている．

また，世の中の動向を見ると，アメリカのセキュリティ機関である NIST がハードウェアセキュリティのベストプラクティスの検討を開始したり，日本においても経済産業省が発行しているサイバー・フィジカル・セキュリティ対策フレームワークにおいてハードウェアの信頼性が言及されたりと，ハードウェアセキュリティの重要性の認識が広まっている．

システムの基盤となるハードウェアのセキュリティの知見は，セキュリティ分野の読者に限らず，幅広い読者に有用であると考え，本特集を企画した．本特集では，ハードウェアに対する攻撃やハードウェアを利用したシステムの堅牢化など，ハードウェアセキュリティに関する最新動向を広く俯瞰する．本特集の構成は以下のようになっている．

(1) ハードウェアに対する物理攻撃

ハードウェアはシステムの信頼の起点であり，安全なシステムを設計し運用するために，ハードウェアに対する攻撃を理解する必要がある．
東北大学 本間尚文氏と上野嶺氏が，ハードウェアへの物理的なアクセスによる攻撃手法について整理を行い，具体的な攻撃手法について解説している．

(2) ハードウェアを用いた暗号処理の高速化

ハードウェアを用いたセキュリティ機能の強化として，複数の署名を集約して署名サイズを削減する

集約署名やデータを暗号化したまま検索が可能な秘匿検索などの高機能暗号の高速化が挙げられる．

横浜国立大学 坂本純一氏と吉田直樹氏が，高機能暗号に用いられる数学的操作のハードウェアによる高速化について，ハードウェアの実装例を基に解説している．

(3) ハードウェアトロージャンの脅威と検出

ハードウェアを用いてシステムを堅牢化するためには，ハードウェア自体が信頼できなければならない．この際，IC 製造のサプライチェーンにおいて，チップ設計者が意図しない機能（ハードウェアトロージャン）の混入が脅威として指摘されている．

奈良先端科学技術大学院大学／産業技術総合研究所 林優一氏と産業技術総合研究所 川村信一氏が，ハードウェアトロージャンの全体像を整理し，その発見手法について解説している．

(4) 計測セキュリティ

IoT システムやサイバーフィジカルシステムは，センサから情報を収集し，その情報に基づいてアクチュエーションを行う．よって，測定の妨害やセンサや認識アルゴリズムをだますような攻撃が行われると，システム全体に影響を与える．

横浜国立大学／産業技術総合研究所 松本勉（本特集のゲストエディタ）と産業技術総合研究所 鈴木大輔氏が，センサを用いたシステムモデルを解説するとともに，攻撃対象となるセンサやシステムに与える影響について整理している．加えて，問題解決に向けた複数のアプローチを挙げている．

(5) Trusted Execution Environment によるシステムの堅牢化

暗号化などのクリティカルな機能を保護するために，それらの機能と一般的なアプリケーションの実行空間を CPU によって分離する技術（Trusted Execution Environment, TEE）の活用が期待されている．

産業技術総合研究所 須崎有康氏と本特集のエディタである NEC／横浜国立大学 佐々木貴之が，TEE のコンセプト，複数の実装とその特性について整理している．加えて，TEE の活用が見込まれるユースケースの紹介がなされている．

(6) 自動車サイバーセキュリティの基本

通信機能を備えたコネクテッドカーが普及し始めているが，自動車が攻撃を受け，自動車の制御システムに異常が発生すると，重大な事故につながる可能性がある．

産業技術総合研究所 Camille Gay 氏が，車載ネットワークの概要や，実際の攻撃事例，自動車業界特有の課題について解説している．

以上のように，ハードウェアセキュリティの分野では攻撃と防御の両方の観点からの検討や，IC チップレベルからシステムレベルまでの検討が行われており，日々技術が進歩している．本特集で紹介したハードウェアセキュリティに対する取り組みが，安全・安心な社会の実現に貢献することを期待したい．

（2020 年 3 月 2 日）

［ハードウェアセキュリティの最新動向］

①ハードウェアに対する物理攻撃
―サイバーだけでなくフィジカルも守る―

基般

本間尚文 東北大学　上野　嶺 東北大学

高まる物理攻撃のリスク

Cyber Physical System（CPS）や Internet of Things（IoT）といった新しい情報通信の形態においては，従来のサイバーセキュリティに加えて，実世界との接点となるハードウェアのセキュリティ（ハードウェアセキュリティ）が重要となる．現在，秘匿通信や認証といった情報セキュリティ上の機能は主に暗号技術によって実現されているが，ハードウェアへの物理的なアクセスによる攻撃（物理攻撃）は，暗号技術をも無効化し得る．また，そうした物理攻撃は，しばしば従来の情報セキュリティ技術の想定範囲外となるため，別途脅威分析や対策が必要となる．本稿では，以上の背景から，近年注目が高まるハードウェアに対する物理攻撃とその対策技術を概説する．

物理攻撃とは

本稿で取り上げる攻撃および対策は，主に暗号処理を実行する LSI（大規模集積回路）を対象に研究開発がなされてきたものである．これは，暗号処理の対象となるデータは本来保護されるべきものであり，最も攻撃の標的となり得る（攻撃に成功した場合の価値が高い）ことに起因する．しかし，近年では，これを発展させた汎用プロセッサに対する攻撃や機械学習処理への攻撃などの報告も増加傾向にある．

さて，本稿では，ハードウェアへの物理攻撃の中でも，特に現実的な脅威とされ，多くの事例が報告されている機密性に対する攻撃，すなわち処理中のデータを不正に収奪・解読することを目的とする攻撃について説明する．そのほかにも機能を錯乱・停止する攻撃やデータや処理の改ざん・偽造を行う攻撃，悪意のあるハードウェア機能（ハードウェアトロイなど）の埋込みによる攻撃などがあるが．それらについては本特集の他稿等をご参照いただきたい．

図 -1 に代表的な物理攻撃とその分類を示す．物理攻撃は，攻撃対象のハードウェアに手を加えるかどうかにより侵襲攻撃（Invasive attack）と非侵襲攻撃（Non-invasive attack）に大別される．侵襲攻撃では，LSI パッケージを開封・加工し，高解像度の電子顕微鏡や収束イオンビーム装置などにより，その内部構造や回路動作を静的に解析する．いわゆるリバースエンジニアリングも侵襲攻撃に分類できる．侵襲攻撃は IC カード内の LSI などに対しきわめて高い攻撃能力を持ち得るが，そのような攻撃は一般に高価な装置と高いスキルを必要とするため，実行できる攻撃者は限定される．

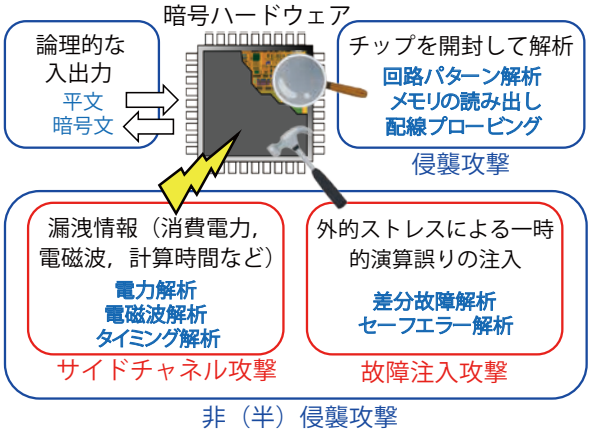


図 -1　代表的な物理攻撃とその分類例

一方，非侵襲攻撃は，その名の通りハードウェアの開封や加工等を伴わない攻撃である．その代表例が，ハードウェア動作中に副次的に生じる物理量（サイドチャネル情報）を観測して情報を奪うサイドチャネル攻撃である．これまでさまざまなサイドチャネル情報を利用する攻撃が報告されており，電力変動を利用する電力解析攻撃，漏洩電磁波を利用する電磁波解析攻撃，処理時間を利用するタイミング攻撃，発生する音を利用した音響解析攻撃などがよく知られている．これらの特徴は，侵襲攻撃と比べて安価な装置で実現でき，基本的に攻撃の痕跡を残さないことである．

もう1つの主要な非侵襲攻撃としては故障注入攻撃が知られている．サイドチャネル攻撃がサイドチャネル情報の観測を基本とする受動的な攻撃であるのに対し，故障注入攻撃は外部からハードウェアが誤動作する操作を加えて，その演算結果から情報を奪う能動的な攻撃である．誤動作の誘発には，たとえば電源電圧やクロック信号などに摂動（微細なゆらぎ）を加える方法が知られている．

近年では，チップ開封等を伴うが回路機能を恒久的に破壊せずに，回路動作を動的に解析する半侵襲攻撃（Semi-invasive attack）も見られる．同攻撃では，サイドチャネル情報の高精度な観測に基づくサイドチャネル攻撃や精緻な故障誘発を用いた故障注入攻撃といった，より強力な攻撃が実現されることが知られている．

以降では，典型的な非侵襲攻撃であるサイドチャネル攻撃と故障注入攻撃について述べる．

サイドチャネル攻撃

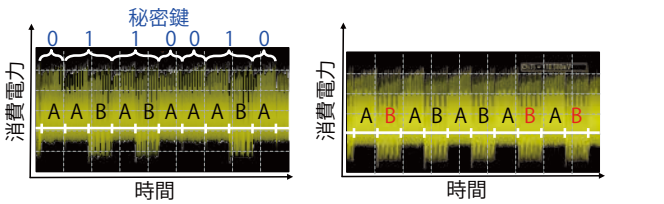
典型的な攻撃手法と対策

典型的なサイドチャネル攻撃の手法を，電力解析攻撃を例に解説する．電力解析攻撃では，ハードウェア動作中に生じる消費電力（電圧）の時間変化をディジタルオシロスコープなどの計測器で観測し，その観測データから処理内容を推定する．1990年代後半にKocherらによって単純電力解析（SPA：Simple Power Analysis）と差分電力解析（DPA：Differential Power Analysis）が発見されて以降，現在もその拡張や対策が盛んに研究されている[1]．なお，ほかのサイドチャネル情報（放射電磁波や動作タイミング）を用いた場合にも同様の解析手法が有効である．

SPAは測定した1つもしくは少数の観測波形を直接調べることで秘密情報を求める攻撃である．一例として，暗号処理を行うソフトウェアでは，しばしば秘密情報により命令系列が異なるため，その違いを波形から読み取ることで鍵を導出できる（図-2（a））．図のRSA暗号ハードウェアでは秘密鍵のビットが0もしくは1の場合にそれぞれ処理A（自乗算）もしくは処理AB（自乗算と乗算）を実行するため，電力波形から処理Aと処理Bを区別することで秘密鍵を推定できる．

DPAは大量の観測波形を統計解析することで秘密情報を求める攻撃である．数百から数十万といった波形数を必要とする一方で，SPAのように攻撃対象のアルゴリズムや構造に関する事前知識を必須とせずノイズに対しても強いという特徴を有する．データ依存性が小さく単一もしくは少数の波形観測では困難であった対象（暗号処理の場合，共通鍵暗号を処理するハードウェアなど）に対しても有効な攻撃とされる．

上記よりも攻撃者が有利な攻撃シナリオとして，攻撃対象の事前解析結果を活用することでより強力に秘密情報を収奪するプロファイリング攻撃もある．



(a) 未対策の電力波形：AとBの2つの演算パターンを消費電力から区別することで秘密情報を推定できる

(b) ハイディング対策を施した電力波形：ダミーの演算を挿入することにより演算パターンから秘密情報が推定が困難に

図-2　暗号ハードウェアへの単純電力解析と対策の例

事前情報の収集には攻撃対象と同等でかつ攻撃者が自由に操作・観測できる参照ハードウェアを用いるため，攻撃の前提条件は SPA や DPA と比べて厳しい．しかし，IC カードのような量産されるハードウェアやオープンソースソフトウェアを利用したシステムでは，考慮されるべきシナリオである．近年では，事前情報の学習に機械学習を用いた攻撃の報告が相次いでいる．

上記サイドチャネル攻撃への典型的な対策には，「隠蔽（ハイディング）」と「遮蔽（マスキング）」ある．ハイディングは，ハードウェアのサイドチャネル情報と内部処理や中間値との依存関係を隠す対策である．ハイディングの具体例として，図 -2（b）のようにダミーの演算あるいは相補的な演算を挿入し，内部処理が漏れを防止する対策がある（図 -2 (b)）．このときハードウェアは，単位命令あるいは各クロックで一定量の電力を消費するように設計される．一方，マスキングは，演算に用いる値にあらかじめ乱数を用いて変換し，サイドチャネル情報とアルゴリズムによって決まる真の中間値とを無関係とする対策である．マスキングによる対策は，アルゴリズム，アーキテクチャ，回路方式などさまざまな設計レベルでの適用が報告されている．

アーキテクチャラルサイドチャネル攻撃

近年，報告が急増しているサイドチャネル攻撃として，アーキテクチャラルサイドチャネル攻撃が挙げられる [2]．同攻撃は対象のアーキテクチャ的な特徴を利用することで，攻撃者が自らのプロセスを介して他者が実行中のプロセスの処理内容やデータを取得する．その代表例が 2018 年に報告された Meltdown と Spectre である．

図 -3 にアーキテクチャラルサイドチャネル攻撃のシナリオ例を示す．ここでは，攻撃者と他者がハードウェアを共有し，それぞれの演算コアで自身のプロセスを実行すると想定する．一般に，多くの演算コアでは階層的なキャッシュメモリを採用しており，ユーザはラストレベルキャッシュおよびメインメモリを共有する．攻撃者はたとえば Flush＋Reload や Prime＋Probe と呼ばれる手法を用いて他者のプロセスによるデータ読込を判別し，他者が実行した命令や処理データを収奪する．ここで，Flush＋Reload や Prime＋Probe では，当該データがキャッシュもしくはメインメモリから読み込まれるロード命令にかかる時間を観測することで，被攻撃者が当該データにアクセスしたかどうかを推測する．これにより，たとえば，被攻撃者が単位時間内で自乗算もしくは乗算を実行したか推測できるため，RSA 暗号に対し上述の SPA と同等の攻撃を実行することが可能となる．

アーキテクチャラルサイドチャネル攻撃は，上述の物理的アクセスを伴うサイドチャネル攻撃と異なりリモートで実行可能であるため，現在拡大するクラウドサービスが対象となり得る．特に，オープンソースの暗号ライブラリに対するアーキテクチャラルサイドチャネル攻撃による脆弱性が指摘されている．

故障注入攻撃

故障注入攻撃は，ハードウェアが実行する（暗号）演算に一時的な誤りを誘発し，誤った演算結果から処理内容を解析する．サイドチャネル攻撃対策が施された（暗号）ハードウェアであっても故障注入攻撃により秘密情報が取得される恐れがある．典型的

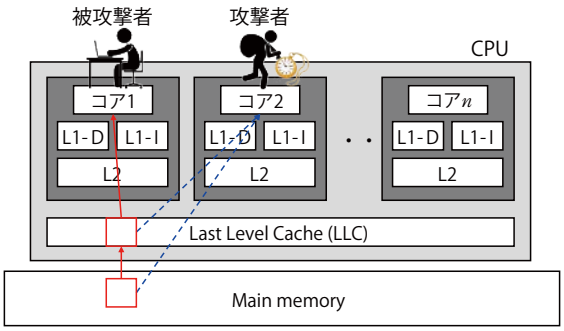


図 -3　LLC に対するアーキテクチャラルサイドチャネル攻撃のイメージ

な故障注入攻撃である RSA 暗号に対する Bellcore 攻撃や共通鍵暗号に対する差分故障解析（DFA：Differential Fault Analysis）では，理想的には 1 回の演算誤りから秘密情報を完全に抽出できる [3]．

一例として，図 -4 に RSA 暗号に対するセーフエラー解析攻撃を示す．図 -2（b）のように解析対象のハードウェアは演算 B のダミーを挿入するハイディング対策が施されており SPA では秘密鍵を推定することができないとする．そこで，攻撃者は演算 B（本来秘密鍵ビットが 1 のときのみに実行される乗算）実行時に誤りを発生させて，最終出力結果が正しいかを確認する．故障を注入した演算 B がダミーであった場合，故障の影響は最終結果に影響しない（図 -4（a））．一方，演算 B が本来の演算の場合，故障の影響が伝搬し，最終結果は誤りを含む出力となる（図 -4（b））．こうして，攻撃者はハイディング対策によって挿入されたダミーの演算 B と本来の演算 B を区別することができ，ダミーの演算 B を取り除くことによりハイディング対策を無効化し，秘密鍵を推定することが可能となる．

故障注入攻撃に対する対策は，センサやシールドを用いる対策と冗長性による対策がよく知られている．前者は物理的変動を検知・阻害するハードウェアを用いて攻撃の兆候を検知あるいは攻撃そのものを阻害する．たとえばレーザ照射によるメモリのビットフリップを検知するセンサなどが考案されている．後者は検算（たとえば，同じ処理を複数回実行し結果を確かめるなど）や誤り訂正符号により計算結果が正しいことを検証し，誤りを検知した場合は出力の停止等を行う．ただし，これらの対策により故障を検知しても検知後の処理内容から情報が漏洩する可能性がある点に注意が必要である．また，上述のセーフエラー攻撃では演算誤り発生の有無という情報のみを用いて秘密情報を取得するため，検算型対策のみでは防ぐことは難しい．このように想定される攻撃に応じて適切な対策を施すことが求められる．

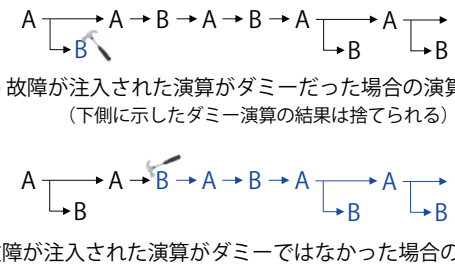


図 -4　RSA 暗号ハードウェアへの故障注入攻撃（セーフエラー解析）

今後の展望

本稿では，ハードウェアに対する物理攻撃の脅威と対策について概説した．サイドチャネル攻撃に代表される物理攻撃は，報告から 20 年が経過した今でも，日々新たな手法が報告されており，今後も半導体製造技術や計測・解析技術の進歩によって発展していくと予想される．ハードウェア設計者は，どのような物理攻撃の脅威が設計対象にあるかを考え，あらかじめ対策を施すことが肝要である．本稿がそうした脅威を把握する一助となれば幸いである．

参考文献

1) Mangard, S. et al. : Power Analysis Attack : Revealing the Secrets of Smart Cards, Springer (2007).
2) Yarom, Y. : Mastik : A Micro-Architectural Side-Channel Toolkit, https://cs.adelaide.edu.au/~yval/Mastik/ (Jan. 2020).
3) Joye, M. and Tunstall, M. : Fault Analysis in Cryptography, Springer (2012).

（2020 年 2 月 4 日受付）

本間尚文（正会員）　homma@riec.tohoku.ac.jp

東北大学電気通信研究所教授．専門は計算機システムおよび情報セキュリティ．用途や環境に応じた安全な情報システムの構築に興味がある．日本学術振興会賞，ドイツイノベーションアワードなどを受賞．博士（情報科学）．

上野　嶺（正会員）　ueno@riec.tohoku.ac.jp

東北大学電気通信研究所助教．専門は情報セキュリティおよび暗号実装．暗号を用いた情報システムの安全性評価に興味がある．Kenneth C. Smith Early Career Award in Microelectronics，船井研究奨励賞などを受賞．博士（情報科学）．

［ハードウェアセキュリティの最新動向］

②ハードウェアを用いた暗号処理の高速化

坂本純一 横浜国立大学　吉田直樹 横浜国立大学

IoT 時代の暗号技術

インターネット上を流れるデータには盗聴や改ざんの危険があるため，暗号技術を用いたデータ保護が求められる．すべての“モノ”がインターネットに接続される IoT（Internet of Things）時代には膨大な数のユーザがインターネット上で通信を行うため，利用される暗号技術にもそれぞれのユーザのニーズに合わせた“機能”が求められている．何らかの特徴的な機能を持つ暗号は“高機能暗号”と呼ばれ，IoT 時代に表出する課題を解決するものとして期待・開発されている．高機能暗号の 1 つの例として，集約署名を図 -1 に示す．この図は左側の LAN（Local Area Network）内の n 個の機器が送信したディジタル署名をゲートウェイが集約（1 つにまとめる）してから WAN（Wide Area Network）側に送信している．集約することで WAN 上を流れるデータ量が削減できるため通信時間の短縮やネットワーク帯域圧迫を回避することができる．またサーバ側では集約された署名を検証するだけで n 個のディジタル署名を一度に検証できるため，検証にかかる時間や電力を節約できる．

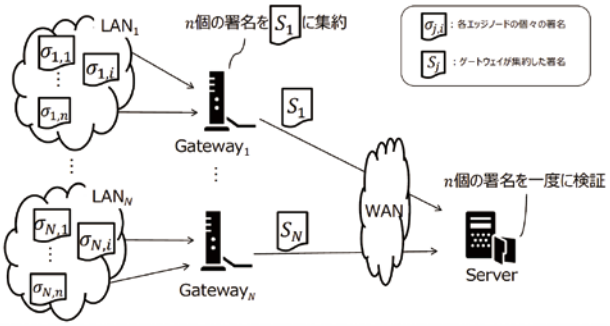


図 -1　高機能暗号の例：集約署名

集約署名のほかにも秘匿検索や代理人再暗号化など高機能暗号の例は枚挙にいとまがない．例に挙げた高機能暗号はペアリング演算と呼ばれる複雑な数学的操作を利用することで効率的に構築できることが知られている．しかしこのペアリング演算自体の計算コストは高く，高機能暗号の実用化に向けてペアリング演算の計算性能向上が必要とされている．

ペアリング演算に求められる性能

ペアリング演算のアプリケーション例として，図 -1 に示した集約署名プロトコルを考える． LAN 側の署名生成や集約は低コスト計算で構成され，サーバ側の署名検証にのみペアリング演算を必要とする集約署名プロトコルが知られている．署名生成・集約は計算リソースの乏しい IoT 機器でも達成可能である一方で，サーバ側の署名検証には潤沢な計算資源を用いた高速なペアリング演算が求められる．ここでいう高速性はレイテンシを指す．サーバは不定期に集約署名を受け取るため一度に大量のデータを処理するというよりも受け取った署名をいかに素早く検証するか―すなわちレイテンシ―が重要である．レイテンシを低減するためにはソフトウェア実装よりもハードウェア実装が有効である．

表 -1 に代表的なハードウェア実装ペアリング演算の計算時間を示す．この表の実装結果は実装対象や費やした回路リソース量が異なるため公平な比較ではないが，上記シナリオを考慮した場合最も適しているものは，計算時間が最も短い文献 1）である．

本稿ではハードウェアを用いたペアリング演算の高速化に焦点を置き，FPGA 実装において最速のレイテンシを達成しているハードウェア構成[1]を特に解説する．

ペアリング演算

暗号に用いられるペアリング演算は入力 P，Q に対する二項演算

$$e:G_1 \times G_2 \to G_3$$
$$e(P,Q) \mapsto R$$

で次の 3 つの性質

1. 非縮退性：任意の P（または Q）に対して $e(P,Q)=1$ なら $Q=0$（または $P=0$）
2. 双線形性：$e(P_1+P_2,Q)=e(P_1,Q)\cdot e(P_2,Q)$
   $e(P,Q_1+Q_2)=e(P,Q_1)\cdot e(P,Q_2)$
3. 計算可能性：多項式時間で計算可能

を満たすものである．G_1，G_2 を素数 p に対する有限体 F_p 上の楕円曲線群とすることで効率的なペアリング演算を構成できることが知られており，ペアリング演算は細かく分解していくと F_p 演算で構成されている．ペアリング演算の効率的な計算アルゴリズムを提案している文献 2）によれば，実用的なセキュリティレベルの（254 ビット素数位数体上で構成される）ペアリング演算には約 1 万回の F_p 乗算，約 5.8 万回の F_p 加算，4 回の F_p 逆元計算が必要とされている．したがってほとんどのペアリングプロセッサは剰余加算器，剰余乗算器，逆元演算器で構成されることが多い．またほとんどの F_p 演算は F_p 上の既約多項式で定義された 2 次拡大体 $F_{p^2}=F_p[i]/(i^2-\beta)$，$\beta=-1$ 演算に利用されるため，F_p 多項式演算の高速化も重要となる．

表 -1　代表的なハードウェア実装ペアリング演算の計算時間

	実装対象	回路リソース	時間
[1]	xcvu9p-2	5421 CLBs, 460 DSPs	61 μs
	xc6vlx240t-1	11672 slices, 500 DSPs	153 μs
[3]	xc6vlx240t-3	5163 slices, 144 DSPs	375 μs
[4]	xc6vlx240t-1	5237 slices, 64 DSPs	409 μs
[5]	65 nm ASIC	323k Gates	554 μs
[6]	65 nm ASIC	3205k Gates	62 μs

低レイテンシペアリングプロセッサの構成

文献 1）で提案されている低レイテンシペアリングプロセッサの概要図を図 -2 に示す．このプロセッサは前置加算器，剰余乗算器，定数倍演算器，後置加算器，逆元演算器の 5 つの演算器で構成されている．シーケンサにはプログラムに相当するものが格納されており，あらかじめ最適にスケジューリングされた計算順序に従って各演算器を駆動する．このように複数の演算器を持ち，それらをペアリング計算のために制御する機構を持つハードウェアのことをペアリングプロセッサと呼ぶ．逆元演算器以外の 4 つの演算器は直列に接続されており，F_p 多項式の演算に特化している．たとえば F_{p^2} の自乗算

$$z_0+z_1 i=(x_0+x_1 i)^2$$
$$=(x_0+x_1)\cdot(x_0-x_1)+2x_0x_1 i$$

を計算する際にはまず x_0+x_1 および x_0-x_1 が前置加算器で計算され，その結果の積が剰余乗算器で計算される．$2x_0x_1$ は剰余乗算器および定数倍演算器で計算される．このような小さな定数による乗算はシフト操作により低コストで実装できるため，剰余乗算器を 2 度利用するよりも効率的である．細かな差異はあるが，ほとんどのペアリングプロセッサがこのように演算器を直列に接続し，多項式演算を高速化する構成をとっている[1), 3)～6)]．

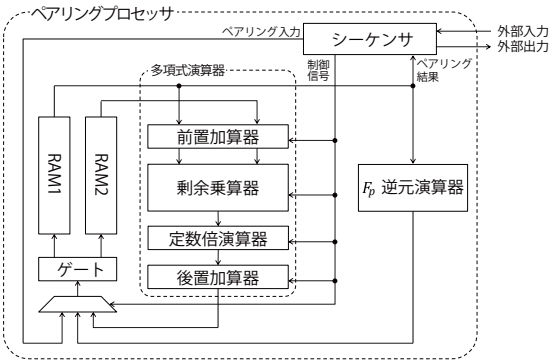


図 -2　ペアリングプロセッサの構成例

逆元演算はペアリング演算中に数回しか現れないため，専用の演算器を持たずにフェルマーの小定理に従い剰余乗算器を使って計算する構成も存在する[4), 5)]．しかしながら逆元演算は非常にコストがかかる計算であるため専用演算器による回路リソースを増やしてでも高速に実行したい．拡張ユークリッド互除法を利用して逆元を計算する専用演算器が一般的である[1), 3), 6)]．

剰余乗算器の高速化

F_p 演算の中でも，剰余乗算は最も計算コストが高くボトルネックとなる部分である．剰余乗算はペアリング演算のほかにも RSA や楕円曲線暗号などの中核を成す計算であり，高速な剰余乗算器は多くのシステムに望まれている．剰余乗算とは $a \times b \bmod N$ のように乗算結果の余りを求める演算である．単純には乗算後に除算（正確には余算）を行うことで計算できるが，除算は非常にコストのかかる演算であるためなるべく排除したい．そのような場合に利用されるのがモンゴメリ乗算に代表される剰余乗算アルゴリズムである．

表 -2 に示すようにモンゴメリ乗算は $a \times b \bmod N$ の代わりに $A \times B \times R^{-1} \bmod N$ を計算する．ここで gcd(·,·) は 2 つの入力の最大公約数を示している．ふつう R は 2 のベキに設定され，2 行目と 3 行目に現れる R による余算および除算はそれぞれビットマスクおよびシフト演算によって効率的に計算可能である．モンゴメリ乗算の入出力は計算したい数に R が乗じられた表現になっているため，最初に R を乗じる処理と最後に R で除する処理のオーバヘッドが生じるが，何度も剰余乗算を行うアプリケーションにおいては相対的にオーバヘッドが小さくなり，高速化に有効な手法である．

文献 3)，6) が表 -2 のモンゴメリ乗算アルゴリズムを採用している．このアルゴリズムは強力だが，ハードウェアに実装しようとすると乗算器の大きさが問題になる．実用的なセキュリティレベルのペアリング演算の場合 F_p の元のサイズが 254bit 程度になるため，表 -2 の 1 行目や 3 行目に現れる乗算には 254bit × 254bit という巨大な乗算器が必要になる．このように大きな乗算器を効率的に実装するのは容易ではないため，乗算幅をより小さな単位に分割したアルゴリズム（表 -3）が提案されている．ここで乗数は $B=\sum_{i=0}^{n-1}(2^k)^i b_i, b_i \in \{0,1,\cdots,2^k-1\}$ というふうに k ビットごとに分割して表現されている．このアルゴリズムはソフトウェア実装では一般的だが，計算依存性[☆1]が高いためにハードウェア実装ではあまり用いられない．図 -3 に k ビット分割モンゴメリ乗算の for ループ 1 段をハードウェア実装し

表 -2　モンゴメリ乗算アルゴリズム

Input:	被乗数 $A=aR \bmod N$, 乗数 $B=bR \bmod N$, 法 N ($N>2$, $\gcd(N,2)=1$), $NN' \bmod R=-1$
Output:	$A \times B \times R^{-1} \bmod N$
1:	$T=A \times B$
2:	$m=TN' \bmod R$
3:	$t=(T+m \times N)/R$
4:	**if** $t > N$ **then**
5:	$t=t-N$
6:	**endif**
7:	**return** t

表 -3　k ビット分割モンゴメリ乗算アルゴリズム

Input:	分割幅 k，分割数 n，被乗数 A，乗数 B, 法 N ($N>2$, $\gcd(N,2)=1$), $NN' \bmod R=-1$
Output:	$A \times B \times R^{-1} \bmod N$
1:	$S_0=0$
2:	**for** $i=0$ **to** $n-1$ **do**
3:	$q_i=(((S_i+b_iA) \bmod 2^k)N') \bmod 2^k$
4:	$S_{i+1}=(S_i+q_iN+b_iA)/2^k$
5:	**endfor**
6:	**return** S_n

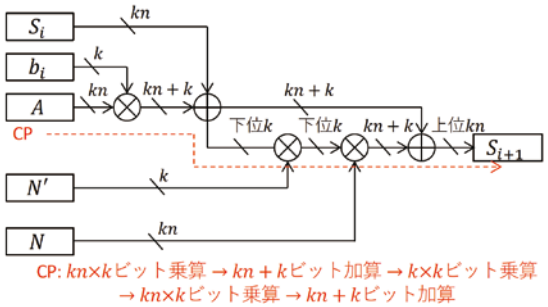


図 -3　k ビット分割モンゴメリ乗算のデータフローとクリティカルパス

☆1　計算依存性：ある計算を始めるために多くのほかの計算結果が必要な場合，計算依存性が高いという．

た際のデータフローを示す．乗算器と加算器が 5 つ直列に並んでおり，並列実行による高速化が見込めないことが分かる．このようなレジスタ間の計算パスのうちハードウェア上で最も長い部分をクリティカルパス（CP）と呼ぶ．長い CP ほど信号の伝達に時間がかかるため，回路を高速に動かすことができなくなる．CP 遅延の削減はハードウェア高速化に必須の要素である．

表 -3 のアルゴリズムの計算依存性を削減し，CP を短くしたものが表 -4 に示す Quotient Pipelining Montgomery Multiplication（QPMM）アルゴリズムである．図 -4 に QPMM の for ループ一段のデータフローを示す．明らかに計算個所が少なくなっており，クリティカルパスはわずか乗算と加算を 1 回ずつ通るのみである（2 つの乗算は依存関係がないため並列に実行できる）．しかしながら演算の幅は図 -3 と比べて増加しており，さらにループ段数も増加している．これは QPMM アルゴリズムが冗長計算を行うことで計算依存性を削減していることに起因する．このような欠点により QPMM は大量のハードウェアを利用してでも高速性が求められるアプリケーションに適しており，文献 1)，5) で提案されているペアリングプロセッサに利用されている．

表 -4　QPMM アルゴリズム

Input:	分割幅 k，遅延定数 d，ブロック数 n，被乗数 A，乗数 B，法 $N(N>2, \gcd(N,2)=1)$, $R=2^{kn}$, $NN' \bmod 2^{k(d+1)}=-1$, $\tilde{N}=(N' \bmod 2^{k(d+1)})N$, $N''=((\tilde{N}-1))/2^{k(d+1)}$
Output:	$S_{n+d+2} \equiv ABR^{-1} \bmod N$

1: $S_0=0, q_{-d}=0, \cdots, q_{-1}=0$
2: **for** $i=0$ **to** $n+d$ **do**
3: $\quad q_i=S_i \bmod 2^k$
4: $\quad S_{i+1}=S_i/2^k+q_{i-d}N''+b_iA$
5: **endfor**
6: $S_{n+d+2}=2^{kd}S_{n+d+1}+\sum_{j=0}^{d-1} q_{n+j+1}2^{kj}$
7: **return** S_{n+d+2}

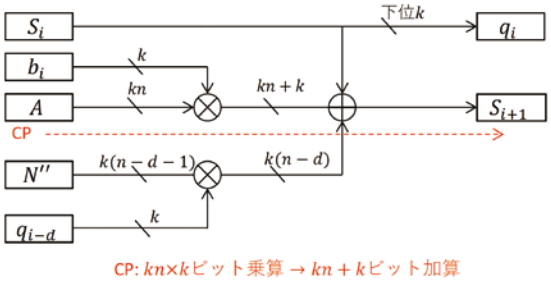


図 -4　QPMM のデータフローとクリティカルパス

今後の展望

本稿ではハードウェアによるペアリング演算の高速化について解説した．IoT 時代の暗号技術である高機能暗号を実現するためにはペアリング演算高速化は不可欠であり，特にサーバサイドアプリケーションでの利用が期待される．また本稿で解説した剰余乗算アルゴリズムは公開鍵暗号全般に利用されるものであるため，今後さらなる高速実装が提案されていくと考えられる．

参考文献

1) Sakamoto, J. et al. : Low-Latency Pairing Processor Architecture Using Fully-Unrolled Quotient Pipelining Montgomery Multiplier, in Proc. of 2019 Asian Hardware Oriented Security and Trust Symposium.
2) Aranha, D. F. et al. : The Realm of the Pairings, in Revised Selected Papers on Selected Areas in Cryptography - SAC 2013.
3) Ghosh, S. et al. : Core Based Architecture to Speed Up Optimal Ate Pairing on FPGA Platform, in Proc. of International Conference on Pairing-Based Cryptography (Pairing 2012) (2012).
4) Yao, G. X. et al. : Faster Pairing Coprocessor Architecture, in Proc. of International Conference on Pairing-Based Cryptography (Pairing 2012), pp.160-176 (2012).
5) Han, J. et al. : A 65 nm Cryptographic Processor for High Speed Pairing Computation, in IEEE Trans. on VLSI, Vol.23, Issue 4, pp.692-701 (2015).
6) Awano, H. et al. : An ASIC Crypto Processor for 254-Bit Prime-Field Pairing Featuring Programmable Arithmetic Core Optimized for Quadratic Extension Field, IEICE Trans. Fundamentals, Vol.E102-A (2019).

（2020 年 1 月 31 日受付）

坂本純一　sakamoto-junichi-ws@ynu.ac.jp
2020 年横浜国立大学大学院環境情報学府博士課程後期修了．博士（情報学）．現同大学院産学官連携研究員．サイドチャネル攻撃やレーザフォールト攻撃，高機能暗号実装の研究に従事．

吉田直樹　yoshida-naoki-jb@ynu.ac.jp
2017 年横浜国立大学大学院環境情報学府博士課程修了．博士（情報学）．2018 年より同大学特任助教．組込みセキュリティの研究に従事．

［ハードウェアセキュリティの最新動向］

③ ハードウェアトロージャンの脅威と検出

基般

林　優一 | 奈良先端科学技術大学院大学／産業技術総合研究所
川村信一 | 産業技術総合研究所

ハードウェアに忍び寄る新たな脅威／ハードウェアトロージャンとは何か？

コスト削減などの理由により，ハードウェアメーカは自社で設計したICチップを安価に製造できるサードパーティのファウンドリを利用している．こうした状況下では，IC製造のサプライチェーンにおいて，チップ設計者が意図しない機能が付加され，特定の状況下ではICの破壊やセキュリティの低下を引き起こす可能性がある．

上述のように設計者の意図に反して付加される回路はハードウェアトロージャン（HT：Hardware Trojan）と呼ばれ，新たなセキュリティの脅威と見なされており，対処の必要なセキュリティ課題の1つとなっている．

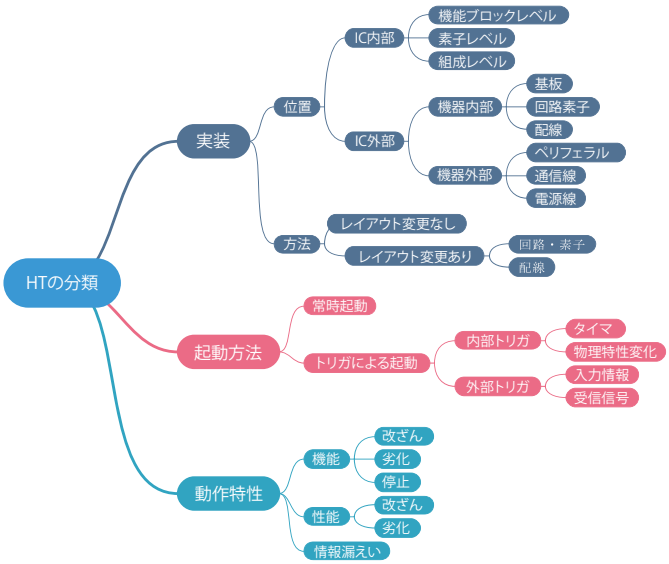


図-1　ハードウェアトロージャンの分類

HTは図-1のように，実装対象，起動方法，動作特性などにより分類され，その組合せは多岐に渡る．本稿ではこうした新たな脅威発見に関する研究動向とHT検知技術について述べる．

HTによる脅威の具体事例と研究動向

HTに関する具体的な脅威事例としては，シリアの核関連と思われる施設の空爆時に用いられたKill SwitchとよばれるHT[1]がある．本例では，シリアのレーダに使用されたICチップに，機能停止を実行できるHTを付加し，軍事作戦を展開する際に遠隔からHTを起動させ，迎撃を阻止したと報じられている．また，民生品では，クラウドサービスを提供する米企業が使用するマザーボードに情報漏えいを引き起こすHTが実装されていた可能性が報じられている[2]．一方，こうした事例において，HTが実際に実装されたと確実に結論付ける報告はなく，また，実装を疑われた側もHTの存在を完全に否定するには至っていない．

今後こうした脅威を抑止するためには，機器設計，製造後のテストでの検出技術や，こうした脅威を疑われた場合に，潔白を証明できる検査技術も求められている．完全な証明ができないまでも，これだけの検証を行ったと説明できることは重要である．

上述した背景の下，HT検出のための研究が近年盛んに行われている．図-2はHTに関する論文の年ごとの出版数とそれらを引用する論文数の推移を表している．2000年を超えたあたりから，論文

数が増加し，2018 年に至るまで増加を続けており，それらの論文を引用する論文も同様の傾向にある．また，図 -2 の論文の国別内訳は図 -3 のようになっており，アメリカ，中国において特に活発に研究が行われている．さらに，出版された論文の助成金は National Science Foundation（NSF）が 114 件，National Natural Science Foundation of China が 66 件，United States Department of Defense が 21 件，Fundamental Research Funds for The Central Universities が 14 件，Semiconductor Research Corporation が 12 件と研究費の面から見てもアメリカと中国におけるサポートが大きく，HT 検出技術や実装困難化技術の開発に力を入れていることが分かる．

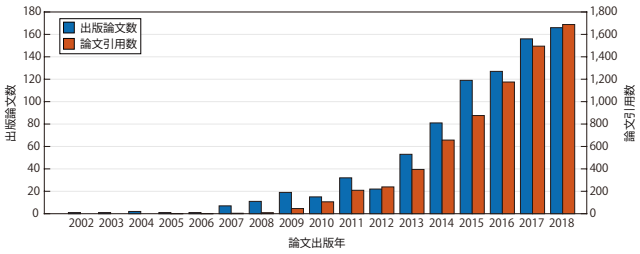


図 -2　HT に関する論文数とその引用件数の推移

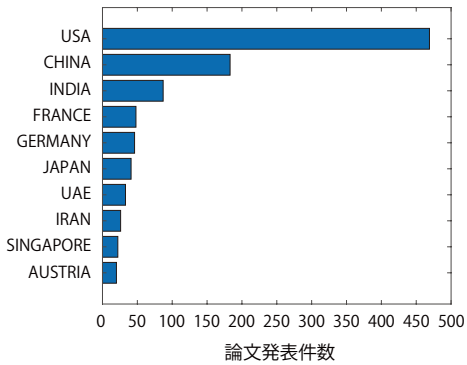


図 -3　HT に関する国別論文出版数（上位 10 カ国）

HT 検出技術の研究動向

図 -2 に挙げた論文のうち，引用件数が多い HT 検出・実装困難化に関連する論文およそ 100 件に着目し，その中で検討されている手法について分類を行った（図 -4）．また，図 -5 は引用数の多い論文をクラスタリングし，クラスタごとの引用関係を示している．

サイドチャネル情報：最も多く提案されている対策手法の 1 つにサイドチャネル情報を用いた HT の検出がある．この手法では HT が実装されていないと仮定されるデバイスの物理特性（消費電力，放射電磁界，実行時間の遅延など）をあらかじめプロファイリングし，これを基準として，HT の実装が疑われるデバイスと比較を行い HT 実装の有無を判断する．

この手法の利点は，対象を非破壊で検査できる点にある．一方，HT が混入していないことが保証されている「ゴールデンサンプル」が必要となり，「これをどこから入手するのか？」という問題が付きまとう．また，製造バラツキによってもサイドチャネル情報は変化する可能性がある．さらに，検出手法の多くは計測量としてサイドチャネル情報を利用することが多く，図 -5 に示す通り，検出および実装困難化技術の多くはサイドチャネル情報のクラスタと接

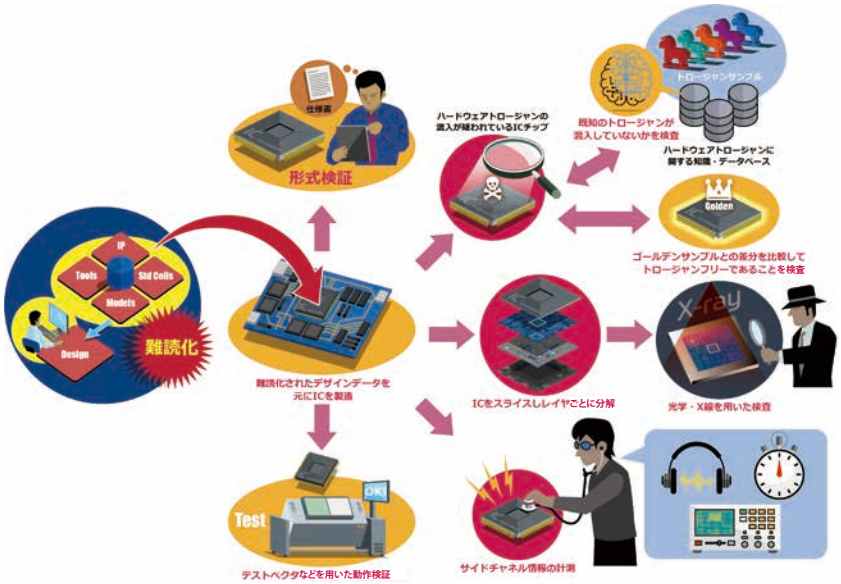


図 -4　ハードウェアトロージャンの検出および挿入困難化手法 [3)]

続されている．

ゲートレベルの特性評価：サイドチャネル情報の次に検討されている検出手法にゲートレベルの特性評価を利用した手法がある．この検出手法ではゲートレベルの物理特性に着目し，それに応じた電力や実行時間遅延などを用いてHTが挿入されたか否かを判断する．しかし，ゲートレベルの物理特性はIC製造過程におけるばらつきの影響を受けることが多いため，HT挿入による特性の変化なのか，製造ばらつきなのかを区別することが難しいため，製造ばらつきを抑える手法に主眼が置かれ検討が進められている．

テストベース：本検出法は，出荷前に通常チップに適用される機能テストのプロセスと同時にHTの検出も行う．たとえば，HTが起動するような入力（テストベクタ）を与えて，その結果起こる異常動作を検出する方法が考えられる．ただし，検出対象となるオブジェクトは不明であり，HTが起動する確率は非常に低いため，効果をあげるには通常の出荷テストとは異なるテストベクタを定義する必要がある．ただし，トロイの木馬を駆動させるテストベクタを必ず定義できるとは限らないため，本手法のみ

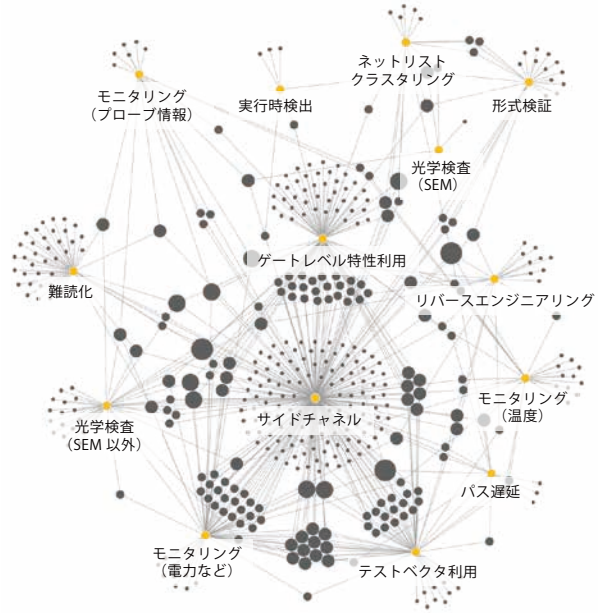


図-5　検出および挿入困難化手法の分類と関係[3)]

での検出は非常に不確実なものとなる．

光学検査：光学検査を用いた方法はIC内部のレイヤ1つずつ除去し，検査対象となるチップを破壊することによって実施される．そのため，光学検査は，リバースエンジニアリング技術に依存した検出手法となっている．光学検査では，走査光学顕微鏡（SOM），走査電子顕微鏡（SEM），およびピコ秒イメージング回路分析（PICA）を使用してレイヤの構造を復元し，収集された画像から最終的なチップのレイアウトを再構築することで，設計者が作成したレイアウトと比較し，HTの実装の有無を判断する．

光学検査は強力な検出手法であるが，コストが高く検出までに多大な時間を要するという問題点がある．

形式検証：ICチップの設計情報にHTが混入していないことを証明するアプローチである．第三者から供給されたICの機能ブロックにHTが含まれないことが証明されれば，チップベンダは安心してこれを使用できる．形式検証の手法を用いて，ICの機能ブロックが与えられた仕様通りに動作し，それ以外の動作をしないことを証明する方法である．たとえば，対象となる機能ブロックに許可されたあらゆる入力パターンに対して，実装物の出力と仕様の出力とが一致することを確認する方法が考えられる．この方法は，回路規模が大きくなると証明に時間がかかるという課題を有する．

電気特性計測：機器の電気計測に基づいてHTを検出手法がある．物理量としては計測しやすいインピーダンスなどに着目し，TDR（Time-Domain Reflectometry）などの手法を用いてHTの有無や実装された位置などを特定する．ただし，本手法もサイドチャネル情報を用いた検出法と同様に多くの場合，ゴールデンサンプルが必要となる．最近では設計データから電磁界シミュレーションにより導出したHTが存在しない電気特性をゴールデンサンプルとして用いる手法も提案されている．また，本手法はIC外部に接続されたHTにも有効である．

ここでは6つの代表的な検出手法についてそれぞ

れの概要を述べたが，こうした手法の高精度化を図るために機械学習を適用する研究も増加している．

本稿では紙面の関係上すべての対策を説明することは困難であるが，各対策などの最新動向については表 -1 に示す論文誌，国際会議で活発に議論されている．そのため，本技術に興味のある読者はこれらで発表された論文を参考にされたい．

現状決定打となる HT 検出・実装困難化の技術なく，複数の技術を組み合わせることが望ましい．前述の 6 つの検知手法のいずれも，それが有効に働くためには，これだけは信頼できるという拠りどころ（信頼の起点）が必要である．たとえば，特定の資格を持った従業員は不正を行わないという仮定や国内の特定の工場で製造された IC には HT は混入しないというような仮定もその一例である．そのため，HT の検出対象となるデバイスにおいて，信頼の起点をどこに置くべきかを考慮した上で，使用する検出技術を適用することが重要である．

HT に立ち向かうには

本稿ではハードウェアトロージャンの脅威，その脅威を抑止するための検出技術について解説した．ハードウェアレベルで実装が行われるハードウェアトロージャンはソフトウェアレベルでの脅威とは異なり，製品出荷後にソフトウェアパッチなどをリリースすることでその脅威を完全に取り除くことは困難である．また，サプライチェーンを利用して機器を製造するメーカ，もしくは，その一部で機器の製造を担うメーカはハードウェアトロージャンの検知，実装困難化についてはもちろん，ハードウェアトロージャンの実装を疑われた場合，その可能性を否定できるような技術を知る（所有する）必要がある．

現在のところ，HT を排除するための決定打は与えられていない状況であるが，HT を検出するために利用できる信頼の起点がどのような部分に設けられるのかを検討し，本稿で解説した検出，実装困難化技術を複合的に応用していくことが現状の解と言えよう．

参考文献

1) Adee, S. : The Hunt for the Kill Switch, IEEE Spectrum (May 2006).
2) Bloomberg Businessweek : The Big Hack : How China Used a Tiny Chip to Infiltrate U.S. Companies (2018), https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
3) 情報セキュリティ工学研究室，http://www.iselab.jp/

(2020 年 2 月 4 日受付)

林　優一（正会員）　yu-ichi@is.naist.jp

2009 年東北大学大学院情報科学研究科博士課程修了，奈良先端科学技術大学院大学・先端科学技術研究科教授．情報セキュリティ，環境電磁工学の研究に従事．IEEE EMC Society 電磁情報漏えいに関する分科委員会委員長．博士（情報科学）．

川村信一（正会員）　shinichi.kawamura@aist.go.jp

1985 年東京大学大学院工学系研究科修士課程修了．2020 年 4 月まで（株）東芝勤務．2018 年より産業技術総合研究所 サイバーフィジカルセキュリティ研究センター　副研究センター長，同ハードウェアセキュリティ研究チーム チーム長兼務．工学博士．

表 -1　HT について活発に議論されている論文誌・学会

	論文誌	会議
1	IEEE Design & Test of Computers	HOST : Hardware-Oriented Security and Trust
2	IEEE Trans. on Very Large Scale Integration Systems	S&P : IEEE Symposium on Security and Privacy
3	IEEE Computer	DATE : Design, Automation, and Test in Europe
4	IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems	ICCAD : International Conference on Computer Aided Design
5	IEEE Trans. on Information Forensics and Security	CHES : Cryptographic Hardware and Embedded Systems
6	IEEE Spectrum	DAC : Design Automation Conference
7	IEEE Transactions on Computers	CCS : Computer and Communications Security
8	IACR Cryptology ePrint Archive	IOLTS : International On-Line Testing Symposium
9	Journal of Electronic Testing	DFT : Defect and Fault Tolerance in VLSI and Nanotechnology Systems
10	ACM Trans. on Design Automation of Electronic Systems	HLDVT : High Level Design Validation and Test

［ハードウェアセキュリティの最新動向］

④ 計測セキュリティ
―サイバー空間と物理空間のつなぎ目における脅威とその対策―

松本　勉 | 産業技術総合研究所　鈴木大輔 | 産業技術総合研究所

計測セキュリティとは

計測セキュリティは，CPS（Cyber Physical Systems）やIoT（Internet of Things）の特徴である，物理空間から収集した情報をサイバー空間で扱う際に発生する脅威へ対抗するための技術である．計測セキュリティについて解説する前に，CPS/IoTのシステム構成について外観について概観してみよう．CPS/IoTの典型的なシステム構成を図-1に示す．構成要素としては，まず物理空間の情報を収集するセンサを搭載した機器がシステムの末端に必ず存在する．次にその機器はゲートウェイを経由してクラウドに接続される．そしてゲートウェイあるいはクラウドでは，収集した情報に対する分析処理を行い，その結果は機器へフィードバックされ，機器が持つアクチュエータの制御に用いられる．このようにCPS/IoTは，センサから情報を収集し，アクチュエータの制御が行われるまでの大きなループをデータが循環するシステムと言える．

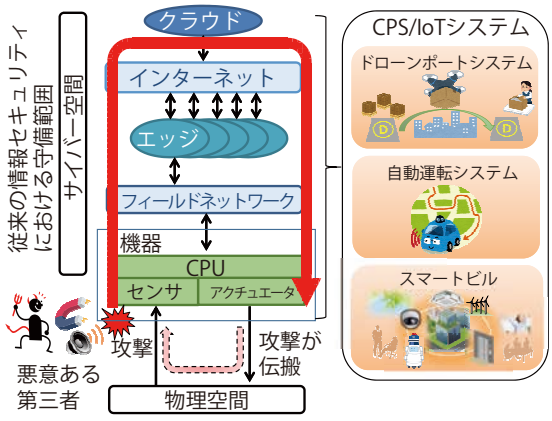


図-1　CPS/IoTのシステム構成と計測セキュリティ

計測セキュリティは，末端のセンサに対して意図的な攻撃を行う悪意ある第三者を仮定し，どのような攻撃が可能か，その攻撃に対してはどのような対策が可能かを，実際にその脅威が現実となる前に先回りして研究している分野である．したがって，攻撃方法としては「そこまでやるのか」と思われる方法が数多く存在するが，それらの攻撃は技術の進歩によって，現実的な攻撃に発展する可能性があることを研究者間では（暗黙的に）共有しており，手段を制限せずさまざまなアプローチで研究が行われている．

具体的なイメージをつかんでもらうために，計測セキュリティが扱う脅威の例をいくつか挙げる．たとえば，自動運転システムにおいて，外界環境をセンシングするための車載センサが攻撃されることによって，事故などの人命にかかわるリスクが発生する可能性がある．あるいは自律運転中のドローンが持つ姿勢センサに対する攻撃は，ドローンの落下事故につながるかもしれない．スマートスピーカのマイクへの攻撃によって，家の外からいつの間にか情報家電が操作されるかもしれない．以上に挙げたような攻撃は，すでに実製品を用いて概念実証が示されたシナリオである．

このように，センサを利活用した新しいシステムの普及に伴い，センサを狙った攻撃に関する脅威が深刻化する恐れがある．本稿では，さまざまなアプローチが示されているセンサへの攻撃を整理し，セキュアなシステム設計にフィードバックする上での課題を探る．

計測セキュリティの研究事例

自動運転や自律型ロボット等の自律システムでは，センサ情報をリアルタイムに処理するのでセンサへの攻撃がシステムに与える影響を注視する必要がある．そこで本章では図-1の一形態として図-2（a）に示すセンサを用いた自律システムのモデルでセンサへの攻撃を整理する．図-2（a）のモデルは，センサ情報を用いた認知・判断と制御機能を担うコントローラと動的な特性を持つシステムから構成される．人が介在するシステムでは人がコントローラへの目標値を入力するが，自律システムではセンサを用いた周辺計測と，その計測値に対する認知・判断の処理で目標値を算出する．また，センサはフィードバック制御を行うためにシステムの状態を計測するためにも用いられる．以下の節では，この自律システムに対するセンサへの攻撃を「攻撃対象のセンサ」，「攻撃に用いる媒体」，「計測値への影響」，の3つの視点から整理する．

攻撃対象のセンサ

図-2（b）の青枠に示されるさまざまなセンサが攻撃対象となっている．攻撃対象のセンサは，大別して能動型と受動型に分類できる．能動型とは，LiDAR（レーザを用いた測距センサ）やレーダなどセンサ自身が出したエネルギーの反射を計測する仕組みを持つセンサを指す．これらのセンサは，図-2（a）で周辺計測に用いられることが多い．受動型は，ジャイロセンサやマイクなど計測対象から発せられるエネルギーを受信するだけの仕組みを持つセンサを指す．これらのセンサは，図-2（a）で状態計測に用いられることが多い．ただし，この分類は必ずしも厳密ではない．たとえば，イメージセンサ（カメラ）は計測の方式によって能動型と受動型が混在する．また，GPSは受信機単体で見れば受動的に見えるが，システム全体としては能動的である．

ここで重要なポイントとしては，次に説明する攻撃に用いる媒体との関係である．センサが計測で用いる媒体は真っ先に攻撃にも利用される可能性がある．たとえば，レーダであれば自身が用いる帯域と同じ電波が，マイクであれば再生可能な周波数帯域の音が攻撃に利用できる．さらに興味深いのは，センサが用いる媒体とは異なる媒体を用いた攻撃事例

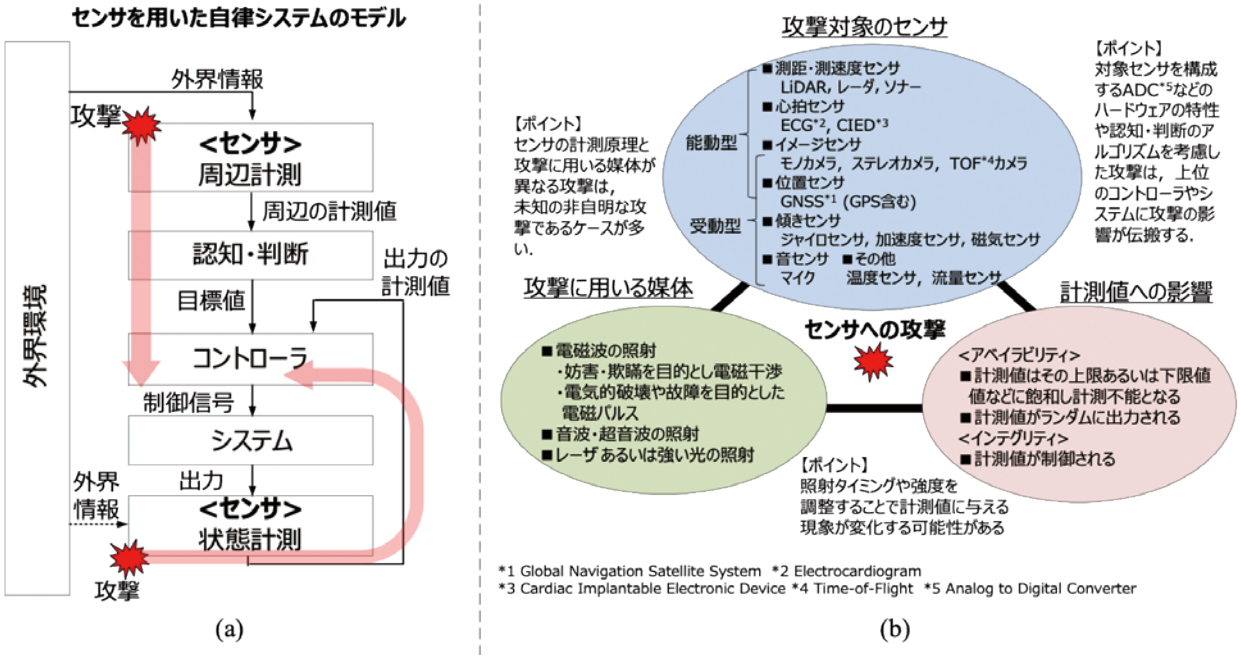


図-2 センサに対する攻撃の全体像

が多数報告されている点である．たとえば，加速度センサに超音波を照射する攻撃や，マイクにレーザを照射する攻撃である．このように，さまざまな視点から攻撃の可能性を探る研究が行われている．

攻撃に用いる媒体

攻撃に用いる代表的な媒体を，図-2（b）の緑枠に示す．電磁波，音波，超音波，レーザあるいは強い光の照射などによる攻撃が知られている．これらは単純な照射にとどまらない．照射が計測値に与える影響を詳しく分析し，照射時に適切な変調を加えることで，最終的には計測値を自由に制御可能な事例が報告されている．また，同時に複数の媒体を用いて高度な制御を行う攻撃が存在する．例として，文献1）ではジャイロセンサや加速度センサに超音波を照射することで計測値を狂わせる攻撃が示されている．これは，MEMSセンサ（微細な機械要素と電子回路を利用したセンサ）のばね・重り構造が共振周波数を持つためである．照射時にセンサ内のアンプやローパスフィルタの特性を考慮して照射する超音波に振幅や位相変調を加えることで，計測値をコントロールできる．

計測値への影響

攻撃が計測値に与える影響は図-2（b）の赤枠に示すように「アベイラビリティ」と「インテグリティ」の2つのケースに大別できる．カメラが強い光によってホワイトアウトする現象などの計測値が上限値あるいは下限値などに飽和するケースや，レーダに対するジャミングのように計測値がでたらめな値を示すケースは，アベイラビリティに影響を及ぼす攻撃である．一方で，前述した変調を加えた超音波の照射のように，計測値を制御できる攻撃は，別の物理現象を計測したように「なりすまし」が可能なことを意味する．すなわちこれはインテグリティに影響を与える攻撃と言える．

脅威としては，インテグリティを脅かす攻撃が深刻である．アベイラビリティの侵害も同じく深刻な脅威であるものの，センサが故障する脅威と同じ影響と考えることができるため，システムの信頼性の観点で織り込み済みであることを期待できる．また，計測できないことはシステムとしては検知しやすいため，対処しやすい．以上から，完全性を脅かす攻撃，たとえばシステムが気が付かないうちにセンサの計測結果が操作されている攻撃が，計測セキュリティで扱う重要な脅威と言える．

前述の通り，この攻撃の影響範囲はセンサだけにとどまらない．図-2（a）において認知・判断のアルゴリズムを考慮してセンサを攻撃することで周辺の計測値を制御し，認知・判断の出力である目標値を攻撃者にとって都合のよい値にすることができれば，センサへの攻撃でコントローラやシステムにまで影響を与えることができる．また，図-2（a）で出力の計測値を制御できれば同様の現象を引き起こすことができる．つまり，自律システムではセンサへの攻撃がシステム全体に波及する可能性があるため，その影響を見極める技術が重要となる．

最近の研究成果では，センサ情報に対して認知・判断のアルゴリズムとしてニューラルネットワークを導入するケースにおいて，ニューラルネットワークの不具合を狙うことで攻撃が可能となる事例が報告されている．文献2）の「敵対的パッチ」と呼ばれる特殊な模様をカメラが撮像すると，図-3のように人の検出が無効化することが知られている．これはセンサ情報に対して計測後にどのような処理が行われるかを考慮した攻撃事例と言える．このほかにも，ノイズ対策のためのカルマンフィルタによるセンサフュージョンを突破可能なセンサ攻撃が示されており[3]，計測の後段にノイズに頑健な処理があっても攻撃の影響がシステムへ貫通することが示唆されている．

図-3　歩行者検知における敵対的パッチの影響

計測セキュリティの保証に向けて

私たちの目指すべき目標は，セキュアなCPS/IoTシステムを構築することである．しかし，目標に至るまでにはまだ多くの課題がある．本稿で挙げる課題の概略を図-4に示す．

課題1：各ドメインでの影響評価

第一に，計測セキュリティは黎明期にあるため，現状では毎年新な攻撃方法が学会等で発表されている．その一方で，それらの攻撃が電力，ビル，FA/PA，自動車など各ドメインのシステムにどの程度の影響を及ぼすのか，判断する手段はほとんど存在していない．論文として公知になる攻撃に関する研究は，固有の実験環境での概念実証であるため，簡単に再現できない．攻撃方法を広く共有し，各ドメインにおけるセンサの用途において攻撃の影響を議論できる枠組みが必要である．このためには攻撃環境の共有や，攻撃方法をシミュレーション可能なモデルとして共有するアプローチが考えられる．

課題2：強化技術と評価技術

第二に，センサへの攻撃がシステムにとって影響を及ぼすのであれば，対抗するためのセキュリティ強化技術が必要となる．また，その有効性を定量化するための評価技術が必要となる．ここで，センサや機器単体でセンサへの攻撃に対抗すべきかは議論の余地がある．攻撃とシステム構成によっては，ゲートウェイやクラウドで効果的な対策が打てるかもしれない．このようにシステムのアーキテクチャの中で，各構成要素がどこまでのセキュリティを担保するのか効果的な対策のアーキテクチャに関する研究が今後必要となる．

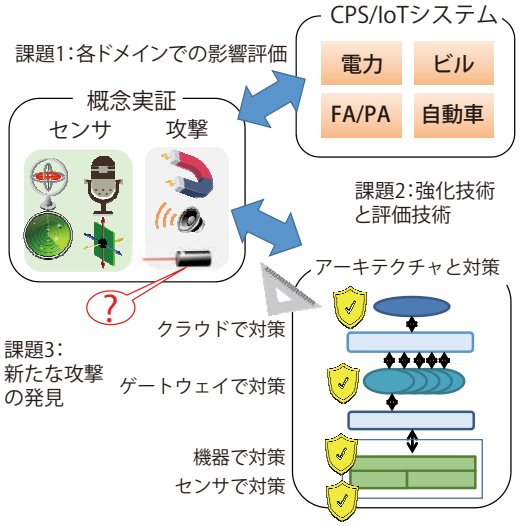


図-4　計測セキュリティの課題

課題3：新たな攻撃の発見

第三に，システムには多種多様なセンサが組み込まれることから，先回りして新たな攻撃，すなわち脆弱性の評価方法を発見することが重要である．予期せぬ攻撃への対策は難しい．計測セキュリティは，センサやアナログ回路から信号処理，システムのアーキクチャなどさまざまな視点で攻撃者の立場で考える必要があるため，「高い攻撃力」を持った人材の育成が必要である．

これらの課題解決を通して，各ドメインでシステムのユーザとベンダの双方が計測セキュリティの視点で要求事項や要求水準が満たされていることを相互に確認できる「セキュリティ保証」の枠組みを確立していく必要がある．

参考文献

1) Trippel, T., Weisse, O., Xu, W., Honeyman, P. and Fu, K. : WALNUT : Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks, IEEE European Symposium on Security and Privacy (EuroS&P) (2017).
2) Thys, S., Ranst, W. and Goedeme, T. : Fooling Automated Surveillance Cameras : Adversarial Patches to Attack Person Detection, arXiv preprint arXiv:1904.08653 (2019).
3) Nashimoto, S., Suzuki, D., Sugawara, T. and Sakiyama, K. : Sensor CON-Fusion : Defeating Kalmanlter in Signal Injection Attack, ACM ASIA Conference on Computer and Communications Security (ASIACCS) (2018).

(2020年2月4日受付)

松本　勉　matsumoto.tsutomu@aist.go.jp

1986年東大大学院工学系研究科博士課程修了，博士（工学）．現在，横浜国大教授および産総研サイバーフィジカルセキュリティ研究センター長．国際暗号学会元理事．電子情報通信学会業績賞，ドコモ・モバイル・サイエンス賞，文部科学大臣表彰・科学技術賞等各受賞．

鈴木大輔　suzuki.daisuke@aist.go.jp

2001年東京理大理工学研究科博士課程前期修了，2011年横浜国立大学大学院環境情報学府博士課程後期修了，博士（工学）．2001年から現在まで三菱電機（株）でセキュリティ技術の研究開発に従事．2019年から産総研客員研究員．

［ハードウェアセキュリティの最新動向］

⑤ Trusted Execution Environment によるシステムの堅牢化

須崎有康 | TRASIO／産業技術総合研究所　　佐々木貴之 | NEC／横浜国立大学

TEE が生まれた背景とコンセプト

過去の OS のセキュリティの歴史を振り返ると，脆弱性の発見とその修正が繰り返されてきた．このため，OS とは独立してクリティカルなプログラムを隔離実行するハードウェア機能 TEE：Trusted Execution Environment（例：Intel SGX, ARM Trust-Zone）が近年の CPU に付加されている．OS とは隔離実行する機能のみならば，今までもインテルアーキテクチャでは SMM（System Management Mode）や ME（Management Engine）があった．しかし，SMM や ME では BIOS のコードや特殊な管理コードに限定されており，第三者が使えるものではなかった．これらに対して TEE は任意のコードが実行できる点が大きく異なる．これにより，課金やコンテンツの DRM（Digital Rights Management）管理など，脆弱な OS からは隔離したいクリティカルな処理を外部のプロバイダが活用できるようになった．この自由度が増したセキュリティ環境を活用するために，研究ばかりでなくビジネスでも注目を集めるようになってきている．

TEE の実装

残念ながら TEE は各 CPU で実装が大きく異なり，セキュリティレベルや適する活用領域が違う．この相違が TEE をバズワード化させており，正しい理解なしに使われて多くの誤解を招いている．以下では，代表的な TEE の実装について解説する．

ARM TrustZone

ARM TrustZone はモバイルデバイス型の TEE を代表する CPU であり，CPU を Secure World と Normal World に分割して通常の OS と Trusted OS を起動する 2 ワールドビューモデルのアーキテクチャである．Normal World には通常のアプリケーションを配置し，Secure World には保護したいアプリケーションを配置することで，Normal World に脆弱性があったとしても，Secure World に配置されたアプリケーションの安全性を保証する．安全性を高めるため，Secure World のソフトウェアは検証が容易なように小さく作られる．

ARM の TrustZone の歴史は古く 2003 年の ARMv6K アーキテクチャから導入されているが，実際に使われるようになったのはスマートフォンで使われている Cortex-A アーキテクチャからである．本稿では Cortex-A を中心に TrustZone を説明する．

図 -1 に TrustZone の概念を示す．TrustZone が提供する基本機能は Secure World と Normal World の提供のみである．World を切り替えるのは SMC（Secure Monitor Call）命令であり，多くの機能はソフトウェアで実現されている．それぞれのワールドでは各 1 つ

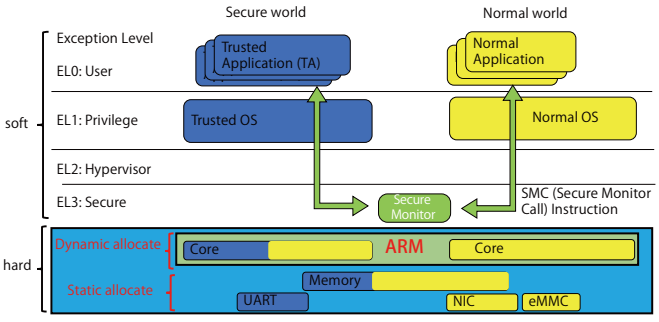


図 -1　ARM TrustZone の概念図（2 ワールドビューモデル）

の OS が実行される．Secure World が使うメモリやペリフェラルは基本的に起動時に設定され，Trusted OS の管理下になる．しかし，割り当てられるメモリは少なく，OS としての機能は限定されたものになる．多くの Trusted OS は TEE インタフェースを規定する団体である GlobalPlatform が定義する TEE Internal API を実装し，暗号やストレージや時間などクリティカルな処理に必要な API のみである．Secure world 内で実行される Trusted OS 上ではこの API を用いて複数の Trusted Application が実行される．

Intel SGX

SGX（Software Guard Execution）は 2015 年にリリースされた Intel Skylake マイクロアーキテクチャから追加されたセキュリティ機能である．SGX は enclave と呼ばれる隔離された実行環境を動的に提供するが，ここでの実行レベルはユーザレベルのみである．OS 相当の機能はハードウェアとして提供される．このため，ARM TrustZone のようは Trusted OS は存在しない．

Intel SDK に従えば，Enclave 内の処理は基本的にプロセス内のライブラリとしてプログラムされ，図 -2 に示すようにシングルアドレスモデルで処理される．Enclave が使うメモリは起動時に確保された最大 128MB の PRM（Processor Reserved Memory）のみを使う．各 Enclave は PRM 内のメモリを切り出した EPC（Enclave Page Cache）が使われる．この Enclave が使うメモリは暗号化されており，攻撃者がメモリに直接アクセスする攻撃（サイドチャネル）への耐性も施されている．

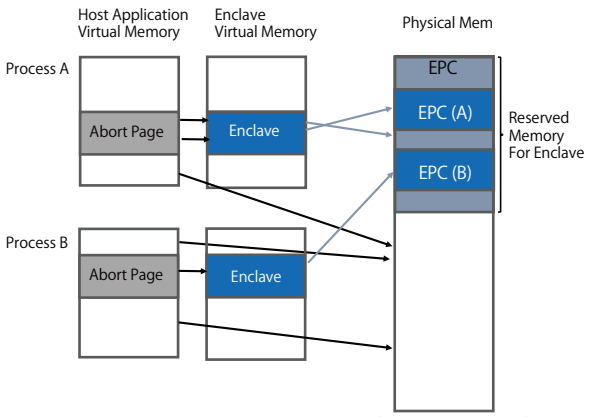


図 -2　SGX でのメモリの使われ方（シングルアドレスモデル）

SGX では実行するバイナリが正規にデバイス上で動作するかを確認する Remote Attestation の機能を提供している．Remote Attestation によりデバイス上の BIOS/UEFI が最新であるか，enclave 内で実行しようとしているバイナリが意図したものであるかを外部から確認することができる．

RISC-V Keystone

RISC-V は命令セットの規格を公開するオープンソース CPU であり，その規格に基づいて各組織や個人が SoC（System-on-a-chip）[☆1] のプラットフォーム仕様や実装まで自ら公開しはじめ，多くの研究のベースに使われているようになっている．本稿では RISC-V で最も開発が活発な TEE である Keystone を取り上げる．

Keystone は ARM と同じ 2 ワールドビューを提供するが，Secure World である Enclave が，各 Trusted Application ごとに動的に作られる．各 Enclave には Trusted OS 相当の Runtime が実行される．このメモリ確保を図 -3 に示す．各 Encalve は RISC-V

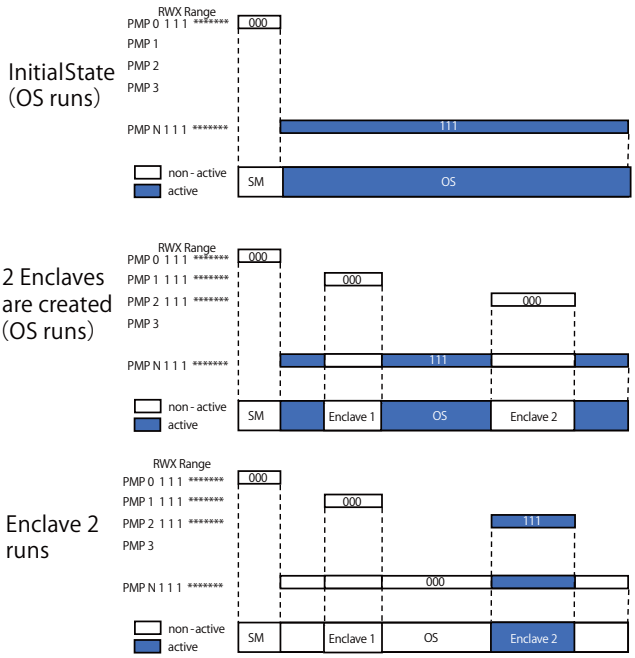


図 -3　RISC-V Keystone でのメモリの使われ方

☆1　CPU や入出力の機能などの周辺機能を 1 つにパッケージしたもの

が提供するメモリ保護機能である PMP（Physical Memory Protection）により，メモリ領域ごとに設定されたアクセス権限情報によって管理される．

図 -3 上段は初期状態であり，ここでは Secure Monitor が PMP の最上位特権，OS（Linux）が最下位特権で割り当てられる．この後，通常のアプリケーションから Trusted Application の生成要求があると Secure Monitor が OS にメモリ開放を依頼し，解放されたメモリに Encalve を割り当てる．図 -3 中段では 2 つ Enclave が割り当てられて OS が走っている状態を表している．図 -3 下段は Encalve2 に制御が移った状態である．この後，Enclave の処理が終れば，メモリを開放・サニタイズして，OS に返却される．

TEE の比較

表 -1 に上記で説明した 3 つの TEE の比較を行った．隔離実行の特徴，仮想化対応，ソフトウェア開発環境，既存の脆弱性などを参照されたい．

TEE のユースケース

本章では，TEE が私たちの生活の中でどのように活用されるか，事例や研究動向を基にその展望について述べる．

セキュリティ機能の保護

TEE の有力なユースケースとしてセキュリティ機能の保護が挙げられる．最近のサイバー攻撃にはセキュリティ機能を無効化した後に実際に被害を与えるような攻撃が観測されている．このような攻撃に対し，TEE を用いてセキュリティ機能を保護することで堅牢なシステムを構築可能である．

保護すべきセキュリティ機能として暗号に用いられる鍵の保護が挙げられる．たとえば TEE が使える Android OS では鍵を管理する keyMaster を TEE 内に実装している．加えて，TEE は，暗号化機能以外のセキュリティ機能を守るためにも用いることができる．たとえば，侵入検知システムを TEE を用いて実装した SGmonitor が挙げられる．

表 -1　TEE 比較表

	ARM TrustZone	Intel SGX	RISC-V Keystone
隔離実行の特徴	1 つの隔離実行環境を起動時に作成．隔離実行環境でのみ使えるデバイスが設定可能．多くの機能をソフトに依存	複数の隔離実行環境を動的に作成．隔離実行環境からデバイスへはアクセスできない．多くの機能をハードで実装．変更不可	複数の隔離実行環境を動的に作成．隔離実行環境にデバイスを割り当てる仕様あり（未実装）．多くの機能をハード・ソフトで変更可能
特権レベル	すべての特権（TEE 内 OS 実装可能．1 つのみ）	ユーザ（ring 3）のみ（TEE 内 OS の実装不可）	すべての特権（TEE 内 OS 実装可能．Enclave ごとに毎回作成）
命令	1 命令（ワールド切替え）（SMC 命令）	18 命令（環境設定など）（特権 13, ユーザ 5）	1 命令（ワールド切替え）（ecall 命令）
メモリモデル メモリ確保 メモリ暗号化	2 ワールドビューモデル 起動時時に固定．ワールド間で利用可能 なし（オプションでは追加可能）	シングルアドレスモデル 起動時時に固定（Intel SGXv1 で最大 128MB） あり（起動時に乱数初期化）	2 ワールドビューモデル 動的で可変．ワールド間で利用可能 なし（研究ロードマップにあり）
Secure Boot	オプション対応あり	対応可能	現状ではない
サイドチャネル耐性	オプション対応あり	あり	現状ではない
信頼の基点（Root of Trust）	基本的になし．携帯は GlobalPlatform の Secure Element の利用例あり	Intel が提供した CPU 固有のもの．変更不可	研究段階
Remote Attestation	基本的にない	Intel が提供したものが使える．隔離実行のみも多い	ある．しかし，現状では信頼の基点がハードウェアではない
仮想化対応	試験的に対応．KVM（TZVisor），Xen	Xen, KVM の VM およびコンテナから利用可．VMware は不可	仮想化自体が試験中
ソフトウェア開発環境	OP-TEE，QSEE，KNOX，Kinibi，Trusty	Intel SDK，SCONE，Asylo，OpenEnclave	Keystone SDK
既知の脆弱性	Boomerang[NDSS18], API/ABI 脆弱性 [CCS19]	Prime+Probe[DIMVA17], ForeShadow[USENIX Sec18], API/ABI 脆弱性 [CCS19]	BOOM（Out-of-Order）Speculative Attacks[CARRV19], API/ABI 脆弱性 [CCS19]

これにより，侵入検知システムへの攻撃や侵入検知システムが扱う情報を保護することができる．

ライセンス管理やペイメント機構の保護

有料のコンテンツをユーザに配信する際には，コンテンツにアクセスする権利のあるユーザのみがコンテンツを利用できるように制御する必要がある．この際，デバイスの持ち主が悪意のあるユーザであったとしても，権限のないコンテンツの閲覧や不正な再配付が行われないように，コンテンツが保護されなければならない．この問題は，TEE の中にライセンス管理機能を配置し，悪意のあるユーザからライセンス管理機構を保護することによって解決することができる．

また，近年は，スマートフォンを用いたペイメントが普及している．安全なペイメントを実現するためには，マルウェアなどによるペイメントの情報の漏洩や，ペイメントのソフトウェアへの攻撃を防ぐ必要がある．TEE によって，スマートフォンのペイメントの機構を保護することが検討されている．

プライバシ情報の保護

TEE の中に格納されている情報は TEE の外から見えないという機密性から，プライバシ情報の保護に用いるユースケースが検討されている．たとえば近年は顔や指紋がスマートフォンの認証に用いられており，生体情報がスマートフォンに保存されている．認証機能や生体情報を TEE の中に配置することで生体データを守ることが可能になる．

クラウドの保護

クラウド環境では，利用者はクラウド事業者のリソースを借りて，それを利用する．もし，クラウド事業者が 100% 信用できなければどうなるだろうか．クラウド事業者が利用者のデータを盗み見たり，改ざんしたりするかもしれない．TEE を用いることで，この懸念を払しょくすることができる．具体的には，Intel SGX のデバイスの持ち主であっても，TEE で保護された領域にアクセスできないという特徴を利用して，クラウドの利用者のみが TEE で保護されたデータにアクセスできるようにすることができる．Microsoft Azure や IBM のクラウドが，TEE に対応した仮想マシンの払い出しに対応している．

AI の保護

近年の AI に用いられる機械学習は，学習データや学習プロセス，学習の結果を攻撃者に改ざんされてしまうと，誤った判断を引き起こし，AI が用いられているシステムが正常に動作しなくなる恐れがある．そのため，AI の保護に TEE を活用する研究が進められている．具体的には，機械学習の基盤である TensorFlow を Intel SGX によって保護する TensorSCONE や，分散処理基盤である MapReduce を SGX によって保護する研究が進められている．

今後の展望

TEE は，情報化社会の安全性を担保するための重要な技術であり，使いやすい実装や活用法の研究開発が活発に進められている．インターネットのプロトコルを定義する IETF においても TEE を活用する TEEP（Trusted Execution Environment Provisioning）などの策定が進んでおり，社会に浸透していく技術である．

（2020 年 4 月 3 日受付）

謝辞　本成果の一部は，国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務「セキュアオープンアーキテクチャ基盤技術とその AI エッジ応用研究開発」の結果得られたものです．

須崎有康（正会員）　k.suzaki@aist.go.jp
1990 年東京農工大大学院中退．その後，電子技術総合研究所を経て，国立研究開発法人産業技術総合研究所／セキュアオープンアーキテクチャ・エッジ基盤技術研究組合．情報理工学博士（東大，2009 年）．本会シニア会員．

佐々木貴之（正会員）　tsasaki@nec.com
2004 年東北大・工卒業．2006 年東大・理・物理学専攻修士課程修了．同年日本電気（株）入社．以来，クラウドセキュリティや，ネットワークセキュリティ，IoT セキュリティの研究開発に従事．現在，同社セキュリティ研究所主任研究員．

［ハードウェアセキュリティの最新動向］

⑥ 自動車サイバーセキュリティの基本 ―車載ネットワークと攻撃例―

基般

Camille Gay | 産業技術総合研究所

自動車におけるセキュリティの懸念

2015 年に FCA 社の Jeep Cherokee に 3G ネットワーク経由で勝手に遠隔操作される可能性のある脆弱性がセキュリティリサーチャーにより発表され，約 140 万台の車両がリコールされた．その事件が広くメディアに報道され，自動車のセキュリティ対策の必要性が初めて世間に知られた．しかし，自動車セキュリティは決して新しい研究分野ではない．自動車にまつわる犯罪は昔から多く存在している．車上荒らし，自動車盗難，自動車部品の偽造，不正改造，メータ改ざんの詐欺等といった迷惑行為が毎日世界中に発生している．また，盗難車は別の犯罪を実行するために使われることが多いので，車の所有者の問題だけではなく，深刻な社会問題でもある．

最近，自動運転のアルゴリズムや運転支援システムの開発が進み，車の ECU（Electronic Control Unit，電子制御機器）が制御できる範囲が広がっている．たとえばステアリングやブレーキ等の致命的な装置が高機能のコンピュータに制御されるようになった．それらのコンピュータが仮に攻撃者に乗っ取られれば，重大な事故を起こせる可能性がある．言い換えると，ECU の脆弱性のインパクトが劇的に上がったといえる．一方，車を Bluetooth，Wi-Fi，インターネット等に接続する“コネクテッドカー”の通信機能が普及してきた．加えて，車と車を接続する“V2V”（Vehicle to Vehicle）の通信機能や，車とインフラを接続する“V2X”（Vehicle to X）の通信機能も実証実験の段階にまで進んでいる．車は電子機器のない機械的な乗り物から，スマートフォンに劣らない接続性を持つ複雑な電子ネットワークに変化した．それらの機能を実現するためには，多くのハードウェア技術やソフトウェア技術が必要である．図 -1 に示す通り，車に脆弱性が潜在する可能性のあるコンポーネントが多くなり，車に脆弱性が存在する確率も劇的に上がった．

自動運転とコネクテッドカーの時代に備え，自動車メーカもビジネスモデルを変えている．自動車を製造するだけでなく，モビリティのディジタルサービスを提供する会社に変化している．そのため，車は乗客の個人情報を多く発生させる・取り扱う乗り物になりつつある．従来の自動車法規に加え，個人情報保護規制に対応する必要が生じた．近年，「ハッカーに遠隔されないか」や「自分の個人情報が車から流出するのではないか」等と，世間から深刻に心配されるようになり，自動車メーカのセキュリティ対策が注目を浴びている．

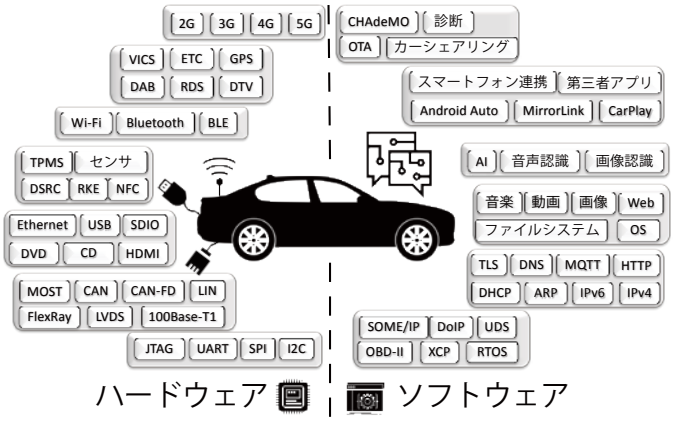


図 -1　車が攻撃を受ける可能性のある機能の例

自動車業界特有の課題

セキュアな車を開発するには，自動車業界は多くの課題を解決する必要がある．まず，自動車業界は複雑なエコシステムでできている．車載ネットワークは多くの ECU で構成されているが，ECU を設計しているのはティア 1 の企業（自動車メーカに直接納入する一次サプライヤ）である．また，それらの ECU に使われるハードウェアやソフトウェアを開発しているのはティア 2 の企業（ティア 1 の企業へ自社製品を供給する二次サプライヤ）である．自動車メーカ・ティア 1・ティア 2 はお互い完全に情報を共有していないため，自動車のセキュリティ対策を管理することは簡単ではない．

ハードウェアセキュリティの分野では，極端な温度での対策は難しいと言われている．一般的に使われている IC カード（クレジットカード等，きわめて薄い半導体集積回路がプラスチックに埋め込まれた認証用のカード）の使用温度範囲は−25 ～ 85℃であるのに対し，車に使われる部品（いわゆる車載グレード部品）の使用温度範囲は最大で−40 ～ 150℃である．IC カード等は極端な温度では動作停止が許されるが，車は極端な温度であっても動作停止・誤動作すれば，乗客の命を危険にさらしてしまう．また，車には非常に高い信頼性が求められている．IC カードの読み取りエラーは，誰でも経験したことはあるだろう．しかし，車のエラーは事故につながる可能性があるため，IC カードと同じ失敗率は許されない．

IC カード等は，故障した場合は交換すれば済む．しかし，車は原因不明の事故に遭った場合，ECU に不具合があったことが疑われる．その不具合の原因を究明するため，不具合解析ができる環境を保障する必要がある．一方，攻撃者に製品が解析されないよう，開発用の機能を無効化したり，ソフトウェアを難読化したりすることがよく用いられるセキュリティ対策（リバースエンジニアリング対策）である．しかし，不具合解析をしやすい環境では，製品を解析しにくくするリバースエンジニアリングの対策は実装しにくい．

広い使用温度範囲で高い信頼性を保障できる対策は高額になる傾向があり，低コストでの量産が求められるある車での採用は一般に難しい．一方，セキュリティレベルが低すぎると，脆弱性が悪用され，リコールや集団訴訟につながるリスクもある．うまくバランスをとることが自動車業界の会社には求められている．

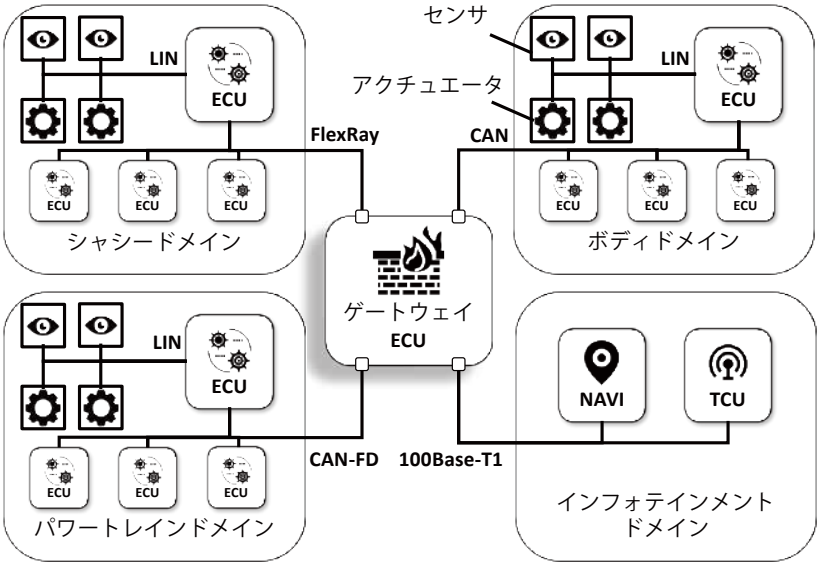


図 -2　車載ネットワークの例

車載ネットワークの概要

現代の車の車載ネットワークの代表例を図 -2 に示す．車は多くの ECU で構成されている．それぞれの ECU に役割が与えられている．たとえば，ブレーキはブレーキ ECU により制御されている．役割を果たすためには，センサとアクチュエータが必要である．ケーブル線の本数を最小限に抑えるため，センサとアクチュエータを同一の LIN バス（Local Interconnect Network）に接続することが多い．また，ECU と ECU の

間の情報交換も多く行われている．たとえば，ブレーキペダルの状態を，ストップランプを制御する ECU に知らせる必要がある．ECU 間の通信のために設計された通信手段には，CAN（Controller Area Network），CAN-FD（CAN with Flexible Data-rate）と FlexRay がある．また，高速通信の車載用通信手段では，MOST（Media Oriented Systems Transport）と 100Base-T1（Automotive Ethernet）が現在の主な選択肢である．

ECU の数が多ければ多いほど，通信量が上がり信頼性が下がるため，ECU をドメイン（サブネットワーク）で分ける考え方が最も浸透している．図 -2 では，よく使用されるドメイン分けを示している．シャシードメインは車の曲がる・止まる機能を実現している．パワートレインドメインはエンジンやトランスミッションの機能を実現している．ボディドメインはドア，窓，エアコンや照明の機能を実現している．インフォテインメントドメインは通信量の多い NAVI とテレマティクス機能を実現している．なお，ドメインをまたぐ ECU 間の通信も必要である．上記のブレーキペダルとストップランプの例では，シャシードメインとボディドメインをまたぐ必要がある．そのため，それぞれのドメインを接続するセントラルゲートウェイが使われている．ゲートウェイはドメインをまたぐメッセージを厳格にフィルタリングするべきではあるが，実際の車両では必ずしもそのように実装されているとは限らない．

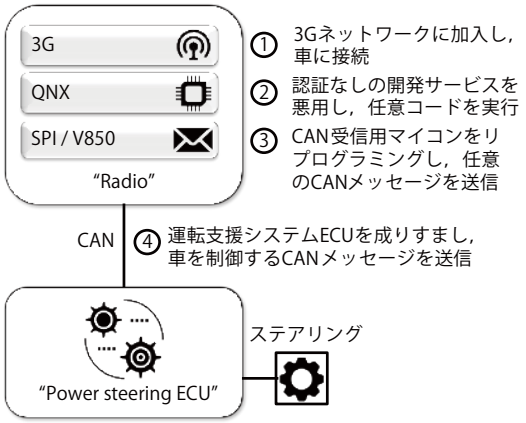


図 -3　Jeep Cherokee 攻撃の概要

実際にあった脆弱性の報告の例

2015 年 Jeep Cherokee（3G からの攻撃例）

2015 年に報告された Jeep の脆弱性 [1] をここで簡単に説明する．攻撃の流れを図 -3 で示す．

①車との遠隔通信手段を確保

Jeep Cherokee の NAVI が接続していた 3G ネットワークには，通信ポートの制限や，クライアントとクライアントの間の通信の制限がなかった．結果として，同じ 3G ネットワークに加入していた研究者は遠距離でも車に接続できた．

② NAVI に任意のコードを実行

NAVI にファイアウォールが設定されず，認証なしの開発用のサービスが稼働していたため，NAVI に任意のコードを実行できた．

③ CAN 通信モジュールに任意のコードを実行

NAVI には CAN バス受信専用のマイコンが搭載されていた．本来，任意のメッセージを送信する機能はなかったが，そのマイコンに認証なしのリプログラミング機能があったことを悪用し，任意のメッセージを送信できるファームウェアで研究者がリプログラミングできた．

④ステアリング ECU 等にメッセージを送信

車にゲートウェイ ECU がなく，NAVI とステアリング ECU は同一の CAN バスに接続されていた．また，CAN バスのメッセージの認証がなかったため，“曲がれ”の命令を送れば，車が曲がった．

2017 年 Tesla Model S　（Wi-Fi からの攻撃例）

2017 年に報告された Tesla Model S の近距離遠隔操作の脆弱性 [2] をここで簡単に説明する．攻撃の流れを図 -4 で示す．

①車との無線通信手段を確保

NAVI に Wi-Fi 機能があり，ディーラーの Wi-Fi ネットワークに自動的に接続する仕様になっていた．しかし，共通のパスワード“abcd123456”での弱い認証しかなかった．成りすましの Wi-Fi ネットワークを立ち上げ，車から接続してもらうことで，通信手段を確保できた．

② NAVI に任意のコードを実行

Wi-Fi 接続後，NAVI が自動的に Web ページをロードしていたが，JavaScript の実行エンジンにソフトウェア脆弱性があり，NAVI で任意のコードを実行できた．また，Linux の公知脆弱性を悪用することで権限上昇し，車載ネットワーク内のイーサネットに任意のメッセージを送受信できた．

③ゲートウェイ ECU に任意のコードを実行

イーサネット接続先のゲートウェイ ECU に，弱い認証の診断機能があり，ゲートウェイ ECU で任意のコマンドが実行できた．

④ ECU 等にメッセージを送信

制御 ECU には共通パスワードを平文で送る弱い認証しかなかったため，制御 ECU のリプログラミングができた．

脆弱性対策と正しい考え方

上記の攻撃の流れをどう防止できるかをここで考える．まず，自動車のセキュリティ対策は，自動車の車両以外でも考える必要がある．ネットワークの通信制限があれば Jeep の攻撃はそもそも成立しなかった．また，セキュリティ対策は，用途に合わせて選ぶ必要がある．前述の Tesla の場合，Wi-Fi の PSK 認証（共通パスワード認証）を採用していたが，MGT 認証（会社向けの認証）を採用していれば Wi-Fi での攻撃は成立しなかった．特に，車を含む IoT 機器は，**全デバイスに共通するパスワード・共通鍵に基づく対策は原則採用しない**方が望ましい．また，車の寿命は 10 年と一般的に言われているが，暗号アルゴリズムにも寿命がある．車がビンテージカーになったときのセキュリティ対策の有効性も考える必要がある．

なお，ここで紹介した攻撃がどれもいろいろなリプログラミング機能を悪用していたとはいえ，リプログラミング機能そのものはセキュリティ対策としても非常に重要である．Jeep の車には遠隔リプログラミング機能（通称 OTA ― Over the Air）がなく，リコールせざるを得ない状態に陥った．一方，Tesla の車には OTA 機能があり，リコールせずに対応ができた．素早い対応が称賛され，顧客からの信頼度も上がった．コネクテッドカーには，**強い認証性を備えた OTA 機能が必要不可欠である**．そして，その **OTA 機能を活用する脆弱性報告対応チームの育成**も重要である．ハッカーの技術は日々進化している．インターネットで車の情報だけでなく，解析用のソフトウェアや，車と通信をするための安価なハードウェアも共有している．自動車業界は秘密主義だから解析されないだろと思うのは禁物である．どんな対策も突破されるかもしれないと思い，**同じ目的の複数の対策を実装するという**考え方が重要である．

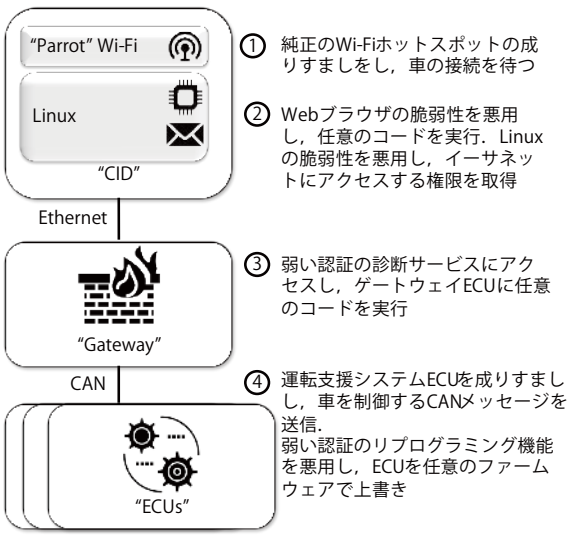


図 -4　2017 年　Tesla Model S 攻撃の概要

参考文献

1) Miller, C. and Valasek, C. : Remote Exploitation of an Unaltered Passenger Vehicle, Black Hat USA (2015).
2) Nie, S., Liu, L. and Du, Y.: Free-Fall : Hacking Tesla from Wireless to CAN Bus, Black Hat USA (2017).

(2020 年 2 月 4 日受付)

Camille Gay　camille.gay@aist.go.jp

産業技術総合研究所サイバーフィジカルセキュリティ研究センター CPSEC 客員研究員．トヨタ自動車（株）コネクティッド先行開発部セキュリティグループ シニア・リサーチャー．

小特集

差分プライバシ

編集にあたって

袖美樹子 | 国際高等専門学校

新型コロナウイルスが猛威を振い，世界保健機関（WHO）の Tedros Adhanom Ghebreyesus 事務局長は 2020 年 3 月 11 日，「新型コロナウイルスはパンデミック（世界的流行）とみなせる」と表明を出した．このような非常事態において，我々に必要な情報とは何か？　どのように提供されるべきか？ それに答える取り組みがいくつかなされた．たとえば東京都は，新型コロナウイルス感染症対策サイトを作成し情報発信を行っている．検査実施人数や軽症・中等症，重症の人数が開示されている．この情報の作成方法には工夫がなされ，データを入れ替えることによりほかの県でもサイト作成が可能となっており，神奈川県でも活用されている．これらのデータは「オープンデータ」として広く一般に提供されている．

我々はディジタル社会に生きており，多様なサービスから豊かな生活を得ている．続々と収集される，ビックデータを用い，さらに高度で便利な新サービスが検討され，提供され続けている．しかし．ビックデータには多くの個人情報が含まれている点は無視できない．危険だから使わないと言えればよいが，現在の社会を考えた場合，その利便性を捨てることは不可能である．それではどうすればよいのか？ この答えとなるものが「プライバシ保護」である．計算機能力の連続的向上もあり，今までは安心と思われていた対策手段でも，プライバシを保護することは難しくなってきていることを加味し，新しい技術が必要とされている．

本小特集ではこの問題を解く鍵とされている，「差分プライバシ」に関して，3 件紹介をいただく．

第 1 の記事は，古川諒氏による**「データプライバシ保護技術と差分プライバシ」**である．パーソナル

データの活用と保護を両立するための技術として研究されてきたプライバシ保護技術について，3つの技術カテゴリ①入力プライバシ保護技術，②出力プライバシ保護技術，③秘密計算技術に分類し解説をいただく．また，差分プライバシの概念，他指標との比較によって，差分プライバシが広く活用可能な安全性指標であることを論じていただく．

第2の記事は，寺田雅之氏による**「差分プライバシの基礎と動向」**である．米国国勢調査局による2020年の国勢調査での差分プライバシ導入の背景を紹介いただき，差分プライバシの定義とその意味するところを解説いただく．加えて差分プライバシを普及させていく上での現状の課題と今後の展望について解説していただく．

第3の記事は，福地一斗氏，佐久間淳氏による**「局所差分プライバシの最新動向」**である．Google, Appleなどの企業でユーザプライバシ保護を行う技術として，局所差分プライバシは実際に運用されサービスに導入されている．本稿では局所差分プライバシの定義とその意味するところを解説いただく．さらに活用の例を挙げ，実世界のサービスで局所差分プライバシがどのように運用されているかを紹介いただく．

安全で安心を担保しつつ，その利便性と豊かさを享受できるディジタル社会にするためには，プライバシ保護はなくてはならない技術である．今までは，その場しのぎのプライバシ保護であったが，差分プライバシの登場によって，統一的に安全性を評価する指標を手に入れることができた．加えて利用目的に合致したプライバシ保護を行うことが可能となった意義は大きく，差分プライバシとビックデータ活用による新たなサービスの提供が期待できる．

(2020年3月20日受付)

［差分プライバシ］

1 データプライバシ保護技術と差分プライバシ

古川　諒 | NEC

パーソナルデータ活用とデータプライバシ保護技術

近年 ICT の進化，特にスマートデバイス・IoT（Internet of Things）機器の普及に伴い，個人にかかわる情報（パーソナルデータ）は，氏名や年齢，住所，ゲノムといった個人に固有の情報のみならず，購買履歴や動画や Web サイトの閲覧履歴，位置情報などの個人の行動を表す履歴情報や，顔画像・動画などのリッチメディアなど多岐に渡り，さまざまな事業者や組織によって収集されるようになってきた．深層学習の進化に端を発するビッグデータ活用の機運の高まりはこれらのパーソナルデータの活用に対してもおよび，社会的・産業的に有用な知見を得ることが期待されている．

典型的なパーソナルデータ活用といえば企業・組織が自分たちで収集したデータのみを用いて，サービス向上や顧客ごとにカスタマイズされたサービス（パーソナライズドサービス）を提供するものである．このような活用方法はパーソナルデータおよびその分析結果が収集した主体の中にとどまるため，有効な同意に基づいてパーソナルデータを収集できていればプライバシ侵害につながることは少ない．

一方で，国政調査のようにパーソナルデータから算出した統計値を公開したり，近年では MLaaS (Machine Learning as a Service) のように機械学習モデルを第三者が使えるように公開したり，第三者に分析してもらうためにデータを提供したりといった活用方法もある．このような活用方法では悪意ある第三者によって，提供された情報から元のパーソナルデータの一部が漏洩し，個人に不利益をもたらす危険性がある．たとえば，2009 年に Netflix がレコメンデーションアルゴリズム開発コンテストのためにユーザの映画評価情報を公開したところ，ほかのレビューサイトで公開されていた情報との突合により個人が特定され，個人が隠していた映画視聴履歴が漏洩してしまい，訴訟に発展するといった事件が発生している．

データプライバシ保護技術はこのようなパーソナルデータの活用と保護を両立するための技術として研究されてきた．これらの技術ではパーソナルデータそのものを加工したり，分析結果を加工したりすることで，機微な情報と個人との紐づけを防止しながら活用することを目的としている．

本稿ではこれらのデータプライバシ保護技術についての概観を解説し，本小特集で焦点を当てる差分プライバシの位置づけについて述べる．

データプライバシ保護技術の概観

データプライバシ保護技術の分類の 1 つに「入力プライバシ保護技術」「出力プライバシ保護技術」「秘密計算技術」の 3 つの技術カテゴリに分ける方法がある．本稿ではこの分類をベースに解説を行う．

それぞれの技術カテゴリは以下のように説明できる．

- 入力プライバシ保護技術：分析処理に入力するパーソナルデータを加工することで分析者によるプライバシ侵害のリスクを低減する技術

- 出力プライバシ保護技術：パーソナルデータに対する分析結果からのプライバシ侵害のリスクを低減する技術
- 秘密計算技術：暗号やそれに類する技術により，データ分析者に対してパーソナルデータを秘匿しながら分析を行う技術

図 -1 はデータ保有者が保有するパーソナルデータをデータ収集者が収集し，統計処理や機械学習などの分析処理の実行者であるデータ分析者が収集されたデータを分析し，分析結果を最終的に利用する過程において，各技術カテゴリの関係を示したものである．ここで，データ収集者とデータ分析者が同一であったり，違う人物であったりする場合☆1 もあるし，同様に，データ分析者と分析結果利用者が同一であったり，違う人物であったりする場合☆2 があることに注意されたい．

図中で同じ色の矢印は一連のデータフローを表しており，図中には 4 つの考えられるデータフローを示している．これらのデータフローのうち，フロー①，③はデータ収集者，データ分析者，分析結果利用者がすべて異なる人物でもプライバシ保護が可能なデータフローである．一方でフロー②はデータ収集者とデータ分析者の間でプライバシ保護がされないため，両者が同一の人物であることが求められ，フロー④はデータ分析者に対してパーソナルデータは秘匿されるが分析結果は加工されていないため，分析結果利用者がデータ収集者であることが求められる．

以降の節でそれぞれの技術カテゴリにおいて利用される技法について簡単に述べる．

入力プライバシ保護技術

図 -1 に示したように入力プライバシ保護技術はデータ保有者（個人）またはデータ収集者によって実行される．基本的には入力された個票データを加工し，第三者に公開できる個票データを出力する技術である（図 -2）．

入力プライバシ保護技術に使用される加工技法の代表例を表 -1 に示す．入力プライバシ保護技術はこれらの加工技法を組み合わせて個票データを加工し，公開した個票データから個人と機微な情報を紐づけられてしまうリスクを低減する技術と言える．

出力プライバシ保護技術

出力プライバシ保護技術はデータ分析者が分析処

☆1 この場合，データ収集者とデータ分析者の間にはたとえばデータを売買するような関係がある．

☆2 この場合，データ分析者と分析結果利用者の間にはたとえば分析結果を売買するような関係がある．

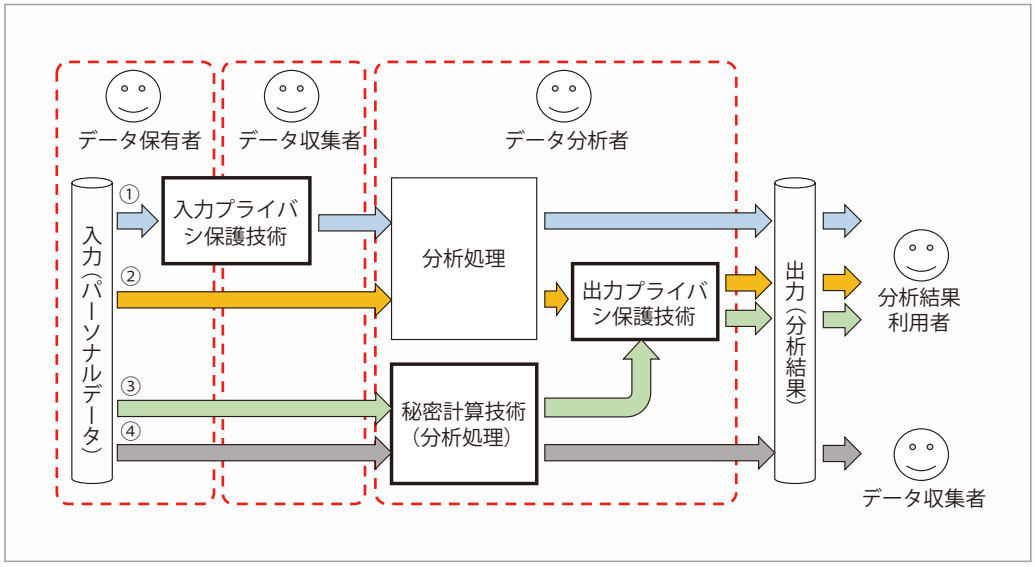


図 -1　プライバシ保護技術カテゴリの関係性

理を行い，分析結果利用者に対して出力する際に実行され，個票データを分析した結果を何らかの形で制御することでプライバシを保護する．

出力プライバシ保護技術では図 -3 のように主に分析結果に乱数的なノイズを付加する技法が用いられる．また，分析結果利用者が知りたい統計情報を指定するようなモデルの場合，複数の統計出力によりプライバシが漏洩しないかを検査し，出力を抑制するクエリ監査と呼ばれる技法もある．

秘密計算技術

秘密計算技術では暗号技術などによりデータを秘匿したまま分析処理を実行する．秘密計算技術は大きく分類して秘密分散を用いた方法，準同型暗号を用いた方法，ハードウェアを用いた方法があり，それぞれ速度や安全性，計算に参加するパーティ数などが異なる．

秘密計算技術は他の 2 つとは異なり，出力される処理結果は元データに対する処理結果と一致する．このため分析結果からのプライバシ侵害を防ぐためには別途出力プライバシ保護技術などと組み合わせる必要がある．

ID	年齢	性別	郵便番号
1	25	男	111-1111
2	30	女	222-2222
3	32	男	333-3333
4	61	女	444-4444

年齢	性別	郵便番号
25-30	男	111-11**
25-30	女	222-2***
32	*	333-****
60以上	*	44*-****

図 -2　入力プライバシ保護技術による加工の例

表 -1　入力プライバシ保護技術の加工技法 [1)]

加工技法	加工内容
削除	列，行，セルなどの単位で属性値を削除する
仮名化	識別子を削除または置き換える
一般化	値を上位の概念や範囲に置き換える
曖昧化	特に大きい，または小さい数値をまとめる（〇〇以上など）
ミクロアグリゲーション	複数のレコードの値をその集合の代表値に置き換える
ノイズ付加	値に乱数的なノイズを加える
データ交換	レコード間で値の（確率的な）入れ替えを行う
疑似データ生成	元データと統計的性質が類似するように人工データを生成する

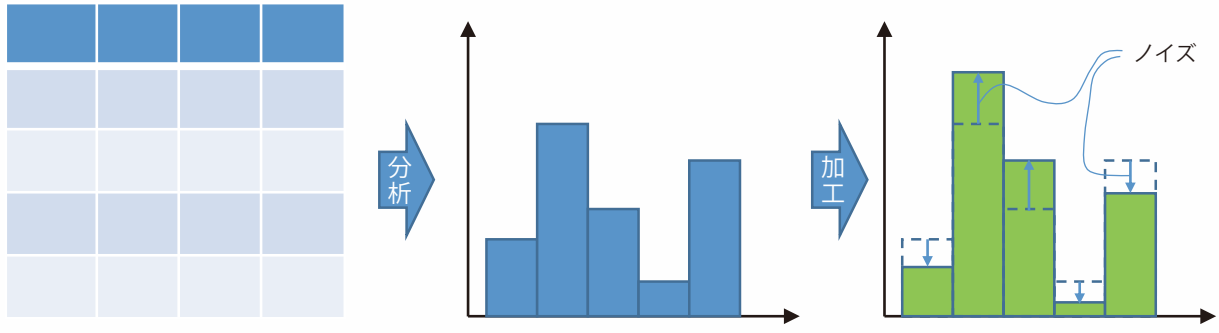


図 -3　出力プライバシ保護技術の加工の例

差分プライバシの位置づけ

差分プライバシの概念

前述のとおりノイズ付加やデータ交換などの乱数を用いた技法（攪乱的技法と呼ぶ）は入力プライバシ保護技術においても出力プライバシ保護技術においても用いられている．しかしながら，「どのようなノイズであればどの程度安全なのか」明確な基準がないことは長らく問題であった．

Dwork によって提案された“差分プライバシ”[2]は，攪乱的技法に対する安全性を数学的に定義した指標である．詳細な定義は後の記事に譲るが，端的に言えば「（ノイズが付加された）出力が 2 つの近しいパーソナルデータ集合の間で区別ができないのであれば安全である」ということを定義した指標である．つまり，差分プライバシを満たせば，2 つの近しいデータ集合の（任意の）差分が出力に影響を与えないようにノイズが加わることになるため，出力から確定的に差分の内容を特定できなくなり，プライバシを保護できるのである（図 -4）．このような定義により，特に攻撃者の前提知識や攻撃方法を仮定せずに，任意の分析方法☆3 に対して安全性を議論できることが注目を浴びている．

差分プライバシは入力プライバシ保護，出力プライバシ保護どちらの指標としても利用されている．つまり，適用対象の処理として統計値や機械学習などにノイズを付加する場合には出力プライバシ保護に，ノイズを付加した疑似データを出力する場合には入力プライバシ保護に使用されることになる．また，近年ではデータ保有者（個人）からパーソナルデータを収集する際に保有者側でノイズを付加するプライバシ保護が注目を集めており，このようなケースでも差分プライバシを利用できる．このケースでは差分プライバシの派生である“局所差分プライバシ”が提案されており，多くの研究がされている．

☆3 実際には差分プライバシを満たすように分析方法を改変する必要があり，改変が困難な場合もある．

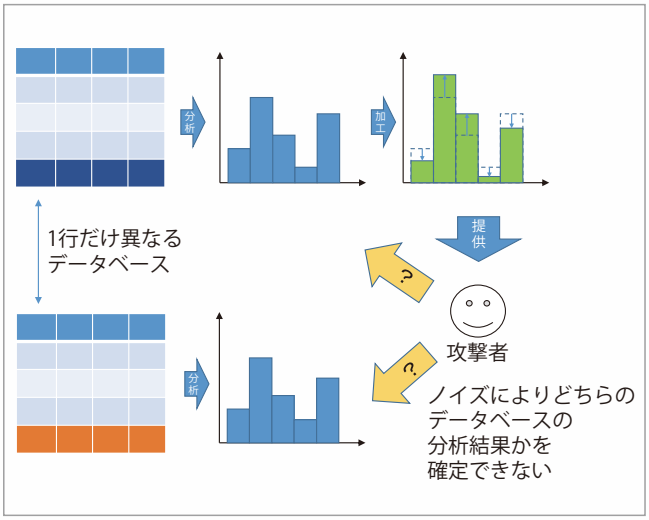


図 -4　差分プライバシのイメージ

差分プライバシと他指標の比較

ここで，入力プライバシ保護技術においてよく用いられる k- 匿名性[3]と比較をしてみよう．k- 匿名性とは，加工された個票データにおいて個人の識別に使用できる属性（たとえば年齢，性別，郵便番号などであり，これらを総称して準識別子と呼ばれる）の組合せが少なくとも k 人以上同じである場合 k- 匿名性を満たすという指標である．

表 -2 はそれぞれの指標に対して対応する技術カテゴや指標が対象としている加工技法，指標を利用できるプライバシ保護の実行者や攻撃者の仮定をまとめている．差分プライバシに対しては適用対象とする処理の観点で，前節で述べた「統計分析・機械学習等」「疑似データ生成等」「個人からのデータ収集」と 3 つに分けてその特性を詳細に示している．「個人からのデータ収集」のケースは前述した局所差分プライバシが適用されるケースにあたる．

表 -2 から分かるように，k- 匿名性がデータ収集者の実行する非攪乱的な加工に対してのみ適用できるのとは異なり，差分プライバシはデータ分析者，データ収集者，データ保有者が実行する攪乱的な加工に対して適用できることが分かる．また，k- 匿名性は攻撃者が前述した準識別子を知っており，出

力された個票データに含まれる準識別子との一致を見ることで個人を特定するような攻撃に対する安全性を定義しているが，差分プライバシは攻撃者がどのような知識を持っているか，どのような攻撃を実行するかによらず一元的に安全性を議論できる．

このように，差分プライバシはデータプライバシ保護技術の中で，広範な攪乱的技法に適用可能な安全性指標であると位置づけられる．以上の整理が以降の記事の理解を助けるものであれば幸いである．

参考文献

1) 内閣官房：技術検討ワーキンググループ報告書（第5回），https://www.kantei.go.jp/ jp/singi/it2/pd/dai5/siryou2-1.pdf
2) Dwork, C. : Differential Privacy, Proc. 33rd Intl. Conf. Automata, Languages and Programming - Volume PartII, LNCS, Vol.4052, pp.1-12 (2006).
3) Sweeney, L. : k-anonymity : A Model for Protecting Privacy, International Journal on Uncertainty, Fuzzi-ness and Knowledge-based Systems,10(5), pp. 557-570 (2002).

（2020年2月26日受付）

■古川　諒（正会員）　rfurukawa@nec.com

2008年東京工業大学総合理工学研究科博士前期課程修了．同年NEC入社．以来，アクセス制御，プライバシ保護，ブロックチェーンの研究に従事．

表-2　*k*-匿名性と差分プライバシの比較

指標	*k*-匿名性	差分プライバシ		
		統計分析・機械学習等	疑似データ生成等	個人からのデータ収集（局所差分プライバシ）
技術カテゴリ	入力プライバシ	出力プライバシ	入力プライバシ	入力プライバシ
対象とする加工技法	一般化・削除・曖昧化などの非攪乱的技法	ノイズ付加，データ交換などの攪乱的技法		
保護の実行者	データ収集者	データ分析者	データ収集者	データ保有者
攻撃者の知識	準識別子	仮定しない		
対処できる攻撃	個人の特定	仮定しない		

［差分プライバシ］

2 差分プライバシの基礎と動向

寺田雅之 | NTT ドコモ先進技術研究所

「その場しのぎのプライバシ保護」からの決別

差分プライバシ (differential privacy) は，日本ではまだあまり実用例を聞くことは多くないが，米国では Google や Apple などの IT 企業が採用を進めるのみならず，公的機関が大規模に活用する段階まで実用化が進んできている．

2019 年 10 月に米国の国勢調査局[☆1]が“A History of Census Privacy Protections”と題されたパンフレット[☆2]（図 -1）を公開した．これは米国での国勢調査におけるプライバシ保護の歴史をすごろくのような形で年表化したものだが，その 2010 年のところに「その場しのぎのプライバシ保護 (ad-hoc privacy protections) を使う最後の国勢調査」との記載がある．

米国では国勢調査は 10 年に一度実施されるので，次は 2020 年――つまり今年である．2010 年を最後に「その場しのぎのプライバシ保護」から決別し，次はどうするか．

このパンフレットによれば「2020 年の国勢調査データは差分プライバシにより守られるだろう (2020 Census data products will be protected using differential privacy)」と高らかに宣言されている（図 -2）．

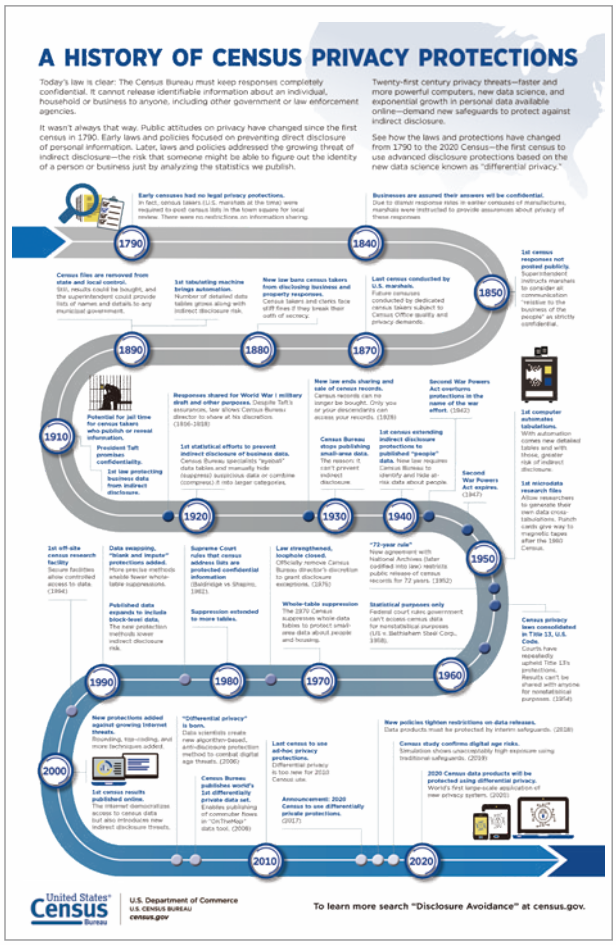


図 -1　米国国勢調査のプライバシ保護の歴史

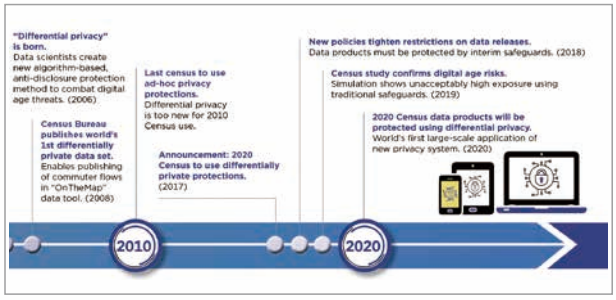


図 -2　2010 年以降を拡大

☆1 US Bureau of Census.「センサス局」と訳されることも多いが，本稿では同局の公式日本語サイトの表記にならい「国勢調査局」と記載する．

☆2 https://www.census.gov/library/visualizations/2019/comm/history-privacy-protection.html

なぜ差分プライバシか

米国国勢調査局は，なぜいままで自らが実施してきたプライバシ保護手段に対して「その場しのぎ(ad-hoc)」という言い方をしてまで差分プライバシを導入しようとしているのだろうか．その背景として，データの増加や計算機能力の向上によって（いままで現実的なリスクとして想定していなかった）プライバシ暴露への懸念が現実的になったこと，特にデータベース再構築(database reconstruction)と呼ばれる攻撃に対する脆弱性を無視できなくなってきたことが挙げられる[1]．

データベース再構築攻撃

データベース再構築攻撃とは，簡単に言えば，

- 複数の（それぞれ安全に見える）データを重ね合わせ，
- そこから導出される制約充足問題を解決する

ことによって，それらのデータに含まれる個人の情報を特定する攻撃である（図-3）．

この攻撃の強力なところは，一見して安全に見えるデータであっても，実際に攻撃を適用してみるとドミノ倒しのように多数の個人に関する情報が特定され得る（場合によってはすべての情報が特定されてしまう）ことにある．また，重ね合わせるデータの組合せが変われば導出される制約充足問題も変わるため，仮にある特定のデータの組合せがデータベース再構築に対して安全だったとしても，別のデータとの重ね合わせに対しても安全とは限らない．

この攻撃は計算量が大きい（NP困難とされる）制約充足の解決を必要とし，いままでは単なる理論的な可能性であるとして深刻に捉えられてこなかった．しかし，今日の計算機環境やSATソルバーなどの進化に伴い，米国国勢調査局のJ. M. Abowd氏はこの攻撃が「理論上のリスクから対策が求められる課題に変化した」☆3と表明している．

想定外といたちごっこ

これは，既知の攻撃やリスクに対しては安全なデータであっても「想定外」の新しい攻撃に対しては安全と言えないことを示している．

また，新しい攻撃が見つかって何らかの対策を施したとしても，次の「想定外」が見つかればさらに対策が必要となる．このような「いたちごっこ」をいつまでも繰り返しても安全を確信することはできない．また，攻撃への対策は何らかのデータの改変を伴うため，対策を重ねるたびにデータの有用性もどんどん低下することになる．

このいたちごっこから脱却するためには，（未知の攻撃も含めた）任意の攻撃に対して安全性を保証するようなプライバシ保護の枠組みが必要となる．

☆3 https://science.sciencemag.org/content/363/6423/114/tab-e-letters

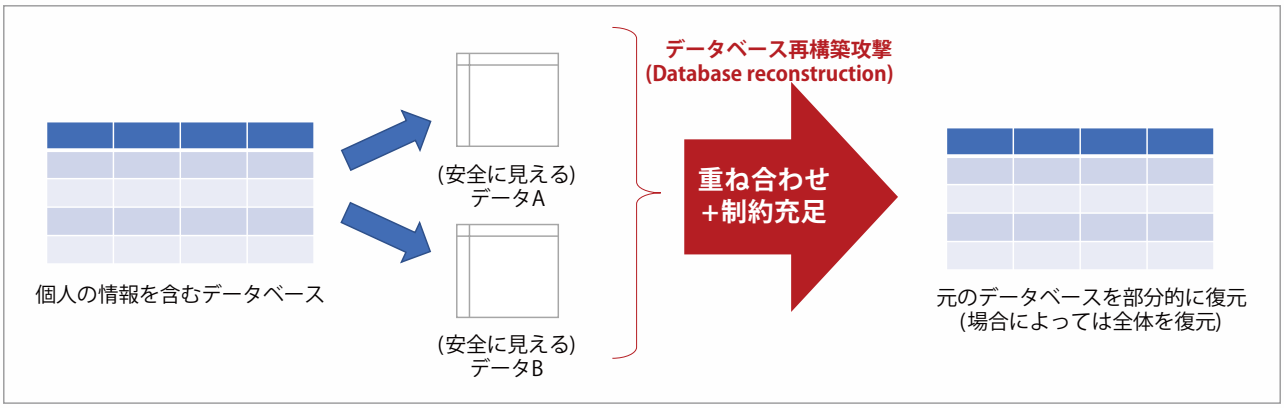


図-3　データベース再構築攻撃

差分プライバシの定義

差分プライバシは，この任意の攻撃に対する汎用的な（“ad-omnia”な）安全性を実現するためのプライバシ保護の枠組みであり，さまざまなプライバシ保護手段に対して統一的な安全性指標を与える．しばしば誤解されるが，差分プライバシ自体は**特定のプライバシ保護手段を表すものではない．**

差分プライバシを満たすプライバシ保護手段は「メカニズム」と呼ばれる．その代表例としてLaplace（ラプラス）メカニズムと呼ばれる手法がよく使われるが，Laplace メカニズムはあくまで差分プライバシを実現する手段の１つであって差分プライバシそのものではない．たとえばPRAM (post randomization) や幾何メカニズム (geometric mechanism) など，ほかにも差分プライバシを満たすメカニズムは数多く存在する．

差分プライバシは，これらのさまざまなプライバシ保護手段，すなわちメカニズムに対して統一的な安全性指標を提供する．この安全性指標は“ϵ”で表現され，以下の定義により与えられる．

定義 1. 任意の隣接したデータベース D_1 および D_2 ($D_1, D_2 \in \mathcal{D}$) に対し，ランダム化関数 (*randomized function*) $Q' : \mathcal{D} \to \mathcal{R}$ が下式を満たすとき，Q' は ϵ - 差分プライバシ（ϵ -*differential privacy*, 以下 ϵ -*DP* と略記する）を満たす．ただし，ここで S は Q' の出力空間 $\mathcal{R}$ の任意の部分空間である ($S \subseteq \mathcal{R}$).

$$\Pr[Q'(D_1) \in S] \leq e^{\epsilon} \cdot \Pr[Q'(D_2) \in S]. \qquad (1)$$

初めて見る人にとっては，そっとページを閉じたくなるような謎の定義だと思うが，後で直感的な説明を試みるので少しだけ我慢してほしい．

この定義において，ランダム化関数 Q' がそれぞれのメカニズムに相当する．ランダム化関数とは，計算結果に乱数ノイズを付与するなど，出力がなんらかのランダム性を持つ関数を表す[☆4]．

あるメカニズムが ϵ -DP を満たすとき，ϵ (≥ 0) の値が小さいほど安全性が高いとされる．$\epsilon = 0$ のときそのメカニズムは完全な安全性を持ち（ただし出力されたデータからは何の情報も得られない），$\epsilon = \infty$ ならば何の安全性も保証されない[☆5]．

差分プライバシの意味

さて，この差分プライバシの定義は何を意味するだろうか．一見しただけではそもそもプライバシ保護と何の関係があるかすら分かりにくい．そこで，以下に（なるべく）直感的な説明を試みる．

データベースとメカニズム

説明に先立って「データベース」と「メカニズム」を中心に用語を説明する．

データベースとは１つ以上のレコードから構成されるデータであり，それぞれのレコードは各個人に対応するものとする[☆6]．このデータベース (D とする）を加工し，なんらかの有益な情報を取り出すことを考える．

D から情報を取り出すための加工処理を問合せ (query) と呼び，Q と表記する．これには D から有益な情報を取り出すためのあらゆる処理が考えられる．たとえば平均や分散などの統計量の取得や，仮名化データの作成，クロス集計表やデータキューブなどの集計データの作成，D を学習データとした機械学習のモデル生成など，さまざまなデータ活用におけるデータの収集・加工プロセスは，すべて「問

☆4 つまり，差分プライバシを満たすメカニズムは原則として攪乱的 (perturbative) であると言える．

☆5 たとえば，一般に k- 匿名性を実現するためのアルゴリズムは差分プライバシを実現しない（$\epsilon = \infty$ となる）．これは，k- 匿名性はリンケージ攻撃以外（たとえばデータベース再構築攻撃）に対して安全性を保証しないことを反映している．

☆6 データベースが単一のレコードのみからなる（ある個人のデータしか含まない）とき，ここでの差分プライバシを特に局所（local）差分プライバシと呼ぶこともある．

合せ」として一般化して考えることができる．

ここで，問合せの出力 $Q(D)$ はデータ活用に有益な情報だけでなく，D に含まれる個々のレコードに関する情報をなんらかの形で含み得る．つまり，$Q(D)$ から個人のプライバシが暴露され得ることに注意が必要となる．

そこで，問合せによるプライバシの暴露を防ぎつつ有益な情報を得るために，$Q(D)$ をそのまま出力するのではなく，$Q(D)$ と似ているがプライバシ保護のための措置が施された $Q'(D)$ を出力することを考える．たとえば Q の出力の一部を確率的に変化させたり，Q の出力にノイズを加えたりして Q' を構成する．

この問合せ Q をプライバシ保護のために書き換えた Q' がメカニズムである（図 -4）．データ活用の観点からは，Q' の出力が持つ統計的性質が元の Q のそれをなるべく保持する☆7 ことが求められるが，あまり Q の出力と Q' の出力が似すぎているとプライバシが保護できない．つまりメカニズム Q' には有用性と安全性のトレードオフの関係が存在する．有用性については必要な統計的性質が定まれば定量的に評価できるが，Q' はどのような性質を持っていれば安全と言えるだろうか．

差分プライバシの定義が意味すること

メカニズム Q' の安全性について，定義 1 は「ϵ が十分に小さいとき，攻撃者はいかなる個人のプライバシも Q' の出力から確信を持って得ることはできない」ことを保証する．なぜこのようなことが言えるかについて，出題者と回答者の 2 人の間でのゲームを用いて考える．

このゲームにおいて，出題者は互いに隣接したデータベースである D_1 と D_2 を持ち，そのどちらかにメカニズム Q' を適用して出力 s を得る（どちらに適用したかは回答者に内緒である）．回答者は出題者から提示された s を見て，それが D_1 と D_2 のどちらから導出されたかを当てようとする（図 -5）．

ここで，データベースが互いに隣接するとは「1 つのレコードだけが違って，ほかのレコードはすべて同じ」ことを意味する．ここでは，たとえばデータベース D_1 に含まれているある 1 人（A さんとする）に関するレコードが D_2 では削除されており，その他のレコードは同一であるとする☆8．

また，Q' は問合せ Q を書き換えたものである．ここでは Q を「データベース中に含まれる，ある条件を満たすレコードの数」を数える問合せ（計数問合せ）とし，Q' はその出力に整数ノイズを加えてランダム化したものとする．

Q' はランダム化により確率的にふるまうため，$Q'(D_1)$ と $Q'(D_2)$ はいずれも確率変数となる．式 (1)

☆7 どのような統計的性質を保持すると有用であるかは応用による．

☆8 なお，隣接の定義として，このほかに「A さんのレコードだけが別の人のレコードにすげかえられている」とする場合もある．本来，どちらの定義を使うべきかはメカニズムによって使い分ける必要があるが，ここでの例（単一の計数問合せ）ではどちらの定義を使っても違いはない．

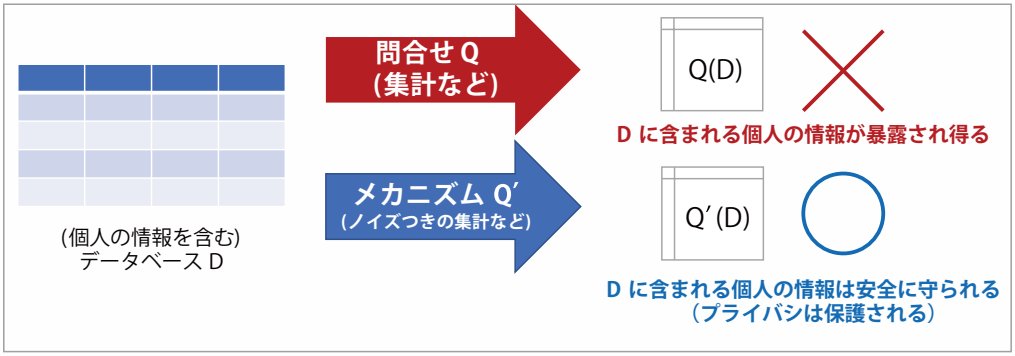


図 -4　問合せ Q とメカニズム Q′ の関係

は，$Q'(D_1)$ と $Q'(D_2)$ の分布が「ほとんど同じ」であること，すなわち任意の s に対して $\Pr[Q'(D_1)=s]$ と $\Pr[Q'(D_2)=s]$ の比が最大でも $e^{\epsilon}:1$ を超えないことを求める．このような性質を満たすノイズとしては，両側幾何分布に従う乱数や，Laplace 分布に従う乱数を（小数点以下を丸めて）離散化したものなどが挙げられる☆9．

このとき，ϵ が十分に小さければ，$Q'(D_1)=s$ となる確率と $Q'(D_2)=s$ の確率がほとんど同じになるので，回答者は s が D_1 と D_2 のどちらから導出されたのかを見分けようがない．ここで，（そもそも A さんの情報を含まない D_2 より得られた）$Q'(D_2)$ から A さんのプライバシが暴露されることはあり得ないため，それと見分けがつかない $Q'(D_1)$ から A さんのプライバシが暴露されることもない．したがって，A さんのプライバシは任意の攻撃から守られる．

より正確には，$\epsilon=0$ でない限り，上記の 2 つの確率の違いから，出力 s を得た回答者はそれが D_1 と D_2 のどちらに由来するかを推測することはできる．しかし，片方の確率が 0 となることはない☆10 ため，回答者はこれを確信することはできず，その推測結果にかならず過誤が発生し得る☆11．つまり出題者は回答者の推測に対して「それは決めつけだ」と否認する余地がある（否認可能性 (plausible deniability) が与えられる）．

D_1 と D_2 は（$\mathcal{D}$ 上の）「任意の」隣接したデータベースであるため，これはデータベースの中身がどのようなものであっても成立し，A さんではなく他のレコードに対応する人，つまり B さんでも C さんでも任意の人に関して同様に成立する．

すなわち，Q' が ϵ-DP を満たすとき，Q' は（$\mathcal{D}$ 上の）任意のデータベースに含まれるすべての人に関して上記の安全性を提供する．

差分プライバシの特徴

差分プライバシは，ϵ-DP を満たすメカニズムに対して，その実現方式にかかわらず，ϵ の値に応じた安全性を共通的に保証する．これは，異なるプライバシ保護方式の間で安全性を比較するための共通の物差しを与え，安全性を揃えた上で有用性を比較することを可能にする．また，合成定理 (com-

☆9 前者は幾何メカニズム，後者は Laplace メカニズム（に対して整数丸めという事後処理をしたもの）に相当する．

☆10 もしどちらかの確率が 0 になることを許すと式 (1) が成立しなくなる．「任意の隣接するデータベース」という条件から D_1 と D_2 を入れ替えても成立が求められることに注意．

☆11 どの程度「確信できない」かは，たとえば検定における検出力の上限（検出力が有意水準の e^{ϵ} 倍を超えることはない）として与えられる．

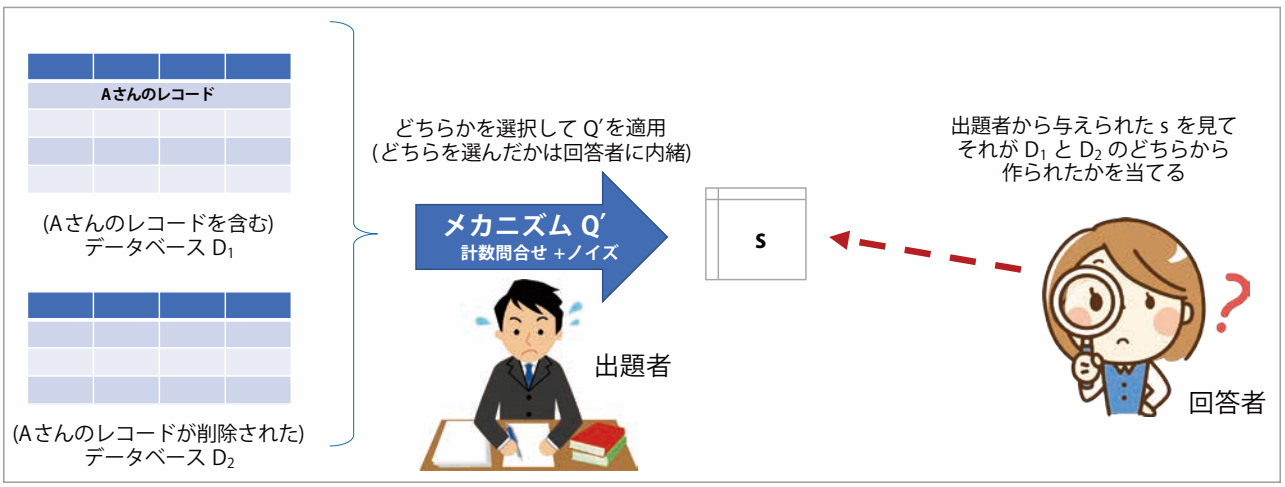


図 -5　ゲームの概要

position theorem)[☆12] と呼ばれる強力な定理により，差分プライバシを満たす新しいプライバシ保護方式を，既存の方式から組み合わせて構築できることを可能にする．

異なる方式間の安全性の比較

データベースからなんらかの情報を安全に取り出したいとする．それを実現するプライバシ保護方式が複数あるとき，どの方法を使うことが最も望ましいだろうか．差分プライバシは，この意思決定をするために必要となる，安全性に関する共通的な指標を与える．

あるデータベースに含まれるレコードを属性値の組合せごとに集計して分割表（クロス集計表）[☆13] を作成することを考える．たとえばある試験結果のデータベースから男女別の合否人数に関する集計結果をまとめたもの，つまり（男性，女性）×（合格，落第）の 4 つのセルにそれぞれ該当人数を記入したものが分割表に相当する．

安全な分割表を出力するための方式としては，分割表のそれぞれのセルの値に乱数ノイズを加える方法や，元のデータベースの一部を「男性→女性」「合格→落第」などとランダムに書き換えてから（普通に）集計する方法などがある．たとえば Laplace メカニズムは前者に相当し，PRAM は後者に相当する．さて，どちらがより安全に有用性が高いデータを出力できるだろうか？

このような問いに対し，差分プライバシは安全性指標である ϵ に基づいた比較を可能にする．つまり，それぞれの方式において ϵ という共通の物差しを使って安全性を揃えた上で，それぞれの方式の有用性を比較すれば，どの方式を用いるのが最適であるかを決めることができる[☆14]（図 -6）．

別の言い方をすれば，新たなプライバシ保護の手法を考案したとき，上記の定義に照らし合わせて ϵ の値を計算することができれば，その手法は ϵ の値に応じた安全性を持つことが保証される．つまり，考案した新たな手法について，安全性の基準を揃えた上で従来の手法に対するメリットやデメリットを比較することが可能になる[☆15]．

☆12 後述の並列合成定理との対比から，直列合成定理（sequential composition theorem）とも呼ばれる．
☆13 集計対象となる部分集合が互いに素となる集計表．
☆14 なお，有用性の指標を元の分割表との誤差としたとき，一般に Laplace メカニズムのほうが PRAM より有用性が高い（誤差が小さい）[2]．
☆15 これがないと「ぼくのかんがえたさいきょうのほうしき」が本当に最強かどうか比べようがないので，プライバシ技術の健全な発展のために実はけっこう重要な性質である．

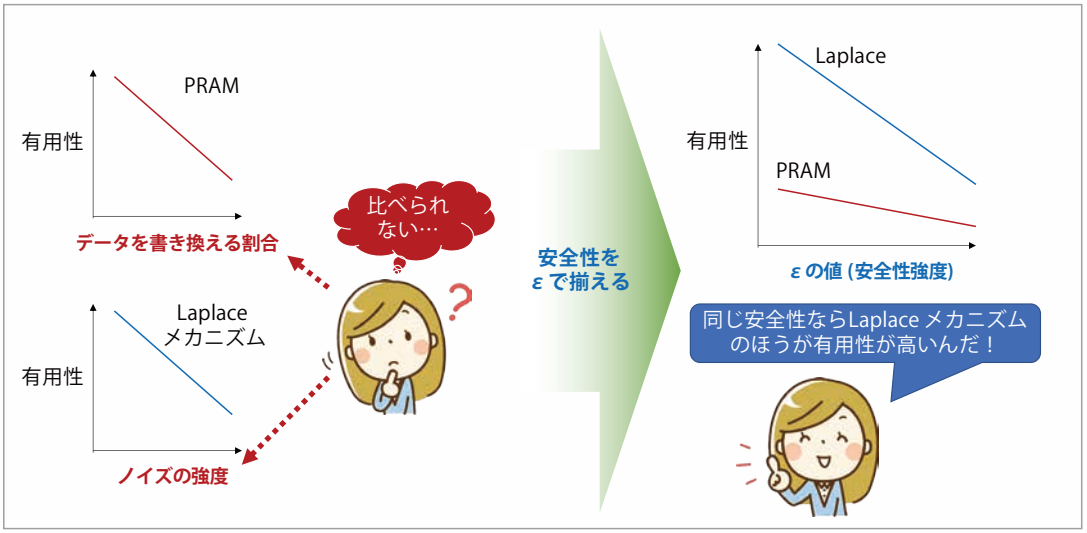


図 -6　安全性指標 ϵ を共通の物差しとして比較

合成定理

合成定理は，複数のメカニズムを合成したときの安全性を与える定理であり，以下で示される．

定理 1. それぞれ ϵ_i-*DP* を満たす n 個の問合せ Q'_i があり，Q' はそれらの Q'_i の列挙，つまり $Q'(D) = (Q'_1(D), Q'_2(D), \ldots, Q'_n(D))$ とする．このとき，Q' は $(\sum_{i=1}^{n} \epsilon_i)$-*DP* を満たす（図 -7）．

この定理は，複数のメカニズムを組み合わせて，新しい（より複雑な）差分プライバシを満たすメカニズムを構成することを可能にする．たとえば，ϵ_1-DP を満たすメカニズム Q'_1 と ϵ_2-DP を満たすメカニズム Q'_2 があるとする．このとき，$Q'(D) = f(Q'_1(D), Q'_2(D))$ として Q' が構成されるなら[☆16]，Q' は $(\epsilon_1 + \epsilon_2)$-DP を満たすことが保証される．

また，この定理は，差分プライバシを満たすメカニズムがデータベース再構築攻撃に対して一定の安全性を持つことを保証する．たとえば攻撃者がデータベース D から出力された $Q'_1(D)$ と $Q'_2(D)$ を得たとする．これらを重ね合わせて得られる任意の出力は，合成定理により $(\epsilon_1 + \epsilon_2)$-*DP* を満たすメカニズムの出力であるとみなせる．つまり，これらの重ね合わせによりどのような制約充足問題を得たとしても，$(\epsilon_1 + \epsilon_2)$-DP が与える安全性を超えて攻撃者が情報を得ることはない．

なお，合成定理の特殊な場合として，**定理 1** において Q'_i が適用されるレコードの集合が互いに素であるとき，Q' にはより強い安全性が与えられる．これを並列合成定理（parallel composition thorem）と呼び，具体的にはこのとき Q' は $(\max_i \epsilon_i)$-DP を満たす．

並列合成定理は，たとえば分割表を作成する際に，表の次元数（セル数）が増えても各セルに加えるノイズの強度は同じでよい（安全性は変わらない）ことを保証する．この性質は，たとえば国勢調査のような大規模な集計データのプライバシを保護するにあたって特に有用である．

☆16 f は任意の関数であるが，$Q'_1(D), Q'_2(D)$ のほかに D から導出された値を参照しないものとする．

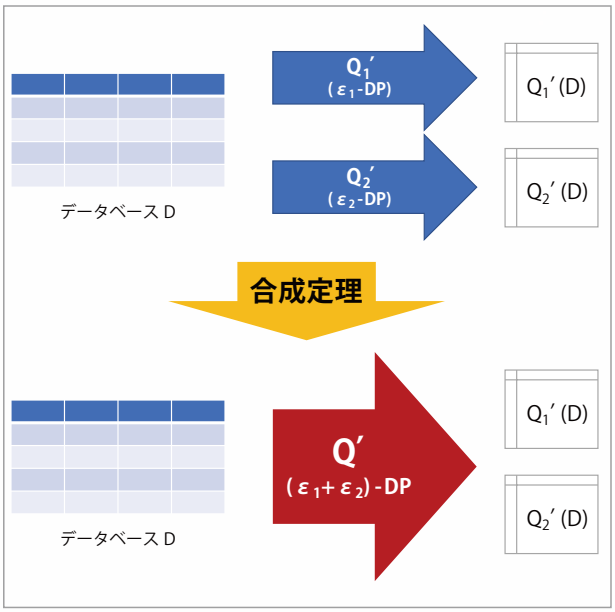


図 -7　合成定理

課題と今後の展望

差分プライバシはさまざまな有用な特徴を備え，その実現も簡単[☆17]であるが，まだ日本では普及が進んでいるとは言えない．何が導入を阻害しており，その解決には何が求められるのだろうか．

定義と ϵ の直感的理解の難しさ

まず 1 つに，定義 1 の直感的な理解の難しさが挙げられる．一見だけでこの定義が何を意味を持つことを理解するのは難しい（筆者自身も，最初に見たときはまったく分からなかった）．本稿が理解の一助となれば幸いであるし，今後さらに一般向けの解説が充実していくことが期待される．

また，このことにも関係するが，ϵ の値をいくつに設定すべきかが分かりにくいことも課題である．式 (1) を見ても ϵ の値がどの程度の安全性を意味するかは直感的に分かりにくい．また，ϵ がいくつで

☆17 たとえば Laplace メカニズムは，Python+NumPy なら一行で実装できる．

あれば十分に安全として社会的に認知されるかは，数式だけで定められるものではない．

ただし，冒頭で紹介した米国国勢調査局による差分プライバシの採用は，この ϵ の値の決定に関する問題への初めての大規模な取り組みと捉えることもできる．ϵ の値を決定するにあたっての考え方や具体的な値などについて，信頼できる公的機関による先行事例ができることによって状況が大きく変化していくことも考えられる．今後の動向に注目していきたい．

差分プライバシは厳しすぎる?

差分プライバシに対するよくある批判として，差分プライバシは厳しすぎる（データの有用性が不足する）というものがある．しかし，その理由が差分プライバシの定義が厳しすぎるためとは限らない．そもそもプライバシリスクが高すぎるデータを出力しようとしていたり，用いるメカニズムが適切ではなかったりすると，当然ながら有用なデータは得られない．

たとえば行動履歴データを匿名化して提供しようとする場合など，出力するデータが細かすぎると適切な ϵ を満たした上で高い有用性を持つ出力を得ることは困難である．しかし，このようなデータはそもそもプライバシ暴露のリスクがとても高いデータであり，差分プライバシは「適切に」そのリスクの高さを反映しているだけとも考えられる．差分プライバシを適用する以前に，安全性と有用性のトレードオフの観点から適切な粒度でデータを出力するように設計する，というプライバシ保護の鉄則を十分に検討することが重要である．

また，差分プライバシは安全性に関して統一的な保証を与えるが，その有用性はメカニズム次第である．差分プライバシを満たすメカニズムは無数に存在☆18し，それぞれ出力の統計的性質は異なる．つまり，応用ごとに適切なメカニズムは異なるものであり，不適切なメカニズムを用いると十分な有用性は得られない．たとえばPRAMはほとんどの問合せに適用可能な汎用性が高いメカニズムであるが，前述の通りこれを分割表の保護に使っても適切な ϵ の元に有用な出力を得ることは難しいだろう．

これまでの研究により，さまざまな応用に向けたメカニズムの提案や改善が進められている[3), 4)]．特に，近年では深層学習などの機械学習において差分プライバシに基づくプライバシ保護を実現する研究も活発になされている．差分プライバシの実用にあたっては，これらを参考に応用ごとに適したメカニズムを選択することが重要であるとともに，今後の技術の進展によるさらなるメカニズムの充実が期待される．

差分プライバシの先へ

ただし，定義1の要求が厳しすぎる側面がまったくないかというと，そうとも言い切れない．たとえば，あるメカニズムが任意の攻撃に対して一定の安全性を備えていても，それが ϵ として表せないケースも存在する．最後に，この ϵ では捉えきれない安全性に関する取り組みについて簡単に紹介する．

差分プライバシを実現するメカニズムとしてはLaplaceメカニズム（Laplaceノイズの加算）が代表的だが，より一般的な正規分布に従うノイズの加算（Gaussメカニズムと呼ばれる）では駄目なのだろうか．答えは駄目で，実際に定義1に照らして計算してみると $\epsilon = \infty$ となり，Gaussメカニズムは差分プライバシにおいて安全ではない．

これは，正規分布の裾のほうの極限遠点，つまり実際には値が発生することがあり得ないような領域で，式(1)における2つの確率の比が発散してしまうことによる．しかし，このようなほぼ発生しないことが明らかな（想定外の攻撃にはなり得ない）事象のために「安全ではない」としてしまうことは，安全性定義として厳しすぎる側面があるとも言える．

☆18 合成定理の存在から，任意のメカニズムの合成により新しいメカニズムを作り出すことができる．

(ϵ, δ)- 差分プライバシ

そこで，差分プライバシの変種として「ある一定以下の確率でなら，出力が差分プライバシを満たさないことを許容する」指標が提案されている．これを (ϵ, δ)- 差分プライバシ ((ϵ, δ)-DP) と呼び[☆19]．定義 1 における式 (1) を以下に置き換えたものとして定義される．

$$\Pr[Q'(D_1) \in S] \leq e^{\epsilon} \cdot \Pr[Q'(D_2) \in S] + \delta .$$

この式は式 (1) の右辺に δ を足したものであり，$\delta = 0$ のとき (ϵ, δ)-DP は ϵ-DP と等価となる．この定義も差分プライバシと似た安全性や合成定理を与えるが，$\delta > 0$ のとき，$\Pr[Q'(D_1) \in S] > 0$ かつ $\Pr[Q'(D_2) \in S] = 0$ となり得ることに注意したい．これは，メカニズムの出力値によっては，それが D_1 由来か D_2 由来かを攻撃者は決定的に知ることができてしまう（プライバシが決定的に暴露される）可能性があることを意味する[☆20]．

つまり，プライバシ保護において否認可能性を重視する立場からは，(ϵ, δ)-DP は安全性定義として逆に「ゆるすぎる」ところがあると言える．

レニー情報量に基づく定義

2016 年頃から議論されはじめた比較的新しい変種として，式 (1) の代わりにレニー情報量 (Rényi divergence) を用いて $Q'(D_1)$ と $Q'(D_2)$ の分布の近さとする定義が挙げられる（文献 5)，6）など）．具体的な安全性定義に少しずつ差異があるが，これらはいずれも決定的なプライバシ暴露の危険を排しつつ，Gauss メカニズムの安全性を定義可能にする点で共通している．また，これらの安全性定義の元では差分プライバシより効率良くメカニズムを合成できる（合成による安全性の低下が小さく抑えられる）という特徴を持つ．

ただし，これらの定義が与える安全性は差分プライバシと似て非なるものである．その解析は差分プライバシほどには進んでおらず，定義の解釈も差分プライバシよりさらに難しい（レニー情報量の概念の理解を必要とする）．そのため実用までの道程はまだ険しいと考えられるが，Gauss メカニズムの安全性を定義可能なことやメカニズム合成の効率が良いことは，高い有用性を備えた新しいメカニズムの構築に有効な性質である．プライバシ保護における，より高いレベルでの安全性と有用性のトレードオフの実現への期待から，今後の議論の進展に注目したい．

☆19 本来の差分プライバシと異なる（より弱い定義である）ことを明確にするために，(ε, δ) - 弱 (weak) 差分プライバシ，もしくは近似 (approximate) 差分プライバシとも呼ばれる．

☆20 なお，Gauss メカニズム自体は決定的なプライバシ暴露を起こさない．

参考文献

1) Garfinkel, S., Abowd, J. M. and Martindale, C. : Understanding Database Reconstruction Attacks on Public Data. ACM Queue, 16(5):28-53 (Oct. 2018).
2) 寺田，山口，本郷：匿名化個票開示への差分プライバシの適用，情報処理学会論文誌，58(9):1483-1500 (Sep. 2017).
3) Dwork, C. : Differential Privacy : A Survey of Results. In Proc. 5th Intl. Conf. Theory and Applications of Models of Computation, pp.1-19. Springer (2008).
4) Zhu, T., Li, G., Zhou, W. and Yu, P. S. : Differentially Private Data Publishing and Analysis : A Survey. IEEE Trans. Knowledge and Data Engineering, 29(8):1619-1638 (Aug. 2017).
5) Bun, M. and Steinke, T. : Concentrated Differential Privacy : Simplifications, Extensions, and Lower Bounds. In Theory of Cryptography, pp.635-658 (Nov. 2016).
6) Mironov, I. : Rényi Differential Privacy. In Proc. 2017 IEEE 30th Computer Security Foundations Symposium (CSF), pp.263-275 (Aug. 2017).

(2020 年 3 月 2 日受付)

■寺田雅之（正会員） teradam@nttdocomo.com

携帯電話ネットワークの運用データに基づく人口統計の作成と交通渋滞予測などの社会予測への応用，および大規模データのプライバシ保護に関する研究に従事．2017 ～ 2018 年度 CSEC 研究会主査．博士（工学）．

［差分プライバシ］

3 局所差分プライバシの最新動向

福地一斗　佐久間淳 | 筑波大学／理研 AIP

データ収集時のプライバシ保護

局所差分プライバシは，Google[1]，Apple[2] などの企業において，ユーザのプライバシ保護を行う技術として実際に運用しているサービスに導入されている．このため局所差分プライバシは非常に注目を集めており，研究も盛んに行われている．

差分プライバシ（DP）と局所差分プライバシ（LDP）は，個人情報を漏洩してはいけない範囲に違いがある．図 -1 で示すような，基本的な統計処理の流れを考える．それぞれの個人(図 -1 左) がデータを保持しており，それを収集者（図 -1 中央）へ提供する．収集者は収集した個人データに対して統計処理を行い，それを解析者（図 -1 右）へ公開する．差分プライバシでは，収集者が解析結果を解析者に公開するときに個人データが漏洩しないようにプライバシ保護処理を行う．収集者は生の個人データを閲覧することができるため，個人が収集者を信頼できる必要がある．一方，局所差分プライバシでは収集者が個人データを収集する際にプライバシ保護処理を行い，各個人のデータが漏洩しないようにする．したがって，信頼できない収集者に対する個人データの漏洩も防ぐことができる．多くのインターネット上のサービスでは収集者に対する個人データを提供する際のプライバシが問題となるため，局所差分プライバシが注目されるようになってきている．

局所差分プライバシの定義

最も簡単な状況の場合，局所差分プライバシでは図 -2 で示すデータ提供モデルを考える．ユーザはデータをそのまま収集者に送信したくないため，ノイズを加えるなどのランダム化処理を行うことでデータが読み取れないように加工を行う（図 -2 左半分）．収集者は処理済みデータのみを受け取る（図 -2 右半分）ため，送られてきた情報からはユーザの個人データを読み取ることが難しくなる．局所差分プライバシでは，ランダム化処理したデータから個人データの読み取りが難しくなるような条件を提供する．ランダム化処理が満たすべき条件を定めるために図 -3 のような状況を考える．図 -3 では，個人データが 3.5 であった場合と 4.5 であった場合でランダム化処理の結果の出力分布の違いを表している．赤が 3.5 のときの出力分布であり，青が 4.5 のときの出力分布である．もしこの 2 つの分布が十分近かった場合，収集者はランダム化処理したデータが 3.5 だったのか 4.5 だったのか区別することができない．つまり，収集者はランダム化処理したデータから元の値を推測することができないということができる．局所差分プライバシにおけるプライバシの保証は，このように 2 つの値に対して行ったランダム化処理の出力分布が近いことを要求する．具体的には，ランダム化処理を関数 M で表したとき，任意の異なる入力 x，x'と任意の M の出力ドメインの部分集合 S について，

$$\mathbb{P}\{M(x) \in S\} \leq \mathrm{e}^{\epsilon}\, \mathbb{P}\{M(x') \in S\}, \qquad (1)$$

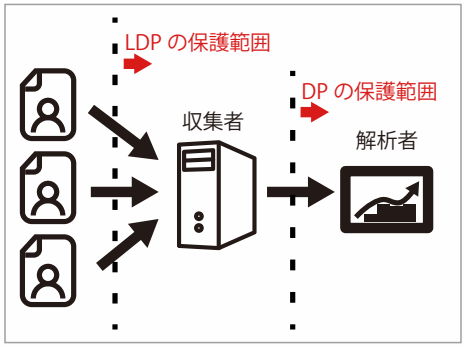


図 -1
差分プライバシと局所差分プライバシのプライバシ保護範囲

が満たされるならばランダム化処理 M は ϵ- 局所差分プライバシが満たされていると定義する．ここで，$\epsilon>0$ はプライバシバジェットと呼ばれるパラメータであり，小さいほど強いプライバシ保護を要求する．もし $\epsilon=0$ であるならば，収集者は個人データの情報をまったく得ることできないため完璧なプライバシ保護を実現しているが統計情報もまったく得られない．また，$\epsilon=\infty$ であるならば，収集者は個人情報そのものを受け取ることができるが，プライバシ保護はできていない．実際には，統計情報をある程度の精度で得ることが可能な中で最も小さい値を ϵ として設定することによって，プライバシと統計処理の有用性を両立することができる．

局所差分プライバシの研究分野では，上記の ϵ- 局所差分プライバシ条件を満たしたランダム化処理されたデータから，さまざまな統計的な情報を効率的に抽出する方法が開発されている．

対話可能性

局所差分プライバシには，ユーザや収集者の間のやりとりの制限を定めた**対話可能性**という概念がある．やりとりの制限が強いほど処理の複雑さや待ち時間などのユーザへの負荷が小さくシステムへの導入が容易であるが，統計処理の精度を犠牲にしてしまう．他方，統計処理の精度を向上させるためやりとりの制限を緩めると，エンジニアリングによってユーザの負荷を減らす工夫が必要になってくる．ただし，制限を緩めたとしても必ず統計処理の精度が向上するとは限らない．もし制限を緩めても統計処理の性能が向上しなければ，ユーザへの負荷が比較的少ないモデルを採用した方がよい．このような背景があり，対話可能性の違いによる統計処理の性能差の解析は現在研究が続けられているホットトピックとなっている．

本稿では主要な対話可能性として，対話なし，公開コインモデル，逐次的対話，完全対話を紹介する．図 -4 にそれらのモデルの対話の制限の強さ，ユーザへの負荷の大きさ，統計処理の精度の相対関係をまとめる．

対話なし (non-interactive)．図 -2 で示したデータ提供モデルは最も簡単な，ユーザが一斉にランダム化して収集者がそれらの処理済みデータを一旦収集してから統計処理を行うモデルである [3]．このようなモデルは，対話なしモデルと呼ばれる．このモデルの利点は，ユーザが行うランダム化処理が他のユーザや収集者の処理に依存していないため，ユーザの負担が少ない点にある．スマートフォンにあるデータをランダム化して収集者に送信するなどといった実際のアプリケーションを考えると，通信が安定していなかったり，処理能力が少なかったりするため，ユーザの処理の負担はなるべく少ないほうがよい．対話なしモデルはこのような状況に適している．一方で，このモデルの欠点は，ノイズを多量に入れなければいけなくなる可能性があるため，精度がそこまで高くない統計処理では有用な統計情報が得られないことである．後で紹介するような平均の推定など単純な統計量の推定はできるが，少しでも複雑な

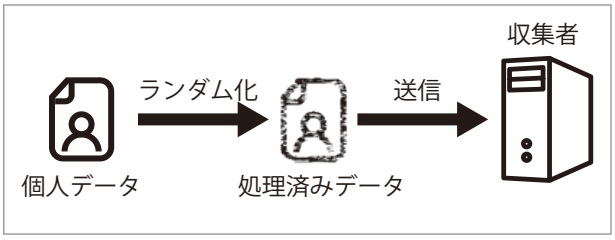


図 -2　データの加工／送信モデル

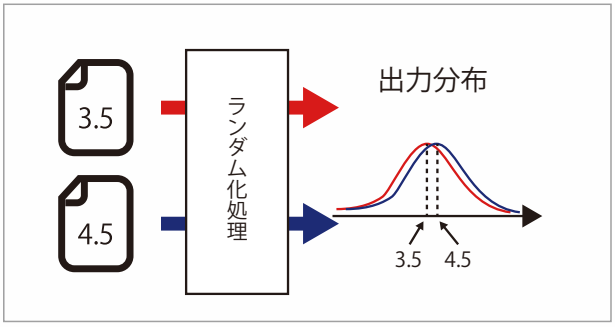


図 -3　差分プライバシの定義

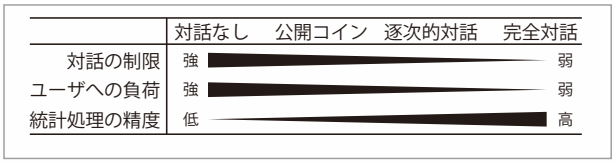


図 -4　対話可能性の特徴まとめ

統計的情報が欲しい場合はこのモデルの適用は難しい.

公開コインモデル (public-coin model). 公開コインモデル[4]では，ユーザがランダム化する際にユーザと収集者全員に共有された乱数を活用できる．共有した乱数を用いてデータの圧縮などを行うことによって，統計処理の精度を向上させることができる．一方，このモデルでは乱数の共有を行わなければいけないため，ユーザの負担は対話なしモデルと比べて多少増加する．しかし，収集者が乱数を生成してユーザがそれをダウンロードしてからランダム化を行うといった実装を行えば対話なしモデルに比べたユーザの待ち時間の増加はほとんどないと言える．

公開コインモデルはユーザ負担の増加が少ないが，対話なしモデルに比べて大きな精度の向上がある．このため，後に紹介するGoogleやAppleの事例では公開コインモデルを採用している．また，離散分布における一様性の検定などのタスクにおいて統計処理の性能が優位に向上することが理論的に示されており[4]，公開コインモデルが有用であることが見て取れる．

逐次的対話 (sequential interactive). 逐次的対話モデルではユーザ1人ずつ逐次的にデータの収集を行う[5]．データの収集を行う際に，データ収集者はその時点以前に収集したデータから計算した情報をユーザに送り，ユーザはランダム化処理にその情報を活用することができる．これによりユーザが送る情報をその時点以前に収集者が得た情報をもとに適応的に選択することができるため，統計処理の性能を向上させることができる．一方で，あるユーザがランダム化処理を行うためには，他のユーザのデータ収集処理が終わっていなければならないため逐次的な処理しかできず，データ送信の際にユーザに待ち時間を生じさせてしまう可能性がある．

逐次的対話モデルは，確率的勾配降下法などの確率的一次最適化のアルゴリズムのように逐次的にデータへアクセスしながら処理するアルゴリズムへの相性がよい．確率的勾配降下法は深層学習などのモデルの構築でも用いられているため，プライバシに配慮した機械学習を行うための対話モデルとしての研究が盛んに行われている．

完全対話 (full interactive). 完全対話モデルは，逐次的対話よりも柔軟な対話可能性であり，その一例として，同じユーザに対して何回もデータ収集を行うことが可能なモデルである．通常のプライバシを考慮しない深層学習などでは同じユーザのデータを何回も使って学習を行うため，そのアルゴリズムをプライバシ保証しつつ実行したい場合はこのモデルを考える必要がある．このモデルでも逐次的対話モデルと同様に，収集者がこれまで得た情報をユーザへ渡さないとランダム化処理を行うことができないため，データ送信の際にユーザに待ち時間を生じさせてしまう可能性がある．一方で統計処理の性能は，完全対話モデルを導入することによって逐次的対話モデルに比べて優位に向上するタスクがあることが知られている[6]．

局所差分プライバシの実現手法

ここでは簡単な局所差分プライバシのアルゴリズムとして，2値の離散データ提供するランダム化処理とスカラー値の平均値を推定するためのアルゴリズムを紹介する．

2値の離散データ提供（ランダマイズドレスポンス）. 最も簡単なランダム化処理の例として，2値の離散データを提供するランダマイズドレスポンスを紹介する．ユーザのデータを $x \in \{0, 1\}$ であるとすると，ランダマイズドレスポンスによる処理の結果 z は以下の式で書ける．

$$z = \begin{cases} x & \text{w.p. } e^{\varepsilon}/(1+e^{\varepsilon}) \\ 1-x & \text{w.p. } 1/(1+e^{\varepsilon}). \end{cases} \tag{2}$$

式 (2) は，$e^{\epsilon}/(1+e^{\epsilon})$ の確率で x がそのまま提供され，$1/(1+e^{\epsilon})$ の確率で x を反転して提供することを表している．そのまま提供される確率と反転する確率の比が e^{ϵ} になるため，ϵ- 局所差分プライバシを保証することが分かる．ランダマイズドレスポンスは単純であるがプライバシを保護しつつ1bitの情報を送るには効率的で

あるため，さまざまなアルゴリズムのコンポーネントとして用いられている．

平均値推定のためのスカラー値提供. ユーザは個人データとしてスカラー値を保持しており，収集者は個人のプライバシを保証しつつそれらのスカラー値の平均を得たいという設定を考える．ユーザ側のランダム化処理は次の手順で行う．1) 自分が持っているスカラー値の絶対値が一定値より小さくなるようにクリッピング[☆1]を行う，2) クリッピングしたデータに平均 0，スケールパラメータ $1/\epsilon$ のラプラス分布から得られたノイズを加える，3) ノイズを加えたデータを収集者に送信する．上記の処理では，スケールパラメータを適切に設定したラプラス分布からのノイズを加えることによって ϵ - 局所差分プライバシを保証し，送信したデータから元の値が推測できないようにしている．局所差分プライバシでは非有界なデータをそのまま扱えないが，クリッピング処理によって扱えるようにしている．収集者は，ランダム化したデータを受け取り単純に標本平均を計算することで平均の推定値が得られる．このアルゴリズムは真の平均が $[-1, 1]$ の範囲にある場合，誤差が最も小さいことが知られている[5]．

局所差分プライバシの応用事例

本章では局所差分プライバシの応用事例として Google の Web ブラウザからユーザの Web 閲覧に関する情報の頻度統計収集と Apple の iOS デバイスからユーザのデバイス利用に関する頻度統計収集を紹介する．それぞれの事例の概要を表 -1 にまとめる．

Google の局所差分プライバシ

概要：Google の Web ブラウザ Chrome にはエンドユーザによる Chrome の利用統計を収集するための仕組みとして Randomized Aggregatable Privacy-Preserving Ordinal Response (RAPPOR)[1] と呼ばれるアルゴリズムが利用されている．RAPPOR はプライバシを保護しつつ多数のクライアントから離散値や連続値，文字列などで表される情報を収集し，その頻度やヒストグラムを推定することを目的として設計されており，実装が公開されている[☆2]．

システム：RAPPOR では，デバイスサイドの計算はブラウザで実行される（図 -5）．ユーザから収集された情報（たとえば URL やコンピュータ上で実行されているプロセス名）はブラウザ上でランダム化された上でサーバに送信される．サーバは多数のユーザから集めたランダム化情報から，頻度情報を推定する．

基本のメカニズム：RAPPOR のデバイスサイドのプライバシ保護はランダマイズドレスポンスを応用した手法で実現されている．まずは最も単純な離散値の扱いについて紹介する．ユーザがサーバに提供する情報 v

☆1 閾値 T によるスカラー値 x のクリッピングの結果は $\max\{\min\{x, T\}, -T\}$ で得られる．

表 -1　Google と Apple による局所差分プライバシ応用事例の比較

	Google	Apple
クライアント	Chrome	iOS デバイス
対象データ	カテゴリカルデータ，文字列等	カテゴリカルデータ，文字列等
応用先	プロセス頻度統計，URL 頻度統計等	絵文字頻度統計，音声再生頻度統計等
特徴	Bloom filter による情報の圧縮	ハッシュ関数による情報の圧縮
対話可能性	公開コインモデル	公開コインモデル

☆2 Rappor（Randomized AggregatablePrivacy Preserving Ordinal Responses）．http://www.chromium.org/developers/design-documents/rappor

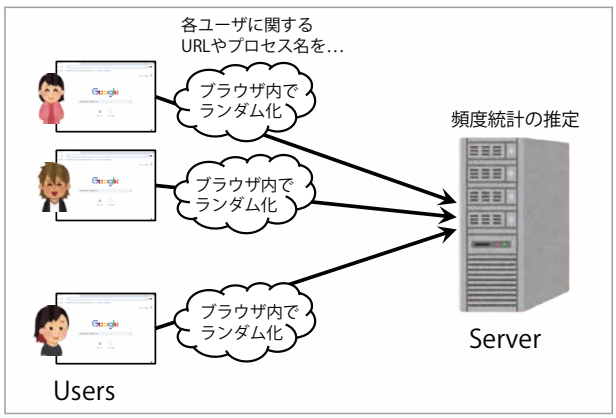


図 -5　Chrome による局所差分プライバシを用いた頻度統計の推定

を k-bit のバイナリベクトルとする. v はユーザの個人情報であり，これをサーバに提供する前にデバイスサイドでランダム化によるプライバシ保護を行う．具体的には，RAPPOR では v の第 i 要素を v_i としたとき，以下のようにランダム化を行う .

$$v_i' = \begin{cases} 1, & \text{with prob. } 1/2f \\ 0, & \text{with prob. } 1/2f \\ v_i, & \text{with prob. } 1-f \end{cases} \quad (3)$$

サーバサイドでは，ユーザから収集したランダム化バイナリベクトルを集計し，各ビットが 1 である割合を推定する．このような情報提供の方式は One-time basic RAPPOR と呼ばれる．各ユーザの操作は各ユーザが独立に構成した乱数生成器に基づき行うことができるため，この手法の実行は対話なしモデルに基づくものである.

メカニズムの拡張：実際の応用においては，きわめて大きいドメインサイズを持つ情報についての統計を得たい場合がある．文字列のバリエーションは文字列長に対して指数的に増加するため，これを表現するためにはユーザは非現実的な長さのバイナリベクトル用いる必要がある．これを避けるために，RAPPOR では Bloom filter を用いた情報の圧縮を導入している. Bloom filter は，任意に指定した要素 $x \in \mathcal{X}$ が集合 $X \subseteq \mathcal{X}$ に含まれるか否かを判定するための確率的データ構造である. Bloom filter は $\mathcal{X}$ のサイズにかかわらず，集合を k-bit のバイナリベクトルで表現でき空間効率性がよいが，その代償として，問合せ結果には偽陽性（指定した要素が集合には含まれていないにもかかわらず，含まれていると出力すること）が含まれる .

文字列情報を RAPPOR で取り扱うためには，ユーザ側の文字列情報を，Bloom filter の構成要素であるハッシュ関数に入力し，その出力であるバイナリベクトル B を式 (3) でランダム化して提供する．利用するハッシュ関数の数を h としたとき，式 (3) によるランダム化は $\epsilon = 2h \ln \frac{1-1/2f}{f/2}$ について ϵ-LDP が保証される. Bloom filter を用いた RAPPOR は各ユーザが同一のハッシュ関数を構成する必要があることから，すべてのユーザが同一の乱数生成器に基づき計算を実行する必要がある．このことから，この手法の実行は公開コインモデルに基づくものである.

応用：Chrome に設定されている homepage の URL 頻度統計調査に対する RAPPOR の適用例を紹介する.

データ収集は調査に Opt-in したユーザから約 1,400 万件のレポートを対象とした. Chrome の homepage や検索エンジンのページは malware の標的となっており，ユーザの同意なく悪意あるサイトの URL に書き換えられることがある．こういった設定の頻度統計を大規模に取得することが目的である．収集は 2 個のハッシュ関数 (k=2) を用いた 128 個の Bloom filter が用いられ，パラメータは q=0.75，p=0.5，f=0.75 と設定された．ここで q，p は式 (2) に関連するパラメータであり，q は入力ビットをそのまま出力する確率，p は入力ビットを反転して出力する確率である．このとき達成されるプライバシは ϵ =0.5343 における LDP となる．この設定において，頻度が統計的に有意に 0.1% より大きい homepage の URL ドメインを推定したところ，8,616 個ある候補のうち，31 ドメインの頻度を得た .

Apple の局所差分プライバシ

概要:Apple の iPhone 等の iOS デバイスにも，ユーザからデバイスの利用に関する統計情報，特に頻度情報を収集するための 2 つの仕組みが実装されている [2].

システム：Apple の方式では，デバイスサイドの計算は iOS デバイスで実行される（図 -6）．イベント（たとえばキーをタイプする，Web サイトを訪問する）が発生するたびにその情報は局所差分プライバシを満たすようにランダム化され，デバイス上に蓄積される．一定量の情報が蓄積されたタイミングで，ランダム化データは Ingestor と呼ばれるサーバに送信される. Ingestor では送信元（つまりユーザのデバイス）の IP アドレスやデバイスの識別情報，タイムスタンプなどを消去し，データを Aggregator と呼ばれるサーバに送信する.

Aggregator では収集情報から頻度情報を統計的に推定する．

メカニズム：Apple のシステムでは，Private Count Mean Sketch (CMS) と呼ばれる，離散値，連続値，文字列など任意のデータを，ハッシュ関数を利用して $\{-1.+1\}$ を要素に持つ長さ m のベクトルに符号化（sketch と呼ばれる）した上でランダム化する手法が利用されている．デバイスサイドでは k 個のハッシュ関数 $h_1, \ldots, h_k$ をランダムに生成する．各ハッシュ関数は $h_i: \mathcal{D} \to \{1, \ldots, m\}$ なる写像である．ここで，$\mathcal{D}$ は頻度をカウントする対象となる任意のデータのドメインであり，ハッシュ関数が構成可能なデータ型であれば何でも構わない．通常は $|\mathcal{D}| \gg m$ であるため情報の損失があるが，ドメインサイズが小さい場合は圧縮せず $\mathcal{D} = \{1, \ldots, m\}$ としてよい．

データの要素 $d \in \mathcal{D}$ の符号化を説明する．まず k 個あるハッシュ関数のうち 1 つをランダムに選択する．ここでは h_j が選ばれたとする．このとき，d は $v \in \{-1, 1\}^m$ に以下のように符号化される

$$v_i = \begin{cases} 1, \text{ if } i = h_j(d) \\ -1, \text{ o.w.} \end{cases} \tag{4}$$

その後ベクトル v をランダム化する．具体的には，各 bit の符号を独立に $\frac{1}{e^{\epsilon/2}+1}$ の確率で反転する．このように生成されたランダム化ベクトル v'は，ϵ 局所差分プライバシを保証することが証明される．この方式でも各ユーザが同一のハッシュ関数を構成する必要があることから，この手法の実行は公開コインモデルに基づくものである．

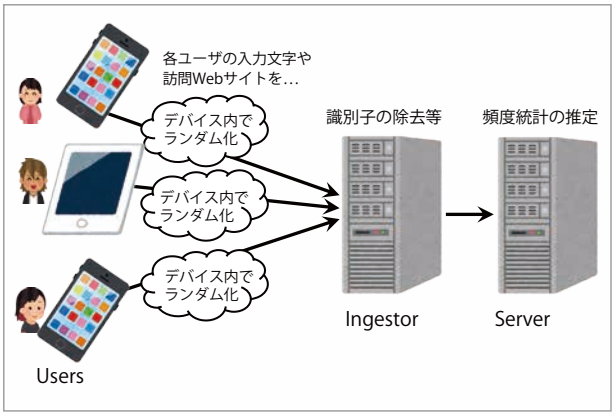


図 -6　iOS デバイスによる局所差分プライバシを用いた頻度統計の推定

続いてサーバサイドの処理を説明する．サーバサイドでは，各ユーザ i から，$(v'^{(i)}, j^{(i)})$ を収集する．ここで $v'^{(i)}$ はユーザ i の情報を符号化の上ランダム化した情報，$j^{(i)}$ はユーザ i がランダムに選択したハッシュ関数のインデクスである．続いて収集したランダム化データを，スケッチ行列 $M \in \mathcal{D}^{k \times m}$ に集約する．集約の詳細はここでは触れないが，集約の結果，要素 d の頻度の不偏推定量を得ることができる．文献 2）では分散の上界がプライバシバジェット ϵ，ユーザ数 n，データドメインのサイズ $|\mathcal{D}|$，ハッシュ関数の出力のサイズ m の関数として導出されている．

分散の上界は推定精度の限界を与えており，小さければ小さいほど高い推定精度が期待できる．原理的には分散の上界とプライバシはトレードオフの関係にある．きわめて多数のユーザからの情報収集を行う Apple のシステムにおいては，これらのファクタに加えてサーバサイドのランタイムやデバイスサイドのネットワーク帯域なども考慮する必要がある．直感的には k はサーバのランタイム，m はユーザデバイスの帯域に関係しており，データを収集可能なユーザ数および想定するプライバシバジェットに応じて，k と m をチューニングする必要がある．

応用：文献 2）で紹介されている局所差分プライバシを保証した頻度分析の応用例を紹介する．

Web サイトの中には計算リソース（CPU あるいはメモリ）を大量に消費するものが存在し，そのような Web サイトを特定するための調査を行った．この調査では HCMS[☆3] が利用され，パラメータは m=32,768, k=1024, ϵ=4, p=250,000 とセットされた．調査結果からは，そのような Web サイトには動画サイト，ショッピングサイト，ニュースサイトなどが含まれることが推定

☆3 文献 2）では基本となる Private Count Mean Sketch に加え，その拡張として，デバイスからサーバへの通信をわずか 1 ビットに抑えた手法（Private Hadamard Count Mean Sketch，HCMS）が導入されている．詳細は原論文を参照されたい．

された.

応用事例に対する批判的意見：文献 7）では iOS を通じてユーザが局所差分プライバシを利用しつつ Apple にデータを提供した場合に，消費されるプライバシバジェットが分析されている．この研究では，差分プライバシによるデータ提供の応用事例である emoji, new words, deeplinks, lookup hints について，macOC Version 10.12 の静的および動的コード解析と実験を通じて消費されるプライバシバジェットを調査した☆4．その結果，データの 1 回の提供で消費されるバジェットは 1 あるいは 2 であるが，上記 4 つの調査のためのデータ提供はシステム全体を通じて 1 日あたり 16 のバジェットを消費し得ることを示した．局所差分プライバシにおける $\epsilon=16$ はプライバシが強く保護されているとは言えず，またそのことが明示的にユーザに示されているわけでもないことから，著者らは差分プライバシを通じたデータ収集においては十分な透明性を確保するべきであることを主張している．

まとめと今後の展開

局所差分プライバシは統計的な理論保証を可能にするプライバシ保護の仕組みであり，これまでに紹介したように多くのユーザを擁するプラットフォーマーがユーザからの情報収集に利用してきた．局所差分プライバシでは，個人データにノイズが加わった状態でプラットフォーマーへ提供されるため，誰かがなんらかの手段を用いて提供されたデータを見ることができたとしても個人のプライバシ保護を保証できるという意味で有用性が高い．差分プライバシは原理的にプライバシ保護と推定される統計量の精度がトレード・オフの関係にあるが，データを提供するユーザ数が多ければ多いほどその精度は一般に改善することが期待される．ただし，きわめて多くのユーザからの情報提供を受けることが可能な状況であっても，上記の批判にあるように十分なプライバシ保護が保証されているとは言えない場合もあり，十分なプライバシ保護と高い精度での推定を両立できる方法の開発は今後も続くと考えられる．

☆4 Engineering Privacy for Your Users，https://developer.apple.com/videos/play/wwdc2016/709/

参考文献

1) Erlingsson, Ú., Pihur, V. and Korolova, A. : Rappor : Randomized Aggregatable Privacy-preserving Ordinal response, In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. pp.1054-1067 (2014).
2) ADP Team et al. : Learning with Privacy at Scale, In : Apple Machine Learning Journal 1.8 (2017).
3) Kasiviswanathan, S. P. et al. : What Can We Learn privately?, In: SIAM Journal on Computing 40.3, pp.793-826 (2011).
4) Acharya, J. et al. : Test without Trust : Optimal Locally Private Distribution Testing, In:Proceedings of Machine Learning Research. Ed. by Kamalika Chaudhuri and Masashi Sugiyama, Vol.89. Proceedings of Machine Learning Research, PMLR, pp.2067-2076 (2019).
5) Duchi, J. C., Jordan, M. I. and Wainwright, M. J. : Local Privacy and Statistical Minimaxrates, In: 2013 IEEE 54th Annual Symposiumon Foundations of Computer Science. IEEE, pp.429-438(2013).
6) Joseph. M. et al. : The Role of Interactivity in Local Differential Privacy, In: 2019IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS) , pp.94-105 (2019).
7) Tang, J. et al. : Privacy Loss in Apple's Implementation of Differential Privacy on Macos 10.12, In: arXiv preprint arXiv:1709.02753 (2017).

（2020 年 3 月 17 日受付）

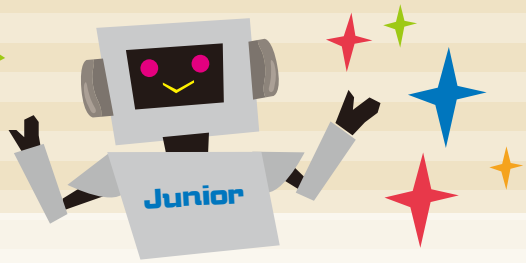
■**福地一斗**　fukuchi@cs.tsukuba.ac.jp

2018 年より理化学研究所革新知能統合研究センターの特別研究員として勤務．2019 年より筑波大学助教，同年より理化学研究所革新知能統合研究センターの客員研究員（兼任）へ従事する．機械学習の公平性やプライバシに関する研究を中心に行っている．

■**佐久間淳（正会員）**　jun@cs.tsukuba.ac.jp

2004 年東京工業大学総合理工学研究科助手，2009 年筑波大学准教授，2016 年同教授，現在に至る．2016 年 理化学研究所革新統合知能研究センターグループリーダー（兼任）．機械学習と知識発見，AI セキュリティとプライバシの研究に従事．

集まれ！ジュニア会員！！



今回は前回に引き続き，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．

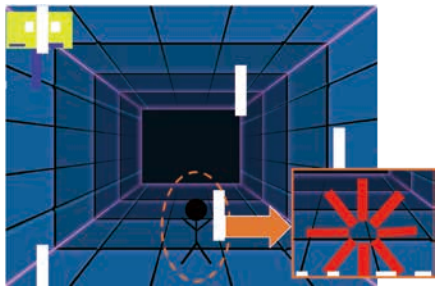
本イベントではプログラミング環境 Scratch と，プログラミング可能な小さなコンピュータである micro:bit を利用して，保護者の方と一緒にアニメーションやゲームを制作しました．今回は制作された作品の中から 1 つの作品を紹介します．

作品紹介

マイゼンシスターズ大好きさんの作品
「棒人間ミサイルよけゲーム」

https://scratch.mit.edu/projects/355704394/

micro:bit を使って棒人間を動かして，敵からのミサイルをよけて遊ぶゲームです．micro:bit の A ボタンを押すと棒人間は左に動き，B ボタンを押すと右に動きます．棒人間にミサイルが当たってしまうと棒人間は爆発します．こだわったポイントは，棒人間のキャラクタを丸と直線を利用して自分で作ったところです．敵やミサイル，ミサイルに当たってしまったときの絵も自分で作っています．ミサイルに当たったときに音を鳴らすように改良したいです．



●作品の画面キャプチャ

●棒人間のコスチューム

●ミサイルのプログラムの一部

せっかくの棒人間のキャラクタなので，何度も復活させてあげてもいいですね．制限時間を設定したり，よけられたミサイルの数を得点にしたり，ゲーム性を高めていってみましょう．また，音を鳴らしたいときには「音」カテゴリーにあるブロックを利用します．あらかじめ用意された音だけでなく，自分の声などを録音して利用することもできます．

作品に登場するキャラクタにオリジナリティがあっていいですね．また，ミサイルは Scratch のクローン機能（スプライトを複製する機能）を利用して何発も発射されるプログラムになっていて，とても楽しいゲームになっています．

今回紹介した作品のように，micro:bit はキャラクタを操作するコントローラとして利用することもできます．キーボードの矢印キーで操作する作品を，micro:bit で操作するように改良してみると，また違った楽しみのある作品になるかもしれません．ぜひ試してみてください．

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

「集まれ！ジュニア会員！！」の Web ページができました
https://www.ipsj.or.jp/magazine/jrlist.html

Web ページでは，このコーナーで紹介されたプログラムのソースコード一覧が掲載されています．
連載記事を読んでソースコードに興味を持った方，ぜひ参考にしてみてください．

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）

ETロボコン：異色の情報系ロボコン
― 光る若手にインタビュー ―

編集にあたって

平山貴司 | 岩手大学

ETロボコンは，巷でイメージされるロボコンとは一線を画す，情報系のロボコンです．ロボコンなのにロボット本体の工夫や改造が禁じられています．では何を競うのかというと，ロボットを自動制御するソフトウェアです．業界用語で言うところの組込みソフトウェアの技術を競います．

2019年は，全国の企業や大学など259チームがETロボコンにエントリしました．9月に地区大会が行われ，各地区から選ばれた代表チームによるチャンピオンシップ大会が，11月20～21日にパシフィコ横浜で開催されました．本会もETロボコンに協賛しており，毎年本会から優秀な学生等のチームに若手奨励賞を贈っています．本会とかかわりの深いコンテストですので，ミニ特集として取り上げることにしました．本ミニ特集では，ETロボコンの概要と学生主体の2チームへのインタビューからなる，3本の記事をお届けします．

ETロボコンは，ソフトウェア重視の異色の情報系ロボコンということもあり，インタビューに入る前に，読者の皆さんにETロボコンの事前の説明が必要です．そこで「**ソフトウェア教育・実践の場としてのETロボコン―時代に合わせたモデリング課題の提供―**」では，ETロボコン本部審査委員長に，ETロボコンの特徴・狙い・ルールなどを中心に概説していただきます．ETロボコンでは，組込みソフトウェア技術教育をテーマに挙げており，モデル審査が行われます．参加チームは，競技に先立ってソフトウェアの設計図であるモデル図を実行委員会に提出し，審査を受けます．競技に勝つだけでなく，ソフトウェアの品質を担保することも求められます．これがETロボコンの最大の特徴です．総合成績は，競技とモデル審査の総合評価で決まります．

ETロボコン2019では部門やクラスが分かれており，本ミニ特集では，上級者向けのデベロッ

パー部門アドバンストクラスに出場したチームに注目します．その中から光る若手を取り上げたいと思い，優秀な成績により表彰を受けた学生主体の2チームに，ETロボコンへの取り組みについて尋ねます．出場することになったきっかけ，ロボットの制御，スピード競技，ボーナス課題のブロックビンゴ，モデル図，ETロボコンを通じたスキル向上などについて，Q&A形式でチームの学生の代表4名に答えていただきます．

「**KAMOGAWAの訓練生にインタビュー**」の「KAMOGAWA」は，競技3位・若手奨励賞に輝いたチームです．競技において，課題を見事パーフェクトクリアし，会場を大いに湧かせました．この点が評価されて，若手奨励賞が贈られました．インタビューでは，専門校で1年間毎日のように取り組んだ様子が語られています．次の若い世代へのメッセージも送っています．

「**がんちゃん+Xの学生にインタビュー**」の「がんちゃん＋X」は，TOPPERS賞を受賞したチームです．総合成績でも4位と健闘しました．モデル図において信頼性や保守性の高い実装設計がなされている点を評価されて，TOPPERS賞が贈られました．2月から11月まで学業の合間を縫って取り組んだ努力が語られています．辛かったことや楽しかったことの話も織り交ぜられています．

ETロボコンには名だたる企業のチームも多数出場しています．その中で，学生チームが表彰台に上がったことは快挙です．学生の活躍を紹介することで，本会の学生会員やジュニア会員など若手の読者層を元気づけられればと思います．

（2019年11月18日）

［ETロボコン：異色の情報系ロボコン ― 光る若手にインタビュー ―］

①ソフトウェア教育・実践の場としてのETロボコン
―時代に合わせたモデリング課題の提供―

土樋祐希 | ETロボコン本部審査委員長／富士ゼロックス

ETロボコンとは

組込みエンジニアの育成を目指したソフトウェアコンテスト

ETロボコンは組込みシステム技術協会（JASA）が主催するソフトウェアコンテストである．正式名称は「ETロボットソフトウェアデザインコンテスト」である．組込みソフトウェアエンジニア育成を目指したコンテストであり，他のロボットコンテストにはない特徴的な取り組みを行っている．2019年には長年の組込み産業界の人材育成への貢献が認められ，「情報化促進貢献個人等表彰」の経済産業大臣賞を受賞することができた．本稿ではETロボコンの特徴を紹介する．また，時代とともに必要とされる技術は変化しており，ETロボコンも提供する課題を変えてきている．2019年の競技とその狙いについても説明する．

ETロボコンの特徴

全国の企業・学生チームが競う大会

ETロボコンは2002年に開催されたUMLロボコンにその端を発する．当時，日本であまり普及していなかったUML（Unified Modeling Language／モデル統一言語）を実践的に使う場を提供する目的で有志に行われた大会であった．2005年よりJASAが主催となり，ETロボコンと改名した．2019年で18年目となり，今では全国12地区で地区大会が開催され，250を超えるチームが参加している大会となっている．地区大会で優秀な成績を残したチームは11月のET/IoTテクノロジー展と併設で開催されるチャンピオンシップ大会（CS大会）に出場する権利を得る．ETロボコンに参加するのは企業チームだけではなく，大学・高専・高校など学生チームも競う．学生チームであってもハンディキャップは一切なく同じルールで競う．近年学生チームは活躍しており，2018年度はCS大会17表彰のうち11表彰が学生チーム（企業連携含む）であった．このように幅広い層で切磋琢磨できるコンテストとなっている．

全チームで共通の走行体を使用

ETロボコンはLEGO MINDSTORMSで作成された走行体を使用した競技である．走行はソフトウェアによる自律走行である．大きさが12畳にもなるコース（図-1）を人間の操縦なしに走行させ，走行にかかった時間と課題（難所）をクリアした際に得られるボーナスによって競技の成績が決まる．ETロボコンの大きな特徴の1つは，参加カテゴリ（クラス）ごとに使用する走行体の組み方が決められていることである．図-2に

図-1　ETロボコンの様子

2019 年のアドバンストクラス（中級者用クラス）で使用した走行体を示す．ロボットの機械的な性能差は存在せず，搭載するソフトウェアによってのみ差が出ることになる．この点が他のロボットコンテストと大きく異なる点と言える．

最大の特徴はモデル審査

ET ロボコンの最も大きな特徴はモデル審査である．参加者は作成したソフトウェアやシステムの設計図を作成し，事前に提出する．この際，設計図にはシステムを作る上で必要となる要素や振舞いを UML などで図示化したモデルとして表現する．ソフトウェアは建築物やメカなどと異なり，直接触ったり見たりすることができない無形のものである．そのため，全体を俯瞰することが難しい．最悪ソフトウェアができた後に期待した機能や性能となっていないことが判明するということもある．モデルという形で見える化することで他者とのコミュニケーションをとりやすくし，レビューなどを通じて早い段階で品質を高めることが必要となる．これは実際の開発の中でも重要な手法である．ET ロボコン参加者は全部で A3 用紙 6 枚に設計情報をまとめたモデルシートとして提出する．図 -3 に 2019 年度のモデルシートの一部（分析部分）を示す．図 -4 は 2019 年度にアドバンストクラスで提示された記述内容である．要求・分析・設計・制御と開発を行う上で必要となる各フェーズでモデルを使った記述が求められている．提出されたモデルシートは ET ロボコン実行委員に属する審査員によって行われる．記述するモデルの項目が細分化され，それぞれに対して審査基準を用意している．基本的にはそれに従い審査をする．基準だけでは評価しにくい部分もあるため，審査は複数人で行う．審査員個人による評価を行った上で，集合レビューを通じて評点を決定する．項目ごとに 0（記述なし）～ 3（最高点）といった形で評価し，そのモデルの点数を決定する．この点数により順位付けを行う．ET ロボコンでは「競技」，「モデル審査」，後述する「総合」の 3 種類の表彰を設けている．競技が悪いチームもモデルが良ければモデル審査で表彰している．また，参加者には審査結果を評価ランクとして伝える．評価ランクは A ～ D となっており，A が一番良いランクとなる．審査員のコ

図 -2　2019 年の走行体 HackEV

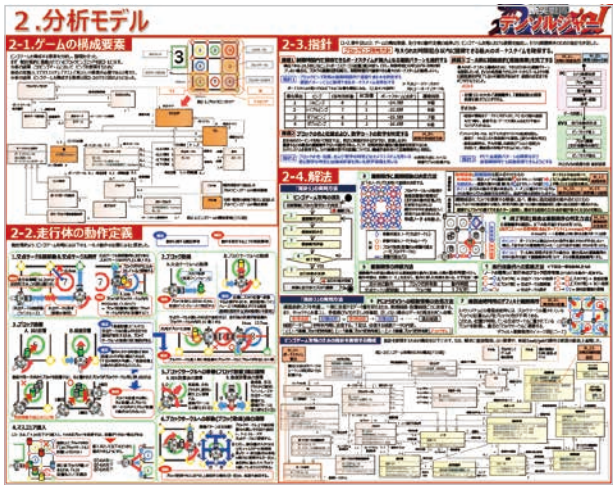


図 -3　提出モデルの例

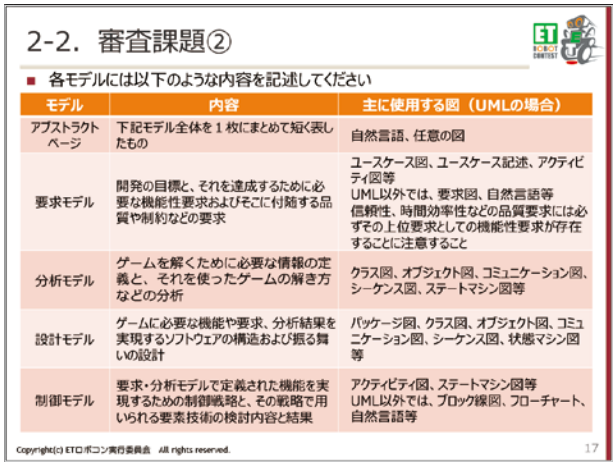


図 -4　審査の内容（2019 年審査規約より）

メントも提供されるため，参加チームは自分たちの強みや弱みを知ることができ，さらなる学びにつなげることができる．同じ課題に対してこれだけ多くの参加チームが設計資料を公開するのも他のコンテストにはない特徴である．参加者は公開された他チームのモデルを参考にすることでさらに理解を深めることができる．このようにETロボコンは単にソフトウェアを作るだけでなく，開発する上で重要な設計技術を学べる場としての仕組みを用意している．

総合成績は競技と審査で決まる

ETロボコンでは競技結果とモデル審査結果を合わせた総合成績が最も重要な成績となる．総合成績は競技･モデルの結果を正規化し，それらの調和平均によって求める．図-5に2019年の結果を示す．縦軸が競技，横軸がモデル審査の結果である．右上に近いほど総合成績が良い．調和平均を使用しているため，競技・モデルどちらかが良いだけでは総合の上位になることができない．両方をバランス良く作り上げる必要がある．このような仕組みにより，設計と実装の両方のスキルを伸ばすインセンティブを与えている．

ETロボコンの競技と狙い

2019年の競技

図-6に2019年のアドバンストクラスで使用したコースを示す．競技では各チームL（左）／R（右）コースを一度ずつ，計2回の走行を行う．図の中央上のSTARTから2チーム同時に左右に分かれて走行体を走らせ，中間ゲート1(3)，中間ゲート2(4)を経由してGOALゲート(5)まで走行する．GOALまでにかかった時間が「走行タイム」として記録される．走行タイム取得後は「難所」と呼ばれる課題をクリアすることで，追加のボーナスタイムを得られる．走行タイムから獲得したボーナスタイムを引いた結果が「リザルトタイム」である．競技成績としてはこのリザルトタイムが使用される．1回の走行あたりの時間は走行と難所攻略合わせて2分以内である．この時間内でいかにボーナスを獲得するかが重要となる．2019年度はブロックビンゴという課題を設定した．図-7はブロックがセッティングされた状態である．本課題では3×3のマスと左上に設置した数字カードを用いる．大きく2つのボーナス獲得方法がある．1つは線分の交点に置かれている赤・青・緑・黄のカラーブロックを動かし，同じ色のマスの中の円（ブロックサークル）に移動させて，縦横のビンゴを作るというものである．ビンゴは最大4つまで作成でき，ビンゴの数が多いほど大きなボーナスを獲得できる．もう1つは左上の数字カードを読み取り，黒ブロックをその番号に指定されたブロックサークルに運ぶというものである．どちらの課題もコース内のブロックの現在位置を認識してルートを判断する必要がある，そうしないと動かすべきでないブロックまで動かしてしまうためである．時間も限られているため，できるだけ短い経路を

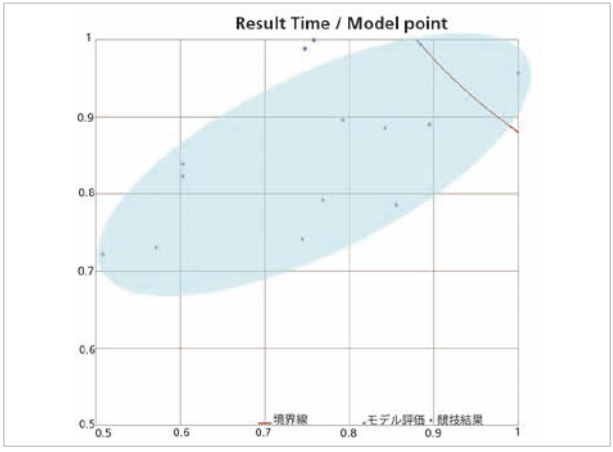


図-5　総合成績の算出（2019年CS大会より）

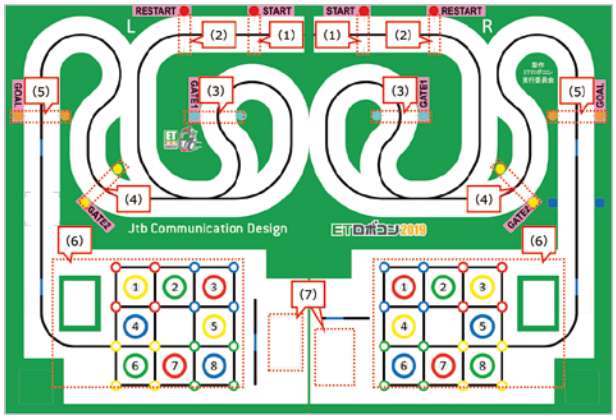


図-6　2019年コース（アドバンストクラス）

通る必要がある．こうした情報をどのように持ち，どう経路を作り出しているかはモデル審査上でも重要なポイントである．また，もう1つ重要な要素がある．それはブロックの色の判定や数字カードの読み取りである．ブロックの色と数字はスタート直前にランダムに決められる．スタート前に人間が指示を与えることはできないため，ロボットを含む走行システムで自律的に判断する必要がある．このため，コース内には据え置き型のカメラを設置している（図 -8 左）．参加チームはカメラとPC を接続し，PC 側で取得した画像（図 -8 右）を AI などで解析し，その結果をロボットに送るといった構成が必要となる．

競技の狙い

これまでの ET ロボコンではロボット単体で攻略できる競技課題が多かった．2019 年はカメラによる画像処理などを前提とした競技課題を提供した．これはさまざまなものがつながることが前提となりつつある AI/IoT 時代において，組込みソフトウェアエンジニアもさまざまなシステムを使うことが必要になると考えたためである．その結果，参加チームはブロックの色検知にブロック配置前後の画像差分，数字カードの認識には機械学習といった技術を取り入れていた．大会後のアンケートでも今回の ET ロボコンで初めてこうした技術に取り組んだというチームが多数あった．図 -9 はモデルシートに記述された画像処理の例である．

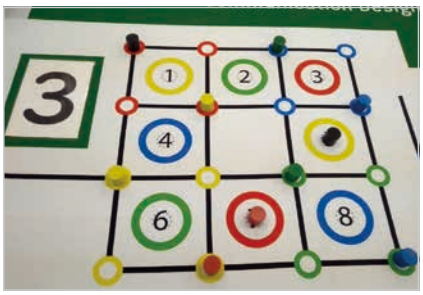


図 -7　ブロックビンゴ

図 -8　カメラ（左）取得される画像（右）

ET ロボコンの成果と課題

以上説明してきたとおり，ET ロボコンでは組込みソフトウェアの開発スキルを習得するための各種の取り組みを行っている．参加者アンケートでも 73% がモデリングを学ぶことができたと回答しており，ほかにもプログラミング（55%），開発プロセス（33%）を学べたとの回答があった．実践を通じてソフトウェア開発に必要なスキルを向上できていると言える．しかし，近年では参加者数が減少傾向にある．働き方改革により企業では使える工数が少なくなっているというコメントも多く寄せられている．こうした声に応え，2019 年はコースを左右対称にすることで L/R の課題を共通化して作業量を減らすとともに，2 回の走行のうちの良い方を競技成績として使うよう変更した．競技の負担が減った分，モデルのレベルも上がっている．しかし，今後も工数対効果は厳しく問われることが予想される．新しい技術を取り入れながら，どう全体をバランスさせるかが今後の課題と言える．

（2020 年 1 月 19 日受付）

土樋祐希　Yuki.Tsuchitoi@fujixerox.co.jp
1997 年富士ゼロックス入社．複合機のソフトウェア開発に従事し，モデル駆動開発環境の立ち上げに携わる．2010 年から会社の ET ロボコン参加を推進し，2015 年に本部審査委員となる．2018 年より本部審査委員長．

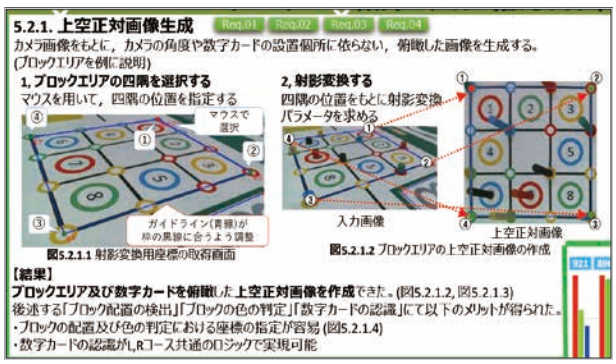


図 -9　画像解析の例

［ETロボコン：異色の情報系ロボコン ― 光る若手にインタビュー ―］

② KAMOGAWAの訓練生にインタビュー

小西康介　内田賀子
神原太朗　竹歳留加
京都府立
京都高等技術専門校

（聞き手）平山貴司
岩手大学

本稿では，ETロボコン2019のデベロッパー部門アドバンストクラスにおいて競技3位・若手奨励賞に輝いた「KAMOGAWA」の代表4人に，ETロボコンへの取り組みについて尋ねていきます．紙面の都合上，質問の「～について，教えてください」は，「～について」と短縮しています．

―ETロボコンに参加することになったきっかけについて．

ロボットを動かしたい，技術の勉強がしたい等の理由は各々ありますが，「在校中に何か実績を残したい」という思いが，ETロボコンに興味を持ったきっかけです．

私たちの在籍する京都府立京都高等技術専門校システム設計科は，実務を想定した情報技術の課題に取り組んでいます．その課題の1つにETロボコンがあります．ETロボコンを通して開発の上流工程から下流工程まで体験すること，納期に向けてチームでプロジェクト管理を実践することが目的です．2017年にはプライマリークラスで関西地区大会3連覇と全国優勝を達成しました．その翌年の2018年にはアドバンストクラスに出場し，関西地区大会で準優勝しました．先輩たちの実績からETロボコン参加への思いを強くし，アドバンストクラスでのチャンピオンシップ大会総合優勝を目標にチームを結成しました．

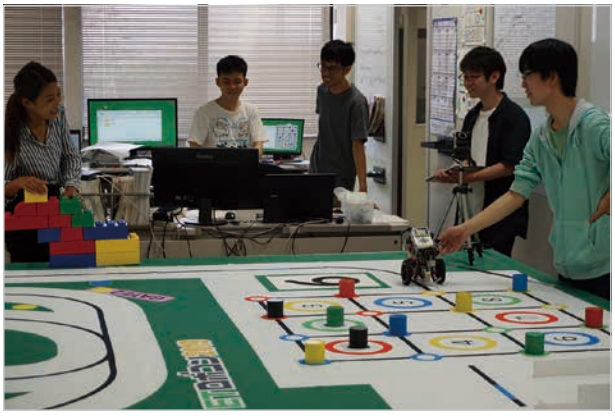


図-1　校内のコースで走行テストする様子

―代表4人の皆さんが担当したところについて．

小西：プロジェクト管理とモデル作成を担当しました．モデル作成では，私たちが考えた内容をいかに分かりやすく伝えるかを検討しました．

内田：ブロックビンゴエリアでのロボットの走行経路を算出する経路探索プログラムの開発を担当しました．私たちの想定する経路は数十万通りあり，その中から制限時間内に最適解を算出することに苦心しました．

神原：Webカメラでブロックの色と配置，数字カードを認識する画像認識プログラムの開発を担当しました．経路探索プログラムはこの認識結果を前提に動作するため，特にロバスト性を意識して試行錯誤を重ねました．

竹歳：ロボット制御に関する開発を担当しました．ゴールまでの走行やブロックビンゴでの基本動作の開発，ショートカットのルート作成等に取り組みました．

―ロボットの制御について．

ロボットのハードウェアは改造が認められていません．また，ロボットはレゴのパーツで組み立てるので，モータやセンサには個体差や照明などの外部環境が走行に大きく影響します．そういったハードウェアの特性や環境の変化に対応できるソフトウェアを開発しました．ハードウェアの性能が限られていたからこそ，その中で安定して走行する方法を考えることができたと思います．

―スピード競技について．

地区大会では確実にチャンピオンシップ大会の出場権を獲得するために，スピードよりも安定性を重視しました．一方，チャンピオンシップ大会では競技1位を目指すため，安定性よりもスピードを追求しました．より速度を上げ，モータの回転数の限界値を超えないように緩やかに曲がるショートカットや高速走行でのライン復帰を実装しました．これらにより全国トップレベルのスピードを実現できました．

―ボーナス課題のブロックビンゴについて．

地区大会終了の時点で，私たちのチームは制限時間の120秒以内にクリアできていないものがありました．しかし，ライバルチームの中にはすべてのボーナスタイムを獲得しているところもあり，チャンピオンシップ大会で戦うには全ボーナスタイム獲得が絶対条件でした．ロボットがスタートからブロックビンゴエリアに到着するまで約30秒かかるため，残りの90秒でブロックビンゴとガレージ停止をすべて終える必要があり，繰り返しテストすることでスピードと安定性の落としどころを見極めていきました．

テストを行うにあたり，全地区大会で実際に出題された初期配置を映像で確認し，両コース合わせて約100パターンを洗い出しました．それをもとに制限時間内に全ボーナスタイムを獲得する成功率を高めていきました．

ところが，チャンピオンシップ大会の1走目で予期せぬ動作をし，コースアウトしてしまいました．ピットに戻りログデータを確認したところ，地区大会には現れなかった初期配置を引き当てていたことが分かりました．リスク分析を行い，本番を想定したシミュレーションを繰り返し行っていたことで，1走目の失敗に焦ることなく2走目に臨み，完全攻略できました．また，1走目の失敗があったからこそ2走目の全ボーナスタイム獲得を達成したときの喜びもより一層大きなものになったと思います．

―カメラ画像による認識について．

最も苦労したことは，ブロックの色認識が照明環境によって大きく左右されることでした．校内のテストでは成功していたものが，地区大会前の試走会で誤認識するトラブルが発生しました．その後，試走会と校内のログデータを比較し，色認識に用いる色相・明度・彩度の範囲や判定の順序等を見直しました．試走会での失敗から学び，ロバスト性を向上させたことで，地区大会，チャンピオンシップ大会では正確な色認識を実現しました．

―モデル図について．

完成度を高めるために意識していたことは，できる限りレビューを行い，多くの意見を聞くことです．全員のメンバがモデルを作成するのは初めてだったこともあり，できるだけ多くの意見をフィードバックすることが重要と考えていました．校内で4人の先生に繰り返しレビューをお願いするだけでなく，ETロボコン主催の勉強会に積極的に参加し，実行

図-2　チャンピオンシップ大会でブロックビンゴを攻略する様子

委員の方々にもレビューをお願いしました．勉強会で具体的なアドバイスを得るため，提出締切の 2 カ月前までにモデル全体の 80％を完成させることを目標に取り組みました．また，地区大会終了後にもモデルを持参し，実行委員の方々に積極的にアドバイスを聞いて回りました．たくさんのレビューを受けることで自分たちでは気づかなかったことに気づき，そのつどモデルに反映させることで，完成度を高めていきました．

―ET ロボコンを通じたスキル向上について．

設計や開発等の技術的なスキルが向上しました．しかし，それ以上にチームで働く力が身に付きました．今回の結果は，このメンバでなければ絶対に到達できませんでした．メンバにはそれぞれ長けた能力があり，それが上手く掛け合わさったことで結果につながりました．チームの目標を実現するための自分の役割を考え，主体性を発揮し率先して働きかける力は，これから仕事をする上で必ず活きると思います．

―全体を振り返って，辛かったこと，楽しかったこと．

地区大会の試走会では，想定していた走行がまったくできず，ブロックビンゴエリアに到達する前にコースアウトするというトラブルが起きました．何より悔しいことは，メンバが長い時間をかけて取り組んでいたものが発揮できずに終わってしまうことです．また，問題に直面したとき，チーム内で意見の食い違うこともあり，苦しい思いもしました．それでも，チームで 1 つの目標に向かって，課題を 1 つ 1 つ自分達で解決していく，その過程は楽しいものでもありました．多くの失敗を経験し，悔しい思いをしましたが，最後にチャンピオンシップ大会では実力をすべて発揮できたことにチームで喜びを分かち合いました．

―皆さんの次の若い世代に向けて，メッセージをお願いします．

ET ロボコンを経験して最も感じたのは，人との繋がりの大切さです．勉強会や大会でのライバルチーム，実行委員の方々との交流は貴重な経験になりました．私たちが成果を出せたのはたくさんの人の協力があったからです．そして何よりも，同じ想いを共有し，1 つの目標に向かって打ち込めるメンバに出会えたことはかけがえのない財産です．次の若い世代の皆さんにも，人との繋がりを常に意識して課題に取り組んでほしいと思います．

―ありがとうございました．

KAMOGAWA は，競技において驚異的なリザルトタイム（競技点）を叩き出し，会場を湧かせました．専門校で 1 年間毎日のように取り組んだ成果です．光る訓練生たちの社会での活躍に期待です．

（2020 年 1 月 19 日受付）

図 -3　チャンピオンシップ大会表彰式の様子

小西康介，内田賀子，神原太朗，竹歳留加
京都府立京都高等技術専門校に在籍する 5 人でチーム「KAMOGAWA」を結成する．ET ロボコン 2019 デベロッパー部門アドバンストクラスに出場し，チャンピオンシップ大会で競技部門 3 位，若手奨励賞を受賞する．

平山貴司（正会員）　hirayama@cis.iwate-u.ac.jp
1999 年群馬大学大学院工学研究科博士後期課程修了．2001 年より岩手大学理工学部講師．ディジタルシステムの自動設計の研究に従事．

［ETロボコン：異色の情報系ロボコン ― 光る若手にインタビュー ―］

③ がんちゃん+Xの学生にインタビュー

海沼滉樹　佐野祐輔
槇　翔史　山内大七洋
岩手大学大学院

（聞き手）平山貴司
岩手大学

本稿では，ETロボコン2019のデベロッパー部門アドバンストクラスにおいてTOPPERS賞を受賞した「がんちゃん+X」の代表4人に，ETロボコンへの取り組みについて尋ねていきます．紙面の都合上，質問の「～について，教えてください」は，「～について」と短縮しています．

―ETロボコンに参加することになったきっかけについて．

私たちが所属する研究室が，数年前からETロボコンに参加していたことがきっかけでした．私たちは学部4年生だった2017年から岩手大学チームとしてETロボコンに参加していました．当時の主要メンバは大学院生で，学部メンバはその補佐といった形でした．また，プログラムの開発やモデルの作成にかけられる時間も少なく，特にモデルの知識が不足していたこともあり，地区最下位という散々な結果に終わりました．2018年から社会人エンジニアとの連携チームとなり，ETロボコンに携わる時間が増え，チームの技術力も急上昇しました．

図-1　活動中のメンバの様子

―代表4人の皆さんが担当したところについて．

海沼：スピード競技[☆1]の開発・調整を担当しました．ロボットの制御は会場の照明環境に大きく左右されるため，調整には非常に苦労しました．

佐野：スピード競技の開発・調整を担当しました．乾電池の残量によってロボットの挙動が変わるため，最高電圧での動きに合わせた調整に非常に苦労しました．

槇：スピード競技のプログラムを担当しました．特に後輩メンバの指導や他のメンバが書いたプログラムの細かな修正などに力を入れていました．

山内：分析モデルの作成を担当しました．自分たちがどのように競技を攻略しようとしているかを，分かりやすく正確に伝えるように努めました．

―ロボットの制御について．

ETロボコンは一般的なロボコンとは違い，ロボット本体は全チーム統一で改造することができません．さらに，ロボットはレゴのパーツで作られるため，モータやセンサの個体差や照明環境に大きく左右されるという難しさがあります．そのため，ソフトウェアでいかに工夫し制御するか，あらゆる環境に対応できるようなロバスト性の高いプログラムを作ることが求められます．

☆1　START から GOAL までの走行．

毎年継続して参加し，引き継ぎをきちんと行ってノウハウを蓄積できているチームが，全国上位の成績を収めています．私たちのチームも約半数のメンバが数年間継続して参加してきたことで，全国上位の成績を収めることができました．

また，特に学生メンバは制御工学が専門ではなく，参加当初は素人同然でしたが，実際に開発をして試行錯誤を繰り返すことで感覚を養い，全国上位チームになるまでの技術を身につけることができました．それでもチャンピオンシップ大会では失敗してしまい，まだまだ詰めが甘かったと悔やんでいます．

―スピード競技について．

スピード競技で好タイムを獲得するためにはライントレースのみではなく，コースのショートカットが重要となります．その一方で，コース上には障害物が置かれ，その位置は本番当日まで非公表というルールがあるため，決まったルートに絞って作り込むことができない制約があります．これに対処するため，複数パターンのショートカットを開発しました．ただし，使える可能性のあるショートカットパターンのすべてを作り込むことはできないので，過去のチャンピオンシップ大会や地区大会での障害物配置を分析し，本番で使えそうなルートに絞り開発を行いました．本番では安全性のため，控えめなショートカットしか披露できず残念に思っています．

また，走行スピードにはバッテリ電圧が大きく影響する[☆2]ため，本番で使用する最高電圧の状態は新品の乾電池でも一度しか走らせることができません．私たちのチームでは地区大会までに約400本，チャンピオンシップ大会までに約200本の単三乾電池を消費しました．

―ボーナス課題のブロックビンゴについて．

私たちのチームの走行速度とブロックビンゴの制限時間を考慮した結果，「ダブルビンゴ」というボーナスを達成する目標を立てました．ダブルビンゴを達成するために必要なブロックの移動順序を検討したところ，高々30パターンしかないことを突き止めました．30パターンの中から最適な経路を算出し，どのような初期配置でも私たちのチームの目標を確実に達成できるようソフトを実装しました．

地区大会やチャンピオンシップ大会に向けて，どのような初期配置でも目標を達成できるように，およそ200パターンの初期配置でテストとデバッグを重ねました．とても地道な作業ではありましたが，予期しないバグを発見することが何回かあり，実際の環境でテストを行う大切さを実感しました．その結果，チャンピオンシップ大会ではチームで立てていた目標を達成することができました．

―モデル図について．

モデル図の作成に必要なUMLの文法は，参考

☆2 全チーム共通バッテリで，競技が始まると交換することができない．

図-2　TOPPERS賞受賞時の様子

図-3　チャンピオンシップ大会でブロックを運搬している私たちのチームのロボット

書を用いて一から学びました．文法を学ぶこと以上に，ソフトの静的な構造を示したければクラス図，各クラスの振舞いを示したければステートマシン図というように，伝えたい事柄に合わせた図の選択が難しいところでした．

2019 年の大会テーマは「EDGE を極めろ!」であり，画像処理や AI が重点技術となっていました．私たちのチームでもカメラシステムによる画像処理を採用していて，ブロック情報の読み取りや数字カードの数字の読み取りをモデル図に重点的に記載しました．また，競技進行中に異常が発生してしまった場合でも可能な限り競技を継続できるように，さまざまな観点から異常処理を検討しているのが私たちのチームのモデルの強みです．

モデルの品質をより高いレベルにするには，より多くの人数でレビューを繰り返すことが大事です．私たちのチームもメンバ全員でレビューを繰り返し，用語の統一や細部のレイアウトまで修正を行いました．レイアウトの修正を専門としたメンバがいたほどです．もう 1 つ，規約をきちんと読み込むことが大事です．モデル審査のポイントについては，ET ロボコン実行委員会からあらかじめ規約で提示されています．ソフトの長所をアピールすることは最も重要ですが，何が求められているかを理解することも必要です．

― ET ロボコンを通じたスキル向上について．

ET ロボコンを通じて，チーム開発のスキルが向上しました．チーム開発では，単に個々人の能力が高いだけでは良いものを作ることはできません．メンバ間で足並みを揃えることが重要になります．活動を始めた当初はメンバ間に技術力の差が大きく，意思疎通も図ることができませんでした．それでも，社会人の方にプログラム開発やモデルの書き方などについて技術指導をしていただくことで，チーム全体の技術力を向上させ，足並みも揃えていくことができました．一方，メンバによって担当する仕事の量に偏りがあったり，なかなかスケジュール通りにいかず，徹夜で作業することになったりなど，難しい面も多々ありました．社会に出てからは，チーム開発が主になってきます．チーム開発のスキルのみならず，今回の活動で培った経験を活かしていきたいと考えています．

―全体を振り返って，辛かったこと，楽しかったこと．

ロボコンでの活動全体を振り返って，自分たちが開発したプログラムによって良い結果を得られたときに最も喜びを感じました．私たちのチームは，2 月の半ばからおよそ 9 カ月を開発に費やしてきました．基本的に毎週土曜日の活動でしたが，チャンピオンシップ大会直前には夜遅くまで開発したり，休日返上で調整したりと，たくさんの苦労がありました．また，社会人との連携チームということで，かけられる時間の違いや考え方の違いなどのすり合わせにも苦労しました．苦労が大きかった分，本番でうまくいったときの達成感も大きかったです．

―皆さんの次の若い世代に向けて，メッセージをお願いします．

ET ロボコンに限らず，こういった長期間のチーム開発にはモチベーションの維持が大切だと感じます．開発ではうまくいかなかったり，時間を取られたりと大変な面も多くあります．開発に行き詰まったときには，一人で抱え込まずに周りのメンバに相談したり，息抜きに別のことをしたりするとモチベーションを維持し続けることができると思います．

―ありがとうございました．

がんちゃん +X は，TOPPERS 賞受賞に加えて，総合成績でも 4 位と健闘しました．学業の合間を縫って取り組んだ成果です．光る学生たちの社会での活躍に期待です．

（2020 年 1 月 19 日受付）

海沼滉樹，佐野祐輔，槇　翔史，山内大七洋
ganchan-plus-X-2019@kono.cis.iwate-u.ac.jp
岩手大学大学院に在籍する上記 4 人と，学部生，教員，社会人が集い，がんちゃん +X を結成する．ET ロボコン 2019 デベロッパー部門アドバンストクラスに出場し，チャンピオンシップ大会で総合 4 位の成績を収め，TOPPERS 賞を受賞する．

平山貴司（正会員）　hirayama@cis.iwate-u.ac.jp
1999 年群馬大学大学院工学研究科博士後期課程修了．2001 年より岩手大学理工学部講師．ディジタルシステムの自動設計の研究に従事．

解説
Article

準委任契約はアジャイル開発を促進できるか

―アジャイル開発導入に躊躇する発注側の課題―

秦泉寺久美 | 日本電信電話株式会社　NTT ソフトウェアイノベーションセンタ

ディジタルディスラプションの時代に発注側企業でアジャイル開発が流行らない理由

なぜアジャイル開発が流行らないのだろうか．ディジタルディスラプションによって新興の企業が老舗の企業よりも安価に同様のサービスを実現できる時代が到来し，老舗企業の収益構造の見直しが喫緊の課題となっている．新しいサービスを早く市場に充て，早くフィードバックを得，早く顧客を獲得していく必要がある．必要最低限の機能（MVP：Minimum Viable Product）を短期間の開発[☆1]にて積み上げていくアジャイル開発はソフトウェア開発によるサービス実現の手段として旧来主流であったウォータフォール開発に比べて格段にフィットすると考えられている．日本でもアジャイル開発を活用したという有志によるさまざまなカンファレンスが開催され，登壇するにも倍率が高く，聴講するにもチケットはすぐ売り切れるという盛況ぶりである．アジャイル開発への興味は皆あるのだ．しかし，このような状況にもかかわらず，アジャイル開発が所属企業およびグループ会社でなかなか推進できないのはなぜだろうか．発注側の会社としてアジャイル開発の活用が進まない理由を考えてみた．

- 年間計画をもとに予算を計画通りに使いきる文化なので，そもそも計画を逸脱することを是とするアジャイル開発は馴染まない
- 内製もしくは受託開発にてアジャイル開発を行う十分なスキルセットがない
- 開発者の現場への張り付きを考えると，受託側の単金（作業時間当たりの費用）の高止まりが予想され，アジャイル開発が従来手法に比較して生産的な開発なのかが見極められない
- 発注側で運用されている諸制度がアジャイル開発に適用できない

1番目の課題は根が深い．企業の在り方そのものを再考する必要があるので，本稿では触れない．2番目の課題は，発注側企業がソフトウェアの完成責任をすべて自社で持つという覚悟の下，アジャイル開発人材育成を組織的戦略的に実施する必要があり，今しばらく時間がかかりそうだ．一方，3番目の課題は，筆者の企業ではトライアルを通じ仮説検証がなされ，作業単金の高止まりがあったとしてもアジャイル開発の方が生産性が良い可能性が見え始めている[1)]．

では，4番目の課題はどうであろうか．受託でのソフトウェア開発では契約形態が何であれ，あらかじめ決められた要件や作業に対して対価を払うことを前提にしている．この前提をもとに，企業は周辺の法制度を遵守するために厳格な内部統制の下，運用設計をしている．具体的には発注側企業は受託会社への利益供与，買いたたき，偽装請負等を回避す

☆1 アジャイル開発の代表的な手法である“スクラム”では，短期間の開発を“スプリント”と呼ぶ．

るためにさまざまなタイミングでチェック体制を敷いている．しかし，この前提がそもそも成り立たない場合，すなわち，要件や作業が契約開始時には明確には決まっておらずフィードバックによって常時変化する場合，これまでと同様な運用が可能だろうか．おそらく，どの発注側の企業も躊躇するはずである．つまり，厳格に設計された制度運用の中で，想定外の状況を許容するアジャイル開発を導入するには大きな障壁があるのだ．それ故，開発担当者がいくらアジャイル開発の経験を蓄積しても，特例，トライアルの範疇を出ず，全社的に推進していこうという機運にならない．本稿ではこの課題にフォーカスし，一現実解について解説する．

契約形態の課題

ソフトウェア開発を受託で行う形態としては民法における請負契約，準委任契約と労働者派遣法における派遣契約の 3 つがある．

なぜ派遣契約が採用されないか

発注側企業にとっては形式的には派遣契約が一番アジャイル開発に親和性が高いとされている．しかし，受託会社にとっては，社員の稼働貸しに終始し企業の将来的な発展につながらないので，（すでに SI[☆2] を生業としている受託会社にとっては）派遣契約を選択することを渋る傾向がある．また，グループ企業派遣の 8 割規制など，親会社子会社間で派遣できる人数が労働者派遣法で制限されているため，上限に達してしまい契約を締結できない場合がある．また，前章でも述べたが，発注側のアジャイル開発スキルセットが相応にならない限り，派遣契約が締結できても，プロジェクトは回らない．派遣契約は，受託でのアジャイル開発の促進という意味では，意外にも実効的ではない契約である．

☆2 システムインテグレーション．

請負契約が馴染まない理由

請負契約では要件が確定していることが契約の前提となるため，そもそも一契約でアジャイル開発をすることには向いていない．複数回契約を締結する場合，契約に要する稼働増を無視できない（スプリント期間以上に契約締結処理に期間を要しかねない）．仮にできたとしても，頻繁に上がってくる要求と瑕疵の切り分けと対応を迅速にすることが困難であることが予想される．これは発注側にとっては大問題である．また，受託側にとっても，何が何でも期限内に瑕疵を切り分け修正するためには瑕疵対応のための稼働を期間内に別途捻出せざるを得ない．請負契約でアジャイル開発をすることは発注側受託側双方にとって非常にリスクが大きい契約なのである．

準委任契約は解決策になるのか

生産物に対価を支払う請負契約に対して，準委任契約は作業時間に対して対価を支払う契約で，受託側に生産物の完成責任，瑕疵責任はない．ソフトウェアの完成責任，瑕疵責任は発注側企業にある．発注側にとっては相当の覚悟が必要であり，逆に言えば，「1 億円かけて何もできなくても文句が言えない可能性がある」契約であり，さらに，単に受注側の稼働を確保しているととられかねない偽装請負の疑義を持たれる可能性のある，リスクが高い契約なのである．ここ 2，3 年前までソフトウェア開発において準委任契約を事実上採用していなかった発注側企業も多いのではないだろうか．筆者の所属企業も例外ではない．

とはいえ，発注側のスキル不足，受託側の都合で締結しにくい派遣契約やそもそもアジャイル開発が馴染まない請負契約に比較して，準委任契約は発注側が成果物に対してすべての責任を取るという覚悟の下，法制度を遵守できる運用設計をすればアジャイル開発を推進していける可能性がある．

すなわち，抜本的な解決策ではないものの，途上解としては有用と思われる．以上により，本稿では，

準委任契約（改正民法における「履行割合型」の準委任契約）を前提に話を進める．

契約周辺の法制度遵守にかかわる課題

図 -1 にアジャイル開発とウォータフォール開発の定義をする．ウォータフォール開発は最初に要件（インプット）が確定し，要件に対するアウトプットとしてソフトウェアが生産される開発である．一方，アジャイル開発は，この一連のインプットとアウトプットがごく短期間に繰り返される開発と定義する．頻繁なリリースに対するフィードバックによって要件が進化していく．開発チーム（受託側）とプロダクトオーナ（発注側）は密なコミュニケーションによって次の要件を選択し詳細化していく．まとめるとアジャイル開発は以下の特徴を持つ開発であると定義できる．

- ソフトウェアの継続的デリバリ
- フィードバックによる要件進化
- 密なコミュニケーション

なお，本稿で述べる契約運用設計はスクラムを想定しており，デイリーリリースが求められる場合には対応できないことに留意されたい．

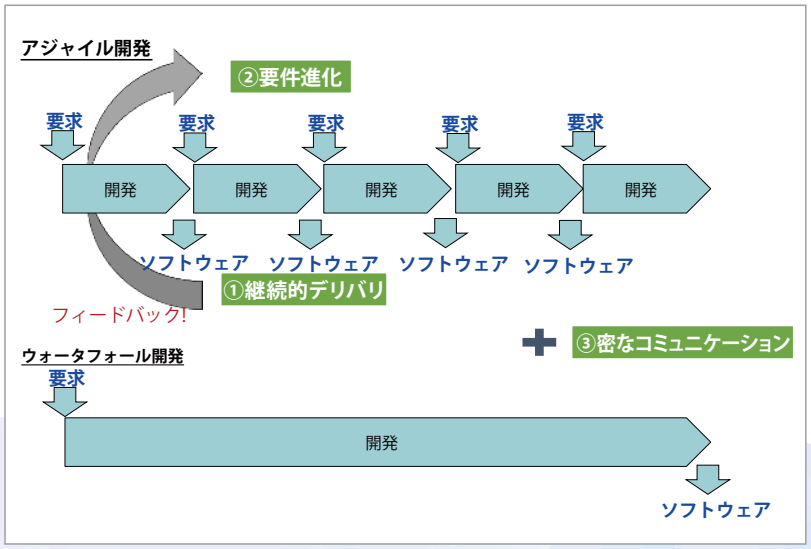


図 -1　アジャイル開発とウォータフォール開発

発注側が留意する主な法制度

準委任契約に限らず日本のソフト開発で大きな比率を占めている請負契約においても，発注側企業に共通的に留意する必要がある法制度的な観点をいくつか紹介する（ただし，すべてを網羅しているわけではない）．

- ソフトウェアの適切な資産化（税制）
- 適切な作業指示と期間内の支払い（下請法）
- 偽装請負リスク回避（労働者派遣法）

1 番目の観点では，納品されたソフトウェアをさらに事業等に使う場合，実体を固定資産化（以降，単純に資産化と表記）し，固定資産税を支払う必要がある．資産価値はソフトウェアの発注費用以外にも発注側の労務費を合わせて計上する必要がある．

2 番目の観点では，買いたたきや支払い遅延によって多大な影響を被る財務体力の弱い受託会社を保護するために，下請法にて規制されている [2]．違反すると受注側企業の死活問題になるだけでなく，「弱者いじめ」として発注側の社会的な責任が問われる．そのため，下請法対象案件と対象外の案件が混在する場合は対応漏れリスクを考慮して，全契約を下請法対象として扱う場合もある．　3 番目の観点では，作業責任者への作業指示や受託側での勤務管理の徹底などの枝葉が注目されがちだが，本質は，本来なら派遣契約で実施すべきところを請負契約や準委任契約（両者をまとめて法律的に「請負」と記載）で実施すると“請負を偽装している（いわゆる「偽装請負」）”として，労働者派遣法に抵触するという点である [3]．

なぜアジャイル開発だと対応が困難になるのか

元々ウォータフォール開発による請負契約を想定した法制度遵守のための運用が，アジャイル開発の場合は適用

できなくなる場合がある．それはなぜか．ウォータフォール開発の場合は，資産化，作業指示，支払いは１契約に対して原則１回である．一方，アジャイル開発はこれらのプロセスが開発期間に何度も生じることになる．このため，ウォータフォール開発を想定した運用ではアジャイル開発に対応できないのである．アジャイル開発を推進していくためには，適切な契約形態をベースに外部監査にも耐えられる運用を内部統制に則って設計することが重要である．つまりトップダウン的なアプローチが必要である．

準委任契約でアジャイル開発を推進するためには

図 -2 に留意すべき法制度をアジャイル開発の特徴に関連付けて示す．まず，ソフトウェアが継続的にデリバリされることは，そのタイミングでの適切な資産化がされなければサービスに利用できない，ということを意味する．そのためには，デリバリのタイミングで受託側から作業終了報告書を受領し，受託会社への支払い額を確定させ，発注側の労務費を合わせて資産として計上することが必要である．

第２に，顧客や市場からのフィードバックを受けて，いわゆる請負における瑕疵対応も含めて頻繁に要件が進化する点については，新たな要件が追加になるたびに，適切な作業指示を支払い期限とともに発注書面として発注側企業から発行することが必要である．そして，期限内の支払いを確実に実施する．支払い期限は下請法では給付より 60 日以内としている．給付をどのタイミングとして規定するかによって支払い期日がウォータフォール開発と異なる場合があることに留意する．

第３にコミュニケーションであるが，一般的に偽装請負リスク回避で言われている受託側作業責任者への作業指示はもちろんのこと，そもそも派遣契約の方が適切であるとの疑義を持たれないことが重要である．第２の特徴で述べた都度の作業指示と作業指示に対する作業時間の合意，作業実績に基づく支払い額の確定をすることが重要である．

法制度を遵守するための契約スキーム例

これらの点を考慮し，契約の運用を設計し，契約スキーム化する．契約書は契約条件を条文化したものであるが，契約スキームを反映する必要がある．

図 -3 に筆者の組織で実施した法制度遵守を盛り込んだ契約スキームを一例として示す．準委任契約をベースとしており，１回の開発にあたって１契約を締結し，一定の期間ごとに「個別業務」を規定する．要件の進化と継続的デリバリに対する対応は個別業務ごとの「個別業務指示書」によって作業指示を行い，それに対応する「作業終了報告書」に作業実績の報告を受け，それに対する支払いを繰り返すことで対応する．個別業務指示書と作業終了報告書を便宜上１枚の様式として「個別業務指示書兼作業終了報告書」として運用することも可能である．

フローをさらに詳細に見てみよう．文献 4）にあるように１回の開発期間に複数回の個別契約を締結するものと異なり，本スキームの契約締結回数は１回であるので，契約にかかる稼働・

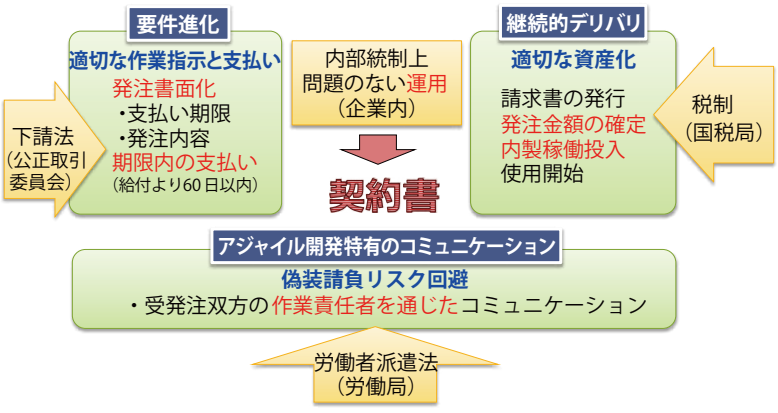


図 -2　アジャイル開発と関連法制度の俯瞰図

期間は従来型と変わらない. 各個別業務の指示は「個別業務指示書」の中でバックログの粒度で行われる. 個別業務指示の合意は文献 4）でも提案がある「連絡調整会議」と呼ばれる発注側受託側の作業責任者を交えた会議にて合意される. 個別業務指示書は下請法の三条書面を兼ねており, 発注内容（作業内容）, 支払い期限などの情報が過不足なく記載される（言い換えると, 個別業務指示書が下請法三条書面として機能するような体裁であることが望まれる）.

作業期間が満了し個別業務が終了すると,「作業終了報告書」が受託側から発行され, 個別業務指示書で指示された作業に対して作業実績が記載される. この作業実績にあらかじめ契約書で合意している作業単金を乗じた金額が発注側から受託側に支払われる. 個別業務で指示される内容は, 機能構築作業だけでなく不具合修正や環境構築など, すべての作業が含まれる. 支払い額が確定したらこれらを内製稼働分と合わせて資産計上する.

すなわち, 個別業務単位に作業指示, 支払い, 資産化がなされる. 個別業務をスクラムにおけるスプリントと呼びかえれば, スプリント単位で要件の進化に対応し, スプリント単位で継続的にデリバリされたソフトウェアのサービス導入が法制度を遵守した上で可能となる.

ただし, 支払いの期限については, 筆者の所属組織では, 個別業務開始日から給付があると考え, ここを支払い期限の起点とする運用をして, 最大限のリスクヘッジをしている（図 -4 参照）. 請負契約などは「納品物の引き渡し」を「給付」と誰もが解釈できるが, 準委任契約は何をもって給付とみなすか, 意見が分かれるところだ. 筆者の所属組織のような運用の場合は, 個別業務開始から 60 日以内（約 2 カ月以内）の支払いが求められるため, 発注側の支払い処理の稼働期間を考慮すると, 個別業務（もしくはスプリント）の期間は長くても 4 週間（約 1 カ月）程度になる. 図 -4 に個別業務完了日に給付があるとした場合との比較を示した. 後者の方が支払い期限に余裕があることが分かる.

契約書には何が書かれるのか

契約スキームが決まったら, 契約書の雛型を作成する. 表 -1 に契約書条文項目例を示す. 契約書は契約スキームを反映した契約条件とそれ以外の契約条件に分類できる. 契約スキームを反映した部分は契約期間, 作業単金, 契約金額の上限, 支払いの期日などが明示される. その他の契約条件（著作権, 損害賠償, 不可抗力など）は受発注双方で合意の上, 契約書条文として書かれる.

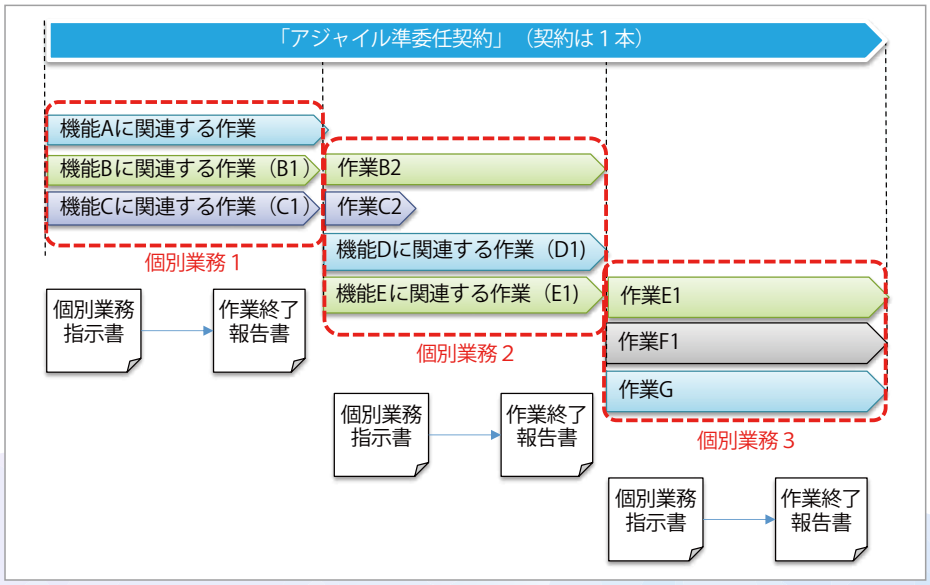


図 - 3　契約スキーム

より迅速な契約締結, 支払いのために

契約書が合意できたら, いよいよ契約を締結するわけだが, 契約から支払いまでを電子的に実施することが重要である. 特に支払いは従来の請負契約と異なり準委任契約では 1 契約に対

して複数回実施される．システム的な紐づけが対応されていないと，案件数が増加した場合に管理稼働が度外視できなくなる．特例ではなく定常運用を目指すのであれば，契約スキームに合致した会計・契約システム変更もぜひ念頭に入れておきたい．

表 -1　契約書条文項目例

分類	説明	代表的な状況	法制度
契約スキームを反映した条件	法制度を遵守するための運用を反映	目的 全体プロジェクト 対価 作業責任者 連絡調整会議の設置 個別業務 個別業務の終了確認 請求と支払い	(基本事項) (基本事項) (基本事項) 偽装請負リスク回避 偽装請負リスク回避 下請法 下請法 下請法
それ以外の条件	運用以外の個々の条件	資料の貸与・提供 権利義務の譲渡 著作権の帰属 産業財産権 機密情報 損害賠償 解除 不可抗力 存続条件 合意 準拠法 反社会勢力の排除 個人情報保護 など	

アジャイル開発の効果と運用のアジリティは両立できるか

契約スキームや契約書を策定しても，アジャイル開発の効果と運用のアジリティ（契約手続きの機敏さ）が両立できなければ意味がない．よって，筆者の所属組織では，準委任契約によるアジャイル開発のための運用を整備し，契約書雛型を作成し，2018 年 8 月からトライアルを実施した．受託側にはグループ会社 2 社が受託側会社として参画した．

トライアルでは以下の 3 つの観点を確認した．

- 運用のアジリティ
- アジャイル開発の効果
- アジャイル開発の生産性

詳細は文献 1），5）を参照いただきたいが，運用のアジリティの観点では，トライアル 10 件を評価した結果，運用稼働は従来の請負と同程度との評価になった．支払いの回数が増加したものの，各々の検収時のプロセスが請負に対して激減したため（納品証跡作成，検査証跡作成が不要になるなど），稼働は相殺された格好になった．アジャイル開発の効果はスピード，ビジネス価値，チームビルディングの 3 つの観点とも高い評価となった．生産性につ

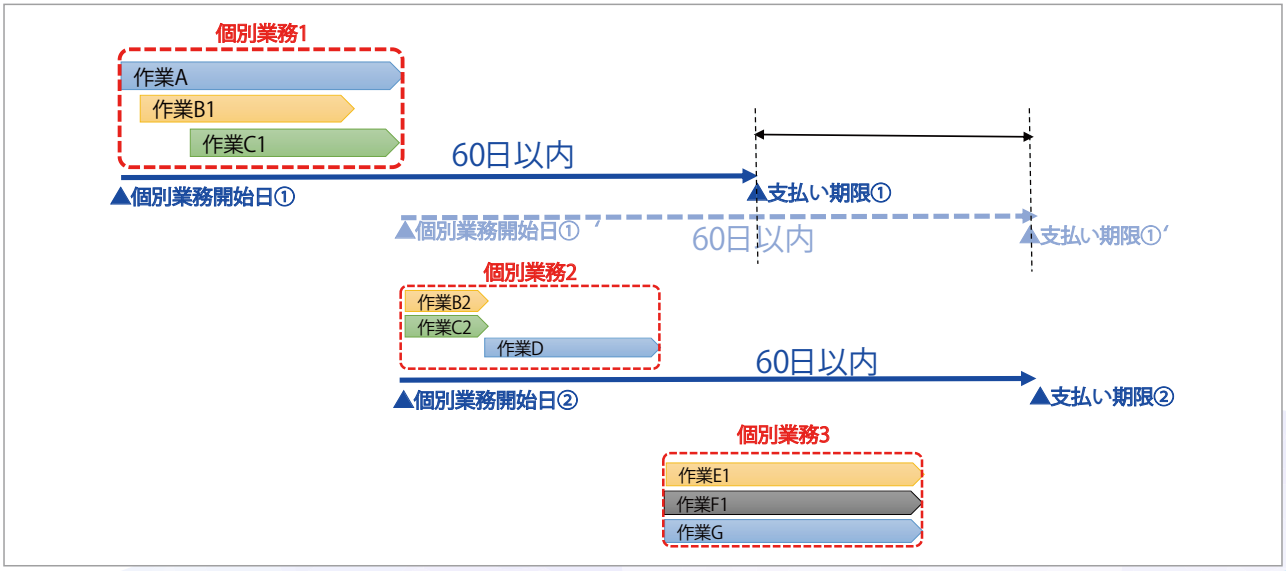


図 -4　下請法における給付より 60 日以内の支払いの考え方の例

いては，準委任の作業単金が請負の 3 割増しという結果にはなったが，機能が使われる率が 10％改善すれば総合的な費用はアジャイル開発がウォータフォール開発と同程度になることがシミュレーションから分かった[1]．アジャイル開発は MVP を積み上げるものである．ムダを極力削除する考え方がベースにあるので，条件は容易に達成できると考える．

筆者の所属組織はトライアル開始から 1 年を経過した 2019 年 7 月に前述の評価を行い，アジャイル開発の効果と運用のアジリティの両立，および生産性の見通しを得たことで，トライアル終了を待たずに次年度からの本格運用を決めた．

準委任契約はアジャイル開発を促進できるか

トライアルでの検証は我々に重要な知見をもたらしたが，それにもまして着目したいのは 2018 年 8 月から 2020 年 1 月末時の 1 年半において，さらに契約数が伸び，27 件の準委任契約が締結されたという事実である．1 月現在はまだトライアル期間ではあるが，もはや定常運用の案件数と言っても過言ではない．今後もアジャイル開発は増加していくと思われる．法制度を遵守するための運用をトップダウン的に設計し，定常運用が可能であれば準委任契約はアジャイル開発を促進できると結論付けてよいだろう．

最後に，本稿の課題設定を振り返ってみる．ディジタルディスラプションの時代が到来している事実，老舗企業は収益構造を見直さなければいけないこと，そのためにはアジャイル開発をサービス開発の核として顧客や市場に対して迅速に価値を提供し続ける必要があることを再掲する．準委任契約によるアジャイル開発はきちんと運用設計すれば監査に十分耐えられる安心安全な定常運用が可能である．つまりアジャイル開発は手段として使っていけるのだ．残る課題は，年間計画をもとに予算を計画通りに使いきる文化の見直しや，アジャイルエンジニアの戦略的な育成などアジャイルがフィットする企業の在り方に変えていくべきである，ということを最後に提言したい．

参考文献

1) 秦泉寺久美，神　明夫，夏川勝行：VSM を用いたアジャイル開発の生産性指標の提案とウォータフォール開発との比較，情報処理学会ソフトウェア工学研究会 (SE) (Dec. 2019)．
2) 経済産業省：情報サービス・ソフトウェア産業における下請法適正取引等の推進のためのガイドライン　平成 29 年改訂，2017．労働者派遣法（2017）．
3) 厚生労働省：労働者派遣・請負を適正に行うためのガイド (2015)．
4) （独）情報処理推進機構：非ウォーターフォール型開発に適したモデル契約書（2012）．
5) 秦泉寺久美，神　明夫，夏川勝行：アジャイル開発のための準委任契約制度設計と課題，情報処理学会第 85 回電子化知的財産社会基盤研究会 (EIP) (Sep. 2019)．

(2020 年 1 月 31 日受付)

■秦泉寺久美（正会員）　kumi.jinzenji.hz@hco.ntt.co.jp

1991 年早稲田大学大学院理工学研究科修士課程修了．同年，日本電信電話株式会社（NTT）入社．画像処理，符号化，通信の研究開発，ソフトウェア開発標準策定などソフトウェア工学の研究に従事．博士（国際情報通信学）．電子情報通信学会会員．

べた語義

Vol. 105

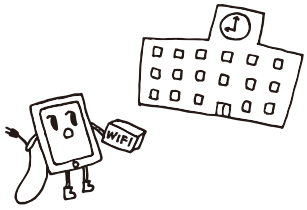
CONTENTS

【コラム】1 人 1 台学習者端末について考える… 望月 陽一郎
【解説】実践的演習を伴うサイバーセキュリティ公開講座の取り組み… 丸山 一貴・佐々木 伸彦・高谷 宏幸
【解説】再帰的思考のすすめ… 中川 正樹

COLUMN

1 人 1 台学習者端末について考える

基般



今回の 2018 年 PISA 調査の結果から読解力の低下が報道でとりあげられていますが，単なる読解力ではなく，「ディジタルの世界で求められる読解力の低さ」，つまり日本の学校における「授業において子供たちに ICT 機器を使わせる場面の少なさ」「学習者端末が少なすぎる現状」が明らかになったことのほうが重大な課題だと考えます．政府から「小学校中学校の子供たち 1 人に 1 台ずつの学習者端末を整備」の話が出てきたのは，これまでも言われてきた自治体間の整備率の差を埋めるためにはやや遅すぎるとも思えます．今の整備状況などを把握するため，学校の先生方・教育委員会の方々などを対象に「小学校中学校で使用する学習者端末」について，Web 上でアンケートを行ってみました．関心の高さからか，数日で 100 以上の回答があり，あらためて現状が分かってきました．たとえば，現在の学習者端末の整備状況については，「コンピュータ室に 40 台」しかないという回答が 34.6%，「コンピュータ室に 40 台＋教室で使う端末が数クラス分程度」が 33.6%，つまり 70% 近くが，コンピュータ室に行かなければ使う機会が少ない，ということです．この環境でディジタル情報を分析・理解し，活用する力を子供たちにつけさせようというのはやはり無理があり，だから 1 人 1 台学習者端末の整備が必要なのです．では 1 人 1 台端末が整備されたら，先生方はどのくらい子供たちに使わせるのでしょうか．アンケートの結果では，「ほぼ毎時間使わせたい」という回答が 29.0%，「1 日に数時間」が 46.7%，「1 日に 1 時間くらい」が 15.9% でした．つまり 90% をこえる人が，「毎日使わせたい」と思っている．先生方は「環境があれば子供たちに使わせたい」のです．

しかし，だからといって性急な整備，特に端末を入れることだけを考えた整備は，かえって使えない環境を生みます．これまでも「ネットに全員のパソコンをつないだら動かなくなった」という話は，学校ではよく聞いたものです．1 人 1 台端末を支える校内の高速ネットワーク，学校からネットへの太い回線，端末を充電するための電源確保など，学校という施設を大きく作り変えるくらいのことをしないと，本当に「授業で子供たち一人ひとりが端末を使う」時代は来ないのではないでしょうか．整備を担当する自治体の教育委員会の担当者がそういった俯瞰的な環境整備を構想することが必要であるとともに，外部からの適切なパッケージ提案が行われることが今一番大切なことであると思います．

望月陽一郎（大分県立芸術文化短期大学）

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

ARTICLE

実践的演習を伴うサイバーセキュリティ公開講座の取り組み

丸山一貴　明星大学
佐々木伸彦　ストーンビートセキュリティ（株）
高谷宏幸　マカフィー（株）

興味の入口としての公開講座

一般の方にとってはサイバーセキュリティというと高度に複雑であり，理解が難しく恐いものであると思われがちである．また，報道される際には事件としての側面から，個人情報漏洩の規模や被害額，責任の追及といった部分が大きく取り上げられ，技術的な側面は置いてきぼりになることが多い．そうした中，2014 年にサイバーセキュリティ基本法が成立し，セキュリティ分野の人材育成に一層注目が集まるようになった．企業では社内の人材を教育するため，サイバーセキュリティに関する演習付きの研修を外部に委託するケースが増えた．その一方で，大学では，学生向けに同様の機会を設けたり教材を準備したりするのは難しいこと☆1や，CTF（Capture The Flag）☆2のようなイベントは専門性が高く未経験者が初めに学ぶ題材としてはハードルが高いという問題があった．

セキュリティではプログラムや OS，ネットワークといった幅広い分野の理解が必要なことから，学生が自身の専門分野を活かせる可能性があることと，専門分野以外にも興味を持つことの必要性を感じてもらうことが重要である．そこで我々は，PC の操作は問題なくできるが，セキュリティについては素人である 10 代の生徒・学生を主な対象として，実践的な演習形式でその一端に触れる機会を設けようと考えた．2015 年に第 1 回を開催して以降，毎年 1 回，明星大学情報学部主催の無償の公開講座としてこれを運営している（図 -1）．2019 年のアンケートでは参加者の約 90% が「非常に満足」「満足」と回答し，後述する演習参加者に限定すると「満足」以上は 100% であった．本稿ではこの取り組みの概要と課題について述べる．

☆1　一部の学科にカリキュラムとして導入している大学は存在する．
☆2　サイバーセキュリティ技術に関する競技であり，ネットワークやバイナリ解析等の幅広い分野の技術が必要とされる．

講座の構成と参加形態

公開講座は休日午後の約 4 時間を利用して開催しており，大きく分けて 3 部からなる．第 1 部は講演として，サイバーセキュリティに関する基礎と最新情報を，その年のテーマに合わせて簡単に紹介する．第 2 部は公開講座のメインイベントである演習を行う．前半は前提知識やツール類の紹介をハンズオン形式で行い，後半は用意した課題に取り組んでチームごとの成果を競う．前半で扱う内容は，後半の課題に取り組むためのヒントを兼ねており，参加者は教材に例示されたコマンドの使い方等を参考にしながら課題に挑戦していく．第 3 部は演習内容の講評と全体の総括，質疑応答を行

図 -1　公開講座の様子

うとともに，優秀な成果を上げたチームを表彰する．

参加形態は演習参加と聴講参加の 2 種類を設定している．演習参加は，第 2 部で実際に 1 人 1 台のノート PC を使って課題に取り組むことができる．生徒・学生の優先枠を設け，2019 年は 36 名の演習参加者を募集した．演習参加者は 3 人で 1 チームを構成し，協力して課題に取り組む．聴講参加は演習を行わず，第 2 部では演習参加の様子を見守る形になる．

講座の運営には 2 つの課題があり，1 つは参加者の前提知識やスキルの違いである．演習参加者は高校生と大学生（大学院生を含む），社会人からなるが，間口を広くするという意図から，参加募集の際に専門的な知識や経験を要求していない．結果として，(1) 教材に出てくる用語等が分からない参加者や，(2) キー入力により起動するコマンドラインツールの取り扱いに不慣れで，第 2 部前半のハンズオンをスムーズに進められない参加者が存在している．

(1) の対策として，用語等の必要な知識を事前に学習できる簡易な予習教材を準備し，明星大学の学習管理システム☆3 を通じて演習参加者に配布している．2019 年は，事前登録した演習参加者の約 84% が予習課題にアクセスしていた．(2) に対しては，いわゆるティーチングアシスタントのようなサポートスタッフを数名配置して，個別の質問に対応しながら演習を進めることで解決を図っている．

講座運営のもう 1 つの課題は，聴講参加者の支援である．聴講参加者は，演習中は室内を自由に移動して演習参加者の PC 画面を見ながら，進捗状況を見守る形になる（図 -2）．しかし，画面内のコマンドの表示などは見づらく，また，各チームの進捗状況を把握することは難しい．この対策については後述する．

演習のテーマ

第 2 部の演習で出題する課題のテーマは年により異なり，サイバー攻撃を扱う回とディジタルフォレンジックスを扱う回に分けられる．ここではそれぞれの課題の概要と，いずれの回でも共通して課しているレポーティングについて述べる．

❑ サイバー攻撃

サイバー攻撃を扱う回では，演習参加者は攻撃者の立場になり，運営側である我々が用意した攻撃対象のシステムを外部から調査する．システムには典型的な脆弱性☆4 が残されており，そこからシステム内部に侵入して重要情報を取得する，というシナリオである．攻撃者の視点を学ぶことで，防御側，すなわち攻撃を受ける側としてどのような対策が必要か，何を学ぶべきかを考えるきっかけを提供している．

2015 年の第 1 回は，当時のマカフィー(株)がトレーニングプログラムのために用意していた課題をベースにしており，演習参加者は攻撃側と防御側に分かれていた．しかし，防御側の参加希望者が少ないため，現在は攻撃側のみを募集している．防御側の視点は，後述するフォレンジックスの回で取り上げている．

❑ フォレンジックス

フォレンジックスを扱う回では，演習参加者は企業の情報システム部門の立場になる．運営側である我々は，攻撃を受けて情報漏洩が発生した状態の情報システムを準備しておく．演習参加者には社の重

図 -2　演習中の聴講参加者

☆3 講義資料の配布やレポートの提出を管理できる Web システム．いわゆる LMS（Learning Management System）．

☆4 もろくて弱い状態のこと．セキュリティホールのこと．

役から，社外からの通報により個人情報の漏洩が発覚したため，原因と漏洩の経緯を調べるよう業務指示があった，というシナリオである．

現実には，フォレンジックスの作業そのものは社内スタッフでは行わず，専門的な外部企業に委託するケースも多い．しかし，フォレンジックスの作業を理解しておくことで，情報システムの企画や設計，運用において何に注意が必要であるか，意識を高めるきっかけになると考えている．

❑ レポーティング

演習の最後は，どちらのテーマを扱った回でも，必ずチームごとに簡単なレポートを提出する．レポートには，いつ，どんな原因で何が起こったか，どんな対策が考えられるかを，簡潔に記載してもらう（図 -3）．客観的な事実に基づいて，具体的な対策まで含めて報告することで，演習で取り組んだ内容を効果的に振り返ることができる．第 3 部の講評では，レポートの内容について簡単に触れ，課題の進捗がよかったチームや適切な対策を報告したチームを紹介して表彰する．

IoT サイバーセキュリティ演習

ここではより具体的な内容の紹介として，2019 年に実施した IoT サイバーセキュリティ演習について，テーマ設定の背景と当日の進行や参加者の様子を紹介する．

図 -3　レポートの記入

❑ テーマ設定の背景

IoT（Internet of Things，モノのインターネット）は，あらゆる機器がインターネットに接続することで，我々の生活や仕事などを豊かにしてくれることが期待されている一方で，サイバーセキュリティの脅威が懸念されている．2018 年に公開された映画『名探偵コナン ゼロの執行人』でも IoT デバイスが登場し，話題になった．

実際，IoT デバイスに対するサイバー攻撃は年々増加傾向にあり，2016 年には Mirai[☆5] と呼ばれる IoT デバイスをターゲットとしたマルウェアが出現している．Mirai は脆弱な IoT デバイスへ不正侵入し，ボットネット[☆6] と化して，かつてないほどの大規模なサイバー攻撃（DDoS 攻撃[☆7]）を発生させた．その後，Mirai のソースコードがインターネットで公開されたこともあり，Mirai の亜種が次々と発生し，今もインターネット上で活動を続けている．

Mirai の攻撃は，典型的な ID とパスワードの組合せで次々とログインを試みるという非常に古典的な手法だったが，世界中で何十万台もの IoT デバイスがこの方法で不正侵入されてしまった．より身近になる IoT デバイスへの侵害は，これまで以上に，我々の生活に直結する甚大な被害を与えかねない脅威となり得るが，IoT デバイスにおけるセキュリティ対策やその理解は，まだまだ十分な状況とは言えない．デバイスが多様化しても，いつの時代も，セキュリティ対策は基本が重要であることを理解してもらうため，2019 年は IoT に関するサイバーセキュリティをテーマとして演習を実施した．

❑ 演習の題材

第 2 部の演習は，架空の鉄道事業者が運用する

☆5 Mirai は，脆弱な IoT デバイスへ不正侵入し，それらデバイスをボットネットとして悪用するマルウェア．ターゲットとするシステムや Web サイトに対して大量の通信トラフィックを送信し，サービス妨害攻撃（DDoS 攻撃）を行う．

☆6 マルウェア感染や不正侵入などによって，攻撃者の指令によって動く端末のことをボットと呼ぶ．ボットが大量に構成されたものをボットネットという．

☆7 Distributed Denial of Service attack，分散型サービス妨害攻撃．

「鉄道の運行管理システム」をテーマとした．この事業者では，離れた事務所からも電車の走行を把握できるようにして監視業務の運用を効率化したいという要望があり，監視用の IoT カメラが新設された，という状況を設定した☆8．

演習では，走行する鉄道模型（N ゲージ）と信号機に見立てた LED ライト，これらを制御する運行管理システム（Raspberry Pi）からなる演習セットを各チームに提供し，シナリオに沿って課題に取り組んでもらった．シナリオは，IoT カメラを調査して脆弱性を発見し，それを利用することで内部の運行管理システムへアクセスするという流れである．最終的に運行管理システムの認証を突破することができれば，鉄道模型を動かしたり，LED ライトを自由に点灯させたりすることが可能になる（図 -4）．

例年の演習とは異なり，鉄道模型や LED ライトといった目に見える変化を生む機器があることで，より積極的に課題に取り組む様子が見られた．特に，ほかのチームが鉄道模型を動かし始めると，「うちのチームも頑張らないと」という反応があり，会場全体が盛り上がっていた印象を受けた．

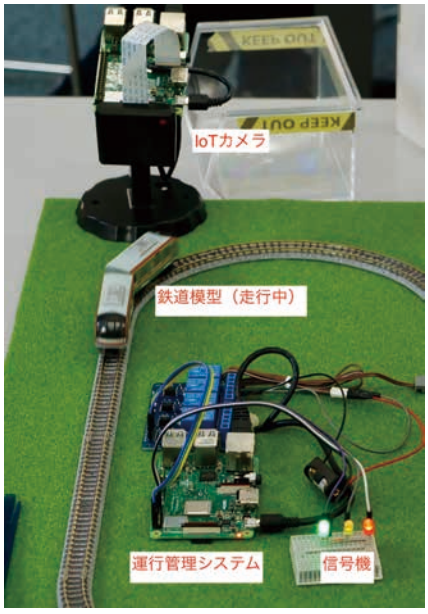


図 -4　鉄道模型を使用した演習セット

☆8 実際の鉄道運行システムはインターネットから隔離されているため，今回のテーマのような事態は発生しない．あくまで，IoT の脅威を勉強するための架空の設定である．

課題と今後の計画

講座の運営については大きく 2 つの課題があり，1 つは演習参加者の前提知識やスキルの違い，もう 1 つは演習中の聴講参加者の支援である．前者の対策についてはすでに述べたが，後者の対策として演習の進捗状況の可視化と解説を検討している．

可視化については Facebook CTF☆9 の利用を試みた回もあったが，単に課題の到達度を表示するだけでなく，チーム内のコミュニケーションの状況や試行錯誤の様子を見せられるとより効果的であると考えている．演習中の講師やサポートスタッフがそれらの表示を指し示しながら解説することで，聴講参加者の理解度向上を期待している．

2020 年度はハードニング（hardening，堅牢化）に焦点を当てた内容を検討しており，これらの改善案を盛り込んで実施することを目指している．

（2020 年 2 月 15 日受付）

丸山一貴（正会員） kazutaka@acm.org

2004 年東京大学大学院修了．博士（情報理工学）．同大情報基盤センター助教等を経て，2013 年明星大学情報学部情報学科准教授．プログラム開発環境やユーザインタフェースの研究，大学における ICT サービスの設計と運用に従事．

佐々木伸彦 sasaki@stonebeat.co.jp

2015 年にストーンビートセキュリティを設立，代表取締役．2016 年から外務省最高情報セキュリティ責任者（CISO）補佐官を務める．脆弱性診断や情報セキュリティコンサルティング，トレーニング講師など幅広く活躍中．CISSP，CISA，GCFA，LPIC-3 Security.

高谷宏幸 Hiroyuki_Takatani@McAfee.com

2005 年マカフィーに入社し，セールスエンジニアとして営業活動の技術的支援業務に従事．2014 年以降，プロフェッショナルサービス本部のシニアトレーナーとしてセキュリティ研修サービスを展開している．

☆9 CTF の運営を支援する Web アプリケーション．現在はオープンソース化されている．

ARTICLE

再帰的思考のすすめ

中川正樹
東京農工大学

今，教員生活を終わろうとしているこの時点で，これまでに「美しい」と思った再帰的な考え方をまとめてみたいと思う．難しいと思われるところは読み飛ばしていただきたい．

数学的帰納法

今から約 50 年前，高校生のときに数学で一番美しいと思ったのは数学的帰納法であった．n=1 のときに成り立つことと，n=k–1（あるいは n<=k–1）のときに成り立つと仮定し，n=k でも成り立つことを示して，したがって，すべての自然数 n で成り立つという証明法である．例として，次の等式を証明してみよう．

$$1+2+3+4+\cdots+n=\frac{1}{2}n(n+1)$$

n=1 のときは，$1=\frac{1}{2}1(1+1)$ なので，明らかに成り立つ．次に，n=k–1 のときに成り立つと仮定する．つまり，n に k–1 を代入して，

$$1+2+3+4+\cdots+(k-1)=\frac{1}{2}k(k-1)$$

が成り立つと仮定とする．これを用いて，次のように n=k でも成り立つことを示す．

$$\begin{aligned}&1+2+3+4+\cdots+k\\&=1+2+3+4+\cdots+(k-1)+k\\&=\frac{1}{2}k(k-1)+k=\frac{1}{2}k(k+1)\end{aligned}$$

したがって，n=1 で成り立って，2 で成り立って，. . . ，k–1 で成り立って，k で成り立つというやり方である．

数式微分

大学 3 年生のときに，LISP という言語で数式微分のプログラムを書いた．数値微分ではなく，入力に x^2 を与えると $2x$ を返す微分である．変数がアルファベット 1 文字だけで，数も 1 桁，かつ，四則演算だけの数式は次のように定義できる．下で，「｜」は「または」の意味である．

式＝項＋式｜項－式,
項＝因子×項｜因子／項,
因子＝(式)｜変数｜数,
変数＝ a|b|…|x，数 =0|1|…|9.

ある数式の x による微分 D は次に従う．

D(項＋式) = D(項) + D(式),
D(項－式) = D(項) − D(式),
D(因子×項) = D(因子) ×項＋因子× D(項),
D(因子／項)
　= (D(因子) ×項－因子× D(項)) ／ (項)^2,
D((式)) = (D(式)),
D(変数) = if 変数 = x, then 1 else 0,
D(数) = 0.

数式微分のプログラムは，表記の違いはあるが，原理的にほとんどこの通りである．そして，実行は，たとえば次のようになる．

D(x^2+3x+1)=D(x^2)+D(3x+1)
=D(x)×x+x×D(x)+D(3x)+D(1)
=1×x+x×1+D(3)×x+3×D(x)+0

$=x+x+0\times x+3\times 1+0=2x+0+3+0$

$=2x+3$

プログラムを書いてみると，数式の微分そのものよりも，結果を整理する（たとえば，$1\times x=x$，$x\times 1=x$，$x+x=2x$，$0+3+0=3$，無駄な括弧を外すなどのための）プログラムの方がはるかに長くなったのを記憶している．詳しく学びたい読者は文献 1)，2) を参照されたい．

典型的な再帰プログラム

再帰のプログラムで典型的なのは「ハノイの塔」の解法手順を出力するプログラムである．ベトナムのハノイにある寺院には，3 本の柱（A, B, C）と，真ん中に穴の開いた大きさがすべて異なる 100 枚の石でできた円盤があるという．元々はすべての円盤が柱 A に刺さっていて，僧侶たちが 1 枚ずつ移動し，すべての円盤を柱 C に移動しようとしている．僧侶が 100 枚の円盤を移動し終わった瞬間，この世は消滅するという．図 -1 は円盤が 5 枚のときの課題を示す．円盤は重ねられて柱 A に刺さっており，それらをすべて柱 C に移動する．ただし，1 枚ずつしか移動できず，しかも，小さな円盤の上にそれよりも大きな円盤を重ねてはならない．どの円盤も移動後は，いずれかの柱に刺しておかなければならない．そのために柱 B を補助として利用する．

さて，n 枚の円盤を柱 A から柱 C へ，柱 B を補助に使って移動する手順を示す言語 C のプログラム 1 を完成してみよう．1 枚のときは自明である．n 枚のときは，上の n–1 枚を柱 B に移し，一番下の円盤を柱 C に移してから，柱 B の n–1 枚を柱 A による補助で柱 C に移せばよい．プログラムの□の中には，a, b, c いずれかの変数が入るので，適切なもので埋めて実行してみよう．

円盤 1 枚を 1 分で動かせるとして，移動を始めてからどれぐらいの時間で終了するか考えてみてほしい．安心して眠れると思う（なかなか計算できなくて眠れないかもしれないが……）．ちなみに，ハノイには 10 回ぐらい行ったが，いまだにこの寺院には行き当らない．

コンパイラ

筆者が若いころは計算機科学がまだ黎明期で，日本ではまだその教育が確立しておらず，大学院に入ってから，英国の Essex 大学の修士課程に留学する機会を得た．そこでは，初期の人工知能の論文もたくさん読んだが，学部科目で，言語 C などの高水準言語から機械語に翻訳するコンパイラというプログラムを読んだ．プログラムが上例の数式と同

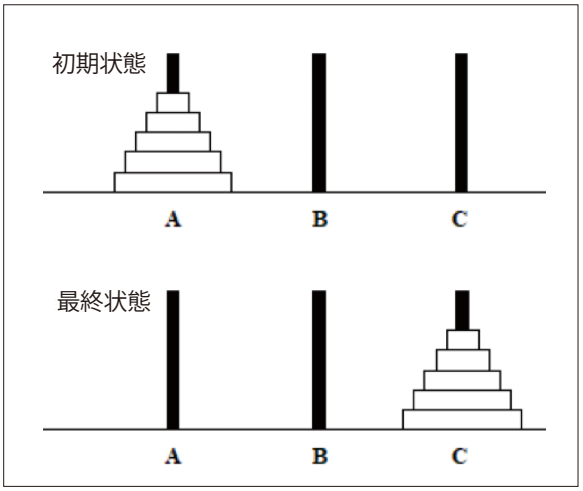


図 -1　ハノイの塔（5 枚のとき）

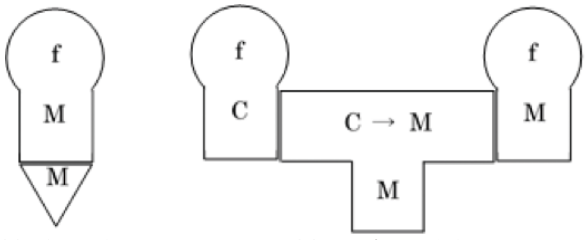
```
#include <stdio.h>
void hanoi(char a, char b, char c, int n)
/* move n disks from a to c using b */
{
   if(n==1) printf("Move a disk from %c
      to %c.¥n", a, c);
   else {
      hanoi(□, □, □, n - 1);
      printf("Move a disk from %c to %c.
      ¥n", □, □);
      hanoi(□, □, □, n - 1);
    }
}
int main()
{
   int n;
   printf("Tower of Hanoi¥n");
   printf("How many disks? ");
   scanf("%d", &n);
   hanoi('A', 'B', 'C', n);
}
```
プログラム 1　解法手順を表示するプログラム

じように厳密な再帰的文法で定義されることを利用して，高水準言語から機械語への変換を再帰法に従って行う．そのプログラムの行数は予想よりはるかに少なかった．この分野の成果は計算機科学の金字塔の１つと言えるだろう．

そして，小さい言語からより大きい言語に拡大していく方法（bootstrapping）にも感嘆した．図 -2（a）に示すように，機械語 M で動作するコンピュータを▽で中に M，機械語 M で記述された機能 f を実行するプログラムを鍵穴形で下に M，上に f で書く．プログラムを実行させることで，f の機能が発揮する．

コンパイラは機能として，言語 C から機械語 M に変換するので，図 -2（b）で示すように，鍵穴の上の半円を四角に変形し，中に C → M と書く．言語 C で書かれた任意の機能 f のプログラムを同じ機能を持つ機械語 M のプログラムに変換する．

最初のコンパイラは小さい言語（μ C と書こう）のために作り，その言語 μ C でフルスペックの言語 C のコンパイラを書けば（図 -3 の左端），そのコンパイラをコンパイルすることで，フルスペック C のコンパイラが得られる（図 -3 中央）．これを動作させれば，任意の機能 f のプログラムをコンパイルできる（図 -3 右）．言語 C だけでなく，別の言語でもよい．興味のある人は Earley [3] を読んでほしい．



(a) 機能 f の実行　　(b) コンパイラの機能

図 -2　記述言語と機能の実行

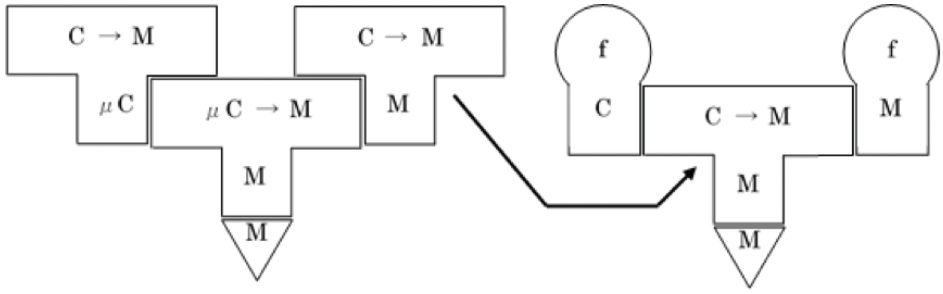


図 -3　小さい言語のコンパイラを作って大きい言語のコンパイラを作る

分割統治法

自然数は１から始まって，それに１を加えたものも自然数という一番単純な構造を持つ．木構造は幹から次々に枝に分かれてどこかで葉になる構造を持つ（そうでない変な植物もあるが）．プログラムは枝や葉に種類がある木構造である．こうした構造を処理するプログラムを書くとき，構造を分解して部分ごとに解法を適用し，それらの結果をまとめることで構造全体を処理する方法を分割統治法と呼ぶ．要素数が n のときに，たとえば，分割しないと n^2 の処理時間になる方法を，上手に分割することで $n \log n$ で処理できるようになる．数学やプログラムあるいはデータのように明確な構造を持つ対象だけでなく，さまざまな対象で分割統治法は採用されている．学校のクラス分けやグループ分け，企業や組織の部や課への分割とそれらの管理である．大規模な問題を効率的に処理できるプログラムを書ける人は大組織の管理や運営にも能力を発揮するはずである．したがって，誰もがプログラムを書いてみることに賛成である．逆に，プログラムを書いたこともない経営者や管理者が，情報システムの企画責任者になることにはリスクを感じざるを得ない．メガ銀行が統合するときに起きたトラブル，大手コンビニの電子決済システムの穴など，枚挙にいとまがない．

落語

修士課程を出て，経済的な理由から博士課程に行かずに農工大の助手として採用してもらった．講座の教授は高橋延匡（のぶまさ）先生だった．計算機システムで多くの業績を残された先生なのだが，落語好きで「えんきょうさん」と呼ばれていた．その先生から落語には再帰の概念も登場するという話を聞いた．それは「あたまやま」である．

あるケチな男がサクランボの種を捨てるのが惜しいと飲み込んだら，頭のてっぺんから桜が生えてきて，春になると満開になる．町人が花見に押しかけて宴会をする．しかし，そのうるささに耐えかねて，桜を抜いてしまう．すると，その穴に雨が溜まって池になり，魚が増える．今度は，町人が昼夜を構わずに釣りに来る．うるさくて眠ることもできない．その男は「いっそ死んでしまえ」と，その池に身を投げる．無理矢理に図にすると図 -4 のようになる．

別の例は「のっぺらぼう」である．ある商人の男が身投げをしようとする若い女を助けてみると，顔に目も鼻も口もないのっぺらぼうである．男は「世の中，なまじ目や鼻がついているために苦労している女は五万といる」となだめつつも，内心では血が引く思いで，蕎麦屋の屋台に駆け込む．息も切れ切れにその話をすると，蕎麦屋は「こんな顔ですかい」とのっぺらぼうの顔で振り向く．男は慌てて家に逃げ帰り，奥さんにその話をする．すると，奥さんが「こんな顔？」と振り向く．男は気を失う．しばらくして，奥さんに起こされて男は目を覚ます．「変な夢でも見てたんじゃない」と言われて，夢だったのかと，その夢の話をする．そうすると奥さんが「こんな顔？」と振り向く．男は気を失う，…….

これらの話は繰り返し（loop）ではない．再帰（recursion）なのだ．

図 -4　あたまやま

振り返って

再帰が美しいのは，一番単純な場合の処理を定義し，単純でない場合には問題を分解して部分の処理に自分自身を呼んで結果をまとめる記述をすればよいことである．何回ループするなどの記述は不要である．先人は再帰プログラムを実行できるようにするために，計算を途中で保留して，次の計算を始め（その計算をまた途中で保留し，次の計算を始める，……），結果が返ってきたときに計算を再開するためのスタックというデータ構造を生み出した．

当方は農工大の助手に採用してもらって 41 年間，手書きパターン認識とタブレットのユーザインタフェースの研究をし，実用化もできた．

この原稿とあまり関係のない研究のように思われるかもしれないが，課題解決のさまざまな局面で再帰が登場した．まさに，自分の思考法の柱の 1 つが再帰であった．

参考文献

1) 平野拓一：記号数式処理，http://www.takuichi.net/hobby/symbolic/
2) 渡邉慶一：LIST でやる記号微分，https://www.slideshare.net/KeiichiWatanabe/lisp-102975121
3) Earley, J. and Sturgis, H.: A Formalism for Translator Interactions, Communications of the ACM, 13, 10, pp.607-617 (1970).

（2020 年 1 月 12 日受付）

中川正樹（正会員） nakagawa@cc.tuat.ac.jp

1979 年東京農工大学工学部助手．1997 年教授．現在，副学長．手書きパターン認識とユーザインタフェースなどの研究・教育に従事．理学博士．2016 年文部科学大臣表彰，東京都功労者表彰など受賞．

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）

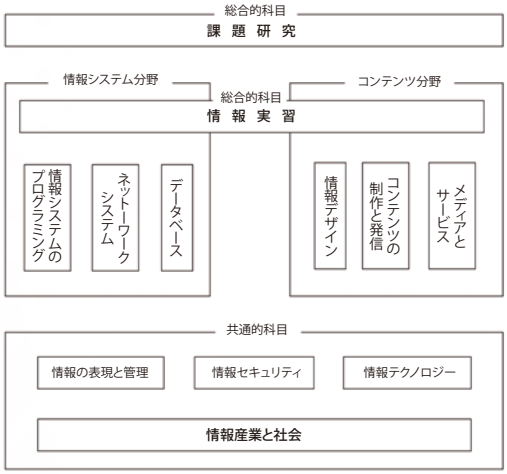
基般

専門学科「情報科」における情報コンテンツ分野の指導

長堂忠司　沖縄県立美来工科高等学校コンピュータデザイン科

専門教科「情報」について

高等学校の教科「情報」には，各学科に共通する科目のほかに，情報に関する専門教育を主とする学科において開設される専門教科「情報」の科目も存在する．高等学校学習指導要領（平成 30 年告示）解説においてその科目・分野構成は以下のように示されている（図 -1）．



■図 -1　専門教科情報科の科目および分野の構成

専門学科「情報科」設置状況

情報に関する専門教育を主とする学科は全国に 18 校，そのうち沖縄県には 2 校 3 科設置されている．本校には「情報システム分野」を担う IT システム科（以下 IT 科）と，「情報コンテンツ分野」を担うコンピュータデザイン科（以下 CD 科）がそれぞれ単独学科として設置されている．また，沖縄県立名護商工高等学校には両分野を包括的に学ぶ総合情報科が設置されている（2020 年 1 月末現在）．

専門学科を作ってきた若手教員たち

沖縄県における専門学科勤務経験者数

沖縄県は 2004 年度から情報科教諭の採用を継続的に行ってくれていて（採用試験は教科「情報」実施初年度の 2003 年から），2020 年 1 月現在で 45 名

が採用されている．そのうち専門高校での勤務経験を有する職員の延べ人数を，2003 年から今年度までを対象に今回独自に調べたところ 37 名であった．また，本校の各科および名護商工高等学校での勤務経験を有する職員を赴任形態別に分類したところ，表 -1 のようになった．

若手教員中心の立ち上げ

本校の IT 科ならびに CD 科は，その立ち上げ当初から若手教員中心の職員構成で，4 年目には唯一のベテラン教諭が退職して本校で採用された職員ならびに臨任だけの状態になった．それからしばらくは毎年のように初任者を受け入れ，その際に勤務していた臨任が採用試験に合格し，数年後に再度初任者として赴任，という流れを繰り返してきた．彼らは頼るべきベテランがいないまま，手探りで生徒をどのように育てていくのか，新しい教科・学科の姿をどのようにしていくのかを日々考え，努力を重ね創り上げてきた．彼らは専門学科で多くのことを学び成長して転勤していき，2 校目・3 校目でもその成果を発揮している．

他校採用者の赴任と引き継ぎ・発展

その一方で，普通校採用の教諭が 2 校目に赴任する流れもでき，さらに 3 校目の赴任校のケースもできつつある．なお筆者が初の 3 校目赴任者であり，後輩たちが築き上げてきたものを継続発展させる役目を背負っている．

■表 -1　赴任形態別の勤務経験者数（重複あり）

赴任形態（勤務年限）	IT 科	CD 科	名護商工
初任者採用（3 ～ 5 年）	10	7	5
他校採用後転勤（5 ～ 7 年）	3	4	5
臨任・補充（1 ～ 3 年）	3	4	1
合計	16	15	11

■図 -2　パソコン甲子園 2019 入賞作品

CD 科で扱う分野

現在 CD 科で扱っている分野は以下の通りである．

静止画

Photoshop を用いた画像の補正・加工，Illustrator のベジェ曲線によるイラスト制作を指導している．また，各種コンテストへの応募作品制作に取り組ませている（図 -2）．

Web

1 年次に HTML & CSS，2 年次にレスポンシブルデザイン・レイアウトをそれぞれ指導している．また，週 3 時間× 5 週 JavaScript による簡易ゲーム制作を指導している．3 年次選択科目では PHP ならびに XAMPP を活用している．Adobe 製品は用いずテキストエディタでコーディングさせている．

動画（実写・アニメーション）

1 年次 3 学期に動画編集ソフト（Premiere・After Effect）の基礎，2 年次 4 月から 9 月にコンテスト出品を通した動画作品制作（テーマに応じたストーリー制作・絵コンテ指導を含む）の指導を行っている．10 月から 12 月は情報モラル・セキュリティ関連動画制作，3 学期はフリーテーマで動画制作を行った．

ゲーム（ノベル・シューティング・3D）

3 年次課題研究で希望者に対して制作に取り組ませている．Unity・Enchant.js・TyranoBuilder 等のゲーム開発環境を用いるほか，開発環境に頼らずに作り上げる生徒もいる（図 -3）．

■図 -3　課題研究作品（ノベルゲーム）

3DCG

2年次に週3回×5週程度でモデリング・テクスチャ・アニメーションの概要を指導している．また，3年次課題研究で希望者には3Dプリンタの活用法，ボーン・アニメーションまで含めて取り組ませている．

音・音楽

2年次に週3回×5週程度でGarageBandの基本的な使用方法ならびにコード進行を用いた簡易作曲法を指導し，32小節の長さの自作曲制作に取り組ませている．また，Adobe Auditionによる音声データ編集ならびに録音機材の利用方法も指導している．

さまざまな出力装置の活用

IllustratorやPhotoshopで制作した静止画作品を転写用紙に印刷しマグカップやTシャツに転写する実習を取り入れている．3年次課題研究ではシール台紙に印刷しカッティングプロッタで切り込みを入れる研究に携わる生徒もいた．またレーザ加工機でコースターに静止画作品を焼く実習も行った．

融合型

3年次課題研究のテーマ設定時に，複数の分野にまたがるテーマを希望する生徒がいる．たとえば，2019年度は，将来ゲーム会社に就職を希望していることならびにVTuberに興味がある生徒が「VTuberになるための動画制作」をテーマにした．彼は3Dモデリングとテクスチャを Blender，アニメーションを Unity，動画編集は Premiere，音声編集は Audition と，さまざまなソフトウェアを活用し動画作品を仕上げた（図-4）．

なお，上記の各分野は，目的（核となる技術，分野を拡げる等）に応じて，年間，学期ごと，5週程度と指導期間が異なることに留意が必要である．

■図-4　VTuber制作に使用したソフトウェア

授業実践

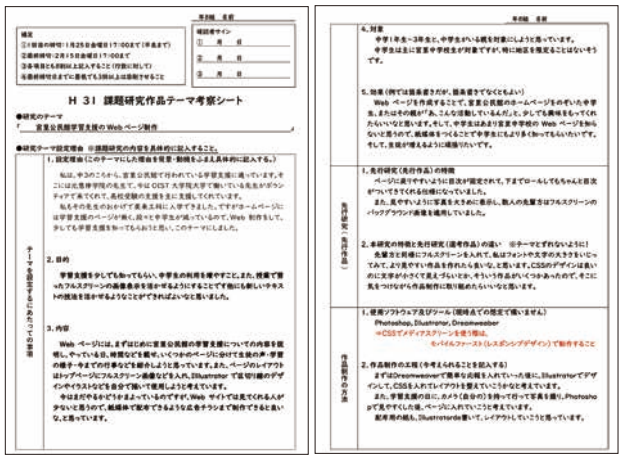
課題研究

CD科では3年次に原則履修科目「課題研究」(3単位)ならびに学校設定科目「マルチメディア実習」(3単位)において作品制作に取り組ませている．主な分野は静止画・動画・Web・ゲーム・3DCGで，身の周りの問題を発見してそれを研究テーマとし，解決手段としてのコンテンツ制作に取り組ませている．その指導の流れと取り組みを述べる．

テーマ設定（2年3学期）

テーマ設定においては，まず，テーマおよびその設定理由・目的・内容・対象・効果・先行研究の調査と本研究との違い，使用ソフトウェア，開発工程について「課題研究テーマ設定シート」に一通り記入させ，CD科職員と面談を行う（図-5）．

面談では，デザイン（ここでは「問題解決＋解決策としてのコンテンツ制作」）の視点に立っているか，自分本位のものになっていないか，生徒自身の力量を考慮して原則1年間で完結できそうか，環境



■図-5　課題研究テーマ設定シート

問題のような個人の力量だけでは対処できず検証もできないものではなく，身の周りから探しているか，目的・対象が明確になっているか，内容を読んで完成形が予想できて相手に伝わるか，学科の設備で対応できるか，外部とのやりとりが発生するか，といった点を確認し，不明点があれば生徒に発問する．これらの面談を複数の教職員と繰り返す中で生徒と教員の間で完成イメージを固め，また共有していく．

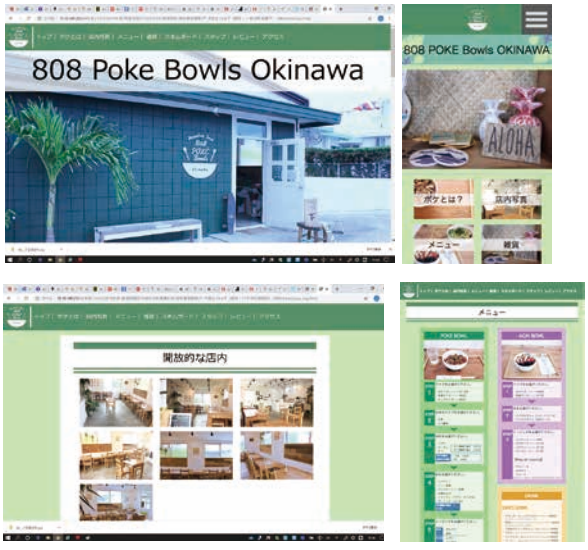
なお，課題設定の際には「問題は現実と理想の差である」ことを伝え，それを念頭において課題を見つけるよう助言している．

完成予想図・試作品制作（4月～6月）

テーマ設定が終了したら，静止画ならストーリーボード，動画なら絵コンテ，Webならワイヤーフレーム，といったような完成予想図を作成させ，イメージをより具現化させてから制作に取りかかる．その際，できる限り作品の中核になる部分から始めるように勧めている．これは，中間発表の際にその部分に対するレビューを徹底的に行うことで，その後の制作が間違った方向にいかないようにするためである．

中間発表（7月初旬）

学科設立当初から指導助言をいただいている沖縄県立芸術大学美術工芸学部デザイン専攻の講師を交えて，研究に対する指導助言を行っている．適宜プレゼンテーションの指導も行っている．



■図-6　課題研究作品（Webデザイン）

作品制作（中間発表終了後～10月末）

中間発表での指摘を踏まえた上で本制作に取りかかる．なお，進路活動や他の課題も同時並行で取り組むため，生徒にかかる負荷には十分気を配っている．図-6は作品の一例（Web）である．

検証と手直し（11月～12月）

テーマ決めの際に設定した対象に応じた検証を行っている．たとえば，中学生向けにCD科紹介パンフレットを制作した生徒は，実際に中学校に出向き中学生に紹介してアンケートを実施したり，親戚の経営する飲食店のWebサイトを新規に制作した生徒は，来店した客にサイトを見てもらい感想をいただいたり，といった活動に取り組ませている．なお，事前にアンケート用紙を制作・提出させ，研究開始時に設定した対象に対し，狙った効果が得られることを確認できるかチェックした上で実施させている．

最終発表（1月初旬）

中間発表と同様に講師を交え，作品自体の仕上がりと課題に対する成果を中心に総括を行う．

レポート制作・手直し（1月中旬以降）

最後に作品紹介を含めた研究成果をA4縦2段組4ページのレポートにまとめさせている（図-7）．それを製本して後輩が課題研究に取り組む際の参考資料として利用できるようにしている．また各種イベントで生徒作品と一緒に展示している．

なお，一連の活動は基本的には個人で自主的に取

■図-7　課題研究レポート

り組ませ，毎回の授業で担当教諭と進捗状況・今後の方向性・問題点とその解決についてやりとりを行っている．

上記で述べた課題研究は歴代の CD 科教諭並びに沖縄県立芸大美術工芸学部の講師との連携により培われてきたものを継続してきたものである．

また筆者は指導にあたってはウォーターフォールモデルを意識し，不明点は前工程に戻ってなくしてから作業を進めること，段階的詳細化によって物事を明らかにすること，逆に視野が狭まっている場合は拡げるよう支援している．

開発速度も求められる現代社会では，その手法にも速度が求められる．さまざまな手法がある中でも一度ウォーターフォール型の開発経験をしておけば，ほかの手法にも対応がしやすいだろうと考え，指導にあたっている．

ミュージックビデオ制作

これまでの経緯

これまで CD 科では音・音楽に関する指導を後回しにしてきた．何もない状態から教材を作成せざるを得なかったことと，音ならびに音楽の指導の目途が立たなかったためである．そこに前任校で DTM（Desk Top Music）の教材開発ならびに指導経験を有する筆者が赴任してきたことから，これまで積み重ねてきた Visual の技術と新しくもたらされた Audio・Sound の技術を統合するための指導が可能となった．そこで今年度 3 年生の「情報コンテンツ実習」という授業でミュージックビデオ制作に取り組むことにした．なお 2 年生の「情報コンテンツ実習」において動画編集（アニメーション・実写）ならびに DTM と作曲の基礎を事前に指導してあった．

指導の実際

制作にあたっては，前述の課題研究では，個人で制作に取り組むことから，長期間のグループ活動がこれまでなされていなかった経緯も考慮し，3 ～ 4 名のグループ活動を取り入れた．そのグループ編成は教師側で行った．就職した先の企業で団体行動する際には人の好き嫌いを超えてチームとして 1 つの課題に取り組む必要があるので，その経験ができるようにすること，自らの得意・不得意の適性を考えられるようにすること，全グループの作品が同じレベルになること，を狙ってのものである．

編成にあたっては，「作詞＆メロディ」「リズム」「動画」の 3 分野のどれを担当したいのかを生徒に回答してもらった結果と，事前に把握しておいた生徒の能力・適性・興味関心とを照らし合わせ，各グループの技量が均等になるよう調整を行った．

実際の指導にあたっては，最初に作品のテーマについてグループで討議をさせた．その際，完成イメージを創り上げ，それをメンバ全員が共有すること，質問された際に全員が同じ趣旨の発言ができるようになることを求めた．作品のテーマが決まらないグループには「卒業」とか「夢」といったキーワードやモチーフを与え，そこからイメージを膨らませ，テーマとするように助言した．

制作にあたっては，すでに各班に Audio が得意な生徒，Visual が得意な生徒が割り振られており，彼らが率先して作品作りに取り組んでいることから，授業中は基本的に俯瞰しつつ困っていそうなグループを見つけては助言を与えるスタイルに終始した．

実際の制作期間は 5 月中旬から 10 月半ばの半年程度で，夏休み前までは Audio 担当は作詞作曲，Visual 担当は絵コンテ・動画コンテ制作を行い，2 学期に入ってから歌の録音と動画制作にそれぞれ取り組んだ．締切の 10 月中旬までには全グループが完成にこぎつけてくれた（図 -8）．

題材としての動画の魅力

ここで動画を構成する諸要素について，我流ながら段階的に詳細化することを通して，教材としての有用性と可用性について述べる．

■図 -8　ミュージックビデオ作品

まず動画の Visual 部分は残像効果を利用したものであり，静止画の連続的な変化によりもたらされることから，ある瞬間の一コマを静止画としてとらえることができる．その静止画はさらに，実写，アニメーション，プログラミング（メディアアート）等に分類できる．Audio 部分に関しては音 (Sound) であり，自然・環境の音，楽器の音，シンセサイザなどの機械音等に分類できる．ちなみに音と連なり・重なり・周期性が音楽（Music）となる．

それら個々の要素に焦点を当てた授業展開も可能であるし，それらのうちどの要素を用いるのかの取捨選択，どのように連ねていくのかといった構成についても扱うことができる．さらにその中に伝えたいことをどのように織り込んでいくのかといった視点も織り込むことができる．本科のような専門学科のように授業時数を多く確保できない共通教科においても，上記の要素のうち重点的に指導したい・すべき部分の見極めを行えばよい．

評価に関しては造形の五要素（形·色·材質·空間·時間）や音楽の三要素（リズム・メロディ・ハーモニー）等の視点から，まずは良否の 2 段階から入り，その段階数を深化することでよりきめ細やかな評価ができる．さらにこれらの要素に関する評価語の語彙力を上げることによって生徒に対して速いレスポンスでの指導もできるようになり「指導と評価の一体化」が可能となる．

これから情報コンテンツ分野の指導に取り組むことになったとき「何を教えるのか」「どのように教えるのか」「評価をどのように行うか」といった不安がつきまとうが，これらの諸要素がその障壁を下げる一助となれば幸いである．

生徒たちが興味・関心を抱きやすい題材なのでそれをうまく活用できればやっていて楽しく，有意義で手ごたえのある授業になると思う．

さまざまな外部連携

本科はさまざまな外部連携を実施している．具体的には，沖縄県立芸術大学美術工芸学部デザイン専攻の講師による課題研究作品への定期的な指導および助言，沖縄土産制作企業との連携による商品デザイン実習などが挙げられる．さらに今年度（2019 年度）は新たに Web 制作会社による Web マーケティングに関する講義ならびに仮想クライアント向けの広告バナー制作およびそのプレゼン実習，弁理士による著作権・肖像権・知的財産権等に関する講習，沖縄県立総合教育センターとの研究協力ならびに同センターによる農工商連携実習，とさまざまな連携を行った．

専門教科「情報」って?

私が大学を卒業するときにとある教授から「この先の人生で必ず数学についてあらためて意識することがある」という言葉を贈ってもらった．あれから二十年以上たって今は送り出す立場となっている．先の連携実習の中でも農業・工業・商業といった専門教育に携わる先生方はふとしたときに「農業とは」「工業とは」「商業とは」について口にしていた．情報科とはいえコンピュータ科学から一番遠い本科に勤務する教諭として，本科で学ぶ生徒たちに対して，どのように話せばよいのかを常に考えている．情報コンテンツ分野の指導に携わるようになって 12 年目が終わろうとしている今は，「『情報とは五感から得られることのうち○○にとって必要なもの』で，その情報を収集・処理・加工・表現・伝達・扱うことを学んでいるんだよ，その情報を生みだす仕事なんだよ」と伝えている．

情報ならびに情報が付く言葉が表すものは軒並み変化・変容の速度が速くその抽象度も高くて的確に簡潔に述べることが難しいし危険である．だがどんな児童・生徒にも伝わるような言葉を常に追い求め，そのための実践・研鑽・交流を重ねていきたい．

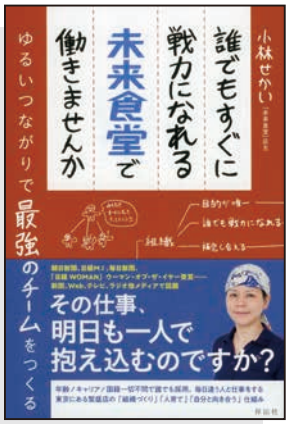
（2020 年 2 月 18 日受付）

長堂忠司　nagadout@open.ed.jp
沖縄県立美来工科高等学校コンピュータデザイン科教諭．琉球大学理学部数学科卒業．2004 年情報科教諭として採用，2015 年より現任校勤務．

…森田 一（富士通研究所）

誰でもすぐに戦力になれる未来食堂で働きませんか

ゆるいつながりで最強のチームをつくる



小林せかい 著
祥伝社（2019），240p.，1,600 円+税，ISBN：978-4-396-61683-0

この本を手に取ったわけ

研究であっても開発であっても，1 人でできることは限られており，規模が大きくなればチームを組み協力して立ち向かわなくては解決できない．これを読んでいる方の中でも，リーダとしてチームを運営しなくてはならない立場の方は多いのではないか．

そういったときに，メンバの誰もが高いレベルで仕事内容にも詳しければよいのだが，そううまくはいかないことも多々ある．たとえばこんな状況を考えてみる．集まったチームメンバの得意分野はさまざまで，経験もベテランから新人まで，メンバ内の能力差も大きい．新人には簡単な作業を割り振ったつもりでも，相手にとってはそうではなく手戻りとなってしまう．納期に追われていて，一から教育しなおすような時間はとれない．リーダが穴を埋める形で負担が増え，新人の教育は後回しになる負のループに陥ってしまう……．こういったチーム運営の難しさはどこにでもあるのではないだろうか．

未来食堂

この本は「未来食堂」の店主である小林せかいさんの強いチーム作りについての本である．未来食堂では 50 分働くと一食無料となる「まかない」という仕組みがあり，せかいさんとまかないを対価に働くまかないさんだけで食堂を運営している．

まかないさんとなるためには，ほぼ選別はなく，食堂に一度来た人であればどんな人でも受け入れ，その日の食堂を回していく．

仕事に参加する障壁を少しでも下げてチームを運営する参考になればとこの本を手に取った．この環境がそのまま当てはまる職場はなかなか存在しないと思うが，ここで書かれている考え方は幅広く応用がきくものと考え紹介する．

構成

本書は序章を含めて全 5 章で構成されている．第 1 章は「組織……どうやって場をつくるか」．良い組織とは，目的が明確で，誰でも戦力になれ，それぞれの良さを補完しあえる組織，と定義し，チームの中でリーダの役割やチームを良い組織にするための仕組みについて解説している．第 2 章では「人……どうやって人を育てるか」．人のパフォーマンスを能力とモチベーションの掛け算として，能力を高める方法と，モチベーションを保つ方法について．第 3 章は「自分……どうやって自分に向き合うか」．リーダとしての心構えについて，人とのかかわり方から自分自身の成長まで幅広く述べている．第 4 章では「巻き込む力で『一人』を超える」，人に物事を頼む際のコツについて書いている．本稿では，特に第 2 章に絞って紹介する．

どうやって人を育てるか

未来食堂では誰でもまかないさんとして仕事に参加できる．これは誰でもできる簡単な仕事だけをまかないさんに切り出しているわけではなく，人が育つ仕組みを作ることで，誰でも仕事に参加する能力を身につけられる組織を作り上げたことがその理由である．本書第 2 章に沿って内容を紹介する．

「入れ子型」体制

人を育成するコストは非常に大きく，通常の業務に加えて育成も同時並行で行おうとすると，どうしても通常業務にしわ寄せが出てしまう．入れ子型体制は育てるコストをリーダや教育係が負担するのではなく，チームで分散する体制である．リーダがメンバをフォローし，そのメンバが次のメンバをフォローするように，フォローする者とされる者が入れ子になる体制である．

経験が浅くても教える側にまわることで，アウトプットを早い段階からすることができるため定着が進み，能力差が近い者同士で教えあうことになるため育てる際の負荷も比較的小さく済む利点がある．

単に先輩が後輩を育成するのとは何が違うのかというと，直属の入れ子以外には直接フォローしない等，仕組み化されていることで，属人化や風化することなく育成の体制を維持し，育成の分担を分散できる点である．

「二人三脚」育成法

入れ子型体制とセットになっている育成法が「二人三脚」育成法である．この育成法では，教える／教えられるという関係から，一緒にやっていく，という関係に概念を捉えなおすことを行う．教えられる側は教えられている間は，仕事に貢献できず自尊心を高められないばかりか，手間をかけて申し訳ないと萎縮してしまうことにもつながるとし，「教える」ではなく，一緒にやっていき，フォローするというやり方を説いている．

モチベーション

著者はモチベーションは高めるものではなく，保つものとしている．モチベーションを外部から高めようとするのは難しく，それよりはモチベーションを下げる要因を除くほうが簡単であるとしている．

さらに，モチベーションを保つには，したいことを自分で探し，実行することが重要としている．したいこと（＝新しいこと）をすれば，多くの場合失敗することになるが，失敗も成功のために必要なステップであると認識することで，失敗を乗り越えることがモチベーションの向上にもつながる，としている．

誰でもすぐに即戦力

１つ１つのやり方に，すべて理由やエピソードが書かれており，分かりやすく納得がいく形でかかれているので，試してみようと思える良いビジネス書である．実際に自身の環境に適用するには，咀嚼し再構築しなければ，厨房のやり方を開発の現場へ持っていくことはできないとしても，自身のやり方を見直す良いきっかけとなった．

まだ実力不足だからまずは育成という考え方ではなく，まず戦力になれる環境づくりが育成のためにも大事なのだろう．人不足，エンジニア不足が叫ばれる昨今，どこまで間口を広げられるかは重要な課題となってくるのではないだろうか．

（2020 年 3 月 4 日受付）

森田　一（正会員）　hmorita@fujitsu.com
2014 年東京工業大学大学院総合理工学研究科博士取得（工学）．2014 年京都大学 特定研究員（2017 年 3 月まで），2017 年富士通研究所 入社．自然言語処理研究に従事．

連載

5分で分かる!? 有名論文ナナメ読み

梅谷信行（東京大学）

Prévost, R. et al : Make It Stand : Balancing Shapes for 3D Fabrication

ACM Transactions on Graphics 32（4）

CG 分野でのモノづくり研究

三次元プリンタに代表されるコンピュータで制御される工作機械が身近になるにしたがって，ディジタル表現のメディアが，音声や画像だけでなく，実在の物へと幅を広げている．しかしながら，実在の物は，物理法則によって支配されるため，たとえば折れたり倒れたりしないように，物理を考慮にいれて形を設計しなければければならない．そうした中で，三次元印刷された物体の強度を上げたり，物体の変形や色を忠実に実現したりという，さまざまな要求に対して計算機を用いた設計方法がコンピュータ・グラフィクスの研究分野で積極的に研究されている．コンピュータ・グラフィクスの研究というと，字面からは計算によって画像や動画を合成する学問であるという印象を受けるが，もはや研究対象はディスプレイ上のピクセルにとどまらず実世界のモノづくりへと範囲を広げている．本稿では，そんな三次元プリンティング向けの設計支援システム研究の先駆けとなった論文の１つを紹介する．

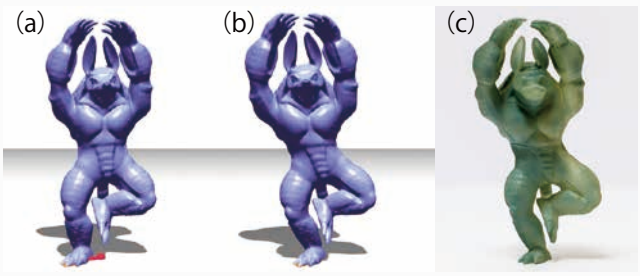


図 -1　(a) 自立しない形状，(b) 自立させるように外形を最適化した結果，(c) 3D プリントされた形状［Prévost et al. から引用］

姿勢安定性と最適化

この論文は，三次元プリントされた物体が床の上で安定して立つように，形状を変形させるような技術を提案している．たとえば，変わった姿勢をしたキャラクタはバランスを崩して自立しないことが多いが，キャラクタの内部の空洞の形状を変えたり，姿勢を微妙に変えたりすることで，重たい台座に固定する必要なく自立させることができる（図 -1）．

変形が無視できるような硬い物体を，平らな床の上においたときにそれが安定するためには，物体の重心位置と，床との接触点の位置関係が重要である．接触点の凸包を計算したときに，その凸包の中に物体の重心位置から床に下ろした垂線の足が含まれる場合は，物体は自立して立つことができる．そこで，物体の重心位置を凸包に入るように形状を変更すればよい（図 -2）．

重心を望みの位置にするように形状を変更する方法は多々あるが，この論文では（1）物体の内部の変更，（2）物体表面形状の変更という 2 種類の方法について提案している．物体の内部の変更で

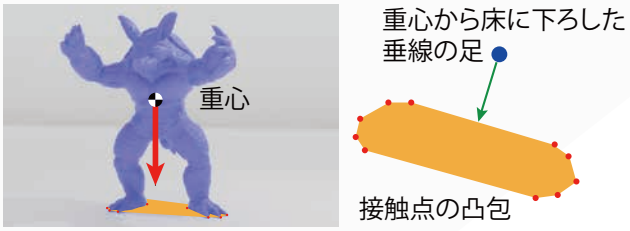


図 -2　三次元物体を床に安定に立たせるための条件

は，物体の内部の空洞の形を制御することによって重心を変えるものだが，空洞の形は非常に自由度が高く扱いづらい．そこでこの論文では，空間を格子を用いて離散化するボクセル方式の形状表現を用いている．物体の内部だけを変更して重心を動かせる範囲には限界がある．そこで，物体の表面形状も必要に応じて変更する．一般的に物体の表面形状は非常に自由度が高いので，この論文ではユーザに数個の点を物体内部に入力させ，その点周りの剛体変形に基づいて物体全体を滑らかに変形させる線形ブレンドスキニングという技術を用いて変形させる．

重心の位置が凸包に収まりつつ，形状の差を最小化するように目的関数を定めて，最急降下法にて最適化することで望みの形状を得ることができる．この最適化の処理は高速で，最適化された形状をユーザが対話的に逐次編集することも可能である．著者らはYouTubeに解説動画をアップロードしているので，興味を持たれた読者はぜひとも参考にしてほしい：
https://www.youtube.com/watch?v=_drZksLRx94

その後の研究に与えた影響

三次元プリンタは，任意の三次元の形状を，さほど大きな制約なしに出力できるので，オリジナルな一品物を作るのに適している．三次元プリンタの種類によっては，任意の色を印刷することができたり，弾性のある材料を使ったり，性質の異なる材料を任意の割合で混ぜることができ，その表現の自由度は非常に大きい．三次元プリントされた物にいろいろと機能を持たせるべく，たとえば力をかけても壊れないようにしたり，コマのように回転しやすくしたり，ロボットように関節をつけて動くようにしたりなど，さまざまな物理を考慮した設計支援の研究がなされている．これらの研究では，ユーザが対話的に設計に参加できるインタフェースが提案されていることが多く，ユーザの創造を妨げないよう手法が工夫されている．筆者らも，三次元プリンタを使って任意の形状をした笛を，音響シミュレーションを元に対話的に作る研究や，よく飛ぶ手投げ飛行機を対話的に設計するシステムなどを提案している．

生産技術の発達によって同じ物を大量に自動で製造することが可能になったが，高度にカスタマイズされた物を人間の介在なしに自動で作れるようになる日はまだまだ遠いだろう．製造がディジタル化され自動化されたからといって，その製造のために使われるディジタル形状データを自動的に生成することは困難であるからだ．設計には使いやすさや，見た目の良し悪し，製造のしやすさなど，定量化の難しいさまざまな要因を考慮しなければならない．計算機が人間の設計を賢くサポートして，自由に人間の意図を反映させられるようにするためには，まだまだ課題が多く残されている．

(2020年1月9日受付)

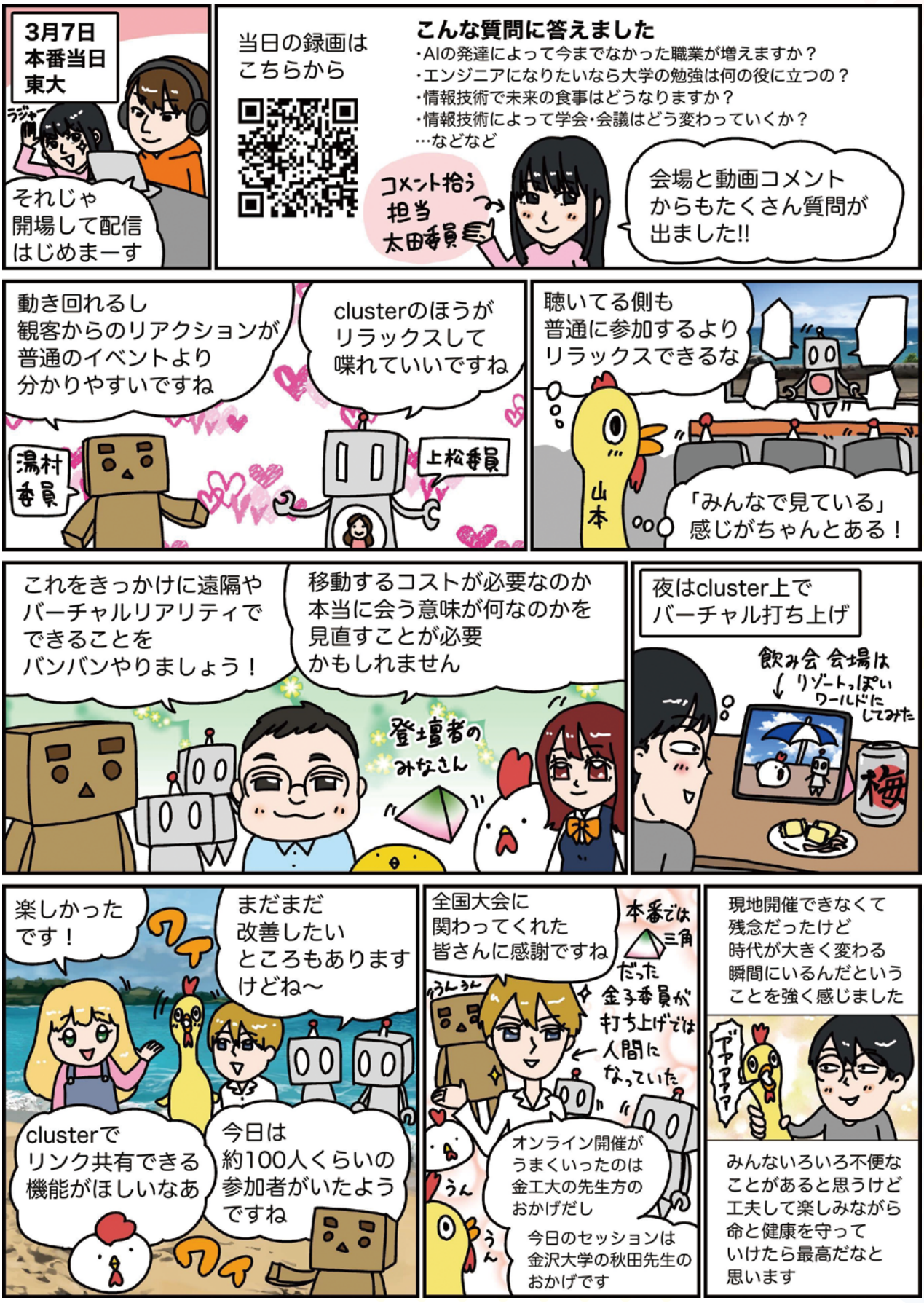
梅谷信行 n.umetani@gmail.com

2012年東京大学情報理工学系研究科博士後期課程修了．オートデスク研究所の主任研究員などを経て，現在，東京大学情報理工学系研究科特任講師．博士（コンピュータ科学）．

その8 全国大会がオンライン開催！ 公開セッション「先生，質問です！」の裏側お見せします

漫画：山本ゆうか（Twitter @ymmox）

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


3月7日
本番当日
東大
それじゃ
開場して配信
はじめまーす
当日の録画は
こちらから
こんな質問に答えました
・AIの発達によって今までなかった職業が増えますか？
・エンジニアになりたいなら大学の勉強は何の役に立つの？
・情報技術で未来の食事はどうなりますか？
・情報技術によって学会・会議はどう変わっていくか？
…などなど
コメント拾う担当
太田委員
会場と動画コメント
からもたくさん質問が
出ました!!
動き回れるし
観客からのリアクションが
普通のイベントより
分かりやすいですね
clusterのほうが
リラックスして
喋れていいですね
湯村委員
上松委員
聴いてる側も
普通に参加するより
リラックスできるな
山本
「みんなで見ている」
感じがちゃんとある！
これをきっかけに遠隔や
バーチャルリアリティで
できることを
バンバンやりましょう！
移動するコストが必要なのか
本当に会う意味が何なのかを
見直すことが必要
かもしれません
登壇者の
みなさん
夜はcluster上で
バーチャル打ち上げ
飲み会 会場は
リゾートっぽい
ワールドに
してみた
梅
楽しかった
です！
まだまだ
改善したい
ところもありますけどね〜
clusterで
リンク共有できる
機能がほしいなあ
今日は
約100人くらいの
参加者がいたようですね
ワイ
全国大会に
関わってくれた
皆さんに感謝ですね
本番では
三角
だった
金子委員が
打ち上げでは
人間に
なっていた
うんうん
うん
オンライン開催が
うまくいったのは
金工大の先生方の
おかげだし
今日のセッションは
金沢大学の秋田先生の
おかげです
現地開催できなくて
残念だったけど
時代が大きく変わる
瞬間にいるんだという
ことを強く感じました
アアアア
みんないろいろ不便な
ことがあると思うけど
工夫して楽しみながら
命と健康を守って
いけたら最高だなと
思います

編集委員退任にあたって

2016年4月から塚本編集長のもと2年間，2018年4月から稲見編集長のもと2年間，合計4年にわたり，会誌編集委員を務めさせていただきました．この間，本務先の任務の都合もあり，会誌編集委員として十分な戦力になれなかったことは申し訳なく思っております．とはいうものの，会誌編集委員会での活動では，貴重な経験をさせていただきましたので，その経験をここでご紹介させていただき，編集委員退任のメッセージとしたいと思います．会誌編集委員会に参加させていただいて，まず感じたことは，委員会の運営体制がしっかりと確立されているということでした．情報学を取り巻く環境の目まぐるしい変化を敏感に捉え，特定の専門分野以外の一般の読者でも読めるように記事化して，タイムリーに読者に届けるという要求事項を満たしながら，月刊で会誌を刊行していくことは並大抵のことではありません．編集長のリーダシップ，多様性を受容する委員会の雰囲気，委員間のクリエイティブな議論，各委員の主体的な働きが，イノベーティブな会誌編集を導いたのではないかと考えております．連載漫画「IT日和」や「巻頭コラム」をはじめとして，企画段階から最終チェックに至るまでを，定例会とSlackを併用して進めていく作業は楽しい経験でした．学会公式LINEスタンプの作成の際には，オンラインで委員からスタンプのネタ集めをしていたので，いくつかアイディアを入れさせていただきましたが，（今明かしますが）「ACKを返して」が採用されたことは密かに嬉しく，このネタでも取り上げてくれるのかと学会の懐の深さをしみじみ感じたのを覚えています（本誌2017年4月号の漫画「情報処理学会公式LINEスタンプができるまで」に詳しい説明がありますのでぜひご覧ください）．編集長からは，委員就任の間に小特集か特集を1つは企画運営してほしいと言われておりましたが，結果的に「ビブリオ・トーク」や「ぺた語義」での数編の記事の寄稿にとどまってしまい，会誌編集委員としての職責を十分に果たさないまま退任することをお詫びいたします．一方で，私としては会誌編集委員会活動への参加を通じて，情報処理学会のポテンシャルの高さを実感するとともに，イノベーティブな編集委員会の実現の仕方に関する多くのヒントを得ることができました．このような機会を与えてくださったことに深く感謝いたします．会誌編集委員会がイノベーティブであり続け，本誌がますます充実していくことを願ってやみません．

（田名部元成／横浜国立大学）

編集委員退任にあたって

2016年の夏，昔同じ職場で働いていた前任者の先輩からの声掛けがきっかけで，3年半にわたり会誌編集委員会の仕事にかかわる機会をいただきました．2011年から4年間，学会論文誌運営委員会の情報システムグループで論文編集にかかわっていたので，1年半ぶりの本会への復帰でした．前回の論文誌編集では，投稿論文の査読を軸に，研究分野の専門性を掘り下げる「深さ」を意識した活動を進めてきましたが，今回の会誌編集を振り返ると，多くの研究分野を対象として多様な読者に情報処理の魅力を伝える「広さ」を意識する活動が多かったと感じています．

会誌編集委員の任期前半で印象に残っているのは，2017年の10月号に掲載された「ビブリオ・トーク―私のオススメ―：世界天才紀行　ソクラテスからスティーブ・ジョブズまで」の執筆です．日常業務で注目論文を紹介することはありましたが，書籍を対象としたことはなく，書籍の選定や書評の切り口の参考になればと，今までは十分目を通していなかった諸先輩方の記事を読み返し，多様な背景に感心するとともに，学術分野としての情報処理の広さを再認識する機会となりました．任期後半では，職場での遠方出張と委員会が重なることが増えてしまい，会誌作りに十分貢献できませんでしたが，編集活動における皆さんの想いに触れ，多くの学びを得ることができました．

編集委員にかかわった3年半は，新しい読者開拓のために，将来の本会の分野を支えるジュニア会員世代向けのコンテンツを充実させる変化のときだったと感じています．編集委員を始めた当初，小学校6年生だった自分の子供は高校生となりましたが，編集委員の任期中にコンピュータに興味を持ち，プログラミングの学びを深めていった時期とも重なります．最初こそScratchでのゲーム作りなど遊びの延長でしたが，オンライン講座でPythonなどの言語を習得した今では複雑なコードも書けるようになっています．ジュニア世代の能力の高さを身近で目の当たりにしたことで，彼らの世代をしっかりと巻き込むことができれば，情報処理の分野はさらに発展していくことを肌で感じています．

3年半の編集委員を通して，編集にかかわる皆さんの専門分野の広さと見識の高さに触れる貴重な機会をいただいたことに感謝しています．今回の経験を研究業務にも活かして，情報処理の発展に引き続き貢献していきます．

（井本和範／（株）東芝）

編集委員退任にあたって

2019 年度末をもって，会員サービス分野（MWG）の編集委員を退任させていただきました．MWG は，会議レポートのとりまとめ・閲読や，「会員の広場」に掲載するモニタコメントの閲読などを担当しています．

4 年前に編集委員に着任させていただいたときは，「情報処理」がどのように編集され出版されているのか，まったく分からない状態でした．1 年目・2 年目には，MWG の業務をほかの編集委員とオンラインで分担して担当させていただく中で，以前よりも会誌の内容に興味を持って読ませていただく機会が増えました．ときには，モニタコメントを閲読させていただく中で興味を持った記事の内容を，あらためて確認させていただくこともありました．また，直接会ったことがないほかの人の原稿を閲読・修正するという経験により，自身で論文などを執筆するときにも増して，正しい日本語の使い方や分かりやすい文章の構成を意識する習慣が身につきました．

幹事・主査を担当させていただいた 3 年目・4 年目では，MWG の業務のとりまとめをさせていただきました．さまざまな方に会議レポートの執筆をお願いした際に，快く引き受けてくださったことには，本当に感謝いたしております．また，MWG 以外の編集委員の方も参加する会誌編集委員会本会議に主にオフラインで参加させていただくようになり，会誌が全体としてどのように作られていくかを知りつつ，会誌のあるべき姿（たとえばオンライン化など）や記事の内容の検討に参加させていただきました．稲見編集長をはじめとする編集委員会の方々と，新年会など会誌編集委員会とは違う場所での議論をさせていただいたのも楽しい思い出です．ちょうどこのころに，会誌編集委員会では Slack が主な連絡手段として使われるようになり，オンラインでの議論もさらに活発に行われるようになったと感じています．

また，ビブリオ・トークへの寄稿を行って，これまで書いたものとは異なる種類の文章を書かせていただく経験もさせていただきました．ビブリオ・トークの記事が紹介した本の著者の方の目にもとまり Twitter で拡散いただいたことで，あらためて情報処理学会誌の影響の大きさを感じることとなりました．

本当に多くの刺激を受けて，さまざまなことを学ばせていただいた 4 年間でした．MWG の皆様，会誌編集委員会本会議の皆様，事務局の皆様，モニタの皆様や会議レポート執筆者の皆様のおかげだと感じております．今後とも「情報処理」が時代に合わせた発展をしつつ，多くの人に愛される会誌となりますよう，陰ながら応援させていただきたいと思います．

（谷田英生／富士通研究所）

● 論文誌ジャーナル掲載論文リスト
Vol.61 No.5（May 2020）

【特集：情報システム論文】

■ 特集「情報システム論文」の編集にあたって　阿部昭博
■ スイング計測装置を用いたプロ野球選手の特性分析に関する研究　田中成典 他
■ 留学生を対象とした観光行動特性分析手法の提案とその活用に向けた考察　蘭　天陽 他
■ ITIL 導入におけるシステム運用者の変容の段階　角田　仁
■ サーバ 1 台で構成可能な秘密分散法を用いた行列乗算の効率的でセキュアな委託計算　岩村恵市 他

【一般論文】

■ HIDS アラート調査のための HTTP リクエストとホストイベントの関連付け手法　鐘本　楊 他
■ 秘密分散法を用いた効率的な秘匿大小比較プロトコル†　藤井　航 他
■ メンテナビリティ・セーフティ・セキュリティを考慮した IoT システム向けリスク評価手法の開発　佐々木良一
■ 機械学習を利用した創作物の知的財産的価値への寄与の評価のための情報理論的な測度について*　金子　格
■ 統計的検定学習支援用ウェブアプリケーション BuMoc の開発　朴　壽永 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
（May 2020）

【論文誌 コンシューマ・デバイス＆システム Vol.10 No.2】

■ Improving Face Recognition for Identity Verification by Managing Facial Directions and Eye Contact of Event Attendees　Akitoshi Okumura 他
■ 機械学習を用いたツイート解析と統計的異常検知による通信障害検出システム　山田尚志 他
■ ARIA：シミュレーション・エミュレーション連携基盤を利用したインタラクティブな都市型水害の被害予測システム　廣井　慧 他

会員の広場

今月の会員の広場では，3 月号へのご意見・ご感想を紹介いたします．まず，巻頭コラム「TOKYO 2020 大会に向けて」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．

■開催が危ぶまれる新型ウイルス騒ぎの中でなければ興味深く読めただろうと思います．（匿名希望）

特別解説「量子コンピュータを用いた量子超越実験」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．

■量子超越実験の解説を読んで，量子コンピュータの応用を特集で取り上げていただきたいと思いました．（滝内邦弘）

■筆者は限られた紙面で努力されたとは思うが，非専門家が理解するには解説不足，一方で専門家にとっては自明な類いの解説ではないか．記事の価値を疑問に感じた．（匿名希望）

■量子計算の困難さと実験のポイントが「量子計算の仕組み」の節の中に含まれており，読みにくさを感じた．（匿名希望）

特別解説「神奈川県ハードディスク流出事件」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．

■物理的破壊を推し進めるのではなく，論理的なデータ消去技術を洗練すべきという意見に納得した．（匿名希望）

■専門分野でなくとも自身も考えながら読むことができた．（國武悠人／ジュニア会員）

特集「5G 時代の幕開けに向けた研究開発と実証」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．

■諸外国に比べて数年は遅れていると理解していた我が国の 5G に関する研究開発が 2020 年春の商用サービス本格展開の準備として，3 年間の実証実験を実施し，技術検証やさまざまなユースケースの有益性について慎重に確認を行ってきていることを知り，有意義であった．（匿名希望）

■ 5G を特集されたのは時宜を得ていると思う．世界的にも注目されている中，国際動向，我が国の位置づけなどの解説が欲しかった．せっかく各分野の専門家が執筆されているだけに残念．（中島一郎）

■ボリュームがあり見応えがありました．利用者視点からの記事も増えるとよいと思います．（匿名希望）

■「eMBB」，「URLLC」，「mMTC」という環境がハードで，サービスがソフトと考えると，環境を使い切るようなソフトがまだ，日本では見えていないように思える．今回の特集は，今の環境で動くサービスのカタログと感じた．驚くようなサービスの出現と，実現のための研究，課題解決に期待する．（匿名希望）

■少し難しかったです．（匿名希望／ジュニア会員）

教育コーナー「ぺた語義」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．

ぺた語義：高校における新教科「情報」ができたころのこと

■背景が分かりやすく書かれていた．（匿名希望）

連載「情報の授業をしよう！：東京都立石神井高等学校での情報の授業」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．

■すぐに授業に活かせる実習例が端的に書かれていて，役立ちます．（匿名希望）

連載「5 分で分かる !? 有名論文ナナメ読み：Jacob Devlin et al. : BERT : Pre-training of Deep Bidirectional Transformers for Language Understanding」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．

■深層学習関連の記事はいつも途中で分からなくなるのですが，どこがブレークスルーなのか，具体的にどういう仕組みにしたのか，分かりやすかったです．（匿名希望）

■機械翻訳，質問応答，評判分析に関するブレークスルーの要点が理解でき有意義だった．（匿名希望）

連載「IT 紀行：難しくて理解不能 !?　第 61 回プログラミング・シンポジウムに行ってみた！」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．

■左ページの左側がスタートになり，読みやすくなりました．（匿名希望）

■ IT 紀行はせっかくイラストを採用しているので，先生方の特徴を捉えた似顔絵だけでなく説明にも直感的に分かるようなイメージを期待します．グラフィックレコードという技法があるので参考にされるとよいのではないでしょうか．（滝内邦弘）

連載「先生，質問です！」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．

■ロボット訓練士とサイボーグ技工士のお話が面白かったです！（匿名希望）

■会誌の「先生，質問です！」が，「『先生，質問です！』公開セッション」として全国大会で公開されたのは，親しみが増すきっかけとなり，よかった．（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．

■過去に掲載された記事のアップデート情報．（匿名希望）

■時事的なテーマについての記事を読みたい．（匿名希望）

■動画での解説コンテンツ．アニメーション等で理解しやすくなることを期待．（匿名希望）

■記事が検索できるとよいです．（匿名希望）

■フィードバックや改版ができる記事，双方向コンテンツなど．（匿名希望）

■ジュニア向けのプログラミング教育記事と，そのプログラミング環境とのリンクや，作ったユーザアプリの公開と相互コメントがあると面白そうです．（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．

■ビブリオ・トーク―書評―のジュニア会員版のコーナーを作ってほしいです．（匿名希望／ジュニア会員）

■コロナウイルスの影響でさまざまなイベントがオンライン開催となっております．現場の対応で苦労した点などをご紹介いただけたらと思います．（匿名希望）

■なぜデマが広まるのかを取り上げてほしいです．（匿名希望／ジュニア会員）

■台湾のオードリータン大臣にインタビューしてほしい．（角田洋太郎／ジュニア会員）

■応用数学に利用されているコンピュータの種類，適用分野等関係する諸々の事柄をお願いいたします．（匿名希望）

■量子コンピュータや 5G は，人間が最も苦手とする「待つこと」へのストレスを飛躍的に解消してくれると期待しています．現在，世の中は新型コロナウイルスで大混乱．特効薬の開発など，「待つこと」の課題は尽きません．日本が誇る ICT の総力をあげて，世界にお手本を示したいものです．（匿名希望）

■ Processing で文字を出す方法を教えてほしいです．専門用語の解説があるともっと分かりやすいです．（神長春花／ジュニア会員）

■高大接続教育に興味を持っております．特に情報分野について．新学習指導要領に備え，どのような変革が期待されているか（特に大学側）．（匿名希望）

■読みたくなる解説とか概要が目次に入っていると，興味のある記事に出会えてよいと思いました．（匿名希望）

■新型コロナウイルスに対する情報技術の取り組み（東京都の感染状況 BI ツール等），全国大会のチャレンジも読んでみたいです．（匿名希望）

【本欄担当　伊藤将志・欅　惇志／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

IPSJ 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 でご確認いただきますよ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
	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「快適な運用管理を支えるインターネットと運用技術」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-F.html	6月8日（月）		
	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）		
5月14日（木）～ 5月15日（金）	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 https://www.ipsj.or.jp/kenkyukai/event/cvim222.html	3月6日（金）	当日可　要申込 （マイページにて 受付予定・準備中）	★オンライン開催
5月14日（木）～ 5月15日（金）	第111回グループウェアとネットワークサービス・ 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	3月11日（水）	当日可　要申込 （マイページにて 受付予定・準備中）	★オンライン開催
5月14日（木）～ 5月15日（金）	第89回コンピュータセキュリティ・ 第49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	3月13日（金）	当日可　要申込 （マイページにて 受付予定・準備中）	★オンライン開催
5月15日（金）	北陸支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			富山大学 五福キャンパス
5月19日（火）	関西支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			大阪市中央公会堂
5月20日（水）	中国支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			広島YMCA 国際文化センター
5月21日（木）	東海支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			★書面開催
5月21日（木）	九州支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			★オンライン開催
5月22日（金）	北海道支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			北海道大学
5月25日（月）～ 5月26日（火）	第66回ユビキタスコンピューティングシステム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ubi66.html	4月6日（月）	当日のみ	慶應義塾大学 殿町タウンキャンパス(予定)
5月27日（水）	第25回デジタルコンテンツクリエーション研究発表会 http://www.ipsj.or.jp/sig/dcc/	4月28日（火）	当日のみ	中京テレビ本社 （愛知県名古屋市中村区）
5月28日（木）～ 5月29日（金）	第183回マルチメディア通信と分散処理・ 第95回モバイルコンピューティングとパーベイシブシステム・ 第81回高度交通システムとスマートコミュニティ合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/dps183mbl95its81.html	4月9日（木）	当日可　要申込 （マイページにて 受付予定・準備中）	★オンライン開催
5月28日（木）～ 5月29日（金）	第149回システムソフトウェアとオペレーティング・システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/os149.html	4月16日（木）	当日のみ	那覇市IT創造館
5月29日（金）～ 5月30日（土）	第31回教育学習支援情報システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/cle31.html	4月9日（木）	当日のみ	京都工芸繊維大学
6月1日（月）～ 6月2日（火）	第188回ヒューマンコンピュータインタラクション・ 第56回エンタテインメントコンピューティング合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/hci188ec56.html	4月10日（金）	当日可　要申込 （マイページにて 受付予定・準備中）	★オンライン開催
6月3日（水）	2020年度定時総会 https://www.ipsj.or.jp/topics/soukai20200603.html			学士会館
6月1日（月）～ 6月2日（火）	第129回プログラミング研究発表会 https://sigpro.ipsj.or.jp/pro2020-1/	5月1日（金）	当日のみ	筑波大学 計算科学研究センター
6月3日（水）～ 6月4日（木）	第109回オーディオビジュアル複合情報処理研究発表会 https://www.ipsj.or.jp/kenkyukai/event/avm109.html	4月15日（水）	当日のみ	函館コミュニティプラザ Gスクエア
6月4日（木）～ 6月5日（金）	第88回電子化知的財産・社会基盤研究発表会 https://www.ipsj.or.jp/kenkyukai/event/eip88.html	4月15日（水）	当日のみ	立教大学 太刀川記念館
6月6日（土）	第152回情報システムと社会環境研究発表会 https://www.ipsj.or.jp/kenkyukai/event/is152.html	4月13日（月）	当日のみ	青山学院大学 青山キャンパス
6月6日（土）	第123回人文科学とコンピュータ研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ch123.html	4月15日（水）	当日のみ	亜細亜大学
6月6日（土）～ 6月7日（日）	第127回音楽情報科学・第132回音声言語情報処理合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/mus127slp132.html	4月3日（金）	当日のみ	ヤマハ本社事業所（浜松）
6月10日（水）	東北支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			東北大学　青葉山キャンパス
6月12日（金）	四国支部報告会 https://www.ipsj.or.jp/annai/shibu/shibu_tayori2020.html			愛媛大学
6月24日（水）～ 6月26日（金）	マルチメディア、分散、協調とモバイル（DICOMO2020） シンポジウム http://dicomo.org/	3月20日（金）		ロイヤルホテル土佐 （高知県安芸郡）
6月25日（木）～ 6月26日（金）	第54回組込みシステム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/emb54.html	5月14日（木）	当日のみ	東京工業大学 大岡山キャンパス
6月27日（土）	第44回ゲーム情報学研究発表会 https://www.ipsj.or.jp/kenkyukai/event/gi44.html	5月18日（月）	当日のみ	佐世保工業 高等専門学校
6月29日（月）～ 7月1日（水）	第128回数理モデル化と問題解決・ 第62回バイオ情報学合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/mps128bio62.html	5月8日（金）	当日のみ	琉球大学50周年記念館

7月10日（金）	第50回インターネットと運用技術研究発表会 https://www.ipsj.or.jp/kenkyukai/event/iot50.html	5月15日（金）	当日のみ	アクロス福岡
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1日（火）～ 9月2日（水）	第110回オーディオビジュアル複合情報処理研究発表会 https://www.ipsj.or.jp/kenkyukai/event/avm110.html		当日のみ	北海道大学 札幌キャンパス
9月1日（火）～ 9月3日（木）	FIT2020 第19回情報科学技術フォーラム https://www.ipsj.or.jp/event/fit/fit2020/			北海道大学 札幌キャンパス
9月2日（水）～ 9月4日（金）	The 15th International Workshop on Security（IWSEC 2020） https://www.iwsec.org/2020/index.html	3月23日（月）		Happiring Hall and Fukui International Activities Plaza, Fukui, Japan
9月7日（月）～ 9月9日（水）	DAシンポジウム2020―システムとLSIの設計技術― http://www.sig-sldm.org/das/			鳥羽シーサイドホテル
9月10日（木）～ 9月12日（土）	ソフトウェアエンジニアリングシンポジウム2020（SES2020） https://ses.sigse.jp/2020/			株式会社日立製作所 横浜研究所
9月26日（土）～ 9月27日（日）	2020年度（第73回）電気・情報関係学会九州支部連合大会 http://www.jceee-kyushu.jp/	7月8日（水）	講演・参加など申込受付は6月8日より	九州産業大学
10月28日（水）～ 10月30日（金）	The 13th International Conference on Mobile Computing and Ubiquitous Networking（ICMU2020） http://www.icmu.org/icmu2020/	5月20日（水）		機械振興会館

2021年

1月18日（月）～ 1月21日（木）	26th Asia and South Pacific Design Automation Conference（ASP-DAC 2021） http://www.aspdac.com/aspdac2021/	日本科学未来館

2020年度定時総会の開催について

会長　江村克己

2020年度定時総会を下記により開催いたします．総会の案内状は，5月中旬頃に法律上の社員である代表会員の方々にお送りいたします．ご欠席の場合には，必ず委任状をご返送ください．

なお，新型コロナウイルス感染症拡大を受け，開催方法の変更などの可能性がございますので，最新情報はWebでご確認いただきますようお願いいたします．

記

日　　時　2020年6月3日（水）15：00～16：45頃
会　　場　学士会館（〒101-8459 東京都千代田区神田錦町3-28）
次　　第　1. 2019年度に係る報告
2. 新名誉会員の推薦
3. 新役員の選任
4. 2020年度に係る計画（報告）
5. 会費滞納会員の取り扱い（報告）
6. 表彰（功績賞ほか）

照会先　一般社団法人情報処理学会管理部門

Webページ（https://www.ipsj.or.jp/）更新情報

［トピックス］

4月10日	日本学術振興会育志賞第11回（2020年度）推薦募集における本会からの推薦について
4月10日	学会著作物をICT人材育成のためのオンライン教育に無償で利用いただけます ～新型コロナウイルス感染症緊急事態宣言を受けてのオンライン教育等の利用拡大に向けて～
4月7日	新型コロナウイルス感染症の感染拡大防止に伴う緊急事態宣言による学会事務局業務等について
4月3日	新型コロナウイルス感染症の影響による学会事務局業務等について
4月3日	インターンシップ情報（広告）のお申し込み受付中
4月1日	［プレスリリース］2020年度認定情報技術者（CITP）企業認定の審査日程のお知らせ
4月1日	代表会員名簿（2020年度）
4月1日	2020年度シニア会員申請のご案内（締切：7/31迄）
3月30日	FIT2019の講演申込を開始しました
3月30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
3月28日	2020年度役員改選の投票結果について
3月27日	子供たち（小中高校生）の自宅学習支援プロジェクト
3月26日	高等学校共通教科情報科の大学入学共通テストでの実施に関する意見
3月26日	［プレスリリース］認定情報技術者（CITP）企業認定において リコーITソリューションズを認定
3月25日	「数理・データサイエンス・AI（リテラシーレベル）モデルカリキュラム～データ思考の涵養～（案）」への意見

人材募集
（有料会告）

有料会告

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

申込期限：毎月 15 日を締切日とし翌月号（15 日発行）に掲載します．

掲載料金：国公私立教育機関，国公立研究機関　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

■国立天文台研究教育職員（情報セキュリティ室講師）

募集職種　研究教育職員　講師　1 名
所　　属　国立天文台情報セキュリティ室
専門分野　情報通信技術（ICT）または関連分野
応募資格　博士号取得者
着任時期　採用決定後なるべく早い時期
提出書類（英文にて提出すること）　（応募書類の詳細な条件について，国立天文台採用情報 <https://www.nao.ac.jp/en/contents/job-vacancy/job-20200323-itso.pdf> を必ずご確認ください）
(1) カバーレター，(2) 履歴書，(3) 論文リスト（SPIE と COSPAR を含む査読論文とその他を区別すること．特許についても記載のこと），(4) 国際共同研究を含む研究歴，(5) 本職に対する抱負，(6) 応募者とその直属の上司の連絡先（E-mail アドレスと電話番号），(7) 評価書 3 通以上
応募締切　2020 年 6 月 15 日（17:00（JST））
提 出 先　国立天文台求人公募システム < https://jobregister.nao.ac.jp/ >
照 会 先　E-mail: JobRegister-contact-10@nao.ac.jp
そ の 他　応募前に提出書類欄に記載のURLを必ずご覧ください

■上智大学理工学部情報理工学科

募集人員　助教　1 名（5 年任期，ただし昇任の可能性あり）
専門分野　ヒューマンデータサイエンス，画像処理工学，AI（ロボティックス関連も含む），ブレインマシンインタフェース（人間の知的情報処理や人間にかかわるあらゆるデータ処理等に関する研究および教育ができる方）
担当予定科目　学科基礎科目，ゼミナール，卒業研究指導のほか，専門分野に応じて，機械学習・ニューラルネットワーク，画像処理工学，生体医工学，ヒューマンコミュニケーション等から数科目．また，Applied Computer Science，研究論文指導を含む大学院科目等
応募資格　博士または Ph.D を取得済み，または着任までに取得見込みであること．その他については下記 Web ページをご覧ください
着任時期　2021 年 4 月 1 日
応募締切　2020 年 6 月 30 日（必着）
送 付 先　〒 102-8554 東京都千代田区紀尾井町 7-1
上智大学理工学部長　陸川政弘
照 会 先　〒 102-8554 東京都千代田区紀尾井町 7-1
上智大学理工学部情報理工学科長　澁谷智治
E-mail: dp-icses-ofc@sophia.ac.jp　Tel(03)3238-3320
そ の 他　詳細については，上智大学公式 Web ページ (https://www.sophia.ac.jp/jpn/info/employment/DIC_202003.html) をご覧ください

■九州工業大学大学院情報工学研究院 生命化学情報工学研究系

募集人員　（女性限定公募）助教　1 名
（任期：採用日から 5 年間　テニュアトラック制度を適用）
専門分野　バイオインフォマティクス
着任時期　2020 年 9 月 1 日以降の早い時期
応募締切　2020 年 7 月 10 日（必着）＊応募書類は郵送のみ受付
照会先／送付先　〒 820-8502 福岡県飯塚市川津 680-4
九州工業大学大学院情報工学研究院生命化学情報工学研究系
系長　倉田博之
E-mail: kurata@bio.kyutech.ac.jp　Tel(0948)29-7828
そ の 他　URL：http://www.iizuka.kyutech.ac.jp/lab/index5
【勤務地】飯塚キャンパス：福岡県飯塚市川津 680-4
【給与】「テニュアトラック制度（採用日から 5 年間）での雇用期間」および「テニュア審査後に任期なしとして雇用された後」ともに，国立大学法人九州工業大学における第二期年俸制適用教育職員の給与に関する規程による
【勤務時間】専門型裁量労働制
詳細は，https://bio.iizuka.kyutech.ac.jp/news/2020/0413-502.html を参照

■東京都市大学メディア情報学部情報システム学科

募集職種　教授または准教授，あるいは講師（常勤／任期付き・テニュアトラック）
募集人員　a. システムデザイン　1 名　b. ICT アセスメント　1 名
着任時期　2021 年 4 月 1 日
専門分野　a. ソフトウェア工学，システム開発，プロジェクトマネジメント，要求工学，サービス工学
b. 経営情報システム，ICT アセスメント，ICT マネジメント，IT サービス，組織管理
応募締切　2020 年 8 月 31 日（必着）
そ の 他　詳細：東京都市大学採用情報　メディア情報学部情報システム学科　https://www.tcu.ac.jp/recruitinformation/

IPSJ MAGAZINE Vol.61 No.6 (June 2020)

CONTENTS

Preface

546 **A Modest Contribution to Democracy from a City that Can See the World's Tomorrow**
Tatsuo IGARASHI (Mayor of Tsukuba)

Special Article

548 **Report on On-line Holding of the 82nd National Convention**
Yasuo OKABE (Steering Committee Chair of the 82nd National Convention / Kyoto Univ.) and Minoru NAKAZAWA (Program Committee Chair of the 82nd National Convention / Kanazawa Institute of Technology)

552 **How can We Introduce and Manage Hospital Information Systems - Analaysis of Uda City Hospital Case**
Tomohiro KURODA (Kyoto Univ. Hospital)

Special Features

Latest Trends in on Hardware Security

558 **0. Foreword**
Tsutomu MATSUMOTO (Yokohama National Univ. / National Institute of Advanced Industrial Science and Technology (AIST)), Takayuki SASAKI (NEC /Yokohama National Univ.) and Masaki ISHIGURO (Mitsubishi Research Institute, Inc.)

560 **1. Physical Attacks on Hardware**
Naofumi HOMMA and Rei UENO (Research Institute of Electrical Communication, Tohoku Univ.)

564 **2. Hardware Acceleration of Cryptographic Processing**
Junichi SAKAMOTO and Naoki YOSHIDA (Yokohama National Univ.)

568 **3. Hardware Trojan Threats and Its Detection Methods**
Yuichi HAYASHI (Nara Institute of Science and Technology / National Institute of Advanced Industrial Science and Technology (AIST)) and Shinichi KAWAMURA (National Institute of Advanced Industrial Science and Technology (AIST))

572 **4. Instrumentation Security**
Tsutomu MATSUMOTO and Daisuke SUZUKI (National Institute of Advanced Industrial Science and Technology (AIST))

576 **5. System Hardening by Trusted Execution Environment**
Kuniyasu SUZAKI (Technology Research Association of Secure IoT Edge Application Based on RISC-V Open Architecture (TRASIO) / National Institute of Advanced Industrial Science and Technology (AIST)) and Takayuki SASAKI (NEC Corp. / Yokohama National Univ.)

580 **6. Basics of Automotive Cybersecurity (Automotive Networks and Exploitation Examples)**
Camille GAY (National Institute of Advanced Industrial Science and Technology (AIST))

Differential Privacy

584 **0. Foreword**
Mikiko SODE TANAKA (International College of Technology)

586 **1. Data Privacy Preserving Technologies and Differential Privacy**
Ryo FURUKAWA (NEC)

591 **2. Differential Privacy**
Masayuki TERADA (Research Labs., NTT DOCOMO, Inc.)

600 **3. Recent Advances in Local Differential Privacy**
Kazuto FUKUCHI and Jun SAKUMA (University of Tsukuba / RIKEN AIP)

ET RoboCon : A Unique Robot Contest of Software Design for Embedded Technology - Interviews with Shining Students -

608 **0. Foreword**
Takashi HIRAYAMA (Iwate Univ.)

610 **1. ET RoboCon as an Opportunity of Software Education and Practice - Modeling Exercise to Fit Current Engineering Needs -**
Yuki TSUCHITOI (Fuji Xerox Co., Ltd.)

614 **2. An Interview with KAMOGAWA**
Kosuke KONISHI, Kako UCHIDA, Taro KOBARA, Luca TAKETOSHI (Kyoto Prefectural Kyoto Technical Institute) and Takashi HIRAYAMA (Iwate Univ.)

617 **3. An Interview with Ganchan+X**
Koki KAINUMA, Yusuke SANO, Takafumi MAKI , Tanami YAMAUCHI (Graduate School of Iwate Univ.) and Takashi HIRAYAMA (Iwate Univ.)

Article

620 **Can Delegation Agreements Promote Agile Software Development? - Challenges for Agile Adoption of Ordering Companies -**
Kumi JINZENJI (NTT Corp., NTT Software Innovation Center)

"Peta-gogy" for Future

627 **On the Learner's Device Assigned to Each Child One by One**
Yoichiro MOCHIZUKI (Oita Prefectural College of Arts and Culture)

628 **Public Lecture of Cyber Security Exercise**
Kazutaka MARUYAMA (Meisei Univ.), Nobuhiko SASAKI (Stonebeat Security Inc.) and Hiroyuki TAKATANI (McAfee Co., Ltd.)

632 **Recommendation of Recursive Thinking**
Masaki NAKAGAWA (Tokyo Univ. of Agriculture and Technology)

Let's Learn Informatics

636 **Guidance in the Information Content Field in the Professional Subject "Joho"**
Tadashi NAGADOU (Okinawa Prefectural Mirai Technical High School)

557 **Shopping Boast**
607 **Gathering to Share Original Programming Projects for Junior**
642 **Biblio Talk**
644 **Skimming a Famous Paper in Five Minutes**
646 **IT Travelog Manga**

次号（7 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.

「特集」さようなら，パスワード付き ZIP メール
セキュリティシアター／ PPAP とはなにか―その発展の黒歴史―／ PPAP のセキュリティ意義／現代のカーゴカルト

「小特集」サイバー・ウォーズ
サイバー攻撃（国内外のサイバー攻撃の現状についての事例紹介）／機械学習とサイバーセキュリティ（機械学習等 AI 技術を用いたサイバーセキュリティの研究・運用の現状の総説）／安全保障と ICT（国内外の国際関係論的議論の総説）／海外の安全保障と ICT ／インテリジェンスと ICT（ロシアにおけるインテリジェンス，サイバー攻撃と技術について）／サイバー攻撃に関する国際法：タリン・マニュアルについて／座談会：サイバー戦争，フェイクニュースとエンジニア

教育コーナー：ぺた語義
連　載：IT 紀行／集まれ！ジュニア会員 !! ／買い物自慢／ 5 分で分かる !? 有名論文ナナメ読み／情報の授業をしよう！／先生，質問です！／ゼロからはじめるアルゴリズム／ビブリオ・トーク
コラム：巻頭コラム
会議レポート：SANER 2020 会議報告／バーチャル学会開催後記― VR 空間に見出す次世代の学会形式―

ご意見をお寄せください！

【6 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 6 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：「世界のあしたが見えるまち」から民主主義へのささやかな貢献を …… 10-1-［　］
特別解説：情報処理学会第 82 回全国大会　実録 緊急オンライン開催 …… 10-2-［　］
特別解説：電子カルテの安全な導入と運用…… 10-3-［　］
買い物自慢：3D プリンタのキットを買ってみた …… 10-4-［　］
特集：ハードウェアセキュリティの最新動向
0. 編集にあたって …… 10-5-［　］
1. ハードウェアに対する物理攻撃 …… 10-6-［　］
2. ハードウェアを用いた暗号処理の高速化 …… 10-7-［　］
3. ハードウェアトロージャンの脅威と検出 …… 10-8-［　］
4. 計測セキュリティ …… 10-9-［　］
5. Trusted Execution Environment によるシステムの堅牢化 …… 10-10-［　］
6. 自動車サイバーセキュリティの基本 …… 10-11-［　］
小特集：差分プライバシ
0. 編集にあたって …… 10-12-［　］
1. データプライバシ保護技術と差分プライバシ …… 10-13-［　］
2. 差分プライバシの基礎と動向 …… 10-14-［　］
3. 局所差分プライバシの最新動向 …… 10-15-［　］
連載：集まれ！ジュニア会員 !! …… 10-16-［　］
ミニ特集：ET ロボコン：異色の情報系ロボコン
0. 編集にあたって …… 10-17-［　］
1. ソフトウェア教育・実践の場としての ET ロボコン　…… 10-18-［　］
2. KAMOGAWA の訓練生にインタビュー …… 10-19-［　］
3. がんちゃん +X の学生にインタビュー …… 10-20-［　］
解説：準委任契約はアジャイル開発を促進できるか…… 10-21-［　］
ぺた語義：1 人 1 台学習者端末について考える…… 10-22-［　］
ぺた語義：実践的演習を伴うサイバーセキュリティ公開講座の取り組み…… 10-23-［　］
ぺた語義：再帰的思考のすすめ…… 10-24-［　］
情報の授業をしよう！：専門学科「情報科」における情報コンテンツ分野の指導 …… 10-25-［　］
ビブリオ・トーク：誰でもすぐに戦力になれる未来食堂で働きませんか　…… 10-26-［　］
5 分で分かる !? 有名論文ナナメ読み：Prévost, R. et al : Make It Stand : Balancing Shapes for 3D Fabrication…… 10-27-［　］
IT 紀行：全国大会がオンライン開催！　公開セッション「先生，質問です！」の裏側お見せします …… 10-28-［　］

〔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）テーマに興味が持てなかった　g）その他（下記に具体的にご記入ください）

〔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〕ハードウェアセキュリティの最新動向：a）専門家　b）非専門家 …… 13-1-［　　］
〔13-2〕差分プライバシ：a）専門家　b）非専門家 …… 13-2-［　　］
〔13-3〕ET ロボコン：異色の情報系ロボコン：a）専門家　b）非専門家 …… 13-3-［　　］

〔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，などご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ご感想，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, 短期セミナ, IT フォーラム, ソフトウエアジャパン, 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，アドバイザリーボード
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/

■ 編集室 ■

ハードウェアセキュリティの各領域の第一人者に多大なご尽力をいただき，本特集を完成させることができた．この場をお借りして，感謝を申し上げたい．ハードウェアレイヤは馴染みの薄い読者も多いと思われるため，本特集を編集するにあたり，各記事の著者と編集委員が協力して記事をブラッシュアップした．その結果，どの記事も分かりやすく，面白い内容になっていると思う．本特集が，情報処理の基盤となるハードウェアのセキュリティを理解する助けになれば幸いである．また，この特集をきっかけとして，ハードウェアセキュリティの研究領域と他の研究領域の境界で，研究者・技術者の間での交流や，コラボレーションによる新たな技術が生まれることを期待したい．

（佐々木貴之／本特集エディタ）

本小特集企画の始まりは，会議でポロっと発した「差分プライバシ」というワードが，編集委員の皆様にとって初耳で興味を持っていただけたことでした．差分プライバシ自体は特別新しい概念ではないですし，専門家の方からはいまさらな特集に見えるかもしれません．でも，さまざまな分野の研究者が集まっている編集委員の中でこの反応であれば，幅広い読者のいる情報処理で特集をしてもよいのではないかと思い企画をしてみました．未熟者ゆえ小特集ですけど．

さて，この小特集，著者の先生方を集めるに苦労をしました．というのも，国内で差分プライバシを解説していただくのに皆様が納得する人選というはなかなかないですから．ご多忙のため引き受けていただけないこともありますしね．一番の問題は私の人脈のなさだったりしますが……．結局のところ（私以外は）とても信頼のおける先生方にご執筆いただけたので，個人的にはとても読み応えのある小特集になったと思っております．なお，企画者本人である私が執筆したのは苦肉の策です．私の記事は専門家の方からは時代遅れで稚拙な内容に見えてしまう可能性を危惧してはおりますが，何とぞご容赦いただければ．

EU における一般データ保護規則（GDPR）の施行だったり，日本の個人情報保護法の再改正であったり，パーソナルデータの取り扱いは日に日に注意しなければならないようになってきています．でも，うまく活用できればとてつもなく有用かもしれないという期待は計りしれません．差分プライバシがすべてを解決してくれるとは思いませんが，今最も有望視されている研究対象だと思っています．本小特集で興味を持った方々がこの分野の研究に手を伸ばす１つのきっかけとなれば幸いです．

（古川　諒／本小特集エディタ）

ET ロボコンは異色の情報系ロボコンです．本会も協賛しており，毎年若手奨励賞を贈っています．本会誌で特集するのにピッタリの話題です．2019 年は，11 月にチャンピオンシップ大会が開催され，「KAMOGAWA」が若手奨励賞を受賞しました．そこで，この機会に ET ロボコンのミニ特集を企画することになりました．

ET ロボコンは，ロボットを自動制御する組込みソフトウェアの技術を競うコンテストです．全自動ロボットの競技ですので，人間が操縦することはありません．大学や高専などの学生チームだけでなく，名だたる企業の社会人チームも参加して，手加減なしのガチンコ勝負が繰り広げられます．このように，巷でイメージされるロボコンとはだいぶ様相が異なりますので，まずは概要説明が必要です．そのため，ミニ特集の筆頭記事として，ET ロボコン本部審査委員長に，ET ロボコンの特徴・狙い・ルールなどを中心に概説していただきました．

さて，本ミニ特集の企画にあたって何を狙いにしようかと考えたときに，本会が贈る賞の名前に入っている「若手」という言葉にピンときました．そうだ，若手チームを取り上げて，本会の学生会員やジュニア会員を元気づけることを特集の狙いにしよう，ということになりました．そのため，概要記事に続いては，優秀な成績により表彰を受けた学生主体の２チーム「KAMOGAWA」と「がんちゃん +X」に，ET ロボコンへの取り組みについて尋ねるインタビュー記事を掲載しています．彼ら光る若手の熱いメッセージが，読者の皆様の心に届きますように．

（平山貴司／本ミニ特集エディタ）

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 (JAC) 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 JAC (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

掲載広告カタログ・資料請求用紙

広告のお申込み

■広告料金表

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 6 号　掲載広告（五十音順）

□インタフェース …… 表 2　　□ すべての会社を希望
□講談社 …… 表 2 対向
□とめ研究所 …… 前付最終上

■資料送付先

フリガナ
お 名 前 ＿＿＿＿＿＿＿＿＿＿

勤 務 先 ＿＿＿＿＿＿＿＿＿＿ 所属部署 ＿＿＿＿＿＿＿＿＿＿

所 在 地 （〒　　-　　）＿＿＿＿＿＿＿＿＿＿

TEL（　　）　　-　　FAX（　　）　　-

ご専門の分野 ＿＿＿＿＿＿＿＿＿＿

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

賛助会員のご紹介

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

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

●●● 賛助会員（20 ～ 50口）

（株）日立製作所

富士通（株）

日本電気（株）

三菱電機（株）

（株）サイバーエージェント

日本アイ・ビー・エム（株）

●●● 賛助会員（10 ～ 19口）

（株）リクルート

グーグル合同会社

（株）NTT ドコモ

（株）東芝

日本電信電話（株）

日本マイクロソフト（株）

（株）フォーラムエイト

●●● 賛助会員（3 ～ 9口）

（一社）情報通信技術委員会

（株）NTT データ

グリー（株）

楽天技術研究所

（一財）インターネット協会

情報サービス産業協会

トレンドマイクロ（株）

NTT コムウェア（株）

NTT テクノクロス（株）

（株）うえじま企画

沖電気工業（株）

キヤノンマーケティングジャパン(株)

コアマイクロシステムズ（株）

三美印刷（株）

（株）セプテーニ

ソニー（株）

チームラボ（株）

（株）テクノプロ
テクノプロ・デザイン社

パナソニック（株）

みずほ情報総研（株）

2020 年度 情報処理学会シニア会員申請のご案内

本会は，2014 年度より情報処理分野において継続的な貢献が認められ，学会活動を通して本会の発展に寄与する正会員に対し，将来にわたって引き続き学会活動の中心となって，学会の発展，ひいては社会への貢献をいただくという趣旨のもと，「情報処理学会シニア会員制度」を設けております．

シニア会員の申請有資格者様におかれましては，本制度の内容をご確認の上，ぜひとも申請をいただき，本会シニア会員として今後もなお一層の積極的な学会活動，ご活躍をいただければ幸いです．多くの方からの申請をお待ちしております．

なお，「シニア会員」の称号取得は，2019 年度より「フェロー」推薦を得るための条件となりました．

2020 年度シニア会員申請および申請手続き要項

以下の要項をご確認の上，学会 Web サイト内のシニア会員 Web ページより，「シニア会員申請フォーム」に申請書類を添付して事務局までご送信ください．また，事務局シニア会員担当あて電子メール，および郵送での申請も受け付けております．

Web ページ	https://www.ipsj.or.jp/annai/aboutipsj/seniormember/seniormember.html
申請対象者	2020 年 4 月 1 日現在で**正会員として連続 5 年以上在会**の方が対象です． ＊年齢不問，学生会員としての在会期間は対象外です．
申請受付締切	**2020 年 7 月 31 日（金）まで**
申請書類	シニア会員申請書 1 通 シニア会員推薦書 2 通（推薦書は 2 名分必要です）
申請方法 （①～③いずれかの方法で申請してください）	申請は自己申告による申請と第三者申告による申請がございます（詳細は Web ページをご確認ください）． **■自己申告の場合の申請方法** **① Web サイト申請フォームから申請** 1. 上記 Web ページより「シニア会員申請書」をダウンロード，必要事項を記入してください． 2. 推薦者に該当する 2 名の方より「シニア会員推薦書」を入手してください． 3.「申請書」，「推薦書 1」，「推薦書 2」の順に計 3 ページ分を PDF にて 1 つのファイルにまとめてください． 4. 上記 Web ページ内の「シニア会員申請フォーム」に必要事項をご入力頂き，3. で作成したファイルを添付して受付期間内に申請してください． **② 電子メールで申請** soumu@ipsj.or.jp あてのメールに必要事項をすべて入力済みの「申請書」1 通，「推薦書」2 通を添付してお送りください． **③ 郵送にて申請** 事務局管理部門シニア会員担当へ必要事項をすべて記載した「申請書」1 通，「推薦書」2 通（いずれもサイズは A4 判）をお送りください． ①，②，③とも事務局にて受付後，受付完了メールを申請者・推薦者にお送りしますのでご確認ください． **■第三者申告の場合の申請方法** **【申告者（推薦者）】**第三者による申告の場合，申告者（推薦者）は次項 1 ～ 6 のいずれかに該当する本会員に限ります．また，申告者は推薦者の一人となります． **① Web サイト申請フォームから申請** **② 電子メールで申請** **③ 郵送にて申請** いずれも自己申請の場合と同様．
推薦者	推薦者は下記 1 ～ 6 のいずれかに該当する方です．2 名の方から推薦書をいただいてください（推薦者は上記 Web ページにて確認できます）． 1. 本会名誉会員　2. 本会フェロー　3. 本会役員及び役員経験者　4. 本会支部長及び支部長経験者　5. 本会研究会主査及び研究会主査経験者　6. 本会シニア会員
審査方法	申請書類に基づき，本会総務財務運営委員会で審査を行い，理事会へ諮ります． 【審査基準】本会関連分野の技術者，科学者，教育者，技術管理者で，連続して 5 年以上本会正会員として在会しており，本会の諸活動の支援および諸事業において，貢献が認められる方．
結果連絡	2020 年 10 月ごろ，申請書に記載のメールアドレスへ審査結果を連絡します（審査状況によっては日程が変更になる可能性があります）． 申請が認定された方は，本会 Web ページにお名前を掲載し，後日「シニア会員認定証」を会誌発送先の住所へお送りします．

申請・照会先：〒 101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F
情報処理学会事務局 管理部門 シニア会員担当
TEL：03-3518-8374　　e-mail: soumu@ipsj.or.jp

FIT2020 検索

2020 FIT

第 19 回情報科学技術フォーラム

https://www.ipsj.or.jp/event/fit/fit2020/

会期 2020.9.1 Tue. - 3 Thu.　**会場** 北海道大学 札幌キャンパス

主催 情報処理学会 (IPSJ)　電子情報通信学会 情報・システムソサイエティ (ISS) ヒューマンコミュニケーショングループ (HCG)

電子情報通信学会の情報・システムソサイエティ（ISS）とヒューマンコミュニケーショングループ（HCG）、および情報処理学会（IPSJ）は、今年も「第 19 回 情報科学技術フォーラム (FIT：Forum on Information Technology)」を開催します。
本フォーラムは、両学会の大会の流れをくみ、2002 年から毎年秋に開催されているもので、多くの研究発表や多彩な企画を通じて、広く情報科学技術分野にわたる最新情報の収集、タイムリーな情報発信、他分野研究者との交流、などのための絶好の機会となっております。

無料公開
2020
9.2(水) 午後

船井業績賞記念講演

半世紀を経て　いつでもどこでも CG 時代に

西田 友是　広島修道大学教授（東京大学名誉教授）／プロメテック CG リサーチ所長

講演募集

登録申込／投稿受付開始：2020年3月30日(月)
講演申込締切：2020年5月8日(金) 15:00
最終原稿送信締切：2020年6月19日(金) 15:00
※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 サイトよりお願いします。

講演種別

選奨論文　4~8 ページ程度

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講演形式で『選奨論文』を選択してください。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。2 次審査は FIT 終了後実施され、上位 3 名が船井ベストペーパー賞、次点数名が FIT 論文賞の受賞者となります。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。

一般論文　2~8 ページ程度

費用

会員	正員	10,000円	学生	6,000円
非会員	一般(社会人)	24,000円	学生	12,000円

※追加ページ代　3ページ目からは1ページあたり4,000円の追加費用が発生

聴講募集

事前予約受付期間(予定)：2020年5月15日(金)～7月10日(金)
(詳細はFIT2020 Webサイトに掲載致します)

費用

会員	10,000円(事前予約)	12,000円(当日)
一般非会員	20,000円(事前予約)	24,000円(当日)
学生	無料(論文集なし)	

問合せ先：一般社団法人 情報処理学会 事業部門［FIT2020 事務局］
〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F Tel: 03-3518-8373 Fax: 03-3518-8375
E-mail: ipsjfit@ipsj.or.jp

〒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(〇三)三五一八―八三七四
振替口座 〇〇一五〇―四―八三四八四
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

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　TEL.03-3367-0571 FAX.03-3368-1519
雑誌　05269-06
4910052690608
01600