2020年6月10日印刷　2020年6月15日発行（毎月1回15日発行）
ISSN 0447-8053

IPSJ MAGAZINE

情報処理

2020 7
Vol.61 No.7
通巻 664 号

特集　サイバー・ウォーズ

小特集　さようなら，意味のない暗号化 ZIP 添付メール

巻頭コラム

教科書通りじゃない情報処理，それが拡張現実
川田十夢

電子版もご覧ください
電子版を読む（会員無料）情報学広場
iPhoneなどで読む（有料）Kindle
電子版を購入（有料）Fujisan

教育コーナー：ぺた語義
連　載：IT 紀行／5 分で分かる!? 有名論文ナナメ読み／集まれ！ ジュニア会員!!／買い物自慢／ 古機巡礼 / 二進伝心／
　　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
会議レポート

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

Classembly Devices®

Interface Made in 日本

リスクに強い国内自社生産
無人遠隔地を任せられる性能を。

−40℃ 温度拡張 +70℃

広温度範囲とパフォーマンスを両立
Intel Atom E3950 (Apollo Lake) 搭載
車載 CD で、−40℃～+70℃、
省エネ CD で、−30℃～+60℃の広い動作温度範囲に対応

CAN・LAN×3 豊富な IO

車載 CD には CAN(ControllerAreaNetwork)/CAN FD×1 搭載
LAN×3 ポート , シリアルポート , 汎用入出力など豊富な IO を用意
USB3.0, USB2.0 も、トータル 4～6 ポート搭載

多様なディスプレイ出力

最新の多画面対応　DisplayPort v1.2に対応
現場で根強い要望のアナログRGBをはじめ、
DVI-D, HDMI 1.4b等、選択できます。

電源ブチ切り®～自動再起動

オンボードSSD, ソフトウェアのROM化, 電源ブチ切り®
ソフトウェアによる書き込み保護を実現　セキュリティにも強い
検証： 3000 回電源ブチ切り® 試験クリア

瞬低・電源電圧変動に強い

DC+6V～DC+37Vのワイドな電源入力
電源が安定しない車載用を中心に、さまざまな環境対応
不安定な電源環境下での連続運転や復電時の自動復旧に対応
瞬低対策用電源装置をオプション品として用意

車載CD用
型式:JPS-BUETCA

省エネCD用
型式:JPS-BUSTC

信頼性

耐振動性能:5G、耐衝撃性能:100G
コンプライアンス試験, ノイズ試験,
低温・高温起動試験, 電圧変動試験
温度サイクル試験
自社設備による各種EMC試験を行えます。

あらゆる現場に多彩なモデルを用意

無人環境・遠隔地での利用想定に加え、現場の声に応える多彩なモデルを用意

DOS モデルをラインナップ

Interface DOS System(日本語環境モデル), (ネットワークモデル)をラインナップ
これまでDOSを使用したシステムを使っているお客様のシステム移行や、
高いリアルタイム性を活かしたシステムを実現できます。
車載CDの他に「長期安心FAC」も6型式用意しております。

長期安心FAC
DOS搭載も
6モデル用意

DOS搭載車載CD
型式:STC-B018(J)
Intel Atom D525 搭載
CAN+DIOモデル
DOS日本語環境モデル
※在庫限り

車載 CD

A5サイズの薄型コンピュータ　車載 CD
HDDレス, FANレスで過酷な環境にも耐えられる耐環境性
広温度範囲−40℃～+70℃対応
CANを搭載し、車載での使用に最適

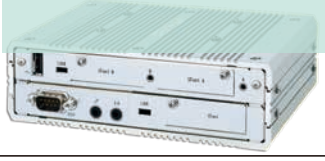
BOX 型モデル
ハードウェアRAID機能を搭載
計測制御, データロガーに最適

片面集中モデル
コネクタを片面に集中
狭所でのインタフェースケーブル取回し性が向上

省エネ CD

省エネ CD
はがきサイズ, 低消費電力の組込向け超小型コンピュータ
狭いスペースでも設置でき、堅牢, 無音で
耐振動・耐衝撃に優れ幅広い環境に対応

CFast3 スロットモデル
補助デバイスにCFastが3スロット搭載
大容量データ格納や
データの移動等に最適



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

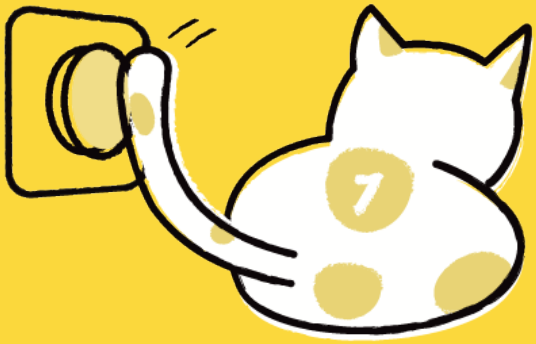
URL：www.interface.co.jp　E-mail：support@interface.co.jp

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-20-000431-01

第 11 回 OGIS-RI Software Challenge Award

一度だけつかえる
ソフトウェアコンテスト
～アナタガツカウノハドンナトキ～



あなたの自由で柔軟な発想で、これまでにないソフトウェアを考えてみてください。
みなさまのチャレンジをお待ちしています！

OSCA
OGIS-RI Software Challenge Award

第 11 回 OGIS-RI Software Challenge Award
一度だけつかえる ソフトウェアコンテスト
～アナタガツカウノハドンナトキ～

OSCA はオージス総研が主催する学生の方々を対象としたソフトウェアコンテストです。毎年異なるテーマを設定し、テーマと関連するソフトウェアのアイデアを募集します。

●応募内容
一度だけつかえるソフトウェア (IT システム) のユニークで革新的なアイデア

●審査のポイント
独創性／技術的な工夫／実現可能性／有用性（ビジネス / 社会）／面白さ（エンターテイメント性）

※ 審査は外部からお招きしたゲスト審査員と当社のメンバーが行います。

●応募資格
高校、高専、専門学校、大学、大学院の個人またはグループ

●開催スケジュール
エントリー　：6 月 11 日（木）～ 7 月 30 日（木）
応　　募　：7 月 31 日（金）～ 8 月 20 日（木）
一次審査結果通知　：　9 月 10 日（木）　← 一次審査と二次審査は書類審査です
二次審査結果通知　：10 月 15 日（木）
本選および表彰　　：11 月 10 日（火）　← 本選はプレゼンテーションによる審査です

●本選会場 ※
オージス総研 東京本社 会議室（JR 大崎 駅から徒歩 6 分）
※ 本選出場チームの本選会場までの交通費を 1 チーム 12 万円を上限として支給します
※ 新型コロナウイルスの感染状況によっては本選をオンラインで開催する場合があります

●賞
最優秀賞：50 万円、優秀賞：20 万円、ゲスト審査員賞：20 万円、他

※ コンテストの内容および規定は予告なく変更する場合があります。

オージス総研
株式会社オージス総研　OGIS-RI Co.,Ltd.
本社　：〒550-0023　大阪市西区千代崎 3 丁目南 2 番 37 号（ICC ビル）　TEL 06-6584-0011
東京本社：〒141-0033　品川区西品川 1 丁目 1 番 1 号大崎ガーデンタワー 20 階　TEL 03-6712-1211

2020 年度コンテストの詳細は下記をご覧ください。
コンテスト専用ウェブサイト
www.ogis-ri.co.jp/otc/contest/osca2020/

〔表 2 対向〕

7

PREFACE

巻頭コラム

662　教科書通りじゃない情報処理，それが拡張現実　川田十夢

SPECIAL FEATURES

特　集

サイバー・ウォーズ

664　0.　編集にあたって　長倉克枝・江間有沙
666　1.　攻撃対象領域の増大に伴い高度化する攻撃戦略　名和利男
672　2.　機械学習を用いたサイバーセキュリティ技術の発展　高橋健志・古本啓祐・韓　燦洙
678　3.　情報通信技術（ICT）と安全保障　佐藤丙午
687　4.　タリン・マニュアルについてーサイバー攻撃に関する国際法―　中谷和弘
693　5.　ロシアのインテリジェンス機関とICT　小泉　悠
700　6.　座談会：技術者とサイバー・ウォーズ―アルゴリズムやフェイクニュースが“兵器”に―
栗原　聡・鳥海不二夫・平　和博・須川賢洋／司会：長倉克枝・江間有沙

小　特　集

さようなら，意味のない暗号化ZIP添付メール

706　0.　編集にあたって―儀式セキュリティPPAP：日本のセキュリティ・ルネサンスに向けて―　崎村夏彦
708　1.　PPAPとはなにか―その発展の黒歴史―　大泰司章
714　2.　PPAPのセキュリティ意義　楠　正憲
719　3.　我々はなぜPPAPするようになってしまったのか　上原哲太郎
724　4.　座談会「社会からPPAPをなくすには?」　崎村夏彦・大泰司章・楠　正憲・上原哲太郎

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.7（2020 年 7 月号）
通巻 664 号

情報処理

教育コーナー：ぺた語義
735 新型コロナウイルスと中高生情報学研究コンテスト 中山泰一
736 教科「情報」・情報教育の担当者としてカリキュラム・マネジメントに参画する 田﨑丈晴
740 スリランカの初等中等情報教育 和田 勉

連載：ゼロからはじめるアルゴリズム
744 最初に考えること：何を行うのか 真鍋義文

連載：情報の授業をしよう！
748 小学校における ICT 活用の試行錯誤―教員によるソフトウェア開発を通して― 鍋谷正尉

753 連載：集まれ！ジュニア会員！！

連載：ビブリオ・トーク―私のオススメ―
754 センスメイキング 本当に重要なものを見極める力 上松恵理子

連載：5 分で分かる!? 有名論文ナナメ読み
756 Lee Organick et al : Random Access in Large-Scale DNA Data Storage 阪本哲郎・瀧ノ上正浩

連載：買い物自慢
759 子供とプログラミングで遊べるトイドローンを買ってみた 酒井 潤

760 連載：先生，質問です！

連載：古機巡礼 / 二進伝心
762 2019 年度情報処理技術遺産および分散コンピュータ博物館 旭 寛治

会議レポート
766 SANER 2020 会議報告 野田訓広・徳井翔梧
768 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― 亀岡嵩幸

連載：IT 紀行
780 ニコニコ学会βの逆襲!! これからのイノベーションの在り方を考えてみた 山本ゆうか

770 名誉会員の紹介
773 2019 年度功績賞
775 2019 年度論文賞／2019 年度業績賞
776 2019 年度情報処理技術研究開発賞／2019 年度マイクロソフト情報学研究賞／2020 年 IPSJ/ACM Award for Early Career Contributions to Global Research ／ 2020 年 IPSJ/IEEE-Computer Society Young Computer Researcher Award ／2019 年度優秀教育・教材賞／2019 年度学会活動貢献賞
777 2019 年度感謝状／2019 年度ソフトウエアジャパンアワード／2019 年デジタルプラクティス論文賞／2019 年度フェローのご紹介
778 論文誌ジャーナル掲載論文リスト／論文誌トランザクション掲載論文リスト
779 英文目次／次号予定目次
782 会員の広場
784 IPSJ カレンダー
786 人材募集
788 アンケート用紙
790 編集室
791 掲載広告カタログ・資料請求用紙
792 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：
五十嵐悠紀・井上 仁・江渡浩一郎・江間 有沙・大石 康智・大川 徳之・太田 智美・岡本 雅子・折田 明子・桂井 麻里衣・金子 格・川上 玲・河原 亮・久野 靖・欅 惇志・崎村 夏彦・須川 賢洋・袖 美樹子・高木 拓也・戸田 貴久・長倉 克枝・中島 一彰・西川 記史・坂東 宏和・細野 繁・堀井 洋・福地健太郎・坊農 真弓・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.

教科書通りじゃない情報処理，それが拡張現実

■川田 十夢

新型コロナウイルスの影響で，世界中の市民が先の見えない閉塞感に苛まれている．6月以降のあなたが，どのような心持ちで毎日を過ごしているのか．4月の私は，想像しながらこの原稿を書いている．

最初期は，飛沫感染の啓蒙になるような，目に見えない空気の流れを可視化するべきではないかと考えた．手を動かしてすぐ，悪い意味で無駄なことだと思いとどまった．ウイルス感染リスクがあることを自覚しながら，仕事場へ出かけなければならない人たちが膨大にいる．漫然とした閉塞感のなか，束の間の開放感を提供できるような，やがて根本的なルール変更につながるような，クリティカルな拡張現実を実装しないと私の存在価値はない．

申し遅れました．通りすがりの天才，川田十夢です．AR三兄弟という開発ユニットの長男を担当しています．ミシン会社で特許開発などに従事して10年，AR三兄弟として10年の月日が流れました．ARといえば，情報処理学会員のパイセンたちのおかげで現在があるのですが，エンタテインメント領域でさまざまな先行事例を数えたという意味では，若干の功績があるのだと思います．かの暦本純一さんからは，ラジオ番組出演の際「ARはAR三兄弟のものになった」と言っていただきました．もちろんサービストークだとは思いますが，真に受けるのが私の取り柄なのでございます．ここは気分良く，改ページと代えさせていただきます．

■川田 十夢
AR 三兄弟長男

1976 年生．開発者．AR 三兄弟．長男．通りすがりの天才．毎週金曜日 20 時から J-WAVE『INNOVATION WORLD』が放送中，『WIRED』で巻末連載．最新著作『拡張現実的』が発売中．

口調と論旨を元に戻す．有事に何を可視化するかが問われている．たとえば，電車の混み具合を可視化するのはどうか．平時であれば座れるかどうか程度のメリットだったが，有事のなか混雑を避けるのはすなわち命を守ること．累計データを元にした予測シミュレーションを提供するアプリは存在するが，有事である．予測では歯が立たない．電車に限らず，全国のリアルタイムな人口分布に紐付くビッグデータをお持ちの方がいたら提供してほしい．日本地図に，町々の混み具合や地域ごとの感染リスクを可視化，天気予報のように確認してから外へ出かけるよう呼びかけたい．病院への負担もいち早く軽減するべき．医師の経験を宿したAIをスマホで提供，それを介したオンライン処方箋，そして自宅までの配達を含む医薬品提供までの一貫サービスを合法化するべき．

不要不急の拡張だけでは息が詰まってしまう．シルク・ドゥ・ソレイユの団員たちが一時解雇されている．彼らの経験をモーションデータ化，売り物にして当事者へフィードバックする仕組みを作りたい．人混みの少なくなった近所で，あるいは自宅のテーブルで，拡張現実的なサーカスを存分に楽しめるよう整備したい．最新のiPadはLiDARスキャナを搭載．不断のドリフトや不十分なオクルージョンのせいで，夢から覚めることはない．有事以前から，サーカスではもう扱えなくなってしまった曲芸を披露する動物たちを登場させることもできる．閉塞感やルールを越えて見せてこその，拡張現実なのである．

特集
Special Feature

サイバー・ウォーズ

編集にあたって

長倉克枝　江間有沙 | 東京大学未来ビジョン研究センター

機械学習を中心とした人工知能（AI）技術が，国家安全保障やインテリジェンスといった分野でも活用が進みつつある．これはまさに「サイバーウォーズ（サイバー上の戦争）」であり，情報系の研究者や開発者も他人事ではない．普段考えることが少ないこれらの領域の現状と機械学習やロボティクス等の技術とのかかわりについて知っておくことは，研究者・開発者が社会に役立つ適切な研究開発に取り組む上で有用である．

このような問題意識のもと，情報技術がサイバー攻撃や安全保障でどのように利用され，どのような問題が起きているのかを知るため，編者らは2018年12月と2019年6月に「AIと安全保障／セキュリティ」をテーマに3回のセミナを開催した．本特集はセミナに登壇いただいた方々に執筆をお願いした．セミナ登壇者以外で本特集に寄稿いただいたのは中谷氏である．サイバー攻撃に焦点をあてた特集とするにあたって，国際法的な観点も重要であるため依頼し，ご快諾いただいた．

本特集は5編の解説と座談会からなる．名和氏による**「攻撃対象領域の増大に伴い高度化する攻撃戦略」**では，「サイバーフィジカル」などサイバー空間と実空間の一体化が進展する中で，サイバー脅威が発生，深刻化する要因を「攻撃対象領域」と「攻撃戦略」という2つの概念を用いて概説された．サイバー脅威主体へのモニタ活動を長らく行っている名和氏だからこその視点で，企業や国家の現状を的確に解説している．

続く高橋氏らによる**「機械学習を用いたサイバーセキュリティ技術の発展」**は，深刻化するサイバー攻撃への対抗手段として用いられる効率化・自動化された機械学習技術を解説している．フェイクニュースや自動運転のハッキングなどサイバー攻撃の対象が多様化するだけではなく，攻撃そのものが自動化されつつあることに対し，技術には技術で対抗をしていくという点で今後の展開が期待されるものである．

サイバー攻撃の範囲は，個人や企業だけではなく国家安全保障にまで及ぶ．佐藤氏の**「情報通信技術（ICT）と安全保障」**は1990年代以降，情報技術が

いかに軍事に用いられてきたかを概説している．特に，近年では人工知能が兵器システムの自律化が問題となっており，アメリカ，中国やロシアなど各国の軍事戦略も相まって国連で議論が行われている．軍事的効率性と人道規範を共存させるという難しい課題に現在，直面しているといえよう．

サイバー攻撃に関する国際法のルールを包括的に記述したものとして「タリン・マニュアル」がある．中谷氏は，2017 年に刊行された『サイバー攻撃に適用される国際法に関するタリン・マニュアル 2.0』の作成者の一人であり，解説書を 2018 年に刊行している．**「タリン・マニュアルについて―サイバー攻撃に関する国際法―」**は複雑化，多様化するサイバー空間におけるルール作りの難しさと深遠さを示してくれる一稿である．

サイバー攻撃やインテリジェンス機関の活動を考えるにあたって存在感のある国にはアメリカや中国などが挙げられるが，歴史的な観点からロシアの存在を無視できない．小泉氏による**「ロシアのインテリジェンス機関と ICT」**は，近年ますます存在感をましているロシアのインテリジェンス機関が，実際にどのようなオペレーションを展開しているのかの概要と具体事例を紹介している．2014 年のウクライナ危機は記憶に新しい人も多いだろう．

最後の座談会では，サイバー攻撃や安全保障上の問題に対し，研究者は何を心にとめて研究や議論していけばいいのか，論点の整理を専門家の方々（栗原氏，平氏，鳥海氏，須川氏）に行っていただいた．特に昨今ではフェイクニュースなども「兵器」と見なされるようになってきており，大学や民間企業の研究者にも安全保障の議論は他人事ではなくなっている．研究者の倫理観はどうあるべきなのかなどについて議論が展開された．

本特集が，研究開発を行っている読者の皆様，そして今後，情報系の研究開発に携わろうと考えている未来の研究者が社会との接点に思いを巡らすきっかけとなれば幸いである．

（2020 年 5 月 7 日）

［サイバー・ウォーズ］

①攻撃対象領域の増大に伴い高度化する攻撃戦略

名和利男 | サイバーディフェンス研究所

サイバーリスク・ランドスケープの限界

我が国における国家としてのサイバーセキュリティは，2018 年 7 月 27 日閣議決定により変更された「サイバーセキュリティ戦略」にある．この中で，戦略策定の前提として，サイバー空間がもたらす「恩恵」とこの空間における「脅威」の状況を的確に認識する必要があると言及している．一般に，サイバー空間における脅威は，大規模自然災害と異なり，人為的要素の占める割合が非常に大きい．そして，サイバー空間を利活用または実空間と一体化する領域は，拡大の一途をたどっており，それぞれの相互依存も増大している．そのため，リスクが複合的に重なり，多岐にわたる深刻なリスクを発生させており，時間の経過とともに大きく変動している．

このようなリスクを的確に認識する努力として，世界経済フォーラムにおけるグローバル・リスク・ネットワーク作業部会が，複合的なリスクを風景（ランドスケープ）として見渡そうとする試みをしており，2017 年に公表した「グローバルリスク報告書」において，サイバーリスクを組み込んだリスク・ランドスケープを示した．

しかし，サイバー空間と実空間の一体化が進展する中で，なぜサイバー脅威が発生するのか，どのようにしてサイバー脅威が深刻化していくのかなどを説明した見識は，技術的な観点で個別に分散しており，網羅的かつ客観的に示したものが少ない．政府機関から責任ある情報として公開された文書においても，かなり抽象的な表現にとどまっている．また，一般的なインターネット利用者は，漠然とした事例やサイバーリスクに関する情報を得られるようになってきているが，昨今のサイバー脅威に適合したセキュリティ意識と行動（対策）を変容させるような見識を十分に得られているとは言いがたい．

そこで，本稿において，一般的なインターネット利用者に昨今のサイバー脅威に適合したセキュリティ意識と行動（対策）に変容を与えることをねらい，筆者のサイバー脅威主体へのモニタ活動の経験から得られた「攻撃戦略（Attack Strategy）」と「攻撃対象領域（Attack Surface）」という 2 つの概念に基づいた状況認識を共有させていただく．まず，昨今の防衛企業に対する攻撃戦略を理解する上で象徴的な事例をいくつか紹介する．その上で，攻撃を増大させる大きな要因を IT 利活用の進展と照らし合わせて説明する．

攻撃戦略 (Attack Strategy)

実際の攻撃戦略の変化は，防衛関連組織に対するサイバー攻撃事例をレビューすることで，その一端を垣間見ることができる．

2016 年 オーストラリア

2016 年 11 月，オーストラリア国防省と契約する同国の Tier4（四次サプライヤ）レベルの防衛企業が不正アクセスに遭い，F-35 戦闘機，P-8 哨戒機，

C-130 輸送機，JDAM 誘導装置およびオーストラリア海軍の艦艇に関する技術情報が漏洩した．これらに「極秘」に該当する情報は含まれていなかったが，商業上重要な情報であり，国防や軍事に関する米国技術の輸出を管理する「ITAR（International Traffic in Arms Regulations)」によって「取扱注意」に指定されたものだった．不正アクセスを受けた防衛企業は，従業員は 50 名程度で，すべての IT システムを経験年数 9 カ月の担当者が一人で管理していた．また，同社のネットワークに緩衝領域（DMZ）が設けられておらず，定期的にセキュリティパッチを適用する保守体制も未整備であった．さらに，すべてのサーバにおいて共通の管理者 ID ／パスワードが使われ，多くのホストサーバがインターネットに接続した状態であった．オーストラリア国防省は，直接的なシステム被害はなかったが，サプライヤーである防衛企業に預けていた軍事関連情報が漏洩したことによる二次的被害が発生した．

2016 年 韓国

同年 10 月，韓国軍の Web サイトやイントラネットなどすべての IT サービスを統合管理する「国防統合データセンター（DIDC)」のネットワークに接続する 3,200 台の PC が不正アクセスを受けたことが発覚し，A4 用紙 1,500 万枚相当分の機密情報を盗まれた．この機密情報は，金正恩（キム・ジョンウン）朝鮮労働党委員長を殺害する「斬首作戦」とも言われる「作戦計画 5015」など，2 ～ 3 級の軍事機密が数多く含まれており，米軍から提供された機密資料や写真もすべて流出したと推定された．この主たる原因は，インターネット接続網と内部閉鎖網上の PC にワクチン（ウイルス対策ソフト）の検知パターンを配信する中継サーバが第三者に乗っ取られたことと，インターネット接続網と内部閉鎖網の両方に接続するファイル共有サーバ等が設置されていたことであった．つまり，攻撃ベクタは，ワクチン提供事業者というサプライヤを経由したものであった．

2016 年は，これら 2 つの防衛関連企業へのサイバー攻撃だけでなく，諸外国において多数発生した．その大半において「防衛関連組織に対するサプライチェーン攻撃」という共通性が見られた．

2017 年以降 日本

2016 年 12 月以降，防衛関連企業の NEC が不正アクセスを受けた侵入を受け，2017 年 7 月の外部との暗号通信の解読に成功するまで，内部サーバに保存されていたファイル 27,445 件への不正アクセスがされていたことが判明した．これらの情報には秘密情報は含まれていなかったが，潜水艦用センサの情報（海上自衛隊）など自衛隊装備に関連する資料が含まれていた．また，この侵入は，2014 年頃の地方の北陸地方の子会社の PC がマルウェア感染し，そこを起点に NEC 本社ネットワークに広がった可能性がある．

2019 年 3 月，同じく防衛関連企業の三菱電機の中国拠点において，ルータの脆弱性を通じて侵入され，ウイルス対策システムの管理サーバが侵害を受けて，そのアップデート機能を悪用したラテラルムーブメントが発生した．その後，この拠点で乗っ取られた海外アカウントが悪用され，国内拠点に侵入された上で，同様な手口でラテラルムーブメントが発生し，攻撃者の目的に合わせたように中間管理職の PC を標的にした攻撃が仕掛けられた．これにより，厳重な管理が求められる注意情報が外部に流出した可能性がある．

これら国内の 2 つの防衛関連企業に対するサイバー攻撃は，2016 年における韓国やオーストラリアをはじめとした諸外国の防衛関連企業に対する攻撃戦略から大幅に進展しており，「防衛関連組織グループ内の脆弱な外部拠点に対するサプライチェーン攻撃」になったと見ることができる．

攻撃戦略の進展

諸外国における防衛関連組織は，IT の利活用や

導入を進めており，そのグループの各拠点でも同様である．防衛企業の本社は，顧客（防衛省等）から直接的に影響を受ける形で，相応のコストとリソースをかけて，セキュリティ確保のための取り組みや新しい技術の導入が図られている．しかし，各拠点は，コストやリソースの制約があるため，喪失したセキュリティを取り戻すことが困難となるケースが目立っている．つまり，防衛関連組織グループ全体で，攻撃対象領域が増大しているのである．このため，攻撃戦略が進展したと考えられる．

攻撃対象領域（Attack Surface）

攻撃対象領域が増大している状況を，企業の情報ネットワークの変遷で説明する（図 -1）．

有線 LAN ベースのネットワーク

無線 LAN が一般に普及する前，企業における情報ネットワークは有線 LAN が主流だった．この有線 LAN は，物理的な配線が必要であるため，オフィスレイアウトに影響を受けていた．当時の日本企業の多くは，事務作業の能率的遂行のために最適化された配置として島型のレイアウトを採用し，1 つの課（事務機構の小区分）内での情報が行き渡りやすくさせる反面，複雑な階層構造の組織の中で課をまたぐ情報共有の必要性を少なくさせていた．そのため，有線 LAN のネットワークトポロジは，そのような島型レイアウトに影響を受ける形で，課単位でセグメント（ブロードキャストが届くネットワークの範囲）を分けていることが多かった．

このような情報ネットワークの環境にある PC がコンピュータ・ウイルスに感染した場合，課単位のセグメントというネットワークの壁を超えることが困難であるため，ラテラルムーブメント（偵察，認証情報の盗用，隣接 PC への侵入の攻撃プロセス）による被害拡大は限定的になる．つまり，ネットワーク構成の仕組みに，事実上のファイアウォール（ネットワークとネットワークの間に位置して不正アクセスをブロックするためのシステム）の機能が内在していたといえる．

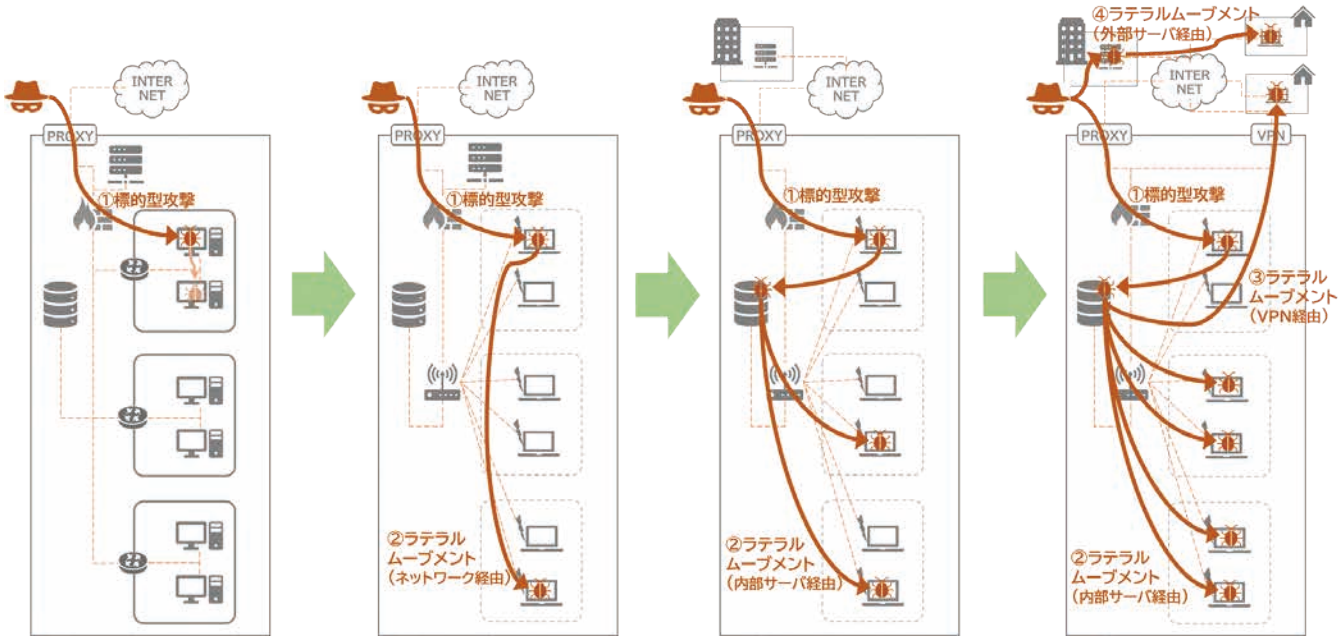


図 -1　企業ネットワークにおける利用形態の移り変わり

無線 LAN ベースのネットワーク

2000 年代中頃から，フリーアドレス（オフィスに社員の固定席を作らずに自由な席で仕事を行える仕組み）を導入する企業が増加したと同時に，一気に無線 LAN の普及が一気に進んだ．このフリーアドレスは，スペースコスト削減や社内コミュニケーションの活性化，自由な行動スタイルによる生産性の向上を期待したものとされてきたが，近年は，働き方の改革の一環として採用される一面もある．また，無線 LAN は，物理的な配線が必要なく，オフィスレイアウトに影響を受けないため，フリーアドレスとの親和性が高い．

ところが，有線 LAN の環境で得られたセキュリティ対策の機能は，無線 LAN を導入することでその一部を喪失した．最も大きなものが，オフィスレイアウトの物理的構成に影響を受けて実現していたセグメントである．これを無線 LAN で実現するには，ユーザのアクセス管理による論理的なセグメントを設けることになる．特に，フリーアドレス環境では，ユーザ権限を管理するための認証用のサーバを構築し，安定かつ厳格な運用を継続していかなければならないため，大きなコスト負担と労力が発生する．一部の企業は，フリーアドレスへの環境移行をコスト削減の一環で実施したため，新たに発生するセキュリティ対策のためのコストや労力をできるだけ避ける姿勢を持つ．現実的には，無線 LAN のセキュリティをパスフレーズによる単純なアクセス制御で運用するケースが少なくない．そのため，企業内の情報ネットワークのセグメントが複数の課をまたぐ，あるいは事実上消失してしまった．

このように，無線 LAN が急速に普及した過程の中で，セグメントの範囲を大幅に広げてしまった情報ネットワークの環境にある PC がコンピュータ・ウイルスに感染して，課をまたいでラテラルムーブメントを発生させた事例が散見されている．

Active Directory 中心のネットワーク

その後，企業の事業や人員の拡大，IT 依存の業務形態の定着，インターネットを通じたクラウドサービスの普及などにより，管理すべき PC の数が増加した．これにより，企業の IT 管理者の業務は膨大になり，IT に不慣れなユーザへのヘルプ業務が積み重なったため，IT 管理コストが大幅に増加した．これを解消する 1 つの手段として，Active Directory と呼ばれる「情報ネットワーク内の PC やユーザアカウントをまとめて管理できる機能」の利用をはじめた．この Active Directory が提供する主な機能は，情報ネットワーク内で使用する「ID・パスワードの管理」，「アクセス権限の設定・管理」，「ソフトウェアの設定・管理」，「USB メモリ等のメディア利用の設定・管理」，「プリンタなどの接続機器の設定･管理」，「Active Directory に関連したサーバに対する操作ログの取得」などである．これにより，企業，IT 管理者，ユーザに大きなメリットやコスト削減をもたらす一方，Active Directory に対する不正アクセスが発生すると，企業内のすべての PC が乗っ取られる，あるいはラテラルムーブメントによる甚大な感染拡大が発生するリスクを受け入れることになった．

さらにここ数年，企業は，オンプレミス（自社施設の構内に機器を設置してシステムを導入・運用する IT 情報基盤）あるいはホスティング（通信事業者などの専用の施設内に設置されたサーバにインターネットを通じて利用する IT 情報基盤）に要にかかわる運用・保守のコストやセキュリティにかかわる対策・管理・運用のコストを削減するために，IT 情報基盤そのものを MSP（マネージド･サービス・プロバイダ）と呼ばれる「顧客の利用する PC・サーバやネットワークなどの IT 情報基盤の運用・監視・保守などを行い，利用可能な状態を維持するサービスを提供する事業者」に委託する傾向が見られる．

このような企業の IT 管理の変化により，自社内

のIT情報基盤の管理におけるソフトウェアへの依存度が急激に高まり，さらに自社の指揮命令関係にない第三者にIT情報基盤の管理を委託するという形態が作られた．つまり，自社の責任で直接的にセキュリティコントロール可能な領域を大幅に喪失したことになる．特に，使用しているソフトウェアに脆弱性が発見され，侵害可能な状況が発生した場合，それを解決するためのセキュリティパッチの作成は，そのソフトウェアの開発元が行う．つまり，使用しているソフトウェアに脆弱性が発見された場合，企業は回避策を講じながら，セキュリティパッチが適用されるまで，待つことしかできないのである．

2018年12月，外務省が「中国を拠点とするAPT10といわれるグループによるサイバー攻撃について」というタイトルの報道官談話を発表した．このAPT10の攻撃ベクターは，MSPのネットワークに侵入し，顧客である企業のデータ窃取やネットワークに侵入することである．つまり，攻撃者は，企業に直接攻撃をせず，委託先（MSP等）を経由して攻撃を仕掛けることができるようになってきたのである．

VPNネットワーク

2020年2月頃から，国内において新型コロナウイルス感染症対策の1つとして，テレワーク（リモートワーク）を緊急導入する企業が急増した．テレワークは，自宅利用型テレワーク（在宅勤務），モバイルワーク，施設利用型テレワーク（サテライトオフィス勤務等）といった種類があり，社内の情報ネットワーク上のサーバに安全に接続するためには，VPN（インタネット上の仮想的な専用線）の利用が必要となる．VPNは基本的に一度ユーザがIDとパスワードで認証が成功すると，通信接続が継続する．つまり，つなぎっぱなしの状態になる．そのため，テレワークでマルウェアに感染したPCがVPNを通じて社内の情報ネットワークに接続すると，他のPCに対するラテラルムーブメントによるマルウェア感染の被害を発生させる可能性がある．これは，社内の情報ネットワークとインターネット間の境界防衛により実現していたセキュリティの一部を喪失したことを意味する．

実際に，VPNに関連したセキュリティインシデントが増加してことを受けて，2020年3月，米国国土安全保障省のCISA（サイバーセキュリティ・インフラストラクチャセキュリティ庁）が，新型コロナウイルス対策に伴うテレワークのVPN利用について，企業にセキュリティ上の注意喚起を行った．

攻撃対象領域の増大

近年，日本は，少子高齢化による労働人口の減少という社会環境の要因に加え，経済のいっそうのグローバル化の進展に伴う国際競争力の激化により，企業の生産性向上が重要課題となっている．これを受けて，多くの企業は，生産性向上とともに，コスト削減も期待できるITの利活用や導入が加速度的に進んでいる状況である．しかし，この過程において，企業の情報ネットワークや仕組みで得られていたセキュリティの一部が喪失していることの認識は十分ではない．それ故，喪失したセキュリティを取り戻すための取り組みや新たな技術の導入の必要性に対する理解が十分に得られない．一部ではいまだに，意思決定層がコストや人的リソースを増やすことに対する費用対効果を求めるという不条理を作り出しているため，レベルの低くなったセキュリティ状態が継続する．新たなITの利活用や導入を積み重ねていくたびに，セキュリティレベルをさらに押し下げているのである（図-2）．

このような状況を観察している攻撃側は，標的となり得る企業が攻撃対象領域を自ら増大させていると見ている．この攻撃対象領域とは，主にソフトウェア環境を攻撃対象として許可されていない第三者（攻撃者）が当該環境にデータを入力する，あるいはデータを抽出することを可能とするさまざまな

ポイント（攻撃ベクタ）の総計のことである．企業における攻撃ベクタは，多くなればなるほど組合せの数が指数関数的に増えるため，その組合せにより作られる攻撃戦略は複雑化かつ多様化する．結果として，攻撃側は，標的とした企業に対する攻撃目標の達成を容易にすることができるようになり，その規模を拡大させている．

企業が，このような悪循環が発生していることを自ら認識し，喪失しているセキュリティを確実に取り戻すための取り組みや新しい技術の導入を図り，その効果測定を徹底していかなければ，今後のサイバー攻撃による被害は，ますます甚大化していくことになる．

意思決定層の正常性バイアス

現在，企業の事業活動の推進において，サイバーセキュリティの戦略が必須となってきている．その戦略策定の前提として，意思決定層が「リスクを的確に認識」することが必要不可欠である．ところが，意思決定層の一部に，認識すらできていない，あるいはそれを避けようとする姿勢を持つ者が存在する．また，意思決定層を補佐する周辺の幹部社員が，意思決定層の認識レベルを向上させようと，多大な労力とコストをかけて努力しているが，彼らにとっての上位者にあたる意思決定層の認識や行動を変容させることは容易なことではない．特に，「現場」のサイバーセキュリティ対策に従事する者にとっては，サイバー攻撃への対処そのものより，意思決定層の低い認識による悪影響のほうが厄介で難儀なものとなってきている．

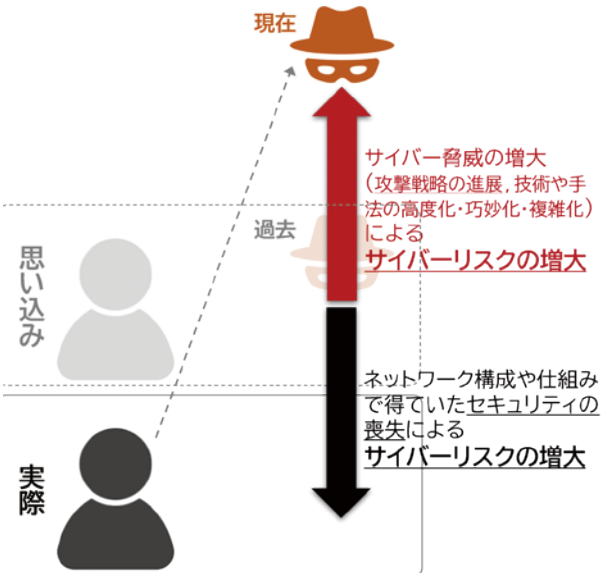


図 -2　思い込みに起因するサイバーリスクの増大

数年前から，国内のさまざまな領域でサイバーセキュリティ人材の育成事業が活発に行われているが，素晴らしい技術や知見を習得した彼らを活躍させる職場環境の整備やキャリアパスはいまだ十分とは言えない．さらに，意思決定層は，コストやリソースを必要とする取り組みや新しい技術の導入の重要性を訴える「現場」に寄り添う姿勢は，皆無に近い．

つまり，実際のサイバーセキュリティのレベルを押し下げているのは，「攻撃者の悪意のある行為」に加え，「意思決定層における正常性バイアス」と言える．正常性バイアスとは，自分にとって都合の悪い情報を無視したり，過小評価したりしてしまう人の特性である．

本稿では，主に「攻撃戦略（Attack Strategy）」と「攻撃対象領域（Attack Surface）」という 2 つの概念に基づいた状況認識を共有した．私たちは，サイバーリスクを増大させている要因の 1 つに，防御側の意思決定層によるリスク認識の不足に起因するセキュリティ低下があることを明らかにする必要がある．そして，意思決定層は，自らのリスク認識の不足が技術以上の喫緊の課題となっていることを受け入れ，今すぐに喪失し続けているセキュリティを取り戻す行動に着手しなければならない．

（2020 年 3 月 29 日受付）

名和利男　nawa@cyberdefense.jp
1971 年，北海道生まれ．航空自衛隊等を経て，2009 年にサイバーディフェンス研究所に参加．現在，宇宙システムや核物質防護を含めた重要インフラ領域におけるサイバー脅威対処や能力構築のためのサイバー演習に専念．

［サイバー・ウォーズ］

② 機械学習を用いたサイバーセキュリティ技術の発展

高橋健志　古本啓祐　韓　燦洙　情報通信研究機構

求められる自動化技術

増加するサイバースペース上の脅威に対応するためには，脆弱性管理やマルウェア分析をはじめ，さまざまなセキュリティオペレーションを実施する必要がある．しかしながらそれを十分に実現するのに必要な人的リソースは不足しており，その拡充およびオペレーションの効率化・自動化が必須である．前者については大学等教育関係機関が尽力しているが，後者については我々研究者が検討している領域である．ここでは，人のナレッジやノウハウをコンピュータに伝授し，徐々にコンピュータにより代替する手法を検討する必要があるが，機械学習はそれを実現する有効な手段であり，積極的に活用されるようになってきている．

機械学習は画像認識，テキスト分類，感情分析，音声認識，バーチャルパーソナルアシスタントなどの領域で広く活用されてきており，近年の発達は目覚ましいものがある．サイバーセキュリティ領域においても，スパムメールフィルタリング，フィッシング検知，フェイクニュース検知，フェイクレビュー検知，生体認証，マルウェア分析，自動運転セキュリティなど，さまざまな領域にてすでに活用されてきている．これは最近になって発生した事象ではなく，たとえばスパムメールフィルタリングについては 10 年以上前から検討が進められてきており，その当時から機械学習自体の弱点を突いた攻撃の可能性まで検討がなされてきている．とはいえ，最近になって機械学習を適用するのに必須となる計算機環境およびツール群の入手が容易になってきたことにより，より広くさまざまなケースに機械学習を活用する試みがなされるようになってきている．もはや機械学習を用いること自体には新規性はなく，機械学習は強固なサイバーセキュリティを実現するのに必須不可欠なツールとなっている．本稿では，機械学習がサイバーセキュリティ領域の研究開発でどのように活かされているのか，その概観をお伝えすべく，いくつかの領域での機械学習の活用事例を紹介し，その後に我々が実施している活動を紹介したい．

活用される機械学習技術

セキュリティオペレーションの自動化が扱う技術領域は広い．各種のオペレーションのすべての領域で機械学習の活用の可能性は検討されているだろう．とはいえ機械学習を用いる都合上，学習対象となるデータセットを準備可能な領域でしか研究開発を実施することはできない．データセット種別の観点から当該領域を大まかに整理すると，図 -1 に示す通り，通信トラフィック・ログの分析，ソフトウェアのバイナリやコードの分析，そしてテキスト情報の分析といった 3 つの領域に整理することができる．これらの領域では，そ

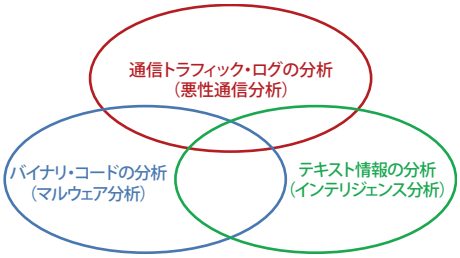


図 -1　主な分析対象領域

れぞれ悪性通信検知，マルウェア検知，インテリジェンス分析などの研究がなされている．実際には，サイバーセキュリティオペレーションの自動化を高い精度で実施するためには，これらの複数の領域にまたがって分析を実施する必要があることも多い．この整理を精緻に検討する意義はないものの，下記ではおおむねこの領域区分に沿っていくつかの領域をピックアップし，研究開発の現状を俯瞰したい．なお，関連する研究領域は広く，上記に限るものではない．たとえば，匿名化された投稿から投稿者を特定するプライバシ関連の技術や，機械学習自体のセキュリティについても多数の報告がなされているが，それらについては本稿では省略する．

通信トラフィック・ログを分析する

通信を分析する研究領域では，ネットワーク上の通信パケットそのものを分析する，もしくは通信のログを分析する等のものが存在する．通常の通信とは異なる通信や，マルウェア特有の通信パターンに類似するものを検知する技術など，さまざまなものが存在している．その中で筆者らが追跡している研究領域を下記に紹介する．

ネットワーク侵入検知の自動化

ネットワーク侵入検知システム（IDS）には大きくシグネチャ方式と異常検知方式が存在する．シグネチャ方式は誤検知率は低いが，シグネチャが登録されていない未知の攻撃（ゼロデイ攻撃）を検知することができない．シグネチャ方式は既知のシグネチャから攻撃パターンを分類または異常なデータから新しいシグネチャを抽出することに機械学習手法が用いられている．異常検知方式はゼロデイ攻撃を検知できる可能性があるものの，誤検知率が比較的高い．異常検知方式は異常なネットワークトラフィックを分類・クラスタリングする手法が用いられている．通常IDSは両方式を組み合わせたハイブリッド方式が用いられる．この分野は長期にわたり研究がなされている分野であるが，いまだに進展が報告されている．たとえば，トラフィックデータから特徴を抽出し，そこから改めて元データを生成する際に生じる再構成誤差に着目し，その値が大きい際に異常判定する技術などが提案されている．

悪性URLの検知・評価

フィッシングやドライブバイダウンロード攻撃を引き起こす悪性URLを特定すべく，異なるデータセットを用いたさまざまな方式が報告されている．いくつかのアプローチが存在するが，その1つは，ホスト名やプライマリドメイン，トップレベルドメインなど，URLの文字列自体に悪性サイトの特徴があると考えるものである．これらのものの中には，Whois情報やAS番号，ドメインの年齢など，ドメインに関する情報を利用するのも報告されている．別のアプローチとして，悪性URLに到達するまでのURL遷移を追跡し，その遷移から読み取れる情報，すなわち悪性URLまでのホップ数などを特徴として悪性URLがソーシャルエンジニアリング攻撃かドライブバイダウンロード攻撃のどちらに属するものかを判別することも可能になってきている．また，実際に訪問するページ自体を分析するアプローチも存在する．スタイルシートやJavaScript，ページのリンク構造など，さまざまな着眼点からの分析が報告されており，たとえばJavaScript分析の際の障壁となる難読化対策については，JavaScriptのコードをバイトコードレベルで分析することにより解決する技術などが報告されている．

ユーザの悪性サイトアクセス傾向分析

上述の悪性URL分析の研究の延長線上に位置づけられるものではあるが，目指しているものが悪性URLの検出ではなく，ユーザ自体の特性の分析になっている研究も存在する．たとえば，携帯電話網での通信ログから各ユーザのWebブラウジング記録に関する特徴量を抽出し，それに基づき同ユーザが近い将来に悪性URLを訪問する可能性があるかどうかを予測する手法なども報告されている．

暗号化通信の分析

通信を分析する技術領域では，暗号化通信の分析

も多数報告されている．セキュリティ対策を実施する際には，時に暗号化された通信やバイナリを分析する必要があり，暗号化された通信の中身を識別するのに機械学習を活用する研究もさまざまなものが報告されている．たとえば，Android および iOS アプリから発せられる暗号化された通信を分析することでアプリのフィンガープリントを抽出する技術が報告されている．さまざまなアプリやマルウェアが常に登場するため，教師あり学習を用いることによるスケーラビリティが課題となることが多いため，教師なし学習を用いた手法も検討されている．

バイナリ・コードを分析する

バイナリを分析する研究領域では，アプリの中からマルウェアを検知する技術や，その機能を分析する技術が検討されてきている．ここではそのうちのマルウェアの分類技術について概観を紹介する．マルウェアの機能とその潜在的な影響を分析するマルウェア解析技術は，セキュリティ分野における重要課題の１つである．マルウェア解析には大きく，サンドボックス上でマルウェアを実際に実行して調査する動的解析と，マルウェアを実行せずに調査する静的解析がある．これらの解析には従来，属人的な高い分析スキルが必要とされていたが，機械学習を用いてその解析を代替する技術の検討が進められている．

動的解析に基づくマルウェア検知

従来大量のマルウェア検体を自動的に検知・分類するのにシグネチャを用いていたが，そのシグネチャの準備には多大な工数を要するため，機械学習の活用によりシグネチャを用いない分析技術が検討されてきた．その特徴量には，逆アセンブルが不要な動的解析を用いるものが多数報告されており，システムコールやアプリケーションプログラミングインターフェース（API）などの呼び出し情報を特徴量として抽出する．マルウェア検知に加え，そのファミリーの分類なども実現可能である．

バイナリ分析に基づくマルウェア検知

近年は機械学習を用いた静的解析に関する報告が活発になっている．バイナリを分析する際にソースコードが手元にあれば，そのままそれを分析することが可能であるが，マルウェアを分析する際にはソースコードを入手できるケースは限定的である．そのため，分析を実施する前に，通常はバイナリを逆アセンブルもしくは逆コンパイルする．そこから得られたコードから特徴量を抽出し，分析を実施する．マルウェア検知という目的では，バイナリ間の類似度を評価することにより，マルウェアに近しいものか否かを判断する技術が存在するが，利用する特徴量，およびその類似度の指標などにもさまざまなものが報告されている．特徴量としては，バイナリから再構成した制御フローグラフや命令文そのもの，関数の引数の数や型など，さまざまなものが用いられており，それらは深層学習等の機械学習技術を用いてベクトル化され，そのベクトルを元に，バイナリ間の距離を評価する．これらの技術により，マルウェアの新種・亜種を効率的に検出することが可能となり，その結果に基づきマルウェアのシグネチャを自動で作成することで，より一層マルウェア解析の自動化が期待できる．

コード分析に基づくマルウェア検知

ソースコードが提供されている場合には，上述のような逆コンパイル処理は不要であり，より分析しやすいソースコードをそのまま分析することが通例である．また，ソースコードが提供されていなくとも，Android の APK や Java などのように比較的容易に人間が解読可能なコードへと変換可能なものも存在する．これらのコードを分析する際には，たとえば API コールや関数名を特徴量としたクラスタリングなどを実施することで，マルウェア検知やその機能分類などを実施することができる．

テキスト情報を分析する

テキスト情報を分析する研究領域では，SNS 等の投稿のセンチメンタル分析やフェイクニュース分析など，さまざまなものがあるが，ここではその中の脅威インテリジェンスに焦点を絞り，紹介する．脅威インテリ

ジェンスとは，アナリストなどにより生成された，セキュリティオペレーションに資する有益かつ重要な情報であり，通常，信頼性が高いと考えられる．脅威インテリジェンスとして収集された情報を，セキュリティインシデントの解析へ活用する動きが近年進んでいる．以下に，そのインテリジェンスを生成・分析する技術についていくつか紹介する．

脅威インテリジェンスの生成

各セキュリティベンダが定期的に発行しているセキュリティレポートや個人のブログ記事，Twitter などのSNS 上に投稿されているインシデント情報は，自組織内で発生したセキュリティインシデントの解析に有用である．しかし，これらの情報は自然言語で記述されており，独自のフォーマットで記載されていたり，独自のタグ付けがなされているケースがほとんどである．そのため，非構造化された脅威情報を解析に利用する場合，そのままではコンピュータへの侵入を示す痕跡情報などと自動的に突合させることや適切なラベルを自動付与することは難しい．これまではセキュリティオペレータが経験に基づいてセキュリティレポートなどから有益な情報を収集してきたが，機械学習技術を活用することにより，非構造化文書からのインテリジェンス抽出，ラベル付け，そして標準化された共通フォーマットにてレポートを自動生成する技術が検討されてきている．その際には，機械学習だけではなく，抽象的な概念モデルであるオントロジなどを活用するケースなども見受けられる．

情報のアノテーション

自然言語からインテリジェンスを生成する技術と近しいものに，情報のアノテーションを付与する研究も報告されている．これは，脆弱性や脅威に関する情報について，より詳しい情報を付加するものである．たとえば，インシデントレポートや脅威情報に対し，その内容がサイバーキルチェーンの中のどのフェーズに関するものなのかを分析し，その情報を付与するものが報告されている．サイバーキルチェーンは標的型攻撃などの攻撃活動を 7 つのフェーズに分解する考え方である．これは攻撃者の行動分析に役立てることが可能である．

ノイズ情報の検知・特定

多数のセキュリティ情報が存在する一方で，中にはノイズとなる情報が存在するケースも存在する．構造化された情報の中にもそのようなものが存在することもあり，それを特定する研究も報告されている．このようなノイズは，ヒューマンエラーに起因することも多く，ノイズの原因を特定し，修正することでより価値の高いインテリジェンスを生成することが可能となる．たとえば，自然言語情報から類推される脆弱なソフトウェアバージョン群と，実際にインテリジェンスに記載されている当該情報を比較し，一致しないものを自動検出する技術などが報告されている．上記のノイズに悪意があるケースとして，たとえばフェイクニュースなども存在しており，それを検知する技術も報告されている．セキュリティオペレーションで用いられるデータセットの中に悪意のあるユーザアカウントから投稿された情報が含まれている可能性も十分に考えられ，データセットの汚染を検知する技術についても検討が進められている．

データセットの準備

ここまで複数の領域をピックアップしてサイバーセキュリティ領域での機械学習技術の活用研究について紹介したが，本分野においては，研究データセットをいかにして確保するかが重要となる．研究を実施したくとも，その研究を実施するための分析対象となるデータセットを構築できなければ，機械学習は適用できない．そして，競争力の高い研究開発を実施するためには，質の高くユニークなデータセットと，信頼性および説得力のあるラベルを付与することが必要不可欠となる．

競争力のあるデータを収集する

大手検索エンジンや ISP，ソーシャルメディアサービ

スプロバイダなどは，膨大なデータを持っており，それらのデータを利用できることにより競争力の高い研究を実施することが可能となる．こういったデータにアクセスできない場合には，それらのデータと差別化のできるデータをいかにして収集・構築するかが，最終的な研究成果の質に大きく影響する．

筆者らの例では，我々はダークネット通信網を 10 年以上の期間観測しており，この期間の長さが競争力の源泉となっている．また，数千人の被験者を集め，ブラウザ上での Web アクセス履歴収集なども実施しており，大手検索エンジンから比べると規模は小さいものの，ユーザのブラウザ上での操作を追跡できる粒度での情報収集が，差別化要因になっている．

データをラベリングする

教師あり学習を実施する際には，データにラベルを付与する必要があるが，基準が明確でなく苦慮するケースが多い．たとえばマルウェア検知技術の場合には，あるバイナリがマルウェアであるか否かのラベル情報を付与することになるが，何をもってマルウェアとすべきかという基準は明確ではない．さまざまな工夫がなされているが，約 90 社のアンチウイルス製品の結果が収集できる VirusTotal の情報を元に，複数の情報源から多数決でラベル名を決定する手法なども提案されている．また，専門家によるラベル付けを実施するケースも多数報告されているが，通常，取り扱うデータのコンテクストでの専門家は機械学習の専門家ではない．そのため，機械学習の専門家ではない方々が効率的かつ効果的にラベル付けを実現可能にするためのインタフェースの研究なども報告されている．

我々の取り組み

日本では，2018 年度に官民研究開発投資拡大プログラム（PRISM）が創設されている．これは高い民間研究開発投資誘発効果が見込まれる領域に各府省庁の研究開発施策を誘導し，官民の研究開発投資の拡大，財政支出の効率化等を目指すものであり，情報通信研究機構は 2019 年度には九州大学，神戸大学，横浜国立大学，早稲田大学と連携し，この PRISM の AI 技術領域においてサイバー攻撃ハイブリッド高速分析プラットフォームの研究開発を実施してきた．我々はこれまでも機械学習を用いたサイバーセキュリティの研究開発を実施していたが，PRISM により方向性を持って技術を連携・発展させることにより，技術の飛躍的向上を実現すべく，研究活動を実施している．

図 -2 に，サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発概要を示す．本研究開発では，インターネット上で新たなマルウェア活動の発生を自動的に瞬時に検知し，それに関連する情報を自動的に生成･抽出し，必要なエンティティに必要なセキュリティアラートを提供する技術の研究開発を実施している．分析対象となるデータとして，ダークネットトラフィック，ライブネットトラフィック，マルウェアサンプル，脅威インテリジェンスなどを主に利用している．それらのデータから特徴抽出・前処理を実施した上で，複数の分析を並行して実施し，その分析結果をリアルタイムに

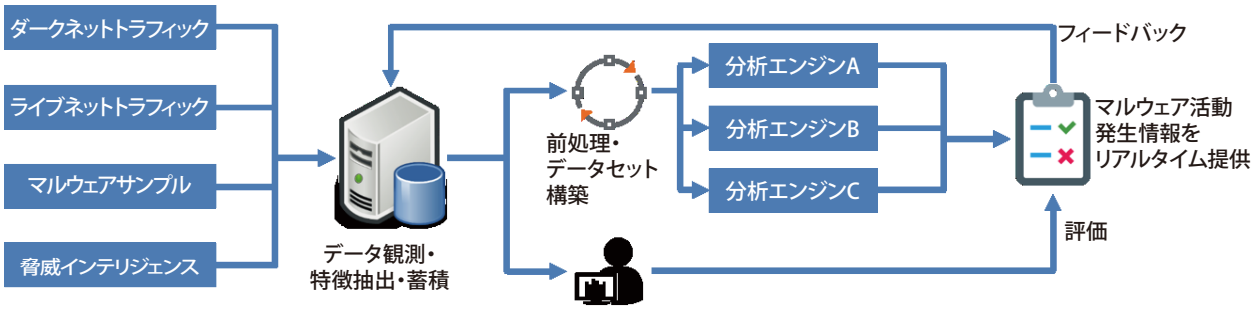


図 -2　サイバー攻撃ハイブリッド高速分析プラットフォームの研究開発概要

ユーザに提供する．また，アナリストによる評価を適宜実施し，その結果を反映した学習も可能な形になっている．分析対象領域としては，上述にある通信トラフィック・ログの分析，バイナリ・コードの分析，テキスト情報の分析の 3 領域すべてにまたがる研究開発を実施しているが，その中で今回の目的に合致した技術を絞って検討していく．

本研究開発ではさまざまな要素技術の研究を実施しているが，筆者らが手掛けているものをいくつか以下に紹介する．まず，我々は悪性の通信を検知・分析する研究として，マルウェア活動の発生検知，およびセキュリティアラートのスクリーニング技術の研究を実施している．前者ではインターネット上のダークネットと呼ばれる利用されていないアドレス空間に到着するパケットを分析することにより，マルウェアの活動が新たに発生するのを自動的に検知する技術を検討している．後者では，セキュリティアプライアンスが生成するセキュリティアラートの中で，特に重要性の高いものを自動的に抽出する技術を検討している．また，マルウェアを含む攻撃のツール自体を検出・分析する研究として，マルウェアの系統樹分析，および囮文書の評価の研究開発を実施している．前者では，マルウェアの機能を分類し，マルウェアの進化の過程が分かる系統樹の自動構築を検討している．後者では，標的型メールに添付されるファイルの内容の信憑性評価を実施している．

サイバー攻撃ハイブリッド高速分析プラットフォームを実現するには，上記を含む各種の要素技術を連携させる必要がある．本研究開発では，これらの要素技術の効果的な連携手法も検討しているが，その際には実際のオペレータの利用を想定した検討を進めている．

今後の研究開発の方向性

機械学習により，これまで実現し得なかったセキュリティオペレーションの自動化が実現し始めている．特に，人手により分類することが処理時間的に非現実的であったものが自動化されるメリットは大きい．スパムメールの検知や通常とは異なる通信の検知，マルウェア検体候補のスクリーニングなど，機械学習により効率化を実感できているオペレーションも存在する．一方で，機械学習だけですべてのセキュリティ課題を解決することはできない．実際，現時点でのセキュリティ学会での発表を俯瞰すると，機械学習に依存しない発表も多数存在する．また，機械学習の限界を示唆する論文も提出されてきている．

これまでの数年間は機械学習の適応可能性を広く探してきた時代であると感じているが，これからはその可能性の模索を継続して実施するとともに，より深く分析するための機械学習技術の活用の検討が求められると考えている．より深く分析するためには，領域が細分化されがちな研究業界において，積極的にその領域の壁を乗り越える努力が必要不可欠である．そして，セキュリティオペレーションの現場にあるノウハウをより色濃く吸収し，機械学習などにより再現することにより，地道に技術を成長させていく必要がある．攻撃者は技術の発展を待ってくれるわけではないため，従来のヒューリスティックベースの技術の発展と機械学習技術を用いたセキュリティ技術の発展を並行して実施し，融合していくことで，スピード感のある研究開発をしていきたい．

（2020 年 4 月 6 日受付）

高橋健志　takeshi_takahashi@nict.go.jp
2005 年早稲田大学大学院博士課程修了．タンペレ工科大学，（株）ローランド・ベルガーを経て，現在，情報通信研究機構に勤務．機械学習技術を用いたセキュリティ業務の自動化技術の研究開発に注力．CISSP，情報処理安全確保支援士．

古本啓祐（正会員）　k.furumoto@nict.go.jp
2018 年神戸大学大学院博士課程後期課程修了．現在，情報通信研究機構に勤務．機械学習を用いた脅威インテリジェンス分析およびトラフィック解析に関する研究に従事．

韓　燦洙　han@nict.go.jp
2018 年九州大学大学院修士課程修了．現在，同大学博士後期課程在学，および情報通信技術機構に勤務．機械学習を用いたマルウェアおよびトラフィック解析に関する研究に従事．

［サイバー・ウォーズ］

③ 情報通信技術（ICT）と安全保障

佐藤丙午 | 拓殖大学

戦争と技術

安全保障と情報通信技術の間には，歴史的に密接な関係がある．戦争において，時間，距離，場所による制約を技術的に乗り越える試みは，人類の歴史とともに古い．たとえば，トロイの陥落を狼煙や篝火で連絡したエピソード，アラマダの海戦におけるプリマスからロンドンへの連絡，米国の南北戦争におけるテレグラフの活用，近い歴史の中では，第一次世界大戦時の軍事上の発見として，機械化とラジオ技術が挙げられることが多い☆1．

第二次世界大戦以降の戦争や国際関係では，特に情報通信技術の飛躍的進化が，その動向を大きく左右してきた．情報通信技術は Information and Communication Technology（ICT，日本では IT と呼ばれることが多い）と呼ばれるようになり，米国の第二次オフセット戦略の下で軍事面での活用が拡大した．ICT の軍事的意義が実証されたのは，1991 年の湾岸戦争である☆2．この戦争は，ネットワーク中心戦闘（Network Centric Warfare）の軍事的可能性が実証された戦争とされる．

さらに 90 年代以降，旧ユーゴスラビアをめぐる紛争，さらには同時多発テロ後の対テロ戦争やイラク戦争などにおいて，攻撃手段の効率化や拡大に加え，暗号技術や解析技術の活用による情報作戦の分野でも，ICT の活用が進んだのである．特に，映像技術，計算技術，衛星技術により，通信，指揮統制，偵察監視，兵力の効率化，ナビゲーション，そして気象分野などの分野で軍事利用は拡大した．21 世紀の戦争では，ICT によって獲得した情報を人工知能（Artificial Intelligence：AI）で処理し，兵器システムの自律化につなげる試みも見られる．

ICT と安全保障の関係を考察する上で，軍事技術革命（Revolution in Military Affairs：RMA）と社会の関係の分類および，その後の情報 RMA における議論が，基本的な思考枠組みとなる．RMA と社会の関係では，社会の変化が RMA をもたらす，もしくは RMA によって社会の在り方が変化する，など，軍事社会学的な議論が展開されてきた．そして，情報 RMA の議論では，アンドリュー・マーシャル（Andrew Marshal）が進めた ICT を使用した軍の作戦の効率化についての政策論が進められた☆3．

本稿では，1990 年代の RMA の議論を出発点として，国際関係論を基盤に，軍事社会学と政策論の双方で進化した ICT と安全保障の関係を振り返る．その上で，2020 年代の議論を展望し，ICT を含む新興技術の安全保障上の課題を説明する．

RMA 論と軍事技術開発

1990 年代の RMA の議論や，GW ブッシュ（G. W. Bush）政権期の軍事変革（Transformation），オバマ（Barack Obama）政権期の第三のオフセット戦略などに見られるように，科学技術の進化は戦争の在り方を変え，それが国家戦略や，軍事的な調達政

☆1 Krepinevich, A. F. Jr. : The Military-Technical Revolution : A Preliminary Assessment (CSBA, 2002).

☆2 クレピネビッチの評価は，最初 CSBA より 1992 年に発表され，その後更新版が 2002 年にまとめられた．Krepinevich, A. F. Jr. : The Military-Technical Revolution : A Preliminary Assessment (CSBA, 1992).

☆3 Davis, N. C. : An Information-Based Revolution in Military Affairs, in John Arquilla, David Ronfeldt, eds., In Athena's Camp: Preparing for Conflict in the Information Age (RAND, 1997).

策に影響を及ぼす．米国の各政権で語られた軍事技術と安全保障に関する政策は，それぞれ政治的用語は異なるが，実質的には類似の事象を扱ってきたものである．その本質は，技術の進化が国際社会をどのように変えるか，そしてその中で米軍が目指すべき状態は何か，である．

技術進化が見られる限り，戦争の進化も止まらない．歴史を振り返っても，火薬の発明，蒸気機関などの内燃機関の登場，通信技術の発達，そして原子力の活用も，技術進化が戦争を変えた例として考察できる．特に原子力の軍事利用では，戦争の目的を，戦闘による破壊ではなく，抑止（戦争を止めること）へと変化させた[☆4]．

このように，科学技術が国際システムを変革する潜在性があることは，多くの研究者によって指摘されてきた[☆5]．科学技術の成果を軍事面に適用し，それが革新的な成果につながるとすれば，各国にとって，科学技術は国際政治におけるパワーを補正する重要な手段となる．その際，科学（Science）と技術（Technology）のうち，科学的知見を国家として蓄積し，動員できるのが有効か，もしくは社会的に必要な機能を技術的に実現する能力が必要なのか，議論が分かれてきた．また，科学技術のオーナシップの問題は，さらに科学技術と国家の関係を曖昧にしている．政府主導で技術開発プロジェクトを推進した時代は終わり，今日の国際社会において，国家は技術開発の主導者ではなく，すでに存在するものの受益者に過ぎないとの主張も存在する．この場合は，科学技術を効果的に動員できた国が，国際社会でパワーを行使することが可能になる．

その際，科学技術が社会に及ぼす長期的なインプリケーションについて，社会の変化と科学技術の関係を説明する上で，社会の変化が科学技術の進化を促すのか，科学技術の変化に合わせて社会が適用するのか，という概念的な二分法で議論されることがある[☆6]．

たとえば，19 世紀の工業文明の到来とともに，内燃機関を中心とした軍事技術革命が進行した．この最大の受益者は近代海軍建設で先行した英国であった．英国は工業化を前提とする海軍を維持する上で，世界各地に拠点が必要となった．これが，植民地主義の 1 つの側面である．他の欧州諸国も世界規模の海軍建設に乗り出し，整備・修理・補給等の拠点を求めたため，帝国主義の拡大につながったと解釈される．つまり，軍事技術の革命が，国際社会に影響を与えた一例といえる．

戦略爆撃の歴史からも，技術が社会に大きく影響を与えたことが分かる．戦略爆撃は，戦略論との関係の中で社会を変えていった．戦略爆撃は，航空機の発達とともに考案された攻撃方法であるが，上空からの爆弾投下の精度は低く，反撃による被害と，付帯被害が大きいという欠点があった．しかし，作戦に関連する被害の軽減が必要という社会的要請に直面したとき，特に米軍は 3 つの選択肢に直面した．それらは，価値攻撃（戦略爆撃による都市攻撃），原爆（効率的に反撃の手段を奪う），そして精密誘導爆撃である[☆7]．

冷戦という特別な戦略環境の下，米国はソ連に対して科学技術の優越性を維持するとともに，ソ連の通常兵器による急襲に対抗するため，情報通信技術を活用した精密誘導兵器の開発と，それに合わせた戦略の採用へと進んだのである．この選択は，米軍が情報の優越の下でのみ作戦を実施するという特徴をもたらした．

ただし，米国によるこの戦略の採用は，1970 年代にソ連のオガルコフ（Marshal Nikolai V. Ogarkov）による軍事技術革命の議論に触発されたもの

☆4 Brodie, B. : Strategy in the Missile Age (RAND, 1959).
☆5 Weiss, C. : How Do Science and Technology Affect International Affairs?, Minerva, Vol.53, No.4, pp. 411-430 (2015).
☆6 Liaropoulos, A. N. : Revolutions in Warfare : Theoretical Paradigms and Historical Evidence," The Journal of Military History, Vol.70, No.4 (2006).
☆7 Sapolsky, H. M. eds. : US. Military Innovation since the Cold War: Creation without Destruction (Routledge, 2009).

であった．ソ連が考案し，米国が採用したこの「エア・ランド・バトル（Air-Land Battle）」の重要なポイントは，情報の優越の維持と，情報通信技術の活用である．後に 1991 年の湾岸戦争で国際社会が目撃したように，ステルス技術，各種センサ技術，GPS 誘導兵器，レーザ管制兵器，衛星通信，暗視装置等の活用による，戦闘の効率化と彼我の軍の被害の限定は，目に見える形で実現したのである☆8．

もちろん，湾岸戦争でこのトレンドが確定し，その後のトランスフォーメーションや第三のオフセット戦略へと，その後の軍事技術と戦略が自動的に転換したものではなく，伝統的な兵器を重視する勢力からの抵抗，予算の優先をめぐる兵種間の争い，特に陸軍からの抵抗などに直面している．さらに，2001 年 9 月の同時多発テロ後，軍の作戦に対する社会の要請も変化した．テロ組織や反体制勢力を壊滅するためには，航空戦力による精密爆撃ではなく，陸上兵力が，低強度能力しか持たない敵と低強度紛争を戦う必要が生まれた．

しかし，陸上における低強度紛争でも，また海上においても，ICT による戦闘の効率化は，技術進化の中で必要不可欠になっていった．特に位置情報の把握，偵察活動，部隊間の情報伝達など，作戦を促進する条件の部分で，ICT の活用は作戦運用を助けた．2003 年のイラク戦争において，ストライカー旅団を中核とする軽機動部隊がイラク国内に侵入して，ごく短期間にバグダッドを制圧できた理由の 1 つに，米国側の情報の優越があったことは言うまでもない．そして，ICT による作戦効率の追求は，戦争の進化の合理的な結論に至ることになる．

たとえば，2010 年代の後半に政策として確立する「マルチ・ドメイン戦略（日本ではクロス・ドメイン戦略）」は，各軍種間の統合作戦の推進，その一環として各軍種の作戦に対する相互の作戦協力が前提となる☆9．具体的には，地上部隊は近接して敵対勢力を撃破するのではなく，遠隔攻撃を行い，また別の部隊は特殊部隊化して精密誘導爆撃の着弾点の観測および連絡要員として活用する，などの戦い方が一般的になる．ICT は，これらの作戦を可能にする技術（Enabling Technology）と位置付けられる．

ICT を活用した戦争の変化が，そのまま国家関係の変化に直結するものではない．多くの科学技術は，戦闘方法の効率化に貢献するが，社会変革を企図していない．変革との関連では，たとえば，アメリカ革命やフランス革命以降進んだ自由主義および民主主義の世界的な普遍化が，国家動員を合理化して徴兵の制度化を促した面はある．一般的な兵役制度の下では大人数の兵員が確保可能とあり，特に陸上戦力が必要な戦争（占領戦）の遂行には有利となる．

しかし，ICT の活用が進み，占領戦の必要性が下がった戦略環境では，兵員の数は必要ではなく，個々の要員の技術的専門性が重要になる．サイバー空間まで戦闘領域を拡大するとすれば，そこにおける戦闘員は，ハッカーや SE，さらにはゲーマーなどが最適な「兵員」となる☆10．つまり，ICT と国家関係の変化に相関を見るとすれば，戦闘方法と戦争様相の変化が同時に発生した際に，特定の社会条件（社会の構造変化が発生している等）の下で発現すると理解すべきなのであろう．

そして，ICT を含む新興技術などを活用する戦争が，社会条件とは無関係に，社会の構造変化につながるかどうか，注目すべきなのであろう．

ICT と安全保障における文化的要因

一般的に社会の構造変化は，所定の社会条件に影響され，ICT と安全保障の関係では，それが文化

☆8 湾岸戦争によって，1980 年代に欧州で想定された戦略を中東地域で展開した米軍は，戦争の方法についても，陸上勢力と航空勢力のバランスの逆転をなし遂げた．この方法は，ボスニア（1995 年）およびセルビア（1999 年）における戦闘にも引き継がれた．戦略爆撃の歴史は，Pape, R. A. : Bombing to Win : Air Power and Coercion in War（Cornell, 1996）に詳しい．

☆9 Joint Doctrine Note（JDN）1-18, Strategy (Washington, DC: U.S. Government Printing Office, 25 April 2018).

☆10 Harris, S. : @ War : The Rise of Cyber Warfare (Headline, 2014).

的要因と，包括的な意味で，社会における技術の価値に左右される．

戦争において，各国が考案する選択肢の傾向は異なる．入手可能な技術レベルと，地理的および地政学的な戦略環境に応じて，各国はそれぞれ異なった戦術を採用する．さらに，その選択内容には，文化的な要素も存在する．たとえば，国際関係論の現実主義や，戦略論的に考えて，日本は核保有を選択しても不思議ではないとされる．しかし，被爆体験からくる反核感情の影響から，核兵器開発への道を歩んでいない☆11．

安全保障における文化的要因には，経験から導かれた教訓として蓄積されたものも存在する．本土に対する直接攻撃に過剰に反応する米国，戦争で獲得した領土を失うことを極端に嫌がる中国やロシアなども，文化的要因から自由ではない．このため，文化的要因による戦術選択を助けるものとして，科学技術の位置付けを考慮すべきである．

1970 年代後半以降，米国が欧州においてエア・ランド・バトル戦術を重視した理由の 1 つに，共産圏勢力が西ドイツに地上軍で急襲をかけた場合，防御線を突破されて西ドイツや NATO 軍の中核部分や，在欧の戦術核施設を破壊され，反撃手段が限定されることに対する恐怖があった．このような戦術的劣勢を挽回するためには，核兵器による反撃あるいは先制攻撃が考えられるが，それは世界規模での核戦争を覚悟する必要がある．全面核戦争を回避するためには，共産圏勢力の攻撃の兆候を早期に探知し抑止のメッセージを強化するか，攻撃を受けたとしても，少数の戦力で効果的に侵略を撃破する必要がある☆12．ここに，C4IR の強化の中核を担うものとして，ICT が重要な意味を持つのである．

この問題を文化的に見ると，可能な限り人的被害を限定したい米国の社会的要因が深く関係する．米国は 1960 年代から 1970 年代初頭までベトナムでの泥沼に苦しんでいた．北ベトナム軍や南部に侵入したベトコンと米軍との軍事力の差は明確であったが，北ベトナム側は非対称戦争で米軍に被害をもたらした．この結果，米兵の消耗は大きく，米国内においても可視化できる被害が続出したため，国民の世論は反戦に傾いたのである．民主主義国において，国民の支持が欠ける戦争を遂行するリスクは大きい．ベトナム戦争後の米国は，戦争において人的被害を最小限にする方策を模索してきた．

湾岸戦争を経て，1996 年 7 月に公表された Joint Vision 2010 では，米軍の将来は，大規模兵力ではなく，小規模で精強な兵力に依存し，長射程な精密誘導ミサイルなどの，遠隔地からの兵力投射能力を重視することになる，としている☆13．つまり，米軍への被害を限定し，個別の戦闘の行方が世論に与える影響を管理することを重視しているのである．ただし，1990 年代中葉に示された航空戦力重視の RMA は，米国内では大きな批判に直面した．戦争の最終的な結果を決めるのは陸軍であるとの主張は根強く，たとえ陸上戦闘で米軍に被害が出たとしても，航空優越では勝利を収めることができないため，航空作戦は陸上作戦に従属するとの主張が見られた☆14．

米国における技術開発は，人道的問題に起因するケースが多い．たとえば，イラク戦争後に米軍の兵站を担った PMC が反体制勢力に攻撃され，場合によっては残忍に殺害され，映像化されたことがある．この事件が米国の世論を硬化させた経験に基づき，兵站の自動化を目指す自動運転技術開発への投資が増大した．さらに，福島原発事故のように人間による作戦が不適な環境や，イラクでの反乱掃討作戦などで経験した，混乱した都市部での近接戦闘の回避などを目的に，ロボット開発も進められている．

☆11 岸　俊光『核武装と知識人：内閣調査室でつくられた非核政策』（勁草書房，2019 年）．

☆12 Skinner, D. W : Air Land Battle, Professional Paper 463 (CAN, 1988).

☆13 Joint Chiefs of Staff, Joint Vision 2010.　同様の点は，Joint Vision 2020 にも盛り込まれている．

☆14 Press, D. G : The Myth of Air Power in the Persian Gulf War and the Future of Warfare, International Security, Vol. 26, No.2, pp. 5-44 (Fall, 2001).

AIの開発は，自動運転技術やロボットなど，新興技術の軍事転用が進められ，戦略への影響が展望される中で，その可能性が追及されるようになった．

ICTは軍事作戦のすべての局面に関係するため，米国におけるRMA論議とは直接的に関係なく進展した．米国では2012年にパネッタ（Leon Panetta）国防長官が，「現在の戦争を戦いつつ将来の挑戦に準備する」との方針を発表し，陸軍対空軍の戦略爆撃論争に一応の終止符が打たれた．そして，将来への挑戦において，統合運用の下での作戦の効率化の追求が進められたのである．

この方針は2014年にヘーゲル（Chuck Hagel）国防長官により，第三のオフセット戦略として再確認され，トランプ（Donald Trump）政権も方針を引き継いだ☆15．2018年の国防戦略では，米軍の目標はテロ組織との戦いや小規模紛争を戦うことではなく，国家間の戦略競争を戦うことと規定し，特に中国やロシアを念頭において，米国の軍事的優越性の再確立を目標として掲げている☆16．この間の米国の技術政策における目標は明確である．それは，新興技術により，戦闘における目標探知や攻撃，さらにはその評価までを含めた「キル・チェーン」を効率化することで，新たな戦場のネットワークシステムを構築することと解釈できる．

「キル・チェーン」は攻撃サイクルとも呼ばれる．攻撃サイクルの効率化は，米国だけの問題ではなく，中国やロシア，また日本においても同じ方向を向いていた．たとえば，サイクルの中でAIを活用する方針は，（攻撃手段の自律化を含め）米国ではなく中国や韓国，さらにはイスラエルなどの方が効率的に実施している面がある．米国の比較優位が減退した理由は，米軍がRMA論争を繰り広げ，各軍が将来の挑戦に向けた必要な投資を制限したためである．したがって，米国が優越を再確立するためには，伝統的な軍を強化するのではなく（ICTの適用は，強化のための手段であるとする見方もある），新たな戦争の方法の確立が必要とされたのである．

このため，第三のオフセット戦略およびトランプ政権の安全保障政策の下では，新興技術の可能性を念頭に，新たな戦争の方法の模索が続けられてきた．この方法は，技術に合わせて兵器開発を行う，いわゆる「技術決定論」とは異なる．技術決定論は，先端的な技術の開発が実現した後に，それを活用した兵器開発を検討するものである．一般的には，「ある技術から兵器を作る」という方が理解しやすいかもしれない．これに対し，「兵器主導開発論」では，必要な兵器構想の下で技術開発が進むという形態を想定する．

技術決定論と兵器主導開発論は，兵器開発においていくつかの前提の下で成立する．技術決定論では，そもそも新興技術は開発されるものであり，技術へのアクセスを含めて，その兵器への技術の応用の程度が問題となる．兵器主導開発では，技術開発に必要な資金や人的資源の確保を兵器の発注側である政府が保証する形をとるため，閉鎖された環境の下で進められることになる．たとえば，米国の軍事産業は第二次世界大戦における政治経済体制の下で，生産態勢が規定され，兵器主導開発への適応が容易な構造になっている．

しかし，ICTを含めた新興技術の開発は民間企業主導で進められ，各国において，軍の側は技術開発の受益者になるという構図の下にある．このため，民間分野と軍事分野の協力が必要になっているのである．

新興技術と官民協力

社会的な意味を含め，技術により，戦争の方法が根本的に変化するかどうかは，新しくて古い，安全保障議論の重要なポイントである．恐らく安全保障

☆15 Ellman, J., Samp, L. and Coll, G. : Assessing the Third Offset Strategy, CSIS (March 2017).
☆16 https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

論の教科書には，防衛装備の基本的な機能として「動く」，「撃つ」，「交信する」を挙げて，それぞれの機能の進化の方向性を説明していくだろう．

「動く」機能には，自軍による兵器等の操作に加え，相手の行動を探知して突入する行動等が含まれる．この領域では，IoT などの利用範囲の拡大に助けられ，低コストで広範に存在する民間分野の技術を活用して，遠隔地での探索活動等も，新たな役割と規定される．さらに，治安活動目的で利用される顔認証技術や携帯電話の位置情報の活用，さらには決済ツールの利用など，ICT の活用により，広範なデータ収集と分析が可能になっている．これら広範なデータ収集の手段としては，宇宙における衛星，サイバー手段なども想定され，その解析には，将来的には量子計算機などが使用されると指摘される．

「動く」機能の高度化において，センサーなどを大量に配置してデータを収集して状況把握能力を高めることは，戦場における「マス」の復活を意味する．人的コストの削減と正確性を目的としてユビキタスに配置されたセンサーから収集されたデータは，人間では処理できない分量のため，必然的に AI の活用が進む．そして情報処理能力が高度化すれば，IoT を含めて，低コストで配置できるセンサの数は増加する．同時に，もし動力源の問題が改善されるとすれば，規模（小型化と大量生産）と速度の問題が解決され，自律兵器の開発は加速度的に進むことになる．

自律化された兵器の特徴と課題は，データ収集から判断に至るまで，「キル・チェーン」の下に分割された各種機能の自律化をシステムとして運用することになるため，戦闘自体は，システムの無力化を目的とすることに重点が置かれる．その意味で，戦争の進化において，「撃つ」機能は実態的には大きく変化することになる．安全保障論では，攻撃方法として対価値攻撃と対軍事攻撃という二分法を導入したが，システム自体の無力化が必要になるということは，攻撃対象としての価値と軍事とが区別困難になっていくことを意味する．

つまり，新興技術の発達により，「撃つ」機能がサイバー攻撃，通信妨害，電子戦闘，ソフトウェアに対する攻撃（書き換えや情報盗取など）などまで拡大することになり，それらがハードウェアに対する攻撃と同等の価値を持つことになる．さらに，「動き」と「撃つ」が高機能化することになると，探知から攻撃までの時間が短縮され，戦闘が軍事的合理性の下で高速化される可能性が生まれる．これは，戦争が外交と並ぶ政治の手段ではなく，それ自体に別の価値を持つことを意味する．それを，戦争の「ゲーム化」と呼ぶことも可能であろう．そして極端に言うと，「ゲーム化」され，政治性を失う戦争において，実態上，前線と後方の区分が曖昧になり，既存の国際法の適用は困難になる．そして，戦闘員同士ではなく，社会全体が軍事的なリスクに直面することにつながる．

さらに，「交信する」機能において，軍の指揮命令系統に特有の中央での管制ではなく，前線の部隊や「プラットフォーム」間の通信による，分散化されたネットワークの戦闘へと変化する．航空部隊におけるロイヤル・ウィングマンは，母艦となる戦闘機が複数の異なる機能を持つドローンを操作する戦闘システムである．同様のシステムは，潜水艦でも運用されており，陸上の戦車システムの無人化を含めると，戦場での情報収集・分析および作戦運用を分散化するのは，各軍種で進められていることが分かる．同時に，プラットフォームの小型化により，操作員が指揮統制するターミナルの数は増加傾向にある．人間が操作可能なターミナルの数を超える場合，そこでも自律化が進められることになる．

「交信する」機能の基礎インフラである通信関係の技術では，5G 通信の普及が進む．通信技術と計算技術（量子科学の発達が期待される）の先に，暗号化技術や脳計算インタフェース技術を含む，さまざまな製品開発と実用が期待されており，軍事面ではスウォームやロボット化技術への期待が大きい．これらは，技術に対する期待が先行し

ている例であり，実際に民間技術の軍事転用が円滑に進むとは限らない．

包括的な表現を使用するとすれば，この問題は，技術のオーナシップと官民の技術協力の問題と規定できる．

技術のオーナシップ問題について，新興技術などの技術の知的所有権は，一般的に特許や占有等で開発者に帰属しており，たとえ国内に存在する技術であったとしても，政府は自由に使用できるものではなく，ユーザの一人に過ぎないということである．官民の技術協力については，特に防衛装備開発には大学や研究開発機関を含む，民間分野の協力が不可欠であるにもかかわらず，技術的に先行する民間分野は，軍事研究に抵抗があったり，軍事分野への協力には経済的に魅力がないなどの理由で協力に抵抗する，という問題である☆17．

中国においては，この問題を「軍民融合」で乗り越えようとしている．中国のように，権威主義的な国家資本主義の下では，AI などの新興技術の開発と利用を，人民解放軍が選択的に利用することが可能である．そして，社会のデータを独占的に収集し，利用することも可能となる☆18．日米のような民主主義や自由主義を掲げる国家群は，ICT などの新興技術を活用した新しい戦争において，技術の活用に関する官民協力には制約が多く，なおかつ社会の体制は硬直的である．

では，新興技術を活用する新たな戦争は，国家資本主義勢力が有利になり，国際システムもパワーの変革に向かうのだろうか．多くの研究が，米中関係において，米国の通常抑止能力の浸食が，これまで米国が影響力を維持してきた世界の各地域を不安定にすると指摘している．地域の不安定化は，米国の抑止力の低下や限定と同時に，各国の経済政策や国際政策に対し，中国が影響を行使することで，それぞれの国内政治が不安定化することによっても出現する．中国の進める国家資本主義，もしくは「新中華圏」の構築に対して，米国が有効に対抗する体制を構築しない限り，米国の漸進的衰退の懸念は続くことになる．

自律兵器開発の課題

軍事力の近代化において，ICT をレガシー・システムに最適化し，その更新に資源を投入するのであれば，米国に限らず，ロシアであったとしても中国との量的な競争に勝利することはできない．中国はすでに AI を含めた新興技術への投資を拡大し，「新しい戦争」への体制を強化している．このため，日米両国は質的な競争により，パラダイムの異なる戦争での勝利を追求しなければ，既存の国際秩序の不安定化に直面することになる．

異なるパラダイムの戦争の構成要素である新興技術が「キル・チェーン」を効率化する上で，2 つの課題が生じている．1 つが，軍事システムの開発における民間部門と軍事部門の協力体制の構築である．2018 年の Project Maven をめぐる Google 社内の議論や，2019 年の Microsoft の全国防総省のクラウド受注問題を見る限り，民間企業と軍の関係には複雑な愛憎関係が存在する．この問題は，中国では表面化しにくい．今後，米中の間で，民間企業との協力関係をめぐる不均等な競争条件が，どのように変化するか，注目する必要がある．

第二の問題は，自律兵器開発をめぐる倫理の問題である．兵器の自律化による課題については，2014 年以降特定通常兵器使用禁止制限条約（CCW）の下で議論されており，2019 年には 11 項目の指導原則が合意されている．自律化された兵器はもたらす問題は，人間の意図を超えて自律的に攻撃を展開し，国際人道法が順守されない状態が生じるという懸念である．米国は 2020 年 2 月に，AI と軍事の関係を規定する 5 つの倫理原則に合意してい

☆17 What is Project Maven? The Pentagon AI project Google employees want out of, Global News, April5, 2018.
☆18 Kai-Fu Lee : AI Super-Powers : China, Silicon Valley and the New World Order (HMH, 2018).

る[☆19]．しかし，国際社会，米国，そしてそれ以外の国々との間で，倫理原則や遵守ガイドラインが異なるとすれば，それが緩い国が新興技術の兵器化で有利な立場を獲得することに対する懸念は大きい．

この2つの要素は，ICTなどの新技術を新たな戦争に向けて活用すべきかどうかという議論の現代的な本質になる．1991年の湾岸戦争後は，精密誘導に管制可能な戦略爆撃の利用が，戦争の革命かどうか議論され，陸上兵力に対する航空兵力の優位が主張された．米国社会としては，これは犠牲者ゼロ戦略として歓迎すべき方向性だったのであろう．しかし，米国が戦略的競争相手ではなく，テロ組織や反体制勢力を撃破し，掃討する「小さな」戦争や反乱鎮圧作戦も重視される過程で，1990年代に議論されたRMAではなく，ICT等を利用した効率的な小部隊や特殊部隊作戦の中に，新興技術の活用方法を模索するようになった．その成果の1つが，ビンラディン暗殺作戦であった．

しかし，中国やロシアなどのような戦略的競争相手の出現とともに，これら諸国との対抗手段として，新興技術の役割が再定義されていった．技術決定論と兵器開発論の枠内にとどまらない兵器開発の方法が検討され，そこで伝統的な兵器システムを前提とした戦争を前提とした安全保障戦略の非効率が強調されるようになった．量的および質的な優位を背景に，たとえ，敵対相手が米軍の脆弱な部分で一時的に優勢を確保したとしても，スピードを伴う展開能力と，相手の状況を正確に把握する能力によって反撃し，勝利することができる力は，米国の通常抑止の基盤を構成した．しかしその能力が，戦略的競争相手の登場とともに無効化され，勝利を実現できなくなった状況での戦略の在り方は，従来の安全保障政策の変更を迫るものとなったのである．

ICTなどの新興技術には，上記の2つの制約があったため，概念的には，パラダイムの異なる兵器システムを構築する方法と，伝統的な兵器システムにICTなどの新興技術を組み込んで能力更新を図る方法が存在した．後者の方法は，既存のドクトリンや組織運営を合理化する方法であり，過去，多くの軍で試みられ，多くの場合は失敗に終わった．前者の方法は，新たな戦略，ドクトリン，組織構成が必要になるため，軍の持つハードウェアだけでなく，作戦運用などのソフトウェアも更新する必要がある．成功が保証されていない手法の採用には，組織内の抵抗が大きい．

つまり，ICTの技術的状況や，新興技術の可能性を考慮し，米中の戦略バランスの問題を考えると，自律兵器の採用は不可避であるが，その採用の方法をめぐって，人道規範と軍事的効率性を共存させる方策を模索する必要があったのである．

将来の課題

過去に発生したと評価される軍事技術の革命が，国際システムの変革にまで至った例は少ない．たとえば，特定の武器弾薬や，それを利用した戦術の変更により，特定の国が大国の地位へと上昇した例は多いが，その地位が構造的に維持され続けた例は少ない．この理由として考えられるのは，技術は伝播・拡散するため，技術をベースにしたパワーは平準化されるためとされている[☆20]．

平準化は，国際的な技術移転に加え，軍事システムの維持コストによる長期的なパワーの低減によってももたらされる．さらに，その時点で優越した軍事システムを無効化する新兵器システムの開発も大きな影響を与える[☆21]．新興技術が出現する際，各国が常に神経質に反応する理由は，先行して行った軍事投資が無駄になるのではないかという恐怖があるためである．ICTを含む新興技術の作戦運用への

☆19 DOD, Release : DOD Adopts Ethical Principles for Artificial Intelligence (Feb. 24, 2020).

☆20 Schmid, J. : The Diffusion of Military Technology, Defence and Peace Economics, DOI: 10.1080/10242694.2017.1292203

☆21 Brodie, B. : Sea Power in the Machine Age, Princeton University Press, pp.105-23, 434 (1943).

適用において，それが「キル・チェーン」の中で可能性を高める技術であることから，伝統的な兵器システムの更新にも，さらには新しい戦争の方法においても使用される．新興技術による戦争の変革は，政治的な効果が伴う必要はない．

長期的に見ると，平準化の防止は困難であり，その速度を遅らせることで，比較優位を確保することが現実的な方策になる．もちろん，敵対国に欠ける技術を特定して管理する手法も存在する．たとえば，中国の軍民融合や攻撃的な技術獲得戦略，さらにはAI大国を目指す方針などは，国家政策として平準化を目指すとともに，それを超えて優位的な立場の獲得を目標とするものと解釈できる．このため，米国を中心とする西側諸国が，中国の技術政策に神経質な反応を示すのも，これまでの軍事技術の歴史を振り返ると，自然な反応である．

ICTを含む新興技術による軍事技術革命は，その中核技術が民間企業にあり，情報やデータ等も民間企業が保有しているため，それらを利用して他国がキャッチアップするのは容易である．この問題は，情報作戦（Information Warfare）において一層明確になる．もし双方が同じレベルの情報と技術を持っており，その平準化が不可避的に進むのであれば，重要な技術や情報を保護する側が，比較優位を持つことになる．中国の国家資本主義との競争が懸念される理由は，技術や情報の保護において，中国が不均等な条件を作り出しているためである．米国がオバマ政権の二期目以降，新興技術の管理方法を検討してきたのも，技術や情報の防護の戦略的意義を理解しているためであろう．

比較優位をもたらすもう1つの要素が，空間的制約である．各国は，その戦略的環境に合わせた兵器の採用を進める．国家間の係争地に物理的に近くで作戦活動を実施する場合，兵站や整備補給等の拠点に近い方が有利になる．その量的優位に対抗するために質的優位を追求するのが一般的な反応であるが，ICTを含む新興技術では，質的優位を実現するのが困難な事例が多く，場合によっては平準化の速度を加速することが想定される．

このように，ICTは各国の安全保障に，大いなる機会と課題を投げかけており，この問題を継続的に評価分析することが必要なのである．

（2020年4月2日受付）

佐藤丙午　hsatou@ner.takushoku-u.ac.jp
一橋大学大学院修了．防衛庁防衛研究所主任研究官を経て，2006年より拓殖大学海外事情研究所教授，2013年より国際学部教授．拓殖大学国際学部・海外事情研究所副所長（現職）．専門は，国際関係論，安全保障論．

［サイバー・ウォーズ］

応
般

④タリン・マニュアルについて ―サイバー攻撃に関する国際法―

中谷和弘 | 東京大学大学院法学政治学研究科

本稿においては，サイバー攻撃に関する国際法のルールを包括的に記述したタリン・マニュアルについて説明する．まず，タリン・マニュアルとは何かを述べた上で，タリン・マニュアルの主な内容について概観する．最後に，タリン・マニュアル以降の国際法上の諸課題について触れることにしたい．

タリン・マニュアルとは

タリン・マニュアルとは，エストニアの首都のタリンにある北大西洋条約機構（NATO）のサイバー防衛協力センター（Cooperative Cyber Defence Centre of Excellence, CCDCOE）に法律専門家が個人的資格で集まって，サイバー攻撃に関する国際法のルールをコメンタリとともに記述したものである．この作業は，米国海軍大学校の Michael Schmitt 教授を中心にすすめられ，まず 95 の規則とコメンタリからなる「サイバー戦に適用される国際法に関するタリン・マニュアル」（Tallinn Manual on the International law Applicable to Cyber Warfare）がまとめられ，2013 年 4 月に Cambridge University Press から刊行された．後にタリン・マニュアル 1.0 と呼ばれるようになったこのマニュアルは，第 1 部「国際サイバー安全保障法」および第 2 部「サイバー武力紛争法」からなり，これらは「有事・戦時」を対象にしたものである．その後，さらに「平時」におけるルールにつき検討がなされ，『サイバー行動に適用される国際法に関するタリン・マニュアル 2.0』（Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations）がまとめられ，2017 年 2 月に同じく Cambridge University Press から刊行された．

タリン・マニュアル 2.0 は 154 の規則とコメンタリからなり，第 1 部「一般国際法とサイバー空間」，第 2 部「国際法の特別の体制とサイバー空間」，第 3 部「国際の平和及び安全とサイバー活動」，第 4 部「サイバー武力紛争法」から構成されている．第 3 部の一部と第 4 部はタリン・マニュアル 1.0 をほぼそのまま取り入れている．

私自身は，legal experts の 1 人としてタリン・マニュアル 2.0 の作成に関与し，2015 年 6 月から 2016 年 3 月にかけて 3 回にわたり各 1 週間開催されたタリンでの会議に参加した．英語の原著は 598 ページからなる大部のものであり，相当複雑な議論も展開されているため，各規則の訳とコメンタリの要旨を日本の読者に分かりやすく示す必要があると感じ，河野桂子氏（防衛研究所，現在，NATO CCDCOE）および黒崎将広氏（防衛大学校）とともに『サイバー攻撃の国際法　タリン・マニュアル 2.0 の解説』を 2018 年 4 月に信山社から刊行した．

タリン・マニュアルは，サイバー攻撃に関する国際法ルールを「作成」したり「提案」したりするものではない．既存の慣習国際法（国際社会のすべての国家に等しく適用される不文法）がサイバー空間にも適用されるという前提（これは西側先進諸国を中心とする少なからぬ諸国家の基本的立場でもある）の下に，サイバー攻撃に適用される慣習国際法を明文化し，コメンタリとともに記

述するという作業である．Pablo Picasso は“I do not seek, I find.”と言ったが，まさに慣習国際法を「発見」するという地味だが重要かつ容易ではない作業である．

タリン・マニュアル 2.0 の主な内容

タリン・マニュアル 2.0 は，次の 20 項目から構成されている．

第 1 部「一般国際法とサイバー空間」（General International Law and Cyberspace）は，1. 主権（Sovereignty, 規則 1 ～ 5），2. 相当の注意（Due Diligence, 規則 6 ～ 7），3. 管轄権（Jurisdiction, 規則 8 ～ 13），4. 国家責任法（Law of International Responsibility, 規則 14 ～ 31），5. それ自体は国際法によって規律されないサイバー行動（Cyber Operations not per se Regulated by International Law, 規則 32 ～ 33）からなる．第 2 部「国際法の特別の体制とサイバー空間」（Specialised Regimes of International law and Cyberspace）は，6. 国際人権法（International Human Rights Law, 規則 34 ～ 38 ），7. 外交及び領事法（Diplomatic and Consular Law, 規則 39 ～ 44），8. 海洋法（Law of the Sea, 規則 45 ～ 54），9. 航空法（Air Law, 規則 55 ～ 57），10. 宇宙法（Space Law, 規則 58 ～ 60），11. 国際電気通信法（International Telecommunication Law, 規則 61 ～ 64）かならなる．第 3 部「国際の平和及び安全とサイバー活動」（International Peace and Security and Cyber Activities） は，12. 平和的解決（Peaceful Settlement, 規則 65），13. 干渉の禁止（Prohibition of Intervention, 規則 66 ～ 67），14. 武力の行使（Use of Force, 規則 68 ～ 75），15. 集団的安全保障（Collective Security, 規則 76 ～ 79）からなる． 第 4 部「サイバー武力紛争法」（The Law of Cyber Armed Conflict）は，16. 武力紛争法一般（The Law of Armed Conflict Generally, 規則 80 ～ 85），17. 敵対行為の遂行（Conduct of Hostilities, 規則 86 ～ 130），18. 特定の人，物及び活動（Certain Persons,Objects,and Activities, 規則 131 ～ 145），19. 占領（Occupation，規則 146 ～ 149），20. 中立（Neutrality, 規則 151 ～ 154）からなる．タリン・マニュアル 2.0 は，サイバー攻撃が各分野の国際法ルールとの関連でどう位置づけられるかを包括的に検討した成果であり，サイバー攻撃という観点から国際法全般を鳥瞰するものとなっている．

ここでは，以下，タリン・マニュアル 2.0 の主な内容について概観することにしたい．

第 1 に，サイバー攻撃の定義について．規則 92 は，「サイバー攻撃とは，攻撃としてであるか防御としてであるかを問わず，人に対する傷害若しくは死，又は物に対する損害若しくは破壊を引き起こすことが合理的に予期されるサイバー行動である」と規定する．データへの攻撃を目的とするサイバー行動も，個人の死傷や物体の損壊・破壊をもたらすことが予見可能である場合にはサイバー攻撃となる．

第 2 に，主権侵害と干渉について．規則 4 は，「国家は，他国の主権を侵害するサイバー行動を行ってはならない」と規定する．領域外からのサイバー行動については，サイバー・インフラの物理的損害が発生した場合のみならず機能の喪失が生じた場合も主権侵害となる．政府機能の行使に必要なデータの改変・削除も主権侵害となる．干渉の禁止については，規則 66 は，「国家は，他国の国内又は対外事項に，サイバー手段による場合も含め，干渉してはならない」と規定する．ここで禁止される干渉とは国家が自己決定できる事項（国内管轄事項）に対して強制を伴う介入をすることである．

第 3 に，武力攻撃と自衛について．一定以上の「規模および効果」を有するサイバー攻撃は国際法上の「武力攻撃」に該当する．その場合には，武力攻撃を受けた国は個別的自衛権の発動が，その友好・同盟国は集団的自衛権の発動が可能となる．規則 71 は，「武力攻撃の水準に至るサイバー行動の目標となる国家は，固有の自衛権を行使することが

できる．サイバー行動が武力攻撃に該当するか否かは，その規模および効果による」と規定する．多数の人間を殺傷したり，財産に重大な損害・破壊をもたらすサイバー行動は，武力攻撃に必要な規模および効果を有する．自衛権の発動としての措置は，サイバー手段によるものと非サイバー手段によるものの双方が想定される．個別的自衛権の行使には，「必要性と均衡性」（規則 72）および「急迫性と即時性」（規則 73）の要件を満たす必要があり，集団的自衛権の行使にはさらに「被害国の要請」（規則 74）の要件も満たす必要がある．なお，テロリスト等の非国家主体によるサイバー攻撃も武力攻撃の主体になり得るため，これに対して自衛権の行使が可能というのが，legal experts の多数意見である．ただし，主権原則を規定する上記の規則 4 との関連で，自衛権が行使できるのは，非国家主体の所在地国の同意がある場合か，所在地国が武力攻撃に効果的に対応する意思または能力を欠いている場合に限られる．先制的自衛については，実行可能な最後の防衛の機会だと考えられる場合には認められるという見解が多数意見であった．

第 4 に，国際法上違法な（ただし武力攻撃には至らない程度の）サイバー攻撃に対しては，被害国は対抗措置（countermeasures）をとり得る．規則 20 は，「国家は，他国が自国に対して負う国際法上の義務違反への反応として，対抗措置（性質上サイバーであるか否かを問わない）をとる権限を有する」と規定する．対抗措置には，サイバー手段によるものも想定され得るが，現実には対抗措置の中心を成すのは経済的措置である．サイバー攻撃が発生した場合に被害国がとる反応で現実に採用かつ公表されているものは，サイバー手段による反撃ではなく，経済的な措置（特にサイバー攻撃に責任を有する個人や団体の金融資産の凍結）である．なお，外交上の措置（相手国の外交官・領事官の追放や大使館・領事館の閉鎖命令，自国の外交官・領事官の召喚や大使館・領事館の閉鎖など）も経済的措置と同様にサイバー攻撃への反応として発動されるが，こういった外交上の措置は非友好的であってもそれ自体裁量的にとり得る報復（retorsion）であって，対抗措置とは国際法上区別される．対抗措置が容認される（＝違法性が阻却される）ためには，均衡性（規則 23）をはじめとする要件を満たす必要がある．規則 24 は，「被害国のみが対抗措置（性質上サイバーであるか否かを問わない）をとることができる」と規定する．対抗措置をとることができるのは国家のみであり，たとえばサイバー攻撃を受けた企業自らが対抗措置をとることはできない．また，直接の被害国以外の第三国が対抗措置をとることは通常はできない．

第 5 に，国家機関によるサイバー攻撃について．規則 15 は，「国家機関又は国内法によって統治権能の一部を行使する権限を付与された個人若しくは団体によってなされたサイバー行動は，当該国に帰属する」と規定する．法令や契約によって他国にサイバー攻撃を行う法的権限を付与された企業の行動も，国家に責任が帰属する．企業が権限を逸脱してハック・バックをした場合にも，その行為は国家に帰属する．なお，ゾンビ・コンピュータによる DDos 攻撃のような場合もあるため，ある国家のサイバー・インフラからサイバー攻撃がなされたからという事実だけでは，当該国に責任が帰属するという証拠としては不十分である．

第 6 に，私人等の非国家主体によるサイバー攻撃について．規則 17 は，「非国家主体によってなされたサイバー行動は，次の場合に国家に帰属する．(a) その指示に従い又はその指揮若しくは命令下でなされた場合，又は (b) 国家が当該活動を自己の活動として認め，かつ採用した場合」と規定する．非国家主体には，個人のハッカー，ハッカー集団，サイバー犯罪組織，IT 関連企業，サイバー・テロリスト，反政府勢力等が含まれる．なお，(a) 又は (b) に該当しない場合には，国家は私人によるサイバー攻

撃に関して一切の責任を負わないわけではなく，次に見る相当の注意を欠いていた場合には，結果として責任を負うことになる．国際法の国家責任のルールに従い，私人によるサイバー攻撃に対しては，私人の本国や領域国には直接国家責任は帰属しないが，相当の注意義務を欠いたために損害が生じた場合には，相当の注意義務の不作為故に結果として当該国に国家責任が生じることになる．

第 7 に，相当の注意と経由国の責任について．規則 6 は，「国家は，自国の領域又は自国の政府の支配下にある領域若しくはサイバー・インフラが，他国の権利に影響を与え重大で有害な結果を生じるサイバー行動のために使用されることを許さないよう，相当の注意を払わなければならない」と規定する．規則 7 は，「相当の注意義務は，他国の権利に影響を与え重大で有害な結果を生じるサイバー行動を終了させるために，国家が当該状況において実行可能なすべての措置をとることを要求する」と規定する．相当の注意義務の程度は，先進国と途上国では異なり得る．経由国の責任に関しては，規則 6 のコメンタリでは，A 国に所在するハッカー集団が C 国にあるサイバー施設を使って B 国に対するサイバー攻撃を実施したが，C 国がそれを知りながらも攻撃を終了させるための実行可能な措置をとらなかった場合には，C 国は相当の注意原則の違反になるとする．これに対して，たとえばデータが通過するだけの国家が相当の注意義務を負うかについては，サイバー行動を了知し，かつそれを終了させるため実行可能な措置をとれる場合には，相当の注意義務を負うが，通過国は一般には悪意あるトラフィックを了知し得ないので，相当の注意義務を負う場合は現実には例外的になると考えられる．

第 8 に，サイバー諜報（cyber espionage）について．「5. それ自体は国際法によって規律されないサイバー行動」は，サイバー諜報を念頭においている．規則 32 は，「国家による平時のサイバー諜報はそれ自体は国際法に違反しないが，それを遂行する方法は国際法違反となり得る」と規定する．諜報（スパイ行為）一般は，国際法上，禁止はされていないが，各国の国内法で刑事罰を科すことは可能という独自の法的性質を有している．サイバー諜報についても基本的に同様であり，サイバー諜報それ自体は国際法違反とはいえないが，行動によってはたとえば干渉という国際法違反になることがある．

第 9 に，サイバー通信の停止について．規則 62 では，「(a) 国家は，部分的又は完全に，自国領域内における国際サイバー通信業務を停止することができる．当該停止の即時の通知が他国に対してなされなければならない．(b) 国家は，国内法令，公の秩序若しくは善良の風俗に反すると認められ，又は国家の安全にとって危険である私用のサイバー通信の伝達を停止することができる」と規定する．この規定は，国際電気通信連合（ITU）憲章 35 条及び 34 条 2 項に基づくものである．2011 年のアラブの春のように反体制運動が SNS で広まった際に国家がサイバー通信を停止することは，国際電気通信法の下では国家の権利であるが，規則 35「個人は，サイバー関連活動に関し，他で享受するのと同じ国際人権を有する」には違反する可能性があることに留意する必要がある．

第 10 に，軍事目標主義について．規則 99 は，「民用物はサイバー攻撃の対象とされてはならない．コンピュータ，コンピュータ・ネットワークおよびサイバー・インフラは，それらが軍事目標である場合にはサイバー攻撃の対象となる」と規定する．規則 100 は，「民用物は，軍事目標ではないすべての物をいう．軍事目標は，その性質，位置，用途又は使用が軍事活動に効果的に資するものであってその全面的又は部分的な破壊，奪取又は無効化が，その時点における状況において明確な軍事的利益をもたらすものをいう．軍事目標はコンピュータ，コンピュータ・ネットワークおよびサイバー・インフラを含み得る」と規定する．武力紛争法の基本原則の 1 つである軍事目標主義は，1949 年ジュネーヴ条

約第 1 追加議定書 52 条でも規定されており，タリン・マニュアルでも採用されている．なお，民生及び軍事の両用に使用される物については，規則 101 が,「民用及び軍事の双方の目的に私用される物（コンピュータ，コンピュータ・ネットワークおよびサイバー・インフラを含む）は，軍事目標である」と規定する．

タリン・マニュアルの評価と残された国際法上の課題

タリン・マニュアルは，個人的資格でタリンに集った有識者が考えるサイバー攻撃に関する国際法にとどまるものであるが，ほかに包括的にサイバー攻撃に関する国際法ルールを提示したものがないこともあって，国際社会においてすでに一定の権威を有する文書になっている．Legal experts は，各国政府や国際組織が参照・引用してくれることを期待しつつ，タリン・マニュアルを作成した．ただし，タリン・マニュアル 2.0 が公表されてから 3 年経つが，諸国家の反応はいまだ様子見といったところである．諸国家としては，サイバー攻撃をめぐる状況がどう推移するか不明確な現状において,「規則○○は慣習国際法になっているが，規則 XX は慣習国際法になっていない」といった何らかの見解を表明することが，将来自国にとって不利な証拠となることを恐れて慎重になっているのかもしれない．国連では，サイバーセキュリティに関する政府専門家会合（GGE）が 2004 年以来，5 会期にわたって検討をしてきたが，サイバー空間に国際法が適用されることについては共通の了解が得られたものの，西側諸国と中国・ロシア等との見解の対立等から，国際法の実体内容の詳細については目立った成果はなかった．2018 年 12 月の国連総会決議に基づき，第 6 会期の GGE が立ち上がり，2021 年の国連総会で報告書を提出することになっている（また，サイバーセキュリティに関する国連オープン・エンド作業部会も 2018 年の国連総会決議に基づき創設された）．

もちろん，タリン・マニュアルは万能のものではない．タリン・マニュアルはサイバー攻撃に関する詳細な実体ルールを示したが，現実に最初に問題となる「誰がサイバー攻撃をしたか」をはっきりさせるのに必要な事実認定の機関は国際社会には存在せず，また事実認定と証拠に関する手続ルールはタリン・マニュアルの射程範囲外である（タリン・マニュアルはすでに完結したプロジェクトであり，タリン・マニュアル 3.0 は想定されていない）．有責者の確定にあたっては，立証の程度を従来の国際裁判で用いられてきた一般的基準よりもゆるやかなものにしないと，およそ立証が困難になるといった指摘もなされている．

サイバー攻撃に対処するためには，さらに，信頼醸成措置（Confidence Building Measures）や能力構築措置（Capacity Building Measures）も重要である．信頼醸成措置は冷戦下の米国・ソ連間および西側諸国・東側諸国間の一連の合意（米ソホットライン協定，米ソ核戦争防止協定，米ソ公海事故防止協定，欧州安全保障協力会議ヘルシンキ最終議定書など）を端緒とするものであり，潜在的な敵対国との間での緊張緩和や緊急時対応等を内容とするものである．サイバー分野での信頼醸成措置として，米国とロシアが 2013 年 6 月 17 日に「情報・通信技術の安全に関する協力」（Cooperation on Information and Communications Technology Security）という合意文書をとり交わしたことが注目される．同文書において，米ロは，① Computer Emergency Response Teams（CERT）間のリンク，②核リスク減少センターを通じての通報の交換，③ホワイトハウス・クレムリン間の直接コミュニケーション・ラインの創設，の 3 点で合意した．また，米国と中国は，2015 年 9 月 25 日に，両国は知的財産権のサイバー窃盗を行ったり知りながらサポートしたりしないことで合意し，ロシアと中国は，2015 年 4 月 30 日に，

互いにサイバー攻撃を行わないことで合意した．信頼醸成措置は，意図的なサイバー攻撃には無力かもしれないが，偶発的なサイバー攻撃を予防し，また損害を小さくするためには一定の効果を有し得るものである．

なお，信頼醸成措置はより広い意味で用いられることがあり，たとえば，外務省 Web サイト「サイバーセキュリティ 日本のサイバー分野での外交（https://www.mofa.go.jp/mofaj/annai/page5_000250.html）では，信頼醸成措置の推進の中に，米国，オーストラリア，英国，フランス，インド，イスラエル，エストニア，ロシア，EU，ASEAN 等とのサイバー対話，日中韓 3 カ国の枠組での協議・対話や ASEAN 地域フォーラム（ARF）におけるサイバーセキュリティに関する会期間会合が紹介されている．能力構築措置は，主に先進国から途上国へのサイバー・セキュリティ分野での人材・技術・資金等の支援である．上記の外務省 Web サイトによると，日本は ASEAN 諸国に対して，重要インフラ防護，サイバー犯罪対策，CRIST（Computer Security Incident Response Team），法執行機関の能力強化等の支援を進めている．

サイバー攻撃対処条約は必要であろうか．西側諸国の見解は，すでにサイバー攻撃に関する慣習国際法が存在するから新たな条約は不要というものである．これに対して，中国やロシアや一部の途上国の見解は，必要というものである．ただし，ここには裏があることに注意しなければならない．後者の諸国がサイバー活動について最も恐れているのは，アラブの春の再現（反体制活動が SNS を通じて広まること）であり，新たな条約には情報の国家統制条項を入れことを最重要視していることである．これに対して，西側諸国の見解は表現の自由，情報の自由を最重要視している．もし国連総会でサイバー攻撃対処条約が議論されるとなると，多数派を占めるのは途上国であり，その多くは非民主主義国家であるため，情報の国家統制条項が入ってしまう可能性が高い．さらに，条約作成には長年を要する上，サイバー攻撃を行っていると疑われる肝心の国家は条約に入らないかもしれない．「すでに慣習国際法は存在し，適用できる以上，新たな条約は不要」という西側諸国の見解は，こうした裏事情まで勘案すると，合理的であることが分かる．そして，慣習国際法を同定する際に最も有用な指針となるのが，まさにこのタリン・マニュアルなのである．この意味で，タリン・マニュアルはサイバー空間における「法の支配」に大きな貢献をしたものといえよう．

（2020 年 3 月 4 日受付）

中谷和弘
1983 年東京大学法学部卒業．東京大学法学部助手，助教授等を経て，1999 年より東京大学大学院法学政治学研究科教授．国際法専攻．日本学術会議会員，サイバーセキュリティ―戦略本部本部員．

［サイバー・ウォーズ］

応
般

⑤ ロシアのインテリジェンス機関とICT

小泉　悠 | 東京大学先端科学技術研究センター

サイバー空間で存在感を増すロシア

サイバー時代の安全保障を論じるにあたり，ロシアは台風の目となった感がある．実際，米国大統領選への介入をはじめとして，サイバー空間におけるロシアの存在感はかつてなく高まっており，メディアでもロシアのサイバー戦について目にする機会が増えた．他方，こうした領域におけるロシアの活動実態は，同国の秘密主義もあってことさらに分かりにくく，誰がどのような手段を用いているのかが今ひとつ明確に論じられていないようにも思われる．

そこで本稿では，ロシアにおけるインテリジェンス機関の活動，特に情報通信技術（ICT）を用いたそれについての解説を試みた．ロシアにはどのようなインテリジェンス機関が存在し，どのような活動を展開しているのか，その中でICTがどのような役割を果たし，どの程度のインパクを有しているのかがここでの焦点である．

「インテリジェンス」と「インテリジェンス機関」

インテリジェンス機関について論じるには，まず「インテリジェンス（Intelligence）」という言葉の意味するところを定義する必要があろう．小林の整理によれば，この言葉は主に①プロダクトとしてのインテリジェンス（政策決定者に提供される分析・加工された知識），②プロセスとしてのインテリジェンス（プロダクトを生産するための情報の要求，収集，分析，報告，フィードバックのサイクル），③組織としてのインテリジェンス（インテリジェンス活動に従事する情報機関）の3つに分類することができる[1]．

このうち，インテリジェンス活動の具体的な内容を示すのは②であり，一般的に情報収集手段別に次の4つに分類されることが多い．

- HUMINT：人的インテリジェンス（合法・非合法の人的接触によって得られた情報の分析･加工）
- SIGINT：信号インテリジェンス（通信等，電気信号の傍受によって得られた情報の分析・加工）
- IMINT：画像インテリジェンス（偵察機や偵察衛星等が撮影した画像情報の分析・加工）
- OSINT：オープンソース･インテリジェンス（公開情報の分析・加工）

ここで注意すべきは，インテリジェンス・プロセスがインテリジェンス機関の活動全体と必ずしも一致しないということである．後述するように，ロシアのインテリジェンス機関が関与する活動はきわめて幅広い分野にわたっており，狭義のインテリジェンス活動は全体のごく一部であるとさえいえる．

また，インテリジェンス機関といってもさまざまであり，広義には検察などの捜査機関や税務機関まで含まれる場合がある．しかし，本稿では論点の拡散を防ぐため，これを「ラズヴェートカ（разведка）」に従事する機関に限定したい．これは何かを探り出す行為全般を指すロシア語であり，たとえば資源業界では探鉱の意味で用いられる．一方，国家や安全保障の文脈でこの言葉が用いられる場合，その意味

するところは，狭義のスパイによる諜報活動や軍事的な偵察活動と理解することができよう．

現在のロシアにおいて，こうした文脈で「ラズヴェートカ」に従事する機関は，旧国家保安委員会（KGB）系の情報機関である連邦保安庁（FSB）および連邦対外情報庁（SVR），そしてロシア軍参謀本部直轄の情報機関である情報総局（GRU）の3つである（ちなみにGRUやSVRの「R」はこのラズヴェートカの頭文字を取ったもの）．各機関の活動内容はそれぞれの出自や任務によって異なるが，表-1はこれを「○」（各機関が主たる任務として実施しているもの），「△」（副次的任務として実施されていると推測されるもの），空欄（ごく不活発ないしまったく実施されていないと考えられるもの）に分類した．

ここから読みとれるように，GRUは三大インテリジェンス機関の中で唯一，外国における公然・非公然のHUMINT能力を有している．また，GRUは航空宇宙軍の運用する偵察衛星や偵察機，海軍の運用する情報収集艦や深海工作艇，GRU直轄の電波傍受基地等，大がかりなアセットを用いたSIGINTおよびIMINTを実施する能力を有する点でも旧KGB系機関とは一線を画す．

一方，FSBはKGBの国内監視機関であった第2総局（VGU）を中心とし，プーチン政権下では同じく旧KGB系の国境警備機関や通信傍受機関，対テロ特殊部隊等がここに統合された．本稿のテーマとの関連においては，電話・インターネット監視システムである「即時捜査手段システム（SORM）」によってロシア国民のインターネット・トラフィックを無制限に監視・追跡し得る能力を有している点が言及されるべきであろう．これらのHUMINT/SIGINT能力は主としてロシア国内での反体制派，チェチェン等の非合法武装勢力，組織犯罪等の監視に用いられているが，一部ではこれら監視対象組織に対するインテリジェンス活動が国外でも展開されていると見られる．

SVRの前身はKGBの国外諜報機関であった第1総局（PGU）であり，いわゆるスパイ活動を主任務とする．ただ，PGUは外国に設置した電波傍受拠点を用いたSIGINTも行っていたとされ，恐らく現在のSVRも同様であろう．

まとめるならば，ソ連のGRUとKGBは共にインテリジェンス活動の一環として大規模なSIGINTを実施してきたのであり，現在のロシアがサイバー空間でICTを用いて展開している諜報活動（エスピオナージュ）はその延長上に位置付けることができよう．

ただし，ICTが持つ意味はこれにとどまらない．元々ロシアのインテリジェンス機関は狭義のインテリジェンスに限らず，多様な活動を担ってきた．GRU，FSB，SVRが国内外での暗殺や，ICTを用いたサイバー破壊活動，偽情報（フェイクニュース）の流布による情報操作といった活動（詳しくは後述）を多数実施していることはその好例である．ICTを用いたものに限って言えば，インテリジェンス機関が関与する活動は表-2のように整理することができよう．

表-1　ロシアのインテリジェンス機関とその活動内容

類型	具体的な活動内容	旧KGB系機関		ロシア軍
		FSB	SVR	GRU
HUMINT	外国における公然活動（武官派遣等）			○
	外国における非公然活動（諜報活動等）	△	○	○
	国内における反体制派等の監視	○		
	国境における出入国管理	○		
SIGINT	航空機・艦艇・人工衛星によるSIGINT	△		○
	外国における通信傍受等	○	○	○
	国内における通信傍受等	○		
	保秘通信回線等の運用	△	△	△
OSINT	外国の公開情報分析	○	○	○
	国内の公開情報分析	○	△	△
IMINT	航空機・艦艇・人工衛星によるIMINT	△		○

（出典）筆者作成

すでに述べたように，サイバー空間におけるエスピオナージュは古来から行われてきたSIGINT活動の延長にあり，これはコンプロマートも同様である．インテリジェンス機関が入手した情報を用いてターゲットの名誉を毀損したり，その可能性を示唆することで協力を強制する事例はインテリジェンスの歴史上，きわめて古くから観察されてきた．この意味では，ICTは古典的インテリジェンス活動に新たなツールを付加したものにすぎないが，そのターゲットとなる社会，経済，安全保障等がますますサイバー空間に依存するようになりつつあることは，インテリジェンス全体におけるICTの重要性を増加させているといえよう．情報操作もまた，インテリジェンス機関の活動類型としてやはり古くから存在してきたが，ICTはその影響力をかつてなく拡大する役割を果たした．ソーシャル・ネットワーキング・サービス（SNS）等，個人への伝達性が高いサイバー・メディアを用いることで，偽情報や歪曲された情報をより的確に，広範囲に流布することが可能となるためである．

一方，ICTはインテリジェンス機関の活動に新たな領域，すなわちサイバー・サボタージュを作り出した．ブッシュ（George W. Bush）政権およびオバマ政権においてサイバー安全保障担当の大統領補佐官を務めたリチャード・クラーク（Richard A. Clark）らが述べるように，コンピュータで制御される産業・金融インフラやオフィス機器は，それが閉鎖型ネットワークであるか否かを問わず，敵対勢力にとって格好の攻撃対象となる[2]．社会の中に広く，膨大に存在しているコンピュータ制御機器が暴走すれば，大規模な火災や爆発が発生し，社会活動を大混乱させ，経済を崩壊させることも不可能ではないためである．これは，かつて破壊工作員や戦略爆撃機が担っていた任務をサイバー空間経由で実施するものと位置付けられよう．

ロシアはサイバー空間で何をしているか

概念的整理は以上のとおりとして，今度はロシアのインテリジェンス機関が実際にどのようなオペレーションを展開しているのかを見ていこう．

まずは概況である．米国の戦略・国際研究所（CSIS）は，政府機関，軍需企業およびハイテク企業が標的となったサイバー攻撃および100万ドル以上の損害を出したサイバー攻撃を「顕著なサイバー事案」と定義し，2006年から事例を収集してきた．これによると，ロシアは中国に次いで世界第2位のサイバー攻撃発信地であり，2019年前半までの約13年間で合計100件近い事例が確認されている[3]．この中には国家が関与しないサイバー犯罪も含まれていようが，その多くは軍や情報機関が実施ないし実施の指令・調整を担当する国家的なサイバー活動であると考えられる．

しかも，ICTを用いたロシアのインテリジェンス機関の活動は，表-2で示した諸類型をほぼ完全にカバーする，フルスペクトラムなものである．以下，過去の事例から主要なものを挙げてみたい．

エストニアに対するサイバー・サボタージュ

2007年4月，旧ソ連のエストニアでロシア系住民による大規模な暴動が発生すると，その翌日からエストニアの政府機関，メディア，銀行システムなどが一斉にDDoS攻撃を受け始め，社会システム

表-2　ICTを用いたインテリジェンス機関の活動

類型	内容
諜報（エスピオナージュ）	サイバー空間における情報の窃取
名誉毀損（コンプロマート）	入手した情報の流布による名誉毀損またはその脅し
情報操作	事実に基づかないものを含めた情報の流布・歪曲による民心の捜査
破壊活動（サボタージュ）	サイバー空間を経由した物理的・非物理的打撃

（出典）筆者作成

が麻痺状態に陥った．のちに「タリン事件」と呼ばれるこの出来事は，サイバー攻撃が一国の首都機能を麻痺させた初の事例とされ，北大西洋条約機構（NATO）によるサイバー防衛卓越研究拠点（NATO CCDCOE）の設置やサイバー攻撃に対する対処指針（「タリン・マニュアル」）の策定につながった．

ところで，この攻撃はそれまで知られていたDDoS攻撃のような一過性のものではなく，数週間に渡る継続的な攻撃であった点が注目される．また，攻撃には世界50カ国のコンピュータ100万台以上が参加していたが，多くのコンピュータの所有者は攻撃に参加したという自覚はなく，何者かにコンピュータを乗っ取られて「ゾンビ」化させられていた．これだけ大規模なサイバー攻撃を誰が行ったのかは現時点でも明らかでないが，ロシア政府が何らの音頭を取った疑いは濃厚とされている．

グルジア戦争：同時進行する軍事作戦とサイバー戦

2008年8月，グルジアの分離独立地域であるアブハジアおよび南オセチアをめぐってロシアの間で戦争が発生したが，この最中にグルジア政府は間断ないDDoS攻撃を受けた．地上戦が始まる数時間前，StopGeorgia.ruというフォーラムがネット上に出現し，同フォーラムがグルジア政府機関のサーバ一覧を表示してDDoS攻撃を行うようにネットユーザ達に呼びかけたのである．この結果，グルジア政府機関のサーバは軒並みダウンし，ネットを使用した情報収集や連絡・調整，対外広報などが行えなくなってしまった．

当然，StopGeorgia.ruにはロシア政府の関与が伺われる．実際，StopGeorgia.ruに75.126.142.110というIPアドレスを提供していたIT企業Steady-HotをWHOIS検索してみると，その所在地が参謀本部情報総局のすぐ隣のブロックであることが判明したとの報道がある．

SIPRNetへの侵入

2008年10月には，米国の機密ネットワークである「秘密インターネットプロトコル・ネットワーク（SIPRNet）」がロシアによる侵入を受けた．SIPRNetは国防総省が機密情報を扱うために構築した「防衛情報システムネットワーク（DISN）」の一部であり，インターネットには接続されていない孤立型システムであったため，外部からの侵入はそれまで一度も確認されていなかった．のちの調査によると，ロシアの情報機関は米軍基地などあちこちにバックドアを仕込んだUSBメモリを放置し，それを拾った米側職員がSIPRNetに差し込んだことで侵入を許したとされる．

ウクライナ危機とサイバー戦

2014年2月，ウクライナで政変が発生すると，ロシアは軍事介入に踏み切り，これと同時に大規模なサイバー攻撃を展開した．ウクライナ危機におけるサイバー戦の特徴は，敵対国の双方が激しいサイバー攻撃の応酬を展開している点にある．これは敵対国同士が言語を共有しているという特殊性に原因が求められようが，サイバー攻撃が双方向的な応酬として実施された事例は珍しいのではないかと思われる．双方ともに最も多いのはDDoS攻撃で，Webサイトの改ざん等がこれに次ぐが，このほかにもマルウェアを用いてウクライナの送電網管理システムへの攻撃が行われ，大規模な停電が発生した事案（2015年）や，会計ソフトの脆弱性を衝いた広範な政府機関・企業への攻撃で重要インフラが機能不全に陥る事案（2017年）など，烈度の高いサイバー・サボタージュ事例も少なくない．

他方，ウクライナのハッカーグループ「サイバー・フンタ」は，ロシアのウラジスラフ・スルコフ（Владислав Сурков）大統領補佐官（プーチン（Владимир Путин）大統領のブレーンとして知られる）のメールサーバに侵入して大量のメールを窃取し，公開するという攻撃を行った．暴露さ

れた情報は1ギガバイトにもおよび，その中にはロシアによるウクライナ介入の具体的な計画やこれを主導した人物などに関する情報が多数含まれていた．ICTによるエスピオナージュと情報戦の融合事例といえよう．

ロシア・ゲート

2016年の米国大統領選に対するロシアの介入疑惑，いわゆる「ロシア・ゲート」疑惑についてはすでに多くの著作や研究成果があるので，ここでは詳しくは触れない．

ただ，「ロシア・ゲート」が複合的な性格を有していることだけは指摘しておこう．すなわち，①トランプ（Donald Trump）陣営が大統領選を戦うにあたってロシア側となんらかの協力（共謀）を行っていたという疑惑，②ロシアが民主党全国委員会（DNC）等にハッキングを仕掛けてメール類を摂取していたという疑惑，③ロシアがSNSやインターネット広告を用いて大量の偽情報を発信していた疑惑，の三重構造であり，このうち，本稿のテーマに強く関連するのは②であろう．

当時，DNCのサイバーセキュリティはきわめて杜撰であり，ロシアによる侵入は純粋に技術的にみてさほど困難であったとは思われない．侵入が発覚してからの連邦捜査局（FBI）による対応が鈍かったことも，ロシアによる継続的な侵入を許すことにつながった．逆にいえば，ロシアは比較的初歩的なハッキング技術できわめて大きな政治的効果を得たわけであり，サイバー戦の非対称性を示す典型例といえよう．

ハッカーとインテリジェンス機関

プーチン大統領は2017年，「ハッカーというのはフリーのアーティスのようなものだ」と述べたことがある．つまり，ハッカーはそれぞれ自分の興味や愛国心にしたがってハッキングを行っているのであって，政府がそれを統制することはできないという理屈である．

ただし，サイバー戦の実施主体に民間の個人ないし集団が含まれていることはまったくの嘘ではない．多くのケースにおいてGRU，FSB，SVRといった政府機関はサイバー攻撃を自ら実施するのではなく，金銭や愛国心を動機とする民間のハッカーを「サイバー民兵」として組織化し，その実行に当たらせていると見られている[☆1]．

他方，大規模かつ継続的なサイバー戦の実施には相当の金銭的・人的リソースを必要とすることから，サイバー攻撃のすべてが「サイバー民兵」に委託されていることもまた想定しにくい．ロシア発の「先進的かつ継続的な脅威（APT：Advanced Persistent Threat）」としては，APT28やAPT29が知られているが，前者についてはその正体がGRU所属の2つの組織（第26165軍事部隊および第74455軍事部隊）であることが明らかにされている．このほか，継続的なサイバー戦を行っている主要なハッカーグループは，なんらかの形でロシア政府機関と一体ないし密接な関係にあるものと考えられよう．**表-3**は，以上の関係性を整理したものである．

では，こうした広範な活動を展開するインテリジェンス機関同士は，どのような関係にあるのだろうか．つまり，彼らは相互に協力しあっているのか，それとも独立に活動しているのだろうか．

結論を先に述べるならば，各インテリジェンス機関は同一の目標を追求しつつも相互に連携する関係にはない可能性が高い．この点を裏付けるのが，サイバー・インテリジェンス企業Check Point Researchがマルウェア分析ツールの開発企業Intezerと合同で行った調査である．両社は，ロシアのインテリジェンス機関が用いているとされるマルウェアのサンプルを大量に収集し，これを構成するモ

☆1 ジェフリー・カー（Jeffrey Carr）は，グルジアに対するサイバー攻撃に関して，クレムリン（ロシア政府）が「ナーシ」のような官製青年運動にサイバー攻撃任務を与え，「ナーシ」はさらに一般のハッカーを雇って実際のサイバー攻撃部隊にするという三層のモデルを描いている[4]．

ジュールやソースコード間の類似性を独自開発したツールで分析するという手法により，各インテリジェンス機関間の関係性を割り出すことに成功した．以下，両社の報告書[5]の主要な知見のサマリーから，本稿との関連において重要な部分を転載する．

- 本調査は，この種のものとしては初であり，かつ最も包括的である．

  きわめて強力な国家における異なったサイバー諜報機関間の繋がりをマッピングするために，数千のサンプルが初めて収集され，分類，分析された．
- 多くのケースにおいて，ロシアのアクターはほかのアクターとコードを共有していない．

  各アクターは異なったオペレーションのために異なったマルウェア・ファミリー間でコードを使いまわしているが，各アクター間で共有されているツール，ライブラリ，フレームワークは存在しない．
- ロシアにおいて APT に分類されるアクターないし組織は，それぞれ独自のマルウェア開発チームを有しており，長年に渡って似たようなマルウェア・ツールキットとフレームワークを別個に開発してきた．これら多くのツールキットが同じ目的に用いられていることを考えると，これら別個の活動には冗長性があるということになろう．
- これらの発見は，ロシアがオペレーションを安全に行うために多大の努力を図っていることを示している．

  異なる組織が広範なターゲットに対して同じツールを使い回すのを避けることにより，彼らはあるオペレーションが露見してもほかのオペレーションが危険に曝されないようにすることができる．

要するに，ロシアのインテリジェンス機関は独自のマルウェア開発部門を抱え，似たような目的のためであってもほかの機関が開発したマルウェアを流用することはしていない（あるいはそうした協力を行う関係にはそもそもない）ということである☆2．

☆2 問題の報告書によると，異なるインテリジェンス機関のマルウェア間にも共通性が存在するケースが稀にではあるが観察される．ただし，これはダーク Web 等で配布されたオープンソースを用いた結果であり，インテリジェンス機関間の連携の結果ではないとされている．

表 -3　ロシアの主要なハッカーグループと政府機関との関係

グループ名	別名	想定される上位・関連組織	主要な活動
APT28	Pawn Storm, Fancy Bear, Sofacy, Tsar Team, Strontium, Sednit	GRU	・米大統領選挙への介入（2016 年） ・欧州諸国・国際機関に対する侵入 ・その他多数
APT29	Dukes, Cozy Bear, Monkey	FSB または SVR	・米大統領選挙への介入（2016 年） ・米国を含む世界各国の国家機関に対する侵入 ・その他多数
Turla	Snake, Venomous Bear, Uroburos, Group 88, Waterbug	FSB	・スイス国防省・軍需企業に対する侵入 ・東欧諸国の領事館に対する侵入 ・韓国政府機関に対する侵入
Black Energy	Sandworm, Voodoo Bear, Electrum	不明（GRU ？）	・グルジアへの DDoS 攻撃（2008 年） ・ウクライナの電力網に対するマルウェア攻撃（2015 年）
Koala	Energetic Bear, Dragonfly, Group 24, Crouching Yeti	不明（ロシア政府が関与）	・エネルギー，原発，水，航空，重要製造業等に対する侵入（2014 年～）
TEMP.Armaggedon	-	不明（ロシア政府が関与）	・ウクライナの保安・法執行機関に対する攻撃
TEMP.Isotope	Dragonfly 2.0, Energetic Bear	不明（ロシア政府が関与）	・米国の電力網に対する侵入
TEMP.Veles	-	中央化学機械研究所（TsNIIKhM）	・産業用制御システム（ICM）に対する侵入

（出典）筆者作成

サイバー時代におけるロシアとの向き合い方

本稿の主な結論は次のとおりである．

第1に，ICTは，インテリジェンス機関が古典的な活動を新たな手段で継続するためのツールであり，しかもその効果はICTの普及によってきわめて大きくなっている．ことにロシアのインテリジェンス機関がSNSを用いて米国のような先進国の社会を大きく揺るがせたことは，今後の安全保障を構想する上で大きなインパクトを有しているといえよう．

第2に，ICTを用いたインテリジェンス機関の活動は物理領域にも及ぶようになっている．戦時の破壊活動や限定的な暗殺に限らず，きわめて低コストかつ短時間で社会や政治に混乱や破壊をもたらす能力をロシアのインテリジェンス機関は有するようになった．これは狭義のインテリジェンスという観点からのみロシアのインテリジェンス機関を理解することがますます困難になりつつあることを意味する．

第3に，ロシアのインテリジェンス機関は相互に独立して任務を遂行しており，単独の事案を阻止しても同じような事案が別の手段で遂行される可能性が高い．ここまで述べてきたことを併せて考えるならば，Check Point ResearchとIntezerが用いたような大規模な計量的手法によってロシアのインテリジェンス機関が有する能力を全体として把握し，抑止・対処戦略へとつなげる必要があろう．

参考文献

1) 小林良樹：インテリジェンスの基礎理論，立花書房，pp.6-8 (2011).
2) リチャード・クラーク，ロバート・ネイク：世界サイバー戦争，徳間書店（2011）．（原題：Richard A. Clark and Robert K. Knake : CYBER WARFARE : The Next Threat to National Security and What to Do About It, Harper Collins, 2010）．
3) CSIS, Significant Cyber Incidents, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
4) Carr, J. : Inside the Cyber Warfare : Mapping the Cyber Underground, O'Reilly, pp.118-119 (2011).
5) Cohen, I. and Bassat, O. B. : Mapping The Connections Inside Russia's APT Ecosystem, Check Point Research and Intezer (2019), https://research.checkpoint.com/2019/russianaptecosystem/

（2020年3月25日受付）

小泉　悠　nuclearblue1982@gmail.com

1982年千葉県生まれ．早稲田大学大学院政治学研究科修了（修士）．民間企業勤務，外務省専門分析員，ロシア科学アカデミー客員研究員，（公財）未来工学研究所特別研究員等を経て2019年より現職．ロシアの軍事・安全保障政策を専門とし，『「帝国」ロシアの地政学』（東京堂出版）等の著書がある．

［サイバー・ウォーズ］

⑥ 座談会：技術者とサイバー・ウォーズ

―アルゴリズムやフェイクニュースが“兵器”に―

栗原　聡（慶應義塾大学）　鳥海不二夫（東京大学）　平　和博（桜美林大学）　須川賢洋（新潟大学）
司会：長倉克枝（東京大学）　江間有沙（東京大学）

アルゴリズムやフェイクニュースが“兵器”として使われる事例が相次ぐ中，技術者は何に気をつけ，どうしていけばよいのか．さまざまな立場の専門家に語っていただいた．

“兵器”としてのフェイクニュース

長倉：中国やロシアの「ハイブリッド戦争」では，サイバー戦や情報戦が組み合わされ，アルゴリズムやフェイクニュースが“兵器”として使われることが指摘されています．平さんはご著書『悪のAI論　あなたはここまで支配されている』（朝日新書）などでも書かれていますが，最近の事例をご紹介いただけますか．

平：典型的なハイブリッド戦争は，2014年のロシアによるクリミア併合前後のウクライナ危機です．リアルの武力に加えて，サイバー攻撃とフェイクニュースの組合せの中でロシアが作戦を展開しました．

一方，フェイクニュースで皆さんが一番ご存知なのは2016年の米大統領選挙ですね．これはリアルの武力は入っていませんが，サイバー攻撃とフェイクニュースを組み合わせた，いわゆるハードパワーとソフトパワーの間のシャープパワーの典型例として挙げられています．たとえば，ロシア軍参謀本部情報総局（GRU）のハッカーの標的型フィッシング攻撃によって，ヒラリー・クリントン（Hillary Clinton）陣営の選挙対策本部長を務めたジョン・ポデスタ（John Podesta）氏のGmailのパスワードが奪われた事件があります．同氏の大量のメールが暴露サイト「ウィキリークス」で公表され，それを“証拠”として，「クリントン氏が児童虐待の地下組織に関与している」という「ピザゲート」と呼ばれる陰謀論が拡散する構図もありました．

このサイバー攻撃とフェイクニュースの組合せという構図は，2020年の米大統領選挙でもすでにその兆候が表れているという報道もあります．

長倉：サイバー攻撃やフェイクニュースの拡散をロ

左から，鳥海氏，栗原氏，平氏，須川氏

シアが行っているということですが，実際に手を動かしているのはどういった人たちですか？

平：米大統領選挙のフェイクニュースを作る部分は，インターネット･リサーチ･エージェンシー（IRA）という，サンクトペテルブルクの組織が主に担っているとされています．ここは民間企業ですが，実質的オーナは「プーチンの料理人」と言われる人物で，GRU の活動と連携していると見られています．

フェイクニュースの拡散は，Facebook や Twitter のようなプラットフォームが主な舞台となります．拡散には，ロシアとは直接の関係がない多様なプレーヤもかかわっています．米国内のトランプ（Trump）支持層や，米ロいずれとも関係のない，広告収入目当てで拡散したマケドニアの若者たち，さらには内容のインパクトから拡散に加担してしまった一般ユーザなどです．“兵器”としてフェイクニュースを仕込んでいる人たちの外縁で，その拡散を知らず知らずに担っている大勢の人たちがいるということになります．

そのベースとなっているのが，人々の関心・注目を集めることが経済的価値を持つという「アテンション・エコノミー」．そして，これに最適化しようとするアルゴリズムを担う IT 企業であり，それを実際に支えているのがソフトウェアエンジニアということですね．

鳥海：なぜフェイクニュースが“兵器”になるかというと，それを喜ぶ人たちがいるところをうまく突いているからです．フェイクニュースを作ったり流したりする技術はいくらでもできますが，それが拡散して人々の心に入っていくのは，技術にプラスして心理的な要素を活かさないといけない．そこには広報的に，人の心に刺さるものを作るという技術も必要ですね．そのフェイクニュースを流したことで喜ぶ人が一定数います．その人たちがフェイクニュースを“真実”に引き上げていくので，結果として無関係の人たちが信じてしまう．

ただ，平さんがおっしゃったサイバー攻撃とフェイクニュースは，分けて考えた方がいい．サイバー攻撃で（フェイクニュースの）ネタを持ってきて，フェイクニュースを作る．つまり，サイバー攻撃は製造側で，フェイクニュース拡散は流通側となります．こう分けて考えたときに，流通側については社会がそれを許容している状況があります．

平：2016 年の米大統領選では，拡散（流通側）についても，ロシアの IRA の関係者が 2014 年頃から米国内で現地調査をして，激戦州に焦点を絞った政治的マーケティング分析を行っています．民間企業がマーケティングをしてターゲティング広告を打つのと同じ手法で，“兵器”としてのフェイクニュースの拡散を行っていると言えます．

鳥海：（ネットで）フィルタバブルが現象として発生していて，そこでエコーチェンバーが起こることが分かっているので，こうしたマーケティングが有効になりました．

須川：従来，選挙や政治に対してこうしたマーケティングは行われてきませんでしたが，これが有効だということが分かってきたので使われるようになってきたということですね？

鳥海：そうですね．本来は候補者にとって有利な情報を流すという正当なやり方だったのが，対抗馬に対して不利な情報を流したりフェイクニュースを流したりする戦略も含めてマーケティングの手法が使われるようになりました．

須川：ディジタル・ゲリマンダの中にフェイクニュースも含まれるという捉え方は，ここ数年で政策科学の研究者の間でも共通認識になっています．そのディジタル・ゲリマンダはハイブリッド戦の 1 つのサブセットになっていますが，そこまではまだ多くの人に認識されていません．選挙や政治の側面でのみ捉えてしまう場合がほとんどで，フェイクニュースが“兵器”だとまで捉えられる人はまだまだ少ないのが現状です．

人間そのものが“兵器”

江間：アルゴリズムが“兵器”になる，というのが今回の対談のテーマですが，何が“兵器”なのかという概念を考え直していく時期にあるという気がしています．

栗原：今のインターネットにしても，SNSのような情報を伝搬させる仕組みにしても，まだまだ技術は未熟な状況です．そして，アルゴリズムが“兵器”という捉え方は否定しませんが，そもそも人間自体が“兵器”なのだと思います．公平な判断などできるわけがなく，自分の好みというフィルタと，自分でも気がつかない自分が持つバイアスを加味して，条件反射的に拡散する場合もあれば，意図的にフェイク情報を流したりもする．

たとえばミサイルのような複雑なシステムは，設計から製造まで入念な計画に従って作業が行われるわけですが，フェイクニュースの拡散による間違った世論形成やデマの拡散による社会混乱発生といった「攻撃」は不特定多数の人々の行為の創発現象により具現化します．フェイクニュースをミサイルに見立てた場合，いつどこで誰がミサイルを発射するのかをあらかじめ特定することはできず，防ぎようがありません．つまり，意図的に創発を制御できる人がいるとすれば，それは確実に成功することになります．

しかし，創発の怖さは作り出す側も完璧に制御できないところにあります．特に意図せず起こる創発が大きな混乱を招きます．そうした創発をどのように解明するのか，どう介入して制御していけるのか，そういった課題の解決こそ僕らがやる仕事であると考えています．僕ら人間はそう簡単に自分たちの行動を変えることはできませんが，テクノロジーが引き起こす現象であれば変えることができるはずです．我々研究に携わる者として一矢報いたい気持ちがあります．

須川：戦国時代でも日露戦争でも情報を“武器”にするということは行われてきましたが，今はネットワークの時代になり，拡散のスピードが速くなりました．もちろんそれは技術のおかげですが，一方でそれを制御するための技術もまた必要になります．

エンジニアと社会の位置関係

長倉：ケンブリッジ・アナリティカ（CA）の元エンジニアで内部告発を行ったクリストファー・ワイリー（Christopher Wylie）は著書で自身のCAでの仕事を振り返り「アルゴリズムは武器だ」と書いています．ただ彼は初めからそう知った上で仕事をしていたわけではありません．エンジニアとして気をつけることはできるのでしょうか？

須川：セキュリティはよく『スター・ウォーズ』のフォースに例えられます．ホワイトサイドorダークサイドという意味ですが，そうなれば当然にダークサイドに墜ちないようにしてほしいです．

鳥海：エンジニアに「あなたのフォースを正しく使いましょう」と言うわけですか．ジェダイはそんなに多くないので監視できていますが，エンジニアは世界に何百万人，何千万人といるので，その人たちに「あなたの作っているものは武器になり得る」と言っても……．よく考えると，ジェダイもちょいちょいダークサイドに落ちてますし．

平：ただ，エンジニアと社会の位置関係はイメー

ジしておいたほうがいいでしょう．国際政治から国内政治，軍事ビジネスに至る色々な場面で，今の社会はソフトウェアでできています．特にフェイクニュース絡みのアテンション・エコノミーで言うと，そこに最適化させたコードやソフトウェアは場合によっては民主主義に具体的なネガティブ・インパクトを与えています．その全体像の中で，エンジニアは，「私がやっていることは何か」というイメージを持つ必要があるのかもしれません．その“兵器”と自分が書いたコードがまったく遮断されたものではなくて，どこかでつながっている可能性があることは，意識しておいた方がいいのではないでしょうか．

まったくイメージしないところでつながってしまうというのは，まさにケンブリッジ･アナリティカの事例，さらにスノーデン事件で明らかになった，米国家安全保障局（NSA）による世界規模のネット監視もそうです．FacebookやGoogleといった民間企業が持っているデータを，テロ監視のような，民間企業の本来の目的や用途とはまったく違う形で使っていた．民間企業のデータが，知らぬ間に安全保障に流用されるという，思わぬ「底抜け」が起きている状況も，目の前の現実として理解しておくことが必要だと思います．

須川：データの収集と利活用は法律に触れる違法なやり方は論外で，ケンブリッジ・アナリティカによるFacebookのデータ利用も明らかな規約違反です．むしろ問題なのはグレーゾーンの場合で，そこに手を付けるかどうかは，エンジニアの倫理観が出てくるところではないでしょうか？．

鳥海：エンジニアとしてはグレーゾーンには手を付けると思うんですね，普通に．ただ，問題はエンジニアの行動原理がどこにあるかで，基本的に企業ならもっと上位で意思決定をしています．そこで意思決定されてエンジニアに指示された場合，それが黒ではなくてグレーで上が責任を持つのなら，エンジニアにはどうしようもないですよね．黒なら「倫理観」で止めることもできるでしょうけれど．そんな状態で「倫理観」と言われても，誰の倫理観かが問題です．それはエンジニアよりも意思決定者の問題になるのではないでしょうか．

栗原：映画『ダイ・ハード4.0』で悪役側がサイバーハッキング用のシステムを作るため，広くプログラマをバイトとして募集するのですが，開発を依頼されるプログラムはハッキングシステムを構成する個々のサブシスシムなので，それ自体では全体のシステム像が分からないような設定となっていましたね．バイトを引き受けたプログラマは，自分たちがまさか悪事の片棒を担いでいるなど思うわけもなかったのです．

最近ではディジタルツインなどと呼ばれますが，実世界を同じものをサイバー空間でも構築する動きもあります．サイバー空間では良いことも悪いことも物理空間と比べてより急速に強調されてしまいます．こうした状況で，何がホワイトでどこからがダークなのかの線引きが曖昧というのはきわめて厄介です．

鳥海：完全なホワイトからダークに落ちる可能性すらいくらでもあります．そこでエンジニアに「気をつけなさい」と言っても，ホワイトなことまでできなくなるだけな気がします．

平：“兵器化”するアルゴリズムの問題は，アルゴリズムとして優れているものが，社会の文脈に落とし込んだときに，相容れない結果を生み出してしまう可能性がある，という点です．たとえば，プ

ロダクトやサービスを作るプロセスのどこかで，エンジニア的ではない価値観を挟むことが必要ではないかな，と考えています．法律やガイドラインによって禁止されていなくても，社会の常識というか，世間知，世間相場のような価値観を入れるべきではないかと．メディアの感覚で言うと「編集」のようなプロセスです．そのプロダクトやサービスが，作り手の本来の意図を超えて，どんなインパクト及ぼす可能性があるのか，といった世間相場の“ものさし”を当ててみるということです．

ユーザ側も倫理観を

長倉：栗原さんは『AI 兵器と未来社会　キラーロボットの正体』（朝日新書）を昨年（2019 年）9 月に出されるなど，メディアでも安全保障と AI について積極的に発言されています．AI 研究者としては珍しいですが，なぜ安全保障と AI にかかわられるのでしょうか？

栗原：僕ら人類は，今のところ，地球における生存競争を生き抜いてきた頂点に君臨してますよね．そして，それをなし得た大きな要因が我々の持つ社会性です．しかし，人間が集団で社会生活を営む場合，実は 300 人くらいの集団が限界だとされていますが，今やそれを大幅に超える複雑な社会に人間は飲み込まれてしまっているのだと思います．もはや自分たちで制御できない状況です．ただ，これを招いたのはテクノロジーなのですから，逆にテクノロジーで解決しなければならない．

一方，進化の大原則は適者生存であり，そもそも生物は適応したものが生き残り，そうじゃないものは淘汰されます．その意味では我々ホモサピエンスなんて最悪ですからね（笑）．ホモサピエンスは同類であるネアンデルタール人を絶滅させ，これまでどれだけの種を絶滅させてきたのか．ホモサピエンスが誕生して数万年ですが，生物学的に，たとえば我々の闘争本能など何も変わっていないのです．それは，昨今の世界情勢を見るに自明かと思います．我々は何の解決もしてないし，進歩もしていない．

長倉：人間には闘争本能があり，そもそも争いは起こるものということですね．

須川：「衝突が起こり得る」という前提のもとで安全保障という概念があるわけですからね．

平：エンジニア，企業といったサービスの作り手だけでなく，受け手，ユーザのリテラシーを底上げしていく必要もあります．たとえば，ハイブリッド戦争の話で言えば，ネットのユーザ一人ひとりがすでに戦争に加担しているという現実がある．それを意識していくことも重要だと思っています．

鳥海：まさにユーザ側の倫理が重要になります．エンジニアが倫理観を持つのは，エンジニアが結果を予見できる状況です．でも，今の社会全体が複雑系になっている状態では，大体の場合予想外のことによって大きなダメージが生じます．そこでは倫理観はなんの役にも立ちません．

そこでは平さんがおっしゃる通り，エンジニアが作ったときには想定しなかった新たに生じた状況に対して，ユーザが何らかの倫理観を持って行動することによって良い方向に収束する可能性はあると思います．

意図的に作った結果なのか，意図せずにできてきた結果なのかによって話が変わってきますが，今は少なくともエンジニアとしては意図しなかったものが他者の手によって新たな方向に持ってい

かれることが非常に多いので，一人ひとりがそういうことが起き得るというふうに考えるしかないんじゃないかと思います．

正しく声を上げる

江間：では『情報処理』読者，特に若い人たちはどうしていけばいいでしょうか．

栗原：正しく声を上げるしかないんじゃないでしょうか．包丁職人は包丁を料理に使ってほしくて作っているし，人を刺すために使ってほしくない．僕らも同じで，悪いことには使ってほしくないですよね．それを言うしかないじゃないですか．

平：今の社会の骨格や基盤はソフトウェアからできていて，エンジニアは社会を支えるさまざまなパーツを作っている．その使命感と倫理観は，明確に持っていてほしいなと思います．

エンジニア一人ひとりの倫理観を表明することは可能だし，それによって倫理観に反する使われ方に歯止めをかける事例もあります．たとえばGoogleが米国防総省のAIプロジェクト「Project Maven」への参加を進めていた中で，現場のエンジニアを含む多くの社員が，それに対して「ノー」と言う声を上げた．結果としてGoogleはその計画をストップさせました．

フェイクニュースについては，アルゴリズムをアテンション・エコノミーに過剰に最適化させてきてしまったことが，今の問題の肝とも言えます．

現在は，このアテンション・エコノミーがすべて，と思ってしまいがちですが，特に若い人たちが，“そうではない枠組み”を発想することで，また違う世界を開いていってほしいと思っています．

鳥海：10年前の社会と今の社会では倫理観が違うんですよね．今，若い人たちに我々が倫理観を押し付けても，10年後，20年後には変わるものです．

須川：僕らは，権力に対して逆らうとか，軍事的な匂いのするものに対して抵抗することが正しい倫理観だとインプットされてきた世代なんですよね．でもこれからはこの考え方だけでは通じなくなるのは明白で，だからこそ技術や政治経済，安全保障までを俯瞰して考えることができるような技量が必要になるのではないでしょうか？

日時：2020年2月27日
場所：東京大学

栗原　聡（正会員） satoshi@keio.jp
慶應義塾大学理工学部教授／電気通信大学人工知能最先端研究センター特任教授．慶應義塾大学大学院卒業，NTT研究所，大阪大学，電気通信大学を経て現職．博士（工学）．群知能・汎用AI研究などに従事．近著は『AI兵器と未来社会 キラーロボットの正体（朝日新書）』．人工知能学会倫理委員会アドバイザー．

鳥海不二夫（正会員） tori@sys.t.u-tokyo.ac.jp
東京大学大学院工学系研究科准教授．計算社会科学，人工知能技術の社会応用などの研究に従事．情報法制研究所理事．人工知能学会，電子情報通信学会，日本社会情報学会，AAAI各会員．

平　和博 taira_k@obirin.ac.jp
ジャーナリスト，桜美林大学教授（リベラルアーツ学群メディア（ジャーナリズム）専攻）．早稲田大学卒業後，朝日新聞社入社．社会部，シリコンバレー駐在，科学グループデスク，編集委員，IT専門記者などを担当．2019年から現職．

須川賢洋（正会員） masahiro@jura.niigata-u.ac.jp
新潟大学法学部助教．修士（法学）．専門：サイバー法．コンピュータ犯罪，ディジタル知的財産，情報セキュリティ制度など先端技術と法律の関係を中心に研究．本会「電子化知的財産と社会基盤（EIP）研究会」幹事．

長倉克枝 katsue.nagakura@gmail.com
東京大学未来ビジョン研究センター客員研究員．

江間有沙 ema@ifi.u-tokyo.ac.jp
東京大学未来ビジョン研究センター特任講師．科学技術社会論．国立研究開発法人理化学研究所革新知能統合研究センター 客員研究員．人工知能学会倫理委員会副委員長．

小特集

さようなら，意味のない暗号化 ZIP 添付メール

編集にあたって

―儀式セキュリティ PPAP：日本のセキュリティ・ルネサンスに向けて―

崎村夏彦 | NAT コンサルティング

見世物小屋セキュリティ

セキュリティ・シアターという言葉がある．筆者は見世物小屋セキュリティと呼んでいるものだ．米国の著名なセキュリティ研究者である Bruce Schneier によって 2003 年頃に使われ始めた単語で，その意味するところは「セキュリティが向上したというお茶の間の安心感のために，実質的なセキュリティ向上には寄与しない対策に投資する行為」のことを意味する．

アメリカで作られた単語であるから，アメリカでもこうした意味の疑わしい対策はある．よく引き合いに出されるのは，空港におけるむき出しの銃を抱えた武装州兵のパトロールである．事情をよく知らない一般消費者からすれば，彼らはテロリストから自分たちを守ってくれていると思うのであろうが，実は州兵の銃には銃弾が装填されていないので，テロリストの来襲には対応できない．まさに，「安心」対策であって「安全」対策にはなっていない例と言えよう．

こうしたセキュリティ・シアターでとられる対策の大きな特徴に，芝居の脚本で出てきそうな脅威を扱うという点がある．芝居で扱う脅威は，現実にそれが大きな影響を持つかどうかよりも感情に訴えることを旨とする．たとえば，テロリストが靴底に爆弾を隠して持ち込んで，自分の乗る飛行機が爆破されるなどだ．確かにその可能性はあるかもしれない．しかし，そこだけ塞いでも，他の道を塞がなければ，単に迂回されるだけなので意味がない．セキュリティ対策は包括的に行われなければならず，あまりに狭い範囲の対策で安心するのは，誤った安心感というべきものであろう．そして，このような誤った安心感を得るための対策は有害である．

有害である理由はいくつかある．

1. 安心感を得たために，本来するべき対策をしなくなる．
2. 安心感を得るために不必要な費用をかけ，本来の対策にまわす費用が少なくなる．

などがその代表例だ．

一歩進んだ儀式セキュリティ

しかし，靴底爆弾のチェックというのは，一応科学的な根拠があることはある．これに対して，怪しげな宗教の壺やら儀式などには科学的根拠はない．さらに，最近では「新型コロナウイルスを消毒する」として，信者の口に塩水でスプレーを吹きかける儀式をして集団感染を起こす教団まである始末である．こうした科学的根拠のない心の平安のための対策のことを，セキュリティ・シアターを一歩進めて，筆者は儀式セキュリティと呼んでいる．そして，日本にはこうした儀式セキュリティが多い．こうした儀式セキュリティの代表例が，昨今，情報漏えい対策として日本でのみよく見られるようになった「PPAP」である．

PPAP については，第 1 章以降で詳しく触れるが，ざっくりいうと，パスワード付き暗号化ファイルを作って添付ファイルとしてメールで送り，同じメールアドレスに今度はパスワードを送るという対策である．途中の経路の情報漏えい対策や誤送信防止対策として行われるようであるが，元のメールを受け取れる人ならば，次のパスワードも受け取れるので意味はない．つまり，科学的根拠はない．それどころか，受け取り手は，メールゲートウェイでのウイルスチェックなどができなくなるところなど，上記の新型コロナウイルス拡散儀式的ですらある．

儀式セキュリティと日本人

さて，この PPAP であるが，海外ではほとんど見ることができない，印章（ハンコ）と並ぶ日本に特徴的な慣行である．紙＋印鑑というのも，原本性と本人同意の確認を目的としているのだからセキュリティ対策と言えるだろうが，PPAP 同様科学的根拠はない．

はじめからなかったわけではない．かつては，目の粗い紙にインクや墨など連続的に濃度が変わり，書いたあとは酸化が進み経時的変化を反映できる手段で内容を染み込ませて記録し，毎回ランダム性が付与されるために複製が難しいとされる手掘りのハンコで印章を押すことにより改ざん検知と作成者認証をしていたのだから科学的なセキュリティ対策になっていた．

しかし，現代で紙とハンコを要求する人たちは，このことをきちんと考えているだろうか？　外見だけを儀式としてなぞっているのではないだろうか？現状は，表面にコーティングが施されたコート紙に，均質かつ安定的なトナーで表面に着色，印影から 3D プリンタで安価に複製できる印章を使って印影をつけているわけだが，内容は表面に均質に付着しているだけなので修正は可能だし，寸分たがわぬ印章をつけることも容易である．紙＋印章というセキュリティ手段は完全に危殆化してしまっているのだ．科学的根拠はない．あるのは儀式としての意味だけである．そして，これを非難するものは異端として糾弾される．

日本における
セキュリティ・ルネサンス

実はパスワード付きファイル送付も，紙に文を記載して朱肉を付けるという行為も，正しく行えば効果はある．問題は，どのような脅威に対応しようとしているかを考えるのをやめてしまい，儀式として行い続ける行為である．

本特集では，第 1 章で PPAP が生まれた経緯，第 2 章，第 3 章でそれぞれの立場からの PPAP の評価と大対策，第 4 章で「社会から PPAP をなくすには？」と題し座談会を行い，より良い方策を検討している．

本特集が，科学的根拠のない儀式を盲信する中世的セキュリティ感から日本を脱却させる「セキュリティ・ルネサンス」成立の一助となれば幸いである．

（2020 年 4 月 15 日）

［さようなら，意味のない暗号化 ZIP 添付メール］

1 PPAP とはなにか
―その発展の黒歴史―

大泰司章 | PPAP 総研

PPAP とはなにか

企業間の取引においては，見積書，発注書，発注請書，請求書，契約書等の取引文書をはじめとして，技術文書やイベントの案内等，さまざまな文書が，メールにファイル添付という形で共有されている．その際，これは日本特有の現象だと思われるが，パスワードつき ZIP ファイルが添付され，そのパスワードが 2 通目のメールで届く，という実に奇妙なことが行われている．1 通目の添付ファイルを奪えるようであれば，2 通目も奪うことができるはずで，セキュリティ的な意味がないように思われる．それにもかかわらず，受信側は毎回復号化しなければならず，負荷は非常に高い．

このようなメールの送り方を PPAP と名付けて，やめようという活動をしている．

【P】assword つき ZIP ファイルを送ります
【P】assword を送ります
【A】n 号化
【P】rotocol

話は 2016 年にさかのぼる．当時，S/MIME（エスマイム，Secure/Multipurpose Internet Mail Extensions）用の電子証明書を販売していた関係でパネルを制作することになった．そのときに作ったコピーが「まだ ZIP ファイル＋パスワードで消耗してるの?」というものであった．いまひとつだな，もう少しインパクトがほしいなと思っていたところ，ちょうど PPAP（もちろん Pen-Pineapple-Apple-Pen のほうである）が流行っており，「PPAP って何かのプロトコルみたいだよね」と誰かが Facebook で言ったのを見て，思いついたものである．

Internet Week 2016 では「組織間の安全なファイル送受信を考える～暗号化 ZIP は何のため～」というテーマでパネルをした．このころは，PPAP に反対すると，PPAP を自動で行うソリューションのベンダが放っておかないぞと警告されていたが，実際に彼らと話をしてみると，「PPAP 自体はやめたいがユーザがいるのでやめられない．PPAP の代わりのオンラインストレージの機能はすでに持っているし，設定で簡単に変更可能」と言われて拍子抜けした．

2017 年 3 月には「くたばれ PPAP !」という Facebook グループを作った．今ではメンバが 1,000 人近いグループになっている．PPAP の事例から情報セキュリティまで多様な話題が飛び交っており，有益な情報交換ができたと思っている．

2018 年には「働き方改革」がさかんに言われるようになった．そこで，PPAP を非効率な取引慣行の象徴と捉え，紙やハンコの廃止（電子契約元年）に加えて，PPAP をやめることで，組織や働き方を改革しようという打ち出し方をしている．

PPAP の歴史

2000 年前後から，それまでの郵便や FAX に代わって，メールに取引文書等のファイルを添付して送ることが増えたように思う．送受信の手間も少なく，スピードも速く，ディジタルデータのまま再利用できることもあり，取引文書のやりとりは画期的に効率化されたが，赤い印影つきの紙にこだわる経理等管理部門が壁となって全面的に電子化とまではいかなかった．電子ファイルをカラー印刷することで赤い印影をつけたり，FAX を併

用したりした．不思議なことに，FAX は経理担当によっては原本扱いをしてもらえるのだ．

当初は Word や Excel，PDF ファイルがそのまま添付されていたが，徐々に添付ファイルのみが ZIP 暗号化されるようになってきた．もちろん，PGP（Pretty Good Privacy）や S/MIME によって本文ごとの暗号化は可能であったが，一般のユーザには導入が難しかった．

exe ファイルを送って受信側で自動解凍するというものもあった．exe ファイルは受信側で受け取れないことがあるので，拡張子をいったん ex_ にして送信し，受信者側で exe に戻すということも行われていた．

ZIP ファイルのパスワードは，「御社の名前です」「今日の日付です」というものだったり，そのつど生成する複雑なものだったりしたが，やがて，2 通目に自動で送られてくるようになる．これが 2010 年頃からどんどん増えたという印象を持っていて，2010 年代の中頃には，大企業の多くが PPAP になってしまった．

一方で，ここ数年，ファイル共有はより便利な方法にシフトしつつあるのも事実である．

まず，オンラインストレージの使用頻度が上がっている．昔から無料で手軽に使える宅ふぁいる便がよく使われていたが，最近は OneDrive，Google Drive，Dropbox，Box 等での共有も普通になってきた．それ以外にも，グループウェア，特にサイボウズ Live は企業や団体間の情報共有でよく使われていた．

技術部門，特に IT 関係では，すでにメールではなく Slack 等のメッセンジャーが利用されているし，また，昨今テレワーク対応ということで Zoom，Webex，Skype といったオンラインミーティングのツールでもファイル共有がされている．

ここ数年注目すべき動向としては電子契約の爆発的拡大である．契約や受発注の業務プロセスの中で，自然とファイルを送受信することになるので，これも PPAP メールを減らす要因になるだろう．

なお，以上は主に企業間取引の販売部門での状況であり，他の分野では様相が違っているかもしれない．特定の分野では Rights Management や S/MIME，PGP も使われている．

PPAP の分類

すべてのファイルが対象か，パスワードを別経路で送っているかを軸にすると，表 -1 のように4つに分類できる．

- タイプ A:すべての添付ファイルを暗号化し，パスワードを同じ経路で送る．送信者は情報の機密性を評価する必要がなく，一律に暗号化される．添付ファイルは暗号化することが社内規定で決まっていることが多い．送信者は，手動の場合は暗号化の負荷が高いため，PPAP 自動化ソリューションが使われることになりやすい．狭義の PPAP．
- タイプ B：すべての添付ファイルを暗号化し，パスワードを別の経路で共有するもの．
  タイプ A に比べて，送信者側も受信者側も負荷がかかる．多くの案件を抱えている人にとっては非常にきつい．
- タイプ C：暗号化が必要なファイルのみを暗号化し，パスワードを同じ経路で送るもの．
  送信者がせっかく暗号化が必要だと自分で判断し，暗号化をしているにもかかわらず，パスワードを同じ経路を送ってしまうのは惜しい．
- タイプ D：暗号化が必要なファイルのみを暗号化し，パスワードを別の経路で共有するもの．これが本来は望ましい形．送信者側はファイルの暗号化の必要性を判断しなければならないし，手動で暗号化することが多いため，送信側の負荷は高いが，受信側は復号するファイルの数が減る．

狭義の PPAP（タイプ A）なのか，広義の PPAP（タイプ A，B，C，D）なのか区別をしないと，議論が発散しがちである．ここでは狭義の PPAP に絞って述べたい．

■表 -1　PPAP の分類

		暗号化する対象となるファイル	
		すべて	暗号化が必要なもののみ
パスワードの送信経路	同	タイプ A	タイプ C
	別	タイプ B	タイプ D

なぜ PPAP を使うのか

受信側からすると負荷が高い PPAP であるが，なぜ使われるのであろうか？

「PPAP は，ISMS やプライバシーマークを取得するタイミングで社内に導入された．ISMS やプライバシーマークが悪いのだ」と言われることがある．それは本当だろうか？

メール誤送信防止サービスの一部として市場では取引されていることから，メール誤送信防止市場の規模の推移から広まった時期を推定することができる可能性がある．市場規模については図 -1 のとおり ITR 社の調査を見つけることができた．2016 年度以降のものしか公表されていなかったが，2015 年度以前のデータがあれば分かることがあるかもしれない．

一方，ISMS やプライバシーマークで，PPAP を実際に推奨する審査員やコンサルタントを探したが，残念ながら今のところ見つかっていない．どうも，ISMS，プライバシーマーク犯人説は都市伝説の様相を見せている．

それでは，ISMS やプライバシーマークでメールの暗号化がどのように取り扱われているか見ていこう．

ISMS でのメールの添付ファイル暗号化の取り扱い

ISMS とは

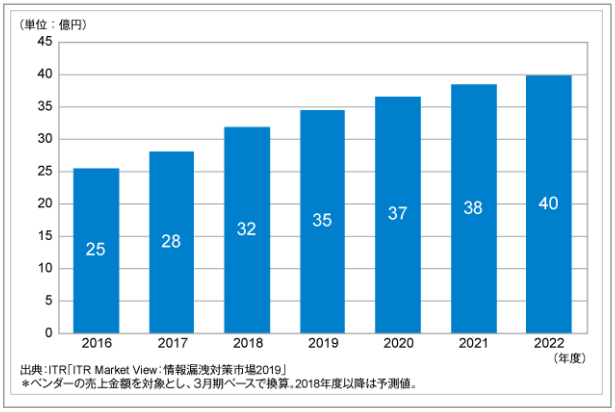
ISMS とは，Information Security Management System（情報セキュリティマネジメントシステム）の略で，情報の CIA（「機密性（Confidentiality）」，「完全性（Integrity）」，「可用性（Availability）」）を保護するための体系的な仕組みである．

ISMS を構築するにあたって，必要となるのが ISO/IEC 27001（JIS Q 27001）という ISMS の国際規格である．この規格には，ISMS をどのように構築，実施，維持，改善すべきなのかが記載されている．特に管理策については，ISO/IEC 27002 というガイドライン規格があり，管理策を導入する際の参考になる．

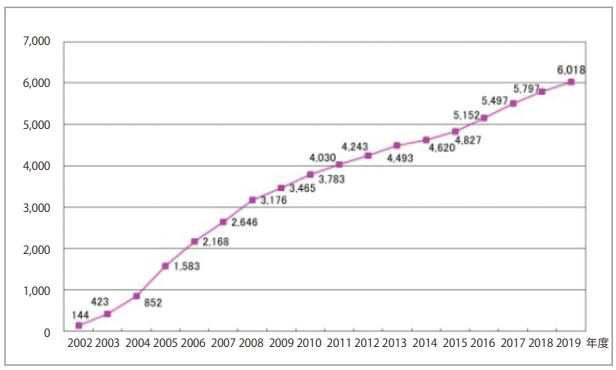
「ISMS 認証」とは，第三者である ISMS 認証機関が，組織の構築した ISMS が ISO/IEC 27001 に基づいて適切に運用管理されているかを，利害関係のない公平な立場から審査し証明することである．したがって，「ISMS 認証」によって，組織は，ISO/IEC 27001 という国際規格に沿って，情報セキュリティを画するための仕組みを持ち，その仕組みを維持し継続的に改善していることを，顧客や取引先に対して客観的に示すことができる．この「ISMS 認証」を取得するには，ISMS 認証機関に申請し，審査を受ける必要がある．

ISMS 認証の取得数は図 -2 のとおり，年々増え続けており，昨年度 6,000 件を超えている．PPAP が広まったのが 2010 年前後だとすると，増勢が落ち着いている時期にあたるようにも見える．

JIS Q 27000:2014（情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項）においては，「電子的メッセージ通信に含まれた情報は適



■図 -1　メール誤送信防止市場規模推移および予測（2016 ～ 2022 年度予測）[1]



■図 -2　ISMS 認証登録数の推移（数値は各年度末．2019 年度は 11 月 11 日現在）[2]

切に保護しなければならない」とあるだけで，当たり前のことながら抽象的な記述になっている．

一方，JIS Q 27002:2014（情報技術―セキュリティ技術―情報セキュリティ管理策の実践のための規範）においても，メールの添付ファイルの暗号化というレベルの記述はない．

情報資産の他社への転送方法は，自社でリスク分析をした上で決めるべきことで，それが維持できており，できれば改善することが望ましいということだ．

関係者周辺からも，PPAP 蔓延に関する有益な情報は得られなかった．

プライバシーマークでのメールの添付ファイル暗号化の取り扱い

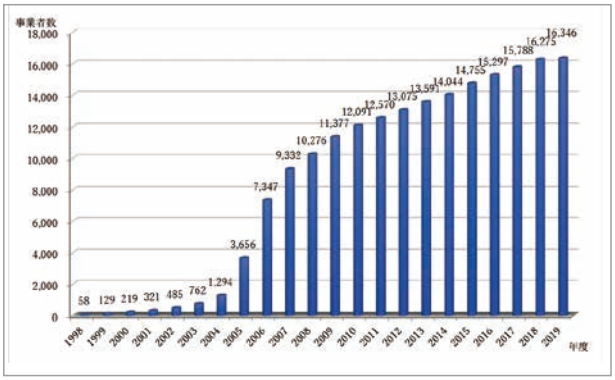
プライバシーマーク制度は，事業者の個人情報を取り扱う仕組みとその運用が適切であるかを評価し，その証として事業活動においてプライバシーマークの使用を認める制度である．

プライバシーマーク制度は，日本産業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」をベースとした審査基準による審査を経て，事業者の個人情報の取扱いが適切であるかを評価している．JIS Q 15001 は，個人情報保護法等，法令への遵守も包含している．そのため，事業者にとっては法律への適合性はもちろんのこと，自主的により高い保護レベルの個人情報の管理体制を確立し運用していることを，取引先や消費者に示すことができる制度として活用されている．

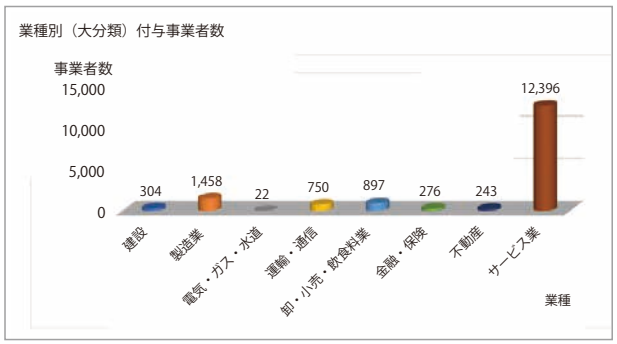
図 -3 がプライバシーマークの付与事業者の推移である．個人情報保護法が施行されたのが 2005 年度であり，やはりその前後で急増していることが分かる．その後の伸びと PPAP との関係はあるのだろうか．

図 -4 は，業種別（大分類）の付与事業者数である．サービス業が圧倒的に多いので，表 -2 にサービス業の内訳を掲載した．PPAP 企業といえば，官公庁，金融機関，製造業等伝統的大企業というのが直観的なイメージだが，実際にプライバシーマークを取得している企業の業種分布とは一致しそうにない．

「JIS Q 15001:2006 をベースにした個人情報保護マネジメントシステム実施のためのガイドライン―第 2 版―」によると，「盗聴される可能性のあるネットワーク（たとえばインターネットや無線 LAN 等）で個人情報を送信する際に，個人情報の暗号化又はパスワードロック等の秘匿化の措置を講じていること」とある．



■図 -3　付与事業者の推移（1998 年度～ 2019 年 9 月 30 日時点）[3)]



■図 -4　業種別（大分類）付与事業者数 [3)]

■表 -2
業種別（中分類）付与事業者数（抜粋）[3)]

洗濯・利用・浴場業	12
駐車場業	12
その他の生活関連サービス業	142
旅館，その他の宿泊所	5
娯楽業	21
自転車整備業	6
機械・家具等修理業	30
物品賃貸業	47
映画・ビデオ制作業	60
放送業	54
情報サービス・調査業	6,667
広告業	548
専門サービス業	1,007
協同組合	18
その他の事業サービス業	3,298
廃棄物処理業	83
医療業	39
保健衛生	170
社会保険，社会福祉	72
教育	46
学術研究機関	11
政治・経済・文化団体	48

はたしてPPAPが「秘匿化の措置」といえるかどうかだろうか.

一方で，Webサイトに掲載されているためか，添付ファイル暗号化の根拠としてJISAの審査基準[4]が引用されることもあるようである.

【書類審査】において，「(3)【第23条】個人情報を含む添付ファイルを取扱う際に，セキュリティ対策（データの暗号化，パスワード設定など）の措置を講じることを新たに追加した」と書かれている.

PPAPは，確かに「データの暗号化，パスワード設定」ではあるが，「セキュリティ対策」なのだろうか.

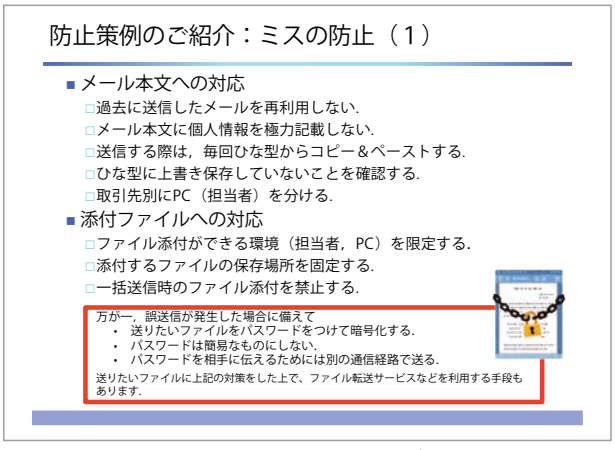
なお，JIPDECには，「お役立ちツール，社内教育用参考資料，基本編：個人情報の取扱いに関する事故を起こさないために」というも資料があったので，図-5に示す.

「パスワードを相手に伝えるためには別の通信経路で送る」と書かれている.

IPA「対策のしおり」

さらに，少々古いものであり，直接ISMSやプライバシーマークとは関係がないが，「IPA対策のしおり シリーズ(7) 電子メール利用時の危険対策のしおり(2012年6月8日第4版)」という資料があった. 図-6に示す.

「復号のためのパスワード等は，別の通信手段を利用して相手に伝えることが重要ですが，」と書かれている.



■図-5　防止策例の紹介：ミスの防止（1）[5]

なぜ都市伝説が生まれたのか

以上見てきたように，すべての添付ファイルを一律にZIP暗号化し，同じ経路の2通目でパスワードを送るような事態は，制度や基準，ガイドライン作成の場では，想定されていなかったようだ. 直接の要求事項ではないとはいえ，パスワードは「別の通信経路で送る」と明示的に書かれている文書もある.

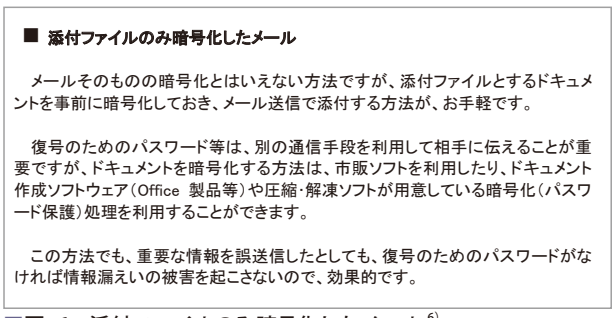
PPAPを利用している企業（以下，PPAP企業）は，ISMSもプライバシーマークも審査に通りそうにない. それにもかかわらず，通るためにPPAPを始めた，通るためにはPPAPソリューションが必要，と言う人がいるのは不思議なことだ.

審査に割ける限られた時間の中で，おそらくメールの添付ファイルの暗号化の方法にまでコンサルも審査員も考えが及んでいないのであろう.

あるいは，取引先にのみ負荷をかける，意味のない「送信側自己中心的セキュリティ」ということに気付いていて，その後ろめたさから，認証取得のためという言い訳をしているのだろうか.

このように，情報セキュリティや個人情報にかかわりたくないし，まして情報の秘匿性の判断などしたくない送信側ユーザ，形式を整えて認証が取れればよい送信側管理部門，ユーザの要望に応えざるを得ないメールソリューションベンダ，特にメールについては関心がない審査関係者，そして発注元企業の発信するメールに対してものが言えない受信者，これらの関係者が見事にバランスしている状態が生じている可能性がある.

こうした謎を解くため，今後ISMSとプライバシーマー


■ 添付ファイルのみ暗号化したメール

メールそのものの暗号化とはいえない方法ですが、添付ファイルとするドキュメントを事前に暗号化しておき、メール送信で添付する方法が、お手軽です。

復号のためのパスワード等は、別の通信手段を利用して相手に伝えることが重要ですが、ドキュメントを暗号化する方法は、市販ソフトを利用したり、ドキュメント作成ソフトウェア（Office 製品等）や圧縮・解凍ソフトが用意している暗号化（パスワード保護）処理を利用することができます。

この方法でも、重要な情報を誤送信したとしても、復号のためのパスワードがなければ情報漏えいの被害を起こさないので、効果的です。

■図-6　添付ファイルのみ暗号化したメール[6]

クのコンサルとして現場に入ってみようと思う．しかるべき時期に続報ができれば幸いである．

今後の新たな歴史の創造に向けて

PPAP 企業は，少なくとも，意味のない自社のルールにこだわり，取引先に負担を強いても何とも思わないカルチャーを持つ企業だということがいえる．PPAP 企業の現場では，実はやめたいが管理部門に到底言えないという声もよく聞く．このような企業は効率的な取引を行えない企業だというシグナルとして PPAP を活用することができるだろう．

そこで，どの企業が PPAP 企業なのかという情報を集めて公開することには意味があると考えられる．また，PPAP に限らず，さらに，以下のようなデータを集めることにより，取引の効率性をスコアリングできるかもしれない．

●取引文書に紙とハンコを要求するか
● FAX を使っているか
●対応している電子契約，EDI（Electronic Data Interchange）の種別
●業者登録，取引口座開設時の手続き
●決済方法
● SDGs（Sustainable Development Goals），CSR（Corporate Social Responsibility）に関する取引先への要求事項
●情報セキュリティに関する取引先への要求事項
●個人情報保護に関する取引先への要求事項

こうしたスコアができれば，取引の効率性を評価されることなく，取引先にのみ負担を強いていた調達方法が変わるきっかけになるだろう．優秀な取引先を確保するためには自ら変わらなければならないということだ．

あわせて，こうしたスコアが投資家からの評価に影響することになれば，PPAP をはじめとする非効率な取引慣行は大きく変わるだろう．

今や，取引文書のやりとりだけでなく，企業の枠を超えてコラボレーションを行うことが必須となっている．その際に，自社の営業秘密の秘匿性を評価し，先方の会社と共有すべき情報と共有すべきでない情報の選別ができない従業員は，そもそもコラボレーションに参加すべきでないし，しても成果は上げられないであろう．PPAP に頼った情報共有をするような従業員は使えないということだ．

もちろん，情報の選別ができない従業員がいることは事実である．そのような従業員は，そもそも対外的な情報のやりとりが発生する業務をやらせてはいけない．それこそ PPAP の強制によるコントロールをするのではなく，社外へのすべての情報発信を禁止すべきだ．

いずれにせよ，メールに限らず社外への情報発信の方法を全従業員一律に規制するやり方はすでに限界に来ている．もっとも，それらの教育や基準作成，評価を個別企業が行うことは負担が大きい．営業秘密の取り扱いや社外との共有のスキルを評価できる資格が必要になってくるだろう．

取引先への迷惑も顧みず，全社員が全添付ファイルを自動的に暗号化する PPAP は，各個人が得意なやり方に応じて，場所や時間に縛られない働き方をする「真の働き方改革」とはまったく相いれない．遅かれ早かれ PPAP はなくなるに違いない．

参考文献

1) ITR：メール誤送信防止市場規模推移および予測（2016 ～ 2022 年度予測），https://www.itr.co.jp/company/press/190207PR.html
2) ISMS-AC：ISMS 認証登録数の推移（数値は各年度末．2019 年度は 11 月 11 日現在），https://isms.jp/topics/news/20191112.html
3) JIPDEC：プライバシーマーク付与事業者情報（2019 年 9 月 30 日時点），https://privacymark.jp/certification_info/jdi6lq00000017af-att/pmark_data_20190930.pdf
4) JISA におけるプライバシーマーク審査項目の一部改訂について，https://www.jisa.or.jp/service/privacy/tabid/831/Default.aspx?itemid=31
5) JIPDEC：お役立ちツール 社内教育用参考資料 基本編：個人情報の取扱いに関する事故を起こさないために，https://privacymark.jp/system/reference/pdf/tools_accidents_1_note.pdf
6) IPA：対策のしおり シリーズ（7）電子メール利用時の危険対策のしおり（2012 年 6 月 8 日第 4 版），https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf

（2020 年 3 月 31 日受付）

■**大泰司章** otaishi@gmail.com

三菱電機，日本電子計算，JIPDEC を経て，PPAP 総研設立．電子契約，電子署名，メールや Web のなりすまし対策を普及．PPAP やハンコ等の非効率な取引慣行を変えて，真の働き方改革を目指す IT コンサルとして活動中．

［さようなら，意味のない暗号化 ZIP 添付メール］

2 PPAP のセキュリティ意義

楠　正憲 | 国際大学 Glocom

なぜか日本でだけ定着している PPAP

俗にいう PPAP とは，パスワード付き ZIP ファイルと パスワードを，電子メールで送付する方式を指す．組織によっては添付ファイルを自動的に暗号化 ZIP に変換する仕組みがメールシステムに組み込まれ，組織外に添付ファイル付きのメールを送信すると，自動的に暗号化 ZIP ファイルに格納し，ZIP ファイルとパスワードに分けて送信する設定となっている．こうした製品はメール誤送信対策ソフトと総称され，ヒューマンエラーによるメールの誤送信に対して一定の効果があると主張しているベンダもある．こうした誤送信対策ソフトは日本国内に限って，官公庁や金融機関をはじめとした大企業で広く導入されている．

例：https://www.lrm.jp/mailzipper/attachment-encryption/

PPAP の何が問題なのか

PPAP の基本的な問題は，暗号化 ZIP ファイルの送信・受信者ともに負担が重いにもかかわらず，通信の傍受に対して何ら防御の意味を持たないことである．暗号化する対象のデータと，そのデータを暗号化・復号化する鍵とを同じチャネルでやりとりしてしまうと，暗号化 ZIP ファイルを窃取できる攻撃者は，その復号化に用いる鍵を窃取することも可能となってしまうので，通信経路上での傍受からデータを保護するための暗号化としては何ら意味がない．

近年では PC だけでなくスマートフォンやタブレットでメールを送受信する機会が増えている．iOS や Android では添付ファイルをプレビュー表示する機能を具備しているが，出荷時の状態では簡単に ZIP ファイルを開けない場合があるほか，仮に開ける場合も暗号化 ZIP を展開するための操作は煩雑で，検索などの機能が適切に機能しない．

また，これらの障壁を乗り越えて暗号化 ZIP を展開できたとしても，日本語ファイル名が文字化けすることが多い．文字化けは PKWARE 社が設計した ZIP ファイルフォーマットの規格が，ファイル名の文字コードを規定していないことに起因する．一般に Windows の ZIP 暗号化ソフトは ZIP ファイルフォーマットの文字コードとして，non-Unicode アプリケーション向けの設定文字コード（日本語版であれば CP932 いわゆるシフト JIS）でエンコードするのに対して，iOS や Android アプリケーションは UTF-8 を前提にデコードする場合が多く，文字化けが発生してしまう．

PPAP がセキュリティ的に意味がなく，操作が煩雑なだけではない．近年のメールシステムでは，添付ファイルに対して詳細な解析を行っている．ウイルス対策ソフトによるシグニチャ型の既知のマルウェア検査に加えて，サンドボックス装置の仮想マシン上で添付ファイルを実際に開き，不審な挙動を行わないかどうかの確認などが行われる．暗号化 ZIP で送られてきた場合，同時に送信されたパスワードを使って復号して検査する機能を具備していない限りは，暗号化 ZIP 内のファイルについて検査が行われない．技術的には暗号化 ZIP と対応するパスワード通知メールとを解析して，ZIP ファイルを復号することも難しくはないはずだが，送信者が受信環境として前提にできるほど普及してはいない．

このように暗号化 ZIP ファイルとパスワードを同時に同じチャネルで送ることは，送受信者双方のユーザビリティを悪化させる上に，セキュリティ的には機密保護

の観点から何ら意味がなく，シグニチャ型のマルウェア対策やサンドボックスによる検疫を迂回してしまうことから，受信者に大きなリスクを負わせてしまうことになる．

最低限の機密性を確保できる暗号化 ZIP の運用とは

では，どのような電子メールの暗号化であれば，セキュリティを確保できるだろうか．実は暗号化 ZIP ファイルでも機密性を保つ方法がある．具体的には暗号化 ZIP ファイル本体のみを電子メールで送って，ZIP ファイルの暗号化・復号化に用いるパスワードは別経路で共有する方法だ．たとえば対面でのパスワード生成規則の事前共有，電話や郵送，SMS，ソーシャルネットワーク等の他経路を用いてパスワードを受け渡す方法が考えられる．相手の電話番号など他の連絡方法を知らず，電子メールによる連絡しかできない場合であっても，パスワードを平文でやりとりするのではなく，両者が共有している知識に基づく間接的な表現方法でパスワードを表現することによって，それなりに機密性を確保できると考えられる．

この方法のメリットは仮に暗号化 ZIP を間違った相手に誤送信してしまったとしても，誤送信先との間でパスワードを共有していなければ，受信者が容易には解読できないことだ．暗号化 ZIP ファイルとパスワードとを別チャネルでやりとりする場合，両方を誤って同じ相手に送ってしまうリスクは小さい．このことが暗号化 ZIP ファイルを利用することで誤送信対策になるという認識に繋がり，ISMS や P マークの審査において「個人情報を含む添付ファイルを取り扱う際に，セキュリティ対策（データの暗号化，パスワード設定など）の措置を講じること」（情報サービス産業協会 2010 年）といった規定が設けられるようになったと考えられる．
https://www.jisa.or.jp/service/privacy/tabid/831/Default.aspx?itemid=31

こうした規定が各組織のセキュリティポリシーに追加されて，かかる規定を確実に遵守させる方法として，外部アドレス宛の電子メールについて，添付ファイルを自動的に暗号化するソリューションが普及したと考えられる．しかしながら誤送信対策として暗号化 ZIP が有効なのは，誤送信先が復号のためのパスワードを知らないことが条件となる．システムによって自動的に暗号化 ZIP ファイルとパスワードを送付してしまっては，この条件を満たすことができない．こうしたシステムを使って，暗号化 ZIP とパスワードを同一チャネルで送ってしまっては，メールの誤送信対策としてはまったく機能しない．こうした仕組みをメールの誤送信対策として採用している組織は，セキュリティポリシーが形骸化してしまって，適切なリスク管理を行えていないことが推定される．

暗号化 ZIP 以外の安全なデータの受け渡し

これまで電子メールの暗号化にあたっては，暗号化 ZIP よりも優れた方法が考案されてきた．公開鍵暗号方式によって共通鍵を交換する方法として，古くは 1991 年，Phillip Zimmermann が PGP (Pretty Good Privacy) を発表している．この方式は 1996 年 RFC 1991 PGP Message Exchange Formats として標準化されて，後に RFC 2440 を経て RFC 4880 と更新されている．PGP では鍵管理を利用者自身が行う必要があり，暗号や PGP について，ある程度の専門知識が必要となる．PGP はオープンソースソフトウェアの開発や，ソフトウェアの脆弱性報告などに使われている．

利用者による鍵管理を必要としない方式として，認証局が証明書を管理する PKI を利用する S/MIME が RSA Data Security によって開発された．S/MIME は Microsoft Outlook をはじめとした多くの電子メールクライアントに採用されて，一時は暗号化メールの本命と目されたものの，署名・暗号化に用いる電子証明書の価格が高止まりしたため普及には至らなかった．その後 Hotmail や Gmail などの Web メールの流行，ス

マートフォンの普及でスマホ用メールアプリで S/MIME 対応が進まなかったことから，普及のタイミングを逸してしまった．

暗号化メールは通信路の暗号化には有効だが，正規の受信者が復号したデータを第三者に転送することを防ぐことはできない．このため 2000 年代に入ってからは，電子メール自体を暗号化するアプローチから，メールを転送されても正規の受信者しか開けないように，DRM 技術を用いて暗号化に使う鍵管理を集約する製品が登場した．たとえばマイクロソフトは Office IRM (Information Rights Management) を Microsoft Office 2003 から導入した．Office IRM はディレクトリサービスや文書管理サーバの権限管理と連動して，メールの転送や印刷も含めて制限できる．しかしながら他社製品との相互運用性に欠け，組織間で運用するには多くの課題があった．

添付ファイルからクラウド上でのファイル共有へ

2010 年代に入り，電子メールに MIME でファイルを添付するよりも，クラウド上でファイルを共有して適切な権限管理を行うことが，適切に文書管理する方法として定着した．Box などのストレージサービスが組織間のデータ共有方法として広く使われ，Google が Web 上で複数人で単一のファイルを開いて同時に編集できる機能をリリースして Microsoft も追随した．ID フェデレーションとクラウドサービスの普及によって組織を超えた ID 管理と連動した権限管理が当たり前となって，メールにファイルを添付するのではなく，組織を超えてクラウド上でファイルを共有して，必要な者にアクセス権限を付与する方法が普及した．

このように複数組織がクラウド上で単一のリソースにアクセスする方法は，電子メールの添付ファイルとして暗号化したファイルをやりとりする方法と比べ機密を保持する上でメリットが大きい．いちどデータを相手に送ったとしても，いつでも事後的にアクセス権限を剥奪できる．データ自体を送った場合は復号化した後のデータの印刷や転送を禁止できないが，クラウドサービス上のデータにブラウザからアクセスできる権限を付与した後も，印刷や転送の権限は個別に制御できる．

電子メールの添付ファイルからクラウドサービスへの移行にはほかにも理由がある．Windows では添付ファイルを開くアプリケーションを呼び出す際 DDE と呼ばれる仕組みが使われるが，文書ファイルに偽装してマクロや実行ファイルを実行させることを防ぐことが難しい．iOS や Android ではプログラムとデータを分離して取り扱うが，Windows は後方互換性のためにメールの添付ファイルを実行できてしまう仕組みが残されており，今でも標的型攻撃に悪用されがちだ．これを防ぐためには iOS や Android のようにファイルの閲覧とプログラムの実行とを明確に分けて，プログラムごとにアクセスできる資源を分離する必要があるが，後方互換性との両立は難しい．

もちろんクラウドを通じたリソース共有にも課題はある．各クラウドサービスの ID が厳格に管理されていることが前提で，フィッシングによる ID 詐取や，誤って攻撃者のリンクを踏んだ場合のトークン窃取などに対して対策が必要となる．多要素認証や，安全なトークン管理などを通じて，ID を厳格に保護することが重要だ．しかしながら従前の添付ファイルと比べて，データの集中管理と，資源管理の厳格な分離を実現することは容易と考えられる．

電子メールからビジネスチャットへ

クラウド時代に入って変化したのはファイルの共有方法だけではない．メッセージのやりとりも，電子メールではなくチャットが広く使われるようになった．この動きは法人よりも先に個人で起こっている．米国では 2002 年に LinkedIn，2003 年に Friendstar が登場，日本では 2004 年に Gree と mixi が登場，その後 Facebook，Twitter など高いシェアを持つ SNS が登場したことで，個人間のコミュニティがメーリングリス

トからソーシャルネットワークに移行し，SNS に組み込まれた個人間通信でのコミュニケーションが広がった．

この流れを決定的にしたのがスマートフォンの普及とともに流行した KakaoTalk, LINE, Whatsapp といったメッセンジャーアプリだ．こうしたチャットアプリは電話帳を元にソーシャルグラフを形成して，知り合い同士のコミュニケーションを容易にする．電子メールと違ってチャットアプリでは知り合いとしかメッセージのやりとりをせず，悪意ある第三者が紛らわしいメッセージを送ることが難しい．やりとりの開始にあたっては，利用者の明示的な許可が必要となる．また電子メールと異なり個別システムが縦割りで閉じていることが前提で，標準化を待たずサーバとアプリのプロトコル変更が容易となる．

これらのチャットアプリは利用者が通信相手を明示的に管理しているので，これらを鍵管理と連動させることで，容易に暗号化を実現できる．日本で広く使われている LINE や Facebook Messenger，Apple の iOS に標準で組み込まれている iMessage，ロシアが遮断を試みて失敗した Telegram などは，E2E 暗号化 (End to End Encryption) を実現しているとされる．E2E 暗号化によってサービス提供者がメッセージを傍受することが難しくなることが期待されるが，いずれもオープンな実装ではなく，鍵管理をサービス事業者に委ねていることから，安全性を外部から検証することは難しい．

消費者向け SNS に遅れて企業向け SNS が数多く登場し，ビジネスチャットへと発展した．2009 年にリリースされた Yammer は 2012 年マイクロソフトに買収され，2011 年には日本で Chatwork が，2013 年には西海岸で Slack が登場している．買収した Yammer を Office 365 の一部として提供していたマイクロソフトは 2016 年 Teams を発表してビジネスチャットとビデオ会議を統合した．

これらビジネスチャットが特徴的なのは従前の組織単位の情報システムではなく，組織をまたいだプロジェクトのメンバ間のコラボレーションを支援していることだ．電子メールやファイルサーバが企業単位で整備されて，標準プロトコルを使って組織間を結ぶ方式だったのに対して，ビジネスチャットは単一のクラウドサービスとして提供されて，組織を超えたプロジェクトのメンバに対して安全なサービスを提供する．ビジネスチャットだけでなくさまざまなクラウド上の SaaS が ID Federation と API で結合して，組織を超えてシームレスにサービスを構築できる時代がきた．

従前の電子メールがメールサーバ，メールクライアント，認証局の間で三すくみとなって安全で使い勝手の良い暗号化メールを提供できない間に，SNS やチャットアプリ，ビジネスチャットが一気通貫で ID・クラウドサービス・各 OS 向けアプリを提供して世界で広く使われるようになった．取り残された電子メールの世界で，使い勝手の悪い暗号化 ZIP が日本では細々と使われ続けてきた．

取り残される日本の「セキュア」な組織

残念ながら PPAP が残っているような会社では，こうしたクラウドサービスを使うことが難しい場合が多い．たとえば情報漏洩対策として Office 365 や G Suite, Slack などはフィルタリングされ，ブラウザ仮想化によって複雑な Web アプリはまともに動かず，情報を端末側に残さないためにシンクライアントを使っていて，常に画面の動きがモッサリとしていたりする．

そういった組織でも外部とのやりとりはあるので，シャドー IT として私用スマホで Gmail や LINE, Dropbox が業務に使われる．昨今の新型コロナ対策のような大規模のテレワークは想定されておらず，VPN の帯域が逼迫して，整備したつもりのテレビ会議システムが適切に機能しない．迷惑メール対策は厳重に行われ，サンドボックス装置も入っているが，他社から暗号化 ZIP が送られてきても復号できず十分に機能しない．暗号化 ZIP にファイル名を文書ファイルのように偽装した実行ファイルを仕込むと簡単に引っかかっ

てしまう．

このようにルールと仕組みがチグハグなまま何を守っているか分からなくなってしまったのは日本固有のITガバナンスも影響していると考えられる．日本における情報セキュリティは2001年のCodeRed・Nimdaウイルス流行，2003年のBlasterウイルス流行に続いて，2005年に個人情報保護法が完全施行されたため，当初は制度対応として進められてきた．組織規定の整備は専門家ではないローテーション人事の中で継ぎ接ぎに行われ，セキュリティ・ソリューションはインシデントのたびにベンダ提案として再発防止策として積み重なり，リプレースの際にも外すことのリスクを判断できず，どれも廃止できないために，多数のソリューションが複雑に絡み合う．その中で見当違いのメール誤送信対策としてのPPAPは生き残り，従前の情報漏洩対策の前提と矛盾するクラウドサービスは遮断せざるを得ない．

そういった組織であっても，社外とのコラボレーションやデータのやりとりは頻繁に発生するため，業務を回すためにシャドーITが横行し，監視が難しい暗号化ZIPの添付ファイルが飛び交う．あちこちで微妙にバージョンが異なるファイルが散在し，印刷や外部への転送を止めることができない．個人情報漏洩で社会面に載ることに怯えてConfidentialityばかりが肥大化し，IntegrityやAvailabilityを脅かす他のリスクと真剣に向かい合ってこなかった組織の末路だ．

組織を超えた共同作業と業務継続の確保へ向けて

1990年代LANとイントラネットの普及当初は，部門単位でネットワークが構築されてきた．2000年代前半にブロードバンド常時接続の普及にセキュリティ対策が追いつかず，世界規模でBlasterウイルスの爆発的感染を招いた．日本では個人情報保護法の施行とも相俟って情報漏洩対策を全社的に推進するため，部門単位ばらばらに整備されたITから，全社規模のITへと統制を働かせるように改革が進んだ．

しかしながら伝統的な組織の多くはジェネラリスト中心のローテーション人事で専門家を育てず，規程類はローテーション人事で継ぎ接ぎを重ねて，セキュリティ対策はベンダ任せでインシデントのたびに再発防止策の積み上げで整備してきた．その結果いざ新型コロナウイルスの爆発的感染で在宅勤務への急速な転換が必要となったとき，円滑に機能しない硬直的なシステム，使い勝手を犠牲にしながら大して安全ともいえない不便なシステムができあがってしまった．

新型コロナ対策による前例なき長期に渡る大規模な在宅勤務の継続を経て，これまで整備したインフラがうまく機能しなかった組織は，数年かけてITシステムの総点検を行う必要が出てくるのではないか．非対面でも社内外と円滑に共同作業を実施できる情報システムの実現のために，Blaster・個人情報保護法施行を契機に日本の組織が積み上げてきた情報セキュリティ対策をゼロベースで見直して，目的と手段をセットで再構築する必要が出てくる．

具体的なリスクを洗い出して実効的な対策を打つためには，システムとして従前の境界型セキュリティを見直すだけでなく，規程類の整備とシステム構築を一体的に検討できるように，プロパーとベンダとの関係や役割分担も見直す必要が生じる．PPAPの不条理は見直すべきITシステムを取り巻く矛盾の一端にすぎない．

（2020年4月5日受付）

■楠　正憲（正会員）　masanork@gmail.com

マイクロソフト，ヤフーなどを経て2017年からJapan Digital Design CTO．内閣官房 政府CIO補佐官としてマイナンバー制度を支える情報システム等の構築に従事．

［さようなら，意味のない暗号化 ZIP 添付メール］

3 我々はなぜ PPAP するようになってしまったのか

上原哲太郎 | 立命館大学

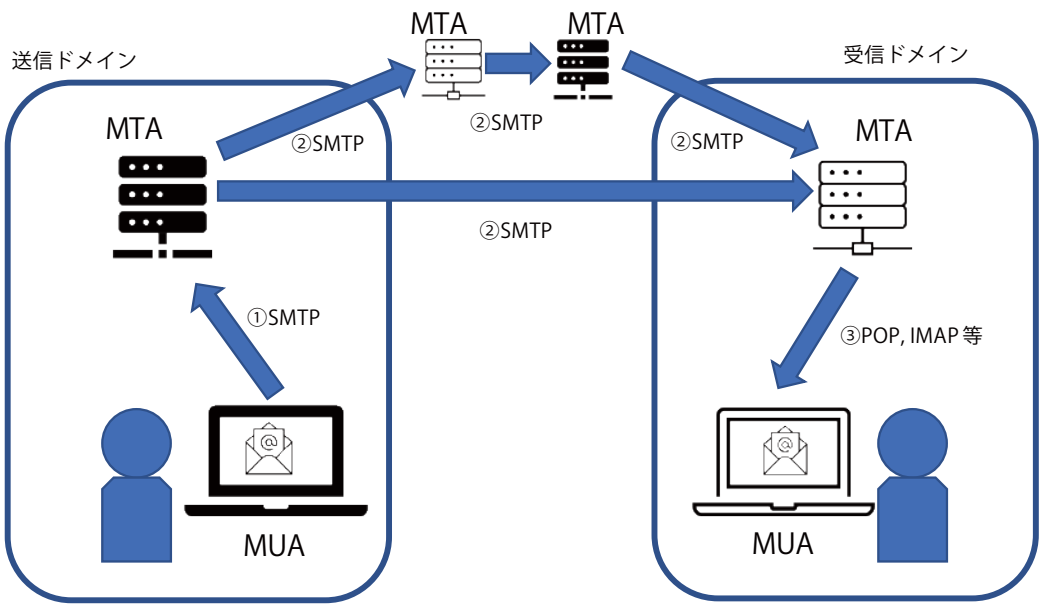
PPAP はなぜ生まれたか

情報システムのセキュリティ確保には技術的対策は欠かせないが，技術を運用するのは人だ．人に頼る限りは技術的に見て誤った対策でも広く使われるようになってしまうことがある．その最たるものが PPAP，すなわちパスワードにより暗号化されたファイルとそのパスワードを同経路で送ってしまうことであろうと思う．PPAP の定義については名付け親たる大泰司氏の別稿に譲るとして，ここでは「なぜ PPAP が生まれ，ここまで普及したのか」を論じよう．

電子メールは，そもそもセキュリティ上とても悩ましい存在である．インターネットがまったくの性善説で運営されていたころに生まれた電子メールは，そもそも認証や暗号化の仕組みに乏しい．電子メールは図 -1 にあるように，送信側の組織（送信ドメイン）と受信側の組織（受信ドメイン）に分かれた組織が協調して送受信を行う．その手順は，大きく分けて以下のような 3 段階からなる．

①送信者の MUA（Mail User Agent，いわゆるメーラと呼ばれるクライアントプログラム）から送信側の組織の MTA(Mail Transfer Agent, SMTP サーバ) に SMTP でメールを送信する．この際，利用者認証である SMTP AUTH や，SSL/TLS を用いた暗号化とサーバ認証である SMTPS の利用は必須とされていない．

②送信ドメインの MTA から，受信ドメインの MTA に SMTP で，直接または他の MTA を経由して送信する．この際，SSL/TLS を利用して受信側 MTA を



■図 -1
電子メール伝送の仕組み
How e-mails are transferred

認証し暗号化するSMTPSは必須とされていない．

③受信ドメインでMTAのメールボックス内に格納された電子メールを，受信者のMUAがPOPまたはIMAP経由で受信する．この場合はメールボックスに対する利用者認証は行われるが，やはり暗号化は必須とされていない．

電子メールがSMTPで配送されるようになった初期には，これらのいずれも段階においても通信は暗号化されておらず，その規格すらなかった．現在③は，認証に使われるパスワードを保護する観点からSSL/TLSで暗号化されることが多い．①においては主に迷惑メール送信を抑止する観点から暗号化や利用者認証を行う例が増えてきた．しかし②のMTA間通信については，暗号化はまだまだ十分ではない．仮に暗号化されていたとしても，複数のMTAを中継した通信である場合には，その中間のMTAにおいて盗聴等が行われない保証はない．何より利用者にとって送信前にその電子メールがどのようなMTAを辿って相手まで届けられ，またその通信や間で暗号化されるか確かめる手段はない．受信者にとっても（ヘッダから類推は一応できるものの）途中経路で盗聴されなかったか確かめる手段もない．

これらのことから，電子メールの送受信の仕組みだけ見れば，どこかに盗聴やなりすましの可能性が残っている．そもそも電子メールはその到達性も保証されていない，まさにベストエフォートなサービスである．しかしその緩さ故に利用や運用のコストを低く抑えることができ，それが電子メールの広い普及を支えてきたとも言える．

その後，次第にインターネットがインフラとしての重要性を増し，セキュリティ上の脅威が認識されるにつれ，インターネット上のどこかでの盗聴の脅威に備えて何らかの暗号化が必要であるという認識は広まった．この問題の解決には，メール本文や添付ファイルを暗号化する必要がある．そのため公開鍵暗号を用いたエンド・トゥ・エンド(E2E)での暗号化と電子署名による送信者認証を可能とするメール暗号化方式として，PGPやS/MIMEが提案され規格化された．しかし，HTTPSなどの通信路暗号化方式がサーバ側に公開鍵と秘密鍵のペアを持ちさえすればよいのに比べ，メールの場合はすべての利用者がそのメールアドレスに対応する公開鍵と秘密鍵を個別に持って管理する必要があり，この鍵の管理の煩雑さやコスト（特にS/MIME用の電子証明書コスト）が嫌われ，メールの標準的な暗号化は普及しなかった．

この状況でひねり出されたのが「添付ファイルをパスワードによる共通鍵で暗号化する電子メール」である．その暗号化も，当初は専用のソフトウェアが用いられる例もあったが，汎用性がありパスワードによる暗号化が可能なZIP形式が次第に主流となった．重要なファイルをZIPで圧縮しつつパスワードを用いて暗号化してから添付ファイルとして送付し，パスワードについては文書やFAXなどの別の手段で共有する手法が広まった．さらに，PマークやISMSなどのセキュリティ認証取得に際して「重要な情報を含むメールは暗号化すること」が求められたことにより，このようなパスワードによる暗号化をセキュリティ対策として認める動きが広がった．

しかしこのパスワードの伝達を電子メール以外の手段で行うことはきわめて煩雑であり，運用コストが高い．そこで，苦肉の策として「パスワードを別メールで送付する」という規定で運用する組織や企業が現れ，PPAPが誕生したのだろうと考えている．さらに，このような方式が各組織においてセキュリティ対策として認められてしまったことや，その疑わしい有効性に対して「メールによる情報漏えいの主なリスクは盗聴ではなく誤送信であり，その対策として一定の効果がある」という理屈がひねり出されたことにより，一気に普及が加速したように感じている．

このPPAPの普及にはもう1つ要因があるので

はないだろうか．一般にセキュリティ対策はシステムの利用者に負担を強いる．PPAP はまさに利用者にとって「余計な一手間」であって，本来ならこのような運用負荷を増すセキュリティ対策は受け入れられなかったかもしれない．しかし，特に技術的知識が十分ではないホワイトカラーの人々にとっては，パスワードはきわめて身近で分かりやすいセキュリティ対策である．ZIP ファイルを作成してパスワードを設定するという手間が，まさにセキュリティ対策をしているという実感，満足感を生んでしまうがために，PPAP はセキュリティ対策として広く受け入れられるようになったのではないだろうか．

PPAP に意味はあるか

現在では多くの企業や組織が添付ファイルの外部送信の際の PPAP を内規で義務づけたり，果ては PPAP を自動で行うシステムを導入している．しかし PPAP にセキュリティの観点からは効果がないことは明らかだ．暗号化されたファイルと，その復号に必要なパスワードを同一経路で送る限り，片方を入手できる攻撃者は他方も入手できるからである．

では実際にそのようなメールの読み取りは行われているのだろうか．最近被害が多いビジネスメール詐欺（Business E-mail Compromise : BEC）では，実際の取引でやりとりされているメールに突然割り込む形で，別の銀行口座への振込先変更などの指示をメールで送りつけ，金銭を奪取する手口が知られている．このようなことが可能なのは，その取引に関するメールをずっと覗き見られているからである [1]．その読み取りはマルウェアによって端末の制御をまるごと奪ったり，電子メールの読み出しに必要なアカウント（ID とパスワード）をフィッシング手法などによって奪ったりすることが先に行われているからだと考えられている．つまり電子メールの盗聴は攻撃の前段階として，きわめて広く行われると考えてよい．電子メールのアカウントそのものが奪われている状況では，すべての電子メールは攻撃者に読み取られるわけだから，PPAP はセキュリティ対策としてまったく役に立たない．

加えて，多くの場合はパスワードを用いて暗号化された ZIP ファイルの解読はそれほど困難ではないから，実は攻撃者にとっては，パスワードを知ることさえ必要がない．暗号化 ZIP ファイルの解読はオフラインでの総当たり攻撃が可能であるので，相当複雑なパスワードでない限り解読が可能である．少し古いデータであるが，文献 2）によると 2012 年当時の 1 台のパソコンで ZIP パスワードを 1 秒間に 45 億回試行可能であった．2020 年の現在，仮に 1 秒間に 100 億回のパスワード試行が可能なパソコンを用いると，英小文字と数字の組合せ 8 桁のパスワード全試行は 282 秒しかかからない．これに文字種として英大文字を加えたとしても，総当たりに要する時間は 6 時間ほどでしかない．オフライン攻撃に耐え得るパスワードは十分な文字種の複雑さと長さを要するが，文書など別の手段でこのパスワードを受信者に伝え，正しく入力してもらうのはきわめて繁雑な作業になってしまう．

このように，パスワードに頼ったファイル暗号化は，セキュリティを保つためにはきわめて煩雑な作業を受信者に強いることとなり，労働生産性に少なからぬ悪影響を与えていると思われる．ところが PPAP 方式を採る限り，普通の平文メールに比べてセキュリティ的なリスクが下がっているかはきわめて疑わしい．さらに，現在のメールを用いた業務で最も注意すべき標的型メール攻撃に対して，暗号化 ZIP ファイルは受信側 MTA でのマルウェア対策を無効化してしまうため，かえって受信者のセキュリティリスクを高めている恐れがある．このように，PPAP はセキュリティ向上には事実上役に立っておらず，生産性の低下とマルウェア混入リスクを高めるだけの存在ではないだろうか．

PPAP の代替手段はあるか

ここで原点に戻って，そもそも電子メールのセキュリティはどうあるべきで，PPAP に代わるセキュリティ対策はどうあるべきなのかを考察する．

ここでは，電子メールのセキュリティ対策として

①通信経路における盗聴のリスク

②メール送信者を詐称したメールを受信するリスク

③メール送信時に誤った受信者を指定し，内容を読み取られるリスク

上記 3 つのリスクを軽減することを考える．PPAP は本来①を軽減するために考えだされたものと思われるが，実際にはすでに述べたように盗聴防止としては役立たない．②はマルウェアや BEC 対策として重要だが，PPAP では対策できず，むしろマルウェア対策には有害である．③に関しては，すでに述べたように PPAP が一定の防止策となるという意見があるが，それは暗号化したファイルを送信してからパスワード送信までに誤送信に気づく可能性がある，という主張であり，少なくとも自動化された PPAP ではリスク軽減に役立たない．

では，このようなリスクを軽減するべくファイルを送信するにはどうしたらよいのだろうか．

(1) 最優先で考えるべきは，やはり S/MIME や PGP といった，E2E での暗号化を実現する技術の利用である．これらの技術は上記リスクの①と②を軽減することができる．ただし，③については，送信アドレスを誤って指定し，かつ送信先の公開鍵を保有していた場合には防止できないのでリスク軽減は難しい．また，S/MIME や PGP はその運用コストが嫌われてきた歴史があり，限られた組織や利用者を除いては今後も普及する見込みは薄いと思われる．

(2) そこで代替案として考えられるのが，既存の電子メール基盤の強化である，すでに述べた通り PPAP が生まれる原因となった電子メールのリスクは上記①，より具体的には MTA 間の通信の暗号化と相互認証が保証されていないことである．しかし現在はメールの転送トポロジは単純になってきており，送受信ドメイン以外に属する MTA が配送に介在する可能性は低い．さらに転送経路の SSL/TLS 暗号化も進んでおり，受信ドメインの MTA が TLS 対応であることを広報したり，TLS 以外での受信をしないことを宣言できる MTA-STS（MTA Strict Transport Security）という規格の普及も始まっている（RFC 8461）．よって，現在は MTA 間通信における盗聴のリスクはかなり小さくなっている．ここで不足しているのは，電子メールの送信者が，この MTA 間通信が安全に保護されていることを事前に知る手段である．ここは適切なツールが提供され，MUA と統合されることが今後求められてくると思う．これさえ提供されれば，送信者はそれを用いて経路の安全性を確認できれば，ファイルを暗号化せずに電子メールに添付し送信できるようになるはずである．

(3) いま現実に利用可能な策としては，Google Drive や OneDrive，Dropbox といったクラウドストレージの利用が考えられる．電子メールにファイルを添付する代わりに，これらのストレージを参照するための URL を電子メールに記述する方法である．これらクラウドストレージは通常 HTTPS を用いているので，上記①のリスクは相当低減される．受信者も同じクラウドストレージにアカウントを所有していれば，送信者も受信者を確実に指定できるし，受信者も送信者を確認しやすいので，上記②や③のリスクも低減できる．仮に送信者が受信者を間違って指定してしまったら，気づいた時点でファイルの共有を無効にすればよい．

この種のクラウドストレージによるリスクとして残るのは，クラウドストレージ事業者自身によりファイルを読み取られるリスクである．このリスクの低減には，そもそもクラウドストレージ上に置くファイルを ZIP 等でパスワード暗号化しておいて，メールでそのパスワードを伝える方法がある．もちろんこの場合も電子メール盗聴によるリスクは残るが，クラウドストレージ側でも送受信者双方が利用者認証されているという前

提であれば問題にならない.

なお，このようなファイル授受に特化したクラウドストレージとして Firefox Send がある．このシステムは以下のような特徴を持っている.

(a) ファイル送信者は Web ブラウザを用いてファイルをクラウド上に登録するが，その際にブラウザ内で暗号鍵が生成され，ファイルが暗号化されてアップロードされる．その暗号鍵はクラウド側には伝わらないので，クラウドストレージの運営者もそのファイルを復号することができない．その暗号鍵はブラウザで生成される受信用 URL 内に含まれている．この URL をメールで送信する.

(b) 送信者はファイルをクラウドに登録する際に，ファイルの有効期限を指定できる．その長さは最長 7 日であり，これを越えたファイルは削除されるため，漏えいリスクが軽減されている．さらに，ファイルのダウンロード回数も指定でき，これも最大 100 回である．さらに，ダウンロード URL がメール誤送信等で漏えいした場合でも直ちに URL を無効にすることで，ファイル自体の漏えいのリスクを最小にすることができる.

(c) 受信者はメール内に含まれる URL をクリックすることで，ファイルをダウンロードすることができる．この際, URL 内に含まれる暗号鍵によりファイルはブラウザ内で自動的に復号される.

このように Firefox Send はクラウドストレージにおける E2E 暗号化をほぼ実現しており，その意味で優れたファイル送信手段であると言える．ただし，厳密には受信時に暗号鍵を含む URL が一瞬クラウドに伝わってしまうため，厳密にはそこでクラウド事業者にファイルを復号されてしまう恐れがある．そこでオプションとして，ファイルアップロード時にブラウザ上でパスワードを入力することができる. このパスワードはファイル暗号化にも併用されており，かつ URL には含まれていないので，このパスワードをメールで受信者に送信することでクラウドの運営者にファイルを復号されるリスクも排除でき，完全な E2E 暗号化を実現できる.

もちろん基本的なこととして，電子メールのセキュリティにはその送受信用のアカウントを保護することや，マルウェア対策を行うことは欠かせない．また，上記リスク②に対応するための送信ドメイン認証（DKIM や SPF（RFC 7208）など）も重要である．電子メールがその送受信時に DNS を利用することから，DNSSEC など DNS の信頼性を上げる技術の利用も必要である．逆に言えばそれらを前提とすれば現在，すでに述べた通りメールの通信路における盗聴リスクはかなり下がっているため，添付ファイルをわざわざ暗号化する意味は失われつつあると思われる．この認知が広がれば，PPAP のように単に手間を増やすだけの，役に立たないセキュリティ対策はやめて，単にファイルをそのまま電子メールに添付した方がましという空気感が醸成できるのではないかと思っているのだが，それは楽観にすぎるだろうか.

参考文献

1) （独）情報処理推進機構，ビジネスメール詐欺「BEC」に関する事例と注意喚起（2017）.
2) （株）ディ・アイ・ティ：パスワードの最大解読時間測定，セキュリティ調査レポート Vol.3（2012）.

（2020 年 5 月 16 日受付）

■上原哲太郎（正会員） t-uehara@fc.ritsumei.ac.jp

和歌山大学，京都大学，総務省を経て 2013 年より立命館大学情報理工学部教授．専門はサイバーセキュリティ，システム管理，ディジタル・フォレンジック．入力しにくいだけの Excel 帳票や無駄な押印の撲滅にも興味を持つ.

［さようなら，意味のない暗号化 ZIP 添付メール］

4 座談会「社会から PPAP をなくすには?」

崎村夏彦 | NAT コンサルティング　大泰司章 | PPAP 総研
楠　正憲 | 国際大学 Glocom　上原哲太郎 | 立命館大学

PPAP の定義

崎村：さて，本日は「社会から PPAP をなくすには?」というテーマで座談会を行いたいと思います．アジェンダですが，PPAP の定義，PPAP 賛成の論拠への反論，より良い方策を議論します．まず PPAP の定義ですが，オフラインで鍵を共有するのも PPAP だと思っている方もいらっしゃるようなのですけれども，それは違いますよね．

大泰司：1 通目に ZIP を暗号化して添付ファイルを送って，2 通目でパスワードを送るというやり方です．2 つの軸があって，パスワードを同じ経路を送るか，違った経路で送るか．もう 1 つは，すべての添付ファイルを暗号化するか，自分で判断して特定のファイルだけ暗号化するか．自動で添付ファイルを暗号化して送るソリューションを使うと，すべての添付ファイルを暗号化し，同じ経路でパスワードも送信することになる．これを，この議論では PPAP と呼びたいと思います．

上原：この議論では，暗号化 ZIP が送られて，すぐそのあとにパスワードが追いかけていくスタイルに限るということですよね．

PPAP 賛成の論拠への反論

誤送信防止

崎村：PPAP の定義は分かったので，PPAP 賛成の論拠への反論を挙げていきたいと思います．

上原：PPAP 賛成派の意見には何があるのでしたっけ．

大泰司：手動で送って，2 通目までの間に間違えたなと気が付くケースがあるというものです．

上原：それだけを論拠に頑張っているんですかね．自動の場合はまったく意味がないですよね．

大泰司：ないですね．ただ，多くの場合はこのソリューションを誤送信防止ツールと銘打って売ってます．送る前に，本当にこの宛先でいいですかとダイアログが出てきて，OK，OK，OK とクリックしないと送信されない．大体この機能が入っています．

上原：それは，添付ファイル暗号化とは関係ないよね（笑）．送信前にメーラーでメールアドレスを確認する機能を付ければいい．

楠：この問題は根深くて，本当にいちいち OK を押さなければいけないし，そのあと保留され，さらにメール上，リンクを組んでどこかのページで挿入をするみたいなフローが入っていたりする．

　あとは，会社によっては，上司を CC に入れないと添付ファイルを送れずに，自分だけで送ろうとすると自動的に止まるとか，いろんなバリエーションがある．

上原：上司の承認を得るために，上司を CC に入れ，CC に入っている上司が OK を押さないとメールが出ていかないというのは，それはそれでガバナンス上，意味はなくはない．だけど，それは添付ファイルとは関係ない気がします．

崎村：添付ファイルあるなしでリスクが異なるという

のはあり得ます．だから上司がもう1回，その添付ファイルが正しいかどうかを確認するのはありかもしれない．

以前，知っているケースでは，ちゃんとPDFにした見積書を提出しなければいけないのに，Excelをそのまま添付してしまって，中のコスト構造やなんかが全部ばれてしまった．上司が確認したくなるというのも分からんでもない．でも，PPAPとはまったく関係ないですよね．

上原：そうだと思うのですよ．だから少なくともZIPで暗号化するのというのは相手にコストをかけているだけなので，まったくセキュリティ上の意味はないですよね．

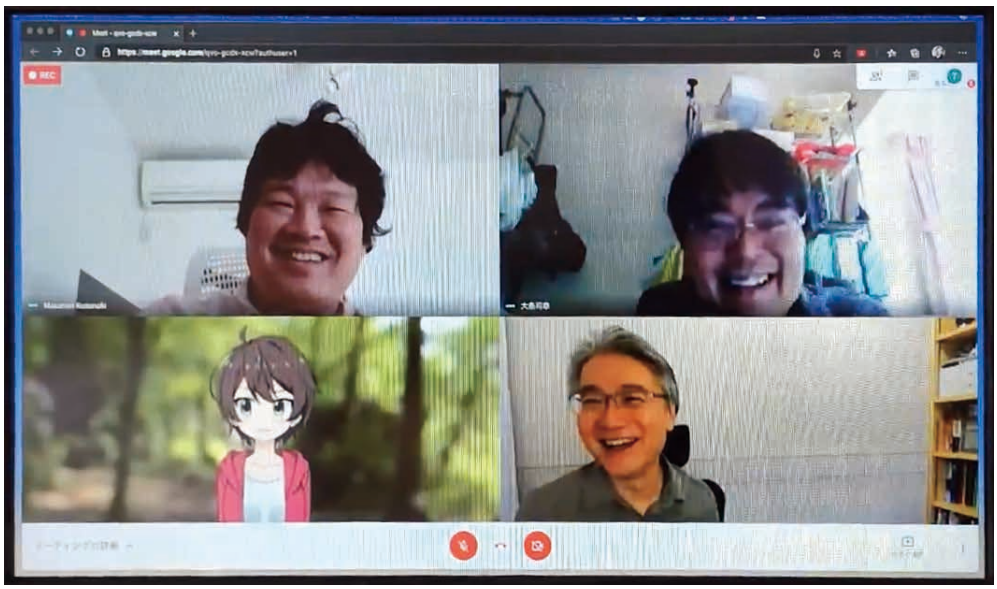
崎村：ないと思います．あと，誤送信防止ということだと，僕，実は2005年ぐらいに社内のR&Dでプロトタイプをつくったことがあります．実際には運用されなかったのですけど．まず，メールの最初の3行に相手の所属と会社名と名前を入れる．メールを送信するとゲートウェイがその最初の3行を読んで，会社名とドメインとをマッチさせ，マッチしないと本人にメールがきて，ドメインがマッチしないけど本当にいいですか?と確認をとるというものです．

大泰司：それと同じようなシステムについて，誤送信防止システムを出しているベンダさんから相談がありました．それで，日本のすべての会社のドメインリストを提供してくれないかと言われたのだけど，それはできなかった．

崎村：大きな会社だと大抵取引先登録をしているので，そこからドメインを引っ張ってくればいいと思ったのですよね．あと上場企業だったら当然引っ張れるし．技術的には可能で，メールを送れなくするわけではなくて，本当にドメインがマッチしないけどいいんですかと確認するだけだから．いや違っていてもいいんだといってやれば，それはそれで問題ない．

上原：誤送信で一番多いパターンというのは，たとえば，メーラーがアドレス補完機能を持っていて，立命館大学の上原にメールを出すときに，宛先にueharaまで打ち込んだら補完されて，そこでエイヤーと出してしまうと，実は全然違うコンプリーションしていて，まったく違う人に送信してしまうパターンなのではないですか．誤送信防止の人たちが主張しているのはほかにどんなパターンがあるのですかね．

楠：たとえば，ルール上，組織以外は全部BCCに入れなければいけないのに，CCに入れて，個人情報



■座談会の様子
左上：楠　正憲
左下：上原哲太郎
右上：大泰司章
右下：崎村夏彦

漏洩になってしまうケースとか.

上原：でもそれもPPAPと関係ないね. CCをチェックすればいいわけですよね.

楠：そういう機能も入っていたりします.

崎村：アドレスの補完機能があるからこそ誤送信が減ると考える人たちもいるわけですね. ただ，皆さん失敗からしか学ばないので，補完機能で誤送信したということがあると，3カ月後ぐらいに補完機能が使用禁止になったりする.

間違ったPDCA (Plan-Do-Check-Action) が日本中をまわっていて，基本的にその機能がなくしたミスというのはミスとしてカウントされない. あらかじめ登録してある，相手が分かっている，謝れば済む相手しか補完されないはずなのに，その補完機能をオフにしていると全然訳の分からない人に送られてしまうというのがある.

取引先として登録してある人だったら，もう面が割れて，たぶん知っている人だから，間違って送ってしまった，ごめんなさい，で済んでしまうわけですよね. しかし，まったく面識のない人に送られてしまって事件になるリスクを考えると，後者の方が実はリスクの度合いとしては大きいような気がするのですけれども.

ISMSやPマークが要件としているという都市伝説

上原：やはり，こう，納得感がある理由がないのに何でこんなに使われているのですかね.

崎村：人によっては，ISMS (Information Security Management System) が要求するからとか，Pマーク (プライバシーマーク) が要求するからとか，そういう都市伝説があって，その都市伝説に従って実装している人たちも結構いるみたいです.

上原：Pマーク説は結構あちこちで聞きますよね. それで，大泰司さんは結局その犯人捜しはしたんでしたっけ.

大泰司：犯人捜しして，見つからなかったのですよ.

上原：やはり見つからなかった.

大泰司：ただ，誤送信防止のソリューションを出しているベンダがPマークの審査基準がこう改定されているから，これに対応しなければいけませんというようなことは書いていますね. では本当にPマーク審査の現場でどうなっているのか聞いてもらったけれども，分からなかったです.

それで，JIPDEC (一般財団法人日本情報経済社会推進協会) の中に教育用・研修用資料としてガイドラインのようなものがあったのですが，それを見たら，個人情報は暗号化しましょう，そのファイルを送ったときにはパスワードは別の手段で送りましょうと書いてある.

上原：別の手段とは書いてありますね.

楠：うん. 正しい.

上原：別の手段だったら正しいのですけれども，別の手段というのが同じ手段のメールにいつの間にか化けているということですかね.

大泰司：うん. そうですね.

崎村：審査基準の中に，個人情報を送るときは暗号化，安全管理措置をとることとは書いてある. でも，キーを同時に送っていたら安全管理措置として崩壊している.

楠：ただ，そこまで中身を見ない，チェックリスト式のセキュリティの人たちというのは，自分の頭でリスク評価をできない人が多くて. 対策しているかどうかと，その方法は社会で使われている実績ある方法かという，この2つを気にしている. 確かにPPAPはこれを非常によく満たすいいソリューションなんですよね.

上原：本当に広く，セキュリティを売りにしておられる大上場企業さまがお使いなので困ってしまう.

楠：たまによく訓練された日経BPの編集者なんかだと，ZIPはメールで送ってきて，パスワードはSMSかFacebookメッセージで送ってくる人はいますね.

崎村：それは正しい.

上原：まあ，正しいは正しいですね.

崎村：だから僕がもしパスワード付きZIPをやるのだったら，頻繁にやりとりする相手だったら，あらかじめ

両者で秘密鍵を決めておいて，それで送るようにすればいいですよね．

楠：私の働いている保秘を大事にする某所ではまさにそのやり方を使っているのですが，プロジェクトの数だけ約束事があると，最終的に破綻するのですよ．もうね，何カ月かおきに同僚に頼んでポストイットに書いてもらうという儀式が（笑）．

崎村：ただね，PPAP のほうが相対的に楽というのは，なぜかというと効果がないから．

PPAP に代わる安全な方式

SMTPS の強制

崎村：さて，では PPAP に代わる安全な方式の議論したいと思います．

上原：相手との SMTP の経路が SSL 対応になっているのだったら，もうそのまま送ればと思っています．安全という意味では十分安全．いまは通信区間にセキュリティリスクはあまりない．むしろ末端がこわい．マルウェアやフィッシングで ID を取られ，メールボックスの中を盗み見られていることのほうが問題．そっちを守ることにエネルギーを使うべき．経路のことはあまり気にしなくていいんじゃないか．

崎村：何を守ろうとしているかという部分ですよね．経路の安全性と到達先での安全性と 2 つある．あと PPAP な人たちがよく言っている誤送信防止．

上原：誤送信防止対策は別の方法でやるべき．G メールは送信ボタンを押してからしばらくは取り消せるようになった．PPAP で送ってから気が付くと主張する人たちは，このことをどう思っているのかなと．確かに僕も気が付くことがあるのですね，あっ，しまった，送り損ねた，戻そうみたいなのはたまにある．でも逆に言うと，あれで十分じゃんと．それが 1 つ目ですね．

事前鍵交換共通鍵暗号化ファイル添付

崎村：次に，事前鍵交換の共通鍵暗号化ファイル添付．本来の PPAP の在り方としては，あらかじめオフラインで共通鍵を交換しておいて，以後，その鍵でファイルを暗号化してメールに添付する．そうすると，鍵の長さが十分であれば，強度は十分となる．そもそもの誤送信対策で，元々やられていた本来の暗号化 ZIP の使い方．相手との間で事前に共有した鍵があるから，それ以外のところに送っても大丈夫，だから誤送信対策としても機能する．

楠：それこそが本来の誤送信対策なのですよ．

上原：ただ，十分長くて複雑な鍵じゃないといけない．某役所の仕事はこの事前共有鍵方式．UX 的にはしんどい．

楠：プロジェクトとか，研究会の数だけ覚えるのはまず困難．

崎村：こういうのは 1Password みたいなパスワード管理ソフトを使うしかない．

大泰司：またはモニタのまわりが付箋だらけになると．それでも分からなくなるから，前は部下に開けてもらっていました．

崎村：1Password は企業モードがあって，こういうシークレットキーを複数人でシェアできる．まさにそういうためのものではないかと．

楠：その問題を公開鍵暗号でクリアしてくれて僕らは幸せな時代を生きているはずなのに，なんでこんなにシェアードシークレットのハンドリングにこの 21 世紀に苦労しているんでしたっけ．70 年代にシャミアさまとかが解いてくれた大事な問題なはずなのだけれども．

公開鍵暗号化ファイル添付

崎村：その流れだと，次に出てくるのが公開鍵暗号化ファイル添付，アリスとボブがそれぞれの公開鍵を一定の場所に公開しておいて，その公開鍵を使ってファイルを暗号化して．PGP とか．

上原：PGP の鍵を公開しておいてやりましょうというのは，たとえば，IPA の届け出がその方式ですよね．

楠：PGP を使えないと届け出ができないというのはな

かなかすごいハードルが高い感じで.

崎村：UI（User Interface）や, Windows や Mac に最初から入っていないなどの問題ですよね. 逆に言えば, 皆が持っていて, UI も良いという状態になれば使えるということではある. エストニアは ID カード配布と同時に署名・暗号化のためのソフトを配っています.

公開鍵メッセージ暗号化（S/MIME）

上原：私はまだ細々と S/MIME で抵抗を試みています. 私のメールは S/MIME 署名されているのですけれども, この S/MIME 署名している鍵はどこにあるかというと, G さまが保管しておられます（笑）.

楠：G Suite ですか.

上原：そうです. G Suite の中でやっています.

崎村：私もやれるのですけれども, やって意味があるのかどうか（笑）.

楠：だいぶ哲学的な問いですよね.

上原：ええ.

崎村：多くのメーラーが, 特に携帯など, S/MIME で暗号化されてきているメッセージは読めない.

上原：暗号化は読めないですね.

楠：添付ファイルが読めるか微妙な感じ.

崎村：本文が表示されなくなってしまったとか.

上原：smime.p7s だって「ウイルスみたいなファイルが付いているけれども, 何ですか」というお問合せをいただく（笑）. あるいは, ゲートウェイで削除しましたというメッセージ付きで向こうに届くとか（笑）.

大泰司：サニタイズされてしまうのですよ.

上原：そうなのですよね. まあでも S/MIME はやればやるほど普及しない理由はよく分かってしまって（笑）. 昔はファイル名に日本語が交じると正規化アルゴリズムの実装が微妙に異なっていて, 検証が失敗するとか互換性問題があった. それはだいぶ解決したのですが, 一方で鍵管理の問題が解決しない. 私は S/MIME で届いたメールが暗号化されていたら IMAP（Internet Message Access Protocol）の Inbox に復号した状態で保存してほしいと思うのです. 暗号化したまま置いていると, その古いファイルを取り出すために自分の古い証明書をずっと持っておかないといけないから. でも, これがすごく難しい. そういううまい UI を提供してくれているメーラーがない. 署名にしても, 古い証明書をずっと履歴管理できるメーラーじゃないと昔のメールの署名確認に困る. なので, 両方の意味で, S/MIME はちょっとつらいのは実情かなと.

楠：やはり鍵管理そのものが人類に早すぎたのではないかと. 鍵管理というのはやはり難しい.

崎村：でも, だとすると, 暗号というのはすべての問題を鍵管理の問題に置き換える話・技術だから, 暗号化は無理筋という話になってくるわけですね.

楠：まあだからよろしく GAFA（Google Apple Facebook Amazon）に守ってもらおうという流れになってしまう.

上原：それで, その古いメールを取り出すたびに思うのですけれども, さっきの楠さんの話ではないですけれども, なんで S/MIME というのは 1 年ごとに証明書を更新しなくてはいけないんだっけと思うわけですよ（笑）.

大泰司：今, 3 年. 今度 2 年になったのかな.

上原：だんだん縮んでいっているので.

大泰司：特に暗号化に期限の短いものを使う必要は全然なくて, 署名のほうはまあしょうがない. 実際に使っていると S/MIME の暗号化はすごい楽ですよ. もう普段, 意識していないぐらいに.

上原：ただ, S/MIME の暗号化で普段, 意識しないとおっしゃるのはすごくよく分かるのですが, 意識せずに使えるというのは実は逆にネックになっているような気もしていて, ちゃんと自分は暗号化して送れているのかとか, 暗号化したものをちゃんと受け取ったのかというのをちゃんと確認する習慣を削いでいくような気がするのですよね. それはそれでいいのかみたいな気がして.

DNS を使った ID ベース暗号

上原：一応そこもですね，私，ささやかながら抵抗を試みていて．学生さんにつくってもらって情報処理学会の研究会で発表したのですが，DNS（Domain Name System）ベースの公開鍵暗号をつくっています．公開鍵というか，いわゆる ID ベース暗号なのですが，ID ベース暗号の公開パラメータをドメインごとに DNS で公開する．そうするとその DNS の管理がちゃんとしている限りにおいては，そのドメインで使っている ID ベース暗号のパラメータは DNS で入手できるから，それを使ってお互いにやりとりができる．有効期限の議論は，危殆化したことをドメインのほうが認識するまではエクスパイアしないという（笑）．そういう運用ルールで考えていて，危殆化したら DNS の鍵を入れ替える，その代わり古い鍵はあるルールで残して公開を続けるみたいな，そんな仕組みで設計しているところなのです．

メールのセキュリティというのは，S/MIME の普及が進まない間に別の方向に進化していて，PKI（Public Key Infrastructure）では SMTPS，POPS，IMAPS などの転送レイヤだけうまく技術が普及している．それより上位レイヤは，DKIM（DomainKeys Identified Mail）など，ひたすら DNS に頼っているわけです．

楠：SPF も含めて．

上原：SPF（Sender Policy Framework），さらに DMARC（Domain-based Message Authentication, Reporting and Conformance）ができて，それで今度，トランスポート層が SSL に強制されていることを MTA-STS（Mail Transfer Agent Strict Transport Security）で公告するようになってと．全部 DNS に頼っていて，それをみんな信用できているのだったら，DNS に残ったリスクというのは，みんな目をつむれるのかなと．今の PKI は DNS を信頼できないものとして扱いますけれども，DNS を信頼する公開鍵暗号系を標準化できないのかなというのは今ちょっと思ってて．

楠：結局 PGP が流行らなかったのは公開鍵の交換のところで，これをキー・サーバをつくるのではなくディレクトリをと考えたとき，インターネットでグローバルにスケールしているディレクトリは DNS という話に間違いなくなりますからね．

上原：そうなのですよね．キー・サーバがまったくスケールしないことが分かっていながら進むうち，やはりみんな使わなくなった．

楠：本当はあれってブロックチェーンも解になりそうな気もしたのですが，トラストレスと言っているからなのか，あまりこっちの用途には広がらなかったですね．

上原：そうですね．

崎村：まだちょっとその辺は頑張ってみたいなとか思っているのですけれども，その変形としてこの間，僕は自分の公開鍵を Twitter でツイートしたのですけれども（笑）．

上原：せっかく暗号技術も進んできたのだから，運用も UX もそんなにおかしくならない全体をデザインしたスマートな仕組みにしないと S/MIME の置き換えになるようなメッセージングは出てこないような気がしていて．それが進むまでは PPAP がなかなか打ち倒せるようなものにならない．でも PPAP というのは UX 的には最低なのにどうして死なないんだとは思っています（笑）．

崎村：いや，あれはコンプラで強制されるから．

楠：あのコンプラ村の人たちの UX への関心の低さって何なんでしょうね？

崎村：ユーザブル・セキュリティとか，ヒューマン・セントリック・セキュリティとかと対局にいる感じ．しかし，PPAP を強制する人たちって，本質的にセキュリティが分かってないんでしょうね．分かってたらあんなことしないはずだから．日本のローテーション人事の特質で，専門家を当てないというところにも問題があるかもしれない．だから日本だけで PPAP がはやるみたいな．

上原：1 つ確実に言えることは，ルールを決めて守らせる人が，エンジニアリングにも UX にも仕事の効率

を保つことにも興味がない．本来は，どうやって効率を上げるかを考えてもらわなければならないはずなのに．

崎村：科学的理由がないところでのドグマがあって，そのドグマによって強制される儀式を踏んでいれば，科学的に間違っていてもそれが正当化されてしまう．科学的に安全を求めるのではなく，儀式によって安心を求めているように思える．

楠：安全なものをくださいと言っても，完璧に安全なものなどない．それが認知的不協和を呼ぶ．セキュリティに金をかければかけるほど不安になる病．だから安心を求めにいく．

認証連携ファイルアクセス制御

崎村：認証連携ファイルアクセス制御は，アクセスを許す相手の属性（通常はメールアドレスなど）を指定して，当該ファイルへのアクセス制御を行う仕組みです．それでそのファイルへのリンクをメールやチャットなどで送る．これが海外で割とメインストリームになってきているのかなという気がします．

大泰司：今，PPAP の自動化ソリューションを使っている企業はこれを簡単に導入できるはず．オプション料金がかかるところと，そのまま標準についているところがありますけど．

楠：やはり私の原稿でも書きましたが，結局，添付ファイルをやめてリンクを送ればいいんじゃないかと．そうすれば，添付ファイルにアクセスするというか，送りたかったものにアクセスするタイミングでもう 1 回，認証認可も走るし，あとから取り消すこともできる．今，Office 365 も，G Suite も，大体そんな実装になってきている．添付ファイルではなく，クラウドなりでファイル共有サービスとの連携に寄せていけば，ストレージも余計に食わないし，メリットはでかい．

崎村：これが結構，実はメインストリームに今なってきている感じがしますよね．

クラウド共有

上原：ただ，そういうクラウドはだれか分からない管理者が見ているかしれないから信用しないというのは分からんでもない．その意味で面白いのは Firefox Send．クラウドに確かに保管されるのだが，まずアップロードのところで暗号化される．Firefox Send 管理者には中身は見えない．鍵は URL に含まれた状態で相手に送られる．相手がメールを開いて，Firefox Send のサーバにアクセスしにきた瞬間に鍵が届いて，解きながらダウンロードされる．すごくよくできているなと思うのです．

ただ，惜しむらくは，URL に鍵が含まれているので，最後の瞬間に鍵がサーバにいっている．あと一歩 end-to-end 暗号化に足りない．

ただ，よく考えたら，その Firefox Send を運営する立場からすると，自分のところにあるストレージは全部暗号化されているので，たとえば，それこそ捜査機関がやってきて，お前，出せと言われても，いや知りませんと言えるというのが一番の実はメリットなのではないかなと思いながらあれを見ていたのですね．

崎村：Firefox Send みたいなのはどのカテゴリですかね．

楠：あれはクラウド共有の一種類なのかな．end-to-end encryption までやっているとちょっと違いますけれどもね．Firefox Send，好きすぎて，会社用に立てましたよ（笑）．

上原：いや，会社用に自分で Firefox Send を立てるというのが一番安全でいいと思うのですよね．Firefox Send のもう 1 つの欠点は送信者の認証がないこと．メールが送信者認証されていればいいのですけれども．Firefox Send を自ドメインで運営すれば，少なくともその組織からきたというのが分かる．

楠：はい．

崎村：わたしは，Firefox Send じゃないけど，NextCloud を自分のドメインで立てて，そこからリンクを共有するとかやってます．結局この手のものとい

うのはあれですよね，送信者認証，受信者認証，メッセージ認証，この 3 つと，それに基づく認可に尽きるのですよね．

上原：そうですね．はい．

楠：それで今，Firefox Send をまず立ててみて，銀行の業務要件に従ってそういうファイル受け渡しツールとかをつくれたら PPAP の代わりに売れないかなとか検討したのですが（笑），結局 end-to-end encryption している瞬間，ウイルススキャンをかけるみたいな要件を満たせなくてつらいみたいな．

上原：いや，だから，Firefox Send の受け取り手順に 1 枚かませて，受信側組織はファイルをダウンロードしてウイルスチェックをしてからエンドユーザに渡すみたいなソリューションとセットでやればいいかと思っているのですよ．

楠：それはそういうサーバ立てて復号するのですよね．

上原:ええ．だからまあそういうのをちゃんと動かすサーバをつくらなければいけないんですけど．

楠：ああ，受ける側でそれをインターセプトしてというのはなんかだんだん何のために何をやりたいのかが分からなく．

上原：まあでも自分の組織の中で閉じてできるのなら，たとえばその受け取った Firefox Send の URL を社内のある Web Form に突っ込むと，sanitize してから送ってくれるみたいなソリューションでもいいと思っていて．

楠：受け手のソリューションを別に用意するという．

上原：そうそう．そうです．

楠：代わりにファイルをダウンロードして，無効化なり，アンチウイルスなり，チェックをかける．

上原：そうそう．それでそのあとメールでエンドユーザに送ったら元の木阿弥かもしれないので，たとえば，共有フォルダにぽこんとその人の権限で置いてくれみたいな．

楠：ではそういう Firefox Send に Selenium かなんかでアクセスをして，ひと通りのことをやってくれるやつを端末側で用意をしてやる．

上原：そうです．はい．

楠：なるほどな．なんかそこまで立てるのだったら，もうちょっと素敵なプロトコルにしたくなるな（笑）．

上原：まあそれはそうですね．はい．

組織超えグループウェア

楠：でも Firefox Send って，若干関心が高まったのというのはやはりみんな宅ふぁいる便難民になったときだと思うのですけれども．あの宅ふぁいる便がリスク管理部門をクリアしていたというのは一体何だったのかなと．

大泰司：あとなくなってしまったのですけれども，サイボウズ Live を使っている時期がありましたね．会社をまたいでグループをつくるとき，よく使われていましたね．

上原：組織越えのグループウェアみたいなものですよね．

崎村：そうそう．

大泰司：今，その人たちはだいたい Slack にいったんですよね．でも，Slack に移れないおじさんが結構，残ってしまいました（笑）．そういう人たちはいま Facebook に流れ込んでいる．

楠：でも，メッセンジャーでは置き換えにならない．業務で使うのだったら，どちらかと言うと Slack などのビジネスチャットなのかなと．

上原：システム管理部門にすごく力があれば，一番いい逃げ先は今，Teams だと思う．だけど，テナントデザインがすごい難しい．

楠：それは Active Directory の運用の細かいところが．

上原：いや，そもそもチームをつくるという権限をだれに与えるかとかですね．あと，チームでつくると，グループウェアとしてファイル共有ができたりするのですが，その仕組みが，あの上にあるのですよ，何だっけ．

楠：SharePoint.

上原：SharePoint の上にあるのですよ．その連携が，いろいろ気持ち悪いのですよね．

楠：SharePoint をパーツっぽく使っているおかげで，

Teams でごにょごにょやっているといつの間にか SharePoint 側に不思議な枝が生えていきますよね.

上原：そうそうそう．不思議なファイルが SharePoint にできるのですよね．それもなんか気色悪くて.

楠：しかもそれもみんな検索の対象とかにいつの間にかなっている.

上原：そうそうそう．それで，ある大学の先生から聞いてびっくりしたのですが, Teams でフォルダを掘るときに, 最初, 適当な名前で付けておいて, あとでちゃんとした名前に変えても, SharePoint にできるフォルダが，その最初の名前のまま（笑）.

楠：リソース名だけ変わる.

上原:リソース名だけ変わるので（笑），最初「ほげほげ」で作ると，「ほげほげ」というフォルダが SharePoint 側にできて，ずっとそのまま（笑），ひどいシステムだということが分かった.

楠：なかなか切ないものがありますね.

上原：びっくりしましたね.

大泰司：だから今そんな感じでプロジェクトごとに使うツールが別々でものすごい大変.

ビジネスチャット

楠：それで言うと，我々はもはや電子メールではなくて LINE とか，Telegram とか，素晴らしい end-to-end encryption ソリューションを持っているわけで，メールが残っているのは法人の問題ですよね．業務で使えるのだったら，どちらかと言うと，Slack とか，ビジネスチャット系なのかなというふうに.

上原：まあ電子メールがいいのはインターオペラビリティがちゃんと確保されていること．あと，これはもう文化の問題ですが，仕事の依頼を LINE で送るとは何事だと怒り出す人がいる（笑）.

崎村：昔はメールだって怒られたのですけれどもね.

上原：そうそうそう（笑）.

大泰司：昔ね，メールで怒られていましたよ（笑）.

上原:今はメールも，マナーと流儀と仁義を切ればちゃんと認められるようになった．だからインスタントメッセージングでも，インターオペラビリティあるかたちで標準のものが出てきてくれればいいのですが，ちょっと望み薄なので，しばらくはメールの地位は揺るがないという気はしているのですよね.

楠:そうなのでしょうね，XMPP（Extensible Messaging and Presence Protocol）とか，一時期，インスタントメッセージングプロトコルの標準化の議論もだいぶあって，iMessage などオープンな仕組みにつながったりしましたが，あまり流行らなかったですね.

上原：結局，まだまだメッセージングの世界は囲い込みをしないことには競えないのですよね，きっと.

楠：あとは結局，ことごとく UX にかかわるものが規格に響いてきてしまうから，標準に乗った瞬間に中途半端なものしか出せないというのはある気がしますね.

上原：なるほどね．それはそうですね.

楠：やはり鍵のハンドリングというのは，最後，一番，プロプラで残りそうな部分というか, PKIX WG（PKI の標準化を議論する IETF のワーキンググループ）がうまくいかなかったことによって，オープンでやってうまくいった動きはあまり少ない.

業務システム

大泰司：電子契約というのはここ 1 ～ 2 年でどんどん入ってきている．調達や営業部門では，見積書が PPAP できて，イラッとするところですが．でも，これはもう電子契約にどんどん移っていきますね.

崎村：定型業務は電子契約や CRM（Customer Relationship Management）にどんどん移っていくという話ですね.

楠:そう，寄せていくのが大事．ツールがないところだと，添付ファイルのようななんでも送れる仕組みを使って，その結果問題を起こしたりする．要りもしない実行ファイルとかも送れるようになっていて.

上原先生ともよく話しているのですが，電話にしても，メールにしても，好きに入力した文字列で指定した相手に自由にものを送れる仕組みはやはり限界

がある．社内コミュニケーションなど密度の高いやりとりは，Slack や Teams など，決まった相手とのやりとりに限定したものに寄せていく．それで電子メールの使い道をできるだけ日々の業務から減らしていく．大代表のメールに入れると，セールスフォースで CRM で反応するみたいな，汎用メーラーを使わないようにしていくのが本当はいいのだろうなと．

上原：そうですね．

崎村：だから業務で，いわゆる電子メールを使うのは本来間違っていると思うのですね．これは金融機関のコンサルをやっていたときにも強く言って，ネットワークの分離などではなく，本来は顧客向けのメールだったらちゃんと CRM から出せと．そうすると文面のコンプライアンスも何もかも全部入るわけですよね．EUC (End User Computing) をやるなと．電子メールなんていうのは EUC の最たるものだろうと．

楠：しかもメールボックスというのは個人単位なので，人事異動があったときに管理できなくなる．社外とのやりとりは全部 CRM でいいんじゃないかなと．

上原：メールがいろんなものの非効率を生んでいる．組織内でも添付ファイルをつくって，ご査収くださいとかいうのを組織内でぐるぐる回しながら，いろんなバージョンのファイルが散逸していく．リスクも増えていくし，バージョン管理もできない．あの状況を何とかしないといけないという意味でも，メールはもうなくしてしまったほうがいいと思っていますね．

大泰司：オンラインストレージを使うのがいいと思います．現実にもうかなりそうなっている．PPAP の誤送信防止ソリューションのベンダも，大手は設定 1 つでオンラインストレージを使うようになっている．

楠：なんか明らかに異なる文化圏があって，VDI (Virtual Desktop Infrastructure) が入っていて，フィルタリングソフトで主要なクラウドサービスはみんなフィルタリングしている一連の会社や役所がある．あの文化圏の人たちは，在宅勤務のサポートに苦慮しているような感じになっていますが，これからどうするのでしょうかね．

より良い方式のまとめ

崎村：大体，出揃いました．議論に出た「より良い方式」をまとめますと，まず第 1 に，できるだけ通常のメールを使うのはやめる．通常の業務は汎用メールクライアントを使うのではなく，CRM，EDI (Electronic Data Interchange)，電子契約システムなどの業務システムを使って行う．これらが SMTP を使う場合には TLS を強制する．

非定形のコミュニケーションは，お互いに認証されている Slack や Teams などの「ビジネスチャット」を使う．ファイルはこの上で送るか，「認証連携ファイルアクセス制御」の効いているクラウドストレージを使う．そんなところでしょうか．

楠：この辺に落ち着く気しかしないですね．

日時：2020 年 4 月 24 日
場所：オンラインにて

■**崎村夏彦（正会員）** nat@nat.consulting

本会 SC 27/WG 5 主査．OpenID Foundation 理事長．ディジタル・アイデンティティとプライバシに関する国際標準化が専門．著した規格に OpenID Connect, JWS, JWT など．

■**大泰司章** otaishi@gmail.com

三菱電機，日本電子計算，JIPDEC を経て，PPAP 総研設立．電子契約，電子署名，メールや Web のなりすまし対策を普及．PPAP やハンコ等の非効率な取引慣行を変えて，真の働き方改革を目指す IT コンサルとして活動中．

■**楠　正憲（正会員）** masanork@gmail.com

マイクロソフト，ヤフーなどを経て 2017 年から Japan Digital Design CTO．内閣官房 政府 CIO 補佐官としてマイナンバー制度を支える情報システム等の構築に従事．

■**上原哲太郎（正会員）** t-uehara@fc.ritsumei.ac.jp

和歌山大学，京都大学，総務省を経て 2013 年より立命館大学情報理工学部教授．専門はサイバーセキュリティ，システム管理，ディジタル・フォレンジック．入力しにくいだけの Excel 帳票や無駄な押印の撲滅にも興味を持つ．

■表 -1　PPAP に代わる安全な方式

項番	方式名	方式説明	メモ	経路安全性	到達先安全性	誤送信耐性（受信者認証）	送信者認証	マルウェアチェック	デメリット
				送信から受信までの経路上で盗み見られることに対処してあること.	到達先のメールボックスをマルウェアが見ていても読み取れないようにすること.	意図した送付先以外は読み取れないようにすること.	受信者が，そのメッセージが誰から送信されたかが分かること.		
1	SMTPS の強制	SMTP MTA Strict Transport Security (MTA-STS) https://www.rfc-editor.org/info/rfc8461 DNS を用いてドメインが SMTPS を強制してるかどうかを宣言.		○ TLS による.	× 到達先安全性は守れない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	× 送信者認証は含まれない.	○	?
2	事前鍵交換共通鍵暗号化ファイル添付	A と B がファイルを交換するときに，あらかじめオフラインで共通鍵を交換しておいて，以後，その鍵でファイルを暗号化してメールに添付する.	本来の PPAP のあり方．鍵は十分に長くないといけない．鍵の管理と利用には 1Password のような企業モードがあり複数で鍵を共有できるパスワード管理ソフトを使うしかない.	△ 暗号化強度はパスワード強度に依存する.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	○ ファイルの暗号化と送信先の指定が合致しなければ読むことはできない.	○ パスワードが安全に管理されていれば送信者認証が可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	鍵をプロジェクトごとに覚えるのは困難.
3	公開鍵暗号化ファイル添付（PGP など）	A と B がそれぞれの公開鍵を一定の場所に公開しておき，その公開鍵を使ってファイルを暗号化してメールなどに添付する.	メール以外でも使える．キーサーバがスケールしない．受け取り手の端末にソフトがインストールされていないのがネック．エストニアでは全国民に当該ソフトを配布，国民 ID カードを使って処理できるようになっている.	○ 暗号強度は暗号方式に依存.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	○ ファイルの暗号化と送信先の指定が合致しなければ読むことはできない.	○ 送信者認証が可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	ソフトが普及していない.
4	公開鍵メッセージ暗号化（S/MIME）	PKI の個人証明書をベースに MUA で公開鍵で暗号化・署名する.		○ 暗号強度は暗号方式に依存.	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	○ 署名をつければ可能.	△ マルウェアチェックがゲートウェイでできない．エンドポイントでする必要あり.	エンドユーザが使えないと，サポートコストが上がってしまう.
5	DNS を使った ID ベース暗号	ID ベース暗号を用いた実用的電子メールシステムの設計と実装（2019-IOT-044）. http://id.nii.ac.jp/1001/00194748/	DNS が信頼できるのであればこれに頼った鍵配布ができるのではという考え方.	△ DNS になりすましの危険がある．ただし可能性は低い?	キーストアにマルウェアがアクセスできなければ，自動的に読まれることはない.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	○送信者認証が可能.	秘密鍵を送信側・受信側の MTA で管理する運用を想定．その場合 MTA でマルウェアチェックできる.	まだ標準化されていない.
7	認証連携ファイルアクセス制御	アクセスを許す相手の属性を指定して，当該ファイルへのアクセス制御を行う（ABAC）．そのファイルへのリンクをメールやチャットなどで送る.	現在のメインストリームになってきている．PPAP ソリューションには実はすでにオプションとしてあるものが多い.	○ TLS による.	サーバ上のファイルを自動で読まれることは，認証がしっかりしていればない．また，いつ誰によって読まれたかのログを取ることもできる．ダウンロード後は End Point Security のレベルによる.	△ アクセス制御がかかるため，誤送信しても読めないようにすることは可能.	△送信者が自ドメインでサーバを立てればある程度可能．リンクの送信にビジネスチャットなどを利用すれば可能.	マルウェア配布サイトかどうかは，URL のレピュテーションである程度管理可能．これに，エンドポイント検知を組み合わせる.	クラウド事業者のサーバを使うと，クラウド事業者の管理者や監督する国の政府にに読まれてしまうのではないかという心配がある.
8	クラウド暗号化ファイル共有	暗号化したファイルをクラウドに置き，それを解く鍵と URL を相手に送る．受信者が URL にアクセスすると，復号化されてダウンロードされる（例：Firefox Send）.	会社用に自分で Firefox Send を立てるのが，一番安全でよいのではないか.	○ TLS による.	× マルウェアがパスワード付きリンクを読めるとファイルも読めてしまう.	× 誤送信対策にはならないので，ほかの誤送信対策と組み合わせて使う.	△送信者が自ドメインでサーバを立てればある程度可能．リンクの送信にビジネスチャットなどを利用すれば可能.	マルウェア配布サイトかどうかは，URL のレピュテーションである程度管理可能．これに，エンドポイント検知を組み合わせる.	パスワード付きリンクを読めるとファイルも読めてしまう.
9	組織超えグループウェア	サイボウズ Live などを，他組織の人とも使う方式.	今なら Teams など.	○ TLS による.	適用される認証強度による.	△ 登録したユーザのみに送れる．ただし，間違った部屋に送ることはあり得る．その場合も削除可能.	○ 登録したユーザのみが使える.	エンドポイントで検知	グループウェアにおけるアカウント作成・招待が手間.
10	ビジネスチャットにおける添付ファイル	Slack や Teams など.		○ TLS による.	適用される認証強度による.	△ 登録したユーザのみに送れる．ただし，間違った部屋に送ることはあり得る．その場合も削除可能.	○ 登録したユーザのみが使える.	エンドポイントで検知	グループウェアにおけるアカウント作成・招待が手間.
11	業務システム	電子契約，ERP，CRM などを使う方式.	定型業務は，業務システムに寄せていく．社外とのやりとりは，本来は業務システムを通じて行うべきで，メールソフトのような End-User-Computing はやめるべき.	○ TLS による.	受信者のシステムによる.	○ 業務内容に応じて送信先が自動的に選ばれる.	△ 業務システムが利用するプロトコルによる．電子署名をつけるなどすれば，送信者認証は可能.	△業務システムが利用するプロトコルによる.	定型業務のシステム化が必要

ペた語義

Vol. 106

CONTENTS

【コラム】新型コロナウイルスと中高生情報学研究コンテスト…中山 泰一
【解説】教科「情報」・情報教育の担当者としてカリキュラム・マネジメントに参画する… 田﨑 丈晴
【解説】スリランカの初等中等情報教育… 和田 勉

COLUMN

新型コロナウイルスと中高生情報学研究コンテスト

本年（2020 年）3 月 7 日，本会第 82 回全国大会にて，第 2 回中高生情報学研究コンテストの審査を行いました．全国から 60 チームの参加があり，中高生研究賞の最優秀賞 1 チーム，優秀賞 2 チーム，奨励賞・情報処理教育委員会委員長賞 1 チーム，奨励賞・初等中等教育委員会委員長賞 1 チーム，奨励賞 10 チーム，入選 16 チームを選出しました．中学生の活躍が目覚ましく，最優秀賞は中学生，上位 15 チームのうち 6 チームが中学生でした．詳細は，中高生情報学研究コンテストのページ（https://www.ipsj.or.jp/event/event_chukousei.html）をご覧ください．

第 2 回中高生情報学研究コンテストは無事に実施されました．このコラムはその第一報です．コラムの執筆をお受けしたのは 2 月 16 日，本会会誌編集委員会と初等中等教育委員会の担当者間で打ち合わせして，今号で第一報を掲載し，次号（2020 年 8 月号）の特集「中高生の情報教育に関する支援活動―第 82 回全国大会を中心に―」につなげると決めたのでした．次号の特集もぜひご覧になってください．

2 月 16 日の打合せ時点で，第 82 回全国大会は金沢工業大学で開催，中高生情報学研究コンテストも同大学での開催で進めていました．ところが急転直下，翌 17 日には日本物理学会が新型コロナウイルス対策で同学会第 75 回年次大会の Jr. セッション中止を発表，本会でも中高生を金沢に集めていいのかという慎重意見が強くなります．

日々状況は悪くなっていき，2 月 20 日に本会全国大会運営委員会が緊急の会議を開催，翌 21 日に現地開催を中止してオンライン実施を進めると発表しました．第 82 回全国大会の一般セッションと学生セッションは Zoom を使って，前号（2020 年 6 月号）に掲載された「先生，質問です！」は cluster を使って，リアルタイムでの実施になりました．

中高生情報学研究コンテストでは，参加チームにポスター PDF と 400 字の説明テキストの提出を求め，それらを Web ページに掲載する方式にしました．本会の各種委員にそれぞれの研究へのコメントを寄せてもらい，そのコメントも掲載しました．講評と審査結果は YouTube の IPSJ チャンネルを使って配信しました．この方式にしたのは，Zoom などのリアルタイムの会議システムを使えない場合を心配してでしたが，2 月 27 日には内閣総理大臣の休校要請があり中高生は学校に行けなくなりましたから，適切な方式だったようです．

さて，私は本会初等中等教育委員会副委員長を 4 年間務め，2018 年度と 2019 年度は中高生情報学研究コンテストを担当しました．今年度，本会理事に選出していただきました．これからも本会の教育・人材育成の活動を推進していきたいと考えております．

中山泰一（本会教育担当理事／電気通信大学）

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

ARTICLE

基専

教科「情報」・情報教育の担当者として カリキュラム・マネジメントに参画する

田﨑丈晴
東京都中部学校経営支援センター経営支援室

高等学校学習指導要領（平成 30 年告示）は，平成 31 年度から移行期間となり，総則をはじめ，教科書等の対応を要しない場合など可能な範囲で取り組みを推進することとなりました．そのため，本稿は，すでに意欲的に取り組んでいる高等学校にとっては，次年度以降，さらに取り組みを充実させるための確認にとどまるかもしれません．今回の学習指導要領改訂により，教科「情報」の担当者が，学校の一員として，教育課程の編成・実施，そして，さらなる改善にかかわることがこれまで以上に求められています．「情報 I」の指導法や，これからの情報環境の構築，といった内容ももちろん大切なのですが，それらが学校の教育課程のどの部分に位置づけられるかなど，学校全体を見渡して考え行動することもまた，大切です．

現在私が担当している学校経営支援業務の 1 つに，所管する学校の教育課程の編成・実施・管理が適正に行われるための支援があります．令和 2 年度教育課程においては，コミュニケーション能力の育成の一環として情報活用能力の育成を学校の教育目標を達成するための基本方針に含めたり，教科「情報」の科目の設置においては，将来的に「情報 I」のみならず，「情報 II」の設置を見通して選択科目を設置するなど，新しい学習指導要領の完全実施に向け，少しずつ対応され始めていることを実感しています．

今後，各学校において，カリキュラム・マネジメントを推進し，新しい学習指導要領に基づく教科・科目の編成を検討するとき，教科「情報」もしくは情報教育を担当する先生方が，各学校でのカリキュラム・マネジメントに積極的に参画するには，という視点で紙面が許す限り整理しました．

学習指導要領（平成 30 年告示）の総則を確認する

高等学校学習指導要領（平成 30 年告示）[1] 第 1 章 総則　第 1 款 5 には，カリキュラム・マネジメントについて，以下の記載があります．

> 各学校においては，生徒や学校，地域の実態を適切に把握し，教育の目的や目標の実現に必要な教育の内容等を教科等横断的な視点で組み立てていくこと，教育課程の実施状況を評価してその改善を図っていくこと，教育課程の実施に必要な人的又は物的な体制を確保するとともにその改善を図っていくことなどを通して，教育課程に基づき組織的かつ計画的に各学校の教育活動の質の向上を図っていくこと（以下「カリキュラム・マネジメント」という．）に努めるものとする．

ここで，カリキュラム・マネジメントとは，教育課程に基づき組織的かつ計画的に各学校の教育活動の質の向上を図っていくことを指しています．所属している学校において，情報教育は教育課程においてどのような位置付けがなされているか，意図的計画的に情報教育が行われるようになっているかを理解しておくことは，カリキュラム・マネジメントに参画するための第 1 歩と言えます．そして，教育活動の質の向上のために必要と思う考えを整理する際，教育の目的や目標の実現に必要な教育の内容等を教科等横断的な視点で組み立

てる，という考えに立っているか，という点もあわせて検討し，工夫しながら教育課程の改善につなげることが求められています．

また，第 6 款の 1 のアには，

> 各学校において，校長の方針の下に，校務分掌に基づき教職員が適切に役割を果たしつつ，相互に連携しながら，各学校の特色を生かしたカリキュラム・マネジメントを行うよう努めるものとする．また，各学校が行う学校評価については，教育課程の編成，実施，改善が教育活動や学校運営の中核となることを踏まえ，カリキュラム・マネジメントと関連付けながら実施するよう留意するものとする．

と示されている通り，「校長の方針の下に」実施されることが重要です．情報教育にかかわる校務分掌，教科「情報」を含めた情報教育の推進役としての教科や情報教育の実施に関係する学年等，情報教育に関係する担当者が「校長の方針の下に」連携し役割を果たし，情報教育を推進することが求められます．

さて，情報教育の推進について，第 2 款 2 (1) には，以下の記載があります．

> 各学校においては，生徒の発達の段階を考慮し，言語能力，情報活用能力（情報モラルを含む），問題発見・解決能力等の学習の基盤となる資質・能力を育成していくことができるよう，各教科・科目等の特質を生かし，教科等横断的な視点から教育課程の編成を図るものとする．

ここから，情報活用能力 (情報モラルを含む) は，学習の基盤となる資質・能力の 1 つとして位置づけられていること，また，各教科・科目等の特質を生かし，教科等横断的な視点から，と示されていますので，教科「情報」の指導だけではなく，学校全体でさまざまな教科等で相互に関連させながら育成できるよう計画し，教育課程を編成することが求められています．そのためには，情報活用能力について，教科「情報」や情報教育を担当する先生だけではなく，学校全体で共有することが必要になります．

情報活用能力については，平成 28 年 12 月の中央教育審議会答申 [2] において，

> 情報活用能力は，世の中の様々な事象を情報とその結び付きとして捉え，情報及び情報技術を適切かつ効果的に活用して，問題を発見・解決したり自分の考えを形成したりしていくために必要な資質・能力である．

とし，さらに，同答申の別紙 3-1 において，資質・能力の 3 つの柱に沿って再整理されました．高等学校学習指導要領 (平成 30 年告示) 解説総則編 [3] では，この情報活用能力についての考え方を改めて示し，さらに，

> 情報活用能力をより具体的に捉えれば，学習活動において必要に応じてコンピュータ等の情報手段を適切に用いて情報を得たり，情報を整理・比較したり，得られた情報をわかりやすく発信・伝達したり，必要に応じて保存・共有したりといったことができる力であり，更に，このような学習活動を遂行する上で必要となる情報手段の基本的な操作の習得や，プログラミング的思考，情報モラル，情報セキュリティ，統計等に関する資質・能力等も含むものである．

と，具体的に示しました．この，学習の基盤となる資質・能力としての情報活用能力を学校として身につけさせるため，教科「情報」だけではなく，教科「情報」以外の教科や総合的な探究の時間等の学習活動を通して，教科等横断的に身につけさせるためにカリキュラム・マネジメントを行い，具体的に指導計画を立て，実行することが求められています．

カリキュラム・マネジメントに参画する

教科「情報」や，教科「情報」以外の教科や総合的な探究の時間等の学習活動を通して，教科等横断的に情報活用能力を身につけさせるための具体的な指導計画を立てる役割については，学校により異なります．探究活動の指導計画を立てる校務分掌や委員会等があるかもしれませんし，各教科の主任で構成する会議があてはまる組織かもしれませんし，教務を担当する校務分掌がまとめているかもしれません．また，担当者の立場なのか，担当ではなく連携する

立場なのかによってもかかわり方が異なりますが，学校において，誰が担当しているのかを知り，自らの立場で何ができるか考え行動することが，カリキュラム・マネジメントにおいては重要です．

教科等による指導，という点では，学習指導要領（平成 30 年度）解説総則編[3]によれば，各学科に共通する教科「情報」（共通教科情報科）は，情報活用能力の育成の中核を担うものという位置付けとして記載されています．このことから，学校ごとの実情に即して設定されている教育目標や，学校として身につけさせたい力等を踏まえ，共通教科情報科における必履修科目で育成する情報活用能力について検討する際，それは，学校における情報活用能力の育成の中核を担う想定で検討したほうがよいと言えます．しかしそれは，共通教科情報科がすべてを担うということではありません．共通教科情報科ではどのようなことを学ぶかを校内で共有し，連携する立場の関連する教科や総合的な探究の時間等における指導において，共通教科情報科で学んだことをどのように定着させ，また発展させることで，情報活用能力を確実に身につけさせるのか整理し，実行するということです．

すでに，共通教科情報科以外の科目で情報活用能力の育成に資する指導が行われていますから，まずは，どの科目で，どのような内容で行われているのかを把握し，共通教科情報科や，関連する教科等の指導内容を見直したり調整したりしつつカリキュラムとして整えるほうが現実的かもしれません．

このことについて考えやすくするために，筆者は，2017 年度から 3 年間非常勤講師として大学で担当した「情報科教育法」の教材として「資質・能力から年間指導計画を構想するシート」（図 -1）を作成し，活用しました．授業では，総合的な探究の時間の時間で，図に示すような計画で探究活動が行われるとした場合，共通教科情報科の科目（シートでは教科書等を用いた授業研究を行う関係で，「情報の科学」を指定）を担当する教員として，何月頃に，どのような力を身につけさせる指導を行うか，学校の教育目標や，育成したい資質・能力も念頭に入れつつ考え，図に書き込みながら整理するワークを行いました．この大学では，高等学校の情報の教員免許のほかに，中学校と高等学校の数学の教員免許を取得することができましたので，数学との関連についても考えてよいことにしました．学生は苦労していましたが，検討の流れの例は次のようになります．総合的な探究の時間で，6 月から 8 月の期間で情報収集を行うことが予定されているとき，共通教科情報科の担当者として，情報の授業で学んだことを活かして総合的な探究の時間での学びを充実させるためにはどうしたらよいか，ということから検討をはじめます．そして，共通教科情報科の授業で，情報やメディアの特性を踏まえ，情報と情報技術を活用できるようにする授業を，何月頃に実施したらよいか，6 月より前にして，情報の授業で体験したことを思い出しながら取り組めるようにするか，総合的な探究の時間と同じ 6 月からで設定し，情報の授業で学んだことをすぐに活用できるようにするか，どちらが効果的か，と，少しずつ具体的に検討を進めます．そして，身につけさせたい力をどのような学習活動を通して，どの単元で扱う

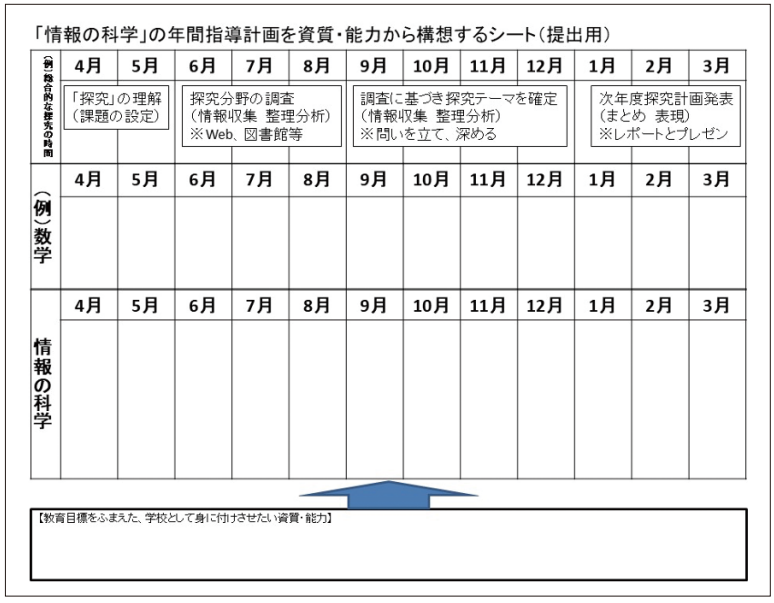


図 -1　共通教科情報科の年間指導計画を資質・能力から構想するシート

のか，ということを考えながら年間指導計画に対応させ，年間指導計画を仕上げていきます．このように資質・能力の育成と科目での指導項目とを連動させながら年間指導計画を考えることは学生にとっては大変だったと思いますが，中には数学の授業と情報の授業でクロス・カリキュラムを考える学生もおり，教科等横断的な視点を取り入れて年間指導計画を考えさせることができました．

実際に学校では，学年は1年生から3年生までであり，教科等は，総合的な探究の時間や数学や情報だけではありませんので，図-1の表を，3学年，すべての教科等に拡張して，共通教科情報科の学びとの関連を確認することは，学校全体でカリキュラム・マネジメントを進める上で有効です．

そもそも図-1では，何年生での1年間（の一部分）を指しているのかは，明らかになっていません．筆者は大学の授業では，1年生の一部分である，という設定で授業を行いました．

1年生であれば，中学校で身につけたことを念頭に置きつつ，共通教科情報科の科目を，高校生が学習の基盤としての資質・能力に位置付けられる情報活用能力の基礎をしっかり身につける中核として位置付けることは容易です．共通教科情報科において，十分な指導が行われることにより，生徒たちが1年生で身につけた情報活用能力を，2年生以降，共通教科情報科の選択科目「情報II」を含め，探究的な学びが本格的に展開される他教科の科目や総合的な探究の時間等で活かされるようつなげることができます．

2年生の場合，1年生で情報活用能力を身につけさせる役割をどの科目等が担うのか，2年生に設置された共通教科情報科の必履修科目が，情報活用能力を身につけさせるための中核としての役割を果たして担えるのか，2年生で本格的に探究活動が展開される他教科の科目や総合的な探究の時間等の履修が，共通教科情報科の履修と並行することになり，情報活用能力を確実に身につけさせる上で効果的か，などの検討課題が考えられます．3年間を通した情報活用能力の育成という視点で十分な検討が必要です．

新しい学習指導要領では，共通教科情報科は，「情報I」と「情報II」の科目構成となり，「情報II」では，新しい学習指導要領において，「情報Ⅰ」および「情報II」で身につけた資質・能力を総合的に活用し，情報活用能力を活用して問題の発見・解決する活動を通して，新たな価値の創造を目指し，情報と情報技術を適切かつ効果的に活用する資質・能力を高めるよう指導することなどが求められています．「情報I」「情報II」という，順序性がある科目編成となったことにより，教科指導の系統性を考慮した教育課程の編成が可能となりました．「情報II」の設置について，情報活用能力をさらに効果的に身につけさせる選択科目として，また，教科指導の系統性を考慮に入れ教育課程を編成するという視点で検討する良い機会です．

生徒が入学してから卒業するまでに，情報活用能力を確実に身につけさせるために，生徒はどの段階でどのようなことを学ぶのかを考え整理しつつ，学校としての指導計画を組織的に検討して，新しい学習指導要領に基づく教育課程を編成することは，ゴールではありません．カリキュラム・マネジメントは，改善を繰り返しながら，教育活動の質の向上を図る取り組みです．教科「情報」や情報教育を担当する先生方が，学習の基盤としての資質・能力の1つである情報活用能力の育成を通して，教育活動の質の向上に貢献できる機会を十分活かすことが，今後ますます期待されます．

参考文献

1) 高等学校学習指導要領（平成30年告示），pp.19-32.
2) 幼稚園，小学校，中学校，高等学校および特別支援学校の学習指導要領等の改善および必要な方策等について（答申）（平成28年12月，中教審第197号），p.37，別紙3-1.
3) 高等学校学習指導要領（平成30年告示）解説総則編，pp.54-56，pp.266-269.

（2020年4月7日受付）

田﨑丈晴（正会員） take@tasaki-data.info

2003年から私立学校教員，2005年から東京都公立学校で教諭，主任教諭，主幹教諭として教科「情報」を担当する．2015年東京都西部学校経営支援センター支所　学校経営支援主事，2018年から東京都中部学校経営支援センター経営支援室　学校経営支援主事．

ARTICLE

スリランカの初等中等情報教育

和田　勉
長野大学

スリランカ訪問から（続）

2018 年 3 月，辰己丈夫先生（放送大学）と筆者，およびこのとき筆者が指導していた同国出身の留学生とでスリランカ（スリランカ民主社会主義共和国：旧名セイロン）を訪問し，政府の教育省（Ministry of Education）（図 -1）およびいくつかの大学および初等中等教育機関を訪問した．このうち，いくつかの学校への訪問を中心とした報告はすでに記した [1]．本稿はその続編であり，教育省に訪問して同省の担当者にインタビューしたことを中心に，University of Sri Jayawardenepura において同大学の先生方からお聞きしたことを交え，同国の情報教育を中心として，筆者が理解したところを記す．なお文献 1)，2) に述べたことは重ねて述べないので，これらをあわせてお読みいただきたい．

図 -1　スリランカ政府教育省

スリランカの情報教育と試験の制度 [3]，[4]

スリランカの初等中等教育での学年は Grade1 から始まる通し番号で呼ばれ，以下の学校種に区分けされている（表 -1）．

Junior Secondary から Collegiate までが中等教育（Secondary）であり，大学（University）へはそれを終えて進学する．義務教育は Junior Secondary までであるが，Senior Secondary までは学ぶことが教育省により強く勧められている [4]（文献 4）では「GCE O/L（Ordinary Level：後述）までは」と記されている）．

日本の初等中等教育の制度では，まず学習指導要領があり，それに則っての学校教育があり，それに則る形で高校入試や大学入試の制度・試験内容が設定されている．それに対して同国では逆に，まず，Grade を進むにつれて受ける試験の枠組みがあり，それに対応するように教育課程の枠組みと内容が規定されているようである．同国の教育の枠組み全体は英国と共通点が多く，これはスリランカが以

表 -1　学校種およびそれぞれに含まれる Grade と年齢

学校種	含まれる Grade の範囲	各 Grade の児童生徒の年齢
Primary	Grade 1 ～ Grade 5	5-6 才 ～ 9-10 才
Junior Secondary	Grade 6 ～ Grade 9	10-11 才 ～ 13-14 才
Senior Secondary	Grade 10 ～ Grade 11	14-15 才 ～ 15-16 才
Collegiate	Grade 12 ～ Grade 13	16-18 才 ～ 17-19 才

前は英領セイロンでありまた現在もイギリス連邦（Commonwealth of Nations）の一員であるなど，歴史的に英国との関係が深いことが関係していると思われる[4), 5)]．

教育省およびUniversity of Sri Jayewardenepuraでのインタビューの際に各学校種における教育制度をいろいろ質問したが，日本のように「小学校段階では何々を教えており，中学校段階では何々を……」という答えはなかなか得られず，得られたのは「各試験（後述）のこれこれに対応した科目としてはこれこれがある」という回答ばかりだった（図-2，図-3）．

児童生徒は，学年を進むにしたがって以下の情報分野に関する試験を受ける[4)]：

- Senior SecondaryのGrade 10または11にはGCE（General Certificate of Education，一般教育修了証明）のO/L（Ordinary Level，普通段階）の試験がある．いくつかの科目から選択して受験するようになっているが，この中にいくつかの教科の内容が合わさったBasket Subjectの試験があり，この中に情報（IT）分野が含まれている．
- またGrade 12にはGIT（General IT）の試験があり，これは当該年度の生徒全員が受けるものである．GITとは，生徒がその専門分野にかかわらず皆受ける試験であり，専門的な深い内容のものとは区別されている．
- さらにGrade12または13にはA/L（Advanced Level，上級段階）の試験もある．A/L試験は多くの科目から選択して受験するようになっており，その中に情報関係の科目が2科目ある．

初等中等教育の学校は，学校種ごとに独立して設置されているのではなく，小学校相当から高等学校あるいは短期大学相当の学年までが1つのまとまった学校として設置されている．初等中等教育の学校は以下の3タイプに分かれる[3)]．

- Type1AB　Grade1から13までが設置されている学校（1A，1Bでなく1ABと呼ばれる．）
- Type1C　1ABと同様だがA/Lの科学分野は扱っていない学校
- Type2　Grade1から11まで，または6から11までが設置されている学校
- Type3　Grade1から5までが設置されている学校

これらをあわせ，全土で約10,000校の学校があるが，そのうちの約4,000校で情報（IT）の授業を必修として行っている．

A/L試験に対応して，すべての分野をあわせ，シンハラ語で53，タミル語で53，英語で10～12の授業が設けられ，生徒はそのうち3つを選択する．そのうちの情報（IT）の授業は，科学系（Science stream），芸術系（Art stream），共通系（Common stream），技術系（Technology stream），およびさまざまな分野から選択できる共通カリキュラム（Common curriculum）に分けられる．

図-2　University of Sri Jayewardenepura

図-3　University of Sri Jayewardenepuraの先生方へのインタビュー，手前は筆者らと同行した同国出身の留学生

大学（University）進学を希望する生徒はこれらを学んだ上で A/L 試験を受験する．大学に進む生徒のうち約 20％が情報分野専門の学部学科に進学する．

教員養成・教師教育

初等中等教員の資格として，我が国の教員免許に相当するような，統一された制度はないようで，教員養成は 17 カ所の教育機関で行われている．教員の研修は，NIE（National Institute of Education, 国立教育研究所）が中心になって行われており，それ以外にもいくつかの機関で行われている．

教育事情雑感

ここでは，インタビュー中に聞きだした印象深いことに関して順不同に述べる．

教育省でのインタビューで，日本では常に問題となる以下のことを問いかけてみた：
「日本では初等中等教育に関し『自分は（うちの子は）将来情報技術の職業に就くつもりはない．それなのになぜ情報分野を学ばなければいけないのか』という声が多く困っている．貴国ではどうか？」

返ってきた答えは「初等中等教育では情報分野のうち一般的（general）なことを学ばせているのでそういう問題はない．職業教育は中等教育のあとで（それを専門として選ぶ者だけに）教えている．これは良い方法だ」であった．国情がまったく違い，日本でこのような声が上がること自体，よく理解できないようだった．

同国での情報教育に関する問題は，上記のようなことではなく，多くの学校（特に都市部以外）で情報機器やネット設備の整備が不十分であることとのことであった．前述の，約 10,000 校の初等中等教育学校のうち約 6,000 校で情報分野の授業が行われていないのは，設備面の事情から実施が困難なためであり，行われている 4,000 校の中でも高速インターネット接続（ADSL や光接続）があるのは約 2,500 校とのことだった．情報教育に関する苦情といえばまずはこの設備面（それにより情報教育が行えていないこと）に関することであり，政府はなによりもこの設備面での改良を目指しているとのことであった．

教育省でのインタビューでは，以下のことも聞いてみた：

「貴国では，高度な情報技術を身につけてプログラマや IT エンジニアになれば，社会的に尊敬され高収入も得られる，と想像するが，これは正しいか？」

答えは明確に「そのとおり」であった．スリランカに限らず，過去に筆者が訪れたいくつかの国，特に先進国とは呼ばれていない国では，すべて共通してこれが「そのとおり」であった．というよりむしろ，それらの国ではこんなことは議論するまでもなく当然のこととして，教える側だけでなく学ぶ多くの児

図 -4　小中高等学校（女子校）Vishaka Balika Vidyalaya，Sapugaskanda，文献 1）参照

童生徒学生も当たり前に認識しており，だからこそ努力して学んでいる．問題はそんなことではなく，それに向かうための手段すなわち設備であったり教育体制の問題であったり，である．

情報教育に限らないのだろうが，スリランカに限らず過去に見学などで訪れた諸外国に関する知識から，振り返って我が国を見ると，何かが根本的に異なる．多くの学生・生徒が「学びたい，それによりより「上」を目指したい」と考えている・それが当然である国々と比較して，我が国は，学ぶことに意味を見出していない学生・生徒が多く，教える側・その枠組みを用意する側が「学びたくないのになぜ強制するのか？」という苦情に日常的に相対するまるで次元の異なる世界になっていることを繰り返し感ずる．

図 -5　最大都市 Colombo の風景

図 -6　首都 Sri Jayawardenepura Kotte のレストラン

❑ スリランカの街中

訪問で見た街中を写真 3 枚で紹介する．最大都市は Colombo だが首都は Sri Jayawardenepura Kotte である．といっても Colombo との間は市街が連続している（図 -5，図 -6）．図 -5 に見える特異なデザインの高層ビルや塔（Lotus Tower）は訪問時はまだ建築中であった．図 -7 は街中にたくさん走っている三輪タクシーで，タイのトゥクトゥクなどと似ているがスリランカでは Three-Wheeler などと呼ばれる．

参考文献

1) 和田　勉：スリランカの学校訪問記，情報処理，Vol.61, No.4, pp.393-396 (Apr. 2020).
2) エディリシンハチャトリカ，和田　勉：スリランカの初等中等・一般情報教育と情報入試・検定，情報処理学会 コンピュータと教育研究会 144 回研究発表会, 2018（平成 30）年 3 月 17 日（土）, Vol.2018-CE-144 No.13, pp.1-5.
3) Ministry of Education – Sri Lanka “School Census Report – 2017, http://www.statistics.gov.lk/education/School%20Census%20Report_2017.pdf
4) Wikipedia 英語版：Education in Sri Lanka，2020 年 3 月 30 日閲覧.
5) Wikipedia 日本語版：イギリス連邦，2020 年 4 月 30 日閲覧.

（2020 年 4 月 6 日受付）

和田　勉（正会員） wadaben@acm.org

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

図 -7　三輪タクシー

最初に考えること：何を行うのか

真鍋義文 | 工学院大学

アルゴリズムとは

この連載は，アルゴリズムをまったく知らない人がアルゴリズムを学ぶことを目的としています．皆さんはアルゴリズムという言葉を聞いたことがありますか？　聞いたことがない人も，スマホにアプリをダウンロードして使ったことがある人は多いでしょう．アプリは，皆さんが行いたい作業（チャット，ゲーム，その他いろいろありますね）を行ってくれるものです．そこには，必ずアルゴリズムが使われています．

スマホのアプリはプログラムの一種です．そこで，アルゴリズムの前にプログラムの説明をします．スマホやパソコンの中にはCPU（シーピーユー）（中央処理装置）が入っています．これは主な処理を行う，人でいえば脳にあたる部分です．スマホのチャットであれば，画面のどのあたりをタッチしたかというデータから送信メッセージを作ったり，受信したデータを文字に変えて画面に表示したりする処理を行うのがCPUです．CPUは足し算やかけ算など，さまざまな計算を行うことができますが，チャットなどの複雑な作業を行うにはそれらの単純な計算を組み合わせて実行する必要があります．チャットの作業を行うために足し算やかけ算などをどのような順序で実行すればいいかをCPUは知らないため，そのやり方をCPUに教える必要があります．このやり方を示した手順書がチャットのプログラムです．人がプログラムの形で手順を書き，その手順に従ってCPUが処理をすることで，目的の作業（たとえばチャットやゲームなど）を行うことができます．

しかし，目的の作業を行うやり方は1通りとは限りません．たとえば道が碁盤の目のようになっている京都や札幌の町で北西に行くときには，まず北に進んで次に西に進む，まず西に進んで次に北に進む，という2つのやり方が考えられます．

プログラムの場合も，1つの作業をするやり方はいく通りも考えられます．このやり方のことをアルゴリズムと呼びます．プログラムを行った結果のよしあしは，アルゴリズムのよしあしに大きく左右されます．この連載では，良いアルゴリズムとはどのようなもので，どのようにして良いアルゴリズムを得るか，について説明します．

アルゴリズムを考えるときには，まず「何を行うのか」という作業の目標を決める必要があります．目標があいまいであっては，やり方も決められません．この第0回目では「何を行うのか」という目標設定について例を挙げて説明をします．

ケーキ分割問題

目標設定の例として，ケーキ分割問題を考えます．図-1の細長いケーキを2人で分けます．この場合，目標はどうなるでしょうか？　もちろん，2人の取り分が同じになるように分けられればベストです．ケーキではなくようかんであれば，大きさが同じになるように2つに分けることは簡単にできて，それでいいでしょう．しかし，図-1のケーキは右端にだけイチゴが多いので，大きさが同じになるように

2つに分けてもそれらは同じにはなりません．のっているイチゴやキウイを1つ1つ取り出して2つに分ければよい，という人もいるかもしれませんが，数が多いとたいへんです．同じにすることはあきらめざるを得ない場合も多いでしょう．

さらにやっかいな話として，人によって好みが違うことがあります．イチゴが大好きな人や，フルーツの種類にこだわりのない人もいるでしょう．人の好みも考えたいです．

そこで，目標を「2人の取り分が同じになるように分ける」ではなく，「2人とも満足するように分ける」ことにします．満足していることを，どのように目標としてきちんと表すことができるでしょうか？

満足していることを，2人とも「自分の取り分の価値は，相手の取り分の価値以上である（自分の好みの尺度で見て，同じか，自分の取り分の方が良い）」と感じていること，と表すことが考えられています（図-2）．太郎さんと花子さんの2人で分けたとき，図-2では左側を太郎さん，右側を花子さんがもらっています．太郎さんは自分がもらった左側の方が右側と同じか，より価値が高いと考えています．花子さんは自分がもらった右側の方が左側と同じか，より価値が高いと考えています．このとき，相手の取り分を見て「あっちの方がいい」とうらやむことがないので，分け方に2人とも不満がありません．これを，うらやむことがない，という意味で無羨望（むせんぼう）と呼びます．

図-1　右端にイチゴが多い細長いケーキ

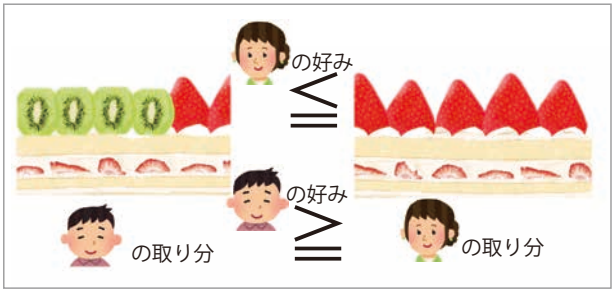


図-2　無羨望

目標を「無羨望になるように分けること」と決めましょう．では，無羨望な分け方はどんなアルゴリズムで求められるでしょうか？　ただし，ここでは2人とも相手の好みは分からないものとします．

2人の無羨望アルゴリズム

AとBの2人で分けるときは以下のアルゴリズムが考えられています．

1. Aがケーキを自分の好みで価値の等しい2つに切り分ける
2. Bが2つのうち好きな方を選ぶ
3. Aが残った方をもらう

この分け方が無羨望であることを説明します．まず，Bはステップ2で2つのうち自分にとって良い方を選べば残ったAの取り分の価値以上のものをもらうことができます．また，Aにとって2つの価値は同じなので，Bがどちらを選んでも，自分の取り分はBの取り分の価値と同じとなります．

もし，Aがステップ1で手順に従わずに2つの価値が違うように切り分けた場合には価値が高い方をBに取られるかもしれません．Bの好みを知らないAがこれを避けるためには，手順の通りに2つの価値を等しくしなければいけません．

3人で分ける場合の無羨望なアルゴリズムはたとえば文献1）に，4人以上で分ける場合の無羨望なアルゴリズムは文献2）にあります．

無羨望アルゴリズムの問題点

無羨望という目標を満足するアルゴリズムが見つかったので，一見これで良いように思えますが，実はこのアルゴリズムには問題点があります．このアルゴリズムではAとBとで行う手順が違うため，誰にどちらの役目をしてもらうかを決めないといけません．ところがこのアルゴリズムは，Bに有利なものとなっています．最初に2つに切り分けるAは，2つの価値が同じになるように切るので全体の価値の半分の価値をもらいますが，Bの好みがAの好みと違うときには，Aがもらったケーキは全体の価値の半分を超える価値となることがあります．

このことを確かめるため，図-1のケーキで，イチゴが大好きな花子さんとフルーツにこだわりのない太郎さんでこのアルゴリズムを行ってみましょう．花子さんがAの役目を行うとしたら，花子さんはケーキを大きさで半分にするのではなく，左側を大きくするでしょう（図-3）．イチゴがもらえないのだとしたら，その分，ケーキを多くもらう，というのが花子さんにとって価値が同じになる分け方になります．この2切れを見た太郎さんは左側を選んで，半分より大きな価値をもらいます．

太郎さんがAの役目を行うとしたら，太郎さんはケーキを大きさが同じになるように切り分けるでしょう（図-4）．この2切れを見た花子さんは，右側を選んでイチゴが多くのっている分だけ半分より大きな価値をもらいます．

このことを知っていたら，このアルゴリズムを行うときに2人ともBの役目をやりたがります．仕方がないのでじゃんけんで役目を決めると，じゃんけんに負けてAの役目になった人は勝ってBの役目になった人をうらやむことになります．

じゃんけんは公平な決め方なのでこれでいい，という人もいるかもしれません．しかしじゃんけんで決めていいのであれば，「じゃんけんで勝った方がケーキを全部もらう」というアルゴリズムでもかまわない，ということになってしまいます．じゃんけんで価値の違うものを割り当てることはうらやむことが起きる良くないやり方です．

うらやむことがない無羨望のアルゴリズムのはずなのに，相手をうらやむという変なことになってしまいました．何がいけなかったのでしょう？

それは，目標を無羨望としたことにあります．無羨望だけを目標としては，ほんとうに公平な分け方はできません．アルゴリズムの中での役目についての羨望（うらやむこと）がない，ということも目標に入れることが必要です．AとBでアルゴリズムを行うときにAの役目をする人がBの役目をする人をうらやむことがなくて，Bの役目をする人が

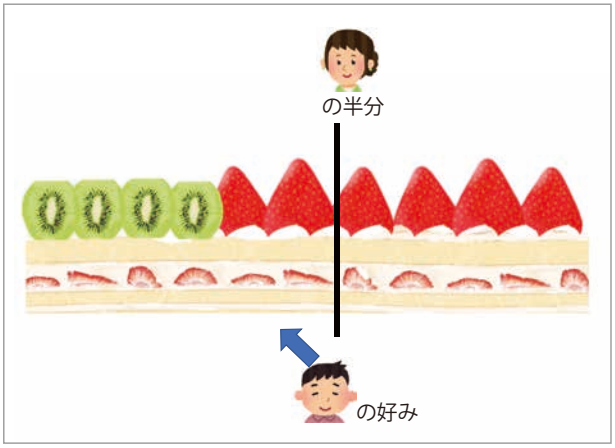


図-3　花子さんが半分に切る場合

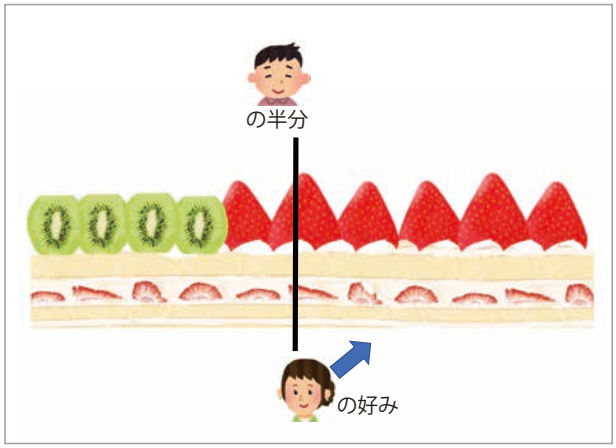


図-4　太郎さんが半分に切る場合

Aの役目をする人をうらやむこともない，ということが必要になります[3]．

役目の羨望がないアルゴリズム

そこで，目標を「役目についての羨望がなく，分け方は無羨望となる」に変えます．この新しい目標を達成するアルゴリズムの例は，以下のようになります．

1. AとBが，自分の好みで価値が半分になる場所を同時に示す
2. 2人が示した場所が同じならば，その場所で切ってくじびきでどちらにするかを決める
3. そうでないときは，2人が示した場所の真ん中で切って，それぞれが示した場所を含む方をもらう（図-5）

図-5の例では，太郎さんの示した場所は，花子さんが示した場所より左側にあるので，太郎さんは真ん中の点線で切ったうちの左側を，花子さんは右側をもらいます．もしも太郎さんの示した場所が花子さんが示した場所よりも右側になった場合には，太郎さんが右側をもらいます．

このアルゴリズムの正しさは以下の通りです．

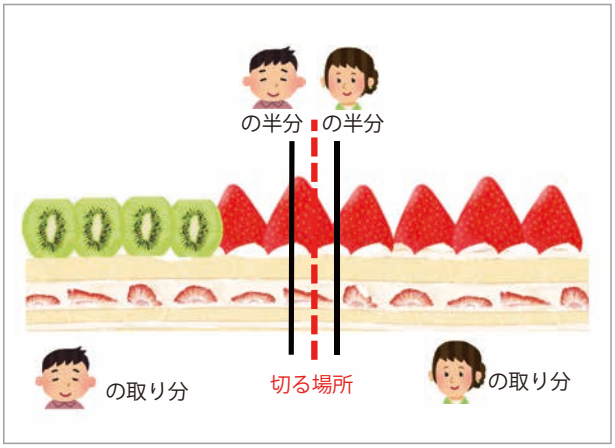


図-5　役目の羨望もないアルゴリズム

(1) 2人が示した場所が同じならば，この場所で切った2切れはAにとってもBにとってもちょうど半分の価値になります．ですから，くじびきの結果左右どちらをもらうことになっても無羨望です．
(2) 2人が示した場所が違うときには，AもBも自分の好みで半分よりも多くもらっていることになります．相手の取り分は半分より少ない，と思うので無羨望です．

また，このアルゴリズムではAとBが行うことはまったく同じなので，役目について他の人をうらやむことはありません．このアルゴリズムは「役目についての羨望がなく，分け方は無羨望となる」という目標を満たしています．

目標設定の大切さ

ケーキ分割問題を例に，目標設定がまずいと良くない結果となることと，目標設定が違うとアルゴリズムも違ってくることを示しました．

アルゴリズムを考える場合には，まず最初に目標は何か，それは本当に正しい目標なのか，ということをよく考えることが必要です．

参考文献

1) 伊藤大雄：パズル・ゲームで楽しむ数学，森北出版，pp.34-35 (2010).
2) Aziz, H. and Mackenzie, S. : A Discrete and Bounded Envy-free Cake Cutting Protocol for Any Number of Agents, Proc. of IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS), pp.416-427 (2016).
3) Manabe, Y. and Okamoto, T. : Meta-envy-free Cake-cutting and Pie-cutting Protocols, Journal of Information Processing, Vol.20, No.3, pp.686-693 (2012).

（2020年3月30日受付）

真鍋義文（正会員）　manabe@cc.kogakuin.ac.jp

工学院大学情報学部システム数理学科教授．1985年大阪大学大学院基礎工学研究科修士課程修了．同年日本電信電話（株），2013年から工学院大学．分散アルゴリズム，暗号理論などに興味を持つ．博士（工学）．

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

小学校における ICT 活用の試行錯誤
―教員によるソフトウェア開発を通して―

鍋谷正尉　渋谷区立千駄谷小学校

小学校の ICT 環境の中で，授業の準備に最も大きな影響を及ぼすのはソフトウェアではないだろうか．ハードウェアやネットワークの整備が十分であっても，そこで利用できるソフトウェアやサービスの整備状況によって，そのポテンシャルを活かせるかどうかは変わってくる．現場教員として，その点に最も注目して活動してきた結果，教員自身によるソフトウェア開発に行き着いた．以下では，小学校の ICT 環境の変遷について概観したあと，自分のツール開発について説明していく．

小学校の ICT 環境の変遷

1990 年代

1990 年代の小学校は，1 校に数台のパソコンしか設置されていなかったが，1990 年代後半になると，インターネットに接続する学校が増えてきた．当時勤務していた学校では，インターネットを使うときに学校の電話回線で接続していた．それらの活用は，熱心な教員のもとで行われており，全体への広がりはまだまだであった．その後，パソコン室が整備され，端末は数十台になっていく．パソコン室では既存の授業支援用ソフトウェアのほかに，教員が開発したソフトウェアを使う活動が試みられていた．

2000 年代

情報発信の手段として，学校が Web ページを開き始めた．児童による情報発信の手段としても意識されて授業での活用が始められた．また授業で使う ICT 機器として電子黒板が登場した．授業では，教室前方の電子黒板を全員で見るような活用がよく見られた．そのためディジタル掛図のようなソフトウェアが増えていった．プレゼンテーションソフトウェアや HTML によって提示資料を作成する教員が多く見られるようになった．中には Visual Basic や Flash でソフトウェアを開発する教員も現れ，その周辺の

教員による活用も試みられるようになってきた．

2010 年代

児童が使うデバイスとしてのタブレットは，授業の方法にこれまでとは異なる選択肢をもたらした（図 -1）．それまで一般的だった，情報を得たり作品を作ったりする活動に加えて，情報のやりとりを行う活動が登場した．そして，私の勤務校において児童に 1 人 1 台のタブレットが整備された．

2020 年代・これから

ついに文部科学省の GIGA スクールプロジェクトにより，1 人 1 台を前提とした ICT 環境の整備が一気に進もうとしている．そして今，社会はコロナウイルスへの対応に全力を注いでいる中で，多くのことを人の移動なしに，ICT を通じて実施しようとする方向にある．学校においては，これまでの活用の経験を活かすチャンスである．それとともに，教員が ICT 活用の可能性を広く認識し，望ましい ICT 環境がどのようなものであるべきか考える機会となっている．今後の実践に大きな影響が期待される．

教員によるツールの開発

開発のきっかけ

時代によって活用するツールは大きく変わってきた．時代にあった教材を提供したいという思いから，その時々の環境を最大限活かせるような活用を試みてきた．しかし，いざ教員がディジタル教材を活用した授業を実践しようとすると，思っていたことを実現できない場合が少なくない．たとえば，ソフトウェアの仕様でやりたいことが実現できない，機能が多すぎて使い方を習得できない，実現するための手間が多すぎる，中途半端な契約のため使いたいソフトウェア・サービスが使えない，などで，一教員の立場では解決できない問題ばかりであった．そして，最も危惧されたのは，取り組もうとした教員がこれらの問題によって ICT の活用から離れてしまうことであった．

■図 -1　シェアオピを使用した授業の様子

これらのことから，ツールに対する教員の学習コストを押さえるために，必要最低限の機能だけを実装したシンプルなツールを開発することにした．

開発環境とツールの変遷

1990 年代は HTML による提示教材や Flash による動画教材，操作を伴う教材を作成していた．また Visual Basic による Windows 向けのソフトウェアも開発してきた．しかし，これらは大きな課題を抱えていた．それは OS の壁である．OS の世代が変わるごとに使えなくなるケースが出てきたことから，2000 年代半ば以降はマルチプラットホームに出力できることを重視してツールを選択している．具体的には HTML5/CSS3/JS を中心に，Unity などのツールがこれにあたる．これらは一度開発すると，ほとんどの OS 上で使えるように出力することができる．

シェアオピの開発

小学校の担任は全教科を指導することから，さまざまな教科での活用を視野に，意見交換や思考の整理を行うためのシンプルなツールが必要であると感じていた．そこで，テキストや画像をカードとして投稿しグループ全体で共有することと，それを整理しながら動かすという機能を実装したツールを開発

することにした．意見（Opinion）を共有（Share）することからシェアオピと名付けた．図 -2 は，シェアオピを用いて，クラスの児童たちが提出した意見を集めて表示している様子である．

現在の勤務校は１人１台のタブレットが整備されているため，児童には授業でのタブレット活用の経験が積み重なっている．まずは児童の様子を観察したり，意見を聞いたりした結果に基づき，ツールの設計について，次のように考察した．「使いやすいツールとは，すぐに使えるもの，軽快に動くもの，同じ操作は同じ結果になるもの」．

そこで機能を絞り，モードのないシンプルな操作体系のものを，Web ベースで作ることにした．

まず，テキストをカードとして投稿する機能とそのカードをドラッグで動かす機能の２つだけを実装して，実際の授業で使ってみた．児童は簡単な解説を聞いた後，使いながらすぐに操作を習得することができた．そのあと１カ月ほど，授業で試用してみたところ，学習活動に必要な機能について多くの声が得られた．たとえば「カードに色をつけられないですか？　つけると種類ごとに分かりやすくできると思う」「写真を入れられると便利です．説明がしやすくなります」「カードが増えると見にくいから，大きさを調整できるといいな」といった声である．その中からいくつかを追加して，シェアオピの開発に区切りをつけた．

■図 -2　シェアオピの使用例

授業への効果は明らかであった．児童が意見を表す機会が増え，その手段としての ICT 活用の頻度が上がったのである．また投稿はシェアオピに記録されていることから，児童自身のニーズに応じて振り返りをするようになった．このような児童主体の活動が多く見られるようになった．シェアオピの使い始めには説明等の時間や手間がかからないので，すぐに学習活動に入れるようになり，ICT 活用の利点を実感する機会が増えた．そして，児童は自発的に自分たちの話し合い活動でもシェアオピを使い始めた．教科の学習の中での体験が，自分たちの学習への適用のイメージを作ったようである．そして自分たちなりの活用スタイルで使いこなしている．図 -3 は，児童が自分のタブレットでシェアオピに意見を入力する画面の様子である．

教員の側にも動きがあった．まず管理職がこのツールを目にとめてくれた．すぐに校内に周知されたところ，ほかの教員から「自分の授業でも使ってみたい」という声が届いた．おかげで，校内で，複数学年において，何件もの実践がなされた．それが本校の教員たちにとっても，ICT 活用の利点を実感する機会となったのではないかと考えている．

この開発により，授業の中で活用しやすいツールの要素について次の４点に整理できた．

1）機能が絞られていること
2）操作にモードがないこと

■図 -3　シェアオピに意見を入力する様子

3）目的の実行までのステップ数が少ないこと
4）機能と操作が1対1で対応していること

さまざまな機能を実装して多機能化していくと，活用範囲が広くなるようなイメージがある．しかし多くの場合は，機能を切り替える手順が複雑になるため機能が埋もれ，活用されにくい状況に陥ってしまう．ツールはあくまでも学習を支援するためのものであり，本来やるべき学習よりもツールの使い方の習得に時間を取られるようでは，多くの教員は，そのようなツールは使用しない．

ツールに「できる」ことと，ツールを「使える」ことの間には深い溝がある．前述の4点のポイントを抑えることでその溝を乗り越えることができるのではないかと考えた．

シェアオピによる実践事例

社会「身の回りの工業製品」

単元の導入として，工業製品と私たちの暮らしとのかかわりを調べ，自分たちの生活の実態と豊かさについて考える活動を行った．

1）教室内の工業製品を分類する．

導入の活動として，シェアオピで教室内の工業製品の写真を載せたコンテンツを用意して，分類活動を行った（図-4）．

■図-4 「身の回りの工業製品」の教材

2）自分の家の工業製品の写真を集める．

児童用タブレットはLTE回線で繋がれており，自宅でもインターネットを活用できる．児童はタブレットを自宅に持ち帰り，写真を撮ってシェアオピに投稿して，次時の学習の準備を行った．

3）2）の写真を分類して意見交換を行う．

自分の家の工業製品を分類する活動を通して，工業と自分との生活のかかわりについて考えた．また他者の分類に触れたり意見交換したりすることで，より深く考える機会とした（図-5）．

この実践では，児童用のタブレットの機能をフル活用した活動を設定した．シェアオピは校内外においても使い方は変わらないため，児童も家庭での活動をスムーズに行うことができたようであった．

算数「偶数と奇数」

数の分類活動を通して．偶数と奇数の特徴について考え，そのルールに気づく活動を行った．活動全般でシェアオピを活用した（図-6）．

1）個別に分類する．
2）全体で検討して，ルールを話し合う．
3）適応問題に取り組む．

図画工作「わたしが名画」

名画を参考にして，自分がその中の人物になりきるために服や装飾品を作る．最後には作ったものを

■図-5 「身の回りの工業製品」の授業の様子

着用して額縁に入り，なりきり写真を撮る活動を行った（図 -7）．なりきり写真と感想の共有に Web を活用した（図 -8）．渋谷区教育研究会・図工部会の実践である．

1）数枚の名画を資料としてタブレットで提示．
2）児童は選択した名画を観察して，真似したい服や装飾品を作る．
3）2）を着用して，なりきり写真を撮る．
4）3）の写真や感想をシェアオピに投稿し，交流する（図 -8）．

成果のまとめと今後の展望

シェアオピの開発から多くのことが得られた．学習活動における利点として次の点を挙げておく．

児童にとっての利点

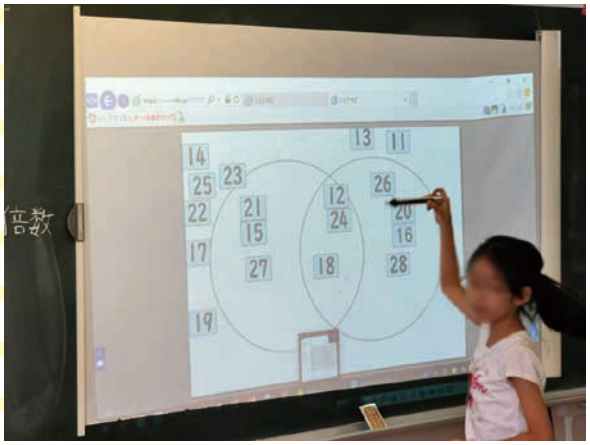
- 素早く学習活動に入れるため，学習内容に集中しやすい．
- 挙手による発表より敷居が低く意見を出しやすい．
- 友だちの意見をモニタしながら活動を進められる．

教員にとっての利点

- 機能がシンプルなため，活用のイメージが持ちやすい．
- 素早く利用を始められるので，1 時間のさまざまな段階に取り入れやすい．
- デフォルトで記録が残るので評価に活かしやすい．
- 利用時の児童への使い方やトラブルによる対応が少ない．

私はこのような開発を続けてきた．シェアオピの開発では多くの実践を重ねたことで，改めてこの活動に大きな意義を見出すことができた．今後も現場の一教員として授業支援ツールの開発を続けていくことで，小学校における ICT 活用の可能性を追求すべく，試行錯誤を続けていくつもりである．

（2020 年 4 月 26 日受付）



■図 -6 「偶数と奇数」の授業の様子

■図 -7 「私が名画」の授業の様子

■図 -8 シェアオピでの交流の様子

鍋谷正尉　oyasai@nby.jp
小学校講師・図書館員・会社員などを経て，2004 年小学校教諭として東京都に採用．所属自治体の教員 ICT 研修の運営に参加してきた．2019 年～渋谷区立千駄谷小学校（ICT プロジェクトリーダ）．

集まれ！ジュニア会員！！

2020年3月の本会第82回全国大会にて「Exciting Coding! Junior @Kanazawa」を開催予定でしたが，残念ながら中止となってしまいました．今回は，このプログラミングワークショップに，ファシリテータとして参加してもらう予定だったジュニア会員の作品を紹介します．2017年に開催した「Exciting Coding! Junior」に参加し，普段からプログラミングを楽しんで続けている方です．「Exciting Coding! Junior @Kanazawa」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を利用した作品制作を予定していたため，その準備としてmicro:bitを利用した作品に取り組んでもらっていました．

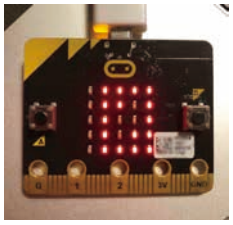
作品紹介　神長春花さんの作品「micro:bitで点字クイズ！！」

https://scratch.mit.edu/projects/356447016/

micro:bitのLED部分に表示される点字の読み方を当てる二択クイズです．クイズでは，micro:bitのLED部分に四角で囲まれた点字が一文字表示され（図：点字が表示される様子），Scratchの画面には読み方の選択肢として2つのひらがなが左右に配置されて表示されます（図：選択肢が表示される画面キャプチャ）．解答は，micro:bitのAボタンとBボタンを利用します．左の文字が正しいと答えたい場合はAボタン，右の場合はBボタンを押します．正解か不正解かは，Scratchの画面とmicro:bitのLED部分の両方にメッセージで表示されます．クイズはランダムにくり返して出題され続けます．点字には1～2年前から興味を持っていたため，点字とmicro:bitを組み合わせた作品にしました．

●作品のスタート画面キャプチャプログラムの一部

●選択肢が表示される画面キャプチャ


●点字が表示される様子（これは「か」を表す）

プログラムを見ると，正解が「左」か「右」かで分けて考えているため，同じようなブロックのまとまりが，正解が「左」と「右」の場合の両方に出てきます．選んだ答えを変数を使って覚えているように，正解が「左」なのか「右」なのかも変数を使って覚えておくと，同じようなブロックのまとまりを1つにすることができます．（https://scratch.mit.edu/projects/385700942/）

micro:bitに搭載されている25個のLEDを点灯し，点字に見立てるのは，とてもいいアイディアですね！　点字に関する知識がなくても，何度もくり返し遊ぶうちに覚えられそうです．興味のある題材をプログラムで表現しようとすることはすばらしいです．中級，上級のクイズも楽しみにしています．

4回にわたってmicro:bitを用いた作品を紹介してきました．micro:bitには今回の作品で利用されている25個のLEDと2つのボタンに加え，加速度センサなどのセンサや外部装置と接続するための端子が搭載されています．コンピュータの中の世界と現実世界とをつなぐ作品制作をぜひ試してみてください．

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

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

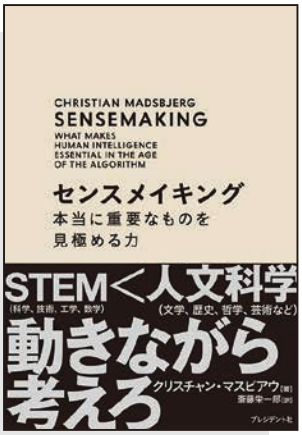
本企画では，ジュニア会員の方の作品・プログラムを募集しています．氏名，ニックネーム，ご連絡先メールアドレス，会員番号，作品に利用しているプログラミング言語，作品タイトル，作品の説明，こだわったポイントを，以下の宛先までお送りください．

会誌編集部門　E-mail：editj@ipsj.or.jp

担当：吉田　葵（青山学院大学）

…› 上松恵理子（武蔵野学院大学）

センスメイキング
本当に重要なものを見極める力



クリスチャン・マスビアウ 著，斎藤栄一郎 翻訳
プレジデント社（2018），368p.，1,800 円＋税，ISBN：978-4833423069

センスメイキングとは

センスメイキングとは実践的な知の技法である．アルゴリズム思考は「量」をこなし，膨大なデータを処理できるが，センスメイキングの力があればそれを深堀りして「奥行き」を追求することができる．

ルーツを見ると実践知をフロシネスと提唱したギリシャの哲学者，アリストテレス（Aristotelés）にたどり着く．フロシネスとは知識と経験の両方を融合したものである．無機質な情報と数字だけのすべてを削ぎ落した薄いデータだけでは，ひとたび市場に変化が生じると迷走する可能性が高い．そのような状況下では，本能的な文脈に立ち返り厚いデータの本領を発揮されるという．

今，人々は STEM（科学・技術・工学・数学）やビッグデータからの知識一辺倒になっている．人間の価値や判断は先の見えない変化がつきものだが，確実なデータと自然科学的な手法のみに偏り，人間の営みを物理法則や機械的メカニズムだけで説明しようとすると自然科学の法則で割り切れないあらゆる形式の文化的知識に対して感度が鈍ってしまう．そのため人文科学や社会科学のトレーニングも大事であるという．

これらのことを鑑み，本当に重要なものを見極める力，目利きになる方法とは何かを多くの事例で明らかにしている．

センスメイキングの事例

スーパーマーケット事例でも薄いデータ対応の限界を示している．本書にあったスーパーマーケットの事例では，ビッグデータの分野ではエキスパートで，対象セグメントについては完璧に理解し，顧客ごとに抽象的なセグメントモデルが用意されていた．たとえば夕方来店する仕事を持つ女性客が主に購入する商品もさっと調べることができ，データ通りの予測をつけることが簡単だった．

しかし，実際にはそうとはならなかった．ダイニングテーブルの写真を何千枚か撮影した結果，調査対象の全地域でテーブルが食事とは無関係なものであふれていた．都市部では毎日 5 時に帰宅し 6 時に食卓につける人などほとんどいないため，事前に献立をきっちり計画して，買い物リストに沿って食材を買う人など少なかったのだ．その時々の気分に応じて直感的に買い物をしていたことが分かった．

このことが示すことは，購入点数や来店客のタイプをカウントしたり追跡したりするのが重要ではなく，体験を現象として捉えなおすことの重要性であった．店のどこに何があるのか分かりやすく配置し，簡単で健康的な夕食の材料が豊富にする「夕方の慌ただしさ」への対応こそが求められたのだった．

目利きになる

求められるのはデータの目利きになることである．「これまではこうなる」という数字だけで筋を通そうとするアルゴリズムでの判断は先行き不透明な時代に意味を持たない．

前例のない新型コロナウイルスに立ち向かってい

る私たちの社会は，情報がとても重要なことを提示している．このような大変化の時代には，企業や組織が先行きに不透明感を抱くのが現実である．センスメイキングはこの手の恐怖や不安を切り抜けるための道筋を示す．データの分析ツールは哲学，文化人類学，文学，歴史学，芸術学などの多くの分野から集めた厚いデータを採り入れて，適切な文脈を選べるように誘導してくれる．また，センスメイキングによりデータを組み合わせ，何かを的確に語らせるための切り口が身につき，データの総和を大きく上回るような解釈ができるようになるのである．

世界が脅威にさらされている今だからこそ，センスメイキングは，本当に重要なもの，注目すべきものを見極める力を与えてくれる重要な概念といえるだろう．

（2020 年 4 月 13 日受付）

上松恵理子（正会員） uematsu@star.rcast.u-tokyo.ac.jp
武蔵野学院大学国際コミュニケーション学部准教授，東京大学先端科学技術研究センター客員研究員，本会（情報処理教育委員会・データサイエンス教育委員会・教員免許更新講習委員会・会誌編集委員会）委員．

書評（ビブリオ・トーク）・会議レポート募集のお知らせ

情報処理学会会誌編集委員会では，会誌「情報処理」に掲載する書評，および会議レポートを広く会員の皆さまから募集しています．

1. 募集対象　次の 2 種類の記事について，原稿を募集します．書評に関しては，「ビブリオ・トーク―書評―」，「ビブリオ・トーク―私のオススメ―」の 2 つのカテゴリを設けます．

a-1）ビブリオ・トーク―書評―：過去 2 年間に出版された，本会会員にとって有益な図書についての紹介もしくは批評．

a-2）ビブリオ・トーク―私のオススメ―：お気に入りの本の紹介．

b）会議レポート：情報処理に関する国際規模の会議・大会の報告など，時事性が高く，本会会員に広く知らせる価値のある話題．

2. 応募資格

原則として本会会員に限ります．

3. 応募の手続き

1）表　　題：ビブリオ・トークの場合は，書評もしくは私のオススメの投稿カテゴリ，著者名，書名，ページ数，発行所，発行年，価格，ISBN を書く．会議レポートは，見出しを書く．書評，会議レポートの別を左肩に書く．

2）評者名（会議レポートの場合は筆者名）・所属・評者連絡先（住所，E-mai，Fax など）の記載を忘れずに．

3）本　　文：ビブリオ・トークは 1,500 字以内または 3,000 字以内（1 または 2 ページ）．会議レポートは 2,100 字前後で書く．

4）そ の 他：（必要であれば）参考文献，付録，図，表をつける．詳しくは「原稿執筆のご案内／書評・会議レポート」（https://www.ipsj.or.jp/magazine/sippitsu/shohyonews.html）を参照してください．

4. 原稿の取扱い

投稿された原稿は会誌編集委員会で審査し，採否を決定します．採用にあたっては原稿の修正をお願いすることがあります．あらかじめご了承ください．

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

連載

5分で分かる!? 有名論文ナナメ読み

阪本哲郎　瀧ノ上正浩（東京工業大学）

Lee Organick et al : Random Access in Large-Scale DNA Data Storage

Nature Biotechnology, Vol.36, pp.242-248（2018）

遺伝子だけではない DNA

DNA は我々生物の細胞の中に存在し，遺伝情報を担っていることは皆さんご存知の通りである．しかし，遺伝子とはまったく無関係に，DNA をマテリアルとして，さらには情報処理媒体として利用しようと考えている人々がいることをご存知だろうか．計算機科学者 Adleman（RSA 暗号の開発者の一人）による DNA 分子を用いたハミルトン閉路問題を解く並列計算の研究（DNA コンピューティング）や，DNA オリガミといった DNA ナノテクノロジーの研究など，DNA が「情報を持った分子である」という特徴を巧みに用いた斬新な研究が多くなされてきている[1), 2)]．

そして今日，DNA は情報の長期記憶媒体（ストレージ）としても注目され始めている．本来，DNA は生物の持つ膨大な遺伝情報を記憶するメディアであり，ストレージとしての利用を考えるのは当然といえば当然である．実際，DNA は非常に安定な分子であり，永久凍土から回収された 70 万年前のウマの骨から DNA を取り出し，全ゲノムの解析に成功した事例もある．さらに注目すべき点はその情報密度である．仮に 1 塩基 2 ビット換算をすると，1 グラムの DNA 分子で 230 エクサバイト（230 × 10^6 テラバイト）の容量がある．もちろん，冗長性を持たせる必要やその他の技術的制約から実際にはこの値よりも小さくなるが，それでもメディアとしての可能性を秘めていることは想像にかたくない．

DNA ストレージの基本的なアイディア

まず，一般的な DNA ストレージがどのような原理で動作するか説明する．DNA ストレージであってもその動作の流れは HDD などの通常のストレージと同じであり，符号化，書き込み，読み出し，復号化の 4 段階に分けて考えることができる（図 -1（a））．

まず「符号化」について説明する（図 -1（a）i）．記録したいバイナリデータを塩基配列に変換する必要がある．たとえば，00 を A，01 を T，10 を G，11 を C のような変換ルールによって変換できる．この塩基配列を一定の長さ（数十塩基）ごとに断片化しておく．この段階でランダム化や誤り訂正符号の付与なども行われる．断片にはそのアドレスを表す配列が追加され，さらに特別な配列が断片の両端に追加される．この特別な配列は全断片に共通する配列で，復号の際に必要になる．ここまでのプロセスはコンピュータ上で行われる．

次に「書き込み」操作について説明する（図 -1（a）ii）．それぞれの断片配列を DNA 合成技術により分子として実体化させる．具体的には，塩基 1 つ 1 つを化学反応で繋げることで，指定した塩基配列を持つ DNA 断片を化学合成することができる．すべての DNA 断片を合成したら，それらを混ぜた水溶液を調製し，これが DNA ストレージとなる．

次に「読み出し」操作について説明する（図 -1（a）iii）．この水溶液中に含まれる DNA 断片の配列を，次世代シーケンサなどの装置を用いて塩基配列情報

として読み出す．配列の読み出しは，分子が多ければ多いほど精度が高くなるため，Polymerase Chain Reaction 法（PCR 法）を用いて水溶液中の DNA 分子を大量に複製させてから行うことが一般的である．

PCR 法とは，DNA 上の特定の配列（我々が指定できる）に挟まれた部分配列を複製する技術である（図 -1（b））．配列の符号化の際に，断片の両端に特別な配列を追加したのは，後にその断片を PCR 法により複製させるためである．この特定の配列に相補な一本鎖 DNA をプライマーと呼び，複製の際に，複製したい DNA とともに混ぜる（図 -1（b）i）．温度を上昇させると二重らせんが解け，プライマーが結合する相補の部分が露わになる（図 -1（b）ii）．この状態で少し温度を下げると，一本鎖状態の複製したい DNA の両端にプライマーが結合し（図 -1（b）iii），DNA ポリメラーゼ（合成酵素）と呼ばれるタンパク質が相補鎖を伸長していく（図 -1（b）iv）．以上の 1 回のルーチンで DNA 分子は 2 倍に増えるため，多数回繰り返すことで DNA 分子数は指数関数的に増加する．以上が PCR 法の大まかな説明である．

最後に「復号化」について説明する（図 -1（a）iv）．読み出された断片配列を，アドレスを元に並び替え，元のバイナリデータに復元する．復号化の操作は符号化の逆操作であり，同様にコンピュータ上で行われる．

DNA ストレージ上でのランダムアクセス

この論文の著者らは，動画，画像，音声，文章といったさまざまな種類のデータ（計 35 種類 200 メガバイト）を DNA ストレージに保存し，それぞれのデータを復元することに成功した．これは当時知られていたほかの DNA ストレージよりも 1 桁ほど容量が大きいものである．それを可能にしたのが著者らの考案した DNA ストレージ上でのランダムアクセスである．

記録したいデータが複数ある場合を考えてみる．すべてのデータを順番に繋げて 1 つのデータとして記録することがまず考えられるが，読み出しの際にもすべてのデータを復元する必要があり無駄が多い．これは読み出し精度の観点でも問題である．そこで，データごとにプライマーの配列を用意し，読み出しの際には必要なデータのみを取り出せるようにする，つまりランダムアクセス可能にする，というアイディアが今回紹介している論文の肝である（図 -1（c））．

たとえば，2 種類のデータ X，Y の DNA が水溶液中にあるとき，両者に同じプライ

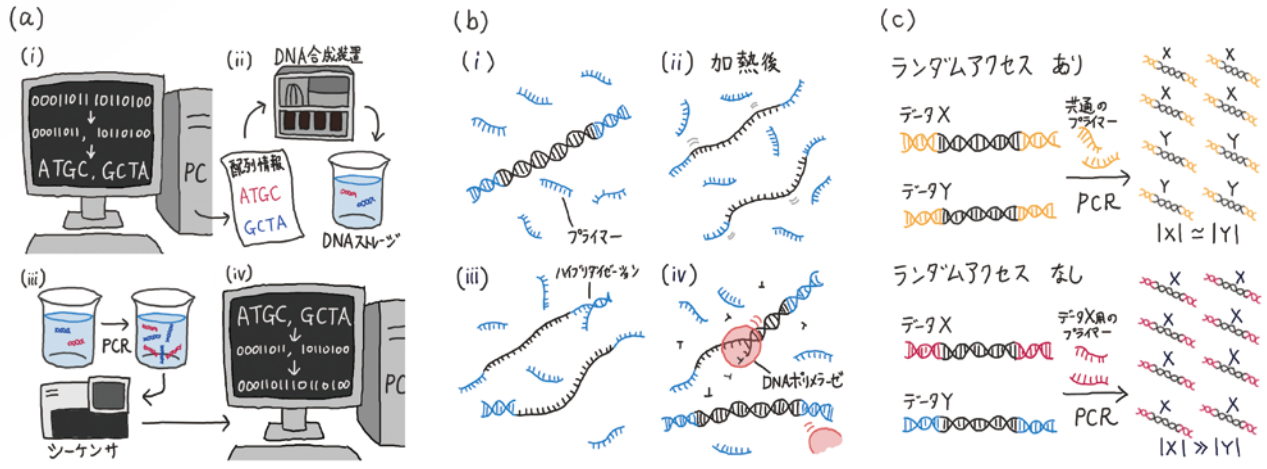


図 -1　（a）DNA ストレージの仕組み，（b）PCR 法の概要，（c）ランダムアクセス，データ X のみ増幅する例

マーを用いた場合，PCR 法により X，Y が同程度複製されてしまう．一方で，あらかじめ異なるプライマーを用いるように設計しておけば，PCR 法の性質により，複製されるデータをどちらか一方に制限できるのである（図 -1（c））．

DNA ストレージのこれから

DNA ストレージ上でランダムアクセスが可能になることで読み出しの精度が向上し，結果的に DNA ストレージの容量を上げることに成功した．しかし，課題も多く残されている．一番の問題はそのスループットである．実用的な DNA ストレージとしては数キロバイト／秒程度の書き込み速度が求められるが，それを達成するためには今日の全 DNA 合成会社が 1 年間に合成する量を 2 週間で合成するくらいの速度が必要である．また，DNA ストレージを操作する装置の小型化も望まれる（同グループが近年報告した自動書き込み読み取り装置では，テーブルいっぱいのサイズ）．

DNA ストレージの長所は冒頭に述べたが，実はほかにも考えられる．それは DNA コンピューティングや分子ロボティクスへの応用である．分子ロボット，特にその情報処理部分を担うと期待されている DNA コンピュータとは，同じ DNA を用いているという点で入出力を共通にすることができる．さらに，DNA は生体分子であることから，生体内で活動する分子ロボット[3]を考えた場合に，その生体親和性は問題ないだろう．細胞の中で全遺伝子を保持している細胞核のようなものを人工合成できるようになるかもしれない．このように，DNA ストレージの技術は，さまざまな分野へと応用されていくことが期待される．

参考文献

1) 小宮　健，瀧ノ上正浩 他：DNA ナノエンジニアリング，近代科学社 (2011).
2) 瀧ノ上正浩：生体内で働く分子ロボットの実現へ：情報媒体としての DNA 分子と DNA コンピューティング，情報管理（JST）(2017).
3) Murata, S., Konagaya, A., Kobayashi, S., Saito, H. and Hagiya, M.：Molecular Robotics：A New Paradigm for Artifacts, New Generation Computing (2013).

（2020 年 4 月 17 日受付）

阪本哲郎　tetsuro53@gmail.com

東京工業大学情報理工学院修士課程修了．

瀧ノ上正浩　takinoue@c.titech.ac.jp

2007 年東京大学大学院理学系研究科物理学専攻より博士（理学）取得．2011 年東京工業大学講師，2016 年より同大情報理工学院准教授．JST さきがけ研究者，フランス ENS 招聘教授などを兼任．専門は DNA の生物物理学と DNA ナノテクノロジー．

連載 買い物自慢

酒井 潤 (Splunk, Inc.)

第9回

子供とプログラミングで遊べるトイドローンを買ってみた

安価で手軽にドローンを飛ばしてみたい，狭い室内でもおもちゃ感覚でドローンを飛ばしたいという方がいたらオススメしたいのが，Ryzo 社が提供する Tello EDU のドローンです．数十万円もする高価なドローンではなく，1 万 1160 円（DJI Store 2020 年 3 月時点）で購入できる比較的安価なおもちゃのようなドローンです．また，Apple 社が提供する iPad からも子供向けの無料プログラミングアプリケーションが提供され，グラフィカルな GUI でお子さんでもドローンを飛ばしながら楽しくプログラミングを学ぶことが可能です．

■ドローンのスペック

- サイズは 98 × 92.5 × 41mm
- 重さ 87g
- Micro USB Charging Port
- 最大飛行距離 : 100m
- 最大スピード : 8m/s
- 最大飛行時間 : 13 min
- 最大飛行高度 : 30m
- カメラフォト : 5MP (2592 × 1936)
- カメラのビデオ : HD720P30
- カメラ Format: JPG(Photo); MP4(Video)

上記注目してほしいのがサイズと重さです．手のひらサイズのコンパクトなサイズで，重量も軽いため，万が一，人に当たってしまっても大怪我をするということもないかと思います．また小型なので，外出せずに室内でも安全に遊べるところが非常に魅力的かと思います．

■スマホやタブレットで簡単コントロール

スマホやタブレットにダウンロードできる無料アプリがあり，アプリから簡単に操作が可能です．また，別売りで上級者向けのコントローラもありますが，スマホアプリで十分に操作できましたので，特に専用のコントローラがなくても大丈夫かと思います．

また，初心者でも簡単にドローン操縦が楽しめる機能もあります．その 1 つにトスというものがあり，手のひらにのせた Tello Drone を放り投げて飛ばしたり，着陸する際にも手のひらに着陸させるということもできます．また Flip 機能というものがあり，飛んでいるドローンを前転させたり，後転させたりとアクロバティックな操作もボタン 1 つで簡単に操作できますので，ドローン飛行を見ている人たちを魅了して操縦する楽しさもあります．

■飛行中に撮影もできる

安価なドローンですが，カメラも付いておりますので，飛行風景を撮影できるのも 1 つの魅力かと思います．静止画や動画もとれますし，360 機能といって，ドローンが空中で 360 度横に回転して周りの風景の動画を撮影してくれる機能もあります．

■ Python や Go でカスタマイズで自動操縦ができる

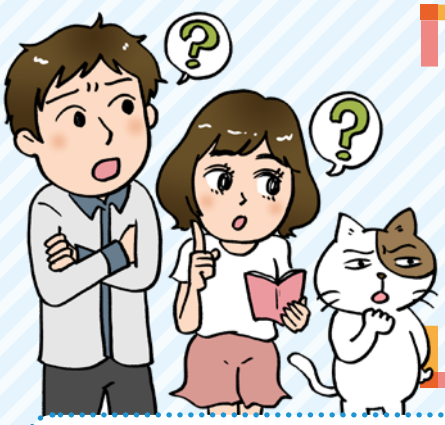
上級者向けになってしまうのですが，Tello EDU はドローンを操縦するための API を提供しているため，Python や Go 言語などお好きなプログラミング言語でドローンを操縦することが可能です．Python に関しては，Tello も SDK を提供しておりますし，Go 言語では，Gobot というロボティクス開発 IoT フレームワークのオープンソースで Tello Drone を操作するライブラリも作られているため，ある程度のプログラミング知識がある方であれば簡単にドローンの自動操縦プログラミングも可能かと思います．私も Udemy というオンライン教育プラットフォームで講師として，どのようにドローンを操縦するかのコースを以下に出しておりますので，ご興味ある方は覗いてみてください．コースの中では，Tello Droe のカメラを使って，人の顔を認識し，追従するプログラミングのやり方を教授しております．

- 現役シリコンバレーエンジニアが教える未経験者のための Python ドローンプログラミング
- 現役シリコンバレーエンジニアが教える Go 入門 ＋ ドローンプログラミング

それでは，皆さまも，Tello Drone を通して，世界で注目されているドローン技術を実際に触れながら楽しまれてください．

(2020 年 3 月 12 日受付)

※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．



連載

先生，質問です！

ドラえもんの実現にはさまざまな機能が必要そうです．今回はそれら機能とかかわりの深い研究に取り組まれている専門家の皆さんに回答いただきました．

神長春花
【ジュニア会員】
小学生

Q いつかドラえもんのようななんでも出せてコミュニケーションがスラスラできるロボットはできますか？

A 「なんでも出せて」とは，ドラえもんがおなかの四次元ポケットから取り出すさまざまな「ひみつ道具」のことですよね．NHK でも 2019 年末にドラえもん 50 周年の特集をやりましたが，ひみつの道具は 1,600 以上もあるようです．そのうちのいくつかは形を変えて実現してきています．「メロディお玉」も東大名誉教授の嵯峨山茂樹先生が自動作曲システムを，「とうめいマント」も稲見昌彦先生（東大）が透明人間システムをそれぞれ発明していましたよね．情報処理学会の研究者の多くが小さいころからドラえもんのまんがを読んで「こんなことできたらいいなあ．じゃあやってやるぞ」と思って謎を解いている人が多いと思います．もう 1 つの質問ですが，「コミュニケーションがスラスラできるロボット」ですが，これはすごく良い点に気づきましたよね．たぶん，のび太が「何をしようかと考えている」ことにドラえもんが「のび太君，『まさか〇〇できたらいいなあ』，なんて考えているんじゃないだろうね？」とスラスラとコミュニケーションできるようになるかという質問だと思います．これは「相手の意図を理解する」研究ですが，もう少し経てばロボットができるようになると思います．

萩田紀博
【正会員】
大阪芸術大学

石黒　浩
【正会員】
大阪大学

A アニメのドラえもんのようにすらすら話をするためには，人の考えや感情をある程度理解し，自分も自分の考えを持ちながら，感情豊かに声の調子や表情を変えて話す能力が必要になります．これらの機能を全部実現できるのは，30 年とか 40 年先になるかもしれませんが，いつかはアニメのドラえもんくらいに話せるロボットは出てくる可能性はあると思います．

A

タイムマシン，もしもボックス，どこでもドアなどのすごいひみつ道具がなんでも出せるようになるかは回答者には分かりません．しかし，対話が情報のやりとりであり，人間が情報処理を行っている以上，いつかはドラえもんのようにコミュニケーションがスラスラできるロボットはできるでしょう．

人間もそうですが，コミュニケーションがスラスラできるためには，相手と価値観や目的を共有する必要があります．相手の心は見えません．そのため，対話を通して，価値観や目的をすり合わせていく必要があります．ドラえもんとのび太はよく喧嘩をします．人間同士もそうです．相手の言葉に傷ついたり，喜んだりします．こうしたことを通して，より円滑なコミュニケーションができるようになっていきます．ドラえもんが未来に帰ると言ったとき，のび太はドラえもんが安心して未来に帰れるように，ジャイアンに立ち向かっていきました．これは，一緒に過ごす中で，ドラえもんの価値観を理解したからでしょう．

現状の対話システムは，一般に価値観は変わりません．目的も変わりません．ユーザに自身の価値観を押し付け，システムが理解できるように伝えないと会話が成り立ちません．これからの対話システムは，人間と歩み寄るようなものになっていかなければなりません．お互いの価値観や目的をすり合わせることができれば，人間とコンピュータの連携は深まっていくでしょう．人間同士ではできなかった問題解決も実現できるようになると思います．そうした人間とコンピュータのやりとりから数々のひみつ道具も産まれてくるのかもしれませんね．

東中竜一郎
〔正会員〕
名古屋大学

大武美保子
〔正会員〕
理化学研究所

ご質問は大きく 2 つの機能，1）なんでも出せる，2）コミュニケーションがスラスラできる，が実現できるかを問うています．1）なんでも出せる，は，ドラえもん本体というよりドラえもんの道具を作れるかどうかなので，ここでは 2）について考えてみます．

回答の時点での対話技術は，話題の範囲を限定することにより，いろいろな質問に答えられるようになっています．のび太がドラえもんを必要とする状況は，スネ夫に自慢話を聞かされてくやしい，ジャイアンをやっつけたい，など，かなりパターン化されているので，これまでのドラえもんとのび太の会話データを集めれば，それらしいコミュニケーションができると思います．ただ，質問では，「ドラえもんのように」と比喩であって，ドラえもんそのものではないので，ドラえもんとまったく違う状況だと，スラスラ答えられませんね．

ご質問いただいた方は，それらしく見えることではなく，本当に共感してくれることを期待していると思います．ところが，心の働きを突き詰めると，ふるまうことによって気持ちを感じる仕組みになっているという説があり，適切にふるまえばよいと割り切ることも可能です．2）は 1）の機能と比べると，物理法則上の制約はないので，質問に対する応答の観点で，同じようなコミュニケーションは，今でもある程度できるし，今後の研究でもっとできるようになると思います．

「先生，質問です！」への質問はこちら

https://www.ipsj.or.jp/magazine/sensei-q.html

基般

2019年度情報処理技術遺産および分散コンピュータ博物館

旭　寛治 | 歴史特別委員会 幹事

情報処理技術遺産および分散コンピュータ博物館の認定制度

現存する情報処理技術関連の貴重な史料に対して，その保存の努力を称えるとともに末永く後世に伝えることを目的として，情報処理学会歴史特別委員会によって設けられた制度．第1回の2008年度は国立科学博物館で，翌年からは全国大会の場で認定式を行い，情報処理技術遺産には認定証の盾を，また分散コンピュータ博物館には認定書とプレートを，それぞれ関係者に贈呈している[1)～3)]．

今年は，新型コロナウイルス感染症の拡大防止対策として，全国大会の現地開催が中止になった．そのため，当初認定式を予定していた3月6日を認定日とし，認定証の贈呈は後日別の場を設けて行うこととした．認定内容については，6月3日にオンラインで開催された定時総会で報告された．

❑ 情報処理技術遺産

今回認定された情報処理技術遺産は次の5件である．スーパーコンピュータは比較的製造年代が新しく,「遺産」と呼ぶにはふさわしくないこともあって,これまであまり認定してこなかったが,「京」が引退し，一つの時代が終わったタイミングでまとめて取り上げることにした．

- **NEC スーパーコンピュータ SX-2 パッケージ：** SX-2は，多重並列動作ができる高性能ベクトル演算パイプラインを4セット（演算器数最大16個）使用するとともに，我が国で初めての水冷方式によるマルチチップLSI高密度パッケージなど最新技術を採用することによって6nsという超高速マシンサイクルを達成し，当時の世界最高速である1.3ギガFLOPS[☆1]での演算性能を実現した．1985年，日本電気製造．
- **FACOM VP シリーズ E モデルの MCC ボード：** スーパーコンピュータVPシリーズのベクトル処理装置には，400および1,300ゲートのLSIと4キロビットのRAMモジュールを搭載したMCC

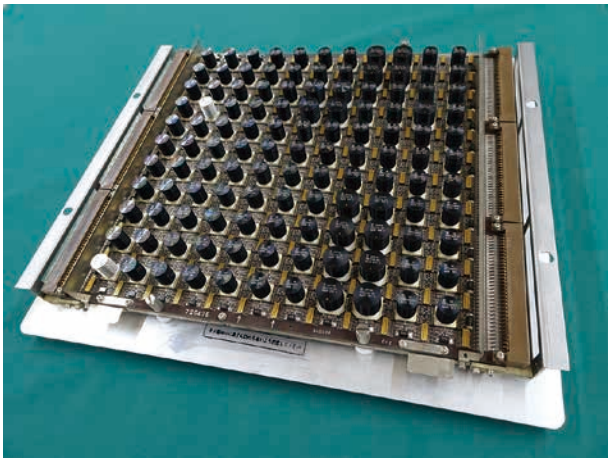
☆1 1秒間の浮動小数点演算回数．

SX-2システム

（Multi-Chip Carrier）高密度実装ボードが使用された．1985 年春，VP-400 が旧・航空宇宙技術研究所[☆2] で世界で初めて 1 ギガ FLOPS を超える性能を実現した．E モデルは命令を追加した性能改良モデル．1987 年，富士通製造．

- **HITAC S-820：**命令並列パイプラインおよびベクトル要素並列パイプラインの採用，リンク式ベクトル起動等によりベクトル演算性能の向上を図るとともに，アクセス時間 2.5ns で容量 7 キロビットの高速 RAM と 2,500 ゲートの論理素子を 1 チップに納めた専用ベクトルレジスタ素子を搭載し，シングルプロセッサとしては当時世界最高速の 3 ギガ FLOPS の性能を実現した．1987 年，日立製作所製造．
- **地球シミュレータ：**地球温暖化などの地球規模でのシミュレーションを目的に旧・宇宙開発事業団[☆3]，旧・日本原子力研究所[☆4]，旧・海洋科学技術センター[☆5] の 3 法人が開発．2002 年 6 月に LINPACK ベンチマークで実効性能 35.86 テラ FLOPS を記録してスーパーコンピュータの計算性能の世界ランキングである TOP500 でトップを獲得し，以後 5 期連続でトップの座を占めた．2002 年，日本電気製造．
- **スーパーコンピュータ「京」：**文部科学省が推進した「革新的ハイパフォーマンス・コンピューティング・インフラの構築」プロジェクトの中核システムとして理化学研究所と富士通が共同で開発を行い，2012 年 9 月に共用を開始した．2011 年に世界で初めて 10 ペタ FLOPS の計算性能を達成した．「京」による科学研究も高く評価され，スパコン分野で最も権威あるゴードン・ベル賞を 2 度受賞している．

☆2 現・JAXA.



FACOM VP シリーズ E モデルの MCC ボード

保存されている HITAC S-820 の拡張記憶および主記憶筐体

☆3 現・宇宙航空研究開発機構.
☆4 現・日本原子力研究開発機構.
☆5 現・海洋研究開発機構.

地球シミュレータ：2002 年 4 月ニューヨーク・タイムズ紙に “Computonik” として掲載された写真

❑ 分散コンピュータ博物館

今回認定された分散コンピュータ博物館は次の1件である.

- **富士通 DNA 館**：富士通が長年にわたり引き継いできた高い目標にチャレンジするという“DNA”を，富士通グループの次世代に継承する研修の場として，2006年に沼津工場に開設された．メインフレームの組み立てに使われていた広さ3,000平方メートルのフロアを改修し，同社のコンピュータ，周辺機器，部品，これらを用いたソリューションサービス群など，約11,000点の機器と資料を展示している.

展示されている「京」

富士通 DNA 館

パンフレット「情報処理技術遺産」（写真）やWebサイト「コンピュータ博物館*」に，認定された遺産や博物館の解説記事と写真が掲載されているので，ご覧いただきたい.

(*) http://museum.ipsj.or.jp/

参考文献

1) 和田英一：情報処理技術遺産および分散コンピュータ博物館認定式，情報処理，Vol.50, No.5, pp.369-374 (May 2009).
2) 旭　寛治：2017年度情報処理技術遺産および分散コンピュータ博物館認定式，情報処理，Vol.59, No.6, pp.544-550 (June 2018).
3) 旭　寛治：2018年度情報処理技術遺産および分散コンピュータ博物館認定式，情報処理，Vol.60, No.7, pp.656-658 (July 2019).

(2020年5月18日受付)

旭　寛治（名誉会員） asahi@fw.ipsj.or.jp

（株）日立製作所基本ソフトウェア本部長，ストレージソリューション本部長，（株）日立テクニカルコミュニケーションズ代表取締役等を歴任．1999年本会理事，2005年副会長．歴史特別委員会幹事．コンピュータ博物館実行小委員会主査．本会フェロー.

情報処理技術遺産認定証

情報処理技術遺産パンフレット

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

「情報処理」カタログ同封サービスのご案内

カタログ同封サービスとは？

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

お申し込み方法と掲載までの手続き

❶封入希望月の**前月 15 日**までに下記事項を記載の上、問合せ先までお申し込みください。
- ◆会社名，担当者，連絡先（住所、Tel、Fax、E-mail） ◆封入希望号
- ◆サイズ ◆カタログの簡単な内容説明
- ◆割引対象にあたる場合はその旨記載ください。

❷封入希望月の遅くとも**前月末日**までに下記事項について手配をお願いします。
- ◆カタログ見本を問合せ先までお送りください（PDF、Fax 可）。
- ◆納品業者をお知らせください。

❸**納品日は封入希望月の 5 日（土曜、日曜、祝日の場合は翌営業日）です。**日付指定にて必要枚数（20,000 枚）を印刷し指定の納品先へお送りください。
- ※納品先は、お申し込み後にご連絡いたします。
- ※納品が遅れますと同封ができない場合がございます。その場合はキャンセルとさせていただきます。

❹カタログを同封した学会誌を発行日にお送りしますので、ご確認ください。

❺後日請求書をお送りしますので振込手続きをお願いします。

1 通あたり約17.5 円！ **基本価格　350,000 円**（税抜）

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

大学や共催事業はさらに割引も！

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

大学 / 研究所 / 賛助会員（基本価格の 40% Off ！）	210,000 円（税抜）
情報処理学会主催・共催事業＊（基本価格の 80% Off ！）	70,000 円（税抜）

＊情報処理学会研究会主催、共催を含む

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

問合せ先

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

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

SANER 2020 会議報告

SANER 2020 概要

今回我々が参加した International Conference on Software Analysis, Evolution, and Reengineering（SANER 2020）は，IEEE が主催するソフトウェア解析・進化・リエンジニアリングに関する国際会議である．本年（2020 年）は，2 月 18 日から 21 日にかけてカナダのロンドンで開催された．18 日には 4 つの併設ワークショップが行われ，19 日から 21 日の 3 日間で本会議が行われた（**図 -1**）．

本年は，新型コロナウイルス流行のため，いくつかの国で渡航制限が発せられており，多くの研究者がリモート参加することとなった．具体的な人数は公表されなかったが，約 150 名が現地参加，約 40 名がリモート参加していた．

本会議では，Research Track のほか ERA（Early Research Achievements），Tool，Industrial，RENE（REproducibility Studies and NEgative Results），Journal First，LBI（Late Breaking Ideas）の 6 トラックで論文が募集された．各トラックの採択数／投稿件数（採択率）は，Research：46/170（27%），ERA：16/49（33%），Tool：6/10（60 %），Industrial：4/11（36%），RENE：2/4（50%），Journal First:5/6（83%），LBI:4/8（50%）である．

Research Track 論文のうち，以下の 1 編が Best Paper Award に選出された．

- Yuyao Zhang, Siqi Ma, Juanru Li, Kailai Li, Surya Nepal and Dawu Gu, “SMARTSHIELD: Automatic Smart Contract Protection Made Easy”

この論文では，ブロックチェーンのスマートコントラクトに対し，セキュリティ上危険なコードパターンを自動修正するツール SMARTSHIELD を提案している．バイトコードレベルでの構造・意味・フロー解析を行い，バイトコード変換により安全なコントラクトへ書き換える．実験では，91.5%（87,346/95,502）のセキュリティ上危険なコードパターンを修正できたと報告されている．

また，10 年前に同会議で発表された論文の中でその後の研究に最も影響を与えた論文を表彰する Most Influential Paper Award には，次の 1 編が選ばれた（SANER の前身会議の 1 つである Working Conference on Reverse Engineering（WCRE）より選出）．

- Sonia Haiduc, Jairo Aponte, Laura Moreno and Andrian Marcus, “On the Use of Automated Text Summarization Techniques for Summarizing Source Code”, In Proc. WCRE, pp.35-44 (2010).

自然言語テキストから要約を自動生成する技術を利用し，ソースコードに対する要約の自動生成を試みた論文で，ソースコード要約生成の研究分野に大きな影響を与えている．本レポート執筆時点で，10 年間での被引用数は 181 件となっている．

基調講演

基調講演は，本会議の各日午前に行われた．初日は，Queen's University の Ying Zou 教授より，“Effective Management of Clones” というタイトルで講演があった．ソフトウェアの各版におけるコードクローン検出結果を追跡することで，クローンがどのように進化するか（進化パターン），不具合に繋がりやすいクローン特徴にはどのようなものがあるか等を分析し，そこから得られた知見について述べられていた．たとえば，クローンコード群が整合性を失いつつ局所性を変化させた場合や，古いクローンコード群をシステムの別の個所へコピーした場合に不具合リスクが高くなる，といった分析結果について述べられていた．

2 日目は，Kent State University の Jonathan I. Maletic 教授より，“srcML a Retrospective: The Trials and Tribulations of Building Real Software in an Academic Environment” というタイトルで講演があった．アカデミアでいかにして使える・使われる実用的なソフトウェアを開発できたかについて，Maletic 教授らが開発しているツール srcML を題材に，2000 ～ 2020 年の開発ロードマップについて述べられていた．成功の要因として，開発の中期で大きな資金獲得ができたこと（ABB（ASEA Brown Boveri）から 60 千ドル／年，NSF（National Science Foundation）から 800 千ドル），GCC（GNU Compiler Collection）等の

図 -1　SANER 2020 本会議の様子

外部ツールに依存しない設計としたため外部ツールの破壊的な更新（インタフェース変更等）の影響を受けなかったこと，等が挙げられていた．

3日目は，Microsoft Research の Christian Bird 氏による，“Lessons and Insights from Tech Transfers at Microsoft”という講演があった．本講演では，ソースコードのリスク推薦ツールをマイクロソフトの開発現場に適用するときに，失敗した経験や成功した経験を，研究成果を開発現場に移管しようとしている人に向けた教訓として述べていた．

セッション・トラック

SANER は，ソフトウェア解析・進化・リエンジニアリングに関する幅広いトピックを取り扱っている．セッションとしては，バグ・リファクタリング・ソフトウェア進化等が設けられ，おおむね昨年と同類のセッション群であった．昨年度（2019 年度）に引き続き mixed session の形式であり，Research，ERA，Industrial 等の複数トラックの発表を混在させて 1 つのセッションが構成された．

SANER 2020 における新規点としては，ERA トラックでの Journal Reflection 論文の募集，LBI トラックの新設がある．

Journal Reflection 論文は，3 〜 7 年前に出版された論文が，現在・これからの研究にどのような影響を与えているか・与えられなかったかを議論するものである．既存研究の成果・可能性を十分に精査せず，新規アイディアの探求ばかりに着目しがちな現行の傾向を問題視し，Journal Reflection 論文の募集が行われた．ERA 採択論文のうち 3 編が Journal Reflection 論文であった．Journal Reflection 論文の発表では，数年前に出版された，例外処理のバグ傾向に関する論文や，動的影響波及解析の精度に関する論文の成果が，どのような形で引用・利用されているか分析した結果や，今後の研究に繋がるアイディア・ビジョンについて述べられていた．

LBI トラックは，新規性の高い研究課題・解決手法を議論する場であり，近年，他の主要会議（ASE，ICSME）においても導入が始まっている．ERA トラックと違い，手法の実装・実験結果の提示が求められないため，研究のより早期段階で，研究コミュニティからフィードバックを得たい場合に適している．また，新規研究者の参入を容易にしたいという目的もある．LBI 論文の発表では，機械学習システムのドキュメンテーション方法に対するアイディアや，記号実行のガイドとして強化学習を用いるアイディア等が述べられていた．発表スライドは，参加者の興味・意見を上手く引き出すように構成されており，実現可能性や有効性について活発な質疑応答・議論が行われていた．

ワークショップ

SANER 2020 では以下の併設ワークショップが開催された．

- Workshop on Validation, Analysis and Evolution of Software Tests（VST）
- International Workshop on Intelligent Bug Fixing（IBF）
- International Workshop on Emerging Trends in Software Engineering for Blockchain（IWBOSE）
- International Workshop on Software Clones（IWSC）

今年のワークショップはすべて昨年からの継続開催となっている．本章ではこれらのワークショップについて簡単に紹介し，筆者が参加したワークショップ IWSC の基調講演を紹介する．

VST は，ソフトウェアテストの検証，解析，進化をメイントピックとしており，確率的ソフトウェアモデリングによるバグ限局の提案や，オブジェクト指向言語のテストケース自動生成技術の弊害となり得る内部オブジェクトの設定可能性に関する 110 個の OSS の調査などの発表があった．

IBF は，高度なバグ修正をメイントピックとしており，機械学習に基づく脆弱性検出に高い影響を及ぼす要因の実証研究や，OSS で修正不能（wontfix）とタグ付けされたバグレポートを実証的に調査した研究などの発表があった．

IWBOSE は，ブロックチェーンを対象としたソフトウェア工学をメイントピックとしている．イーサリアムプラットフォームにおける再入可能性の脆弱性を検出するフレームワークの提案，暗号通貨の価値の固定化に向けたブロックチェーンを用いた財務モデルの提案などの発表があった．

IWSC は，ソフトウェアクローンを取り扱っており，構文的なクローン検出の精度改善のためにソースコードを LLVM に基づく中間表現に変換する手法や，クラウド上で容易にクローン検出してインタラクティブにクローンの分析が可能なシステムの実装などの発表があった．IWSC の基調講演は，Polytechnique Montréal の Foutse Khomh 准教授よる，“New Frontiers in Software Clones Research”であった．クローン検出やクローン進化について取り上げ，クローンの発生パターンの分類や機械学習を利用したクローン検出法，そして欠陥を含む恐れがあるクローンの進化パターンの調査について，論文を紹介しながら述べていた．

総括・次回開催予定

SANER への論文投稿数は年々増加傾向にある．扱うトピックに大きな変化はないが，Journal Reflection，LBI といった新たな試みも見られる．ソフトウェア保守に関する有益な議論の場として，今後のさらなる発展に期待したい．次回 SANER 2021 はハワイのホノルルにて 2021 年 3 月に行われる予定である．

（野田訓広，徳井翔梧／（株）富士通研究所）

会議レポート

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―

バーチャル学会 2019

2019 年 12 月 14 日，バーチャル学会の第 1 回会議となるバーチャル学会 2019[☆1] がバーチャルイベントプラットフォーム cluster（クラスター（株），日本）とソーシャル VR プラットフォーム VRChat（VRChat Inc，米国）にて行われた．近年学会開催における参加者の移動コスト削減という観点から学会のオンライン化がなされ，特に 2020 年には COVID-19 拡大により中止や延期が相次ぎ，Zoom などの遠隔会議ツールを使用したオンライン学会が行われている．また IEEE VR 2020 では Hubs（Mozilla，米国）を利用した VR 空間での研究発表がなされるなど VR 空間を利用したイベント開催やコミュニケーションは各地で行われており，こうした動きの中でユーザレベルでは VR 空間を単なる遠隔コミュニケーションの場ではなく，新しい世界の 1 つと考えコミュニティ形成や社会活動が行われている．バーチャル学会は今後高度に発達した VR 空間によりもたらされる，言ってしまえば“VR 世界”につながる社会活動の一環として VR 空間での価値創造の形を検討・共有し，それを継続して行うコミュニティを立ち上げることを目的として開催された．学会での発表内容には，VR 技術やその応用に加えて，VR 技術と直接の関係を持たない科学技術に関するものが含まれる．

当日は，cluster での基調講演と VRChat でのポスターセッションの 2 部構成にて行われた．cluster が一対多のコミュニケーションを主眼に置くのに対し VRChat は多対多のコミュニケーションに対応しているという点で異なっている[☆2]．

学会の様子はバーチャル学会公式 YouTube チャンネルとおきゅたん bot 氏のチャンネル[☆3] より YouTubeLive を通して配信された．配信のアーカイブは現在も公開されている[☆4] ため，ぜひご覧いただきたい．基調講演は会場に 100 人ほどが来場し，配信の瞬間最大視聴者数は 308 人であった．ポスターセッションでは 80 人以上が参加し，配信の瞬間最大視聴者数は 190 人であった．

基調講演

基調講演は cluster にて行われ，学術領域，産業応用，ユーザ目線という異なる背景を持つ 3 名の講演者より過去，現在，未来の VR 技術について自身の取り組みを踏まえた幅広い視点での講演がなされた．

東京大学の稲見昌彦教授は「Virtual Cyborg」というタイトルのもと，これまでの学術会議におけるオンライン会議の実施例やニコニコ学会β[☆5] といった一般向け学術イベントを紹介しつつアカデミックカンファレンスの新しい形を皮切りにバーチャルリアリティ技術の軌跡をたどった．そして，未来の VR 技術が社会をどのように変化させるか，私たちの生活はどのように豊かになるかを Human Augmentation（人間拡張）の視点から語り，学術領域の奥深さ，面白さを分かりやすく伝えた（**図 -1**）．

（株）桜花一門の桜花一門代表はコンシューマ向け HMD（Head Mounted Display）を用いたサービス開発事業を行う背景から「応用 VR 工学ってのを考えてみた」というタイトルのもと VR 技術を社会に広く普及させるために重要な明確な利益について PC 普及の流れを追いながら解説した．

（株）HIKKIY の動く城のフィオ取締役 CVO は「アバター文化の過去，現在，未来」というタイトルにて VR 空間でのコミュニケーションにおいて重要なアバターの変遷と現状の課題，それを解決する自社の取り組みを発表した．

ポスターセッション

ポスターセッションでは VRChat にて 12 件の発表が行われた．“VR 技術”，“アート”，“感覚知覚”，“アカデミック”という 4 つのセッションにて 3 件ずつの発表がなされた．セッション会場は発表者と聴講者が自由にディスカッションできるように設定されており，学会特有の新しい出会いや価値創造の場が提供された．

“VR 技術”セッションでは VR 技術を活用した取り組みや技術開発に関する発表が行われた．夜石は VR 空間における文字入力インタフェース[☆6] を開発し，VRChat 内で

☆1 https://sites.google.com/view/virtualconference-2019
☆2 執筆時 2020 年 3 月現在，cluster は多対多のコミュニケーションにも対応．
☆3 https://www.youtube.com/c/OcutanBotVRChannel
☆4 基調講演 : https://youtu.be/Tzo6hMmbmS8
ポスターセッション : https://youtu.be/bQdvQs713nY
☆5 https://niconicogakkai.tumblr.com/About
☆6 VR 用キーボード（Pieinput），https://yorunoisi.booth.pm/items/1277273

図 -1　cluster での基調講演の様子

使用できるデモの展示を行った．でちでちはスタンドアロン型 HMD である Oculus Go を使用した VR 体験の展示と普及活動から得られた知見を共有し，実社会における VR 体験の需要と効果を報告した．Voxel Kei は VR 空間における奥行きを持った映像表現手法とフォトグラメトリ技術を用いた実空間の VR 空間への再構成技術について 3D モデルを用いて報告した．特に Voxel の発表はポスターの内容が聴講者の位置によって変化するという VR 空間ならではの技法を用いており，新たな発表手法の可能性を見せた（**図 -2**）．

“感覚知覚”セッションでは人間が知覚するさまざまな感覚について考察を深める議論が行われた．Holographic[☆7] のよーへん，じゅりこは VR 空間におけるアバターを用いたコミュニケーションに求められるジェンダーロールについて報告した．VR 適性研究所のりーば，なりはららは一部ユーザより“ファントムセンス”と呼ばれる VR 空間内で生じる錯覚知覚現象についてフィールドワークを行った結果を報告した．yus998 はワイヤと DC モータを用いた振動触覚提示デバイス Hapbeat を開発し，VR 体験との親和性を報告した[☆8]．

“アート”セッションでは VR 技術を用いたアート表現に関して報告がなされた．天野ステラは VR 空間における天体教育について報告し，従来のプラネタリウムでは表現できなかった星座の奥行き表現を発表した．また，同氏はセッション会場の空を星座に書き換え聴講者を驚かせた（**図 -3**）．小江華あきは VR 空間内での漫画表現に着目し，3 次元空間内で漫画を表示するため各コマに奥行きを持たせ読者の視点に応じて画像が変化する手法を報告した[☆9]．ヨツミフレームは VRChat における自身の個展の開催結果を報告し，VR 空間における芸術展示会の実現性と来場者動向から読み取れるユーザ傾向について述べた[☆10]．

“アカデミック”セッションでは VR 技術に限らない学術領域の発表がなされ，VR 空間における学会開催の間口を広げた．固体量子は物理学分野より超伝導について紹介し，超電導の原理や身近な超電導の例を分かりやすく紹介した．しましま P は地球化学分野より生化学と地質学の境界領域にある分子の化石について発表した．アイシア＝ソリッドはデータサイエンティストの視点から VR 技術を用いた幾何的関係の可視化の有用性について発表した．

☆7 Holographic, https://www.youtube.com/c/361deg
☆8 Hapbeat, https://hapbeat.com/
☆9 VR MANGA WORLD for STYLY (image movie), https://youtu.be/0eZRNCLxz9k
☆10 VR メディアアート「1% の仮想展」, https://y23586.net/1pov/

図 -2　Voxel の発表ポスター
（左：遠くから見た場合，右：近くで見た場合）

ポスター発表に使用したすべてのポスターはバーチャル学会 2019 公式サイトより参照できるため，こちらもぜひご覧いただきたい．

VR 空間という新しい学会の場

バーチャル学会 2019 は全工程が VR 空間にて行われた．物理拠点を持たないことで会場の準備や移動にかかるコストがなくなり，運営の負担が軽減されていた．また，ビデオチャットなどを用いた従来のオンライン会議と異なり，VR 空間にアバターを用いて参加することでその“場”に存在している感覚を得ることができ，学会において重要な参加者同士のコミュニケーションが促進されていた．

当然課題もあり，現在行われている学会をそのまま VR 空間に置き換えることは現状の技術では難しい．たとえば，既存の VR プラットフォームでは数十人が同一の空間で自由に会話することは通信量や PC の処理能力の問題から難しい．また，遠隔会議全般の課題として，発表が各人の音響環境に依存しており，参加者全員の音響に対するリテラシ向上と運営からの周知徹底，トラブル対応能力が求められる．ただし最も重要なのはこれらの欠点を理解した上で VR 空間という新たな環境に合わせた運営方法や文化を形成していくことである．物理現実の学会をそのまま代替するのではなく，必要な要素を取り出して再構築する，そういった意味においても昨今の状況は新時代の学会形成を行う良い機会であることは間違いない．

大会実行委員長より

VR 空間でのコミュニケーションは急速に普及しており，ある面では現実を超えた要素を含み，今後ますます発展することは明らかです．こうした時流に抵抗なくアクセスし，活用することはいち研究者として大切にしていきたいマインドであります．依然制約の多い VR 空間ではありますが，確実に新しい世界への道は拓かれています．今後はこの流れを広く普及させ，各分野にて VR 空間における価値創造を促進できればと考えております．最後にバーチャル学会 2019 にご協力いただいた皆様にこの場を借りてお礼申し上げます．

（亀岡嵩幸／電気通信大学，バーチャル学会実行委員長）

図 -3　VRChat でのポスターセッションの様子

名 誉 会 員 の 紹 介

第 642 回（2020 年 1 月）の議を経て，下記の方が 2020 年度定時総会（2020 年 6 月 3 日）において名誉会員に推挙されました．
（記載は会員番号順）

西尾　章治郎 君
にしお　しょうじろう

1975 年 3 月	京都大学工学部卒業
1980 年 3 月	京都大学大学院工学研究科博士後期課程修了（工学博士）
1980 年 4 月	京都大学工学部　助手
1980 年 6 月～ 1981 年 5 月	カナダ・ウォータールー大学　客員研究助教授
1988 年 10 月	大阪大学基礎工学部　助教授
1989 年 10 月	大阪大学情報処理教育センター　助教授
1992 年 8 月	大阪大学工学部　教授
2000 年 4 月～ 2003 年 8 月	大阪大学サイバーメディアセンター長
2001 年 4 月～ 2008 年 3 月	文部科学省　科学官（研究振興局）
2002 年 4 月	大阪大学大学院情報科学研究科　教授
2003 年 8 月～ 2007 年 8 月	大阪大学大学院情報科学研究科長
2007 年 8 月～ 2011 年 8 月	大阪大学　理事・副学長
2015 年 8 月～現在	大阪大学　総長

本会関係略歴

（1）1983 年入会
（2）理事（1998 年度～ 1999 年度）
（3）副会長（2012 年度～ 2013 年度）
（4）会長（2017 年度～ 2018 年度）
（5）2001 年度フェロー
（6）2007 年度，2008 年度，2010 年度論文賞
（7）2010 年度功績賞

受賞

2011 年	紫綬褒章受章
2016 年	文化功労者

土井　美和子　君
（どい　みわこ）

1979 年	東京芝浦電気（株）（現（株）東芝）入社
2005 年	第 20 期日本学術会議　会員
2008 年	（株）東芝　研究開発センター　首席技監（2014 年退社）
2011 年	第 22 期，23 期日本学術会議　会員
2013 年	大阪大学　招へい教授
2014 年	情報通信研究機構　監事
2014 年	東京農工大学　客員教授
2014 年	（株）国際電気通信基礎技術研究所　客員研究員（2016 年退社）
2015 年	（株）野村総合研究所　取締役
2016 年	奈良先端科学技術大学院大学　理事
2019 年	（株）三越伊勢丹ホールディングス　取締役
現在	東北大学　理事

本会関係略歴

（1）1984 年入会
（2）理事（2004 年度～ 2005 年度）
（3）副会長（2007 年度～ 2008 年度）
（4）2001 年度 Best Author 賞
（5）2008 年度学会活動貢献賞
（6）2008 年度フェロー
（7）2009 年度功績賞

Ｚｉｄｅ　ＤＵ 君

Education

1982	B.S., Beijing Univ. for Sci & Technology, on Computer Science
1984	M.S., Inst. of Computing Tech, Chinese Academy of Sciences (CAS), Computer Architecture

Work Experience

1984 ～ 1988	Inst. of Computing Tech., CAS, Beijing, Assistant research professor, On Computer Aided Design on Architecture
1988 ～ 1989	Twente University, the Netherlands, Visiting Scholar
1989 ～ 1996	Inst. of Computing Technology, CAS, Associate Research Professor
2005 ～ 2008	President of Intel Olympiad in Informatics
2009 ～ 2015	Secretary General of ICT Committee of World Federation of Engineering Organizations
1996 ～ 2004	Deputy Secretary General of China Computer Federation (CCF)
2004 ～ Present	Secretary General of CCF

Awards

2010	Distinguished Service Award by Intl. Olympiad in Informatics

2019年度功績賞

功績賞は，情報処理に関する学術または関連事業に対し特別の功労があり，その功績が顕著な会員に贈呈されます．

本年度の受賞者は関連規程に基づき，第643回理事会（2020年3月）の議を経て，下記の3君に決定され2020年度定時総会*（2020年6月3日）において，表彰報告されました．（記載は会員番号順）

* 新型コロナウイルス感染症の影響により表彰式は中止となったため，賞状および賞牌の発送をもって表彰といたしました．

富田 悦次君
とみた えつじ

本会正会員富田悦次君（フェロー）は，永年にわたりオートマトン・言語理論，学習理論，組合せ最適化などの分野において研究と教育に携わり，先駆的で優れた業績を挙げられました．

まず同君は，決定性文脈自由言語の等価性判定問題に対し，統一的でまったく新たなアルゴリズムを考案され，合わせて，国際的にも早い段階から計算論的学習理論の新方式を提唱されました．教科書『オートマトン・言語理論』（森北出版）は初版から改訂第二版にわたって計30増刷を重ね，当分野の教育に多大の寄与をされました．また組合せ最適化問題の中では，人と人とのつながりに代表されるような大規模なネットワークデータの解析において本質的な役割を果たす，クリークと呼ばれるグラフ構造に非常に早い段階から注目し，クリーク抽出に関する研究を永年にわたり先導してきました．中でも，極大クリーク全列挙のために考案した最適アルゴリズムは，アルゴリズム分野にとどまらず，幅広い分野から活用，引用され，世界的に高く評価されています．最大クリーク抽出問題についてもいくつかの高速アルゴリズムを次々と開発し，それらは多くの引用をされ，同問題の近年発展の国際的中心の一つとなっています．これらのアルゴリズムは，共同研究として多くの応用にも巧みに活かされています．

以上に関連したいくつかの国際会議では，実行委員長，プログラム委員長，大会委員長，招待基調講演などを務められています．上記の卓越した研究業績に対しては，船井情報科学振興賞（2003年），電子情報通信学会フェロー（2003年），および本会フェロー（2003年度），などを授与されています．また極大クリーク全列挙論文は，理論計算機科学の著名論文誌であるTheoretical Computer Scienceから2005～2010年最多被引用論文賞（2010年）を受賞し，重ねて同誌の創刊40周年に際しては，出版年（2006年）論文中の最多被引用論文表彰（2015年）も受けています．なお，同論文のGoogle Scholar上引用文献数は700件超であり，出版後10数年でのこの値は理論計算機科学分野においては非常に高く，さらに現在も増加を続けています．

本会においては，会誌編集委員会主査（基礎・理論分野，1982年度～1983年度），数理モデル化と問題解決研究会主査（1999年度～2000年度），コンピュータサイエンス領域委員会委員長（2003年度～2005年度），理事（教育／調査研究担当，2005年度～2006年度）などを歴任され，特に若手研究者の育成，情報教育の充実に努められました．

以上のように，同君が，国内外の情報科学分野，ならびに本会の活動の発展に尽くした功績は，まことに顕著であります．

松本 裕治君
まつもと ゆうじ

本会正会員松本裕治君（フェロー）は，永年にわたり，自然言語処理の研究に携わり，当該分野を国際的に牽引してこられました．

自然言語処理において，形態素／統語解析，語彙知識獲得，機械学習に基づく言語処理など一貫して基盤技術に関する研究を推進し，計算言語学・自然言語処理分野を代表する研究者の1人として数多くの先駆的な業績を挙げるとともに，多数の優秀な人材の育成に貢献されています．また，基礎研究にとどまらず，種々の言語解析システムを開発し，共有可能なツールとして公開してきました．特に，形態素解析システム「茶筌」は，多くの研究開発環境で利用されており，日本語形態素解析の定番といえます．同君の自然言語処理システムの研究開発と共有化に関する努力は，我が国における自然言語処理研究，ひいては多くの関連分野に貢献されました．

経歴としては1979年に京都大学を修士で修了し，電子技術総合研究所（現，産業技術総合研究所）に入所した後，1984年には英国インペリアルカレッジ計算学科の客員研究員として論理プログラミングの研究を進め，1985年には（財）新世代コンピュータ技術開発機構の研究室長代理，1988年からは京都大学の助教授，1993年からは奈良先端科学技術大学院大学の教授として着任され，さまざまな研究を進められました．

これらの卓越した研究業績は，ASTEM ソフトウェア文化賞，日本 OSS 貢献者賞，本会フェロー，ACL Fellow や本会を含む複数の学会での論文賞などを受けており，国内外で高く評価されています．また，言語資源協会理事，本会自然言語処理研究会主査（1998 年度～ 2001 年度），本会理事（2004 年度～ 2005 年度），フェロー（2005 年度）等の要職を歴任され，計算言語学・自然言語処理分野における国際的なリーダーとして当該分野を牽引されました．

以上のように，同君が，国内外の情報処理分野の発展と教育・研究，ならびに本会の活動の発展に尽くされた功績は，まことに顕著であります

笠原　博徳　君
かさはら　ひろのり

本会正会員笠原博徳君（フェロー）は，永年にわたり並列処理技術，マルチプロセッサ・スケジューリング，自動並列化コンパイラ，マルチコアアーキテクチャの研究に従事され，多くの優れた業績を挙げられました．特に，同君が，本会での議論をベースとして，世界で初めて開発に成功したマルチグレイン並列化，プログラム全域にわたるキャッシュメモリ最適化，コンパイラによる消費電力削減等の技術は，論文誌および国際会議での論文に加え，50 件以上の国際登録特許としても発表されており，上記分野の技術発展に大きく貢献されました．

また，同君は，本会計算機アーキテクチャ研究会主査，会誌および論文誌編集委員会主査等の経験に基づき，IEEE Computer Society President，Executive Committee，Board of Governors, IEEE Technical Activity Board，文部科学省情報科学技術委員会，NSF プロジェクト評価委員会等の委員，経済産業省／ NEDO アドバンスト並列化コンパイラ・情報家電用マルチコア・グリーンコンピューティング等のプロジェクトリーダ，産業競争力懇談会理事等を歴任し，研究・人材育成・産学連携の発展に大きく寄与されました．

同君の業績は，国内外で高く評価され，本会坂井記念特別賞，IEEE CS Golden Core Member Award・Spirit of Computer Society Award，文部科学大臣表彰科学技術賞，IEEE Fellow 等を受賞されておられます．さらに，IEEE CS President として，IPSJ-IEEE CS Young Researcher Award を発足させるなど，本会の国際的プレゼンス向上にも大きな貢献をされています．

以上のように，同君が世界の情報処理分野の発展への寄与を通し，本会の活動の発展に尽くされた功績はまことに顕著であります．

各 賞 表 彰 等（概 要）

詳細は Web サイト（https://www.ipsj.or.jp/award/sho_index.html）をご覧ください

2019 年度論文賞の表彰

本賞の選考は，表彰規程および論文賞受賞候補者選定手続に基づき，論文賞委員会（委員長　湊真一）が，対象論文 563 編 * につき慎重に審議を行いました．その結果，下記の 6 編が受賞候補論文として選定され，理事会承認（2020 年 3 月 26 日付，定款上の理事会決議の省略手続きによる）を得て決定されました．

受賞者は，本会表彰規程により，6 月 3 日に開催された 2020 年度定時総会 ** において表彰報告されました．

* 選考を行ったのは「論文誌ジャーナル」「Journal of Information Processing」「論文誌コンシューマ・デバイス＆システム」「論文誌デジタルコンテンツ」「Transactions on Computer Vision and Applications」の 5 誌です．以下 7 誌については対象論文がそれぞれ 50 編に満たないため，論文賞選定は翌年以降に持ち越すこととしました．
「論文誌プログラミング」「論文誌数理モデル化と応用」「論文誌データベース」「論文誌コンピューティングシステム」「論文誌教育とコンピュータ」「Transactions on Bioinformatics」「Transactions on System LSI Design Methodology」

** 新型コロナウイルス感染症の影響により表彰式が中止となったため，表彰状などの発送をもって表彰といたしました．

【情報処理学会論文賞】

○「PR-SCTP を用いた分割ダウンロード方式における所要時間とブロック到達順序を考慮した要求方式」

［情報処理学会論文誌 Vol.60, No.2, pp.469-478（2019）］

武田　和也 君　　舟阪　淳一 君（正会員）

○「ジャミング転移による硬さおよび形状の提示が可能な食感提示システムの提案」

［情報処理学会論文誌 Vol.60, No.2, pp.376-384（2019）］

笹川　真奈 君　　新島　有信 君（正会員）
青木　良輔 君（正会員）　渡部　智樹 君（正会員）
山田　智広 君（正会員）

○「敵対的生成ネットワークを用いた 3 次元点群形状特徴量の教師なし学習」

［情報処理学会論文誌 Vol.60, No.7, pp.1315-1324（2019）］

上西　和樹 君　　古屋　貴彦 君（正会員）
大渕竜太郎 君（正会員）

【Journal of Information Processing Outstanding Paper Award】

○「Chosen Message Attack on Multivariate Signature ELSA at Asiacrypt 2017」

［Journal of Information Processing Vol.27, pp.517-524（2019）］

Yasufumi Hashimoto 君
Yasuhiko Ikematsu 君
Tsuyoshi Takagi 君（正会員）

【情報処理学会論文誌 コンシューマ・デバイス＆システム 優秀論文賞】

○「ノンストップ顔認証システムによる大規模イベントのチケット本人確認の性能改善」

［情報処理学会論文誌 コンシューマ・デバイス＆システム Vol.8, No.1, pp.27-38（2018）］

奥村　明俊 君（正会員）　星野　隆道 君
半田　　享 君　　西山　雄吾 君
田淵　仁浩 君（正会員）

【IPSJ Transactions on Computer Vision and Applications Outstanding Paper Award】

○「Effective hyperparameter optimization using Nelder-Mead method in deep learning」

［IPSJ Transactions on Computer Vision and Applications, 2017, 9:20］

Yoshihiko Ozaki 君
Masaki Yano 君
Masaki Onishi 君（正会員）

※上記（　　）の会員情報は論文掲載時のものです．

2019 年度業績賞の表彰

本会では，産業界における顕著な業績を顕彰するため，業績賞を設けております．

本賞は，情報技術に関する新しい発明，新しい機器や方式の開発・改良，あるいは事業化プロジェクトの推進において，顕著な業績をあげ，産業分野への貢献が明確になったものを選定し，その貢献者に贈呈するものです．

本年度の受賞者は，表彰規程および業績賞候補者選定手続に基づき，中川副会長を委員長とする選定委員会において厳正な審査を行い，理事会承認（2020 年 3 月 26 日付，定款上の理事会決議の省略手続きによる）を得て，下記の 3 件の業績の貢献者 12 名に決定されました．

受賞者　は，本会表彰規程により，6 月 3 日に開催された 2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため，表彰状などの発送をもって表彰といたしました．

○「世界トップクラスの性能を実現したオープンな高次元ベクトル近傍検索の開発」

岩崎雅二郎 君（正会員）　宮崎　大輔 君
加藤　優介君　　森本　浩介 君
菅原　晃平 君

○「低被ばく化 X 線透視診断装置向け映像処理技術の研究開発と実用化」

荻野　昌宏 君（正会員）　高野橋健太 君
鈴木　克己 君

○「防災や交通渋滞等の社会課題解決に寄与する「リアルタイム人口統計」の開発実用化」

寺田　雅之 君（正会員）　赤塚　裕人 君
深澤　佑介 君（正会員）　石黒　　慎 君

2019 年度情報処理技術研究開発賞の表彰

本会では，情報学の主要な分野で，その研究・開発において国際的に顕著な貢献が認められる企業所属の若手研究者を表彰するため「情報処理技術研究開発賞」を設けております．

本年度の受賞者は表彰規程および情報処理技術研究開発賞候補者選定手続に基づき，岡部副会長を委員長とする選定委員会において厳正な審査を行い，理事会承認（2020 年 1 月 31 日付，定款上の理事会決議の省略手続きによる）を得て決定されました．

受賞者は，本会表彰規程により，6 月 3 日に開催された 2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため，表彰状などの発送をもって表彰といたしました．

○「カメラ画像を用いた周辺環境認識技術の研究開発」
関　　晃仁 君（正会員）

2019 年度マイクロソフト情報学研究賞の表彰

本会では，日本マイクロソフト株式会社の協力により，情報学の主要な分野で，その研究・開発において国際的に顕著な貢献が認められる若手研究者を顕彰するため，マイクロソフト情報学研究賞を設けております．

本年度の受賞者は表彰規程およびマイクロソフト情報学研究賞候補者選定手続に基づき，岡部副会長を委員長とする選定委員会において厳正な審査を行い，理事会承認（2020 年 1 月 31 日付，定款上の理事会決議の省略手続きによる）を得て決定されました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため表彰状などの発送をもって表彰とし，2020 年度定時総会にて表彰報告いたしました．

○「統計的歌声合成技術の研究開発」
大浦圭一郎 君（正会員）

○「ユーザの情報受容性を向上させる情報提示タイミングに関する研究」
大越　　匡 君（正会員）

2020 年 IPSJ/ACM Award for Early Career Contributions to Global Research

本年の受賞者は，両学会より推薦された候補者のうち，論文実績や Global Research の観点で候補者を絞り，賞選定手続きに基づいて ACM 代表者を含む賞選定委員会において厳正な審査を行い，理事会承認（2020 年 2 月 28 日付，定款上の理事会決議の省略手続きによる）を得て決定されました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため表彰状などの発送をもって表彰とし，2020 年度定時総会にて表彰報告いたしました．

○「Mobile Interactive Systems for Intellectual Productivity Support」
矢谷　浩司 君（正会員）

2020 年 IPSJ/IEEE-Computer Society Young Computer Researcher Award

本年の受賞者は，両学会より推薦された候補者より，賞選定手続きに基づいて両学会による賞選定委員会において厳正な審査を行い，理事会承認（2020 年 2 月 28 日付，定款上の理事会決議の省略手続きによる）を得て決定されました．

* 新型コロナウイルス感染症の影響により発表の場が中止となったため，2020 年度定時総会にて報告いたしました．

○「Research on Intelligence-driven Engineering of Dependable Smart Systems」
石川　冬樹 君（正会員）

○「Outstanding Achievements on Microprocessor Architecture」
塩谷　亮太 君（正会員）

○「Outstanding Research on Human Activity Recognition for Wearable Computing」
村尾　和哉 君（正会員）

2019 年度優秀教育・教材賞の表彰

本会では，情報処理教育に関して優れた教育者ならびに教材開発者を顕彰するため，優秀教育賞ならびに優秀教材賞を設けております．

本年度の受賞者は，表彰規程および同賞候補者選定手続きに基づき，萩谷昌己情報処理教育委員長を委員長とする選定委員会において厳正な審査を行い，理事会承認（2020 年 3 月 26 日付，定款上の理事会決議の省略手続きによる）を得て，決定いたしました．

受賞者は，本会表彰規程により，6 月 3 日に開催された 2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式は中止となったため，表彰状などの発送をもって表彰といたしました．

【優秀教材賞】

○「倫倫姫と学ぼう！情報倫理：多言語情報倫理・セキュリティ教育オンラインコースの開発」
上田　　浩 君（正会員）

2019 年度学会活動貢献賞の表彰

本会では，特定分野の運営，または会員サービスの向上への貢献を顕彰するため，学会活動貢献賞を設けております．

本年度の受賞者は，表彰規程および学会活動貢献賞候補者選定手続きに基づき，選定委員会において厳正な審査を行い，理事会承認（2020 年 1 月 31 日付，定款上の理事会決議の省略手続による）を得て，決定されました．

受賞者は，本会表彰規程により，6 月 3 日に開催された 2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式は中止となった

ため，表彰状などの発送をもって表彰といたしました．

○**「学会誌における編集業務への貢献」**
　金子　　格 君（正会員）
○**「論文誌への査読貢献」**
　寺西　裕一 君（正会員）　由井薗隆也 君（正会員）
　寺田　　努 君（正会員）
○**「デジタルプラクティスへの査読貢献」**
　掛下　哲郎 君（正会員）
○**「第 81 回全国大会開催への貢献」**
　吉村　賢治 君（正会員）
○**「FIT2019 第 18 回情報科学技術フォーラム開催への貢献」**
　谷口　秀夫 君（正会員）

2019 年度感謝状の贈呈について

本会の運営等への貢献に対する感謝の意を表するため，感謝状を贈呈しております．

本年度は，規程に基づき，理事会承認（2020 年 1 月 31 日付，定款上の理事会決議の省略手続による）を得て，贈呈が決定し，6 月 3 日に開催された 2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため，表彰状などの発送をもって表彰といたしました．

○**「プログラミングコンテスト SamurAI Coding への貢献」**
　大塚　信吾 君

2019 年度ソフトウエアジャパンアワードの表彰

本会では 2004 年度から毎年産業界向けのイベントとして「ソフトウエアジャパン」を開催しており，同イベントにおいて，日本発の世界に誇るソフトウエアの研究者，開発者，技術者で，情報技術分野において特に産業界への功労がありその業績が顕著であると共に，今後の産業界への活躍が期待できる方へ「ソフトウエアジャパンアワード」を贈呈しております．

本年度の受賞者は，技術応用運営委員会，IT フォーラム推進委員会の各委員および情報処理学会フェロー，各研究会主査から推薦された候補者のうち，表彰規程およびソフトウエアジャパンアワード選定手続きに基づき，選定委員会において厳正な審査を行い，理事会承認（2020 年 3 月 27 日）を得て決定いたしました．

受賞者は，本会表彰規程により，2020 年度定時総会 * において表彰報告されました．

* 新型コロナウイルス感染症の影響により表彰式は中止となったため，表彰状などの発送をもって表彰といたしました．

○**「オープンソース脆弱性スキャナ「Vuls」の開発」**
　神戸　康多 君

2019 年デジタルプラクティス論文賞の表彰

デジタルプラクティスの目的は，ICT 実務の現場での実践やそこから生み出される知見を広く社会全体で公開共有し再利用することです．この目的に最もかなう論文を 1 年に 1 編選び「デジタルプラクティス論文賞」を贈呈しております．

本年の受賞者は，2019 年に発行されたデジタルプラクティス Vol.10, No.1 ～ No.4 の全 49 編（招待，一般投稿，推薦）の中から，表彰規程およびデジタルプラクティス論文賞選定手続きに基づき，細野繁編集委員長を委員長とする選定委員会において厳正な審査を行い，理事会承認（2019 年 12 月 17 日付，定款上の理事会決議の省略手続きによる）を得て，決定いたしました．

* 新型コロナウイルス感染症の影響により表彰式が中止となったため表彰状などの発送をもって表彰とし，2020 年度定時総会にて表彰報告いたしました．

○**深層学習によるコンクリート護岸劣化領域検出システムの開発**
　齋藤　彰儀 君　　上総　虎智 君
　平木　悠太 君　　天方　匡純 君
　吉田　武司 君

2019 年度フェローのご紹介

2019 年度「情報処理学会フェロー」は，関連規程に基づき，フェロー選定委員会において厳正な審査を行い，理事会承認（2020 年 2 月 28 日付，定款上の理事会決議の省略手続きによる）を得て，下記の 16 君に決定されました．

なお，2019 年度フェローには，2020 年度定時総会 * フェロー認証式（2020 年 6 月 3 日）において，認定報告されました．

詳細は Web サイト（https://www.ipsj.or.jp/annai/aboutipsj/fellow/fellow.html）をご覧ください．

* 新型コロナウイルス感染症の影響により認定式は中止となったため，認証状などの発送をもって認定といたしました．

○**「非構造・半構造情報処理 とデータ・クラウドセキュリティの研究開発への貢献」**
　浦本　直彦 君（正会員）
○**「動画像国際標準化および大規模データ処理技術の実用化に対する貢献」**
　栄藤　　稔 君（正会員）
○**「先駆的 ICT 人材育成および知的活動の思考プロセスの測定と分析に関する研究」**
　大場みち子 君（正会員）
○**「時間データベースに関する先駆的研究」**
　川越　恭二 君（正会員）
○**「高階モデル検査に関する研究および IFIP に対する貢献」**
　小林　直樹 君（正会員）
○**「CG における非写実的表現等の先駆的研究」**
　斎藤　隆文 君（正会員）
○**「データ工学と数理科学を中心とした教育への貢献」**
　白田由香利 君（正会員）
○**「高スケーラブルデータベース統合基盤の研究開発と標準化に対する貢献」**
　土田　正士 君（正会員）

○「組織の情報セキュリティインシデント対処技術の研究開発に対する貢献」
鳥居　悟 君（正会員）
○「国際的な女性技術者支援活動への貢献」
橋本　隆子 君（正会員）
○「広域データ通信の品質向上手法の発明ならびに実用化」
長谷川輝之 君（正会員）
○「セキュアなデータ利活用技術の研究開発」
冨士　仁 君（正会員）
○「画像処理および情報システム技術の研究開発と学会運営への貢献」
前田　章 君（正会員）
○「データ統合と群衆データベースシステム研究開発および学会運営への貢献」
森嶋　厚行 君（正会員）
○「人物顔画像分析及びアニメーション合成の研究と実用化に対する貢献」
森島　繁生 君（正会員）
○「ヒューマンコンピュータインタラクション研究領域に対する貢献」
暦本　純一 君（正会員）

● 論文誌ジャーナル掲載論文リスト
Vol.61 No.6（June 2020）
【一般論文】
■ 漸化式を用いるクンマー関数 U(a,b,x) の数値計算法と打ち切り誤差　吉田年雄 他
■ Proxy オブジェクトを用いた解析妨害 JavaScript コード解析支援システムの実現 *　上川先之 他
■ プライバシーポリシーの適切な同意取得に向けた表現・表示方法に対する利用者評価の調査　篠田詩織 他
■ 匿名加工を伴う 2 パーティ秘匿クロス集計の完全準同型暗号による実現と性能比較 *　片山源太郎 他
■ 少ない棋譜からの将棋プレイヤ棋力推定手法の提案　馬場　匠 他
■ コンテンツのユーザに与える感情を考慮したコンテンツ推薦手法の検討 *　藤田　俊 他
■ 声量制御のためのホワイトノイズ手法と音声フィードバック手法 †　竹川佳成 他
■ 集団コミュニケーションにおける挙手の印象への手の高さと人数の影響―スクリーンと VR ヘッドセットの各提示環境において―　南出　健 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
（June 2020）
【論文誌 プログラミング Vol.13 No.3】
■ Lift 中間言語における動的長配列の追加　新美和生 他

【論文誌 教育とコンピュータ Vol.6 No.2】
■ 我が国の小中学校を対象とした教育の情報化の進展　東原義訓
■ 大学教育における学習分析の活用事例　島田敬士
■ プログラミング学習支援ツール pgtracer を自学習に活用した授業実践と学習行動の分析　村田美友紀 他
■ 自然言語処理と可視化を利用した履修選択支援システムの実用化　美馬秀樹
■ 小テストの点数パターンによる学習者のクラスタリングとその推定　古川雅子 他

IPSJ MAGAZINE Vol.61 No.7 (July 2020)

CONTENTS

Preface

662 **Augmented Reality is Information Processing That is Not as Textbooks**
Tom KAWADA (AR3Bros. The First-born Son)

Special Features

Cyber Wars

664 **0. Foreword**
Katsue NAGAKURA and Arisa EMA (The Univ. of Tokyo)

666 **1. Increasing Sophistication of Attack Strategies as Attack Surface Grown**
Toshio NAWA (Cyber Defense Institute, Inc.)

672 **2. Boosting Cybersecurity with Machine Learning Techniques**
Takeshi TAKAHASHI, Keisuke FURUMOTO and Chansu-Han (National Institute of Information and Communications Technology)

678 **3. The ICT and National Security : An Issue for Strategic Analysis**
Heigo SATO (Takushoku Univ.)

687 **4. On Tallinn Manual : International Law Concerning Cyber Attacks**
Kazuhiro NAKATANI (Graduate Schools for Law and Politics, Univ. of Tokyo)

693 **5. Russian Intelligence Organs and ICT**
Yu KOIZUMI (Research Center for Advanced Science and Technology, The Univ. of Tokyo)

700 **6. Engineers and Cyber Wars**
Satoshi KURIHARA (Keio Univ.), Fujio TORIUMI (The Univ. of Tokyo), Kazuhiro TAIRA (J. F. Oberlin Univ.), Masahiro SUGAWA (Niigata Univ.), Katsue NAGAKURA and Arisa EMA (The Univ. of Tokyo)

Goodbye, Fatuous Encrypted Zip Attachments

706 **0. Foreword - Ceremony Security PPAP : Towards the Renaissance of Information Security in Japan (Goodbye Automated Password Protected ZIP Mail)**
Nat SAKIMURA (NAT. Consulting LLC.)

708 **1. What is PPAP? - The Dark History of Its Development -**
Akira OTAISHI (PPAP Research Institute)

714 **2. Security Blurriness of PPAP**
Masanori KUSUNOKI (Center for Global Communications, International Univ. of Japan)

719 **3. Why Do We E-mail Both Password-protected Zip Files and Their Passwords?**
Tetsutaro UEHARA (Ritsumeikan Univ.)

724 **5. Discussion "How to Get Rid of PPAPs from Society?"**
Nat SAKIMURA (NAT. Consulting LLC.), Akira OTAISHI (PPAP Research Institute), Masanori KUSUNOKI (Center for Global Communications, International Univ. of Japan) and Tetsutaro UEHARA (Ritsumeikan Univ.)

"Peta-gogy" for Future

735 **Informatics Research Contest for Junior and Senior High School Students during the High Alert due to Novel Coronavirus**
Yasuichi NAKAYAMA (The Univ. of Electro-Communications)

736 **As a Person in Charge of Subject "Information"/ Information Studies Participate in Curriculum Management**
Takeharu TASAKI (Tokyo Metropolitan School Management Support Center Central)

740 **Primary and Secondary Education of Informatics in Sri Lanka**
Ben Tsutom WADA (Nagano Univ.)

Algorithm Starting from Scratch

744 **What to Solve?**
Yoshifumi MANABE (Kogakuin Univ.)

Let's Learn Informatics

748 **Trial and Error of ICT Utilization in Elementary School**
Masai NABEYA (Sendagaya Elementary School)

Series : Pilgrimage to Vintage Computers / Trail Blazers' Recollections of 0's and 1's

762 **2019 Nomination of the Information Processing Technology Heritages**
Hiroharu ASAHI (Secretary of the Committee of History of Computing)

753 **Gathering to Share Original Programming Projects for Junior**
754 **Biblio Talk**
756 **Skimming a Famous Paper in Five Minutes**
759 **Shopping Boast**
760 **Questions for Experts**
766 **Conference Report**
768 **Conference Report**
780 **IT Travelog Manga**

次号（8 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」プログラミング教育の最前線
ついに始まった小学校プログラミング教育―その現状と課題―／プログラミングもあそびになる．ロボット工学が身近になるロボットトイ「toio」／Maker Education　作ることを通して学ぶ／プログラミングの大衆化が始まった／地域におけるプログラミング学習コミュニティ　CoderDojo の果たす役割／創造はじめのいっぽ，Apple I/TK-80/MSX が生んだ感動をすべてのこどもたちへ！

「小特集」中高生の情報教育に関する支援活動―第 82 回全国大会を中心に―
中高生情報学研究コンテストの発展に期待する／中高生情報学研究コンテストの概要・意義・効果／中高生情報学研究コンテストの審査の様子／中高生情報学研究コンテストの作品紹介／教員から見た中高生情報学研究コンテスト―教科「情報」と「総合的な探究の時間」の連携―／初等中等教員研究発表セッション―情報処理学会第 82 回全国大会―

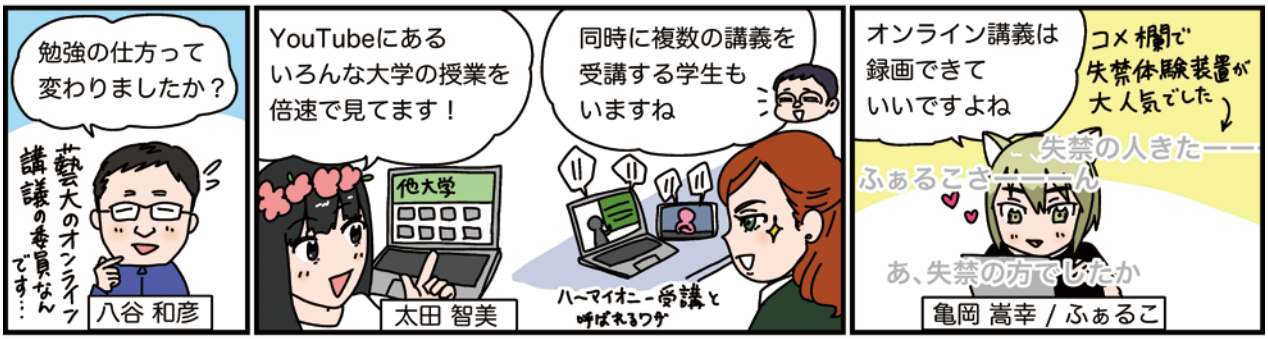
報告：2019 年度論文賞の受賞論文紹介／ 2019 年度業績賞紹介／ 2019 年度マイクロソフト情報学研究賞紹介／ 2019 年度情報処理技術研究開発賞紹介

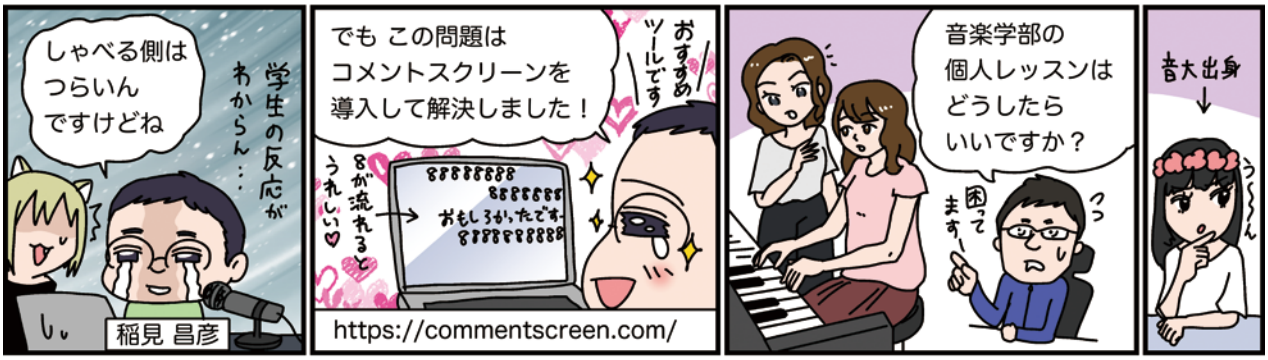
教育コーナー：ぺた語義
連　載：IT 紀行／買い物自慢／ 5 分で分かる !? 有名論文ナナメ読み／先生，質問です！／ビブリオ・トーク
コラム：巻頭コラム
会議レポート：DATE 2020 会議報告

その9 ニコニコ学会βの逆襲！！ これからのイノベーションの在り方を考えてみた

漫画：山本ゆうか（Twitter @ymmox）

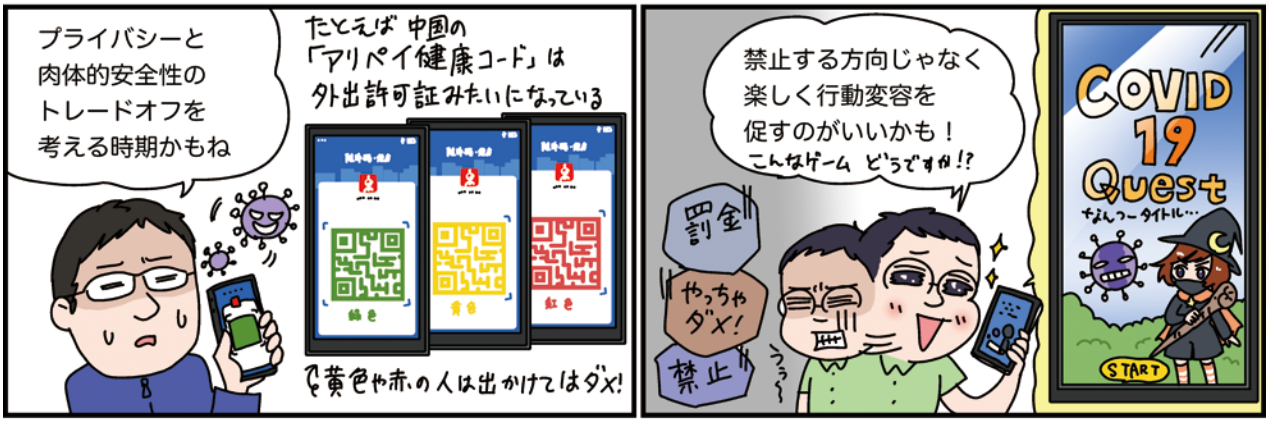
授業について考えてみた





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

プライバシーと行動トラッキングについて考えてみた



研究について考えてみた

まとめ(?)

お知らせ

- 2020年12月中旬にバーチャル学会を開催予定です！アカデミックな内容なら分野は問いません．ぜひご応募ください！
  https://sites.google.com/view/virtualconference2020/home
- Tsukuba Mini Maker Faire 実行委員会ではメイカーのアイディアや技術を防災に応用することを目的とした公募プログラム「防災テックチャレンジ」を開催しています．目に見えないウイルスと戦う防災をテーマに何か作ってみてはいかがでしょうか？
  https://tmmf.jp/2020/?p=2384 （2020年6月30日締切）

今月の会員の広場では，4月号へのご意見・ご感想を紹介いたします．まず，特集「新たなモビリティ時代のサイバーセキュリティ」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．

■モビリティというと，車の自動運転を思い浮かべたが，陸•海•空それぞれにあることを改めて認識した．（匿名希望）

■できれば，個々のモビリティだけでなく，それらが連携したMaaSや，モビリティをセンサとして組み込んだ社会システムに対する課題も知りたいところでした．編集者が触れていたように，それは次のテーマとして楽しみにしています．（匿名希望）

「2. 自動車分野のCASE革命とサイバーセキュリティ」
■CASE革命のそれぞれの要素に対してどのようなセキュリティの課題があるかを分かりやすく，しかも網羅的に解説していただき，納得感のある良い記事であった．（伊藤雅樹）

「3. 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ」
■鉄道で用いられるシステムのどこにどういうセキュリティリスクが潜んでいて，どう対策を取っているかといった記事を期待したが，そうした具体的な内容が薄かったのが残念．もちろん，書くことでリスクが上昇する危険もあるのだが，そんなリスクを上回るほどの対策がなされていると信じている．（伊藤雅樹）

連載「買い物自慢：GR IIIでスマートフォンとカメラの二刀流生活」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．

■書き手のこだわりが見えて「買い物自慢」の記事を毎回楽しみにしています．もちろんこのままで記事が続くならその記事を読みたいですが．会員に公募するとか，賛助企業等のイチオシ製品のモニタを仲介して紹介してみるなどの可能性もあるかな?と考えています．ぜひ長く続いてほしいと思っています．
（滝内邦弘）

解説「高専プロコン30年の歩み」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．

■高専プロコンがどうやってつくられたのか，陰でどのような人が努力しているのかがよく分かったので良かったです．
（匿名希望／ジュニア会員）

連載「ビブリオ・トーク：人工知能を活用した研究開発の効率化と導入•実用化《事例集》」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．

■書評ではなく，目次の羅列のようだった．（匿名希望）

連載「情報の授業をしよう!:情報Iを意識した授業をしよう！」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．

■Good practice, Good trialで，多くの教員に参考になる記事だと思う．（匿名希望）

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．

■「先生，質問です!」の「情報は地球を何秒で周るか」という質問に対して，2人の回答者の解釈がまったく異なっているのが興味深かった．（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．

■専門家の先生だけではなく，幅広い会員から意見を出し合うような場を作って，それをピックアップしていただくような会誌になると，オンラインになる意味があるのではないかと思います．（匿名希望）

■内容が専門的なので，最初になぜこの内容を選定したのか意図と図解で明示してもらえるとありがたいです．（匿名希望）

■《連載：5分で分かる!? 有名論文ナナメ読み》Mark Weiser : Program Slicing（石尾 隆）のように，専門家の方は知っているが，初心者にはあまり知られていない技術の紹介の記事があると嬉しいです．（武藤熙麟／ジュニア会員）

■それぞれ一見関連がないような記事が，実は関係あるかもしれないといったAI推論的な情報が提供されると想像力（創造力）発揮の一助になるかもしれません．（匿名希望）

■新型コロナウイルスの感染拡大に伴い，本会関係で多数の方が対策，対応，解決などにかかわっているかと思います．その知見を会誌よりも素早くオンラインで公開いただけたら，他分野の方も参照できて役に立つのではないかと思いました．
（匿名希望）

■キーワード検索，ネットワーク検索，キーワードのネットワーク表示などデータの可視化年表．（匿名希望）

■オンライン版になると，よりタイムリーな企画・編集が可能になるでしょうか．現在，オンライン授業の必要性が突然生じていますが，オンライン用のカメラやマイクなどの話から，オンラインシステムについて，また，中高生，大学生向けの授業

の展開案など，次号ですぐに読むことができるようになっているとよいだろうと切実に思いました．（柏野和佳子）

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．

■評価しながらすべての記事を読むのは初めての経験でした．モニタでなければ恐らく読まなかったと思われる記事の中にも興味深い記事が多数あること，学会が情報処理の普及のため会員以外の人・組織に対しても幅広く活動していることなどが分かり大きな収穫でした．（匿名希望）

■世の中，コロナウイルス（とオリパラ延期）で大混乱だが，テレワークが一気に加速した．テレワークにはITが不可欠であり，どのような技術・サービスが支えているのか，特集しても面白いだろう．（伊藤雅樹）

■今世界的に問題となっているコロナウイルスと関連する医療とICTとのかかわりについてです．たとえば，病気内容のみならず，発病した人の足取りや感染経路を分析するための手法等の議論が聞けると嬉しく思います．（匿名希望）

■香川県のゲーム条例について，本会の会員の人の考えを聞きたいです．（匿名希望／ジュニア会員）

■ VRの未来予測．（匿名希望）

■リモートワークの課題について．（匿名希望／ジュニア会員）

■立花孝志（ネットでの政策投票システムについて）（國武悠人／ジュニア会員）

■小中高の教育者のためのWGを作り，教育専門の議論をすることが大切です．（匿名希望）

■論文誌で多く読まれている論文のランキングや要旨をまとめたものがたまにあると，研究者ではない読者に論文誌への興味が持てると思う．（角田洋太郎／ジュニア会員）

■量子ソフトウェア研究会が開設されたこともあり，量子コンピューティング関連の特集があってもよいのではないか．過去にも特集はあったが，「基本原理の分かりやすい解説」等と「専門的で高度な内容」の間を埋めるものが足りないと感じている．（匿名希望）

■セミナーやソフトウエアジャパンなどのイベントで取り上げられているテーマを紹介していただきたいです．（匿名希望）

■世界中の人々の行動が大きく変わっている今，ICTの使い方も大きく変わってきているはずなので，たとえばネットワークの帯域使用量の変化など，分野別にまとめて，現状と取り組み状況や今後の対応などについて解説していただけるとありがたいです．（匿名希望）

■最近おしゃれな誌面になっていると感じていましたが，今号は特に特集や解説のデザインが良いと思いました．（柏野和佳子）

■著者の立場では既知だとしても，非専門者から見たら既知でない用語や概念が多い業界なので，著者各位には丁寧な解説を求めたい．（匿名希望）

【本欄担当　大岸智彦・荒　宏視／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「組込みシステム工学」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-M.html	6月18日(木)		
	論文誌トランザクションデジタルプラクティス 「変革の先にあるコンタクトセンター」特集論文募集 https://www.ipsj.or.jp/dp/cfp/tdp0102s.html	7月17日(金)		
	論文誌「ソフトウェア工学」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-H.html	8月3日（月）		
	論文誌「情報システム論文」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-L.html	8月7日（金）		
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）	5月29日(金)	★オンライン開催
6月25日（木）	第178回コンピュータグラフィックスとビジュアル情報学 研究発表会 https://www.ipsj.or.jp/kenkyukai/event/cg178.html	5月28日(木)	当日のみ	慶應義塾大学
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21日(木)	当日可 要マイページより申込	★オンライン開催
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）	当日可 要マイページより申込	★オンライン開催
6月29日（月）	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14日(木)	当日可 要マイページより申込	★オンライン開催
7月2日(木)	第205回ソフトウェア工学研究発表会 https://www.ipsj.or.jp/kenkyukai/event/se205.html	5月11日(月)	当日可 要マイページより申込	★オンライン開催
7月3日(金)～ 7月4日(土)	第244回自然言語処理研究発表会 https://www.ipsj.or.jp/kenkyukai/event/nl244.html	5月28日(木)	当日可 要マイページより申込	★オンライン開催
7月9日(木)～ 7月10日(金)	第117回ドキュメントコミュニケーション研究発表会 https://www.ipsj.or.jp/kenkyukai/event/DC117.html	5月19日(火)	当日可 要マイページより申込	★オンライン開催
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22日(金)	当日のみ	アクロス福岡
7月20日（月）～ 7月21日（火）	第90回コンピュータセキュリティ・第38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/csec90spt38.html	5月14日(木)	当日のみ	札幌コンベンションセンター
7月27日（月）	第129回数理モデル化と問題解決研究発表会 https://www.ipsj.or.jp/kenkyukai/event/mps129.html		当日のみ	Luxor "MGM Resorts' International'(ラスベガス)
7月29日（水）	The 4th cross-disciplinary Workshop on Computing Systems, Infrastructures, and Programming（xSIG2020） http://xsig.hpcc.jp/2020/	3月6日（金）		フェニックス・プラザ （福井市民福祉会館）
7月29日（水）～ 7月31日（金）	第175回ハイパフォーマンスコンピューティング研究発表会 （SWoPP2020） https://www.ipsj.or.jp/kenkyukai/event/hpc175.html	5月26日(火)	当日のみ	フェニックス・プラザ （福井市民福祉会館）
7月29日（水）～ 7月31日（金）	第150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（SWoPP2020） https://www.ipsj.or.jp/kenkyukai/event/os150.html	5月26日(火)	当日のみ	フェニックス・プラザ （福井市民福祉会館）
7月29日（水）～ 7月31日（金）	第233回システム・アーキテクチャ研究発表会（SWoPP2020） https://www.ipsj.or.jp/kenkyukai/event/arc233.html	5月26日(火)	当日のみ	フェニックス・プラザ （福井市民福祉会館）
7月29日（水）～ 7月31日（金）	第130回プログラミング研究発表会（SWoPP2020） https://sigpro.ipsj.or.jp/pro2020-2/	5月26日(火)	当日のみ	フェニックス・プラザ （福井市民福祉会館）
7月31日（金）	第139回情報基礎とアクセス技術研究発表会 https://www.ipsj.or.jp/kenkyukai/event/IFAT139.html	6月25日(木)	当日可 要マイページより申込	★オンライン開催
8月27日（木）	2020年度電気関係学会東北支部連合大会 https://www.ecei.tohoku.ac.jp/tsjc/index.html	6月25日(木)		★書面発表
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/			★オンライン開催

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3日(木)～ 9月4日(金)	令和2年度電気・電子・情報関係学会東海支部連合大会 https://www.ipsj-tokai.jp/rengo2020/	7月8日(水)		★オンライン開催
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12日（土）	2020年度電気・情報関係学会北陸支部連合大会 http://2020.jhes.jp/			福井大学 文京キャンパス
9月20日（日）	2020年度関西支部　支部大会 https://kansai.ipsj.or.jp/sibutaikai_2020/	6月12日(金)		大阪大学 中之島センター
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	★オンライン開催
10月13日（火）	連続セミナー2020「IoTやAIを支えるデータ流通基盤」 https://www.ipsj.or.jp/event/seminar/2020/		当日可 要マイページより申込（準備中）	★オンライン開催
10月26日（月）	連続セミナー2020「人工知能技術と人間の思考・感性」 https://www.ipsj.or.jp/event/seminar/2020/		当日可 要マイページより申込（準備中）	★オンライン開催
11月11日（水）	連続セミナー2020「AI技術の産業応用：現在と未来」 https://www.ipsj.or.jp/event/seminar/2020/		当日可 要マイページより申込（準備中）	★オンライン開催
12月14日（月）	連続セミナー2020「量子コンピュータとソフトウェア」 https://www.ipsj.or.jp/event/seminar/2020/		当日可 要マイページより申込（準備中）	★オンライン開催

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
3月10日(水)～ 3月12日(金)	インタラクション2021 https://www.ipsj.or.jp/kenkyukai/event/s-hi2021.html			学術総合センター 一橋講堂
3月18日(木)～ 3月20日(土)	情報処理学会　第83回全国大会 https://www.ipsj.or.jp/event/taikai/83/			大阪大学 豊中キャンパス

Webページ（https://www.ipsj.or.jp/）更新情報

［トピックス］

5月15日	人材募集情報（Vol.61 No.6）
5月15日	会誌「情報処理」Webカタログ（Vol.61 No.6）
5月15日	論文誌「組込みシステム工学」特集 論文募集
5月12日	論文誌「ネットワークサービスと分散処理」特集 論文募集
5月7日	FIT2020 講演申込の受付を5月13日15時まで延長しました
5月6日	FIT2020 オンライン開催について
4月30日	「情報科学の達人」育成官民協働プログラムをスタート
4月28日	2020年度定時総会の開催について
4月28日	2020年度「C&C賞」候補者推薦について
4月28日	インターンシップ情報（広告）のお申し込み受付中
4月22日	情報処理学会創立記念日に寄せて
4月17日	論文誌「情報システム論文」特集 論文募集

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

■学校法人奈良学園

募集人員　学内システム技術担当者（事務職員）　1 名
応募資格　情報通信技術（コンピュータおよびネットワーク）について専門的知識を有し，新しい技術に積極的に取り組む意欲のある方
採用年月日　可能な限り早い時期（採用内定後調整）
提出書類　履歴書，職務経歴書（既卒者），最終学校卒業証書（写）または卒業見込証明書，最終学校成績証明書
業務に関連する資格を有している場合そのコピー
応募締切　随時
送 付 先　〒 636-8503 奈良県生駒郡三郷町立野北 3-12-1
Tel(0745)73-6561
照 会 先　事務局総務部人事課　事務職員採用係
そ の 他　【雇用期間】雇用期間の定めなし
【勤務地】法人本部事務局　奈良県生駒郡三郷町立野北 3-12-1
【詳細】http://www.naragakuen.jp/jobs/

■国立情報学研究所

募集人員　准教授，助教　あわせて若干名（任期は 5 年間．教授採用を考慮する場合もある．なお，採用後，優れた業績を出された場合は，昇任または任期のない職への任用を行う場合があります）
研究開発分野　①情報学プリンシプル研究分野，②アーキテクチャ科学研究分野，③コンテンツ科学研究分野，④情報社会相関研究分野
応募資格　原則として博士の学位取得または取得見込みの方（人文・社会科学系の研究者にあっては，これに準ずる方を含む）
着任時期　原則として 2021 年 4 月 1 日
提出書類　(1) 履歴書，(2) 研究業績（論文，著書リストおよび主要業績 3 編について，併せて添付すること），(3) 学会における活動状況，(4) 職域における活動状況，(5) 社会における活動状況，(6) 推薦書／照会先，(7) 就任後の抱負：任意の様式による（2,000 字程度）．このうち (1) から (5) は後述の Web ページから所定様式をダウンロードし，その様式に従って作成してください．なお (6) と (7) は自由形式とします
応募締切　2020 年 6 月 26 日（必着）
送 付 先　〒 101-8430 東京都千代田区一ツ橋 2-1-2
「情報・システム研究機構国立情報学研究所長」宛
「応募書類在中（研究教育職員）」と朱書し，書留郵便等，配達証明相当がある方法にて送付のこと
照 会 先　国立情報学研究所　総務部総務課人事チーム
E-mail: koubo2020@nii.ac.jp
そ の 他　書類審査および面接による．面接は書類審査合格者を対象とし，これにかかわる旅費，宿泊費等は自己負担となります．応募にあたっては，必ず国立情報学研究所 研究教育職員 公募要領の Web ページ（http://www.nii.ac.jp/about/recruit/）に従って，提出書類を作成・送付してください

■豊橋技術科学大学情報・知能工学系

募集人員　助教　1 名（任期：5 年（再任は審査により 1 回限り 3 年，最長 8 年まで））
専門分野　音声言語処理（音響処理・言語処理を含む音声言語情報全般），またはマルチモーダルインタラクション技術（音声を中心とした多モダリティを用いるインタフェースなど），または自然言語処理（機械学習に基づく言語処理全般）
担当科目　情報・知能工学にかかわる演習や実験などの科目
着任時期　2020 年 11 月 1 日以降なるべく早く
応募締切　2020 年 6 月 30 日（必着）
照 会 先　情報・知能工学系　教授　北岡教英
E-mail: kitaoka@tut.jp
そ の 他　提出書類・提出先など詳細：https://www.tut.ac.jp/about/docs/koubor2.4.23.4j.pdf

■豊橋技術科学大学メディア・ロボット情報学分野

募集人員　助教　1 名（任期：5 年（再任は審査により 1 回限り 2028 年 3 月 31 日まで））
専門分野　CG や画像などの視覚的なメディアコンテンツに関連する研究分野
応募資格　博士の学位を有し（または，着任までに取得見込みであり），専門分野に業績があり大学院学生の研究指導補助ができ，

情報系の実験科目の担当が可能な方
着任時期　2020 年 11 月 1 日以降のできるだけ早い時期
提出書類　1）履歴書（学歴, 職歴, 受賞等, メールアドレス明記), 2）研究業績リスト（学術論文, 国際会議論文（査読付き), 著書, 解説論文, 特許などに分けて記載), 3) 主要論文別刷 (3 編以内), 4) 学会・社会における活動状況, 5）外部資金の獲得実績, 6）これまでの研究活動の概要（A4 で 2 枚程度), 7）着任後の教育研究の抱負（A4 で 2 枚程度), 8）所見を伺える方 1 名以上の連絡先
応募締切　2020 年 6 月 30 日（必着）
送 付 先　〒 441-8580 愛知県豊橋市天伯町雲雀ケ丘 1-1
豊橋技術科学大学情報・知能工学系　北崎充晃
封筒の表に「教員応募（情報・知能工学系：メディア・ロボット情報学分野助教)」と朱書し, 簡易書留で郵送してください
＊提出書類は原則として返却いたしません
照 会 先　情報・知能工学系　栗山　繁
E-mail: sk@tut.jp　Tel(0532)44-6737
そ の 他　【選考方法】第 1 次選考（提出書類による選考), 第 2 次選考（プレゼンテーションを含む面接)
詳細は, 当大学法人の Web ページ (https://www.tut.ac.jp/about/docs/koubor2.4.23.1j.pdf) をご覧ください

■大阪電気通信大学総合情報学部情報学科

募集人員　准教授または講師　1 名
専門分野　メディア情報学（人工知能処理, 拡張現実感, モバイルアプリケーション等)
着任時期　2021 年 4 月 1 日までのできるだけ早い時期
応募締切　2020 年 7 月 31 日（必着）
照 会 先　総合情報学部情報学科　主任　南角茂樹
E-mail: nankaku@osakac.ac.jp（件名を「情報学科公募」)
そ の 他　詳細「大阪電気通信大学 専任教員（総合情報学部 情報学科）の公募について」
https://www.osakac.ac.jp/etc/recruit/96

■富山大学学術研究部工学系

募集人員　助教　2 名（1 名は女性限定)【任期】5 カ年, 再任可
所　　属　学術研究部工学系（工学部工学科電気電子工学コース担当)
専門分野　電気電子工学分野
応募資格　着任時までに, 博士または Ph.D. の学位を有し, 大学院修士課程および博士課程における教育・実験指導が担当できること
着任時期　2020 年 11 月 1 日以降のできるだけ早い時期
応募締切　2020 年 7 月 31 日（必着）
提出書類／送付先　詳細は URL を参照
照 会 先　工学部工学科電気電子工学コース　コース長　中　茂樹
E-mail: nak@eng.u-toyama.ac.jp　Tel(076)445-6731
URL: https://www.u-toyama.ac.jp/outline/employ/index.html

ご意見をお寄せください！

【7 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 7 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：教科書通りじゃない情報処理，それが拡張現実…… 10-1-［　］
特集：サイバー・ウォーズ
0. 編集にあたって …… 10-2-［　］
1. 攻撃対象領域の増大に伴い高度化する攻撃戦略 …… 10-3-［　］
2. 機械学習を用いたサイバーセキュリティ技術の発展 …… 10-4-［　］
3. 情報通信技術（ICT）と安全保障…… 10-5-［　］
4. タリン・マニュアルについて …… 10-6-［　］
5. ロシアのインテリジェンス機関と ICT …… 10-7-［　］
6. 座談会：技術者とサイバー・ウォーズ …… 10-8-［　］
小特集：さようなら，意味のない暗号化 ZIP 添付メール
0. 編集にあたって …… 10-9-［　］
1. PPAP とはなにか …… 10-10-［　］
2. PPAP のセキュリティ意義 …… 10-11-［　］
3. 我々はなぜ PPAP するようになってしまったのか …… 10-12-［　］
4. 座談会「社会から PPAP をなくすには？」…… 10-13-［　］
ぺた語義：新型コロナウイルスと中高生情報学研究コンテスト…… 10-14-［　］
ぺた語義：教科「情報」・情報教育の担当者としてカリキュラム・マネジメントに参画する …… 10-15-［　］
ぺた語義：スリランカの初等中等情報教育…… 10-16-［　］
ゼロからはじめるアルゴリズム：最初に考えること：何を行うのか…… 10-17-［　］
情報の授業をしよう！：小学校における ICT 活用の試行錯誤 …… 10-18-［　］
連載：集まれ！ジュニア会員 !! …… 10-19-［　］
ビブリオ・トーク：センスメイキング…… 10-20-［　］
5 分で分かる !? 有名論文ナナメ読み：Lee Organick et al : Random Access in Large-Scale DNA Data Storage …… 10-21-［　］
買い物自慢：子供とプログラミングで遊べるトイドローンを買ってみた…… 10-22-［　］
連載：先生，質問です！…… 10-23-［　］
古機巡礼 / 二進伝心：2019 年度情報処理技術遺産および分散コンピュータ博物館 …… 10-24-［　］
会議レポート：SANER 2020 会議報告 …… 10-25-［　］
会議レポート：バーチャル学会開催後記…… 10-26-［　］
IT 紀行：ニコニコ学会βの逆襲！！　これからのイノベーションの在り方を考えてみた…… 10-27-［　］

〔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〕サイバー・ウォーズ：a）専門家　b）非専門家 …… 13-1-［　　］
〔13-2〕さようなら，意味のない暗号化 ZIP 添付メール：a）専門家　b）非専門家 …… 13-2-［　　］

〔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 ■

「特集が出るのが夏だからサマーウォーズならぬ，サイバー・ウォーズにしよう」このようにして特集の名称は決まった．細田守氏が監督の『サマーウォーズ』（2009 年）は，サイバー空間上での謎の人工知能との戦争を描いた映画である．10 年以上たった現在，サイバー空間と現実空間は想像以上に関係し合い，深刻化している．国という単位での安全保障においても，陸海空という従来の三領域に加え，サイバー空間は宇宙と並んで重要領域と見なされている．さらにはフェイクニュースなどの「攻撃」も，民主主義の脅威として兵器扱いされるなど，サイバー空間における課題はこの 10 年で解決するどころか，拡張の一途をたどっている．

しかし，課題に対して技術的に対策をとること，法律で対応すること，国際的な連携で囲い込むこと，技術者の倫理観の醸成を行うことなど，とれる対策は多様にある．本特集では，各分野の専門家がそれぞれの「戦場」で見聞きしてきたことを寄稿いただいた．この戦争は情報系の研究者だけではなく，さまざまな人たちとの協力と連携があって対応できるものだと改めて特集を通じて考えさせられた．

2020 年 5 月現在，私たちは COVID-19 という敵との終わりの見えない戦いにさらされている．医療や教育が遠隔になり，テレワークも導入されるなど，私たちの生活や仕事空間は，かつてないスピードでサイバー空間上へと移行している．サイバーウォーズは，他人事ではなく，私たち一人ひとりが意識し取り組むべきものだ，ということを，今こそ心にとどめておく必要があるだろう．

（江間有沙／本特集エディタ）

まず最初にお詫びをしたい．このような特集では，本来は賛成派と反対派の両方の意見を載せるべきである．そうであって，はじめて適切な議論となるはずである．だが，今回は，PPAP 賛成派または推進派の原稿を載せることができなかった．書いていただける推進派は見つけられなかった．

もし次回があるのであれば，そのような推進派の方を交えて，より本質を突いた議論を行いたい．そうすることで，はじめて問題解決の糸口が見えてくると考えられる．

この意味のない暗号化 ZIP 添付メールの問題は，「部屋の中の象」である．「部屋の中の象」とは，誰もが目にして問題であると認識しているのに，どうにも対応しようがなく，その問題がそのまま居座り続けているというものである．

私たちはセキュリティや UI･UX について，さんざん議論し，研究対象としてきている．「情報処理」でも何度も扱ってきている．この分野への技術投資はすさまじい金額のはずだ．

だが，そのような私たちの努力をあざ笑うかのように，PPAP は今日も私たちの目の前に存在している．

私は研究とは，「目の前にある問題」を解決できなければならないと考えている．この目の前にある巨大な問題を解決できずに，セキュリティや UX を論じるのは，そもそもおかしいのではないだろうか．

今回は，理想的な先生方に原稿を執筆していただき，議論していただいた．今回の小特集が，この巨大な問題を解決する糸口となることを期待している．

（江渡浩一郎／本小特集エディタ）

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 7 号　掲載広告（五十音順）

□インタフェース …… 表 2
□オージス総研 …… 表 2 対向

□ すべての会社を希望

■資料送付先

フリガナ
お 名 前 ＿＿＿＿＿＿＿＿＿＿

勤 務 先 ＿＿＿＿＿＿＿＿＿＿ 所属部署 ＿＿＿＿＿＿＿＿＿＿

所 在 地 （〒　　-　　） ＿＿＿＿＿＿＿＿＿＿

TEL（　　）　　-　　FAX（　　）　　- ＿＿＿＿＿＿＿＿＿＿

ご専門の分野 ＿＿＿＿＿＿＿＿＿＿

お問合せ・お申込み・資料請求は

広告総代理店 アドコム・メディア（株）

Tel.03-3367-0571　Fax.03-3368-1519　E-mail: sales@adcom-media.co.jp

賛助会員のご紹介

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

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

●●● 賛助会員（20 ～ 50口）

（株）日立製作所

富士通（株）

日本電気（株）

三菱電機（株）

（株）サイバーエージェント

日本アイ・ビー・エム（株）

●●● 賛助会員（10 ～ 19口）

（株）リクルート

グーグル合同会社

（株）NTT ドコモ

（株）東芝

日本電信電話（株）

日本マイクロソフト（株）

（株）フォーラムエイト

●●● 賛助会員（3 ～ 9口）

（一社）情報通信技術委員会

（株）NTT データ

グリー（株）

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）

●●● 賛助会員（2口）

（株）KDDI 研究所

NEC ソリューション
イノベータ（株）

NTT アドバンステクノロジ（株）

鉄道情報システム（株）

（株）ナレッジクリエーション
テクノロジー

（一財）日本データ
通信協会

（一財）日本規格協会

日本放送協会
放送技術研究所

（株）日立システムズ

【A～Z】

Arithmer（株）
（株）ATJC
（株）ATR-Trek
bokk（株）
（株）CIJ
（株）CIJネクスト
（株）CyberOwl
合同会社DMM.com
freee（株）
GMOペパボ(株)
（株）GV
（株）HBA
JapanTaxi（株）
JRCエンジニアリング(株)
（株）ＪＲ東日本情報システム
（株）JTB川崎支店
（株）K＆S
（株）KDDI総合研究所
MHIエアロスペースシステムズ(株)
NECソリューションイノベータ(株)
NECネットイノベーション(株)
NECフィールディング(株)
NTTアドバンステクノロジ(株)
NTTコムウェア(株)
（株）NTTデータ
（株）NTTデータ・アイ
（株）NTTデータ関西
（株）NTTデータ九州
（株）NTTデータ数理システム
（株）NTTデータ東北
NTTテクノクロス(株)
（株）NTTドコモ
（株）OKIソフトウェア
（株）PFU
（株）PLAY
（株）POL
（株）QUICK
SCSK（株）
（株）Spelldata
TDCソフト(株)
TIS（株）
（株）UNCOVER TRUTH
YKK（株）

【あ行】

アイアンドエルソフトウェア(株)
(株)アイヴィス
アイシン・エィ・ダブリュ（株）
アイシン精機(株)
アイシン・ソフトウェア(株)
(株)アイズファクトリー
(株)アイ・ピー・エス
アイホン(株)
(株)アイレップ
アシアル(株)
(株)アットウェア
(株)アドバンスト・メディア
(株)アドバンス トラフィック システムズ
アビームシステムズ(株)
(株)アピリッツ
(株)アルファシステムズ
(株)アルフィー
(株)いい生活
池上通信機(株)
伊藤忠テクノソリューションズ(株)
インクリメント・ピー（株）
(一財)インターネット協会
(株)インテック
インフォサイエンス(株)
(株)ヴァル研究所
ヴィスコ・テクノロジーズ(株)
(株)うえじま企画
(株)駅探
(株)エクサ
エヌ・ディー・アール(株)
(株)エム・オー・シー
(株)エルザジャパン
オークマ(株)
(株)大塚商会
(株)オーム社
沖電気工業(株)
オムロン(株)

【か行】

国立研究開発法人 科学技術振興機構
(公財)画像情報教育振興協会
(学)片柳学園日本工学院八王子専門学校
(学)河合塾
(一財)機械振興協会
キヤノンITソリューションズ(株)
キヤノンマーケティングジャパン(株)
キヤノンメディカルシステムズ(株)
共立出版(株)
(株)近代科学社
グーグル合同会社
(株)クヌギ
グリー（株）
(株)グリットウェブ
(株)ぐるなび
(株)けいけい
(株)コア 中四国カンパニー
コアマイクロシステムズ(株)
(株)構造計画研究所
国立国会図書館
(株)小松製作所

【さ行】

サイオス(株)
(株)サイバーエージェント
(一財)材料科学技術振興財団
サクサ(株)
サクシード(株)
三協印刷(株)
三美印刷(株)
三友工業(株)
(株)シーエーシー
システム・オートメーション(株)
(株)ジャステック
(株)ジャストイット
(株)ジャパンテクニカルソフトウェア
(一社)情報サービス産業協会
(独)情報処理推進機構
(一社)情報通信技術委員会
新世代Ｍ２Ｍコンソーシアム
(株)数理計画
(株)スカイディスク
スズキ(株)
住友化学(株)
住友電気工業(株)
(学)聖学院
(株)セガ
セコム(株)
(株)セプテーニ
(株)ソケッツ
ソニー（株）
(株)ソフトウェアコントロール
(一財)ソフトウェア情報センター 特許・技術情報センター
(株)ソリトンシステムズ

【た行】

(株)タンタカ
チームラボ(株)
(株)中電シーティーアイ
(一社)中部産業連盟
中部電力(株)
通研電気工業(株)
(株)ディー・エヌ・エー
(株)ディスコ
(株)データグリッド
テクノスデータサイエンス・エンジニアリング(株)
(株)テクノプロ　テクノプロ・デザイン社
デジタルプロセス(株)
鉄道情報システム(株)
(公財)鉄道総合技術研究所
(公財)電気通信普及財団
(一社)電子情報技術産業協会
(株)電盛社
(株)デンソー
(株)デンソーITソリューションズ
(株)デンソーアイティーラボラトリ
(株)デンソークリエイト
(一財)電力中央研究所
東海ソフト(株)
東海旅客鉄道(株)
(株)東芝
東芝インフォメーションシステムズ（株）
東芝システムテクノロジー（株）
東芝情報システム(株)
東芝デジタルソリューションズ(株)
(株)働楽ホールディングス
(株)東和システム
トーヨー企画(株)
特許庁
(株)トヨタシステムズ
トヨタ自動車(株)
(株)豊田中央研究所
トレンドマイクロ(株)
(株)ドワンゴ

【な行】

(株)ナレッジクリエーションテクノロジー
(株)ニコンシステム
西日本電信電話(株)
日鉄ソリューションズ(株)
日鉄日立システムエンジニアリング（株）
日本アルゴリズム(株)
(一財)日本データ通信協会
日本電気(株)
日本電信電話(株)
日本アイ・ビー・エム(株)
(公社)日本化学会
(一財)日本規格協会
日本銀行
国立研究開発法人 日本原子力研究開発機構
日本システム開発(株)
(一財)日本情報経済社会推進協会
(一社)日本情報システム・ユーザー協会
日本電子計算(株)
(一財)日本品質保証機構
日本放送協会 放送技術研究所
日本マイクロソフト(株)
日本無線(株)
日本ユニシス(株)
(株)野村総合研究所

【は行】

パーソルキャリア(株)
(株)ハイエレコン
(有)バクサリー
パナソニック(株)
パナソニック(株) ライフソリューションズ社
(株) 半導体エネルギー研究所
(株)ビービット
(株)ビズヒッツ
(株)日立インフォメーションエンジニアリング

(株)日立国際電気
(株)日立産業制御ソリューションズ
(株)日立システムズ
(株)日立社会情報サービス
(株)日立製作所
(株)日立製作所 中国支社
(株)日立ソリューションズ
(株)日立ソリューションズ・クリエイト
(株)日立ソリューションズ西日本
(株)日立ソリューションズ東日本
(株)ビッグツリーテクノロジー&コンサルティング
(株)ファースト
フェアリーデバイセズ(株)
(株)フォーカスシステムズ
(株)フォーラムエイト
富士通(株)
(株)富士通アドバンストエンジニアリング
(株)富士通エフサス
(株)富士通ソーシアルサイエンスラボラトリ
富士フイルム(株)
フューチャー (株)
古野電気(株)
(株)ブレアパッチ
(株)ベネッセコーポレーション
(株)堀場製作所

【ま行】

(株)牧野フライス製作所
マツダ(株)
みずほ情報総研(株)
三井情報(株)
(株)ミックナイン
(株)ミツトヨ
(株)三菱UFJ銀行
(株)三菱UFJトラスト投資工学研究所
三菱UFJモルガン・スタンレー証券(株)
三菱スペース・ソフトウエア(株)
三菱電機(株)
三菱電機インフォメーションシステムズ(株)
三菱電機インフォメーションネットワーク(株)
三菱電機コントロールソフトウェア(株)
三菱電機メカトロニクスソフトウエア(株)
三菱プレシジョン(株)
武蔵野美術大学
(株)メイテツコム
モバイルコンピューティング推進コンソーシアム(MCPC)

【や行】

(株)安川電機
ヤフー (株) Yahoo! JAPAN研究所
ヤマハ(株)

【ら行】

楽天(株)
リードエグジビションジャパン(株)
(株)リクルート
(株)リコー
(株)リックテレコム
(株)両備システムズ
(株)リンク

＜入会予定＞
アミューズメントメディア総合学院
(株)ディンプス

注）一般社団法人・一般財団法人・公益社団法人・公益財団法人はそれぞれ（一社）・(一財)・(公社)・(公財）と省略した.

協力協定学会との正会員会費相互割引について

各学協会との協定により，正会員会費が割引になります．ぜひ，ご活用ください．
本会 Web ページ（https://www.ipsj.or.jp/member/kyoryoku.html）にも掲載しております．

●協力協定学会名・相互割引率（正会員会費が割引対象）

IEEE	(The Institute of Electrical and Electronics Engineers, Inc.)	10％
IEEE-CS	(IEEE Computer Society)	10％
ACM	(Association for Computing Machinery)	20％
CSI	(Computer Society of India)	20％

※協力協定学会の会員費割引については，海外関連団体（https://www.ipsj.or.jp/annai/kanrenlink/os_relation.html）をご参照いただき，直接お問い合わせください．

●本会への申請方法
会費割引を希望する正会員は，マイページの「登録情報変更」で「会員相互割引」の協定学会名から１つ選択し，その会員番号を入力します．
初めて申請する方は上記協力協定各学会正会員の会員証コピーを Fax 等で送ってください．割引適用は１学会分といたします．
自動継続のため次回からは会員証のコピーは不要です．
※これから入会を希望する方も入会申込［本申請］の画面から同様に申請できます．
・マイページはこちら⇒ https://www.ipsj.or.jp/mypage.html
・入会申請はこちら⇒ https://www.ipsj.or.jp/nyukai_kojin.html

■照会先：会員サービス部門　E-mail:mem@ipsj.or.jp　Tel(03)3518-8370　Fax(03)3518-8375

FIT2020 第 19 回情報科学技術フォーラム開催の御案内

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。

今回は新型コロナウイルス感染症への対策として、現地開催を中止し、同期間にオンライン開催することといたしました。皆様、奮ってご参加下さい。

講演論文集（冊子、DVD-ROM）も販売を行います。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：オンライン開催

■開催イベント企画　※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

◎特別講演

2日 9:30-12:00

「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

「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

「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）

［トップコンファレンスセッション］

最近数年間に各分野のトップレベルの国際会議・学術雑誌で発表された論文の著者に、その内容を紹介して頂く特別なセッションです。

優れた研究内容を把握できるとともに、その著者たちとの質疑応答や情報交換ができる貴重な機会です。ぜひご活用ください。

［イベント企画］

各学会の関係研究会や委員会などから構成されるプログラム委員会において、ホットなトピック、分野横断的な研究テーマ、学生や若手へのメッセージを込めた話題などを中心に、多くの興味深いイベントを企画中です。以下はその一部を抜粋したものです。内容や日時は変更される場合があります。最新の情報は Webページでご確認ください。

1日	13:10～15:10	デジタル・ゲリマンダーの最新情勢
	15:30～17:30	次世代映像符号化国際標準VVCの技術動向および今後の映像符号化について
	15:30～17:30	一人一台端末による学びを支えるデジタル学習環境
2日	9:30～12:00	「未来を拓く」博士教育リーディングから情報科学の達人プログラムへの接続
	15:30～17:30	研究機関でアジャイル開発しませんか
	15:30～17:30	AI・ビッグデータ解析，IoT領域人材のプロフェッショナル資格化を考える
3日	9:30～12:00	モビリティのためのCV/PR技術
	9:30～12:00	DXを推進する俊敏なシステム開発・運用―アジャイルにつなぐビジネスとICT　～デジタルプラクティスライブ～
	9:30～12:00	社会選択への計算論的アプローチ

［研究会連携］

電子情報通信学会および情報処理学会のいくつかの研究会が、FIT2020のプログラムとして開催されます。詳細は Webページでご確認ください。

■聴講参加費（税込）

参加区分	オンライン特別価格
会　員	6,000円
非会員	12,000円
学　生	無料

※会員、非会員の聴講参加費には電子版講演論文集（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（無料）には電子版講演論文集は付いておりません。電子版講演論文集付きを希望の場合、参加費は 2,000円となります。

※会員、非会員、学生の参加区分の区別は以下の通りです。

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、CCF）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)。

■聴講参加の申込

申込締切：2020年9月3日（木）FIT最終日まで

申込方法：FIT2020 Webサイトからお申込み下さい。

※オンライン参加のご案内をお送りいたします。参加方法を事前にご確認いただくには、なるべく早めのお申込みをお勧め致します。

■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	一般 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

※残部がある場合、学生の方には講演論文集DVD-ROMを学割価格4,000円にて販売致します。

※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

■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、締切後も残部のある限りお申込を受付いたします。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

〒101-0062 東京都千代田区神田駿河台一―五
編集人 稲見昌彦
発行所 東京都千代田区神田駿河台一―五 一般社団法人 情報処理学会
発行人 木下泰三
電話 東京(〇三)三五一八―八三七四 振替口座 〇〇一五〇―四―八三四八四
印刷所 東京都荒川区西日暮里五―九―八 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

近代科学社 好評既刊

IT研究者のひらめき本棚
ビブリオ・トーク：私のオススメ

2017年9月発売　定価 1,980円(本体1,800円＋税)

編:情報処理学会 会誌編集委員会

判型　A5変　152頁　ISBN 978-4-7649-0548-1 C3004

月刊『情報処理』の人気連載をまとめた本がついに登場！

情報処理学会誌『情報処理』で好評連載中の「ビブリオ・トーク　-私のオススメ-」がついに一冊の書籍に！

この連載でIT研究者の方々が紹介した，デマルコやカーニハン，ヘネシー＆パターソン，更にはアシモフやホーガン，伊藤和典，というバラエティに富んだラインナップを40本収録.

序文は，第一回担当である人工知能研究者・中島秀之.

さらに帯に，メディアアーティスト・落合陽一の推薦文をいただき,IT研究者を目指す学生にもオススメの一冊！

■紹介書籍(一部)

◇ ハッカーと画家
◇ プログラム書法(第2 版)
◇ Computer Networks 5th Edition
◇ ディジタル作法
◇ 珠玉のプログラミング
◇ Computer Architecture, 5thEdition A Quantitative Approach
◇ Operating Systems Design andImplementation (3rd Edition)
◇ 機動警察パトレイバー風速40メートル
◇ ピープルウエア 第3 版
◇ Computer Lib /Dream Machines
◇ 未来の二つの顔
◇ 生体用センサと計測装置(ME 教科書シリーズ)
◇ Cooking for Geeks―料理の科学と実践レシピ
◇ ハッカーのたのしみ
◇ ぼくの命は言葉とともにある(9歳で失明18歳で聴力も失ったぼくが東大教授となり，考えてきたこと)
◇ 部分と全体 私の生涯の偉大な出会いと対話
◇ 夜明けのロボット(上)(下)
◇ ポスト・ヒューマン誕生
◇ 理科系の作文技術
◇ 現代倫理学入門

を含む40銘柄を紹介。

※ご注文は、お近くの書店様へ

□　お問合せ先
〒162-0843 東京都新宿区市谷田町2-7-15
株式会社近代科学社 営業部　TEL 03-3260-6161 ／ FAX 03-3260-6059
sales-corporate@kindaikagaku.co.jp　　http://www. kindaikagaku. co. jp

定価（本体 1,600 円＋税）

本誌広告一手取扱い アドコム・メディア株式会社
〒169-0073 東京都新宿区百人町 2-21-27　TEL.03-3367-0571　FAX.03-3368-1519

雑誌　05269-07

4910052690707
01600