

# 情報処理

2021

3

Vol.62 No.3  
通巻 672 号

特集

オンライン

## DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ ～サプライチェーンにおけるトラスト (信頼) の構築に向けて～

解説

プログラミング的思考がわからない



巻頭コラム

エモーショナルなロボットを作るわけ  
青木俊介

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



Web公開 (無料/有料)  
note

教育コーナー：べた語義

連載：IT紀行 / 5分で分かる!! 有名論文ナナメ読み / 情報の授業をしよう! / 先生が質問です!! / ビブリオ・トーク  
委員会から  
会議レポート  
学会活動報告

一般社団法人

情報処理学会

Information Processing Society of Japan

The Fujitsu logo, consisting of the word "FUJITSU" in a white, sans-serif font with a stylized infinity symbol above the "i".

shaping tomorrow with you

# 変わりつづける未来を、 信じられる未来へ。

くらしは、ビジネスは、ものづくりは、  
医療は、都市は、教育は、インフラは、  
信頼できるものに、なれるか。

ただし、変革をとげられるか。

それぞれの存在意義を、見つめ直し、  
持続可能なカタチに自らを進化させる。

もろく崩れやすい、この世界を、  
より柔軟で、つよく、確かなものに変えていく。

デジタルは、その力になるはずだ。

DX、わたしたちはそのパートナーとして、  
データや、テクノロジーから価値を生み出し、  
進むべき未来の姿を再構想します。

## Reimagine.

問いかける。明日が、はじまる。

富士通 reimagine

検索



# 「情報処理」 カタログ同封サービスの ご案内



カタログ同封サービスとは？

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

## お申し込み方法と掲載までの手続き

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

1 通あたり  
 約17.5 円！

**基本価格 350,000 円**  
 (税抜)

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

大学や  
 共催事業は  
 さらに割引も！

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

大学 / 研究所 / 賛助会員  
 (基本価格の 40% Off !)

**210,000 円**  
 (税抜)

情報処理学会主催・共催事業\*  
 (基本価格の 80% Off !)

**70,000 円**  
 (税抜)

\* 情報処理学会研究会主催、共催を含む

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

## 問合せ先

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

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



## PREFACE

## 巻頭コラム

- 122 エモーショナルなロボットを作るわけ 青木俊介

## SPECIAL FEATURES

## 特集

DX（デジタル・トランスフォーメーション）時代の  
サプライチェーン・セキュリティ

～サプライチェーンにおけるトラスト（信頼）の構築に向けて～

- 124 編集にあたって 石黒正揮・手塚 悟・佐々木貴之  
126 概要

## お知らせ

特集記事はオンラインのみの掲載となります（本誌には「編集にあたって」「概要」のみ掲載されます）。オンライン記事（電子図書館）の閲覧方法につきましては本誌 129 ページに掲載しておりますのでご確認くださいませよう願いたします。

## ARTICLE

## 解説

- 130 ■ ★f プログラミング的思考がわからない 遠藤 諭

## 教育コーナー：ぺた語義

- 135 ■ ★f ハイフレックス授業 渡辺博芳  
136 ■ ★f 第 13 回全国高等学校情報教育研究会全国大会（オンライン大会） 小原 格

## 連載：情報の授業をしよう！

- 140 ■ ★f 新学習指導要領「情報 I」の授業を考えよう—LINE スタンプの制作から学ぶコミュニケーションと情報デザイン— 富田 平

## 連載：★f ビブリオ・トーク—書評—

- 146 情報系のための離散数学 石井一夫

## 連載：★f 5分で分かる!? 有名論文ナナム読み

- 148 Jooho Kim and Makarand Hastak : Social Network Analysis : Characteristics of Online Social Networks After A Disaster  
廣井 慧

## 150 連載：★f 先生が質問です!!

## 学会活動報告

- 152 IFIP—情報処理国際連合—近況報告 相田 仁  
162 創立 60 周年記念事業：実施概要報告／創立 60 周年記念論文表彰（概要）

## 委員会から

- 164 第 83 回全国大会にて「デリバリー」始めます! 坊農真弓

## 会議レポート

- 166 Recsys 2020 参加報告 関 喜史

## 連載：IT 紀行

- 168 VR 界の大イベント「Vket」を主催する、動く城のフィオさんについてみた まいてい 999

## 《記号の説明》

■ 基礎 ■ 専門家向け  
■ 応用 ■ 一般（非専門家）向け ★f ジュニア会員向け  
 ※各記事に指標がついていますので参考にさせていただきます

常時更新中!

## 「情報処理」オンライン版 目次

[https://www.ipsj.or.jp/magazine/contents\\_m\\_e.html](https://www.ipsj.or.jp/magazine/contents_m_e.html)

※オンラインでのみ掲載している記事の目次を掲載しております(目次から電子図書館の各記事へリンクしております)。



### ■ Vol.62 No.3

特集: DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ  
～サプライチェーンにおけるトラスト (信頼) の構築に向けて～

e1 ■ 1. サプライチェーンにかかわるセキュリティを確保するための仕組みと制度  
～社会的な説明責任を果たすためのアプローチ～ (石黒正揮)

e7 ■ 2. サイバー・フィジカル・セキュリティ・フレームワークを活用したサプライチェーン・セキュリティの確保  
(奥家敏和)

e14 ■ 3. サプライチェーン・セキュリティの脅威と対策の動向 (小川隆一・小山明美)

e21 ■ 4. 制御機器のセキュリティ認証制度 (神余浩夫・山田 勉)

e28 ■ 5. 第三者認証によるサプライチェーン・セキュリティの確保とアシュアランス (登山慎一・Ethiraj, Sudhir Kumar Raj)

e34 ■ 6. 米国を中心とした第三者機関によるセキュリティ評価の動向—製品リスク評価のためのセキュリティ認証— (吉岡俊郎)

e37 ■ 7. ソフトウェア部品表 (SBOM) に基づくリスク管理

—オープンソース・ソフトウェア (OSS) および商用ソフトウェアのリスク管理のための SBOM — (松岡正人)

## 「情報処理」note

<https://note.com/ipsj>

※人気記事や最新記事のちら見せ, 無料で読める記事などさまざまなコンテンツを公開していきます。



- 129 【ご案内】会誌「情報処理」のオンライン記事について
- 145 2021年度会誌「情報処理」モニタ募集のお知らせ
- 170 会員の広場
- 172 IPSJカレンダー
- 174 有料会告
- 177 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

- 178 [重要] 過去のプログラミング・シンポジウム報告集の利用許諾について
- 179 英文目次
- 180 編集室/次号予定目次
- 181 掲載広告カタログ・資料請求用紙
- 182 賛助会員のご紹介

### ■会誌編集委員会

編集長: 稲見 昌彦

副編集長: 大山 恵弘・加藤 由花・中田真城子

担当理事: 清水 佳奈・井上 創造

本号エディタ:

五十嵐悠紀・石黒 正揮・上松惠理子・江波浩一郎・大石 康智・  
大川 徳之・太田 智美・折田 明子・桂井麻里衣・金子 格・  
川上 玲・河原 亮・楠 房子・櫻 惇志・斎藤 俊則・  
佐々木貴之・須川 賢洋・袖 美樹子・手塚 悟・高木 拓也・  
中島 一彰・西川 記史・坂東 宏和・古川 雅子・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

理事からのメッセージ:

[https://www.ipsj.or.jp/annai/aboutipsj/riji\\_message.html](https://www.ipsj.or.jp/annai/aboutipsj/riji_message.html)

### ■情報処理学会事務局本部

〒101-0062 東京都千代田区神田駿河台 1-5 化学会館 4F

Tel(03)3518-8374 (代表) Fax(03)3518-8375

E-mail: soumu@ipsj.or.jp <https://www.ipsj.or.jp/>

郵便振替口座 00150-4-83484

銀行振込 (いずれも普通預金口座)

みずほ銀行虎ノ門支店 1013945

三菱 UFJ 銀行本店 7636858

名義人: 一般社団法人 情報処理学会

名義人カナ: シヤ) ジョウホウシヨリガツカイ

### ■規格部 情報規格調査会

〒105-0011 東京都港区芝公園 3-5-8 機械振興会館 308-3

Tel(03)3431-2808 Fax(03)3431-6493

E-mail: standards@itscj.ipsj.or.jp <https://www.itscj.ipsj.or.jp/>

■支 部 北海道/東北/東海/北陸/関西/中国/四国/九州

電子版  
-DIGITAL VER-



Kindle



Fujisan



情報学広場



# エモーショナルなロボットを作るわけ

■ 青木 俊介



筆者は現在、家庭向けのコミュニケーションロボットを作る会社、ユカイ工学(株)の代表を務めている。家庭の中でロボットが必要とされる場面は、まだ多くないのが現実だが、これからどのようなロボットが家庭の中で必要とされていくのだろうか。僕たちのアイデアを紹介したい。

僕たちのプロダクトのユーザさんの行動から見つけた、ロボットの効用がある。それは、ロボットをメッセージャーとして利用すると、人に言うことを聞いてもらいやすくなるという効用だ。弊社では「BOCCO (ボッコ)」というコミュニケーションロボットを2015年から商品化している。ロボットの形をしたスマートスピーカーのような製品で、スマートフォンのアプリからテキストを送信するとメッセージを読み上げる機能がある。これを使って、ロボットがあたかもしゃべっているかのように自分のメッセージを伝えたりすることができる。

小学生のお子さんが、運動会が嫌いで、練習が始まると学校に行きたがらないというユーザさんがいた。そこで、毎朝BOCCOを使ってお子さんを励ましてあげることで、なんとか運動会の当日まで毎日学校に通うことができたという。また、一人暮らしの高齢者の家族がいるユーザさんの話では、家族が電話で薬を飲んでいるか確認すると反発されてしまうのに、BOCCOのリマインド機能を使って「お薬を飲む時間だよ」と

■ 青木 俊介  
ユカイ工学 (株) 代表

東京大学在学中にチームラボを設立、CTO に就任。その後、ピクシブのCTO を務めたのち、ロボティクスベンチャー「ユカイ工学」を設立。「ロボティクスで世界をユカイに」というビジョンのもと家庭向けロボット製品を数多く手がける。2014年家族をつなぐコミュニケーションロボット「BOCCO」を発表。2017年しっぽのついたクッション型セラピーロボット「Qoobo」を発表。2015年よりグッドデザイン賞審査委員。



伝えてあげると、素直に飲んでくれるようになったという。

このように、ロボットには人の感情を動かしたり、行動を引き出す役割があるのではないだろうか。掃除機ロボットについても、実は同じことが言える。充電ドックに戻るのに失敗しているのを見ると、なぜか「頑張ってくれたんだなあ」という、応援したくなるような気持ちになることがある。人はロボットという存在に感情を引き起こされてしまうのだ。ロボットはとてもエモーショナルな存在なのだ。

では、この効用を活用するとどんなロボットが実現できるのだろうか。ロボットはどんな役割を担うようになるのだろうか。僕は、『となりのトトロ』の世界観に近いのではないかと考えている。この映画の中では、人の周りにいろんな妖怪たちが潜んでいる。そしてその妖怪たちが、なんとなく子供たちを見守っていて、子供たちを幸せに導いてくれる。未来のロボットも、おそらく、人間の身の回りにいろいろな種類のものがいて、それらが協調して人間の生活をサポートするようになるのではないか。人が毎日運動をしたり、薬を飲んだり、学習をしたりする習慣づけをロボットがサポートしてくれる。人の行動の意図や願望を把握し、なんとなくユーザの望むウェルビーイングが実現するようにロボットが行動を導いてくれる。そのような未来の妖怪のような存在がロボットの目指すべき姿ではないだろうか。

## 特集

# DX（デジタル・トランスフォーメーション）時代のサプライチェーン・セキュリティ

～サプライチェーンにおけるトラスト（信頼）の構築に向けて～

## 編集にあたって

石黒正揮 | (株) 三菱総合研究所 手塚 悟 | 慶應義塾大学 環境情報学部

佐々木貴之 | 横浜国立大学

産業のデジタル化、グローバル化が進展するに伴いさまざまな企業や利用者（コンシューマ）が相互連携により新しい製品・サービスが創出されるとともに、新たなビジネス機会が生まれている。たとえば、大規模なサプライチェーンを構成する自動車分野では、インターネット接続により、ナビゲーション、インフォテイメント、モビリティ・サービス（MaaS：Mobility-as-a-Service）、自動運転等の新たな機能やサービスが従来の自動車産業の枠を超えて、AIやソフトウェアにかかわるベンチャーなど多様な関係者との協業により創出され、それらの機能をアップグレードしていくことも可能となっている。また、ポストコロナ時代のニューノーマル（新常态）に向けて、サプライチェーンにおける組織やモノにかかわるデジタル変革（DX）が進展している。

このようなサプライチェーンの複雑化、グローバル化に伴い、連携する組織やシステムへの攻撃ポイントが増加し、波及的な被害の連鎖によるセキュリ

ティ・リスクが拡大している。自動車、ロボットなど日本が強みとする産業においては、デジタル化が進むサプライチェーン・エコシステムにおける企業間のサイバーセキュリティにかかわる説明責任と信頼性の確保が競争力の根幹となる。このようなことから、本特集では、サプライチェーンの複雑化、グローバル化に伴い生じるセキュリティの脅威やリスクの動向とその対策および今後の課題や展望についてまとめてみた。

サイバーセキュリティは技術、組織、制度など包括的な取り組みが不可欠であることから、本特集では、産官学の専門家の知見を結集して幅広い視点からまとめることとした。

本特集の構成は以下の通りである。

(1) サプライチェーンにかかわるセキュリティを確保するための仕組みと制度

(株) 三菱総合研究所 石黒正揮が、サプライチェーンの発展に伴うセキュリティにかかわる本質的な課

題とその解決のための仕組みについて解説した。さまざまな取引主体による協業に伴い生じるガバナンスの欠如、サプライチェーン全体を通じた信頼性の欠如に対して、責任主体の明確化、ほかのステークホルダーに対する説明責任の確保と信頼性の付与（セキュリティ・アシュアランス）について有効なアプローチや取り組むべき課題についてまとめた。

#### (2) サイバー・フィジカル・セキュリティ・フレームワークを活用したサプライチェーン・セキュリティの確保

経済産業省 奥家敏和氏に、ものがつながるサイバーフィジカルシステムにおけるセキュリティ対策についての取り組みをまとめていただいた。産業社会を「企業間のつながり」「フィジカル空間とサイバー空間のつながり」および「サイバー空間におけるつながり」という3つの切り口で捉えて、総合的に守るべき機能・役割を提示している。

#### (3) サプライチェーン・セキュリティの脅威と対策の動向

(独) 情報処理推進機構 小川隆一氏、小山明美氏にサプライチェーンの脅威と対策の動向についてまとめていただいた。多数の取引関係によるサプライチェーンの発達に伴いセキュリティリスクの増大、対策コストの増大が課題となっている。多岐に渡る

リスクに対して、対策チェックシートの共通化、納品後の脆弱性対応のための情報共有、ガイドラインの活用、契約要件の見直しなど現実面として実施できることの重要性が示されている。

#### (4) 制御機器のセキュリティ認証制度

三菱電機（株）神余浩夫氏、（株）日立製作所 山田勉氏に、サプライチェーンセキュリティにかかわる主な国際標準動向についてまとめていただいた。グローバル化するサプライチェーンにおいてセキュリティの確保は、国際経済連携、技術共同開発、安全保障など多くの点で重要になっている。

調達者が、個々の製品のセキュリティ規格適合およびセキュリティレベルを評価するのは技術的、コスト的に負担が大きく、第三者認証に向けたセキュリティ認証スキームの開発が急務となっている。IEC 62443, NIST SP800-82, 経済産業省サイバーフィジカルセキュリティフレームワークなど代表的な標準や認証制度について特徴や関係性について示すことで、それらの活用の参考情報を提供する。

#### (5) 第三者認証によるサプライチェーン・セキュリティの確保とアシュアランス

テュフズードジャパン（株）登山慎一氏、TÜV SÜD Sec-IT GmbH, Ethiraj, Sudhir Kumar Raj氏により第三者認証によるセキュリティ確保に関する

動向についてまとめていただいた。サプライチェーンが抱えるサイバーリスクに対して、ネットワーク化されたデジタル社会がサイバーセキュリティへの信頼を構築するための新しい枠組み「Charter of Trust」に基づく取り組みについてまとめている。

### (6) 米国を中心とした第三者機関によるセキュリティ評価の動向

(株) UL Japan 吉岡俊郎氏に、米国における認証制度に関する動向とその意義についてまとめていただいた。米国ではIoTのセキュリティ試験・認定を政府主導で推進している。セキュリティ試験やソースコード・設計文書・リスクマネジメントプロセス等を含めたレビューを第三者の立場で行うことで、製品が適切に設計され、かつその設計が正しく実装されているかどうか客観的に確認することができるなどの意義について示されている。

### (7) ソフトウェア部品表 (SBOM) に基づくリスク管理 ソフトウェア部品表 (SBOM) に基づくリスク管理の動向について、日本シノプシス合同会社 松岡

正人氏にまとめていただいた。近年のソフトウェアは大多数にOSSが含まれ、コード全体の70%程度を占めていたと報告されており、OSSの脆弱性は商用ソフトウェアの脆弱性に大きな影響を与えると同時に、ライセンス違反のリスクを抱えている。開発と運用、言語と実行環境、システムの構成と利用されているコンポーネント、これらの組合せにより、開発プロセスの各フェーズでSBOMの情報を解析し必要に応じて脆弱性の修正や、緩和策の導入などを行う体制が重要であることを示している。

本特集で紹介したサイバーセキュリティに関する産官学の包括的な取り組みと今後の課題への対応により、日本の産業競争力をさらに強化してブランド力を向上させることに寄与することを期待したい。

(2021年1月8日)

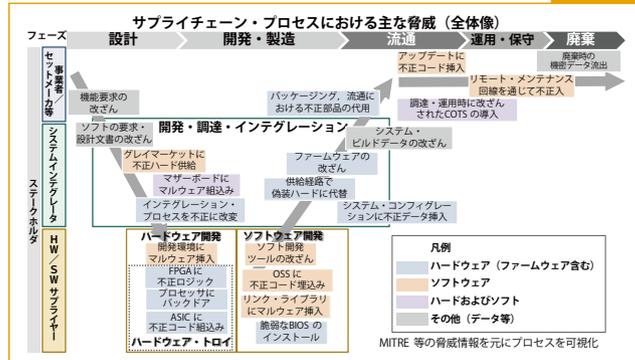
## DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ ～サプライチェーンにおけるトラスト (信頼) の構築に向けて～ 概要

### 1 サプライチェーンにかかわるセキュリティを確保するための 仕組みと制度

～社会的な説明責任を果たすためのアプローチ～

石黒正揮 | (株) 三菱総合研究所

デジタル・トランスフォーメーションの進展に伴い、サプライチェーンの複雑化、グローバル化が進んでいる。これに伴い、個々のステークホルダーだけではセキュリティの確保が難しくなっている。サプライチェーン・セキュリティ確保のためには、さまざまな基準等から目的や分野の固有性を考慮して、適切な基準を選択することが重要である。一方で、セキュリティの強化自体だけでなく、ステークホルダー間の説明力の向上は、サプライチェーンを通じたリスクを低減するために不可欠である。そのためのアプローチとしてセキュリティ・アシュアランスとサプライチェーン・ガバナンスに関する意識啓発、ガイドラインの整備などが重要となる。



基  
専  
般



## 概要

### 5 第三者認証によるサプライチェーン・セキュリティの確保とアシュアランス

登山慎一 | テュフズードジャパン (株)

Ethiraj, Sudhir Kumar Raj | TÜV SÜD Sec IT GmbH

近年、デジタル技術によるビジネスの変革(デジタル・トランスフォーメーション:以下DX)によって汎用技術、ネットワーク化が進んだ結果、すべての産業においてITの重要性が高まってきている。特にサプライチェーンに向けたサイバー攻撃は、ITへの依存が増していくにつれて重大な事業リスクとして顕在化してきている。

本稿ではサプライチェーンが抱えるサイバーリスクに関して解説し、新たな試みとして発足した「Charter of Trust」が進めているサプライチェーンのセキュリティ対策について解説する。



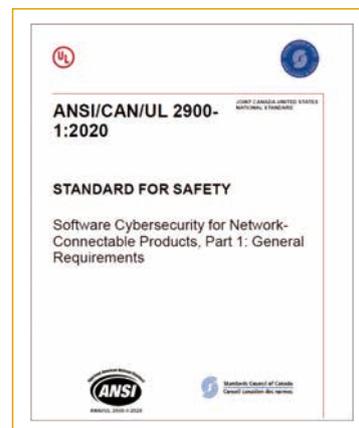
基  
専  
応  
般

### 6 米国を中心とした第三者機関によるセキュリティ評価の動向

—製品リスク評価のためのセキュリティ認証—

吉岡俊郎 | (株) UL Japan

IoT機器の脆弱性リスクやサプライチェーンのセキュリティ担保が近年注目される中、米国において第三者機関のセキュリティ評価に基づく認証制度であるUL Cybersecurity Assurance Programが策定されている。本稿ではその背景と要求事項、IoT機器に対する第三者評価を行うことの意味について説明する。



基  
専  
応  
般

### 7 ソフトウェア部品表 (SBOM) に基づくリスク管理

—オープンソース・ソフトウェア (OSS) および商用ソフトウェアのリスク管理のためのSBOM—

松岡正人 | 日本シノプシス合同会社

ソフトウェア部品表(SBOM)は、ソフトウェアの構築に使用されるさまざまなコンポーネントの詳細とサプライチェーンの関係を記載したモノである。再帰的に利用されたソフトウェアコンポーネントを構成する成分のリストで構成され、ソフトウェアコンポーネント、それらのコンポーネントに関する情報、およびそれらの間の関係を識別して一覧表示したものである。



基  
専  
応  
般

特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

# 1 サプライチェーンにかかわるセキュリティを 基 専 応 般 確保するための仕組みと制度

～社会的な説明責任を果たすためのアプローチ～



石黒正揮 | (株) 三菱総合研究所

## サプライチェーン脅威の拡大

Web サービスの情報基盤を提供するデジタル・プラットフォーム、デジタル・サービスの集約・提供を行うアグリゲータ、消費者自らが Web サービスを生み出すプロシューマなどさまざまな企業等などから構成されるビジネス環境（「ビジネス・エコシステム」と呼ぶ）を活用することで新しい価値を迅速に生み出す成功事例が増えている。従来から巨大なサプライチェーンを構成する自動車産業においても、系列による固定的なサプライチェーンから、AI ベンチャー、タクシーや鉄道など移動手段を組み合わせたサービスを提供する MaaS (Mobility-as-a-Service) 事業者など新しいプレイヤーとの連携を積極化し、自前主義からスピードとイノベーションを重視した分野横断的なビジネス・エコシステムへと業界構造が変革している。

一方で、サプライチェーンやエコシステムの変革に伴い、多様な主体（ステークホルダ）がかかわることでセキュリティ・リスクが増大している。情報処理推進機構による「情報セキュリティ 10 大脅威 2020」では、サプライチェーンの弱点となる企業への攻撃が、組織に対する 10 大脅威の上位に位置付けられ、サプライチェーンを通じたセキュリティの確保が重要な課題としている。また、イギリス政府

CERT-UK の調査レポート<sup>☆1</sup>では、サプライチェーンにおけるセキュリティリスクの 92% は脆弱な中小企業を狙ったものとしている。

近年、5G 通信インフラにおいて米国政府が中国ベンダ数社の製品に安全保障上の問題があるとして国際貿易における製品排除に動いている。米国では、2011 年に偽装品に関する国防省への報告が義務化されており（GIDEP (Government-Industry Data Exchange Program)）、2011 年から 2015 年までにマイクロチップの偽装品などを含む 450 件以上の偽装品に関する報告がなされサプライチェーンにかかわる脅威について危機感が強い。

サプライチェーンにかかわるセキュリティ脅威を取引にかかわる組織（ステークホルダ）と開発から廃棄に至るライフサイクル・プロセスを 2 軸として俯瞰したものが図-1 である。

脅威は、開発の上流から廃棄に至るまで全体に渡り存在する。近年は、プロセッサへの不正ロジック、バックドアの組込みなどハードウェア・トロイの脅威も高まっており、ソフトウェアによるセキュリティだけでは対策が困難である。

このようにサプライチェーンの複雑化・グローバル化と、サプライチェーン・インシデント（事故）の増加により、企業、政府におけるサプライチェーン・セキュリティに対する危機感が高まっている。

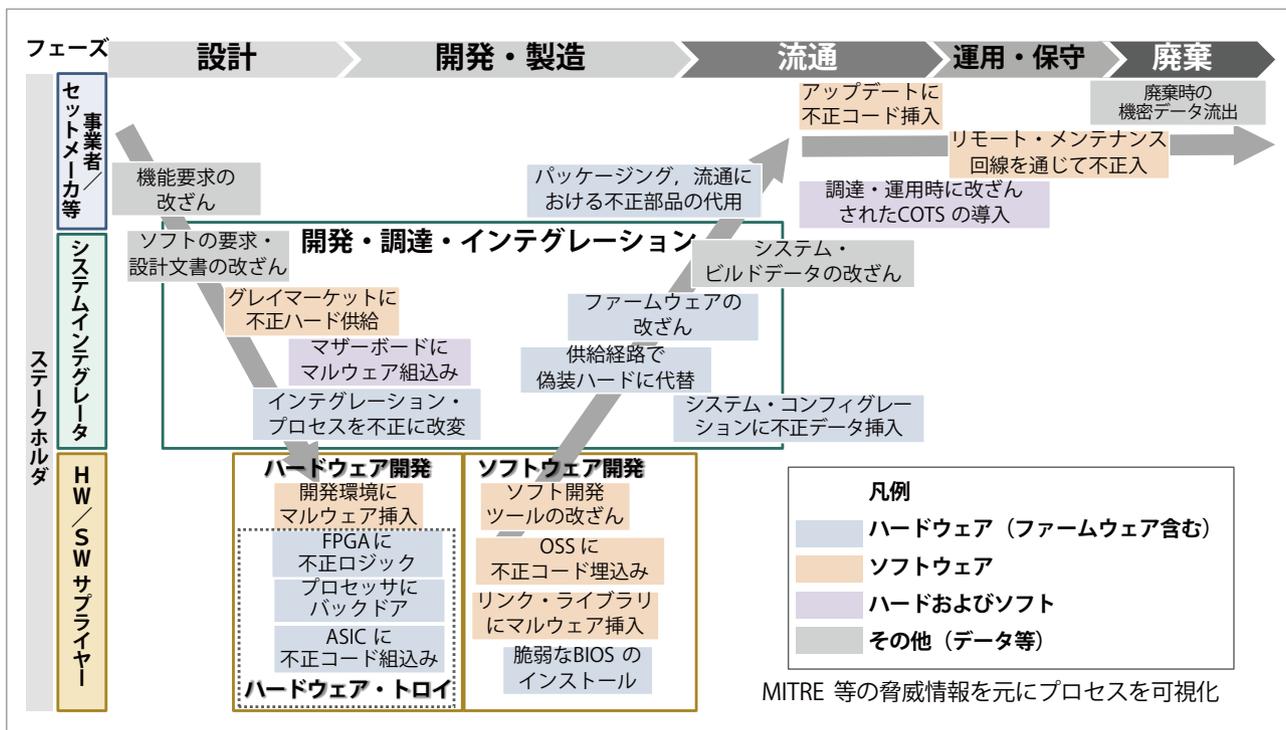
☆1 CERT-UK, Cyber-security risks in the supply chain.

## サプライチェーンの構造と脅威

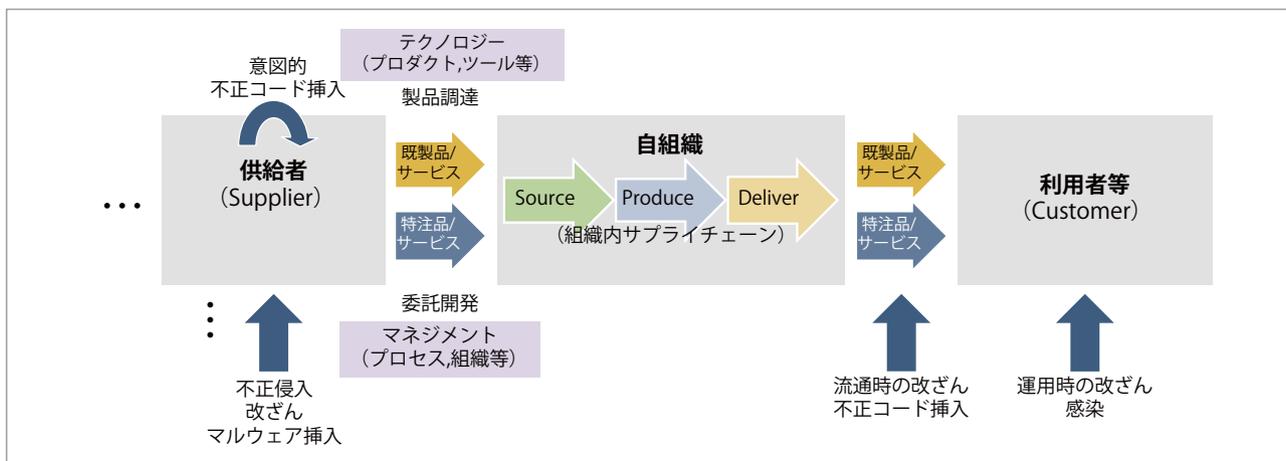
サプライチェーンの構造と脅威の関係を一般化したものが図-2である。

サプライチェーンは製品・サービスの供給者から最終利用者に向けて多段的につながっている。サプライチェーン脅威としては、供給者の開発プロセスへの不正侵入、改ざん、マルウェア挿入や流通過程

での不正コードの挿入、運用・アップデート時の改ざんなどが挙げられる。調達・供給は、既成品と特注（委託開発）に大きく分かれ、適用できる対策に違いがある。既成品等の場合、開発プロセスに関与できないため対象製品・サービスに対して検証技術などのテクノロジーを適用しセキュリティを確保する。特注の場合、開発やSIの発注から受入れに至るまでのプロセスにおける管理・監査等のマネジメ



■図-1 サプライチェーン・プロセスにおける主なセキュリティ脅威



■図-2 サプライチェーンの一般的な構造と脅威の関係

特集  
Special Feature

ントを適用することも可能である。

## サプライチェーンセキュリティ基準の活用アプローチ

サプライチェーンセキュリティに活用できる基準等は既存のものだけでも多数存在するが、基本構造、目的、産業分野への特化など関係性が複雑であり、適切な基準群を組み合わせ、適切なレベルとコストで対策することが難しい。図-3は、サプライチェーンにかかわる基準、標準等を、現在の導入状況に応じて、どのように追加補強し包括的な対策を実現するかについて選択の考え方を俯瞰したものである。

サプライチェーンセキュリティの確保のためには、以下の手順で関連基準を選択し組み合わせることで、コストと対策レベルのバランスを確保することが妥当である。

### ①ベースとするフレームワークの選択

代表的なセキュリティ・フレームワーク (NIST

Risk Management Framework, Cybersecurity Framework, ISO/IEC 27000 シリーズなど) をベースとして選択し対策の全体構造を設定し、②以下の具体化を検討する。

### ②産業分野に応じた基準の追加選択

産業分野固有の対策と経済性を高めるカスタマイズを行った基準を選択し、対策コストと達成レベルの費用対効果を高める。

### ③重点課題による選択

改ざん検査、調達、偽装対策など重点課題に応じて強化したい対策基準を選択・導入する。

さらに具体的な選択方法の詳細については割愛するが、各領域に精通した専門家との協力により組合せを検討することも有効である。

## 説明責任とセキュリティ・アシュアランス

サプライチェーンにおいては、各ステークホルダ

①ベースとするフレームワークの選択				
	NIST 利用	現在利用フレームワーク無	ISO/IEC 利用	産業固有または組織固有の基準
セキュリティフレームワーク	NIST Risk Management Framework SP800-53	NIST Cybersecurity Framework 経済産業省 サイバーフィジカルセキュリティ対策フレームワーク	ISO/IEC 27001 ISO/IEC 27002	Critical Manufacturing Sector Cybersecurity Framework Implementation Guidance
サイバーサプライチェーン	NIST SP800-161 NIST SP800-171 NIST IR 7622	IoT推進コンソーシアムIoTセキュリティガイドライン	ISO/IEC 27017	FFIEC, OCC Guideline IEC/ISA62443-2-4 FS-ISAC 3rd Party Software security control Types Cybersecurity Procurement Language for Energy Delivery Systems
産業別標準・認証	NIST SP800-82 NIST IR 7628	Energy Sector Cybersecurity FW Implementation Guidance Cybersecurity and Risk Management Best Practice: CSRIC WG4	ISO/IEC 27011 ISO/IEC 27015 ISO/IEC 27019	NERC CIP; C2M2 CSRIC TISAX AIAG Cyber Security 3rd Party Information Security UL VCSP
ソフトウェア完全性 (改ざん検査)	SAFECode Software Integrity guidelines			
セキュリティ調達	ANSI/ESD S20.20-2007; C-TPAT; AEO; TAPA; Electronics Industry Citizenship Coalition(CICC); Dodd-Rank Conflict Mineral Requirements			
偽装対策	SAR Standards, MITRE Attack Pattern			
適合性評価	Common Criteria(ISO/IEC 15408) Certification, The Open Group Trusted Supplier Program; AZLA Accreditation; ISO9001 Certification, EDSA Certification, UL CAP			

② 産業分野に応じた基準の選択  
③ 重点課題による選択

■ 図-3 サプライチェーン・セキュリティ基準等の選択指針と手順

によるセキュリティ確保は必要条件であるが、セキュリティを確保していることをほかのステークホルダに説明し信頼を得ることができなければ十分とは言えない。特に、調達元に課される事故責任が厳格になればなるほど、調達先に対する説明責任の要求レベルは高くなる。セキュリティ自体の強化と、他のステークホルダに対してセキュリティの説明責任を果たしていることは必ずしも一致しない。高いセキュリティを達成していても、グローバルに通用する説明責任を果たさなければ契約が獲得できないなど企業にとっては影響が大きい。ステークホルダ間での信頼性の確保を意味する Trustworthiness (信頼性保証) という概念について、NIST SP800-39 では、「Trustworthiness は、セキュリティ機能とアシュアランスの2つの異なる概念の組合せ」として定義されている。

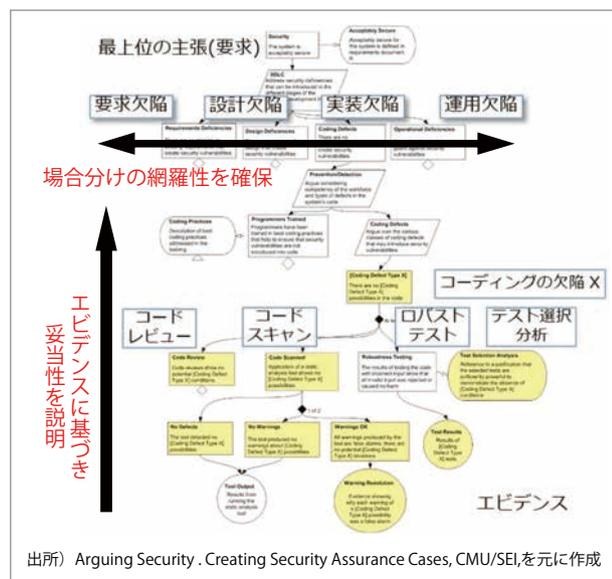
説明責任を果たす上で、何をどの程度やらなければならぬか？ その判断を行う上でアシュアランス・ケースの考え方が重要である。アシュアランス・ケースは、システムに関する主張や要求が満たされていることを根拠情報 (エビデンス) と論証に基づき体系的、客観的に示すための説明文書である。機能安全規格の認証においては、アシュアラ

ランス・ケースの提示が要件化されており、セキュリティ分野では、IT 機器のセキュリティ認証基準 ISO 15408 (コモン・クライテリア) の評価保証は同様の考え方に基づいている。図-4 は、アシュアランス・ケースの例を示すものである。

たとえば、ソフトウェアの欠陥がないことを示す場合に、要求欠陥、設計欠陥、実装欠陥、運用欠陥等がないことなどを体系的、網羅的に示しつつ、それらを階層的に掘り下げることで、最終的にはテスト結果のデータなどのエビデンス (根拠情報) まで視覚的に示すものである。アシュアランス・ケースの論証は納得性のある説明ができることが重要であり、固定的なやり方ではなく柔軟に考え方を示すことで対応可能である。国際標準に基づく認証に慣れていない国内企業の中には、セキュリティ要求事項に対して、硬直的な対応にこだわり対策コストがかさむことで競争上の不利を招くケースが見られるが、要求事項の本質を理解することで、柔軟な説明が可能であり、説明責任を確保しつつ、意味の無い不必要な対策コストを低減することがセキュリティ・アシュアランスを実現する上で重要となる。

## サプライチェーン・ガバナンス

インフラ・システムの構築・運用においては、市場メカニズムに任せていただけではセキュリティ対策投資が十分に進まないということがセキュリティ経済学の研究で示されている。インフラ事故発生時のインフラ事業者に対する事故責任の明確化、損害額の適切なリスク定量化と把握、発注者と受注者のセキュリティ技術の理解に関する情報の非対称性などが原因となり、インフラ事業者が必要なセキュリティ対策予算を確保することができず、技術的なセキュリティ対策を受託するベンダのインセンティブの低下、モラルハザードを招くためである



■図-4 アシュアランス・ケースのイメージ

特集  
Special Feature

(図-5) <sup>☆2</sup>。このような問題は、サプライチェーン・ガバナンスの欠如と行うことができる。

このような問題を解決するためには、インフラ事業者に対する事故責任の明確化とともに、インフラを構築するエンジニアリング会社と技術的に対等に渡り合える専門家によるPMC (Project Management Consultant) を設置することで、必要なセキュリティ対策の要件化とそれに対する適合性確認または第三者認証によるセキュリティ・アシュアランスが重要となる。

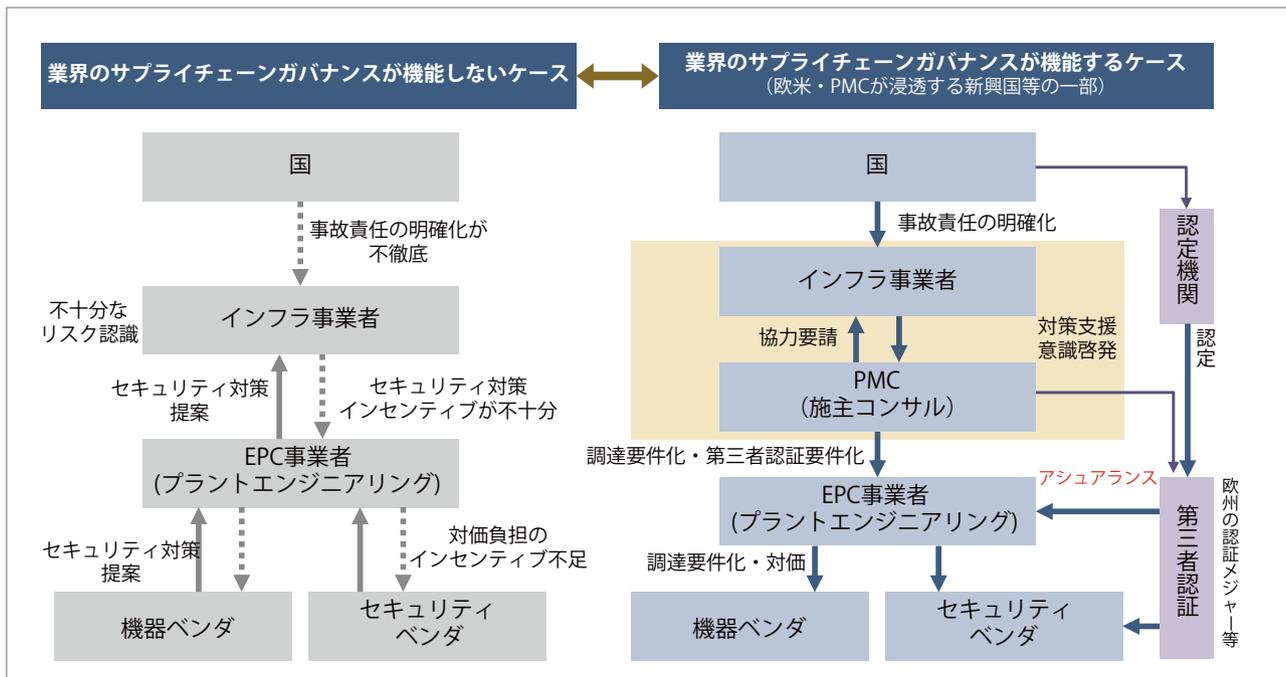
### 適合性評価国際標準と認証制度

セキュリティ対策の説明責任を向上させる手段として、ISO/IEC 17000 適合性評価に対応した認証制度等がある。これには、第三者認証と自己適合宣言がある。サイバーセキュリティにかかわる国際標準、認証制度は国、標準化団体により整備が進められている。これらの標準、規準等の中から自組織に

有効なものを選択し、適合性評価を実施することは、説明責任を向上させる有効な手段である。図-6は、セキュリティ分野の適合性評価にかかわる制度を分類したものである。

制度は、政府による強制基準 (規制)、政府調達基準、任意制度に分けることができる。電力などの重要インフラで事故の影響が大きい場合、強制基準となる例がある。また、認証制度 CC (Common Criteria), CMVP (Cryptographic Module Validation Program) などは政府調達基準とする国は多く、国際相互承認が進み、認証取得件数は増加傾向にある。また、EDSA (Embedded Device Security Assurance) などプラント分野における国際的な調達要件や ISMS (Information Security Management System) などサイバー保険料の割引に認証取得が条件とされる例もある。セキュリティ対策を促進し、サプライヤー間の説明責任を向上させる上で、各分野のリスクと要求レベルに応じてこのような選択肢を活用することは効果的である。産業分野ごとに、脅威トレンドや損害リスクの規模、システムに要求されるレベルの違いが大きいため、図-3でも

<sup>☆2</sup> 詳細は、特集「デジタルエコノミー時代のサイバーセキュリティ」、サイバーセキュリティ経済学, 情報処理, Vol.59, No.12 (Dec. 2018) を参照。



■図-5 サプライチェーンの責任関係とガバナンスの課題

特集  
Special Feature

示した通り、汎用的な共通フレームワークと産業別、目的別に具体化した基準など自組織に適した基準を適切に選択できることはきわめて重要である。

## 今後の課題と展望

以上の動向および制度・仕組みを踏まえ、改めて今後の課題をまとめると以下の通りである。

### • 対策フレームワークと分野最適化した基準の整備の必要性

フレームワークに対して分野のリスク、要求レベルに応じて適切にカスタマイズした基準が未整備な分野についてはカスタマイズが期待される。現在整備中の自動車分野、医療機器分野などが例である。

### • セキュリティ・アシュアランスに関する基盤整備

セキュリティ強化自体と他のステークホルダへの説明責任の確保の違いを意識し、グローバルに受け入れられるセキュリティ・アシュアランスのガイダンスやテンプレート集の作成が期待される。

### • サプライチェーン・ガバナンスの確保

業界のリスクに応じてステークホルダの責任および関係者の責任分界点の明確化と業界ガイドラインの整備が必要である。

### • デジタル・トラスト・プラットフォームの構築

サプライチェーンを通じた信頼の連鎖の確保のための技術的、組織的なセキュリティ評価認証結果の情報共有プラットフォームの構築は有効である。

以上のような取り組みを通じて、今後進展するデジタル・エコシステムやサプライチェーンにおけるセキュリティの向上が期待できる。

(2020年11月2日受付)

謝辞 本稿は、内閣サイバーセキュリティセンターの「サプライチェーンリスク対応のための技術検証体制構築に関する調査」、経済産業省の「平成30年度高度な自動走行システムの社会実装に向けた研究開発・実証事業（自動運転が活用されるコネクテッド技術に関する国内外動向調査）」、NEDOの「SIP重要インフラ等におけるサイバーセキュリティの確保に関する検討」等の委託調査において（株）三菱総合研究所が実施した成果等を参考まとめたものです。調査等を通じて、内閣サイバーセキュリティセンター、経済産業省自動車課、内閣府SIPプロジェクトの皆様大変にお世話になりました。皆様には深く感謝を申し上げます。

■ 石黒正揮（正会員） masa@mri.co.jp

博士（情報科学）。東京大学大学院理学系研究科情報科学専攻修士課程修了。現在、（株）三菱総合研究所サイバーセキュリティ戦略グループ。専門は、サイバーセキュリティ、デジタル戦略、デジタル・エンジニアリング、AI/数理データ解析、リスク評価、日米欧アジアにおけるセキュリティ政策・技術戦略、セキュリティ経済学、デジタル経済学。調査コンサルティングに従事する。

区分	認証制度	スキーム オーナー	基準/標準	認定機関	認証機関	国際相互承認MRA	概要	
政府 調達基準※	任意	CSMS	(METI/JIPDEC)	CSMS認証基準 (IEC 62443-2-1相当)	JIPDEC	JQA, BSI Japan	なし	制御システムを対象としたセキュリティマネジメントシステム
	任意	ISMS	(METI/JIPDEC)	ISO 27000シリーズ	JIPDEC	JQA, TÜV Rheinland, DNV	IAFで 検討中	組織の情報セキュリティに関するマネジメントシステム、セキュリティ向上と国際的な信頼向上が目的
	Common Criteria	CCEVS	NIAP (NIST, NSA)	ISO/IEC 15408	NIAP	NIAP (CC testing Lab's)	CCRA 17カ国	IT関連製品（複合機、情報システム、ICカード、ソフトウェア等）の情報セキュリティ（JISEC 制度 2001年創設、2003年CCRAに加盟）
		JISEC	(経産省/IPA)	ISO/IEC 15408	IPA/NITE	IPA (ECSEC等)		
	CMVP	CMVP	米NIST/ 加CSEC	FIPS 140-3 ISO/IEC 19790	NIST (NVLAP)	CygnCom, InfoGuard等	NIST-IPA 共同認証 (2012年)	暗号モジュールの暗号アルゴリズムの実装と鍵、ID、パスワード等の重要情報のセキュリティ確保（CMVP1995開始、JCMVP2007年正式運用開始）試験ツールJATTを用いて実施するため、暗号アルゴリズムの深い知識は不要。
		JCMVP	(経産省/IPA)	JIS X 19790 (FIPS 140-3)	IPA/NITE	IPA (ITSC, ECSEC等)		
強制	NERC-CIP	FERC	CIP V5	FERC	NERC	なし	電力事業者等に対するサイバーセキュリティ対策	
強制	中国CCC	国家認証認可監督管理委員会 (CNCA)	中国国家標準 (GB)	CNCA	指定認証機関 (CQC等)	なし	輸入されるITセキュリティ製品、自動車関係、電気製品等の指定製品の安全確保、環境保全（中国政府調達品の自国品優遇制度の懸念あり）	
民間 任意	EDSA/ISA Secure	ISCI	EDSA標準 (IEC 62443-4-2等 に相当)	ANSI/ACCLASS (米国)	Exida	IAF	制御システム・コンポーネントのセキュリティ確保。Wurldtech, Achilles等のツールを用いる	
	CAP	UL	UL 2900 (IEC 62443参照)	JAB (日本)	CSSC CL			
	TUV SUD IEC 62443 certification	TUV SUD	IEC 62443-4-1, 3-3, 2-4	—	ULのみ	なし	ネットワーク接続型製品ならびにシステムのサイバーセキュリティ確保。Synopsisのツールなどを用いる	
	情報セキュリティ格付	(株) ISレーティング	マネジメント成熟度 等	—	(株) ISレーティング	なし	企業や組織が取り扱う技術情報、営業機密、個人情報についてセキュリティのレベルを格付	

■ 図-6 適合性評価等にかかわる制度の整理

特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

## ② サイバー・フィジカル・セキュリティ・ 基 専 応 フレームワークを活用したサプライ チェーン・セキュリティの確保

奥家敏和

経済産業省商務情報政策局  
サイバーセキュリティ課

### サイバー・フィジカル・セキュリティ 対策フレームワーク (CPSF) の策定

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会「Society 5.0」の実現を提唱している。また、経済産業省では、「Society 5.0」の実現へ向けてさまざまなデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取り組みを推進している。

あらゆるものがつながる「Society 5.0」「Connected Industries」では、企業間・産業間のネットワーク化が進展して新たなつながりが生まれる中で、付加価値を創造するための一連の活動であるサプライチェーンの形態も、これまで取引することのなかった新たな相手を巻き込んだ柔軟かつ動的な構成へと変化する。また、サイバー空間とフィジカル空間が相互に作用しあう中での新たな付加価値の創造も期待される。

高度にネットワーク化され、動的に構成されるサプライチェーンにさまざまな主体が参加するような状況においては、一企業が取り組むセキュリティ対策だけでサイバーセキュリティを確保していくことには限界がある。このため、それぞれの企業がセキュリティ・バイ・デザイン等の観点を踏まえて、企画・設計段階から製品やサービスのサイバーセキュリティ対策を実施することに加え、ビジネス活動の

レジリエンスまで考慮に入れた上で、関連企業、取引先等を含めたサプライチェーン全体としてセキュリティ対策に取り組むマルチステークホルダによるアプローチや、データ流通におけるセキュリティも含めて、サイバーセキュリティ確保に取り組む必要がある。そのため、経済産業省では、「産業サイバーセキュリティ研究会ワーキンググループ1 (制度・技術・標準化)」を中心として、新たな産業社会において付加価値を創造する活動が直面する新たなリスクに対応していくためのセキュリティ対策の指針を「サイバー・フィジカル・セキュリティ対策フレームワーク」(以下、「CPSF」)として取りまとめ、2019年4月18日に初版を公表した。

CPSFは、産業界全体を対象としたサイバーセキュリティ対策を考えるためのモデル的枠組みである。一方、各産業分野で守るべき資産やセキュリティ対策に割けるリソース等が異なることから、WG1の下に産業分野別SWGを設置し、CPSFをベースに各産業分野におけるセキュリティ対策の検討を進めている。その上で、CPSFをベースに対策を進めるにあたって、サイバー空間とフィジカル空間のつながりにおける信頼性の確保やソフトウェア管理など、さらに詳細な検討が必要とされる分野横断的課題を検討するために、3つのタスクフォース (TF) を設置し、議論を進めている。

本稿では、CPSFの基本的な考え方およびCPSFの社会実装に向けた取り組みの1つとして、分野横断的課題の1つであるIoT機器・システムにもとめられるセキュリティ・セーフティ対策についてま



特集  
Special Feature

視野に入れた信頼性の確認などがなされて初めて信頼性が確保されるといえる。

第三層：サイバー空間におけるつながり

最後に、「サイバー空間におけるつながり」では、サイバー空間で流通するデータそのものが信頼性の基点となる。サイバー空間では、多様なデータが生成・編集・加工され、さまざまな主体の間で自由に流通することで、柔軟で動的なサプライチェーンが形成されることとなり、それこそがサイバー空間で付加価値を創造する基礎となる。「Society 5.0」[Connected Industries]では、マネジメントの信頼性が確認された企業・組織だけではなく、さまざまな主体がこれらの活動に関与する可能性があることや、また、主体が判明しないデータを活用しなければならないことにも留意しなければならない。そのため、目的どおりの価値を創造するためには、プロセスに関与するデータそのものの信頼性の確保が不可欠となる。

このように、サイバー空間とフィジカル空間が一体化した社会における付加価値の創造活動においては、3つの視点から信頼性を確保するセキュリティの取り組みが必要であり、これらを「層」として信頼性の基点と捉えることで、発生し得るインシデント、そのリスク源を明らかにし、対策の方向を示す

ことが可能となる。

リスク源の洗い出しと対応方針の整理

三層構造モデルに基づいて、各層において守らなければならない機能・役割の整理が可能となる。CPSFでは、表-1に示すように各層の特性、機能・役割と想定される分析対象の具体的なイメージをはじめとして、新たなリスク源を洗い出す際に考慮すべき観点をまとめており、リスクアセスメントにおける分析対象の明確化に活用することができる。

セキュリティ対策の概要

CPSFでは、図-2に示すように、各層における機能、セキュリティインシデント、リスク源、対策要件を整理している。具体的には、CPSFの添付Bで各層の機能、想定されるセキュリティインシデント、セキュリティインシデントを引き起こし得るリスク源と、リスク源に対するセキュリティ対策要件との対応関係を示している。また、添付Cでは、実際にセキュリティ対策を講じる場合の対策の範囲や、対策を導入・運用する場合の相対的成本等を考慮したレベル別のセキュリティ対策例を示している。これらを活用することで、企業・組織等のセキュリティ対策の担当者は、対象となる企業・組織等の

階層	特性	機能・役割	分析対象	分析対象の具体的なイメージ
第1層	各組織の適切なガバナンス・マネジメント	各組織のセキュリティマネジメント 【信頼性の基点】組織・マネジメント	組織で管理されるモノ・システム等 組織内で流通するデータ等	社員、従業員 企業のIT資産等
第2層	フィジカル空間とサイバー空間のつながり拡大	フィジカル空間とサイバー空間との間のデータのやりとり 【信頼性の基点】ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	データを転写するモノ・システム 転写されるデータ等	センサ アクチュエータ 3Dプリンタ 監視カメラ等
第3層	サイバー空間で組織を超えた多様・大量のデータの流通・処理	データの送受信、加工・分析、保管 【信頼性の基点】データ	データを送受信/加工・分析/保管するモノ・システム 組織を超えて流通するデータ等	サーバ ルータ スマートメータ オープンデータ等

■表-1  
三層構造に基づく分析対象および具体的なイメージ

特集  
Special Feature

システムや動的に重要度が変化する守るべき資産の重要度、リスクアセスメントの結果に応じた適切なセキュリティ対策を検討することができる。

## CPSF のさらなる社会実装に向けて

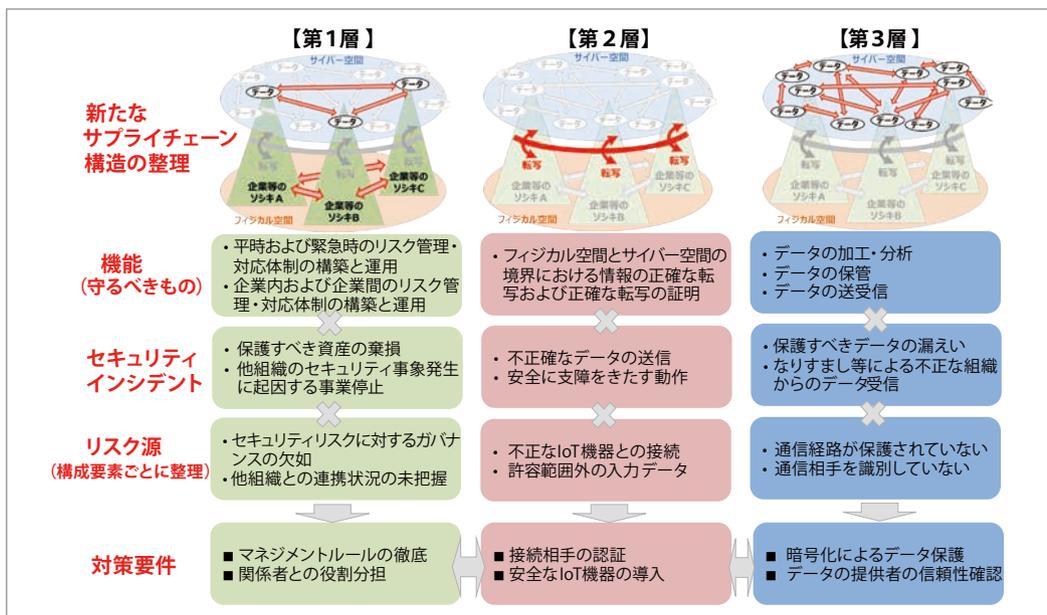
経済産業省サイバーセキュリティ課では、CPSFの産業界への具体的な実装を目指して、産業構造や商習慣などの観点から踏まえて、各産業分野で求められる具体的なセキュリティ対策の検討を推進している(図-3)。特に、さらに、IoT 機器・システムの信頼性(第2層)、データマネジメント(第3層)、ソフトウェアの管理手法といった産業横断的な対策が求められる課題については、タスクフォースを立

ち上げて別途検討を進めている。

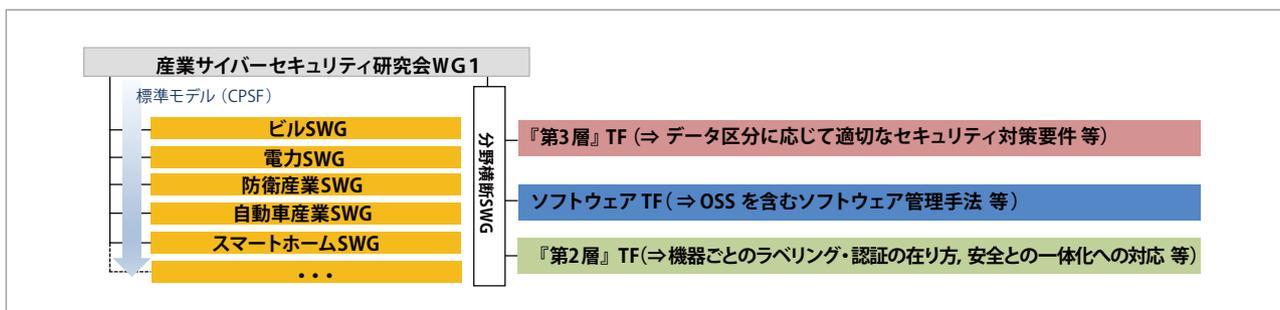
## IoT セキュリティ・セーフティ・フレームワークの策定

先述のとおり、「Society 5.0」においては、フィジカル空間とサイバー空間の境界における転写機能の正確性を確保することが特に重要となる。フィジカル空間とサイバー空間をつなぐ機器・システム、すなわちIoT 機器・システムのセキュリティの確保が重要になる。

IoTセキュリティガイドライン(平成28年7月IoT推進コンソーシアム、総務省、経産省)でも触れられているように、簡易な情報サービスの分野に使用されるIoT 機器と、工場や社会インフラシス



■ 図-2 各層におけるセキュリティ対策の概要



■ 図-3 CPSFに基づくセキュリティ対策の具体化・実装の推進

## 特集

## Special Feature

テム等の安全にかかわる分野で使用される IoT 機器では、求められるセキュリティレベル、セキュリティ対策の目的、優先度が異なる。今後、IoT の活用の拡大に伴い、それぞれの分野の特殊性・多様性を踏まえて、使用分野ごとに個別・具体的な IoT 機器・システムに対して実際のセキュリティ対応が進んでいくことになると考えられる。その過程において、サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して、包括的に課題を捉える統一的な手法が欠如しているため、それぞれの分野や業界において別々の検討プロセスを経て、独自のセキュリティ・セーフティ対策等が設定されることが懸念される。それぞれの対応策に不整合が生じれば、社会として新たな仕組みを受容・管理していくためのコストが増大する恐れがある。そこで、IoT システムの信頼性（第 2 層）に関する横断的課題議論する TF においては、『サイバー空間とフィジカル空間のつながり』における信頼性確保をテーマに議論を行い、IoT セキュリティ・セーフティ・フレームワークを策定した。

### フレームワークの基本的考え方

サイバー空間とフィジカル空間をつなぐ新たな仕組みである IoT にはさまざまな形態およびそれに伴うセキュリティ上の課題があり、さらに、実際にインシデントが発生した場合の被害の態様もきわめて多様である。IoT を構成する機器・システムに対して一律のセキュリティ要求を設定した場合、仮にその要求が満たされていても、それでは多様なセキュリティ上の課題に十分に対応することはできない。

IoT 機器・システムのセキュリティ対策を検討する際は、この多様性に対してどのようにアプローチするのかがポイントとなる。本フレームワークでは、サイバー空間とフィジカル空間をつなぐ新たな仕組みである IoT 機器・システムの“多様性”という論点にアプローチするための手段として、この仕組みを構成する機器・システムについて、リスクの捉

え方とその対応にかかる基本的な考え方を集約した 3 つの軸を活用し、カテゴリ化するとともに、適切な対策の内容を整理して比較・検討できるようにすることを提案している。

### IoT 機器・システムに潜むリスクの整理

前述のとおり、IoT 機器・システムのセキュリティ上の課題は多様なものである。そこで、IoT 機器・システムに潜むリスクに基づいてカテゴリ化し、マッピングする 2 つの軸を設定することとした。

第 1 軸は、発生したインシデントの影響の回復困難性の度合いである。回復の困難性については、まず、人命が失われればそれが回復されることはない。また、インシデントの発生の結果、重度の身体障害が発生した場合、完全に回復できるとはいえないケースが少なくない。こうした、インシデントによる影響が回復できるものか否か、また、回復ができるものについては早期の回復ができるか否か、という判断軸を第 1 軸として設定した。

第 2 軸は、インシデントによる資産の毀損、経済活動や社会への影響等の事象を金銭的価値に換算した場合の大きさを基準としたものである。

2 軸の整理を基に機器・システムをマッピングした例を図-4 に示す。前述のとおり、IoT 機器・システムのセキュリティ上の課題は多様であるため、それぞれの機器・システムにおける適切な対策も一様ではない。しかしながら、このカテゴリに基づいて検討を行うことで、一般に右上にカテゴリ化されるものほどインシデントによる影響が大きい傾向があるため、より重厚な対策が必要であると考えられる一方、左下にカテゴリ化されるものほど、軽微な対策で十分な可能性があると考え整理することが可能となる。

### 求められるセキュリティ・セーフティ要求の整理

第 1 軸と第 2 軸を活用し、フィジカル・サイバー空間をつなぐ機器・システムについて、そのリスクを踏まえてカテゴリ化した上で、本フレームワークでは、IoT 機器・システムのセキュリティ対策を包

特集  
Special Feature

括的に整理するために、求められるセキュリティ・  
セーフティ要求の観点という第3軸を設定する。

第3軸は、図-5のように第1軸と第2軸で形成  
される平面に直交する形で、いわば3次元を構成し、  
第1軸と第2軸によって整理されたそれぞれのカテ  
ゴリに求められるセキュリティ・セーフティ要求の  
観点を示す役割を果たすものである。

第3軸は、セキュリティ・セーフティを確保する

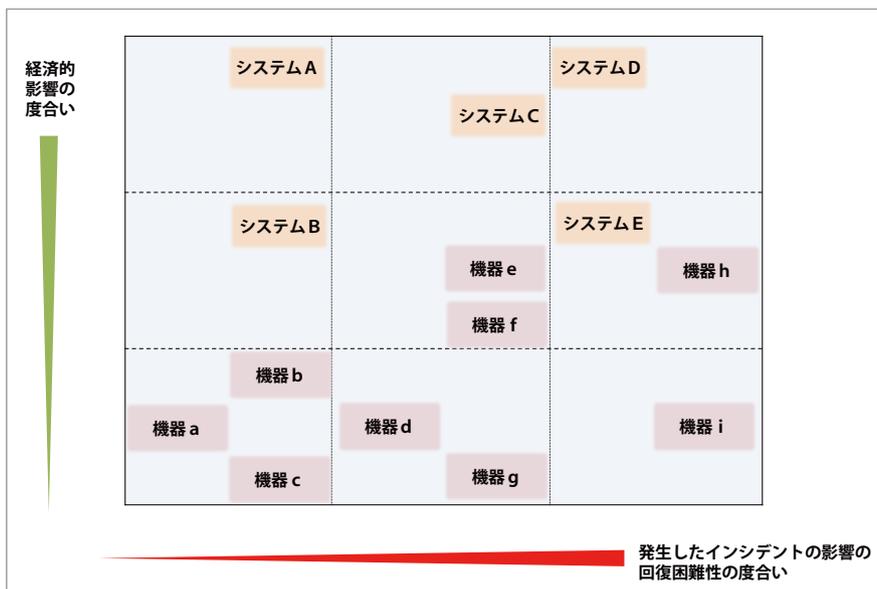
ための手法を以下の4つの観点から整理している。

第1の観点は、運用前（設計・製造段階等）にお  
ける機器・システムの確認要求である。IoT機器が  
実際に利用に供される前の段階で、機器・システム  
そのものが必要なセキュリティ・セーフティ対策を  
講じられていること、または当該機器・システム等  
の生産者や供給者、検査者、場合によっては生産設  
備・工場等が必要な能力条件等を満たしていること

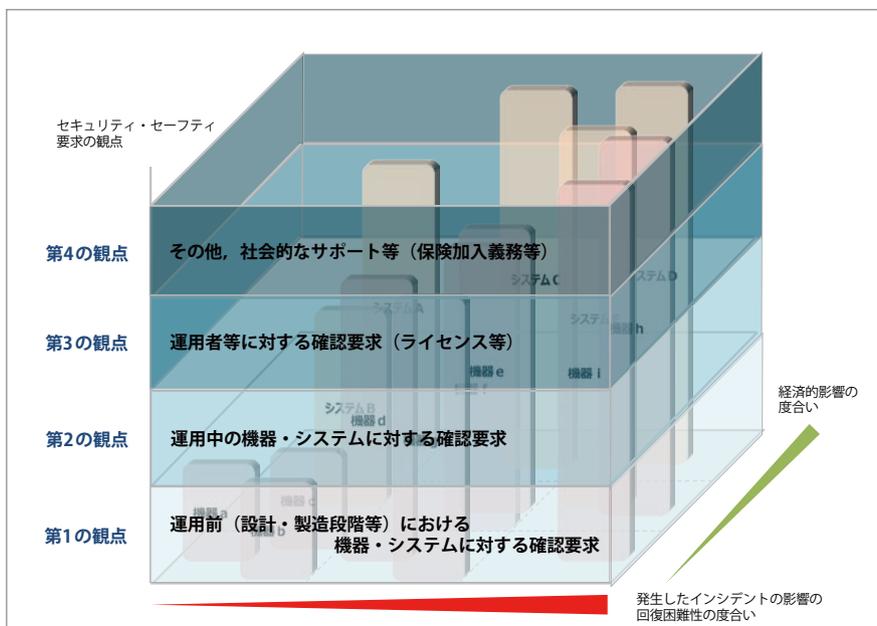
などを確認することを求めるものである。確認の方法に関して  
は、自己宣言や第三者認証などさまざまな形態があるが、求め  
られる確認レベルの専門性や客観性を踏まえて設定されること  
となる。

第2の観点は、運用中の機  
器・システムに対する確認要求  
である。運用中に発生する故障  
や、実施されるソフトウェアの  
アップデートやメンテナンスな  
どによって、想定外の問題が発  
生する可能性があることから、  
運用開始後に、ライフサイクル  
やサービス期間も考慮しながら  
機器・システムを確認すること  
を求めるものである。この観点  
の確実な実施を求めていくため  
には各ステークホルダにおいて  
役割や責任分界点を明確化する  
など、より社会的な仕組みを用  
意することが必要となる。

第3の観点は、機器・システ  
ムの運用・管理を行う者の能力  
に関する確認要求である。機器・  
システムの誤使用・誤操作など  
によって発生するインシデント  
の影響が、セキュリティ・セー



■図-4 フィジカル・サイバー間をつなげる機器・システムの Kategoriz のイメージ



■図-5 カテゴリに応じて求められるセキュリティ・セーフティ要求の観点的イメージ

## 特集 Special Feature

フティ対策だけでは許容できる水準ではない場合には、機器・システムの運用・管理を行う者が当該機器・システムを適切に運用・管理するために必要な能力を持っていることを確認することを要求することになる。

第4の観点とは、そのほか、社会的なサポート等の仕組みの要求である。インシデントが発生した場合の影響が非常に大きく、当該仕組み等の所有者が個々に賠償等の対処を実施することが容易ではないケースの場合には、あらかじめ保険加入を義務付けるなどの社会的なセーフティネットを講じることを求めるものである。

なお、第3軸における4つの観点は、それぞれが必ずしも完全に独立したものではない一方、必ずしもすべての観点での要求が求められるものではない。複数のステークホルダが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダにおける負担について、各ステークホルダが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステー

クホルダ間で合意する必要がある。したがって、機器・システムに対する直接的な対策は当然重要ではあるが、単独のステークホルダがすべての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。

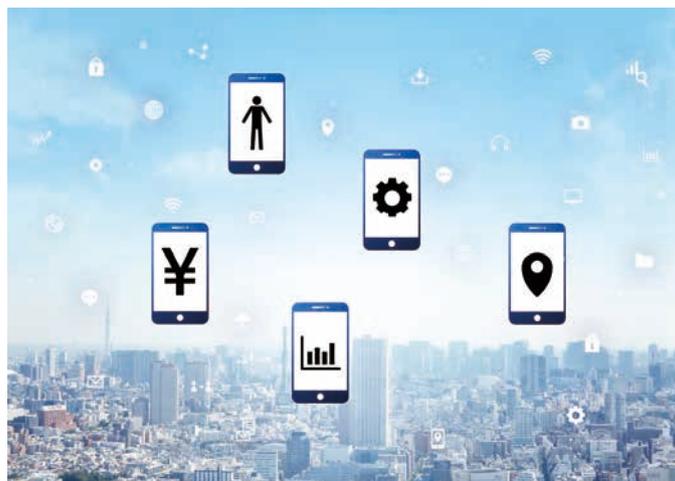
### フレームワークの活用の促進に向けて

今後、IoTを活用しようとする主体が本フレームワークを活用することにより、一定程度の整合性を確保しながらセキュリティ・セーフティ対策を検討することが可能となる。本フレームワークの活用がより一層促進されるため、ユースケースの整理を進めていく予定である。

(2020年12月22日受付)

#### ■奥家敏和

1995年通商産業省(当時)入省。JETRO ニューヨーク、2013年資源エネルギー庁長官官房総合政策課、2015年貿易経済協力局貿易管理部安全保障貿易管理課長、2016年安全保障貿易管理政策課長を経て、2017年より現職。



[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

## ③ サプライチェーン・セキュリティの脅威と 基 専 対策の動向

小川隆一



小山明美



(独) 情報処理推進機構

### IT サプライチェーン

IT システム・サービスの企画・設計・製造・運用・保守・利用・提供等のプロセスを複数の組織が分担し、一連の流れとして活動する形態を IT サプライチェーン (以下、サプライチェーン) と呼ぶ。多くの企業では、IT システム・サービスの調達、開発、運用の業務を系列企業やビジネスパートナー等に委託し、サプライチェーンは事業に不可欠となっている。

本稿では、サプライチェーン上で発生したセキュリティインシデント事例と脅威の種類、脅威、それに対する政府の施策、企業の対策の実態について述べる。

### セキュリティインシデント事例

サプライチェーン上で発生するインシデント事例は日々発生している。本章では代表的な事例を、IPA が 2017 年度に実施した調査およびその後公開された情報を基に紹介する。

#### 攻撃による情報漏えい

既知・未知の脆弱性を突いた攻撃により国内外で情報漏えいが発生している。技術的な対策不備だけでなく、責任分担やルール順守といった組織的な対策の問題も原因となっている。

2011 年、国内のインテリア通販サイトが SQL イ

ンジェクション攻撃を受け、クレジットカード情報が漏えいした。同サイトの構築について契約した当時、関係政府機関から SQL インジェクション攻撃に対する注意喚起、および対応方法が公開されていたが、サイト構築の委託元の要件にはこの脆弱性への対応が指定されず、委託先からも対策の提案はされなかった。

2017 年、プロスポーツリーグのチケット販売サイト、ファンサイトの運用を委託されていたチケット販売会社が Web サイトの脆弱性を攻撃され、個人情報、クレジットカード情報等が漏えいした。これらの情報は保管しないと発注仕様や運用ガイドラインに定められていたが、再委託先で守られず、情報がデータベース・通信ログに残っていた。また委託先はこの運用状況を把握しておらず、確認の不備が本質的な原因だったと報告された。

2018 年、自治体の教育ネットワークシステムの公開用サーバへの不正アクセスが確認され、児童、生徒および保護者の個人情報が流出した可能性が報告された。この公開用サーバは、委託先事業者のデータセンタに設置されたが運用は委託元が行う、という役割分担が委託元の担当者に周知徹底されなかった。このため、放置された脆弱性が悪用されてバックドアが作られた。

#### システム停止・サービス障害

クラウドサービス事業者は担当部分のセキュリ

## 特集 Special Feature

ティについてさまざまな対策を施しているが、システム停止・サービス障害は起きており、利用者が多いことから影響が大きくなることがある。

2019年、クラウドサービスが数時間利用できなくなる障害が世界最大級の実績を持つ複数のクラウドサービス事業会社で発生した。データセンターのメンテナンス作業やオペレーションでの設定変更の誤り、サーバのオーバーヒート等、原因はさまざまであった。クラウドサービスが社内のメールや事務処理システム、ネット販売サイト、受発注システム等の業務システムに幅広く利用されていたため、業績や事業継続にも影響するような支障を与えた。

2019年、自治体向け IaaS (Infrastructure as a Service) でシステム障害が発生し、サービスを利用する複数の自治体で Web サイトが閲覧できなくなる等の障害が発生した。ストレージのファームウェアの不具合に起因したハードウェア故障、およびストレージの復旧後、データへのアクセス処理が正しく動作しないという2つの不具合が複合的に発生したことで復旧に時間を要した。

### 内部不正

委託先や再委託先の従業員による不正は検知が困難であることから発見が遅くなり、長期化して被害が大きくなることもある。

2014年、大手金融機関のシステム保守管理業務を請け負っていた再委託先の元従業員が顧客のカード情報を不正に取得し、キャッシュカードを偽造した。この元従業員は長年同一業務に携わり、システムにかかる権限が集中していた。

同じく2014年、教育出版事業会社で国内最大級の個人情報漏えい事故が発生した。原因は、グループ会社からの業務委託で運用を担当していた元従業員による金銭目的の内部不正だった。

2019年、リース契約満了により返却されたハードディスクの廃棄を再委託された会社の従業員が当該ディスクを窃盗・転売し、消去予定であった自

治体の情報が漏えいした。多くの企業や自治体で IT 機器やストレージのリース契約が行われており、IPA の「情報セキュリティ 10 大脅威」では、内部不正が 2020 年 2 位となるなど、注目された (図-1 参照)。

### 踏み台

調達したツールやソフトウェアの正式なダウンロードサイト、更新サイトが踏み台となってウイルス感染する被害が発生している。手口が巧妙で利用者側の対策が困難な例である。

2017年、ウイルスが混入された PC 最適化無料ツールが正規のダウンロードサーバで配布され、数百万台の PC に対して不正なアップデートが実行されたと推定されている。このウイルスが感染した PC が属するドメインから攻撃対象の企業を選別して攻撃する仕組みで、数十組織が攻撃された。

2019年、PC にプリインストールされたドライバ、アプリケーション等の自動更新機能を悪用した攻撃が報告された。攻撃者は、攻撃対象を数百人のユーザに絞り込み、標的となった PC 上で実行された場合のみ、次のステージのウイルスをダウンロードする仕組みとしていた。改ざんされた更新プログラムが配布された数は数百万台と推測されている。

### なりすまし

取引先を装い、指定口座への振込等を促すビジネスメール詐欺による被害が多数発生している。2017



■ 図-1 内部不正による情報漏えい  
出典) IPA「情報セキュリティ 10 大脅威 2020」

## 特集

## Special Feature

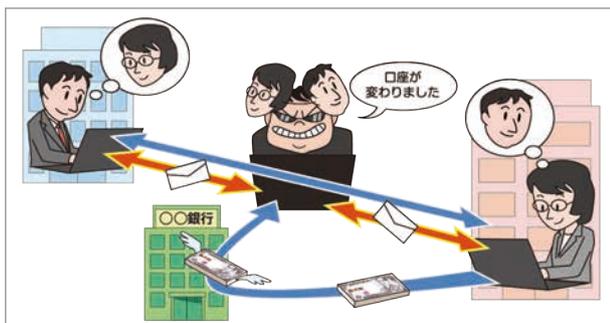
年には日本の航空会社が米国の金融機関になりすました攻撃者から航空機リース料(約3億6,000万円)の不正送金被害に遭った。偽メールのアドレスは正規のものと1文字違いであり、直前に送られていた正規の請求書の「訂正版」として悪意のPDFファイルが添付されるなど、手口は巧妙であった。

何らかの手段によりメールが盗聴され、得られた情報を悪用して取引先になりすまされた場合、メールから攻撃を判断することが困難なことも多く、不正送金の被害が続いている(図-2参照)。

## サプライチェーンの類型とセキュリティの役割分担

インシデントはさまざまな場面で発生しており、さまざまな対策は検討されている。しかし、攻撃の手口の巧妙化やシステム・サービスの複雑化などにより、1つの企業・組織の限られたリソースや情報だけでは、インシデントを防ぐことは非常に困難になっている。サプライチェーン全体でリスクを洗い出し、対策を検討し、各々が役割を果たしていくことが求められる。

サプライチェーンには、取引するものの種別によりいくつかの形態が存在している。以前は取引する主なものは有形の製品、あるいは、人による役務が対象であったが、ビジネスのIT化の急激な発展、クラウドサービスの普及等により、さまざまな形態が利用されるようになった。



■図-2 ビジネスメール詐欺による金銭被害  
出典) IPA「情報セキュリティ10大脅威 2020」

この類型を表-1のように整理する。右側の欄には各類型の実装例を示している。

### 製品・サービスの調達

市販品として調達された製品・サービスのセキュリティ対策は提供者(以下、委託先)が実装しているが、利用者(以下、委託元)の利用開始時に、提供された対策が明示されていないことがある。委託元は、委託先がどのようなセキュリティ対策を実践しているか、セキュリティに関する認証を取得しているか等の情報を入手し、調達後に自社で行う必要があるセキュリティ対策を確認、実施する必要がある。

### 開発の委託・運用の委託

開発・運用委託においては、委託元が必要な機能・サービスを要件として委託先に実装してもらう。セキュリティについても委託元が非機能要件として明示することが望ましいが、委託元にセキュリティの専門知識が十分あるとは限らないため、委託元と委託先でリスク対応を検討し、合意の上で対策を実装することが望ましい。

### サプライチェーンの脅威の類型

サプライチェーンは、委託元・委託先の二者だけでなく、再委託先、再々委託先と、取引関係が連鎖することがある。その一連のサプライチェーンのどこかにセキュリティ上の問題が発生すると、影響がサプライチェーン上のほかの組織に波及する恐れがある。(独)情報処理推進機構(以下、IPA)が

■表-1 サプライチェーンの類型

製品・サービスの調達	IT機器・IoT機器・ツール・ソフトウェア調達
	SaaS/IDaaS
開発(設計・製造・検査)の委託	請負・委任・派遣
運用の委託	自社システム運用・保守
	自社システム監視等のマネージドサービス
	IaaS/PaaS

特集  
Special Feature

発表している「情報セキュリティ 10 大脅威」では、2019 年、2020 年と連続して組織の脅威第 4 位にサプライチェーンがランクされており、深刻な脅威と認識されていることがうかがえる。

図-3 では委託元 A 社と委託先 B 社の間では、委託契約書に基づき、機密情報が適切に取り扱われており、悪意のある第三者からの攻撃を防ぐことができている。しかし、A 社の再委託先 C 社のセキュリティ対策に不備があり、悪意のある第三者の攻撃を防げず、結果として A 社の機密情報が窃取されてしまった例を表している。

同じ企業・グループであれば、セキュリティガバナンスにより、セキュリティポリシーに従った対策の実施、管理を徹底できる。それ以外の場合は契約で二者間のセキュリティに関する権利義務関係を取り決めるが、そのガバナンスはサプライチェーン全体には及ばず、セキュリティ対策が弱い組織が攻撃者に狙われる可能性がある。

サプライチェーンの脅威の類型を表-2 に示す。委託先が管理する情報やシステムが攻撃の対象や障



■図-3 サプライチェーンの弱点を悪用した攻撃  
出典) IPA「情報セキュリティ 10 大脅威 2020」

■表-2 サプライチェーン上の脅威

委託先で被害や事故が発生するもの	運用しているシステムに対する外部攻撃
	システム設定ミスや運用担当者の作業ミス
	開発環境、運用環境への攻撃
販売元や委託先を経由して委託元に被害が発生するもの	内部不正
	不正なプログラムの埋め込み
	脆弱性対策の不備
	踏み台
	なりすまし

害の原因となる場合、および委託先の管理や対策不備により製品・サービスを受け取る委託元に被害が発生する場合、の 2 つの類型がある。

## サプライチェーンリスク対応の現状

前述のように、サプライチェーン上のセキュリティリスク（以下、サプライチェーンリスク）は関連する企業全体に影響する深刻な事業リスクである。以下ではサプライチェーンリスクに対する企業の認識や取り組みについて、IPA の調査結果を交えながら述べる。

### 経営層にとっての課題

経済産業省が公開している「サイバーセキュリティ経営ガイドライン」では経営層が実践すべき指示項目（重要 10 項目）を定めているが、同項目に関する簡易調査（IPA, 2020 年 6 月公開）によれば、企業はサプライチェーンリスク対応（指示 9）を資源のアサイン（指示 3）に次ぐ難しい課題であると認識している（図-4）。サプライチェーンに固有の攻撃手法があるわけではないが、サプライチェーン全体にわたる脆弱性の把握、対策の徹底の難しさが背景にあると考えられる。

### リスク対応の統制

サプライチェーンリスク対応では、共通のセキュリティポリシーの実施、脆弱性の解消、等でサプライチェーン上のセキュリティレベルを一定に保つことが重要であるが、それには委託元が委託先のセキュリティ対策の状況を把握し、必要な対策を実践させることが重要である。しかし、そのための十分な統制（ガバナンス）機能を委託元は持っていない。委託元・委託先の対策実施の約束は通常は契約で行うこととなるが、契約は二者間の権利義務規定であり、再委託先等の義務は明記されない。「委託先は業務を再委託しない」等を委託元が求める場合もあ

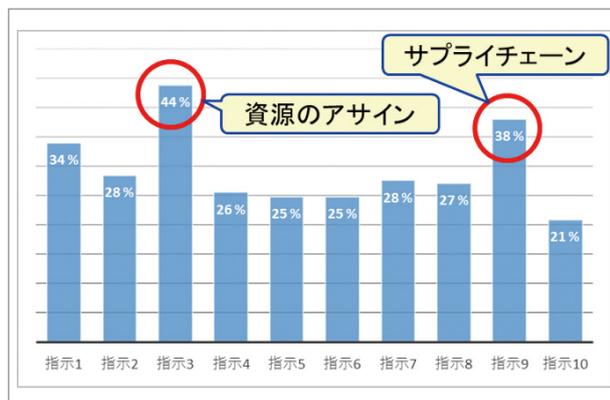
特集  
Special Feature

るが、「再委託先のセキュリティ対策は委託先が責任を持つ」とすることも多い。この場合どうしても統制は間接的になる。

また海外企業との取引がある場合、現地の法制度やIT環境の違い等から統制がさらに難しくなることがあり、海外に製造拠点・販売拠点を持つ企業には大きな課題となっている。

### 対策実施状況・検収時のチェック

委託先のセキュリティ対策が合意どおりに実施されているかのチェック、また、開発委託における検収時のセキュリティチェックは、サプライチェーンリスク管理の核心ともいえる重要な作業である。し



指示1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示2	サイバーセキュリティリスク管理体制の構築
指示3	サイバーセキュリティ対策のための資源（予算、人材等）確保
指示4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示5	サイバーセキュリティリスクに対応するための仕組みの構築
指示6	サイバーセキュリティ対策におけるPDCAサイクルの実施
指示7	インシデント発生時の緊急対応体制の整備
指示8	インシデントによる被害に備えた復旧体制の整備
指示9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策および状況把握
指示10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用および提供

■図-4 重要10項目実践で困っていること  
出典) IPA「サイバーセキュリティ経営が度ライン実践についてのアンケート結果」

かし、契約ごとに委託元が委託先への査察・監査、あるいはテスト等を行うとすると非常に高コストになってしまう。重要インフラシステムの開発等では、監査・ペネトレーションテスト等が入念に行われるが、通常のケースでは委託元がチェックシート等で委託先にセルフチェックを要請し、状況を確認している。ただしこの方式はあくまでセルフチェックであり、委託先の恣意によるバイアス（みんな高評価にして課題が見えなくなる等）は免れ得ない。また委託先から見ると、多くの委託元から似て非なるチェックシートをもらって個々に評価を行う負荷はかなりのもので、丁寧な対応が難しいという指摘もある。

対策実施状況チェックの負荷軽減については、たとえばJASA（日本セキュリティ監査協会）の推進する内部監査人によるチェック、JUAS（日本情報システムユーザー協会）によるセキュリティチェックシート共通化の検討等の試みがあるが、普及にはまだ時間が必要であり、当面は自前のチェックシートを委託元・委託先でうまく使いこなすことが求められる。

なお、ソフトウェア・IT機器調達時のテスト（不審な動作の発見等）も高コストであることからなかなか実践できないのが現状である。一部の機器については第三者機関がテスト・認証する方式（ISO/IEC 15408等）を利用できるが、ほかの場合には代替方式がない。

### リスクの可視化

IPAの2016年の調査では、直接の委託先のセキュリティ対策状況を把握していたとした企業が86%であるのに対し、再委託先以降の対策状況を把握していたとした企業は47%であった（図-5）。

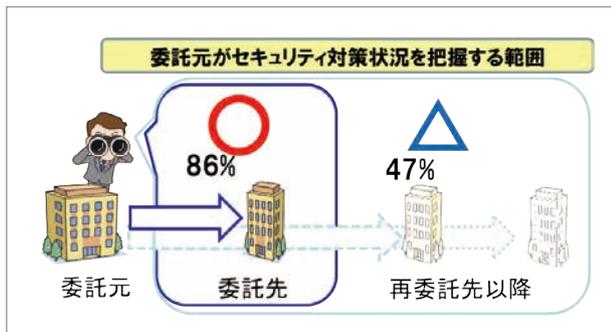
現在サプライチェーンは、海外調達、SaaS等のクラウド利用、IoT機器連携など、長大化・複雑化する傾向にあり、サプライチェーン全体におけるモノと情報のフロー、それらの管理責任、セキュリティ

特集  
Special Feature

対策状況を把握し、リスクポイントを明らかにすることはリスク対応の基本となるべきだが、現状では至難の技であると言える。

複雑化するサプライチェーンのリスクを把握する試みとして、経済産業省が「サイバーフィジカルセキュリティ対策フレームワーク」の構築を推進している。これは、米国 NIST（国立標準技術研究所）の策定した「サイバーセキュリティフレームワーク」を包含し、IoT サービスのサイバーとフィジカル両面にわたるリスクポイントを明確にするためのフレームワークである。

一方、リスク可視化のために企業は何をすればよいだろうか？ 難しい問いだが、次節の「コミュニケーションと情報共有」が1つの手がかりであると考えられる。



■ 図-5 委託元がセキュリティ対策状況を把握する範囲  
出典) IPA「情報セキュリティに関するサプライチェーンリスクマネジメント調査」

## コミュニケーションと情報共有

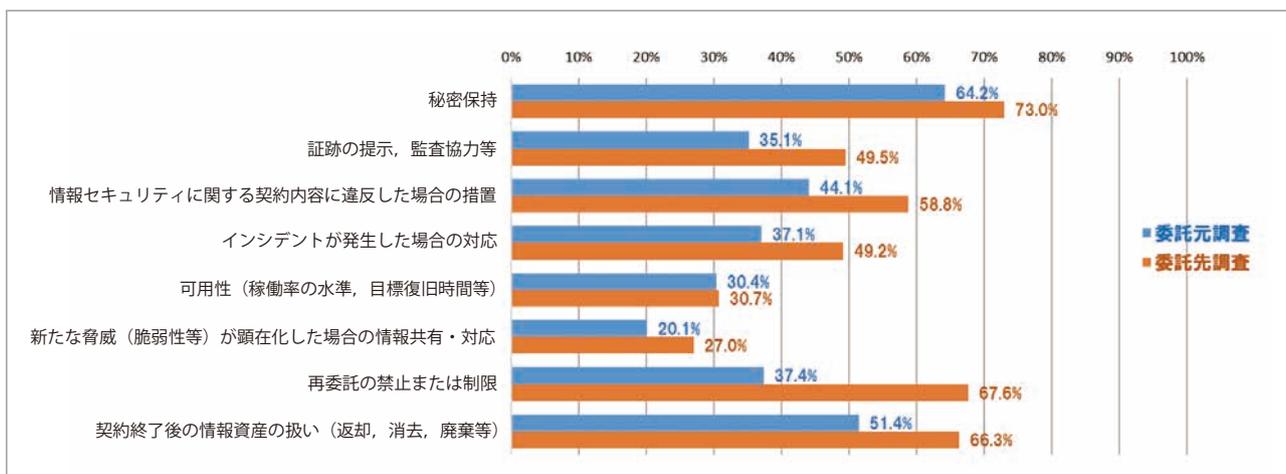
サプライチェーン上のステークホルダーが守るべき資産、対応すべきセキュリティ脅威、除くべき脆弱性について情報を共有し、合意することは重要であるが、これまでの IPA 調査により2つの課題が明らかになっている。

### ①委託元・委託先間の意思疎通のギャップ

日本企業・組織の傾向として、非 IT 系の委託元企業・組織には IT を専門とする人材が少ない。セキュリティに専門知識を持つ人材はさらに少数である。この結果、委託業務のセキュリティ要件が委託元で明らかにできず、委託先に任されてしまうこと、すなわち、委託元がセキュリティリスクを十分に把握しないままのお任せ発注が起り得る。

2019 年の IPA 調査によると、国内の IT 業務委託契約において、委託元が明確にしているセキュリティ要件で 60% を超えたものは「秘密保持」のみであり、ほかの要件には検討が及ばない傾向がうかがえる (図-6)。

IT 人材が委託元企業に少ない状況はすぐには変わらないが、少なくとも、セキュリティの脅威に直



■ 図-6 IT 業務委託時に明示している責任範囲の内容  
出典) IPA「IT サプライチェーンにおける情報セキュリティの責任範囲に関する調査」

面した場合の事業リスクの大小は委託元が判断するべきであり、リスク対応の詳細について委託先と合意することが求められる。

なお上記に関連して、2020年の民法改正において委託元・委託先の役割分担が見直され、委託元は発注の要件を具体化するよう求められている。十分な配慮が必要である。

## ②脅威・脆弱性に関する情報共有意識の弱さ

図-6はまた、納品物に新たな脆弱性が発見された場合等の情報共有・対応について委託元・委託先ともに意識が欠けている状況（契約に明示する割合が20%台）を示している。これによりたとえば、オープンソースを利用した開発委託等で、当該ソフトウェアに脆弱性が発見された場合の対応が後手に回り、攻撃を受ける可能性を高めてしまう（そもそも委託元が納品物にオープンソースが使われている、と把握できていないこともあり得る）。

脅威、脆弱性の情報、あるいはそれに対する対策（パッチ更新等）やインシデントや不具合が発見された場合の対応等について、ステークホルダ間で共有する意識と行動は非常に重要である。契約だけでなく、ITベンダの支援を受けた普及啓発の機会、業界団体やセキュリティ関連非営利団体との連携等を利用するなど、積極的な活動が望まれる。

なお、サプライチェーンに参画する中小企業もこうした情報共有に参画できることが望ましい。これ

に関連して、IPAが事務局となり、2020年11月にサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）が立ち上がった。

## 今後に向けて

本稿ではITサプライチェーンのセキュリティ脅威の類型を整理し、近年のインシデント事例を紹介した。またサプライチェーンリスク対応が企業のセキュリティ対策の中でも難しい課題であることを述べ、IPAの調査活動から得られた課題と対策の状況を紹介した。サプライチェーンに関連したインシデントは多岐に渡り、対応もさまざまである。また2020年に入り、委託先のテレワークにおける情報管理や私用端末・クラウド等の利用規則等、新しい業務形態への対応も必要になっている。企業間での情報共有、ガイドラインの活用、契約の見直し等、本稿で紹介した対策等を参考に実施できるところから始めていただきたい。

(2020年12月1日受付)

■小川隆一（正会員） r-ogawa@ipa.go.jp

1983年東京大学理学系大学院修士課程修了。同年日本電気（株）入社、研究開発に従事。2015年から情報処理推進機構にて調査分析に従事。電子情報通信学会、情報ネットワーク法学会各会員。

■小山明美（正会員） a-koyama@ipa.go.jp

1990年法政大学大学院工学研究科博士前期課程修了。同年日本電気（株）入社。2017年情報処理推進機構に出向し調査分析事業に従事。2018年情報セキュリティ大学院大学情報セキュリティ研究科修士前期課程修了。

特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

## 4 制御機器のセキュリティ認証制度


 基  
専  
応  
般


神余浩夫

三菱電機 (株)



山田 勉

(株) 日立製作所

### 制御システムへのサイバー脅威と対策

#### 制御システムへのサイバー脅威

2010 年以降、社会インフラおよび産業システムを狙ったサイバーセキュリティ・インシデントが増加している。

表-1 に、過去に話題となった制御システム関連のセキュリティ・インシデントを示す<sup>1)</sup>。

各国の専門家は、緊急課題として産業制御システムのセキュリティ対策に取り組みを開始し、国際標準や分野別ガイドラインの開発を進めている<sup>2)</sup>。その対策の骨子は、まず、対象システムの守るべき資産・人命についてリスクアセスメントを実施し、それらをいかなる脅威からどれくらいの堅牢さ (セキュリティレベル) で守るのかを評価する。そして、それぞれのセキュリティレベルに十分なリスク低減対策を講じて、リスクを許容できる程度に抑えることである。

ここで重要なのは、産業制御システムを構成する制御機器、監視装置やネットワーク装置等が求められるセキュリティレベルを満足していなければ、セキュアなシステムを構築できないことである。後付けでファイアウォールや侵入検知装置を追加しても、肝心の制御機器に脆弱性があっては、システムが停止するようなインシデントにとどまらず人身事故や爆発事故まで起こり得る。したがって、制御機器市場において、制御機器のセキュリティ規格適合が注目を集めている。

### 制御機器のセキュリティ認証とサプライチェーン

欧州 CE マーキングのように、製品供給者が規格適合性を自ら表明する自己宣言は、製品のセキュリティ対応を示す簡便な方法である。問題は、その自己宣言の質が製品供給者を信用できるかに依存することにある。やはり、製品を調達するシステム構築者が、自身の責任で製品の規格適合性を評価するべきだろうか。だが、制御機器のセキュリティ規格適合性評価は技術的難易度も、必要な試験機材も、評価の工数も多大であり、調達者側の負担が大きい。

信頼できる第三者による製品の規格適合性評価は、自己宣言と調達者評価の利点を併せ持つ。然るべき審査機関がセキュリティ規格適合性を認証した製品であれば、調達者は安心して購入および使用できる。また、同一製品の評価を繰り返す、何度も自己宣言評

■表-1 最近の制御システムのセキュリティ・インシデント

年	名称	インシデント
2010	Stuxnet	イランのウラン濃縮工場の遠心分離装置を破壊
2015	BlackEnergy	ウクライナの電力システムを停止 = 停電
2016	Industroyer	ウクライナの電力開閉器を操作 = 停電
2017	HatMan (Triton)	サウジアラビア石油プラントの安全計装制御装置を異常停止 = プラントシャットダウン
2020	EKANS	アルゼンチンの配電会社のカスタマサービスに障害

## 特集

## Special Feature

価データを提供することもないので、供給者と調達者の双方の労力も軽減できる。いま、いくつかの国際標準化団体が、セキュリティ規格適合性評価の枠組み(スキーム)の開発および運用を始めつつある<sup>☆1</sup>。

制御機器のセキュリティ証明のためには、製品を構成するハードウェア、ソフトウェア部品についても、セキュリティ保証しなければならない。脆弱性のある怪しい部品は使えないし、脆弱性が見つかった際には迅速にセキュリティパッチが開示されなければ、その部品は採用できない。すなわち、制御機器製品の供給者と調達者を中心に、部品から社会システムまで巨大なサプライチェーンをセキュリティ保証することが、求められている。

本稿では、セキュアな産業制御システムを構築するためのセキュリティ製品認証の国際標準の動向について解説する。さらに、部品や製品のセキュリティを保証するためのセキュア・サプライチェーンの状況についても述べる。

## 制御システムのサイバーセキュリティ標準

### ISA99

制御システムのサイバーセキュリティ標準の草分けは、国際制御学会 (ISA : The International Society of Automation) の「ISA99産業自動制御システムのセキュリティ」である<sup>☆2</sup>。ISA99は、情報漏洩や機密流出を扱う情報セキュリティとは異なり、サイバー脅威から産業オートメーション制御システム (IACS) の操業妨害や事故を防ぐことを目的に開発された。2001年の米国テロにおいて社会インフラがサイバー攻撃を受けたことから、この標準化が急務となった。

ISA99の初版は2004年に発行されたが、当時はUNIXやインターネットなどのオープン技術の脆弱性が狙われることはあっても、各社独自のコントローラやプロトコルが攻撃を受けることはないと考えられていた。そのため、情報セキュリティと同じ製品や技術で

<sup>☆1</sup> SP800-82, <https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final>

<sup>☆2</sup> ISA99, <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>

制御システムも守れるとして、制御システムに特化した技術開発は進まなかった。ところが、2010年にイランのウラン濃縮工場の遠心分離装置を破壊したマルウェア Stuxnet 以降、各社独自のコントローラやプロトコルの脆弱性がサイバー脅威に直接狙われるようになり、ISA99が再評価されることになった。

### IEC 62443

もともと、情報セキュリティ技術の標準化は、「ISO/IEC/JTC1/SC 27 情報セキュリティと個人情報保護」にて議論されていた。しかし、制御システムおよび組込みシステムは、情報セキュリティ専門家にとって未知の分野であり、制御機器各社固有の技術の壁にも阻まれて、議論は進まなかった。

2010年、ISAとIECは産業制御システムのサイバーセキュリティ標準を共同開発することで合意し、ISA99をベースとして「ISA/IEC 62443 産業通信ネットワークシステムセキュリティ」を制定することになった。ISA99はANSI規格でもあったが、IEC国際標準になったことで多くの標準や団体組織との整合性を求められるようになった。

表-2にISA/IEC 62443シリーズの構成を示す<sup>☆3</sup>。標準は読者想定によって、共通、アセットオーナー、インテグレート、制御機器に分類される。斜字は現在開

<sup>☆3</sup> IEC/TC65 work program, [https://www.iec.ch/dyn/www/?fp=103:23:25380131696612:::FSP\\_ORG\\_ID,FSP\\_LANG\\_ID:1250,25](https://www.iec.ch/dyn/www/?fp=103:23:25380131696612:::FSP_ORG_ID,FSP_LANG_ID:1250,25)

■表-2 ISA/IEC 62443 シリーズの構成 (斜字は開発中)

対象	副番 規格名
共通	1-1 Concepts & models
	1-2 Glossary of terms
	1-3 Conformance metrics
	1-4 Lifecycle & use case
アセット オーナー	2-1 Requirements for IACS asset owners
	2-2 Security protection ratings
	2-3 Patch management
	2-4 Requirements for service providers
	2-5 Implementation guidance
インテ グレート	3-1 Security technologies
	3-2 Security risk assessment
	3-3 Security requirements & levels
制御機器	4-1 Product development life cycle
	4-2 Requirements for IACS components

## 特集 Special Feature

発中であり、発行済みのいくつかも改訂を進めている。表-2 以外にも、分野共通規格、分野ごとの標準、規格適合性評価のための基準など、新しい開発提案が続いている。これらの開発提案は国際投票による承認を要するため、現在手続きを進めている。

## NIST

NIST (National Institute of Standards and Technology) は、米国商務省に属する組織であり、サイバーセキュリティに関して多数の技術文書を発行している。主な文書を表-3 に示す。

特に、「SP 800-82 産業制御システムのセキュリティガイド」は、政府機関に産業制御システムを納入する際のセキュリティ要件を規定した文書であり、産業制御システムを構成する分散制御システム、プログラマブルコントローラ、監視システムなどの機能や設定について言及している<sup>3)</sup>。技術的に、ISA99 との関係性が深い。

## 経済産業省サイバーフィジカルセキュリティ対策フレームワーク (CPSF)

経済産業省が策定した CPSF (Cyber Physical Security Framework) は技術標準ではないが、産業システムやサービスのセキュリティ確保のための参照モデルとして国際的に知られている。CPSF の概念モデルを図-1 に示す<sup>4)</sup>。CPSF は、サービスをフィジカル空

間の企業間の繋がり (第1層) と、サイバー空間のデータの繋がり (第3層)、およびその両者間の「転写」機能による繋がり (第2層) から構成される。第1層はモノの動きすなわちサプライチェーン、第3層はデータの動きすなわちバリューチェーン、そして第2層は IoT とみなすことができる。各層が適切な信頼性確保の対策を講じることで、現実のサービスの信頼性 (セキュリティ含む) が保証できる。

たとえば、制御システムに使われる制御機器、およびその部品 (ハードウェア、ソフトウェア) は、第1層の取引により組み立てられる。調達者は、購入する制御機器およびその部品のセキュリティレベルや脆弱性について第3層の情報により調査する。ここで、制御機器の型名やバージョンがセキュリティ情報と正しく紐づいているか、虚偽や誤りがないかは、第2層が保証する。すなわち、すべての層が信頼できてこそ、セキュアな部品調達およびシステム構築ができる。

すでに技術蓄積のある第1層と第3層に比べて、第2層 IoT 転写機能の信頼性技術は、いまだ検討開発段階にあり、今後の発展が望まれる。

## 制御機器のセキュリティ認証

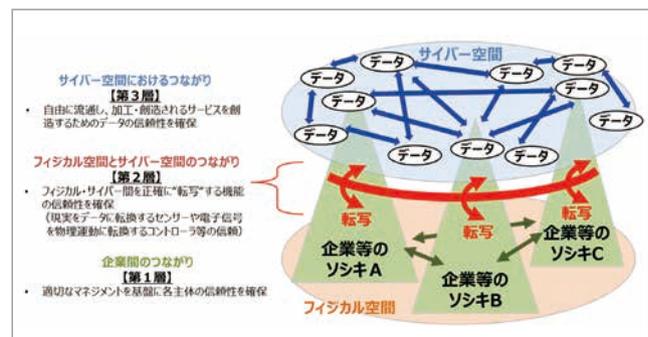
### 自己宣言と第三者認証

製品やサービスが法令や標準等の品質を満足することを保証する方法は、誰が規格適合性を試験および証明するかによって3つに大別される。

第1は、製造者または供給者による自己宣言である。

■表-3 制御システムのセキュリティに関する NIST 標準

文書	表題
SP800-30	Guide for Conducting Risk Assessments
SP800-40	Creating a Patch and Vulnerability Management Program
SP800-53	Recommended Security Controls for Federal Information Systems
SP800-61	Computer Security Incident Handling Guide
SP800-64	Security Considerations in the System Development Life Cycle
SP800-82	Guide to Industrial Control Systems (ICS) Security
SP800-83	Guide to Malware Incident Prevention and Handling
SP800-84	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities



■図-1 CPSF の3層モデル

特集  
Special Feature

製造者は品質保証のために、基準に従った試験を実施するので、それを根拠に規格適合の自己宣言を行う。供給者は、求めに応じて規格適合の根拠や試験結果を開示する。自己宣言は、供給者が信用できるかどうか鍵となる。

第2は、調達者が自らの基準で製品を指定する方法である。セキュリティ規格適合性は、技術的にも難しく、試験機材も高価であり、評価の工数も多く要する傾向にある。調達者に大きな負担がかかるため、余裕のある調達者にしか選択できない。

第3は、信用できる第三者機関による規格適合性試験および認証である。一般に、ISO 17025 試験所および校正機関の能力を有する試験所が、客観的に信用できる条件となる。以上3方式の対比を図-2に示す。

環境条件のように試験が簡単な場合、供給者による試験結果を再現追試できるため、自己宣言でも十分信用できる。しかし、技術的にも高度なセキュリティ規格適合性評価は、再試験が容易ではないことに加えて、供給者の評価が不適切な場合もある。調達者評価も、対象製品すべての脆弱性を調べるのは困難である。したがって、第三者評価が、供給者と調達者にとって評価の労力とコストの点でバランスが良い。特に、複数の調達者が同じ製品の評価を繰り返さなくてよい、供給者が高度なセキュリティ試験機材を揃えなくてもよいので、市場全体での規格適合性評価のコストは抑制できる。

技術的に高度かつ認証の信憑性も求められる制御機器のセキュリティ認証は、第三者認証が主流になる

と思われる。以下では、制御機器のセキュリティ認証制度の状況について述べる。

## ISAsecure

前述のISAは、2011年に審査機関であるISCI (ISA Security Compliance Institute) を立ち上げ、ISAsecure 認証スキームに基づく制御機器のセキュリティ認証を運用している。現在の認証制度は、制御機器の製品認証 CSA (Component Security Assurance, 旧 EDSA 認証)、システム認証 SSA (System Security Assurance) および開発組織認証 SDLA (Security Development Lifecycle Assurance) である<sup>☆4</sup>。

CSA 認証の試験項目を図-3に示す。まず、開発プロセスが IEC 62443-4-1 セキュリティ製品開発プロセス要求に適合しているか、開発文書等が揃っているかを確認する (SDA-C)。開発組織が SDLA 取得済みの場合、この試験の一部が免除される。次に、IEC 62443-4-2 制御機器のセキュリティ機能が要求に応じて実現されているかを評価する (FSA-C)。最後に、既知の脆弱性が塞がれているかを試験により確認する (VIT-C)。

ISAsecure 認証は、ISA/IEC 62443 に忠実かつ分野汎用的であるため、分散制御システム (DCS) や

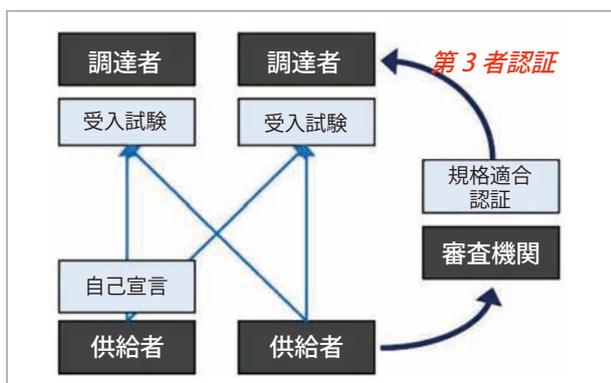


図-2 規格適合性評価の方式の対比

Component Security Assurance (CSA)	
Security Development Artifacts for components (SDA-C)	セキュリティ開発文書 IEC 62443-4-1 に準じた機器の開発・維持プロセス
Functional Security Assessment for components (FSA-C)	セキュリティ機能評価 IEC 62443-4-2 のレベルに沿ったセキュリティ機能
Vulnerability Identification testing for components (VIT-C)	脆弱性特定試験 既知の脆弱性に関するスキャン試験

図-3 CSA 認証 (製品認証) の試験項目

☆4 ISCI, <https://www.isasecure.org/en-US/Certification>

特集  
Special Feature

安全計装システム (SIS) など 42 機種 (2020 年 10 月時点) が認証を受けている。日本でも、(技術研究組合) 制御システムセキュリティセンター (CSSC : Control System Security Center) が、ISCI のライセンスを受けて EDSA 認証を実施している<sup>☆5</sup>。CSSC は現在国内唯一のセキュリティ製品認証機関であり、日本語で審査できる点が、国内供給者から支持されている。

### Achilles

Achilles Communications Certification 制度は、米国 Wurdtech 社 (現在は GE Digital 社の傘下) が、2008 年から開始した制御機器のセキュリティ認証制度である<sup>☆6</sup>。ISAsecure が規格に忠実なため審査に時間がかかるのに対して、審査期間を短縮するために通信堅牢性に注目した試験プログラム Achilles Test Platform を採用している。Achilles Test Platform の対応プロトコルを図-4 に示す。MODBUS/TCP や OPC UA など制御システムの代表的なプロトコルに対応している。Achilles Test Platform は代表的なファジングテスト；想定外の異常データを送信して対象機器の動作を確認するツールであり、多くの審査機関でも使われている。

Achilles 認証には、脆弱性対策の強度によって 2 段階のレベルがあり、Level2 はより厳しい要件となっ

ている。レベル1 認証 276 機種、レベル2 認証 528 機種 (2020 年 10 月時点) が公表されている。

### WIB

WIB (Werkgroup voor Instrument Beoordeling) は、主にオランダとベルギーのプロセス産業エンドユーザが参加する団体である。欧州各国の類似団体と連携して、制御機器のセキュリティ認証制度を運営している。そのために、前述の ISA や NIST などの国際的な標準化組織と連携をとり、標準化案について互換性や試験容易性について相互レビューを行っている<sup>9)</sup>。

WIB 認証の特徴は、ユーザ主導でセキュリティ要件を明確にして、供給者に適合する制御機器やシステムを開発させたことにある。供給者は、ユーザ要求が明確であり、実現性やコストの点で無理がなく、かつ調達条件となっていることから、制御機器の WIB 認証を推進した。WIB 認証には、ゴールド、シルバー、ブロンズの 3 つのレベルがあり、最初からゴールドを狙うのではなく、導入計画に従って段階的にレベルを上げていくことができる。

WIB 認証は石油化学などプロセス産業に特化しており、他分野をカバーする汎用的な認証制度としては認められていない。WIB を含む分野と標準化の関係を表-4 に示す。

☆5 CSSC 認証ラボラトリー, <http://www.cssc-cl.org/>  
 ☆6 Achilles Communication Certification, <https://www.ge.com/digital/applications/achilles-communications-certified-products>

	SCADA	IT
Application	DNP3 Ethernet/IP FF-HSE	FTP HTTP NTP
Presentation	MMS MODBUS/TCP	RDP RPC
Session	SES-92 OPC-UA	SNMP Telnet
Transport	TCP, UDP	
Networks	ICMP, IGMP, IP	
Data Link	LLDP, ARP, Ethernet	

■図-4 Achilles test platform の対応プロトコル

### IEC/CAB/IECEE

IEC/CAB (Conformity Assessment Board) 適合性評価評議会は、製品や組織が IEC 標準に適合するか評価方法や手順を規定し、関連する認証制度を

■表-4 産業分野と標準化状況

対象	汎用	石油化学	電力	スマートグリッド
組織	IEC 62443-2		NERC CIP	NIST IR7628
システム	IEC 62443-3	WIB	IEC 61850	
機器	IEC 62443-4		IEEE 1686	-

とりまとめる。その下部組織の電気機器製品を担当する IECCE (IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components) において、IEC 62443 に基づいた制御機器のセキュリティ認証制度の開発を進めている。

2010 年頃より、IEC/CAB の複数の組織において、さまざまな分野の制御機器セキュリティ認証スキームの議論が並列して始まった。2019 年にそれらの議論は IECCE/CMC (Certification Management Committee) の WG 31 サイバーセキュリティに一本化され、製品、システムおよび組織について IEC 62443 規格適合性評価が議論されている<sup>☆7</sup>。筆者 (山田) も、この WG に参加している。

ISA と IEC が標準化を共同で進めることになったため、ISAsecure スキームを IECCE スキームに統合する案も検討された。しかし、IEC の認証スキームとの整合や ISAsecure 認証済み製品の扱いなど調整がつかず、IEC は独自スキーム (OD-2061) を策定した<sup>☆8</sup>。IECCE 認証スキームは、国際的な認証制度の本命であり、引き続き改訂議論が進められている。

## ENISA

ENISA (European Network and Information Security Agency, 欧州ネットワーク情報セキュリティ機関) は、2004 年に設立された EU の専門機関である。名前の通り、EU 内のネットワークと情報セキュリティ問題を取り扱う。

2019 年に成立した EU サイバーセキュリティ法によると、EU 域内で活動する企業は、情報機器、関連サービスおよび開発プロセスについて認証を受け、取引においてその認証書を開示しなければならないとある<sup>☆9</sup>。ENISA は、認証書に関する欧州共通のサイバーセキュリティ認証フレームワークを提供する。このフレームワー

クは、対象製品やサービスの分類、サイバーセキュリティ技術要件、評価の種類 (自己宣言または第三者評価)、および保証レベル (3 段階) を指定している。

ただし、現時点ですべての製品・サービスの認証手順が完成しておらず、重要分野から順次整備していく計画となっている。

## その他

ドイツの TUV、米国の UL などが IEC 62443 に基づくプライベート認証を開始している。第三者認証は、供給者と調達者の双方にとって納得できる審査機関を選択することが重要である。そのため、その市場地域において実績のある審査機関が選ばれる傾向にある。

幸い、多くの有力審査機関が IECCE スキーム策定に参加しており、将来的には彼らのプライベート認証制度が IECCE スキームに合流および統合していくと予想される。

## セキュアサプライチェーン

産業制御システムのアセットオーナーあるいはインテグレータは、その制御システムをセキュアにするために、要求するセキュリティレベルに十分な制御機器や情報機器を調達しなければならない。調達者が、個々の製品のセキュリティ規格適合およびセキュリティレベルを評価するのは技術的、コスト的に困難であり、第三者認証に向けたセキュリティ認証スキームの開発が急務となっている。

ところで、アセットオーナーやインテグレータと同様の問題が、制御機器供給者にも存在する。コントローラや監視システムは、プロセッサなど多くのハードウェアとソフトウェアの部品から構成されている。それらの部品はバックドア等がなく、既知の脆弱性が塞がれたセキュアな部品でなければならない。もし、新規に脆弱性が見つかった場合は、迅速に対策 (パッチ等) が提供され、エンドユーザにまで届かなければならない。すなわち、すべての部品からエンドユーザまでの巨大なサプラ

<sup>☆7</sup> IEC/CAB/IECCE/CMC/WG 31, [https://www.iecee.org/dyn/www/f?p=106:46:0:::FSP\\_ORG\\_ID:19409](https://www.iecee.org/dyn/www/f?p=106:46:0:::FSP_ORG_ID:19409)

<sup>☆8</sup> IECCE OD-2061, [https://www.iecee.org/documents/refdocs/downloads/od-2061\\_ed.2.0.pdf](https://www.iecee.org/documents/refdocs/downloads/od-2061_ed.2.0.pdf)

<sup>☆9</sup> Regulation EU No.526/2013, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF>

## 特集 Special Feature

イチェーンにセキュリティを要求するようになった。

特に昨年から、大企業から中小企業に至るまで、サプライチェーンの弱点を狙ったサイバー攻撃が顕在化し、政府は政策として対策を進めている<sup>6)</sup>。企業は、自らの事業継続の観点だけでなく、社会的責任としてセキュリティ確保や管理を求められる。具体的には、表-5に示す「共有」「報告」「公表」の3つのアクションであり、これらにより企業のセキュリティ対策への取り組みの可視化を行う。さらに、各分野のセキュリティ対策の取り組みと連動することで、産業界全体のセキュリティ推進につなげる。

前述のNISTやENISAもセキュアなサプライチェーンに注目しており、認証制度とリスク管理を彼らのフレームワークに取り込んでいる。

## 将来に向けて

産業制御システムがセキュリティ国際標準に適合していることを客観的に示すことで、システムのセキュリティ

■表-5 サプライチェーン全体のセキュリティ確保のために求められる行動

共有 (Share)	報告 (Report)	公表 (Announcement)
① サプライチェーン共有主体間での高密度な情報共有	② 機微技術情報の流出懸念時の経産省への報告	③ 適切な場合の公表
重要なサプライチェーンを共有する企業間で、サイバー攻撃を受けて影響が及んでいる可能性がある場合には、お互いに高密度な情報共有をすることが望ましい。	軍事転用可能性のある技術情報(輸出管理対象を目的)の流出は安全保障環境に影響を与えるおそれ、流出の可能性がある場合は、経済産業省への報告が望ましい。	サイバー攻撃による被害が甚大で影響する範囲の特定が難しく、広く関係者を巻き込んでしまう可能性があり、情報共有では被害拡大の抑制を図ることが難しいと考えられる場合には、速やかにサイバー事案について公表をすることが望ましい。
中小企業を含めたサプライチェーン全体のサイバーセキュリティ対策の強化 →サイバーセキュリティ対策の取り組みを可視化		

性を証明できる。そのためには、セキュリティ標準の第三者認証を得た制御機器やソフトウェアを適用することが、市場原理としても効果的・効率的である。しかし、話は制御機器にとどまらず、制御機器が採用したプロセッサやソフトウェア等の部品まで、脆弱性対応が求められる。すなわち、部品からエンドユーザまでの巨大なセキュア・サプライチェーンが求められている。

セキュア・サプライチェーンは国内問題でなく、国際経済連携、技術共同開発、安全保障など多くの側面を持つ。難問ではあるが緊急課題であり、関係者のご協力をお願いしたい。

### 参考文献

- 1) 宮地：制御システムセキュリティの現在と展望—この1年間を振り返って—, JPCERT/CC 制御システムセキュリティカンファレンス 2020.
- 2) 神余：機能安全と制御セキュリティの標準化動向, 情報処理 Vol.58, No.11 (Nov. 2017).
- 3) SP 800-82 Rev.2 : Guide to Industrial Control Systems (ICS) Security, CSRC, NIST (May 2015).
- 4) サイバー・フィジカル・セキュリティ対策フレームワーク, 経済産業省商務情報政策局サイバーセキュリティ課, 2019年4月.
- 5) WIB Plant Security Working Group : Process Control Domain Security Requirements for Vendors, Report: M2784-X-10 ver2.0 (Oct. 2010).
- 6) 昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性について, 経済産業省商務情報政策局サイバーセキュリティ課, 令和2年6月12日.

(2020年11月3日受付)

#### ■神余浩夫 Kanamaru.Hiroo@db.mitsubishielectric.co.jp

三菱電機(株) 先端技術総合研究所 首席技師長。産業制御システムの研究開発に従事。IEC 61508 機能安全, IEC 62443 サイバーセキュリティ, IEC TR 63069 機能安全とサイバーセキュリティ両立性, IEC/CAB/IECEE/CMC/WG 32 機能安全認証の国際エキスパート。ISA 日本支部長。

#### ■山田 勉 tsutomu.yamada.bs@hitachi.com

(株)日立製作所 制御プラットフォーム統括本部 制御セキュリティ設計部所属。制御システムのセキュリティコンサルティングに従事。IEC 62443 サイバーセキュリティ規格, IEC/CAB/IECEE/CMC/WG 31 サイバーセキュリティ認証の国際エキスパート。

特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

## 5 第三者認証によるサプライチェーン・セキュリティの確保とアシュアランス


 基  
専  
応  
般


登山慎一

テュフズードジャパン (株)



Ethiraj, Sudhir Kumar Raj

TÜV SÜD Sec IT GmbH

### デジタル技術によるビジネスの変革 (デジタルトランスフォーメーション： 以下 DX) がもたらすサプライチェーン のサイバーリスク

経済活動を複数の企業がチェーンのように繋がり、製品、サービスを消費者に供給するサプライチェーンのスタイルは IT 化によって最適化、効率化へと繋がるビジネスモデルを成功させた。IT 化は、あらゆるものをデジタルに変換してビッグデータと化し、それをマーケティングに活かしていく次世代のビジネスモデルへと構造を変えてきている<sup>1)</sup>。

従来、事業の補助的な役割を担っていた IT は、事業を一体化させる基幹的な役割へと飛躍し事業のコアへと移り変わった。その結果、サプライチェーンは IT への依存を格段に高めていき IT なしではビジネスの成功は考えられないほど依存度が高まってきた。

サプライチェーンの IT 依存は、サイバーリスクという新たな経営課題に直面し、現在その対応に追われている。サイバーリスクの 1 つに、サプライチェーンが依存する IT システムにサイバー攻撃を受けるリスク、もう 1 つはサプライチェーンによって構築された IT システムの安全性である。IT システムへの

サイバー攻撃は、サイバー空間で発生したサイバーインシデントがフィジカル空間に悪影響を及ぼし、フィジカル空間で発生したサイバーインシデントがサイバー空間に悪影響が及ぼすといった空間を超えた新たなインシデントを考慮する必要がある。つまりサプライチェーンの IT 依存は、空間を超えたサイバーインシデントを自ら招き、事業の継続を危ぶませる重要リスクになり得ることを意味する。

一方でサプライチェーンが構築する IT システムそのものにもサイバーリスクを同様に考慮に入れなければならない。サプライチェーンが要求したセキュリティ基準に満たない IT 製品や IT サービスがいったん納入されてしまうと、導入当初からウイルスに感染していて情報漏洩が起きてしまうケースやサイバーインシデントから機器の破損、事業の中断に至ってしまう恐れがある。サプライチェーンは、IT システムのセキュリティ対策として適切なセキュリティ基準を明確に示した上で信頼あるサプライヤーと連携を図ることも重要である。

もしサイバーセキュリティ対策を怠って脆弱性を抱えたまま IT システムを導入し稼働してしまうと、最悪の場合は、業務の停止、知的財産および顧客の個人情報の盗難など経営やステークホルダに悪影響を招いてしまう。さらに顧客の安全を脅かす事態を

招いた場合には消費者からの信頼を失い、企業ブランドの失墜から、顧客のロイヤリティにも影響が及ぶこともあり得るなど企業は最悪の事態を想定しておかなければならない。

## サプライチェーンの安定に向けた対策

サプライチェーンが抱えるサイバーリスクの解決に向けて、サイバーセキュリティ対策のフレームワーク、標準規格、ガイドライン (ISO 27001 & 20243, IEC 62443, NIST CSF, METI CPSF など) といった国際的な標準規格を傘下のサプライヤーに準拠させていくことも1つの有効な手段である。サプライチェーン傘下のサプライヤーに国際的に広く活用されているサイバーセキュリティの標準規格を準拠させることは、サプライチェーンが抱えるサイバーリスクが低減されて、事業の安定とビジネスの拡大をもたらす効果に繋がり、さらにはDXへの参入に向けた障壁が下がるなど相乗効果が期待できる。

近年、DXに向けて急速に構造を変えてきている産業システムを抱える事業者はサプライヤーに向けてサイバーセキュリティの標準規格を準拠させていく試みが進められている。傘下のサプライチェーン間をネットワークで繋ぎ、さらに外部のインターネットに広げて新たな価値を創出するインダストリー4.0のビジネスモデルを考える上でサイバーセキュリティ対策は非常に複雑だ。

産業システムの設計、開発、構築、運用を担う組織には、システムを保有しているアセットオーナー、システムを設計、構築するインテグレータ、システムを構成するデバイスを製造するコンポーネントメーカーと大きく3つの事業者に分類される。アセットオーナーが要求するセキュリティレベルを実現するには、サプライヤー (インテグレータ・コンポーネントメーカー) のセキュリティ管理能力と産業システム・デバイスの技術的なセキュリティ能力に大きく依存してしまうため、産業システムの安定には信

頼性の高いセキュリティ標準規格を必要としている。

このような流れからサプライチェーンはセキュリティ対策として傘下のサプライヤーに、産業用オートメーションおよび制御システムのセキュリティ: IEC 62443 シリーズの適用を試みている。IEC 62443 シリーズは、サプライヤーの開発、構築、運用、保守といった事業者のセキュリティ管理・実装能力を強化する要求と産業システム・デバイスをサイバーリスクから保護していく技術的な要求で構成された産業システム向けのサイバーセキュリティ標準規格である。

サプライチェーンが保有する産業システムをサイバー攻撃から保護することを目的とする場合、セキュリティ技術の実装と確実なセキュリティ機能の実行を要求している IEC 62443-3-3, IEC 62443-4-2 に準拠した産業システム・コンポーネントを導入していくことが効果的だ。また産業システムの導入にかかわるサプライヤーの信頼性を検討していく際には、セキュリティ管理、セキュリティ技術の実装に向けたセキュリティプロセスのマネジメントを要求している IEC 62443-2-4, IEC 62443-4-1 に準拠したサプライヤーに産業システムの構築を委託させることが効果的である。

標準規格をサプライヤーおよび導入する産業システムに準拠させていくセキュリティ対策は、サイバーリスクに直面しているサプライチェーンにとってリスク低減に繋がる有効なセキュリティ対策となり得て、さらにセキュリティ対策が定着することで安定した事業継続に期待が持てる。

## サイバーセキュリティ標準規格の採用と認証制度の活用

従来、標準化の対象はH鋼やネジといった有形製品の性能や評価方法を対象としていたが、近年、サイバーセキュリティの分野にまで対象が拡大してきている。この傾向は巨大なサプライチェーンの出

現で目が行き届かなくなった産業システム、サービス、プロセスにまで消費者が不安を覚え始め、そこに信頼を求める消費者ニーズが反映された形だ。

DXの普及とIT依存によってサイバーリスクが増大しているサプライチェーンに対して、消費者はサイバーセキュリティ標準規格の採用とサイバーセキュリティ対策の確実性を求めている。たとえば、産業システムに要求されたセキュリティ機能が実装され実行されている、あるいはサプライヤーは所定のセキュリティ要件を遵守して設計、開発、構築、運用のプロセスを実行しているなどセキュリティに対するサプライチェーンの姿勢が問われている。

今後、サプライチェーンがビジネス規模を拡大していくためには、産業システム、サービス、プロセスにサイバーセキュリティ標準規格を採用させてマーケットに責任を持つことが当然のように求められる環境になるであろう。このような環境下で社会的責任の信頼を得るには、第3社認証制度のような正式なプロセスを組み入れることが多くの点で有益である。最も重要なことは産業システム、サービス、プロセスがサイバーセキュリティ標準の要件を満たしていることを証明することである。サイバーセキュリティ標準規格であるIEC 62443の認証は、サプライチェーンのサイバーセキュリティ対策を強化し、さらに信頼ある社会的責任の裏付けを持った事業者として社会システムの中に好意的に組み込まれていく制度である。

第3者認証制度は企業がマーケットに参入するための最低条件に位置付けられるなど各分野において広く活用されている。古くは貿易障壁の除去を目的として導入された制度だったが、さらに必須の要求事項として消費者の健康と安全そして環境保全を加えたことでWTO加盟国の政府調達に必須の要件として義務付けられているなど有益な制度として各方面で活用されている。このような背景から昨今グローバル市場において入札条件、システム仕様の中に確実なセキュリティ対策を証明する手段として

IEC 62443を始めとするセキュリティ認証を信頼性の保障として求めるケースが増えてきている。

## サプライヤーの信頼

サプライチェーンは新たにサプライヤーを組み入れる際、そのサプライヤーを多角的に評価しなければならない。サプライヤーの評価にはサプライチェーンのルールに沿った評価基準を採用し、自己評価、第3者評価などの評価プロセスを通じてサプライヤーの信頼性を立証していく必要がある。サプライチェーンは、新たなサプライヤーによってもたらされるさまざまなリスクを考慮にいれていくとリスク管理の負担は拡大するが、事業のリスクに直結するサイバーリスクに対しては徹底した対策を実行していくことが求められる。

サプライチェーンのサイバーセキュリティ対策を考えていく上で、すでに広く認知されベストプラクティスとして受け入れられている国際標準規格を評価基準として採用していくのもリスク低減の効果に加え相乗効果も高い。つまりサプライチェーンが傘下のサプライヤーに、標準規格の導入を徹底させるだけで全体のセキュリティリスクが低減し、さらにはリスク管理の負担が軽減されるなどステークホルダーからの信頼獲得にも結び付けることができる。

国際標準規格をベストプラクティスとしてサプライヤーの評価基準に取り入れる流れは、欧州で発足したサイバーセキュリティに関する憲章「Charter of Trust」に採用されている。

「Charter of Trust」は、サプライチェーン内のサイバーセキュリティ基盤を確保するために傘下のサプライヤーが対処すべき基本的なセキュリティ対策をIEC 62443シリーズなどに代表される国際的なサイバーセキュリティ標準規格を参照してフレームワーク（ベースライン要求事項）を策定しているので、次の章より紹介していく。

## 「Charter of Trust」 “より安全なデジタルの未来を共に”

「Charter of Trust」<sup>2)</sup>は、より安全なデジタルの未来を創造するために先進的な企業や組織がグローバルでサイバーセキュリティに取り組んでいくことを目指した共同憲章である。2018年にミュンヘンで開催したセキュリティカンファレンスにおいてシーメンスが発起人となり、現在までに19のメンバが賛同している。筆者が所属するテュフズード<sup>3)</sup>は、Charter of Trustのメンバとして積極的に参加している組織の1つだ。独立した組織として培ったノウハウを活かし、重要なシステム、機密データの保護、さらにデジタル社会における事業継続の支援に向けて貢献している。

あらゆるものがインターネットに繋がることで現代生活の多くの側面を変えたIoT化は、大きなチャンスを生み出す一方で、リスクも生み出している。チャンスとリスクが混在したデジタル社会に向けて「Charter of Trust」は、3つの重要な原則を掲げている。

1. 個人と企業のデータを保護
2. 人・企業・インフラへの被害を防止
3. ネットワーク化されたデジタル世界への信頼が根付き、成長するための信頼できる基盤を構築

サイバーセキュリティは、デジタル経済の成功に欠かせない要素である。そのためにはデジタル技術は人々や組織にとって安全で安心な信頼のおける技術でなければならない。「Charter of Trust」のメンバとともにテュフズードは、「Charter of Trust」の基本原則（図-1、10原則）に署名をして安全で信頼できるデジタル世界の実現に向けて取り組みを開始している。

「Charter of Trust」はサイバーセキュリティの先駆者として、会員企業、サプライヤーおよびデジタル社会に向けて、サイバーセキュリティのベースラインとなるセキュリティ要件を策定しセキュリティレベルの向上を目指している。

たとえば、サプライチェーン傘下のサプライヤーに対する直接的なセキュリティ要件は、基本原則の



■図-1 「Charter of Trust」の基本原則（10原則）

第2章“デジタル・サプライチェーン全体での責任”で「ベースライン要求事項」として発表している<sup>4)</sup>。具体的には、サプライチェーン全体のセキュリティ確保を目的として、サプライヤー向けにデータ保護、従業員への教育などプロセス、技術、人の要素を含めた8つのカテゴリ、17の基本的なセキュリティ要求事項をベースライン要求事項として定義している。また、この章では、ベースライン要求事項の採用に加え、その要求事項の効果的な適用を確実にするために、サプライヤーの重要性を評価する手法としてリスクベースのアプローチを推奨している。

#### < ベースライン要求事項 >

- 1- データのライフサイクル全体を通してデータを保護する。
- 2- IEC 62443 シリーズのようなベストプラクティスと整合性のあるセキュリティポリシーを実施しなければならない。
- 3- インシデント対応はタイムリーに顧客に提供されること。
- 4- サイト全体で物理的なセキュリティ対策が実施されていること。
- 5- 第三者を含めたID管理およびアクセス制御と監視を実施すること。
- 6- 基盤となるインフラを定期的にスキャンし、テストして整合性を維持する。  
事業継続と災害復旧の手順を実施し、必要に応じてサービス中断のためのセキュリティ対策を組み込むことで、可用性を維持する。
- 7- 製品、サービス、ソリューションのサポート期間を設定し、可用性を確保する。
- 8- 従業員のためのセキュリティトレーニングと訓練を定期的実施する。

サプライチェーンにとって重要度の低いサプライヤーには、自己宣言 (Self-Declaration) 自己検証 (Self-Assessment) などの実施をもってベースライ

ン要求事項への適用が求められている。一方サプライチェーンにとって重要度の高いサプライヤーには確実なセキュリティ対策を証明する証拠書類の提出 (Document proof) をもってベースライン要求事項への適用を要求している。ベースライン要求事項は、IEC 62443 や ISO 27001 などのさまざまなセキュリティ規格を参照して作られているため、それらの認証はセキュリティ対策を証明する証拠の1つになり得る。

サプライヤーがサイバーセキュリティ対策のベストプラクティスとしてベースライン要求事項を取り入れることは、セキュリティレベルの向上に繋がり、さらにステップアップしグローバルな国際標準レベルにまでセキュリティレベルを引き上げることでIEC 62443 や ISO 27001 などの認証も視野に入れることができる。

「Charter of Trust」の重要なメッセージの1つに、国際標準とベストプラクティスを調和させることにある。サイバーセキュリティに関するさまざまな国際標準がすでに存在する中で、「Charter of Trust」は、ベースライン要求事項をグローバルな国際標準にマッピングすることで、調和のプロセスを目指している。この憲章は、ビジネス、政治、テクノロジーが一体となってデジタルへの信頼を構築することを目指している。

また基本原則の第7章では、公共インフラなど社会性、重要性の高い分野には、第三者認証の積極的な採用を推奨している。第三者認証制度は、組織や顧客、ステークホルダーに信頼の価値を提供することでビジネスを活性化させることを目的としているため、サプライヤーに認証取得を促す動きはサプライチェーン・セキュリティの側面を確実に強化し、デフォルトでのセキュリティ確保に繋がると考えられている。

## 「サプライチェーン・セキュリティ」の強化に向けて

サイバーセキュリティの脅威の大半はサプライチェーンに関係しているといった見方もある中で、今回はサプライチェーン・セキュリティについて取り上げてみた。新たな試みである「Charter of Trust」では、具体的にサプライチェーンに適用可能なセキュリティのルール<sup>5)</sup>を策定し実行に向けて着実に動き始めている。この憲章の目的はセキュリティルールへの厳守よりむしろサイバーセキュリティのレベルを向上させることにあり、セキュリティ要求事項を通じた支援を提供することにある。「Charter of Trust」に参加しているグローバル企業の傘下には全体で100万社を超える規模のサプライヤーを抱えている。サプライチェーン・セキュリティの強化に向けて、「Charter of Trust」では、その規模を結集してサプライチェーン全体が抱えているサイバーリスクの不安を取り除くことを宣言している。まだ始まったばかりの新たなグローバルでのサイバーセキュリティ対策の取り組みは、デジタル社会を結束させ一丸となることで確実性がもたらされ、サプライチェーンにおけるDXの発展に繋がるものとして期待されている。

### 参考文献

- 1) 経済産業省 「通商白書 2015」第2章 第1節。
- 2) Charter of Trust : 公式 Web サイト, <https://www.charteroftrust.com>
- 3) TÜV SÜD : TÜV SÜD : Charter of Trust, <https://www.tuvsud.com/en/themes/charter-of-trust>
- 4) Charter of Trust : Common risk-based approach for the Digital Supply Chain, <https://www.charteroftrust.com/wp-content/uploads/2020/02/20-02-11-CoT-P2-phase-1-report.pdf>
- 5) Charter of Trust : Driving security in an insecure world.

(2020年10月30日受付)

#### ■ 登山慎一 Shinichi.Toyama@tuvsud.com

テュフズードジャパン(株)、COM事業部に在職中。セキュリティカンファレンスへの登壇、業界紙への執筆等を通してサイバーセキュリティ、IoTセキュリティ分野を中心にセキュリティビジネスをリード。ネットワーク機器のベンダでエンジニアを経験した後、Slerでシステムの運用管理およびセキュリティプロジェクトに従事。認証業界でIT、OTに加えクラウドを含めたセキュリティ認証のプロジェクトを担当。

#### ■ Ethiraj, Sudhir Kumar Raj Sudhir.Ethiraj@tuvsud.com

ネットワーク機器メーカーのエンジニアとしてネットワークコンサルティングに従事した後、現職では試験・検査・認証を融合させたサイバーセキュリティのベースとなるソリューション開発に取り組み、サプライチェーンへの導入に向けてグローバルで主導。



特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

## 6 米国を中心とした第三者機関によるセキュリティ評価の動向

基  
専  
般

—製品リスク評価のためのセキュリティ認証—



吉岡俊郎 | (株) UL Japan

### サプライチェーンセキュリティ

近年、製品開発時に外部委託先を含めたサプライチェーン全体でセキュリティを考慮することは、IoT時代においてますます重要となってきている。また、IoTの普及によりネットワークに接続されるデバイスが増え、それらが相互に接続される場合もある。1台のデバイスのセキュリティが破られることで、ほかのデバイスにも不正にアクセスされる恐れがある。IoTには利点も多い反面、攻撃者にとってはIoT機器がエントリーポイントともなり得るものである。

そのような中、米国では2016年2月9日、サイバーセキュリティ対策の方針としてオバマ政権(当時)より「Cybersecurity National Action Plan (CNAP)」が発表された。発表内容には外部の有識者などで構成する委員会の設置や、190億ドルの予算確保などが含まれる。

また同発表の中では、「国土安全保障省は、サイバーセキュリティ保証プログラムを開発するためにIoT製品分野における規格策定機関として、米国 Underwriter Laboratories Inc. (以下、UL) および他の業界パートナーと協力しており、冷蔵庫であれ医療用輸液ポンプであれ、“モノのインターネット”内のネットワークデバイスを試験・認定し、新製品を購入時にセキュリティ基準を満たしていることが認定されていることを確認できるようにする」

とも述べられている<sup>☆1</sup>。

### UL CAP と UL 2900 規格

このような背景で開発されたセキュリティ認証制度がUL CAP (Cybersecurity Assurance Program) であり、UL および連邦政府・学会・産業界を代表する関係者により開発された。ULは、1894年に米国で設立された安全認証機関で、家電製品・自動車・産業機器・電子部品・エネルギー関連機器等の分野でサービスを展開し、2020年11月現在では143カ国以上に拠点を構えている。また、ULは安全規格策定機関として規格作成能力を保有し、これまでに約1,600のUL規格が策定され、うち50%以上がANSI規格(米国国家規格)として採用されている。

UL CAPは、IoTのサプライチェーンにおけるコネクテッド製品を試験・認証するための制度であり、コネクテッド製品のセキュリティに関するベストプラクティス等を規定した「UL 2900」規格群を基に実施される。本制度には、網羅的に脆弱性を検査する「脆弱性診断」、攻撃者の観点から攻撃が成功するかどうかを確認する「ペネトレーション試験」、さまざまな入力を行うことで脆弱性を検査する「ファジング試験」、ソースコードや実行コードを実行せずに構文や処理フローなどの解析を行う

☆1 <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>

## 特集

## Special Feature

「静的コード解析・バイナリ解析」といった製品に対する試験に加え、「開発プロセス」「リリース後のパッチ管理プロセス」の確認といったソフトウェアの設計開発や運用体制に対する評価も含まれる。これらの検証をクリアした製品には1年間有効の認定書が発行される。認定書には評価実施時に参照されたNIST脆弱性データベース<sup>☆2</sup>の日付も記載されるため、どの時点での脆弱性の情報を基に上記の検査が行われたかが分かるようになっている。

UL 2900規格はソフトウェアのセキュリティに一般的に求められる事項（一般要求事項）を含むPart1、および特定分野の製品要求事項を含むPart2で成り立っている。このうちUL 2900-1（一般要求事項）、UL 2900-2-1（ヘルスケアシステム）、UL 2900-2-3（セキュリティ・ライフセーフティシグナリングシステム）は米国国家規格協会（ANSI）およびカナダ標準審議会（SCC）により承認されている。またUL 2900-2-1は米国食品医薬品局（FDA）により Recognized Consensus Standard に認定されている。これにより、ネットワーク接続型の医療機

器を製造・開発し、米国FDAへの申請を行う際には、同規格を参照することができる。

## UL 2900 要求事項

例としてUL 2900-1規格の要求事項を取り上げる。序文において、本規格の趣旨として3点が述べられている。

- 製品に対するソフトウェア開発者（ベンダもしくはその他サプライチェーン）のリスクマネジメントプロセス要求事項。表-1の「リスクマネジメント」のカテゴリがこれに相当する。
- 脆弱性・ソフトウェアの弱点・マルウェアの存在に対する製品評価・試験方法。表-1の「脆弱性・エクスプロイト」と「ソフトウェア脆弱性」のカテゴリがこれに相当する。
- 製品アーキテクチャ・設計におけるセキュリティリスクコントロールに関する要求事項。表-1の「リスクコントロール」、「製品および使用に関するドキュメンテーション」のカテゴリがこれに相当する。

さらに、医療分野を対象とする規格であるUL

☆2 <https://nvd.nist.gov/>



■図-1 UL2900-1:2020規格

■表-1 UL 2900-2-1規格 主要要求事項

カテゴリ	項目
製品および使用に関するドキュメンテーション	製品設計ドキュメンテーション
	製品使用時ドキュメンテーション
リスクコントロール	リスクコントロール
	アクセスコントロール・ユーザ認証
	リモート通信プロトコル
	機密情報 製品マネジメント
リスクマネジメント	ベンダ製品リスクマネジメントプロセス
脆弱性・エクスプロイト	公知脆弱性試験
	マルウェア試験
	不正入力試験（ファジング）
	ペネトレーションテスト
ソフトウェア脆弱性	ソフトウェアの弱点の分析
	静的ソースコード解析
	静的バイナリー・バイトコード解析

## 特集 Special Feature

2900-2-1（ヘルスケアシステム）においては、組織観点でのセキュリティ要求事項として「品質マネジメントシステム」「購買プロセス・購買におけるリスクマネジメントプロセス」「製品アップデートリリース・パッチマネジメントプロセス」「廃棄プロセス」に関する内容が盛り込まれている。

このように、IoT 製品に関するセキュリティ試験やソースコード・設計文書・リスクマネジメントプロセス等を含めたレビューを第三者の立場で行うことで、製品が適切に設計され、かつその設計が正しく実装されているかどうかを確認することができる。

### 第三者評価により得られるメリット

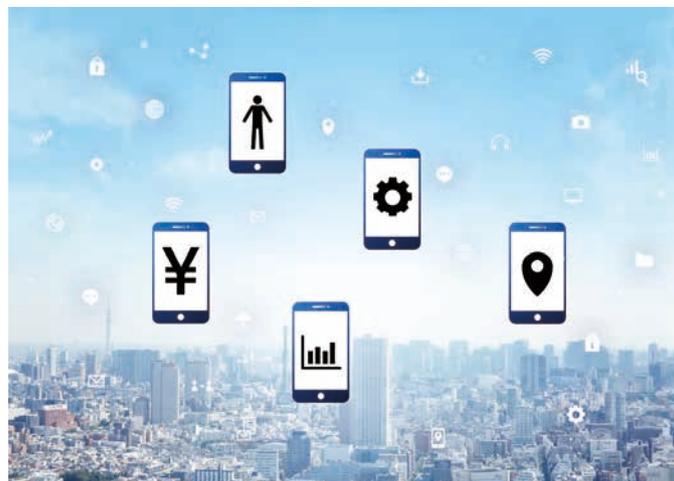
このような第三者機関によるセキュリティ評価を

実施し認証を取得することで、製品のセキュリティレベルに対する客観的な評価を得ることができる。これは市場における製品展開上の差別化要因となり得る。また、製品内の一部コンポーネントに対する評価ではなく機器全体に対する評価を行うこととなるため、包括的なセキュリティ評価が可能となっている。

(2020年11月4日受付)

■吉岡俊郎 toshiro.yoshioka@ul.com

法政大学卒業。システムエンジニア・プロジェクト管理業務を約10年経験後、Gemalto（現・タレス DIS）などを経て2020年よりUL Japanにてプログラママネージャとしてサイバーセキュリティ業務に携わる。



特集

Special Feature

[DX (デジタル・トランスフォーメーション) 時代のサプライチェーン・セキュリティ]

# 7 ソフトウェア部品表 (SBOM) に 基づくリスク管理

基  
専  
応  
般

— オープンソース・ソフトウェア (OSS) および  
商用ソフトウェアのリスク管理のための SBOM —



松岡正人 | 日本シノプシス合同会社

## ソフトウェアのリスク管理のための SBOM

米国 NTIA の Allan Friedman 博士は、2019 年の Black Hat で「Transparency in Software Supply Chain : Making SBOM a reality」と題する講演を行い「工業製品は保守のために BOM が用意されているのに、なぜソフトウェアにはこれがないのか?」と述べた。

### ■表-1 SBOM 情報の例

※各項目のうち、推移や一覧、ほかのソースへのリンクについては参考例として弊社製品の画面およびリンク先の情報を貼り込んでいる。

項目	情報												
URL	<a href="https://github.com/apache/tomcat">https://github.com/apache/tomcat</a>												
ライセンス	Apache License 2.0 <a href="http://www.apache.org/licenses/LICENSE-2.0">http://www.apache.org/licenses/LICENSE-2.0</a>												
脆弱性情報 (CVE)	CVE-2019-0221, CVE-2019-0232, CVE-2019-10072, CVE-2019-17569, CVE-2020-1935, CVE-2020-1938, CVE-2020-9484, CVE-2020-11996, CVE-2020-13935, CVE-2020-13934 ※各項目をクリックすることでMITREなどのCVEのソースを参照可能であることが望ましい												
バージョン	3.3.x (archived), 4.1.x (archived), 5.5.x (archived), 6.0.x (archived), 7.0.x, 8.0.x (superseded), 9.0.x, 10.0.x ※各バージョンをクリックすることで、詳細なバージョンの履歴と、関連する実行環境などの技術情報などが参照できることが望ましい												
最終更新日	2020/10/16												
コミット数の推移													
発見されたバグの推移													
開発者数の推移													
依存関係	<table border="1"> <thead> <tr> <th>依存関係</th> <th>バージョン</th> <th>ライセンス</th> <th>フェーズ</th> </tr> </thead> <tbody> <tr> <td>WebGat/WebGat</td> <td>6.0</td> <td>なし</td> <td>開発中</td> </tr> <tr> <td>WebGat/WebGat</td> <td>v8.0.0.M21</td> <td>なし</td> <td>開発中</td> </tr> </tbody> </table>	依存関係	バージョン	ライセンス	フェーズ	WebGat/WebGat	6.0	なし	開発中	WebGat/WebGat	v8.0.0.M21	なし	開発中
依存関係	バージョン	ライセンス	フェーズ										
WebGat/WebGat	6.0	なし	開発中										
WebGat/WebGat	v8.0.0.M21	なし	開発中										
従属関係	<table border="1"> <thead> <tr> <th>使用した脆弱性情報</th> <th>バージョン</th> <th>ライセンス</th> <th>フェーズ</th> </tr> </thead> <tbody> <tr> <td>WebGat/WebGat</td> <td>6.0</td> <td>なし</td> <td>開発中</td> </tr> <tr> <td>WebGat/WebGat</td> <td>v8.0.0.M21</td> <td>なし</td> <td>開発中</td> </tr> </tbody> </table>	使用した脆弱性情報	バージョン	ライセンス	フェーズ	WebGat/WebGat	6.0	なし	開発中	WebGat/WebGat	v8.0.0.M21	なし	開発中
使用した脆弱性情報	バージョン	ライセンス	フェーズ										
WebGat/WebGat	6.0	なし	開発中										
WebGat/WebGat	v8.0.0.M21	なし	開発中										

ソフトウェア部品表 (SBOM) は、ソフトウェアの構築に使用されるさまざまなコンポーネントの詳細とサプライチェーンの関係を記載したモノである。再帰的に利用されたソフトウェアコンポーネントを構成する成分のリストで構成され、ソフトウェアコンポーネント、それらのコンポーネントに関する情報、およびそれらの間の関係を識別して一覧表示したものである (表-1)。

本稿では SBOM を用いたリスク管理方法について概論し、個別の課題について併記する。

## どのようなリスクを管理するか

ソフトウェア開発では、自ら書いたものと第三者が書いたものとの 2 種類のソフトウェアを組み合わせることが一般的である。これらのプログラム・コードには、バグやセキュリティ上の問題となる「脆弱性」と呼ばれるものも含まれる可能性がある。CVE (Common Vulnerabilities and Exposures) は、米国政府の支援を受けた非営利団体 MITRE 社が個別製品中の脆弱性を対象として採番している識別子である。日本では JPCERT/CC<sup>☆1</sup> や IPA<sup>☆2</sup> が研究者などが発見した脆弱性をソフトウェアや製品の製造元とともに脆弱性の特定と修正を行い、CVE として公開している。CVE を付与することにより、ある組織が発行する脆弱性対策情報と、ほかの組織が発行する脆弱性対策情報が同じ脆弱性に関する情報であるかを判断するのに活用できる。また情報同士の相互参照や関連付けに利用できる。

オープンソース・ソフトウェア (以下 OSS) の数は増

☆1 <https://www.jpcert.or.jp/>

☆2 <https://www.ipa.go.jp/>

## 特集 Special Feature

え続けており、一方でコミュニティが活動しなくなることで開発が放棄されるものも増えつつある。OSSの脆弱性に伴うリスクをどのように管理するかが大きな課題となってきた。2020年オープンソース・セキュリティ&リスク分析(OSSRA)レポート<sup>☆3</sup>では、調査した1,253本の商用ソフトウェアの99%にOSSが含まれ、コード全体の70%を占めていたと報告されており、OSSの脆弱性は商用ソフトウェアの脆弱性に大きな影響を与えている点で「リスク因子」である。

別のリスク因子は「OSSのライセンス」である。ライセンス違反の事例についてはここでは詳細に述べないが、いくつかの事例がIPA(独)情報処理推進機構のサイトなどで参照できる。

### SBOM 管理の実際

SBOM管理のための標準化や関連する情報をコンポーネントに埋め込むための手法が開発されても、管理自体を手作業で行うのでは効率が悪すぎる。現実的にはSCA(Software Composition Analysis:ソフトウェア・コンポジション解析)ツールを利用する必要があり、SCAツールは商用で提供されている。

SCAツールは、公開されている脆弱性情報やライセンス情報だけでなく、さまざまな調査データも含めてデータベースに格納してある。管理対象となるソースコードやバイナリーを専用のツールを使って解析し、内包されているソフトウェアコンポーネントをデータベースと照合することで峻別することができる。特定できたコンポーネントには、その由来やサプライチェーン上のリスクとなり得る情報を紐づけることができる。

しかし、多くの場合問題となるのは「Snippet(スニペット)」と呼ばれる、コードの一部だけをコピーする場合である。スニペットによって起こり得るリスクとは「ライセンス違反」が主であり、訴訟の対象となることで製品の販売差し止めや損害賠償に至る場合もある。しかし、それらのコードの断片がどのコンポーネント由来の

ものであるのかを突き止めるために100%合致する解析結果を得ることは非常に困難であることから、いわゆる「誤検知」が発生する可能性がある。これを回避するにはソースコード管理を厳密に行い、由来の不明なスニペットを排除する必要がある。

バイナリーで流通するコンポーネントの扱いは技術的な難易度が非常に高いため、現時点で利用可能なツールはほとんど存在していない。Black Duck Binary-Analysis<sup>☆4</sup>、Clarity<sup>☆5</sup>、CodeSentry<sup>☆6</sup>などがあるが、URGENT/11<sup>☆7</sup>などの組込み機器の開発で問題となる脆弱性を検知することができるツールは限定されるため、用途によっては期待する分析結果を得られないこともある。

仮想化によって高可用性や高いスケーラビリティを実現しているクラウド環境では、アプリケーションと実行環境をコンテナ化することで高度で柔軟な運用を可能にしている。このコンテナイメージもバイナリーであり、開発と運用とを一体で管理するDevOpsを実現する重要な技術として利用が拡大しているが、コンテナそのものもイメージごと解析する必要が出てきており、いくつかのSCAツールで解析できる。

このように、開発と運用、言語と実行環境、システムの構成と利用されているコンポーネント、これらの組み合わせにより、開発プロセスの各フェーズでSBOMの情報を解析し必要に応じて脆弱性の修正や、緩和策の導入などを行う体制が必要なのは言うまでもない。

(2020年10月22日受付)

☆4 <https://www.synopsys.com/ja-jp/software-integrity/security-testing/software-composition-analysis.html>

☆5 <https://www.insignary.com/>

☆6 <https://www.grammatech.com/codesentry-sca>

☆7 <https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce>

■松岡正人 masato.maysuoka@synopsys.com

長岡工業高等学校電気科卒業。組込み含むソフトウェア開発を10年余り経験後、日本ラショナルソフトウェア、日本マイクロソフト、カスペルスキーなどを経て2019年より日本シノプシス JNSA IoT Security WG リーダー、ASTER 理事。

☆3 <https://www.synopsys.com/blogs/software-security/ja-jp/2020-ossra-findings-infographic/>

## 【ご案内】会誌「情報処理」のオンライン記事について

会誌「情報処理」の特集記事は、これまで冊子、オンライン（電子図書館）の両方に掲載しておりましたが、次のとおり オンラインのみへの掲載 に変わりました。また、オンライン限定記事の掲載も始まりました。

◆開始月：2020年11月号（発行日：2020年10月15日）

◆閲覧方法：会員区分によって異なりますので以下をご確認ください。

### 【個人会員の皆様】

電子図書館（情報学広場：<https://ipsj.ixsq.nii.ac.jp/ej/>）にログインし、該当記事のpdfをダウンロードしてください。すでに電子図書館をご利用いただいている方は今までどおりです。

電子図書館を初めて利用される方は、会員としてのユーザ登録が必要になります。

未登録の方には毎月上旬に次の件名のメールを送信しておりますので、到着次第、登録してください。

- 件名：[情報学広場:情報処理学会電子図書館] ユーザー登録のご案内
- 差出：ipsj-ixsq@nii.ac.jp

【個人会員】



電子図書館  
(情報学広場)

★詳細：電子図書館利用方法（個人用）－利用までの流れ（<https://www.ipsj.or.jp/e-library/ixsq.html#anc2>）

ご案内メールをお急ぎの方や閲覧方法が分からない方は、会員サービス部門（E-mail: [mem@ipsj.or.jp](mailto:mem@ipsj.or.jp)）に会員番号を添えてご連絡ください。

### 【賛助会員各位・購読員の皆様】

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

#### <手順>

- (1) 「情報処理」の特集ページ（扉または概要ページ）を開く。
- (2) 閲覧申込のURLにアクセスする（またはQRコードを読み取る）。
- (3) 必須事項を入力し送信する。
- (4) 次の件名（3月号の場合）の受信メールに従って、電子図書館から特集のpdfをダウンロードする。
  - 件名：情報処理 2021年3月号（Vol.62, No.3）「チケットコード」とご利用方法のご連絡

#### ★注意事項

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

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



# プログラミング的思考が わからない



遠藤 諭 | (株) 角川アスキー総合研究所

## いまの小学校低学年は めちゃめちゃプログラムが書ける

「第5回 全国小中学生プログラミング大会」<sup>☆1</sup>という2016年に始めたプログラミングコンテストに寄せられた作品の一時審査に追われている。320件以上の応募があり一作品ずつ子どもたちが作った作品のねらいやアピールポイントなどの説明を読み、実際にソフトを起動して確認していく作業。唯一の救いは、応募プログラムの約半数がScratch単体なので、URLをクリックすれば、そのまま動かすことができることだ。

この作業をしていていちばん強く感じるのは、小学校低学年でも《IF》(もし～なら)や《WHILE》(～まで繰り返す)を組み合わせたコードを書きあげていることである。「小学1年生など大人が手伝って応募しているんでしょう?」と思われるかもしれないが、我々のコンテストでは、子どもたちがメーカーフェアよろしく屋台をかまえ審査員がぐるぐると回ってきて十分なやりとりをする。その上での審査なので、彼らがどんなふうに自分で考えどんなふうに作ったのかがわかる。しかも、そのようすがなかなか楽しい。

2019年度、小学2年生でグランプリを獲得した小長井聡介君の作品は、世界的にも有名な渋谷ハチ

公前のスクランブル交差点のシミュレーターだった。実際に、現地に出向いて観察してみたというところまででも、夏休みの自由研究として十分な内容である。それを一歩進めて交通量や人の数を変更できるシミュレーションは、まさにプログラミングならではの醍醐味。いままでの理科、社会などの科目で学べることと、プログラミングがどう繋がってくるのか大人が教えられるような内容である。

子どものクリエイティビティを過小評価してはいけないと思う。まさに、換骨奪胎というべきか——そんな言葉は子どもは知らないはずだが、過去、私が、子どものクリエイティビティでいちばん感動したのは、Discovery Channelで流れた子どもの作った四角いタイヤの車である(小学生か中学生か名前など詳細も記録しておらず)。四角いタイヤの車という大人なら「はいはいカテナリー曲線(懸垂線)をひっくり返したカマボコの連続みたいな地面を走るんでしょ」と言うかもしれない(東京理科大学の数学体験館にある)。ところが、その子の作った車は4つの四角いタイヤの回転角度がズレた状態で装着されている。シャーシの中央にはマブチモーターが1個上向きに固定されていて投げ縄みたいに水平にブルブルと重りを回している。これで、車体全体をガタンガタンと揺らしながら前に進むのだった。そのカッコよさったらなかった。ほぼ、レオナルド・ダビンチかアルキメデスといってもよい。

こんな感じの大人はなかなか考えないようなクリ

☆1 <http://jjpc.jp/>

エイティビティを感じさせる工夫は、我々のコンテストでも見かけるし、それを評価して褒めてあげることでさらに伸びるのだと思う。

しかし、私がひとりひとりの子どもたちに「偉いねー」と声をかけたくなくなってしまうのは、その点だけではない。彼らがScratchなどよくできたプログラミング言語を使ってではあるにしろ、ちゃんと動くプログラムを完成させるところまでやりとげていることだ。というのは、自分がプログラマーとして仕事をしてきた時代のことを思い返すと、あのいまわしい《IF》や《WHILE》によって生み出される混沌がいまもよみがえってくるのである。

## FORTTRAN でデバッグがいらなくなる!

『Coders (コーダーズ) 凄腕ソフトウェア開発者が新しい世界をビルドする』(Clive Thompson 著, 井口耕二訳, 日経BP)によると、世界最初に稼働したプログラム内蔵式コンピュータ EDSAC の開発者 Maurice Vincent Wilkes は、1949年6月のある日、階段を上りかけた瞬間、心の中をよぎるものがあった。それは「これからの人生、自分が書いたプログラムの《間違い探し》に大半の時間を費やすことになりそうだ」というものだった(EDSAC が稼働したのが1949年5月なのでその翌月でしょうか)。嫌な予感というのは当たるもので、それから70年が経過したいまも世界中のプログラマーがデバッグという作業に日夜膨大なエネルギーを費やしている。

2012年の情報処理学会 第74回全国大会(会場: 名古屋工業大学)に、私は「Busicom 141-PF」(Intel 4004を生むことになる電卓)が情報処理技術遺産に選ばれたというので出かけたのだが、筑波大学名誉教授の中田育男先生の講演「コンパイラの最適化を追求して」が印象深い。1954年、IBMが同年発表した「同704」のときに作ったFORTRANは「これでもうデバッグはいらなくなる」というコンセプト

だったというのだ。704のコンパイラは「いま見てもここまで最適化に注力したコンパイラはないといわれる」ほどの物凄く気合の入った製品だったというにもかかわらず、デバッグしなくてよくなるという夢のようなコンセプトは昼気楼だったのだ(余談として紹介されたと思う「HITACの2050には、Modify Next Instructionという便利な命令があった」というお話も今回のこの原稿と深く関係するかもしれないのだが)。

『実録! 天才プログラマー』(マイクロソフトプレス編, 岡和夫訳, アスキー)のなかでは、米マイクロソフトのBill Gates CEOが「ここ5年のうちに、人間のプログラマーと同等の仕事ができるツールが現れると思います」と述べている。この本が出版された1986年頃は、「第四代言語」や「人工知能」が、我々プログラマーをデバッグの沼から救い出してくれるといういま思えばある種の祈りに似た思いが業界にはあった。『ソフトウェア開発の神話』<sup>☆2</sup>という大規模プロジェクトの困難さを述べた古い本が、プログラマーたちの手から手へと伝えられるような形で読まれていた。第四代言語というのは、プログラマーが自分でロジックを組み立てなくてよい非手続き型言語を指すことが多い。人工知能に関していえば、私のいた会社では論理プログラミング言語「Prolog」の研修があった。COBOLのエラーメッセージを読み込んで適切なデバッグの指針を示すエキスパートシステムを提供しようとしていたのだ。欧州の某研究所から導入したものだったが、製品として発売されることはなかったと思う(ネットで調べるとその元になった論文などが見つかったりするのだが)。

<sup>☆2</sup> 『ソフトウェア開発の神話』(“The Mythical Man-Month: Essays on Software Engineering”, Frederick Phillips Brooks, Jr. 著, 山内正弥訳, 企画センター, 1982)。IBM S/360とそのオペレーティングシステムの開発者がソフトウェア開発における諸現象を述べたもので原著は1975年。

## 論理的にアルゴリズムを考えるのをやめよう

プログラミングで仕事をしていくときに大切なのは論理的な思考であるなどといわれる。子どもがプログラミングを学ぶことで論理的な思考がやしなわれるなどとも言われる。ところが、完全に論理的にきっちりとやれない生き物だから我々は人間なのである。ここにプログラミングというものの宿命的な矛盾がある。

それでも多くのプログラマたちがこれまでやれてきたのは、たとえば、頭で考えずにリングノートに書きだして、それを眺めてできるだけフラットで分かりやすいコードに落としてきたからだ。むしろ、頭の中で動かしてみるというのは四角いタイヤの車を走らせるような抜群なアイデアを思い浮かべる瞬間であるべきなのだ。それも、たぶん私のプログラマ時代の同僚たちと同じように鉛筆でスケッチを描き、うまくいかないときは破り捨て（だからリングノートなのだ）、あるいは手を動かして簡単な実験を積み重ねて作り上げていったはずである。プログラミングに関しては、むしろ論理的に思考することを避けることで、ソフトウェアの世界は回ってきたようなところがある。

NHK for School の番組『テキシコー』は、地上波の E テレでも放送されたのでご覧になった方も多いと思う。いまでも公式サイトで 2020 年に放送されたすべての番組を見ることができる<sup>☆3</sup>。「コンピュータを使わずにプログラミング的思考を育む」とうたわれていて、「分解、組み合わせ、一般化、抽象化、シミュレーション、プログラミング的思考を獲得せよ!」と、軽快なリズムのテーマ曲とともにナレーションが入る。

『テキシコー』では、オープニングでいきなり紙生物（かみせいぶつ）「ゲソタラズ」がテーブルの

上を歩くところが見る人たちを引き付ける。仕掛けは、中国の屋台で平たい水槽の中の金魚に金属片を呑み込ませておいて下から磁石で操るのと同じようなものである。ただし、パッと見には複雑そうに見えるゲソタラズ（足の数が 6 本しかないなのでこの名前なのではないでしょうか？）の歩き方が楽しい。ハエと同じ交互三脚歩行をするだけなのだが、もったいぶった動きで人間の視覚統合力が試される感覚が、実はとてもプログラミング的だといえる。

もう 1 つ、これは # 1 のいちばん最後にビデオ取材的に出てくる郵便局のお話。郵便局では毎朝《組み立て》という作業を行う。この組み立てで使うのが《配達原簿》というリストで、それによって配達員はひと筆書き的に一方通行や右折禁止を配慮して郵便物を配達できるのだそうだ。いうまでもなく、しかもその制限の中では最短ルート的なものになっているのだろう。まさに巡回セールスマン問題の現実版みたいな感じのことをやっている。プログラマなら「おぉーっ、そうでしょうそうでしょう」と声を上げた人も多いはず。

しかし、# 1 の前半にでてくるプラレールを使ったやつがなんとも《IF》と《WHILE》の匂いのするものだ。公式サイトの「実際（じっさい）に電車を走らせると…?」と題した動画を見ると、頭の上から煙を吐いて「計算できません」<sup>☆4</sup>と言いたくになってしまう内容である。サイトの動画を見てただくのがよいのだが、円形のプラレールの上を電車が走っていくと遮断機にぶつかって止まる。実は、レールのほうがグルグルと回る仕掛けになっていてその端に固定された三角形も一緒に回ってきて遮断機を持ち上げ、電車はそれをくぐってまた走りだす。以下繰り返す……。かなりビックリする動きだ。

パズルのように自分で考えて意外な答えが出るの

<sup>☆3</sup> <https://www.nhk.or.jp/school/sougou/texico/>

<sup>☆4</sup> 1960 年代のテレビドラマ『宇宙家族ロビンソン』に出てくるロボットのフライデー（正しくは B9 モデル・マーク 3 型気圧観測ロボット）がよく発したセリフ。実際には煙をあげることはなく矛盾した問題でショートしたのは『禁断の惑星』のロビーである。

は楽しい。トグルスイッチみたいなしくみを学ぶのも大変によい。『キートンの船長』など無声映画の説得力みたいな力強さもあるのだが、それだけにまじめに頭の中で考えてついていくのがつらくなりそうになる。

プログラミングで楽しいのは（というよりもうまくいくときというのは）、ゲソタラズの足と磁石とか、配達原簿を作ったところで、ほとんど90パーセント決まる。誰が見てもすぐにわかる。それに対して、プログラミングで苦しいのは（つまりうまくいかないバグがでるときというのは）、アルゴリズム的な仕掛けを考えてやろうとしたときなのだ。それは、かなりシンプルなものでもナゾの呪文のようになりがちだ。

だから論理的にアルゴリズムでやることをできるだけやめるべきと思っていたら、1カ月ほど前に「なるほどそうか！」と言いたくなることがあった。仕事で、競技プログラミングのAtCoderに参加している東大生と筑駒1年生にインタビューしたときのこと。競技プログラミングというのは、ご存じのとおり与えられた問題を解くプログラムを制限時間内

にいくつ正しく書くかという文字どおりの競技である。彼らは、問題を見たときに自分の頭に入っているアルゴリズムを応用できるかどうか《宝さがし》のような感じだというのだ。プログラミングの競技だから自分で問題を解くロジックをウンウンと考えだすのだと思ったら、そうではなくて、もっと直観的でスピード感のあるデザインに近い作業のようにも聞こえた。そもそも、プログラミングの問題を解く過程というのは、そうした作業のあとに具体的なコードとして書き下していくこととの2段階からなっている。プログラムに落とす部分は文法的に正しく書いていくだけですよねということだった。

よく考えれば、その場でオリジナルのアルゴリズムを考えても時間はかかるし間違いが起こる可能性も高くなる。十分に枯れていてパフォーマンス等の評価も数学的にされているアルゴリズムが、与えられた問題にどうフィットするか？という戦略のほう有利なのは間違いない。そんなの楽しくないしそればかりだったら新しいアルゴリズムは生まれないという意見もあるだろう。しかし、これは仕事でプログラミングをやる場合にもあてはまるし、ということはこれからプログラミングをはじめの人にもいえることになる。学ぶべきは柱の立て方ではなくて、建築物で使われてきたさまざまな構造の種別をきっちりやることなのではないかと思える。

ゲソタラズ、配達原簿に加えて、純粹培養競技プログラマーとも言われたりする彼らの話を聞いていたら、私のプログラミング的思考に対する気分は少しラクになった。

(2020年12月10日受付)



図-1 本文にも古い話がいくつも出てくるが、紙テープ鑽孔機をネットオークションで落札してパソコンにつないで遊んでいる。『アーケードゲーム・タイポグラフィ ビットマップ書体の世界』（大曲都市著、グラフィック社）に掲載されたSpace InvadersやXEVIIOUSやVirtureRacingやらのフォントで花文字出力するプログラムを書いて打ち出している。漢字は恵梨沙フォント。鑽孔機はアマダのNPR-8000、紙テープはコクヨや紀州製紙や巴川製紙所だが巴川を最後に生産終了しているらしい。

■遠藤 諭 s-endoh@lab-kadokawa.com

(株)角川アスキー総合研究所 主席研究員。プログラマーを経て1985年アスキー入社、1991年より月刊アスキー編集長、2013年より現職。『マーフィーの法則』、『超』整理手帳などを企画。著書に『計算機屋かく戦えり』、『近代プログラマの夕』、『ゼネラルパーパス・テクノロジー』（野口悠紀雄との共著）など。『AI白書2020』アドバイザー。

# 情報処理学会トランザクションデジタルプラクティス 特集号論文募集

## 「DXのプラクティス ～ニューノーマル時代を生き延びる～」

● ● ▶ [投稿締切] 2021年3月10日(水) 17:00 ◀ ● ●

経済産業省がとりまとめた「デジタル経営改革のための評価指標（「DX推進指標」）」（2019年7月）では、DX（デジタルトランスフォーメーション）を次のように定義しています。

“企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること”  
DX推進指標は、企業が自社の状況を自己判定できる仕組みを提供し、東京証券取引所と連携した、「DX銘柄」を発表するなどにより、DXの推進を図っています。また、国がDX推進状況を審査し認定する、「DX認定制度」の申請受付が、2020年11月に始まっています。

2018年の経済産業省の「DXレポート～ITシステム「2025年の崖」克服とDXの本格的な展開～」では、タイトルにあるように2025年を1つの目標として企業等に変革を促しています。

2020年のCOVID-19により余儀なくされたワークスタイル変容などにより、DXのニーズは加速され、その変化は後戻りできないものとなっています。

このような状況の下、情報処理学会の学会誌2020年11月号では、「DX（デジタルトランスフォーメーション）特集として、DXの定義、我が国の現状、技術、教育、人材育成、企業における実践、デジタルプラットフォームに関する12本の論文が掲載され、DXに関する包括的な情報共有を行いました。

論文誌トランザクションデジタルプラクティスの本特集では、更に踏み込んでデータとデジタル技術を活用し、業務効率の向上、顧客提供価値の向上、ニューノーマル時代のワークスタイル変革に取り組んだ実践事例・実証実験、及びDX実現に活用できる技術の実践事例などから得られた知見（プラクティス）を含む論文を募集します。プラクティスの例としては、下記に挙げるようなものを想定していますが、これに限定されるものではありません。

- ・DX実現において活用した技術及び技術の利用方法
  - ・データ収集、データ活用、特に組織をまたがるデータ活用の工夫点
  - ・DXを促進する技術：製品・ソリューションの開発手法
  - ・DX推進のための人材育成、組織改革の実践
- 皆様の、積極的な論文投稿をお待ちしています。

※投稿要領：Web サイトをご覧ください→ <https://www.ipsj.or.jp/dp/submit/tdp0201s.html>（応募資格は問いません）

※掲載号：2021年10月号（Vol.2 No.1）

※特集エディタ：境 真良（IPA 社会基盤センターDX推進部長）

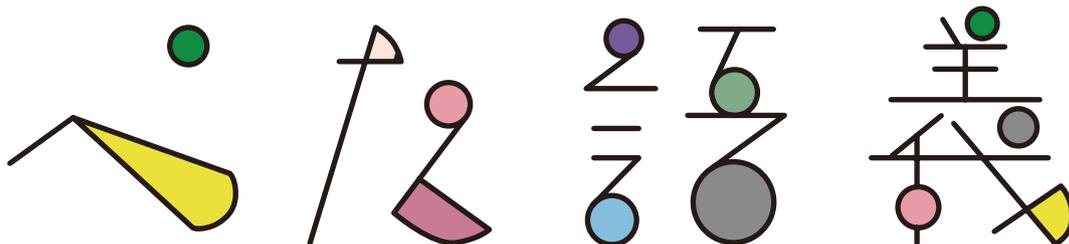
※特集号編集委員：編集委員長：吉野松樹（日立）

副編集委員長：細野 繁（東京工科大学）

編集委員：青木学聡（京都大学）、荒木拓也（日本電気）、西山博泰（日立製作所）、鎌田真由美（日本マイクロソフト）、飯村結香子（NTT）、石井一夫（久留米大学）、今原修一郎（東芝）、江谷典子（Peach・Aviation）、大嶋嘉人（NTT）、鬼塚 真（大阪大学）、上條浩一（日本IBM）、斎藤彰宏（日本IBM）、坂下 秀（アクタスソフトウェア）、佐藤 聡（筑波大学）、佐藤裕一（富士通研究所）、澤谷由里子（東京工科大学）、澤邊知子（日本大学）、立床雅司（三菱電機）、新田 清（ヤフー）、浜 直史（日立製作所）、濱崎雅弘（産業技術総合研究所）、平井千秋（日立製作所）、藤瀬哲朗（三菱総研）、藤原一毅（国立情報学研究所）、横井直明（日立製作所）

アドバイザー：喜連川優（国立情報学研究所・東京大学）

（論文募集公開時点（2020年12月））



Vol.114

## CONTENTS

【コラム】ハイフレックス授業…渡辺 博芳  
【解説】第13回全国高等学校情報教育研究会全国大会（オンライン大会）…小原 格



## COLUMN ハイフレックス授業



コロナ禍の影響で2020年度はほとんどの大学でオンライン授業が行われた。オンライン会議システムを活用した同期型の授業、講義ビデオや資料を配信する形の非同期型の授業など、オンライン授業の実施形態はさまざまであった。そのような中で「ハイフレックス授業」が注目されている。

ハイフレックス授業は、各回の授業に対面で教室に参加するか、同期型オンラインで参加するか、または非同期型オンラインで参加するかを学生が選択できる授業である。オンラインと対面のハイブリッドで、授業への参加形態がフレキシブルなことから、ハイフレックスと呼ばれている。単に利便性の向上と言うことだけではなく、各回の授業にどのモードで参加するのが自分の学びにとってベストかを、学生が主体的に判断して授業に参加するという側面もあるようだ。

帝京大学宇都宮キャンパスでは、4月からオンライン授業を開講し、緊急事態解除後の6月からは一部で対面授業も開始した。そこで、このタイミングで、私が担当していた情報リテラシーの授業ではオンラインに加えて教室への出席も認めることとした。この授業は教材の掲載や小テスト、課題提出などで従来からLMS（学習管理システム）を活用していたので、LMSのオンライン会議機能を使うことで同期型のオンライン授業を比較的容易に実施できた。オンライン授業では、学生側のネットワーク環境も考慮して、授業中の説明はすべて収録して後から視聴できるようにし、LMSの掲示板やメールで質疑応答も受け付けていたので、非同期型での学習も可能であった。6月からはそこに対面参加の選択肢も加わり、ハイフレックス授業となった。

この授業は92名の履修者に対して教員2名が担当し、教室へは10名～18名程度が参加した。学生にも好評で、アンケートに「対面授業とオンライン授業とが選択できる点、いずれにしても授業の質に差異がなかった点がとてもよかった」と記述した学生もいた。また、「今日は提出した課題へのコメントを直接聞きたいので教室に来た」と主体的に参加形態を選んでいると思われる学生も見受けられた。

学生にとって参加形態がフレキシブルなハイフレックス授業であるが、教員が授業日に出張などで都合が悪くなった場合に、「今週は非同期型だけになります」などとして、教員にとってもフレキシブルな運用ができると、教員も学生もHappyになれそうだ。ハイフレックス授業はコロナ禍の「正の遺産」となるのではないだろうか。



渡辺博芳（帝京大学）（正会員） hiro@ics.teikyo-u.ac.jp

1988年宇都宮大学大学院工学研究科修士課程修了。栃木県庁を経て1991年帝京大学理工学部・助手、現在、同教授、同大学ラーニングテクノロジー開発室・室長、博士（工学）。教育工学・情報教育に関する研究に従事。

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

# 第13回全国高等学校情報教育研究会全国大会 (オンライン大会)

小原 格

東京都立町田高等学校

## オンライン大会とその軌跡

2020年8月16日、全国高等学校情報教育研究会(以下単に「全高情研」という)による初めてのオンライン全国大会が開催された。ここでは、このオンライン大会について、母体である全高情研やその全国大会、また、オンライン大会に至る過程、大会の内容等について、それらの舞台裏も含め、簡単に解説をしていきたい。

## 全高情研とは

全国高等学校情報教育研究会(以下単に「全高情研」という)は、2003年に高等学校新教科「情報」がスタートしたことを受け、2008年に発足した、各自治体等の情報教育等研究会が集まった全国的な組織である(図-1)。全国の高等学校における情報教育の研究推進ならびに会員相互の研鑽をはかることを目的とし、発足以来、毎年、8月に全国大会を開催し、教科「情報」ならびに情報教育の発展に寄与してきた。

情報科は現在、普通科では「社会と情報」「情報の科学」のそれぞれ2単位(週2時間)の選択必修と授業数が少ない。そのため、各研究会においても、特に小規模校が多い地方の自治体によっては、他教科、たとえば数学とともに情報の授業を受け持つなど、いわゆる「兼担」が行われている学校も多い。年によって情報科を担当する教員が変わってしまうことなどもあり、各自治体等における研究会の有無、組織上の位置づけや名前、また、その運営方法等もさまざまである。このこともあって、全高情研では発

足当時より各研究会からの加盟登録方式をとっており、2020年現在、32の情報教育等研究会が加盟している。現在も、新学習指導要領における必修「情報I」の実施に向け、その輪を広げているところである。

## 全国大会

全高情研の大きな特徴として、現場の教員による手作りの運営が挙げられる。特に全国大会では、毎年、その年に開催される自治体等の情報教育等研究会が中心となり、前年度までの大会役員や経験者などによる有志とともに実行委員会が組織される。前年度までに大会を実施した経験やノウハウを元に、開催地の意向も踏まえ、一緒に大会を作り上げていく。多くの研究会にとって、全国大会の経験が初めてにもかかわらず、協力しあい、皆でノウハウを共有することによって会を運営し、大会を成功裏に収めてきた。

全国大会は、2008年の東京大会に始まり2019年の和歌山大会まで毎年行われ、12回を数えるようになった。全高情研発足当初は、現場教員の運営上の負担から、隔年で大会を実施するような案もあったが、すでに毎年の恒例行事として定着している。こ



図-1 全高情研サイト

れもひとえに、実行委員はもちろん、参加者の情報教育や情報科教育に対する思い、未来を託す子供たちによりよい教育を施したいという熱意によるものと感じている。

## 愛知大会からオンライン大会へ

2019年8月、第12回和歌山大会開催時に次年度2020年8月の愛知大会がアナウンスされ、その翌月には開催予定地である愛知県立大学にて、実行委員会も兼ね現地下見や調査が行われた。愛知県の先生方による熱心で計画的・献身的・着実な取り組みにより、用意周到に準備が進められ、2020年1月にはすでに大方が完了し、順調に4月のポスター発表および口頭発表の申込受付が始まる予定であった。

2月、3月に入り、新型コロナウイルス感染症の蔓延による東京オリンピックの延期、各種学会の大会延期、大学の閉鎖等の発表も相次ぐようになり、想定を上回る緊急事態に、4月8日、2020年度の愛知大会の中止が正式にアナウンスされた。多くの学校で、臨時休校の措置や遠隔授業に向けての準備等が進められ、学校現場は相当混乱していたにもかかわらず、最後まで怠らずに大会開催に向けて準備をしていた中での苦渋の決断でもあり、特に、中心となって準備をされていた愛知県の先生方の無念さはいかばかりかと感じている。

当時、2020年3月2～4日に開催された「第12回データ工学と情報マネジメントに関するフォーラム／第18回日本データベース学会年次大会（DEIM2020）」が初の大規模なオンラインセッションを行い、注目を集めていた。全高情研も、何とか全国大会の火を消さずに灯していきたい、また、情報教育の研究会だからこそ、オンラインで、最低限の内容でもよいから実施していきたい、という思いから、オンライン大会の可能性を研究・模索しはじめたのもこのころである。ただ、教員の間でビデオ会議システムについてようやく認知・利用が進んできたころであり、本格的に利活用していくためのノウハウをまだ持ち

合わせている者は非常に少なかった。

そのとき、オンラインでの大会ノウハウを持つ国立情報学研究所およびシスコシステムズ合同会社のご協力をいただけることとなり、一気にオンライン大会開催への道が開けることとなった。この場をお借りしてお礼を申し上げたい。

## オンライン大会への準備

2020年第13回愛知大会の中止に伴い、オンライン大会は別組織で行われることとなり、主催は全高情研事務局、共催は東京都高等学校情報教育研究会<sup>2)</sup>（以下単に「都高情研」という）として、実行委員会形式で開催されることとなった。コロナ禍で移動もままならないこともあり、打合せもオンライン中心で行われた。

まずは、自分たちで大会のノウハウを身に付けるべく、5月30日に行われる都高情研総会・研究協議会をオンラインで実施することとした。内容は、一斉方式の総会と、オンライン教育の現状に関する東京・神奈川・大学の3つの簡単な報告と各分科会にわかれてのセッションである。全体会および報告はWebEx Eventsを活用し、大規模のセミナーを実施する方法を身に付けるとともに、分科会ではそれぞれWebEx Trainingを活用し、双方向の顔が見えるやりとりの方法を身に付けることができた。実質1時間程度ではあったが、100名を超える申込者の全員がリモートで接続する形の研究会を初めて経験することにより、全国大会でのイメージや課題を共有することができた貴重な体験であったと感じている(図-2)。

## オンライン大会の実施

5月30日の都高情研総会の後、6月4日に第1回のオンライン大会実行委員会が開催された。急場にもかかわらず、実行委員として、埼玉・神奈川の先生方をはじめ、愛知・大阪・兵庫の先生方も遠隔参加・協力をいただけることとなり、総勢20名以上の実行委員会組織となった。

以下に大会の概要等を示す。詳細は参考に挙げた



全高情研 Web サイト<sup>1)</sup>を参照されたい。

## □ 大会要項

○第13回全国高等学校情報教育研究会全国大会  
(オンライン大会)開催について

### (1) 目的

全国の情報教育関係者がオンラインでの、講演、研究発表、協議、情報交換等とおして、これからの教科「情報」の在り方および課題解決の方策を探り、実践的な指導力の向上を図る。

### (2) 日時

2020年8月16日(日)

13時30分から16時30分まで

### (3) 場所

オンライン(WebExによる会議室への参加)

### (4) 内容

- 開会行事
- 基調講演 (13時45分～14時45分)
- 分科会1 (14時55分～15時25分)
- 分科会2 (15時30分～16時00分)
- 閉会行事

その他、オンデマンド(Web上)発表

### (5) 参加費

無料

### (6) 主催等

主催：全国高等学校情報教育研究会

共催：東京都高等学校情報教育研究会

後援：国立情報学研究所、シスコシステムズ合同会社、アドビ(株)(Adobe KK)、情報処理学会、日本情報科教育学会、日本産業技術教育学会、情報教育学会研究会(IEC)、全国専門学科「情報科」高等学校

長会、東京都教育委員会、埼玉県教育委員会、神奈川県教育委員会、愛知県教育委員会

協賛：各加盟都道府県研究会・部会等

## □ 当日運営

大会当日、近隣の一部の実行委員は本部(都立立川高等学校)に集合し、大会運営に当たった(図-3)。都高情研総会時に会長挨拶の回線状況が非常に悪かったこともあり、会長挨拶等の重要場面においては、感染対策を施した上で、集合したパソコン教室にて実施した。

配信されるカメラを最後部のPCに設置し、スタジオ風を利用して出演者が入れ替わる方式を採用することとした。

また、分科会時は、ハウリングを起こさないよう、ほかの端末はヘッドセット等を利用するとともに、1つの分科会に対して、司会、計時、チャット質問収集記録の3名の係を置き、遠隔でも効率的に分業できる工夫を行った。

## □ 基調講演

### 「新しい情報科に向けて準備をしよう」

国立教育政策研究所 教育課程研究センター研究開発部  
教育課程調査官 鹿野利春 氏

新学習指導要領の内容を再確認するとともに、実施に向けての準備・心構えや、現在の小中学校における情報教育の現状等をお話しいただいた。

## □ 分科会

3つの会議室を用意し、14時55分からの分科会1、15時30分からの分科会2の計6名の発表があった。



図-2 都高情研研究協議会「大学での遠隔教育」



図-3 大会本部

紙面の都合上、詳細は割愛させていただく。

## ○分科会 1

- 総合学科1年次「社会と情報」でのWebプログラミング実践

愛知県立高蔵寺高等学校 田中 健 氏

- コミュニケーションと情報デザインに関する指導案の作成

埼玉県高等学校情報教育研究会 富田 平 氏

- テキストマイニングによるアニソンの歌詞分析—分析から時代背景を読み取ろう—

神奈川県立茅ヶ崎西浜高等学校 鎌田高徳 氏

## ○分科会 2

- 愛知県におけるオンライン学習支援に関する取り組み

愛知県立尾西高等学校 柴田謙一 氏

- 教科「情報」における「主体的に学習に取り組む態度」を育てる学習活動の提案と試行

広島大学附属福山中・高等学校 平田篤史 氏

- 情報Iにおける探究的学びとプロトタイピングの授業設計

奈良女子大学 竹中章勝 氏

## □動画発表(オンデマンド)

分科会でのオンラインリアルタイム発表とは別に、あらかじめ動画を提供していただき、当日その動画を公開する形で17名の発表が行われた。なお、紙面の都合上、具体的なタイトル・内容および発表者については割愛させていただく。参考文献として挙げた全高情研のサイト<sup>1)</sup>をぜひ参照されたい。

## 成果と課題

コロナ禍の中、何とか今年度の全国大会が途切れずに開催されることになり安堵する半面、今回のオンライン大会実施を通して、オンラインならではの利点や難しさが浮き彫りになったように感じている。それぞれの面を確認していきたい。

利点は何と言っても「現地に行かなくても済む」こ

とである。運営側にとっても、愛知や大阪の実行委員が遠隔で参加し、感染症を気にすることなくさまざまな協力をしていただくことができた。また、WebEx等のWeb会議ツールが用意できれば、現地の会場費やパネル等のレンタル費用、交通の心配をする必要もない。参加者についても同様で、特に子育てや介護等、家から長時間離れられない方も、自宅にしながら気軽に参加できるメリットは大きい。交通費や宿泊費もかからず、経済的でもあるだろう。

半面、難しさとして、運営側としては会議システムに習熟する必要があるが、また、突発的なトラブルに対して準備がしづらい点が挙げられる。今回はCiscoによるサポートを受けることができたため、利用方法に関しては大きな問題はおきなかったが、常にこのような恵まれた環境であるとは限らない。また、回線が不安定でつながらなくなる、接続側の発表者の音声でなかったりマイクの音が聞こえなかったり、というトラブルも今回実際におき、運営側だけでは対応できない事態も起こり得る。参加者は画面を見続けることになり、モニタに慣れない方にとって、長時間の開催が苦痛に感じてしまうことも考えられるだろう。さらには、特に懇親会など、直接的な人間関係を構築する場が非常に限られてしまう、ということも挙げられる。

今後、Web会議ツール等のノウハウは積み重ねられていくことが想定されるが、人間関係の構築をどのように進めていくのか、などには、より一層のICT活用方法の研究と、発想の転換などが必要になっていくと思われる。オンラインならではの全国大会の考え方も、ますます洗練されていく必要があるだろう。

### 参考文献

- 1) 全国高等学校情報教育研究会, <http://www.zenkojoken.jp/> (2020.11.14 閲覧)
- 2) 東京都高等学校情報教育研究会, <http://www.tokojoken.jp/> (2020.11.14 閲覧)

(2020年11月30日受付)



小原 格 (正会員) ohara@johoka.info

東京学芸大学卒業。1993年数学科教諭として東京都に採用。2003年より情報科。文部科学大臣優秀教職員表彰。現在、東京都立町田高等学校指導教諭、東京都教職員研修センター認定講師、青山学院大学、電気通信大学非常勤講師等。





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

# 新学習指導要領「情報Ⅰ」の授業を考えよう —LINE スタンプの制作から学ぶコミュニケーションと情報デザイン—

富田 平 | 埼玉県高等学校情報教育研究会／埼玉県立浦和第一女子高等学校

## 研究会の活動概況

### これまでの取り組み

埼玉県高等学校情報教育研究会は、現在8名の研究委員で活動しており、毎年共通のテーマを設定して研究論文をまとめている。初年度の「情報モラルに関するアンケート調査」から始まり、その後も新学習指導要領「情報Ⅰ」を見据えた研究活動を行っている。本活動内容は、全国高等学校情報教育研究会の全国大会においても毎年発表をしている(図-1)。

### 2019年度の研究活動

2019年度は、2022年度の新学習指導要領「情報Ⅰ」を見据えて、反転学習を意識しながらプログラミング教育に関する動画教材を作成した。図-2、図-3は作成した動画教材の一例であり、硬貨の並べ替えによってクイックソートの仕組みを説明している。

本研究を通して、生徒の理解度に合わせて授業を進めることのできる動画教材とプログラミングの親和性は高いという知見が得られた。一方、動画教材の作成には大きな労力と時間が必要である。した

### これまでの歩み(13年間)

年	研究内容
2008	情報モラルに関するアンケート調査
2009	情報機器を利用する上でのコミュニケーションの工夫
2010	情報機器を利用する上でのコミュニケーションの工夫
2011	コミュニケーション能力の向上を目的とした授業の工夫
2012	生徒の思考力・問題解決能力の育成を図る授業実践
2013	新教育課程に向けた年間指導計画の作成と分析
2014	LINE等ソーシャルメディアに関する指導について
2015	「社会と情報」の中で論理的思考力を養う授業案
2016	プログラミングに関するアンケート調査
2017	反転学習を意識した動画教材の作成
2018	反転学習を意識した動画教材の作成
2019	プログラミング教育を見据えた動画教材の検討
2020	新学習指導要領「情報Ⅰ」(2)コミュニケーションと情報デザインに関する指導案の作成

図-1 全国高等学校情報教育研究会(全国大会)での発表内容

がって、動画をクラウド上で共有し、誰でも動画を視聴できる環境の整備が課題である。

## 2020 年度の研究活動

### 研究背景

2020 年度は、新学習指導要領「情報 I」を指導することを見据えて、「(2) コミュニケーションと情報デザイン」に関する指導案を作成し、実践することになった。特に、「情報デザイン」というキーワードに着目し、受け手に分かりやすく情報を伝える活動ができるように指導案を作成することにした。本稿では、「LINE スタンプの制作から学ぶコミュニケーションと情報デザイン」というテーマで作成した授業案を紹介する。

### 授業の目的

本授業は、LINE スタンプの制作を通して、より良い情報デザインについて考えられる知識・技能や思考力・判断力・表現力を身に付けることが目的である。LINE とは、生徒が日頃からコミュニケーションツールとして身近に利用するアプリケーションであり、LINE スタンプとは会話の中で文字の代わり

にメッセージとして送るイラストなどの画像のことである（以下、特に必要でない限り LINE スタンプのことを「スタンプ」と表記する）。

ここで、「知識・技能や思考力・判断力・表現力を身に付ける」という部分が、学習指導要領上での項目を指すのか確認する。「知識・技能」の部分は、「(ア) メディアの特性とコミュニケーション手段の特徴について、その変遷も踏まえて科学的に理解すること」と「(ウ) 効果的なコミュニケーションを行うための情報デザインの考え方や方法を理解し表現する技能を身に付けること」を特に意識して授業案を作成した (図-4)。

「思考力・判断力・表現力」の部分は、「(イ) コミュニケーションの目的を明確にして、適切かつ効果的な情報デザインを考えること」と「(ウ) 効果的なコミュニケーションを行うための情報デザインの考え方や方法に基づいて表現し、評価し改善すること」を特に意識して作成した (図-5)。

適切かつ効果的なスタンプを作成するためには、受信者がどのような反応を示すか推測することが重要である。制作者が求めている意図や思惑と受信者



■図-2 作成した動画教材の一例



■図-3 作成した動画教材の一例 (外部リンク)

**高等学校学習指導要領(平成30年告示)解説**

ア 次のような**知識及び技能**を身に付けること。  
 (ア)メディアの特性とコミュニケーション手段の特徴について、その変遷も踏まえて**科学的に理解すること**。  
 (イ)情報デザインが人や社会に果たしている役割を理解すること。  
 (ウ)効果的なコミュニケーションを行うための**情報デザインの考え方や方法を理解し表現する技能を身に付けること**。

■図-4 高等学校学習指導要領解説 (知識・技能)

**高等学校学習指導要領(平成30年告示)解説**

イ 次のような**思考力、判断力、表現力等**を身に付けること。  
 (ア)メディアとコミュニケーション手段の関係を科学的に捉え、それらを目的や状況に応じて適切に選択すること。  
 (イ)**コミュニケーションの目的を明確にして、適切かつ効果的な情報デザインを考えること**。  
 (ウ)効果的なコミュニケーションを行うための**情報デザインの考え方や方法に基づいて表現し、評価し改善すること**。

■図-5 高等学校学習指導要領解説 (思考力・判断力・表現力)

のリアクションには、ズレが生じる可能性があるからだ。このズレを認識し、伝えたい情報を伝えられるようにするために、複数回にわたって評価・改善することを意識して授業を実施した。

## 授業の流れ

### LINE スタンプのガイドラインから、 情報デザインについて考える (1 時間目)

まず、LINE スタンプの1つである「LINE クリエイターズスタンプ」の制作ガイドラインおよび審査ガイドラインに則って制作することを説明する (図-6)。

LINE クリエイターズスタンプとは、「LINE クリエイターズマーケット」で販売されているスタンプのことで、審査が通れば誰でも販売できるスタンプである。LINE クリエイターズスタンプの制作ガイドラインには、スタンプの数や画像サイズなど詳しくルールが記述されている。このルールを遵守して制作することも重要であるので、画像の解像度やデータ量など、科学的な視点を理解させた上で制作させている。また、審査ガイドラインには禁止事項が記述されている。会話やコミュニケーションに適

さないもの、視認性が悪いものなどさまざまであるが、この内容を理解した上でスタンプを制作するように伝えた (以下、制作ガイドラインおよび審査ガイドラインのことを「ガイドライン」と表記する)。

これらのガイドラインを通して、情報デザインとは何か、ユニバーサルデザイン、色彩、色の与える情報などについて理解を深めさせた。そして、情報デザインが人や社会に果たす役割を理解させるように指導した。

### ターゲット層を想定して、効果的なスタンプを企画する (2 時間目)

2 時間目は、スタンプの企画書を作成する (図-7)。まず、スタンプを使用するターゲット層の情報収集と整理をマインドマップによって行った。マインドマップとは、頭の中で思考していることを放射状にキーワードやイメージを広げて描き出したものである。ターゲット層を明確にすることで、コミュニケーションの目的を明確にし、適切かつ効果的な情報デザインを考えさせるという基盤をマインドマップによって固めることができる。そして、スタンプの立案、企画書の制作、提出を行い、教員からのフィードバックを得て改善するという流れで進めた。

### デザインを確定する (3 ~ 4 時間目)

3 時間目は、スタンプのデザインを確定させる (図-8)。2 時間目で立案したスタンプのデザインと企画書を用いて、生徒同士で簡単なプレゼンテーションを行わせた。そのときに、相互評価を実施することで、必要に応じてスタンプを改善する機会を

#### 授業内容

時間	内容
1 時間目	スタンプ制作の概要 / 情報デザインとは

- LINEスタンプの制作ガイドライン  
LINEスタンプの審査ガイドライン を紹介する
- 情報デザインとは何か  
「ユニバーサルデザイン」「色彩」「色の与える情報」について  
(情報デザインが人や社会に果たしている役割を理解させる)



■図-6 授業内容 (1 時間目)

#### 授業内容

時間	内容
2 時間目	スタンプの企画

- ターゲット層の情報収集と整理 ⇒ マインドマップ
- スタンプ立案→企画書制作→提出→教員のフィードバック→改善
- どのようなスタンプであればターゲット層に使ってもらえるかを検討  
(コミュニケーションの目的を明確にして、効果的な情報デザインを考えさせる)

■図-7 授業内容 (2 時間目)

#### 授業内容

時間	内容
3 時間目	スタンプのデザイン確定
4 時間目	紙ベースでスタンプのデザイン

- 3 時間目  
前時間の調査に基づいて立案したスタンプデザインと企画書をもとに生徒同士でお互い簡単なプレゼンテーションを行う。  
→相互評価→改善
- 4 時間目  
スタンプを紙に書き、スマートフォンのカメラ機能で取り込む。

■図-8 授業内容 (3 ~ 4 時間目)

設けた。4時間目は、紙ベースでスタンプのデザイン（確定版）を作成し、スマートフォンのカメラ機能で取り込む作業を行った。

### スタンプの制作を行う（5～8時間目）

5時間目から8時間目は、「ibisPaint X」というスマートフォンやタブレット端末に対応した画像編集ソフトウェアを用いてスタンプの制作を行う（図-9）。取り込んだ画像を下書きレイヤーに設定して、スタンプの画像をスマートフォンやタブレット上で制作していく。

なお、スマートフォンやタブレット端末を持っていない生徒に対応できるように、学校で数台のタブレット端末を準備している。

本時では、ガイドラインを再度確認すること、スタンプを1つ制作したら担当教員のチェックを受けるよう生徒に伝えている。図-10は授業の様子であるが、このように意欲的に取り組んでいる生徒の姿が多く見られた。

担当教員によるスタンプの確認は、生徒によって進捗状況が大きく異なるので、生徒が尋ねてきたタ

イミングで随時フィードバックすることにした。授業時間内で対応できない生徒は、次の授業にフィードバックする時間を設定することで、円滑に進めることができた。

### スタンプを発表する（9～11時間目）

9時間目は、Google スライドを使用してプレゼンテーションの準備を行った。10～11時間目は、5～6人のグループを作ってそれぞれ発表を行い、相互評価を実施した。最後に各グループの優秀作品をクラス全体で発表した（図-11）。

相互評価では、ターゲット層を調査して制作できているか、目的に沿ったスタンプが制作できているか、スタンプのガイドラインに則って制作できているか、などを1～5の得点で評価させるようにした。

### 制作されたスタンプ（例）

生徒が制作したスタンプを紹介する。

1つ目は、女子高生をターゲット層にして制作された芋けんぴのキャラクターである（図-12）。「芋けんぴあ〜ん」「芋けんぴーす」「芋けんぴえん」「芋けんぴーん」「いもる」といったスタンプで、実際にLINEでどのようなコミュニケーションが行われるのか独自に分析した上で制作されたものになっている。

2つ目は、埼玉県民をターゲット層にしたスタンプである（図-13）。「暑すぎ熊谷かよ」「テンション上尾」「とりあえず大宮集合」「お茶飲もう狭山の」「ネギ食べよう深谷の」といったスタンプで、埼玉県民なら思わず使いたくなるようなデザインとなっている。

時間	内容
5時間目 ～8時間目	「ibisPaintX」という画像編集ソフトウェアを用いてスタンプの制作を行う。取り込んだ画像を下書きレイヤーに設定して、スタンプの画像をスマートフォンやタブレット上で制作していく。

- ・ LINEスタンプのガイドラインに則って制作
- ・ 1つできたら教員のチェック→改善

図-9 授業内容（5～8時間目）



図-10 授業での様子

時間	内容
9時間目	プレゼンテーション資料作成・発表準備 ※ googleスライドを使用する
10時間目 ～11時間目	1チーム5～6人のグループでプレゼンテーションを行い、相互評価を実施する グループ内での優秀作品をクラス全体で発表

図-11 授業内容（9～11時間目）

## 授業を実施する上での留意点

### 科学的な理解を深める

スタンプを制作する過程で、科学的な理解を深めることを意識させることが大切である。たとえば、ガイドラインには、スタンプ画像（選択式）の場合、解像度は横 370px × 縦 320px（最大）、サイズは 1 個あたり 1MB 以内など細かく決められている。これらをよく確認しながら制作させることで、画像のデジタル表現について理解を深めさせている。

### 類似の作品がないか、画像検索で確認しながら作る

著作権に関して、すでに制作されている著作物と類似していないか検証を行っている。具体的には、下書きレイヤー用の画像を取り込んで、Google の画像検索機能を使用して、似たものがないか確認させる時間を設けている。万一、似たようなデザインがあった場合は、スタンプのデザインを作成し直して、再度スマートフォンのカメラ機能で取り込む作業を行った。

### スタンプの販売は、各家庭の判断にゆだねる

授業では、スタンプを制作するところまでを実施することにしている。もちろん、スタンプを販売す

ることも可能であるが、納税義務の可能性が生じる。そのため、スタンプの販売に関しては各家庭の判断にゆだねる形をとっている。

## 授業を振り返ってみて

### ユーザは、制作者の意図通りに使用するには限らない

授業の中で制作したスタンプについて、教員側からのアドバイスや、生徒同士で相互評価をする機会を複数回取り入れたことで、カラーユニバーサルデザインなど、情報デザインの考え方に基づいて表現し、必要に応じて改善することができた。ユーザは、制作者の意図通りにスタンプを使用するには限らないということを相互評価によって認識できたことは大きな収穫である。

### 身近な素材でプロダクト側の立場を経験することで

#### デザインへの視野を広げる

生徒は、自分が関心を持っているものや身近な生活の中にあるものをスタンプの題材にすることで、主体的に授業に取り組むことができていた。

また、普段ネットワークサービスをユーザの立場で利用しているが、今回はプロダクト側の立場を経験したことにより、新たな見方や考え方を広げることができたのではないかと考える。

さらに、自身が作成したスタンプを教員や他の生徒に紹介する活動を通して、プレゼンテーション能力を高めることができた。今後においても、主体的・対話的で深い学びを実現する授業を実践し、問題解決能力や言語能力を育んでいきたいと考えている。

(2020年11月15日受付)



■図-12 生徒の作品（芋けんぴのスタンプ）



■図-13 生徒の作品（埼玉県のスタンプ）

富田 平 tomita.taira.a7@spec.ed.jp

埼玉県立浦和第一女子高等学校教諭、埼玉県情報教育研究会委員長。

## 2021 年度会誌「情報処理」モニタ募集のお知らせ

会誌編集委員会

会誌「情報処理」をより良くするために編集委員一同努力を続けておりますが、会員の方々の評価や希望をうかがい、今後の改善に役立てるために、モニタ制度を設けております。関心のある方はぜひふるってご応募ください。

**応募の資格** 本会会員で、モニタの役割を積極的に果たしていただける方。

**モニタの役割** 学会 Web ページ (<https://www.ipsj.or.jp/magazine/enquete.html>) から、毎月アンケートに回答する。  
◇記事に対する評価 ◇記事に対する感想 ◇意見 ◇記事テーマの提案  
◇そのほか全般的な意見・提案など

注) 記事をすべて読むといったことは必ずしも必要ではありません。自分の立場や問題意識、得意とする分野などを基準とした「独断と偏見による」自由な意見を期待します。

**期 間** 原則として1年間(2021年4月～2022年3月)。\*最長3年までとします。

**対 象 号** 会誌「情報処理」62巻5号～63巻4号

**謝 礼** 貴重なご意見をいただいた方には薄謝または記念品を贈呈します。

**募集人員** 特に定めませんが、応募者数によっては当委員会で調整させていただくことがあります。

**応募締切** 2021年2月25日(木) 必着

**そ の 他** ジュニア会員で、会誌(冊子体)の送付を希望される方には、モニタ期間中会誌を送付いたします。(先着50名、アンケート(12回)に必ず回答いただくことを条件とします)  
希望する場合は、申込書の要望欄に<会誌送付希望>とお書きください。

**申 込** 以下 Web ページ内<2021 年度 会誌「情報処理」モニタ申込フォーム>よりお申し込みください。

<https://www.ipsj.or.jp/magazine/topics/2021monitor.html>



**照 会 先** 情報処理学会 会誌編集部門(モニタ係) E-mail: editj@ipsj.or.jp



この記事のこんなところが良かった!



こんな記事が読んでみたい!



この記事のここを改善してほしい

ご意見お待ちしております!



連載

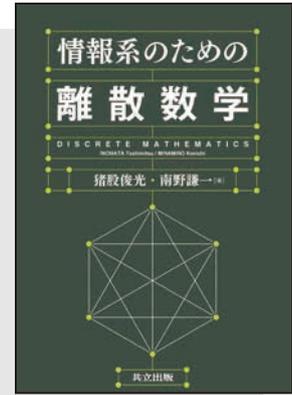
ビブリオ・トーク  
- 書評 -

… 石井一夫 (久留米大学)

## 情報系のための離散数学

猪股俊光・南野謙一 著

共立出版 (2020), 2,500 円+税, 200p., ISBN : 978-4-320-11436-4



離散数学という何を思い浮かべるであろうか？本書籍の目次の章立てを見ると、データ分析を行う上で必要となるデータの表記法、計数方法、論理的作法、関数、木構造、グラフ理論など、データの処理方法に関係するリテラシーが網羅されている。これらはプログラミングを学ぶ上でのデータ型、条件分岐、関数など、その基盤となるリテラシーを含んでいる。さらに、統計学における確率論や、離散型データの処理、条件付き確率、線形モデルなどの基盤ともなっている。

これらの事項は、本書で離散数学自体を学んでいるときにはその重要性を意識することはないが、いざデータを扱うようになり、統計やプログラミングを駆使するようになると、日常的な概念として必要となってくる。そういう意味で、データとプログラミングを扱うものにとっては、不可欠な基盤となる事項をまとめた書籍になっている。

いくつか、例を示そう。

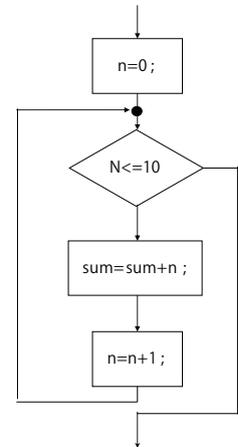
第1章は「命題論理」の章として、真偽が定まる式や文である命題について解説されており、「否定」、「かつ」、「または」などの論理式に関する事項がまとめられている。これは、プログラミングで出てくる「条件分岐」や「論理演算」を考える上での基礎となるものである。逆に言えば、離散数学の命題や論理式をコンピュータ上で実装したものが、プログラミングの条件分岐や論理演算であるという見方もできる。

第2章は、「集合の基礎」について書かれている。集合の要素や、全体集合、部分集合など集合同士の関係などを論じている。これらはプログラミングでの「データ型」の考え方の基礎になる。Pythonで登場する配列で扱うリストやタプル、辞書、セットなどの概念やその処置の基礎になるものである。さらには、統計学における確率論で出てくる「標本空間」と「事象」を考える上での基礎にもなる。集合の「共通部分また

は積集合」は統計の「積事象」に、集合の「合併集合または和集合」は統計の「和事象」に対応する。

第3章の「帰納的定義と証明技法」では、数学的帰納法や背理法について述べられている。数学的帰納法は数学における証明技法であるが、私個人的には累積和のアルゴリズムを連想する。たとえば、1から10までの総和を求めるCのコードは以下のように書ける。また、これをフローチャートで視覚的に表現すると下右図のようになる。

```
# include <stdio.h>
main()
{
    Int n, sum ;
    sum = 0 ;
    for (n=0 ; n <= 10 ; n=n+1)
        sum = sum + n ;
}
```



数学的帰納法とは、自然数に関する命題  $P(n)$  がすべての自然数  $n$  に対して成り立っていることを証明するための証明技法であるが、以下のような3ステップからなる。

- (1)  $n = 0$  のとき、 $P(0)$  が成り立つことを示す。
- (2) 任意の自然数  $k$  に対して、「 $P(k) \Rightarrow P(k + 1)$ 」が成り立つことを示す。
- (3) 以上の議論から任意の自然数  $n$  について  $P(n)$  が成り立つことを結論づける。

上記のコードのうち、 $sum = 0$  が (1) に、for ブロックが (2) に対応する。こうしてみるとアルゴリズムは、数学の証明技法を取り込んでいる。

また背理法は、統計という検定で用いられる。集団 A と集団 B の平均値が異なることを検定 (証明) したい場合、まず、集団 A と集団 B が等しいという仮説 (帰

無仮説)を設定しておき、その仮説が成立する確率を計算し、それが5%未満というような通常あり得ない確率が出てきたときに、帰無仮説を棄却して、集団Aと集団Bの平均値が等しくないという対立仮説を採択する。この手法は本章でいう背理法そのものである。

第4章の「数え上げの基礎」では、順列、組合せ、2項定理が解説されているが、統計の離散型確率分布で登場するベルヌーイ試行や2項分布を理解する上で、不可欠な概念である。

第5章は「関係」について取り上げている。関係とは、2つの事象の相互作用を抽象化したもので、包含関係 ( $A \subset B$ )、同値関係 ( $A = B$ ) など、命題や論理式、集合、グラフにおける複数の変数やオブジェクトの関連性を表現する基礎になる。

きわめつけは、第6章の「関数の基礎」で、関数は、プログラミングや、線形代数、解析学、統計学などのあらゆる分野での重要概念として登場する。プログラミングやデータ分析では、関数は不可欠のツールである。最後の3章は、グラフ理論に関する話題が展開されている。

第7章「グラフの基礎」でグラフの基本事項とその処理について、第8章「木と探索」では閉路を持たないグラフである木構造について、第9章「ネットワークと各種グラフ問題」では、重み付きグラフであるネットワークについて解説されている。グラフとネットワークもプログラミングで利用されている例は多数ある。

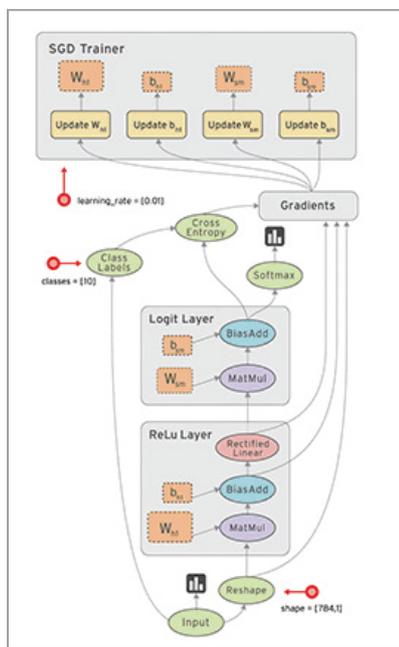


図-1 TensorFlow の data flow graph 実施例  
[https://docs.w3cub.com/tensorflow/guide/programmers\\_guide/graphs/](https://docs.w3cub.com/tensorflow/guide/programmers_guide/graphs/) より引用

先に示したフローチャートも一種の有向グラフと考えることができる。機械学習で用いられるニューラルネットワークは典型的な重み付きグラフである。最新のトレンドとして TensorFlow の data flow graph が挙げられる。TensorFlow はそのデータ処理を data flow graph として構築する。data flow graph では、ノードは計算ユニットを表し、エッジ (= edge, 辺) は計算で使用したり生成したりするデータを表す (図-1)。

本書は、大学における専門課程での「離散数学」のテキストとして使用されてきたものをもとに書かれている。しかし、これら関連の用語が簡潔に理解しやすい形で説明され、知識の整理にとっても役に立つ。基本的用語もコンパクトにまとまって説明されているため、辞書がわりにも使えそうである。

本書を通読するにあたり、興味深い書籍と読み比べたので紹介する。結城浩著『プログラマの数学第2版 (SBクリエイティブ)』(2018年)<sup>1)</sup>である。この本(以後、「結城本」と称する)でも、論理(第2章)、数学的帰納法(第4章)、順列・組み合わせ(第5章)が取り上げられており、グラフ理論も第3章(剰余)で具体的な例が登場する。本書と結城本を読み比べると、本書の内容がよりイメージしやすく、理解しやすくなるのでおすすめである。

ところで、小学校におけるプログラミング教育の必修化が2020年度からはじまった。その目的は、プログラミングを通じて論理的思考力を高めることにあるという。先に、「離散数学の命題や論理式をコンピュータ上で実装したものが、プログラミングの条件分岐や論理演算であるという見方もできる」と述べたが、その意味ではこの考え方は理にかなっていると思われる。しかし、プログラミングには論理的思考以上に、人間のアイデアをコンピュータ上で実装し実用化するための言語という役割があると考えている。

参考文献

- 1) 結城 浩:プログラマの数学第2版, SBクリエイティブ (2018). (2020年10月18日受付)

石井一夫 (正会員) ishii\_kazuo@med.kurume-u.ac.jp

久留米大学バイオ統計センター准教授。専門分野:ビッグデータ分析, 計算機統計学, データマイニング, 数理モデリング, 機械学習, 人工知能。2015年度本会優秀教育賞受賞。2019年度本会シニア会員。2020年(株)エヌ・ティー・エス学術顧問。日本技術士会フェロー, APEC エンジニア, IPEA 国際エンジニア。





Joocho Kim and Makarand Hastak :

Social Network Analysis : Characteristics of Online Social Networks After A Disaster

International Journal of Information Management, Vol.38, Issue1, pp.86-96 (Feb. 2018)

## 災害時におけるソーシャルメディアの役割

災害時においてソーシャルメディアは、(1) 災害状況に関する情報の効率的かつ効果的な取得、(2) 自助、共助における支援活動のサポートと促進、(3) 災害対応機関への情報提供、リクエストなど、公衆情報の流通に大きな役割が期待される。筆者の体感では、災害時におけるソーシャルメディアの分析は2010年頃から急増したように思う。2010年ハイチ地震では、(3)の示すようなソーシャルメディアの双方向性を活かした動きは少なかったが、被災状況に関する多くの投稿がなされ、現地の惨状が世界中に発信された。2011年の東日本大震災では、被害報や支援団体の活動状況の情報提供のほか、孤立地域からの救助要請や救援物資の要請など双方向にソーシャルメディアを活用する動きが見られた。この頃から比較的規模の大きい災害が発生するたびに、Twitter, Facebook, Google+, YouTube, Instagramなどのソーシャルメディアが、情報提供の状況、情報拡散の程度、応急対応・救援への効果などのさまざまな観点から分析されてきた。2020年11月現在のGoogle Scholarにおけるソーシャルメディアと災害に関する論文数は、1,620,000件であり、高い関心が払われていることが分かる。

一方でこれらの有益な事例分析や知見抽出の手法開発は、そのほとんどが実用化と言えるまでの取り組みの共有や計画、対応策への導入まで至っていない。それは、ソーシャルメディアの利用形態が規模や地域、時節等、外因に影響されやすく、収集、流通するデータが事例によって異なることに起因する。つまりある意味、安定性に欠ける情報リソースであ

るためと考えられる。それにもかかわらず、大規模な災害が発生するたびに多くの研究者たちによってこのような分析が行われているのは、ソーシャルメディアが災害対応にとって有効・有益である可能性が見出されてのことだろう。これまでになされてきた災害時のソーシャルメディア解析の研究は、そのほとんどが一つひとつの事例であるが、筆者の個人的な考えではこうした事例の積み重ねによる帰納的な体系化が、多くの研究者がソーシャルメディアに感じている可能性を具現化していく道だと思う。

## 米国ルイジアナ州洪水での分析事例

本論文は2016年に米国で発生した洪水を取り上げたものであり、こうした積み重ねに必要な基礎分析を示したことに特徴がある。著者は、緊急対応時におけるソーシャルメディアネットワークの特性を把握するため、いくつかの主要な解析手法を適用した。解析の対象は2016年8月に米国ルイジアナ州を襲った洪水<sup>1)</sup>である。12日から降り続いた雨は記録的な豪雨となり、同州の多くの川で最高水位を更新した。特にAmite Riverでは洪水水位を4メートル以上上回り、広い地域で大規模な洪水が発生した。この洪水により13人が死亡し、約10万棟の家屋や建物が被災、2万人以上が浸水した家や車の中、医療機関から救助された。8月12日に州知事による、14日に大統領による非常事態宣言が発令されている。

著者がこの分析を行った背景として、同洪水に対する報道の少なさが挙げられる。4年前の2012年10月にニューヨーク市を含む米国東部を襲ったハリケー



ン・サンディは、当時の主要ニュースであるロンドンオリンピックや米国大統領選挙より多くの関心を集めていたが、ルイジアナの洪水では、米国大統領選挙とリオオリンピックに多くの報道時間が割かれた。当時、史上最悪とも言われた洪水が起こっているにもかかわらず、洪水に関する報道は圧倒的に不足しており、これによりソーシャルメディアは現地の情報入手手段として大きな役割を果たしていたと考えられる。

本論文で利用されたのは、2016年8月12日から12月1日にルイジアナ州の州都バトン・ルージュ市のFacebookページに投稿されたデータである。同期間内に1,171人のユーザと21,115件のアクティビティがあった。これらのデータを利用して、中心性、コミュニティ構造、センチメント分析が行われている。

著者ははじめに、David HarelとYehuda Korenが2000年に報告したfast multiscale layout algorithm<sup>2)</sup>を利用して、バトン・ルージュ市を中心とする1,171の頂点、21,115のエッジを持つネットワークグラフを描画した。このネットワークグラフに基づいて各頂点の重要性を調べるため、次数中心性、固有ベクトル中心性、媒介中心性の評価を行っている。特徴的な分析結果のみを述べると、各中心性および次数分布の上位10件は個人ユーザであり、緊急情報をオンラインの友人と積極的に共有していたことが示される。しかし、高い媒介中心性を示す頂点はバトン・ルージュ市を含む6つの組織、機関であり、これらのコミュニティは、バトン・ルージュ市との間の緊急情報フローを処理しその流れを制御するゲートキーパーの役割を果たしたと言える。

続いて、2002年にMichelle GirvanとMark EJ Newmanによって発表されたGirvan-Newman algorithm<sup>3)</sup>を利用してネットワークのコミュニティ構造を分析した。対象期間中に最も共有された投稿は、バトン・ルージュ市の情報サービス部門によって作成された氾濫推定マップである。このマップは、911の出動や被災者の捜索・救助に役立ったほか、市教区職員およびその他の公務員により、被災地の画像などが積極的に共有された。このマップの共有

や更新のリクエストをはじめとして、避難所の位置や災害廃棄物の処理方法と廃棄場所、被災者の支援情報、寄付など地域性の高い話題に関するコミュニティが全体の38%を占めた。

わずかではあるが、これらの投稿の内容についてのセンチメント分析にも触れられている。投稿のうち77%がThanksなどを含むポジティブな言葉を含んでおり、ほとんどが洪水、災害復旧チーム、災害廃棄物の処理に関連していた。さらに多くの被災者がプライベートメッセージを介して自宅の住所を共有し、周辺の廃棄物の処理をリクエストするなどのやりとりも見られた。

本論文で語られているのは、前述したように1つの災害についてのソーシャルメディアの分析の一事例である。長期間の洪水が続くなかで市または個人が中心となり、特に、バトン・ルージュ市が取り組んだ氾濫推定マップを主として、地域性の高い情報をやりとりしていたことが分かる。著者は結びとして、緊急時にタイムリーな情報を受け取ることの重要性と、情報拡散の点での有用性、さらには地方、州、および全国の異なるレベルで分析を行う必要性について述べている。発表から3年経った現在では、本論文は多くの解析者たちに1つの有益な解析事例として紹介されている。本論文で示されたような分析によって、一歩ずつではあるが、災害におけるソーシャルメディアの役割が明確化され、有用な情報や利用形態が明らかになっていくと考える。

#### 参考文献

- 1) FEMA, Louisiana Severe Storms and Flooding (DR-4277), <https://www.fema.gov/disaster/4277>
- 2) Harel, D., and Koren, Y.: A Fast Multi-Scale Method for Drawing Large Graphs. International symposium on graph drawing, Springer, Berlin, pp.183-196 (2000).
- 3) Girvan, M., and Newman, M. E. J.: Community Structure in Social and Biological Networks, Proceedings of the National Academy of Sciences 99.12: pp.7821-7826 (2002).  
(2020年12月7日受付)



廣井 慧 (正会員) hiroi@dimis.dpri.kyoto-u.ac.jp

2014年慶應義塾大学大学院メディアデザイン研究科後期博士課程修了。博士(メディアデザイン学)。2020年より京都大学防災研究所准教授。防災情報システム、災害の時空間データ解析に関する研究開発に従事。



イラスト：© Marie Katsurai

このコーナーでは、全国の学校・教育関係者の皆様が抱えるちょっとした疑問やお悩みを受け付けています。

第1回は、従来の対面授業とは異なる評価の在り方についてご相談いただきました。



**駒谷昇一先生**  
[正会員]

**オンライン授業では  
どのように成績を評価していますか？**

オンライン授業の成績評価をどう行うのか。Google フォームでオンラインテストを実施しましたが、紙ベースのテストよりも正答率が高くなっています。テスト中にWebページや講義用スライドを検索しているからなのですが、それを防ぐ方法もなく、どのようにオンラインテストを実施したらよいのか悩ましいです。どのような工夫があるのか、教えていただければ幸いです。

Q

A

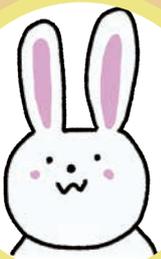
Facebook, Twitter, Web 回答フォームを通じて集まったアイデアをご紹介します！

以前より、ネットがつかえるPC教室でWebテストを実施してきました。授業で教えた個別の知識そのものではなく、その組合せや応用を出題します。たとえば算数なら $2 \times 3$ の答えでなく、12と8の公倍数を問題にする。地理ならば「他県に接していない都道府県はいくつあるか？」と問います。知識が身につけていれば簡単に解けるが、ネットでは見つけるのに時間がかかる問題とすればよいわけです。ネットは利用できるという前提で試験する方が時代に合っているでしょう。

Web



**金子 格先生**  
[正会員]



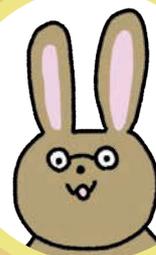
**ティープランニング先生**  
[正会員]

学籍番号で答えが変わるように問題を用意し、不正行為のリスクを減らしています。学籍番号を入力すると自動採点できるようにしています。

Web

画像処理の授業を担当しています。以前は紙ベースの小テストや定期試験を行っていましたが、オンライン授業になったため Moodle での実施に変更しました。問題は 5 × 5 程度の簡単な入力画像に対して手動で画像処理アルゴリズムを適用・計算してもらい、その数値結果を解答してもらいました。Moodle の問題バンクとランダム出題機能を使って、1 問あたり数値を変えた類似問題を 3 問用意して、そのうちの 1 つをランダムに出題しました。紙ベースよりも採点作業が楽になりました。また、不正防止にも一定の効果があったかと思えます。学生アンケートでも「不正がしにくい公正な評価方法がよかった」と複数名の回答がありました。今後、対面授業に戻っても、計算機室でのオンライン試験実施も検討しています。

Twitter



上瀧 剛先生  
熊本大学

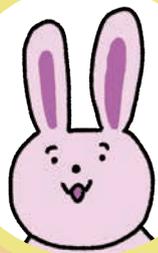
今のところ私の担当授業では「オンラインでのテストは実施しない」に帰着しています。ご質問の意図に反する回答になっているかもしれませんが、自分の事例を紹介させていただきます。少しでもご参考になれば幸いです。

【事例 1】講義+演習科目：オンライン授業になる前と同様に、授業中に行う計算機を使用する演習のレポートを毎回課しました。以前と違い、目の前に学生がいなかったためちょっとしたケアをしづらかった分、レポートのフィードバックで細かくアドバイスしました。

【事例 2】講義科目：講義内容の概要（+ちょっとした問題）をレポートとして毎回提出してもらいました。「スライドや板書をただ写しているだけ」「単語しか頭に入っていない」では困りますので、あらかじめ文章として書くように（たとえば個条書きは減点対象として）伝えました。

評価がまた悩ましいですが、レポートごとに 5 段階評価で採点し、合計点で最終評価としました。なお、オンラインということを考慮し、レポートの締切にはある程度の猶予を持たせ、また提出していない学生には個別に催促もしました。いずれにせよ「学生の理解度がより高まること」、つまり「調べること」「学生同士での相談」「教員への質問」などはどの授業でも以前より強く推奨しており、その理念はオンライン授業になっても変わりません。

Web



鈴木大三先生  
筑波大学

皆様の参考になれば幸いです！ 次回もお楽しみに！

「先生が質問です!!」への質問・回答受付

- ▶ 質問受付: <https://www.ipsj.or.jp/magazine/senseiga-q.html>
- ▶ 回答募集: 情報処理学会 Facebook ページ (@IPSJ.official)  
Twitter アカウント (@ipsj\_shinsedai)



質問受付

# IFIP—情報処理国際連合— 近況報告



相田 仁 | IFIP 日本代表 / 東京大学

IFIPは2020年に創立60周年を迎えた。情報技術（IT）の発展へ貢献をしてきた歴史があるが、現在のIT分野の状況の中で、今後どのような存在となるかが課題とされている。元々国連のユネスコの支援の下創設され、各国のメンバ学会の代表の集まりであるIFIPの総会（GA：General Assembly）は、毎年1回開催され、IT領域全体にかかわる多くの問題について議論が行われる。

2020年の総会は、本来9月にフランスのトゥールーズで開催し、その後、パリのユネスコで60周年イベントを開催する予定であった。しかし、新型コロナウイルス感染症のため、総会は初めてオンライン開催となり、60周年イベントは、来年度あらためて開催することとなった。

今回の総会には、各国のメンバ学会 代表者が28名、特別会員（International Members at Large）のACMおよびCLEIから2名、国代表ではない役員7名、技術委員会（Technical Committee: TC）の委員長13名、準会員（Affiliate Members）から1名、名誉会員2名の総勢53名の総会構成員のほか、オブザーバ4名、IFIP事務局1名が参加した。日本からは日本代表として今回から相田が、今回で任期満了となるIFIP副会長として前日本代表の村山氏が、オブザーバとして本会の木下事務局長が参加した。

これまで総会では多くの議題があり、十分な検討時間がとれなかった。このことから、昨年度より総会の前に開催される役員会でおおむね課題を検討し、その結果を総会初めに会長が報告するというスタ

イルで進められた。これにより、最重要課題を総会で議論することにした。今回はオンラインで時差なども考慮し、1日目は中央欧州時間（CET）で12:00～15:00、2日目は12:00～13:00と予定されていたが、1日目は予定を超え16:30に終了した。

## IFIP全般の状況

2020年9月時点の総会の構成員は次の通りである。IFIPのメンバ学会の数は昨年度と変わらず37、各国における国代表以外の特別会員はウクライナの1組織、国際的な特別会員としてACMおよび中米の組織CLEI（Centro Latinoamericano de Estudios en Informatica）の2組織が登録されている。このほか、準会員として4組織が登録されている。技術委員会は13あり、それぞれの委員長が総会メンバとなる。TCは1～14番まであり、4番は医療情報のTCであったが、独立して準会員のIMIA（International Medical Informatics Association）となったので、現在は欠番となっている。このほか、Ex Officio Memberと呼ばれる国代表ではない役員は7名、名誉会員が7名である。

メンバ学会については、2018年12月末に、ハンガリー、スペイン、デンマークの3カ国が脱退した。現在、タンザニア、ボツワナ、タイ、バングラデッシュの参加にむけて、努力している。一方、スウェーデンが今後の脱退を検討している。そのスウェーデン代表が、今回、副会長に選出されている。

## 規約改正

会長から4件の規約改正が諮られた。

1件目は総会メンバの投票権に関して定款 (Statute) 8.1 との間で長らく不整合があったことに関して規程 (Bylaw) 6.1.1 を修正するもので、投票の結果承認された。

2件目は同じく投票権の表に関して規程内での不整合を解消するため新たに規程 6.1.2 を追加するもので、投票の結果承認された。

3件目は規程 2.9 で会費支払いの遅れている会員に対して、従来はペナルティとして、総会での投票権のみ行使できないことになっていたのに対して、役員やカウンシラーへの被選挙権もなくすようペナルティを強化するもので、投票の結果承認された。

4件目は IFIP Fellow に関する規程 5.4 を全面改正するもので、定款 9 の取り決めに基づき総会の 40 日前に案が配付されたところ、Member Societies Assembly での議論も経てドイツの Rannenberg 氏から3点の修正提案がなされ、採決の結果、これらの修正を行った上で承認された。

改正後の規約類は IFIP Web ページの Rules & Forms から参照できる。

## 役員を選出

今回、役員については、任期満了の後任等について、投票が行われた。今回で退任する副会長村山優子氏の後任には、3名の候補から、スウェーデン代表の Jan Gulliksen 教授 (スウェーデン王立工科大学) が選出された。カウンシラー (Councillor) は、今期で任期満了 (1期3年で2期まで) となる Jerzy Nawrocki 教授 (ポーランド代表、ポズナン工科大学) および連絡がなく退任とみなされていた元スリランカ代表の Yasas Abeywickrama 氏の後任の2名の枠について、3名の推薦があり、TC9 Chair の David Kreps 教授 (英国、サルフォード大学) および TC14 Chair の Rainer Malaka 教授 (ドイツ、ブレーメン大学) が、選出された。

なお、退任役員は、村山氏のほか、財務担当の Declan Brady 氏 (アイルランド代表)、カウンシラーの Jerzy Nawrocki 教授の3名であった。これらの退任者には、感謝のトロフィーが授与された。

このほか、財務委員会の委員長代理として、Raimundo Macêdo 教授 (ブラジル代表、バイーア連邦大学)、技術委員会 (TC) の集まり TA (Technical Assembly) Chair には、TC13 Chair の Philippe Palanque 教授 (フランス、ポール・サバティエ大学) が任命された。新副会長の Jan Gulliksen 教授は、前 TC13 (Human-Computer Interaction) Chair なので、役員会のメンバに当該分野の関係者が増えたと捉えることもできる。

## 倫理綱領および行動規範

TC9 Chair の Kreps 氏から IFIP 倫理綱領 (Code of Ethics) 案について説明があり、投票の結果採択された。IFIP 倫理綱領は IFIP のメンバ学会の価値観を表現したものであり、ICT を専門的職業とする者が取るべき行動要請を示すものである。詳細は <https://www.ifip.org/images/stories/ifip/public/Announcements/code%20of%20ethics%20booklet.pdf> を参照されたい。

また、Honorary Secretary の Bramer 氏から IFIP の関係者が維持すべき行動の高い標準を掲げた IFIP 行為規範 (Code of Conduct for Officials) の案について説明があり、投票の結果採択された。また、IFIP の定款 5.5 として、この行為規範を参照する新たなパラグラフを設けることが投票の結果承認された。これらの条文は IFIP Web ページの Rules & Forms から参照できる。

## 表彰関係

IFIP 内での活動についての貢献者への The Service Award は、今回は、TC8 (Information Systems) から推薦された2名への授与が決定された。また、技術分野で顕著な功績を遺した IFIP 内

の技術委員会等の組織に属するメンバに与えられる IFIP Fellow Award には、14 名の候補者の中から 12 名の受賞者が決定された。これらの受賞者は、IFIP の Web ページで公開されている。

## 財務関係

2019 年度の収入総額は、31,660 ユーロでほぼ前年度同様で、予想を上回った。出版や国際会議などの活動からの収入増による。ただし、会費収入は相変わらず減少傾向にある。会費のディスカウント等のため 2018 年度より約 5 千ユーロの減収である。支出総額は、450,224 ユーロで、事務局経費が 65% を占めており、さらその 80% を人件費が占めている。昨年度を除いて、例年、赤字は予算よりも少ない。2019 年度は、予算上では 227,324 ユーロの赤字が計上されていたが、最終的に 139,555 ユーロの赤字にとどまった。これは、技術委員会経費が少なかったことや、予定されていた事務局の増員が延期されたことによる。赤字分については、資産の予想外の運用益により補填され、最終的には黒字としている。さらに、電子図書館やマーケティングの経費 27,296 ユーロは、資産運用益から補填している。

IFIP の資産運用は、従来、英国の UBS が運用してきたが、英国の EU 離脱に伴う UBS 側の方針変更により 2019 年 12 月で終了した。先述したとおり、最終年度の運用益は予想外の増益となった。現在、資産は、事務局が日々利用するオーストリア内の銀行にあり、預金利子しか得られない状況である。

このような状況下で、2020 年度は、各 TC の予算をいったん一律 30% カットした上で、TC の予算が不足したときに使うことができる TC Support Pool を設けることが提案されたが、TC 側から TC がこれまでに貯めた TC Fund は TC の自由に使えるはずだとの反発があり、TC Support Pool の金額を 30% 削減額と同額に増額する修正が提案され、承認された。いずれにしても、資産運用の補填がなければ、例年赤字となることが問題で、今後は、予算申請のための提出物の確認等、対策が必要となる。

2020 年度は、新型コロナウイルスの影響で、イベント収入が激減していることから、予測不能な状態である。さらに、このような状況下で 2021 年度については、どのように対応すべきかを、総会メンバからの提案を募っている。

## 出版関係

現在 IFIP Publication に対するオープンアクセスは、新 IFIP Digital Library (<https://hal.inria.fr/IFIP/>)、Springer Link (<https://link.springer.com>)、IFIP Select ([www.ifip.org/select](http://www.ifip.org/select))、旧 IFIP Digital Library ([dl.ifip.org/](http://dl.ifip.org/)) の 4 つのチャンネルで行われている。

新 IFIP Digital Library は 2010 ~ 2018 年の Springer からの出版物と 2019 年までの出版物へのリンク、それに最初の 3 冊の eCollection (Springer でない出版) が掲載されている。Springer からの出版については、Springer が著者コピーと著者の Web ページを除く 3 年間の排他的出版権を有しているため、最新の出版物については、目次が提示され、著者の原稿へのリンクと、Springer Link へのリンクが提示されている。前者は出版後 3 年経っていれば、一般の利用者が原稿を入手できる。一方、後者は Springer Link の加入者のみが論文を入手でき、一般の利用者は、出版後 4 年経った後、このリンク経由で論文を入手できる。

eCollection の掲載は論文あたり 10 ユーロであり、興味のあるイベントは事務局にコンタクトされたい。また、Algol 68 の本のような文書の置き場としても活用いただきたい。

TC6、とりわけ前 TC6 Chair の Aiko Pras 教授のボランティアにより、主に 2005 ~ 2012 年の proceedings を含む多くの IFIP 出版物が引き続き旧 Digital Library に置かれている。しかし、このライブラリには許諾・公表されているよりも多くの proceedings が置かれているため、旧 Digital Library の URL が新 Digital Library にリダイレクトされたとしても、これらの proceedings に対する

リンクは残さないといけないため、旧ライブラリから新ライブラリへの移行は予想していたより難航している。

Springer Link 内の IFIP 出版物は出版 4 年後から無料でアクセス可能となる。これは Springer との契約が続く限り有効で、1996 に IFIP と Chapman and Hall で契約した以降の出版物に適用される。

Retrodigitize された proceedings に関しては 4 年ではなく 3 年後に開放される。多くの古い proceedings は 2013 に retrodigitize されたので 2016 に利用可能となった。

Springer で出版された IFIP イベントの proceedings に関しては、50 部までの印刷したコピーを、送料を除き無料で受領することができる。ただし、注意すべきこととして、Springer はこれを一時的（通常イベントの 2 週間前から 2 週間後まで）な Springer Link への無料アクセスに変更しようとしている。すでに Springer はデフォルトの無料コピー数を 25 部に変更しており、残り 25 部は明示的に要求する必要がある。また、会議後に proceedings を発行する場合は会議後 9 カ月以内にファイルを送らないと無料の印刷物は得られない。

IFIP Select は IFIP の TC や WG (Working Group) で行われている優れた研究をより広める目的で、IFIP の会議録に掲載された論文のうち最も優れたものに対して、2～3 ページの解説ページを付け加えたものである。そこには解説ページと IFIP Digital Library または Springer Link などに置かれた元の論文へのリンクが格納されている。Springer との合意により、Springer Link に置かれた論文に関しても、年間 2 冊が 12 カ月間無料でアクセス可能である。

その他 TC3, TC11, TC14 の 3 つの TC が論文誌を発行している。

IFIP eCollection のような Springer を経由しない出版に関して、これまで Springer が行っていた IFIP テンプレートとの適合性や参考文献の適切性といった品質保証をどのように行っていくか、IFIP TA との間で議論中である。

## 各種委員会等報告

Member Societies Assembly, InterYIT, Professionalism Program (IP3), TA, モノのインターネットに関する領域委員会 (Domain Committee on Internet of Things), デジタルエクイティ委員会 (Digital Equity Committee) の各委員会から報告があった。なお、IP3 については、本号に別途報告がある。

## 会議開催予定

次回の役員会は、2021 年 3 月 23～24 日にベルリンで開催される予定。

次回総会は 2021 年 9 月にフランスで開催する予定だが開催都市は未定。

IFIP 60 周年イベントは 9 月 28 日に UNESCO を含む 2021 年 9 月 20～28 日にフランスで開催する方向で UNESCO に申し入れており、UNESCO から支援する旨回答を得ているが、具体的な日程に関する回答はまだない。

WCC (World Computer Congress) はインドが開催に興味を持っているが、現在の状況を鑑み延期の予定。

WITFOR (World Information Technology Forum) は具体的な計画はないが、新型コロナウイルス関係で会員に役立つイベント等をオンラインで開催する方向で会長の下にアドホック委員会を設けることとなった。

WCF (World CIO Forum) については、当面開催しない。

## その他

ACM の Gerrit van der Veer 氏から ACM が中心となって取りまとめた Computing Curricula 2020 (CC2020) を IFIP 総会として支持 (endorse) してほしいとの提案があり、総会参加者が内容を確認する時間を確保するため、総会終了後に電子投票にか

けられることになった。

#### 参考文献

- 1) 村山優子：IFIP—情報処理国際連合一近況報告，情報処理，Vol.61, No.3, pp.296-300 (Mar. 2020)。

## TC1 (Foundations of Computer Science)

代表：廣川 直(北陸先端科学技術大学院大学)

TC1は計算機科学の基礎に関する専門委員会である。2020年4月に国際会議ETAPS (European Joint Conferences on Theory and Practice of Software)にてWG chairを交えたTC1会合を開催する予定であったが、新型コロナウイルスの影響のためキャンセルされた。そのためビデオ会議システムによるオンライン会合を2020年10月5日に開催した。TC1が果たす役割を議題の中心に、発展途上国での若手研究者支援のためのサマースクール実施、基礎研究の社会における役割・最新の動向を社会へ発信する試案などが話し合われた。

TC1の学術活動主体は8つのWGにある。人事に関してはWG 1.2 (Descriptive Complexity)とWG 1.3 (Foundations of System Specification)でchairの改選があり、Martin Kutrib氏(ドイツ)とMarkus Roggenbach氏(イギリス)の再任と就任が決まった。日本からは山田晃久氏(産業技術総合研究所)がWG 1.6 (Rewriting)の新たなメンバとして加わった。2019年7月～2020年9月までの期間にTC1のWGが関与する国際学会開催が14計画されていた。しかし新型コロナウイルスのため2つは中止に、7つはオンラインでの実施となった。

## TC2 (Software Theory and Practice)

代表：五十嵐淳(京都大学)

2020年度のTC2会議は、Zoomを使って7月13日に開催された(当初はベルリンで開催される国際会議ECOOP (the European Conference on Object-Oriented Programming)に合わせて開催さ

れる予定だった)。昨年度改選があり、TC2 chairはドイツTU BraunschweigのIna Schaefer、vice-chairはドイツUniv. Duisburg-EssenのMichael GoedickeとオーストリアTU WienのStefan Biffl、secretaryはフランスInria/Sorbonne Univ.のJulia Lawallとなっている。会議の主な内容は次の通りである。(1)各WGのメンバに関して議論し、新しいWG Chairとして、WG 2.1: Peter Höfner (Australian National University), WG 2.3: K Rustan M Leino (Amazon Web Services), WG 2.6: Robert Wrembel (Poznan University of Technology), WG 2.15: Jim Woodcock, temporary (University of York)が承認された。また、11名の新しいWGメンバと1名の名誉メンバが承認され、12名が除名された。(2)Robert Wrembel氏がIFIP service awardを受賞した。(3)5月開催予定であったWG 2.13 International Conference on Open Source Systemsが延期の上、2021年1月開催予定(開催形式は検討中とのこと)であることが報告された。TC2のWebページ<https://ifip-tc2.paluno.uni-due.de/>

## TC3 (Education)

代表：斎藤俊則(星槎大学)

2020年のTC3定例カンファレンスOpen Conference on Computers in Education 2020 (OCCE 2020)は2020年1月6～8日にムンバイ市内(インド)のTata Institute of Social Scienceで開催された。Empowering Teaching for Digital Equity and Agencyの副題の元、合計で115名の参加者があり、51件の発表とスピーチがあった。また、この会合に合わせてTC3定例ミーティングが2020年1月8日および9日に開催された。このミーティングにてTC3 chairであったSindre Røsvikの6年間の任期が終了し、Don Passeyが新たなchairに就任した。

## TC5 (Information Technology Applications)

代表：村山優子(津田塾大学)

TC5は、情報技術のアプリケーションを支えるための基本概念、モデル、理論のほか、多様なアプリケーション等学際的な研究開発にかかわる。第60回年次会議は2020年11月9日に、コロナ禍のためオンラインで開催された。役員は、2期目のChairを務めるTadeusz Czachorski教授(ポーランド科学アカデミー Institute of Theoretical and Applied Informatics)、Vice Chairは、Erich J. Neuhold教授(ウィーン大学)とDimitar Velev教授(国立ソフィア総合経済大学)、幹事はPhilippe Dallemagne博士(スイス電子工学・マイクロナノテクノロジー・センター:CSEM)の体制である。今回、役員交代があり、Vice ChairのNeuhold教授は、任期満了に伴いGyörgy L. Kovacs博士(ハンガリー代表)の後任となった。また、従来、広報および出版・イベントについて、それぞれ異なる2名の担当者が割り当てられていたが、これらを統合し、新たにPeter Hehenberger教授(アッパーオーストリア応用科学技術大学, Wels校)が担当することとなった。

なお、2020年7月よりTC5日本代表を中野冠教授(慶應義塾大学)から村山が引き継いだ。

現在、11のWGが活動している。PLM(Product Life-cycle Management, 製品ライフサイクル管理)、画像処理、バーチャルエンタープライズ、生産システム、環境と情報通信技術等多様な課題に取り組む。現在、WG 5.8(Enterprise Interoperability)とWG 5.12(Architectures for Enterprise Integration)の統合が検討されているものの、反対意見もあり、なかなか進まない。

生産システムや生産管理システムにかかわるWG 5.7(Advances in Production Management Systems)には、前日本代表の中野教授を始め日本人メンバが12名登録されている。昨年度の中野教授のTC5報告(情報処理 Vol.61 No.3)にもあるとおり、IoT関連で国際連携に遅れた日本に代わり、

韓国からのメンバ、Moon教授(ソウル国立大学校)が、アジア太平洋州担当の副主査を務める。当該WGの国際会議APMS(Advanced Production Management System)は、2020年8月30日～9月2日に、現地の参加者のために予定通りセルビアで開催、海外からの参加者向けにはオンライン開催となり、ハイブリッド形式で実施された。なお、当該WGでは役員交代があり、新たにGregor von Cieminski氏(ハンガリー, ZF HUNGÁRIA KFT.)がChairとなった。

さらに、2020年6月には、新たに、災害情報処理(IT in Disaster Risk Reduction: ITDRR)のWG 5.15が立ち上げられた。これまでIFIP領域委員会として3年間活動してきたグループで、村山がChair、TC5役員のNeuhold教授とVelev教授がVice Chair等を務める。

2020年3月以降の各WGの国際会議は、おおむねオンラインで開催されている。なお、WG 5.10(Computer Graphics and Virtual Worlds)で、年次国際会議CyberWorldsの創設等の貢献をされた國井利泰会津大学初代学長(名誉教授)は、2020年11月3日に逝去された。謹んで故人のご冥福をお祈り申し上げる。

## TC6 (Communication Systems)

代表：相田 仁(東京大学)

2020年の第1回会合は、2020年5月22～26日にパリで開催されるIFIP Networkingの後に予定されていたが、新型コロナウイルスの影響でIFIP Networkingがオンライン開催に変更となったため、TC6会合も2020年7月15日にオンラインで開催されたが、50分ごとに接続が切れ、別のURLに再接続する形で実施された。オンライン開催に伴い、WG報告等は事前に資料を提供することで時間短縮が図られた。会合では主にIFIPとSpringerの間の契約が変更されたことをふまえて、今後のTC6のイベントにおける出版方針について意見が交換された。

TC6活動に関する懸念事項としては、イベント

への参加者の減少傾向が続いていること、IFIP から脱退する国があると次期役員選出の際にそれらの国の人を選出することができないことが挙げられている。

## TC7 (System Modelling and Optimization)

代表：櫻井鉄也(筑波大学)

TC7 Conference および TC7 meeting は隔年に開催され、2020 年がその定例開催年であり、第 29 回の TC7 Conference が、エクアドル共和国 Quito 内の Escuela Politecnica Nacional で開催される予定であった。同学の Juan Carlos 教授が主体となり、その運営について PC メンバの間で E-mail によって議論が行われてきた。南北アメリカから plenary speaker 5 名、その他から 4 名が選出されている。しかし、Covid-19 の影響で 2021 年 8 月 31 日～9 月 4 日に延期された。

傘下の WG について、TC7 はその設立・改廃の際にかかわるのみであり、各 WG はほぼ独立に各々の活動を続けている。会議期間中に行われる TC7 meeting において各 WG の活動の報告が行われるが、TC7 Conference や TC7 へのかかわりに対する積極さにも、各 WG の間に依然として違いがある。

## TC8 (Information Systems)

代表：内木哲也(埼玉大学)

TC8 は組織および社会での活動基盤である情報システム (Information Systems) の計画立案から、分析設計、開発、運用管理、利用評価、さらには組織設計や社会的評価までも含む、人間—技術システムのマネジメント全般を対象としている。2020 年は第 51 回 TC8 年次総会が IFIP-GA に合わせフランス共和国トゥールーズで開催予定であったが、コロナ禍の予定変更で 9 月 23～24 日に遠隔にて、9 カ国の代表委員と 6WG 代表委員の 19 名により開催された。今回は、遠隔で短時間の審議を余儀なくされたため、各 WG と継続中の TC8 の社会

貢献事業の活動状況についての審議が中心で、基本的に次年度も各活動を継続することで了承された。なお、改選となる Vice Chair は会期中に候補を絞れなかったが、現在 Janusz Kacprzyk (Polish NR) と Jolita Ralyté (Switzerland\_NR) の 2 名が候補となり、遠隔投票の実施中である。今回は 2021 年 8 月 26～27 日に遠隔で、2022 年は欧州情報システム国際会議 ECIS の前後にルーマニア共和国にて開催の予定。

## TC9 (ICT and Society)

代表：小向太郎(中央大学)

TC9 (ICT and Society) は、隔年でシンポジウム HCC (Human Choice and Computers) を開催しているほかに、10 の WG を設置して活動を行っている。TC9 の 2020 年度の年次会合は、7 月 27 日にオンラインで行われ、HCC や WG の活動について議論した。この数年取り組んできた WG 再編の効果が確認された。なお、TC9 Chair の David Kreps が中心となって取りまとめた倫理指針 (IFIP Code of Ethics and Professional Conduct) が、2020 年 9 月の IFIP General Assembly において承認されている。

HCC (第 14 回) は、「データ駆動型社会における人間主体のコンピュータ利用」をテーマに、2020 年 9 月に東京の中央大学市谷田町キャンパス (中央大学 iTL) で開催される予定であったが、新型コロナウイルスの影響で中止となり、投稿された論文は電子書籍として Springer から出版することになった。2022 年の HCC (第 15 回) は、中央大学市谷田町キャンパスで実施する予定である。

## TC10 (Computer Systems Technology)

代表：金川信康(日立製作所)

TC10 はコンピュータシステムの技術、すなわち各階層における設計・評価技術とその概念、方法論、ツールに関する情報交換と協調促進を目的としてい

る。執行部は2019年より Chair: Paolo Prinetto (イタリア代表), Vice Chair: Achim Rettberg (ドイツ代表) 以下21名のメンバから構成されている。

2020年度のTC10会議は6月9日にオンラインで開催され、近年低迷気味であるTC活動を活性化(revitalizing)させる方法(メンバ名簿の再確認、年2回の会議開催等)について話し合われた。

TC10は10.2 - Embedded Systems, 10.3 - Concurrent Systems, 10.4 - Dependable Computing and Fault Tolerance, 10.5 - Design and Engineering of Electronic Systemsの4つのWGより構成されている。

WG 10.2は60名のメンバにより構成されているが日本からの参加がないことが今後の課題である。

WG 10.3のメンバは57名で、日本からは4名参加している。本会ではシステムソフトウェアとオペレーティング・システム研究会が分野としては関連している。

WG 10.4は63名のメンバから成り、日本から5名参加している。このほかに20名(内2名は日本国籍)の名誉メンバがいる。電子情報通信学会のデペンダブルコンピューティング研究会が連携している。本会ではコンピュータセキュリティ研究会が分野として関連しており、実質的な連携活動の可能性について話し合っている。

WG 10.5は49名のメンバに加えて8名の名誉メンバを擁し、日本からは3名のメンバと1名の名誉メンバが参加している。本会ではシステムとLSIの設計技術研究会が活発に連携している。

#### TC11 (Security and Privacy Protection in Information Processing Systems)

代表：越前 功(国立情報学研究所)

TC11は情報セキュリティに関連する分野を取り扱うTCである。TC11の活動は全体活動とWG活動に分かれており、全体活動ではTC11の運営を決める年次ミーティングと国際会議SEC(International Information Security Conference)を開催している。WG活動では各WGが国際会議

やワークショップ等を開いている。

今回のSEC2020は、35回目となり、新型コロナウイルスの蔓延のため、5月に予定されていた会議を、オンラインで2020年9月21～23日の3日間に開催された。今回は、TC11スロベニア代表のTatjana Welzer教授(マリボル大学)が組織委員長となり、TC11元Chairで現IFIP副会長のKai Rannenberg教授(ドイツ, ヨハン・ヴォルフガング・ゲーテ大学)とマリボル大学のMarko Hölbl教授がプログラム委員長を務めた。

例年通り、SEC2020に先立ち9月20日にTC11の年次委員会がオンラインで開催された。会議は、グリニッジ標準時で10時～13時までで開催された。例年は終日行われるが、今回は時差のある中でオンライン開催のため、短い会議となった。来年のSEC2021は、ノルウェーのオスロで2021年6月22～24日に開催予定である。TC11ノルウェー代表Audun Jøsang教授(オスロ大学)が中心となり準備中である。

TC11では、現在14のWGが活動している。

#### TC12 (Artificial Intelligence)

代表：栗原 聡(慶應義塾大学)

TC12は1989年に設立され、現在、Ulrich FURBACH教授(コブレンツ＝ランダウ大学, ドイツ)がChairを務めている。AI(人工知能)全般をカバーしており、現在33カ国が参加し、Knowledge Representation and Reasoning, Machine Learning and Data Mining, Intelligent Agents, Web Semantics, Artificial Intelligence Applications, Knowledge Management, Social Networking Semantics and Collective Intelligence, Intelligent Bioinformatics and Biomedical Systems, Computational Intelligence, の9つのWGが運営されている。

## TC13 (Human-Computer Interaction)

代表：北村喜文(東北大学)

Human-Computer Interaction の分野を担当する TC13 の各国代表が集まる全体会議は、当初 2020 年 3 月にイタリアのミラノで開催される予定であったが、世界的に新型コロナウイルス感染が拡大し始めたためにキャンセルされ、6 月 22 日にオンラインで開催された。そこで TC13 Chair の選挙が行われ、これまで Chair を務めてきた Philippe Palanque (フランス・Toulouse 3 大学教授) が 2 期目 (最終) の Chair を継続することが満場一致で決まった。次回の全体会議は、2020 年内に欧州で開催される予定の国際会議に合わせて何とか対面またはハイブリッド形式で開催したいと調整中である。

TC13 主催の国際会議 INTERACT (International Conference on Human-Computer Interaction) は隔年開催であるが、今回はイタリアのバーリで 2021 年 8 月 30 日～9 月 3 日に開催される (<http://www.interact2021.org/>)。論文投稿の締め切りは 2021 年 1 月 20 日である。

IFIP TC13 の詳細は、Web ページ <http://ifip-tc13.org/> 参照のこと。

## TC14 (Entertainment Computing)

代表：星野准一(筑波大学)

TC14 は、2002 年 SG16 (Specialist Group on Entertainment Computing, Chair: 中津良平氏) として出発し、設立以来 5 年が経過した 2006 年 8 月にチリ、サンチャゴで行われた IFIP 総会において、TC への昇格が認められ、TC14 として活動を開始することとなった。中津氏の Chair の任期が終了したので、2012 年度に 2002 年より Vice Chair を務めていた Matthias Rauberberg 氏 (オランダ) が Chair に選出された。

2019 年から Rainer Malaka 氏 (ドイツ) が Chair を担当しており、Vice Chair は Letizia Jaccheri 氏

(ノルウェー)、Esteban Clua 氏 (ブラジル)、星野准一 (日本) である。中津良平氏は WG 14.3 の Chair また星野は WG 14.4 Entertainment Games の Chair を兼任している。

昨年 1 年間の TC14 の構成員の変更・主たる活動は以下の通りである。

- (1) TC14 の主催する国際会議 ICEC2020 の開催準備を進めている。
- (2) 2020 年 9 月時点で TC14 の国際委員の数は 26 名、WG の数は 10 である。

## IP3 (International Professional Practice Partnership)

代表：掛下哲郎(佐賀大学)

IP3 は、各国の高度 IT 人材資格制度を認定することにより、世界の IT 専門家の強化に資することを目的としている。本会は、IP3 の活動が認定情報技術者 (CITP) 制度の確立に有意義と考え、2009 年 6 月より参加し、ボード・メンバを務めている。参加団体は、オーストラリア ACS、南アフリカ共和国 IITPSA、カナダ CIPS、日本 IPSJ、ニュージーランド IITPNZ、ジンバブエ CSZ、韓国 KIISE、エジプト ITI、スリランカ CSSL、オランダ NGI/VRI、スイス SI の 11 学会と、IIBA、ISACA の 2 協会である。

現在、IP3 は IT 技術者が遵守すべき倫理綱領・行動指針の検討を主に推進している。

本会は、1～2 カ月ごとに開催されるオンライン会議による理事会への出席に加え、ML を活用して各種の活動を行った。現在、本会ではデータサイエンティスト資格に関する検討およびデータサイエンス分野における大学専門教育レベルの標準カリキュラムの策定を進めているため、IP3 に対しても進捗状況の報告を行っている。また、ISO/IEC JTC1/SC7/WG20 にて ISO/IEC 24773 の改訂作業が山場を迎えているので、関連する情報提供も行っている。

**TC1 : Foundations of Computer Science**

- WG 1.2 Descriptive Complexity
- WG 1.3 Foundations of System Specification
- WG 1.5 Cellular Automata and Discrete Complex Systems
- WG 1.6 Rewriting
- WG 1.7 Theoretical Foundations of Security Analysis and Design
- WG 1.8 Concurrency Theory
- WG 1.9 Verified Software (joint with WG 2.15)
- WG 1.10 String Algorithmics & Applications

**TC2 : Software : Theory and Practice**

- WG 2.1 Algorithmic Languages and Calculi
- WG 2.2 Formal Description of Programming Concepts
- WG 2.3 Programming Methodology
- WG 2.4 Software Implementation Technology
- WG 2.5 Numerical Software
- WG 2.6 Database
- WG 2.7 User Interface Engineering (joint with WG 13.4)
- WG 2.8 Functional Programming
- WG 2.9 Software Requirements Engineering
- WG 2.10 Software Architecture
- WG 2.11 Program Generation
- WG 2.13 Open Source Software
- WG 2.14 Service-Oriented Systems (joint with WG 6.12/8.10)
- WG 2.15 Verified Software (joint with WG 1.9)
- WG 2.16 Programming Language Design

**TC3 : Education**

- WG 3.1 Informatics and digital technologies in School Education
- WG 3.3 Research into Educational Applications of Information Technologies
- WG 3.4 Professional and Vocational Education in ICT
- WG 3.7 Information Technology in Educational Management

**TC5 : Information Technology Applications**

- WG 5.1 Global product development for the whole life-cycle
- WG 5.4 Computer Aided Innovation
- WG 5.5 Cooperation infrastructure for Virtual Enterprises and electronic business (COVE)
- WG 5.7 Advances in Production Management Systems
- WG 5.8 Enterprise Interoperability
- WG 5.10 Computer Graphics and Virtual Worlds
- WG 5.11 Computers and Environment
- WG 5.12 Architectures for Enterprise Integration
- WG 5.13 Bioinformatics and its Applications
- WG 5.14 Advanced Information Processing for Agriculture
- WG 5.15 Information Technology in Disaster Risk Reduction (ITDRR)

**TC6 : Communication Systems**

- WG 6.1 Architectures and Protocols for Distributed Systems
- WG 6.2 Network and Internetwork Architectures
- WG 6.3 Performance of Communication Systems
- WG 6.6 Management of Networks and Distributed Systems
- WG 6.8 Mobile and Wireless Communications
- WG 6.9 Communication Systems in Developing Countries
- WG 6.10 Photonic Networking
- WG 6.11 Communication Aspects of the e-World
- WG 6.12 Service-Oriented Systems (joint with WG 8.10/2.14)

**TC7 : System Modelling and Optimization**

- WG 7.2 Computational Techniques in Distributed Systems
- WG 7.3 Computer System Modeling
- WG 7.4 Inverse Problems and Imaging
- WG 7.5 Reliability and Optimization of Structural Systems
- WG 7.6 Optimization - Based Computer Aided Modeling and Design
- WG 7.7 Stochastic Control and Optimization
- WG 7.8 Nonlinear Optimization

**TC8 : Information Systems**

- WG 8.1 Design and Evaluation of Information Systems
- WG 8.2 The Interaction of Information Systems and the Organization
- WG 8.3 Decision Support
- WG 8.4 E-Business Information Systems: Multi-disciplinary research and practice
- WG 8.5 Information Systems in Public Administration
- WG 8.6 Transfer and Diffusion of Information Technology

- WG 8.9 Enterprise Information Systems
- WG 8.10 Service-Oriented Systems (joint with WG 6.12/2.14)
- WG 8.11 Information Systems Security Research (joint with WG 11.13)
- WG 8.12 Industrial Information Integration

**TC9 : ICT and Society**

- WG 9.1 Computers and Work
- WG 9.2 Social Accountability and Computing
- SIG 9.2.2 Special Interest Group on Framework on Ethics of Computing
- WG 9.3 Intelligent Communities
- WG 9.4 The Implications of Information and Digital Technologies for Development
- WG 9.5 Our Digital Lives
- WG 9.6 Information Technology: Misuse and The Law (joint with WG 11.7)
- WG 9.7 History of Computing
- WG 9.8 Gender, Diversity and ICT
- WG 9.9 ICT and Sustainable Development
- WG 9.10 ICT Uses in Peace and War

**TC10 : Computer Systems Technology**

- WG 10.2 Embedded Systems
- WG 10.3 Concurrent Systems
- WG 10.4 Dependable Computing and Fault Tolerance
- WG 10.5 Design and Engineering of Electronic Systems

**TC11 : Security and Privacy Protection in Information Processing Systems**

- WG 11.1 Information Security Management
- WG 11.2 Pervasive Systems Security
- WG 11.3 Data and Application Security and Privacy
- WG 11.4 Network & Distributed Systems Security
- WG 11.5 IT Assurance and Audit
- WG 11.6 Identity Management
- WG 11.7 Information Technology: Misuse and The Law (joint with WG 9.6)
- WG 11.8 Information Security Education
- WG 11.9 Digital Forensics
- WG 11.10 Critical Infrastructure Protection
- WG 11.11 Trust Management
- WG 11.12 Human Aspects of Information Security and Assurance
- WG 11.13 Information Systems Security Research (joint with WG 8.11)
- WG 11.14 Secure Engineering

**TC12 : Artificial Intelligence**

- WG 12.1 Knowledge Representation and Reasoning
- WG 12.2 Machine Learning and Data Mining
- WG 12.3 Intelligent Agents
- WG 12.5 Artificial Intelligence Applications
- WG 12.6 Knowledge Management
- WG 12.7 Social Networking Semantics and Collective Intelligence
- WG 12.9 Computational Intelligence
- WG 12.10 Artificial Intelligence & Cognitive Science
- WG 12.11 AI for Energy & Sustainability (AIES)

**TC13 : Human-Computer Interaction**

- WG 13.1 Education in HCI and HCI Curricula
- WG 13.2 Methodologies for User-Centered Systems Design
- WG 13.3 Human Computer Interaction, Disability and Aging
- WG 13.4 User Interface Engineering (joint with WG 2.7)
- WG 13.5 Human Error, Resilience, Reliability, Safety and System Development
- WG 13.6 Human-Work Interaction Design
- WG 13.7 Human - Computer Interaction & Visualization (HCIV)
- WG 13.8 Interaction Design and International Development
- WG 13.9 Interaction Design and Children
- WG 13.10 Human-Centered Technology for Sustainability

**TC14 : Entertainment Computing**

- WG 14.1 Digital Storytelling
- WG 14.2 Entertainment Robot
- WG 14.3 Theoretical Foundation of Entertainment Computing
- WG 14.4 Entertainment Games
- WG 14.5 Social and Ethical Issues in Entertainment Computing
- WG 14.6 Interactive TeleVision
- WG 14.7 Art and Entertainment
- WG 14.8 Serious Games
- WG 14.9 Game Accessibility
- WG 14.10 Sound and Music Computing

## 創立 60 周年記念事業：実施概要報告

創立 60 周年記念事業実行委員会  
委員長 江村 克己

創立 60 周年記念事業は、学会創立 60 周年を記念して、情報処理にかかわる学界、教育界、産業界をはじめとするすべての方々が明日の情報社会に関する夢を持って議論する契機もしくは里程碑となることを願って、第 629 回理事会（2018 年 6 月）において①記念全国大会、②記念会誌、③記念論文、④ 60 年のあゆみ出版、⑤記念出版、⑥記念式典、以上 6 つの事業の実施を決定いたしました。

以降、それぞれの事業は、記念事業実行委員会ならびに各事業実施委員会のもとで推進され、今年度末をもって記念事業としての推進は終了いたします。各記念事業の実施内容につきましては、当会 60 周年記念事業サイト (<https://www.ipsj.or.jp/60anv/index.html>) に掲載をさせていただいておりますのでご参照ください。

折しも本会創立 60 周年にあたる 2020 年、世界中を襲った新型コロナウイルス感染症 (COVID-19) の影響により、当初 2020 年 10 月末に開催を予定しておりました記念式典は、感染防止の観点から開催を断念せざるを得ない結果となりましたが、本会の還暦にあたるこの 60 周年、またこれからのニューノーマル社会に向けてメモリアルメッセージを後世に残しておくことは当会の使命であり、急遽「学会創立 60 周年記念週間」を企画し 11 月下旬にメモリアル Web ページを公開させていただきました。また、記念週間期間中に福田敏男 IEEE 会長をお招きし、創立 60 周年記念講演を実施いたしました。

この報告では、特にメモリアルページに掲載の「情報処理学会創立 60 周年宣言」ならびに 2020 年 10 月 30 日に行われた創立 60 周年記念パネル討論「情報社会の未来を拓く：情報技術と学会の過去、現在、未来」の概要と受賞記念論文についてご報告いたします。

最後になりますが、この度の記念事業遂行にあたっては、会員皆様をはじめ関係皆様のご多大なるご支援・ご尽力に対しまして、ここに深く感謝申し上げます。

### 1. 情報処理学会創立 60 周年宣言

2019 年 12 月に武漢で発生した新型コロナウイルス (COVID-19) は現在も猛威をふるっており、世界的に最重要かつ喫緊の課題はコロナ感染症防止と経済活動の両立です。また、コロナ禍の先には、特に日本では少子高齢化や過疎化をはじめとする長期的な課題が待ち受けています。

これらの困難な社会課題を解決するには、多様な当事者とともに課題に取り組むローカルな活動が求められます。たとえば、コロナ禍を機に各地域の公的機関のデジタル革新を進めるために最初にすべきは、地域が抱える課題を地域の担い手である市民と共有することです。また、産業／医療介護／少子化対策等多様な分野における課題を解決するには、それぞれの分野の担い手とともに分野固有の課題に取り組まなくてはなりません。情報処理は、これら課題を解決するための強力なツールとして、次の深みへと深化し、社会へ受け入れられる必要があります。そのためには、情報処理の最先端の新しい領域を開拓し続ける創造力と、多様な人々を繋ぐ場と情報に関する学びの場を社会全体に対して提供す

る推進力が求められます。

そして、各地域における多様な活動を通して得られた課題解決のプラクティスは、ローカルにとどめてはなりません。普遍化し発信することにより、グローバルに通ずる新価値創造に繋げていきます。

60 周年の節目にあたり、国内に根ざす学会として我々が目指すところを以下に宣言します。

- (1) 情報社会において各地域や各分野の担い手とともに先端技術で社会課題を解決し、そのプラクティスをグローバルに通ずる新価値創造に繋げる
- (2) 情報処理の最先端を先導する学会として常に新しい領域の開拓と人材ネットワークの構築に寄与する
- (3) 情報に関する学びの場を提供し、生涯にわたる個々人の成長に寄与する

### 2. 創立 60 周年記念パネル討論

「情報社会の未来を拓く：情報技術と学会の過去、現在、未来」

日時／会場：2020 年 10 月 30 日 (金) 14:00 ～ 16:30

明治記念館

第 1 部 14:00 ～ 15:00, 第 2 部 15:30 ～ 16:30

第 1 部では、歴代の会長をパネリストとしてお招きし、「学会のこれまでの振り返りと今後の展開」をテーマに議論が行われ、積極的に失敗をしてほしい、新しい芽、論文が書きにくいテーマに光をあててほしいなどの今後の学会に対する期待を語っていただきました。第 2 部では、多方面でご活躍の著名な方々をパネリストとしてお招きし、「これからの学会のデザイン」をテーマに、学会の外からの視点を取り入れた多様な議論が繰り広げられました。ダイバーシティの推進、学会の価値は研究の第三者評価を示すことなどのこれからの学会の在り方に対する意見が述べられました。最後にパネリストの方々よりみんなに開かれた学会になってほしいとのエールをいただき、パネル討論を終了しました。



パネル討論参加者

敬称略 (左から富田、喜連川、笠原、福田、江村、白鳥、落合、田島、古川)

- (1) 第 1 部：学会のこれまでの振り返りと今後の展開

司会：江村克己 (情報処理学会 会長／日本電気 NEC フェロー)

パネリスト：

白鳥則郎 (情報処理学会 第 25 代会長／東北大学 名誉教授)

古川一夫 (情報処理学会 第 26 代会長／日本ガイシ 取締役, パソナグループ取締役)

喜連川優 (情報処理学会 第 27 代会長／国立情報学研究所 所長／東京大学 教授)

富田達夫 (情報処理学会 第 28 代会長／情報処理推進機構 理事長)



### 「積極的に失敗をしてほしい」

まず、世の中の速い動きに学会の提言が追いついていないという司会からの問題提起に対して議論がなされました。学会は多くの提言をしているが、もっと主体で動くべきであり、まずやってみればそれを小中高や地方の大学、企業が真似できるとの意見をいただきました。また、日本は一度失敗すると再度立ち上がるのが難しい風土があるので、失敗事例を披露してそれをリカバーできる環境を作ってほしいとの意見や、もっとタイムリーに学会員の誰もが発信できる環境を作ってほしいなどの意見をいただきました。

### 「新しい芽、論文が書きにくいテーマに光を」

次に、論文が書ける領域が偏っている中、従来の価値観を超えた次のチャレンジがどこにあるのかという司会からの問いかけに対し議論が行われました。論文の採択率だけで評価するのではなく、変わった研究をやっている人を育て、OSや基盤など地味なところを頑張っている人を評価し、研究のダイバーシティを高めるために、ここに力を入れてほしいと大学に発信すべきであるとの意見をいただきました。また、外から見て学会が面白い議論をしているコミュニティに見えるようになってほしいとの期待や、論文特集号では、評価が不十分でも面白いものを採択すべきであるなどの議論がなされました。



パネル討論第1部参加者  
敬称略（左から江村、白鳥、古川、喜連川、富田）

### (2) 第2部：これからの学会のデザイン

司会：江村克己（情報処理学会 会長／日本電気 NEC フェロー）

パネリスト：

笠原博徳（IEEE Computer Society 2018 会長／早稲田大学 副総長）

福田敏男（IEEE 2020 会長／名城大学 教授／早稲田大学 特命教授）

田島 玲（Yahoo! JAPAN 研究所 所長）

落合陽一（筑波大学 准教授／CEO of Pixie Dust Technologies, Inc）

### 「ダイバーシティの推進」

コミュニティ、ヒューマンネットワークを形成する場であることが学会の肝であり、ダイバーシティの中からアイデアが生まれてくるとの認識から、トップのレベルアップとともに、裾野を広げていくことが大事であるとの議論がなされました。また、ローカルならではの圧倒的触り感や祝祭性を実現していくためには、発信の仕方は論文だけではなく、デモ、ビデオなどの形でもよいことや、研究者以外の人とどう対話するかが大事であるなどの議論がなされました。若い人が社会のニーズを産業界の人と触れ合うことで地球の将来のために研究していると思える場になってほしいなどの意見もいただきました。

### 「学会の価値は第三者評価」

研究成果を発信して的確なフィードバックを得る場合は学会以外にはなく、本会が選別した論文はためになるものであると保証することが学会の価値であるとの意見から、クオリティの高いものを選定する、信頼できるレビューの仕組みを作ってしまうばよいなどの議論がなされました。



パネル討論第2部参加者  
敬称略（左から江村、福田、笠原、田島、落合）



- Towards a Complete Perspective on Labeled Tree Indexing: New Size Bounds, Efficient Constructions, and Beyond  
Shunsuke Inenaga (Kyushu University)

### <概要>

A labeled tree (trie) is a compact representation of a set of strings. This paper considers the labeled tree indexing problem, and provides a number of new results. Kosaraju [FOCS1989] proposed the suffix tree for a backward trie, where the strings in the trie are read in the leaf-to-root direction. We call a usual trie as a forward trie. Despite a few works after Kosaraju, indexing forward/backward tries is not well understood yet. We show a full perspective on the sizes of indexing structures such as suffix trees/arrays, DAWGs, and CDAWGs, for forward and backward tries. Some of them take  $O(n)$  space in the size  $n$  of the input trie, while the others can occupy  $O(n^2)$  space. Further, we show that there is a compact  $O(n)$ -space implicit representation of the DAWG for a forward trie, whose naive representation requires  $O(n^2)$  space. This compact representation allows for simulating each DAWG edge traversal in  $O(\log \sigma)$  time, and can be constructed in  $O(n)$  time and space over any integer alphabet of size  $\sigma = O(n)$ . This readily extends to the first indexing structure that permits bidirectional pattern searches over a trie within linear space in the input trie size.

Info-WorkPlace 委員会企画「お届けInfo」

# 第83回全国大会にて“デリバリー”始めます!

坊農真弓 | Info-WorkPlace 委員会委員長 / 国立情報学研究所

**お届けInfo**とは、学会で発表されたできたてのほやほやの情報や知識を、有志の取材をしてくださる会員（以下、デリバリー会員）がその場の臨場感とともに、学会会員の皆さま（以下、カスタマー会員）のお手元にお届けするサービスです。家族のイベントで参加できない、家族の病気やさまざまな事情があつて参加できない……。このようなカスタマー会員のアクセシビリティを確保します。

※今回のデリバリーは抽選とさせていただきます。抽選結果はデリバリーの発送をもってかえさせていただきます。

## オンライン業務で大忙し編



第83回情報処理学会 全国大会 イベント企画

## お届けInfo

2021年3月18日(木) - 20日(土)



### スケジュール

- オーダー募集期間：大会プログラム開示から2021年2月末まで
- 大会期間：2021年3月18日(木)-20日(土)  
デリバリー：当該イベント実施後から大会期間終了まで  
note掲載：大会期間終了後3ヶ月以内

このイベントを企画している Info-WorkPlace 委員会は、ダイバーシティ社会を活性化するために育児中・介護中といった様々なライフイベントの只中にある会員をサポートする活動に取り組んでいます。

デザイン：木塚あゆみ





## 会議レポート

# Recsys 2020 参加報告

### Recsys の概要と実施形態

Recsys (ACM Conference on Recommender Systems) は情報推薦を専門に扱う国際会議である。2020 年は 9 月 22 日から 26 日まで本来であればブラジルのリオデジャネイロで開催予定であったが、COVID-19 の影響によってオンラインでの開催となった。参加者数は 1,168 名と過去最高となっており、例年どおり学術:産業で 36%:64% と産業側の参加者が多い。5 日間の会期中で最初の 3 日間が本会議、4 日目と 5 日目が Workshop と Tutorial に割り当てられている。本会議では Keynote が各日 1 件ずつ実施される。発表区分としては研究論文である Long Paper と Short Paper に加え、過去の研究の再現に焦点を当てた Reproducibility Paper, Demo, 新しい結果を報告する Late-Breaking Results, 産業界での取り組みを紹介する Industrial Talk がある。オーラルセッションではすべての Long Paper, Reproducibility Paper, Industrial Talk, そして少数の Short Paper の発表が実施され、それ以外はポスターセッションでの発表となった。Industrial Talk では Netflix, Amazon といったおなじみの企業に加えて、家具量販店の IKEA からの発表、そして (株) サイバーエージェントの子会社であるマッチングエージェントが提供するマッチングサービスである「タップル誕生」に関する発表を SBX Technologies と合同で行っていた。投稿総数はここ数年と大きく変わらなかったものの、Long Paper の比率がこれまでより 10% ほど増える結果となっていた。採択率

は Long Paper 18%, Short Paper 20% であり、日本からの採択は 4 件であった。ほかの発表区分に関しては採択率は未公表である。

図 -1 に示すように、プログラムはオンライン開催の中で 1 つのセッションが 2 回実施されるという、筆者の知る限りでは独自の形式であった。これは参加者が時差にかかわらず発表の議論に参加できる機会を平等に提供することを目的としており、たとえば日本時間の深夜 1 時からのセッションは日本時間の正午 12 時から実施されている。Recsys は以前もオーラルセッションはシングルセッションのみで行うなどコミュニティとして活発に議論を行うことを目指しており、この工夫にもそうしたコンセプトが感じられた。発表者は両方のセッションに参加し発表と質疑を行う。これにより参加者は自分のタイムゾーンに合った時間にセッションに参加することができる。ほかの学会では開催地のタイムゾーンに合わせて生活することを余儀なくされるが、Recsys ではこの工夫により日本時間で生活しながらすべての発表に参加することができた。発表者としても発表する 2 つのセッションもタイムゾーンが考慮されており特に不便を感じることはなく、2 回とも議論が活発に行われ非常に有意義であった。このように参加者が活発に議論を行うための工夫がなされているのが、Recsys の特徴だと感じる。

### 研究トピック

以下、個人的に注目したトピックとしてバイアスを扱った研究とユーザ心理を扱った研究について紹介する。いずれも推薦システムのサービスにおける評価に大きくかわるトピックであるといえる。

### 推薦システムにおけるバイアス

コミュニティ全体としてはバイアスへの注目の高まりを強く感じた。第 1 の Keynote はインディアナ大学の Filippo Menczer 氏による「4 Reasons Why Social Media Make Us Vulnerable to Manipulation」であり、ソーシャルメディアにおけるバイアスに関する講演で、フェイクニュースの拡散やエコーチェンバー現象などプラットフォームの

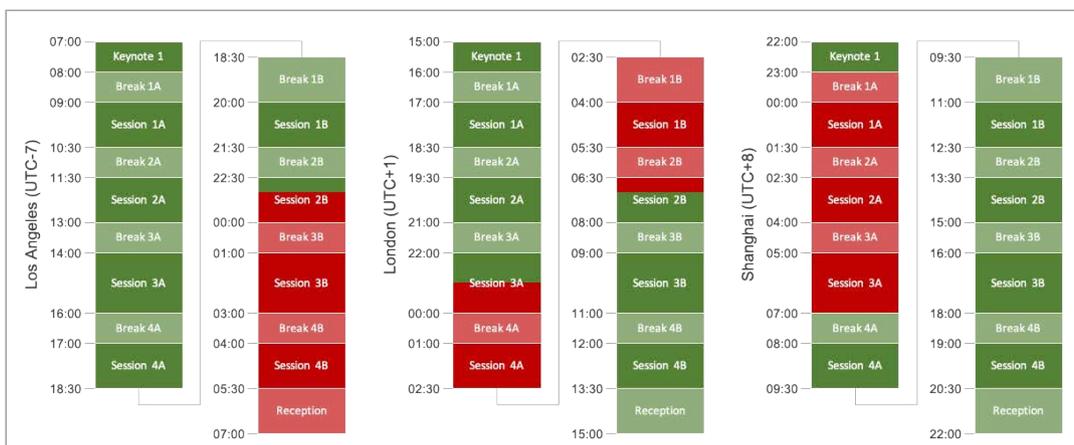


図 -1  
各タイムゾーンごとの会議スケジュール  
参照元：  
<https://recsys.acm.org/recsys20/online-format/>

特性や推薦システムとのかかわりについて議論されていた。第2のKeynoteは元Yahoo! LabのVice PresidentであるRicardo Baeza-Yates氏による「Bias in Search and Recommender Systems」であり、推薦システムのアルゴリズムや評価プロセス自体に含まれるバイアスについて広く議論されていた。研究トラックでも評価やバイアスに関する発表が多く、チュートリアルや、Workshopでも数多くのトピックで扱われていた。注目の高まりを感じるとともに、個人的にはバイアスという言葉がかなり大きな意味を持つようになってきていることを懸念している。研究トピックや研究者によってバイアスという言葉の意味や、研究目的にばらつきがあると感じており、このあたりの整理が今後行われていくことを期待したい。

## ユーザ心理を考慮した推薦システムの分析と評価

もう1つのKeynoteにおけるChatbotプラットフォームを提供しているJuji, incのCEOであるMichelle Zhou氏による「"You Really Get Me": Conversational AI Agents That Can Truly Understand and Help Users」は心理学の知見を推薦システムに活用することについて対話型推薦システムの事例を中心に議論していた。特に個性(Personality)に焦点を当て、個性の定義、推定、活用について心理学研究における伝統的な定義や知見をまとめ、推薦システムにおける活用の事例について紹介していた。心理学の側面から推薦システムについて論じる研究にはこれまであまり触れてこなかったが、特に最後に紹介されていたACM Transactions on Interactive Intelligent Systems, Volume 10, issue 3における特集「Data-Driven Personality Modeling for Intelligent Human-Computer Interaction」には興味深い内容が多く、こうしたトピックに関心を持たれた方はぜひ一読することをおすすめする。

Industrial TalksでのNetflixによる「A Human Perspective on Algorithmic Similarity」もユーザ心理を考慮した発表であったといえる。代表著者のSchendel氏は認知心理学の博士号を持つNetflixのUX Research Directorを務める人物であり、計算機科学研究者と異なった視点での分析が非常に興味深いものであった。この発表は推薦システムにおける「類似性」とはなにかをさまざまな角度から検証したものである。彼らは検証の結果、類似性は「the Placement」、「the Person」、「the Context」の3つによってその役割や重要性が変化すると述べている。the Placementは推薦が配置される場所によって類似性の意味合いが変わることを指しており、たとえばあるアイテムを消費した後に異なるアイテムを推薦する場合、1つのアイテムを推薦する場合と、複数のアイテムを推薦する場合では1つのアイテムを推薦する場合のほうがユーザからの類似性に対する期待値は高いということが示されている。またトップページにおける推薦より、作品再生後に表示され

る推薦である「More Like This」や検索結果など、ユーザの特定のアクションに対する推薦のほうが類似性に対する期待値は高い。the Personは類似性はユーザの知識や背景によって異なるということを示す。アイテム同士の類似性を測る際に「broad driver」と「specific driver」という2種類の特徴を導入する。broad driverは「SF」「ホラー」などのような表層的な特徴で、だれもがその特徴が一致していれば類似していると感じるような特徴である。一方でspecific driverは主演の俳優や監督が共通といった類似性を判断するのに一定の知識が必要である特徴や、「懐かしい」などユーザの感情に基づいた特徴を示す。specific driverはユーザごとに異なるため、うまく推薦できたときはユーザの満足度を強化することができるが、外した場合には推薦システムへの信頼を失う恐れがある。最後のthe Contextは推薦を受け取る時のユーザの状態に類似性は依存することを指している。1つ目のthe Placementもユーザの状態であるといえるが、こちらはサービス外における状態や過去の消費アイテムなど、サービスのインターフェースの外の情報に焦点を当てている。例としてある恋愛リアリティショーを見たユーザが次に行った行動を紹介している。直感的には多くのユーザが続きや同種の作品を消費しそうに感じるが、ほかの恋愛リアリティショーを続けて見たユーザは18%しかおらず、55%のユーザがその作品の続きをそのまま見なかったと報告している。この要因にはユーザの状態が関係していると推測しており、たとえば時間がないからなにか短い作品を見ようといった状態や、昔見たものを再度見たり、まったく異なるジャンルの作品を気分転換に見たいという状態があるのではないかとしている。このようにジャンルなどの類似性がユーザの行動にもたらす影響は異なるので、分析と適切な理解が必要であることを述べていた。こうした実践的な問題はあまり研究の文脈では議論されないことが多いが、実サービスに近い推薦システムの領域では重要な問題となり、特に産業界からの参加者の強い関心を誘っていたように思う。

## 寄稿にあたり

現代のWebにおいて推薦システムは当たり前機能になりつつあり、その重要性は日々増している。そんな中でRecsysは推薦システムが抱える問題について先進的で有意義な議論を行うことができる会議である。ぜひ投稿・参加を検討いただき、国内での推薦システムの議論がより活発になることを望む。



(関 喜史 / (株) Gunosy)

その13 VR界の大イベント「Vket」を主催する、動く城のフィオさんに会ってみた

漫画：まいてい 999

VR空間の一面に佇む  
IPSJブース…



この人は稲見編集長  
編集長アバターが24時間鎮座!?

そう…ここは広大な3D空間の中に、個人や企業が創作物を思い思いに展示して

気に入ったものがあればWEBサイト経由で実際に購入もできるという  
VR界世界最大の催しが…

# バーチャルマーケット (略してVket)である!!!



取材者：かずちゃん(IPSJ) & まいてい999(絵描き) おまけのおきゆたん

2018年から半年に1回開催して  
今回で5回目です!



自分で作成した3Dのアバターを  
展示・販売できる、多くの企業の協賛も  
頂いている大規模なお祭りイベントです!

Vket主催  
VR法人HIKKY  
動く城のフィオさん

Vketをはじめた  
きっかけは?

ちょうど2018年あたりが世の中の的にも  
VRの転機でした



低価格  
VR機器の発売



VR業界の拡大

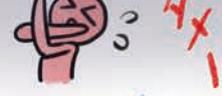
身体的な理由からの  
VRで社会復帰

バーチャルキャラクターの  
YouTubeなどでの活動  
(VTuberの走り)

いくつかのVRコミュニケーション  
サービスの開始

そして、混沌としたアバターの  
入手環境を改善しようという意識が高まってきて

違法にゲームなどから  
抽出されたキャラ  
用途(規約)が  
合わないデータの  
無断流用



「アバター  
作ってみた!」

「アバターで  
使ってOK!」

VR用アバター用途を前提とした  
3Dモデルの販売・配布が流行り始めました

そこでVketという共通の作品発表の場があれば  
 アバターを求める人やVRに興味のある企業とクリエイターが巡り合う  
 きっかけとなるのではと思いました

さらにリアルでのウィンドウショッピングのように  
 知らなかった作品との偶然の出会いも  
 VRだと実現できたりします



アバター以外にも小物とか何でも  
 ありだから新しい出会いも多いよ!!



Vketがきっかけで仕事に繋がった  
 クリエイターさんもいます?



例えば、前回に個人ブースを出しての方が  
 企業の方の目に留まって、Vket5では  
 協賛企業ブースの制作に携わったりしました



Vket制作は、ごく一部の方を除いてバーチャルだけで全て実現できています

現実での、国・場所・時間・性別・年齢・見た目  
 に全くとらわれない!!



ちなみに次回の  
 Vketは常設になるそうです!!

出展も遥かに  
 簡単らしいよ

次は失敗しないぞ!!



まいてい999 twitter: @mighty999

IT関連の会社員。80年代のマイコン・パソコンブーム  
 時代をネイティスに生き当時のPC雑誌に4コマや  
 イラストをハガキ投稿しまくった結果、今に至る。  
 2014年から「おきゅたん」を生み出して今のVR界  
 全体を生温かく見守っているニッチ大王、でも貧乏。



バーチャルマーケット 5  
<https://www.v-market.work/v5/>



(株) HIKKY  
<https://www.hikky.life/company>



今月の会員の広場では、12月号へのご意見・ご感想を紹介いたします。まず、特集「情報と防災」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。

#### 「0. 編集にあたって」

■災害情報システムの抱える問題点を俯瞰するとともに、本特集の各記事へのスムーズな導入部となっている。また、提案されている災害関連図の考え方は、情報システムならではの特色を活かせる可能性があると思われ、今後の発展が期待できる。  
(丹羽邦彦)

■日本にて多くの震災を経験した身として、今号の情報と防災の特集はとても興味深かったです。東日本大震災のときはTwitterが大きく活用され、しばらく学会でもSNSでの情報拡散についての研究発表をよく目にしました。基盤システムが構築された後、いかに正しく使われるか、正しい情報をいかに多くの人に届けるかについても引き続き研究され、より良いものとなることを期待しています。  
(佐伯嘉康)

#### 「3. なぜ防災情報システムは使えないのか？」

■内容的には想像しているとおりが、公表されたことに敬意を表する。  
(匿名希望)

■「0. 編集にあたって」の記事で、「住民一人ひとりに個別の災害情報が届く」には恐怖を感じた。これを突き詰めれば、いわゆるトロッコ問題に突き当たるのではないだろうか。災害情報は、可能な限り平等に届けるべきであり、「1. 地震観測のこれまでと未来」の最後に書いてあるように「人々が自分自身にとってより良い選択を自発的に取れるように手助けする」のがあるべき姿ではないだろうか。それは「個別の災害情報」ではないと思う。  
(伊藤雅樹)

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。

■4名の回答者の方々の答えを読んでとても面白く奥が深い事柄だと思いました。  
(松浦満夫)

■大半の回答者が質問に対しきちんと回答していないのが気になった。  
(匿名希望)

■漫画家に依頼したのは、とてもよかったと思いました。毎回、少し離れた分野の人に依頼するのは効果的かもしれませんが。  
(風間一洋)

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

『『アルゴリズム体験ゲーム』から『プログラミング体験ゲーム』へ』  
■アルゴリズムをゲーム感覚で習得するための課題解決型ゲームソフト「アルゴロジック」について解説されているが、テーマがかなり絞られているので興味を持つ読者層が狭いのではないかと。できればもう少し範囲を広げて「課題解決型ゲームソフト」全般について解説していただき、一事例として「アルゴロジック」に触れていただく方がよいのではないかと。(丹羽邦彦)

連載「ビブリオ・トーク：イノベーターズ」については、以下のようなご意見・ご感想をいただきました。

■今月のビブリオ・トークは面白くて、紹介されていた本にとっても興味を惹かれたので読んでみたいと思います。(匿名希望)

連載「5分で分かる!? 有名論文ナナム読み：Garfinkel, T. and Rosenblum, M.: A Virtual Machine Introspection Based Architecture for Intrusion Detection」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。

■いつも有名論文ナナム読みを楽しみにしています。  
(匿名希望/ジュニア会員)

連載「IT紀行：Google×情報処理学会! 高校生のためのオンラインセッションを見てみた」については、以下のようなご意見・ご感想をいただきました。

■紹介されていた再生リストを閲覧しました。(匿名希望)

コラム「対面の価値」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。

■首藤先生のコラムが大変興味深かったです。オンライン化によるコスト削減効果に対して、対面の価値が定量化しにくく、コスト削減圧力に抵抗しがたいという部分は思わず膝を叩きました。私自身も対面の価値を感じるのですが、それをうまく数字には表せません。情報学の新たな研究分野かもしれないと思います。  
(服部充洋)

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。

■動画サイトと連携して、著者の講演を視聴できるようになるといいと思いました。  
(服部充洋)

■草稿執筆、編集まで読者が参加できるような、Wikiのような記事作りの仕組みがあると面白いと思う。  
(佐伯嘉康)

■インタビュー記事に連動した動画・音声の提供。(金子雄介)

■オンライン版ができると、携帯で通勤の間や隙間時間にさっと読めるようになってほしいです。読むだけではなく動画での配信などのコンテンツがあればもっと広がりが出ると思います。  
(匿名希望)

■紙と電子の複合版でなく、紙またはPDFで送ってほしい。紙と電子の両方を見るのは不便です。(匿名希望)

■前回のモニタ回答でも述べたが、会誌の印刷イメージを再現しただけのPDFでは電子化の意味がない。「2.『防災×情報』の基盤と将来への期待」の記事(e13ページ)にも「国の緊急災害対策本部がとりまとめた被害報はWebサイト上で公開されたが、明らかに紙をスキャンした資料をまとめたPDFであった。」と、PDFの役立たなさは公知の事実である。PDFでの電子化は電子化の利点が多くない。コスト削減にはなると思うが、読者(会員)にとっては1冊ずつを購入しているわけではないのでコスト削減のメリットも感じられない。また、紙に印刷された文書を読むという優れたインタフェースを妨げられ、読むためにはログインしてダウンロードするという面倒な作業が必要となり、さらに印刷物に比べて操作性に劣るPCで読むという、手間もかかる上にきわめてアンフレンドリーなインタフェースを強いられる。このような電子化は即刻やめるべきである。電子化するなら電子化するだけの(読者にとっての)メリットが実感できるようにしていただきたい。たとえば、「e5ページ」最終段落の「震源に近い観測的で」は「震源に近い観測点で」の誤字であろう。せつかくの電子版なら修正してほしい。ただし、この程度(修正の容易さ)のメリットはメリットとも言えないが、本アンケートの[8-2]も、前回に引き続き「ハイブリッド」の選択肢がない。回答する立場に立って考えているのか、大いに疑問である。(伊藤雅樹)

■ボリュームが少なかった。会誌としてある程度統一した方がよいのでは。電子版と会誌の在り方について考える必要があると感じる。(笹部聖也)

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。

■巻頭コラムで、新しく発足する「デジタル庁」に所属予定の方に、ご自身の参画理念(真情)を語っていただけたらと思います。(匿名希望)

■「情報の授業をしよう」では、言語学習を通して私たち生徒の何を育成しようとして取り組んでいるのかといった視点でまとめてほしい。(匿名希望/ジュニア会員)

■Cyber Deceptionあるいはそれに近いテーマを取り上げてほしい。(匿名希望)

■富岳についての特集。(中井彩乃)

■ジュニア会員向け記事の充実も良いが、大学生(非情報系学部を含む)が目を通したい基礎的な話題も充実するとさらに良い。(金子雄介)

■対面でのユーザスタディを必要とする研究において、コロナ禍での研究の進め方の工夫、苦勞、失敗談などの記事を読みたい。(匿名希望)

■情報学や情報工学への展望を哲学的視点から論じることがあってもよいのではないか。(匿名希望)

■西菌さんの記事は前回に引き続き興味深く読ませていただきました。世界レベルのプロスポーツ選手だった方の技術記事を読めるというのは非常に貴重なことだと思います。(匿名希望)

■各国の情報学の大学教育について知りたいです。海外に比べて日本がどんな立ち位置にあるのか知りたいです。(匿名希望)

【本欄担当 山本岳洋・加藤千裕/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、こちらでもご参照ください。会誌や掲載記事に関するご意見・ご感想は学会Webページでも受け付けております。今後もより良い会誌を作るため、ぜひ皆様のお声をお寄せください。

皆様にとって会誌をより役立つものとするため、

- ・記事に対する感想、意見
- ・記事テーマの提案
- ・会誌または学会に対する全般的な意見、提言
- ・その他、情報処理技術についての全般的な意見、提言

など自由なご意見、ご感想をお待ちしております。

なお、「道しるべ」については

<URL: <https://www.ipsj.or.jp/magazine/sippitsu/michishirube.html>>で

これからのテーマ案を募集しており、いただいたご意見をまとめております。

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

掲載に際しては、編集の都合上、ご意見に手を加えさせていただくことがありますので、あらかじめご了承ください。

なお、意見の投稿に伴う、住所、氏名、所属などの個人情報については、学会のプライバシーポリシーに準じて取り扱いたします。<URL: <https://www.ipsj.or.jp/privacypolicy.html>>

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

ご意見をお寄せ  
ください!



## IPJS カレンダー

※新型コロナウイルス感染症拡大を受け、開催方法の変更、開催中止などの可能性がありますので、最新情報を Web でご確認くださいませう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「デジタル社会の情報セキュリティとトラスト」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/21-P.html">https://www.ipsj.or.jp/journal/cfp/21-P.html</a>	2月24日(水)		
	論文誌「トランザクションデジタルプラクティス」[DXのプラクティス～ニューノーマル時代を生き延びる～]特集論文募集 <a href="https://www.ipsj.or.jp/dp/submit/tdp0201s.html">https://www.ipsj.or.jp/dp/submit/tdp0201s.html</a>	3月10日(水)		
	東海支部2020年度学生論文奨励賞論文募集 <a href="https://www.ipsj-tokai.jp/jigyoushourei/">https://www.ipsj-tokai.jp/jigyoushourei/</a>	3月15日(月)		
	論文誌「社会課題を解決するコラボレーション技術とネットワークサービス」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-D.html">https://www.ipsj.or.jp/journal/cfp/22-D.html</a>	3月29日(月)		
	論文誌「ニューノーマル時代の高度交通システムとパーベイシブシステム」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-E.html">https://www.ipsj.or.jp/journal/cfp/22-E.html</a>	3月31日(水)		
	論文誌「インタラクションの理解および基盤・応用技術」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-J.html">https://www.ipsj.or.jp/journal/cfp/22-J.html</a>	4月16日(金)		
	論文誌「ネットワークサービスと分散処理」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-K.html">https://www.ipsj.or.jp/journal/cfp/22-K.html</a>	4月30日(金)		
	論文誌「若手研究者」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-F.html">https://www.ipsj.or.jp/journal/cfp/22-F.html</a>	4月30日(金)		
	論文誌「人文科学とコンピュータ」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-C.html">https://www.ipsj.or.jp/journal/cfp/22-C.html</a>	5月11日(火)		
	論文誌「新しい生活様式を見据えたインターネットと運用技術」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-H.html">https://www.ipsj.or.jp/journal/cfp/22-H.html</a>	5月17日(月)		
	論文誌「ソフトウェア工学」特集への論文募集 <a href="https://www.ipsj.or.jp/journal/cfp/22-L.html">https://www.ipsj.or.jp/journal/cfp/22-L.html</a>	8月2日(月)		
2月16日(火)～ 2月17日(水)	第181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 <a href="https://www.ipsj.or.jp/kenkyukai/event/cg181.html">https://www.ipsj.or.jp/kenkyukai/event/cg181.html</a>	1月12日(火)	当日可 要マイページより申込	★オンライン開催
2月19日(金)	第91回電子化知的財産・社会基盤研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/eip91.html">https://www.ipsj.or.jp/kenkyukai/event/eip91.html</a>	12月18日(金)	当日可 要マイページより申込	大阪経済大学 +オンライン開催
2月26日(金)	第112回オーディオビジュアル複合情報処理研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/avm112.html">https://www.ipsj.or.jp/kenkyukai/event/avm112.html</a>	1月25日(金)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第132回数理モデル化と問題解決研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/mps132.html">https://www.ipsj.or.jp/kenkyukai/event/mps132.html</a>	1月7日(木)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第98回モバイルコンピューティングとパーベイシブシステム・第69回ユビキタスコンピューティングシステム合同研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/mb198ubi69.html">https://www.ipsj.or.jp/kenkyukai/event/mb198ubi69.html</a>	1月13日(水)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第41回セキュリティ心理学とトラスト研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/spt41.html">https://www.ipsj.or.jp/kenkyukai/event/spt41.html</a>	1月13日(水)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第52回インターネットと運用技術研究発表会 <a href="https://www.iot.ipsj.or.jp/meeting/52-cfp/">https://www.iot.ipsj.or.jp/meeting/52-cfp/</a>	1月14日(木)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第207回ソフトウェア工学研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/se207.html">https://www.ipsj.or.jp/kenkyukai/event/se207.html</a>	1月18日(月)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	第151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 <a href="https://www.ipsj.or.jp/kenkyukai/event/os151.html">https://www.ipsj.or.jp/kenkyukai/event/os151.html</a>	1月18日(月)	当日可 要マイページより申込	★オンライン開催
3月1日(月)～ 3月2日(火)	九州支部「火の国情報シンポジウム2021」 <a href="https://www.ipsj-kyushu.jp/events/hinokuni-init">https://www.ipsj-kyushu.jp/events/hinokuni-init</a>	1月25日(月)		★オンライン開催
3月3日(水)～ 3月4日(木)	第136回音声言語情報処理研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/slp136.html">https://www.ipsj.or.jp/kenkyukai/event/slp136.html</a>	1月18日(月)	当日可 要マイページより申込	★オンライン開催
3月4日(木)～ 3月5日(金)	第225回コンピュータビジョンとイメージメディア研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/cvim225.html">https://www.ipsj.or.jp/kenkyukai/event/cvim225.html</a>	1月4日(月)	当日可 要マイページより申込	★オンライン開催
3月4日(木)～ 3月5日(金)	第84回高度交通システムとスマートコミュニティ研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/its84.html">https://www.ipsj.or.jp/kenkyukai/event/its84.html</a>	1月20日(水)	当日可 要マイページより申込	金沢港ターミナル 2F セミナールーム and/or オンライン
3月5日(金)	第45回ゲーム情報学研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/gi45.html">https://www.ipsj.or.jp/kenkyukai/event/gi45.html</a>	1月21日(木)	当日可 要マイページより申込	★オンライン開催
3月5日(金)	第20回高齢社会デザイン研究発表会 <a href="https://www.ipsj.or.jp/kenkyukai/event/asd20.html">https://www.ipsj.or.jp/kenkyukai/event/asd20.html</a>	1月29日(金)	当日可 要マイページより申込	★オンライン開催

開催日	名 称	論文等応募締切日	参加締切日	開催地
3月5日(金) ~	第15回アクセシビリティ研究発表会	1月18日(月)	当日可 要マイページより申込	★オンライン開催
3月7日(日)	<a href="https://www.ipsj.or.jp/kenkyukai/event/aac15.html">https://www.ipsj.or.jp/kenkyukai/event/aac15.html</a>			
3月8日(月) ~	第155回情報システムと社会環境研究発表会	1月14日(木)	当日可 要マイページより申込	青山学院大学 青山キャンパス and/or オンライン
3月9日(火)	<a href="https://www.ipsj.or.jp/kenkyukai/event/is155.html">https://www.ipsj.or.jp/kenkyukai/event/is155.html</a>			
3月10日(水) ~	インタラクション2021		当日可 要マイページより申込	学術総合センター/ 一橋講堂 and/or オンライン
3月12日(金)	<a href="https://www.interaction-ipsj.org/2021/">https://www.interaction-ipsj.org/2021/</a>			
3月11日(木)	第65回バイオ情報学研究発表会	2月4日(木)	当日可 要マイページより申込	★オンライン開催
3月13日(土) ~	第159回コンピュータと教育研究発表会	1月22日(金)	当日可 要マイページより申込	千里金蘭大学 +オンライン開催
3月14日(日)	<a href="https://www.ipsj.or.jp/kenkyukai/event/ce159.html">https://www.ipsj.or.jp/kenkyukai/event/ce159.html</a>			
3月15日(月) ~	第178回ハイパフォーマンスコンピューティング研究発表会	1月12日(火)	当日可 要マイページより申込	★オンライン開催
3月16日(火)	<a href="https://www.ipsj.or.jp/kenkyukai/event/hpc178.html">https://www.ipsj.or.jp/kenkyukai/event/hpc178.html</a>			
3月15日(月) ~	第192回ヒューマンコンピュータインタラクション研究発表会	1月18日(月)	当日可 要マイページより申込	★オンライン開催
3月16日(火)	<a href="https://www.ipsj.or.jp/kenkyukai/event/hci192.html">https://www.ipsj.or.jp/kenkyukai/event/hci192.html</a>			
3月15日(月) ~	第186回マルチメディア通信と分散処理・	1月28日(木)	当日可 要マイページより申込	★オンライン開催
3月16日(火)	第92回コンピュータセキュリティ合同研究発表会			
	<a href="https://www.ipsj.or.jp/kenkyukai/event/dps186csec92.html">https://www.ipsj.or.jp/kenkyukai/event/dps186csec92.html</a>			
3月15日(月) ~	第113回グループウェアとネットワークサービス研究発表会	1月29日(金)	当日可 要マイページより申込	★オンライン開催
3月16日(火)	<a href="https://www.ipsj.or.jp/kenkyukai/event/gn113.html">https://www.ipsj.or.jp/kenkyukai/event/gn113.html</a>			
3月16日(火) ~	第133回プログラミング研究発表会	1月15日(金)	当日可 要マイページより申込	★オンライン開催
3月17日(水)	<a href="https://sigpro.ipsj.or.jp/pro2020-5/">https://sigpro.ipsj.or.jp/pro2020-5/</a>			
3月16日(火) ~	第130回音楽情報科学・第59回エンタテインメント	1月28日(木)	当日可 要マイページより申込	★オンライン開催
3月17日(水)	コンピューティング合同研究発表会			
	<a href="https://www.ipsj.or.jp/kenkyukai/event/mus130ec59.html">https://www.ipsj.or.jp/kenkyukai/event/mus130ec59.html</a>			
3月18日(木) ~	情報処理学会 第83回全国大会			★オンライン開催
3月20日(土)	<a href="https://www.ipsj.or.jp/event/taikai/83/">https://www.ipsj.or.jp/event/taikai/83/</a>			
3月25日(木) ~	第236回システム・アーキテクチャ・	1月20日(木)	当日可 要マイページより申込	★オンライン開催
3月26日(金)	第194回システムとLSIの設計技術・			
	第56回組込みシステム合同研究発表会 (ETNET2021)			
	<a href="https://www.ipsj.or.jp/kenkyukai/event/arc236sldm194emb56.html">https://www.ipsj.or.jp/kenkyukai/event/arc236sldm194emb56.html</a>			
3月25日(木) ~	第33回教育学習支援情報システム研究発表会	1月22日(金)	当日可 要マイページより申込	東京大学 +オンライン開催
3月26日(金)	<a href="https://www.ipsj.or.jp/kenkyukai/event/cle33.html">https://www.ipsj.or.jp/kenkyukai/event/cle33.html</a>			
3月26日(金)	第142回情報基礎とアクセス技術・	1月31日(日)	当日可 要マイページより申込	★オンライン開催
	第120回ドキュメントコミュニケーション合同研究発表会			
	<a href="https://www.ipsj.or.jp/kenkyukai/event/ifat142dc120.html">https://www.ipsj.or.jp/kenkyukai/event/ifat142dc120.html</a>			
3月29日(月)	第2回量子ソフトウェア研究発表会	2月15日(月)	当日可 要マイページより申込	★オンライン開催
	<a href="https://www.ipsj.or.jp/kenkyukai/event/qs2.html">https://www.ipsj.or.jp/kenkyukai/event/qs2.html</a>			
8月25日(水) ~	第20回情報科学技術フォーラム			東北学院大学 (オンライン)
8月27日(金)	<a href="https://www.ipsj.or.jp/event/fit/fit2021/">https://www.ipsj.or.jp/event/fit/fit2021/</a>			

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

#### [トピックス]

- 1月15日 人材募集情報 (Vol.62 No.2)
- 1月15日 会誌「情報処理」Web カタログ (Vol.62 No.2)
- 1月14日 論文誌「若手研究者」特集 論文募集
- 1月14日 論文誌「ネットワークサービスと分散処理」特集 論文募集
- 1月5日 新年の挨拶
- 12月18日 過去のプログラミング・シンポジウム報告集の利用許諾について
- 12月15日 2021年度 会誌「情報処理」モニタ募集
- 12月15日 会誌「情報処理」Web カタログ (Vol.62 No.1)

**情報処理学会 第 83 回全国大会**  
**イベント企画のみの聴講参加は「無料」!! オンライン特別価格です。**  
**申込はこちらから⇒ <https://www.ipsj.or.jp/event/taikai/83/>**  
**ぜひ皆様お誘い合わせの上、奮ってご参加ください**

## 情報処理学会 第 83 回全国大会 聴講申込 『コロナ新時代の情報処理』

大会会期：2021年3月18日（木）～20日（土）  
 大会会場：オンライン開催  
 共 催：大阪大学  
 後 援：全国高等学校情報教育研究会

情報処理学会第83回全国大会の「大会聴講参加」の申込を受付中です。オンライン開催のため今回は特別価格となっております。

- イベント会場・特別会場において開催される「特別講演/招待講演/イベント企画/各種展示」を聴講・ご覧になる場合  
→「大会イベント企画限定聴講参加」（無料）
- 上記に加え、「一般セッション/学生セッション」を聴講する場合  
→「大会共通聴講参加」（有料）

イベント企画のみ聴講希望の方は、大会 Web ページから申込みをする際、「大会イベント企画限定聴講参加」にお申し込みください。  
 通常の一般セッション・学生セッションも聴講希望の場合は、「大会共通聴講参加」にお申し込みください（聴講参加費は有料となります）。

**申込受付期間：2020年12月7日（月）～2021年3月20日（土）大会最終日まで**

**招待講演・特別講演企画【聴講参加無料】**：招待講演4件と特別講演3件を予定しております。

招待講演 -1	18日（木）16：30～16：45	Impact of COVID-19 on education and academic activities in Korea (The Korean Institute of Information Scientists and Engineers)
招待講演 -2	18日（木）16：45～17：00	Challenges and Responsibilities in Operation of IT Community After the COVID-19 Pandemic (China Computer Federation)
招待講演 -3	18日（木）17：00～17：15	未定 (IEEE Computer Society)
招待講演 -4	18日（木）17：15～17：30	Computing Machinery Shapes Our Future - Let's Join Forces ! (Association for Computing Machinery)
特別講演	19日（金）15：20～16：20	「コロナ新時代を実現するデジタルトランスフォーメーション」
	19日（金）16：20～17：20	「研究現場のデジタルトランスフォーメーションとその先にある AI 駆動型科学 - ロボティック・バイオロジーによる生命科学の加速 -」
	20日（土）15：30～17：30	IPSJ-ONE

**イベント企画【聴講参加無料】**：各イベント企画では、その分野の最前線で活躍されておられる方をお招きし、講演・パネル討論等の開催を予定しております。

第1 イベント会場	18日 9：30～11：30	「2020年サイバー事件回顧録～技術と法制度の両面から～」
	18日 12：40～15：10	「コロナ新時代の情報処理（生活）～DXによるニューノーマルの実現に向けて～」
	19日 9：30～11：30	「コロナ新時代の情報処理（教育）～高等教育におけるニューノーマルの模索～」
	19日 12：40～15：10	「コロナ新時代の情報処理（研究）～COVID-19対策における富岳の活用～」
	20日 9：30～12：00	「2025年実施の大学情報入試への展望」
	20日 13：20～15：20	「情報科学の達人1.0」
第2 イベント会場	18日 12：40～15：10	「～コンピュータバイオニアが語る～『私の詩と真実』」
	19日 9：30～11：30	「スポーツテック ～デジタルプラクティスライブ～」
	19日 12：40～15：10	「企業研究者の『熱い想い』をお届けします」
	19日 15：20～17：20	「9th IPSJ International AI Programming Contest SamurAI Coding 2020-21 World Final」
	20日 10：00～15：00	「第13回情報システム教育コンテスト」
第3 イベント会場	18日 12：40～15：10	「『アジャイル開発のソフトウェアモデル契約』のその後」

第3 イベント会場	19日 9:30～11:30 「New Normal における学会活動在り方デザイン」 19日 12:40～15:10 「量子技術を利用した次世代アクセラレータの活用」 19日 15:20～17:00 「論文必勝法」 20日 9:30～12:00 「初等中等教員研究発表セッション」 20日 13:20～15:20 「中高生情報学研究コンテスト」
第4 イベント会場	18日 9:30～11:30 「AI TECH TALK」 18日 12:00～14:30 「インダストリアルセッション」 18日 15:00～17:30 「IT 情報系キャリア研究セッション」 19日 15:00～17:30 「IT 情報系キャリア研究セッション」 20日 9:30～13:00 「Exciting Coding! Junior @ Osaka ～みんなで一緒にプログラミングしよう～」 20日 13:20～15:50 「IT 情報系キャリア研究セッション」
特別会場	20日 11:00～13:00 「『先生質問です!』 & 『編集委員会』 公開セッション」

一般セッション・学生セッション【聴講参加 有料】:

約1,500件の研究成果発表があります。大会3日間でおおよそ30会場を使用して、190あまりのセッションが生まれ、活発な発表、議論・討論が行われます。

■聴講参加費・講演論文集代(税込)

オンライン開催のため今回は特別価格となっております。学生の大会共通聴講参加費が「無料」です。

申込種別	価 格
大会イベント企画限定聴講参加	無料
大会共通聴講参加(正会員) *全論文のPDFアクセス権付	5,000円
大会共通聴講参加(一般非会員) *全論文のPDFアクセス権付	9,000円
大会共通聴講参加(学生会員・ジュニア会員・学生非会員)	無料

◇留意事項

- ※「大会イベント企画限定聴講参加」は、特別講演、招待講演、イベント企画、IT情報系キャリアセッションのみ聴講参加可能です。一般セッション・学生セッションの聴講はできませんのでご注意ください。
- 一般セッション・学生セッションも聴講参加希望の場合には、大会共通聴講参加(有料)のほうにお申し込みください。学生の方は大会共通聴講参加費が「無料」です。
- ※「大会共通聴講参加」は、一般セッション・学生セッションを含む大会すべてのセッションの聴講参加が可能です。
- ※講演参加申込の方、座長の方、イベント企画者および登壇者は聴講参加申込は不要です。聴講参加をお申し込みになりますと二重申込となりますのでご注意ください。

■講演論文集代(税込・送料込)

残部のある限り販売を行います。受け取りは大会終了後の郵送となります。

申込種別	予約価格(2/4迄)	価 格
講演論文集分冊(個人・法人問わず)	13,000円	14,000円
講演論文集セット *DVD-ROM 1枚付き(個人・法人問わず)	60,000円	66,000円
講演論文集 DVD-ROM(個人)	10,000円	
講演論文集 DVD-ROM(法人)	60,000円	

■聴講参加および講演論文集の申込、詳細は、以下のサイトからお願いいたします。

第83回全国大会公式 Web サイト <https://www.ipsj.or.jp/event/taikai/83/>

■問合先

〒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 事業部門  
電話 (03) 3518-8373  
FAX (03) 3518-8375  
E-mail: ipsjtaikai@ipsj.or.jp



# FIT2021 第20回情報科学技術フォーラム

## 選奨論文・一般論文 講演募集予告

会 期：2021年8月25日（水）～27日（金）

会 場：東北学院大学（オンライン）

FIT2021 Web ページ <https://www.ipsj.or.jp/event/fit/fit2021/>

受付期間(予定)：2021年3月29日（月）～5月7日（金）

◆論文ページ数：2～8ページ程度 ◆講演時間：20分

◆3ページ目以降は追加ページ代（4,000円／ページ）が必要です

電子情報通信学会 情報・システムソサイエティ (ISS) 並びにヒューマンコミュニケーショングループ (HCG) と情報処理学会 (IPSJ) は、2002年から毎年秋季に合同で「情報科学技術フォーラム(FIT: Forum on Information Technology)」を開催しています。2021年8月には、記念すべき第20回目を東北学院大学（オンライン）で開催します。FITは、両学会の大会の流れをくむものであると同時に、従来の大会の形式にとらわれずに新しい発表形式を導入し、タイムリーな情報発信、活気ある議論・討論、多彩な企画、他分野研究者との交流を実現してきております。皆様の研究成果発表の場として、標記のとおり論文発表を募集致しますので奮ってお申込み下さい。

### ●申込主要日程（予定）

登録申込／投稿受付期間：2021年3月29日（月）から 2021年5月7日（金）まで

最終掲載原稿締切：2021年6月18日（金）

※ FIT2017 より、査読付き論文は廃止とし、選奨論文制度を取り入れました。

※ 登録申込と原稿投稿は上記のFIT2021 Webページよりお願い致します。詳細は決定次第 Webページでお知らせ致します。

### ●表彰

FITには、以下の表彰制度がありますので是非ともチャレンジして下さい。

いずれの賞も、電子情報通信学会又は情報処理学会の会員であることが受賞条件となりますのでこの機会に是非御入会下さい。

船井ベストペーパー賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上3件選定。賞金は船井情報科学振興財団より20万円贈呈。
FIT 論文賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上7件程度選定。賞金はFIT 運営委員会より5万円贈呈。
FIT ヤングリサーチアワード賞	2021年12月31日現在で33歳未満の講演者（選奨論文および一般論文）の中から、発表件数の1.5%を上限として選定。賞金はFIT 運営委員会より3万円贈呈。本賞受賞は本人に対し一回のみ。
FIT 奨励賞	一般発表のセッション毎に座長の裁量で優秀な発表を1件その場で選定（該当なしもあり）。FIT 終了後に賞状を贈呈。

### ●選奨論文（4～8 ページ程度）

投稿された論文の担当研究会を決定していただきます。FIT2021 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において投稿時に適切に選択して下さい。

船井ベストペーパー賞、FIT 論文賞への審査を希望する場合は、Web からの講演申込みの際に必ず論文形式で『選奨論文』を選択して下さい。但し、賞を前提とした論文形式となりますので、電子情報通信学会又は情報処理学会の会員であることが投稿条件となります。非会員の方は御入会手続きをお済ませの上御投稿下さい。選奨論文はFIT 初日の選奨セッションに組み込まれ、各セッションにて選奨委員2名による1次審査を行います。1次審査の結果は当日の夕方までに大会会場に掲示されます。2次審査はFIT 終了後実施され、上位3件が船井ベストペーパー賞、次点7件程度が FIT 論文賞の受賞となります。

※4 ページ以上の投稿が必須ですが、3 ページ目からは追加ページ代（4,000 円／ページ）が発生します。例えば6 ページ投稿の場合、4 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000 円×4＝16,000 円」の追加費用が必要となります。

### ●一般論文（2～8 ページ程度）

FIT2021 Web ページに掲載の研究会取り扱い分野をよく御確認のうえ御自身の論文内容と一致した研究会を、申込者御自身の責任において適切に選択して下さい。

※3 ページ以上の投稿される場合は、3 ページ目からは追加ページ代（4,000 円／ページ）が発生します。例えば4 ページ投稿の場合、2 ページ分の追加ページ代が発生しますので、講演参加費のほかに「4,000 円×2＝8,000 円」の追加費用が必要となります。

### ●論文誌推薦制度

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

### ●問合せ先（FIT2021事務局）

〒101-0062 千代田区神田駿河台1-5 化学会館4階

情報処理学会 事業部門 TEL. 03-3518-8373 FAX. 03-3518-8375 E-mail: ipsjfit@ipsj.or.jp

## ● 論文誌ジャーナル掲載論文リスト

Vol.62 No.2 (Feb. 2021)

### 【特集：ネットワークサービスと分散処理】

- 特集「ネットワークサービスと分散処理」の編集にあたって  
菅沼拓夫 他
- ユーザ近傍から多くのコンテンツを配信する重複の少ないNDNの  
キャッシュアルゴリズム 中田有哉 他
- マルチメディア通信と分散処理研究領域における論文価値の意識  
調査とその活用 木原民雄 他
- Effective Route Scheme of Multicast Probing to Locate High-  
loss Links in OpenFlow Networks Nguyen Minh Tri 他
- An Adaptive Traffic Signal Control Scheme Based on Back-  
Pressure with Global Information Arnan Maipradit 他
- Receiver-Prioritized Next Transmission in Multichannel MAC  
Protocol for Wireless Ad-hoc Networks Ushio Yamamoto 他
- ARを用いたセンサ位置設定システムの設計と評価 田上敦士 他
- 密集無線LANにおける公平性向上のためのリンクアダプテーショ  
ンを伴った送信電力・信号検出閾値制御 坂井渉太 他
- Dynamic Swarm Spatial Scaling for Mobile Sensing Cluster in  
Noisy Environment Eiji Nii 他
- プロセス生成を高速化する資源プール機能の実現と評価  
谷口秀夫 他
- ロープウェイ式カメラモニタリングにおける効率的なロープの設置  
場所決定手法 勝間 亮 他
- Localization with Portable APs in Ultra-Narrow-Band-based  
LPWA Networks Miya Fukumoto 他
- Wi-Fi RTTと機械学習を用いた位置推定の提案と評価  
長沼慶弥 他
- Flexible Imputation Method for Sensor Data based on  
Programming by Example: APREP-S Hiroko Nagashima 他
- 車載器非搭載車両を考慮した協調認識のためのモバイルエッジコ  
ンピューティング支援型車両情報共有システム 佐竹颯太 他
- CNNを用いた予測に有効なナンバープレート写真用トレーニング  
データの検討 鈴木友哉 他
- 極値分割とDynamic Time Warpingによるデータ類似度評価手法  
森 郁海 他
- 情報流通においてデータ提供への対価を決定する第三者エージェ  
ントを用いた自動交渉 戸嶋丈士 他
- 複合センサーを用いた屋内環境における行動認識に関する実装と  
評価 中沢 実 他
- 作業を代表するフォルダの推定と分類による仮想フォルダ生成シス  
テム 西 良太 他
- 重要図表を考慮したEnd-to-Endの学術論文要約システム  
佐藤照大 他
- 大規模なインタラクティブシミュレーションのためのデータの階層  
化と拡散を特徴とする分散システム 山岡久俊 他
- 協力型オンラインRPGコミュニケーションのための絵文字定型文を  
用いたチャットシステムEMO-GコミュニケーターII 宗森 純 他

### 【特集：インタラクションの理解および基盤・応用技術】

- 特集「インタラクションの理解および基盤・応用技術」の編集に  
あたって 志築文太郎 他
- 幅の異なる経路が連結されたコーナリングタスクのモデル化  
薄羽大樹 他
- Motor WidthとVisual Widthの差を考慮したポインティングのモ  
デル化 薄羽大樹 他
- 日本語形態素文字種境界法によるデータベース検索量の削減  
米持幸寿 他
- 一人称ライフログ映像からの顔検出に基づいた社会活動計測  
奥野 茜 他

- ウェアラブルコンピューティングにおける周波数操作による聴力自  
在化技術の提案\* 渡邊拓貴 他
- 掌上装着魚眼カメラを用いたフリーハンドARのための手指姿勢  
推定 丸山裕介 他
- ShearSheet: 静電容量タッチパネルに装着可能な透明シートを用  
いた剪断入力インタフェース 藤田和之 他
- スキーポールによる携帯端末操作に向けたユーザ定義型ジェス  
チャの設計と認識 岡田友哉 他
- Bubble Gaze Lens: バブルレンズ法の視線操作への適用  
崔 明根 他
- Bring Your Own Pointer: 複数の携帯端末によるad hocなマル  
チポインティング手法 佐藤光起 他
- 選択ターゲット候補の半円状再配置によるスマートフォンでの片手  
選択操作手法の提案 秋葉翔太 他
- PhKey: 指節をキーとして利用するウェアラブル機器向け入力イン  
タフェース 中村喜宏 他
- ブラインドを拡張した新たな情報提示手法の研究 本間貴士 他
- 知的環境構築のための測定システムを利用した濃度予測モデルの  
評価 守谷元一 他
- 移動エンタロピーを用いた集団スポーツにおける潜在的情報伝達  
の分析手法 田中 毅 他
- 野球における指導者の主観的評価によるスイング特性  
藤山雅洋 他
- 多人数遠隔コミュニケーションにおける肯定的感情表出支援の効  
果と支援適用タイミングの決定 二瓶美巳雄 他
- 雑談対話ロボットの言語的協同によるユーザの共感促進と対話継  
続欲求の向上 楊 潔 他

### 【一般論文】

- Hardness of Instance Generation with Optimal Solutions for  
the Stable Marriage Problem Yuki Matsuyama 他
- 商店を直線表現したTransRecモデルに基づく電子商店街の商品  
推薦アルゴリズム 大堀祐一 他
- 販売履歴データに基づく中古ファッションアイテムの出品価格推定  
モデルの提案 桑田 和 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

(Feb. 2021)

### 【Transactions on Bioinformatics Vol.14】

- Selective Inference for High-order Interaction Features  
Selected in A Stepwise Manner Shinya Suzumura 他
- Efficient Reaction Deletion Algorithms for Redesign of  
Constraint-based Metabolic Networks for Metabolite  
Production with Weak Coupling Takeyuki Tamura 他



### 【論文誌 コンピューティングシステム Vol.14 No.1】

- 小さい定数個の単精度行列への分割を用いた尾崎スキームによる  
倍精度行列乗算のゲーミング用GPU上での評価 七井香樹 他
- Power Prediction for Sustainable HPC Shigeto Suzuki 他



## 【Transactions on System LSI Design Methodology Vol.14】

- Computational Lithography Using Machine Learning Models  
Youngsoo Shin
- Scalable Hardware Architecture for fast Gradient Boosted Tree Training  
Tamon Sadasue 他
- A Case Study on FPGA Implementation of Parts Counting Orientation Recognition Method for Industrial Vision System  
Qiaochu Zhao 他



## 【論文誌 教育とコンピュータ Vol.7 No.1】

- 大学教育における DX の実現に向けて  
常盤祐司
- 一般情報教育におけるプログラミングのスキルの習得度とプログラミングの考え方の理解度の関係  
吉田典弘 他
- 観察支援システム FishWatchr を用いた「自律型対話プログラム」の実践方法の改善と評価  
山口昌也 他

- 幼稚園児のビスケットプログラムにおける繰り返し続けるプログラムの理解の分析  
渡辺勇士 他



## 【論文誌 デジタルコンテンツ Vol.9 No.1】

- 衣服シワに対するキャラクターイラスト特有の陰影形状のリアルタイムレンダリング  
青木明優花 他
- Bubble-Pixels: 気泡を用いた図形描画のための水中ディスプレイ  
宇川拓人 他
- Smart Layer Splitter : pix2pix を用いたデジタルイラスト制作の色塗り工程における自動レイヤ分けシステム  
渡邊 優 他
- 画像接合技術に基づく広視野画像のための隠消現実感達成法  
山崎賢人 他
- セルフメンタルヘルスケアシステムの継続利用促進に向けたチャットボット利用  
紙田 剛他



## 【重要】過去のプログラミング・シンポジウム報告集の利用許諾について

2020年12月18日

プログラミング・シンポジウム委員会

情報処理学会発行の出版物著作権は平成12年から情報処理学会著作権規程に従い、学会に帰属することになっています。

プログラミング・シンポジウムの報告集は、情報処理学会と設立の事情が異なるため、この改訂がシンポジウム内部で徹底しておらず、情報処理学会の他の出版物が情報学広場 (= 情報処理学会電子図書館) で公開されているにもかかわらず、古い報告集には公開されていないものが少からずありました。

プログラミング・シンポジウムは昭和59年に情報処理学会の一部門になりましたが、それ以前の報告集も含め、このたび学会の他の出版物と同様の扱いにしたいと考えます。過去のすべての報告集の論文について、著作権者(論文を執筆された故人の相続人)を探し出して利用許諾に関する同意をいただくことは困難ですので、一定期間の権利者搜索の努力をしたうえで、著作権者が見つからない場合も論文を情報学広場に掲載させていただきたいと思っております。その後、著作権者が発見され、情報学広場への掲載の継続に同意が得られなかった場合には、当該論文については、掲載を停止いたします。

この措置にご意見のある方は、プログラミング・シンポジウムの辻尚史運営委員長(tsuji@math.s.chiba-u.ac.jp)までお申し出ください。

加えて、著作権者について情報をお持ちの方は事務局まで情報をお寄せくださいますようお願い申し上げます。

期間：2020年12月18日～2021年3月19日

情報処理学会著作権規程

<https://www.ipsj.or.jp/copyright/ronbun/copyright.html>

## ●● 2021年度 役員・代表会員選挙 パスワード送付方法変更のご案内 ●●

2021年度役員・代表会員選挙は「Web投票」にて実施いたします。

今回より、選挙のご案内はマイページに掲載し、投票用パスワードは郵送を廃止し、マイページにご登録済みのE-mailアドレスあてに送信いたします(対象：名誉会員・正会員(会費納入済み)の方)。

E-mailで送信された投票用パスワードにて投票用Webサイトよりご投票ください。

投票受付期間は2021年2月1日から26日の予定です。

■照会先：事務局管理部門選挙担当 Tel(03)3518-8374 Fax(03)3518-8375

**CONTENTS**

**Preface**

- 122 **Why We Make Emotional Robots**  
Shunsuke AOKI (Yukai Engineering Inc.)

**Special Features**

**Supply Chain Security in The Age of Digital Transformation**

- 124 **Foreword**  
Masaki ISHIGURO (Mitsubishi Research Institute, Inc.) , Satoru TEZUKA (Keio Univ.) and Takayuki SASAKI (Yokohama National Univ.)
- 126 **Outline**

**Article**

- 130 **I Don't Know How to Love Programming Thinking**  
Satoshi ENDO (KADOKAWA ASCII Research Labs., Inc.)

**"Peta-gogy" for Future**

- 135 **HyFlex Courses**  
Hiroyoshi WATANABE (Teikyo Univ.)

- 136 **National High School Information Education Study Group National Convention**  
Tsutomu OHARA (Tokyo Metropolitan Machida High School)

**Let's Learn Informatics**

- 140 **Thinking about Classes of "Information 1" - Learning Communication and Information Design through Making LINE Stamp -**  
Taira TOMITA (Saitama Prefectural Urawa Girls' Upper Secondary School / Saitama Society for the Study of Information Education)

- 
- 146 **Biblio Talk**
- 148 **Skimming a Famous Paper in Five Minutes**
- 150 **Questions from Experts**
- 152 **IP SJ Activity Report**
- 162 **IP SJ Activity Report**
- 164 **Committee Reports**
- 166 **Conference Report**
- 168 **IT Travelog Manga**

**Online Only**

**Special Features**

**Supply Chain Security in The Age of Digital Transformation**

- e1 **Mechanisms and Systems to Achieve Supply Chain Security**  
Masaki ISHIGURO (Mitsubishi Research Institute, Inc.)
- e7 **Supply-chain Cybersecurity Policy in Japan**  
Toshikazu OKUYA (Ministry of Economy, Trade and Industry)
- e14 **Trends of ICT Supply Chain Security Threats and Countermeasures**  
Ryuichi OGAWA and Akemi KOYAMA (Information-technology Promotion Agency, Japan)

- e21 **Security Certification Scheme for Automation and Control Components**  
Hiroo KANAMARU (Mitsubishi Electric Corp.) and Tsutomu YAMADA (Hitachi Ltd.)
- e28 **Ensuring Supply Chain Security through Third Party Certification**  
Shinichi TOYAMA (TÜV SÜD Japan Ltd.) and Ethiraj, Sudhir Kumar Raj (TÜV SÜD Sec IT GmbH)
- e34 **3<sup>rd</sup> Party Cybersecurity Assurance Program**  
Toshiro YOSHIOKA (UL Japan, Inc.)
- e37 **Overview of Software Bill of Materials (SBOM)**  
Masato MATSUOKA (Nihon Synopsys G.K.)

**読後のご意見をお送りください**

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

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

一般社団法人 情報処理学会 会誌編集部

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



アンケートページ  
QR コード

サプライチェーン・セキュリティ分野における第一人者の方々には、原稿ご執筆に多大なご協力をいただきました。年末年始にもかかわらず事務局の方を含め皆様にとって大事な時期であるにもかかわらず関係者には大変なご尽力をいただきました。

サプライチェーン・セキュリティは、サイバーセキュリティ分野の中でも今後特に重要になると考えられる分野で、進化する

新しい領域における課題と取り組みについて高度な内容を捉えつつ、読みやすさにも配慮してご執筆いただきました。

ご執筆者、関係者の尽力のおかげで、期限内に無事特集として結実し、セキュリティ分野における今後の方向性を指し示す道しるべとなることが期待されます。

石黒正揮（本特集エディタ）



## 次号（4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」面白いぞ量子技術

※本編はオンライン版のみ掲載となります

量子コンピュータのあけぼの／量子アニーリングは死んだのか？／量子技術を利用した次世代アクセラレータの活用／量子コンピュータを用いた金融計算／量子コンピュータと量子化学計算—量子コンピュータによって量子化学は恩恵を受けるのか？—／量子計算は機械学習に使えるか—近未来／誤り耐性量子計算のための量子アルゴリズム—／ダイヤモンド量子センサの可能性—ピンクダイヤモンドが高感度なセンサに—／量子暗号の原理と実用化に向けた動向—絶対安全な通信の実現に向けて—／量子コンピュータハッカソン—コミュニティによる量子人材育成—

※オンライン版のみ掲載となります

解説：「情報教育課程の設計指針」解説 ..... 萩谷昌己

教育コーナー：ぺた語義

連載：5分で分かる！有名論文ナナメ読み／情報の授業をしよう！／先生、質問です！／ビプリオ・トーク

コラム：巻頭コラム

会議レポート：VLDB 2020 会議報告

### 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は、学術目的の利用に限り、無償で転載利用いただくことが可能です。ただし、利用の際には予め申請いただくようお願い致します。

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

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

### Notice for Photocopying

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

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

<All users except those in USA>

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

<Users in USA>

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

..... 広告のお申込み .....

■ 広告料金表

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

■ 「情報処理」

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

■ 問合せ・お申込み先

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

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

..... 掲載広告の資料請求 .....

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

■ 「情報処理」 62巻3号 掲載広告 (五十音順)

富士通..... 表2       すべての会社を希望

■ 資料送付先

フリガナ お名前	_____		
勤務先	_____ 所属部署		
所在地	(〒 _____ )	_____	
	TEL ( _____ )	-	FAX ( _____ )
ご専門の分野	_____		



お問合せ・お申込み・資料請求は

広告総代理店 **アドコム・メディア(株)**

Tel.03-3367-0571 Fax.03-3368-1519 E-mail: sales@adcom-media.co.jp

## 賛助会員のご紹介

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

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

### ●●● 賛助会員 (20 ~ 50口)

**HITACHI**  
Inspire the Next

(株) 日立製作所



三菱電機 (株)

**FUJITSU**

富士通 (株)



(株) サイバーエージェント

Orchestrating a brighter world

**NEC**

日本電気 (株)



日本アイ・ビー・エム (株)

### ●●● 賛助会員 (10 ~ 19口)

**RECRUIT**

(株) リクルート

**Google**

グーグル合同会社

**docomo**

(株) NTTドコモ

**TOSHIBA**

(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

**NTT DATA**

(株) NTTデータ



GREE (株)

**Rakuten**  
Institute of Technology

楽天技術研究所

**IA Japan**

(一財) インターネット協会



(一社) 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)

**uejima**

(株) うえじま企画



エッジテクノロジー (株)

**OKI**

沖電気工業 (株)



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



コアマイクロシステムズ (株)

**SANBI**

三美印刷 (株)



(株) セプテーニ

**SONY**

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

**Panasonic**

パナソニック (株)

**MIZUHO** みずほ情報総研

みずほ情報総研 (株)

# 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&パターンソン、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  | ◇ 機動警察パトレイバー風速40メートル            | ◇ 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) |
| ◇ プログラム書法(第2版)   | ◇ ピープルウェア 第3版                   | ◇ 部分と全体 私の生涯の偉大な出会いと対話                             |
| ◇ Computer Networks 5th Edition                              | ◇ Computer Lib /Dream Machines  | ◇ 夜明けのロボット(上)(下)                                   |
| ◇ デジタル作法   | ◇ 未来の二つの顔                       | ◇ ポスト・ヒューマン誕生                                      |
| ◇ 珠玉のプログラミング   | ◇ 生体用センサと計測装置(ME教科書シリーズ)        | ◇ 理科系の作文技術   |
| ◇ Computer Architecture, 5th Edition A Quantitative Approach | ◇ Cooking for Geeks—料理の科学と実践レシピ | ◇ 現代倫理学入門  |
| ◇ Operating Systems Design and Implementation (3rd Edition)  | ◇ ハッカーのたのしみ                     | を含む40銘柄を紹介。  |

※ご注文は、お近くの書店様へ

□ お問い合わせ先

〒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>

<https://www.ipsj.or.jp/event/taikai/83/>

情報処理学会 全国大会

検索



情報処理学会

## 第83回全国大会

大会テーマ：コロナ新時代の情報処理

開催日 2021.3.18(木)～20(土)

会場 オンライン開催 (Zoom)

受付期間 2020.12.7(月)～2021.3.20(土)

聴講参加費(税込) オンライン特別価格となっております!

申込種別	費用
大会イベント企画限定聴講参加	無料
大会共通聴講参加(正会員)*全論文のPDFアクセス権付	5,000円
大会共通聴講参加(一般非会員)*全論文のPDFアクセス権付	9,000円
大会共通聴講参加(学生会員・ジュニア会員・学生非会員)	無料

皆さまざまのご参加をお待ちしております

大会イベント企画 (聴講無料)

## 3/18(木)

2020年サイバー事件回顧録  
～技術と法制度の両面から～

AI TECK TALK

コロナ新時代の情報処理(生活)

～DXによるニューノーマルの実現に向けて～  
～コンピュータバイオニアが語る～

「私の詩と真実」

「アジャイル開発のソフトウェアモデル契約」  
のその後

インダストリアルセッション

IT情報系キャリア研究セッション

## 3/19(金)

コロナ新時代を実現するデジタルトランスフォーメーション  
研究現場のデジタルトランスフォーメーションとその先にある

AI駆動型科学—ロボティック・バイオロジーによる生命科学の加速—

コロナ新時代の情報処理(教育)

～高等教育におけるニューノーマルの模索～

スポーツテック～デジタルプラクティスライブ～

New Normalにおける学会活動在り方デザイン

コロナ新時代の情報処理(研究)

～COVID-19対策における富岳の活用～

企業研究者の「熱い想い」をお届けします

量子技術を利用した次世代アクセラレータの活用

9th IPSJ International AI Programming Contest

Samurai Coding 2020-21 World Final

論文必勝法

ランチョンセッション

IT情報系キャリア研究セッション

## 3/20(土)

IPSJ-ONE

2025年実施の大学情報入試への展望

第13回情報システム教育コンテスト

初等中等教員研究発表セッション

Exciting Coding! Junior@Osaka

～みんなと一緒にプログラミングしよう～

「先生質問です!」&amp;「編集委員会」公開セッション

情報科学の達人1.0

中高生情報学研究コンテスト

IT情報系キャリア研究セッション



共催：大阪大学



後援：全国高等学校情報教育研究会

定価 1,760円 (本体 1,600円 + 税 10%)

本誌広告一手取扱い アドコム・メディア株式会社

〒169-0073 東京都新宿区百人町 2-21-27 TEL.03-3367-0571 FAX.03-3368-1519

雑誌 05269-03

4910052690318  
01600

〒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 一般社団法人 情報処理学会  
発行人 木下泰三電話 東京(03)351-8183  
振替口座 〇〇一五〇一四一八三四八四印刷所 三美印刷株式会社  
東京都荒川区西日暮里五―十六―七

会員外発売所 東京都千代田区神田錦町三―一