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

IPSJ MAGAZINE

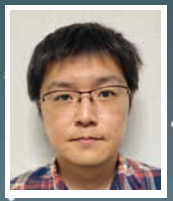
情報処理

2020
2
Vol.61 No.2
通巻 659 号

特集　ブロックチェーン技術の最新動向

特別解説　OUR Shurijo　みんなの首里城デジタル復元プロジェクト

解説　Bitcoinの革新性が導くWeb 3―cryptoeconomicsという方法論とトラストレス―



巻頭コラム

ゲームAIの進歩から見る，AI時代で大切なもの
木原直哉

電子版もご覧ください

電子版を読む（会員無料）
情報学広場

iPhoneなどで読む（有料）
Kindle

電子版を購入（有料）
Fujisan

教育コーナー：ぺた語義
連　載：IT紀行／5分で分かる!? 有名論文ナナメ読み
　　情報の授業をしよう!／先生，質問です!／ビブリオ・トーク
会議レポート

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

Interface

Interface Made in 日本

十二歳

2008年12月

ハガキサイズで実現
ゼロスピンドル・ファンレス
I/Fも回路も一切妥協なし！

開発者「(絶句)・・・。」それでも実現に走る。
熱対策▶省電力▶放熱構造とやること満載。
部品選定からすべて見直し、Atom+ オンボード SSD、ハガキサイズでファンレスを実現。
2008年12月ついに製品出荷を開始しました。

2009年12月

ブチ切りはここから始まった。

不意の停電での OS 破損は致命的。今までの PC では実現できないブチ切り機能を省エネ CD に搭載。ROM 化、EWF 運用、電源断想定の回路構成で実現。ブチ切りは、停電以外にも、一括電源 OFF、セキュリティ対策など、産業用コンピュータの新しい使い勝手を実現しました。

2009年6月

温度拡張 -30℃から +80℃
多様なストレージも必要

ファンレスで温度拡張するために、筐体、部品配置、省エネ CD から更に進化。
放熱構造を強化、各種ストレージ搭載構造、CAN 、DIO を追加搭載。温度拡張 +I/F の充実で、2009年6月リリースしました。

2010年10月

瞬停対応

省エネCD・車載 CD は、組込用途として単体運用も当然あり、瞬低対策用電源が必要。DC 電源の瞬低対策用電源は世の中にない。安全な電池の選定、発動時の振る舞いを徹底検証。屋内実験にとどまらず、自動車アクセサリ電源を使っての検証などを繰り返し、2010年10月リリースしました。

省エネ Classembly Devices®

基本は変えず、
これからも
創り続けます。

車載 Classembly Devices®

2019年 Apollo Lake 搭載省エネ CD

型式：STC-JH13B(L8XA)40A2
クアッドコア CPU AtomE39501.6GHz 搭載
動作温度　−30℃〜+60℃
GbLAN×3、USB3.0×4、シリアルポート ×2
3画面対応　DisplayPortV1.2

- 2009年10月 I/O モデル追加 最大4種の I/O カードを組合せ
- 2010年4月 片面集中モデル登場
- 2011年5月 ソルコン CD シリーズ登場
- 2011年6月 Atom E680T 搭載省エネ CD 登場 ハガキサイズで温度拡張
- 2012年5月 Atom N2800 搭載省エネ CD 登場 デュアルコア CPU
- 2014年4月 Atom E3845 搭載省エネ CD 登場 クアッドコア CPU・温度拡張
- 2015年6月 CFast3 スロットモデル 省エネ CD 登場

Interface

開発者の話 ■基板は小さいが高機能なため、部品が載らず回路を工夫した■放熱や耐振動耐衝撃のため筐体を大幅に改良■黒筐体おしかった■シミュレーションを駆使した開発■極小部品で、生産技術も苦労した■実装もハンダ付けも難しかった■評価時の部品交換さえ一苦労■機能と省電力、FAN レスをバランスしないといけない■高温でパフォーマンスを出すのが大変。■温度拡張では、これまでにない高温や低温での動作が必要。しかもファンレス。■部品の温度上昇を範囲に収めるため、検証は苦労の連続■連続稼働を意識して寿命部品を極力使わない設計をした■最新プラットフォームに対応■タフコン CD、ソルコン CD など IO を強化■Windows、LINUX に対応　■年末年始も缶詰で没頭した。■AC アダプタも温度拡張の特別製を用意した。■似たような製品が後追いでたくさん出てきて、びっくりした■業界初のオンボード SSD の信頼を問われ徹底検証■筐体が熱いと言われるたびに筐体放熱を説き続けました■CF コネクタ規格が固まらない時期に採用を決定■苦労したけどお客様に喜んでもらえてよかった。■これからも頑張って製品化を続けます。
我が子達をよろしくお願いします。

2019年 Apollo Lake 搭載車載 CD

型式：ETC-JH14B(W10XB)30A2
クアッドコア CPU AtomE39501.6GHz 搭載
動作温度　−40℃〜+70℃
ECC メモリ対応
GbLAN×3、USB3.0×2、USB2.0×4、シリアルポート ×1、CAN/CANFD×1
3画面対応　DisplayPortV1.2、HDMI 採用

- 2010年4月 車載Ⅱモデル登場
- 2011年5月 タフコン CD シリーズ登場
- 2011年6月 Atom E680T 搭載車載 CD 登場
- 2012年5月 Atom N2800 搭載車載 CD 登場 デュアルコア CPU
- 2014年4月 AtomE3845 搭載車載 CD 登場 クアッドコア CPU・温度拡張 Core i7 4650U 高性能車載 CD 登場
- 2015年6月 BOX 型コンピュータ登場 現場に置けるタフなサーバ

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

詳しくはwebsiteまで www.interface.co.jp

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

開発キット（SDK)によるクラウドアプリのプログラミング技術を競う！

THE 7TH Cloud Programming World Cup

第7回 学生クラウドプログラミングワールドカップ

表彰式：2019年11月14日（木）

WORLD CUP AWARD ワールドカップ賞

Emotional Voice Support

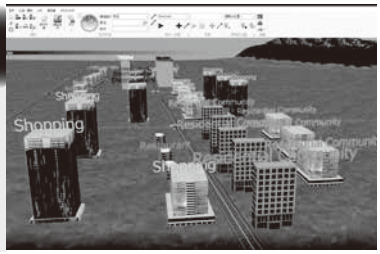
梱山女学園大学（日本）
チーム名：M's Lab

ドライバーの認知行動をサポートする本UC-win/Roadプラグインは、ドライバーの視線追跡情報を使用して「周りを見ましょう」などの適切な音声アナウンスを生成する。また、合成音声は怒り、喜び、悲しみなどの感情パターンを表現でき、感情はドライバーの状況（例えば緊急回避）に応じて選択される。交通事故を減らすことを目的とした作品となっている。

HONORABLE JUDGE AWARD 審査員特別賞

Environment Design and IT Award
福田 知弘 氏

Urban trunk road and functional area planning based on big data analysis
上海大学（中国）
チーム名：MAGIC



SNSデータ分析とモデルシミュレーションという2つのモジュールで構成された、都市全体の機能エリアと都市幹線道路を合理的に計画し、都市設計を行うシステム。

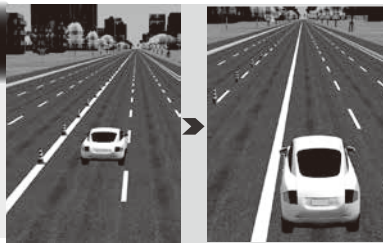
Best Optimization Award
佐藤 誠 氏

Emergency Vehicle Plugin
北京建築大学（中国）
チーム名：Brochet

自動操縦のテクノロジーとモノのインターネット機能を使って、緊急車両の交通の効率を改善する作品。EVPにより前方の民間車両に回避コマンドをリアルタイムで送信。

Creative Solution Award
楢原 太郎 氏

Tidal Lane Simulation
上海大学（中国）
チーム名：NULL



渋滞緩和のため午前中は都市に流入する方向の車線を増やし、夜のピーク時には都市部から出る車の車線を増やすよう交通流を変化させる可変式の車線を運用している。

Future transport design Award
Pencreach Yoann 氏

Implementation of digital twin for vehicle and its surroundings
国民大学校（韓国）
チーム名：KaAI

パノラマカメラとLidatセンサーを融合し車両の周囲の情報を取得。センサーからの同期画像を使用したYOLOをトレーニングデータに使用して他の車や物を検出する。

※表示価格はすべて税別です。※製品名、社名は一般に各社の商標または登録商標です。

株式会社 フォーラムエイト 東京本社
東京都港区港南 2-15-1 品川インターシティ A 棟 21F
Tel （代表）03-6894-1888 （営業窓口）0120-1888-58
Fax 03-6894-3888 | E-mail f8tokyo@forum8.co.jp
◆ショールーム：東京・大阪・名古屋 ◆セミナールーム：東京・大阪・名古屋・福岡・仙台・札幌・金沢・岩手・宮崎・沖縄／上海・青島・台北・ハノイ・ヤンゴン
FORUM 8 フォーラムエイト®
www.forum8.co.jp

情報処理学会編集の教科書シリーズ！

IT Text コンピュータアーキテクチャ 改訂2版

小柳 滋・内田啓一郎 共著　　A5判／256頁／定価（本体2,900円＋税）

コンピュータアーキテクチャの理論、技術の要点を、大学の講義に即してコンパクトにわかりやすく解説した教科書です。改訂にあたり、より大学の講義で使いやすく、現状に合った内容へと見直しを図りました。1コマ15回の講義で、コンピュータアーキテクチャの基礎から発展までを勉強できる構成です。

TCP/IP解説書の決定版！ 時代の変化によるトピックを加え内容を刷新！

マスタリングTCP/IP 入門編 第6版

井上直也・村山公保・竹下隆史・荒井 透・苅田幸雄 共著　　B5判／392頁／定価（本体2,200円＋税）

ベストセラーの『マスタリングTCP/IP 入門編』を時代の変化に即したトピックを加え、内容を刷新した第6版です。豊富な脚注と図版・イラストを用いたわかりやすい解説により、TCP/IPの基本をしっかりと学ぶことができます。プロトコル、インターネット、ネットワークについての理解を深める最初の一歩として活用ください。

ソフトウェア開発の名著、第2版登場！

リファクタリング 既存のコードを安全に改善する 第2版

Martin Fowler 著／児玉公信・友野晶夫・平澤 章・梅澤真史 共訳
B5変判／456頁／定価（本体4,400円＋税）

リファクタリングとは何か、なぜリファクタリングをすべきか、どこを改善すべきか、実際の事例で構成され、ソフトウェア開発者にとって非常に役立つ書籍です。第2版では、約20年前のオリジナル原稿の構成は変えず、大幅に書き換えられているほか、サンプルコードがJavaからJava Scriptになるなど、現代的にアレンジされています。

“わかパタ”第2版出来ました！

“続・パタ”とともによろしくお願いします！！

わかりやすい パターン認識 第2版

石井健一郎・上田修功・前田英作・村瀬 洋 共著
A5判／272頁／定価(本体2,800円+税) ISBN 978-4-274-22450-8

続・わかりやすい パターン認識 教師なし学習入門

石井健一郎・上田修功 共著
A5判／340頁／定価(本体3,200円+税) ISBN 978-4-274-21530-8

オーム社 Ohmsha
〒101-8460 東京都千代田区神田錦町3-1　www.ohmsha.co.jp
TEL 03(3233)0853　FAX 03(3233)3440　定価は変更になる場合があります。

2

PREFACE

巻頭コラム

SPECIAL ARTICLE

特別解説

SPECIAL FEATURES

特　集

ブロックチェーン技術の最新動向

ARTICLE

解説

Jr. 指標にジュニア会員向けが追加されました。

《記号の説明》

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

※各記事に指標がついていますのでご参考になさってください

IPSJ MAGAZINE
情報処理学会誌

Vol.61 No.2（2020 年 2 月号）
通巻 659 号

情報処理

■情報処理学会事務局本部
〒 101-0062 東京都千代田区神田駿河台 1-5　化学会館 4F
Tel(03)3518-8374（代表）　Fax(03)3518-8375
E-mail: soumu@ipsj.or.jp　https://www.ipsj.or.jp/
郵便振替口座　00150-4-83484
銀行振込（いずれも普通預金口座）
みずほ銀行虎ノ門支店　1013945
三菱 UFJ 銀行本店　7636858
名義人：一般社団法人　情報処理学会
名義人カナ：シヤ）ジヨウホウシヨリガツカイ
■規格部　情報規格調査会
〒 105-0011 東京都港区芝公園 3-5-8　機械振興会館 308-3
Tel(03)3431-2808　Fax(03)3431-6493
E-mail: standards@itscj.ipsj.or.jp　https://www.itscj.ipsj.or.jp/
■支　部　北海道／東北／東海／北陸／関西／中国／四国／九州

ゲーム AI の進歩から見る，AI 時代で大切なもの

■ 木原 直哉

AI対人間のゲーム勝負．オセロ，チェス，バックギャモン，将棋，囲碁とどんどんトッププロがAIに負かされ，その波は不完全情報ゲームの麻雀とポーカーにも押し寄せてきています．麻雀AIのSuphxが天鳳10段を達成したニュースは記憶に新しいところです．2017年，1対1での勝負でカーネギーメロン大学のポーカー AIが人間のトッププロに勝ち越しました．これは，プロの目から見てもはっきりと追い越されたことを認めざるを得ない内容，結果でもありました．2019年7月，フェイスブックとカーネギーメロン大学の共同チームが，ノーリミットホールデムの6人戦でトッププロに勝った，という内容のニュースが出ました．私もブログで書いていて，興味があれば検索して欲しいのですが

「今のトッププロと呼んで良いプロは実験に参加した5人中1人だけ」

「結果は実はAIが負けていて，運の補正の結果勝ちとしているが，補正の妥当性に疑問」

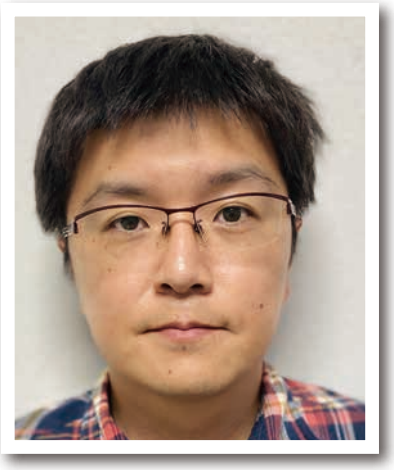
というのが現状であって，まだ人間を超えたとは言えない状況です．

さて，AIや強力なナッシュ均衡計算ツールの登場でポーカーの具体的なプレイは以前と比べてどうなったか．あくまでAIの登場前から今でもプロとしてやっている私の感覚に過ぎないのですが，

- 基本的な原則にかなり忠実であり，非常に丁寧で慎重なプレイが多い
- 一方，攻めるときは非常に大胆に攻める

■ 木原 直哉
プロポーカープレイヤー

1981年生まれ，北海道出身．2011年，1浪3留3休の末，東京大学地球惑星物理学科卒業．子どものころから色々なゲームをやり込む．大学休学中にポーカーに出会い，学費と生活費をポーカーで稼ぎながら大学に復帰．卒業後そのままプロに．2012年，WSOPポットリミットオマハ6マックスで優勝．



この2つが特徴だと感じます．ニュースでは派手なプレイが紹介されやすいですが，AIは全体として非常にディフェンシブで負けにくいプレイを選ぶ印象です．強い手をコール側にかなり回してきます．それを利用し，ベットに対して非常に広くコールしてきます．そして，状況が有利（強い手を持っている時ではなく，展開とボードが有利）な時がくると，強い手を持っていても弱い手を持っていても，綺麗にバランスを取って非常に大胆に攻めてくるのです．バックギャモンもそうです．15年前のAIもすでに人間よりはるかに強かったですが，それと比べて今のAIは，より綺麗なプレイを多く選び，基本原則から外れる美しくないプレイを否定するのです．こう考えると，2016年の将棋電王戦，佐藤名人（当時）vs Ponanzaの勝負が思い出されます．Ponanzaが，派手な手を一切出さず，ごく自然な手を積み重ねるだけで佐藤名人を圧倒して2連勝した将棋です．どうしてもこのAI時代，派手なAIの活躍が印象に残ります．しかしほとんどの局面で，AIは基本に忠実で堅実なプレイを奨励してくるのです．AIが強くなればなるほどその傾向は今のところ強くなってきているように感じます．ゲームは実生活の一部を切り取って簡略化したようなものだと私は思います．ゲーム以外において「基本とは何か」という根本的な問題は残ります．しかしAI時代は多くの人のイメージとは裏腹に，より基本に忠実であり続けることが求められる時代なのではないでしょうか．

OUR Shurijo みんなの首里城デジタル復元プロジェクト

川上　玲 | 東京大学大学院情報理工学系研究科

プロジェクトの概要

2019年10月31日に首里城で発生した火災を受けて，筆者は「OUR Shurijo みんなの首里城デジタル復元プロジェクト」[☆1]を立ち上げた．これは，一般の方から首里城の写真やビデオを収集し，在りし日の首里城の3次元モデルを復元するものである．その目的は，焼失してしまった建造物の代わりに利用できる観光資源として，収集したデータからコンテンツを作成し，首里城周辺の方々に無償で提供することにある．多数の画像からの3次元復元自体は技術的な成熟期に入っているため，3次元復元そのものよりは，写真を撮った個人の属性やその思い出と3次元モデルを紐づける方に主眼がある．すなわち，多くの人間の気配がするようなコンテンツの作成や，それによるユーザへの新しい体験の提供を目指している．興味のある方はぜひ，Webサイトの1分半ほどのビデオをご覧いただきたい．

新しい体験とは，どのようなものか．たとえば，図-1はインターネット上の画像50枚とメンバの知人の家族写真1枚から復元したモデルを示している．図に示すように，各画像のカメラ位置が，3次

☆1 https://www.our-shurijo.org

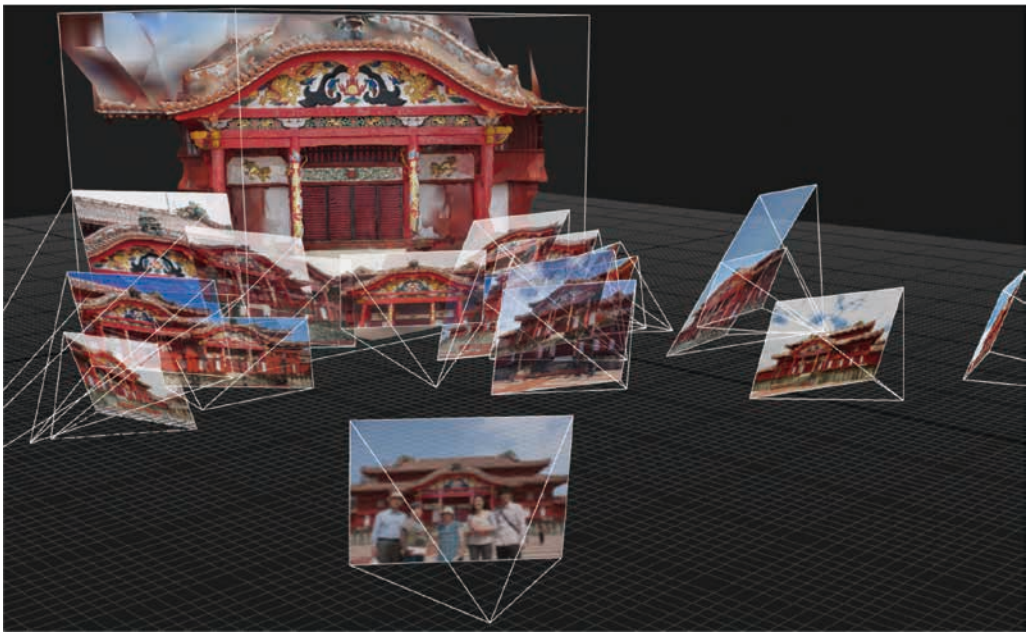


図-1
50枚ほどのインターネット上の画像とメンバの知人の家族写真から復元した首里城の3次元モデル

元復元の過程で推定できる．そこで，その場にそれを撮影した個人の思い出や画像（今回は匿名化されたものを想定）を表示する．個人の性別，年齢，出身地なども収集しているので，ユーザは首里城を通して，そこを訪れた人々を想像しつつ，その人生の一部に触れることができる．また，投稿時に撮影時期の入力が必須となっているため，時代ごとのモデルを作ることが可能である．特に，古いアナログ写真のスキャンの投稿を呼び掛けており，これらのデータから復元ができれば，世界でも例がないものができる．仮に，数十年前の写真からモデルができたとして，これに当時の思い出が付与されていたとしたら，同時代を生きたものにとって感慨深いものになるのではないだろうか．

現地にはどのように貢献できるだろうか．まず，作成した3次元モデルやコンテンツは無償で沖縄の自治体に寄付をする予定で，著作権フリーで運用していただくことを考えている．現地でAR/VRグラスやシアターなどで見られるような複数のコンテンツを届けたい．収益になりそうであれば売上は復元に活用していただければと思う．また，画像や映像の収集の際にデータの公開の可否も確認しているため，許諾があるものについては匿名化加工をした上で，無償で公開する予定である．地元の方々は写真をお持ちでない方も多いだろうから，世界中からの支援で写真が集まることや，個人の想いが可視化されて届くことで，喜んでいただけることを願う．

現在のデータ収集状況は，毎夕6時に，Twitterでbotが収集状況を報告しているので誰でも見ることができる．画像の募集は2019年11月5日に開始して，原稿の執筆時点（11月26日）で，約2,300人から2万3千ファイル，93GBが集まっている．国と地域としては，日本が5割，台湾が2割，タイ，中国，米国，ヨーロッパ各国，オーストラリアなどと続く．珍しいところではペルーやウクライナがある．思い出も全体の約半数の方からいただけており，実例がWebサイトに掲載されている．Webサイトのページビューが約32,000回，YouTubeのビデオの再生回数は約8,400回である．

今後の展望であるが，データが多ければ多いほど，観光資源としてのコンテンツが色々と作成できるはずであり，長く楽しめるものになるはずである．また，最終的には，コンテンツの作成が現地の学生の手で継承されていくよう継続性も確保するべく準備を進めている．メンバは急場の寄せ集めのチームゆえ，3月末を目途に一旦プロジェクトはけじめをつけ，NPO法人の形式として残りの宿題を継承できるように準備を整えている．ここから逆算して，2020年の成人式くらいまでに写真とビデオの募集を停止する予定である．情報処理の読者諸氏にもぜひ，データの収集にご協力をお願いしたい．特に古い写真の発掘にご協力をいただければこの上なくありがたい．

文化財のディジタル化の現在

文化財のディジタル保存に関しては，世界にさまざまな取り組みが存在する．世界的に有名なものとしては，CyArkというNPOの取り組みや，Google Open HeritageやMicrosoft AI for Cultural Heritageなど大手IT企業の取り組みがある．日本でもさまざまに取り組まれてきた[1), 2)]．筆者もe-Heritage Workshopに2010年から運営側としてかかわっている．ほかには，筆者の知るかぎり，熊本大学などによる熊本城の石垣照合システム，東京大学の大石岳史や芳賀京子らによる文化財の形状解析の取り組み，立命館大学での着物の質感のディジタル化，京都大学での高精細アーカイブ化・無形文化財のアーカイブ化，NIIによるバム遺跡の復元，などが思い浮かぶ．件の首里城に関しては，2016年にNHKが8Kカメラでヘリコプターから撮影した画像で3次元モデルを復元しており，現在Web上でインタラクティブに操作できる形で公開されている[3)]．文化財のディジタル化に関しては，近年は世

界中でさまざまなスタートアップが出始めているように思う．

OUR Shurijo チームの特色

筆者らの OUR Shurijo チームは火災後に急場で寄せ集まった集団ではあるが，さまざまな専門性を持ったメンバで構成されている．まず，Raiz New Media（スペイン）の創業者の 2 人，および，Iconem（フランス）の CEO と CTO に参加してもらうことができた．両社とも文化財のディジタル化を生業とするベンチャーで，Raiz New Media は，Flickr から首里城の写真を収集し作成したモデルを 11 月 1 日には Twitter で投稿している．Iconem はノートルダム大聖堂の火災に関し，Open Notre-Dame というプロジェクト（写真からの 3 次元復元を用いてさまざまなコンテンツを作成するもの）を Microsoft と共同で発足している．両社ともすぐにメンバに加わってくれ，データ提供や技術的な助言がすでにある．そのほかには，沖縄出身のエンジニア，建築系のスタートアップや VR コミュニティに所属する個人，3 次元復元で著名な研究者，琉球の歴史研究家，高校生の教育活動も行うファシリテータ，メディアの運営に携わる個人，メディアアーティスト，デザイナー，法律の専門家，など多様である．学生も原稿執筆時点で 6 名おり，それぞれの得意分野で活躍している．

ソフトウェアは CapturingReality 社の Reality Capture のライセンス提供を受けており，また公開されている VisualSFM, CMVS, COLMAP なども用いている．作成中のモデルは Sketchfab というモデル共有サイトにアップしていく予定である．情報処理の読者諸氏にも時々 Web サイトを覗きにいらしてモデルの進捗を確認しつつ，写真提供などで，ぜひプロジェクトにご協力をいただければと思う．最終成果も楽しみにお待ちいただきたい．

参考文献

1) Ikeuchi, K., Oishi, T., Takamatsu, J., Sagawa, R., Nakazawa, A., Kurazume, R., Nishino, K., Kamakura, M. and Okamoto, Y. : The Great Buddha Project : Digitally Archiving, Restoring, and Analyzing Cultural Heritage Objects, International Journal of Computer Vision 75(1): pp.189-208 (2007) .
2) Ikeuchi, K. and Miyazaki, D. Eds. : Digitally Archiving Cultural Objects, Springer (2008).
3) https://www.nhk.or.jp/vr/AR/shurijo/

（2019 年 12 月 2 日受付）

■川上　玲（正会員）　rei@hc.ic.i.u-tokyo.ac.jp

2008 年東京大学大学院情報理工学系研究科博士課程修了．博士（情報理工学）．同大学院情報学環などを経て 2018 年より同大学院特任講師．コンピュータビジョンに関する研究に従事．

2020 年度会誌「情報処理」および「デジタルプラクティス」モニタ募集のお知らせ

会誌編集委員会
デジタルプラクティス編集委員会

会誌「情報処理」および「デジタルプラクティス」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　「情報処理」巻末の所定用紙または学会 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（2020 年 4 月～ 2021 年 3 月）．**＊最長 3 年までとします．**
対 象 号　会誌「情報処理」61 巻 5 号～ 62 巻 4 号，および年に 4 回 Web ページ（https://ipsj.ixsq.nii.ac.jp/ej/（PDF 版））（https://www.ipsj.or.jp/dp/contents/publication/index.html（HTML 版））にて公開される「デジタルプラクティス」（電子版のみ）．
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　**2020 年 2 月 27 日（木）必着**
＊申込書を Fax するか，または E-mail でお申し込みください．
＊ Web ページ（https://www.ipsj.or.jp/magazine/topics/2020monitor.html）でも受け付けています．
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／照会先　情報処理学会　会誌編集部門（モニタ係）

2020 年度会誌「情報処理」および「デジタルプラクティス」モニタ申込書

宛先：情報処理学会　会誌編集部門（モニタ係）　E-mail: editj@ipsj.or.jp　Fax(03)3518-8375

氏　名

会員番号　（　　）

住　所　〒

所　属
E-mail:
Tel（　　）　　-
Fax（　　）　　-
年　齢　（　　歳）

業種：(a) 企業（サービス業）(b) 企業（製造業）(c) 研究機関 (d) 教育機関（小・中・高校・高専・大学・大学院など）
(e) 学生 (f) 学生（ジュニア会員）(g) その他

職種：(a) 研究職 (b) 開発・設計 (c) システムエンジニア (d) 営業 (e) 本社管理業務 (f) 会社経営・役員・管理職
(g) 教職員（小・中・高校・高専・大学・大学院など）(h) 学生 (i) 学生（ジュニア会員）(j) その他

要望，コメントなど：

特集
Special Feature

ブロックチェーン技術の最新動向

編集にあたって

吉濱佐知子 日本アイ・ビー・エム（株）

サトシ・ナカモトを名乗る人物がビットコインの論文を発表して10年が経過しました．現在世の中に流通している仮想通貨（暗号資産）は数百種類以上もあり，新技術の発表や取引所への攻撃など，さまざまな観点で連日ニュースを賑わせています．一方，企業間コンソーシアムなどのクローズドな環境でブロックチェーンを使う試みも多く，国内外の銀行間コンソーシアムや証券市場，貿易金融やサプライチェーンなど，多くの取り組みが発表されており，実証実験を超えた本格運用への移行もはじまっています．

このように注目を浴びているブロックチェーン技術ですが，技術的に正確な理解をするのが時として困難となっています．ひところのブロックチェーンブームのおかげで，ブロックチェーンの基本的な仕組みについて解説した記事は比較的多くなってきています．一方，ブロックチェーンの実装は非常に多くの種類がありますが，比較的未成熟な技術であるために，常に新しい方式が提案され，日進月歩の進化を遂げています．こういった「基本」を超えた一歩先の取り組みについては，まとまった技術情報がなかなか見つからないというのが実情です．

本特集は，ブロックチェーンに関連する技術の最新動向について解説を行い，今後の技術開発を促進するための基礎となるような情報を提供することを目指して企画いたしました．

なお，いわゆるブロック構造のデータを持たない実装もあることから，一部の記事ではブロックチェーンの代わりに分散台帳技術（DLT：Distributed Ledger Technology）という語を用いていますのでご了承ください．

佐古和恵氏，古川諒氏，中川紗菜美氏の共著による「**Bitcoin技術のその後の動向**」では，現在ビットコインの抱えるさまざまな課題を解決する取り組みについて，解説を行っています．特にビッ

トコインは単位時間あたりのトランザクション処理件数が少ないという課題があり，これを回避するためにブロックチェーンの外で処理を行う仕組みがいろいろと考案されています．また，新しい暗号アルゴリズムを用いて複雑な取引条件を実現する仕組みについても解説しています．

ブロックチェーンは分散台帳技術であるために，参加者すべてに台帳の情報が共有されるという性質があり，取引のプライバシが保護できないことが懸念されます．長沼健氏の**「分散台帳上での匿名送金とその監査について　ゼロ知識証明を利用したセキュアプロトコル」**では，zk-SNARK というゼロ知識証明プロトコルによる，取引のプライバシ保護の仕組みについて解説しています．

松尾真一郎氏の**「ブロックチェーンの安全性―攻撃や脆弱性とその対策―」**では，ブロックチェーンで満たすべきセキュリティ目標とはなにか，またそれを実現するために必要な技術はなにかということを，6 つのレイヤに分類して解説しています．また，現在知られている代表的な脆弱性を紹介するとともに，将来的な暗号の危殆化などの懸念に対する考察を行っています．

齋藤新氏の**「分散台帳技術におけるコンセンサス・メカニズム」**では，ブロックチェーンで使われる分散合意アルゴリズム（コンセンサス）の仕組みを中心に解説を行います．ビットコインを始めとする多くの仮想通貨では，Proof-of-Work（PoW）という参加者間の計算競争によってブロックを追加していく方式が取られていますが，エネルギーの無駄遣いや安全性などが問題となり，これに変わる新しいアルゴリズムが考案されています．この記事では，誰でも参加できるパブリック型と，参加許可制のプライベート型のそれぞれのタイプのブロックチェーンについて，代表的なアルゴリズムやその特徴を紹介しています．

（2019 年 11 月 18 日）

［ブロックチェーン技術の最新動向］

① Bitcoin 技術のその後の動向

基般

佐古和恵 | NEC　古川　諒 | NEC　中川紗菜美 | NEC

サトシの Bitcoin

動作概要

2008 年にサトシナカモトが考案した Bitcoin [1] の基本的な構成要素として，各アカウントが保有する「Bitcoin」を別のアカウントに移転するトランザクションと，このトランザクションデータを記録する分散台帳（ブロックチェーン）がある．各アカウントは公開鍵に紐づく．A アカウントから B アカウントに X Bitcoin（以下，資産の単位の場合は BTC と表記する）を移転するトランザクションには A アカウントの署名データが付与される．このトランザクションが発生したときに，A アカウントに X BTC が存在すると台帳に記載されており☆1，なおかつ署名データが正しければ，このトランザクションデータは分散台帳に記録され，A のアカウントの残高が X BTC 減額され，B のアカウントの残高は X BTC 増額される．分散台帳に記録される際に，トランザクションはブロック単位でまとめられ，Proof of Work（PoW）と呼ばれる処理時間がかかるコンセンサスアルゴリズムが実行される [2]．このため，多くても 1 秒にせいぜい数十トランザクションしか分散台帳に記録されない．

課題

Bitcoin 方式に関しては，多くの課題が存在する．ここですべてリストできるものではないが，主なものを挙げると，

1. PoW 方式に起因して，多くの計算機資源が必要になること
2. 単位時間に取り扱えるトランザクションの数が少ないこと
3. トランザクションが将来にわたって確定するという保証はないこと
4. すべてのトランザクションが公開されているため，いつどの口座間でどのくらいの取引があったかが周知になってしまうこと
5. 支払条件を限定的にしか表現できないこと

がある．それぞれについて，いくつかの代替案が提案されている．たとえば，計算資源の課題 1 には PoW 方式の代わりになる PoS（Proof of Stake）方式などが提案されている．課題 2 に関しては，1 つのブロックにより多くのトランザクションが含められるように，ブロックのサイズを大きくする案や，ブロックに記載するトランザクションのサイズを小さくする Segwit（Segregated Witness）☆2 などの案が提案され，一部実用化されている．課題 3 はファイナリティの問題と呼ばれ，PoW 方式に起因する．そこで，誰もがノードになれる現行の Permissionless 方式ではなく，ノードになる人が事前に決められている Permissioned の方式が考えられている．課題 4 のプライバシに関しては Zcash☆3 など，新たな方式が提案されている．課題 5 に関しては，支払条件をスマートコントラクトとして表現できる Ethereum などの方式が開発されている．

☆1 具体的には，台帳には，A アカウントが使える残高を表現する UTXO と呼ばれる複数のパラメータで表現されている．

☆2 https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki

☆3 https://z.cash/

本稿の概要

本稿では，上記の課題 2 に対して，PoW 方式はそのままで，Bitcoin の外部においたメカニズムによって，多くのトランザクションが高速に実施できる Payment Channel 手法について紹介する．また課題 5 の対策として Bitcoin の機能を拡張するため，ほかのブロックチェーンに資産移転する Side-chain と呼ばれる方式を紹介する．さらに Bitcoin に使われている署名方式を Schnorr 署名に変更することで同じく課題 5 に対応する方式も述べる．

Payment Channel

前述したとおり，Bitcoin は単位時間あたりに処理できる取引量が小さい．これを解決するために提案されたのが Payment Channel と呼ばれる技術である．

通常，Bitcoin で取引をする際には取引ごとにトランザクションを作成し，それぞれが台帳に記載される必要がある．これに対し，Payment Channel はトランザクションを Bitcoin の外側（off-chain）で一時的に保持するようにし，あるタイミングで複数の取引による最終結果のみをまとめて台帳に反映する技術である（図 -1）．

これにより台帳に記載するトランザクション数が減少するため単位時間で可能な取引数を向上できる．ここでは，特定の 2 者間で単方向および双方向に支払いが可能な Micro Payment Channel と，それを用いて任意の 2 者間での取引を実現する Lightning Network について述べる．

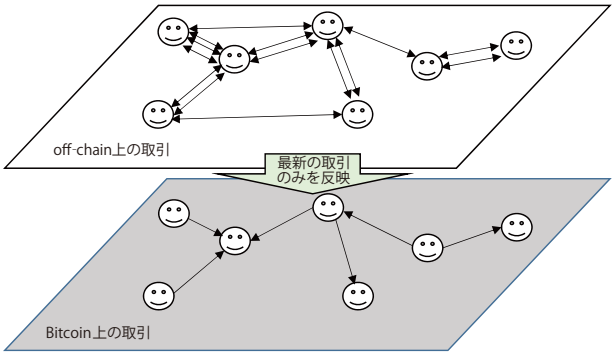


図 -1　Payment Channel の概要

単方向の Micro Payment Channel

まずは 2 者間で単方向の支払いが可能（A から B へは可能だが B から A は支払い不可）な Micro Payment Channel 技術について述べる．ここでは，たとえば，ビデオの毎分視聴するごとに料金を Bitcoin で支払う場合を考えてみよう．

複数の取引をまとめて処理をする場合，途中の取引内容は台帳に記載されないため，正しく取引が処理されずに一方が損をする可能性がある．このため，Micro Payment Channel では相手に不正をされても他方が損をしないような工夫をしている．その工夫の 1 つは，Bitcoin に実装されているマルチシグ口座を活用する．A と B のマルチシグ口座とは，A と B の両方が署名をしないと，この口座からの Bitcoin を移動できないというものである．

A から B への支払いを頻繁に行う場合，まず A が保有する Bitcoin の一部を，A と B のマルチシグ口座に移動するトランザクションを発行する．これが Bitcoin の分散台帳に記載されると，この額がマルチシグ口座にデポジットされたことになる．以後，この講座をデポジット口座と呼ぶ．

今後，A から B に Bitcoin で支払う場合には，A はこのデポジット口座から B に支払うトランザクションデータを作成して，署名して B に渡す．たとえば 1BTC をデポジットしていて 0.1BTC を支払う場合には，「デポジット口座から B に 0.1BTC，A に 0.9BTC を移転する」というトランザクションに A の署名を付与して B に送るのである．このトランザクションが B に署名され，Bitcoin の台帳に記載されれば B は 0.1BTC を入手できる．しかし，これでは通常の Bitcoin より高速にならない．

そこで，B は次の A の支払いまで待つのである．A は次の 1 分を視聴したら，今度は「デポジット

口座からBに0.2BTC，Aに0.8BTCを移転する」というトランザクションデータに署名してBに送る．このように，視聴時間が経過するたびに累計したトランザクションデータを作成してBに送る．視聴が一段落した，あるいはデポジットが空になった段階で，Bは最後のトランザクションデータに署名する．このトランザクションがBitcoinの台帳に記載されることで取引の総計が反映される（図-2）．

ただし，Bがトランザクションを Bitcoin の台帳に記載しなかった場合，デポジット口座は塩漬けになってしまう．この問題を解決するために，「一定時間たてばAの署名だけでもデポジット口座からの移動を可能とする」[☆4]，という条件を付けてデポジット口座を作成する．これによりBが一定時間の間にトランザクションを記載しなければ，Aはデポジット口座から資金を回収できるのである（図-3）．

なお，一定時間後に資金移動が有効になる機能（script）はBitcoinのTime Lock Contract（TLC）と呼ばれる．のちに紹介するLightning Networkでは，これに加えてハッシュ値の有無により，口座に振り込まれるかどうかを決定するHash Time Lock Contract（HTLC）scriptも登場する．

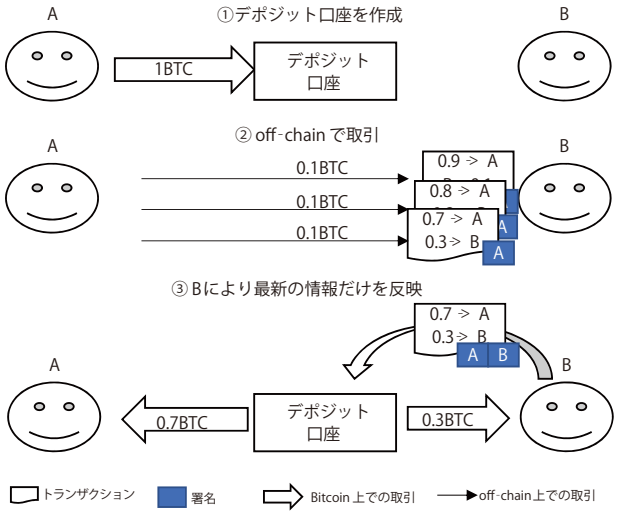


図-2　単方向の Micro Payment Channel

☆4　あるブロックの高さ以上でなければ口座から移動するトランザクションは有効にならない，と指定することにより実現される．

双方向の Micro Payment Channel

双方向の Micro Payment Channel では取引を行う両者がそれぞれ資金を出し合ってデポジット口座を作成し，お互いが最新取引を反映したトランザクションを持ち合い，どちらかが最新のトランザクションを Bitcoin の台帳に記載することで複数の取引をまとめて反映する（図-4）．

Bitcoin の移動が単方向の場合には取引を重ねるたびに受け取り側が受け取る金額が高くなるため，最新のトランザクションを Bitcoin の台帳に記載するのは当然であったのに対し，双方向の場合はチャネルに参加する両者にとって最新の取引を反映したトランザクションを送信するのが最良であるとは限らない．このため，最新でないトランザクションを送信した場合にペナルティを与える仕組みが必要である．

たとえば，AとBが同額をデポジットしたAとBのデポジット口座から「Bに0.8BTC, Aに0.2BTCを移転する」という取引1（図-4の②における2番

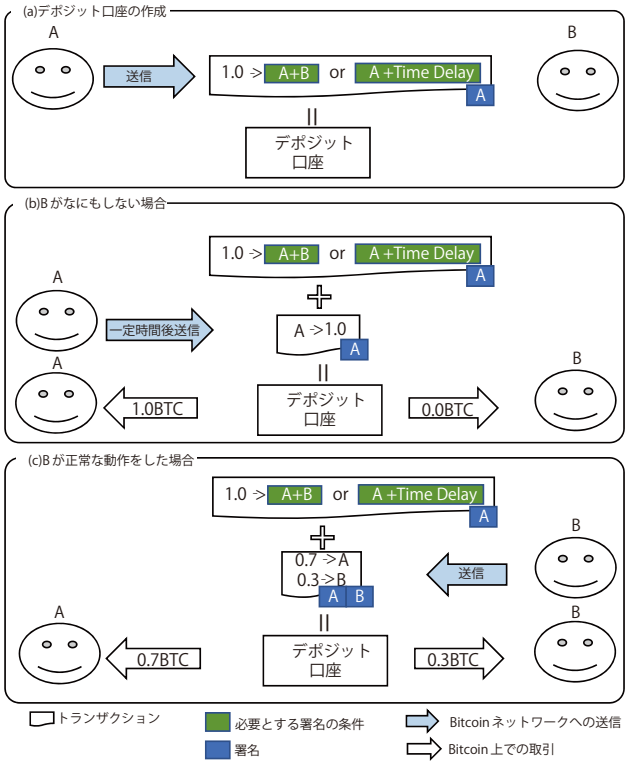


図-3　デポジット口座の塩漬けの防止

目の取引を指す）のあと，「A から B に 0.1BTC を移転する」という取引（図 -4 の②における 3 番目の取引）を行う場合を考える．この場合，2 つの取引の総和として「デポジット口座から，B に 0.9BTC，A に 0.1BTC を移転する」という取引 2 に更新されるべきである．しかし A にとって取引 2 でなく取引 1 を有効にした方が得になるので，B は A が取引 1 を有効にすることを防がないといけない．

そこで B は「B に 0.8BTC，A に 0.2BTC を移転する」という取引 1 において TLC を用いて「A への 0.2BTC は一定時間がたたないと移動できず，さらにこの 0.2BTC は A と B のデポジット口座へはいつでも移動できる」という条件を指定した取引にする．さらに，取引 2 の直前に，取引 1 が台帳に記載された場合に，「A への 0.2BTC は A と B のデポジット口座を経て B に移転する」というトランザクション（BRT, Breach Remedy Transaction）に A の署名を得る．これをもらっておいてから，取引 2 を実行すれば，A は不正をするインセンティブがなくなる．なぜならば，取引 1 に A の署名を追加して取引 1 を確定させても，自分の口座にいれるには時間がかかり，さらにその間に B が BRT を使って B の口座に移転させてしまう恐れがあるからである．

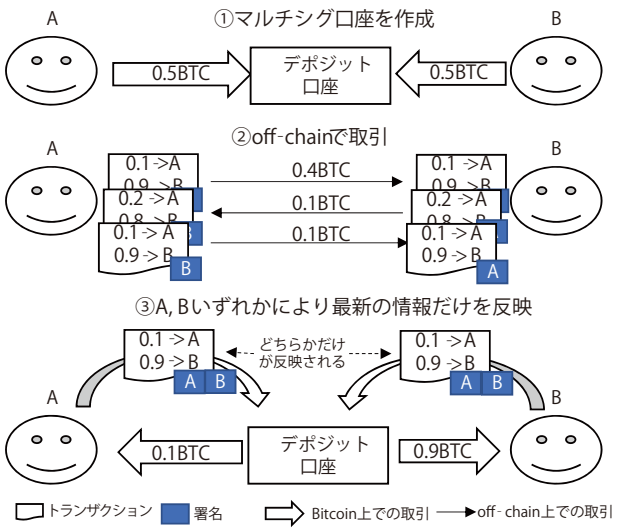


図 -4　双方向の Micro Payment Channel

上記は，A の不正を防止する観点で B が作成する取引について述べたが，同様に A も，B の不正を警戒して対称的に同じトランザクションを実施する．このような複雑な仕組みにより両者が最新の取引を Bitcoin に反映するように誘導し，双方向に支払いが可能となるのである．

Lightening Network

Micro Payment Channel では取引する 2 者ごとにデポジット口座を作成する必要があった．このため，ある利用者が 100 人の相手と Payment Channel による取引をしたければ，大量の Bitcoin をデポジットしなければならず，現実的には不可能である．

Lightning Network[3] はこの問題を解決するために生まれた技術である．Lightning Network では 2 者間の取引をリレーすることで，たとえばユーザ A とユーザ B，ユーザ B とユーザ C の間に Micro Payment Channel が存在すれば，A と C の間でも取引が可能である（図 -5）．これにより A と C の間のデポジット口座なしに A と C の間で取引ができる．

Micro Payment Channel をリレーする上で最も問題となるのは仲介するユーザによる持ち逃げである．たとえば A から B を経由して C に支払いを行う場合に，A から B に支払われた段階で B が C に支払わなければ B による持ち逃げが可能となる．

このような仲介者による持ち逃げを回避するための方法として，次のような手続きが提案されている．まず，最終的な支払先（A から C に支払う場

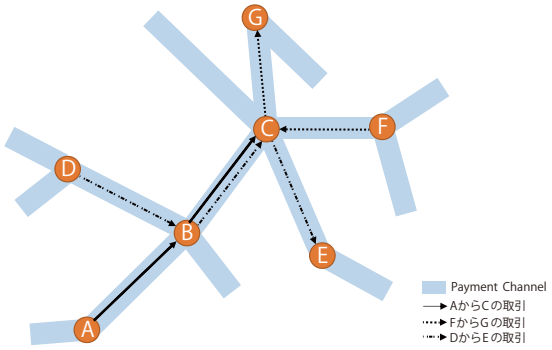


図 -5　Lightning Network のイメージ

合にはC）がランダムな数Rを作成し，これをハッシュ化したH＝h(R)を支払元（この場合はA）に送付する．Aは仲介をするBに対して支払いを行うが，このときにBがある期間内にH＝h(R')となるR'を送らないと，自分の口座にはいらないような条件を指定する．（これをHTLC（Hashed Time Lock Contract）と呼ぶ）．このようにすることで，R'を知らないBは自由に資産を入手することはできなくなる．同様にBからCへの支払いについても，R'をCが知っている場合にのみCへ資産移転が可能になる．CはR'の1つであるRを知っているため，資産を入手可能である．Cは自分への支払いを有効化する際にRを公開するため，ほかの仲介者もそれぞれ支払われたコインを使用できるようになる．図-6ではAとBの間にそれぞれ0.5BTCずつ拠出しているデポジット口座，BとCの間に同様に0.5BTCずつ拠出している口座がある場合に，HTLCを使用してAからCに0.1BTCの取引をBを経由して行う例を示している．このような仕組みにより，仲介者はリスクなく支払いを仲介できる．

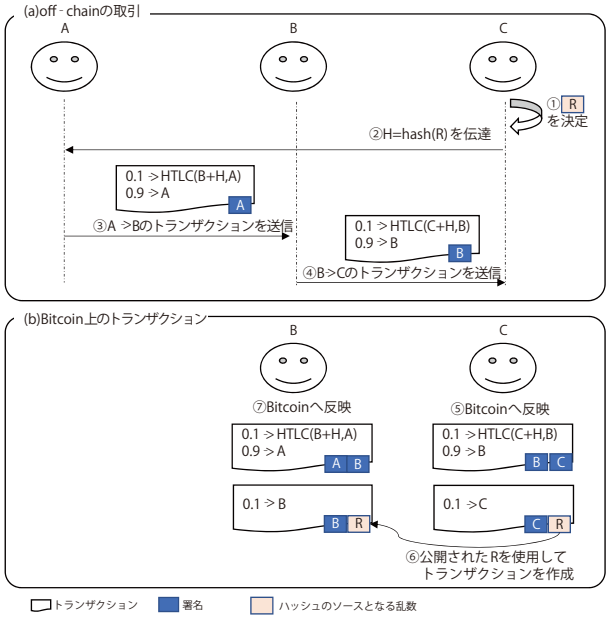


図-6　HTLCを使用したリレーの仕組み☆5

☆5　図-6中のHTLC（B+H,A）はBの署名+R′または一定時間後にAの署名で使用可能な口座を表す．

ブロックチェーン間の移転

Side-chainの概要

Side-chainとは複数のブロックチェーン間で資産を移動する技術を用いて，Bitcoinではサポートされていない機能の追加を別のブロックチェーンで行うことを可能としている．Side-chainの主な目的はこのようにBitcoinの機能拡張ではあるが，Bitcoinに記載されるトランザクションの量が減ったり，高速なSide-chainを採用することで結果的にスループットの向上にも寄与する．先に記述した課題2や5への対策になる．

Side-chainの実現例

では，Side-chainではどうやって複数のブロックチェーンの間で資産を移動するのであろうか．

資産移動の方法の1つとしてFederated pegと呼ばれる方法が用いられている．Federated pegでは信頼できる複数の運営者からなる運営チームの存在を仮定している．Bitcoin上でAから運営チームのマルチシグ口座へのトランザクションが台帳に記載されると，Side-chain上では運営チームのマルチシグ口座からSide-chain上のAの口座宛のトランザクションが送信され，AはSide-chain上での取引が可能となる．Side-chainでの取引後にAの資産をAのBitcoin上の口座に戻す際には，運営チームの仲介を経て逆の工程が実行されることになる．

しかしながらFederated pegでは仲介の運営チームやSide-chain上のルールを信頼する必要があり，Bitcoinのトラストモデルが変わってしまうとの指摘もある．

仲介不要のAtomic Swap

2つのブロックチェーン間の資産を仲介者なく交換することを目的にAtomic swapと呼ばれる手法の研究も近年さかんになっている．これを応用して，Side-chainを実現する方法もある．ここでは，

HTLC 機能がある 2 つのブロックチェーン間の資産を交換する手法を紹介する．

たとえば，A は Bitcoin の暗号資産を持ち，B は Litecoin と呼ばれる別の暗号資産を持っているとする．お互い，すでに合意した交換レートで A は B に Bitcoin を，B は A に Litecoin を渡すとする．A, B それぞれ Bitcoin ならびに Litecoin に口座を持っている前提である．

まず，HTLC に使うハッシュ値 H＝h(R) を A が決め，A は，Bitcoin 上で，H＝h(R') となる R' を示した場合にのみ，B に資産移転ができるようにするトランザクションを作成し，台帳に記載する．これを確認した B は，同様に Litecoin 上で，R を示した場合にのみ，A に資産移転ができるようにするトランザクションを作成し，台帳に記載する．そして，A は Litecoin 上で R を公開して，この資産を入手する．このとき，公開された R を使って，B も Bitcoin を獲得でき，中間者を介さずに資産交換ができることになる．

Schnorr 署名の活用

本章では，Schnorr 署名と呼ばれる Schnorr が提案した準同型性のある署名アルゴリズムを使って，Bitcoin の機能を拡張する方式を紹介する．ここで準同型性とは，同じメッセージ m に対して，公開鍵 Y1 と Y2 の署名から，公開鍵 (Y1＋Y2) の署名を合成できることを指す．

Schnorr 署名

現在，Bitcoin で活用されている署名は ECDSA 署名（Elliptic Curve Digital Signature Algorithm）である．ECDSA 署名も Schnorr 署名も，楕円曲線 E 上の点 G を用いて位数 q の巡回群を構成し，秘密鍵 x に対して Y＝xG が公開鍵となる．どちらの方式も，hash 関数 h とメッセージ m に対して署名時に乱数 r を生成する．ECDSA の署名要素 s は s＝(h(m)＋[rG]x))/r mod q であらわされる．なお，ここで [rG] は，点 rG の x 座標の値を示す．

Schnorr の署名要素 s は s＝r－h(m||[rG])x mod q となる．ここで, || は連結である．どちらも署名データを (s, rG) とする☆6．

ECDSA 署名の検証は，srG＝h(m)G＋[rG]Y であるかどうかを確認する．Schnorr 署名の検証は sG＝R－h(m||[R])Y を確認する．

Schnorr の方式の準同型性について述べる．秘密鍵 x1, x2 と対応する公開鍵 Y1, Y2 に対して，署名者 1 と署名者 2 がそれぞれ乱数 r1, r2 を生成し，お互いに R1＝r1G, R2＝r2G を送り合った上で，下記のデータを作成する．

s1' ＝ r1－h(m||[r1G＋r2G])x1 mod q

s2' ＝ r2－h(m||[r1G＋r2G])x2 mod q

このとき，Schnorr 署名の準同型性により署名 (s1'＋s2', r1G＋r2G) は，公開鍵 Y1＋Y2 に対する正しい署名になっている．

これは，Y1 と Y2 のマルチシグ口座に対する署名が 1 つの署名で構成できるということと，お互いに秘密鍵をもらさずに相互に正しく署名を生成していることが確認できることを意味している．

Discreet Log Contract

次に，この Schnorr 署名を応用して，従来の Bitcoin の script では表現できなかった支払条件を安全に付与することができる Discreet Log Contract[4] と名付けられた方式を紹介する．Bitcoin の script を使わずに支払条件を規定できるため scriptless script と呼ばれる方式の 1 つである．

実現する契約例

この方式で実現する支払条件は，A と B がたとえば，今週末の金曜日に Z 社が発表する価格で取引をする，ということをその週の月曜日に契約する方式である（図 -7）．

☆6 Schnorr の署名データを (s, c=h(m||[rG])) の対とする場合もある．

Z社の役割は，発表する価格Pに対して，Z社の署名を付けることと，そのとき利用する署名に使う乱数rについて，R＝rGをあらかじめ公開しておくことである．

準備

まず，Micro Payment Channelのように，AとBのマルチシグ口座を設立し，そこにAとBは同額（M BTC）をデポジットする．以後，この口座をデポジット口座と呼ぶ．週末の発表価格の可能性がP1からPnである場合，Aは各Piについてトランザクションを作り自分の署名を付与し，Bに送付する．すなわち，Aは，デポジット口座からBのPiマルチシグ口座にM＋Pi BTCを，残りのM-Piを自分の口座に移動させるトランザクションを作り自分の署名を付与してBに渡す．Bは受け取ったデータの正しさを確認する．

ここでBのPiマルチシグ口座とは，Bの公開鍵と価格Piから生成される口座であり，Z社がRを用いてPiの署名を発表したら[☆7]，Bがその口座から資金を移動できるものである．

Bの Pi マルチシグ口座の作り方

変形Schnorr署名を用いる場合，会社Zの公開鍵Yzに対して，Zの価格Piに対するRを用いた署名siというのは，siG＝R－h(Pi||[R])Yzを満たす．この右辺は，署名siを知らなくても作成できるものである．そこで，Piのマルチシグ口座は，Bの公開鍵YBに，この右辺の値，すなわちsiGを加えたものとする．これらは公開されているものなので，誰でも作成することができる．

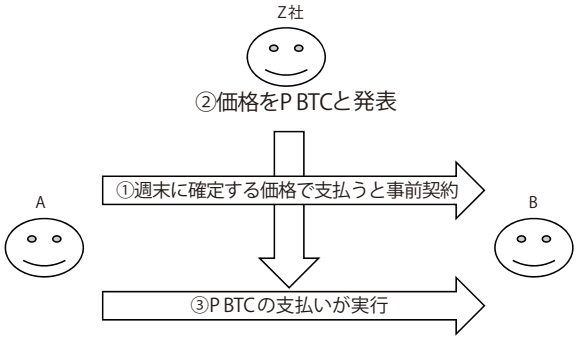


図-7　Discreet Log Contract による契約例

☆7 Z社はTrusted Third Partyであるという仮定を置いており，AまたはBと結託して不正な価格を発表することは想定していない．

価格 Pi の発表前の不正防止

Aは準備したトランザクションにAの署名をしてBに渡す．この準備の段階ではBにはメリットはない．これらのトランザクションにBが署名を付与して台帳に記載することは自由に行えるが，A,Bマルチシグ口座の残高を考慮すると，このうち1つの移転しか有効にならない．価格が発表される前に，どれか1つのトランザクションに自分の署名を追加して台帳に記載しても，その価格が発表されなければ，そのPiマルチシグ口座から自分の口座へと資金移動ができないので，塩漬けになってしまう．したがって，この時点ではBは何も不正を働くことはできないのである．

価格 Pi の発表後の手続き

会社Zが週末の金曜日に決定した価格Pkの署名skを，事前に公表したRを用いて発表すると，Bは，デポジット口座から自分のPkマルチシグ口座にM＋Pk入金されるトランザクションに署名し，台帳に記載する．さらに，この口座から自分の口座に戻すトランザクションを発行する必要がある．

この移動するためにはBのPkマルチシグ口座の公開鍵に対する秘密鍵が必要になる．BのPkマルチシグ口座の公開鍵とは，Bの公開鍵YBにskGを加えたものであり，その秘密鍵はBの秘密鍵にskを加えたものであるため，Bは容易に計算することができ，無事所定額を入手できることになる．AはBがこれらの処理を実行してくれたら，残高が自分の口座に振り込まれる．

持ち逃げ対策

ここで，どちらかが正しく処理を実行しなかった場合に備えた対策について述べる．まず，Aが正しく処理を実行しなかった場合に備えて，BもAと対称の同様のトランザクションを作成してAに送る．そして，A, Bともにトランザクションがそ

ろったところで，デポジット口座に入金をする．また，一方が間違ったトランザクションを発行してデポジット口座の金額を塩漬けしてしまった場合に備えて，一方の Pi マルチシグ口座からの引き落としが一定時間なく，タイムアウトした場合には，自分の口座に取り込めるようなトランザクションにする，という工夫が必要である．

技術と普及について

Bitcoin の希少性から，暗号資産として保有したり，投資目的で売買したりする人が増え，その人たち向けに，自身が保有する Bitcoin を円やドルと交換する交換業者がサービスを開始している．

2008 年にサトシナカモトが考案した Bitcoin は粗削りだがあまりに衝撃的であった．それ故，さまざまな改良を加えようとする技術の発展の流れと，粗削りなまま実際に使っていこうとする社会の流れがあった．技術が広く普及すると，その技術を改良することが難しくなる．そのため，Bitcoin の改良を試みるさまざまな亜種が出現する一方，元々の Bitcoin はそのままで，それにアドオンする形で課題を解決する方式が乱立している．必ずしも技術者が良いと思う方式が広がるわけではない中で，これからも Bitcoin 技術の改良は多産多死で続いていくのであろう．

参考文献

1) Nakamoto, S. : Bitcoin : A Peer-to-Peer Electronic Crash System (2008).
2) 佐古和恵：フィンテック：2. 透明性と公平性を実現するブロックチェーン技術，情報処理，Vol.57, No.9, pp.864-869（Sep. 2016）.
3) Poon, J. and Dryja, T. : The Bitcoin Lightning Network : Scalable Off-Chain Instant Payments, https://lightning.network/lightning-network-paper.pdf (2016).
4) Dryja, T. : Discreet Log Contracts, https://adiabat.github.io/dlc.pdf (2019).

（2019 年 10 月 8 日受付）

佐古和恵（正会員） KazueSako@nec.com
京都大学理学部（数学）卒業．セキュリティとプライバシを両立させる電子投票，電子抽選，匿名認証などの研究に従事．ISO TC307 ブロックチェーンと分散台帳技術　国際エキスパート．日本学術会議連携会員．博士（工学）．

古川　諒（正会員） rfurukawa@nec.com
2008 年東京工業大学総合理工学研究科博士前記課程修了．同年 NEC 入社．以来，アクセス制御，プライバシ保護，ブロックチェーンの研究に従事．

中川紗菜美 sanami-nakagawa@nec.com
筑波大学大学院システム情報工学研究科リスク工学専攻修了後，NEC にて，ブロックチェーン応用などの研究開発に従事．

［ブロックチェーン技術の最新動向］

② 分散台帳上での匿名送金とその監査について
ゼロ知識証明を利用したセキュアプロトコル

長沼　健　日立製作所

技術背景：透明性 vs 匿名性

近年，Bitcoin，Ethereum をはじめとする暗号通貨，およびそのコア技術であるブロックチェーンが新しい決済システムの基盤として大きな注目を集めている．Bitcoin などのブロックチェーンベースの暗号通貨の特徴として，銀行などの中央機関を必要とせず（非中央集権），低い手数料で決済処理を行える点が挙げられる．たとえば，Bitcoin ではオープンな P2P ネットワーク上に送信された取引情報（以下，トランザクションと呼ぶ）を不特定多数のマイナーと呼ばれるノードが正当性を確認した後，ブロックにまとめられ，Proof-of-Work（PoW）と呼ばれる特定の閾値以下のハッシュ値を求める作業を行うことで承認処理を行っている．承認されたトランザクションは，ブロックチェーンと呼ばれる P2P ネットワーク上の分散台帳に記録される．また，Bitcoin のトランザクション，および分散台帳は，P2P ネットワーク上の全ノードが参照可能であるため，どのユーザからどのユーザにコインの送金が行われたかといった取引に関する情報は，ネットワーク参加者全員が確認できる．結果，非常に透明性の高い送金システムといえるが，一方でこの透明性は，セキュリティの文脈において匿名性と背反する☆1．当然，トランザクションを生成するユーザが，送／受金者，送金額などの機微情報を暗号化することで匿名性を確保可能だが，マイナーがトランザクションの正当性を確認できないといった問題が発生する（たとえば，UTXO：Unspent transaction output モデルにおいてトランザクションの input の金額の合計値は output の合計値と一致しているか，であったり，送金額は正の値か，といった正当性の確認ができない）．

この相反する透明性と匿名性を両立するためにゼロ知識証明と呼ばれる技術の利用が検討されている．たとえば，Zcash（暗号通貨の名称）では，zk-SNARK[1)] と呼ばれるゼロ知識証明プロトコルを用いて，この問題を解決している．具体的には，Zcash ではユーザがトランザクションの送／受金者，送金額といった機微情報を暗号化しつつ，zk-SNARK を使ってマイナーにその正当性を証明することでトランザクションの承認処理を行っている．

本稿では，Ethreum 等でも利用が検討されているこの zk-SNARK と，それを用いた匿名送金機能（Zcash プロトコルの一部）を暗号技術の非専門家向けに解説する．さらに，このような匿名性の高い暗号通貨が，マネーロンダリングなどの不正な送金手段として利用される恐れが指摘されているが，ゼロ知識証明を用いることで，適切な監査機能を実現できることも紹介する．そして最後に，これら暗号通貨，匿名送金機能，その監査の実社会での利用にあたっての課題を述べたい．

☆1　本稿では，匿名化という言葉を「どのノードからどのノードにいくらの送金が行われたか」といった送／受金者のリンク情報，および金額の秘匿化といった意味で用いる．Bitcoin などの暗号通貨では，ノードの ID（アドレスと呼ばれる）はユーザの本名ではなく，ランダムなバイナリ値に仮名化されているため，通常の意味で，ある程度の匿名性は確保されている．

ゼロ知識証明の分散台帳への応用

本章では，ブロックチェーン上での匿名性確保，およびトランザクションの正当性検証に，ゼロ知識証明がどのように利用されているかを解説する．

ゼロ知識証明とは？

ゼロ知識証明とは，ある命題 X（多くの場合，秘密情報に関係する）に対して，証明者 P と検証者 V の間でデータを送受信し，P が V に命題 X が正しいことを確信させ，かつ命題が正しいこと以外の情報を V に与えないプロトコルである．この定義だけでは，何を意図しているのか分かりづらいので，以下，ゼロ知識証明の具体例を見ていく．

たとえば，証明者 P は，アルゴリズムが公開されているハッシュ関数 H とその出力値 A に対して，$H(x)=A$ となるような秘密の入力値 x を知っていることを検証者 V に証明したいとする．当然，P は V に x を開示することで知識を有していることを証明できるが，秘密の入力値 x が漏れてしまいゼロ知識証明とはならない．ゼロ知識証明プロトコルでは，x の代わりに x から生成されるゼロ知識証明値 π を証明者 P が計算し，(π, H, A) を検証者 V に渡し，V が特別な検証処理を行い，V は「命題:P が $H(x)=A$ となるような秘密の入力値 x を知っている」を確認する．このとき，ゼロ知識証明値 π から x に関する情報がいっさい漏洩しない点がポイントである．

分散台帳への応用

具体的にゼロ知識証明が，ブロックチェーンでどのように利用されているかを解説する前に，直感的な利用のイメージを述べる． UTXO モデルでは，トランザクションの input として，まだ使われていない（二重支払でない）コインが指定され，output として，複数のアドレスとそのアドレスに対する送金額が指定される．もしこのとき，匿名性確保のため，トランザクション内のアドレス，送金額情報が暗号化されていたら，マイナーはトランザクションの正当性（二重支払ではないか，input の合計金額は output の合計金額と一致しているか，金額は正の値かなど）が確認できない．この問題を解決するために，トランザクション生成者は，正当性検証用のゼロ知識証明をトランザクションに対して与える．つまり，ゼロ知識証明の文脈で述べると，証明者 P はトランザクション生成者（ブロックチェーンの一般ユーザ）であり，検証者 V はマイナーであり，証明する命題 X は，「このトランザクション内のアドレス，送金額情報等は暗号化されていますが，二重支払いなどの不正はなく，ルールに従い正しく生成されています」である．

zk-SNARK の解説

本章では，Zcash などで利用されている代表的な zk-SNARK : Pinocchio 方式を解説する．

なぜ zk-SNARK なのか？

zk-SNARK とは，zero-knowledge Succinct Non-interactive ARgument of Knowledge の頭文字を取った言葉である．つまり，簡潔（Succinct）かつ非対話型（Non-interactive）なゼロ知識証明という意味である．非対話型という言葉は，ゼロ知識証明の検証処理の際に，証明者 P と検証者 V の間で複数回のデータのやりとりが発生しない，つまり，証明者 P が一方的にゼロ知識証明 π を検証者 V に送り，検証者 V が検証処理を実行することを意味する．前章で述べた通り，ブロックチェーン上でゼロ知識証明を利用する際，P2P ネットワーク上の不特定多数のマイナーが検証者 V となるため，証明者 P が，全マイナーノードと対話を行うことは非現実的である．よって，ゼロ知識証明をブロックチェーン上で利用する際には，非対話型が必須の条件となる．また，簡潔という言葉は，ゼロ知識証明 π のデータサイズが証明したい命題 X を算術回路（もしくは

ブール回路）[☆2]で表現した際のサイズによらず一定であることを意味する[☆3].

表 -1 に zk-SNARK を含む代表的な非対話型ゼロ知識証明方式（zk-SNARK，zk-STARK，Bullet proof）の比較を示す．ブロックチェーン上でゼロ知識証明を利用する際に，トランザクションデータにゼロ知識証明 π を追加するが，このデータサイズによって，トランザクションの手数料が変わる[☆4]．よって，手数料削減かつ台帳サイズ圧縮によるスケーラビリティ向上のために，ゼロ知識証明値のデータ長が短い（命題 X の回路サイズの増加に対して証明長が一定），簡潔な方式が望ましい．以上，2 つの理由から zk-SNARK がブロックチェーンで利用されている．一方で，現状提案されている zk-SNARK 方式は，セットアップの際に，信頼できる第三者機関が必要であり，かつ量子計算機に対する耐性を持たない点に注意する．

☆2 通常，ゼロ知識証明技術では，証明したい命題を算術回路（もしくはブール回路）で表現し，証明者が規定された出力値を与える入力値を持つことを証明する．

☆3 さらに検証者の計算量が回路の既知入力サイズの定数倍以下である必要もある．

☆4 本稿執筆時（2019 年 9 月）の Bitcoin では，1byte あたり 0.0000005BTC（=50 satoshi）の手数料設定で，30 分程度でブロックチェーンに取り込まれている．手数料はマイニングに対する報酬となるため，手数料の低いトランザクションはブロックに取り込まれづらくなる．

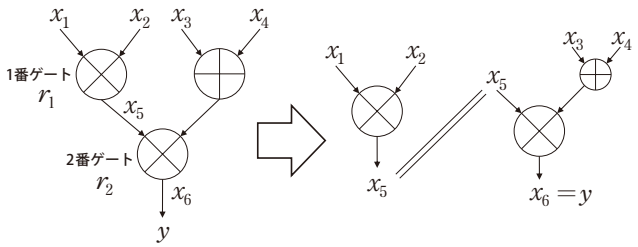


図 -1　算術回路とその R1CS 表現

Pinocchio 方式の概要

本節では，Zcash にも利用されている代表的な zk-SNARK である Pinocchio 方式を解説する（いくつか説明を簡略化している．より正確な方式を知りたい読者は文献 1) を参照されたい）．

数式を用いた説明の前に，直観的な方針を述べると，回路中の全ゲートの左からの入力値，右からの入力値，と出力値の間にある満たすべき関係式を多項式で表現し，証明者の知識をその多項式の係数（を知っていること）に変換する．さらに，証明者はその多項式の係数を暗号化し，検証者に渡し，検証処理を行うことで知識証明を行う．この暗号化状態での検証処理にはペアリング暗号の技術を用いる．

以下，図 -1 の左側に示すような 4 つの入力値 $[x_1, x_2, x_3, x_4]$ と 1 つの出力値 $[y]$ を持つ，深さ 2 の関数（算術回路）$f(X_1, X_2, X_3, X_4)=(X_1\times X_2)\times(X_3+X_4)$ を考える．この関数 f の出力値 y に対して $f(x_1, x_2, x_3, x_4)= y$ となる入力値 $[x_1, x_2, x_3, x_4]$ を知っていることをゼロ知識証明する例を考える（実際にはハッシュ関数のような複雑な算術回路に対して証明を行う）．

Pinocchio 方式では信頼できる第三者によって，全ユーザが利用するシステムパラメータを生成する事前の処理が必要である（Setup 処理と呼ぶ）．

Setup 処理（信頼できる第三者機関が事前に行う）

1. 関数 f 内の各掛算ゲートに番号を振り（図中の 1 番ゲート，2 番ゲート），その出力値を新しい変数 $[x_5, x_6]$ とする．
2. 各掛算ゲートに対して乱数 $[r_1, r_2]$ を生成し，ターゲット多項式 $t(X):=(X-r_1)(X-r_2)$ を計算する．
3. 関数 $\phi_1(X)$ を $\phi_1(r_1)= 1, \phi_1(r_2) =0$ となるよう

表 -1　ゼロ知識証明方式の比較表（N は回路サイズ）

	証明サイズ	P の計算量	V の計算量	第三者機関	耐量子性
zk-SNARK	288bytes	$O(N*\log(N))$	$O(1)$	必要	なし
zk-STARK	45 ～ 200KB	$O(N*\text{poly}\log(N))$	$O(N*\text{poly}\log(N))$	必要なし	あり
Bullet proof	～ 1.5KB	$O(N*\log(N))$	$O(N)$	必要なし	なし

に生成する（1 番ゲート上で値が 1，2 番ゲート上で値が 0 となるラグランジュ型補間多項式）．同様に関数 $\phi_2(X)$ を $\phi_2(r_1)=0$, $\phi_2(r_2)=1$ となるように生成する．

4. $t(X)$ と $\{\phi_1(X), \phi_2(X)\}$ を公開する．

このとき，多項式

$$x_1\phi_1(X) \times x_2\phi_1(X) - x_5\phi_1(X) \qquad (1)$$

は，$X=r_2$ を解に持ち，さらに $X=r_1$ を解に持つ必要十分条件が，$x_1 \times x_2 = x_5$ であることに注意する（1 番ゲートに対応する制約条件）．また，多項式

$$x_5\phi_2(X) \times (x_3\phi_2(X)+x_4\phi_2(X)) - x_6\phi_2(X) \qquad (2)$$

は，$X=r_1$ を解に持ち，$X=r_2$ を解に持つ必要十分条件が，$x_5 \times (x_3+x_4) = x_6$ であることに注意する（2 番ゲートに対応する制約条件）．この算術回路の変形で重要な点は，深さ 2 の算術回路が式（1），（2）のような，いくつかの制約条件の付いた深さ 1 の回路（Rank-1 Constraint System）で表現可能である（図 -1 の右側参照）．より一般の回路に対しても，同様の方法で深さ 1 の回路と制約条件で表現できる．

この多項式と各ゲートに対して $A(X)$:=[左からの入力値]，$B(X)$:=[右からの入力値]，$C(X)$:=[出力値] をまとめると，

$$\overbrace{(x_1\phi_1(X)+x_5\phi_2(X))}^{\text{左からの入力値}} \times \overbrace{(x_2\phi_1(X)+x_3\phi_2(X)+x_4\phi_2(X))}^{\text{右からの入力値}}$$
$$-\overbrace{(x_5\phi_1(X)+x_6\phi_2(X))}^{\text{出力値}} = A(X)B(X)-C(X) =: P(X),$$

$P(X)$ が $X=r_1, r_2$ を解に持つ（ターゲット多項式 $t(X)$ で割り切れる）ための必要十分条件は，$x_1 \times x_2 = x_5$ かつ $x_5 \times (x_3+x_4) = x_6$ が成立することとなる．このように多項式 $P(X)=A(X)B(X)-C(X)$ がターゲット多項式 $t(X)$ で割り切れるかどうかによって算術回路の正しい入出力値のペアか表現することを QAP : Quadratic Arithmetic Program と呼ぶ．

今，正しい知識 $f(x_1, x_2, x_3, x_4)=y$ を満たす，(x_1, x_2, x_3, x_4) を有する証明者 P は，実際に (x_1, x_2, x_3, x_4) を代入することで，$A(X)=a_2X^2+a_1X+a_0$ の係数を計算可能である．$B(X)$，$C(X)$ に関しても同様である．さらに，$P(X)$ は $t(X)$ で割り切れるので，$H(X) := P(X)/t(X) = h_2X^2+h_1X+h_0$ の係数も計算可能である．この計算によって，証明者 P の持っている知識が多項式の係数情報に変換された．よって，証明者 P は，「命題：ターゲット多項式 $t(X)$ に対して

$$A(X)B(X) - C(X) = H(X)t(X) \qquad (3)$$

を満たす多項式 $A(X), B(X), C(X), H(X)$ の係数を知っている」を検証者 V に証明することで，本来示したい「命題 : $f(x_1, x_2, x_3, x_4)= y$ を満たす，(x_1, x_2, x_3, x_4) を知っている」を証明可能である．これにはペアリング暗号の技術を利用する．ペアリング暗号とは，ペアリングと呼ばれる双線形写像を用いた公開鍵暗号の一種である．

$$e : G_1 \times G_2 \longrightarrow G ; (g_1^a, g_2^b) \longmapsto e(g_1, g_2)^{ab},$$

を（アルゴリズムが公開されている）ペアリング写像とする．先ほどの Setup 処理実行者は，事前に乱数 s を生成し，$(g_1, g_1^s, g_1^{s^2}, g_2, g_2^s, g_2^{s^2}, g_2^{t(s)})$ をシステムパラメータとして公開する．このパラメータを利用することで，$A(X)= a_2X^2+a_1X+a_0$ の係数 (a_0, a_1, a_2) を知る証明者 P は，$g_1^{a_0} \cdot (g_1^s)^{a_1} \cdot (g_1^{s^2})^{a_2} = g_1^{A(s)}$ を計算可能である．同様に，$g_2^{B(s)}, g_1^{C(s)}, g_1^{H(s)}$ も計算可能である．つまり，多項式 $A(X), B(X), C(X), H(X)$ の点 s での評価値が，指数部分となる離散群の元を求めることが可能である． 証明者 P は，ゼロ知識証明値 π として，

$$\pi=(g_1^{A(s)}, g_2^{B(s)}, g_1^{C(s)}, g_1^{H(s)})$$

を検証者 V に渡す[☆5]．そして検証者 V は，システムパラメータの $g_2^{t(s)}$ を使い，以下の等号が成立するかを確認する．

$$e(g_1^{A(s)}, g_2^{B(s)})=e(g_1^{H(s)}, g_2^{t(s)})\cdot e(g_1^{C(s)}, g_2)$$

左辺の指数部分は $A(s)\cdot B(s)$ であり，右辺の指数部分は $H(s)\cdot t(s)+C(s)$ となる．もし，証明者 P が正しい知識を持ち，$A(X), B(X), C(X), H(X)$ を計算可能であれば，(3) 式が成立するため，上式の等号も成立する．検証者 V は，この等号の成立を確認することで，証明者 P が正しい知識 $f(x_1, x_2, x_3, x_4)=y$ となる (x_1, x_2, x_3, x_4) を知っていることを確認する．注意として (3) 式は，多項式としての等号であり，それを点 s での値の一致のみで検証を済ますことに違和感を感じるかもしれない（偶然，値が一致する場合があるので），しかし実用上は，ペアリングのパラメータを大きく設定することで，偶然一致する確率を限りなく 0 に近づけることが可能である．また，この構成方法から分かるように Setup 処理時の乱数 s は秘密のパラメータであり，g_1^s から s を求めることが計算量的に困難であるなどの仮定を必要とする．同時に乱数 s が秘密情報であることから，zk-SNARK の運用には信頼できる第三者による Setup 処理が必要な理由も明らかである．

実は上述のプロトコルは正しい知識を持つことを証明しているが，ゼロ知識証明にはなっておらず，π から入力値に関する情報が漏れる．$A(X)$ 等に乱数 δ で $A(X)+\delta t(X)$ とマスクすることで，ゼロ知識性を達成することが可能である．

[☆5] 正確には，f の出力値 y に対応する部分 $x_6=y$ の代入計算は検証者側で実行する．

Zcash プロトコルの解説

本章では，代表的な匿名暗号通貨である Zcash において送／受金者のリンク情報がどう秘匿化されているかを解説する．

図 -2 は，Alice から Bob に送金を行う際のイメージである．H をアルゴリズムが公開されているハッシュ関数とし，システム管理者，もしくは信頼できる第三者によって，以下に示す手順 4 の命題に対する Pinocchio 方式のシステムパラメータが生成，公開されているものとする．送金の処理手順は以下のとおりである．

1. Alice は受金者アドレスを秘匿（図では− − −）したトランザクションをブロックチェーンに

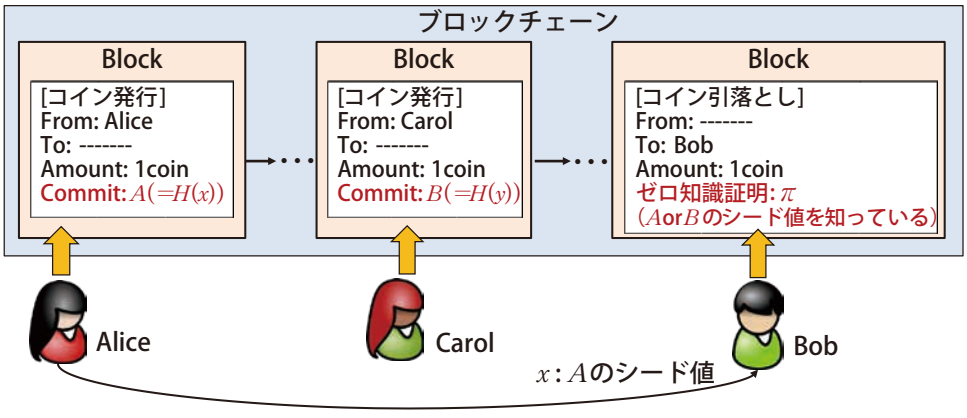


図 -2　送金を行う際のイメージ

送信する．この際に秘密のシード値 x を生成し，そのハッシュ値 $A=H(x)$ をコミットメント値としてトランザクションデータに追加する（匿名コイン発行）．

2. Carol も同様に受金先を秘匿化し，コミットメント値 $B=H(y)$ 付きトランザクションをブロックチェーンに送信する（匿名コイン発行）．
3. Alice は Bob に発行済み匿名コイン A のシード値 x を渡す．渡す方法はブロックチェーン外部の通信手段でもよいし，Bob の鍵で暗号化してブロックチェーンに書いてもよい．
4. Bob は発行済みの全匿名コインのコミットメント値（図では A, B）に対して，「命題：ハッシュ関数 H の出力値が A or B となる入力シード値を知っている」を証明するゼロ知識証明 π を生成し，送金者アドレスを秘匿化したトランザクションデータにこの証明を追加し，ブロックチェーンに送信する．

上述のプロトコルにおいて，ゼロ知識証明を検証するマイナー，およびほかのユーザは，実際に Bob がコミットメント値 A，もしくは B のどちらのシード値を知っていたかは分からない．しかし，少なくともどちらか 1 つのシード値を知っていたことは確認できる（コインを受け取る権利は持っている）．結果として Alice から送金が行われた事実を秘匿することが可能である．このプロトコルでは送／受金者のリンクは秘匿化されているが，送／受金者のアドレス，送金額は秘匿化されていない（たとえば，ユーザごとに送金額が異なる場合，送金額から受金者が特定可能である）．また，Alice による二重支払いや Bob による二重引落しを防止する機能もない． 実際の Zcash プロトコルでは，より複雑なトランザクション（Sprout/Sapling）と，それに対応したゼロ知識証明を利用して，これらの問題に対応している．

匿名送金に関する監査

前章までに述べたように，匿名暗号通貨はユーザのプライバシを守る一方で，マネーロンダリングなどの不正な送金手段として利用される恐れが指摘されている．

匿名暗号通貨が実社会に受け入れられるためには，従来の金融機関，もしくはほかの仮想通貨と同様，当局による適切な監査に対応する必要がある．以下に述べるように，ゼロ知識証明を再び利用することで，一般のブロックチェーンユーザには，送金の流れが秘匿化されているが，監査当局には秘匿化が解除可能な仕組みが構築できる．

匿名暗号通貨において，通常の暗号通貨のように監査を実現する簡単な方法は，トランザクション内で秘匿化されている情報を監査者の公開鍵で暗号化し，監査用の情報としてトランザクションデータに追加することである．こうすることで一般のブロックチェーンユーザに情報を秘匿しつつ，秘密鍵を持つ監査者にのみ情報へのアクセス権限を与えることが可能である．しかし，この際に問題となるのはマイナーの存在である．マイナーは監査者ではないので，暗号化されている監査用の情報が，正確な情報なのか確認できない．この問題に対して，トランザクション生成者は，ゼロ知識証明を利用することで，暗号化されている監査用の情報が正しく生成されていることを証明できる．つまり，「命題：暗号化されている監査用の情報は，監査者の公開鍵で暗号化されており，さらにその平文はトランザクション内の秘密情報と一致する」を zk-SNARK などを使って証明する．たとえば前章の例では，Bob が実際には $A=H(x)$ のシード値を知っていることを示す情報を監査者の公開鍵で暗号化し，さらにそのことを示すゼロ知識証明をトランザクションデータに追加することで，監査者は Alice から Bob への送金の流れを把握することが可能である（具体的な方式は，文献 2）参照）．

暗号通貨の価値から見える課題

暗号通貨が持つ本来の価値として，非中央集権性とは別に手数料の安い決済手段といった側面がある．たとえばBitcoinでは，手数料自体をBTCで払っているため，1BTCの価格が高騰するとそれに合わせて手数料も高騰する．その結果として，安い決済手段としての価値が低落し，価格に対して負のフィードバックが働く．

よって最終的にある均衡点となる金額に落ち着くが，その金額は銀行，クレジットカードなどの通常の決済手段に比べて安価であることが望ましい（そうでなければ既存の決済手段が利用される）．2019年現在，暗号通貨に関しては投機的な取引が活発なため，まだこの均衡点には到達していない．

本稿では代表的な匿名暗号通貨Zcashとその基盤技術であるゼロ知識証明方式zk-SNARK，それを使った監査機能の実現方法について解説した．

すでに見てきたとおり，匿名暗号通貨では，誰が誰にいくら送金したか，といった情報を第三者に秘匿することができる．結果として投機的な売り買い情報が見えにくくなり，通貨価格の安定化が期待される．

現状，ゼロ知識証明を使った匿名暗号通貨は，トランザクションのデータサイズが増加するため，手数料の観点からまだ一般の利用割合は高くない．

一方で秘匿性の高さからマネーロンダリングなどの不正な送金手段として利用されている．この問題に対しては，監査機能を付与し適切な監視を行うことが望ましい．当然，監査機能の追加はさらなる手数料の増加を招く．良貨が悪貨に駆逐されないためにもインセンティブを与えるなどの利用促進に向けた施策，運用が望まれる．

参考文献

1) Parno, B. et al. : Pinocchio: Nearly Practical Verifiable Computation, In IEEE Symposium on Security and Privacy, S&P (2013).
2) Naganuma, K. et al. : Auditable Zerocoin, In European Symposium on Security and Privacy Workshops, EuroS&PW (2017).

(2019年10月8日受付)

長沼　健　ken.naganuma.dn@hitachi.com
日立製作所研究開発グループ所属，東京大学大学院新領域創成科学研究科博士課程在学中，入社以来モバイルアプリケーション，GPS利活用，車載無線セキュリティ，医療データ分析の研究開発に取り組む．2014年より暗号通貨，ブロックチェーンの研究開発に携わる．

［ブロックチェーン技術の最新動向］

③ ブロックチェーンの安全性 ―攻撃や脆弱性とその対策―

松尾真一郎 ジョージタウン大学

ブロックチェーンのセキュリティを再考する

2008 年の Satoshi Nakamoto が公開した Bitcoin の登場は，電子的な送金を信頼できる第三者によらずに実現するプロトコルを提示した．そして，Bitcoin のコア技術である，不特定多数の利用者による台帳の安全な更新と管理を実現する技術を取り出して，ブロックチェーン技術と名付けて扱われるようになった．ブロックチェーン技術が，それまでの技術に比べて新しいのは，台帳の更新が（参加や脱退がいつでも認められる）不特定多数の参加者によってのみ行われる点と，台帳の更新に際して，プログラムによる多様なロジックを組み込むことが可能になっているという点である．

一方で，ブロックチェーンが「これまでにないセキュリティ」を提供するような議論を目にすることも少なくないが，一般論としてセキュリティの向上は，性能や使い勝手などの何かの犠牲によって成り立つものである．また，すべての面においてセキュリティを担保したり，ゼロリスクにするということは，現実的にはほぼ不可能である．本稿では，この視点に基づきブロックチェーン技術がもたらす安全性の範囲（セキュリティ目標），ブロックチェーンのセキュリティに関する理論的な議論の現状，現在指摘されている脅威と脆弱性，そしてセキュリティ向上に向けた研究開発の方向性について述べる．

ブロックチェーンにかかわるセキュリティの全体像

ブロックチェーンのセキュリティ目標（Security Objectives）

ブロックチェーン技術に関する議論は，かなり幅広い応用を見据えたものになりがちであるが，最も本質的に提供する機能は，「不特定多数の参加者が管理する共通の帳簿が存在し，その帳簿を一定のロジック（たとえば Bitcoin のような支払いでは，支払い者の残高を減少させ，受領者の残高を同額だけ増額させるという足し算と引き算）に基づいて，事象の発生順序を保証しながら更新していく．攻撃者が一度合意した更新を覆す可能性は無視できるほど小さい」という点にある．これがブロックチェーンの必須のセキュリティ目標であり，それ以外のセキュリティ目標は，すべてオプションであることに注意が必要である．たとえば，トランザクションにおけるプライバシ保護や，アプリケーションレベルでの利用者認証や処理の整合性は，ブロックチェーン技術を利用したアプリケーション固有の追加的なセキュリティ目標である．

ブロックチェーンのセキュリティ確保のためのレイヤ

一般に，あるセキュリティ目標を達成するには，基盤的な暗号技術，その組合せ，実装，そして運用にいたる異なるレイヤにおいて，適切な検討がなされることが必須である．あるレイヤで正しく構築された技術は，ほかのレイヤの技術が正しく使ってく

れることを暗黙のうちに仮定しているが，その仮定に反した使われ方をされることがある．たとえば，仮に安全な暗号技術を使っていても，暗号鍵の運用が杜撰であればその効果は無になる．2018 年から 2019 年にかけて発生した，取引所のセキュリティインシデントは，杜撰な暗号鍵の運用に起因している．この例にもあるように，安全なブロックチェーンの設計，実装，そして，運用のために，すべてのレイヤで正しい技術の利用や運用を行う必要がある．

ブロックチェーン技術と，それを利用したアプリケーションにおいては，おおむね図 -1 のような 6 つのセキュリティに関係するレイヤが存在する．下から順番に説明する．1 番下にあるのが，基盤的な暗号アルゴリズムと呼ばれる技術で，ブロックチェーンにおいては SHA-2 などのハッシュ関数や ECDSA[☆1] などの電子署名技術がそれに当たる．これらの技術は，日本においては電子政府推奨暗号リストを作成する CRYPTREC[☆2] において評価され，ISO/IEC JTC 1 SC 27 などで標準化が行われている．続くバックボーンプロトコルは，ブロックチェーン技術の根幹プロトコルの部分である．P2P ネットワークや，合意プロトコルがセキュアであるかどうかを確かめる必要がある．3 番目のレイヤは，よりアプリケーションに近いセキュリティ目標を実現するためのレイヤで，プライバシ保護やトランザクション自体が安全に処理されることを確認する必要がある．4 番目のレイヤは支払いや契約などの応用的なロジックを安全に実行するためのレイヤで，Bitcoin や Ethereum などに実装されているスクリプト言語の安全性に関係する．5 番目のレイヤは，安全な実装に関するもので，ブロックチェーン技術とそのアプリケーションを実装するソフトウェアコードや，暗号鍵を守りながら暗号処理を行うハードウェアなどの安全性を確認するレイヤである．そして最後のレイヤは，鍵管理，監査などを行う運用のレイヤである．それぞれ，ISO/IEC などで，標準的な技術や運用手法が定められており，ブロックチェーンにおいてもこれらの標準への適合を確認する必要がある．

☆1 楕円曲線暗号に基づく電子署名アルゴリズム．ISO 標準になっている．
☆2 総務省と経済産業省による，電子政府推奨暗号リストなどを作成する委員会．

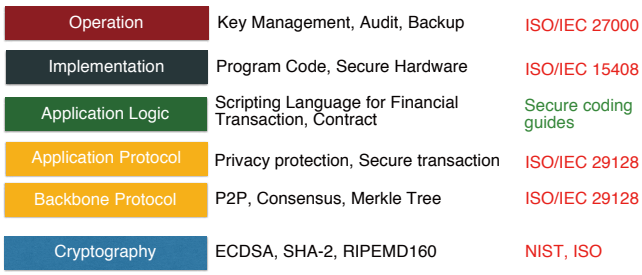


図 -1　ブロックチェーンにおけるセキュリティのレイヤ

ブロックチェーンの基盤技術に関する理論的な議論

本章では，ブロックチェーンの必須のセキュリティ目標の部分（前述の 2 番目のレイヤ）の安全性について，現在のアカデミアの議論を述べる．

2015 年の Eurocrypt[☆3] において，J. Garay らは，Bitcoin で提案された Proof-of-Work を利用した合意アルゴリズム（Nakamoto Consensus）について，セキュリティ目標に繋がる 2 つの性質 Common Prefix と Chain Quality を定式化した[1]．Common Prefix とは，Honest な（プロトコルに従う）参加者の任意の 2 者のペアは，ある一定ラウンド以前の共通のチェーンを共有しているという性質であり，Chain Quality は，Honest な参加者が作成し合意するブロックの比率が，Dishonest な（プロトコルに従わない）参加者のブロックに比べて十分に取れている性質を表している．また同論文では，台帳に必要な性質として Persistence と Liveness を定式化している．Persistence は，あるトランザクションが承認されて以降，ある 1 人の Honest の参加者が所持するブロックの中で，一定ブロック経過した後には，合意が覆ることがない性質である．

Liveness は Honest なアカウントホルダが作成した

☆3 IACR（International Associaltion of Cryptologic Research）主催の暗号学におけるトップカンファレンスの 1 つ

トランザクションは一定のブロックが作成された後にHonestな参加者に承認される性質である．そのため，攻撃者によるDenial of Service攻撃ができないという性質である．この定式化に従い，同論文では，Nakamoto Consensusが，攻撃者のハッシュパワーが全体の1/2以下である場合に，すべての通信の同期が取れているという強い前提のもとに，上記の性質を満たしていることを証明した．この定式化の後，R. Passらは，Eurocrypt 2015の結果を拡張して，台帳に必要な新たな性質としてChain Growthを定義した．これは，Honestな参加者の間では，合意され共有されるブロックが一定数続いていくという性質である．その上で，同期性に関する制約を少し緩め，通信遅延の上限が設定される範囲において，Bitcoinがこの性質を満たすことを示している[2]．現在のブロックチェーンの安全性証明は，基本的にはこの定式化のもとに議論されている．一方で，Bitcoinの合意アルゴリズムについて，同期性に関する仮定を含めた現実を捉えた議論はまだ途中であり，今後の研究の進展も必要である．

上記の議論は，純粋にハッシュパワーやノードの数に依存した安全性の定式化であるが，ブロックチェーンが安全に保たれ続けるためには，Dishonestなノードのハッシュパワーを上回るHonestなノードが常に必要であり，これを維持するためにマイニングによる報酬の付与がシステムに組み込まれている．この報酬に応じてノードを維持するかどうかは，経済学的な合理性の分析が必要であり，ゲーム理論的解析の要素が入ってくる．現在の安全性の定義では，この点を捉えることはできていないため，現在の大きな研究テーマの1つとなっている．

ブロックチェーンの脅威や脆弱性の現状

ブロックチェーンプロトコルに関する一般的な脅威と脆弱性

ブロックチェーンの根幹である合意アルゴリズムにおいて，最も一般的に知られているのは51% Attackである．これは攻撃者が全体のハッシュパワーの50%を超えるハッシュパワーを有するとき，新たに作られるブロックの内容を自由にコントロールできるようになるため，過去のトランザクションデータを用いてDouble Spending（二重支払い）を成功させることができる．もしくは，新たなブロックに何もトランザクションを入れないというDenial of Service攻撃を行い，暗号資産自体を無効化することもできる．一方で，前述の通り，マイニング報酬を与えることにより，結託しない数多くの参加者がネットワークに参加するインセンティブがある．現状では，少数のマイニングプールのハッシュパワーを足すと51%攻撃は可能となるが，Bitcoinにおいては現時点では発生していない．一方で，十分なハッシュパワーを得られていない暗号資産では，この攻撃が発生している例がある．

そのほかに二重支払いを引き起こす可能性がある攻撃の例として以下のようなものがある

— Finney Attack：まず，支払い者が自分でマイニングしたコインを自分へ支払い，そのトランザクションが入ったブロックを作成し，ほかのネットワーク参加者に送信せずおいておく．次に，そのコインを商店への支払いに使う．商店がトランザクションの承認前に商品を発送したのを確認した後に，元の自己支払いのトランザクションデータをブロックチェーン上で承認する．トランザクションの承認までの期間が短い場合には，この攻撃の成功の確率が高まる．

— Brute Force Attack：十分なハッシュパワーを持つ攻撃者があらかじめ2つのチェーンを事前にマイニングして用意しておく．長いチェーンには自分がコントロールするノードへの送金，短いチェーンには同じ資金の商店への支払いを記録しておく．短いチェーンで商店への支払いを終わり，確定されるまで十分な時間が経過した後に，長い方のチェーンを送信し，商店への支払いを上書きする．

そのほかに，ブロックチェーンのプロトコル実行における攻撃の例として以下のようなものがある．

— Selfish Mining Attack：あらかじめ長いブロックのチェーンをマイニングしておき，そのブロックを隠し持っておいて，のちに公開することで，一度合意したチェーンを覆す攻撃．この攻撃が存在することで，正しいと思っていたマイニングをするユーザのマイニングパワーが無駄になり，正しいマイニングを個別に行うインセンティブが低下する．

— Sybil Attacks：攻撃者がたくさんの利用者のコピーを作り出し，合意において有利な立場を得ようとする攻撃．Proof-of-Work や Proof-of-Stake は，この攻撃の可能性を減らすための仕組みであるが，確率が完全に 0 になるわけではない．

暗号技術の危殆化と量子計算機

安全性と処理性能を同時に追求する現代暗号において，ある暗号アルゴリズムが永久に安全であるという仮定を置くことはできない．多くの場合，計算機の処理能力の向上に従い，暗号技術を破るために必要な時間が減少して攻撃の成功が現実的になったり，そもそものアルゴリズムの設計自体にミスがあり，期待していた安全性が担保できないケースがある．過去にも，米国連邦政府標準暗号であった DES：Data Encryption Standard や，やはり米国連邦政府標準ハッシュ関数である SHA-1 にはアルゴリズム上の脆弱性が発見され，それぞれ AES：Advanced Encryption Standard，SHA-2[☆4] と新しいアルゴリズムへの切り替えがなされている．同様に，暗号技術の安全性のパラメータである鍵データのサイズ（鍵長）は，攻撃者の計算能力に応じて設定する必要がある．現在，RSA[☆5] などの電子署名アルゴリズムでは 2048 ビット（楕円曲線を利用した ECDSA のような電子署名アルゴリズムでは 224 ビット相当）の鍵を使うことが推奨されているが，計算機能力がこれからも向上することを想定すると，いずれ鍵長を伸ばす必要がある．

上記のように，暗号技術が期待していた安全性を保てなくなることを危殆化（きたいか）と呼ぶ．暗号技術の危殆化が発生した場合，取る方法は 2 つある．計算機の能力が向上してその時点での鍵長が不足した場合には，公開鍵暗号や電子署名アルゴリズムであれば，より大きなサイズの鍵に変更して，同じアルゴリズムを使うことが可能だ．しかし，アルゴリズムそのものに脆弱性が発見された場合，さらに共通鍵暗号やハッシュ関数で鍵長やハッシュ値のサイズが不足する場合，アルゴリズムそのものを変更しなくてはいけない．

ブロックチェーンにおいて，暗号技術の危殆化が発生した場合，どういう問題が起きるのだろうか．たとえば電子署名の偽造が簡単にできるようになれば，過去のトランザクションを人が作成したかどうかの見分けがつかなくなる．ハッシュ値のコリジョン（複数の別の値のハッシュ値が同一になること）が見つかれば，一度合意したブロックからほかのブロックへの合意を覆すことができる可能性が増す．それでは，ブロックチェーンにおいて，暗号技術に危殆化が見つかった場合，新しい暗号技術に移行することはできるのだろうか．答えは，そんなに簡単ではない．それはブロックチェーンに格納する新しいデータに適用する暗号アルゴリズムを変更するだけでなく，ブロックチェーンの検証に必要な過去のデータの有効性を延長しなくてはならないからだ．筆者らは，電子署名と証明書の有効期間を延長する技術である長期署名の技術を用いて，ブロックチェーンの有効性を延長する技術を提案している[3]．過去の例では，標準的な暗号アルゴリズムでも，その発明から 20 年から 30 年で危殆化が発生している．ブロックチェーン上の帳簿のデータは長期間，あるいは永久に安全性を保つ必要があり，一方で暗号技術には危殆化のリスクが常に存在することから，危殆化が発生した際のより安全な暗号への移行スキームと運用についての研究が，さらに求められる．

☆4 2001 年に制定された米国標準ハッシュ関数．
☆5 RIvest Shamir，Adleman によって提案された公開鍵暗号方式．

暗号技術の危殆化に関する，もう1つ大きな懸念は量子計算機の発展だ．汎用的な量子計算機の上で1994年に発表されたShorのアルゴリズムを用いると標準的な公開鍵暗号の基盤となっている素因数分解問題や離散対数問題がより効率的に解けることが知られている．また，1996年に発表されたGroverのアルゴリズム，1997年に発表されたSimonのアルゴリズムによって共通鍵暗号の解読における探索を効率化することで知られている．一方で，現在のところ，ハッシュ関数の衝突困難性，第二原像困難性，一方向性をより効率的に破るアルゴリズムは知られていない．本稿では，汎用的な量子計算機の実現性や，暗号技術の解読に至るまでの期間についての議論は行わないが，中長期的には，汎用的な量子計算機の存在がブロックチェーンのセキュリティに影響する可能性が存在する．現在，汎用的な量子計算機が存在したとしても安全性が保たれる暗号技術（耐量子計算機暗号）の研究が進んでいるが，耐量子計算機暗号は暗号鍵のサイズや，電子署名のサイズが非常に大きくなることが知られており，現状ではブロックチェーンに応用することはできない．将来的には，耐量子計算機暗号とブロックチェーンへの適用の理論的研究が必要と考えられる．

ネットワークレイヤに起因する脆弱性

言うまでもなく，ブロックチェーン技術は，足回りのグローバルなインターネットが正しく機能していることが大前提である．そのため，ブロックチェーンのプロトコルは，インターネットに対する攻撃が行われたときにでも正しく動作するかは保証の限りではない．その例として2017年のIEEE Security and Privacyで，Maria Apostolakiらが，BGPプロトコル（インターネットのルーティングに用いられる基本プロトコル）に対する攻撃を利用することで，ブロックチェーンのブロックデータの伝達を妨害する攻撃を発表している[4]．このような研究は，本稿で示した，参加者間の同期に関する前提に対する攻撃の一種と見なすこともできる．

実装攻撃

冒頭に述べたセキュリティのレイヤの中で，プロトコル以外に注目する必要があるのが，実装面での脆弱性である．ここでの実装は，ソフトウェア実装，ハードウェア実装の両方である．すでに，Bitcoin，その他のブロックチェーンにおいて，脆弱性情報がCVE[☆6]レコードとして脆弱性データベースにも数多く登録されている．また，一般のユーザの署名鍵を安全に管理するために，ハードウェアウォレットが開発され，一部利用されている．ただし，安全であることを謳っているハードウェアウォレットであっても，実際にサイドチャネル攻撃などの実装攻撃で，署名鍵が取り出せるケースが報告されている．

セキュリティ向上に向けて

取引所セキュリティの強化について

ブロックチェーンに関するセキュリティに関して，一般に大きく懸念されているのは，暗号資産を取り扱う取引所（交換所）が攻撃されて，暗号資産が流出する事件が多発していることだろう．元々のBitcoinの論文には，取引所自体の存在が仮定されておらず，すべての参加者が自身の署名鍵を自らの責任で漏洩しないように管理することが暗黙の要求事項になっている．しかし，一般の利用者が，正しく署名鍵を管理することが簡単ではなく，また円やドルなどの一般的な通貨との交換も簡単ではないことから，署名鍵を預かりつつ，暗号資産と一般的な通貨の交換を行う取引所が利用されるようになった．本来のブロックチェーンは，51%のマイニングパワーを持つ攻撃者がいない限り安全であることを目指して設計されており，何らかのプロトコル参加者が故障したとしても問題なく動作することが特徴だ．しかし，取引所はいわゆる単一障害点になり得る．2018年以降多発している取引所からの暗号資産の流出は，これらの単一障害点を

☆6 Common Vulnerabilities and Exposures：個々の脆弱性情報につけられる識別子．

守ることが難しいことを示している．

現在の取引所のシステムには，安全なモデル実装が用意されておらず，取引所ごとにバラバラに設計と実装がされている．また，安全なシステムの設計ノウハウを持たない事業者がサービスを行っているケースもある．そのため，取引所のセキュリティ強化は，ブロックチェーンシステム全体の安全性を確保し，利用者に広く安心して利用できるようにするために必須である．セキュリティ専門家も加わっている CGTF（Croptoasset Governance Task Force）では，取引所のシステムを情報セキュリティマネジメントシステム：ISMS の手法を用いてリスク分析し，Security Control を検討するためのサポート文書を作成している [5]．

スマートコントラクトと形式検証

2016 年に発生した The DAO 事件では，Ethereum 上に構築したスマートコントラクトを実行するソフトウェアにおいて，再帰呼び出しを行う際のトランザクションのロックの処理に不備があり，暗号資産が自動的に流出する事象が発生した．Bitcoin のような単純な支払いのロジックではなく，より高度なビジネスロジックのためのプログラムを構築する際に，バグの発生がブロックチェーンのレイヤの問題を引き起こす可能性がある．このような事象を防ぐために，スマートコントラクトのバグの可能性を減らす手段として，形式検証を行うための研究が進められている．この研究には，大きく 2 つの方向性があり，スマートコントラクトのコードを形式検証し，セキュリティの問題が発生するトレースが存在しないことを示す方法と，形式検証可能な範囲にスマートコントラクトの言語を制限する方向である．

TEE（Trusted Execution Environment）

CPU 上に，秘密情報を用いる演算を行う独立した領域を用意し，秘密情報を保持する仕組みである TEE（Trusted Execution Environment）の利用は，ブロックチェーンにおける暗号鍵を利用した処理のセキュア化と，Zk-SNARK などのブロックチェーンのプライバシ保護のための暗号処理の実現，そしてスケーラビリティ確保の意味で，広く注目されており，関連論文も多く発表されている．TEE 自体のセキュリティについては，まだ未熟な点もあるが，セキュリティとスケーラビリティの両方を向上する手段として，TEE の活用は有望な方向性の 1 つであり，今後の研究の発展が期待される．

今後の研究課題

本稿では，ブロックチェーンにまつわるセキュリティの全体像を俯瞰し，ブロックチェーン自体とそのアプリケーションを構築する際に留意すべきセキュリティのレイヤ，現時点で明らかになっているセキュリティ上の問題，そしてセキュリティ向上のための検討の方向性を示した．ブロックチェーンにおけるセキュリティの定式化，およびセキュリティに関する依存関係の解析はまだ道半ばであり，引き続き研究が必要な状況である．

参考文献

1) Garay, J., Kiayias, A. and Leonardos, N. : The Bitcoin Backbone Protocol : Analysis and Applications, In : Oswald, E. and Fischlin, M. (eds), Advances in Cryptology - EUROCRYPT 2015, EUROCRYPT 2015. Lecture Notes in Computer Science, Vol.9057, Springer, Berlin, Heidelberg (2015).
2) Pass, R., Seeman, L. and Shelat, A. : Analysis of the Blockchain Protocol in Asynchronous Networks, In : Coron, JS., Nielsen, J. (eds), Advances in Cryptology - EUROCRYPT 2017, EUROCRYPT 2017, Lecture Notes in Computer Science, Vol.10211, Springer, Cham (2017).
3) Sato, M. and Matsuo, S. : Long-Term Public Blockchain : Resilience Against Compromise of Underlying Cryptography, 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, pp.1-8 (2017).
4) Apostolaki, M., Zohar, A. and Vanbever, L. : Hijacking Bitcoin : Routing Attacks on Cryptocurrencies, 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, pp.375-392 (2017).
5) Sato, M., Shimaoka, M. and Nakajima, H. : General Security Considerations for Cryptoassets Custodians, draft-vcgtf-crypto-assets-security-considerations-03 (work in progress) (Jan. 2019).

(2019 年 10 月 22 日受付)

松尾真一郎　shinichiro.matsuo@georgetown.edu
ジョージタウン大学 Department of Computer Science 研究教授．CyberSMART 研究センターでブロックチェーン研究ディレクターを務める．国際学術研究ネットワーク BSafe.network 共同創業者．

［ブロックチェーン技術の最新動向］

基般

④ 分散台帳技術における コンセンサス・メカニズム

齋藤　新　日本アイ・ビー・エム（株）

コンセンサスとは

本稿では，分散台帳技術（以下，DLT）で使用されるコンセンサス・メカニズムについて解説する．人口に膾炙（かいしゃ）しているのは「ブロックチェーン」という用語であるが，厳密にいうと特定のデータ構造を指す用語であるため，本稿では分散台帳技術，略して DLT，の用語を用いる．コンセンサスとは，分散・並列アーキテクチャを採用する DLT において，データを保持するノードそれぞれの状態を同期する仕組みの総称である☆1．攻撃者やノードの故障からデータを守るため，また，同時アクセスやネットワーク分断のもとでもデータの整合性を担保するため，さまざまなコンセンサスが使用されている．それぞれは前提とする障害モデルおよび想定する攻撃が異なり，性能についても一長一短がある．

本稿では，まずコンセンサスの研究の歴史について概説し，コンセンサスに求められる性質について紹介する．次に，各 DLT 実装で使われるコンセンサスのそれぞれについて解説する．最後に，それぞれのコンセンサスにおける耐障害性・耐改竄性を比較して議論する．

コンセンサス研究の歴史

はじめに，コンセンサスの研究・開発の歴史について簡単に触れる．DLT には大きく分けて 2 つのタイプがある：不特定の参加ノードを想定するパブリック型，参加ノードが特定されているプライベート型☆2 である．1980 年代，はじめにプライベート型の実装に対する研究が始まり，その後 2000 年前後になってパブリック型 DLT のベースとなる技術の研究が進んだ．

プライベート型：ビザンチン将軍問題

1982 年，Lamport らが命名した「ビザンチン将軍問題」[1] がコンセンサスに関する著名な問題である：

> ビザンチン帝国の将軍たちがある都市を包囲していると仮定する．将軍たちはその都市を攻撃するか，撤退するかを合意したい．攻撃が成功するためには，全員で攻撃する必要がある．将軍たちは互いに遠く離れており直接通信ができないため，使者を送ってメッセージを届けるものとする．
>
> ただし，将軍の中には裏切り者がいて，合意を妨害しようとするかもしれない．また，使者がメッセージを届けるのに失敗する可能性がある．メッセージが改竄される可能性もある．
>
> この状況のもとで，もし忠実な将軍たちの意見が（たとえば攻撃に）一致している場合に，彼らは正しい合意（攻撃）に至ることが可能であるか．

裏切り者の将軍はメッセージを意図的に送らない

☆1　分散合意，分散コンセンサス，などさまざまな呼びがあるが，本稿では「コンセンサス」で統一する．また本稿では，コンセンサス・アルゴリズムをしばしば省略してコンセンサスと呼ぶ．

☆2　ここでは，パーミッション型，コンソーシアム型などもこれに含める．

こともできるし，矛盾する複数のメッセージも送れることに注意されたい．このような攻撃者の設定は，この問題にちなみ「ビザンチン障害」と呼ばれる．ビザンチン障害に対して耐性があることを，ビザンチン耐性（BFT；Byzantine Fault Tolerance）を持つ，と呼ぶ．

この問題は1980年Peaseらが提案したものである[2]．彼らは，将軍の総数をN人，そのうち裏切り者の数を高々f人とした場合に，メッセージの送受信に関する条件をいくつか仮定すれば，$N \geq 3f+1$のとき合意に至ることが可能であること，またそれが下限であることを示した．Lamportらはこの問題をビザンチン将軍問題と命名し，手続き的な解法を与えた（図-1）．

これらのアルゴリズムはノード間でメッセージのブロードキャストを繰り返すため性能が芳しくなかった☆3．しかし，1988年にCastroらが効率の良いPBFT（Practical BFT）アルゴリズム[3]を提案し，この分野での研究が加速した．現在では，非常に大きなノード数に対して動作するもの，ノードのオンライン／オフライン状態の変更が激しい場合にでも効率が良いもの，DoS攻撃に耐性を持ちつつスケーラビリティを確保するもの，などの変種が提案されている．

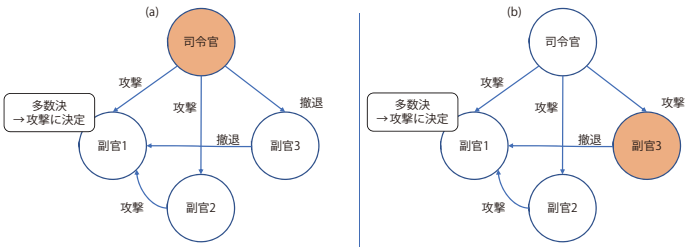


図-1　$N=4$，$f=1$の場合のビザンチン将軍問題の解法
1人の司令官の命令を$N-1$人の副官に伝える，という問題に帰着している．矢印はメッセージを表す．ここでは副官1に関係するメッセージのみ表示している．副官はほかの副官に受け取ったメッセージを転送，各副官は届いたメッセージの多数決を自身の合意結果とする．このとき，(a) 司令官が裏切る場合，(b) 副官が裏切る場合，のいずれも正しく「攻撃」に合意できている．なお，$f>1$の場合は再帰的にさらなるメッセージのやりとりが必要になる．

基本的にはこれらのアルゴリズムは多数決の性質を利用したものである．つまり，1ノード1票と見なして投票させ，多数派の意見を正当なものとして信じる，ということである．したがって，参加ノード数が特定できないパブリック型の実装には適用できない．

Hashcashと Proof of Work

一方，参加ノード数が特定できないパブリック型の実装においては，計算リソース，つまり現実における時間や電気代というコストをユーザに払わせることにより信頼性を担保する仕組みが考えられた．

これらのベースになっているのが，1997年にBackによって提案されたHashcashというスパムメール防止システムである☆4．当時，電子メールの送信コストがほぼ0であることからスパムメールが問題になっていた．Hashcashは，メールを送信する際にはある条件を満たすハッシュ値を与えるような文字列を見つけることを要求するものである（図-2）．そのためには多数のハッシュ計算が必要になる．これにより送信コストに見合わないスパム送信の抑制につながると考えられた．受信者の立場からすると，送信にコストがかかっているメールほど読むに値する，と判断することができた．

Hashcashと，データ同期を促進するようなインセンティブ設計をもとにして作られたのが，2008年にNakamotoにより提案されたビットコインである．台帳にブロックを作成するためにはHashcashとほぼ同様の計算を行う必要がある．

近年では，大量のハッシュ計算に伴う計算リソースの浪費などが指摘され，総称してProof of Stake

```
X-Hashcash: 1:20:1303030600:adam@cypherspace.org::McMybZIhxKXu57jd:ckvi
```

図-2　Hashcashにおいて，メールヘッダの`X-Hashcash`フィールドに格納する値の例（Wikipediaより）．送信するメールにより定まっている情報に加えて，送信者が選んだ`McMybZIhxKXu57jd`という nonce を含んでいる．このフィールド値全体のSHA-1ハッシュ値は16進で`00:00:0b:7c:...`となり，先頭20ビットが0である．この20という値が3～4文字目に含まれている．

☆3　たとえばLamportらのアルゴリズムの通信回数は$O(N^f)$である．

☆4　http://www.hashcash.org/papers/announce.txt

と呼ばれる種類のコンセンサスが多数提案されている．詳細については後述する．

障害モデルおよび通信環境の前提

コンセンサス・アルゴリズムについて比較・議論する際によく用いられる 2 つの障害モデルについて述べる．

クラッシュ障害（不作為障害）は一般的な「障害」の意味に近く，ノードの停止・クラッシュなどが含まれる．一方，ビザンチン障害（作為障害）はメッセージの改竄，矛盾するメッセージの送信，意図的にメッセージを無視するなど，コンセンサス・プロトコルに従わないあらゆる振る舞いを示すような障害，もしくは攻撃を指す．たとえば Paxos や Raft はクラッシュ耐性を持ち，PBFT はビザンチン耐性を持つコンセンサス・アルゴリズムである．

また，ほとんどの場合，通信に関しては非同期，つまり，あるメッセージの送信と受信は異なるタイミングで起こることが仮定される．そして，送信されたメッセージが欠落する，もしくは，送信順と受信順が異なるなどの可能性を想定することがほとんどである．一方で，電子署名技術など暗号技術の発達に鑑みて，送信途中のメッセージは改竄されない・送信者は偽造できない，との仮定を置くことがほとんどである．

コンセンサスに求められる性質

コンセンサスには，前述のような障害モデルなどを仮定した上で，以下の性質が成り立つことが求められる [4]：

1. Liveness/Termination：合意プロセスが開始したらいずれは完了すること，すなわち各ノードが「ある値に合意できた」と判断した状態になること．
2. Agreement：各ノードが思っているその「合意した値」はノード間で一致すること．
3. Validity：ノード間で一致するその「合意した値」は誰かが実際に提案した値であること．これは，常にある一定の値に合意したものと見なすような自明なアルゴリズムを排除するためである．
4. Finality：各ノードの「合意に至ったという判断」「合意した値」がいったん確定すると覆らない．

1 ～ 3 は古典的な分散合意においてよく議論された性質である一方，4 は成り立つことが前提であった．近年の分散台帳では 4 が完全には成り立たないことが多い．他には頑健性，すなわち攻撃に対してシステムが安定であること，および，処理性能（レイテンシ，スループット）などがアルゴリズム評価の対象となる．

コンセンサス・メカニズムの限界

残念ながら，コンセンサスに関する完全なアルゴリズムというものは存在しない．これまでにいくつかの結果が知られている．

- CAP 定理：ネットワーク分断（P）を想定したデータ同期システムにおいて，完全な整合性（C）および可用性（A）を同時に満たすコンセンサス・メカニズムは存在しない．2000 年に Brewer によって提唱され☆5，2002 年 Gilbert らによって証明された☆6．現在のコンセンサス・アルゴリズムは障害ノード数に関して一定の上限を持つという事実はこの定理に裏付けられている．
- FLP 定理：少なくとも 1 台のクラッシュ耐性を持ち，決定的☆7 なアルゴリズムを持つコンセンサスは存在しない．1985 年に Fisher らによっ

☆5 Brewer, E. A. : Towards Robust Distributed Systems (Abstract), In : Proceedings of the Nineteenth Annual ACM Symposium on Principles of Distributed Computing, PODC '00, Portland, Oregon, USA: ACM, p.7, ISBN: 1-58113-183-6, doi: 10.1145/ 343477.343502 (2000), http://doi.acm.org/10.1145/343477.343502

☆6 Gilbert, S. and Lynch, N. : Brewer's Conjecture and the Feasibility of Consistent, Available, Partition-tolerant Web Services, In: SIGACT News 33.2, pp.51-59, ISSN: 0163-5700. doi: 10.1145/564585.564601 (June 2002), http://doi.acm.org/10.1145/564585.564601

☆7 決定的とは，ノードの状態と受け取ったメッセージから次の状態が一意に決まる，という意味である．

て証明された[☆8]．実際，これまでに知られているクラッシュ／ビザンチン耐性を持つアルゴリズムは非決定的な動作を行う．特に liveness を担保するために乱択アルゴリズムやタイムアウトを使用している．

主要な DLT 実装におけるコンセンサス

パブリック型 DLT のコンセンサス・アルゴリズム

パブリック型 DLT の典型的なコンセンサス・アルゴリズムでは，以下の処理が並行して行われる（図 -3）：(1) 各クライアントはトランザクション（送金など，台帳を変更するための指示）をいずれかのノードに送信する．(2) それを受け取ったノードは他のノードに配布する．(3) ノードは未処理のトランザクションをまとめて 1 つのブロックを作成し，それを自己の台帳に追加して他のノードにも配布する．(4) 他ノードからブロックを受け取ったノードはそれを自己の台帳に追加する (5) ノードは台帳に存在するブロックのうち正当であると判断するものを承認し，承認情報を他のノードに配布する．(6) 他ノードから承認情報を受け取ったノードは，自己の台帳の正当な最新状態を決定する．承認は台帳の状態が分岐した場合に，正当な状態（ブロックチェーンの場合は正当なブランチ）を決定するために必要な処理である．

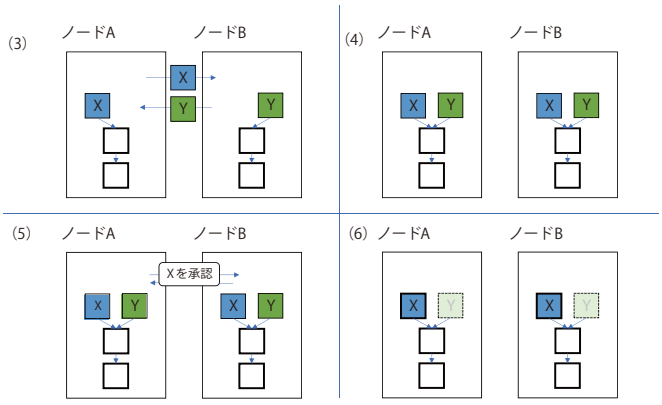


図 -3　パブリック型で標準的に使われるコンセンサス．各四角形がブロックを表す．ブロックは上に追加されるものとする．太字の枠線は承認されたブロックを表す．(6) においてブロック X を含むブランチがその時点でのメインブランチである．

処理 (3)，(5)，(6) は実装による差異が大きい．以下の解説では特筆しない限り，上記のアルゴリズムもしくはそれを微修正したものが用いられているものとする．

ビットコイン

ビットコイン（通貨記号 BTC）は 2009 年に稼働を開始した，最も古い DLT 実装の 1 つである．コンセンサスとしては PoW と Nakamoto コンセンサスを採用している．トランザクションとはアドレス A から B への送金であり，ブロックは 1 個以上のトランザクションの列である．

前述の処理 (3) において，ブロック生成は任意のノードが行うことができる．正当なブロック生成のためには，作成しようとするブロックのヘッダのハッシュ値が，その時点で決められているターゲット値より小さくなるように，ヘッダに含める nonce を探索する必要がある[☆9]．ターゲット値が小さくなるほど nonce を見つける難易度が増す．ビットコインでは，ネットワーク全体で 10 分に一度ハッシュ生成が成功するような難易度に設定されている．生成するブロックには自分に報酬（採掘報酬[☆10]）を支払うようなトランザクションを含めることができる．これがトランザクションを処理しネットワークを維持するインセンティブになっている．

ビットコインでは，処理 (5) および (6) におけるブロックの承認と承認の処理は，ブロック生成時に行われる．ブロック生成においては直前のブロックを指定する（正確には直前のブロックのハッシュ値をブロックヘッダに含める）必要があり，これがそのブロックを承認している処理にあたる．複数の

☆8 Fischer, M. J., Lynch, N. A. and Paterson, M. S. : Impossibility of Distributed Consensus with One Faulty Process, In: Journal of the ACM 32.2, pp.374-382 (1985).

☆9 このブロック生成処理は鉱石の発掘にちなんでマイニングと呼ばれる．マイニングを行うノードはマイナー（miner）と呼ばれる．

☆10 ビットコインでは一定期間ごとに半減し，最終的には 0 になるように設計されている．

ノードが並列にブロックの作成を行うため，時にはブロックのチェーンが分岐することがあり得る．その際にはメインとなるチェーン（メインブランチ）が決められ[☆11]，その上にあるブロックだけが有効になる．前述の採掘報酬は，作成したブロックがメインブランチに将来的に含まれ続けないと使用することができないため，直前のブロックを選択するということは，メインブランチに含まれるべきブロックを指定することに相当し，ひいてはそのブロックを承認することに相当する．まとめると，ビットコインではブロックを作成できたということは，報酬を受け取る権利およびブロックを承認する権利を得たことにあたる．

なお，ビットコインには小さなプログラム（スクリプト）を実行する仕組みはあるものの，署名やハッシュ値のチェックなどに用途が限られている．したがって基本的には，スマートコントラクトを自由に記述・実行する仕組みはないと見なしてよい．

Ethereum

Ethereum（通貨記号 ETH）は 2015 年，Buterin らによって提案，開発された DLT 実装である．

ビットコインと比較したときの大きな特徴は，チューリング完全なスマートコントラクトを実行する仕組みである．スマートコントラクトの実行基盤としてスタックベースの Etherum VM（EVM）を搭載する．高級言語として Solidity などが使用されている．EVM でのコード実行にはステップごとに一定の gas（手数料）が必要である．Ethereum ではアドレスにスマートコントラクトを紐付けることができ，そのアドレスにコインを送ることによりスマートコントラクトの実行が行える．送られたコインはトランザクション作成者が指定したレートで gas に変換され，その gas 量を上限として EVM で実行される．

なお，Ethereum は PoW ベースのアルゴリズムを採用する．ブロック生成間隔は 30 秒程度である．

Tezos

Tezos（通貨コード XTZ）は Liquid PoS（LPoS）と呼ばれる PoS の変種を採用する DLT 実装である．Tezos の最大の特徴は処理性能は目指さず，形式検証を用いて動作の正しさを追求するとしていることである．そのために関数型言語 OCaml で実装されており，一部のモジュールの正しさは Coq[☆12] などを使って証明されている．スマートコントラクトを実行する Michaelson VM についても，型付きのものが採用されている．

もう 1 つの特徴として，コンセンサス・プロトコルを自己更新する機能を持つ．これによりプロトコル変更に伴うハードフォーク問題を解決するとしている．コンセンサスのコア部分はブロックのフォークをどう解決するかということ，トランザクションを処理することにより台帳の状態がどう変更されるかを決定することである．Tezos ではこの部分のプロトコルがプラガブルになっている．プロトコル更新提案トランザクションが提出可能な時期が決まっており，提出されたプロトコルに対してコイン保持者からの投票，テストネット上での動作確認を行い，最終投票で更新が決定すると新しいプロトコルに差し替えられる．

LPoS コンセンサスでは 10,000XTZ を 1 単位（コインロールと呼ばれる）としてブロック作成・承認の権利が与えられる[☆13]．各コインロールは ID を持つ．以前のブロックに格納された乱数から生成権利を持つコインロール ID が生成される．なお，ブロック生成の最短間隔は 1 分であり，204 × 84 ブロック単位で作成・承認権利の割当が行われる．実際にブロックを作成・承認すると報酬が与えられる．また，これらの権利は他者に委譲できる．それに対しても報酬が得られるので，1 ロールに満たな

☆11 なお，参照実装では，それぞれのチェーンに含まれるブロックの難易度（ブロック作成時のターゲット値の逆数）の和を積算し，最も大きいものをメインブランチと見なすようになっている．

☆12 OCaml ベースの定理証明系．

☆13 前述のプロトコル変更に対する投票も同様である．

い保持者については委譲により資産を増やすことができる．現在はコインを保持し続けると報酬が年率5.5% 程度になるように設計されている．

IOTA

IOTA は台帳のデータ構造として DAG を採用する DLT 実装である．IoT ネットワーク向けのスケーラブルな DLT 実装を目指しており，特徴的な設計がなされている．コンセンサスとしては PoW でも PoS でもないと言える．

典型的な分散台帳では，トランザクションは時系列順に並べられる．ブロックチェーン[☆14]と DAG（有向非巡回グラフ）が，トランザクションの依存関係を表現する主要な方法である．ほとんどの実装で，複数のトランザクションがまとめられ，ブロックの単位で扱われる．

ブロックチェーンではジェネシス・ブロックを先頭として，すべてのブロックが直列に並べられる．ほぼ同時にブロックが作成されたなどの理由により，あるブロックの直後ブロックが複数になった場合には，どちらか一方だけが正当なブロックとして承認される．

一方で，DAG ではトランザクションの依存関係を半順序として表現する．たとえば，IOTA の DAG ではブロックではなく，個々のトランザクションを直接台帳に追加する．その際，あるトランザクションの直後トランザクションが複数になること，および，トランザクションの直前トランザクションが複数になること，のどちらも，状態の不整合を引き起こさない限り許される．

IOTA では，トランザクション追加時に，クライアント（IoT 機器などを想定している）は簡単な PoW[☆15] を行う必要がある．さらに，直前トランザクションを 2 つ指定する必要がある．これはトランザクションの承認にあたる．参照実装における指定方法は，より承認されているトランザクションの子孫が多く選ばれるようなランダムウォークで選ぶことになっているが，次に示すように，互いにコンフリクトするトランザクションを先祖に含むような指定はできない．

これを図 -4 の例で説明する．トランザクション B_i が追加された直後の状態 S_i において A が 100 コイン，B と C が 0 コインを持っているとする．この後にトランザクション B_{i+1} : $[A \rightarrow B : 100]$，および，トランザクション B_{i+2} : $[A \rightarrow C : 100]$ が追加されたとする．そうすると 2 つの状態が同時に存在する：前者のトランザクションを追加後の A と C が 0 コイン，B が 100 コイン持っている状態 S_{i+1} と，後者を追加後の A と B が 0 コイン，C が 100 コイン持っている状態 S_{i+2} である．DAG を採用する場合，どちらもこの時点では有効な状態として見なされる．

しかし，ここで両者を直前トランザクションとして持つ B_{i+3} が台帳に追加されたとする．この場合，B_{i+3} 追加後の状態は直前トランザクションを推移的にたどったすべてのトランザクションを反映したものになるべきであるが，負の残高を許さない場合，これは不可能である．したがって，B_{i+3} は B_{i+1} か B_{i+2} のどちらか一方しか直前トランザクションとして指定，つまり承認できない．これにより，いずれか一方のトランザクションのみが正当なものとして承

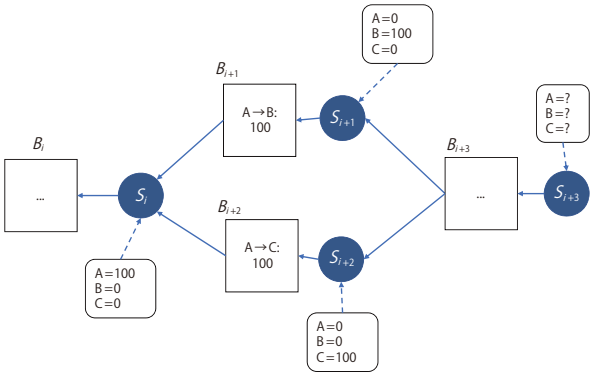


図 -4　DAG においてトランザクションが追加できない例．トランザクション B_i を処理した直後の状態を S_i とする．S_{i+3} は B_{i+1} と B_{i+2} の結果を反映させる必要があるが，負の残高を許さない限り不可能である．

☆14 ここではデータ構造の名称としてブロックチェーンという用語を使用する．

☆15 Nonce を 3^8 個の候補から探す必要がある．

認されるので，台帳全体の整合性は保たれる．

DAG 方式はトランザクション作成・承認作業が並行して行えるので処理性能のスケーラビリティに寄与すると考えられているが，そのためには前述したような非整合性が早期に解消されるようなトランザクション追加アルゴリズムになっていることが求められる．

IOTA は採掘報酬およびトランザクション手数料を持たないため，ノード保持者および資産保持者に対する直接的なインセンティブがないことについては議論がある．

プライベート型 DLT のコンセンサス・アルゴリズム

前述したように，プライベート型 DLT では finality を持つ，多数決ベースのコンセンサスが用いられる（次節参照）．計算能力が票数に相当するパブリック型と異なり，それぞれのノードの重みを対等に 1 票と見て投票していることになる．クラッシュ耐性のためには参加ノード数の約半数まではクラッシュしてもよい．その場合でも過半数の投票を集めることができれば合意に至ることができる．ビザンチン耐性のためには約 1/3 まで（このしきい値を f とする）はビザンチン障害ノードでもよい．この場合には一致する $f + 1$ 個の投票を集めることが必要である．

このアルゴリズムが正しく働くためには，TX の実行結果が決定的であることが求められる．ある 1 ノードが作成した（TX とその実行結果を含む）ブロックを他ノードが承認さえすればよい，パブリック型のアルゴリズムとは対照的である．

性能を追求する実装が多いのもプライベート型 DLT の特徴である．初期のビットコインが 7TPS（transactions per second）程度であったのに対し，数百～数千 TPS に到達するようなものも存在する．

プライベート型の実装はほぼすべてがスマートコントラクトをサポートすることもあり，台帳のデータ構造としてアカウントベースを採用することがほとんどである．

ビザンチン耐性 vs. クラッシュ耐性

ここではビザンチン耐性を持つアルゴリズムとして PBFT，クラッシュ耐性を持つアルゴリズムとして 2014 年に提案された Raft[5] を取り上げる．これらはさまざまなコンセンサス・アルゴリズムのベースとなっているので，ここで両者のアルゴリズムを比較しつつ紹介する（図 -5）．以下，トランザクションを TX と略記する．

どちらも参加ノードのうち 1 台をリーダー

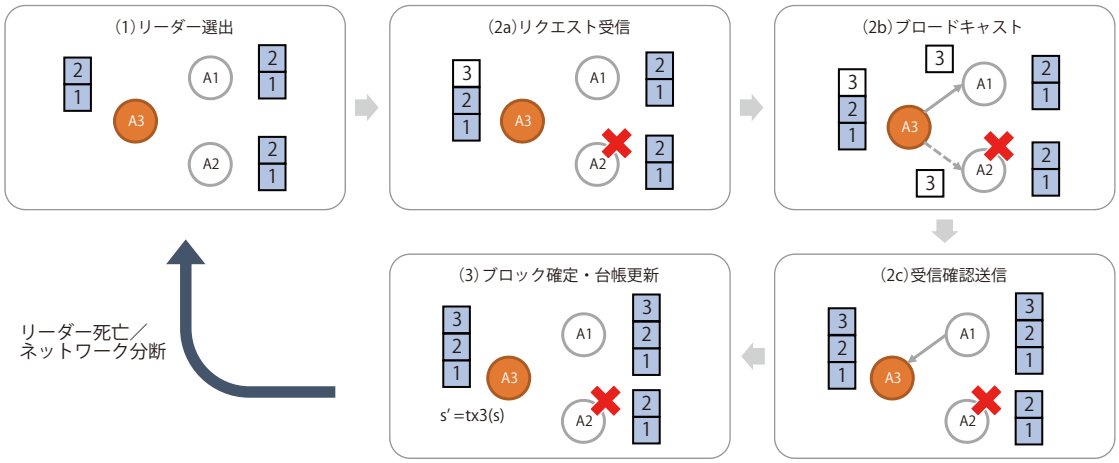


図 -5　全部で A1 ～ A3 の 3 台のノードがいて，A2 は一時的に停止しており，ステップ（1）でノード A3 がリーダーとして選ばれた場合における，Raft コンセンサスの処理概要．

(leader) として，その他をバックアップとして扱う．(1) リーダー選挙 (leader election)，(2) リーダーによる TX の受付とレプリケーション，を繰り返すことにより可用性を保ちつつデータの整合性を担保する．この (1) ～ (2) のサイクルは view, term, epoch などと呼ばれる．

ステップ (1)：初期状態，もしくはリーダーと一定時間通信できないノードが現れた場合，システムは (1) のリーダー選挙に入る．Raft では立候補したノード，PBFT ではノード ID 順で次のノード，がリーダー候補になる．候補者以外はいずれかの候補に投票する．リーダー候補は過半数など，一定数の投票を集めるとリーダーとして認められ，上記 (2) のステップが始まる．どの候補も定足数に至らなかった場合は選挙をやり直す．

(2) のステップでは，クライアントはリーダーに TX を送る (図 -5 (2a))．リーダー以外，つまりバックアップノード，に送った場合についてはそのノードがリーダーに転送するか，クライアントにリーダーへの再送を要求する．リーダーは受け取った TX の直列化を行う，つまり TX にシーケンス番号を割り振る．その後，Raft の場合はリーダーはバックアップにそれを送信し，バックアップはそのままコピーする (図 -5 (2b))．PBFT の場合はビザンチン耐性を保つために 3 ラウンドのやりとりを行い[☆16]，最終的にバックアップにコピーされる．いずれのアルゴリズムにおいても，TX を受け取りそれに合意するバックアップは acknowledge を返信する (図 -5 (2c))．一定数の ack がリーダーに集まったら，その TX は合意された (コミットされた) と判定される．各ノードはその TX を実行して台帳の状態を更新する (図 -5 (3))．

まとめると，バックアップがリーダーに従うことにより TX 列のコンセンサスをとるアルゴリズムである．このような仕組みを，強いリーダー (strong-leader) と呼ぶ．

Hyperledger Fabric

Hyperledger Fabric (以下，Fabric) はオープンソース・コンソーシアム Hyperledger のプロジェクト名および実装名である．Fabric は処理性能を追求するために，やや変わったコンセンサスを採用している．アーキテクチャとしては，オーダラーと呼ばれる，TX を整列する特権ノードを設けたことと，TX の仮実行 (シミュレーション) をあらかじめ行っておき，それが決定的であることを事前に確認する，という特徴を持つ．また，台帳としては DLT で典型的な KVS に加えて，CouchDB など JSON データを格納できるドキュメントストアを採用することにより，ビジネスアプリケーションで必要とされる複雑な検索が可能である．

コンセンサス・アルゴリズムは以下の通りである[☆17]：たとえば，ある時点で A が 200 トークン，B が 200 トークン持っていると仮定する．これは台帳に KVS のデータとして格納されていると考えてよい．ただし各エントリはバージョン属性を持つ．バージョンはエントリに書き込みがあるとインクリメントされる．ここでは A, B のバージョンがそれぞれ v1, v3 であるとする．このとき，$[A \rightarrow B : 100]$ をスマートコントラクトとして実行する場合，この TX は以下のように処理される．(1) クライアントは各ノードにこの TX を送信し，シミュレーションを依頼する．各ノードは実際に台帳の状態を変更せずに，これを実行した場合，KVS に対してどのような読み書きを行うかという read set/write set を返信する．これらをまとめてエンドースメントと呼ぶ．Read set にはシミュレーション中に読み出すエント

☆16 複数ラウンドを要する理由は以下の通りである：Raft においてはいずれのノードも嘘をつかないため，リーダーしか送れないメッセージがバックアップに届いた場合，それはたしかにリーダーが各バックアップに同じメッセージを送ったものである．しかし，ビザンチン耐性を持つためには，悪意あるノードがリーダーを騙って送信してきた可能性や，悪意あるリーダーが各バックアップに矛盾するメッセージを送っている可能性を考える必要がある．そのため，他のバックアップに確認をとり，本当にリーダーからそのメッセージが届いたか否かを確かめる必要があるからである．

☆17 バージョン 0.x と 1.x でアーキテクチャが大きく異なる．ここでは 1.x について説明する．

リとそのバージョン，write set には書き込みを行うエントリとその値を記録する．上記の例では，正しいノードは read set として $\{A : \text{v1}, B : \text{v3}\}$，write set として $\{A : 100, B : 300\}$ を返すはずである．(2) もしノードたちが返すエンドースメントに不一致があれば TX の実行失敗となる．これは一般にはスマートコントラクトの非決定性を表す．(3) もし一定数が一致していれば，それらを当該 TX に含めてオーダラーに送る．(4) オーダラーは各ノードから受け取った TX を順序付けした後，複数個をまとめてブロックを作成し，これをノードたちに配布する．(5) ノードは受け取ったブロックに含まれる各 TX に対し，後述する MVCC 検証を行う．検証を通ったものを合意済みと判断し，TX に含まれる write set を台帳の状態に反映する．その際にはバージョンがインクリメントされるため，エントリ A, B のバージョンはそれぞれ v2, v4 となる．

MVCC（multi-version concurrency control）検証は TX の台帳への反映時，シミュレーション時の write set をそのまま適用できるか否かを判定する方法である．具体的には，TX の反映時において，write set に含まれるそれぞれのエントリのバージョンが，現在の台帳（KVS）の対応するエントリのバージョンと等しくなければならない．これにより，シミュレーション時の TX の実行結果と，TX 反映時点のそれとが一致することが保証される．

Corda

Corda は R3 コンソーシアムにより開発されているプライベート型 DLT 実装である．金融取引に使用されることを念頭においた実装であるとしており，たとえば，契約文書を DLT 内のデータに紐付けることができるようになっている．Corda は自らの実装をブロックチェーンでないとしている．

Corda で扱う資産を作成する際には利害関係者全員の署名が必要である．たとえば借用証書（IOU）であれば，少なくとも債権者と債務者の署名を必要とする．作られた IOU は不変である，つまり，IOU の内容を変更する際には既存の IOU を廃棄して新しく作成する必要がある．これは UTXO 的なデータの管理方法である．利害関係者間で資産の複雑なやりとりを行うスマートコントラクトを実装することが可能であり，これは flow と呼ばれる．

Corda の特徴の 1 つは，台帳上に記録される各資産を利害関係者の間でしか共有しないことである．Fabric や Quorum など他のプライベート型 DLT でも部分的には見られるが，全データに関してこのような設計をとる実装は珍しい．しかし，これはシステムがビザンチン耐性を持たないということである．なお，ある資産が第三者に譲渡されるなど，二重支払いのチェックが必要になる場合には，ノータリー（notary）と呼ばれる特権ノードがチェックを行う．

各アルゴリズムの比較

最後に，コンセンサス・アルゴリズムによる性能の違いを比較する例として，耐障害性・頑健性の比較を行う．

PoW vs. PoS

パブリック型 DLT におけるコンセンサスには参加者（台帳を維持する者，コインを保持する者）へのインセンティブ，ならびに，同一人物が多数のアカウントを作成して多数派を装うシビル攻撃への耐性が求められる．これらは，誰が（優先して）ブロックを作成できるのか，誰がブロックを承認できるのか，ブロック作成や承認への報酬はどう与えられるか，という観点から分類される．

それを実現する主要なアルゴリズムが PoW（Proof of Work）と PoS（Proof of Stake）である．

PoW では Hashcash と同様に，計算能力を使用してブロックを作成させることによりシビル攻撃を防止する．作成したブロックが承認されると作成者に報酬が与えられる．ただし報酬が使用できるのはそのブロックがメインブランチに乗っている場合の

みである．一般にはブロック列が分岐した場合，より大きな計算能力が費やされている方をメインブランチとして採用する．

PoW において指摘される問題点の 1 つは，計算能力の無駄遣いである．Krause らによると，4 大暗号資産のマイニングに使用される電力量はスロベニアのそれに匹敵する[☆18]．マイニングで行っている計算は，基本的には（ランダム値に見えるような）ハッシュ値の計算であり，意味のある計算をさせることはできない．

また，PoW のインセンティブ設計上の問題点も挙げられている．一般的には，報酬はその暗号資産のネットワークおよび台帳の維持に貢献する参加者に与えられるのが望ましい．PoW では報酬はブロックの作成者（マイナー）に与えられる．マイナーは報酬を得たらそれをただちに売却してリアルマネーが得られる．ところが，暗号資産の価値を信じてそれを保持し，使用し続ける利用者にはまったく報酬が与えられないことが問題視されている．

一方，PoS では，その暗号資産を保持している，または，持ち続ける参加者に報酬を与えるような設計をとっている．ブロックの作成権利が現在の所持金額に比例してランダムに決められている実装が多い．また，ブロックの作成には計算コストがほぼかからないような設計が典型的である．また，どちらのブロックを正当なものとして認めるかという承認（投票ともいう）を，ブロック作成者以外でも行えるようになっている．ただし，ブロックの作成などに計算コストがかからないため，チェーンの分岐を促進したり二重投票を行うことが容易である．その対策として供託金制度を採用し，不正と見られる行動に関しては供託金を没収するなどの設計がよく見られる．ただし，PoS の有効性については現在でもいろいろな議論がある．

PoW ではネットワーク全体の計算能力の 51% を独占することにより，好きなブランチをメインブランチにすることができる（51%攻撃）．コインを持っている攻撃者は，あるブランチで取引所にコインを譲渡し現金を受け取る．その後で他のブランチをメインブランチに切り替えることにより，現金は攻撃者にあるまま，コインを譲渡した歴史を消すことができる．実際に，規模の小さい暗号資産のいくつかでは実際に 51% 攻撃が発生している．

ナイーブな PoS はより攻撃を受けやすい．PoW はブランチの切り替えには計算コストがかかり，失敗すると努力は無駄になる．しかし PoS ではブロックの作成が比較的容易である．そのため攻撃者は不正なブロック・ブランチを作成したり二重承認することなどが行いやすい（nothing at stake 攻撃）．対応策としては不正な行いに対してペナルティを設けることである．たとえば Tezos では，ブロック作成者と承認者にデポジットを払わせ，不正が発覚した場合にはそれらを没収する設計になっている．

パブリック型 vs. プライベート型

DLT がパブリック型であるか否かは，コンセンサス・アルゴリズムを含むアーキテクチャ全体に大きな影響を与える．

パブリック型においては台帳の維持のため，ブロックの作成者や承認者にインセンティブを支払う設計がとられている．また，相対的に大きな計算能力を持つ，もしくは，コインを長期保有している参加者が優遇されるような仕組みを持つ．欠点としては，ほとんどのアルゴリズムは厳密な意味でのファイナリティを持っていない．たとえばビットコインでは 51% 以上の計算能力を持っていると，これまでの合意結果を覆すようなブロック列を作成することが可能である．

なお，数は少ないが，EOS のようにパブリック型とプライベート型のハイブリッドなアルゴリズムを採用することにより，参加者を限定しないにもか

[☆18] Krause, M. J. and Tolaymat, T. : Quantication of Energy and Carbon Costs for Mining Cryptocurrencies, In: Nature Sustainabil-ity 1.11, pp.711-718. doi: 10.1038/s41893-018-0152-7 (2018), https://doi.org/10.1038/s41893-018-0152-7

かわらずファイナリティを実現する実装も見られる．

プライベート型 DLT は，主要な特徴として，PBFT など，ファイナリティを持つコンセンサスを採用できることが挙げられる．これは，あるトランザクションを処理する間は参加ノード数が固定であり，そのすべてを把握できていることによる．また，PoW を採用するパブリック型 DLT と異なり，無駄な計算能力を必要としない．これは高い処理性能にもつながる．

一方，パブリック型はその限られた非集中性のために，真の分散台帳でないという指摘も見られる．性能・処理速度・匿名性確保のために特権的なノードを設けることにより，単一障害点が発生したり，厳密な意味でのビザンチン耐性を損なう例が多い．たとえば Fabric の認証局・オーダラー，Corda のノータリー，Quorum の maker などである．これらの完全な解決は難しいが，それらの特権ノードをクラスタリングしそれらのコンセンサスをとることによりある程度解決できる．ただし性能は犠牲になる．

コンセンサス・アルゴリズムの課題と技術開発の方向性

これまでさまざまな DLT 実装ならびにコンセンサス・アルゴリズムが提案されてきた．しかし，DLT は非中央集権型システムにおける銀の弾丸ではなく，すべての要求を満たすことは難しい．今後は，これまでに明らかになった欠点を克服しつつ，それぞれの用途により特化した DLT の研究・開発が進むと著者は考えている．

たとえば，プライベート型 DLT は PBFT に代表されるような多数決ベースのアルゴリズムを使用してファイナリティのあるコンセンサスを実現している．一方で，少なくとも参加者の 2/3 以上がオンライン状態でないと合意プロセスが進まない，など可用性（もしくは liveness）の欠点が存在する．一般に strong leader を採用するアルゴリズムではリーダーの責務が大きく，パフォーマンス・ボトルネックおよび攻撃の対象になり得る．それを解決するため，たとえば，複数リーダーを許容する MirBFT のようなアルゴリズムが提案されている [6]．

参考文献

1) Lamport, L., Shostak, R. and Pease, M. : The Byzantine Generals Problem, In: ACM Trans. Program, Lang. Syst., Vol.4, No.3, pp.382-401, issn: 0164-0925. doi:10.1145/357172.357176 (July 1982), http://doi.acm.org/10.1145/357172.357176
2) Pease, M., Ousterhout, J. and Lamport, L. : Reaching Agreement in the Presence of Faults, In: J. ACM, Vol.27, No.2, pp.228-234. issn: 0004-5411, doi: 10.1145/322186.322188 (April 1980), http://doi.acm.org/10.1145/322186.322188
3) Castro, M. and Liskov, B. : Practical Byzantine Fault Tolerance, In : Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI' 99, pp.173-186 (1999).
4) Volzer, H. : A Constructive Proof for FLP, In : Informaion Processing Letters, Vol.92, No.2, pp.83-87 (2004).
5) Ongaro, D. and Ousterhout, J. : In Search of an Understandable Consensus Algorithm, In: 2014 USENIX Annual Technical Conference (USENIX ATC 14), Philadelphia, PA: USENIX Association, pp.305-319, IBSN: 978-1-931971-10-2 (June 2014), https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro
6) Stathakopoulou, C., David, T. and Vukolic, M. : Mir-BFT: High-Throughput BFT for Blockchains, In: CoRRabs/1906.05552, arXiv: 1906.05552 (2019), https://arxiv.org/abs/1906.05552

(2019 年 10 月 22 日受付)

齋藤　新　shinsa@jp.ibm.com

2001 年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，同年日本アイ・ビー・エム（株）入社，現在に至る．分散台帳技術における形式検証の研究に従事．2018 年より同大学院情報理工学系研究科博士後期課程に在学．

Bitcoin の革新性が導く Web 3

― cryptoeconomics という方法論とトラストレス―

首藤一幸 | 東京工業大学

Ethereum 開発者会議 Devcon 5

2019 年 10 月, Ethereum の開発者会議 Devcon 5 が大阪で開催され, 3,000 人以上の参加がありました (図 -1). Ethereum は暗号通貨の 1 つですが, 世界中の計算機を 1 台の仮想計算機に仕立てるスマートコントラクトという仕掛けをはじめ, 先進的な試みを数多く進める一大プロジェクトでもあります. Devcon 5 では私たちの研究グループも 2 件の発表をしてきました[1), 2)] (図 -2, 3).

2 日目となる 10 月 9 日 (水) の朝には, Ethereum の創始者, その 1 人である Vitalik Buterin 氏による基調講演がありました (図 -4). その中身は, ひたすら技術の話でした. これに限らず, Devcon の講演はその多くが技術 (か, さもなくばコミュニティかプロジェクト) についてのもので, どの講演も生半可な知識ではつい

図 -1　オープニングの和太鼓パフォーマンス

図 -3　首藤研メンバ (永山)

図 -2　筆者 (首藤)

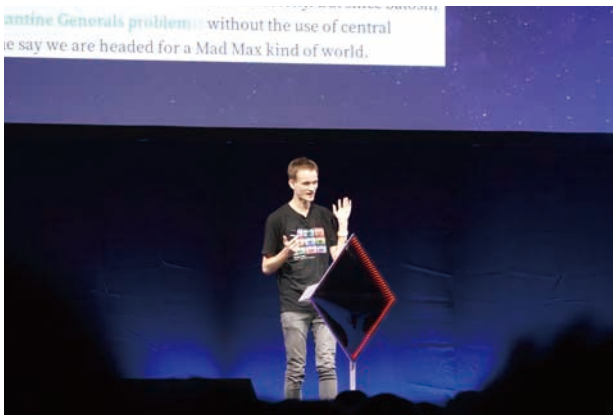


図 -4　基調講演を行う Vitalik Buterin 氏

ていけないものでした.

Cryptoeconomics

Vitalik の基調講演は「Satoshi Nakamoto は何を発明したのか?」という問いかけから始まりました. Satoshi Nakamoto は, 2008 年に発表された Bitcoin の原論文に著者として記されている名前です. つまり Vitalik は聴衆に「Bitcoin は何が革新的だったのか?」と問いかけたわけです.

そして, この問いに対する Vitalik 自身の回答は「cryptoeconomics」でした. cryptoeconomics とは, 暗号 (cryptography) と経済的動機づけ (economic incentives) を組み合わせることを指します. Bitcoin は, 公開鍵暗号方式や署名といった暗号関連の方式に加えて, 暗号通貨 BTC を欲しがる人々が行うマイニング[☆1], つまり経済的な動機付けによって支えられているわけです.

もっとも, この cryptoeconomics という言葉には, 誤解を招きやすい, という批判もあり, 筆者も同感です. つまり, 暗号通貨 (cryptocurrency) を表す俗語 crypto に, 経済学を表す economics がくっついた語になっているので, 暗号通貨に関する経済学, という意味に誤解されてしまうのです.

Vitalik は続けました. Bitcoin は cryptoeconomics を使って, 重み割り当て問題 (weight assignment problem) と動機づけ問題 (incentive problem) を解決した, と. 前者は, 1 人が無数の大勢になりすますことをいかに防ぐか?という問題で, マイニングにて計算処理 (Proof of Work) をさせることで解決しました. 後者は, いかに皆にまっとうな参加をさせるか?という問題で, マイニングの報酬としてコインを与えることで解決しました.

ただ, 実のところ, インターネット上の分散システムにて経済的動機づけを導入するアイディアは, Bitcoin が最初というわけではありません. たとえば, 筆者は, 分散コンピューティングとかボランティアコンピューティングと呼ばれる分野の研究をしていたころ, そうしたアイディアの 1 つに出会いました. 分散コンピューティングの代表は SETI@home で, つまり, インターネット上の大勢の参加者で手分けして大量の計算をしよう, というわけなのですが, 実際は, 計算をさぼって報酬や名声だけを受け取ろうとする参加者が現れかねません. よくある解決策はこうです. 複数人, たとえば 5 人 (5 台) に同じ計算を割り当てます. その 5 人の計算結果が一致したら採用します. 誰かが異なる結果を返したら, 怪しいので, 多数決で多数派の結果を採用するな

☆1 皆で競って大量の計算を行い, 行った計算の量に応じた確率で当選, つまりブロック生成に成功して, 報酬としてコインを受け取れる仕組み.

【コラム】開発者コミュニティにおける精神的支柱

Vitalik の講演を聞いて, 筆者は, Java の父と言われる技術者 James Gosling 氏を思い出しました. Gosling 氏は Java コミュニティの精神的支柱でした. 1996 年から 2017 年に開催された Java の開発者会議 JavaOne では, Gosling 氏が壇上に現れると聴衆は熱狂したものでした.

Devcon 5 開催時点で, Ethereum 上の暗号通貨 ETH には 2 兆円を超える時価総額がついています. ともすると, Ethereum のまわりにはお金にだけ興味ある人々も寄ってきて, Devcon だって大変なことになりかねません. ところが素敵なことに, Devcon の主役は技術者でした. 皆, 来たるべき分散型 (distributed)・非集中型 (decentralized) の社会を信じて, それを自分たちの手で招来しようと行動する人々です. これはもちろん Ethereum 財団や関係者の努力の賜物ですが, 何よりも, 精神的支柱である Vitalik 自身がそのように未来を創ろうと純粋に行動している技術者であるからでしょう.

り，再度別の人にその計算を割り当てるかする，というものです．この方式には，せっかくの計算能力が実質的に 1/5 になってしまうという問題があります．

そのころ出会った 1 本の論文 [3] は，参加者への経済的動機づけを活用した別の解決策を提案していました．ある計算は 1 人だけに割り当て，たまに計算の依頼側でも検算を行って結果を照合し，さぼりを検出するのです．参加者は，さぼりによる利得と，検算によってさぼりがばれた場合のペナルティを比べて，ペナルティの方が大きければさぼる方が損なので，さぼらない，というわけです．この論文が発表された場は，まさに，Financial Cryptography '01（金融に関する暗号学）という名前の国際会議でした．この国際会議は 2014 年から Bitcoin についての会議を併催するなど，暗号通貨についての研究成果が多く発表されています．

経済的動機づけの影の面

みんなが欲しがるお金を動機づけにうまく活用したことが cryptoeconomics の光の面だとすれば，それと表裏一体で発生する影の面もあります．お金による動機づけで支えられた何かは，お金で破られ得るのです．

2018 年は，暗号通貨の盗難事件が相次ぎました．事件の大きさで言えば 1 月のコインチェック事件が一番でしょうが，5 月に起きた 2 つの事件は，別の意味で筆者の目を引きました．2 つの事件とは，Bitcoin Gold 20 億円相当の盗難と Monacoin 1,000 万円相当の盗難です．これら 2 つの事件は，暗号通貨取引所のセキュリティ云々という話ではなくて，暗号通貨それ自体が攻撃されて盗まれた，と報道されました．いわゆる 51% 攻撃です．

マイニングを行う性能をハッシュレートと言い，ハッシュ毎秒（H/s）で表します．ある暗号通貨のマイニングを行う全計算機について合計したものを，俗に，その通貨のハッシュレートとも言います．ある通貨について，ハッシュレートの過半数，およそ 51% を占めることができれば，承認されたかに見えた取引をなかったことにできます．つまり，改ざんできます．これがいわゆる 51% 攻撃です．Bitcoin などメジャーな暗号通貨では千とか万とかいう数の計算機がマイニングを行っているため，ハッシュレートは大変な大きさになります．一体，どれだけの計算機を買えば 51% 攻撃できるのか……と思いきや，今どき，クラウドがあります．計算機を買い揃えずとも，クラウドを一時的に借りることができます．そして，ハッシュレートを元に計算すると，51% 攻撃に足る計算能力を借りるにはいくらかかるのかも分かります [4]．暗号通貨の攻撃は金次第，というわけです．費用対効果，つまり，攻撃で得られる金額が費用を上回るなら，悪い人にとっては，攻撃しない手はないのです．

ハッシュレートが上がると 51% 攻撃に必要な金額は上がり，ハッシュレートが下がると必要額も下がります．ここで危険なのは，暗号通貨（や，暗号通貨が支えるブロックチェーンに載っているその他の価値）およびその取引量と比較してハッシュレートの方が低い状況です．つまり，攻撃する側の費用対効果が高い状況です．ハッシュレートが低下した場合，それに応じて暗号通貨の価値もほどよく下がれば狙われてしまう可能性は上がりませんが，そううまく連動はしないでしょう．

Bitcoin や Ethereum など暗号通貨の大多数が採用する Proof of Work（PoW）で行われるマイニングでは，計算能力でコインを支えています．それに対して，今後の Ethereum 2.0 が採用する Proof of Stake（PoS）で行われるステーキング☆2 では，コインでコインを支えることになります．PoW と PoS，どちらが前述の 51% 攻撃に対して頑健か，も興味深い議論テーマです．支える側と支えられる側のどちらもコインであって連動性が高いため，PoS の方が頑健性が高い気もしますが，計算能力よりコインの方が売買や貸し借りしやすいため価格操作しやすく，頑健性は低いかもしれません．

☆2 皆で競ってコインを供託金として差し出し，差し出したコインの量に応じた確率で当選，つまりブロック生成に成功して，報酬としてコインを受け取れる仕組み．

インセンティブ不整合

暗号通貨は，コインを欲しがる人々の動機を巧みに活用して，整合性を保ちつつコイン取引情報を承認しています．ここで，承認する対象をコイン取引情報のほかにも広げたものが，ブロックチェーンです．さまざまな応用が期待されているのはご存知の通りです．コインに限らずさまざまな財貨の追跡，公証役場が行うようなデータの存在証明，金融（DeFi）を手始めとした組織の自動運営（DAO）などなど．

暗号通貨では，コインへの動機でコインを支えています．ブロックチェーンでは，コインへの動機でさまざまな応用を支えることになります．ところが，ブロックチェーンを支える人たち，つまりマイニングやステーキングを行う人たちは，別に，応用を支えてあげたいわけではなく，コインが欲しいだけです．

ここでもし，コインの価値が暴落したら何が起こるでしょうか．マイニングの参加者が減ったり，ステーキングに必要なコインが値下がりして，51% 攻撃に必要な金額が下がり，改ざんを行いやすくなります．ブロックチェーンを応用したい人にとっては，コインの値段といった外部環境の変化によってブロックチェーンの能力が損なわれる，ということになります．

このように，応用する側と支える側の動機が揃っていないことを指して，私たちは「インセンティブ不整合（incentive mismatch）」と名付けました [5]．動機を揃える一般的な方法があればいいのですが，今のところ見付けることはできていません．次善の策ですが，危険が迫ったブロックチェーンから逃げ出すことができれば，アプリケーションは守られます．文献 5）では，この，移送（マイグレーション）の方法を検討しました．

Bitcoin は何が革新的だったのか？

Vitalik は，Satoshi Nakamoto が発明したものは cryptoeconomics であった，と言いました．発明した，は言い過ぎの感があります．が，それでも，皆のコイン欲しさを引き出して活用するとここまでのことができると実証したこと，また，Ethereum をはじめ，続く試みを山ほど生み出したことは，本当にすごいことです．

一方で，では Satoshi Nakamoto は何を発明したのか？　純粋に科学的に考えると，「不特定多数」の参加者（計算機）によって不整合なく取引情報などを承認していく方式，です（図 -5）．

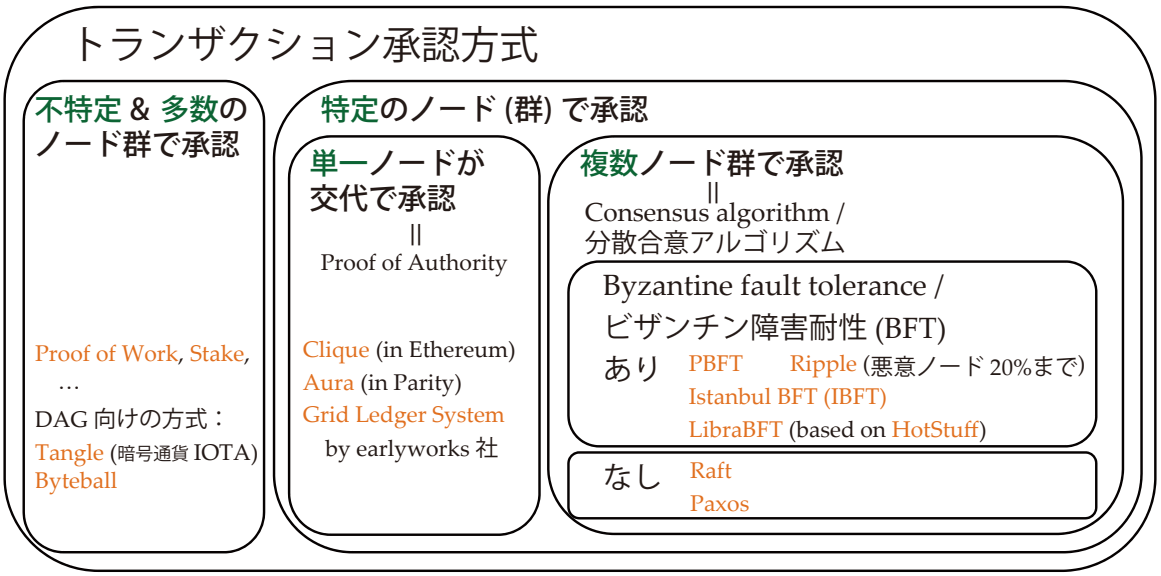


図 -5　トランザクション承認方式の分類

Vitalik は Devcon 5 の基調講演にて，ビザンチン将軍問題は Leslie Lamport 氏が 1982 年の時点で解決した，と述べましたが，その解決法は，Bitcoin や Ethereum には適用できません．Lamport 氏による解決や PBFT といった他の分散合意アルゴリズム（consensus algorithm）は参加者が「特定少数」であることを前提としているためです．参加者の数が増えると，合意に至るまでに必要な通信の回数が膨大になるので，現実的には，数台〜数十台がいいところでしょう．また，合意のためのやりとりを始めてから完了するまで，参加者の増減が許されません．暗号通貨での取引承認には千，万という多数の計算機が関与するので，故障といったトラブルは常にどこかで発生します．増減なしという前提は現実的ではありません．

それに対して，Satoshi Nakamoto が Bitcoin 論文で提案した取引承認方式は，Bitcoin のネットワークを構成する千，万の「不特定多数」で，実際に機能しています．

トラストレスから Web 3 へ

「不特定多数」による取引承認という革新が，Bitcoin が「トラストレス（trustless）」であると言われることの技術的基礎をなしています．トラストレスとは，ブロックチェーンの文脈では，人間や組織を信頼(trust)せずとも済む，という意味です．いやいや Bitcoin のソースコードやその開発者を信頼してるのでしょう？という指摘もありますが，ともあれ，信頼する対象やその形はこれまでの決済システムとはずいぶん違ったものとなっています．

暗号通貨が現れるより前の決済システムは，法定通貨にせよクレジットカードにせよ Suica にせよ，国なり銀行なり大企業なりを信頼することで成り立つものでした．それが暗号通貨では，そうした強大な権力者に身を委ねずに済むのですから，自由を信奉する人々がその可能性に大きな期待をかけるわけです．

ネットに目をやると，そこはもはや，Google 社，Facebook 社，Apple 社など何社かの巨人に支配されたようにも見えます．たとえば，スマートフォンを便利に活用して暮らす限り，よほど気を配らない限り，メッセージなどのやりとりや日々の移動先といったプライベートな情報はそうした企業群に筒抜けです．

1990 年代から 2000 年代にかけて，SNS の出現などによって普通の利用者もネットに向けて発信できるようになり，この現象は Web 2.0 と呼ばれました．それから十数年，ブロックチェーンに熱狂した人々の一部は，Web 2.0 は Google 社といった巨人たちに握られてしまったのである，と位置付け，その次のネットを Web 3 と名付けて目指し始めました．

まだ存在しない Web 3 が何であるかを厳密に定義するのは時期尚早ですが，ブロックチェーンが示した可能性にインスパイアされ，それを活用しようとしていることは確実です．すなわち，巨人たちによる支配ではなく非集中であること，また，データだけでなく実世界の価値も載り，流れること，です．

Web 3 がやってくるのかどうか，まだ誰にも分かりませんが，非集中の技術・社会を愛する筆者としては共感するところ大です．ブロックチェーンやそれを含む分散システムの研究を通じて，貢献していきます．

参考文献

1) 永山，首藤：Simulating Ethereum Network with SimBlock, lightning talks, Devcon 5（2019 年 10 月）．
2) 首 藤：SimBlock, lightning talks, P2P Summit, Devcon 5,（2019 年 10 月）．
3) Golle, P. and Stubblebine, S.：Distributed Computing with Payout：Task Assignment for Financial - and Strong-Security, Financial Cryptography '01（FC01）（2001 年 2 月）．
4) Crypto51, https://crypto51.app/
5) 首 藤，神 田，斉 藤：Towards Application Portability on Blockchains, IEEE HotICN 2018（2018 年 8 月）．

（2019 年 11 月 20 日受付）

謝辞　Web サイト [4] や暗号通貨取引所の取り組みを教えてくださった竹井悠人さん，本稿に有益なコメントをくださった斉藤賢爾さん，宮澤慎一さん，神田伶樹さんに感謝します．

■**首藤 一幸（正会員）** shudo@is.titech.ac.jp

2001 年早大大学院博士後期課程修了．博士（情報科学）．産業技術総合研究所研究員，ウタゴエ（株）取締役最高技術責任者を経て，2008 年より東京工業大学准教授．2009 年より IPA 未踏 PM を兼任．

ぺた語義

Vol. 101

CONTENTS

COLUMN

プログラムを投稿してみませんか

応般 Jr.

中学生のときに MSX2+ というコンピュータを買ってもらい，そこからプログラマとしての道が始まりました．当時は，複数の雑誌に読者から投稿されたプログラムを掲載するコーナがあり，そこに掲載されたゲームのプログラムを実行したり，改良（改悪？）したりして楽しんだことを憶えています．現在のようにプログラムをネットからダウンロードできるようなことはなく，紙に印刷されたプログラムを自分で入力（いわゆる写経）するしかありませんでしたので，入力ミスでゲームが止まるとか，無敵になるとか，いろいろと経験しました．写経プログラミングの学習効果については賛否があるようですが，少なくとも他人のプログラムを読むことには意味があるようで，プログラミングの基礎を自然に学ぶことができたように思います．その後，本格的なゲームを作りたいと思い，高校・大学と情報系の学科に進学，途中でゲーム作りを学ぶには別の学校だったんじゃないか？とやや後悔しつつも，今はゲームとは無縁のプログラムをそれなりに楽しく作っています．

さて，本誌では，本会セミナー推進委員会にご協力いただき，ジュニア会員の皆さんがプログラミングを始めるきっかけや目標になればと考え，連載「集まれ！ジュニア会員！！」の中で，皆さんから投稿されたプログラムを紹介しています．また「ぺた語義」では，今号から 4 号連続の予定で，プログラミング言語 Processing の入門記事を掲載します．

ジュニア会員の皆さん，開発したプログラムを本誌に投稿してみませんか？　Scratch や Processing はもちろん，その他，どのような言語で開発したプログラムでも OK，内容も自由です．今のところ投稿が少ない状況ですので，掲載率はかなり高めです．積極的な投稿をお待ちしています．

坂東宏和（獨協医科大学）

「集まれ！ジュニア会員！！」の投稿方法

対象作品：オリジナルのプログラムであれば，プログラミング言語・内容はどのようなものでもかまいません．

投稿方法：（18 歳未満の方は保護者の同意をもらってから）下記の情報を電子メールで本会会誌編集部門（editj@ipsj.or.jp）宛に送付してください．
- 氏名，ニックネーム（掲載時の名前），連絡先メールアドレス，（本会会員の場合には）会員番号
- 作品に利用しているプログラミング言語
- 作品のタイトル，作品の説明とこだわったポイント（簡単で OK）
- プログラム一式（メールの添付ファイルとして送付してください．Scratch のようにネット上でプログラムを確認できる場合には，URL だけでもかまいません）

その他　：掲載が決まった際には，本会ジュニア会員になっていただく必要があります．また，本会による作品の無償公開をご承諾いただいた上で，承諾書等☆1☆2 を提出していただく場合があります．
掲載された方には，掲載誌，および，IPSJ グッズを差し上げます．

☆1　論文付録データの取り扱いに関する規程（https://www.ipsj.or.jp/copyright/ronbun/supple.html）
☆2　論文誌付録データの学会利用に関する承諾書・チェックリスト（https://www.ipsj.or.jp/copyright/ronbun/furoku-shodakusho_checklisti.html）

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

ARTICLE

Processing でプログラミングに挑戦！ —第 1 回 図形を描いてみよう—

杉浦　学
鎌倉女子大学

この連載について

この連載では，プログラミングの経験が少ないジュニア会員を対象に，プログラミングの入門記事を 4 回にわたって掲載していきます．命令をマウスで組み立てる（Scratch のような）タイプのプログラミング経験があり，命令を文字で入力することに挑戦したいというジュニア会員の皆様（主に中学生〜高校生）を読者として想定しました．

記事の中には「練習問題」や次号までの「宿題」を用意してあります．文章を眺めるだけでなく，実際に手と頭を動かしながら読んでみてください．

Processing とは

プログラミングを簡単に説明すれば「コンピュータが理解できる言葉を使って，実行してほしいことをコンピュータに伝えること」といえるでしょう．

この連載では，コンピュータが理解できる言葉として，「Processing（プロセッシング）」を利用します．Processing を使えば，画面に図形を表示して動かしたり，ユーザの操作に反応したりする仕組みを手軽に作ることができます．

Processing は Java というプログラミング言語をもとにして作られています．短い命令でいろいろなことができるように工夫されており，プログラミングの初心者でも扱いが簡単です．Processing の生い立ちなどを詳しく知りたい場合は，文献 1）の『Processing をはじめよう 第 2 版』を読んでみてください．

準備

さっそく Processing を使ったプログラミングの準備をはじめましょう．Processing の公式サイトのダウンロードページ（https://processing.org/download/）にアクセスし，お使いの PC のオペレーティングシステム（OS）にあったファイルをダウンロードしてください（図 -1）．Windows で使う場合の手順を簡単に解説していきます．

図 -1　OS にあったファイルをダウンロード

Windows の場合は「processing-X.X.X-windows64.zip」という圧縮ファイル（X.X.X はバージョン番号）がダウンロードされるので，これを展開します．展開が完了すると「processing-X.X.X」というフォルダができるので，分かりやすいところ（たとえばデスクトップなど）に移動しておきましょう．フォルダの中の「processing.exe」をダブルクリックすれば，Processing が起動します（図 -2）．設定によってはセキュリティの警告が表示される場合がありますが，その場合は「アクセスを許可する」を選択してください．

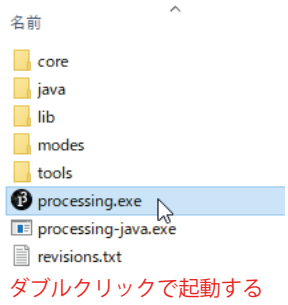


図 -2　Processing の起動

初回の起動時には「Welcome to Processing 3」と書かれた小さなウィンドウが表示されます．「Show this message on start up」のチェックを外してから，「Get Started」をクリックします（図 -3）．

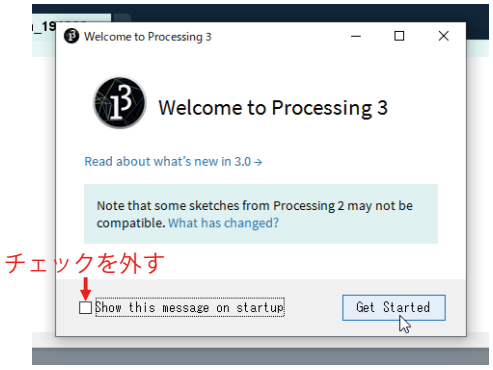


図 -3　初回起動時の設定

Processing を起動した直後の画面を図 -4 に示します．

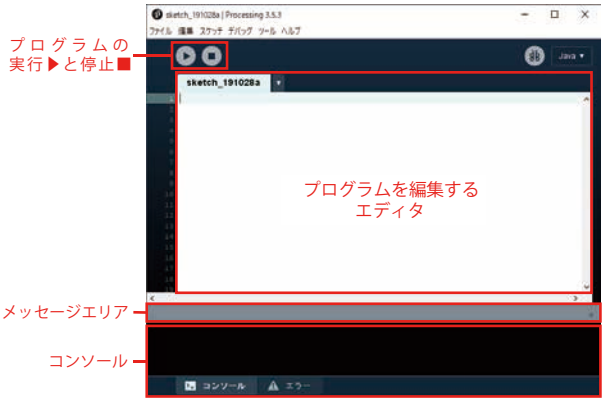


図 -4　起動直後の画面と各部分の名称

最初に日本語の入力と表示ができるように設定しておきましょう．ファイルメニューから「設定」をクリックし，「エディタとコンソールのフォント」を日本語が表示できるものに変更しておきます（図 -5）．エディタのフォントサイズも少し大きめ（たとえば 14）にしておくとよいでしょう．画面の例では「MS ゴシック」の「14」ポイントに設定しています．

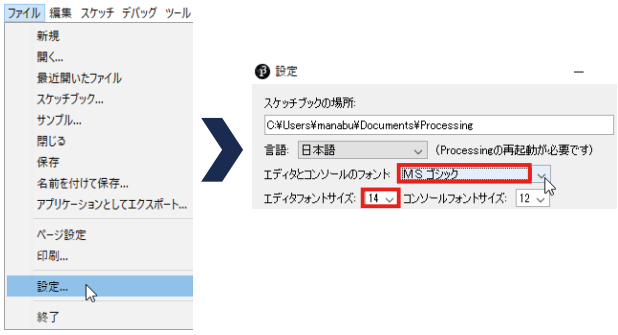


図 -5　フォントとサイズの設定

さっそくプログラムを書いて，実行してみましょう．Processing ではプログラムのことを「スケッチ（Sketch）」と呼びます．

最初は円を描いてみましょう．スケッチ 1 の内容をエディタにすべて半角で打ち込んでください．入力ができたら，プログラムを実行するために▶のボタンをクリックし，結果を確認しましょう．

```
ellipse(50,50,80,80);
```

スケッチ 1　最初のスケッチ（円を描く）

小さなウィンドウが開き，そこに円が表示されたはずです（図 -6）．スケッチの実行を停止するには■のボタンをクリックします．命令の意味については，あとで詳しく説明していきます．エラーが表示されてうまく動作しないときは，スケッチ 1 の内容が間違いなく半角で入力できているかを確認してください．

図 -6　最初のスケッチの実行

新しいスケッチには「sketch_XXXXXXX」という名前が自動的につきます．XXXXXXX は 6 桁の日付と a からはじまるアルファベットです．スケッチを保存するには，ファイルメニューから行います．Windows の場合は，ドキュメントの Processing というフォルダの中に，スケッチごとにフォルダが作成されて保存されます．たとえば，2019 年の 10 月 28 日に最初に作ったスケッチは「sketch_191028a」というフォルダの中に保存されます．フォルダの中にある「sketch_191028a.pde」というファイルをダブルクリックすると，編集の続きが行えます．スケッチの名前は自由に変更することができますが，全角の文字は自動で「_（アンダーバー）」に置換されます．半角で分かりやすい名前を入力して保存するようにしましょう．

基本的な命令の形

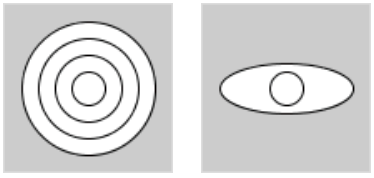
最初に試したスケッチ 1 の内容を詳しく解説し，命令の基本的な形やエラーについて整理しておきます．

スケッチ 1 は「左から 50 ピクセル，上から 50 ピクセルの位置を中心にして，幅 80 ピクセル，高さ 80 ピクセルの円を描け」という命令です．人間が相手の場合，紙を渡して「円を描いて」と頼めば，ほどよい大きさの円を描いてくれると思いますが，コンピュータの場合はそうはいきません．どの位置にどのような大きさの円を描くのか，細かく指示してあげる必要があります．

❑ 練習問題

スケッチ 1 に円を描く命令を追加して，お手本を参考に的と目玉の模様を描いてみましょう．

ヒント：上に書いた命令から先に実行され，画面の奥から図形が描かれます．



＜解説＞

的の模様を描くスケッチの例

```
ellipse(50,50,80,80);
ellipse(50,50,60,60);
ellipse(50,50,40,40);
ellipse(50,50,20,20);
```

目玉の模様の解答例は，スケッチ 3 を参照してください．

命令の基本形を図 -7 に整理しました．これを理解すれば，ほかの図形の描画などにも応用できます．Processing にはさまざまな「関数」と呼ばれる部品が用意されています．それらのうちの 1 つが円を描くための ellipse 関数です．関数は「よく使う便利な命令の集まりに，分かりやすい名前をつけて使えるようにしたもの」と理解すればよいでしょう．関数の処理に必要なパラメータ（動作を決める数値や文字など）をカッコで囲んで指定します．円の場合は 4 つのパラメータを指定して，描きたい円の詳細をコンピュータに伝えます．

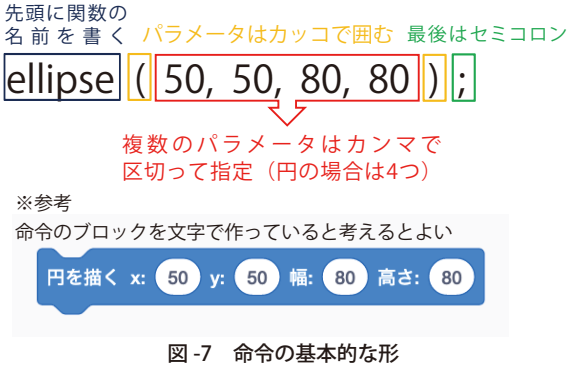


図 -7　命令の基本的な形

命令を書く際には，大文字小文字も含めて厳密に一字一句間違えないようにする必要がありますが，打ち間違いや勘違いは誰にでもあるものです．入力をしている途中や，スケッチを実行しようと思ったときに赤い波線が表示されたり，行が黄色でハイライトされたりすることがあります．これはスケッチの文法間違いなどのエラーを示しています．エディタの下のほうにあるメッセージエリアに，エラーの内容が表示されます．それをヒントに修正をする必要があります(図 -8)．

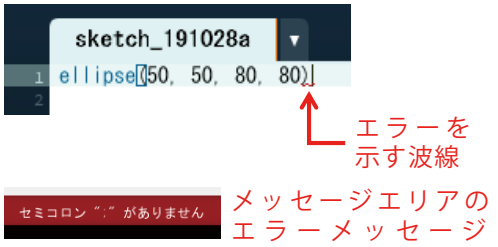


図 -8　エラーの表示

❑ 練習問題

次のスケッチはエラーで実行できません．修正すべき部分を考えてみましょう．実際にエディタに入力してみるのもよいでしょう．

```
ellipse 50,50,100,100;
ellipse(50 50,80,80);
elipse(50,50,60,60)
```

＜解説＞

1 行目：パラメータを囲むカッコがない
2 行目：最初の 50 の後にカンマが抜けている
3 行目：ellipse のつづりが間違っているし，行末のセミコロンがない

スケッチの命令はすべて半角で入力します．誌面だと分かりにくいですが，スケッチ 2 の 1 行目は最後のセミコロンが全角です．2 行目は 2 番目のパラメータの前に全角のスペースが入っています．スケッチ 2 のように書いてしまうと，エラーが発生して実行ができません．

```
ellipse(50,50,80,80);
ellipse(50,　50,80,80);
```

スケッチ 2　全角の入力でエラーになる例

命令の本体を書くのに全角は使えませんが，スケッチに日本語でメモ書きを加えることはできます．これを「コメント」と呼びます．複数行の場合は /* と */ で囲み，1 行の場合は // をはじめの部分に記入します．コメントは灰色の文字色で表示されます．目玉の模様を描くスケッチにコメントを追加した例がスケッチ 3 です．

```
ellipse(50,50,80,30); //白目を描く
ellipse(50,50,20,20); //黒目を描く
```

スケッチ 3　目玉の模様を描く(コメント付)

Processing のエディタにはスケッチを自動的に読みやすくしてくれる機能があります．編集メニューの「自動フォーマット」がそれです (図 -9)．こまめに自動フォーマットをすれば，カンマの後にスペースが挿入されたりして，スケッチを読みやすい状態に保つことができます．

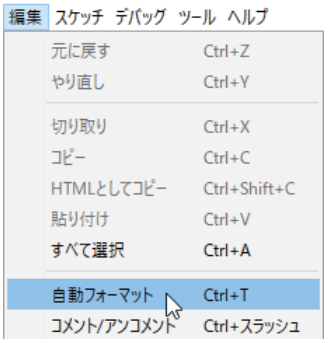


図 -9　自動フォーマット

座標と図形

コンピュータの画面はピクセルと呼ばれる細かい点が集まってできています．この点に座標をつけることで，画面上の位置を指定します．Processingの場合は，実行結果を表示する画面の左上が原点(0, 0)に設定されます．画面の大きさを指定しない場合は，自動的に縦横が100ピクセルの画面が開きます．スケッチ1を実行したときの画面の大きさと座標を図-10に示します．

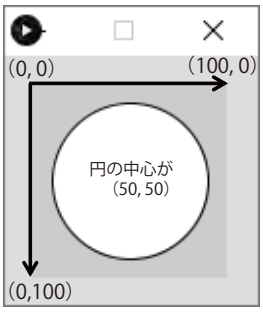


図-10　画面の大きさと座標

画面の大きさを指定したい場合は，スケッチの最初にsize関数による設定を加えます．幅480，高さ120のウィンドウを開き，ウィンドウの中心(240, 60)の座標に1ピクセルの大きさの点(point)を描くには，スケッチ4のように命令します．

```
size(480,120);
point(240,60);
```

スケッチ4　ウィンドウの中心に点を描く

基本的な図形を描画するための関数と座標などのパラメータを図-11に整理しました．試しにいろいろな図形を描いてみましょう．

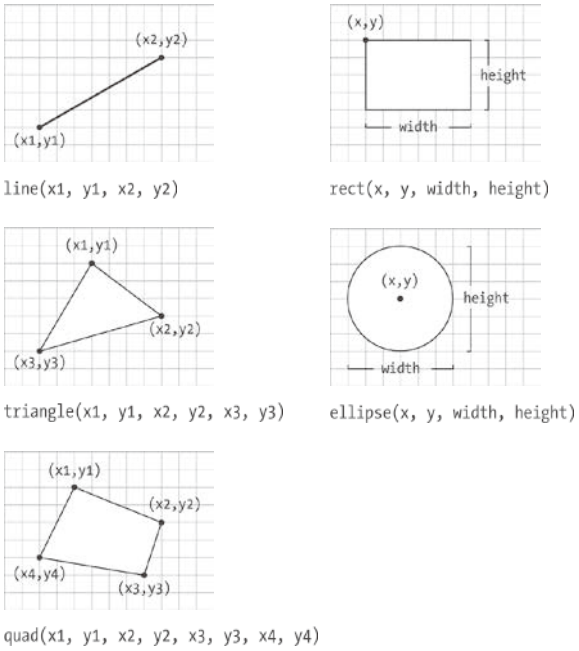
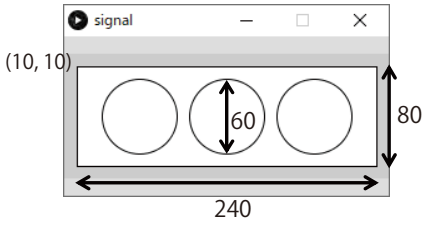


図-11　いろいろな図形を描く関数（文献1）P.19より）

● 宿題

お手本を参考に，信号機を描いてみましょう．今回はモノクロですが，次号で色を付けていく予定です．



画面のサイズは横260，縦100
円の中心は左から(60, 50)(130, 50)(200, 50)

参考文献

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

(2019年10月31日受付)

杉浦　学（正会員）　manabu@kamakura-u.ac.jp

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

基礎

第 12 回全国高等学校情報教育研究会 全国大会（和歌山大会） Next Stage ～次代の担い手を育む情報教育～

肥田真幸
和歌山県教育庁学校教育局県立学校教育課（兼）義務教育課

全国大会開催への思い

私は，県立高等学校の教諭であった 2017 年度，本県での全国高等学校情報教育研究会（以下，全高情研）全国大会の開催を和歌山県情報教育研究会（以下，県情研）に提案した．同じ思いの教員の賛同を得て，大会開催に至った．

本県の情報教育の気運を高めるため，全高情研全国大会を和歌山の地で開催することは，私にとって以前からの目標の 1 つであった．そのため，2018 年度に教育委員会へ異動した後も，実行委員の一人として情報教育の推進に邁進し，第 12 回全高情研全国大会（和歌山大会）の運営にかかわってきた．

本大会は，大会運営をはじめ，たくさんの方々の協力のもと，県内外から多くの方々に参加をいただき，盛大に開催することができた．

本稿では，本大会について報告するとともに，全国大会を地方で開催する意義や今後の展望，本県の情報教育の取組について述べる．

第 12 回全高情研全国大会（和歌山大会）の報告

平成から令和に改元し，新しい時代が幕開けした今年（2019 年），8 月 10 日・11 日の 2 日間の日程で開催された．

主催である全高情研は，高等学校で「情報」を教える教員の情報交換を目的とした団体である．全国の情報科担当教員や情報教育の関係者が事例発表や情報交換を行う場として，年に一度，全国大会を開催している．

本大会は，第 12 回大会であり，国立大学法人和歌山大学を会場として開催し，全国から 378 名が来場した．この参加者数は，東京都で開かれた第 10 回の記念大会に次ぐ人数であり，地方開催では最多となった．

開会行事では，県情研会長・大会実行委員長である県立和歌山工業高等学校長 西村文宏氏による開会宣言の後，全高情研会長・東京都立田無高等学校長 山下一郎氏から開会の挨拶があった．続いて，来賓として和歌山県教育委員会教育長 宮﨑泉氏，国立大学法人和歌山大学長 伊東千尋氏から祝辞をいただき，大会が幕開けした（図 -1）．

今大会のテーマは，「Next Stage ～次代の担い手を育む情報教育～」である．これは，第 1 回大会のテーマである「Next Stage ―新たに広がるネッ

図 -1　開会式の様子

トワークの構築―」を参考にして掲げたものである．情報教育が次のステージに進み，本大会が次代の「はじまり」として，新しいスタートを切るという思いが込められている．

本テーマにあるように，情報科にとって新しい時代の「はじまり」ともいえる新学習指導要領の実施を見据えた内容を含んだ実践事例等が，28 の分科会（図 -2）ならびに 24 のポスターセッションで発表された．

本大会の分科会，ポスターセッション発表では，特に「プログラミング教育」に関する事例が多く，注目を集めた．新学習指導要領ではプログラミング教育が小学校から必修化され，中学校でプログラミング教育に関する内容が充実し，高等学校「情報Ⅰ」でも必修化されるといった動向の中，全国の情報科担当教員のプログラミング教育への注目度はより高まっていると考える．今回，本県からも，本県が推進するプログラミング教育について分科会発表を行った．

また，「情報Ⅰ」の年間指導計画や，新学習指導要領の内容として充実が図られているデータ利活用，情報セキュリティ，情報モラル，情報デザイン等に関する事例発表にも注目が集まった．

新学習指導要領における情報科目の授業の検討，実施に向けた準備が各地域で始まり，次代を担う生徒に必要とされる資質・能力の育成のためには，これまで以上に教員の高い専門性が求められている．

図 -2　分科会発表の様子

各分科会において発表後の質疑応答や情報交換も活発に行われ，参加者にとって新しい課題の発見や解決につながる有意義な時間となった．

基調講演では，東京大学・慶應義塾大学教授（元文部科学大臣補佐官）鈴木寛氏による，「AI 時代の教育」と題したご講演をいただいた．その中で，国内外の教育に関する調査報告や動向，AI 時代に求められる資質・能力，論理的思考力や情報活用能力の重要性，また情報産業への人材育成が急務であること等，Society 5.0 に向けた教育や人材の育成等の課題と展望についてお話をいただいた．

基調講演に引き続き，文部科学省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 鹿野利春氏による講評講演が行われた．講演では，社会の変化に伴う情報教育の進展について触れられ，情報科担当教員として，不断の研究や教育実践，その蓄積，そして共有が大切であるといった内容のお話をいただいた．

閉会行事では，大会実行委員長の挨拶の後，次回の開催県である愛知県情研会長・愛知県立安城東高等学校長 花井和志氏による挨拶があった．続いて，神奈川県高等学校教科研究会情報部会長・神奈川県立横浜立野高等学校長 菊地勇人氏が閉会のことばを述べ，大会は幕を閉じた．

全国大会を地方で開催する意義

本大会を本県で開催したことによって，地方での全国大会開催はとても意義があると感じた．それは，全国大会開催が，本県の情報科が抱える課題解消に向けた，効果的な一歩となったからである．

情報科については，本県を含み次のような課題を持つ地域が多い．

- 情報科を専門とする教員が少ない．
- 次年度に教科担当者が代わる学校もあり，教科研究部会や研修会等への継続的な参加者が少ない．
- 各学校における教科担当者が一人であることが多

く，授業の内容について，校内で相談しにくい．

各地域が抱えるこれらの共通した課題は，情報教育を推進しようにも，各学校の担当教員の意識を高めにくいといった状況を生む．全国大会の開催によって，これらの課題の解決に向けた，いくつかの糸口を見出すことができた．

その１つ目は，これからの教育において，情報科の授業の必要性がより高まっていることを参加した教員が感じてくれたことである．本県では情報科専門教員が少ない中，各学校から情報科担当教員等が大会運営スタッフとして，50 名近く参加してくれた．他県スタッフからも，「県内スタッフのこの人数は前例がない．和歌山県の運営は力強い」と称賛の声をいただいたほどである．県内スタッフとして参加した教員が，運営にかかわりながら，全国の授業実践や動向を知ることで，「情報Ⅰ」「情報Ⅱ」という新科目への期待とそれを効果的に実施していこうとする意識がより高まったように感じる．

また，本県では今年度（2019 年度）から，「きのくに ICT 教育」（※内容は最後に触れる）の推進を本格的に開始しており，各学校でプログラミング教育をはじめとする情報教育を推進している．こうした中，今回の全国大会の開催は，プログラミング教育を担当する教員の意識をより前向きに変えるといった相乗的な効果をもたらした．

２つ目に，教員のコミュニティが活性化されたことである．前述したとおり，本大会の参加者数は，378 名であった．これは，実行委員として尽力してくれた教員が目標を１つにし，大会の開催を広く周知した成果である．

また，実行委員会の母体である県情研に所属する教員が，前年度から会議を重ねるうちに，教員間のコミュニケーションがより活性化され，つながりが強くなった（図 -3）．こうした中，各教員の大会の成功を切望する思いが高まり，さまざまな場面で，積極的に情報を共有していこうという動きが生まれた．このことが何よりも有益であった．

さらに，全高情研のメンバから大会運営のノウハウを得る中で，本県教員と他地域の教員とのつながりが広がった．これは，今後，県内の情報教育を進めていく上で，強みとなるであろう．

３つ目に，情報科の授業の実施にあたって，教員が主体的に取り組む意識をより高めたことである．実行委員会のメンバをはじめ，スタッフとして参加した県内の教員が各分科会やポスターセッション，基調講演や講評講演を通じて，情報教育の全国的（世界的）な動向を「自分事」として捉えてくれた．このことによって，多くの情報科担当教員が，AI リテラシー教育やデータ利活用，プログラミング教育等の必要性やこれからの社会におけるその役割を主体的に考え，子供たちに教えるべき内容を更新していく必要があることを再認識することができた．

本大会は，本県の高等学校における情報教育推進のまさに起爆剤となり，情報教育を重視し進めていくきっかけとしても重要な意味を持つものになった．私は，このきっかけを土台として，これからも県内の情報科担当教員の意識・専門性・教科指導力の向上ために邁進し，本県の情報教育を牽引していきたい．

地域の教科研究部会の意義

地方における研究部会が果たす役割は大きいものがある．県内では，県情研が教科研究部会の役割を担い，情報科の授業の質向上を図ってきた．

図 -3　全国大会本部での打合せの様子

県情研の全高情研への加盟は，まだ歴史が浅いが，全国大会の開催を成功に導く上で，情熱を持った教員とそれを束ねる県情研の存在および功績は大きかった．他地域においても，教科研究部会をはじめとした情報を共有できる機会やコミュニティの構築を図ることは，情報教育の推進にとって有効な手立てになると考える．情報科担当教員の指導力向上や教員同士の情報共有，相談しやすい環境づくりは，情報教育が要となるであろう次代の教育の充実に向けて非常に重要な要素であり，次代を担う子供たちの育成に大きな影響を与えるものである．

和歌山県「きのくに ICT 教育」

最後に，本大会でも発表させていただいた，本県が推進している「きのくに ICT 教育」を紹介したい．本県では，新学習指導要領の実施に先立ち，今年度（2019 年度）から県内すべての小・中・高等学校および特別支援学校で，発達の段階に応じた体系的なプログラミング教育を実施している．

小学校では，5・6 年生で各 8 時間，中学校では技術・家庭科（技術分野）で 3 年間を通して合計 25 時間，高等学校では共通教科情報科の授業で 20 時間程度のプログラミング教育を，小・中・高等学校で体系的に実施することとしている．

また，小・中・高等学校それぞれのプログラミング教育に関する学習指導案を県教育委員会で作成し，プログラミング教材とともに配布した（図 -4）．さらに，校種ごとの教員研修の実施やプログラミング教育支援員等の学校への派遣，公開授業等の実施など，プログラミング教育の推進に努めている．

「きのくに ICT 教育」を通して，次代で活躍できる情報活用能力に長けた人材が本県から多く育つことをめざしている．

図 -4　きのくに ICT 教育・学習指導案

きのくに ICT 教育に関する情報

- 学習指導案
  https://www.pref.wakayama.lg.jp/prefg/501100/ictforum.html
- 和歌山県教育広報テレビ番組「はばたく紀の国～教育は今～」
  https://www.pref.wakayama.lg.jp/prefg/500100/kouhou/habatakukinokuni/habatakukinokuni.html
  https://www.youtube.com/watch?v=sTIX0ZJ9mko&feature=youtu.be

（2019 年 11 月 8 日受付）

肥田真幸　hida_m0001@pref.wakayama.lg.jp

2012 年，高等学校教員として和歌山県に採用される．現在，和歌山県教育庁学校教育局県立学校教育課（兼）義務教育課に所属．情報科担当指導主事として情報教育，ICT 教育の推進等を担当している．

● 論文誌ジャーナル掲載論文リスト

Vol.61 No.1（Jan. 2020）

【特集：活き活きとしたスマートシティを実現する高度交通システムとパーベイシブシステム】

■ 特集「活き活きとしたスマートシティを実現する高度交通システムとパーベイシブシステム」の編集にあたって　齋藤正史
■ Bikeinformatics : an introduction of informatics to the motorcycle researches and the development of new generation motorcycle-based personal vehicles　Tomoya Kitani
■ Smartphone-based Mental State Estimation : A Survey from a Machine Learning Perspective　Yusuke Fukazawa 他
■ Bandwidth Control Method and Available Bandwidth Estimation Method for Aggregated Traffic　Tetsushi Matsuda 他
■ 分散アンテナを用いたアクセスポイントによる無線 LAN 端末位置推定方式　細田真道 他
■ 特徴点地図と単眼カメラ画像の時系列照合によるロバスト位置推定手法の提案　武山洪二郎 他
■ Method to Improve Accuracy of Indoor PDR Trajectories Using a Large Number of Trajectories*　Kosuke Yotsuya 他
■ 運転者が保持する車間時間に着目した交通流シミュレーションによる交通流と交通事故防止についての解析　隅田康明 他
■ FlowScan : Estimating People Flows on Sidewalks Using Dashboard Cameras Based on Deep Learning　Yusuke Hara 他
■ Anomaly Detection Method “Cumulative Sum Detection” for In-Vehicle Networks　Jun Yajima 他
■ DeepCounter : 深層学習を用いた細粒度なゴミ排出量データ収集手法　三上量弘 他
■ 平面交線を用いた 3 次元点群データの位置合わせ手法の開発　北川悦司 他

【オープンイノベーションを加速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「オープンイノベーションを加速するコラボレーション技術とネットワークサービス」の編集にあたって　大平雅雄
■ Vection 誘発映像と前進動作による坂道シミュレーション　本岡宏将 他
■ 気持ちの共有を支援するウェアラブルパブリックディスプレイのシールプロトタイプ　西村優里 他
■ 参照物体を用いた大きさの印象を伝える画像インタフェース　松　佳奈 他
■ 地域に関する新たな発見を促す散策支援システム *　福島　拓 他
■ migaco : 子供が楽しく歯みがきが行えるようにするための歯ブラシ動作計測機能付きアプリケーション　市村　哲

【一般論文】

■ Fast Directional Energy Interchange Used in MCMC-Based Autonomous Decentralized Mechanism toward Resilient Microgrid　Yusuke Sakumoto 他
■ 音声中の検索語検出におけるクエリの関連語を利用したリスコアリング方式　丹治　遥 他
■ 文のトピックを考慮した単語置換によるユーモア発話を行う対話型エージェント *　呉　健朗 他
■ 消費者行動モデルに基づく商業地域コミュニティにおけるポイント付与効果の分析　家入祐也 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

（Jan. 2020）

【論文誌 プログラミング Vol.13 No.1】

■ 組込マイコン向け C コンパイラにおけるストアの融合とループ化の実装　千葉雄司 他
■ Finding Errors in Registrations of Local Variables Using Coccinelle for Accurate Garbage Collection　Tomoharu Ugawa 他

【論文誌 データベース Vol.13 No.1】

■ 説明性向上のためのユーザレビューを用いた観光スポットの対応付け手法　潘　健太 他
■ Detection of Mergeable Wikipedia Articles Utilizing Multiple Similarity Measures　Renzhi Wang 他
■ 大規模時系列テンソルによる多角的イベント予測　本田崇人 他
■ Secondary Index を活用する NoSQL スキーマ推薦によるクエリ処理高速化　涌田悠佑 他
■ ゲートレス鉄道サービスに向けた GPS 位置情報を用いた乗車区間判定方式の評価　根本　潤 他

【Transactions on Bioinformatics Vol.13】

■ A Bayesian Nonparametric Topic Model for Microbiome Data Using Subject Attributes　Tasuku Okui

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

動画制作授業のすゝめ ―動画制作の授業を通して「問題解決」を実践する―

飯田秀延　東京都立小金井北高等学校

授業の概要と意義

アプリケーションソフトウェアの操作方法が主な動画制作の授業は，画一的な作品しか生まれない傾向にある．また，ソフトウェアが変わると，操作ができなくなることも多い．これでは情報の活用能力が得られたとは言いがたい．そこで課題解決型のアクティブ・ラーニングの手法をとり入れ，能動的に動画制作（問題解決）を行うことにより，生徒の創造的な思考力や，問題を発見したり解決したりする能力を育むことを目的とした授業実践を行ったので，紹介する．

この授業は，5～6名ごとにグループを作り，グループごとに1つの動画作品を制作する．生徒は，途中で教員に対して作品内容のプレゼンテーションを行う．また，最後にクラス全体で上映会を行い，生徒全員による相互評価を行う．

テーマはグループごとに自由（ただし公序良俗に反しないこと）とし，機材の貸し出し等も行わない．撮影場所や衣装なども生徒の自由とする．また，編集に使用するソフトウェアも自由とする．ちなみに本校の場合，ソフトウェアについては，半数ほどの生徒はPC教室にインストールされていたAdobe社のPremiereあるいはMicrosoft社のムービーメーカーを使用していたが，残りの半数の生徒はフリーソフトであるAviUtlや，iPhoneアプリのInShotなどを自前で用意して使用していた．

グループ内で役割分担を決め，プロジェクトマネジメントを意識[1]しながら，役割に従って作業を行う．スケジュール管理も生徒が行う．

このように課題解決型のアクティブ・ラーニングの手法をとり入れることにより，グループ内でコミュニケーションをとり，自主的に作業を行うことで，「知識および技能」や「思考力・判断力・表現力」

のみならず，「学びに向かう力，人間性」などの向上も図れる．

本授業により期待される効果を表 -1 に示す．

授業の準備

授業の冒頭で，以下の 2 項目を明確に示す．

- 作品を相互評価する際の基準
- 上映会までの授業スケジュール

なお今回の授業では，全部で 6 時間（1 カ月程度）の授業を想定している．

授業では過去の優秀な作品を数本，見本として上映する．過去の作品（比較的できのよいもの）を自由に閲覧できるよう，共有のドライブなどに置いておくのも効果がある．

生徒に対して，ネットワーク上でグループのメンバが自由に読み書きすることができる十分な容量の作業スペースを用意する必要がある．

教員が機材などの準備を行わない．そのため生徒たちは，作品スタイル，使用するアプリケーションソフトウェア，必要な機材，役割分担，スケジュールなどをグループ内でお互いに話し合い，検討することにより，可能な範囲でその都度選択する．それぞれの機材やソフトウェアの長所・短所および操作方法を，教え合ったり自分たちで発見したりしながら学習できる．そのため，機器やソフトウェアの操作方法を，一斉講義型による授業よりも効果的に身に付けることができる．

■表 -1　本授業により期待される効果

	期待される効果
主体的に学習に取り組む態度	グループメンバでの話し合いで，テーマ，使用するアプリケーションソフト，機材，スケジュール管理などのすべてを決めさせることにより，生徒に自主的に取り組む態度を持たせることができる．
生徒自ら課題を設定する機会の設置	従来のように見本と同じような作品を制作するのではなく，制作内容をグループごとの話し合いで自由に決定することにより，生徒自らが課題を設定する機会が得られる．
生徒が思考・判断・表現をする機会	作品スタイル，使用するアプリケーションソフト，必要な機材，役割分担，スケジュールなどを生徒たちがグループ内でお互いに話し合い検討し決定することにより，グループごとにさまざまな作品が生まれ，生徒が思考・判断・表現をする機会が得られる．
自己評価や相互評価などの実施	お互いの作品に対して自己評価および相互評価を行うことにより，さまざまな価値観や表現に接する機会が得られる．
多様な成果物	1 つとして同じようなもののない映像作品が，グループごとにできあがる．

授業の流れ

役割分担を決める

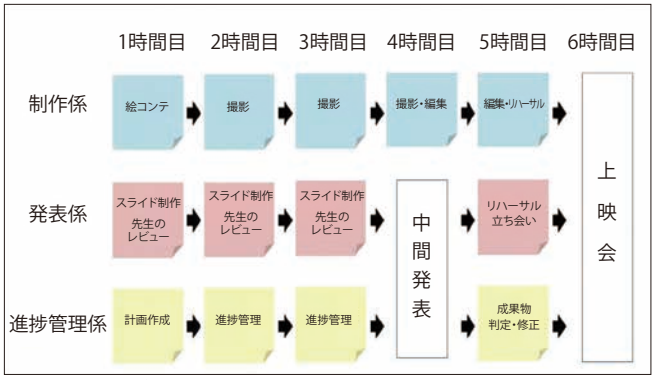
役割分担の例を下記に示す（6 人の場合）．

- 制作係（4 名）
- 発表係（1 名）
- 進捗管理係（1 名）

制作係は，撮影や編集を実際に行う．シナリオ制作，BGM，絵コンテ，機材調達，小道具，撮影場所，撮影機材などに関して責任を持つ．発表係は，作品の内容や進捗を授業の中で教員に報告し，レビューをしてもらうと同時に，その内容をグループに伝える．進捗管理係は，計画の作成と確認，全体の進捗の把握，リスク管理，上映会の運営や振り返りなど，グループのまとめ役を担う．なお役割分担については，各校の生徒の実態に応じて適宜設定してもよい．

スケジュールを決める

進捗管理係を中心にスケジュールを決める．スケジュールの例を図 -1 に示す．なお，スケジュールは付箋などで作成し，変更があるたびに進捗管理係が更新を行っていくようにするとよい．



■図 -1　スケジュール例

ストーリーを作る

制作係は絵コンテを作成する（図 -2）．教員はあらかじめ絵コンテ用紙を印刷して用意しておくとよい．

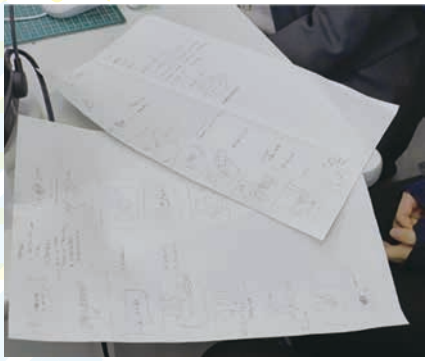
絵コンテで具体的なシーンをイメージすることができたら，どのように撮影するのかを計画する．どのカメラを使うのか，いつどこで撮影するのか，誰が出演するのか，出演の交渉や撮影の許可は必要なのか，三脚や照明は必要なのか，BGM はどうするのかなど，計画をしなければいけないことはたくさんある．

撮影を行う

制作係を中心に，計画に従って撮影を行う（図 -3，図 -4）．この授業では，作業の過程を自分たちで計画し実行することで主体性が生まれ，撮影を能動的に行う姿が見られる．なおグループによっては休日に校外で撮影を行うことも考えられるので，撮影マナーを守るよう注意する必要がある．

No.

シーン/カット	画面/絵	内容/セリフ	時間
シーン カット			
シーン カット			



■図 -2　上：絵コンテの様式例　下：生徒が制作した絵コンテの例

編集を行う

制作係を中心に，撮影した映像の編集を行う（図 -5，図 -6）．多くの動画編集ソフトウェアは，おおむね「設定」「タイムライン」「プレビュー」の 3 つの要素から構成される．ソフトウェアに応じて適宜作業を行う（近年はスマートフォンのアプリで編集を行う生徒も多いので，それを許可してもよいと思われる）．

なお，動画編集ソフトウェアで編集した動画は，そのままでは動画ファイルにならない．最後にレンダリング作業をして MP4 や WMV などの形式の動画に変換する．この際，AVI 形式などの非圧縮の形式で出力してしまうと容量が大きくなりすぎるので注意が必要である．

■図 -3　撮影風景の例（屋内）

■図 -4　撮影風景の例（屋外）

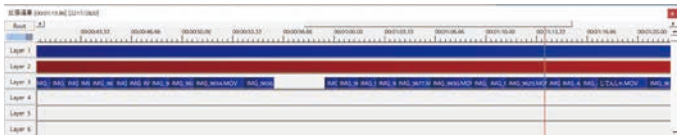
プレゼンテーションの準備

発表係は，グループの進捗を毎時間教員に報告してレビューをしてもらい，その結果をグループへフィードバックする．また，中間発表では，グループの作品の内容に関するプレゼンテーション行う．

なお，この中間発表の作業は，撮影や編集を行わない生徒が暇になるのを防ぐことが目的でもある．したがって，もしそのような生徒が出ないような学校であったり，時間的に中間発表を行うことが難しかったりするようであれば，発表係を置かずに，撮影と編集の作業に注力させてもよい．


設定画面


プレビュー画面


タイムライン

■図 -5　編集ソフトウェアの例

■図 -6　編集風景

上映会と相互評価

最後に上映会および相互評価を実施する．すべての生徒がそれぞれのグループの作品に対して，たとえば①企画力 ②技術力 ③努力 ④独創性・芸術性の 4 項目について 5 段階で評価を行う（図 -7）．なお，簡単なコメントも記入させ，各班にフィードバックしてもよい．

お互いの作品に対して相互評価を行うことにより，さまざまな価値観や表現に接する機会が得られる．

留意事項

課題解決型のアクティブ・ラーニングをとり入れた動画制作の授業の大まかな流れを紹介した．以下に，いくつかの留意事項を述べる．

教員はファシリテータ

教員の主な役割は，教室の中を絶えず巡回して，話し合いが停滞しているグループの議論を活性化させたり，積極的に参加していない生徒に参加を促したり，作業で分からないことがある生徒に技術的な助言を与えたりするにとどめ，できるだけ「教えない」ように徹したい．

機器の進歩は早い

スマートフォンなどの情報機器の進歩は早い．学校で機材を用意してもすぐに陳腐化してしまう．そのため，機材は生徒の自前のものを使用させるのが

	①企画力	②技術力	③努力	④独創性 芸術性
1 班	5	4	3	3
2 班	4	3	5	5
3 班	4	2	3	2

■図 -7　相互評価シートの例

よい. 生徒は意外と情報機器を活用できていない(スマートフォンのデータをPCに移す方法を知らない生徒も多い). 自前の機材を使用させることは, 身の回りの情報機器の活用方法を学ばせる良い機会にもなる.

著作権等の取り扱い

授業内での閲覧にとどめ, 安易にSNSなどにアップしないように注意を促す必要がある.

ほかの教員とのコミュニケーション

生徒には「くれぐれもほかの先生の迷惑にならないように」という注意を行うが, それでも撮影に際して, ほかの教員に迷惑をかける可能性がある. そのため, 特に担任の教員を中心に関係しそうな教員にあらかじめ授業の内容などを説明し, 理解しておいてもらう必要がある. 場合によっては職員会議などの場で周知しておくことも, トラブルを回避するためには大切である.

作品例と生徒の反応

本校で制作されたある年の1クラス分の作品の例(サムネイル)を図-8に示す. このクラスでは最も短い作品で約30秒, 最も長い作品で約15分であったが, おおむね3分ほどのものが多かった. また, 授業外の撮影は, 1～2週間程度放課後や早朝に集まって撮影したり, 休日に校外で数日にわたって撮影したりした班もあった. このようにして, 非常に多彩な作品(力作)が制作された.

アンケートの結果, ほとんどの生徒が, この授業によって, 主体的に学習に取り組む態度が育成されたと実感していることが確認できた[2]. また「今回のようなアクティブ・ラーニングの授業を今後も受けたいか」という質問に対しては, 86%の生徒が「ぜひ受けたい」または「どちらかというと受けたい」と回答した. 生徒自身も, このような授業は楽しく効果があるものだと感じているようである. 本稿が, 高等学校の先生方における授業改善の一助になれば幸いである.

参考文献

1) 駒井明喜：SE力 自ら成長し最高の成果をあげる方法, TAC出版 (2014).
2) 飯田秀延：アクティブ・ラーニングによるビデオ制作実習の実践, 東京都高等学校情報教育研究会研究紀要, pp.29-33 (2013).

(2019年10月31日受付)

飯田秀延 Hidenobu_Iida@member.metro.tokyo.jp
1994年松下技研(株)入社. 画像処理に関する研究開発に従事. 2017年入都. 現在情報科主幹教諭.

■図-8 作品例

IPSJ MAGAZINE Vol.61 No.2 (Feb. 2020)

CONTENTS

読後のご意見をお送りください

本誌では，現在約 120 名の方々に毎号のモニタをお願いしておりますが，より多くの読者の皆さんからのご意見，ご提案をおうかがいし，誌面の充実に役立てていきたいと考えておりますので，毎号巻末に掲載しております所定の用紙または Web ページ（https://www.ipsj.or.jp/magazine/enquete.html）をお使いいただき，奮って事務局までお寄せください.

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

…▸ 米谷雄介（香川大学 創造工学部／総合情報センター）

ティッピング・ポイント
―いかにして「小さな変化」が「大きな変化」を生み出すか

マルコム・グラッドウェル 著，　高橋　啓 訳
飛鳥新社（2000），310p.，1,700 円+税，ISBN：978-487031-394-1

ティッピング・ポイントとは何か？

本書は「あるアイディアや流行もしくは社会的行動が敷居を越えて一気に流れ出し，野火のように広がる劇的瞬間のこと」をティッピング・ポイント（ティップ（tip）は「傾く」という意味）と名付けています．本書は，シューズブランドの人気上昇，ニューヨーク市の犯罪率の低下，病気の感染，「セサミ・ストリート」成功の秘訣，エアウォーク社の販売戦略，禁煙運動がなぜ功を奏さないのかなどの具体的な事例を紹介し，さまざまな領域における「感染」について述べています．これらの感染現象は，一見すると，不可解で，不合理で，予測を超えたものであるように見えます．このような直感に対し，これらの感染現象に共通する原則を見出し，提案しているのが本書です．また，本書では，このような原則の存在は我々人間が誰しも変革を起こす潜在能力と知的活動の力を持つことを意味している，とも述べられています．本コラムの読者が，爆発的感染の 3 原則に基づいて周囲の世界を眺め，「どこを押せば世界が傾くのか」を考えることのきっかけに知見を利用してもらえれば幸いです．

爆発的感染の 3 原則

原則 1：少数者の法則

1 つ目は，少数者の法則です．これは，「情報を伝える人の要因」に関する原則です．上記のような種々の社会的伝染が成功する鍵は，ある特別な社会的資質の備わった人物が関与しているかどうかにかかっていると本書は述べています．それは，「コネクター（媒介者）」「メイヴン（通人）」「セールスマン」の 3 種類の人物です．

コネクター（媒介者）は人脈のプロです．知り合いが多く，また単に知り合いが多いというだけでなく，さまざまな世界，文化領域を股にかけた活動をしているという特徴を持ちます．メイヴン（通人）は情報のプロです．知識を蓄えており，また蓄えるだけでなく有用な知識を人に教えたがっているという特徴を持っています．セールスマンは説得のプロです．メイヴンは情報源の役割を果たし，コネクターが通信路の役割を果たすのに対して，セールスマンは受け手に応じて情報を分かりやすく再構成する役割といえます．

原則 2：粘りの要素

2 つ目は，粘りの要素です．これは，「情報そのものの要因」に関する原則です．人に強い印象を与えるための鍵は，アイディアそのものに備わる品質にあると思われがちですが，社会的伝染においては，必ずしもそうではなく，「余白の部分」で提示方法にちょっとした工夫を加えることで一気に伝播させることができると述べられています．広告や予防注射のお知らせ，「セサミ・ストリート」の成功などの事例から，アイディアの見方を変えさせる，アイディアへの渡りになる補足情報を加える，アイディアを繰り返し伝えるといった提示方法によって，

メッセージを記憶に粘らせ，行動を変えさせることができることを示しています．

原則 3：背景の力

3 つ目は，背景の力です．これは「情報を受け取る背景となる環境の要因」に関する原則です．これを象徴する犯罪学の理論に「割れた窓」と呼ばれる理論があります．これは，割れた窓を放置すれば，その地域には人の目がなく何をしても許されるという雰囲気を作り出し，さらに犯罪を呼び込むという環境による刺激の重要性を示したものです．幸い個人の性格の要因は変えられませんが，環境の要因は変えることができ，これをもって社会を望ましい方向に変えることができます．

本書を取り上げた動機

私が本書を取り上げようと思った動機は，私の現在の取り組みに関係しており，似たような理由で状況を改善したい方も多かろうと思ったからです．私は現在，香川県の小学校におけるプログラミング教育の活性化や，香川県高松市のスマートシティの推進に関与しています．私は，これらに共通する課題は，関与する人材（仲間）をいかに増やすかにあると思っており，ティッピング・ポイントはムーブメントを起こせる可能性を示唆している点で魅力的に映りました．とはいえ，結局のところ，何か具体的な施策の着想が得られたわけではありませんが……．いずれにしても情報の周辺部分（情報を伝える人，情報を引き立てる情報，情報を受け取るときの背景）を考えることは 1 つの手段として持っておくとよいと思います．興味がある方は本書をぜひ手にとってみてほしいと思います．

（2019 年 10 月 31 日受付）

米谷雄介（正会員） kometani@eng.kagawa-u.ac.jp

2010 年東京理科大学工学部第二部卒業．2014 年同大学院博士後期課程修了．博士（工学）．2017 年より，香川大学 助教．現在に至る．センサによるデータ収集，プラットフォームによるデータ蓄積，AI によるデータ解析，VR によるデータ可視化の一連のサイクル（IoT）に基づく知的支援・学習支援の研究開発に従事．教育システム情報学会，日本教育工学会，電子情報通信学会，各会員．

連載

5分で分かる!? 有名論文ナナメ読み

松尾真一郎（ジョージタウン大学）

Satoshi Nakamoto :
Bitcoin : A Peer-to-Peer Electronic Cash System

cryptography mailing list at metzdowd.com

ナナメ読み？　ご無体な

まずはじめに，いくら旧知の仲といえ，この論文を5分でナナメ読みできるような解説を依頼した会誌編集長は控えめに言って頭がおかしい．それは使っている技術が高度であるからではない．むしろ，Bitcoinを構成する要素技術は，提案から10年以上経過したものばかりで，枯れている技術である．しかし，それらが精巧なガラス細工のように組み合わさって生まれたエコシステムの価値を5分のナナメ読みで理解ができると考えているとすれば，本当に頭がおかしい．

Bitcoin以前の技術は，なぜソレを実現できなかったのか

この論文において，Bitcoinは以下のように記述されている（訳：崎村夏彦氏）[1]．

— 同意している二者が信頼できる第三者を必要とせず，直接取引が可能な，トラストの代わりに暗号的証明に依拠する電子支払いシステム
— 分散されたピア・ツー・ピアのタイムスタンプサーバを使って，トランザクションの時間的順序の計算機的証明を生成することによる，二重支払い問題を解決するシステム

この記述から分かるように，Bitcoinは二重支払いを防止する電子支払いシステムが目的である．その目的だけなら，昔から実現可能だった．それを信頼できる第三者を必要とせずに実現できそうな，初めての現実的な方式であるというのが，暗号研究者にとって「ヤラレタ」と思わされたところだ．しかし，この偉業を5分で分かった気になれと思うのは，やはり頭がおかしい．

元々，もしある人が信頼できる（秘密を守ってくれるし，嘘もつかない，言われたことをやってくれる）というのであれば，システムのセキュリティ確保は非常に簡単である．決められた処理を確実に，かつセキュアに実行してくれる第三者が存在して，その第三者と相互認証した上で暗号通信をすれば，システム全体のセキュリティは保たれる．しかし，皆さんも実体験しているように，世の中に「ここだけの話」は存在しないし，裏切る人は多いし，信頼できる第三者が機能しなくなることもある．暗号プロトコルの研究者は信頼できる第三者という仮定がなくても，数式だけで安全な世界を作ることを夢見て研究をしている．だからこそ，この論文はエポックメイキングなのだ．

二重支払いを防止するシステムなら，ATMを使った銀行送金は古くからすでに実現されている．通貨を発行する中央銀行が存在し，通貨は完全に信頼可能で，ATMが置かれている銀行と銀行間のネットワークが完全に信頼できれば，容易に目的を達成することができる．では，ATMや銀行間ネットワークをPCやインターネットに置き換えたらどうなるだろうか．この状況での支払いを実現する電子マネーの研究は1990年代から存在する．たとえば，日本銀行とNTTによる電子現金プロトコルは，現金を模擬して100円なら"100"というデータを中央銀行が発行し，そのデータそのものを現金同様として扱えるようにした．もち

ろん，単純に 100 というデータだけなら誰でも作ることができるので，二重支払いどころかお金は作りたい放題になるので，Bitcoin と同じく偽造や二重支払いを防止するために送金の意思表明を電子署名を用いて実現している．別の方法として，スマートカードの物理的セキュリティを完全に信頼した上で，支払いのときの残高管理をスマートカード，銀行口座，そして通貨を発行する中央銀行の間で齟齬なく行えばいいとする方式もあった．この際にも，電文に矛盾が起きないように，暗号技術が使われていた．これを 5 分で理解することを要求するのは控えめに言って頭がおかしいので，文献 2)，3）などの論文をじっくりあたってほしい．

ただ，1990 年代のこれらの試みでは，前述の暗号技術者の夢は実現されていない．中央銀行や銀行は信頼できる第三者のままだ．お金としての帳簿を管理する主体（中央銀行，銀行）が，系全体の信頼点になっているからである．暗号プロトコルの研究において，信頼できる第三者を減らす伝統的な手法として，暗号処理に必要な秘密情報を複数の主体に分割し，その複数の主体の一部が不正したとしても処理が行える手法がある．分散復号，分散署名，マルチパーティー計算などがその例である．しかし，これらの権限分割はあらかじめ決められた人の間でなされるだけで，悪い人を排除して，新しい良い人を加えるなどの自由度はなかった．これを 5 分で理解することを要求するのは控えめに言って頭がおかしいので，文献 4)，5）などの論文をじっくりあたってほしい．

Bitcoin が出した答えの妙はどこにあるのか

信頼できる第三者が不要で，二重支払いを解決するシステムを作る別の発想をしたのが Bitcoin である．それは，支払いのデータをローカルでやりとりしつつあとで誰かが集計して帳簿を更新するのではなく，共通帳簿全体を系に参加する全員が共有し一定時間ごとに多数のプレーヤで力を合わせて帳簿データを更新していくという発想の転換だ．

取引の前後関係は，10 分単位で支払い要求を束にして，ハッシュ値を連鎖させて証明している．これは，1990 年に提案されたリンクトークン式タイムスタンプ☆1 と同じ技術で目新しくない．むしろ，問題は，それを分散環境でどう実現するかだ．当然，多数のプレーヤの中には悪い人がいるので，悪い人がいたとしても正しく帳簿が更新されないといけない．ここで Bitcoin が出した答えは，過半数のハッシュ関数の計算能力を持つプレーヤが正直な参加者であれば正常に動作するプロトコルを用いて，正直なプレーヤを増やすことで悪いプレーヤを少数派にするという発想だ．そのために，Bitcoin のプロトコルは，いつでも誰でも参加していいし，ネットワークから抜けてもいい，という許可不要な構造になっている．Bitcoin に，マイニングと呼ばれる処理があり，Proof-of-work のゲームを正しく解いた人に 10 分に 1 回，一定額の報酬としての Bitcoin が与えられるのは，ネットワークの参加者を増やしてセキュリティを向上させるためだ．そして，複数の人で共通の帳簿を更新するためには，「分散合意」と呼ばれるプロトコルを実行する必要がある．これは分散コンピューティングの根幹をなす研究テーマであり非常に数多くなされている．しかし，実用的な時間で解決しようとすると，ネットワークに参加するノード数や，ネットワークの同期に関する前提条件が厳しいことも分かっている．そこで，不特定多数のプレーヤが自由に出入りできる Bitcoin においては，新たな合意プロトコルが作られた．これは潔い割り切りをしていて，あとで合意が覆る可能性があってもいいので，確率的に合意をとる仕組みになっている．さらに，暗号処理に対する攻撃をすれば，Bitcoin でも二重支払いは可能となるが，プレーヤに悪い気を起こさせないためにも，自分が持って

☆1 タイムスタンプサービスの方式の 1 つ．利用者が作成する原データのハッシュ値を時系列にそって関連付けるリンク情報を生成する．各タイムスタンプトークンは 1 つ前に発行されたタイムスタンプトークンに必ず依存するように生成される．

いる計算機リソースを暗号の攻撃に費やすのではなく，Proof-of-work のゲームに勝って報酬を得たほうが合理的になることを目指して設計されている．

上記を 5 分で分かった気にさせることを要求するのは控えめに言って頭がおかしい．さらに，Bitcoin がビザンチン将軍問題☆2 を解いたという触れ込みで記事を書く人がたくさんいるが，提案された合意アルゴリズムはビザンチン将軍問題を解いていない．これを理解するのに 5 分で足りないことは明らかだろう．この辺については，文献 1) を熟読いただきたい．

上記で分かるように，解きたい問題や達成したい性質と，使われているテクニックの関係が必ずしも一対一対応していなくて，複雑に絡み合っている．この関係は，正確には現時点でも未解明であって，Bitcoin の登場から 10 年経った今でも，後追いで研究が続けられている．さらに言えば，解きたい課題を完全に解いているわけでもない．このことは，5 分どころか 5 年でも分かるわけがない．

でも本当は，やりたいことを 100% は実現できていない!

信頼できる第三者を不要にするという理想は，実は達成していない．暗黙のうちではあるが，ソフトウェアを実装するエンジニアを信頼している．また電子署名を使っている以上，秘密にすべき署名鍵を厳重に各々が管理することが前提になっているが，それを一般のユーザに求めるのは酷であり，耐タンパ性を持ったハードウェアウォレットの安全性を仮定しても，その設計者や製造者に信頼点を移しただけである．つまり，エンジニアにかかる責任が大きくなっただけとも言える．鍵管理は無理だからこそ，暗号資産の交換所に鍵を預けているケースもあるが，そうすると交換所が信頼できる第三者になってしまう．この辺の裏事情も含めて 5 分で分かるように説明せよというのは，控えめに言って頭がおかしい．

本稿を最後まで見て興味が湧いた読者の皆様は，この論文をむしろ温故知新のきっかけとして，過去の関連論文を時間をかけて読み直して，そしてこの論文を噛むほどに何度も味が出るスルメのように味わってほしい．

☆2 いくつかのコンポーネントが故障している，あるいは，コンポーネントが故障したかどうかの情報が不完全である，という状態で，全体で正しい合意形成ができるかどうか，という分散コンピューティングの問題の 1 つ．

参考文献

1) 松尾真一郎，楠　正憲，崎村夏彦，佐古和恵，佐藤雅史，林　達也，古川　諒，宮澤慎一：ブロックチェーン技術の未解決問題，日経 BP 社．
2) 中山靖司，森畠秀実，阿部正幸，藤崎英一郎：電子マネーの一実現方式について―安全性，利便性に配慮した新しい電子マネー実現方式の提案―，金融研究，第 16 巻第 2 号，日本銀行，金融研究所，1997 年 6 月号．
3) 藤崎英一郎，岡本龍明：エスクロー電子現金，電子情報通信学会論文誌 IT95-51, ISEC95-46, SST95-112, pp.7-12 (1996).
4) Shoup, V. : Practical Threshold Signature, EUROCRYPT 2000, LNCS 1807, pp.207-220 (2000).
5) Ben-Or, M., Goldwasser, S. and Wigderson, A. : *Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation*, STOC '88 Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing, pp.1-10.

(2019 年 9 月 3 日受付)

松尾真一郎　Shinichiro.Matsuo@georgetown.edu

ジョージタウン大学・研究教授，CyberSMART 研究センター・ディレクター，NTT Research Inc. Head of Blockchain Research. BSafe.network 共同設立者．

書評（ビブリオ・トーク）・会議レポート募集のお知らせ

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

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

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

a-2）ビブリオ・トーク―私のオススメ―：お気に入りの本の紹介．

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

2. 応募資格

原則として本会会員に限ります．

3. 応募の手続き

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

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

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

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

4. 原稿の取扱い

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

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

IPSJ メールニュースへ広告を出しませんか？

広告を IPSJ メールニュースで配信しています．本会会員が主な読者なので，ターゲットを絞った広告に最適です．

●配　信　数：約 29,000 通（原則毎週月曜日配信）
●読　者　層：本会会員および非会員
●形　　式：テキストのみ．等幅半角 70 字× 5 行．URL を入れてください．
●掲載位置：ヘッダ（目次の上）
　　フッタ（本文の最下行）
●掲　載　料：ヘッダ：1 回 50,000 円（税抜）※ 3 社限定
　　フッタ：1 回 20,000 円（税抜）
　　※それぞれ行数超過については別途相談
●申　込　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
　　または，情報処理学会 会誌編集部門　E-mail: editj@ipsj.or.jp　Tel(03)3518-8371
●申込締切：毎週水曜日締切，翌週月曜日配信となります．
●見　　本：

―［広告］―――――――――――――――――――――――――――――――

■■■　　○○セミナー　　■■■

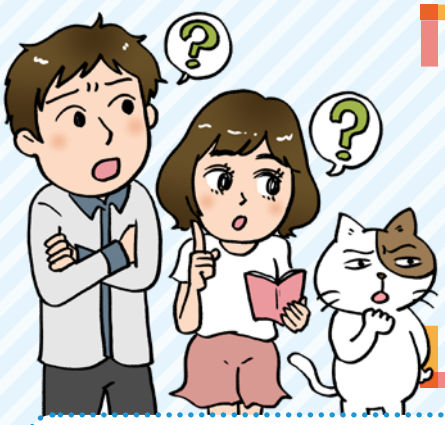
開催日時：1 月 10 日（火）・11 日（水）・12 日（木）13：00 ～ 17：00

会場：○○コンベンションセンター

会費：情報処理学会会員の方には割引があります．

詳細はこちらをご覧ください：http://www.....com/

―――――――――――――――――――――――――――――――［広告］―



連載

先生，質問です！

久しぶりの本コーナー．今回は中学生からの質問に 3 名の方が答えてくださいました．

人の脳をロボットにうつすことができるのか？
また，もし人間の行動をロボットでおきかえられるなら，人間の意識や魂があれば永遠に生きることは可能ですか？

Q

匿名希望
［ジュニア会員］
中学生

原理的には可能です．ただ，まだ実現するための技術がないので，実現には時間がかかると思います．人の脳をロボットにうつすことが可能だという理由は，脳も結局は物質でできていて，その本質は情報だからです．脳の中の情報をコンピュータに転送するためには，脳の情報を読み取る技術と，それをコンピュータ上で再現する技術が必要です．現在はまだ脳の情報がそこまで詳細に読み取れないので，その技術を開発しなければなりません．これはけっこう難しいことなので，時間がかかりそうです．でも，その技術さえできてしまえば，それを再現することはそこまで難しくはなさそうです．そして，コンピュータ上に再現してしまえば，情報を保存しておくことさえできれば，人間の意識が特定の身体やハードウェアから自由になるので，永遠に生きることも可能です．現在，人間を含めた生物が死んでしまうのは，ハードウェアを入れ替えることができないからなので，脳をディジタル化すれば，自分のバックアップをとっておくこともできるし，自分を 100 万人同時に世に出すことも可能になります．たぶん，人類はこういうディジタルな存在にいずれは置き換わっていくでしょう．でも，あくまでも今は原理的に可能と言えるだけで，実現するためにはたくさんの研究が必要です．

A

金井良太
(株) アラヤ

本企画の問合せ先

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

石黒　浩
〔正会員〕
大阪大学

A

人間の脳も複雑なコンピュータだと捉えれば，いつかは人間の脳をロボットにうつすことは可能になるように思います．しかし，人間の脳や体をロボットに置き換えたとしても，機械も壊れる可能性はありますから，永遠に生きることは不可能です．また意識や魂があればいいかというと，特に魂についてはそれが何であるかは現時点ではまったく不明で，永遠に生きるための条件になるかどうかは分かりません．

A

質問を次のように読み替えさせてください．「意識を電子頭脳にうつすことはできるか？　その中で永遠に生き続けることは？」私は 20 年程度で，両者とも実現可能であると考えています．意識を宿す脳も所詮は電気回路であり，巷を賑わせる AI 技術と，そのしくみにおいて決定的な差がないからです．

ただし，その方法は，脳から意識を吸い出して電子頭脳に流し込むといったものにはなりません．意識を含む脳の情報処理は無数のニューロン間の結合強度に埋め込まれており，コンピュータと違って，ソフトとハードが不可分なためです．以下，私の意識の移植を例に，現在考えている手順を示します．

まずは，ヒト一般の脳のゼロイチの配線構造を電子顕微鏡で読み取って人工神経回路網（電子頭脳）の初期結合強度とします．それに，感覚運動入出力を与え，学習則を適用することでニュートラルな意識を宿します．次に，私の脳をその電子頭脳に接続して両者の意識を一体化します．最後に，記憶や感情，さらには意思決定の癖などを共有することで，電子頭脳の意識を「わたし色」に染めていきます．それらが完遂した暁には，ナマモノの脳が滅びた後にも，私の意識は電子頭脳の中で永遠に生き続けることになるでしょう．

撮影：新井卓

渡辺正峰
東京大学

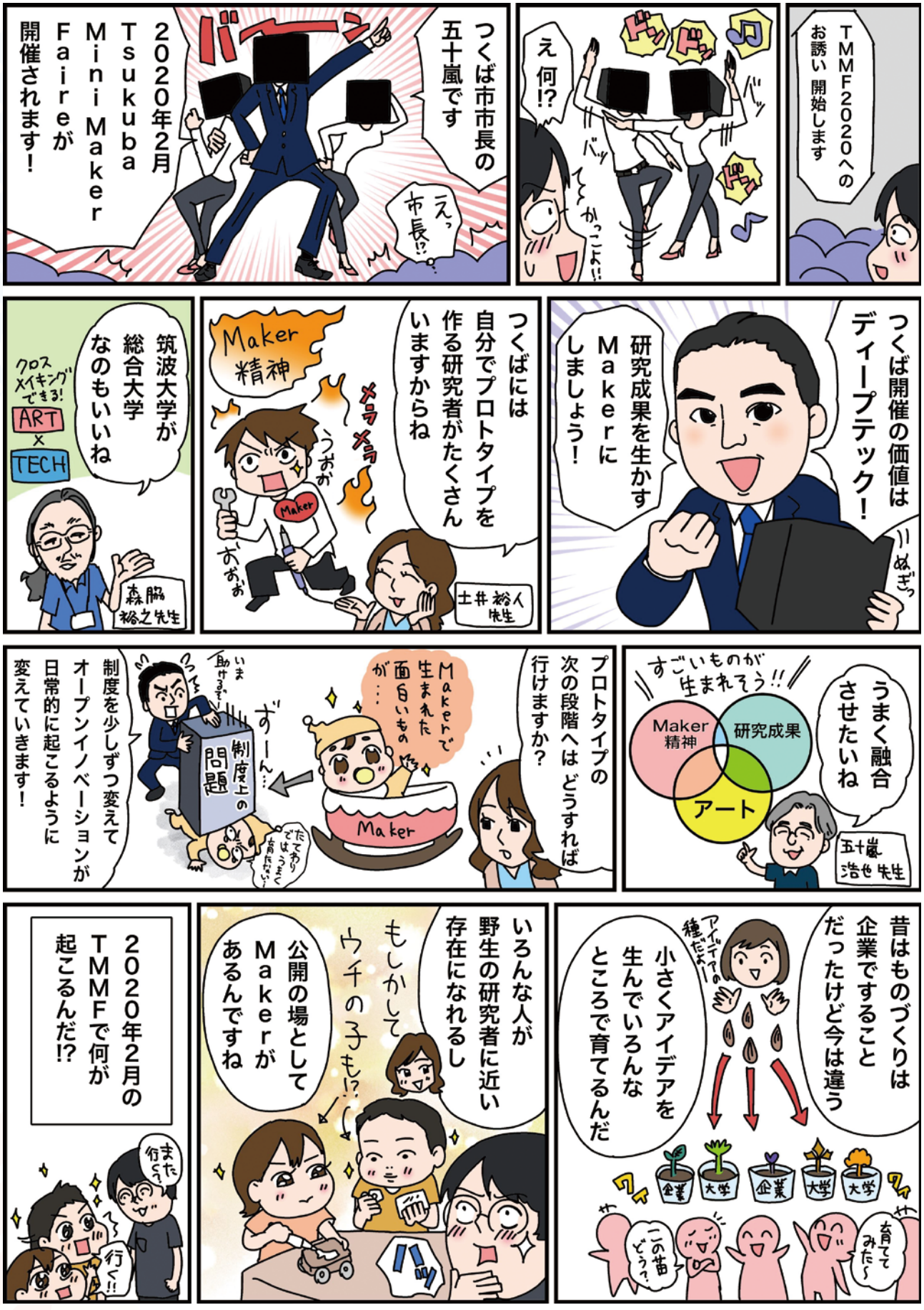
「先生，質問です！」への質問方法

▸ **メールで質問：** 下記を記載し，E-mail: sensei-q@ipsj.or.jp にメールを送信ください．
（1）質問（必須）（2）名前（任意）（3）区分（必須）：小学生／中学生／高校生／高専生／大学生／大学院生／社会人／その他・無回答（4）会員種別（必須）：ジュニア会員／学生会員／正会員／非会員（5）連絡用メールアドレス（任意）

▸ **Web から質問：** 下記の Web ページ内の投稿フォームから質問をご記入ください．
「先生，質問です！」質問募集のお知らせ　https://www.ipsj.or.jp/magazine/sensei-q.html

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

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


TMMF2020へのお誘い 開始します
ドンドン
え 何!?
かっこよ!!
バーン
つくば市市長の五十嵐です
えっ 市長!?
2020年2月 Tsukuba Mini Maker Faireが開催されます!
つくば開催の価値はディープテック!
研究成果を生かすMakerにしましょう!
ぬぎっ
つくばには自分でプロトタイプを作る研究者がたくさんいますからね
Maker精神
メラメラ
うおが
おおお
土井裕人先生
筑波大学が総合大学なのもいいね
クロスメイキングできる!
ART × TECH
森脇裕之先生
うまく融合させたいね
すごいものが生まれそう!!
Maker精神
研究成果
アート
五十嵐浩也先生
プロトタイプの次の段階へはどうすれば行けますか?
Makerで生まれた面白いものが…
Maker
ずーん…
制度上の問題
いま助けるぞ!
たてわりではうまく行かない!
制度を少しずつ変えてオープンイノベーションが日常的に起こるように変えていきます!
昔はものづくりは企業ですることだったけど今は違う
アイデアの種だよ!
小さくアイデアを生んでいろんなところで育てるんだ
企業
大学
企業
大学
大学
育ててみた〜
この苗どう?
いろんな人が野生の研究者に近い存在になれるし
もしかしてウチの子も!?
公開の場としてMakerがあるんですね
2020年2月のTMMFで何が起こるんだ!?
また行く?
行く!!

このページから読んでね！

その5 Maker Faire Tokyo 2019 に行って来た！ ～来月の Tsukuba Mini Maker Faire に向けて～

漫画：山本ゆうか（Twitter @ymmox）

ICCV 2019 参加報告

ICCV について

International Conference on Computer Vision (ICCV) 2019 は，2019 年 10 月 27 日から 11 月 2 日にかけて，韓国ソウル市内に位置する COEX Convention Center にて開催された．ICCV は IEEE Computer Society と Computer Vision Foundation が主催するコンピュータビジョンに関する主要な国際会議の 1 つであり隔年開催されている．ICCV の h5-index[☆1] は 2019 年 11 月現在で 129，CORE[☆2] のカンファレンスランキングによると A* となっており，コンピュータビジョンに関する国際会議では Computer Vision and Pattern Recognition (CVPR)，European Conference on Computer Vision (ECCV) に並びトップカンファレンスの 1 つである．

オープニングセッションで今回の ICCV についてさまざまな数値データが公開されたのでいくつか紹介する．まず発表数について，論文投稿数 4,303 本のうち採択数は 1,075 本であり，そのうち口頭発表数は 200 本であった．選定にあたり，2,500 名以上の査読者が携わっていることが明らかにされた．今年は 17 回目の開催となるが，参加者は 7,500 人を超え，前回の ICCV 2017 と比較しても 2.4 倍以上となり（**図 -1**），世界的にもコンピュータビジョンへの注目度が急速に上昇していることがうかがえる．開催地韓国からの参加者が最も多く，次いで中国やアメリカからの参加が多かった．日本は 4 番目に多かったが中国からの参加者の半数程度と割合としてはやや少なく感じた．また，企業等 56 団体がスポンサーとなっており，ポスター会場に併設の EXPO では NAVER 社など韓国企業を中心に，さまざまな企業等から 72 件の展示が行われた．

ICCV 2019 のプログラムを簡単に紹介する．開催期間のうち 3 日間は Tutorial や Workshop に割り当てられており，基調講演や招待講演もこの期間に行われた．また，本会議は開催期間のうち 4 日間を占めており，口頭発表は 2 会場のパラレル形式の全 13 セッションで構成された．発表の様子は，2 会場それぞれの入り口の大きなモニタと，別の部屋のスクリーンに同時中継され，各自が好きなように聴講することができた（**図 -2**）．ポスターセッションは期間中 7 回開催されたが 1 回あたり約 130 件もの発表が行われ，どのポスターにも多くの参加者が集まり活発な議論が行われていた．ポスターセッションと同時にデモセッションも設けられており，インタラクティブに動作する技術展示が行われた．また，ポスター会場に併設された企業ブースでは採用のためのスタッフやテーブルも用意されていることが多く，デモや展示の説明の傍ら，学生と企業従業員が対話している様子もよく見られた．

トピック紹介

図 -3 は，論文タイトルに使用されたキーワードから得たワードクラウドである．近年の傾向として，少ない教師データ，あるいは教師データなしで問題を解く Weakly supervised や Unsupervised Learning などのキーワードが比較的多くなったように見受けられる．3 次元データを扱うものも多く，さらに視野を共有しないカメラ間での人物や物体の照合問題に関する

☆1 過去 5 年でその会議や雑誌で出版された論文の h-index（被引用数が h 回以上であるものが h 本以上ある）．

☆2 The Computing Research and Education Association of Australasia．カンファレンスランキングは，被引用率や採択率，主催者や会議にかかわる主要な人物の研究実績等の組合せによって評価される．

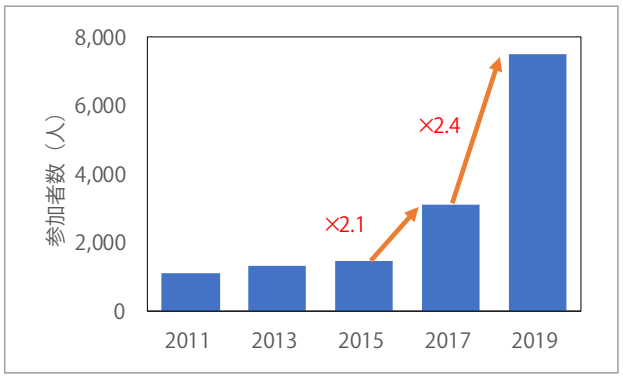


図 -1　近年開催分の参加者数の推移
（ICCV 2019 正式公開データから筆者が作成）

図 -2　会場の様子
上図：口頭発表会場内，下図：口頭発表会場入り口付近，
右図：ポスターセッション会場の様子

Re-Identification といったキーワードなども見られた．GAN（Generative Adversarial Network）に関してもいまだ熱が冷めておらず，ポスターセッションで特に活発な議論が行われていた．そのほか，画像や映像に加え，音声やテキスト，センサデータなどの別のチャネルを用いたものもいくつか見られた．デモセッションでは，CVPR や ECCV など他会議で発表された論文を発展させたデモ等も行われた．たとえば，Re-Identification と表情認識技術を活用し，空港を訪れる人々のジャーニー（動きやその時々の感情など）を分析可能にすることで顧客満足度を高める取り組み [1] 等も紹介された．

ICCV 2019 では，Best Paper Award が 1 本 [2]，Best Student Paper Award が 1 本 [3] 選定された．Best Paper を受賞した論文について簡単に紹介する．

“SinGAN: Learning a Generative Model from a Single Natural Image” [2] が Best Paper Award として選定された．近年のディープラーニングを用いたコンピュータビジョン分野における研究の中で，GAN は非常に注目度が高く，これまでもさまざまな論文が発表されてきた．従来の GAN は，高品質な画像生成を行うためにはモデルの学習に多量の画像を用いる必要があったが，SinGAN は学習用画像を 1 枚のみ用いることを実現している．SinGAN のポイントは階層ピラミッド構造を持つネットワークと，さまざまな解像度に対応し得る生成器ネットワークであり，学習画像からさまざまな情報を引き出すことができるため，わずか 1 枚の学習画像で画像から画像への多様な変換を可能にした．GAN を用いたさまざまなタスクに応用可能とし，発表では低解像度画像から高解像度画像への変換や，画像調和（**図 -4**），画像の修正，入力画像に類似の画像が生成できることを活かしたアニメーションなどが紹介された．選定された論文は口頭発表に加えオープニングセッションの後にも内容を説明する機会が与えられており，SinGAN の応用例紹介のシーンでは，会場から驚きの声がもれるなど現地でのインパクトも大きかった．この論文だけでなく，画像 1 枚のみを用いて学習する GAN の発表がいくつかあり（InGAN [4] など），GAN 研究の流れの変化を感じた．

先述の通り，ほかにも幅広い観点で数多くの発表があったため，それぞれの論文を参照されたい．

ICCV 2021

次回の ICCV は，2 年後にカナダのモントリオールで開催されることが決定している（開催日程は本報告執筆時点で未定）．コンピュータビジョン研究のトレンドや世界の研究者の熱を直接感じることができるため，コンピュータビジョンに興味を持たれている方や研究を始めたばかりの皆様にもぜひ参加してみていただきたい．

参考文献

1）Sugianto, N. and Tjondronegoro, D. : Deep Residual Learning for Analyzing Customer Satisfaction using Video Surveillance, 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS) (2018).
2）Shaham, T. R. et al. : SinGAN : Learning a Generative Model from a Single Natural Image, The IEEE International Conference on Computer Vision (ICCV), pp.4570-4580 (2019).
3）Duff, T. et al. : PLMP - Point-Line Minimal Problems in Complete Multi-View Visibility, The IEEE International Conference on Computer Vision (ICCV), pp.1675-1684 (2019).
4）Shocher, A. et al. : InGAN : Capturing and Retargeting the “DNA” of a Natural Image, The IEEE International Conference on Computer Vision (ICCV), pp.4492-4501 (2019).

（吉岡隆宏／富士通研究所）

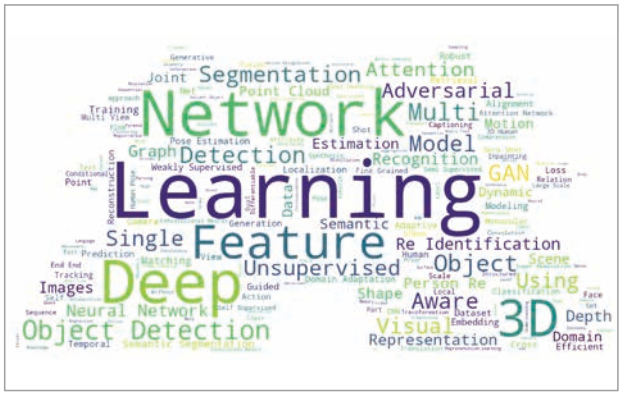


図 -3　ICCV 2019 ワードクラウド
（発表論文タイトル一覧から筆者が作成）

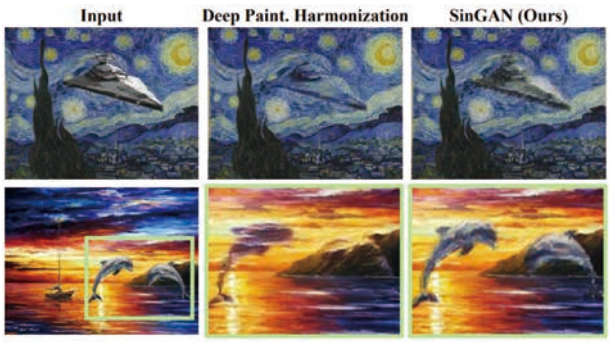


図 -4　SinGAN による画像調和の結果例
文献 2）中から引用（図 -13）．図右が SinGAN の出力．絵画中の詳細な描写を残しつつ，追加した部分にテクスチャの特徴などの大域的な情報を反映して調和しているのが分かる

今月の会員の広場では，11 月号へのご意見・ご感想を紹介いたします．まず，巻頭コラム「E-mail との長い長い戦い」については，以下のようなご意見・ご感想をいただきました．

■電子メールの功罪を考えさせられた．グループウェアはツールではなくプロセスから考えるべきだと思った．（高島洋典）

特集「ディジタルタイプ」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．

■フォントに関して非常に勉強になったが，LaTeX に関連づけた記事が 1 本あるとよかった．（島野顕継）

■タイプやフォントの歴史的成り立ちから IT への関連という掘り下げは非常に興味があり，読んでいて面白かったです．（竹原豊和）

■昔，文書処理システムの開発に携わっていた時期があるので，大変興味深く読ませていただきました．UD フォントに関する記事がありましたが，前に当事者研究の特集で，視認性とは別に理解しやすいという意味での読みやすいフォントの話題が出ていたので，それに関する記事もあるとよかったと思います．（匿名希望）

■進化するフォント技術を改めて知る良い機会になりました．デザイナの苦労が分かる良い内容でした．（匿名希望）

■フォントはプレゼンテーションを作成するときにも非常に重視するものであり，フォントに関する専門的な観点からの解説が非常に分かりやすくまとめられており役に立ちました．（浜辺裕多／ジュニア会員）

「1．UD フォント」
■ UD フォントについては，今回改めてイワタとパナソニックの開発・命名によるものと知った．Web フォントについても初めて知り，特集全体を興味深く読んだ．（柏野和佳子）

■親しみやすい内容であり，かつ資料なども読み取りやすかった．（永江毘加里／ジュニア会員）

連載「論文必勝法：採否判定結果が届いたら」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．

■「論文必勝法」は背中を押していただけたようなあたたかな視点からまとめられていて，挑戦してみたくなりました．（匿名希望）

■博士号取得を目指しているため，論文必勝法の連載は大変参考になります．（匿名希望）

連載「情報の授業をしよう！：中学におけるタブレット端末を活用した，学習における思考プロセスの可視化」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．

■思考プロセスの可視化と記録は今後とても重要になってくると思います．課題の指摘もありましたが継続して克服し，授業や教育に活かすところまで進めていただきたいと思いました．（滝内邦弘）

連載「5 分で分かる !? 有名論文ナナメ読み：King, G., Pan, J. and Roberts, M. E. : Reverse-engineering Censorship in China : Randomized Experimentation and Participant Observation」については，以下のようなご意見・ご感想をいただきました．

■今回は社会問題の調査研究であり，いつもと毛色が異なるもので新鮮でした．調査対象が政府／国家という扱いの難しいものでしたが，そのような対象にチャレンジする研究があるということに驚きました．（匿名希望）

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

■分野外の技術の最新動向が効率的に収集できるので大変助かります．（匿名希望）

連載「古機巡礼 / 二進伝心：オーラルヒストリー：戸田　巌氏インタビュー」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．

■「技術者が一番上位のアーキテクチャを自分の頭で考えなくなった」との指摘は，強く胸に刺さりました．（匿名希望）

■非常に興味深く拝読しました．記事最後尾の「編集部注」を最初に記述していただければ，記事の背景を理解した上で読むことができ，より読みやすくなると思いました．（匿名希望）

オンライン版で読みたい記事，期待するコンテンツについて以下のようなご意見やご要望をお寄せいただきました．

■今号ならば，ディジタルタイプのフォントの違いをWebでボタンをクリックする等して変形操作などができるとよい．（島野顕継）

■図に動きをつける，ブラウザで読みやすい形式にするなど，記事がより分かりやすくなると，電子化の意義があるのではないでしょうか．（角田洋太郎／ジュニア会員）

■関連情報へのリンク，動画を使って視覚的に分かりやすいコンテンツ．（匿名希望，滝内邦弘，永江毘加里／ジュニア会員，伊藤雅樹）

■紙媒体に書き込み，付箋などをよく用いますので，オンライン版でもそれらの機能があると助かります．またバックナンバーの記事検索機能はぜひ実現してほしいところです．（匿名希望）

■仮想通貨，ブロックチェーンに関する特集，初心者向けの論文募集等．（浜辺裕多／ジュニア会員）

■会員の疑問や興味に，別の会員が答えるような記事．専門の少し違うもの同士の質問と応答などの記事は興味が広がりそうに思う．（柏野和佳子）

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

■ディジタルフォレンジックに関する最新の研究についての特集を希望します．（匿名希望）

■NGNやインターネットバックボーンなど基盤ネットワークを取り巻く現状について解説してほしい．（角田洋太郎／ジュニア会員）

■量子コンピュータについて解説してほしいです．（匿名希望／ジュニア会員）

■情報処理は対象が広く，特定分野に偏った記事は掲載しにくいかもしれないが，各研究会でのホットトピックについて知る機会があるとよい．（匿名希望）

■初等中等教育におけるキーボードリテラシーに興味を持っています．（匿名希望）

■学会での発表資料のつくりかたや作法の紹介があるとよいと思いました．ジュニア会員は知る機会がないのではないでしょうか．（匿名希望）

【本欄担当　荒　宏視，山本岳洋／会員サービス分野】

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

皆様にとって会誌をより役立つものとするため，
・記事に対する感想，意見　・記事テーマの提案　・会誌または学会に対する全般的な意見，提言
・その他，情報処理技術についての全般的な意見，提言
など自由なご意見，ご感想をお待ちしております．
なお，「道しるべ」については
<URL：https://www.ipsj.or.jp/magazine/sippitsu/michishirube.html> で
これからのテーマ案を募集しており，いただいたご意見をまとめております．
※ご意見，ご感想を会誌に掲載させていただいた方には薄謝または記念品を進呈いたします．

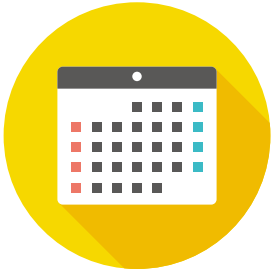
掲載に際しては，編集の都合上，ご意見に手を加えさせていただくことがありますので，あらかじめご了承ください．
なお，意見の投稿に伴う，住所，氏名，所属などの個人情報については，学会のプライバシーポリシーに準じて取り扱いいたします．　<URL：https://www.ipsj.or.jp/privacypolicy.html>

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

IPSJ カレンダー

開催日	名　称	論文等応募締切日	参加締切日	開催地
	論文誌「ユーザブルセキュリティ」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/20-Z.html	2月24日（月）		
	2020年度 会誌「情報処理」および「デジタルプラクティス」モニタ募集 https://www.ipsj.or.jp/magazine/topics/2020monitor.html	2月27日（木）		
	論文誌「持続可能な社会を実現するコラボレーション技術とネットワークサービス」特集への論文募集 https://www.ipsj.or.jp/journal/cfp/21-C.html	3月23日（月）		
1月15日（水）～ 1月16日（木）	第186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 https://www.ipsj.or.jp/kenkyukai/event/hci186.html	11月15日（金）	当日のみ	大濱信泉記念館 （沖縄県石垣市）
1月15日（水）～ 1月16日（木）	第127回プログラミング研究発表会 https://sigpro.ipsj.or.jp/pro2019-4/	11月15日（金）	当日のみ	医療イノベーション推進センター
1月15日（水）～ 1月17日（金）	International Conference on High Performance Computing in Asia Pacific Region（HPCAsia2020） http://sighpc.ipsj.or.jp/HPCAsia2020/			アクロス福岡
1月23日（木）～ 1月24日（金）	第231回システム・アーキテクチャ・ 第190回システムとLSIの設計技術合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/arc231sldm190.html	11月12日（火）	当日のみ	慶應義塾大学 日吉キャンパス
1月23日（木）～ 1月24日（金）	第109回グループウェアとネットワークサービス・ 第27回コンシューマ・デバイス＆システム・ 第24回デジタルコンテンツクリエーション合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/gn109cds27dcc24.html	11月13日（水）	当日のみ	隠岐島文化会館 （島根県隠岐郡）
1月23日（木）～ 1月24日（金）	第220回コンピュータビジョンとイメージメディア研究発表会 https://www.ipsj.or.jp/kenkyukai/event/cvim220.html	11月8日（日）	当日のみ	奈良先端科学技術大学院大学
1月24日（金）	高度交通システム（ITS）研究フォーラム2020 https://www.ipsj.or.jp/kenkyukai/event/itsf2020.html		1月15日（水） 当日可 *論文集が不足した場合は事前申し込み優先	慶應義塾大学 日吉キャンパス
1月24日（金）～ 1月25日（土）	ウィンターワークショップ2020・イン・京都 http://wws.sigse.jp/2020/	12月9日（月）	当日可 事前申込割引： 1月10日（金）まで	YIC京都工科自動車大学校
1月29日（水）～ 1月30日（木）	第176回アルゴリズム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/al176.html	12月2日（月）	当日のみ	下呂市民会館 大会議室
2月1日（土）	第122回人文科学とコンピュータ研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ch122.html	12月18日（水）	当日のみ	佐賀大学理工学部
2月4日（火）	情報処理学会×最先端表現技術利用推進協会主催 短期集中セミナー2019「ここまで来た！空間表現の先端事例と技術動向～ CG/CV/VR/HCIの最先端～」 https://www.ipsj.or.jp/event/s-seminar/2019/IPSJxsoatassoc/index.html	1月28日（火） 定員になり次第		株式会社フォーラムエイト セミナールーム
2月7日（金）	ITフォーラム2020 https://www.ipsj.or.jp/event/itf/itf2020/index.html		1月31日（金） 定員になり次第	学術総合センター・ 一橋記念講堂会議室
2月13日（木）～ 2月14日（金）	第131回音声言語情報処理研究発表会 https://www.ipsj.or.jp/kenkyukai/event/slp131.html	12月25日（水）	当日可	加賀・片山津温泉 佳水郷
2月14日（金）	第87回電子化知的財産・社会基盤研究発表会 https://www.ipsj.or.jp/kenkyukai/event/eip87.html	12月22日（火）	当日のみ	佛教大学 二条キャンパス
2月15日（土）～ 2月16日（日）	第153回コンピュータと教育研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ce153.html	12月24日（火）	当日のみ	大阪教育大学 天王寺キャンパス
2月17日（月）	第197回知能システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ics197.html	12月27日（金）	当日のみ	沖縄県青年会館
2月17日（月）～ 2月18日（火）	第126回音楽情報科学研究発表会 https://www.ipsj.or.jp/kenkyukai/event/mus126.html	1月9日（木）	当日のみ	東京工業大学 大岡山キャンパス
2月27日（木）～ 2月28日（金）	第108回オーディオビジュアル複合情報処理研究発表会 https://www.ipsj.or.jp/kenkyukai/event/avm108.html	1月10日（金）	当日のみ	沖縄セルラー電話 株式会社（予定）
2月27日（木）～ 2月28日（金）	第232回システム・アーキテクチャ・第191回システムとLSIの設計技術・第53回組込みシステム合同研究発表会（ETNET2020） https://www.ipsj.or.jp/kenkyukai/event/arc232sldm191emb53.html	1月6日（月）	当日のみ	与論町中央公民館
2月27日（木）～ 2月28日（金）	第148回システムソフトウェアとオペレーティング・システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/os148.html	1月14日（火）	当日のみ	高知工科大学 永国寺キャンパス

3月2日（月）～ 3月3日（火）	第48回インターネットと運用技術研究発表会 https://www.ipsj.or.jp/kenkyukai/event/iot48.html	1月7日（火）	当日のみ	名古屋大学 東山キャンパス
3月2日（月）～ 3月3日（火）	第94回モバイルコンピューティングとパーベイシブ・ 第65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 https://www.ipsj.or.jp/kenkyukai/event/mbl94ubi65.html	1月10日（金）	当日のみ	名古屋大学 IB電子情報館
3月2日（月）～ 3月3日（火）	第36回セキュリティ心理学とトラスト研究発表会 https://www.ipsj.or.jp/kenkyukai/event/spt36.html	1月16日（木）	当日のみ	沖縄県青年会館
3月5日（木）～ 3月7日（土）	情報処理学会　第82回全国大会 https://www.ipsj.or.jp/event/taikai/82/			金沢工業大学 扇が丘キャンパス
3月7日（土）～ 3月10日（火）	第198回知能システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/ics198.html	1月17日（金）		ルスツリゾートホテル
3月8日（日）～ 3月10日（火）	第30回教育学習支援情報システム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/cle30.html	1月16日（木）	当日のみ	神戸大学 瀧川記念学術交流会館
3月9日（月）～ 3月11日（水）	インタラクション2020 https://www.interaction-ipsj.org/2020/	12月23日（月）	当日可	学術総合センター内 一橋講堂
3月12日（木）～ 3月13日（金）	第128回プログラミング研究発表会 https://sigpro.ipsj.or.jp/pro2019-5/	1月10日（金）	当日のみ	早稲田大学 西早稲田キャンパス
3月12日（木）～ 3月13日（金）	第182回マルチメディア通信と分散処理・ 第88回コンピュータセキュリティ合同研究発表会 https://www.ipsj.or.jp/kenkyukai/event/DPS182CSEC88.html	1月29日（水）	当日のみ	情報セキュリティ大学院大学
3月12日（木）～ 3月13日（金）	第61回バイオ情報学研究発表会 https://www.ipsj.or.jp/kenkyukai/event/bio61.html	2月6日（木）	当日のみ	北陸先端科学技術大学院大学知識科学研究科
3月16日（月）	第177回アルゴリズム研究発表会 https://www.ipsj.or.jp/kenkyukai/event/al177.html	1月21日（火）	当日のみ	東北大学 青葉山東キャンパス
3月16日（月）～ 3月17日（火）	第221回コンピュータビジョンとイメージメディア研究発表会 https://www.ipsj.or.jp/kenkyukai/event/cvim221.html	1月8日（水）	当日のみ	京都大学
3月16日（月）～ 3月17日（火）	第187回ヒューマンコンピュータインタラクション研究発表会 https://www.ipsj.or.jp/kenkyukai/event/HCI187.html	1月20日（月）	当日のみ	国士舘大学 世田谷キャンパス（梅ヶ丘校舎）
3月16日（月）～ 3月18日（水）	第173回ハイパフォーマンスコンピューティング研究発表会 https://www.ipsj.or.jp/kenkyukai/event/hpc173.html	1月21日（火）	当日のみ	北海道立道民活動センター（かでる2・7）



Webページ（https://www.ipsj.or.jp/）更新情報

［トピックス］

12月2日	第82回全国大会講演申込受付を12月6日まで延長しました
12月1日	IS ディジタル辞典～重要用語の基礎知識～（第2版）公開！！
11月28日	2020年度 会誌「情報処理」および「デジタルプラクティス」モニタ募集
11月27日	論文誌「実社会を支える暗号・セキュリティ・プライバシ技術」特集 論文募集
11月26日	IT フォーラム2020 参加申込受付を開始しました
11月26日	2019年度「優秀教育賞」および「優秀教材賞」推薦のお願い
11月22日	短期集中セミナー2019 参加申込受付中です
11月22日	論文誌「エンタテインメントコンピューティング」特集 論文募集
11月20日	認定情報技術者（個人認証）2019年度更新申請案内

人材募集
（有料会告）

有料会告

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

申込期限：毎月 15 日を締切日とし翌月号（15 日発行）に掲載します．

掲載料金：

国公私立教育機関，国公立研究機関	税抜 20,000 円（税込 22,000 円）
賛助会員（企業）	税抜 30,000 円（税込 33,000 円）
賛助会員以外の企業	税抜 50,000 円（税込 55,000 円）

＊本会誌へ掲載依頼いただいた場合に限り，追加料金 税抜 4,000 円（税込 4,400 円）で同一内容を本会 Web ページに掲載できます．

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

＊特に指定がないかぎり履歴書には写真を貼付のこと

■名古屋大学大学院情報学研究科 情報システム学専攻

募集人員　准教授または助教　1 名
専門分野　情報システムのプラットフォーム（計算機アーキテクチャ，並列化等ソフトウェア最適化設計技術，LSI 等情報システム設計技術，組込みシステムなど）に関する教育研究
応募資格　博士の学位を有する方
着任時期　2020 年 10 月 1 日以降のなるべく早い時期
提出書類　履歴書，研究業績リスト，主要論文別刷，これまでの研究概要，今後の研究計画，教育についての抱負，応募者の業績について問い合わせることのできる方 2 名の氏名と連絡先
応募締切　2020 年 3 月 27 日（必着）
送付先／照会先　〒 464-8603 愛知県名古屋市千種区不老町 C3-1（631）　名古屋大学大学院情報学研究科
情報システム学専攻長　結縁祥治
E-mail: yuen@i.nagoya-u.ac.jp　Tel(052)789-3649
そ の 他　詳細は Web ページ（http://www.i.nagoya-u.ac.jp/）をご覧ください

FIT2020 第 19 回情報科学技術フォーラム
選奨論文・一般論文 講演募集予告

会　期：2020年9月1日（火）～3日（木）
会　場：北海道大学 札幌キャンパス（北海道札幌市北区）

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

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

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

有料会告

電子情報通信学会 情報・システムソサイエティ（ISS）並びにヒューマンコミュニケーショングループ（HCG）と情報処理学会（IPSJ）とは、2002年から合同で毎年秋季に、「情報科学技術フォーラム(FIT：Forum on Information Technology)」を開催しており、2020年9月には第19回目を北海道大学で開催します。**本フォーラムは、両学会の大会の流れをくむものですが、従来の大会の形式にとらわれずに、新しい発表形式を導入し、タイムリーな情報発信、活気ある議論・討論、多彩な企画、他分野研究者との交流、などを実現してきております。皆様の研究成果発表の場として、標記のとおり論文発表を募集致しますので奮って御応募下さい。**

●申込主要日程（予定）

登録申込／投稿受付開始：2020年3月30日（月）　→　登録申込締切：2020年5月8日（金）
最終掲載原稿締切：2020年6月19日（金）
※ FIT2017 より、査読付き論文は廃止とし、選奨論文制度を取り入れました。
※ 登録申込と原稿投稿は上記のFIT2020Webページよりお願い致します。詳細は決定次第 Webページでお知らせ致します。

●表彰

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

船井ベストペーパー賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上 3 件選定。賞金は船井情報科学振興財団より 20 万円贈呈。
FIT 論文賞	選奨論文の中から、FIT 学術賞選定委員会で審査の上 7 件程度選定。賞金は FIT 運営委員会より 5 万円贈呈。
FIT ヤングリサーチャー賞	2020 年 12 月 31 日現在で 33 歳未満の講演者（選奨論文および一般論文）の中から、発表件数の 1.5%を上限として選定。賞金は FIT 運営委員会より 3 万円贈呈。本賞受賞は本人に対し一回のみ。
FIT 奨励賞	一般発表のセッション毎に座長の裁量で優秀な発表を 1 件その場で選定（該当なしもあり）。FIT 終了後に賞状を贈呈。

●選奨論文（4～8 ページ程度）

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

●一般論文（2～8 ページ程度）

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

●論文誌推薦制度

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

●問合せ先（FIT2020事務局）

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

情報処理学会創立 60 周年記念（第 82 回）全国大会
イベント企画のみの聴講参加は「無料」!!
事前申込はこちらから⇒ https://www.ipsj.or.jp/event/taikai/82/

情報処理学会創立 60 周年記念（第 82 回）全国大会 聴講事前申込
『サステイナブルな情報社会』

大 会 会 期：2020 年 3 月 5 日（木）～ 7 日（土）
大 会 会 場：金沢工業大学 扇が丘キャンパス（石川県野々市市扇が丘）
共　　催：金沢工業大学
後　　援：石川県、全国高等学校情報教育研究会、野々市市教育委員会

情報処理学会創立 60 周年記念（第 82 回）全国大会の「大会聴講参加」の事前申込を受付中です.
■ 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 ページから事前申込みをする際，「**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）.

事前申込受付期間：2019 年 12 月 6 日 (金) ～ 2020 年 2 月 7 日 (金)

招待講演・特別講演企画【聴講参加無料】：60 周年を記念した招待講演 4 件，特別講演 5 件を予定しております.

招待講演 –1	6 日（金）16：45 ～ 17：00　Data Center Trends: Infrastructure for Intelligent Society （The Korean Institute of Information Scientists and Engineers）
招待講演 –2	6 日（金）17：00 ～ 17：15　未定（China Computer Federation）
招待講演 –3	6 日（金）17：15 ～ 17：30　未定（IEEE Computer Society）
招待講演 –4	6 日（金）17：30 ～ 17：45　未定（Association for Computing Machinery）
特別講演	5 日（木）13：20 ～ 13：50 「大規模医療データの研究開発への利活用～次世代医療基盤法で何が可能となったか～」（仮）
	5 日（木）14：00 ～ 17：00 「SDGs の実装に向けた IT の役割」
	5 日（木）17：10 ～ 18：00 「初音ミク ファン メイド ミニライブ IPSJ-39」 ※事前抽選制
	6 日（金）9：30 ～ 11：30 「～コンピュータパイオニアが語る～『私の詩と真実』」
	6 日（金）12：40 ～ 14：20 「歴代会長パネル討論」
	7 日（土）15：20 ～ 17：50　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 6 号館 334 多目的ホール	5 日　9：30 ～ 12：00 「これからの一般情報教育 why, what, how」 7 日　9：30 ～ 12：00 「情報学のトップ才能からエリートへ－才能の発掘、接続、達人の養成－」
第 2 イベント会場 23 号館 218	5 日　9：30 ～ 12：00 「DX（デジタルトランスフォーメーション）で『2025 年の崖』をどう超えるか」 6 日　9：30 ～ 11：30 「はじめての人文情報学：情報処理技術で文化資料の分析に挑戦しよう！」 6 日　12：40 ～ 15：10 「IoT に関する国際標準化動向と日本の取組み」 7 日　9：30 ～ 12：00 「激変！情報入試を取り巻く環境」 7 日　13：10 ～ 15：10 「地域で自走するプログラミング教育」
第 3 イベント会場 23 号館 221	5 日　9：30 ～ 12：00 「2019 年サイバー事件回顧録～技術と法制度の両面から～」 6 日　9：30 ～ 11：30 「誰のための契約なのか？～アジャイル開発のソフトウェアモデル契約」 6 日　12：40 ～ 15：10 「論文必勝法～良い論文，良い査読，良いジャーナルを目指して～」 6 日　15：30 ～ 17：45 「8th IPSJ International AI Programming Contest SamurAI Coding 2019-20 World Final」 7 日　9：30 ～ 12：00 「AI・ビッグデータ解析、IoT 領域人材のプロフェッショナル資格化を考える」 7 日　13：10 ～ 15：10 「デジタルプラクティスライブ（仮）」

第 4 イベント会場 23 号館 330	5 日　9：30 ～ 12：00　「研究 100 連発 in 石川」 6 日　9：30 ～ 11：30　「MEC(Multi-access Edge Computing) への挑戦」 7 日　9：30 ～ 12：00　「CC2020: Computing Curricula 2020 プロジェクト」 7 日　13：10 ～ 15：10　「信用スコアの期待と課題」
第 5 イベント会場 23 号館 211	7 日　9：30 ～ 12：00　「初等中等教員研究発表セッション」
特別会場 23 号館 105 / 26・27 号館	7 日　9：30 ～ 13：00　「Exciting Coding! Junior ～みんなで一緒にプログラミングしよう～」 7 日　11：00 ～ 13：00　「『先生質問です！』公開セッション」 7 日　13：10 ～ 15：10　「中高生情報学研究コンテスト」

有料会告

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 日間でおよそ 30 会場を使用して，190 あまりのセッションが組まれ，活発な発表，議論・討論が行われます．

懇親会【有料】：

毎回多数の方にご参加をいただき親睦を深めております．当日申込のみとなります．
開催日時：2020 年 3 月 6 日（金）18：00 ～ 20：00（予定）
開催会場：金沢工業大学 扇が丘キャンパス内

IT 情報系キャリアセッション【無料】：

学生の専攻分野と就職を結ぶ「合同キャリア説明会」です．2020 年 3 月 5 日（木），3 月 6 日（金）の 2 日間にかけて，分野ごとに企業ブースを設けます．

ランチョンセミナー【無料】：

スポンサー企業様によるランチョンセミナーを開催いたします。

■聴講参加費・講演論文集代・懇親会参加費（税込）

申込種別	予約価格（2/7 迄）	当　日
大会イベント企画限定聴講参加	無料	無料
大会共通聴講参加（正会員）＊全論文の PDF アクセス権付	9,000 円	10,000 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	15,000 円	17,000 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	無料
懇親会参加 一般（正会員・一般非会員）	−	5,000 円
懇親会参加 学生（学生会員・学生非会員）	−	3,000 円
懇親会参加 学生（ジュニア会員）	−	1,000 円
講演論文集分冊（個人・法人問わず）	13,000 円（送料込）	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（送料込）	66,000 円
講演論文集 DVD-ROM（個人）	10,000 円（送料込）	
講演論文集 DVD-ROM（法人）	60,000 円（送料込）	

■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，各種展示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．
※「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．
※ DVD は大会参加者限定で会場特別販売（5,000 円）いたします．
※ 講演論文集，DVD-ROM 共に，大会開催前の事前発送は致しておりません．受取りは大会終了後の郵送となります．当日会場でも販売いたします．
※ 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．

■聴講参加および講演論文集の予約申込，詳細は，以下のサイトからお願いいたします．

第 82 回全国大会公式 Web サイト　https://www.ipsj.or.jp/event/taikai/82/

■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

◆◆ 有料会告について ◆◆

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

記

■掲載条件

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

■申込方法　任意の用紙に，件名，申込者氏名，勤務先，職名，住所，電話番号および請求書宛先，Web掲載の有無（人材募集のみ）などを記載し，掲載希望原稿を添えて下記の申込先へお申し込みください．

■原稿の書き方

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

●人材募集：　次の項目を明記し，E-mailまたはFax，郵送にてお送りください．
［募集職種，募集人員，（所属），専門分野，（担当科目），応募資格，着任時期，提出書類，応募締切，送付先，照会先］
＊なお，都合により編集させていただく場合がありますので，ご了承ください．

■申込期限　毎月15日を締切日とし，翌月号（15日発行）に掲載します．

■掲載料金　掲載号発行日に料金を請求いたしますので，3カ月以内にお支払いください．

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

ご寄付のお願い

情報処理学会は、情報処理に関する学術および技術の振興をはかることにより、
学術、文化ならびに産業の発展に寄与することを目的に各種事業を戦略的に展開しております。
今回、学会活動の更なる活性化を図る上で会員の皆様からご寄付を頂戴いたしたく、お願いを申し上げる次第です。

皆様から頂きますご寄付は

情報技術を通じて、人類及び世界の発展に資するため
情報技術を中心に学術および技術の振興に資するため
将来を担う人材の育成に資するため

などの観点に照らし、下記の項目に活用させて頂く所存です。

今回ご寄付をお願いしたいのは現金に加えて、情報技術に関わる有形無形の資産（著作物、電子的コンテンツ、特許、ソフトウェア等）、ボランティアで提供いただける役務提供（経験や知識に基づく役務）なども含みます。
お預かりいたしましたご寄付のうち使途のご指定のあるものは、そのご意向に沿った活用をさせて頂き、
ご指定のないものは、その使途を学会活動の活性化に有効な諸事業で活用させて頂きます。
今後も会員の皆様の絶大なるご支援・ご協力を頂きながら、学会発展のために努力して参る所存でありますので、
何卒よろしくお願い申し上げます。

＊ご注意 情報処理学会は寄付金に対する税金が優遇される特定公益増進法人ではございません。

IPSJ　寄付

会員他寄付

現金
資産
役務

IPSJ
学会活動に活用
役務提供

活用先

教育・育成
情報入試　子ども教室　パソコン教室
社会貢献
表彰
国際活動
規格標準化
情報資産保存
学会諸事業
その他





詳しくはこちら

https://www.ipsj.or.jp/annai/other/donation.html

お問合せ

一般社団法人　情報処理学会　管理部門
〒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　FAX 03-3518-8375
soumu@ipsj.or.jp

ご意見をお寄せください！

【2 月 10 日頃までにお出しください】

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

［コード］

〔1〕ご氏名

〔2〕ご所属　　Tel.（　　）　　-

〔3〕E-mail:

〔4〕業種：（a）企業（サービス業）（b）企業（製造業）（c）研究機関　（d）教育機関（小・中・高校・高専・大学・大学院など）
（e）学生　（f）学生（ジュニア会員）（g）その他…… 4-［　］

〔5〕職種：（a）研究職　（b）開発・設計　（c）システムエンジニア　（d）営業　（e）本社管理業務
（f）会社経営・役員・管理職　（g）教職員（小・中・高校・高専・大学・大学院など）
（h）学生　（i）学生（ジュニア会員）（j）その他 …… 5-［　］

〔6〕年齢：（a）10 代　（b）20 代　（c）30 代　（d）40 代　（e）50 代　（f）60 代以上 …… 6-［　］

〔7〕性別：（a）男性　（b）女性 …… 7-［　］

〔8-1〕あなたはモニタですか？：（a）はい　（b）いいえ　…… 8-1-［　］

〔8-2〕あなたのご意見は「会員の広場」（会誌および Web）に掲載される場合があります．その場合：
（a）実名可（氏名のみ掲載）（b）匿名希望　（c）掲載を希望しない …… 8-2-［　］

〔9〕どちらの媒体で記事をお読みになりましたか？
（a）冊子版　（b）情報学広場（電子図書館）（c）Kindle　（d）fujisan　（e）その他…… 9-［　］

〔10〕今月号（2020 年 2 月号）の記事は良かったですか．下記の記事すべてについて評価をご回答ください．
［a…大変良い　b…良い　c…普通，どちらとも言えない　d…悪い　e…読んでいない］

巻頭コラム：ゲーム AI の進歩から見る，AI 時代で大切なもの …… 10-1-［　］
特別解説：OUR Shurijo　みんなの首里城デジタル復元プロジェクト …… 10-2-［　］
特集：ブロックチェーン技術の最新動向
0. 編集にあたって …… 10-3-［　］
1. Bitcoin 技術のその後の動向…… 10-4-［　］
2. 分散台帳上での匿名送金とその監査について …… 10-5-［　］
3. ブロックチェーンの安全性 …… 10-6-［　］
4. 分散台帳技術におけるコンセンサス・メカニズム …… 10-7-［　］
解説：Bitcoin の革新性が導く Web 3 …… 10-8-［　］
ぺた語義：プログラムを投稿してみませんか…… 10-9-［　］
ぺた語義：Processing でプログラミングに挑戦！　…… 10-10-［　］
ぺた語義：第 12 回全国高等学校情報教育研究会全国大会（和歌山大会）　…… 10-11-［　］
情報の授業をしよう！：動画制作授業のすゝめ…… 10-12-［　］
ビブリオ・トーク：ティッピング・ポイント…… 10-13-［　］
5 分で分かる !? 有名論文ナナメ読み：Satoshi Nakamoto : Bitcoin : A Peer-to-Peer Electronic Cash System …… 10-14-［　］
連載：先生，質問です！…… 10-15-［　］
IT 紀行：Maker Faire Tokyo 2019 に行って来た！～来月の Tsukuba Mini Maker Faire に向けて～ …… 10-16-［　］
会議レポート：ICCV 2019 参加報告 …… 10-17-［　］

〔11〕本号で最も良かった記事は何ですか？　上記〔10〕の設問の記事番号から 1 つだけ選び（例：10-8 の記事の場合は「8」と記入），その理由をご回答ください．上記に掲載されていない記事の場合はタイトルを直接ご記入ください．
〔11-1〕良かった記事 …… 11-1-［　］
〔11-2〕この記事に対する貴方の立場：a）専門家　b）非専門家 …… 11-2-［　］
〔11-3〕選んだ理由（下記から，いくつでも選択可）…… 11-3-［　］
a）技術・研究動向がよく分かった　b）知的興味をかきたてられた　c）新たな知識を得ることができた　d）内容が平易で理解しやすかった
e）その他（具体的に下記にご記入ください）

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

〔12-1〕良くなかった記事 …… 12-1-［　　］

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

〔12-3〕選んだ理由（下記から，いくつでも選択可）…… 12-3-［　　］

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

〔13〕今月の特集に対する貴方の立場を教えてください．

〔13-1〕ブロックチェーン技術の最新動向：a）専門家　b）非専門家 …… 13-1-［　　］

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

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

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

■ 各種問合せ先 ■

一般社団法人 情報処理学会（本部）　※支部所在地等詳細はリンクされている各支部ページでご参照ください．
〒 101-0062 東京都千代田区神田駿河台 1-5　化学会館 4F　　Fax(03)3518-8375　https://www.ipsj.or.jp/

担　当	E-mail	Tel(ダイヤルイン)	取り扱い内容
■ 会員サービス部門			
会　員	mem@ipsj.or.jp	03-3518-8370	入会，会費，変更連絡，退会，在会証明，会員証，会誌配布，会員特典，会費等口座振替，海外からの送金，賛助会員，電子図書館
■ 会誌編集部門			
会誌編集	editj@ipsj.or.jp	03-3518-8371	会誌「情報処理」の掲載内容，広告掲載，出版，コンピュータ博物館（情報処理技術遺産）
著作権	copyright@ipsj.or.jp		転載許可，著作権
デジタルプラクティス	editdp@ipsj.or.jp		デジタルプラクティス（DP）の編集・査読，DP レポート
図　書	tosho@ipsj.or.jp	03-3518-8374	出版物購入
■ 研究部門			
論文誌	editt@ipsj.or.jp	03-3518-8372	論文誌（ジャーナル／ JIP ／トランザクション）の編集・査読
調査研究／国際／教育	sig@ipsj.or.jp		研究会登録，研究発表会，研究グループ，シンポジウム，国際会議，IFIP 委員会，情報処理教育委員会，アクレディテーション対応
■ 事業部門			
事　業	jigyo@ipsj.or.jp	03-3518-8373	全国大会，FIT，プログラミングコンテスト，プログラミング・シンポジウム，協賛・後援
技術応用	event@ipsj.or.jp		連続セミナ，短期セミナ，IT フォーラム，ソフトウエアジャパン，その他講習会
認定情報技術者制度	ipsj.citp@ipsj.or.jp		認定情報技術者制度
■ 管理部門			
総務／庶務	soumu@ipsj.or.jp	03-3518-8374	総会・理事会，支部，選挙，総務系選奨，関連団体，アドバイザリーボード
経　理	keiri@ipsj.or.jp		出納，送金連絡
システム企画	sys@ipsj.or.jp		システム企画，セキュリティ，電子化委員会，電子図書館，IPSJ メールニュース
■ 情報規格調査会			
規格部門	問合せフォーム https://www.itscj.ipsj.or.jp/contact/index.html		ISO/IEC JTC 1での情報技術の標準化業務 〒105-0011 東京都港区芝公園3-5-8　機械振興会館308-3 Tel (03)3431-2808　Fax (03)3431-6493　https://www.itscj.ipsj.or.jp/

■ 編集室 ■

私は，仕事上の肩書にも「ブロックチェーン」がついていますし，比較的ブロックチェーンに詳しいヒトと言われることが多いです．しかし，ここだけの話ですが，実はビットコインなどの仮想通貨（暗号資産）を実現するパブリック型のブロックチェーンにはあまり詳しくないのです．これは所属する企業がエンタープライズ型のブロックチェーン推しなせいでもありますし，生来賭けごとのセンスがない私が，仮想通貨の投資ブームを横目で見て敬遠していたせいでもあります（結果的には手を出さなくて正解でした）．

実は，情報処理学会会誌でブロックチェーン特集のエディタをやらないかというお話をいただいた際に，正直「またか」と思いました．ちょうどほぼ並行して2019年7月発行のデジタルプラクティス論文誌でもフィンテック・ブロックチェーン特集のゲストエディタをやらせていただいており，エンタープライズ型については結構カバーしてしまっていたのです．しかし，ピンチをチャンスへ．せっかくの機会なので，「私が読んでみたい記事」を，第一線で活躍される研究者の皆様に書いていただこうということで，本特集を企画させていただきました．一般的なブロックチェーンの基本的な仕組みは，本やWebですでにいろいろ解説が出ていますのでどこかほかで読んでいただいて，その次の「一歩先」を楽しんでいただければと思います．

実は昨年くらいからブロックチェーンに関する国際学会がいくつも出現し，これまで産業界主導だった技術開発にアカデミアの注目が集まっていると感じます．本特集を機会に，日本の技術者の方々にもブロックチェーンの奥深さを感じていただければ幸いです．

（吉濱佐知子／本特集ゲストエディタ）

次号（3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」5G時代の幕開けに向けた研究開発と実証

5Gの実現に向けた取り組み／5G時代のサービス協創とシステムトライアル―幅広い業界とのパートナーシップと5G総合実証試験―／社会を変える5Gへの取り組み―社会課題の解決やワクワク体験の実現に向けて―／5G総合実証実験における取り組み―5G超高信頼・超低遅延通信のトラック隊列走行への適用―／5Gの最新の研究開発技術動向と「情報通信の民主化」への期待／ローカル5Gエリアの可用性向上のための検討―プライベートマイクロセル構造の高度化技術―

学会活動報告：IFIP―情報処理国際連合―近況報告 ……村山優子

教育コーナー：ぺた語義
連　載：IT紀行／5分で分かる!? 有名論文ナナメ読み／先生，質問です！／情報の授業をしよう！／ビブリオ・トーク
コラム：巻頭コラム

掲載広告カタログ・資料請求用紙

広告のお申込み

■広告料金表

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

■「情報処理」

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

■問合せ・お申込み先

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

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

掲載広告の資料請求

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

■「情報処理」 61 巻 2 号　掲載広告（五十音順）

□インタフェース …… 表 2
□エクセルソフト …… 表 3 対向
□オーム社 …… 前付最終
□近代科学社 …… 目次前上
□日立製作所 …… 表 4
□フォーラムエイト …… 表 2 対向
□ すべての会社を希望

■資料送付先

フリガナ
お 名 前 ＿＿＿＿＿＿＿＿＿＿

勤 務 先 ＿＿＿＿＿＿＿＿＿＿ 所属部署 ＿＿＿＿＿＿＿＿＿＿

所 在 地 （〒　　-　　）＿＿＿＿＿＿＿＿＿＿

TEL（　　）　　-　　FAX（　　）　　-

ご専門の分野 ＿＿＿＿＿＿＿＿＿＿

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

賛助会員のご紹介

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

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

●●● 賛助会員（20 ～ 50口）

（株）日立製作所

富士通（株）

日本電気（株）

三菱電機（株）

（株）サイバーエージェント

日本アイ・ビー・エム（株）

●●● 賛助会員（10 ～ 19口）

（株）リクルート

グーグル合同会社

（株）NTT ドコモ

（株）東芝

日本電信電話（株）

日本マイクロソフト（株）

（株）フォーラムエイト

●●● 賛助会員（3 ～ 9口）

（一社）情報通信技術委員会

（株）NTT データ

グリー（株）

楽天技術研究所

（一財）インターネット協会

情報サービス産業協会

トレンドマイクロ（株）

NTT コムウェア（株）

NTT テクノクロス（株）

（株）うえじま企画

沖電気工業（株）

キヤノンマーケティングジャパン(株)

コアマイクロシステムズ（株）

三美印刷（株）

（株）セプテーニ

ソニー（株）

チームラボ（株）

（株）テクノプロ
テクノプロ・デザイン社

パナソニック（株）

みずほ情報総研（株）

（株）レコチョク

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

「情報処理」カタログ同封サービスのご案内

カタログ同封サービスとは？

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

お申し込み方法と掲載までの手続き

❶封入希望月の**前月 15 日**までに下記事項を記載の上、問合せ先までお申し込みください。
- ◆会社名，担当者，連絡先（住所、Tel、Fax、E-mail） ◆封入希望号
- ◆サイズ ◆カタログの簡単な内容説明
- ◆割引対象にあたる場合はその旨記載ください。

❷封入希望月の遅くとも**前月末日**までに下記事項について手配をお願いします。
- ◆カタログ見本を問合せ先までお送りください（PDF、Fax 可）。
- ◆納品業者をお知らせください。

❸**納品日は封入希望月の 5 日（土曜、日曜、祝日の場合は翌営業日）です。**日付指定にて必要枚数（20,000 枚）を印刷し指定の納品先へお送りください。
- ※納品先は、お申し込み後にご連絡いたします。
- ※納品が遅れますと同封ができない場合がございます。その場合はキャンセルとさせていただきます。

❹カタログを同封した学会誌を発行日にお送りしますので、ご確認ください。

❺後日請求書をお送りしますので振込手続きをお願いします。

1 通あたり約17.5 円！

基本価格　350,000 円（税抜）

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

大学や共催事業はさらに割引も！

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

大学 / 研究所 / 賛助会員（基本価格の 40% Off ！）	210,000 円（税抜）
情報処理学会主催・共催事業＊（基本価格の 80% Off ！）	70,000 円（税抜）

＊情報処理学会研究会主催、共催を含む

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

問合せ先

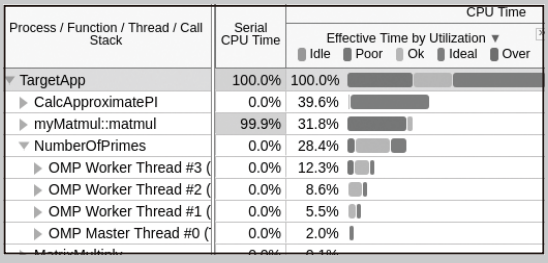
［広告代理店］アドコム・メディア（株）　E-mail: sales@adcom-media.co.jp
〒 169-0073 東京都新宿区百人町 2-21-27
Tel.(03)3367-0571　Fax.(03)3368-1519

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

インテル® Parallel Studio XE は、C/C++、Fortran や Python* が使用されたソフトウェアの計算処理の高速化を支援します。近年、増加を続けるプロセッサーの全てのコアや、インテル® アドバンスト・ベクトル・エクステンション 512 (インテル® AVX-512) を有効活用できる機能を提供します。

並列コードの構築

C/C++ と Fortran コードをインテル® コンパイラーでコンパイルすると、インテル® プロセッサーのパフォーマンスを最大限に引き出すよう最適化されたバイナリーが生成されます。必要に応じて、OpenMP* などのプログラミング手法や同梱されるライブラリーを適用することで、より高いパフォーマンスを発揮させることが可能です。



インテル® VTune™ プロファイラーによるスレッド解析の結果。アプリケーション TargetApp の処理時間の内訳で、特に関数 myMatmul::matmul が Serial CPU Time (単一コアのみの実行時間) のほとんどを占めていた。

インテル® C++/Fortran コンパイラー

- 第 2 世代 インテル® Xeon® スケーラブル・プロセッサーを含むインテル® プロセッサー向けの最適化
- OpenMP* 4.5 と 5.0 による汎用的なスレッド並列と SIMD 並列のプログラミング

高速な Python* 実行環境

"インテル® Distribution for Python*"

最適化済みのパフォーマンス・ライブラリー

数値計算、画像 / 信号処理、並列化テンプレート、データ解析

並列コードの解析

ソフトウェアの現状のパフォーマンスを分析し、問題点を調べます。(※) かかった処理時間について、CPU 使用率、FLOPS、メモリー帯域幅といった様々なハードウェアの要素と、プロセス / スレッド、関数 / ループ、ソースコード行といったソフトウェアの要素に分類および対応付けて把握することで、高速化のために取り組むべき問題を明確にすることが可能です。

※ インテル® Parallel Studio XE Professional Edition または Cluster Edition でのみ利用可能

製品の詳細に関するお問い合わせ先 :

XLSOFT エクセルソフト株式会社
Tel: 03-5440-7875 Fax: 03-5440-7876 E-mail: intel@xlsoft.com
お問い合わせフォーム : www.xlsoft.com/jp/qa

製品詳細はこちらから
www.xlsoft.com/intel/ipsj2

https://www.ipsj.or.jp/event/taikai/82/　情報処理学会　全国大会　検索

一般社団法人 情報処理学会 Information Processing Society of Japan × KIT 金沢工業大学

情報処理学会 創立60周年記念
第82回全国大会

大会テーマ：サステイナブルな情報社会

開催日　2020. 3. 5(木)→3. 7(土)

会　場　金沢工業大学 扇が丘キャンパス
（石川県野々市市扇が丘7-1）

事前予約　2020.2.7（金）まで　当日参加もOK

無料イベント

3/5（木）

SDGsの実装に向けたITの役割
初音ミク ミニライブ（抽選）
これからの一般情報教育Why, what, how
DX（デジタルトランスフォーメーション）で
「2025年の崖」をどう超えるか
2019年サイバー事件回顧録
研究100連発in石川
IT情報系キャリア研究セッション

3/6（金）

情報処理技術遺産認定式
～コンピュータパイオニアが語る～「私の詩と真実」
歴代会長パネル討論
はじめての人文情報学：情報処理技術で文化資料の分析に
挑戦しよう!
IoTに関する国際標準化動向と日本の取組み
誰のための契約なのか？
～アジャイル開発のソフトウェアモデル契約
来たれ!ワークライフバランス伝道師2020
8th IPSJ International AI Programming Contest
SamurAI Coding 2019-20 World Final
MEC (Multi-access Edge Computing) への挑戦
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

3/7（土）

IPSJ-ONE
情報学のトップ才能からエリートへ
―才能の発掘、接続、達人の養成―
激変!情報入試を取り巻く環境
地域で自走するプログラミング教育
AI・ビッグデータ解析、IoT領域人材のプロフェッショナル
資格化を考える
デジタルプラクティスライブ
CC2020：Computing Curricula 2020プロジェクト
信用スコアの期待と課題
初等中等教員研究発表セッション
Exciting Coding! Junior
～みんなで一緒にプログラミングしよう～
「先生質問です!」公開セッション
中高生情報学研究コンテスト

〒101-0062 東京都千代田区神田駿河台一―五
編集人 稲見昌彦
発行所 東京都千代田区神田駿河台一―五 一般社団法人 情報処理学会
発行人 木下泰三
電話 東京（〇三）三五一八―八三七四
振替口座 〇〇一五〇―四―八三四八四
印刷所 東京都荒川区西日暮里五―九―八 三美印刷株式会社
会員外発売所 東京都千代田区神田錦町三―一 株式会社 オーム社

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

雑誌　05269-02

4910052690202
01600