国立情報学研究所ニュース　ISSN 1883-1966（Print）　ISSN 1884-0817（Online）

NII Today

69
Sep. 2015

National Institute of Informatics News

NII Interview

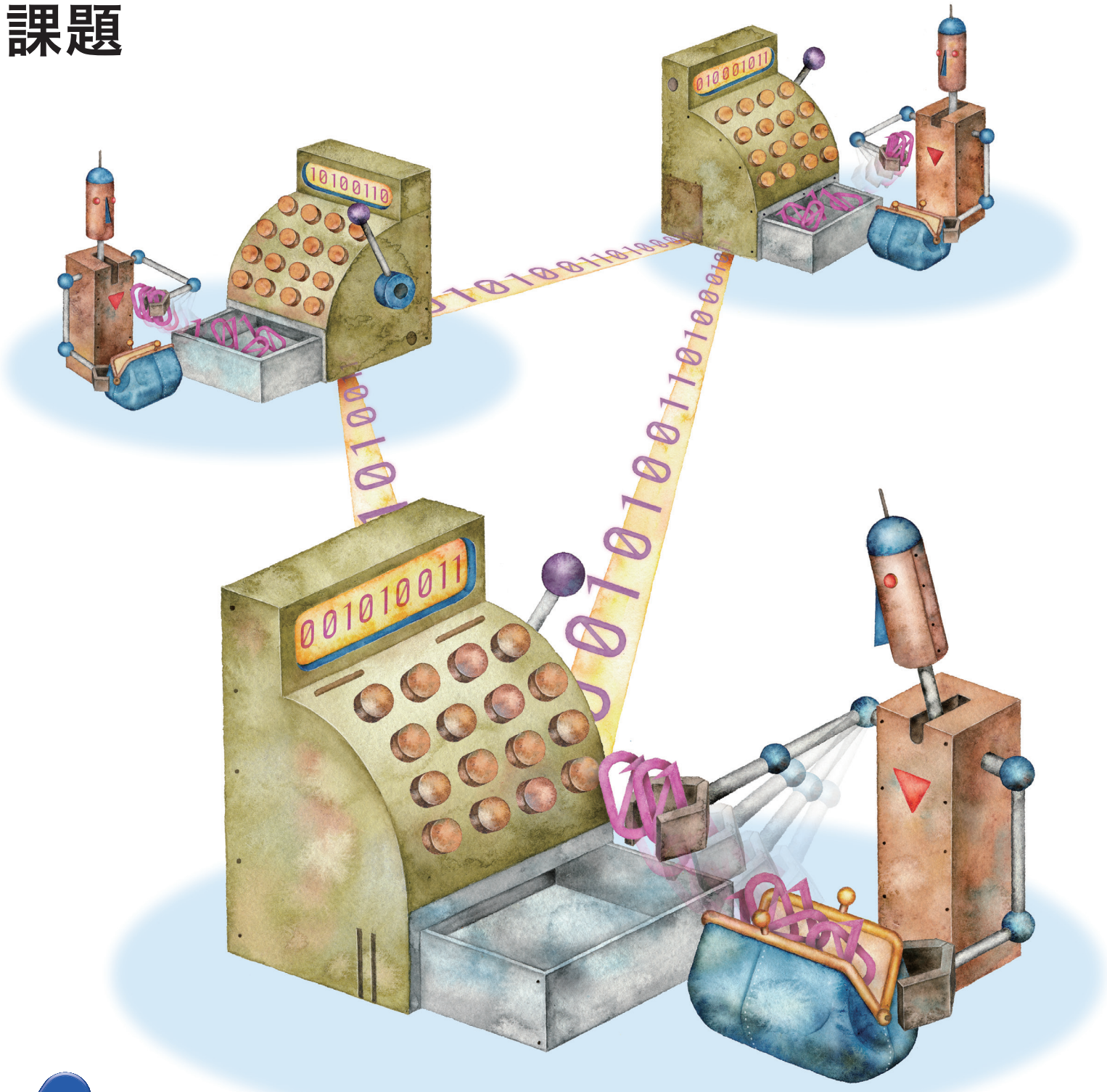
黎明期にある仮想通貨をどう捉えるか

仮想通貨に技術的跳躍をもたらしたブロックチェーン技術

「ビザンチン将軍問題」とは何か

Feature

仮想通貨の技術と課題



大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

黎明期にある仮想通貨をどう捉えるか

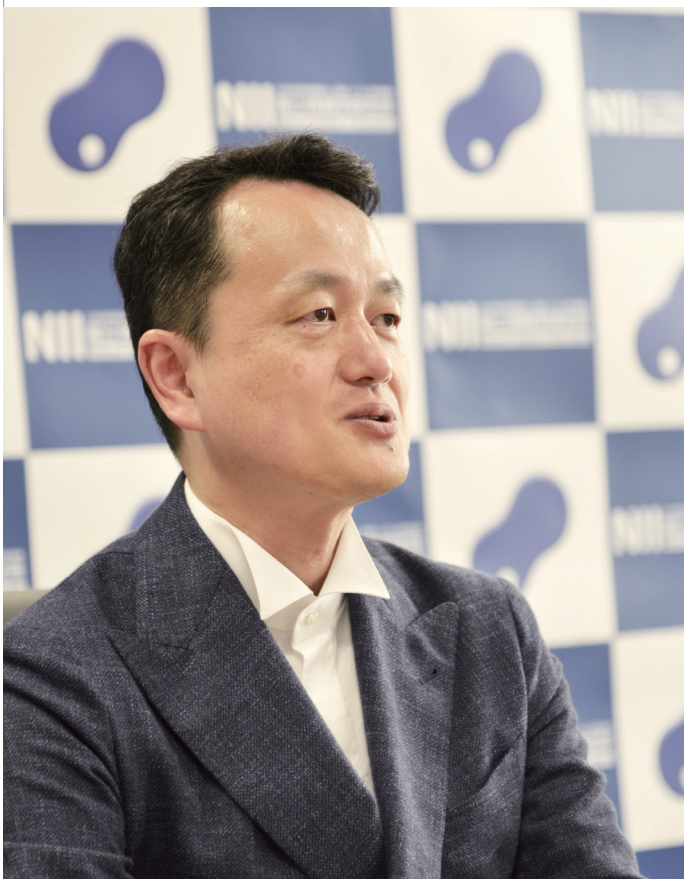
仮想通貨の技術がもたらす世界

岡田仁志［国立情報学研究所 情報社会相関研究系 准教授／総合研究大学院大学 複合科学研究科 准教授］
聞き手：**大河原克行氏**［ジャーナリスト］

ビットコインに代表される「仮想通貨」が世界的に注目を集めている。しかし、技術的にも社会的にも解決すべき課題が残る。不正送金の手段となり得ることや、一部、取引所の破綻などの問題もあり、肯定的に広く評価されているとは言いがたい。一方で、仮想通貨に関する技術は一歩ずつ着実に進んでおり、今後さらに法制度の整備が進むと予想されることから、将来、大きな潮流になる可能性を秘めている。

なぜ、仮想通貨は注目されるのか。情報制度論の研究者として、1995年より電子マネーの研究に取り組み、既存の法体系ではカバーしきれない電子商取引などの研究を手掛けてきた岡田仁志准教授は、「仮想通貨を取り巻く環境は、1995年前後のインターネットの黎明期に似ている」と言う。岡田准教授に、仮想通貨の問題点と課題、それを支える技術や仕組みについて聞く。

岡田仁志 OKADA Hitoshi



仮想通貨を取り巻くリスク

大河原　日本では、ビットコインを取り巻く事件によって、仮想通貨が何であるのか正しく理解される以前に、危険なものというイメージが先行しているように思います。仮想通貨とは危険なものなのでしょうか。

岡田　仮想通貨という大きなくくりで議論すると、その結論を誤ります。一つ目は、技術そのものにどれほどのリスクがあるのかという観点。そしてもう一つは、仮想通貨を扱う取引所や現行の制度やルールにどれほどの危険が存在するのかという点。少なくとも、この二つの観点からリスクを見る必要があるでしょう。前者については、ビットコインをはじめとする分散型仮想通貨には発行主体が存在せず、国家の裏付けがないという点で、これまでの通貨とは仕組みが大きく異なり、そこに不安を感じる人が多いのかもしれません。

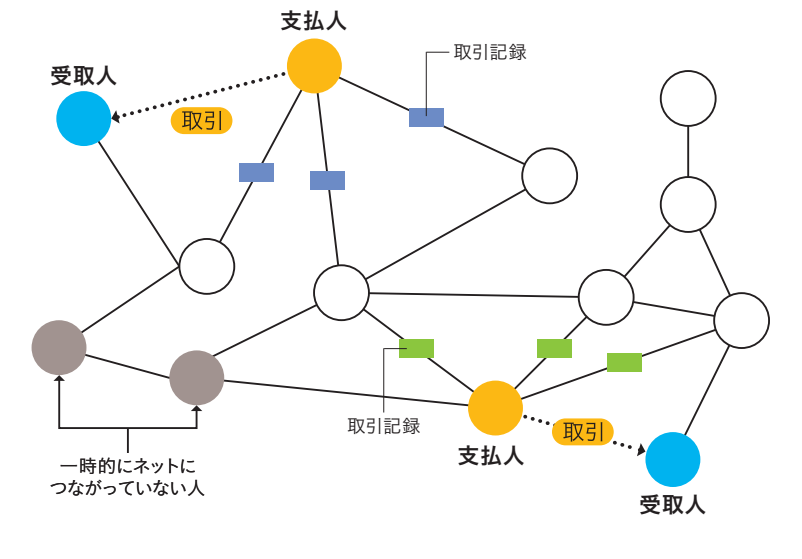
大河原　ビットコインを例にあげると、参加者全員が秘密鍵と公開鍵の2種類のペアになった鍵を持つという暗号技術によって取引が守られています。さらに、中央管理型の電子マネーとは異なり、「ブロックチェーン」（詳細は P6-7）という方式を用いることで、参加者全員の記録によって支払い情報の正しさを担保する仕組みとなっていますね。その点では、秘密鍵が壊れたり、失われたりしない限り、利用者自身が持つビットコインをしっかり確保できる環境ができている。Mt.Gox の場合も、取引所としてのセキュリティが確保され、社内からのア

仮想通貨の代表であるビットコインの仕組み

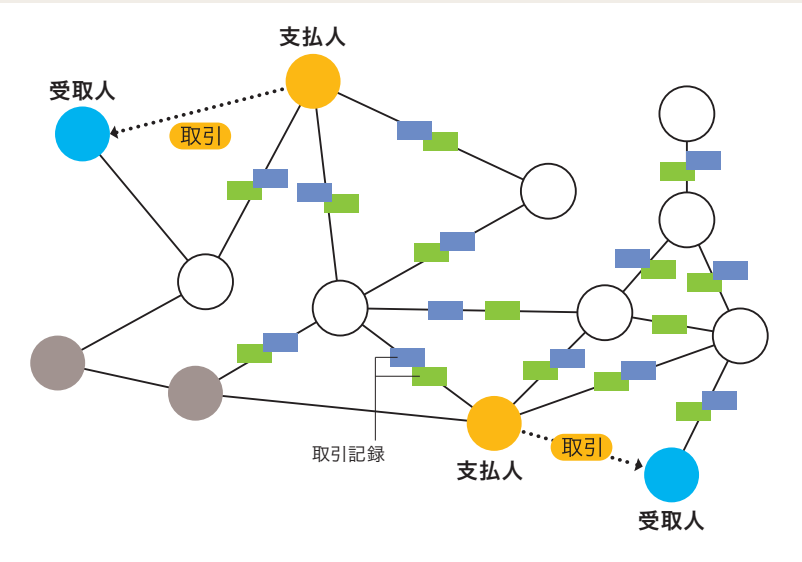
ビットコインは、「Satoshi Nakamoto」と名乗る実在性が未確認の人物の論文（“Bitcoin: A Peer-to-Peer Electronic Cash System.”（November 2008）．／https://bitcoin.org/bitcoin.pdf）が原点となっており、P2P（ピアツーピア：すべての参加者がネットワークの一部としてサーバにもクライアントにもなる方式）型で構成される電子的に取引される仮想通貨。国家の裏付けはなく、ネットワークを通じて流通する決済手段である。ネットワークで送受信が可能な「独立性」、複製や偽造ができない「安全性」、使用者や使用履歴が特定されない「プライバシー」を担保するネットワーク技術をベースに、電子貨幣の一つの理想像を実現したと言える。とくに、発行者や中央管理者を持たないにもかかわらず、実際の貨幣と同様に、当事者間で直接譲渡が可能な「転々流通性」や、額面を分割して使用可能な「分割可能性」の機能を持つことは特筆すべきであり、現状の日本の電子マネーと大きく異なる。

ビットコインのもう一つの大きな特徴は、「採掘作業」によって通貨が発生する点だ。採掘とは、直近の数百件の取引情報をブロックと呼ばれる帳簿に格納し、これに直前のブロックのハッシュ情報を加え、さらに、乱数を加えながらハッシュ関数の値を取り続け、ハッシュ関数で得られた値において、0が一定個数並ぶまで計算を続けるというもの（詳細はP6-7）。採掘（計算）には約10分間の作業が必要で、計算結果を導き出して「採掘」に成功した勝利者だけが、ビットコインの取引記録に新たな記録を追加する権利を得て、一度の採掘で現時点では25BTCを入手できる（4年毎に半減させられる）。そして、参加者がその計算結果を認めることで、取引の正しさが保証される。一方、受け取った仮想通貨を次に送金するためには、電子財布の中に格納されている秘密鍵による電子署名とそれを検証してもらうための公開鍵が必要である。

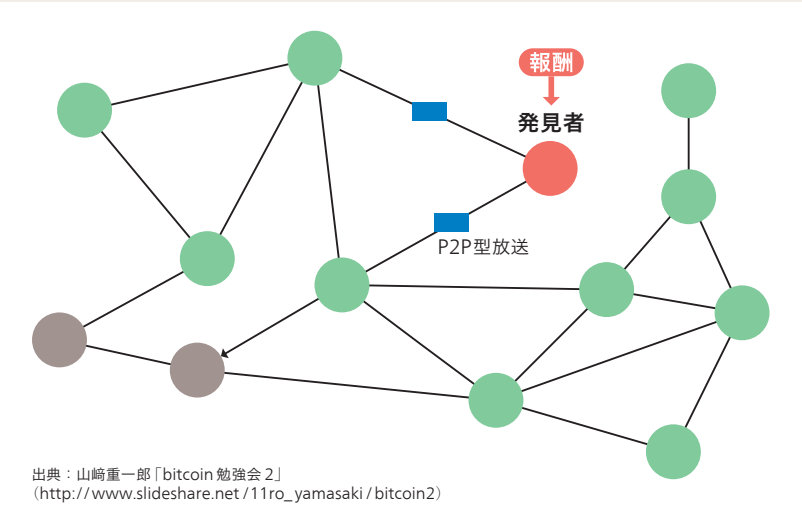
このように技術の組み合わせにより、中央管理者がいなくても転々流通性が担保され、取引の正しさが保証される点が、ビットコインが多くの研究者を惹きつける理由と言える。



図A｜ビットコインの取引発生
ビットコインのソフトウェアを起動すると、自動的にP2Pネットワークに接続される。新しく取引が発生すると、支払人が「取引」のデータを全参加者に向けて放送する。

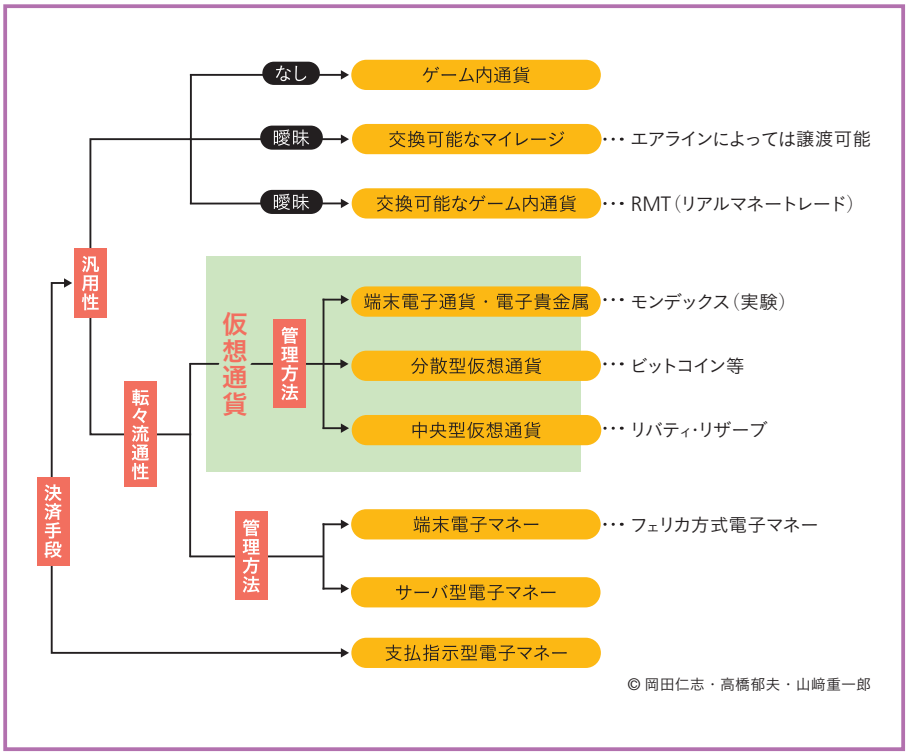


図B｜P2Pネットワークの放送
P2Pネットワークのノード（中継点）は、受け取った「取引」のデータを他のノードにパスする。バケツリレー方式でパスを回し、やがてすべてのノードに伝達される。



出典：山崎重一郎「bitcoin勉強会2」
（http://www.slideshare.net/11ro_yamasaki/bitcoin2）

図C｜プルーフ･オブ･ワークを発見
「採掘」に参加するノードは、0が一定個数並ぶような値を発見するまで計算を繰り返す。最初に値を発見したノードは、発見した値をすべてのノードに向けて放送する。



図｜仮想通貨と電子マネーの分類

クセス管理が強固であれば、あのような事件は起こらなかったはずです。

岡田　その点で、今、問題とすべきなのは、仮想通貨そのものの仕組みや技術的な課題ではなく、先に挙げた二つのリスクの観点の後者である取引所の技術的課題や、それらを管理する制度だといえます。銀行業務は、銀行法によって認可された企業だけが行うことができますが、仮想通貨については規制がない。金融庁は取引所を免許制あるいは登録制とする方向で検討を始めたと報じられていますが、そうした仕組みによって信頼できる取引所を制度面から支えることも必要でしょう。

今年 6月、マネーロンダリングを規制する国際組織である金融活動作業部会（FATF）は仮想通貨の規制強化を求め、取引所に対する免許制導入などを提言しました。米ニューヨーク州は仮想通貨ビジネスに関するライセンス制度の運用を開始している。こうした制度面の整備は、仮想通貨の広がりに大きく影響するでしょう。ただ、免許制や登録制とする場合、仮想通貨の特徴を踏まえたものにしなければなりません。これまでの銀行法の延長線上で、金融業のノウハウを持つことを前提に認可するだけでは不十分です。仮想通貨は ICT 環境での運用を前提としていますから、ICT の十分な知識とノウハウを有し、セキュアな環境を実現することが不可欠です。そうした意味で、仮想通貨の普及には情報セキュリティ監査がより重要な要素を担うことになると考えています。

仮想通貨は普及するのか？

大河原　現状では、仮想通貨はまだアーリーアダプターと呼ばれる一部の人たちが使っているに過ぎません。日本で仮想通貨は広がるのでしょうか。

岡田　国内だけなら、仮想通貨の必要性はあまり感じられないかもしれません。日本は金融インフラが整備され、貨幣にしても、商品券や電子マネーにしても、信用された主体によって発行されたものだけを使用してきた文化があります。また、リスクが発生した際にも、多くの場合は救済されてきた。しかも、これだけ電子マネーが広がりをみせ、日本全国どこでも、コンビニエンスストアでも鉄道でも手軽に電子マネーが使える中で、あえて仮想通貨を使う必然性はないでしょう。

しかし、2020年に向けて外国人観光客を2000万人にまで増やすという政府目標を実現する上で、仮想通貨への対応は避けて通れないものになる可能性があります。成田空港に到着した外国人観光客が最初に困るのが、1杯目のコーヒーを飲む時です（笑）。日本ではクレジットカードの少額決済を嫌う傾向がありますから、日本円に両替をしておかないと、コーヒー 1杯すら飲むことができない。これが仮想通貨で購入できれば、スマートフォンを持っているだけで済む。すでに六本木や銀座などにはビットコインで決済できる店舗がありますが、2020年に向けて、小売業やサービス業では仮想通貨の利用環境の整備を視野に入れた検討が進むかもしれません。

もう一つは、企業における国際間取引で仮想通貨を利用する動きです。為替の影響を受けず、共通の通貨価値で取引ができ、しかも、手数料がほとんどかからないという点で、国際間取引における仮想通貨の利用が増えていくことが予想されます。日本では今後、TPP（環太平洋経済連携協定）により、国際間取引の増加が見込まれます。その中で仮想通貨活用の動きも出てくると思います。

大河原　日本にいると、そこまで仮想通貨が普及するようには感じられません。

岡田　確かにそうかもしれませんね。しかし、欧米では静かに仮想通貨の活用が広がっています。旅行予約サイト大手の米エクスペディアやパソコン大手のデルが決済に仮想通貨を活用し始めています。また、銀行口座を持たない人たちが多い新興国で、インターネットとスマホの普及とともに仮想通貨の活用が広がることが予想されます。仮想通貨の口座を持ち、スマホから金融取引を行うという使い方が一気に広がる可能性がある。よく「周回遅れのトップランナー」と言われますが、新興国においては、インターネット、スマホ、仮想通貨という組み合わせは、金融インフラを整備する上で効率的な提案の一つでしょう。利便性の高さが認識されれば、これまで以上に普及

が加速するのは明らかです。

実は、ビットコインの性質は、1995年にイギリス・スウィンドンで実証実験が行われた電子マネー「モンデックス」と「現金らしさ」という側面で少し似たところがあり、インターネットによる決済やデバイスの広がりなどの条件が整ったことで、かつて各国の銀行まで巻き込んだ取り組みがいよいよ実現しつつあるともいえます。そして、当時を知る人たちが、このビットコインに大きな期待を寄せ、利用促進に向けた整備を進めようとしているのも興味深いことです。ちなみに、現状の電子マネーと仮想通貨の最大の違いは、不特定の者との間で決済の手段として利用され、さらにそれを譲受人が第三者に譲渡し得る「転々流通性」を持つことにあります。そういった意味では、現実の貨幣により近い性質も持ち得るのです。

大河原　米マサチューセッツ工科大学（MIT）はメディアラボの伊藤穰一所長が中心となってビットコインの普及に向けた最先端研究機関を設立すると発表しました。これはどんな影響を及ぼしますか。

岡田　ビットコインの仕組みには一定の評価があり、ゆえに多くの研究者や企業が関心を払ってきたわけですが、その一方で、新たな技術に実際の動きが追随できていないという課題がありました。「ビットコインファウンデーション」がその役割を果たしてきましたが、より技術中立的な研究機関の登場が求められています。MITが中立的な立場で中核技術の進化を支えるような形になれば、仮想通貨の技術研究をさらに発展させることになるでしょう。

仮想通貨は インターネットに似ている

大河原　仮想通貨が世界中を巻き込んだ金融システムの変革を促す可能性があるということですか？

岡田　今の仮想通貨を取り巻く環境を見ていると、1995年前後のインターネットの黎明期によく似ているんですね。インターネットもビットコインも中央管理者がいないという点で似ているし、当時はそれがどんな技術なのか、本当に安全で信頼できるものなのかが議論され、未知の技術に対する懐疑的な意見も多かった。一方で、メリットについてもよく議論されていました。その後、インターネットは世の中を大きく変えました。そして、今では仕組みを気にする人はほとんどいません。それぞれがリスクを知りながら活用しています。仮想通貨も同じで、今はその仕組みやリスク、メリットに注目が集まっています。インターネットの時もそうでしたが、多くの人がメリットを感じれば、自然と普及していくものです。

大河原　ビットコインに所有権が成立するかどうかが議論されているようですが、仮想通貨はモノとして捉えればいいのでしょうか。

岡田　日本では、昨年3月に国会でも質問があったように、ビットコインは通貨かモノかという二者択一の議論が展開されました。政府答弁は、少なくとも通貨には該当しないことを確認していますが、モノであると定義したわけではありません。まずは、仮想通貨が通貨としてどう位置づけられるのかを議論しなければなりません。

仮想通貨は国際的な取引にも活用されるものですから、欧米の動きを注視しながら、日本の制度をつくる必要がある。一方、米国では、通貨とは法的な強制通用力を持ち、流通性があり、慣習的に利用されているものと定義していますが、仮想通貨に関しては強制通用力を持たないものであるとされています。つまり、任意で受け取れば支払いとして成り立つが、通貨としての属性をすべて備えるわけではないということです。日本でも同様に、相手の同意を得た上で取引の対価に利用できる任意通貨として認める方向が適していると思います。ただ、日本法と米国法では通貨の位置付けが異なりますので、法的整合性をとるための検討が必要です。

まず、仮想通貨の制度的リスクと技術的リスクを洗い出して、次にその技術や仕組みを正しく理解し、それに対応する準備を始めることが必要でしょう。将来を見据えて、ビットコインの基幹技術であるブロックチェーンに関しても、日本が最先端の技術や知識を蓄積しておくことが不可欠だと強く感じています。

（写真＝佐藤祐介）

インタビュアーからのひとこと

発行主体を持たない仮想通貨は、これまでの通貨制度とは大きく異なることから、不安視する声があるのも当然だ。しかし今こそ、発想の転換が求められているのではないか。インターネットやモバイル環境が社会インフラとして定着した時代においては、仮想通貨の利活用は避けては通れないものになる。とくに、過去のしがらみがない新興国では一気に仮想通貨が利用されるようになるだろう。日本人の発想の転換が遅れると、国際取引における競争力を失うかもしれないという危機感すら感じる。リスクが大きいという先入観を持つのではなく、まずは仮想通貨を正しく理解することが大切だ。

大河原克行 OHKAWARA Katsuyuki

ジャーナリスト。1965年、東京都出身。IT業界の専門紙の編集長を経て、2001年からフリーランスジャーナリストとして独立。25年以上にわたってIT産業を中心に幅広く取材、執筆活動を続ける。現在、ビジネス誌、パソコン誌、ウェブ媒体などで活躍。

仮想通貨に技術的跳躍をもたらしたブロックチェーン技術

取引を支える技術には応用可能性も

山﨑重一郎
［近畿大学産業理工学部情報学科 教授］

通貨を電子情報としてネットワークで流通させるために、さまざまな技術やシステムが模索されてきた。その中でも、ビットコイン型の仮想通貨が研究者の関心を集める要因は、発行主体も管理者も持たずに健全性を保つ、巧みな仕組みと技術にある。その取引の健全性を裏付けている「ブロックチェーン技術」とはどのようなものなのか。ブロックチェーン応用システムの研究に取り組む近畿大学の山﨑重一郎教授に、技術的観点から解説してもらった。

仮想通貨とは、「国家の裏付けがなく、ネットワークなどを介して流通する決済手段」です。通貨を電子情報としてネットワークで流通させるには、現物の貨幣と同様に、不特定多数の人との決済に利用できる流通性と、受け取った人が第三者に譲渡できる連続譲渡性という二つの要素を合わせた「転々流通性」を持たせなければなりません。実用化のためには、取引内容の改ざんや二重使用などの不正を防ぐことも必要です。

転々流通性と不正使用防止の両立は、「信頼できる第三者」が存在する中央管理型のシステムなら実現できます。ただし、第三者の信頼性を確保するためには運用コストがかかり、手数料の高騰などの問題が生じるでしょう。

技術を緻密に組み合わせた仕組み

そうした課題を鮮やかに解決したのがビットコインです。「Satoshi Nakamoto」と自称する謎の人物が2008年に発表した論文に記述されていた仮想通貨の構想は、ソフトウェアと分散型ネットワークシステムのみで不正使用を防止しながら、インターネットを介した転々流通を可能にするものでした。

構成要素となっている個々の技術は、実は目新しいものではなく、これまで実際に利用されてきた実績のある技術です。それらの堅実な技術を緻密な構想の下で見事に組み合わせ、仮想通貨に技術的跳躍をもたらしたのがビットコインの仕組みなのです。

基盤となるのは、ネットワーク上で対等な状態にある端末どうしを直接接続してデータをやりとりする、P2P（ピアツーピア）型のネットワークです。ビットコインのソフトウェアをインストールして起動すると、自動的にそのネットワークに接続されます。

P2P型のネットワークには、中心となるようなサーバやストレージはありません。取引のデータが蓄積されるのは、利用者それぞれの端末です。ビットコインを送金する際には、送金者は「取引記録（トランザクション）」と呼ばれるデータを、受領者だけでなくネットワークに接続している利用者全員に向けて送信します。そして、送信された取引記録は、「ブロックチェーン」と呼ばれるデータベースに蓄積されていきます。

ブロックチェーン技術とは

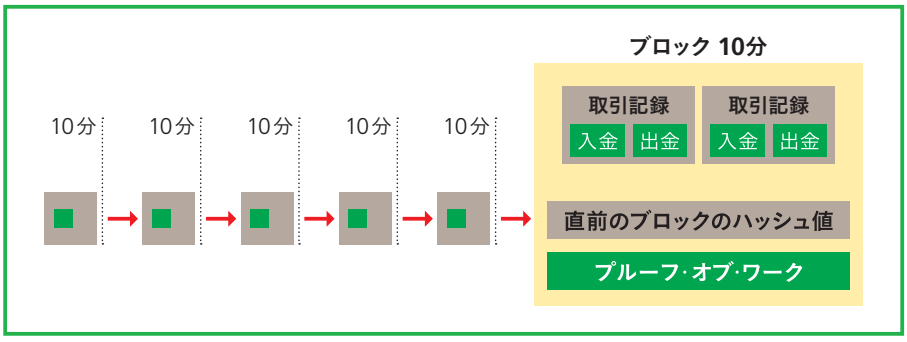
このブロックチェーンへのデータ蓄積方法が、ビットコインの核心部です。

ビットコインの利用者は、ある計算競争に参加することができます。その競争とは、暗号学的ハッシュ関数を利用したもので、概念的に説明すると、サイコロを振って、ある数より小さい目を最初に出した人が勝利者になるというようなものです。

計算競争の勝利者は、直前の約10分間の取引記録を検証し、計算の解（プルーフ・オブ・ワーク）とともに「ブロック」と呼ばれる1つのデータの塊にまとめ、ビットコインの利用者すべてに送信します。受け取った利用者がそれぞれブロックの内容を検証し、問題ないと判断されれば、そのブロックは既存のブロックと接続されて保存されます。

このようにブロックが次々と作成、確認されて、時系列で接続されていくことから、このデータベースをブロック

図｜ブロックチェーンの仕組み



チェーンと呼んでいます（図）。ブロックチェーンは、取引記録を書き込む帳簿としての役割とともに、タイムスタンプとしても機能しています。もし、過去にさかのぼって取引内容を改変しようとすると、各ブロックに含まれたプルーフオブワークをもう一度計算し直すという膨大な手間が必要になり、事実上不可能です。その仕組みが、仮想通貨の実用化に不可欠な要素である取引の非可逆性や二重使用の防止を支えています。

人間の「欲望」を利用

計算競争のインセンティブは、ビットコインの報酬です。計算競争が行われるたびに、一定額（現在は25BTC）のビットコインが新規発行され、直近約10分間に行われた取引の手数料とともに、計算競争の勝利者のものとなります。これが、あたかも金の採掘のようであることから、計算競争は「採掘（マイニング）」と呼ばれています。

ビットコインのソフトウェアは、おおよそ10分間で正解が出るような難易度に調整しながら、計算競争の問題を出題し続けています。採掘には誰でも参加できますが、勝利するためには、約10分間に他者より多くサイコロを振る力が必要で、より多くの計算能力を持つほうが有利です。計算能力を高めるには多額の投資と電力コストが必要になりますが、勝利者になればビットコインの報酬が得られるのです。

発行主体も管理者もないシステムでは、一見、圧倒的な計算能力を持つ利用者が現れたり、一部の利用者が結託したりすれば、不正を働くことも可能に思えます。しかし、ビットコインの価値はビットコイン経済が健全であってこそ保たれるものであり、不正行為によりシステムそのものを破綻させるのは合理的ではありません。

もちろん、堅牢性の高い公開鍵暗号技術や電子署名、すべての取引の整合性を検証可能にする帳簿記述方式など、不正を防止する技術はきちんと用意されています。それに加えて、採掘の仕組みとブロックチェーンの技術によって、人間の欲望をシステム全体を発展させるドライビングフォースとしつつ、健全性の確保にも利用するという、実に巧みなアイデアです。

分散型ネットワークにおいて、偽の情報に惑わされずに正しい合意を形成する方法は「ビザンチン将軍問題」（詳細はP8-9）として知られていますが、ビットコインはその難問に対して、ブロックチェーンのシステム設計によって解決を試みた例と言えるでしょう。

電子情報に原本性を持たせる

このように、ブロックチェーン技術は、電子的に記録された事象を積み上げ、ブロックというクロニクル（歴史的記録）とすることによって、改変を不可能にしました。これまで困難と考えられてきた、電子情報に原本性を持たせることに成功したのです。さらに、タイムスタンプ機能も有することから、事象の発生順序も証明できます。

こうした特性から、地域通貨システムはもちろん、公共関連の申請や届出のシステム、公文書を扱う社会情報基盤などへの応用も可能です。記録の真正性、時間的な優先性の根拠、所有の移転などをサイバーの世界だけで証明する手段として、社会に大きな変化をもたらす可能性を秘めています。（構成＝関亜希子）

山﨑重一郎
YAMASAKI Shigeichiro

近畿大学産業理工学部情報学科教授。専門はモバイル・エージェント、公開鍵認証基盤など。現在は社会情報基盤としてのブロックチェーン技術の応用に関する研究を行っている。

「ビザンチン将軍問題」とは何か

ビットコインが通貨になるには、その解決が不可欠

仮想通貨の不正使用とビザンチン将軍問題

ビットコインを仮想通貨として利用するには、取引内容の改ざんや二重使用などの不正を防がなければならない。こうした不正は、情報学やコンピュータサイエンスでは「ビザンチン将軍問題」(Byzantine Generals Problem)と呼ばれる問題とよく似ている。

さて、ビザンチン将軍問題とは、2014年にチューリング賞を受賞した数学者のレスリー・ランポート博士(Leslie Lamport)らが考案した分散システム上の信頼性に関わる問題である[1]。なお、ランポート博士はLaTeX(電子組版システムTeX用の論文作成用マクロパッケージ)の作成者として有名だが、研究者としての専門は分散システムの基本アルゴリズムである。

ビザンチン将軍問題の舞台は、ビザンチン帝国の将軍たちがそれぞれ部隊を率いて敵を包囲している戦場である(図1)。各部隊はそれぞれ離れた場所にいて、伝令を相互に送ることでしか連絡できない。戦局は、将軍たちがいっせいに指令を出して攻撃を仕掛ければ勝てるが、一部の部隊だけで攻撃を仕掛けると負けてしまうという状態。つまり、攻撃か撤退かのどちらかを、全将軍が一致して同意しなければならないのだ。しかし、将軍たちの中には裏切り者、つまり敵に寝返っている将軍がいるかもしれない。裏切り者の将軍は、他の将軍から攻撃の提案を受けると、撤退の提案にすり替えて別の将軍に伝達するかもしれない。そうなると、一部の将軍は攻撃指令と撤退指令の両方を受け取ることも想定される。最悪、一部の部隊だけが攻撃を開始してしまい、負ける可能性もある。

図2-Aにおいて、攻撃(または撤退)を提案した将軍は、他の将軍たちにその提案を送る。その提案を受け取った将軍は別の将軍に転送するとする。しかし、将軍2が裏切り者の場合は、攻撃を撤退(または撤退を攻撃)に替えて将軍3に送る。このとき将軍3は最初の提案が攻撃だったのか撤退だったのかわからない。なお**図2-B**のように、ビザンチン将軍問題では、攻撃(または撤退)を提案した将軍が裏切り者である場合も想定する。この場合は他の将軍たちに、攻撃または撤退を替えて送ることもある。

さてビザンチン将軍問題とは、(裏切り者ではない)誠実な将軍たちが全員一致で攻撃または撤退に同意できる場合、つまり正しい判断に対して、将軍たちの判断を全員一致へと導く方法を考えることである。ランポート博士らの研究により、裏切り者の将軍がN人のとき、誠実な将軍が2N＋1人以上であれば、誠実な将軍どうしの判断が一致できることがわかっている。将軍4人のうち1人が裏切り者である場合(N＝1)を**図3**に示す。

耐故障性のある分散システムに対する難問

ランポート博士は、このビザンチン将軍問題を、耐故障性のある分散システムにおける同意問題として考えた。ここで言う分散システムは複数のコンピュータが協調することで、1台のコンピュータではできないような処理を実現するものとする。いま話題のクラウドコンピューティングも、分散システムの一形態にすぎない。また、同意とは複数のコンピュータで同じ値を持つことである。

同意したい値を通信で他のコンピュータへ送ればいいと思うかもしれないが、コンピュータは壊れることがあるし、複数のコンピュータがあればそれだけ壊れるコンピュータも増える。故障しても、そのまま止まれば対処のしようがあるが、動き続け、しかも間違った通信や処理を始めると非常にやっかいな問題となる。つまり、ビザンチン将軍問題では、故障しても止まらずに、間違った動作を行うコンピュータを裏切りの者の将軍に見立て、他の正常なコンピュータを誠実な将軍に見立てることで、複数の正常コンピュータが同じ値を持つ方法やその条件を扱ったというわけだ。

図1 | ビザンチン軍による敵軍包囲

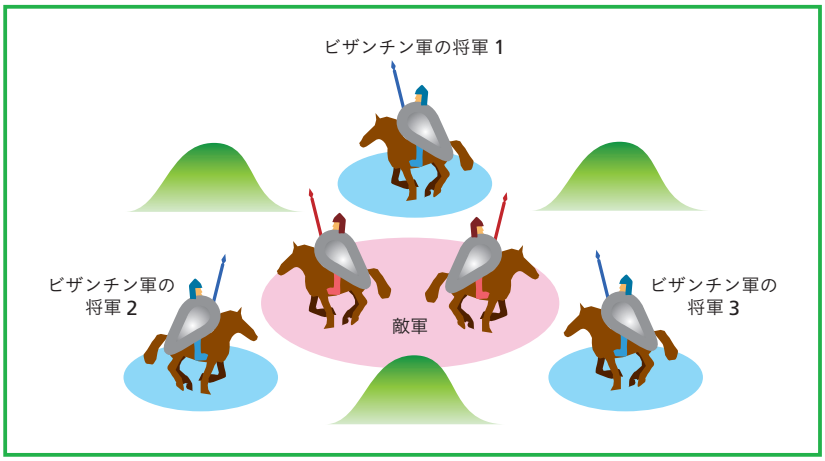


図2 | 3人のビザンチン将軍（裏切り者1名を含む）

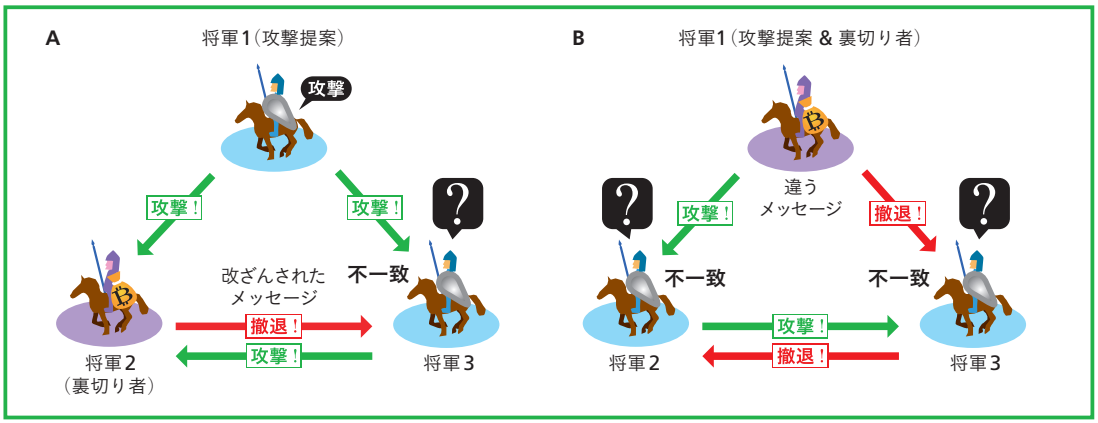
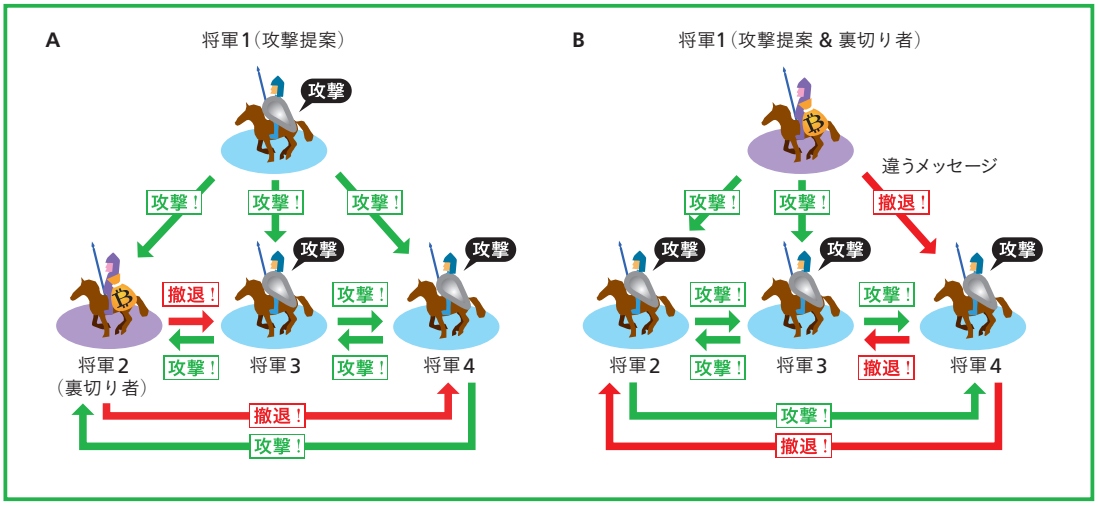


図3 | 4人のビザンチン将軍（裏切り者N＝1名、4≧3N+1）



なお、ビザンチン将軍問題は分散システムの教科書であればたいてい取り上げられるポピュラーな話題であり、さらに故障の結果、予測不能な不具合を起こすことをビザンチン故障と呼ぶこともある。これはコンピュータの故障の中でも一番面倒なケースとなる。

問題を解決しなければビットコインは成立しない

ビザンチン将軍問題とビットコインとの関係であるが、ビットコインでは、取引の改ざんや二重使用がビザンチン将軍問題における裏切り者の将軍に相当し、逆に言えばビザンチン将軍問題を解決しないとビットコインは通貨として成立しない。そこでビットコインは、不正を発見・抑止するメカニズムを導入している（P6-7参照）。これはブロックチェーンと呼ばれる10分単位の取引記録を作るには膨大な計算を必要とするようにし、最も早くブロックチェーンを計算した者にビットコインを渡すことで記録作成のインセンティブを与えるというもの。一方で、過去のブロックチェーンを改ざんしようとすると膨大な計算が必要になるように設計されており、取引の改変が困難なことが、仮想通貨としての継続性を保証している。

これは見方を変えると、ビットコインにおけるブロックチェーンのメカニズムは、ビザンチン将軍問題における不誠実な将軍への対応策としてみることができ、将来、仮想通貨の取引に限られた状況における、ビザンチン将軍問題に対する新しい解法につながるかもしれない。

ちなみに、ランポート博士はユーモアのセンスがある研究者で、例題としてビザンチンの将軍を持ち出したのはランポート博士のユーモアからであった。ランポート博士は、ビザンチン将軍問題以外にも、パクソス（Paxos）アルゴリズムと呼ばれる、古代ギリシャの島の議会を舞台にした分散同意システムも提案している。ビザンチン将軍問題では裏切り者の将軍だったが、パクソスアルゴリズムでは、議員が議会途中に帰ってしまうケースを、コンピュータの故障と回復の比喩として考えた。ランポート博士は、このアルゴリズムに関する最初の論文[2]を1990年に学術ジャーナルに投稿したが、ユーモアたっぷりに古代ギリシャの議会を例にアルゴリズムを説明したため、そのジャーナルの編集者は冗談だと思い込んだのか、論文をそのまま放置してしまい、結局、論文がジャーナルに掲載されたのは投稿から9年後の1998年になったという、前代未聞の事件まで起きた。

なお、パクソスアルゴリズムは、その後、クラウドコンピューティングでは複製データの更新処理などの根幹技術として使われている。ビザンチン将軍問題と同様に有名になる日も近いかもしれない。

（文／図＝佐藤一郎［国立情報学研究所 アーキテクチャ科学研究系 教授］）

参考文献

[1] Leslie Lamport, Robert Shostak, Marshall Pease: "The Byzantine Generals Problem", ACM Transactions on Programming Languages and Systems, Vol.4, No.3, pp. 382-401, 1982.

[2] Leslie Lamport: "The part-time parliament", ACM Transactions on Computer Systems, Vol.16, No.2, pp. 133-169, 1998.

News 1 オープンハウス2015 ～“NII研究100連発”に沸く オープンフォーラム2015も開催

NIIの研究や事業を一般から研究者まで幅広い層に向けて紹介する「オープンハウス2015」を6月12日、13日に開催しました。

喜連川優所長は「新SINETに向けて：全国・対米100ギガ化を目指す～NIIが描くe-infrastructure」と題して活動報告。NIIが大学や研究機関に提供している「学術情報ネットワーク（SINET）」が来春に100ギガ化される意義と、その最たる例であるクラウド化やオープンサイエンスなどへの影響について論じました。基調講演は株式会社KADOKAWAの角川歴彦取締役会長に登壇いただきました。

今年の新たな取り組みは「NII研究100連発」＝写真。研究者10人が一人7分30秒の中で各10件、計100件の研究を発表しました。「デモ・ポスター展示」では研究者が自分たちの取り組みの一端を展示するとともに来場者からの質問にも答えました。若い世代へのアプローチにも力を入れ、小中学生を対象とした「情報学ワークショップ」を初めて開催。「女子高生のためのサイエンスLife Café」や都立戸山高校の生徒による「プレゼン実践！」も行いました。来年のオープンハウスは5月27日、28日に開催します。

6月11日、12日には「オープンサイエンスに向けた学術情報基盤」を主題に、教職員やセキュリティ担当者、学術向けITベンダらを対象とした「学術情報基盤オープンフォーラム2015」も開催。NIIは研究・教育活動に不可欠な学術情報基盤の整備・拡充を推進しており、大学などの学術界で期待が高まるオープンサイエンスを支援する上で学術情報基盤に求められているものは何かなどについて議論しました。

News 2 今年度の市民講座始まる ～第1回のテーマは「音声合成技術」

今年度の「市民講座」が開始。第1回は7月29日に開催しました。年間の主題は「情報学最前線」。生活と深く結びついた話題を通じて最新の研究結果を6回にわたって分かりやすく解説します。

今回は音声情報処理が専門の山岸順一准教授（コンテンツ科学研究系）が「おしゃべりなコンピュータ～音声合成技術の現在と未来～」と題し、1950年代から研究が始まった音声合成を学術的側面から解説。講義映像はNII公式サイトで11月中旬公開予定です。

8月20日には第2回を開催。「サクサク動くスパコンを作る～低遅延ネットワーク・トポロジの追究～」と題し藤原一毅特任准教授（アーキテクチャ科学研究系）が講師を務めました。今後の日程は裏表紙を、詳細や参加申し込みはNII公式サイトの市民講座のページ（http://www.nii.ac.jp/event/shimin/）で。

News 3 「ビッグデータ」めぐり意見交換 ～産官学連携塾

NIIの研究者と企業や自治体の関係者が出会い、意見交換できる場を提供する産業界向けの公開講座「第3回NII産官学連携塾」を7月22日に開催しました。

主題は「ビッグデータを始める前におさえておくこと」。前半はデータマイニングやアルゴリズム研究が専門の宇野毅明教授（情報学プリンシプル研究系）がビッグデータの現状とこれを扱う上の要点を解説し、インフラの発達で膨大な情報を入手しても何に利用してよいのか分からない例が多い中、データ解析技術を持つ者と現場担当者との共同作業がビジネスチャンスを見出すために重要であるなどと述べました。後半は若手の坂本一憲助教（アーキテクチャ科学研究系）と秋葉拓哉助教（情報学プリンシプル研究系）も加わって参加者同士が業務で抱えているビッグデータの状況・課題を共有し協議しました。

次回は10月13日に開催し、プライバシー侵害への対策を研究する越前功教授（コンテンツ科学研究系）が担当する予定です。詳細や参加方法はNII公式サイトでお知らせします。

Flash

▸ NII・国語研共同研究2015 公開研究会

7月24日開催。本年度設置した「データセット共同利用研究開発センター」が取り組む国立国語研究所との共同研究の一環。「言語資源構築における諸問題：権利問題を中心に」を主題に、両機関の取り組みの解説や参加者も交えた全体討論などを実施。

▸「ERATO感謝祭 Season II」

8月3日、4日開催。河原林健一教授（情報学プリンシプル研究系）が研究総括を務める「JST ERATO河原林巨大グラフプロジェクト」による研究成果発表会。発表の対象はトップ会議に今年採択されたものに限定し、2日間で計22件の発表や討論などを実施。

Topics

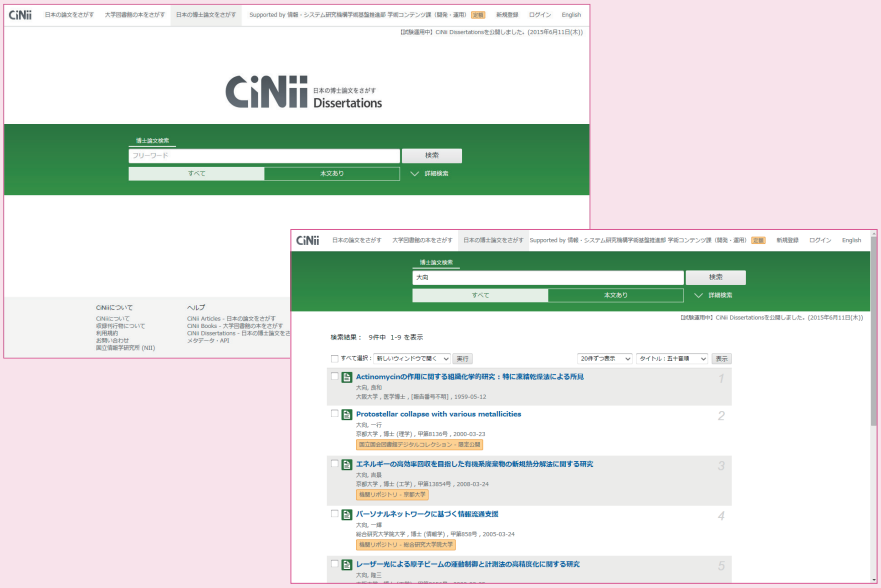
国内の博士論文を一元検索 CiNii Dissertations 試験運用開始

日本の博士論文を一元的、網羅的に検索でき、電子化されて公開されている博士論文の本文も表示できる国内唯一のサービス「CiNii Dissertations（サイニィ ディザテーションズ）」を開発し、6月から試験運用を開始しました。正式公開は本年10月の予定。「CiNii Dissertations」（http://ci.nii.ac.jp/d/）はどなたでも、利用可能です。

「CiNii Dissertations」で検索できる博士論文のデータは、国立国会図書館が所蔵している大正12年（1923年）9月以降の国内博士論文約57万件、国立国会図書館が平成3年（1991年）度から平成12年（2000年）度までに受け入れて電子化した「国立国会図書館デジタルコレクション」約13万件（電子化された本文データ含む）、及び、各大学の機関リポジトリの収録データ計約13万件です。

これまで博士論文を利用するには、上記の国立国会図書館や大学の蔵書検索をそれぞれ調べる必要がありました。「CiNii Dissertations」ではそれらを一括して網羅的に検索することが可能です。さらに、本文が電子化されて公開されている場合、数クリックで本文を閲覧することができます。「CiNii Dissertations」は博士論文の検索や本文の閲覧の利便性を格段に向上させる「ワンストップ」サービスを提供します。

「CiNii Dissertations」は、論文検索サービス「CiNii Articles（サイニィ アーティクルズ）」、大学図書館所蔵資料の検索サービス「CiNii Books（サイニィ ブックス）」に続き、NIIが提供する学術情報検索データベースサービス「CiNii（サイニィ）」の三番目の機能です。CiNiiのサービス開始から10年間で磨かれた共通の検索インターフェイスを採用しています。



博士論文は、最先端の研究成果が記述された学術的価値が高い資料として、国立国会図書館や大学図書館が学位授与機関を通じて収集してきました。平成25年（2013年）3月の学位規則改正で、博士論文は原則としてインターネットで公表されることになり、大学などの学位授与機関は自機関の研究成果を社会に発信するプラットフォームである学術機関リポジトリを通して博士論文を公開するようになっています。

▶ 国内刊行電子リソース共有サービス「ERDB-JP」を開発

NIIと国公私立大学図書館協力委員会で構成される「大学図書館と国立情報学研究所との連携・協力推進会議」は、大学や出版社等が一緒になって構築していく国内刊行電子リソースの共有サービス「ERDB-JP（Electronic Resources Database-JAPAN）」を開発し、6月からパートナー（データ作成機関）の募集を開始しました。

ERDB-JPで、日本国内で発行されている電子ジャーナルの情報を正確にデータベース化することによって、CiNiiや大学図書館の検索サービスから論文本文への適切なリンクを形成することができるようになります。

現在は大学図書館などをパートナーの対象としていますが、今後、出版社等にも拡大し、データ品質の一層の向上に取り組んでいきます。

SNS

「これ、いいね！」

Facebook、Twitterアカウントの最も注目を集めた記事（2015年5月～7月）

国立情報学研究所NII（公式） Facebook
www.facebook.com/jouhouken/

国内唯一 日本の博士論文を一元的、網羅的に検索できる新サービス「CiNii Dissertations」の試験運用を開始
（2015/06/24）

国立情報学研究所NII（公式） Twitter
@jouhouken

[NII NEWS] 国内唯一 日本の博士論文を一元的、網羅的に検索できる新サービス「CiNii Dissertations」の試験運用を開始
（2015/06/23）

つぶやくビット君 Twitter
@NII_Bit

教育誌の取材を受ける秋葉拓哉助教。国内外のプログラミング大会で次々に優秀な成績を収めた高校、大学時代の思い出を振り返りました。プログラミングコンテストにはもうでない？と聞かれて「戦場を変えました。今の戦場はアルゴリズムの研究です」
（2015/05/19）

Essay

金融と情報、そして仮想通貨

羽田昭裕 HADA Akihiro
［国立情報学研究所 客員教授／
日本ユニシス株式会社 総合技術研究所長］

金融業は装置産業といわれてきた。主な装置はICTである。当初から続くのが、バックシステムと呼ばれる、約定データを受け取り財務諸表を作成するシステムで、さらに市場や顧客とのチャネル、経営・リスク管理やマーケティング支援、それらを結ぶハブなどで「装置」を構成している。1970年代までは実体経済と金融市場が寄り添っていて、大切なことは決済や現金取引を遠隔的に即時、大量に扱うことであった。言い換えると、金融で扱われる情報は、売買や融資に伴う「私秘性」を持ち、実体経済という「重力」が作用していて、「装置」はそうした私秘性や重力を切り離した「データ」を電子的に処理するものだった。

その後、ロンドン証券取引所の改革から始まった実物資産の証券化や金融の価格、業務分野、商品設計、対外取引の自由化後、金融市場は実体経済の幾層倍もの規模になっている。証券化や自由化へのICTの貢献は、「装置」の地球規模のネットワーク化が実現して金融取引データのやりとりから空間や時間の制約を取り除いたことと、もともとは情報にまつわるリスクのヘッジを目的とした金融工学を高度化したことといわれる。データ処理の高速さと数理的な難解さが、擬似的な私秘性を生み出したともいえよう。

そして、金額と付随する条件だけという金融商品の性格と、リアルタイムで切れ目のない処理に対する要求から、金融取引は総じて自動化やセルフサービス化が進んできた。またICTは資産運用力や新商品開発力の強化を助け、堅牢さに加えて柔軟さを持つバックシステムは金融システムが提供する中核機能が分散し各金融機関から自立するのを促した。

すると、eビジネスの流儀で、ほかの業界と同様、周辺的な領域にICTを利用して新しいビジネスモデルを持ち込む新規参入者が現れる。最近では、そうした新規事業者が始めた金融サービスへの、従来の利用者の期待とは異なる期待に対応する、仮想通貨や個人の資産管理などのFinTechが注目されている。

これから先、周辺的な仮想通貨が中心的になるかもしれない。その場合、いろいろな時間と空間の制約が取り除かれ、過剰流動性を保ったままグローバルな金融取引の中心が仮想空間に移っていくのだろうか。むしろ、IoT（Internet of Things）やCPS（Cyber Physical System）を活用した新しい生産・物流の登場とともに擬似的な重力が生み出されて新しい実体経済となり、従来の投資対効果などとは異なる新たな企業経営の目標を持つというほうが、情報学のテーマも増えて面白そうだ。

今後の予定

10月13日｜第4回産官学連携塾「情報学×ものづくり×地方創生―Privacy Visorの研究開発から社会実装へ―」（コンテンツ科学研究系 越前功教授ほか）

10月21日｜第2回 SPARC Japan セミナー2015（オープンアクセス・サミット2015）「科学的研究プロセスと研究環境の新たなパラダイムに向けて―e-サイエンス，研究データ共有，そして研究データ基盤―」（主催）

10月22日｜市民講座 第3回「もっと手軽にCG制作～アルゴリズムとUIの合せ技～」（コンテンツ科学研究系 高山健志助教）

11月10日～12日｜第17回図書館総合展（後援・出展）

11月26日｜市民講座 第4回「私たちは何を知っているのか～暗黙の知識を紡ぐオントロジーとコーパス～」（社会共有知研究センター 川添愛特任准教授）

11月29日｜大学共同利用機関法人シンポジウム（出展）

12月2日～4日｜大学ICT推進協議会年次大会（出展）

表紙の言葉 レトロなレジスターとユーモラスなロボットが演じるシーンから、今後、機械＝テクノロジーがもたらしてくれるであろう夢のある『仮想通貨』の世界観を感じていただければ嬉しいです。

情報から知を紡ぎだす。
NII
国立情報学研究所ニュース［NII Today］第69号 平成27年9月
発行｜大学共同利用機関法人 情報・システム研究機構 国立情報学研究所
〒101-8430 東京都千代田区一ツ橋2丁目1番2号 学術総合センター
発行人｜喜連川 優　監修｜佐藤一郎
表紙画｜城谷俊也　編集｜田井中麻都佳
制作｜株式会社マツダオフィス／株式会社アテナ・ブレインズ
本誌についてのお問い合わせ｜総務部企画課 広報チーム
TEL｜03-4212-2164　FAX｜03-4212-2150　e-mail｜kouhou@nii.ac.jp

情報犬ビットくん（NII キャラクター）

http://www.nii.ac.jp/about/publication/today/