OPINION PAPER

NIRA オピニオンペーパー
no.26/2016.December

ブロックチェーンは社会をどう変えるか

ブロックチェーンは「帳簿(台帳)のイノベーション」といわれる。この技術を使うことで、モノやカネの取引記録を確実に保管し、信頼のおける取引を効率的かつ迅速に、国境を越えて実現することが可能となる。また、政府もデータベースにある国民の個人情報を、より安全に守ることができる。ブロックチェーンは仮想通貨の基礎技術にとどまらず、これまでのビジネスの仕組みや公共サービスを飛躍的に改善する、まさに新たな社会インフラとなり得るものである。

他方、ブロックチェーンは、未成熟な技術であり、解決しなければならない課題も多い。こうした技術を社会基盤に組み込んでいくには、利用者に信頼される技術であることが大前提となる。そのため、官民は次の4点を実践していくべきと考える。第1に、政府はデジタル社会の明確なビジョンを示し、官民がチームとなって課題を共有しながら研究開発を進めていくことである。第2に、政府は自らがブロックチェーン導入検討の実践者となり、小さい事業でトライアルを重ね、大きく育てていくアプローチをとっていくことである。第3に、政府は民間企業の技術開発の芽をつまないよう配慮し、イノベーションを進めやすい環境を整備することである。そして第4に、民間企業の側も、こうした技術で実現できる情報のシェアという特徴を生かした新たなビジネスを構築する際に、システムのオープン化・標準化を推進することである。企業経営者は、ビジネスモデルの見直しや技術とビジネスの双方を理解できる人材の育成など、自社の経営戦略を今一度真剣に検討する必要があろう。

翁　百合
Yuri Okina
NIRA総合研究開発機構理事／
日本総合研究所副理事長

概要　ブロックチェーンは社会をどう変えるか

第Ⅰ部　ブロックチェーンの特徴とメリット

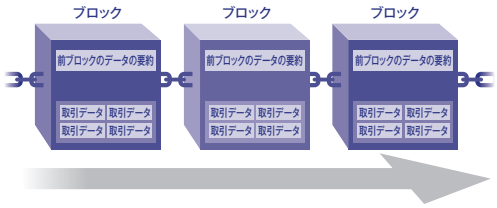
1　ブロックチェーンの仕組み

ブロックチェーンは、仮想通貨ビットコインやエストニアのデジタル政府で使われている技術である。「帳簿(台帳)のイノベーション」ともいわれ、従来の帳簿と異なる。以下特徴を見てみよう。

①　電子データで記録

一定量の取引情報などのデータを、ひとかたまりのブロックとして集約し、承認プロセスを経て確定したブロックをチェーン(鎖)状につなげて記録していく。

図　ブロックチェーンイメージ

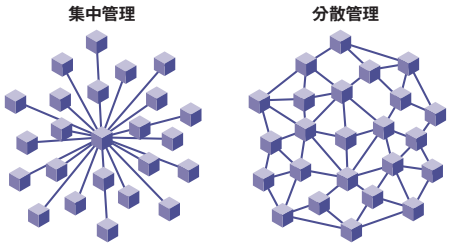


(本文P4図1より)

②　分散型台帳

ブロックチェーンの参加者全員がすべての取引情報(たとえば、仮想通貨の取引記録)を保管することで、同じ内容の台帳を各人が管理する。従来は、データを集中管理するのに対し、ブロックチェーンはネットワーク参加者が分散して管理をする。分散型台帳テクノロジーといわれるゆえんである。

図　集中管理と分散管理のイメージ



(本文P5図2より)

③　参加者間の合意

ブロックチェーンに参加する人がそれぞれに管理する台帳の内容は、常に同じものでなければならない。そのために参加者同士で、管理する台帳の内容が正しいものであると合意する必要がある。この合意の方法を「コンセンサス・アルゴリズム」と呼ぶ。

このようにデータを分散して共有し、参加者間の合意によって正当性を確かめていくというプロセスは、草の根的・民主主義的なコンセプトに基づいている。

2　ブロックチェーンの分類

ビットコインの場合、ネットワークに接続する環境さえあれば、世界中のどこにいても、誰もが利用することができる。このように参加者が限定されていないブロックチェーンをUnpermissioned型と呼ぶ。これに対し、参加者が限定され、許可された者しか参加することのできないブロックチェーンをPermissioned型と呼ぶ。

3　メリットは何か

こうした特徴を踏まえると、ブロックチェーンを使うメリットは、①システム障害に対して耐性が強い②データの改ざんが困難である③低コストである、といえる。さらに、ブロックチェーンにスマートコントラクト(当事者間の契約をブロックチェーン上に記述し、プログラム化して自動執行させる仕組み)を載せることにより、取引の一層の効率化や利便性の向上、ビジネスの広がりが期待できる。

第Ⅱ部　ブロックチェーンの実用例

1　仮想通貨

ビットコインをはじめとする仮想通貨は、ブロックチェーンを活用した電子的な通貨である。その種類は現在700を超え、時価総額は約140億ドルといわれる。投資資産としてだけでなく、決済や海外送金の手段としてすでに実生活で利用されている。多くの仮想通貨取引所も存在し、先進国各国も仮想通貨に対する法整備を行なったところだ。

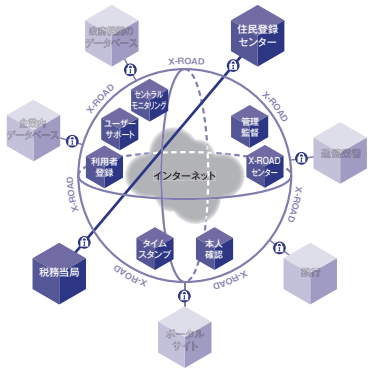
2　政府のプラットフォームに活用

エストニア政府は、X-Roadと呼ばれるプラットフォームによって、行政のデジタル化を実現し、各省庁が別個に持つデータベース同士をインターネット経由で接続し、相

執筆に当たり、研究会メンバーである岩下直行日本銀行決済機構局審議役FinTechセンター長、柳川範之NIRA総研理事／東京大学教授、加藤善大フューチャーアーキテクト株式会社テクノロジーイノベーショングループシニアスペシャリストから貴重なご意見、ご示唆をいただいた。研究会コーディネート及びAppendixは林祐司(NIRA総研)が担当した。なお、文中の誤りはすべて筆者の責任である。

互参照を可能としている。そしてひとたびデータの改ざんが起こると、それが過去のどの時点で、どの箇所で起こったものか、1秒間隔で検出することが可能となっている。これにはKSIと呼ばれる独自のブロックチェーン技術が使われている。ブロックチェーンが電子政府サービスの信頼性を高める役割を果たしているといえる。

図　X-Roadイメージ



（Appendix P12図より）

3　商取引や投資のインフラを提供

金融業界では、証券取引所のポスト・トレード処理（株などの取引が成立した後の処理のこと）や銀行のさまざまな新ビジネスに備えた実証実験も行なわれている。実用化段階にあるエストニアのファンダービーム社は、スタートアップ企業の投資資金をブロックチェーン上で募り、流動化するビジネスを展開している。

金融以外の分野でも、ロンドンのエバーレッジャー社は、ダイヤモンドの鑑定情報や取引履歴をブロックチェーンに保存し、安全かつ効率的なサプライチェーンの実現に向けてビジネスを拡大中である。

第Ⅲ部　ブロックチェーンを社会インフラとするために

1　ブロックチェーンの課題

ブロックチェーンはまだ新しい技術であり、多くの課題があるのも事実だ。現状では、大量のデータの処理に対応できなくなる、秘匿すべき個人情報の保護をどう担保するか、参加者間の合意形成の手法にさまざまな課題がある、スマートコントラクトで想定しない事態への対応が難しい、などの課題がある。

2　社会はどう変わるか

こうした課題はあるが、インターネットの活用が大前提となる情報化社会において、信頼性と効率性を高める仕組みの提供可能性を広げる意義は大きい。人々が安心して使える効率的なデジタル公共サービスが、世界各国で実現するかもしれない。特に社会インフラが十分に整備されていない発展途上国などにおいては、利用者の生活上の課題解決につながる。ビジネスの分野に関しても、サプライチェーンや物流にも大きなインパクトを与え、生産性を向上させるだろう。そして産業のアーキテクチャーを変えたり、新たなビジネスが次々と生まれる新たなプラットフォームとなるかもしれない。金融の分野においては、通貨としての活用のほか、貿易金融、証券取引、シンジケートローンなどの既存のオペレーションが改善し、これまでの金融ビジネスモデルを大きく変える可能性もある。

3　政策提言

ブロックチェーンを社会基盤に組み込むためには、利用者が技術導入のメリットを感じて信頼し、「分散」「合意」「共有」といったコンセプトを理解することが必要だ。またブロックチェーンは、他の技術と結びついてより高度な情報化社会を実現するテクノロジーの1つであるという認識を持つことが重要である。こうした認識に立ち、官民は次の4点を実践していくべきと考える。

第1に、政府はビジョンを示し、官民で課題共有して、研究開発を推進すべきということだ。デジタル社会のビジョンを明確に掲げ、デジタル化推進を図ることが求められる。また、政府が積極的に課題をオープンにし、官民がチームとなって課題を共有しながら研究開発を進めていくべきである。

第2に、政府は自らがブロックチェーン導入検討の実践者となるべきということだ。その際、小さい事業でトライアルを重ね、大きく育てていくアプローチをとっていくことが重要である。

第3に、政府は民間企業の技術開発の芽をつまないように配慮し、イノベーションを支援すべきということだ。英国の「レギュラトリー・サンドボックス」などを参考に、民間企業がイノベーションに挑戦しやすい環境を整えることも必要だ。また、金融面では、イノベーションを進めやすい規制手法を考え、整備していくべきである。

第4に、民間企業の側も、こうした技術で実現できる情報のシェアという特徴を生かした新たなビジネスの構築を模索すべく、システムのオープン化と標準化を推進することである。企業経営者は、ビジネスモデルの見直しや、技術とビジネスの双方を理解できる人材の育成など、自社の経営戦略を今一度真剣に検討する必要があろう。

第Ⅰ部　ブロックチェーンの特徴とメリット

はじめに

―日本国内でも使えるお店が少しずつ増えてきた仮想通貨ビットコイン。この通貨を使えば、銀行を介さなくても、個人と個人との間で直接送金ができる。国境や為替レートを気にする必要もない。

―行政に関わるあらゆる情報が電子的に管理されるデジタル政府を実現した北欧の小国エストニア。国民IDを活用してほとんどの行政手続きがオンラインで行なえる。

これらには、実はブロックチェーンと呼ばれる画期的な技術が用いられている。ブロックチェーンは「帳簿のイノベーション」ともいわれる。これまで紙で記録していた取引の履歴情報などがすべて電子的に保管されるようになり、それを関係者が合意の上、分散して保有することが可能となった。その技術は仮想通貨だけにとどまらない。世界のさまざまな企業、金融機関、そして政府が、この技術を使った多様なサービスの実証実験を行なっているのも、新たなビジネスやデジタルガバメントの可能性が広がると考えているからに他ならない。

たとえば、市場では、電子的に契約を記述した取引情報を分散して持ち合うことにより、付加価値の高いサービスを低コストで提供できる可能性が広がる。また行政においては、公共サービスの手続きがネット上で瞬時に完結することで、私たちの生活が飛躍的に便利になるかもしれない。現在の予想をはるかに超えた、これまでのビジネスの仕組みを大きく変えていく社会インフラとして機能することが大いに期待できる。

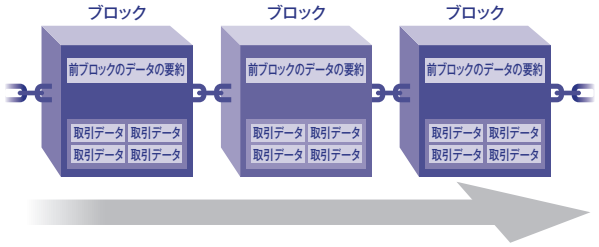
他方、ブロックチェーンの仕組みは複雑で、慎重論が多く聞かれるのも事実である。そこで本稿では、第Ⅰ部で、こうした現状を踏まえ、ブロックチェーンの仕組みをわかりやすく説明し、第Ⅱ部では、実際の活用例を見ていくとともに、第Ⅲ部では、ブロックチェーンが今後どのように社会を変えていくのか、その発展を実現するために何をすべきかについて論じる。

1　ブロックチェーンの仕組み －重要なコンセプトとフィロソフィー－

ブロックチェーンという呼び名は、カネやモノの取引の履歴情報を電子的に記録しながら、そのデータをブロックとして集約、さらに連鎖（チェーン）して組成することに由来している（図1）。

ブロックチェーンの利用者は、パソコンや携帯端末などを使い、ブロックチェーンネットワークにアクセスする。幅広く活用されているブロックチェーンネットワークの多くにはインターネットが使われている。ブロックチェーンを一言でいうと「取引の履歴情報をブロックチェーンネットワークに参加する全員が相互に分散して保管維持し、参加者がお互い合意をすることで、そのデータの正当性を保証する分散型台帳（distributed ledger）」となる。

図1●　ブロックチェーンイメージ



以下、もう少し詳しく説明してみたい。

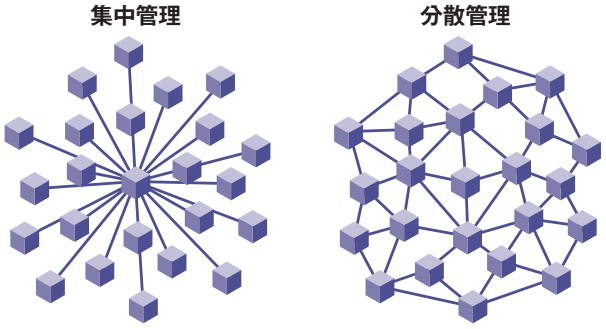
分散型台帳：取引のデータを複数の参加者が分散して管理する

ブロックチェーンは、今までの帳簿または台帳の発想やコンセプトと何が異なるのだろうか？かつての台帳は、紙に取引内容を書き込むことによって管理されていた。近年では、紙に代わり、情報が電子化（デジタル化）されているものの、特定の組織や人が集中管理を行なうという構造は同じである。たとえば、証券取引所などの中央機関が1カ所で管理する、いわば中央集権的な管理だ。こうした管理の問題点としては、例に挙げた取引所の場合、取引履歴データなどを記帳するためのシステムなどにコストや時間がかかり非効率なだけではなく、サイバー攻撃により情報が失われるというリスクがある。このため、システムダウ

ンを想定したデータバックアップやBCP(ビジネス・コンティンジェンシー・プラン：事業継続計画)対策に多大なコストをかけているのが現状である。

これに対して、ブロックチェーンの発想は、取引履歴を記録するデータベースをネットワーク参加者で分散して保有し、管理を行なうというものだ(図2)。複数のネットワーク上の参加者のコンピューター同士をPeer-to-Peerで直接接続し、モノやカネなどの取引情報を互いにやりとりして確認し、その履歴情報を共有し続ける(以下では、各コンピューターをブロックチェーンの参加者という意味で、ノードという)[1]。

図2● 集中管理と分散管理のイメージ



参加者間の合意：取引のデータの整合性について参加者はどう合意するのか

カネやモノの取引データの整合性について、ネットワーク参加者間でどのように合意するのか？ブロックチェーンで使われている、合意を得るためのメカニズムをコンセンサス・アルゴリズム(合意形成のための計算方法)というが、合意にはさまざまな手法が存在する。

仮想通貨ビットコインの場合、マイナー(採掘者)と呼ばれる人々が、自発的に電気代を大量に消費してコンピューターに計算をさせて答えを出す「マイニング(採掘)」競争をする[2]。その計算競争の勝利者は、その答えとともに、ビットコインによる送金データの塊をブロックとして承認し、参加者へ伝播(でんぱ)する。こうした競争によって承認された取引であることを証明する仕組みを、プルーフ・オブ・ワーク(PoW、Proof of Work)という。承認された内容は、それぞれのノードに記録として保存されていく。

こうした承認行為には、マイナーが正当な承認を行なうと手数料を得られることで計算競争への参加意欲を持つと同時に、その競争下では不正を働くためのコストが膨大なものとなるという経済インセンティブを内包させることで不正も抑止している。ビットコインタイプのブロックチェーンは、この参加者間の競争的なチェックという革新的なメカニズムによって、悪意のある参加者が存在し得る環境下においても不正を許さない仮想通貨を生み出した。

そして、承認されたすべての記録が、台帳として整合性を保った状態で存在し共有されている。整合性について最終的に合意する具体的な仕組みはこうだ。マイニング競争の勝利者が承認したブロックを受信した各ノードではこれを検証し、不整合がなければ承認されたものとして取り込む。ただし不整合がある場合にはこれをはじく。まれに(複数のマイナーにより)答えがほぼ同時にみつかり、各ノードが複数のブロックを受信することがある。こうした場合にはチェーンが分岐して、どちらも正しく承認された正当なチェーンといえる状況となってしまう。だがビットコインでは「最も長く連なったチェーンを正しいチェーンとみなす」というルールを決めてあるため、しばらく待てば、最長のチェーンが適正であると判断することができる[3]。分岐が起きるといわば二重支払いといえる状況になるが、結果として長いチェーンを採用すれば、一方の支払いのみを採用する判断が可能だ。

ブロックチェーンネットワーク上での取引：国境を越えてカネ、モノの取引を展開

ブロックチェーンがこのように透明で、かつフラットなネットワークの仕組みを基盤としているのは、その根底に草の根的・民主主義的なコンセプトがあるからだ。そもそもブロックチェーンはビットコインを起源とした技術であり、中央集権的な組織や国に依存しない取引の実現をめざして生まれたものなのである。

ブロックチェーンの特徴の1つに、参加する全員が安全かつ平等に、分散的に情報を共有化しながら「つながり」を実現でき、グローバルにネットワーク展開できるインフラとして機能する、というものがある。誰でも参加できるタイプのブロックチェーン(詳細は「2. ブロックチェーンの分類」を参照)の場合、ノードである構成員は、カネ、モノの取引を、国境を越えて自由に展開でき、世界中どこにいても参加することができる。さらにノードが増え、ブロックチェーンのネットワークが拡大すればするほど、影響力が指数関数的に拡大していくというネットワーク効果を発揮することが可能となる。

1 Peer-to-Peerとは、中央サーバーを用意せず、個々の端末(Peer)がお互いに接続しあうことで成立するネットワークのこと。
2 マイニングビジネスに投資をしている人は世界各国におり、手がけている会社は多いが、10社程度がその大半を占めている。マイニング作業の多くは、電気代が安いため中国で行なわれている。
3 1承認あたり平均10分かかるが、確定するためには、確率的に6回の承認(6ブロック、約60分)以上待つことが求められている。

2　ブロックチェーンの分類 －参加者を限定するか、しないか－

ブロックチェーンにはさまざまなタイプがあり、それぞれの活用目的に合ったタイプが使われている。分類の基準の1つは、取引の確認やブロックの生成といった行為に誰でも自由に参加できるか(Unpermissioned)、それとも関与する参加者が管理者によって許可された者に限定されているか(Permissioned)、ということである(表1)。前者をパブリック型ともいう。また、後者のうち取引の確認やブロックの生成にかかわる管理者が単独の場合はプライベート型、複数の場合はコンソーシアム型と分類される。

表1●　ブロックチェーンの分類

	Permissioned 参加するために管理者から許可されることが必要	Unpermissioned 管理者は不在でだれでも参加可能
ノード参加者	特定の参加者	不特定の参加者
類型	プライベート型 コンソーシアム型	パブリック型
コンセンサス・アルゴリズム	PBFT[3](プラクティカル・ビザンチン・フォルト・トルランス)など	PoW(プルーフ・オブ・ワーク) PoS[1](プルーフ・オブ・ステーク) PoI[2](プルーフ・オブ・インポータンス)など
使用例	NASDAQ (一部の未公開株取引) JPX(日本取引所グループ) (実証実験)	ビットコイン、イーサリアム エバーレッジャー社 ファンダービーム社

注1：PoS(プルーフ・オブ・ステーク)は、PoWの代替システムにあたるもので、コインを持っている割合(Stake)によってブロック承認の権利を決める方法のこと。
注2：PoI(プルーフ・オブ・インポータンス)は、ノードごとの取引額や残高を指標とした分析により、個別のノードの重要性を計算し、より重要なノードに承認の優先権を与える方法のこと。
注3：PBFT(プラクティカル・ビザンチン・フォルト・トルランス)は、参加者のうち約3分の2の合意により書き込みが行なわれる仕組みで、高速な合意形成が可能。なお、PermissionedでもPoW、PoS、PoIなどを使うこともある。

誰でも参加できるUnpermissioned型ブロックチェーン

まず、当該ブロックチェーンへの参加者が特定されていない、不特定の参加者(Unpermissioned)によるタイプの典型例は、仮想通貨ビットコインである。Unpermissioned型ブロックチェーンには管理者がいない。このタイプのブロックチェーンは、参加者が増えれば増えるほどネットワークが保持するデータは改ざんされにくくなる。

管理者の許可が必要なPermissioned型

もう1つのタイプは特定の参加者(Permissioned)だけがブロックチェーンに参加できるものである。このタイプは、ブロックチェーン管理者の信頼(トラスト)を得られた人々(または企業や機関)しか、ブロックチェーンに参加できない。Permissioned型は、ネットワークへの参加を許可する管理者がいるため、中央集権的でありそもそもブロックチェーンのめざす姿と呼べるのかという議論もあるが、この場合でも参加者間でのデータベースの分散保有は行なわれている。こうしたブロックチェーンは、PoWよりスピーディーで効率的なコンセンサス・アルゴリズムで取引を承認することが多い。すでに信頼(トラスト)された参加者間での情報共有となるので、安全性がある程度担保され、スピードと効率性を求めることができるといえる。

3　メリットは何か

PermissionedであれUnpermissionedであれ、両者に共通している大きな特徴は、従来1つの組織、機関が、多大なコストをかけて一元管理していた台帳を、分散型ネットワークで参加者が相互に持ち合い、Peer-to-Peerで取引の正当性を証明しながら取引をまとめ、チェーン(連鎖)の情報として保存していくことであると捉えられる。この特徴から得られる、ブロックチェーンを使うメリットについて、以下見ていこう。

①　障害に強い

まず、分散型ネットワークシステムの特徴を利用した、高い「可用性」が挙げられる。すなわち、一部のノードがダウンしても、他のノードが情報を共有しているので、問題が大きくなりにくい。このため、ダウンタイムなく取引が継続できる。金融や政府部門では、現行のシステムでも高い可用性を実現している場合がほとんどだが、そのために高価なハードウエアやバックアップ施設、対応のための多大な労力が必要になる。安価なハードウエアをネットワークでつないで高い可用性を比較的容易に実現したところに、ブロックチェーンの特筆すべき優位性がある。

なお、集中型のシステムでは容易だが、大規模な分散型のシステムでは、すべてのノードが同時に同じデータでなければならないという一貫性の確立が難しいという側面がある。これに対しビットコイン・ブロックチェーンの場合は、承認回数を重ねることで整合性・一貫性が高くなるというアプローチをとっている。このため、厳密には100%のファイナリティを確保できないが、前述の通り一般的には6回の承認回数を重ねることで「確定とみなす」という現実解を提供している。

② データの改ざんが難しい

ブロックチェーンのブロックは、連鎖するデータ構造となっており、1つ前のブロックの情報を要約しながらつながり(前掲図1参照)、共有される。そのため、過去の取引を改ざんしようとすると、それ以降連なっているすべての連鎖するブロックの内容を書き換えねばならず、また全ノードのブロック内容を書き換えなければならないため、データの改ざんが非常に困難といえる。このため、通貨として利用した場合に、不正取引を防止する機能を安価に構築できる。ビットコインの場合には、前述の通り二重払いを防止するため、長いチェーンを優先するルールなど、工夫がされている。

③ 仲介者を省いて低コストに

たとえばインターネット上に構築したブロックチェーンで国際送金を行なう仕組みを作れば、現行システムのように多くの金融機関や仲介者を経由しないで済む。その分取引の手数料が不要となり、安価かつ迅速になる。また全ノードがデータを持つため透明性が向上し、中央集権的な仕組みにおいて必要とされる監査などの仕組み(ガバナンス)の必要性が低下し、こうした管理コストの低減にもつながる。

複雑な契約を自動化できるスマートコントラクト

これら①～③のメリットを生かし、さらにブロックチェーンによる取引内容にスマートコントラクトを載せれば、取引に付随する複雑な処理を自動的に処理できるようになる。スマートコントラクトとは、当事者間の私的契約をプログラム化しブロックチェーン上に記述、これを自動的に執行する仕組みを意味する。取引に伴う複雑な処理についても自動で契約締結、保存、取引を完結できるということだ。スマートコントラクトにより、従来取引に付随していた膨大な手作業が不要となる。

またスマートコントラクトとIoT(インターネット・オブ・シングス、すべてのモノがインターネットで接続されてネットワーク化し、自動操作、制御などさまざまなビジネスが可能となること)がつながることで、たとえばレンタカーを借りる時、車のドアの前に立ち、スマートフォンで代金を支払った瞬間、スマートコントラクトが契約を自動執行し車のドアが開く、といったことも可能になるかもしれない。

ネットワーク上でデータベースがオープンに共有されることで、取引の信頼性を担保し効率化を図ろうとするブロックチェーンに、スマートコントラクトを載せることにより、取引をさらに効率化できる可能性が高まる。また、個人、企業、国がオープンに結びつき、カネ、モノ、サービスなどの流れが統合していき、一層利便性が高まっていく可能性がある。

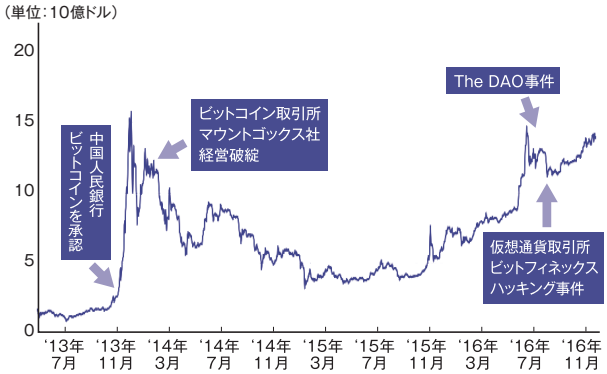
第Ⅱ部　ブロックチェーンの実用例

日本で金融取引をはじめさまざまな領域への適用をめざし、実証実験が行なわれているブロックチェーン。だが世界に目を向けると、すでにビジネスとしてスタートしているものも存在している。ここではいくつかの実用例を紹介する。

1　仮想通貨の時価総額は増加

仮想通貨の種類はすでに700種類を超えるといわれ、時価総額の合計は約140億ドル(2016年12月時点)まで増加している。その中で85%と圧倒的なシェアを占めているのはビットコインである。ビットコインを含む仮想通貨では、「価値情報の移転記録」としてブロックチェーンが使われている。仮想通貨は手数料も安く、国内の決済や海外送金の手段として使われているが、主に値上がりを期待した投資用の資産として保有されている。日本においても多くの仮想通貨取引所が存在しており、2016年、他の先進国同様、マネーロンダリングへの対応や利用者保護のための法制整備が行なわれたところである。仮想通貨はフィンテックベンチャー企業だけでなく、メガバンクをはじめとする多くの金融機関からもさまざまな角度から関心を持たれている。

図3●　仮想通貨時価総額の推移



注:The DAO事件(6月)については後述。ビットフィネックス(取引所大手、香港)事件では、6千万ドル余りものハッキングが発覚した(8月)。
(出所)ホームページ"Coin market cap"から入手したデータに加筆修正
https://coinmarketcap.com/charts/

2　政府のプラットフォームに活用

第Ⅰ部で述べたように、ブロックチェーンは帳簿技術のイノベーションであり、事実証明としてのデータ履歴(個人の健康情報、不動産などの財産の所有権、納税など)の「台帳」として、より安全にデータを保管、利用できるというメリットがある。この点を生かし、政府などの公共部門において活用が始まっている。具体的には、エストニア電子政府の中でブロックチェーン技術が用いられている[4]。

実用例1　ガードタイム社によるエストニア電子政府への貢献(詳細は、Appendix参照)

エストニアは、国民の個人IDを活用し、住民情報や、カルテ、処方箋などの健康情報の管理、納税、投票など、さまざまな行政サービスを電子化している。国民にとって利便性が高く、コストが小さな電子政府を実現している。また、非居住者に対しても永住者同様の安全なデジタルIDをエストニアが発行し、公証サービスなどが受けられ、会社も設立できるようになっている(e-Residency)。既存のレガシーシステム同士を直接結ぶ「X-Road」という相互連携ネットワークがプラットフォームとなっており、政府内の情報連携の鍵となっている。「X-Road」とは、各省庁が個別に持つデータベース同士を、インターネットを介してつなげて、相互参照を可能とするデータ交換基盤を示す。データは暗号化され、署名を付与して送信される。政府のデータベースは、銀行や通信会社にも接続が許されている。

この「X-Road」に独自技術を提供しているのが、2006年にエストニアでスタートしたガードタイム社である。同社のブロックチェーン技術であるKSI(Keyless Signature Infrastructure)は、大規模に分散されたデータの改ざんをリアルタイムに検知できる。実は内部犯行を含めると、データ改ざんの完全防止は難しいという現実がある。そのため、改ざんに気づくことができ、改ざんされる前の状態に戻すことを可能とす

4　厳密には、モノやカネの取引が行われていないので、本論稿で記載しているブロックチェーンの特徴とはやや異なる印象があるが、ガードタイム社のKSIは、過去からのデータの要約をチェーンで結び、改ざんをすぐに検知できる仕組みとなっており、広くブロックチェーン技術であると捉えられている。

ることで安全性・信頼感を供与している。安全性に対する国民からの信頼は、納税や健康情報に基づく新たな行政サービスの展開が次々と可能となっている理由の1つといえる。

現在、世界では、エストニアの取り組みに続き、不動産の情報に関する情報の登録、公文書のアーカイブなども含めて、電子政府化の取り組みの中でブロックチェーンを使う試みや、実証実験がさまざまな国で行なわれている。

3　商取引や投資のインフラを提供

仮想通貨をさまざまな資産に置き換え、その資産取引をマッチングし、金融取引のみならず、商流や移転記録の管理をすることによって、従来にはないサービスを創出する企業も出てきている。前述のスマートコントラクトを載せることによって、大きな利用の可能性の広がりが期待されている。

まず金融面では、米国のNASDAQが一部の未公開株式の取引用にパイロットシステムを稼働させたほか、スタートアップ企業の投資資金を募りこれを流動化するビジネス(実用例2　エストニアのファンダービーム社)や、シェアリングサービスに付随するリスクに対応する保険を提供するビジネス(英国セーフシェアー社)などもスタートしている。さらに、証券分野のポスト・トレード処理(株などの取引が成立した後の事後処理のこと)の効率化などに向けた実証実験が世界各地で行なわれている(表2)。

実用例2　ファンダービーム社によるスタートアップ企業の投資資金の応募と流動化

エストニアのファンダービーム社は、2013年にスタートしたベンチャー企業である。同社は、スタートアップ企業に対する投資を募る仕組みをブロックチェーン上で提供している。投資額に応じて独自のトークン(ネットワーク上で使われる一種の仮想通貨のようなもの)を発行し、セカンダリー・マーケット(流通市場)でトークンを売買することも可能、つまり、当該スタートアップ企業が成長し資金を返せる段階(exit)を待たずに、投資資金を流動化して、投資家の間で売買ができる仕組みを実現している。このトークンは、パブリック型ブロックチェーンとして発行されている。

また同社は、投資に必要な情報を提供するためのデータバンクとしての役割も果たしている。世界中の15万社を超えるスタートアップ企業のデータ、そしてそれらに出資をする2万を超える投資家の情報などを自動収集し提供(投資家の詳細情報はブロックチェーン外で管理し同社がプライバシー管理を行なっている)。グローバルにビジネスを展開しており、日本の投資家も同社を介して、スタートアップ企業への投資を行なっている。

また、ブロックチェーンは、効率の高いサプライチェーンの実現やシェアリングサービスの安全な提供など、さまざまな目的を持った多様な企業から関心を持たれている。たとえば、貿易取引については、バークレイズ銀行とイスラエルのスタートアップ企業ウェーブ社の取り組みによって貿易取引業務の時間とコストを著しく削減することに成功するなど、貿易関連企業の関心が高まっている(表2)。また、ダイヤモンドや絵画といった、動産取引にブロックチェーンが用いられている事例もあり、鑑定情報や取引履歴を安全に保存することが、その財の価値を引き上げることにつながり、革新的なビジネスとなっている(実用例3　英国のエバーレッジャー社)。

実用例3　エバーレッジャー社によるダイヤモンド取引

英国のエバーレッジャー社は2015年にスタートしたベンチャー企業である。ダイヤモンドを鉱山から消費者の手に渡るまで追跡し、ダイヤモンドの鑑定情報や取引履歴、移転証明などをブロックチェーン上で記録・管理する。現在管理しているダイヤモンドの数は約98万個。外部にAPI(アプリケーション・プログラミング・インターフェースの略で、あるシステム・サービスを利用するための手順やデータ形式などを定めた規約のこと)を公開することで警察や保険会社もデータを参照可能である。このデータにより、保険金詐欺なども防げることから、ダイヤモンドの価値自体を引き上げ、後述する社会的な問題を解決するエコシステムを作り上げることに成功している。相互確認が必要な鑑定書などの情報はパブリックブロックチェーン、機密情報はプライベートブロックチェーンを活用し、スマートコントラクトによって取引や売買が容易となっている。「記録の改ざん不可」「データを分散し

て安全に管理」「スピーディーな情報共有」といったブロックチェーンのメリットは、ダイヤモンドの管理に非常にマッチしているといえる。古くからダイヤモンドの取引市場では盗難や鑑定書の偽造、また宝石にかける保険金の詐欺などが頻発、またマネーロンダリングやテロ資金の温床ともいわれている。同社のビジネスモデルは、こうした業界の不健全性、社会的な問題をブロックチェーンという新技術で解決したい、という発想から生まれたと、創業者であるMs. Kempは語っている。

冒頭述べたように、日本においては金融取引の分野を中心に積極的に実証実験が行なわれている。たとえば、JPXにおけるポスト・トレード処理の事例、また住信SBIネット銀行の入出金取引・振り込み処理の事例などが挙げられる。

海外に目を向けると、実用例として具体的に紹介した2社だけでなく、英国セーフシェアー社や米国NASDAQなど、すでに実験の域を越えビジネスとしてスタートしている事例も見られるほか、さまざまな分野における実証実験が、世界各地で現在一斉に進んでいる状況といえる。

表2● ブロックチェーンを活用した実施例および実証実験

（2016年12月時点）

組織名称	種別	取り組み内容
セーフシェアー社（英国）	スタートアップ企業	2015年にスタートしたベンチャー企業。車や部屋の貸与といったシェアリングビジネスのプラットフォーマーに対して保険を提供する代理業を行う。シェアリングサービスの利用者は不特定多数に及ぶが、セーフシェアー社はこうした転々と移り変わる取引情報などをブロックチェーンで管理し、保険会社へ提供している。
バークレイズ銀行（英国）	銀行	英国4大銀行の一角。クロスボーダーの金融連合R3CEVで共同開発したCordaを用い、銀行間スワップ取引の契約書をブロックチェーン上で伝達するスマートコントラクトのデモを行なう。また9月には同行初のブロックチェーンベースの貿易取引を成功させた。
ロンドン証券取引所（英国）	証券取引所	CME（シカゴマーカンタイル取引所）などと共同でPost Trade Distributed Ledger Working Groupを立ち上げ、ブロックチェーンを使った証券ポスト･トレードの研究を進める。
JPX（日本取引所グループ）	証券取引所	日本IBMと野村総研をパートナーとして、それぞれ異なる実装手法により、株式市場におけるポスト･トレード業務にDLT（Distributed Ledger Technology）を用いる実証実験を行なった。証券会社や保管振替機構など6組織が参加し、証券発行や取引照合、資金決済など7項目にわたる検証により可能性と課題を整理した。
住信SBIネット銀行	銀行	国内のネット専業銀行。預金の入出金や振込、残高管理などの銀行勘定系取引について実証実験を行なった。ブロックチェーンを活用した不動産取引における担保権の設定抹消や、売買代金決済についても研究を開始。
NASDAQ（米国）	証券取引所	米国の新興企業向け株式市場。ブロックチェーン技術スタートアップである米チェイン社と提携して一部の未公開株式取引システムNasdaq Linqを 自社開発、株式の発行や売買を行なうパイロットシステムを稼働 。また太陽光エネルギーを証券化した電力証書をブロックチェーン上で流通させる取り組みも公表した。
DTCC（米国）	証券保管振替機関	米証券保管振替機構の持株会社。Linux FoundationやIBM、インテルなどが協働し立ち上げたHyperledger Projectの参加メンバー。OTCデリバティブ（店頭デリバティブ）、CDS（クレジットデフォルトスワップ）取引やレポ取引などブロックチェーンを活用したさまざまな実証実験を行っている。

（出所）ヒアリング等により作成

（Appendix）

エストニア電子政府の取り組みについて

1　IT先進国エストニア

世界トップレベルの電子国家

北欧バルト諸国の1つであるエストニア共和国は、人口約131万人、国土面積4.5万平方キロメートル（日本の約9分の1）の小国だが、デジタル先進国として世界中の注目を集めている。エストニアは、1991年に旧ソ連から独立を回復するまでの約50年間、長くロシアの支配下にあり、常に「国家がいつなくなってもおかしくない」という脅威にさらされていた。そのため、国の根幹をなす国民の情報を電子的に持つことにより、たとえ国土がなくなったとしてもサイバー上で国家を維持することを可能とすべく、電子国家という発想を持つに至ったともいわれている。

独立回復から25年がたち、エストニアはデジタル先進国と呼ばれる“D5（エストニア、英国、イスラエル、ニュージーランド、韓国の5カ国）”の一角となるまでに至った。European Commissionが公表するEUデジタル経済・社会ランキング1位と、その躍進はめざましい。

名だたるスタートアップ企業を輩出

エストニアにはスタートアップ企業が多く存在する。代表的な企業としては、インターネット電話サービスのスカイプ、海外送金サービスのトランスファーワイズ、モバイルペイメントアプリのポコペイなどがある。人口1人当たりのスタートアップ企業数は欧州一だ。こうした背景には、個社の斬新な発想や優れた技術力があったのはもちろんのことだが、エストニア政府自身が電子政府化を強力に推進していったということも大きな要因といえるだろう。

2　エストニア電子政府の具体的取り組み

国土面積に比して人口が少ないエストニアでは、公共サービスを行き渡らせるためにITの活用は必須だったといえる。独立以来進めてきたIT化の取り組みの中でも、特に中核となるものについて紹介する。

国民ID番号活用による手続き効率化、低コスト化

エストニアがデジタル社会普及の鍵として最も重視したのは国民のID、つまり公的機関による国民の存在の証明であった。政府は国民へID番号を付与し、2002年からIDカードの発行を開始。15歳以上のすべての国民にIDカードの所持を義務づけた（罰則規定はなし）。全人口の96％を超える人がアクティブなIDカードを持っている。

カードにはICチップが埋め込まれており、公的個人認証用と、電子署名用の2つの鍵が埋め込まれている。これらの技術要素となっている公開鍵暗号技術は、ブロックチェーンでも利用者本人の特定や、不正使用の防止などに使われている。

このIDカードによって、行政に関わるすべての情報はデジタルで管理される。現在3,000以上のe-サービスを提供しており、結婚、離婚、不動産売買以外の行政手続きはすべてオンラインで行なうことができ、ほぼすべてのサービスがモバイル対応している。またIDの付与と同時に、政府は固有のメールアドレスを国民に対し発行し、行政からの通知を送ることが可能である。いわばダイレクトに個人に届く電子版官報だ。エストニア政府によると、こうした行政のデジタル化によって、手続きの99％がオンライン対応になり大幅な効率化が実現したといわれている。その中の具体的効果を取り上げると以下の通りである。

—電子署名の導入により1人当たり年間1週間分の労働時間削減（GDP2％に相当）
—国会の閣議時間が5時間から30分に短縮
—法人登記の完了まで最短18分
—税金の電子納付率98％、確定申告完了まで最短3分
—e-Healthの導入により病院の待ち時間1/3に短縮、処方箋の99％が電子化
—i-Voting（電子投票）の導入でコストが1/2.5へ減少
—e-Police導入により検挙率50倍

エストニア政府のIT関連年間予算はわずか5,000万ユーロ（＝約60億円）と、他国に比べて圧倒的に少ない（フィンランド20億ユーロ、英国200億ユーロ）。エストニアはオープンソースを活用しながらこうした電子化を実現したといわれており、日本の大手企業一社のIT関連費用より少ない予算で運用されているのも、驚くべき点である。

表　エストニアのIT戦略の歩み

2000	●税金のネット申請を開始 ●モバイルバーキング開始
2001	●電子住民登録開始 ●X-Road運用開始
2002	●e-School（スクールマネジメントシステム）稼働 ●電子署名導入　●国民IDカード発行
2003	●IDバスチケット発行 ●電子不動産登記開始
2005	●電子投票開始
2007	●モバイルID発行開始　●X-RoadにKSIを導入 ●e-Policeシステム稼働
2008	●e-Healthシステム稼働
2010	●電子処方箋の導入
2011	●スマートグリッド運用開始
2012	●電気自動車充電ネットワーク稼働
2013	●X-Road Europe構想
2014	●e-Residency開始 ●Data Embassy構想

（出所）エストニア政府資料に加筆修正

省庁間のデータベースを相互連携させるX-Road

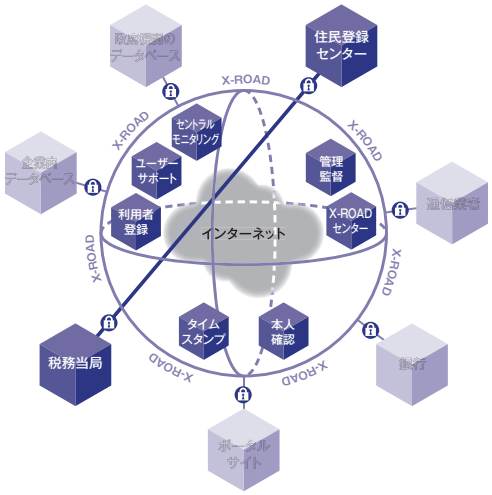
エストニア政府が低予算でこうした電子化を実現した背景には、各省庁のデータベースを連携させる、X-Roadと呼ばれる仕組みがある。これは、各省庁が別個に持つ住民登録情報やヘルスケアの情報などのデータベース同士を、それぞれPeer-to-Peerでつなげ、情報の相互参照を可能とするデータ交換基盤を指す。ブロックチェーンの分散管理というコンセプトに通じる技術を、データベースの中央集権的な一元管理が主流であった2001年から稼働を開始しているという点で、この取り組みは先進的だったといえる。

X-Roadの通信手段は、インターネットを利用している。X-Roadへの接続は、すべてセキュリティーサーバー(下図の各ノードにある鍵のマーク)を経由して行なわれ、データは暗号化され、署名を付与して送信、全ログが記録される。またX-Road全体のオペレーションを統括するX-Roadセンターのセントラルサーバーでは、ログの監視や利用者の本人確認などをつかさどっている。実際のデータのやりとりはそれぞれのデータベース同士が通信を行なっており(同図の太いライン)セントラルサーバーを経由していない。

各省庁が、それぞれ異なる仕様のデータベースで管理している情報もインタラクティブに交換でき、また膨大なコストをかけレガシーシステムを刷新せずとも、それを生かしたままでのデータ連携を可能とする。またX-Roadは銀行や通信会社など、民間企業も接続を許されている。たとえば銀行ではインターネットバンキングと連携させ、国民IDによる個人認証と合わせ、政府のデータベースに個人情報を確認する手段として活用されている。

X-Roadのシステムを考案・開発したのはエストニアのIT企業であるサイバネティカ社である。そして、ログの整合性を常時監視しセキュリティー面を担保するために後述するガードタイム社のブロックチェーン技術であるKSI(Keyless Signature Infrastructure)が採用されている。民間の技術を活用し、セキュリティーを確保しつつ民間にもオープンにした政府基幹システムとして注目される。

図　X-Roadイメージ



(出所)エストニア政府資料に加筆修正

政府が保管する国民の個人情報は極力減らす

エストニア政府は、極力国民の個人情報は持たないようにしようと考えている。この考えは、エストニア政府機関は国民から直接得た個人情報を2回以上聞いてはいけないというデータワンスポリシーともいうべき政策に反映されている。たとえば住民票に個人の住所が登録された場合、その個人が運転免許証を取得する際にはあらためて住所を告知する必要はない。X-Roadを使えば、運転免許証データベースが住民票データベースに直接住所の情報を取りにいける。また、1つのデータはあくまで1カ所の格納場所になければならず、複数のデータベースに保管してはいけないというポリシーも定めている。この政策には、データの管理コストを低減する、という意図もある。

利用者は、自分の情報が閲覧された場合には、必ずログを参照できるような仕組みになっている。そして目的外などの、違法な閲覧行為には非常に大きなペナルティーが課せられることとなっている。

国民以外にもIT基盤を広く世界に開放

エストニアは、こうしたデジタルプラットフォームを自国で抱え込まず、広く世界に開放する試みも始めている。2014年12月からスタートしたe-Residencyと呼ばれるサービスは、エストニア国民に限らず、非居住者に対しても同様のデジタルIDを発行し、電子政府のサービスの利用や、安全な本人認証ができるようにしたものだ。たとえば非居住者がエストニアで銀行口座を開設しようとした場合、スカイプなどの映像通信で銀行と面会することにより、国外からでもオンライン上でエストニアの銀行口座を開くことが可能となる。同様に非居住者による起業も容易に行なえる。政府によると2016年11月時点で131カ国から、当初計画の3倍以上にあたる1万5,000件もの申請があり、1,000社以上ものスタートアップ企業が設立された。

こうした方法により仮想エストニア国民を増やし、スタートアップ企業を誘致していくことは、エストニア経済の活性化へとつながる可能性が大きい。のみならず、エストニアがこうしたプラットフォームをオープンにすることで、世界中のアイデアやノウハウを借りながら、このプラットフォームのアプリケーションを充実させ、より大きな経済効果を得ることができるというメリットもある。実際に金融取引に欠かせない個人認証の仕組みを備えているとして、e-ResidencyのID管理手法が世界の金融機関やフィンテック企業から注目を集めている。欧州の都市で、e-Residencyをすべての市民に発行し、マネーロンダリング防止に活用しよう、と検討している話もあるようだ。EU加盟国間のデータ連携にX-Roadを活用しようとするX-Roadヨーロッパ構想というプロジェクトも進行中だ。

3　ガードタイム社によるエストニア電子政府への貢献

政府はこうした基盤を構築するために積極的に民間企業と連携、その技術を採用している。ここでX-Roadのセキュリティー面を担保するガードタイム社を紹介しよう。

ガードタイム社は、エストニアのセキュリティー企業として2006年に創業。本社はアムステルダムだが、旧ソビエト時代の暗号研究の中心地であったエストニアにR&D拠点を配置している。最大の取引先は米軍であり、その他エストニア、米国、EU、UAE、中国など多くの政府をクライアントに持つ。中国とは多数の契約があり、中国独自の暗号技術の開発を手助けしているという。米国NSA（国家安全保障局）は“今後の脅威はデータ改ざん”としており、ガードタイム社はこうした機密データの整合性を守る事業に特化している。

国家機関レベルのデータ改ざんを検知するKSIブロックチェーン

KSI（Keyless Signature Infrastructure）は、複数の機関で大量発生するデータの改ざんを検知する、ガードタイム社独自の技術だ。KSIは自身でデータを保持している訳ではなく、その点、本論で述べているブロックチェーン技術との違いはあるが、外部のデータベースに格納されているデータが、いつ、どこで発生したかの要約（ハッシュ）をチェーンにする仕組みであり、広義のブロックチェーン技術といえる。KSIは、改ざんが行なわれた場合、過去のどの時点、どのデータ発生箇所で改ざんされたかを1秒間隔で検出することができる。改ざん検知に特化しているからこそ、リアルタイムな検知が可能といえよう。

また台帳（データ）そのものを持たず任意のデータ発生源を取り扱うことができるため、レガシーシステムから発生するデータの改ざん検知にも適用でき、システム間でデータを秘密にしておくことが可能だ。ガードタイム社はKSIをエストニア政府のX-Roadに提供することにより、電子政府サービスの信頼性を向上する基盤となっている。

ビットコインは国家のデータ管理には不適

「ビットコインのブロックチェーンやイーサリアムはガバナンスが不明瞭であり、国家のデータ管理には使えないだろう。」とガードタイム社のCTOであるMatthew Johnsonは語っている。PKI（公開鍵基盤）も万能ではなく、PKIでもすべてを解決するのはスケーラビリティの面で困難だという。世の中の仕組みは、秘匿性（情報を秘密にすること）と整合性（対改ざんなど）を同時に扱おうとしている点が課題だと説いている。

また、エストニアはロシアから幾度もサイバー攻撃を受けており、その教訓として、どれが正しい時点のデータかを知ることができ、正しい状態へ戻す対応ができることが最も重要だと述べている。情報漏えい、改ざんなど、未知の脅威に対抗する完全対策はないため、脅威が発生し得ることを認めた上で効率的に対処することが重要、という意図であろう。

4　理想はインビジブルガバメント

サービスを徹底的に簡素化する

エストニアはインビジブルガバメント＝見えない政府をめざす。真のサービスとは、利用者も気づかないうちにすべての手続きが簡単に、意識せずとも完結すべきものだと考えている。パソコンの画面上でマウスをクリックする回数にまで気を配り、すべてのサービスで徹底した簡素化を実現することをめざしている。たとえば2000年からスタートしている確定申告の電子化において、最短3分で完了するという事例を紹介したが、これはわずか3回のクリックで完了するようにデザインされている。

民間企業や利用者のIT基盤活用を政府が支援

また、政府がいろいろなことに前面に立って関与するのは最小限にすべきだとも考えている。X-Roadの運用でも、認証・セキュリティーが保証されたプラットフォームはきっちりと整備するが、具体的な活用方法については民間企業や利用者の工夫を促している。あくまでも政府のスタンスは、運用していく過程で直面する問題や障害については積極的に協力をしていこうというものである。e-Residencyを稼働する際も、国外での銀行口座開設を可能とする法改正を9カ月かけて可決に導いた。こうした国民の利益に資することに労力を惜しまない姿勢は、IT化の初期段階からも一貫していたといえる。2002年、当時まで決して高いとはいえなかった、国民のITリテラシーを向上させる施策として、政府は民間と協力し、ルックアットザワールドプロジェクトを立ち上げた。公民館などの公共施設において、無料でインターネットの使い方を教えるという地道な活動だ。この活動は時間に余裕のある高齢者などに口コミで広がり、開始から2年、人口の約10％にあたる13万人への教育を終えた時点で、ほぼすべての国民がPCやモバイルでネット接続をするようになったという。

第Ⅲ部　ブロックチェーンを社会インフラとするために

1　ブロックチェーンの課題

ブロックチェーンは新しい技術であるだけに、まだ多くの課題を内包している。これらは、大きく技術自体の課題、ビットコインなどを支える合意の手法に関する課題、事業化する際に生じる課題に分けられる。以下、順次見ていくこととしよう。

まず、ブロックチェーン技術自体の課題としては、次のようなものがある。

① 大量の取引に対応できなくなる

スケーラビリティ(拡張性)の問題である。ブロックチェーンの取引が多くなるにつれて、ブロックに格納する情報の容量も大きくなる。たとえば1秒に数千・数万というような大量の取引を考えた場合、ブロックチェーンがたちまち長大化し、ノードに必要なディスク容量、ネットワーク資源、マシンパワーが大きくなるため、ブロックチェーンに参加できるノードが限られてしまう。これは同時に限られたノードのみが参加メンバーとなる、いわば集中化を招く可能性もある。

これについては情報をコンパクトに格納するなど、さまざまな技術的対応が検討されているが、たとえば世界中のクレジットカード決済、証券取引などを賄うだけのスケーラビリティを確保するにはまだ時間がかかるだろう。特に広域で利用されることの多いUnpermissioned型のブロックチェーンについての顕著な課題である。

② プライバシーの保護と分散管理の両立が難しい

本来台帳を持ち合うという透明性が特徴のブロックチェーンであるが、一方で、個人の財産情報などの秘匿性が必要な使い方を求められることがある(たとえば、保有する証券の情報など)。プライバシーの保護と情報を分散的に保有するという利用方法に矛盾があるように見えるが、秘匿性を確保しないとビジネスとしては成り立ちにくい。これについては暗号鍵の持ち方、秘匿したまま情報を処理する方式などが検討されつつある。

次にビットコインなどの仮想通貨として使われているブロックチェーンのPoWというコンセンサス・アルゴリズム技術については、以下のような課題がある。なお、Permissioned型ブロックチェーンの代表的なコンセンサス・アルゴリズム技術であるPBFTなども完成されたものではなく、堅牢(けんろう)性の向上などの課題に向けたコンセンサス・アルゴリズムの研究開発が続けられている。

③ 即時性の必要な取引には向かない

PoWの場合の承認スピードの問題である。ビットコインで使われているPoWの場合、データの整合性と処理効率のバランスから約10分間ごとにブロックが作成されるよう調整されており、即時性が必要とされる取引には向かない(前述の脚注で示した通り、合意が覆らないことの保証のためにはおおむね6ブロック必要といわれており、約1時間必要ということになる)。そうしたスピードの遅さを克服するためには、10分待たずにそれを使う当事者がリスクをとって取引を行なう対応をしている実例もある。また、複数のブロックチェーンを連携させることによる技術(これをサイドチェーンという)を活用して、この欠陥を克服しようという動きもある。

④ 本当に低コストになるかわからない

PoWを利用する場合、電力などシステム全体としてのコストが本当に低くなるのかということが指摘されている。実際に最終的にそのコストを負担するのは利用者になるのではないか、結局それでは安上がりではないのではないか、という見方も根強い。

さらに、ブロックチェーンをビジネスとして実装していくためには以下のような課題がある。

⑤ 周辺のアプリケーション機能の開発や標準化が必要

ブロックチェーンのみで業務システムを完結できることは少ない。たとえば銀行の勘定系などにブロックチェーンを入れていこうとすると、周辺アプリケーション機能が同時に開発される必要がある。また複数の銀行間でコンソー

シアムを築こうとすれば、ともに持ち合う台帳を共有していかなければならないため、標準化が必須となる。今後、ブロックチェーンが普及していくためには、ブロックチェーン基盤を開発する各企業にとってはオープンAPIや、分散台帳のデータ形式や台帳間のインターフェースの標準化といった対応が鍵になる。

⑥　契約では想定しない事態への対応が難しい

スマートコントラクトが完全でない場合への対応である。すべての事象を予想して網羅的にスマートコントラクトに定めておくことは極めて難しい。次に紹介するThe DAOの問題が典型である(詳細は以下「参考　The DAOを巡る問題と示唆」を参照)。スマートコントラクトには法的拘束力はなく、あくまでも私的な統治である。そこには限界があり、いざとなると法的な解決を図る局面も出てくると考えられる。このための私的な統治方法の一層の工夫や保険手当てなど損失負担への対応なども考えていく必要があるだろう。

(参考) The DAOを巡る問題と示唆

The DAOとはドイツのブロックチェーンスタートアップ企業であるSlock.itがEthereum Foundationと連携して設立した事業投資ファンドである。DAO (Decentralized Autonomous Organization: 一般に「分散型自律組織」と呼ばれる)というコンセプトを実証するために、2016年4月よりパブリック型ブロックチェーンのイーサリアムで記述されたスマートコントラクトによるファンドを組成し、資金調達を開始、6月までの間にイーサリアム上の通貨「イーサ」を1億5,000万米ドル相当集めた。ところが6月17日、The DAOのスマートコントラクトのバグを狙ったハッカーにより、そのうちの5,000万米ドル相当が流出するという事件が起こる。ハッカーはThe DAOのスマートコントラクトに規定される、契約を分割できる機能を用いて“子DAO”を作り、The DAO本体から資金を繰り返し移転させていった。ハッカーは「自分は公開されたスマートコントラクトに基づき出金をしただけだ。何も違法なことはしていない」と主張した。

この事象に、もはやThe DAOだけで対処することはできず、プラットフォームであるイーサリアム自体にも影響が及んだ。イーサリアム創設者のVitalik Buterinは、流出した資金をThe DAOに戻すため、既存のイーサリアムと互換性のない新しいイーサリアムプログラムを全ノードに配布し更新を求める「ハードフォーク」を提案。この提案に対して賛否両論の議論が過熱したが、結果として2016年7月20日にノードの大半の賛同を得て、ハードフォークは実行された。しかしこの対応に反発する声も根強く、現状ではいまだ旧版のプログラム(イーサリアムクラシックと呼ばれる)上で、旧イーサも継続して取引されている。同じイーサリアムで新旧2つが併存する、という不安定な状況が続いている。

Vitalik Buterin氏は、イーサリアムがまだ実験中のシステムであるとして、ハードフォークによる対応はやむを得ないと弁明した。まさに今回の一連の騒動は、プログラムのバグを明らかにしただけではなく、本文中にあるようにスマートコントラクトの不完全性を浮き彫りにした。現段階では、あらゆる可能性を想定してあらかじめ完全なコントラクトを準備することは非常に困難といえる。しかし、サイバースペースでは、特定の国の規制や法執行を受け入れない仕組みにおいては、「Codeが法律である」として、それを恣意的(しいてき)に変更するべきではないという主張もあった。結局は何か問題が生じた時に、Codeに完全に依存するのではなく、状況に応じた人間による解釈・判断がまだ必要なのかもしれない。オフチェーンでの当事者間の話し合いによる解決方法を決めておいたり、または権限の一端を既存の権威ある管理機関などにまかせたりするといった、ガバナンスの方法について当面議論を継続していかなければならない。一方で、サイバースペースの自治を求める人々と、各国の司法当局、規制当局がどのように折り合いをつけていくかという課題が明らかになってきたともいえる。

2　ブロックチェーンは今後社会をどう変えるか

本稿の冒頭に、ブロックチェーンは社会の新たなインフラとなる可能性を秘めた技術であると述べた。ブロックチェーンの活用により、個人レベルでの利便性向上、新しい付加価値の高いビジネスモデルの誕生と発展、さらに取引の効率化などを通じた産業の再編、政府や企業の生産性向上などを通じて、経済社会の発展が期待できる。以下、検討してみよう。

安心して使える公的サービスの実現

情報を分散して管理し、改ざんを極めて困難にするブロックチェーンは、情報化社会における信頼性をより高め

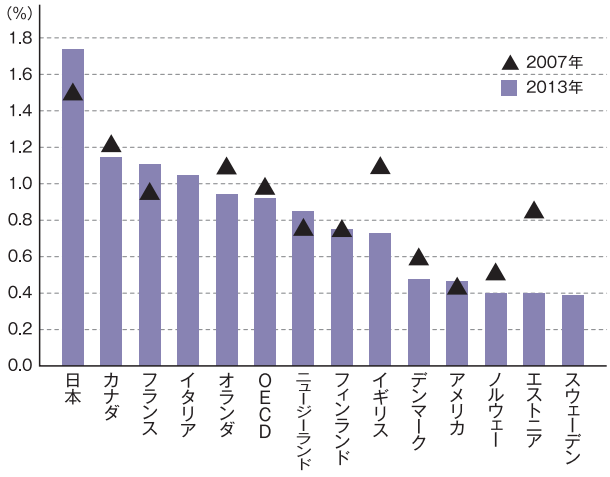
る仕組みを人々に供与する可能性を持つ。特に、公共部門においてその活用範囲が大きいことはエストニア政府の取り組みとその成果からも明らかである。

エストニアでは、政府の仕事が大胆に効率化している。たとえば、税徴収の効率性の水準は、国際的に見るとエストニアは圧倒的に高く、効率性が主要先進国のなかで最も低いわが国と比較するとその差は顕著であることがわかる(図4)。また、医療や不動産などあらゆる場面で個人の情報がデジタルに記録され、許可された人や企業などがそれを活用できる。これにより、民間企業や医療関係機関における生産性も高まり、人々の暮らしの利便性も高まっている。また、プライバシー対応策としては、万一個人のデジタルな秘匿情報を許可していない他人が見れば、それがすぐに検知、データ履歴として書き込まれ、非常に大きなペナルティーが課されることにより、個人が安心して便利に公的なデジタルサービスを使えるようにしている。

こうした利便性を実現するためには、政府が、個人情報を保護しつつ、個人番号を政府や医療機関などで共有すること、デジタル化に対応した適切なプライバシー対策を有効に行なっていること、そして個人情報などの正しさを証明するインフラを提供していることが前提となっており、ブロックチェーンがその鍵を握る1つの技術といえる。

また、安定した政府が成立しておらず、社会インフラが十分整備されていないような発展途上国の人たちや中東の難民のような人たちにとっても、ブロックチェーンによる分権的、草の根的な社会インフラの提供を通じて、社会的弱者の金融包摂といった厚生の向上、利用者の生活上の問題の解決が期待される。

図4● 税徴収の効率性についての国際比較



注1. 税徴収の行政コストの税収に占める割合を示したもの。なお、国によって事情が異なるため、国際比較に当たっては注意が必要。
注2. エストニアの2007年には税関費用も含まれているが、2013年には含まれていない。
(出所) OECD "Government at a Glance 2015"(2015)をもとに加筆修正

取引履歴を活用した新たなビジネスチャンス

民間ビジネスの分野においても、ブロックチェーンという新たなプラットフォームは、新しいビジネスチャンスを生み、あらゆる業種のビジネスのあり方を大きく変える可能性を秘めたものである。第Ⅱ部で紹介したように、たとえば、ダイヤモンドの鑑定情報をブロックチェーン上でデータ化することにより、これまで横行していた鑑定書の偽造や詐欺をなくし、安心して取引ができる流通プラットフォームを作るといった新しいビジネスチャンスが生まれているのは好事例である。

ブロックチェーン技術の発展は、スマートコントラクトなどが織り込まれていくことによって、取引を効率化し、付加価値向上をサポートするインフラとしての発展が見込まれる。このため、取引にかかわる企業の業務が大幅にスリム化して生産性の向上を促すことが期待できる。また、そうした取引情報を活用して、企業はさらに付加価値の高いビジネスを展開できる可能性も広がる。特に、ブロックチェーン技術は、IoTとも親和性が高いといわれており、その応用が期待されている。ブロックチェーンとIoTがつながることで、異業種間でのセンサーデータ(検知した分析に適したデータ)活用、その情報に基づくスマートコントラクトでの自動制御、さらにはこれに対応した金融サービスの提供が可能となるだろう。これにより、サプライチェーン、物流の効率化、シェアリングエコノミーの健全な発展や、ヘルスケアなどの分野を、業種を越えて効率的に発展させる方向に作用すると考えられる[5]。

この結果として、今までこうしたビジネスに取り組んでいたプレーヤーやビジネスの統合が進むなど、産業のアーキテクチャー、業界区分を大きく変化させる可能性を秘めている。また、情報とモノとカネの流れが結びつくことによって取引されるモノの価値自体を上げたり、カネやモノの取引履歴情報によって、不正の防止、犯罪の解決など社会的課題を解決したりしていく可能性も秘めている。

金融ビジネスにおける取引の効率化

金融ビジネス分野に関しても、貿易金融、証券取引、シンジケートローンなどさまざまな分野で、取引の効率化が

5 たとえば、セーフシェアー社(英国)の取り組みにより、保険が提供されることによって安心してシェアリングサービスを使えるようになり、カーシェアや民家への宿泊などがさらに広がる可能性がある。

進み、金融機関のオペレーションが大きく改善したり、そこで得られる情報を活用した金融サービスを展開できる可能性が広がる。保険ビジネスも、ブロックチェーンの発展に対応して、スマートコントラクトにより保険支払いを自動化するなど、新しいサービスを提供できる機会が拡大する可能性がある。米国の中央銀行である連邦準備制度は、クロスボーダー送金や貿易金融、証券取引やデリバティブ取引の分野において、コスト削減や迅速性確保などの潜在的な社会的メリットは大きいとしている。いまだ発展途上の技術であるため、決済システムの信頼性確保に十分に注意を払いつつ、この技術を注視し、サポートする姿勢を明らかにしている[6]。

不特定参加者の仮想通貨はどこまで発展するであろうか。もちろん現時点では専ら値上がり益狙いの資産として保有されているものが多いとはいえ、実際に通貨として利用される仕組みを整備していこうとする動きもある。こうした仮想通貨を活用した取引が、少しずつ広がっていく可能性はあり、いつの日か既存通貨を脅かす存在となる可能性もある。

現在、日本の金融機関はさまざまなブロックチェーンの実証実験を行なっているが、仮想通貨を使った取引も含めて、まだ実現しているものはない[7]。しかし、このような実証実験を経て今後は具体的な利便性の高いサービスが提供されてくる可能性があるほか、証券取引などにも導入が進めば全体として金融機関のビジネスモデルを将来的に変えていく可能性を秘めている。

3　政策提言

以上述べてきたように、ブロックチェーン技術は、未成熟ではあるが、経済社会の発展を実現する潜在的に大きな可能性を秘めた技術といえる。上記のような社会を実現していくためには、ブロックチェーンという新しい技術の研究開発や実装に向けて、官民ともに、以下の2つの認識を持つことが重要だ。

第1に、潜在的に可能性のある新しい技術は、まずそれを適用するサービス自体を利用者が「安心で便利でメリットが大きい」と感じなければ信頼を獲得できず、結果的にその技術の活用も広がらないという点である。ブロックチェーン技術は、国や民間企業が提供する1サービスにとどまらず、社会の共通のインフラとなる可能性を秘めているが、そうしたインフラにまで発展するためには、この技術の持つ「分散」、「合意」、「共有」を特徴とするコンセプトに対する国民の理解も必要となる。そのためにも、この技術に内在するさまざまな課題を克服するための研究開発と、セキュリティーへの取り組みが一層これから重要となろう。こうした取り組みにより「分散」型のオープンなシステムは、「集中」してデータを管理する従来型のシステムと共存しながら発展することができるだろう。

第2に、モノや財、サービスのバーチャル化、ネットワーク化が進んだ社会において、有形・無形の価値を写し取る技術としてブロックチェーンは位置づけられるという点である。IoT、ビッグデータ分析とAI（人工知能）の活用といった、情報技術を活用した利便性の高い社会を実現していくための1つの重要な技術となり得る。こうした全体観を持って、技術の開発や実装を進めていく必要がある。

こうした認識に立ち、官民は次の4点を実践していくべきである。

提言1　政府は今後のデジタル社会についてビジョンを示し、官民チームでの課題共有・研究開発を推進すべき

政府は、急速に進む最先端の情報技術革新についての理解を深めて、今後のデジタル社会に向けて明確なビジョンを示し、それに向けた課題を明らかにしつつ、取り組みを率先して推進すべきである。このことは、ブロックチェーン技術に限らないが、ブロックチェーンにおいては特に必要となる姿勢として強調したい。

たとえば、英国では、政府の1組織である政府科学局が、フィンテック、またはブロックチェーンといった新しい技術の発展について、早い段階で官民双方に対して、こうした技術革新のもたらす未来社会へのビジョン、技術やセキュリティーなど普及のために必要な課題、規制のあり方などについてまとめた報告書を打ち出し、技術の発展と普及のための環境整備を進めてきている。実際に、これらの報告書によって、フィンテック企業が、規制のグレーゾーンであっても心配せずに実証実験ができる「レギュラトリー・サンドボックス」（Regulatory Sandbox）が生まれた。

6　Brainard FRB理事による2016年10月7日のスピーチ“Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement”参照。

7　日本の金融機関における実証実験ですでに公表されているものとしては、住信SBIネット銀行の勘定系への導入の取り組みや、三菱東京UFJ銀行のブロックチェーン技術を活用した仮想通貨発行およびこれによる海外送金の実証実験など。

日本では、2016年に経済産業省がブロックチェーンに関する報告書をとりまとめ、金融庁もフィンテックサポートの総合窓口を開設した。日本銀行もフィンテックセンターを作り、ブロックチェーンの課題についても民間企業も含めた議論を積極的に行ない始めている。しかし、各部署での活動が、全体としての大きな動きにはなっていないのが現実だ。さらに、政府は2013年6月「世界最先端IT国家創造宣言」を策定してはいるものの、その進捗は国民の目には見えてこない。

政府はより具体的に「徹底的に効率的な政府の実現」、「利便性の高いIoTネットワーク社会の実現」などのビジョンを示し、新技術の開発、実装を含めたデジタル化推進の取り組みを、大まかなマイルストーンを示しながら加速していくことが求められる。そして、政府内でこうした先端技術の導入検討を担う部署を明確に位置づけ、官民連携の取り組みを進める必要がある。IT新技術を社会に取り入れるために、政府自身が、理論的、実践的な課題が何であるかを積極的に公開し、それについて大学、企業などから、技術、システムの知見、かつ実践的な応用力を持つ専門家を集めてチームを作って共同で研究開発ができるような環境を用意するといったことも必要であろう。

提言2　政府はグローバルな観点からブロックチェーン技術を理解し、自ら導入検討の実践者となるべき

今後本格化するデジタル社会では、官民を問わず、膨大かつさまざまな種類の業務の効率化や高い信頼性が常に求められ、ブロックチェーンは、それを実現し得る可能性を秘めた技術の1つと位置づけられる。

そこで、政府は、グローバルな視野を持って、民間企業と連携しつつブロックチェーン技術を学び、自ら率先して、政府内での導入可能性を検討すべきである。その際、エストニア政府のブロックチェーン技術を活用した電子政府への取り組みなども参考にすべきであろう。ブロックチェーン技術でデータ改ざんを防ぐ措置を徹底している点、各省庁が持つ既存のデータベースをインターネットで結ぶことによって比較的安価にデータを共有し、相互参照を可能としている点、また、民間企業にもオープンな基幹システムを提供している点などは特筆に値する。

また、エストニアでは、政府が掲げるIT戦略の下で、国民へのIT教育を徹底して行ないつつ、事業化においては、まず小さい事業から始めて課題を解決しながら大きく育てる手法をとっている。こうしたアプローチをとることで、IT技術への国民の信頼を得ることに成功している。技術のみならず、普及方法においても参考にすべき点は多い。

さらに、日本では政府がIT技術を導入する際、これまでは政府が規格を作って発注するという方式がとられてきたが、こうしたやり方は急速に技術革新が進む今日のような時代にはそぐわない。発展途上の技術については、規格を作成する段階から官民が共同して研究開発を重ね、より効果的、かつ安全な設計をめざすべきである。

なお、近年日本でも導入されたマイナンバーに関しては、個人情報の扱いに十分留意した上で、政府内や特定の民間企業が必要とされる業務により適切に利用できるようにし、これを活用したデジタル化をスピードアップし、国民の利便性を高めるよう取り組む必要がある。この点においても、小さなトライアルを重ねて、課題を把握し、改善しながら適用先を拡大していくという方法をとることが効果的である。小さな事業化を積み重ねる中で、民間事業者は費用対効果も検証した上で参入するかどうかの選択ができ、また、現場での対応や国民のニーズの把握も進むものと思われる。

提言3　政府は民間企業がイノベーションを進めやすい環境を整備するべき

さらに、政府は、ブロックチェーン技術に関する民間企業のイノベーションを積極的に支援していくべきである。民間企業でこうした技術の活用を広げるために必要な環境整備上の課題を整理して、研究開発や実践的な取り組みを進めやすくするべきである。人手が不足している日本にとって、ビジネスの分野でブロックチェーンが導入されることによりさまざまな業種で生産性の向上や新しいビジネスが推進される可能性を考えれば、積極的に支援する意義は大きい。今後ブロックチェーンの実装が進むにつれて考えるべき法制整備、税制対応などの論点が出てくると思われるが、政府は技術の発展の芽をつまないという視座を持って検討を深めることが重要であろう。

金融分野の場合、既存のレギュレーションとの関係が課題となる。わが国では仮想通貨取引所については、2016年に先進国と同様のマネーロンダリング対応や利用者保護のための法律整備が行なわれた。今後も、マネーロンダリング対応、消費者が安心して使えるための枠組みを考慮していく必要がある。また、既存の規制との関係がグレーな

分野の新しい試みについては、政府は、利用者保護やリスクの管理などに配意しつつ、イノベーションを阻害しない実験場としての前述の「レギュラトリー・サンドボックス」のような支援環境を用意したり、イノベーションを進めやすい規制手法を考え、整備していくべきである。さらに、技術革新のスピードを考えると、政府による規制よりも、新しい担い手による自主規制のあり方などの検討がより必要とされるかもしれない。利用者が安心、納得して使えるような環境づくりや、決済システムの信頼性を維持しつつ技術の信頼性を向上させるために、官民の協力体制構築に配意する必要がある。

海外でも、英国の中央銀行であるイングランド銀行が、アクセラレータープログラムを自ら作り、民間企業に外注するのではなく、自らパートナー企業を選んで、連携して新しい技術を学んでいる点も興味深い。監督する側、監督される側で線引きするのではなく、民間とともに新しい技術を学び、時代に合った金融市場のモニタリングや規制監督のあり方を考えていく姿勢が伺われる。

提言4　民間企業はシステムのオープン化と標準化を推進すべき

ブロックチェーンのような分散的システムの構築にあたっては、システムのオープン化、標準化への対応が必須である。企業は、これまでの自前主義にこだわらず、実証実験を共有してイノベーションに取り組み、また、APIを公開するなどシステムのオープン化、標準化への対応をしていくべきである。

今般、国際標準化機関であるISOにおいて、「ブロックチェーンと電子分散台帳技術に係る専門委員会」が設立された。この委員会において、ブロックチェーンにおけるシステム、アプリケーション、ユーザー間の互換性やデータ交換に係る国際標準化活動が議論されていく予定だが、日本においてもこのような動きに乗り遅れないよう、積極的に関与していくことが求められるだろう。

技術進歩の流れは速い。ブロックチェーンというシステムのネットワーク効果を考えると、オープン・イノベーションにより、こうした技術が多方面に広がり、情報・取引ネットワークが政府や企業など参加者間で縦横に連携、つながるようになり、グローバルに大きく広がっていくことが、さらなる付加価値を生んでいく可能性が高い。そうした潜在的なビジネスの広がりの可能性を十分考えて、企業は今後の経営戦略を検討し、技術力を磨いてビジネスモデルの改革につなげていく必要がある。新しいビジネスモデルに進化していくためにも、今後の企業は、業種を問わず、経営陣に技術系の人材を配置し、スピーディーな経営判断ができるようにしていくこと、技術とビジネスの双方を理解できる人材の育成や、エンジニアの積極的な採用などが必須となっていくであろう。

翁　百合（おきな ゆり）
NIRA総合研究開発機構理事／日本総合研究所副理事長

なお、ヒアリングにご協力いただいた方の一覧はホームページ http://www.nira.or.jp/pdf/201612opinion_hearing.pdf をご覧ください。

NIRA
NIPPON INSTITUTE FOR
RESEARCH ADVANCEMENT

PDFはこちらから

NIRAオピニオンペーパーは、ホームページでもご覧いただけます
http://www.nira.or.jp/president/opinion/index.html

NIRAオピニオンペーパー［no.26］
2016年12月7日発行

発行人：牛尾治朗

※本誌に関するご感想・ご意見をお寄せください。
E-mail:info@nira.or.jp

公益財団法人 NIRA総合研究開発機構
〒150-6034 東京都渋谷区恵比寿4-20-3
恵比寿ガーデンプレイスタワー34階
TEL:03-5448-1710　FAX:03-5448-1744
http://www.nira.or.jp/index.html