ブロックチェーンとスマートコントラクトオートメーション：スマートコントラクトがデジタルビジネスをどう自動化するのか？

第5回（全5回）

パブリックブロックチェーンとプライベートブロックチェーンが最終的に実現するのは、デジタル通貨以上のもの、すなわち、デジタル・ビジネス・フローである。

pwc

今回の「PwC Technology Forecast」では、ブロックチェーンとスマートコントラクトオートメーションに関するレポート（全5回）とインタビュー記事をご紹介します。

ブロックチェーンテクノロジーについてなじみの薄い方であれば、全5回のレポートを全て読まれることをお勧めします。ブロックチェーンに精通している方は、第1回と第5回だけでも読まれてみてはいかがでしょうか。いずれにせよ、インタビュー記事は一読の価値があります。

第1回　序論と将来像
第2回　ブロックチェーンの定義
第3回　なぜ、ブロックチェーンが重要なのか？
第4回　プライベートブロックチェーンか、パブリックブロックチェーンか、それともその両方か？
第5回　スマートコントラクトがデジタルビジネスをどう自動化するのか？
インタビュー：Coin SciencesのGideon Greenspan氏。パブリックブロックチェーンに代わるものをテーマとしています。

スマートコントラクトに期待されるプロセスパフォーマンス

分散型P2P（ピア・ツー・ピア）市場に熱い期待を寄せる人々、ビットコインブロックチェーンに無限の可能性を見る人々、そして新たなデジタル取引環境の中で立ち位置を確保しようと奮闘する銀行といった関係者たちの間で、「クリプトローヤー」と呼ばれる人々、つまり暗号化技術について専門知識を有する弁護士が注目を集めるようになってきている。こうした弁護士の中には、法的拘束力があるコンピューター処理が可能なコードを何十年間も扱ってきた人もいる。今や、こうした専門知識を持つ人々が、ブロックチェーンに基づく新しいスマートコントラクトに大きな影響力を持つ存在となりつつある。

スマートコントラクトは、二者以上の当事者間で交わす、デジタル署名された、コンピューター処理が可能な契約である。ネットワーク上のバーチャルな第三者（ソフトウエアエージェント）が、こうした契約の条項（少なくともその一部）を実行・執行することが可能である。

コンピューター科学者であり、法学者であり、暗号専門家でもあるNick Szabo氏は、今注目を集めているクリプトローヤーの代表例である。Szabo氏は1993年に「スマートコントラクト」という新語を作りだし、以来、デジタル通貨やコンピューター処理が可能な契約記述用のプログラミング言語の開発に取り組んでいる。Szabo氏の仕事は、ブロックチェーン時代における新たなスマートコントラクト誕生の土台を形成している。Szabo氏によるスマートコントラクトへの数多くの貢献の中に、2002年に契約分析のために開発された「ドラフティング言語」がある。これは、契約書の条項における曖昧性を減らし、論理性を強化することに重点を置いた言語である。これが法律専門用語とプロシージャコードとの間の架け橋となった。この言語の開発により、Szabo氏は人間の言語が持つニュアンスを失ってしまうことなく、コンピューター処理の力を活用することに成功した[1]。

今日、スマートコントラクトにおいて用いられるスクリプト言語には、Szabo氏の初期の取り組みが踏襲されているが、中でもEthereumなどのプロトコルでは一段と視覚的な手法を採っている。Ethereumは現在、マイクロソフトによるBaaS（サービスとしてのブロックチェーン）提供の一環として利用可能となっている。同プロトコルの言語はEtherScriptと呼ばれ、色分けされたモジュール方式で表現され、人間に読みやすく直観的に理解できるように工夫されている。一例として、EtherScriptで書かれた販売契約を次ページの図に示す。

[1] Nick Szabo『A Formal Language for Analyzing Contracts』2002年
http://szabo.best.vwh.net/contractlanguage.html（参照日:2016年1月7日）

EtherScriptの例

出典:『What is Ethereum?』EtherScripter 2016年 http://etherscripter.com/what_is_ethereum.html（参照日:2016年1月7日）

契約を記述するスクリプト言語の目的は、既存の言語をベースにしながら、それをよりインタラクティブなものにし、自動化を進めることにある。ブロックチェーンを用いた取引は、ほんの出発点にすぎない。ここから出発して、複数当事者間のルールに基づく、極めて精巧な環境を創り出すことができるかもしれないのだ。

Szabo氏やEthereumプロジェクトをはじめとするさまざまな取り組みにより、コンピューター処理が可能な契約を実現するテクノロジー自体はもはや障壁ではなくなった。現在、真の障壁として立ちはだかっているのは、古くから定着する人間中心の法的プロセスである。中には古代ローマ時代にまでさかのぼることができるものすらある。

次に現れようとしているのは、すでに開発されているもののわずか1歩〜2歩先にあるものである。従ってそれは「革命」というほどではなく、いわば「進化」のワンステップにすぎない。進化の足跡を振り返り、先行した取り組みについてよく理解すること、またそこから将来実現するかもしれないさまざまな可能性についてヒントを得ることは、役立つものである。

スマートコントラクトの先駆けとなったもの

取引を促進するために、オンラインショッピングサイトでは何十年にもわたり、本質的には一方通行の契約形態を提供してきた。こうしたサイトを使用した経験があり、そのサービス条項に馴染みがある人も多いだろう。ショッピングサイトが提供する契約条項は柔軟性に欠けるが、評判がランキングで明らかにされているようなプロバイダーを介して行う少額取引であれば十分事足りる。サービス利用規約の文言はプロバイダーの支配下にあり、買い手は提示された条件に合意するか、さもなくばどこかよそで買ってくださいという話にしかならない。またどちらの側からも比較的低レベルの検証しかできない。買い手は出店

者およびサイト上の主張を信頼するか、それともしないかである。出店者の側は不払いのリスクを負ってくれるものとして、クレジットカード発行者を信頼するのみである[2]。

MERS（住宅ローン電子登録システム）などオンライン取引プロセスの管理システムも、スマートコントラクトの先駆け的存在である。MERSは中央管理を行う仮想の譲渡抵当権者として機能し、さまざまな当事者間でのやりとりのフローや、所定の住宅ローンにおける役割を簡略化する[3]。

紙のドキュメントとコードの両方を使用したハイブリッド型契約、デュアルインテグレーション

ブロックチェーンは、言うまでもなくドキュメントファイルの真正性やバージョニングを検証できる。そこから発想されるのが、紙に書かれたドキュメントとコードを合わせて使用する契約モデルである。コードを使ってコンピューターが実行可能な言語で契約条件を明確に表すことができても、例えば、契約違反やその結果としての訴訟が生じた場合に備えて、やはり従来型の手段を遂行するために書類のバックアップもファイルに保存する。

スマートコントラクトベンダーであるEris Industries社を創立する前、CEOのCasey Kuhlman氏とCOOのPreston Byrne氏は弁護士として開業していた。両人は法制度が本質的に書類事務に依存していることも、取引にかかわる一連のプロセスの法務面で多くの人間の関与が必要であることも（少なくともしばらくの間は）、よく理解している。

2015年にPwCのインタビューでKuhlman氏は次のように指摘している。「相手方当事者との紛争を抱えていたとします。そんな時にスマートコントラクトのコードを証拠として裁判所に提出することを想像してみてください。そのコードが必ずしもコンピューター言語でなくても、比較的人間が読み取りやすいコードであったとしても、裁判所の人たちは『頭がおかしいのではないか?』という目であなたのことを見るでしょう。コードとデータを調べて、それを執行することができる裁判官など、世界中に恐らく五人もいないのではないでしょうか。だからこのデュアルインテグレーションというアイデアが生まれたのです」

[2] 本セクションにおける考察の大半は、次の情報源に示唆を得ている。Samuel Bourqueおよび Sara Fung Ling Tsui『A lawyer's introduction to smart contracts』 http://www.crypto-law.com/doc/A%20Lawyer's%20Introduction%20to%20Smart%20Contracts.pdfで入手可能。Ethereum HK:Samuel Bourque on Smart Contracts and DAO's』YouTubeビデオ 2014年9月28日 https://www.youtube.com/watch?v=cTYqRClh3Mo（参照日:2016年1月8日）

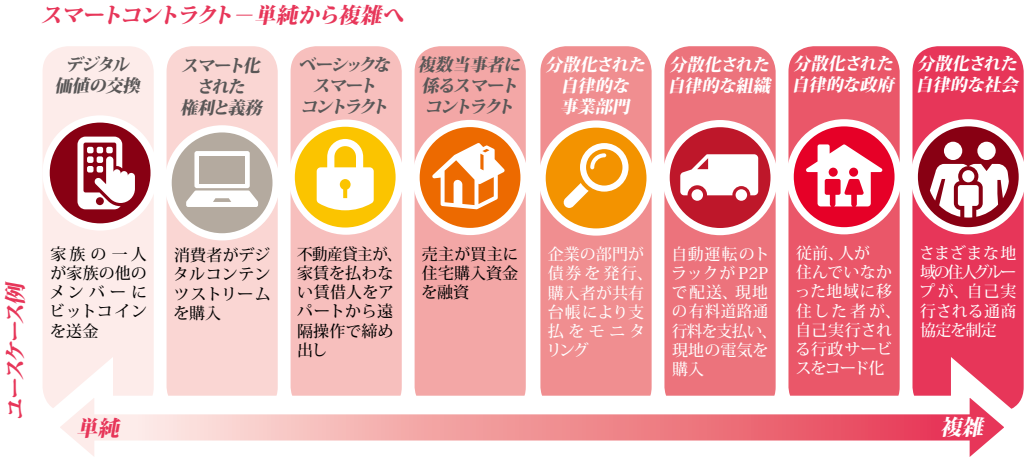
[3] 『FAQ』Mortgage Electronic Registration Systems https://www.mersinc.org/about-us/faq（参照日:2016年1月8日）

下表は、スマートコントラクトの数ある潜在的メリットをまとめたものである。ただし、これらのメリットが全てのケースに当てはまるとは限らないということに留意されたい。

従来型契約	スマートコントラクト
1~3日	数分
手作業による送金	自動送金
エスクローが必要	エスクローが不要な可能性がある
コストが高い	コストが極めて低い
当事者がその場にいなければならない（手書きの署名）	当事者はバーチャルに存在すればよい（デジタル署名）
弁護士が必要	弁護士が不要な可能性がある

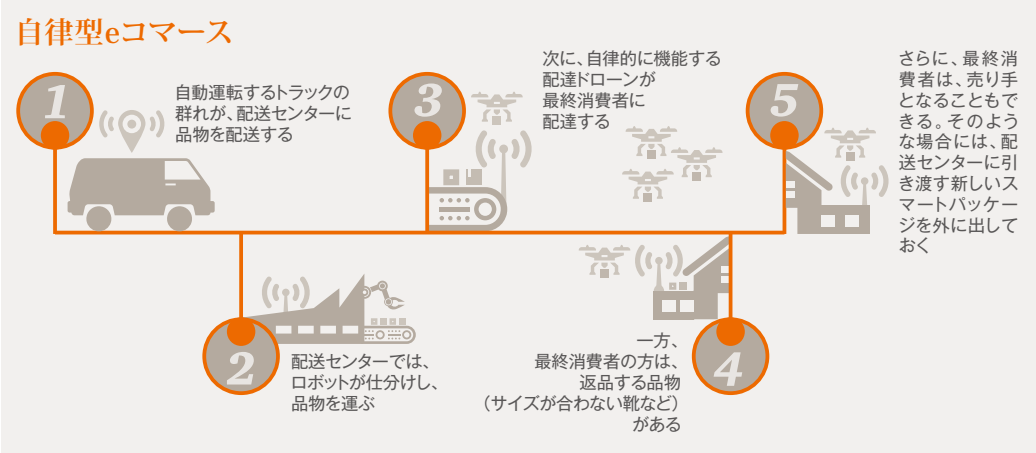
長期ビジョン

夢想家や空想家は、果てしない可能性を思い描く。会社が丸ごと自動的に運営される（分散化された自律的な組織）ばかりか、ある種の政府（分散化された自律的な政府）や社会の一側面までもが、自動化される可能性を想像している。



コンテキスト化されたスマートコントラクトのウェブ内で、ソフトウエアエージェントを立ち上げて、動的に分散化された自律的な組織を一つ一つマネージすることは十分想像できる。バーチャルな正規化データ環境においてなら、そのソフトウエアエージェントが、手を伸ばし、知識およびその他デジタル資産、またはデジタル化された資産をつかみ取ることも可能となる。

そのようなウェブとして思い描くことができる一例が、自律型eコマースである。自動運転するトラック群が、配送センターに品物を配送する。配送センターでは、ロボットが仕分けして、品物を自律的に機能する配達ドローンに載せる。次に、ドローンが最終消費者に配達する。一方、最終消費者の方では、返品したい品物（サイズが合わない靴など）があり、ドローンが配送センターに持ち帰ることができるようにスマートパッケージを外に出しておく。そうした個々の手順が、スマートコントラクトのウェブ上で、バーチャルな第三者として機能し、法的地位を有する一つまたは複数のソフトウエアエージェントによって、管理・実行されるということもあり得るだろう。



このような長期ビジョンを持つことは良いことである。そうしたイメージを思い描くことで、新しい着想を得たり、方向性が定まったりするからだ。しかしながら、先に挙げたさまざまなスマートコントラクトのうち、2020年までに実現可能とみられ、具体化する可能性が高いのは、初めの方の比較的単純な部類のものだけである。とはいえ、2020年代には、比較的単純な自己実行力契約のいくつかは、大規模化が可能になると考えられる。そのようなケイパビリティが育てば、ゆくゆくは、種々の取引カテゴリー全体で、コンプライアンス確保が今より容易になるだろう。ただし、実現への道には、多くの障害が立ちはだかる。

導入における主な課題

スマートコントラクトという夢がある。しかし、もう一方には現実が立ちふさがる。企業が、現行の取引環境を、スマートコントラクトに変えようと思えば、それは非常に根本的な変革であることから、数多くの困難な障害を乗り越えなければならない。さらに、その過程では、傾斜角のきつい学習曲線を上るという試練が待ち受けている。

まず、ビジネスエコシステム中の多くの役割が変わる必要があると思われる。弁護士は、コンピューターが読み取れるコードの書き方を学ばなければならないし、裁判官は、その解釈の仕方を学ばなければならない。そうでなければ、解釈の妥当性については専門家証人の証言に依拠することになる。開発業者は、幅広い分野から最先端技術を取り入れなければならない。何が最良の技術かについては、混乱が激しく、最先端技術に対する認識は低い。下記に、スマートコントラクトの導入に当たって直面すると想定される障害の一部を挙げる。これらは、あくまでも、ほんの一部にすぎない。

- **普及のS字カーブ：**新しい技術やシステムの導入に際して、その普及は、ほぼ例外なくS字カーブのパターンをたどる。当初はほとんど水平状だが、数年後にはより垂直に近づく
- **法規制環境は整うのが遅い：**ビジネスエコシステムの中でも、規制制度は、最も柔軟性に欠け、最も自動化が遅れている要素の一つである。スマートコントラクト自体、この問題に対する取り組みの一つの出発点となるかもしれないが、単一の解決法は存在しない。いずれにせよ、この点について掘り下げるのは、本稿の主旨ではない

- **ビジネスエコシステムの複雑性：**ビジネスに係るテクノロジー、プロセスおよび手続きなどの既存基盤によって、多くの前提や条件が決まるので、スマートコントラクトケイパビリティを特定のビジネスプロセスの中で構築する方法を検討するときに、これらの前提や条件を見直す必要がある
- **先行する競合サービス：**例えば、SaaS（サービスとしてのソフトウエア）市場のベンダーを通じたP2P融資などは、スマートコントラクトほど先進的ではないが、より成熟しており、急成長している[4]。ルールベースシステムなど既存基盤および他の先行レガシーIT基盤についても検討することが求められる
- **ベストプラクティスをめぐる不確実性：**スマートコントラクトにおけるベストプラクティスとはどんなものであるのか、そして、標準はどのようにして決定されるのか？例えば、『Reactive Manifesto』[5]で説明されている疎結合を実現する最新の原理や、マイクロサービス[6]におけるメッセージ駆動型プログラミングなどを、スマートコントラクトコードにどのように取り入れることができるのかについては、まだ不明瞭である。また、スマートコントラクトは、まだ生まれたばかりであることから、大きな課題を抱えている。合意事項をコーディングする他の方法がすでに多数存在しており、それら既存の方法は、すでに実用に用いられているということである

結論：スマートコントラクトが約束するもの、そしてより大きなチャレンジ

Amazon.comがオンライン書店として、eBayがオークションサイトとして、サービスを開始し、やがてB2C（企業―消費者間）eコマースの主流となったモデルの誕生から、20年以上が経過した。Forrester社が最近行った予想によると、米国のオンライン小売の商取引は2015年に3,340億米ドルに達したが、まだ小売総売上高の10％ほどで、2019年までに対前年伸び率が8％に鈍化する。同様に、Forrester社の予想では、米国のB2B（企業間）eコマースにおける2015年の売上高は1.1兆米ドルで、米国のB2B総売上高の12％強であり、2019年までに対前年伸び率が6.7％に鈍化する[7]。

こうした歴史的変遷を、eコマースを実現してきたテクノロジーの進歩との関連からさかのぼってみよう。SSL（Secure Socket Layer）暗号化通信がNetscape Browserに追加されたのは1994年で、Tim Berners-Lee氏が初のウェブブラウザーを発表したのは1990年のことだった。インターネットの基礎となるTCP／IPネットワーキングプロトコルが二つの大学で最初にテストされたのは、1975年。その後、企業の研究所などがしぶしぶ重い腰を上げて、これをさらに精査するようになったのは、1984年に入ってからのことである。要するに、eコマースの実現テクノロジーが開発されるのに実に20年、eコマースが成熟するのにさらに20年がかかったのである。

---

[4]『Peer pressure: How peer-to-peer lending platforms are transforming the consumer lending industry』PwC white paper 2015年2月 http://www.pwc.com/us/en/consumer-finance/publications/peer-to-peer-lending.html （参照日:2016年1月29日）

[5]『The Reactive Manifesto, a statement of systems architecture principles』2014年9月16日 http://www.reactivemanifesto.org/（参照日:2016年1月29日）

[6]『What is Microservices Architecture? Think Ant Colonies, Beehives, or Termite Mounds』PwC Emerging Technology のブログ 2014年8月25日 http://usblogs.pwc.com/emerging-technology/what-is-microservices-architecture-think-ant-colonies-beehives-or-termite-mounds/（参照日:2016年1月29日）

[7] Sucharita Mulpuru、Victoria Boutan、Carrie Johnson、Susan Wu、Laura Naparstek『Forrester Research eCommerce Forecast, 2014 To 2019 (US)』Forrester 2015年4月22日 https://www.forrester.com/Forrester+Research+eCommerce+Forecast+2014+To+2019+US/fulltext/-/E-res116713 およびAndy Hoar、Carrie Johnson、Patti Freeman Evans、Susan Wu、Jacob Milender『US B2B eCommerce Forecast:2015 To 2020』Forrester 2015年4月9日 https://www.forrester.com/US+B2B+eCommerce+Forecast+2015+To+2020/fulltext/-/E-res115957 （参照日:2016年2月2日）

一方、「取引のインターネット」は、すでにいくつかの方法で実現可能となっている。具体的に言うと、法的インフラの既存基盤水準が低い場所あるいは、元来法制度があまり複雑ではない法域における内部B2Bシナリオなどでは、スマートコントラクトをテストし、改良する機会が存在している。そのようなシナリオでは、スマートコントラクトが実用化されるまでに、eコマースほど長くはかからないかもしれない。加えて、主要金融機関は、ブロックチェーンに基づく取引の実験に対して、渋々どころか、むしろ意欲的に取り組んでいる。また、言うまでもなく、テクノロジーセクターの関心や関与の度合いも高い。公共のセクターでは、OpenBazaarなど、ブロックチェーンに基づくP2P市場の大胆な実験的試みが、すでに開始されている。

独占所有された秘密の方法や公開された方法を用いて、法的合意文書のコーディングを行うことも、今日では、実現可能であると考えられる。より単純な、分かりやすいプロセスの場合には、もはや実現テクノロジーが存在しているのである。しかしながら、バグの問題を解決する必要がある上、プロセスを変えるのは困難である場合が多く、ITインフラ自体もより進化する必要があると思われる。

より複雑なスマートコントラクトや、分散化された自律的な機能、事業部門や組織となれば、課題はいっそう大きい。

とはいえ長期的に最も期待されるのは、エージェントによって管理された複雑なP2P取引の自動化である。言い換えれば、インターネット、エージェントのウェブ、スマート取引、スマートコントラクトの組み合わせによって実現される、高効率の「モノのインターネット」である。2010年代の終わりまでは手直しと試行錯誤が続けられるだろう。ある意味、1990年代後半とよく似た状態である。さらにブロックチェーンと人工知能の双方関連のスタートアップ企業が何百社も誕生していること、それらの企業に対してベンチャーキャピタルから潤沢な資金が投じられていることを考え合わせると、試行錯誤の時期の後にはドットコムブームの時のように一気に拡大・発展して、一時的な過熱状態を迎える可能性も予感される。2020年代後半になるまでは、企業においてはGartner社が言うところの「幻滅期(Trough of Disillusionment)」を経て、今日とは大幅に異なる取引環境の本格的採用への道を歩んでいるかもしれない。

お問い合わせ先

PwCコンサルティング合同会社
〒100-6921 東京都千代田区丸の内2-6-1
丸の内パークビルディング
03-6250-1200(代表)

松崎 真樹
パートナー
maki.matsuzaki@pwc.com

田中 玲
パートナー
rei.r.tanaka@pwc.com

一山 正行
ディレクター
masayuki.m.ichiyama@pwc.com

「PwC Technology Forecast」について

PwCのテクノロジーイノベーションセンター(CTI)が刊行する「Technology Forecast」は、新たなテクノロジーや最新動向について掘り下げ、経営者やテクノロジー担当幹部の皆様をテクノロジーがもたらす機会における活用戦略の開発面で支援いたします。

これまでの「PwC Technology Forecast」では、さまざまな新テクノロジーやトピックを取り上げてきましたが、その多くが、今日のテクノロジーやビジネスに係る主要問題となっています。「Technology Forecast」についての詳細は、www.pwc.com/technologyforecastをご覧ください。

www.pwc.com/jp

本報告書は、PwCメンバーファームが2016年5月に発行した『Blockchain and smart contract automation: How smart contracts automate digital business』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル(英語版)はこちらからダウンロードできます。 www.pwc.com/us/en/technology-forecast/blockchain/gideon-greenspan-interview.html
日本語版発刊月: 2016年9月　　管理番号: I201605-11