連載 国際商取引学会リレー講座

国際商取引の新展開

第二部　グローバル・コンプライアンスと技術革新
第6回　スマートコントラクトと法の役割

高橋宏司*

Ⅰ　スマートコントラクトとは

スマートコントラクト（smart contract）とは，中央サーバに置かれたコンピュータプログラムと異なり，ブロックチェーン上に展開され，ネットワークのノード（参加端末）によって分散的に保持され，独立して実行されるコンピュータプログラムである。スマートコントラクトを用いて作成されたアプリケーションは，分散型アプリ（DApp: Decentralized Application）と呼ばれ，そのうち組織の動きを模したものは，分散自律組織（DAO: Decentralized Autonomous Organization）と呼ばれることがある。

Ⅱ　よくある誤解～スマートコントラクトは「契約」？

スマートコントラクトの概念は，1990年代にも提唱されたことがあったが，それが広くブロックチェーンの文脈で用いられるようになった端緒は，2013年に公表されたイーサリアムのホワイトペーパー[1]である。そこでは，同ブロックチェーン上に展開されるプログラムを書くことを指して，「スマートコントラクトを書く」と表現された。この言葉は，イーサリアムに世間の耳目を集めることに貢献したが，法的な意味の「契約」との混同も招いた。前述したとおり，スマートコントラクトは，ブロックチェーン上に展開されるコンピュータプログラムにすぎず，契約ではない。前記ホワイトペーパーの著者は，2018年になって，「私は『スマートコントラクト』という言葉を用いたことをかなり後悔している。『永続的なスクリプト（persistent scripts）』のように，凡庸で技術的な表現を用いるべきだった。」と述懐している[2]。スマートコントラクトが「永続的なスクリプト」であると言えるのは，それが一旦ブロックチェーン上に展開されると，各ノードに分散的に保持され，独立して実行されるため，攻撃や改竄に対する耐性が高いからである。

Ⅲ　ハッキングから生ずる私法上の問題

コンピュータプログラムが複雑になるとバグの混入が宿命的に起こり，この点，スマートコントラクトも例外ではない。スマートコントラクトには，バグを突くハッキングの標的になり易い特性もある。それは，内部に暗号資産を保管できるにもかかわらず，コードが公開されているためにバグも可視化されており，見つかったバグの除去もできない[3]という特性である。

バグを突くハッキングが現実化した一例が2016年に起きたThe DAO（Tは大文字）事件である。The DAOは，ある開発者グループによってイーサリアム上に展開された分散自律組織であり，ベンチャーキャピタルファンドとして機能させることが意図されていた。The DAOには，ファンドマネージャーは存在せず，代わりにスマートコントラクトによって，仮想通貨の出資受入れから配当の付与までのすべての処理がプログラムされていた。しかし，コードに存在していたバグがハッカーに突かれ，出資された仮想通貨が大量に流出する事態に発展した。本事件では，ブロックチェーンが巻き戻される措置が取られて流出が回復されたが，このような技術的解決は，不可逆性というブロックチェーンの基本思想に真っ向から反するため，異例の措置である。

では，スマートコントラクトのハッキング事例では，被害者にどのような法的救済が可能であろうか。ハッカー自身の身元は，ブロックチェーンに匿名性があるために割り出しにくい。そこで，バグのあるスマートコントラクトをブロックチェーン上に展開したコード開発者や，その利用を勧誘した者に対して不法行為責任等が問われることになろう。しかし，開発者の身元も，コードが匿名でブロックチェーン上に展開されると判明しにくい。また，開発者の責任には理論的に困難な問題もある。すなわち，コンピュータプログラム一般について，バグを民法や製造物責任法上の「瑕疵」や「欠陥」とみなすべきかが問題となるほか，スマートコントラクトのように公開され，鑑査可能なコードについて，利用者の自己責任論（caveat lector）が妥当するかが問題となり，さらに，バグが見つかっても除去できないというスマートコントラクトの特性をどう考えるかも問題となる。ちなみに，日本の判例には，スマートコントラクトに関するものではないが，契約に従って納入されたソフトウェアにバグがあった事例で，「バグといえども，システムの機能に軽微とはいえない支障を生じさせる上，遅滞なく補修することができないものであ……るような場合には，プログラムに欠陥（瑕疵）があるものといわなければならない」と判示したものがある[4]。

Ⅳ　予測市場と刑事罰

スマートコントラクトの利点である改竄耐性と鑑査可能性が活かされる分散アプリの例に，予測市場がある[5]。予測市場は，参加者が賭け金を拠出し，正確な予測に対して賞金が支払われる仕組みになっているため，それが中央サーバ上のプログラムによって行われるならば，運営者によって横領その他の不正が行われるおそれがある。運営者の存在しない分散アプリでは，賭け金はスマートコントラクトに管理され，プログラム通りに賞金が支払われるので，不正のリスクを回避できる。

予測市場は，商品価格や天候等の様々な不確実性をヘッジする手段を提供するという社会的効用を有し得るが，法域によっては，賭博とみなされ，参加者に賭博罪が成立し，その運営者に賭博場開帳罪等が成立する可能性がある。スマートコントラクトにより運営される分散アプリには，運営主体が存在しないものもある。しかし，スマートコントラクトと直接にやりとりするにはコマンドラインを使わなければならず，一般大衆にとってハードルが高いため，それを容易にするウェブサイト等のユーザ・インターフェイスが提供されることが多い。予測市場に利用者を導くウェブサイトが存在すれば，その開設者が賭博の運営者とみなされる可能性があるであろう[6]。他方，スマートコントラクトの開発者には，賭博罪の幇助犯が成立する可能性があるが，民事責任と同様，技術開発に対する萎縮効果を回避する要請とどのように折り合いを付けるかが問題となる。日本には，著作権法違反の幇助犯の成立が問題となったウィニー事件判決[7]があり，同判旨の射程も問われよう。

Ⅴ　分散型金融と規制

分散型金融（Defi）とは，金融の分散型アプリであり，スマートコントラクトを利用して仲介業者の存在なく運営されるものである。一般に，規制は技術ではなく，行為主体に対して適用されるので，スマートコントラクト自体は規制されない[8]。すると，仲介業者が存在しない分散型金融に対して証券規制や為替規制等の金融規制がどのように適用されるかの疑問が生じよう。しかし，実際には，分散型金融の運営の分散度は様々であり，ほとんどの場合，収益化

——もくじ——

*たかはし こうじ，同志社大学教授

等の目的で，何らかの主体が何らかの態様で関与している。また，規制の名宛人にも，各々の規制によって異なるが，様々な行為主体が含まれる。スマートコントラクト自体は，一旦ブロックチェーン上に展開された以上は，自壊（self-destruct）関数が埋め込まれていない限り，機能停止できない。しかし，ユーザインタフェースを提供する主体に規制を及ぼし[9]，使い勝手を悪くするなどして，違法性のある分散型アプリを休眠状態に追い込むことは不可能でないであろう。

前述した予測市場は，リスクヘッジという点でデリバティブやP2P保険に類似した機能を営むので，金融規制にも抵触しうる。ところが，取引所等の仲介業者を名宛人とする規制は，スマートコントラクトを利用し，運営主体の存在しない予測市場には適用できない。米国商品先物取引委員会（CFTC：Commodity Futures Trading Commission）の委員長であるBrian Quintenz氏は，個人的資格で2018年に行った講演[10]において，スマートコントラクトを利用した予測市場が同委員会の管轄に服するとの仮定に立った上で，コード開発者に規制が及ぶかを検討した。そして，いったんパブリックドメインに置かれたスマートコントラクトを個々の利用者がどのように使用するかについては統制できないとの開発者側からの反論を予期しつつも，開発者は，コード作成時点で規制に反する使用がなされる可能性を合理的に予見できたならば，違反の幇助者としての責任を問われることがあるとの見方を示した。

証券規制の対象となるトークンの発行やその取引の場の運営も，スマートコントラクトを利用すれば，発行主体や運営主体なしで行うことができる。前記The DAO事件に関し，米国証券取引委員会（SEC：Securities and Exchange Commission）は報告書[11]を公表し，その中で，仮想通貨の出資者に対してブロックチェーン上で付与されたトークンは，1933年証券法（Securities Act）および1934年証券取引所法（Securities Exchange Act）の適用対象となる「証券（securities）」に該当し，The DAOは証券の発行者であるとの理解を示した。また，2018年には，EtherDeltaというスマートコントラクトを利用したトークンの取引プラットフォームに関し，同委員会は，それが「取引所（exchange）」に該当し，1934年証券取引所法5条の下で登録されるか，登録免除の要件を備えるべきであったと判断した。そして，EtherDeltaの開発者で，その利用者を呼び込むウェブサイトの運営も行っていた者に対して，同条違反を引き起こしたとして，同法21C(a)条の下で排除措置命令を発出した[12]。このように，スマートコントラクトの技術自体は規制されないとしても，証券規制は様々な行為を対象とするので，周辺の行為主体に対して規制を及ぼすことができる。

多くの分散型金融アプリの共通項として，暗号資産の預託を受ける主体が存在せず，代わってスマートコントラクトがそれを管理することが挙げられる。しかし，アプリの運営を管理できる秘密鍵[13]をコード開発者が保持している例が多いのが実態であり，実質的な受託主体として開発者にカストディ規制が及ぼされる可能性もあるであろう。

分散型金融アプリは，多額の暗号資産を匿名で手軽に移動することができるので，資金洗浄規制（AML/CFT）とも緊張関係に立つ。分散型金融で使われた暗号資産を法定通貨に交換する際には，主体の存在する取引所（交換所）が利用されることになるので，当該交換業者を規制することで足りるとするか，それとも分散型金融の利用者に対しても何らかの規制を及ぼすべきかの政策判断が求められよう。

分散型金融のスマートコントラクトは，通常，ボーダレスなネットワークに展開されているため，いずれの国が規律管轄権を有するかも問題となる。金融規制では，一般に属地主義が受け入れられているが，その具体的基準には行為地や効果発生地等がある[14]。米国証券取引委員会は，IPアドレスに依拠して米国からのアクセスを排除する（geofencing）だけでは，米国の規律管轄から免れるには十分ではないとの見解を示している[15]。

〔注〕

1 https://ethereum.org/ja/whitepaper/.

2 https://twitter.com/vitalikbuterin/status/1051160932699770882.

3 スマートコントラクトは，一旦ブロックチェーン上に展開され，分散的に保持されると修正できない。ただし，コントラクトAに宣言された状態変数を更新するためのコードをコントラクトBに書き，Bを代理呼出し（delegate call）する関数をAに書いておけば，新しいコントラクトB2を作成し，それが新たな呼出先となるよう，呼出先を指定する引数（アドレス）を変えてAの関数を実行することによって，利用者がアクセスするAのアドレスは変わらないまま，実行されるコードをBからB2に切り替えることができる（https://docs.openzeppelin.com/learn/upgrading-smart-contracts）。

4 東京地判平成9年2月18日判タ964号172頁。

5 イーサリアムのスマートコントラクトを活用したAugurなどの例がある。

6 Augurのユーザビリティを高めるウェブサイトを運営するVeilというサービスが登場したが，法遵守の困難等を理由に閉鎖された（https://medium.com/veil-blog/next-steps-for-veil-133777c4a774）。

7 最決平成23年12月19日刑集65巻9号1380頁。

8 マルタの2018年革新的技術アレンジ・サービス法（Innovative Technology Arrangements and Services Act）第III編（Part III）は，技術を対象とする認証制度を定めている点で例外的である。

9 表現の自由と緊張関係に立つが，ドメインネームの使用差止めもあり得る。

10 GITEX Technology Week第38回年次総会（2018年10月16日）における講演（https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16）。

11 "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" Exchange Act Release No. 81207（2017年7月25日）.

12 In re Zachary Coburn, Exchange Act Release No. 84553（2018年11月8日）.

13 「管理者キー（admin key）」と呼ばれることがあり，それに紐付くアドレスのみが呼び出すことができるよう，分散型アプリ内の関数の条件を設定することができる。

14 詳しくは，拙稿「証券関係法規の規律管轄権とICO（Initial Coin Offering）」国際法外交雑誌117巻4号（2019年）9頁以下。

15 In re Block.one, Securities Act Release No. 10714（2019年9月30日）para. 10.