2018 年 9 月 13 日　森本紀行はこう見る

スマートコントラクトが作る映画「マトリックス」の世界

スマートコントラクトとは何かと問われて、明確な定義を返すことは誰にもできないでしょう。しかし、例えば、商品の売買契約において、一方で通貨の移動を暗号化するのならば、他方で商品の移動も暗号化すべきではないか、そうすることで、契約、即ちコントラクトは、スマートになるのではないか、そういう見通しはたちます。では、契約がスマートになるとは、どういうことか、そして、その先に何があるのか。

スマート（smart）という形容詞は、例えば、お金につけてスマートマネー（smart money）というとき、機をみるに敏な投資家、頭のいい投資家、巧みな投資家、悪い表現を使えば他人をだし抜く狡猾な投資家になるわけですが、契約につけてスマートコントラクト（smart contract）というときも概ね似たような意味になるのだろうと思われます。つまり、契約そのものが高度な知能を備えて巧みに約定内容を執行するということです。実際、そのような意味において、用語自体は確立されつつあるのでしょう。

しかし、大多数の人にとって、スマートコントラクトの具体像は描き得ないものであり、漠然たる想念すら抱き得ないものかと思われます。そのなかで、ひとつ間違いなくいえそうなことは、契約当事者の関与が契約の成立に限られ、成立した契約は当事者の関与なくして自動的に執行されるということならば、一種のプログラムのようなものだということです。

そして、スマートコントラクトがプログラムのようなものだとしたら、プログラムが走る電子情報空間が設定されなければならず、契約当事者間の完全な情報の対称性が確保される必要があるのですから、現在の技術環境のもとでは、ブロックチェーン上に展開されるのだろうと考えられるわけです。

具体性がないと全く理解できないので、例えば、極めて単純な物品の販売契約をもとに考えてみてはどうでしょうか。

A が B に X というものを売却する契約を考えます。この契約は、A と B という二つの当事者をもった一個の契約です。一個の契約ですが、A が X を B に引き渡す行為と、B が A に代金を支払う行為という二つの独立した行為を内包していますから、契約が成立しても、A と B の行為が完了しない限り、契約は終了しないのです。

これをスマートにすると、契約が成立し、そのなかで引き渡し期日を約定しておくことにより、期日が到来したとき、自動的に電子情報空間の記録が変更になって、X に関する所有権者の記録上の名義が A から B に移転し、資金管理口座の残高の記録が代金分だけ A において増加し B において減少します。まさに、プログラムが自動執行されたのと同じことです。

つまり、スマートコントラクトにおいては、契約が成立した瞬間に、約定内容に忠実に将来時点の記録が書き換えられ、契約は終了しているのです。このことは、契約とは、当事者が約定された内容に従って行為することを予定している以上、当然のこととも考えられます。

しかし、予定は予定であって、予定通りに行かない場合があるからこそ契約しておく、それが契約の本質ではないでしょうか。

事前に記録された通りに未来が生起していくのならば、スマートコントラクトは神の域に達するということかもしれず、誰も神になれないのならば、スマートコントラクトは不可能である、確かに、そう考えるべきかもしれません。

契約においては、予定に齟齬した場合に備えた条項を含めたり、全く想定し得なかった事情変更についても当事者が誠意をもって事態の打開を図る義務を負うように定めたりして、不確実な未来に対処しています。そこに契約の本質があるとすれば、スマートコントラクトは契約ではなく、不確実な未来を完全に予測し得ない以上、一般的には不可能である、それが現在の技術水準における通説なのでしょう。

しかし、逆にいえば、特殊な条件のもとで、一定の技術が確立しさえすれば、スマートコントラクトが可能になると考えるほうが知的に進歩的であり、創造的であろうとも思われます。

ところで、スマートコントラクトにおいては、仮想通貨による決済が前提にされているようですが、法定通貨による決済はできないのでしょうか。

法定通貨の利用は絶対に不可能、逆にいえば仮想通貨の利用が絶対不可欠の要件なのかは、よくわかりません。しかし、必須の要件として、スマートコントラクトは一個のプログラム的なものとして完結していなければならないのですから、資金決済は、その一部に完全に内包されなければならないのです。この条件を成就させるためには、仮想通貨の利用が不可欠になるのではないかと想像されます。

また、技術的には、仮想通貨の電子情報空間が先行し、そこに商取引を結合させることで、スマートコントラクトへの道が開かれたと考えるべきかもしれません。実際、どのような商取引を実行するにしろ、必ず資金決済を含むわけですから、スマートコントラクトを資金の方向から構想することが自然なのでしょう。

哲学的な話ですが、普通の契約の場合は、当事者の履行行為が事実を変動させるわけですが、スマートコントラクトの場合は、記録が事実を変動させると考えていいのでしょうか。

スマートコントラクトでは、当事者の履行行為を必要とせず、契約そのものが自己を履行するといってもよく、契約の成立自体において未来の履行が完了するのですから、その時点で事実関係が変動するのだと考えるほかないでしょう。哲学的には、ひとたび契約が成立すれば、その後は、神の書いた筋書きに従って歴史が自動的に展開すると考えるのと同じだと思われます。

故に、ここに、スマートコントラクトの決定的難点が露呈するのです。問題は、不動産の登記になぞらえてみれば、すぐにわかることで、スマートコントラクトの前提は、いわば登記されていることを権利関係だと認めるのと同じですから、登記内容の絶対的な真実性という限りなく非現実的な想定をおかざるを得ないことです。

もちろん、現実には、登記内容の誤りや改竄を完全に防ぐことはできないので、日本では、登記の公信力を認めていないのです。公信力の付与というのは、登記内容を真実だと信じて取引を行ったものを法律的に保護することです。

逆に、スマートコントラクトになじむものの代表に、登記制度があげられているようですが。

そこに、スマートコントラクトを支持する人の自信が表れているのです。要は、絶対に誤謬や改竄が起き得ない登記制度を技術的に実現させればよく、そこに使われる技術こそ、仮想通貨やスマートコントラクトを支える技術と同じものなのだということです。

不動産の登記制度に限らず、理論的には、同様な権利関係を記録する仕組みを多くのものに拡大することができ、また、技術の進化により、その拡大を急加速させることができるのならば、それだけ、スマートコントラクトの適用範囲も拡大するということです。例えば、自動車等の機材のレンタルやリースなど、考えれば直ぐに多様な適用の可能性に思い当たるはずです。

絶対に誤謬や改竄が起き得ない記録方法は、技術的に可能なのでしょうか。

誤謬や改竄とは何かという問いは、裏返せば、真理とは何かという問いになるわけで、哲学的というよりも、もはや完全に哲学の領域に属することです。

さて、誤謬や改竄とは何かといえば、同一の権利を主張するものが複数発生してしまうなど、権利関係に矛盾が生じる事態にほかなりません。従って、真理とは何かといえば、ある権利を主張するものに対して、反論が生じ得ないことです。反論できないということは、自ら主張し、また他人の主張に同意したことについて、後に、それを自ら否定することはできないということです。

簡単な例でいえば、ケーキを二人の間で真に二等分するということは、問題を転換して二人の間で絶対に紛争が起きないように切るということですから、二人の間で、一方が切り、他方が先に自分の好きなほうを取るという手続きを合意することにより、実現できるということです。

また、ある特定のものについて、一定期間中、多数当事者間で活発な売買がなされたとき、その期間中の取引データを当事者全員が共有し、そのなかの誰かが各自の期末残高データの正しい値を算出して他の全員に配布し、各人が自己の取引履歴を参照して正しさを確認するという手続きを定めておけば、その手続きのもとで正しいと合意されたデータは、紛争の不可能性という意味で、絶対的真理になるわけです。

こうした合意形成の技術的な仕組みは、多年、多方面から研究されてきたのでしょう。そして、例えば、その一つの成果がブロックチェーンに結実したのだと考えられます。

では、その合意形成手続き自体における瑕疵、あるいは、それに対する不正、例えば合意の捏造等はあり得ないのでしょうか。

その不可能性を証明するのがビザンチン将軍問題（Byzantine Generals Problem）であって、ここまでくると、最高度に技術的で判断しかねるわけですが、仮想通貨やスマートコントラクトを支持する側からいえば、ビザンチン将軍問題は解かれたことになっているのでしょう。ただし、ここには、おそらくは、不存在証明の不可能性と同じ困難があって、絶対に不正は起き得ないという保証はないのかもしれません。

仮想通貨やスマートコントラクトの場合、不正があったときも、不正が変更不能な真実になってしまうはずですから、非常に危険ではないでしょうか。

飛行機は墜落する、阿蘇山の破局的噴火により火砕流が四国の伊方原子力発電所に達する、どこにもリスクはあります。要は、リスクを許容することによって享受される利益との関係において、リスクを許容できるかという社会学的問題に帰着するだけのことです。

暴論を吐けば、仮想通貨やスマートコントラクトの場合、危険とはいっても、飛行機や原子力と違って生命の安全にかかわることではなく、所詮は経済の問題なのですから、分野によっては、許容できるリスクも大きくなるのではないでしょうか。

スマートコントラクトがスマートになりすぎる危険性はないのでしょうか。

スマートコントラクトを哲学としてとらえると、事実の変更が記録されるのではなく、記録の変更が事実を変更することになるので、その極限において、私に関する記録が変更されると、私が変化することにならざるを得ないわけです。

さて、この映画「マトリックス」の世界があり得るかということですが、理論的には、あり得るのではないでしょうか。少なくとも、絶対にあり得ないとはいえないでしょう。もっとも、感覚的には、その確率は阿蘇山の破局的噴火の確率よりも小さそうですけれども。

以上