1. 現スマート コントラクトの限界 vs ハイパースマート コントラクト

「スマート コントラクト」の概念は、イーサリアム ブロックチェーンの悪評と分散型台帳技術に対して高まった需要が原因で、一般的な名称になりました。しかし、そのアイデア自体は新しいものではありません。仮想通貨の研究で知られる暗号研究者のニック・サボー（Nick Szabo）は、1996 年にすでにスマート コントラクトについての論文を執筆しています。サボー氏は、スマート コントラクトという用語を、どちらの当事者が契約を遂行するかを定めたプロトコルを含む、デジタル形式で明記された一連の契約と定義しました。

また、同氏が 1996 年に発表した論文では、デジタル革命により、現行の契約締結方法が一変するだろうと予測されています。以前はコストがかかり過ぎたアルゴリズムも、コンピューターでの実行が徐々に可能になっており、サボー氏が「スマート コントラクト」と称したものに対するアルゴリズムがいずれ開発されると同氏は早い段階から予見していました。ブロックチェーン ベースのスマート コントラクト、または自己実行型コントラクトは、非常に簡易で厳正な一連の条件（例えば、トリガーとなるイベントを伴うオプション契約またはエスクロー契約）に基づいて自動的かつ安全に、また仲介業者を挟む必要なく、義務の遂行と仮想通貨の支払いを行うよう開発されました。スマート コントラクトの活用によりビジネス チャンスはいくつも生まれますが、その**重要な制限事項**は慎重に考慮されるべきです。

まず初めに、イーサリアム プラットフォームにおけるスマート コントラクト実装の現状は、完全に安全とは言えません。プログラミング言語における、危険かつ短絡的な設計上の選択は、多くのビジネスにとって致命的な影響をもたらしかねません。私たちはすでに DAO の不運な結末で、その例を目の当たりにしています。それ以来、スマート コントラクトにおけるその他多くの脆弱性が報告されています（N. Atzei, 2017）。

次に、行動、言語、文章の形で締結された契約とは対照的に、スマート コントラクトは、コードに組み込まれた「単なる」コンピューター プログラムです。当事者は存在するのか、もしくはただの非中央集権のコンピューター プログラムであるのかといった、法律的観点から見た場合に、契約として見なされるのかは未だに不明瞭です（Lauslahti, Mattila, & Seppälä, 2017）。加えて、スマート コントラクトは非常に「厳格」です。なぜなら、利用規約はコードに組み込まれているため変更することができず、人間のみが判断できるような、実生活の多様性や構成における調整の要求に対応することができないからです。

http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

さらに、もう一つの大きな問題として、他のあらゆるコードと同様に、スマート コントラクトは欠陥が生じる傾向にある点が挙げられます。ただ他のコードとは違い、スマート コントラクトは書き換えを行うことができません。つまり、一度デプロイしたコードに深刻な欠陥がある場合、スマート コントラクトは、それに依存するシステム全体に極めて有害な影響を及ぼす恐れがあります。

さらなる制限として、外部的事象に対するスマート コントラクトの動作を変更することが、設計上不可能である点が挙げられます（ブロックチェーンにおけるすべての状態の変化は、完全に確定的でなくてはいけません）。これは、現代のバリュー チェーンが非常に複雑であるという事実（世界中の iPhone サプライヤー ネットワークを思い浮かべてみてください）と対照的であり、確率的かつ動的な自動最適化、および何兆もの処理ベース取引の実行に使用する AI、機械学習、ビックデータ解析のアルゴリズム（本書では「ハイパースマート アルゴリズム」または単に AI アルゴリズムと定義）に対する需要はますます高まります。

「契約」というよりは、「取引」の方がスマート コントラクトを説明する用語として適切でしょう。本来ならばスマート コントラクトは、非中央集権型組織だけではなく、既存の中央集権型または分散型ビジネス モデルも自動化するはずです。しかし、商品の流れ（「どの商品がどこから誰に、どのような経路をたどって配達されるか」）、情報の交換（文書を含む）、そしてお金（支払い）の観点から言えば、バリュー チェーンはアルゴリズムによってすでに自動かつ最適な稼働が可能という事実にもかかわらず、ここの参加者間での信用の欠乏、および手続き上の制限が原因で、これらのバリュー チェーンは未だに準最適のままです。結果として、商品の流れは AI アルゴリズムで可能になるスピードよりも遅く、管理上および支払いサイクルの面倒な処理によって、いわば「制約」を受けています。

この問題に対する決して高価ではない解決策は、AI アルゴリズムとブロックチェーン技術の融合であり、これはハイパースマート コントラクトの新しい概念を創出します。ハイパースマート コントラクトは、情報と文書の非中央集権型管理、正常な実行による仮想通貨の即時決済などを含む、複雑な商取引を最適化および自動化します。

事実、2017 年 11 月 6 日、正体不明の人物が Parity のマルチシグネチャー ウォレットの機能が依存していたスマートコントラクトを削除し、3 億ドル相当のイーサリアムが凍結された。参照: http://read.bi/2hHcDiK （最終確認: 2017 年 12 月 18 日）Parity は前回のバグを 7 月に修正。3200 万ドル相当のイーサリアムが盗難にあった。