FERI INFORMATION

進化するインターネット

中村 宇利
（一般社団法人情報セキュリティ研究所　代表理事　）

世界中のすべての国々が現在進行中のパンデミックによって、破壊的な被害を被った。

今も侵略者によって国土を破壊され、自国の明日を見いだせない国がある。

世界が分断され、互いに会うことさえ難しくなってしまっても、私達にはインターネットという素晴らしい道具がある。リアルタイムで互いの状況を確かめられるだけでなく、メールやチャット、ビデオ電話/会議で、互いを慰めあい、元気付けられる。さらには行政サービスやビジネスの一部までネットで済ませられるようになった。

しかし今でも、インターネットで利用できるのは情報だけだ。経済の血液とされるお金を決済するためには、専用の決済用ネットワークを使用しなければならない。インターネットでは、これらの決済ネットワークへの決済指示や、着金通知を受け取ることだけしかできない。

世界が分断と破壊から立ち上がるには、世界の金融システムの抜本的改革が必要である。すべての人々が等しく自由に使える金融（決済）ネットワークが必要だ。もしインターネットで本物の現金が扱えたら。特定の金融機関や、赤の他人と共有の台帳に記録されることもなく、匿名で使え、硬貨や紙幣のように財布から財布へ直接送金出来たら。山奥や海上や災害時などインターネットに繋がってないときでも使えたら。世界中の誰もが願う究極のお金。これこそがデジタルの現金である。仮想などではなく、台帳など必要なく、硬貨や紙幣のように使えるデジタルの現金。国家が発行するデジタルの現金、CBDC（Central Bank Digital Currency、中央銀行デジタル法定通貨）が、全国民を等しく、お金の偏在というくびきから解き放つ。

このデジタルの現金を実現するため、世界中の研究者がしのぎを削ってきた。特に 1980 年代から台帳など使わない「現金」を作ることを目的とした様々な試みが行われ、巨額の資金が投入された。最大の壁は情報セキュリティであり、未完の暗号技術が致命傷となって、すべてが 21 世紀を待たずに消えていった。

それでも人類は、デジタルの現金に想いを寄せてきた。台帳を使うという古い概念を持ち出して、「仮想」と注意書きが付いていても「通貨」だから同じようなものだと自分自身を言い聞かせる人がいる。毎日事件、事故が起こっても、それは技術の問題ではなく使う人の問題だと事実を歪曲して信じ込む人がいる。ブロックチェーンは膨大なエネルギーと計算資源を必要とする相互監視システムに過ぎない。ブロックチェーンに対する賛辞のすべてが間違っているにも関わらず、それほどにデジタルの現金は魅力的である。仮想通貨には批判的な人でも GAMFA の寡占（Web2.0）から逃れようとする人々はブロックチェーンを用いた Web3.0 には期待する。たとえ相互監視であろうとも、毎日事件が報道されても、一部の企業や国家に牛耳られるよりましだという。その中心的サービスで

ある NFT（Non-Fungible Token）に対する関心の高さは異常な程だ。NFT を用いれば、誰でもデジタル著作物を提供でき、さらにネット上での特定、登記、譲渡ができるという。その結果、インターネットにおける、唯一の成功ビジネスモデルと言われる広告モデルだけでなく、リアルな世界の様々なビジネスモデルも可能となるという。

デジタルの現金は、超高速に暗号解読を行うことができるとされる量子コンピュータにも耐えられる情報理論的安全性に基づいた完全暗号によってのみ実現される。従来の暗号は、有限の計算能力を有する攻撃者を想定したとき、現実的な範囲の時間では暗号が解読されることがない「計算量的安全性」を基に作られた。現在のネット通信でも主流の公開鍵暗号方式や、80 年代から 90 年代にかけてのデジタルの現金を作るための暗号などほとんどの暗号方式はこれを基にしている。ところが、今世紀に入って量子コンピュータが急速に発達し、実用が間近に迫ると、暗号技術に対する現実の脅威となってくる。本格的な量子コンピュータ時代においては、「情報理論的安全性」に基づく、どれだけ時間をかけても決して解読されない完全暗号が必要とされる。台帳方式（バーチャル）ではない、現金方式（リアル）の暗号技術を用いる貨幣発行・管理技術は「Crypto Cash」と名付けられ、ようやく完成した完全暗号によって実用化された。この Crypto Cash によるデジタルの現金は、所有者に正確に保管され、正確に譲渡される。面倒な台帳など必要としない。

インターネット上で現金を扱うことを目的として、すでに各国で CBDC の導入検討が始まっている。ちなみに発展途上国では、従来のブロックチェーンによる CBDC への応用も検討されているが、ブロックチェーンが包含する、緩慢な決済時間、台帳の肥大化、それ故の膨大な電力、計算資源の消費に悩まされている。CBDC どころか、はるかに小規模の従来の暗号資産の運用さえ禁止し始めた国々はすでに 50 カ国を超えるとされる。その上情報セキュリティ上の脆弱性は致命的で、毎日のように巨額の盗難事件が発生している。

ついにインターネットは情報だけを扱う情報共有ネットワークから、情報と価値を扱う情報＆価値共有ネットワークに進化する。デジタルの現金以外にも、様々な価値を特定し、その正確な移動を実現する。誰もが自分の意志で、価値の所有を証し、価値を移動する。当事者だけがこれらの情報を共有し、他人に監視されることはない。Web3.0 の実現が未熟な技術故に困難であろうとも、インターネットそのものが進化することで、Web3.0 の理念は受け継がれ、人類は再び自由を手に入れる。インターネットは誰かのものでも、誰かの支配下でも、誰かの監視下でもない、自由のインフラとして完成する。

以上