

分散型ウェブ「Web3」の思想分析 ——歴史学的アプローチから

1・はじめに——Web3を歴史的に定義することの困難

Web3の歴史を論じる際、最初にして最大の問題は対象の定義そのものにある。「Web3」「Web 3.0」「分散型ウェブ」はしばしば互換的に用いられるが、本来は同一ではない。インターネットの父と呼ばれるティム・バーナーズ＝リーらが2006年に提示したセマンティック・ウェブは、情報に機械処理可能な意味(メタデータ)を付与し、データの発見、統合、再利用を促進する「現在のウェブの拡張」であった。これに対し、2014年に実業家で仮想通貨イーサリアムの共同創設者であるギャビン・ウッドが論じたWeb 3.0は、ブロックチェーンやP2P通信、暗号技術を用い、信頼すべき仲介者を減らす「ポスト・スノーデン型」のウェブである。したがって本報告では、後者の系譜をWeb3と表記し、セマンティック・ウェブと区別する。

もともと、政策文書や産業界の言説では、この区別は必ずしも維持されていない。日本のデジタル庁『Web3.0研究会報告書』は、Web3.0を単一の技術として定義せず、「分散アプリケーション環境と、その下で構築される世界観」として扱い、暗号資産、DeFi、NFT、DAO、DID、メタバースまでを関連領域として列挙する。他方、経済産業政策では「ブロックチェーン上でトークンを媒体として価値の共創・保有・交換を行う経済」という経済圏の意味が前面に出る。米国政府のデジタル資産政策も、ブロックチェーン、スマートコントラクト、DeFi、デジタル資産を詳細に論じながら、Web3を一貫した制度概念として確定してはいない。ここでの曖昧さは単なる用語上の混乱ではない。Web3が、技術、産業、経済圏、社会像、政治思想を同時に指す「運動概念」であることを示している。

方法論上、本報告は「Web3」という呼称を過去へそのまま投影しない。ビットコイン以前の暗号通信、電子現金、P2P、オープンソースをすべてWeb3の前史として回収すれば、歴史は現在を準備する直線的な物語になってしまう。そこで、同時代の一次史料が用いた問題設定と語彙を確認したうえで、後代のWeb3言説がそれらをいかに引用し、接続し直したかを区別する。分析対象は技術の発明順序だけでなく、設計文書、宣言、政策文書、企業のサービス説明に現れる「信頼」「分散」「所有」「プライバシー」の意味変化である。

ゆえに歴史学的分析では、Web3の本質を現在の定義から遡及的に確定するのではなく、各時代の担い手が何を問題とし、どの技術に解決を託し、後代がそのうち何を選択してWeb3と呼んだのかを問う必要がある。本報告の中心的な仮説は、Web3とは初期インターネットとサイファークの単純な到達点ではなく、両者の思想をトークン経済に適合する形で選択的に再編したものである、というものである。

2・初期インターネットの思想からサイファーク運動へ

初期インターネットの分散性は、後世に語られるような全面的な反国家・反企業思想から生まれたわけではない。ARPANET以来のネットワークは、

公的資金、大学、研究機関、企業、標準化団体の協働によって形成された。そこで重視されたのは、異種ネットワークを接続する相互運用性、障害に対する頑健性、特定用途に固定されない汎用性であった。エンド・ツー・エンド原則は、可能な限り機能を通信網の内部ではなく端末側に置き、ネットワーク中核を単純に保つという設計上の判断である。RFC 1958 も「知性はエンドにある」と整理した。この原則は利用者や開発者がネットワーク所有者の許可を得ずに新しい応用を追加できる環境を支えたが、それ自体が国家や組織を不要とする政治綱領だったわけではない。

また、IETF に代表される標準化文化は、公開された文書、参加可能な討議、緩やかな合意、動作する実装を重視した。ここでは権威の否定よりも、権威を単独の主体に独占させず、異なる実装が接続できる共通規則を形成することが重視された。すなわち初期インターネットの分散性とは、無統治ではなく、開放的な標準と多元的な制度による統治であった。この点は、後に「コードだけで中央管理を代替する」と語られる Web3 像との重要な差異である。

1980 年代末から 1990 年代に登場したサイファークは、この技術的分散性に、より明確な政治的意味を付与した。ティモシー・メイの「クリプト・アナキスト宣言」は、暗号化された通信、匿名的な契約、追跡困難な取引が、課税、規制、秘密管理、信用のあり方を変えると予測した。エリック・ヒューズの「サイファーク宣言」は、電子時代の開かれた社会にはプライバシーが必要であり、それは政府や企業の善意ではなく、匿名決済、電子署名、暗号、匿名通信システムを自ら実装することで確保されると主張した。「サイファークはコードを書く」という標語は、政治的要求を法制度への請願ではなく、作動する技術へ翻訳する態度を象徴する。

この系譜の中間には、デイヴィッド・チャウムの匿名電子現金、アダム・バックの Hashcash、ウェイ・ダイの b-money など、暗号技術によって決済と信用を再構成する複数の試みが存在した。重要なのは、ビットコインが無から生まれたのではなく、電子署名、ハッシュ、プルーフ・オブ・ワーク、P2P 配信という既存要素を、中央発行者なしに取引順序を合意する制度へ統合した点である。この統合によって、サイファークの規範は、継続的に稼働する経済ネットワークとして可視化された。

ただし、サイファークの内部にも差異があった。国家規制から離脱する暗号アナキズム、言論・通信の自由を守る市民的自由論、プライバシー保護技術を実装する工学的実践は、重なりながらも同一ではない。さらに彼らの中心的関心は、今日の Web3 で強調される「デジタル資産の所有」以上に、通信内容や実名を秘匿し、監視者が個人情報収集できない状態を作ることにあった。初期インターネットの開放的標準とサイファークの暗号的自己防衛が交差した地点に、中央機関を介さない電子現金という課題が現れたのである。

3・サイファーク運動から Web3 へ

2008 年のサトシ・ナカモト論文は、サイファークが長く追究してきた電子現金の問題に、P2P ネットワークとプルーフ・オブ・ワークを組み合わせた解答を示した。論文の出発点は、インターネット商取引が金融機関とい

う「信頼される第三者」に依存しているとの批判である。ナカモトは、二重支払いを防ぐ中央機関の代わりに、取引履歴を公開し、参加ノードが計算量に基づいて単一の履歴へ合意する仕組みを提示した。ここでは「信頼」は消滅したのではなく、制度的主体への信頼から、暗号学的証明、経済的誘因、分散的な検証手続への信頼へ置換された。

ビットコインがサイファークから継承したのは、第一に仲介者への不信、第二に公開鍵暗号による仮名的参加、第三にコードとプロトコルによる規則執行、第四に国境を越えて参加できるネットワークである。他方、そこには変容もあった。ヒューズが重視した「取引の選択的開示」や通信の秘匿に対し、ビットコインは全取引履歴を公開台帳に記録する。利用者は実名ではなく公開鍵で表現されるが、取引分析によって関連づけられ得る。つまり匿名性は完全な不可視性ではなく、公開性と仮名性の組合せへ変化した。また、プライバシーを守る道具という理念に、希少なデジタル資産を保有し、ネットワーク参加者へ経済的報酬を与える仕組みが結合した。

この転換をウェブ全体の構想へ拡張したのが、ギャビン・ウッズの2014年の論考である。ウッズは Web 3.0 を、組織や政府が情報を濫用し得るというスノーデン事件後の認識に立つ「ゼロトラストの相互作用システム」とした。公開情報は分散的に公開し、合意すべき情報はコンセンサス台帳に置き、私的情報は暗号化して開示しない。さらに、静的コンテンツ配信、仮名的メッセージング、トラストレスな取引、統合ユーザーインターフェースを組み合わせ、中央サーバーと権威への依存を減らす構想を提示した。ここでは Web3 は暗号資産市場の別名ではなく、通信、保存、名前解決、合意、アプリケーションを再設計する包括的なインターネット像であった。

しかし、その後に普及した Web3 言説では、この四要素のうちコンセンサス台帳とトークン化が突出した。プライバシー保護通信、端末間メッセージング、分散ストレージは周縁化され、「読む・書く・所有する」という簡潔な発展段階論が広まった。この語りは Web3 の新規性を説明しやすい一方、Web1 を単なる閲覧型、Web2 を単なるプラットフォーム型として単純化し、電子メール、ウェブ標準、P2P、自由ソフトウェアなど、従来から存在した分散的实践を見えにくくする。Web3 は過去を継承しただけでなく、自らを歴史的必然として提示するために過去を再編集したのである。

4・換骨奪胎された Web3？——商業化と再中央集権化

2020 年代に Web3 が投資・産業政策の語彙となるにつれ、その意味は「中央管理者に依存しないウェブ」から「ブロックチェーンを利用する事業領域」へ拡張した。NFT 市場、暗号資産交換所、ウォレット、RPC 接続、クラウド上のノード運用など、利用者とブロックチェーンの間には多数の仲介サービスが形成された。モクシー・マーリンスパイクは、一般利用者が自らノードを運用せず、ウォレットやアプリが少数の API 事業者の応答を信頼している点を指摘した。ブロックチェーンの台帳が分散していても、入口、表示、検索、鍵管理、クラウド、開発者向け基盤が集中すれば、利用経験と市場支配は再び中央集権化し得る。技術面から Web3 を検討した研究においても、現

行サービスが従来型インターネット・インフラへ依存していることが指摘されている。

ビッグテックによる Web3 も、この矛盾をよく示す。AWS は Amazon Managed Blockchain を、パブリックおよびプライベート・ブロックチェーン上で Web3 アプリケーションを構築するための「フルマネージドサービス」と位置づける。Google Cloud もノード運用、RPC、データ分析、スタートアップ支援を Web3 事業として提供する。これらは開発コストを下げ、障害耐性や普及可能性を高める一方、Web3 への接続を巨大クラウド事業者のアカウント、API、課金、運用判断に依存させる。「分散型サービスを中央集権的クラウド上で効率的に提供する」という形容矛盾は、単なる偽善ではなく、利用者が自らサーバーやノードを管理したがないというインターネット史上反復されてきた問題への市場的解答でもある。

この変化は「理念の裏切り」とだけ理解すべきではない。分散化には、単一障害点を減らす技術的分散、意思決定権を配る政治的分散、資産や報酬を配る経済的分散、複数事業者が競争できる市場的分散がある。Web3 の商業化は、技術的分散を維持しながら運用と市場を集中させる場合もあれば、中央企業がオープンなプロトコルへの接続を提供することで市場参入を広げる場合もある。したがって企業参加の有無ではなく、依存先の代替可能性と権力の可視性を検証する必要がある。

したがって Web3 の現状を、理念の完全な失敗か、技術の必然的進化かの二者択一で評価することはできない。歴史的にみれば、分散化は常に複数の層から構成されてきた。台帳が分散していてもインターフェースは集中し得るし、企業が運営していても標準やデータ形式が開放され、退出や移行が容易であれば利用者の自律性は一定程度確保される。逆に DAO やトークン投票を採用しても、初期保有者、開発チーム、取引所、クラウド事業者へ権力が集中することはあり得る。問うべきは「分散しているか否か」ではなく、技術、経済、ガバナンス、インフラの各層で、誰が規則を変更でき、誰が排除され、利用者がどこまで検証・移行・拒否できるかである。

本報告の結論は、Web3 が初期インターネットとサイファーパンクの思想を継承しつつ、その重点をプライバシーと相互運用性から、所有、交換、インセンティブへ移したということである。Web3に残ったのは、仲介者への不信、暗号による自己防衛、オープンな参加、コードによる規則形成であった。他方で薄れたのは、データをそもそも収集させないプライバシー、非商業的な公共財としての標準、複数の制度主体が支える多元的統治である。Web3 の思想史は、分散化が中央集権の単純な反対語ではなく、時代ごとに異なる主体が異なる目的で再定義してきた争点であることを示す。ゆえに Web3 研究には、ブロックチェーンの性能や市場規模だけでなく、その技術がどの過去を記憶し、どの過去を(意図的に)忘却することで正当化されているのかを問う歴史学的な視点が必要である。