第７部

非中央集権的なデータセキュリティとトラスト delight WGの設立

阿部 涼介、押川 拓夢

第１章　はじめに

2021年後半ごろより，ブロックチェーン技術などを礎にして，いわゆる“Web3.0”と呼ばれる新たなWebのアーキテクチャを模索する議論が活発に行われている[*1]．これらは，ブロックチェーン技術等を活用し，非中央集権的なスキームでデータセキュリティを担保することで，多様なアプリケーションのアーキテクチャを再考する動きと理解できる．また，その中でも“トラスト（信頼）”は重要なキーワードである．W3Cの新たな標準であるVerifiable CredentialsやDecentralized Identifiersは，ブロックチェーン技術に触発されて議論されたものではあるが，必ずしもブロックチェーン技術へ依存せずに活用が可能なものである[21、22]．こうした技術等を活用することで，インターネット上を流れる情報を検証可能にすることで，今まで暗黙のうちに信頼していた情報を検証可能にできると期待できる．

一方で，Tim Berners-Lee卿は，ブロックチェーン技術を活用する所謂“Web3.0”を“Web”と呼称することに対して批判的な立場を表明するなど，批判的な見方も存在する[23]．技術とは乖離した議論が散見されることも事実であり，これらの技術を活用し，中央集権的なエンティティに依存せず自律分散的かつ検証可能なデータ流通をデザインするためには，技術とそれらに実現される社会の両面からの冷静な議論が必要である．筆者らのグループでは，ブロックチェーン技術とそのアプリケーションに対して冷静な立場を取りつつも，研究開発を進めてきた．またWIDEプロジェクトの中でも，かねてより合宿でBoFやワークショップを開催してきた．更なる研究開発を促進し，これらの議論に貢献できる人材育成を目的として，筆者らはブロックチェーン技術をはじめとした非中央集権的な技術の研究活動を行う“Delight WG”を設立した．

第２章　Delight WG概要

Delight WGの設立申請時の活動内容及び活動計画を掲載する．

2.1　活動内容

ブロックチェーンに代表される非中央集権的な仕組みによるデータセキュリティの担保を礎にした様々なアプリケーションが注目を集めている．しかし，ブロックチェーンだけでは既存のインターネットが抱える問題は解決できず，データセキュリティをはじめとした技術的な視点および，それらによって実現が期待される社会の視点，両面からの研究開発が求められる．本WGは，ブロックチェーンを中心にデータセキュリティ，P2P等の下支えになる技術を含めた研究開発を行いながら，関連技術に取り組む人材育成およびコミュニテイ形成を目的とする．具体的には，以下のような研究に取り組むが，これに限らない多角的な視点から議論する．

- 非中央集権的なデータセキュリティの担保によって実現されるアプリケーション開発
- ブロックチェーン自体の標準アーキテクチャ /安全性検証/性能向上の研究
- 非中央集権的な情報システムと一体になった社会システムの検討

＊1　これらは既存の“Web3.0”と呼ばれる“Sematic Web”とは異なる．

• 関連技術に取り組む人材育成/コミュニティ形成

2.2 活動計画

本計画はブロックチェーンに着目した計画であるが，並行して他の関連領域に関する議論も他のWGなどと協調しながら実施する．

• 随時活動計画の更新・定例ミーティングの実施
• 2022/10 WG立ち上げとWIDE内での参加呼びかけ/対外組織との議論の座組み検討
• 2023/3 WIDE合宿における議論の進捗報告/アプリケーションの検討と求められる要件の整理
• 2023/6 アプリケーションの基盤としてのブロックチェーン等の技術に求められる安全性/性能の整理
• 2023/9 WIDE合宿における議論の進捗報告/ここまでの議論をもとにした技術・アプリケーションの実装
• 2023/12 議論の対外発表およびWIDE外を含めたコミュニティ形成のための座組の実装

2.3 2022年度の活動

2022年はWGの立ち上げを行い，キックオフミーティングを含む2回のミーティングと，12月研究会にてミーティングで行われた議論を紹介した．キックオフミーティングでは，WGに参加したメンバより研究アイディアのブレインストリーミングを行った．その結果，以下のようなアイディアが共有された．

• ブロックチェーン/Verifiable Credentials等の応用の議論
  – Verifiable CredentialsベースのWGメンバー証明書
  – デジタル住民票
  – 医療/ヘルスケアとVerifiable Credentials
  – メタバースとブロックチェーン*2
• ブロックチェーン技術の改善
  – 異なるブロックチェーン基盤の性能等の比較
    * 比較メトリックの検討
      · Proof of Work/Proof of Stake等異なるコンセンサスアルゴリズムの比較
    * ブロックチェーン基盤の計測
  – コンポーネントが疎結合なブロックチェーン基盤
    * アプリケーション基盤として仮想通貨を前提としないブロックチェーン
  – スマートコントラクトセキュリティ
  – 独自ブロックチェーン/性能評価のためのテストベットの構築

第3章 おわりに

インターネット上を流れるデータの信頼性を担保する試みは，内閣官房デジタル市場競争本部による“Trusted Web”など，多様な側面から議論が行われている[4]．ブロックチェーン技術は，そうしたデータおよび社会活動のプロセスの信頼性を向上させる技術として期待が高まる一方，課題の多く残る技術である．必ずしもブロックチェーン技術ありきではなく，自律分散的に動作するインターネット上で，中央集権的な権威者に任せず，どのようにデータの信頼性を担保できるかという目的ベースで議論することが肝要である．また，その目的に貢献するべく，ブロックチェーン自体も改善及び応用の議論を継続して行っていくことが重要であると考えられる．2023年度はこれらの議論を進めながら，人材育成に関する取り組みについても勉強会の開催などを計画している．

*2 SDM WGとの共同での議論を検討中である．