第１部

特集1 WIDEボード夏合宿（2021）開催概要

鈴木 茂哉、Rodney Van Meter、浅井 大史

第１章　はじめに

WIDEプロジェクトでは、毎年夏期休暇中に研究の先取りをするため、学び、戦略を構築するために、WIDEのボードメンバ主催の合宿である通称「ボード夏合宿」を実施している。トピックをボード会議で選定し、ボードメンバがチェアとなってプログラムを組み立て、実施される。

2021年の夏ボード合宿は、「Classical-Quantum Hybrid Human-Centric Internet Architecture」というテーマで、現在進行中である3つの重点活動領域を中心としたシステムアーキテクチャ議論を行った。

第２章　背景

WIDEプロジェクトでは、かねてよりインターネットのあり方について、機会を見つけ、様々な議論を行ってきている。一つの例としてあげられるのは、WIDE DESiGN[1]であり、WIDEプロジェクトにおいて「人間中心のデザイン」を文書にしたのは、当時の研究活動が初めてであったと記憶する。

一つ目の視点は、「インターネットアーキテクチャ再考」という視点であり、インターネットプロトコルの高度化に伴い複雑化したモデルを、データパスとデータフローサブレイヤの分離によるアーキテクチャ上の見直しを行おうというもので、これがここ数年のWIDEにおける "ReARCH" の活動となっている。

二つ目の視点は、量子インターネットである。量子インターネットの実現には、量子ビットに対する直接的操作が必要なのは言うまでも無いが、量子ビットに対する操作には古典的インターネットによる古典情報の通信が必要である（量子インターネットと区別するために「古典的インターネット」あるいは「Classical Internet」と呼ばれる）。通信と制御という視点でいうならば、これらは「量子データプレーン」を量子ビットの物理実装が担い、「量子コントロールプレーン」を古典的インターネットが担うという関係性がある。ReArchのようなアーキテクチャ再設計を考えるとき、量子インターネットアーキテクチャの実装を前提としたデザインを考慮するのは自然であろう。

三つ目の視点はインターネットにおけるトラストの拡大を目標とする Trusted Webである。2020年度に慶應義塾大学SFC研究所ブロックチェーン・ラボで始められたデジタルアイデンティティについてのホワイトペーパ[2]が公開され、本報告書の別の報告[3]にあるように、内閣官房デジタル市場競争会議におけるTrusted Web推進協議会[3]での議論へと発展している。ここで、WIDE DESiGN文書を読み直してみると、一見して直接関係ない議論がなされているようにも見えるTrusted Webが、WIDE DESiGNの議論が行われていたときに意識されていた「人間中心」コンセプト、すなわち、インターネットのアプリケーションレイヤデザインには標準として作り込まれていなかったデジタルアイデンティティ技術の分散協調型の実装とその活用とも表現できる。さらに、デジタルアイデンティティ技術の活用は、インターネットにおける通信を担うレイヤの高度化のために、識別子の用い方とともに再考すべき要素である。すなわち、一つ目の "ReArch" との関係もあることになる。

これらの視点から、将来のインターネットデザインを考えるためには、これらの最新活動領域における知識を共

有し、アーキテクチャの議論を進めることに意義があることが分かる。さらに、これらの領域は、WIDEプロジェクトの研究者が先導している領域でもある。

これらの背景から、2021年の夏ボード合宿は、これら最新三活動領域における理解を深め、インターネットアーキテクチャ再考の手がかりとすることを目的とした。

第３章　実施概要

実施概要を以下に記載する。

- オンライン、二日間 (2021/8/2 〜 2021/8/3)
- フォーマット:
  - イントロ(3トピック)
  - ブレークアウト
    チェアが恣意的にバランスを見て5グループへメンバ配分。二日間でほぼ同じメンバで構成
    - 一日目: 前提無しのClean-slate 志向の議論
      二日目: 現実志向の議論
  - まとめ

- 英語のみ
- 参加者数: ボード25名、一般10名 (一般: 量子インターネット系6名、IP系3名、Trusted Web系1名)

第４章　鍵となるリサーチクエスチョン

議論は、鍵となるリサーチクエスチョンを起点として進めた。以下、Foundation、Philosophy、Design の3点についてのクエスチョンを英文で挙げる。

4.1　Foundation

- From quantum side, I want to know why current internet is not mainly based on satellite. Technically difficult? If so, the same reason may be also true for quantum.
- From quantum Internet side, where can the quantum Internet contribute to solve the current Internet problems? (Just only on the security?)
- What are concepts on designing new distributed computing with a speed faster than light? (managing appropriately? -> after the concept, security? -> What is your security target? -> If not yet, let's talk after applications assumed.)
- From the application point of view, what is the key differences between quantum link and optical link, other than the level of synchronicity? (e.g. delay? bandwidth?), Based on that how we can adopt it on the architecture, or just considering trustworthy internet?
- How to scale non-E2E communication? What is the requirement to build non-E2E fundamental system which scale?
- What is the actual meaning of the identity in Future Internet? The discussion is based on the existing metrics such as actuality, linkability, revocation ability etc.
- What is the key application of Quantum Networking. In terms of cyber security viewpoint, it is not necessary quantum cryptography (but sufficient), but it is also applicable just a post quantum cipher such as lattice encryption.
- How will the impact on the network change in each situation where quantum computing is deployed in the cloud, at the edge, and on end devices?
- What is the impacts of new and significant improvement of hardware (layer 1 and 2) to the classical Internet architecture, including how to include (invite them to the Internet system) new segments with new L1/L2 technologies?. Same question by how to use the Internet.
- How do we handle changes at the operational level? What kind of trust layer is needed to support Shigeya's vision?
- Can we still maintain multiple "personalities" on the Internet? Anonymity and others
- What and how typical user use Quantum Internet?

4.2 Philosophy

- Is “clean slate” possible? Internet was designed as “clean slate” but additionally people brought tons of “desires” which requires patches to the original idea resulting a complex system. When we define a network architecture in “clean slate” basis, it may be okay then, but when it is deployed, many unexpected new requirements might be brought in and still need patch work extensively.
- Can we make a clean slate and deploy it while maintaining the interoperability to the current architecture or we need to switch entirely and cut off the old system and force them to use the new one?
- What rough architecture can we choose when we predict that its components will change drastically? (Current quantum internet is something like analog telephone network, but final goal will be internet (asynchronous network).
- Do we have a new concept/design principles/ philosophy for the new architecture?
- What is the concept (goal and principle) of the next generation of the Internet. Maybe, IOWN has clear goal, but I don’t think that is our principle.
- What are the problems and requirements (to solve them) of each projects which are not solved inside the individual project, but can be solved by other projects? If each project has dependency each other then we will have a good collaboration among them, but if there is no overlapping issues, then, what can we get..?
- On each topic have a discussion on their layer/field. Those of them can be combined with each other on their own layer. That can make the quite good layering on their field to make a fair abstraction. To make an abstraction, we need a philosophy on the next architecture. What will be that?
- Can we make *ONE* integrated Internet, or not? Should we?
- What is the future narrow waist to replace IP?

4.3 Design

- Should we consider long-term security (information theoretic security) in future internet?
- What should we do about resource management (multiplexing) in the Quantum Internet?
- For trusted web, how can we prevent copying or moving an attribute information (like PII). need to trust them? how can we detect the abuse of such data? can quantum internet help to solve these problems in the future?
- Will the user identity need to be used or needed down below application layer?
- How we can establish sustainable trust of information platform, or information circulating on it.

第５章　まとめと今後のアクション

様々な議論が行われ、議論の一旦のまとめとして、マインドマップ風にまとめたものが図1である。

最後に、今後のアクションをまとめた。

5.1 WIDEとQuantum Internet Task Force[4]のコラボレーション

- Meetings
  - Strategy meeting @Sept. WIDE Camp
  - 1/month C+Q seminar/info sharing session online, Sept-March(Bilateral seminars on important basic topics, 45 minutes C, 45 minutes Q)
  - Consider all-day tech meeting @December WIDE Meetings

- Shared technical work topics:
  - Concrete use cases: begins w/ info sharing, then figure out how deep it needs to go
  - Mux-ing & resource management: detailed technical work urgent (req, spec, simulation & emulation)
  - Naming: detailed technical work urgent (affects all protocols) (req, spec, sim & emu)

- AAA: principles & design; implementation not urgent
- Programming model: batch → adaptive → coprocessor → distributed (long term research)

- ReArchでは、名前に関連した議論を行う (人、量子インターネットにおける構成要素等)
  - Trusted Webとの連係

5.2 ReArch での活動

- Have Interim meeting
- Reviewing current internet architecture
  - Including discussion with with Mobile operators
  - ISPs, business side
- Trusted Web Discussion
- Launch discussion at WIDE September Camp
- ReArch maybe multiple-WG activity
  - Area ? Parent working group?
  - (Lessons: IAB at IETF is not discussing architecture)
- Discussion group at IPA on future architecture (oe, sekiya, panda)
- (discussion relates to 'K' Testbed)
- Freedom of Internet is important
- We're not under the control of Government

第６章　まとめ

夏合宿においては、Quantum Internet / ReArch + Trusted Web (Identity/Identifier) における深い議論ができた。特に、Quantum Internetを進める上での理解、(Classical) Internet をどのようにしてゆくかの礎が出来てきたと考えられる。今後の活動に結びつける予定である。

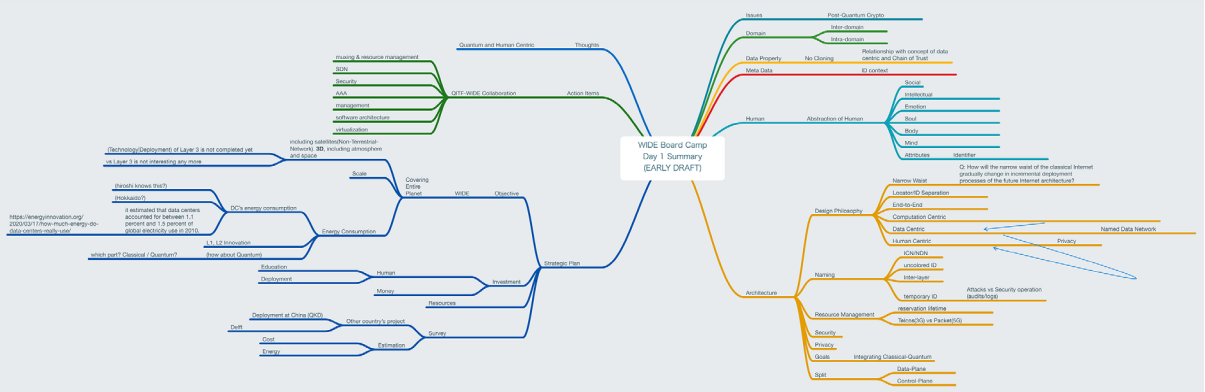

図1　MindMap - WIDE Board Camp Day 1 Summary-2021-08-03-0843