Computer Security Symposium 2017
23 - 25 October 2017

Web PKI と Bitcoin を事例にした 基盤技術の普及と信頼の社会受容に関する考察

林 達也[†1]　島岡 政基[†2]　砂原 秀樹[†1]

概要：インターネット上の信頼において Web PKI は社会の基盤として既に受け入れられているといってよい．これは RSA 等の暗号アルゴリズムや TLS 等のプロトコルといった技術面，関連製品のステークホルダーによる合意形成のコミュニティやガバナンス，インタラクションに関する教育や啓蒙を含んだ認知度向上等，様々な構成要素により成立している．一方，注目を集めている Bitcoin は既に経済に影響を与えており，価値の流通に関する基盤技術として今後社会に受け入れられる可能性がある．本稿ではインターネット時代の社会基盤における信頼の構成要素に関し，特に技術からのアプローチがどのように受け入れられるかについて Web PKI と Bitcoin を比較し考察を試みる．

キーワード：トラスト，公開鍵基盤，ブロックチェーン

Considered the spread of component technology and acceptance of trust into society with reference to Web PKI and Bitcoin

Tatsuya Hayashi[†1]　Masaki Shimaoka[†2]　Hideki Sunahara[†1]

Abstract: In trust on the Internet, Web PKI has already been accepted as the component of society. This includes various components such as technology aspects. cryptographic algorithms (RSA etc.) and protocols (TLS etc.), and more. Community and governance of consensus building by stakeholders of related products. Awareness raising including education and enlightenment on interaction. Meanwhile, Bitcoin attracting attention has an impact on the economy and there is a possibility that it can be accepted by society in the future as a component technology concerning the distribution of value.
In this paper, we try to compare Web PKI and Bitcoin with respect to the constituent elements of trust in the social infrastructure of the Internet age, especially how the approach from technology is accepted.

Keywords: Trust, Public Key Infrastructure, Blockchain

1. はじめに / Introduction

日本語では一言で「信頼」と表現される事象は実は非常に多義的であり，多くの側面を有する．特にインターネットが普及し情報社会を実現したといってよい現在では古典的な信頼の観点が変化し，結果として新たに技術と社会の二つの側面から捉え直す必要が生じている．

いわゆるサイバースペースにおける技術的な信頼に関しては，Public Key Infrastructure (PKI) を中心にした共通認識が進み，特に Web における PKI (Web PKI) は既に社会の基盤として受け入れられている．これは，RSA 等の暗号アルゴリズムや Transport Layer Security (TLS) / Secure Socket Layer (SSL)等のプロトコルといった技術的な側面から，CA/Browser Forum(CABF) [1]のような関係製品のステークホルダー(利害関係者)による合意形成のコミュニティやそこにおけるガバナンス，Pad Lock(鍵マーク) アイコンや Extended Validation (EV) SSL のグリーンバーの様なユーザーのインタラクションに関する教育や啓蒙を含んだ認知度の向上等，様々な構成要素により成立している．

一方, 近年目覚ましいほどの注目を集めている Bitcoin は，Crypto Currency (仮想通貨)として実際に現実の経済に影響を与えており，価値の流通に関する基盤技術として今後社会に受け入れられる可能性がある．

同時に，これらのウェブや Bitcoin の普及の背景には，暗黙の内にインターネットの技術的・社会的アーキテクチャが影響を及ぼしている．その典型的な例はドメインネームシステム(DNS)や，Internet Corporation for Assigned Names and Numbers (ICANN)や Internet Assigned Numbers Authority (IANA)に代表されるドメイン名や IP アドレス等におけるインターネットの資源管理の仕組みだろう．

本稿では，インターネット時代の社会基盤における信頼の構成要素に関し，技術からのアプローチがどのように社会に受け入れられるかについて Web PKI と Bitcoin を比較し考察を試みる．

1.1 動機と目的 / Motivation and Goal

本稿の動機として以下の三点がある．まず，現在進行形で社会受容されつつある Bitcoin が興味深い事例であるこ

†1　慶應義塾大学大学院メディアデザイン研究科
Graduate School of Media Design, Keio University
†2　セコム株式会社 IS 研究所
SECOM CO., LTD., Intelligent Systems Laboratory

と．第二に，Web PKI という既に社会に受容されたケーススタディがあり，これと Bitcoin を対比することで一定の成果が得られることが期待出来ること．最後に，これによって社会に受容されるにあたって必要な信頼の構成要素を洗い出し，Bitcoin や新しい技術の社会受容におけるあるべき姿の考察に繋げることである．その為，本稿の目的として以下を検討した．

1. 社会受容された基盤技術である Web PKI の背景にはなにがあるか？
2. 社会受容の視点で Bitcoin に今後必要になるものはなにか？
3. 洗い出された要因における受容者 = 利用者視点での要点はなにか？
4. 基盤技術における社会受容の決め手になる要因はなにか？

これらを踏まえてインターネット時代の基盤技術の信頼と社会受容に必要な要因を考察することとしたい．

特に，今までは信頼される側の視点で整理されてきたことの多い信頼の課題を，需要者 = 利用者 (ビジネス的な立場，そして消費者)の視点で整理することで，社会受容と信頼の関係性の明確化に繋げたいと考える．これは，社会受容されるということは，本稿を読み書きする我々のような人種によるものだけではなく，高齢者でも低年齢の子供(但し，教育や倫理の側面で議論の余地がある)でも受け入れられることを指すのではないかと考える故である．

1.2 手法と対象

歴史的経緯や事例を挙げ，Web と Bitcoin における社会受容の要因を洗い出し，分類した．

ここで，Web PKI と Bitcoin を比較するに辺り，いくつかの前提を明確にしておく．信頼を得るという点において，Trusted Third Party の存在を前提として明示的にトラストに取り組んでいる Web PKI に対し，一般にはトラストレスなどと言われている Bitcoin をどう捉えるか？著者らは，Bitcoin がインターネットを前提としてその上に構築されており，シードノードの検出に DNS を利用している点，Bitcoin Core と呼ばれるソフトウェアの開発とリリースを担っている開発者集団に事実上大きな権限がある点に着目し，これらが暗黙の信頼に応える体制になっていることなどを踏まえ，十分に比較が可能であると判断している．同時に，この比較によって明示的なモデル化がいまだ為されていない Bitcoin の暗黙の構成要素とその不足分を洗い出すことを目的としている．純粋に比較出来ない部分もあるが，技術面はあくまで一要素に過ぎず，比較の主眼は信頼が受容者からみてどう成立するかであり，インターネット上で普及する相互接続性のあるアプリケーションが如何にして信頼を獲得するかを確認し，そこにある全体の要因を比較することを目的とする．

2. 背景 / Background

2.1 信頼の多義性，多様性

信頼という単語は非常に曖昧であり，それを定義することはとても難しい．英語においても，Trust の類義語として Belief, Reliability, Confidence 等，多くの単語があり，日本語における信頼がどれを指すのかは状況によって様々である．

情報システムにおける技術的な信頼として，ISO/IEC では

> "degree to which a user or other stakeholder has confidence that a product or system will behave as intended" [2]

という定義がなされている．日本語に訳すと

> "ユーザーまたは他の利害関係者が，製品またはシステムが意図した通りに振る舞うという確からしさ"

だろうか．また，ここでは Trust の定義に Confidence という表現を使っており，Trust の概念は Confidence よりも大きなものであることが示唆されている．

技術に閉じない信頼の定義に関しては，以下のような表現があり，

> 「もし何も信頼することのできない人がいるとすれば，その人は既知の道を歩くこともできなければ，自室で眠ることすらできないだろう．」奥田秀巳．信頼の倫理学的考察．学位論文．広島大学 (Hiroshima University), pp.15, 2015. [3]

古典的には，

> 人間についての知と無知のあいだの中間状態 ― G. Simmel (1900)

> （信頼は）幾分神秘的で無形の要素とみなされており，おそらく慎重な定義を受け付けない ― Giffin (1967)

> 社会的な複雑性を縮減するメカニズムのひとつである．手元にある情報から与えられた以上のものを引き出すことによって成立する ― N. Luhmann (1973)

> (信頼とは) 不確実性がある状況で，(中略)相手の判断や意思決定に任せておこうとする心理的な状態 ― 中谷内一也 (2008)

などといった定義がなされている．本稿における信頼の定義においては， 上記の各種定義を踏まえつつ，英単語としては”Trust”を想定・対象とし，その主体を信頼する当事者，社会受容の観点における受容者の視点で

> 「"社会的な複雑性を縮減する" 目的で "自身が対象を評価する行為"」

を「信頼」とここでは表現することとしたい．

また本稿では，社会に受容されている状態を表現する目的で，Everett M. Rogers による”Diffusion of Innovations” [4] でのイノベーター理論における 5 つの分類，イノベーター，アーリーアダプター，アーリーマジョリティ，レイトマジョリティ，ラガードを使用する．

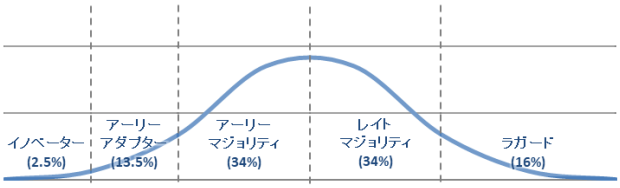

Figure 1

3. Web PKI の信頼構成要因

ここでは，標準化に携わった経験から，Web PKI における社会受容の観点での信頼の構成要因を洗い出してみたい．

3.1 文化的背景・ニーズとユースケース

ウェブの普及において，Web PKI の存在はおそらく欠かせない．過去，World Wide Web が普及していく過程で，安全な通信を望むニーズが生じたことは間違いない．初期は電子商取引等という単語で表現されていたそこには，明らかなニーズとユースケースがあった．もちろん，当時はそれが成功するかは未知であったが，成功に至る過程で必要になったものは重要な要素だろう．

これを支えた技術的要因は，なんといっても公開鍵暗号アルゴリズムの現実的な実装とデプロイメントだろう．ここで改めて触れるまでもないが，多様なユーザに情報を発信するウェブと公開鍵暗号の親和性は非常に高かったといえる．

3.2 コミュニティとガバナンス

ニーズに応える形で技術的な解決がなされた後に，およそ通信に関わる，つまりインターネット上の技術に関して確実に検討課題となるのが標準化である．標準化のプロセスは様々だが，標準化団体 (Standards Development Organization, SDO) と呼ばれる組織によって標準として認められることがほとんどである．標準化の目的は，少なくとも表向きはインターオペラビリティであり，そこにはアルゴリズム，プロトコル，フォーマット，振舞いや表示などの様々な要素がある．これらに関してステークホルダーで合意し，それを実装し，何かしらの手法でインターオペラビリティを担保し確認しつつ，利用者に届けること(デプロイメント)が SDO の最終的な目的といえる．Web PKI でいえば，RSA 等の暗号アルゴリズムや，X.509 等のフォーマットを含んだコンポーネント，SSL や TLS のようなプロトコル，実装としてのウェブブラウザや Web サーバーがある．

Web PKI のケースが興味深いのは，社会的な受容において，これらの技術的な要因だけではなく(Web PKI の)モデルにおける信頼性を担保するために認証局のルールやポリシーを普及の比較的初期から必要とした点である．(もちろん，Web PKI 以外にもインターネットそのものにおいても，資源管理等における ICANN や全体のガバナンスにおける Internet Governance Forum 等がある)

ステークホルダー同士の合意事項としての WebTrust for CA や，CA/Browser Forum のコミュニティ，そこにおけるルールやポリシーなどを整備することで最終的に今の Web PKI が実現されている．

3.3 デプロイメントとユーザビリティ

標準化もポリシーの実施も，最終的には利用者に使われることを目的としており，製品のデプロイメントとそれらのインターオペラビリティの確保もその為である．受容者の観点で見直した場合，これはユーザビリティを高めることが目的といっていい．快適に，安心して，実用的に使えるか，という社会受容と信頼そのものである．標準化においてデプロイメントが重要視されるのはこれゆえである．

また，デプロイメントとコミュニティの関係性において，利用者からの何かしらの問い合わせやフィードバックを受け取り，可能であれば今後に反映していく(と期待出来る)点も重要である．反映の実際に関してはプロトコル等のバージョンアップがわかりやすいが，その他にも(その是非はさておき)EV SSL のグリーンバーの様な形で結実することもあるだろう．

Web PKI の社会受容の観点において，注目したい点としてインディケーションによる受容者への安全性の保証の観点がある．

古くは，Pad Lock アイコン(鍵マーク)と呼ばれる表示があった．これは，ウェブブラウザにおいてそのページが SSL(TLS)による通信をしていることを表しており，このマークが表示されているページは安全であることを示している．通常の(SSL のない)状況が安全ではないことが喧伝される中，利用者が個々確認するという負担はかかるものの，これは非常にわかりやすく，安全な通信を求める全てのステークホルダーにとって嬉しいものであった．その後，複雑性を増すウェブの世界で安全なシステムを実現する為に，この表示の背景で求められるステークホルダーへの要求はどんどん大きくなっていき，Pad Lock アイコンは CABF を中心とした議論などを踏まえつつ EV SSL のグリーンバー表示とセットになる形へ変化していく．この際，「安全である」ことを認識してもらうための教育啓蒙学習コストは比較的高くかかっており，Web PKI というエコシステムが一定以上の一定以上の役割を果たしていることを示しているだろう．

わかりやすい安全性表示を行うことで複雑性を縮減する例としては信号機があげられる．これはほぼ完全に社会に受容され信頼を得ている例だろう．警戒色である赤が危険を示すこと等を踏まえて，緑・黄色・赤の三色により安全性・危険性を評価可能にしており，これにより学習コストを最小限にしつつ社会の安全性を実現している．また，文化的違いはあれど日本だけでなく多くの国で広く受容され，国際的にも国際照明委員会によって" CIE S 004/E-2001 Colours of Light Signals" [5] という形で標準化されている．もちろん，EV SSL の表示が緑であることも無関係ではないだろう．(アクセシビリティの観点では課題もあるが，ここでは触れない)

信号技術は歴史が深く，ここでは一部を恣意的に取り上げる形になっているが，特に着目したい点は，信号機が緩やかに時間をかけていくつかの世代を経て社会受容されてきた点である．特に初期は個々の国家制度として整備されたものが，国際的な社会受容に至る過程には非常に長い時間がかかっているだろう．一方，Web PKI の表示に関しては，比較にならないほどの速度で，国際的に受容された点である．これはインターネット時代という今までとは違う特異な時代背景と，既にある信号機のような信頼の仕組みに則った点などが要因としてあげられる．

4. Bitcoin の信頼構成要因

4.1 文化的背景・ニーズとユースケース

Bitcoin の社会受容の要因はある意味では明確である．本来 Bitcoin は経済的な価値の移動のみを目的としたものであり，喧伝されるその他の要素は付随するものに過ぎない．その意味で，汎用的な情報交換ツールであるメールや，アプリケーションを動作させるプラットフォーム足り得るウェブとは現時点では異なっている．

その普及の要因として推測される点は，大きく下記の 2 点があると考える．

1) マーケティング的側面

本稿からは逸脱するので触れる程度に留めるが，"Crypto Currency"や「コイン」,「マイニング」という単語を使ったことは，いわばマーケティング的な観点で社会受容に大きく寄与したと思われる．

2) 時勢

1980 年代後半に電子マネーの研究や実証実験が盛んに行われたのにも関わらず普及に至らなかった経緯，他にもタイムスタンプサービスなどの近しい技術はあったがおおよそ社会受容されたとは言い難い状況を踏まえ，なぜ Bitcoin は衆目に集めるに至ったのか．当然，様々な要因があったと思われるが，一番大きいのは環境であり時勢であろう．

世界的には，インターネットが「社会受容された」後に，インターネットのような一国に閉じない国際的な環境で流通・利用可能な経済価値の移動手段という潜在的ニーズに対して，実現可能だと信じられる状況を前提にソリューションを提示したという点は大きい．つまり，タイミングの問題であり，段階的な成熟度合いやニーズの問題という，マーケティングの世界ではありふれた要素を満たしたからに他ならない．特徴的なのは，暗号や技術を中心とした生々しさのある Bitcoin が，非常に速い速度で受容されつつある点だ．これは，インターネットの普及や計算機資源の大幅な向上という環境の影響があるだろう．(昔，注目を浴びたものの社会受容に至らなかった技術が現在の環境下で普及の気配を見せるケースは，人工知能等も含め最近いくつか見受けられるように思われる)

これらの背景には Bitcoin を支える文化的側面の影響も大きい．スノーデン事件の例を引くまでもなく，当局による監視・管理を嫌う一定の人々が存在するのはよく知られた事実であり，暗号技術がそこに一定以上寄与していることは間違いない．暗号学者であるデビッド・チャウム(David Chaum)は "Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985) [6]において"digital pseudonym" 等の概念を提示し，これが後にサイファーパンク(cypherpunk) と呼ばれる，暗号技術による社会変容を目指す人々の集団に繋がる．提案者である Satoshi Nakamoto の実体が不明だという点も含め，Bitcoin もその系譜に連なる技術だといえるだろう　　．

2010/5/22 に Laszlo Hanyecz が 10,000 bitcoin(BTC)で L のピザを 2 枚購入した [7]ことは Bitcoin において非常に重要な事象である．象徴的な意味で利用者に実利を示しただけでなく，「ピザの提供者が Bitcoin を信頼に値する」と判断したのである．象徴的な意味ではあるが，Bitcoin がサイファーパンク達の社会的実験から現実的な手段に変わった瞬間だといえる．残念なことに，この延長上にはランサムウェアの支払い等，物理社会から遠いブラックマーケットにおけるインターネットでの価値移動での需要に繋がったが，ピザと犯罪の双方において Bitcoin はこれらの需要に応えたといえる．結果的に，これらの事実がニュースとなり，Bitcoin はキャズムを越えることとなった．

4.2 コミュニティとガバナンス

Bitcoin のコミュニティとガバナンスに関しては本稿執筆時の 2017 年 8 月 1 日前後に大きな変化があった．これは，技術的，商業的，政治的など様々な側面から，フォーク(fork)と呼ばれる分断を行う動きである．フォークについては本稿執筆者の文章を参照されたい．

> "ブロックチェーンの応用に大きな影響を与えるガバナンス上の課題である「フォーク（fork)」が，ビットコインを含む世界の開発コミュニティの間で物

議を醸している．「フォーク」とは，公開されているソフトウエアを分岐（fork）させ，新しいプロダクト／コミュニティとして独立する動きを指す．主にオープンソースソフトウエア（OSS）に特有のアクションである．コミュニティとしてみれば「分派」というイメージだろうか．OSS の分野におけるフォークは，ガバナンスを担保するための手段として，いわば非常用に用意されている．通常はなんとかしてコミュニティの内部で問題の解決を目指す．つまり，フォークが発生するのは，コミュニティ内の話し合いが決裂しているケースがほとんどだ．OSS の場合，その多くは自由に開発・利用できるライセンス（FLOSS（Free/Libre and Open Source Software）ライセンスなどと言われる）であり，ソフトウエアの「ほぼコストなしでコピー可能」という特性と合わせれば，たやすく分派できる．つまり，コミュニティの健全性が損なわれている場合は，方針を同じくする仲間とフォークすれば，ソフトウエアの利用者に対して多大な負担をかけずに，そのソフトウエアのコミュニティ（と開発）を継続できるわけだ．OSS の世界での古く，そしてよく引き合いに出されるフォークの例としては，GNU Compiler Collection（GCC）と Experimental/Enhanced GNU Compiler System（EGCS）がある．これは，後日再統合された例としても有名だ．ビットコインにおいても，古くは「Bitcoin XT」や「Bitcoin classic」などのフォークの提案があった．最近でも，The DAO の事件におけるイーサリアム（Ethereum）のハードフォーク／ソフトフォークの議論が記憶に新しい．" (「国際的な存在感が希薄すぎる日本のブロックチェーン業界 – 連載 : ブロックチェーンは本当に世界を変えるのか」http://itpro.nikkeibp.co.jp/atcl/column/16/062400138/090100006/ より)

今回生じたのは，SegWit と呼ばれる Bitcoin が持つ課題を解決するための新たな機能拡張の採用に伴うもので，この是非を問う形で Bitcoin から Bitcoin Cash と呼ばれる fork を行うという一団が現れた．詳細は割愛するが，本稿の論点として，ソフトウェアコードの fork と本件が明らかに違うという点を指摘したい．ソフトウェアは，fork をしても fork 前のソフトウェアの利便性が損なわれるものではないのに対し，Bitcoin の fork はいわば台帳の fork であり，「データを共有している」=「どのデータを参照するかが変わる」という点が大きく異る．Bitcoin の開発者は OSS の文化に大きく影響を受けており，それは github という OSS 文化の最前線で開発を行っていることからもわかる．しかし，サイファーパンク的な背景を持つエンジニア主体の彼らが，この fork による影響を，社会的な観点から検討していたかというと疑問の余地がある．ビジネスを行う対立者が Bitcoin Cash 等を擁するのは十分想定されることだが，何よりも一般の利用者にとってこれは混乱以外の何物でもない．過去，OSS コミュニティがガバナンスの課題を解決するために Free Software Foundation (FSF)を設立したことや，Linux Foundation が設立されたこと，なによりインターネットが Internet Governance Forum(IGF)を作るに至った過程などを活かしていない点は残念である．そして，この点は技術と社会を繋ぐ信頼において重要な点だろう．

しかし，ここには背反する要素がある．Bitcoin Cash の fork にみる統制の無さは，転じて一国の法制度の支配が及ばないというインターネットの特性とそのインターネット上の価値移動手段としての Bitcoin の需要において表裏の関係であり，受容者はこの事をある程度理解しているはずである．Bitcoin Cash による fork はこのことを明確に示しており，普及されたものに対する要求要素について，「Bitcoin は大切だが反して不満もあるので，過去としては Bitcoin でもあり，自分達にとっては未来はより都合の良いもの(改変物 = Bitcoin Cash)でもあって欲しい」という背反する要望となって表れている．これは，中谷内ら [8]が指摘するように，コンテクストによって受容の観点が異なることを体現している．

結果的に，Bitcoin Cash は 2017 年 8 月末時点ではほとんど成果を出すことが出来ておらず(ブロック数の進展がほぼない) ，目的に対して混乱と不安，不信の影響が表れた形となった．

サイファーパンク的な，ひいてはインターネット的な動きの一方，消費者的な不安を解消する為の動きとして，仮想通貨という括りで Bitcoin などを法的に定義することや法的に規制・統制する話題が，Bitcoin Cash の話題より以前から頻出している．我が国でも「情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律」(平成 28 年 3 月 4 日提出，平成 28 年 5 月 25 日成立)(http://www.fsa.go.jp/common/diet/190/) [9]により，「資金決済に関する法律」(「資金決済法))および「犯罪による収益の移転の防止に関する法律」(「犯収法」)が改正され，仮想通貨の取り扱いが国家的にどういう形になるかが明示された．これは社会を変容させたといっていい事象であり，明確な社会受容のひとつの要素だといえるだろう．

これは同時に，法律の改正が必要であると考える何かしらの要望があったことを表わしている．仮想通貨の定義やルールが必要だと考えた人(達)がおり，実際に法改正される程にはその影響があったわけである．法改正が社会受容の大きな推進力となったことは間違いないだろう．

Web PKI は需要に対して，コミュニティとガバナンスで応え，ポリシーを利用者に提示しそれを実施することで「信頼を勝ち得」た．これらは Bitcoin においても重要になると思われるが，文化と De-Centralize という特性故に簡単には

実施出来ないだろう.

4.3 デプロイメントとユーザビリティ

Bitcoin のデプロイメントとユーザビリティに関しては，まだまだ課題が多い.

P2P ネットワークという Bitcoin の特性は，稼動状態にあるノードを如何に全ての利用者に更新してもらうかというインセンティブ設計にかかっており，前述の SegWit のようなケースでもコミュニティ外で大きな議論になるほどである．コミュニティが未成熟な Bitcoin においては現時点でも喫緊の課題である.

Web PKI においてはブラウザというユーザとの接点があり，インタラクションが生じるアプリケーションがデプロイメントされていた．そして，そのブラウザをいわばトラストアンカーにしていた点が Web PKI の妙味であり社会受容の要因であった．しかし，現時点での Bitcoin においては明確なアプリケーションを利用する形ではなく，多くの利用者は単なるウェブサービスとして間接的に利用しているにすぎない．今後にブラウザに相当する役割が期待できるのはウォレットと呼ばれるソフトウェアであるが，現時点では標準化にはまだまだ遠いと言わざるを得ない．これは利用者にとっては非常にネガティブな要素であり，社会に受容される技術になるために Bitcoin が満たすべきひとつの課題だろう.

5. 考察 / Consideration

ここまでの要素の抽出を踏まえて，最終的な社会における受容と信頼に関して考察したい.

5.1 文化的背景・ニーズとユースケース

インターネット時代における ICT 技術の社会受容に関しては，世代によって全く異なる様相を呈しており，「社会全体」での受容とは必ずしも一致しない．つまり，受容者(受容したと思っている人物)からみた視点と，社会としての視点が一致するとは限らない．更に，日本国内の世代別人口分布を鑑みると，ICT 技術を社会的に受容するであろう若い世代とそうでない世代の比率から，技術的なものに対して社会全体での均質な社会受容が難しいことが推察される．これは，社会全体での「効率的な技術の運用」という ICT 技術の目指している状況との差異を表わしている．同時に，特定の世代で大きな影響力を持つ何かが他の世代へ波及していく可能性を考慮することも可能であろう．具体的には，若年層は LINE を信頼しているが，中年層は信頼しておらず，年配者によっては存在すら知らない，といった状況で，既に受容している若年層からの働きかけにより，中年層や年配層へ波及していく可能性である.

この状況は古典的社会受容のモデルとは一致していない可能性が高い．Web PKI の事例の興味深い点は，この世代別，国別の差異を越え，インターネット全体の社会受容満たした点にある．そして，これは Bitcoin もおそらく同等の状況を目指すことになるだろう.

5.2 コミュニティとガバナンス

Web PKI 以前，例えばメールにおいてはインターオペラビリティのみが求められ，資源管理(DNS 等)や，プロトコル(SMTP)，フォーマット(RFC822)がそれを担うことで社会受容された．これが Web PKI になると，これらの要素はもちろん，加えて更にポリシーやガバナンスなども含めた，より厳しい要求に応える必要が出てきた．これらは，まさにコミュニティが担うべき重要な役割であり，Bitcoin に不足している大きな要因だ.

ここで明確なのは，社会受容における「ガバナンス」の重要性だろう．技術は当初，技術として世に出ることが主だが，イノベーター理論での後段に至るにつれ，社会は，いわば利用者を代弁する形でガバナンスを信頼の手段のひとつとして求める．利用者が安心してその技術を使うための要求のひとつとして，何か被害が生じた際の管理主体を求める心理が働く．受容者にとって，(怪しいサイトが危険であるという教育啓蒙という信頼の観点も含めて)ウェブサービスは適切な管理がなされていることを望むし，そこへアクセスする為のインターネットはサービスプロバイダによって管理されていることを望む．そこではまたクレジットカードを使うにあたって安全に Pad Lock アイコンが緑色に表示されていることも望まれる．ここでの信頼はまさに複雑性の縮減メカニズムであり，技術的であるか否かはほとんど影響がない．Web PKI において CABF が期待され求められた役割は，技術を社会に受け入れる過程でなにかしらの課題がある場合の窓口としてコミュニティの存在が求められた点であろう．これは，Web が W3C を，インターネットが IETF 等を，それぞれ必要としたのと同様だといえる．Bitcoin においては，Scaling Bitcoin Workshop のような取り組みはあるものの，こういったフィードバックを受け入れガバナンスを担当するコミュニティが存在しない.

受容者にとって，コミュニティの存在とそこにガバナンスの意向をきちんと持つかは，Web PKI においても Bitcoin においても等しく重要である．これを鑑みた上で，社会受容の為のガバナンスにおいては，ルールまたはポリシーなどの枠組みを有しており，そのことを関連する専門家群に知ってもらう必要がある(知られていなくてはならない)．なお，普及の度合いがあがるほど，ガバナンスの必要性を問われるケースが出てくるほど，実際のガバナンスにおける執行力(エンフォースメント)が問われることが予測されるが，この点に関して契約行為と監査を枠組みとしようという取り組みに Trust Framework という取り組みが存在す

る． [10] [11] [12]

インターネットの事例から見るに，後からルールを徹底することは難しく，関係するステークホルダーが少ない内にルールを策定する方が容易であることは間違いない．一方，余りにも初期にルールを策定することは，そのコストだけでなく将来を見通すことが出来ない等の課題があり難しい．20 年かかった Internet Governance は非常にわかりやすい事例であろう．但し，Web PKI においては社会の変化と共にステークホルダーも変わり，求められる要求事項も変わっているという事実がある．つまり，変化に合わせてルールやポリシーを変更出来る必要があり，同時にコミュニティに対するフィードバックとエンフォース，そしてデプロイすることの重要性が勘案されていることが社会受容への要因となるだろう．

そして，ここに社会受容を，そして信頼を加速するひとつの要素が垣間見えてくる．ルールやポリシーは意図しない限り作ることは出来ないが，積極的に作成することで，社会における受容を早めることが出来る可能性がある．

5.3 デプロイメントとユーザビリティ

インターネット時代における社会受容の要因として，受容者自身での利便性と利用可能性がほぼイコールで結びついている点は大きい．メールやウェブのように身近に利用される，または利用したいと思った際に手間がかからず低コストで利用可能な形でデプロイメントされた状況である必要がある．(おそらく，LINE の社会受容はこれらを大幅に飛び越えた事例だと思われるが，本稿の目的を越えるためここでは割愛する)

Bitcoin において，Web PKI の背景に暗号があることが既に広く認知されていたことによって，Crypto Currency の信頼性が向上した可能性は高い．インターネットより前の時代においては，受容者にとって暗号とは推理小説や映画におけるシーザー暗号程度の知識だったものが，インターネット時代では

「仕組みは理解していないにも関わらず暗号を利用しているから安全 (だと専門家が言っているから安全)」

という構造に至っている．Bitcoin はこれを踏まえて Crypto Currency という用語による信頼を勝ち得たことは間違いなく，Bitcoin の現状の普及過程において，これが有効に作用しているのは間違いないだろう．(レイトマジョリティやラガードまで同様に至るかについては議論の余地が大いにあるが) これは同時に Web を信頼する世代までにしか Bitcoin が信頼に至らない可能性があることを示唆してもいる．

ここにある課題として，Bitcoin は Web PKI ほどコミュニティやガバナンス構造などの含めた全体が未成熟であり，受容者に対する信頼の提供が不足しているといえる．

社会受容においては受容にかかる時間という観点もある．基盤技術の社会受容にとって必要になるのは社会的認知であるが，これは当該技術(およびそれを利用した製品)の存在の伝播が必要になる．インターネットも Web も依存している下位の構成要素と自身の情報伝播速度によって，イノベーター理論の後段へと至った．具体的にいえばニュース等による伝搬であるが，これは通信媒体であるインターネットやウェブでは自身がそれを担う事が可能であったのに対し，Bitcoin はそういった手段を持たない点が大きく異なる．

ユーザビリティの観点で，Web PKI と Bitcoin で大きく異なるのが，利用者が直接インタラクションするアプリケーションの有無である．サーバ・クライアントというモデルで動いていた Web と，P2P ネットワークを中心とした Bitcoin では，求められるものが異なる可能性は高く，ブラウザが担っていた役割をウォレットが担う必要はない．一方，暗号の力で経済を動かした Bitcoin において，その中央の主体を持たないという特性を考えれば，より受容者に近づくことは本質的であるようにも思える．

5.4 基盤技術における信頼性の要因と考察

我々は，社会受容と信頼にはかなり高い関連性があると考えているが，本稿をまとめるに辺り，その差異といえる部分においても一定の検討を行いたい．

制度的な背景を持つ社会的な信頼行為は，情報の伝播速度や世代間の教育啓蒙のような精緻化見込みモデル(ELM) [13]のような物理的制約も考慮したモデルであったように思う．一方，インターネット時代の信頼行為において大きく変化した点がいくつかある．ひとつは情報の伝達における物理的特性の欠落．ひとつは速度・時間共に生理的感覚と大きく逸脱した情報伝達環境．ひとつは，長期間における情報の蓄積・参照可能性である．世界的なインターネットの広範な普及は 2000 年前後からと言われるが，そこから考えると社会はまだインターネットの影響について高々 20 年弱しか経験しておらず，社会的な 1 世代すら内包出来ていない中で，これらがどう社会に影響していくかは今後の大きな課題だといえるだろう．例えば，インターネット以前の制度設計者は多くの関連事項をこなすことが出来る専門家としてスケールしていたことが推測される．例えば，郵便や電話等の制度に関して，制度設計者はその時代の社会における影響範囲について把握可能であっただろう．一方，Web PKI においてスケールに課題があることは，2012 年の時点で「デザイナーの暗黙知」として課題視されている． [14]

ここにおいては，社会性によらない個対個での信頼という要素が大きくなる可能性もあり得るのではないだろうか．この場合，おそらく複雑性の縮減に寄与する要素はおそら

く ICT 技術であり，技術によって個人がエンパワーメントされ，社会性への依存を低減するという可能性である．対政府や監視という観点ではないが，ある意味ではインターネット的であり，サイファーパンク的とも言えるだろう．

複雑化の縮減という視点で Web PKI を見た場合，

1. 公開鍵暗号の専門家である暗号研究者から，
2. ソフトウェアやインターネットにおける実装者，
3. ビジネスを推進するステークホルダー(受容者においては専門家)，
4. これらの関係者が集まるコミュニティとその運営者，
5. そのコミュニティを評価し制度設計を行う専門家，
6. その制度やコミュニティを評価し喧伝するより一般に近い専門家，

といったように複雑性を低減する形で階層的に，より受容者に近付いてくることがわかる．当たり前のことに思えるが，前述の信号機の例がこのような明確な形で行われていたとは考えづらく，これを国による統制によらず特定の専門性を有するコミュニティで実現していることは一考に値するだろう．階層化の理由として考えられるのは，いくつかの項目であげたように，専門家のスケーラビリティの問題，つまりインターネット社会の専門性の拡大化・複雑化や，役割を担うコミュニティとしての継続性等から生じていると考えられる．

これが，技術に関するインターネット時代の社会受容において強化すべきひとつの要因ではないだろうか. つまり，専門家同士の連鎖的な階層によって，複雑性の縮減を期待可能な状況にあるか，そしてそれを受容者が評価可能か，である．

ここまで, Web PKI と Bitcoin を題材にインターネット社会における社会受容という観点で，主に受容者の視点から何が重要視されるかを見てきた．

昨今，信頼というキーワードが取りざたされる背景には，現在のインターネット社会の変化速度が非常に早く専門性が求められる故に，複雑性を縮減する目的で，専門家の階層構造を評価する必要性が高くなってきたことがあるのではないだろうか．信じるに足ると評価するために，国による制度化を求める人もいれば，ソーシャルな関係性で評価を行う人もいるだろう．

受容者に届き得る社会受容の要因の中で，技術を展開する側から制御可能な要因はなにか．残念なことにそれは技術そのものやその信頼性ではないが，既存のインターネット上における信頼の階層構造の一端に紐づくことと，コミュニティによるガバナンス構造によって信頼の階層を評価可能にすることだといえるだろう．

変化が早いこと，そして求められる専門性が変化しやすいことはインターネット時代における信頼のひとつの課題である．受容する立場において，対象を評価した際にこれが可能であると思えることが信頼であり，これを解決できる体制・状況が，技術に関する信頼を今後最も受容しやすくする条件だといえるだろう．

6. 参照文献

1. **CA/Browser Forum. CA/Browser Forum. (オンライン) https://cabforum.org/.**

2. Standardization Organization forInternational. ISO/IEC 18014-2:2009 3.24.: International Organization for Standardization, 2009.

3. 奥田秀巳. 信頼の倫理学的考察.: 広島大学, 2015.

4. Rogers M. Everett. Diffusion of Innovations.

5. Illumination Commission onInternational. CIE S 004/E-2001 Colours of Light Signals.: International Commission on Illumination, 2001.

6. Chaum David. Security without Identification: Transaction Systems to Make Big Brother Obsolete. 1985.

7. Hanyecz Laszlo. Bitcoin Forum. (オンライン) 2010 年 5 月 18 日. (引用日: 2017 年 8 月 28 日.) https://bitcointalk.org/index.php?topic=137.msg1195#msg1195.

8. 中谷内 一也 George Cvetkovich. リスク管理機関への信頼 : SVS モデルと伝統的信頼モデルの統合. 2008.

9. 情報通信技術の進展等の環境変化に対応するための銀行法等の一部を改正する法律. (オンライン) 2016 年 3 月 4 日. http://www.fsa.go.jp/common/diet/190/.

10. Eve Maler,et al.. Open Identity Trust Framework Model. 2010.

11. 島岡政基，佐藤周行. 学認における属性交換フレームワーク. コンピュータセキュリティシンポジウム 2013 論文集, 2013(4), pp.486-493, 2013 年 10 月.

12. 島岡政基. 認証基盤から見た情報システムの信頼とトラストフレームワークの抽象化,. コンピュータセキュリティシンポジウム 2016 論文集, 2016(2), pp.1137-1144, 2016 年 10 月.

13. Petty E., and John T. Cacioppo.Richard. Attitudes and persuasion: Classic and contemporary approaches. 1996.

14. 島岡政基. 暗号と社会の素敵な出会い : 3. トラストと暗号技術の関係性. 情報処理学会, 2015-10-15.

15. 島岡政基, 松本泰. SSL 証明書の事例に見る暗号アルゴリズムの移行問題—収束しない 2010 年問題—. 電子情報通信学会論文誌 B Vol.J94-B No.1 pp.1-13, 2011/01/01.