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

島岡 政基[1]

概要：技術の高度化と社会の複雑化が進むほどに，人は信頼なしに社会で生活していくことが難しくなってきている．中でも情報システムは，従来の社会システムと比べ成長・普及が早く，信頼を確立するために必要な時間を十分に確保することが難しい．そこで，本稿では社会学・心理学の分野における信頼の概念を整理しつつ，情報システムの世界における先行事例として Web PKI や認証連携トラストフレームワークの事例を踏まえ，情報システム全般に適用可能な汎用トラストフレームワークを提案した．匿名加工情報の提供や暗号アルゴリズムの信頼性評価にこれを適用し，信頼を確立するための考察に資するものであることを示した．

キーワード：信頼，トラストフレームワーク，認証基盤

1. はじめに

技術の高度化と社会の複雑化が進むほどに，人々がそれらの仕組みをすべて理解することは難しくなり，何らかの形でそれらを信頼して利用することが避けられなくなってきている．言い換えれば，技術や社会制度が広く利用される上では，如何にして利用者の信頼を得るかが重要な要素のひとつとなってきた．社会基盤化した情報システムにおいても例外ではなく，情報システムの信頼性 (trustworthiness) を高めるための検討も活発になってきたところだが，信頼という言葉の曖昧性が故に，その検討も模索的なものが多く方向性が定まっていないように見受けられる．

この信頼という言葉は，我々はごく日常的に使っている言葉であるものの，およそ抽象的な概念であり，社会学や心理学においても議論が定まっていないのが現状である．日本語では信頼や信用，信任，英語でも Trustworthy, Confidence, Reliability など様々な類義語があるように，それぞれに少しずつ異なる意味を持つ．しかしながら，その語句の多様性に加えてそれぞれの定義・解釈にも諸説あり，社会学・心理学などにおいても議論が収束しないほどに，きわめて曖昧な概念である．学術的な信頼の探求も重要であることに疑念の余地はないが，社会基盤化した情報システムを支えるにあたっては，その信頼性を高める技法の確立もまた欠かせない．特に，貨幣制度に代表される象徴的通票[*1]や医師などの専門家システムといった，従来の社会システムよりも遥かに早く成長・普及する情報システムにおいては，如何にして確かな信頼を早期に確立できるか，が重要となってくる．そのためには，情報システムを利用する人々が情報システムに対する信頼を円滑に確立するための要点は何なのか，また信頼される側の情報システムにとって利用者からの信頼を円滑に得るための要点は何なのか，を情報システムとその利用者の関係性，さらにはそれを取り巻く社会における両者の位置づけなどの点から明らかにしていく必要がある，と筆者は考える．

そこで本稿では，信頼を理解して円滑に確立するために，2 節で社会学・心理学の分野も含め信頼研究を俯瞰し，信頼の概念を整理する．3 節では，社会実装された情報システムとして信頼を確立してきた Web PKI(Public Key Infrastructure) と認証連携トラストフレームワーク (Trust Framework, TF) について概観し，信頼確立のポイントを分析する．4 節では，3 節までの内容を踏まえ，TF を認証以外の用途に応用できるよう抽象化した汎用 TF を提案することで，情報システムが信頼を得るにはどうすればいいかについて考察する．

2. 信頼研究の俯瞰

個々の情報システムが社会から信頼される存在になるた

[1] セコム株式会社 IS 研究所
Intelligent Systems Laboratory, SECOM CO., LTD.

[*1] いずれの場合でもそれを手にする個人や集団の特性にかかわりなく『流通』できる，相互交換の媒体を指す．

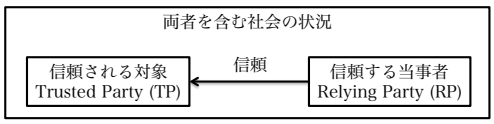

図 1 信頼の基本的構図 [2]

めに我々は，信頼を確立する手法，信頼を構成する要素技術など，いわば信頼を使いこなすための様々な技法を研究開発していくことになるだろう．様々な信頼の技法を研究開発するにあたっては，信頼の表面的な理解にとどまらず適確に理解しておくべきである．そこで本節では，社会学や心理学も含め幅広く信頼研究の動向について概観する．

はじめに本稿で扱う信頼についてスコープを示しておく．具体的な議論は次節以降で展開するが，信頼の平易な定義の一例として，荒井の「個人 A が個人 B を信頼することは，B の表明したことや (表明しない場合は) 社会的に倫理的と考えられることを B が行うと，A が期待することである」を援用する [1]．ここで，「B の表明したことや (表明しない場合は) 社会的に倫理的と考えられること」を本稿では便宜上「期待する文脈」と表記する．荒井も示している通り，期待する文脈はしばしば暗黙的であり[*2]，また暗黙であるが故に相互の誤解を生じやすい側面も見受けられる．

また，信頼を構成する実体としては，図 1 の通り信頼する当事者 (Relying Party, RP) と信頼される対象 (Trusted Party, TP)，そして両者を含む社会の状況の 3 要素を，千葉が示している [2]．具体的な例を示して説明する．Alice が Bob を信頼して金を貸す，という行為は，Bob が借金を返さない可能性を認識しながらも，Bob は借金を返すはずと予期しているからこそ成立する．即ちここでの Alice が期待する文脈は「Bob は借金を返す」である．Bob が借金を返す理由は Alice に対する直接の好意や仁義だけとは限らず，例えば Alice と Bob の共通の友人 Carol に借金踏み倒しを吹聴されたくないから，という可能性も考えられる．このように両者だけの関係にとどまらず，両者を含む社会を構成要素としている点は，社会もまた何かしら信頼に影響を与え得る存在であることを意味している．

2.1 信頼とはそもそも何なのか

信頼という概念は，我々の社会生活になくてはならない極めて日常的なものである一方で，まだまだ明らかになっていない点，論理的に説明しきれない点は多い．本節では，信頼という行為が果たす社会的意義，今日の社会における信頼の重要性など，いわば信頼の性質に関する研究動向を示す．

信頼は，概念こそ古くから存在するものの，研究として活発になってきたのは 20 世紀後半である [3], [4], [5], [6]．社会の複雑化が進むとともに，その不確実性が高くなってくることで，社会における信頼の重要性が増してきた．複雑化した社会において，人はすべての社会現象を理解して正しく予測することはおよそ難しくなり，より精通した他者あるいは社会システムを信頼することによって，複雑化という問題を (表面的に) 解決している．

Simmel は，「完全に知っている者は信頼する必要はないし，完全に全く知らない者は，当然のことであるが，信頼することなどできない」と述べ，信頼を「人間についての知と無知のあいだの中間状態」あるいは「知と無知の両面性 (あるいは二重性) を持つ」と表現した [3]．また，信頼が実際には社会の複雑性を単純化している (確実性を高めている) わけではなく，むしろ信頼によってより不確実性を上げている，との見方もされている [7]．

信頼は，過去から入手し得る情報を過剰利用して将来を規定する，というリスクを冒す行為と捉え，また「複雑性を縮減するメカニズム」と最初に表現したのは Luhmann である [4]．これは，信頼が過去の情報を未来に向けて過剰に利用するものであり，信頼する対象について十分な情報を過剰に持たないながらも何らかの知識が必要である，という点で Simmel の洞察に整合する．過去の情報から未来を期待する行為は，信頼する対象の同一性が前提となっている．これは後述の信頼における認証の重要性に繋がるものと言える．

Giddens において信頼は「人間やシステムを頼りにすることができるという確信」として定義され，そこでの確信は，他者の誠実さや愛，あるいは抽象的原理 (専門技術的知識) への「信仰」を表現していると言う [6]．Giddens は，社会の近代化にともない人格的信頼から抽象的システムへの信頼，いわゆるシステム信頼が重要性を増す，と述べている．この抽象的システムとは，前述した象徴的通票や専門家システムを意味しており，これらは必然的に信頼を伴うものだとも述べている．システム信頼は，「顔の見えないコミットメント」即ち一般の人が不案内な知識に対して抱く信頼であり，人格的信頼は「顔の見えるコミットメント」即ち人の誠実さの表れに対して抱く信頼である．

このように，解き明かしていこうするほどに，信頼は矛盾が多く，およそ合理性に欠ける行為である一方で，社会生活を営む上で不可欠の行為であることが，よく理解できる．

2.2 何が信頼を構成するのか

どのような要件を満たせば信頼を得ることができるのか，信頼を構成する要素，いわゆる規定因は何なのか，という研究は特にリスク認知の分野において，近年活発に議論されている．

信頼の規定因については，Barber の「技術的能力への期待」と「受託責任を果たすことへの期待」が古典的規定因

[*2] むしろ明示的である場合の方が少ない印象を受ける．

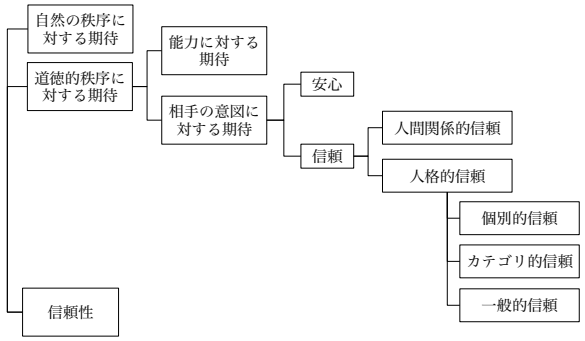

図 2 信頼の概念整理 [7]

としてしばしば援用されている [5]．これは説得コミュニケーション研究における，説得の効果を上げる要因としての「説得者の専門性にもとづく能力 (competence)」と「説得者の意図についての信頼性 (trustworthiness)」[8] とも整合する．山岸は，これを「能力に対する期待」と「意図に対する期待」と位置づけた上で，意図に対する期待を中心に図 2 のように細分化している [7].

一方で，古典的規定因だけでは説明のつかない信頼も多いことが近年指摘されており，これら古典的規定因に加えて図 3 のように「価値共有への期待」，すなわち (問題にかかわる主要な) 価値を自分と共有できている，または類似していると感じることが，信頼に大きな影響を与える，とされている [9]．中谷内は，期待する文脈への関心が高い RP の場合は，その文脈に対して価値感の親しい TP ほど信頼しやすく，一方で期待する文脈への関心が低い RP の場合は，価値感よりも能力や意図の方が強く効く，という実験結果を示した [10], [11].

> 例えば，産業廃棄物処理場の建設を社会・経済活動の枠組みでとらえて費用対効果を重視して是非を判断すべきという人と，地域住民の健康問題として考え，健康リスクの程度で判断しようという人と，さらには，都市部の廃棄物を地方の過疎地域に押しつけるという構図でとらえて倫理的問題として論じる人とでは，この問題についての主要な価値が異なっている．[10]

価値共有は，文脈に対する RP の価値観と TP の価値観が共有できているかどうかである．例えば，処理場は環境に悪影響を与えるという価値観を RP が抱いている場合には，悪影響はないと主張する TP は例え能力や動機付けが高くても信頼されにくい，というものである．また，価値共有が信頼に与える影響は文脈に対する RP の関心の高さによって変化することも明らかにされた [10].

2.3 信頼は管理し得るのか

情報システムや情報技術の分野においても，信頼の計算モデルや実装を中心に，プライバシーや信頼の応用まで広く対象とする，いわゆる Trust Management の研究が進

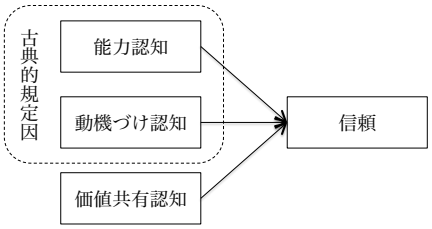

図 3 信頼の規定因

んでいる．Blaze らは，従来一体的に提供されることの多かった認証と認可を明に機能区別することによって，アプリケーションポリシにもとづいたアクセス制御モデルを提案・実装した [12]．これは，認証 (公開鍵暗号にもとづく署名検証) がアプリケーションに依らない一方で，認可はアプリケーション毎のポリシにもとづいて判断すべきであり，これらを区別することによって信頼の管理が実現できる，という考え方にもとづいている．Marsh は，信頼を計算可能な概念として形式化すること [13] に取り組んだ先駆者の一人であり，これを契機に信頼の計算モデルに関する様々な研究が活発化し始めたと言ってよいだろう．

一方で Trust Management は，信頼を計算可能な概念で捉え直し，コンピュータネットワーク上に実装しようとする取組であるが故に，実社会への展開・応用にギャップが生じ始めているのではないか，という懸念も指摘されている [14].

3. 認証基盤から学ぶ信頼

情報システムは，その急速な社会基盤化と複雑化の両面で，信頼が欠かせないものになってきた．社会学・心理学における信頼研究を情報システムに適用するには，どのような観点で情報システムを俯瞰すればよいのか．認証基盤は，その社会基盤化と認証連携による複雑化によって，情報システムの中でも早い段階から信頼を必要とし，かつその実現に取り組んできた．

本節では，実際に信頼を確立してきたケーススタディとして Web PKI と認証連携 TF を概観し，信頼確立のポイントについて分析する．

3.1 Web PKI

Web PKI は，Web サーバと Web ブラウザの間の通信において秘匿・認証などの目的で用いられる公開鍵基盤 (Public Key Infrastructure) であり，複数のルート認証局と，各ルート認証局の下につながる (多段の) 中間認証局，いずれかの中間認証局から証明書を発行される Web サーバ，また同 Web サーバにアクセスする Web ブラウザなどのクライアントによって構成される．Web PKI で典型的なサーバ認証では，サーバ証明書を提示する Web サーバが TP，Web サーバを信頼する Web ブラウザが RP とし

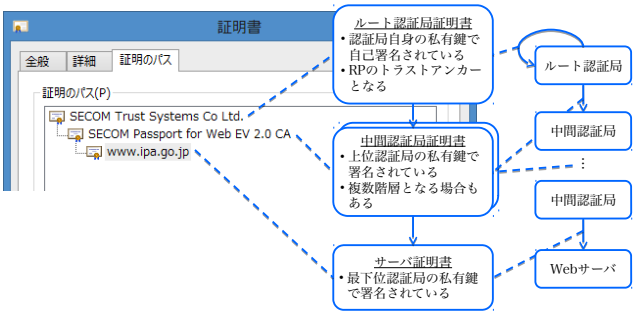

図 4　Web PKI の証明パス

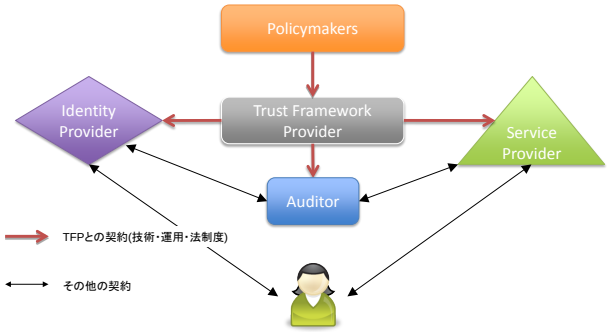

図 5　Open Identity Trust Framework Model[15]

て振る舞う事になる．

ルート認証局から (複数の) 中間認証局を経て発行されるサーバ証明書までの経路は証明パスと呼ばれ，ルート認証局の自己署名証明書 (以下，ルート証明書) を起点とした，証明パスの各ノードに対して発行される証明書の集合によって構成される．Web PKI においてルート証明書は，主要な OS や Web ブラウザに登録されており，Web ブラウザ (の利用者) はサーバ証明書の有効性確認にあたり，これらルート証明書からの証明パスを辿れることが必須となる．Web PKI の証明パスの例を図 4 に示す．

ルート証明書の登録規準は各 OS・ブラウザベンダによって個別に規定されている．各登録規準では，各ルート認証局が WebTrust for CA や ETSI TS 102 042 などの認証局運用監査基準[*3]に準拠することを求めている．即ち，証明書ポリシおよび認証局運用規程 (Certificate Policies and Certification Practice Statement, CP/CPS) を規定・公開し，またそれらに従って運用されていることを担保するため，定期的な外部監査を受ける必要がある．

本稿執筆時点の主要な OS・Web ブラウザに登録されているルート認証局の自己署名証明書の数は，Windows で 356 件，OS X で 187 件，Mozilla で 174 件，iOS 9 では 188 件となっている．

3.2　認証連携とトラストフレームワーク

認証連携は，Web サービスなどにおいて，利用者の認証機能を第三者である認証事業者に委託する仕組みであり，SAML(Security Assertion Markup Language) や OpenID Connect などが広く利用されている．ここで，Web サービスの提供者を SP(Service Provider)，認証事業者を IdP(Identity Provider) と呼ぶことにする．SP と IdP は，それぞれにセキュリティポリシが異なる場合も多く，例えば，SP は IdP の提供する認証情報の信頼性について，IdP は認証情報を提供する SP の情報管理の安全性について，それぞれ評価してお互いの信頼性や安全性を評価した上で連携，即ち信頼関係の確立の是非を判断することになる．

SP が複数の IdP と連携したり，逆に IdP が複数の SP に認証情報を提供することになると，個々に信頼関係を構築することは煩雑となる．そこで，何らかの共有可能なポリシーを策定して，これに同意する SP と IdP であれば個別判断することなく容易に連携することを可能とするのが，いわゆる認証連携トラストフレームワーク (以下認証連携 TF) である．認証連携 TF の典型的なモデル，Open Identity Trust Framework(OITF) Model を図 5 に示す [15].

認証連携 TF では，IdP および SP は，トラストフレームワークプロバイダ (TFP) を介して信頼関係を確立する．TFP は，Policymakers(PM) が策定したポリシーにもとづいて運営され，TFP と IdP あるいは SP の間の契約によって，このポリシーを IdP および SP に対して遵守させる．IdP および SP が継続的にポリシーを遵守していることを確認するため，TFP は Auditor(監査人) [*4]を用いて IdP および SP を定期的に査定する．

こうした認証連携 TF の歴史は，2000 年代前半の米連邦政府における e-Authentication の一連の取り組み [16] を契機に徐々に進み，特に学術分野では世界的に，学術機関と電子ジャーナル事業者を中心に導入が進んでいる．具体例としては，国内外の学術分野における事例として国立情報学研究所が運営する学認 [17][18]，米 InCommon など[*5] の他，国内産業界においては経済産業省が普及を推進している ID 連携トラストフレームワーク [19]，海外では OpenIdentityExchange が OITF Model をベースとした様々な TF の普及を推進している[*6].

3.3　考察

本節では，各ケーススタディから信頼の構成要素や規定因，課題などについて考察する．

3.3.1　期待する文脈の明文化

一般に PKI では CP/CPS として記述すべき項目が CP/CPS フレームワークとして標準化されており [20],

*3　本稿では，複数の組織が共通して参照するものを基準，個別の組織等が個々に規定するものを規準と表記する．およそ PM の策定するものが基準，TFP の規定するものが規準と考えればよい．

*4　TF や TFP によっては Assessor(査定人) と表記している．

*5　本稿執筆時点で，学認には 183 の IdP と 75 の SP，InCommon には 424 の IdP と 2,782 の SP がそれぞれ参加している．

*6　〈http://oixnet.org/registry/〉(参照 2016-08-12)

Web PKI においても，前述の認証局運用監査基準でこれに準ずることを求めている．即ち，RP が TP の証明書を信頼するにあたり，どのような事項が担保されるのかが明文化されている．このような運用に依存する規程の明文化は，PKI 普及前は個々の認証システムの運用事業者に依存しており，必ずしも明文化されていないことも多かった．旧来の，認証機能が一体化されているアプリケーションサービスであれば，これはあまり問題ではなかった (サービス提供者をおよそ信頼しないような利用者はそもそもそのサービスを利用しないため)．

RP が TP を信頼するにあたっては，期待する文脈があることを 2 節で述べた．誤解を恐れずに言えば，CP/CPS はある意味この「期待する文脈」に相当するものである．正確には，RP が本質的に期待するものは CP/CPS に記載されているような内容ではなく，もっと直接的に TP である Web サーバが信頼できるかどうかが知りたいものと考えられるが，CP/CPS によって RP が認証局に期待できる (担保される) 範囲が明文化されている，という意味では期待の明文化ということができよう．

3.3.2 能力の形式化

前節の通り Web PKI では認証局が担保できる範囲が明文化されたが，それが継続的に実施されている能力を持っているかどうかについては認証局自身を信頼するしかない，というのでは説得力に欠けてしまう．そこで Web PKI におけるルート認証局は，前述の監査規準にもとづいて定期的な外部監査を受け，またその監査報告書を公開することにより，CP/CPS で明文化した内容を継続的に実施する能力を持っていることを形式化している．これは，後述のトラストコントロールの形式化と捉えることもできるかも知れない．また，このように TP の能力を形式化することは，RP における「能力に対する期待」との間のギャップを解消する上でも効果が期待できる．

3.3.3 トラストフレームワークへの発展

TF の考え方は，Web PKI や認証連携を中心に認証基盤の信頼を高めようとする流れの中から自ずと洗練されてきたものである．例えば，Web PKI を TF に当てはめて考えてみると，(ルート) 認証局が TP，ブラウザ (の利用者) が RP，ルート認証局を登録するブラウザベンダが TFP，WebTrust for CA などの認証局運用監査規準 (を策定する組織) が PolicyMaker と捉えることができる．即ち，TF は Web PKI では暗黙に構成されていた枠組みが明文化されたものと言える．特に，ルート認証局を登録するブラウザベンダは，Web PKI では当初あまり重要視されていなかったプレイヤーだったが，結果的に最も重要なポジションとなり，この存在を明文化した TF の功績は大きいと言える．

4. 情報システムの信頼を支えるには

前節までに議論してきた TF は，認証情報の連携を前提としたものであった．本節ではこれを抽象化し，一般的な情報システムに適用可能な汎用的な TF を提案する．

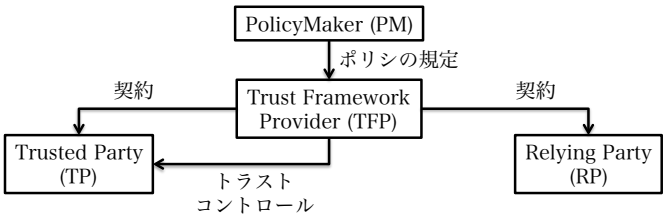

図 6 トラストフレームワークの抽象化

4.1 トラストフレームワークの抽象化

図 5 の OITF Model を，認証連携に限らず汎用的な TF にするために，図 6 のように抽象化してみる．

汎用 TF では，参加する TP,RP は TF の運営主体となる TFP と契約する．契約のひな形を公開するなどによって，契約の公正性を訴求することも可能である．

TFP は，TP に準拠させるべき TFP 規準について，TFP 独立[*7]の PM が策定するポリシを参照することで，TFP は利己性がないことを訴求できる．また，PM の定める基準に追加する TFP 独自要件が少ないほど，客観的に中立性を示しやすくなる．これは，TFP が TP ないし RP に対する独立性を十分に示せない場合などにおいて，TFP の独立性を担保する上で有効と考えられる．

TP は，TFP の規準に準拠し TF に参加することで，複数の RP に必ずしも個別対応することなく，効率的に信頼関係を構築することができる．特に，後々 TF に参加してくる RP に対しても同様の効果が得られることは，RP 変化が激しい領域では大きなメリットと言えるだろう．一方，TP は TFP 規準に継続的な準拠性を保証するために，TFP が定めるトラストコントロールに従う義務を負う．トラストコントロールは，本稿においては所定の規準への継続的な準拠性を示す手法一般を表す用語として用い，詳細は次節で後述する．

RP は，複数の TP と信頼関係を構築する必要がある場合などは，同じく TF に参加することで，同じ TF に参加する TP と効率的に信頼関係を構築することができる．RP は，TFP 規準にもとづき明に TFP と契約する．ここでの契約は例えば利用同意事項への同意なども含むものとする．汎用 TF においては，RP は TFP 規準への準拠を必須としないが，先述の認証連携のように，RP 側にも一定の準拠性が求められるケースはあり得る [18]．必要に応じて RP にも準拠を求めるなど TF を拡張することが望ましい．

[*7] ここで言う独立は，統制上の独立であり，必ずしも組織的な独立は必要としない．

4.2 トラストコントロール

TFP は，TFP 規準に対する TP の継続的な準拠性を何らかの方法で確認することが期待される．本稿では，この確認に用いる方法一般をトラストコントロールと呼ぶことにする．トラストコントロールの具体的な手法としては，一定の監査技能を有する第三者による外部監査，TP 自身による自己査定 (self-assessment)，TP 同士による相互評価，監査技能を特に必要としない利用者などによる評判制度など，様々な手法が考えられる．いずれの手法でも，継続的な準拠性を確認するための要件を定め，これを満たしていることを継続的に満たすことによって，トラストコントロールが実現される．

いずれの手法をトラストコントロールとして採用するかは，PM あるいは TFP が決定すればよいが，当然ながら手法毎に一長一短があるので，個々の TF のエコシステムにあった手法を選択することが望ましい．以下に，上記 4 手法の長短を定性的に示す．

4.2.1 外部監査

一定の監査技能を有する監査人が実施するため，もっとも厳格な準拠性確認が期待できる一方，一般に監査コストは他の手法と比較すると決して小さくない．監査コストを負担するのは直接的には TP または TFP であるため，外部監査の採用は負担主の事業規模・予算規模などに大きく依存すると考えられる．

4.2.2 自己査定

要件やチェックリストなどをもとに TP 自身が確認して，準拠性を TFP に報告する．当然ながら組織的な不正を検知しにくい問題があり，厳格性は高くない．また，査定に一定の技能を必要とするようだと，TP 内部に十分な技能を確保できなければ適切な査定が行われないリスクも存在する．一方で，査定人は業務フローなどには精通している可能性が高いため，性善説が通用する範囲においては一定の効果が期待できる．

4.2.3 相互評価

同じ TF に参加する TP 同士が相互に確認する．自己査定よりは中立性があり，また相互に行うことでコスト相殺が期待できるため，自己査定と外部監査の中間的な位置づけとなる．しかしながら，少なからず他 TP へ情報開示が必要なため，情報漏洩リスクの懸念もあり，競合組織であれば現実的ではない，などの課題が考えられる．

4.2.4 評判制度

RP など特に監査技能を必要としない一般他者に評価してもらう．十分な評価者数がいれば，統計的な有意性が期待できるが，ごく少数であると有意な結果として示せない．また，十分な評価者数を確保できたとしても，十分な評価技能がなければ評価結果が網羅性に欠ける，ばらつきがひどい，バイアスの疑いを無視できないなどのリスクが想定される．さらには，一時の評価にとどまらず継続的に評価を行ってもらう仕組みも欠かせないため，これらのリスクを補うような何かしらのインセンティブ設計が別途必要になると考えられる．

4.3 汎用トラストフレームワークのユースケース

抽象化した汎用 TF を，後述の 2 つのユースケースに当てはめる．これらのユースケースは，いずれも信頼性が求められる典型的な情報技術・情報システムを対象とする一方で，その信頼の確立には技術的な安全性 (いわゆる能力への期待) だけでは不十分であることも認識されている．そこで，汎用 TF に当てはめることによって，信頼をどのように確立すればよいかについて考察する．3 節のケーススタディおよび本節で示すユースケースについて，汎用 TF の各役割に当てはめた結果を表 1 に示しておく．

4.3.1 匿名加工情報の提供

2015 年 9 月の個人情報保護法改正によって，個人情報保護に関する規制が強化される一方で，パーソナルデータ利活用に向けた匿名加工情報制度が創設された[*8]．同制度は特定の個人を識別できないよう加工された匿名加工情報であれば本人同意なしに第三者提供を可能とするものである．個人情報を提供する利用者としては，匿名加工情報の加工方法などがプライバシー侵害を生じない程度の安全性を備えているのかが気になるところである．

こうした背景を踏まえ，同制度において各プレイヤーがどのような立場に位置しており，またどのような役割を果たすべきかについて，汎用 TF に当てはめて考察してみる．

利用者から個人情報を預かり，第三者に匿名加工情報として提供する匿名加工情報取扱事業者 (以下，取扱事業者) は，その提供にあたり認定個人情報保護団体 (以下，認定団体) の規定する個人情報保護指針 (以下，保護指針) に準拠することが求められる．保護指針は認定団体によって異なるが，認定団体は個人情報保護委員会 (以下，保護委) の定める個人情報保護委員会規則 (以下，保護委規則) に従って，各業界に合った適切な加工方法等を保護指針として定めることが望ましく (同法 53 条 1 項)，定めた際には保護委に届け出なければならず (53 条 2 項)，保護委はそれを公表しなければならない．同法改正 53 条 4 項において，認定団体の義務として，保護指針を遵守させるために必要な指導，勧告その他の措置をとらなければならない旨が義務化された．これら改正法における役割に照らし合わせれば，保護委が PM，認定団体が TFP，取扱事業者が TP，利用者個人が RP という位置づけでとらえることができる．

個人情報を預ける利用者個人は，TFP である認定団体と必ずしも契約関係を持たないが，TP に個人情報を提供するにあたっては TP 自身よりも，認定団体の保護指針に妥当性があること，また同認定団体が各取扱事業者に対し

[*8] 〈http://www.meti.go.jp/press/2016/08/20160808002/20160808002.html〉(参照 2016-08-12)

表 1 トラストフレームワークのユースケース

役割	Web PKI	学認	匿名加工情報の提供	暗号技術の安全性
PM	WebTrust for CA	学術認証運営委員会	個人情報保護委員会	CRYPTREC
TFP	ブラウザベンダ	国立情報学研究所	認定個人情報保護団体	(IPA, CELLOS)
TP	(ルート) 認証局	学術機関	匿名加工情報取扱事業者	暗号製品提供ベンダ
RP	ブラウザ	学術サービス提供者	個人	暗号製品ユーザ

て適切なトラストコントロールを実現できていることを確認することが理想的と言える．保護指針の妥当性については，保護委への届け出と公表によって一定の信頼性を期待できるが，取扱事業者に対するトラストコントロールは，義務であることが明確である以外には具体的な記述がない．継続性の観点で言えば，本ケースは定常的な運用ではなく情報提供が対象であるので，例えば匿名加工情報を提供する頻度が少なければ都度確認で，あるいは頻度が高ければ定期的に確認するなど，工夫の余地はあると考えられるが，いずれ具体的な議論を踏まえてトラストコントロールが実現されるような TF になることを期待したい．

4.3.2 暗号アルゴリズムの信頼性評価

現在広く使われている暗号アルゴリズムは，脆弱性の発見や計算機の処理性能も含め解読技術の発達などにより，時間とともに安全性が低下していく．現在の情報システム (特に情報通信システム) の多くは，何らかの形で暗号技術を利用してやり，その暗号技術の安全性は暗号アルゴリズムに依拠している．即ち，情報通信システムを安心して利用するには，暗号アルゴリズムの継続的な安全性確保が必要となる．安全な暗号アルゴリズムを選定し，またその安全性を継続的に監視する組織の一例として，暗号技術検討会 (CRYPTREC) が挙げられる．CRYPTREC は，国内で利用実績の高い暗号アルゴリズムを対象に，その安全性について技術評価を行い，一定の安全性が確保されているものを推奨候補暗号リスト，安全性確保に注意を必要とするものを運用監視暗号リストとして分類し，十分な安全性確保が難しくなった暗号アルゴリズムはいずれのリストからも削除する，という活動を行っている．即ち，理想的には暗号技術を実装した製品を提供するベンダ[*9](以下，暗号製品提供ベンダ) は，これら一連のリストを参照・準拠することで，製品の暗号技術に関する安全性を保つことが可能である．

しかしながら，CRYPTREC による安全性評価は，本来政府の情報システムで利用する暗号アルゴリズムを対象としていることもあり，迅速性よりも正確性がきわめて重視され，リストの見直しは基本的には年度単位である[*10]．このため，近年の暗号アルゴリズムに対する攻撃頻度の高まりに対して，必ずしも十分に対応しきれていないという課題がある．

こうした CRYPTREC を中心とした暗号技術の安全性評価の仕組みを TF に見立てるならば，CRYPTREC が PM，暗号製品提供ベンダが TP，同システムの利用者が RP として位置付けられる．このケースにおいて明確に TFP の役割を果たすプレイヤーはいないが，実質的に TFP に近い役割を果たしている組織として，情報処理推進機構 (IPA) や暗号プロトコル評価技術コンソーシアム (CELLOS) が挙げられる．IPA は，メジャーな暗号技術のひとつである SSL/TLS に関して CRYPTREC の暗号リストに準じる形で適切かつ詳細な暗号アルゴリズムの利用を推奨する暗号設定ガイドラインを発行した [21]．CRYPTREC が発行する暗号リストが公開鍵暗号や共通鍵暗号など暗号アルゴリズムのレベルのリストのみであるのに対して，同ガイドラインは SSL/TLS で設定する暗号スィートや鍵長まで含めた詳細なチェックリストを提供しており，暗号製品提供ベンダにとって参照しやすい形になっている．一方の CELLOS は，主要な暗号アルゴリズムに脆弱性が発見された場合に，極めて迅速に影響度を分析したレポートを発行することを活動目的のひとつとしており，やはり迅速に対処したいと考える暗号製品提供ベンダにとって有益な情報源となっている．ただし，他のユースケースと異なり，IPA，CELLOS はいずれも暗号製品提供ベンダや暗号製品ユーザとの間に契約関係はなく，従ってトラストコントロールも不在である．強いて挙げるなら，IPA の暗号設定ガイドラインに含まれるチェックリストを用いることで，暗号製品提供ベンダが自己査定を行うことは可能である．

このように TF を適用してみると，信頼を維持していく上でのミッシング・ピースも見えてくる．暗号製品の安全性評価についての信頼を確立するには，TFP にあたる組織が不在であり，これを確立してトラストコントロールを実現することが求められる．IPA や CELLOS といった組織は，結果的に TFP に近い役割を果たしてはいるものの，TP に対するトラストコントロールを利かせるとなった場合に，これらの組織が適切かどうか，またトラストコントロールとしてどのような手法が望ましいか，改めて検討する必要はあるだろう．

4.4 考察 ～継続性と価値共有～

情報システムの信頼を考えるにあたり，そのライフサイクルの短さ，あるいは技術が登場してから普及するまでが

[*9] オープンソースソフトウェアを提供するコミュニティなどもある意味ではこれに該当する．
[*10] 実際，暗号アルゴリズムの安全性評価を正確に行うには高度な専門知識と時間をかけた評価検証が極めて重要である．

短期間化している状況を踏まえると，従来の「過去の情報から未来を期待する」信頼では，いつか噛み合わなくなる恐れがある．新しい技術，新しい情報システムが，過去の十分な情報なしに短期に信頼を獲得するためには，能力や動機付けといった一朝一夕には獲得が難しい古典的規定因よりも，価値共有を適切に活用することが望ましいかもしれない．

一方で，価値もまた短期間に変動する性質があり，例えば昨日までガン治療にまったく問題意識を持っていなかった人も，身内がガンを患えば途端にガン治療に対する価値観が変わった，などはよく聞く話である．つまり，仮にトラストコントロールによって TP の価値継続性を確認・保証できたとしても，RP の持つ価値そのものが変化する可能性がある．

価値共有という規定因が信頼において果たす役割は，その確立という初期段階と，信頼の維持という継続段階において，区別して考える必要がある，あるいは価値共有を経時変化する動的パラメータとして捉え直すなど，引き続き議論が必要と考えている．信頼の目標を，その確立という初期段階だけでなく維持という継続段階まで見据えるならば，確立段階での価値共有と，継続段階でのトラストコントロールが重要になるだろう，というのが筆者の主張である．継続的な信頼を支えるのは，まさに過去の情報から未来を期待する行為であり，そこには能力や動機付けといった，継続性の高い規定因[*11]が重要になってくるものと考えられる．

5. おわりに

情報処理技術の社会基盤化が進み，人々は情報システムを日々当たり前のように利用する時代になった．一方で，情報処理技術の発展と社会基盤化は一層の複雑化を社会にもたらし，信頼の重要性が増してきている．本稿では，社会学・心理学の分野も含め広く信頼研究を俯瞰し，信頼の概念を整理した．早い段階から信頼の概念が重視されてきた認証基盤の事例として，Web PKI や認証連携 TF を取り上げ，信頼がどのように実装されてきたかを分析した．これらの分析を踏まえ，認証連携 TF を認証以外の用途にも応用できるよう抽象化した汎用 TF を提案した．信頼を必要とする典型的な情報技術・情報システムの事例として匿名加工情報の提供および暗号アルゴリズムの信頼性評価に対して適用・考察を行い，それぞれの事例において信頼を確立する上での利点や課題の分析に資することを示した．

参考文献

[1] 荒井一博：文化・組織・雇用制度: 日本的システムの経済分析，有斐閣 (2001).

[2] 千葉隆之：信頼の社会学的解明に向けて，年報社会学論集， Vol. 1996, No. 9, pp. 211–222 (1996).

[3] Simmel, G.: *Philosophie des geldes*, Berlin: Duncker& Humblot. (1900). 居安正訳: 貨幣の哲学, 白水社 (1999).

[4] Luhmann, N.: *Vertrauen: ein Mechanismus der reduktion sozialer Komplaxitat*, Ferdinand Enke Verlag (1968). 大庭健, 正村俊之訳: 信頼—社会的な複雑性の縮減メカニズム, 勁草書房 (1990).

[5] Barber, B.: The logic and limits of trust (1983).

[6] Giddens, A.: *The Consequences of Modernity*, Cambridge: Polity Press (1990). 松尾精文, 小幡正敏訳: 近代とはいかなる時代か?——モダニティの帰結, 而立書房 (1993).

[7] 山岸俊男：信頼の構造: こころと社会の進化ゲーム，東京大学出版会 (1998).

[8] Hovland, C. I., Janis, I. L. and Kelley, H. H.: Communication and persuasion; psychological studies of opinion change. (1953).

[9] Earle, T. C. and Cvetkovich, G.: *Social trust: Toward a cosmopolitan society*, Greenwood Publishing Group (1995).

[10] 中谷内一也：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，社会心理学研究， Vol. 23, No. 3, pp. 259–268 (2008).

[11] 中谷内一也，工藤大介， 尾崎拓：東日本大震災のリスクに深く関連した組織への信頼，心理学研究，Vol. 85, No. 2, pp. 139–147 (2014).

[12] Blaze, M., Feigenbaum, J. and Lacy, J.: Decentralized trust management, *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on*, IEEE, pp. 164–173 (1996).

[13] Marsh, S. P.: Formalising trust as a computational concept (1994).

[14] 菊池浩明ほか：IFIP TM 2012 参加報告，研究報告セキュリティ心理学とトラスト (SPT)， Vol. 2012, No. 45, pp. 1–6 (2012).

[15] Maler, E., Nadalin, A., Reed, D., Rundle, M. and Thibeau, D.: The Open Identity Trust Framework (OITF) Model. 〈http://blogs.technet.com/b/identity/archive/2010/03/03/open-identity-trust-framework-model-whitepaper.aspx〉（参照 2016-08-12）.

[16] Burr, W. E. et al.: *Special Publication 800-63-2: Electronic Authentication Guideline*, NIST (2013).

[17] 西村健ほか：日本における学術認証フェデレーションとその役割および効果 (インターネット運用・管理, 一般)，電子情報通信学会技術研究報告. IA, インターネットアーキテクチャ， Vol. 111, No. 375, pp. 5–8 (2012).

[18] 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， Vol. 2013, No. 4, pp. 486–493 (2013).

[19] 経済産業省：「ID 連携トラストフレームワーク」の構築のための実証事業. 〈http://www.meti.go.jp/policy/it_policy/id_renkei/〉（参照 2016-08-12）.

[20] Chokhani, S., Ford, W., Sabett, R., Merrill, C. and Wu, S.: "RFC 3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework ", November 2003, *Obsoletes RFC2527*.

[21] 情報処理推進機構：SSL/TLS 暗号設定ガイドライン (2015).

[*11] もちろん能力や動機づけが一概に継続性が高いとは限らない．ここではあくまでも価値との一般的な比較で挙げている．