ID エコシステム実現に必要となる ID 連携トラストフレームワークの研究

八　木　晃　二（専修大学大学院経営学研究科）
大曽根　　匡（専修大学経営学部）

A Study on ID Federation Trust Framework for Realizing ID-Ecosystem

Koji YAGI（Graduate School of Business Administration, Senshu University）
Tadashi OSONE（School of Business Administration, Senshu University）

As entering into the big data era, it is essential for business activities to utilize various big data. It is the arrival of the era in which ID（Identifiers）are attached to everything related to persons, things and money, and ID are used to collect, link, analyze, and utilize information. It is important to realize the ID-Ecosystem for that purpose. And to realize it, it is effective to create a structure of ID Federation Trust Framework that efficiently execute identity federation. However, for individuals, it is important to combine enjoyment of convenience by utilizing big data and privacy protection on the other side. In this research, we study the problem and solution of the mechanism on ID Federation Trust Framework from the viewpoint of privacy protection.

キーワード：ID 連携，プライバシー保護，個人情報保護，ID 管理，本人確認
Key words：identity federation, privacy protection, personal information protection, identity management, identity verification

1. はじめに

ビッグデータ時代を迎え，企業においては，競争力優位性を確保するために，情報に ID（識別子：Identifier）を付番し，それに紐づく情報を収集・連携・分析・活用することが頻繁に行われている。例えば，ある顧客にレコメンド情報を提供する場合に，自社の保有する購買履歴情報だけではなく，複数他社の保有する購買履歴情報や閲覧履歴情報を，ID を使って情報連携し，最適なレコメンド情報を提供するといったサービスが行われている。ID を使用した情報連携の仕組みは ID 連携と呼ばれるが，ID 連携技術の開発と標準化が進んだことにより，サイト間での認証や認可をベースとした ID 連携を容易に実装することが可能になり，サイト間での情報連携は急速な勢いで広がっている。

このように，サイト間での ID 連携は技術的には容易になってきた。しかし，ID 連携するためには，サイトを提供する事業者間でのプライバシーポリシーや個人情報の取扱いに関する取り決めの調整や，ID 連携する際の本人同意の取得とその方法の取り決めなど，個人情報保護法に則った多くの取り決めや契約を行う必要がある。加えて，ビッグデータを活用して企業の事業活動をさらに活性化するためには，複数の事業者をまたがった多対多のサイト間で ID 連携を行うことが必要となる。ところが，プライバシーポリシーや個人情報保護方針は事業者によって異なることも多く，サイトを提供する事

受付：2017 年 10 月 1 日
受理：2017 年 11 月 13 日

業者間での取り決めや契約の調整には，非常に多くのコストと時間を費やしてしまうという課題がある。

この課題解決のためには，複数事業者のサイト間で多対多の ID 連携を効率的に行う ID エコシステムの実現がのぞまれている。そして，ID エコシステム実現のためには，ID 連携トラストフレームワークの構築が有効であり，2015 年から日本でも導入に向けた検討が始まっている。本論文では，まず ID エコシステム実現に必要となる ID 連携の仕組みについて整理する。さらに，多対多のサイト間での効率的な ID 連携の仕組み作りに必要となる ID 連携トラストフレームワークを概観し，先行事例として米国の ID 連携トラストフレームワーク構築の動向について述べる。そして，日本における ID 連携トラストフレームワークの検討状況と課題についてまとめ，日本での ID 連携トラストフレームワーク構築の課題に対する解決策について考察する。

2. ID エコシステム実現に必要な ID 連携の仕組み

ID エコシステムとは，複数事業者のサイト間で ID 連携を実現することによって，業界内での情報流通と取引を活性化させ，ビジネスの発展を促進するエコシステムのことである。利用者にとっては，自分の使いたい ID を使用して，複数事業者の提供する様々なサービスを利用することが可能となる利便性の高いシステムである。例えば，ネットスーパーやホテル予約サイトへのログインとサービス利用を，普段使用している Yahoo! や Facebook などの SNS の認証機能を使用して実行することが可能となる。

本章では，ID エコシステムを実現するための基盤として必要となる ID 連携の仕組みについて概観する。まずサイト間での ID 連携の仕組みについて整理し，その ID 連携を支える技術とその標準化及び普及状況について概観する。そして，多対多のサイト間で効率的に ID 連携を行うために必要となる信頼の枠組みの構築の必要性について，当時筆者も検討に参加した野村総合研究所発行の第 148 回 NRI メディアフォーラム資料［2011］（文献［11］）を先行研究の基にして，考察する。

2.1 ID 連携技術の進歩と普及

（1） ID 連携の構成要素

ID エコシステム構築のためには，ID 連携，すなわち，ID を使用して異なるサイト間で認証結果や個人情報を連携する仕組み作りが必須となる。ID 連携の仕組みは，図 1 に示すように，基本的にシステム提供者とシステム利用者の 2 者から構成される。さらに，システム提供者は，ID 発行管理者とサービス提供者の 2 者から構成される。以下に，その構成要素と各々に必要な機能と行為を示す。

① システム提供者

システム利用者がサービスを利用するためのシステムを構築し提供する。ID 発行管理者とサービス提供者から構成される。

1） ID 発行管理者

システム利用者に対して，ID に関する発行管理と，システム利用者から提供される個人情報の管理を行うシステムを構築し提供する。必要に応じて，サービス提供者に対して，認証結果と個人情報の連携を行う。具体的には，以下の機能を提供する。

・システム利用者に対する ID の発行管理機能

・システム利用者の個人情報の取得管理機能

・発行した ID を使用した認証機能
・サービス提供者への認証結果の連携機能
・サービス提供者への個人情報の連携機能

2)　サービス提供者

ID 発行管理者から連携された認証結果，個人情報を使用して，システム利用者に対してサービス利用に必要なシステムを構築し提供する。具体的には，以下の機能を提供する。

・システム利用者からのサービス利用の受付機能
・ID 発行管理者からの認証結果の連携機能
・ID 発行管理者からの個人情報の連携機能
・システム利用者へのサービス利用の提供機能

②　システム利用者

システム提供者が提供するシステムを使って，サービスを利用する。具体的には，以下の行為を行う。

・ID 発行管理者に対する ID の発行要求行為
・ID 発行管理者に対する個人情報の提供行為
・サービス提供者に対するサービス利用要求行為
・ID 発行管理者の認証機能を使用したサービス提供者サイトへの認証要求行為
・ID 発行管理者とサービス提供者間での情報連携に対する同意行為
・サービス提供者が提供するシステムを使ったサービス利用行為

図 1 に示す 3 つの構成要素が各々の機能を果たすことにより，ID を使用した情報連携が実現される。なお，本稿で示す ID は，システム提供者がシステム利用者を識別するために付番した ID のことであり，かつ，システム利用者がシステム提供者のサイトにログインする際に使用するログイン ID のことである。本来，識別子としての ID とログイン ID は意味合いが異なるが，本稿では厳密に区別をしない。

(2)　ID 連携の定義と実現方法

ID 連携とは，システム利用者があるサイトにログインする際に，普段使用している別のサイトの認証機能を使用してログインし，そのサイト間で情報連携を行うことである。現在，OpenID，OAuth，SAML（文献［3］，［4］，［9］）といった ID 連携（認証・認可）の技術が開発され，標準化が進み，ID

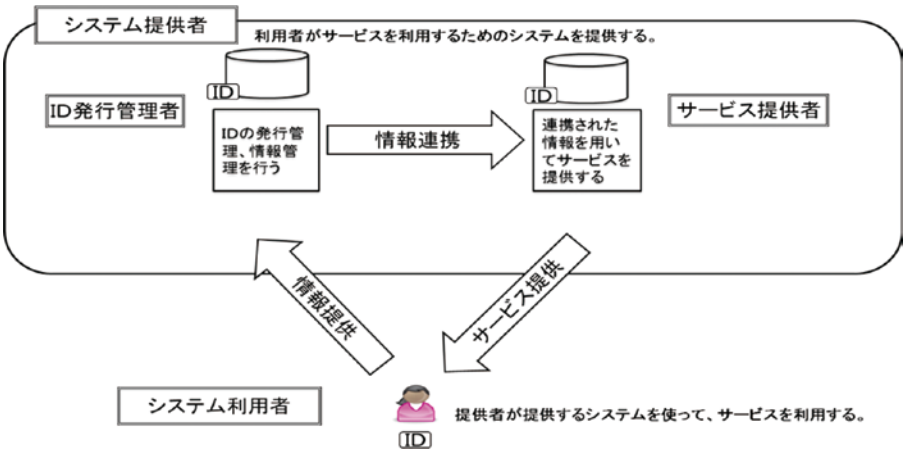

図 1　ID 連携の構成要素

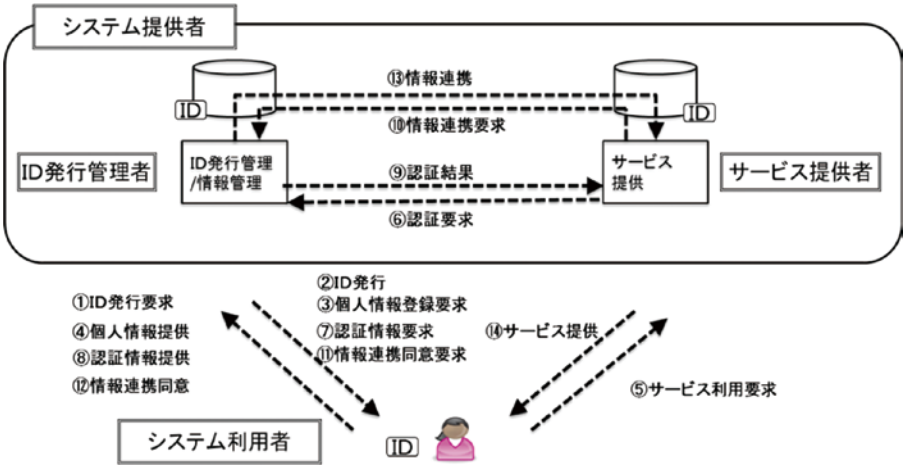

図 2　ID 連携の業務フロー

連携は普及期を迎えている。特にインターネットでのサイト間では OpenID や OpenID Connect 技術を用いた ID 連携が頻繁に行われている。ここでは，OpenID 技術を用いた ID 連携の業務フローを，図 2 を用いて説明する。その手順は，以下の通りである。

① システム利用者が，ID 発行管理者に対して，ID の発行要求を行う。
② ID 発行管理者が，システム利用者に対して，ID の発行を行う。
③ ID 発行管理者が，システム利用者に対して，個人情報の登録要求を行う。
④ システム利用者が，ID 発行管理者に対して，個人情報の登録提供を行う。
⑤ システム利用者が，サービス提供者に対して，サービスの利用要求を行う。
⑥ サービス提供者が，ID 発行管理者に対して，認証要求を行う。
⑦ ID 発行管理者が，システム利用者に対して，認証情報の入力要求を行う。
⑧ システム利用者が，ID 発行管理者に対して，認証情報の入力提供を行う。
⑨ ID 発行管理者が，サービス提供者に対して，認証結果の情報連携を行う。
⑩ サービス提供者が，ID 発行管理者に対して，個人情報の連携要求を行う。
⑪ ID 発行管理者が，システム利用者に対して，個人情報連携の同意要求を行う。
⑫ システム利用者が，ID 発行管理者に対して，個人情報連携の同意を行う。
⑬ ID 発行管理者が，サービス提供者に対して，個人情報の情報連携を行う。
⑭ サービス提供者が，システム利用者に対して，サービスを提供する。

この業務フローで重要な部分は，手順 ⑪ と ⑫ により，システム利用者本人の同意をベースとした ID 連携を可能にしているところである。

2.2　信頼関係の構築と ID エコシステムの実現

(1)　信頼関係の構築

事業者をまたがった ID 連携の実現のためには，技術的にシステム連携するだけではなく，事前にサイトを提供する事業者間で多くの取り決めや確認をする必要がある。以下にその主なポイントをあ

げる。

・ID 連携をするサイト同士の，プライバシーポリシーの確認
・ID 連携をするサイト同士の，個人情報保護方針の確認
・連携する情報の内容の取り決め
・連携する情報のそもそもの取得目的の確認。情報連携が取得目的に入ってない場合には，システム利用者への同意取得や公開する方法の取り決め
・ID 連携を解消する際の取り決め
・連携する情報管理の事業者間での責任分解点及び賠償責任の取り決め
・上記の確認や取り決めを行った後の事業者間での契約の締結

このように，ID 連携を実現するためには，連携元と連携先との間で上記の様々な確認や取り決めをすること，つまり信頼関係を構築することが前提となる。その上で，ID 連携技術を活用して ID 連携システムを構築することとなる。

（2） ID エコシステムの実現

ID 連携技術の進歩によって ID 連携をシステム的に構築することが容易になってきた現在では，技術的な ID 連携システム構築よりも，事前の信頼関係構築作業により多くの時間とコストが費やされている。さらに，事業者がより積極的にビッグデータ活用を推進するためには，複数事業者をまたがって多対多のサイト間での ID 連携を，速く低コストで行う環境の実現が望まれている。ID 連携技術の標準化や API 化が進んだことにより，多対多のサイト間での ID 連携システムを構築することは技術的には容易となったが，しかし，実際の信頼関係の構築は 1 対 1 の事業者間での関係構築ですら大変な作業であり，多対多の信頼関係構築のためには，膨大な時間とコストを要している。

この課題解決のためには，速く低コストで多対多の信頼関係構築を効率的に行える環境，すなわち，ID エコシステムを実現することが望まれている。ID エコシステムが実現できれば，図 3 に示すような多対多のサイト間での信頼関係を効率的に構築することが可能となる。野村総合研究所［2011］（文献［11］）は，民間事業者の発行した ID を活用した ID エコシステムの実現により 10 兆円を越える経済効果を試算している。

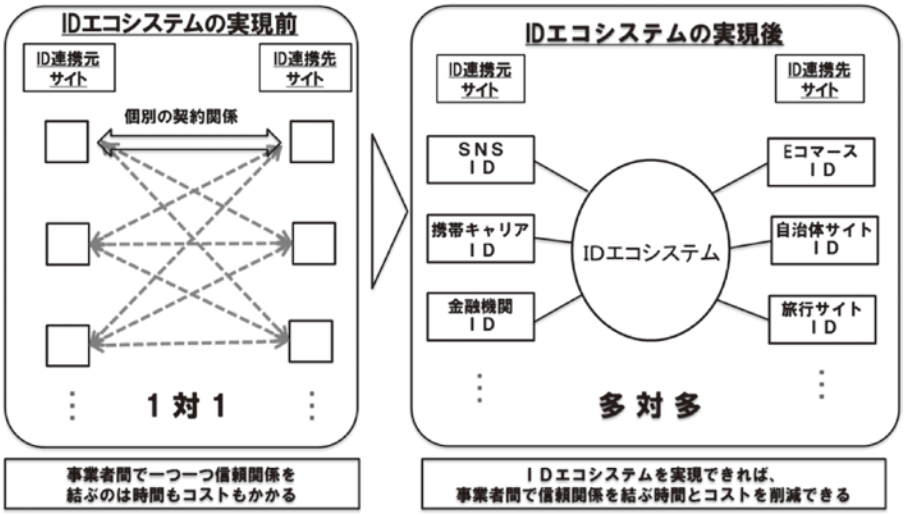

図 3　ID エコシステム実現による信頼関係の構築

3. ID 連携トラストフレームワーク構築の動向

2 章で述べた多対多のサイト間で効率的に ID 連携を行うために必要な信頼の枠組みを構築する手段として，ID 連携トラストフレームワークがある（文献［12], [13], [14]）。その内容は，サイト間での信頼関係を構築するために必要となる取決めや確認作業を，各事業者に代わって第三者が，サイトの事業者間の契約関係も含めて行うことによって，多対多のサイト間の信頼関係を保証するフレームワークである。信頼関係の構築を事業者に代わって第三者が行うことによって，信頼関係構築に要する事業者負担が軽減され，事業者からみると速く低コストで複数事業者間での信頼関係を構築することが可能となる。数年前から米国で検討が始まり，米国での国民 ID 制度の枠組みとして実装が行われている。日本では，2015 年から経済産業省を中心に本格的な検討が開始されている。

本章では，まず ID 連携トラストフレームワークを概観し，この分野で先行する米国の ID 連携トラストフレームワーク構築の動向について述べる。そして，日本の ID 連携トラストフレームワークの検討状況を経済産業省発表の “ID 連携トラストフレームワーク”［2015］（文献［6］）などに基づいて分析し，その課題について考察する。

3.1 ID 連携トラストフレームワークとは

ID 連携トラストフレームワークとは，複数事業者間での信頼関係構築の作業において，サイトの事業者間で行わなければならない取決めや契約のために費やされる時間とコストの削減を実現するために，その作業を肩代わりする第三者による統制の仕組みのことである。

第三者の統制の仕組みでは，まず「ルール作成者」が信頼関係構築に必要な条件となるルールを作成し，そのルールへの適合性の監査を行う監査機関を認定する。そして，認定された「適合性の監査機関」がルールに基づき監査要件を作成し，システム提供者（ID 発行管理者とサービス提供者）の監査を実施する。実際の監査の実施は，多数のシステム提供者に対して実施する必要があるため，監査機関が認定した「認定監査人」が行う。この統制の仕組みを表 1 に示す。この表は，経済産業省発表の “ID 連携トラストフレームワーク”（文献［6］）および一般財団法人日本情報経済社会推進会議発表の “ID 連携トラストフレームワークを活用した官民連携の在り方に関する調査研究（平成 27 年度）”［2015］（文献［1］）を参考にまとめたものである。

そして，図 4 に示すように，この統制の仕組みが，ID 発行管理者とサービス提供者を監査し，認定

表 1　ID 連携トラストフレームワークの統制の仕組み（[1][6] をもとに筆者らで作成）

名称	役割	担当
ルール作成者	ID 連携トラストフレームワークにおける要求事項やルールを作成する。適合性監査機関の認定基準を策定する	第三者（政府や，業界）
適合性の監査機関	ルール作成者が策定したルールに基づき，保証レベルを定義し，保証レベル毎に事業者が満たすべき技術，運用面での監査要件を作成する。監査を行う監査人を認定し，監査人の監査結果に基づき事業者を認定する	第三者（第三者機関）
認定監査人	適合性の監査機関が作成した監査要件に基づき，事業者に対して監査を実施する	第三者（監査人）

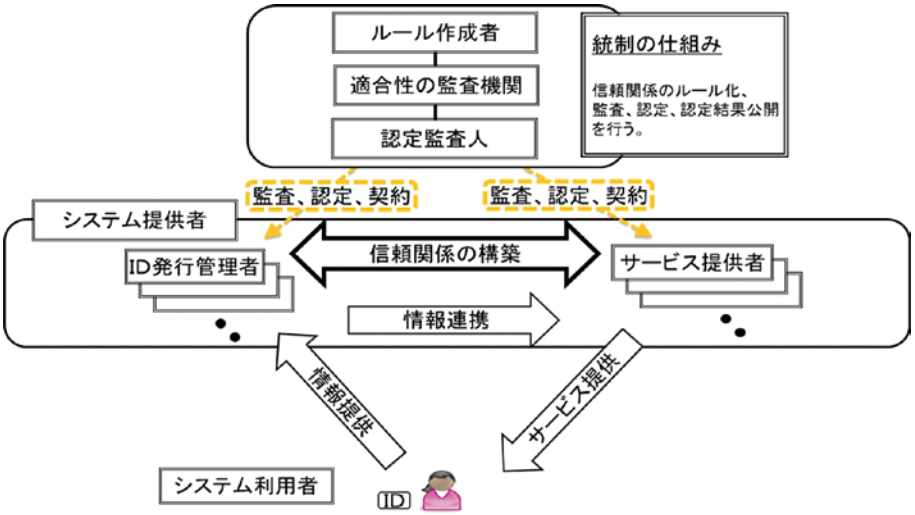

図 4　ID 連携トラストフレームワークの概念図（[1][6] をもとに筆者らで作成）

し，契約する。この仕組みによって，各事業者が個別に ID 連携の相手のセキュリティに関する信頼度を確認したり，契約交渉したりする必要がなくなるため，信頼関係構築のための時間とコストを抑えることが可能となる。

3.2　米国の ID 連携トラストフレームワーク構築の動向

米国では，2010 年 6 月に発表された NSTIC（National Strategy for Trusted Identity in Cyberspace）の国家戦略の中で，米国政府の推進する「国民 ID 制度」として，OITF（Open Identity Trust Framework）という名称で ID 連携トラストフレームワークの採用が決まり遂行されている（文献［7］,［12］,［13］）。OITF では，米国連邦政府の一般調達局と国防総省共管の ICAM（Identity, Credential, & Access Manage-

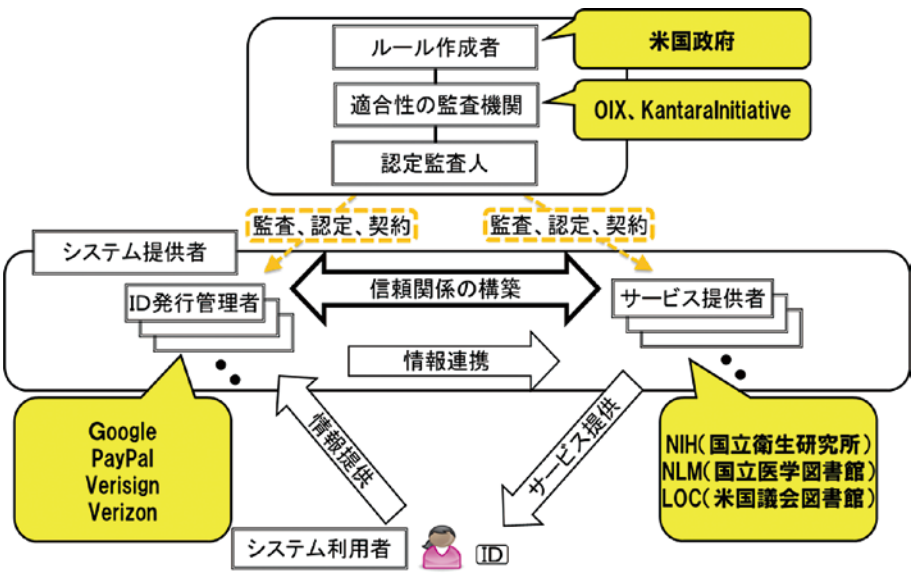

図 5　米国の ID 連携トラストフレームワークと国民 ID 制度（[7][12][13] をもとに筆者らで作成）

ment）が“ルール作成者（Policy maker)”となり，OIX（Open Identity Exchange）などの“監査機関”が認定した“監査人”が，そのルールに基づいて，Google，PayPal 等の“ID 発行管理者”の監査を実施し，認定を行う。この関係を図 5 に示す。これにより，米国民は，“認定された民間 ID”を用いて，“電子政府サービス”を利用可能となるのである。例えば，米国民は Google の ID を用いることで，いつでも米国議会図書館文献調査や書籍の貸し出し等の行政サービスを利用することができる。

そして，現在の米国の ICAM の基準では，サービス提供者を政府機関に限定している。つまり，民間 ID を使って電子政府のサイトにログインすることを可能にすることによって，電子政府利用の活性化を図っている（文献［7]，[12]，[15])。

3.3 日本の ID 連携トラストフレームワーク構築の動向

日本においては，近年になり筆者らが長年にわたり提案してきた ID 連携トラストフレームワーク構築の必要性が認識され，2015 年 11 月から経済産業省と JIPDEC（一般財団法人日本情報経済社会推進協会）を中心に「ID 連携トラストフレームワーク戦略委員会」が立ち上がり，数回の委員会が開催され，具体的な検討の緒についた段階といえる。

日本の ID 連携トラストフレームワークの検討内容を米国と比較すると，以下の 3 点に特徴がみうけられる。

① ID 発行管理者が使用する認証トークンとして，個人番号カードを中心に検討が進んでいる点である。米国では，民間 ID 発行の ID を使用して，電子政府のサイトにログインすることから検討が進んでいる。日本の場合は逆の発想で，国が発行する ID であるマイナンバーを使用することをベースにして，民間事業者がサービス提供者として認証結果と情報を連携することから検討が進められている（文献［1]，[8])。

② 日本のマイナンバー制度の認証機能は民間企業での活用も検討されているので，民間企業の事業者同士での ID 連携することが想定されている。そのために，ID 発行管理者とサービス提供者の信頼関係構築の要件として，図 6 に示すように「ID の本人確認の保証レベル」に加えて，事業者のプライバシー及び個人情報保護の信頼レベルを表す「信頼レベル」が追加されている（文献［6])。

③ 「ID の本人確認の保証レベル」として，実社会での日本の ID 利用の現状を考慮して，「ID の付番・発行時の身元確認のレベル」と「認証時の当人確認のレベル」の 2 軸を検討している。現在日本で検討されている ID 連携トラストフレームワークの中で使用する ID は，「ID の付番・発行時の身元確認のレベル」と「認証時の当人確認のレベル」のペアリングによって，表 2 に示す 4 つの保証レベルに分類されている。本論文では，以降「ID の付番・発行時の身元確認のレベル」と「認証時の当人確認のレベル」を掛け合わせたペアリングによる分類を，ID 連携トラストフレームワークにおける「ID の本人確認の保証レベル（LOA： Level of Assurance)」と呼ぶことと定義する。経済産業省の ”ID 連携トラストフレームワーク”（文献［6]）及び文献［1]，[5］を参考に，「ID の本人確認の保証レベル」の分類の内容を表 2 に示す。サービス提供者は，システム利用者に対してサービスを提供する際に，「ID の本人確認の保証レベル」に応じて利用可能とするサービスを分けて提供する必要がある。

図 6　日本版 ID 連携トラストフレームワークの保証レベル（出所：文献［6］）

表 2　ID の本人確認の保証レベル（［1］［5］［6］をもとに筆者ら作成）

保証レベル	付番・登録時の身元確認のレベル	認証時の当人確認のレベル	発行方法	例
1（低い）	不要	パスワード（6 桁以上）	Web サイトより発行。又は，電子メール送付	SNS が提供する無料の旅行案内や，グルメサイトなど
2（中程度）	信用ある機関の登録情報の参照	パスワード（8 桁以上）	登録住所への郵送など	社員証による決済など
3（高い）	公的身元証明書	多要素認証	電子メール送信と郵送を併用など	診療履歴を受取るなど
4（かなり高い）	対面での確認	ハードウェアトークン付多要素認証	手渡し，本人限定郵便など	

4.　ID 連携トラストフレームワーク構築の課題と解決策

4.1　ID 連携トラストフレームワーク構築に必要な信頼関係

ID 連携トラストフレームワークは，システム提供者の中の ID 発行管理者とサービス提供者，およびシステム利用者の 3 者から構成される。この構成者の間で信頼関係を構築することが，ID 連携トラ

ストフレームワーク構築の基本となる。

信頼関係の構築のためには，誰が（信頼元），誰を（信頼先）信頼するために，どういう要件を満たしていればよいのかを明確にし，要件を満たしていることを第三者が保証していることが必要となる。そして，システム提供者の中の ID 発行管理者とサービス提供者，およびシステム利用者の 3 者の視点からみた必要な信頼関係をまとめることが肝要であり，以下に，筆者の考える信頼関係構築のために必要となる信頼要件と要件実現の具体的策を示す。

（1） ID 発行管理者視点での信頼関係

ID 発行管理者にとっての信頼関係構築のためには，システムを利用する者がなりすましでなくシステム利用者本人であることが必要であり，加えて，個人情報を提供する相手であるサービス提供者が信頼できる事業者であることの保証が必要となる（表 3）。

（2） サービス提供者視点での信頼関係

サービス提供者にとっての信頼関係構築のためには，ID 発行管理者から連携されてくるシステムを利用する者がなりすましでなくシステム利用者本人であることが必要であり，加えて，個人情報の提供元である ID 発行管理者が信頼できる事業者であることであることの保証が必要となる（表 4）。

（3） システム利用者視点での信頼関係

システム利用者にとっての信頼関係構築のためには，個人情報を提供する先の ID 発行管理者が信頼できる事業者であることが必要であり，加えて，利用するサービスを提供するサービス提供者が信頼できる事業者であることの保証が必要となる。さらには，関連するシステム提供者全体の中で，システム利用者が自己情報を把握，統制できる状態にあることが必要となる（表 5）。

そして，この（1）から（3）の信頼関係を，第三者の統制機能によって，そのフレームワークの範囲において保証する仕組みを構築することが ID 連携トラストフレームワーク構築の基本である。

4.2 日本の ID 連携トラストフレームワーク構築の検討課題

4.1 節で示した ID 連携トラストフレームワーク構築に必要な信頼関係の内容について，“ID 連携ト

表 3 ID 発行管理者視点からみた信頼要件と要件実現の具体策

信頼元	信頼先	信頼要件	要件実現の具体策
ID 発行管理者	システム利用者	認証要求をしてくるシステム利用者が本人であること	身元確認と当人確認の保証レベルの基準策定，監査制度確立，監査結果の公開
	サービス提供者	情報提供する先のサービス提供者が，情報提供しても大丈夫な信頼できる事業者であること	プライバシー保護及び個人情報保護の観点から信頼できる事業者であることの確認，公開

表 4 サービス提供者視点からみた信頼要件と要件実現の具体策

信頼元	信頼先	信頼要件	要件実現の具体策
サービス提供者	システム利用者	ID 発行管理者から連携されるシステム利用者が本人であること	身元確認と当人確認の保証レベルの基準策定，監査制度確立，監査結果の公開
	ID 発行管理者	情報提供元の ID 発行管理者が，信頼できる事業者であること	プライバシー保護及び個人情報保護の観点から信頼できる事業者であることの確認，公開

表 5　システム利用者視点からみた信頼要件と要件実現の具体策

信頼元	信頼先		信頼要件	要件実現の具体策
システム利用者	システム提供者	共通（システム提供者全体）	個人情報を提供する先において，個人情報を自己情報コントロールできる環境であること	個人情報が情報連携において，いつ，どこで，どういう目的で利用されているかを把握でき，かつ統制可能であることの確保 ID 発行管理者とサービス提供者を自分で選択できることの確保 情報連携で使用する ID を自分で選択できることの確保
		ID 発行管理者	個人情報を預ける ID 発行管理者が信頼できる事業者であること	プライバシー保護及び個人情報保護の観点から信頼できる事業者であることの確認，公開 個人情報活用において権力を持ち過ぎていないこと，および過去に個人情報に関する不正利用のない事業者であることの確認，公開
		サービス提供者	利用したいサービスを提供するサービス提供者が信頼できる事業者であること	プライバシー保護及び個人情報保護の観点から信頼できる事業者であることの確認，公開 システム利用者が要求するサービスを提供している事業者であることの確認，公開

ラストフレームワーク活用した官民連携の在り方に関する調査研究（平成 27 年度）”（文献［1］）をベースにして，日本での検討状況を確認してみる。まず，表 3 と表 4 に示したシステム提供者視点からみた信頼実現の具体策は，図 6 に示されているように保証レベルと信頼レベルの基準策定の検討が進んでおり，具体化が進められているといえる。しかし，表 5 に示したシステム利用者視点からみた信頼要件の実現策についての検討は緒についたばかりであり，具体的な方式は殆ど示されていない。経済産業省発表の「トラストフレームワークを用いた個人番号の利活用推進のための方策」（文献［8］）においても，システム利用者が安心して個人情報を提供できない課題への対応の必要性が記述されているが，具体的な実現策は今後の検討という状態にある。そこで本論文では，4.1 節（3）で示したシステム利用者視点での信頼要件を実現するために解決しなければ課題を，以下の 3 つの視点から整理し，解決策について考察する。

①　システム利用者の ID 発行管理者への信頼関係の不安の課題

システム利用者は，情報システムや ICT，法制度ついて素人である。システム利用者に対して，信頼できる機関が ID 発行管理者の信頼度を客観的に評価して情報提供する仕組みが必要である。特に重要となるのは，システム利用者にとって直感的に理解しやすくする工夫である。ID 発行管理者の信頼度を直感的かつ客観的に判断できる仕組みがない現状では，ID 連携トラストフレームワークはシステム利用者から信用されず，利用されない絵に描いた餅となってしまう。

②　システム利用者のサービス提供者への信頼関係の不安の課題

現在の情報社会では，多くの偽サイトの存在が社会問題となっている。システム利用者対して，信頼できる機関がサービス提供者サイトの信頼度を客観的に評価して情報提供する仕組みが必要である。そしてその仕組みは，ID 発行管理者と同様に，システム利用者にとって直感的に理解しやすい仕組みでなくてはならない。

③ 自己情報コントロールへの不安の課題

プライバシー保護に必要な自己情報コントロールの確立のためには，システム提供者内の ID 連携環境において，いつ，どこで，どういった目的で自分の個人情報を使用しているのかを把握できる仕組み作りが必要である。そして，問題を認識した場合には，訂正や利用停止など自己情報を統制できる仕組みが必要となる。現在の日本の ID 連携トラストフレームワークの検討では，ログイン ID としてマイナンバーの使用と自己情報コントロール対応策としてのマイナポータルの検討が先行している。

システム利用者が利用するサービスによって，ログイン ID としてマイナンバーの使用だけではなく，保証レベルの異なる民間企業のログイン ID を使用可能とすることが必要である。そのことによって，システム利用者は，自己情報が国の監視下にあるという不安を払拭できるだけでなく，自分のログイン ID とそれに紐づく情報を自分でコントロールできるという安心に繋げることができることとなる。

これらの 3 つの視点からみた課題を解決することによって，システム利用者が安心して使える便利な仕組みを構築することが可能となる。

4.3 日本の ID 連携トラストフレーム構築課題の解決策

日本の ID 連携トラストフレームワーク構築では，システム利用者視点での信頼関係構築に必要な仕組みについて，具体的な検討は始まったばかりの段階にある。ID 連携トラストフレームワークの構築にとって，4.2 節で示したシステム利用者視点からみた 3 つの課題を解決することは，最優先課題と考えられる。そこで，本論文では，この 3 つの課題に対する具体的解決策を提案する。

（信頼要件 1）システム利用者が ID 発行管理者を信頼するための要件

「システム利用者が，ID 発行管理者に対して安心して個人情報を提供できる」ことを保証するための要件であり，以下に示す仕組み作りが必要である。

① ID 発行管理者のセキュリティに関する信頼度を公開する仕組み

ID 発行管理者が，プライバシー保護及び個人情報保護の観点から信頼できる事業者であることを，公開情報を利用して確認できる仕組みの構築が必要である。具体的には，ID 連携トラストフレームワーク検討委員会で検討されている図 6 の信頼レベルの基準の策定と，その基準に沿った監査の実施，監査結果をシステム利用者に対してわかりやすく知り得る状態での公開する仕組みの構築である。その仕組みには，既に運用されている P マーク制度（プライバシーマーク制度）や ISMS 制度（情報セキュリティマネジメントシステム適合性評価制度）と，マイナンバー制度（文献［2］）の中で具体化が開始された PIA（プライバシーインパクトアセスメント）（文献［10］）を加えた，事業者の信頼度を評価し公開する仕組みの導入が必要と考える。さらに，これらの評価内容は非常に専門的な内容でシステム利用者には理解し難いものであるため，これらの評価内容をシステム利用者にとって理解しやすく，正しく信頼度を評価できる情報に整理し，公開する仕組み作りが必要である。そして，システムの素人であるシステム利用者に対しては，ある程度直感的に理解できる仕組みが必要である。その実現のためには，例えば図 7 に示すようなレーダーチャートを使った分かり易い情報公開などの仕組みを構築すべきである。

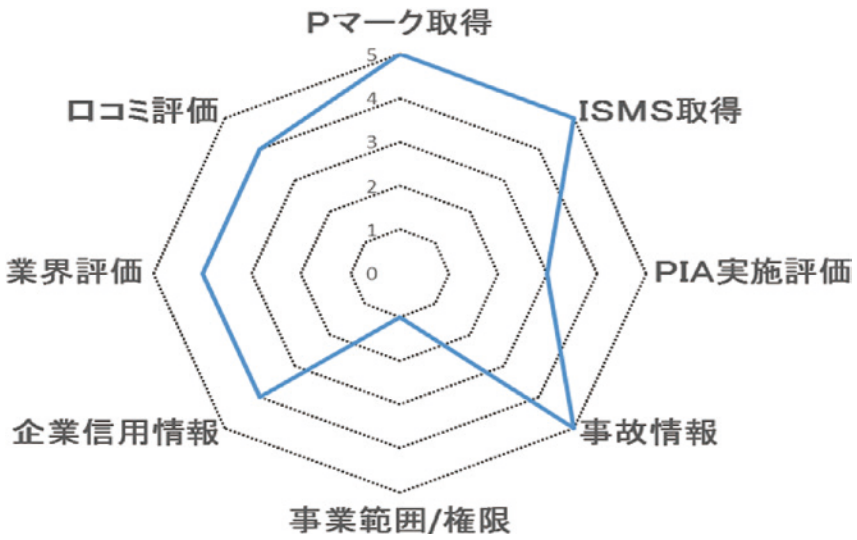

図 7　ID 発行管理者の信頼度・信用度評価レーダーチャートのイメージ

②　ID 発行管理者の事業者としての信用度を公開する仕組み

ID 発行管理者の事業者としての事業内容，財務状況，法令順守状況などを，公開情報を利用して確認できる仕組みの構築が必要である。加えて，ID 発行管理者が，個人情報の活用に対して強力な権力を持たないこと，過去に個人情報の活用に関して事故や問題を起こしていない事業者であることを客観的に知り得る環境の構築が必要である。その仕組みの実現のためには，帝国データバンクや東京商工リサーチなどの調査会社による企業信用情報，四季報による投資情報，飲食店の口コミ評価情報，旅行会社のホテルや旅館評価のような業界での評価情報などを加味した情報の公開が有効であると考える。しかし，これらの情報を全て加味することは膨大な情報量になってしまうため，システム利用者が容易に理解可能で，かつ事業者の信用度を判断できるよう情報を整理し，公開することが必要である。その実現のためには，① の信頼度評価の情報と合わせて図 7 に示すようなレーダーチャートを使った情報公開の仕組みなどを構築すべきである。

（信頼要件 2）システム利用者がサービス提供者を信頼するための要件

「システム利用者が，サービス提供者が提供するサービスを安心して利用できる」ことを保証するための要件であり，以下に示す仕組み作りが必要である。

①　サービス提供者のセキュリティに関する信頼度を公開する仕組み

サービス提供者が，プライバシー保護及び個人情報保護の観点から信頼できる事業者であることを，公開情報を利用して確認できる仕組みの構築が必要となる。その実現には，（信頼要件 1）の ① と同様に，システム利用者が直感的に理解しやすい仕組み作りが有効である。

②　サービス提供者の事業者としての信用度を公開する仕組み

サービス提供者の事業者としての事業内容，財務状況，法令順守状況などを，公開情報を利用して確認できる仕組みの構築が必要となる。特に，提供しているサービス内容と事業内容のマッチングや，サービス内容にふさわしい信用できる財務状況の企業であるか否かなどを判断するための情報公開をする仕組みの構築が必要である。その実現には，（信頼要件 1）の ② と同様の仕組み作りが有効である。

（信頼要件 3）システム利用者がシステム提供者全体を信頼するための要件

「システム利用者が，システム提供者全体の中で自己情報コントロールを実現できる」ことを保証するための要件であり，以下に示す仕組み作りが必要である。

① 自己情報を把握し統制する仕組み

ID 連携トラストフレームワークの中で，自分の ID とそれに紐づいた個人情報が，いつ，どこで，誰に，どういう目的に使われているのかを知り得る仕組みの構築が必要である。そして，使用されている自分の ID と個人情報に対して，訂正や利用停止などの統制ができる仕組みの構築が必要である。日本の ID 連携トラストフレームワークの検討では，個人情報保護法と番号法に則り，マイナポータルという自己情報コントロールの仕組みを構築して対応することが計画されている。ただ，マイナポータルは個人番号に対応した範囲でのみ検討されているという課題がある。マイナポータルで検討されているような仕組みを，範囲を広げて民間企業のログイン ID を含めた幅広い仕組みを作ることが必要である。

② ID 発行管理者を選択できる仕組み

ID 連携トラストフレームワークの中で，自分が利用したいログイン ID を複数の選択肢の中から，自分で選択できる仕組みの構築が必要である。現在の日本の ID 連携トラストフレームワークの検討では，公的個人認証を使用した ID のみの検討が先行している。業務が要求する信頼度要求レベルの低い認証においては，公的個人認証を使用せずに民間企業の発行するログイン ID も使用できる仕組みを作ることが肝要である。この仕組みを実現することによって，民間企業の参加数も増え，システム利用者の利便性が向上し，ID 連携トラストフレームワークの普及が進むこととなる。

ログイン ID を選択するということは，ID 発行管理者を選択とするということを意味する。その選択の仕組みは，システム利用者に対して，図 7 のイメージ図に示したような直感的に選択の判断ができる仕組みに加えて，プルダウンメニューのような形式で一覧の中から容易に ID 発行管理者を選択できる便利な仕組み作りが必要である。

③ サービス提供者を選択できる仕組み

ID 連携トラストフレームワークの中では，自分が利用したいサービス提供者を複数の選択肢の中から，自分で選択できる仕組みの構築が必要である。その際には，②と同様にシステム利用者に対して，図 7 のイメージ図に示したようなある程度直感的に選択の判断ができる仕組みと，プルダウンメニューのような形式で一覧の中から容易にサービス提供者を選択できる仕組み作りが必要である。

以上の 3 つの信頼要件の実現に必要となる具体的な仕組みを構築することが，システム利用者も含めた信頼関係の構築につながり，システム利用者からみて，提供されたシステムを安心して利用できる環境が整うことになると考える。

5. ま と め

ビッグデータ時代を迎え，ビッグデータの有効活用のために ID エコシステムを実現すること，そして，その実現手段として ID 連携トラストフレームワークを構築することは有効である。しかし，効率的なビッグデータ活用とプライバシー保護の両立は重要な課題であり，この両立のためには，システム利用者を含めた信頼関係を構築することが必須である。そのためには，4 章で述べたようにシ

ステム利用者の視点からみた以下の 3 つの信頼要件の実現が肝要である。

・システム利用者が，ID 発行管理者に安心して個人情報を提供できる

・システム利用者が，サービス提供者のシステムを安心して利用できる

・システム利用者が，システム提供者内で自己情報コントロールができる

日本の ID 連携トラストフレームワークの検討は始まったばかりであるが，今後の検討において，システム利用者視点からみた信頼要件の確立を実現することで，効率的なビッグデータ活用とプライバシー保護が両立した ID 連携トラストフレームワークの構築が可能となると考える。システム利用者からの信頼があって初めて，ID 連携トラストフレームワークが実社会の中で受け入れられ運用されていくこととなる。そして，ID 連携トラストフレームワークの構築のためには，その仕組みの構築コストを誰が負担するのか，このフレームワークに参加する動機付けは何かなど，まだまだ検討課題が残されている。いずれも情報技術の発展と法制度の整備だけでは解決できない，ビッグデータ時代の社会基盤をどう構築するかという課題である。

今後の研究では，ビッグデータの有効活用とプライバシー保護の両立した社会基盤のあり方について，さらに具体的な研究を深めていきたい。

謝辞

本論文の作成にあたり，数々の有益なご指摘を賜った査読者の方々，丁寧にご指導いただいた魚田勝臣専修大学名誉教授に謹んで感謝の意を表する。

参 考 文 献

［1］ 一般財団法人日本情報経済社会推進協会 電子情報利活用研究部，“ID 連携トラストフレームワークを活用した官民連携の在り方に関する調査研究（平成 27 年度）”，2015 年，（2017-02-21），http://www.meti.go.jp/policy/it_policy/id_renkei.

［2］ 宇賀克也，『番号法の逐条解説』，有斐閣，2015.

［3］ Oasis sstc, ”security assertion markup language version 2.0（saml 2.0）”,（2017-02-21），http://saml.xml.org/saml-specifications.

［4］ ”Openid authentication 2.0-final”,（2017-02-21），https://openid.net/specs/openid-authentication-2_0.html.

［5］ 各府省情報化統括責任者（CIO）連絡会議，“オンライン手続におけるリスク評価及び電子署名・認証ガイドライン”，2010 年 8 月，（2017-01-04），http://www.kantei.go.jp/jp/singi/it2/guide/guide_line/guideline100831.pdf.

［6］ 経済産業省，“ID 連携トラストフレームワーク”，（2017-02-21），http://www.meti.go.jp/policy/it_policy/id_renkei/.

［7］ 経済産業省 満塩尚史，“ID 連携トラストフレームワークの推進”，2014 年 1 月，（2017-06-06），https://jics.nii.ac.jp/?action=pages_view_main&active_action=repository_view_main_item_detail&item_id=77&item_no=1&page_id=43&block_id=435.

［8］ 経済産業省，“トラストフレームワークを用いた個人番号の利活用推進のための方策”，2014 年 4 月，（2017-09-27），http://www.kantei.go.jp/jp/singi/it2/senmon_bunka//number/dai3/siryou3.pdf.

［9］ ”The oauth 2.0 authorization protocol”,（2017-02-21），http://tools.ietf.org/html/draft-ietf-oauth-v2.

［10］ 瀬戸洋一，伊藤洋昭，六川浩明，新保史生，村上康二郎，『プライバシー影響評価 PIA と個人情報保護』，中央経済社，2010.

［11］ 野村総合研究所第 148 回 NRI メディアフォーラム，“「ID エコシステム」導入の効果―国民 ID 制度に民間の活力を生かす”，2011 年 2 月，（2017-02-21），https://www.nri.com/jp/event/mediaforum/2011/forum148.html.

［12］ Federal identity, credentialing, and access management : Trust framework provider adoption process（tfpap）for levels of assurance 1, 2, and non-pki 3, 2009.

［13］ Mary Rundle, Eve Maler, Anthony Nadalin, Drummond Reed, Mary Rundle, and Don Thibea, ”The open identity trust framework（oitf）model.”, 2010 年 3 月,（2017-02-21）, http://www.openidentityexchange.org/wp-content/uploads/2017/02/open_identity_trust_framework_model_2010.pdf#search=%27open+identity+trust+framework%27.
［14］ 八木晃二,『完全解説 共通番号制度』, アスキーメディアワークス, 2012.
［15］ 八木晃二,『マイナンバー法のすべて―身分証明, 社会保障からプライバシー保護まで―共通番号制度のあるべき姿を徹底解説』, 東洋経済新報社, 2013.