トラストサービスの国際連携構想

慶應義塾大学　環境情報学部 教授　手塚（てづか）　悟（さとる）

1. はじめに

昨今、石油等の従来型資源と同様に、データを貴重な資源として取り扱う動きが、世界中で広がってきている。

GAFAに代表されるようなデータ資源獲得を中心とした覇権競争が激化しており、この競争を制したものが世界を制すると言っても過言ではない状況になってきている。このデータ資源をいかに安心安全に流通させ、今後の世界的レベルでの健全なデジタル社会を実現できるかが問われている。2019年6月に開催されたG20の場においても、重要な課題の一つとして、このデータ流通を取り上げたことは、世界的課題としての関心の高さを表している。

本稿においては、世界を取り巻くデータ流通の現状を概観し、それを支えるトラストサービスとトラスト基盤について考察するとともに、トラストサービスの国際連携構想について説明する。

2. データ流通の重要性とその状況

(1) 重要性

我が国では、2016年1月に閣議決定された「科学技術基本計画」において、初めて「世界に先駆けた『超スマート社会』の実現(Society 5.0)」が明記された。世界では既に、モノづくり分野を中心に、ネットワークやIoT等を活用した取組みが表明されているが、我が国ではモノづくりだけでなく様々な分野に拡大し社会変革につなげていくさらに広い概念を提唱している。

このように、我が国においては、現在Society 5.0が中心的施策となっており、これらを梃子として、国際的な産業競争力を付け、重要インフラの輸出にも貢献することが重要である。そのためにも、更なるビジネス力の強化を目指し、安心安全なデータ流通の基盤構築を推進することは不可欠である。より安心安全の向上が図られたSociety 5.0を構築し、一層進化した概念の導入が必要である。

(2) 状況

我が国のSociety 5.0におけるデータ流通の強化により、さらに魅力的なサービス等を提供するのは最も重要な取組みであるが、さらにこれらの様々なサービスの国際的な拡張性をどのように実現するかが重要な課題の一つである。

世界を取り巻くデータ流通の現状を概観すると、日米欧等においては、「自由と信頼」を原則としたデータ流通の概念のもと、個人、企業、政府等が生み出す膨大なデータを越境して利活用できる環境の検討を始めようとしており、特に我が国が先頭に立って推進していこうと国を挙げて標榜している。このように、世界を取り巻くデータ流通の状況を見ると、「データ流通圏」という概念が導出されつつある。

我が国のような石油等の従来型資源の乏しい国からすると、資源としてのデータは、我が国の国際競争力の源泉となる最も重要なものである。そこで、官民一体となって、このデータ資源を最大限活用する環境整備が必要不可欠であり、安心安全なデータ流通の基盤構築を可及的速やかに推進することが重要な課題である。具体的には、個人情報、知的財産情報、重要インフラ情報、安全保障情報等の国をまたいだデータ流通の基盤を整備することになるため、国際連携を踏まえたルール作りを急がなければならないと考える。

3. トラストサービスの重要性とその状況

(1) 重要性

我が国では、トラストサービスに関して、2019年6月14日に閣議決定された「世界最先端デジタル国家創造宣言・官民データ活用推進基本計画の変更について」や、2019年6月21日閣議決定された「経済財政運営と改革の基本方針2019について」でトラストサービスの記述が掲載された。それに前後して、2019年8月7日高度情報通信ネットワーク社会推進戦略本部官民データ活用推進戦略会議の「デジタル時代の新たなIT政策大綱」にもトラストサービスの記載がされた。その内容を以下に記す。

「サイバー空間での自由で安心・安全なデータ流通を支える基盤として、データの改ざんや送信元のなりすまし等を防止する仕組み（トラストサービス）の在り方について、国際的な相互運用性の観点も踏まえ、2019年中を目途に結論を得て、速やかに制度化を目指す。」

このように、トラストサービスとは、従来のサービスの機能としては同じであっても、その品質が全く別次元の高い

レベルで保障された、つまり機能の真正性が保証されたサービスである。

このトラストサービスを実現する基盤として、「トラストサービス基盤」を構築する。一般にサービスを構成する共通の機能から構成するものを基盤と呼ぶが、ここで言う「トラストサービス基盤」は共通機能の真正性を確実に保証した基盤のことである。

機能の真正性を保証するとはどういうことかと言うと、例を挙げていえば、サイバー空間で扱われるヒト、組織、モノ、データ等のオブジェクトの真正性が保証され、これにより初めて、これらのオブジェクトが取り扱う様々な機能の真正性が保証されるという、真正性保証の連鎖により実現するものである。さらに、これらの機能の真正性の保証により、それらの機能で構築されたサービスも真正性が保証されると言う連鎖である。

このように、真正性保証の連鎖により構成された信頼に値するサイバー空間をいかに実現するか、つまりSociety 5.0の様々なサービスの安全性をどのように保証するかが、今後のサイバー空間の健全な発展につながっていくかどうかの鍵である。

(2) 状況

(ア) EUの動向

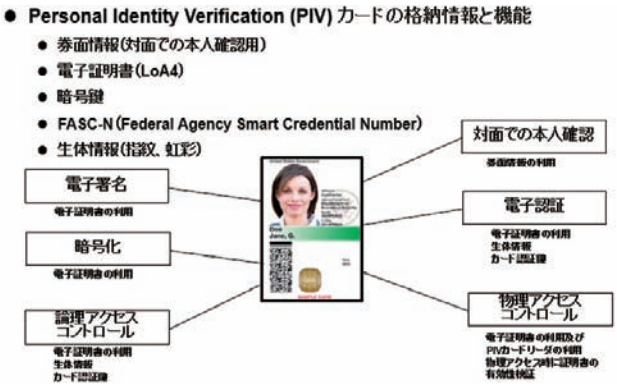
EUの動向を概観すると、2014年9月に施行されたelectronic IDentification, Authentication and Signature Regulation (eIDAS法) が、EUの28か国に共通基盤であるトラストサービス基盤を構築し、その上で実現するトラストサービスを提供することで、EU全域における「Digital Single Market」の実現を目指している。言い換えれば、EUの28か国におけるトラストサービスによる市民のデジタル経済活動の実現である。

具体的には、eIDAS法は、我が国のマイナンバー法、公的個人認証法、電子署名法、タイムスタンプに関わる指針等、これらを統合した法律であるので、図1に示すようなEUの加入国で発行されている国民カードのICチップ内に、認証用、署名用の2つの用途別の秘密鍵と電子証明書が格納されている。

図2にeIDAS法の下で構成されるトラストサービスとトラスト基盤を示す。なお、EUにおける相互認証の技術的な手法としては、Trust List (TL) 技術で実現している。EUの相互認証を実現する認証局は、技術的にはTLで米国のBridge Certificate Authority (BCA) とは異なる技術であるので、米国のような相互認証を実現する認証局のトポロジーはないが、EUの28か国が参加していることから、少なくとも我が国の相互認証を実現する認証局より大規模であると考えられる。

■図1. フランスの国民カードの概要

■図2. トラストサービスの概要



■図3. PIVのICカードの概要

(イ) 米国の動向

米国の動向を概観すると、米国は政府内のシステムのトラスト化を既に実現している。具体的には、トラスト基盤として、図3に示すような政府職員にはPersonal Identity Verification

(PIV) のICカードを配布し、認証用、署名用、暗号用の3つの秘密鍵とそれに対応する3つの電子証明書をICチップ内に格納し、資料や設計書等のコンテンツに対して、誰が作成したかを署名用の電子認証書を使って実現する。さらに暗号化をすることで、仮に漏えいしたとしても内容を解読できないようにしている。その上、認証用の電子証明書を使うことで、サイバー空間においても本人認証を確実に行い、米国政府内の様々なシステムやコンテンツへのアクセス制御を可能としている。こうすることで、PIVのICカードが1つあれば、サイバー空間での処理が安全に実現されている。併せて、物理的アクセス制御にも使用している。

さらに、米国の政府調達にも使われていることから、民間企業側にはPIV-I (Interoperable) というICカードが発行されている。この発行には、米国INST SP800-63のスキームが使われている。これらのPIV、PIV-Iを発行する相互認証を実現する認証局のトポロジーを図4に示す。なお、米国における相互認証の技術的な手法としては、BCA技術で実現している。

図4を見ると、我が国における国内の相互認証を実現する認証局のトポロジーと米国におけるそれとは規模において明らかに違いがある。米国は、政府調達にこの巨大な認証基盤をトラストサービス基盤として利活用している。具体的な利用としては、現在我が国でも話題になっている米国INST SP800-53対応に関するサプライチェーンのトラストサービス基盤である。米国はこのような戦略の下に、トラストサービス基盤の整備をしていると考える。

さらに、トラストサービスサービスに関しては、米国政府調達等で導入する米国NIST SP800-53の技術仕様で策定されているクラウドセキュリティ基準Federal Risk and Authorization Management Program (FedRAMP) の認証を取った製品群で構築したクラウドで、トラストサービス基盤を提供する模様である。

(ウ) EU・米国と我が国の比較

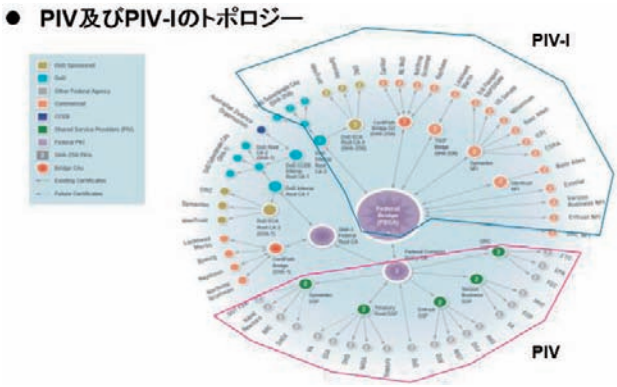
EUは、加盟国28か国の市民が信頼されたデジタル経済環境での「Digital Single Market」を実現するために、eIDAS法によるトラストサービス基盤としての国民カード (eIDカード) を活用して、トラストサービスを実現している。米国は、政府内システムと政府調達に関連する分野において、トラストサービス基盤としてのPIV、PIV-Iを活用して、トラストサービスを実現している。

一方の我が国は、Society 5.0やサプライチェーンの分野において、トラストサービス基盤としてのマイナンバーカードや法人、ヒトの認証を活用して、トラストサービスを実現することを今後に向けて推進していく必要がある。

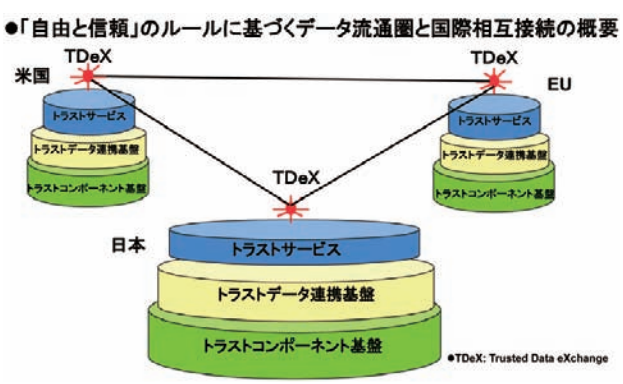
4. 国際連携を踏まえたトラストサービス

「自由と信頼」のルールに基づくデータ流通圏と国際連携を考えた場合、図5のようなアーキテクチャを検討する必要があると考える。日本・EU・米国の3極において、トラストサービス、トラストデータ連携基盤、トラストコンポーネント基盤の3層構造を構築し、その上にデータ取引所であるTrusted Data eXchange (TDeX) を介して、3極でのデータ流通を実現する構想である。

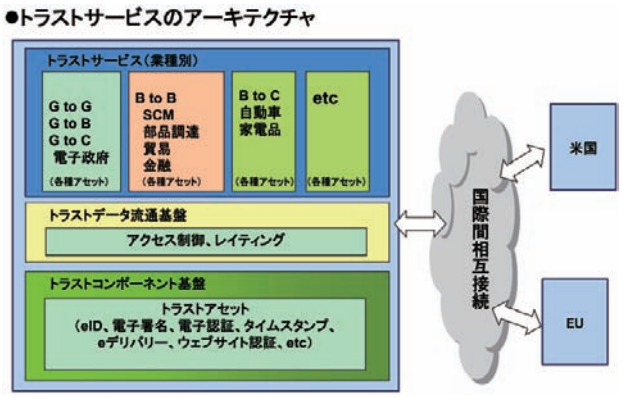
さらに、図6のとおり、トラストコンポーネント基盤が、今まで説明してきたトラスト基盤にあたり、機能としてはeID、電子署名、電子認証、タイムスタンプ、eデリバリー、ウェブサイト認証等がある。その上で、EU・米国と我が国がトラストサービス基盤で国際連携をする日が必ず来ると考え、現在、図8のような「International Mutual Recognition」



■図4. PIV及びPIV-Iのトポロジー



■図5. データ流通圏と国際相互連携



■図6.　トラストサービスにけるアーキテクチャ

を検討している。

図7において、米国のFBCAはFederal Bridge Certificate Authorityのことであり、図4で示した相互認証を実現する認証局のトポロジーを簡略化したものである。EUのEULoTLは、EU List of Trust Listのことで、28か国のTLを束ねたリストを表している。技術的にはEUと米国では方式が違うが、概念上は図7のように考えても、International Mutual Recognitionの検討には特に問題はない。また、我が国の範囲で赤い色で書かれている部分はいまだ実現されていない部分であり、今回の国際連携を考える意味では基本的には必要となる認証局である。

JBCAとは、Japan Bridge Certificate Authorityのことであり、米国のFBCAとEUのEULoTLとの連携をする部分である。この部分の責任元がどこの組織になるのかを決めることが我が国にとっては必須であり、EU Commission・米国政府とのInternational Mutual Recognitionを検討するためには、早急に決めなければならない。

そのためにも、直ちに我が国において、政府レベルと民間レベルの検討チームを設立し、さらに官民合同チームでの検討を通して、EU・米国との3極での検討を開始すべきである。

5. おわりに

我が国が、データ流通を支えるトラストサービス基盤の構築を他の国よりいち早く実現することは、国際的な産業競争力を秀でたものとする最大のチャンスである。そのためにも、本稿で示したトラストサービス基盤は、安心安全なデータ流通を実現するための最も重要な機能であり、それら機能の真正性の保証が必要不可欠である。

その上で、トラストサービスの国際連携構想を推進することで、いかに世界における我が国の国際競争力を最大限に発揮し、かつ維持していくかが問われている。

■図7.　トラストサービスとトラスト基盤の国際相互認証