［ディジタルエコノミー時代のサイバーセキュリティ―ディジタルトランスフォーメーション促進の基盤確立に向けて―］

② 国際連携を踏まえたトラストサービスとトラスト基盤

手塚　悟 | 慶應義塾大学

背景

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．世界ではすでに，モノづくり分野を中心に，ネットワークやIoT等を活用した取り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さまざま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．

実際，Society 5.0の実際の取り組みとしては，サイバー空間とフィジカル空間（現実空間）が高度に融合した超スマート社会である「データ駆動型社会」を未来の姿として共有し，共通基盤としての「サービスプラットフォーム」構築も現在進行中である．さらには，データ駆動型社会を表しているSociety 5.0により，さまざまなデータのつながりから製造業等を中心とした新たな付加価値を創出していくConnected Industriesも提唱され，サプライチェーンでの「サービスプラットフォーム」構築も推進されつつある．

以上のように，我が国においては，現在Society 5.0やサプライチェーン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つけ，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，さらなるビジネス力の強化を目指し，サービス品質の向上は当然としても，サイバーセキュリティの観点からはより安全性の向上が図られたSociety 5.0やサプライチェーンを構築し，一層進化した概念の導入が必要である．

トラストサービスとトラスト基盤

サイバーセキュリティの観点から見れば，Society 5.0やサプライチェーンの機能強化により，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り組みであるが，その一方でこれらのさまざまなサービスの安全性をどのように保証するかが最大の課題になる．

1つの解決策として「トラストサービス」と「トラスト基盤」の導入がある．トラストサービスとは，従来のサービスの機能とは同じであってもその品質がまったく別次元の高いレベルで保証された，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，下記のような「トラスト基盤」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いうと，例を挙げていえば，サイバー空間で扱われるヒト，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さまざま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いう連鎖である．

以上のように，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させ，今

後のサイバー空間の健全な発展につなげていくかが問われている.

オブジェクトの真正性保証

サイバー空間における，オブジェクトの真正性保証とは, ヒト, モノ, データ等のオブジェクトがいかに「なりすまし」や「改ざん」のない状態でさまざまなサービスや機能が取り扱われるかどうかにある.

つまり，サイバー空間の中では，ヒトの場合にはいかに「本人」であることの真正性が保証されるかであり，モノの場合にはいかに「本物」であることの真正性が保証されるかであり, データの場合にはいかに「完全」であることの真正性が保証されるかである.

これらを実現するには，以下に示す考え方が必要になる.

識別：Identification

信頼のおける機関からヒト，モノ，データ等に対する ID やクレデンシャルを割り振ることである.

(1) ヒトに対する ID の割り振り方に関する国際的レベルでの標準としては，米国 National Security Standard Technology（NIST）の“Digital Identity Guidelines”[1] があり，3 レベルの ID と紐づくクレデンシャルの割り振り方が示されている.

例を以下に示す.

- **ハイレベルの割り振り方**

本人と直接対面で ID を割り振り，その ID に紐づくクレデンシャルをハードウェアトークンの中に収納する.

- **ミドルレベルの割り振り方**

本人と直接対面で ID を割り振り，その ID に紐づくクレデンシャルをソフトウェアトークンの中に格納する.

- **ローレベルの割り振り方**

本人の自己申告により ID を割り振り，その ID に紐づくクレデンシャルをハードウェアでもソフトウェアでもどちらでもよいトークンの中に格納する.

これらの国際的な基準からすると，我が国のマイナンバーシステムにおいては，ID であるマイナンバー，さらにはマイナンバーカードの IC チップ内に格納される公的個人認証システムの本人の秘密鍵とそれに対応する公開鍵証明書は, IC チップがハードウェアトークンに相当するので，ハイレベルの割り振り方で実現されているといえる．つまり，ヒトの場合の「本人」であることの真正性保証が確実にいえる世界最高水準のシステムである.

また，Society 5.0 やサプライチェーンの場合は，企業ユースが多いと考えられるので，ヒトという場合には，法人のヒトとなり，マイナンバーのような個人の場合とは異なる．このような場合には，すでに 2018 年 1 月に施行した「電子委任状の普及の促進に関する法律（電子委任状法）」を活用することで，法人のヒト，すなわち一般社員の真正性保証を確実に実現することができる.

(2) モノに対する ID の割り振り方に関して国際的には，IoT の進展により，さまざまな通信機器や製造装置等のモノに ID を割り振るが，ID を割り振る対象が重要である.

- **割り振る対象**

一般的には，完成品であるモノに ID を割り振るが，サプライチェーンを考えた場合には，サプライチェーン網の半完成品や部品にも ID を割り振ることが必要であるので，これらに対しても適応できるようにする必要がある.

これらの ID の割り振りにより，サプライチェーン網での ID による管理の下，「模造品」の対策や「バックドア」等の不正なハードウェアやソフトウェアの侵入を回避することで，本物であることの真正性保証を実現することが可能となる.

(3) データに対する ID の割り振り方については，ヒト，モノについては信頼のおける機関が ID を与える形で割り振るが，データの場合には，データそれ自体を使って，一般にはハッシュ関数の性質を利

用して，データが１ビットでも違えば違う値になることから，データの場合には，このハッシュ値をもってIDとする．

このハッシュ値の性質を使うということは，Society 5.0のデータ駆動型社会においては，このデータが核であり，サプライチェーンにおいては設計図面等が重要なデータであるので，ハッカー等の悪意のある人がプログラムや設計図面等のデータを改ざんした際には，改ざん前のデータと照合することで，改ざんされたかどうかを検証することができるため，データの「完全」であることの真正性保証を確認することが可能となる．

認証：Authentication

サイバー空間においては，ヒト，モノ，データ等のオブジェクトが，お互いにネットワークを介して連絡を取るときに，お互いの相手が「なりすまし」や「改ざん」のない，真正性が保証された相手であることの「認証」が検証し保証されたならば，その後は信頼の下で次のステップに進み，最終的にトラストサービスを実現する．

このお互いの相手を認証することを，「オブジェクト認証」と呼び，サイバー空間の中では，常にお互いネットワークを介してつなぐときに，まずは「オブジェクト認証」の処理から入ることで，真正性の保証を実現する．

認可：Authorization

サイバー空間においては，「オブジェクト認証」をした後は，そのオブジェクトが，ヒトのオブジェクトの場合，たとえば，Society 5.0の環境下では，データ連携のためにデータベースにアクセスすることが考えられる．その際，データベース上にあるデータの特性からアクセスして良いヒト，悪いヒトのアクセス制御をする必要がある場合には，そのヒトの属性を検証してデータベースへのアクセス「認可」を与える．

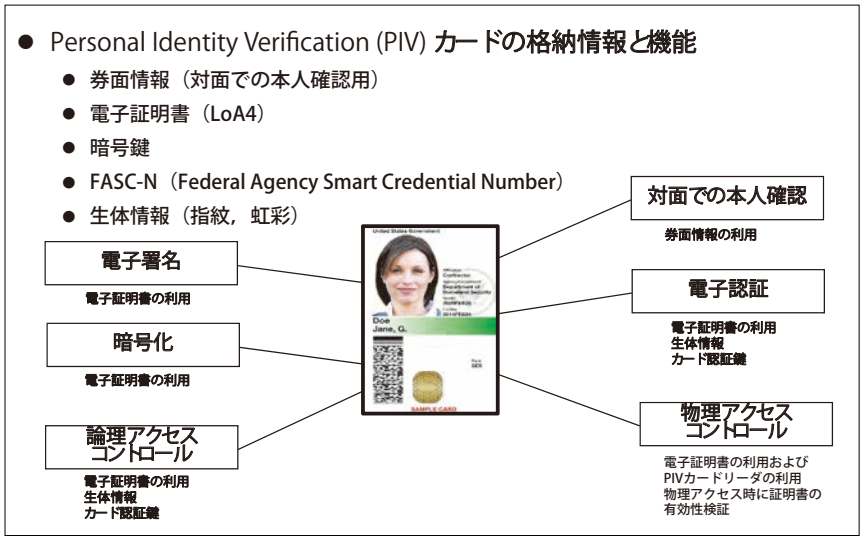
この「認可」の機能は，トラストサービスがどのような属性を持ったヒト，モノ，データ等のオブジェクトに，トラストサービスのどのレベルの機能を提供するかを決定するメカニズムである．

海外の動向

以上，我が国のSociety 5.0やサプライチェーンを支える「トラストサービス」と「トラスト基盤」，さらには「オブジェクトの真正性保証」に関して述べてきたが，このような環境は，海外，特に米国・EUではどのようであるか，次に概観する．

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すでに実現している．具体的には，トラスト基盤として，図-1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



■図-1　PIVのICカードの概要

プ内に格納し，資料や設計書等のコンテンツに対して，だれ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，仮に漏洩したとしても内容を解読できないようにしている．

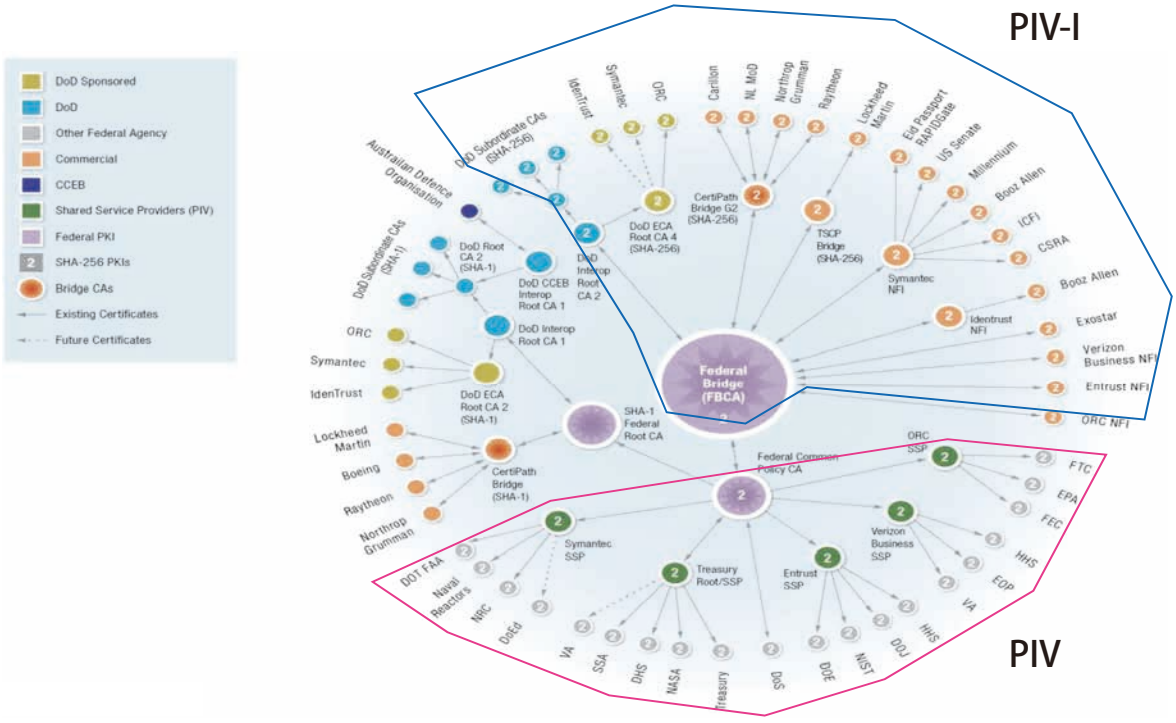
その上，認証用の電子証明書を使うことで，サイバー空間においても本人認証を確実に行い，米国政府内のさまざまなシステムへのアクセス制御を可能としている．こうすることで，PIV の IC カード 1 つあれば，サイバー空間での処理が安全に実現されている．併せて，物理的アクセス制御にも使用できる．さらに，米国政府調達にも使われていることから，民間企業側には PIV-I（Interoperable）という IC カードが発行されている．この発行には，米国 INST SP800-63 のスキームが使われている．

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 -2 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，Bridge Certificate Authority（BCA）技術で実現している．

この図 -2 を見ると，我が国の相互認証を実現する認証局のトポロジーと米国のそれとは規模において明らかに違いがある．米国は，この巨大な認証基盤を活用して，米国政府調達のトラスト基盤として利用している．

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 対応である．つまり，今までに示してきたサプライチェーンのトラスト基盤である．米国はこのような戦略の下に，トラスト基盤の整備をしていると考える．

さらに，トラストサービスに関しては，このトラスト基盤を活用し，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，トラストサービスを提供する模様である．



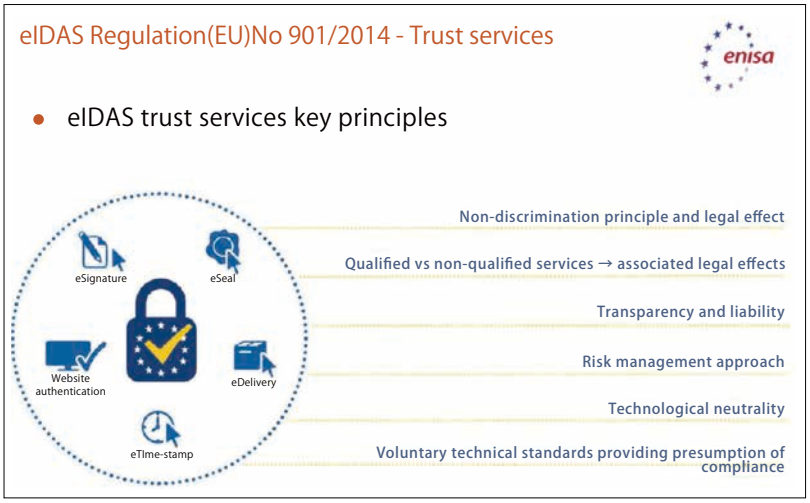
■図 -2　PIV および PIV-I のトポロジー

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 カ国に共通基盤であるトラスト基盤を構築し，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 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 カ国における市民の経済活動のトラスト化の実現である．

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，タイムビジネスにかかわる指針を統合した法律であるので，図 -3 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 つの用途用の秘密鍵と電子証明書が格納されている．

■図 -3　フランスの国民カードの概要



■図 -4　EC におけるトラストサービスとトラスト基盤の状況

図 -4 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 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 カ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．

米国・EU と我が国の比較

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．

EU は，加盟国 28 カ国の市民が信頼された経済環境での Digital Single Market を実現するために，eIDAS 法によるトラスト基盤としての国民カードを活用して，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，トラスト基盤としてのマイナンバーカードや法人の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推進する必要がある．

国際連携

すでに米国・EU のトラストサービスとトラスト基盤の動向は述べたが，今後近いうちに，米国・EU と我が国がトラストサービスやトラスト基盤で国際連携をする日が必ず来ると思われる．そこで，図 -5 のような「International Mutual Recognition」を検討してみることにする．

図 -5 において，米国の FBCA は Federal Bridge Certificate Authority のことであり，図 -2 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 カ国の TL を束ねたリストを表している．

先にも述べた通り，技術的には米国と EU では方式が違うが，概念上は図 -5 のように考えても，International Mutual Recognition の検討には問題ない．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といえる．

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になるのかが，我が国にとって必須であり，米国政府・EU Commission 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，ただ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も通して，米国・EU との 3 極での検討を開始するべきである．

今後に向けて

我が国における Society 5.0 とサプライチェーンの実現は，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．そこで，従来からの日本製品の品質に，セキュリティの機能を加えることで，世界に類のないサービスや製品を提供し，世界の最先端を歩んでいくことが重要である．

そのためにも，本稿で示したトラストサービスとトラスト基盤は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．

今後は，トラストサービスとトラスト基盤の国際連携を推進することで，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．

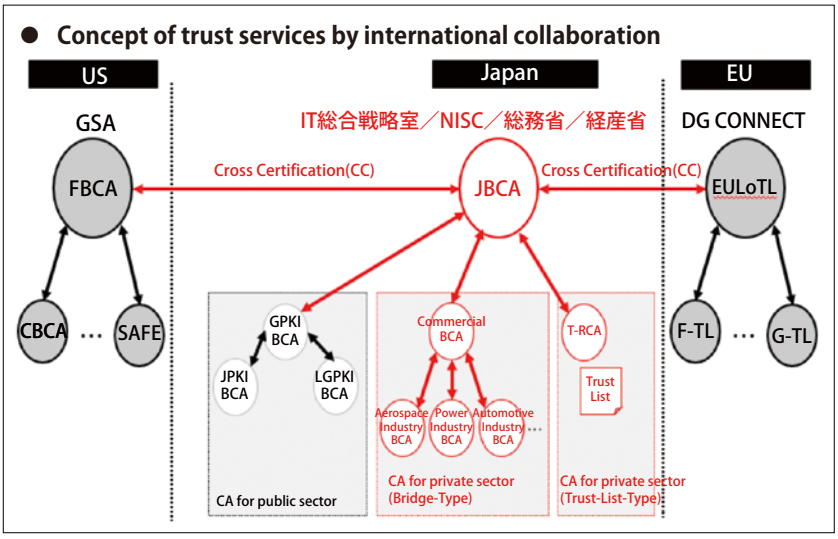
参考文献

1) National Security Standard Technology (NIST) : Digital Identity Guidelines, Special Publication (SP) 800-63, Version3 (2017).

(2018 年 9 月 11 日受付)

手塚　悟（正会員） tezuka@sfc.keio.ac.jp

慶應義塾大学大学院政策・メディア研究科特任教授．2004 年度，2008 年度本会論文賞，IEEE-IIHMSP2006 Best Paper Award，2013 年度情報セキュリティ文化賞等を受賞等．個人情報保護委員会委員等，情報ネットワーク法学会理事長等．著書に，「マイナンバーで広がる電子署名・認証サービス」日経 BP 社等．



■図 -5　トラストサービスとトラスト基盤の国際相互認証