インターネット時代の本人確認基盤に関する考察
ー NAF から GAF へ ー

才所 敏明[†1]　　辻井 重男[†2]

概要：官民を問わず国民向けのサービスがインターネット経由のサービスへ移行する中，インターネット経由の利用者の本人確認がますます重要となりつつある．日本では，民間サービスの本人確認は個々のサービス事業者ごとに実施しているのが現状であるが，このような個別サービス事業者ごとの本人確認は多くの課題を抱え，インターネット依存を強める日本社会の発展の障害になりかねない．そこで，インターネット経由のサービス事業者に対し専門組織による高度な本人確認機能の提供を前提とした日本の本人確認基盤 NAFJP（National Authentication Framework in Japan）の必要性およびその構成を提案する．
インターネット経由のサービスの本人確認においては，利用者の身元確認方法は各国の法制度や施策に基づくため，またインターネット経由の利用者の当人認証方法も利用者が使用する IT 環境が各国の事情により異なるため，身元確認および当人認証から構成される本人確認の具体的方法は各国で異なるものと想定される．そこで，海外（インド，米国，英国）のインターネット経由の本人確認の現状を調査し，各国の事情に応じた NAF 構築の現状・動向等を把握，提案する NAFJP との比較を示す．
インターネット上のグローバルなサービスが利用可能な本人確認基盤 GAF（Global Authentication Framework）を提案する．GAF は各国の NAF による本人確認の結果を利用し国境を越えた個人情報・プライバシー情報の収集・提供が不要な本人確認基盤である．更に本稿では，各国の NAF を利用した GAF 実現のための検討課題を整理する．

キーワード：インターネット，本人確認，記憶，所有物，生体特徴，本人確認基盤，NAF，NAFJP，身元確認，当人認証，GAF

A study on Identification and Authentication Framework in Internet Era
ー From NAF to GAF ー

Toshiaki Saisho[†1]　　SHIGEO TSUJII[†2]

Abstract: As the service for citizens, regardless of the public and private sector, shifts to the service via the Internet, it is becoming more and more important to authenticate the user via the Internet. In Japan, the user authentication of private sector service is currently carried out for each individual service provider, but such user authentication for each individual service provider has many problems. It becomes a factor that hinders the development of Japanese society that depends on the Internet. Therefore, we propose the necessity and composition of the Japanese authentication framework NAFJP (National Authentication Framework in Japan), which provides a high-level user authentication function by professional organizations to service providers via the Internet.
The user authentication method is assumed to vary from country to country, because the method of user's identity proofing is based on the legal systems of each country and because the method of authenticating the identity of the user via the Internet varies depending on the IT environment. Therefore, we first investigate the current status of user authentication via the Internet overseas (India, United States, United Kingdom), grasp the current status and trends of NAF construction according to the circumstances of each country, and compare it with the proposed NAFJP.
We propose GAF (Global Authentication Framework), which is a user authentication framework which global services on the Internet can use. GAF is a user authentication framework that does not need to collect and provide personal information and privacy information across national borders by using the results of user authentication result by NAFs in each country. Furthermore, in this paper, we propose issues such as the structure and implementation of GAF (Global Authentication Framework) based on NAF of each country.

Keywords: identification, authentication, internet, national authentication framework, NAF, NAFJP, global authentication framework, GAF

1. はじめに

我が国をはじめ世界はインターネット依存社会へ移行しつつある．我が国の様々の行政サービス，民間サービスもインターネット経由のサービスへ移行する中，インターネット経由の利用者の本人確認がますます重要となりつつある．

日本では，行政サービスのオンライン本人確認はマイナンバーカードの利用へ集約される方向にある．しかし，民間サービスにおいては独立した本人確認サービスも一部で

†1　（株）IT 企画
Advanced IT Corporation　http://advanced-it.co.jp/
中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：toshiaki.saisho@advanced-it.co.jp）
†2 中央大学研究開発機構
Research and Development Initiative, Chuo University
（Mail：tsujii@tamacc.chuo-u.ac.jp）
【 論文原稿：上記*の文字書式「隠し文字」 】

は利用されてはいるが，それぞれのインターネット上のサービス事業者が個別に多様な本人確認方法を利用し本人確認を行っているのが実情である．そのため，複数のサービスを利用する利用者は，それぞれのサービス事業者の登録手続きに従って，それぞれのサービス事業者が求める本人確認のための公的書類，会員カード等の固有の所有物を提示する必要がある．また利用者は，サービス利用の都度，それぞれのサービスが求める本人確認手続きに従って，本人確認のための情報を提示する必要がある．更に，このような本人確認のためのパスワード等の情報，ハードトークン等の所有物を安全・確実に管理しておく必要がある．

このような個別サービスごとの本人確認の現状には多くの課題が存在する．

ア：利用者の課題

①サービス利用の都度，サービス事業者ごとに異なる本人確認情報の提示が求められる，利便性の悪さ

②多くの本人確認情報の安全・確実な管理のための，利用者の負担

イ：事業者の課題

① 利用者の本人確認情報の安全・確実な運用・管理のための，事業者の負担

② インターネット上のサービスシステム開発時に求められる本人確認機能の個別実装のための，事業者の負担

ウ：社会の課題

① 本人確認関連技術の発展の成果である新たな本人確認手段の各事業者での採用の遅れによる，社会におけるインターネット高度利用の遅れ

以上のような民間分野における個別のサービス事業者ごとの本人確認の課題を克服するには，本人確認機能をそれぞれのサービス事業者から切り離し，本人確認を専門事業者に委託する仕組みが有効である（図 1）．利用者は，本人確認サービス事業者に，固有の ASID（本人確認サービス利用者 ID）と利用者の本人確認情報を紐づけて登録し，様々のインターネット上のサービスの利用登録時には，サービス事業者ごとの利用者固有の ISID（インターネット上のサービス利用者 ID）と ASID を紐づけて登録しておく．サービス利用時の本人確認は全て本人確認サービス事業者が担当し，インターネット上のサービス事業者はその結果を確認しサービスを提供する仕組みである．

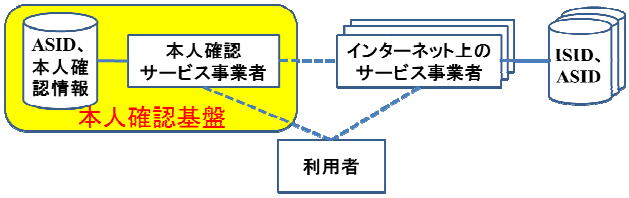

図 1　本人確認機能の分離モデル

本稿の 2 章にて，本稿で使用する本人確認の概念・用語の整理を行い，3 章では，本人確認機能の分離・独立を前提とした日本の本人確認基盤について，先行している行政サービス分野の本人確認基盤の現状と，遅れている民間サービス分野において期待される本人確認基盤の構想をまとめている．4 章では，日本と対比するため，インド，米国，英国の，行政・民間の両分野の本人確認サービスの現状・動向をまとめ，日本を含め 4 カ国の本人確認基盤の現状・動向の比較を行っている．5 章では，各国の本人確認基盤をベースに，国境を越えたインターネット上のサービス時代に向けたグローバルな本人確認基盤の構想・構成をまとめ，その実現のための検討課題について考察している．

2. 本人確認基盤（Authentication Framework）

インターネット上のサービスシステムがサービス要求を受けた場合に，そのサービス要求者がサービスシステムに登録されている正規の利用者かどうかの判断が必要となる．正規の利用者であることが確認できれば，システムはその利用者の権限に応じた範囲での利用を認可する．本稿では，サービス要求者がシステムに登録されている正規の利用者 ID と紐づけられた認証情報に合致するかどうかを判定する機能を当人認証機能と称している．また，当人認証機能により確認できた認証情報を有する利用者 ID に対応する利用者の実名，住所等，利用者を特定できる情報の取得およびその情報の妥当性を検証する機能を身元確認機能と称している．

本人確認機能は，身元確認機能および当人認証機能から構成され，身元確認の信頼レベルおよび当人認証の信頼レベルに応じ，本人確認の信頼レベルが決定される．

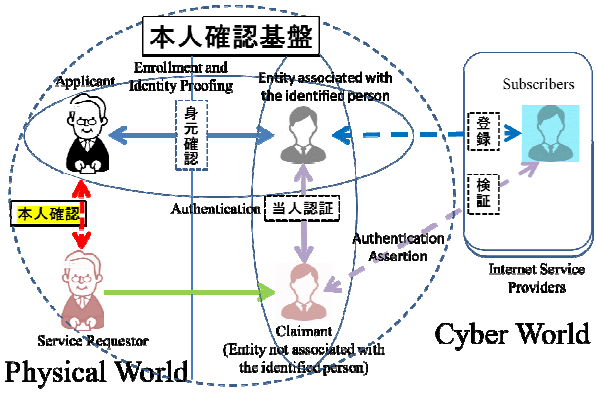

図 2　本人確認基盤

身元確認の信頼レベル，当人認証の信頼レベルおよび本人確認の信頼レベルの具体的な内容については，既報告（[2]）を参照願いたい．

なお，実社会（Physical Society）の活動においても本人確認を行った上でのさまざまのサービスが展開されており，実社会でも本人確認基盤は重要である．本稿では，主としてインターネット上のサイバー社会（Cyber Society）での本人確認基盤を対象に論じるが，その身元確認では，各国

の政府や実社会で活動する信頼できる本人確認サービス事業者の本人確認の結果として発行される本人証明書・ID カード等が利用されることが多い．

3. 日本の本人確認基盤 NAFJP（National Authentication Framework in Japan）

本章では，まず本人確認機能の独立・分離が進んでいる日本のインターネット上の行政サービス分野における本人確認基盤の現状を整理し，次に第 1 章で述べた課題克服を念頭に，日本のインターネット上の民間サービス分野における本人確認基盤 NAFJP およびその構成例を提案する．

3.1 日本の行政サービス向け本人確認基盤（現状）

日本では住民基本台帳による確実な身元確認の後，国民一人一人に固有の番号であるマイナンバーが付与される．このようにマイナンバーは，身元が確認された個人と紐づけられた ID であり，窓口での本人確認の後，マイナンバーカードも交付される．マイナンバーカードは信頼できる政府機関が発行する ID カードで，実社会での本人確認のために，行政分野のサービスに限らず民間サービスにおいても使用されている．

マイナンバーカード発行の際には，RSA 暗号の固有の公開鍵・秘密鍵ペアが割り当てられ，当人認証に使用される公開鍵証明書と秘密鍵がマイナンバーカードに書き込まれる．同時に，マイナンバーカード受領者が定めたパスワードも所有者確認のためのパスワードとしてカードに書き込まれる．

サイバー社会で提供されるインターネット経由の行政サービス利用にあたっては，パスワードによるマイナンバーカードの所有者確認の後，マイナンバーカード内の秘密鍵による署名および利用者証明用電子証明書を行政サービス部門へ送信し，行政サービス部門は電子証明書の検証，公開鍵による署名検証，更に電子証明書の有効性を地方公共団体情報システム機構（JLIS）に確認することにより，当人認証が実施される（図 3）．行政サービス分野では，マイナンバーカードによる身元確認・当人認証により，インターネット時代に向けた本人確認の仕組み（行政サービス向け NAFJP）が整ったといえる．

今後は，マイナンバーカードの普及促進（2020 年 6 月現在 16.8%）と，技術革新・普及に応じた当人認証方式の高度化，マイナンバーカードの機能の高度化等が期待される．

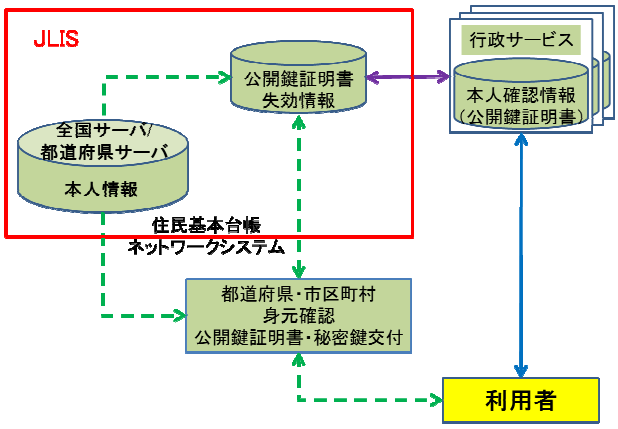

図 3　日本の行政サービス向け NAFJP（現状）

3.2 日本の民間サービス向け本人確認基盤構想（提案）

インターネット経由の民間サービスでは，身元確認・当人認証は個別のサービス事業者が担当しているのが実情である．その結果，多くの課題が存在することは 1 章で述べたとおりである．

政府としては，民間分野においても，行政サービス部門と同様の仕組みによる本人確認が可能なように，JLIS サービスの民間事業者への提供を進めているが，現実には活用は進んでいない．課題は，マイナンバーカード内の利用者証明用電子証明書を事業者側で都度受信するか蓄積・管理しておく必要があり，利用者には署名を求める，利用者の署名を検証する，利用者証明用電子証明書の有効性を JLIS に確認する，等のプロセスを民間の個々のサービス事業者が実装し運用することが必要なことである．つまり，電子証明書の有効性検証のみは JLIS に依頼できるが，それ以外の当人認証機能は個々のサービス事業者が実装し運用する必要がある．

そこで，身元確認にはマイナンバー制度および JLIS のサービスを利用し，民間サービス向けの当人認証を専門的に行う事業者を活用する，日本の民間サービス向け本人確認基盤（以降，特段の記載がない限り，単に NAFJP と略記）の構築を提案する（図 4）．

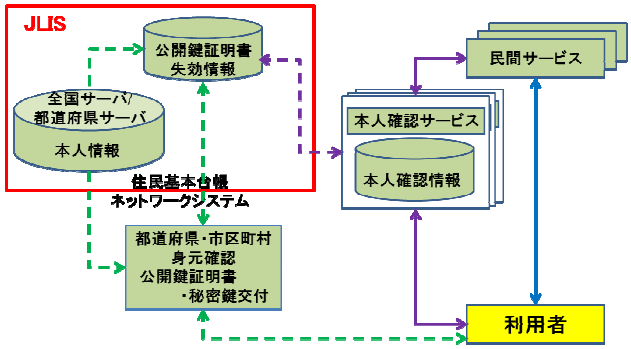

図 4　日本の民間サービス向け NAFJP（構想）

NAFJP における本人確認サービス事業者は，マイナンバー制度/JLIS サービスを利用しつつ利用者の身元確認を実施し，本人確認情報の登録を受け付ける本人確認情報登録

事業者と，その本人確認情報（当人認証情報）を利用しインターネット経由の当人認証を実施する当人認証サービス事業者の 2 種の事業者から構成されるものとする．本人確認情報登録事業者および当人認証サービス事業者が採用する当人認証方式は，本人確認技術の開発・評価を行う専門機関の評価結果に基づき，安全な方式を採用するものとし，またそのような安全な当人認証方式を正しく実装し運用しているか，個人情報・プライバシー情報の管理等，適切なセキュリティ対策をとっているかどうかについて，本人確認サービス事業者認定機関による監査・認定を受ける仕組みにより，NAFJP における本人確認サービスの安全性・信頼性を担保する仕組みを想定している．

NAFJP の構成は，本人確認サービスと利用者，インターネット上の各サービスとの連携方法に応じ，二つの構成を想定している．それぞれの構成案を図 5～図 6 に示している．

図 5 に示す NAFJP/A は，利用者中継型であり，利用者側のシステムに負荷がかかるが，最もプライバシー保護に適した形態である．図 6 に示す NAFJP/B は，インターネット上のサービス事業者中継型であり，従来は事業者自身で行っていた本人確認をアウトソーシングする形態である．

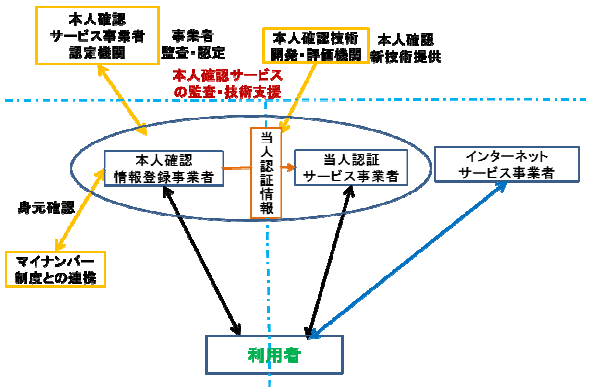

図 5　利用者中継型 NAFJP/A

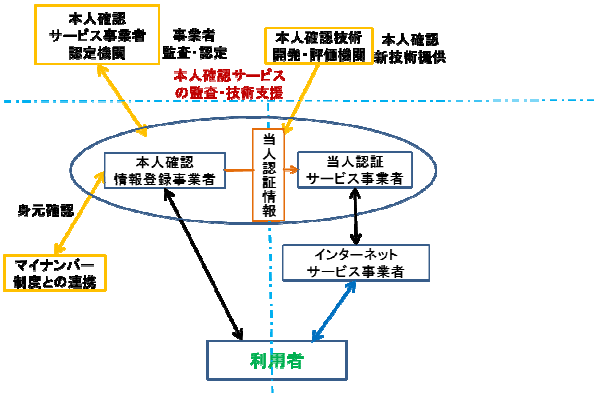

図 6　インターネット上のサービス事業者中継型 NAFJP/B

4.　海外の本人確認基盤の現状・動向

本章では，インド，米国，英国を例に，各国の本人確認サービスの現状，本人確認基盤 NAF 構築の現状・動向をまとめ，日本の現状，提案する NAFJP との比較を示している．

4.1　インド（[6]，[7]）

インドでは 2009 年 1 月に UIDAI（固有識別番号庁：Unique Identification Authority of India）が設立され，国民 ID 番号制度「アドハー（Aadhaar）」により全ての国民への 12 桁の固有の番号（アドハー番号）の付与が進められている．登録者は身分証明用カードである紙製のアドハーカード（当初バーコード，現在は QR コード使用）が交付される．2018 年には，人口約 13 億人中，約 12 億人がアドハーに登録している．

アドハー登録の際，アドハー番号の付与の他，個人の名前，生年月日，住所，携帯番号やメール ID などの他，当人認証情報として両手の指 10 本の指紋，両方の目の虹彩，顔画像が採取され，アドハー番号と紐づけられ Central Identities Data Repository (CIDR)に登録される．UIDAI は CIDR を利用しアドハーに基づくネット経由の本人確認サービス，身元確認および当人認証のサービスを提供しており，実社会での本人確認のために，行政分野のサービスに限らず民間分野においても利用されている．

アドハーは本人確認の他，電子署名等の 5 つの機能を提供し，2016 年にはオープン API としての集積体インディア・スタックのパイロットが実施され，インターネット上のセキュアなサービスの構築に利用されている．インドではインディア・スタックが行政・民間の両分野の共通のインターネット上の本人確認基盤として利用されている．

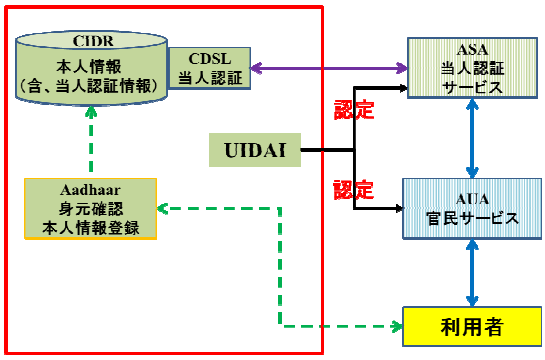

図 7　インドの本人確認基盤 NAFIN
National Authentication Framework in India

以上のようにインドでは，採用されている技術や仕組み，運用上のセキュリティには課題も指摘されているが，実社会およびインターネット上のサイバー社会，行政サービスおよび民間サービスに共通のインド固有の本人確認基盤（NAFIN）の構築・高度化・普及を，政府主導で展開している．

4.2　米国（[8]，[9]，[12] ～ [15]）

2001 年の 9.11 同時多発テロの実行犯 19 名のうち，18 名が（違法入手も含め）州政府発行の ID を入手していたという事実から，テロ対策としてしっかりとした ID 制度を確立すべく，また偽造免許証や不法入国者の排除を目的にリアル ID 法という法律が 2005 年に制定された．

リアル ID 法では，各州が運転免許証（DL）や身分証明書（ID）を発行する際の統一基準を定めている．具体的には「最低限記載しなければならない情報」，「申請に当たり最低限必要な文書」等が規定されており，また「各州は申請時に提出される文書の真正性を確認しなければならない」等を規定している．リアル ID 法の施行は 2020 年 10 月 1 日となっており，以降ではリアル ID 法に準拠しない運転免許証や身分証明書は使用できなくなる．(新型コロナウイルスの感染拡大を受け，施行が 2021 年 10 月 1 日まで 1 年延期となった．)

リアル ID 法では，固有の免許証番号や身分証明書番号を割り当て，個人の名前，生年月日，性別，住所等，登録する情報を規定し，各州には情報の真正性の確認求めているが，当人認証情報の登録は規定されていない．登録された情報は各州で DB にて管理されるが，連邦政府のゲートウェイを経由し，他の州からの情報検索も可能となる模様．

リアル ID 法の施行により，国としての各個人への ID 付与・管理の仕組みが徹底されることになる．リアル ID 法に基づく ID カードは，信頼できる政府機関が発行する ID カードで，実社会での本人確認のために，行政分野のサービスに限らず民間分野においても使用される見込みである．

一方，2017 年 4 月には数百件の行政サービスへのアクセスが政府機関を問わず同一のユーザ名で行えるシングルサインオン・プラットフォーム login.gov を立ち上げた．login.gov における当人認証では，多様な 2 要素認証，多要素認証が用意され，利用者が選択可能となっている．行政サービスの一部ではアクセス時に身元確認を要求するが，身元確認を要求する最初の行政サービスアクセス時にのみ，login.gov は利用者に州政府が発行した免許証や身分証明書の写真のアップロード等，身元確認のための情報提示を求めている．Login.gov は，インターネット上での行政サービスにおける本人確認の仕組みを提供している．

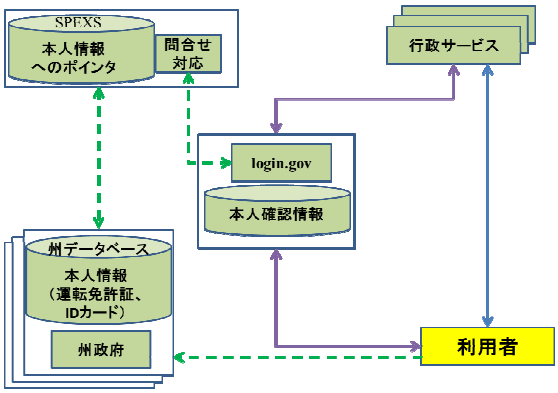

図 8　米国の行政サービス向け本人確認基盤 NAFUS
National Authentication Framework for public services in US

民間サービス分野では，既に多数の身元確認・当人認証を提供する本人確認サービスベンダが競争しつつ活動しており，利用者は本人確認サービスベンダを適宜選択し利用できる体制は整っている．なお，本人確認サービスベンダが提供する本人確認のレベル（身元確認・当人認証レベル）は，GSA（General Service Administration）が NIST Special Publication 800-63-3 の定義に準じ規定している．GSA は本人確認サービスベンダの本人確認機能やサービスを評価し，適切なベンダを Trust Framework Provider として認定している．利用者は，認定された本人確認サービスベンダの中から，必要なレベルの身元確認・当人認証を提供する信頼できるベンダの選定が可能となっている．

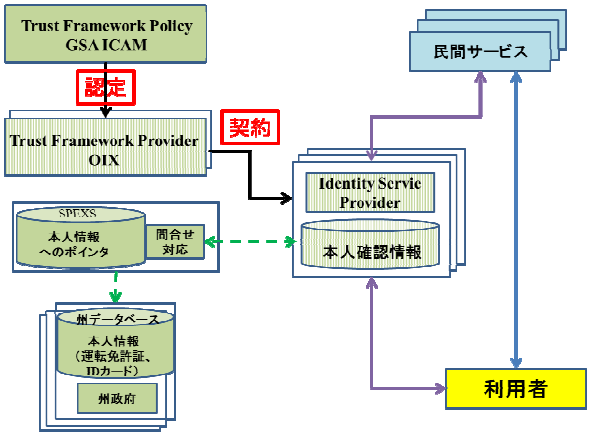

図 9　米国の民間サービス向け本人確認基盤 NAFUS
National Authentication Framework for private services in US

以上のように米国では，実社会の分野では行政サービス・民間サービス共通の本人確認基盤としてリアル ID 法に基づく ID カードが利用される見込みである．インターネット上のサイバー社会では，行政サービス分野および民間サービス分野は異なる仕組みで本人確認基盤の構築・高度化・普及が展開されているが，本人確認機能の技術基準の規定やベンダ評価・認定は政府主導で実施されている．

4.3　英国（[10]，[11]）

2006 年，国民 ID カード法が成立，国民 ID 登録簿の構築とその登録簿に基づき ID カードの発行が始まった．国民 ID 登録簿には，氏名，性別，生年月日，住所の他，生体情報を含む身体的特徴の登録が可能であった．ID カードの取得は任意だが，身分証明書として，また EU 域内パスポートとして使用できた．しかし，費用対効果の問題やプライバシーへの懸念から，また政権交代の影響もあり，2010 年に国民 ID 登録簿の廃止を規定した ID ドキュメント法が成立した．

国民 ID カードは廃止されたが，2001 年に政府がスタートさせた年齢保証のための ID カード発行スキーム PASS（Proof of Age Standards Scheme）に基づく ID カード発行は継続され，2018 年には 5 百万枚に達した模様．実社会では，民間サービスの他，一部の行政サービスにおいても利用者の年齢確認に利用されている．

国民 ID 登録簿が廃止された後，新たに IDAP（Identity Assurance Program）がスタートし，2016 年には GDS（Government Digital Service）が開発した政府機関のデジタルサービス利用のためのシングルサインオンシステム GOV.UK Verify のサービスが開始された．GOV.UK Verify は現在，5 社の民間の本人確認サービスを利用し運用されており，22 の政府機関のデジタルサービスと連携されている．GOV.UK Verify と契約している民間の本人確認サービスは，免許証やパスポート，各種の ID カードにより本人確認を行い，GOV.UK Verify へ結果をオンラインで通知する．GOV.UK Verify は，本人確認された利用者の場合は希望する政府機関のデジタルサービスの利用を可能としている．しかし，GOV.UK Verify は期待されたほど利用者および連携する政府機関が増えない状況から，GDS は政府機関のデジタルサービスにおける GOV.UK Verify の独占的立場を終了させ民間の本人確認サービス事業者との競争状態へ移行する方針である．

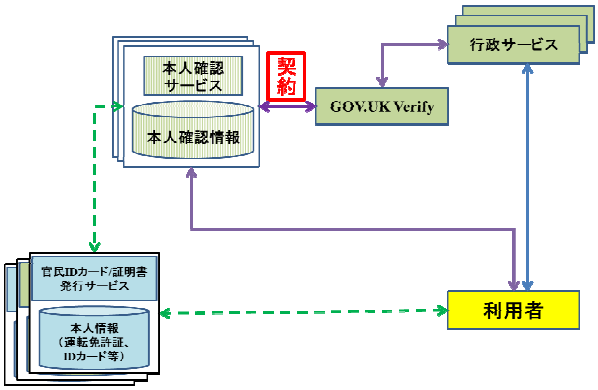

図 10　英国の行政サービス向け本人確認基盤 NAFUK
National Authentication Framework for public services in UK

民間サービス分野では，本人確認サービスを提供する事業者も数多く存在し，また民間の本人確認サービスを利用している GOV.UK Verify も，今後，民間向けの本人確認サービスを提供する模様である．また，2014 年に設立されたロンドンの会社 Yoti は各種の ID カード，証明書による身元確認，各種の認証情報を利用した当人認証サービスを展開している．NCSC（National Cyber Security Centre）が本人確認に関する技術のガイドラインを作成し，民間のサービス事業者および本人確認サービス事業者をサポートしている．

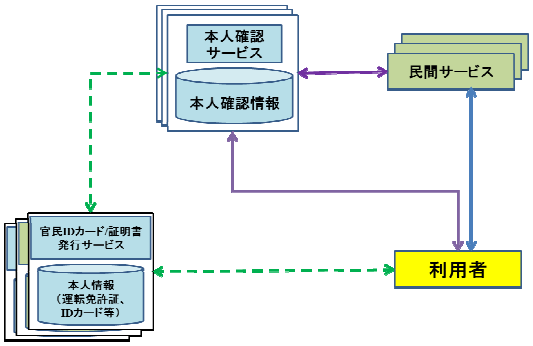

図 11　英国の民間サービス向け本人確認基盤 NAFUK
National Authentication Framework for private services in UK

以上のように英国では，実社会の分野では国民番号，国民 ID カード等は存在せず，PASS に基づく年齢保証 ID カードや免許証，その他，民間で発行される ID カード等が本人確認に利用されている．なお，現在，国民番号，国民 ID カードが必要との議論も再燃しており，EU を離脱することが本議論を加速させる可能性も考えられる．

インターネット上のサイバー社会での行政サービス分野では，GOV.UK Verify および民間の本人確認サービス事業者による本人確認基盤の構築・高度化・普及を目指している．本人確認技術やその標準化，相互運用性等の面では政府がサポートする予定である．民間サービス分野では本人確認基盤は民間主導で構築・高度化・普及が展開されているが，本人確認機能に関するガイドライン等の作成により政府が適切な本人確認機能の実装・サービスを支援している．しかし，本人確認サービス事業者の評価・認定等は実施されていない．

4. 4　各国のサイバー社会での本人確認基盤の比較

図 12 に各国のインターネット上のサイバー社会での本人確認基盤の現状を，行政サービス分野，民間サービス分野に分け，更に身元確認機能，当人認証機能，および技術・事業者の監査・認定機能について，その推進母体が官か民かも含め表示している．なお，日本の民間サービス分野の欄は，本稿で提案している将来確立すべき NAFJP に基づき記載している．

インドは，政府が行政・民間の両分野のインターネット上のサービスの本人確認基盤の構築・高度化・普及を推進し，両分野における一定レベルの本人確認結果の信頼性の確保を目指している．

米国は，行政分野のインターネット上のサービスの本人確認基盤の構築・高度化・普及を政府が推進している．民間分野のインターネット上のサービスの本人確認基盤の構築・高度化・普及については市場競争の原理を活用しているが，政府機関が本人確認サービス事業者の監査・評価を行うことにより事業者の認定を実施，本人確認結果の一定レベルの信頼性の確保を目指している．

英国は，行政分野のインターネット上のサービスの本人確認については，身元確認は民間事業者に委託し，当人認証は政府がその構築・高度化・普及を推進している．身元確認を委託する民間事業者の身元確認サービスの監査・評価は政府機関が行い，事業者の認定を実施，本人確認結果の一定レベルの信頼性の確保を目指している．民間分野のインターネット上のサービスについては，本人確認（身元確認・当人認証）の方法や信頼レベルに関するガイドラインを提示してはいるが，事業者の監査・評価に基づく認定等は実施していない．なお英国では，国民番号，国民 ID カードが必要との議論も再燃しており，その如何によっては本人確認基盤が将来大きく変わる可能性もある．

日本は，行政分野のインターネット上のサービスの本人確認基盤の構築・高度化・普及は政府が推進しているが，民間分野のインターネット上のサービスについては，本人確認（身元確認・当人認証）に関するガイドラインは提示されず，また事業者の監査・評価や認定等の制度も存在しない．日本としても，民間サービス分野においても，本人確認結果の一定レベルの信頼性が確保された本人確認基盤の確立を目指すべく，NAFJP を提案している．

	サービス分野	身元確認	当人認証	監査・認定
インド（2009～）	行政	UIDAI（Aadhaar，CIDR）		
	民間			
米国（2005～）	行政	GSA（Login.gov）		
	民間	（Trust Framework Provider）		GSA（NIST）
英国（2010～）	行政	GDS（GOV.UK Verify）	（certified companics）	GDS
	民間	（民間事業者）		NCSC（技術ガイドライン）
日本	行政（2013～）	マイナンバー制度		
	民間（NAFJP）	JLISサービスの利用を想定	認定された事業者を想定	公的機関を想定

図 12　各国のサイバー社会での本人確認サービスの比較

5. グローバルな本人確認基盤（GAF）に向けて

身元確認機能は各国固有の法制度や政府の施策に基づき実現されており，またインターネット経由の利用者の当人認証機能についても，各国の利用者/事業者の IT 利用環境は異なり利用する当人認証方式/技術も異なるため，身元確認および当人認証から構成される本人確認の具体的方法は各国で異なるものと想定され，各国固有の本人確認基盤（NAF）が構築されることになろう．

一方，民間分野のインターネット上のサービスはグローバルなサービスへ発展することは必至であり，グローバルなインターネット上のサービスのための本人確認基盤もまた，今後重要となろう．

グローバルなインターネット上のサービスの一つであり，KYC を求められる暗号資産サービスの分野では，個別に身元確認機能を実装し運用を行っている暗号資産システムが現れている．また，複数の国の身分証明書類や ID カード等の検証による身元確認機能を提供するグローバルなサービス事業者も現れている．しかしいずれの場合も，身元確認は，それぞれの国の公式の身元確認の仕組みとの連携による身元確認では無く，信頼できる機関が発行した証明書や ID カード等に記載されている情報を利用者が送信した画像から読み取り身元確認を行っている．利用者/事業者の身元確認のための作業負担，身元確認の信頼性の低さ，個人情報/プライバシー情報の国境を越えた海外の事業者へ送信する利用者のリスク等，課題が多い．

そこで，筆者らが提案する各国の本人確認基盤（NAF）をベースにしたグローバルな本人確認基盤（GAF：Global Authentication Framework）の構築を提案する．その構成案を図 13 に示す．本人確認に使用する個人情報/プライバシー情報は各国の NAF が管理し，GAF は NAF による本人確認の結果のみを受け取る方式で，利用者は国境を越えた事業者への個人情報/プライバシー情報の提供を不要としつつ，グローバルなインターネットサービスは GAF 経由で確実な本人確認を可能とする構想である．

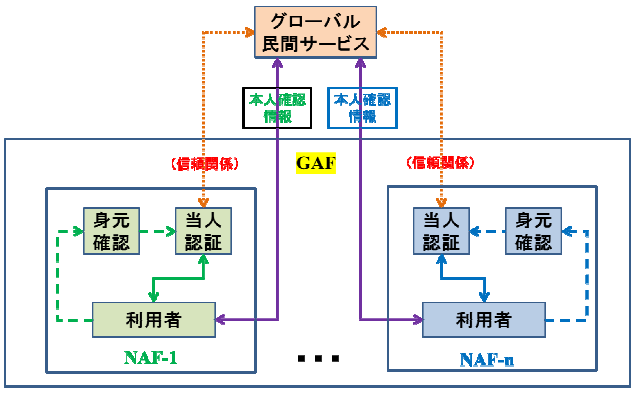

図 13　GAF：Global Authentication Framework

グローバルな本人確認基盤 GAF が信頼できる仕組みとして効率的に運用可能とするためには，以下のような課題を解決する必要がある．

(1)本人確認レベルに関する各国間での合意

本人確認レベルは，当人認証レベルと身元確認レベルに依存する．当人認証レベルと身元確認レベルからの本人確認レベル算出方法については GAF に参加する各国間での

合意が必要.

(2)各国 NAF で使用する当人認証方式の当人認証レベルに関する各国間での合意

各国の NAF では多様な当人認証方式が使用されるものと考えられる．各国で使用されているそれぞれの当人認証方式の当人認証レベルについては，各国間で合意が必要.

(3)各国 NAF で使用する身元確認方式の身元確認レベルに関する各国間での合意

各国の NAF では多様な当人認証方式が使用されるものと考えられる．各国で使用されているそれぞれの当人認証方式の当人認証レベルについては，各国間で合意が必要.

(4)各国 NAF 発行の本人確認情報の内容・形式の標準化

認証情報の連携については，SAML や OpenID Connect で標準化が既に実施されている. 各国の NAF による本人確認結果および本人確認レベル等を SAML あるいは OpenID Connect の仕様へ組み込み，SAML や OpenID Connect の枠組みを GAF で活用可能とする必要があろう.

6. おわりに

インターネット依存が急速に進んでいる我が国の社会において，セキュリティの基本である本人確認が，個々のインターネット上のサービス事業者で分散実施されていることには多くの課題がある．我が国がこのような課題を克服し安心・安全なインターネット依存社会として発展するためには，専門的な本人登録・確認サービス事業者によるサービス，本人登録・確認サービス事業者を支援する組織等から構成される本人確認基盤（NAFJP）の構築が必要である．本稿では，日本の本人確認基盤 NAFJP の構想および構成案を提案している.

国レベルの本人確認基盤は，シンガポール，オーストラリア，インド，カナダ等の海外でも構築され，あるいは構築されつつある．本稿では，インド，米国，英国の 3 カ国の本人確認基盤を調査し，現状・動向をまとめている．このような先行している各国の現状・動向を参考にしつつ，日本固有の事情を加味し，日本なりの本人確認基盤の構築を目指す必要がある．NAFJP はこのような方針に基づき，構想および構成案を策定したものである.

更に，民間分野のインターネット上のサービスのグローバル化進展に伴い必要となる，海外の利用者の本人確認の仕組みの実現を目指し，国別の本人確認基盤（NAF）をベースにグローバルな本人確認基盤（GAF）の構想を策定した．また，GAF が有効に円滑に運用されるための課題を提示した.

社会がインターネット依存を強めるのは必至であり，インターネット上での活動の基本である本人確認機能はますます重要となろう．NAFJP の早期の社会実装を目指し，また各国の NAF ベースのグローバルな本人確認基盤 GAF 構想の具体化に向け，調査研究を実施する予定である.

参考文献

[1] 才所敏明，辻井重男，「日本における本人確認基盤（NAFJA）の考察 － National Authentication Framework in Japan －」，情報処理学会・第 85 回コンピュータセキュリティ研究発表会，2019 年 5 月 24 日.

[2] 才所敏明，「NAFJA における本人確認方法に関する考察 － National Authentication Framework in Japan －」，コンピュータセキュリティシンポジューム 2019（CSS2019），2019 年 10 月 21 日.

[3]「2018 年度情報セキュリティの脅威に対する意識調査」報告書，独立行政法人情報処理推進機構，2018 年 12 月.
https://www.ipa.go.jp/files/000070256.pdf

[4]「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」，各府省情報化統括責任者（CIO）連絡会議決定，2019 年 2 月.
https://cio.go.jp/sites/default/files/uploads/documents/hyoujun_guideline_honninkakunin_20190225.pdf

[5]「Society5.0 を見据えた個人認証基盤のあり方について」(報告)，Society5.0 を見据えた個人認証基盤のあり方懇談会，2018 年 6 月.
http://www.soumu.go.jp/main_content/000560861.pdf

[6]「What is Aadhaar」，Unique Identification Authority of India, Government of India.
https://uidai.gov.in/what-is-aadhaar.html

[7]「Technology for 1.2 Billion Indians」，Unique Identification Authority of India，Government of India.
https://www.indiastack.org/

[8]「Simple, secure access to government services online」，General Services Administration，USA.
https://www.login.gov/

[9]「Developing Trust Frameworks to Support Identity Federations」，NISTIR 8149，January 2018.
https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8149.pdf

[10]「Be sure your users are who they say they are」, Government Digital Service，UK.
https://www.verify.service.gov.uk/

[11]「Yoti is the new way to prove your identity」，Yoti.
https://www.yoti.com/

[12]「Digital Identity Guidelines」, NIST Special Publication 800-63-3, June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[13]「Digital Identity Guidelines: Enrollment and Identity Proofing Requirements」，NIST Special Publication 800-63A，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[14]「Digital Identity Guidelines: Authentication and Lifecycle Management」，NIST Special Publication 800-63B，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

[15]「Digital Identity Guidelines: Federation and Assertions」，NIST Special Publication 800-63C，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf

【 この位置に改ページを入れ, 以降のページを印刷対象外とする 】