日本における本人確認基盤（NAFJA）の考察
ー　National Authentication Framework in Japan　ー

才所敏明[†1]　　辻井重男[†2]

概要：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。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アクセス者の本人確認がますます重要となりつつある。インターネットサービス事業者は利用者の協力を得、個別に本人確認を実施しているのが我が国の現状である。複数のインターネットサービスの利用者は、それぞれのサービス事業者が提供する本人確認手続きにのっとって、それぞれのサービス事業者が求める本人確認情報を登録し利用時に登録したそれぞれの本人確認情報を提示する必要があり、登録した多くの本人確認情報を安全に管理することが求められている。また、利用者の本人確認情報は多数のインターネットサービス事業者それぞれの管理にゆだねられているため、セキュリティ意識・対策レベルの低いインターネットサービス事業者からの本人確認情報の漏洩事件も多発している。本稿では、本人確認を個別のインターネットサービス事業者ごとに実施している我が国の現状の課題を指摘、その克服のために、専門事業者による本人確認サービスを前提とした我が国の本人確認基盤（NAFJA）を提案する。また、NAFJA の社会実装を具体化するに当たり、今後さらに検討が必要な課題について考察する。

キーワード：インターネット依存社会，本人確認，記憶，所有物，生体特徴，本人確認基盤，National Authentication Framework，NAF，NAFJA

Considerations about
National Authentication Framework in Japan(NAFJA)

TOSHIAKI SAISHO[†1]　　SHIGEO TSUJII[†2]

Abstract: Japan and also whole world are shifting to the strongly internet dependent society. Authentication of users via the Internet is becoming increasingly important because various government services and private services are shifting to services via the Internet. In Japan, the service provider via internet is conducting user authentication individually by user's cooperation. Users who use multiple services need to register the personal authentication information required by each service provider according to the authentication procedure provided by each service provider. In this paper, I point out the current problem of Japan that carries out user authentication for each individual Internet service provider, and in order to overcome that problem, I propose the National Authentication Framework in Japan (NAFJA). Also, I point out the issues that need further examination in the future for implementing NAFJA in Japan.

Keywords: user authentication, internet dependent society, national authentication framework, NAF，NAFJA

1. はじめに　*【*の文字書式「隠し文字」】

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アクセス者の本人確認がますます重要となりつつある。

現在の日本では、行政サービスはマイナンバーカードの利用を中核とした本人確認へ集約される方向にある。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は利用されてはいるが、多くはそれぞれのインターネット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。複数のインターネット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が提供する本人確認手続きに従って、それぞれのサービス事業者が求める本人確認のためのパスワード等の秘密の情報、会員カード等の固有の所有物や、生体特徴を提供する必要がある。独立行政法人情報処理推進機構（IPA）の「2018年度情報セキュリティの脅威に対する意識調査」報告書によれば、利用者一人当たり平均 8.5 個のアカウントを保有し対応するパスワードを管理していることになる。管理するアカウント数は毎年増加している。また、同報告書によれば、統計データは無いが、金融機関の多くはワンタイムパスワード装置（ハードトークン）を使用しており、ハードトークンによる本人確認の利用者も多いものと思われる。利用者は、このような利用するサービスが求める本人確認手続きに従って、あらかじめ本人確認情報を登録する必要があり、同時に利用者自身も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等を安全・確実に管

* †1 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）
【 研究報告用原稿：上記*の文字書式「隠し文字」 】

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。

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、利用者の利便性の悪さ

②本人確認情報を多くのサービス事業者に提供する、利用者の不安

③多くの本人確認情報の手元での安全・確実な管理のための、利用者の負担

④それぞれのサービス事業者のセキュリティ意識・対策のレベルのばらつき等による、本人確認情報の漏洩事件の多発

⑤本人確認関連技術の発展に伴う新たな本人確認手段への、サービス事業者ごとの対応の必要性

本稿では、日本社会が今後ますますインターネット依存社会へ移行する中、現状の様な個別のインターネットサービス事業者ごとの本人確認の課題を克服するため、本人確認機能を個別のサービス事業者から切り離し、少数の専門事業者によるサービス体制へ移行することを提案する。

2. 独立した本人確認サービスの可能性と課題

本章では、インターネット上のサービス事業者が、独立した本人確認サービスを利用し利用者へサービスを提供する場合の、利用者、インターネットサービス事業者、本人確認サービス事業者間の連携方法について整理する。また、独立した本人確認サービスを導入した場合の効果と課題について考察する。

(1)独立した本人確認サービスを利用したインターネットサービスの構成案

独立した本人確認サービスを利用する場合、三つの構成案が考えられる。それぞれの構成案、インターネットサービスを利用する場合の手順について述べる。

なお、本構成案の前提条件等は以下の通り。

＜前提条件＞

1.ASID（Authentication Service ID）は、本人登録・確認サービス登録者に割り当てられる本人確認サービス利用者 ID とする。

2.ISID（Internet Service ID）は、インターネットサービス登録者に割り当てられるインターネットサービス利用者 ID とする。

3.本人登録・確認サービス事業者は、利用者の本人情報（名前、住所等の本人を特定・追跡可能な情報）、本人確認方法、本人確認に必要となる本人確認情報（パスワード、所有物、生体特徴に関する情報）を、ASID に対応付け、管理するものとする。

4.インターネットサービス事業者は、ASID と ISID の対応の他、提供するサービス内容に応じ求める本人確認レベルを管理しているものとする。

構成 A：利用者中継型の利用構成

本人確認を必要とするインターネットサービスを利用する場合、利用者が本人確認サービス事業者およびインターネットサービス事業者との中継を実施し、本人確認サービス事業者およびインターネットサービス事業者間の直接のやり取りは存在しない構成である。

利用者は、本人確認サービス事業者へ本人確認を要請し、受領した本人確認結果と ISID をインターネットサービス事業者へ提供し、ISID に対応する本人確認が確実に実施されたことを示す。インターネットサービス事業者は、利用者から提供された本人確認結果から、本人確認サービス事業者の信頼性を確認し、更に本人確認結果の妥当性を確認し、サービス提供の可否を判断する（図 1）。

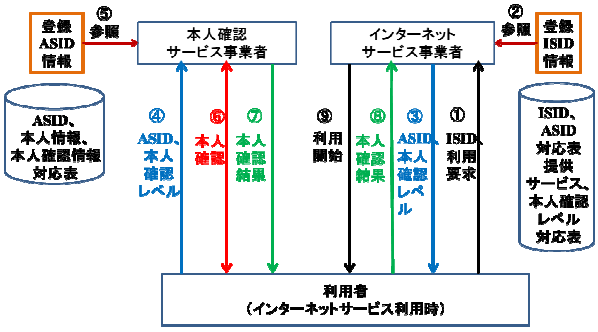

図 1　利用者中継型の利用構成

構成 B：インターネットサービス事業者中継型の利用構成

本人確認を必要とするサービスを提供するインターネットサービス事業者が、利用者のサービス提供の要求に対し、本人確認サービス事業者へ利用者の必要なレベルの本人確認を要請する構成である。

インターネットサービス事業者は、利用者からのサービス提供要求を受けた時点で、要求されたサービス内容に対応し定められた本人確認レベルに応じた利用者の本人確認を本人確認サービス事業者へ要請する。本人確認サービス事業者は、インターネットサービス事業者経由、利用者へ本人確認のための手続を要請し、本人確認結果をインターネットサービス事業者へ提供する。インターネットサービス事業者は、本人確認サービス事業者から提供された本人確認結果の妥当性を確認し、サービス提供の可否を判断する（図 2）。

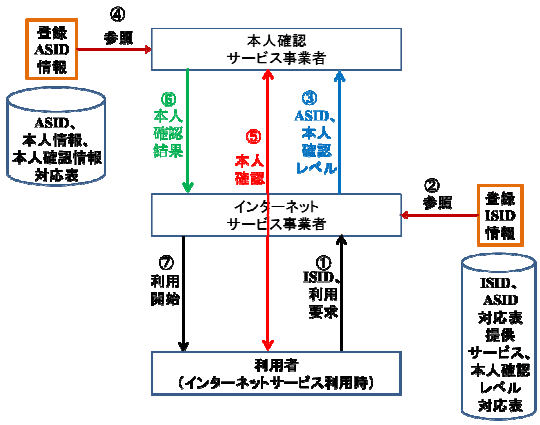

図 2　インターネットサービス事業者中継型の利用構成

構成 C：本人確認サービス事業者中継型の利用構成

本人確認サービス事業者の中継により、インターネットサービス事業者が利用者の必要なレベルの本人確認の結果を得、サービス提供の可否を判断する構成であるが、サービス提供時は、インターネットサービス事業者が利用者へ直接サービスを提供する構成である（図 3）。

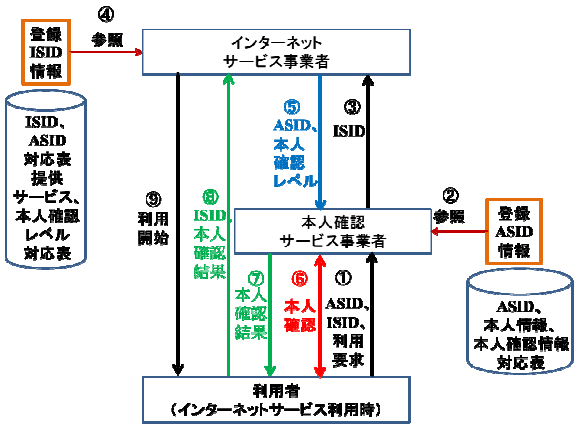

図 3　本人確認サービス事業者中継型の利用構成

(2)独立した本人確認サービス導入の効果と課題

A～C のいずれの利用構成でも、共通に期待できる効果は以下の通りである。

①利用者にとっての効果

＊本人確認のための秘密の情報や所有物の安全・確実な管理負担の大幅な軽減

＊本人確認情報の提供先が限定されるため、本人確認情報の漏洩不安の大幅な軽減

＊本人確認情報の更新が一括で実施可能

②各種インターネットサービス事業者にとっての効果

＊利用者の本人確認機能の実装が不要（新たなサービスの導入が容易に）

＊利用者の本人確認結果への責任を本人確認サービス事業者へ移転可能

＊利用者の個人情報である本人確認情報の管理が不要（個人情報漏洩リスクを回避可能）

＊本人確認技術の進歩に応じた新たな本人確認サービスの社会実装を本人確認サービス事業者へ期待可能

A～C のいずれの利用構成でも、共通に想定される課題は以下の通りである。

＊本人確認機能の過度の集中の場合の弊害

＊本人確認情報の大量漏洩リスクの存在

＊独立した本人確認サービスのコスト負担の在り方

社会実装にあたっては、以上のような効果を確実に達成しつつ課題を克服する仕組みを工夫する必要がある。

なお、三つの利用構成 A～C には、それぞれ以下のような固有の特徴・課題がある。

構成 A：

NIST SP 800-63-3 で定義されている Digital Authentication Model と同一の構成である。

インターネットサービス事業者の負担が最も少なく、利用者（システム）の役割（負担）が大きい構成であるが、本人確認サービス事業者へ利用者とインターネットサービス事業者との関係を開示する必要が無く、利用者のプライバシー保護を重視した構成と言える。

構成 B：

現在、インターネットサービス事業者が個別に実施している本人確認機能を、本人確認サービス事業者へ委託（アウトソーシング）する構成である。利用者には負担をかけないので、社会実装が容易な構成と言える。

本構成の場合、一般には利用者が利用するインターネットサービスを本人確認サービス事業者へ開示することになるが、プライバシー保護上、問題となる場合は、インターネットサービス事業者が匿名で本人確認サービス事業者へ本人確認を委託する方式を採用する必要がある。

また、インターネットサービス事業者経由実施される本人確認手続きの際のやり取りは、インターネットサービス事業者に漏えいしないよう、利用者・本人確認サービス事業者間で暗号化し実施する必要がある。

構成 C：

本構成は、構成 A の場合の利用者（システム）の負担を軽減しつつ、構成 B の場合のインターネットサービス事業者経由の本人確認手続きを回避できる構成である。

しかし、構成 B と同様、利用者が利用するインターネットサービスを本人確認サービス事業者へ開示することになり、プライバシー保護上、問題となる場合は、インターネットサービス事業者が匿名で本人確認サービス事業者へ本人確認を委託する方式を採用する必要がある。

3.　日本の本人確認基盤（NAFJA）の提案

本章では、独立した本人確認サービス事業者の利用を前提とした日本の本人確認基盤（NAFJA：National Authentication Framework in Japan）を提案する。

NAFJA は大きく次の四つの機能から構成されている。

＊本人登録サービスへの登録
＊インターネットサービスへの登録
＊インターネットサービスの利用
＊本人登録・確認サービスの監査・支援

前章で検討した三つの利用構成の内、3.1 にて構成 A をベースに策定した NAFJA 構想（NAFJA/A）について、3.2 にて構成 B をベースに策定した NAFJA 構想（NAFJA/B）について、想定する機能・手続き等を説明する。構成 C の要素機能は構成 A、B に含まれているため、構成 C をベースとした NAFJA 構想（NAFJA/C）については説明を省略する。

なお、構成 A、B、C は、2 章で述べたようにそれぞれ特徴ある構成であり、インターネットサービスの特質に応じ、個々のインターネットサービスごとに適切な構成の NAFJA を選択し利用することを想定している。

3.1 構成 A をベースにした NAFJA/A

図 4 に NAFJA/A の構成を示している。各機能について想定している手続、手順は、以下の通り。

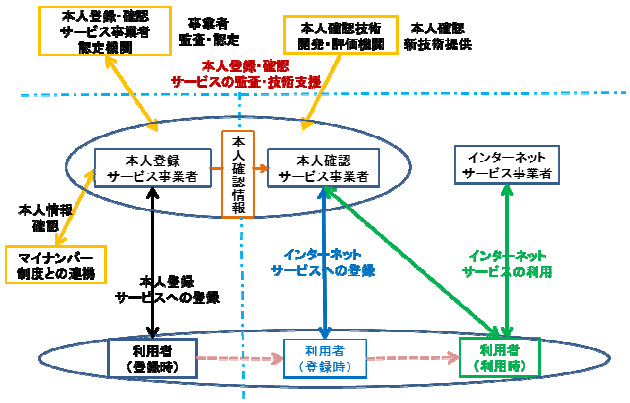

図 4　National Authentication Framework in Japan（NAFJA/A）

(1)本人登録サービスへの利用者登録の仕組み（図 5）

利用者が本人登録サービスへ登録する際の手続は以下の通り。

①窓口にて本人情報、本人確認情報等を提示する。オンラインでの本人登録も、窓口と同程度の本人確認が可能な条件の場合は許容可能であるが、登録時の本人確認の確実さが NAFJA の信頼性の根拠でもあり、慎重な対応が必要である。
提示する本人確認情報は、顔写真付きの公的に発行された証明書を想定している。例えば、マイナンバーカードやパスポート等。

②窓口では、目前の本人を公的に発行された証明書の写真で確認すると共に、マイナンバーによる JLIS への問い合わせ等により情報の確認も行ない、確実な本人確認を実施する。

③インターネット経由の本人確認に使用する情報を登録する。インターネット上の各種サービスでは、そのサービス内容に応じ様々なレベルの本人確認が求められる。記憶による本人確認、所有物による本人確認、生体特徴による本人確認が可能な情報を登録できる必要があるが、利用者の希望により登録情報を選択できるものとする。例えば、記憶（パスワード）、所有物（ワンタイムパスワードシステム（ソフト、ハード）、スマホ/携帯、マイナンバーカード等）、生体特徴（顔、指紋、虹彩等）が想定される。本人確認に使用する情報は、本人登録・確認サービス事業者間で共有されることを想定している。

④本人確認およびインターネット経由の本人確認に使用する情報の登録終了後、利用者個々に割り当てられる ASID（本人確認サービス ID）と共に、鍵ペア、公開鍵証明書等を USB メモリ/IC カード/CD-ROM 等のメディアで交付する。なお、交付された情報を利用したインターネット経由の本人確認が正しく動作するかどうかのチェックが、窓口にて行えることが望ましい。

以上の手続のように、しっかりとした本人確認の元、インターネット経由の本人確認が可能な情報の登録を行う。

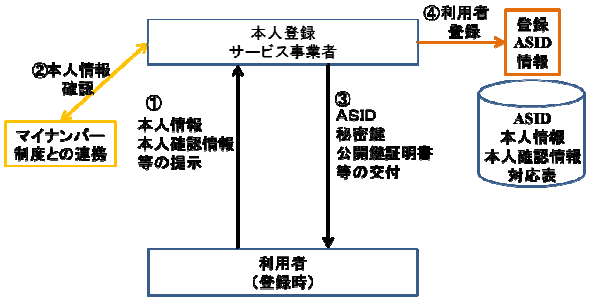

図 5　本人登録サービスへの本人確認情報等の登録

(2)インターネットサービスへの利用者登録の仕組み（図 6）

利用者がインターネットサービスへ利用を申し込む際の手続は以下の通り。

①利用者は、インターネットサービスへ利用登録を要求する。

②インターネットサービスは、利用者へ利用登録時に求める本人確認レベル・方法を通知する。

③利用者は、本人確認サービスへ自身の ASID（本人確認サービス ID）およびインターネットサービスに指定された本人確認レベル・方法を通知する。

④本人確認サービスは、利用者が ASID に対応し登録している本人確認方法の中で、指定された本人確認レベル・方法に該当する本人確認方法を入手する。

⑤本人確認サービスは、該当する本人確認方法を利用者へ提示し、利用者が選択した方法により、本人確認を実施する。

⑥本人確認サービスによる利用者の本人確認終了後、本人確認サービスは利用者へ結果を通知する。

⑦利用者は、自身の ASID と本人確認結果をインターネットサービスへ通知する。

⑧インターネットサービスは、ASID と本人確認結果を確認し、新たに ISID（インターネットサービス ID）を発行し、ISID と ASID の対応を登録する。
⑨利用者へ登録完了および ISID を通知する。(利用者は、引き続きインターネットサービスを利用可能となる。)

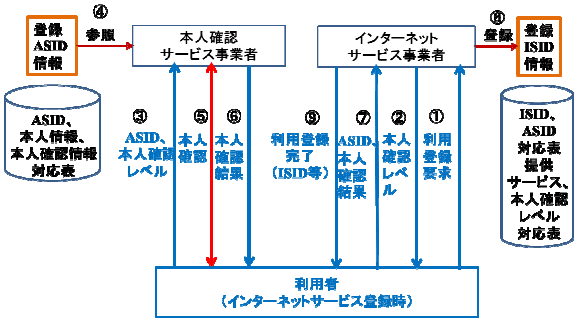

図 6　インターネットサービスへの利用者登録

(3) 利用者のインターネットサービス利用の仕組み（図 7）

利用者が登録済みのインターネットサービスを利用する際の手続は以下の通り。

①利用者は、ISID を提示し、サービス利用を要求する。
②インターネットサービスは、ISID に対応する ASID を確認する。
③インターネットサービスは、利用者へ ASID および利用時に求める本人確認レベル・方法を通知する。
④利用者は、本人確認サービスへ自身の ASID と指定された本人確認レベル・方法を通知する。
⑤本人確認サービスは、利用者が ASID に対応し登録している本人確認方法の中で、指定された本人確認レベル・方法に該当する本人確認方法を入手する。
⑥本人確認サービスは、該当する本人確認方法を利用者へ提示し、利用者が選択した方法により、本人確認を実施する。
⑦本人確認サービスは、利用者へ本人確認結果を通知する。
⑧利用者は、インターネットサービスへ本人確認結果を通知する。
⑨インターネットサービスは、本人確認結果を確認し、サービスを提供する。

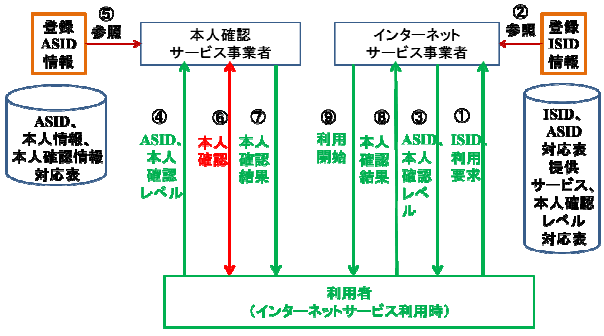

図 7　インターネットサービスの利用

(4)本人登録・確認サービス事業者の監査・支援の仕組み

安全・確実な本人確認を保証する NAFJA の構築・運用においては、本人登録・確認サービスのセキュリティ面の安全性、NAFJA で採用する本人確認技術・方法の妥当性を評価・検証する仕組みが重要である。

①本人登録・確認サービス事業者の評価・認定の仕組み

NAFJA による本人確認結果が信頼できるか、利用者やインターネットサービス事業者が本人登録・確認サービスを安心して利用できるかは、本人登録・確認サービス事業者が安全・確実に本人登録・確認を実施しているか、本人確認情報を安全に管理しているか等の本人登録・確認サービス事業者のセキュリティに強く依存している。

安心・安全な NAFJA の構成・運用には、本人登録・確認サービス事業者のセキュリティに対する第三者による監査・評価・認定等の仕組みが不可欠である。

②本人確認技術の評価・認定の仕組み

本人確認技術の発展、利用者の IT 環境の変化は、今後も継続するものと考えられ、NAFJA においても時代時代に応じた適切な本人確認方法の採用が必要であり、本人確認方法の安全性や本人確認レベルの技術的評価・検証機能を果たす専門的組織が不可欠である。

3.2　構成 B をベースにした NAFJA/B

NAFJA/B も大きく四つの機能から構成（図 8）されており、以下、各機能について想定している手続、手順等を説明する。

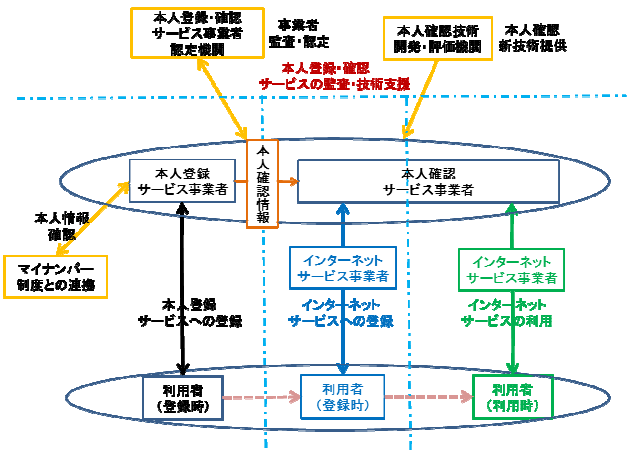

図 8　National Authentication Framework in Japan（NAFJA/B）

(1)本人登録サービスへの利用者登録の仕組み

NAFJA/A と同一であり、説明は省略。

(2)インターネットサービスへの利用者登録の仕組み（図 6）

利用者がインターネットサービスへ利用を申し込む際の手続は以下の通り。

①利用者は、ASID（本人確認サービス ID）および必要な本人情報等を通知し、インターネットサービスへ利用登録を要求する。
②インターネットサービスは、本人確認サービスへ、ASID、インターネットサービスが求める本人確認レベ

ル・方法を本人確認サービスへ通知し、本人確認を要請する。

③本人確認サービスは、指定された本人確認レベル・方法をベースに、登録されている ASID の本人確認情報から、可能な本人確認方法を確認する。

④本人確認サービスは、インターネットサービスが期待する本人確認レベルを満たしており、利用者が必要な本人確認情報を登録していて、実施可能な本人確認方法を利用者に提示し、その中で利用者が選択した方法に基づき、本人確認を行う。本人確認はインターネットサービス経由行うが、本人確認のために使用される通信情報は秘匿され、インターネットサービス事業者に漏洩しないような工夫が必要である。

⑤本人確認サービスによる利用者の本人確認終了後、本人確認サービスはインターネットサービスへ結果を通知する。

⑥本人確認が成功であった場合は、インターネットサービスは利用者の ISID を発行し登録する。登録する情報は、ISID、ASID、およびインターネットサービスが必要とする本人情報を想定している。その後、利用者へ登録完了および ISID を通知する。利用者は、引き続きインターネットサービスを利用可能とする。

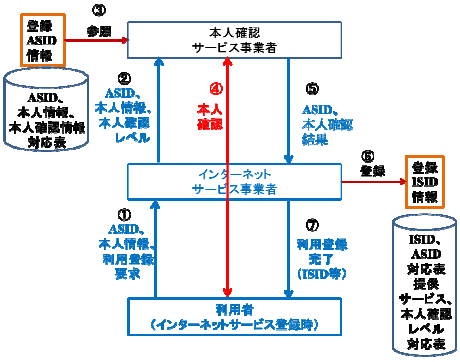

図 9　インターネットサービスへの利用者登録

(3) 利用者のインターネットサービス利用の仕組み（図 7）

利用者が登録済みのインターネットサービスを利用する際の手続は以下の通り。

①利用者は、ISID、ASID 等の情報を通知し、サービス利用を要求する。

②インターネットサービスは、ASID および期待する本人確認レベル・方法を本人確認サービスへ通知し本人確認を要請する。

③本人確認サービスは、指定された本人確認レベル・方法をベースに、登録されている ASID の本人確認情報から、可能な本人確認方法を確認する。

④本人確認サービスは、インターネットサービスが期待する本人確認レベルを満たしており、利用者が必要な本人確認情報を登録していて、実施可能な本人確認方法を利用者に提示し、その中で利用者が選択した方法に基づき、本人確認を行う。本人確認はインターネットサービス経由行うが、本人確認のために使用される通信情報は秘匿され、インターネットサービス事業者に漏洩しないような工夫が必要である。

⑤本人確認サービスによる利用者の本人確認終了後、本人確認サービスはインターネットサービスへ結果を通知する。

⑥本人確認が成功であった場合は、インターネットサービスは利用者へサービスを提供する。

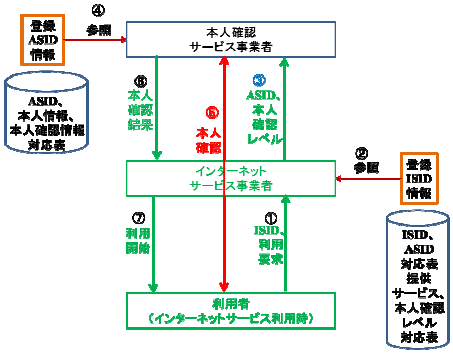

図 10　インターネットサービスの利用

(4)本人登録・確認サービス事業者への監査・支援の仕組み

NAFJA/A と同一であり、説明は省略。

4. NAFJA の具体化のための主要な検討課題についての考察

NAFJA の構想概要は前章で述べたとおりであるが、具体化のために詰める必要がある課題も多い。本章では、主要な課題を提示し、克服方針や克服のために必要な検討内容等を整理する。

(1)採用する本人確認情報の選定

インターネット経由の本人確認要素技術として、パスワードを利用する記憶による本人確認、スマホや各種 IC カード等を利用する所有物による本人確認、虹彩、指紋、顔等を利用する生体特徴による本人確認が利用されているが、利用者の多様な希望に対応できるよう、出来る限り多くの本人確認のための情報登録が行えることが望ましい。

現状・将来の利用者の利用環境・利便性を考慮しつつ、それぞれの本人確認要素技術の技術評価結果を踏まえ、採用する本人確認要素技術の選定および登録する本人確認情報の要件等を定める必要がある。

記憶による本人認証、所有物による本人確認、生体特徴による本人確認、それぞれの本人確認要素技術による本人確認の安全性や信頼性については、既に数多くのガイドラインが存在しており、NAFJA での利用を前提とした統一的な視点での整理により、NAFJA で採用する本人確認情報の選定は可能であろう。

(2)採用する本人確認方法の選定とそれぞれの本人確認レベルの特定

本人確認は、一般に本人確認要素技術を組合せた本人確

認方法により実施される。本人確認方法についても既に数多くのガイドラインが存在しており、NAFJA での利用を前提とした統一的な視点での整理により、NAFJA で採用する本人確認方法の選定も可能であろう。

最近は生体特徴を利用した本人確認方法の実用化も期待されている。生体特徴を利用した安全な本人確認方法として筆者の一人が考案し ISO/IEC JTC1 SC27 にて国際標準に採用されている ACBio（ISO/IEC 24761）、所有者認証に生体特徴を利用した所有物による本人確認方法である FIDO 等、その他、記憶や所有物を組み合わせた新たな本人確認方法も数多く提案されており、最新の研究開発成果を反映しつつ、また利用者の利用環境や利便性を考慮しつつ、安心・安全な本人確認方法を提供する必要があろう。

なお、一般にインターネットサービスでは、特定の本人確認方法に拘ることは少なく、本人確認結果の信頼レベルを重視するため、それぞれの本人確認方法の本人確認結果への信頼レベル（本人確認レベル）をあらかじめ登録しておく必要がある。本人確認方法に応じた本人確認結果の信頼レベル（本人確認レベル）は、NIST SP 800-63-3B にて定義されている AAL（Authentication Assurance Level）を参考に、選定した本人確認方法を具体的に評価することにより決定することが可能であろう。

(3)本人確認情報および本人確認方法の登録・更新

利用者が登録する本人確認情報および本人確認方法は、本人登録･確認サービス事業者間での共有を想定しており、登録形式を定め管理する必要がある。

生体特徴による本人確認に使用する生体特徴データの交換形式については、ISO/IEC JTC1 SC/37 にて国際標準化されている（ISO/IEC 19794 シリーズ）。NAFJA においても、標準化された交換形式による登録が望ましい。記憶による本人確認や所有物による本人確認の本人確認情報の格納形式については同様の規定､ガイドラインは存在せず､また、本人確認方法の格納形式についても、同様の規定、ガイドラインは存在しないが、NAFJA では交換形式・登録形式を定めておく必要がある。

利用者が登録する本人確認情報および本人確認方法は、必要に応じ変更可能とする必要がある。過去の本人確認の監査を可能とするために、一旦登録された本人確認情報および本人確認方法は長期的に保全される必要があり、NAFJA ではブロックチェーンの利用を想定している。なお、コンソーシアムタイプのブロックチェーンとすることにより、本人登録サービス、本人確認サービスおよび監査機関等からのアクセスのみを可能とし、なおかつ、ブロックチェーン上に登録されている本人確認情報および本人確認方法の暗号化等による保護のための工夫が必要となろう。

(4)本人登録・確認サービス利用ログの収集・管理

本人登録・確認実施時には、その実施内容、結果も含め記録し、将来の監査に備えておく必要がある。

本人登録・確認サービス利用ログは長期的に保全されることが望ましい。NAFJA では、本人登録・確認サービス利用ログの収集においても、ブロックチェーンの利用を想定している。なお、コンソーシアムタイプのブロックチェーンとすることにより、本人登録サービス、本人確認サービスおよび監査機関等からのアクセスのみを可能とし、なおかつ、ブロックチェーン上に登録されている本人確認サービス利用ログの暗号化等による保護のための工夫が必要となろう。

(5) 本人登録・確認サービスの監査・評価・認定

NAFJA が安全・確実に運用されるためには、利用者の本人確認情報・本人確認方法を管理し利用する本人登録・確認サービス事業者の適切なセキュリティ対策や、適切な本人登録・確認手続きの実施が不可欠である。

利用者が安心して事業者のサービスを選定・利用できるよう、第三者機関による監査・評価やその結果に基づく事業者の認定等が必要となろう。

具体的には、本人登録・確認サービス事業者としての監査項目を既存の監査制度等へ加え、その結果に基づき、信頼できる事業者としての認定を実施することが望ましい。

(6)本人の特定・追跡の仕組み

本人登録サービスの窓口で利用者が提示する本人特定・追跡情報の確認を、日本国籍を有する利用者の場合はマイナンバー制度、外国籍の利用者は在留管理制度等との連携により実施するのが望ましい。制度上およびシステム上、マイナンバー制度、および在留管理制度との連携が難しければ、代替の仕組みの検討が必要となろう。

なお、利用者の登録時点の本人確認では、本人の特定・追跡が可能なよう、基本 4 情報やマイナンバーの確認を行うことを前提としており､NIST SP 800-63-3A で定義されている IAL（Identity Assurance Level）のレベル 3（IAL3）の採用を想定している。

5. 既存の SSO システムとの関連

NAFJA は、シングルサインオン（SSO）システムとして利用できるが、既存の SSO システム SAML（V2.0)および OpenID Connect と大きく異なる点は、本人登録サービス事業者による利用者の確実な本人確認にある。個人情報の基本 4 情報等の確認による、万一の場合の利用者の実世界での特定・追跡性の保証にある。インターネット依存社会におけるサイバーセキュリティの確保には、サイバーワールドのエンティティとリアルワールドのエンティティとの確実な紐づけが不可欠であり､NAFJA はそのための基盤となることを目指している。リアルワールドのエンティティとの確実な紐づけを保証するには、各国固有の国民 ID 制度（日本ではマイナンバー制度)等との連携が不可欠であり、NAF もまた各国固有の仕組みとして実装されるものと考えられるが、グローバルなインターネット上で活動する利

用者の実世界での特定・追跡性に関する保証については、各国間での共通認識・連携が必要となろう。

NAFJA と既存の SSO システムとの関係については、インターネットサービス事業者による NAFJA のネイティブな利用に限らず、SAML や OpenID Connect ベースの ID 連携サービス事業者経由の NAFJA 利用も想定され、将来は NAFJA と SAML や OpenID Connect との連携により、利用者の実世界での特定・追跡性に関する保証サービスである NAFJA と連携しつつ、グローバルなインターネット上での各種サービスの利用・提供が可能になるものと期待される。

NAFJA の技術仕様については、詳細は今後の検討であるが、多くのメカニズム、プロトコル、データ形式等は、SAML や OpenID Connect の仕様そのものあるいは拡張仕様の採用が考えられる。将来の NAFJA と SAML や OpenID Connect との連携を考慮し、出来る限り仕様の共通化を目指す必要があろう。

6. おわりに

本稿では、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サービス事業者で分散実施されていることの課題を指摘、我が国が安心・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（NAFJA）の構築が必要なこと、および NAFJA の具体的構成案、NAFJA 実現のための課題とその克服のために今後検討が必要な項目を示した。

本稿では、マイナンバーカードベースの行政分野の本人確認基盤とは独立に、民間サービスのための本人確認基盤の構想を策定した。行政分野の本人確認基盤においても、マイナンバーカードのみではなく生体特徴を利用した本人確認の採用も必要になる時期がくるであろうし、民間サービスにおいてもマイナンバーカードの活用は大変期待されており、我が国の本人確認基盤の一本化の議論もいずれ必要となろう。

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導入され、あるいは導入の議論・検討が進められている。我が国においても、国レベルの本人確認基盤の必要性が認知され、研究開発および社会実装に向けた議論や活動が活発に行われることを期待したい。

謝辞 本論文の執筆において有益なアドバイスを頂いた、静岡大学創造科学技術大学院・西垣正勝教授に感謝する。

参考文献

[1] 「オンライン本人認証方式の実態調査」報告書，独立行政法人情報処理推進機構，2014 年 8 月．
https://www.ipa.go.jp/files/000040778.pdf
[2] 「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
[3] 「本人確認をした属性情報を用いた社会基盤構築に関する調査研究」調査報告書，一般財団法人日本情報経済社会推進協会，2014 年 3 月．
http://www.meti.go.jp/meti_lib/report/2013fy/E003274.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] 「Digital Identity Guidelines」，NIST Special Publication 800-63-3, June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[7] 「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
[8] 「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
[9] 「Digital Identity Guidelines Federation and Assertions」，NIST Special Publication 800-63C，June 2017.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf
[10] 「諸外国における国民 ID 制度の現状等に関する調査研究報告書」，国際大学・グローバル・コミュニケーション・センター，2012 年 4 月．
http://www.soumu.go.jp/johotsusintokei/linkdata/h24_04_houkoku.pdf
[11] 「Security Assertion Markup Language (SAML) v2.0」，OASIS，March 2005.
http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
[12] 「Errata to OpenID Connect Specifications Approved」，OpenID Foundation，November 2014.
https://openid.net/2014/11/09/errata-to-openid-connect-specifications-approved/
[13] 「個人識別符号に関する海外・国内動向の調査研究報告書」，三菱総合研究所，2018 年 3 月．
https://www.ppc.go.jp/files/pdf/201803_kojinshikibetsu_fugou.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 】