NAFJA における本人確認方法に関する考察
ー National Authentication Framework in Japan ー

才所 敏明*

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。現在、民間のほとんどのインターネットサービスでは、個々のサービス事業者が個別に本人確認を行っている。利用者の本人確認のための本人確認情報の入手・管理やそれを利用した本人確認プロセスの実行は、多くのサービス事業者が個別に実施しているのが現状である。今後もインターネット経由のサービスへの移行が進むことが予想され、利用者の個人情報・秘密情報である本人確認情報のサービス事業者ごとの分散管理による漏洩リスクはますます増大し、利用者も多くのインターネットサービス事業者ごとの個別の本人確認方法への対応の負担も増大せざるを得ない。そこで筆者は、インターネット依存を強める我が国において、本人確認機能を少数の専門的組織に集約し、多くのサービス事業者の負担やリスクを軽減し、また利用者の利便性向上と個人情報・秘密情報漏洩のリスク軽減を目指す、本人確認基盤（NAFJA：National Authentication Framework in Japan）の構築を提案する。また本稿では、2017 年 6 月に発行された NIST SP 800-63-3 で示されている米国での Digital Identity に関するガイドラインおよび 2019 年 2 月に各府省情報化統括責任者（CIO)連絡会議で決定された「行政手続における本人確認の手法に関するガイドライン」を調査・整理し、それらの内容を踏まえ NAFJA における本人確認方法について考察する。

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，NAF，NAFJA，身元確認，当人認証

A study on Identification and Authentication method at NAFJA
ー National Authentication Framework in Japan ー

Toshiaki Saisho*

Abstract: As services for the public, whether public sector or private sector, shift to services via the Internet, identification and authentication of users via the Internet is becoming increasingly important. At present, in most private sector Internet services, individual service providers perform individual identification and authentication. At present, many service providers individually carry out acquisition and management of identification and authentication information. The risk of leaks due to decentralized management of individual identification and authentication information, which is personal information and confidential information of users, by each service provider increases, and the risk of the service provider who executes inappropriate identification and authentication processes also increases. Therefore, I propose the construction of National Authentication Framework in Japan (NAFJA) aiming to reduce the risk of confidential information leakage by concentrating the identification and authentication function into a small number of specialized organizations. I expect NAFJA reduces the burden and risk of many service providers, and also improves convenience for users and personal information protection. In this paper, I analyze the guidelines on Digital Identity in the United States, which are shown in NIST SP 800-63-3 published in June 2017, and also analyze “Guidelines on the method of identity verification in administrative procedures” decided in February 2019 at the CIO liaison meeting of each ministry, and then I consider the method of identification and authentication in the NAFJA.

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

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アクセス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は利用されてはいるが、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。そのため、複数のサービスを利用する利用者は、まず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の情報等を提供する必要がある。また利用者は、インターネットサービスを利用の都度、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

* （株）IT 企画　http://advanced-it.co.jp/
mail：toshiaki.saisho@advanced-it.co.jp

物等を安全・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。

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

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には、本人確認機能を個別のサービス事業者から切り離し、本人確認サービスを提供する少数の専門事業者によるサービスを前提とした、日本における本人確認基盤（NAFJA：National Authentication Framework in Japan）の社会実装が必要である。

NAFJA の構想およびその社会実装のための課題や解決のためのアプローチなどについては“日本における本人確認基盤（NAFJA）の考察－National Authentication Framework in Japan－”（[1]）を参照願いたい。

本稿では以下、第 2 章にて論文（[1]）で提案した三つの NAFJA システム構成案を説明する。第 3 章では、NIST 発行の“Digital Identity Guidelines”シリーズのドキュメント（[5]～[8]）で示されている本人確認保証レベルを中心とした NAFJA の本人確認方法に関連する内容のポイントを、また第 4 章では各府省情報化統括責任者（CIO）連絡会議で決定された“行政手続における本人確認の手法に関するガイドライン”（[3]）で示されている行政手続きにおける本人確認手法に関連する内容のポイントをまとめている。最後に、第 3 章、第 4 章の国内外の関連ガイドラインの内容を踏まえた NAFJA における本人確認方法についての検討結果を第 5 章にて報告し、第 6 章にて考察をまとめている。

2. NAFJA システム概要

独立した本人確認サービスを利用する NAFJA の構成は、利用者およびインターネットサービスとの連携方法に応じ、三つの構成案が考えられる。それぞれの構成案を図 1～図 3 に示している。なお、本構成案の前提条件等は以下の通りとする。

＜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、本人確認に使用する本人確認情報（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保証レベルおよび本人確認方法を管理しているものとする。

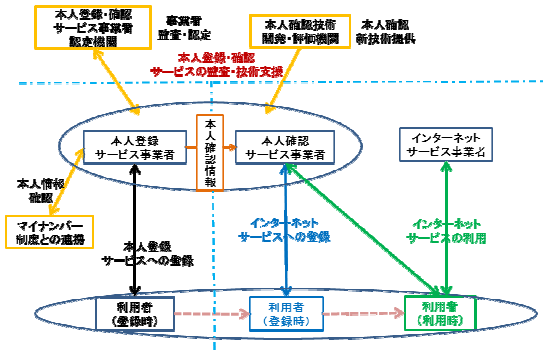

図 1　利用者中継型の NAFJA/A

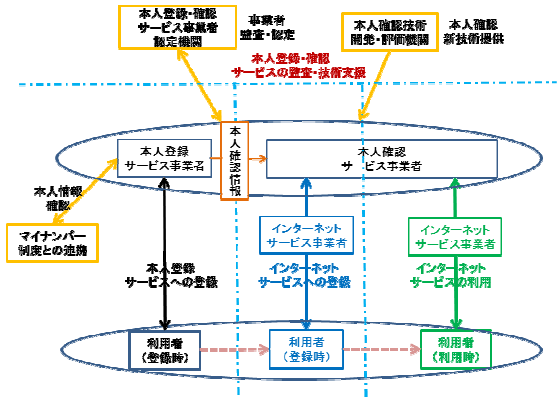

図 2　インターネットサービス事業者中継型の NAFJA/B

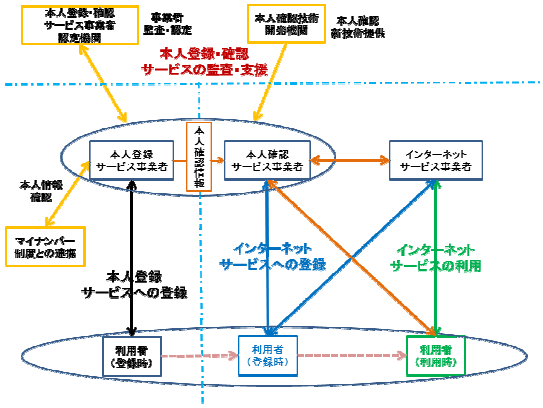

図 3　本人確認サービス事業者中継型の NAFJA/C

3. “Digital Identity Guidelines”（NIST SP 800-63-3）における本人確認保証について

アメリカ国立標準技術研究所（National Institute of Standards and Technology, NIST）では、2017 年 6 月、ディジタルアイデンティティに関する一連のガイドラインの改訂版（SP 800-63-3 シリーズ）を発行した。日本をはじめ各国は、NIST のガイドラインを参考に各国のガイドラインを策定しており、我が国でも次章で述べる“行政手続による本人確認の手法に関するガイドライン”も大きく影響を受けている。

NIST の SP 800-63-3 シリーズは、Digital Identity Guidelines の全体の枠組を示している SP 800-63-3、Enrollment and Identity Proofing Requirements についてまとめている SP 800-63-3A、Authentication and Lifecycle Management についてまとめている SP 800-63-3B、Federation and Assertions についてまとめている SP 800-63-3C、から構成されている。図 4 に SP 800-63-3 で定義されている Digital Identity Model を示している。黄色枠で示す部分が SP 800-63-3A に、赤枠で示す部分が SP 800-63-3B に、青枠で示す部分が SP 800-63-3C に、それぞれ対応している。

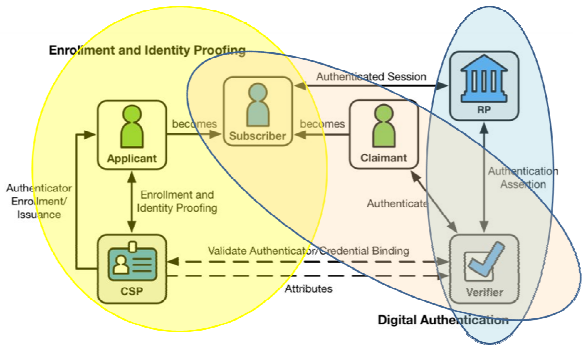

図 4　NIST 定義の Digital Identity Model
（SP 800-63-3[5]に記載されている図に加筆し作成）

図 5 が、NIST 定義の Digital Identity Model（図 4）に NAFJA の構成要素を割り当てた図である。Digital Identity Model のシステム構成は、NAFJA/C に近い構成となっている。

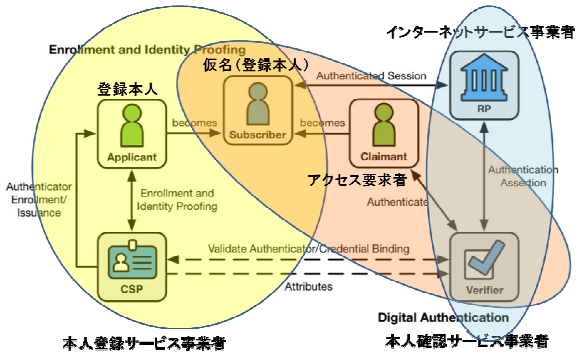

図 5　NIST Digital Identity Model と NAFJA との対応関係

本章では、NAFJA における本人確認方法および本人確認保証レベルについての検討・考察を目的として実施した SP 800-63-3B（Authentication and Lifecycle Management）の調査結果をまとめている。

一般に本人であることを示す証拠としては、本人しか知り得ないはずの情報を知っていること（記憶による確認）、本人しか持っていないはずの物を持っていること（所有物による確認）、本人しか持っていないはずの生体特徴を持っていること（生体特徴による確認）、の 3 種が存在する。SP 800-63-3B では、3 種の本人確認情報を利用した本人確認方式が提示されている（図 6）。

Entity	Claimant	
Authenticator Type	Activation Factor	Prompt/Signal from Verifier
	Authenticator	Information to Verifier
Memorized Secret	—	—
	—	Password/PIN
Look-Up Secret	—	Prompt
	Secret Table	Password/PIN
Out-of-Band Device	—	Out-of-Band Secret/Signal
	Out-of-Band Device	Received Secret/ Identifying Key
Single-Factor OTP Device	—	—
	OTP Device	Generated Password
Multi-Factor OTP Device	PIN/ Biometrics	
	OTP Device	Generated Password
Single-Factor Cryptographic Software	—	Challenge nonce
	Cryptographic Software	Generated Secret
Single-Factor Cryptographic Device	—	Challenge nonce
	Cryptographic Device	Generated Secret
Multi-Factor Cryptographic Software	PIN/ Biometrics	Challenge nonce
	Cryptographic Software	Generated Secret
Multi-Factor Cryptographic Device	PIN/ Biometrics	Challenge nonce
	Cryptographic Device	Generated Secret

図 6　本人確認方式一覧
（SP 800-63-3B[7]の内容を整理し作成）

SP 800-63-3B に示されている、Verifier が実施する本人確認結果は Claimant が Subscriber 当人かどうかを示すものであり、その確認結果の確実さを示す指標として本人確認保証レベル（AAL : Authentication Assurance Level）を定義（図 7）している。また、それぞれの本人確認保証レベルに対応する代表的な本人確認方法が例示されている（図 8）。

本人確認保証レベル	対応するSubscriberとClaimantとの紐づけに関する要件
AAL1	AAL1 では, Claimant が Subscriber に紐づく Authenticator を管理下に置いていることが, ある程度の確からしさで確認できるレベル. AAL1 では Single-factor Authentication が必須となり,Authentication を成功させるには, Claimant がセキュアな Authentication Protocol を通じて Authenticator を保持・管理していることを証明する必要がある.
AAL2	AAL2 では, Claimant が Subscriber に紐づく Authenticator を管理下に置いているということが, 高い確度で保証されるレベル. セキュアな Authentication Protocol によって, 2つの異なる Authentication Factor を保持・管理していることを証明する必要がある. AAL2 以上では, Approved Cryptographic テクノロジーも必要となる.
AAL3	AAL3 では, Claimant が Subscriber のアカウントに紐づく Authenticator を管理下に置いているということが, 非常に高い確度で保証されるレベル. AAL3 の Authentication は, 暗号プロトコルによる鍵所有証明 (Proof of Possession) に基づいている. AAL3 は AAL2 と似ているが, AAL2 に加え Verifier Impersonation 耐性のある“ハードの” Cryptographic Authenticator を要求する.

図 7　本人確認保証レベルとその要件
（SP 800-63-3 翻訳版[9]を参考に作成）

本人確認保証レベル	AAL1	AAL2	AAL3
Authenticator およびその組合せ	* Memorized Secret	* Memorized Secret	* Memorized Secret
	* Look-Up Secret	に加え以下の一つ	に加え以下の二つ
	* Out-of-Band Device	• Look-Up Secret	• SF OTP Device
	* SF OTP Device	• Out-of-Band Device	• SF Crypto Software
	* SF Crypto Software	• SF OTP Device	* Memorized Secretに加え
	* SF Crypto Device	• SF Crypto Software	• SF Crypto Device
	* MF OTP Device	• SF Crypto Device	* SF OTP Device
	* MF Crypto Software	* MF OTP Device	に加え以下の一つ
	* MF Crypto Device	* MF Crypto Software	• MF Crypto Software
		* MF Crypto Device	• MF Crypto Device
			* MF Crypto Device

図 8　本人確認保証レベルに対応する本人確認方法一覧
（SP 800-63-3B[7]の内容を整理し作成）

4.　“行政手続による本人確認の手法に関するガイドライン”における本人確認保証について

平成 30 年 7 月 20 日に「デジタル・ガバメント実行計画」（デジタル・ガバメント閣僚会議決定）が策定され、当該計画に基づき、各種行政手続きをデジタル化する際に必要となるオンラインでの本人確認に対する考え方及び手法をまとめたものが、平成 31 年 2 月 25 日に各府省情報化統括責任者（CIO）連絡会議で決定された「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」（以下、CIO ガイドラインと略記）である。平成 31 年 3 月 15 日には、行政手続きを原則、電子申請に統一するデジタルファースト法案が閣議決定され、我が国の行政手続きはオンライン化が加速するものと思われる。

CIO ガイドラインでは、SP 800-63-3B で定義されている本人確認保証レベル AAL を当人認証保証レベル、また SP 800-63-3A で定義されている Identity Assurance Level（IAL）を身元確認保証レベルと、呼称は異なるが、基本的には NIST 800-63-3A,B と同一内容である。CIO ガイドラインでは、更に IAL と AAL の組み合わせにより、Claimant が Applicant であることの確認レベル（本人確認レベル）を A～D に分類し、各レベルに対応する本人確認手法例およびその特徴を整理している。以下に示す図 9 は、NAFJA の検討のために、CIO ガイドラインの内容を本人確認レベルと必要な保証レベルの対応表としてまとめたものである。また、図 10 は、NAFJA が個人を対象とした本人確認基盤を目指しているため、CIO ガイドラインの個人を対象とした記載内容に限定し整理したものである。

オンラインによる本人確認レベル	必要な保証レベル	
	身元確認保証レベル	当人認証保証レベル
A	レベル3 対面での身元確認	レベル3 耐タンパ性が確保されたハードウェアトークン
B	レベル2 遠隔又は対面での身元確認	レベル2 複数の認証要素
C	レベル1 身元確認のない自己表明	レベル1 単一又は複数の認証要素

図 9　本人確認レベルと必要な保証レベル
（CIO ガイドライン[3]を参考に作成）

本人確認レベル	手法例	実現できること・特徴
A	・マイナンバーカード（署名用電子証明書）による身元確認でアカウントを作成。 ・マイナンバーカード（利用者証明用電子証明書）による当人認証を実施。 ※マイナンバーカード：PIN＋IC カード（耐タンパ性ハードウェアトークン）	・個人の基本4 情報を毎回確認。 ・耐タンパ性を有したハードウェアトークンであるマイナンバーカードにより、非常に高い信用度で「身元確認」、「当人認証」を実施。
B	・マイナンバーカード（署名用電子証明書）等による身元確認でアカウント作成。 ＜マイナンバーカードによる身元確認が行えない場合、対面での身分証明書等の確認や郵送した申請書（捺印付）、印鑑証明書、公的証明書（住民票等）等の確認によりアカウントを作成。＞ ・マイナンバーカード（利用者証明用電子証明書）等による当人認証を実施。 ＜マイナンバーカードによる当人認証が行えない場合、その他の多要素認証による当人認証を実施。＞ ※多要素認証の例： －ID・パスワード＋二経路認証アプリ －ID・パスワード＋ワンタイムパスワード生成アプリ －ID・パスワード＋生体認証	・登録時に個人の基本4 情報を確認。 ・認証プロセス時には、登録時の個人と同一の個人であることを確認。 ・登録時に相当程度の信用度のある「身元確認」を行い、マイナンバーカード（利用者証明用電子証明書）等の多要素認証を用いることにより相当程度の信用度のある「当人認証」を実施。
C	・身元確認を行わずにオンラインでアカウントを作成。 ・単要素認証で当人認証を実施。 ※単要素認証の例： －ID・パスワードのみ －認証デバイスのみ －生体認証のみ	・個人を正確に確認する必要がない場合を対象。 ・毎回のアクセスが、同一の者により行われていることを確認しており、ある程度の信用度のある「当人認証」を実施。

図 10　本人確認手法例およびその特徴
（CIO ガイドライン[3]を参考に作成）

5. NAFJA における本人確認方法に関する検討

本稿では、第 3 章、第 3 種で整理した国内外の関連ガイドラインの内容を参考に検討した、NAFJA における本人確認方法、について報告する。

5.1 NAFJA における身元確認

NAFJA は、日本における民間のインターネットサービス全般での活用を目指すと共に、ネット経由であっても確実な本人確認を目指した本人確認基盤である。そのため、利用者の登録時点では、確実な身元確認が実施されることを前提としているため、SP 800-63-3A で定義されている Identification Assurance Level 3（IAL3）の身元確認を想定している。具体的には、以下の要件を想定している。

①対面により本人確認

原則は対面による本人確認とする。

CIO ガイドラインでも認められているオンライン/郵送による本人確認への拡大は別途検討要。

②マイナンバーカードにより本人確認

原則はマイナンバーカードによる本人確認とする。

マイナンバーカードによる本人確認が難しい場合は、写真付きの公的証明者（パスポート、免許証、在留カード等）の利用を可能とする。

③マイナンバー制度を利用し本人の身元確認

マイナンバーカードまたはマイナンバー通知カードに記載されてマイナンバーにより地方公共団体情報システム機構（J-LIS）へ問い合わせ、本人情報の確認を実施する。

NAFJA では、身元確認後、登録申請者（Applicant）は登録者（Subscriber）として登録され識別子（ASID）が発行され、当人認証を求める Claimant が Subscriber と同一かどうかの確認に使用する本人確認方法および本人確認情報の登録を受け付ける。

本人確認方法は、あらかじめ定められた方法からの選択となり、選択した本人確認方法に必要な本人確認情報が登録可能となる。具体的な本人確認方法例については 5.3 にて述べる。

なお、本人確認情報として、マイナンバーカード以外の所有物の情報登録時はその所有物の正当な所有者であることの確認、生体特徴のテンプレート採取時は採取デバイスの妥当性等の確認が必要となる。

5.2 NAFJA における本人確認レベル

NAFJA で想定している本人確認レベルと必要な保証レベルの対応表を図 11 に示す。5.1 に示したように NAFJA では身元確認は対面を原則としているため、CIO ガイドラインの対応表（図 9）とは異なっている。

NAFJAでの本人確認レベル	必要な保証レベル	
	身元確認保証レベル	当人認証保証レベル
A	レベル3 対面での身元確認	レベル3 耐タンパ性が確保されたハードウェアトークン
B	レベル3 対面での身元確認	レベル2 複数の認証要素
C	レベル3 対面での身元確認	レベル1 単一又は複数の認証要素

図 11　NAFJA での本人確認レベルと保証レベルの対応

5.3 NAFJA における当人認証

NAFJA の当人認証に使用する本人確認方法については、SP 800-63-3B で定義されている本人確認保証レベル AAL（図 7）および対応する本人確認手法例（図 8）を参考にし、現在、我が国のインターネットサービスで利用されている本人確認方法の採用を想定している。具体例は以下の通り。

①Memorized Secret のみによる本人確認（AAL1）

インターネットショッピング等、多くのサービスサイトで利用されているパスワードによる本人確認方法である。

NAFJA の利用により、サイトごとのパスワードの記憶は不要となる。また、本人確認サービスへのログイン時のパスワードによる本人確認と統合可能で、利用者にとっての利便性は大きく向上することが期待される。（Memorized Secret による本人確認と本人確認サービスへのログイン時の本人確認との統合による利便性は、他の本人確認方法に共通である。）

②Memorized Secret に加え Look-Up-Table による本人確認（AAL2）

オンラインバンキングサービスに利用されている

本人確認方法である。

NAFJA の利用により、サイトごとの Look-Up-Table の管理は不要となる。利用者にとっての利便性は大きく向上することが期待される。しかし、利用者にとっては、本人確認のみのための Look-Up-Table の管理は負担が多く、採用するサービスは減少するものと思われる。

③Memorized Secret に加え Out-of-Band による本人確認（AAL2）

インターネットサービスへのログイン後の、リスクベース認証、追加認証として多く利用されている本人確認方法である。

当面はスマートフォン/携帯電話の利用となろうが、ウェアラブルデバイスの普及に伴い、利便性の高い本人確認方法として利用が広がるものと思われる。

④Memorized Secret に加え SF OTP Device による本人確認（AAL2）

多くのオンラインバンキングサービスで利用されている本人確認方法である。

NAFJA の利用により、本人確認登録サービス事業者による SF OTP Device の配布が必要となるが、サイトごとの複数の SF OTP Device の管理は不要となり、利用者にとっての利便性は大きく向上することが期待される。

⑤MF Crypto Device の一つであるマイナンバーカードによる本人確認（AAL3）

CIO ガイドラインに記載されているマイナンバーカードによる本人確認である。Claimant 側の NFC 機能搭載 PC/スマートフォン等によるマイナンバーカード利用環境の普及に伴い、AAL3 レベルの本人確認を前提としたインターネットサービスも増加するものと思われる。

5.4 生体認証による本人確認の可能性

生体認証による本人確認は、歴史はあるが本格的な実用化には至っていない。2020 年の東京オリンピックで急増する海外観光客対応のため、日本人出帰国手続への顔認証技術の導入が平成 29 年度より始まり、また海外観光客の安全性・利便性向上を目指した手ぶらショッピング等への応用など、実証実験も活発に行われ始めてきたが、このような生体認証の応用の動きも、生体認証に使用する機器はサービス提供者側の管理下にあるという、銀行の ATM や入退室管理システムと同じ従来型の利用パターンに限られている。

NAFJA では、オンラインでアクセスを要求する Claimant の手元で生体認証を行う必要があり、生体認証に使用する機器は一般には本人確認サービス事業者の管理下には無い。もちろん、生体認証に使用する機器が安価になれば本人登録・確認サービス事業者が利用者へ配布する方式も考えられるが、近々に実現する可能性は無い。Claimant の管理下の機器による生体認証の場合、その結果の信頼性を本人確認サービス事業者がどのように確認できるかが課題となる。

このようなオンラインでの本人確認へのローカルな生体認証の適用に対する課題への二つの主要なアプローチ（ACBio、FIDO）の概要、および NAFJA で利用する場合の課題等を以下にまとめている。

(1)ACBio（Authentication Context for Biometrics）[10]

ACBio は、筆者が 2000 年頃より検討に着手したインターネット経由の確実な本人確認が可能な仕組み「本人確認保証フレームワーク」の研究を発展させた成果であり、2004 年に ISO/IEC JTC1/SC27 に提案、その後、筆者がプロジェクトエディタに就任、国際標準化活動を展開、2009 年 5 月に国際標準 ISO/IEC 24761：ACBio（Authentication Context for Biometrics)として発行された。

ACBio では、生体認証に関わる処理の全てを Claimant 側で実施するモデル（ローカル認証）から、Claimant 側では生体特徴の採取のみとし以降は全て Verifier 側で実施するモデル（サーバ認証）まで、多様な生体認証モデルに対応できるよう考案した仕様となっており、Claimant 側での生体認証に関わる処理の結果と共に、Verifier がその結果の正当性を検証するためのデータを提供するプロトコルおよびデータ形式を定めている。Claimant 側での生体認証に関わる処理は、単一の機器あるいは複数の機器で実行され、各機器の製造企業は機器の諸元・製造企業・型番・シリアルナンバ等が記載されているデバイス証明書を発行するものとし、各機器の機能や性能やセキュリティに関する第三者による評価結果も属性証明書として公開されていることを前提とし、Verifier はネット上に公開されているデバイス証明書、各種属性証明書および、Claimant から直接送付されてくる各機器の入出力データへの署名から、Claimant 側で実施された生体認証に関わる処理結果の妥当性のレベルを確認する仕組みである。

ACBio ベースの生体認証モデルを NAFJA へ登録する場合、Applicant は NAFJA で認定された ACBio ベースの生体認証機器を使うものとし、その生体認証機器の情報（デバイス証明書等）およびその場で採取したテンプレートを本人確認情報として登録することになろう。なお、Claimant 側でテンプレートとの照合を実施するモデルの場合は、本人登録サービス事業者が署名したテンプレートを Applicant へ提供することになろう。

ACBio に基づく本人確認方法は、デバイス証明書の検証が実施されるため SP 800-63-3B で定義されている SF Crypto Device または MF Crypto Device に該当し、本人確認保証レベルは AAL2 または AAL3 に該当する。また ACBio では、生体認証による本人確認あるいは Claimant 側での生体認証に関わる処理結果の正当性確認が Verifier 側で実施されるため、更に高い本人確認保証が得られるものと期待

される。

(2)FIDO（Fast IDentity Online）[11]

2013 年に発足した FIDO アライアンスは、パスワードに頼らない新しい本人確認方法の標準化を進めている。具体的には、公開鍵暗号方式に基づく Crypto Device を Authenticator として利用し、Authenticator の Activation Factor の一つとして生体認証も位置づけられている。つまり生体認証が Claimant 側で完結（ローカル認証）し、その認証成功時に Claimant の Authenticator と Verifier 間での認証が開始される。ACBio との本質的な違いは、生体特徴を利用したサーバ認証をサポートしていないことである。FIDO としては、多くの開発ベンダ・利用企業の合意がとれる範囲に限定した仕様で早期の標準化・実用化を目指す戦略であろう。

FIDO に基づく本人確認方法は、SP 800-63-3B で定義されている MF Crypto Device に該当し、本人確認保証レベルは AAL3 に該当する。

FIDO による生体認証を利用した本人確認方法を NAFJA へ登録する場合、Applicant は認定された Authenticator および生体認証装置を本人登録サービス事業者の窓口へ持参し、確認を受け登録することになろう。

5.5 NAFJA で採用する本人確認手法の追加・見直し

IT の発展、社会の IT 環境の変化・進展は目覚ましく、今後、より確実で利便性の良い新たな本人確認方法が出現するものと思われる。本人確認基盤の安全性・信頼性・利便性の向上は、我が国のインターネット社会の発展を支える基盤であり、IT の発展、社会の IT 環境の変化・進展に応じ、またしっかりとした技術評価結果に基づいた、NAFJA で使用する本人確認手法の追加・見直しが必要となろう。

6. おわりに

(1)NAFJA の必要性

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（NAFJA）の構築が必要である。

なお、マイナンバーカードの普及に伴い、民間のインターネットサービスもマイナンバーカードによる本人確認への移行が進み、インターネットサービス事業者は個人個人の秘密情報を本人確認情報として管理する必要が無くなり、利用者の利便性も本人確認方法の統一により改善されることが期待される。これは、インターネット利用における確実な本人確認と利用者の利便性改善の大きな一歩となることは確かであろうが、今後もますますインターネット依存を強めるであろう我が国としては、IT 技術・IT 利用環境の急速な変化に応じた新たな本人確認手法への柔軟な対応を可能とする NAFJA への期待は大きい。

(2)NAFJA における本人確認方法

また本稿では、NAFJA の社会実装に向け、想定される具体的構成案を示し、“Digital Identity Guidelines”（NIST SP 800-63-3）における本人確認保証および“行政手続による本人確認の手法に関するガイドライン”における本人確認保証について調査・整理し、その上で NAFJA における身元確認保証、当人認証保証および採用すべき本人確認方法について考察した。

本人確認方法は時代時代の研究開発・製品開発状況および社会の IT 環境の変化に応じ確実で利便性の良い最新の方法へスムーズに移行できる仕組みが NAFJA でも必要である。

また、NAFJA では複数の本人登録サービス事業者、本人確認サービス事業者を前提としている。その事業者間での本人確認方法や本人確認情報の安全な共有をどのように行うかが課題となる。NAFJA では、ブロックチェーンの活用を想定しているが、今後の検討課題である。

(3)グローバル展開に向けて

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。

なお、本稿では NAFJA における利用者の身元確認およびネット経由の当人認証を対象に検討した。身元確認については、各国固有の事情に基づく National ID System が構築・運用されることになり、日本ではマイナンバーカード、マイナンバー制度を活用した確実な身元確認を想定している。当人認証についても、各国社会の IT 利用環境の違いから採用される本人確認方法や本人確認情報は異なることになろう。

しかし、各国の確実な身元確認の仕組み、当人認証の仕組みにより得られた本人確認結果は、国境のないインターネット社会での様々のサービスで利用される必要がある。今後検討すべき NAFJA による本人確認結果の内容や形式は、NIST のガイドライン SP 800-63-3C および SAML や OpenID Connect の仕様との整合性を考慮し検討する必要があろう。

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]「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] 「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

[4] 「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

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

[6]「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

[7]「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

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

[9]「Digital Identity Guidelines (翻訳版)」，NIST Special Publication 800-63-3，June 2017.
https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html

[10]「ISO/IEC 24761:2009 “Information technology -- Security techniques -- Authentication context for biometrics”」, Mar. 2009.
https://www.iso.org/standard/41531.html

[11] FIDO Alliance，https://fidoalliance.org/