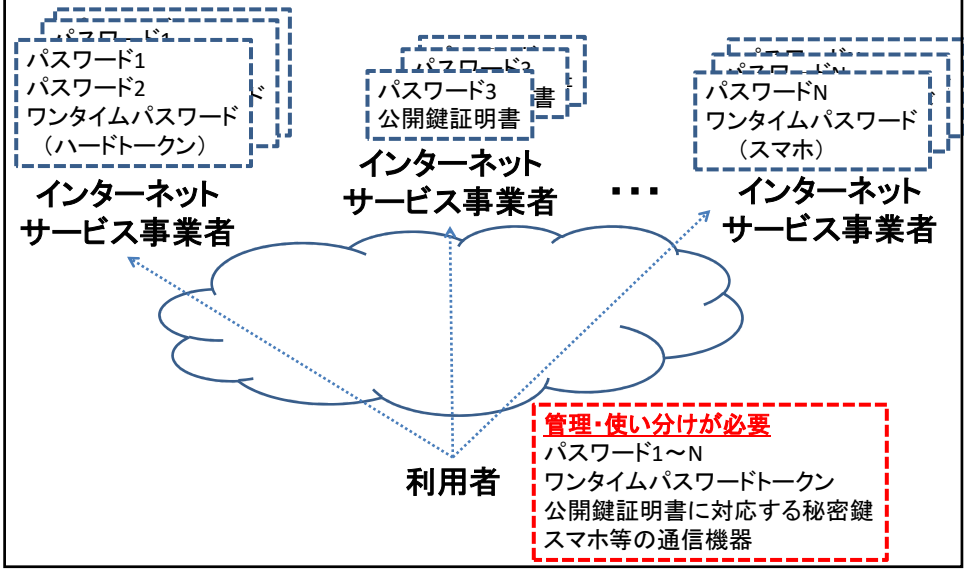
CSS2019

NAFJPにおける
本人確認方法に関する考察
(National Authentication Framework in Japan)

2019年10月21日
(株)IT企画　才所敏明
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

説明項目一覧

インターネットサービスにおける本人確認の現状



個別サービスごとの本人確認の課題

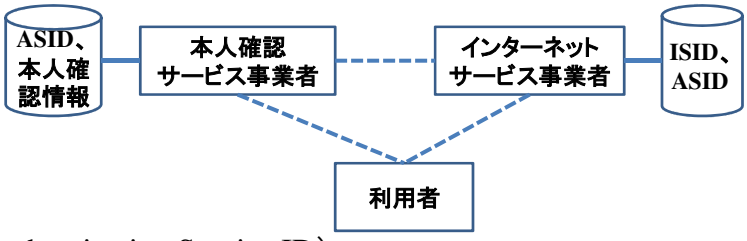
①多くの本人確認情報の安全・確実な管理のための、利用者の負担

②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

③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
（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）

④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負担

独立した本人確認サービスのモデル



ASID（Authentication Service ID）：

本人確認サービス事業者から割り当てられる本人確認サービス利用者ID

ISID（Internet Service ID）：

インターネットサービス事業者から割り当てられるインターネットサービス利用者ID

本人確認サービス事業者：ASIDと対応付け、

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）、

本人確認情報（パスワード、所有物、生体特徴に関する情報）を管理

インターネットサービス事業者：ISIDと対応付け、

ASIDおよび、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

独立した本人確認サービス 期待される効果

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

＊本人確認手続きが一定レベル標準化されることによる、利便性の向上

＊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 5分■

独立した本人確認サービスを利用した日本の本人確認基盤（NAFJP）

National Authentication Framework in Japan

本人確認基盤としての基本機能

①身元確認機能

確実な身元確認（特定・追跡性の保証）

ネット経由の当人認証のための情報の確実な登録

②当人認証機能

“①身元確認機能”で登録された

当人認証情報に基づく確実な当人認証

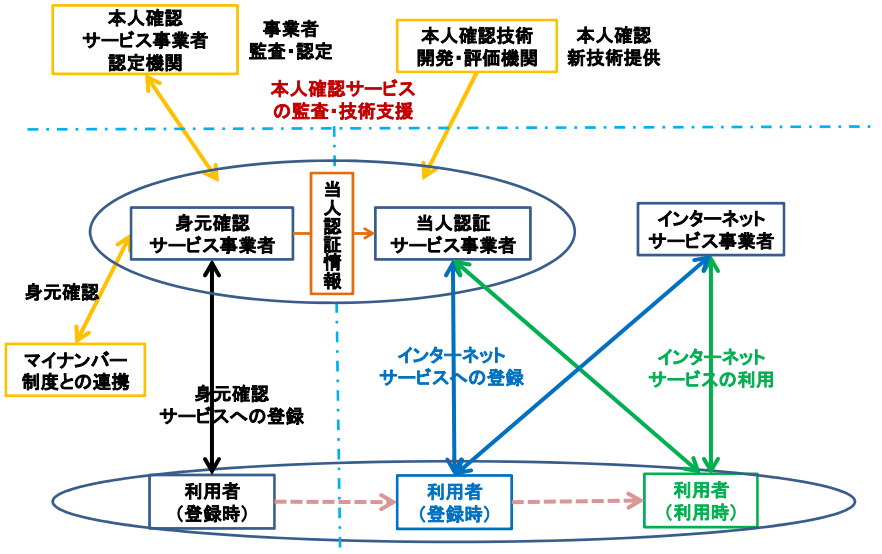
③インターネットサービスにおける利用者確認機能

インターネットサービスで定義した本人確認レベルに応じた

“①身元確認機能”**および** “②当人認証機能”による

本人確認結果の確認

利用者中継型の本人確認基盤（NAFJP/A）



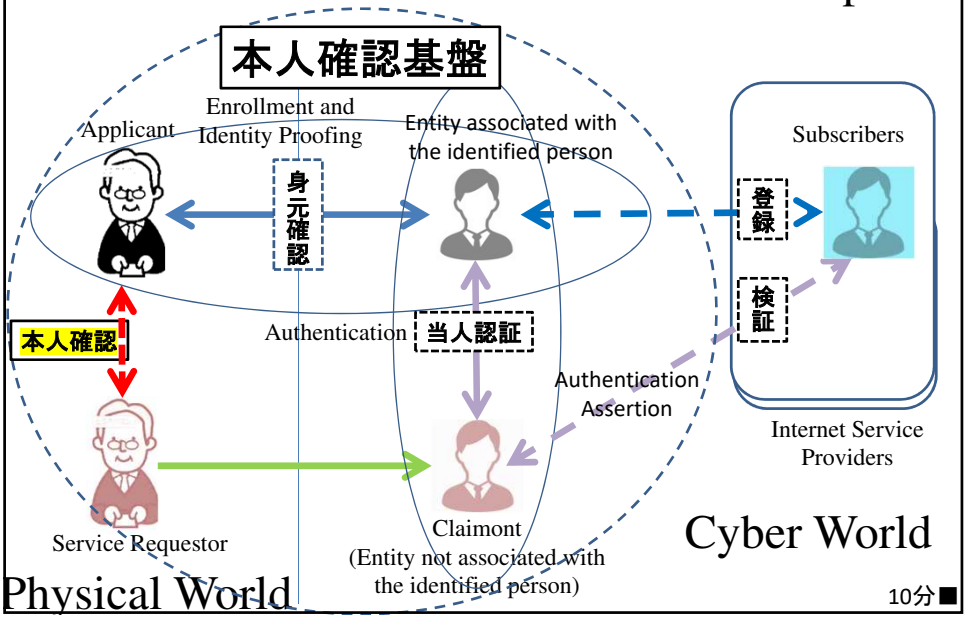
NAFJPの構成説明

①本人確認機能は、
登録時の窓口での身元確認を担当する事業者と
登録利用者に対するネット経由の当人認証を担当する事業者
による社会実装を想定

②本人確認基盤による本人確認の信頼性を高めるには、
本人確認基盤を支える組織の
第三者機関による監査等の仕組み（機能）が必要
➔本人確認サービス事業者認定機関

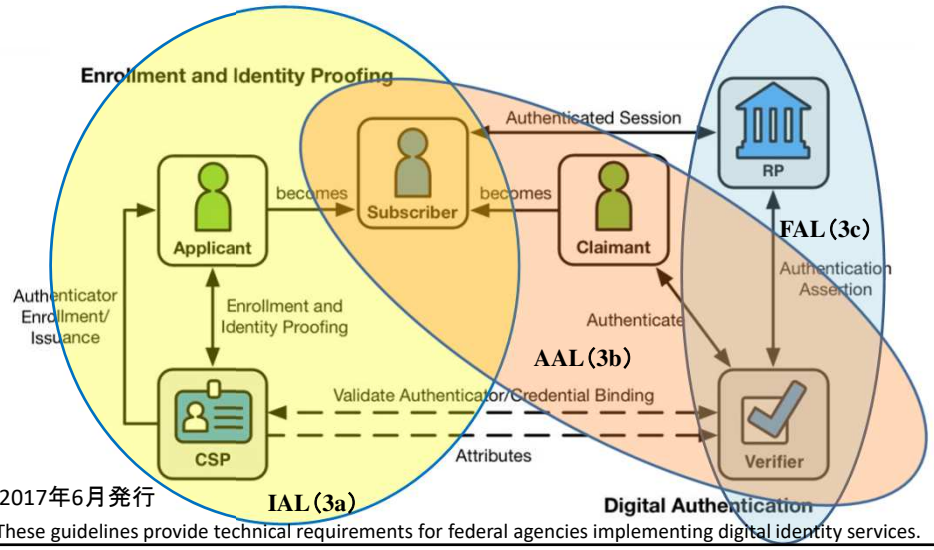
③我が国のインターネット利用の高度化、利活用促進には、
先進的で安全・確実な本人確認機能の研究開発、
早期の社会実装を支援する仕組み（機能）が必要
➔本人確認技術開発・評価機関

NAFJP
（National Authentication Framework in Japan）



10分■

Digital Identity Model（NIST SP 800-63-3）



2017年6月発行

These guidelines provide technical requirements for federal agencies implementing digital identity services.

IAL（Identity Assurance Level）

IAL1：Applicant を現実世界の特定の Identityと紐づける必要はない
提供される Self-asserted Attribute は確認も検証もされない

IAL2：Applicant が現実世界の Claimed Identity と、
適切に関連づけられていることをエビデンスにより証明が必要
（Remote ないしは対面での Identity Proofing が必要）

IAL3：対面での Identity Proofing が必要
識別に用いる Attribute は Authorized かつ訓練を受けた
CSP の代理人によって検証されることが必要

▼

AAL（Authentication Assurance Level）

AAL1：Subscriberのアカウントに対して結び付けられている
単一要素または多要素のAuthenticatorを
Claimantが所有・制御の証明が必要

AAL2：Subscriberのアカウントに対して結び付けられている二つの
異なるAuthentication要素をClaimantが所有・制御の証明が必要
（Approved Cryptographic技術がAAL2及びそれ以上では必要）

AAL3：Subscriberのアカウントに対して結び付けられている
一つのハードウェアベースのAuthenticatorと，
一つのVerifierなりすまし耐性を備えるAuthenticatorを
Claimantが所有・制御の証明が必要 ▼

Authenticator

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

Entity	Claimant	
Authenticator Type	Activation Factor	Prompt/Signal from Verifier
	Authenticator	Information to Verifier
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

（SP 800-63-3Bの内容を整理し作成） ▼

3．NISTのガイドライン概要

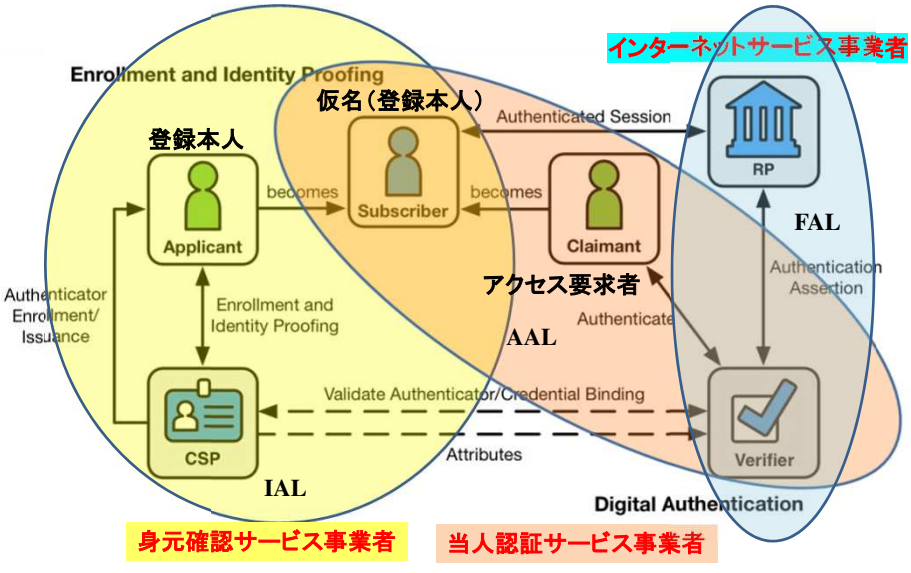
Authentication Assurance Level

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

（SP 800-63-3Bの内容を整理し作成）▼

3．NISTのガイドライン概要

NAFJPとDigital Identity Modelとの関係



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 25 日

平成 30 年 7 月 20 日にデジタル・ガバメント閣僚会議決定された「デジタル・ガバメント実行計画」に基づき、**各種行政手続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**。

「電子的な本人確認の手段についても、行政手続における本人確認等の手法として広く用いられているマイナンバーカード等を用いた電子署名に加え、情報システムの取り扱う情報や行政サービスの性質等を勘案し、電子署名以外の電子認証等の適切な技術選択を行うことが重要である。また、**電子認証に関しては、近年技術標準の検討も進んでおり、国際的な標準化（米国 NIST SP800-63-3 等）とも整合性を持った取組を推進する必要がある。**」

身元確認保証レベル

レベル1（IAL1）：身元識別情報が確認される必要がなく、
身元確認の信用度がほとんどない。
身元識別情報は自己表明若しくは自己表明相当である。

レベル2（IAL2）：身元識別情報が遠隔又は対面で確認され、
身元確認の信用度が相当程度ある。

レベル3（IAL3）：身元識別情報が特定された担当者の
対面で確認され、身元確認の信用度が非常に高い。

▼

当人認証保証レベル

レベル1（AAL1）：認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、単要素若しくは複数要素を使うことにより、当人認証の信用度がある程度ある。

レベル2（AAL2）：認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、複数要素を使うことにより、当人認証の信用度が相当程度ある。

レベル3（AAL3）：認証要求者が身元識別情報と紐付けられており、認証情報の3要素のうち、耐タンパ性を有するハードウェアを含む複数要素を使うことにより、当人認証の信用度が非常に高い。

本人確認レベルと必要な保証レベル

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

本人確認手法例およびその特徴

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。

▼

NAFJPにおけるける本人確認方法の考察

①国際的な標準化（NISTガイドライン等）との整合性が重要
　CIOガイドラインもNISTのガイドラインベース

②身元確認はマイナンバーカードベース
　JLISのサービスを活用

③当人認証は、日本のIT利用環境をベースに方法を評価・選定
　マイナンバーカードベースの当人認証が望ましいが・・・
　将来は、行政サービス向けの
　　本人確認サービスとの統合が望ましいが・・・

④今回は考察の対象外としたが、NAFJPでは不可欠
　CIOガイドラインではFederationは想定していない

想定しているNAFJPにおける身元確認レベル

NAFJP 身元確認 レベル	身元確認内容	NIST ガイドライン 対応レベル	CIO ガイドライン 対応レベル
3	①対面による申請 ②マイナンバーカードの所有および写真による申請者確認 ③マイナンバー制度	3	3
2	①オンラインによる申請 ②マイナンバーカードの所有による申請者確認 ③マイナンバー制度を利用した身元確認	2	2

①今後、より確実な本人確認へのニーズを踏まえ、確実な身元確認を原則とする（NISTにおける身元確認レベル1は対象外とする）
②マイナンバーカード提示の代わりに、マイナンバーおよび写真付きの公的証明書の提示による代替も可

想定しているNAFJPにおける当人認証レベル

NAFJP 当人認証 レベル	当人認証内容	NIST ガイドライン 対応レベル	CIO ガイドライン 対応レベル
3	①パスワードおよびマイナンバーカードによる当人認証	3	3
2	①パスワードおよびOut-of-Bandデバイスによる当人認証	2	2
1	①パスワードによる当人認証	1	1

①Out-of-Bandデバイスとしては、スマホ/携帯を想定
②レベル3を超える当人認証が将来社会実装されることを想定

5. NAFJPにおける本人確認

想定しているNAFJPにおける本人確認レベル

NAFJP 本人確認 レベル	必要な保証レベル	
	身元確認 レベル	当人認証 レベル
A	3	3
B	2	2
C	2	1

①将来、レベルAを超える本人確認レベルの可能性を想定

6. おわりに

NAFJP実現に向けた課題

①新たな当人認証方式の社会実装が容易な仕組み

必要に応じ、社会のコンセンサスを得、生体認証も含め新たな方式を追加

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式の追加、スムーズな移行の仕組みが必要

②本人登録・確認サービス事業者間の情報共有・秘匿

NAFJPでは複数の身元確認サービス事業者、当人認証サービス事業者を前提、その事業者間での当人認証方法や当人認証情報の安全な共有をどのように行うかが技術課題の一つ

③NAFJPを構成する組織・機関の具体的実現

身元確認・当人認証サービス事業者（本人確認サービス事業者）

本人確認サービス事業者認定機関

本人確認技術開発・評価機関

6. おわりに

各国のディジタルIDシステムの例1

SecureKey Concierge, Canada
(~50% adoption)
- Federated system launched in 2012 led and operated by financial institutions
- Enables authentication only with a range of public and private sector institutions through online login

UK Verify, UK
(<10% adoption)
- Federated system launched in 2016 by public sector, with private identity providers
- Enables authentication only with a set of public sector departments through online login, with plans to expand to private sector institutions

BankID, Sweden
(~75% adoption)
- Launched in 2003 by financial institutions, now recognized by the government
- Enables digital authentication and signature with limited data sharing for use with public and private sector institutions through smart card or digital device (mobile or computer)

e-ID, Estonia
(90+% adoption)
- Launched by public sector in 2000, with over 940 public and private sector institutions connected today
- Facilitates authentication, data storage and sharing, and digital signature through chip based card or digital keys

DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH JANUARY 2019（McKinsey & Company）

6. おわりに

各国のディジタルIDシステムの例2

Digital Identification System (SID), Argentina
(<10% adoption)
- Recently launched by government in coordination with private sector
- Will enable remote biometric authentication across public and private sector services

National eID, Nigeria
(<10% adoption)
- eID card launched by public sector in partnership with Mastercard in 2014
- Enables authentication through chip based card and data sharing for KYC, with potential additional future use cases under consideration

Aadhaar, India
(90+% adoption[1])
- Launched in 2009 by agency established by public sector
- Enables biometric digital authentication, as part of broader digital ecosystems with additional functionality
- Key use cases include direct transfer of benefits to bank accounts, e-KYC, digital document storage

DIGITAL IDENTIFICATION: A KEY TO INCLUSIVE GROWTH JANUARY 2019（McKinsey & Company）

各国の本人確認の仕組み ハーモナイゼーションが必要

①身元確認は、各国のNational ID Systemに依存

身元確認については、各国固有の事情に基づき構築されるNational ID Systemの利用を想定、日本ではマイナンバー制度を活用した確実な身元確認を想定

②当人認証についても、各国のIT利用環境に相当程度依存

当人認証についても、各国のIT利用環境に応じ異なる方式となることが想定

③インターネットサービスのグローバル性から、認証連携（Federation）方式は国際標準化が不可欠

今回は詳細な検討は行わなかったが、認証連携方式については、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ことが必要

④各国の事情で異なるであろう身元確認・当人認証方式であっても、それぞれが保証するレベルについては、各国間での合意が必要

終