JICSAP
Japan ID Connect with Secure Authentication
Promotional association

本人認証技術導入ガイドライン
【基本知識編】
第一版

2019 年 10 月

一般社団法人　ID 認証技術推進協会（JICSAP）

Copyright© 2019 JICSAP All rights reserved.

JICSAP
Japan ID Connect with Secure Authentication Promotional association

目次

1．　はじめに……1
(1)　ガイドラインの目的……2
(2)　本ガイドラインにおける本人認証のコンセプト……2
2．　認証とは……4
(1)　認証の基礎知識……4
(2)　本人認証を構成する機能……6
(3)　本人認証の機能分担……7
①　本人確認（IV：Identity Verification）……7
②　利用者識別（UI：User Identification）……8
③　利用者検証（UV：User Verification）……8
(4)　利用者登録とサービス利用の関係……10
(5)　認証のレベル……10
(6)　認証とリスク・利便性……12
3．　認証技術……14
(1)　認証技術の分類……14
①　持ち物……14
②　記憶……14
③　生体……15
(2)　多要素認証……15
(3)　途上認証……15
(4)　認証技術の一覧……17
①　「持ち物による認証」に使われる技術……17
②　「記憶による認証」に使われる技術……20
③　「生体による認証」に使われる技術……21
(5)　認証の実装方法……23
①　QR コード決済における認証……23
②　IC カード決済取引における利用者検証……24
③　生体認証におけるローカル照合とサーバ照合……25
④　3-D セキュアによる本人認証……26
4．　認証技術評価……27
(1)　利用者評価……27
(2)　事業者評価……29
5．　ユースケース…
6．　用語定義……36

JICSAP 会員に限り開示

Copyright© 2019 JICSAP All rights reserved.

JICSAP
Japan ID Connect with Secure Authentication Promotional association

更新履歴

更新日	バージョン	更新内容
2017 年 10 月 19 日	Ver. 0.1β	新規作成
2019 年 9 月 30 日	Ver. 0.99β	JICSAP 会員からの意見募集実施
2019 年 10 月 8 日	Ver. 0.99β	一般からの意見募集（パブコメ）実施
2019 年 10 月 23 日	Ver. 1.0	一般公開（5 章「ユースケース」のみ会員限り公開）

■商標について
・本書に記載されている会社名、製品名等は、各社の商標または登録商標です。

■免責事項
一般社団法人 ID 認証技術推進協会（JICSAP）は、本ガイドラインに含まれるすべての事項につき、いかなる表明も保証も行いません。本ガイドラインを利用する者は、自己の責任と負担において本ガイドラインを利用するものとし、協会は本ガイドラインの利用により関連事業者、利用者、その他第三者に生じた損害・損失・負担等の一切の結果についていかなる責任も負わず、本ガイドラインを利用する者は協会に対していかなる責任の追及も行わないものとします。

■注意事項
・本書の内容は発行時点のものであり、予告なく変更する場合があります。
・出典を明記していない図表等は、JICSAP が本ガイドラインのために作成したものです。
・本書の内容を JICSAP の許可なく、複製・転載することを禁止いたします。

Copyright© 2019 JICSAP All rights reserved.

JICSAP
Japan ID Connect with Secure Authentication Promotional association

１．　はじめに

現代のデジタル化された社会において、本人認証技術を使用する機会はリアル、サイバー空間を問わずに急増している。キャッシュレスをはじめとした生活サービスのオンライン化や、入退室管理、情報アクセス管理などサービスのデジタル化が進む一方で、不正ログイン、不正アクセスなどによる被害が増大し、社会問題化しつつある。

本人認証は、サービス利用時の本人確認を確実・安定的・短時間・低コストで行うために、本人確認の代替として利用者識別と利用者検証を行うものである。本人認証はまた、サービス利用者の安心・安全を確保する機能であるが、サービスを提供する事業者（以下、事業者）がその実装方法を誤れば不正利用のリスクが高まる恐れがある。

他方で、事業者による本人認証の導入にあたっては、本人認証技術の種類と組合せが複雑化し、「自社のサービスにどれを採用したらよいのかわからない」との声が寄せられている。本人認証技術は多様化しているが、それぞれ安全性、導入容易性、コスト、利便性などに一長一短があり、またサービスの内容により求められる要素は異なる。 その選択・採用においてはこれらの要素に配慮した総合的な判断が求められる。

そこで ID 認証技術推進協会（JICSAP）では、利用場面ごとに現在の社会で主に採用されている本人認証技術についてユースケース（導入場面）ごとに整理し、あるべき本人認証技術の選択において参考となるガイドラインを策定することとした。本ガイドラインは、【基本知識編】として、本人認証技術の全体概要を俯瞰する目的で編纂された。 今後も、本人認証におけるセキュリティレベルの考え方や、個別の本人認証技術に対する客観的な評価軸の策定、ユースケース（導入場面）を特定した本人認証技術のあり方などについて、ガイドラインの策定を目指すものである。

なお、本人認証技術を取り巻く環境は日々刻々と変化している。読者は本ガイドライン記載の内容にとらわれることなく、常に最新の状況を参照しつつ、自社に適した本人認証技術を選択することが肝要である。また、本ガイドライン以外にも、業界団体、関連当局等が本人認証に関する指針やガイドラインを策定している場合があり、これらも参照されたい。

本ガイドラインが、本人認証技術を導入してサービスを提供する事業者、ならびに、本人認証機能を提供する製品やソリューションを開発・供給する事業者にとって、信頼性の高いサービス提供を可能にするための一助となれば幸いである。

(1)　ガイドラインの目的

本書の目的は、本人認証の導入を検討する事業者が、多数存在する認証技術の中から、自らのサービスに適した認証技術を導入する際に参考となるガイドライン（指針）を示すことにある。

また認証技術とともにそのユースケース（導入場面）も示すことで、技術一覧とユースケースの関係性や、これらを利用する際の考え方、留意事項を明確にして、上記目的を果たすことを目指す。

(2)　本ガイドラインにおける本人認証のコンセプト

本人認証技術の導入を検討する事業者が、自らのサービスに適した認証技術を選択して導入する際には、以下に掲げる①～⑥の 6 つの観点のそれぞれについて、検討を行うことが望ましい。

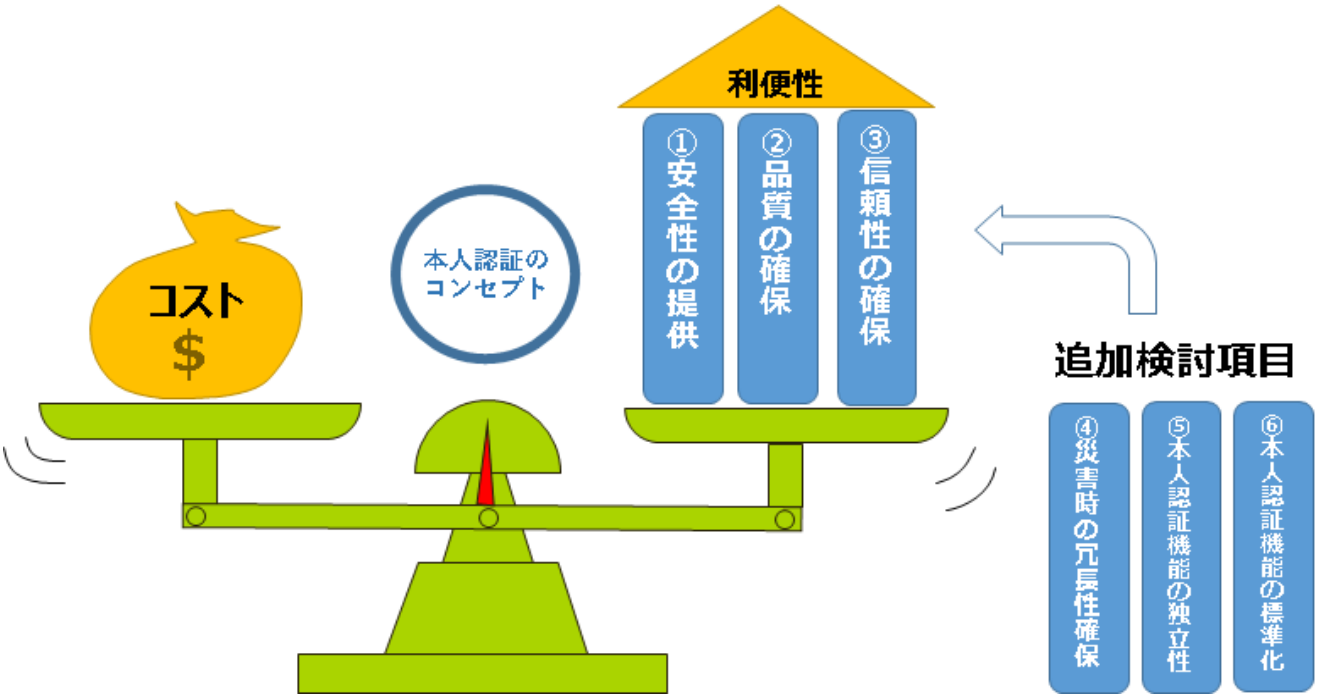

図 1　本ガイドラインにおける本人認証のコンセプト

①　安全性の提供

本人認証技術の選択・採用においては、安全性を考慮する必要がある。本人認証における安全性とは、認められた本人だけが情報や資産にアクセス可能であり、正当でない者によるアクセスである「成りすまし」のリスクが許容可能なレベルに抑えられている必要がある。

また、本人認証における安全性は、一連の認証手続きが人間対応と機械対応のどちらによりなされるのか（有人・無人）や、オフラインとオンラインのどちらで処理されるか、といった導入環境によっても変わり得るため、それらに応じた安全性を考慮する必要がある。

② **品質の確保**

本人認証技術の選択・採用においては、導入しようとする本人確認方法や本人認証技術に関して、それぞれの品質を理解したうえで導入する必要がある。本人認証における品質とは、「認証精度が高い（取り違えない・本人を排除しない）」、「反応速度が速い」、「使い勝手が良い」などの尺度がある。これらの総体として、正当な権利を有する利用者に対して正しくサービスを提供できることが、本人認証技術の品質である。

③ **信頼性の確保**

本人認証技術の選択・採用においては、信頼性が高く、使いやすい技術であることが重要である。本人認証における信頼性とは、災害時などの特殊な状況を除き、いかなる場合でも本人認証機能を提供し続けることを指す。システムダウンや認証エラーの発生はサービス停止に繋がるため、発生しない、もしくは発生時に代替手段の適用を可能とするなどの観点が求められる。

④ **災害等発生時の冗長性の確保**

本人認証技術の選択・採用においては、災害等発生時にサービスを継続する必要性や方針の有無についても考慮したほうがよい。災害等発生時にもサービス提供が必要な場合には、認証技術が正常に稼動しない場合も見据えて、代替手段等により冗長性を確保することが望ましい。

⑤ **本人認証機能の独立性**

本人認証技術の選択・採用においては、本人認証機能そのものは自社サービスの機能とは分離し、独立した機能として実装するように考慮したほうがよい。 本人認証機能が独立した状態であれば、自社サービス機能の変更・拡張に影響されずセキュリティ更新が容易になり、セキュリティ監査の負荷も軽減する。また将来他の自社サービスを立ち上げるうえでも、この独立した本人認証機能を共有利用でき有用である。

すでに本人認証を実施している他社本人認証ソリューション（プロバイダから提供される本人認証の肩代わりをしてくれるサービス）が存在する場合、本人認証機能の共通化や、API 連携等の方法を用いてそれらを流用することもできる。

⑥ **本人認証機能の標準化**

本人認証技術の選択・採用においては、本人確認業務を効率化・高度化していく観点からの検討も必要である。自社と同様のサービスが採用している本人認証の仕組みを参考にしながら、標準化された認証技術の選択・採用を考慮したほうがよい。

上記 6 つの観点を検討する際には、システム提供にかかるコスト（設備投資代、運用費用など）との均衡を踏まえて、判断することが求められる。特に①②③は必須の検討項目であり、④⑤⑥は追加検討項目と位置付けられる。それぞれの観点をより手厚くした分だけコストは増加するのが一般的であり、事業者が提供しようとするサービスのリスクに見合った本人認証技術を選定することが望ましい。

同様に、それぞれの観点を追及し過ぎれば、本人認証技術を利用する際の利便性を損なう可能性があるため、本人認証技術の選択・採用においてはコストや利便性等にも配慮した総合的な判断が求められる。

２．　認証とは

（1）　認証の基礎知識

本書で扱う認証とは、本人認証のことを指す。

本人認証とは、「ある人が、相手に本人であることを証明させて、検証すること」をいう。

例えば、A 氏が B 氏に対して B 氏が本当に「B」であることを証明させ、それを A 氏が検証するとき、「A 氏は B 氏を認証する」と表現する。また、その際に、A 氏のことを認証者（もしくは検証者： verifier）、B を被認証者（もしくは証明者：prover）と呼ぶ（図２）。

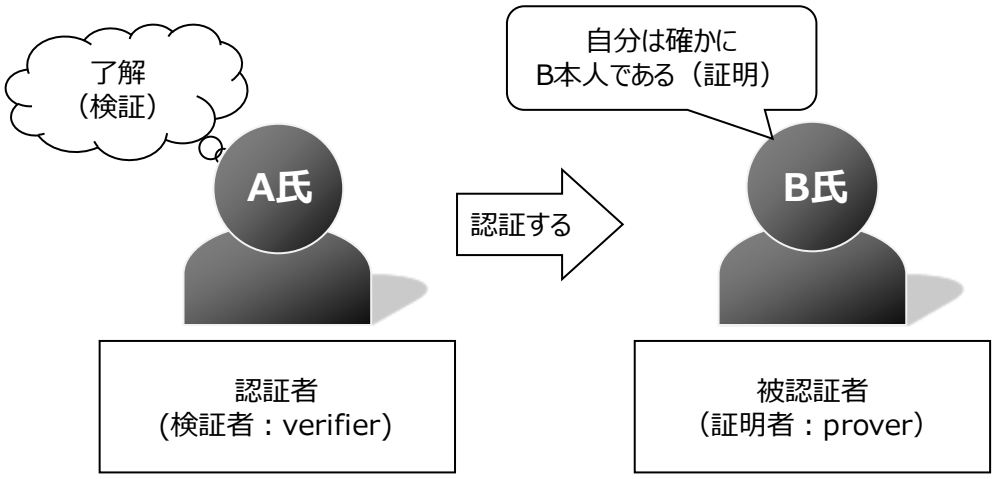

図２　本人認証の基本的な仕組み

上記のように、A 氏が B 氏のことを一方的に本人認証する形態を「片側（片方向）認証」という。これに対して、同時に B 氏も A 氏のことを本人認証する形態を「相互（双方向）認証」（図３）という。

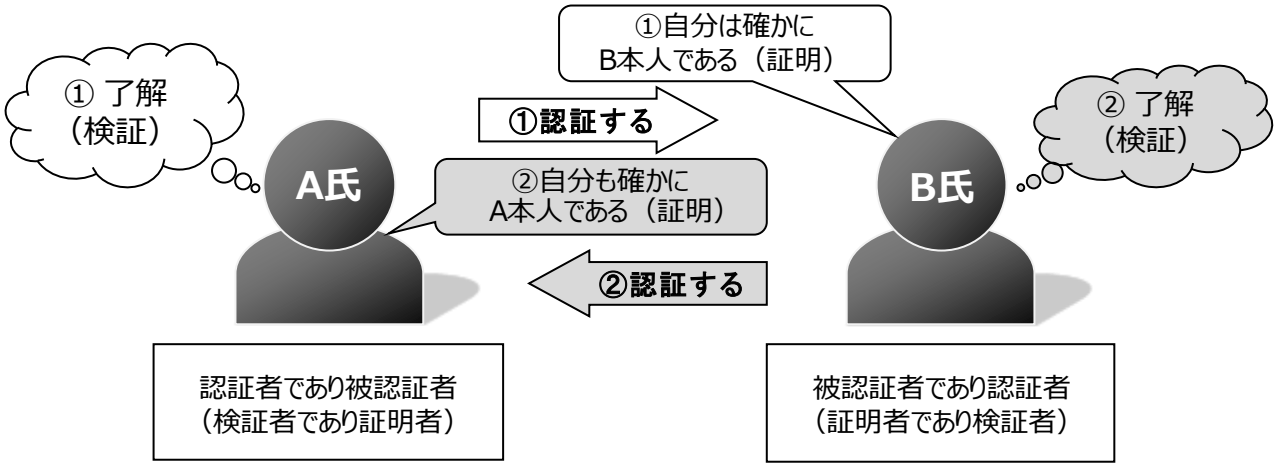

図３　相互（双方向）認証は、お互いに本人認証し合う仕組み

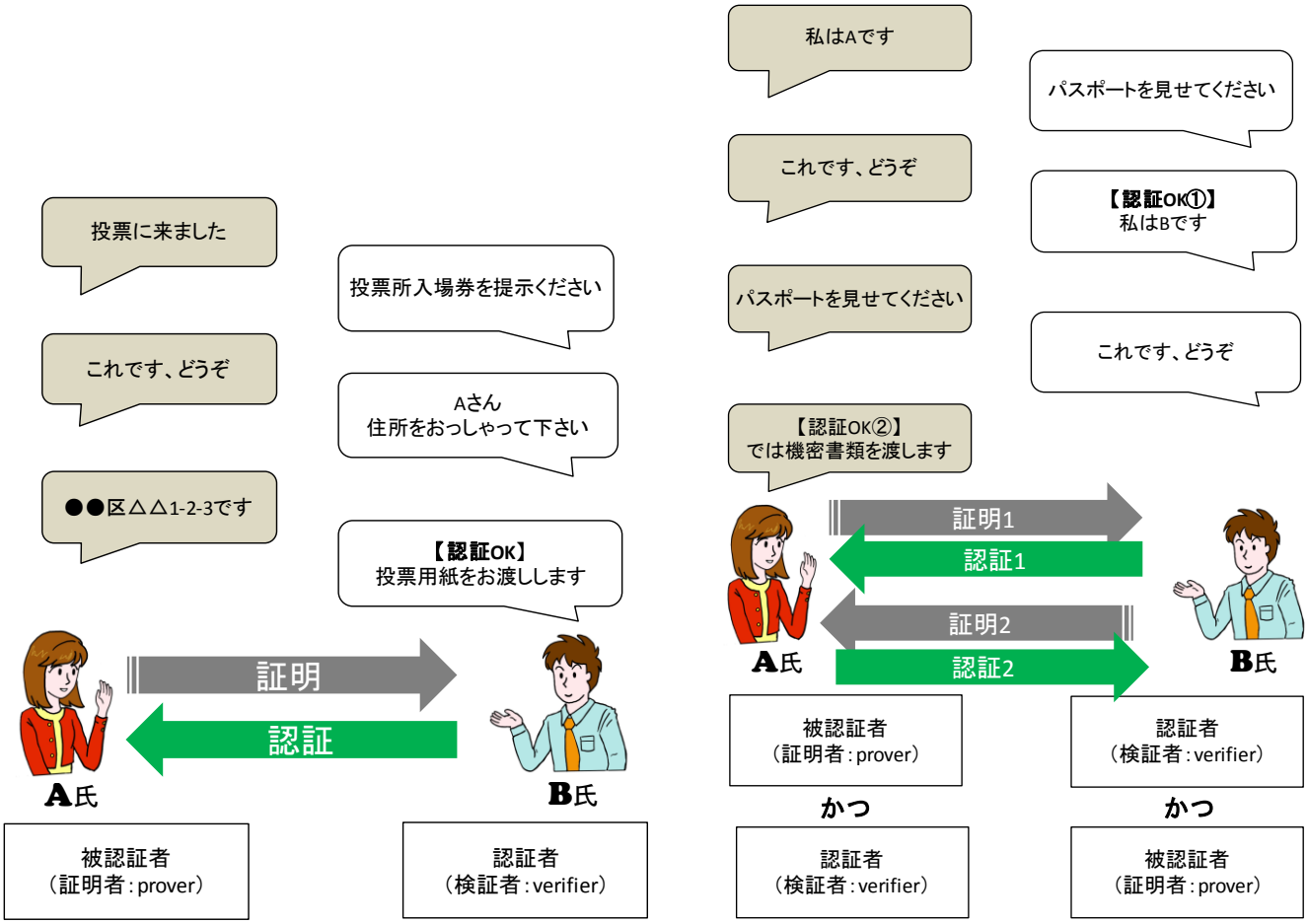

図４　片側認証と相互認証の例

コラム：　本人認証には、属性認証（ゆるい認証）も存在する。本ガイドラインではこれらも本人認証の一部としてスコープ範囲として考える。 属性認証とは、A 氏が B 氏に対して、自分がある属性に適合することを証明する（個人特定まではしない）ことをいう。例えば、B 氏に対し、A 氏が成人であることを証明することなどが該当する。（この場合、B 氏に対し、A 氏であることを証明する必要はない）

(2) 本人認証を構成する機能

現代のデジタル技術を活用した「本人認証」（User Authentication＝UA）は基本的に、以下の 3 つの機能によって構成され、実行される。

本人認証（UA） ＝ ①本人確認（IV） ＋ ②利用者識別（UI） ＋ ③利用者検証（UV）

「本人確認」（Identity Verification＝IV）、「利用者識別」（User Identification＝UI）、「利用者検証」（User Verification＝UV）

実行された結果、本人認証（UA）の成功（または不成功）を以て、サービス利用が許可（または不許可）となる。

ただし、本人認証（UA）は運用により、利用者識別（UI）のみ、もしくは利用者識別（UI）＋利用者検証（UV）を実施することにより、本人確認（IV）を代替することが可能である。この場合の本人認証（UA）は、事業者が利用者を「本人であることに間違いないか」の確認行為は実施しないが、事前に登録した利用者マスター情報（事業者が保有する資格証明情報）との照合により本人確認（IV）が行われることになる。

なお、サービス利用の許可は「認可(Authorization)」と呼ばれ、「本人認証」とは別のプロセスとなる。「認可」は、サービス提供範囲が細かくレベル分けされているような場合は、利用者のサービス利用許可レベル（アクセス権限）を特定し、サービスへのアクセスを許可する。

理解を助けるため、決済サービスを事例として、本人認証に使用される各書類とその名称を図 5 に示す。

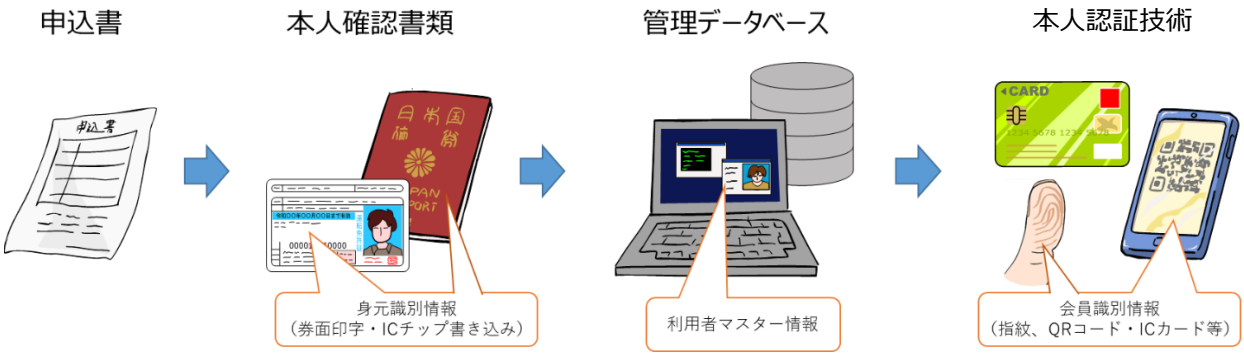

図 5　本人認証に使用される各書類と名称（決済サービスの例）

(3) 本人認証の機能分担

IV、UI、UV の果たす機能や役割の全体像は図 6 の通り。以下ではそれぞれの機能分担について、解説する。

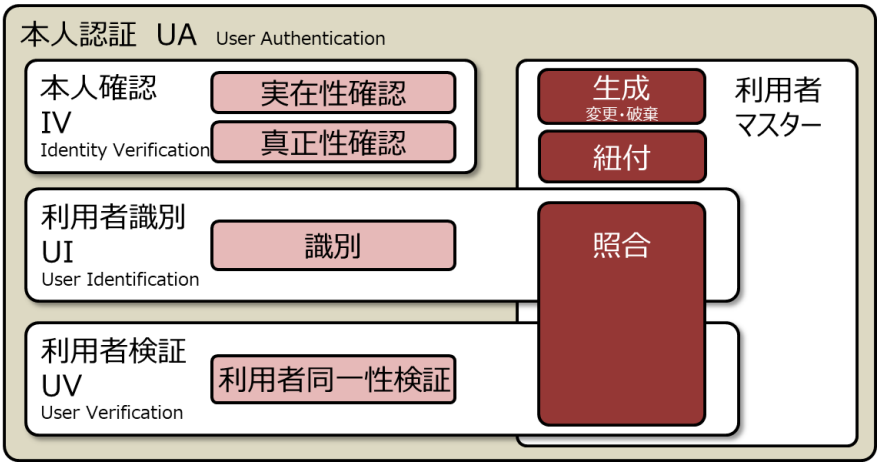

図 6 本人認証の全体

① 本人確認（IV：Identity Verification）

本人確認は、事業者が利用者を、「本人であることに間違いがないか」確認する行為である。

事業者は、本人確認書類の提示などを通じて利用者の身元識別情報を参照し、利用者の「実在性」と「真正性」を確認した後、届出内容にしたがって、利用者識別情報の生成と利用者との紐付けを行い、利用者マスター情報として登録する。更に、利用者検証情報を暗号化や改ざん防止等のセキュアな対策を講じて利用者マスターへ登録する。

【IC クレジットカードの例】

- 利用者が書面やインターネットなどを通じて申告した本人確認情報と、添付された運転免許証コピーなどの本人確認書類を照合し、個人の特定や、個人の実在性確認などを行う。
- 事業者は、利用者を一意に特定するための会員番号等の利用者識別情報を唯一無二の固有データとして生成し、利用者から申請の暗証番号を利用者検証情報として、IC クレジットカード（IC チップ）に書き込み、IC クレジットカードを発行する。
- 事業者は、IC チップ内、および、IC クレジットカード券面に利用者の氏名等を記録することにより、利用者マスター情報と利用者の紐付けを行う。

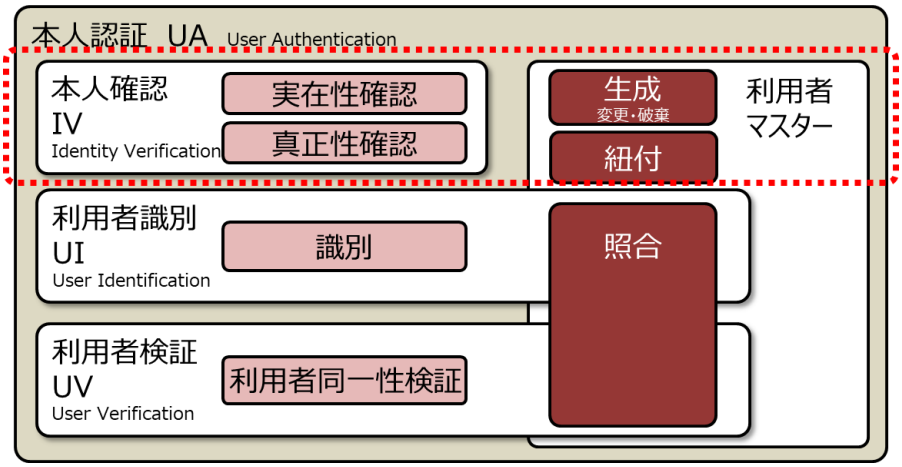

図７ 本人確認＆登録（変更･破棄含む）

② 利用者識別（UI：User Identification）

利用者識別は、事業者が利用者を「特定する」行為である。

事業者は、利用者が IC カードなどの認証技術を用いて提示した利用者識別情報をシステム上で照合し、利用者の特定と、資格の有効性を確認する。

【IC クレジットカードの例】

・ 利用者が IC クレジットカードを決済端末に挿入あるいはタッチすることにより、会員識別情報が決済端末側に伝達され、IC クレジットカードと決済端末がお互いに真正性を確認し合う。照合結果が OK（一致）であれば、次のステップに移る。※PIN レス取引などでは、そのまま金銭取引が可能になる。

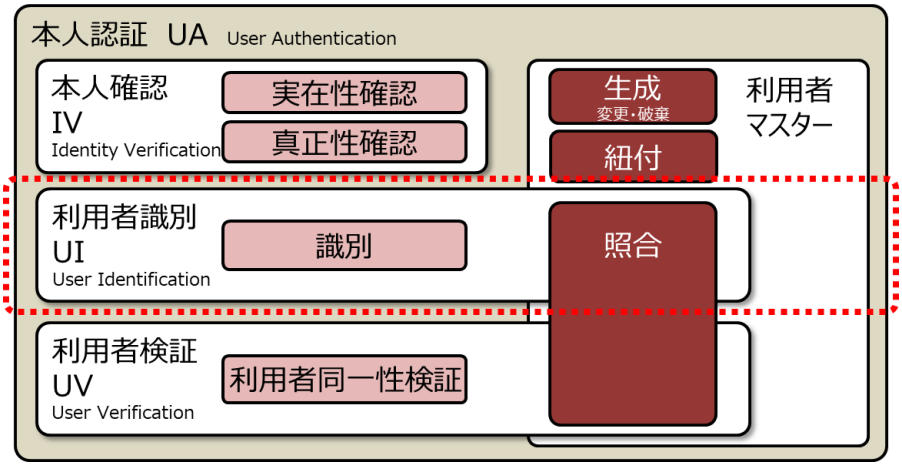

図８ 利用者識別

③ 利用者検証（UV：User Verification）

利用者検証は、事業者が利用者の「同一性を検証する」行為である。

事業者は、利用者が提示した利用者検証情報と利用者マスター情報との照合（一致）を実施し、同一性を確認する。

【IC クレジットカードの例】

・ 利用者自身があらかじめ指定しておいた暗証番号（日本では数字４桁を使用）を、決済端末の入力装置から打ち込み、提示した IC クレジットカード（会員識別情報を含む）を利用するための正当な権利を持った利用者であるかを確認する。照合結果が OK（一致）であれば、その後の金銭取引が可能になる。

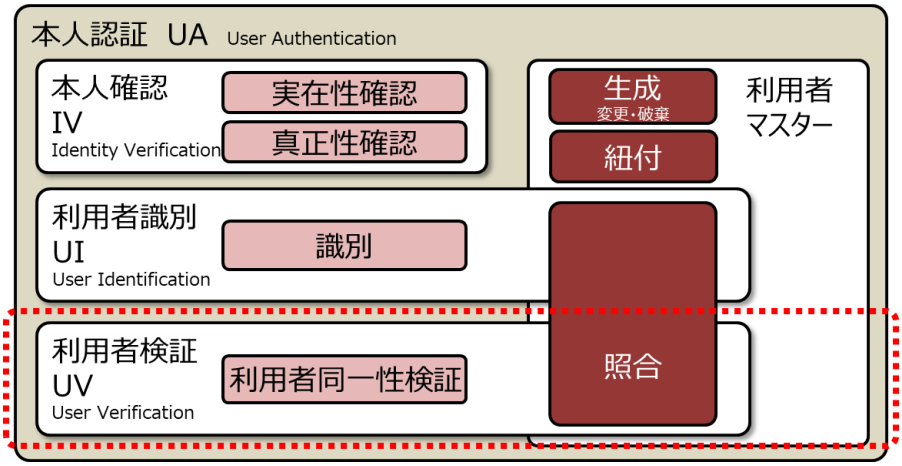

図９　利用者検証

本人認証を必要とする代表的なサービス事例について、そのそれぞれが「IV＋UI＋UV」をどのように実施しているか、表１に示す。

表 1 サービスにおける IV＋UI＋UV の実施例

	サービス登録		サービス利用(本人認証)	
	本人確認(IV)	登録	利用者識別(UI)	利用者検証(UV)
映画のチケット	なし	チケットの発行	チケットの提示(所有)確認	なし
利用者本人限定のコンサートチケット	・Webサイトなどから指名、住所などの利用者個人情報を入力 ・本人確認書類による実在性及び真正性確認	・利用者マスター情報の登録 ・利用者識別情報付きチケットの発行	・利用者識別情報付きチケットによる確認	・本人確認書類(或いは利用者マスター情報)の照合
プリペイドカードでの支払い	― (しないものが多い)	プリペイドカードの発行(カード番号の付与) 申込書でPIN登録	プリペイドカードの提示(所有)確認	PIN入力(残高照会やオンライン入金時など)
ID・パスワードでログインする会員サイト	リターンメール(Eメール等)による実在性の確認	ID・パスワードの生成・登録	IDの入力・照合	パスワードの入力・照合

コラム： 本人確認における IV と KYC の関係性

「KYC（Know Your Customer）」は銀行口座の開設などで実施される顧客本人の真正性・実在性を確認する行為であるが、その方法については法的な規制があり、確認方法に一定のルールがある。（犯罪収益移転防止法 4 条 1 項に取引時確認を行うことが義務付けられている。※資金移動業者等も含まれる（2 条 2 項）、e-KYC については、犯罪収益移転防止法施行規則 6 条 1 項 1 号ホ～ト（2）に確認方法が追加されている）

これに対し、本ガイドラインが定義する「IV（Identity Verification）」は本人の真正性・実在性が確認する行為そのものを指し、その手段は問わない（必ずしも KYC を実行しなくてもよい）。

(4) 利用者登録とサービス利用の関係

サービス利用時の「本人確認」を確実・安定的・短時間・低コストで行うために、継続的に利用するサービスは、利用者登録の後、サービスを利用する形態を取ることが多い。

例えば、クレジットカード新規入会等の利用者登録では、「本人確認」を経て、「利用者識別情報の生成・登録」と「利用者検証情報の生成・登録」を実施する。その後、クレジットカードを使って支払いを行う等のサービスを利用する際には、「本人確認」の代替として「利用者識別」と「利用者検証」を実施する。サービスレベルによっては「利用者検証」を実施しない場合もある。

また、銀行が発行するキャッシュカードの例のように、利用が可能になるまでの手続きとして、「口座開設」、「キャッシュカード発行申請（ATM 利用者登録）」と、複数の手順（手続き）が必要になるケースがある。この場合、それぞれの手続きに関して利用者登録が必要になる。

(5) 認証のレベル

本人認証は、IV・UI・UV の各場面において導入する「認証技術」の種類や、組み合わせての併用、ID 認証に適用する回数の多寡によって、その強度（レベル）が変わる。守りたい対象の重要性や、不正被害時の深刻度が増すほどに、高い強度が求められる。その一方で、守るべき対象の内容によっては、さほどの強度は求められない場合もある。

本ガイドラインにおける「守りたい対象」とは、認証される側である被認証者が有する「各種サービスを利用する権利」（預金口座から自身のお金を引き出す権利、特定施設へ入る権利、対価の授受と引き換えに商品やサービスを受領する権利等）と定義している。

また、導入分野によっては遵守が必須となる法規制等により、認証のレベルが必然的に決定される場合がある。

認証技術の選択・採用に際して事業者が設定する認証のレベル（保証レベル）は、各種サービスを不正利用されることがないように、サービス提供側の視点で検討する必要がある。その際にはリスク評価の実施が必要になるが、そのための基準や方法については米国・国立標準技術研究所（NIST）が発行する「デジタル・アイデンティティ・ガイドライン」（NIST SP 800-63-3）や、これを基準に採用して日本政府が発行した「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」（2019 年 2 月、各府省情報化統括責任者（CIO）連絡会議決定）などが詳しいので、参照されたい。

本ガイドラインでは、リスク評価によって事業者が求める認証のレベルを算出するアプローチではなく、導入する認証技術の違いを起点とした。具体的には、先述の NIST 文書も参考にしつつ、IV・UI・UV の各場面に採用する認証技術の種類によって 5 段階のレベル分けを規定した（表 2～4）。その際の要求事項としては、認証の 3 要素である「持ち物」「記憶」・「生体」を適用した。

認証技術の種類を問わず、複数のものを組み合わせて使用することで、区分されたレベル以上の評価を得ることも出来る。但し、認証を行う経路が同じ場合は、そこを攻撃された場合はその効果を得られなくなる為、経路が異なるアプローチの検討にも留意されたい。

JICSAP
Japan ID Connect with Secure Authentication Promotional association

表２　本人確認（IV）の要求事項

保証レベル	サービス登録時の確認方法 持ち物による本人確認要求事項	例	本人確認	公的証書（コピー）	公的証書（原本）	公的証書（顔写真なし）	公的証書（顔写真付き）	公的証書記載住所居住確認
レベル0 保証なし	・本人確認は行わない	・券売機での切符現金購入	－	－	－	－	－	－
レベル1 低い保証	・何らかの手段で本人確認を行う （学生証・社員証・名刺・メールアドレス 等） ・公的証書は求めない	・展示会の入場登録の際に名刺を渡す ・通学定期券購入申し込み時に学生証を提示する	○	－	－	－	－	－
レベル2 中程度の保証	・氏名、住所、生年月日が記載された現在有効な公的証書（コピー）の提出 ・顔写真付きの公的証書は求めない	・公的証書例：健康保険証/住民票 等	○	○	－	○	－	－
レベル3 高い保証	・氏名、住所、生年月日、顔写真が記載された現在有効な公的証書（原本）の提示 ・顔写真と申込者の顔が同一人物と推察出来るかを確認	・公的証書例：マイナンバーカード/パスポート/運転免許証 等 ・査証申込時のパスポート提示	○	×	○	×	○	－
レベル4 最高位の保証	レベル3に加え ・公的証書記載住所への居住事実の確認	・クレジットカード、キャッシュカード受取の際の本人限定受取郵便	○	×	○	×	○	○

【凡例】○可　×不可　－不要

（出典）NIST「デジタル・アイデンティティ・ガイドライン」（NIST SP 800-63-3）などを参考に、本書にて作成

表３　利用者識別（UI）の要求事項

保証レベル	利用アイテム（例）			要求事項	特記
	持ち物 媒体に 記録されたID	記憶 利用者が 記憶したID	生体 利用者の 生体情報を 紐づけたID		
レベル0 保証なし	適用不可	適用不可	適用不可	なし	本人認証には利用者識別が必須
レベル1 低い保証	静的QRコード	電話番号 メールアドレス	適用不可	何らかの手段で利用者識別を行う	レベル固有の要求事項はない
レベル2 中程度の保証	動的QRコード	適用不可	顔認証・指紋認証	IDの偽造・改竄は限定的	
レベル3 高い保証	ICカード	適用不可	虹彩認証・静脈認証	IDの偽造・改竄は困難	
レベル4 最高位の保証	CC認証取得ICカード	適用不可	現時点で該当なし	IDの偽造・改竄は現実的に不可能	

（出典）NIST「デジタル・アイデンティティ・ガイドライン」（NIST SP 800-63-3）などを参考に、本書にて作成

表４ 利用者検証（UV）の要求事項

保証レベル	利用アイテム（例）			要求事項	特記
	持ち物 所有しているから 正当	**記憶** 憶えているから 正当	**生体** 閾値を越えたから 正当		
レベル0 保証なし	利用者検証は 行わない	利用者検証は 行わない	利用者検証は 行わない	なし	
レベル1 低い保証	静的QRコード	4桁の暗証番号	人による目視確認	何らかの手段で利用者検証を行う	レベル固有の要求事項 はない
レベル2 中程度の保証	動的QRコード	大小英文字、数字、 記号を組み合わせた 8文字以上の パスワード	顔認証・指紋認証	持ち物: 媒体の偽造・改竄は限定的 記憶: 他人による推測は現実的に不可能 生体: 成りすましは限定的	
レベル3 高い保証	ICカード	適用不可	虹彩認証・静脈認証	持ち物: 媒体の偽造・改竄は困難 生体: 成りすましは困難	
レベル4 最高位の保証	CC認証取得ICカード	適用不可	複数生体認証組合せ	持ち物: 媒体の偽造・改竄は現実的に不可能 生体: 成りすましは現実的に不可能	

（出典）NIST「デジタル・アイデンティティ・ガイドライン」（NIST SP 800-63-3）などを参考に、本書にて作成

(6) 認証とリスク・利便性

リスク（なりすまし、転売など）を評価のうえ認証レベルを決定するが、導入する認証手段は利便性も考慮する必要がある。本人認証を厳格化しすぎると利便性を損なうため、リスクと利便性をバランスして決定する。

【コンサート入場時の例】

認証レベルと利便性について、コンサート入場時の本人認証を導入する事例として考えてみる。

昨今コンサートチケットの販売において、人気アーティストのコンサートチケット等入手が困難なチケットが高額な値段で転売されるケースが目立っている。運営側は消費者が適正な値段でこれらのチケットが入手できるようにするためと、反社会勢力等の資金源にならないようにチケットの不正転売防止に取り組んでいる。

その方法として、コンサート会場への入場時にチケットを購入した方の本人認証をおこない、本人でないとチケットを利用できなくする仕組みが採用されている。

まずチケットを購入する際、氏名、住所等個人を特定する情報を登録する。 チケットには氏名・住所が記載され、購入者のもとへ届けられる。 コンサート入場時にチケット（個人情報を明記）を提示するとともに、身分証明書を提示し、個人情報（氏名・住所）を突き合わせ、さらに顔写真とチケットを持参した人物の顔を照合して、購入した本人かを確認したうえで入場を許可する。（図１０）

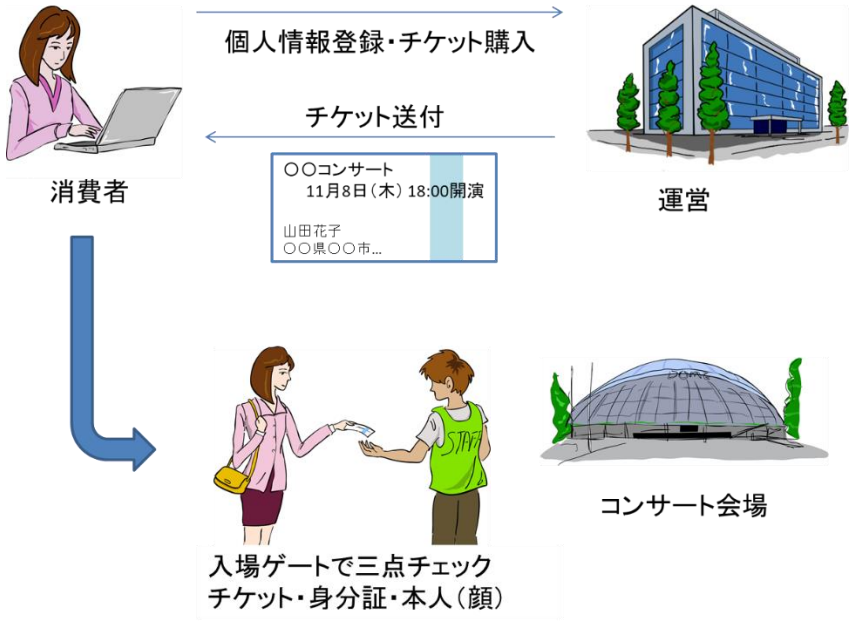

図１０　　コンサート入場時の本人認証（例）

このような仕組みとすることで第三者にチケットを転売することは困難になる。 ただし、チケットの転売を防ぐことはできるが、一人ひとり確認していくため、チケットだけを確認して入場する場合に比べて時間がかかり、入場に際し長蛇の列になってしまう場合がある。これは購入者にとっては利便性（スムーズに入場できるか）という点でマイナスになってしまう。また、本人にしか使えないチケットは、突如都合によりコンサートへ行けなくなってしまった購入者が知人等へ譲る、といったことも行えなくなり、こうした利便性も損なう。

このように認証レベル（チケットに本人認証を導入する）と利便性（入場のスムーズさ、他人への譲渡）をどうバランスするか、検討して導入を決定する必要がある。

３．　認証技術

(1)　認証技術の分類

本人認証に用いられる認証技術に関し、本ガイドラインでは「持ち物」・「記憶」・「生体」の 3 要素に分類する。それらは UI・UV のために単独で使用、もしくは複数を併用することができる。また、「持ち物」・「記憶」・「生体」のそれぞれのカテゴリにおいて、さまざまな技術や手法が存在する。

そうした中で、本人認証のために認証技術を導入しようとする事業者は、安全性のレベル、利便性、導入コストなどを勘案し、導入場面に適した認証技術を選択して利用する必要がある。

①　持ち物

「持ち物」は利用者識別（UI）と利用者検証（UV）の双方でよく活用される。

・「持ち物」による利用者識別（UI）とは「持ち物を使ってユーザーを特定すること」を示す。
　例）クレジットカードを提示することでクレジットカードの所有者であることの確認、さらにカード記載の会員番号の会員であることを確認する、など
・「持ち物」による利用者検証（UV）とは「持ち物を使って利用者であることを確認（検証）すること」を示す。
　例）運転免許証を提示し免許証を提示した人物が誰であるのか確認する、など

脅威：　チケットやクレジットカード、免許証の偽造や複製（コピー）、などがある。持ち物の偽造や改ざんなど、なりすましの難易度は持ち物に採用される技術によって異なる。
対策：　IC チップの採用、QR コードの動的生成、ホログラムの採用による偽造、改竄の困難化や多段階/多要素認証の採用による他の方法でのなりすまし抑止など
適用例：チケット、運転免許証、パスポート、クレジットカード、キャッシュカード、保険証、スマホアプリ、など

②　記憶

「記憶」は利用者識別（UI）と利用者検証（UV）の双方でよく活用される。

・「記憶」による利用者識別（UI）とは「記憶による情報を元にユーザーを特定すること」を示す。
　例）インターネット上の各種サービスにおける ID（アカウント）としてメールアドレスを登録する場合、など
　※メールアドレスは「利用者識別（UI）」に利用されるのみで、「利用者検証（UV）」には別の情報（パスワード等）が活用される場合などを指す。
・「記憶」による利用者検証（UV）とは「記憶による情報を元にユーザーを確認（検証）すること」を示す。
　例）暗証番号やパスワード、秘密の質問（あなたのお母さんの旧姓は？）、など

脅威：　リスト攻撃、ブルートフォースアタック（総当り攻撃）などがある。記憶の種類（生年月日など）によっては、推測されやすい可能性がある。また記憶に関する認証情報の漏洩時には第三者が当該情報を入力するだけでなりますしが可能となるため、漏洩後そのままでの耐性は低い。
対策：　一定回数の入力誤りによるアカウントロック、他人に推測されやすいパスワード設定を不可とする、など
適用例：暗証番号やパスワード、秘密の質問（あなたのお母さんの旧姓は？）、など

③　生体

昨今、持ち物や記憶の代わりに「生体」の情報を利用者識別（UI）や利用者検証（UV）に活用するケースが増加している。

・「生体」による利用者識別（UI）とは「生体情報を元に利用者を特定すること」を示す。
　例）顔をカメラで撮影することによりカメラの前のユーザーが誰であるか特定する、など
・「生体」による利用者検証（UV）とは「生体情報を元に利用者が本人であることを確認（検証）すること」を示す。
　例）銀行 ATM を利用する際、静脈で照合する、など

脅威：　他人受入や本人拒否、データ漏洩・改ざん、偽造生体（指紋シリコン、顔写真など）がある。生体の偽造、改ざん、なりすましは一般的に難しいが、難易度は採用される生体の部位（モダリティ）や技術によって異なる。

対策：　他人受入/本人拒否の閾値を調整する、ライブネス検証（生体検知）、多段階/多要素認証の採用による他の方法でのなりすまし抑止　など

適用例：顔認証、指紋認証、指／手のひら静脈認証、虹彩認証　など

(2) 多要素認証

前述のように、「持ち物」・「記憶」・「生体」の 3 要素に分類される認証技術は、単独で使用する以外に、複数の技術を組み合わせて利用することができる。当然ながら、単独で行う認証よりも、複数を組み合わせて実行される認証のほうが、より高度なセキュリティを実現できる。

このように複数の認証技術を組み合わせて利用する場合、それらが「持ち物」・「記憶」・「生体」のうち同一区分に属する認証技術を複数回組み合わせることを「多段階認証」、区分の異なる認証技術を複数回組み合わせることを「多要素認証」と呼ぶ。

ただし、その際の留意点として、人間の身体的特徴に由来する生体情報は基本的に秘匿できない（外界に露出している）ことから、3 要素のうちの「生体」だけは、単独で使用するべきでなく、多要素認証の一部として使用することを推奨しているガイドラインもある（NIST「デジタル・アイデンティティ・ガイドライン」SP 800-63B）。

(3) 途上認証

2 章の（3）「本人認証の機能分担」で見てきたように、本人認証（UA）を実際に運用する場面では、「②利用者識別（UI）」のみ、もしくは「②利用者識別（UI）」と「③利用者検証（UV）」を用いることで、「①本人確認（IV）」を代替（省略）するケースが多い。

【再掲】

本人認証（UA）　＝　①本人確認（IV）　＋　②利用者識別（UI）　＋　③利用者検証（UV）

しかし、近年の巧妙な不正手口では、この「①本人確認（IV）」を代替（省略）する運用の隙を突いて、正しい権利を有する本人になりすました他者が「②利用者識別（UI）」を提示、もしくは「②利用者識別（UI）」＋「③利用者検証（UV）」を行使する事例も増加している。

これらの不正リスク対策としては、「②利用者識別（UI）」の提示、もしくは「②利用者識別（UI）」＋「③利用者検証（UV）」の行使を、異なる方法で（多要素）、複数回組み合わせるなどの措置が有効である。
とりわけ、一連の「本人認証（UA）」フローにおいて、従来は最初の一度だけ行われることの多かった「①本人確認（IV）」を、以降の取引においても、適宜、定期的に実施することによって、これらの不正リスクを大幅に低減できる。

本人認証においても、クレジットカード会社の「審査」や「与信」の運用と同様に、「初期」だけでなく、「途上」を定期的に点検することの重要性が高まっている。

(4) 認証技術の一覧

本人認証に利用される代表的な認証技術について、本ガイドラインでは「①持ち物」、「②記憶」、「③生体」に分けて記載する。

① 「持ち物による認証」に使われる技術

表 5 QR コード

技術名	QR コード
技術の解説	2 次元コードの一種。 白と黒で表現される点（セルとよぶ）でデータを表現する。 格納できる情報量の上限は 2,953 バイト(8bit バイトモード、誤り訂正レベル L、バージョン 40)。 ISO/IEC 18004 として国際標準規格に制定されている。
技術の使い方	【ディスプレイ：動的 QR コード】 本人確認のためのデータを QR コード化して、ディスプレイ上に表示（ワンタイム）し、これを対面の QR コードリーダで読み取ってデータを確認し、認証する。一定時間が経過すると表示している QR コードを更新する。
	【印刷媒体：静的 QR コード】 本人確認のためのデータを QR コード化して、紙やプラスチックカードなどに表示し、これを対面の QR コードリーダで読み取ってデータを確認し、認証する。 動的 QR コード（ワンタイム式）と比較してコピーされやすいリスクがある。 このため、複製防止の印刷技術と組み合わせて利用する場合もある。
技術の浸透	広告宣伝用途では WEB サイト誘導に広く使われている。 認証用途ではビルの入館、コンサートチケットに QR コードが印字されている。中国では決済用途で QR コードが浸透しており、利用者は 7 割に達する状況。
類似技術	【磁気カード・IC カード】 認証用途ではよく磁気カード・IC カードと QR コードが比較される。 磁気カード・IC カードの場合、カードという物理的な媒体が必要。携帯電話等に IC チップとして内蔵しているものもある。 QR コードと異なる点は、データの書き換えが可能である点。

表 6 IC カード

技術名	IC カード
技術の解説	データの記憶や演算処理機能を持つ集積回路 （IC） を組み込んだカードのこと。 IC チップ自身に耐タンパー性があり、変造や解析が難しいのでセキュリティ機能に優れている。 通信方式は、接触型と非接触型があり、それぞれ幾つかの方式が標準化・規格化されている。
技術の使い方	IC カード用のリーダを使用して、IC カード内のデータを確認し、認証する。
技術の浸透	金融・決済の分野で広く使われている。 また、身分証明書としても公的・民間ともに広く使用されている。

類似技術	－

表 7 ワンタイムパスワード

技術名	ワンタイムパスワード（OTP）
技術の解説	自動的に生成される認証用の英数字コードで、 リソースにアクセスする際に、一度限りの認証にのみ有効な値。
技術の使い方	キーホルダー型、カード型、携帯電話のアプリや、SMS、メール等で、一度限り有効なパスワードを生成し、利用者に入力させることで認証する。
技術の浸透	近年では、オンラインバンキング等や金融関連のログインやバンキング処理を行なう際に本人確認のために使用され始めている。 また、クラウドサービス等にログイン時の本人確認のための多要素認証用途等にも採用されている。
類似技術	【IC カード】 多要素認証用途では PKI 対応 IC カードと OTP が比較される。 IC カードの場合、リーダライタ等が必要となり、端末毎に相性があるが、OTP の場合、特に他に用意するデバイスがない。 【パターン認証】 毎回、入力値が違う点で比較される。OTP との大きな差として、パターン認証は記憶しているパスワードを記憶しているパターンで同じ『記憶情報』の認証に対し、OTP の場合生成するデバイスを所有する事を担保としている『所有情報』の認証である。
その他	SMS を用いた OTP は、NIST 等のガイドラインから非推奨となっている

表 8 HCE

技術名	HCE（Host Card Emulation）
技術の解説	プラスチックカードの代替としてスマートフォンを利用し、NFC 通信を行う技術のひとつ。HCE はデータを SE（Secure Element）などの特別なハードウェアを使わず、スマートフォンの不揮発メモリ上に格納する。
技術の使い方	携帯電話本体メモリに本人確認のためのデータを格納後、NFC リーダ／ライターと通信を行うことにより、デバイスや本人確認の認証を行う。
技術の浸透	グローバルでは、カード決済などで広く利用されている。欧米などで銀行の Wallet アプリ、交通系のモバイルチケットなどにおいて、HCE が採用されるケースが増えている。また Google Pay や Samsung Pay でも HCE の技術が採用されている。
類似技術	【SE（Secure Element）】 SE は耐タンパー性を有する半導体製品であり、携帯電話の UIM などに搭載されている。そのため、高いセキュリティを要求するクレジットカードデータの格納などで利用されている。それに対して HCE は SE が不要であることにより、コスト面で優れているものの、金融や決済用途で利用

	するためには、SE と同様の機能をクラウド上に置くなどのセキュリティ対策を講じる必要がある。
備考	スマートフォン（モバイルデバイス）の耐タンパー性のない領域にデータを書き込む場合、セキュアではないという前提を置き設計すべきである。そのため、ID/Password、カード番号等をそのままアプリケーションに保有せず、他の符号に置き換える技術（トークナイゼーション）や、暗号鍵の技術を利用して、万が一、情報が漏洩しても被害が甚大にならないように工夫しなければならない。 HCE を活用し、本人に紐づく情報（ID 情報、クレジットカード情報等）を新規に登録する場合、モバイルデバイスにデータを格納（プロビジョニング）する必要があると考えられるが、その際には認証技術の 3 要素である「持ち物」「記憶」「生体」のいずれか、もしくはその組み合わせにより認証することが求められる。 一方、利用者検証（UV）にはスマートフォンの保有者認証機能を活用するなど、各取引においての本人確認を行うなどの対応が求められるケースが多い。

表 9 銀行口座照合

技術名	銀行口座照合
技術の解説	アカウントに銀行口座情報を登録時（＝口座振替登録時）に、当該利用者（預金者）が口座開設時に本人確認済みか登録情報との照合とともに確認する方法。＝本人確認方法。「犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）」第４条第１項に規定する取引時確認（「犯罪による収益の移転防止に関する法律施行規則」第１３条第１項第１号及び「犯罪による収益の移転防止に関する法律施行規則及び疑わしい取引の届出における情報通信の技術の利用に関する規則の一部を改正する命令（平成 24 年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第１号）」附則第６条に規定する方法による。）の業務を銀行に委託しているということ。
技術の使い方	－
技術の浸透	金融・決済の分野で広く使われている。
類似技術	－

② 「記憶による認証」に使われる技術

表 10 PIN

技術名	PIN（PIN 認証技術）
技術の解説	クレジット取引にて、本人確認のための手段の一種。 複数の数字列からなるデータを用いて本人確認を行う。 PIN の取り扱いに関しては、ISO 9564 に従うことが推奨されている。 パスワード（PIN）は複数の数字列からなるデータであり、ISO9564 では 4～12 桁と定義されている。 一般的に日本では、4 桁とされている。
技術の使い方	本人確認のための PIN を入力し、 カードの IC チップ内に保存された PIN と照合し認証（オフライン PIN 認証）する、もしくは、オンラインネットワークを経由してカード会社のシステム上で照合し認証（オンライン PIN 認証）する。第 3 者が類推しにくい文字列を設定させる必要がある。（誕生日や電話番号を設定することは NG とする等） ・パスワードロック（PIN ロック） : あるクレジットカードで一定回数連続 PIN を誤入力すると、そのクレジットカードでの取引が制限される（使用不可となる） PIN の誤入力回数は時間の経過でリセットされるものではなく、正しい PIN が入力され照合された段階でリセットされる。 例) PIN 誤入力が 3 回で PIN ロックされる場合 ある取引①にて PIN を 2 回連続で誤入力する。正しい PIN がわからなかったためクレジット取引をやめ現金で取引を行う。 その後、取引②にて PIN を 1 回誤入力する。取引①から数えて連続で 3 回 PIN を誤入力したため、PIN ロックされる。 ※ 取引②で正しい PIN を入力した場合、PIN の誤入力回数はリセットされる。 PIN ロック解除のためには、カード発行会社に連絡する必要がある。
技術の浸透	クレジット取引での本人確認の手段として、一般的に使用されている。 PIN 入力専用機器を使用せず、スマートフォンやタブレット端末を経由し PIN 入力を実施する手段が注目されている。
類似技術	【生体認証】 本人確認のための手段として、生体認証があげられる。生体認証の場合、数字を記憶する必要が無いが、認証対象によっては読み取りの精度に課題がある。

表 11 秘密の質問

技術名	秘密の質問
技術の解説	ある特定の質問に対して、本人しか知りえない答えを登録し、それと照合することで本人かどうか確認する認証技術
技術の使い方	「出身地は？」「母親の旧姓は？」という人により答えが異なる質問に対して、「名古屋」「鈴木」など、利用者が決めた回答を登録しておき、認証時に登録した回答が入力されたかどうかで登録した利用者か判断する。 PIN を忘れて認証できないような場合、これを補完するものとして使われることが多い
技術の浸透	様々なインターネットサービスで広く使われるようになっている。
類似技術	PIN、パスワード、パスフレーズ

③ 「生体による認証」に使われる技術

表 12 指紋認証

技術名	指紋認証
技術の解説	生体認証の一種。指紋の形が人によって異なることを利用し、本人認証を行う。
技術の使い方	あらかじめ、手の指の指紋を登録しておき、認証が必要な際に登録データと照合を行い、その類似度により本人かどうかの判定を行う。登録データは最大で 10 指分となる。
技術の浸透	指紋照合は犯罪捜査などでも使用されており、指紋認証は生体認証の中では比較的古くから普及。センサーが小型・低価格なため、昨今では、 スマートフォンやタブレットなどに内蔵されており、パーソナルデバイス を中心に幅広く利用されている。
類似技術	生体認証（バイオメトリクス認証）として、他に虹彩、静脈、顔、声紋等の方式がある。

表 13　静脈認証

技術名	静脈認証
技術の解説	生体認証の一種。静脈の形が人によって異なることを利用し、本人認証を行う。主な例として、指静脈認証、手のひら静脈認証、手の甲静脈認証が存在する。
技術の使い方	あらかじめ、手のひらや指、手の甲の静脈を登録しておき、認証が必要な際に登録データと照合を行い、その類似度により本人かどうかの判定を行う。使用する部位によって登録できるデータ数が異なる。
技術の浸透	普及当初は銀行 ATM などに限られていたが、その後入退室装置や PC ログオン認証などの企業セキュリティの分野にも拡大し、図書館の本の貸出しや、コンビニの決済などカードレス用途にも適用されている。
類似技術	【指紋認証】 読み取りセンサーが小型で比較的安価なため、携帯電話、スマートフォンなどの個人端末に利用される。静脈認証と比較すると認証精度が低い。 【顔認証】 認証精度は静脈認証に劣るが、携帯電話、スマートフォン、PC に搭載されているカメラを利用した認証が可能。

表 14　顔認証

技術名	顔認証
技術の解説	生体認証の一種。顔の特徴点（目、鼻、口端など）の位置や特徴点間の距離が人によって異なることを利用し、本人認証を行う。
技術の使い方	あらかじめデータベースに顔画像を保管しておき、認証が必要な際に登録データと特徴点データの照合を行う。経年変化の影響を受けにくい特徴を選択することで認証精度が向上する。
技術の浸透	顔照合はカメラ以外の特別なハードウェアを必要としないため、幅広く利用されている。映像監視システムとして空港警備、スタジアムやショッピングモール、駐車場など大規模集客施設のセキュリティ等の用途や、アクセスコントロール、犯罪捜査、サービス向上目的などで利用される。2017 年 10 月 18 日から、羽田空港の上陸（帰国）審査場で顔認証ゲートの運用が開始された。また、スマートフォンのログインや本人認証機能として利用され、スマートフォンでの金融取引の認証手段としても代替されている。 顔認証は撮影画像から顔を見つける「顔検出」と、データベース画像と比較し同一人物かを判定する「顔照合」に分かれる。顔認識は、撮影画像から「顔検出」を行い、「年齢」「性別」「表情」などの様々な属性を特定する。顔認証、顔認識はその目的によって用語が使い分けられることが多い。
類似技術	バイオメトリクス認証として虹彩、指紋、静脈、声紋等の方式がある。

(5) 認証の実装方法

以下は認証技術について、本人認証の場面ではどのように実装しているかを紹介する。

① QR コード決済における認証

商品を購入して支払する場面において、認証に QR コードを媒体として利用する場合がある。それら QR コード決済における認証の方式には 2 種類が存在し、以下、それぞれについて説明する。

・Consumer Presented Mode（消費者側提示モード）

消費者が商品の代金を支払う際に、携帯端末の画面に QR コードを表示して店舗側の QR コードリーダにかざして（読み取らせて）決済する。 表示される QR コードは消費者の ID 情報であり、クレジットカードを提示するのと同等である。

ただし、クレジットカードに比較して、QR コードは簡単に複製が可能である。（画面のスクリーンショットや画面をカメラで写真撮影するだけでも複製できる）このため、複製してもつかえないようなセキュリティ対策が必須となる。

[動的 QR コード]

上記のセキュリティ対応のため、QR コード決済でよく使われる手法としては、QR コード内に有効期限の情報を付加し、QR コードを読み取った際に QR コードが有効期限内にあるかをチェックする「動的 QR コード」がある。

この有効期限が短ければ、複製した QR コードを他で使われる前に有効期限が切れるため、複製された QR コードの不正利用を防止できる。

また QR コードは ISO で仕様が公開されており誰でも作成・読取が可能な技術であるため、QR コード内に有効期限のようなセキュリティ情報を格納する場合は、必ず暗号化などの偽造・改ざんを防ぐ処置が必要となる。

CPM 方式を利用する場合、店舗側に QR コードリーダが必要となる。POS に QR コードリーダを接続するのは投資が必要であるため、小規模な店舗では導入の障害になる。最近では POS の代わりにタブレットやスマートフォンで QR コード決済を行える仕組みもあり、導入しやすい状況になってきている。

消費者が QR コードを提示する方式はカードを提示するのと感覚的に同じであり、受け入れやすい仕組みである。

・Merchant Presented Mode（店舗側提示モード）

商品を購入して決済する場面において店側が QR コードを提示し、消費者が携帯端末で QR コードを読み取って決済する。店が掲示する QR コードは、請求書に相当するデータが含まれている場合と、店側の ID に相当する情報が含まれている場合の大きく 2 つの内容となっている。

読み取った後の支払い確認（払うという意思確認は本人認証が前提で成り立つ）を行う。

請求書が含まれた QR コードを表示する場合は店舗側に表示機器が必要になるが、とにかく画面があればよいため、導入しやすい仕組みである。表示される QR コードは請求書であるため消費者側が不正行為をしにくい仕組みである。

一方、店舗が ID を掲示する方式は消費者が QR コードを読み取った後に決済額を端末に入力して決済する方式となっている。

[静的 QR コード]

QR コードは ID で固定となっており、QR コードを印刷したものを提示して利用する。上記の「動的 QR コード」に対して、こちらは「静的 QR コード」と呼ばれることがある。 静的 QR コードによる QR コード決済の場合一度だけ QR コードを印刷すれば利用可能であるため、小店舗や屋台などでも導入が容易で、特に中国で広がっている。

静的 QR コードは、導入が簡単である分、セキュリティは脆弱な面があり、掲示している QR コード（ID）を張り替えられ代金を搾取される詐欺事件なども発生している。

決済時に QR コードを読み取る、というのは消費者にとっては馴染みのない行動であり、決済時にやり方が分からず手間取る場合があり、消費者にたいする利用方法の提示などのケアが必要である。

② IC カード決済取引における利用者検証

IC チップを搭載したクレジットカード（以降、IC カード）にて、支払いする場面において、利用者検証として PIN 認証が必要となることがある。

PIN 認証の方式には 2 種類が存在し、以下、それぞれについて説明する。

・オフライン PIN:

カードの IC チップ内にカード発行時に PIN 情報が保存されており、その PIN 情報を用いて PIN 認証を行う方式である。IC カードでの支払い時に、カード保有者が PIN 入力装置（注）を利用して数字（PIN 情報）を入力する。カード保有者が入力した PIN 情報と、IC カード内の PIN 情報とを照合し、一致した場合に利用者検証成功となる。

オフライン PIN では、オンラインネットワークを介すことなく PIN 認証が IC カードと決済端末間で完結するため、PIN 情報のネットワークからの漏洩リスクが低い。

ただし、IC チップ内に PIN 情報を持つカードを使用する必要があるため、PIN 情報の変更時にカードの再発行が必要となる。

・オンライン PIN:

カード発行会社のシステム上に登録された PIN 情報を用いて PIN 認証を行う方式である。

IC カードでの支払い時に、カード保有者が PIN 入力装置（注）を利用して数字（PIN）を入力する。

カード保有者が入力した PIN 情報と、オンラインネットワークを経由してカード会社のシステム上の PIN 情報とを照合し、一致した場合利用者検証成功となる。

オンライン PIN では、オンラインネットワークを経由して PIN 情報を照合するため、オフライン PIN と比較して、PIN 情報の漏洩リスクが高くなる。IC チップ内に PIN 情報を持たないカードの場合、PIN 情報の変更時にカード会社のシステム上の PIN 情報の変更で対応できるため、カードの再発行が不要となる。

オフライン PIN/オンライン PIN のどちらを実施するかは、EMV 仕様に従い、IC カードと決済端末機能の組み合わせにて判断される。

（注）決済カードのデータセキュリティ基準を策定する PCI SSC（PCI Security Standards Council）が定めた、PIN を入力するデバイスに関するセキュリティ基準（PCI-PTS）の認証を受けた装置。

③　生体認証におけるローカル照合とサーバ照合

生体認証では、あらかじめ本人に由来する情報をセンサー等でデータ化し、テンプレートとして登録しておき、認証時に同様に取得した情報と照合し、両者の一致度を利用して本人の同一性を判定する。一般的に、生体データ（テンプレートおよび照合用の情報）は、センサーで取得した画像などのデータをそのまま利用せず、本人性を示す特徴情報を抽出するなど、非可逆的に変換し、さらに暗号化して利用される。また、国内では改正個人情報保護法により個人識別符号と定義され、個人データの１つとして位置づけが明確化されるとともに、適切な安全管理措置を行うことが求められる。生体データ保護技術が施されている場合には、漏洩時の報告義務がないと考えられている。欧米など諸外国では、プライバシーに関する情報としてさらに慎重な取り扱いが求められる地域がある。

以下、生体データをネットワーク上に流通させない方式をローカル照合と呼び、ネットワーク上に生体データが流れる方式をサーバ照合と呼ぶ。

・ローカル照合

生体データを端末内あるいは可搬媒体に格納し、生体データをネットワーク上に流通させることなく、端末内あるいは可搬媒体内に閉じた形で認証を実施する。ISO/IEC 7816-11:2017 及び ISO/IEC 24787:2018 では IC カードでの生体認証について標準化されている。この可搬媒体は、悪意のある攻撃者から容易に生体情報を抜き出せないような仕組み（情報暗号化、耐タンパーなど）や、不正な端末や IC カードの使用を防ぐための相互チェックを行う機能が重要となる。ローカル照合を利用したサービスでは、生体データを利用者が管理することになるため、サービス事業者のリスクが少なくなるメリットがある。その一方で、サービス事業者は、可搬媒体を被認証者に配布する必要があり、コストの負担が問題となる。ローカル照合の具体例としては、銀行 ATM の認証で採用されている。

また、スマートフォンのロック解除で用いられている生体認証や、コンシューマ向けの P C・タブレットで用いられる生体認証は、ほとんどがローカル照合に分類される。例として業界団体 FIDO（Fast IDentity Online）アライアンスで標準化されている認証方式は、端末内に保持されたテンプレートを用いて端末内で生体認証を行い、PKI と同様に公開鍵暗号を用いた署名技術を利用して認証結果をサーバ側で検証するものである。オンラインサービスを利用するための本人認証技術仕様となっているが、ここでの定義においては、生体データはネットワーク上に流通しないためローカル照合に位置づけられる。

・サーバ照合

生体データをクライアント端末からサーバに送り、サーバ側で生体認証を行う方式で認証する。PC ログオンシステムや入退室システムなど、主に企業内で閉じたネットワーク環境や VPN などで接続された安全性を高めたネットワーク環境で利用される。サーバ照合においても、生体データには暗号化など適切な管理が求められる。サーバ照合は、IC カードなど可搬媒体の配布を利用したローカル照合と比較すると、初期コストの面では可搬媒体の配布が不要であり、運用コストの面ではカード忘れ、紛失・破損時の再発行が不要となるメリットがある。このようにサーバ照合によってテンプレートの集中管理を実現できるだけでなく、複数人で共用するクライアント端末に全ての利用者のテンプレートを置く必要もなくなる。とくに、このようなサーバ側に置かれた複数の生体データに対して特定した結果を利用する 1:N 認証は、ID レス認証、手ぶら認証とも呼ばれ、利便性向上の効果を得ることができる。ただし、1:N 認証では、テンプレートの数が増えるほど他人を誤って受け入れるリスクが増えるため、十分に高い認証精度を持った生体認証技術を利用することが重要となる。

コラム： FIDO(Fast IDentity Online)

FIDO は、共有の秘密（共通鍵）の対極にある「公開鍵暗号」を用いることで、共通鍵の代表例であるパスワードそのものを不要とすることをコンセプトに開発されたオンライン認証に関する仕様。「公開鍵暗号」に必須となる「秘密鍵」の保管場所には、①生体認証機能を搭載するスマートフォンなど（UAF 仕様：Universal Authentication Factor）、②パソコンに USB 接続などでつながる 2 要素認証用のセキュリティキーなど（U2F 仕様：Universal 2nd Factor）、の 2 種類がある。2018 年にはこれらの認証機能を Web ブラウザに組み込んで使いやすくした「FIDO2」の仕様が追加された。例えば UAF では、スマートフォンなどのデバイス上で生体認証を行い、認証結果だけを公開鍵によりネットワーク上に流通させるため、オンライン上の盗聴やサーバからの生体情報漏えいのリスクがなくなる。認証デバイスの保持が前提となるが、スマートフォンが普及した現在では有力な認証システムの一つといえる。

④ 3-D セキュアによる本人認証

3-D セキュアは、EC 決済利用時の本人認証サービス。EC サイトなどでの非対面での商品購入時において、EC 店舗に代わりカード発行会社がカード利用者の本人確認を実施する。

2000 年代より主に EC サイト（ブラウザ）に導入され、クレジットカード利用時の本人認証に活用されてきたサービスであり、更にセキュリティを向上させた次世代版「2.0」もリリースされている。また、この「2.0」は、スマートフォンの普及に伴い、スマートフォンアプリ上でも利用可能になっている。

参考：https://www.emvco.com/emv-technologies/3d-secure/

・本人認証方法

EC サイトで利用金額が確定しクレジットカード情報を入力すると、クレジットカード発行会社から利用者に対し、本人を確認するためのパスコードの入力を求める画面が表示され、入力された情報がクレジットカード発行会社側で確認されれば本人認証「成功」となる。

近年では、カード発行会社が独自にリスクベース認証を実施したり、入力するコード値をランダムに指定・通知するワンタイムパスワード化することにより不正利用の抑止に活用されている。

・普及状況

2019 年より順次 2.0 が開始され、利用環境が整備されていく予定。

2.0 の導入により、スマートフォンアプリや、決済用途以外での本人認証、リスクベース認証によるフリクションレスフロー（利用デバイスや加盟店、利用金額などのデータを元にカード発行会社がパスコード入力なく本人認証が完了すること）にて本人確認が完了することから EC 加盟店での不正利用抑止策として期待される認証サービスとなる。

4. 認証技術評価

システム・サービス構築時の認証レベルや運用ポリシーの策定にかかわる認証技術について、本ガイドラインの評価を記載する。

(1) 利用者評価

利用者から見た認証技術の利便性、安全性についての評価を記載する。

○持ち物による認証

【利便性】

・現在、幅広い利用シーンで用いられ、利用者が受け入れやすい（操作に慣れている）点で、利便性は上がる。
・利用シーンごとに持ち物を準備し、複数の持ち物を常時携帯する必要がある点で、利便性は下がる。
・持ち物の紛失、盗難に注意し、管理する持ち物が多くなる点で、利便性は下がる。
・動的パスワードは、専用の持ち物（ハードウェアトークンやアプリなど）が必要になる点で、利便性は下がる。

【安全性】

・持ち物に顔写真などの個人情報を含む場合は、なりすましのリスクが下がる点で、安全性は上がる。
・持ち物は紛失、盗難、個人情報漏えいによる不正利用や偽装のリスクがある点で、安全性は下がる。

○記憶による認証

【利便性】

・現在、幅広い利用シーンで用いられ、利用者が受け入れやすい（操作に慣れている）点で、利便性は上がる。
・静的パスワードは専用の持ち物が不要になる点で、利便性は上がる。
・複雑なパスワードは管理が難しくなる点で、利便性は下がる。

【安全性】

・パスワードは他人が推測できる場合、不正利用や偽装のリスクが上がる点で、安全性は下がる。
・パスワードは複雑にしたり、利用シーンごとに作成したりすることで、情報漏えい時の不正アクセスのリスクが下がる点で、安全性は上がる。
・パスワードは複数シーンで共通にする場合、情報漏えい時の不正アクセスのリスクが上がる点で、安全性は下がる。

○生体による認証

【利便性】

・現在、幅広い利用シーンで用いられ、持ち物が不要になる点で、利便性は上がる。
・定期的な情報更新（パスワード変更など）の頻度が低く、手間が少ない点で、利便性は上がる。
・認証精度に個人差がある点で、利便性は下がる。
・利用シーンごとに専用設備を使用することが多く、都度登録が必要になる点で、利便性は下がる。
・個人によっては、生体情報の登録に抵抗感を覚え、生体による認証を使用しない場合がある点で、利便性は下がる。

【安全性】

・持ち物や記憶による認証と比較して、利用者起因の情報漏えいやなりすまし等のリスクが低い点で、安全性は上がる。
・個人によっては、生体情報の登録に抵抗感を覚え、生体による認証を使用しない場合がある点で、安全性は下がる。

表 15 認証技術の利用者評価一覧

分類	認証技術の種類	利便性	安全性 等
持ち物	紙媒体（カード）	・下がる （専用の持ち物が必要）	・上がる （顔写真がある場合は、目視による確認が可能）
	紙媒体（QRコード）	・下がる （事前の印刷が必要）	・下がる （なりすましのリスクがある（持参人＝本人））
	磁気カード 接触／非接触 IC カード	・下がる （専用の持ち物が必要）	・上がる （顔写真がある場合は、目視による確認が可能）
	携帯電話／ スマートフォン	・上がる （専用の持ち物が不要）	・上がる （デバイスへの認証も必要になる）
	動的パスワード	・下がる （生成デバイス（ハードウェアトークンやアプリなど）の所持が必要）	・上がる （他の記憶による認証技術に対して、情報漏えいのリスクが少ない）
記憶	静的パスワード 秘密の質問 パターン入力	・上がる （持ち物が不要のため、利用しやすい）	・下がる （情報漏えいによる偽装、不正利用のリスクがある）
		・下がる （利用シーンごとにパスワードを作成する）	・上がる （情報漏えいによる偽装、不正利用のリスクを下げる）
生体	指紋／静脈／虹彩／ 顔／動作 など	・上がる （持ち物が不要のため、利用しやすい）	・上がる （利用者起因の情報漏えいやなりすまし等のリスクが低い）

(2) 事業者評価

事業者から見た認証技術の安全性、導入容易性、コストについての評価を以下に示す。

表 16 認証技術の事業者評価一覧

分類	手法/技術名	安全性	導入容易性	コスト	解説
持ち物	QR コード	低	易	中	QR コードを紙媒体に印刷またはスマホ画面に表示し、表示された QR コードを装置で読み取って認証する手法。QR コードはコピーが容易であり、複製防止対策が必要になる。 複製しにくくする仕組みとして動的 QR コードを用いることも可能。QR コードを読み取る装置も、スマホ、専用リーダ、カメラ（QR 読み取りソフト）など充実しており、コストに合わせた仕組みを導入しやすい。認証に必要な情報を QR コードに格納することで、オフラインでも認証が可能。
	ワンタイムパスワード	高	中	高	一度限り（ワンタイム）のパスワードを生成して認証する手法。ワンタイムで利用するため、セキュリティ性は高い。ただし利用者一人一人に対してパスワードを生成するための装置が必要になるため、導入コストは高くなる。
	IC カード	高	難	高	IC カード（媒体）で利用者を認証する手法。IC カードを偽造することは困難であるため、媒体としてのセキュリティは高い。一方で、IC カードを利用者ごとに発行し、認証する場合も専用の IC カードリーダが必要となり、IC カードの発行管理も必要なため、導入には手間がかかり、コストは高くなる。
	銀行口座情報照合	高	難	高	金融機関の登録情報を参照するため信用性とセキュリティ性は高い。
記憶	パスワード設定	低	易	低	利用者に英数字記号等を用いたパスワードを設定させる手法。同一パスワードを他サイトでも重複使用している場合の情報漏えい時になりすましログインされるリスク有り。また、フィッシング詐欺等にも弱い。仕組みとしては導入しやすい。パスワード設定ルールによって強度の強弱を調整可能で、利用者が忘れた場合も再設定可能。
	秘密の質問設定	低	易	低	特定の質問と、利用者が設定する回答を登録し、利用者に回答を提示させることで認証する手法。パスワードと同様のリスク有り。パスワードを忘れたときなどに補完するための手法として使う。仕組みとしてはパスワードとほぼ同じであり、導入は容易。
生	指紋認証	高	難	高	指紋認証機能を持つスマートフォン等の端末保有者が端末に登録済

体	(情報端末利用)				みの指紋と照合することで端末保有者であることを確認する手法。セキュリティの強度はスマホ端末機能に依存するが、他の認証方法と比べて一般的に高い。端末側で保有者認証が完了するため、仕組みとしてはコストがかからず導入可能。 国際規格の FIDO に準拠した運用が望ましい。 予めアカウントに登録したパスワードに紐付け、パスワードを直接入力しなくても端末の生体認証機能で照合を行っている。
	顔認証 (情報端末利用)	高	難	高	上記指紋認証と同様に、顔認証機能を持つスマートフォン等の端末保有者が端末に登録済みの顔情報と照合することで端末保有者であることを確認する手法。セキュリティ強度が端末に依存する点も同様で、他の認証方法と比べて一般的に高い。導入する仕組みやコスト等は、端末による指紋認証と変わりはない。 国際規格の FIDO に準拠した運用が望ましい。 予めアカウントに登録したパスワードに紐付け、パスワードを直接入力しなくても端末の生体認証機能で照合を行っている。
多要素認証／多段階認証	認証番号 (電話 IVR)	中	易	中	本人確認を行うための電話による二要素認証手法。 実在する電話番号に架電（電話番号の実在確認＝アカウント登録時に設定した電話番号に架電することで本人確認を行う）し、受電すると IVR で認証番号を伝える。 パスワード忘れの際に使用。利用者本人であることを確認するための手法。※利用者の個人情報を保有していない場合に、利用者本人であることをスマホ端末、メールアドレス、電話番号の保有状況を確認することで利用者確認としている。
	メール通知確認※二要素認証	中	易	中	本人確認を行うためのメールによる二要素認証手法。 実在するメールアドレスに送信（メールアドレスの実在確認＝アカウント登録時に設定したメールアドレスに送信することで本人確認を行う）。 パスワード忘れの際に使用。 利用者本人であることを確認するための手法。※利用者の個人情報を保有していない場合に、利用者本人であることをスマホ端末、メールアドレス、電話番号の保有状況を確認することで利用者確認としている。
	身分証明書提出と郵便物到着確認による本人確認	高	難	高	身分証明書をカメラで撮り、本人情報（氏名、住所、生年月日等）を入力し、身分証明書と本人情報を有人目検で確認したうえで、更に本人住所宛に転送不要郵便を送付し、受取を確認したことで本人確認完了とする方法。 本人確認のために人手や郵送といった手間がかかるため、仕組みを導入するハードルは高い。

６．　用語定義

本ガイドラインにおける用語の定義を記す。

表 21　本ガイドラインにおける用語定義

用語	意味	対応英語
本人認証	ある人が、相手に本人であることを証明させて、検証する行為。	User Authentication (UA)
本人確認	ある人が、相手に関して、「本人であることに間違いがないか」確認する行為。氏名、住所、生年月日、性別などの情報について、運転免許証など公的書類の提示を求めることで実施する場合があり、これを「身元確認」と呼ぶ。	Identity Verification (IV)
利用者識別	ある人が、相手を「特定する」行為。	User Identification (UI)
利用者検証	ある人が、相手の「同一性を検証する」行為。	User Verification(UV)
認証	真正性（同一であること）を確認すること。 当事者の身元識別情報に関する信用を確立する行為。	Authentication
認可	利用者のサービス利用許可レベル（アクセス権限）を特定し、サービスへのアクセスを許可する行為。	Authorization
本人	その人自身。代理ではない者。 本人認証の成功を以って、利用者は本人と特定される。	Identity
利用者	サービスを利用する人。	User
事業者	利用者に対して何らかの役務を提供する者。サービス提供者。	Service Provider
トークン	利用者が所持し管理している何らかの情報。「ハードウェアトークン」、「ソフトウェアトークン」、「ワンタイムパスワードトークン（OTPトークン）」「パスワードトークン」などが代表例。決済サービスに利用される応用技術では、他の意味で使われることがある。	Token

【参考文献】

本ガイドラインの作成にあたり、参考とした資料や文書は下記の通り。

文書名：「連邦政府機関向けの電子認証にかかわるガイダンス」
英書名：E-Authentication Guidance for Federal Agencies
発行者：米国行政管理予算局（OMB：Office of Management and Budget）
コンテンツ：OMB M-04-04
リンク：
原文 https://www.ipa.go.jp/files/000025386.pdf
独立行政法人情報処理推進機構（IPA）による日本語訳 https://www.ipa.go.jp/files/000025320.pdf
発行日：2003 年 12 月

文書名：「デジタルアイデンティティガイドライン」
英書名：Digital Identity Guidelines
発行者：アメリカ国立標準技術研究所（NIST）
コンテンツ：SP 800-63-3、SP 800-63A、SP 800-63B、SP 800-63C
リンク：
原文 https://doi.org/10.6028/NIST.SP.800-63-3
日本語訳 https://openid-foundation-japan.github.io/800-63-3-final/sp800-63-3.ja.html
発行日：2017 年 6 月発行
備考：
電子認証は、電子的な手段によって情報システムに提示されるユーザー身元識別情報の信用を確立するプロセスである。認証対象となる個人はこれらの手段を通じて、自分がなんらかの秘密情報を知っていることまたは所持していることを証明する。
本技術指針は OMB のガイダンスである『E-Authentication Guidance for Federal Agencies』[OMB 04-04]を補足するものである。

文書名：「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」
発行者：各府省情報化統括責任者（CIO）連絡会議決定
発行日：2019 年 2 月発行
リンク：
原文 https://www.kantei.go.jp/jp/singi/it2/cio/kettei/20190225kettei1-1.pdf
概要 https://www8.cao.go.jp/kisei-kaikaku/suishin/meeting/bukai/20190305/190305bukai04.pdf

文書名：「オンライン本人認証方式の実態調査」報告書
発行者：独立行政法人情報処理推進機構（IPA）
リンク：
原文 http://www.ipa.go.jp/security/fy26/reports/ninsho/index.html
発行日：2014 年 8 月

JICSAP
Japan ID Connect with Secure Authentication
Promotional association

JICSAP 認証技術部会　参加メンバー※

	氏名	所属
（部会長）	鴨 井　誠	東芝インフラシステムズ株式会社
（技術検討 WG 主査）	田 野　敦	株式会社デンソーウェーブ
（ユースケース検討 WG 主査）	矢 是 泰 士	オムロン ソーシアルソリューションズ株式会社
	梅 本 正 敏	株式会社エヌ・ティ・ティ・データ
	田 部 典 之	株式会社エヌ・ティ・ティ・データ
	広 田 智勢子	株式会社エヌ・ティ・ティ・データ
	後 藤 敏 宏	オムロンソフトウェア株式会社
	桑久保　恵	共同印刷株式会社
	広 川 知 剛	共同印刷株式会社
	武 藤 麻 由	共同印刷株式会社
	金 澤 周 平	JR 東日本メカトロニクス株式会社
	須 栗　翔	JR 東日本メカトロニクス株式会社
	古 賀 康 介	株式会社ジェーシービー
	長 岡 大 介	ジェムアルト株式会社
	石 川 勝 章	大日本印刷株式会社
	稲 垣 将 太	大日本印刷株式会社
	米 木　淳	TIS 株式会社
	多田羅 政 和	株式会社電子決済研究所　（二役）
	谷 口 敬 太	東芝インフラシステムズ株式会社
	中 山 健 司	凸版印刷株式会社
	伊名岡 健太郎	富士通株式会社
	渡 辺 宏一郎	LINE Pay 株式会社
（事務局）	多田羅 政 和	一般社団法人 ID 認証技術推進協会（JICSAP）
	吉 川 貴 浩	一般社団法人 ID 認証技術推進協会（JICSAP）

記載順は、役付委員を除き所属企業名称の五十音順。同一企業内では委員氏名の五十音順。

※認証技術部会会合に 3 回以上の出席実績がある委員のみを掲載。

JICSAP
Japan ID Connect with Secure Authentication
Promotional association

JICSAP 認証技術部会　活動経緯

＊2016 年 6 月 10 日（金）～2017 年 5 月 29 日（月）までの全 9 回、認証技術部会の前身となる活動として、
「事業運営委員会付け『JICSAP 認証技術研究 WG』」を開催。検討成果を引き継いで発足した

＜2017 年度＞

2017 年 7 月 27 日（木）	15:30～17:00	部会（第 1 回）
2017 年 9 月 8 日（金）	13:00～14:30	技術検討 WG（第 1 回）
	15:00～16:30	ユースケース検討 WG（第 1 回）
2017 年 10 月 30 日（月）	15:00～17:00	部会・合同 WG（第 2 回）
2018 年 1 月 18 日（木）	10:00～12:00	部会・合同 WG（第 3 回）
2018 年 2 月 23 日（金）	10:00～12:00	部会・合同 WG（第 4 回）
2018 年 3 月 20 日（火）	13:00～15:00	部会・合同 WG（第 5 回）

＜2018 年度＞

2018 年 4 月 26 日（木）	13:30～15:30	部会・合同 WG（第 6 回）
2018 年 5 月 24 日（木）	10:00～12:00	部会・合同 WG（第 7 回）
2018 年 7 月 6 日（金）	13:30～15:30	部会・合同 WG（第 8 回）
2018 年 9 月 5 日（金）	10:00～12:00	部会・合同 WG（第 9 回）
2018 年 10 月 11 日（木）	10:00～12:00	部会・合同 WG（第 10 回）
2018 年 11 月 8 日（木）	10:00～12:00	部会・合同 WG（第 11 回）
2018 年 12 月 5 日（水）	10:00～12:00	部会・合同 WG（第 12 回）
2019 年 1 月 10 日（木）	10:00～12:00	部会・合同 WG（第 13 回）
2019 年 2 月 7 日（木）	10:00～12:00	部会・合同 WG（第 14 回）
2019 年 3 月 20 日（水）	10:00～12:00	部会・合同 WG（第 15 回）

＜2019 年度＞

2019 年 4 月 24 日（水）	10:00～12:00	部会・合同 WG（第 16 回）
2019 年 5 月 22 日（水）	10:00～12:00	部会・合同 WG（第 17 回）
2019 年 6 月 6 日（木）	10:00～12:00	部会・合同 WG（第 18 回）
2019 年 7 月 4 日（木）	10:00～12:00	部会・合同 WG（第 19 回）
2019 年 8 月 1 日（木）	10:00～12:00	部会・合同 WG（第 20 回）
2019 年 9 月 5 日（木）	13:00～15:00	部会・合同 WG（第 21 回）

以上

JICSAP
Japan ID Connect with Secure Authentication
Promotional association

本人認証技術導入ガイドライン
【基本知識編】
第一版

発行者：　一般社団法人 ID 認証技術推進協会

発行日：　2019 年 10 月 23 日