JICSAP
Japan ID Connect with Secure Authentication
Promotional association

本人認証技術導入ガイドライン
【サービス設計編】
第 1.0 版

2022 年 12 月

一般社団法人　ID 認証技術推進協会（JICSAP）

Copyright© 2022 JICSAP All rights reserved.

JICSAP
Japan ID Connect with Secure Authentication Promotional association

目次

1．　はじめに……4
2．　提供サービスへの本人認証技術の導入……5
(1)　本人認証技術を組み込む方法……5
(2)　守るべき資産……7
(3)　本人認証の適用範囲とサービスの制約事項……7
(4)　ターゲット利用者……9
(5)　本人認証の強度……9
①　本人確認（IV）……9
②　利用者識別（UI）＋利用者検証（UV）……10
③　「JICSAP 本人認証フレームワーク」を用いた本人認証強度の評価方法……12
(6)　本人認証のバリエーション……19
①　『シングルサービス』と『サービス連携』……19
②　連携したサービスでの「JICSAP 本人認証フレームワーク」活用事例……21
(7)　留意すべき観点……24
①　リスク分析に基づくサービス設計時の留意点……24
②　利便性・コスト・強度のバランス……24
③　法律・レギュレーション……24
④　規約……25
⑤　セキュリティ（個人情報管理）……25
コラム①：　係員による「目視」認証は、生体認証と呼べるのか？……26
3．　事例集……28
(1)　シングルサービス……28
①　入室制限された場所での認証……28
②　銀行での取引……29
(2)　サービス連携……34
①　決済手段の連携……34
②　共通ポイントカード連携……37
③　デジタル商品券連携……39
コラム②：スマートフォンを活用した認証……43
4．　おわりに……48
5．　用語定義……48

Copyright© 2022 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
2022 年 10 月 4 日	0.99c	JICSAP 認証技術部会内意見募集実施
2022 年 11 月 17 日	0.99d	JICSAP 内部意見募集実施
2022 年 11 月 30 日	0.99e	会員限定の記載内容意見募集実施
2022 年 12 月 20 日	1.0	一般公開（一部に会員限り公開ページあり）

■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© 2022 JICSAP All rights reserved.

JICSAP
Japan ID Connect with Secure Authentication
Promotional association

１．　はじめに

ID 認証技術推進協会（JICSAP）が、本人認証技術導入ガイドライン【基本知識編】を発行してから 2 年ほど経過したが、その間にも、様々な本人認証技術を活用したサービスが提供されている。

本【サービス設計編】では、実際のサービス提供事例を【基本知識編】で示した、本人認証の方程式（「本人認証（UA） ＝ 本人確認（IV） ＋ 利用者識別（UI） ＋ 利用者検証（UV）」）に基づいた本人認証ガイドライン分析フレームワークに展開し、分析・比較を行う。各提供サービスが実現している認証レベルの差異を明確化することにより、安全性、導入容易性、コスト、利便性などの観点を加味しつつ、サービス設計時のセキュリティレベルや、個別の本人認証技術に対する評価の勘所になる事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。読者は本人認証技術導入ガイドライン【基本知識編】及び、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、本人認証技術導入ガイドライン【基本知識編】及び、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。

本人認証技術導入ガイドライン【基本知識編】及び、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。

２．　提供サービスへの本人認証技術の導入

事業者が新たに何らかのサービスを提供しようとする場合、当該のサービスが「本来の権利を有する人に対してのみ、正しく、適切に提供される」ことを目的として、本人認証技術を導入することがある。

本章では、事業者が本人認証技術の導入を伴うサービス設計を検討する際に、考慮すべき観点や、本人認証のバリエーションなどについて整理する。

(1)　本人認証技術を組み込む方法

サービス設計を行う場合、事業者（サービス提供者）が、本人認証技術導入ガイドライン【基本知識編】で示した本人認証のコンセプトの６つの観点に従い（図１参照）、システム提供にかかるコストとの均衡を踏まえて、判断することが求められる。

一般的には本人認証技術の認証レベルを上げる事でコストは増加し、利便性は低下する傾向がある。事業者が提供するサービスに対するリスクアセスメント（リスクの査定）を行い、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。

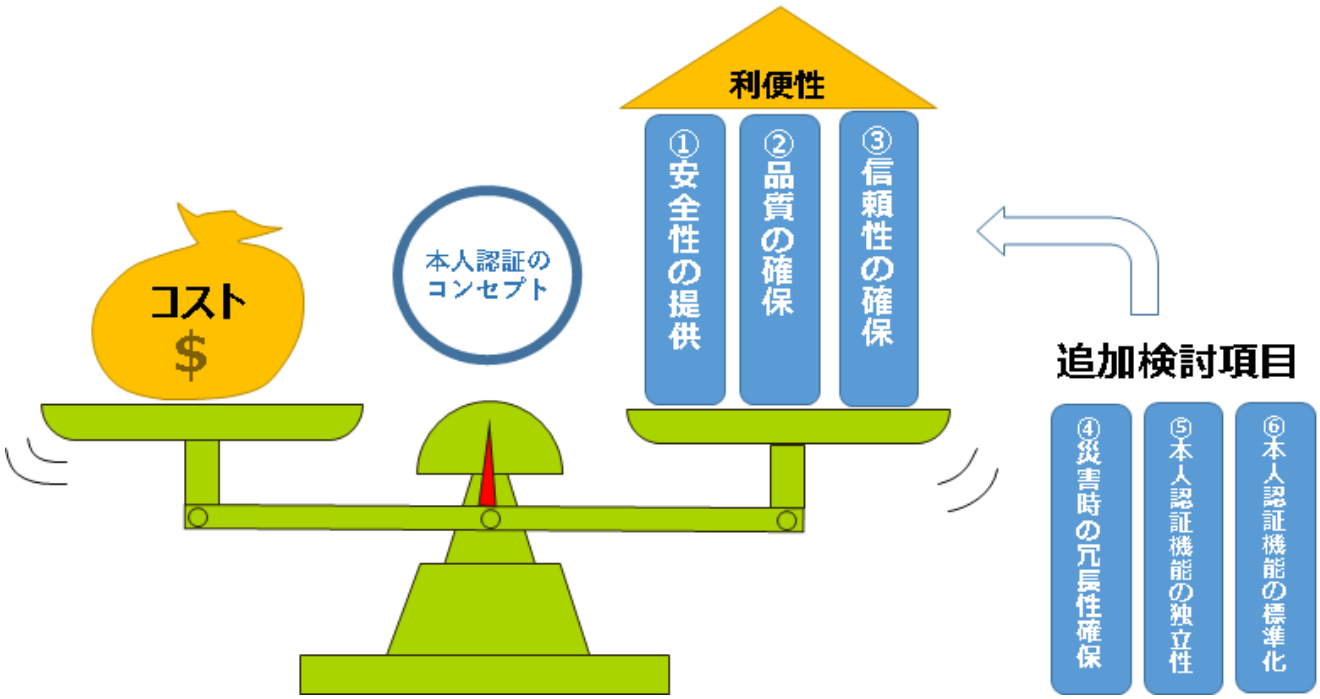


図１　本人認証のコンセプトの６つの観点（【基本知識編】再掲）

事業者（サービス提供者）が、自身のサービスについて本ガイドラインで示す分析用フレームワークを用い、分析を行う事でサービスの全体像を整理しやすくする事で、懸念事項を確認する。サービス提供時の流れについて【基本知識編】にて定義した本人認証のフレームワークを用いて説明する。

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

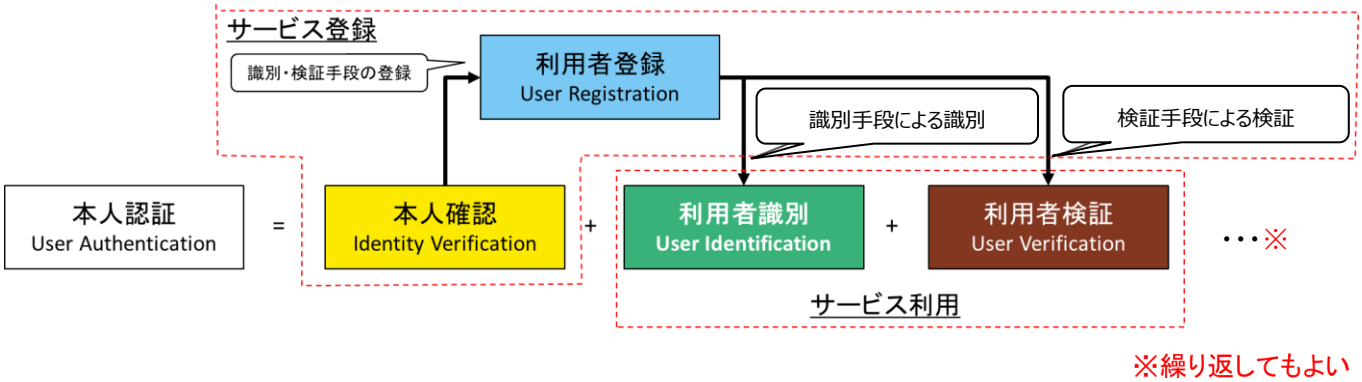


図 2　本人認証の概念図

図 2 の概念図は、サービス登録時に本人確認（IV）が行われた後に、利用者登録が行われ、サービス利用時に利用者識別（UI）及び利用者検証（UV）が行われる事を示している。

サービス登録時には、本人確認を実施後に以後のサービス利用時に有資格者である事を示すための利用者識別手法の登録、及び利用者検証手法の登録が行われる。

なお、JICSAP で定めた上記用語と関連して、経済産業省の開催する「オンラインサービスにおける身元確認に関する研究会」が 2020 年 4 月に公表した「オンラインサービスにおける身元確認手法の整理に関する検討報告書」では、本人確認（IV）のことを「身元確認（Identity Proofing）」、利用者識別（UI）と利用者検証（UV）を合わせたものを「当人認証（Authentication）」と定義し、使用している。また、身元確認と当人認証を含めた全体を「本人確認」と呼んでいる。

両者は言葉の相違こそあるが、考え方としてはほぼ同様に位置付けられるので、参考として図 3 に両者の言葉遣いの違いを掲載する。

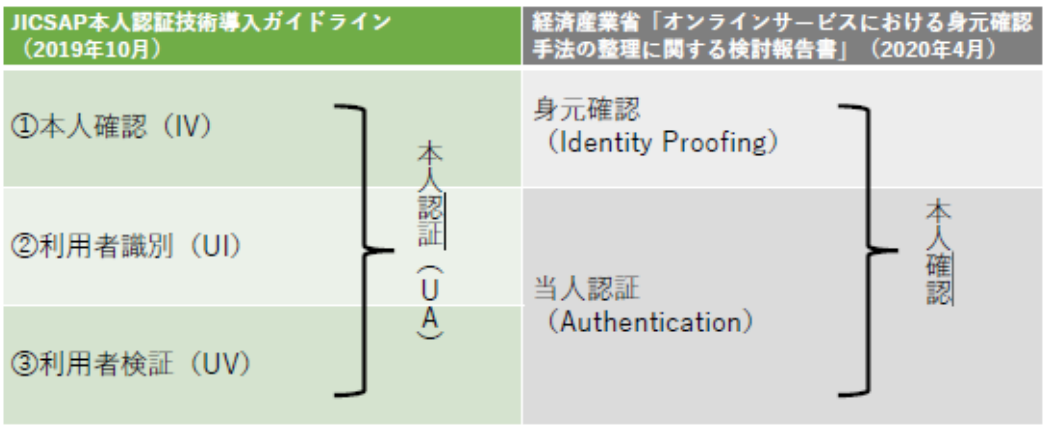


図 3　経済産業省報告書と本ガイドラインの用語比較

次項目以降で、リスクアセスメントを行う上での勘所について、「守るべき資産」、「何を行いたいか」、「ターゲット利用者」、「観点」の各項目を挙げて、留意点について記載する。

(2) 守るべき資産

サービスを提供するにあたっては、そのサービスで最も重視する守るべき資産が何かを定義した上で、その守るべき資産に対し多面的にリスクを考慮する必要がある。守るべき資産が、本人確認（IV）、利用者識別（UI）、利用者検証（UV）の要素を用いてどう担保出来るかの検討が必要になる。

- 身体及び精神的安全の場合
  身体及び精神的安全が損なわれることにより、サービス利用者は身体的、精神的苦痛、不便を被る。場合によっては影響が長期にわたったり、或いは死亡する可能性がある。従って各種法令等も確認の上、サービス設計を行う必要がある。

- 金銭の場合
  金銭には、現金、キャッシュレスサービス（カード決済、スマートフォン決済、ポイントサービス等）、商品券、キャッシュバック等がある。金銭については、利用者毎で失った際の影響度が異なるため、サービス設計の際は保証の範囲をどのようにするか検討しておく必要がある。
  また、ポイント、キャッシュバックについては、一部税金などの公金を拠出するケースもあり、分配時の公平性を考慮する必要がある。いずれのケースでも、サービスで利用できる上限金額（1 回の利用額、1 日の利用額、チャージ額上限、キャッシュバックの上限等）や利用回数を定める等の方法により、分配の公平性を制御できる可能性がある。

- データ（情報）の場合
  提供するサービスが持ち得るデータが流出する事によるリスクは何か、影響の範囲を考慮してサービス設計を行う必要がある。
  - 個人情報の場合
    日本国内での個人情報保護法や、欧州の GDPR（一般データ保護規制）など各国で個人情報の取扱いについて法令化が進んでいる。サービス登録、利用時に個人情報を取得する場合は各国の法規に照らし合わせた個人情報の保護が必要となる。詳細は（４）観点⑥セキュリティ（個人情報管理）を参照されたい。
  - 企業情報の場合
    なりすましによる入退場ゲートの突破、情報漏洩や、スマートフォンアプリで収集したマーケティングデータ等の流出は企業のイメージの低下だけでなく、事業に影響するケースが考えられる。本人認証を活用したサービス設計を行う上で、なりすましや、サイバーテロの脅威に対してどのように対応するかの検討が必要となる。

(3) 本人認証の適用範囲とサービスの制約事項

本ガイドラインの目的は以下の２点となる。

①サービス提供者において何らかの利益をもたらす事を目的とせず、提供者、利用者のお互いが平等にサービスを提供・対価を受け取ることが可能なこと

②第三者が不正に認証を行うことで利益となる情報を取得することにより、誰かかが有利になるようなサービスとならないこと

なお、サービス設計をする上で安全に機微な情報(守るべき資産)を管理する為の注意すべきサービス登録(本人確認・利用者登録)及びサービス利用(利用者認証)の設計方法の勘所は以下の通り。サービス設計時の要求仕様、運用面、セキュリティの面でのサービス提供においては、これらを参考にして検討することが望ましい。

- 利用者の範囲
  対象となる利用者の明確化が必要
  1 人あたりの開設・保有可能アカウント数の制約の有無
- サービス提供の範囲

対象とする地域を限定するか
サービス提供者（加盟店）の業態範囲はどうするか
※全国のチェーン展開する店舗、地場の店舗、オンライン店舗等の考慮

- サービス利用対価の授受、利用制約
  利用上限を設けるか（1 アカウントあたり、1 回の利用あたりで）
  課金上限を設けるか（サービス提供者のリスク回避）
  有効期限を設けるか
  1 日あたりの利用回数制限を設けるか
- サービス利用範囲
  対象商品の制限が必要か（転売リスクへの対応）
  利用シーンの限定（対面：店頭、非対面：オンライン）

(4) ターゲット利用者

本人確認（IV）、利用者識別（UI）、利用者検証（UV）において、どの認証技術要素を使用するべきか選択する場合、ターゲット利用者の年齢、IT リテラシー、障害の有無、国籍などを考慮する必要がある。

- デジタル機器未保有者への考慮
  子供や高齢者の中にはスマートフォン等のデジタル機器を保有していない方々も多く 、スマートフォンを利用した利用者識別は利用できない可能性があるので考慮する注意がある。
- IT リテラシーの考慮
  ターゲット利用者の IT リテラシーを考慮し、認証端末やスマートフォンアプリのユーザーインターフェイスや操作性について考慮する必要がある。
- 障害者への考慮
  認証方法のうち、特に生体認証を利用する場合、その生体認証を利用できない障害者への対応について考慮する必要がある。
- 外国人への考慮
  外国人の利用については、外国人を前提とした本人確認書類の選択が必要となる。国内在住か訪日外国人かによっても、保有している本人確認書類が異なっているため、考慮する注意がある。

考慮すべきターゲット利用者がたとえ利用者全体の一部であったとしても、適切な方法または代替手段を検討することが望ましい。また上記以外にも考慮すべきターゲット利用者のケースがあると思われるので、サービス事業者は、サービス設計時において、利用者の属性を踏まえた上で、本人認証方法や利用者識別（UI）、利用者検証（UV）で使用する認証技術要素を検討する必要がある。

(5) 本人認証の強度

① 本人確認（IV）

サービス登録時に行う本人確認にも強度が存在し、強度レベルは、『レベル 0：本人確認無し』、『レベル 1 ：自己申告（本人の申告内容を正とし、本人確認とする）』、『レベル 2 ：自己申告 ＋ 民間の証明情報（公的身分証明書を使わず、民間の契約内容等で本人確認を実施）』、『レベル 3 ：自己申告 ＋ 民間の証明情報（省略可） ＋ 公的身分証明』の 4 段階で定義する。本人確認行為の強度レベルを図 4 に示す。本人確認にどのレベルが要求されるかは、そのサービスでどのようなものを提供するかで変わってくる。

尚、民間の証明情報には民間レベルで限りなく本人と断定できるようなものから、自己申告内容を補足するものまで多種多様あり、民間の証明情報のみでもレベル感が変わる事が想定される。

図４　本人確認（Identity Verification）行為のレベル感

②　利用者識別（UI）＋利用者検証（UV）

【基本知識編】にて示した利用者識別（UI）、利用者検証（UV）の要求事項について、その一部を改め表１、２に表す。これらの考え方に基づいた『保証レベル』を使用して分析を行う。

表１　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	**知識** 利用者が 知っている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２ 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	**知識** 知っているから正当	**生体** 閾値を越えたから正当	**痕跡** 利用者らしいから正当		
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	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	ユーザー環境（PC、スマートフォンなど）や、過去の同サービス利用情報（購入履歴、位置情報、動作履歴など）によるリスクベース認証	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 知識：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 痕跡：持ち物、知識、生体と組合せ、他人によるなりすましリスクは限定的	
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 痕跡：持ち物、生体と組み合わせ、不正は困難	
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 痕跡：持ち物、生体と組み合わせ、不正は現実的に不可能	

（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

【基本知識編】では利用者識別（UI）および利用者検証（UV)の技術要素を「持ち物」、「記憶」、「生体」と表現していたが、「記憶」は、第 3 者から与えられる（知り得る）情報と、本人のみが知り得る情報（記憶）の 2 つに分類されるため、本書では改めて「知識」と再定義した。

表 3　知識（情報、記憶）の分類

認証技術要素	分類	内容	適用例
知識	情報	第 3 者から与えられる（知り得る）もの	利用者 ID、クレジットカード番号、など
	記憶	本人のみが知り得るもの	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

利用者検証（UV）については、省略する事ができる。また、昨今の認証技術では、本人確認で登録された ID に紐づけられた過去の購入履歴や、PC、スマートフォンなど利用者のデジタル環境に付随する位置情報、動作履歴を元に、利用者らしさを評価して検証を行う手法が注目されており、「痕跡」の枠を追加している。

【基本知識編】では言及していない「痕跡」は、認証技術部会の議論の中で整理された新技術要素である。「痕跡」は、ユーザーがサービスを利用しようとする際に、あらかじめ本人の同意を経て、ユーザーが利用中の環境に関する情報（PC、スマートフォンなど）や、過去の同サービス利用における購入履歴や、位置情報、動作履歴などの情報を確認することで利用者らしさを評価して認証する技術である。ただし、痕跡での検証は単独でなく、必ず「持ち物」「知識（情報、記憶）」「生体」の識別手段を元に用いられる。本人の痕跡を元にリスクベースで認証を行う使い方が多く、痕跡情報が不十分なケースは、他の 3 つの認証技術要素を要求する使い方が一般的であるため、「痕跡」の保証レベルは組合せる技術要素によって変化する。

守るべき資産が何であるか次第で、どこまでの痕跡を元に認証を行うかの要求レベルは異なる。

③　「JICSAP 本人認証フレームワーク」を用いた本人認証強度の評価方法

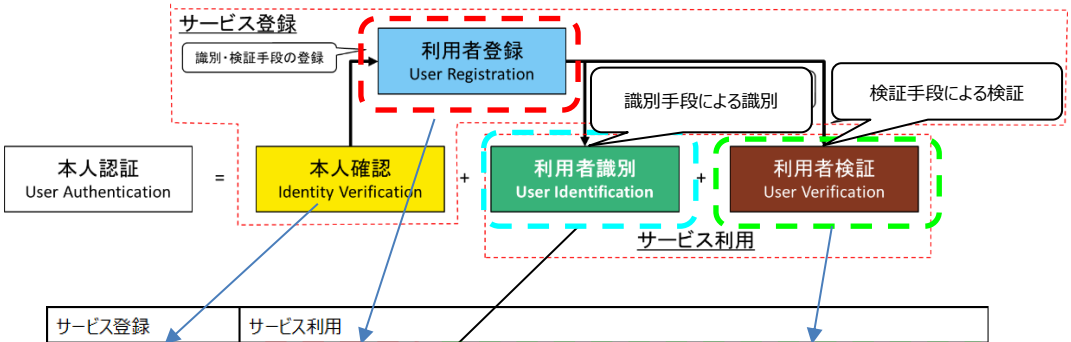
本人認証強度の評価について、フレームワークを活用して整理する方法を下記に示す。『本人認証フレークワーク』には図 5 に示すものを使用する。

サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI： UV：		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明			なし	持ち物	知識（情報、記憶）	生体	痕跡
			利用者識別（UI）	持ち物					
				知識（情報、記憶）					
				生体					
IV レベル：			UI、UV レベル：						

図 5　本人認証フレームワーク

このフレームワークと、図 2 で紹介した「本人認証の概念図」の 本人確認（IV）・利用者識別（UI）・利用者検証（UV）との関連性を図 6 に示す。サービス登録時の本人確認（IV）を左側に記載し、サービス利用時の利用者識別（UI）と利用者検証（UV）をそれぞれの利用する認証技術要素毎でどのような組み合わせで行っているかを示す事が出来るよう、L 型マトリクス形状で表現した。

本人確認後にサービス利用時に使用するための利用者登録要素は、本人確認の ID が引き継がれる事を表すため、本人確認（IV）から矢印を引き、サービス利用時に使用するための利用者登録（利用者識別（UI）に用いる認証技術要素、利用者検証（UV）に用いる認証技術要素）を L 型マトリクスの死角にあたる箇所に配置する。



サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI： UV：		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明			なし	持ち物	知識（情報、記憶）	生体	痕跡
			利用者識別（UI）	持ち物					
				知識（情報、記憶）					
				生体					
IV レベル：			UI、UV レベル：						

図 6　本人認証の概念図（図 2）と本人認証フレームワーク（図 5）の関係性

本人認証フレームワークの使い方について順を追って以下に記載する。

フレームワークは、以下の流れで記載し、分析を行う。

① 本人確認（IV）の分析
② 本人確認（IV）を元に、ID を引き継ぎ、サービス利用時に使用する利用者登録の分析
③ 利用者登録で定めた利用者識別（UI）、利用者検証（UV）の認証技術要素を L 型マトリクスの該当箇所に配置
④ 利用者識別（UI）、利用者検証（UV）のレベル分析
⑤ 全体を俯瞰したサービスの分析

① 本人確認（IV） ＜要素記入＆レベル分析＞

本人確認（IV）は、サービス登録時に使用された「自己申告」の内容、「民間の証明情報」の内容、「公的身分証明」の内容について項目毎に具体的な技術要素を白枠の部位に記載する。該当しない場合は「なし」と記載する。図 4 で示した本人確認（IV）のレベルを下に記載する

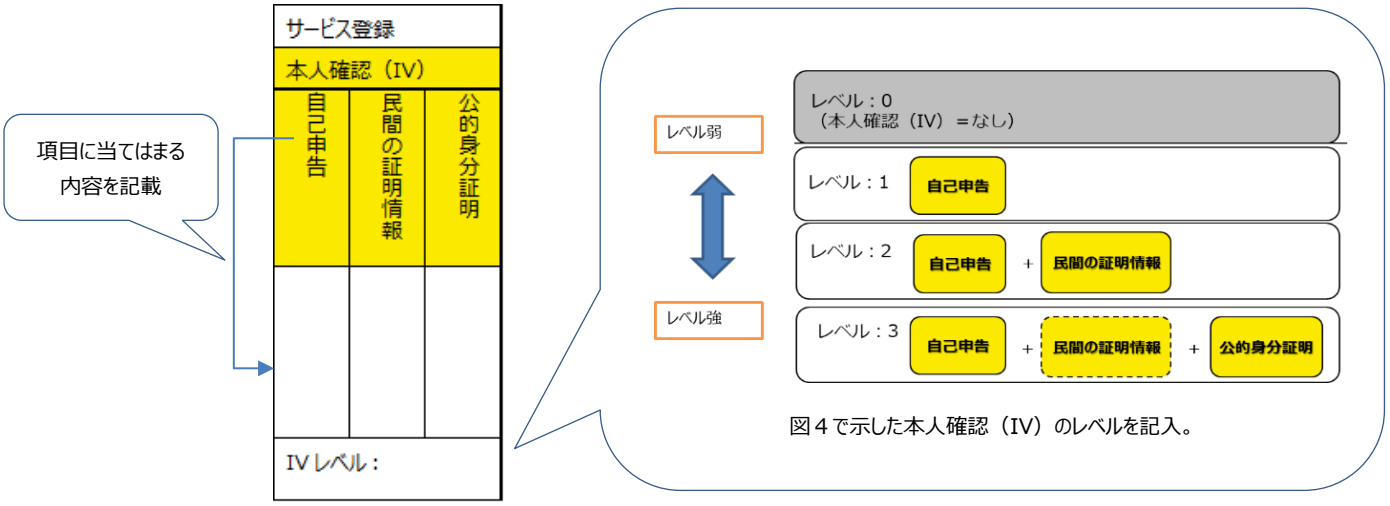


図 4 で示した本人確認（IV）のレベルを記入。

② 利用者登録 ＜要素記入＞

利用者登録は、本人確認（IV）で確認出来た内容を元に、ID（Identity）を引き継ぎ、サービス利用時に使用するための利用者を確認する手段を登録する。

ここには、②利用者識別（UI）＋ 利用者検証（UV）に記載の技術要素（赤枠内の例）を参考に、サービス利用時の利用者識別（UI）と、利用者検証（UV）に対応する技術要素を記載する。利用者検証（UV）を省略するケースは、「なし」と記載する。

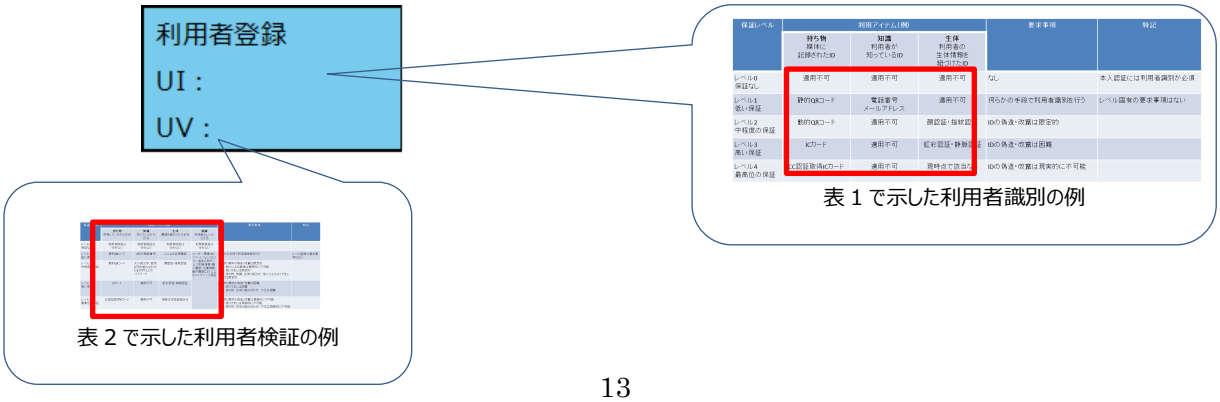


表 1 で示した利用者識別の例

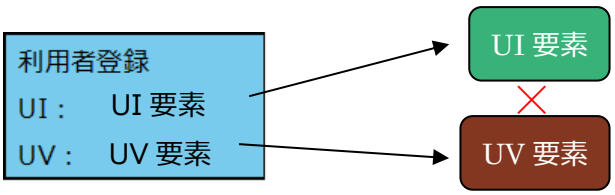
表 2 で示した利用者検証の例

③利用者識別（UI）　利用者検証（UV）　＜要素配置＞

利用者登録で定めた利用者識別（UI）、利用者検証（UV）の認証技術要素をそれぞれ色別に四角で囲い分析の準備を行う。

組合せを示すため、利用者識別（UI）の技術要素、利用者検証（UV）の技術要素を「×」を使い組合せを示す。

サービスによっては、利用者検証（UV）を省略するケースは、UV の技術要素、組合せの「×」は省略する。

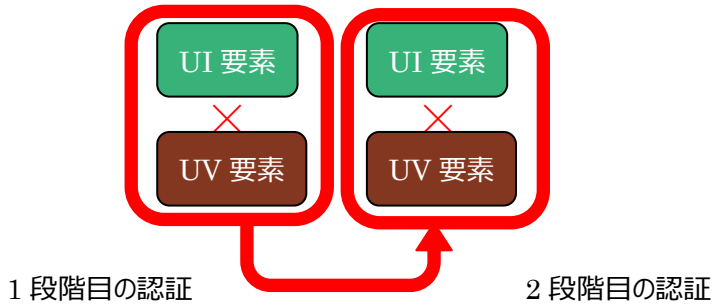


次に、利用者識別（UI）、利用者検証（UV）のＬ型マトリクスの該当技術に利用者識別（UI）、利用者検証（UV）の組合せをプロットする。

例）利用者識別（UI）：持ち物、利用者検証（UV）：知識（情報、記憶）をＬ型マトリクスにプロット

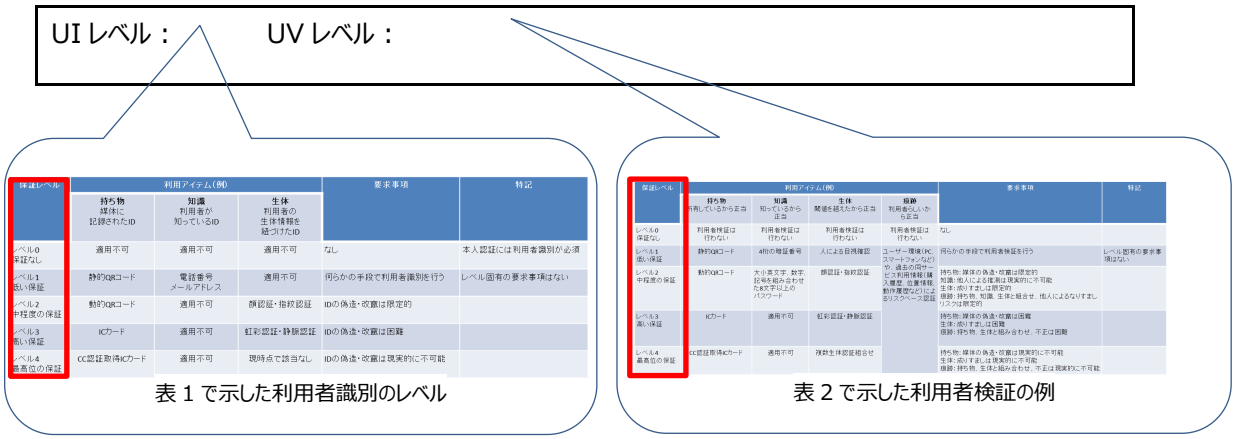
利用者登録 UI：UI 要素 UV：ＵＶ要素		利用者検証（UV）				
		なし	持ち物	知識（情報、記憶）	生体	痕跡
利用者識別（UI）	持ち物			UI 要素		
	知識（情報、記憶）			UV 要素		
	生体					

多要素/多段階認証を記載する場合、1 段階目の要素、2 段階目、n 段階目の要素をそれぞれ記載し、手順を示すため、1 段階目の認証を囲んだ上で次の段階の認証要素に向けて矢印で示す。



④利用者識別（UI）　利用者検証（UV）　<レベル分析>

利用者識別（UI）、利用者検証（UV）のレベルについて、②利用者識別（UI）＋ 利用者検証（UV）に記載の技術要素（赤枠内の例）を参考に、サービス利用時の利用者識別（UI）と、利用者検証（UV）に対応する保証レベルを記載する。



保証レベル	利用アイテム(例) 持ち物 媒体に記録されたID	知識 利用者が知っているID	生体 利用者の生体情報を紐づけたID	要求事項	特記
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	

表 1 で示した利用者識別のレベル

保証レベル	利用アイテム(例) 持ち物	知識	生体	組合	要求事項	特記
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	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	ユーザー環境(PC、スマートフォンなど)や、過去の同サービス利用情報(購入履歴、位置情報、動作履歴など)による(リスクベース認証)	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 知識: 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 複数: 持ち物、知識、生体と組合せ、他人によるなりすましリスクは限定的	
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 複数: 持ち物、生体と組み合わせ、不正は困難	
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 複数: 持ち物、生体と組み合わせ、不正は現実的に不可能	

表 2 で示した利用者検証の例

⑤　サービス全体の分析

フレームワークでサービス全体の流れを記載後、 本書第 2 章 「提供サービスへの本人技術の導入」に記載がある観点に対し、自社で検討するサービスがどのように構成されているかを改めて検証する。懸念事項があれば吹き出し等を用いて表中に記載するなどの使い方が出来る。

以降では、ユースケースごとに分解したフレームワークに当てはめ紹介していく。

(イ) SNS アプリの分析例

【ユースケースの概要】

SNS 利用に特化したアプリサービスについての分析例を図 7 に示す。サービス登録時には「氏名、生年月日、電話番号 or メールアドレス、性別」等を自己申告し、申告した情報の裏付けとして、SMS 認証で申告した本人の実体性の確認が行われるため、民間の証明情報に記載する。そのため、図左側の本人確認（IV）のレベルは 2 となる。続いて、サービス利用時には、自己申告した内容を元に利用者登録が行われる。次回ログイン時に使用するための利用者識別（UI）用には自己申告の際に記載したメールアドレス又は電話番号が登録され、（今回の場合、自己申告の内容が引き継がれ、ユーザーは意識せず UI が設定されるケースが多い）、利用者検証（UV）用には新たにパスワードの設定を行う。

サービス利用時（図の右側）は、実態のアカウントへのログインに際し、利用者登録時に設定した利用者識別（UI）と、利用者検証（UV）を使う事で本人認証が行われ SNS サイトにアクセスできる。今回のケースでは、メールアドレス又は電話番号は第 3 者から与えられる（知り得る）知識（情報）のため UI レベル 1 、パスワードは知識（記憶）のため UV レベル 1 となる。

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：メールアドレス or 電話番号
UV：パスワード</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td rowspan="2">自己申告</td><td rowspan="2">民間の証明情報</td><td rowspan="2">公的身分証明</td><td>なし</td><td>持ち物</td><td>知識 （情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>氏名、生年月日、電話番号またはメールアドレス、性別</td><td>SMS認証</td><td>なし</td><td>知識 （情報、記憶）</td><td></td><td></td><td>メールアドレス又は電話番号
×
パスワード</td><td></td><td></td></tr>
<tr><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：2</td><td colspan="7">UI レベル：1　UV レベル：1</td></tr>
</table>

図 7　SNS アプリの本人認証フレームワーク分析

SNS サービスによっては、同一の ID とパスワードを入力すれば、複数の PC やスマートフォンからログイン、サービス利用が可能なものもある。

（ロ） ポイントカードでの分析例

【ユースケースの概要】

会員向けサービスで、サービスを利用するとポイントが貯まり、貯まったポイントで支払い等にも充当することも出来る。

＜電子化される前（図８）＞

サービス登録時には「氏名、電話番号」等の本人確認（IV）レベル１の自己申告でポイントカード（例：バーコード付き）が発行される。続いて、サービス利用時には、ポイントカードに自己申告と同じ氏名を記名して利用者登録を行う。利用時は、この記名済ポイントカードを店舗で出して利用者識別（UI）が行われる。ポイントカードは、第 3 者から与えられる（知り得る）知識（情報）のため、UI レベル１となる。

サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI：記名済ポイントカード UV：なし		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明			なし	持ち物	知識（情報、記憶）	生体	痕跡
			利用者識別（UI）	持ち物	記名済ポイントカード				
氏名、電話番号	なし	なし		知識（情報、記憶）					
				生体					
IV レベル：1			UI レベル：1　UV レベル：なし						

自己申告だけのため、ポイントカードを保有している人物＝利用者という運用

図８　ポイントカード（紙）の本人認証フレームワーク分析

＜電子化された後（図９）＞

サービス登録時には「氏名、生年月日、電話番号、メールアドレス、郵便番号」等を自己申告し、申告した情報の裏付けとして、リターンメールで申告した本人の実体性の確認が行われるため、民間の証明情報に記載する。そのため、図左側の本人確認（IV）のレベルは２となる。続いて、サービス利用時にはアプリを使用するため、ユーザーの端末にアプリをインストールした上で、自己申告した内容を元にアプリ上で利用者登録を行う。ログイン時に使用するための利用者識別（UI）用には自己申告の際に記載したメールアドレスが登録され、利用者検証（UV）用には新たにパスワードの設定を行う。

サービス利用時は、アプリへのログインに際し、利用者登録時に設定した利用者識別（UI）と利用者検証（UV）を使う事で本人認証が行われ、アプリ上のポイント情報（バーコード等）が表示される。今回のケースでは、メールアドレス又は電話番号は第 3 者から与えられる（知り得る）知識（情報）のため UI レベル１、パスワードは知識（記憶）のため UV レベル１となる。

なお、アプリ上に表示されるバーコードや QR は、動的に生成されたその場（1 回）限りで使用されるものだが、利用者が自覚して能動的に提示するものであることから、利用者識別（UI）の手段として記載している。

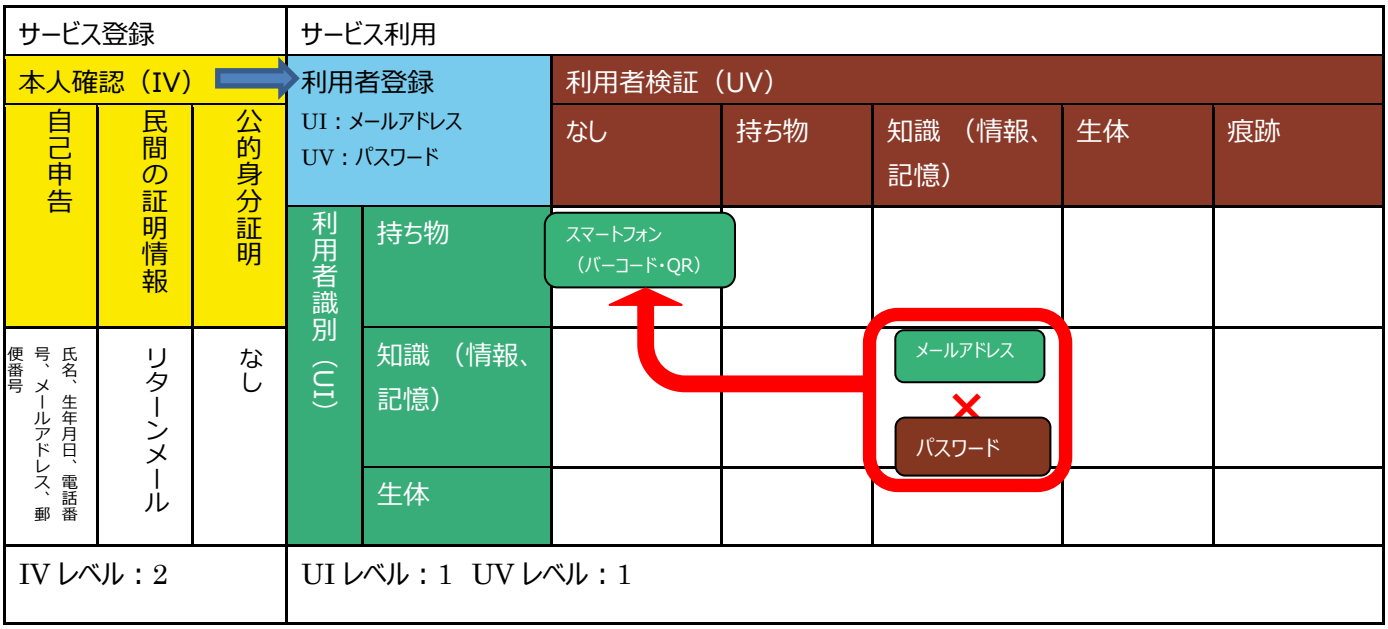


図９　ポイントカード（電子化）の本人認証フレームワーク分析

このように、同じ事例を比較する際にも本フレームワークを活用すると、認証レベルの差異が見え易くなる。

電子化されたポイントカードの登録の際は、民間の証明情報として、上記のリターンメール以外にも、電話番号認証、SMS 認証等を使用するケースもある。また、発行済みポイントカードにバーコード等の識別番号や、セキュリティ情報がある場合は、その情報と紐づける方法で本人確認を実施するケースもある。

表 4　ポイントカードサービス登録時の本人確認（IV）例

例	本人確認（IV）		
	自己申告	民間の証明情報	公的身分証明
Case 1：電話番号認証	氏名、生年月日、性別、住所、電話番号	電話番号認証	なし
Case 2：SMS 認証	同上	SMS 認証	なし
Case 3:　カード券面情報上書き	同上	発行済みカード情報	

(6) 本人認証のバリエーション

① 『シングルサービス』と『サービス連携』

サービス設計を行う場合、独自のサービスで本人認証を完了させるケースと、自社もしくは他社が提供している既存のサービスを活用して支払い等の連携を行うケースがある。前者を『シングルサービス』、後者を『サービス連携』として分けて扱う。

それぞれのサービスにおけるメリット、デメリットを示す。

- シングルサービス

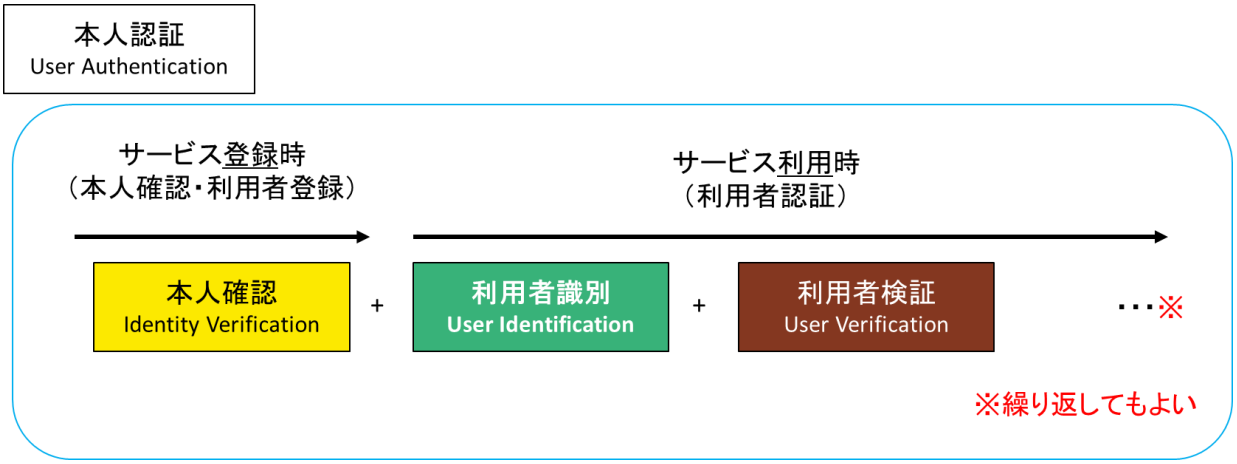


図 10 『シングルサービス』のイメージ

➢ メリット

これまで触れてきた守るべき資産、何を行いたいか、ターゲット利用者の内容を自社内で検討してサービス提供を行う事が出来るメリットがある。

➢ デメリット

独自の仕様になるため、要件定義、システム設計、運用面でコストが嵩むケースがある。

- サービス連携

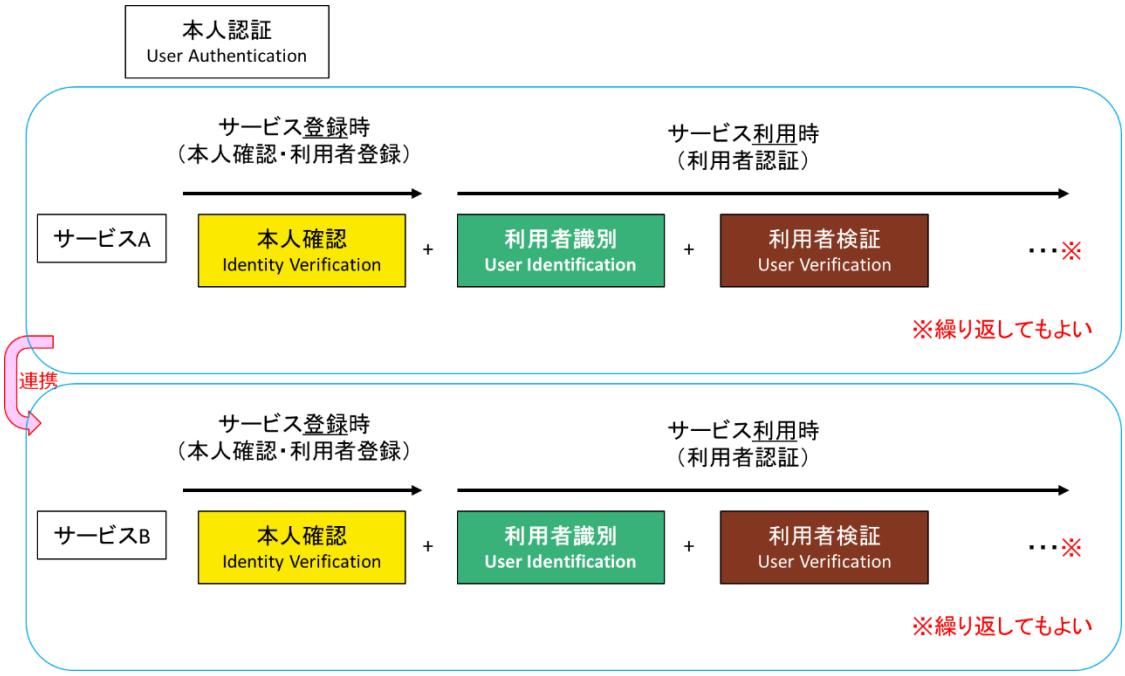


図 11 『サービス連携』のイメージ

- メリット
  一部の機能を既存の仕組みを活用する事で実現できる。
  個人情報等、取扱いに注意が必要なものを既存のサービスで代用する事で、自社保有しなくても良くなる。
- デメリット
  活用する機能の本質（守るべき資産、何を行いたいか、ターゲット利用者）が提供するサービスにマッチしているかを確認しないと、リスクが生じるケースがある。

市場で一般的に使用されているサービスでも、連携する内容によっては本人認証技術である「本人確認（IV）、利用者識別（UI）、利用者検証（UV）」の認証レベルが低いものに引っ張られて思わぬ問題が発生する事がある。そのため、サービス連携するケースでは、全体の技術要素のレベルが、サービス事業者が提供しようとするサービスにて守るべき資産が要求するレベル感を満たしているかどうかの検証が重要になる。

② 連携したサービスでの「JICSAP 本人認証フレームワーク」活用事例

ここでは交通系 IC カードのオートチャージ事例について分析する。

【ユースケースの概要】

交通系 IC カードでの残高を自動改札にタッチした時点で確認を行い、残高が一定金額以下になった場合には自動的に事前登録しておいたクレジットカードより一定金額のチャージが行われる仕組みについて分析する。

交通系 IC カード利用の流れとしては、「無記名式」交通系 IC カードの発行が必要となる。「無記名式」交通系 IC カードは、チャージしておけば何方でも使用出来るため、本人認証技術の枠外となる。本人認証技術内の記名式交通系 IC カードを使用するためには、カナ氏名、生年月日、性別等の自己申告が必用となる。本人確認（IV）はこの時点ではレベル 1 相当となる。

実際の利用時は、交通系 IC カードを改札や、交通系 IC カードの読み取り装置にかざすだけで良い。交通系 IC カード自体が持つセキュアな領域に情報が入っており、利用者識別（UI）は IC カードのセキュリティレベルに依存するためレベル 3 となる。

<table>
<tr><td colspan="3">サービス登録</td><td colspan="6">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：交通系 IC カード
UV：なし</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td>自己申告</td><td>民間の証明情報</td><td>公的身分証明</td><td>なし</td><td>持ち物</td><td>知識 （情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">カナ氏名、生年月日、性別、</td><td rowspan="3">なし</td><td rowspan="3">なし</td><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td>交通系 IC カード</td><td></td><td></td><td></td><td></td></tr>
<tr><td>知識 （情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：1</td><td colspan="6">UI レベル：3 UV レベル：0</td></tr>
</table>

図 12 「記名式」交通系 IC カードで改札利用 <シングルサービス>

「記名式」交通系 IC カードは、クレジットカードを紐づけて交通系 IC カードへのオートチャージ設定が可能となる。チャージ残高が設定金額以下の状態で改札機等に交通系 IC カードカードをかざすと自動的にチャージされる。クレジットカードの紐づけは、本人確認（IV）手段にサービス事業者ごとに特長がある。

「記名式」交通系 IC カードに、クレジットカードのサービスを連携させる例の分析内容を下記に示す。

「記名式」交通系 IC カードで改札利用 <シングルサービス>

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：交通系 IC カード UV：なし		なし	持ち物	知識（情報、記憶）	生体	痕跡
カナ氏名、生年月日、性別	なし	なし	利用者識別（UI）	持ち物					
				知識（情報、記憶）					
				生体					
IV レベル：1			UI レベル：3　UV レベル：0						

交通系 IC カード

連携

改札機等での「記名式」交通系 IC カードへのオートチャージ

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：交通系 IC カード UV：なし		なし	持ち物	知識（情報、記憶）	生体	痕跡
交通系 IC カードの ID	※1	なし	利用者識別（UI）	持ち物					
				知識（情報、記憶）					
				生体					
IV レベル：2			UI レベル：3　UV レベル：0						

交通系 IC カード

図 13 「記名式」交通系 IC カードへのオートチャージ <サービス連携>

※1　以下の例で運用されているケースがある。

例	本人認証要素		
Case 1：プラスチックカード X 人力認証 窓口での本人確認	申し込みはがき（郵送）氏名	記名式交通系 IC カード名義	交通系会社が発行したクレジットカード名義
Case 2：プラスチックカード X 機械認証 専用端末（ATM）での本人確認	クレジットカードの暗証番号	↑ （カナ氏名、生年月日、性別）	↑
Case 3：スマートフォン X 機械認証 オンラインでの本人確認	クレジットカードの PAN,暗証番号	スマートフォンに内蔵された FeliCa チップ	各社が発行したクレジットカード

それぞれ、利便性を向上させるため、サービス利用時の利用者検証（UV）を省略しているが、本人確認（IV）でサービス全体の担保を行っているケースになる。オートチャージの上限額は規約や、設定等で制限をかける事によって、紛失した際のリスクを考慮したサービス設計となっている。

このように『サービス連携』の事例を分析する際には、連携元となるシングルサービスのフレームワークを上側に記載し、連携先のサービスを下に記載し、それぞれが連携されている状態を記載する。連携元で利用者登録された UI が、連携先の本人確認（IV）において自己申告の要素として利用される。

(7)　留意すべき観点

①　リスク分析に基づくサービス設計時の留意点

本人認証に関わるサービス設計において、それぞれのユースケースを想定し、リスクを考慮する必要がある。

想定されるリスクの事象に合わせ、本人確認（IV）、利用者識別（UI）、利用者検証（UV）の認証レベルを検討し、可用性、利便性なども考慮した対策を検討する。

（イ）メールアドレスのみで本人確認（IV）するケース

1 人が複数のアカウントを保有できるという特性がある。1 人 1 アカウントの制限を行いたい場合、重複獲得などのリスクが生じる。

本人確認（IV）で個人特定が難しい場合には、利用者検証（UV）等で重複獲得を防ぐなど工夫をする必要がある。「デジタル商品券」のユースケース参照

（ロ）本人確認（IV）情報の上書きについて

本人確認（IV）を行い一旦登録された情報の更新を可能とする場合については、本人確認（IV）情報の書き換えの際にリスクに応じた権限付与が必要になる。

「コラム①」のユースケース参照

（ハ）ログイン情報の不正取得によるアカウントの乗っ取り

ID/パスワードによるアプリログインを行っている場合、アカウント情報の漏洩等によりなりすましやアカウントの乗っ取りのリスクがある。リスクに応じて二要素認証等の追加認証を行う必要がある。

「チャージ連携　Case 1」のユースケース参照

（ニ）自社会員向けサービスを他社ユーザーへ開放する場合

自社会員向けに構築したサービス（ハウスカード）を、他社ユーザーへ開放する場合、本人確認（IV）のレベルが低いとなりすまし等の脆弱性が生じる。第三者認証（民間の証明情報）や公的身分証明を付加するとよい。

「サービス連携」の複数のユースケース参照

②　利便性・コスト・強度のバランス

サービス登録時の本人確認（IV）手段と本人確認（IV）レベル、サービス利用時の利用者識別（UI）、利用者検証（UV）手段と利用者識別（UI）、利用者検証（UV）レベルが提供するサービスに見合っていないと、利便性を欠き、コストが上がり、強度が下がることに注意したい。サービス設計においては、利便性を上げ、コストを下げ、そして強度を上げることがそれぞれ必要である。しかし、利便性と強度、コストと強度はそれぞれトレードオフの関係にあり、利便性を上げた場合、強度は下がり、強度を上げた場合、コストも上がる。そのため、サービス設計は、提供するサービスに見合ったサービスの利便性・コスト・強度のバランスをとることが要求され、またサービス内容の変化に合わせてそれらをリバランスすることも重要である。

③　法律・レギュレーション

サービスの用途によっては、公的機関や業界団体による、認証方式への規制やガイドラインが存在する場合がある。通常それらは、一定以上の強度の認証方式を求めるものである。

例をあげると、銀行口座を開設する場合、犯罪収益移転防止法に準拠した KYC が求められる。また、犯罪クレジットカードの番号を扱うシステムの場合、PCI DSS（Payment Card Industry Data Security Standard）への準拠が求められる。PCI DSS では、システムにログインする際に二要素以上の認証を用いることが求められる。また、厚生労働省の「医療情報システムの安全管理に関するガイドライン」でも、医療情報を扱うシステムでは二要素認証を採用するよう求めている。

クレジットカードの番号、住所・電話番号・メールアドレス等の個人情報は、情報漏洩時に速やかに本人に連絡をする必要がある（改正個人情報保護法）。

本人から個人情報削除の要請があった場合、速やかに対応できるよう運用設計が必要となる。

犯罪収益移転防止法の規定により、同法で定められた方法でサービスの登録時の本人確認(IV)を行うことが必要になるケースもある。

④ 規約

サービス提供にあたり、サービス登録の本人確認時に規約にて本人認証等に関する項目を定めることで、サービス提供者とサービス利用者の責任を明確にする必要がある。規約に含める主な項目には、以下がある。

- 利用時の本人確認について … サービスを利用時にサービス提供側が要求する「サービス利用者の情報の種類」や「利用者認証の方法」など
- 本人以外の使用について … 「不正使用(第三者の使用)」、「譲渡」、「代理人による利用」など、本人以外が使用することに対する可否
  また、偽造・盗難などによる不正利用時の対応など
- 管理について … 「端末やパスワードの管理の推奨や条件」、「盗難や紛失時の対応」など
- 責任範囲と罰則 … 「サービス提供者側が負う責任範囲」や「上記を違反時などのサービス継続可否や条件」など
- 個人情報の取扱い … 個人情報の種類や利用目的、管理方法など

⑤ セキュリティ（個人情報管理）

サービス設計のなかで留意するセキュリティ項目

- 個人識別符号（顔や指紋、静脈等）は、適切な範囲を適切な手法で取り扱わなければならない。
- クレジットカードの番号を取り扱う場合は、PCI DSS※に準拠しなければならない。
  ※③法律・レギュレーションのクレジットカード例参照
- クレジットカードの番号等を電子的に記録した場合、不要に長期間保有しないよう定期的な棚卸する必要がある。
- 個人情報を第三者へ提供する場合、原則としてあらかじめ本人の同意を得なければならない。
  また第三者から個人情報の提供を受けた場合、一定事項（いつ、誰の、どんな情報、誰から・・・）を記録しなければならない。

コラム①： 係員による「目視」認証は、生体認証と呼べるのか？

近年、本人認証の際に用いられる機会が多くなった「生体認証（Biometrics）」。指紋や静脈、顔貌といった個々人に固有の「生体」情報を用いた認証技術を指すが、2001 年 9 月 11 日に発生した「アメリカ同時多発テロ事件」以降、国際テロに対する未然防止策として普及が加速したと言われる。

この「生体」を用いた認証を利用する場合、あらかじめ事前登録の際にキャプチャーして保存しておいた本人の生体情報と、今まさにサービスを利用しようとする本人の生体情報とをその場で見比べ、一致しているか不一致かの判断を下さねばならないことから、もっぱら機械が活用されている。特に、対象が不特定多数で膨大な登録者数を誇るサービスでは、本人認証の比較・照合・判定に人間が介在しない、機械とデジタル技術を用いる方法だけを指して「生体認証」ととらえるのが一般的である。

しかし、実際には人間による「人力」の生体認証も可能である。古くは「富山の薬売り」などに語り継がれる、顔や背格好、声といった買い手の特徴情報をすべて記憶していたという売り手のエピソードは有名だが、地域の商店スタッフや仕事仲間、学校の友人など、考えてみれば私たちは毎日当たり前に「相手」のことを、確かにその相手であると認めながら生きている。

さらに、専門家になると、相手を不特定多数に広げたとしても「人力生体認証」の精度はより強固になる。例えば、パスポート（旅券）や運転免許証、マイナンバーカードなどを発給する窓口の係官は、生体情報と、現れた本人とを見比べる際の勘どころを会得している。

これらの「人力生体認証」では平常時、誰でも外界に露出している顔貌が多く利用されるが、実は指紋や声（音声）、筆跡などの方法であっても、違いを見破れるプロは存在する。

ところが「人力生体認証」には落とし穴がある。意図的に、誤った相手に対して、認証を融通してしまう可能性があることである。係員の目視による比較・照合の結果は明らかに「別人（認証エラー）」なのだが、それとは別の何らかの理由による判断が働き、「本人（認証 OK）」の判定を返してしまうケースがある（ユースケース参照）。

故意でなかったとしても、過去の経験や記憶にあいまいな点があり、間違った判定につながることもある。この場合の脆弱性は、「人間の弱さ」にあるといえる。

本ガイドラインの検討を進める過程では、「人力生体認証」が強い本人認証として認められる場合と、それとは真逆に最低ランクの本人認証に位置付けられる場合とが存在している点に大いに注目した。「人力生体認証」の導入を検討する際には、最も注意していただきたい視点である。

【ユースケースの概要： 警備員による目視チェック】

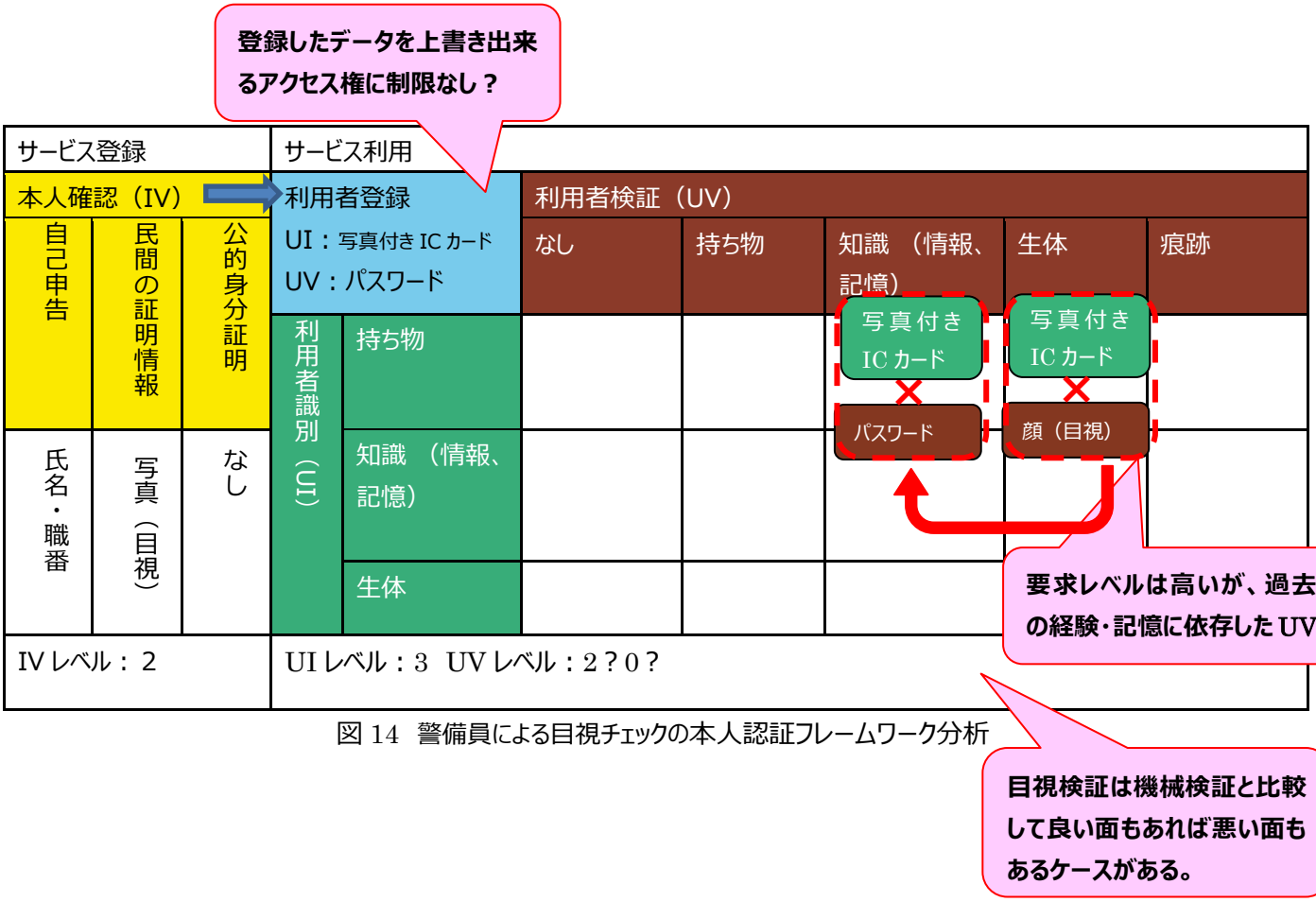


図 14 警備員による目視チェックの本人認証フレームワーク分析

重要施設では、入出を許可された有資格者の入出記録が求められ、係員による第一のゲート、有資格者である事を検証するための写真付き IC カードによる第 2 のゲートを設け運用するケースがある。有資格者である本人が、第 2 のゲートで使用する写真付き IC カードを紛失してしまい、当日勤務していない別の有資格者の IC カードを無断で持ち出し使用。係員は、写真付き IC カードが通過している本人と顔が違う事に疑いを持ちつつも面識のある方のため第一のゲートを通過。ＩＣカードでの利用者検証でエラー警告が出たが、ここも係員の判断で良かれと思いシステム内の ID の識別情報の上書き（利用者登録の更新）が行われ、第 2 のゲートを通過する事案が発生。係員の過去の経験・記憶に依存した利用者検証（UV）となっている点が脅威となった。

３．　事例集

本事例集は、これまで述べてきたサービス設計の内容について、実際のサービスに当てはめて分析した内容を示す。
サービス設計時の参考のため記載する。

(1) シングルサービス

①　入室制限された場所での認証

本人確認を行う上で「守るべき資産＝データの場合」として入室制限された場所での認証例を記載する。

【ユースケースの概要】
企業等で一部の人のみが出入りできる部屋の写真付きＩＣカードの利活用について分析する。

本サービスを登録する際には、社員の氏名、職番等の情報を元に申請書類を作成（自己申告）し、申請者とICカードの券面に付く写真との一致性、更には所属する部署等の上司承認を経て本人確認（IV）がなされる。この時、公的身分証明書までの要求は無いため、本人確認（IV）のレベルは２に分類される。
セキュリティ性を担保するため、IC カード（持ち物）で利用者識別（UI）し、利用者しか知りえない暗証番号（記憶）で利用者検証（UV）を行い、検証結果が合致すれば部屋の鍵が開く。暗証番号は、４桁の暗証番号とする。
写真付きICカードは、IDの偽造・改竄は困難な事から、持ち物としての保証レベル：３（高い保証）になる。また暗証番号は、何らかの手段で利用者検証を行う手段として使用される一般的なものであるため、保証レベル：1(低い保証)になる。

フレームワークに当てはめたものを下記に示す。

<table>
<tr><td colspan="3">サービス登録</td><td colspan="6">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：写真付きICカード
UV：暗証番号</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td>自己申告</td><td>民間の証明情報</td><td>公的身分証明</td><td>なし</td><td>持ち物</td><td>知識（情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">氏名・職番</td><td rowspan="3">上司承認・写真（目視）</td><td rowspan="3">なし</td><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td></td><td></td><td>写真付きICカード
×
パスワード</td><td></td><td></td></tr>
<tr><td>知識（情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：2</td><td colspan="6">UI レベル：3　UV レベル：1</td></tr>
</table>

図 15　入室制限された場所での本人認証フレームワーク分析

本人確認（IV）のレベルは公的身分証書を使用しないため、レベル２に相当するが、企業内の限られた範囲での運用と見ると、社員の職番が公的身分証明書と同じレベルとしてみなす事もでき、本人確認（IV）は最高レベル３とみなす事が出来る。
本ユースケースは、本人確認（IV）及び、利用者識別（UI）の持ち物としての偽造・改竄が困難なレベルにする事で、利用者検証（UV）を簡素化したケースとなる。

② 銀行での取引

本人確認を行う上で「守るべき資産＝金銭」の最高峰として銀行での現金引き出しの例を記載する。

【ユースケースの概要：口座開設】

銀行口座の開設は、2007 年 3 月に成立、公布された犯罪収益移転防止法（犯収法）に基づき実施される。2018 年 11 月に法改正が行われ、非対面での身元確認（所謂 eKYC）が可能となり、オンラインでの口座開設が可能となった。

Case1 窓口での開設

店頭に利用者が出向き、申込書を記入する。これに本人確認書類を添えて銀行の係員に提出する。係員は、本人確認書類の内容を確認する。この時、公的身分証明書の顔写真と本人を見比べる。本人確認（IV）は犯収法に沿って KYC が行われるためレベル 3 となる。
申し込みの後、利用者宛にキャッシュカード・ネットバンクのログイン用情報などが利用者に届けられる。生体認証キャッシュカードを使いたい場合、利用者は店舗に出向いて生体情報を登録する。

※ここでは、サービス登録に着目して記載

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：
UV：</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td rowspan="2">自己申告</td><td rowspan="2">民間の証明情報</td><td rowspan="2">公的身分証明</td><td>なし</td><td>持ち物</td><td>知識（情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">電話番号、氏名、郵便番号、住所</td><td rowspan="3">本人確認郵便での所在確認</td><td rowspan="3">免許証・マイナンバーカード等</td><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>知識（情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：3</td><td colspan="7">UI レベル：　UV レベル：</td></tr>
</table>

図 16 銀行窓口での口座開設時の本人確認

Case2：オンラインでの開設

利用者は、銀行が準備した口座開設用アプリを使い、公的身分証明書と自らの顔写真をカメラで撮影する。その後、申し込みの必要事項を入力する。民間の証明情報に記載の顔画像は公的身分証明書にある顔写真と申請者が一致しているかという観点で行われるため、事業者のよっては、様々な角度で画像を撮像し、カメラ越しの本人の実体性を確認する手段が取られている。本人確認（IV）は犯収法に沿って eKYC が行われるためレベル 3 となる。

申し込み完了後、口座番号・キャッシュカード・ネットバンクのパスワード等が利用者に届けられる。生体認証キャッシュカードを使いたい場合は、利用者が店舗に出向いて生体情報を登録する。

※ここでは、サービス登録に着目して記載

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：
UV：</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td rowspan="2">自己申告</td><td rowspan="2">民間の証明情報</td><td rowspan="2">公的身分証明</td><td>なし</td><td>持ち物</td><td>知識（情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>電話番号、メールアドレス</td><td>顔画像</td><td>免許証・マイナンバーカード・住基カード</td><td>知識（情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：3</td><td colspan="7">UI レベル：　UV レベル：</td></tr>
</table>

図 17　オンライン（非対面）での口座開設時の本人確認

【ユースケースの概要：出金】

Case 1：ATM での出金

利用者が ATM を操作して、自らの口座から現金を引き出す。利用者識別（UI）として、カード（持ち物）を使用し、利用者検証（UV）として、①暗証番号若しくは事前に店舗で登録した②生体情報を使用する。ATM にカードを挿入することに加え、暗証番号もしくは、生体認証の検証が成功しないと出金できない。

① 暗証番号での利用者検証

1－1：カード＝磁気カード（MS カード）の場合

サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI：磁気カード UV：暗証番号		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明			なし	持ち物	知識（情報、記憶）	生体	痕跡
窓口開設 or オンライン開設			利用者識別（UI）	持ち物			磁気カード × 暗証番号		
				知識（情報、記憶）					
				生体					
IV レベル：3			UI レベル：2　UV レベル：1						

磁気カード（MS カード）はスキミングリスクがある

図 18　利用者識別（UI）に磁気カード（MS カード）を用いたサービス利用

1－2：カード＝IC カードの場合

サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI：IC カード UV：暗証番号		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明			なし	持ち物	知識（情報、記憶）	生体	痕跡
窓口開設 or オンライン開設			利用者識別（UI）	持ち物			IC カード × 暗証番号		
				知識（情報、記憶）					
				生体					
IV レベル：3			UI レベル：3　UV レベル：1						

IC カードは暗号化されているためスキミング被害にあいにくい

図 19　利用者識別（UI）に IC カードを用いたサービス利用

暗証番号は 4 桁の簡易的な物であるため、利用者識別用のカードのレベルを上げる事でスキミング対策が行われつつある。一般的に磁気カード（MS カード）に比べ、IC カード搭載のカードの方が保証レベルは高い。

② 生体認証での利用者検証

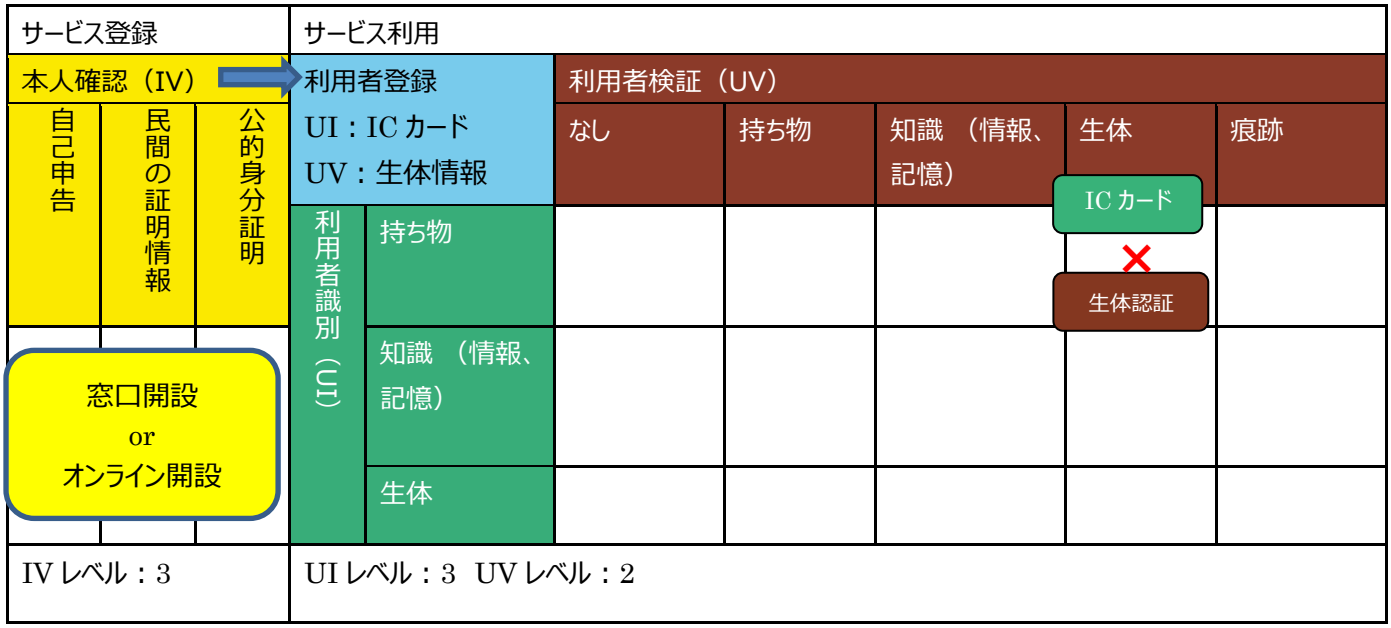


図 20 利用者検証（UV）に生体認証を用いたサービス利用

①の暗証番号での利用者検証以外にも、利用者は店舗に出向いて生体情報を登録する事で生体を使った利用者検証を使用できる。生体情報は、IC カード内に保存されており、登録された生体情報（指紋、静脈など）と照合して利用者検証を行う。

ただ、すべてのＡＴＭに生体認証用の機器が付いているわけではないので、磁気カード＋暗証番号での取引額、IC カード＋暗証番号での取引額、ＩＣカード＋生体認証での取引額を変えて運用し、もしもの時のリスク低減を行っているケースもある。

近年は、上記 2 パターンに加え、利用者識別（UI）としてカードの代わりに生体情報を入れた QR コード（持ち物）、利用者検証（UV）として生体認証（QR コード内の生体情報とのオフライン認証）で出金が出来る実証実験が行われている。使用する QR コードの見た目は通常の QR コードと一緒だが、生体情報にはセキュリティがかけてある特殊な物となっている。

Case 2：オンラインでの出金

利用者がネットバンクの画面を操作して、自らの口座から他の口座へ現金を振り込む。①利用者識別（UI）に口座番号、利用者検証（UV）にパスワードを求める。②2 段階認証として、利用者識別（UI）に口座番号、利用者検証（UV）に One Time Pass（OTP）を求める。OTP の検証が成功しないと出金できない。加えて、③過去の痕跡情報を元に、通常使用と異なる接続方法や、端末からの操作が行われた場合、④追加の利用者検証（UV）を求める場合もある。これは、所謂リスクベース認証であり、サービス提供者で定めた利用者検証（UV）が一定のレベル以上と判断した場合、認証し、一定レベル以下の場合は、④追加の利用者検証（UV）が行われる。ユーザーの確からしさを確認する目的でサービス登録時に定めた利用者識別（UI）、利用者識別（UV）手段を使い有資格者のユーザーである事を確認する。

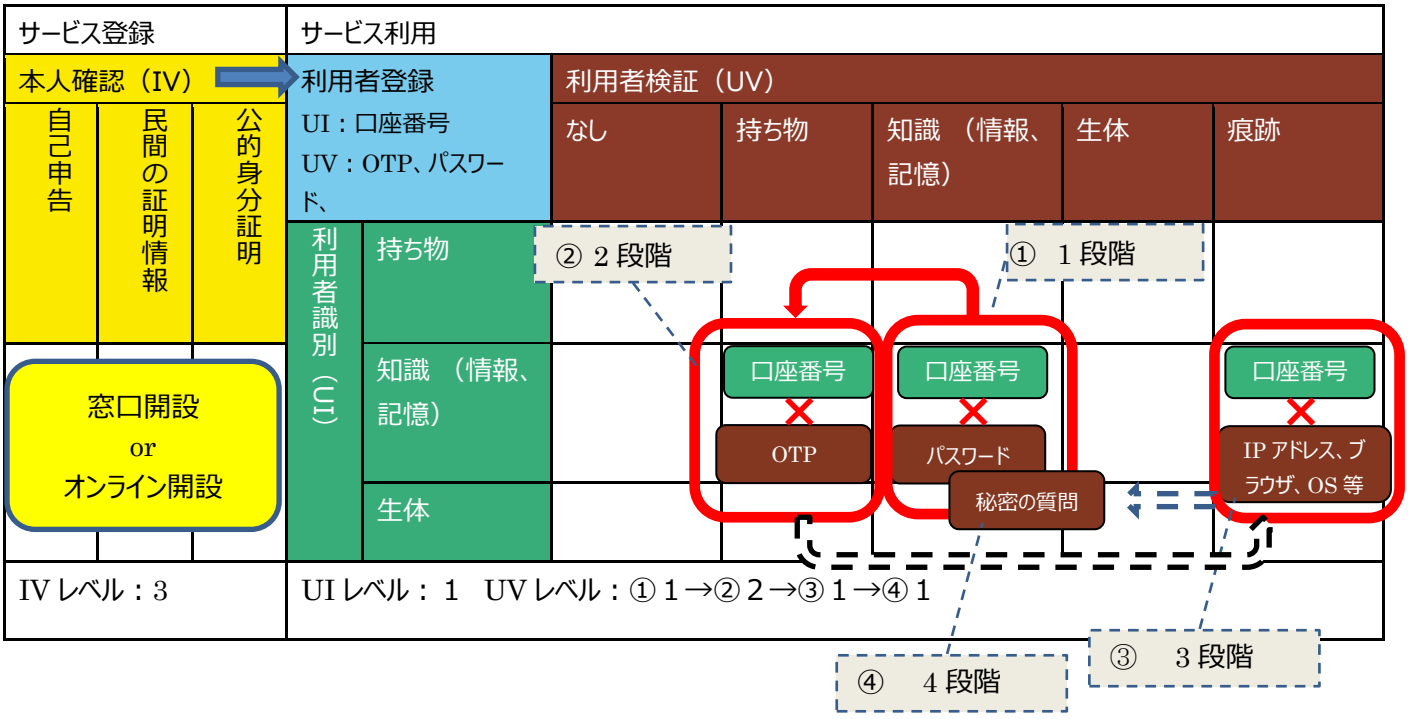


図 21 オンライン出金の事例分析

(2)　サービス連携

①　決済手段の連携

本人確認を行う上で「守るべき資産＝金銭の場合」とし決済手段の連携例を記載する。

【ユースケースの概要】

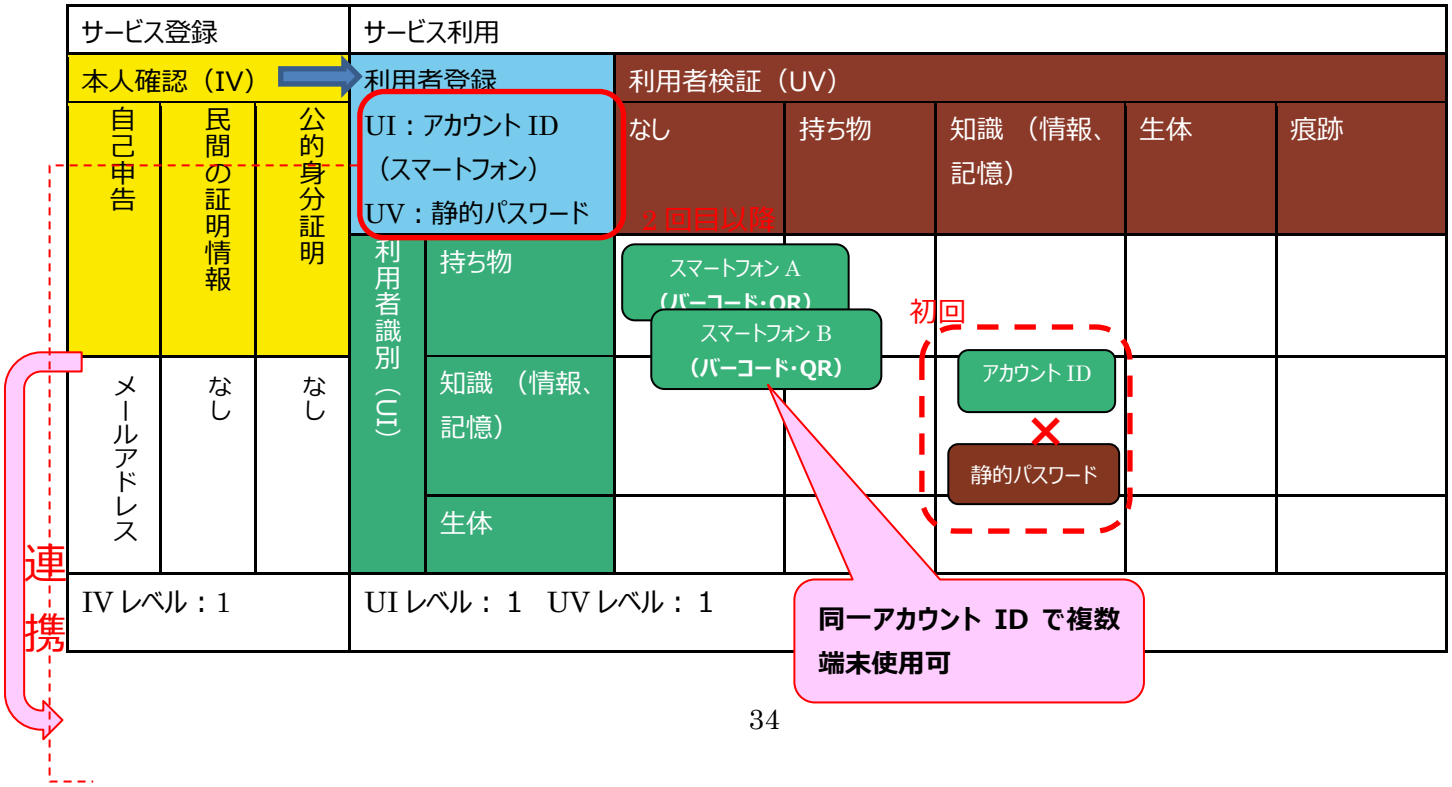
スマートフォンアプリに決済手段を登録し、CPM 方式のコード決済活用について分析する。

(イ) Case 1: 複数端末からのログインを許可するサービスへのクレジットカード連携

一般的にスマートフォンアプリの場合、ユーザーの広告配信や、マーケティングの目的でメールアドレスの登録を自己申告とするケースが多い。利用者登録には、ID（UI）＝保証レベル 1 、パスワード（UV）＝保証レベル 1 を設定し、利便性を重視し、サービス使用する場合は初回のみログインが求められ、2 回目以降は ID,パスワードで利用者検証されたスマートフォンを所持する事で利用者識別（UI）がなされ、利用者検証（UV）が省略される。

このアプリに決済手段を登録する場合は、本人確認（IV）の際に、アカウント ID、パスワード、クレジットカードの券面に表示されている番号（PAN）による自己申告を行い、民間の証明情報として一般的にクレジットカードの裏面に表示される CVV の入力と、クレジットカード会社のなりすまし防止の仕組み（3D secure 認証）による厳格な検証を実施しているケースもある。
利用時は、ベースとなるスマートフォンアプリと同様に利便性を重視した運用を取るケースが多い。リスト型アカウントハッキングの標的になりやすい
フレームワークに当てはめたものを下記に示す。

スマートフォンアプリサービス登録、利用



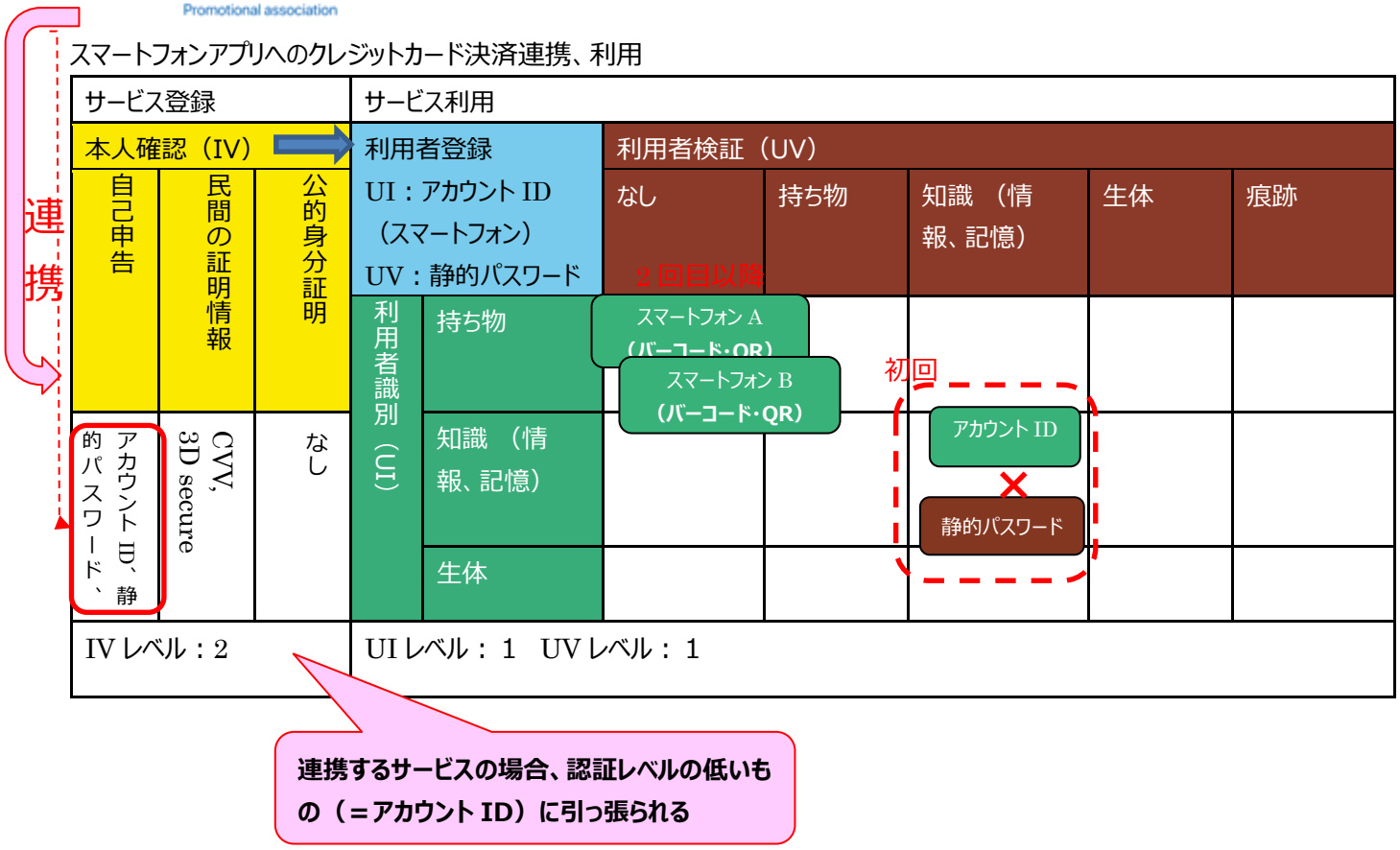


図 25 複数端末からのログインを許可するスマートフォンアプリへのクレジットカード連携分析

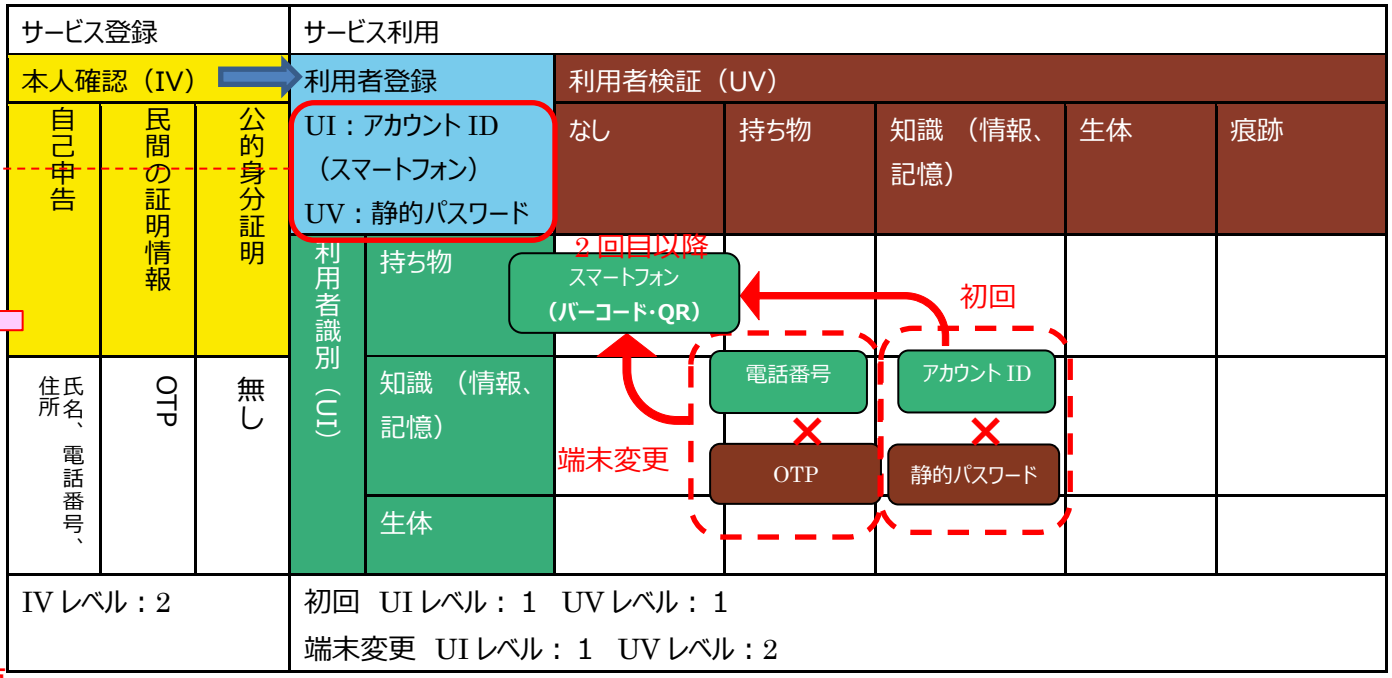
(ロ) Case 2: 複数端末からのログインを許可しないサービスへの銀行口座からのチャージ連携

複数端末からのログインを許可しない場合、サービス登録時の本人確認（IV）のレベルが一段上がる。自己申告には、個人を特定し易くなるための電話番号を用い、民間の証明情報として、OTP（ワンタイムパスワード）を使い、登録するスマートフォン等の端末の前に本人が居て操作しているかの確認を行う。利用者登録には、アカウント ID（UI）＝保証レベル 1 、パスワード（UV）＝保証レベル 1 を設定するが、利便性を重視し、サービス使用する場合は初回のみログインが求められ、端末が変更になると、改めて電話番号に SMS 等で通知される OTP での認証が走る仕組みを準備するケースもある。通常使用の場合は、2 回目以降は ID,パスワードで利用者検証されたスマートフォンを所持する事で利用者識別（UI）がなされ、利用者検証（UV）が省略される。

このアプリに決済手段（銀行口座チャージ）を登録する場合は、本人確認（IV）の際に、アカウント ID、パスワード、民間の証明情報として、銀行アプリ、暗証番号、OTP による検証を実施しているケースもある。
利用時は、ベースとなるスマートフォンアプリと同様に利便性を重視した運用を取るケースが多い。

フレームワークに当てはめたものを下記に示す。

スマートフォンアプリサービス登録、利用



連携

スマートフォンアプリへの決済連携（銀行口座チャージ）、利用

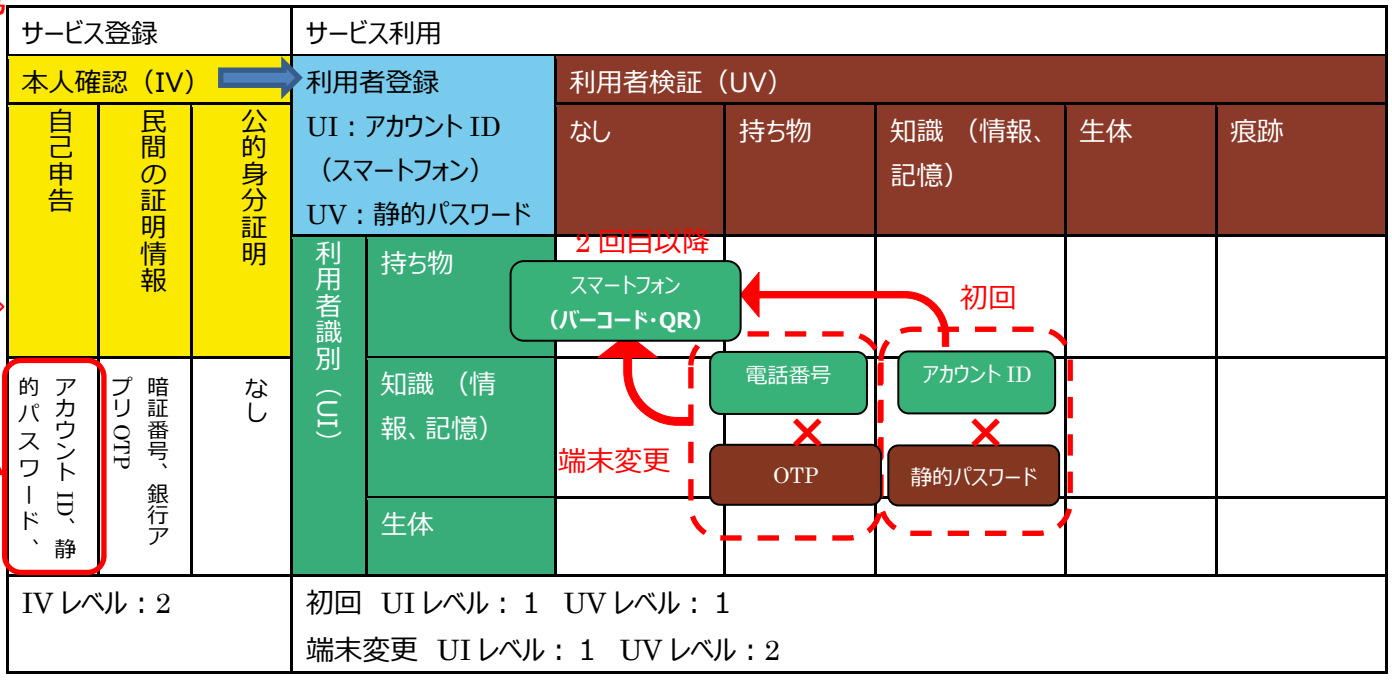


図 26 複数端末からのログインを許可するスマートフォンアプリへの銀行口座チャージ連携分析

② 共通ポイントカード連携

本人確認を行う上で「守るべき資産＝データの場合」とし共通ポイントカード連携の例を記載する。

【ユースケースの概要】

本ユースケースは、コンビニ ATM で現金をチャージして、QR 決済（CPM：Consumer Presented Mode）にて決済できるスマートフォンアプリのサービスに対し、共通ポイントカードを連携する仕組みについて分析する。

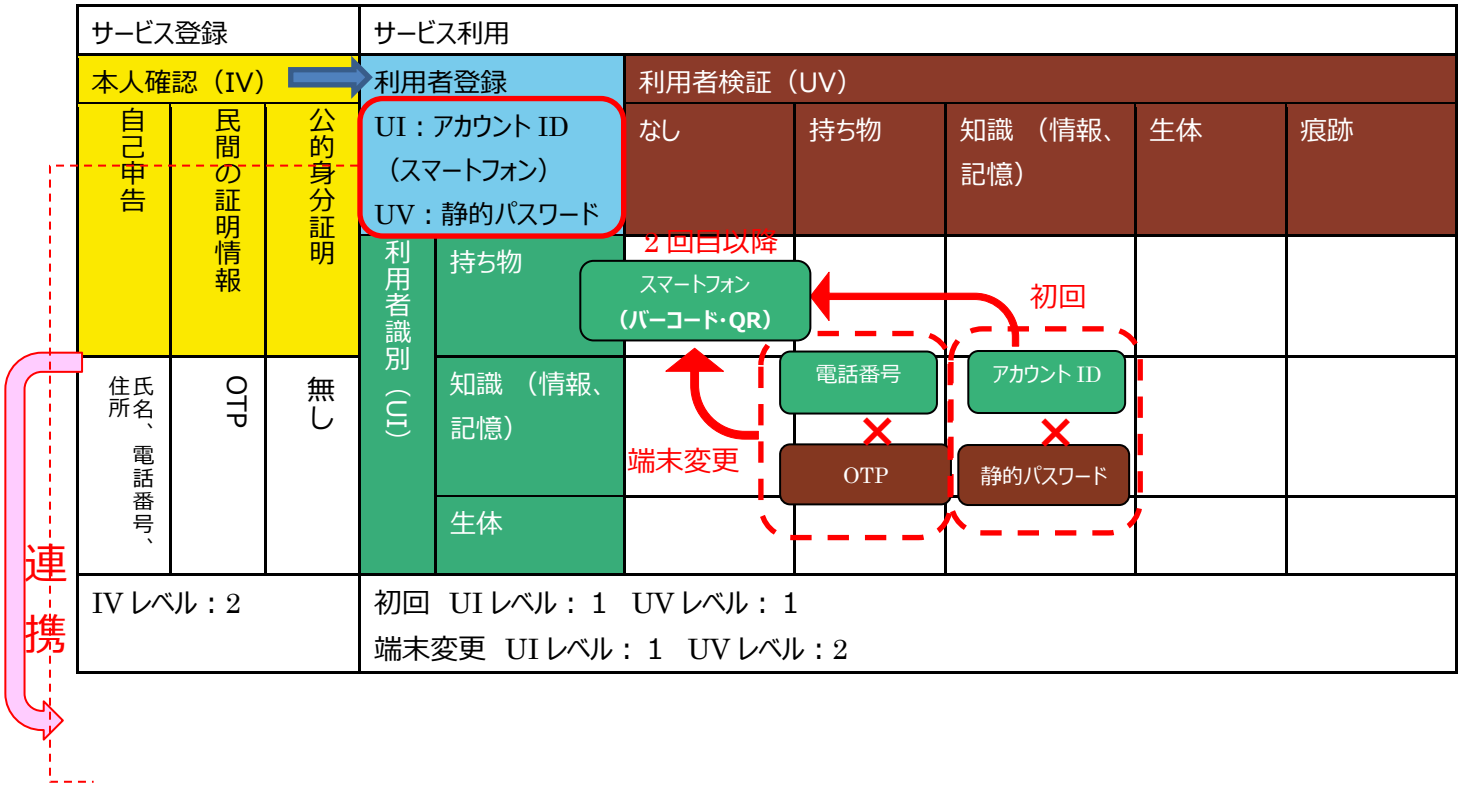
ポイントチャージ、ポイント使用を共通ポイントカードにて実現する。スマートフォン決済は、①の事例の（ロ）のケース同様の事例とする。

このアプリに共通ポイントカードを連携する場合は、本人確認（IV）の際に、連携元のアカウント ID、パスワード及び、共通ポイントカードの ID が自己申告として使用され、民間の証明情報として、共通ポイントカードを生成した際の情報に基づいた検証を実施しているケースもある。例えば SMS 認証等がある。

利用時は、ベースとなるスマートフォンアプリと同様に利便性を重視した運用を取るケースが多い。共通ポイントカードを使用する場合は、スマートフォン決済アプリ上に紐づけられた共通ポイントカードのバーコード等が表示される。

フレームワークに当てはめたものを下記に示す。

スマートフォンアプリサービス登録、利用



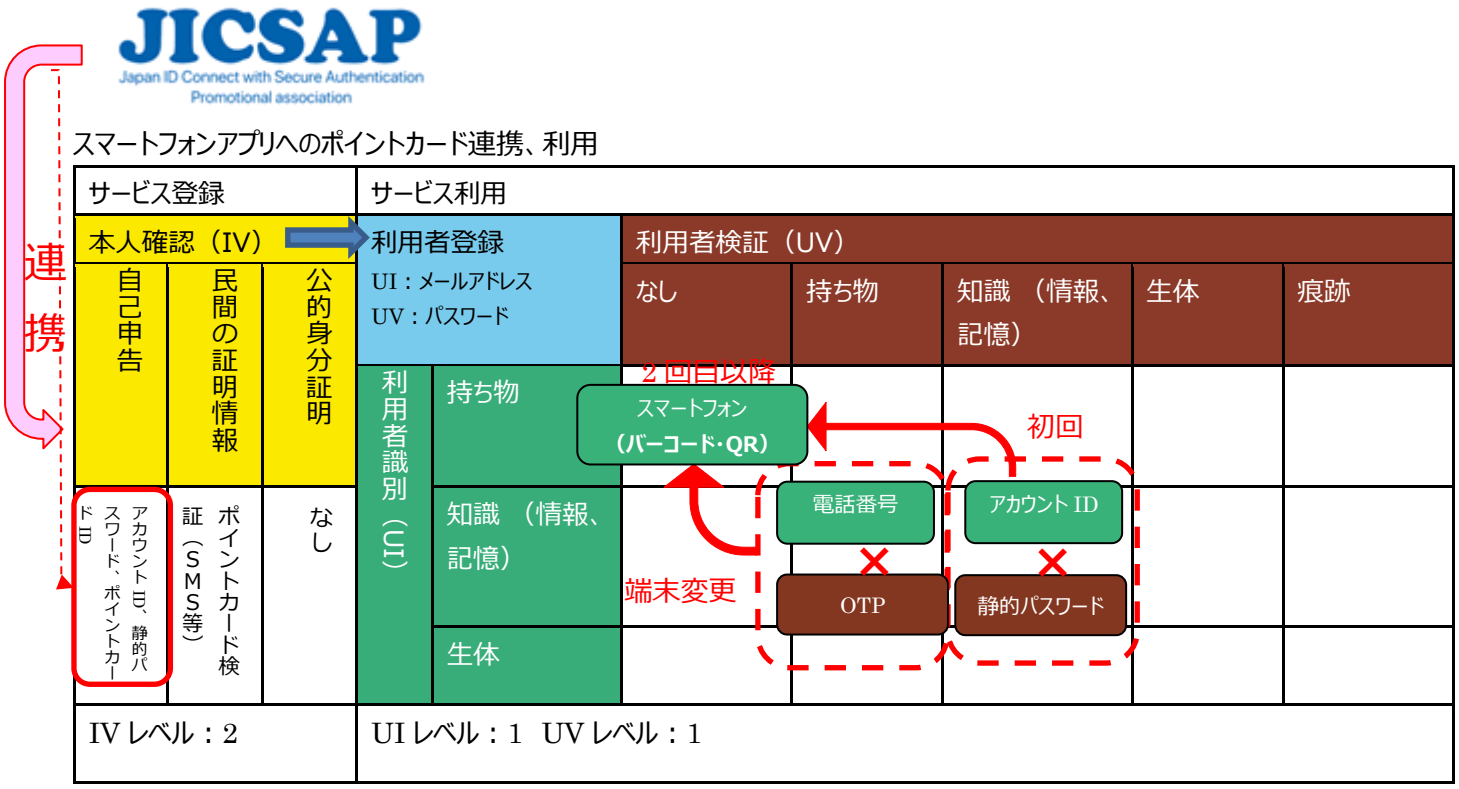


図 27　スマートフォンアプリへのポイントカード連携分析

③　デジタル商品券連携

本人確認を行う上で「守るべき資産＝金銭の場合」としデジタル商品券での例を記載する。

【ユースケースの概要】

本ユースケースは、コンビニ ATM で現金をチャージして、QR 決済（MPM：Merchant Presented Mode）にて決済できるスマートフォンアプリの地域限定サービス（以降、ローカル Pay と表現）に対し、地域活性化のため事前の応募を元に一定のプレミアム率を付与したデジタル商品券をローカル Pay の仕組みを活用して行うサービス連携についての事例を分析する。

【実現したいサービス】

プレミアム率の付与は、1 人 1 回に限定して配布（規約上でローカル Pay は 1 人 1 アカウントまでを制限）

Case 1：メールアドレスのみの本人確認

＜スマートフォン決済＞

本サービスを登録する際には、アプリをインストール後、サービス利用時に使用する 4～8 桁の PIN（暗証番号）の登録、及びメールアドレスによる自己申告を元に、実体性を確認する事で本人確認（IV）がなされる。メールアドレスに対応した利用者識別用の ID がアプリ上で振られる。この時、本人確認（IV）のレベル 1 に分類される。

有資格者の判定を行う際は、アプリを入れたアカウント ID（持ち物）で利用者識別（UI）し、サービス登録時に定めた PIN（暗証番号）（記憶）又は Touch ID/Face ID（生体）を元に、システム上で利用者検証（UV）を行い、店内に掲示された QR コードを読み取る MPM の動作に入る。QR コードを読取った後に支払い金額を入力し、加盟店のスタッフが確認する事で支払いが完了する。決済アプリへのチャージは事前に店舗で行う。

アプリを入れたスマートフォン（持ち物）は、媒体の偽造・改竄は限定的であるレベル：2（中程度の保証）である。あらかじめ定めた PIN（暗証番号）（記憶）は、何らかの手段で利用者検証を行う手段として使用される一般的なものであるため、保証レベル：1(低い保証)となり、Touch ID/Face ID（生体）は、なりすましは限定的であるため、保証レベル 2（中程度の保証）となる。

フレームワークに当てはめたものを下記に示す。

スマートフォン決済（PIN の場合）

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：アカウント ID（スマートフォン） UV：PIN		なし	持ち物	知識（情報、記憶）	生体	痕跡
メールアドレス	なし	なし	利用者識別（UI）	持ち物			アカウント ID × PIN		
				知識（情報、記憶）					
				生体					
IV レベル 1			UI レベル：2　UV レベル：1						

規約で 1 人 1 アカウントにしているが、複数のメールアドレスで登録は可能

図 28　メールアドレスで本人確認するスマートフォン決済の分析

<デジタル商品券>

本サービスを登録する際には、スマートフォン決済アプリをインストールしたスマートフォンのアカウントによる自己申告及び、そのアカウントでデジタル商品券に応募し、当選結果を元に本人確認（IV）がなされる。メールアドレスに対応した利用者識別用の ID による自己申告となるため、ここでも本人確認（IV）のレベル 1 に分類される。

サービス利用時は、スマートフォン決済同様のため説明は割愛する。

フレームワークに当てはめたものを下記に示す。

スマートフォン決済（PIN の場合）

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：アカウント ID（スマートフォン） UV：PIN		なし	持ち物	知識（情報、記憶）	生体	痕跡
メールアドレス	なし	なし	利用者識別（UI）	持ち物			アカウント ID × PIN		
				知識（情報、記憶）					
				生体					
IV レベル 1			UI レベル：2　UV レベル：1						

連携

デジタル商品券（スマートフォン決済連携）

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：アカウント ID（スマートフォン） UV：PIN		なし	持ち物	知識（情報、記憶）	生体	痕跡
アカウント ID	なし	なし	利用者識別（UI）	持ち物			アカウント ID × PIN		
				知識（情報、記憶）					
				生体					
IV レベル 1			UI レベル：2　UV レベル：1						

図 29　メールアドレスで本人確認するスマートフォン決済へのデジタル商品券連携分析

一定のプレミアム率は公平感のため、個人を特定する必要がある。

本ユースケースは、チャージ式であり、チャージバリューから決済されるため、本人特定を求められる仕組みとなるため問題とならなかったが、デジタル商品券として連携された場合に、実現したいサービスである「プレミアム率の付与は、1 人 1 回に限定して配布」に対しては個人の特定が必要であったが、連携の際に「メールアドレス」のみで IV してしまったため、一人が複数アカウントを持つことができてしまった。このように実現したいサービスの目的に対し、連携元のサービス、連携先のサービス全体でサービスモデルを検証する必要がある。

Case 2：メールアドレス及び電話番号認証での本人確認

＜スマートフォン決済＞

本サービスを登録する際には、アプリをインストール後、サービス利用時に使用する 4～8 桁の PIN（暗証番号）の登録、及びメールアドレスによる自己申告に加え、電話番号認証により、実体性を確認する事で本人確認（IV）がなされる。メールアドレスに対応した利用者識別用の ID がアプリ上で振られる。この時、本人確認（IV）のレベル 1 に分類される。

サービス利用時は、Case1 同様のため説明は割愛する。

フレームワークに当てはめたものを下記に示す。

スマートフォン決済

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2">利用者登録
UI：アカウント ID（スマートフォン）
UV：PIN</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td rowspan="2">自己申告</td><td rowspan="2">民間の証明情報</td><td rowspan="2">公的身分証明</td><td rowspan="3">利用者識別（UI）</td><td>なし</td><td>持ち物</td><td>知識（情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td>持ち物</td><td></td><td></td><td>アカウント ID
×
PIN</td><td></td><td></td></tr>
<tr><td>メールアドレス</td><td>電話番号認証</td><td>なし</td><td>知識（情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3"></td><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル 2</td><td colspan="7">UI レベル：2　UV レベル：1</td></tr>
</table>

図 30　メールアドレス＋電話番号で本人確認するスマートフォン決済分析

電話番号認証により、1 人の回線契約数以内に制約する事が可能だが、複数アカウントの保有はまだ可能。

＜デジタル商品券＞

Case 1 同様のため説明は割愛する。

Case 1 と比較し、Case 2 は、電話番号での本人確認が追加となるため、容易に複数のアカウントが作る事は出来るメールアドレスと比較し、デジタル商品券が実現したいサービスである「プレミアム率の付与は、1 人 1 回に限定して配布」に対しては個人の特定が確実に行えるわけではないが、電話番号を複数保有する労力に対するリターンによっては高い効果が期待される。

スマートフォン決済

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：アカウント ID（スマートフォン） UV：PIN		なし	持ち物	知識（情報、記憶）	生体	痕跡
メールアドレス	なし	電話番号認証	利用者識別（UI）	持ち物			アカウント ID × PIN		
				知識（情報、記憶）					
				生体					
IV レベル 2			UI レベル：2 UV レベル：1						

連携

デジタル商品券（スマートフォン決済連携）

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：アカウント ID（スマートフォン） UV：PIN		なし	持ち物	知識（情報、記憶）	生体	痕跡
アカウントID	なし	なし	利用者識別（UI）	持ち物			スマートフォン × PIN		
				知識（情報、記憶）					
				生体					
IV レベル 1			UI レベル：2 UV レベル：1						

図 31 メールアドレス＋電話番号で本人確認するスマートフォン決済へのデジタル商品券連携分析

自己申告のみのため、連携元の IV の強度に依存。電話番号認証を行っているため、一定レベルの抑止力はある。

コラム②：スマートフォンを活用した認証

【ユースケースの概要： SIM の契約・開設】

同じスマートデバイス（スマートフォン）でも本人確認レベルが異なるケースが存在するため、事業者が提供するサービスが求める要求レベルによっては、スマートフォンや、タブレット端末、PC 等での本人認証技術に頼ったサービス設計を行うとリスクを生じる事がある。要因としては、携帯端末の通信用 SIM では本人確認が不十分なケースがあるためである。近年、国内にて審査なしで SIM を契約出来るケースが極端に減っているが、以下に SIM 契約の際の審査あり、無しのケースについて比較してみる。

Case 1：審査なしプリペイド式携帯電話（SIM）※音声なしの例で記載

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2" rowspan="2">利用者登録
UI：SIM
UV：なし</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td>自己申告</td><td>民間の証明情報</td><td>公的身分証明</td><td>なし</td><td>持ち物</td><td>知識 （情報、記憶）</td><td>生体</td><td>痕跡</td></tr>
<tr><td rowspan="3">なし</td><td rowspan="3">なし</td><td rowspan="3">なし</td><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td>SIM
×
なし</td><td></td><td></td><td></td><td></td></tr>
<tr><td>知識 （情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル： 0</td><td colspan="7">UI レベル： 1　UV レベル： 0</td></tr>
</table>

本人確認を実施せずに入手が可能

挿し込めば使える

図 32　審査なしプリペイド式携帯電話（SIM）の分析

Case 2：審査あり携帯電話（SIM）

<table>
<tr><td colspan="3">サービス登録</td><td colspan="7">サービス利用</td></tr>
<tr><td colspan="3">本人確認（IV）</td><td colspan="2">利用者登録
UI：SIM
UV：なし</td><td colspan="5">利用者検証（UV）</td></tr>
<tr><td rowspan="2">自己申告</td><td rowspan="2">民間の証明情報</td><td rowspan="2">公的身分証明</td><td rowspan="3">利用者識別（UI）</td><td>持ち物</td><td rowspan="2">SIM
×
なし</td><td></td><td></td><td></td><td></td></tr>
<tr><td>氏名・年齢等</td><td>なし</td><td>本人確認書類</td><td>知識（情報、記憶）</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3"></td><td>生体</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td colspan="3">IV レベル：3</td><td colspan="7">UI レベル：3　UV レベル：0</td></tr>
</table>

					なし	持ち物	知識（情報、記憶）	生体	痕跡
自己申告	民間の証明情報	公的身分証明	利用者識別（UI）	持ち物	SIM × なし				
氏名・年齢等	なし	本人確認書類		知識（情報、記憶）					
				生体					
IV レベル：3			UI レベル：3　UV レベル：0						

挿し込めば使える

図 33　審査ありプリペイド式携帯電話（SIM）の分析

Case1 も、Case2 も、共にスマートデバイスでの通信は可能で、Case1 は本人認証を行っていないため、同一人物が複数回線を契約した場合でも、本人確認が無いため、提供したいサービスが 1 人 1 アカウントに限定したい場合に抑止力としては弱くなる。一方で、Case2 については契約時に本人確認を行っている事、複数回線を所持する費用以上のリターンを得られるようなサービスでない限りは、期待値として、一定の抑止力になる事が想定出来る。

【ユースケースの概要：スマートフォンで本人認証を行う場合】

本ガイドライン発行時点では、スマートフォン用の OS は大きく 2 種類存在するが、それぞれで本人認証を行うケースは、おおよそ類似している。以下に代表的なパターンについて記載する。

Case 3：スマートフォンの初期登録、利用者検証無しで使用する場合

Case 1：審査なしプリペイド式携帯電話（SIM）※音声なしの例で記載

サービス登録			サービス利用						
本人確認（IV）			利用者登録		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	UI：SIM UV：なし		なし	持ち物	知識（情報、記憶）	生体	痕跡
			利用者識別（UI）	持ち物	SIM × なし				
なし	なし	なし		知識（情報、記憶）					
				生体					
IV レベル：0			UI レベル：1　UV レベル：0						

本人確認を実施せずに入手が可能

挿し込めば使える

又は

Case 2：審査あり携帯電話（SIM）

サービス登録			サービス利用						
本人確認（IV）			利用者登録						
自己申告	民間の証明情報	公的身分証明	UI：SIM UV：なし						
					SIM × なし				
氏名・年齢等	なし	本人確認書類							
IV レベル：3			UI レベル：3　UV レベル：0						

連携

挿し込めば使える

前頁継続

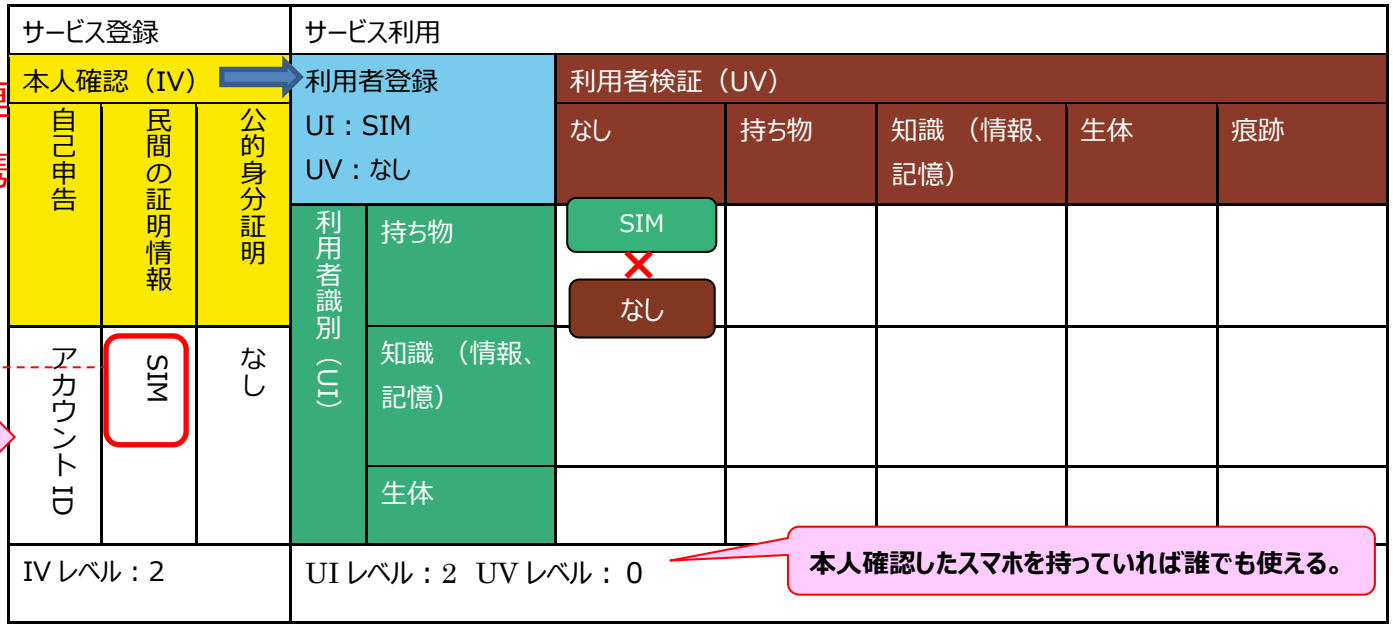


図 34 スマートフォンの初期登録、利用者検証無しで使用する場合の分析

Case 4：スマートフォンの初期登録、暗証番号、パターン認証で使用する場合

Case1 or Case2

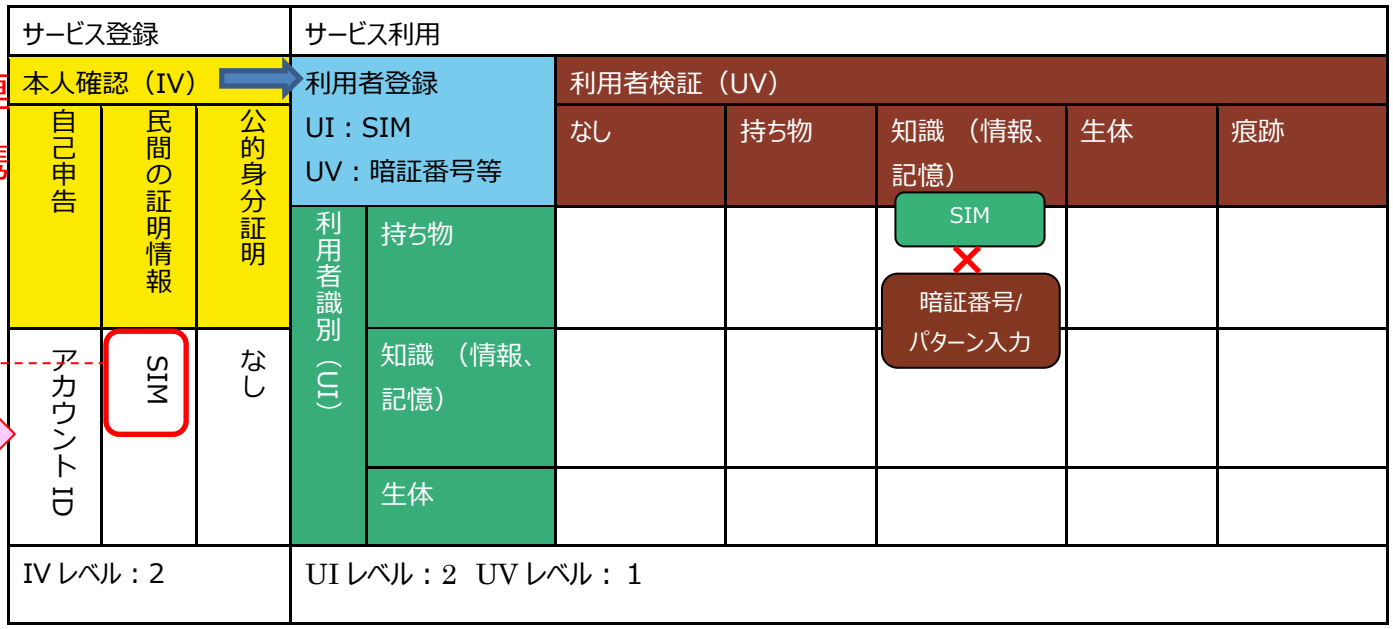


図 35 スマートフォンの初期登録、暗証番号、パターン認証で使用する場合の分析

Case 5：スマートフォンの初期登録、指紋認証/顔認証で使用する場合

連携

Case1 or Case2

サービス登録			サービス利用						
本人確認（IV）			利用者登録 UI：SIM UV：指紋/顔		利用者検証（UV）				
自己申告	民間の証明情報	公的身分証明	利用者識別（UI）		なし	持ち物	知識 （情報、記憶）	生体	痕跡
				持ち物				SIM × 指紋/顔	
アカウントID	SIM	なし		知識 （情報、記憶）					
				生体					
IV レベル：2			UI レベル：2　UV レベル：高						

図 35　スマートフォンの初期登録、指紋認証/顔認証で使用する場合の分析

Case3～5 の通り、スマートフォン側の本人認証レベルはスマートフォンを所持するユーザー側の設定により異なるため、デバイス側で本人を担保する事が難しい。サービス提供者はその事を理解した上でサービスの用途に応じてサービス登録時や、サービス利用時の認証レベルを見直す必要がある。

また、事例集においては、スマートフォンでの認証については上記特性があるためあえて記載しない事とする。

４．　おわりに

本【サービス設計編】では、提供サービスに対し、本人認証技術を適応する際の押さえるべきポイントについて記載し、実例について「JICSAP 本人認証フレームワーク」を用い分析を行ってきた。近年は、自社でクローズした本人認証技術でのサービス提供にとどまらず、他社が提供する既存サービスを活用する等のサービス連携をするケースが多く見られる。本文や、事例にも記載したが、連携するサービスが自社で実現したいサービスレベルを満たしているかどうかについて、事例を参考に「JICSAP 本人認証フレームワーク」を活用して分析頂き、検証頂ければ幸いである。

近年注目されつつある無人店舗やメタバース等の新しい利用シーンにおいても、本人認証技術の実装方法は多様化しつつある。今後も JICSAP 認証技術部会では、様々な事例を通じて得られた知識を既存のガイドラインの改訂や、新規ガイドラインの策定を通して本人認証技術の活用に寄与出来るよう努めていきたい。

５．　用語定義

本ガイドラインにおける用語の定義を記す。

表５ 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。「本人」は「Identity」とも英訳できるが、本ガイドラインでは必ずしも本人認証を必要としない利用者認証を検討範囲に含んでいるため、ここでは「User」と英訳する。	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
利用者登録	サービス利用時に使用する利用者検証（UI）、利用者識別（UV）で使用する手段を登録する。	User Registration
知識（情報、記憶）	【基本知識編】で「記憶」と記載した要素。 第 3 者から与えられる（知り得る）情報と、本人のみが知り得る情報（記憶）の 2 つで構成される。	Something You Know
痕跡	過去の購入履歴、ログインデバイス等、蓄積された本人らしさを示す要素。	Something You Left
GDPR	欧州における一般データ保護規制。個人情報保護の観点で制定された。	General Data Protection Regulation
ハウスカード	自社会員向けサービスで使用する独自カード。「持ち物」に分類される。	House Card
MPM	加盟店が決済用の情報（QR コード等）を提示し、利用者が提示された情報を元に決済を行う方式。	Merchant Presented Mode
CPM	利用者が決済用の情報（QR コード、バーコード等）を提示し、加盟店が提示された情報を元に決済を行う方式。	Consumer Presented Mode

【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：「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」
発行者：一般社団法人キャッシュレス推進協議会
リンク：
原文 https://paymentsjapan.or.jp/wp-content/uploads/2022/02/Fraud_Prevention_Guideline.pdf
発行日：2019 年 4 月発行（Ver.1.0）

文書名：「オンラインサービスにおける身元確認手法の整理に関する検討報告書」
発行者：経済産業省「オンラインサービスにおける身元確認に関する研究会」
リンク：
概要 https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf
原文 https://www.meti.go.jp/press/2020/04/20200417002/20200417002-3.pdf
発行日：2020 年 4 月発行

文書名：「コード決済における不正な銀行口座紐づけの防止対策に関するガイドライン」
発行者：一般社団法人キャッシュレス推進協議会
リンク：
原文　https://paymentsjapan.or.jp/wp-content/uploads/2022/02/Fraud_Prevention_Guidelines_bkac_linked.pdf
発行日：2020 年 9 月発行（Ver.1.0）

文書名：「資金移動業者等との口座連携に関するガイドライン」
発行者：一般社団法人全国銀行協会
リンク：
原文　https://www.zenginkyo.or.jp/fileadmin/res/news/news321130.pdf
発行日：2020 年 11 月発行

文書名：「犯罪収益移転防止法の概要」
発行者：JAFIC 警察庁刑事局組織犯罪対策部組織犯罪対策企画課犯罪収益移転防止対策室
リンク：
原文　https://www.npa.go.jp/sosikihanzai/jafic/hourei/data/hougaiyou20211122.pdf
発行日：2021 年 11 月時点版

文書名：「eKYC 導入指針」
発行者：一般社団法人キャッシュレス推進協議会
リンク：
原文 https://paymentsjapan.or.jp/wp-content/uploads/2022/02/eKYC_ImplementationGL_v1.0-1.pdf
発行日：2021 年 12 月発行（Ver.1.0）

文書名：「クレジットカード･セキュリティガイドライン [3.0 版]」
発行者：クレジット取引セキュリティ対策協議会（事務局：一般社団法人日本クレジット協会）
リンク：
原文　https://www.j-credit.or.jp/download/news20220309b1.pdf
概要　https://www.j-credit.or.jp/download/news20220316a1.pdf
発行日：2022 年 3 月

文書名：「EMV 3-D セキュア導入ガイド」
発行者：クレジット取引セキュリティ対策協議会（事務局：一般社団法人日本クレジット協会）
リンク：
原文　https://www.j-credit.or.jp/download/news20220309b1.pdf
概要　https://www.j-credit.or.jp/download/news20220309b7.pdf
発行日：2022 年 9 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　（～2022 年 6 月）
	原　弘樹	東芝インフラシステムズ株式会社　（2022 年 6 月～）
（リスク検討 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
（評価検討 WG 主査）	宮 崎　学	株式会社デンソーウェーブ
	梅 本 正 敏	株式会社エヌ・ティ・ティ・データ
	後 藤 敏 宏	オムロン ソーシアルソリューションズ株式会社
	浜 崎 桂 介	オムロン ソーシアルソリューションズ株式会社
	桑久保　恵	共同印刷株式会社
	広 川 知 剛	共同印刷株式会社
	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
	阿 部 友 紀	株式会社ジェーシービー
	平 山　純	株式会社ジェーシービー
	石 川 勝 章	大日本印刷株式会社
	小野寺 裕 哉	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
	中 村 裕 也	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

＊2020 年 1 月 23 日（木）～2022 年 11 月 10 日（木）までの全 35 回、本ガイドライン策定に係る活動として、「JICSAP 認証技術部会付け『評価検討 WG』『脅威分析 WG』」を開催した。

＜2019 年度＞

2020 年 1 月 23 日（木）	10:00～12:00	部会・合同 WG（第 1 回）
2020 年 2 月 27 日（木）	10:00～12:00	部会・合同 WG（第 2 回）
2020 年 3 月 26 日（木）	10:00～12:00	部会・合同 WG（第 3 回）

＜2020 年度＞

2020 年 4 月 16 日（木）	9:00～11:00	部会・合同 WG（第 4 回）
2020 年 5 月 21 日（木）	10:00～12:00	部会・合同 WG（第 5 回）
2020 年 6 月 25 日（木）	9:00～11:00	部会・合同 WG（第 6 回）
2020 年 7 月 14 日（火）	10:00～12:00	部会・合同 WG（第 7 回）
2020 年 7 月 30 日（木）	9:00～11:00	部会・合同 WG（第 8 回）
2020 年 9 月 3 日（木）	9:00～11:00	部会・合同 WG（第 9 回）
2020 年 9 月 9 日（水）	9:00～11:00	部会・合同 WG（第 10 回）
2020 年 10 月 8 日（木）	9:00～11:00	部会・合同 WG（第 11 回）
2020 年 11 月 12 日（木）	9:00～11:00	部会・合同 WG（第 12 回）
2020 年 12 月 23 日（水）	9:00～11:00	部会・合同 WG（第 13 回）
2021 年 1 月 28 日（木）	9:00～11:00	部会・合同 WG（第 14 回）
2021 年 3 月 4 日（木）	10:00～12:00	部会・合同 WG（第 15 回）

＜2021 年度＞

2021 年 4 月 8 日（木）	10:00～12:00	部会・合同 WG（第 16 回）
2021 年 5 月 6 日（水）	10:00～12:00	部会・合同 WG（第 17 回）
2021 年 6 月 3 日（木）	10:00～12:00	部会・合同 WG（第 18 回）
2021 年 7 月 8 日（木）	10:00～12:00	部会・合同 WG（第 19 回）
2021 年 8 月 5 日（木）	10:00～12:00	部会・合同 WG（第 20 回）
2021 年 9 月 9 日（木）	10:00～12:00	部会・合同 WG（第 21 回）
2021 年 10 月 7 日（木）	10:00～12:00	部会・合同 WG（第 22 回）
2021 年 10 月 14 日（木）	10:00～12:00	部会・合同 WG（第 23 回）
2021 年 11 月 11 日（木）	10:00～12:00	部会・合同 WG（第 24 回）
2021 年 12 月 16 日（木）	10:00～12:00	部会・合同 WG（第 25 回）
2022 年 1 月 6 日（木）	11:00～12:00	部会・合同 WG（第 26 回）
2022 年 2 月 3 日（木）	10:00～12:00	部会・合同 WG（第 27 回）
2022 年 3 月 3 日（木）	10:00～12:00	部会・合同 WG（第 28 回）

JICSAP
Japan ID Connect with Secure Authentication Promotional association

<2022 年度>

2022 年 4 月 7 日（木）	10:00～12:00	部会･合同 WG（第 29 回）
2022 年 5 月 12 日（木）	10:00～12:00	部会･合同 WG（第 30 回）
2022 年 6 月 2 日（木）	10:00～12:00	部会･合同 WG（第 31 回）
2022 年 7 月 7 日（木）	10:00～12:00	部会･合同 WG（第 32 回）
2022 年 9 月 1 日（木）	15:00～17:00	部会･合同 WG（第 33 回）
2022 年 10 月 6 日（木）	10:00～12:00	部会･合同 WG（第 34 回）
2022 年 11 月 10 日（木）	10:00～12:00	部会･合同 WG（第 35 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
【サービス設計編】
第 1.0 版

発行者：　一般社団法人 ID 認証技術推進協会
（JICSAP）
発行日：　2022 年 12 月 20 日