



マイナンバーカード・デジタルIDによる金融DXのこれから

xID株式会社

2023年10月26日

自己紹介



日下 光
HIKARU KUSAKA



xID株式会社 代表取締役CEO

マイナンバーカードに特化したデジタルIDソリューション「xID(クロスアイディ)」を提供するGovtech企業



一般社団法人Govtech協会 代表理事

公共調達だけでなく、多様な官民での共創による公共・行政分野のデジタル化を推進するための政策提言等を行う団体



デジタルアイデンティティ推進コンソーシアム

一般社団法人デジタルアイデンティティ推進コンソーシアム 理事

JPKI・デジタルアイデンティティの官民利活用推進やアーキテクチャ整備を支援する業界団体

その他の取り組み、役割

浜松市デジタルスマートシティフェロー

茨城県日立市デジタル化推進・評価委員

神奈川県鎌倉市スマートシティ推進参与

IPA(DADC)専門委員

2023年度 総務省地域情報化アドバイザー

xID株式会社のご紹介

xIDは、日本初のマイナンバーカードに特化したデジタルIDソリューションを提供するGovtech企業です

総務大臣認定の公的個人認証サービスを提供する事業者として、2020年4月から日本初となる民間デジタルIDサービスに特化した事業者として、大企業を中心にさまざまな事業者と連携

会社情報

会社名 xID株式会社 (クロスアイディ)

設立年月日 2012年5月28日

代表者 代表取締役CEO 日下 光

資本金 259,590,400円

社員数 43名(非常勤含む)

拠点 本社: 東京都千代田区内幸町2丁目1-6
日比谷パークフロント19F
サテライトオフィス: 香川県高松市(かがわDXラボ内)

事業 マイナンバーカードに特化した総合デジタルIDソリューション開発基盤の提供

※2023年8月現在

加盟団体など

国際標準仕様に準拠した開発



国内初となるJPKI活用推進の業界団体としてデジタル庁と連携し、JPKIのさらなる利活用に向けたアーキテクチャ整備を支援



雑誌・メディアの紹介

行政関連機関誌や一般メディアなどでもマイナンバーカードに特化した事業者として注目



自治体導入実績

マイナンバーカード活用サービスとして、No.1の自治体導入実績

マイナンバーカードと連携したデジタルIDアプリを提供するパイオニアとして、2020年4月からマイナンバーカードを活用した取り組みを自治体と展開



導入自治体数
417
自治体
全国1788自治体のうち



※2023年6月現在

デジタルIDの活用を広げる、戦略的パートナーシップ(業務資本提携含む)

事業シナジーのある各分野の実績あるパートナー企業とのパートナーシップ(出資含む)で、デジタルIDによる課題解決、付加価値創出を推進

MS&AD

あいおいニッセイ同和損保

業務提携

SAISON
Ventures

業務資本提携

 **SCALA**

業務資本提携

 **SOMPO LIGHT VORTEX**

業務資本提携

 **DGFT**
DG Financial Technology

業務提携

 **横浜銀行**

Hamagin DG Innovation Fund

業務資本提携

 **SMBC**
三井住友銀行

業務資本提携

 **両備システムズ**

業務資本提携

身分証の写真をアップロードするタイプの本人確認の課題

画像だけでは身分証の偽造は検証できないため、身元の偽装は容易

身元確認は本人確認書類の真正性検証(validation)と、提示された本人確認書類と当該本人が一致しているかの検証(verification)の2つのプロセスから成立するが、我が国で一般的に利用されている画像解析型eKYCには、validationのプロセスがなく、身元確認の意味をなしていない。(本来はvalidationプロセスとして、発行者台帳との照合等が必須とされているが、民間企業がこれを行う方法がないため黙認され、骨抜きとなっている)

法令で求めている = 安全ではない

犯罪収益移転防止法は、特定取引時に本人確認を行い、その証跡を一定期間保管することを金融機関等に求めているが、法令で本人確認の強度を保証している訳ではない。(赤信号を無視するのは違法であるが、赤信号で交差点の安全性を保障している訳ではなく、悪意をもって信号を無視することは容易であるのと同じ)

また、そもそも現状の犯収法ではFATF勧告における顧客調査措置(CDD)の履行が不十分と指摘されており、電子署名(マイナンバーカード)を活用したより強固な身元確認プロセスへの移行が想定されているなかで、eKYCは過渡期の技術として近い将来淘汰されてゆくものと考えられている。

出典:毎日新聞(2019/1/12)



偽造 発行機関も区別できない本物の高い品質にこだわります! のことならお任せください!

- 業界NO1を誇る信頼のお店
- 納品前に構成確認が出来る!
- 満足まで何回も修正可能! **だから安心!**

詐欺は根絶しています。専門家と設備を揃えてあり、本日本国内の郵便局から発送し、顧客に追跡番号を連絡す

ネット上にあふれる偽造身分証販売サイトの例

JPKI利活用による社会課題の解決 – 目視確認による本人確認手法の限界-

ホーム > ニュース > 社会

SIMカード再発行でスマホ乗っ取り、不正送金...男2人を全国初逮捕

2023/02/23 14:10

 この記事をスクラップする   

不正入手したスマートフォンの通信用SIMカードを使い不正送金したとして、愛知県警は22日、自称自営業の男(27)(神奈川県寒川町)、飲食店店員の男(38)(東京都台東区)の両被告(詐欺罪などで起訴)を、不正アクセス禁止法違反と電子計算機使用詐欺の疑いで再逮捕した。



愛知県警察本部

他人になりすましてSIMカードを再発行させてスマホを乗っ取り、不正送金などを行う手口は「SIMスワップ」と呼ばれ、被害は世界で広がりつつある。県警によると、国内で不正送金に関与した疑いによる逮捕は全国初という。

発表では、2人は昨年7月、仲間と共謀し、大阪府の40歳代男性名義で再発行したSIMカードを利用し、スマホを使って金融機関のアプリに不正にログイン。男性名義の口座から約600万円を両被告らの管理する口座に送った疑い。

両被告は、**偽造した運転免許証を使って被害男性のSIMカードを再発行させた**として、詐欺罪などで起訴されている。

出典：読売新聞オンライン

「警察官でも気づけないほど精巧に偽造」18年間 無免許運転の男(51)を逮捕【長崎】

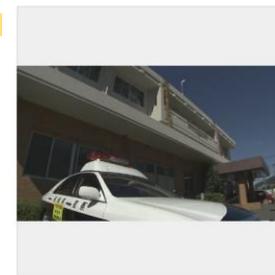
2/20(月) 14:06 配信  72   

 NBC長崎放送

無免許で車を運転中に携帯電話を利用した上、**偽造された運転免許証を提示した疑い**で、福岡県の51歳の男が逮捕されました。

男は18年間、無免許で運転していたということです。

[【写真を見る】「警察官でも気づけないほど精巧に偽造」18年間 無免許運転の男\(51\)を逮捕【長崎】](#)



長崎放送

逮捕されたのは、福岡県福岡市の51歳の会社員の男です。

警察によりますと、2021年7月、長崎県時津町の国道206号で、交通取り締まり中の警察官が『携帯電話を見ながら軽乗用車を運転』していた男を発見。停車させ、運転免許証の提示を求めたところ、**「偽造された免許証」を提示した**ということです。

警察によりますと、**『警察官も一見して分からないような精巧に偽造された免許証』**だったため、その場は「携帯電話使用等」で交通反則告知書(青切符)の交付を行いました。

その後、警察で『交通違反の登録』を行う際に、本人の名前と免許証番号が異なることが分かったということです。

出典：Yahoo!ニュース

AIを悪用した不正や詐欺がすでに実在

YAHOO! JAPAN ニュース IDでもっと便利に新規取得 ログイン 誰でもZOZOTOWNが+10%お得に

キーワードを入力 | Q

トップ 速報 ライブ 個人 オリジナル みんなの意見 ランキング
主要 国内 国際 経済 エンタメ スポーツ IT 科学 ライフ 地域

AIがビデオ通話で「友達」になりすまし。会社社長が8500万円の振り込み詐欺被害：中国

5/30(火) 11:41 配信 10



中国でAIを悪用した振り込み詐欺事件が発生した

中国でこのほど、人工知能（AI）を悪用した振り込み詐欺事件が発生した。犯人はAIを使って実在の人物の顔と声を複製して被害者の友人になりすまし、わずか10分弱で430万円（約8500万円）をだまし取った。

警察によると、被害に遭った福建省福州市のテック企業の経営者A氏は4月20日午前11時40分、SNSアプリの微信（WeChat）で連絡してきた友人とビデオ通話を始めた。ちょっとした会話の後、友人は「知り合いが入札の保証金として430万円を必要としているが、法人口座同士で口座

振替手続きをしないとならない。あなたの会社の法人口座を利用させてくれないか？」と切り出した。

A氏がなんの疑いもなくキャッシュカードの番号を伝えると、友人は「お金はもうあなたの口座に振り込んだよ」と言って、振込み伝票のスクリーンショットを送ってきた。A氏は着金を確認することなく、11時49分に430万円を2回に分けて指定された口座に振り込んだ。

出典: Yahoo!ニュース
<https://news.yahoo.co.jp/articles/3dbf2c210df467745a020702a2d2eaf53eaf5d7f>

1F2-GS-10a-02

The 35th Annual Conference of the Japanese Society for Artificial Intelligence, 2021

Deepfakeを用いたe-KYCに対するなりすまし攻撃と対策の検討 Research on a Deepfake based spoofing attack for e-KYC and its countermeasures.

川名のん 長沼 健 吉野 雅之 太田原 千秋 富樫 由美子 笹 晋也 山本 恭平
Non Kawana Ken Nagamura Masayuki Yoshino Chiaki Otahara Yumiko Togashi Shinya Sasa Kyohei Yamamoto

株式会社日立製作所 研究開発グループ
Hitachi, Ltd. Research & Development Group.

e-KYC: electric-Know Your Customer is Internet for opening an account at a bank. Also to see if it is possible to spoof a user authentic made an original e-KYC application based on application requests random actions, such as the experiment, the spoofing attack was successful. Also, we summarize some countermeasures.

1. はじめに

Deepfakeとは、Deep learning（深層学習）とFakeされたデータで、機械学習の技術を用いて、動画を別の人物の顔に差し替える技術のことである。だけでなく音声にも技術が適用され、偽の映像、音によって生成することが可能である。また、DeepfakeやソースコードはGitHub上に一般公開されてお技術やノウハウを習得できる。

Deepfakeによって生成された偽の映像は極めて本物の映像と区別することが難しく、これによる様々な問題が発生する。例えば著名人にながら行うことによる政治上的印象操作や、既存の動画を振り付けることによる人権侵害などが深刻な存在。2020年10月には、Deepfake技術を用いて偽販売していたことによる人権侵害として、日本国内人が逮捕された。彼らはインターネットで入手した数々の動画を生成していき、これを偽の人物として利用するための数値の低さがわかる。

本稿では、Deepfakeが金融機関で行われる非本人確認 e-KYC に対する脅威になりえるかを用いて検証した結果を述べる。具体的な方法は、行われている e-KYC を参考しつつ、スマートを用いた顔認証を行う模擬 e-KYC アプリを作成し、Deepfake を生成するソフトを用いてなりすまし攻撃が可能かを実験した。実験が作成した模擬 e-KYC アプリに対しては、実際になりすまし攻撃が成功したことを確認した。このことは、Deepfake に対して現実的な脅威である事を示しており、必要とする。本稿では、現状考えられる e-KYC 対策についても提案する。

連絡先: 川名のん, 株式会社日立製作所 研究開発グループ
システムイノベーションセンター, non.kawana.by@hitachi.com

1F2-GS-10a-02

The 35th Annual Conference of the Japanese Society for Artificial Intelligence, 2021

ンク部分で顔と口唇の動きを検出する効果も期待される。
• 生体認証との連携
Deepfake に関わらず、一般的ななりすまし攻撃技術である、スマートフォンや専用デバイスを用いた顔認証などの生体情報と本人を結びつけることにより、結果に本人のみが申請でき、本人の確認も確実にできる。
• SIM 番号登録
このなりすまし攻撃の対策になる。犯罪者を目的として口唇認証するユーザは、複数の口座を開設する事が予想される。スマートフォンの SIM 番号を登録することで、SIM カードを変えない限り一生につき一日限のみしか

6. おわりに

本稿の実験では、実際の e-KYC システムではなく、独自に作成した模擬的 e-KYC システムを用いてなりすまし攻撃を行った。また、Deepfake 技術は Avatarify という、顔写真1枚で人物になりすますことができる OSS を用いた。実験のシナリオとしては、Avatarify を用いて他人になりすまし、e-KYC の本人確認を突破、不正に口座を作成する、というものである。本稿では本人容貌の撮影を、運転免許証の持ち主でない人物が Avatarify を用いて当該人物になりすました顔で撮影し、運転免許証の顔と照合が成功するか実験を行った。この撮影の際には、なりすました顔をモニターに表示させ、それをスマートフォンのインカメラで撮影する手法を取った。
本実験の結果、なりすました顔が運転免許証の人物であると判定され、なりすまし攻撃が成功した。これにより e-KYC で他人になりすまし、金融機関において不正に口座を作成するという脅威が現実的なものであると分かった。
さらに本稿では、対策技術の検討も行った。今後は検討した対策技術の実装および、それを用いて再度の実験、および評価を行う必要がある。

参考文献

- [1] 金融庁「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」の公表について、<https://www.fsa.go.jp/news/30/somote/20181130/20181130.html>
- [2] R. Tolouani, R. V. Rodriguez, J. Fierrez, A. Morales and J. O. Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection," arXiv: 2001.00179 [cs.CV], 2020.
- [3] Facewap, <https://github.com/Deepfakes/facewap>
- [4] DeepFoolish, <https://github.com/josiah/DeepFoolish>
- [5] Avatarify, <https://github.com/ailevk/avatarify>
- [6] A. Siamini, S. Lathuillière, S. Tulyakov, E. Ricci, N. Sebe, "First Order Motion Model for Image Animation," arXiv: 2003.08036 [cs.CV], 1 Oct 2020.
- [7] MTCNN, <https://github.com/ipazc/mtcnn>
- [8] InsightFace, <https://github.com/deepinsight/insightface>
- [9] Y. Li, M.-C. Chang, S. Lyu, "No One Knows: Detecting AI Generated Fake Videos by Detecting Eye Blinking," 2018 IEEE International Workshop on Information Forensics and Security (WIFS), 2018.
- [10] Microsoft, New Steps to Combat Disinformation, <https://blogs.microsoft.com/on-the->

6. おわりに

本稿の実験では、実際の e-KYC システムではなく、独自に作成した模擬的 e-KYC システムを用いてなりすまし攻撃を行った。また、Deepfake 技術は Avatarify という、顔写真1枚で人物になりすますことができる OSS を用いた。実験のシナリオとしては、Avatarify を用いて他人になりすまし、e-KYC の本人確認を突破、不正に口座を作成する、というものである。本稿では本人容貌の撮影を、運転免許証の持ち主でない人物が Avatarify を用いて当該人物になりすました顔で撮影し、運転免許証の顔と照合が成功するか実験を行った。この撮影の際には、なりすました顔をモニターに表示させ、それをスマートフォンのインカメラで撮影する手法を取った。

本実験の結果、なりすました顔が運転免許証の人物であると判定され、なりすまし攻撃が成功した。これにより e-KYC で他人になりすまし、金融機関において不正に口座を作成するという脅威が現実的なものであると分かった。

さらに本稿では、対策技術の検討も行った。今後は検討した対策技術の実装および、それを用いて再度の実験、および評価を行う必要がある。

デジタル社会の実現に向けた重点計画(案)抜粋

- 下記資料内の2.カードの機能向上③では本人確認手法のカードへの一本化が記載されている。
- これらを鑑み今後は犯罪収益移転防止法並びに携帯電話不正利用防止法における本人確認では(ホ)(ハ)などの本人確認方法は利用が難しくなる可能性が考えられる

安全・安心で便利な国民生活に向けたマイナンバーカードの機能拡充と安全安心対策

基本的な考え方

- マイナンバーカードは、確実・安全な本人確認・本人認証ができる「**デジタル社会のパスポート**」。
- カードの機能拡充に向け、**①カードの利便性向上、②カードの機能向上、③安全・安心対策の3本柱**にそって施策を推進する。
- マイナンバーカードへの理解を促進し、**希望する全ての国民が取得できるよう、円滑にカードを取得していただくための申請環境及び交付体制の整備を促進する。**

マイナンバーカード累計の申請件数

令和5年5月末	9,705万件
令和4年5月末	5,880万件
前年同期比	+3,824万件

3本柱

(「デジタル社会の実現に向けた重点計画(案)」に掲載された主な施策)

1. カードの利便性向上	2. カードの機能向上	3. 安全安心対策と取得環境整備
<p>① 各種カードとの一体化</p> <ul style="list-style-type: none"> 健康保険証 運転免許証 医療費助成制度受給者証/接種券/乳幼児健診等受診券/母子健康手帳 在留カード <p>② 簡素化、利便性向上</p> <ul style="list-style-type: none"> 介護保険証のペーパーレス化 ハローワークでの受付のペーパーレス化 「ねんきん定期便」のマイナポータルでのプッシュ通知 スマホで障害者手帳情報を利用できる民間サービスの普及 大学キャンパスのデジタル化・デジタルガバメント教育の充実 カードの利活用を中心に、地域のデジタル実装の優良事例を支えるサービス/システムをカタログ化 オンライン市役所サービスの充実 <p>③ スマートフォンへの搭載</p> <ul style="list-style-type: none"> 本年5月の電子証明書機能のAndroid端末への搭載に続き、iOS端末への搭載について実現検討 スマホによる健康保険資格確認 モバイル運転免許証 	<p>① 次期カードの検討開始</p> <ul style="list-style-type: none"> 2026年中を視野に次期カードの導入を目指す (「次期マイナンバーカードタスクフォース」を設けて検討。法改正が必要な場合は次期通常国会への提出を目指す。) <検討事項> 券面デザイン 券面記載事項(性別、マイナンバー、仮名、国名、西暦等) 電子証明書の有効期間(5年)の延長 早期発行体制の構築 カードの公証名義 <p>② カード更新のオンライン化</p> <ul style="list-style-type: none"> 成人以降のカード更新を完全オンライン化できないか、カードに要求される身元確認保証レベル等について整理の上、更に詳細を検討 <p>③ 本人確認手法のカードへの一本化</p> <ul style="list-style-type: none"> 犯収法、携帯電話不正利用防止法に基づく本人確認手法は、カードの公的個人認証に原則一本化。 本人確認書類のコピーはとらない 	<p>① カードの安全安心対策</p> <ul style="list-style-type: none"> カードを活用するサービスのトラブルに関して、デジタル庁が中心となり、関係府省庁等が連携して、効果的な情報共有や対策の調整、一丸となった情報発信を行うことにより、互全の対策を迅速かつ徹底して実施 その際、事案に関するデータやシステムの総点検や新規データの誤登録の防止策の徹底を実施。人為的ミスリスクを低減させるため、人が介在する機会を減少させるようデジタル化の取組を推進 個別事案に対して、徹底した点検・再発防止 コンビニ交付サービスにおける誤交付 保険証の紐づけ誤り 公金受取口座の誤登録 マイナポイントの誤紐づけ <p>② カードの取得環境の整備</p> <ul style="list-style-type: none"> 施設職員や支援団体等の支援によるカードの代理交付・申請補助等 市町村による施設等への出張申請受付 郵便局におけるカードの申請

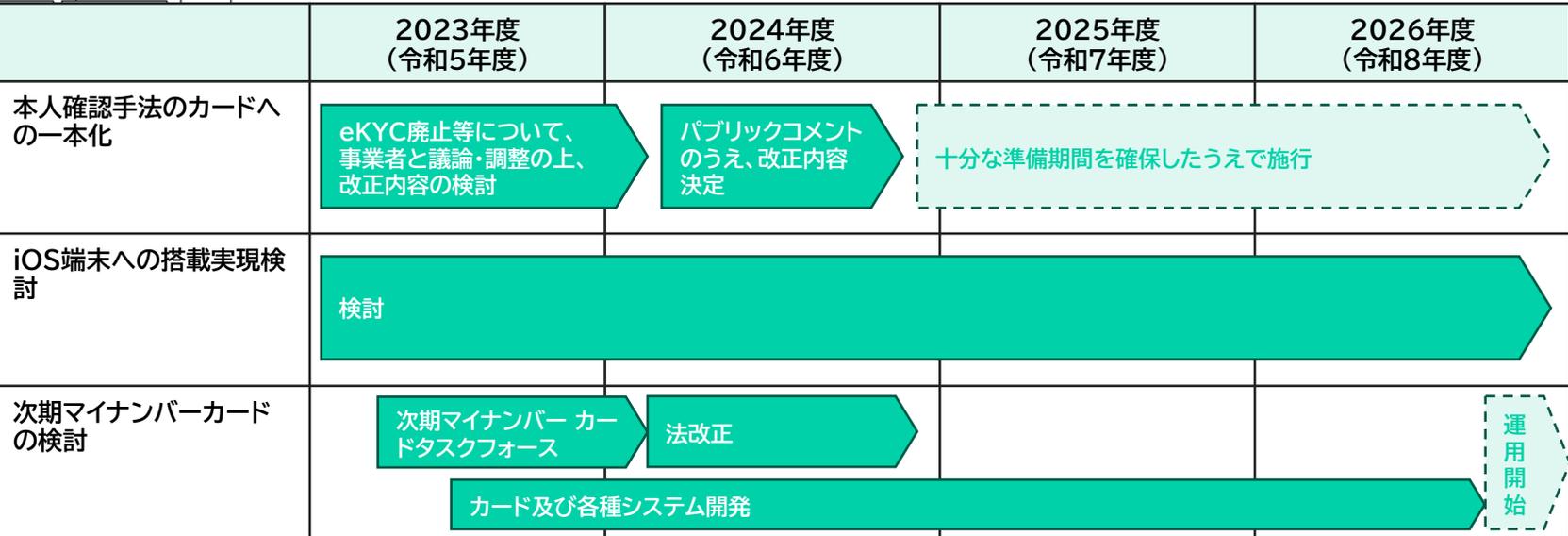
2

※<https://www.digital.go.jp/councils/social-promotion/38606249-07b3-4176-a538-58e0c64a488>

デジタル社会の実現に向けた重点計画で示された工程表

安全・安心で便利な国民生活に向けたマイナンバーカードの機能拡充と安全安心対策 工程表 ※赤字は新規		実施済み の事項	2022年度 (令和4年度)	2023年度 (令和5年度)	2024年度 (令和6年度)	2025年度 (令和7年度)	2026年度 (令和8年度)	省庁	
各種 カードとの 一体化	健康保険証	保険医療機関等のオンライン 資格確認の単別義務化 (導入に準備期間として、 カードを診察券として代用す ることが仕組みとして可能)	保険医療機関等の オンライン資格確認の 原則義務化	医師等、柔道整復 師、中級・初級 師、中級・初級 師のオンライン 資格確認の義務	運用開始	令和6年度 保険証廃止		デジタル庁 総務省 厚生労働省	
	運転免許証	全国共通の運転者管理シ ステムの整備 (→令和4年 12月) 改正運交法が成立 (令和 4年4月)	国庫の運転者管理シ ステムの移行 一体化に必要なシステム改修	運用開始	令和6年度 運転免許証とマイナンバーカードの 一体化			警察庁	
	医療費助成制度受給者証 /接種券/乳幼児健診等 受診券/母子健康手帳	マイナンバーでの接種歴の 履歴 乳幼児健診等の結果のマ イナンバーでの提供 (令和2年6月~)	実証 (医療費助成制度 接種券/乳幼児健診 等受診券)	令和5年度中に、希望する自治体で実施 職次、機能・実施自治体を拡大し、全国的に運用					デジタル庁 厚生労働省 こども家庭庁
	在留カード		検討	法案提出 準備 (政省令、システム整備等)					
カードの 利便性向上	介護保険証のペーパーレス 化			共有すべき情報等の 検討・見直し	システム開発	先行			
	ハローワークでの受付のペ ーパーレス化	令和4年10月よりロー ワークでのマイナンバーカード 受付システムの利用開始		マイナンバーカード受付システムの運用開始	原則ハローワーク				
	「ねんきん定期便」のプッシュ 通知			システム開発・構築等					
	スマホで障害者手帳情報を 利用できる民間サービスの 普及	マイナンバー連携を活用し、 スマートフォンアプリやア プレットで手帳情報を簡単に 利用することが、民間の仕組 みにより可能。	障害者手帳情報 のデジタル化等	インターネット予約対応 手帳情報を簡便に利用できる民間の仕組みの活用方 情報提供による要					
	大学キャンパスのデジタル 化・デジタルガバメント教育 の充実	活用に関する先進事例の 周知 (令和5年2月~) デジタルキャンパスに関する 中期目標・中期計画への記載 (令和4年4月~)	先進事例の大学への周知	国立大学法人の中期目標・中期計画への記載	授業で使える動画の作成・周知・各学校における活用				
	優良事例を支えるサービス/ システムをカタログ化			カタログ 第1版 仕様書	カタログ・モデル仕様書の 充実	DN			
	オンライン市役所サービス (マイナンバーからの各種 手続)の充実	引継ぎ手続オンラインサービス (令和5年2月~) バネポート実用申請 (令 和5年3月~)		手数料等支払い (令和5年8月頃)・履歴 ・公的年金等の扶養利率等申告書提出 (令 和5年2月~) 生活保護受給給付金の差別情報照 マイナンバーの活用					
	スマホへの搭載について実 現検討				検討				
	スマホによる健康保険資格確 認	資格実務情報等のオ ンライン資格確認の 後継義務化		スマホからの資格 確認の構築					
	モバイル運転免許証	調査研究の実施 (令和5 年3月報告書取りまとめ)	諸外国の調査研究の 実施	デジタル資格実証・開発する際の資格者証等も搭載 運用の検討も実施 ・マイナンバーカードと運転免許証の一体化の運用開始					
カードの 機能向上	次期マイナンバーカードの検討			次期マイナン カードタスクフォース	法改正			デジタル庁 総務省	
	カード更新オンライン化の検討			完全オンライン化できないか、更に詳細を検討				デジタル庁 総務省	
	本人確認手法のカードへの一本化			eKYC廃止等について、 事業者と議論・調整の上、 改正内容の検討	パブリックコメン トのうえ、改正 内容決定	十分な準備期間を確保したうえで施行		デジタル庁 総務省 金融庁等	
	インシデント体制の強化								

- 今年度内に画像解析型eKYCの廃止等に向けて検討
- 来年度には改正内容を決定
- 25年度より移行期間を一定設けて施行



デジタル社会の実現に向けた重点計画(案)説明資料

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/38606249-07b3-4176-a538-58e0c64a488a/dd76edf1/20230606_meeting_conception_outline_01.pdf

マイナンバーカード(JPKI)は、政府が発行するトラストアンカー

- マイナンバーカードは、市役所にて権限のある職員によって、必ず対面して厳格な本人確認を行った上で発行されます。マイナンバーカードは、偽造・複製が不可能なICチップを内蔵しており、それをを用いることで、オンライン上においても、対面と同等レベルの本人確認強度を実現しています。



対面による厳格な本人確認



- 偽造・複製の不可能なICチップ
- 本人のみが知るパスワード

ICチップには秘密鍵(巨大な乱数)が入っている。その数値は外から一切見ることはできないので、コピーもできない。したがって世界でただ一つだけこのカードの中に存在する数値といえる。

パスワードはこのICカードに対して設定するので、正しいカードと対応するパスワードが両方揃わないとICチップは動作しない。



対面と同等の本人確認強度をオンラインで実現

強固なセキュリティ

- パスワードが漏洩しても、カードが攻撃者の手に渡らない限り、なりすましは不可能。
- カードが奪取されても、パスワードがなければ使えず、規定回数パスワードを間違えるとロックされる。

マイナンバーカードの交付率状況

2023年6月18日 時点の数値 [データの定義](#)

デジタル庁
Digital Agency



1日あたり (直近4週平均)

11,455

先週の合計

72,869

前週の合計: 79,646 (-6,777)



1日あたり (直近4週平均)

76,269

先週の合計

330,719

前週の合計: 416,100 (-85,381)



1日あたり (直近4週平均)

58,922

先週の合計

259,527

前週の合計: 336,586 (-77,059)

有効申請件数と交付枚数

週次

累計

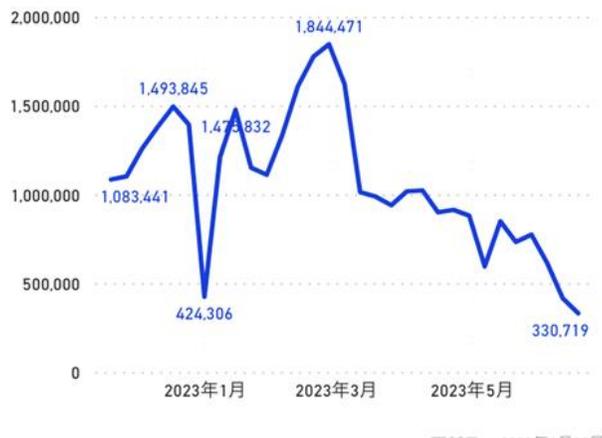


更新日: 2023年6月18日

登録件数

週次

累計

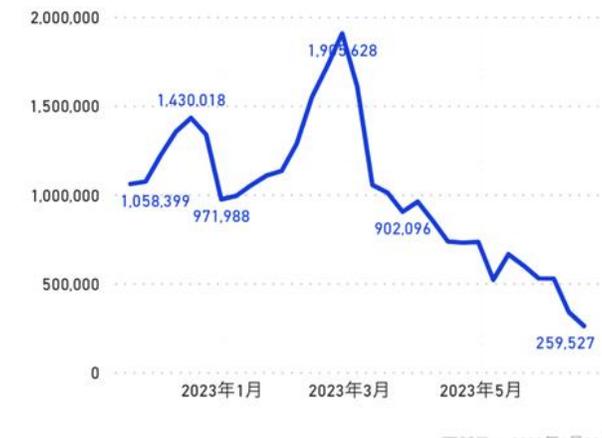


更新日: 2023年6月18日

登録件数

週次

累計



更新日: 2023年6月18日

金融サービスが抱える、利便性とセキュリティのジレンマ・課題

課題1

オンライン本人確認の煩わしさとコスト

多くの顧客は、何枚もの身分証写真や顔写真を金融サービスで提出することは多くの顧客にとってUXが悪く、申込プロセスにおける離脱に繋がります。また、現在の収法では、オンライン完結による画像アップロード型のeKYCを利用する場合、最終的には人の目視による確認を無くすことができません。即時に申込が完結しない顧客体験は顧客の離脱に繋がるだけでなく、金融機関にとってのコスト増にも繋がっています。

課題2

課題が残る、継続的顧客管理

口座開設時などにおける本人確認が適切に行われていたとしても、継続的顧客管理の手法はいまだ郵送などアナログのままで、コスト面、運用面を含めた課題があります。口座開設後に口座自体が他人の手に渡っている、あるいは不正な送金操作を第三者にされるリスクもあります。顧客体験を損なうことなく不正や詐欺と戦う対策が必要です。

課題3

フィッシング詐欺・不正ログイン対策

今やネット被害で最も多いのが、金融サービスをターゲットにしたフィッシング攻撃による詐欺被害と、それによる不正ログインです。高齢者の多い日本では、過度に顧客負担のかかるセキュリティ対策はサービスの利便性・顧客満足度の低下に繋がります。また、顧客のITリテラシーに依存する形でのフィッシング詐欺対策の啓蒙などにも限界が来ています。

マイナンバーカードを活用することで、デジタル時代の金融サービスの課題を顧客の利便性とセキュリティ担保を両立しながら解決可能

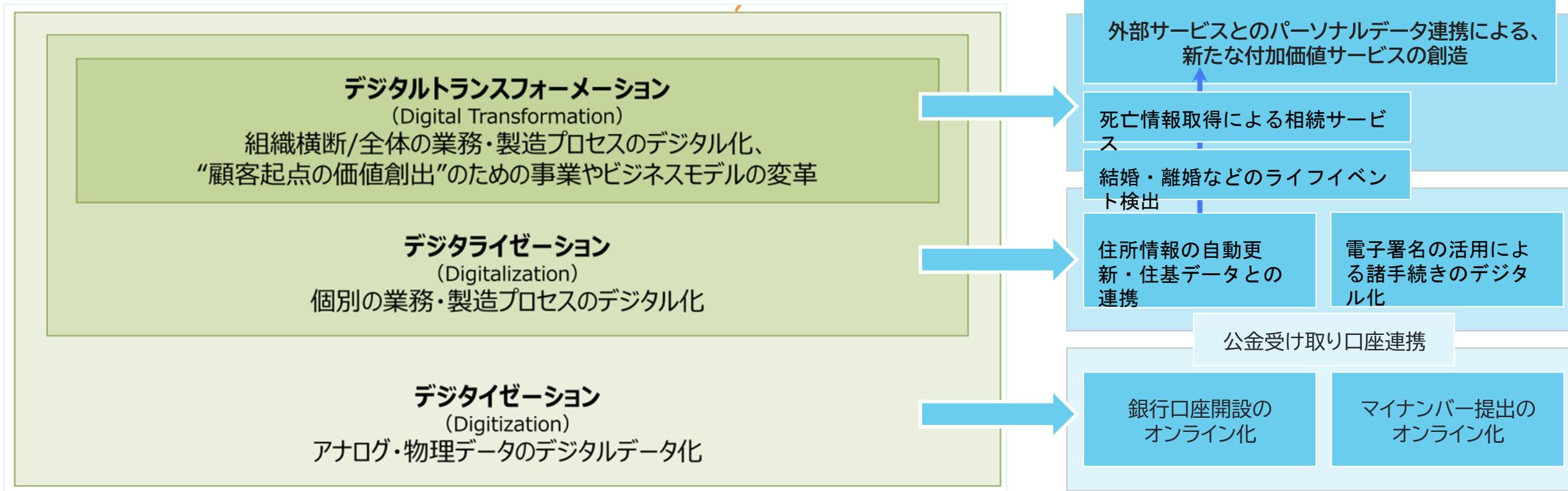


交付率約 **74.5%**

申請率約 **77.5%**
(令和5年7月23日時点)

金融機関におけるマイナンバーカード活用によるデジタル化・DXの方向性

経済産業省「DXレポート2 中間取りまとめ(概要)」より



マイナンバーカード活用にかかる課題は、xIDがすべて解決

公共・行政分野で導入実績No.1のマイナンバーカード事業に特化した企業だからこそ得られる経験・知見を、プロダクト改善や実装サポートにも活用し、徹底的に自治体と事業者双方の利便性向上にフォーカス

xID マイナンバーカードの活用の幅を広げるスマホアプリとAPI

ユーザー向けアプリ



スマホひとつでマイナンバーカードが便利に使える無料のデジタルIDアプリ

開発者向けAPI



マイナンバーカードを活用した機能が簡単に実装できる開発者向けAPI

SmartPOST マイナンバーカードを活用した通知・郵送DXサービス



自治体職員

- 特定住民への個別デジタル通知の実現
- デジタル通知化による印刷・郵送コストの削減
- 開封状況の確認を通じた、EBPMの促進
- LGWAN経由で利用できる使いやすい管理画面

住民

- xIDアプリは無料で利用可能
- 時間・場所を選ばず、スマホからお知らせを確認
- デジタル通知による付加価値の向上
- なりすましやフィッシング詐欺からの保護

自治体職員は、LGWAN-ASPサービスとして提供されるSmartPOST管理画面から、マイナンバーカードで認証を済ませた住民のスマートフォンに対して安全かつ、簡単にデジタル通知を送ることが可能です。

- 全国400を超える自治体様と事例を創出。マイナンバーカード事業にかかる知見が豊富
- 様々なサービスと連携しマイナンバーカードを活用するプログラム(API)を提供
- 国のマイナンバーカード関連の検討会にも参加し、最新の動向を踏まえてサービスを開発、アップデート

マイナンバーカード活用にかかわる面倒をなくし、課題解決をこれ一つで

- マイナンバーカードの活用によって解決できるこれまでの課題はあるものの、マイナンバーカードを活用していく上での新たな課題が顕在化
- xIDは、マイナンバーカードで解決できる課題はもちろん、活用する上での課題解決も行う、デジタルIDソリューションです

ニーズに合わせて、選べる実装方法

マイナンバーカードの公的個人認証機能の利用にはネイティブアプリが必須です。xIDなら、自社アプリを持っていないWebサービスにも、自社アプリへの組み込みにも対応可能です。

ユースケースに応じた、コストの最適化

ユースケース次第では、公的個人認証機能をそのまま利用することでむしろランニングコストが増加することがあります。xIDなら、xIDアプリの利用で、ユースケースに応じてコストを最適化する実装方法の検討が可能です。

省庁への必要手続きも簡単に

犯罪収益移転防止法などの法令対応のオンライン本人確認で利用する場合、総務大臣認定取得のための届出が必要になります。xIDを利用する場合、必要な手続きは当社が対応します。

Googleログインのように簡単に実装できる、使いやすいAPI※

マイナンバーカードの公的個人認証機能の利用にはネイティブアプリが必須です。xIDなら、自社アプリを持っていないWebサービスにも、自社アプリへの組み込みにも対応可能です。

E2E暗号化技術で、プライバシー保護を前提とした実装が可能

xIDアプリなら、本人同意の上で必要最小限の個人情報のみを利用者スマホ端末とのエンドツーエンドで暗号化状態で通信し取得する実装ができるため、保持する社内で管理する個人情報を最小化できます。

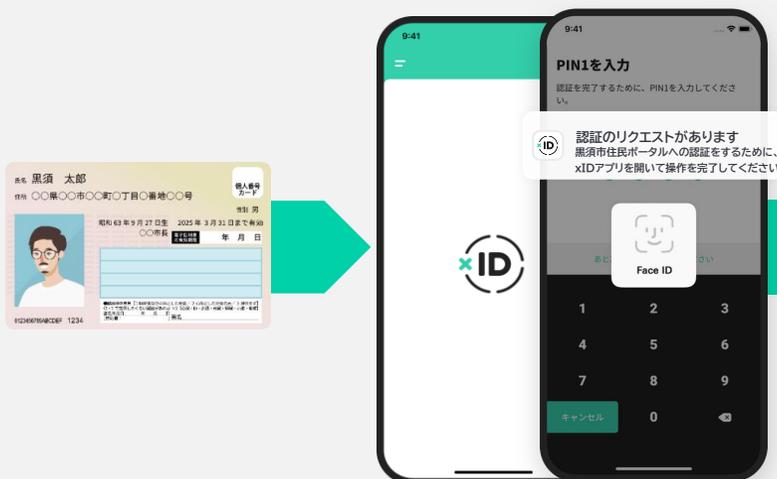
複雑で検討事項の多いマイナンバーカード活用は、ミスのできない不可逆な検討事項も少なくありません。単に機能やコスト比較だけで選んでよいのかさえ一般的には分からず、自社内では専門的な知識も不足していることがほとんどです。xIDは、マイナンバーカードに特化したデジタルIDソリューションの提供会社として、マイナンバーカードを活用するすべての企業にとって、最適な課題解決の提案を顧客サービスへの深い理解へのこだわりを持って、サポートします。

xIDアプリとは？

xID マイナンバーカードを、スマートに

マイナンバーカードをもっと便利に、よりスマートに利用できる、無料のデジタルIDアプリ

マイナンバーカードで本人確認して、
自分専用のIDを無料で作成(最短60秒)



xIDアプリが使えるサービスなら

毎回のカード読み取り不要
初回登録以降は、アプリだけで完結※1

PIN(パスワード)入力不要
スマホ端末の生体認証でパスワードレスログイン

面倒な個人情報入力も、スマートに
名前・生年月日・性別・住所は自動入力でミスなく便利に。
さらに、引越などによる住所変更も自動で更新※2

オンライン本人確認も、スマートに
公的個人認証を利用して、行政・金融サービスで利用できる
厳格なオンライン本人確認※2を写真撮影不要で簡単に

自治体からの大切なお知らせの受取り
対応する自治体からの大切なお知らせを
いつでもどこでもオンラインで受取り

xIDアプリと連携しているさまざまなサービス
が、ID一つで利用可能に



xIDアプリの導入事例

官民を問わず、さまざまなアプリ、ウェブサービスなどのログイン認証・本人確認・ID連携に、xIDアプリが導入されています



生体認証(or PIN入力)を完了してサービスに戻る

2

認証ボタンをタップしてxIDアプリに自動遷移

1

導入事例

アプリ

ブラウザ

アプリ

ブラウザ

練馬区
母子健康手帳アプリ「ねりすく」

全国300自治体以上が導入
「LoGoフォーム電子申請」

SOMPO Light Vortex
トータルヘルスケアアプリ
「WiTH Health」

クレディセゾン
クレジットカード入会申込

マイナンバーカードを活用する際の課題を解決するデジタルIDソリューション

Before

マイナンバーカードを読み取るためだけにいくつものアプリをダウンロードさせられる

- 複数の読取専用アプリのダウンロードが必要
- カード読み取りは用途を問わず、**毎回必須**
- **パスワード手入力も毎回必須**

読み取りアプリA

読み取りアプリB

読み取りアプリC



公共交通サービス



行政サービスなど



民間サービス

- 自社アプリへの組み込みなど実装ハードルが高い
- 手続き・法令対応コスト

開発会社

After

公共・行政サービスも、民間サービスも。ユーザーも事業者もxID一つで利用可能に

- xID一つで、さまざまサービスを利用可能に
- カード読み取りはID生成時と、必要な時だけ
- **生体認証でパスワード入力も不要に**



公共交通サービス



行政サービスなど



民間サービス

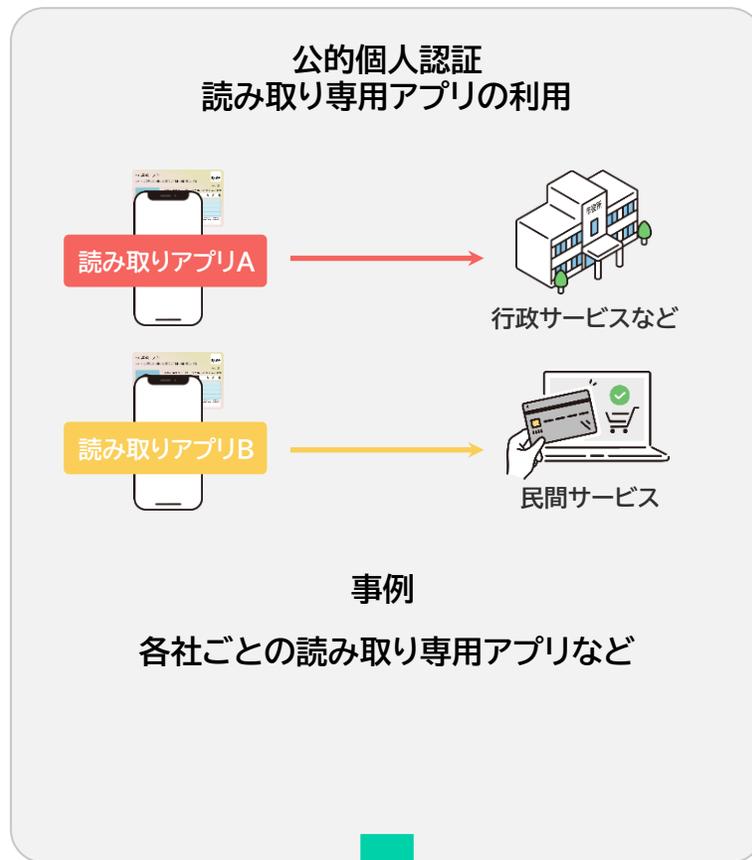
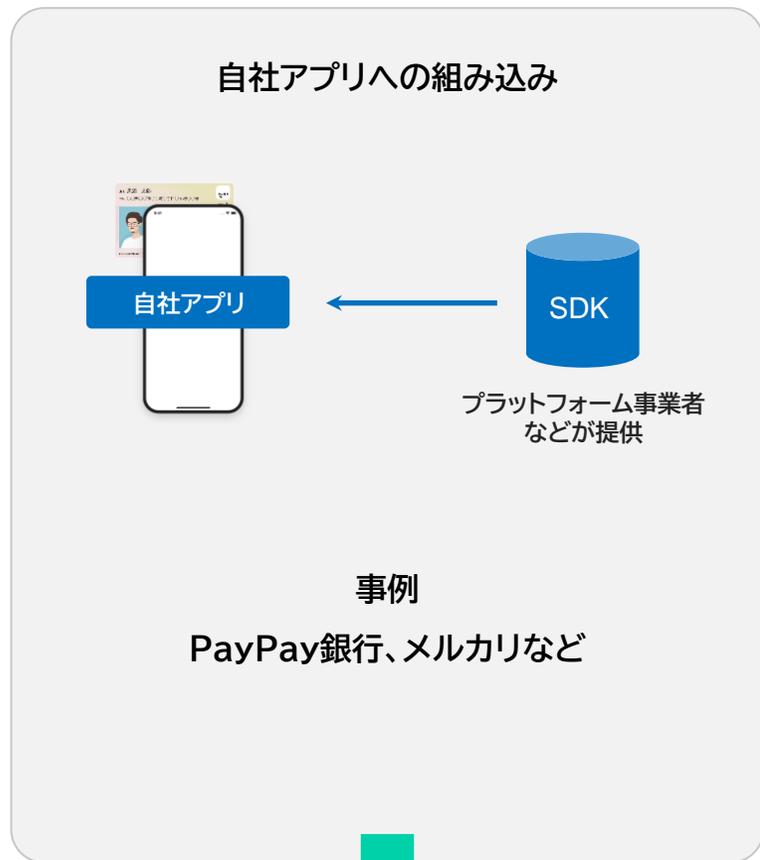
銀行・証券・保険などの
金融サービスにも、
もちろん利用可能です



xID API For Developers

- 国際標準仕様のAPIで簡単に実装可能
- ネイティブアプリ不要！ブラウザサービスでも利用可能

公的個人認証の活用に向けた利用方法3類型 - 現状 -

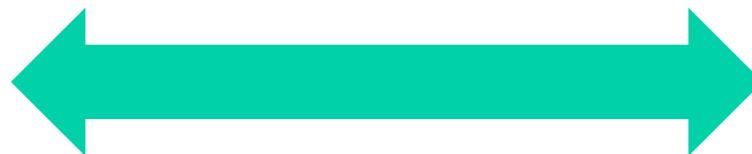
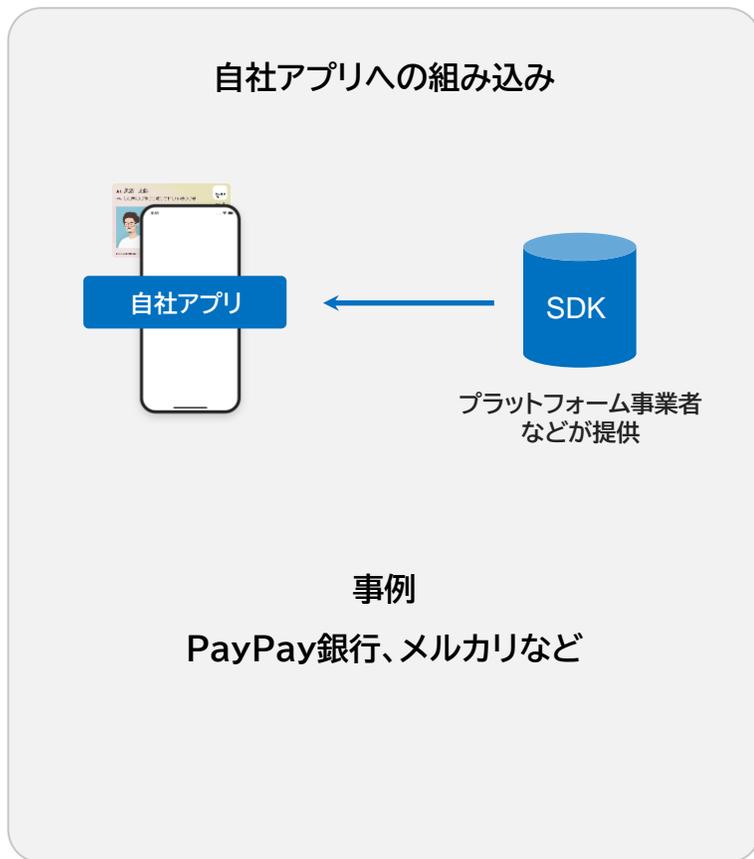


犯罪収益移転防止法における本人確認で利用するなどのワンタイムユースケースでは別アプリのインストールが不要なのでUXの観点から選択されるケースが多い

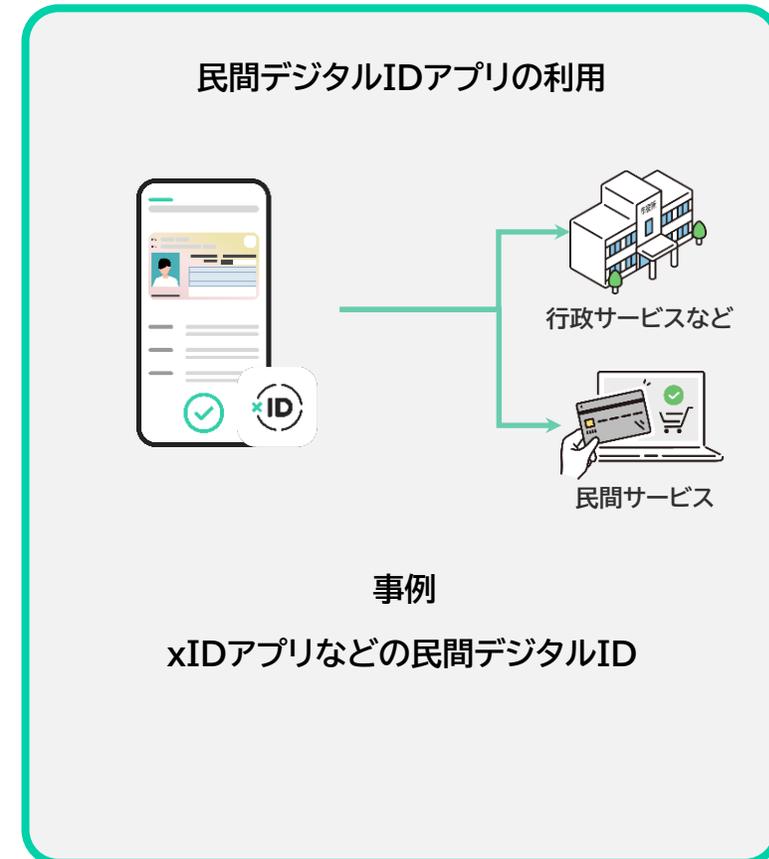
特に自治体の場合、ネイティブアプリで提供するサービスが少なかったため民間デジタルIDが出るまではこのケースがほとんど

ネイティブアプリ提供の少ない自治体などのユースケースで広がる

公的個人認証の活用に向けた利用方法3類型 - 今後 -



自社アプリの有無、自社アプリのユーザー規模や
解決した課題に応じて選択



ニーズに合わせて選べる、2つの実装方法

	 <p>犯罪収益移転防止法方式への対応を 自社アプリ内だけで完結させたいなら</p> <h2>xID SDK</h2>	 <p>デジタルIDアプリとの連携で、低コストに あらゆるユースケースに対応できる</p> <h2>xIDアプリとAPI連携</h2>		
自社アプリ (利用可能な環境)	必要 (ネイティブアプリのみ)	不要 (ネイティブアプリ・ブラウザサービス)		
利用可能な機能	UX最重視! 自社アプリのユーザー基盤があり、ワントイムのユースケースなら		コストと拡張性 さまざまな機能をトランザクションコストを気にせず利用できる!	
	電子署名 (署名用電子証明書) ○	電子署名 (利用者用電子証明書) ○	電子署名 (署名用電子証明書) ○	電子署名 (利用者用電子証明書) ✗
	基本4情報+マイナンバー取得 (券面事項入力補助AP) ○	最新4情報の取得※1 △	基本4情報+マイナンバー取得 (券面事項入力補助AP) ○	最新4情報の取得※2 ○
	xIDログイン・電子署名 ✗	他サービスとのID連携 ✗	xIDログイン・電子署名 ○	他サービスとのID連携 ○
導入にかかる期間	1ヶ月～ (同意画面など追加構築が必要)		最短1ヶ月 (OpenID Connect準拠のAPIで既存サービスへの実装も比較的簡単)	
総務大臣認定の届出	必須 (当社が代行して手続き)		用途次第では不要	

マイナンバーカードを活用した機能が簡単に実装できるxID API

開発者向けAPI

xID API For Developers

xID APIs for Developersの特徴



実装が簡単

OAuth2.0やOpenID Connectなどの業界標準仕様に準拠したセキュアなRest APIで簡単に実装ができます。



API

APIは本番環境に加え、無償のテスト環境を用意しています。



サポート

当社のTechチームが、状況に応じて、ユースケースに合わせた実装のアドバイスをいたします。

COMING SOON

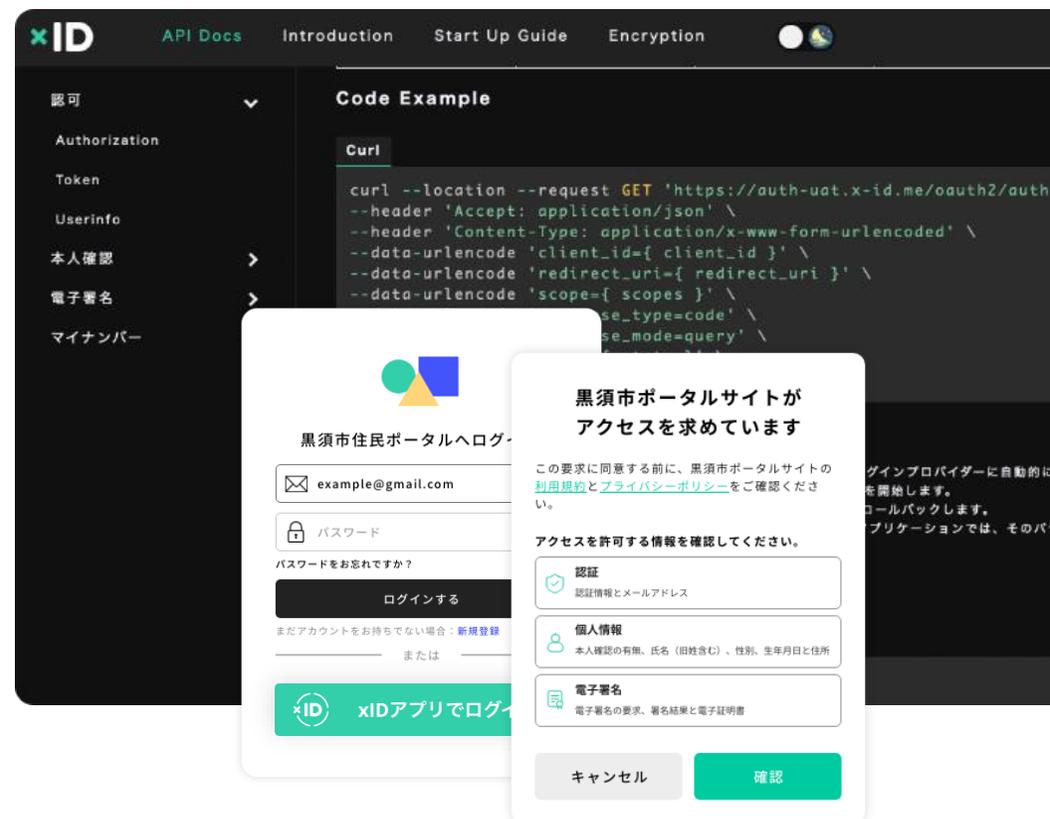


ダッシュボード

APIの利用状況やトランザクションが確認できる管理画面を提供します。

誰でも簡単にマイナンバーカードを活用したオンライン本人確認や認証・電子署名が実装できるID基盤です。

xIDのAPIソリューションを活用することで、面倒な手続きなしにマイナンバーカードの公的個人認証の仕組みを導入したり、OpenID Connect等の国際標準仕様に準拠した認証・認可機能の実装が可能になります。認証・認可・電子署名・E2E暗号化によるマイナンバーの受け取りなどサービスに合わせてご利用できます。



開発者向けxID APIs

- xIDは、エンドユーザー向けモバイルアプリとサーバーサイドAPIから構成されており、認証、署名の主要機能を備えたアプリケーションです。認証フローは、OpenID Connectの国際標準仕様に準拠しています。認証APIに加え、利用用途に合わせてAPIを組み合わせてご利用いただけます。



個人情報確認API

公的個人認証(署名用電子証明書)を活用し、基本4情報(名前・性別・生年月日・住所)の正確な情報を提供します。



電子認証API

ユーザーのスマホ端末をマイナンバーカードで認証することでパスワードレスログインのためのセキュアな認証器に。多要素認証でなりすましや、リスト型攻撃対策のセキュリティリスクを低減します。



電子署名API

xID署名用電子証明書を利用しデータに電子署名を行うことで、データの偽装や、改ざん防止・否認防止することができます。電子署名法に準拠(第二条3項)した当事者の電子署名にご利用いただけます。



マイナンバーAPI

本人確認がされたxIDアプリから安全かつ確実に当人のマイナンバーの提供を受けることができるAPIです。公開鍵暗号の仕組みを使い、利用者から事業者に暗号化された状態でマイナンバーが提供されます。



本人確認情報更新API

ユーザーの失効情報確認を実施し、失効していた場合、マイナンバーカードを読み取り個人情報の更新をリクエストします。更新が完了したユーザーのみ以降対象サービスを利用できるように設定が可能です。



公的個人認証API

マイナンバーカード署名用電子証明書による身元確認を実施し、申請データに対して、当該電子証明書による電子署名を付与します。国の法令で定められている手続きや犯収法における本人確認として活用します。

住所更新をスマートに”実現する、最新基本4情報自動提供サービス

APIで簡単実装

郵送費や事務コストの削減

事前の本人同意により、氏名・住所を更新



公的個人認証サービスにおける本人同意に基づく基本4情報の提供について

(参考) 公的個人認証サービスにおける本人同意に基づく基本4情報の提供 (デジタル社会の形成を図るための関係法律の整備に関する法律)

11

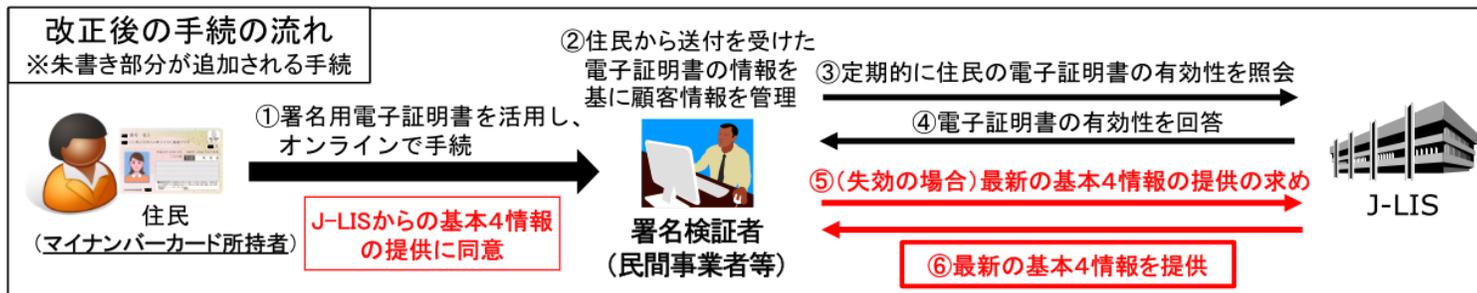
改正の背景

- 公的個人認証サービスにおいては、署名用電子証明書を利用する民間事業者等(署名検証者)は、署名用電子証明書の有効性のみを地方公共団体情報システム機構(J-LIS)に確認する仕組みであるが、住所変更等により署名用電子証明書が更新された住民について、当該住民の最新の住所情報等を取得することへのニーズが高まっている。
- これを受け、「マイナンバー制度及び国と地方のデジタル基盤抜本改善ワーキンググループ報告」において、本人同意に基づき基本4情報を署名検証者に提供する仕組みを構築し、令和4年度にサービスを開始することを目指すこととされた。

- 令和5年5月16日より、本人の同意を前提として、住所などの基本4情報を提供するサービスが開始される予定。
(令和4年10月13日河野デジタル大臣記者会見より)

公的個人認証法の一部改正

- 署名検証者(民間事業者等)の求めがあった場合で、本人の同意があるときは、J-LISは、最新の基本4情報(氏名、生年月日、性別及び住所)の提供を行う。
- 署名検証者は、受領した基本4情報について、安全確保措置を講じるとともに、目的外利用・提供の制限が課される。



改正の効果

- 署名検証者においては、直接本人に照会することなく、住民の最新の住所情報等を取得することが可能に。
- 住民においては、個々の署名検証者に対する住所等の変更手続が不要に。

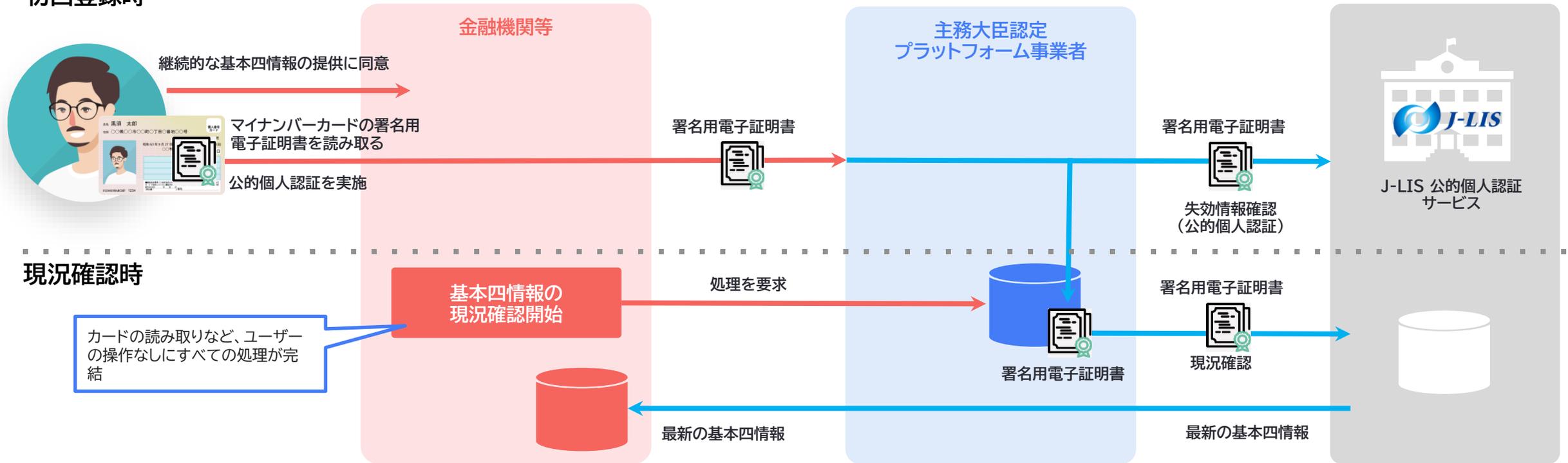
施行期日: 公布の日から2年以内で政令で定める日

出典: 公的個人認証サービスと紐付けられた民間IDの利活用に関する課題整理 | 総務省

最新基本4情報提供の仕組み

※本機能はJ-LISから仕様詳細が公表されていないため、実際のサービス提供時には仕組みが異なる可能性があります。予めご了承ください。

初回登録時

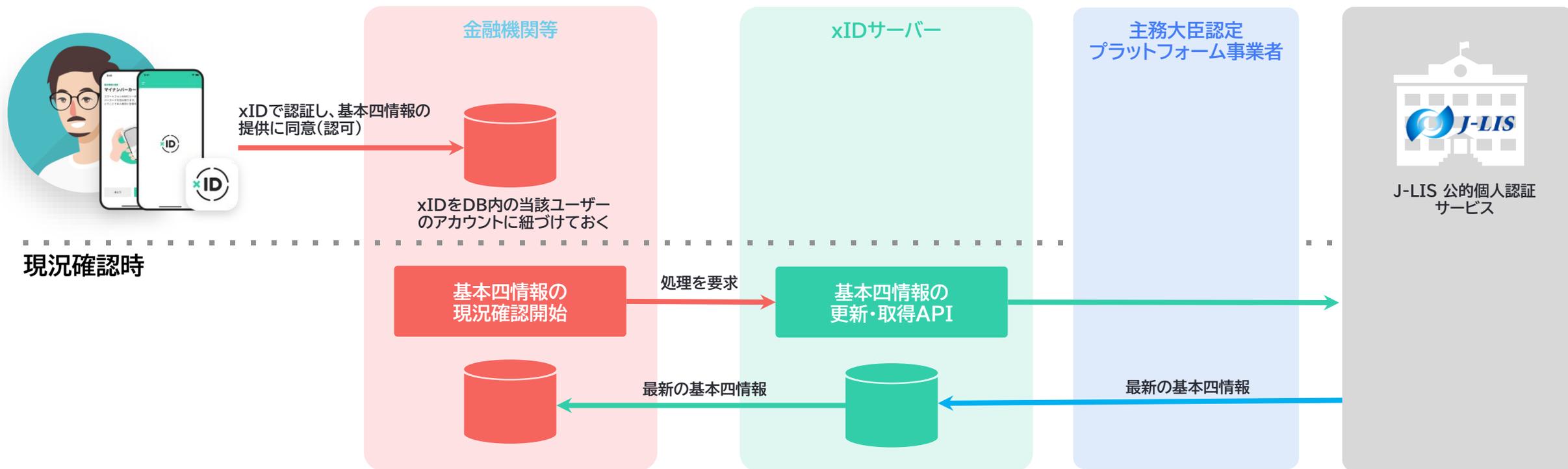


- J-LISが、マイナンバーカードの当該電子証明書の失効情報確認だけでなく、失効情報に基づく最新の基本四情報を提供することにより、任意のタイミングで当該利用者の、現況を更新することが可能になります。
- 初回登録時に公的個人認証を行う必要があるため、通常は主務大臣による認定(みなし認定事業者)を取得したうえ、公的個人認証サービスPF事業者署名検証業務並びに電子証明書の保管業務を委託する必要があります。
- 初回登録時に、継続的な現況確認と最新の基本四情報の提供について、利用者の同意を取得する必要があります。
- マイナンバーカードの読み取りアプリを含めたすべてのシステムを構築する必要があります。

xID APIによる、最新基本4情報提供の仕組み

初回登録時

※本機能はJ-LISから仕様詳細が公表されていないため、実際のサービス提供時には仕様が変わる可能性があります。予めご了承ください。



- xIDが最新基本4情報提供のAPIを提供することにより、カード読取アプリを開発したり、マイナンバーカードの電子証明書を直接取り扱ったりすることなく、実装が容易なxID APIのみで、任意のタイミングにおける最新の基本4情報を取得することが可能になります。
- 継続的な基本4情報提供の同意は、xIDアプリ登録時に完了します。
- xID社が持つ、最新の基本4情報を、利用者同意の元金融機関等に提供することが可能です。その際、アプリの操作等は一切不要となる予定です。
- 上記の処理を行うに際し、マイナンバーカードは不要です。(xIDアプリの初回登録時に読み取り済みのため)

参考:銀行アプリなどとxIDのID連携により、住所変更を自動化

xIDアプリへ自動遷移し生体認証

※xIDアプリ未インストールの場合はアプリをダウンロード(90秒で登録完了)

本人同意完了後以降、xID APIによってお客様のその後の操作なしに、引越し時の最新住所、結婚、離婚時などの姓名の変更の際に最新情報を取得可能に



完全オンライン完結でのマイナンバー収集

- xIDを活用することで、金融業務にてマイナンバーの収集が求められる際のマイナンバー収集の完全オンライン化を実現。
- 顧客情報は公的個人認証により本人確認を実施した情報のため、データの目視確認が不要となり業務が自動化。
- 従来までの申請書類(番号確認・身元確認書類)の郵送が不要になり、xIDアプリを活用して個人番号提出が可能。

従来の課題

利用者目線

1

身分証と番号確認書類の提出

身分確認と個人番号確認が必要なため、身分証のコピーと通知カードや住民票の写しなどを郵送または写真撮影を行う必要がある。

金融機関目線

2

紙の開封とチェック

金融機関側では郵送物の開封と書類の目視確認にかかる職員の発生している。

3

番号確認後の取り扱い

確認した個人番号についてはシステムへの手入力またはBPO事業者への委託のため追加でのコストが発生。



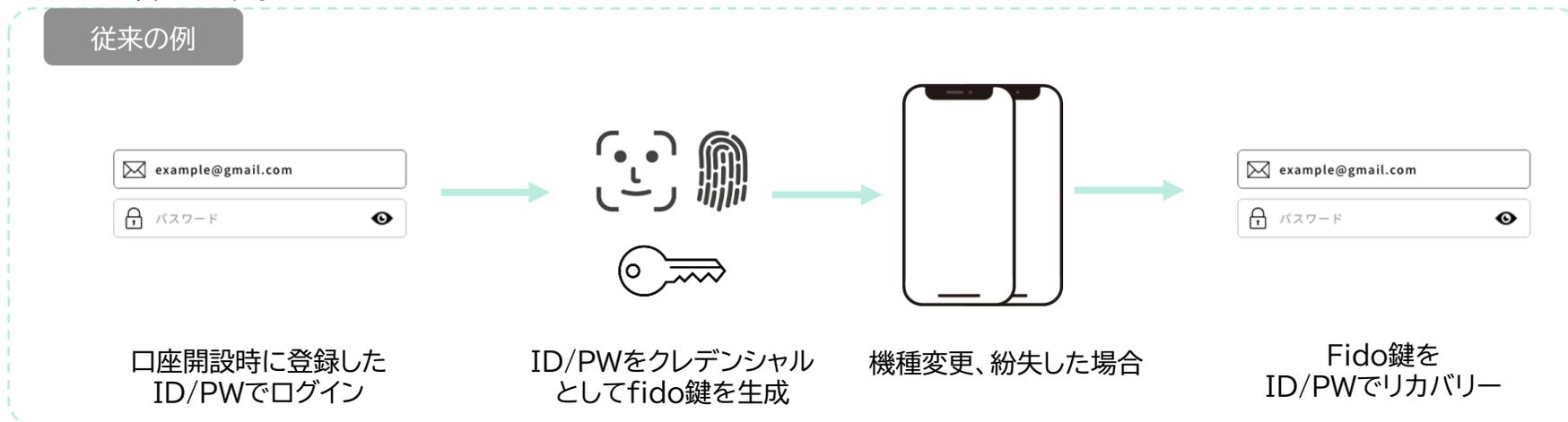
解決策

xIDを活用することで、公的個人認証とマイナンバー提出をオンラインで実現。
間違いのない個人情報とマイナンバーは自治体の業務も自動化。



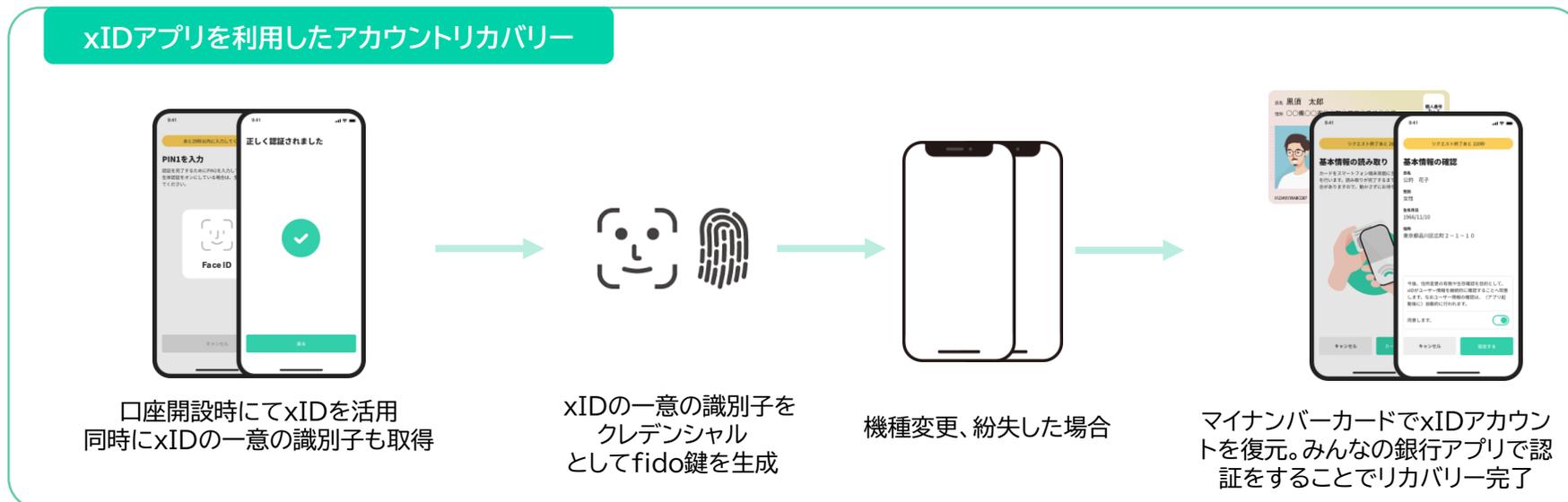
xIDを活用したアカウントリカバリーについて

機種変更をした際の従来のアカウントリカバリーとxIDを活用した際のアカウントリカバリーについてご説明をさせていただきます。



課題認識

- fido認証自体はセキュアである一方でID/PWをクレデンシャルとして利用している場合には機種変更時に一定のなりすましリスクが発生する
- 悪意のある人間が他者に口座を譲渡する際においてもID/PWの共有のみで譲渡可能ためハードルが低い



実現すること

- 機種変更時に口座開設時にxIDで利用したマイナンバーカードを利用してxIDのアカウント生成が必要なためなりすましリスクを低減することが可能
- xIDは機種変更をした場合であっても同じマイナンバーカードからは同じxIDアカウントを復元可能

金融機関(銀行)との各フェーズにおける取り組み例

xID連携による継続的顧客確認による既存業務の効率化からスタート。
ID連携顧客を増やし、最終的に共通IDの活用によって外部の非金融サービスとのパーソナルデータ連携による
新たな付加価値サービスの創造を実現する

2023年度

2024年度

2025年度

フェーズ1

継続的本人確認による
マイナンバーカード連携

フェーズ2

公的個人認証による
オンライン口座開設
マイナンバー収集業務
公金受け取り口座連携

フェーズ3

リスクベースの送金時の電子署名利用
による不正利用防止強化

フェーズ4

外部サービスとのパーソナルデータ連携に
よる、新たな付加価値サービスの創造

官民共通のデジタルIDとして広がるxID

xIDは、様々なサービスの共通IDとして活用できます。また、当社の既存パートナー企業を含めて、今お使いのシステムにxID APIを組み込むことも可能です





信用コストの低いデジタル社会を実現する