資料４－１

DIPC

本人確認手法のJPKI一本化を前提とした、不正対策と利便性の高い本人確認の実現

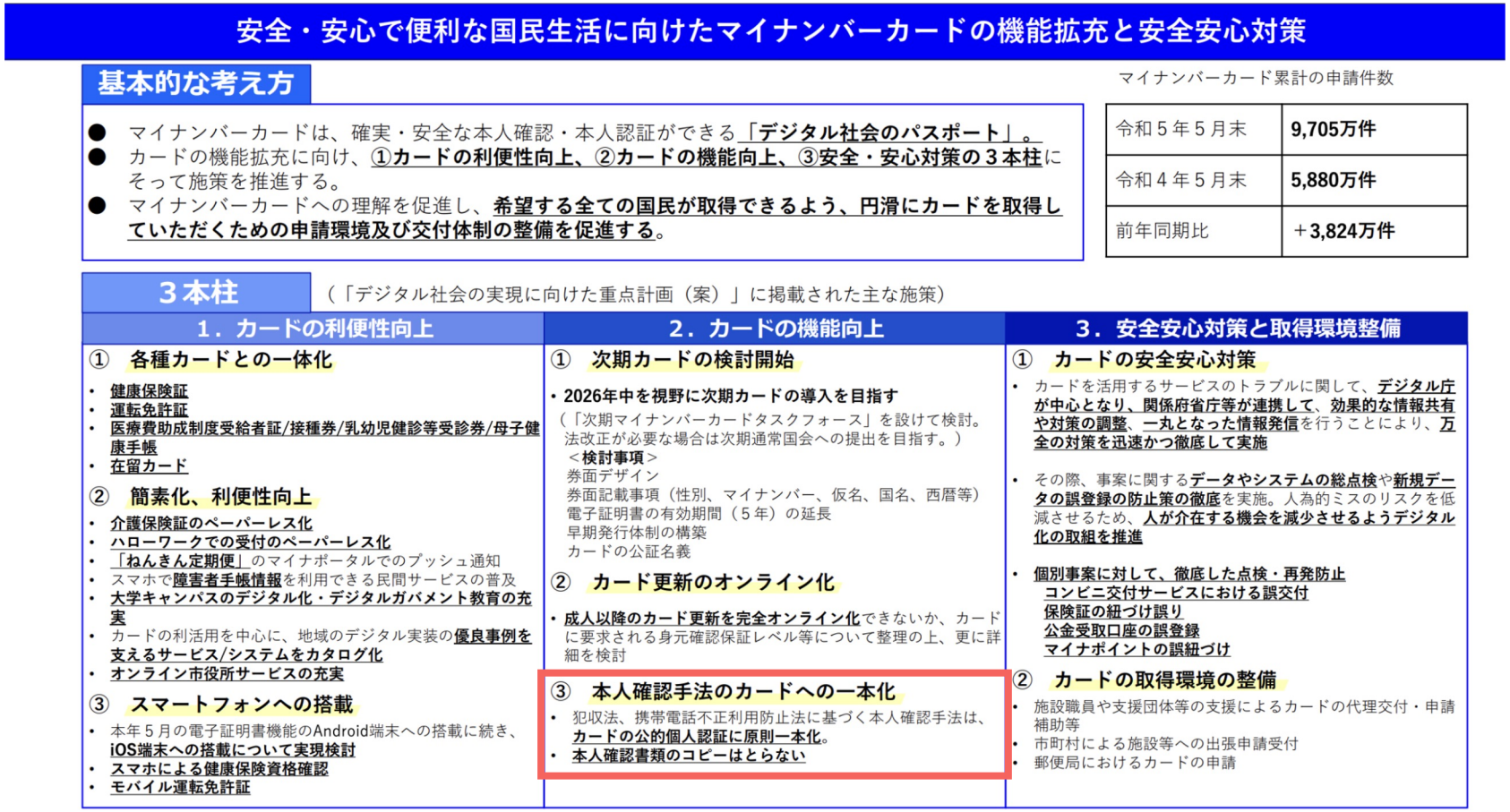
DIPC 理事/Govtech協会 代表理事 日下 光

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

2024年5月15日

前提- デジタル社会の実現に向けた重点計画(案)抜粋 -

- 昨年5月に公開された下記資料内の2.カードの機能向上の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
- 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)(ヘ)などの本人確認方法は利用を廃止していく方向で政府は検討



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

① 各種カードとの一体化

- 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

② 簡素化、利便性向上

- 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

③ スマートフォンへの搭載

- 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

２．カードの機能向上

① 次期カードの検討開始

- **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

② カード更新のオンライン化

- **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

③ 本人確認手法のカードへの一本化

- 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**

３．安全安心対策と取得環境整備

① カードの安全安心対策

- 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、**万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。人為的ミスの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

② カードの取得環境の整備

- 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-a538-58e0c64a488a/

台帳照合を行わない画像解析型本人確認(eKYC)の課題

画像だけでは身分証の偽造は”確実な検証”ができないため、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、日本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、画像解析型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)

ネット上にあふれる偽造身分証販売サイトの例

従来の書類の画像+容貌による本人確認手法の限界

マイナカードの情報でネットバンク口座を無断開設か…７０代女性が１４００万円だまし取られる

2024/03/10 13:42　この記事をスクラップする

北海道警札幌厚別署は８日、札幌市厚別区の７０歳代女性が、約１４００万円をだまし取られる被害に遭ったと発表した。女性のマイナンバーカードの情報などを基に、女性名義のインターネットバンキングの口座を無断で作り、振り込ませたとみられる。同署は、新たな特殊詐欺の手口の可能性があるとして注意を呼びかけている。

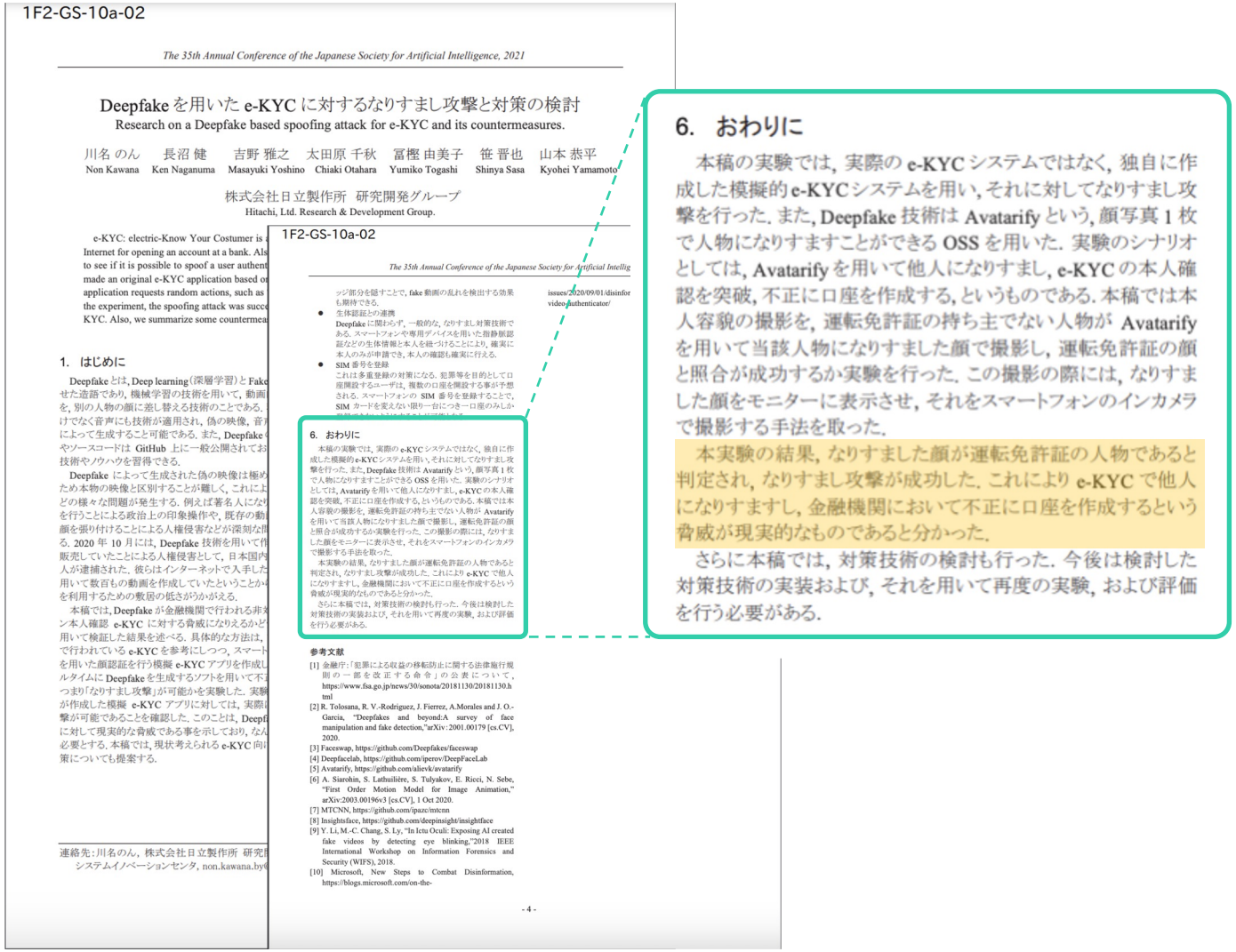
マイナンバーカード

発表によると、女性の自宅に１月中旬、「総合通信局」の職員や警察官を名乗る人物から「口座の情報が流出している」などと電話があった。女性はスマートフォンの機種変更を指示され、スマホのビデオ通話機能で自分の顔やマイナンバーカードを相手側に示した。

その後、相手は「あなたの口座が凍結される」などとして預金の移し替えを持ちかけ、振込先に女性名義のネットバンク口座を提示。女性は、口座が開設されたことを知らなかったが、不審に思わず２月２８日、二つの金融機関の窓口から現金を振り込んだという。

窓口の職員も詐欺と気付かず、同署は「振込先が本人名義の口座のため、不審に思わなかった可能性が高い」としている。

出典：読売新聞オンライン


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　冨樫 由美子　笹 晋也　山本 恭平
Non Kawana　Ken Naganuma　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.

1. はじめに

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，それに対し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．

出典：日立製作所研究開発グループ
https://www.jstage.jst.go.jp/article/pjsai/JSAI2021/0/JSAI2021_1F2GS10a02/_pdf/-char/ja

オンラインの本人確認手法強化に伴う対面本人確認による不正

公的個人認証によってオンラインでの本人確認が強化されることで、対面本人確認が次の不正のターゲットに

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

YAHOO! JAPAN ニュース　IDでもっと便利に新規取得　ログイン　［おトク］10%OFFクーポンあります

キーワードを入力

トップ | 速報 | ライブ | エキスパート | オリジナル | みんなの意見 | ランキング

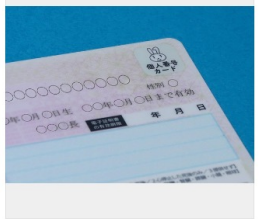
主要 | 国内 | 国際 | 経済 | エンタメ | スポーツ | IT | 科学 | ライフ | 地域

225万円のロレックス、偽造マイナカードで勝手に購入　“目視”ベースの本人確認が抜け穴に

5/10(金) 7:00 配信　111

ASCII

スマホを勝手に機種変更される、225万円するロレックスを勝手に購入されるなど、偽造マイナンバーカードを使った被害が後をたたない。背景にあったのは、顔写真付き身分証を使った“目視”ベースの本人確認だ。


写真：アスキー

スマホを勝手に機種変更される、225万円するロレックスを勝手に購入されるなど、偽造マイナンバーカードを使った被害が後をたたない。

東京都の風間ゆたか都議は、4月17日に偽造マイナンバーカードを悪用されて携帯電話を乗っ取られたとXで明かした。その後もPayPayで勝手にチャージや決済の操作をされた上、クレジットカードで10万円を超える被害にあったという。

大阪府八尾市の松田憲幸市議は5月2日、偽造マイナンバーカードを使った犯罪に巻き込まれたことをやはりXで明かした。4月30日に偽造カードを使ってスマホを機種変更されていたことがわかり、5月1日にはオンラインショップで225万円もするロレックスの腕時計「デイトナ」を購入される被害にあったという。

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

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8500万円の振り込め詐欺被害：中国

5/30(火) 11:41 配信　10

36Kr Japan

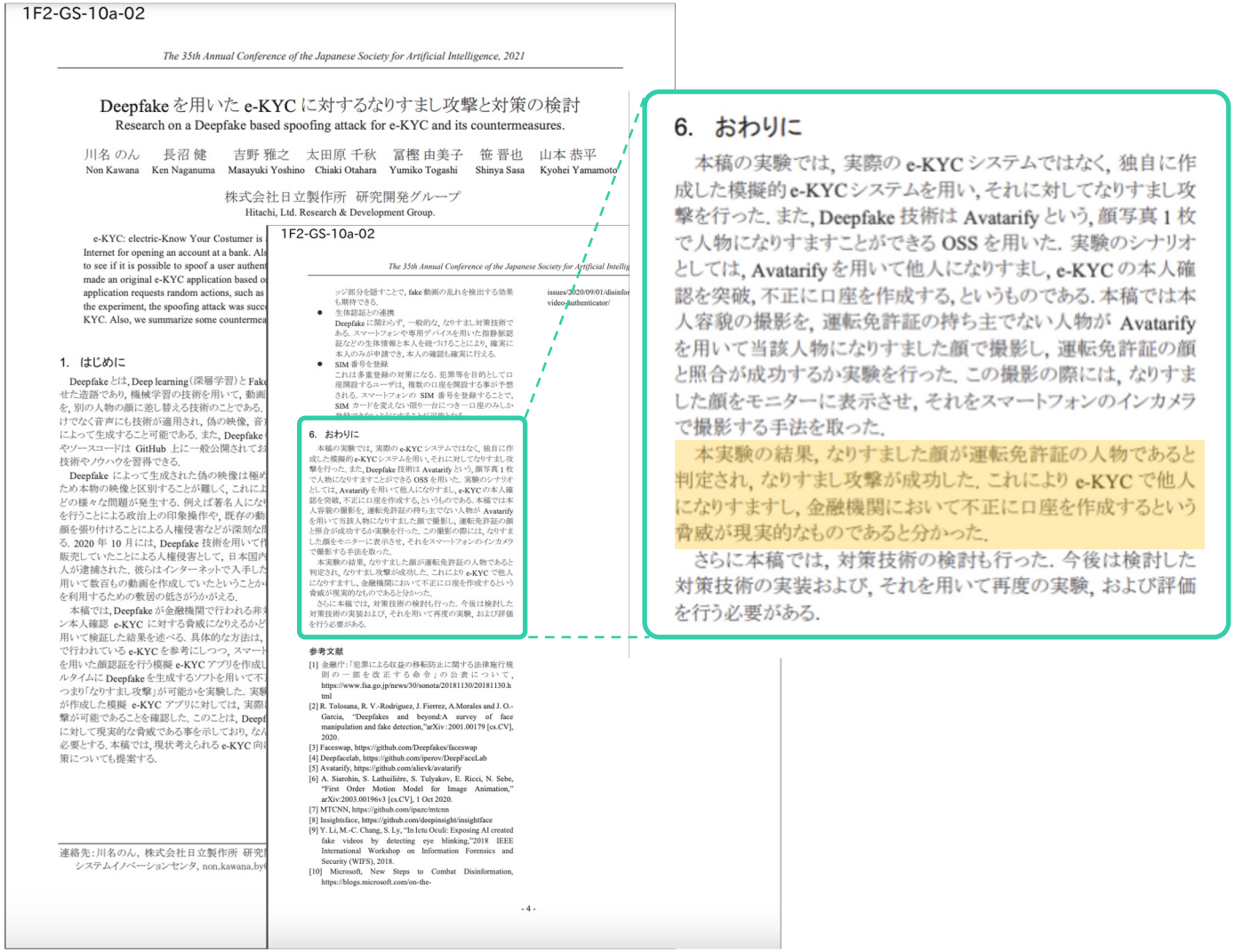
中国でAIを悪用した振り込め詐欺事件が発生した

中国でこのほど、人工知能（AI）を悪用した振り込め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430万元（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430万元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430万元を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　冨樫 由美子　笹 晋也　山本 恭平
Non Kawana　Ken Naganuma　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 Costumer is
Internet for opening an account at a bank. AIs
to see if it is possible to spoof a user authent
made an original e-KYC application based o
application requests random actions, such as
the experiment, the spoofing attack was succ
KYC. Also, we summarize some countermea

1. はじめに

Deepfake とは，Deep learning（深層学習）と Fake
せた造語であり，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．
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
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
ため本物の映像と区別することが難しく，これに
どの様々な問題が発生する．例えば著名人にな
を行うことによる政治上の印象操作や，既存の動
顔を張り付けることによる人権侵害などが深刻な
る．2020 年 10 月には，Deepfake 技術を用いて
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
用いて数百もの動画を作成していたということ
を利用するための敷居の低さがうかがえる．

本稿では，Deepfake が金融機関で行われる非
ン本人確認 e-KYC に対する脅威になりえるか
用いて検証した結果を述べる．具体的な方法は，
で行われている e-KYC を参考にしつつ，スマー
を用いた顔認証を行う模擬 e-KYC アプリを作成
ルタイムに Deepfake を生成するソフトを用いて不
つまり「なりすまし攻撃」が可能かを実験した．実
が作成した模擬 e-KYC アプリに対しては，実際
撃が可能であることを確認した．このことは，Deepf
に対して現実的な脅威である事を示しており，な
必要とする．本稿では，現状考えられる e-KYC 向
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
システムイノベーションセンタ，non.kawana.by

1F2-GS-10a-02

The 35th Annual Conference of the Japanese Society for Artificial Intelli

ジ部分を隠すことで，fake 動画の乱れを検出する効果も期待できる．
- 生体認証との連携
  Deepfake に関わらず，一般的な，なりすまし対策技術である．スマートフォンや専用デバイスを用いた指静脈認証などの生体情報と本人を紐づけることにより，確実に本人のみが申請でき，本人の確認も確実に行える．
- SIM 番号を登録
  これは多重登録の対策になる．犯罪等を目的として口座開設するユーザは，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台につき一口座のみしか

issues/2020/09/01/disinfor
video-authenticator/

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，それに対し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 で他人になりすますし，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/sonota/20181130/20181130.html
[2] R. Tolosana, 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] Faceswap, https://github.com/Deepfakes/faceswap
[4] Deepfacelab, https://github.com/iperov/DeepFaceLab
[5] Avatarify, https://github.com/alievk/avatarify
[6] A. Siarohin, S. Lathuilière, S. Tulyakov, E. Ricci, N. Sebe, "First Order Motion Model for Image Animation," arXiv:2003.00196v3 [cs.CV], 1 Oct 2020.
[7] MTCNN, https://github.com/ipazc/mtcnn
[8] Insightsface, https://github.com/deepinsight/insightface
[9] Y. Li, M.-C. Chang, S. Ly, "In Ictu Oculi: Exposing AI created 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-

- 4 -

出典：日立製作所研究開発グループ
https://www.jstage.jst.go.jp/article/pjsai/JSAI2021/0/JSAI2021_1F2GS10a02/_pdf/-char/ja

オンライン本人確認手法のJPKI一本化を前提に

オンライン本人確認手法のJPKI一本化を前提に、合わせて発生しうる課題についても解決することで、不正対策を強化しつつも、特定事業者の負担を減らし、ユーザーにとっても利便性高い本人確認ができる社会を実現

実現していただきたいことと、その背景

携帯電話不正利用防止法、犯罪収益移転防止法の本人確認手法規定をできるだけ揃える

背景

- 事業者が、グループ企業内で通信事業、金融事業を両方運営しているケースも増えてきており、両省令における本人確認手法の規定が揃っていないことで、事業者の対応負担が上がる
- 社会全体の本人確認にかかるコストを下げる

実現に向けた検討案

オンライン本人確認手法の原則JPKI方式への一本化

従来のオンラインで完結できる本人確認手法で主流である書類の画像+容貌の写真アップロード（いわゆるeKYC厚み方式）の廃止

依拠による本人確認の見直し

これまで犯収法にのみ適用のあった、既に行われた本人確認結果の活用を、携帯法にも適用することで、JPKI一本化による不正対策強化を実現しつつ、事業者やユーザーにとっての利便性を考慮した本人確認を実現

対面本人確認における真贋判定

オンライン本人確認の厳格化によって、対面本人確認が相対的に脆弱になることで、対面本人確認を狙った不正がこれまで以上に増加することを防ぐ

オンライン本人確認手法の原則JPKI方式への一本化

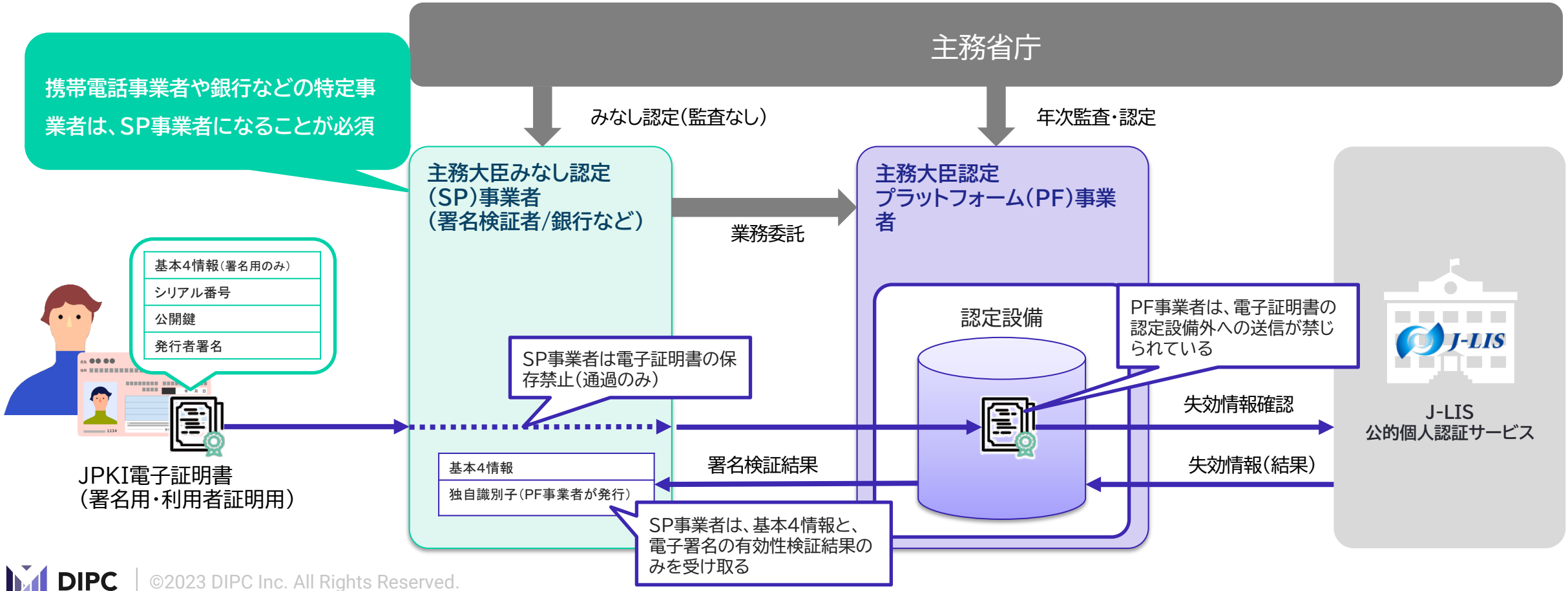
従来のオンラインで完結できる本人確認手法で主流である
書類の画像＋容貌の写真アップロード（いわゆるeKYC厚み方式）の廃止

携帯電話事業者・金融機関を含む700社以上の企業に影響
※eKYCサービスを提供する主要企業の公開情報等から試算

JPKI一本化による旧来方式の廃止だけでは、先行してデジタル化に取り組んできた事業者にとってJPKIへの対応への追加開発などの投資負担が大きくなり、社会全体として前向きな改正とならないのではないか？

参考：公的個人認証プラットフォーム（PF）事業者制度

- 民間事業者が、マイナンバーカードの電子署名を検証（認証）するためには、主務大臣より監査をうけ認定を取得する必要がある
- 認定事業者は、利用者の電子証明書を安全な認定設備内に保管することが義務付けられ、外部送信や目的外利用が厳しく禁じられている
- 認定事業者に、電子証明書の保管を含めた署名検証業務のすべてをPF事業者へ委託することで、設備監査を受けることなく簡易な手続きで認定事業者としてみなす（みなし認定＝SP事業者）制度がある



依拠による本人確認の見直し

現在、犯収法にのみ導入されている、他事業者の実施済み本人確認結果への依拠を、携帯電話不正利用防止法にも導入し、
さらに両省令の適用事業者間（銀行と携帯電話事業者）でも本人確認結果を活用可能に

省令	犯罪収益移転防止法	携帯電話不正利用防止法
規定	施行規則第十三条	規定なし
依拠元	特定事業者に限定 （銀行などの金融機関やクレジットカード会社）	-

JPKIによる本人確認は、大臣認定事業者が署名検証者になることでしか実施できず、その署名結果や電子証明書は、
大臣認定プラットフォーム事業者の設備環境内でしか保管できない

JPKIを前提に考えると、本人確認結果の依拠元は、これまでの「特定事業者」に限定することなく、
公的個人認証（JPKI）で本人確認を実施済みの事業者 ＝ 大臣認定のPF事業者またはSP事業者
とすることで、両省令の施行規則および依拠元の本人確認の厳格さ（IAL）を揃え、かつ
事業者、ユーザーにとって負担の少なく利便性の高い本人確認が実現できるのではないか？

JPKIを前提とした依拠による本人確認を拡大するには当人認証が重要

依拠元の本人確認結果を、第三者に流用されないようにするためには、当人認証レベルを揃える必要がある

	現在	今後
依拠による本人確認が可能な省令	犯罪収益移転防止法のみ	犯罪収益移転防止法および携帯電話不正利用防止法
依拠元	特定事業者に限定 （銀行などの金融機関やクレジットカード会社）	公的個人認証（JPKI）で本人確認を実施済みの事業者 ＝ 大臣認定のPF事業者またはSP事業者
身元確認レベル（IAL）の信頼性	他の特定事業者が犯収法に準拠した本人確認を実施したことを信頼	大臣認定のPFまたはSP事業者が、公的個人認証法に準拠して、署名用電子証明書で本人確認を実施した記録を信頼
当人認証レベル（AAL）の信頼性	特に規定などはない？	**要検討** （依拠元のJPKIによる本人確認実施者がAAL2以上の当人認証で保証するなど）

当人認証が弱いと、本人確認済み結果を
第三者に悪用されるリスクがある

参考：当人認証：ID・パスワードではダメなのか？

ID・パスワードによる認証の限界（人間の認知能力の限界）

- Yahoo! JAPANのアンケートによると、60%以上が「複数のサービスでパスワードを使いまわしている」と回答（2020年7月）
- IDとパスワードは過去の情報流出事故等から、ダークウェブ等で既に大量に流通していると考えられており、今後も情報流出事故を完全に防ぐ事は難しい
- ID・パスワードを認証に用いる以上、流出したIDとパスワードを使った**「リスト型攻撃」**による不正アクセスを防ぐことは難しい
- 近年は**「フィッシング型攻撃」**によってID・パスワードが奪取され、不正アクセスを招く事案が多発している

ID・パスワードのみの認証（単要素認証）は不正アクセスによって突破されることを前提として利用する必要がある。

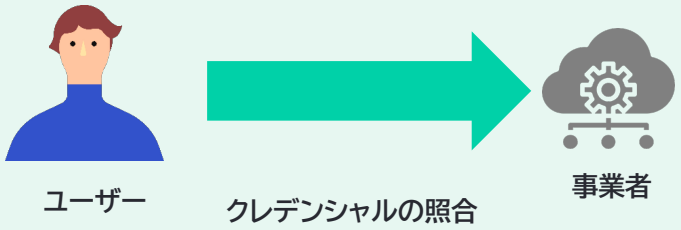
不正にアクセスされても、リスクが大きくないサービスでのみ利用すべき

近年では、携帯電話のショートメッセージ（SMS）にワンタイムパスコードを送信することで、パスワードに加えて携帯電話の所持確認を行うことで、多要素認証を行うケースも増えていますが、以下のような課題があります。

- 電話番号が失われたり、電話番号が変更されたりすると容易に復旧できない（復旧手段が狙われる）
- SMS送信毎に通信料金が発生する
- フィッシングには攻撃には対処できない

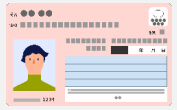
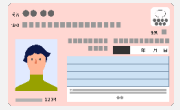
参考：本人確認とは？

本人確認のプロセスは、通常は「身元確認」と「当人認証」の2つの異なるプロセスに分けられます

	目的	プロセス
身元確認  身分証の提示と登録	• 当該ユーザーが実在することを確認する • 当該ユーザーの本人特定事項（基本4情報等）と、その正確性を確認する • 当該ユーザーを重複無く、唯一の自然人に帰着させて登録する	1. 本人特定事項とエビデンス（身分証）を提示・収集する 2. 提示されたエビデンスが本物であるかを確認する（Validation） 3. 提示されたエビデンスが登録しようとしている当人のものかを確認する（Verification） 4. 身元確認完了後、クレデンシャルを発行する
当人認証  クレデンシャルの照合	• ある行為の作業者が、まちがいなく期待される当人によってなされていることを確認する • 操作者と事業者の保持するアイデンティティ情報を確実に対応付ける	• クレデンシャル＝認証の3要素（知識・所持・生体）のいずれかを照合する

参考：本人確認の保証レベル

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によると、
身元確認、当人認証、双方ともにその信頼性を3つのレベルに分けて評価し、低く評価されたほうのレベルを本人確認の保証レベルとみなす

保証レベル	身元確認レベル （Identity Assurance Level / IAL）	当人認証レベル （Authenticator Assurance Level / AAL）
レベル3 身元が対面で確認され 信用度が非常に高い	• 写真付き身分証明書の対面での確認 • 公的な台帳との照合 • 重複登録ではないことの確認 	• 複数の認証要素による認証（多要素認証） • 暗号プロトコル • 耐タンパー性のあるハードウェア 
レベル2 身元が遠隔又は対面で確認され 信用度が相当程度ある	• 公的な台帳との照合、もしくは公的証明書の添付 • 電子署名もしくは署名捺印 	• 複数の認証要素による認証（多要素認証）  SMS認証等
レベル1 信用度ほとんどなし 自己表明相当	• 電子メールの到達確認 	• 単要素による認証 

対面本人確認時における身分証の真贋判定をする方法

- 現在は目視確認による真贋判定に頼っており、精度の高い偽造身分証が台頭してくると真贋判定は困難になっていく
- 真贋判定機は一部導入があるものの、判定結果についてはメーカー保証はない状況
- ICチップ読み取りなどの、マイナンバーカードの真正性が確実に検証可能な仕組みの導入の必要性

マイナンバーカード券面の提示を受けた際に、真贋判定を行う手法

判定手法	目視確認	真贋判定機	New ICチップの読み取りなど
判定結果	目視確認の実施者が真正かどうか判断	真贋判定機に挿入することで、 判定結果が表示される	ICチップの読み取りにより、技術的にカードの真正性が確実に証明される
課題	券面のホログラムや印字など、 人間の目で本物と見分けるには限界あり。	複数メーカーが提供しているものの、すべての店頭窓口で導入されているわけではない。 メーカーは、真贋判定結果を保証していない。	各事業者の店頭窓口への設備投資など コスト面の課題

マイナ保険証の
カードリーダーの活用

懸念点や課題

- カードリーダーと連携する検証ソフトの開発や実装
- 端末費用やアプリケーションの利用料

ユーザースマホ端末上の
アプリで検証

懸念点や課題

- スマホ端末の非所持ユーザーへの対応（新規契約者など）
- アプリやシステムの利用料など

参考：ユーザースマホ端末上のアプリで検証方法

- 既存のアプリを利用することで、無料でカードの真贋の検証が可能

ユーザーのスマホ端末上でICチップ読み取りなどで マイナンバーカードの真贋検証が可能な無料アプリの一例

JPKI利用者ソフト

- iOS/Androidで利用可能
- 無料
- 利用者用証明書または署名用電子証明書の読取り
- J-LISが提供

xID（クロスアイディ）アプリ

- iOS/Androidで利用可能
- 無料
- 署名用電子証明書の読取り
- xIDが提供

検証方法（例）