一般社団法人OpenIDファウンデーション・ジャパン
KYCワーキンググループ

サービス事業者のための、本人確認手続き（KYC）に関する調査レポート

2020年1月
第1.0版

はじめに **3**
KYCワーキンググループ概要と活動目的 3
KYCの定義 **4**
1-1. 本人確認（KYC）とは 4
1-2. 本人確認（KYC）対象となる属性 6
1-3. 本人確認 （KYC） の方法 9
国内事業者におけるKYCの現状 **10**
2-1. 国内事業者におけるKYCの現状調査 11
2.2. 国内事業者に適用される各種業法 18
2-2-1. 犯罪収益移転防止法における本人確認手法 19
2-2-2. 電子署名法における本人確認について 21
2-2-3. 公的個人認証について 24
2.3. KYC事業者が提供するソリューション 25
2-3-1. 株式会社NTTドコモ 本人確認アシストAPI 25
2-3-2. オープンソース・ソリューション・テクノロジ株式会社 LibJeID（リブジェイド） 26
2-3-3. KDDI株式会社 本人確認支援サービス 27
2-3-4. 日本電気株式会社 本人確認サービス「Digital KYC」 29
2-3-5. 株式会社TRUSTDOCK KYC as a Service 30
次世代の目指すべきKYCの姿に向けて **32**
3-1. 海外のKYCサービスの動向 32
3-2. 理想の本人確認（KYC）とは 33
3-3. 本人確認（KYC）の共通化に向けた取り組み 34
3-4. 本人確認（KYC）の共通化とビジネスモデル 36
3-5. 目指す姿に向けての課題 37
KYCに関連する技術要素の調査 **38**
4-1. オンラインにおける本人確認（KYC）のための技術 38
4-2. OpenID ConnectとKYC 42
[コラム 1] 本人確認書類に使われる文字について 43
[コラム 2] Decentralized Identifier（DID）とは 44
用語一覧 **48**
執筆者一覧 **50**

はじめに

本書は、サービス事業者が利用者登録に際して行う本人確認プロセスの設計を行う際に参考とすることを目的にOpenIDファウンデーション・ジャパンが主催するKYCワーキンググループが作成した文書である。

近年、サービス利用登録を行う際のなりすましや身元詐称などによる犯罪が多発しており金銭的な被害も大きくなってきている。金融機関や携帯電話事業者などにおいては利用者登録の際の本人確認の厳格化に関する法整備が進み、それらの犯罪行為への対策が取られてきているが、他の事業者における法整備が十分な状況と言える状況ではない。また、各管轄官庁や業界団体の主導による法令化やガイドライン整備が個別に進んでいることにより、利用者の目線では何度も類似した本人確認が行われ、また事業者目線においても事業を跨いだ本人確認済み情報の共有やプロセスの共通化が出来ず業務効率の向上が見込めない状況にある。

本書では利便性の向上や業務効率化のための第一歩として、①本人確認・KYCとは何なのか、②現状各種事業者が行っている本人確認プロセスはどのような物なのか、③各種法令による要求事項はどのようなものなのか、④国内のKYC関連サービスを提供している事業者のソリューションにはどのような物があるのか、⑤次世代の理想とする本人確認プロセスはどのような物なのか、⑥理想を実現するためにはどのような課題を解決する必要があるのか、について取りまとめている。また、関連する技術要素や昨今注目を集めているブロックチェーンをアイデンティティ領域に活用することにより資格情報等の属性の保証を行うための取り組みである分権型アイデンティティ技術、米国OpenID Foundationで策定に向けたワーキンググループ活動が開始されているID保証に関するOpenID Connectの新仕様であるOpenID Connect for Identity Assuranceについても触れた。

尚、本人確認やKYCなど本書内で使用する用語については本書巻末の用語一覧に定義を記載しているので、適宜参照しつつ読み進めて頂きたい。

本書がこれから本人確認プロセスの実装を検討している事業者や、本人確認・KYCをサービスとして提供しようと考えている事業者が、本人確認・KYCそのものに関する理解、現状と今後の展望についての概略を知る上での一助となれば幸いである。

KYCワーキンググループ概要と活動目的

2019年1月よりOpenIDファウンデーション・ジャパン内のワーキンググループとして活動。本人確認・KYCの現状の課題の分析を通じて次世代KYCのあるべき姿、法令やガイドラインとして調整・整備すべき事項、およびOpenID Connect等のID連携標準が具備すべき機能の洗い出し・検討を行い、社会実装へつなげていくためのきっかけを作ることを目的として活動している。

1. KYCの定義

本章ではKYC（Know Your Customer）業務についての定義を行い、企業担当者が自社サービス等においてKYC業務を行う際に注意すべき事項などについて言及する。

1-1. 本人確認（KYC）とは

KYCという言葉は広義かつ概念的なものであるため、まずは本書内でKYCの中でも最もフォーカスをあてる「本人確認」を念頭に置き定義づけを行う。

KYCの定義を行うに際し、古くからKYC業務を行ってきた金融業界を参照モデルとした。まずは金融業界においてFATF（Financial Action Task Force）というマネーロンダリング等の防止などを目的とした国際機関が発行するドキュメント内の勧告[1]を参考に下図のとおり整理を実施した。

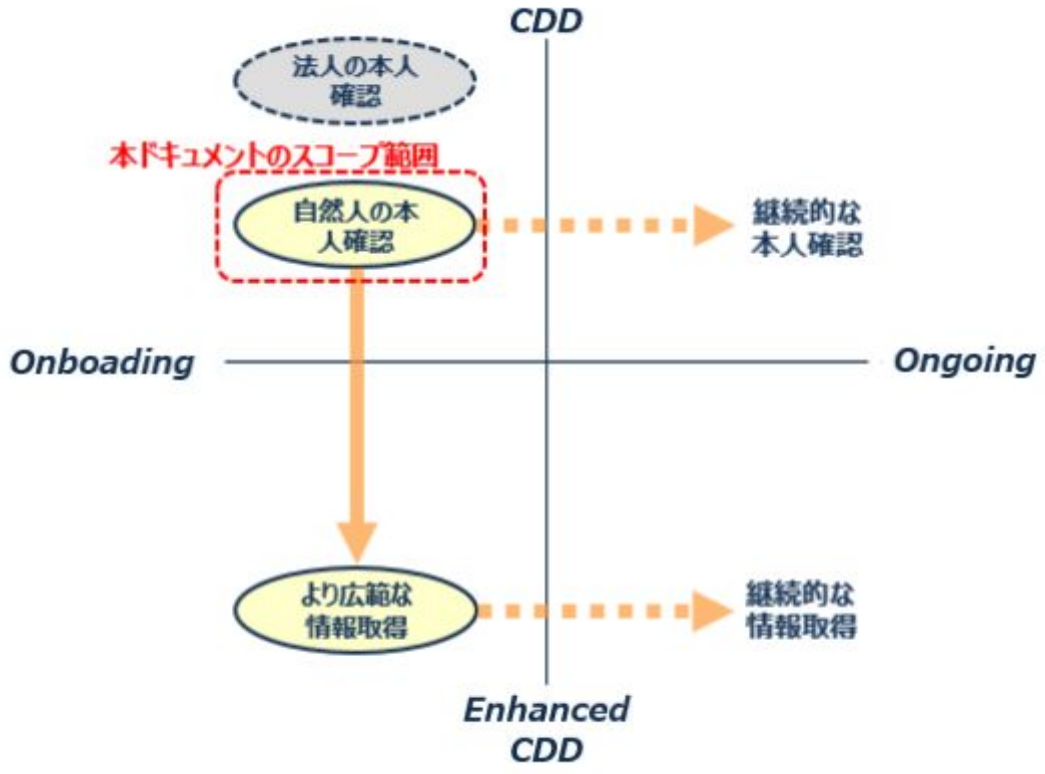

図1-1 本人確認の概念

FATF勧告内では本人確認の対象としては、法人と自然人の2種類が定義されている。尚、同勧告においてはKYCという用語は使われておらず、CDD（Customer Due Deligence）、Enhanced CDDという用語で記載されており、CDDでは信頼性のある機関が発行した証明書や情報を利用し、顧客の本人確認を行う必要性が、またEnhanced CDDでは、取引のリスクに応じて、顧客の職業や資産

[1] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html

状況、収入、資産、外部データベースの調査（反社リストとの突合）などを行う必要性が定義されている。

本人確認を行うタイミングとしては、Onboarding（初回）の他に、Ongoing（継続的）に本人確認を行い、常に顧客の情報を最新化しておくことも求められている。

広義の本人確認という観点では図1-1に記載されている内容すべてが含まれているが、本書においては自然人のOnboarding時のCDDを中心に、本人確認の実施方法を考察していくものとする。

尚、本人確認と混同しやすい用語としては当人確認（認証）という用語がある。当人確認は本人確認が完了しアカウント登録が行われた後に、アカウントの繰り返しの利用に際して同一性の確認を行うためにログイン認証として実施される。広義の本人確認には当人確認も含む考え方もあるが、本書のスコープ外とした。
また、関連する概念として、発行したアカウントを他のサービスに連携する際に利用されるOpenID ConnectなどのID連携プロトコルも存在するが同様に本書のスコープ外とした。

図1-2 本人確認（KYC）と当人確認（認証）とID連携

1-2. 本人確認（KYC）対象となる属性

KYCを実施する際において、個人のどのような情報を確認するのか、また本人確認を行う際に何をもって正しい本人確認とするかに関しては様々な方法が存在する。国内および海外でのKYCに関連する代表的な法律について整理した内容が表1−1となる。

国内では、犯罪移転収益防止法、携帯電話不正利用防止法、古物営業法などにおいて、対象事業者が本人確認を行うことを義務付けている。それぞれの法律の目的は異なるものの、本人確認の定義はほぼ共通となっており、自然人の本人確認として実施する項目としては、氏名、住所[2]、生年月日の3点の確認については共通して必要となる。これらの3点の詳細な確認方法については、それぞれの法律の施行規則などで規定されている。[3]

アメリカでは9−11テロ事件を契機とした発効したUSA PATRIOT Act　第三章において、金融機関での口座開設時の本人確認が規定されており、名前、住所の確認、及び米国政府の提供するテロリストのリストとの照合が義務付けられている。

表1−1 国内外の法律における本人確認事項

	法律	法律の目的	法律内でのKYCの定義*強調部分が対象属性
国内	犯罪収益移転防止法	犯罪による収益の移転防止を図り、併せてテロリズムに対する資金供与の防止に関する国際条約等の的確な実施を確保するため	4条1項 本人特定事項（自然人にあっては**氏名、住居及び生年月日**をいい、法人にあっては名称及び本店又は主たる事務所の所在地をいう。）

[2] 住所のかわりに住居の確認を求める法律もある。住居は住所よりもやや広い概念として用いられているようであるが，大きな違いではないと考えて，本書では特に区別なく扱うこととする
[3] 本書内で参照している各種法律の正式名称は用語集にて定義をしている

	携帯電話不正利用防止法	携帯音声通信事業者による契約者の管理体制の整備の促進及び携帯音声通信役務の不正な利用の防止	3条1項 携帯音声通信事業者は、携帯音声通信役務の提供を受けようとする者との間で、役務提供契約を締結するに際しては、運転免許証の提示を受ける方法その他の総務省令で定める方法により、当該役務提供契約を締結しようとする相手方について、次の各号に掲げる相手方の区分に応じそれぞれ当該各号に定める事項（以下「本人特定事項」という。）の確認（以下「本人確認」という。）を行わなければならない。 一　自然人　**氏名、住居及び生年月日** 二　法人　名称及び本店又は主たる事務所の所在地
	古物営業法	盗品等の売買の防止、速やかな発見等を図るため	第15条 古物商は、古物を買い受け、若しくは交換し、又は売却若しくは交換の委託を受けようとするときは、相手方の真偽を確認するため、次の各号のいずれかに掲げる措置をとらなければならない。 一　相手方の**住所、氏名、職業及び年齢**を確認すること。 二　相手方からその住所、氏名、職業及び年齢が記載された文書（その者の署名のあるものに限る。）の交付を受けること。 三　相手方からその住所、氏名、職業及び年齢の電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。以下同じ。）による記録であって、これらの情報についてその者による電子署名（電子署名及び認証業務に関する法律（平成十二年法律第百二号）第二条第一項に規定する電子署名をいい、当該電子署名について同法第四条第一項又は第十五条第一項の認定を受けた者により同法第二条第二項に規定する証明がされるものに限る。）が行われているものの提供を受けること。

米国	USA PATRIOT Act	2001年のテロリズムの阻止と回避のために必要かつ適切な手段を提供することによりアメリカを統合し強化するための法律 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001	SEC. 326. VERIFICATION OF IDENTIFICATION. (2) MINIMUM REQUIREMENTS.—The regulations shall, at a minimum, require financial institutions to implement, and customers (after being given adequate notice) to comply with, reasonable procedures for— (A) verifying the identity of any person seeking to open an account to the extent reasonable and practicable; (B) maintaining records of the information used to verify a person's identity, including **name, address, and other identifying information**; and (C) consulting lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

1-3. 本人確認(KYC)の方法

KYCの方法については大きく分けて、オンラインもしくは、オフライン(対面)での実施というチャネルの観点と、KYCを事業者自らが実施するか、それとも信頼できる他者からの情報を元に実施するかの観点が存在する。図1-2にそれぞれの観点での日本における代表的な本人確認方法を記載する。

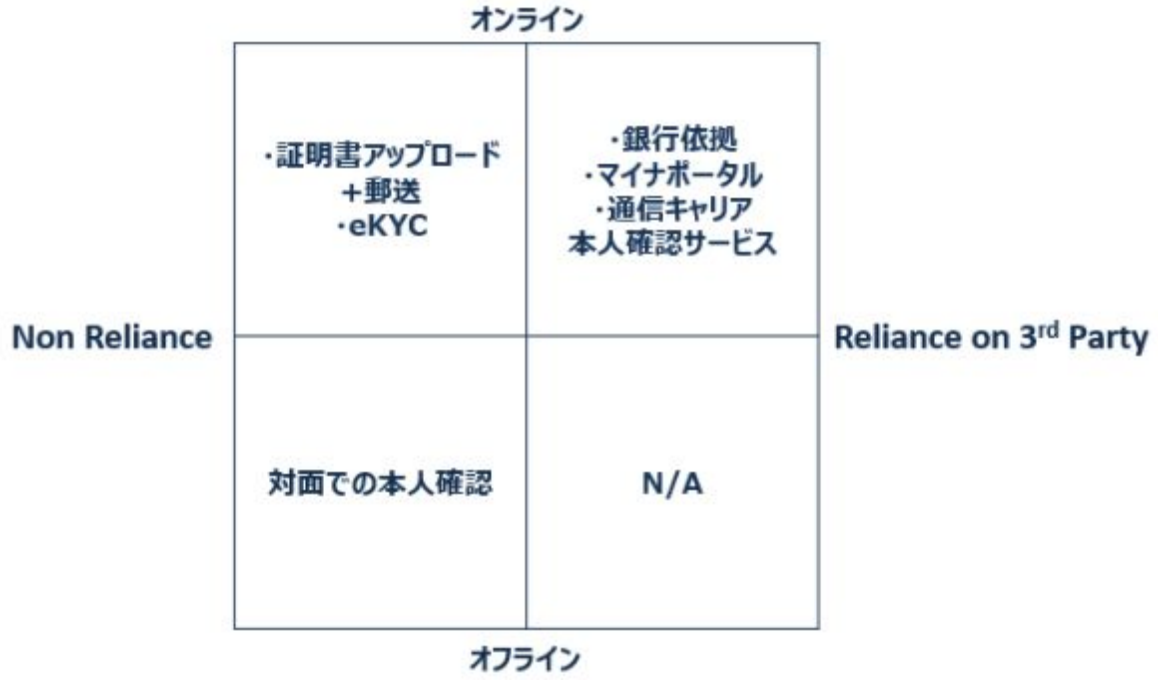

図1-2 本人確認(KYC)の方法

尚、実際の本人確認の手法にはオンラインやオフラインなどで様々な方法が存在するが、それらについては2章以降で詳述する。また、本書で解説するオンラインでの本人確認手法(特にeKYCと呼ばれる)については、現時点で活用が可能なもの、将来的に利用が見込めるものなどの解説を行う。

2. 国内事業者におけるKYCの現状

KYCとは「Know Your Customer」の略で、事業者が、対象となる個人が自社の顧客として適切かどうかを確認する行為全般を指すことは前述の通りであり、業種毎に適用される法令やガイドラインなどにより確認すべき内容・要件が定められている。例えば、金融機関においては、口座開設時などに顧客に運転免許証などの本人確認書類の提出を求め本人確認を行うことが法により義務づけられている。

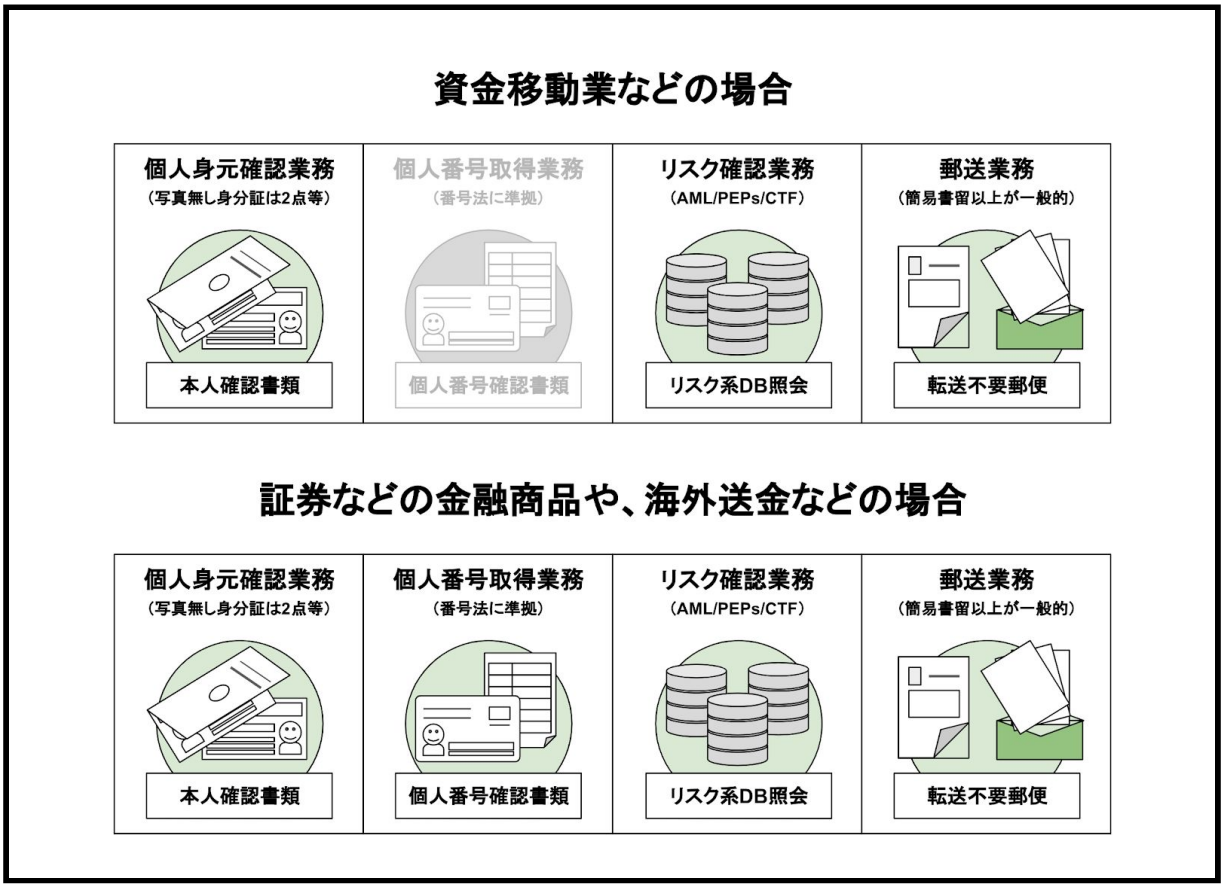

図2-1 業種により必要な要件の例

尚、本人確認（KYC）は金融機関のみならず広く行われている。行政機関で証明書の取得や行政手続きを行う際や、前述の携帯電話不正利用防止法の他にも出会い系サイト規制法（インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律）などの業法に従い実施するケース、業法等の規制がなくとも事業者が自主的に実施するケースも存在する。

2-1. 国内事業者におけるKYCの現状調査

本ワーキンググループでは、現状の日本国内における様々な業種の事業者のKYCの現状のヒアリング調査を行った。調査は資金移動やクレジットカードなどの金融・保険業、携帯電話などの情報通信業、他にも古物の取扱い事業者を対象とし、本人確認の目的、根拠法、確認手法、確認書類、確認のタイミングを調査した。

表2-1 クレジットカード事業者の調査結果

業種	金融・保険業
調査対象の事業者	クレジットカード事業者
本人確認の目的	・法対応上必須対応 ・企業側自主防衛（虚偽不正申込対策、反社会的勢力チェック等）
根拠法	犯罪収益移転防止法
対象業務	・クレジットカード契約（キャッシング機能追加含む）の締結 ・融資専用カードの契約締結と貸付 ・ビジネスカードの契約締結 ・証書貸付の契約締結 ・200万円超の入金
確認方法	対面 ・本人確認書類の提示 非対面 ・本人確認書類（写）の送付＋転送不要郵便での郵送 ・金融機関確認（KYCの依拠） ・取引時確認済み顧客であるかの確認 ・本人限定受取郵便（特伝型）
確認タイミング	・クレジットカード契約（キャッシング機能追加含む）の締結時 ・融資専用カードの契約締結時 ・ビジネスカードの契約締結時 ・証書貸付の契約締結時 ・200万円超の入金時
確認項目	1．通常の取引 ＜個人・法人共通＞ ・本人特定事項（氏名、住居（住所）、生年月日） ・取引を行う目的 ＜個人の場合＞ ・職業 ＜法人の場合＞ ・事業内容 ・実質的支配者の確認による本人特定事項（実質的支配者の氏名、住居（住所）、生年月日）
	2．ハイリスク取引 下記いずれかに該当する取引の場合、厳格な顧客管理による確認を

	行う。 ・なりすましの疑いがある取引 ・本人特定事項もしくは利用目的等を偽っていた疑いがある顧客との取引 ・マネーロンダリング対策が不十分であると認められる特定の国・地域（イラン・北朝鮮）に居住している顧客との取引 ・外国PEPsとの取引（法人と取引をする際の実質的支配者が外国PEPsに該当する場合を含む） ＜厳格な顧客管理による確認項目＞ 200万円超の入金時や証書貸付による200万円超の貸付時の場合 ・過去に確認した本人確認書類以外の書類による本人特定事項の確認 ・「取引を行う目的」「職業(個人の場合)」「事業内容(法人の場合)」「実質的支配者(法人の場合)」の申告による確認 ・資産および収入の状況の確認 外国PEPsの場合 ・過去に確認した本人確認書類以外の書類による本人特定事項の確認（個人・法人・代表者全て） ・「取引を行う目的」「職業(個人の場合)」「事業内容(法人の場合)」「実質的支配者(法人の場合)」の申告による確認 ・実質的支配者との関係性が確認できる書類の確認（法人の場合）
確認書類	＜個人の場合＞ a)顔写真付きの本人確認書類 運転免許証、運転経歴証明書、旅券（パスポート）、個人番号カード（マイナンバーカード）、住民基本台帳カード（顔写真付）、身体障害者手帳、外国人登録証明書、在留カード、特別永住者証明書 上記の他に、官公庁が発行、発給した書類その他これに類するもので、顔写真、氏名、住居（住所）、生年月日の記載があるもの b)顔写真なしの本人確認書類 国民健康保険被保険者証、健康保険被保険者証、船員保険被保険者証、国家公務員組合証、地方公務員共済組合　組合証、印鑑登録証明書、住民票の写し、住民票の記載事項証明書 上記の他に、官公庁が発行、発給した書類その他これに類するもので、氏名、住居（住所）、生年月日の記載があるもの a),b)の本人確認書類に現住居（住所）の記載がない場合や、顔写真なしの本人確認書類1点のみの「提示」を受け、確認する場合は、下記の本人確認書類以外に補完書類を徴求する。 ・国税または地方税の領収書、納税証明書 ・国または官公庁が発行した書類 ・社会保険料の領収書 ・公共料金の領収書（電気、ガス、水道、NHK、NTT東日本・西日本固定電話）
	＜法人の場合＞ ・登記事項証明書 ・印鑑登録証明書
有効期限がない確認	発行日から6ヶ月以内のもの

書類の場合、発行日からいつまで有効とするか	
確認記録の項目	＜個人・法人共通＞ ・取引時確認を行った者の氏名その他の当該者を特定するに足りる事項 ・確認記録の作成者の氏名その他の当該者を特定するに足りる事項 ・本人確認書類の提示を受けたときは、提示を受けた日付及び時刻 ・本人確認書類(写し)の送付を受けた日付 ・取引関係文書を送付した日付 ・「取引の目的」「職業・事業の内容」「実質的支配者の本人特定事項」の確認を行った日付 ・取引時確認を行った取引の種類 ・顧客等が取引を行う目的 ・取引記録等を検索するための口座番号その他の事項 ・本人確認書類の保存方法・保存場所・保存期間 ・口座番号その他の顧客等の確認記録を検索するための事項（確認記録がない場合にあっては、氏名その他の顧客等又は取引を特定するに足りる事項） ・取引の日付 ・取引の種類 ・取引に係る財産の価額 ・財産の移転を伴う取引にあっては（当社の場合は、200万円を超える入金）、当該取引等及び当該財産の移転元又は移転先の名義その当該移転元又は移転先を特定するに足りる事項
	＜個人の場合＞ ・顧客等又は代表者等の本人特定事項の確認を行った方法 ・本人確認書類又は補完書類の提示を受けたときは、本人確認書類又は補完書類の名称、記号番号その他の本人確認書類又は補完書類を特定するに足りる事項 ・顧客等の本人特定事項（氏名、住居及び生年月日） ・職業 ・顧客等が自己の氏名及び名称と異なる名義を取引に用いるときは、当該名義及び顧客等が自己の氏名と異なる名義を用いる理由 ・在留期間等の確認を行ったときは、旅券又は許可書の名称、日付、記号番号その他の当該旅券又は許可書を特定するに足りる事項
	＜法人の場合＞ ・法人顧客の本店に代えて、本人確認書類又は補完書類に記載のある営業所等に取引関係文書を送付するときは、営業所の名称、所在地その他当該場所を特定するに足りる事項及び当該場所の確認の際に提示を受けた本人確認書類又は補完書類の名称、記号番号その他の当該書類を特定するに足りる事項（書類又はその写しの送付を受けたときには当該書類又はその写しを必ず添付） ・顧客等の本人特定事項（名称及び本店又は主たる事務所の所在地） ・代表者等（特定取引の任にあたっている人）による取引のときは、当該代表者等の本人特定事項（氏名、住居及び生年月日）、当該代表者等と顧客等との関係及び当該代表者等が顧客等のために特定取引等の任に当たっていると認めた理由

	・事業の内容、事業の内容の確認を行った方法及び書類の名称その他の当該書類を特定するに足りる事項 ・実質的支配者の本人特定事項及び実質的支配者との関係並びにその確認を行った方法（確認に書類を用いた場合は、書類の名称その他の当該書類を特定するに足りる事項を含む）
	＜ハイリスク取引の場合＞ ・厳格な顧客管理が必要な取引について、本人確認書類もしくは補完書類の提示を受け、又は本人確認書類（写し）もしくは補完書類（写し）の送付を受けたときは、提示又は送付を受けた日付 ・資産及び収入の状況の確認を行ったときは、確認を行った事項に応じ確認を行った日付 ・資産及び収入の状況の確認を行ったときは、確認を行った方法及び書類の名称その他の当該書類を特定するに足りる事項 ・外国PEPsに該当するものであるときは、その旨及び外国PEPsであると認めた理由 ・外国PEPsに該当するものにおいて、既に行った取引時確認（関連取引時確認）確認記録を検索するための当該関連取引時確認を行った日付その他の事項
保管方法	保管方法：データベースによる保管および原本保管
本人確認記録の保存期間	顧客情報消滅から最大10年 （犯収法上は7年だが貸金業法上必要な項目があるため）

表2-2 仮想通貨交換業者の調査結果

業種	金融・保険業
調査対象の事業者	仮想通貨交換業
本人確認の目的	・法対応上必須対応 ・マネーロンダリング防止 ・企業側自主防衛（不正申込対策、反社会的勢力チェック等）
根拠法	・犯罪収益移転防止法 （以下、犯罪収益移転防止法、施行令、施行規則をそれぞれ、法、令、規則と表記し、自然人を対象として代表的な事項を記載。詳細は原文参照のこと）
対象業務	仮想通貨交換業
確認方法	仮想通貨交換業者の取引は、その大半がインターネットを利用した非対面で行われているため、ここでは非対面取引の確認方法について記載する。 ・顧客より本人確認書類（写し）の送付を受け、当該本人確認書類に記載されている住居に宛てに、取引関係文書を転送不要郵便で送付する等の方法（規則六条）
確認タイミング	・顧客との間で、特定業務（仮想通貨交換業）の内、以下の特定取引等を行う場合

	－ 特定取引（法四条一項、令七条、規則五条） ※ 仮想通貨の交換等を継続的に行う契約等及び 特別の注意を要する取引 （疑わしい取引、同種の取引の態様と著しく異なる取引） － ハイリスク取引（法四条二項、令十二条） ※ なりすましの疑い、又は本人特定事項を偽っていた疑いが ある顧客との取引、特定国等に居住・所在している顧客 との取引、外国PEPsとの取引等 ・取引時確認等を的確に行うため、当該取引時確認をした事項に係る情報を最新の内容に保つ等の措置を講ずる場合（法十一条）
確認項目	＜通常の取引時確認＞（法四条一項、規則六条） 前述の「確認方法」及び顧客からの申告により、以下の項目を確認する。 ・本人特定事項（氏名、住所、生年月日） ・取引を行う目的 ・職業 ＜厳格な取引時確認＞（法四条二項、規則十四条） ハイリスク取引に該当する場合、上記の「通常の取引時確認」に加え、以下の確認を行う。 ・本人特定事項について、追加の本人確認書類又は補完書類の提示又は送付による確認なお、提示又は送付を受ける書類は「通常の取引時確認」とは別の書類であること。また、なりすましの疑い、又は本人特定事項を偽っていた疑いがある顧客との取引である場合、関連取引時確認の際とは異なる書類を少なくとも一点用いること。 ・200万円を超える財産の移転を伴うものである場合、資産及び収入の状況の確認
確認書類	・本人特定事項を確認する書類として、運転免許証、運転経歴証明書、在留カード、特別永住者証明書、旅券（パスポート）等（規則七条一項） ・資産及び収入の状況を確認する書類として、源泉徴収票、確定申告書、預貯金通帳等（規則十四条四項）
有効期限がない確認書類の場合、発行日からいつまで有効とするか	各事業者の定めによる
確認記録の項目	前述の「確認項目」の他、確認記録の作成者の氏名、本人確認書類若しくは補完書類又はその写しの送付を受けた日付等（規則二十条）
保管方法	文書、電磁的記録等の方法（規則十九条）
本人確認記録の保存期間	特定取引等に係る契約が終了した日から7年間（法六条二項）

表2-3 携帯電話事業者の調査結果

業種	情報通信業
調査対象の事業者	携帯電話事業者

本人確認の目的	不正利用防止
根拠法	携帯電話不正利用防止法
対象業務	・音声通信役務 ・携帯通信役務
確認方法	対面 ・本人確認書類（原本の提示）など 非対面 ・本人確認書類（写し）の送付＋転送不要郵便または書留郵便
確認タイミング	・携帯電話の契約時 ・譲渡時 ・貸与業者の貸与時
確認項目	・本人確認書類の確認（氏名、生年月日、現住所が記載されており、すべて有効期限内のもの） ・現住所がない本人確認書類の場合、あらかじめ印字されているか、ボールペンなど消せないもので記入されているものに限る ・住所の確認 ・新規契約のお客さまに親展（転送不要）にて「ご契約内容確認のお願い」を送る
確認書類	・運転免許証、在留カード、特別永住者証明書、マイナンバーカード、パスポート ・国民健康保険、健康保険、船員保険、後期高齢者医療若しくは介護保険の被保険者証、健康保険日雇特例被保険者手帳、国家公務員共済組合若しくは地方公務員共済組合の組合員証、私立学校教職員共済制度の加入者証又は自衛官診療証 ・国民年金手帳、児童扶養手当証書、特別児童扶養手当証書、母子健康手帳、身体障害者手帳、精神障害者保健福祉手帳、療育手帳又は戦傷病者手帳 ・印鑑登録証明書、戸籍の謄本若しくは抄本、住民票の写し又は住民票の記載事項証明書 ・イからニまでに掲げる書類のほか、官公庁から発行され、又は発給された書類その他これに類するもので、当該自然人の氏名、住居及び生年月日の記載があり、当該自然人の写真があるもの ・イからホまでに掲げる書類のほか、官公庁から発行され、又は発給された書類その他これに類するもので、当該自然人の氏名、住居及び生年月日の記載があるもの ＜補助書類＞ ・公共料金領収証、または「マイナンバー」の印字がない住民票 ＜その他＞ その他、毎月のお支払いの手続きに必要なもの ・クレジットカード ・キャッシュカード ・預金通帳＋お届け印
有効期限がない確認書類の場合、発行日	発行日から6か月以内のもの

からいつまで有効とするか	
確認記録の項目	・本人確認を行った者の氏名その他の当該者を特定するに足りる事項 ・本人確認記録の作成者の氏名その他の当該者を特定するに足りる事項 ・相手方に係る次に掲げる事項 ・本人確認を行った日付 ・本人特定事項 ・本人確認を行った方法 ・本人確認に用いた書類又は電子証明書の種類及び記号番号その他の当該書類又は電子証明書を特定するに足りる事項
保管方法	顧客管理システムに保持 （法律上は「書面」「マイクロフィルム」「電磁的記録方法」と定められており、顧客管理システムは「電磁的記録方法」にあたる）
本人確認記録の保存期間	・携帯電話契約中は保持 ・解約後3年間は保持

表2-4 古物取引事業者の調査結果

業種	古物取引商等
調査対象の事業者	古物取引事業者
本人確認の目的	・法対応上必須対応 ・マネーロンダリング防止 ・企業側自主防衛（不正対策等）
根拠法	古物営業法
対象業務	古物の買取
確認方法	身分証写真の確認 + 集荷 + 本人の銀行口座への振込
確認タイミング	・契約締結時 ・1万円以上の取引時
確認項目	申請時 ・住所、氏名、職業及び年齢 確認時 ・住所、氏名、年齢
確認書類	運転免許証、健康保険証、パスポートなど
有効期限がない確認書類の場合、発行日からいつまで有効とするか	なし
確認記録の項目	確認書類の情報

保管方法	データベースに保管している
本人確認記録の保存期間	事業者次第のところがあり不明

2.2. 国内事業者に適用される各種業法

ヒアリング調査をした事業者以外でも各種業法により本人確認（KYC）に関する要件が定められている。下表が調査を行った各種業法による要件の概要である。

表2-5 各種業法による本人確認（KYC）に関する要件

	犯罪収益移転防止法	外為法	国外送金等調書法	携帯電話不正利用防止法	古物営業法	出会い系サイト規制法
対象業界・企業	銀行・証券・資金移動・仮想通貨、電話受付代行など	銀行・資金移動業など	国際送金など	携帯電話、音声通話など	古物買取など	婚活サイトなど
本人確認の目的	マネーロンダリング・テロ資金供与防止	マネーロンダリング・テロ資金供与防止	脱税防止	携帯電話を使った犯罪等の防止	マネーロンダリング防止	青少年保護育成
確認書類の例	写真付き本人確認書類 または 写真なし本人確認書類2点	写真付き本人確認書類 または 写真なし本人確認書類2点	マイナンバー取得書類	写真付き本人確認書類 または 写真なし本人確認書類2点	写真付き本人確認書類 または 写真なし本人確認書類2点	本人確認書類1点
本人特定事項等	・氏名 ・生年月日 ・住居	・氏名 ・生年月日 ・住所又は住居	・氏名 ・生年月日 ・個人番号	・氏名 ・生年月日 ・住所	・氏名 ・年齢 ・住所 ・職業	・児童でないこと
確認のタイミング	口座開設時 ハイリスク取引時 継続的顧客確認	海外送金時、両替時	海外送金時	回線の新規契約時 名義変更時	1万円以上の取引時	アカウント開設時

このように業種毎に各種業法や規制が存在しており、事業者は遵守することが求められる。これからKYCプロセスの設計～実装を行う事業者においては、遵守すべき業法および各種業法が成立

した背景にある本人確認を行う目的を十分に理解して設計～実装を行うことが望ましい。

ここからは各種業法による要求事項を深く理解するために犯罪収益移転防止法の要求事項を例にオンライン本人確認の時代に向けた動向を深堀する。また、オンライン本人確認を行う上で必要となる電子署名や公的個人認証に関する本人確認要件についても触れる。

2-2-1. 犯罪収益移転防止法における本人確認手法

従来の非対面本人確認手法

平成30年11月29日までの犯収法の非対面における一般的な本人確認手法は、「写真付きの本人確認書類の写し送付＋転送不要郵便」（犯収法施行規則の6条1項1号で規定）となっていた。
例えば写真付きの本人確認書類（例：運転免許証など）の写真をアップロードし、その内容を確認するという手法である。主な確認項目としては、確認書類の有効期限が切れていないか、書類に隠れや破損がないかなどが含まれる。写真アップロードの代わりに、コピーを郵送するなどの方法も考えられる。
その後、簡易書留などを用いて転送不要郵便を自宅に送ることで、居住確認を行う。ハガキ・封筒など郵便物の種類は問わないが、配達確認を行うことが重要である。配達確認では、簡易書留の配達状況を郵便局などから連携する方法に加え、郵便物にアクティベーションコードを印刷しておき、郵便物受け取り後、利用者にアクティベーションコードを事業者のWEBサイトに入力してもらうことで配達確認をする方法などが存在する。後者の方法を用いると、利用者は郵便物を受けとった直後に取引を開始することができる。
この他に、非対面の確認方法として、電子署名を用いる方法がある。電子署名法における認定認証事業者が発行した電子証明書（氏名，住所及び生年月日の記録のあるもの）、公的個人認証法における署名用電子証明書等と、これら電子証明書に基づく電子署名が行われた情報の送信を受ける方法である。この方法を用いれば、オンラインの手続きだけで確認が完結する。

犯罪収益移転防止法におけるeKYC新手法

平成30年11月30日の改正犯収法にて、「転送不要郵便」が不要な新手法が定義され、ユーザが口座開設完了までにかかる全体の時間を短縮することができるようになった。これまでは、郵便による住所確認により、通常1～2日、土日を挟むと、3～4日ほど、口座開設完了までに時間がかかっていたものが、最短で当日に口座開設を完了することができる様になった。

eKYC新手法は、犯収法施行規則の6条1項1号で規定されており、端的には
・ホ：本人確認書類撮影＋本人容貌撮影
・ヘ：本人確認書類ICチップ読取＋本人容貌撮影
・ト：(本人確認書類撮影 or ICチップ読取)＋銀行連携
の手法がある。

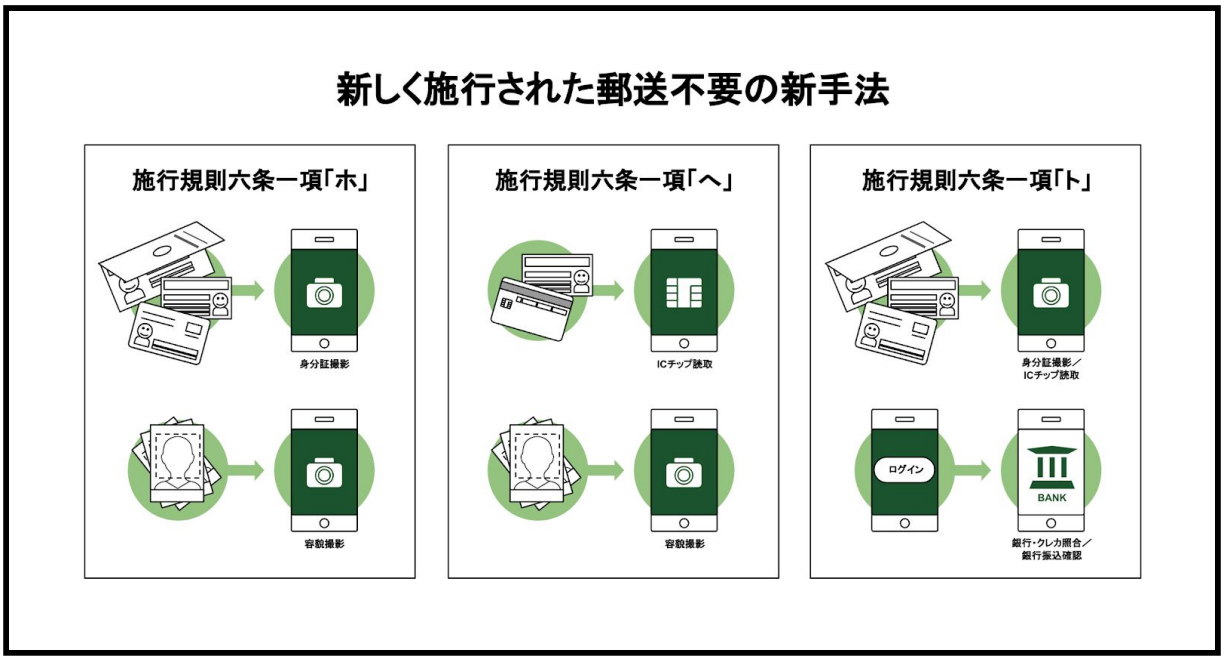

図2-2. 犯罪収益移転防止法におけるeKYC新手法

本人確認書類の真正性を確認するために、ホでは、原本を所持していることを確認するために、表面、裏面に加えて「厚みその他の特徴」を撮影する必要がある。また、本人確認を行うその場で撮影されていることの証明が必要とされている。へでは、運転免許証などに内蔵されたICチップを読み記載事項を取得することで、改ざん耐性を高めている。また、ホ、へでは、その場で端末を操作している人の容貌を撮影し、本人確認書類に貼り付けられた、または、ICチップに内蔵された写真と一致しているか確認する必要がある。このように、郵送を不要とする代わりに、本人確認書類の真正性確認は厳格になっており、一部メディアで言われているように、eKYCは規制緩和と捉えてしまうのはミスリードであり、オンラインでの様々な金融取引での詐欺やマネーロンダリングが多発する昨今、単純な規制緩和ではなく、本人確認の確認を強めるための法改正である、と認識すべきである。言い換えればデジタル時代に対応するためにアナログな世界から移行して行くにあたってのボーダーラインを引いた、と捉えることができる。

2-2-2. 電子署名法における本人確認について

本節では金融や古物のような事業者への適用される業法とは少し主旨の異なる電子署名法について触れる。様々な事業者がオンラインでサービスを提供する様になり、個人から提供される本人確認書類の真正性の確認は非常に重要なものとなってくることは容易に想像がつき、電子署名を行う事業者自身が行う本人確認（KYC）についても重要となってくる。

電子署名法は、本人による一定の要件を満たす電子署名が実施されている場合に、電子文書等が真正に成立した（本人の意思に基づいていること）と推定することを定めた法律である。電子署名法に基づく電子署名は、例えば、電子申請や電子契約、様々な文書の電子保存などに用いられている。さらに、電子署名法では、電子署名に関して本人確認を行う認証業務（電子署名に用いる電子証明書を発行する認証局）で一定の基準を満たすものを特定認証業務として定めている。さらに、特定認証業務は主務大臣（総務大臣、経済産業大臣及び法務大臣）の認定を受けることができる。認定を受けた事業者は認定認証事業者と呼ばれる。

認定認証事業者の基準の一つとして、電子署名法第六条第二項では、利用者の本人確認（真偽確認）を主務省令で定める方法で行うことと定められている。それを受けて、同法施行規則の第五条で具体的な方法について定められている。
電子署名法施行規則第五条を要約すると以下のようなものになる（代理人のケースは割愛する）。

表2-6 電子署名法における本人確認（KYC）に関する要求事項

<table>
<tr><td colspan="3">以下の(I)、(II)のいずれか</td></tr>
<tr><td colspan="3">(I)
以下の書類の提出
・住民票の写し/住民票記載事項証明書
・戸籍の謄本/抄本/領事官の在留証明/これらに準ずるものとして主務大臣が告示で定める書類
かつ、以下の(イ)～(ニ)のいずれか一つ以上。</td></tr>
<tr><td></td><td>（イ）</td><td>以下のいずれか一つ
・旅券
・在留カード
・特別永住者証明書
・官公庁が発行した免許証、許可証もしくは資格証明書
・許可証もしくは資格証明書
・個人番号カード
・官公庁が職員に対して発行した写真入り身分証</td></tr>
<tr><td></td><td>（ロ）</td><td>利用の申込書に押印した印鑑に係る印鑑登録証明書</td></tr>
<tr><td></td><td>（ハ）</td><td>本人もしくは差出人の指定した名宛人に代わって受け取ることができる者に限り交付する郵便（名宛人等であることの確認を行うものに限定）、または、これに準ずる方法で申込事実の有無を照会する文書を送付し、これに対する返信を受領する方法。郵便受け取り時の確認方法は以下のいずれか。

(1) 上記（イ）のいずれか一つ以上
(2) 健康保険、国民健康保険、船員保険等の被保険者証、共済組合員証、国民年金手帳、国民年金、厚生年金保険若しくは船員保険に係る年金証書又は共済年金、恩給等の証書のいずれか二つ以上。
(3)（2）の書類のいずれか一つ以上に加え、学生証または会社の身分証明書または公の機関が発行した資格証明書（（イ）のものを除く）。いずれも写真入りのものに限る。</td></tr>
<tr><td></td><td>（ニ）</td><td>（イ）（ロ）（ハ）に掲げるものと同等なものとして主務大臣が告示で定めるもの</td></tr>
<tr><td colspan="3">(II) 公的個人認証法の署名用証明書による利用申込者の真偽の確認</td></tr>
</table>

上記に加え、当該認定認証事業者において電子証明書がすでに発行されている場合は、その電子証明書を用いて本人確認することが認められている。但し、新たな電子証明書の有効期限は、旧証明書の発行日から5年未満となっている[4]。

[4] 2020年1月の施行規則改正では、告示で定めた士業団体の証明書に限っては「旧証明書の発行日から5年未満」の制限に縛られないものとなった。

認定認証事業者が実際にどのように利用申込者の本人確認を行っているかについては、認定認証事業者が公開している証明書ポリシー(Certificate Policy)で確認することができる。例えば、「セコム認証サービス セコムパスポート for G」[5]の認証ポリシーでは以下のように記述されている。

表 4.1-1 提出書類

タイプB（基本型）		1 利用申込書 2 印鑑登録証明書（発行日から3か月以内のもの）注9） 3 住民票の写し（発行日から3か月以内のもの）注7） 4 戸籍全部事項証明書または戸籍個人事項証明書（発行日から3か月以内のもの） 注8） 5 振込控えもしくは振込控えのコピー（原則必須とする） 注1） 6 代理受取人の印鑑登録証明書（発行日から3か月以内のもの）注4） 7 変更する氏名ローマ字を証明できる書類（パスポート(身分事項のページ)のコピーまたは特別永住者証明書（氏名、有効期限が記載されている面）のコピーまたは在留カード（氏名、有効期限が記載されている面）のコピー） 注10）
タイプB（属性型）	個人用	1 利用申込書 2 印鑑登録証明書（発行日から3か月以内のもの）注9） 3 住民票の写し（発行日から3か月以内のもの）注7） 4 戸籍全部事項証明書または戸籍個人事項証明書（発行日から3か月以内のもの） 注8） 5 振込控えもしくは振込控えのコピー（原則必須とする） 注1） 6 代理受取人の印鑑登録証明書（発行日から3か月以内のもの）注4） 7 変更する氏名ローマ字を証明できる書類（パスポート(身分事項のページ)のコピーまたは特別永住者証明書（氏名、有効期限が記載されている面）のコピーまたは在留カード（氏名、有効期限が記載されている面）のコピー） 注10）
	個人事業主用	1 利用申込書 2 印鑑登録証明書（発行日から3か月以内のもの）注9） 3 住民票の写し（発行日から3か月以内のもの）注7） 4 戸籍全部事項証明書または戸籍個人事項証明書（発行日から3か月以内のもの） 注8） 5 振込控えもしくは振込控えのコピー（原則必須とする） 注1） 6 代理受取人の印鑑登録証明書（発行日から3か月以内のもの）注4）

図2-3. セコム認証サービス資料より(本人確認時の提出書類～抜粋)

[5] https://repository.secomtrust.net/PassportFor/G-ID/repository/CP.pdf

2-2-3. 公的個人認証について

公的個人認証サービスは、住民基本台帳に基づき電子証明書を発行するものである。電子証明書には署名用と認証用の2種類があり、署名用は電子申請における申請書類などへの電子署名に用いられ、認証用はマイナポータルやその他のインターネットサイトへのログイン時の当人確認に用いられる。

公的個人認証サービスについて、公的個人認証法が制定されており、その中で、2種類の電子証明書の内容、発行方法や受け取り方法、電子証明書の発行業務を行う地方公共団体情報システム機構（JLIS）、電子証明書の失効確認を行う際の届出制度についての大枠の要件が定められている。さらに、法律施行令と施行規則によって、より詳細な要件が規定されている。公的個人認証の電子証明書は、希望者に対し、住民基本台帳に従って発行される。住民基本台帳を備える市町村や区の市町村長や区長を経由して地方公共団体情報システム機構が発行する形となる。

2種類の電子証明書はマイナンバーカードあるいは総務省令が定める電磁記録媒体に格納されることとなる（2019年12月18日現在はマイナンバーカードのみ）。マイナンバーカードのICチップ内に格納されるが、マイナンバー自体とは直接の関連がなく、電子証明書にマイナンバーに関する情報は記載されることはない。2種類の電子証明書は誤用を防ぐため、使用時に入力するPINがそれぞれ異なる長さで設定される。認証用電子証明書は4桁の数字に対し、署名用証明書は数字とアルファベットが混在した6桁から16桁の文字となっている（認証用電子証明書のPINはマイナンバーカードの住民基本台帳用のパスワードや券面事項入力補助用のパスワードとは異なるものを設定できる）。マイナンバーカードへの格納については第4章も参照されたい。

署名用電子証明書は、その証明書の内容に基本4情報（住所、氏名、生年月日、性別）が記載されている。そして、住民票の消除や基本4情報に変更があった場合には、その署名用電子証明書は失効される仕組みとなっている。署名用電子証明書を署名付き文書と共に受領者に送ることで、受領者は電子証明書の基本4情報に基づいて本人確認することができる。署名用電子証明書の利用は本人確認を伴う電子申請やサービス申込時の本人確認の用途に適しているといえる。

一方の認証用電子証明書には識別子（電子証明書のシリアル番号）が記載されるのみで基本4情報は記載されない。住民票の消除以外の基本4情報の変更においても認証用電子証明書は失効されない。認証用電子証明書はインターネットサイトのログイン時にそのまま使えることを想定している。署名用電子証明書と認証用電子証明書の対応関係は電子証明書の記載内容自体では判別できないが、JLISに問い合わせることで対応関係を確認することができる。JLISによる照合結果を受け、サービス開始時の本人確認用の申請書類に用いた署名用電子証明書と、以降のサービス利用時のログイン認証に用いた認証用電子証明書が同一の者に属するものであることを確認することができる。認証用電子証明書を更新した場合は電子証明書のシリアル番号が変更されるが、更新前後の同一性はJLISに問い合わせることで確認できる。

上記の利用例のように署名用電子証明書と認証用電子証明書の失効情報を取得して検証を行う民間の事業者や組織は、総務省の定める基準に従い総務大臣の認定を受けたうえで、JLISに対して失効情報取得の届出が必要となる。認定と届出に関してはいくつか形態がある。一つ目は公的個人認証サービスを利用したい（失効情報を確認したい）事業者が直接、総務大臣認定を受け、JLISに届出を行うケースである。二つ目は、ある事業者が公的個人認証サービスによる本人確認

システムの管理を外部のある事業者に委託するケースである。この場合は、システム管理業務を行う委託先の事業者と委託元の事業者が申請や認定の審査に関して対応することとなる。三つ目は複数の事業者が公的個人認証サービスによる本人確認システムの管理を特定のプラットフォーム事業者に委託するというケースである。この場合は、申請や認定の審査に関する対応はプラットフォーム事業者が担うこととなり、委託元となる事業者はそれらの手続きや審査に関する負担は解消される。

2.3. KYC事業者が提供するソリューション

前節までで触れて来たとおり、各種業法はオンライン本人確認を前提とした新たな手法の採用を進めてきており、本人確認（KYC）自体をサービスとして提供する新たな事業者が登場してきている。ここではKYCワーキンググループの会員企業の提供するソリューションを紹介する。

2-3-1. 株式会社NTTドコモ 本人確認アシストAPI

NTTドコモの「本人確認アシストAPI[6]」は、NTTドコモの携帯電話の契約の際に携帯電話不正利用防止法に基づき本人確認した情報を利用して、本人確認の支援をするサービスである。

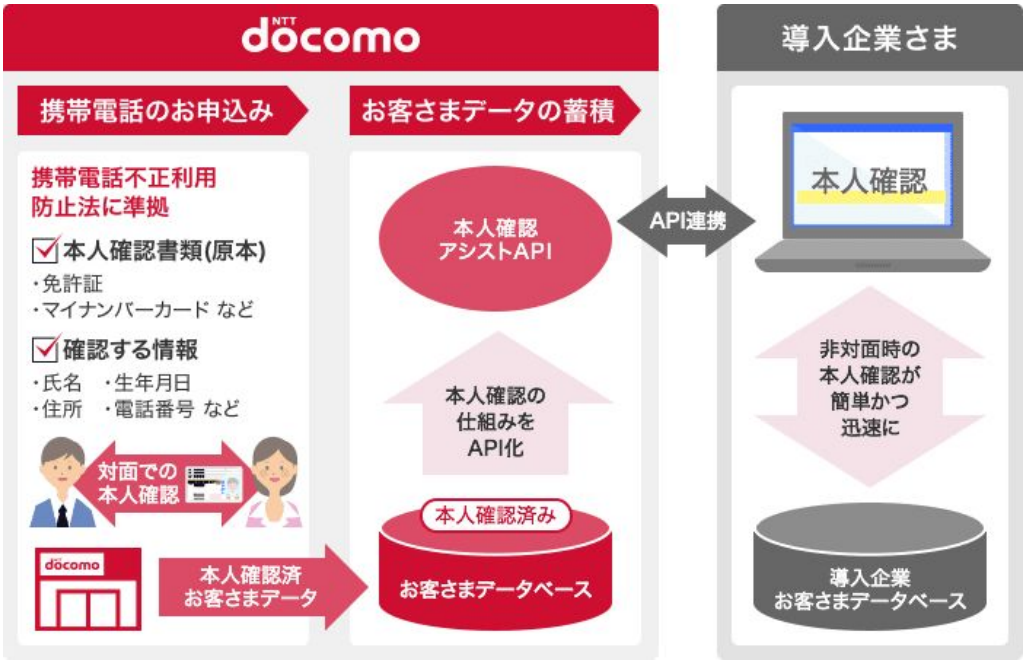

図2-4. 本人確認アシストAPI概要

スマートフォンやタブレットなどでアクセスしてきている携帯電話の契約者情報を連携することで、リアルタイムに本人確認をすることができる。

また、オプションサービスとして携帯電話事業者独自の機能として下記の2つの機能を提供している。

[6] https://www.nttdocomo.co.jp/biz/service/kyc/

①dアカウントログイン
「dアカウントログイン」とは、NTTドコモで提供している共通IDであるdアカウントを利用できる「ログイン代行サービス」である。dアカウントは、スマートフォン・タブレット・パソコンなどでNTTドコモのサービスを利用する時や、dポイントやd払い/ドコモ払いを利用する時に必要なIDである。
「dアカウントログイン」を利用可能なユーザは約6,000万人である。NTTドコモの携帯電話の契約の有無にかかわらず、dアカウントを保有するユーザが利用することが可能である。
※ dアカウントログインのみをご利用することも出来るが、本人確認アシストAPIを利用可能なユーザは、NTTドコモの携帯電話の契約をお持ちのお客様のみとなる。

②回線認証限定オプション
NTTドコモの通信設備下（3G／LTE）での通信に限って、dアカウント認証を行うオプションサービス。所持しているSIMカードの情報と予めNTTドコモに届け出た暗証番号を用いて認証するため、スマートフォンやタブレットなどの利用者を限定することができる。
※Wi-Fi環境下での通信時には3G／LTEに切り替えることを促すエラー画面を出すことができる。

2-3-2. オープンソース・ソリューション・テクノロジ株式会社 LibJeID（リブジェイド）

LibJeID（Library for Japanese Electronic IDentity：リブジェイド[7]）はスマートフォンのNFCで本人確認書類のICチップ読取機能を実装するためのライブラリである。自社で本人確認を必要とするアプリを開発する企業や、KYC事業者が自社のKYCソリューションに組み入れることでICチップ読取の機能を簡単・確実に実装することが可能となる。

2-2-1節の犯罪収益移転防止法におけるeKYC新手法にて記載した通り、2018年11月の犯収法の改正により、ICチップ内データを利用した本人確認手法（施行規則六条一項「へ」）が認められ、既存の本人確認アプリやKYCサービスにICチップ読取機能の追加を求める企業・KYC事業者が増加している。

LibJeIDを活用することで、施行規則六条一項「へ」に則したICチップ読取機能の実装が可能となる。

図2-5. LibJeID概要

[7] https://www.osstech.co.jp/product/libjeid

また、マイナンバーカードを利用した施行規則六条一項「ル」の公的個人認証におけるクライアント側の実装も可能である。
※サーバ側の実装は公的個人認証のプラットフォーム事業者、署名検証事業者になることが必要。

2-3-3. KDDI株式会社 本人確認支援サービス

KDDI 本人確認支援サービス[8]は、au携帯電話の契約時に携帯電話不正利用防止法に基づいて本人確認を実施した個人情報を、ユーザ許諾を取得した上で、パートナー企業様からAPIで送付いただいた個人情報の照合を行い、照合結果を返却するサービスである。

ユーザの操作は情報提供の許諾同意および4桁暗証番号の入力のみとなるため、スピーディな本人確認が可能となる。

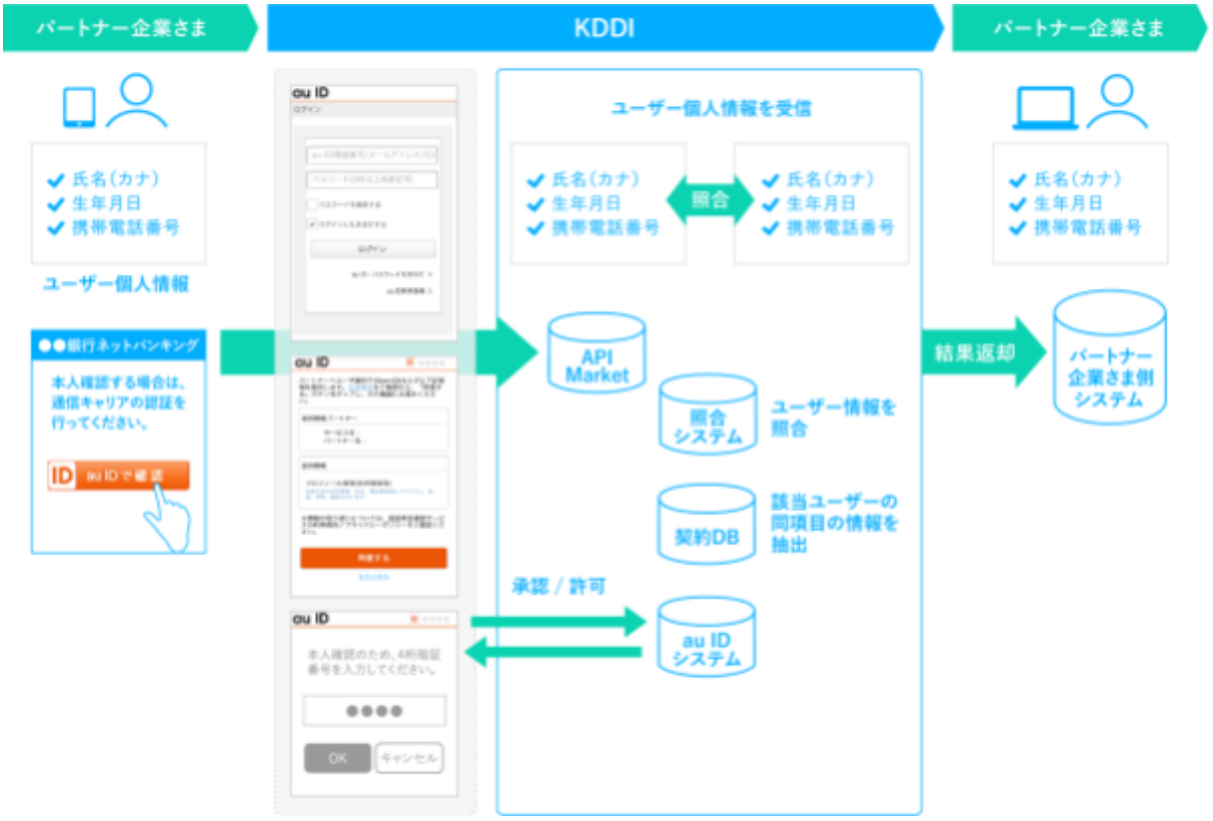

図2-6. 本人確認支援サービス概要

[8] https://iot.kddi.com/services/iot-cloud-apimarket/identification/

2-3-4. 日本電気株式会社 本人確認サービス「Digital KYC」

NEC 本人確認サービス「Digital KYC[9]」は、改正犯罪収益移転防止法に則した形で銀行や証券等の口座開設やサービス入会申し込み時に本人確認書類とスマホ申請者（カメラ）が同一人物かを、NECが得意とする顔認証技術を用いた生体認証技術を活用して検証する。また、口座開設時の登録した顔情報をそのままダイレクトアプリ等の認証（FIDO[10]認証）にて活用することが可能である。本人確認書類（マイナカード、免許書、パスポート等）の文字をAI-OCRで自動読込み機能により後方事務の負担軽減に貢献することが可能である。

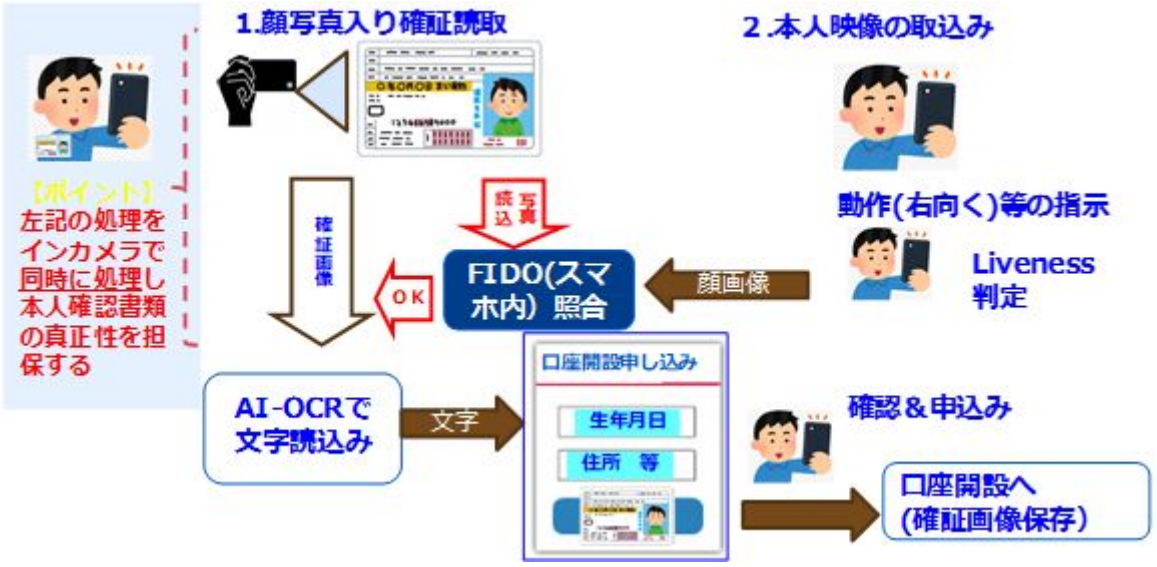

図2-7. Digital KYC概要

【NEC 本人確認サービス「Digital KYC」の主な特徴】

- 既存の金融機関様等のアプリに組み込みやすいように本人確認サービスをSDKで提供
- 容貌と顔写真の照合や、ランダム性のチェックはスマートフォン内で実施することで、通信品質等に影響されずスムーズに本人確認可能
- フロントカメラで「本人確認書類」と「本人の顔」の同時取得時、およびランダムな顔動作指示認証（ライブネス）機能を用いて本人認証を行うことで偽装を防止
- AI-OCRをスマートフォン（Android/iOS）上で実装することで、リアルタイム処理によるユーザビリティの向上、サーバサイドに個人情報を送らないことによるセキュリティの向上
- カメラに写った画像の品質（反射、影等）と簡易的な真贋判定を実施（特許出願済）し、識字率がよい画像を自動取得してOCR処理を行うことによる後方事務作業の軽減が可能
- 運転免許証、マイナンバーカードのICチップを読み込む機能による真贋判定の向上と後方事務作業の軽減が可能（拡張機能）
- 口座開設時の登録した顔情報をそのままダイレクトアプリ等のFIDO認証にて活用可能
- 世界トップクラスの顔認証技術（Bio-IDiom）[11]の利用による精度の高い照合を実現
- 大規模ユーザの採用実績（LINE Pay様、じぶん銀行様等、多数の大規模導入実績あり）

[9] https://jpn.nec.com/fintech/kyc/index.html
[10] FIDO: Fast IDentity Online の略語で、従来のパスワードに代わるとみられている認証技術
[11] https://jpn.nec.com/biometrics/index.html

2-3-5. 株式会社TRUSTDOCK KYC as a Service

TRUSTDOCKは、KYCに必要な業務プロセスを、クラウドサービス化して提供している。業務ソフトウェアやツールだけを提供するSaaS（Software as a Service）とは異なり、目視を含め必要なオペレーションも含め「KYC as a Service」として提供している。

日本で唯一のデジタル身分証アプリとeKYC/本人確認APIサービスでは、犯収法をはじめ、携帯電話不正利用防止法、古物営業法、労働者派遣法、出会い系サイト規制法、民泊新法など、各種法律に準拠したKYCをAPI組み込みのみで実現することが可能である。

図2-8. KYC as a Service概要

郵送不要でネット完結の本人確認を実現するeKYC専用ソフトウェアである、デジタル身分証アプリ「TRUSTDOCK」は、施行規則六条一項「ホ／ヘ／ト／チ」をはじめ、公的個人認証による「ワ」など、あらゆる本人確認手法を内包した身分証専用のアプリである。同アプリは「運転免許証／運転経歴証明書／パスポート／マイナンバーカード／住基カード／在留カード／特別永住者証明書」など幅広い本人確認書類に対応している、唯一のデジタル身分証アプリである。

デジタル身分証アプリとセキュアにAPI連携するKYCプラットフォームとして、国内外を問わず、広くデジタルアイデンティティ基盤の構築を行い、社会への貢献を目指す。

	H30/11/29まで	TRUSTDOCKの対応	H30/11/30以降	H32/4施行予定
1	イ 写真付き本人確認書類1点の提示(対面)	×	イ 写真付き本人確認書類1点の提示(対面)	イ 写真付き本人確認書類1点の提示(対面)
2	ロ 本人確認書類1点の提示(対面)＋転送不要郵便物等	×	ロ 本人確認書類1点の提示(対面)＋転送不要郵便物等	ロ 本人確認書類1点の提示(対面)＋転送不要郵便物等
3	ハ 本人確認書類2点の提示(対面)	×	ハ 本人確認書類2点の提示(対面)	ハ 本人確認書類2点の提示(対面)
4	ニ 保険証等1点の提示(対面)＋住所記載の補完書類1点の送付	×	ニ 保険証等1点の提示(対面)＋住所記載の補完書類1点の送付	ニ 保険証等1点の提示(対面)＋住所記載の補完書類1点の送付
5			ホ (新設) 専用ソフトウェアにて 写真付き書類の写し1点(厚みその他の特徴＋本人確認時に撮影されたもの)の送信 ＋ 容貌(本人確認時に撮影されたもの)の送信	ホ 専用ソフトウェアにて 写真付き書類の写し1点(厚みその他の特徴＋本人確認時に撮影されたもの)の送信 ＋ 容貌(本人確認時に撮影されたもの)の送信
6			ヘ (新設) 専用ソフトウェアにて 写真付き・ICチップ付き本人確認書類のIC情報の送信 ＋ 容貌(本人確認時に撮影されたもの)の送信	ヘ 専用ソフトウェアにて 写真付き・ICチップ付き本人確認書類のIC情報の送信 ＋ 容貌(本人確認時に撮影されたもの)の送信
7			ト (新設) 専用ソフトウェアにて 書類の写し1点(厚みその他の特徴＋本人確認時に撮影されたもの)の送信 or ICチップ情報の送信 ＋ 銀行・クレカ情報との照合 or 既存銀行口座への振込	ト 専用ソフトウェアにて 書類の写し1点(厚みその他の特徴＋本人確認時に撮影されたもの)の送信 or ICチップ情報の送信 ＋ 銀行・クレカ情報との照合 or 既存銀行口座への振込
8				チ (変更) 本人確認書類の原本1点の送付 or ICチップ情報送信 or 書類1点(厚みその他の特徴＋本人確認時に撮影された証明)の送信 ＋ 転送不要郵便
9	ホ 本人確認書類の写し1点の送付 ＋ 転送不要郵便	○ 運用中	チ 本人確認書類の写し1点の送付 ＋ 転送不要郵便	リ (新設) 本人確認書類の写し2点の送付 or 本人確認書類の写し1点+補完書類1点の送付 ＋ 転送不要郵便
10				ヌ (新設) 給与振込口座の開設、または 有価証券でマイナンバー済みの場合 本人確認書類の写し1点の送付 ＋ 転送不要郵便
11	ヘ 本人限定郵便	○ 開発完了	リ 本人限定郵便	ル (変更) 本人限定郵便(受取時の確認書類は、写真付き本人確認書類でないとダメ)
12	ト 電子証明書＋電子署名	×	ヌ 電子証明書＋電子署名	ヲ 電子証明書＋電子署名
13	チ 公的個人認証(電子署名)	△ 実証実験済	ル 公的個人認証(電子署名)	ワ 公的個人認証(電子署名)
14	リ 特定認証業務の電子証明書＋電子署名	×	ヲ 特定認証業務の電子証明書＋電子署名	カ 特定認証業務の電子証明書＋電子署名

図2-9. 犯罪収益移転防止法への対応状況

3. 次世代の目指すべきKYCの姿に向けて

ここまで国内の本人確認に関する状況や本人確認(KYC)に関するソリューションを説明してきた。本章では次世代に向けて目指すべき姿を検討する為、先行する海外の事例について調査を行い、今後の本人確認(KYC)の理想像を定義するための検討軸の設定、および確認済み属性を安全に共有するためにOpenID Foundationが策定を進めている仕様について解説する。また、次世代KYCが普及するために必要となるビジネスモデルはどのようなものなのか、今後解決すべき国内の現状とのギャップについても述べる。

3-1. 海外のKYCサービスの動向

海外では、サービス提供者に対して本人確認機能の提供や業務代行を行う事業者(本書内ではKYC Providerと呼ぶ)が出てきており、①政府による電子化された本人確認書類による本人確認、②銀行による本人確認、③携帯電話事業者による本人確認と大きく3パターンあることがわかった。

しかし、日本においては①～③を1社で提供できる有力なプレイヤーが確立していないこと、また、サービス提供者がサービス提供者の責任で本人確認をしなければならないことなどの理由により、①～③の本人確認が普及していない状況にある。

また、平成30年11月の犯罪収益移転防止法の改正に伴い、非対面での本人確認手法が法制度化されたことから、金融業界では様々なKYCソリューションの提供者がでてきている。しかしながら、犯罪収益移転防止法の本人確認手法は、最終的には人手での確認が必要でコストがかかるため、金融業界以外では費用対効果に見合わないのが現状である。

そのため、本人確認手法が法制度化されていない業界では、犯罪収益移転防止法ほど厳格ではなく、かつ人手の確認が不要な本人確認のガイドラインの策定が求められている。

表3-1. KYC Providerのパターン

	パターン	概要	例
①	政府による本人確認を利用	政府が発行した電子的な本人確認書類またはIDにより本人確認を行う	エストニア(eIDカード[12]) インド(India Stack, Aadhaar[13])
②	銀行による本人確認を利用	銀行口座開設時の本人確認済みの情報を利用し、銀行口座のIDにより本人確認を行う	スウェーデン(Bank ID[14])
③	携帯電話事業	携帯電話契約時の本人確認済みの	韓国(T Authenticaion[15])

[12] https://e-estonia.com/solutions/e-identity/id-card/
[13] https://indiastack.org/
[14] https://www.bankid.com/en/
[15] https://www.gsma.com/identity/wp-content/uploads/2018/10/SKT-Turkey-presentation-final.pdf

	者による本人確認を利用	情報を利用し、携帯電話事業者のIDまたは電話番号で本人確認を行う	アメリカ（Payfone[16], Zenkey[17]） GSMA（Mobile Connect[18]）

3-2. 理想の本人確認（KYC）とは

理想的な本人確認（KYC）の姿を定義するため、「制度面」「認知度」「ユーザカバレッジ」「ユーザ体験」「セキュリティ」「コスト」の6つの観点で課題と目指すべき姿について議論・整理を行った。

例えば、金融与信については、信用情報機関がアグリゲータとして、割賦販売やクレジットカードの開設等の際に情報を集約し標準化することで、信用情報提供を行っている。本人確認においても、同様のアプローチで本人確認手法や確認対象属性の標準化を行い業務集約することで効率化が図れるのではないか、というような議論を行った。

表3-2. 理想の本人確認（KYC）に関する観点

	観点	課題	目指すべき姿
1	制度面	業界や法制度において本人確認に関する法制度ややり方がバラバラ	金融業界だけでなく、様々な業界において統一的な本人確認のガイドラインが制定されている
2	認知度	本人確認手法やKYC Providerについて認知度が低い	本人確認手法やKYC Providerに対してエンドユーザに対する認知・理解ができている
3	ユーザカバレッジ	日本国内において1社で日本の人口をカバーできるKYC Providerが存在しない。	複数の本人確認手法や適切なKYC Providerを提供し、日本の人口をカバーする
4	ユーザ体験（UI/UX）	エンドユーザのアクセス環境によって、提供される本人確認手法やKYC Providerが制限される	エンドユーザのアクセス環境（スマートフォン、パソコン）や利用状況（所持している本人確認書類、銀行口座、携帯電話など）により適切な本人確認手法を提供できる
5	セキュリティ	KYC Providerの当人認証のセキュリティによっては別人の本人確認がされてしまう 。	KYC Providerの当人確認（認証）の基準の標準化が必要
6	コスト	犯収法においては、最終的に人手での確認が必要なため、コストがかかる。	AI等の技術を利用し、本人確認のプロセスを完全に自動化することで、コストを下げる

[16] https://www.payfone.com
[17] https://myzenkey.com
[18] https://www.mobileconnect.io/

上記をふまえ、本人確認（KYC）の理想像として、サービス事業者がエンドユーザのアクセス環境や利用状況に応じた複数の本人確認手法を提供することが望ましい（下図）。しかし、サービス事業者が複数の本人確認手法を提供することは開発・運用コストがかかるため、本人確認を束ねる外部事業者であるKYC Providerが必要となると考えられる。

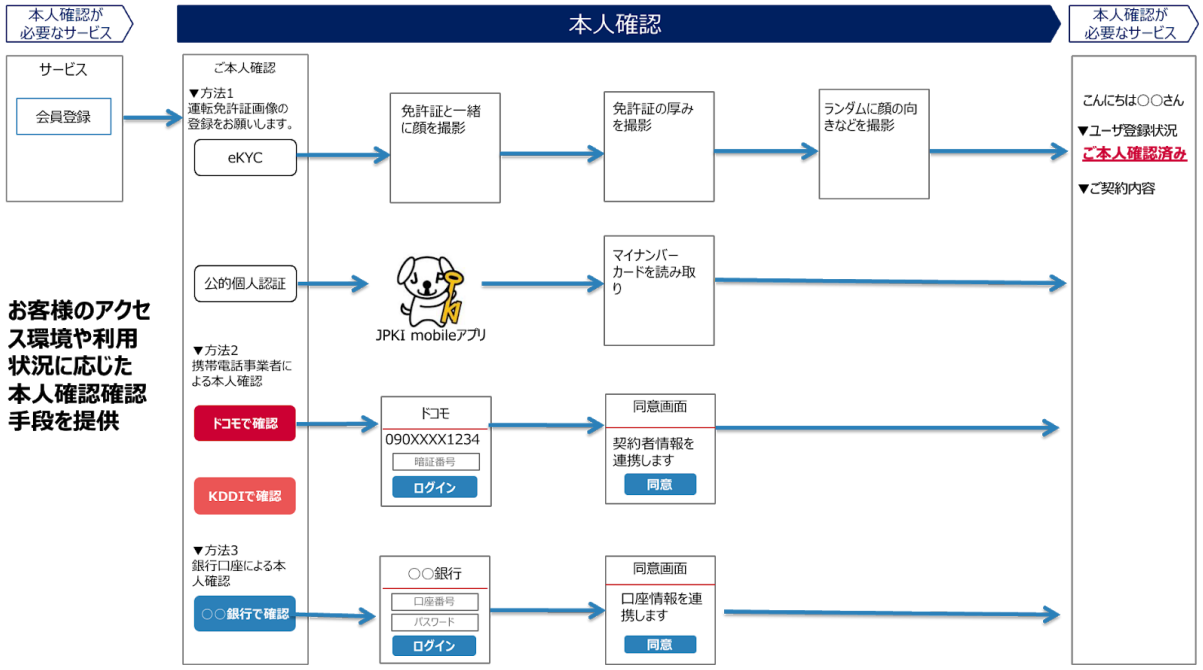

図3-1. 顧客登録における理想的な本人確認（KYC）の姿

3-3. 本人確認（KYC）の共通化に向けた取り組み

本人確認において、業界で定められている法律により本人確認するべき属性情報が異なっている。共通的な項目は氏名・生年月日・住所の属性情報のみである。

今後本人確認の共通化を進めるにあたり、確認対象として共通化すべき属性の案を下表に示す。尚、OpenID Foundationでは2020年よりeKYC and Identity Assurance Working Group[19]を立ち上げ、本人確認に関するプロトコルと属性の標準化に向けたOpenID Connectの新しいプロファイルであるOpenID Connect for Identity Assurance[20]の策定を進めている。

下表では共通化すべき項目として、本人確認をした本人確認書類に関わる情報、KYC Providerで本人確認した時の年月日情報、本人確認の受付を事後に確認できる受付番号を記載している。これらの属性情報を本人確認時に取得しておくことによりサービス事業者が個別に本人確認用の属性を個人から取得しなおすことなく再利用することが可能になるはずである。

[19] https://openid.net/2019/12/28/openid-connect-for-identity-assurance-now-has-a-dedicated-home/
[20] https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

また、他にも共通化の検討が必要な項目として生体認証情報、信用スコア情報、住所コード、地域メッシュコードを記載した。これらの属性情報はそもそも本人確認用の属性として利用可能なのか制度面・技術面の両面からの検討が必要であり、今後議論が必要となってくるだろう。

表3-3. 共通化すべき本人確認属性

	カテゴリ	項目	詳細	OpenID Connect for Identity Assurance上の定義
1	共通的な項目	氏名	本人確認する人の氏名	4.2 claims Element name
		氏名カナ	本人確認する人の氏名カナ	
		住所	本人確認する人の住所	4.2 claims Element address
		生年月日	本人確認する人の生年月日	4.2 claims Element birthdate
2	共有化した方がいい項目	本人確認書類の区分	運転免許証、保険証、マイナンバーカード、パスポート、在留カードなど何の本人確認書類で本人確認したのかの区分情報	4.1.1.1 id_document document:type
		本人確認書類の番号	運転免許証番号、保険証番号などの番号 ※マイナンバーは事業者によって取得できないため、対象外	4.1.1.1 id_document document:number
		本人確認書類の券面画像データ	本人確認書類の券面の画像データ	
		本人確認書類の有効期限	運転免許証、保険証、マイナンバーカード、パスポート、在留カードなどの有効期限	4.1.1.1 id_document document:date_of_expiry
		本人確認手法の区分	犯収法施行規則で定められた本人確認手法や、その他の法制度で定められた本人確認手法、KYC Providerで本人確認したなどの区分情報	
		前回本人確認日	KYC Providerにて前回法律に基づいて本人確認をした年月日（例：銀行窓口で前回本人確認した年月日や、携帯電話の機種変更時に本人確認した年月日など）	
		アカウント開設日	KYC Providerにてアカウントを開設した時期（例：銀行口座を開設した年月日や携帯電話を契約した年月日 など）	4.1.1.1 id_document document:date_of_issuance

		本人確認受付番号	本人確認の依頼を受付時に払いだすユニークな番号。事後に確認するときに利用する。	3.2 txn Claim transaction id
3	共有化に検討が必要な項目	生体認証情報	顔認証、指紋認証、静脈認証、虹彩認証などの生体認証に関わる情報	
		行動履歴のスコアリング	各事業者によって保持しているエンドユーザの行動履歴をスコアリングした情報	
		住所コード	住所表記のブレを吸収するために、住所コードで照合 ※国土地理協会が発行する「全国町・字ファイル」に掲載されている住所コード	
		地域メッシュコード	住所表記のブレを吸収するために、地域メッシュコードで照合 ※JIS X 0410 地域メッシュコードなど	

3-4. 本人確認（KYC）の共通化とビジネスモデル

本人確認（KYC）の共通化を進める上で忘れてはならないのが、共通化によりサービス事業者やKYC Provider、ソリューション提供者などのステークホルダーにとって共通化モデルがビジネスとして成立するかどうか、という観点である。

現状、一部のKYC Providerや本人確認手法のソリューション提供者はサービス事業者に対して、トランザクションに応じた対価（API課金など）を得られる仕組みで提供している。しかしながら、本人確認に関する市場規模は未知数なところもあり、トランザクション数と価格がスケールしていない状況にあり、普及までにはしばらく時間がかかる見通しである。

本人確認（KYC）の共通化はエンドユーザやサービス事業者にとって間違いなくメリットがあると考えられるため、今後は現状の本人確認に関するコストを明確化（人件費・郵送費など）し、外部サービスを利用することでコストメリットがあることを訴求していく、という活動が必要となる。

3-5. 目指す姿に向けての課題

ここまで理想の本人確認（KYC）を実現するには、サービス事業者が個人に対して複数の本人確認手法を個人の利用シナリオに併せて提供していくこと、そのためには確認対象属性の標準化、確認手法やKYC自体をサービスとして提供する外部サービス事業者であるKYC Providerの存在が重要であることを述べた。

しかし、現状の国内における本人確認の状況を見ると前節で触れたビジネスモデルの件の他にも様々な課題が見えてくる。例えば、その一つが本人確認（KYC）に利用する本人確認書類自体の限界に関する物である。

現状の本人確認書類は、ある時点での正しい本人特定事項を表しているものと推定できるものではあるが、当該の個人に関する最新の状況を表しているとは限らない。運転免許証とパスポートを例に挙げると、運転免許証は住所や氏名に変更があった場合などは、記載事項変更[21]を届け出なければ更新されない。また、海外滞在中に一時帰国で運転免許証を更新する場合は、一時滞在先を住所地とした免許証の更新が認められてしまう[22]。同様にパスポートについても、住所については所持人が自由に記入可能であり居住確認などは行われない。これらの事情により、レアケースではあるが、運転免許証やパスポートの自体の真正性確認を行ったとしても記載されている情報が個人に関する最新の属性を表していない可能性が存在する。
また、他の課題として、本人確認書類に記載される属性を使っても本人特定が困難なケース（氏名・住所・生年月日等が一致するケースや、容貌が似通っているケース）も考えられる。

もちろん、これらの本人確認書類自体の限界に起因する本人確認（KYC）の難しさが存在したとしても、政府機関においては本人確認書類の番号をもちいた本人確認が可能であり、法律上でKYCが要求されているケースにおいては、大きな問題とはならない。しかし一方で、サービス事業者が自発的に本人確認（KYC）を行うケースや、サービス事業者が確認に使った属性情報を活用する場合は、このような限界が存在していることを十分に念頭において運用すべきである。

今後、KYC Providerなど外部サービス事業者の利用が促進されてくると、多くの事業者が本人確認（KYC）を気軽に利用できるようになると考えられるが、本人確認書類に頼った本人確認だけでなく、オンラインで政府のもつ最新のデータベースを参照できる様にする等の対応が必要になってくるだろう。

[21] https://www.npa.go.jp/policies/application/license_renewal/japan.html#p3
[22] https://www.npa.go.jp/policies/application/license_renewal/living_abroad.html

4. KYCに関連する技術要素の調査

ここまで本人確認（KYC）に関する現状と今後の展望について述べたが、本章ではKYCに関連する技術要素について解説を行う。

4-1. オンラインにおける本人確認（KYC）のための技術

本節では顧客に非対面本人確認を実施したいサービス事業者のために、技術的な視点にフォーカスして解説する。まず始めに、オンライン（非対面）における本人確認に利用されている技術について解説する。

本人確認を実施する主な目的のひとつは法令準拠であるが、現在の法令で記載されている施行規則で判断する限り、オンラインで完結するものはまだまだ少ない。多くは対面による本人確認の要求や、郵送による確認プロセスが含まれている。しかし、昨今では国もマイナンバーカードの普及に尽力していることや、インターネット上での本人確認の規制強化を強めていることなどを背景に、オンラインで完結する本人確認手法が緩和されつつあり、その流れは今後も期待できる。オンラインで完結する本人確認手法のメリットはいくつかあるが、主な導入のモチベーションは本人確認終了までの速さとコストにある。本技術を解説する前に、第3章の表3-2「理想の本人確認（KYC）に関する観点」をベースに非対面本人確認における技術的な評価軸を定義する。ソリューションを採用しようとした時のひとつの判断になれば幸いである。

表4-1. オンライン本人確認に関する技術の評価軸

評価軸	内容
ユーザカバレッジ	ユーザ環境においてその技術が利用できる範囲が広いかどうか。汎用ブラウザ環境だけで利用できるのが最も望ましい。アプリ提供で実現する場合は、インストールという障壁がある。特化デバイスが必要なケースではより適用範囲は小さくなるだろう。特にWEBサービスの場合、本人確認処理への誘導がWEBサイト側からになると想定されるので、アプリへの誘導は大きなハードルになる。適用範囲が狭い場合、せっかく導入した本人確認が利用されず、その他の確認手段に流れコストが増加する恐れがある。
ユーザ体験（UI/UX）	本人確認プロセスに到達したユーザが、離脱することなく本人確認に成功した確率。複雑な行動をユーザに求めるほど、ユーザは面倒になって本人確認処理をやめてしまう。本人確認プロセスまで到達したユーザは、強いサービス利用意思を有して来訪してきていると考えられるため、ここでの離脱は売り上げに直結する可能性が高い。そのため、離脱の小さい優れたユーザ体感が重要である。
セキュリティ	その技術によって獲得した本人確認情報が正しいかどうか。運転免許証やマイナンバーカードなどのカードは比較的簡単に見た目を模倣した偽造カードを製造できるので、そういったなりすましに対する対策が求められる。また、本人確認書類と登録しようとする本人の一致性を見極める能力も必要となる。こういった対策がなされ

	ていないと、悪意を持った攻撃者に侵入され被害を生み出す可能性が高くなる。
コスト	その技術を利用するためのコスト。コストには初期導入費用や年間の維持費用、及びサービス品質を維持するためのコストなども含まれる。基礎となるセキュリティが脆弱な技術は、攻撃対策のために常に改善を実行するコストが必要となるであろうし、複雑な仕組みを持つ技術は、OSバージョンアップなどに追従する費用が大きくなる可能性も高くなる。

ここでは上記の評価軸を念頭に、現段階で最もニーズがあると想定される犯収法の施行規則において、現実的にユーザストーリーとして採用される可能性がありそうな非対面手法をピックアップし、利点・欠点を交えていくつか解説していく。

- 本人確認書類の画像送信＋本人の容貌の画像送信
  犯収法施行規則6条1項1号ホに則った適用例を紹介する。本技術の特徴は汎用カメラと本人確認書類のみで実現できることにある。最大の利点として、犯収法に準拠した形で構成できる技術のうち、唯一Webブラウザ上で完結できるソリューションであり広い適用範囲を持っている。しかし、カメラで撮影した本人確認書類の情報を根拠とするので、偽造カードの流用や、本人確認書類の顔画像と被写体のユーザの顔の一致性の精度、OCRの精度などセキュリティ上心配も少なくない。また、法令施行規則の準拠のために複雑な遷移を兼ね備えていることが多い。

- ICカード読み取り+本人の容貌の画像
  犯収法施行規則6条1項1号ヘに則った適用例を紹介する。本方式の特徴はICチップ付き本人確認書類をICカードリーダで読み込ませ、そこから取得する本人確認情報を利用することによって実現することである。ICカードから読取る情報としては氏名、住居、生年月日、容貌画像が求められる。本方式の対象となる主たる本人確認書類は運転免許証、マイナンバーカード、在留カードである。パスポートは住居情報がICチップに格納されていないため本方式の対象とならない。
  利点としてはICチップの情報は発行主体によって電子署名がなされており公開鍵暗号基盤によって真正性の検証が可能であるため、世に溢れているほぼ全ての偽造本人確認書類が券面に印刷された情報のみの模倣であることを考えると、偽造カードを利用される恐れがほとんどないことだ。公開鍵暗号基盤による真正性の検証のためにはトラストアンカーとなる各本人確認書類の発行主体からCA証明書を取得・管理することが必要となる。
  真正性の検証はICチップに不正にアクセスされ、データが改ざんされるなどした場合に検知する仕組みである。そのうえICチップ付本人確認書類は不正利用への耐性として、上記以外にも様々な機能を有している。

  下記にその一例をあげる。

  ・アクセス制御
  スキミングのような意図しないアクセスに対し入力行為を介在させることで防いでいる。制御方法は発行時に設定された暗証番号か券面記載情報の入力を要求することで実現さ

れ、本人確認書類を所持していれば利用できる情報（＝券面記載情報）へのアクセス制御は券面記載情報で、マイナンバーカードにおける2種類の証明書、運転免許証における本籍などの券面に記載されていない情報へのアクセスは暗証番号を利用して制御することが多い。運転免許証については券面記載情報（氏名、住居、生年月日）へのアクセスも暗証番号での制御となっているが、警察庁からは発行時に設定する暗証番号のうち券面記載情報へアクセスするための暗証番号は券面記載情報を元に設定するよう通達[23]が行われている。

・ICチップの複製防止
ICチップを複製するクローニング攻撃という手法に対応する。
ICチップ内に保持している秘密鍵で乱数に対して署名を行い、公開鍵で署名検証する。ICチップ内の秘密鍵が対タンパー性を有しており複製がされないという特徴と組み合わせることで、ICチップが複製された場合の検知が可能となる。

本人確認書類ごとにこれらの機能が実装されているかは統一されておらず実装状況は下表のようになっている。

表4-2. 本人確認書類のICチップ機能実装

	運転免許証	マイナンバーカード	在留カード	パスポート
犯収法施行規則“へ”への適用	○	○	○	×
真正性の検証	○	○	×	×
アクセス制御	暗証番号	暗証番号、券面表記情報	券面表記情報	券面表記情報
複製防止	×	○	×	○

もう一つの利点としてテキストデータや画像データは券面記載の物が利用できるため、カメラやスキャナで取得した時と比べて劣化・誤りがないことも挙げられる。注意するべき点としては、上述の通り、ICカードの読み取りはスキミング対策[24]としてデータアクセスを暗証番号（マイナンバーカード・運転免許証）や券面記載情報（マイナンバーカード・在留カード）で保護しており、読取の際に入力を求められる。特に運転免許証を利用し真正性の検証まで含めた本人確認を行う場合、利用者は発行時に設定した2種類の暗証番号（いずれも4桁のもの）の入力する必要があるため、いずれかを覚えていない場合は利用不可能となる。本方式が利用できない場合の回避策として他の本人確認手法との併用などを検討する必要がある。券面記載情報を利用する場合にも、10桁を超える券面記載情報を入力する必要があるためOCR機能を搭載するなどしてユーザ体感を向上させることが望ましい。

[23] https://www.npa.go.jp/pdc/notification/koutuu/menkyo/menkyo20150820.pdf
[24] かばんや財布の外からのスキミング防止であれば、券面にクレジットカードのCVVのように読み取り用の番号を書いておけば足りる。券面自体が相手に渡っている場合には、券面事項は相手に渡っているのでスキミング防止をする意義は無い。一方、券面表示事項ではない本籍に関しては、保護するメリットがある。したがって、券面表示事項表示用のPINは廃止して券面にCVVのようにして記載、券面非表示事項表示用のPINはそのまま残すようにすると、本当の意味でのeKYCができる人口が5年で成人人口の8割以上まで大幅に増えるので、日本のデジタル化ということを考えても望ましいと考えられる

本方式の実現にはICカードリーダが必要となることもあり、これまで大きく普及はしていなかったが、近年のスマートフォンがほとんどNFC機能付きであるため、スマートフォンアプリで実現可能な手法として今後普及が促進していくと考えられる。Android OSでの対応が中心だったが、2019年9月に公開されたiOS13でのNFC Type-B読み取り対応により、Android, iOSでNFC読取機能が実現可能となった。
ただし、ICカードの読み取りはW3Cで規定されていないため、純粋なWEBブラウザからは利用できない。そのため、本方式はアプリを利用して実行されるのが一般的になるだろう。
　ユーザ体感としてはアプリのインストールやPINの入力などの課題もあるが精度の高い情報が得られるため失敗による離脱は少ないことが期待される。

- 公的個人認証
犯収法施行規則6条1項1号ルなど様々な法令において、本人確認手法として認められている公的個人認証を利用した方式について説明する。公的個人認証については、2章2-2-3で触れられている通りとなる。国が推し進めているマイナンバーカードを利用した本人確認であり、様々な用途での適用が期待できる。仕組みとしては、マイナンバーカードの中に保存されている署名用電子証明書をICカードリーダ経由で利用して、特定の電子ファイルに電子署名及び送信を行い、総務省の認可を受けた事業者が署名検証を行うことで実現する。
本方式の利点はICカードリーダで読み込んだマイナンバーカードの署名用電子証明書を利用するためのパスワードを入力するだけでよく「犯収法施行規則6条1項1号ホ、ヘ」では必要であった顔写真の送付が必要ないことである。
欠点としては未だ普及率が2割程度のマイナンバーカードでしか利用できない手法であること、署名用電子証明書のパスワード（6～16桁）を利用者が覚えている必要があることだ。
事象者側にとっては署名用電子証明書の検証者になるためには総務省の認可を受ける必要があるため、手続きコストおよび認可準拠のためのコストも必要となる。
他の方式で必要な写真の送付がないため、ユーザ体験は紹介した方式の中で最も良く、受け取ったデータを事業者側で判別できない等の失敗率も最も低いといえる。
本方式の課題はマイナンバーカードの普及率が低いことだが、国がマイナンバーカードの普及を進めていることや、電子申請が普及していくにつれて、今後ユーザにとって活用しやすい方式となっていくことが期待される。

4-2. OpenID ConnectとKYC

前節ではオンラインにおける本人確認（KYC）において本人確認書類を利用するための技術について説明したが、各サービス事業者が各技術を実装していくのはコスト面を考えても現実的には難しい。

そこで本節ではKYC Providerとなる事業者が保持する本人確認済み属性情報をAPI経由で提供する技術について解説する。すでに精度の高い顧客情報を持っている事業者から提供して貰えば、そのようなプロセスを省略できる可能性があるためである。この方法は自分の顧客が、他事業者のサービスと契約していることを前提としているので、当該の事業者は全国民レベルでのシェアと高い精度の本人確認情報を保有していることが求められる。

日本においてそのような事業者は携帯電話事業者や銀行が想起される。一般的に、銀行や携帯電話事業者が有するレベルの本人確認性があれば、ほとんどのサービス提供者にとって十分な品質を有していると思われる。ただ、現状として法的に他事業者が取得した本人確認情報を用いて別のサービスの本人確認手法とすること（依拠）はほとんど許容されていない。そのため、現時点では依拠を前提としたKYCは適用範囲が、ごく一部の法的要件か民間利用に限られることになるが、本件についてはEUからの流れであるeIDAS規制が日本でも適用の議論が進み、民間におけるトラストプロバイダーの認可などによって依拠が緩和されていくことを期待したい。現時点では（2020年1月現在）、日本では2章で紹介したNTTドコモ・KDDIに加えて三菱UFJ銀行がすでにOpenID Connect・OAuthにより保護されたAPIを利用した本人確認を支援するサービスを展開している。

Open ID Connectを利用することでサービス提供者は非常に簡単に顧客情報を取得できるようになる。しかし現状のOpen ID Connectの仕様では、機能的な不足が否めない。例えば、UserInfoエンドポイントから住所を取得するケースにおいて、ただ住所が取れるだけでなく、取得日時やどのような証明情報から取得したのか？など付帯的な情報も欲しいケースが当然考えられる。将来的な依拠が緩和された後の世界感を考えると犯収法やeIDAS規制などにも対応できる必要がある。

そういった厳格な本人確認性にも対応できる仕様として第3章でも述べた通り、新しいOpenID ConnectのプロファイルであるOpenID Connect for Identity Assuranceの策定が進んでいる。OpenID Connect for Identity Assuranceは、マネーロンダリング防止法、電気通信法、テロ対策法、eIDAS などのような法律や規則を満たすことを目的に策定を進めている仕様で、OpenID FoundationのeKYC and Identity Assuarance Working Groupにて議論が行われる予定である（2020年1月現在）。現在の犯罪収益移転防止法では OpenID Connect for Identity Assuaranceに依拠することは出来ないが、他の法的要件や民間利用においての利用は十分利用可能なものになるだろう。

OpenID Connect for Identity Assuaranceを利用することで、主に以下のようなことが標準化される予定だ。

- 本人確認プロセスに関する情報とその取得方法
- 本人確認済み情報の利用目的の通知と同意取得方法
- UserInfo Response として必要な属性の指定と必須属性の指定

これらの内容によって、RPはユーザやOPに対して

- サービスが本人確認しなければならない属性の明示的な要求
- ユーザに属性情報の利用目的の説明と、同意の取得

を行うことができるようになり、OPからの情報取得については、
- 自身のサービスで必要な最小限の個人情報の取得（データ最小化原則の達成）
- どのようなレベルや本人確認書類に基づいて本人確認を行ったかの取得

が行えるようになる見込みだ。

詳細については、OpenIDファウンデーション・ジャパンの翻訳・教育ワーキンググループが日本語訳が公開[25]されているので、ぜひ御一読いただきたい。

[コラム 1] 本人確認書類に使われる文字について

邦人・外国人に関わらず人の氏名の表現方法は複数存在する。邦人氏名に含まれる旧字体・新字体、外国人名に含まれるアキュートやウムラウトなど、これらの表記の揺れが本人確認業務を妨げる要因となる場合がある。例えば外国人がカタカナ表記で氏名を登録した場合に、これを証明する本人確認書類が無いために本人確認手続きを行えないという問題があります。この様なトラブルを避けるため各種本人確認書類[26]の券面に記載される文字集合、およびICチップに記録される文字符号化方式の整理を行った。

住民票

- 広域交付される住民票は住基ネット統一文字が使用される
- この文字集合においてもすべての氏名は網羅されておらず、住基ネット残存外字というものが存在する
- この文字集合はUnicodeをベースにしているもののUnicodeと互換性がない
- この文字集合を符号化したデータは基本的に住基ネットの外部に出てこないはずだが、住民票や個人番号カードなどの本人確認書類に印字されるのでOCR読み取り時に注意が必要となる

個人番号カード

個人番号カードの券面には住民票と同様に住基ネット統一文字で印字される。ICチップの内には各種アプリケーション・プログラム(以下AP)に氏名と住所が記録されている。

- 券面確認AP: 住基ネット統一文字をPNG画像形式で記録
- 券面入力補助AP: 統合端末文字
- 公的個人認証AP 電子署名用証明書: 統合端末文字

この統合端末文字とは住基ネット統一文字をJISX0213:2004に縮退した文字集合であり、代替文字とも呼ばれる。

[25] https://openid-foundation-japan.github.io/openid-connect-4-identity-assurance-1_0.html
[26] 対象とした本人確認書類は住民票・運転免許証・パスポート・在留カード・個人番号カード

運転免許証

- ICチップ内の氏名・住所: JIS X 0208:1978 (旧JIS)
- これ以外の文字はビットマップ画像で格納

パスポート

- MRZ領域の氏名、ラテンアルファベットで記載される、ダイアクリティカルマーク[27]は使われない、長い氏名は省略される場合がある
- VIZ領域の氏名、ダイアクリティカルマークを利用できる

在留カード・特別永住者カード

- 券面氏名: 基本的にパスポートのMRZの氏名を転記する、漢字圏の外国人は漢字を併記できる
- この時の漢字はJIS 第1～4水準+JIS 補助漢字+法務省告示の176字
- パスポート非所持のレアケースでは漢字氏名のみが記載されることもある
- ICチップ氏名: 券面のTIFF画像
- ICチップ追記住所: JIS X0213:2004

[コラム 2] Decentralized Identifier(DID)とは

本コラムでは視点を変えて、別の技術課題について解説する。先ほどまでに紹介したOpen ID Connectを利用した属性情報の取得は、一言で言えばRP信頼型のモデルであると言える。このモデルはIdP/OP側がRPを審査し、信頼に値すると判断された事業者に対してのみ、ユーザの個人情報が提供されることになる。仮にRP側がIdP/OPから取得したユーザの個人情報を漏洩してしまった場合、IdP/OP側の評判も毀損するリスクが発生するため、RPはIdP/OPから様々なセキュリティ要件を求められることになるだろう。それは仕方がないことであると考えられるが、一方で普及阻害の要因になりえる。

実店舗ではどのような方法で顧客の本人確認を実施しているか、あらためて考えてみよう。例えば、レンタルビデオショップで会員登録を実施する場合、おおむね以下のフローで実行される。

1. 店員は顧客に利用規約が記載された申し込み用紙の記入を求め、免許証の提示を求める
2. 顧客はそれに同意した場合に利用規約への同意とともに、免許証を店に提示する
3. 店員は免許証の正しさを確認するとともに、免許証と本人の一致性を目視などで確認する
4. 確認が終了すると免許証を返却し、利用規約に基づき店側で運用を実施する

上記のプロセスで重要なのは店側が免許証を利用してビジネスをすることについて、Identityを提供する側に位置付けられる免許証の発行者である警察庁に対して、許諾を取得していない点にある。これは、言い換えればIdP/OPからの許諾なしに本人確認情報を扱っていると言える。リアル店

[27] áやäなど発音を区別すべき場合に文字に付される記号のこと

舗で実施されている「店側が特定の証明書が利用可能な本人確認書類名になることを認識でき、ユーザの同意に基づきその証明書の提示を受け、店側が正しくその証明書から本人確認性を検証できる仕組み」をオンラインで実施しようとした取り組みが、Decentralized Identity Foundation（DIF）[28]やSovrin Foundation[29]、World Wide Web Consorsium（W3C）[30]が標準化を進めているDecentralized Identifier（DID）および関連技術の規格である。DIDは、特定の分散台帳（例: ブロックチェーン）におけるリソース（DIDドキュメント）の識別子を示す。DIDドキュメントは識別される対象のエンティティ（DIDサブジェクト）について記述したものになる。その記述には、DIDサブジェクトが自身の認証時に使うための、公開鍵や仮名化された生体情報なども含まれる。また、DIDサブジェクトに関する属性やクレームなども記述内に加える事が可能だ。DIDドキュメントの例を見てみよう。

```
{
  "@context": ["https://www.w3.org/ns/did/v1", "https://w3id.org/security/v1"],
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }, {
    "id": "did:example:123456789abcdefghi#keys-2",
    "type": "Secp256k1VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyHex": "02b97c30de767f084ce3080168ee293053ba33b235d7116a3263d29f1450936b71"
  }],
}
```

*@contexts*はDIDドキュメントを利用するシステム同士が利用するプロトコルやスキーマを双方が解釈できることを確かにする。*@context*には複数のURIを設定できるが、その場合、順番にURIが参照・評価され、1つ目のURIはhttps://www.w3.org/ns/did/v1でなければならない。このパラメタはDIDドキュメントに必須だ。

*id*はDID Subjectと呼ばれる。DIDドキュメントが記述し、そしてDIDが識別するエンティティを指す。*did:example:123456789abcdefgh*はご覧のとおり、コロンにより分割されている。そのうち最初の*did*は、URLにおけるスキーム（例: "https://"）のようにSchemeと呼ばれる。一方*example*は特定分散台帳でどのように扱うかを定めるMethodになる。今回の例では*example*だが、Sovrin FoundationのDID Methodを使っている場合は*sov*を指定することになる。最後の文字列はMethod Specific IDであり、これについては説明は不要だろうが、ユニークな識別子だ。この3つのパラメタからDID Subjectが構成される。このパラメタもDIDドキュメントに必須だ。

最後に*publicKey*はその名の通り、電子署名や暗号化といった暗号学的オペレーションに利用するパラメタだ。

他にもいくつかパラメタがあるため、詳細はW3Cのドキュメント[31]などを見てほしい。こういったパラメタが組み合わさったDIDドキュメントが、分散台帳上に記録・公開される。

[28] https://identity.foundation/
[29] https://sovrin.org/
[30] https://www.w3.org/
[31] https://www.w3.org/TR/did-core

ここまでDIDドキュメントの概要を紹介したが、*publicKey*は実は必ず含まなければいけないものではない。しかし、レポートの趣旨である本人確認に深く関わるので、本カラムに記載させていただいた。どう関わるかを説明するため、一度、冒頭でにあげたレンタルビデオショップの例に戻ろう。本人確認に使われる免許証は警察庁が発行する事は前述の通りだ。本来、免許証はただ単に運転できる技能を証明する許可証（License Certificate）のような性質でしかない。なぜ、それが本人確認として利用できるのだろうか。

それは、1. 警察がすでに免許証に記載された情報を確認した事実をある程度、信頼できる 2. 耐タンパ性を免許証というカードがある程度、保証されている、という性質を免許証が保持しているからである。

こういった要件をDIDで実装できないか検討が進んでいる。仮に警察、ビデオショップ、利用者がDIDの住人だった場合、それぞれがDIDドキュメントを持つことになる。そして、発行者である警察が公開鍵を持つのであれば、当然、ペアになる秘密鍵も保持していることになる。秘密鍵を使えば、既存の仕組みと同様に、警察がデジタルに発行した免許証に署名を付与することができる。

イメージとして、次のようなデジタル免許証になるだろう。

```
{
  "@context": [
    "https://w3id.org/credentials/v1",
    "https://example.com/poice-vocab/v1"
  ],
  "id": "urn:uuid:xxxxxxxxxxxxxxxxx",
  "type": ["VerifiableCredential", "JapaneseDriverLicenseCredential"],
  "issuer": "did:example:police-id-in-example-ledger",
  "expires": "2025-01-20T00:00:00Z",
  "claim": {
    "id": "did:example:video-rental-user-id-in-example-ledger",
    "givenName": "Kengo",
    "familyName": "Suzuki",
   "address": "Somewhere in Tokyo",
    /* 警察により生成されたその他のクレーム */
  },
  "proof": {/* 警察の電子署名 */}
}
```

このようなデジタル免許証をビデオショップで登録処理に利用する場合、次のようなフローになるだろう。

1. ビデオショップ（で指定されたアプリ）がどのようなクレームを取得したいかを提示する
2. ユーザーが同意する
3. ビデオショップがクレームを取得する
4. 警察の電子署名を、issuerである警察のDIDドキュメント内の公開鍵で検証する

これにより、ビデオショップは警察が確かに発行したこと ＝ 身元確認情報が確かであるかを検証できる。つまり、リアル店舗で実施されている「店側が特定の証明書が利用可能な本人確認書類名になることを認識でき、ユーザの同意に基づきその証明書の提示を受け、店側が正しくその証明書から本人確認性を検証できる仕組み」が実現できた状態になる。

現在、こういった技術仕様はW3CのVerifiable Credentialというワーキンググループでも検討されている。今後、目が離せない内容になるだろう。

また、今回、物理的な免許証が実現している「耐タンパ性」については、別の仕組みが必要だ。DIDでは「Wallet」という仕組みでの解決が見込まれるが、レポートの趣旨からは外れる。もし、興味があればHyperledger Aries[32]やUrsa[33]などをご覧いただきたい。

[32] https://www.hyperledger.org/projects/aries
[33] https://www.hyperledger.org/projects/ursa

用語一覧

本書で用いた用語について解説する。

用語	意味/正式名称
KYC	顧客確認、Know Your Customerの略称。 本書ではお客様を知るための行為を総称してKYCと定義する。
本人確認	身元確認、Identity Proofingとも呼称する。 信頼できる機関が発行した本人確認書類を確認すること（真正性確認を含む）
eKYC	eKYCとはelectronic Know Your Customerの略。 本書では、電子的＝オンラインでお客様の本人確認をする行為を指す。 代表的な例としては、平成30年11月の犯収法の改正により、犯収法施行規則第6条第1項第1号に記載をされた本人特定事項の確認方法のうち、郵送不要の新手法にホ・ヘ・トの方法などがある。
本人確認書類	本人を確認するために公的機関から発行された証明書・書類の総称。 運転免許証、日本国パスポート、マイナンバーカード、住民票、健康保険証、在留カードなど
本人特定事項	本人確認書類の属性情報（氏名、生年月日、住所、有効期限、顔写真など）から本人と特定するための情報を指す。法律によって確認する情報が異なるケースがある。
本人確認手法	本人特定事項の確認方法のことを指します。例としては、犯収法施行規則第6条第1項第1号や、携帯電話不正利用防止法第3条第1項、電子署名法施行規則第5条などに記載されている確認方法などがあげられる。
当人確認	認証（Authentication）を指す
ID連携	認証連携と呼ばれることもある。SAMLやOpenID Connectにより実現されるRPとIdP/OPの間でのID情報の連携（フェデレーション）を指す
IdP	Identity Providerの略。アイデンティティ情報をRPへ提供する
OP	OpenID Provider。OpenID ConnectにおけるIdPの呼称
RP	Relying Party。一般的にIdP/OPからID情報を受け取るアプリケーションの事を指す
犯収法/犯罪収益移転防止法	・犯罪による収益の移転防止に関する法律[34] ・犯罪による収益の移転防止に関する法律施行令[35] ・犯罪による収益の移転防止に関する法律施行規則[36] 金融機関等の取引時確認、取引記録等の保存、疑わしい取引の届出の義務など、資金洗浄及びテロ資金供与対策のための規制を定める法

[34] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=419AC0000000022
[35] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=420CO0000000020
[36] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=420M60000f5a001

	律。犯罪収益移転防止法とも呼称する。
外為法	外国為替及び外国貿易法[37]
国外送金等調書法	内国税の適正な課税の確保を図るための国外送金等に係る調書の提出等に関する法律[38]
携帯電話不正利用防止法	・携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律[39] ・携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則[40] 振り込め詐欺など携帯電話を不正に利用した犯罪を防ぐための法律。
出会い系サイト規制法	インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律[41]
電子署名法	電子署名及び認証業務に関する法律（平成十二年法律第百二号）[42]
公的個人認証法	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律[43]
CDD	顧客管理、カスタマーデューデリジェンス（Customer Due Diligence)とも呼ぶ。 リスク低減処置として、個々の顧客に着目し、自らが特定・評価したリスクを前提として、個々の顧客の情報や当該顧客が行う取引の内容等を調査し、調査の結果をリスク評価の結果と照らして、講ずべき低減措置を判断・実施する一連の流れのこと

[37] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=324AC0000000228
[38] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=409AC0000000110
[39] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=417AC1000000031
[40] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=417M60000008167
[41] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=415AC0000000083
[42] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=412AC0000000102
[43] https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=414AC0000000153

執筆者一覧

OpenIDファウンデーション・ジャパン KYCワーキンググループ

ワーキンググループ・リーダー

OpenIDファウンデーション・ジャパン理事

富士榮　尚寛（伊藤忠テクノソリューションズ株式会社）

ポリシーパート主担当

株式会社TRUSTDOCK

菊池　梓

技術パート主担当

オープンソース・ソリューション・テクノロジ株式会社

濱野　司

執筆メンバ（所属50音順）

所属	氏名
株式会社FOLIO	鈴木　研吾
KDDI株式会社	白田　弘幸
KDDI株式会社	松井　利樹
株式会社NTTドコモ	栗山　盛行
株式会社オプティム	菊池　佑
セコム株式会社	佐藤　雅史
ソフトバンク株式会社	作田　宗臣
株式会社ディーカレット	池田　雄一郎
日本電気株式会社	宮川　晃一
株式会社レピダム	名古屋　謙彦

ワーキンググループメンバ（所属50音順）

所属	氏名
KDDI株式会社	小畑　雅人
NTTテクノクロス株式会社	久米田　博
NTTテクノクロス株式会社	松島　知也
エクスジェン・ネットワークス株式会社	李　伝民

エントラストジャパン株式会社	佐藤　公理
株式会社オージス総研	金井　敦
株式会社オージス総研	小林　融
オープンソース・ソリューション・テクノロジ株式会社	今井　啓
セコム株式会社	長谷川　佳祐
ソフトバンク株式会社	小松　隆行
ソフトバンク株式会社	東海　哲行
ヤフー株式会社	伊藤　雄哉
伊藤忠テクノソリューションズ株式会社	寺岡　卓也
伊藤忠テクノソリューションズ株式会社	岡本　俊一
一般財団法人日本情報経済社会推進協会	紅谷　昭光
日本マイクロソフト株式会社	安納　順一

OpenIDファウンデーション・ジャパン事務局
　事務局長
　　真武　信和
　副事務局長
　　曽我　紘子

各種法律に関する記載に関する査読
　宮内・水町IT法律事務所　弁護士　宮内　宏