eKYC 導入指針

一般社団法人キャッシュレス推進協議会

Ver.1.0

2021 年 12 月 28 日

【履歴】

2021 年 12 月 28 日　新規制定（Ver. 1.0）

目次

【用語集】 4
1. はじめに 6
1.1. 本指針策定の背景と目的 6
1.2. 本指針の位置付け 7
1.3. 本指針が想定する事業者 7
1.4. 本指針が対象とする顧客管理プロセスの局面 7
1.5. 本指針が対象とする取引時確認と eKYC 8
2. 取引開始時の顧客管理 9
3. 取引時の顧客確認 19
3.1. 犯収法上の確認済みの確認 20
3.2. AML/CFT ガイドライン上の継続的顧客管理の要請 21
3.3. 業態ごとの一般的な当人認証 22
3.4. 顧客情報の更新 22
4. まとめ 24

【用語集】

No.	用語	定義
1	顧客管理	マネー・ローンダリングおよびテロ資金供与対策に関するリスクベースアプローチにおいて、特に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をいう（AML/CFT ガイドライン（No.8）の Ⅱ-2(3)(i)参照）。CDD(No.10)ともいう。 FATF 勧告 10 では、顧客およびその実質的支配者を特定し、収集情報を検証すること、顧客の取引の目的その他の属性を理解すること、およびこれらを継続的に実施し取引が顧客属性と整合的かを確認することを指す。
2	当人認証	本人確認（No.4 参照）のうち、認証の 3 要素（生体、所持、知識）のいずれかの照合で、その人が作業していることを示すこと（同一性）。
3	取引時確認	犯罪による収益の移転防止に関する法律（以下、犯収法）に基づき、同法上の特定事業者が特定業務のうち特定取引（対象取引、特別に注意を要する取引）およびハイリスク取引を行う際に実施すべき確認措置のことをいう（犯収法第 4 条第 6 項）。顧客が自然人の場合には、本人特定事項、取引を行う目的、職業を確認する必要がある（犯収法第 4 条第 1 項各号）。
4	本人確認	本指針では、犯収法上の「本人特定事項の確認」と同義で使用する。 本人確認は「身元確認」と「当人認証」に分けて整理することができる。
5	本人特定事項	犯収法第 4 条第 1 項第 1 号で規定される事項。自然人にあっては、概ね氏名、住居及び生年月日をいう。
6	身元確認	本人確認（No.4 参照）のうち、登録する氏名・住所・生年月日等が正しいことを証明/確認すること（実在性）。
7	AML/CFT	Anti-Money Laundering / Countering the Financing of Terrorism。資金洗浄およびテロ資金供与対策
8	AML/CFT ガイドライン	金融庁が公表する「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」（2018 年 2 月 6 日公表。その後の改正を含む）および経産省が公表する「クレジットカード業におけるマネー・ローンダリング及びテロ資金供与対策に関するガイドライン」（2019 年 8 月 30 日制定。その後の改正を含む）のことをいう。両ガイドラインは、ほぼ同内容である。
9	BPO	Business Process Outsourcing。eKYC 関連ビジネスにおいては、サービスプロバイダが eKYC 技術要素を組み込んだ自動判定ソリューションを提供することの他、事業者が行うべき目視確認等のオペレーションを BPO サービスとして提供することが多い。
10	CDD	Customer Due Diligence。顧客管理（No.1）と同義。
11	eKYC	2018 年 11 月末の改正によって認められた犯収法施行規則で規定される「オンラインで完結する自然人の本人特定事項の確認方法」で用いられる身分証の撮影、IC チップ読取、あるいはこれらに関連する OCR 等の技術要素を利用する方法で実施する自然人の本人特定事項の確認のこと（同規則 6 条 1 項 1 号ホ、ヘ、ト、チ（一部対象外））を指す。本指針では、これに加えて、電子署名検証を利用する方法で実施する自然人の本人特定事項の確認（同規則 6 条 1 項 1 号ヲ、ワ、カ）も含めるものとする。また、これらの確認方法を構成する技術要素そのものを指すことがある。

No.	用語	定義
12	J-LIS	地方公共団体情報システム機構。マイナンバーカード等の発行・管理や公的個人認証サービスを提供する地方共同法人。
13	KYC	Know Your Customer。犯収法上の特定事業者にとっては同法に定める「取引時確認」がこれに当たる。FATF 勧告では、顧客管理（No.1）、CDD(No.10)と同義で用いられる場合がある。

1. はじめに

1.1. 本指針策定の背景と目的

社会のデジタル化が進展し、コロナ禍もあいまって金融取引における非対面チャネルの利用も拡大している。このような環境下で、健全な金融システムを維持するための重要な要素である本人確認の方法についても従来の対面や郵送による確認からオンラインでの確認への変化が社会的にも要請されている。オンラインで完結する本人確認、いわゆる eKYC が犯収法上認められ、当該要件を充足するソリューションが登場したこと、マイナンバーカードの普及率が増加していること、さらには不正防止の観点から当協議会をはじめとするキャッシュレス関連団体が定めるガイドライン[1]等において取引時確認等が求められていること等から、犯収法上の特定事業者等が eKYC を導入する動きが活発となっている。

一方で、キャッシュレス推進協議会（以下、協議会）が会員に対して実施した eKYC に関するアンケート（2020 年 9 月実施）では、犯収法上の特定事業者の回答数 21 社中、導入済みが 4 社、導入予定が 6 社にとどまっており、半数以上の 11 社が未導入との結果となった。

事業者	合計	導入済み	導入予定	未導入
クレジットカード	13	1	3	9
資金移動業	4	3	1	0
銀行	4	0	2	2
合計	21	4	6	11

このような結果となる背景には、eKYC が顧客に与える環境、事業者にもたらすメリット、提供しうる手法等の選択肢、また、eKYC 導入に伴って留意すべき事項や eKYC ソリューションプロバイダ（以下、プロバイダ）各社の違いについて十分な情報が得られていないこと、そして eKYC そのものに対する理解が浸透していないこと等も理由として考えられる。

そのため、以下を目的として本指針を策定する。

1. 従来の方法と eKYC による方法との相違点を整理し、顧客管理プロセス全体において eKYC が担う役割や導入意義を明確にする

[1] たとえば、「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」（一般社団法人キャッシュレス推進協議会）等

2. 事業者が犯収法上規定されている本人確認の方法、プロバイダ、eKYC ソリューションが提供する各種機能を選択する等、eKYC 検討における合理的な意思決定を行うための留意点を整理する
3. eKYC 導入の意思決定や顧客管理プロセスの運用が AML/CFT 対策として事業者に内在するリスクに応じて適切かどうかを確認する際の留意点を整理する

本指針は、これから eKYC 導入を検討する事業者だけではなく、検討中、あるいは導入済みの事業者、さらには導入しないことを決定した事業者にとっても、それぞれの意思決定の妥当性や、顧客管理プロセス運用における有効性の整理、確認に役立つものとなることを企図している。

1.2. 本指針の位置付け

本指針は、上記の目的に資する参考情報として位置付けるものであり、特定事業者に対する遵守を義務付けるものではない。

1.3. 本指針が想定する事業者

本指針は、犯収法上の特定事業者の立場にあるクレジットカード事業者、資金移動業者、銀行を想定して策定するが、他の特定事業者や特定事業者以外の顧客管理を行う事業者、あるいはこれらの事業者に対するソリューション提供事業者等においても、参考になるものと思料する。

1.4. 本指針が対象とする顧客管理プロセスの局面

本指針は、事業者が行う顧客管理プロセスのうち、以下の 2 つの局面を対象とする[2]。

1. 取引開始時の顧客管理：新規顧客受入れ局面であり、口座開設における犯収法上の取引時確認がこれに該当する
2. 既存顧客の顧客管理：取引関係を確立した後に、顧客が個々に取引を実施する局面（犯収法上のいわゆる「確認済みの確認[3]」、AML/CFT ガイドラインで求められるリスクベースアプローチでの継続的な顧客管理、および犯収法上の「取引時確認をした事項に係る情報を最新の内容に保つための措置」がこれに含まれる）

本指針においては、いずれも「自然人」すなわち、個人に対し「非対面」で実施される顧客管理プロセスを対象とする。

---

[2] 対象局面は、犯収法状の取引時確認として求められるものに限らず、たとえば特定取引以外の取引時にも行われる当人認証等、実務上利用されているものも含む。

[3] 「3. 取引時の顧客管理」参照。

1.5. 本指針が対象とする取引時確認と eKYC

犯収法上の本人確認の方法は eKYC も含めて同法施行規則第 6 条 1 項 1 号に列挙されており、それぞれの本指針での取扱いは以下の通りとなる。

条文	概要	本指針対象	本指針での取扱い
イ～ニ	本人確認書類の提示（＋本人確認書類もしくは補完書類の郵送受領または取引関係文書の書留・転送不要郵便送付）	対象外	対面要素を含むため、検討対象外とする
ホ	本人確認書類の画像＋容貌の画像	対象	eKYC として取扱う
ヘ	IC チップ情報＋容貌の画像	対象	eKYC として取扱う
ト	本人確認書類の画像又は IC チップ情報+銀行等への顧客情報の照会	対象	eKYC としてト(1)のみ取扱う（ト(2)預金口座少額振込確認は検討対象外とする）
チ	本人確認書類の画像又は IC チップ情報+転送不要郵便	対象	eKYC として左記のみ取り扱う（以下、単に「チ」の方法という場合には、左記の方法を指す） （また、チのうち本人確認書類の原本の送付は、「チ（原本）」の方法と表記し、「従来の方法」として言及する）
リ	本人確認資料送付＋転送不要郵便	対象	eKYC には該当しない「従来の方法」として言及する
ル	本人限定受取郵便	対象	同上
ヲ	電子署名法上の認定者による認証	対象外	eKYC だが導入事例がないため、検討対象外とする
ワ	公的個人認証	対象	eKYC として取扱う
カ	公的個人認証法上の署名検証者による特定認証	対象外	eKYC だが導入事例がないため、検討対象外とする

まず、eKYC を用いる方法として「ホ」「ヘ」「ト」「チ」「ワ」を取扱う。さらに、eKYC を用いない「従来の方法」として「リ」、「ル」、さらに犯収法施行規則第 13 条第 1 項[4]を取り扱う。

[4] 取引時確認が必要となる場面での確認方法として、犯収法施行規則第 6 条 1 項 1 号以外に、同法施行令第 13 条第 1 項第 1 号、施行規則第 13 条第 1 項が別途定められている。前者（施行令第 13 条第 1 項第 1 号）は、預金に関する契約の締結等、金融サービスの提供そのものを外部委託する場合に取引時確認を不要とする方法であり、本指針のスコープとは異なる。一方、後者（施行規則第 13 条第 1 項）は、取引時確認の確認方法を規定するものであり、対面や郵送が不要な方法であるため、本指針でも取り扱う。後者（施行規則第 13 条第 1 項）の内容は、資金移動業者、クレジットカード会社、保険会社等の一定の特定事業者が顧客と契約を締結し、当該契約に基づく取引の際に、預金口座振替やクレジットカードで決済する場合は、この特定事業者は、当該預金口座あるいはクレジットカードを

2. 取引開始時の顧客管理

「従来の方法」として「チ（原本)」、「リ」、「ル」さらに、犯収法施行規則第 13 条第 1 項の取引時確認プロセスを整理すると以下の通りとなる。

取引時開始時の「従来の」取引時確認プロセス

#	プロセス	（6 条 1 項 1 号チ（原本）・リ） 本人確認資料＋転送不要郵便	（6 条 1 項 1 号ル） 本人限定受取郵便	（13 条 1 項） 他事業者の取引時確認依拠
0	申込画面の提供	・下記申込のための画面を提供、店舗等での申込書面を用意等		
1	申込書類の入手	・事業者のウェブ上の申込 URL にアクセスする。（もしくは、店頭等で申込書を入手する、もしくは、ウェブを通して資料請求を行い、申込書の郵送を受ける。）		
2	申込書類の提出	・申込画面に必要情報を入力する。（もしくは、申込書類を手書き等で記入し、特定事業者の従業員に提示する、もしくは所定の宛先に郵送する。）		
3	本人確認書類の提出	・指定された組合せの本人確認書類のコピーや原本を添付し、所定の宛先に郵送する。	・本人限定受取郵便受取時に本人が郵便局員等に対して写真付き本人確認書類を提示する。	・本契約で利用する振替口座、クレジットカードに関する情報を提示する。
4	申込情報の収集と登録	・上記申込画面で顧客が入力した情報が顧客 DB に連携される（もしくは郵送で届いた申込書類の情報を顧客 DB へ手入力する）。受領した書類については紙ベースもしくはスキャンして保存することが多い（送付を受けた本人確認書類（の写し）はスキャン等による保存が必須）。		
5	本人確認書類、同一性および申込内容の検証	・収集した本人確認書類のコピーや原本を確認し、真正性を目視確認する。 ・申込書類記載が示す人物と申込人が同一であるかを、申込書記載内容と本人確認書類との整合性（氏名、住所、生年月日など）等によって目視確認する。	・#12 の郵便局員等からの結果伝達を確認する。	・振替口座、クレジットカード提供事業者が、取引時確認済であり、当該確認記録を保存している者であることを確認する（当人認証）。 ・事業者が上記他事業者による確認完了を確認する[5]。
6	上記以外の情報確認	取引の目的、職業その他の申込情報を確認する。		

提供している他の特定事業者が当該預金口座、クレジットカードに関する「取引時確認を行い」、かつ、その「確認記録を保存していること」を確認する方法によって、取引時確認を行うことを認めるものである（当該特定事業者と他の特定事業者が、この方法を用いることについて事前に合意をしていることが条件となる。)。多くのクレジットカード事業者はこの方法を用いているため、クレジットカード契約において eKYC が積極的に導入されない理由とされている。一方で eKYC 導入に踏み切る理由としては、顧客が取引時確認に応じるための選択肢をなるべく多く提供して、離脱率を抑え、口座開設手続を確実かつスムーズに行えるようにするといったことが挙げられる。また、一般社団法人日本資金決済業協会「銀行口座との連携における不正防止に関するガイドライン（資金移動業)」（令和 2 年 12 月 3 日）では、「資金移動業アカウント作成時における犯罪収益移転防止法上の取引時確認を同法施行規則 13 条第 1 項第 1 号に規定する方法により実施する場合には、実効的な取引時確認済みの確認、資金移動業者における継続的顧客管理の充実等の観点から、提携銀行の情報と照合することなどの方法により、資金移動業の利用者から申告を受けた本人特定事項(氏名・住所・生年月日)が正確か確認する必要がある。」としている。

5 資金移動業アカウント作成時の取引時確認の場合には、資金移動業者における継続的顧客管理の充実等の観点から、提携銀行の情報と照合することなどの方法により、資金移動業の利用者から申告を受けた本人特定事項(氏名・住所・生年月日)が正確か確認することが求められている点、前注のとおりである。

#	プロセス	（6 条 1 項 1 号チ（原本）・リ） 本人確認資料＋転送不要郵便	（6 条 1 項 1 号ル） 本人限定受取郵便	（13 条 1 項） 他事業者の取引時確認依拠
7	スクリーニング	顧客受入方針に基づき、謝絶先あるいはハイリスク顧客を、システム、紙ベースでのスクリーニングあるいは自己申告に基づき特定する。システムによるスクリーニングの場合は、ヒットの判定処理を確認する。		
8	顧客リスク評価	上記検証、スクリーニング、顧客属性その他の情報に基づき、顧客リスク評価を行う。		
9	追加調査（EDD）	上記顧客リスク評価の結果、追加調査が必要と判断した場合、追加情報や資料提示を顧客に求める。		
10	承認	口座開設の可否を判断する。リスクに応じた判断（取引承認、一部取引の制限、謝絶等の対応や、疑わしい取引検知や該当した場合の届出等を含む）		
11	登録	・上記の一連の情報を登録する。	・上記の一連の情報を登録する。	・上記の一連の情報を登録する。
12	顧客が取引実施に必要なものの送付	・書留・転送不要郵便でクレジットカード、銀行カード等を送付する。	・本人限定受取郵便でクレジットカード、銀行カード等を送付する。 ・郵便局員等が本人限定受取郵便配達時に、本人確認書類の真正性および本人との同一性を目視確認し、結果を事業者に伝達する。	・クレジットカード、銀行カード等を送付する。

（凡例）黒字：顧客、青字：特定事業者、オレンジ：銀行その他

これに対して、eKYC による取引時確認プロセスである「ホ」「ヘ」「ト」「チ」「ワ」毎の整理結果は次ページのとおりである。「従来の方法」との比較を容易にするために、従来の方法のうち、6 条 1 項 1 号リを代表的な例として示した。

取引時開始時の eKYC 取引時確認プロセス

#	プロセス	eKYC を用いない方法	eKYC を用いる場合 1				
		（6 条 1 項 1 号リ） 本人確認資料＋転送不要郵便	（6 条 1 項 1 号ホ） 本人確認書類の画像＋容貌の画像	（6 条 1 項 1 号ヘ） IC チップ情報＋容貌の画像	（6 条 1 項 1 号ト） 本人確認書類の画像又は IC チップ情報+銀行等への顧客情報の照会	（6 条 1 項 1 号チ） 本人確認書類の画像又は IC チップ情報+転送不要郵便	（6 条 1 項 1 号ワ） 公的個人認証サービスの署名用電子証明書
0	申込画面の提供	・下記申込のための画面を提供	・プロバイダが画面を提供	・プロバイダが画面を提供	・プロバイダが画面を提供	・プロバイダが画面を提供	・プロバイダが画面を提供
1	申込書類の入手	・事業者のウェブ上の申込 URL にアクセスする。（もしくは、店頭等で申込書を入手する、もしくは、ウェブを通して資料請求を行い、申込書の郵送を受ける。）	・申込 URL にアクセスする。	・申込 URL にアクセスする。	・申込 URL にアクセスする。	・申込 URL にアクセスする。	・申込 URL にアクセスする。
2	申込書類の提出	・申込画面に必要情報を入力する。（もしくは、申込書類を手書き等で記入し、所定の宛先に郵送する。）	・申込画面に必要情報を入力する。	・申込画面に必要情報を入力する。（下記 3 により一部の情報入力を省略することも可能）2	・申込画面に必要情報を入力する。（下記 3 により一部の情報入力を省略することも可能）2	・申込画面に必要情報を入力する。（下記 3 により一部の情報入力を省略することも可能）2	・申込画面に必要情報を入力する。（下記 3 により一部の情報入力を省略することも可能）2
3	本人確認書類の提出	・指定された組合せの本人確認書類のコピーを添付し、所定の宛先に郵送する。	・本人確認書類を撮影する。 ・自分の顔を撮影する。	・本人確認書類の IC チップをスマホ等で読み込ませる。 ・自分の顔を撮影する。	・ホと同 ・へと同 ・すでに口座を有する銀行のサイトにログインし、本人確認情報提示を了承する。	・ホと同 ・へと同	・本人確認書類上の IC チップをスマホ等で読み込ませる。
4	申込情報の収集と登録 3	・上記申込画面で顧客が入力した情報が顧客 DB に連携される（もしくは郵送で届いた申込書類の情報を顧客 DB へ手入力する）。書類については紙ベースもしくはスキャンして保存する。	・上記申込画面で顧客から収集した情報および下記 5 で検証した結果が事業者のサーバに連携される。	・上記申込画面で顧客から収集した情報および下記 5 で検証した結果が事業者のサーバに連携される。	・上記申込画面で顧客から収集した情報および下記 5 で検証した結果が事業者のサーバに連携される。	・上記申込画面で顧客から収集した情報および下記 5 で検証した結果が事業者のサーバに連携される。	・上記申込画面で顧客から収集した情報および下記 5 で検証した結果が事業者のサーバに連携される。
5	本人確認書類、本人性および申込内容の検証	・収集した本人確認書類のコピーを確認し、真正性を目視確認する。 ・申込書類記載が示す人物と申込人が同一であるかを、申込書記載内容と本人確認書類との整合性（氏名、住所、生年月日など）等によって目視確認する。	・本人確認書類撮影 4 ・容貌撮影 5 による判定結果を提示。 ・上記確認を目視確認し判定する。（当該部分（の一部）を BPO として受託するケースあり）6	・IC チップ読取 2 ・容貌撮影 5 による判定結果を提示。 ・上記確認を目視確認し判定する。（当該部分（の一部）を BPO として受託するケースあり）6	・本人確認書類撮影 4 または IC チップ読取 2 による判定結果を提示。 ・銀行は、顧客の了承を受けて、当該顧客が本人確認済であることを確認し、氏名、住居及び生年月日をプロバイダに提供。7 ・確認結果を提示 ・上記プロバイダの確認結果を検証する。（当該部分（の一部）を BPO として受託するケースあり）6	・本人確認書類撮影 4 または IC チップ読取 2 による判定結果を提示。 ・上記プロバイダの確認結果を検証する。（当該部分（の一部）を BPO として受託するケースあり）6	・IC チップを読取り、J-LIS に電子証明書の確認を依頼。2 ・J-LIS は紹介を受けた電子証明書の確認結果をプロバイダに回答。7 ・確認結果を提示。 ・上記プロバイダの確認結果を検証する。6
6	上記以外の情報確認 8	・取引の目的、職業その他の申込情報を確認する。					
7	スクリーニング 8	・顧客受入方針に基づき、謝絶先あるいはハイリスク顧客を、システム、紙ベースでのスクリーニングあるいは自己申告に基づき特定する。システムによるスクリーニングの場合は、ヒットの判定処理を確認する。					
8	顧客リスク評価 8	・上記検証、スクリーニング、顧客属性その他の情報に基づき、顧客リスク評価を行う。					
9	追加調査（EDD）8	・上記顧客リスク評価の結果、追加調査が必要と判断した場合、追加情報や資料提示を顧客に求める。					
10	承認 8	・口座開設の可否を判断する。リスクに応じた判断（取引承認、一部取引の制限、謝絶等の対応や、疑わしい取引検知や該当した場合の届出等を含む）					
11	登録 3	・上記の一連の情報を登録する。	・上記の一連の情報を登録する。（プロバイダへの委託範囲によってはプロバイダより連携を受けられる情報あり）	・上記の一連の情報を登録する。（プロバイダへの委託範囲によってはプロバイダより連携を受けられる情報あり）	・上記の一連の情報を登録する。（プロバイダへの委託範囲によってはプロバイダより連携を受けられる情報あり）	・上記の一連の情報を登録する。（プロバイダへの委託範囲によってはプロバイダより連携を受けられる情報あり）	・上記の一連の情報を登録する。（プロバイダへの委託範囲によってはプロバイダより連携を受けられる情報あり）
12	顧客が取引実施に必要なものの送付	・書留・転送不要郵便でクレジットカード、銀行カード等を送付する。	・ビジネス上、必要な場合には、顧客あて、クレジットカード、銀行カード等を送付する。9	・ビジネス上、必要な場合には、顧客あて、クレジットカード、銀行カード等を送付する。9	・ビジネス上、必要な場合には、顧客あて、クレジットカード、銀行カード等を送付する。9	・書留・転送不要郵便で顧客あて、クレジットカード、銀行カード等を送付する。9	・ビジネス上、必要な場合には、顧客あて、クレジットカード、銀行カード等を送付する。9
13	非機能要件	—	・非機能要件の整備・運用 10				

（凡例）黒字：顧客、青字：特定事業者、緑字：eKYC サービスプロバイダ、オレンジ：銀行その他、解説ポイント

解説ポイント１：eKYC の方法

・ eKYC を導入するか否かの検証、また導入する場合であっても eKYC（ホ、ヘ、ト、チ、ワ）のいずれの方法を採用するかについては、まず、顧客ニーズに沿った方法に限定して採用するのか、顧客に選択肢を多く与える趣旨からなるべく多くの方法を利用可能とするのか等の基本方針をはじめ、以下の観点からの検討が必要である。

① 基本方針の明確化[6]
② それぞれの方法ごとに利用可能な本人確認書類の種類
③ それぞれの方法によって顧客に求められる動作（入力、撮影、ふるまい）[7]
④ それぞれの方法で想定し得る、なりすまし・偽造リスクに対する評価とそれに対するコントロールの強度と事業者（あるいはプロバイダ）が行うべき対応負荷の評価
⑤ それぞれの方法にかかるコスト[8]
⑥ それぞれの方法における開発・導入の提供方法[9]
⑦ 事業者が顧客に提供する商品・サービス・チャネル[10]

---

6 単に eKYC の導入を目的とせず、本来は事業者のビジネス（顧客に対する商品・サービス提供における DX の在り方）、金融犯罪対策、顧客体験(CX)、コスト等の複数の観点で、いずれに軸足を置いて eKYC を位置付けるのかによって採用すべき方法、プロバイダ、その他の選択肢の見極めがなされるべきである。

7 それぞれの方法によって求められる動作が異なる（たとえば容貌撮影の有無等。表中のプロセス「3 本人確認書類の提出」の行を参照。）といった観点に加えて、規制要件を実現するために各プロバイダがどのような動作を顧客に求めるのかといったプロバイダ毎の創意工夫（解説ポイント：４，５参照）の考察も必要である。

8 コストは、現行の方法での郵送その他紙ベースでの処理（記録の保存は大きなファクターとなる。（解説ポイント：３参照））を前提とした運用コスト、金融犯罪に晒されるリスクに伴うコスト（レピュテーション等の見えないコストも含まれる）と導入による追加コスト（もしくはコストの削減効果）との関係を明確にしたうえでの見極めが重要である。プロバイダによって、個々の方法ごとに個別に初期費用が発生する場合、採用する方法の組合せによって様々な費用パターンとなる場合、どの方法を選択しても（一つのみ選択する場合でも）同額となる場合等の違いがある。運用費用については、同一プロバイダであっても、方法によって一件当たり単価が異なる。

9 犯収法のそれぞれの方法について対応可能なものがプロバイダによって異なる点は検討の重要なポイントである。各プロバイダとも、方法に応じて Web 版、SDK 版、個別開発それぞれのソリューション開発・導入方法を用意しており、事業者の顧客に対するサービス形態等に応じて選択する必要がある。プロバイダによって犯収法施行規則が定める方法毎に提供方法が異なる点、あるいは犯収法施行規則が定める方法によってはそもそも Web 版では実現できない（IC チップ読取の場合）ものがある点等、留意が必要である。また Web 版については、（事業者のドメインとは異なる）プロバイダへの URL 遷移が顧客の不安を招き得るとの配慮から、事業者ドメイン内で完結するような工夫もプロバイダによって認められる。

10 eKYC のそれぞれの方法（ホ、ヘ、ト、チ、ワ）の選択は、事業者が提供する商品・サービス、チャネルにも大きく依存する。

解説ポイント２：IC チップ読取

- 「へ」、「ト」、「チ」、「ワ」は、IC チップ読取で対応する eKYC である[11]。IC チップ読取による方法は、顧客が申込情報を入力する前に IC チップ読取りのプロセスを先行させ、読取済み情報を自動入力とすることによって、顧客の入力負担・入力ミス、事業者の確認負荷の軽減が期待される（本人確認書類を確認する方法についても、OCR 読取によって顧客の入力負担を減らすことは可能であるが、顧客が撮影またはコピーした書類の OCR 読取の安定的運用にはいまだ課題が残る。）。対応可能な本人確認資料および IC チップ読取のために必要な手順はそれぞれの方法により以下のとおり異なる。
- まず、「へ」、「ト」、「チ」については、運転免許証、在留カード、マイナンバーカードが対応可能である。このうち、運転免許証の場合は、IC チップ読取にあたって、４桁×2 の暗証番号入力が必要であり、当該暗証番号を失念している場合、この方式を利用できない[12]。在留カード、マイナンバーカードの場合は券面記載の番号入力で足りるため、失念によって利用できないという局面は想定されない。「ワ」については、対象本人確認資料はマイナンバーカードのみであり、6～16 桁の暗証番号入力が求められ、これについても顧客において暗証番号を失念している可能性が否定できない。
- IC チップ読取は、券面記載情報のカメラ等による読取と比較すると、偽造、なりすましリスクに対して相対的に堅確性が高いほか、既述の通り CX 向上[13]や事業者負荷軽減にも資する。他方で、離脱リスク等とのかねあいで採用の可否を検討する必要がある。

解説ポイント３：記録の保存

- 申込情報を保存するプロセスは、顧客より申込情報を受領するプロセス、これをもとに本人確認書類、申込情報等から本人性を検証するプロセスと並び、事業者の負担が大きい領域である。従来、紙ベースで収集していた本人確認資料の保存は、eKYC の導入により、電子的な保存を可能とする点で負担が軽減されることが期待される。これに加えて、プロバイダによっては、本人確認資料の機微情報などのマスキングを BPO の一環として提供するところもある。さらには保存プロセスを委託することも選択肢となり得る。（この場合の委託先は、プロバイダと同一である必要はない。）

---

[11] 「ト」、「チ」は本人確認書類の画像による対応も可能であるが、ここでは IC チップ読取で対応することも可能である。

[12] また、金融分野における個人情報保護法に関するガイドラインの適用がある場合には、運転免許証の IC チップに含まれている本籍地情報について同ガイドライン上の機微情報としての取扱いが必要であり、削除することが望ましい。

[13] 顧客負担に関しては、上述のとおり顧客の申込情報入力の省略ができる可能性があり、また容貌撮影についても、への方法は容貌撮影が必要であるものの、ト、チ、ワの場合は不要である。

・　eKYC を導入する場合においても、事業者として明確な記録の保存の方針を定めておく必要がある。事業者として保存する場合（あるいは保存する情報）、プロバイダ側に保存を委託する場合（あるいは委託する情報）、それぞれのオペレーションの特性・リスク、セキュリティ基準や、保存に関連するコストを見極めたうえで方針を策定すべきである。特に、保存プロセスを外部委託する場合は、個人情報保護法等の法令や委託先である事業者の個人情報保護方針に照らして、委託先において適切な管理が行われること、顧客への説明責任[14]が確保されることを事業者として確認する必要がある。自社保存の場合は、プロバイダ側で一時的にせよ保存される情報の削除タイミング等を、委託するサービス範囲も踏まえて明確に合意事項として定めておくべきである。

解説ポイント４：本人確認書類の撮影

・　顧客から提示のあった本人確認資料は、本人確認書類撮影によってその真贋を確認することになる（ホおよびト、チにおいて該当する場合）。撮影枠をランダムに指定しその枠に書類が収まった場合のみ自動撮影する（撮影済みの画像の流用等を防ぐ）、他人の証明書裏面使用の手口を防ぐために動画で自動撮影する、OCR により券面上の文字を認識し申込内容等との整合性確認やフォーマットチェック、ディジットチェックを実施する等、本人確認書類の真贋性判定にはプロバイダの創意工夫が見られる。OCR の精度（読取率）もその後の目視確認の負担に影響を与えるため、プロバイダ比較の重要な要素となる。さらに、プロバイダからどのような品質の情報（撮影結果）の提示を受けるのか[15]も事業者の目視確認負担に大きな影響を与える。プロバイダ毎のサービス

---

[14] 個人情報保護法第 20 条（令和 3 年改正個人情報保護法における第 23 条）で安全管理措置を講じることが義務付けられているほか、令和 3 年改正個人情報保護法第 32 条および同法施行令第 10 条に以下のように規定されている。

法第三十二条　個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

（中略）

四　前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

施行令第十条　法第三十二条第一項第四号の政令で定めるものは、次に掲げるものとする。

一　法第二十三条の規定により保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）

（以下略）

[15] たとえば、撮影枠を設定しその中に本人確認書類が収まるように撮影を行わせる場合、枠に収まっているかどうかに関わらず撮影結果のみを受領する形（枠に入って適切に撮影されたかどうかについては事業者の目視確認に委ねる）とするか、そもそも撮影時に枠に入っているか等のある程度の品質確認を自動的に行い一定の基準を満たした場合にしか撮影されない形とするのかによって、事業者側の目視確認負担に影響を与え得る。

レベルを標準サービス、オプションサービス毎に見極めることが重要である（解説ポイント 6 参照）。

解説ポイント 5 ：容貌撮影

・ 顧客の容貌撮影をもって、当該容貌が本人確認書類上の写真と一致しているか、撮影された容貌が申込者本人のものかを確認する必要がある。なりすまし等を防ぐ目的でいわゆるライブネス確認が実装されているが、まばたき、首振り、表情筋、文字読み上げ、光反射、手振れ検知等の手法には各社創意工夫が見られる。なお、eKYC の方法（ホ、ヘ）やソリューションの提供方法（Web 版、SDK 版）によってライブネス確認の方法も異なる点に留意が必要である。

・ また、各社とも撮影画像と本人確認資料上の写真との照合精度についてもプロバイダ各社の有する技術の特徴があり、照合率[16]等から比較・検討する必要がある。解説ポイント 4 と同様、ここでも、プロバイダから撮影結果の提示を受ける前提として、どの程度の品質確認が事前になされているのか[17]によって事業者の目視確認の負担は異なり得る。

解説ポイント 6 ：本人確認書類や容貌撮影に基づく判定

・ 解説ポイント 5 の本人確認書類の撮影、解説ポイント 6 の容貌撮影、もしくは解説ポイント 2 の IC チップ読取を踏まえ、プロバイダからは判定結果が事業者に提供される。判定結果の提供は、①本人確認書類の撮影結果、OCR 読取結果、申込情報、容貌の撮影結果および顔照合判定（スコア等によって表示）等の個別の情報が連携され、これらの情報に基づき判定を行うための管理画面等を事業者側で整備し、目視確認を行うケースと、②プロバイダ側で事業者において目視確認を実施するための管理画面も提供するケース、さらには③事業者が実施すべき目視確認プロセスも BPO として対応するケースがある。

・ ①に関しては、プロバイダが関連情報を提示する前提として、解説ポイント 5 及び解説ポイント 6 で記載した通り、どれだけ事前の品質確認が確保されていたかによって、提示された後の、事業者側で行うべき目視確認の負担が変わり得ることに留意が必要である。

・ ②に関しては、管理画面の提供が基本サービスなのか、オプションサービスなのかは、プロバイダによって、あるいは eKYC の方法によって異なり得る。また事業者が行うべき目視確認の度合いは、たとえば判定結果（照合判定スコア）等に応じて決定するこ

16 本来は同一人物なのに別人物と判定してしまう（フォルスネガティブ）比率、本来は別人物なのに同一と判定してしまう（フォルスポジティブ）比率ともに少ないことが求められる。

17 たとえば帽子等の遮蔽物着用判定、手振れ判定、大きさ判定等によって一定の撮影品質を確保しているか等、ここでもプロバイダによって創意工夫が見られる。

とが求められるが、このような要件定義に資する情報や知見をプロバイダが適切に提供できるかといった点も考慮に入れる必要がある。

- ③に関しては、BPO サービスをプロバイダ自らが提供する場合とプロバイダのパートナー企業が提供する場合の 2 つが想定される。また、BPO サービスにおいて行われる目視確認の基準については、委託先プロバイダ（ないしはパートナー）が一律に提示する基準となる場合と事業者毎に基準を柔軟に設定できる場合に分かれる。さらに後者については決めるべき観点をあらかじめ基準として定め、柔軟かつ容易に設定できるようにしている例も見られる。BPO のサービスレベルについては、判定結果の責任分担を明確にするほか、たとえば 24 時間 365 日対応か、判定方法毎にどの程度の処理時間が見込まれるか等についてもプロバイダ毎の特徴を理解する必要がある。
- 確認ポイント 6 は、eKYC ソリューション選定の大きなファクターということができる。本人確認書類の撮影、容貌撮影等において、顧客体験（撮影のみならず全体操作の円滑さ、迷う局面が少ないことも含めて）が確保され、結果として離脱率が満足いくレベルであること、偽造・なりすましに対して精度が高く堅牢なコントロールが実現していること、事業者の目視確認負担軽減への配慮がなされていること、それぞれ相反する要素もある 3 つの目的のバランスをどう捉え、どれだけ同時実現できるのかを見極める必要がある。

解説ポイント 7：プロバイダ以外の第三者の関与

- eKYC においてプロバイダ以外の第三者の関与が求められる方法として、「ト」（本人確認書類の画像又は IC チップ情報＋銀行等への顧客情報の照会）と「ワ」（公的個人認証サービスの署名用電子証明書）の 2 つのケースがある。それぞれ他の方法にはない特徴を有する。
- 「ト」（本人確認書類の画像又は IC チップ情報＋銀行等への顧客情報の照会）については、プロバイダが提供する本人確認書類の撮影もしくは IC チップ読取と、その後のプロセスである銀行への顧客情報の照会との関係について、プロバイダによって取組姿勢が異なる。
- まず、プロバイダ自身の対応範囲を撮影結果もしくは IC チップ読取結果のみを提示するまでとし、銀行側確認結果の事業者への提供については別のプロバイダと事業者間で別途の契約が必要とするケースがある。この場合事業者は、各プロバイダと別個に契約したうえで、それぞれから取得した結果の照合・確認作業を自ら行うことが想定される（当該部分の更なる BPO は可能である）。
- 次に、対応範囲として、撮影結果もしくは IC チップ読取結果のみの提示に加え、銀行からの確認結果も統合した照合結果を事業者に提供する領域までカバーするプロバイダも存在する。

・　いずれにしてもこの方法は、事業者自らが実施しなければならない本人確認の相当部分を、取時確認の実績が豊富な銀行に依拠できるところが一番のメリットであり、特に取引時確認の実務経験が浅い事業者とっては、銀行のノウハウを活用することが可能となる。ただし、サービス提供の関係者が増えることに伴う追加コストの発生や、顧客における作業が増える点は考慮する必要がある。また、この方法は、顧客にとっては、自身が有する預金口座の銀行がこのサービスに参加していないと利用できない点、依拠される銀行側が把握している顧客情報と事業者が把握している顧客情報との間で不一致[18]が相応の確率で発生し得る点等にも留意が必要である。

・　「ワ」（公的個人認証サービスの署名用電子証明書）では、公的機関（J-LIS）が関与することとなる。この方法の最大の特徴は、公的機関がマイナンバーカードに内在する電子証明書の有効性を確認する役割を担うため、本人確認書類の撮影、容貌の撮影を要せず、本人確認の相当部分を公的機関に事実上委ねられるという点にあり、顧客負担、事業者負担の軽減が最も期待される方法であると言える。しかしながら、マイナンバーカードの普及が途上であること、IC チップ読取の際の暗証番号入力やロックに伴う離脱[19]が懸念されること、Web ブラウザでのサービス提供ができず顧客のスマートフォンアプリのインストールが必要となることには留意が必要である。

解説ポイント８：本人確認以外の取引時確認

・　解説ポイント１～７までは取引時確認のうち、本人確認[20]に関する部分である。この部分は、eKYC ソリューションを導入することにより、CX 向上、事業者のコスト削減、金融犯罪対策の実効性向上へ貢献することが期待される。ここでは、本人確認以外の取引時確認プロセスおよび顧客受入れの際の顧客管理に、プロバイダの提供サービスがどのようなインパクトを及ぼし得るのかを整理する。

・　まず、犯収法上は、ハイリスク取引に当たる場合には、通常の特定取引の場合とは異なる確認方法が求められるため、ハイリスク取引に該当する疑いを検知することが必要となる。例えば、顧客が外国 PEPs に該当するか否かの確認である。

・　また、事業者は、AML/CFT ガイドライン上で対応が求められる事項に対応するため、顧客受入方針を定め、新規顧客の受入時に当該方針で定められる高リスク先、あるいは謝絶対象先に該当するかどうかのスクリーニングを行うことが重要である。そのためには、職業等、身元確認に必要な情報以外の情報も収集しなくてはならない。また、AML/CFT ガイドライン上で求められるリスクベースアプローチの実践のためには、リ

18　例えば、住所変更を行った場合において、新住所（事業者が把握している情報）と旧住所（銀行側が把握している情報）による不一致が想定しうる。

19　個々の事業者としてだけではなく、たとえば業界団体から利用者への啓もう活動、あるいはマイナンバーカード利用促進の観点から政府機関からの広報活動をより積極的に行うことも有用である。

20　厳密には、本人確認のうち「身元確認」に該当する部分である。

スクが高いと判断した顧客に対しては、リスクに応じて追加的な調査や取引制限等の必要性を検討し、実施することが求められる。なお、事後的な確認および対外的な説明のためには、調査結果、判断過程などの承認プロセスを記録し保存することが必要である。この中でプロバイダが提供可能な業務としては以下が挙げられる。

- スクリーニング：前もって登録しておいた顔情報[21]が一致した顧客からの申込みがあった場合、アラートを発する機能をオプションで提供するプロバイダがある。たとえば過去に問題があったり、謝絶したりした顧客の顔情報を登録することによって、同一人物が仮に異なる氏名等で申し込んでも検知可能となる。さらには既存顧客のすべての顔情報を登録することで当該顧客の顔情報の悪用の検知等も技術的には可能となる。当該機能は事業者ごとに提供する場合と事業者横断で照合を行う機能を提供する場合の双方がある。また顔情報ではなく、特定の氏名、生年月日を指定すると、一定のあいまい度で情報ベンダーによる商業用データベースに登録されているウォッチリスト（反社会的勢力、経済制裁対象者、外国 PEPs[22]等）とのスクリーニング結果、氏名等でインターネットや商業用データベース等を検索し、合致した記事情報を提供するものもある。
- 顧客リスク評価：上記スクリーニングに加えて、行動解析による不正検知の機能を提供しているプロバイダも見られる。これは顧客リスク評価あるいはその先の取引モニタリングへの活用を視野にいれたものである。とりわけプロバイダとして得意分野である顔情報を利用することによって特徴ある検知機能が発揮されること[23]が期待できる。

解説ポイント 9 ：事業者が顧客に提供する商品・サービス・チャネル

- 解説ポイント 1 のうち、「⑦事業者が顧客に提供する商品・サービス・チャネル」に関連して、eKYC のそれぞれの方法（ホ、ヘ、ト、チ、ワ）のいずれを採用するかは、事業者が提供する商品・サービス、チャネルの特質も踏まえる必要がある。たとえば、預金口座、クレジットカードの場合は、最終的に転送不要郵便でカードを顧客に送付することが想定される。この点で、eKYC 部分の顧客負荷がほかの方法に比べて軽い（容貌撮影不要、書類撮影もしくは IC チップ読取のみで完了する）チの方法も選択しうる。

解説ポイント 10：非機能要件

---

21 顔画像そのものではなく、特徴を数値化した状態で保有する（当該数値から顔画像を復元することはできない）といった工夫が見られる。なお、当該工夫も含め、プロバイダが保有する顧客関連情報についての個人情報保護法上の手当てについては、問題がないことを確認する必要がある。

22 外国の政府等において重要な地位を占める者

23 たとえば行動解析によって、いつもと異なる遠隔地での利用や高額利用といった高リスク事象が発生した際に容貌撮影を求めて本人かどうかを判断するといったような利用方法が想定される。

・　ここまで主に機能要件を中心に考察したが、あわせて非機能要件を見極めることも重要である。検討すべき非機能要件の例は以下のとおりである。

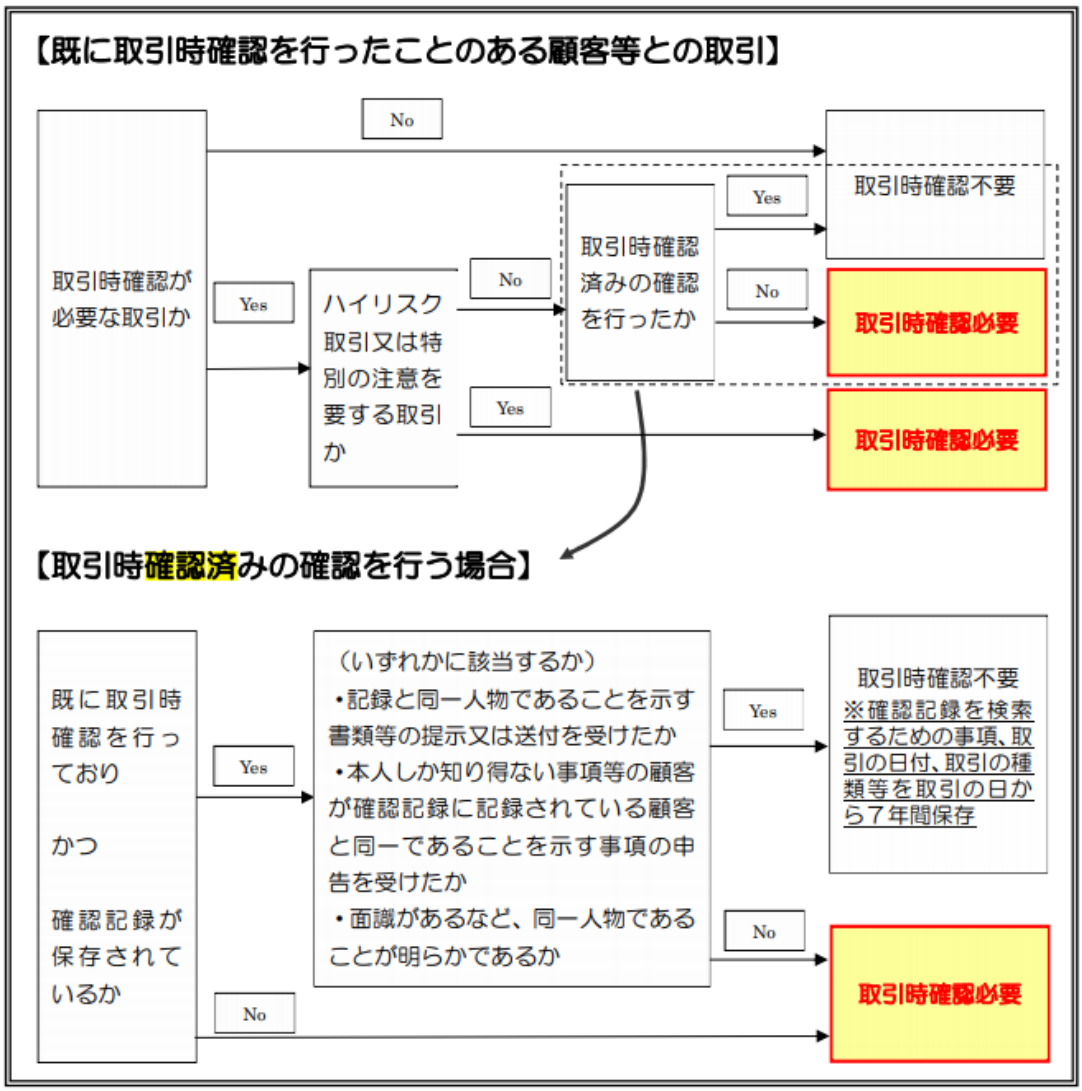
非機能要件		説明
可用性	稼働率	eKYC サービスの稼働率が自社業務の目標稼働率と整合しているか。
	復旧目標	eKYC サービスが停止した場合のサービス復旧までの目標復旧時間が自社の業務目標復旧時間と整合しているか。
	障害・災害対応	eKYC サービスに障害や災害により支障が生じた場合、縮退するなど、自社の最低限のサービスレベルを維持できるか
	災害復旧	大規模自然災害等で eKYC のデータセンターが被災した場合にサービスが継続可能か。
性能・拡張性	レスポンス	eKYC サービスの処理時間は、自社業務で求められるレスポンス時間を実現可能か。
	処理増加時の拡張	eKYC サービスの処理能力は、サービス提供中であっても、容易に増強可能か。
運用・保守性	運用時間	eKYC サービスの提供時間(メンテナンスを含む)は自社のサービス提供時間と整合しているか。
	バックアップの責任	プロバイダと自社のデータのバックアップの責任は明確になっており、全体として確実にデータのバックアップが取得されているか。
	運用監視	プロバイダのシステム監視サービスは、自社の運用監視方針及び要件と整合しているか。
	障害連絡	eKYC サービスに障害が発生した場合の対応は、自社の障害対応方針及び要件と整合しているか。
	マニュアル	管理画面を提供する eKYC の場合、顧客が利用するためのマニュアルが提供されるか。
	変更管理	eKYC サービスの変更にあたっては、変更内容や影響範囲を事前に連絡されるか。
移行性	サービス移行	eKYC サービスへの移行に際し、問題はないか。
セキュリティ・プライバシー	セキュリティ管理態勢	プロバイダが情報セキュリティに関わる認証を取得することで、情報セキュリティ管理態勢を構築しているか。 また、プロバイダのセキュリティ方針や管理水準等は、自社のものと整合しているか。
	セキュリティ対策	公的なセキュリティ基準を用いた自己評価や外部評価を実施し、事業者が求める水準のセキュリティ対策を実施しているか。
	データ保管先	eKYC サービスで扱うデータの保管先は国内であることを確認しているか。海外である場合はそのリスクについて需要可能か。
システム環境	実装方式/環境	モバイルアプリの SDK 版、ブラウザ版、SaaS など、自社が求めるサービスの方式や利用環境にプロバイダが対応しているか。

3.　取引時の顧客確認

本章では、顧客（自然人）を受け入れて取引関係を確立した後（口座が開設された後）に、当該顧客が個々に取引を実施する局面を対象とする。

3.1.　犯収法上の確認済みの確認

まず犯収法上は、特定事業者が取引を行う顧客等について既に取引時確認を行っており、かつ、当該取引時確認について記録（確認記録）を保存している場合には、通常の特定取引を行う際に、記録されている者と同一であることを示す書類等の提示又は送付を受けるか、顧客等しか知り得ない事項等の申告を受けることにより、顧客等が当該記録と同一であることを確認するとともに、確認記録を検索するための事項、取引等の日付、取引等の種類を記録し、取引の日から７年間保存すれば、取引時確認済みの顧客等との取引として、改めて取引時確認を行う必要はないとされている。（いわゆる「確認済みの確認」。下図[24]参照。）



[24] JAFIC「犯罪収益移転防止法の概要」より。(hougaiyou20210719.pdf (npa.go.jp))
なお、平成 23 年改正犯罪収益移転防止法の施行前に確認をしたことのある顧客等との取引については別途の取扱が定められているおり留意が必要。

これにより、口座開設段階で取引時確認を完了した顧客に対しては、取引時には、基本的には本人確認のうち当人認証を実施すればよいことになる。本対応を可能とするための前提は以下のとおりである。

① ハイリスク取引または特別の注意を要する取引ではないこと等の確認ができていること
② 確認記録が保存されていることの確認[25]ができていること

3.2. AML/CFT ガイドライン上の継続的顧客管理の要請

上記の確認済みの確認の実施体制の整備に加えて、既存顧客については、スクリーニング、取引モニタリング等 AML/CFT 対応としての要求事項に対し、リスクに応じて適宜対応できていることが必要である。

例えば、AML/CFT ガイドラインでは、継続的顧客管理として、疑わしい取引の検知および届出のほか、以下を含む対応を事業者に求めている。

イ．取引類型や顧客属性等に着目し、これらに係る自らのリスク評価や取引モニタリングの結果も踏まえながら、調査の対象及び頻度を含む継続的な顧客管理の方針を決定し、実施すること ロ．各顧客に実施されている調査の範囲・手法等が、当該顧客の取引実態や取引モニタリングの結果等に照らして適切か、継続的に検討すること ハ．調査の過程での照会や調査結果を適切に管理し、関係する役職員と共有すること ニ．各顧客のリスクが高まったと想定される具体的な事象が発生した場合等の機動的な顧客情報の確認に加え、定期的な確認に関しても、確認の頻度を顧客のリスクに応じて異にすること ホ．継続的な顧客管理により確認した顧客情報等を踏まえ、顧客リスク評価を見直し、リスクに応じたリスク低減措置を講ずること 特に、取引モニタリングにおいては、継続的な顧客管理を踏まえて見直した顧客リスク評価を適切に反映すること

また、AML/CFT ガイドラインでは、取引モニタリングに関しては、以下を含む適切な体制を構築し、整備することが求められている。

イ．自らのリスク評価を反映したシナリオ・敷居値等の抽出基準を設定すること ロ．上記イの基準に基づく検知結果や疑わしい取引の届出状況等を踏まえ、届出をした取引の特徴（業種・地域等）や現行の抽出基準（シナリオ・敷居値等）の有効性を分析し、シナリオ・敷居値等の抽出基準について改善を図ること

[25] この要件から、eKYC によって実施した取引時確認の記録を保存することの重要性が確認できる。すなわち記録の保存を eKYC プロバイダ等に委託している場合も、事業者として、当該委託先がこの要件に照らして記録の保存を適切に実施していることの確認、事業者が必要としたときに適時適切に当該情報にアクセスできることの確認等を実施する必要がある。

3.3. 業態ごとの一般的な当人認証

上記前提の下に、事業者毎に、取引関係確立後（口座が開設された後）の個々の取引の局面で行われる当人認証を整理すると以下のとおりとなる。

まず、クレジットカード事業者の場合は、特定取引等（特別に注意を要する取引およびハイリスク取引）を行う場合には、犯収法上の取引時確認や確認済みの確認を実施する必要があるが、それ以外の場合については、上記 3.2 への対応として、顧客が決済時にクレジットカードを提示し（認証の所持要素）、暗証番号を入力する（認証の知識要素）ことによって当人認証が行われている[26]。

次に、資金移動業者の場合は、特定取引等（10 万円超の現金取引、特別に注意を要する取引、ハイリスク取引）を行う場合には、犯収法上の取引時確認や確認済みの確認を実施する必要があるが、それ以外の場合については、上記 3.2 の対応として、カード決済であればクレジットカードと同様であり、スマホ決済の場合は、上記 3.2 の対応として、入出金・決済時に、スマホで認証（ユーザ ID、暗証番号、顔認証等の知識要素、生体要素による）を行うことが想定される。

最後に、銀行の場合は、特定取引等を行う場合には、犯収法上の取引時確認や確認済みの確認を実施する必要があるが、それ以外の場合については、上記 3.2 の対応として、入出金・送金時に銀行カードの提示（所持要素）および暗証番号の入力（認証の知識要素）ないしは生体認証（生体要素）を行うことによって認証が完結している。また、カード提示を前提としないインターネットバンキングにおいては、ユーザ ID（認証の知識要素）、暗証番号（認証の知識要素）、顔認証（生体要素）等によって認証が完結する。

このように、所持要素以外の認証要素のみが求められる局面[27]では、事業者は認証の仕組みの整備が必要になる。プロバイダの多くは、このような認証ソリューションも提供している。事業者として認証の仕組みを整備するにあたって（あるいは整備済みであっても）、プロバイダのソリューションについて、コスト・顔認証技術の優位性、その他の関連ソリューションとの組合せでの総合力等から、当該ソリューションを活用することも選択肢の一つとなり得る。

3.4. 顧客情報の更新

上記 3.3 の通り、継続的顧客管理は幅広い概念であるが、このうち、顧客情報の更新については、犯収法第 11 条においても、「特定事業者は、取引時確認、取引記録等の保存、疑わしい取引の届出等の措置を的確に行うため、当該取引時確認をした事項に係る情報を最新

---

[26] 一定額未満の低額決済の場合は、知識要素による認証不要とすることが認められている。

[27] 現状は所持を前提としている取引も今後 DX 化の進展とともに認証の在り方は大きく変化し得る。たとえば「顔パス」決済等の実現が想定される。

の内容に保つための措置を講ずる」ことが義務付けられている[28]。また、金融庁の「マネロン・テロ資金供与対策ガイドラインに関するよくあるご質問（ＦＡＱ）[29]」において、「リスクに応じた頻度により、あるいは、随時に顧客情報を更新する必要」があるとされ、実践の具体例が示されている。

継続的顧客管理として求められる顧客情報の更新は、犯収法の要件である取引時確認に該当するものではないため、金融サービスの特性やリスクに応じて、事業者としての適宜の確認を実施することが求められる。

顧客情報の更新は、銀行等が実務適用を始めているところであるが、顧客との接点についてはオンライン化が進んでおらず、郵送が中心とならざるを得ない現状であり、以下のような課題が認められる。

①郵送で案内しても宛所なしの不着返却が多い
②届いても回答を得られない比率が高い
③多くの苦情を寄せられる
④回答があったものについても書類不備などが多い
⑤顧客対応や書類不備確認、入力対応等の負担（あるいは事務委託のコスト）が重い

これらの課題に向けた解決策として eKYC ソリューションの活用の可能性を整理すると以下のとおりとなる。

1. (ホ)本人確認書類の画像＋容貌の画像を活用する方法

   顧客のメールアドレスを把握している等、電子的な連絡が可能な場合は、本人確認も含めた顧客情報の更新依頼は比較的容易と思われる。流れとしては、本人確認情報の更新の有無を質問し、更新の必要がある場合、改めて「ホ」の方法により、本人確認書類および容貌の撮影を求めることになり、郵送に比べれば離脱リスクは低下することが期待

---

[28] かかる犯収法上の義務については、パブリックコメント回答で、「最新の内容を把握するために調査を行うことまでを求められているものではない」、「本人特定事項等の変更があった場合に顧客等が特定事業者にこれを届け出る旨を約款に盛り込むこと等を想定しております」との解釈が示されている（平成 24 年 3 月 26 日警察庁および共管各省庁「『犯罪による収益の移転防止に関する法律の一部を改正する法律の施行に伴う関係政令の整備等及び経過措置に関する政令案（仮称）』等に対する意見の募集結果について」21 番、128 番、131 番）。もっとも、AML/CFT ガイドライン上の継続的顧客管理では犯収法上の義務を超える対応が求められている点、上記 3.2 および本文で言及する金融庁「マネロン・テロ資金供与対策ガイドラインに関するよくあるご質問（ＦＡＱ）」のとおりである。

[29] 令和３年３月 26 日公表。その 62 頁において、「継続的な顧客管理については、顧客に係る全ての情報を更新することが常に必要となるものではなく、顧客のリスクに応じて、調査の頻度・項目・手法等を個別具体的に判断していただく必要があります。一般的には、高リスク先については１年に１度、中リスク先については２年に１度、低リスク先については３年に１度といった頻度で情報更新を行うことが考えられます。これ以上、期間を延ばす場合には、合理的かつ相当な理由が必要になるものと考えます。」と実践の具体例の１つが示されている。

される。ただし、継続的顧客管理に対する顧客の理解が浸透しない中で、どこまで本人確認書類および容貌の撮影に応じるかは不透明である。なお、継続的顧客管理は取引時確認とは異なる法律要件であり、たとえば容貌の画像まで必要とするかどうか、必要とするのはどのような場合か等については、事業者ごとにリスクを踏まえて検討すべき点である。

2. (ヘ)IC チップ情報＋容貌の画像を活用する方法
   上記「ホ」と同じことが言える。
3. (ト)本人確認書類の画像又は IC チップ情報+銀行等への顧客情報の照会を活用する方法
   銀行自体が継続的顧客管理に苦慮している中、銀行への顧客情報の照会をもって、事業者として実施すべき継続的顧客管理（顧客情報の更新）が適切に完了したと整理するのは困難と思われる。
4. (チ)本人確認書類の画像又は IC チップ情報+転送不要郵便を活用する方法
   継続的顧客管理は取引時確認要件とは異なるものであり、ここで求める転送不要郵便までを求めるものではなく、上記の「ホ」または「ヘ」を活用する方法で代替できる。
5. (ワ)公的個人認証サービスの署名用電子証明書を活用する方法
   同様の IC チップ読取を行う「ヘ」等の方法と異なり、「ワ」は電子証明書が有効かの確認を J-LIS に委ねるものであり、事業者としての本人確認負担軽減および、金融犯罪対策の堅確性向上が期待される。顧客体験の向上という意味では、郵送、あるいは他の eKYC の方法と比べれば利便性は高いと思われる要素がある一方で、既述の通り、暗証番号の失念、電子証明書失効の場合の取扱、さらにはマイナンバーカードの普及が途上であることが懸念材料となり得る。この点で、令和 3 年 5 月に成立した「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」において定められた、マイナンバーカード機能のスマホ搭載、本人同意を前提とした基本 4 情報（氏名・住所・性別・生年月日）の提供は、継続的顧客管理に大きな変革をもたらす可能性があり、動向に注視していく必要がある。特に、基本 4 情報の提供は、事業者が定期的に J-LIS から基本 4 情報の内容確認（必要に応じた更新結果）を取得することができるものとなり、顧客に対する確認が不要となる。

上記の通り、継続的顧客管理において eKYC は相応の付加価値をもたらす可能性が高いと言える。ただし本人確認情報の更新は、継続的顧客管理の一部であり、その他の要素（本人確認情報以外の顧客属性情報の更新、顧客リスク評価、取引モニタリング）も踏まえた金融犯罪対策実効性・顧客体験向上、事業者負荷軽減を検討する必要がある。

4. まとめ

eKYC プロバイダが提供するサービスは進化し続けている。また FATF による第 4 次対日相互審査報告書の公表を受け、法改正やより厳格な当局目線が予想される中、現行の eKYC の法律要件も変わってくる可能性も否定できない。またコロナ禍の中で、次々と新たな金融犯罪の手口が開発される等、悪用する側の技術進歩も著しい。このような外部環境、規制環境について常に注視し続けることが重要である。

顧客管理プロセスが法律要件に照らして適切であることの最終責任はあくまで事業者側にある。この点で、個々の顧客に対する新規受入時の判定の相当部分はプロバイダに委託したとしても、以下の点については事業者として適切にモニタリングし委託者責任も含めた責務を果たす必要がある。

- ✓ プロバイダの判定プロセス（品質、可用性、レスポンス等）が当初合意したレベルを適切に充足しているか
- ✓ 上記運用状況も含め、当初合意したレベルが、直近の環境変化やリスクを踏まえて適切であるかの適宜の有効性検証

さらに、eKYC も含めた本人確認だけではなく、eKYC を利用することで成り立っている取引時確認プロセスおよび顧客管理体制全体の堅牢制確保が事業者に求められる。

上記を確保するためには、eKYC 導入の際に、基本方針（適用範囲、適用手法・技術、その他の要件定義明確化と、なぜその内容としたのかについての、ビジネス戦略およびリスク評価に基づく意義、理由の明確化、当該 eKYC を含む本人確認プロセスが、全体の取引時確認プロセスにおいて整合的に位置づけられていることの明確化）とこれに基づく具体的な要件定義、運用基準の文書化が求められる。

以上