BOJ Reports & Research Papers

決済システムレポート別冊シリーズ

Payment and Settlement Systems Report - Annex

オンラインでの本人確認（eKYC）に関する国際標準と関連技術

日　本　銀　行
決 済 機 構 局
2023 年 4 月

（決済システムレポート別冊シリーズについて）

日本銀行は、決済システムの動向を鳥瞰し、評価するとともに、決済システムの安全性・効率性の向上に向けた日本銀行および関係機関の取組みを紹介することを目的として、「決済システムレポート」を定期的に公表している。

「決済システムレポート別冊シリーズ」は、決済システムを巡る特定のテーマについて、掘り下げた調査分析を行うものである。今回は、オンラインでの本人確認（eKYC）のコアとなる技術的観点に関し、国際標準である ISO 5158 や諸外国から公表されている各種法令や規格等を参考に、昨今の議論内容を俯瞰する。

【本レポートに関する照会先】
日本銀行決済機構局決済システム課　（post.pr@boj.or.jp）

2023 年 4 月
日 本 銀 行
決 済 機 構 局

オンラインでの本人確認（eKYC）に関する国際標準と関連技術

■要　旨■

昨今、モバイル端末の普及と、それを活用した金融サービスの提供が進むにつれ、オンラインでの本人確認（eKYC）が広がりつつある。本人確認は、金融サービスを提供する上で欠かすことができない根源的な業務である。デジタル社会の中、この本人確認をオンラインで正確に行うことは、世界各国で金融サービス提供者にとって重要な課題になっている。

本稿では、eKYC に関する国際標準とそれに関連する諸外国における議論について、主に技術面を中心に整理する。メインのテーマは、オンラインでの顧客の本人確認方法とサービスへの活用策についてである。オンラインで本人確認を行う際、その結果がどの程度確かに本人であると言えるのか、提供するサービスのレベルに応じて、その確認の強度を設定する考え方を整理する。こうした方法は、国際標準化機構（ISO）のほか、諸外国でも様々な形で議論されており、本稿でそれらの内容を紹介する。

加えて、本稿では、オンラインで本人確認を行う上での個人情報保護、および、モバイル端末側のセキュリティについても検討する。オンラインで本人確認を行う際、その人の持つ属性という個人情報を扱うことになる。そのため、個人情報の保護やセキュリティに配慮する必要が生じる。この個人情報保護の論点も、ISO での整理とともに、諸外国での整理も合わせて紹介する。そして、個人情報を適切な環境で取り扱うためのモバイル端末側のセキュリティ機能の構成についても、ISO における整理を基に紹介する。

本稿の内容が参考になり、より安全で効率的なオンラインでの本人確認が実社会の中で広まると幸いである。

（白紙ページ）

目次

オンラインでの本人確認（eKYC）に関する国際標準と関連技術

1. はじめに

昨今のモバイル端末の普及に伴い、オンラインでの金融サービスの需要が急速に高まっている。金融サービス提供者にとって、顧客（金融サービス提供者が提供するサービスの利用者のことを言う）の本人確認は欠かすことができない業務である。オンラインで本人確認（eKYC：electronic Know Your Customer）を正確に行うことは、世界各国でモバイル金融サービス提供者にとっての重要な課題になっている。

こうした中、諸外国では、eKYC にかかる要件や手法等にかかる法制化や標準化が進められている。これらを比較してみると[1]、内容面での差異は一部見られるものの、相互に重なる部分も多い。それは、eKYC は、プライバシーやセキュリティを保護しつつも、サービス提供に必要十分な正確性が確保される必要があるという、諸外国で共通した考え方があるためだと思われる。

こうした諸外国で共通する要件や手法を参考にすることは、eKYC の安全性や信頼性等を確保する上で有益である。こうしたことから、国際標準化機構の金融サービス専門委員会（ISO/TC 68）では、オンラインで顧客の本人確認をする際に活用可能な、国際標準としての考え方やその手法を整理し、ガイドラインとして取り纏めた。

本稿は、この国際標準化機構（ISO）で策定されたモバイル金融サービスにおけるオンラインで顧客の本人確認を行う際の国際標準の内容を中心に、eKYC にかかる各国の法令や規格の内容を交えながら、eKYC に関する主に技術的な内容について概説する。本稿は、3 つの項目から成り立っている。一つ目は、モバイル金融サービスにおける顧客の本人確認の方法とその結果をサービスに活用する際の考え方、二つ目は、顧客の本人確認における個人情報保護、そして、三つ目はモバイル端末側のセキュリティについてである。

本稿の構成を詳説すると、第 2～4 節では、一つ目のモバイル金融サービスにおける顧客の本人確認の方法とその結果のサービスへの活用策について議論する。まず、第 2 節において、一般的なオンラインでの顧客の本人確認方法を紹介する。その上で、第 3 節で、モバイル金融サービスで顧客の本人確認に使われるアイデンティティがどの程度確

[1] 諸外国における eKYC にかかる要件や手法等にかかる法制化や標準化に関連する内容については、後述する本稿の 4.2. 節や 5.2. 節で議論している。

からしいかを示す「保証レベル」という考え方について説明する。そして、第 4 節で、この「保証レベル」の考え方を用いて、顧客の本人確認の結果をサービスレベルに反映している事例を紹介する。

次いで、第 5 節では、二つ目のモバイル金融サービスでの eKYC におけるプライバシー保護について、顧客の個人情報保護にあたって守るべき基本的な考え方を、ISO の規格や諸外国のルールを基に整理する。そして、第 6 節では、三つ目の個人情報を適切な環境で取り扱うために必要なモバイル端末側のセキュリティ構造について、ISO の規格を参照しつつまとめる。最後、第 7 節で、全体のまとめを行って本稿を締めくくる。

2. 金融サービスと eKYC

本人確認（KYC: Know Your Customer）は、金融サービスを提供する上で、欠かすことができない業務である。昨今のモバイル端末の普及、社会のデジタル化の進展に伴い、オンラインでの本人確認（eKYC）を行う場面が増えている。

こうした状況を受け、ISO/TC 68 では、オンラインで顧客の本人確認（Customer Identification）を行う上で、異なる要件にも対応可能な適切な手法を選択する際の共通的な考え方を整理し、2023 年 1 月に国際標準 ISO 5158「モバイル金融サービスにおける顧客の本人確認に関するガイドライン」を公表した[2]。この顧客の本人確認は、eKYC のコアとなる技術である[3]。

---

[2] 正式名称は、ISO 5158:2023, "Mobile financial services — Customer identification guidelines"。https://www.iso.org/standard/80948.html 参照。

[3] KYC（Know Your Customer）, Identification の用語の定義に関しては、ISO 5158 では ISO 12812-1（モバイル金融サービスの一般的なフレームワーク）および ISO/IEC 24760-1（アイデンティティマネジメントのフレームワーク）を参照するとある。そして、それらの規格では、

・ KYC（Know Your Customer）:
"process to verify the identity of a customer in order to prevent financial crime, money laundering and terrorism financing.（金融犯罪、マネー・ローンダリングおよびテロ資金供与を防止するために、顧客のアイデンティティを確認するためのプロセス）" [ISO 12812-1:2017, 3.18]

・ Identification:
"process of recognizing an entity in a particular domain as distinct from other entities.（特定のドメインにあるエンティティを、他のエンティティと区別して認識するプロセス）" [ISO/IEC 24760-1:2019, 3.2.1]

と定義している。eKYC（electronic Know Your Customer）は、用語の定義にかかる節に記載されていない。ISO 5158 のイントロダクションには、”Customer identification is at the core of eKYC.”との記載がある。

なお、本稿では、KYC を「本人確認」、eKYC を「オンラインでの本人確認」、Customer Identification を「顧客の本人確認」と訳している。もっとも、これ以降では、Customer Identification については「顧客の本人確認」という用語を使うが、KYC、eKYC については本人確認という言葉は使わず、それぞれ KYC、eKYC と表記する。なお、「オンラインで顧客の本人確認を行う」という言葉は、「オンラインで Customer Identification

まず、以下において、オンラインで顧客の本人確認を行うとはどういうことなのか、整理を行う。

2.1. 顧客の本人確認におけるアイデンティティ

アイデンティティと属性

本稿では、ある自然人が持つ特徴あるいは所有しているものを「属性（Attribute）」と呼び、ある自然人にかかる属性の集合体のことを「アイデンティティ（Identity）」 と定義する[4]。属性には、自然人に特徴的なこと、例えば、

- 顔の輪郭、指紋や虹彩といった生体固有の情報
- 住所、電話番号といった、各自然人が選択して取得した情報
- 国民 ID、免許書番号、パスポート番号など、国家等が割り当てた情報
- 位置情報などの個人情報

などがある。

モバイル金融サービス提供者がオンラインで顧客の本人確認を行う際には、モバイル金融サービス提供者の顧客はあらかじめサービス提供者が運営するサーバ上に自らの属性を登録する。実際にその顧客の本人確認を行う際には、顧客が自らの属性の一部の情報を提示し、その情報をモバイル金融サービス提供者がサーバ上の情報と照合する。照合の結果、両者が同一であると判断することによって、オンライン上で顧客の本人確認を実施できたことになる[5]。

ISO 5158 においてアイデンティティ属性とは、顧客の本人確認に用いる属性のことである。以下、本稿で属性という言葉は、このアイデンティティ属性のことを指して議論をすすめる。

を行う」ことを意図して表記している。また、単に「本人確認」とある言葉は、KYC および identification の意味を含む言葉として用いている。

[4] この記述は、ISO/IEC 24760-1:2019（アイデンティティマネジメントのフレームワーク）を参考にしている。なお、ISO/IEC 24760-1:2019 では、用語の定義として、
attribute: "characteristic or property of an entity（エンティティの特性または性質）"
identity: "set of attributes related to an entity（エンティティに関連する属性の集合）"
と記載されている。

[5] 犯罪による収益の移転防止に関する法律（以下、犯収法）では、本人確認を、本人特定事項（自然人の場合、氏名、住居及び生年月日）の確認としており、これは、いわゆる取引開始時に本人を確認する身元確認のことを指している（身元確認についての詳細は 4.2.1 節参照）。もっとも、本稿での本人確認とは、取引開始時に行う身元確認だけではなく、取引実行時に本人であることを確認する当人認証や、サービス提供を受ける意思確認を含むなど、あらゆる取引場面を想定した、犯収法の定義より広くとらえたものである。

オンラインで顧客の本人確認を行う際に用いる属性の選択

モバイル金融サービス提供者が顧客の本人確認を行う際に用いる属性の選択においては様々なバリエーションが考えられる。ISO 5158 では、顧客の本人確認に用いる属性として国際規格 ISO 24366（自然人識別子<NPI：Natural Person Identifier>の規格）で定義されているデータレコード（表 1 参照）を参照することを推奨している（ISO 24366 については、後段 BOX （1）参照）。もちろん、これに止まらず、金融サービスの性質によっては、これに加えて、位置情報（自宅やオフィスの住所）、勤務先、職種、役職、出向先、収入、家族構成、緊急連絡先など、属性の追加も考えられる[6]。また、各法域の本人確認の規制やマネー・ローンダリング規制（AML: Anti-Money Laundering）など、顧客を識別するためのいくつかの必須属性を各法域の規制上が定義している場合もあることにも、留意が必要である。例えば、日本の場合には、犯罪による収益の移転防止に関する法律（以下、犯収法）第 4 条に取引時確認事項にかかる規定があるほか、現在議論中の欧州の eIDAS2.0 案には、適格電子属性証明に含む必要がある情報が定義されている[7]。

なお、ISO 5158 では、NPI 発行者は、各法域の規制に応じて、アイデンティティ情報プロバイダー（Identity Information Provider：IIP、属性情報を提供する組織）あるいは、アイデンティティ情報オーソリティ（Identity Information Authority：IIA、属性情報の妥当性や正当性を証明できる組織）とみなすことができるとしている[8]。

---

[6] 例えば、クレジットカードや住宅ローンの申込の際に、顧客にここで例示した属性情報の提示を求める金融機関が見られる。

[7] 例えば、欧州の eIDAS2.0 では、適格電子属性証明に含む必要がある情報として

1. 住所（Address）
2. 年齢（Age）
3. 性別（Gender）
4. 民法上の身分（Civil status）
5. 家族構成（Family composition）
6. 国籍（Nationality）
7. 資格（Educational qualifications, titles and licenses）
8. 専門的な資格、許可（Professional qualifications, titles and licenses）
9. 公的な資格、許可（Public permits and licenses）
10. 財政情報（Financial and company data）

が列挙されている（参考：濱口総志、「eIDAS2.0 - eIDAS 規則の改正案の解説-」、https://www.jipdec.or.jp/library/report/20210713-3.html）。

[8] IIP 中で、信頼できる情報を出せる組織が IIA に該当する。なお、現在公表されている ISO 24366:2021 には、NPI 発行者にかかる規定はない。

表 1：自然人識別子（ISO 24366）が定める自然人の属性を示すデータレコード

データ要素	必須情報の要素か否か
法律上の名前　― 名字	必須情報
法律上の名前　― ミドルネーム	オプション
法律上の名前　― 下の名前	必須情報
別名（愛称等）	オプション
別名の種類（定義に沿ったコードを入力）	オプション
誕生日	必須情報 （例外あり）
産まれた国	必須情報 （例外あり）
電話番号	オプション
電話番号の種類（固定・携帯／オフィス・個人等）	必須情報 （登録有の時）
電子メール	オプション
電子メールの種類	必須情報 （登録有の時）
国籍	必須情報
住所	必須情報
住所の種類（本宅／別宅等）	必須情報
法域（国家）が発行した ID 番号	必須情報
法域（国家）が発行した ID の種類	必須情報
ID を発行した法域(国家)	必須情報
性別	オプション
生体情報	オプション
情報のステータスを表すフラグ	必須情報
情報の変更理由	オプション
情報変更日	必須情報
確認フラグ	必須情報
確認にあたっての元情報	必須情報

出典：ISO 24366:2021

2.2. 金融サービスにおけるオンラインでの顧客の本人確認プロセス

ここでは、モバイル金融サービス提供者が顧客の本人確認を行う際のプロセスを提示する。

2.2.1. 取引開始前に行う顧客の本人確認

まず、取引を開始する前には、顧客は、モバイル金融サービス提供者が求める「検証可能な属性」と「その属性を裏付けられる証拠」を提示する。

顧客が提示する証拠

オンラインでの顧客の本人確認において、顧客が提示する証拠の具体例としては、以下の 3 種類が考えられる。

- デジタル化された物的証拠：
  例：運転免許証やクレジットカードをデジタルカメラで撮影したデータなど。
- デジタルアイデンティティ：
  例:デジタル署名を生成することができる IC カードなどに格納されたトークン、所有者の生体等の属性（指紋など）を含むデジタル証明書やソフトウェアなど。
- オンライン上のアイデンティティ情報データベース：
  例：携帯電話会社の顧客データや金融機関の口座情報のデータベースにアクセスして取得したデータ、政府機関が運用するアイデンティティ情報オーソリティ（IIA）にアクセスした取得したデータなど。

顧客の証拠提示方法

顧客がその証拠を提示する方法には、主に以下の 3 つのパターンが考えられる。

- 顧客に情報を提示してもらう方法。例：
  - 顧客に記入表を示し、名前や住所などの情報を文字で入力してもらう。
  - 顧客に、自撮りで撮影した顔写真や、センサーを用いて取得した指紋情報をアップロードしてもらう。
- 属性を裏付ける証拠から判読する方法。例：
  - 顧客に、免許書等、身分証明書の写真をアップロードしてもらう[9]。
  - 顧客に必要な属性情報を含んだデジタル ID 文書（通常はデジタル署名付き）を提示してもらう。
- パブリックのデータベースから取得する方法[10]。例：
  - 専門の第三者機関であるアイデンティティ情報プロバイダー（IIP）から属性を取得する。
  - 信頼性等をあらかじめ確認できたアイデンティティ情報オーソリティ（IIA）から属性を取得する。

[9] その際、動画を活用するなど偽造の身分証明書への対策が必要である。

[10] データベースから属性を取得する際、その属性を検索するために、例えば、指紋センサーに指を押し付ける、顔写真を撮るなど、属性を検索してリンクさせるための追加情報を顧客に要求することがある。例えば、実際に入国審査においてパスポートにリンクするデータベースへアクセスする時や、インドのアーダール（Aadhaar）システムへアクセスする時などで既に行われている。

モバイル金融サービス提供者による確認と情報と証拠の保管

モバイル金融サービス提供者は、様々な手段を用いて、顧客から提供された属性や証拠の真正性、有効性、適格性を検証することとなる。そして、検証後は、取引時など、顧客の本人確認を行う際に利用できる形で、かつ、情報の安全性を確保したうえで、属性情報と証拠の保管を行うことも重要である。

特に生体認証は顧客の本人確認の際によく使われるが、生体認証には以下の 2 種類があり、それぞれ登録する生体情報の保管場所が異なり、情報保護の方策などのリスク管理面に大きな違いが生じることに留意が必要である。

- クライアント照合：
  身分証明書に印刷されている顔画像、IC チップに格納されている生体情報、顧客のモバイル端末にて生体情報を保存、といった、顧客の手許にある媒体に情報が保管されている状態で、認証を行う方式。

- サーバ照合：
  サーバに生体情報が保存されている状態で、認証を行う方式。

2.2.2. 取引時に行う顧客の本人確認

取引開始後は、顧客が実際に取引を行う際などに、顧客の本人確認を行った上で、サービスを提供することになる。こうした取引時の顧客の本人確認が必要な際には、本人のアイデンティティを対象に同一性の評価を行う。もっとも、アイデンティティは、2.1 節で述べたように属性の集合体であり、全ての属性の確認は不可能である。そのため、実務上はモバイル金融サービス提供者が、必要十分と判断する、１つあるいは複数の本人の属性情報を選択し、顧客にそれらの属性の提示を求め、モバイル金融サービス提供者が保有している属性情報との同一性を判断することとなる。この必要十分性の判断については、第 3 節で議論する。

2.3. 属性情報やその証拠の正確性を担保する上での課題

属性情報やその証拠の正確性を担保するには、いくつかの課題がある。

まず、顧客が提示する証拠の正当性を評価する上では、正しい証拠の仕様を事業者が認識する必要がある。運転免許証やパスポートといった本人確認書類として一般的に用いられている証拠であっても、これまで、偽造防止等の観点から、度々その仕様が変更さ

れており、仕様変更のたびに正しい証拠の仕様のアップデートが必要になる[11]。

属性情報によっては、時間の経過に伴って変化して、適切に顧客の本人確認ができない場合が生じることがある。そのような属性情報の場合は、ビジネスおよびコンプライアンス上の要件に沿った属性情報の継続的な維持管理（追加／削除／更新）が必要である点に留意が必要である。

3. オンラインでの顧客の本人確認用アイデンティティの保証レベルとその評価

3.1. 保証レベルの定義

2.2.2 節で述べたように、オンラインで取引時に顧客の本人確認をする場合、本人の属性を対象に評価を行う。その際、確認に用いる属性の種類、確認方法、確認結果等に応じて、本人であることが、どの程度確からしいか、を判断することになる。この確からしさの程度のことを「保証レベル」と定義する。換言すれば、「保証レベル」とは、アイデンティティを構成する属性やその証拠に応じて、アイデンティティの確実さの度合を示す指標のことを意味する。

ISO 5158 では、アイデンティティに対して、以下の 5 つの評価軸を設定しており、「保証レベル」は評価軸に対応する成分を含む 5 次元以上のベクトルとして表現できる。なお、ベクトルの各成分は 0 以上 1 以下の値をとる[12]。なお、ISO 5158 では、評価軸は 5 つに限られることを意味するものではない、とも付言している。

---

[11] 例えば、日本のパスポートが発行開始以降 11 回（戦後以降でも 7 回）変更されていることからもわかるように（https://www.mofa.go.jp/mofaj/files/000432934.pdf）、世界各国でパスポートの仕様変更は散発的に行われている。そのため、全ての変更を把握するためには相応にコストがかかる。また、日本の運転免許証の場合は、2007 年から IC カード対応された際、全国一斉ではなく約 3 年をかけて、都道府県別に段階的に導入が進められ改訂されたが、こうした段階的導入が行われる場合も正当性確認のためのコストを要する傾向がある。また、現在も、運転免許証は、各都道府県の公安委員会毎に発行されており、印刷される公安委員会の公印やフォント、氏名欄では氏名の始まる位置や文字間の空白の数等、記載事項に違いがある。変更される度にこうした違いをすべて把握するには相応にコストがかかる作業となっている。

[12] ISO 5158 では、ベクトルの各成分の値は、0 以上 1 以下の範囲であることが推奨されているが、モバイル金融サービス事業者のニーズに応じて異なる値域をとることもできるとしている。

モバイル金融サービス提供者の顧客xのアイデンティティの保証レベル（$\overrightarrow{AL\_IDx}$）：

$$\overrightarrow{AL\_IDx} = (AL\_U, AL\_E, AL\_P, AL\_W, AL\_R, \dots)$$

ベクトルの成分（評価軸）：

① AL_U：アイデンティティの一意性
② AL_E：アイデンティティと実在人物との対応
③ AL_P：提示された属性が顧客本人と一致する度合い
④ AL_W：サービスに申し込む意思
⑤ AL_R：顧客への連絡可能性

一般的に、サービス内容のほか、各国のマネー・ローンダリング対策（AML）などの規制等要件、あるいは、顧客本人であることの確からしさをより高めたいビジネスニーズなどに応じて調整し、評価軸数を追加することが考えられよう。また、特定の顧客について、時間の経過等に応じて評価軸数を増減させることも考えられる。

モバイル金融サービスでの顧客の本人確認の結果判定

モバイル金融サービス提供者が、顧客のアイデンティティをもって、顧客本人だと確認するにあたっては、保証レベル（$\overrightarrow{AL\_IDx}$）の各成分の値が、そのモバイル金融サービス提供者があらかじめ定めた閾値を超えるかどうかで判断する。なお、ベクトルではなく、その大きさ、すなわち単純なスコア値（スカラー）を計算する必要がある場合は、各次元の重み付けを定義し、合計値を求める方法も考えられる。

なお、ISO 5158 では、具体的な閾値の値やスコア値の計算方法は、特段定めていない。モバイル金融サービス提供者は、提供するサービスの内容に応じて求める保証レベル（$\overrightarrow{AL\_IDx}$）の値を設定することが考えられる（事例を 4.1.節にて紹介する）。逆に、顧客の本人確認の結果得られた保証レベル（$\overrightarrow{AL\_IDx}$）の値に応じて、顧客ごとに異なるサービスを提供する運用も考えられる。

3.2. 保証レベルの評価基準

以下では、ISO 5158 が示すそれぞれの保証レベルの要素について、その評価基準を簡単に示す（詳細は ISO 5158 本書をご確認いただきたい）。

3.2.1. 顧客のアイデンティティの一意性（AL_U）の評価基準

AL_Uは、モバイル金融サービス提供者が、顧客のアイデンティティを一意に特定できる度合いを示す値である。具体的な評価基準は、表２のとおりである。

表２：アイデンティティの一意性（AL_U）

AL_U値	状況	評価の基準
0	顧客を一意に特定できる保証がない	顧客は、登録やログインしなくてよい。
0 を超え 1 未満	顧客を一意に特定できるかが不明確	サービスの提供に際して、顧客は、名前や位置など、一部の属性情報を提供している。
1	顧客を確実に一意に特定できる	サービスの提供に際して、顧客は、固有の属性（国民 ID 番号や生体情報など）、あるいは、複数の属性情報の組み合わせによって個人の特定が可能な情報を提供している。

出典：ISO 5158:2022 Table1 を参考に筆者作成

3.2.2. アイデンティティと実在人物との対応（AL_E）の評価基準

AL_Eは、アイデンティティが正しい実在人物であることの証拠（身分証明書や写真画像等）の厳密さや強度を示す値である。顧客が提示する証拠の正確性（AL_E）の具体的な評価基準は、表３のとおりである。なお、評価の基準にある ISO/IEC TS 29003[13]の LoIP（Levels of Identity Proofing）ついては後段 BOX（２）を、NIST（National Institute of Standards and Technology、米国立標準技術研究所）の IAL（Identity Assurance Level）ついては 4.2.2.節を参照のこと。

表３：アイデンティティと実在人物との対応（AL_E）

AL_E値	状況	評価の基準
0	信頼できない証拠	証拠が無効、 または、 証拠の発行者が、提供者の KYC 方針に合致していない、もしくは、 LoIP1(ISO/IEC TS 29003)、IAL1(NIST)と同等である。
0 を超え 0.9 未満	部分的には信頼できる証拠	証拠の発行者が、 (a)①提供者の KYC 方針に合致している、または、②LoIP2/3 (ISO/IEC TS 29003)、IAL2/3(NIST)と同等、 かつ、 (b)①リモートで検証可能な物的証拠の偽造防止策、または、②デジタルエビデンスの真正性・完全性を検証可能なデジタル署名などのセキュリティ手段を提供している。

[13] ISO/IEC で始める規格は、ISO と IEC（International Electrotechnical Commission、国際電気標準会議）とが、共管しているものである。

0.9 以上 1 未満 （注）	本物で有効な証拠	証拠の発行者が、 (a)①提供者の KYC 方針に合致している、または、②LoIP2/3 (ISO/IEC TS 29003)、IAL2/3(NIST)と同等、 かつ、 (b)①デジタルエビデンスやアイデンティティ情報プロバイダー（IIP）からの情報が提供され、②デジタル署名やセキュアな通信プロトコルなどのセキュリティ手段で保護され、③失効チェックメカニズムで真正性・有効性も検証される 。

注：100%の信頼性を保証する術はないため 1 にはならない（以下、3.2.3.、3.2.4.、3.2.5.も同様）。

出典：ISO 5158:2022 Table2 を参考に筆者作成

AL_Eの値を決めるに当たって行う評価は顧客の属性ごとに行う。ある属性に対する証拠が複数ある場合は、①証拠の中で最も評価値が高いものをその属性の評価値とする方法と、②証拠ごとに重みづけをしてその属性の評価値を算出する方法が考えられる。その上で、顧客の本人確認の全体の保証レベルAL_Eとしては、保守的に考え、複数の属性の評価値のうち、最も値が小さい属性の評価値とすることが考えられる。

3.2.3. 提示された属性が顧客本人と一致する度合い（AL_P）の評価基準

AL_Pは、提示された属性や証拠が顧客本人のものと一致する度合い示す値である。この値は、認証プロセスにおける認証強度の違いとなって現れる。属性や証拠が顧客本人のものであることの保証レベル（AL_P）の具体的な基準は、表４のとおりである。

表４：提示される属性が顧客本人と一致する度合い（AL_P）

AL_P値	状況	評価の基準
0 を超え 0.1 未満	申請者が登録顧客である可能性は低い。	①知識ベース認証（例：支払履歴）、もしくは、②登録生体情報へのリスク等の管理策がない生体認証。
0.1 以上 0.9 未満	申請者が登録顧客であることをある程度保証。	リスク管理措置（例：支払履歴の場合は、申請の場所、操作習慣等の確認）を実施した知識ベース認証、登録生体情報への一定のリスク等の管理策を実施した生体認証。
0.9 以上 1 未満	申請者が登録顧客である確度が高い。	対面での確認と同等の方法（例：登録生体情報への十分なリスク等の管理策を実施した生体認証）。

出典：ISO 5158:2022 Table3 を参考に筆者作成

属性や証拠が顧客本人のものであることを確認する方法

一般に、属性や証拠が顧客本人のものであることを確認する方法は以下の 3 つある。

- 知識認証（例：支払履歴、パスワード）。
- 所持品認証（例：店舗等の物理的な場において、顧客が ATM などの機械や従業員に、ID カードや登録済みのモバイル端末などを提示して行う認証）。

- 生体認証。

この 3 つの認証方法のうち、eKYC において当人認証を行う方法としては生体認証が最もよく使われる。生体認証には、指紋、顔、虹彩、静脈パターン等、物理的な生体物を用いた認証である物理的生体認証（biophysical biometrics）や、画面タッチの圧力やキーボード入力時のくせ等、筋肉・骨格・神経システム等の違いから生じる個人の「行動のくせ」を利用した認証である生物力学的生体認証（biomechanical biometrics）などいくつかの方法がある。ここでは、主に物理的生体認証を想定して議論を進める。

生体認証の保証レベルは、大きく分けて、以下 2 点によって差が生じることになる。

- 生体情報自体の品質。
- セキュリティやリスク管理状況：例えば、①実装する生体認証手法のリスクの把握、②提示攻撃（プレゼンテーション・アタック）[14]の検知機能（詳細は ISO/IEC 30107<バイオメトリクスの提示攻撃検知>を参照）、③実装する生体認証手法の「誤受入率（FAR：False Acceptance Rate）」および「誤拒否率（FRR：False Rejection Rate）」など。

ISO 5158 では、生体認証の保証レベルの評価を行う際は、生体認証システムのセキュリティ評価には ISO/IEC 19792 を、生体認証システムの性能評価には ISO/IEC 19795 を、生体認証に対する攻撃対策には ISO 19092 を参考しつつ行うことが考えられることを指摘している（各引用規格の概要は後段 BOX （３）を参照）。

なお、昨今、知識認証・所持品認証・生体認証の 3 つの認証方式以外にも、モバイル端末等に搭載されたセンサーで捉えた顧客の生活習慣のパターン情報を使って個人を認証するライフスタイル認証といった、新たな認証方式も提案されている。GPS 情報のほか Wi-Fi や携帯電話の基地局情報から、モバイル端末の位置と時刻を日々蓄積すると、利用者の行動履歴を把握できる。例えば、通勤・通学者の場合、定期的にほぼ同時刻に出発し、同一交通手段で、同一の目的地に行くことから、位置情報に普段の行動パターンが現れる。また、アプリの利用状況のデータを日々蓄積し認証に活用することも考えられる。例えば、電車通勤者の場合、毎日ほぼ同時刻の通勤時に、同じアプリを同じ時間使うというパターンが現れやすい。こうした日常生活での行動パターンと端末の挙動が一致

[14] 人工物等を用いて生体特徴を偽造するなど、何らかの情報をセンサーに提示してなりすましを試みる攻撃のこと。詳細は、例えば、宇根正志「生体認証システムにおける人工物を用いた攻撃に対するセキュリティ評価手法の確立に向けて」、金融研究 第 35 巻第 4 号、2016 年、https://www.imes.boj.or.jp/research/abstracts/japanese/kk35-4-3.html 参照。

しているかどうかを、認証に活用することが可能となっており[15]、認証方式自体も今後の技術の進展が予想される分野となっている。

3.2.4. サービスに申し込む意思（AL_W）の評価基準

AL_Wは、モバイル金融サービス提供者が、サービスに申し込む顧客の意思や意図の確認度合いを示す値である。評価基準は、表５のとおりである。

表５：サービスに申し込む意思（AL_W）

AL_W値	状況	評価の基準
0 を超え 0.1 未満	申請者の意思を黙示的に確認。	取引条件の確認(チェックボックス等へのチェック)。
0.1 以上 0.5 未満	申請者の意思を明示的に確認。	明示的な記載による確認。
0.5 以上 0.9 未満	申請者とリアルタイムで会話し意思を確認。	遠隔ビデオ対話での個別の質問による確認。
0.9 以上 1 未満	物理的な確認。	窓口や訪問などで個別の質問を伴う物理的な確認。

出典：ISO 5158:2022 Table4 を参考に筆者作成

3.2.5. 顧客への連絡可能性（AL_R）の評価基準

AL_Rは、モバイル金融サービス提供者が、顧客と必要なときに確実に連絡が取れる情報を取得している度合いを示す値である。顧客の本人確認に関する全体的なリスク管理のために必要な情報である。評価基準は、表６のとおりである。

表６：顧客への連絡可能性（AL_R）

AL_R値	状況	評価の基準
0	保証なし	物理的な住所、電話番号、電子メール、その他連絡先情報が未確認。
0 を超え 0.9 未満	オンラインでの保証	①顧客が連絡先情報を提示し、電話をかける、メールや携帯電話のワンタイムパスワードなどの手段で確認できる。②物理的な住所が身元証明書と照合できる。
0.9 以上 1 未満	対面での保証	①顧客が物理的な住所を提示し、郵便などの手段で事実が確認できる。②従業員が顧客を直接訪問し確認できる。

出典：ISO 5158:2022 Table5 を参考に筆者作成

[15] 詳細は、例えば、橋本崇、「スマートフォン等での決済サービス業務にかかるリスクマネジメント：本人認証のあり方に注目して」、金融研究 第 40 巻第 2 号、2021 年、https://www.imes.boj.or.jp/research/abstracts/japanese/kk40-2-3.html 参照。

4. オンライン本人確認用アイデンティティの保証レベルの各国での適用

4.1. ISO 5158 の適用事例

次に、サービス内容に応じた顧客の本人確認の方法を検討したい。顧客の本人確認の保証レベルを向上すれば向上するほど、精度は向上するものの、利用者の手間の増加やサービス提供業者のシステム投資等、様々なコストが上昇する。そのため、提供するサービスの内容に応じた顧客の本人確認の保証レベルの適切な設定が必要となる。

上記にて議論した保証レベルの（$\overrightarrow{AL\_IDx}$）の値を活用し、顧客の本人確認のレベルに応じたサービスを提供している事例として、中国とマレーシアの例を ISO 5158 の記載内容に沿って以下に紹介する[16]。

4.1.1. 中国の金融機関口座

中国の金融機関の口座には、顧客の本人確認の要件に応じて以下の 3 つの分類があり、それぞれの分類が満たす $\overrightarrow{AL\_IDx}$ の成分の値は表 7 のようになる。

表 7 ：中国の金融機関の口座における顧客の本人確認の要件と保証レベル

分類	KYC 要件	提供サービス	$\overrightarrow{AL_IDx}$の成分値での要件表記例
I 類	対面での確認。	入金、出金、投資、送金、購入物の決済、請求書支払に利用可能。 口座残高や取引額に制限はない。	$AL\_U = 1$ $AL\_E \geqq 0.9$ $AL\_P \geqq 0.9$ $AL\_W \geqq 0.9$ $AL\_R \geqq 0$
II 類	遠隔での確認可。同一の名前の I 類銀行口座が必要。 生体認証の利用を推奨。	入金、投資、購入物の決済、請求書支払に利用可能。 口座からの支払いは 1 日 10,000 元までの制限有。	$AL\_U = 1$ $AL\_E \geqq 0.9$ $AL\_P \geqq 0.1$ $AL\_W \geqq 0.1$ $AL\_R \geqq 0$
III 類	遠隔での確認可。同一の名前の I 類銀行口座が必要。 生体認証利用を推奨。	購入物の決済、請求書支払いに利用可能。 口座残高が 1,000 元未満の制限有。	$AL\_U = 1$ $AL\_E \geqq 0.9$ $AL\_P \geqq 0.1$ $AL\_W \geqq 0.1$ $AL\_R \geqq 0$

注：II 類と III 類は、顧客が選択することによって分類が異なる。

出典：ISO 5158 Table B.1、Table B.2、および、白木 幹二「中国における個人預金口座開設の規制強化について」[17]、宋 良也「中国のネット専業銀行への取り組み－『百信銀行』について」[18]を参考に筆者作成

[16] ISO 5158 では、保証レベル $\overrightarrow{AL\_IDx}$ との関係性については整理されていないが、顧客の本人確認の基準に関して、インド（Aadhaar）、シンガポール、スウェーデンの事例にも言及がある。また、日本の犯収法にかかる記述もある。

[17] https://www.ncbank.co.jp/hojin/asia_information/chuzaiin_news/pdf_files/shanghai_201707.pdf

[18] http://www.nicmr.com/nicmr/report/repo/2016/2016spr16web.pdf

4.1.2. マレーシアの決済サービス事業者

マレーシアのペイメントアカウント（銀行以外の決済サービス事業者が提供する主に支払いを目的として使用するアカウント）の場合は、顧客確認（CDD：Customer Due Diligence）の状況に応じて 2 つの分類があり、以下の表 8 のように表記できる。

表 8 ：マレーシアのペイメントアカウントにおける顧客の本人確認の要件と保証レベル

分類	KYC 要件	提供サービス	$\overrightarrow{AL_IDx}$の成分値での要件表記例
Non-CDD	必要なし	最大残高:5,000MYR 1 回の取引上限:3,000MYR 購入物の決済のみ利用可（現金化は不可）	$AL\_U \geqq 0$ $AL\_E \geqq 0$ $AL\_P \geqq 0$ $AL\_W \geqq 0$ $AL\_R \geqq 0$
CDD	承認済身分証明書の提示と、氏名・識別番号・国籍・住所・携帯電話番号・誕生日・取引目的の情報提供	•送金可能 •為替取引可能 •現金化可能 ウォレット内の金額に上限あり （上限値は事業者が設定）	$AL\_U = 1$ $AL\_E > 0$ $AL\_P \geqq 0$ $AL\_W \geqq 0$ $AL\_R > 0$

出典：ISO 5158　TableB.3、TableB.4 および STICPAY「海外送金ポリシー：マレーシア」[19]を参考に筆者作成

4.2. 評価方法に関する議論

eKYC における保証レベルの評価方法に関する議論は、世界中で様々な形で行われている。本稿では、日本、米国、欧州（eIDAS）の事例を紹介する。

なお、ISO 5158 はアイデンティティの保証レベルを定めているが、以下に示す日本、米国、欧州の事例は、本人確認の保証レベルについて議論している。もっとも、eKYC は、アイデンティティを確認することであるため、オンライン上で本人確認を行う場合、アイデンティティの保証レベルと本人確認の保証レベルとは実質的には同じになるが、見方が異なっている点には留意が必要である。

4.2.1. 日本

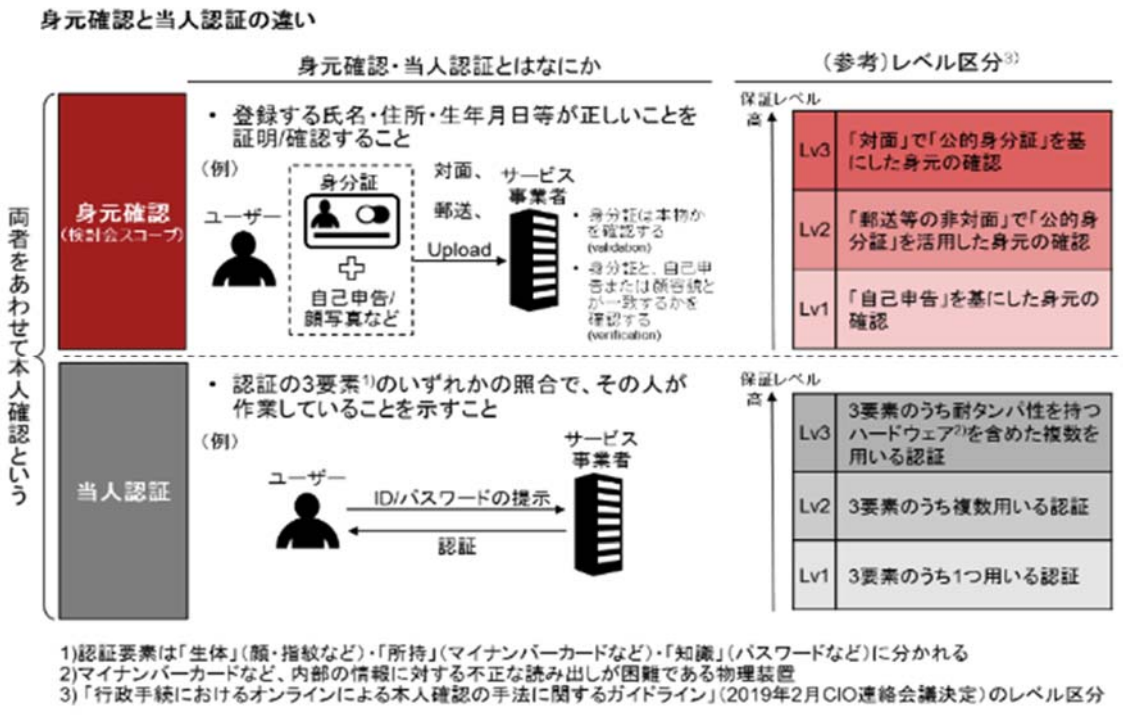
ISO 5158 には、犯収法の内容を基にした、現在日本で実施されている KYC 手法にかかる記述がある。なお、保証レベル $\overrightarrow{AL\_IDx}$ による分類はされていない。

サービス提供者が、顧客に対して、本人確認の程度に応じて、異なるサービスを提供す

[19] https://www.sticpay.com/ja-JP/news/news_detail/international-money-transfer-policy-malaysia

ることは広く行われている。このために本人確認の評価軸を設けて、確認の程度を保証レベルに分類する手法が、これまで政府の検討会等、さまざまな形で検討が進められてきた。例えば、2020 年 4 月に公表された経済産業省の「オンラインサービスにおける身元確認手法の整理に関する検討報告書[20]」では、a)身元確認と b)当人認証という 2 つの評価軸に、それぞれ 3 段階の保証レベル区分を設ける形で設定している（図 9 参照）。身元確認とは、利用者が提示した証拠（例えば運転免許証）を基に、そこに書かれた属性情報（例えば、名前や住所、生年月日の情報）が実在することを確認する行為のことであり、上記 3.2.2.節の「アイデンティティと実在人物との対応（AL_E）」に 3.2.5.節の「顧客への連絡可能性（AL_R）」の評価軸を合わせた評価軸と考えられる。当人認証とは、認証の 3 要素（知識認証・所持品認証・生体認証を言う、詳細は 3.2.3.節参照）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であり、3.2.3.節の「提示された属性が顧客本人と一致する度合い（AL_P）」と同等の評価軸と考えられる。

図 9 ：日本における本人確認の評価とその保証レベル



出典：経済産業省「オンラインサービスにおける身元確認手法の整理に関する検討報告書」（概要版）[21]

[20] https://www.meti.go.jp/press/2020/04/20200417002/20200417002.html

[21] https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf

その後、デジタル庁の「トラストを確保した DX 推進サブワーキンググループ」の第４回（2022 年 1 月 25 日開催）では、独立行政法人情報処理推進機構（IPA）デジタルアーキテクチャ・デザインセンター（DADC）が、デジタル本人確認の保証レベルについて、身元確認と当人認証の保証レベルをマトリクスとして表現し、レベル分けの整理を行ったうえで、本人確認手法を定めた日本の法令等をあてはめた整理を行っている（表 10 参照）[22]。

表 10：身元確認と当人認証の保証レベル

b)当人認証レベル / a)身元確認レベル	レベル１ 知識・所持品・生体の３要素のうち１つの認証要素を活用	レベル２ ３要素のうち複数の認証要素を活用	レベル３ 耐タンパ性[23]が確保されたハードウェアトークンの活用
レベル３ 対面での身元確認			レベル A
レベル２ 遠隔又は対面での身元確認		レベル B	
レベル１ 身元確認のない自己表明	レベル C		

注：レベル１，２，３の区分は ISO 5158 での区分とは必ずしも一致しない。

出典：肥後 彰秀、「サービスに応じたデジタル本人確認ガイドラインの検討」[24]

この身元確認と当人認証の評価事務に沿って評価レベル分けしたものを、本人確認手法を定める現行の法令およびサービス等を当てはめた場合の例について、以下の表 11、表 12 のように整理されている。

[22] 「トラストを確保した DX 推進サブワーキンググループ」の第4回の資料、議事概要は、https://www.digital.go.jp/councils/trust-dx-sub-wg/GLvad6b1/参照。

[23] 耐タンパ性とは、機器や装置、ソフトウェアなどが、外部から内部構造や記録されたデータなどを解析、読み取り、改ざんされにくくなっている状態のこと。6.3.節にあるよう、モバイル端末のセキュア・エレメント（SE）は耐タンパ性を持っている箇所である。

[24] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/093e09a7-2ffe-4a41-971a-5c0dcfd3c0b3/20220125_meeting_trust_dx_02.pdf

表 11：法令等が定める本人確認手法を上記マトリクスにマッピングした例[25]

a)当人認証 b)身元確認	レベル 1 3 要素のうち 1 つの認証要素を活用	レベル 2 3 要素のうち複数の認証要素を活用	レベル 3 耐タンパ性が確保されたハードウェアトークンの活用
レベル 3 対面での身元確認			・犯収法ワ (犯収法規則 6 条 1 項 1 号) ・公的個人認証
レベル 2 遠隔又は対面での身元確認	・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (犯収法規則 6 条 1 項 1 号) ・口座連携(犯収令 13 条 1 項 1 号)	・公的身分証以外の身分証のアップロード ・公的身分証のアップロード ・犯収法ホ (施行規則 6 条 1 項 1 号) ・口座連携(犯収施行令 13 条 1 項 1 号)(※1) ・身元確認の API 連携(銀行 API/キャリア API)(※1) ・犯収法ヘ (犯収法規則 6 条 1 項 1 号) ・犯収法ヲ (犯収法規則 6 条 1 項 1 号)	・犯収法ヘ (犯収法規則 6 条 1 項 1 号) ・犯収法ヲ (犯収法規則 6 条 1 項 1 号) ・身元確認の API 連携(キャリア API)(SIM 利用) (※1)
レベル 1 自己表明	・身分証に基づかない自己申告での登録	・身分証に基づかない自己申告での登録	

※1 アカウント作成後は身分証不要

出典：肥後 彰秀、「サービスに応じたデジタル本人確認ガイドラインの検討」

[25] 犯収法のホヘヲワ（犯収法規則 6 条 1 項 1 号）とは、犯罪による収益の移転防止に関する法律施行規則第 6 条第 1 項第 1 号にそれぞれ定められている本人確認方法である。具体的には以下の通り。

ホ 顧客等から、事業者が提供するソフトウェアを使用して、本人確認用画像情報の送信を受ける方法

ヘ 顧客等から、事業者が提供するソフトウェアを使用して、本人確認用画像情報の送信を受けるとともに、顧客等から当該顧客等の写真付き本人確認書類に組み込まれたモバイル端末等に記録された情報の送信を受ける方法

ヲ 顧客等から、認定業者が発行し、かつ、その認定に係る業務の用に供する電子証明書や電子署名が行われた特定取引等に関する情報の送信を受ける方法

ワ 顧客等から、マイナンバーカードの署名用電子証明書や電子署名が行われた特定取引等に関する情報の送信を受ける方法

また、犯収施行令 13 条 1 項 1 号とは、犯罪による収益の移転防止に関する法律施行令第 13 条第 1 項第 1 号に定める、既に確認を行っている顧客等との取引に準ずる取引のことを指す。

表 12：日本のサービスについて、本人確認手法を上記マトリクスにマッピングした例

a)当人認証 b)身元確認	レベル 1 3 要素のうち 1 つの認証要素を活用	レベル 2 3 要素のうち複数の認証要素を活用	レベル 3 耐タンパ性が確保されたハードウェアトークンの活用
レベル 3 対面での身元確認		・古物商 A (※1) ・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・シェアリングエコノミーA 社 (※2)	・犯収法の特定事業者 ・携帯電話事業者(※1) ・電子サイン A (※1)
レベル 2 遠隔又は対面での身元確認	・マッチングアプリ ・シェアリングエコノミーB 社	・犯収法の特定事業者 (※1) ・携帯電話事業者 (※1) ・古物商 B (※1) ・シェアリングエコノミーB 社 (※2) ・マッチングアプリ (※3) ・たばこ会員登録 (※3) ・公営ギャンブル (※3) ・eMAFF プライム (オンライン本人確認) ・gBiz プライム (郵送) ・引越し	・電子サイン A (※1) ・口座開設 (ネット完結) (※2) ・たばこ会員登録 (※3) ・公営ギャンブル (※3)
レベル 1 自己表明	・gBiz・eMAFF (エントリー) ・電子サイン C (※1)	・電子サイン B (※1)	

※1 法令に基づく、※2 自主的取組、※3 自主的取組 (年齢確認のみ)
注：gBiz：行政サービスの共通認証システム、eMAFF：農林水産省共通申請サービス

出典：肥後 彰秀、「サービスに応じたデジタル本人確認ガイドラインの検討」

こうした下、「トラストを確保した DX 推進サブワーキンググループ」は 2022 年 7 月、報告書を取りまとめた。その中では、行政手続を中心に、日本の実情に応じた整理が行われている。具体的には、「身元確認の保証レベル（IAL：Identity Assurance Level）」と「当人認証の保証レベル（AAL：Authenticator Assurance Level）」の 2 つの軸に対し、 3～4 つのレベルに分けて、保証レベルが定義されている（表 13 参照）。

表 13：日本のデジタル庁が行った保証レベルにかかる整理

（IAL におけるユースケースのマッピング）

IAL	証拠（エビデンス）	本人確認方法	ユースケース
IAL-3	信頼できる機関により電子的対面で確認に身元証明可能なもの	対面で確認	マイナンバーカードを使用した対面での申込み
		非対面	マイナンバーカードを用いた電子著名
	発行元保証されている身元証明可能なもの	対面での有資格者による確認	マイナンバーカードの発行
		対面相当オンライン(eKYC)	オンラインでの身元証明書上の本人写真とリアルタイム本人画像のマッチング
	⋮	⋮	⋮
	発行元保証されている身元証明可能なもの	オンライン登録後対面で確認	オンラインでの銀行口座開設→カード受け取り時本人確認
IAL-2	信頼できる機関により電子的に身元証明可能なもの	非対面で確認	オンラインでのマイナンバーカードリーダーを用いた口座開設
	発行元保証されている身元証明可能なもの	非対面で確認	オンラインでの本人確認書類（画像アップロード等）を用いた EC サイト会員登録
IAL-1	身元確認のない自己表明可能なもの	身元確認なし	サービス登録時におけるメールアドレスでの通達確認

※対面には「リモートでの対面(supervised remote)」も含む

（AAL とユースケースのマッピング案）

	認証プロセス	ユースケース
AAL-3	AAL-2 に加えて、認証取得済みのハードウェアベースのなりすまし性耐を持つ認証子の利用が必須。	マイナポータル：マイナンバーカードの利用者証明用電子証明書利用のユーザ認証によるログイン
		e-Tax: IC カード方式・リモート署名利用による申告
		ビジネスバンキング：FIDO Security Certification L3 を取得したセキュリティキーを利用した二要素認証を使った大金の送金
AAL-2	多要素認証、認証取得済みの暗号化手法の利用が必須。なりすまし耐性を持つ認証子の利用が推奨。	e-Tax: Smart ID 方式・リモート署名利用による申告
		ネット証券：ユーザ名＋パスワード＋ソフトウェアトークンを使った認証取得済みの暗号化手法によるワンタイムパスワードによる認証を使った振込先銀行の変更
	⋮	⋮
AAL-1	一要素認証	ネット証券：ユーザ名・パスワードによるログイン
		ビジネスチャットーサピス：AAL-1 のメールアドレスへのリンク送信とそのリンクを踏むことによるユーザ認証
AAL-0	認証なし	e コマース：新規 Cookie による穀客の新規カート維持

出典：デジタル庁、「トラストを確保した DX 推進サブワーキンググループ報告書」[26]

4.2.2. 米国

米国では、2017 年 6 月、NIST（米国立標準技術研究所）が認証に関するガイドライン「Electronic Authentication Guideline（電子的認証に関するガイドライン）」第 3 版

[26] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/658916e5-76ce-4d02-9377-1273577ffc88/1d463bfc/20220729_meeting_trust_dx_report_01.pdf

（NIST SP 800-63-3）を発表した[27]。NIST SP 800-63 は、アメリカ政府機関がオンラインで本人確認を行うシステムを構築する際の実装ガイドラインであるが、クレジットカードにおける PCI-DSS や金融情報システムセンター（FISC）の安全対策指針など、各種のガイドラインにも数多く引用されている。なお、2020 年 6 月には、改訂作業を検討していることが公表され、2022 年 12 月にはこの改正版（NIST SP 800-63-4）のドラフトが公表されている[28]。

NIST SP 800-63-3 では、評価軸として、ユーザの身元確認、ユーザの当人認証、連携方法の 3 つの軸を設定し、それぞれ 3 段階の保証レベルを設定し、評価を行っている（表 14 参照）。このうち、ユーザの身元確認（IAL）は、3.2.2.節で前述した通り、ISO 5158 の顧客が提示する証拠の正確性（AL_E）の評価基準に引用されている。

表 14：NIST SP 800-63-3 におけるデジタル本人確認の評価軸と保証レベル

身元確認の保証レベル	Identity Assurance Level（IAL）（SP 800-63A）	ユーザが申請者（Applicant）として新規登録（SignUp）する際に、CSP（Credential Service Provider）が行う本人確認（Identity Proofing）の厳密さ、強度を示す	Lv.1	本人確認不要、自己申告での登録でよい
			Lv.2	サービス内容により識別に用いられる属性をリモートまたは対面で確認する必要あり
			Lv.3	識別に用いられる属性を対面で確認する必要があり、確認書類の検証担当者は有資格者
当人認証の保証レベル	Authenticator Assurance Level（AAL）（SP 800-63B）	登録済みユーザー（Claimant）がログインする際の認証プロセス（単要素認証 or 多要素認証、認証手段）の強度を示す。	Lv.1	単要素認証で良い
			Lv.2	2 要素認証が必要、2 要素目の認証手段はソフトウェアベースのもので良い
			Lv.3	2 要素認証が必要、かつ 2 要素目の認証手段はハードウェアを用いたもの（ハードウェアトークン等）
連携方法の保証レベル	Federation Assurance Level（FAL）（SP 800-63C）	ID トークンや SAML Assertion 等、Assertion のフォーマットやデータやり取りの仕方の強度を示す	Lv.1	アサーション（RP（Relying Party:アプリやサービスの提供者）に送る IdP（Identity Provider: Id のプロバイダー）での認証結果データ）への署名
			Lv.2	署名に加え、対象 RP のみが復号可能な暗号化
			Lv.3	Lv.2 に加え、Holder-of-Key Assertion の利用（ユーザごとの鍵と IdP が発行した Assertion を紐づけて RP に送り、RP はユーザがその Assertion に紐づいた鍵を持っているか（ユーザの正当性）を確認）

出典：JIPDEC「NIST SP 800-63-3 の概要と今回の改訂がもたらす影響」[29]を参考に NIST SP 800-63-3 を参照しながら筆者作成

[27] https://pages.nist.gov/800-63-3/sp800-63-3.html

[28] https://csrc.nist.gov/publications/detail/sp/800-63/4/draft

[29] https://www.jipdec.or.jp/library/report/20171127.html

4.2.3. 欧州

欧州では、2014 年、EU 域内で健全な電子取引ができるよう eIDAS と呼ばれる規則を制定し、2016 年に施行された。具体的には、eIDAS では、電子取引に紙文書と同等の法的効力を与える電子本人認証（eID）、電子署名、タイムスタンプ、e シール、その他の認証証明に関する規則が制定されている。eIDAS も改訂が検討されており、2021 年には eIDAS2.0 として改訂案が欧州委員会で採択され、意見公募が行われている。

eIDAS の下では、電子識別(eID)スキームに関し、3 つの保証レベルに従って分類されている（表 15 参照）。

表 15：eIDAS 規則における保証レベル

保証レベル	概要	具体例
Low	• 個人の身元に対して限定された程度の信頼度を提供。アイデンティティの誤用又は改ざんリスクを減らすことを目的。 • eIDAS 仕様外の簡易なトラストサービス • トラストサービスプロバイダによって提供。事後監査が必要	• サービスへの入会を、本人がウェブページを通じてセルフで行うケース。 • 本人性確認等は実施しない。
Sub-stantial	• 個人の身元に対して Substantial（重要）という保証レベルを備えた高い信頼度の電子識別手段。 • アイデンティティの誤用又は改ざん防止を目的したもの。 • 仕様に幅がある	• サービスへの入会において、個人のアイデンティティ情報の提示が必須とするケース。 • サービス利用時に、ユーザ ID／パスワード認証、および多要素認証（SMS へのワンタイムパスワード送付等）を必要とする。
High	• 厳密に守るべき要件やポリシーが定められている • 適格トラストサービスプロバイダによって提供。定期的な監査が必要 • 個人の身元に対して Substantial レベルの信頼度を提供。アイデンティティの誤用又は改ざんのリスクを大幅に減らすことを目的	• サービスへの入会において、有人・対面による本人確認を必須とするケース。サービス利用時の認証は、国民 ID カード等スマートカードの利用を必要とする。

出典：デジタル庁「トラストを確保した DX 推進 SWG（第４回）事務局説明資料」[30]

5. オンライン本人確認とプライバシー保護

ここまで、「保証レベル」という考え方を用いたオンラインでの顧客の本人確認方法と、その運用事例について検討してきた。オンラインでの顧客の本人確認プロセスでは、モバイル金融サービス事業者が、顧客の一部の属性をあらかじめデジタル空間上に保有

[30] https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/093e09a7-2ffe-4a41-971a-5c0dcfd3c0b3/20220125_meeting_trust_dx_01.pdf

しておき、実際に本人確認を行う際には、顧客から提示された属性と、デジタル空間上にある属性の情報を照合する。その照合の際には、顧客の属性である個人情報を扱うことになる。そのため、個人情報の保護やセキュリティに配慮する必要が生じる。こうした観点を踏まえ、ISO 5158 では、一つの節を設けて、関連する規定を参照する形でセキュリティとプライバシー保護について論じている。

個人情報保護に関しては、諸外国でも様々な議論が進展している。また、時代の要請もあり、ISO においても規格が網羅的に整備されつつあり、ISO 5158 でもこうした他の ISO 規格を参照している。本稿では、以下、オンラインでの顧客の本人確認におけるプライバシー保護の論点を整理する。

5.1. ISO 規格におけるプライバシー保護

5.1.1. ISO 5158 が参照するプライバシー・フレームワーク規格

個人情報である属性情報は、収集状況とサービス提供時に行う処理の状況に応じた対応が実施されていることを保証する必要がある。そのため、ISO 5158 では、個人情報の扱いには、全面的に ISO/IEC 29100（プライバシー・フレームワーク）が掲げる原則に従うべきであるとしている。この ISO/IEC 29100 は、個人識別可能情報[31]の処理作業における関係者を整理し、役割を定義しているほか、情報のセキュリティ対策要件を規定し、概念レベルのプライバシー保護の枠組みを示した国際標準であり、既知のプライバシー保護例を提示している（後段 BOX （４）①を参照）。

5.1.2. 具体化したプライバシー保護に関する ISO 規格

プライバシー保護に関しては、ISO/IEC 29100 を基に、それを具体化する形で多くの ISO 規格が起案されている（図 16 参照）。

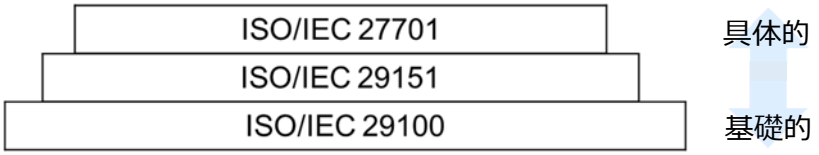
例えば、ISO/IEC 27701 は、プライバシー情報マネジメントシステム（PIMS）について書かれた国際標準である。同規格は、情報セキュリティマネジメントシステム（ISMS）、具体的には ISO/IEC 27001 および ISO/IEC 27002 のアドオン（拡張）規格として位置づけられているものとなっており、情報セキュリティマネジメントシステムの要求事項に加え、個人識別可能情報を処理する際に影響を受ける可能性のあるプラ

[31] 本稿 2.1 節で定義した「属性」との関係で言えば、モバイル金融サービス提供者が顧客の本人確認を行った結果、顧客であると判定した際に用いた属性の組み合わせが、個人識別可能情報と言える。

イバシーを保護するための要求事項およびガイドラインを規定している。この ISO/IEC 27701 は、フレームワークとしての抽象度の高い ISO/IEC 29100 を、より組織内のルール作りに参照しやすい形で提示しているものとなっている（後段 BOX （４）②を参照）。

ISO/IEC 29151（個人識別可能情報保護のための行動規範）は、個人情報保護に関連するリスクおよび影響評価によって特定された要件を満たすために、統制を実施する際の統制目標、統制方法およびガイドラインを規定している。この規格も、ISO/IEC 27002 に基づくガイドラインを規定しており、ISO/IEC 27701 の基礎になっている文書でもある。

図 16：プライバシー・フレームワークに関連する ISO 規格の関係



出典：筆者作成

5.1.3.プライバシー影響評価に関する ISO 規格

個人情報を取り扱う情報システムの導入や改修に際して生じる個人情報保護への影響を事前に評価し、個人情報の漏洩や改変などの問題の提言に有効なリスク評価手法として、プライバシー影響評価 PIA（Privacy Impact Assessment）がある[32]。この PIA は、個人情報，特にプライバシー情報を扱うシステムを構築する際に実施するリスクコミュニケーション手法となっており、ISO 22307 や ISO/IEC 29134 で国際標準化されている。

ISO 22307 は、2008 年に発行された ISO の金融サービス専門委員会である ISO/TC 68 で起案された金融分野におけるプライバシーを保護する影響評価の要求項目を規定した規格である（ただし、金融分野以外の他の業種にも適用できるとしている）。具体的には、①PIA 計画、②PIA 評価、③PIA 報告、④十分な専門的知識、⑤独立性と公共性の程度、⑥対象システムの意思決定時の利用、といった 6 項目を PIA 実施における要求事項として規定した。

一方、ISO/IEC 29134 は、2017 年に発行されたプライバシー影響評価の手順と報告

[32] 瀬戸洋一（編著）・長谷川久美（著）、「ISO/IEC 29134 対応　プライバシー影響評価実施マニュアル」、日科技連、2020 年を参考に記述した。

書の構成などの推奨事項を規定した規格である。ISO/IEC 29134 は、ISO 22307 にて定められた PIA 実施における 6 項目の要求事項を踏襲して作成されている。また、プライバシー影響評価の手順として、①評価実施の準備、②評価の実施、③評価結果の報告の大きく分けて、3 つのステップからなることを定めている。この 3 つのステップのうち、①評価実施の準備段階では、評価項目・評価基準を定める必要があるが、ISO/IEC 29134 では、この評価項目のプライバシー保護要件として、ISO/IEC 29100 の記述をもとにするとしている（後段 BOX （４）③を参照）。

5.2. 各国におけるプライバシー保護

個人情報保護の枠組み（プライバシー・フレームワーク）については、各国での法規制やガイドラインの整備も進んでおり、こうしたルールへの対応も求められる。以下、各国の規制やガイドラインについて、その基本的原則の内容を中心に紹介したい。

5.2.1. 米国

米国 NIST は、2020 年に NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management（プライバシー・フレームワーク：企業のリスクマネジメントによるプライバシー向上のためのツール）を発表している。

プライバシーマネジメントシステム（PIMS）を規定する ISO/IEC 27701 が、情報セキュリティマネジメントシステム（ISMS）、具体的には ISO/IEC 27001 および ISO/IEC 27002 のアドオン（拡張）規格となっているように、サイバーセキュリティとプライバシーは密接な関係にある。NIST のプライバシー・フレームワークでは、サイバーセキュリティリスクとプライバシーリスクを次の図 17 のように整理している。

図 17：サイバーセキュリティリスクとプライバシーリスク

出典：寺田眞治、「米国のプライバシー保護に関する動向」[33]

[33] https://www.jipdec.or.jp/library/report/2020716_2.html

NIST のプライバシー・フレームワークでは、ISO/IEC 29134 でも求められている、プライバシーを設計の段階から考慮するというプライバシー・バイ・デザインの概念をサポートし、組織が個人のプライバシーを保護できるよう、より良いプライバシーエンジニアリングの実践を可能にするものとして設計されている。そして、次のような点で組織を支援することができるとしている。

- 製品及びサービスの設計又は展開において、個人のプライバシー及び社会全体に対する悪影響を最小限に抑えつつ、データの有益な利用を最適化する倫理的な意思決定を支援することにより、顧客の信頼を構築すること。
- 現在のコンプライアンス義務を果たすだけでなく、変化する技術や政策環境の中でこれらの義務を果たすために製品やサービスを将来にわたって発展させること。
- 個人、ビジネスパートナー、評価者、規制当局とのプライバシー慣行に関するコミュニケーションの円滑化。

このフレームワークでは、大きく次の 3 つの概念を設定していることが大きな特徴である。この 3 つの概念による整理を通じて、ビジネスやプロジェクトの推進力、組織の役割と責任、プライバシー保護活動とを関連づけることを通じて、プライバシーリスク管理を強化し、より優れたプライバシー基盤を構築できるようにすることを目的としている（具体的に示されている機能とその詳細は、表 18 参照）。

- コア（Core）：プライバシーの観点から持つべき機能のリスト
- ティア（Implementation Tiers）：コアの達成状況を 4 段階で表すもの
- プロファイル（Profiles）：ティアが現状いくつで、目標がいくつかを示すもの

表 18：3 つの概念において具体的に示されている機能とその詳細

要素	機能	詳細
コア	特定	組織のプライバシーリスクの把握
	統制	組織のガバナンス構造の開発
	管理	適切なデータ管理の手法の開発
	通知	データ処理に関するコミュニケーション活動
	対応	プライバシー侵害の対応策
ティア	組織のプライバシー対応の効果を評価する基準	ティア１：部分的な（Partial）
		ティア２：リスク情報を生かした(Risk Informed)
		ティア３：反復可能な(Repeatable)
		ティア４：適応性のある(Adaptive)

プロファイル	組織の現在のプライバシー活動または望ましい結果	コアの 5 つの機能にそれぞれ定義されたカテゴリ及びサブカテゴリに従い自己評価し、現状と目標を比較して改善策を特定する。

出典：寺田眞治、「米国のプライバシー保護に関する動向」

5.2.2. 欧州

欧州（EU）では、個人情報保護という基本的人権の確保を目的とした「一般データ保護規則（General Data Protection Regulation：GDPR）」が、2016 年に発効、2018 年 5 月 25 日から施行された。

GDPR は、その第 25 条にプライバシー・バイ・デザインや、個人情報の収集制限に関する考え方であるプライバシー・バイ・ディフォルトの概念が記載されており、こうした考え方は、GDPR 発効後の 2017 年に発刊された ISO/IEC 29134、および、2019 年に発刊された ISO/IEC 27701 にも反映されるなど、ISO の規格や世界のプライバシー法制やルールに大きな影響を与えてきた。

GDPR における個人データの処理に関する基本原則としては、①合法性、公正性および透明性、②目的制限、③データ最小限性、④正確性、⑤保管制限、⑥完全性および機密性保持、⑦責任という 7 つを掲げている。その内容を以下の表 19 に記す。

表 19：GDPR が定める 7 つの個人データの処理にかかる基本原則

原則	内容
適法性、公正性及び透明性	常に個人データは合法的、公正かつ透明性のある方法で処理される。
目的の限定	個人データは、特定され、明確で、かつ正当な目的のために収集されるものとする。
データの最小化	個人データの処理は目的との関係において、十分であり、関連性があり、かつ、必要な範囲に限定される必要がある。
正確性	個人データは正確で、必要に応じて常に最新に保たれる必要がある。
記録保存の制限	個人データの保管期間は、当初の収集目的を達成するために必要な期間のみにする必要がある。
完全性及び機密性	適切な技術的および組織的セキュリティ対策を行うことによって、個人データの不正な処理、予期しない公開・アクセス・紛失・破壊・変更に対して保護する必要がある。
アカウンタビリティ（説明責任）	個人データを扱う者は上記の遵守に責任を負うとともに、遵守を証明できなければならない。

出典：「Regulation (EU) 2016/679 (General Data Protection Regulation)[34]」Article 5 を参考に筆者作成[35]

[34] https://eur-lex.europa.eu/eli/reg/2016/679/oj

[35] 個人情報保護委員会が仮訳を公表（https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf）しており、その第 5 条の記述を参考にしたが、紙面の都合上、ここでは筆者が記述を若干変更している。

5.2.3. 中国

中国でプライバシー保護や個人情報保護が法制度として整備し始められたのは、比較的最近のことである。体系化の動きは、まず 2017 年 10 月に施行された民法総則に表れる。その後、2021 年 1 月に施行された、さらに上位となる中華人民共和国民法典において、プライバシー及び個人情報保護という章（第 6 章）が新たに設けられ、プライバシー権の定義が初めて規定された[36]。そして、2021 年 11 月には、中国個人情報保護法が施行され、これを補完するデータ越境移転安全評価弁法が 2022 年 9 月に施行された。また、標準化の関係では、2017 年末に「情報安全技術 個人情報安全規範」が国家標準として公表され、2020 年には改正版が公表された。ここでは、この中国国家標準である「情報安全技術 個人情報安全規範」を紹介する。

個人情報安全規範では、個人情報セキュリティに関し、①個人情報の収集、②個人情報の保存、③個人情報の使用、④個人情報の主体の権利、⑤個人情報の処理委託・共有・譲渡・開示、⑥インシデント対応、⑦セキュリティ確保のための組織体制という、7 項目の基本原則を規定し、具体的な対応基準を定めている（表 20 参照）。

表 20：個人情報安全規範が定める個人情報安全基本原則

原則	内容
権限/責任の一致	個人情報の安全を保障し、その個人情報の主体の権益に損害を生じさせた場合には責任を負う必要がある。
目的の明確性	明確で具体的な個人情報処理の目的を有する必要がある。
同意選択	個人情報の主体に個人情報処理の目的・方法・範囲等を明示し、同意を求める必要がある。
必要最小限の使用	個人情報の主体が同意した目的を満たすための必要最小限で個人情報を処理する必要がある。目的達成後は遅滞なくその個人情報を削除する必要がある。
公開・透明性	個人情報処理の範囲・目的・規則等を、明確で判り易く、合理的な方法で公開し、外部の監督を受ける必要がある。
セキュリティ確保	直面するセキュリティリスクに対応可能な安全能力を有し、適切な管理及び技術的手段を講じ、個人情報の機密性・完全性・可用性を保護する必要がある。
主体の関与	個人情報の主体に対して、その個人情報の閲覧・訂正・削除・承認と同意の撤回・アカウントの抹消、苦情の申し立てができる方法を提供する必要がある。

出典：「情報安全技術 個人情報安全規範[37]」第 4 条を参考に筆者作成

[36] この記述は、柊紫央璃・寺田眞治、「中国個人情報保護法と最新の動向」、https://www.jipdec.or.jp/library/itreport/2021itreport_winter03.html を参考にした。

[37] https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=4568F276E0F8346EB0FBA097AA0CE05E

5.3. 生体情報とプライバシー保護

eKYC を行う手段としては、指紋や虹彩などの生体情報を用いて行う生体認証が最も推奨される。その一方で、一般的に、生体情報はプライバシー保護面で特に慎重な取り扱いが必要である。なぜなら、仮に生体情報が流出した場合、個人に固有の生理学的特性または行動的特性のいずれかのプライバシー情報であり、変更することが困難または不可能であるためである。仮に、通信途上での傍受・記録・改ざんの可能性があり、異なるシステム間で伝送され情報が共有されると、システム全体が脆弱になるリスクがある。そのため、金融サービスに利用する場合、データの機密性・完全性を伝送中も保護するほか、必要な生体情報のみ収集することが重要になる。

本人確認の過程で生体情報を収集・利活用する場合、ISO 5158 では、生体情報保護の管理策や暗号化、キャンセラブル生体認証（生体情報を暗号化したまま管理・照合する生体認証）といった技術仕様を取りまとめた規格である ISO/IEC 24745（バイオメトリック情報の保護）の要求事項に従って保護する必要があるとしている（後段 BOX （４）④節を参照）。特に不要な情報は、セキュリティ上問題がないように削除するのが原則であるほか、仮に監査などの理由で保管を要する場合は、ISO/IEC 24745 に沿った情報保護策を図る必要があろう。

また、ISO 5158 を起案した ISO/TC 68 では、ISO 19092 という規格も制定している。ISO 19092 では、金融サービスにおいて生体情報を使用するためのセキュリティ・フレームワークに関する詳細な情報を提供している。モバイル金融サービス提供者が本人確認にあたって生体情報を使用する場合は、ISO 19092 にあるバイオメトリクス・セキュリティ・コントロールのリストが参考になる（後段 BOX （３）④を参照）。

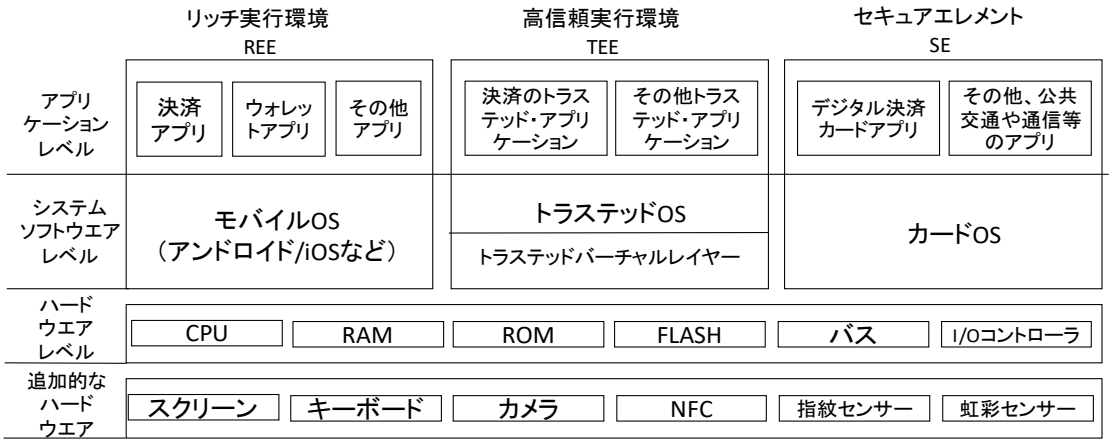
6. プライバシー保護を支えるモバイル端末側のセキュリティ

ここでは、モバイル端末側のセキュリティ機能の構成を整理する。eKYC において、モバイル端末は非常に便利なツールである。金融サービス提供者は、本人確認プロセスにおいて、その保証レベルの向上や、顧客の情報を保護するためには、モバイル端末側が提供するセキュリティ機能を理解してから、活用することが必要である。このため、ISO 5158 では、主に補論において[38]モバイル端末側が提供するセキュリティ機能の概要を整理している。

[38] 本文にも数行の記述がある。

一般的にモバイル端末は、セキュリティ確保のため、REE（Rich Execution Environment：リッチ実行環境）、TEE（Trusted Execution Environment：高信頼実行環境）、SE（Secure Element：セキュア・エレメント）といったセキュリティーレベルごとにソフトウェアの実行領域を分けている（図 21 参照）。ISO 5158 では、ISO/TC 68 で制定した ISO TS 12812-2（モバイル金融サービスのセキュリティとデータ保護）という技術標準を参照しながら、モバイル端末側のセキュリティ機能について整理を行っている（ISO TS 12812 については、後段 BOX （５）を参照）。

図 21：モバイル端末環境の構成



出典：ISO 5158　Figure A.1

以下では、モバイル端末を用いたモバイル金融サービスを提供するアプリケーションについて、どの要素をどこの環境で実行させるのが、セキュリティ上、有効と考えられるかについて検討する。

6.1. REE（リッチ実行環境：Rich Execution Environment）

REE は、一般的なアプリの実行環境を提供する標準的な OS である。REE のアプリケーションレベルのレイヤーでは、銀行アプリ、ウォレットアプリなど、一般的なアプリケーションを実行させる。

REE のシステムソフトウェアレベルのレイヤーでは、一般的なカメラ、USB 機器、タッチスクリーンなどを動作させるドライバーや、アプリを動作させるシステムサービスや管理フレームワークを提供する。また、TEE にアクセスする通信機能や TEE 用の外部 API を提供する機能も提供する。

6.2. TEE（高信頼実行環境：Trusted Execution Environment）

TEE は、REE 環境とは分離させた、セキュリティ関連要件を満たすモバイル端末内の実行環境である。アプリがアクセスするデータや機能に対する保護機能を持ち、攻撃の脅威に対抗できる。TEE は、「トラステッド・アプリケーション」（TA）と呼ばれるセキュリティソフトウェアを安全に実行する機能を備えており、認証済コードの実行、システムの完全性、機密性、真正性、プライバシーやデータアクセス権の保護などのセキュリティ機能を発揮する。

TEE のアプリケーションレベルのレイヤーでは、REE で実行されているアプリと組み合わせつつ、指紋認証、支払い、ID 認証など重要な金融サービス機能を提供するアプリを実行する。

TEE のシステムソフトウェアレベルのレイヤーでは、ハードウェアのリソース（CPU、RAM など）を利用してハードウェアレベルの分離環境を提供する。その上で、例えば、①セキュアなストレージ、信頼できるユーザーインターフェースの提供、信頼できる認証、②システムやアプリでの秘密鍵の扱い、③REE、SE、および外部デバイスとの安全な通信やアクセス制御、といったことを行う。

TEE は、アプリケーションをホストする SE と一緒に使用する場合がある。この場合、信頼できるユーザーインターフェース（ディスプレイとキーパッド）を用いること、および、モバイルデバイスに表示される取引データは SE 上にあるアプリによって生成、送信された情報のみとすることが必要である。

TEE は SE とは異なり、基本的にソフトウェアベースの技術によって実現されると同時に、外部からの耐タンパ性は想定されていない。REE で動作する凶悪型のマルウェア等に対抗するためには、TEE で動作するアプリケーション・ソフトウェア（信頼されたソフトウェア、Trusted Application: TA）に認証処理を実行させ、それ以外の処理を、REE 上の金融サービス用のアプリケーション・ソフトウェアで実行させることが考えられる。そして、マルウェアなどによる外部からの攻撃への耐性を確保するためには、以下の 3 点を満たすことが求められる[39]：

[39] 宇根正志・廣川勝久「モバイル端末を用いた金融サービスにおけるセキュリティ対策としてのセキュア・エレメントと TEE に関する一考察」、情報処理学会研究報告 Vol.2017-CSEC-79 No.2, 2017（https://ipsj.ixsq.nii.ac.jp/ej/?action=repository_uri&item_id=184664&file_id=1&file_no=1）参照。

条件①：認証にかかる処理を行う TA を改変させないこと。

条件②：TA とサーバの間の通信データの盗取・改変を防止すること、または暗号化等によって保護すること。

条件③：TA とサービス利用者の間の通信データの盗取・改変を防止すること。

6.3. SE（セキュア・エレメント：Secure Element）

SE は、信頼できる機関が定めたルールやセキュリティ要件に従って、アプリケーションやその機密データ、暗号関連データ（暗号鍵など）を安全に保持することができる耐タンパ性のあるプラットフォームである。SE は、多様なビジネス実装や市場のニーズに対応するために、組み込み型、一体型、SIM、マイクロ SD 型、スマートカードなど、様々な形態がある。

SE では高いセキュリティを求めるアプリを動作させる。アプリケーションレベルのレイヤーには、金融、公共交通、通信などのアプリを導入するが、そのアプリも出荷時から設定するか、Trusted Service Manager（TSM）[40]の管理下で導入することになる。

また、SE のシステムソフトウェアレベルのレイヤーでは、OS レベルでのセキュア・エンコードや暗号鍵の保存などの機能を提供する。

ISO TS 12812-2 では、モバイル端末のセキュア環境にかかる要件について述べられている。そこでは、SE に対し、ハードウェアレベルのセキュリティとして、物理的に分離されたコンピューティングモジュールで機密データの保存と処理を行うこと、また、機密データは、たとえ攻撃によって SE が物理的に破壊されたとしても、開示攻撃から保護される必要があること、改ざん防止を図るため物理的なセキュリティ機構を用いて設計することや、アプリケーションのデータの秘匿性および完全性を常に提供することなどのセキュリティ上の要求事項を求めている。

なお、SE による認証処理が有効となるためには、以下の 3 点を満たすことが求めら

[40] 主に NFC を利用した様々なサービスについて、それらサービスに関連する利用者情報を安全に管理するシステムのこと。例えば、日本において数多く用いられている NFC サービスであるモバイル FeliCa の場合は、フェリカネットワークス社の管理するシステムが TSM の役割を担っており、サービスを展開する事業者向けに、プラットフォームの運営、サービス展開の支援、「モバイル FeliCa IC チップ」に関するライセンス供与を行っている。

れる[41]。

・条件①：SE 内部で認証にかかる処理を行うアプリケーション・ソフトウェア（SE アプリ）が改変されないこと。

・条件②：SE アプリとサーバの間の通信データが盗取・改変されないこと、または暗号化等によって保護されること。

・条件③：SE アプリとサービス利用者の間の通信データが盗取・改変されないこと。

6.4. ペリフェラルハードウェア（周辺機器）

モバイル端末には、全てではないが、指紋、虹彩、NFC などのハードウェアセンサーやリーダーが搭載されている。指紋認証、支払い、ID 認証など重要な金融サービス機能を提供する場合、これらの機器は、TEE に制御させて、センサー情報を処理する事例が多い。

7. まとめ

本稿では、オンラインでの本人確認（eKYC）の概要について、そのコア技術である顧客の本人確認にかかるガイドラインである ISO 5158 の構成を参考にしつつ、諸外国での議論を取りまとめた。モバイル端末が普及する中、eKYC はますます重要となっており、今後も様々な場面で活用が期待される。これまで見てきたように、諸外国のガイドラインだけ、あるいは、ISO の規格だけの情報があれば、直ちに実務が行えるだけの情報が揃うというものではないが、こうした考え方を土台とすることで、社会が求めるより安全で効率的な eKYC を行うことにつながると考えられる。本稿の内容が参考になり、より安全で効率的な eKYC が実社会の中で広まると幸いである。

以　上

[41] 宇根正志・廣川勝久「モバイル端末を用いた金融サービスにおけるセキュリティ対策としてのセキュア・エレメントと TEE に関する一考察」（先述の脚注 39 と同じ）。

本稿は、ISO 5158 の規格そのものを解説した文書ではありません。ISO 5158 の内容を踏まえ、その他の各種規格や規制を参照したうえで、モバイル金融サービスにおける本人確認および eKYC に関係する世の中の議論を取りまとめたものです。ISO 5158 の記載内容や表記については、必ず原文を確認するようお願いします。また、本稿における ISO 5158 をはじめ ISO 規格の日本語表記は筆者が行ったものです。ISO や日本規格協会によるものではありません。

ISO の金融サービス専門委員会（TC 68）は、国際標準 ISO 5158 をはじめ、金融サービスに必要なセキュリティ、識別子、メッセージフォーマット等に係る様々な国際標準について議論しています。日本銀行決済機構局は、その ISO/TC 68 国内審議団体として国内事務局事務を担当しています。ISO/TC 68 国内委員会に関するご質問、また ISO/TC 68 国内委員会への加入にご興味がある場合等は、日本銀行決済機構局 決済システム課 情報技術標準化グループ（代表 03-3279-1111、メール iso-tc68@boj.or.jp）までお知らせ下さい。

[BOX]　ISO 5158 と関係の深い各種 ISO 規格等の概要

（1）ISO 24366 (Natural Person Identifier : 自然人識別子) 規格の概要

ISO 24366 は、2021 年 10 月に公表された自然人を識別する ID 番号にかかる ISO の国際標準である。ISO/TC 68（金融サービス）委員会が作成した。

ISO 24366 規格では、本文の表 1 に示した自然人の属性を示すデータレコードのほか、規格のスコープと識別子（ID 番号）の構造が定められている。なお、2023 年 4 月現在、この規格に追加すべき内容について、議論が進められている。

規格のスコープ

この ISO 24366 の規格では、マシーンリーダブルで（機械が読んで理解でき）、曖昧さのない自然人識別子とその参照データを規定している。個人情報（個人識別可能な情報）を利用するではなく、個人情報とは無関係な識別子だけを利用することで、金融取引をする自然人を、プライバシーを保護しつつ、一意に識別できることを目的としている。

識別子の構造

識別子は、15 桁の固定長。最初の 13 桁が、自然人を示すコードで、大文字アルファベットもしくはアラビア数字からなる。最後の 2 桁が、チェックディジットで、アラビア数字からなる。

（２）ISO/IEC TS 29003（Identity proofing：身元確認）が定義する身元確認強度

ISO/IEC TS 29003 は、①人物の身元証明にかかるガイドラインと、②Levels of identity proofing（LoIP：身元確認のレベル）、および、これらのレベルを達成するための要件を規定している技術標準である。ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティ、プライバシー保護）委員会が作成した。

この ISO/IEC TS 29003 では、LoIP について以下のように定義されている。

レベル	定義	属性確認	本人と ID との結びつき確認
LoIP1	本人であることの信頼度が低い（ID がコンテキスト内で一意であり、存在するとの仮定があり、かつ、申請者と ID との結びつきがあるとの仮定がある）。	何の確認も行われていない。	何の確認も行われていない。
LoIP2	本人であることの信頼度は中程度（ID はコンテキスト内で一意であり、存在することが中程度に立証されており、ID に対して何らかの拘束力がある）。	属性には裏付けとなる証拠が存在する。	本人と ID との結びつきが 1 つの要素で確認された。
LoIP3	本人であることの信頼度は高い（ID はコンテキスト内で一意であり、ID の存在が強く立証されており、本人は ID に対して強い拘束力を持っている）。	属性には権威ある証拠が存在する。	本人と ID との結びつきが 2 つ以上の要素を用いて確認された。

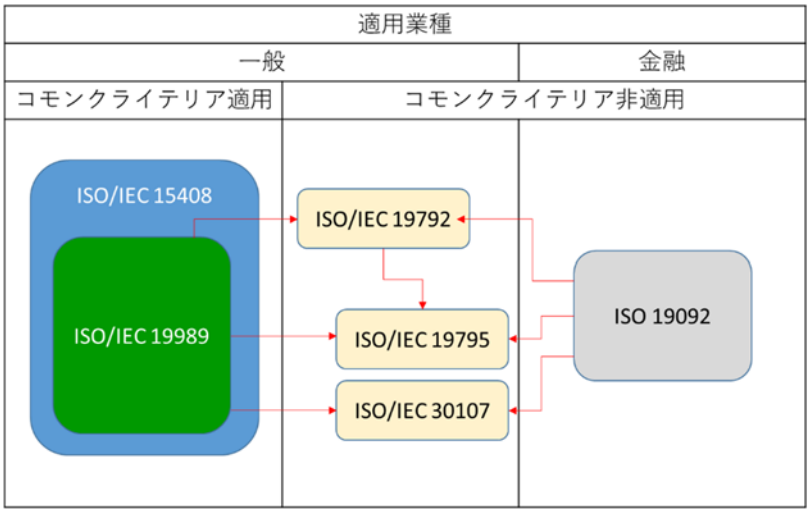
出典：European Union Agency for Cybersecurity(ENISA) “eIDAS COMPLIANT eID SOLUTIONS” Figure 4 を参考に ISO/IEC TS 29003 を参照しながら筆者作成

（3）生体認証のセキュリティ評価に活用可能な国際標準

本文の 3.2.3.節にあるように、ISO 5158 では、eKYC で当人認証を行う方法としては生体認証を活用することが推奨されている。そのため、生体認証のセキュリティ評価は重要事項である。ここでは、生体認証のセキュリティ評価に関係する国際標準を列挙し、関係性を整理したうえで、内容を簡単に概説したい。対象とする規格は以下の通り。

規格	表題	制定委員会	内容
ISO/IEC 15408	情報技術セキュリティの評価基準	ISO/IEC JTC 1/ SC 27 情報セキュリティ、サイバーセキュリティ、プライバシー保護	IT セキュリティ評価を行うための共通的な評価基準を定めたもの。コモンクライテリアと呼ばれる。
ISO/IEC 19792	バイオメトリクスのセキュリティ評価		生体認証製品のセキュリティ評価のあり方を定めたもの。
ISO/IEC 19989	バイオメトリクス・システムのセキュリティ評価の基準と方法論		コモンクライテリアに基づく生体認証製品のセキュリティ評価基準を定めたもの。
ISO/IEC 19795	バイオメトリック性能試験及び報告	ISO/IEC JTC 1/SC 37 バイオメトリクス	生体認証製品の生体認証の性能試験及び報告方法を定めたもの。
ISO/IEC 30107	生体認証による提示攻撃検出		人工物等による、なりすましなどの提示攻撃検出について定めたもの。
ISO 19092	生体認証におけるセキュリティ・フレームワーク	ISO/TC 68 金融サービス	金融サービスにおいて、生体認証を用いる場合のセキュリティの枠組みを定めたもの

これらの生体認証のセキュリティ評価に関する国際標準の参照関係を以下に示す。ISO 19092 は、コモンクライテリアに適合するための要件が厳しいこともあり、既存の標準である ISO/IEC 19792、ISO/IEC 19795、ISO/IEC 30107 の考えに基づき、金融業界向けに、コモンクライテリアとは一定の距離を置いて作られている。



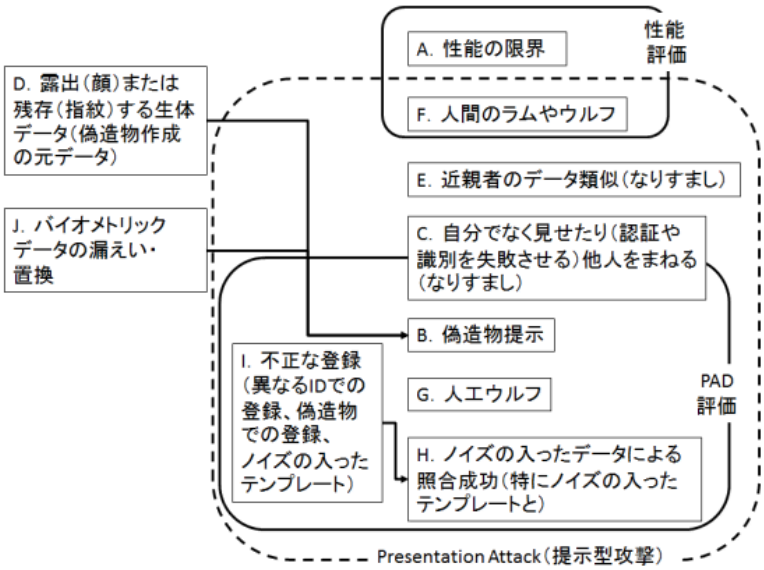
出典：筆者作成

① ISO/IEC 19792（バイオメトリクスのセキュリティ評価）の概要

生体認証の製品やサービス等のセキュリティ評価を行う際は、ISO/IEC 19792 が参考になる。

情報技術に関連する製品やシステムが、セキュリティの観点から、適切に設計され正しく実装されているかを評価する体系として、コモンクライテリア（Common Criteria, 略称 CC）と呼ばれる規格 ISO/IEC 15408 に基づく評価（CC 評価）があり、政府調達案件などで活用されている。しかし、生体認証の製品やシステムのセキュリティ評価には、ISO/IEC 15408 が定める規定だけでは不足があった。ISO/IEC 19792 は、ISO/IEC 15408 に不足しているのは精度となりすまし対策である提示攻撃検知（Presentation Attack Detection: PAD）の評価であることを明らかにし、生体認証システムのセキュリティ評価の考え方をまとめ、2009 年に制定された。

ISO/IEC 19792 は、生体認証製品やシステムのセキュリティ評価のための主な要件を提示することで、ガイダンスとして活用することが想定されている。具体的には、生体認証における脆弱性や脅威を整理し、セキュリティ評価の視点を明確にした。以下の図は、ISO/IEC 19792 の評価の視点をまとめ直したものである。



出典：山田朝彦「生体認証におけるセキュリティ評価と国際標準化」[42]

ISO/IEC 19792 は生体認証のセキュリティ評価の考え方を示したが、CC 評価を可能にしたものではない。CC 評価を可能にしたのは、その後 ISO/IEC 19792 の考えに基づき 2020 年に制定された ISO/IEC 19989 シリーズである（次項②参照）。

[42] https://www.jaisa.or.jp/pdfs/161130/02.pdf

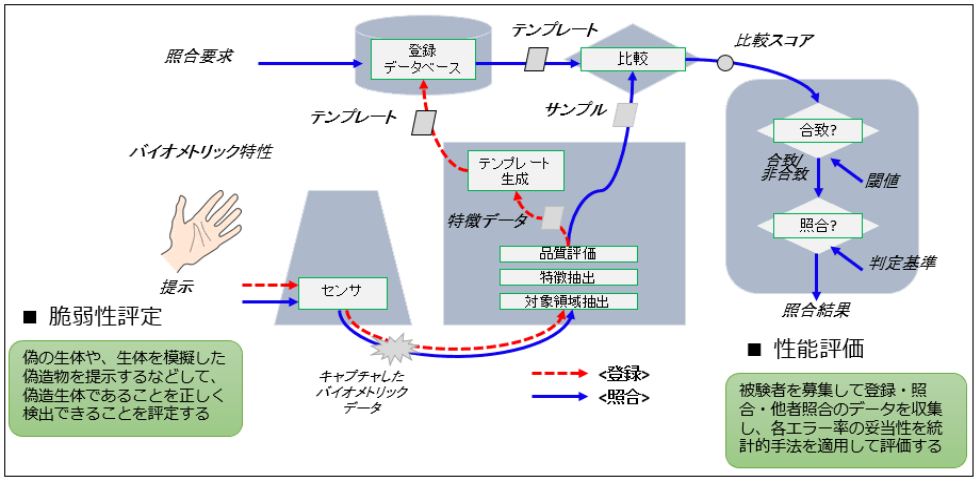
② ISO/IEC 19795 シリーズ（バイオメトリック性能試験及び報告）の概要

生体認証の製品やサービス等の性能評価を行う際は、ISO/IEC 19795 が参考になる。ISO/IEC 19795 はパート 1 から 10 まで（パート 8 は欠番）の 9 パート構成であり、各パートは以下のとおりである。

パート 1 ：生体認証の性能試験及び報告に関する原則及び枠組み
パート 2 ：技術及びシナリオ評価のための試験方法論
パート 3：モダリティ固有の試験
パート 4：相互運用性の性能試験
パート 5：アクセスコントロールシナリオ及び格付けスキーム
パート 6 ：運用評価の試験方法
パート 7 ：カード内バイオメトリック比較アルゴリズムの試験
パート 9：モバイルデバイスでの試験
パート 10：集団構成によって生じる性能の差異の定量化

パート 1 で全般的な指針が示されており、生体認証にかかる性能評価を実施するに当たって、分析のための指標（登録失敗率（FTE：Failure To Enroll）、誤受入率（FAR：False Acceptance Rate）、誤拒否率（FRR：False Rejection Rate））を示すと共に、計画作成・データ収集・記録・分析・報告といったプロセス毎に指針を提示している。

生体認証の CC 評価を規定した ISO/IEC 19989 シリーズでは、性能評価はこの ISO/IEC19795 に準拠している。また、脆弱性評定については次項③の ISO/IEC 30107 シリーズを参考にしている。性能評価と脆弱性評定の関係は、以下の図が参考になる。



出典：金子浩之「コモンクライテリアを適用した生体認証の第三者評価・認証」[43]

[43] https://www.jstage.jst.go.jp/article/itej/72/3/72_255/_pdf/-char/ja

③　ISO/IEC 30107 シリーズ（生体認証による提示攻撃検出）の概要

偽造物によるなりすましなど、生体認証における提示攻撃（プレゼンテーションアタック）検出については、ISO/IEC 30107 が参考になる。ISO/IEC 30107 は、パート 1～4 の 4 パート構成であり、それぞれ以下の内容が記載されている。

パート 1：フレームワーク

―― 提示攻撃に使う道具（Presentation Attack Instrument：PAI）の類型化や、提示攻撃検知（Presentation Attack Detection：PAD）のメカニズムの概要などについて記載している。

パート 2：データフォーマット

―― 検知結果を伝達するためのデータのフォーマットについて規定している。

パート 3：テストとレポート

―― なりすましや隠匿のために PAI が持つべき性質、PAD の提示方法、PAI の作成方法、PAI を使った評価方法、PAI の誤受入率や非 PAI の誤拒否率に対する考え方などについて規定している。

パート 4：モバイルデバイスでの試験のプロファイル

―― パート 3 に基づいて、モバイルデバイス上の PAD 試験の要求事項を規定している。

④　ISO 19092（生体認証におけるセキュリティ・フレームワーク）の概要

金融サービスにおける生体認証へのセキュリティ対策については、ISO 19092 が参考になる。ISO 19092 は、ここで掲げた他の国際標準と異なり、ISO/TC 68（金融サービス）委員会が作成したものであり、金融業務において生体認証を利用する際に特に求められるセキュリティについて規格化したものである。なお、ISO 19092 は、2023 年 3 月に改訂版（第 2 版）が公表された。

ISO 19092 は、金融サービスのリテール決済分野において、クレジットカードまたはモバイル端末などを使用して生体認証を活用するため、各要素技術からシステムレベルに至るまでのセキュリティガイドラインを提示することを目的としている。具体的には、登録時に提示された資格情報の検証、登録・送信・保存・照合・識別の各プロセスにおける生体情報のライフサイクル管理、生体情報の取得・処理に使用する物理的ハードウェアのセキュリティ要件、生体認証のアーキテクチャにかかるセキュリティ要件などを定めている。

また、ISO 19092 には、生体認証を活用するにあたってのセキュリティコントロール策の要件をリスト形式で提示している。このうち、合理的な保証を提供するために、金融取引のバイオメトリクス認証システムに一般的に適用されるセキュリティコントロール策を以下に示す。

物理的セキュリティ	
1	生体認証に用いる装置は、装置内部へ物理的に不正にアクセスできないようにするほか、装置の不正使用又は変更（装置全体の代替を含む）ができないよう、物理的セキュリティ機構を採用すること。
2	すべての公共の場に設置してある生体情報を取得する機器は、ISO 13491-1 及び ISO 13491-2 （リテール金融取引において利用される物理的かつ機能的にセキュアな暗号装置（SCD：Secure Cryptographic Devices）に要求される機能に関する規格）に定義されたセキュリティ要件を満たしていること。厳密な準拠が達成されない要件については、代わりになる管理が実施されていること。
3	個人用バイオメトリクス IC カードは、ISO/IEC 15408（コモンクライテリア）の EAL4+（評価保証レベル 4 以上であること。評価保証レベル 4 は、既存の商用製品の開発に対し、セキュリティに係るエンジニアリングコストの追加を受け入れられ、中レベルから高レベルの保証されたセキュリティを必要とする場合に適用されるレベルである。なお、バイオメトリクスを搭載していない銀行発行 IC カードにも EAL4 以上が求められる。）と同等のセキュリティ要求事項を満たしていること。
4	スマートカード及び SCD ではない個人用のバイオメトリクス機器は、少なくとも、生体情報を処理する際に情報を保護するために使用される鍵の少なくとも一部に信頼できるドメイン（Trusted Domain: TD）を利用し、TD 内でバイオメトリクス処理操作をインスタンス化すること。
5	個人用の TD で保護できない機器上でバイオメトリック処理を行う場合は認証および暗号化を行うこと。
6	生体情報を取得する機器以外の生体情報を扱うシステムは、暗証番号を用いた認証システムと同レベル以上のセキュリティが確保されている前提で設計されていること。
7	プロビジョニング、認証及び監視サービスに使用される HSM（ハードウエアセキュリティモジュール：デジタル鍵を保護および管理し、暗号処理を提供する物理デバイス） API は、一般的にも、アプリケーション固有の部分にもセキュリティ脆弱性に対して安全であると評価されること。
8	生体認証装置の製造者が、ISO 19092 が求めるすべてのセキュリティ要件に準拠していること。
9	内部センサーと特徴抽出の間の経路などの通信路を保護するために、物理的な保護や nonce、challenge、timestamp などのプロトコルメッセージに対して動的データを使用するリプレイ攻撃の対策がなされていること。
論理的セキュリティ	
10	各処理または保管サブシステム内のバイオメトリック情報の真正性、完全性、および機密性を維持するために、認証済みの暗号化メカニズムが使用されていること。
11	サブシステム間の通信チャネルの真正性、完全性及び機密性を維持するために、認証済みの暗号化メカニズムが使用されていること。
12	機密性のために暗号化が行われる際、そのアルゴリズムは ISO/IEC 18033（暗号化アルゴリズムに関する国際標準規格）で定義されているものの一つであること。
13	電子署名を使用して完全性を提供する場合、そのアルゴリズムは、ISO/IEC 9796（メッセージ復元型のデジタル署名方式） または ISO/IEC 14888（署名添付型のデジタル署名方式）に定義されているもののうちの一つであること。

14	エンティティ認証（署名の作成者が本人であること、なりすましされていないことを保証する認証）アルゴリズムについては、ISO/IEC 9798（認証メカニズム）で定義されるアルゴリズムの一つであること。
15	完全性が MAC（Message Authentication Codes、メッセージ認証符号）を使用して提供される場合、そのアルゴリズムは、ISO/IEC 9797（MAC）で定義され、ISO 16609（共通鍵暗号を利用したメッセージ認証の要求事項）に従って検証されたものの 1 つであること。
16	機密性と完全性が一緒に提供される場合、そのアルゴリズムは、ISO/IEC 19772（セキュリティー認証付き暗号化）で定義されたものの 1 つであること。
17	公共の生体認証機器については、鍵管理技術は、ISO 11568（金融のリテール向けサービスの鍵管理）に準拠すること。
18	個人用生体認証機器については、鍵管理技術は、 ISO 11568 に準拠するか、または ISO 11568 と同等のセキュリティを達成すること。
セキュリティコンプライアンス検証	
19	研究にて評価する際、またはセキュリティ監査の際は、生体情報の捕捉、特徴抽出、および比較計算を行うときには、セキュリティ品質もその対象とすること。
20	研究にて評価する際、またはセキュリティ監査の際は、環境 ―すなわち提示されたバイオメトリクスとバイオメトリクス・システムの信号を捕捉するハードウェアとソフトウェアとの間の経路― のセキュリティを対象とすること。
21	研究にて評価する際、またはセキュリティ監査の際は、生体情報の捕捉と特徴抽出のハードウェアとソフトウェア領域の物理的及び論理的セキュリティについて取り扱うこと。
22	研究にて評価する際、またはセキュリティ監査の際は、生体情報の捕捉および特徴抽出を行うサブシステムが存在する場所のセキュリティも対象とすること。
23	研究にて評価する際、またはセキュリティ監査の際は、生体情報を記憶したり、比較したり、決定したりするサブシステムの物理的及び論理的セキュリティを検討すること。
24	研究にて評価する際、またはセキュリティ監査の際は、物理的または論理的に、サブシステム間の通信パスのセキュリティを対象とすること。
25	研究にて評価する際、またはセキュリティ監査の際は、生体情報を参照し、その関連 ID 要素を関連付けるプロセスにおいても、セキュリティ上問題ないことを確認すること。
26	研究にて評価する際、またはセキュリティ監査の際は、関連する ID 管理システムのセキュリティ状況についても対象とすること。
27	研究にて評価する際、またはセキュリティ監査の際は、そのセキュリティ管理プロセスも対象とすること。
28	金融サービス向けの生体認証基準への準拠状況は、独立した第三者検査機関またはその他の評価専門機関によって検証されること。

出典：ISO 19092 Table C.1 を参考に筆者作成

また、生体認証を行う際には、生体情報を扱うため、その個人情報保護が論点になる。ISO 19092 では、生体情報を適切かつ安全に生成、検証、保管、および終了されることを合理的に保証するための管理策として、情報保護面についての管理策も規定している。それに該当する ISO 19092 が定める生体認証データのライフサイクルコントロール策を以下に示す。

データの保存と取り扱い	
29	データの参照分割[44]を使用する場合、以下のセキュリティ要件が適用される。 - 1 つの部分データから実行可能なデータを再構築することが不可能な分割プロセスであること。 - 保存された部分が、偶然の場合を除き、同じ ID または他の ID のいずれについても、他の保存された部分と一致しないことを保証する分割プロセスであること。 - データは登録時にのみ構築された状態で保持され、分割された部分の保存が完了するまでは保持されるが、その後、データおよび保存システムに保存されていない部分は直ちに不可逆的に消去されること。 - データは、認証の間のみ、一致または非一致の決定がなされるまで構築された状態で保持され、その後、すべてのデータが即座に不可逆的に消去されること。 - 1 つの部分データだけでは、いかなる情報も提供されないこと。
身分証明書の登録	
30	金融サービスにおいて、生体認証システムに登録する前に、各登録希望者は、通常、銀行口座の開設時に、関連する ID 管理システムに登録していること。
生体情報の提示	
31	生体情報を認証のために提示する場合、提示攻撃検知メカニズムが設けられていること。
32	不適切な PBP[45]デバイスの不正な調整（キャリブレーション）や妨害行為を防ぐため、適切なポリシー、コントロール、監査手順が作成され、実行されていること。
比較および判断	
33	閾値の不適切な調整を防止するため、適切な方針、管理及び監査手順が作成され、実施されていること。
34	比較スコアの増分値が、連続したスコアではなく、十分なステップサイズを持っていること。
35	アプリケーションプログラムと生体認証システムとの間で完全性を確保するための認証が行われること。
エンロールメント	
36	登録者が、適切な許可を持っていることを保証する仕組みと手順があること。
37	登録時または登録済の生体認証機器の起動前に、登録者の識別を確認する仕組みと手順が用意されていること。
38	生体情報のサンプルが、バイオメトリクスの基準として使用するのに十分な品質であることを確認するための仕組みと手順が設けられていること。

[44] 参照分割（reference splitting）とは、生体情報の漏洩等のリスクを軽減するために、バイオメトリック参照データを分割し、異なる場所（例えば、2 分割バイオメトリック参照データの内、1つを発行者が保持し、他方の部分を TTP (Trusted Third Party：信頼性を持った機関)に送信される。）に保存すること。分割された情報は、比較プロセス中に回復される必要がある。

[45] PBP（Point of Biometric Presentation）は、口座保有者が金融取引を行うために、または将来取引で使用するために支払カードと組み合わせて生体情報を提示するためのヒューマンインタフェース技術のこと。

39	登録時に、登録者から有効なバイオメトリック参照データのみが取得されることを保証するための仕組みと手順があること。
40	バイオメトリック参照データと ID の結合は、承認された暗号アルゴリズムまたは他の承認された手順を 使用して、操作から保護されること。
41	変質した、または古くなったバイオメトリクス・サンプルを受け入れないことを保証するメカニズムおよび手順が設けられていること（ISO/IEC 30107 （生体認証による提示攻撃検出）を参照）。例えば、バイオメトリクス認証機能を起動する前に、独立した認証要素が必要。顔のモーフィング[46]攻撃を防ぐため、ライブ・キャプチャを推奨する。
リファイン、システムやアプリケーションの更改	
42	システムやアプリケーションを更改する際は FMR や FNMR[47]を増加させないこと。すなわち、更改は、識別プロセスの精度または効率を向上させる場合にのみに限ること。
検証	
43	バイオメトリクスの対応する FNMR は、バイオメトリクス管理方針の要件と一致すること。
終了	
44	データの抹消は、権限を有する者又は権限を有する自動化されたプロセスにより実施されること。
45	終了プロセスは、与えられた ID のすべての関連する参照が終了することを保証すること。
46	終了イベントは、将来の監査のために記録されること。
一時停止および再活性化	
47	参照データの一時停止および再活性化は、許可された人または許可された自動化されたプロセスによってのみ実行されること。
48	参照データの一時停止および再活性化は、与えられた ID のすべての関連する参照が、同時かつ確実に一時停止または再活性化されることを保証すること。
49	一時停止および再有効化イベントは、将来監査できるよう、ログを記録すること。
アーカイブ	
50	アーカイブされた生体情報への不正アクセスを防止するために、アクセス制御メカニズムが設けられていること。
51	アーカイブされた生体情報参照は、それが終了したシステムに復元されること、またはそれが非活性化されたときに活性状態に復元されることを防止するための措置がとられていること。
52	アーカイブからの復元は、フォレンジック[48]の目的のためにのみ許可されること。
53	アーカイブからの復元する際は、将来の監査のために、ログを記録すること。

出典：ISO 19092 Table C.2 を参考に筆者作成

[46] モーフィングとは、コンピュータグラフィックスによる映像手法の一つで、あるイメージから別のイメージへ徐々に変化していく様子を動画で表したもの。ある人物の顔が別の人物の顔に連続的に変形していく映像などを作り出すことができる。

[47] FMR（False Match Rate：誤合致率）は、他人を誤って受け入れる率、FNMR（False Non Matching Rate：誤非合致率）は本人を誤って棄却する率のこと。

[48] フォレンジックとは、セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取り組みのこと。

（4）プライバシー保護にかかる国際標準

① ISO/IEC 29100（プライバシー・フレームワーク）の概要

ISO/IEC 29100 は、プライバシー・フレームワークを定めた国際標準である。ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティ、プライバシー保護）委員会が作成した。

組織がシステムにおいて、個人識別可能情報（Personally Identifiable Information：PII）に関連するプライバシー安全対策要件を定義する際の一助となることを目的としている。具体的には、PII の定義、プライバシーに関連する一般的な用語の規定、PII の処理に携わる者及びその役割の定義、プライバシー安全対策要件の説明を行っている。特にプライバシー安全対策要件に関しては、下表に掲げる 11 の点を主要な原則と規定している。ISO/IEC 29100 が定める 11 項目のプライバシー原則は以下の通り。

	原則	概要
1	同意と選択	有効な手段の確立、同意または同意しなかった場合の影響を通知
2	目的の正当性と規定	正当な利用目的の設定と明示、目的変更時の事前同意
3	収集の制限	必要最低限の範囲での情報の取得
4	データ最小化	必要最低限の処理、必要最低限の要員による処理
5	利用、保持、開示の制限	必要最低限の期間での保持、必要な延長保持時のデータロック、利用目的達成できる必要最低限の開示
6	正確性と品質	個人情報の正確性の確保
7	オープンさ、透明性、通知	ポリシー、ポリシーの変更、処理結果、処理を中止させる方法の伝達
8	個人の参加とアクセス	開示要求と訂正要求に関する権利
9	説明責任	個人情報の取り扱いに関する説明責任
10	情報セキュリティ	個人情報の安全管理措置
11	プライバシーコンプライアンス	関連法令の遵守

出典：打川和男、「『ISO/IEC 27018』――クラウド上の個人情報取り扱いに関する国際的ベストプラクティスとは」[49] を参考に ISO/IEC 29100 を参照しながら筆者作成

この 11 の原則に基づいて事業者が、具体的なプライバシー強化技術の実装と利用、全体的なプライバシーマネジメント、外部委託したデータ処理のプライバシー管理策、プライバシーリスクアセスメントなど、詳細な個人情報保護の取り組みを定め、実施することを定めている。

[49] https://atmarkit.itmedia.co.jp/ait/articles/1604/07/news022.html

② ISO/IEC 27701（プライバシー情報マネジメント：PIMS）の概要

ISO/IEC 27701 は、個人情報の処理によって影響を受けかねないプライバシーを保護するための要求事項およびガイドラインを定めた国際標準である。ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティ、プライバシー保護）委員会が作成した。

ISO/IEC 27701 は、情報システムマネジメントシステム（ISMS：ISO/IEC 27001、ISO/IEC 27002）の拡張という形で[50]、組織内のプライバシー管理のために、プライバシー情報管理システム（PIMS）を確立、実施、維持及び継続的に改善するための要件を規定し、指針を提供している。

本文書は、PIMS 関連の要件を規定し、個人情報処理に説明責任を持つ管理者及びデータ処理者に向けたガイダンスを提供するもので、公共及び民間企業、政府機関及び非営利団体を含むあらゆる種類及び規模の組織に適用できるものとなっている。

③ ISO/IEC 29134（プライバシー影響評価：PIA のガイドライン）の概要

ISO/IEC 29134 は、プライバシー影響評価（PIA：Privacy Impact Assessment）の位置づけや実施手順について規定した国際標準である。ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティ、プライバシー保護）委員会が作成した。

プライバシー影響評価は、個人識別可能情報（PII：Personally Identifiable Information）を処理するプロセス・情報システム・プログラム・ソフトウェアモジュール・デバイスなどプライバシーに対する潜在的な影響を評価するための手段であり、利害関係者と協議してプライバシーリスクに対応するために必要な行動を起こすための手段になるものである。

PIA の実施目的は、以下の 3 つ挙げられる。

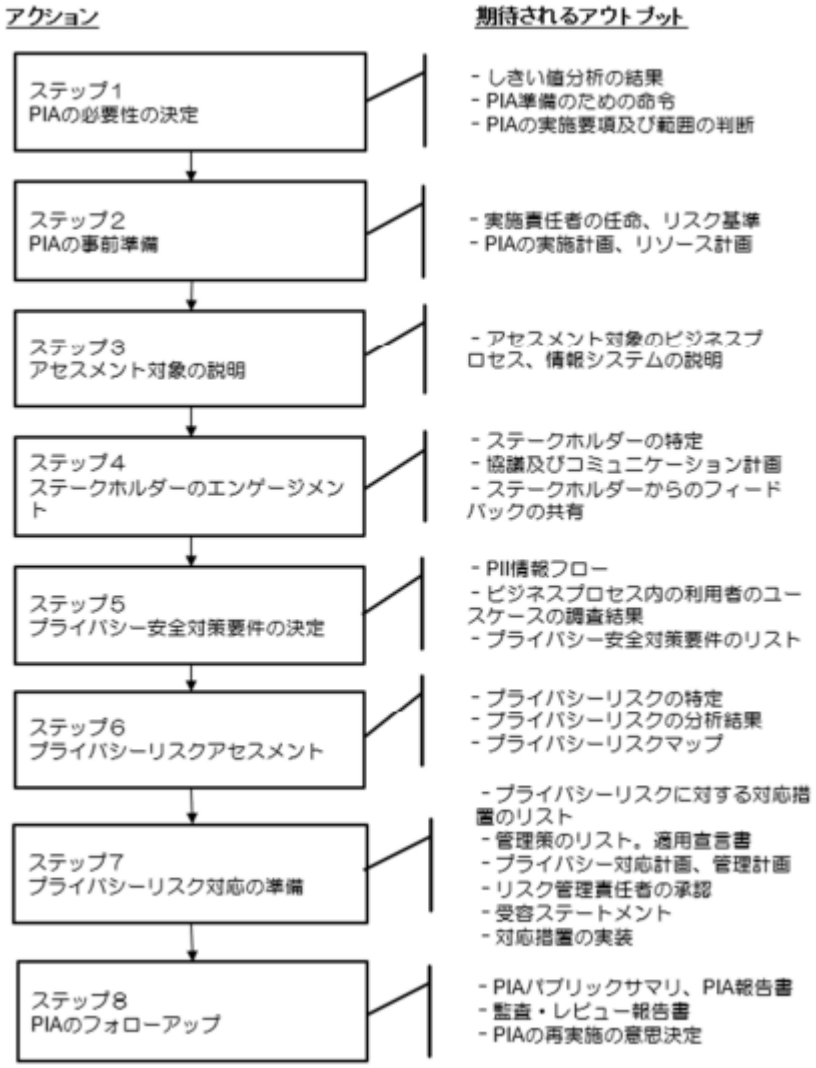
① プライバシー・バイ・デザイン：プライバシー保護を図るために、設計段階から考慮を行うコンセプト）へのインプットを提供すること

② ステークホルダーエンゲージメント：PIA を実施することにより、異なる利害関係をもつステークホルダー間の信頼構築に結び付けること

[50] ISO/IEC 27701 の英文本書のタイトルの表記は、Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management（プライバシー情報マネジメントのための ISO/IEC 27001 および ISO/IEC 27002 の拡張）となっている。

③ デューデリジェンス（事前に、業務の過程で起こり得る潜在的なプライバシーリスクを特定し、対処する PIA のプロセスのこと）

PIA 実施方法について、ISO/IEC 29134 で示されている内容を、ステップに分け、PIA の準備から実施、フォローアップまでの作業の流れと各ステップで期待されるアウトプットをまとめて表記すると以下の図表のようになる。



出典：菊地彰、「プライバシー影響評価（Privacy Impact Assessment）～ISO/IEC29134:2017 の JIS 化について～」[51]

[51] https://www.jipdec.or.jp/library/report/2020721.html

④ ISO/IEC 24745（生体情報保護）の概要

ISO/IEC 24745 は生体情報保護を定めた国際標準である。ISO/IEC JTC 1/SC 27（情報セキュリティ、サイバーセキュリティ、プライバシー保護）委員会が作成した。

生体認証には、確実な認証だけでなく、プライバシー保護も求められる。生体情報（生体的な特性）は、個人に固有な特性であり、理想的には個人に対応付けられるものである。この個人の特性と個人との対応関係があることによって、強力に確実な認証を提供できる。一方、この強力な対応関係はプライバシー上の大きな課題となる。個人情報流出の事故が散見され、個人情報である生体情報についても流出の可能性の懸念が払拭できていない。また、生体認証以外の場合は、認証情報の漏洩に対しては、パスワードを変更する、新しいトークンを発行するといった解決策がある。しかし、生体認証にはこうした解決策が一般的に利用できない。なぜなら、生体的な特性は、個人に固有の生理学的特性または行動的特性のいずれかであり、変更することが困難または不可能だからである。以上のことから、生体認証システムのセキュリティ対策と生体情報に対応する個人のプライバシーを保護するための適切な対策が、不可欠である。

こうした問題意識の下、ISO/IEC 24745 では、生体情報の元になる個人のプライバシーを保護するための適切な対策方法として、以下の策を提示している。

- 生体認証及びそのシステム・アプリケーション・モデルに固有の脅威と対策の分析方法
- 生体登録情報（Biometric Reference：BR）とアイデンティティ参照情報（Identity Reference：IR）とを安全に結びつけるためのセキュリティ要件
- 生体登録情報の保管や比較の際に用いる生体認証のシステム・アプリケーション・モデル
- 生体情報の処理中における個人のプライバシー保護に関するガイダンス

（5）ISO TS 12812 シリーズ（モバイル金融サービス）の概要

ISO 12812 は、モバイル金融サービスの提供および運用管理において、相互運用可能で安全なシステムとなるために必要な対策を示した規格である。ISO/TC 68（金融サービス）委員会が作成した。パート 1 から 5 までの 5 パート構成になっている。それぞれのパートの表題は次の通りとなっている：

パート 1（国際標準：IS）：一般的なフレームワークについて、
パート 2（技術標準：TS）：モバイル金融サービスにおけるセキュリティとデータ保護、
パート 3（技術標準：TS）：金融アプリのライフサイクルマネジメント、
パート 4（技術標準：TS）：個人に支払うモバイル決済、
パート 5（技術標準：TS）：ビジネスとして用いるモバイル決済。

なお、本文 6 節にある、ISO 5158 にて直接引用されている、ISO TS 12812-2 は、ISO 12812 規格のパート 2 にあたり、モバイル金融サービスにおける特にセキュリティとデータ保護をテーマとした規格である。この規格は、モバイル金融サービスの開発者や提供業者が、既存のセキュリティポリシーに従い、相互運用可能なセキュリティメカニズムの評価・選択を支援することを目的としている。もちろん、モバイル金融サービスの利用者にとっても、セキュリティ要件と考慮事項がどのように作用するかを理解することは重要であり、その意味では有益な規格となっている。

具体的な記載内容は以下の通り：

- モバイル金融サービスを運用する際のセキュリティの枠組み。枠組みには、脆弱性、脅威及び対策の分析を含む。
- モバイル金融サービスをセキュアな環境で運用するための最小限の要求事項。
- モバイル端末の認証、金融メッセージの交換、外部認証において用いる暗号プロトコルとメカニズム。
  - モバイル金融サービスのエンド・ツー・エンドでのセキュリティ要件
  - エンド・ツー・エンドのセキュリティ要件
  - セキュリティ認証
  - モバイル電子署名および PKI（公開鍵基盤）
- モバイル金融サービスにおけるセキュアな認証を行う際の相互運用性の問題。
- 機密データ保護のための推奨事項。
- 国内法および規制（例：マネー・ローンダリングおよびテロ資金供与防止対策（AML/CFT））の実施に向けたガイドライン。
- セキュリティ管理に関する考慮事項。