JICSAP
一般社団法人 ID認証技術推進協会

利用シーンに応じた
『顔認証』導入ガイドライン

Version 1.01

一般社団法人 ID 認証技術推進協会（JICSAP）

2023 年 6 月 2 日

公開・更新履歴

更新日	バージョン	更新内容
2023 年 6 月 2 日	1.0	新規作成、一般公開
2024 年 2 月 29 日	1.01	・ 理解補助の目的にて、適用事例（「サービスにおける IV＋UI＋UV の実施例」表）を追加 「2. 顔認証とは - 2.1 顔認証の概要 - 2.1.1 本人認証について」 ・ 現行法律にあわせた記載表現の改訂 「4. セキュリティ対策 - 4.2 個人情報保護法を満たすための対策 - 4.2.1 個人情報の管理に関する一般的な対策」

■商標について
・本書に記載されている会社名、製品名等は、各社の商標または登録商標です。

■免責事項
一般社団法人 ID 認証技術推進協会（JICSAP）は、本ガイドラインに含まれるすべての事項につき、いかなる表明も保証も行いません。本ガイドラインを利用する者は、自己の責任と負担において本ガイドラインを利用するものとし、協会は本ガイドラインの利用により関連事業者、利用者、その他第三者に生じた損害・損失・負担等の一切の結果についていかなる責任も負わず、本ガイドラインを利用する者は協会に対していかなる責任の追及も行わないものとします。

■注意事項
・本書の内容は発行時点のものであり、予告なく変更する場合があります。
・本ガイドラインの記載内容は 2023 年 5 月 10 日時点の情報に基づきます。
・出典を明記していない図表等は、JICSAP が本ガイドラインのために作成したものです。
・本書の内容を JICSAP の許可なく、複製・転載することを禁止いたします。

■本ガイドラインの理解をより深めるために
JICSAP では「本人認証技術」の考え方を整理する目的で、下記のガイドラインを発行しています。本ガイドラインと併せてお読みいただくことで、より一層理解を深めていただけるかもしれません。
・「本人認証技術導入ガイドライン【基本知識編】」（認証技術部会編、2019 年 10 月）
・「本人認証技術導入ガイドライン【サービス設計編】」（認証技術部会編、2022 年 12 月）
https://jicsap.com/

目次

1. はじめに 5
1.1 本ガイドラインの目的と想定読者 6
2. 顔認証とは 7
2.1 顔認証の概要 7
2.1.1 本人認証について 7
2.1.2 顔認証による本人認証について 8
2.2 顔認証システムの概要 8
2.3 顔認証を導入する利点 10
2.3.1 利用者の利点 10
2.3.2 事業者の利点 11
2.4 顔認証導入時の留意点 12
2.4.1 初めて導入する場合＆知識認証・持ち物認証から転換する場合 12
2.4.2 その他の留意点 12
2.5 顔認証技術とプライバシー 13
2.5.1 顔認証とプライバシー保護 13
2.5.2 プライバシー保護に対する諸外国の対応 13
2.5.3 プライバシー保護に対する日本の対応 15
2.6 顔認証技術の評価指標 15
2.6.1 1:1 認証と 1:N 認証 15
2.6.2 評価指標 16
3. 顔認証導入時の検討事項 19
3.1 顔認証の用途 19
3.1.1 顔認証による本人確認（IV：Identity Verification） 19
3.1.2 顔認証による利用者識別（UI：User Identification） 19
3.1.3 顔認証による利用者検証（UV：User Verification） 20
3.2 必要な認証精度 21
3.2.1 ユーザビリティとのトレードオフ 21
3.2.2 誤受入識別率と誤拒否識別率の関係 21
3.2.3 リスクに応じた認証精度の設定 22

3.2.4 性能要件に応じた認証精度の設定 22
3.2.5 認証精度の検討例 23
3.3 対象ユーザー数 24
3.4 必要な処理速度 25
3.5 認証距離と利用者の移動速度 26
3.6 ゲートの有無 27
3.6.1 ゲートの定義と有無について 27
3.6.2 扉の有無について 27
3.6.3 顔認証にて通行の許可を行う場合の留意点 27
3.6.4 鉄道利用時の考察 28
3.7 認証する機器 28
3.8 認証する場所 29
3.9 マスク着用の有無 29
3.10 サービスの提供範囲 30
3.10.1 単一事業者内での顔認証サービス 30
3.10.2 複数事業者に跨る顔認証サービス 30
3.11 マルチベンダー対応 33
4. セキュリティ対策 34
4.1 認証技術によるセキュリティ対策 34
4.1.1 認証技術とセキュリティ対策 34
4.1.2 顔認証技術特有の対策例 35
4.2 個人情報保護法を満たすための対策 36
4.2.1 個人情報の管理に関する一般的な対策 36
4.2.2 顔画像特有の対策や注意点 37
4.2.3 個人情報保護と顔画像の取り扱いに関する参考文献 39
4.3 システムによるセキュリティ対策 39
4.3.1 セキュリティ対策の考え方 39
4.3.2 セキュリティ対策の種類と機能 40
4.3.3 セキュリティ対策の例 41
4.3.4 セキュリティ対策の決定 43
4.3.5 システムのセキュリティに関する参考文献 43
5. 顔認証に対応したシステムの事例 45

5.1 決済システムの例.....45
5.2 入出場ゲートシステムの例.....46
5.2.1 空港での出帰国手続（航空会社、空港会社管理）.....47
5.2.2 空港での出帰国手続（出入国在留管理庁管理）.....47
5.2.3 鉄道の改札機とバス乗降システム.....48
5.3 公共系システムの例.....50
5.3.1 マイナ保険証の本人確認.....54
5.3.2 マイナンバーカード交付時の本人確認.....55
5.4 本人確認システムの例.....56

1. はじめに

私たちが「本人認証」を行う場面は、世の中に沢山ある。銀行の ATM でキャッシュカードと共に暗証番号を入力すること、オフィスに入室する際に ID カードをかざして扉を開けること、病院で保険証や診察券を提示して受診すること、海外に行く際にパスポートで本人を確認して出国することもその一つである。「本人認証」を行う場合に必要とされる手続きは様々である。その中で究極の「本人認証」となるのは、人類全てがユニークに持っている「生体認証」である。

「生体認証」の一つである「顔認証」は、指紋認証や静脈認証のように機械に手を乗せることもなく、また虹彩認証のように機械をのぞき込む必要のない上に非接触で利用でき、利用者からみれば安心で手間の少ない「認証方式」である。また管理する側からすれば、顔認証の精度は高く、顔という他人に貸し出せないものを使用することで高いセキュリティを維持することができるメリットもある。昨今のご時世も踏まえマスクをしたままでも認証できるものが出てきており、現在の顔認証技術を用いるなら、スパイ映画などの変装もちゃんと他人だと判定できるはずである。

一方、容姿をカメラで撮影される仕組みに拒否反応を起こす人もいると思われる。本人に許諾を得ることなくカメラに撮影され、行動をトレース（追跡）されているのではないか、プライバシーの侵害だ、だから顔認証は嫌だという考えにつながっている人も大勢いると思われる。しかし、本人に許諾を得ることなく撮影されるというのは全くの誤解である。最初にはっきりさせておきたいことは、利用者が自分の意思で、すなわち本人が許諾を行い能動的に「顔」で認証を行う「顔認証」と、防犯カメラなどで自分の意思ではなく本人の許諾を得ないまま受動的に「顔」を照合される「防犯などへの応用」とでは、同じ技術をベースにしていたとしても、全く異なる性質のものだということである。本ガイドラインでは、利用者が自分の意思で顔情報を登録し、その顔情報とカメラに撮影される本人の「顔」の情報を照合し利用者自らが利用するもの、そしてそれが利用者による合意の基に行われる行為を「顔認証」として定義し扱うこととする。

「顔」が個人の ID として用いられる社会が想定される一方で、その実現のための技術や方法は多様化している。一般社団法人 ID 認証技術推進協会（JICSAP）では交通・流通をはじめ、想定される各利用場面を対象に、顔認証の導入要件や遵守すべき/揃えておくべき要件を洗い出し、現在稼働しているシステムに関する特性調査・分析を行ってきている。

本ガイドラインでは、各種利用シーンに応じた「顔認証」の導入における要件等に関しまとめ、これから「顔認証」を導入しようと思われている方々への指南となるべく作成した。ぜひお手に取っていただき、参考としていただければ幸いである。

1.1 本ガイドラインの目的と想定読者

本ガイドラインは、本人認証を行うシステムを導入済みの企業・組織が顔認証に対応する、または新規に本人認証を行うシステムを導入する企業・組織が顔認証に対応しようとする際に、参考となるべく情報を取りまとめたものである。

また本ガイドラインでは、顔認証を導入するにあたって、この技術方式にはどのようなメリットがあり、どのような観点で検討し、どのように導入すればよいかについても説明している。

本ガイドラインの想定読者は、「顔認証に対応した本人認証システム」を導入しようとする企業・組織の担当者である。

2. 顔認証とは

本章では、顔認証の概要と特徴について解説する。

2.1 顔認証の概要

現在、様々な分野で生体認証を使ったサービスが導入され始めている。特に顔認証は特殊なデバイスが不要な利点も手伝って、様々な分野で導入が進んできている。顔認証は、利用者の顔情報を利用して認証する仕組みであり、利用者にとっては事前に文字列や記号を記憶したり（知識認証）、特別な認証デバイスを持ち歩く（所有物認証）といった負担がないなど、利便性が高いという特徴がある。

2.1.1 本人認証について

事業者が利用者にサービスを提供する際、その利用者が正当な利用権利を有する本人であることを検証しなければならない場合がある。JICSAP が発行した『本人認証技術導入ガイドライン』の用語に従い、「事業者が、利用者に本人であることを証明させて、検証する」ことを本人認証（User Authentication=UA）と呼ぶ。本人認証は以下の 3 つの機能によって構成され、実行される。

本人認証（UA）=本人確認（IV）＋利用者識別（UI）＋利用者検証（UV）

ここで、本人確認（Identity Verification=IV）は事業者が利用者を「本人であることに間違いがないか」確認する行為であり、利用者識別（User Identification=UI）は事業者が利用者を「特定する」行為である。また、利用者検証（User Verification=UV）は事業者が利用者の「同一性を検証する」行為である。

	サービス登録		サービス利用(本人認証)	
	本人確認(IV)	登録	利用者識別(UI)	利用者検証(UV)
映画のチケット	なし	チケットの発行	チケットの提示(所有)確認	なし
利用者本人限定のコンサートチケット	・Webサイトなどから指名、住所などの利用者個人情報を入力 ・本人確認書類による実在性及び真正性確認	・利用者マスター情報の登録 ・利用者識別情報付きチケットの発行	・利用者識別情報付きチケットによる確認	・本人確認書類(或いは利用者マスター情報)の照合
プリペイドカードでの支払い	― (しないものが多い)	プリペイドカードの発行 (カード番号の付与) 申込書でPIN登録	プリペイドカードの提示 (所有)確認	PIN入力(残高照会やオンライン入金時など)
ID・パスワードでログインする会員サイト	リターンメール(Eメール等)による実在性の確認	ID・パスワードの生成・登録	IDの入力・照合	パスワードの入力・照合

サービスにおける IV＋UI＋UV の実施例

出典： 本人認証技術導入ガイドライン【基本知識編】第一版（一般社団法人 ID 認証技術推進協会、2019 年 10 月）

2.1.2 顔認証による本人認証について

本人確認、利用者識別、利用者検証で用いる認証技術には、「持ち物」による認証（所持認証）、「知識」による認証、「生体」による認証などがある。

「生体」による認証技術のひとつに、顔認識（facial recognition）技術がある。顔認識技術は、顔画像をデータベース上の顔とマッチングさせる技術である。顔認識技術を使って、利用者の「特定」（利用者識別）や利用者の「同一性の検証」（利用者検証）、本人確認をすることができる。

顔認識技術を使って本人認証を行うことを、顔認証（facial authentication）という。

本ガイドラインでは、利用者の同意のもとで顔認識技術を使って本人認証を行う「顔認証」を対象としている（図 1）。顔認識技術を認証以外の用途に使用した例として、例えば防犯カメラによる指名手配被疑者の検出などがあるが、本人認証以外への顔認識技術の適用については本ガイドラインの対象外である。

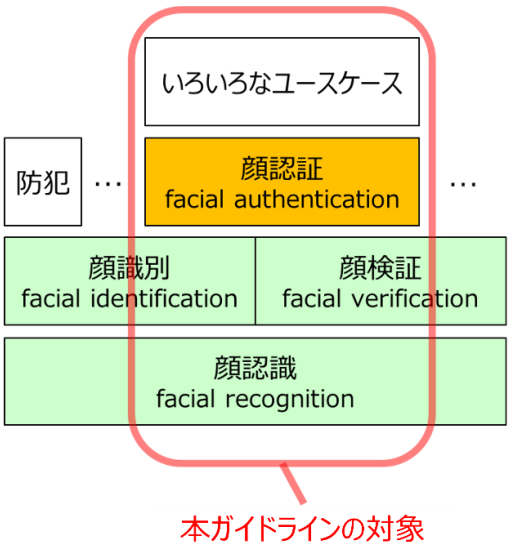


図 1：顔認証と本ガイドラインの対象範囲

2.2 顔認証システムの概要

顔認証システムとは人間の特徴である顔情報から目、鼻、口といった情報を元に人間の個体を認識するシステムのことである。実際の仕組みは提供する企業ごとに異なると思われるが、以下、一般的と思われる方式に関して説明する。

顔認証システムでは、動画や画像から、顔情報を取り出し、特徴点を導き出す。それらの特徴点を突き合わせることで、その顔情報が一致しているかどうかを検証する。

この仕組みを利用し、様々な用途で利用が可能となる。顔認証システムはその実現方法の違いにより、様々な提供形態が存在する。例えば、あらかじめ登録していた顔画像とカメラで撮影している人物が一致しているかを検証したり、免許証の写真とカメラ

で撮影している本人が同一人物であるかを検証するなどの実現方法がある。

前者に関する構成例を図 2 に示す。この場合、顔情報を事前に登録する必要がある。事前に何らかの手段によって、利用者情報と顔情報がデータベースに送られ、データベース上に保管される。このとき、顔情報は顔認証プログラムにおいて照合を行うために特徴点に変換され、利用されることが一般的である。このため、データベースには顔画像もしくはその特徴量もしくはその両方が保持される。カメラで撮影された顔画像は、顔認証プログラムにより、登録されている顔画像と一致しているかどうかが判定される。

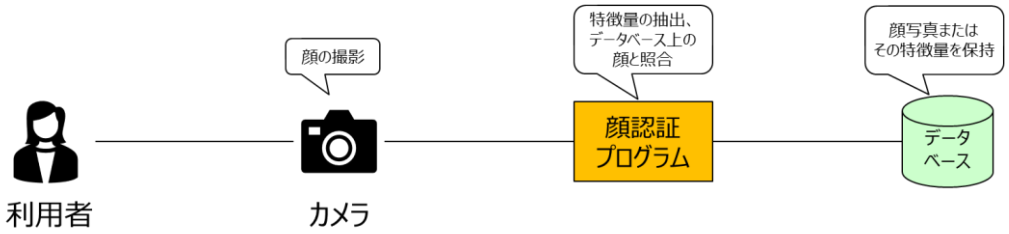


図 2：顔認証システムの概要

顔認証システムでは、人物を特定した後、その本人であるかを認証する 1:1 認証システムと、複数の顔画像の中から誰が撮影されているかを認証する 1:N システムが存在する。1:1 認証システムでは、何らかの手段（身分証などに掲載された顔写真、ユーザー入力による ID 情報、スマートフォン等の固有デバイスからのアクセス、IC カード等）で本人確認する情報と顔画像を送付し、一致しているかどうかを確認する（図 3）。撮影した画像が ID 情報と一緒にサーバーに送られてくると、サーバーは受け取った ID 情報に基づいてデータベースから格納されている顔情報を取り出し、送られてきた顔画像との一致をチェックする。顔画像が一致しているかの判断をサーバー上のエンジンで判断し、OK/NG の判定を返信する。実際のユースケース（利用場面）に応じて、これらの結果をもとに顔認証サービスを提供する。例えば、入退出管理の用途の場合は結果に応じてドアの開閉などの制御に使われる。

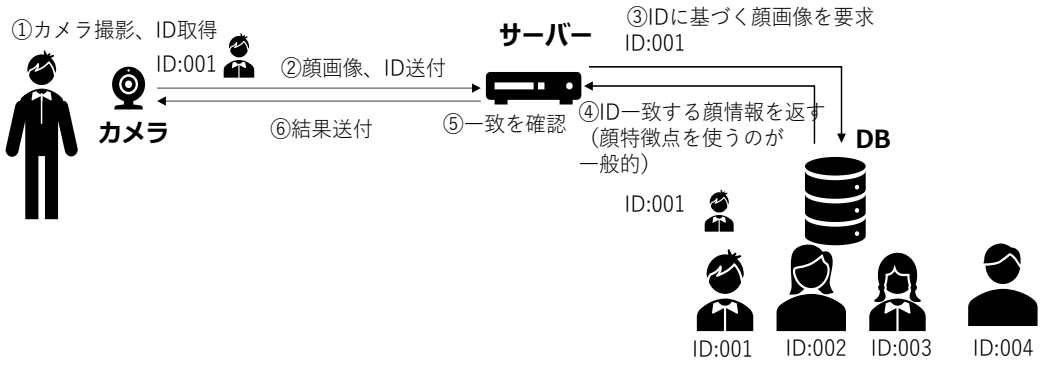


図 3：1:1 照合システム例

1:N 認証システムでは、撮影した顔画像を手がかりとして、あらかじめ登録している複数の顔画像の中から一致している人物を探して認証を行う（図 4）。サーバーに送られた顔画像とデータベースに格納されている顔画像を比較し、一致する顔画像を見つける。ここで一致した顔画像の ID 情報を返送し、顔認証サービスを継続する。このとき、一致する顔画像がない場合もあり、その場合は該当者なしでシステムに返信する。

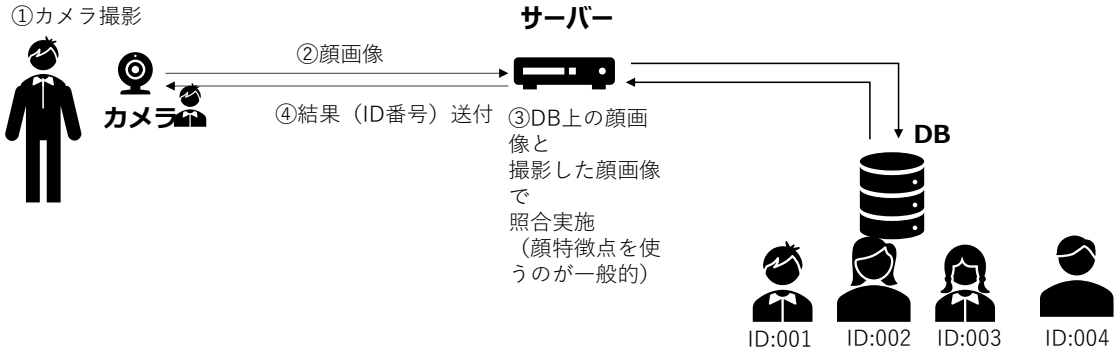


図 4：1:N 照合システム例

2.3 顔認証を導入する利点

顔認証を導入する利点について、利用者の立場、事業者の立場のそれぞれの観点から説明する。

また導入の検討に当たり、本人認証の仕組み自体を初めて導入する場合、知識認証から転換する場合、所有物認証から転換する場合、別の生体認証から転換する場合、別の認証に追加する場合に分けて整理する。

2.3.1 利用者の利点

(1) 初めて導入する場合

後述する知識認証、所有物認証に伴う負担がない。

(2) 知識認証から転換する場合

認証に必要な知識（例：暗証番号）を忘失するおそれがない。忘失に伴う再登録などの負担がない。認証装置に入力するなどの手間がない。

(3) 所有物認証から転換する場合

認証情報や認証機構を保持する媒体（例：IC カード）を紛失（盗難に遭う）、損傷、

忘失するおそれがない。紛失、損傷、忘失に伴う再登録、再発行の手間や媒体費の負担がない。認証装置にかざす、挿入するなどの手間がない。

(4) 別の生体認証から転換する場合

必要な生体部位（例：指紋）を認証機器に認識させる際に、姿勢などの拘束が少なく、円滑な利用が期待できる。同生体部位の状態（発汗、体温高低、指紋の摩耗など）による認識性能に与える影響が少ない。元の生体認証の種類にもよるが、認証装置にかざすなどの手間がなく、同装置への接触が不要で衛生的。

(5) 別の認証に追加する場合

他認証と同時に顔認証を行えるようなシステムとして構築できれば、認証に対する負担が増えない（変化しない）。

2.3.2 事業者の利点

まず、以下の場合によらず、認証装置の設置に自由度がある（また比較的遠隔からカメラによる認証が可能な）ことを利点として挙げておく。

(1) 初めて導入する場合

特筆する事項はない。

(2) 知識認証から転換する場合

利用者が必要な知識（例：暗証番号）を忘失した際に、再登録機能の開発やメンテナンス、再登録に必要な人件費などの負担がない。知識を入手した他人によるなりすましが防止できる。認証に際して顔をカメラに写す行為が必要であるため、犯罪抑止効果が期待できる（悪意を持つ者は顔画像が保存される可能性を嫌う）。手入力などの可動部を排除でき、故障などで可用性が損なわれにくい。

(3) 所有物認証から転換する場合

利用者が認証情報や認証機構を保持する媒体（例：IC カード）を紛失（盗難に遭う）、損傷、忘失した際に、再登録機能の開発やメンテナンス、再登録に必要な人件費などの負担がない。同媒体を確実に利用者に配布するための媒体費、人件費、通信費などが不要。同媒体を入手した他人によるなりすましを防止できる。認証に顔をカメラに写す行為が必要であるため、犯罪抑止効果が期待できる（悪意を持つ者は顔画像が保存される可能性を嫌う）。

(4) 別の生体認証から転換する場合

登録時、確実に本人確認ができる環境であれば、遠隔地からスマートフォンなどを通じた登録が可能。

(5) 別の認証に追加する場合

多要素認証となり、セキュリティレベルを向上できる。既存認証装置と併用しても装置同士が干渉しにくい（冒頭に挙げた設置自由度が特に有効)。

2.4 顔認証導入時の留意点

顔認証を導入する利点と同様、本人認証の仕組み自体を初めて導入する場合、および知識認証や所有物認証から転換する場合について留意点を挙げた上で説明する。また、これらに加えて別の生体認証から転換する場合、別の認証に追加する場合も含めその他の留意点についても整理する。

2.4.1 初めて導入する場合＆知識認証・持ち物認証から転換する場合

知識認証・持ち物認証から転換する場合の利点としては、前記の「なりすまし防止」に優れるがゆえに、知識認証・持ち物認証では可能だった代理認証や、認証知識、媒体の共有・継承ができないことがある。また課題として、認証用登録データの漏洩（なりすましの可能性並びに個人情報漏洩）に懸念があり、仮に漏洩した後で変更ができないこと。（システム構成に依存するが）画像を扱うためネットワーク帯域を確保する必要があること。認証用登録マスターデータ（容量を減らした中間データではなく、元の顔画像）が比較的大容量となり、ストレージ容量を確保する必要があること。認証用登録マスターデータの品質（ピント、露光、ノイズ、画素数など)、バリエーション（枚数、画角、顔の凹凸などの補助データの有無など）で認証性能が変動すること、などがある。

2.4.2 その他の留意点

顔を撮影する環境を安定に保つ必要がある（環境光などの外乱を避ける)。また、利用者（特に若年）の顔の経年変化により利用継続性に制約がある。なりすましに対し一定の耐性があるが、今後の技術進歩により巧妙ななりすまし（立体的な顔模型など）の可能性がある。認証用登録マスターデータの管理・利用については、個人情報保護の観点から利用者同意が必要であり、利用者から要求があった場合は該当データを削除するなどの必要がある。

口元を覆うマスク着用のままでも認証を許容するかどうかは、システム要件によって採否の判断が必要である。また、積極的にマスク着用での認証を拒否するためには検

出機能の追加が必要となる。

認証精度の厳密性については、必要なセキュリティレベルと「2.3.2 事業者の利点」に述べた利点に鑑みて、事業者自身で判断する必要がある。

2.5 顔認証技術とプライバシー

2.5.1 顔認証とプライバシー保護

21 世紀はデータの時代と言われており、データは「新しい資源＝ニューオイル」と位置付けられている。

そんな中、各種センサー、とりわけカメラによる映像取得、そしてその映像データの解析は、技術の進歩とともに様々な場面で、社会的な支援・貢献あるいは事業者等のビジネス創造・拡大につながるものとなっている。

事業者が、カメラ画像等、生活者の情報を取り扱い利用する場合には、個人情報保護法を遵守するだけでなく、生活者のプライバシーや肖像権といった人格的な権利・利益を損なうことのないよう、十分な配慮をすることが求められる。

カメラ画像を利活用する事業の検討・実施、カメラに写り込み得る生活者とのコミュニケーション等において、生活者と事業者間での相互理解を構築するために配慮すべき観点を事業者もしっかり意識、留意する必要がある。特にカメラ画像に基づき個人を識別・特定する目的（顔認証や人物追跡など）でカメラ画像を利活用する場合には、生活者に対するより一層の慎重かつ丁寧な対応が求められる。

被写体となる個人の側から見ると、ソリューション提供企業、ソリューション採用・運用サービス企業による B2B2C（事業者対事業者対消費者）のスキームとなるが、本ガイドラインにのように両者が一体となり指針を公開することには意義がある。

2.5.2 プライバシー保護に対する諸外国の対応

個人情報やパーソナルデータに関する規定は、世界では大きく 3 つのグループに大別されて存在すると考えられる。アメリカ合衆国、中国、EU 域内諸国での対応を例として記載する。

アメリカには当該分野の連邦法は存在せず、各州の州法や各市の条例による制約が主となっている。運用面では一部において、公権力（行政機関）がカメラ画像を使用することに制限が設けられている。

中国においては、セキュリティ 3 法が相次いで制定されている。サイバーセキュリティ法、データセキュリティ法、個人情報保護法である。個人情報を守ることに加えて国家運営、体制を維持することに重きをおいていると言われている。

EU は個人の尊厳をベースに法、規定が制定されている。GDPR（EU 一般データ保

護規制）が有名だが、GDPR はあくまで基本法の位置づけであり、2022 年 5 月には EU データガバナンス法が制定された。また、2022 年 10 月には EU 理事会が EU デジタルサービス法（DSA）を正式に採択。周知期間を経て 2024 年の施行が予定されている。カメラ画像利活用の分野では、欧州委員会傘下の、欧州データ保護会議が指針を既に公表しており、実際の運用事例をベースに利活用の可否を例示している。特に顔認証については、個人の選択に基づき顔認証手段を回避する代替手段（別の認証手段）の提供が義務付けられるなど、厳しい制約が課されている。

■参考情報

＜世界の動き＞
2022 年 10 月、「世界プライバシー会議（GPA）」の中で、以下の件が採択されている。

「顔認識技術」に係る 6 原則の概要
1. 法的根拠：顔認識を利用する組織は、バイオメトリクスの収集及び利用のための明確な法的根拠を持つべきである。
2. 合理性、必要性及び比例性：組織は、顔認識技術の利用に関する合理性、必要性及び比例性を確立し、証明できるようにするべきである。
3. 人権の保護：組織は、特に、プライバシー及びその他の人権に対する不法な又は恣意的な干渉を評価し、保護するべきである。
4. 透明性：顔認識の利用は、影響を受ける個人及びグループに対して透明性のあるものにするべきである。
5. 責任：顔認識の利用には、明確で効果的な責任メカニズムを含めるべきである。
6. データ保護原則：顔認識の利用は、上記で言及した原則を含む、すべてのデータ保護原則を尊重するべきである。

＜ＥＵ域内の動き＞
「欧州データ保護会議（EDPB）」は 2022 年 5 月、「法執行分野における顔認識技術の使用に関するガイドライン」を採択した。

- 法執行分野における顔認識技術（FRT）のユースケースとして下記 6 点が挙げられ、法的側面からの「可否」が提示された。

顔認識技術（FRT）のユースケース	可否
1. 出入国ゲートでの顔認証	○
2. 児童誘拐の被害者の顔識別	○
3. デモ行為を行っている人々やその周辺の映像を DB 化し、その中から暴動を行った人を識別するシステム	×
4. 容疑者の画像と犯罪者データベースとの顔照合による識別	○
5. 公共空間でのリアルタイムのリモート生体識別（顔識別）	×
6. インターネット上で収集した顔画像を DB 化し、警察などのユーザーに顔識別サービスを提供	×

2.5.3 プライバシー保護に対する日本の対応

日本国内においては、二つの角度から当該分野を整理したい。一つは法律による個人情報の正しい取り扱いと、もう一つは個人情報保護法よりも広い範囲に位置するプライバシー配慮である。

前者は個人情報保護法という法、法令遵守である。当該法には、利用目的の特定、利用目的の通知、適正な取得、安全管理措置の義務、利用停止や開示請求への対応などが明記されており、運営事業者はこれを守ることが責務である。

後者のプライバシー配慮に関しては、被写体本人（生活者）への配慮、情報公開の精神をユースケースごとに表記している、経済産業省・総務省 IoT 推進コンソーシアムのカメラ画像利活用 SWG が公表している『カメラ画像利活用ガイドブック』（2022 年 3 月発行）が参考になる。

カメラ画像に関しては、撮影範囲内への写り込みや、設備利用上避けられない経路などがあるため、被写体本人が常に事前の通知を受け、個人情報の取得への暗黙の同意を行っているとは限らない状況で、個人情報の取得が行われる。そのため、事業者は可能な限り誠実な通知を行うことを前提としても、常に「撮影されたくない者への配慮」を行うことが求められる。被写体本人の意図的な行動だけでなく、無意識の行動等も含む膨大な情報が取得されるため、本人が希望・意図する範囲を超えた情報の取得が行われる可能性がある。

そういった不安・不信を払拭するためにも、事業者には透明性のある対応、発信が求められ、法律条文以外の配慮措置の参考となるのが、同ガイドブックである。

すなわち、法律による個人情報の正しい取り扱いと、個人情報保護法より広い範囲に位置するプライバシー配慮を意識した姿勢が、事業者側には求められていると言える。

2.6 顔認証技術の評価指標

2.6.1 1:1 認証と 1:N 認証

認証技術では一般に、ある一つの対象と他の一つ、または複数の参照対象との類似性を評価し、対象同士が同一であるかどうかを判断する。慣例的に、参照対象が一つの場合は 1:1 認証、複数の場合には 1:N 認証と呼ばれるが、認証用の特徴が顔特徴である顔認証の場合であっても同様となる。

1:1 認証では「しきい値」と呼ばれる類似性の基準値との大小比較によって、２つの対象同士が一致しているか否かを判断するが、このような処理の適用例として顔画像による本人認証がある。図 5 では、対象者（左上の青色人物）が A さんであるかどうかを 1:1 認証していることを模式的に示す。

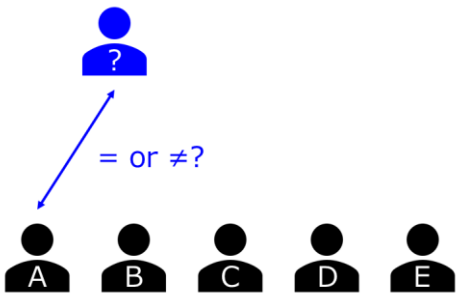


図 5：1:1 認証の例

一方、1:N 認証では複数の参照対象との間の類似性を求める。最も類似しているものを対象と同一であると特定して認証結果とする識別用途、または上位から一定の順位までの類似性をもつ参照対象を候補とする検索用途などの利用例が想定される。例えば、あらかじめ複数の写真が格納された写真用データベースから、自身の写っているシーンを探し出すなどの用途はこの代表例であろう。

また上記の類似性に対して、「しきい値」との比較によって識別結果や抽出候補の有効性を判定し、認証結果とする場合がある。

図 6 では対象者（下段の赤色人物）を A, …, E の参照対象に対して 1:N 認証した(すなわち、A, …, E のうちどれに一番類似するのか？またはどれも類似しないのか？を判定した）結果を求める識別用途の例を模式的に示す。

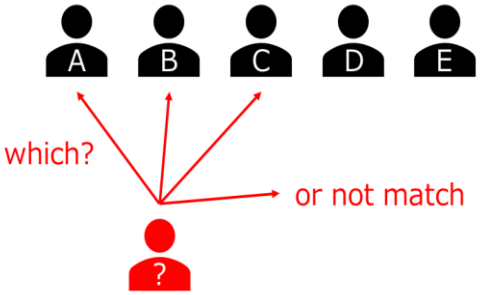


図 6：1:N 認証の例

2.6.2 評価指標

前述のように顔認証技術の一般的用例として 1:1 認証と 1:N 認証とがあるが、これらに対する性能評価指標について、生体認証の性能評価標準である ISO/IEC 19795-1 に定義された指標の一部を用いて、正確性、効率性の観点で表 1 に示す。また、以下ではそれぞれの指標について説明する。

表 1：顔認証技術の性能評価指標例

認証方法	正確性		効率性
	認証	登録	
1:1 認証	FMR （=FRR), FNMR (=FAR)	FTE	Computational workload of biometric comparison
1:N 認証	FPIR, FNIR	FTE	Computational workload for an identification transaction

(1) 1:1 認証の評価指標

認証時の正確性指標 FRR, FAR

FRR（False Reject Rate）：

本人の身元確認要求の照合トランザクションにおいて、誤って拒否する率であり、小さい程、認証時の正確性が高い。

例：正しくは A なのに A ではないと認識してしまう割合。

FAR（False Accept Rate）：

他人の身元確認要求の照合トランザクションにおいて、誤って受理する率であり、小さい程、認証時の正確性が高い。

例：正しくは A ではない人（B,C,D,E）を A だと認識してしまう割合。

登録時の正確性指標 FTE

FTE(Failure to Enroll)：

登録処理を行うべき全対象数に対して、登録失敗した対象数の割合。顔認証処理では、参照用対象（顔画像）を事前に認証可能な形式で登録する必要があるが、画質などの条件によって登録に失敗することがある。一方、一般に登録用画像データは画質良好とする場合が多いが、この場合には FTE は少ないほど良い指標であると考えられる。

処理の効率性 Computational workload

1 回の認証処理を行うために必要となる計算機の処理量を示す。

処理手法の観点からはこの値が小さい方が高効率とみなされるが、使用ハードウェアの処理効率性にも依存する量となる。そこで、代わりに使用ハードウェアと対象データを固定した場合の処理時間を用いることがある。

(2) 1:N 認証の評価指標

認証の正確性指標 FPIR、FNIR

FNIR (False-Negative Identification-error Rate)：

システムに生体情報を登録した利用者による識別トランザクションにおいて、システムの出力が利用者の正しい身元情報を含まない率。

例：図 6 において、登録済みの人 A を A ではないと認識する割合。

FPIR (False-Positive Identification-error Rate)：

システムに生体情報を登録していない利用者による識別トランザクションにおいて、システムの出力がいずれかの身元情報を含む率。

例：図 6 において、D や E を登録済みの人 (A,B,C) のいずれかだと認識する割合。

登録処理時正確性指標 FTE

一般に登録可否確認を行う対象数は多いものの、1:1 認証における FTE と同じ。

認証の効率性　Computational workload

複数の参照対象に対して、1 回の認証（識別、または検索）処理を行うために必要となる計算機の処理量を示す。処理手法の観点からは、この値が小さい方が高効率とみなされるが、使用ハードウェアの処理効率性にも依存する量となる。そこで、代わりに使用ハードウェアと対象データを固定した場合の処理時間を用いることがある。

3. 顔認証導入時の検討事項

本章では、既存のシステムに顔認証を導入する、または新規のシステムを顔認証に対応させる際に検討すべき事項について説明する。

3.1 顔認証の用途

顔認証は、サービス登録時の本人確認に用いるほか、利用者識別や利用者認証に用いることもできる。

3.1.1 顔認証による本人確認（IV：Identity Verification）

事業者が利用者を「本人であることに間違いないか」確認する行為である。

本人確認書類（運転免許証、マイナンバーカード等）の提示などを通じて利用者の身元識別情報を参照し、顔認証を用いて利用者の「実在性」と「真正性」を確認する。その後、届け出内容に従って利用者識別情報と利用者との紐付けを行い、利用者マスター情報として登録（＝利用者登録）する。

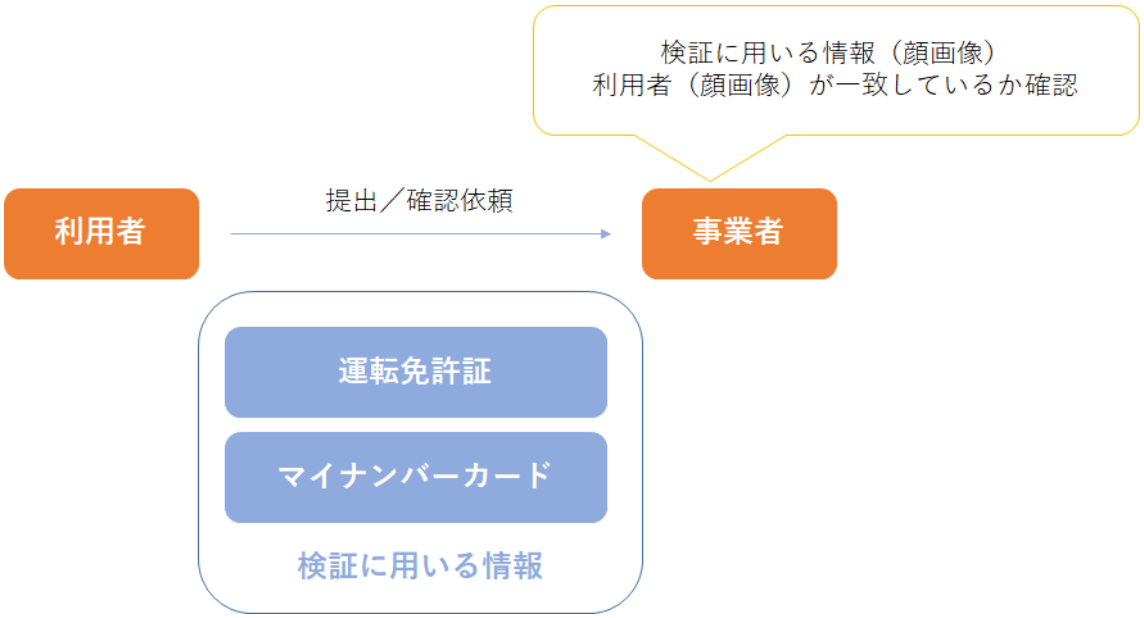


図 7：顔認証による本人確認の例

3.1.2 顔認証による利用者識別（UI：User Identification）

事業者が利用者を「特定する」行為である。

事業者は、利用者が提示した利用者識別情報（顔画像）をシステム上で照合し、利用者の特定とサービス等の条件を満たしているかについて確認する。

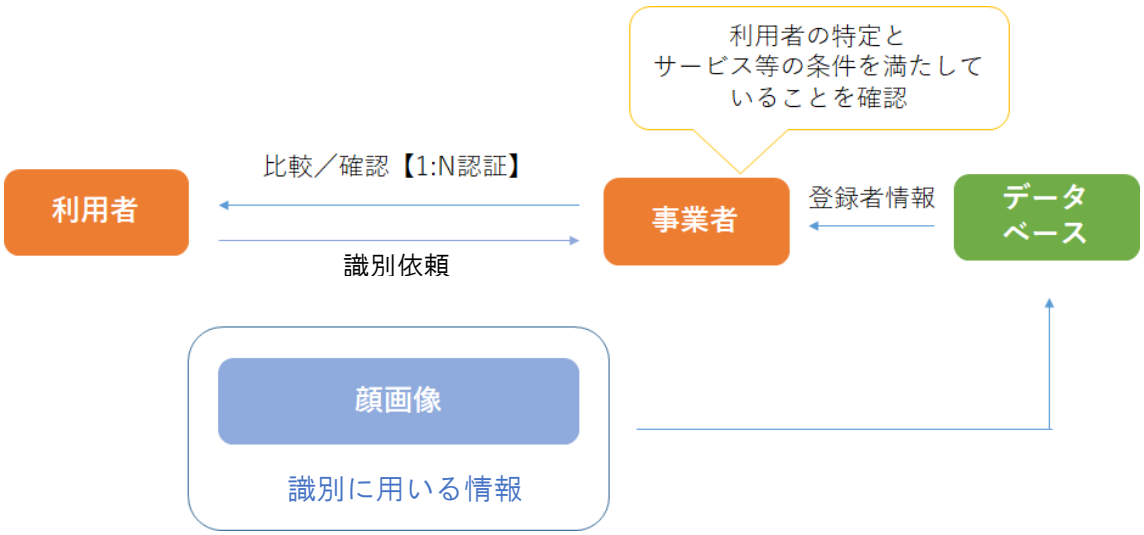


図 8：顔認証による利用者識別の例

3.1.3 顔認証による利用者検証（UV：User Verification）

事業者が利用者の「同一性を検証する」行為である。

事業者は、利用者が提示した利用者検証情報（顔画像）とデータベース等にある検証者情報との照合（一致）を実施し、同一性を確認する。

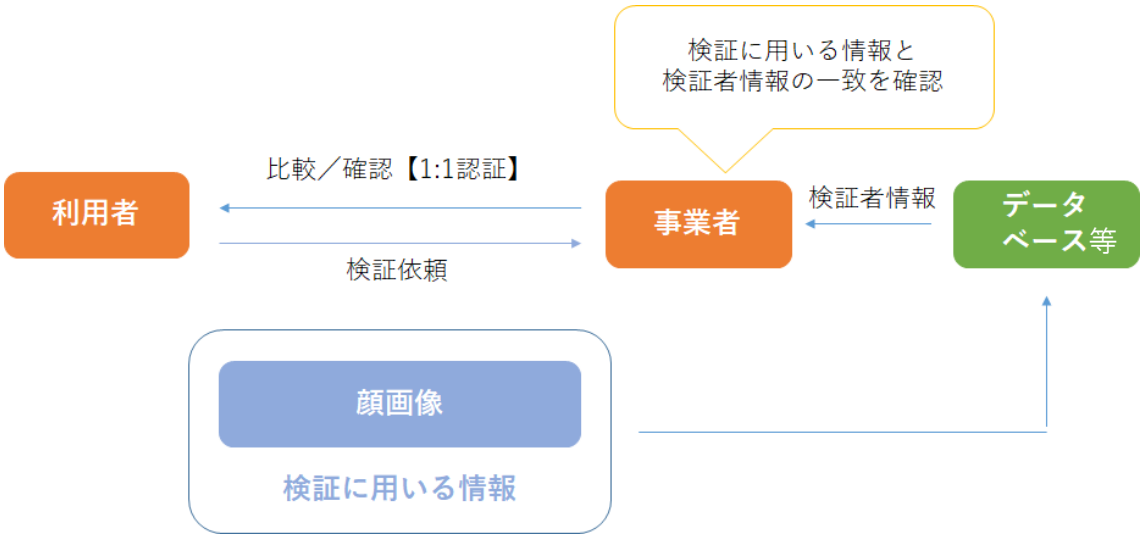


図 9：顔認証による利用者検証の例

3.2 必要な認証精度

3.2.1 ユーザビリティとのトレードオフ

顔認証で必要とされる認証精度は、ユースケースやサービスの要求によって異なる。例えば、利用者の銀行口座からの出金に顔認証を利用する場合は、正規の利用者以外の第三者による利用を許可しないこと、すなわち FAR（FNIR）の低いことが要求される。一方で、例えばアミューズメントパークの園内施設を利用する際に顔認証を利用する場合は、必ずしも低い FAR（FNIR）を求めないという判断を事業者がすることも可能である。

ATM での出金のように認証誤りが許容しがたい場合は、利用者識別を顔認証以外の方法（例：キャッシュカードによる持ち物認証）で行い、さらに利用者検証を顔認証に加えて他の方法との組み合わせ（例：キャッシュカードによる持ち物認証や暗証番号による知識認証＋顔認証による多要素認証）で行うようにすることで、認証精度を高めることができる。

一方で、園内施設の利用のように認証誤りが一定程度まで許容できる場合は、顔認証による利用者識別だけで、（顔パスで）サービスの利用を許可することでユーザビリティを向上させることができる。

一般に、高い認証精度を求めるとユーザビリティ（使い勝手）は低下する。FAR と FRR（FPIR と FNIR）はトレードオフの関係にあるので、例えば低い FAR を求めると FRR が高くなり、正規の利用者が利用を拒否されてしまう確率が高まる。また、利用者に静止してもらったりマスクを外してもらったりすることで認証精度を高めることもできるが、これらもユーザビリティを低下させる要因となる。顔認証以外の認証手段（例：キャッシュカード）と組み合わせる場合もユーザビリティが低下する。

認証精度とユーザビリティはトレードオフの関係にあるので、ユースケースやサービスの要求と提供したいユーザビリティのバランスを考慮して、必要な認証精度を決定する必要がある。

3.2.2 誤受入識別率と誤拒否識別率の関係

物理認証や知識認証と異なり、顔認証には認証失敗も起こり得ることが特徴である。

具体的には、他人を登録した本人と間違えて受け入れる、登録した本人を他人と間違えて拒否する場合がある。この特徴のために顔認証では、誤受入識別率と誤拒否識別率によって認証精度を定義している。

これら顔認証の認証精度を決定するに当たっては、利用されるユースケースやサービスが求める使用要件への考慮が必要である。

顔認証を安心・安全に利用するには、誤受入識別率をできる限り低くする必要があ

る。しかし、誤受入識別率と誤拒否識別率はトレードオフの関係であることから、顔認証を登録した本人が拒否される率も高くなる。結果、認証リトライ（改善後の再撮影）や別の認証手段を併用するなどの必要が生じ、利便性の低下が見込まれる。

顔認証にとって、「認証精度を高くする＝誤受入識別率を低くする」ことは、利便性とのトレードオフでもある。

これらのことから、顔認証の認証精度を決定する要素としては、「誤認証による個人情報の流出や認証後の権限発動によるリスク」と、「顔認証をどのように実行しなければいけないか、その利用環境における性能要件の難易度」が考えられる。

3.2.3 リスクに応じた認証精度の設定

顔認証技術を利用する事業者が、利用者の顔情報そのもの、あるいは紐づけられた情報のうち何を利用するか、加えて顔認証を行った結果により提供する価値やサービスは何か、によってリスクは想定（抽出）できる。

認証行為や認証結果によって、利用者の個人情報などが流出する、取引や与えられたサービスが他人に利用されることで大きな損失につながる場合には、認証精度を高くすべきである。

それに対して、個人を特定せず、個人情報を利用しない、認証結果も利用者への提供や社会へ公開せず、被認証者の損失や社会的損失が見込まれない場合は、認証精度を低くしてもよいと考える。

表 2：「認証責任の重さ」の判定要素

	認証責任の重さ	
	軽い	重い
認証の目的	捜索や統計	個人情報の引き出し
決済の有無	無	有

3.2.4 性能要件に応じた認証精度の設定

顔認証を実行する環境において、認証に要する性能要件の難易度が高いほど、認証精度は低くなる。すなわち、認証の速度、認証登録の量、認証動作の連続実行、認証対象の移動有無が、認証精度に影響する。

利用したい環境や利便性向上の観点から求められる性能要件の難易度が高い場合、他の認証方式との組み合わせや、求められる認証精度の精査などが必要となる。

認証装置が個人向けで、認証対象が動かず、認証操作も応答を前提とした利用であれば、認証精度を高く設定できる。また、認証装置が広範囲を対象に連続認証し、認証対象が動き、認証操作もできない利用であれば、認証精度は低くなる。

後者のような利用要件であっても、多くの認証対象者の中から認証登録者を探して

検知した回数を記録することが要件にあれば、認証精度が低くてもリスクを発現する可能性は低く、そして誤認識が許容できる範囲であれば運用は可能である。

一方、同じ利用要件でも、認証登録者の権限を利用し、決済を実施する必要がある場合には、認証精度に合わせて提供する価値や権限を低減することや、顔認証に近しい他の認証方式との組み合わせ利用を検討することになるだろう。

表 3：「性能要件の難易度」「実行できる認証精度」の判定要素

	性能要件の難易度	
	低い	高い
	実行できる認証精度	
	高い	低い
要求認証速度性能	遅い	速い
認証登録の量	少ない	多い
認証動作の連続性	無	有
認証対象の移動有無	無	有

3.2.5 認証精度の検討例

これまでに挙げたポイントを踏まえ、各用途と場合に応じて、認証精度について検討した一例を以下に示す。

- ATM での出金：誤りが許容できない場合、他の利用者識別手段と顔認証を含む多要素認証（顔認証は静止、かつ、マスクを外す）を組み合わせる
- 電子マネーの利用：誤りが許容しがたい場合、他の利用者識別手段と顔認証（静止、かつ、マスクは着用していてもよい）を組み合わせる
- 社員の入退室管理（入退館ではなく入退室）：一定の誤りが許容できる場合、顔認証のみ（静止、かつマスクは着用していてもよい）とする
- 定期券の利用：事業者のリスク判断により一定の誤りが許容できる場合、顔認証のみ（静止しなくてもよい、かつ、マスクは着用していてもよい）とする
- 園内施設の利用：事業者のリスク判断により一定の誤りが許容できる場合、顔認証のみ（静止しなくてもよい、かつ、マスクは着用していてもよい）とする

上記のように、利用シーンに応じたリスク分析を行い、他の利用者識別手段や認証と組み合わせることも検討する。また、顔認証自体の認証精度やマスク着用の有無についても考慮して、認証精度を決定する必要がある。

3.3 対象ユーザー数

代表的な利用シーンにおいて顔認証が対象とするユーザー数は、1 システムにおいておおむね下記のように想定する。

表 4：対象ユーザー数

1:N の利用シーン	例	ユーザー数（1 システム）
流通系（決済）	・顔認証レジ ・交通系 IC の連携	数千人（小規模） ～数千万人（大規模）
金融	・銀行登録時	数千人（小規模） ～数千万人（大規模）
空港	・パスポート作成	数万人（小規模） ～数千万人（大規模）
オフィスソリューション／施設・イベント	・入退ゲート	数十人（小規模） ～数十万人（大規模）
IT システムログオン	・クラウドへのログオン	数十人（小規模） ～数千万人（大規模）

3.4 必要な処理速度

ここで説明の対象とする「処理速度」は、利用シーンの流れの中で行われる顔認証プログラムによる認証速度のみを指すこととする。また一般的には多くのユースケースにおいて顔認証時の対象は一人であると想定されるため、一度に認証する人数は 1 名を前提とする。

顔認証で必要とされる処理速度は、ユースケースやサービスの要求によって異なる。代表的な例としては、以下が想定される。

- 複数の利用者が列を成し、歩きながら連続で認証していくケース
  （利用シーン例：鉄道改札での入場並びに出場）
- 複数の利用者が待機する中、特定の利用者が立ち止まった状態で認証するケース（利用シーン例：小売店での決済）
- 特定の利用者が立ち止まった状態で認証し、その後作業を行うケース
  （利用シーン例：銀行 ATM での本人認証）

鉄道の改札のように、不特定多数の人が次から次へと利用する用途では、認証自体が目的となり、また流れを止めることはサービスに支障をきたしてしまうため、速い処理速度が求められる。

次に、特定の利用者が立ち止まった状態ではあっても、小売店レジでの決済用途など複数の利用者が後に控えており、かつ認証行為が手続きの最後に行われる場合。この場合も速い処理速度は求められるが、決済などセキュリティ性の高い利用シーンにおいては、処理速度よりも認証の確実性を重視することが望ましい。

また、銀行 ATM のように認証後にも操作を継続する用途では、認証後の操作が目的であり、認証の処理速度のみがサービスに支障をきたすわけではないため、認証時に多少の時間を要したとしても許容される。銀行 ATM のようにセキュリティ性が求められる利用シーンにおいては、確実な認証を最優先とすることが重要である。

一般的に、必要な処理速度はユースケースやサービスの要求によりおおむね決定されるが、ユースケースに応じてその指標（ゲート系はスループット、端末系は処理時間）は異なる。なお、サービスに支障をきたさないためには、処理速度に加え前後のユーザーインターフェースや、サービス利用時の周知など利用者への分かりやすい案内も重要となるため、システムと運用の両面から検討することが効果的である。

3.5 認証距離と利用者の移動速度

認証距離と利用者の移動速度の分布は利用シーンによって異なるため、以下の表にまとめる。

表 5：認証距離と利用者の移動速度

利用シーン	認証距離	利用者の移動速度
交通系 鉄道の改札（乗車券）	約 1.5m （改札機の入口から顔認証機器までの距離）	徒歩の速さ 秒速 1.0～1.6m/s
交通系 駅のチャージ機	0.5～1.0m	立ち止まった状態で認証
交通系 バスの精算機	0.5～1.0m	徒歩の速さ 秒速 1.0～1.6m/s
空港 出国・入国・チェックイン・税関	数十 cm	立ち止まった状態で認証
オフィス 入退場ゲート	0.3～1.0m	徒歩の速さ 秒速 1.0～1.6m/s
IT システムログオン	数十 cm	立ち止まった状態で認証
小売店 セルフレジ・有人レジ	1.0m 程度	立ち止まった状態で認証
銀行 ATM 取引	0.3～1.0m	立ち止まった状態で認証
銀行 ATM 口座開設	50cm 程度	立ち止まった状態で認証
施設 レジャー施設・ホテル	1～2m 程度	徒歩の速さ 秒速 1.0～1.6m/s

3.6 ゲートの有無

3.6.1 ゲートの定義と有無について

本ガイドラインでは、「ゲート」について以下のように定義する。

ゲートとは、駅、建物、イベント会場等での入口/出口に設置される物理的な機器を指す。「通行に対し、扉にて通行を制御するタイプ」と、「スペース、一時設置等の条件があり、扉が無く通行に対しある程度の抑止をするタイプ」がある。”

3.6.2 扉の有無について

顔認証により通行の許可を行う場合、前項で説明した通り、必ずしも扉があるとは限らない。

(1) 扉がある場合

顔認証の処理の結果をゲートと連動させ、ドアやゲートの案内・表示により通行の許可を促す、または抑止を行う。

(2) 扉がない場合

顔認証の処理の結果をこれと連動する案内・表示器または係員誘導により通行の許可を促す、または抑止を行う。

3.6.3 顔認証にて通行の許可を行う場合の留意点

顔認証は様々なシーンで利用されているが、ゲートの有無に関わらず、以下のような条件が整うとより確実な認証が可能となる。

- 人がカメラの前で立ち止まる。
- 人とカメラ間を一定の距離をとる。
- 顔とカメラを同じ高さとする。
- 顔は正面向きとする。
- 1 人ずつ認証を行う。
- 明るさがある。

スループットが求められる駅やオフィスビル等に設置された扉付きゲートにて顔認証を実施する場合、以下のようなことに留意する必要がある。

- 当人の後方にいる人を認証しないこと。(例：1 人ずつ認証する)
  また、認証する通路が複数通路ある場合、他の通路を通過する人を認証しないこと。
- ゲートを通過する意思がある人だけを認証すること。つまり、ゲート外を横切る人を認証しないこと。
- カメラはゲート天板部に取り付けられる可能性が大きいが、カメラの取り付け位置によって人がカメラを見上げたり、見下ろしたりするような条件下でも認証可能なこと。
- 立ち止まると流動阻害となるため、認証対象者は歩きながら認証が行えることが望ましい。

また、認証 NG でドアを閉じる際のタイミングが遅れると、認証対象者がドアで転倒してしまうケースがあり得るため、認証の判定を出す速度は既存で使用している媒体（IC カード、磁気媒体など）と同等以上にすることが望ましい。

留意点のまとめとして、セキュリティを求める場合は、処理速度よりも確実に認証を行い、入出を管理する方が好ましいと考える。しかし、鉄道利用やオフィスビル等、スループットが求められる場所で使用する場合、流動阻害を起こしてはならないため処理速度が必要である。

3.6.4 鉄道利用時の考察

鉄道利用の場合、運賃収受に直結するため本人以外を認証してはならないという必須条件がある。また、不特定多数の鉄道利用者が様々な駅で乗降するため、顔登録の方法、データの持ち方等の課題がある。そのため、実現に向けては小規模な実証実験から開始し、課題解決をしていく進め方が望ましいと考えられる。

3.7 認証する機器

顔認証を行う機器は、①ユーザーの所持端末等の場合、②事業者が施設等に設置する機器、の大きく 2 つに分けられる。前者①は、スマートフォン（スマホ）に搭載される顔認証が一例であり、インカメラに顔を写し、その写った画像と登録されている顔のデータを照合することで本人を認証する。後者②は、オフィスの入退室管理や国際空港のゲート等の顔認証機器がポピュラーであるが、最近は顔認証決済を行う機器や、マイナンバーカードを保険証として活用する場合の顔認証付きカードリーダー等も登

場している。

機器の認証方式としては、人の顔を平面として捉える 2D 顔認証（2 次元）と人の顔を立体的に捉える 3D 顔認証（3 次元）がある。3D 顔認証ではカメラと赤外線の 3D センサーを使い、顔の凹凸までをデータ化するため、2D 顔認証よりもセキュリティは高い。

・カメラ機能
・ディスプレイ部
・電源、外部 I/F
・顔認証機能(アプリ)

図 10：事業者が設置する顔認証機器のイメージ

3.8 認証する場所

顔認証する場所は、屋内が一般的であるが、屋外（半屋外を含む）での顔認証も可能である。ただ、屋内の場合でも極端に暗い場所や明るい場所、逆光となる場所では注意が必要である。同じように屋外の場合でも、雨が降ったり直射日光が当たったり、逆光になったり、夜であったりと、顔を撮影する場所の環境は変化するため、認証精度（顔認証の成功率）を見極めながらの導入が必要となる。

3.9 マスク着用の有無

マスクをつけたままの対象者を顔認証する場合は、認証の成否において NG となる割合が高くなる傾向があるため、顔認証の利用シーンにおいて要求される精度等に対応できる顔認証システムが必要となる。例えば園内施設への入場などゲート利用時に大人数で高速処理が要求される利用シーンや、ATM や POS/決済における高精度の認証が要求される利用シーンなど、それぞれに応じて利便性とマスク着用時の認証精度の影響を慎重に検討して、顔認証システムを設計する必要がある。また、高速、高精度の認証が要求される場合には、マスクを外してもらうか、二要素認証を行うなど工夫が必要な場合もあるので、システム設計において注意する必要がある。

一般的にマスク着用時の認証精度は下がるとされる。さらにマスクの色や形状が認証精度に影響を与える可能性もあるので、利用者に事前の周知・説明を行うことも有用である。

3.10 サービスの提供範囲

顔認証サービスは、単一のサービス事業者・組織内だけで提供する場合と、複数のサービス事業者・組織に跨って提供する場合がある。例えばパスポート（旅券）は、複数の国に跨って、顔による本人確認機能を提供している。

3.10.1 単一事業者内での顔認証サービス

一般に顔認証技術は、撮影した顔画像から顔の特徴量を抽出し、データベースに保存している特徴量と比較・照合することによって認証を行う（図 11）。単一のサービス事業者・組織内だけで顔認証サービスを提供する場合は、このようなシステムで十分である。

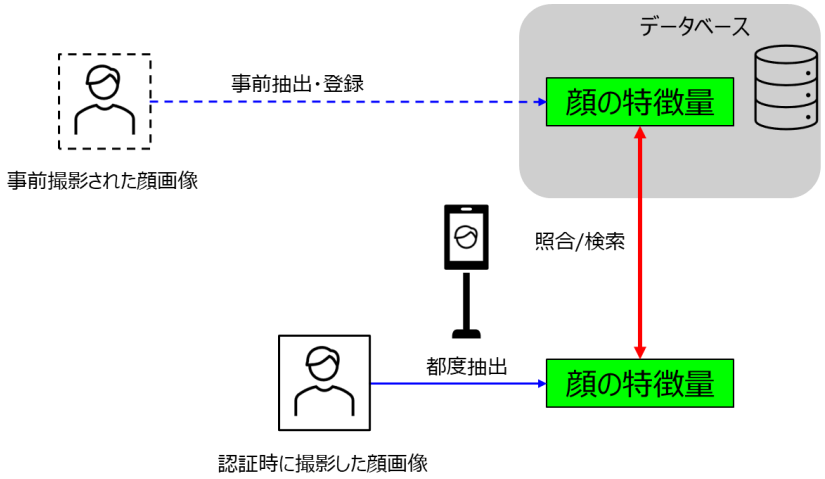


図 11：データベース上の顔の特徴量との比較

3.10.2 複数事業者に跨る顔認証サービス

顔画像から顔の特徴量を抽出する方法や抽出される特徴量は、各サービス事業者が採用する顔認証技術によって異なり、相互に互換性はない。事業者・組織を跨いで顔認証を行うとき、すべての事業者・組織が同一の顔認証技術を採用しているのでない限り、顔認証技術ごとに特徴量を抽出する必要がある。また、顔認証サービスを提供する事業者・組織や採用する顔認証技術の将来的な増加にも対応できることが望ましい。

これを実現するには、いくつかの方法がある。

(1) 顔画像媒体持参方式

一つは、認証済みの顔画像を利用者本人が持ち運び、そこから都度特徴量を抽出して、撮影した顔画像の特徴量と比較・照合するという方法である（図 12）。例えばパスポートやマイナンバーカードは媒体やカード券面に顔画像が掲載されているため、その顔画像を用いて本人認証することができる。

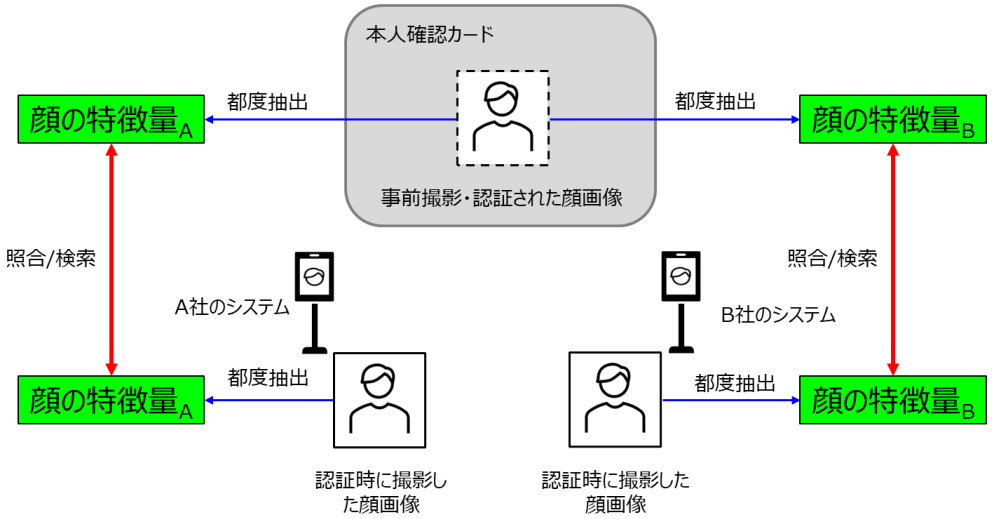


図 12：利用者本人が持ち歩く認証済みの顔画像を使って顔認証する例

(2) 利用者端末内認証方式

顔認証機能を搭載したスマートフォンを用いて、スマートフォン内で顔認証を行い、サービス事業者はその認証結果を信用して利用者検証を行う方法もある（図 13）。例えば FIDO アライアンスが、この方式で Web の認証を行うための仕組みの一つを仕様化している。

この方法は利用者のスマートフォン内で顔認証を行うため、認証精度や不正認証のリスクがそのスマートフォンに依存することに留意する必要がある。

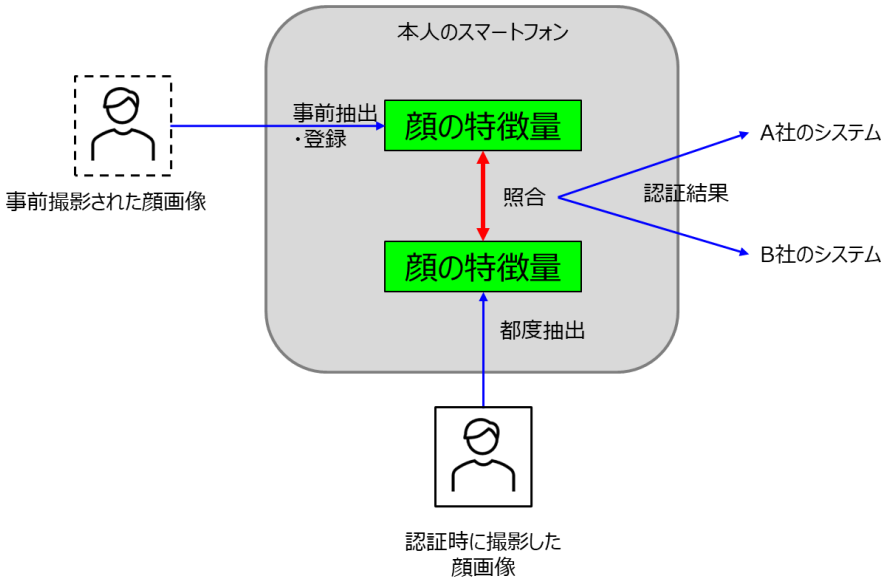


図 13：利用者本人のスマートフォン内で顔認証する例

(3) 顔画像集中保管方式

複数のサービス事業者が結成したコンソーシアムや代表事業者のデータベースに顔画像を保管しておき、その顔画像から各社のシステム向けの特徴量を抽出して、各社のデータベースに保管するという方法もある（図 14）。この方法はシステムが増える度に新たに特徴量を抽出する必要があるが、この仕組みでの顔認証機能の利用を参加事業者内に限定することができる。

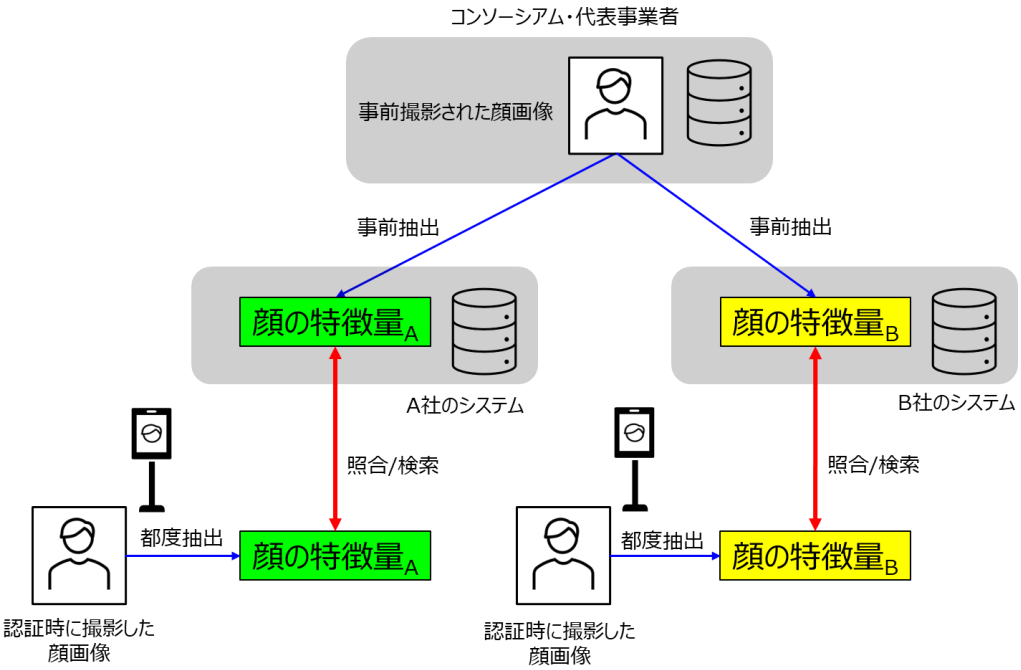


図 14：コンソーシアムなどに顔画像を保管する例

3.11 マルチベンダー対応

サービス事業者の調達戦略上の理由などにより、複数ベンダーの顔認証技術を同時に使用したい場合は、前項で示した「複数のサービス事業者・組織に跨って顔認証を利用する場合」と同様に、使用する顔認証技術ごとに特徴量を抽出する方法を検討する必要がある。その方法として、前項で示したものと同様に、以下が考えられる。

- 利用者本人が持ち歩く認証済みの顔画像を使って顔認証する（顔画像媒体持参方式）（図 12）。
- サービス事業者のデータベースに顔画像を保管し、その顔画像から顔認証技術ごとに特徴量を抽出する（顔画像集中保管方式）（図 14）。

4. セキュリティ対策

4.1 認証技術によるセキュリティ対策

4.1.1 認証技術とセキュリティ対策

代表的な認証技術とそのセキュリティ対策例の一般論を下表に示す。なお、より高いセキュリティ性を要求する場合には、これらの認証技術を組み合わせた認証方法（多要素認証）が用いられる傾向がある。

表 6：認証技術とセキュリティ対策例

	認証技術	概要	例	問題点と対策例
1	知識による認証（知識認証）	なんらかの情報（文字、数字等）をシステムに事前登録し、利用時にユーザーから提示された情報と比較することで認証する方法	・ID、パスワード ・合言葉	認証用知識を知った他人がユーザーとして認証される問題がある。対策は以下など。 ・知識情報用の言葉は、ユーザー関連情報（生年月日、電話番号など）から推測されにくいものを用いる。 ・他人に容易に記憶されにくいように、情報の桁数は極力長くする。
2	持ち物による認証（所持認証）	ユーザー以外は本来所有していないものをシステムに事前登録しておき、利用時に提示された所有物を確認することで認証する方法	・IC カード ・機器固有番号（MAC アドレス、電話番号等） ・ワンタイムパスワード用トークン ・マトリクス認証	所有物を盗用して利用した他人もユーザーとして認証される問題がある。対策は以下など。 ・対象所有物の盗用防止管理。例えば物理的に鍵がかかる場所に保管するなど。 ・対象所有物を複数登録したり知識認証と組み合わせたりして、相互に確認する。例えば IC カードアクセス時に、登録されたモバイルデバイスにアクセス許可用の Web サイトの URL が送信されて確認を行うなど。
3	生体認証	ユーザーの生体情報をシステムに事前登録しておき、利用時に提示された生体情報を確認することで認証する方法	・指紋認証 ・虹彩認証 ・静脈認証 ・顔認証	生体認証に対するなりすましには手間がかかるが、他人の生体情報を模倣した情報提示（偽造物提示）によって他人もユーザーとして認証される問題がある。対策は以下など。 ・情報量を増やしてなりすましに

				くくする。例：指紋認証を複数指で実施する。 ・物理的特性を用いて偽造情報と真の情報とを識別する。

4.1.2 顔認証技術特有の対策例

顔認証技術に用いられる情報はカメラで撮影された画像や映像などであるため、他の生体認証技術と違って、生体情報を読み取るために特殊なデバイスを必要としない。一方でこれらに対する偽造情報（本人の顔写真、顔映像、双子などの類似他人等）をシステムに提示することで、他人を本人として認証させる「なりすまし」（Presentation Attack）が可能となり得る。

このような「なりすまし」を検出する際の性能指標として以下があり、それぞれ値が小さい程性能が良い。

- APCER (Attack Presentation Classification Error Rate)
  偽造情報を真の情報として、誤受入れしてしまう率
- BPCER (Bona Fide Presentation Classification Error Rate)
  真の情報を偽造情報として、誤排除してしまう率

以下には、これら「なりすまし」検出用の対策を示す。

(1) 物理的特性を用いて偽造情報と真の情報とを識別する

本人がシステムに直接撮影された場合と、写真、映像、類似他人が撮影された場合との輝度分布、コントラスト、テクスチャといった画像特徴のわずかな違いを区別することで「なりすまし」を識別する対策がある。この場合、入力デバイスの違いによって以下の分類がある。

・可視光カメラを利用するもの：
機械学習などの手法によって、前述の画像／映像特徴の違いを識別するもの。
特殊な入力デバイスが不要のメリットがあるが、カメラの高度化に伴って、本人撮影画像情報と写真／映像撮影情報との区別が難しくなっており、一般には高精度化しにくい。また類似他人によるものについても、類似の程度に応じて高精度化の困難な場合があり得る。

・追加の入力デバイスを利用するもの：
赤外線などの非可視光カメラを利用した対象物の温度分布や、3D 計測デバイスにより対象物の 3 次元構造を求めることで、対象が人物なのか写真や映像なのかを区別す

るもの。

やや特殊な入力デバイスが必要なためコストや利用シーンに制限がつく可能性がある。また、類似他人の識別に使いにくいとはいうものの、対象が生体や立体構造物であるかどうかという明確な特徴が利用できるため、比較的高精度化しやすい。

(2) システムが指示した動作に対する反応を判断して識別する

生体情報提示を伴う動作をシステムから指示し、その通りに情報が提示されるかどうかで、入力が写真や映像等の偽造情報であるか否かを識別する。例えば指示としては、顔の向きや表情（目をつぶる等）とし、その状態になったことを認証システム側が画像認識技術で検出し、正しい反応かどうかを識別する。

一般的には特殊な入力デバイスが不要、かつ検知すべき特徴も単純であることから比較的高精度化しやすいが、システム提示とユーザーのアクションを伴うことから高速実行はしにくく、利用シーンに制限がつく場合がある。

4.2 個人情報保護法を満たすための対策

4.2.1 個人情報の管理に関する一般的な対策

個人情報保護法（正式名称：個人情報の保護に関する法律）とは、個人情報の適切な利用を促しつつも、個人の権利もしっかり保護することでバランスをとり、保護の対象となる情報の定義や、各情報を利用する際のルールを規定した法律である。

顔画像及び顔画像から得られた特徴量データは、特定の個人を識別できる個人情報として定義されており、個人情報保護法に沿った対策を行う必要がある。なお、個人情報のうち、特定の個人を検索できるよう体系的に構成したものを「個人データ」と呼ぶ。また、個人情報取扱事業者が開示・訂正・消去等の権限を持ち、期間の長短に限らず保有する個人データを「保有個人データ」と呼ぶ。

個人情報保護法において、個人情報データベースなどを事業の用に供している者を「個人情報取扱事業者」と定義しており、個人情報取扱事業者は以下の対策を実施する責務がある。

(1) 個人情報取得時の対策

①事前告知や掲示など

撮影期間・撮影範囲・利用目的・連絡先等の掲示を行う。

②本人の同意取得

取得にあたって本人に同意を得る。防犯カメラによる撮影等、本人から直接同意を得ることが困難な場合には、取得主体・内容・利用目的・問い合わせ先等の必要事項を掲

示して必要範囲内の撮影を行う。

(2) 利用・管理時の対策

①内容の正確性の確保

利用目的達成に必要な範囲で個人データを最新かつ正確な情報に維持する。

②安全管理措置

組織的・人的・物理的・技術的な視点で各種安全管理措置を行う。

・責任者や管理体制、データの台帳管理等の組織的な管理体制を確立する。

・個人データを取り扱う従業員へ内部規定の周知や教育・訓練を実施する。

・入退室管理やワイヤロックなどの物理的な保護を行う。

・アクセス管理・制限、システムのセキュリティアップデート等の対策を行う。

③第三者提供の制限

あらかじめ同意のない状態で第三者への提供を行わない。

④利用者・委託先の監督

利用事業者の従業員や委託先に対し、必要かつ適切な監督を実施する。

具体的には②の安全管理の対策を実施していることを確認する。

⑤通知義務等

個人データを取り扱う事業者は、事業者の名前、利用目的、開示・訂正・利用停止手続きの方法、連絡先等をホームページに掲載するなど、個人データの利用が適正に行われているか確認できるようにする。

⑥開示、訂正、利用停止など

事業者は、本人から保有個人データの開示、訂正、利用停止等の請求を受けたときには、遅滞なく対応する必要がある。「開示」は請求者本人の保有個人データの内容そのものを本人に示すこと、「訂正」は保有個人データの内容が事実でない場合に、事実に合致するように修正すること、「利用停止等」とは保有個人データの利用の停止又は消去の請求を受けた際に保有個人データなどの利用を停止することを意味する。

4.2.2 顔画像特有の対策や注意点

(1) 管理すべき情報の範囲

個人情報保護法において、個人が特定できる顔が写った画像は個人情報として管理する必要がある。また、画像から個人の特徴を抽出して数値化した「特徴量データ」は、個人を識別可能な情報として「個人識別符号」に該当し、個人情報と同様の管理が必要となる。

一方、顔画像を加工・処理することによって取得できるデータの属性情報（性別・年

齢・人種等）や、カウントデータ（人数）、動線データ（どのように移動したのかの軌跡情報）、処理済みデータ（モザイクをかけた顔画像等）については、単体では個人を特定できないため「個人情報」には該当しない。ただし、顔画像や特徴量データ、氏名等と関連付けが可能な状態にすることで個人を特定することが可能となり、「個人情報」に該当するようになるため、注意が必要である。

(2) 個人情報保護法以外の注意点

カメラ画像を取り扱う場合、個人情報保護法を遵守するだけでなく、被写体の自覚的な権利としてプライバシーや肖像権が保護される必要があることにも留意する必要がある。そのため、社会的なコンテキスト（法令や規制の動向、判例・報道等）、技術進展などによる被写体のプライバシーへの影響等を常に確認していく必要がある。また、被写体のプライバシー侵害が生じた際、またはそのおそれがある場合には、迅速に是正措置をとる必要がある。

(3) 防犯カメラ映像等への対応について

防犯カメラの映像では、撮影範囲内への映り込みや通行が避けられないルートなど、暗黙の同意を行っているとは言えない状況で個人情報が取得される可能性があり、生体認証の中でも顔認証特有の課題として「本人が意図しない取得」が発生する。防犯カメラ映像から得られた顔認証データ等を取り扱う場合、以下のような問題も発生する可能性がある。

- 被写体からは「カメラ」としか見えないため、取得された情報の利用目的が把握しにくい。
- 無意識で意図しない行動も取得されてしまうため、本人の想像しない情報が漏洩する可能性がある。
- 映像取得時点では予測できなかった情報が技術の進歩で後日明らかになる可能性がある。

この問題への対策として以下のような配慮が必要である。

- 撮影対象場所の性質に配慮する
  公共の場所であるほど、被写体は撮影をさけることができなくなるため撮影の正当性、必要性、手段を事前に慎重に確認する必要がある。
- 利用目的を特定して通知・公表する
  防犯カメラが作動中であることを設置場所等に掲示するなど、自らの個人情

報が取得されていることを本人が容易に認識できる措置を講ずる必要がある。また、利用目的等の必要事項の通知・掲示等を行う。

- カメラ画像を取得する範囲を必要最小限にする
  時間的範囲、空間的範囲が広がれば広がるほどプライバシーへの影響が広がるため、撮影範囲を必要最小限にするよう努力する。例えば、防犯カメラの設置位置の制限や、プライバシーマスクの設定等が挙げられる。

- 検知や推定を行う範囲を必要最小限にする
  個人識別等に必要な情報以外にも、人種・健康・内心等の情報を抽出・推定したりすることでプライバシー等への影響や、目的外利用につながる可能性があるため、解析範囲を必要最小限にする必要がある。

4.2.3 個人情報保護と顔画像の取り扱いに関する参考文献

- 個人情報の保護に関する法律についてのガイドライン（個人情報保護委員会、2016 年 11 月（2022 年 9 月一部改正）、2023 年 4 月 15 日閲覧）
  https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/

- 「個人情報の保護に関する法律についてのガイドライン」に関する Q&A（個人情報保護委員会、2023 年 3 月、2023 年 4 月 15 日閲覧）
  https://www.ppc.go.jp/personalinfo/faq/APPI_QA/

- カメラ画像利活用ガイドブック Ver3.0（IoT 推進コンソーシアム 総務省 経済産業省、2022 年 3 月、2023 年 4 月 15 日閲覧）
  https://www.meti.go.jp/press/2021/03/20220330001/20220330001.html

4.3 システムによるセキュリティ対策

4.3.1 セキュリティ対策の考え方

顔認証に関する情報が個人情報であることを踏まえると、顔認証を含むシステムやこれに接続するシステムに関しても十分なセキュリティ対策が必要になる。

セキュリティ・インシデントは不注意で発生するものもあるが、外部の攻撃者や内部の不正利用によって発生するものもある。攻撃者は対策の不備や穴を突いてくるため、セキュリティ対策としてはシステム全体に対して網羅的に実施することが重要になる。

また別の重要な考え方として「多層防御」という考え方がある。セキュリティ対策に

おける「多層防御」とは、セキュリティ対策を組み合わせて階層を築くことで、一つの対策が破られても次の対策が攻撃を抑止し、重要部への侵入前に攻撃の検知及び対応できるようにする考え方である。

セキュリティ対策としては、システム全体に対して複数のセキュリティ対策を網羅的に実施することで初めて一定程度のセキュリティを担保することができる。

4.3.2 セキュリティ対策の種類と機能

セキュリティ対策は主に三つの対策に分類される。

表 7：セキュリティ対策の種類

対策の種類	対策の例
技術的対策	機器の導入や設定等により、セキュリティ・インシデントを防止する対策
物理的対策	機器の設置場所の堅牢化等により、脅威の発生を防ぐ対策
人的対策	制度や運用ルールにより、人的なセキュリティ・インシデントを防止する対策

セキュリティで一番弱い部分は、人が関与する部分と言われている。人はミスをするものという前提に立ち、セキュリティ対策を検討することが重要になる。そのため、まずは技術的なセキュリティ対策の導入やシステム自体の自動化処理部分を増やすことで、人の関与する部分を減らすことが重要になる。ただし、コストやシステム制限などにより技術的対策等の導入が難しい場合には、人的対策によって技術的対策の不足分を補える部分もある。

また、セキュリティ対策の機能は、主に三つに分けることができる。

表 8：セキュリティ対策の機能

対策の機能	概要
予防（防止、防御）	・攻撃により被害を受けたり、異常が発生したりすることを未然に防止する対策 ・原則として実施する必要がある対策
検知（被害把握）	・攻撃により被害を受けたことや、異常が発生したことを早期に発見する対策 ・必要に応じて実施する必要がある対策
復旧（事業継続）	・攻撃による被害等により異常が発生した場合、速やかに原状に復帰させる対策 ・可用性が要求されるシステムでは実施する必要がある対策

近年では攻撃が高度化していて、攻撃を完全に防ぐことは非常に難しくなっている。サイバー攻撃を受けることを前提とし、いかに早期にこれを検知し、対処する。そして復旧を早めることで影響を最小限にするという考え方をとる組織が増えている。これらを実現するためには、セキュリティ対策として単に防御を実施するだけではなく、検知と復旧の考えに基づいたセキュリティ対策も重要になる。

4.3.3 セキュリティ対策の例

主なセキュリティ対策の例を以下に示す。攻撃には段階があり、各段階でセキュリティ対策を実施することで多層防御を実現することができる。

表 9：セキュリティ対策の例

用途・目的	概要	対策例
初期進入段階	攻撃の初期段階における、外部との接続点を介したネットワーク経由の攻撃、あるいはシステム設置場所への攻撃者の物理的侵入を防止する目的で実装される対策。 また、攻撃者による、システムへの不正ログイン等を防止する目的で実装される対策。	ファイアウォール（FW）、IPS、アンチウイルス、 パッチ適用、脆弱性回避、 通信相手の認証、操作者認証、入退管理
内部侵攻・拡散段階	システムへの侵入を果たした攻撃者による、内部の情報収集や侵入範囲拡大を防止する目的で実装される対策。	セグメント分割／ゾーニング、APT 対策ツール、アクセス制御、ホワイトリストによるプロセスの起動制限
目的遂行段階	「情報窃取」「データ改ざん」「制御乗っ取り」「システム破壊」等、攻撃者による最終目的の実現を防止する目的で実装される対策。	重要操作の承認、 データ暗号化、データ署名、 フェールセーフ設計
検知	攻撃の実施、あるいは攻撃の成功による被害の発生を早期に検知することを目的に実装される対策。	IDS、アンチウイルス、APT 対策ツール、 統合ログ管理システム、 機器異常検知、機器死活監視、入退管理、侵入センサー
被害把握	攻撃の成功による被害や影響範囲の把握を目的に実装される対策。あるいは、監査における証跡提示のため、攻撃内容の詳細の把握等を目的に実装される対策。	ログ収集・分析、 統合ログ管理システム
事業継続	攻撃の成功による被害を最小限に留めるために実装される対策。あるいは、サービスの継続、被害の早期復旧を実現することを目的に実装される対策。	データバックアップ、冗長化、暗号鍵更新、 フェールセーフ設計

顔認証システムにおいてポイントとなる対策は以下である：

- 個人情報の暗号化
  個人情報を暗号化しておくことで、万一漏えいしてまった場合の影響を最小限に抑えることができる。

- 個人情報の分離保持や非個人情報化
  「特徴量データ」と個人情報を分離して保持したり、システムで不要であれば匿名化して情報を保持することで、漏えいしてまった場合の影響を最小限に抑えることができる。

- 個人情報の逐次更新
  個人情報を保持すること自体がリスクとなるため、不要となった情報はその都度適切なプロセスで更新（削除）する。

- 個人情報を配置するネットワークの分離
  攻撃者がシステムに侵入したとして、ネットワークが分離されていれば容易には個人情報が配置されたネットワークにアクセスできない。

- 個人情報へのアクセス制御の適正化
  適切に定義、制限、分離されたアクセス権によってプログラムによるアクセス、又は自動アクセスを制御することにより、不正アクセスのリスクを軽減する。API 等の使用前に認証処理を行うことなどが本処理に該当する。

- ログ監視
  ログを分析することで被害が出る前に攻撃の兆候を把握し、対処することができる。被害が出てしまった場合でも、早期に対処することで被害を最小限に抑えることができる。

- インシデント発生時の対応手順の作成
  インシデントの発生時に迅速に適切な対処がとれるように、事前に対応手順を作成し、組織内で了承を得ておく必要がある。また訓練等を行うことで確実な対応がとれるようにする。

4.3.4 セキュリティ対策の決定

セキュリティ対策は以下のような手順で策定すると、効率的かつ効果的なセキュリティ対策を取ることができる。

(1) 前提条件（法令・業界標準）の確認

システムを使用する監督官庁等の法令やガイドライン等で示されたセキュリティ関連項目は取り入れる必要がある。

(2) 管理すべき情報資産の洗い出し

管理すべき資産の重要度によって、セキュリティ対策にかけるべきコストは変わってくる。個人情報や組織の機密情報を扱う場合には、それ相当のセキュリティ対策が必要になる。

(3) 情報資産に対するリスクの識別と分析

対象のシステム及び情報資産に対して、どのような脅威事象が起こり得るのか、どのようなリスクになるのかを識別し、分析する。

(4) 特定したリスクの評価（発生頻度、影響度）

識別し、分析したリスクをその発生頻度や影響度などに基づいて評価する。リスクの高いリスクが優先して対処すべきリスクと判断する。

(5) リスクへの対応

それぞれのリスクに対して必要なセキュリティ対策を検討する。セキュリティ対策によって対象のリスクを回避、低減、移転することができ、最終的にリスク受容できるレベルにする。

4.3.5 システムのセキュリティに関する参考文献

- IPA 制御システムのセキュリティリスク分析ガイド 第 2 版（独立行政法人情報処理推進機構、2017 年 10 月（2023 年 3 月最終更新）、2023 年 4 月 15 日閲覧）
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html#section10

- 国民のためのサイバーセキュリティサイト情報管理担当者の情報セキュリティ対策（総務省、2023 年 4 月 15 日閲覧）
  https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/business/business_admin.html

- 重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版

  Framework for Improving Critical Infrastructure Cybersecurity Version 1.1（頁対訳）（NIST/米国国立標準技術研究所、翻訳監修：独立行政法人情報処理推進機構、2018 年 4 月、2023 年 4 月 15 日閲覧）

  https://www.ipa.go.jp/files/000071204.pdf

5. 顔認証に対応したシステムの事例

5.1 決済システムの例

クレジットカード、電子マネー、スマホ決済など、我々の生活の中においてキャッシュレス決済の普及が進んでいる。更にコロナ禍は、人と人の接触が伴う現金決済から非接触決済への転換を人々に促している。その一方で、カードやスマートフォンという「モノ」が盗難に遭ったり、紛失するリスクが生じていることも事実である。

そのような中で、決済時に「モノ」をお財布やカバンなどから取り出す必要がなく、盗難、紛失リスクもない顔認証を利用した決済の実証実験や実用化事例が、各地で始まっている。

顔認証決済の事例として、プロ野球スタジアム内の店舗における顔認証決済システム「facethru（フェイスルー）」について取り上げる（事例の内容はプレスリリース等公開情報を参照した)。「facethru」は顔認証による決済のみでなく、スタジアムの入場にも利用可能であるが、ここでは決済のみにフォーカスする。

「facethru」のスタジアム内店舗決済は下記の 4 つの STEP で行われる。（ユーザー視点で記載）

STEP1 事前登録

顔画像登録 Web サイトより必要情報を入力し、顔写真の撮影とクレジットカード番号、有効期限、セキュリティコード、本人認証用 PIN（暗証番号）の登録を行う。

STEP2 お買い物

スタジアム内の店舗で購入商品を選択する。

STEP3 お会計

購入金額を確認して、店舗内に設置されたカメラで顔を撮影すると、システムに事前登録された顔情報と顔画像を照合し、本人認証を行う。

STEP4 お支払い完了

顔認証が承認され、STEP1 で事前登録した PIN の入力を行うと、同じく事前登録されたクレジットカード番号にて決済が行われる。

出典：パナソニック公式サイト（2022 年 3 月、2023 年 4 月 15 日閲覧）
https://news.panasonic.com/jp/press/data/2022/03/jn220301-2/jn220301-2.html

図 15：利用イメージ

決済においては、料金の誤収受防止並びに支払いの意思表示を明確にするため、顔認証以外に、他の認証を併用することができる。上記の事例「facethru」においてはスタジアム入場も利用可能だが、その際は顔認証のみを利用している。しかし、決済においては PIN 入力が併用されている。決済では、取扱う商品の換金性や金額の大小により決済におけるリスクが異なる。そのため多要素本人認証（顔認証以外に他の本人認証を併用すること）が必要かどうかは、導入事業者によってケースバイケースの選択事項となる。ただし、すべてのユーザーに対して多要素で本人認証を要求すると、ユーザビリティが低下し、顔認証のメリットが享受できない。この問題を回避するために、顔認証のしきい値をやや厳しめに設定し、認証結果が疑義となった場合のみ多要素認証を行うことは有効である。また多要素認証を必須とした場合もフリクションレス（摩擦がない）な顔認証以外の生体認証等を併用することで、ユーザビリティの低下を軽減することが可能である。

また、顔認証決済だけの問題ではないが、事前に顔画像に紐づいて登録されたクレジットカード番号や有効期限、セキュリティコードなどのセンシティブ情報の管理は PCI DSS（カード情報セキュリティの基準）などに準拠する必要がある。

5.2 入出場ゲートシステムの例

入出場ゲートシステムの例として、空港での出帰国手続、鉄道の改札機とバスの乗降システムを取り上げ、システム構成例を示す。

5.2.1 空港での出帰国手続（航空会社、空港会社管理）

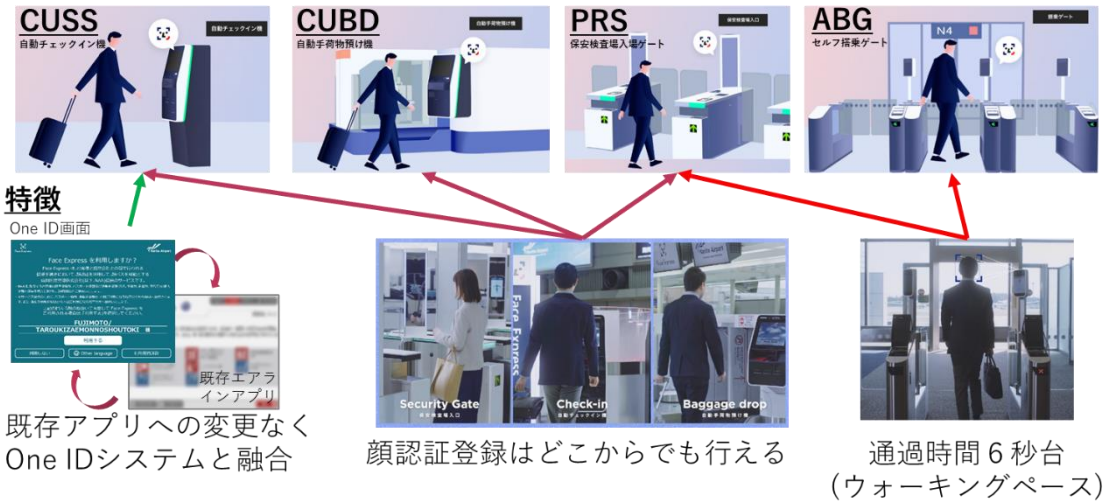
ここでは、空港での搭乗手続きに関する顔認証技術の導入事例を紹介する。

成田空港では、自動チェックイン機でパスポートを照合して顔画像を登録すると、空港でのその後の手荷物預け、保安検査場入口、搭乗ゲートなどにおいて、顔認証で通過又は手続きが可能になっており（図 16）、以下の仕組みにより実現される。①では 1:1 認証、②では①で登録された複数の顔の情報との 1:N 認証が実施される。

① チェックイン時に、パスポートの IC に格納されている顔写真と搭乗者本人が一致していることを確認し、搭乗者本人の顔写真、パスポート情報、搭乗情報を紐づけ、OneID 認証システムに一時的に格納し保持する。

② 以降、手荷物預け、保安検査場入口、搭乗ゲートの端末にて、顔写真撮影が行われ、OneID 認証システムへ照会され、システム内で本人確認が実施される。

なお、顔認証登録は、自動チェックイン機に限らず、自動手荷物預け機、保安検査場入口ゲートでも可能である。



出典：成田国際空港株式会社、日本電気株式会社

※OneID は国際航空運送協会(IATA：International Air Transport Association)が提唱するコンセプト。ID 管理と生体認証に基づく書類不要のプロセス。

※Face Express は成田国際空港株式会社の商標です。

※掲載画像は成田国際空港株式会社のホームページ・YouTube 動画より引用(2023 年 4 月 15 日閲覧)

https://www.narita-airport.jp/jp/faceexpress/

図 16　出国（航空機への搭乗）

5.2.2 空港での出帰国手続（出入国在留管理庁管理）

ここでは、空港での出帰国手続きに関する顔認証技術の導入事例を紹介する。

出国手続きで用いられる顔認証ゲートの一例（図 17）として、利用手順を以下に示

す。②にて 1:1 認証が行われる。

① パスポートの読み取り

顔認証ゲートのリーダーに、パスポートの IC に格納されている顔写真を読み込ませる。

② 顔認証

顔認証ゲートの内蔵カメラで顔写真を撮影し、パスポートの顔写真を用いて認証を行う。なお、撮影された顔写真は、本人確認のための照合にのみ用いられ、保存されない。

提供：パナソニック コネクト株式会社

図 17 顔認証ゲートの例

5.2.3 鉄道の改札機とバス乗降システム

ここでは、鉄道の改札機とバス乗降システムに関する顔認証技術の導入事例を紹介する。

(1) 鉄道の改札機

改札機の一例を図 18 に示す。改札機に備えつけたカメラで顔を捉え、事前登録した顔写真データと照合・承認により改札ゲートを開閉する。

鉄道の改札には、以下が求められる。

- 認証速度性能

  入出場許可と運賃収受を目的としているため、認証、乗車券判定、情報更新を短時間で実施できること。

- 顔画像の取得

公共の場で利用されるため、様々な利用者を想定し、視線誘導などによりカメラに顔を向けてもらうこと。

- マスク、アクセサリの対応
  公共の場で利用されるためマスク、アクセサリを前提に認証が可能であること。

提供：オムロンソーシアルソリューションズ株式会社

図 18　顔認証改札機の例

また、従来の改札機とは異なる形状の、ゲートレスの顔認証改札もある（図 19）。

提供：パナソニック コネクト株式会社

図 19　ゲートレス型の顔認証改札機の例

(2) バスの乗降システム

バスの乗降システムについては、各地で実証実験が行われている。システムの例を図 20 に示す。

システム利用に際しては事前に顔画像を登録しておき、バス乗降口に備え付けられた端末に顔を近づけ認証を行う。

バスの運賃制度はいくつかあり、顔認証の場面も異なる。例えば均一制運賃では乗車時（又は降車時）、区間制運賃では乗車時と降車時に顔認証を実施する。

提供：日本電気株式会社

図 20　バス乗降システムの例

5.3 公共系システムの例

公共系システムにおける顔認証の活用は、いずれも公的機関による厳格な本人確認の下に発行された「公的身分証明書」（＝本人を確認できる公的証明書）の媒体券面（パスポートは身分証明情報の記載ページ）に掲載された顔写真、もしくは媒体に内蔵する IC チップ内に格納された顔写真の電子データを用いて、媒体を持参した人の最新の顔撮影情報との比較照合によって利用者検証が行われる点が特徴となっている。（前章「3.10 サービスの提供範囲」の定義における「複数事業者に跨る顔認証サービス - (1) 顔画像媒体持参方式」で、いずれも「1:1 認証」となる）

顔認証に活用が可能な「公的身分証明書」には以下のものなどがある（2023 年 3 月 31 日時点）。このうち、すでに実際に顔認証の運用が始まっているものとしては、パスポートなどがある。

顔情報の格納方法については、いずれの媒体も、券面への掲載と IC チップ内のデータ記録の両方に対応しているが、IC チップ内のデータを参照する際には媒体の持ち主本人のみが知り得る暗証番号などの入力を求められるケースが多いため、券面に記載された顔写真を照合に利用する事例もある。

●運転免許証
○運転経歴証明書
●パスポート
●在留カード
○特別永住者証明書
●マイナンバーカード（健康保険証として利用する「マイナ保険証」を含む）
○写真付住民基本台帳カード

これらのうち、●で示した 4 種類の「公的身分証明書」に関して、顔情報の登録方法、顔情報が紐付けされた媒体を受け取る際の手続き運用、そして、顔認証を利用する際の特徴を表 10 に示す。

表 10：公的身分証明書における顔情報の登録・受け取り手続き・利用時の特徴

証明書	発行主体	＜顔情報の登録時＞	記録する顔写真の条件
運転免許証	国家公安委員会	・運転免許試験場、運転免許更新センター等で係員が撮影 ・新規の免許取得時、更新時において、都道府県により持ち込み可能な交付所もある	・縦 3cm×横 2.4cm（国外運転免許証申請時に添付する写真サイズは縦 4.5cm×横 3.5c,m） ・無帽（宗教上又は医療上の理由がある場合を除く）、正面、上三分身、無背景 ・申請前 6 か月以内に撮影したもの
パスポート	外務省	・住民登録をしている都道府県のパスポート申請窓口にて申請を行う際に、規程の条件を満たした顔写真を提出する	・縦 4.5cm×横 3.5 cm ・正面を向いて撮影されたもの、背景（影を含む）がないもの、輪郭が露出しているもの ・無帽であるもの（宗教上または医療上の理由により顔の輪郭が分かる範囲で頭部を布などで覆うことが認められる場合を除く） ・目の周辺に、髪の毛、マスク、眼鏡、つけまつげ、まつげエクステ等の一部、あるいはその陰が入ってこないようにすること ・申請日から 6 か月以内に撮影されたもの
在留カード	出入国在留管理庁	・当該上陸許可に係る在留資格認定証明書交付申請や査証申請等で提出されたものから，在留カードに適した写真を入国審査官が選択する ・更新時には適切な写真を用意して持参する	・縦 4cm×横 3cm ・無帽で正面を向いたもの、背景（影を含む。）がないもの、鮮明であるもの ・提出の日前 3 か月以内に撮影されたもの
マイナンバーカード	市区町村による交付	「オンライン申請」 ・登録されたメールアドレス宛に通知される申請者専用 Web サイトにアクセスし、顔写真を登録する 「郵送による申請」 ・個人番号カード交付申請書の「顔写真貼付欄」に、自身で撮影した顔写真を貼付する 「証明写真機による申請」 ・証明写真機によって撮影された顔写真データがオンライン送信される	・縦 4.5cm×横 3.5cm ・最近 6 ヶ月以内に撮影 ・正面、無帽、無背景のもの ・白黒の写真でも可 ・宗教上又は医療上の理由により、顔の輪郭が分かる範囲で頭部を布などで覆う写真を使用する者や、乳幼児、障がいのある者、または寝たきりの者等、やむを得ない理由により適切な規格の写真を撮影できない場合に、特例措置の用意あり ※オンライン申請の場合 ファイル形式：jpeg、カラーモード：RGB カラー（CMYK カラー等は不可）、ファイルサイズ：20KB～7MB、ピクセルサイズ：幅 480～6000 ピクセル、高さ 480～6000 ピクセル

証明書	IC チップからの顔画像データの読み出し	＜顔情報紐付け媒体の受取時（交付時）＞	＜顔認証の利用時（媒体に紐付けされた顔情報と、持参した人の顔撮影情報との比較時＞
運転免許証	・暗証番号 1（数字 4 桁）、暗証番号 2（数字 4 桁）の入力が必要	・暗証番号を IC 免許読取兼バーコード印刷装置に入力すると登録カードが印刷される ・適性検査を受けた後に申請書類を提出し、バーコード読取装置付免許証作成装置に登録カードを読み込ませ、運転免許証の写真を撮影してもらう ・講習の受講後、係官から手渡しで運転免許証を受領	・犯罪による収益の移転防止に関する法律施行規則 第六条（顧客等の本人特定事項の確認方法）の（ホ）（ヘ） ・そのほか、民間が提供する顔認証サービス
パスポート	・暗証番号等の設定なし ・NFC 対応アプリ等にて読み出しが可能。その節には読み出しの前に下記の 3 情報を入力する必要がある。 ①旅券番号（9 桁） ②生年月日（8 桁） ③有効期限（6 桁）	・「申請の時に渡された受理票（受領証）」に手数料を添えて申請 ・窓口の係員が受理票を持参した人の顔容貌を含む本人確認を行った上で交付	
在留カード	・暗証番号等の設定なし ・出入国在留管理庁が無償配布している「在留カード等読取アプリケーション」等にて読み出しが可能	地方出入国在留管理官署窓口での即日交付、郵送による後日交付	
マイナンバーカード	・利用者証明用電子証明書パスワード（数字 4 桁）の入力が必要	・交付通知書（はがき）や運転免許証、健康保険証などの本人確認書類を持参し、交付を受ける ・地方公共団体情報システム機構（J-LIS）が提供する「個人番号カード交付窓口用顔認証システム」を導入する市区町村では、顔認証による本人確認を実施した上での交付	

5.3.1 マイナ保険証の本人確認

(1) 申込方法

マイナンバーカードを健康保険証として利用する「マイナ保険証」は、あらかじめデジタル庁が運営する「マイナポータル」などを通じて申し込みを行うことで、初めて利用できるようになる。「マイナポータル」にはパソコンの Web サイトかスマートフォンのマイナポータルアプリがあり、スマホアプリは「iOS 版」と「Android 版」が提供されている。このほか全国のセブン銀行 ATM を操作することでも、「マイナ保険証」の申し込みが可能である。

いずれの方法であっても、申込者本人のマイナンバーカードの提示（パソコンでは IC カードリーダー、スマートフォンは NFC リーダーモードを使って読み取り。セブン銀行 ATM ではマイナンバーカードを挿入する）と、本人があらかじめマイナンバーカードに設定している「利用者証明用電子証明書パスワード（数字 4 桁)」の入力が求められる。

上記手順後に、画面表示された「保険証利用登録」から「申し込む」を押下すれば、以降はマイナンバーカードを「マイナ保険証」として利用することが可能になる。

マイナンバーカードの健康保険証利用は、2021 年 10 月 20 日から本格運用が始まっており、厚生労働省では「2023 年 3 月末にはおおむね全ての医療機関等での導入を目指す」こととしている。

【参考】
マイナンバーカードの健康保険証利用に関する案内ページ（デジタル庁 総務省 厚生労働省、2023 年 4 月 15 日閲覧）
https://myna.go.jp/html/hokenshoriyou_top.html

(2) 利用方法

「マイナ保険証」は、マイナンバーカードを医療機関や薬局に設置された専用の読み取り端末に提示することで、健康保険証の代わりとして利用できる仕組みである。対応する医療機関と薬局には「マイナ受付」のステッカーが掲出されている。

まず、設置された「顔認証付きカードリーダー」のカード提示部分にマイナンバーカードをセットする。この際、マイナンバーカードに目隠しカバーを装着している場合には外す必要がある。

次に、本人確認の方法として端末のタッチパネル画面に「暗証番号（利用者証明用電子証明書パスワード/数字 4 桁)」か「顔認証」の選択ボタンが表示されるので、「顔認証」を選択する。すると端末のカメラが起動し、マイナンバーカードを持参した人の顔

撮影が行われ、マイナンバーカードに登録された顔写真情報との比較・照合により認証される。なおデジタル庁では、「マスクをしていても、眼鏡をかけていても、帽子をかぶっていても顔認証が可能」と説明している。

また、子どもが「マイナ保険証」を利用する場合には、顔認証以外に、親などの代理人による暗証番号入力か、暗証番号入力が難しい場合には係員による目視でも確認が可能となっている。

最後に端末のタッチパネル画面で「薬剤情報の閲覧・特定健診情報の閲覧」に同意すると、「マイナ受付」の手続きは完了となる。

5.3.2 マイナンバーカード交付時の本人確認

マイナンバーカードは身分証明書としても利用できるため、厳格な本人確認手続きを経た上で、市区町村の窓口にて交付される仕組みとなっている。カードを本人に交付する際には、間違いなく申請した本人に対して正しいマイナンバーカードが手渡される必要がある。

市区町村の窓口では、マイナンバーカードの交付に先立って交付通知書（はがき）や運転免許証、健康保険証などの本人確認書類を持参することで本人確認が行われるが、より厳格な本人確認を行う目的で顔認証を利用したシステムが開発されている。地方公共団体情報システム機構（J-LIS）が提供する「個人番号カード交付窓口用顔認証システム」で、東京都江東区など一部の市区町村窓口において運用が行われている（図21）。

この顔認証システムでは、窓口に現れた本人の顔をカメラで撮影し、マイナンバーカードの顔写真と照合、確認する。証明用写真として不適切な写真であったり、本人と同一性が確認できない写真であったりすることが原因で照合が成功しない場合には、申請を取り消し、改めての申請が必要となる。なお、撮影した写真のデータがシステムに残ることはない。

図 21：顔認証システムの画面イメージ

出典：バイオメトリクスを用いたサービス・ソリューション～マイナンバーカードに関わる顔認証システムの活用（日本電気株式会社、2023 年 4 月 15 日閲覧）
https://jpn.nec.com/techrep/journal/g18/n02/180207.html

【参考】
東京都江東区（マイナンバーカードの交付手続き案内）（2023 年 4 月 15 日閲覧）
https://www.city.koto.lg.jp/060301/kurashi/mynumber/card/94138.html

5.4 本人確認システムの例

スマートフォンアプリサービスによっては本人確認を必要とするサービスがある。例えば、マネーロンダリングなどの不正を防ぐために、金融サービスなどでは「犯罪による収益の移転防止に関する法律」（以下、「犯収法」と呼ぶ）に定められた方法での本人確認が義務づけられている。

従来は対面もしくは郵送での本人確認が主流であったが、2018 年 11 月犯収法施行規則の改正により、オンラインでの本人確認、いわゆる「eKYC」が認められた。

その eKYC 手段の一つとして顔認証を用いた方法があり、具体的には犯収法施行規則 6 条 1 項ホ※の方法がこれに当たる。

施行規則により具体的な方法が定められておりサービス事業者ごとの本人確認手続き（スマートフォン操作）の差異は少ないため、LINE Pay「スマホでかんたん本人確認」を事例として取り上げる。

「スマホでかんたん本人確認」は下記の 3 つの STEP で本人確認の申請が完了する（図 22）。

STEP1 本人確認書類の撮影
STEP2 顔の撮影
STEP3 本人情報の入力

STEP 1　本人確認書類の撮影

本人確認書類に利用する身分証の表・厚み・裏面を撮影します。

カードタイプの身分証を利用する場合

1) 表面の撮影

①撮影に利用する身分証を用意します。
②画面に表示されるガイド枠に合わせて、撮影を行います。
③身分証がはっきりと映るようにします。

2) 厚みの撮影

①身分証の厚み（上側）全体と表面が映るように撮影をします。
②右手でスマホを持って、左手で身分証を持ちます。この時、身分証は手前に少し傾けます。
③画面に表示されるガイド枠に合わせて、撮影を行います。
④身分証を持った指で文字や顔写真が隠れないように注意してください。

※ 身分証の厚みが確認できない場合、本人確認が完了しません。撮影時に身分証の厚みが映っているかご確認ください。

3）裏面の撮影

①撮影に利用する身分証を平らな場所に置きます。

②画面に表示されるガイド枠に合わせて、撮影を行います。

STEP 2　顔の撮影

スマートフォンのインカメラを使用して顔正面と動きの撮影を行います！

1）顔の正面の撮影

①スマートフォンを顔の正面に持ちます。

②表示されるフレーム内に顔全体が映るように位置を調整します。

出典：LINE Pay 公式ブログ「本人確認の方法」（最終更新 2023 年 3 月、2023 年 4 月 15 日閲覧）
https://pay-blog.line.me/archives/16994522.html#topic3

図 22：LINE Pay「スマホでかんたん本人確認」の手順

この本人確認手段で顔認証が用いられている部分は、STEP1 と 2 にかけてである。

STEP1 で本人確認書類の顔写真を認識し、STEP2 で撮影する本人の顔と一致するか認識する部分である。

この工程の認識精度が本人拒否率や他人受け入れ率に影響するため、システムの優劣を左右するといえよう。

同一人物かを判定する技術には AI が用いられており、他の顔認証技術と同様に継続的な改善や技術革新が反映され、進化が激しいと言える。

本ガイドラインは顔認証に焦点を当てているため、本人確認システムの中で顔認証がどのような意味を持つかを説明した。しかし、事業者が犯収法施行規則 6 条 1 項ホに定められた eKYC（本人確認システム）の導入を検討する場合、顔認証の認識精度以外にも、身分証明書の記載文字や厚みの認識精度やエンドユーザーにとってわかりやすい UI/UX であるかなど、総合的な見地でシステムを検討すべきである。

※（顧客等の本人特定事項の確認方法）第六条　法第四条第一項に規定する主務省令で定める方法のうち同項第一号に掲げる事項に係るものは、次の各号に掲げる顧客等の区分に応じ、それぞれ当該各号に定める方法とする。

一　自然人である顧客等（次号に掲げる者を除く。）　次に掲げる方法のいずれか（想定システム構成図などを交えながら解説）

ホ　当該顧客等又はその代表者等から、特定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（当該顧客等又はその代表者等に当該ソフトウェアを使用して撮影をさせた当該顧客等の容貌及び写真付き本人確認書類の画像情報であって、当該写真付き本人確認書類に係る画像情報が、当該写真付き本人確認書類に記載されている氏名、住居及び生年月日、当該写真付き本人確認書類に貼り付けられた写真並びに当該写真付き本人確認書類の厚みその他の特徴を確認することができるものをいう。）の送信を受ける方法

利用シーンに応じた『顔認証』導入要件等に関する研究 WG　参加メンバー

	氏名	所属
主査	初本　勲	ＪＲ東日本メカトロニクス株式会社
副主査	中津留　勉	ソニー株式会社
委員	大熊　喜之	株式会社エヌ・ティ・ティ・データ
委員	浅井　健	オムロン ソーシアルソリューションズ株式会社
委員	萱場　慎	オムロン ソーシアルソリューションズ株式会社
委員	松浦　大輔	オムロン ソーシアルソリューションズ株式会社
委員	上原　輝剛	共同印刷株式会社
委員	金田　尚	共同印刷株式会社
委員	林　邦彦	ＪＲ東日本メカトロニクス株式会社
委員	栗田　太郎	ソニー株式会社
委員	石川　勝章	大日本印刷株式会社
委員	小野寺　貴弘	大日本印刷株式会社
委員	米木　淳	TIS 株式会社
委員	佐々木　楽	株式会社デンソーウェーブ
委員	田野　壮一	株式会社デンソーウェーブ
委員	榎本　暢芳	東芝インフラシステムズ株式会社
委員	加藤　雅一	東芝インフラシステムズ株式会社
委員	助川　寛	東芝インフラシステムズ株式会社
委員	薛　一憲	東芝インフラシステムズ株式会社
委員	飯倉　慎太郎	凸版印刷株式会社
委員	清水　周平	凸版印刷株式会社
委員	島村　徳義	日本信号株式会社
委員	星野　隆	日本信号株式会社
委員	福地　修一郎	日本信号株式会社
委員	小勝　俊亘	日本電気株式会社
委員	坂口　統	日本電気株式会社
委員	西　高宏	日本電気株式会社
委員	國枝　賢徳	パナソニック コネクト株式会社
委員	松原　僚亮	パナソニック コネクト株式会社
委員	見富　志朗	富士通株式会社
委員	渡辺　宏一郎	LINE Pay 株式会社
事務局	多田羅　政和	一般社団法人 ID 認証技術推進協会（JICSAP）
事務局	吉川　貴浩	一般社団法人 ID 認証技術推進協会（JICSAP）

記載順は、WG 役付委員を除き所属企業名称の五十音順。同一企業内では委員氏名の五十音順。

利用シーンに応じた「顔認証」導入要件等に関する研究 WG　活動経緯

＊2020 年 12 月 2 日（水）～2023 年 3 月 14 日（火）までの全 28 回、本報告書策定に係る活動として、JICSAP アプリケーション研究部会付け「利用シーンに応じた『顔認証』導入要件等に関する研究 WG」を開催した。

＜2020 年度＞

2020 年 12 月 2 日（水）	15:00～17:00	第 1 回 WG
2021 年 1 月 19 日（水）	15:00～17:00	第 2 回 WG
2021 年 2 月 17 日（水）	15:00～17:00	第 3 回 WG
2021 年 3 月 17 日（水）	16:00～18:00	第 4 回 WG

＜2021 年度＞

2021 年 4 月 20 日（火）	15:00～17:00	第 5 回 WG
2021 年 5 月 19 日（水）	16:00～18:00	第 6 回 WG
2021 年 6 月 16 日（水）	15:00～17:00	第 7 回 WG
2021 年 7 月 20 日（火）	15:00～17:00	第 8 回 WG
2021 年 8 月 17 日（火）	15:00～17:00	第 9 回 WG
2021 年 9 月 28 日（火）	15:00～17:00	第 10 回 WG
2021 年 10 月 19 日（火）	15:00～17:00	第 11 回 WG
2021 年 11 月 16 日（火）	15:00～17:00	第 12 回 WG
2021 年 12 月 21 日（火）	15:00～17:00	第 13 回 WG
2022 年 1 月 18 日（火）	15:00～17:10	第 14 回 WG
2022 年 2 月 15 日（火）	15:00～17:00	第 15 回 WG
2022 年 3 月 15 日（火）	15:00～17:10	第 16 回 WG

＜2022 年度＞

2022 年 4 月 19 日（火）	15:00～17:00	第 17 回 WG
2022 年 5 月 17 日（火）	15:00～17:00	第 18 回 WG
2022 年 6 月 21 日（火）	14:00～16:00	第 19 回 WG
2022 年 7 月 19 日（火）	15:00～17:00	第 20 回 WG
2022 年 8 月 23 日（火）	15:00～17:00	第 21 回 WG
2022 年 9 月 20 日（火）	15:00～17:00	第 22 回 WG
2022 年 10 月 25 日（火）	15:00～17:00	第 23 回 WG
2022 年 11 月 15 日（火）	15:00～17:00	第 24 回 WG
2022 年 12 月 20 日（火）	15:00～17:00	第 25 回 WG

2023年1月17日（火）　　15:00～17:00　第26回WG
2023年2月21日（火）　　15:00～17:00　第27回WG
2023年3月14日（火）　　15:00～17:00　第28回WG

以上

利用シーンに応じた『顔認証』導入ガイドライン

第 1.0 版（Ver. 1.01）

発行者：　一般社団法人 ID 認証技術推進協会
（JICSAP）
発行日：　2023 年 6 月 2 日