

# 顔認証における責任ある制限 ユースケース：フロー管理

第2部  
パイロットフェーズ：自己評価、監査管理システム、認証

白書  
2020年12月



# 目次

3	はじめに
4	序文
5	序章
7	方法論
9	1. 成田国際空港による自己評価調査票の検証
10	1.1 総合的な枠組みと目的
10	1.2 ケーススタディ:成田国際空港のOne IDプログラム
12	2. 行動原則の順守を検証するための監査枠組み
13	2.1 総合的な枠組みと目的
14	2.2 監査枠組みの構造
16	2.3 監査枠組みからの抜粋
17	3. フロー管理における顔認証技術の責任ある利用を担保するための認証スキーム
18	3.1 枠組みと目的
19	3.2 認証プロセス
20	4. 原則から認証まで:説明責任完了までの行程
21	4.1 顔認証システムが稼働しており、認証取得を希望する組織
23	4.2 顔認証システムの導入を予定している組織
24	4.3 重大な不履行がもたらす結果
25	5. 結論
27	用語集
28	投稿者
30	付属文書
30	付属文書A:成田国際空港の自己評価調査票回答例
36	付属文書B:監査枠組み
47	参考文献

# はじめに

## 顔認証技術の利用に信頼性と透明性を確保する、世界初のグローバルイニシアティブ



**Kay Firth-Butterfield,**  
Head of Artificial  
Intelligence and Machine  
Learning; Member of the  
Executive Committee,  
World Economic Forum



**Hideharu Miyamoto,**  
Senior Executive Officer,  
Narita International Airport  
Corporation, Japan



**Julien Nizri,**  
Managing Director, AFNOR  
Certification, France



**Toshifumi Yoshizaki,**  
Senior Vice-President, NEC  
Corporation, Japan

顧客や従業員、ベンダーを正確に識別するシームレスな非接触型テクノロジーの必要性はかつてないほどに高まっています。航空機の搭乗体験を向上させる顔認証技術とリモート型バイオメトリクス（生体認証）について、昨年世界経済フォーラムは、顔認証技術の責任ある利用を目指したガバナンス枠組みの構築イニシアティブをスタートさせました。昨年の時点ではこのような技術は「あれば便利」というレベルのものでしたが、新型コロナウイルスの世界的パンデミックという前例のない事態においてリモート型バイオメトリクスは必須となっています。

航空業界は数十年間デジタル技術を利用してきましたが、今やAI（人工知能）は待ち時間を短縮し利便性を向上させるなど旅客体験を根底から変えつつあります。しかしこういった進歩にはトレードオフやリスクもあり、顔認証によるバイアスや差別の助長、個人データの流出リスクに厳しい目が向けられています。これらの問題に先手を打つため、本白書ではフロー管理ユースケースにおける顔認証の責任ある利用にグローバルな定義を設定し、この定義を運用するためのガバナンス枠組みを構築しました。

成田国際空港株式会社（以下、成田国際空港）と日本電気株式会社（以下、NEC）は本イニシアティブに参加し、最初の白書「顔認証における責任ある制限を設定する枠組み — ユースケース：フロー管理」で提示された自己評価調査票を検証しました。本白書で

は両社の先駆的な取り組みと結果を公表し、顔認証技術に対してどのように透明性を担保し乗客の信頼を獲得するのか、業界関係者や政策立案者に知見を提供しています。

本白書のもう一つの目的は、顔認証技術を責任ある形で利用するための認証制度と第三者機関による監査に関する対話を促進することです。この点でAFNOR Certificationは本イニシアティブのパイロットフェーズの監査枠組みを設計する上で重要な役割を果たしてきました。現在は第三者認証スキームを検証したい組織がテストを行えるまで準備が整っています。

世界経済フォーラムは、本イニシアティブに参加して政策枠組みを検証・採用し、顔認証システムの信頼ある利用に貢献することを各組織に呼びかけます。

ケイ・ファース＝バターフィールド、AI・機械学習プラットフォーム責任者、世界経済フォーラム執行委員会メンバー

宮本秀晴氏、成田国際空港株式会社 上席執行役員

ジュリアン・ニズリ氏、AFNOR Certification マネージングディレクター

吉崎敏文氏、日本電気株式会社 執行役員



# 序文

## ● 第二弾となる今回の白書では、監査の枠組みと認証スキームという最後のステップに焦点

2019年4月、世界経済フォーラム第四次産業革命センターは「顔認証における責任ある制限」プロジェクトを立ち上げました。このプロジェクトは、堅牢なガバナンス枠組み設計に基づく信頼性と安全性の高い顔認証技術の利用に向け、具体的なガイドライン策定の必要性を説くことを目的としています。当フォーラムでは、最近イニシアティブに参加したフランスと日本をアンカーパートナーとして、マルチステークホルダーによるエビデンスに基づいた政策プロジェクトを主導しています。ワーキンググループの当初の構成員は、顔認証システムの調達を検討している業界の代表者（ADPグループ、フランス国有鉄道（SNCF））、テクノロジー提供者（アマゾンウェブサービス、IDEMIA、INグループ、マイクロソフト）、政策立案者（仏議会議員）、学者、市民団体とAFNOR Certificationでした。

顔認証システムに関するリスクはコンテキスト依存度が高いため、ワーキンググループはプロジェクト設計においてユースケースをベースにしたアプローチを採用しました。システムが搭乗プロセスの迅速化を目的としているか否かに関わらず、顔認証の偽陽性と偽陰性はその後の結果に大きな影響を与えます。したがって実際のアプリケーション、運用中の特定のシステム、そしてそのシステムによって影響を受ける可能性のあるステークホルダー集団（飛行機の乗客など）に焦点を当てることによって、関連するリスクを効果的に軽減するガバナンス枠組みを共同設計できる機会が拡大すると考えました。

検討の結果、ワーキンググループは主に「フロー管理」（顔情報をサービスへのアクセス手段として利用すること）に焦点を当てることとしました。今後、フロー管理のユースケースの拡大が見込まれることがその理由です。例えば東京オリンピックの主催者は選手とスタッフによるスタジアムや五輪施設へのアクセス管理に顔認証を利用すると発表しました<sup>1</sup>。また空港や航空会社も顔認証技術の利用を開始しています<sup>2</sup>。

バランスがとれた実行可能なガバナンス枠組みを設計するため、ワーキンググループは1) 行動原則を設定し、顔認証技術（FRT）の責任ある利用の構成要素を定義する、2) 行動原則の適用を支援するためのベストプラクティスを設計する、3) 自己評価調査票を通じて、行動原則が組織によって順守されているかを評価する、4) 監査の枠組みと認証スキームを通じて行動原則の順守を認証する、という4つの主要なステップから成る方法を考案しました。

認証スキームの設計に向け、監査と認証の世界的なエキスパートであるAFNOR Certificationとのパートナーシップが締結されました。空港にとって顔認証シ

ステムを導入する際の主な懸念点は顧客サービスの低下や中断であることに鑑み、主に2つの理由から顔認証アルゴリズムの監査ではなく、品質管理システムの監査の設計がAFNOR Certificationから提案されました。第一の理由は、空港会社は顧客に提供するサービスの品質に責任を負うことから、その品質を向上させるための方法についてガイダンスを必要としていることです。この点に関しては、ISO 9000品質管理規格に準拠した強固な基盤を構築することによってサポートすることができます。第二に、顔認証アルゴリズムを直接監査することは重要ではあるものの、認証機関にとっては根本的な課題を提起します。例えば稼働中のシステムの性能が常に進化している場合、認証する性能の閾値はどう設定すべきか。法的・倫理的配慮（公平性など）を評価可能な定量的要件にどう変換するのか。人工知能システムの説明可能性の欠如に対処し、解釈可能な決定を下すにはどうしたらよいのか。これらの複雑で未解決の疑問にはさらなる調査が必要です。それでも厳格な手続きのもと組織の監査を行うことで、フロー管理における顔認証技術の責任ある利用の第一水準を担保することができます。

日本のステークホルダーはこのような実践的なアプローチに関心を持ち、空港における顔認証技術の責任ある利用を進めるため、本イニシアティブに参加することを決定しました。日本政府とNECは世界経済フォーラム第四次産業革命日本センターに2名のフェローを派遣し、本イニシアティブの形成に不可欠な役割を果たしています。日本政府とNECは主に2つの理由から非常に重要なパートナーとなっています。第一に、顔認証技術は日本の空港で使用されているため、洞察力に富んだユースケースを提供することができるという点です。年間4,100万人が利用<sup>3</sup>する成田国際空港は昨年、顔認証技術を用いて保安検査と搭乗プロセスの合理化を実現するNECのOne IDサービス<sup>4</sup>を2020年より導入すると発表しました。最近では、日本政府が顔認証技術の利用を規制する生体認証データ保護のガイドブックを公表<sup>5</sup>しています。第二に、成田国際空港はこのプロジェクトの最初の白書<sup>6</sup>で提示された自己評価調査票を用いて顔認証システムの自己評価を行いました。このように、今回の連携は成田国際空港にとって国内と海外の乗客に透明性と説明責任を訴求する良い機会となりました。

2020年2月に発表された最初の白書では、この手法の最初の3つのステップが詳細に提示されています。第二部となる今回の白書では、監査の枠組みと認証スキームの紹介という最後のステップに焦点が置かれています。また、成田国際空港の自己評価調査票への回答も厳格な自己評価の一例として紹介されています。

# 序章

かつてないほど高まる顔認証技術に対する  
バランスのとれたガバナンス枠組みのニーズ



④ 世界経済フォーラムによる本イニシアティブの目的は、顔認証技術の責任ある利用を確立するために総合的なガバナンス枠組みを作ること

ここ数年、主に機械学習やセンサーの進歩による急速な技術進歩によって顔認証技術の開発が進んでおり、研究段階から産業界における導入期に移行しています。顔認証技術は今や銀行、小売、運輸、警察、さらにはヘルスケアなど、公私に渡る生活のさまざまな分野に拡大しています。

顔認証技術は認証と本人確認プロセスの強化のおかげで、電話ロックの解除、飛行機の搭乗、オンラインでの公共サービスへのアクセスなど、社会的に有益な利用の機会を大幅に増やしています。しかしながら、顔認証技術が市民的自由の低下や差別的な結果につながる可能性もあります。たとえば米国では、娯楽施設<sup>7</sup>が消費者に対して事前の通知や同意なしにこの技術を使用した事例があります。また、度重なるリモート型バイオメトリクスのデータ侵害事例<sup>8</sup>や、異論も多いデータスクレイピング手法<sup>9</sup>を使った強力なソリューション構築事例などが報告されています。最近では、この技術が無実のアフリカ系アメリカ人の不当な逮捕と拘束<sup>10</sup>につながった事件もありました。

このような論争をきっかけに政策活動が活発化しています。米国ではカリフォルニア州の2都市（サンフランシスコ<sup>11</sup>、オークランド<sup>12</sup>）、マサチューセッツ州の5都市（ボストン<sup>13</sup>、ブルックライン<sup>14</sup>、ケンブリッジ<sup>15</sup>、ノーザンプトン<sup>16</sup>、サマービル<sup>17</sup>）など、さまざまな自治体が市の機関による顔認証技術の使用を禁止しており、オレゴン州ポートランドの公共空間では利用の公私を問わず、顔認証技術の使用が禁止<sup>18</sup>されています。州レベルでは、ワシントン州が初めて政府による顔認証技術の利用に逸脱防止策を設置する法案を可決<sup>19</sup>しました。法執行機関による顔認証技術使用を恒久的に禁止する連邦法案<sup>20</sup>が民主党議員によって提案されています。本イニシアティブはさまざまな利害関係者によって議論されている数々の政策提案 – さまざまな原則<sup>21</sup>、モラトリウム<sup>22</sup>、そして顔認証技術の規制省庁の創設<sup>23</sup>など – を補完するものです。

さらに大手テクノロジー企業もこのテーマについての立場を公表しています。マイクロソフト<sup>24</sup>は、連邦規制が整備されるまでは法執行機関に顔認証技術を販売することはないとしています。アマゾンウェブサービス（AWS）<sup>25</sup>は、警察による同社のプラットフォーム「Rekognition」の使用を1年間停止しており、IBMは今後顔認証技術の提供、開発、研究を行わない<sup>26</sup>としています。

2020年2月に発表されたAI（人工知能）のガバナンスに関する欧州委員会の白書<sup>27</sup>では、顔認証技術の利用を制限するための追加要件を導入する可能性について積極的に議論されています。1月には同白書の草案で欧州委員会が適切な規制を策定するまで公共空間での顔認証利用を5年間停止<sup>28</sup>することを検討

と報じられていましたが、発表された白書ではこの言及はありませんでした。

このような政策活動の大半は政府および法執行機関による顔認証技術の利用に関わるもので、これは誤用のリスクや抑圧されたグループが監視されるリスクが高いのが、政府および法執行機関の領域にあるからです。確かに生体認証データの感度を考えると、顔認証の使用は本質的にリスクが高いといえます。顔認証を利用して飛行機に搭乗したり、スタジアムに入場したり、顔認証広告を小売で使用したりすることには、プライバシー侵害、属性グループの違いによって生じるパフォーマンスギャップに起因したサービスアクセスの不平等などのリスクが伴います。したがってユースケース全体にまたがるリスクの特定と実効性のあるリスクの軽減が必要となります。世界経済フォーラムの本イニシアティブの包括的な目的は、顔認証技術の責任ある利用を確実にするための総合的なガバナンス枠組みを確立することであり、このスタート地点がフロー管理という一つのユースケースシナリオです。

前白書「顔認証における責任ある制限を設定する枠組み – ユースケース：フロー管理」は、1) 先行テスト導入に基づく政策立案アプローチの提示と、2) それをフロー管理のユースケースへ適用するにあたり4段階で行う手法、という2部構成でした。今回の白書は4章から成り、第1章の成田国際空港のユースケースでは、NECと共同実施した自己評価調査票のテスト結果が詳述されており、回答は付属文書Aに記載されています。第2章ではAFNOR Certificationと共同設計した監査枠組みが紹介され、枠組みの機能、方向性、様々な利用法、構造が詳述されています。枠組みの全文は付属文書Bで参照可能です。第3章は認証スキームの目的、利点とプロセスを説明しています。最終章では、フロー管理への顔認証技術の使用が信頼に値すると実証するために業界関係者が完遂しなければならない行程が、原則から認証発行までの段階的なプロセスとして提示されています。各段階で実行すべき活動についても記載されています。

この2つの白書は顔認証技術の責任ある利用を目指す組織の力になるはずです。両白書には組織が確認すべき文献（行動原則、ベストプラクティス、自己評価調査票、監査枠組み）と、認証を取得するために必要なスキームが提示されています。

2つの白書は、地方、国、国際レベルで顔認証技術についての議論を促すという、より大きな目的にも寄与しています。議論および先行テスト導入は今現在も進行中であり、関係者および議論に関わる意志がある組織はぜひこの世界経済フォーラムの取り組みにご参加ください。



# 方法論

他の顔認証技術ユースケースでも  
再現可能な実証アプローチ



## 4ステップのアプローチ

最初の白書「顔認証における責任ある制限を設定する枠組み－ユースケース：フロー管理」では、顔認証の責任ある利用を担保する堅牢なガバナンス枠組みを構築するための4つの主要ステップ(図1)に基づいた方法を紹介しました。

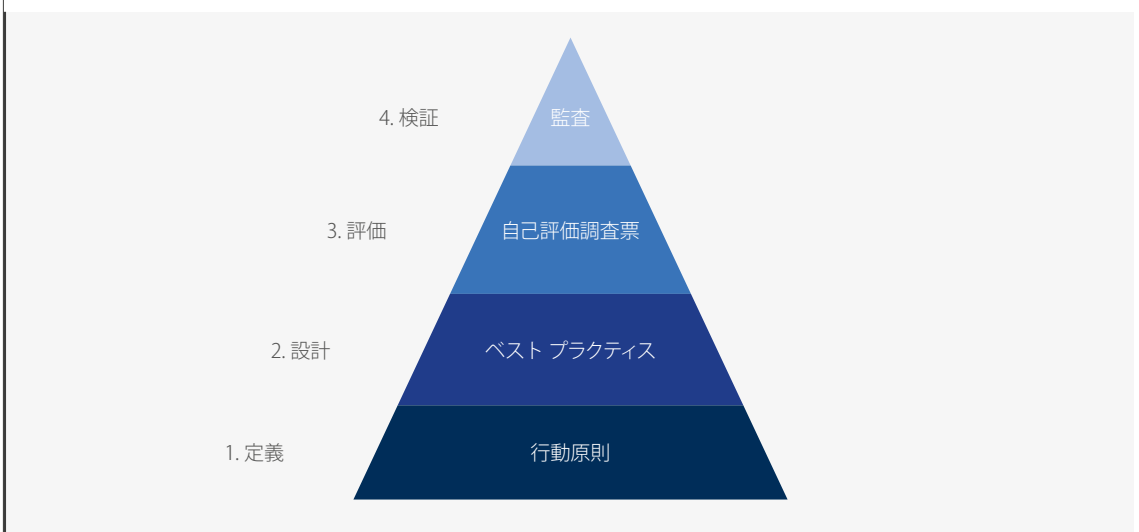
1. **定義：** 一連の行動原則を起案し、顔認証技術の責任ある利用の構成要素を定義しました。政府関係者、顔認証システムを設計・調達する企業、規制機関、学者、市民代表で構成されるワーキンググループの第一の目的は、11原則を中心とした共通の定義を確立することでした。
2. **設計：** 「設計段階から責任を織り込んだ」システ

ム開発を製品チームが行えるよう、ユースケースに合わせた方法論を設計しました。

3. **評価：** 行動原則の順守をユースケースごとに記述した自己評価調査票を通じて、設計されたシステムを評価しました。
4. **検証：** 信頼できる第三者による監査枠組みの設計を通じて、行動原則の順守を検証しました。

各ステップは、顔認証技術の信頼できる利用に向けて業界各社が段階的に追加できるコミットメントのレベルとなっています。

図1： フロー管理ユースケースにおいて顔認証技術の責任ある設計と利用を確保するための4つのステップ



出典) 世界経済フォーラム白書「顔認証における責任ある制限を設定する枠組み－ユースケース：フロー管理」、2020年2月

## 運用前の方針策定パイロットプログラムでのテスト

ガバナンス枠組みの各要素(行動原則、ベストプラクティス、自己評価調査票、および監査枠組み)は方針策定パイロットプログラムでテストされ、実践の知見に基づいて評価されます。結果が満足のいくもの

であった場合、認証スキームへと移行します。認証スキームは本イニシアティブで重要な役割を果たしたAFNOR Certificationを始めとする提携認証機関と連携する形で展開されます。

## 再現性と拡張性のある方法

この4ステップの方法論は他の顔認証ユースケースでも再現可能です。顔認証技術の責任ある展開戦略はどのようなものであれ、その領域における責任ある利用の構成要素を明確に定義するところから始めなくてはなりません。これはマルチステークホルダーのアプローチを通じて一連の原則を立案することで達成できます。適切な設計要件またはベストプラクテ

イスがあれば、その後の製品開発にこの定義を適用することができます。最後に、カスタマイズされた自己評価調査票でテストし、監査枠組みの設計で検証することが可能です。したがって関心を持っているステークホルダーが実施しなければならないのは、これらのツールを自分の環境と業界に適応させるためにはどの項目が必要かを決定するのみになります。



1

# 成田国際空港による 自己評価調査票の検証

初となる顔認証技術の自己評価結果の公開



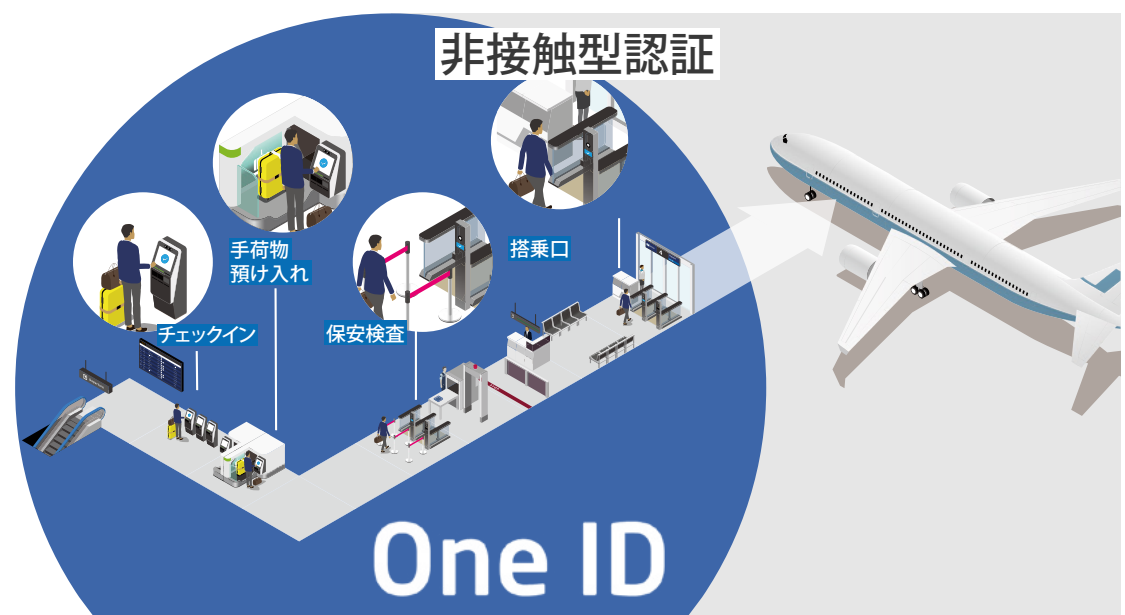
## 1.1 総合的な枠組みと目的

自己評価調査票は、行動原則を確実に順守するために各組織が満たすべき要件を示す自己評価文書としての役割を果たします。成田国際空港のように調査票を単独で使用して既存のプロセスの内部評価を行う（以下を参照）こともできますし、認証プロセスの準備状況を測定するツールとして使用することもできます（第4章を参照）。

自己評価調査票の作成にあたっては、経営陣が任命する部門横断タスクフォースが、各行動原則を取り組むべき具体的な質問に分類します。この点はそこまで詳細に渡ったものではないものの監査の枠組みに似ています。

## 1.2 ケーススタディ：成田国際空港のOne IDプログラム

### ケーススタディの概要



One ID プログラムによってチェックイン、手荷物の預け入れ、保安検査場への入場から搭乗口までの過程がスピードアップします。

出典：NEC提供

世界有数の空港会社である成田国際空港は、利用者に最高の旅客体験を提供することを目指しており、その取り組みは日本が世界でも人気の旅行先であるという観点からも重要です。そのため同空港はチェックインから搭乗までの過程を迅速化する、顔認証技術を利用した「One ID」プログラムの導入を決定しました。このプロジェクトは、乗客が搭乗までの全プロセスを「歩く速度（ウォーキングペース）」で完遂するという明確なビジョンのもと2016年にスタートしました。

このシステムは、セルフサービスキオスクなど最初のタッチポイントで記録された乗客の顔データを利用する設計です。顔データは、乗客のICチップ搭載パ

スポートおよび搭乗券情報に連動しており、乗客はパスポートや搭乗券を提示することなくすべての搭乗手続きを完了することができます。保安検査場への入場や搭乗手続きで立ち止まることなく、歩く速度で通過することができるようになり、乗客が搭乗にかかる時間を大幅に短縮することができるようになると同時に、ウイルスが拡大するリスクを低減させ、新型コロナウイルスのような病気の蔓延を防ぐことにも役立ちます。

同様の解決案を展開することに関心を持っているであろう業界関係者に向けてOne IDプログラムについて紹介します。

### One ID顔認証システムの主な特徴

#### ユーザー体験

航空会社が搭乗ゲートで乗客全員を搭乗させるのに要する時間は通常15分程度です。これを目標として3レーンで250人の乗客を15分以内に搭乗させる実験を設計しました。システム要件

を実装するにあたっては、成田国際空港は法務省出入国在留管理庁の仕様<sup>29</sup>に従い、また米国国立標準技術研究所（NIST）<sup>30</sup>による自動顔認証アルゴリズムの評価結果<sup>31</sup>を参考にしました。

乗客がチェックインから搭乗までウォーキングスペースで進む顔認証システムの実装には、単に顔認証システムの処理能力だけではなく、包括的なアプローチを採る必要がありました。そこでソリューションを提供するNECは、他のベンダーと連携して各タッチポイント（チェックイン時、手荷物預け入れ時、保安検査時、搭乗時）におけるシステムの可用性、信頼性、性能を検証しました。

### バイアスの緩和

顔認証技術に関連したバイアスの問題に対処すべく、成田国際空港はこの分野で世界を牽引するテクノロジープロバイダーのNECを選択しました。NISTは2019年に4つの大規模なデータセットを用いてロバスト調査<sup>32</sup>を行い、顔認証ソフトウェアにおける人種、年齢、性別の影響を調べました。この調査では849万人の約1800万枚の画像を含む連邦政府のデータセットを用いて189のソフトウェアアルゴリズムが評価され、有色人種と女性では顔認証ソフトウェアに有意なバイアスが確認されました。その中でNECのソリューションは高精度を達成し、年齢、性別、民族間のバイアスが最も少ない類に入りました<sup>33</sup>。また成田国際空港は、障害者を取り残さない包摂的な社会を創ることを目的としている国土交通省（MLIT）の「ユニバーサルデザイン基本計画」<sup>34</sup>と、東京オリンピック・パラリンピックに向けた「Tokyo 2020アクセシビリティガイドライン」<sup>35</sup>の実現に取り組んでいます。

NECは顔認証ソフトウェアの設計、検証テストの実施やパラメータ調整を主に担当するとともに、航空会社と連携し、機器設置、照明環境、運用テスト、トレーニングシナリオも担当しました。

### データ保護

顔認証は生体認証技術の中でも最もセンシティブな技術です。そのため顔認証の導入には細心の注意と配慮が必要であり、成田国際空港を利用する年間4000万人以上の乗客のプライバシーに与える影響を考慮しなければなりません。日本政府はこの課題を十分に認識しており、空港において責任ある顔認証技術の導入をするため、MLITは国際航空運送協会（IATA）、個人情報保護委員会、法律専門家、消費者団体の代表者から成るマルチステークホルダーのタスクフォースで「One ID導入に向けた個人データの取扱検討会」を任命しました。ワーキンググループは1年間の調査を実施し、空港でのOne IDプログラム<sup>36</sup>を通じて収集された個人データの管理に関する多面的なガイドブックを発表しました。この文書には、One IDサービスに関わるプライバシーリスクに対処し、高レベルのデータ保護を行うために空港が従うべきプロセスの一覧が含まれています。

成田国際空港はすべてのガイドブックを厳格に適用し、One IDプログラムを責任を持って運用しています。特にデータ漏洩などの重大なリスクに関わるプロセスには細心の注意を払っています。サイバー攻撃は巧妙化しており、政府やグローバル企業であっても防ぐことがますます困難になってきています。このリスクを軽減するため、One ID導入に向けた個人

データの取扱検討会のメンバーは収集した生体認証データを24時間以内に削除することを推奨しており、成田国際空港ではサイバーテストを定期的実施することでサーバーの堅牢性を検証しています。

### 自己評価についての振り返り

成田国際空港では、2016年に導入の検討を開始した当初からフロー管理における顔認証技術の責任ある使用に取り組んできましたが、当時はその目的のために実施すべきプロセスを示した公的なガイドライン等がありませんでした。そのため同空港は当初内部で実施していた過去4年分の振り返りを、この世界経済フォーラムのイニシアティブを活用して日本から世界に広げることを促進します。

MLITがOne ID導入に向けた個人データの取扱検討会とガイドブックの公開を通じて開始した、このマルチステークホルダーのプロセスは有意義なものでした。情報に対する権利や同意に関することなど、調査票に記載されている項目の多くがガイドブックでも扱われているため、自己評価フェーズの準備でも役立ちました。本テーマに関して日本が世界をリードしていることは知られていますが、調査票の回答を見ると（付属文書A参照）さらに前進しており、本取り組みを通じて国内・海外の乗客の信頼度がさらに向上することが期待されます。

しかし、ここに到達するまでには時間がかかりました。成田国際空港は2020年2月初旬に世界経済フォーラムの「顔認証における責任ある制限」イニシアティブに参加しましたが、自己評価プロセスが開始したのは5月初旬で、完了までには6週間と当初の予定よりも長い期間が必要でした。時間を要した要因は2つあります。ひとつには、自己評価調査票はシステム管理のあらゆる側面を網羅した包括的なものであるため、すべての質問に答えるには成田国際空港とNECの様々な部門の関与が必要でした。網羅する要素はデータガバナンス（データセキュリティやプライバシー等）、性能と精度、ユーザーエクスペリエンス（UX）と多岐に渡りました。2つ目は、新型コロナウイルスの感染が拡大し、日本政府が緊急事態宣言を発令したことで活動に中断期間が発生したことでした。

成田国際空港は、本検証が自己評価調査票とそれに付随するプロセスの改善に役立つことを願っています。例えば成田空港ではデータセキュリティに関する項目の強化を推奨しており、チェックインから24時間以内に生体認証データを削除するという同空港の手法を他の事業者も採るよう奨励しています。また、顔認証技術の責任ある利用を担保するために導入されたプロセスは十分な堅牢性を備えているため、本プロジェクトの方法論が提案するような外部監査を実施する必要性は低いかもしれません。One IDプログラムは政府関係者、成田国際空港、航空会社、様々なベンダーや法律専門家が参加するマルチステークホルダー・プロセスを経て設計・実装されています。プロジェクトのパートナーが各自の組織文化に合った実施メカニズムを選択できることが重要になるでしょう。



2

## 行動原則の順守を検証するための監査枠組み

顔認証技術の責任ある利用を確かなものとし、リスク軽減プロセスを検証するための品質管理システム監査



本章では、フロー管理のために顔認証技術を導入した組織が行動原則に準拠していることを検証する監査枠組みの立案に向けたAFNOR Certificationとの共同作業について詳述しています。総合的な枠組みとその目的、利用方法と構造、完了までの事例（監査枠

組みの全文は付属文書Bに記載）を紹介し、また、成田国際空港が実施した自己評価調査票を用いた試験運用から得た考察に基づく、最新版の行動原則についてもまとめています。

## 2.1 総合的な枠組みと目的

### 監査枠組みの機能

監査枠組みの役割は、定義された範囲の監査にかかる要件とプロセスを詳述した参照文書として利用されることです。そのため、この枠組みはベストプラクティスに関するガイダンスの提供、内部監査の実施、新規プロジェクト開発においてプロバイダーが満たすべきニーズを策定する支援に利用できるほか、任意または必須の認証プロセスに参加することを可能にするためにも活用することができます。通常は、監査枠組みの必要性を認識しているステークホルダーがその利用法についても決定します。マルチステークホルダーのコミュニティはこのパイロットプロジェクトの範囲において、フロー管理アプリケーションにおける顔認証技術の責任ある使用について定めた行動原則に準拠していることを検証するツールとして使用できる監査枠組みを立案しました。

### フロー管理アプリケーションの設計

この監査枠組みはフロー管理アプリケーション向けに設計されています。つまり、飛行機への搭乗時やコンサート会場への入場時などサービスの利用に個人の顔の特徴がキャプチャされる場面に限定されます。システム上でサービスを利用するか否かをユーザーに委ねるオプトイン（事前許諾制）が提供されている点が、ユーザーの知識や同意なしに顔認証が導入されるユースケースとは大きく異なります。監査枠組みは行動原則への準拠を検証すると同時に、生体認証データのガバナンスに関する懸念（同意、プライバシーなど）、属性の違いと顔認証システムの性能に関する懸念（バイアスの特定と緩和、性能閾値の定義など）、システムのユーザーエクスペリエンス（UX）を通じたエンドユーザーへの権限付与（情報表示、アクセス権、代替オプションの利用可能性など）に対応するものになっています。フロー管理アプリケーションにおける顔認証の責任ある利用に向けた初の包括的な枠組みとなることを目指していますが、他のユースケース（令状やテロリスクに基づく容疑者の追跡、小売業でのパーソナライズされたショッピング、希少疾患の識別など）やそれらに関連するリスクは適応外です。

### 方針策定パイロットプログラムでの事前テスト

監査枠組みは、AFNOR Certificationや任意参加の空港の協力を得て、方針策定パイロットプロジェクトの結果に基づきテストとレビューが実施されます。そこで十分な結果が得られれば、パートナーの認証機関との協力のもと、監査フレームワークが展開されていくでしょう。

### 品質管理システムの監査

この監査枠組みの草案にあたり、ワーキンググループはエンドユーザーに提供されるサービスの低下・中断につながるリスクを軽減することに焦点を当てました。例えばキャプチャした顔の特徴を利用して乗

客を旅客機に搭乗させる場合、属性グループや身体的特徴が顔認証技術の性能に影響を及ぼしたとしても、サービスを乗客が平等に利用できるよう保証するにはどのようなプロセスを導入すべきか。システムが機能不全に陥ったときに乗客がフライトに乗り遅れる事態を防ぐような、無理のない代替手段はどのようなものか。この枠組みが顔認証システムのアルゴリズムではなく、管理の監査のために設計されているのはそのためです。ワーキンググループがこのような決定を下したのは、顔認証技術の利用者（交通機関やイベント組織など）が顧客に提供するサービスの質に対する責任を負うからです。その点で、行動原則は高品質の顔認証システムの設計と運用の要件として機能する一方で、監査枠組みはエンドユーザーへサービスを確実に提供するために実施すべきプロセスを詳述しています。

### 欧州視点からの構築

監査枠組みの初版は、自己評価調査票と同様にマルチステークホルダー・プロセスを経て起草されました。草案に際してはEU一般データ保護規則（GDPR）に細心の注意を払い、欧州連合（EU）におけるAI（人工知能）技術の倫理的使用を目指しまとめられた、欧州委員会のAIに関するハイレベル専門家グループによる「信頼できる人工知能に関する倫理ガイドライン」も考慮されています。つまり、データ保護責任者はこの枠組みを法的支援と併せて活用することで、EU市民のデータを処理するとき、または日本など、GDPRに基づいてEUと適切な合意を締結した国<sup>37</sup>で業務を行うときにEUデータ保護当局とのコンプライアンスを確認することができます。GDPRが適用される管轄区域に拠点を置いていない組織でも、フロー管理アプリケーションで顔認証技術を使用する際は、エンドユーザーのためにシステムの責任ある管理を改善すべくこの監査枠組みを利用することが推奨されます。実際に世界中の多くの地域でGDPRをグローバルな羅針盤としてデータ保護法の検討が進められています。このような観点から、本白書で紹介したイニシアティブの取り組みは将来、保護法に顔認証技術を統合する一助となると考えています。

### 監査枠組みの使用法

前述したように、マルチステークホルダーのタスクフォースは、監査枠組みをフロー管理アプリケーションにおける顔認証技術の責任ある使用について定める行動原則へ準拠していることを検証するツールとして使用するとしました。しかしながら、この検証はさまざまな補完的な形で実施されることがあります。組織が監査枠組みを使用する方法として以下の4通りがあります。

1. **ベストプラクティスに関するガイド** 組織はこの監査枠組みを顔認証システムの責任ある設計と展開をするための指針として使用することができ

ます。この場合、枠組みは関係する内部チームと外部のプロバイダーがプロジェクト開発中に順守する必要がある仕様と統合されます。

2. **自己評価** 顔認証システムを導入しようとしている組織、または導入した組織は、自己評価調査票と同様の形で監査枠組みを使用して自己評価を行うことができます。ただこの監査枠組みはより包括的であるため、自己検証プロセスはさらに厳密な形で行われます。
3. **認証** 信頼できる第三者機関、理想的には認定を受けた認証機関は、行動原則を順守する意思のある組織が実施するプロセスの堅牢性を評価することができます。

4. **規制** 政策担当者は、フロー管理アプリケーションにおいて顔認証技術を使用している業界関係者に監査を受けるように求める法案を可決することもできます。この場合の監査は法定監査となります。

監査枠組みの第3の用途である認証はこのプロジェクトのために選ばれたもので、これについては次章で説明します。AFNOR Certificationはこのイニシアティブに参加する最初の認証機関ですが、監査枠組みのテストと検証が終了した後は、他の認証機関も招待してこの認証を世界的に提供するためのネットワークを構築していく予定です。

## 2.2 監査枠組みの構造

### “方針策定パイロットプログラムの結果に基づき更新される10原則

監査枠組みを構築するため、行動原則は監査で検証されるべき要件へと形を変えています（以下で説明）。要件は基準ごとに列挙され、3種類に分類されています。

#### 行動原則

初版の行動原則は2020年2月発行の最初の白書で発表されました。マルチステークホルダープロセスで共同草案されたこの原則は、フロー管理アプリケーションにおける顔認証の責任ある使用に向けた要素について定めています。当初は11の原則が挙げられていましたが、効果的な実装、完全性、関連性を確保するためにテスト段階で見直され、改訂されました。その結果、現在では10の原則へと変更されましたが、方針策定パイロットプログラムの最終結果に基づいて今後もアップデートされていく可能性があります。

1. **目的につり合った顔認証システムの使用**  
顔認証システムは使用目的に応じて高度にカスタマイズされるべきです。顔認証システムを使用する組織は、使用するシステムの能力と限界を評価し、そのシステムが目的に適したものであることを確認するための措置を講じる必要があります。
2. **リスク評価**  
顔認証プラットフォームを作成する組織や、サービスやシステムの一部として顔認証を使用する組織は、プライバシーへの影響、エラーの可能性、不当なバイアス、ハッキングやサイバー攻撃に対する脆弱性、意思決定プロセスの透明性の欠如、公民権や人権侵害の可能性などを含む、システムの包括的なリスク評価を行うべきです。
3. **バイアスと差別**  
顔認証システムを使用する組織は、すべての不当なバイアスや結果（顔認証技術に認識されずサービスの質が低下すること）を可能な限り検出し、特定し、改善するために適切な措置を講じるべきです。組織は、バイアスを完全に除去することがAI研究における最大の課題の一つであることを認め、バイアスや不当な結果を最小化するツールやプロセスの実装に必要なリソースを割り当てなければなりません。

4. **プライバシー保護のための設計**  
顔認証システムを利用する組織は、業務支援やシステムの維持だけでなく、システム要件におけるプライバシーへの配慮やテクノロジーの設計・開発・テストなどによってプライバシー保護を支援するシステムを設計する必要があります。
5. **性能**  
顔認証プラットフォームを作成する組織や、サービスやシステムの一部として顔認証を使用する組織は、設計段階（ラボテスト）と展開段階（フィールドテスト）の両方において、システムの精度と性能を評価するための基準に従うべきです。また、性能評価は第三者機関によって監査可能なものとし、システムのユーザーが報告書を利用できるようにすることが求められます。
6. **情報に対する権利**  
顔認証システムの使用に関して質問がある、または情報を必要とするエンドユーザーに情報を提供するためのプロセスを整備すべきです。また、エンドユーザーが希望する場合は自分の生体認証データにアクセスできるようにすべきです。
7. **同意**  
顔認証システムの使用については、説明に基づき、個人が自由に、明確で明示的な同意を提供する必要があります。したがって、明示的な同意なしに固有の生体認証識別子を作成したり維持したりするべきではありません。データの対象者が顔認証技術を利用した新しいサービスに登録するときはいつでも、データ保持期間およびデータ保存の条件に関して明確な同意を表明しなければなりません。
8. **情報の表示**  
顔認証技術を公共の場で使用するとき、それははっきりとした形でエンドユーザーに伝えるために分かりやすく表示すべきです。顔認証システムが使用されるエリアは常にしっかりと区分され、また視覚的な標識を使用してシステムが稼働中であることを個人に分かるように表示する必要があります。



#### 9. 社会的弱者に対するアクセス権

顔認証で除外される人がいてはいけませんし、高齢者や障害者を含むすべてのグループの人々がいつでもアクセスし、使用できなければなりません。例外的に、乳幼児や子供などはこの原則から除外され、顔認証に代わる手段を提供すべき場合があることは認められています。

#### 10. 代替的な選択肢と人間の常駐

公民権侵害を引き起こすなどの重大な結果をもたらす可能性のある使用については、人間によるレビュー（人間による監督）を実施する必要があります。完全自動化されたシステムの場合は、例外や予期せぬエラーへの対処、改善を実施するため、人間が常駐する代替システムを常に設置しておくべきです。顔認証システムに対する妥当な代替手段を常に用意しておく必要があります。

#### 三種類の要件

監査要件へのコンプライアンスはプロセス設計段階、実施段階、運用段階の3つの重要な段階で評価されます。

- 顔認証システムの設計で導入されたプロセスに関する要件 設計段階で導入されたさまざまなプロセスと割り当てられたリソースを評価しま

す。目的は責任ある、信頼できる形での顔認証技術の展開と利用を設計で担保することです。

- 顔認証システム稼働中に実施されるプロセスに関する要件 システムの稼働後も確立されたプロセスに則しているか、継続して実施されているか、長期にわたり維持されているかを検証します。システムの耐久性を確認し、システムの用法や当初の目的からの逸脱がないことを検証することが不可欠であり、これらの要件は**設計段階で設定された期待値を確実に満たすことで、システムの運用・管理に対する信頼を築く一助となっています。**
- システムの機能に関する要件 システムが行動原則に従って動作していることを検証します。一部は設計段階で設定された要件と関連しています。これらの要件によって、システム運用のスナップショットをとらえ、ユーザー体験を検証し、システムが行動原則に従って動作していることを確認するための様々なテストを実行することが可能となり、**システムの責任ある利用**を検証します。



## 2.3 監査枠組みからの抜粋

監査枠組みの全文は本白書の付属文書Bに記載されていますが、その構造を説明するために抜粋を下記に記します。

－ 左の欄には要件番号が記載されています。

－ 中央の欄には要件の説明が記されています。

－ 右の欄には上述した該当する要件の種類が記載されています。

### 顔認証システムの適切な利用

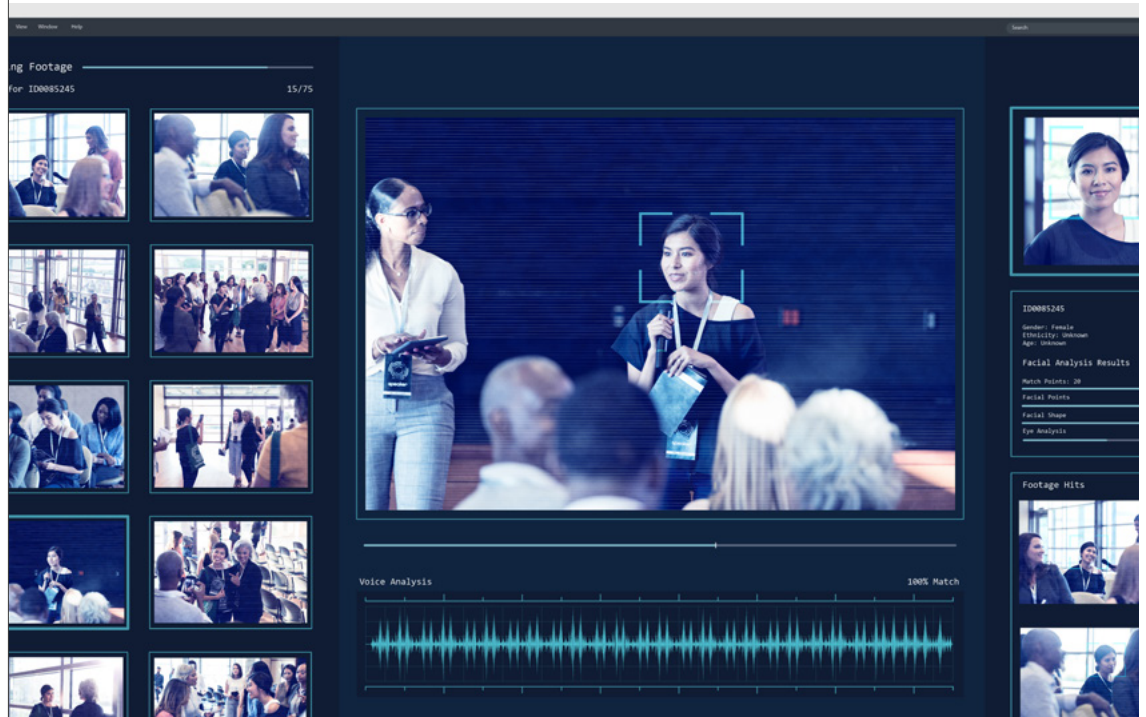
**要件：** 顔認証システムは使用目的に応じて高度にカスタマイズされるべきです。顔認証システムを使用する組織は、使用するシステムの能力と限界を評価し、目的に適したものであることを確認するための措置を講じるべきです。

要件番号	標準的要件の説明	関連するプロセス要件		
		設計	実装	システムの機能に関する要件
1.1	どのような顔認証プロジェクトにおいても、顔認証システムの使用を検討するに至った必要性を説明する必要があります。	✓		
1.2	企業は、システムに割り当てられた目的を達成するための技術的要件を記述し、システムが意図した目的にのみ使用されることを確認しなければなりません。	✓		
1.3	<p>同じニーズを満たす代替案（顔認証以外）にどのようなものがあるかを判断する必要があります。</p> <p>ニーズを満たす、顔認証システムの代替として使用可能な選択肢を特定する必要があります。</p> <p>可能な解決策を分析するための文書化されたプロセスと方法論を用意する必要があります。</p> <p>顔認証技術の使用と、目的および問題解決との関連性を評価します。</p> <p>そのために企業は評価と選定の方法を詳述し、その中には少なくとも以下を含める必要があります。</p> <ul style="list-style-type: none"> <li>－ 特定されたすべての解決策について判明した長所と短所のレビュー</li> <li>－ システムがさまざまなステークホルダー（ユーザー、国家、市民など）にもたらすと期待される便益の定義</li> <li>－ 偽陽性と偽陰性（特に公民権侵害のリスク）の状況を対象としたリスク分析</li> <li>－ 想定される便益の定量的評価</li> <li>－ さまざまな解決案の比較分析</li> <li>－ 解決案として顔認証を選択するに至った結論</li> </ul>	✓		
1.4	顔認証技術の選択に至った前提を検証するために、企業は顔認証の使用の関連性を検証する際のパラメータを定義する必要があります（想定される偽陽性および偽陰性の率や想定性能など）。	✓		
1.5	これらのパラメータは使用段階においてチェックされる必要があります。		✓	
1.6	顔認証システムは、特定の用途の枠組みの中で特定のニーズを満たすために導入されました。顔認証システムを使用する場合は、当初計画された用途に限定し、それらの用途について検証する必要があります。			✓

3

## フロー管理における顔認証 技術の責任ある利用を担保 するための認証スキーム

信頼性の高い監視を確保するために、独立した  
第三者機関が担保する認証スキーム





ワーキンググループは、行動原則へのコンプライアンスを検証する方法のうち、認証に焦点を当て、第三者機関である AFNOR Certificationと提携することを決定しました。同機関は、監査の枠組みを使用し、任意で参加する業界関係者の監査を実施します。今後、認証スキームの検証が進めば、認証機関が監査枠組

みに沿って顔認証技術の評価を行うために必要な能力や資格が特定されることになります。そのような能力と資格を兼ね備えている認証機関には、この認証スキームを導入し実行することを奨励します。本章では、認証スキームの総合的な枠組み(目的、仕組み、対象者など)と認証プロセスの詳細を説明します。

## 3.1 枠組みと目的

### 認証スキームの機能

この認証スキームは、1) 認証を受けるシステムやサービスが事前に定められた品質基準(有効性、効率性、安全性、社会的価値や規範の順守)を満たしているかの確認、および2) 品質の継続的な改善の奨励、を最終的な目標としています。独立した評価を実施し、特定のシステムまたは製品について監査の枠組みで定められた要件をもとに客観的な判断を行うことによって、これを達成します。この認証スキームの当面の目標は、コンプライアンスのレベルを決定することです。そのためこのスキームは、製品やシステムの信頼性の実証を目指す業界関係者にとって、堅牢でありながら柔軟なメッセージを提供することにあります。このプロセスに参加する組織は、通常、競争力の向上、ベストプラクティスの推進、顧客やパートナーとの信頼度の向上、規制要件の順守など、さまざまな目的を追求しています。

### 品質管理の認証

前述したように、品質管理のシステム監査は、ISO 9000ファミリー規格と同様に共同設計されたものです。したがってこの認証スキームは、フロー管理アプリケーション用の顔認証システムの管理に焦点を当て、行動原則へのコンプライアンスを検証対象としています。このイニシアティブの範囲からはずれている認証(製品、サービス、専門技能など)も数多くあります。また認証スキームは申請機関の目的や市場の需要に応じてあらゆる形態をとります。以下では、関連領域における3種類の認証例を紹介し、認証スキームをどのように発展・応用しうるかを説明します。

### 関連領域で認証を受ける利点

- 市場に参入するために必要なステップとしての認証 デジタル領域で新しい市場に参入しようとするサービスプロバイダー、特に大規模な組織や公共部門の組織と連携しているサービスプロバイダーは、ISO/IEC 27001の認証を取得することで情報システムのセキュリティを担保する能力を証

明する必要があります。このような認証により、クライアントは国際的に認められたデータセキュリティプロセスの実装を通じてサービスプロバイダーに委託したデータの機密性、整合性、および可用性を確保できます。

- 規制で許可されている任意のプロセスとしての認証 欧州において個人データを処理する組織にはGDPRを順守する義務があります。この一環として、個人データを委託する下請業者もこの規制に準拠している必要があります。下請業者はGDPR第42条が定めるGDPR認証を受けることで元請業者の不安を解消し、優位に立つことができます。
- 法規制で引用されている認証 フランスでは、医療専門家を代替する形で個人健康データのホスティングサービスを提供する組織は、健康データホスト(HDS)の認証書を取得する必要があります。この部門別の法的義務によって、個人の健康データなどの機密データを処理する主体が、確実なデータ保護のために技術的・組織的な対策を実施することが保証されるのです。

### 認定すべき主体とは

AFNOR Certificationによる監査枠組みのテストと検証が完了した後、目指すべきは他の認証機関がこの枠組みを利用できるようにすることです。さらに、認証プロセスの独立性と公平性を確保するために、認証機関はISO/IEC 17021-1:2015に従って業務を遂行する必要があります。この規格には「あらゆる種類の管理システムの監査と認証を提供する機関の能力、一貫性、公平性に関する原則と要件」<sup>38</sup>が含まれています。この点は今後認証スキームが検証される際に、顔認証技術の評価を有意義に行うために必要な具体的能力や資格の特定等、さらに詳しく検討されることになるでしょう。

## 3.2 認証プロセス

### 対象とする範囲

この認証スキームは、公共または民間の組織が運営する顔認証技術のフロー管理アプリケーション専用設計されています。そのため、この監査枠組みでは顔認証システム管理のどの側面が認証の対象となり、どの側面が認証の対象外となるかが明確に示されています。

### 認定対象

フロー管理に顔認証技術を用いるあらゆる組織がこの認証スキームの対象となります。また、このスキームはシステムの構築を開始し、責任ある管理に向けた最善の方法を考えている設計段階でも、システムを運用中で管理の質を向上させたいと考えている段階でも、どちらにも適用できます。いずれにせよ、評価の対象となるのは、監査の枠組みの要件を効果的に順守しているかどうかという点です。

### 費用の負担者

これは認証書による品質マネジメントシステムの確立を目指す業界関係者や公的機関を対象とした任意の認証スキームであるため、認証プロセスにかかる費用は申請組織が負担することになります。

### 認証監査のアプローチ

認証機関から監査を委託された監査人は、認証プロセスに関わるさまざまな部門と協力し、予定されるプロセスの効果的な実施と監査枠組みの要件への準拠を現場で評価する必要があります。このプロセスには従業員との面接や話し合いが含まれます。また、監査人によるレビューを可能にするため、監査枠組みに適合しているとする根拠は申請組織が用意する必要があります。監査人は、監査に先立ち、申請組織に対してどの従業員機能が審査の対象となる可能性が高いか、またどのようなコンプライアンスの根拠が収集・評価されるかについて明確なガイドラインを提供しなければなりません。

監査では、監査人はAFNOR Certificationの助言により設定された5つのカテゴリーに基づき観察を行います。

- **重大な不履行:** 顔認証管理システムの運用、効率、または改善に疑問を生じさせるような要件の不履行

重大な不履行は是正処置の対象であり、認証書の発行前に対処されなければなりません。

- **軽微な不履行:** 指定された要件を満たしてはいないものの、顔認証管理システムの有効性または改善を損なうほどではない

軽微な不履行は是正措置の対象となるべきものではありませんが、それ単体では認証書の発行を妨げません。

- **要観察な点:** 不履行の潜在的リスク

たとえ認証枠組みの要件を順守しているように見うけられても、組織は慣行を修正し、不履行の潜在的リスクを排除する必要があります。

- **長所:** 認証要件に対応して観察される通常レベルの性能を超える行為

- **注意点:** 監査枠組み要件の順守に関わる観察事項

監査の完了後、監査結果が記載された報告書が申請組織に送付されます。そこで不履行問題が指摘された場合、申請組織は補足文書と実施予定の行動計画を提出することで対応することができます。

### 認証と認証書の発行

監査報告書と監査人の勧告に基づき、認証機関は認証書の発行か追加検証（遠隔監査または現場監査など）の要求、またはその双方の実施について決定します。これを受けて、監査中に是正処置が決定された場合は、その完了を条件に1年間有効の認証書が発行されます。認証書には認証範囲に含まれる顔認証システムの管理側面が明示されます。AFNOR Certificationの監査を受けて認証された組織はAFNOR Certificationのウェブサイトに記載されます。

4

## 原則から認証まで： 説明責任完了までの行程

主要な要素としての外部監査を含む  
成功に向けた実行計画





認証は、フロー管理アプリケーション用顔認証システムの管理を継続的に監視・改善するための実用的なツールを提供することを目的としています。認証書の発行というマイルストーンに向けての行程は大きく2段階に分けることができます。

1. **準備段階** 認証スキームへの申請を検討している組織は行動原則をレビューし、ベストプラクティスを実施し、自己評価調査票を使ってプロセスを自己評価し、認証プロセスの一環として面接の対象者リストを作り、収集・評価の対象となるエビデンスを準備しなければなりません。これによって

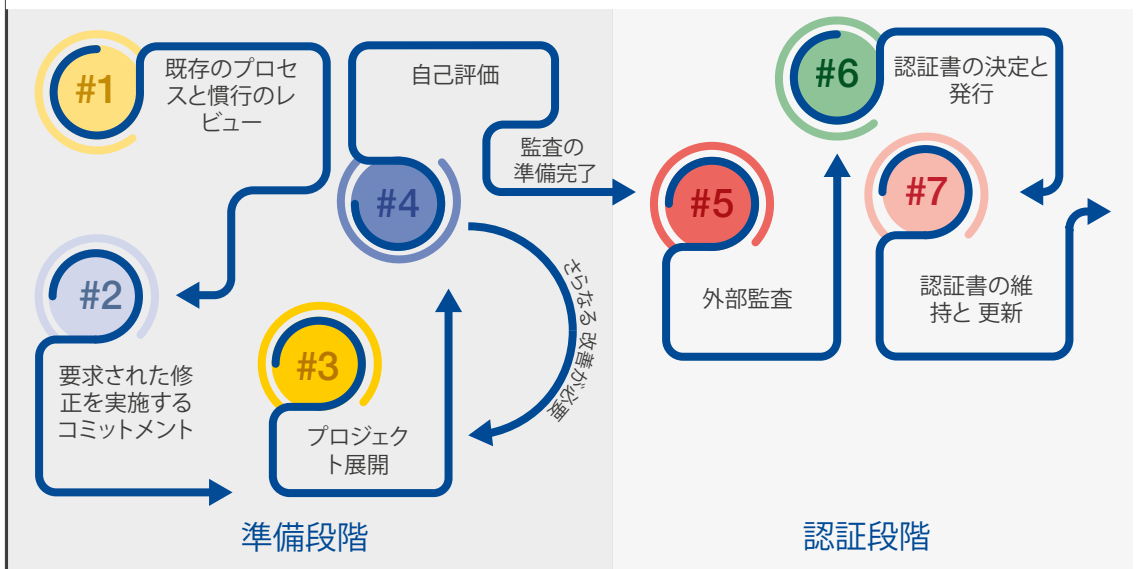
外部監査を成功させ、負担を最小限に抑えることができます。

2. **認証段階** 認定機関は、監査枠組みの要件に照らし合わせて候補組織が実施したプロセスを正式に評価します。この評価の結果により、認証書の発行が決定します。

A) 顔認証システムが稼働中で、認証取得を希望している組織、またはB) 顔認証システムの導入を予定している組織を例として、実施しなければならないステップと関連する流れを図2と図3に示しました。

## 4.1 顔認証システムが稼働しており、認証取得を希望する組織

図2 システムが稼働している場合の認証スキームの7ステップ



出典：世界経済フォーラム

－ **#1 既存のプロセスと慣行のレビュー** すべての申請者はまず顔認証システムの管理プロセスを徹底的にレビューし、次に既存のプロセスと慣行をガバナンス枠組みの要素（行動原則、ベストプラクティス、自己評価調査票または監査枠組み）に照らして評価する必要があります。これによって、アプローチを検証し、監査枠組みの要件を満たすことが可能か確認できます。

－ 実施する内容

- － 部門横断的なタスクフォースを設置
- － 既存のプロセスと慣行の一覧を作成し、それらがガバナンス枠組みの要素と一致しているかどうかを評価
- － 認証プロセスの一環として生成、収集、評価が必要なデータ・根拠の一覧を作成し、既存の文書やデータアーカイブに欠陥がないかを確認

－ プロセスと慣行、またはコンプライアンス実証のために使用されるデータと根拠において欠陥が発見された場合、タスクフォースは経営陣に報告

－ **#2必要な修正を実施するコミットメント** 経営陣は、認証プロセスの実施を内部で検証し、特定された欠陥に対処するために必要なリソースを割り当てます。

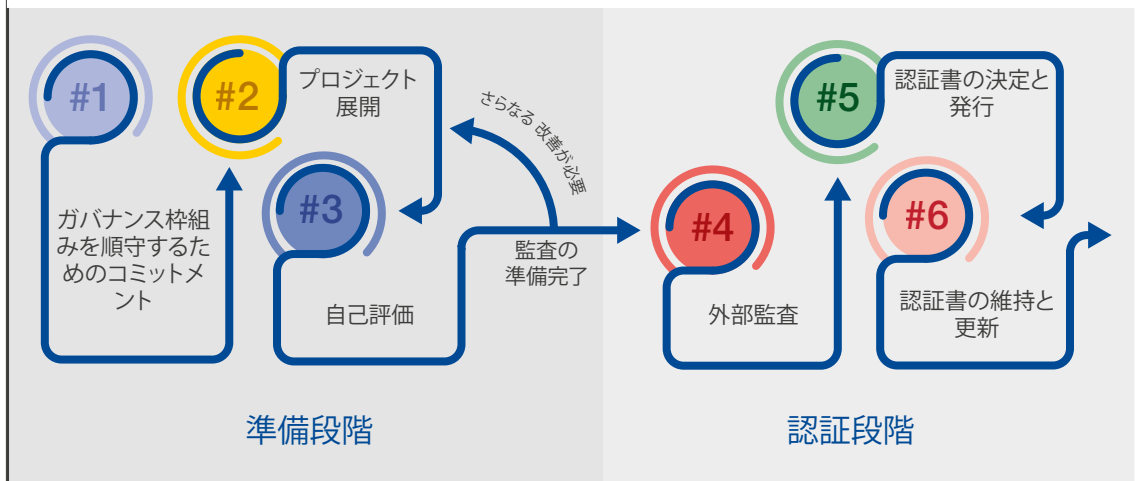
－ 実施する内容

- － 経営陣は、監査枠組みの要件に準拠させるために顔認証システムの修正を組織内で決定
- － 経営陣は組織内（取締役会常務、ユニット長、部門横断タスクフォースのメンバーなど）と組織外（国のデータ保護機関など）の双方について主要なステークホルダーを特定

- **#3 プロジェクト展開** 自己評価プロセスの準備に必要な修正を行います。
  - 実施する内容
    - ガバナンス枠組みをベースとして、既存のプロセスと慣行を修正
- **#4 自己評価** 欠陥を特定し修復したあとには、自己評価を実施し、認証プロセスのための準備がどの程度進んでいるかを測定します。この過程は、自己正当化を避けるために、問題が指摘されたプロセスや慣行の修正に関与していないチームが実施すべきです（自己評価の結果が更なる修正の引き金となる可能性があります）。実務では既存のプロセスと慣行を微調整するためにステップ2と3を複数回繰り返すこともあります。
  - 実施する内容
    - 自己評価または内部監査を実行する専門チームを任命
    - 自己評価調査票か監査枠組み、またはその双方を使用して自己評価を実施
    - コンプライアンスの証拠となるすべての根拠（データと文書）が最新であり、容易に検索可能となっていることを確認
    - 面接の対象となる従業員に対して、監査の一環で面接を受ける可能性があることを通知（監査の重要性と、監査の一環としての面接の重要性を認識）。
    - 自己評価を実施している他の組織（成田国際空港など）と自組織を比較してもよい（自己評価調査票の結果を公表し、顔認証技術の責任ある使用をどのように実現したかを掲示することを奨励）。
  - スケジュールの目安
    - 自己評価は1～2日を超えないようにし、外部監査の条件に従うようにします。潜在的な欠陥を分析し、是正措置を実施するのに要する時間は、自己評価の結果によって変わってきます。
  - **#5 外部監査** 外部監査は認証機関が実施します。外部監査は2つのステップで構成され、第1のステップでは、システムがどのように設計され、実装されたかのプロセスを監査枠組みの要件の観点から調査します。第2のステップでは、現場で実際に運用されているシステムを抜き打ちで監査することで、これらのプロセスの有効性を評価します。
    - 実施する内容
      - 書類審査（システムの設計と実施に関する文書のレビュー）を実施
- 現場活動の監査（関連する業務手順書、文書、データのレビュー）を実施
  - スケジュールの目安
    - 監査には2日が必要。スケジュールは顔認証技術サービスを利用するエンドユーザーの数次第で変わるため、プロジェクトによってはこれよりも長くなる場合がある。システムを運用している場所が複数存在する場合はサンプリング監査方法を実施。
- **#6 決定と認証書の発行** 認証機関は監査結果と監査人の勧告に基づいて決定を下します。すべての要件が満たされている場合は認証書を発行し、そうでない場合は追加の是正措置を要求します。是正措置の要求が行われた場合、申請組織には当該措置を実施する時間が与えられます。
  - 証明書の有効期間は3年間で、年1回のフォローアップ監査に基づいてレビューが行われます。
  - 実施する内容
    - 認証機関は監査報告書を作成し、決定を発表
    - 要件が満たされている場合は認証機関が認証書を発行
- **#7 認証書の維持と更新** 年一回の監査によって要件維持が認定されます。不適合があった場合は認証が取り消されます。
  - 実施する内容
    - 年次監査は以下で構成されます。
      - 書類審査（システム設計・実施に関する文書のレビュー）
      - 現場活動の監査（運用手順のレビュー）
  - スケジュールの目安
    - 維持監査（モニタリング）は1年に1日実施（期間は最初に適用されたサンプリング規則によって変わる）。
    - 3年の有効期間が終了すると、認証書更新のための監査が実施される。更新監査には2日を要する。スケジュールは顔認証技術サービスを利用するエンドユーザーの数次第で変わるため、プロジェクトによってはそれよりも長い時間がかかる場合がある。

## 4.2 顔認証システムの導入を予定している組織

図3 システム未稼働の場合の認証スキームの6ステップ



出典：世界経済フォーラム

### #1 ガバナンス枠組みを順守するためのコミットメント

1) 顔認証システムの設計で導入されたプロセスに関連する要件、2) システム稼働時に当該プロセスの実施に関わる要件、3) システムの機能に関わる要件、の3つが監査の焦点となります。顔認証システムの設計段階にある組織は、「責任を織り込んだ設計」でシステムを構築することができるため、すでに稼働中のシステムを管理している組織よりも有利になります。

#### - 実施する内容

- 顔認証管理システムの設計計画にガバナンス枠組みを使用
- 経営陣はガバナンス枠組みの要素に準拠した責任ある顔認証システムを設計し、実施することを確約（文書とデータを監査時にアクセスしやすい場所に作成・保管することを含む）。
- 経営陣は認証書を発行する権限を持った認証機関と連絡をとり、監査スケジュールを設定

### - #2 プロジェクト展開 自己評価のプロセスを作成します。

#### - 実施する内容

- 経営陣は、監査枠組みの要件に合った顔認証システムの構築を確約
- 経営陣は組織内（取締役会常務、ユニット長、部門横断タスクフォースのメンバーなど）と組織外（国のデータ保護機関など）の両方について主要なステークホルダーを特定
- 経営陣は、ガバナンス枠組みの要素と監査枠組みの要件を自己評価のための仕様書に記載

- #3 自己評価 さまざまなタスクフォースが指摘した欠陥への対応が完了した時点で、組織は自己評価を実施し認証プロセスについてどの程度準備ができているかを把握することができます。このプロセスは、自己正当化の危険を避けるため問題の分析に関与していないチームが担当すべきです（自己評価の結果によってはさらなる修正が必要になることもある）。該当するステークホルダーは既存のプロセスと慣行をそれに合わせて微調整する必要があります。

#### - 実施する内容

- 自己評価または監査を実行するための専用チームを任命（監査枠組み要件2.4）。
- 自己評価調査票または監査枠組みを使用して自己評価を実施
- 成田国際空港など自己評価を実施している他の組織と自組織を比較してもよい。

#### - スケジュールの目安

- 自己評価の期間は1～2日を超えないようにし、外部監査の条件に従うようにする。基準線からの潜在的な逸脱と是正措置実施の分析に要する時間は自己評価の結果によって変わる。

- #4 外部監査 外部監査は認証機関が実施します。外部監査は2つのステップで構成され、第1のステップでは、システムがどのように設計され、実装されたかのプロセスを監査枠組みの要件の観点から調査します。第2のステップでは、現場で実際に運用されているシステムを抜き打ちで監査することで、これらのプロセスの有効性を評価します。

#### - 実施する内容



<ul style="list-style-type: none"> <li>- 書類審査(システムの設計と実施に関する文書のレビュー)を実施</li> <li>- 現場活動の監査(業務手順書のレビュー)を実施</li> <li>- スケジュールの目安 <ul style="list-style-type: none"> <li>- 監査には2日を要する。スケジュールは顔認証技術サービスを利用するエンドユーザーの数次第で変わるため、プロジェクトによってはこれよりも長くなる場合がある。システムを運用している場所が複数存在する場合はサンプリング監査方法を実施</li> </ul> </li> </ul>	<p>が認証書を発行</p>
<ul style="list-style-type: none"> <li>- <b>#5 決定と認証書の発行</b> 認証機関は監査結果と監査人の勧告に基づいて決定を下します。すべての要件が満たされている場合は認証書を発行し、そうでない場合は追加の是正措置を要求します。是正措置の要求が行われた場合、申請組織には当該措置を実施する時間が与えられます。</li> <li>- 実施する内容 <ul style="list-style-type: none"> <li>- 認証機関は監査報告書を作成し、決定を発表</li> <li>- 要件が満たされている場合は認証機関</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>- <b>#6 認証書の維持と更新</b> 年一回の監査によって要件維持が認定されます。不適合があった場合は認証が取り消されます。</li> <li>- 実施する内容 <ul style="list-style-type: none"> <li>- 年次監査は以下で構成 <ul style="list-style-type: none"> <li>- 書類審査(システム設計・実施に関する文書のレビュー)</li> <li>- 現場活動の監査(運用手順のレビュー)</li> </ul> </li> </ul> </li> <li>- スケジュールの目安 <ul style="list-style-type: none"> <li>- 維持監査(モニタリング)は1年に1日実施(期間は最初に適用されたサンプリング規則によって変わる)。</li> <li>- 3年の有効期間が終了すると、認証書更新のための監査が実施される。更新監査には2日を要する。スケジュールは顔認証技術サービスを利用するエンドユーザーの数次第で変わるため、プロジェクトによってはそれよりも長い時間がかかる場合がある。</li> </ul> </li> </ul>

## 4.3 重大な不履行がもたらす結果

この認証スキームの導入は任意であり、軽微な不履行が指摘された場合には企業は必要な是正を行う期間として1ヶ月が与えられますが、重大な不履行が発見された場合には認証が取り消されます。これにより、企業は認証に関する情報提供を直ちに停止し、認証を失ったことを消費者に公表するよう要求されます。

認証が法制化されれば、重大な不履行は現在よりもはるかに重大な結果を伴う形で扱われることになるかもしれません。例えば、

- 指摘された問題が完全に解決するまで、法律で顔認証システムの即時停止を課すことができ、そ

の間認証も停止される(後に認証回復の可能性あり)。

- 指摘された問題に対処するため、一定期間は問題のある顔認証システムの使用を継続でき、期間内に問題が解消されれば認証の停止もないが、解消しない場合はシステムは停止され、認証書も取り消される。

法案には、顔認証システムの即時停止が求められる重大な不履行の種類と、解決後に業務再開するために企業が従わなければならないプロセスの両方が明記されている必要があります。

5

## 結論

フロー管理のユースケースに対する適切な  
規制手段となる認証スキーム



## ④ 顔認証システムの責任ある実装のための基準設計への道を開きうる方針策定パイロットプログラム

顔認証技術に関連した機会とリスクについての認知は世界中で広がっており、技術が社会にもたらす影響力が急速に増大する中、行動を起こすよう求める声が高まっています。米国とEUの一部の政策立案者はこうした要求に耳を傾け、確固としたガバナンス枠組みの整備が急務であることを認識していますが、今後の道筋についてはコンセンサスが得られていない状態です。

我々は、認証制度がフロー管理のユースケースに対する適切な法制的対応であると考えます。AFNOR Certificationのような認証機関に行動原則への適合性の評価を委託することは、フロー管理アプリケーションにおいて顔認証技術の信頼できる設計と使用を保証するためのアジャイルで堅牢な手段です。

本白書の手法に賛同する企業・団体は、顔認証システムを設計・改善する指針であるガバナンス枠組み（行動原則、ベストプラクティス、自己評価調査票、監査枠組み）を活用したレビューを行うことで、厳格なプロセスを踏むことができます。しかし、認証書の発行でこの行程が完了するわけではありません。信頼性を保つためには、評価のための努力を継続することが必要です。したがって、この「顔認証における責任ある制限」プロジェクトの主要パートナーが望むことは、認証を受けた組織がテクノロジーの利用者、顧客、社会全体の利益のために、変容し続けるリスクの特定と軽減に貢献する組織文化を、長期的に根付かせていくことです。

各国政府は、この文化を醸成していく上で、重要な役割を果たしています。パイロット事業が完了し、その成果が証明された暁には、政策立案者には、本白書の提案を考慮に入れた上で、フロー管理アプリケーションに顔認証技術を使用する業界関係者にこの認証を義務づける法律を通過させることが求められます。

このパイロット事業の次のステップは、業界関係者と共に監査枠組みと認証スキームを検証し、認証を受けるにあたり関係者に生じる作業量を評価し、それらをレビューすることです。これが成功すれば、顔認証システムの責任ある適用のための基準設計への道が開かれたことになります。パイロット事業完了後には、この認証モデルの順守と促進に取り組む関係者によるマルチステークホルダーの連合が形成されることになります。

業界関係者、公的機関、市民社会代表者、認証機関、政策立案者、学者など様々なステークホルダーがこの過程に参加して認証モデルを強化し、オープンで実験的なアプローチを通してそのインパクトを確実にすることが望まれます。

ユースケースを用いたこのプロジェクトのアプローチは、他のアプリケーションで顔認証技術を責任ある形で使おうとしているステークホルダーの参考となる可能性があります。本白書の手法を他のユースケースに展開することを検討している組織は、世界経済フォーラム第四次産業革命センターにご連絡下さい。



# 用語集

**顔認証の精度** 顔認証システムの精度は、2つの条件の組み合わせに基づいています。1) システムに登録されている人間がシステムに正しく識別される頻度、2) 登録されていない人間が不一致であると正しく検出される頻度。これら2つの条件は「真」の条件と呼ばれ、2つの「偽」の条件を組み合わせると顔認証システムのすべての可能な結果を記述します（真陽性、真陰性、偽陽性、偽陰性の定義を参照のこと）。

**アルゴリズム** アルゴリズムとは、特にコンピューターで計算を実行したり、問題を解決したりするための一連の命令のことです。アルゴリズムはコンピューターが実行可能なすべてのことの基盤を形成していることから、あらゆるAI（人工知能）システムの基本的な側面です。

**監査** 監査枠組みの基本的な機能は、定義された範囲の監査の要件とプロセスを詳述した参考文献として機能することです。

**バイオメトリクス（生体認証）** バイオメトリクスの対象は指紋、虹彩模様、手形、顔テンプレート、声紋、歩行パターン、署名など（ただしこれらに限定されません）、人の固有の識別可能な属性を識別および認証のために使用するさまざまなテクノロジーです。

**認証** 認証スキームの基本的な機能は、監査枠組みに記載された一連の定義要件に基づいて、特定のシステムまたは製品について客観的な判断に到達するための独立した評価を実施することです。

**コンピュータービジョン** コンピュータービジョンは、人間が行うのと同様の方法でコンピューターが画像を見て識別、処理することを可能にし、適切な出力を行うことを目的としたコンピューターサイエンスの一分野です。

**エンロールメント（登録）** エンロールメントはテンプレート作成のために個人の画像をエンロール（登録）し、個人を認識できるようにするプロセスです。証明に使用される認証システムに個人が登録されると、その人のテンプレートには、プローブテンプレートと比較するテンプレートを決定するために使用されるプライマリ識別子も関連付けられます。

**説明可能性** 説明可能性は、一定の形式で結論に到達する方法を説明して、意思決定についての理解を向上させてシステムのオペレーターやユーザーの信頼を高めることができるAI（人工知能）システムの特徴です。

**顔検出** 検出では人間の顔を見つけたときに、「この画像に1つ以上人間の顔があるか」という質問に答えを出します。

**顔識別（または1対多）** 顔識別は「この未知の人物を登録済みのテンプレートと照合できるか」という質問に答えを出します。識別では、プローブテンプレートをリポジトリに保存されているすべての登録テンプレートと比較するため、1対多マッチングとも呼ばれます。マッチング候補は、プローブテンプレートが登録されている各テンプレートとの一致度に基づいて返されます。

**顔検証（または1対1）** 顔検証は「これらの2枚の画像は同一人物か」という質問に答えるものです。セキュリティやアクセスの状況において検証はプライマリ識別子（顧客IDなど）の存在を頼りにしており、顔認証はその人の識別情報を確認するための第二の要素として使用されます。検証は、プローブテンプレート（1人の人間）は、提示された識別情報に関連付けられた（1人の）人物用に保存されたテンプレートとのみ比較されるため、「1対1」マッチングとも呼ばれます。

**顔認証** 顔認証は、顔の輪郭に基づいてパターンを比較・分析することにより、人物を固有に識別または検証できるバイオメトリクス・ソフトウェア・アプリケーションです。

**偽陰性** 偽陰性とは、探査画像に写っている人物が登録されておらず、登録されていても一致しないと誤って表示するテスト結果のことです。偽陰性の結果は、顔認証のユースケースによって大きく異なってきます。

**偽陽性** 偽陽性とは、探査写真に写っている人物がシステムに登録されていないにもかかわらず、システムに登録されていると誤って表示されるテスト結果のことです。偽陽性の結果は、顔認証のユースケースによって大きく異なってきます。

**プローブ画像** プローブ画像は顔認証システムに送信され、登録された個人と比較するための画像のことです。プローブ画像はプローブテンプレートにも変換されます。登録テンプレートと同様に、画像が高品質であるとテンプレートも高品質になります。

**テンプレート** 人物の画像はテンプレートに変換された後に顔認証に使用されます。1枚または複数の個人の画像から機械で解釈可能な特徴が抽出され、それをもとにその人のテンプレートが作成されます。

**真陰性** 真陰性の場合、探査画像の人物は登録されていないため、一致しません。

**真陽性** 真陽性の場合、探査画像の人物は登録されているため、正しく一致します。

# 寄稿者

## 主な執筆者

秋元一郎、日本電気株式会社シニアマネージャー(グローバルAI事業開発)、世界経済フォーラムコーポレートフェロー

井上裕介、世界経済フォーラム第四次産業革命日本センター、日本政府フェロー

セバスチャン・ルラドゥール、世界経済フォーラムLLC、フランス政府フェロー

ロフレッド・マッドゾウ、世界経済フォーラムLLC、AIと機械学習プロジェクトリーダー

ジェレミー・メジャ氏、フランスAFNOR Certificationプロジェクトマネージャー

## プロジェクトコミュニティ

世界経済フォーラムは、プロジェクトコミュニティのメンバーの洞察に満ちたレビューとフィードバックに感謝します。

ディディエ・バイシェール氏、フランス国会議員

ザビエル・ブロンドー氏、フランス国有鉄道 (SNCF)、ビデオ保護担当部長

ビンセント・ブートー氏、フランスIDEMIA、イノベーションラボ・ディレクター

パスカル・ブリアン氏、フランスADPグループ旅客体験部門IT部長

ローラン・ダーマニ氏、フランスAFNOR Certification副部長

ジャン・リュック・デュージュレ氏、フランスEURECOM デジタルセキュリティ/画像セキュリティ担当教授

マリーヌ・デュノギエ氏、米国Alcatraz組み込みシステム担当ディレクター

ロザンナ・ファニ氏、ベルギー、AI倫理研究者

ルイ・トーマス・フェルナンデス氏、フランス国有鉄道 (SNCF) LAF専門家

ロマン・ガレスヌ＝フォンテーヌ氏、フランスINGグループ、コミュニケーション・制度関係ディレクター

エルベ・ジャンティ氏、フランス国有鉄道 (SNCF) データ販売安全責任者

ブライス・ギルバート氏、フランスAFNOR Certificationサイバーセキュリティ担当プロジェクトマネージャー

イラナ・ゴルビン氏、米国PwC、新興技術・責任あるAI担当ディレクター

ブルース・エディン氏、米国H5主席研究員

マティッサ・ホリスター氏、カナダ・マギル大学組織行動学助教授、世界経済フォーラム学術研究員

リュック・ジュリア氏、韓国サムスン上級副社長・電子最高技術責任者、サムスン戦略・イノベーションセンター

エヴァ・カイリ氏、欧州連合、欧州議会議員

北川 高之氏、成田国際空港株式会社 経営計画部 戦略企画室 アシスタントマネージャー

ブレンダ・レオン氏、米国プライバシーの未来フォーラムシニアカウンセル兼AI (人工知能) 倫理担当ディレクター

ゴートイエ・マルタン氏、フランスADPグループ、空港サービス・製品開発プロジェクト部長

松本 英久氏、成田国際空港株式会社 経営計画部 戦略企画室 マネージャー

フランク・モーラン氏、フランスIDEMIA、旅客円滑化・国境管理担当製品・ソリューション担当ディレクター

セドリック・マジエール氏、フランス国有鉄道 (SNCF) ビデオ保護部長

ミカエル・メシュレ氏、フランス国有鉄道 (SNCF) LAFディレクター

ショーン・ムーア氏、米国Trueface社最高経営責任者兼共同創設者

アーナンド・ラオ氏、米国PwC、AI (人工知能) 部門グローバルリーダー

アーサー・リベモン氏、フランスAFNOR Certification、プライバシープロジェクト部長

マシュー・ロンデル氏、フランスADPグループ空港オペレーション部門、専門知識・運行担当ディレクター

ステファン・セジュールネ氏、欧州議会議員

カレン・シルバーマン氏、米国カンテラス・グループ創業者兼最高経営責任者

エミリア・タンタル氏、ルクセンブルグ・ブラック・スワン LUX、データ・AI (人工知能) 担当チーフオフィサー

イザベル・バルベルデ氏、フランス国有鉄道 (SNCF)、フローオペレーション主任

フィリップ・ワイス氏、フランス国有鉄道 (SNCF) 顔認

証プロジェクト主任

山根 知洋氏、国土交通省 航空局 総務課 政策企画調査室 航空イノベーション推進官

## 独立オブザーバー

また、独立したオブザーバーとしての役割を果たしてくださったフランスデータ保護機関 (CNIL)、特に以下の方々にも感謝します。

マリー・デュボイ・フレズニー氏、法律顧問

フェリシエン・ヴァレ氏、プライバシー専門科学技術者



# 付属文書

## 付属文書A:成田国際空港の自己評価調査票回答例

### 1.顔認証システムの適切な利用

評価に関する質問	成田国際空港による自己評価調査票回答
貴社の顔認証システムの代替案はありますか。そちらを導入しなかったのはなぜでしょうか。これらの代替案の長所と短所を判断するための基準は何ですか。	指紋認識と虹彩認識を代替案として検討しました。比較の結果、以下の点で顔認証の方が優れていると判断しました。  1. 乗客が機器を操作する必要がないため便利  2. 非接触形式で利用できるため新型コロナウイルス感染拡大時に有用だった  3. 誰も持っていない独自の情報を特別な操作なしに収集できる  4. ウォーキングペースというコンセプトが実現できる
貴社システムの目的に対する妥当性をどのように評価しましたか。	以下の3点で評価しました。  1. 高い顔認証精度  2. エンドユーザー（航空会社）の要件を高いレベルで満たせる  3. ウォーキングペース実現に向けた処理性能
貴社システムの目的に対処するための技術的な要件を、該当する機関が理解できる形式で記述してください。	主なポイントは以下のとおりです。  1. 高い顔認証精度  2. ウォーキングペース程度の速さ  3. 既存の航空会社のシステムとの互換性（大規模な修正が必要ない）  4. IATA規格への準拠
偽陽性・偽陰性の状況（特に公民権侵害のリスク）についてリスク分析を行いましたか。	第三者委員会（弁護士、大学教授、消費者団体を含むMLITの個人情報保護委員会）と共に、搭乗間違いのリスクなどを分析しました。

### 2. リスク評価

評価に関する質問	成田国際空港による自己評価調査票回答
以下の側面について、システム使用前（リスク評価の枠組みなど）およびシステム稼働中（監査枠組みなど）に厳密な評価を行いましたか。	
プライバシー	このリスクは第三者委員会（弁護士、大学教授、消費者団体を含むMLITの個人情報保護委員会）によって評価しました。
エラー	システムのユーザー（航空会社など）とシステムのオーナー（成田国際空港）がエラーの原因を判定できるようにするため、システムエラーの監視・検出機能を実装しました。
不当なバイアス	このリスクは第三者委員会（弁護士、大学教授、消費者団体を含むMLITの個人情報保護委員会）によって評価しました。
ハッキングとサイバー攻撃	第三者によるシステム評価であるセキュリティ・バイ・デザインを実施し、侵入テストなどを実施しました。

意思決定プロセスの透明性	承認処理は契約書に基づいて承認機関が行いました。またシステムのユーザー（航空会社など）とのシステム仕様調整ミーティングを開催し、仕様を決定しました。
人権・公民権の侵害	このリスクは第三者委員会（弁護士、大学教授、消費者団体を含むMLITの個人情報保護委員会）によって評価しました。

### 3. バイアスと差別

評価に関する質問	成田国際空港による自己評価調査票回答
<p>不当なバイアスは貴社のユースケースではどのように定義されていますか。</p> <p>それぞれの定義の評価に使用されている指標を説明してください。</p> <p>貴社のリスク分析の枠組みはどうなっていますか。貴社のユースケースにおいて特定された不当なバイアスのリスク、そしてバイアスの評価を行ったエンドユーザーの特徴で記述されたグループについて説明してください。</p> <p>このプロセスでは、リスクはどのように優先順位付けされていますか。競合する利害関係はどのように解決していますか。</p> <p>このケースで適用された不当なバイアスの検出、特定、緩和のための既存のベストプラクティスについて説明してください。</p> <p>特定された主なリスクを軽減するためにどのような行動計画を立てましたか。不当なバイアスのそれぞれのリスクについて、どのような緩和策が特定され、有効性を確保するためにどのように緩和策を評価しましたか。</p> <p>貴社の顔認証システムで使用しているテストケースや受入テストはどのようなものですか。</p> <p>貴社のトレーニングセットの分布はどのようなもので、貴社のシステムのエンドユーザーの分布とどの程度一致していますか。</p> <p>欠陥がある場合はその影響をどのように評価し、是正しましたか。</p> <p>貴社のシステムを導入する際にどのようなトレードオフに直面していますか。それにどのように対処していますか。</p> <p>リリース基準と実際の性能との間に乖離があった場合、乖離をどのように埋めましたか。</p>	<p>パスポートに組み込まれた集積回路(IC)に顔情報が含まれており、他の空港でも採用されていることから、顔認証システムを採用しました。不当なバイアスとは、さまざまな人種の人々、そして車椅子利用者などの障害者に対する性能(指標:精度や認証時間)の差であると定義しました。ただしパスポートにICが組み込まれていない人や、国独自の理由でサポートを受けられない人は対象外としました。</p> <p>システム全体のリスク分析の枠組みとしてISO 31000に基づくJIS Q 31000を使用しました。不当なバイアスの評価については、顔認証システムの検証項目としてNIST等によるパブリックレビューの結果をベンダーに提出させています。</p> <p>システム全体の可用性とセキュリティを最優先としています。システム全体への影響を踏まえて個別機能のレビューを行っています。</p> <p>NISTIR 8280で顔認証ベンダーをレビューし、選択を行った時点で最も優れたアルゴリズムを持つベンダーを選択しました。</p> <p>不当なバイアスの評価については、顔認証システムの検証項目としてNIST等によるパブリックレビューの結果をベンダーに提出させています。選択時点ではNECのシステムが最も精度が高かったことから、そちらを運用と組み合わせることを決定しました。</p> <p>システムとしての受入テスト(局所光環境を考慮した運用試験を含む)をユースケースの観点から実施しました。顔認証システム自体の検証項目として、NIST等のパブリックレビューの結果をベンダーに提出させました。</p> <p>エンドユーザーである航空会社と共にユースケースを設計し、トレーニングシナリオのテスト(システム受入)と作成を行いました。</p> <p>顔認証システム自体の検証項目として、NIST等のパブリックレビューの結果をベンダーに提出させました。</p> <p>個人情報の保護とユーザビリティなどのトレードオフに直面しています。個人情報の保護は、マルチステークホルダーのプロセスで管理されています。</p> <p>太陽光線による顔認証の精度低下を抑えるために、遮光フィルムやカーテンなどの物理的な対策を追加し、顔認証パラメータなどのソフトウェアを調整して要件に従うように対応しました。</p>

## 4. プライバシー保護設計

評価に関する質問	成田国際空港による自己評価調査票回答
データ主体のプライバシーをサポートするために、例えば使用目的に関連する生体認証データの過剰収集を回避するためにどのようなプロセス(タスクフォースなど)やリソース(ベストプラクティス憲章など)を実施しましたか。	会社の個人情報保護室や顧問弁護士と連携し、法的な課題を洗い出して解決の方向性を整理し、航空局や個人情報保護委員会との協議を行いました。  航空局はその後に専門家会議(第三者委員会)を設置し、個人情報保護の観点からマルチステークホルダーのプロセスを導入してプロセスを評価しています。  One IDプログラムの国内展開を前提としたガイドブックを作成しました。
データ保護責任者の役職を設けていますか。	個人情報保護体制については、このプロジェクト開始前に社内規定を整備しており、それに基づいて責任者を配置しています。
高いレベルのデータ保護を実現するため、顔認証システムの製品開発段階でプロダクトマネージャー、法務チーム、UXデザイナー、データサイエンティスト、開発者などの間でどのように緊密な連携を推進していますか。	第三者によるシステム評価であるセキュリティ・バイ・デザインを実施し、侵入テストなどを実施しました。

## 5. 性能

評価に関する質問	成田国際空港による自己評価調査票回答
ラボテストとフィールドテストにおいて貴社のシステムの精度と性能を評価するために、どの既存の規格(例: 国際標準化機構 (ISO)、AFNOR Certification、欧州標準化委員会 (CEN))に従っていますか。貴社が準拠している規格や規範を選択する際にはどのような基準を使用しましたか。	顔認証システムだけでも、ISO/IEC JTC 1/SC 37のバイオメトリクス規格に準拠したNEC製品の最新版を使用しています。
顔認証システムを国立標準技術研究所 (NIST) に提出して評価を受けていますか。	NIST評価 (IR 8271) を参考として使用しています。
顔認証システムの性能結果の監査可能性を確保するために、どのようなプロセスを確立していますか。第三者による十分な監査を可能にするために、どのような手順を取っていますか。	ウォーキングペースという性能要件に基づき、システム試験(機能試験、非機能試験: 可用性、信頼性、性能、生体認証試験)を実施し、検証しました。
検討されたユースケースについて実施された性能試験の妥当性はどのようになっていますか。	妥当性  従来の15分かかる乗客250人搭乗3レーンよりも高い処理能力が求められる搭乗口での実装試験を実施  現行の運用と比較した地上スタッフの削減と省力化の検証
理論的な偽陽性率と偽陰性率の測定値に至る選択された性能の閾値はどのように正当化していますか。	法務省出入国在留管理庁が要求する顔認証ゲートの仕様に準拠しています。



## 6. 情報に対する権利

評価に関する質問	成田国際空港による自己評価調査票回答
エンドユーザーに貴社のシステムの利用と生体認証データの利用について情報を提供するために、どのようなプロセスが実施されていますか。またシステムによる被害が発生したと考えられる場合は、上訴や救済の手段を含め、どのようなプロセスが実施されていますか。ベストプラクティスにはカスタマーサポートや問い合わせへの対応が含まれますが、これに限定されません。	国土交通省の「空港での顔認証技術を活用したOne IDサービスにおける個人データの取り扱いに関するガイドブック」に従って利用者に情報を提示しています。 <ul style="list-style-type: none"> <li>メールアドレス: 同上</li> <li>電話番号: 同上</li> <li>カスタマーサポートFAQ: 同上</li> <li>カスタマーサポートのチャットボット: 予定なし</li> </ul>
データ対象者は、妥当な期間内(例: 30日以内)に機械読み取り可能な形式で個人データ(写真、動画や、アカウントイベント履歴、同意履歴、生体認証データ削除履歴、共有情報、生体認証データの使用履歴など個人のIDにリンクされた生体認証データ)にアクセスしたり、取得したり、削除を依頼したりすることができますか。	データは24時間以内に削除されます。
専門家以外の人でも理解できる形式でシステムの設計と使用の指針となるガバナンス原則を確立し、(ウェブサイトなどで)公開していますか。	ウェブサイトやチラシなどで公開する予定です。
個人がシステムの機能に関する関連情報に匿名でアクセスできるようにするプロセスが確立されていますか。	いいえ。

## 7. 同意

評価に関する質問	成田国際空港による自己評価調査票回答
同意ポリシーでは明白で明確な情報がユーザーに提供されていますか。具体的に以下はどうなっていますか。	登録時のディスプレイに明記されています。情報はウェブサイト上やターミナルビル内に貼られたポスターでも見ることができます。
同意ページは最大2回クリックするだけでアクセスでき、「プロフィール」ページでも見やすく表示されていますか。	ワンクリックでアクセスできます。このページを下にスクロールすると規則が表示されます。手続きが完了する前に操作を中止してもトークンは生成されません。 プロフィールページは表示されていません。
主な規定の概要は同じページに記載されていますか。	はい。
この概要には以下の情報が含まれていますか。	
すべての想定された目的の説明	はい。
データ保持期間	はい。
データ共有ポリシー(データを共有する第三者の明記を含む)	はい。

評価に関する質問	成田国際空港による自己評価調査票回答
データを保護し、安全に保管するための手段	はい。
この概要は専門家でない人にもわかりやすく簡潔で、長さはA4サイズで2ページ以内ですか。	はい。
同意を与えるか与えないかを記載するページでは、既存の目的ごとに表示できるようになっていますか。	ユーザーがすべてに同意しない限り、トークンは生成されません。
これらのオプションはすべて同じページに表示されていますか。	はい。
既存の目的一覧は最新のものとなっていますか。	最新です。

## 8. 情報の表示

評価に関する質問	成田国際空港による自己評価調査票回答
顔認証システムが使用されているエリアに入ったことを個人に知らせるために、どのような手段が導入されていますか。これらの手段は誰にでも目に見える形で明確になっていますか。ユーザーの権利に関するリマインダーは表示されていますか。	顔認証エリアと一般エリアとは、顔認証を示す特殊なロゴマークなどを用いて明確に区別されています。  国土交通省の「空港での顔認証技術を活用したOne IDサービスにおける個人データの取り扱いに関するガイドブック」に従い、空港ではポスターやパネルなどを使用して情報を利用者に提示しています。
施設へのアクセス、フロー管理や公共スペースへの登録の場合、記録ゾーンの情報量が、ユーザーによって定義および識別されたキャプチャスペースを超えることはありませんか。キャプチャスペースがエンドユーザーに理解されていることをどのようにして確認していますか(評価・調査・テストに基づいた根拠を提示してください)。	展開時に顔認証システムを検証し、キャプチャスペースを超えないようにしています。
顔認証システムの目的を伝えるのに十分な大きさのディスプレイが使用されていますか。ディスプレイの視認性と読みやすさはどのようにして確保していますか(評価・調査・テストに基づいた根拠を提示してください)。	顔認証用の特別なロゴと配色を使用することで、ディスプレイの大きさに関係なく視認性を高め、認識しやすいようにしています。

## 9. 弱者グループに対するアクセス権

評価に関する質問	成田国際空港による自己評価調査票回答
高齢者や障害者(視覚・聴覚障害者を含む)を支援するためのシステムの設計と評価について詳しく教えてください。	国土交通省の「空港での顔認証技術を活用したOne IDサービスにおける個人データの取り扱いに関するガイドブック」に従い、空港ではポスターやパネルなどを使用して情報を利用者に提示しています。
顔認証システムは、高齢者や障害者など、誰でも利用できるものになっていますか。	利用できます。  ただし、カメラで画像を撮影できるようにするため、被写体は130cmから190cmの高さに設定されています。

高齢者や障害者を支援するためにどのようなリソースを割り当てていますか。	各タッチポイントにスタッフ（空港と航空会社のスタッフ）を配置しました。
障害者、子供、家族などシステムが機能しない、またはシステムの利用が望ましくない人のための緩和策は、機能することがテストで証明された代替案を使用することであると考えられます。	代替案として、スタッフ（空港と航空会社のスタッフ）による手作業の操作が行われています。

## 10. 代替の選択肢と人間の常駐

評価に関する質問	成田国際空港による自己評価調査票回答
顔と写真付きの身分証明書を照合した結果、特に登録段階で偽陰性が生じた場合、人間によるレビュープロセスを導入していますか。	人間によるレビュープロセスはありません。  搭乗者情報やパスポート情報などの確認のために航空会社のホストに情報を参照するクラウドサービスを追加することで、全自動化と誤検知の排除を実現しています。  エラーが発生した場合には、現在の操作と同様の処理が手作業で行われます。
顔認証システムでは、代替オプションは体系的に実装されており、人間によって操作されていますか（そのような操作スタッフは例外的な状況に対処する訓練を受けていますか）	実施しています。現在、手動操作はスタッフが代わりに行っています。  現在、手動操作はスタッフが代わりに行っています。
合理的ですか。つまり不相応に不利な結果をもたらすことはありませんか（保安検査場の通過時間が2倍になるなど）。	既存のシステムと同等のシステムとして使用でき、以前と同じ処理時間で処理可能です。
バイオメトリクスの利用を拒否する人のための代替プロセスはありますか。	既存のシステムと同等のシステムとして使用できます。代替プロセスとして手動操作が用意されています。



# 付属文書B:監査枠組み

## 1. 顔認証システムの適切な利用

### 要件

顔認証システムは使用目的に応じて高度にカスタマイズするべきです。顔認証システムを使用する組織は、使用するシステムの能力と限界を評価し、そのシステムが目的に適したものであることを確認するために妥当な措置を講じるべきです。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
1.1	顔認証プロジェクトに先立ち、顔認証システムの利用を検討するに至った必要性を定義する必要があります。  企業はシステムに与えられた目的を達成するための技術的要件を説明し、システムが意図した目的にのみ使用されることを確認できるようにしなければなりません。	✓		
1.2	同一のニーズを満たす一連の代替案(顔認証以外)を決定する必要があります。	✓		
1.3	ニーズを満たすためには、顔認証システムの使用に代わる可能性のある選択肢を特定する必要があります。  考えられる解決策を分析するための文書化されたプロセスと方法論を設定する必要があります。  その目的は、顔認証技術の利用目的との関連性を評価し、問題の解決を図ることにあります。  そのために企業は評価と選定の方法を詳細に記述しなければならず、これには少なくとも以下が含まれていなければなりません。 <ul style="list-style-type: none"><li>- 特定されたあらゆる解決策について、特定された長所と短所のレビュー</li><li>- 様々なステークホルダー(利用者、国家、市民など)にとってのシステムの利点の定義</li><li>- 偽陽性および偽陰性の状況を対象としたリスク分析(特に公民権侵害のリスク)</li><li>- 期待される便益の定量的評価</li><li>- さまざまな解決案の比較分析</li><li>- 顔認証解決案の選択につながった結論</li></ul>	✓		
1.4	認識技術の選択に至った前提条件を検証するために、企業はその使用の関連性を検証する際に留意するパラメータを定義する必要があります(予想偽陽性率および偽陰性率、業績予想など)。	✓		
1.5	これらのパラメータは使用段階で確認する必要があります。		✓	
1.6	顔認証システムは、特定の用途の枠組みの中で特定のニーズを満たすために導入されました。顔認証システムを使用する場合は当初計画された用途に限定し、それらの用途に対して検証を行う必要があります。			✓

## 2. リスク評価

### 要件

顔認証プラットフォームを作成する組織やサービスやシステムの一部として顔認証を使用する組織は、プライバシーへの影響、エラーの可能性、不当なバイアスの対象となる可能性、ハッキングやサイバー攻撃に対する脆弱性、意思決定プロセスの透明性の欠如、公民権や人権侵害の可能性などを含む、システムの総合的なリスク評価を行うべきです。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
2.1	<p>顔認証システムの完全なリスクアセスメントを実施する必要があります。分析では以下の項目を考慮しなければなりませんプライバシーに与える影響</p> <ul style="list-style-type: none"> <li>エラーの可能性</li> <li>バイアスの対象となる可能性</li> <li>サイバー攻撃（ハッキングやランサムウェアなど）に対する脆弱性</li> <li>文書化された意思決定プロセスにおける透明性の欠如</li> <li>公民権侵害の可能性</li> </ul> <p>また分析では、リスクを軽減するために実装された解決策をランク付けする必要があります。</p> <p>（付属文書に記載されたリスク評価を実施するためのツールの例を参照してください。）</p>			
2.2	<p>リスク分析にはリスク対策の実装を含める必要があります。</p> <p>また分析では、リスクとリスク軽減のために実施された解決策をランク付けする必要があります。</p>			
2.3	<p>リスク分析と対策で生じた行動を実施し、維持する必要があります。</p> <p>有効性を評価し、運用状態での維持管理を行うための指標を設定する必要があります。</p>			
2.4	<p>顔認証技術ユーザーは行動原則に沿ってプロジェクトを展開していることを確認した上で、システムを構築する必要があります。</p> <p>そのためには、次のいずれかの行動を実行する必要があります。</p> <ul style="list-style-type: none"> <li>自己評価調査票に基づいた自己評価</li> <li>この基準に基づいた内部監査</li> </ul> <p>結果として得られる結論と成果物は、アクセス可能とする必要があります。特に勧告を含めることによってシステムの展開が検証されます。</p> <p>使用されている方法に第三者監査人がアクセスできるようにしなければなりません。</p> <p>行動の原則が順守されていることを確認するためには、このアプローチはシステムの稼働中にも適用する必要があります。</p>			

### 3. バイアスと差別

#### 要件

顔認証システムを使用する組織は、すべての不当なバイアスや結果を可能な限り検出し、特定し、軽減できるようにするために、適切な措置を講じるべきです。組織は、バイアスを完全に除去することがAI（人工知能）研究における最大の課題の一つであることを認め、バイアスや不当な結果を最小化するツールやプロセスの実施に適切なリソースを割り当てなければなりません。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
3.1	顔認証利用の範囲におけるバイアスの定義を提示する必要があります。特に、さまざまなバイアスのレビューを行う必要があります。	✓		
3.2	バイアスの検出、特定、緩和のためにユースケースにおいて適用されたベストプラクティスを提示する必要があります。	✓		
3.3	<p>サプライヤー向けの仕様を設定する必要があります。</p> <p>仕様はすべてのリスク（バイアスを含む）または不公正な結果を可能な限り検出、特定、軽減できることを保証するための適切な措置を講じるため、文書化されたリスク評価に基づいて作成する必要があります。</p> <p>評価には、最低でも付属文書に記載された以下の項目が含まれている必要があります。</p> <ul style="list-style-type: none"><li>ユースケースにおいて特定されたバイアスのリスクと、これらのバイアスリスクの対象となる可能性のあるエンドユーザーグループの特徴の説明</li><li>バイアスのリスクがあるために特別な注意が必要とされるグループを優先的にグループ化したシステムのエンドユーザー特性の定義（例えば、年齢層、性別、民族性などの考慮）</li><li>サングラス、帽子、あごひげ、マスクなどアルゴリズムに影響を与える可能性のあるアクセサリと要素の考慮。仕様ではこれらの状況も考慮に入れる必要がある。</li><li>使用プロセスのさまざまな段階で特定されたバイアスを評価するためのパラメータの実装。これらのパラメータによって特にバイアスのリスクをランク付けすることが可能となる</li><li>利用プロセスの各ステップの分析（画像キャプチャに基づくバイアスやモデル性能に基づくバイアスの観察など）によってバイアスに関連するリスクを特定し、評価する</li><li>バイアスリスクのランク付けとさまざまな利害関係の処理</li></ul>	✓		
3.4	システムの利用によるリスクに関しては、特定されたリスクの軽減方法が定義および文書化できるようになっている必要があります。テクノロジー利用の際に差別につながる可能性のある結果が検出され、可能な限り最善の方法で軽減されることを保証するプロセスとリソースが必要です（付属文書記載の例を参照）。	✓	✓	



要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
3.5	<p>バイアスを軽減するための顔認証システムの性能評価を、使用するパラメータと測定システムの詳細と合わせて、識別された差別のリスクごとに決定する必要があります（付属文書B4記載のモデルを参照）。戦略の有効性を評価および検証するには指標の実装が必要となります。</p> <p>指標への準拠を検証するためには、これらの評価は設計段階およびシステム運用中に実行する必要があります。</p>			
3.6	<p>目標との比較でバイアスのずれが確認された場合には、システム運用中に是正措置および緩和措置を実施する必要があります。</p>			
3.7	<p>アルゴリズム検証のためには受入文書の作成と併せて生体認証システムのテストを実施する必要があります。</p>			
3.8	<p>トレーニングデータの分布を決定し、システム利用者のものと類似する項目と相違する項目を測定する必要があります。差異がある場合は、影響を評価して軽減する必要があります。</p>			
3.9	<p>顧客・利用者にとってのトレードオフ（例えば、テクノロジーによって発生する長所と短所のトレードオフ）を特定し、記述する必要があります。利害の相違が明らかになったときに仲裁解決のプロセスを設定する必要があります。</p>			
3.10	<p>利用者への影響を軽減するため、システム利用中に差別につながる可能性のある状況が検出および軽減されることを保証するためのプロセスとリソース（3.4 参照）を可能な限り最善の方法で実施する必要があります。</p> <p>システムの利用に伴うリスクについては、リスク軽減対策を実施する必要があります。</p>			
3.11	<p>システムが配備でき、使用可能な状態にあると判断するための基準（システムの性能や差別に関わる状況など）を定義する必要があります。</p> <p>使用段階ではこれらの基準への準拠を保証する必要があります。</p>			

## 4. プライバシー保護を支援する設計

### 要件

顔認証システムを利用する組織は、システム要件におけるプライバシーへの配慮やテクノロジーの設計・開発・テスト、業務支援や継続的なシステム保守におけるプライバシー保護支援の実施などによってプライバシーを支援するシステムを設計する必要があります。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
4.1	企業は個人情報の保護に適用される基準や規則を順守する必要があります。		✓	
4.2	生体認証データの機密性を確保するために、文書化されたプロセスとリソースを設定する必要があります。  このプロセスは、システム利用中は展開および維持されている必要があります。	✓	✓	
4.3	高レベルのデータ保護を実施するには、当然のこととしてプライバシーを順守する顔認証製品チーム（プロダクトマネージャー、法務チーム、UXデザイナー、データサイエンティスト、開発者を含む）のトレーニングを実施する必要があります。	✓		

## 5. 性能

### 要件

顔認証プラットフォームを作成する組織やサービスやシステムの一部として顔認証を使用する組織は、設計（ラボテスト）と展開（フィールドテスト）の段階においてシステムの精度と性能を評価するための基準に従うべきです。性能評価は有能な第三者機関によって監査可能なものとし、報告書はシステムのユーザーが利用できるようにすべきです。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
5.1	このテクノロジーのユーザーは、特定のデータベースまたはAPIにアクセス可能なデータベースを構築するには、エンドユーザーの母集団を構成する各サブグループの十分に均等なサンプルが含まれていることをサプライヤーから保証してもらい、それに応じてデータを収集する必要があります。これを行うため、エンドユーザーの特徴がサプライヤーに提供されます。  - サプライヤーは、評価方法の選択に至った基準と、ソフトウェアを選択するために使用された基準を決定する必要があります。  これらの項目はシステムを選択するための仕様の一部となっています。	✓		
5.2	このテクノロジーのサプライヤーは、ユーザーの仕様書で要求された性能閾値の期待値を検証可能とする要素を提供する必要があります。	✓		
5.3	システム運用において、選択された性能閾値（理論的な偽陽性率と測定された偽陰性率を含む）が順守されていることを示し、検証することが可能でなければなりません。		✓	✓

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
5.4	運用評価と報告書は監査可能でなければならず、独立した第三者が相談できるものでなければなりません。		✓	
5.5	性能評価を監査できるようにするためのプロセスを実施する必要があります。監査人がこれらの結果を十分に監査できるようにするためのステップを取る必要があります。	✓	✓	

## 6. 情報に対する権利

### 要件

顔認証システムの使用に関する質問がある、または情報を必要とするエンドユーザーに情報を提供するためのプロセスを整備すべきです。エンドユーザーが希望する場合は自分の生体認証データにアクセスできるようにすべきです。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
6.1	システムの使用と生体認証データの使用をエンドユーザーに通知するための文書化されたプロセスを実装する必要があります。  このプロセスにおいては、システムの使用法の変更を含めてユーザーに通知できるようになっている必要があります。	✓		
6.2	システムと生体認証データの利用状況についてエンドユーザーに通知するためのシステムは永続性があるものとし、システム開発と生体認証データの利用を考慮に入れる必要があります。		✓	
6.3	ユーザーが生体認証データの使用に関する情報にアクセスできるようにする必要があります。  生体認証データの利用に関する情報は最新のものでなければなりません。			✓
6.4	ユーザーが被る不利益な結果に対処するための文書化されたプロセス（深刻化や解決手順など）を実施する必要があります。	✓		
6.5	ユーザーが希望を提示できるようになっていなければなりません。ベストプラクティスには以下を提供することが含まれますが、これに限定されません。 <ul style="list-style-type: none"> <li>– メールアドレス</li> <li>– 電話番号</li> <li>– カスタマーサポートFAQ</li> <li>– カスタマーサポートチャットボット</li> </ul>			✓
6.6	ユーザーから提示された不利益な結果に対してトレーニングの実現と対処が必要です。		✓	
6.7	ユーザーが妥当な期間内（例：30日以内）に個人データ（写真、動画や、アカウントイベント履歴、同意履歴、生体認証データ削除履歴、共有情報、生体認証データの使用履歴など個人のIDにリンクされた生体認証データ）に読み取り可能な形式でアクセスしたり、取得したり、削除を依頼できるようにする必要があります。	✓		✓



要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
6.8	個人データへのアクセス、復元、消去の要求は追跡して実施する必要があります。		✓	
6.9	個人がシステムの運用に関する関連情報に匿名でアクセスできるようにするためのプロセスを実施する必要があります。	✓		✓
6.10	システムの設計と利用を案内するガバナンス規則について、専門家以外の人々が理解できる形で一般の人々に（ウェブサイト上などで）通知する必要があります。			✓
6.11	システム運用に関する関連情報を公開し、アクセス可能にする必要があります。			✓

## 7. 同意

### 要件

顔認証システムの使用については、個人が情報に基づき、自由に、明確で明示的かつ肯定的な同意を提示する必要があります。データ対象者が顔認証技術を利用した新しいサービスに登録するときはいずれも、データ保持期間およびデータ保存の条件に関して明確な同意を表明しなければなりません。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
7.1	ユーザーが顔認証システムの利用について情報に基づいた明示的かつ肯定的な同意を与えることができることを保証するために、同意を対象として実施される措置の定義を提供する必要があります。	✓		
7.2	同意ポリシーはオンラインで提供し、ユーザーに以下の通り、明示的かつ明確な情報を提供しなければなりません。 <ul style="list-style-type: none"> <li>同意ページは最大2回クリックするだけでアクセスできて、「プロフィール」ページに見やすく表示されている</li> <li>主な規定の概要は同じページに記載されており、以下の情報が含まれている <ul style="list-style-type: none"> <li>すべての想定された目的の説明</li> <li>データ保持期間</li> <li>データ共有ポリシー（データを共有する第三者の明記を含む）</li> <li>データを保護し、安全に保管するために実施される手段</li> </ul> </li> <li>この概要は専門家でない人にもわかりやすく簡潔で、長さはA4サイズで2ページ以内とする</li> </ul>			✓
7.3	ウェブ上の同意ページでは、既存の目的ごとに同意を与えるか与えないかを表示できるようになっている必要があります。これらの選択肢はすべて同じページに記載する必要があります。			✓
7.4	各サブスクリプションにおいて、ユーザーはデータ保持期間に対する同意を明確に提示する必要があります。			✓

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
7.5	第三者監査において、企業は各ユーザーが明確に同意を表明したことを証明するために必要な要素を提供する必要があります。		✓	
7.6	企業は同意条項が永続的であり、ユーザーがアクセスできるようになっていることを確認する必要があります。		✓	
7.7	顔認証サービスが進化した場合、既存の目的のリストは最新の状態に保ち、エンドユーザーに明示的に通知する必要があります。  規定は変更を盛り込む形で実施する必要があります。		✓	✓

## 8. 情報の表示

### 要件

公共の場で使用するときには、顔認証技術の利用についてエンドユーザーが理解しやすいようにするため、明確な看板を設置すべきです。顔認証システムが利用されるエリアは常に区切り、個人が分かるように表示すべきです。また視覚的な標識を使用してシステムが稼働中であることを個人に提示する必要があります。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
8.1	顔認証システムの利用に関する情報システムやコミュニケーションの設計については、以下を考慮した上で要件を順守する必要があります。  <ul style="list-style-type: none"> <li>顔認証の利用に関する情報（何をどのように伝えるのかなど）および顔認証システムが使用されるエリア</li> <li>顔認証システムが実施されるエリアを決定する方法</li> </ul>	✓		
8.2	以下を含むすべての情報システムが整備されている必要があります。  <ul style="list-style-type: none"> <li>顔認証システムが使用されるエリアに入る個人に対する明確な情報。この情報は個人が見やすく明確なものとする必要がある</li> <li>インジケータ（視覚的な表示など）によっていつシステムが稼働しているかを個人に知らせる必要がある</li> <li>ユーザーの権利をディスプレイで一覧表示する必要がある</li> <li>顔認証システムの目的をユーザーに知らせる十分な大きさのディスプレイを設置する必要がある</li> </ul>			✓
8.3	ユーザーがキャプチャエリアを明確に理解できるような措置を取る必要があります。		✓	
8.4	情報表示は恒久的な形で掲示し、それを確保するための措置を実施する必要があります。		✓	

## 9. 弱者グループに対するアクセス権

### 要件

顔認証で除外される人がいてはいけませんし、高齢者や障害者を含むすべてのグループの人々がいつでもアクセスでき、利用できる必要があります。乳幼児や子供などこの原則の例外が適切であり、顔認証に代わる代替手段を提供すべき場合があります。




要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
9.1	高齢者や障害者（特に視覚・聴覚障害者）など何人も除外されることがないようなシステムの定義と評価の方法を提供する必要があります。  高齢者や障害者でも顔認証システムを利用可能かどうかについて表示する必要があります。	✓		
9.2	顔認証システムで計画された提供範囲が有効に運用されている必要があります。  ユーザーの提供範囲が一貫しているか、または代替案が適切であるかどうかについても評価が必要です（発生した状況の管理）。		✓	✓
9.3	この原則の例外に対して、顔認証の代替案が提案されるべき場合の定義を定める必要があります。  高齢者・障害者支援のために割り当てられたリソースを記載する必要があります。	✓		
9.4	乳幼児、子供、家族のための代替案の説明を提供し、実施する必要があります。	✓		✓
9.5	何人もこのシステムから排除されないということを確実にする規定を導入する必要があります。システムの有効性を評価し、持続可能にする必要があります（代替案の実施）。		✓	✓

## 10. 代替の選択肢と人の配置

### 要件

公民権侵害を引き起こすなどの重大な結果をもたらす可能性のある使用について人によるレビュー（人による監督）を実施する必要があります。完全自動化されたシステムの場合は例外や予期せぬエラーに対処するため、また改善を実施するため人が常駐する代替システムを常に設置しておくべきです。顔認証システムの使用に対する合理的な代替手段を常に用意しておく必要があります。

要件番号	標準的要件の説明	プロセス要件		
		設計	実装	システムの機能に関する要件
10.1	公民権侵害などの結果を伴う決定につながる可能性のある状況（特に登録段階で、写真付きの身分証明書と顔の照合が偽陰性となる状況）を特定する必要があります。	✓		
10.2	ユーザーのバイアスにつながる状況の発生を予防するため人によるレビュープロセスを実施する必要があります。	✓		✓
10.3	このプロセスはシステム運用において実施・維持する必要があります。		✓	✓

10.4	<p>利用者が誰になるか(乳幼児、子供、家族など)を特定する代替プロセスを実施する必要があります。この代替プロセスでは生体認証の使用を拒否する人も考慮に入れる必要があります。</p>			
10.5	<p>顔認証システムにおいては代替オプションを実施する必要があります、それには以下が必要です。</p> <ul style="list-style-type: none"> <li>- 人が操作するものであること(例外的な状況に対処できるよう訓練を受けている操作スタッフ)</li> <li>- 合理的なものであること。つまり不相応に不利な結果(保安検査場の通過時間が2倍になるなど)をもたらないこと</li> </ul>			
10.6	<p>代替オプションが否定的な結果をもたらないことを保証するためには以下が必要です。</p> <ul style="list-style-type: none"> <li>- 対策の有効性とシステムの改善の分析</li> <li>- 人によるレビュー率の追跡可能性</li> <li>- 公民権侵害など、重大な結果を伴う決定に遭遇した場合の検討</li> </ul>			



付属文書 B1:リスクの定義

リスク番号	特定されたリスク	リスクの記述	リスクの原因

付属文書B2:リスク分析

バイ アス 番号	特定され たリスク	エンドユーザー グループの特徴	リスクに遭遇す る実装プロセ スにおける ステップ	リスク評価パラメータ						リスク分類
-	-	-	-	ユーザーへの影響		差別		公民権		リスク スコア
				重大度	発生確率	重大度	発生確率	重大度	発生確率	潜在的な 重大度
N°1	要記入	要記入	要記入	要記入		要記入		要記入		項目を選ぶ
				項目を 選ぶ	項目を 選ぶ	項目を 選ぶ	項目を 選ぶ	項目を 選ぶ	項目を 選ぶ	項目を選ぶ

リスクレベル特定を可能にする基準(指標)の定義

<p>リスクのレベル</p> <ul style="list-style-type: none"> <li>- 非常に高い = 要定義</li> <li>- 高い = 要定義</li> <li>- 中程度 = 要定義</li> <li>- 低い = 要定義</li> </ul>	<p>発生確率</p> <ul style="list-style-type: none"> <li>- 非常に頻繁 = 要定義</li> <li>- 頻繁 = 要定義</li> <li>- 中程度 = 要定義</li> <li>- 低い = 要定義</li> </ul>
---	--

付属文書 B3:軽減戦略

リスク番号	特定された リスク	リスク軽減戦略		戦略の実績を 測定するための指標	システムに対する 軽減戦略の利点
		設計	実装		

付属文書B4:リスク検出システム

リスク番号	特定された リスク	リスク検出システム	検出の有効性を評価するための運用中の指標の測定		
		戦略の有効性を評価するた めの指標の 実装	I1:	I2:	I3:
		I1			
		I2			
		I3			

# 参考文献

- 1 Shankland, Stephen, "Tokyo 2020 Olympics using facial recognition system from NEC, Intel", CNET, 1 October 2019, <https://www.cnet.com/news/tokyo-2020-olympics-using-facial-recognition-system-from-nec-intel> (accessed 1 October 2020).
- 2 McGinnis, Chris, "Facial recognition is coming to domestic air travel", SFGATE, 8 September 2020, <https://www.sfgate.com/travel/article/Facial-recognition-domestic-flights-15550415.php> (accessed 2 October 2020).
- 3 Opened in 1978, Narita International Airport (Airport code: NRT) offers flights to over 140 domestic and international destinations. It manages about 258,000 take-offs and landings a year. See the Narita International Airport website at <https://www.naa.jp/jp> for more information.
- 4 NEC, "NEC to provide facial recognition system for new 'One ID' check-in to boarding process at Narita Airport", Press release, 28 February 2019, [https://www.nec.com/en/press/201902/global\\_20190228\\_01.html](https://www.nec.com/en/press/201902/global_20190228_01.html) (accessed 2 October 2020).
- 5 Ministry of Land, Infrastructure, Transport and Tourism of Japan, "Guidebook on the handling of personal data in One ID services that utilize face recognition technology at airports", 13 March 2020, [https://www.mlit.go.jp/report/press/kouku19\\_hh\\_000096.html](https://www.mlit.go.jp/report/press/kouku19_hh_000096.html) (accessed 2 October 2020).
- 6 World Economic Forum, "A Framework for Responsible Limits on Facial Recognition – Use Case: Flow Management", White Paper, February 2020, <https://www.weforum.org/whitepapers/a-framework-for-responsible-limits-on-facial-recognition-use-case-flow-management> (accessed 1 October 2020).
- 7 Harwell, Drew and Geoffrey A. Fowler, "U.S. Customs and Border Protection Says Photos of Travelers Were Taken in a Data Breach", The Washington Post, 11 June 2019, <https://www.washingtonpost.com/technology/2019/06/10/us-customs-border-protection-says-photos-travelers-into-out-country-were-recently-taken-data-breach> (accessed 2 October 2020).
- 8 Ibid.
- 9 Manancourt, Vincent, "Controversial US facial recognition technology likely illegal, EU body says", Politico, 10 June 2020, <https://www.politico.eu/article/clearview-ai-use-likely-illegal-says-eu-data-protection-watchdog> (accessed 1 October 2020).
- 10 Burton-Harris, Victoria and Philip Mayor, "Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart", American Civil Liberties Union, 24 June 2020, <https://www.aclu.org/news/privacy-technology/wrongfully-arrested-be-cause-face-recognition-cant-tell-black-people-apart> (accessed 2 October 2020).
- 11 Conger, Kate, Richard Fausset and Serge F. Kovalski, "San Francisco Bans Facial Recognition Technology", The New York Times, 14 May 2019, <https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html> (accessed 2 October 2020).
- 12 Ravani, Sarah, "Oakland bans use of facial recognition technology, citing bias concerns", San Francisco Chronicle, 17 July 2019, <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php> (accessed 2 October 2020).
- 13 DeCosta-Klipa, Nik, "Boston City Council unanimously passes ban on facial recognition technology", Boston Globe, 24 June 2020, <https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban> (accessed 2 October 2020).
- 14 Ruckstuhl, Laney, "Brookline Passes Ban On Municipal Use Of Facial Recognition Tech", WBUR News, 12 December 2019, <https://www.wbur.org/news/2019/12/12/brookline-facial-recognition-technology-ban> (accessed 2 October 2020).
- 15 DeCosta-Klipa, Nik, "Cambridge becomes the largest Massachusetts city to ban facial recognition", Boston Globe, 14 January 2020, <https://www.boston.com/news/local-news/2020/01/14/cambridge-facial-recognition> (accessed 2 October 2020).
- 16 Cote, Jackson, "Northampton bans facial recognition technology, becoming third community in Massachusetts to do so", Mass Live, 27 February 2020 update, <https://www.masslive.com/news/2019/12/northampton-bans-facial-recognition-technology-becoming-third-community-in-massachusetts-to-do-so.html> (accessed 2 October 2020).
- 17 NBC Boston, "Boston Approves Ban on Facial Recognition Technology", 24 June 2020, <https://www.nbcboston.com/news/local/boston-approves-ban-on-facial-recognition-technology/2148450> (accessed 2 October 2020).
- 18 Peters, Jay, "Portland passes strongest facial recognition ban in the US", The Verge, 9 September 2020, <https://www.theverge.com/2020/9/9/21429960/portland-passes-strongest-facial-recognition-ban-us-public-private-technology> (accessed 2 October 2020).
- 19 State of Washington, "Engrossed Substitute Senate Bill 6280", 66th Legislature, 2020 Regular Session, 12 March 2020, <http://lawfilesexxt.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Passed%20Legislature/6280-S.PL.pdf?q=20200331083729> (accessed 2 October 2020).
- 20 Congress.gov, "S.4084 - Facial Recognition and Biometric Technology Moratorium Act of 2020", 116th Congress (2019-2020), <https://www.congress.gov/bills/116th-congress/senate-bill/4084/text?r=1&s=1> (accessed 2 October 2020).
- 21 Future of Privacy Forum, Privacy Principles for Facial Recognition Technology in Commercial Applications, September 2018, <https://fpf.org/wp-content/uploads/2019/03/Final-Privacy-Principles-Edits-1.pdf> (accessed 2 October 2020).

- 22 American Civil Liberties Union, “Coalition Letter Calling for a Federal Moratorium on Face Recognition”, 3 June 2019, <https://www.aclu.org/letter/coalition-letter-calling-federal-moratorium-face-recognition> (accessed 2 October 2020).
- 23 Learned-Miller, Erik, Vicente Ordóñez, Jamie Morgenstern and Joy Buolamwini, Facial Recognition Technologies in the Wild: A Call for a Federal Office, Algorithmic Justice League, 29 May 2020, [https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009\\_FRTsFederalOfficeMay2020.pdf](https://global-uploads.webflow.com/5e027ca188c99e3515b404b7/5ed1145952bc185203f3d009_FRTsFederalOfficeMay2020.pdf) (accessed 2 October 2020).
- 24 Duffy, Clare, “Microsoft president calls for federal regulation of facial recognition technology”, CNN Business, 18 June 2020, <https://edition.cnn.com/2020/06/18/tech/brad-smith-microsoft-facial-recognition/index.html> (accessed 2 October 2020).
- 25 The Amazon blog, “We are implementing a one-year moratorium on police use of Rekognition”, 10 June 2020, <https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition> (accessed 2 October 2020).
- 26 Peters, Jay, “IBM will no longer offer, develop, or research facial recognition technology”, The Verge, 8 June 2020, <https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software> (accessed 2 October 2020).
- 27 European Commission, “On Artificial Intelligence – A European approach to excellence and trust”, COM(2020) 65 final, 19 February 2020, [https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf) (accessed 2 October 2020).
- 28 Espinoza, Javier and Madhumita Murgia, “EU backs away from call for blanket ban on facial recognition tech”, Financial Times, 11 February 2020, <https://www.ft.com/content/ff798944-4cc6-11ea-95a0-43d18ec715f5> (accessed 2 October 2020).
- 29 Ministry of Justice of Japan, “Further Use of Facial Recognition Automated Gates (Notice)”, [http://www.moj.go.jp/ENG-LISH/m\\_nyuukokukanri07\\_00016.html](http://www.moj.go.jp/ENG-LISH/m_nyuukokukanri07_00016.html) (accessed 6 October 2020).
- 30 The National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce. Among its various activities, it runs regular performance assessments of facial recognition solutions from private vendors, public organizations and academic institutions.
- 31 National Institute of Standards and Technology (NIST), “Face Recognition Vendor Test (FRVT), Part 2: Identification”, NISTIR 8271, September 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8271.pdf> (accessed 6 October 2020).
- 32 National Institute of Standards and Technology (NIST), “Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects”, NISTIR 8280, December 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> (accessed 6 October 2020).
- 33 Ibid.
- 34 PR Times, “‘Narita Airport Universal Design Basic Plan’ has been decided”, Press release, 17 April 2018, <https://prtimes.jp/main/html/rd/p/000000234.000004762.html> (accessed 7 October 2020).
- 35 Tokyo 2020 Organising Committee, “The Tokyo 2020 Accessibility Guidelines”, 24 March 2017, <https://tokyo2020.org/en/organising-committee/accessibility> (accessed 6 October 2020).
- 36 Ministry of Land, Infrastructure, Transport and Tourism of Japan, “Guidebook on the handling of personal data in One ID services that utilize face recognition technology at airports”, op. cit.
- 37 European Commission, “EU Japan Adequacy Decision”, Fact sheet, January 2019, [https://ec.europa.eu/info/sites/info/files/research\\_and\\_innovation/law\\_and\\_regulations/documents/adequacy-japan-factsheet\\_en\\_2019\\_1.pdf](https://ec.europa.eu/info/sites/info/files/research_and_innovation/law_and_regulations/documents/adequacy-japan-factsheet_en_2019_1.pdf) (accessed 6 October 2020).
- 38 International Organization for Standardization (ISO), “ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements”, <https://www.iso.org/standard/61651.html> (accessed 7 October 2020).



---

COMMITTED TO  
IMPROVING THE STATE  
OF THE WORLD

---

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

---

World Economic Forum  
91–93 route de la Capite  
CH-1223 Cologny/Geneva  
Switzerland

Tel.: +41 (0) 22 869 1212  
Fax: +41 (0) 22 786 2744  
[contact@weforum.org](mailto:contact@weforum.org)  
[www.weforum.org](http://www.weforum.org)