資料１－４

第 44 回世界プライバシー会議クローズドセッション
2022 年 10 月
顔認識技術における個人情報の適切な利用に関する原則及び期待に係る決議

本決議は、国際執行協力作業部会及び人工知能における倫理とデータ保護に関する作業部会を代表して、スポンサーにより提出されたものである。

スポンサー：

・欧州データ保護監察機関（EDPS)、EU
・連邦データ保護情報コミッショナー（FDPI)、スイス
・情報プライバシーコミッショナー、オンタリオ（カナダ）
・情報コミッショナーオフィス（ICO)、イギリス
・オーストラリア情報コミッショナーオフィス（OAIC)、オーストラリア
・プライバシーコミッショナーオフィス（OPC)、カナダ
・個人情報保護委員会、日本

共同スポンサー：

・データ保護機関、カタルーニャ
・情報・自由委員会、ブルキナファソ
・データ保護機関、オランダ
・データ保護機関、ノルウェイ
・ジブラルタル規制機関、ジブラルタル
・情報アクセス委員会、ケベック（カナダ）
・ジャージー情報コミッショナーオフィス、ジャージー
・国家公共情報アクセス機関、アルゼンチン
・国家情報・自由委員会、フランス
・国家プライバシー委員会、フィリピン
・情報プライバシーコミッショナーオフィス、ニューファンドランド・ラブラドール（カナダ）
・情報プライバシーコミッショナーオフィス、ノバスコシア（カナダ）
・プライバシーコミッショナーオフィス、ニュージーランド
・個人情報保護委員会、韓国
・産業・商業監督官、コロンビア
・個人データ規制管理ユニット、ウルグアイ

第 44 回世界プライバシー会議年次会合クローズドセッション：

顔認識技術（FRT）のプライバシーリスクを強調し、国際執行作業部会（IEWG）と人工知能における倫理とデータ保護に関する作業部会（AIWG）に FRT における個人情報の適切な利用に関する一連の合意された原則及び期待を作成し、促進することを指示した、2020 年 10 月の第 42 回世界プライバシー会議（GPA）のクローズドセッションにおいて採択された、FRT に関する決議を想起し、

調査の実施、文献レビューの実施、GPA メンバーシップへの関与、関連するグロバール・ステークホルダーとの協議並びに原則及び期待の作成により、IEWG と AIWG のメンバーから成るサブグループの設立と FRT に関する決議において設定された指示を達成するための取組みを認識し、

2020 年 10 月の FRT に関する決議の採択に伴い、公共空間、職場、店舗、教育環境、オンライン、戦闘地域など様々な環境において公的部門及び民間部門の組織によるライブの又は遡及的な FRT の開発及び展開が継続していることを認知し、

様々なステークホルダー（規制当局、立法者、開発者、利用者、学術界、市民社会を含む）の間におけるグローバルな討議が継続していること及び、調査結果、ホワイトペーパー、ポジションペーパー、オピニオン、ブログ、学術論文その他のパブリックコミュニケーションにおいて提示された、FRT の利点とリスクに関する彼らのそれぞれの見解を考慮し、

以下を含むがこれらに限られない、政策及びガイダンスの文書の公表を通じた、グローバルな議論に対するデータ保護・プライバシー機関及び国際機関の重要な貢献を認識し、

- 欧州データ保護会議（EDPB）：法執行分野における顔認識技術の利用に関するガイドライン。EU の AI 法案に関する EDPB・EDPS 共同オピニオン。
- カナダの連邦・州・準州プライバシーコミッショナー：警察機関のための顔認識に関するプライバシー・ガイダンス
- カナダの連邦・州・準州プライバシーコミッショナー：警察機関による顔認識の利用に関する法的枠組みに係る勧告
- イギリス情報コミッショナーオフィス：公共空間における顔認識技術の利用に関するオピニオン。公共空間における法執行によるライブの顔認識技術の利用に関するオピニオン。
- 欧州評議会：顔認識に関するガイドライン
- 国連教育科学文化機関（UNESCO）：人工知能の倫理に関する勧告

民間部門、公的部門及び法執行機関による様々な環境における FRT の展開に関連して調査の実施並びに罰金、執行通知及び停止の命令・勧告の発出を含む、データ保護・プライバシー機関の正式な規制上の介入及び執行活動を強調し、

イリノイ州バイオメトリック情報プライバシー法、EU の AI 法案及びカナダの AI・データ法案を含む、FRT の利用を対象とする既存の規制及び立法の動向を考慮し、

FRT の特定の利用に関連する最も重大なプライバシーリスクに関する見解を共有することにより、FRT サブグループの作業に対して行った GPA メンバーのインプットを称賛し、

FRT における個人情報の適切な利用に関する原則及び期待における範囲、用語、明確性、適用範囲及び有用性を改善するための支援を行うことにより、FRT サブグループの作業に対して行った FRT の利用者、開発者、立法者及び市民社会機関のインプットを歓迎し、

データ保護・プライバシー基準の遵守は、世界のどこであろうと、FRT の責任と信頼のある開発及び展開にとって不可欠であることを強調し、

デジタル政策における GPA の発言力を拡大し、規制協力を強化し、そして、世界中で明確かつ一貫性をもって適用されるデータ保護・プライバシーの高い基準を備えた規制環境に向けて取り組むとの GPA2021-2023 年戦略計画におけるコミットメントを再確認し、

利益をもたらす可能性があり、かつ、規制の違いがステークホルダーにとって不確実性をもたらす場合には、明確かつ一貫性のあるデータ保護・プライバシーのグローバル基準の必要性は、FRT のような複雑で高リスクの技術革新の文脈において、特に重要であることを認識し、

第 44 回世界プライバシー会議は、以上を踏まえ、顔認識技術における個人情報の適切な利用に関する原則及び期待を承認し、ここに要約するとともに、附属書において全文を規定する。

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。

第 44 回世界プライバシー会議は、2022～23 年において、次のことを協同することを決議する。

1．次のことを行うエンゲージメント・プランを作成し、実施することにより、FRT に関する GPA の 2020 年決議における任務について引き続き遂行すること。

a. 様々な重要な外部ステークホルダーのグループとともに、これらの原則を促進すること。

b. FRT の開発者及び利用者による実際の適用について評価及び精査を行うこと。

2．IEWG と AIWG が引き続き協同してこれらの活動を実施するとともに、その進捗状況について第 45 回世界プライバシー会議クローズドセッションに報告することを要請すること。

附属書：

顔認識技術における
個人情報の適切な利用に関する
原則及び期待

世界プライバシー会議

イントロダクション

2020 年 10 月に開催された第 42 回世界プライバシー会議（GPA）のクローズドセッションで、GPA メンバーは顔認識技術に関する決議を採択した（以下「決議」と記載）。

決議は、顔認識技術の適用により潜在的にセキュリティや公共の安全に利益をもたら可能性があることを認めるとともに、その技術には、恣意的又は不法な監視を可能にする能力があり、また、侵入性が高く、偏った結果を提供し、データ保護、プライバシー及び人権を侵害する可能性があることも強調している。

公的機関、民間団体及び市民社会は、顔認識技術が対処しなければならないプライバシー上の法的及び倫理的な課題をもたらすことに懸念を表明している。同時に、GPA は以前において、プライバシーに重大な影響を与える問題に関するグローバルな政策、基準及びモデルに向けて取り組む必要性を特定した。これにより、さらに高い水準の規制協力が可能となり、データ保護とプライバシーの課題の効率的な防止、検知及び修正が強化され、デジタル経済に対する監視システムにおける一貫性と明確性が確保される。

したがって、GPA は、リスクの軽減方法についての推奨を含む、顔認識技術における個人情報の適切な利用に関する一連の合意された原則及び期待を作成することを決議した。本文書はその目的にかなうものである。

顔認識について

顔認識とは、ソフトウェアツールが、個人の顔のデジタル画像を分析し、個別の特徴を抽出してバイオメトリックテンプレートにし、1 以上の以前に抽出されたバイオメトリックテンプレートと比較するプロセスである。これは、**検証**（例：個人が主張する身元を検証するための 1 対 1 の比較）又は**識別**（例：バイオメトリックテンプレートの参照データベースに対する未知の個人の画像の 1 対 N 又は N 対 N の比較）の目的で行われる可能性がある。これは、**ライブ又はライブに近い**適用（例：ウォッチリストに対する 1 つ又は複数の顔のリアルタイムの比較）及び**遡及的**適用（例：警察の捜査中における適用など、バイオメトリック参照のデータベースに対する以前に取得された未知の個人の画像の比較）を含む、様々なモードにおいて行われる可能性がある。

決議において認められているとおり、顔認識技術は、個人に固有かつ変化しにくいセンシティブなバイオメトリック情報に基づくものである。これらの識別子を用いて行われる個人に関する決定は、しばしば本人の認識や同意なしに行われ、適切な救済手段がないまま不利

益をもたらす可能性がある。プライバシーへの影響に加えて、顔認識の広範な利用はまた、差別的な影響をもたらし、表現、移動及び結社の自由など、他の基本的人権を行使する能力に影響を与える可能性がある。

原則の適用

これらの原則は、民間部門及び（法執行機関を含む）公的部門の両方の組織による顔認識のすべての種類及び利用に適用される。参照の便宜上、本文書では「顔認識」という用語を使用したが、以下に示す原則は、顔画像及びバイオメトリックテンプレートのあらゆるバイオメトリック分析（人口統計学的な特性、感情の状態等の推定を含む）に等しく適用される。この原則は、顔認識システムの利用者、開発者及び供給者に適用することを目的としている。

重要なのは、以下に示す原則は同等に重要であり、全体として考慮されるべきものであるということである。

最後に、我々は、政府及びデータ保護規制当局が、顔認識技術、特に適切な規制枠組みの確立及び執行に関して重要な役割を担っていることを認識している。しかし、それは本文書の対象外である。

用語

本文書では、以下の用語を使用する：

バイオメトリック：バイオメトリックとは、個人の生理学的特徴（例：人の指紋、虹彩、顔又は手の形状）又は行動的属性（例：歩行、キーストローク・パターン）の測定値のことである。これらの特徴は、概ね永続的なものであり、個人に固有のものであり、かつ、変更が困難又は不可能なもの（すなわち、バイオメトリックの変更には個人の身体の変化が必要になる）である。そのため、センシティブであるとみなすべきである。

バイオメトリックテンプレート：個人のバイオメトリックをデジタルで又は数理的に表したもの。個別のテンプレートのフォーマットは変更可能ではあるものの、バイオメトリックテンプレートは固有のものであり、変更が困難であり、かつ個人と不可分にリンクしている特徴を表すため、センシティブであるとして扱われるべきである。

バイオメトリックプローブ：未知又は未検証の個人から抽出されたバイオメトリックテンプレート。バイオメトリック参照（検証の場合）又は参照データベース（識

別の場合）と比較される。

バイオメトリック参照：既知の身元に紐付いている画像から抽出されたバイオメトリックテンプレート。バイオメトリックプローブと比較される。

参照データベース：バイオメトリックプローブと比較される、バイオメトリック参照のリスト又はデータベース。

法的考慮

以下の原則は、推奨事項（「するべきである（should）」という用語を使用）として表現されている。ただし、原則の多くは、メンバーの管轄内の明示的な法的要件であり、又は、裁判所及びデータ保護当局によってそのように解釈されうるものである。顔認識技術を利用しようとするいかなる組織においても、メンバーの管轄内で適用される法的要件を理解することは義務である。

原則

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。

1.1. 組織は、顔認識のためのバイオメトリクスの利用に関する法的根拠を文書化し、証明する準備を行うべきである。これには、バイオメトリックプローブを作成するために個人の画像を取得するための法的根拠とともに利用されている又は利用される予定の参照データベースを作成し、アクセスし又は修正するための法的根拠の両方が含まれる。これは、法律又はその解釈の変更を考慮するために定期的に見直しがなされるべきである。

1.2. 処理に関して複数の法的根拠が認められる管轄において運用を行う場合、組織は、同意よりも別の根拠が適切であるかどうかを検討するべきである。公的にアクセス可能な空間及び雇用の文脈における顔認識の利用を含む、様々な適用において、組織が、個人から意味のある同意を得ていることを証明することは困難な場合がある。

1.3. 同意が処理の根拠である場合、組織は、同意が意味のあるものであることを確保し、証明できるようにするべきである。これは、同意が、情報提供された上で行われている、具体的で、最新であり、自由に与えられ、不明瞭なものではないことを意味する。これには、(青少年又は社会的弱者の場合など) 個人に意味のある同意を与える能力があるかどうかを考慮することも含まれる。

> 1.3.1. 明示的な同意が望ましい。組織は、多くの管轄において黙示的な同意が同意の基準を満たさないことを認識するべきであり、また、一般的には、センシティブな個人情報の収集については黙示的な同意に基づくべきではない。ただし、顔認識について黙示的な同意に基づくことが可能であると組織が考える状況が生じる場合には、組織は、(i) その状況が適当であること、及び (ii) その状況においては個人が同意したと信じることが合理的であることを証明できるようにするべきである。

1.4. 組織は、顔認識の参照データベースを作成するために、公的にアクセス可能なオンラインプラットフォーム (ソーシャルネットワークサービスを含む) から画像をスクレイピングすることは、多くの管轄において適法又は公正とはみなされず、また、透明性のあるプロセスとはみなされないことを認識するべきである。

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。

2.1. 組織は、顔認識技術を利用する必要性を確立するべきである。関連する情報のセンシ

ティビティを踏まえれば、必要性の確立に係る閾値は高い。閾値には、利用目的が明確に定められること、当該目的の達成においては顔認識技術が有効な場合があること、また、より侵入性の低い手段によっては合理的に当該目的を達成できないことが求められる。必要性の確立は、利便性や望ましさに基づいて行われるべきではない。

2.2. 組織は、顔認識技術の利用の比例性を確立し、証明できるようにするべきである。比例性の確立に係る閾値も高い。顔認識の利用による利益が、個人のプライバシー及びその他の人権に害を及ぼすリスクを明確に上回るべきである。比例性の確立は、以下のとおり行われるべきである。

2.2.1. 組織は、顔認識技術の利用から期待される利益を文書化し、証明できるようにするべきである。また、組織は、システムがこれらの利益を実現したかどうかを評価する方法及びそれ以下では顔認識の利用が停止される利益の水準を明確に規定するべきである。

2.2.2. 組織は、提案された顔認識の利用が潜在的又は既知の害を及ぼすリスクの評価を文書化し、証明できるようにするべきである。これには、個人及びグループに害を及ぼすリスクについての考慮が含まれるべきである。また、組織は、特定されたリスクを軽減するために実施した措置を明確に文書化するべきである。

2.2.3. 識別をする場合、組織は、その技術の利用においては明確な公共の利益があることを証明するべきである。一般的には、商業的な利益は、それ自体では明確な公共の利益とはみなされない。

2.2.4. 検証のために顔認識技術を利用する場合において、原則 1.3 に規定されているとおり、組織が、システムの利用について個人が意味のある同意をしたことを示すことができる場合には、比例性の閾値をより容易に満たすことが可能である。

2.3. 組織は、顔認識技術を利用する合理性を確立するべきである。合理性の確立に係る閾値は高い。合理性とは、個別のケースにおける実情の問題である。合理性は、顔認識技術に関する現在の基準及び慣行だけでなく、社会の期待にも影響される。

2.4. 判断がサンクコストやコミットメントに影響を受けることを避けるため、顔認識システムの購入、開発又は展開に先立ち、合理性、必要性及び比例性の評価を行うべきである。

2.5. 組織は、顔認識の特定の適用による既知の又は潜在的な害が非常に重大であるため意図した利益とは比例しないとした、各データ保護機関のあらゆる決定を認識するべきである。

2.5.1. 特に、組織は、公的にアクセス可能な空間における人間の特徴の認識（顔認識によるものを含む）に関連した潜在的な害により、全ての EEA のデータ保護機関

を含む、複数の国家、地域及び地方のデータ保護機関がこの行為の禁止を提案したことを認識するべきである。

2.5.2. また、組織は、多くのデータ保護機関が、感情の状態の推定など、検証及び識別に関連しない他の形態の顔分析の禁止を要請していることも認識するべきである。

2.6. 合理性、必要性及び比例性に関する組織の評価は、定期的に見直しがなされるべきである。これには、特に、対処する必要性がまだ存在するかどうか、顔認識の利用から期待される利益が実現されたかどうか、事前に特定されなかった害が生じたかどうか、又は特定された害が現在においては利益を上回るほど予想より悪化したかどうかを検討することが含まれる。

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。

3.1. 一般的には、組織は、顔認識技術の利用は個人のプライバシー保護及びプライバシー権に不当に干渉しうるものとみなすべきである。

3.1.1. この干渉は、一般的には、公的にアクセス可能な空間においてこれらの技術を利用する場合に最大となる。組織は、個人が公共空間にいることは、プライバシー又は個人情報の管理に関する合理的な期待を放棄したことを必ずしも意味しないことに特に留意するべきである。原則 2.5.1 により、複数のデータ保護機関は、このような利用の禁止を提案している。

3.1.2. また、干渉は、個人の移動、行動、振舞いを（同じ場所又は複数の場所、特に人のセンシティブな情報が曝される可能性のある場所において）長期にわたって追跡する顔認識の利用により、強まるものである。

3.2. 組織は、（ソーシャルメディアサイトを含む）インターネット上で公的にアクセス可能な個人の画像が、その収集及び利用に関して本人の認識及び同意なしに又は別の法的根拠なしに、バイオメトリックプローブ又はバイオメトリック参照として利用するために、又は顔認識システムの研修のために、収集及び変形されてよいとみなすべきではない。

3.3. データ保護とプライバシー権への潜在的な影響を判断する場合、組織は以下を行うべきである。

3.3.1. （プライバシーへの影響評価、データ保護への影響評価又は人権への影響評価など）適切な影響評価を実施すること。

3.3.1.1. 組織は、プライバシーリスクの評価及び軽減について、影響を受け

る可能性のあるすべての個人に対して透明性を確保するべきである。

3.3.2. システムの機能（例：グループ間における関連する行動の差異）及びシステムの適用（例：システムの展開が個人又はグループに与える影響の差異）の両方に関して、人口統計学的な差異（すなわちバイアス）を考慮すること。また、組織は、顔認識システムの利用に関してグループ間における差異の影響を継続的に評価する方法を検討するべきである。

3.3.3. 顔認識システムの利用目的にかかわらず、公的にアクセス可能な空間における顔認識システムの利用に関連して、表現の自由や結社の自由などの権利に対して「萎縮効果」が生じる可能性や差別の可能性を考慮すること。

3.3.4. 社会的に無視されたグループがシステムの利用に特に影響を受ける可能性がある場合、予想される影響及び害を低減する戦略について、当該グループの代表者たちと協議すること。

3.4. 可能であれば、検証のために顔認証を利用する場合には、同意を拒否又は撤回する個人も含め、バイオメトリクスに基づかない代替手段が利用可能となるべきである。個人は、この代替手段の利用に関して罰せられるべきではない。

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。

4.1. 組織は、個人に対して、以下について情報提供が（平易な言葉で）行われることを確保するべきである。

4.1.1. 取得された本人の顔画像が顔認識システムの対象となる可能性がある又は予定がある場合があること、若しくは本人のバイオメトリックテンプレートが顔認識システムの参照データベースに取り込まれる可能性がある又は予定がある場合があること。顔画像が取得されることについて、個人に対して事前に又は取得時に通知されることが、望ましく、かつベストプラクティスであり、また法律で要求される場合もある。

4.1.2. 顔認識システムに関する本人のデータ上の権利及びその行使方法。これには、本人の顔画像を顔認識システムの対象としないこと、（該当する場合）参照データベースから本人のバイオメトリックテンプレートを削除すること、又は（例えば、バイオメトリック参照の更新により）顔認識システムにおける本人の情報を訂正することを要求することができることが含まれるが、これらに限定されない。

4.1.3. 管轄内の法律により個人に対して提供することが要求されるその他のあらゆ

る情報。これには、情報の保存方法及び保存場所、情報の処理目的、情報の保有期間及び情報が共有される可能性のある組織が含まれる。

4.2. 組織は、年少者及び社会的弱者を含む、すべての個人に対して適切な通知が行われるよう確保する方法を検討するべきである。

4.3. 組織は、顔認識システムの利用に関する標識は、一般的には、それ自体では原則 4.1 の遵守には十分ではないことを認識するべきである。

4.3.1. 処理について同意が必要な場合であって、標識がこの同意プロセスの要素である場合には、標識は、個人が監視対象区域に入る前にはっきりと目に入るようにするべきである。この標識は、その空間にアクセスするためのあらゆる利用可能な代替手段の表示を含むべきである。また、標識は、標準的な監視カメラとは異なり、顔認識が利用中であると明確に表示するべきである。

4.3.2. 標識が組織の通知戦略の重要な部分である場合、表示を読むこと又は理解することが困難となりうる人に対してどのように通知するかを考慮するべきである。

4.4. 遡及的に顔認識を行う場合、組織は、個人がシステムの利用及び目的を確実に認識するための積極的な措置を講じるべきである。これには、システムの利用に先立ってこの情報を公表すること、及び（合理的である限り）システムによって画像を処理された個人に対して特定の通知をすることの両方が含まれる。

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。

5.1. 組織は、顔認識のすべての利用について、ガバナンス及びリスク軽減に係る明確なポリシーを確立し、これらのポリシーの存在と有効性を証明する準備を行うべきである。

5.1.1. 組織は、顔認識に関するガバナンス及びリスクマネジメントに係るポリシーの遵守違反を検知する手段（内部関係者によるものを含む）、並びに遵守違反に対する罰を確立するとともに、維持するべきである。

5.2. 顔認識システムのすべての利用者は、関連するあらゆる内部のプライバシーポリシー、管轄内の法的要件、顔認識システムの限界及びバイアスの可能性、顔の比較の実施方法並びに自動バイアス（すなわち、自動システムによる提案をより重視する人間の傾向）など既知のリスクを軽減する方法について、定期的に研修を受けるべきである。

5.3. 合理的である限り、個人の身元について得られた結論は、関連する研修を受けた人間によって評価されるべきである。これは、個人が当該結論によって重大な影響を受ける場合には特にあてはまる。

5.3.1. 顔認識による識別に基づいて行われた本人についてのいかなる決定に対しても、異議を申し立て、救済を求める機会が個人に対して提供されるべきである。

5.3.2. 組織は、「組織自体又はシステム開発者のどちらが決定するかにかかわらず、システムの提案された適用にとって、「一致」の閾値が合理的であることを確保するべきである。

5.3.3. 組織は、誤一致（偽陽性と偽陰性の両方）及び誤登録（すなわち、参照データベースの不正確さ）に関連するリスクを管理するための軽減戦略を確立するべきである。

5.4. 組織は、顔認識システムの限界を認識し、システムが生成した出力をそれに応じて解釈するべきである。例えば、法執行機関により利用される遡及的な顔認識システムに照らして、「一致」は、 決定的な証拠又は法廷で認められる証拠ではなく、潜在的な手がかりとみなされるべきである。

5.5. 組織は、顔認識システムの有効性、実施中のリスク軽減措置及びガバナンスポリシーの内部遵守状況について、定期的な監査を実施するべきである。

5.6. 組織は、顔認識システムの利用の有効性における人口統計学的な差異を監視し、定期的に評価するべきである。

5.7. 顔認識システムを開発する組織は、その製品における人口統計学的な差異を評価し、保護するために講じた措置及びこれらの評価の有効性（すなわち、人口統計学的な属性のあるグループ間におけるあらゆる既知の行動の差異）を文書化するべきである。

5.8. 顔認識システムの購入その他の利用を検討している組織は、以下を行うべきである。

5.8.1. 原則 5.7 に従って文書化された人口統計学的な差異に関する評価及びそれに対する保護に関する情報を取得すること。

5.8.2. 目的に照らしてデータセットに十分に多様な範囲の個人が含まれていることを確保するため、製品のトレーニング、テスト及び評価の各データセットの人口統計学的な属性に関する情報を取得すること。

5.8.3. 利用目的に対応した方法において製品が設計及びテストされたことを確保すること。例えば、明るくて照らされた場所において管理された環境における検証のために設計された顔認識製品は、暗い場所において高い角度からの又は極めて流動的な環境（例：動く群衆）における認識のためには十分には正確でない可能性がある。

5.8.4. 第三者であるサービス提供者に依存している場合には、原則 5.10 の遵守状況を評価するためのしっかりとしたベンダー・リスクマネジメント・フレームワークとともに、遵守が継続されることを確保するための関連する契約上の保護を整備すること。

5.9. 組織は、顔認識システムに関連するあらゆるデータ侵害について特定し、軽減し、対応し、そして関連データ保護機関に対して通知するための手順及び方針を確立するべきである。

5.10. 組織は、関与するあらゆる第三者が、いかなる法的要件も満たしていることとともに、（第三者に適用される限りで）本文書に示された原則を満たしていることも確保するべきである。

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。

組織は、顔認識システムのライフサイクルを通じて、すべてのデータ保護原則を考慮しなければならない。上記で記載した原則に加え、以下の原則が含まれる。

6.1. プライバシー・バイ・デザイン

6.1.1. 顔認識システムを開発する場合、組織は、プライバシー・バイ・デザインのアプローチを採用して、顔認識システムに最初から保護が組み込まれていることを確保するべきである。

6.1.2. 合理的である場合、組織は、バイオメトリックテンプレート及びあらゆるバイオメトリックの生データの一元的な保存を避けるべきである。例えば、検証の場合、バイオメトリック参照は、（運転免許、パスポート又は社員証明バッジなど）検証される個人が保有する装置又は人工物に保存することができる。（一元的な保存に関する特定の目的が明らかになっている場合であって）バイオメトリックテンプレートが一元的に保存される場合には、強力かつ適切な暗号化措置によって保護されるべきである。

6.1.3. 顔認識システムを利用する組織は、システムの情報ライフサイクルの各段階を通じて、適切な安全保護措置が適用されることを確保するべきである。

6.2. 目的明確化及び利用制限

6.2.1. 組織は、顔認識システムを利用する目的を明確に規定するべきであり、また、法的に認められない限り、当該目的を変更するべきではない。

6.3. データの最小化、保存及び削除

6.3.1. 組織は、(バイオメトリックプローブ又はバイオメトリック参照として利用されるもの、又は参照データベースに保存されるものを含む) バイオメトリックの生データ及びバイオメトリックテンプレートの保存期間を定め、保存する必要がなくなった場合、バイオメトリックテンプレートを削除するべきである。この期間には、時間の経過によりバイオメトリックテンプレートの有用性が低減することが考慮されるべきである。

6.3.2. 一般的には、バイオメトリック参照と一致しないバイオメトリックプローブは、直ちに削除されるべきである。当該画像の保存の制限は、適切な保存方針が存在する場合であって、明確な法的根拠があり、かつ、対象となる処理について明確化された目的に沿っているシステムテストのためなど合理的に必要な場合には許容される。一致したバイオメトリックプローブは特定の期間において保存することができるが、その一致に関連する限りにおいて（すなわち、証拠目的のため、又は本人についてなされた決定に対して個人が異議を申し立てることを可能とするため）利用されるべきである。

6.3.3. 明確化された（かつ適法な）目的にとって必要ではない場合、組織は、顔認識の一致を時系列に関連付けることによって、個人の活動又は行動のプロファイルを作成することを控えるべきである。

6.3.4. 組織は、個人が参照データベースへの登録に同意しなくなった場合、又は削除を要求して削除させる法的な根拠がある場合には、個人が参照データベースからのバイオメトリックテンプレートの削除を要求するためのアクセス可能なメカニズムを整備するべきである。そのような削除は迅速であるべきであり、可能な限り早く（かつあらゆる法的に規定された期間内に）行われるべきである。

6.4. 安全保護措置

6.4.1. 組織は、顔認識システム内の情報について高度なセンシティビティに比例したセキュリティ安全保護措置を実施するべきである。

6.4.2. 組織は、顔認識システム又はそのシステムが収集し又は保存する個人情報のいずれにおいても、不正若しくは意図しないアクセス、誤用、干渉又は紛失が行われないことを確保するために、必要な方針、手順、安全基準及び管理を実施するべきである。

6.4.3 組織は、(第三者によって開発されたものを含む) 展開しようとする顔認識システムには、適切なバイオメトリックテンプレート保護措置が含まれていること、

及びこれらの保護が利用されていることを確保するべきである。可能であれば、これらは、バイオメトリック情報の保護に関する国際的に認知された基準に適合するべきである。

6.4.4. 組織は、進化する脅威の状況に対して十分であることを確保するために、安全保護措置を定期的に見直すべきである。

6.5. データ内容

6.5.1. 組織は、バイオメトリック参照その他のあらゆる、顔認識システムによって収集、生成及び保存される個人情報が、その利用目的にとって十分に正確であり最新であることを確保するべきである。

6.5.2. 組織は、利用目的に関連して不正確な個人情報についてはすべて訂正し、又は削除するための合理的な措置をとるべきである。

6.5.3. 組織は、顔認識システムの利用によく適した画像のみがバイオメトリック参照データベースに取り込まれ、バイオメトリックプローブとして利用されるべきであることを確保するべきである。データ内容の評価においては、少なくとも、ポーズ、照明、画像のサイズ及び解像度並びに顔のオクルージョン（すなわち、眼鏡、帽子、スカーフ及びマスクの存在）を含む、画像の特徴が考慮されるべきである。