行政及び民間等で利用される顔認証システムに対する法的規制に関する意見書

２０２１年（令和３年）９月１６日
日本弁護士連合会

当連合会は，２０１２年に「監視カメラに対する法的規制に関する意見書」（以下「２０１２年意見書」という。）を公表し，監視カメラの設置や運用に関して，プライバシー権や移動の自由，表現の自由，思想信条の自由等が不当に侵害されないよう，基準や要件を定めた法律を制定し規制する必要があること，とりわけ，官民を問わず，データベースとの自動照合による個人識別機能を使用することの禁止等を提言した。また，当連合会は，２０１６年に「顔認証システムに対する法的規制に関する意見書」（以下「２０１６年意見書」という。）を公表して，監視カメラ等で撮影された被写体の顔画像データから顔の特徴等を数値化した顔認証データを生成し，あらかじめ顔認証データを登録したデータベース（以下「顔認証データベース」といい，顔認証データと顔認証データベースを合わせたものを「顔認証データベース等」という。）と照合する顔認証システムについて，これを警察が利用するには法律の根拠が必要であること等を述べた。

しかしながら，未だに，顔認証データベースやこれを利用して照合する顔認証システムに関し，高度のプライバシー侵害性等に配慮する法律は制定されていない。むしろ警察による顔認証データベースや顔認証システムの利用が進んだばかりか[1]，これらの利用が他の行政機関や民間にまで拡大している状況である。かかる状況に鑑み，当連合会は，以下のとおり意見を述べる。

第１　意見の趣旨

１　不特定多数者に対する顔認証システムの利用については，行政部門と民間等とを問わず，市民のプライバシー権等が不当に侵害されないように，国は，①明示の同意のない顔認証データベース等の作成及び顔認証システムの利用の原則禁止，②例外的に行政機関や民間事業者等が顔認証データベース等を作成し顔認証システムを利用することができる場合の厳格な条件，③個人情報保護委員会による実効的な監督，④顔認証システムに関する基本情報の公表，⑤誤登録されている可能性のある対象者の権利保護などを盛り込んだ法律を制定する

[1] 例えば，２０２０年９月１３日付け共同通信ニュース「捜査に顔認証，全国の警察で　３月から運用開始」といった報道もなされている。

など，厳格な規制を行うべきである。

2　前項以外の場合,すなわち特定人に対する顔認証システムについても,また，顔認証データベースを作成しない記録媒体中の顔認証データと特定の照合希望者とのその場限りの照合についても，行政部門と民間部門とを問わず，市民のプライバシー権等が不当に侵害されないように，その利用は，以下の要件を満たす場合に限定されるべきである。

①　それを許容する明確な法律が存在すること

②　同意していない者に対し，顔認証システムが適用されないこと

③　同意に任意性があり，同意しなくても他の方法を選べることなどにより不利益を受けないこと

④　設置者が，個人情報保護委員会に，顔認証システムを設置利用していることを届け出ること

3　少なくとも以下の施策が中止されなければならない。

①　重大組織犯罪の捜査の場合に限定した法律を定めることなく実施される，警察による顔認証システムを利用した捜査

②　医療機関受付での個人番号カードを用いた顔認証システムの利用

③　個人番号カードを健康保険証，運転免許証等と紐付けることにより顔認証データの利用を著しく拡大させ，さらに顔認証システムの利用範囲を拡大させること

そして，行政一般について，顔写真による本人確認で用が足りるにもかかわらず，ことさらに顔認証データの収集及び照合利用をすることは，その取扱いの必要性がないから許されるべきではない。

第2　意見の理由

1　行政機関，民間等[2]での顔認証システムの運用とその拡張

顔認証システムの利用は，日本では，２００２年の日韓共催サッカーワールドカップの際のフーリガン（サッカー観戦時に騒動を起こす者）の入国阻止目的で，関西空港と成田空港の税関に設置，運用されたのが始まりである。

その後，民間でも，テーマパークの年間パスポート取得者が，あらかじめ自分の顔認証データを「年間パスポート有資格者の顔認証データベース」に登録することにより，入口のカメラに顔を向けるだけでＡＩが瞬時に照合し，文字ど

[2] 個人情報保護法制では，①民間事業者，②行政機関，③独立行政法人等の区分があることから，「等」とした。独立行政法人等についても，以下で述べる行政機関に準じた規制が必要である。

おり「顔パス」で入場することができるサービスとして利用されている。また，コンサートチケットが高額で転売されるのを防ぐために，チケット購入者にあらかじめデータを送信させて作成した購入者の顔認証データベースと，来場者の顔とをコンサート会場の入口で照合して入場を許可したり，盗難を防止するために，書店等で万引き犯データベースと来店客の顔とを照合したりといった活用例が増えている。

２０１７年に発売されたスマートフォン「ｉＰｈｏｎｅＸ」では，顔認証による本人確認制度が採用され，その認証の正確さは，指紋認証の１０００倍とされた。正確性は年々高くなっているが，誤認証をゼロにすることはできていない。正確性の向上は，正確な監視につながる点で，濫用された場合におけるプライバシー侵害の深刻さを増やすとともに，正確であるとの信頼ゆえに，誤認証された場合のリスクも高くしている。

一方，行政部門でも，２０１６年に交付が開始された個人番号カード（マイナンバーカード）では，顔認証データを生成可能な顔画像データがＩＣチップに登載されており[3]，自治体においては申請者の顔画像データが顔認証可能な精度であることを確認した後にしか交付されない。

さらに，本年３月から試験運用がなされ，本年１０月から本格運用される予定の個人番号カードと健康保険証の一体化において，厚生労働省は，顔認証機能付きカードリーダーを全額国負担で医療機関に普及するとしている[4]。医療機関の窓口のカードリーダーにマイナンバーカードを置かせて，カードリーダー内蔵のカメラで捉えた患者の顔と，カードのＩＣチップの顔画像データから生成された顔認証データとの一致をチェックすることとなっている。しかも，こうしたマイナンバーカードの健康保険証としての利用について，国は，「将来的に保険証の発行を不要としてマイナンバーカードのみの運用への移行を目指していく」（厚生労働省「オンライン資格確認等システムに関する運用等の整理案（概要）（令和元年６月版）」）として，紙の保険証を廃止することを示唆している。

２０２０年１２月には，２０２４年度末をめどに運転免許証と個人番号カードを一体化する日程が示された。なお，運転免許証には，２００７年から，表面に表示されている顔画像のデータを内蔵したＩＣチップが登載されている。

---

[3] https://www.soumu.go.jp/kojinbango_card/03.html

[4] 厚生労働省保険局医療介護連携政策課「『医療提供体制設備整備交付金実施要領』に関するＱ＆Ａ」（２０２０年７月３日）に，「顔認証付きカードリーダーを導入しない場合は，オンライン資格確認のシステム改修に要する費用等を含め，すべて補助金の交付対象外となります。」とされており，強い政策誘導がなされていると言える。

個人番号カードは，国民の利便性に資するシステムとされ，利便性を求めない市民が生活に支障を来さないよう，任意の取得が前提の制度であったが，健康保険証や運転免許証との一体化により，それを所持しないと生活に支障を来すという形で事実上の強制につながるおそれがある。そのため，個人番号カードの普及を通じた利便性の向上に伴い，市民による顔認証データの行政機関への提出が事実上の義務と化す危険性が高い。

このように，行政においても民間においても，顔認証データや顔認証システムの利用が拡大するという，２０１２年意見書や２０１６年意見書での提言に反した社会的事実が拡大している。

こうした顔認証システムの利用の拡大や，かかる拡大に伴う環境の変化などは，我が国に限ったことではなく，中国など，顔認証システムが，国家による市民の監視に広く用いられている例がある[5]。我が国でも，特に行政機関への規制が欠けると，このような濫用事例すら懸念される。

顔認証システムには，一定の利便性や有用性が認められるが，その反面として，不適切な利用がなされればプライバシー権その他の市民的自由への弊害も著しい。

２　諸外国における顔認証システムに関する規制

(1) ＥＵ

２０１８年５月に適用が開始されたＧＤＰＲ（欧州一般データ保護規則）

[5] ２０１８年2月２６日付けのＮＨＫニュースは，概要，次のように中国の監視カメラ・顔認証技術を紹介している。

「中国では監視カメラが１億７０００万台以上設置されている。顔認証システムで個人を特定しており，例えば赤信号無視で横断歩道を渡ると４００円ほどの罰金を課される。

顔認証システム開発会社の担当者の説明では，顔認証システムで指名手配犯を３０００人逮捕した実績がある。中国のＡＴＭでは，顔認証システムを利用して出金でき，カードも，暗証番号入力も不要である。顔認証システムで，公衆便所の紙の使いすぎも見張っている。反体制派と見られる人物は，北京の地下鉄のカメラで見つかり逮捕された。反体制派とされる中国人作家は，自分たちが常に監視されていたという。」

顔認証システムは，ＡＩによって高速度で処理される。中国が設置・運営する，ＡＩを用いた監視カメラを中心とするコンピュータネットワークは，「天網」（「天網恢々疎にして漏らさず」に由来すると言われている。）と呼ばれ，毎秒３０億回の照合が可能とされる。

新疆ウイグル自治区で少数民族のウイグル族を監視するのに用いられているとの批判もある。

２０１９年には，香港で逃亡犯引き渡し条例改正案に抗議するデモ参加者が，当局による顔認証システムによる監視を回避するために，顔をマスクで覆う対抗策を採った。香港政府は同年１０月，緊急状況規則条例を約５０年ぶりに用いて，デモ隊のマスクや覆面の着用を禁止する覆面禁止条例を，議会手続を経ずに制定し，施行した。マスクなどで顔を覆い個人の識別ができないようにする行為は禁止され，１年以下の禁錮刑などに処せられることとなった。

第９条第１項は,顔認証データを典型とする生体情報の原則収集禁止を掲げ,同条第２項及び第３項が定める例外は，生命に関する利益を保護するために必要な場合や，ＥＵ法又は加盟国の国内法による定めが存在し，重要な公共の利益を理由とする取扱いが必要な場合などに限定されており，民間事業者が収集・利用する場合においても，議会による法律制定がないままの収集は許されない。

また，ＥＵの諮問委員会である欧州データ保護会議（ＥＤＰＢ）のガイドライン（２０１９年の「ビデオ機器を通じた個人データ処理に関するガイドライン」）においても,顔認証システムを用いた空港内のチェックポイントやビルの入退場管理等について,利用者の事前の明示の同意を必要とし,また,同意しない者に顔認証システムを利用しない他の代替手段を提供しなければならないなどとされている。また，監視カメラの管理者は，データ主体である個人からの映像の開示請求に原則として応えなければならないとされている。

さらに，ＥＵではないが，欧州評議会が２０２１年１月に公表した顔認証に関するガイドラインでは，マーケティング目的や防犯目的で，民間企業がショッピングモールなどで個人を識別するための顔認証技術を用いてはならないとしている。

２０１３年には，世界中の人々のインターネットにおける行動の様子について，これらを把握できる立場にあるデジタル・プラットフォーマーが，適法な手続により，諜報機関に情報を提供していたことが元ＮＳＡ（米国国家安全保障局）局員のエドワード・スノーデン氏により明らかにされた。これを意識したＥＵは，プライバシー保護のための規制強化に乗り出した[6]。

２０１６年６月に実施されたイギリスのＥＵ離脱を問う国民投票や，同年１１月のアメリカ合衆国大統領選挙で，勝者側が利用した選挙コンサルティング会社であるケンブリッジ・アナリティカは，このようなインターネット

[6] ２０１５年１０月６日，欧州司法裁判所は，９５年ＥＵデータ保護指令の下で，ＥＵとアメリカ合衆国の個人情報保護レベルが同等であるとして相互流通を認める前提とされていたセーフハーバー協定を無効とした。２０１８年５月に適用が開始されたＧＤＰＲは，諜報機関を含む政府がデジタル・プラットフォーマーに対し容易にアクセス可能な体制（ガバメントアクセスの容易性）を問題とし，このような事態がＥＵに及ばないよう，プライバシー保護を図るために作成された。その後，セーフハーバー協定に代わるものとして定められたプライバシーシールド決定についても，２０２０年７月１６日，欧州司法裁判所はこれを無効とした。ＥＵは，ＧＤＰＲが規定するレベルと同程度のプライバシー保護を，一貫してアメリカ合衆国その他の国に求めている。

における情報をもとに，個人の人格を分析し，特定の考え方を支持する情報に誘導することで選挙に影響を与えたのではないかとの疑問を突き付けた[7]。

(2) アメリカ合衆国

プライバシー保護を重視してきたＥＵとは異なり，アメリカ合衆国では，個人情報が民間事業者の中で自由に流通すること（data free flow）自体が表現の自由であると捉え，その憲法上の地位を高く評価してきた。ＧＡＦＡＭと呼ばれるデジタル･プラットフォーマーは,これを体現する企業として，個人情報を集積し，商業利用を行ってきた。

しかし，ケンブリッジ・アナリティカ事件は，個人情報の自由な流通がむしろ主権者の意思形成をゆがめ，表現の自由を侵害するおそれがあることを明るみに出したため，アメリカ合衆国ではプライバシー権に基づく情報流通（アメリカ流「表現の自由」）の制限が必要であるとの価値観の転換が起きているとされる[8]。現在，デジタル・プラットフォーマーは，それぞれ顔認証システムの利用を制限し，プライバシーを保護する方向へ転向する旨の表明を続々と行っている[9]。

２０２０年１月に発効したカリフォルニア州消費者プライバシー法は，事業者が自ら収集・利用している個人情報の利用目的と利用範囲を開示しなければならず，事後的に求められた場合，その販売を中止，消去しなければならないと規定する。

また，サンフランシスコ市などでは，警察などの市の機関での顔認証技術の利用が禁じられている。

そして，テキサス州，イリノイ州，ワシントン州は顔認証システムを利用したサービスに関する制限立法を行っている。例えば，イリノイ州の生体認証情報私権法（Biometric Information Privacy Act）は，民間企業や民間団体に対し，顔認証データを含む生体認証情報について，本人の事前の同意のない取得等を禁じている。

３　我が国における顔認証システムに対する法的規制の必要性

---

[7] ＳＮＳで捉えられる人格に最も効果的な宣伝をきめ細かく提供することで投票態度を変化させたマイクロターゲティングについては,『ＡＩｖｓ.民主主義　高度化する世論操作の深層』（ＮＨＫ出版新書）に詳しい。

[8] ２０２０年7月２０日に開催された当連合会人権擁護委員会主催の山本龍彦教授（慶應義塾大学）講演会の内容に基づく。

[9] 例えば，２０１８年１２月６日，マイクロソフト社は，顔認証システムに関し，民間事業者の利用に対しても速やかな政府の法規制が必要であると提言している。
https://news.microsoft.com/ja-jp/2018/12/13/blog-facial-recognition-its-time-for-action/

２０１６年意見書で検討したとおり，現在の顔認証システムでは，特定の監視対象者の顔認証データベースをあらかじめ作成している限り，収集された顔画像データから顔認証データを生成した上でＡＩを用いて自動的に検索・照合することが可能である。顔認証データが検索・照合の対象となってしまうと，個人が過去から将来にわたって網羅的な監視対象とされ，その移動履歴が詳細に特定され得る。

したがって，指紋よりもはるかに緻密に個人特定を可能とする生体情報である顔画像データ及び顔認証データには，ＤＮＡ型情報に準じる高度のセンシティブ性がある。

しかも，指紋やＤＮＡ型情報の取得は，押捺行為やＤＮＡ資料の提供等の作為がなければ実現が困難であることから，その同意についても確保される余地がある。しかし，顔認証データの場合，一定程度以上の精度で記録する監視カメラの前を通っただけで，本人が知らないうちに生成され得るし，顔認証システムが実用化される以前から，目視による本人確認目的で顔画像データが収集されてきており（運転免許証の取得・更新が典型である），顔画像データ及び顔認証データにおける高度のセンシティブ性が問題になって以降も，こうした配慮を欠いた取扱いが漫然と続いているのが現状である。

すなわち，顔認証システムが実用化される以前であれば問題とならなかった顔画像データの収集も，顔認証システムが実用化され，警察が現に捜査に活用するようになった現時点においては，２０１６年意見書が指摘したように，厳格な要件を定めてこれを規制しなければならないし，そうした法律がない中で公権力がこれを自由に活用することは許されないというのが，ＥＵ加盟国を代表とする民主主義国家における標準的な考え方である。

当連合会は，指紋，ＤＮＡ型データベース，監視カメラ，顔認証データベース等及び顔認証システムについて，法律による規律を求めてきたが，これは「法治国家」という，民主主義国家であれば当然にクリアされるべき最低要件にすぎない。現在に至るまで法律による規律がなされず，警察権力を代表とする行政機関がフリーハンドでこれらのセンシティブ情報を自由に利用できるという状況は，直ちに是正されるべきである。

法律を定め，顔認証システムに関する利用制限を行うことは不可欠である[10]。

[10] 個人情報保護法や，行政機関個人情報保護法等に適合していれば，個人情報の収集･利用等はすべて適法であるとの誤解も存する。しかし，当連合会が２０１０年１月２２日に公表した「多数の人物･家屋等を映し出すインターネット上の地図検索システムに関する意見書」において検討したように，プライバシー侵害によって不法行為が成立することは判例で確立して

４　法律によって許される利用条件

顔認証データ及びこれを生成することが可能な精度を有する顔画像データは，高度なセンシティブ情報として，その収集，利用及び保存に際しては厳格な要件が求められる。

その利用制限の在り方については，センシティブ情報に対する違憲審査基準として提示された最も厳格な審査基準[11]によるべきである。

そして，現在の顔認証システムには，行政部門と民間とを問わず，例えば以下のようないくつかの類型があるため，これらの類型ごとに利用条件が検討されるべきである。

①　不特定多数者に顔認証システムを利用する場合。典型的には，顔認証データベース（いわゆるブラックリスト）と不特定多数者との照合システム

②　①以外の場合，すなわち特定人に顔認証データを利用する場合。典型的には，あらかじめ同意を得ている有資格者リストとしての顔認証データベースと，特定の照合希望者との照合システム

③　顔認証データベースを作成しないその場限りでの，記録媒体中の顔認証データと特定の照合希望者との照合システム

以下，順に検討する。

(1) 不特定多数者に顔認証システムを利用する場合

ア　顔認証データベース等の作成及び顔認証システムの利用の制限

(1)で取り上げるシステムとしては，２０１６年意見書において検討した，警察による組織犯罪捜査のために活用されている顔認証システムが典型である。警察による利用は上述の最も厳格な審査基準であるべきであり，本意見書は２０１６年意見書に変更を加えるものではない。もっとも，警察以外の行政機関による利用においても，この基準に準じた基準が法定されるべきであるから，本意見書において提言するものである。

おり，個人情報保護法等の施行後も特段緩和されていない（最判平成１７年１１月１１日参照）。総務省が平成３０年３月に定めた「カメラ画像利活用ガイドブック」ｖｅｒ２．０の４頁図表２でも，事業者が配慮すべき範囲について，「個人情報保護法により守られるべき範囲」より大きな部分として，「プライバシー保護の観点で考慮すべき範囲」が示されており，不法行為が成立しないためにプライバシーを配慮すべき範囲が大きいことは，国も認めている。ＧＤＰＲが一般条項とは別に第９条で生体情報の原則収集禁止等を定め，特別な立法を求めているのも，センシティブ性に配慮したプライバシー保護のための上乗せ規制が必要だという同じ趣旨である。

[11] 目的は必要不可欠なやむにやまれぬ利益で，手段はその目的を達成するための必要最小限度のものに限定されることを要求する基準をいう（芦部信喜著・高橋和之補訂『憲法　第５版』（岩波書店）１２４頁）。

２０１６年意見書でも「重大組織犯罪」の捜査に限定すべきとしたように，顔認証データベース等を作成し，顔認証システムを利用することが必要不可欠なやむにやまれぬ利益か否かについては，厳格に解すべきである。

特に，常時，犯罪被疑者や不法出入国者の扱いがなされるがごとき事態は，著しいプライバシー侵害であるにとどまらず，名誉権の侵害も甚だしいので，あってはならない[12]。

(ｱ) 行政機関について

行政機関において，顔認証データベース等の作成及び顔認証システムの利用が許される場合とは，まずは対象者の明示の同意がある場合に限られるのが原則である。

また，対象者の同意なくそうしたことが可能となるのは，重大組織犯罪の捜査に準じる程度の，テロリストの入国防止など，極めて重要な行政目的が存在するとともに，顔認証システムの利用が手段としても不可欠な場合に限定されるべきである。照合の対象となる顔認証データの元である顔画像データも，行政目的の達成のために不可欠な空港などの場所的限定を設けるべきであり，当該場所以外で収集された顔画像データを使用すべきではない。

さらに，以上の条件を満たすか否かを行政機関が独自に判断して顔認証データベースの作成及び顔認証システムの設置・利用が不当に広がらないよう，法律による行政を徹底し，行政機関が顔認証データベースを作成し顔認証システムを設置・利用できるのは，法律が具体的かつ明確に許容している場合に限定すべきである。すなわち，行政･民間に対する顔認証システム規制法が成立した場合，後述のように，民間事業者等に対しては，個人情報保護委員会への許可を通じて監督が及び得る。しかし，行政機関の場合，法治国家及び法の支配の理念から，個別の授権法が必要であると考えられる。そうでなければ，行政機関独自の判断によって必要とされた行政目的のために顔認証システムが運用されることは避けがたいと予想される。２０１６年意見書で示した警察の捜査のた

[12] 小泉雄介「欧米におけるカメラ・顔認証サービスと規制動向」によると，ＦＢＩはパスポート申請写真，ビザ申請者の写真や運転免許証の写真，ニューヨーク市警察ではＦａｃｅｂｏｏｋやＩｎｓｔａｇｒａｍなどのＳＮＳ掲載情報と照合しているが，このような行為は，罪もない善良な市民を常に潜在的犯罪予備軍として捜査下に置くのと同じであるから問題である。２０１６年意見書では，犯罪発生場所との時間的・場所的接着性を要件とし，令状によって収集することを求めている。
https://www.i-ise.com/jp/information/report/2019/20191029_facial_recognition.pdf

めの顔認証システム規制法のような，厳格な例外を定めた個別授権法が不可欠である。

(ｲ) 民間事業者等について

行政機関以外の民間事業者等においても，上記(ｱ)に準じる要件が課されるべきである。

我が国では，このような形態で現に利用されているものとして，書店における万引き犯人等の顔認証データベースと来店客とを照合するシステムがある。ブラックリストに登載されたときの著しいプライバシー侵害及び名誉権侵害に鑑みて，仮に顔認証データベースに登録可能な者の条件を設定するとすれば，当該顔認証データベースの利用者を被害者とする犯罪を行った者に限定するとともに，登録対象者の明示の同意を取得すべきである。

また，顔認証システムの利用は，罪もない多数の来店客を常時，万引き犯データベースと照合することから，一定の制限を設けるべきである。したがって，これを望まない来店客がその存在に気付いて回避し得るよう，そしてその他の来店客のプライバシー侵害を軽減するため，設置場所において犯罪発生の相当高度の蓋然性が存在すること，プライバシー権等に対する不利益がより少ない他の手段がないこと，照合の対象となる顔認証データの元である顔画像データは設置場所で収集されるものに限定されること，顔認証システムにより常時，検索・照合がなされる場所は設置者が管理権限を有する場所であること，顔認証データベース等の作成及び顔認証システムの設置・運用について個人情報保護委員会の許可を受けることといった諸条件を満たすべきである。

(ｳ) 法律に定めるべき内容

以上を踏まえると，顔認証データベース等の作成及び顔認証システムの利用の制限に関し，以下のような内容の法律の制定等が必要である。

① 明示の同意なく顔認証データベース等を作成し，顔認証システムを利用することを原則として禁止すべきである。

② 行政機関において対象者の同意なく顔認証データベース等を作成し，顔認証システムを利用することが許されるのは，以下の条件を満たす場合に限定されるべきである。

ａ 顔認証データベースの登録対象者は，テロリストなど，極めて限定的なものであること

ｂ 達成しようとする行政目的が，入国管理の際のテロリスト等のチ

ェックなど，極めて重要な行政目的であること

c　本人の同一性確認のために，顔認証システムの利用が手段として不可欠であること

d　照合の対象となる顔認証データの元である顔画像データは，行政目的達成のために不可欠な場所で取得されたものに限定し，当該場所以外で収集された顔画像データを使用しないこと

e　顔認証データベースの作成及び顔認証システムの設置・利用について，法律が具体的かつ明確に許容していること

③　行政機関以外の民間事業者等において，顔認証データベース等を作成し，顔認証システムを利用する場合は，以下の条件を満たすべきである。

a　顔認証データベースの登録対象者を，当該顔認証データベースの利用者を被害者とする犯罪を行った者に限定し，かつ登録対象者から明示の同意を取得すること

b　顔認証システムの設置場所において，犯罪発生の相当高度の蓋然性が存在すること

c　顔認証システムの利用よりもプライバシー権等に対する不利益が少ない他の手段がないこと

d　照合の対象となる顔認証データの元となる顔画像データは，設置場所で収集されるものに限定されること

e　顔認証システムにより常時，検索・照合がなされる場所が，設置者が管理権限を有する場所であること

f　顔認証データベースの作成及び顔認証システムの設置・利用について，個人情報保護委員会の許可を受けること

イ　顔認証システムの運用条件等

顔認証データベース等の作成及び顔認証システムの利用を上記アの条件を満たしたものに限った上で，顔認証システムの直接的な利用に限らない運用について，照合対象となるもののプライバシー権を保護するため，２０１２年意見書及び２０１６年意見書の提言に準じた，以下の条件等が満たされるべきである。

①　顔認証データベースと照合される顔認証データは，照合時にのみ生成され，照合終了後，保存されないようにするとともに，顔認証システムの設置場所において取得された顔画像データは，行政上の目的又は民間事業者等の設置目的のための必要がなくなった時点で直ちに廃棄する

こと

② 顔認証データベースに登録する顔認証データは，登録期間を設定し，期間経過後には直ちに消去すること

③ 顔認証システムを目的外利用しないこと

④ 顔認証システムの利用機関等を公示すること。また，現に設置中の監視カメラで顔認証システムを運用している場合は，その場所において，顔認証システムが稼働中であることと，その目的，責任者及び連絡先を明示すること

ウ その他

誤って顔認証データベースに登載されるなどの不当なプライバシー侵害等を防止するため，以下の事項も遵守されるべきである。

① 個人情報保護委員会による監督

個人情報保護委員会が，行政機関及び民間事業者等による顔画像データの収集，顔認証データの生成・取得・利用・廃棄，顔認証データベースの構築・登録・抹消，顔認証システムの利用等が的確に行われているかについて，定期的・実効的にチェックできるようにすること

② 基本情報の公表

設置者は，顔認証システムの仕組や検索・照合の精度について，定期的に公表すること

③ 対象者の権利

顔認証データベースに誤登録されている可能性のある者に開示請求権及び抹消請求権を認めること[13] [14]。これを直接保障することが困難な場合は，個人情報保護委員会を代理機関として適法性の検証を求められるようにすること

---

[13] 東京高等裁判所昭和６３年３月２４日判決も，「他人の保有する個人の情報が，真実に反し不当であって，その程度が社会的受忍限度を超え，そのため個人が社会的受忍限度を超えて損害を蒙るときには，その個人は，名誉権ないし人格権に基づき，当該他人に対し不真実，不当なその情報の訂正ないし削除…を請求しうる場合があるというべきである」と判示し，抹消請求権を認めている。

[14] 当連合会は，２０１６年３月９日，警察庁長官に対し，申立人が過去に暴力団に所属したことがないにもかかわらず，誤って暴力団に所属していたものと登録されたおそれがあり，当該登録に基づき犯罪傾向が進んだ受刑者が収容される刑務所にて処遇されるなどの不利益を受けている可能性が高いとして，「暴力団情報データベース」への登録の有無について申立人からの問合せに回答するとともに，仮にその登録が誤っていることが判明した場合には，当該登録データを削除するよう要望しており，開示請求権及び抹消請求権の重要性について指摘してきたところである。

後段については，設置者自身による開示請求者との直接のやりとりが困難な場合であっても，申し出を受けた個人情報保護委員会が，代理機関として登録の有無，登録されている場合の根拠等をチェックし，適法性の検証を求められるようにすべきこと[15]

(2) (1) 以外の場合，すなわち，特定人に顔認証システムを利用する場合

典型的には，あらかじめ同意を得ている有資格者リストとしての顔認証データベースと，特定の照合希望者との照合システムである。

スマートフォンにおける顔認証システムの利用や，テーマパーク及びコンサート入場の有資格者が自らの利便性のため，任意にそれに同意する場合の顔認証システムの利用については特に問題はない。しかし，同意しない人がそのサービスを一切利用できない立て付けの場合，指紋の１０００倍もの正確さで本人確認ができるとされる情報の提出を事実上強制されることになる。そのため，指紋の強制提出要求の場合と同様，必要性・相当性を満たして民法第７０９条の不法行為が成立しないと言えるかについて問題がある。

そもそも，個人特定性のある顔認証データベース等は，それが一旦濫用されたり流出したりしてしまった場合には，様々な方法で移動履歴や行動履歴を検索される可能性がある上，今後の顔画像データベース等や顔認証システムの高精度化，クラウド等での保存の普及と安価化の可能性などにも鑑みれば，将来の著しいプライバシー侵害を招きかねない。

したがって，特定の人の顔画像データからあらかじめ同意を得て生成された顔認証データで構成されている顔認証データベースと，認証を受けようとする特定の人との一致を照合する制度が利用できるのは，たとえそれが照合を希望する特定人に対するものであっても，市民のプライバシー権等が不当に侵害されないように，それを許容する明確な法律が存在し，かつ同意に任意性があり，同意しなくても他の方法が選択できることなどにより不利益を受けない場合に限るべきである。

なお，同意をしなければサービスが事実上利用できない場合の同意は「任意」の名の下に行われる事実上の強制にほかならず，当然に許容されるべきものではないことを法令等において明記すべきである[16]。

---

[15] 本来，自ら誤登録されているのではないかと思う者からの開示請求が認められるべきである。しかし，現実には存否応答拒否すらなされる可能性があり，実効的な訂正請求権の保障のためには，少なくとも第三者機関によるチェック及びその結果の速やかな開示と，一定期間後の本人への登録理由開示が担保されるべきである。

[16] 脚注１２に引用した資料によると，欧州データ保護会議「ビデオ機器を通じた個人データ

また，同意していない者に対し，顔認証システムが適用されないこと，及び設置者が，個人情報保護委員会に，顔認証システムを設置利用していることを届け出ることを求め，同意のない者へのプライバシー侵害が生じていないか監督可能な仕組みとされるべきである。

(3) 顔認証データベースを作成しないその場限りでの，記録媒体中の顔認証データと特定の照合希望者との照合システム

特定の人の顔認証データを搭載した記録媒体と，監視カメラ等で捉えた対象者との同一性をその場限りで照合する制度についても，顔認証データが濫用により保存された場合には上記(2)同様のリスクがあることから，市民のプライバシー権等が不当に侵害されないように，上記(2)と同様の場合に限定されるべきである。

5　直ちに中止されるべき政策

以上４（1）に述べたところからして，重大組織犯罪の捜査の場合に限定した法律を定めることなく不特定多数の者に対して現実に実施されている，警察による顔認証システムを利用した捜査は直ちに中止されなければならない。

また，４（2）及び（3）に述べたところからして，少なくとも，以下の施策が中止されなければならない。

①　医療機関受付での個人番号カードを用いた顔認証システムの利用

②　個人番号カードを健康保険証，運転免許証等と紐付けることにより顔認証データの利用を著しく拡大させ，顔認証システムの利用範囲を拡大させること

すなわち，①については，これまで顔写真による本人確認すらしなくても大きな不都合は存在しなかった上，当面写真なしの健康保険証と併用されることに照らしても，顔認証システムを利用しなければならないほどの厳格な本人確認は行政上の必要性に欠ける。それにもかかわらず，上述したように，医療機関における顔認証カードリーダーの導入を補助金により強く誘導し，ましてや紙の保険証を廃止して個人番号カードに一元化することで，市民の生命･健康を守るために不可欠な診療行為に関連付けて顔認証システムの利用を事実上義務付けることは，国際的な人権保護基準から著しく乖離する重大なプライバシー侵害であって，実施されるべきではない。

処理に関するガイドライン案」（２０１９年７月１０日）は，空港の顔認証ゲートにおいて，「認識に同意していない旅客の顔特徴データを取得しないようにしなければならない」とされ，コンサート会場の「顔パス」入場等でも同様であるとされる。また，オフィス等の入退場管理に顔認証を用いる場合も，全ての従業員に顔認証を強いるのではなく，それ以外の入場方法（社員証の提示等）も提供しなければならないとされている。

また，②についても，個人番号カードに健康保険証や運転免許証の機能を持たせること（さらには紙の保険証を廃止して個人番号カードに一元化すること）は，多数の市民に対して，顔認証システムとの連動を前提として作成されているマイナンバーカードの携帯を事実上義務付ける結果を招き，顔認証システムによる市民監視の危険性を著しく増大させるものであるから，なされるべきではない。

そして，これらの施策に限らず，行政全般において，顔写真による本人確認で用が足りるにもかかわらず，殊更に顔認証データの収集及び照合利用をすることは，その取扱いの必要性がないから許されるべきではない。

以上