顔認証システムに対する法的規制に関する意見書

２０１６年（平成２８年）９月１５日
日本弁護士連合会

第１　意見の趣旨

１　警察が犯行現場付近における不特定多数の人の顔画像データを収集し，個々人を特定するための特徴点を数値化したもの（以下「顔認証データ」という。）を生成し，これらのデータをあらかじめ生成している特定人の顔認証データで構成されているデータベース（以下「顔認証データベース」という。）との一致を検索して被疑者等の同一性を照合する制度（以下「顔認証システム」という。）について，市民のプライバシー権等の侵害を極力少なくするために，国は，以下の各項の内容を盛り込んだ法律を制定するとともに，関係法令の改正を行う等して，適切な規制を行うとともに，被疑者・被告人等からのアクセス権の保障を認めるべきである。

(1) 利用条件の限定

① 警察が犯罪捜査のために行う，監視カメラ等により記録された顔画像データの収集は，裁判官が発する令状により行うこと（ただし，設置者が権限を有する領域に適法に設置している店舗等の施設内で犯罪が行われた場合の顔画像データを除く。）。

② 犯行現場付近の画像からの顔認証データ生成は，重大な保護法益を侵害する組織犯罪（以下「重大組織犯罪」という。）の捜査に必要な場合に限定し，適法に生成された顔認証データは，捜査のための必要がなくなった時点で直ちに廃棄すること。

③ 警察が既に適法に保有している被疑者・前科者等の顔画像データから顔認証データを生成することが許される場合は，重大組織犯罪の前科者に限定すること。

④ 顔認証データベースに登録する顔認証データは，重大組織犯罪の前科者に限定した上，登録期間を設定し，期間経過後には直ちに消去すること。

⑤ 顔認証データベースの照合は，重大組織犯罪に対する具体的な捜査の必要性がある場合に限定することし，どのような方法なら許されるのか，あらかじめ法律によって条件が明示されること。

(2) 個人情報保護委員会による監督

個人情報保護委員会が，警察による，顔画像データの収集，顔認証データ

の生成・利用・廃棄，顔認証データベースの構築，顔認証データベースへの登録，顔認証データベースの利用状況，顔認証データベースからのデータ抹消等が的確に行われているかをチェックできるようにすること。

(3) 基本情報の公表

顔認証システムの仕組や検索の精度について定期的に公表すること。

(4) 被疑者・被告人等の権利

顔認証システムは，事実に無関係な者のアリバイ（現場不在証明）主張の手段となり得るから，被疑者・被告人等の請求による顔認証システムによる照合が認められるべきであること。また，顔認証データシステムに誤登録されている者に開示請求権及び抹消請求権を認めること。

2　上記内容を盛り込んだ法律ができるまでの間，国家公安委員会は，顔認証データに関する上記内容を含んだ規則を制定し，事前に明示されたルールに則った運用の確保を図るべきである。都道府県警察も，これに則った運用を行うべきである。

3　行政機関は，既に収集済みの顔画像データ等について，顔認証システムの運用に伴うプライバシー権の侵害を防止する観点から，実際の必要以上に高精度な顔画像データの収集・利用を行ったり，必要性なく顔認証データを生成・利用したりしていないかを検証するとともに，以後もこの点に十分に留意すべきである。

特に，都道府県公安委員会が保有している自動車運転免許証作成時の顔画像データを裁判官が発する令状なく捜査機関に提供したり，自ら顔認証データを生成したりしないようにすべきである。

第2　意見の理由

1　はじめに

現在，都市部を中心に，設置主体は多様（警察，事業者，商店街，個人等）だが，全国的に監視カメラの設置が急速に広がっている。その画像が被疑者の早期検挙等に一定の成果を挙げていると社会的に評価されていることから，今後，更に設置範囲が広がり，設置密度も高まることが予想される。それと同時に，監視カメラで記録される顔画像データが高度化し，個人識別をするための顔認証システムに利用されることも着実に進みつつある。これらは，犯罪捜査への貢献度を高めるものと言える。

しかし，顔認証システムには，留意すべき側面もある。監視カメラは，犯罪の発生の有無にかかわらず，無限定に無数の人々の行動を記録するがゆえに，

その管理運用や利用の仕方いかんによっては，無数の人々の肖像権やプライバシー権を侵害する危険性がある。その上，顔認証システムは，膨大な監視カメラ画像から特定の個人を識別することを可能にする検索機能を有しており，これは，人々の行動さえ監視可能とするものであり，更なるプライバシー侵害性を孕んでいる。

当連合会ではこのような状況を憂慮し，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，犯罪の発生を前提とせず，不特定多数人の肖像を，個人識別可能な精度で，連続して撮影し，録画又は配信を行う「監視カメラ」の増加は，プライバシー権等の保障の観点から看過できないこと，そのため，監視カメラの設置及び運用に関して，一定の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等を指摘した。しかし，未だ監視カメラの設置運用に関する法規制のない状態が続いている。

他方で，顔認証システムの技術的発展や実用化が急速に進んでいる。顔認証システムとは，静止画や動画の中から人の顔に当たる部分を抽出し，その部分の中から，目，耳，鼻等の位置関係等の特徴となる地点を抽出した後，顔認証データを生成し，顔認証データベースに登録された顔認証データと照合し，その類似性を判別する制度である。例えば，あるテーマパークでは，年間パスポート取得者は，自らの顔認証データを登録することで，入口のカメラに顔を向ければ，年間パスポート取得者であることを証明するカードを示さなくても，顔認証によって有資格者であることの確認ができる仕組を導入している。また，複数の店舗間で，万引き犯人等の顔認証データを用いた顔認証システムを導入している例がある。いずれの場合も不正利用の危険性はあるが，特に後者は，顔認証データが類似しているというだけの理由で本人の知らない間に監視の対象にされているという事態が起こりかねず，プライバシー権等の侵害に当たるおそれがある。

このような状況を踏まえると，２０１２年意見書において提案した法律が速やかに制定されるべき必要性はますます高まっていると言える。

２　警察に導入された顔認証システムの現状

２０１４年度，全国５都県警察（警視庁，茨城県警察，群馬県警察，岐阜県警察及び福岡県警察）は，顔認証システムを実施する装置（以下「顔認証装置」という。）を実験的に導入した。

警察庁から配備された「可搬型顔画像検出照合装置」は，あらかじめ作成された顔認証データベースと顔認証・照合ソフトウェア（以下「顔認証ソフト」と

いう。）をノート型パソコンに組み込んだものである。このシステムの運用方法の概要は，次のとおりである。

(1) あらかじめ，組織犯罪の前科者等の顔認証データを登録したデータベースを作成しておく。

(2) 犯行現場及び周辺から，監視カメラの画像を収集する。

(3) 顔認証ソフトを使用することによって，(2)の画像の中から人の顔の部分を抽出して顔認証データを生成し，これと(1)とを瞬時に照合することによって，犯罪日時に近接した犯行現場及び周辺に，組織犯罪の前科者等に似た人物がいたか否かを瞬時に探し出す。

警察庁の入札用の仕様説明書によると，その性能は，「１０人以上の顔を同時に検知」，「サングラスやマスク姿，正面でない場合も検知」，「被写体の動きを追跡」，「１０万件のデータベース１秒以内に照合できる」等とある。

3　福岡県弁護士会の調査

福岡県弁護士会が２０１４年に独自に行った監視カメラに関する調査の結果により，以下の点が明らかとなっている。

(1) 福岡県警察は，監視カメラを具体的な組織犯罪が疑われた場合に限定して使用することとしている。組織犯罪捜査に使用目的を限定しており，暴力団対策部（他の県警察における組織犯罪対策課）で使用している。

(2) 福岡県警察組織犯罪対策運営規程（内部規定）に基づいて管理運営している。当該規定は，捜査資料の管理が定められているものであり，暴力団情報が流出しないよう規律するものである。

組織的でない一般犯罪は対象としていないが，規程には明記されていない。

(3) 福岡県警察が自ら設置する監視カメラの画像の他，民間団体が設置した監視カメラの画像も収集することはあり得る。

(4) 顔認証データベースに登録される人物については，組織犯罪を対象とすることからの限定がある。

しかし，上記運用状況には問題がある。すなわち，調査結果によれば，警察庁から顔認証装置を配備された際には，顔認証データの機微性に配慮した運用基準等が作成されておらず，福岡県警察でも作成していない。また，実験的運用がなされている現場で運用基準とされている上記内部規程は，暴力団情報の一般的な管理方法を定めたもので，顔認証装置の使用について，使用できる場合としての対象犯罪や，検索及び照合の対象となるデータベースに登録される者の属性を限定する規定はない。

4　プライバシー侵害の重大性

(1) 顔認証データのプライバシー情報としての性質

顔認証システムは，警察が対象として設定した特定の人物について，顔認証データさえ収集すれば，監視カメラ画像によってその所在を検索及び追跡することができるものである。

人物の同一性を確認及び証明する手段で顔認証データに類似するものとして，指紋やＤＮＡ型のデータベース等が存在する。

指紋押捺制度の合憲性に関する最高裁判所判決（１９９５年１２月１５日）は，「指紋は，指先の紋様であり，それ自体では個人の私生活や人格，思想，信条，良心等，個人の内心に関する情報となるものではないが，性質上万人不同性，終生不変性を持つので，採取された指紋の利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある。（中略）憲法１３条は，国民の私生活上の自由が国家権力の行使に対して保護されるべきことを規定していると解されるので，個人の私生活上の自由の一つとして，何人もみだりに指紋の押捺を強制されない自由を有するものというべきであり，国家機関が正当な理由もなく指紋の押捺を強制することは，同条の趣旨に反して許され」ないとしている。ＤＮＡ型もこれに類する性質を有すると言える。

そのため，現在，指紋及びＤＮＡ型に関する個人情報の収集は警察活動において自由に行うことは許されず,国家公安委員会規則で規制されているが,それらの個人識別機能の高さからすれば，法律による規制が必要である。

顔認証データについては，警察庁の仕様書によれば，「顔画像検索機能」として，「リアルタイム映像からの顔検知画像と登録顔画像の照合が可能であること」とされていることから，いったん登録されれば，例えば，警察庁及び都道府県警察が自ら設置及び管理する監視カメラと組み合わせることにより，特定地点における特定の個人の出現の有無を自動的に検出することが可能であると考えられる。また，「選択した地点の全ての顔検知画像と登録顔画像の照合が可能であること」とされていることから，複数の地点において，特定人の出現の有無を自動的に検出することもできると考えられる。

現時点において，検索の精度の詳細については不明であるが，仮に高い精度で運用されているとすれば,過去に起こった事件の捜査のためだけでなく，事件の発生とは関係なく，現時点における特定人の行動を監視することもできてしまう。

(2) 顔認証データの生成の容易性

顔認証データのデータベースに，顔認証ソフトを使用して，他から収集し

た精度の高い顔画像を照合すれば，特定の個人の顔認証データを自動的に抽出することができる。

従来の監視カメラであれば，人間が動画を直接目視して，被疑者の存否を確認する必要があったため，捜査利用への効率及び正確性の確保といった利便性はあまり高くなかった。これに対して，警察が顔認証ソフトを保有していれば，捜査目的で広く民間団体等から監視カメラのデータを収集すると，その画像が一定程度以上の精度であれば，顔認証データを生成することができ，これを集積した顔認証データベースを作成することができる。警察が自ら街頭や施設内に設置している監視カメラ画像からも，同様のことが可能である。

(3) 深刻なプライバシー権侵害

従来の監視カメラは，肖像権侵害が問題となっていたが，顔認証ソフトが実用化された現在では，様々な場所に設置された監視カメラの膨大な画像から特定の個人が映っている場面のみの検索抽出が可能となった。これを大量に集積することにより，長期間にわたる日常の行動状況を見ることができるため，プライバシー権侵害が問題となっている。

指紋やＤＮＡ型試料は，単独では個人識別性を有しないし，本人が同意しないまま収集されるリスクは比較的低い。しかし，顔認証データの場合は違う。高精度の監視カメラの前を歩いただけで，顔認証データを生成できる顔画像データが収集できる。しかも，顔認証データは，顔認証ソフトの適用により，誰の顔認証画像であっても簡単に生成することができ，多数の監視カメラの連続的な日時情報や位置情報と合わせることにより，どこで何をしていたかまで分かる。そのため，指紋やＤＮＡ型試料と違って，特定の人の行動や私生活を覗き見るのと同じようなことができるという深刻な問題を孕んでいる。

デジタルデータ保存媒体や通信技術の発達により，従来は蓄積が困難であった監視カメラの映像データを長期間大量に保存し転送することが容易になってきている。つまり，いったん警察によって監視対象とされた市民は，過去の，長期間の，広範な場所における行動履歴を，全国の警察によって組織的に検索され監視され利用される状態に置かれることになる。

警視庁は，東京都が策定した「『１０年後の東京』への実行プログラム２００９」[1]に基づく事業として，民間設置のカメラ映像を活用した「３次元顔

[1] 東京都は，２００６年に，オリンピック・パラリンピック招致を目指す１０年後の東京の姿と，それに向けた政策展開の方向性を明示した都市戦略として「１０年後の東京」を策定した。これは，

形状データベース自動照合システム」と「非常時映像伝送システム」の構築に着手している。このような事業に，限定のない顔認証データベースが活用された場合，警察によって無数の個々人の行動履歴を検索及び閲覧し監視できてしまうおそれすらある。

5　法的規制の内容

(1) 法律による規制の必要性

今後，顔認証データシステムが，捜査方法として積極的に活用されるようになるであろうことを踏まえると，その活用が濫用とならないよう，プライバシー保護のための十分な対策が必要である。

そもそも，事件に無関係な市民の画像を網羅的に収集したり，顔認証データを生成したりすることは，憲法が保障する基本権であるプライバシー権を制限するので，これを行う場合は強制捜査として位置づけるべきであり，強制処分法定主義（刑事訴訟法第１９７条第１項ただし書）に則り，事前に捜査方法として法律で許容されていない場合は，実施されるべきではない。

上記システムの規制は，捜査の便宜に偏りがちな警察内で作成される規則や通達・通知によるべきでなく，法律によって許容される条件が規定され，厳格に運用されるべきである。

(2) 監視カメラ画像の収集

２０１２年意見書で述べたとおり，犯行現場付近の監視カメラ画像の提供については，設置者が権限を有する領域に適法に設置している店舗等の施設内で生じた犯罪に関する画像は任意提出によるものとしてよいが，そうでない画像は，捜索差押許可状によって収集されるべきである。

(3) 犯行現場付近の画像からの顔認証データの生成制限・廃棄

犯行現場付近から適法に収集された顔画像データをそのままの状態で利用することは，(2)の収集目的の範囲内であるが，これから更に顔認証データを生成することは，他の顔認証データとの照合を目的とするものであって，プライバシー侵害性が著しく高くなることに留意する必要がある。顔認証システムでは，たまたま偶然現場に居合わせた事件に無関係な市民の行動履歴も探索できるため，全国の警察が便宜性を重視してこれを導入することになれば，プライバシー侵害の危険性が著しく高まる。また，顔認証データの作

東京が近未来に向け，都市のインフラ整備だけでなく，環境，安全，文化，観光，産業等様々な分野で，より高いレベルの成長を遂げていく姿を描き出したものである。「１０年後の東京」計画で掲げた８つの目標を確実に実現するために，毎年度「実行プログラム」が策定されており，「『１０年後の東京』への実行プログラム２００９」は２００９年度に策定されたものである。

成やその照合の過程で誤作動が生じる可能性があるため，誤認逮捕の原因となり得る。このような点を考慮すると，顔認証システムの利用範囲は，法益侵害性が重大な組織犯罪（重大組織犯罪）のみに限定すべきである。従って，犯行現場付近の画像からの顔認証データ生成は，重大組織犯罪の捜査に必要な場合に限定すべきである。

また，いったん作成した顔認証データのうち，顔認証データの不適合等捜査に必要ないことが明らかになった場合は,直ちにこれを廃棄すべきである。顔画像データがあれば，それをもとに顔認証データを作成することができるため，顔認証データとして保存しておく必要はない。

(4) 顔認証データベースへの登録，顔認証データの生成制限・廃棄

顔認証データを顔認証データベースに登録すれば，その後，全国の警察が捜査活動で収集した顔画像から顔認証データを生成し，顔認証データベースに登録されている顔認証データと照合することが可能となるため，捜査機関にとっては極めて便利である。

しかし，このような状態は，顔認証データを顔認証データベースに登録されている者にとっては，常に潜在的犯罪者として監視下に置かれ，全国の様々な場所における犯罪場所での行動の有無を監視されるということを意味する。これは，自分の行動履歴を他人に知られるという意味においてプライバシー権と衝突するだけでなく，犯罪が起これば，常に潜在的被疑者として扱われるという意味において人格権とも衝突するものといえる。

したがって，顔認証データベースへの登録は，重大組織犯罪について有罪判決が確定した者の顔認証データに限定されるべきである。

すなわち，警察が適法に収集した（刑事訴訟法第２１８条第３項等）顔画像データをそのままの状態で利用するのではなく，顔認証データを生成することが許されるのは,顔認証データベースの利用に供する場合のみに限定し，対象者は重大組織犯罪の前科者に限定すべきである。

その場合も，これが無期限に登録され，生涯にわたって犯罪捜査に利用され続けることは，当該人物を常に再犯の可能性のある危険人物として扱い続けることになり，人格権を著しく侵害し合理的でない。当連合会は，「警察庁ＤＮＡ型データベース・システムに関する意見書」（２００７年１２月２１日付け）で，被疑者ＤＮＡ型情報の登録・保管期間を５年から１０年の間で定めることを検討するよう求めているが，顔認証データベースへの登録期間についても，このような期間制限を定めるべきである。そして，その期間を経過した場合には廃棄されるべきである。

(5) 顔認証データベースへの照合

また，顔認証データベースを用いた照合という捜査目的での利用についても，プライバシー権等の保護との均衡から，重大組織犯罪に対する具体的な捜査の必要性がある場合に限定すべきであるとともに，どのような方法なら許されるのか，あらかじめ法律によって条件が明示されるべきである。

(6) 個人情報保護委員会による監督

個人情報の保護に関する法律により設けられている個人情報保護委員会は，個人情報の有用性に配慮しつつ，個人の権利利益を保護するため，個人情報の適正な取扱いの確保を図ることを任務とし，監視・指導・助言等の権限を有する（同法第５１条）。現在，その権限は，民間及び個人番号制の範囲に限定されているが，これを行政機関の業務や警察における個人情報の扱いにも及ぶものとし，顔画像データの収集，顔認証データの生成・利用・廃棄，顔認証データベースの構築，登録，利用，及びデータ抹消等が的確に行われているかをチェックできるよう関係法令の改正がなされるべきである。

なお，都道府県公安委員会の委員は，個人情報の保護に関して専門性を有しておらず，かつ，公安委員会の庶務は，警視庁又は道府県警察本部において処理するものとされている（警察法第４４条）。よって，公安委員会は，警察庁及び都道府県警からの独立性が不十分であるため，監督機関として相応しくない。

(7) 基本情報の公表

上述のとおり，顔認証システムは，現在，一部の警察で試験的に活用が行われており，犯罪捜査への活用が進む可能性があるが，その仕組や検索の精度についてはほとんど公表されていない。実際には十分な精度でないにもかかわらず，過大評価されてしまう場合には，誤認逮捕やえん罪のリスクを高めてしまう。したがって，基本的な情報は定期的に公表し，変更点を明らかにすべきである。

(8) 被疑者・被告人等の権利

顔認証システムは，犯行現場の画像に映っている犯人の顔画像から生成された顔認証データと，犯人以外の者の顔画像から生成された顔認証データの不適合を判断する点においては，事件に関係のない者のアリバイ主張の手段となり得る。したがって，弁護人，被疑者・被告人・再審請求者等の請求による顔認証システムによる照合が認められるべきである。

また，誤って顔認証データベースに登録されてしまった者には，自己の顔認証データが当該データベースに登録されているか否かを問うための個人情

報開示請求権が認められるべきである。これを認める前提として，誤って登録された顔認証データの抹消請求権が認められるべきである。

6　法律制定までの運用について

現在，上述のような法律は未だ制定されていないが，前述の５都県警察では，顔認証装置の運用が行われている。警察による運用についても，顔認証データの要保護性に着目した十分なプライバシー保護対策が取られなければならない。

少なくとも，法的規制の仕組ができるまでの間，国家公安委員会は，顔認証データに関する上記内容を含んだ規則を制定し，事前に明示されたルールに則った運用の確保を図るべきである。また，該当する都道府県警察も，これに則った運用を行うべきである。

7　行政機関において実際の必要以上に高精度な顔画像データの収集・利用，必要のない顔認証データの生成・利用を行わないこと

顔認証システムとは別に，既に行政機関が収集し保有している国民の顔画像データが多数存在する。

たとえば，１９９４年以降，自動車の運転免許証の作成・更新時に，デジタルデータとしての顔画像データが都道府県の公安委員会で収集・保存されている。データの精度によっては，顔認証システムとの連動も技術的に可能であるが，この顔写真データは，実際に車を運転する者が運転免許取得者であるか否かを判別するための運転免許証を作成する目的で収集したものであるから，この顔画像データを裁判官の発する令状なく捜査機関に提供したり，自ら顔認証データを生成したりすることは認められるべきでない。

また，顔認証データの生成が可能となるような高精度の顔画像データを収集及び利用する場合は，それが行政目的達成のために必要不可欠な手段であるかの検討が必要である。

このことは，他の行政機関や地方自治体が業務上の必要から顔画像データを収集し，あるいは既に収集している場合についても当てはまる。したがって，行政機関は，実際の必要以上に高精度な顔画像データの収集・利用を行ったり，必要性なく顔画像データを生成・利用したりしていないかを検証するとともに，以後もこの点を十分に留意すべきである。

8　結論

以上のとおり，当連合会は，意見の趣旨で指摘した内容を盛り込んだ法律が制定され，顔認証システムの運用が規制されるべきであると考える。

以上