犯罪捜査等における顔認証技術の利用に対するプライバシーの保護

海　野　敦　史

Protection of Privacy Toward the Use of Facial Recognition Technologies in Criminal Investigations

Atsushi Umino

Abstract

Japanese law may not sufficiently protect individual's privacy toward the utilization of facial recognition technologies by public authorities for criminal investigations. While such utilization is expanding in recent years, it has some negative impacts. They include increasing threats to reveal one's private life based on the usage of certain software or matching with a database, lack of proper procedures for implementation, chilling effects toward the freedom of expression and association, and difficulty in identifying the violation of fundamental rights. Therefore, it is requested to establish a law to articulate and strengthen the protection of privacy toward the utilization in both substantive and procedural aspects. In the legislation, it is desirable to establish a system to appropriately measure the extent to which the utilization may intrude on people's private lives with reference to the amount of accumulated facial data and the possibility of their matching to other personal data. With this, it is expected that requisite procedures for the utilization as compulsory measures are ensured and that illegality of the utilization without such procedures is stipulated in the law in view of Article 35 of the Constitution of Japan that protects the rights not to be invaded into private spheres. As such, it will be required to clearly specify the conditions and limitations of the utilization of facial recognition technologies for criminal investigations in legislative steps.

Key Words

facial recognition, privacy, private information, personal information, Constitution of Japan, rights not to be invaded into private spheres, fourth amendments of the U.S. Constitution

目　　次

1　序　　論
2　顔認証技術の利用の主な態様
3　顔認証技術の利用をめぐる米国憲法上の議論とその考察
4　我が国における顔認証技術の利用に対するプライバシーの保護
5　結　　論

1．序　　論

近年，官民を問わず，カメラ等に撮影された顔の画像から抽出される顔の骨格や容貌等に関する情報（以下,「顔情報」という）[1] を照合等しつつ，それにより識別される個人本人（以下,「当人」という）の特定や確認等を行う「顔認証」[2] に関する技術（以下,「顔認証技術」という）[3] が，さまざまな局面で利用されている．この顔認証技術の利用（以下,「顔認証利用」という）は，犯罪捜査の局面はもとより，一般的な行政実務においても広がりを見せ始めている．

例えば，行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律27号．以下,「個人番号法」という）に基づく個人番号等が記された「個人番号カード」(個人番号法２条７項参照）は，当人から提出された顔の画像等に基づく情報から，一定のソフトウェアにより目や鼻等の位置関係等を数値化したデータ（以下,「顔特徴データ」という）を生成し，当該カードの受領者の顔情報を顔認証技術の組み込まれた装置（以下,「顔認証装置」という）で改めて確認したうえで，顔特徴データと顔認証装置の顔情報とが一致することを前提に交付されている．それゆえ，個人番号カードに埋め込まれた顔特徴データは，通常の写真とは異なり，相当な確度で当人を特定することが可能なものとなっている．また，警察庁においては，組織犯罪の前科者等の顔特徴データを記録したデータベース（以下,「顔情報データベース」という）を作成のうえ，犯行現場等に設置された監視カメラの画像を収集し，当該画像の中から抽出した顔情報を当該データベースと照合しつつ，現場における前科者等又はそれに似た人物の所在の有無を判定している[4]．これは，警察の責務を定めた警察法（昭和22年法律196号）２条１項の規定を別論とすれば，格別の法律の規定に基づくことなく実施されている．

このような公権力による顔認証利用は，当人のプライバシーに対する懸念を惹起し得る．しかし，我が国では，かかる顔認証利用に対する各人のプライバシー（以下，便宜上「顔認証プライバシー」という）が日本国憲法（以下,「憲法」という）や法律の次元でどの程度保護されているのかという点については不明瞭なまま，実務上の顔認証利用が先行している状況にあるように見受けられる．顔情報は基本的に大衆にオープンな情報であるため，顔認証利用が当人のプライバシーを害すると言えるか否かは必ずしも自明ではないからである．実際，顔認証利用を直接的に禁止する個別法は存在しない中で，それがただちにプライバシーの侵害に当たるとは解されにくい．また，近年における新型コロナウィルスの流行に伴い，各種施設への入退室管理等を行いつつウィルスに対抗する手段として，顔認証技術の有効性に対する国民の認識が大きく高まったこと[5] は，顔認証利用の局面を一層広げていく可能性を秘めているように思われる．

もっとも，顔情報その他の生体情報は，後述するとおり，それ単体としては「個人情報」の一つとして位置づけられ得る中で，生体情報に関するプライバシーの保護は，私的領域の保護等，単なる個人情報の保護を超えた広がりを有するという旨がかねてより指摘されている[6]．ところが，現時点の我が国において，顔認証利用とプライバシーとの法的関係を正面から追究した議論は未成熟である[7]．特に，公権力による顔認証利用がどのような場合にプライバシーの侵害となるのか，また現在の法制度は顔認証プライバシーを適切に保護するのに十分なものとなっているのか，といった問題については，明快な回答が提示されるに至っていない．

一般に，前述の個人番号カードの場合のように，当人も了知しつつ，当人の特定のみを目的として単発的に行われる顔認証利用については，それが当該目的の範囲等を逸脱して行われない限り，プライバシーとの関係が比較的問題となりにくい．これに対し，犯罪捜査や治安の維持等（以下,「犯罪捜査等」という）を目的として，当人の意思に関わりなく，一定の範囲の人物に照準を当てつつ公権力により集中的に行われる顔認証利

用については，プライバシーとの関係が正面から問われ得ると考えられる．かかる観点から，前述の警察庁による顔情報データベースを通じた顔認証利用に対しては，刑事訴訟法（昭和23年法律131号）197条１項但書の規定に基づく強制処分法定主義に即して利用条件が法律上限定されるべきであるという指摘も提示されている[8]．しかし，顔認証利用が刑事手続上の強制処分に該当するか否かということについては，多分に議論の余地があろう．

以上を踏まえ，本稿は，公権力による犯罪捜査等の局面における顔認証プライバシーの法的保護のあり方について，解釈論的な観点から一定の考察を加えるとともに，それを踏まえた立法論的な課題を摘示することを目的とする．その際，顔認証利用が先駆的に広く普及するアメリカ合衆国（米国）では，米国憲法修正４条の規定（以下，単に「修正４条」という）[9]との関係における顔認証プライバシーの保護のあり方が学説等において豊富に議論されていることを踏まえ[10]，当該議論を適宜参照する[11]．具体的には，顔認証利用の主な態様を簡潔に整理したうえで（２節），米国憲法上の主な議論を概観・分析する（３節）．次いで，それを踏まえて国内法上の顔認証プライバシーの保護の状況を整理しつつ，立法論的課題を追究し（４節），一定の結論を導く（５節）．なお，文中の意見にわたる部分はもっぱら筆者の私見であり，その所属組織の見解とは一切無関係である．

２．顔認証技術の利用の主な態様

犯罪捜査等の局面における顔認証利用の主な態様については，以下の各種類に大別することができる[12]．第一に，「顔観察」と称し得る態様で，例えば，①監視カメラにより収集した顔情報の画像を蓄積し読み取りつつ当該カメラの設置場所に居合わせた人々すべての情報を把握するもの，②前記①の情報の把握を監視カメラによるリアルタイム的なモニタリング（以下，「カメラ監視」という）を通じて行うもの，③前記①の情報の把握を第三者により収集された多数の顔情報を通じて行うもの，などがある．

第二に，「顔特定」と称し得る態様で，被疑者等の顔情報を顔情報データベース上の情報（顔特徴データ）と照合しつつ一定の人物像を特定するものである．近年における顔特定は，写真同士の比較等により人力で行われる伝統的な顔情報の照合とは異なり，デジタル化されたデータを通じて瞬時かつ大量に行われ得る．

第三に，「顔追跡」と称し得る態様で，「顔観察」と「顔特定」とが実質的に結合したものである．これは，特定の人物の顔情報を追跡（又は監視）するものであるが，蓄積された顔情報を追跡する場合のほか，カメラ監視を通じてリアルタイム的に顔情報を追跡する場合もあり得る[13]．

これらの顔認証利用の態様は，リアルタイムでの情報の収集等か，それとも蓄積された情報に関する記録の照合等かにより二分することが可能である．同時に，当人の意思に基づき行われるか否かという観点から分類されることもある[14]．いずれにしても，本稿にいう顔認証利用には，単なる顔情報の収集・取得のみならず，当人の属性や私生活ないし私的行動（以下，「私生活等」という）の一端を明らかにする要素を含む情報（以下，「私的情報」という）との照合等により人物像を可視化又は具体化する行為も含まれるところ，それらの特徴を踏まえてプライバシーの保護のあり方を追究することが重要となる．

３．顔認証技術の利用をめぐる米国憲法上の議論とその考察

3. 1　判例の主な議論

米国憲法上，公権力との関係におけるプライバシーの保護の根拠規定は，一般に「不合理な捜索」等を受けることのない権利を保障する修正４条に求められる．判例は，令状手続によらない「捜索」等について，ごく一部の例外を除き，本質的に不合理なものと捉えてきた[15]．そして，修正４条が公権力の不当な物理的侵入行為を防御するのみならず，各人の「プライバシーの合理的な期待」を保護するという判例法理を確立させてきた[16]．

ところが，一部の学説では，かかる法理に根ざす修正４条は，顔認証プライバシーを十分に保護するものではないという旨が指摘されている（3.3参照）．その背景には，少なくとも伝統的な判例においては，警察等による先端的な技術の利用が必ずしも修正４条にいう「捜索」と位置づけられてこなかったという歴史がある[17]．同時に，今日のような情報のデジタル化と距離のあったかつての時代においては，目視での「顔観察」や顔写真の照合等の行為が「プライバシーの合理的な期待」を破るものとは捉えられてこなかったという経緯もある[18]．その前提として，当人が自ら意図的に大衆に露呈したもの（公的空間における顔情報も含まれ得る）は修正４条に基づく保護の対象とはならないという考え方[19]が支配的であったという事情がある．

これに対し，以下に示す近年の複数の判例は，このような捉え方に一定の軌道修正を迫っている．第一に，2012年のJones事件判決（Scalia判事の法廷意見）[20]では，警察当局がGPSの機能を用いて被疑者の車両の位置情報を収集・取得する刑事手続上の捜査（GPS捜査）が令状で定められた範囲を超えて行われたことについて，修正４条にいう「捜索」に該当するとされた[21]．これは，車両の位置情報が「大衆に露呈したもの」と捉え得る中で，それに伴い「プライバシーの合理的な期待」が否定される可能性を克服する形で，その位置情報に対する当該期待を事実上肯定する（修正４条の保護対象とする）考え方であり，この点において伝統的な考え方とは一線を画するものと言える．もっとも，この判例でGPS捜査が「捜索」であることを認定する決め手となったのは，実質的に，GPS受信機器の装着（物理的侵入行為）と当該機器の使用（情報の収集等）との組合せであり[22]，GPS捜査を通じて収集される情報の蓄積の度合いではない．

第二に，2014年のRiley事件判決[23]では，被疑者の逮捕と併せて別途の令状手続を経ずに行われた携帯電話端末及び当該端末に内包された情報の探索について，修正４条にいう「捜索」に該当するとされた[24]．その理由として，一般に携帯電話端末が各人の私生活等に関する多様な情報を大量に含むという点が指摘された[25]．これは，携帯電話端末が本質的に有する情報の量や質に着目し，その包括的な収集がプライバシーに対する脅威となるということを示したものである．すなわち，探索の対象となる情報の量や質によっては，個々の情報単体では「プライバシーの合理的な期待」が否定され得る場合であっても，当該期待が肯定される（修正４条の保護対象となる）という旨を示唆した点において，伝統的な考え方とは異質の要素を有している．

第三に，2018年のCarpenter事件判決[26]では，電気通信事業者が保有する利用者の携帯電話の位置情報を公権力が令状手続を経ずに一定の期間継続的に取得する行為について，修正４条にいう「捜索」に該当するとされた[27]．これは，当該位置情報が当人とは別の第三者たる電気通信事業者から取得するものであるにもかかわらず，それに対して当人の「プライバシーの合理的な期待」を実質的に肯定したという点において，伝統的な考え方（第三者に提供された情報等に対して当該期待は認められないと解する「第三者法理」）[28]とは一定の径庭を有する．なお，この判決は，法廷意見の射程が「監視カメラのような伝統的な監視技術・ツール」には及ばないと説いている[29]．

この点に関連して，一部の学説では，顔認証利用についても，収集・取得される情報の質・量や解析用ソフトウェアの使用等の観点から，街頭等での伝統的なカメラ監視とは大きく異なるという旨が指摘されている．同時に，顔認証利用の実施規模に着目しても，局所的に行われることの多い当該カメラ監視とは区別されるという[30]．特に，第三者が保有する私的情報との照合等を伴う顔認証利用については，ごく短時間で個人の私生活等の相当部分を明らかにする潜在性を秘めており，公権力の権限の濫用が抑制されるべきであるとされる[31]．

一方，その後の下級審の裁判例においては，当人の同意を得ずに行われる顔認証利用はその者の

私的領域を侵害するという旨が端的に説かれている．その理由として，顔認証利用を通じて得られる情報が「詳細，網羅的かつ容易に集積可能」であるという点が指摘されている[32]．また，被疑者のスマートフォンにアクセスするための生体認証については，個人の特定方法や私的情報の集積されたデータベースへのアクセスの可能性の観点から，指紋の提出等と区別され，修正4条に反するという旨を示した裁判例もある[33]．しかし，連邦最高裁判所の判例において，顔認証利用が正面から「捜索」と認定された事案はなく，当該利用が「プライバシーの合理的な期待」を害し得るという認識が形成されるに至っているとは言いがたい状況にある．

3. 2　判例の議論の考察

前述の近年の各判例・裁判例は，伝統的な捜査手法と区別された高度な技術を用いた捜査手法の脅威及びそれが影響し得るプライバシーの利益を問題としている．そして，これらの判例等から，以下の各点が導かれる．それらはいずれも，顔認証利用が修正4条の保護するプライバシーに対する脅威となり得るという旨を示唆するものである．

第一に，一定量の情報の「蓄積」が修正4条に基づく権利の保護を脅かし得るということである．すなわち，継続的なGPS捜査を通じて累積される情報量，携帯電話端末に集積された情報量，一定の期間にわたり電気通信事業者から提供され続ける情報量のいずれもが，修正4条の問題となり得る．これは，単体では「プライバシーの合理的な期待」が認められない情報であっても，それが一定程度蓄積されれば一種のモザイクが形成され，当該期待が認められるようになるという「モザイク理論」の思想[34]に整合的である．ただし，Jones事件判決の法廷意見は，かかる思想自体には否定的な姿勢を示している[35]．

第二に，特定の者に照準を当てた集中的な「監視」が修正4条に基づく権利に対する脅威となり得るということである．これは，Jones事件判決及びCarpenter事件判決から導かれ得る帰結であるが，Riley事件判決で問題となった携帯電話端末内の情報の点検の例からも明らかなとおり，単発的な情報の収集を修正4条に基づく保護対象から外すものではない．情報の収集の実施期間・回数にかかわらず，個人の特定という狙いを超えて，私生活等の様相の把握に結びつき得る形で情報の蓄積が行われることが，修正4条との関係で問題となる[36]．この点についても，モザイク理論の思想に連なるが，それを超えて，集中的な「監視」には情報の遡及的な探索を可能とするという要素があり[37]，当該要素がプライバシーに対して重大な脅威となるという認識を内包するもののように思われる．

第三に，収集・取得された情報の「データベース化」やそれに基づく情報の「解析」の技術等の度合いに応じて，修正4条に基づく権利に対する脅威の程度が変わり得るということである．このことは，当該権利の適切な保護に際しては，収集・取得される情報の量のみならず，当該情報の処理に当たって用いられるソフトウェアの利用や他の情報との照合の可能性等の要素にも踏み込んだ形で，顔認証利用の実態の精査が必要となるということを示している．

犯罪捜査等での顔認証利用については，顔情報が当人において容易に改変可能なものではないということ[38]も手伝って，情報の「蓄積」，「監視」，「データベース化」及び「解析」といった前述の各要素をすべて内包し得る．そのため，その実施の態様によっては，「プライバシーの合理的な期待」を著しく害し得るということが示唆される．それゆえ，近年の判例の論旨の延長線上には，さしあたり，一定の範囲での顔認証利用が修正4条にいう「捜索」として位置づけられる可能性があり，その限りにおいて，顔認証プライバシーが修正4条の保護対象となるという帰結が論理的に導かれ得るように思われる．既述のとおり，連邦最高裁判所の判例は，このような帰結を明示するには至っていないが，今後の更なる判例の蓄積が期待される．

3. 3　学説の主な議論

前述の判例等の議論から導かれ得る帰結は，昨今のデジタル化の進展等を背景に，顔認証利用と修正４条に基づく顔認証プライバシーの保護との関係が正面から問題となる可能性を示している．すなわち，顔情報はそれ単体では隠匿しようのないオープンな情報で「プライバシーの合理的な期待」を肯定しがたいかもしれないが，モザイク理論的な考え方を踏まえれば，顔情報がデータベース化され，必要に応じて他の情報と結合等されつつ公権力に把握されることにより，「プライバシーの合理的な期待」が破られ得る．しかも，蓄積された顔情報の解析その他の処理を通じて当人への「監視」が高度な技術的手段を用いて行われる場合，プライバシーに対する脅威は甚大化する．それゆえ，近年の米国法上の学説においては，顔情報を含む各人の生体情報を修正４条の保護範囲に含めるべきであるとする主張も提示されている[39]．

このように，顔認証プライバシーが修正４条の保護対象となる可能性が考えられる一方で，一部の学説においては，依然として，修正４条の解釈論の枠組みでは顔認証プライバシーが十分に保護されない可能性があるという懸念が示されている．その主な理由や背景事情として，以下の各点が挙げられている．

第一に，一般に警察等による写真撮影が「プライバシーの合理的な期待」を破るものではないと解されている実務にかんがみると，仮に犯罪捜査等における「顔観察」や「顔追跡」に相当の理由を伴う令状が必要となり得るとしても，内部的に行われる「顔特定」については修正４条違反となる余地が乏しいものと捉えられる可能性があるとされる[40]．かかる「顔特定」が当人に特段の実害をもたらさないということが，修正４条の問題となる決め手を欠くという[41]．この点については，「顔特定」における顔情報データベースとの照合等がプライバシーに対する大きな脅威となるにもかかわらず，顔認証利用を直接的かつ個別的に規律する法律を欠いている状況の中で，事実上の「野放し状態」の部分を穴埋めするための立法が求められるとも指摘されている[42]．

第二に，一定の被疑者等に対象を絞って特定の状況で行われる顔認証利用については，合理的なものと捉えられる場合もあるが，特段の嫌疑もなく一般的・概括的に行われる顔認証利用については，修正４条の指向する捜索の合理性を逸脱する可能性が高い．それにもかかわらず，このような顔認証利用の態様の相違とそれに応じた影響について，十分な検討を欠いているという[43]．特に，蓄積された情報に基づく「顔追跡」とリアルタイムでの単純な「顔観察」とを比較した場合，後者の方が詳細な分析が行われる蓋然性が低く，その限りにおいて修正４条の趣旨に抵触する可能性が低下する[44]．これに対し，「顔追跡」に関しては，一定の者に照準を当てつつ，各所に散在する監視カメラのネットワーク等が集積する顔情報の網羅的な精査等を通じて当人の行動を詳細に把握することに結びつく限り，GPS 捜査における位置情報の追跡以上の脅威となり得るとされる[45]．同時に，かかる「顔追跡」が当人の位置情報の収集と結合して行われる場合も少なくなく，そのような場合には，修正４条にいう「捜索」に該当する可能性が格段に高まるという[46]．しかし，これまでの実務上の議論において，かかる捜索の合理性が正面から問題となる機会は乏しかった．

第三に，犯罪捜査等での顔認証利用は，個人の特定のための指紋認証等と異なり，容易に私生活等の様相を明らかにするデータベースを形成しやすく，その場合にはプライバシーやセキュリティに対する重大な脅威となり得るとされる．特に，ソーシャルメディア上の顔情報がそこで示される私的情報と結合すると，かかるデータベースが形成される確度が高まるところ，そのような状態は（第三者法理も手伝って）修正４条の問題と認識されにくいという[47]．しかも，指紋認証等は高度な技術的訓練を経た捜査官等により行われることが一般的であるのに対し，顔認証利用は必ずしもその限りではなく，比較的手軽に実施され得る[48]．加えて，監視カメラ等による顔認証利用は，「公

的空間における匿名性」を事実上剝奪する可能性が高く，この点でもプライバシーに対する脅威となり得るが，それが継続的に行われるものではない限り，修正４条の問題として扱われることは少ないとされる[49]．

第四に，たとえ顔認証利用が修正４条の予定する適正な手続の下で実施されたとしても，そこで用いられるソフトウェアが不適切なものであれば，不正確な形で個人の特定が行われ，その結果として当人のプライバシーその他の利益が害されるおそれもあるとされる．特に，当該ソフトウェアについては，公権力が自ら作成するとは限らず，むしろ私人により開発される可能性が高いということに留意する必要がある．それゆえ，立法等を通じて，当該ソフトウェアの最低限の正確性を確保することが求められるという[50]．

４．我が国における顔認証技術の利用に対するプライバシーの保護

4. 1　顔認証技術の利用に対する憲法上のプライバシーの保護

翻って我が国の法の下では，顔認証プライバシーはどの程度保護されているのであろうか．この問題の追究に当たり，まず，憲法上保護され得るプライバシーとの関係について考察する．

憲法学説においては，憲法13条に根ざして「プライバシーの権利」としての「自己情報コントロール権」が保障されるという考え方（以下，「自己情報コントロール権説」という）が提示され，通説的な地位を占めてきた．自己情報コントロール権説は，「個人の自由な人格の発展」に必要となる「自己の存在にかかわる情報を開示する範囲を選択できる権利」としての「自己情報コントロール権」を措定する[51]．この権利は，「自己情報」の収集，利用，開示（提供）等のあらゆる取扱いの過程における当人による統御ないし自己決定を予定する．そして，自己情報コントロール権の侵害となるのは，個人の人格的自律（道徳的自律）を支える思想，信条，精神，身体に関する基本的な情報（プライバシー固有情報）が当人の意思に反して（すなわち当人の同意を得ずに）公権力により取得，利用，開示等される場合であるという．これに対し，氏名や住所等，当人の人格的自律の存在に直接関わらない外的な事項に関する情報（プライバシー外延情報）については，公権力が適正な方法により取得，利用等しても，ただちに自己情報コントロール権の侵害とはならないとされる[52]．

このような枠組みの下では，顔情報それ自体については，身体に関する情報の一部とはいえ，遺伝子検査により判明する情報や病歴に関する情報等とは異なり，一般に秘匿性が乏しく人格的自律の存在に直接関わるものとは認めがたいことから，プライバシー外延情報に属するものと考えられる．よって，正当な目的及び適正な入手手段が確保される限り，公権力が顔情報を任意に取得，利用等できるという帰結が導かれ得る．ゆえに，自己情報コントロール権説による限り，顔認証プライバシーの保護の程度は必ずしも高くないと言わざるを得ない．

もっとも，近年の学説においては，自己情報コントロール権説に批判的な考え方も提示されており，同説に依拠すること自体の妥当性が争点となり得る[53]．例えば，自己決定の手段的性格や自己情報の利用に対する当人の同意の有効性への疑問等を背景に，憲法13条の規定を根拠として，プライバシーの権利を「自己情報の適正な取扱いを受ける権利」ないし「個人情報の保護を求める権利」として再構成する見解が注目を集めているが[54]，仮にそれによった場合でも，犯罪捜査等における顔認証利用については，「適正な取扱い」の一環として捉えられ得る[55]．当該見解においても，情報の取扱いの適正性を判断する方法に関しては，基本的にプライバシーの保護法益と公権力側の利益との衡量によるなどと説かれるにとどまり，今後の「最大の課題」とされているからである[56]．

最高裁判所の判例は，自己情報コントロール権説を明示的に承認してはいない．むしろ，同説と一定の距離を取りつつ，憲法13条に根ざす「私生活上の自由」の一環として，「みだりにその容ぼ

う・姿態（中略）を撮影されない自由」[57] や「個人に関する情報をみだりに第三者に開示又は公表されない自由」[58] が認められることを示している[59].

しかし，これらは，「個人に関する情報をみだりに取得又は利用されない自由」までをも正面から認めるものではなく，「自己情報」の収集，利用，開示等の各過程における当人による統御ないし自己決定を予定する自己情報コントロール権説の思想とは径庭がある．また，「みだりに容ぼう・姿態を撮影されない自由」（肖像権）が承認されるとしても，公権力が正当な目的により当人の同意や令状手続によることなく写真撮影をすることは，「犯罪捜査の必要上」許容され得ると解されている[60]．同時に，「人が他人から容ぼう等を観察されること自体は受忍せざるを得ない場所」における捜査活動としてのビデオ撮影の適法性も認められている[61]．これらの点にかんがみれば，顔認証利用も写真撮影等とほぼ同様に，基本的には許容されるものとして捉えられる可能性もある[62].

一方，令状手続を経ずに実施されたGPS捜査の適法性等を問題とした近年の判例は，修正4条を「母法」とする憲法35条1項の規定から，「私的領域に『侵入』されることのない権利」（以下，「私的領域不侵入確保権」という）を導いている[63]．この判例の趣旨を踏まえて考える限り，情報の収集・取得に関して「私的領域への侵入」が認められる場合とは，「個人の行動を継続的，網羅的に把握することを必然的に伴う」ことにより「個人のプライバシーを侵害し得る」こととなる場合となろう[64]．このとき，GPS捜査を通じて得られる車両の位置情報とは異なり，顔情報はそれ単体では個人の行動の詳細を示したり推知させたりするものではないことから，その限りにおいて，顔情報の把握は「私的領域への侵入」ないしプライバシーの侵害には該当しないということにもなり得る[65]．一部の学説においても，例えば判例上問題となった強制採尿[66] との比較において，顔認証利用の脅威は相対的に軽微であるという旨が指摘されている[67]．それゆえ，判例の論理の延長線上にも，（令状手続によらない）顔認証利用が私的領域不侵入確保権の侵害には該当しないという帰結（ないし憲法35条1項にいう「捜索」に該当しないという帰結）が導かれる可能性がある.

他方，憲法31条の規定との関係において，公権力の顔認証利用に関して適正な法定手続の保障が求められるか否かについては議論の余地がある．一般に，憲法31条の趣旨は刑事法上の「刑罰」が課される際の手続的保障であると解されているところ[68]，厳密にそれによる限りにおいては，科刑に至らない局面での顔認証利用に法定手続の保障が及ぶものではないということになり得る．もっとも，犯罪捜査の段階における身体や行動等の自由に関わる問題についても当該手続的保障の射程に含めて解する見解が有力であるため[69]，犯罪捜査等の局面における顔認証利用に関してもこれに含まれると解する余地もなお残されている.

この点に関しては，憲法31条に基づく法定手続の保障の範囲をめぐる根本的な解釈論に連なる．この保障が「法の下の平等な正義を実現する不可欠の前提」[70] であるということを踏まえると，厳密に科刑の局面に限定して適用する必然性は乏しい．それゆえ，憲法31条にいう「自由を奪はれ」という文言に着目し，当該保障の範囲について，（刑事手続に限らず）憲法上の「自由」を著しく奪うこととなる行為（以下，「自由剝奪行為」という）[71] 全般に拡大して捉えることが合理的であると考えられる[72]．判例も，第三者の所有物を当人に告知等せずに没収する行為を憲法31条違反としているが[73]，これは（科刑を伴わない）財産的利益に対する著しい制約（没収）を自由剝奪行為と捉えたものと解し得る．同時に判例は，憲法31条に基づく保障が刑事手続以外の行政手続にも及び得るということも示している[74]．ただし，憲法31条が想定する自由剝奪行為とは，「刑罰」が課される水準に相当する自由の剝奪を意味すると考えられることから，「科刑が身体の自由に対して及ぼす制約に準じた水準でのさまざまな基本権（又は基本権法益）に対する著しい制約となる行為」を指すものと解される[75]．これには，個人の

私生活を丸裸にするような著しいプライバシーの侵害も含まれよう．ところが，このような水準に至らないと認められる制約にとどまる限り，ここでいう自由剝奪行為には該当しないと考えられる．ゆえに，単に顔認証利用が行われるというだけでは，必ずしも自由剝奪行為には該当しないと評価される可能性も高く，憲法上常に適正な法定手続が予定されているものとまでは言いがたいように思われる．

もっとも，既に示唆したとおり，顔認証利用の実施の態様によっては，データベースとの照合等を通じた徹底的な「顔追跡」により「個人の行動を継続的，網羅的に把握することを必然的に伴う」形で，私生活等の相当部分を明らかにし得るため，前述の「私的領域への侵入」（私的領域不侵入確保権の侵害）と捉え得る場合は想定される．かかる場合には，当該顔認証利用を自由剝奪行為と評価する（法定手続の保障が及ぶと解する）余地も認められる．しかし，顔認証利用の実施の態様が必ずしも十分にオープンになっていないことも手伝って，かかる評価が困難な場合（基本権の侵害が判定しづらい場合）が多いように思われる．

以上を総合すると，一般的な憲法解釈論に照らす限り，「プライバシーの権利」の内実に関して，学説のように「自己情報コントロール権」又は「自己情報の適正な取扱いを受ける権利」と捉えるにせよ，判例のように「私生活上の自由」又は私的領域不侵入確保権として捕捉するにせよ，顔認証プライバシーは十分な保護を受けることにならないおそれがあると言える．同時に，顔認証利用の実施の態様によっては基本権の侵害と評価し得るものについても，顔認証利用の「装い」（当人の顔を識別・特定する行為にすぎないという外観的要素）それ自体からは，かかる評価がただちに導かれるものではなく，プライバシーの侵害とは認定されない可能性が高い．顔情報そのものは大衆にオープンな情報であって，公権力がこれを収集のうえ利用したとしても，ただちに「私生活上の自由」や私的領域を侵害したとは言いがたいからである．これらのことは，顔認証プライバシーが「プライバシーの合理的な期待」を保護する修正４条の問題となり得ることを示唆する米国憲法上の議論に照らすと，必ずしも合理的な解釈論的帰結とは言えないように思われる．

もっとも，我が国では，修正４条との関連性の高い憲法35条１項のみならず，憲法13条を基軸としてプライバシーの権利が保護されていると解されることが一般的であるため，プライバシーの保護のあり方が修正４条の問題に収斂しがちな米国憲法上の議論とは差異があり，当該議論が顔認証プライバシーの保護に関してそのまま妥当するわけではないという考え方もあろう．しかしながら，我が国においても，憲法35条１項の規定から導かれる私的領域不侵入確保権を中核としてプライバシーが保護されると解することは十分に可能であると考えられ[76]，憲法13条の規定とその解釈論が米国の議論から導かれる示唆を排する理由とはならない．また，顔認証利用が街頭等でのカメラ監視とは区別されるという前述の議論を踏まえつつ，当該利用により得られる情報が「詳細，網羅的かつ容易に集積可能」であり，その実施の態様によっては情報のデータベース化等を介して個人の私生活等の概況の把握に結びつく可能性があるという日米両国に共通する実態を踏まえると，少なくとも，顔認証プライバシーが憲法上の保護の射程から外れると解することの合理性は乏しい．したがって，憲法上の顔認証プライバシーの保護については，その解釈論次第では，不十分なものに終始する可能性を秘めているという問題点を抱えているように思われる．

4．2　顔認証技術の利用に対する法律上のプライバシーの保護

それでは，法律上，顔認証プライバシーはどの程度保護されているのであろうか．現在，公権力による顔認証利用を個別的かつ直接的に規制する法律は存在しない[77]．また，一般的な写真撮影を行う捜査手法を規律する刑事訴訟法上の規定や街頭等でのカメラ監視のあり方を直接規律する個別

法も存在しない．それゆえ，犯罪捜査を目的として顔情報が収集され，顔認証利用が行われることは，警察法２条１項等の規定に基づき，それがみだりに実施されるものでない限り，正当化されるものと解されてきたと考えられる[78]．

他方，顔情報が法律上の「個人情報」に該当する限り，その収集・取得は基本的に個人情報保護法制に基づく規律に服することとなる．そこで，当該規律の主な内実について，以下に整理することとする．

我が国の個人情報保護法制は，かつては，民間部門を規律する「個人情報の保護に関する法律」（平成15年法律57号．以下，「個人情報保護法」という）と，公的部門を規律する「行政機関の保有する個人情報の保護に関する法律」（平成15年法律58号）等から構成されていた．しかし，デジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律37号）により，双方の規律が一元的に個人情報保護法に集約された．その結果，捜査機関を含む行政機関等（国の行政機関，地方公共団体の機関，独立行政法人等及び地方独立行政法人）における個人情報の取扱いについても，個人情報保護法の規律を受けることとなった．

その前提として，個人情報保護法は，「個人の権利利益を保護する」（個人情報保護法１条）ことを目的としつつも，「プライバシーの権利」や自己情報コントロール権を明示的に規定するものではないということに留意が必要である．一部の学説において，個人情報保護法制は「自己情報コントロール権に応じるしくみ」であるとも指摘されているが[79]，判例上自己情報コントロール権が承認されておらず「プライバシーの権利」も一義的に捉えられているわけではないことを踏まえ，あえてこのような権利が明示されなかったという立法の経緯[80]が軽視されるべきではなかろう．

顔情報については，生存する特定の個人を識別可能なものであれば，個人情報保護法上の「個人情報」（個人情報保護法２条１項）に該当する．また，同法２条２項１号にいう「個人の身体の一部の特徴」を示すものであり，それが生存する個人を識別可能な形で電子計算機を用いて可読できるように符号化されている場合には，同条１項２号にいう「個人識別符号」に該当することから[81]，「個人識別符号が含まれるもの」として，個人情報保護法上の「個人情報」に該当すると解される[82]．

それゆえ，「個人情報」に該当する顔情報を警察当局その他の行政機関等が保有するに当たっては，その利用目的の可能な限りの特定，不適正な利用の禁止，不正な手段による取得の禁止，正確性の確保，安全管理措置（情報の漏えい，滅失又は毀損の防止等のための措置）の実施等の一般的な規律が及ぶものの（個人情報保護法61条・63条・64条・65条・66条・69条１項参照），顔情報の収集・取得に際して当人の事前の同意は必要とされていない．これは，民間部門の個人情報取扱事業者（同法16条２項参照）による「要配慮個人情報」（当人の人種，信条，病歴等の取扱いに特に配慮を要する情報．同法２条３項参照）の取得については原則として当人の事前の同意が必要とされていること（同法20条２項参照）との対比において，相対的に（公権力等による）情報の利用を重視した規律であると言える．ゆえに，顔情報単体としての保護の程度は必ずしも高いとは言えない．同時に，これらの規律に対する違反がプライバシーの侵害に該当するか否かについては別途の検討が必要であり[83]，当該規律の存在をもって顔認証プライバシーの十分な保護が図られていると断じることは困難である．

また，国の行政機関が個人情報ファイル（検索可能な形で体系的に構成された個人情報の集合物．個人情報保護法60条２項参照）を保有しようとするときは，原則として，その利用目的等を個人情報保護委員会に通知することが義務づけられ（同法74条１項），地方公共団体の機関を含む行政機関等が保有する個人情報ファイルについては，個人情報ファイル簿を作成・公表することが義務づけられている（同法75条１項）．それゆえ，「個人情報」に該当する顔情報が個人情報ファイルを構成する場合には，これらの規律が関わり得

る．しかし，犯罪捜査等の目的で作成される一定の個人情報ファイルについては，これらの規律の適用対象外となっている（同法74条２項・75条２項）．同時に，個人情報取扱事業者による個人情報データベース内の個人情報の取扱いとは異なり，個人情報ファイル内の顔情報を利用する必要がなくなったときに遅滞なくそれを消去する努力義務（同法22条参照）等は定められていない．ゆえに，顔情報で構成される個人情報ファイルの取扱いについても，顔認証プライバシーを保護する観点からの規律は比較的緩いと言える．

もっとも，顔情報の主体となる当人においては，行政機関の長等（個人情報保護法63条参照）に対して自分自身の個人情報に関する開示請求権（同法76条），訂正請求権（同法90条）及び利用停止請求権（同法98条）を有する．行政機関の長等においては，一定の場合（開示が犯罪捜査等の公共の安全と秩序の維持に支障を及ぼすおそれがあると認めることにつき相当の理由がある情報が含まれている場合等）を除き開示が義務づけられ（同法78条），理由があると認められる場合には訂正が（同法92条），また一定の限度で利用停止が（同法100条），それぞれ義務づけられる．それゆえ，情報の開示・訂正・利用停止の観点からは，一定の範囲で，顔情報が個人情報に該当する場合における当人の権利の保護が図られている．しかし，これらの権利の保護が（憲法上の）顔認証プライバシーの保護の問題として位置づけられるか否かについても，（前述の行政機関等に対する一般的な規律と同様に）慎重な検討が必要である[84]．

他方，顔認証利用に対する手続的統制について考えると，たとえ当該利用が刑事手続上行われる場合であっても，当然に強制処分として法定手続が保障されるということにはならないと考えられる．そもそも刑事訴訟法197条１項但書の規定に基づく強制処分の意義に関しては，必ずしも一義的な解釈が確立しているわけではないが，その出発点となるのが，「個人の意思を制圧し，身体，住居，財産等に制約を加えて強制的に捜査目的を実現する行為など，特別の根拠規定がなければ許容することが相当でない手段」[85]を用いたものという判例の説示である．この定義に照らす限り，顔認証利用については，意思の制圧という意味でも身体等への制約という意味でも，ただちに強制処分性が肯定されるものではない．また，学説上は，相手方の明示又は黙示の意思に反して，その重要な権利・利益に実質的に介入し，又はこれを制約する処分こそが強制処分であると解する見解（以下，「重要権利制約説」という）[86]が有力になっているが[87]，単発的に顔情報を把握されただけでは，「重要な権利・利益に実質的に介入」されたとは言いがたい．もっとも，顔認証利用の実施の態様によっては，前述の「私的領域への侵入」と認められ，これを強制処分と評価する余地も残されているが，自由剝奪行為に関して言及したのと同様に，かかる評価が困難な場合は少なくない．少なくとも，伝統的な写真撮影と同様に顔認証利用が位置づけられる限り，その強制性分性は基本的に否定されることとなる可能性が高い[88]．そして，顔認証利用が強制処分に該当しない場合，憲法35条１項にいう「捜索」への該当性も認めがたく[89]，法定手続の保障の対象とならないのみならず，令状主義の要請も妥当しないということになり得る．

4．3　立法論的課題に関する考察

以上の考察を通じて，憲法の次元でも法律の次元でも，現在の一般的な解釈論の枠組みの下では，犯罪捜査等との関係における顔認証プライバシーが十分に保護されないこととなる可能性が明らかになった．もとより，私的領域不侵入確保権を保護する憲法上，「私的領域への侵入」に至ると認められる態様（徹底的な「顔追跡」により私生活等の相当部分を明らかにするような態様）で行われる顔認証利用については，当人のプライバシーを侵害し得るものとして，正当な理由及び適正な手続によらない限り許容されるものではないということに異論を挟む余地は乏しい．ところが，かかる顔認証利用は，実際には，プライバシ

ーの侵害と評価されないこととなる可能性を秘めている．その背景には，顔認証利用の「装い」が，既に大衆にオープンとなっている単純な顔情報の収集にすぎないといったイメージを色濃くしているということがある．誰しも容易にアクセス可能なオープンな情報であれば，たとえそれが個人情報であっても「プライバシーの合理的な期待」を認めることが一般に困難となり得る．これらを踏まえると，顔認証プライバシーの法的保護が不十分となる可能性を穴埋めするような（適切な保護のための指針が示される形での）積極的な立法政策が求められるように思われる．その立法政策においては，前節で整理した米国憲法上の議論も踏まえ，特に以下の各点に留意することが重要となろう．

第一に，顔認証利用は伝統的な写真撮影やカメラ監視と同視されがちであるが，米国の議論からも示唆されるように，基本的に異質なものと位置づけられる．なぜなら，当該写真撮影やカメラ監視は一般に顔特徴データの抽出による人物像の詳細な分析等を伴わないことが多いのに対し，顔認証利用は，その実施の態様によっては，他の私的情報やデータベースとの照合等により，個人の私生活の様相等を相当程度「追跡」する機能を伴い得るからである．かかる「追跡」を通じて行動パターン等が把握されれば，当人の性格や嗜好等も推定され得る[90]．換言すれば，顔認証利用は，他の私的情報等との紐づけ等を通じて，当人のプライバシーに対する重大な脅威となり得る[91]．同時に，「顔観察」が表現，集会，結社等の活動への参加者に及べば，表現の自由や集会・結社の自由に対する萎縮効果等をも与え得る[92]．これは，顔認証利用が，顔認証プライバシーのみならず，憲法21条１項の規定に基づき手厚く保護される権利をも脅かし得るということを意味する．特に，内輪限りの表現や交流等の活動を指向した結社においては，その構成員に対して行われる「顔観察」が（結社それ自体に対する萎縮効果や結社のプライバシーとの関係において）相当の脅威となろう[93]．

それゆえ，もっぱら「みだりに容ぼう・姿態を撮影されない自由」等の保障の一環として顔認証プライバシーの保護のあり方を考えることは，正鵠を射たアプローチではない．公権力のカメラ監視に関する運用条件を整備するための立法の提案は民間団体等において過去に行われているが[94]，顔認証利用に関しては，伝統的なカメラ監視以上に，（既に整備されている個人情報保護法制上の一般的な規律を超えた形での）立法を通じた運用条件の具体化・明確化が急務となっているように思われる．とりわけ，犯罪捜査等において許容される（又は許容されない）顔認証利用の具体的な態様の特定等，一定の制度的な歯止めの設営のほか，顔情報の収集・取得の段階での利用目的の明示，当該目的に照らして不要となったと認められる顔特徴データの消去・廃棄，必要な顔情報の保存期間や消去の条件[95]，利用されるソフトウェア等の正確性に関する一定の水準の確保等を義務づけ又は規定するための個別法が求められよう[96]．

第二に，米国の学説が指摘する顔認証利用のためのソフトウェア等の問題も含め，顔認証利用は公権力と私人との連携を通じて行われ得ることから，その連携に関わる私人の行為に対する規律が求められ得る．すなわち，公権力による直接的な顔情報の収集を通じた顔認証利用のみならず，関係事業者等の私人との提携による顔情報の取得・利用についても，立法を通じた運用条件の明確化が必要となり得る．特に，捜査関係事項照会（刑事訴訟法197条２項）に基づく関係事業者から捜査機関への顔情報の提供は，実務上，当人の同意を得ずに行われ得るが[97]，当該提供のあり方については，法律の次元で一定の基準等が設けられること（ないし提供が制限される場合が特定されること）が望ましいと考えられる．

第三に，米国の学説が顔認証利用におけるデータベース化の脅威を指摘していることを踏まえ，当該データベース化のあり方に関する規律について検討することが求められよう．実際，我が国の犯罪捜査等では顔情報データベースの利用が行われているが，かかるデータベースの運用（データ

ベース内の情報の管理等を含む）のあり方に関しては，前述のとおり，個人情報保護法上設けられている一定の規律（個人情報ファイル簿の作成等）が犯罪捜査等には適用除外となるなど，必ずしも十分なものとは言えないように思われる．このような規律の欠缺ないし不足については，指掌紋やDNA型情報のデータベースが作成され始めた当時においては，特に学説の批判の対象となってきた[98]．顔情報データベースそれ自体が，他のデータベース等との照合等の可能性を踏まえ，実質的に多様な私的情報の集約体と言い得る中で，それに対する不用意なアクセスが「私的領域への侵入」となる余地が残されている[99]．そこで，憲法31条の趣旨を踏まえ，かかるアクセスを抑止することを含めた顔情報データベースの利用のあり方に関する手続的規律が立法により明確化されることが求められるように思われる．

第四に，我が国では憲法上のプライバシーの保護に関して米国流のモザイク理論の思想が必ずしも広く受容されておらず[100]，法理論としての未成熟性[101]を有する当該思想をそのまま導入することは妥当ではないが，その基本的な趣旨を立法において加味することが求められよう．特に，犯罪捜査等における顔認証利用の限界に関して，①顔情報の蓄積の度合いや他の私的情報との照合可能性等に応じて私生活等の様相の相当部分が把握され得ると認められる水準を客観的かつ的確に判定する枠組み[102]，②当該水準で行われる顔認証利用は「私的領域への侵入」に該当し得るものとして適正な手続[103]によらない限り違法となる旨，を立法上明示することなどが考えられる[104]．

5．結　　論

公権力による顔認証利用は，その実施の態様によっては「私的領域への侵入」（憲法35条1項に反するもの）に該当する可能性がある．それにもかかわらず，現行法上，一般的な解釈論の枠組みに照らす限り，各人の顔認証プライバシーは必ずしも十分な保護を受けるものとはなっていない．最高裁判所の判例上も，公権力による写真撮影等が問題となった事案はあるものの，顔認証利用のあり方がプライバシーの保護の文脈で正面から問われたものはない．

そのような状況の中で，犯罪捜査等における顔認証利用は拡大傾向にあり，被疑者の特定等，捜査活動の最適化に資する一面を有する．反面，かかる顔認証利用については，①一定のソフトウェアの利用やデータベースとの照合等によりプライバシー等に対する脅威を増している，②一般に格別の法律の規定に基づくことなく実施されている，③表現の自由や結社の自由等に対する萎縮効果をもたらし得る，④たとえ実施の態様が「私的領域への侵入」等により基本権の侵害となる場合であっても（顔認証利用の実態が一般に不透明であることも手伝って）それが見えにくい，といった憲法規範に非親和的な要素を内在させている．それゆえ，立法政策上，顔認証プライバシーの保護を実体面・手続面の双方において明確化及び強化するための規律が求められる．

その具体的な立法に際しては，犯罪捜査等における顔認証利用が許容され得る場合を限定的に明示することが求められるように思われる．そのうえで，米国の議論に見られるモザイク理論的な考え方を踏まえることが必要となろう．例えば，顔認証利用が，顔情報の蓄積の度合いや他の私的情報との照合等の可能性に照らして個人の私生活等の相当部分に踏み込むと認められる程度を客観的に判定するための基準を設けつつ，当該程度に達すると認められる場合には，強制処分としての適正な手続を確保するとともに，憲法35条1項が保護する「私的領域」への「侵入」に該当し得るものとして，当該手続によらなければ違法となる旨を明示することが考えられる．このような形で顔認証利用の実施条件や限界が法律上明確化されることは，各人の顔認証プライバシーの保護のみならず，実務上の適切な顔認証利用を促進するうえでも不可欠となろう．

注

1）　個人情報保護委員会の検討会では，顔に関する

情報を電子計算機用に変換した個人識別符号を指す用語として「顔特徴データ」が用いられているが（個人情報保護委員会（2023：５）），本稿では，同様の意味での「顔特徴データ」という用語を一部に用いつつも，符号化された情報に限らず個人の顔に関する情報を広範に指す用語として，「顔情報」という用語を用いることとする．

2） 個人情報保護委員会の検討会では，カメラにより撮影された者の中から「顔特徴データ」を照合して特定の個人を見つけ出すことを「顔識別」，当人の要請に応じてカメラにより撮影された顔画像から抽出される「顔特徴データ」等を照合して当人の本人確認を行うことを「顔認証」と，それぞれ定義している（個人情報保護委員会（2023：５））．しかし，本稿では，①「顔認証」という用語は広く一般的に用いられていること，②社会通念上，「顔識別」も「顔認証」の一環として捉えられる傾向にあること，にかんがみ，「顔識別」と「顔認証」とを厳密に区別することを避け，両者を包含する概念として「顔認証」を用いることとする．

3） 顔認証技術の意義と特徴について，大阪大学（2019：18–25）参照．

4） 武藤（2021：117）参照．

5） 尾崎（2021：99）参照．

6） 新保（2006：59–60）参照．

7） 先行研究の例として，水野（2021：100–108）参照．また，政府の検討会における議論として，個人情報保護委員会（2023）参照．ただし，当該議論は，公権力による顔認証利用ではなく，「犯罪予防」等を念頭に個人情報取扱事業者が個人情報としての顔画像や顔特徴データを取り扱う場合を中心に取りまとめられている．

8） 武藤（2021：118）参照．

9） U.S. CONST. amend. IV.

10） 米国の行政実務上の概況等について，尾崎（2020：32–37）参照．生体情報の利用に関して，石井（2010：312–326）参照．

11） なお，欧州に関しては，一般データ保護規則（General Data Protection Regulation: GDPR, Regulation (EU) 2016/679）や2026年中の適用開始が見込まれている AI 規則案（*See* European Commission (2021); European Parliament (2023)）等に関する議論が参考になる．特に，AI 規則案では，絶対的に禁止される AI（人工知能）の利用の一類型として，法執行を目的として公的空間でリアルタイムにて遠隔生体識別システムを利用する行為が明示されており，顔認証プライバシーの保護のあり方に与える示唆に富んでいる．しかし，紙幅の都合上，これらの議論については本稿では措く．

12） *See* Ferguson (2021: 1116–1125).

13） これらのほか，顔情報に示される人物が本当に問題となる当人であるか否かを確認する「顔確認」と称し得る態様もある．*See* Cavanaugh (2021: 2449). これは，「顔認証」の一形態ではあるが，公権力の行為が「顔確認」にとどまる限り，本稿が問題とする顔認証プライバシーの問題との関わりがさほど大きくないと考えられるため，本稿では基本的に捨象することとする．

14） 鈴木（2017：566）参照．

15） *See* Arizona v. Gant, 556 U.S. 332, 338 (2009).

16） *See* Katz v. United States, 389 U.S. 347, 361 (Harlan, J., concurring).

17） 物理的な侵入行為を伴わない通話の傍受を（修正４条が禁じる）「不合理な捜索」に該当するものではないとした判例として，以下を参照：Olmstead v. United States, 277 U.S. 438 (1928). また，無線受信装置を所持しながら被疑者の同意を得て潜入した一般私人を通じた会話の傍受に関する「捜索」への該当性を否定した判例として，以下を参照：On Lee v. United States, 343 U.S. 747 (1952).

18） 顔情報に対するプライバシーの合理的な期待を否定した判例として，以下を参照：United States v. Dionisio, 410 U.S. 1, 14 (1973).

19） *See Katz*, 389 U.S. at 350–351.

20） United States v. Jones, 565 U.S. 400 (2012).

21） *See id.* at 404.

22） *See id.* at 408.

23） Riley v. California, 573. U.S. 373 (2014).

24） S*ee id.* at 403.

25） *See id.* at 400–401.

26） Carpenter v. United States, 138 S. Ct. 2206 (2018).

27） *See id.* at 2220, 2223.

28） その詳細について，海野（2021：20–21）参照．

29） *See Carpenter*, 138 S. Ct. at 2220.

30） *See* Ferguson (2021: 1142–1143).

31） *See id.* at 1147–1148.

32）*See* Patel v. Facebook, Inc., 932 F.3d 1264, 1273 (2019). ただし，この裁判例については，SNS のタグ付け機能が問題となったものであり，修正 4 条の適用が直接問題となったものではない．そこでは，顔情報のテンプレートが作成された途端に，当人が SNS 等にアップロードした何百枚もの画像等の顔情報と結びつけられ，当人の私生活等の様相を筒抜けにし得るという旨が説かれている．

33）*See In re* The Search of a Residence in Oakland, 354 F. Supp. 3 d 1010, 1016 (N.D. Cal. 2019).

34）その詳細について，海野（2021：108）参照．

35）*See Jones*, 565 U.S. at 412–413.

36）*See* Rubin (2021: 76).

37）*See* Henderson (2016: 935).

38）*See* Sung (2020: 8).

39）*See* Doktor (2021: 568–571, 573).

40）*See* Ferguson (2021: 1152, 1164). *See also* Cavanaugh (2021: 2477).

41）*See* Ferguson (2021: 1128).

42）*See id*. at 1152, 1196–1197.

43）*See id*. at 1147.

44）*See id*. at 1146.

45）*See id*. at 1155.

46）*See* Cavanaugh (2021: 2481–2482).

47）*See* Doktor (2021: 573).

48）*See* Goldberg (2021: 280–281).

49）*See* Chun (2020: 114–115).

50）*See* Goldberg (2021: 269–272, 289, 294).

51）佐藤（2008：490・500），佐藤（2020：203）参照．

52）佐藤（2008：490）参照．

53）自己情報コントロール権説の問題点を整理した管見として，海野（2021：47–56）参照．

54）曽我部（2018：77），曽我部＝山本（2020：131–132・135）〔曽我部発言〕，曽我部（2022：10–12），音無（2021：223），音無（2022：83–85）参照．また，「自己情報の適正な取扱いを受ける権利」と「自己情報コントロール権」との対立点の整理として，小川（2022）55–56頁参照．

55）しかも，たとえ憲法13条の規定から「自己情報の適正な取扱いを受ける権利」が導かれるとしても，それを憲法上のプライバシーの核心と捉える考え方には疑問を挟む余地がある．なぜなら，憲法13条に基づく幸福追求権（包括的基本権）は他の個別の基本権に対して補充的に適用されると解するのが通説である中で（佐藤（2008：294），佐藤（2020：196–197）参照），プライバシーの保護の趣旨を色濃く内包する憲法35条 1 項に基づく基本権の内実等を十分に検討することなくして，憲法13条に基づく権利を憲法上のプライバシーの核心と捉えることは必ずしも合理的ではないからである．海野（2021：64）参照．なお，「自己情報の適正な取扱いを受ける権利」を説く学説の立場からは，憲法35条 1 項の規定に関しては，刑事責任の追及のための情報の収集・取得からの防御を定めたものであるがゆえに，「部分的なプライバシー権」を保障したにすぎないものという旨が説かれている．音無（2021：218–219）参照．しかし，通常の行政手続（非刑事手続）においても各人のプライバシーや私有財産に対する利益が害される可能性があることにかんがみれば，同条項に基づき保障される権利は刑事責任の追及の局面のみに妥当するものではないと解される．その詳細及び令状主義の要請との関係について，海野（2021：137, 139–147, 171–172）参照．判例も，憲法35条 1 項の要請が非刑事手続にも及び得るという旨を示している．最判昭和47年11月22日刑集26巻 9 号554頁，最大判平成 4 年 7 月 1 日民集46巻 5 号437頁，最判平成28年12月 9 日刑集70巻 8 号806頁参照．

56）音無（2021：160, 205, 244）参照．

57）最大判昭和44年12月24日刑集23巻12号1625頁．

58）最判平成20年 3 月 6 日民集62巻 3 号665頁．

59）なお，私人間の紛争に関する事案においては，「プライバシーに係る情報」（最判平成15年 9 月12日民集57巻 8 号973頁）や「個人のプライバシーに属する事実をみだりに公表されない利益」（最決平成29年 1 月31日民集71巻 1 号63頁）が法的保護の対象となるということが承認されている．

60）前掲最大判昭和44年12月24日参照．併せて，最判昭和61年 2 月14日刑集40巻 1 号48頁参照．街頭でのカメラ監視に関して，東京高判昭和63年 4 月 1 日判時1278号152頁参照．

61）最決平成20年 4 月15日刑集62巻 5 号1398頁参照．

62）なお，判例のいう憲法13条に基づく「私生活上の自由」に関しては，公権力による私生活領域への不当な介入を抑制するとともに，私的情報の取扱いが不適切に行われないことを客観法的に要請するものと考えられ，その裏返しとして保障される主観的権利については，消極的な保障にとどまると解される．それゆえ，憲法13条から導かれる「私生活上の自由」は，公権力の行使を統制する

一般原則としての意味合いが強く，これを憲法上のプライバシーの核心的な根拠と捉えることには疑問が残る．海野（2021：62–63）参照．

63） 最大判平成29年 3 月15日刑集71巻 3 号13頁．これを踏まえ，憲法35条 1 項の規定から導かれる私的領域不侵入確保権を憲法上保護されるプライバシーの基軸として捉える管見として，海野（2021：164–168）参照．

64） もっとも，判例（前掲最大判平成29年 3 月15日）は，車両へのGPS受信機器の装着を一次的な「私的領域への侵入」の肯定要素としているようにも見受けられる．しかし，装着という行為自体は物理的な侵入行為の度合いとしては軽く，ただちに「侵入」を肯定する要素とはなりにくい．しかも，これはプライバシーの侵害を可能とする機器の装着を「私的領域への侵入」と捉えたものであり，装着という物理的な侵入行為の前提として，個人の行動の継続的・網羅的な把握を通じたプライバシーの侵害の可能性を視野に入れたものと考えられる．

65） 判例自身も，顔情報の把握という意味で一定の共通性を有する公道上での写真撮影等とGPS捜査を通じた位置情報の把握との相違を明示している．前掲最大判平成29年 3 月15日参照．

66） 最決昭和55年10月23日刑集34巻 5 号300頁参照．

67） 尾崎（2020：39）参照．

68） 土井（2020：157）参照．

69） 土井（2020：180–181），杉原（1981：105–106）参照．

70） 土井（2020：150）．

71） 憲法31条の文言上は「その他の刑罰」となっているが，科刑以外の局面における自由剝奪行為についても，ここでいう「刑罰」に含まれるものと解する余地がある．

72） その詳細について，海野（2021：81–82）参照．

73） 最判昭和37年11月28日刑集16巻11号1577頁参照．

74） 前掲最大判平成 4 年 7 月 1 日参照．

75） 海野（2021：83）参照．なお，基本権とは，実定憲法上の権利のことを指す．また，基本権法益とは，（私人間でも問題となり得る）基本権に関する法益ないし基本権に内在する法益のことを指す．

76） その詳細について，海野（2021：168–171, 185, 346–347）参照．併せて，注55参照．

77） なお，刑事訴訟法218条 3 項は，身体の拘束を受けている被疑者について，裸にしない限り令状なく写真撮影ができるという旨を定めている．

78） 水野（2021：103）参照．

79） 例えば，野村（2020：17）参照．

80） 個人情報保護委員会「関係法令」等資料内：総務省行政管理局「解説 行政機関等個人情報保護法」，https://www.ppc.go.jp/files/pdf/260207siryo1-5.pdf（2024年 1 月 3 日最終閲覧）．併せて，大阪高判令和 3 年 4 月 8 日判タ1484号66頁参照．

81） なお，電子計算機の用に供するために符号化されておらず，そのままでは可読できない顔画像は個人識別符号に該当しない．

82） 松村（2020：252）参照．

83） 例えば，個人情報保護法62条に反して，行政機関等が当人の個人情報（顔情報）を取得するに当たってその利用目的を明示していなかったとしても，そのこと自体は個人の私生活等の様相の把握に直接結びつくものではなく，よって憲法35条 1 項が禁ずる「私的領域への侵入」に該当するとは認めがたいことから，憲法上のプライバシーの侵害となるものではないと解される．

84） 「自己情報」の収集，利用，開示等の各局面を広く包含する自己情報コントロール権説の立場からは，情報の開示・訂正・利用停止に関する積極的権利についても憲法上のプライバシーの権利の一環として捉えられることとなろう．また，「自己情報の適正な取扱いを求める権利」を説く立場からも，当該権利は個々の局面における自己情報の取扱いの適正さを担保するための措置が講じられることをその保護範囲とするという旨が説かれていることから（音無（2022：84）参照．併せて，曽我部（2022：22）参照），同様の帰結となろう．しかし，憲法35条 1 項に基づく私的領域不侵入確保権に関しては，防御権的性質が強く，これらの積極的権利の保護までをも当然に含むものとは解しがたい．また，公権力の行使を統制する一般原則として機能し得る憲法13条の規定（注62参照）についても，公権力による私的情報の取扱いの適正性を確保する観点から，立法を通じた当該積極的権利の創設のあり方を検討するための指針を与え得るものにすぎず，それらの権利を直接保障するものではないと考えられる． 海野（2021：197）参照．したがって，情報の開示・訂正・利用停止に関する積極的権利については，基本的に，憲法上保護されるプライバシーの問題とはやや異

質なものとして位置づけられよう．なお，これらの積極的権利に関する法律上の規定に関しては，刑事事件に関する裁判や司法警察職員が行う処分の執行等に係る保有個人情報については適用されないこととなっている（個人情報保護法124条１項参照）．

85） 最決昭和51年３月16日刑集30巻２号187頁参照．

86） 井上（2014：12）参照．

87） 強制処分の概念をめぐるその他の主な見解として，田宮（1996：72），斎藤（2015：26），稲谷（2017：281-282）参照．

88） 街頭での写真撮影については，重要権利制約説の立場からは，住居内での写真撮影との比較において，プライバシー等を害する度合いの弱さに照らし，強制処分性を有しないものと捉えられてきた．井上（2014：14-15）参照．

89） 有力な学説上，強制処分への該当性は「捜索」への該当性とおおむね互換的に捉えられている．井上（2014：25）参照．併せて，海野（2021：86-87）参照．

90） 水野（2021：104）参照．

91） 尾崎（2020：40）参照．

92） 尾崎（2020：38・45）参照．DNA 型情報に関して同様の点を指摘するものとして，山本（2008：294）参照．

93） このような「内向的表出型の結社」の場合にはプライバシーの保護の必要性が特に高まるという旨の指摘として，海野（2021：241）参照．

94） 日本弁護士連合会（2012）参照．

95） 水野（2021：107）参照．

96） 米国の学説においては，修正４条との関係や修正１条（U.S. CONST. amend. I.）の保護する自由に対する萎縮効果に照らし，（対象者を特定しない）包括的な顔認証利用は原則として禁止されるべきであるという議論もある．*See* Ferguson (2021: 1197-1198). しかし，少なくとも我が国では，憲法13条が「公共の福祉」の確保を要請し，憲法35条１項に基づく捜索等が（必ずしもその合理性を厳密に問わず）適正な手続の下で行われることが予定されていることにかんがみ，捜査活動等の最適化を図る観点も踏まえ，顔認証利用を原則として禁止する立法は行き過ぎであるように思われる．むしろ，顔認証利用が正当に実施され得る場合の特定とその実施手続に関する適切な立法が重要となろう．

97） 岡田＝北山（2020：54）参照．

98） 石井（2010：109・111）参照．併せて，山本（2008：298-299）参照．

99） 学説上は，警察による個人情報のデータベース化を強制処分と捉える見解も提示されている．山本（2017：252）参照．傾聴すべき見解であるが，顔情報のデータベース化それ自体が強制処分なのではなく，当該データベース化を介して顔情報が他の私的情報と結合し，当人の私生活等の相当部分を明らかにする可能性が生じる状態に至ることが，当人の権利・利益を著しく制約するものとして，強制処分に該当し得る（ひいては憲法上の「捜索」として「私的領域への侵入」となり得る）と解することが妥当であるように思われる．

100） もっとも，個人情報保護法上の「個人情報」の定義（特に，特定の個人を識別可能な情報の範囲に関して，「他の情報と容易に照合すること」ができ，それにより識別可能となるものを含めている点．個人情報保護法２条１項参照）については，モザイク理論的なアプローチが反映されている．

101） その詳細について，海野（2021：117-122）参照．

102） 例えば，他の私的情報との照合を通じて当人の日常生活における主要な行動パターン等を推知ないし特定可能と認められる場合には，私生活等の様相の相当部分を知り得るものと判定され得るであろう．

103） 憲法35条１項に基づく権利の制約を正当化する手続は，令状手続を基本としつつも，もっぱら当該手続に限られるわけではないと解される．この点について，稲谷（2017：286），海野（2021：143-147）参照．それゆえ，ここでいう「適正な手続」に関しては，円滑な顔認証利用の実施を促す観点から，その実施主体が当該利用の範囲及びその「正当な理由」を裁判所に提示し，その許可を得たうえで実施するといった仕組み（令状手続に準じた手続）等についても立法政策上検討の余地があろう．

104） 監視カメラを通じた顔認証利用について，原則として令状手続（検証令状）が必要となると説く学説も提示されている．水野（2021：105）参照．しかし，かかる顔認証利用が常に「私的領域への侵入」に該当するわけではなく，その実施の態様に応じて個人の私生活等の相当部分を把握可能と

認められる水準のものに限り当該侵入が認められると解されることから，かかる水準で実施される顔認証利用のみ，令状手続その他の適正な手続が求められるものと解することが妥当であろう．

参考文献

［邦文文献］

石井夏生利（2010）「生体情報の利用とプライバシー保護」堀部政男編『プライバシー・個人情報保護の新課題』商事法務，pp. 309–335.

石井夏生利（2010）「生体情報のデータベース保存とプライバシー～S and Marper v. United Kingdom 事件を中心に～」『法とコンピュータ』28：105–111.

稲谷龍彦（2017）『刑事手続におけるプライバシー保護――熟議による適正手続の実現を目指して』弘文堂.

井上正仁（2014）『強制捜査と任意捜査〔新版〕』有斐閣.

海野敦史（2021）『情報収集解析社会と基本権』尚学社.

大阪大学（2019）「生体認証技術の動向と活用：科学技術に関する調査プロジェクト」『国立国会図書館調査及び立法考査局調査資料』2018–6.

岡田淳＝北山昇（2020）「顔認証技術を用いた biometric data の利用と公共空間におけるプライバシー（下）」『NBL』1183：52–56.

小川亮（2022）「情報提供に対する同意はなぜ必要なのか」『情報法制研究』11：51–67.

尾崎愛美（2020）「犯罪捜査を目的とした顔認証技術の利用に対する法的規制のあり方――米国の議論を参考に――」『情報ネットワーク・ローレビュー』19：30–46.

尾崎愛美（2021）「米国における顔認証技術をめぐる法制度の現状と今後の方向性――Black Lives Matter 運動・COVID–19緊急事態宣言を受けて――」『杏林社会科学研究』36（4）：81–112.

音無知展（2021）『プライバシー権の再構成――自己情報コントロール権から適正な自己情報の取扱いを受ける権利へ』有斐閣.

音無知展（2022）「判例から見るプライバシー権とその再構成」『憲法研究』10：73–86.

個人情報保護委員会（2023）「犯罪予防や安全確保のためのカメラ画像利用に関する有識者検討会報告書（2023年３月）」

斎藤司（2015）「強制処分概念と任意捜査の限界に関する再検討： 強制処分法定主義と議会の『自己決定義務』」川崎英明＝白取祐司編『刑事訴訟法理論の探求』日本評論社，pp. 19–33.

佐藤幸治（2008）『現代国家と人権』有斐閣.

佐藤幸治（2020）『日本国憲法論〔第２版〕』成文堂.

新保史生（2006）「個人情報保護法に基づくバイオメトリクスの利用」『情報メディア研究』4（1）：55–76.

杉原泰雄（1981）「適法手続――憲法31条論――」芦部信喜編『憲法Ⅲ 人権（2）』有斐閣，pp. 86–126.

鈴木武志（2017）「動画顔認証を中心とした生体認証技術：現状と，安全・安心な社会の実現に向けて」『情報管理』60（8）：564–573.

曽我部真裕（2018）「自己情報コントロールは基本権か？」『憲法研究』3：71–78.

曽我部真裕＝山本龍彦（2020）「誌上対談：自己情報コントロール権をめぐって」『情報法制研究』7：128–140.

曽我部真裕（2022）「憲法上のプライバシー権の構造について」毛利透編『講座 立憲主義と憲法学〈第３巻〉人権Ⅱ』信山社，pp. 7–35.

田宮裕（1996）『刑事訴訟法〔新版〕』有斐閣.

土井真一（2020）「第31条」長谷部恭男編『注釈 日本国憲法（3）』有斐閣，pp. 149–294.

日本弁護士連合会（2012）「監視カメラに対する法的規制に関する意見書（2012年１月19日）」

野村武司（2020）「行政機関個人情報保護――行政情報法は情報公開だけじゃない！」『法学教室』482：15–19.

松村英寿（2020）「AI と個人情報・プライバシー」福岡真之介編『AI の法律』商事法務，pp. 247–303.

水野陽一（2021）「顔認証技術を用いた捜査手法に対する規制方法――EU，ドイツにおける議論を参考に――」『北九州市立大学法政論集』49（1/2）：85–108.

武藤糾明（2021）「実装される監視社会ツール」『世界』943：115–126.

山本龍彦（2008）『遺伝情報の法理論――憲法的視座の構築と応用』尚学社.

山本龍彦（2017）『プライバシーの権利を考える』信山社.

［英文文献］

Matthew E. Cavanaugh (2021), *Somebody's Tracking Me: Applying Use Restrictions to Facial Recognition Tracking*, 105 Minn. L. Rev. 2443.

Sarah Chun (2020), *Facial Recognition Technology: A Call for the Creation of a Framework Combining Government Regulation and a Commitment to Corporate Responsibility*, 21 N.C. J.L. & Tech. 99.

Matthew Doktor (2021), *Facial Recognition and the Fourth*

Amendment in the Wake of Carpenter v. United States, 89 U. Cin. L. Rev. 552.

European Commission (2021), *Proposal for a regulation of the European Parliament and of the Council: Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, {SEC(2021) 167 final} – {SWD(2021) 84 final} – {SWD(2021) 85 final}.

European Parliament (2023), P9_TA(2023)0236, *Artificial Intelligence Act: Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* (COM(2021) 0206 – C9–0146/2021 – 2021/0106(COD)).

Andrew Guthrie Ferguson (2021), *Facial Recognition and the Fourth Amendment,* 105 Minn. L. Rev. 1105.

Rebecca Darin Goldberg (2021), *You Can See My Face, Why Can't I? Facial Recognition and Brady*, 5 HRLR ONLINE 263.

Stephen E. Henderson (2016), *Fourth Amendment Time Machines*, 18 U. Pa. J. Const. L. 933.

Ari B. Rubin (2021), *A Facial Challenge: Facial Recognition Technology and the Carpenter Doctrine*, 27 Rich. J.L. & Tech. 1.

Ye-Eun Sung (2020), *The Case for the Use of Facial Recognition Technology*, 2020 B.C. Intell. Prop. & Tech. F. 1.