

信託セミナー

個人情報保護法制等について

個人情報保護委員会事務局法制室企画官 大 星 光 弘



— 目 次 —

はじめに

1. 個人情報保護法について

- (1) 個人情報保護委員会
- (2) 民間部門における主な規律
- (3) 「個人情報」とは
- (4) 「個人識別符号」とは
- (5) 「個人関連情報」とは
- (6) 「要配慮個人情報」とは
- (7) 「個人データ」「保有個人データ」とは
- (8) 「個人情報取扱事業者」とは
- (9) 事業者が守るべきルール

(10) 個人情報保護委員会へのご相談

2. 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の報告書案について

- (1) 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
- (2) 報告書の背景等
- (3) 肖像権・プライバシーに関する留意点
- (4) 顔識別機能付きカメラシステムを利用する際の個人情報保護法上の留意点
- (5) 事業者の自主的な取組として考えられる事項

はじめに

個人情報保護委員会事務局の大星と申します。本日は貴重な場をいただき、誠にありがとうございます。90分という長い時間になりますが、皆さんリラックスして聞いていただければ幸いです。

それでは、個人情報保護法等についてご説明します。今回、ご説明する内容は二つあります。一つ目は個人情報保護法について、ポイントとなるところをご説明したいと思っています。

二つ目に「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の報告書案」と記載しています。駅や空港などを中心に顔識別機能が付いたカメラシステムの導入が広がりつつある中、どういった点に気を付けないといけないのかをまとめましたので、ご参考に聞いていただければと思います。

私自身は、個人情報の中で企業からご相談を受ける立場が多くあります。例えば多くの金融機関でも、ここ数年、銀行の規制緩和などによって広告業務などに関心を持たれているかと思いますが、そういった相談などを受

け付けているところです。それを踏まえて、本日はご説明します。

1. 個人情報保護法について

(1) 個人情報保護委員会

最初に、個人情報保護委員会についてご説明します。資料「個人情報保護法制等について」（以下「資料」といいます。）の2頁をご覧ください。平成28（2016）年1月1日に個人情報保護委員会として新しく設置されています。それまでは個人情報は総務省において管理されていたのですが、全省庁を統括する立場として、個人情報保護委員会が設置されています。

個人情報については、歴史的に人権の意識が非常に高いヨーロッパを中心に法律などができておりますが、それ以外の国でも高まっています。例えば、海外で個人情報に関する法律が最近施行されたものと、2020年にブラジル、2021年に中国とシンガポール、そして2022年はタイで個人情報保護法が施行されています。グローバル活動をする中で、個人情報の国内法制をしっかりと整えていることが重要になってきているかと思えます。

私どもの所掌事務として一つは、最近よくCMが流れていますが、マイナンバーについて監視、監督を行っています。二つ目が、私どもの中心となる個人情報の保護に関する法律に基づいて、適切な事務、監視、監督業務を行っています。

組織は委員長1名、委員8名となっています。消費者庁や公正取引委員会などを思い浮かべていただきたいのですが、これらの独立性の強い組織と同じ立ち位置で事務を行っています。事務局の定員数は令和2年から伸び

ていまして、個人情報の広がりとともに約1.5倍、現在では195名と人数が増えています。

(2) 民間部門における主な規律

次に、民間部門における主な規律についてご説明します。資料3頁をご覧ください。「個人情報」「個人データ」等に関して、4つのルールが並んでいます。なかなか分かりづらい点があるのですが、一つ目は、個人情報を個人から取得する時にどういったことに気を付けないといけないのかを定めた取得・利用に関するルールです。二つ目は、例えば企業などが個人データを取得した後の保管・管理に関するルールがあります。三つ目に、第三者提供に関するルールがあります。四つ目として、個人の権利や利益の観点からの請求や開示などに対応するルールとなっており、この四つに大きく分けられます。

これに対応して、取得の時は、法律上は「個人情報」という位置づけになっています。個人情報とは生存する個人に関する情報で、特定の個人を識別することができるものです。多くの場合は1人の人、例えば本人などから個人情報や名前などをもらうことになるかと思えます。

企業においては、この1人の人からもらった名前を体系的に構成し、容易に検索できる個人情報にしているかと思うのですが、これが個人情報データベースとなります。要するにデータベース化している状況です。その中の一つを構成するのが「個人データ」であり、この個人情報データベースの中の一部の情報です。

そして、最後に「保有個人データ」という区分がありますが、これは開示、訂正、利用停止、消去等の権限を有する個人データです。

要するに、開示等に応じることのできる権限を有する個人データになります。なぜこれを区別しているかといいますと、例えば委託先は個人情報や個人データベースを持っていますが、開示や訂正などは委託元の権限になります。その場合に委託先では開示等ができませんので、主にそういった時に違いが生じるかと思っています。

(3) 「個人情報」とは

次に、個人情報についてももう少し詳しくお話します。資料4頁をご覧ください。個人情報とは、生存する個人に関する情報であって、多くの方が思い浮かべるのが氏名だと思います。重要なのは、それに紐づいた生年月日その他の記述等により、特定の個人を識別することができるものであるということです。

4頁に例示していますが、山田太郎さんという特定の個人を識別する際、今までは会員登録をする時などに取得する名前が主流だったと思いますが、今後、非常に多くなってくるのが顔写真かと思っています。

皆さんの日常生活においても、例えばスマートフォンやパソコンなどでログインする時に顔認証をすることが増えているかと思います。オフィスによっては、入退館時にゲートで顔認証するところもあります。また、空港や駅などでは、チケットなどを読み込んで通過したり受付窓口での手続きを行ったりしていますが、現在、本人の了承を得た上で、顔画像で顔パスするような実験も試験的に始まっているところです。

今後、AIやロボット、IoTなどの分野が盛んになってくると思いますが、これまで人が行っていた受付がロボットになると必ずカ

メラで人を確認していくことになり、個人情報の中で、顔写真を取得することがかなり増えてくると思います。

他にも住所や生年月日がありますが、これ単体では個人を識別することができないため個人情報には該当しません。しかし、名前と組み合わせることによって、個人情報になります。

(4) 「個人識別符号」とは

資料5頁の「個人識別符号」ですが、これも個人情報です。先ほどの例は名前や顔など分かりやすかったのですが、こちらは身体の特徴などを電子計算機の用に供するために変換した符号であり、電子化された数値などになされたものとなります。

5頁に例示していますが、例えば顔認識データは、先ほどの顔画像と異なり、防犯カメラに映り込んだ場合などが考えられます。今後進んでくるのは、本人かどうかを確認するために、例えば顔の特徴を数値化することです。具体的には目の形や鼻のライン、顔の面積に占める目の大きさやパーツのラインなどを数値化してデータ化されたものが顔認識データになってくると思います。

指紋認識データもスマートフォンで登録などをしておりますが、一時期、キャッシュディスプレイペンサーなどの機械でも指紋の認証などがありました。今後、こういったものもあるかと思っております。

他に分かりやすい個人識別符号は、旅券番号や運転免許証、マイナンバーです。これらには顔写真が付いていますが、個人を特定する番号が付いていますので、こういったものも個人情報になってきます。

(5) 「個人関連情報」とは

次に、資料6頁の「個人関連情報」です。これ自体は個人情報というわけではないのですが、生存する個人に関する情報であって、個人情報、仮名加工情報および匿名加工情報のいずれにも該当しないものをいいます。その他というくりに近いのですが、今は、どちらかという個人関連情報が非常に重要になっています。

個人関連情報とは、個人に関する情報として、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報です。特定の個人を識別することができるものは個人情報で、個人関連情報単体では個人を識別することができないのですが、非常に多く問題になっているのは、一つはCookieです。

アンケート結果などでもCookieを理解している人は少なく、非常に分かりにくいものだと思います。ただし、このCookieを使って広告産業がすごく発展している中で、Cookie自体は個人関連情報になります。これについては後程ご説明します。

ウェブサイトなどで商品を購入する機会が特に増えてきましたが、ある個人の購買履歴やサービスの利用履歴のほか、個人の位置情報の取得も多くなっています。特定の人とは分からないけれども、どこを通過しているか、どの辺を回っているかなどの位置情報も増えてくるかと思います。

資料7頁をご覧ください。Cookie自体も非常に複雑で分類が難しいのですが、簡単に言うと大きく分けて二つあります。

一つ目は「ファーストパーティー Cookie」です。これは、ユーザーがアクセスしているドメイン、ページ、サイトが発行している

Cookieです。例えばユーザーがショッピングサイトにアクセスした時に、そのショッピングサイトがユーザーIDやお買い物情報を保存するために発行するものです。例えば一度ページを見て、また次の日にそのページを見た時に、前回の買い物で入れた商品が買い物かごに入っていることがあります。他にも閲覧履歴でこの商品がおすすめというものが出てくると思いますが、そういった用途に使われています。

二つ目は「サードパーティー Cookie」です。これは複数のドメイン間で共有することができるものです。例えば皆さんがYahooでニュースなどを見ると、広告が掲載されていると思います。例えば飛行機の予約をした会社の広告が流れていることがあるかと思いますが、そのように複数のサイトにまたがってユーザーの興味や行動を収集して、どういった広告がユーザーの興味に合うのかといった場合に使われるものです。

このCookieは、他の情報と容易に照合することにより特定の個人を識別することができる場合には、当該情報とあわせて全体として個人情報に該当することになります。例えば会員情報などです。名前などを入力して会員情報を取っているケースが非常に多くなっていると思いますが、それとCookieが結びついている場合には、全体として個人情報となります。

資料8頁に基づきCookie进行分类します。「そのCookie等は他の情報と容易に照合でき、特定の個人を識別できますか」とありますが、そもそも氏名などと紐づいている場合、そのCookieは個人情報に該当します。これについて第三者提供する場合には、原則、本人同意が必要となります。

また、「その Cookie 等は個人関連情報に該当します」とありますが、要するに氏名などと結びついていない場合です。その場合にも、第三者提供する際には気を付けなければいけません。自社が持っている Cookie は個人関連情報であり、個人情報ではないが、渡す先、第三者において個人の会員情報などと結びつけることができる場合には、第三者による本人同意が必要となっています。個人情報と結びつかない場合には、本人同意は不要です。

なぜこんなに詳しく申し上げているかというと、数年前にA社事件というものがありました。A社で登録されている学生の情報を企業に提供することで、企業側は Cookie の ID と氏名等を結びつけていました。今回の令和2年改正法によって、受取側が Cookie 情報と氏名などと結びつけて個人情報となる場合には本人同意が必要である旨を規定しています。

(6) 「要配慮個人情報」とは

次に、資料10頁の「要配慮個人情報」ですが、慎重に扱う必要がある情報となります。人種や、思想や宗教関係などの情報である信条のほか、社会的身分などもあります。これは少し分かりにくいのですが、非嫡出子などです。それから、今後多くなってくるのが病歴です。100歳まで生きる人が多くなっている中で、いろいろな病気にかかる可能性があります。病歴などは、医療関係も含めて個人情報として多くなっています。また、犯罪の経歴がありますが、後ほどカメラ画像のところでご説明します。その他政令で定めるものとありますが、身体障害などです。長生きするようになり、例えば60歳や70歳になって難病にかかるなどということも増えているか

と思います。

(7) 「個人データ」「保有個人データ」とは

次に、資料11頁の「個人データ」および「保有個人データ」です。なかなか理解が難しいところですが、個人情報を取得した後にデータベース化したものを個人情報データベースと呼びます。この中に含まれるものが、それぞれ個人データとなります。データベースの中から一つを抜き出して提供する場合は、ほとんど個人データになると思ってください。要するに、企業の中では、単なる名刺1枚だと規律がかからないのですが、データベース化している場合には、保管・管理に関するルールなどのさまざまな規律がかかってくることになります。

(8) 「個人情報取扱事業者」とは

資料12頁の「個人情報取扱事業者」ですが、個人情報データベース等を事業の用に供している者をいい、皆さんは個人情報取扱事業者にあたるかと思います。「事業の用に供している」とは、一定の目的をもって反復継続して遂行される同種の行為、社会通念上、事業と認められるものです。これは営利、非営利を問わず、例えばOB会など組織化されているものや、マンション組合なども入ります。

よく勘違いが起こりやすいのですが、一つでも個人情報データベースを扱っていれば、個人情報取扱事業者となります。全ての企業は従業員の個人情報をデータベース化していると思いますが、そうすると個人情報取扱事業者にあたることになり、規律がかかることになります。しばしば、特定の取引先の情報をデータベース化しているので、それについての個人情報取扱事業者と勘違いされる場

合が多いのですが、一つでも個人情報データベースを持っている場合は、全て個人情報取扱事業者になります。

例外は、皆さんもよく想像できるのではないかと思います。放送機関や新聞社などは、報道の用に供する目的などの限定はありますが、個人情報取扱事業者としての規律が緩和されています。他にも、本などの著述のように供する場合や、宗教団体、政治団体も、一部例外となっています。

(9) 事業者が守るべきルール

先ほど四つの柱があると申し上げましたが、最初の段階の「取得・利用」のところで気を付けなければならないことを資料13頁にまとめています。

個人情報を取得する前に、個人情報の利用目的をできる限り特定し、利用目的をあらかじめ公表しておく必要があります。おそらくホームページや利用規約などで公表していることが多いのではないかと思います。

個人情報を取得するときに、利用目的をあらかじめ公表していない場合は、本人に通知または公表し、書面での取得の場合は、利用目的を本人に明示しないといけません。これは電磁的記録による時も同じですが、利用目的を本人に明示することが必要となります。先ほど申し上げた要配慮個人情報を取得する場合は、原則、本人の同意を得ることが必要となっています。また、偽りその他の不正の手段による取得はしないとありますが、後述のカメラの小型化が進む中で、カメラが撮影中であるのか分からない状態になっている場合が多くなっています。その場合にきちんと撮影中と掲げれば違反にならないので注意が必要かと思います。

次に、個人情報を利用するときには、利用目的の範囲内で利用し、利用目的の範囲を超える場合は本人の同意を得る必要があります。

関連性があると合理的に認められる場合に限り、利用目的を変更することもできますが、その際は、変更された利用目的を本人に通知または公表する必要があります。

また、違法または不正な行為を助長、誘発するおそれがある方法による利用はしないとありますが、これは、最近の例でいうと破産者マップ（裁判決定で明らかになった破産者の情報を集めてグーグルマップの位置情報でフラグを立て、そのフラグをクリックすると個人名などが出てくるもの）があり、個人情報保護委員会などでも法律に違反するものとして追及しているところです。個人名が書いてあって、その個人名を消したければ、暗号資産などでお金を数万円払わないといけない仕組みになっています。国内なのか海外なのか主体を特定することが非常に難しいのですが、そういった問題も今起きています。

次に、資料14頁の個人データを「保管・管理」するときですが、企業にとっては、個人情報をデータベース化している場合です。

一つ目に、正確で最新の内容に保ち、必要がなくなったときはデータを消去するよう努めるとありますが、特に、必要がなくなったときはデータを消去するという努力義務になっている点に気を付けなければならないと思います。

二つ目に、漏えい、滅失又は棄損の防止その他の安全管理措置を講ずるとありますが、例えば、ファイルのパスワードの設定で、もちろん同じパスワードや分かりやすいパスワードは駄目ですが、場合によっては、暗号化

しているものや、アクセスできる人を制限するなどの安全管理措置をきちんと行ってもらうことが必要です。

三つ目に、従業員に対して、必要かつ適切な監督を行うとありますが、今回ご出席の皆さまは法務部などのコンプライアンス部門の方が多くかと思えます。特に、個人情報に対する理解を広めていくにはどうしたら良いかと悩んでいる方も多いかと思えますが、従業員に対して必要かつ適切な監督を行うことも、法律上、義務付けられています。

四つ目は、データの管理や加工などを委託する場合があるかと思えます。その場合は委託先に対して必要かつ適切な監督を行うことが必要となっています。

五つ目および六つ目は、情報漏えいが生じた場合、委員会や本人に対して報告を行うことが必要です。情報漏えいは上半期で約1,600件ありますが、医療系やカード会社などによる情報漏えいが多いです。医療系では薬を間違えて別の人に渡してしまった場合や、カード会社では本人が引っ越したのに元の住所に誤配した場合など、いろいろな状況があります。

資料15頁は、漏えい等報告の義務化です。今回の改正で新しく個人情報保護委員会に報告することが義務となりました。

報告にも二つあり、速報の場合は概ね3～5日以内、確報は30日以内の報告が義務付けられています。もちろん、速報と確報をまとめて行うこともできます。

15頁には報告しなければいけない内容が記載されています。一つ目の要配慮個人情報の漏えいについては、先ほどの病歴など薬局や医療関係で発生することが多いです。二つ目の財産的被害のおそれがある漏えいについて

は、カード番号やクレジットカード情報などが多くあります。そのほか、不正の目的によるおそれがある漏えいや1,000件を超える漏えい等が対象事案となっており、そのおそれがある場合も含めて報告することになっています。

資料16頁は、第三者提供です。金融機関では、今後、業務が増える中で第三者提供が起る場合があるかと思えます。最初の規約の中で、個人情報については誰に提供するのか明記したうえで同意を得ることが多いかと思えます。

第三者提供する場合は、本人の同意を得ることが必要です。本人の同意を得ないでよい場合は限定されており、その一つが法令に基づく場合で、警察や弁護士からの照会です。おそらく警察との関係で、皆さまもこういった経験があるのではないのでしょうか。また、人の生命、身体または財産の保護のためとして、災害が起こった場合など特別な場合に緊急的に行う必要があります。あとは公衆衛生ですが、最近では、新型コロナウイルス感染性が広がった場合などがあると思います。他には国や地方公共団体への協力や、学術研究機関による場合があります。学術研究機関が企業と共同研究を行っている場合がありますが、基礎的な研究部分について必要な場合は第三者提供が認められています。

次に「オプトアウト手続」についてですが、本人がデータの提供の停止を申し込む場合、特別な例外として、オプトアウト制度を設けています。基本的には本人の同意が必要ですが、申し込みによって本人のデータの提供を停止することができます。これはかなり限定的にやっています。

他には、委託、事業の承継、共同利用を行

う場合があります。多いのは共同利用で、グループ会社などが想定されますが、その場合には、本人が容易に知ることができるように、「①共同利用されること、②データ項目、③利用される範囲、④利用目的、⑤責任を有する者」を明示しなければいけないことを頭の中に入れておいていただければと思います。

少し難しくなってきたのが、資料17頁の海外との関係です。先ほどの第三者提供は国内でしたが、グローバル化が進む中で、個人データを外国にある第三者に提供する場合は、外国に送ることについて同意を得る必要があります。

一つ目は、本人の同意がある場合です。送り先の所在国の名称や、当該外国における個人情報の保護に関する制度の内容、移転先(第三者の事業者)が講ずる個人情報保護のための措置を、本人に対して情報提供しなければなりません。

二つ目は、基準に適合する体制を整備した事業者であることです。日本の個人情報保護法と同様の体制をとっている場合は、本人の同意が不要です。その場合、国内の事業者は、海外の事業者がきちんと対応していることを定期的に確認することや、外国の会社に問題が生じた場合にきちんと対応することが必要になります。こういった情報について、本人の求めに応じて提供することになっています。

三つ目は、我が国と同等の水準国(EU、英国)であることです。

これらについて気を付けなければいけないのが、あくまでも外国に送る場合の同意なので、外国に送る場合はこの三つのどれかを満たす必要があります。

最後は、資料18頁の「公表事項・開示等請

求」です。個人情報保護法は基本的に国が事業者を規律する内容になっていますが、公表事項および開示等請求は個人の権利という観点から規律が設けられています。

一つ目は、公表事項として、どのようなデータがあるのか本人の知り得る状態に置くことが求められています。具体的には、事業者の氏名または名称、住所、法人の代表者名、そして全ての保有個人データの利用目的、請求手続きの方法などです。今回の改正で求められているのが、安全管理のために講じた措置です。また、苦情の申出先や、認定個人情報保護団体に加入している場合は当該団体の名称および苦情申出先を事業者は開示しておく必要があります。

二つ目は、本人から開示を請求された場合には、原則本人に開示します。今回の改正で新たに追加したのは、個人データの授受に関する第三者提供記録です。いつ、誰に対して提供したかということを開示の対象に追加しました。

三つ目は、本人からの請求に応じた対応内容です。まず、内容に誤りがある場合は、訂正、追加、削除をします。利用目的の範囲を超えて利用されている場合や不適正な利用がされている場合、または不正の手段で取得されている場合には、利用停止または消去を求めることができます。同意なく第三者に提供されている場合には、第三者提供の利用を停止または消去します。先ほど、保有個人データを利用する必要がなくなった場合は消去することが努力義務と説明しましたが、利用する必要がなくなった場合や一定の漏えい等事案が生じた場合、または本人の権利もしくは正当な利益が害されるおそれがある場合には、本人の権利利益の侵害を防止するために必要な

限度で、利用停止もしくは消去または第三者提供の停止を行うことができます。

(10) 個人情報保護委員会へのご相談

以上が個人情報保護法制等の内容ですが、資料19頁で個人情報保護委員会へのご相談についてご紹介します。私は「PPC ビジネスサポートデスク」で、新事業における個人情報の取り扱いなど、企業からの個別相談に週に2件ほど対応しています。まずは電話をかけていただき、その後はメール等のやり取りになります。今後、新しい事業を始める中で不明な点などがあれば、ご相談いただければと思います。

2. 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の報告書案について

(1) 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

続いて、「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」の報告書（案）の内容についてご説明します。

金融機関そのものは、カメラ画像とは関係が少し遠いかもしれません。ただ、関係する事業者や取引先などでこういったビジネスが非常に増えてくると思いますので、参考にいただければと思います。

資料20頁をご覧ください。検討会の構成員としては、宍戸座長（東京大学大学院法学政治学研究科教授）をはじめとした先生方をお招きして、令和4年1月から7回開催しています。

顔識別機能付きカメラシステムが駅や空港などで広がりつつありますが、カメラシステ

ムには駅や空港で過去に問題行動を起こした人がカメラ画像に映ります。問題行動とは、例えば駅員を殴った、傷害事件を起こした、あるいは火をつけたなど、パブリックな場所での凶悪な事件が増えていますが、そういった人をデータベースに登録しておきます。

施設の中では、全てが顔識別カメラになっているわけではなく、顔識別カメラは駅や空港などの入口に設置されています。今度、気を付けてみていただければと思いますが、駅や空港、一部の百貨店などでも導入されています。例えば、「渋谷プロジェクト」では、啓文堂書店や、渋谷のスクランブル交差点付近にある大盛堂書店などにより構成されています。

カメラで識別した人を当該施設で過去に問題を起こした人と照合し、もし一致すればアラートが出ます。主要な駅や空港などで導入されているものです。

(2) 報告書の背景等

次に、「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（案）」（以下「報告書」といいます。）をまとめましたので、報告書の内容についてご説明します。カメラ画像について、今後、こういった内容も広まっていくのだと参考に聞いていただければと思います。なお、配布した報告書の黄色のマーカーは、私が引いたものです。

最初は「第1章 本報告書の背景」です。近年、列車内や鉄道駅構内での殺傷事件など、不特定多数の者に危害が及ぶ事件が発生しています。駅や空港などにおける犯罪等に対する要請がより一層高まっているに伴い、犯罪予防や安全確保のために、顔識別機能付

きカメラシステムの利用が広がりつつあります。このようなニュースが広がると、利用者としても不安に思い、導入に賛成する方もいます。ただ、顔識別機能付きカメラシステムは、カメラの中に特定の人物が存在しているか瞬時に自動で把握できることから犯罪予防の観点からは有効なシステムですが、他方で、遠隔で個人を識別することが可能であるという技術特性上、その運用次第では、受忍限度を超える個人のプライバシー侵害等を生じさせるリスクをはらむと思います。

今後のことですが、オリンピックは終わりましたが、2025年に大阪万博があります。海外からもいろいろな人に来てほしいと思っていますが、その中で犯罪が起こらないようにすることが重要であり、顔識別機能付きカメラシステムの導入が進む可能性もあるかと思っています。例えば、ワールドカップ開催国のカタールでは来場者を多数の監視カメラで見るとしていましたが、国際大会においては安全の観点から検討されるかと思っています。

そこで、個人情報保護委員会では、「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」を設置して、本報告書を取りまとめました。

報告書の目次をご覧ください。特徴として三つの柱があります。

第4章では、防犯カメラによる撮影等に関するこれまでの肖像権・プライバシーに関する留意点について整理を行っています。肖像権およびプライバシーは法律で規定されている内容ではなく、裁判上の権利としてよく話題になります。日常生活においてもプライバシーの侵害が話に出てきますが、カメラ画像の観点から気を付ける点を整理しています。

第5章では、個人情報保護法上の留意点を

整理し、第6章では、法律の規制ではありませんが、法律を守っていてもいわゆる炎上など企業への批判が起こる場合があります。炎上しないための事業者の自主的な取組について提言しています。

報告書2頁（本誌174頁）をご覧ください。本報告書の対象範囲は、顔識別機能付きカメラシステムにおいて、顔画像および顔特徴データが用いられる場合を中心にしています。今の防犯カメラで撮影されるとほとんどが顔画像であり、顔識別機能付きカメラシステムを利用すると顔特徴データとなります。これは、先ほど申し上げた、顔の面積の中の目や鼻の大きさ、鼻や口のラインなどの特徴をデータ化したものであり、個人識別符号になるかと思っています。

「(2) 顔識別機能付きカメラを設置する空間的範囲」ですが、今回想定している空間的範囲としては、駅や空港など、不特定多数の者が出入りする大規模な施設が該当します。駅や空港で広がりつつあるのでそのようにお伝えしていますが、例えば、百貨店や大手の総合ディスカウントストアなどでも導入されているとニュースに出ていますので、そういった所にも広がっていくと思います。

「(3) 顔識別機能付きカメラシステムを利用する目的」ですが、犯罪予防や安全確保のために顔識別機能付きカメラシステムを利用する場合を対象としています。脚注7のとおり、商用目的での利用は総務省および経済産業省が取りまとめた「カメラ画像利活用ガイドブック」を参照いただければと思います。

5頁（本誌176頁）の「第2章 用語の定義」ですが、顔特徴データは先ほど申し上げたとおり、「顔の骨格及び皮膚の色並びに目、鼻、口」の位置やラインなどになります。

8頁（本誌177頁）の「第3章 顔識別機能付きカメラシステムについて」です。顔識別機能付きカメラシステムの特徴ですが、12頁（本誌180頁）の「ア 不変性と追跡性」に記載のとおり、顔特徴データは不変性が高いため、長期にわたって特定の個人を追跡することが可能です。また、「イ 自動的、無差別かつ大量の取得」に記載のとおり、撮影範囲に入った全ての人の顔識別をしていくので、無差別かつ大量に取得することができます。それから、「ウ 利用目的の予測困難性」ですが、今まではカメラが設置されていたら防犯カメラだと推測したかと思いますが、今はカメラもさまざまな種類があり、今回のような顔識別を行っているもののほか、広告やデジタルサイネージの一部にもカメラが付いていて、映る人の年齢や性別に合った広告を推測する技術も出てきています。最後に「エ 差別的効果」ですが、アメリカなどで多いです。黒人や白人など肌の色によって検知率が異なり、特に黒人の場合は誤検知が多いようです。特定の人種や肌の色によって検知が曖昧になったりする場合もあるようで、アメリカを中心に問題になっています。

(3) 肖像権・プライバシーに関する留意点

14頁（本誌181頁）の「第4章 肖像権・プライバシーに関する留意点」では、一般の人が分かりにくい肖像権およびプライバシーのことを整理しています。これを記者に話すと「分からないことも多いから整理してもらえると助かる」といった意見がありました。肖像権およびプライバシーで何に気を付けなければいけないのか参考になると思います。

15頁（本誌182頁）をご覧ください。肖像権およびプライバシーの代表的なものが平成

17年11月10日の裁判例です。人の容ぼう等を承諾なく撮影することが不法行為法上違法となるかどうかについては総合考慮によるしつつ、具体的な判断基準を示しました。

15頁（本誌182頁）の②に「人は、みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する」とありますが、不法行為法上違法となるかは、総合的な判断として「被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮」すると考えられています。要するに、絶対的なものではないという相対的な形です。総合考慮して、人格的利益の侵害が、社会生活上、受忍の限度を超えるものといえるかどうかを判断しています。

他にも具体的な裁判例を参考として載せています。22頁（本誌186頁）の④はマンション内にビデオカメラが設置されたことで、マンションを区分所有している人がプライバシーを侵害されたのではないかと撤去を求めた事案です。カメラはエレベーター内、マンション1階の内階段の出入口、1階夜間入口扉付近、1階管理人室のカウンターに設置されたものであること等を指摘したうえで、当該カメラは通常の防犯カメラであって、特定の区分所有者Xの行動を監視するために設置されたものではありません。Xの行動を監視するために設置されたものではないという点ですが、設置の目的の相当性、設置の必要性および設置方法の相当性があるとして、プライバシー侵害を否定しました。

次に、23頁（本誌186頁）の⑤は、原告の自宅近くおよび私道が映っている場合です。道路は、公道であれ私道であれ、人目に触れる空間であるから、一般的には居宅や敷地内

などのようにプライバシー保護の要請が高い空間とは言えませんが、私道部分はいわば家の延長空間として原告らの日常生活に密着した空間であるべきだから、単に道路であることをもって、プライバシーを保護しなくてもよい場所であるとするのは相当ではないということです。家に近い場合は、公道であれ、プライバシー保護に値するという事になっています。

⑥は監視カメラの映像を報道機関に提供した行為が肖像権・プライバシー権を侵害したとして原告が損害賠償を求めたものです。これは店舗における万引きの発生件数や、コンビニにおける犯罪の発生状況等を指摘したうえで、実際に万引きが起きていることなどを考慮しています。撮影の目的が万引きや強盗等の犯罪の発生に対処することであり、人の監視ではないということです。監視カメラが作動していることを知らせることによる犯罪の発生予防であることや、監視カメラが固定されたものであり、特定の顧客を追跡して撮影することはないこと、店舗の内外に10か所程度、監視カメラが作動中である旨の張り紙があり、防犯カメラがあることを周知している点が考慮されています。

このように総合的な考慮という形であり、他にも重要な点に黄色マーカーを付していますので、時間があれば眺めていただければと思います。

第4章は肖像権およびプライバシーについて述べていますが、最近、この報告書が読売新聞などで報道されましたのでご参考までに紹介します。個人情報保護法はこういうプライバシーに弱いものと面白おかしく書かれていたのですが、プライバシーについても踏み込んだことについては評価するというコメン

トがありました。

(4) 顔識別機能付きカメラシステムを利用する際の個人情報保護法上の留意点

30頁（本誌191頁）の「第5章 顔識別機能付きカメラシステムを利用する際の個人情報保護法上の留意点」では、個人情報保護法上の留意点を条文ごとに整理しています。個人情報保護法をはじめ、法律は一般の方にはなかなか分かりにくい点があります。それを分かりやすいとまでは言えないのですが、事業者が導入する際の留意点を報告書としてまとめています。

まず、よく勘違いされやすいのが、防犯カメラの設置場所で映った顔画像や問題発生時の日時や状況、その人の特徴は全体として個人情報に該当します。例えば、2021年9月1日、ドアをこじ開け立入禁止区域に侵入したスーツの40代男性という情報の場合、「男性」とか「スーツ」といった特徴を抜き出して第三者に渡す場合は、おそらくこういった特徴をデータベース化しているため、個人データに該当することがほとんどです。一部分を取り出して提供する場合も個人データの提供として第三者提供に該当することに注意が必要であると述べています。ここは勘違いが多いので、注意書きとして31頁（本誌192頁）にも記載しています。

32頁（本誌193頁）以降も条文ごとに記載していますが、法17条では「利用の目的をできる限り特定しなければならない」とあります。今回の顔識別カメラシステムであれば、防止したい事項や顔識別機能を用いていることを明らかにすることで利用目的の特定を行わなければならないと記載しています。このうち防止したい事項は、少なくとも「犯罪予

防」、「行方不明者の捜索」などとしなければなりません。例示としてテロ防止や万引き防止などの具体的な犯罪行為等の累計を示すことも考えられるとあります。

33頁（本誌194頁）の「利用目的等の通知公表等」については、利用目的を公表しなければいけないのですが、基本的に駅や空港などは自社のホームページで行っている場合が多いかと思います。それに加えて施設内での掲示について、カメラも小型化して一見カメラだと分からないものも増えていますので、利用者への理解を深めるためにも、カメラを設置していることを分かるように掲示することが望ましいと述べています。全てのカメラの設置場所に掲示するように述べているわけではなく、駅や空港などの大規模施設の入口などに代表して置くことが望ましいと述べています。

次は、36頁（本誌195頁）の「不適正利用の防止及び適正取得のための態様」です。不適正な利用をしてはいけないということで先ほど破産者マップの例を申し上げました。例えば防犯カメラもそうですが、その映像に映った人などを面白おかしく SNS に掲載することはもちろん駄目です。特に気を付けないといけないのが、先ほど申し上げたとおり、偽りその他不正の手段により個人情報を取得してはならないということです。最近、小型カメラや電光掲示板等にカメラが内蔵されているものが出てきていて、撮影されていることが非常に分かりづらくなっています。一見して分からないように取得している場合には不正取得に当たる場合もあるので、気を付けていただきたいと思います。

38頁（本誌196頁）の「利用目的の通知公表等の例外」ですが、今回は犯罪予防関係な

ので、出さない場合も多いと思います。特別な事情がある場合には利用目的を公表する義務がないと考え得るかもしれませんが、そういった場合においても慎重な判断をしなければならないことを述べています。

問題になるのが、「要配慮個人情報」です。要配慮個人情報である犯罪の経歴に関して、例えばカメラ画像の中に犯罪行為が映りこむ可能性があります。単に防犯カメラの映像等で犯罪行為が疑われる映像が映ったのみでは、犯罪の経歴や刑事事件に関する手続きが行われたことに該当しないため、要配慮個人情報には該当しないと明確に述べてあります。犯罪が映りこんだ場合は、要配慮個人情報だと誤解する事業者も多いので、それは違うということを明確に述べています。

また、データベースに登録するために要配慮個人情報を取得する場合も、原則としてあらかじめ本人の同意を得なければなりません。例えば、いろいろな鉄道会社がありますが、東京の地下鉄で事件を起こして、別の鉄道会社でまた事件を起こす可能性がある場合に、事件を起こした人を登録することがあるかもしれません。それは確かに要配慮個人情報に当たりますが、例外として、人の生命、身体、または財産の保護のために必要がある場合は、例外として本人の同意を得ないでよいと述べています。

40頁（本誌198頁）の「従来型防犯カメラについての考え方」について、私もこの報告書を検討する際に防犯カメラなどを非常に見るようになりましたが、例えばマンションなどの入口に「防犯カメラ設置中」などを書いてあるかと思います。これまでは防犯カメラは取得の状況から見て防犯目的に使っていることが明らかであったので、通知公表は不要

でした。ただ、不正取得の問題もあるので、防犯カメラが作動中であることを施設等の入口等に掲示するなど、不正取得の観点から、認識可能となっていなければならないと明確にしています。

利用目的の「登録基準」は、利用者の方は非常に気になる点かと思います。どういった人が登録されているのかははっきりしないと、もしかしたら自分も登録されているのではないかと不安になるかと思います。利用目的の達成のために必要最小限の範囲内の情報が登録されるような基準となるよう努めなければならないと明記しています。

少し回りくどい表現ですが、例えば、犯罪行為等の防止を目的とする時は、登録基準の内容は当該犯罪行為等を行う蓋然性が高い者に厳格に限定し、登録時にも当該犯罪行為等を行う蓋然性があることを厳格に判断することが望ましいとあります。これは照合用データベースを導入しているいろいろな企業の方にお聞きしたのですが、かなり厳格に対応しています。特に私たちが知っているような有名な事業者は、ほとんど厳格に対応しています。万引き等においても、その行為が実際に画像に映っている場合のみ登録しています。「多分この人が盗ったのだろう」、「この人が盗っているところはカメラに映っていないが通り過ぎた後に無くなったからこの人だろう」というときは、カメラにはっきり映っていないため登録していないという事業者がほとんどでした。

以上のことを踏まえて、かなり厳格に限定してくださいということを述べています。照合用データベースの登録者数も百人や人の話ではなく、数十人前半ほどであり、かなり厳格に扱っているところが多く、厳しく限定し

ています。

それから、41頁（本誌199頁）の「対応手順」ですが、検知対象者が検知された場合、警備員が飛んでくるのか気になりますが、システムだけではなく、警備員が目視で確認しています。

例えば、顔特徴データ一致率が高い数値でも別人は多くいます。最近はマスクをしている方が多く、誤検知の場合も結構ありますので、目視で確認している事業者がほとんどです。そして警備員がすぐに声を掛けるというわけではなく、遠目から犯罪を犯さないように警戒する対応がほとんどかと思っています。

42頁（本誌199頁）の照合用データベースに登録した情報の「保存期間」ですが、法律では明確に決めていません。情報によって保存期間が違いますので、対象とする犯罪行為の再犯の傾向や、登録対象者が再来訪するまでの一般的に想定される期間等を考慮することが考えられると述べています。

42頁（本誌200頁）の「イ」に「利用目的達成のために利用する必要がないと考えられるため、遅滞なく消去するよう努めなければならない」とありますが、必要がないと思ったらそのままにしておかずに消去することを努力義務ですがしっかりやってくださいと書いています。

44頁（本誌201頁）の「安全管理措置」では五つの措置が義務付けられています。「①組織的安全管理措置」ではシステムを使用できる従業員をきちんと限定すること、「②人的安全管理措置」では従業員に対する適切な研修を行うこと、「③物理的安全管理措置」ではカメラ画像および画像データなどの盗難または紛失等を防止すること、「④技術的安全管理措置」ではシステムへの技術的なアク

セス制御や漏えい防止策をきちんと講ずることなど、安全管理措置をきちんと講じてくださいと述べています。

また、47頁（本誌203頁）の「共同利用」について、特定の者との間で共同して利用される個人データが当該特定の者に提供される場合、一般の方は、自分の顔特徴データが他と共有されているのではないかという心配が起きる可能性があると思います。この場合、共同利用する者の範囲を同一業種内に限定したとしても、全国やある地域全体といった広い範囲で共同利用することが安易に認められるものではないため、なるべく制限的にするべきだと述べています。例えば、外国人の窃盗団による組織的な窃盗などの犯罪が起きていますが、盗難被害にあった商品や、関係ないお店まで共有することはよくないことです。そういったことにも気を付けながら、共同利用する者の範囲を利用目的の達成に照らして真に必要な範囲に限定することが適切だと考えられると述べています。ヒアリングした中では、成田空港や羽田空港などの空港も共有は全くしていませんし、ほとんどのところはかなり厳格に扱っていると思います。

また、48頁（本誌204頁）の「一事業者内での個人データの取り扱い範囲」について、先ほどの説明は他の会社との共同利用でしたが、銀行の支店間でも、共有は真に必要な範囲に限定した利用とすることが適切であると述べています。百貨店でも池袋支店や渋谷支店などがありますが、やはり共有していないという話を聞きます。

それから、保有個人データおよび請求との関係です。犯罪予防関係で、存否が明らかになることで、かえって犯罪が起こる場合があります。その場合、例外として請求などに対

応しなくてもよいことを述べています。例外に当たる場合としては、49頁（本誌205頁）にあるように「当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがある」場合などに該当することが多いかと思います。

開示等の請求は、53頁（本誌206頁）にあるように、原則は応じないといけませんが、内容が内容だけになかなか難しい場面もあるかと思います。ただ、誤登録の場合は丁寧に対応する必要があると思います。

(5) 事業者の自主的な取組として考えられる事項

58頁（本誌211頁）の「第6章 事業者の自主的な取組として考えられる事項」は、法律で義務付けられているものではないですが、炎上しないためにも、実現しようとする内容を明確にして検討し、その内容に照らして必要かつ適切な手段がとられているかどうか確認しましょうということを述べています。

59頁（本誌211頁）の「導入前の影響評価」について、大企業は全ての事業において企業内PIA（Privacy Impact Assessment）をやっているところが多いですが、きちんと事前に確認していくこと、一定期間を設けて試験的实施を行うことが望ましいです。試験的实施の際などに広報することにより、いろいろな議論が出てきますので、被撮影者への十分な説明のほか、様々な広報の手段を活用するとよいかと思います。

60頁（本誌212頁）の「他の事業者との連携」について、地下鉄、私鉄などの鉄道会社がありますが、他の事業者と連携しながら、広報や導入事例の蓄積をしていくことがよいのではないかと述べています。

それから、61頁（本誌213頁）の「導入後の検証」です。不要になった情報がそのままになっていたらいけないので、きちんと内部監査などをしておくことが必要かと思います。

最後に、64頁（本誌215頁）の「顔識別機能付きカメラシステムの検討の観点リスト」で各条文について述べていますが、チェックリストの形式で、こういったことに気を付けなければいけないかをまとめています。導入しようとする事業者にとってはこういったリストがあると助かるという話がありましたので、活用いただくことを期待しています。

また、68頁（本誌217頁）で「施設内での掲示案」なども提示しています。顔識別カメラシステムがどこに設置されているか分から

ないことが多いと思うので、真ん中に写真やイラストなどを入れることで利用者の理解がより広がるのではないかと思います。

以上、カメラ画像の利用について、数年後には広がっていくと思いますので、報告書の内容を導入する事業者に読んでもらうことを期待しています。

私からの説明は以上です。ご清聴ありがとうございました。

本稿は、令和5年1月31日に開催された信託セミナーにおける個人情報保護委員会事務局法制室企画官 大星光弘氏の講演内容を取りまとめたものです。

（おおほし・みつひろ）

〔資料〕



個人情報保護法制等について

令和5年1月
個人情報保護委員会事務局
大星 光弘

本日の説明内容

1. 個人情報保護法について
2. 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の報告書案
3. データマッピング・ツールキット

個人情報保護委員会について①

沿革

➤ 平成28年（2016年）1月1日 個人情報保護委員会 設置

所掌事務

- ①マイナンバー制度に関する事務（監視・監督、特定個人情報保護評価）
- ②個人情報の保護に関する法律（平成15年法律第57号。個人情報保護法）に関する事務、監視・監督（同法を所管）
- ③上記①、②に共通する事務（広報・啓発、国際協力等）

組織

- 委員長1名・委員8名（合計9名）の合議制（行政委員会）
- 委員長・委員は独立して職権を行使（任期5年）
- 委員会事務局の定員数：195名（令和4年度）
[参考] 139名（令和2年度末）、145名（令和3年度）

2

民間部門における主な規律（「個人情報」「個人データ」等@法第4章関係）

【個人情報】

生存する個人に関する情報で、
特定の個人を識別することができるもの
（例：1枚の名刺）

① 取得・利用に関するルール

- ・ 利用目的を特定して、その範囲内で利用する
- ・ 利用目的を通知または公表する。
- ・ 偽りその他不正の手段により個人情報を取得しない。
- ・ 要配慮個人情報の取得は、原則として、あらかじめ本人から同意を得る。
- ・ 違法又は不当な行為を助長し、又は誘発するおそれがある方法により利用しない。
- ・ 苦情等に適切・迅速に対応する。

【個人データ】

個人情報データベース等を構成する
個人情報

→体系的に構成（分類・整理等）され、
容易に検索できる個人情報

（例：名刺管理ソフト内の1枚の名刺）

② 保管・管理に関するルール

- ・ データ内容を正確かつ最新の内容に保つとともに、利用する必要がなくなったときは消去するように努める。
- ・ 漏えい等が生じないよう、安全に管理する。
- ・ 従業員・委託先にも安全管理を徹底する。
- ・ 委員会規則で定める漏えい等が生じたときには、委員会に対して報告を行うとともに、本人への通知を行う。

③ 第三者提供に関するルール

- ・ 第三者に提供する場合は、あらかじめ本人から同意を得る。
- ・ 外国にある第三者に提供する場合は、当該提供について、参考情報を提供した上で、あらかじめ本人から同意を得る。
- ・ 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。

【保有個人データ】

開示、訂正、利用停止、消去等の
権限を有する個人データ

④ 公表事項・開示請求等への対応に関するルール

- ・ 事業者の名称や利用目的、開示等手続などについて事項を公表する。
- ・ 本人から開示等の請求があった場合はこれに対応する。

3

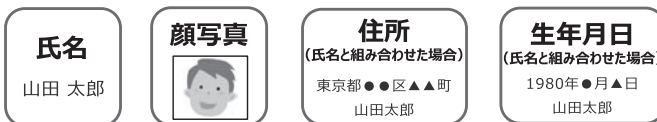
「個人情報」とは（法第2条第1項関係）

○「個人情報」とは、**生存する個人に関する情報**であって、次の各号のいずれかに該当するものをいう。

一 **当該情報に含まれる氏名、生年月日その他の記述等（略）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）**

二 **個人識別符号が含まれるもの**

（例）



4

「個人識別符号」とは（法第2条第2項関係）

○「個人識別符号」は以下①②のいずれかに該当するものであり、政令・規則で個別に指定される。

- ① 身体的特徴等を電子計算機の用に供するために変換した符号
- ② 対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号

○「個人識別符号」に該当するものは、**その情報単体でも個人情報に該当する。**

（参考）個人識別符号に関する政令・規則の内容

- ① 身体の一部の特徴を電子計算機のために変換した符号
→ DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋
- ② サービス利用や書類において対象者ごとに割り振られる符号 ⇒ 公的な番号
→ 旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険者・被保険者番号等

（例）



など

5

「個人関連情報」とは（法第2条第7項関係）

○「個人関連情報」とは、**生存する個人に関する情報**であって、**個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの**をいう。

- **「個人に関する情報」**とは、ある個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表す全ての情報である。
 - 「個人に関する情報」のうち、**氏名、生年月日その他の記述等により特定の個人を識別することができるものは、個人情報に該当**するため、個人関連情報には該当しない。
- また、**統計情報**は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」に該当するものではないため、個人関連情報にも該当しない。

【個人関連情報に該当する事例（※）】

事例1) **Cookie等の端末識別子を通じて収集された、ある個人のウェブサイトの閲覧履歴**

事例2) メールアドレスに結び付いた、ある個人の年齢・性別・家族構成等

事例3) ある個人の商品購買履歴・サービス利用履歴

事例4) ある個人の位置情報

事例5) ある個人の興味・関心を示す情報

6

「Cookie」とは

■ **ファーストパーティーcookie**

ファーストパーティーcookieとは、ユーザーがアクセスしているドメインが発行しているcookie。例えば、ユーザーがショッピングサイトにアクセスしたとき、そのショッピングサイトがユーザーIDやお買い物情報を保存するために発行する。

ファーストパーティーcookieは、そのサイト内でのみユーザーの情報を取得し保存することになる。

■ **サードパーティーcookie**

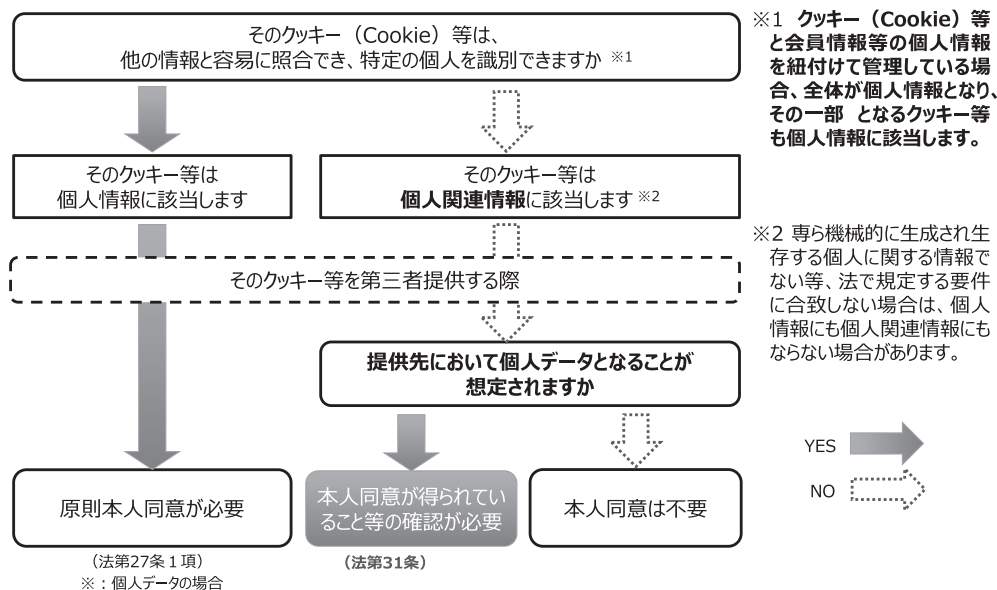
サードパーティーcookieとは、複数のドメイン間で共有することができるもの。複数サイトにまたがってユーザーの興味や行動を収集し、どういった広告がユーザーの興味に合うのかといった場合に使われる。

○他の情報と容易に照合することにより特定の個人を識別することができる場合には、当該情報とあわせて全体として個人情報に該当することになる。

※例えば、会員情報等

7

【参考】クッキー等の第三者提供に係る基本的な考え方（イメージ）

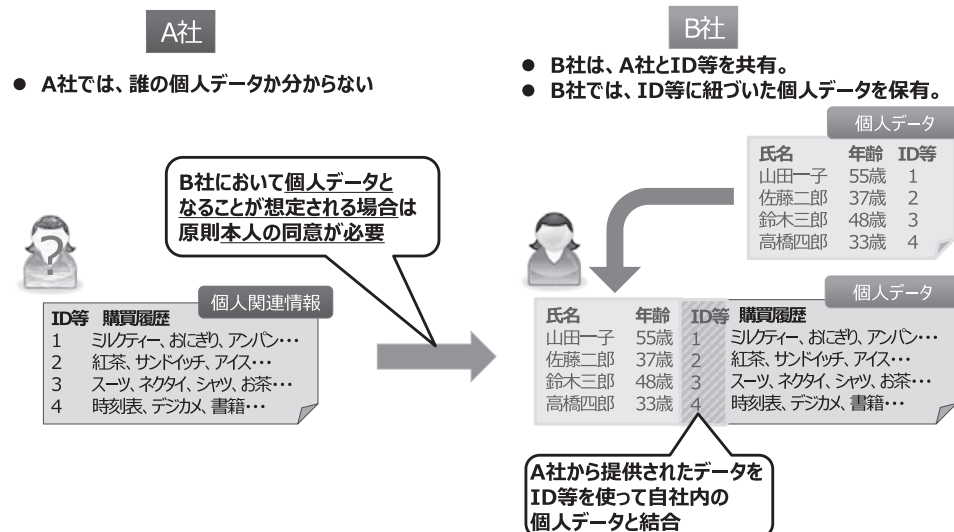


8

個人関連情報の第三者提供規制

R2改正法で新設

- 提供元（A社）では個人データに該当しないが、提供先（B社）において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務付ける。（法第31条）



9

「要配慮個人情報」とは（法第2条第3項関係）

○「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報という。

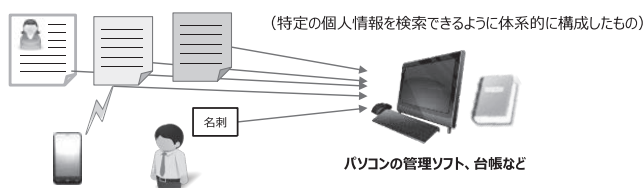
1. **人種**： 人種、世系又は民族的若しくは種族的出身を広く意味する。
2. **信条**： 個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含む。
3. **社会的身分**： ある個人にその境遇として固着して、一生の間、自らの力によって容易にそれから脱し得ないような地位
4. **病歴**： 病気に罹患した経歴
5. **犯罪の経歴**： 前科、すなわち有罪の判決を受けこれが確定した事実
6. **犯罪により害を被った事実**： 犯罪の被害を受けた事実
7. **その他政令で定めるもの**： 施行令・施行令に委任された施行規則で規定
 - ・ 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること
 - ・ 本人に対して医師その他医療に関連する職務に従事する者（以下「医師等」という。）により行われた疾病の予防及び早期発見のための健康診断その他の検査（以下「健康診断等」という。）の結果
 - ・ 健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと
 - ・ 本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと
 - ・ 本人を少年法第3条第1項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと

10

「個人データ」「保有個人データ」とは（法第16条第3項・第4項関係）

○「**個人データ**」とは、**個人情報データベース等**を構成する**個人情報**を言う。

※「**個人情報データベース等**」とは



○「**保有個人データ**」とは、その事業者に**開示等の権限のある個人データ**を言う。

令和2年改正法により、
6ヶ月以内に消去するデータ
（短期保存データ）も、
保有個人データに含まれる。



※ 他の事業者からデータ編集作業のみ委託されて渡された個人データなどは、保有個人データには該当しない

11

「個人情報取扱事業者」とは（法第16条第2項関係）

○個人情報データベース等を事業の用に供している者をいう。

※ 「事業の用に供している」とは

一定の目的をもって反復継続して遂行される同種の行為、社会通念上事業と認められるもの。
営利、非営利を問わない。

- ・ **取り扱っている個人情報が従業者の個人情報のみであっても、個人情報データベース等を事業の用に供している者は、個人情報取扱事業者に該当する（ほぼ個人情報取扱事業者に該当）。**
- ・ 個人情報取扱事業者等のうち、**次に掲げる者が、それぞれ定められた目的で、個人情報等を取り扱う場合は、法第4章の適用除外**とされている。（法第57条）
 - ①放送機関、新聞社、通信社その他の報道機関⇒報道の用に供する目的
 - ②著述を業として行う者⇒著述の用に供する目的
 - ③宗教団体⇒宗教活動の用に供する目的
 - ④政治団体⇒政治活動の用に供する目的

12

事業者が守るべきルール① - 取得・利用

【個人情報を取得する前】

1. 個人情報の利用目的をできる限り特定する。（法第17条①）
2. 利用目的をあらかじめ公表しておく。（法第21条①）

【個人情報を取得するとき】

1. 利用目的をあらかじめ公表していない場合は、本人に通知または公表する。（法第21条①）
書面での取得の場合は、利用目的を本人に明示する。
※例外として、取得の状況からみて利用目的が明らかであると認められる場合（懸賞品の送付など）
2. 要配慮個人情報を取得する場合は、原則本人の同意を得る。（法第20条②）
※例外として、人の生命、身体又は財産の保護のために必要がある場合など
3. 偽りその他の不正の手段による取得はしない。（法第20条①）

【個人情報を利用するとき】

1. 利用目的の範囲内で利用する。（法第18条①）
2. 利用目的の範囲を超える場合は、本人の同意を得る。（法第18条②）
3. 利用目的を変更することもできる。（関連性があると合理的に認められる場合に限り）（法第17条②）
その際は変更された利用目的を本人に通知または公表する。（法第21条③）
4. 違法又は不正な行為を助長・誘発するおそれがある方法による利用はしない。（法第19条）

13

事業者が守るべきルール② - 保管・管理

【個人データを保管・管理するとき】

1. 正確で最新の内容に保ち、必要がなくなったときはデータを消去するよう努める。(法第22条)
2. 漏えい、滅失又は毀損の防止その他の安全管理措置を講ずる。(法第23条)
 ※個人データが漏えい等した場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とする必要があります。
3. 従業員に対して、必要かつ適切な監督を行う。(法第24条)
4. 委託する場合、委託先に対して必要かつ適切な監督を行う。(法第25条)
5. 委員会規則で定める漏えい等が生じたときには、委員会に対して報告を行う。(法第26条①)
6. 委員会規則で定める漏えい等が生じたときには、本人への通知を行う。(法第26条②)

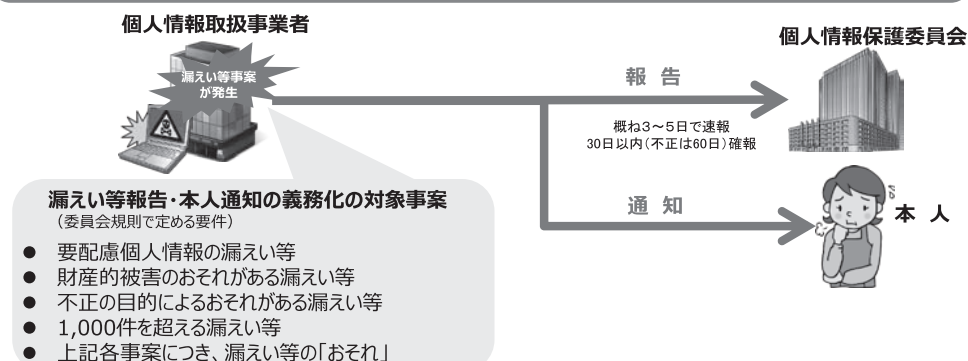
14

事業者が守るべきルール③ - 漏えい等報告等の義務化

- 漏えい等（漏えい、滅失、毀損その他の個人データの安全の確保に係る事態）が発生し、個人の権利利益を害するおそれ大きい場合における、個人情報保護委員会への報告及び本人への通知が、法律上の義務に。

(法第26条①②)

- 従前は、委員会公示に基づく、努力義務とされていた。



※「高度な暗号化等の秘匿化がされている場合」には、漏えい等報告・本人通知の対象外

漏えい等発生時点の技術水準に照らし、①漏えい等が発生又はそのおそれがある個人データについて、第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、②当該技術的措置が講じられた個人データを見読可能な状態にするための手段が適切に管理されていることが必要。

15

3-4-4. 事業者が守るべきルール④ - 第三者提供（1）

【個人データを第三者に提供するとき】

以下のいずれかの場合に、個人データを第三者に提供できる。（法第27条）

1. **本人の同意**を得る。
2. **本人の同意を得ない**場合で、以下 i ～ iii のいずれかに該当する。

i. 以下の①～⑦のいずれかの場合

- ① 法令に基づく場合
- ② 人の生命、身体又は財産の保護のため（かつ本人の同意を得ることが困難）
- ③ 公衆衛生・児童の健全な育成のため（かつ本人の同意を得ることが困難）
- ④ 国や地方公共団体等への協力（かつ本人の同意を得ることにより事務遂行に支障のおそれがあるとき）
- ⑤ 学術研究機関等による学術研究の成果の公表又は教示のためやむを得ないとき ※1
- ⑥ 学術研究機関等が学術研究目的で共同研究先である第三者に提供する必要があるとき ※1
- ⑦ 学術研究目的で学術研究機関等である第三者に提供する必要があるとき ※1

※1 個人の権利利益を不当に侵害するおそれがある場合を除く。

ii. 以下3点すべてを行う（いわゆるオプトアウト手続）

- 本人の求めに応じて、その本人のデータの提供を停止することとしている。 ※2 要配慮個人情報の提供は不可等の制約有。
- 以下の①～⑧をHPに掲載するなど、本人が容易に知ることができる状態にしておく。
 - ①事業者の氏名又は名称、住所、法人の代表者名
 - ②第三者提供を利用目的としていること
 - ③提供される個人データの項目
 - ④提供される個人データの取得の方法
 - ⑤提供の方法
 - ⑥本人の求めに応じて提供を停止すること
 - ⑦本人の求めを受け付ける方法
 - ⑧個人情報保護委員会規則で定める事項
- 本人に通知した事項を個人情報保護委員会に届け出る（個人情報保護委員会はこれを公表）。

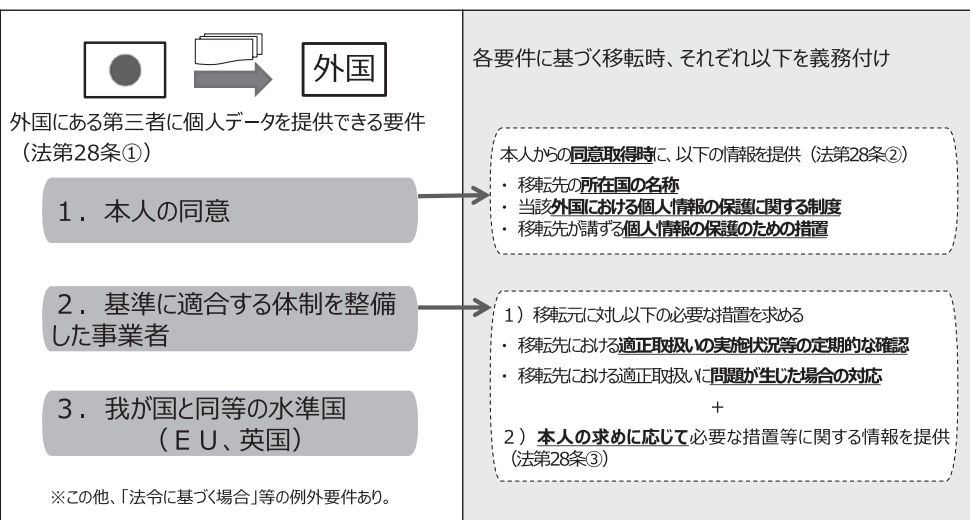
iii. 委託、事業の承継、共同利用を行う

- 共同利用：以下の①～⑤をHPに掲載するなど、本人が容易に知ることができる状態にしておくことが必要。
- ①共同利用されること
 - ②データ項目
 - ③利用される範囲
 - ④利用目的
 - ⑤責任を有する者

16

事業者が守るべきルール④ - 第三者提供（3）

- 以下1～3のいずれかの場合に、**個人データを外国にある第三者に提供**できる。（法第28条①）
- 以下1又は2による外国にある第三者への個人データの提供時について、**移転先の事業者における個人情報の取扱いに関する本人への情報提供の充実等**が必要。（法第28条②③）



17

事業者が守るべきルール⑤ - 公表事項・開示等請求

- 以下の①～⑤について、HPに公表するなど本人の知り得る状態に置く。(法第32条)
 - 当該事業者の氏名又は名称、住所、法人の代表者名
 - 全ての保有個人データの利用目的
 - 請求手続の方法
 - 安全管理のために講じた措置（公表等により支障を及ぼすおそれがあるものを除く。）**
 - 苦情の申出先
 - 認定個人情報保護団体に加入している場合、当該団体の名称及び苦情申出先
- 本人から開示を請求された場合、原則本人に**開示**する。(法第33条)
 - 個人データの授受に関する**第三者提供記録**についても、開示請求対象に追加。
 - 開示方法について、電磁的記録の提供を含め、本人が指示できるように。
- 本人からの請求に応じて、その保有個人データについて、
 - 内容に誤りがある場合には、**訂正・追加・削除**をする。(法第34条)
 - 利用目的の範囲を超えて利用されている場合、不適正な利用がされている場合、又は不正の手段で取得されている場合には、**利用停止又は消去**をする。(法第35条①②)
 - 同意なく第三者に提供されている場合等には、**第三者提供を停止**する。(法第35条③④)
 - 利用する必要がなくなった場合、一定の漏えい等事案が生じた場合、又は本人の権利若しくは正当な利益が害されるおそれがある場合**には、本人の権利利益の侵害を防止するために必要な限度で、**利用停止若しくは消去又は第三者提供の停止**をする。(法第35条⑤⑥)

18

個人情報保護委員会へのご相談

●PPC質問チャット

個人情報保護法等に関する皆様からの 質問に対して 24 時間
回答できるチャットボットサービス

<https://2020chat.ppc.go.jp/>



●個人情報保護法相談ダイヤル

個人情報保護法の解釈や個人情報保護制度についての一般的な質問にお答えしたり、個人情報の取扱いに関する苦情の申出についてのあっせんを行うための相談ダイヤル

<https://www.ppc.go.jp/personalinfo/pipldial/>

電話番号：03-6457-9849

受付時間 9:30～17:30（土日祝日及び年末年始を除く）

●PPCビジネスサポートデスク（要予約）

事業者における個人情報の保護及び適正かつ効果的な活用についての啓発の一環として、新技術を用いた新たなビジネスモデル等における個人情報保護法上の留意事項等に関する相談を受け付け

https://www.ppc.go.jp/personalinfo/business_support/

電話番号：03-6457-9771

受付時間 9:30～17:30（土日祝日及び年末年始を除く）

19

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について**【概要】**

公共空間における犯罪予防や安全確保のためのカメラ画像の適正な利用の在り方について、有識者に個人情報保護法上の観点含め多面的に検討を行い、包括的に整理を行う。

【検討会構成員】 ※構成員（五十音順）

生貝 直人	一橋大学大学院法学研究科准教授
石井 夏生利	中央大学国際情報学部教授
遠藤 史啓	神奈川大学法学部准教授
菊池 浩明	明治大学総合数理学部専任教授
穴戸 常寿	東京大学大学院法学政治学研究科教授（※座長）
新保 史生	慶應義塾大学総合政策学部教授
巽 智彦	東京大学大学院法学政治学研究科准教授
星 周一郎	東京都立大学法学部教授
森 亮二	英知法律事務所弁護士
山本 龍彦	慶應義塾大学大学院法務研究科教授

【これまでの議論】

令和4年1月からこれまで7回開催。

**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（案）**

2022年12月

※本報告書は、今後パブリックコメントに付すことを予定しており、修正される可能性があります。

【凡例】

<u>「法」</u>	<u>個人情報の保護に関する法律（平成15年法律第57号）</u>
<u>「施行令」</u>	<u>個人情報の保護に関する法律施行令（平成15年政令第507号）</u>
<u>「施行規則」</u>	<u>個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）</u>
<u>「平成27年改正法」</u>	<u>個人情報の保護に関する法律及び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の一部を改正する法律（平成27年法律第65号）</u>
<u>「令和2年改正法」</u>	<u>個人情報の保護に関する法律等の一部を改正する法律（令和2年法律第44号）</u>
<u>「通則ガイドライン」</u>	<u>個人情報の保護に関する法律についてのガイドライン（通則編）（平成28年個人情報保護委員会告示第6号）</u>
<u>「Q&A」</u>	<u>「個人情報の保護に関する法律についてのガイドライン」に関するQ&A</u>
<u>「本報告書」</u>	<u>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</u>

第1章 本報告書の背景

1 顔識別機能付きカメラシステムを巡る国内動向

顔識別機能付きカメラシステムの高性能化及び低価格化に伴い、事業者が容易に、犯罪予防や安全確保のために、顔識別機能付きカメラシステムを利用することが可能となっている。また、近年、列車内、鉄道駅構内での殺傷事件等、不特定多数の者に危害が及ぶ事件が発生し、駅や空港等における犯罪予防に対する要請がより一層高まっていることに伴い、犯罪予防や安

全確保のために顔識別機能付きカメラシステムの利用が 広がりつつある。

顔識別機能付きカメラシステムは、カメラ画角内に特定の人物が存在しているか瞬時に自動で把握できることから、犯罪予防の観点からは有効なシステムである。他方、遠隔で個人を識別することが可能であるという技術的特性上、その運用次第では、受忍限度を超える個人のプライバシー侵害等を生じさせるリスクをはらむ。

このような犯罪予防や安全確保のためのカメラ画像の適正な利用の在り方については、我が国においては未だ社会的な共通認識が形成されておらず、また海外においても適切な利用の在り方が模索されている状況にある。

顔識別機能付きカメラシステムの利用は、①同システムの導入により確保しようとする個人及び法人の権利利益並びに社会的法益、②同システムにより検知され特定のアクションの対象となる個人の権利利益、そして③同システムによる検知対象ではないが同システムにより個人情報・個人データが取り扱われる個人の権利利益、が絡むユースケースであり、慎重かつ丁寧な対応が必要である。

このため、顔識別機能付きカメラシステムを導入する際には、個人の権利利益を保護し被撮影者や社会からの理解を得ながら犯罪予防や安全確保を行っていく必要があり、個人情報の取扱いについて透明性を確保し、適正な運用を行うことが重要である。

そこで、個人情報保護委員会は、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（参考資料参照。以下「本検討会」という。）を設置し、顔識別機能付きカメラシステムを導入する際に、個人情報保護法の遵守や肖像権・プライバシー侵害を生じさせないための観点から少なくとも留意すべき点や、被撮影者や社会からの理解を得るための自主的な取組について整理を行った。なお、事業者においては、本報告書に記載されている内容だけでなく、個別具体的な事案にとって必要かつ適切な措置を自ら検討して講ずることも重要である。

本報告書では、まず第3章において、顔識別機能付きカメラシステムの技術的仕組みや利点・懸念、活用場面等、顔識別機能付きカメラシステムを導入するに当たり把握しておくべき基礎的事項について整理する。さらに、第4章では、防犯カメラによる撮影等に関するこれまでの肖像権・プライバシーに関する留意点について整理を行う。第5章では、顔識別機能付きカメラシステムを導入する際の個人情報保護法上の留意点に関する整理を行う。さらに、第6章では事業者が自主的に取り組むことが考えられる事項について整理する⁽¹⁾。

2 本報告書の対象範囲について

(1) 取り扱う個人情報

顔識別機能付きカメラシステムにおいて、顔画像及び顔特徴データが用いられる場合を中心とする⁽²⁾。なお、顔特徴データを抽出することができる精度の画像を撮影できるカメラを設置している場合等であっても、実際に顔特徴データを取り扱っていない限り、本報告書の対象とはしない⁽³⁾。

(2) 顔識別機能付きカメラを設置する空間的範囲

顔識別機能付きカメラシステムにより顔画像を取り扱うことについて事前に本人の同意を得ることが困難な⁽⁴⁾⁽⁵⁾、不特定多数の者が出入りする大規模な空間を対象とする。例えば、駅、空港等の不特定多数の者が出入りする大規模な施設がこれに当たる。

また、特定の地域内の複数の事業者や一事業者内の複数事業所で顔画像及び顔特徴データを共有して犯罪予防や安全確保を行う場合等、一つ一つの空間は小規模であっても、当該顔画像及び顔特徴データの取扱状況を全体的に見れば、上記と同様に、顔識別機能付きカメラシステムにより顔画像を取り扱うことについて事前に本人の同意を得ることが困難な、不特定多数の者が出入りする大規模な空間による取扱いと同視できる場合は、本報告書の対象となる。

なお、厳密に上記の条件に該当しない空間で顔識別機能付きカメラシステムを導入する場合であっても、本報告書の内容を参考にすることができる。

(3) 顔識別機能付きカメラシステムを利用する目的

本報告書は、犯罪予防や安全確保⁽⁶⁾のために顔識別機能付きカメラシステムを利用する場合を対象とする。マーケティングなど商用目的での利用は対象としない⁽⁷⁾。

(4) 顔識別機能付きカメラシステムを利用する主体的範囲

個人情報取扱事業者が個人情報を取り扱う場合を中心とする。

なお、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は、個人情報保護法上、原則として⁽⁸⁾個人情報取扱事業者と異なる規律が課されることから、本報告書の直接の対象とはしていない⁽⁹⁾。しかし、交通機関等を運営する地方公共団体のように、個人情報取扱事業者と同様のサービスを提供している主体が顔識別機能付きカメラシステムを導入する場合においても、本報告書の内容を参考にすることができる。

3 本報告書の位置づけ

本報告書においては、顔識別機能付きカメラシステムについて個人情報保護法の関係する条文について整理を行い、「しなければならない」と記述している事項は同法において義務とされているものであり、「努めなければならない」と記述している事項は同法において努力義務とされているものである。一方、「望ましい」、「考えられる」等と記述している事項については、事業者の特性や規模に応じ可能な範囲で対応することが望まれるものと考えられるものである⁽¹⁰⁾。仮に、「望ましい」と示す一部の対応を実施しない場合であっても、顔識別機能付きカメラシステムに関する取組を全体的に勘案し、被撮影者や社会からの理解を得られるよう、透明性を確保し、適切な運用が行われるようにすることが重要である。

なお、事業者は、単に本報告書に記載された事項をそのまま実施すれば足りると思うのではなく、本報告書に記載されていない事項も含め、当該個別具体的な事案にとって必要かつ適切な措置を十分に検討し、講ずることが重要である。

第2章 用語の定義

本報告書において用いる用語を以下のとおり定義する。

ア 顔特徴データ

顔特徴量のうち法第2条第2項第1号、施行令第1条第1号ロ及び規則第2条に該当する個人識別符号のこと。すなわち、顔の骨格及び皮膚の色並びに目、鼻、口その他の顔の部位の位置及び形状によって定まる容貌を、特定の個人を識別することができる水準が確保されるよう、適切な範囲を適切な手法により電子計算機の用に供するために変換した文字、番号、記号その他の符号。

イ 顔識別

カメラにより撮影された者の中から、その者の顔特徴データと照合用データベースに登録された顔特徴データを照合して登録された顔特徴データの人物を見つけること。

ウ 顔識別機能付きカメラシステム

顔画像を撮影するカメラ及び撮影した顔画像から顔特徴データを抽出し顔識別を行うシステムのこと。

例えば、あらかじめ検知対象者の顔特徴データを登録した照合用データを作成しておき、ある空間にカメラを設置し、当該カメラに映った人の顔画像から顔特徴量を抽出し、照合用データベースに登録された顔特徴データと照合し、検知対象者を見つけるためのシステムがこれにあたる。

エ 顔認証

本人の要請に応じて、カメラにより撮影された顔画像から抽出された顔特徴データとデータベースに登録された顔特徴データを照合して同一性を確認すること。

顔認証機能を搭載するシステムとしては、例えば、入退館システムが考えられる。まず、あらかじめ、ある施設に入館できる者だけをデータベースに登録しておく。そして、当該施設の入口に設置されたカメラで撮影した当該施設に入館しようとする者の顔画像から顔特徴データを抽出し、入館希望者があらかじめ登録したデータベース中の顔特徴データと照合のうえ、一致した場合には入館を許可するシステムである。

オ 顔認識

顔特徴データに基づき個人を自動認識すること。顔識別及び顔認証を含むがこれに限られない。

カ 従来型防犯カメラ

防犯目的で設置されているカメラのうち、撮影した画像から顔特徴データの抽出を行わないもの。

キ 被撮影者

カメラにより撮影される全ての者のこと。顔識別機能付きカメラシステムにおける検知対象者に限られない。

ク 照合

ある顔特徴データと他の顔特徴データの類似性又は被類似性を見積もり、算定、又は測定すること。

ケ 照合用データベース

検知対象者の顔特徴データからなるデータベースのこと。照合のために用いられる。

コ 検知

照合の結果、照合用データベースに登録した顔特徴データと被撮影者の顔画像から抽出した顔特徴データが同一人物である可能性があらかじめ設定した閾値より高いと判定すること。

サ 検知対象者

顔識別機能付きカメラシステムにおいて、検知しようとする者のこと。

シ 登録対象者

顔識別機能付きカメラシステムにおいて、照合用データベースの登録基準に該当する者のこと。

ス 被検知者

顔識別機能付きカメラシステムにおいて検知対象者であると検知された者のこと。

セ 被登録者

照合用データベースに登録された者のこと。

ソ 運用基準

登録基準、対応手順、保存期間及び登録消去基準等の顔識別機能付きカメラシステムを運用するための基準のこと。

第3章 顔識別機能付きカメラシステムについて

本章では、顔識別機能付きカメラシステムの技術的仕組みや特徴、活用場面等について述べる。顔識別機能付きカメラシステムを利用するに当たっては、その仕組みや特徴を理解したうえで、できる限り懸念点を払拭することができる必要かつ適切な措置を講ずることが望ましい。

1 顔識別機能付きカメラシステムやその他防犯システムの機能や動向

(1) 顔識別機能付きカメラシステムの技術的仕組み

顔識別機能付きカメラシステムは、検知対象者の顔画像⁽¹¹⁾及び顔特徴データをあらかじめ照合用データベースに登録しておき、カメラにより取得した画像から抽出した被撮影者の顔特徴データと照合し、被撮影者がデータベースに登録された者と同一人物である可能性が高いと検知した場合にアラート通知等がなされるシステムである。

① 照合用データベースの作成

顔識別機能付きカメラシステムによる検知対象者を定め、その者の顔画像から、特定の個人を識別することができる顔特徴データを抽出し、当該顔特徴データを照合用データベース

に登録する。

② カメラによる撮影

検知対象者の動線等を考慮して検知したい場所にカメラを設置し、当該カメラで通行者を撮影し顔画像を取得する。

③ 顔特徴データの抽出

カメラにより撮影された顔画像の目・鼻・口などの顔の特徴から顔特徴データを抽出する。

④ 照合用データベースとの照合

③で抽出した顔特徴データを、①で作成した照合用データベースに登録された顔特徴データと照合する。

⑤ 検知対象者の検知

照合の結果、③で抽出した顔特徴データと同一人物である可能性が高い顔特徴データが照合用データベースに登録されていた場合にシステムが検知する。

顔識別機能の精度が低い場合、検知対象者を見逃したり、検知対象者でない者を誤判定したりする確率が高まる。また、判定の閾値（どの程度の類似性があれば同一人物であると判定するか）の閾値の設定によっても、検知対象者の見逃しや、検知対象でない者を誤判定する確率が変わる。

⑥ 被検知者への対応

検知対象者を検知した場合には、アラート通知等がなされ被検知者と検知対象者の同一性を確認したうえ、見守りや声掛け等を行うこともある。

顔識別機能付きカメラシステムによる被検知者の検知は、あくまでも近似性による推測に基づくものであり、同一人物であるとの事実を示しているわけではないことに留意が必要である。

(2) 顔識別機能付きカメラシステム以外の映像分析技術

犯罪予防や安全確保のために用いることができるカメラシステムを用いた映像分析技術には、顔識別機能付きカメラシステムによる照合用データベースを作成しない方法として次の技術が考えられる。

ア 侵入検出

カメラ映像の中に検出範囲を設定しておき、特定の個人を識別せずに人・物が検出範囲に侵入したことを検出し、検出時にアラート通知等がなされる。これにより警備員の補助をすることができる。

イ 行動検出/不審物検出

映像枠内の物体を認識し、平常時には発生しない異常行動を検出することができる。例えば、人の急な走り出しや置き去りにされた荷物を自動検出し、アラート通知等がなされる。

ウ 属性推定・人数カウント

映像枠内の者の顔画像から顔特徴量を抽出・分析することで性別や年齢などの属性情報のみ

を推定することができる。笑顔度といった表情や、マスクのような顔装着物を推定することもできる。

また、顔画像から抽出した顔特徴量によっても人数のカウントを行うことができるため、入場者数と退場者数の測定・集計、混雑状況を把握することができる。

エ 混雑度分析

映像枠内にいる人物の占有面積などにより混雑度を分析することができる。混雑度が一定の水準を超えたときに、入場制限を行う等の活用方法がある。

オ 顔画像を用いない人物照合

顔画像ではなく、人物の服装や体型などの外観画像を用いて同一人物を検出することができる。顔や身体の一部が映像に映っていなかったり、カメラに対して正面を向いていなかったりしても、照合が可能である。ただし、一般に照合の精度は顔画像よりも下がる。

カ 動線分析

映像から動線データを作成し分析することが可能である。また、不可視赤外線光線などを用いて動体を検出することで、動線分析を行うことも可能である。

(3) その他の防犯システム、対策⁽¹²⁾⁽¹³⁾

施設内における巡回警備、危険物探知犬の運用、金属探知ゲートの設置、手荷物検査の実施等がある。

小売店における万引対策としては、電子商品監視機器（EAS）等が利用されている。

2 顔識別機能付きカメラシステムを利用することの利点・懸念点

顔識別機能付きカメラシステムの利用については、効率的な犯罪予防や安全確保に高い効果を有する利点があるとされているが、懸念点もある。本項では、国内外の文献等⁽¹⁴⁾において指摘された利点・懸念点について紹介する。

(1) 顔識別機能付きカメラシステムを利用することの利点

顔識別機能付きカメラシステムを利用することで、その撮影範囲に入った者の顔特徴データを容易に取得することができる。また顔特徴データは不変性が高く、一意性があるため、体格や服装を手掛かりにするよりも高い精度で検知・追跡を行うことができる。このような特徴により、犯罪予防や安全確保に高い効果を有し得る。

例えば、一定の基準の下に照合用データベースに登録された者を、一定の場所を通行する者と照合し、検知された者に対する警備を行うことで、一定の場所における犯罪の発生を防止できる蓋然性が高まる。

また、犯罪の被疑者や行方不明者等の検知対象者と複数の顔識別機能付きカメラシステムに映った者を照合することで、迅速に検知対象者を発見することができ、更なる犯罪の発生の防止や、行方不明者の早期発見が可能となる。

(2) 顔識別機能付きカメラシステムを利用することの懸念点⁽¹⁵⁾

他方、顔特徴データや顔識別機能付きカメラシステムの特徴によって、以下の懸念点もある。顔識別機能付きカメラシステムを利用するに当たっては、その利点だけでなく、懸念点も把握したうえで、利用の要否や対応を検討することが重要である。

ア 不変性と追跡性

顔特徴データは不変性が高いため、顔識別機能付きカメラシステムにより、長期にわたり特定の個人を追跡することが可能である。更に、広範囲にわたって複数箇所に設置したカメラで撮影した顔画像を用いて照合を行う場合には、広範囲にわたる特定の個人の行動を追跡することも可能である。

イ 自動的、無差別かつ大量の取得

顔識別機能付きカメラシステムを利用すると、被撮影者が自己の個人情報が取り扱われている事実を認識できず、またその取扱いを受容するか否かを選択することができない状況で、撮影範囲に入った全ての者の顔画像を自動的、無差別かつ大量に取得することができる。

ウ 利用目的の予測困難性

顔識別機能付きカメラシステムにより取得された顔画像は、情報システム上で様々な情報に紐づけることが可能であり、また、顔画像自体から様々な情報を分析・推知することも可能である。

被撮影者は、設置されたカメラの外観から、顔識別機能付きカメラシステムにより顔画像及び顔特徴データが取得されていることや、他のデータベースとの照合やこういった分析がされているか認識することは困難である。

これに加えて、今後の技術の進歩によっては、現時点で予期しない取扱方法が技術的に可能となる可能性が高い。

エ 差別的効果

顔識別機能付きカメラシステムで利用する照合用データベースの作成過程自体に、特定の属性の者への偏見や差別が含まれているおそれがある。

顔識別機能付きカメラシステムが、技術的に特定の属性の者の検知率に差が生じたり、誤作動を起こしやすかったりすることにより、差別的効果が引き起こされるおそれがある。例えば、特定の人種や肌の色によって、検知率が異なってしまう事例がある。

また、顔識別機能付きカメラシステムは、通常、AIが用いられているが、当該AIの学習用データベース自体に偏りがあった場合、一定の属性の者に対して差別的な検知がなされるおそれがある。

オ 行動の委縮効果

自らの顔画像や行動を含む個人情報がいつ、どの範囲で取得され、いかなる目的で利用されているかが明確でないことにより不安になり、行動に対する委縮効果が生じ得る。

3 犯罪予防や安全確保のために顔識別機能付きカメラシステムを利用することが想定される場面

犯罪予防や安全確保のために顔識別機能付きカメラシステムを利用することが想定される場面としては、より具体的には以下の場面が考えられる⁽¹⁶⁾⁽¹⁷⁾。

(1) 犯罪予防

一定の基準を満たす者の顔特徴データを照合用データベースに登録し、犯罪を予防したい場所を顔識別機能付きカメラにより撮影し、被検知者に声掛け等を行うことで犯罪の発生を予防し得る。

(2) 要保護者保護

例えば、行方不明者や迷子の搜索の際に、当該者の顔特徴データを照合用データベースに登録し、当該者が通行する可能性のある場所を顔識別機能付きカメラにより撮影することで効果的に搜索することができる。

第4章 肖像権・プライバシーに関する留意点

顔識別機能付きカメラシステムを利用する場合、個人情報保護法の遵守に加えて、被撮影者の肖像権やプライバシーを侵害することのないよう十分留意する必要がある。本章では、肖像権やプライバシー侵害に基づく不法行為の成否が争われた裁判例（損害賠償請求・妨害排除請求等）等を整理する。ただし、以下に示す裁判例は現時点までに示されてきたものであり、今後新たな考慮要素等が示される可能性があることには注意が必要である。

また、不法行為の成立と個人情報保護法の関係についても述べる。

なお、本章において丸数字を用いるときは、本文中及び脚注18。で示す当該丸数字を冒頭に記載した裁判例のことを指す⁽¹⁹⁾。

1 肖像権・プライバシー侵害を争点とする裁判例

(1) 肖像権・プライバシー侵害を争点とする判例

①最判昭和44年12月24日刑集23巻12号1625頁は、不法行為の成否が争われた事例ではないが、実質的には、肖像権を承認したものと評価されており⁽²⁰⁾⁽²¹⁾、「個人の私生活上の自由の一つとして、何人も、その承諾なしに、みだりにその容ぼう・姿態（以下「容ぼう等」という。）を撮影されない自由を有するものというべきである」と示した。

その後、②最判平成17年11月10日民集59巻9号2428頁が「人は、みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する」とした⁽²²⁾。

(2) カメラ撮影に関する肖像権・プライバシー侵害を争点とする裁判例における考慮要素

②最判平成17年11月10日民集59巻9号2428頁は、上記に加え、人の容ぼう等を承諾なく撮影することが不法行為法上違法となるかどうかについては総合考慮によるとしつつ、具体的な判断基準を示した。

本判例⁽²³⁾は、防犯カメラの撮影に関する事例ではないが、以降の防犯カメラの撮影に関する裁判例でも複数引用されている。

② 最判平成17年11月10日民集59巻9号2428頁（抜粋）

人は、みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する…もともと、人の容ぼう等の撮影が正当な取材行為等として許されるべき場合もあるのであって、ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは、被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して、被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべきである。

上記の判例以降、防犯カメラによる撮影に関する裁判例では、被撮影者の人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを、被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様（方法）、撮影の必要性等により総合考慮することに加え、近時の裁判例では撮影の範囲や撮影された画像の管理方法を検討するものもみられる⁽²⁴⁾。

顔識別機能付きカメラシステムを犯罪予防や安全確保のために利用する場合についての裁判例は、現在のところ見当たらないが、防犯カメラの撮影に関する裁判例において、具体的にどのような事実がこれまで考慮されてきたか、主な裁判例を整理する。

各裁判例の事案及び判示の概要については、本報告書参考資料に記載した。

ア 被撮影者の社会的地位、撮影された被撮影者の活動内容

②では、写真撮影の当時、社会の耳目を集めた刑事事件の被疑者として拘束中の者が、手錠をされる等の状態で、被疑者として出頭して在廷していたことが考慮されている。ただし、本判例は、防犯カメラによる撮影ではなく、写真週刊誌のカメラマンが法廷において撮影をした事案であることに留意が必要である。

イ 撮影の場所、撮影の範囲

撮影の場所に関して、被撮影者が被撮影者宅から外出する際には必ず通る私道について、被撮影者宅の延長区間として被撮影者らの日常生活に密着した空間であることを理由に、単に道路であることをもってプライバシーを保護しなくてよい場所とするのは相当でない、道路であっても、特定の者がテレビカメラによってその行動を継続的に撮影され、監視されるという特別の制約を受けるいわれはないと指摘した裁判例がある（⑤）。

また、マンション建設に反対する運動が行われている場所において、小競り合いなどの不測の事態が生じた際に備えて、証拠保全の目的からカメラを設置している事例において、居宅が

撮影範囲に含まれるものの、室内の様子は窺えないこと、その範囲がわずかであったこと、遠方であるから出入りする人を認識することができないことなどから、その目的に照らし撮影範囲は問題のない範囲だったと判断するものもある（⑨）。

ウ 撮影の目的

カメラを設置する場合の目的について、多くの裁判例において検討されている。

カメラの設置場所を、エレベーター内、マンション1階の内階段の出入口、1階夜間入口扉付近、1階の管理人室のカウンターであること等を認定した上で、当該カメラは通常の防犯カメラであって、特定の者の行動を監視する目的ではなかったことを、侵害の成立を否定する要素として考慮していると思われるものがある（④）。

また、特定の者の行動を監視することが目的であったことを認定した上で、駐輪場、玄関付近、被撮影者が被撮影者宅から外出する際に必ず通る私道部分を継続的に撮影する行為がプライバシーを侵害すると認めたものがある（⑤）。

さらに、カメラを設置した当該コンビニ店舗における万引きの発生件数や、コンビニにおける犯罪の発生の状況等について考慮したうえ、カメラ設置の目的を、犯罪の発生に対処するとともに、犯罪の発生を予防することにあると認めた裁判例や（⑥）、迷惑行為が行われていた事実等をもとに、目的が迷惑行為等の防止であると認めた裁判例がある（⑩）⁽²⁵⁾。

エ 撮影の態様

撮影の態様については、カメラが固定され特定の者を追跡して撮影する機能がないことや（⑥、⑦、⑧、⑨、⑩）、カメラが作動中である旨の周知をしていること（⑥、⑦）、カメラに撮影されることを望まないのであれば他の場所に行くことが可能であること（⑥）は、侵害を否定する要素として考慮されている。また、カメラが店舗の利用者から見えること（⑥）、カメラが通行人から見えること（⑧）、防犯カメラが設置されていることが分かる状態であること（⑨）を考慮する裁判例もある。

オ 撮影の必要性

撮影の必要性は、多くの裁判例において検討されているが、撮影の目的や、撮影の場所、範囲、態様などを考慮し検討されている。

撮影目的が、犯罪行為ないし迷惑行為の防止であるときに、現にカメラの設置場所近隣において犯罪行為が発生していることを、必要性を肯定する要素として考慮する裁判例がある（⑧）。

また、カメラ設置の目的を達成する代替手段がないわけではないことが侵害を肯定する要素として考慮された裁判例もある（⑦）。

カ 撮影された画像の管理方法

撮影された画像の管理方法については、画像の保存期間（⑥（1か月）⑦（2週間）⑧（45日間）⑨（14日14時間）⑩（90時間））が考慮されているところ、少なくとも⑥を前提に管理方法は相当と判断され、⑧であっても侵害を肯定する要素としては考慮されていない。また、閲覧できる者が限定されていること、撮影された画像を他の媒体に保存して持ち出すことができないように管理されていることが侵害を否定する要素として考慮され、画像の管理方法につきマニ

ュアル等を作成することが望ましいとも述べるものがある（⑥）。さらに、1日中モニターに張り付いて映像を見ていたわけではなく、問題が起きた時に確認する程度だったことや、撮影された画像が他の媒体に保存されて目的以外に利用された証拠はないことを考慮するものもある（⑨）。

（3）顔識別機能付きカメラシステムを利用する場合への示唆

これらの裁判例は、顔識別機能付きカメラシステムについて争われた裁判例ではないが、顔識別機能付きカメラシステムの特徴と共通する点がある。このため、顔識別機能付きカメラシステムの利用については、これらの裁判例において考慮されてきた点は、十分注意する必要があるといえる。

なお、顔識別機能付きカメラシステムは、顔特徴量を用いることにより、従来型防犯カメラによる目視よりも、容易に検知対象者を検知し、発見することができる。これにより、顔識別機能付きカメラシステムの追跡の効率性は非常に高い。

このため、顔識別機能付きカメラが様々な場所に設置され、異なる地点間で顔識別が行われる場合には、検知対象者の移動経路を継続的網羅的に相当程度詳細に把握し得ることになり、特定の個人を長期かつ広範にわたり追跡して監視につながるおそれがある。このような点が、肖像権・プライバシーの観点から見た、従来型防犯カメラと顔識別機能付き防犯カメラシステムの大きな違いであり、この顔識別機能付きカメラシステム固有の追跡性のリスクが肖像権・プライバシー侵害の成否の判断に影響を与える可能性がある⁽²⁶⁾。

2 不法行為の成否と個人情報保護法の関係

顔識別機能付きカメラシステムを利用した撮影行為について不法行為が成立する場合、当該撮影行為は個人情報保護法上どのように評価されるべきか。

不法行為法と個人情報保護法はその目的や性格に異なる部分があることから、不法行為が成立する場合、同時に個人情報保護法違反となる場合もあり得るが、不法行為が成立したからといって必ずしも個人情報保護法違反となるわけではない。

個人情報保護法は、本人の利益のみならず社会全体の利益の増進のためにパーソナルデータの利活用を益々促進することが望まれる一方、プライバシー保護の観点からは、これまでと同様、適切な取扱いが求められている⁽²⁷⁾として、平成27年に改正され、本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要する個人情報である要配慮個人情報に関する規律が設けられ（法第2条第3項、法第20条第2項等）、また個人による開示等の求めが裁判所に訴えを提起することができる請求権であることが条文上明確にされた（法第33条第1項、法第34条第1項、法第35条第1項、同条第3項）。さらに、令和2年改正法においては不適正利用禁止規定が新設され、違法又は不当な行為を助長し、又は誘発する恐れがある方法により個人情報を利用することが禁じられることとなった（法第19条）。このように、個人情報保護法は、個人情報の性質や取扱方法を考慮する等、個人の権利利益に配慮している。

そこで、1で紹介した裁判例の動向を踏まえると、不法行為の成否を評価するに当たり考慮される要素は、個人情報保護法上も不適正利用の禁止規定（法第19条）や適正取得規定（法第20条第1項）の解釈などにおいて、考慮されるべきであると考えられる。

したがって、顔識別機能付きカメラシステムを利用するに当たっては、個人情報保護法を遵守するのみならず、肖像権やプライバシー保護の観点からも留意する必要があるし、そのような観点を個人情報保護法の適用においても考慮すべきであると考えられることに留意する必要がある。

（参考） カメラ撮影に関する肖像権・プライバシー侵害を争点とする裁判例

① 最判昭和44年12月24日刑集23巻12号1625頁

【事案の概要】⁽²⁸⁾

事案は、昭和37年6月、京都市内で行なわれた京都府学連のいわゆるデモ行進に際し、被告人らが、許可条件に違反して隊列を乱したと判断した警察官が証拠保全のため写真撮影したところ、被告人が旗竿でその下顎部を突いて1週間の傷害を負わせたというものである。

【判旨】⁽²⁹⁾

何人も、その承諾なしに、みだりにその容ぼう姿態を撮影されない自由を有し、警察官が、正当な理由もないのに、個人の容ぼう等を撮影することは、憲法一三条の趣旨に反し許されない（当該写真撮影は適法な職務執行行為であるとした）。

② 最判平成17年11月10日民集59巻9号2428頁⁽³⁰⁾

【事案の概要】

本件は、刑事事件の被疑者、被告人の法廷における容ぼう、姿態（以下「容ぼう等」という。）を撮影した写真やこれを描写したイラスト画について、いわゆる肖像権の侵害による不法行為の成否が問題とされたものである。

【判旨】

人は、みだりに自己の容ぼう、姿態を撮影されないということについて法律上保護されるべき人格的利益を有し、ある者の容ぼう、姿態をその承諾なく撮影することが法律上違法となるかどうかは、被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して、被撮影者の上記人格的利益の侵害が社会生活上受忍すべき限度を超えるものといえるかどうかを判断して決すべきである。

写真週刊誌のカメラマンが、刑事事件の被疑者の動静を報道する目的で、勾留理由開示手続が行われた法廷において同人の容ぼう、姿態をその承諾なく撮影した行為は、手錠をされ、腰縄を付けられた状態の同人の容ぼう、姿態を、裁判所の許可を受けることなく隠し撮りしたものであることなど判示の事情の下においては、不法行為法上違法である。

③ 東京地判平成18年3月31日判タ1209号60頁⁽³¹⁾

【事案の概要】

Yがビデオ店の防犯カメラに映ったタレントXの写真を週刊誌に掲載したため（ビデオ店からYにカメラの画像の提供がなされた）、Xが損害賠償を請求した。

【判旨】

平成17年判決と同様の枠組み(被撮影者の社会的地位、撮影された被撮影者の活動内容、撮影の場所、撮影の目的、撮影の態様、撮影の必要性等を総合考慮して)を示したうえで、「掲載された写真自体からはその被写体である人物の容ぼう等が肖像権侵害を訴えている当該個人の容ぼう等であることが明らかでない場合であっても、写真の説明文と併せ読むことによって読者が当該個人である旨特定できると判断される場合や読者が当該個人であると考えるような場合には、撮影により直接肖像権が侵害されたとはいえないものの、当該個人が被写体である人物本人であったか否かにかかわらず、当該個人が公表によって羞恥、困惑などの不快な感情を強いられ、精神的平穏が害されることになりはしないというべきであるから、やはり撮影により直接肖像権が侵害された場合と同様にその人格的利益を侵害するといえるべきである」とした。その上で、本件ビデオ店の店内に設置された防犯カメラによって撮影された映像が週刊誌に掲載されるであろうことについては、Xは到底予想しうるものとはいえないこと等を指摘して、上記の人格的利益の侵害を認めた。

なお、防犯カメラを設置して入店者を撮影することが正当化されるのは、「店舗内での犯罪発生を事前に防止し又は事後的に犯罪解明等を容易にするためという防犯目的に限られる」と指摘した上で、被告の行為(マスコミが防犯カメラの目的外利用にあたることを認識しながら、その撮影画像を記事に用いる)は、目的外利用をすることを助長及び促進することから、悪質であると指摘している。

④ 東京地判平成19年 3 月26日 LEX/DB28132442**【事案の概要】**

マンション内にビデオカメラが設置されたことが、当該マンションの区分所有者Xのプライバシーを侵害したとして、撤去を求めた事案。

【判旨】

カメラは、エレベーター内、マンション1階の内階段の出入口、1階夜間入口扉付近、1階の管理入室のカウンターに設置されたものであること等を指摘した上で、当該カメラは通常の防犯カメラであって、Xの行動を監視するために設置されたものではないこと等から、設置目的の相当性、設置の必要性及び設置方法の相当性があるとして、プライバシー侵害を否定。

⑤ 東京地判平成21年 5 月11日判時2055号85頁**【事案の概要】**

YがY宅1階に防犯カメラを設置したことが、X宅の駐輪場、玄関付近、自宅から公道までの私道部分を撮影しているとして、XがYに対しプライバシー侵害に基づき損害賠償を請求した。

【判旨】

本件カメラが、X宅の駐輪場、玄関付近、XがX宅から外出する際に必ず通る私道部分を撮影していること、本件カメラの設置がXらの行動を監視することが目的であったこと、から、プライバシーを侵害するものとして損害賠償を認めた。

なお、私道は不特定多数の者が通行する空間である点について、「道路は、公道であれ、私道であれ、一般の人目に触れる空間であるから、一般的には、居宅や敷地内などのように、プライバシーの保護の要請が高い空間であるとはいえない」が、本件私道部分は、「いわば原告宅の延長空間として原告らの日常生活に密着した空間であるといえるべきであるから、単に道路であることをもって、プライバシーを保護しなくてもよい場所であるとするのは相当でない」ともする。

⑥ 東京地判平成22年 9 月27日判タ1343号153頁**【事案の概要】**

Xが、コンビニの監視カメラにおいて原告を撮影した行為及び原告が映っている映像を報道機関に提供した行為が、肖像権・プライバシー権を侵害したとして損害賠償を求めた。

【判旨】

平成17年の枠組みを示したうえで、「本件監視カメラは、本件店舗を訪れた客の個別的承諾を得ることなく、商品を選定したり、これを購入する姿を無差別に撮影するものであり、客の人格的利益及びプライバシー権が侵害されるおそれを内包するものであるということが出来るから、本件監視カメラによる撮影、撮影画像の提供による公表等が不法行為法上違法といえるか否かは、撮影の目的、撮影の必要性、撮影の方法及び撮影された画像の管理方法並びに提供の目的、提供の必要性及び提供の方法等諸般の事情を総合考慮して、上記姿を撮影され撮影に係る画像を公表等されない利益と上記姿を撮影し撮影に係る画像を公表等する利益とを比較衡量して、上記人格的利益及びプライバシー権の侵害が社会生活上受忍限度を超えるものかどうかを基準にして決すべきである」とし、本件店舗における万引きの発生件数や、コンビニにおける犯罪の発生の状況等を指摘したうえで、撮影の目的が、万引きや強盗等の犯罪の発生に対処するとともに、本件監視カメラが作動していることを知らせることによる犯罪の発生予防であること、本件監視カメラが、固定されたものであり、特定の顧客を追跡して撮影することはないこと、本件店舗の内外に10か所程度、監視カメラが作動中である旨の張り紙をしている上、本件監視カメラのほとんどを客から見えるような位置に設けていること、本件監視カメラにより撮影された画像は1か月間程度保存され、その後は自動的に上書きされることとなっており、これにより撮影された映像は自動的に抹消されること、従業員が本件監視カメラの映像を録画媒体に記憶させた上、店外に持ち出すことは事実上不可能な状況にあること、等から、撮影の不法行為への該当性は否定した。

そのうえで、動画ファイルの提供については、カメラの設置目的と直接関連性は有しないものの、万引きの増加という社会問題に警鐘をならす番組制作のために提供する点で公益目的があるし、カメラ設置目的に間接的に沿うものであること、本件動画ファイルの提供の方法も相当であった等として、この点も侵害を否定した。

⑦ 東京地判平成27年11月 5 日判タ1425号318頁**【事案の概要】**

Yが建物1階にカメラを設置したところ、当該防犯カメラにXらの玄関付近が撮影範囲に含まれていることから、Xらがプライバシー侵害に基づいて、カメラの撤去を求めた。

【判旨】

「人は、みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する…。もっとも、ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは、撮影の場所、撮影の範囲、撮影の態様、撮影の目的、撮影の必要性、撮影された画像の管理方法等諸般の事情を総合考慮して、被撮影者の上記人格的利益の侵害が社会生活上受忍の限度を超えるものといえるかどうかを判断して決すべき」とした。そのうえで、本件カメラが、固定されており、特定人を捉えたら追跡したり、監視を続けたりする性質のものではないこと、防犯カメラ作動中であることを記載したプラスチックのプレートを本件全カメラの下に明示し、カメラの存在が分かるようにしていることが認められること等から、本件カメラには防犯目的が含まれているが監視目的が含まれているとまでは認めることができないこと及び本件カメラの撮影された映像の保存期間は約2週間であって、その期間を過ぎると自動的に上書きされるという仕組みになっていること等を指摘しつつも、カメラには、玄関入口付近に立っていたり、その出入りについて、顔を識別できるほど

ではないものの、かなり鮮明に映ること、（一部の原告については）玄関付近等が常に撮影されていること、（他の原告については）日常の外出時に通行している私道道路（公道に至るまで通行している道路）を利用する際に常に撮影されていること等から、本件カメラが撮影している場所が屋外であるものの、プライバシー侵害の程度は大きい、とした。さらに、カメラを設置する目的を達成するための他の代替手段がないわけではないこと等も考慮し、プライバシーの侵害は社会生活上受忍すべき限度を超えているとして、撤去、損害賠償を認めた。

⑧ 東京地判平成31年 3 月14日 LEX/DB25559868

【事案の概要】

X所有の土地建物から公道に至るためには、私道を通る必要があり、当該私道に接している土地を所有するYが防犯カメラを設置し、当該私道の一部を撮影していたことについて、プライバシー侵害に基づきカメラの撤去を求めた事案

【判旨】

本件防犯カメラが、固定されており、同一の方向及び範囲を撮影するというものであること、本件防犯カメラの下には警備事業者名の表示がされ、通行人は防犯カメラの存在を認識することが可能であること、撮影された映像の保存期間は約45日間であり、期間経過により自動的に上書きされる仕組みとなっていることに照らせば、防犯カメラにより容ぼうを撮影されたとしても、上記撮影場所、範囲及び態様に照らせば、屋外の道路を通行する姿をごく短時間撮影されるというものであり、原告のプライバシー権侵害の程度は低いものといわざるを得ない、また、カメラの設置目的は、犯罪行為ないし迷惑行為の防止が目的であること、現にY宅の近隣において窃盗などの犯罪行為が発生していること等から必要性が否定できない等と指摘のうえ、社会生活上受忍すべき限度を超えるものとは認められないとして、撤去の請求を否定。

⑨ 名古屋地判令和元年 9 月 5 日 LEX/DB25564163

【事案の概要】

Xらの住所地付近の土地に、Yらが分譲マンションの建設計画を立て、建設途中に、建設現場に防犯カメラを10台設置し、これらの防犯カメラによってXらが各住居に出入りする様子等を撮影したことにより、Xらの肖像権、プライバシー権侵害されたとして、Xらが損害賠償を求めた。

【判旨】

「ある者の容ぼう等をその承諾なく撮影することなど、Xらの肖像権等に制約を加えることが不法行為法上違法となるためには、撮影の場所、撮影の範囲、撮影の態様、撮影の目的、撮影の必要性、撮影された画像の管理方法、Xらの肖像権等が制約される程度等諸般の事情を総合的に考慮して、Xらの肖像権等に対する制約が社会生活上受忍の限度を超えるものでなければならない」としたうえで、撮影の場所、範囲が建設現場内および公道で撮影範囲を変更できない仕様（首振り機能なし）であり、奥にXらの居宅が映るものの、その範囲がわずかであったり、室内の様子はうかがえなかったり、遠方であるから出入りする人を認識することができないこと、首振り機能はなく、24時間撮影され、その画像を拡大もできるが、モニターを監視している従業員もいないこと、XらとYらとの間で、小競り合いなどの不測の事態が生じた際に備えて、証拠保全の目的から防犯カメラを設置していたこと、映像の保存期間は約2週間であり、過去の映像に上書き保存されており、撮影された映像が、他の媒体に保存され、証拠保全の目的以外の用途に使用されていないこと等から不法行為の成立を否定した（なお、本判決は監視カメラの設置による不法行為の成立は認めなかったものの、ダミーのカメラの設置による不法行為の成立は認めた）。

⑩ 東京地判令和2年1月27日 LEX/DB25584266**【事案の概要】**

Yが自宅の壁面に防犯カメラを設置（南側通路に向けられて設置）したところ、隣人で本件通路を日常的に利用するXから、プライバシー権等が侵害されたとして、損害賠償・防犯カメラの撤去が請求された。

【判旨】

「防犯カメラで、ある者の容ぼう等をその承諾なく撮影することが不法行為法上違法となるかどうかは、撮影の場所、範囲、態様、目的や必要性のほか、撮影された画像の管理方法等諸般の事情を総合考慮し、被撮影者のプライバシー権をはじめとする人格的利益の侵害が社会生活上受忍限度を超えるものといえるかどうかを判断して決すべき」としたうえで、本件カメラの設置の目的は、一般的な防犯のみならず、Xの行動を注視することも含まれていたことは否定し難いが、本件カメラがX宅の玄関や家の内部を撮影するようには設置されていないこと、本件カメラは固定されており特定人を追跡して撮影する機能はないこと、撮影した映像は別の媒体に移す等の作業をしない限り上書き保存される仕組みであることから、XによるYに対する迷惑行為等を防止する目的であって、その設置には一定の必要性が認められる。

そして、これらの事情に加え、本件カメラの撮影範囲である本件通路は屋外であって全くの私的空間ではないこと、本件カメラによるXの撮影が約3か月間にとどまること等にも鑑みれば、本件カメラの撮影によりXに対するプライバシー権侵害があったことは否定できないものの、その程度は、本件カメラ設置の動機を与えたXにおいて社会通念上受忍限度を超えるものとまではいえない。

⑪ 最大判平成29年3月15日刑集71巻3号13頁⁽³²⁾**【事案の概要】**

本件は、自動車等窃盗で調達した車両で移動して出店荒らしをして回ったという広域集団窃盗・建造物侵入等の事件について、車両に使用者らの承諾なく秘かにGPS端末を取り付けて位置情報を検索し把握する刑事手続上の捜査（以下「GPS捜査」という。）の適法性等が問題とされた事案である。本件においては、被告人が複数の共犯者と共に犯したと疑われていた窃盗事件に関し、組織性の有無、程度や組織内における被告人の役割を含む犯行の全容を解明するための捜査の一環として、約6か月半の間、被告人、共犯者のほか、被告人の知人女性も使用する蓋然性があつた自動車等合計19台に、同人らの承諾なく、かつ、令状を取得することなく、GPS端末を取り付けた上、その所在を検索して移動状況を把握するという方法によりGPS捜査が実施された。

【判旨】

車両に使用者らの承諾なく秘かにGPS端末を取り付けて位置情報を検索し把握する刑事手続上の捜査であるGPS捜査は、個人のプライバシーの侵害を可能とする機器をその所持品に秘かに装着することによって、合理的に推認される個人の意思に反してその私的領域に侵入する捜査手法であり、令状がなければ行うことができない強制の処分である。

⑫ 東京地判平成13年2月6日判時1748号144頁**【事案の概要】**

本件は、原告らが、道路上を自動車で行き交す際、被告が日本全国の道路上に設置、管理している自動車ナンバー自動読み取りシステム（以下「Nシステム」という。）の端末によって、車両の運転席及び搭乗者の容ぼうを含む前面を撮影された上、車両ナンバープレートを判読されて、これらに関する情報を保存、管理されたことにより、肖像権、自由に移動する権利及び情報コントロール権を侵害されたと主張して、被告に対し、不法行為に基づく損害賠償を請求している事案である。

【判旨】⁽³³⁾

Nシステムによって走行車両のナンバーデータを記録、保存する目的につき、自動車使用犯罪発生時において、現場から逃走する被疑者車両を速やかに捕捉し、犯人を検挙すること並びに重要事件等に使用されるおそれの強い盗難車両を捕捉し、犯人の検挙及び被害車両の回復を図ることにあるとしたうえで、Nシステムのテレビカメラによって一時的に走行車両の搭乗者の容ぼう等が撮影されとしても、撮影された画像は瞬時にコンピュータ処理によって走行車両のナンバープレートの文字データとして抽出され、容ぼう等が写っている画像そのものが記録、保存されることはなく、走行車両の搭乗者の容ぼうが写っている画像そのものを人間が視覚的に認識することは一切できないから、Nシステム端末によって、承諾なしに、みだりにその容ぼう等を撮影されない自由が侵害されるものとは認められないとして、肖像権侵害に関するXらの主張を排斥した。

⑬ 最判平成20年 3 月 6 日民集62巻 3 号665頁⁽³⁴⁾**【事案の概要】**

本件は、Xらが、住民基本台帳ネットワークシステムにより行政機関がXらの個人情報を収集、管理又は利用することは、憲法13条により保障されたXらのプライバシー権その他の人格権を違法に侵害するものであると主張して、Xらの住民基本台帳を保管するYに対し、上記人格権に基づく妨害排除請求として、住民基本台帳からの各Xらの住民票コードの削除等を求めた事案である。

【判旨】

住民基本台帳ネットワークシステムにより行政機関が住民の本人確認情報を収集、管理又は利用する行為は、当該住民がこれに同意していないとしても、憲法13条の保障する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を侵害するものではない。

⑭ 大阪地判平成 6 年 4 月27日判タ860号160頁**【事案の概要】**

警察が、大阪市西成区の日雇労働者が多く居住する通称「あいりん地区」において、同地区の街頭防犯用の目的のためとして、15か所の交差点等の高所にテレビカメラ（合計15台）を設置し、西成警察署等においてモニターテレビに映像を映し出すなどして使用しているところ、同地区に居住又は勤務し、あるいは同地区において労働組合活動やボランティア活動等を行っている原告らが、このようなテレビカメラの設置及び使用は、原告らの「公権力から監視されない自由」等を侵すものなどとして、各テレビカメラの撤去及び慰謝料等の支払を求めた事案である。

【判旨】⁽³⁵⁾

本判決は、警察による情報収集活動は、特別の根拠規定がなくても警察法や警職法の当然予定するところであり、情報収集活動の一環としてテレビカメラを利用することも基本的には警察の裁量によるとしながら、同じく警察法や警職法が権限濫用の禁止や警察比例の原則にふれているように、国民の多種多様な権利・利益との関係で、警察権の行使にも自ずから限界があるうえ、密室性や高性能性、安価かつ大量の配置が容易などテレビカメラによる監視の特質にも配慮すべきであるから、その設置・使用にあたっては、(1) 目的が正当であること、(2) 客観的かつ具体的な必要性があること、(3) 設置状況が妥当であること、(4) 設置及び使用による効果があること、(5) 使用方法が相当であることなどが検討されるべきであるとする。

もっとも、このようなテレビカメラの設置・使用による被侵害法益には各種のもの（精神的な自由、経済的な自由、人格的な利益など）が想定され、より厳密にはこれら個々との関係で判断すべきであるから、右基準はむしろ事前の準則的な性格が強いものといえ、本判決も、具体的な権利・利益の侵

害の主張がある場合には、右各要件に留意しつつ、その権利・利益の性質等に応じ、侵害の有無や適法性について個別に検討されることになるとする。

そして、本判決は、以上のような観点から右各基準を検討し、本件テレビカメラの設置・使用は、個々のあるいは集団的な不法行為が行われやすい場所に設置されていること、それらを早期に把握し適切な対策を講じる必要があること、一元的かつ迅速な情報把握や管理は事態の収拾において効果があること、個人を識別・特定したうえで追跡的に監視するような使用がなされているとまでは認められないことなどを勘案して、概ねこれらを充たすものと判断している。

第5章 顔識別機能付きカメラシステムを利用する際の個人情報保護法上の留意点

本章では、顔識別機能付きカメラシステムの利用する際の個人情報保護法上の留意点やそれに関連する望ましい対応について述べる。

顔識別機能付きカメラシステムは、一般の被撮影者にとっては犯罪の予防という効果を受けられる一方で、顔識別機能付きカメラシステムによる個人情報の取扱いや仕組み等が広く認知されていないことにより、自らが不当に監視されているのではないかと不安を生じさせるおそれがある。

このような新技術の利活用を行うためには、社会からの理解を得ることが重要であるところ、顔識別機能付きカメラシステムに関与する事業者は、個人情報保護法に基づく義務を履行するのみならず、自ら情報発信して透明性を確保することが重要である。

透明性を確保することの意義として以下の3つが考えられる。

- ・被撮影者の過大な不安を誘発せず、理解や安心を得ること
- ・事業者が自らの個人情報の取扱いについて精査し、その適正さを検証する機会になること
- ・被撮影者が自らの個人情報の取り扱われ方を知り、開示等の請求や問合せをしたり、事業者の取組についての社会的評価を受けたりする契機になり、それらを通じてより適正な個人情報の取扱いが図られること

事業者は、上記透明性を確保することの意義を踏まえ、単に本報告書に記載した対応をそのまま実施したり、類似事例と同様の対応をするのではなく、個別具体的な事案に応じて透明性の確保や適正な運用のために必要な措置を講ずることが重要である。

なお、本章では据え付けられたカメラにより顔画像が取得される場合を想定しているが、ドローンやロボットに取り付けられたカメラ等の移動することができるカメラで顔識別機能付きカメラシステムを利用する場合であっても、検討の参考にすることができるものである。

1 顔識別機能付きカメラシステムの利用と個人情報保護法の適用について

カメラにより顔画像を撮影し、当該顔画像から顔特徴データを抽出することは個人情報の取扱いに当たる。これは、顔特徴データを抽出後、顔画像を直ちに破棄し、保存しない場合であっても同様である。

例えば、照合用データベースを下記「顔画像とそれに関する情報の例①」のように作成する

場合、特定の個人を識別することができる顔画像に付された発生日時や状況、特徴などの文字情報は、当該顔画像と合わせて全体として個人情報に該当する。

顔画像とそれに関する情報の例①

ID	顔画像	発生日時	状況	特徴
1		2021年 9月1日	ドアをこじ 開け立ち入 り禁止区域 に侵入した。	・男性 ・スーツ ・40代
...	...	...	...	...

なお、顔画像や顔特徴データと、発生日時や状況、特徴などといった文字情報をデータベースAとBで別々に管理した際であっても、下記「顔画像とそれに関する情報の例②」のように、データベースBに含まれる発生日時や状況、特徴単体だけでは特定の個人を識別することができないが、例えばIDを用いてデータベースAと容易に照合することができる場合には、特定の個人を識別することができることから、データベースBに含まれる情報も引き続き個人情報に該当する。この点については、事業者において特に誤りが生じやすいので注意が必要である。

顔画像とそれに関する情報の例②

データベースA		データベースB			
ID	顔画像	ID	発生日時	状況	特徴
1		1	2021年 9月1日	ドアをこじ 開け立ち入 り禁止区域 に侵入した。	・男性 ・スーツ ・40代
...	...	...	...	...	...

容易に照合
できる

←→

次に、顔画像や顔特徴データを体系的に構成して個人情報データベース等を構築した場合、当該個人情報データベース等を構成する個人情報は個人データに該当する。

照合用データベースは、顔特徴データを体系的に構成しているのであれば、個人情報データベース等に該当し、照合用データベースに登録された個人情報は、個人データに該当する。また、そのような照合用データベースから抜き出した一部の情報も個人データに該当する⁽³⁶⁾。

その場合、例えば、法第27条(個人データの第三者提供にかかる規律)等の規律が適用され、「発生日時」や「特徴」のみを第三者に提供する場合であっても、個人データの第三者提供として、法第27条に従って対応を行わなければならない。

2 利用目的の特定、通知公表及びその他の個人情報に係る規律

個人情報保護法上、個人情報を取り扱うに当たっては、その利用目的を特定し、通知又は公表しなければならない。また、適正な取得の観点から、カメラにより自らの個人情報が取得されていることを、被撮影者において容易に認識可能とするための措置を講じなければならない。

利用目的は、個人情報の取扱いに関する規律の要となるものであり、また、この義務は不必要に又はみだりに個人情報を取り扱うことを制限するとともに、個人情報の取扱いの透明性を確保し、被撮影者及び被撮影者になり得る者自らが権利利益の侵害を未然に防止するために必要な対応をとることができる環境を整備しようとするもので、重要な義務である。

そこで、本項では利用目的に関する規律を中心に、個人情報にかかる規律やそれに関連する望ましい対応について整理する。

(1) 利用目的の特定

法第17条第1項

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

個人情報取扱事業者は、個人情報を取り扱うに当たっては、利用目的をできる限り具体的に特定しなければならないが、利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定することが望ましい（通則ガイドライン3-1-1）。

特に、被撮影者から得た顔画像から顔特徴データを抽出して顔識別を行う場合、従来型防犯カメラと同様の外観であるにもかかわらず、顔特徴データを抽出してシステムで照合することにより、人が目視で確認するより検知精度が飛躍的に向上することで権利利益を侵害するおそれが高まっていることを踏まえながら、個人情報取扱事業者は、どのような取扱いが行われているかを本人が利用目的から合理的に予測・想定できる程度に利用目的を特定しなければならない。

このため、特定された利用目的から、本人が自らの個人情報がどのように取り扱われること

となるか合理的に予測・想定できるよう、防止したい事項等や顔識別機能を用いていることを明らかにすることで利用目的の特定を行わなければならない。

このうち、防止したい事項については、少なくとも「犯罪予防」、「行方不明者の捜索」等としなければならないが、例示として具体的な犯罪行為等の類型（例えばテロ防止、万引防止⁽³⁷⁾等）を示すことも考えられる⁽³⁸⁾。

(2) 利用目的等の通知公表等⁽³⁹⁾

法第21条第1項

個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表して
いる場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

顔識別機能付きカメラシステムを設置する場合、(1)で特定した利用目的を被撮影者に通知公表しなければならない。「公表」とは、不特定多数の人々が知ることができるように発表することであるところ、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならない。自社のホームページのトップページから1回程度の操作で到達できる場所への掲載とすることも考えられる（通則ガイドライン2-15）。

また、本人からの理解を得るためにも、できる限り分かりやすく情報提供を行うために、下記のとおり、Webサイト等における公表に加え、情報の重要度に応じて施設内での掲示も行うことが望ましい。

ア 施設内において掲示することが考えられる事項

施設内⁽⁴⁰⁾において掲示することが考えられる事項は、被撮影者が自己の個人情報を取り扱われるに当たり、特に認識しておくべき重要な事項である。そのため、被撮影者が容易に認識できる方法で掲示することが望ましい。例えば、別紙3の施設内での掲示例を参考に、デザインやフォントを工夫したり、アイコンやイラスト等を活用したりすることで被撮影者にとって分かりやすい方法で掲示したり、被撮影者の目線や動線を考慮し、人が出入りする際に目に付きやすい出入口（大規模施設で入口が複数ある場合には一定の大規模な入口）に掲示することが考えられる。また、カメラ画像の活用が多様化していることを考慮し、被撮影者にとってわかりやすいものとするのが望ましい⁽⁴¹⁾。

施設内での掲示事項例⁽⁴²⁾

- 顔識別機能付きカメラシステムの運用主体⁽⁴³⁾
- 顔識別機能付きカメラシステムで取り扱われる個人情報の利用目的
- 問合せ先⁽⁴⁴⁾
- 後述のWebサイトのURL及びQRコード等⁽⁴⁵⁾を掲示

イ Web サイト等に掲示することが考えられる事項

Web サイト等においては、法令上公表又は本人の知り得る状態に置かなければならない情報等のほか、顔識別機能付きカメラシステムによる個人情報の取扱いについて詳細な情報が知りたい被撮影者に対して、下記 Web サイト等に掲示することが考えられる事項等を利用目的の達成を妨げない範囲で公表することが考えられる（以下に示す事項が個人情報保護法の義務なのか、望ましい対応なのかは、別紙2を参照。）。

なお、これらの事項を施設内でアとは別に掲示することも考えられる。

Web サイト等への掲示事項例⁽⁴⁶⁾

- 顔識別機能付きカメラシステムを導入する必要性⁽⁴⁷⁾
- 顔識別機能付きカメラシステムの仕組み
- 顔識別機能付きカメラシステムで取り扱われる個人情報の利用目的⁽⁴⁸⁾
- 運用基準（登録基準、登録される情報の取得元、誤登録防止措置、保存期間等）
- 他の事業者への提供（委託、共同利用⁽⁴⁹⁾等）
- 安全管理措置⁽⁵⁰⁾
- 開示等の請求の手續、苦情申出先等⁽⁵¹⁾

(3) 不適正利用の防止及び適正取得のための態様⁽⁵²⁾

法第19条

個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

法第20条第1項

個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

ア カメラにより個人情報が取得されていることの表示

カメラにより特定の個人を識別できる顔画像を取得する場合、個人情報を取得することとなるため、偽りその他不正の手段による取得とならないよう、カメラが作動中であることを掲示する等、カメラにより自らの個人情報が取得されていることを、被撮影者において容易に認識可能とするための措置を講じなければならない。

特に小型カメラや電光掲示板等に内蔵したカメラ等、カメラが設置されていることが一見して分からない場合は、施設内での掲示等⁽⁵³⁾によって、カメラが作動中であることを、被撮影者において容易に認識可能とするための適切な措置を正当な理由なく講じなければ、偽りその他不正の手段による個人情報の取得に該当するおそれ（法第20条第1項）がある⁽⁵⁴⁾。

イ 差別的取扱いについて

法第19条は、個人情報保護法その他の法令に違反する行為、及び直ちに違法とはいえないものの、個人情報保護法その他の法令の制度趣旨又は公序良俗に反する等、社会通念上適正とは

認められない行為を助長し、又は誘発するおそれがある方法により個人情報を利用することを禁止している。

例えば、AIの学習内容によって、顔識別機能付きカメラシステムの被検知者が、性別の違いや肌の色の違いにより特定の属性の者に対して偏る等の不当な差別的取扱いは、法第19条違反になるおそれがある。

ウ 肖像権・プライバシー侵害への配慮

不適正利用の禁止や適正取得義務違反になるかを検討するに当たっては、防犯カメラの撮影にかかる肖像権やプライバシー侵害等の不法行為の成否を評価するに当たり考慮される要素は、考慮されるべきであると考えられる（第4章2）⁽⁵⁵⁾。

このため、第4章で示した考慮要素を参考にしながら法第19条及び法第20条第1項違反にならないよう留意することが必要である。

(4) 利用目的の通知公表等の例外

法第21条第4項

前三項の規定は、次に掲げる場合については、適用しない。

- 一 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- 二 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
- 三 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- 四 取得の状況からみて利用目的が明らかであると認められる場合

個人情報を取得した場合は、利用目的の通知公表の義務（法第21条第1項）があるが、法第21条第4項各号に該当する場合には、その義務が適用されない。

例えば、どのような防犯対策を行っているかが犯罪を行おうとする者に明らかになることにより防犯の目的が達成されず、施設の利用者の生命、身体、財産その他の権利利益を害するおそれがあったり、顔識別機能付きカメラシステムを利用する個人情報取扱事業者の権利又は正当な利益を害するおそれがあるときなど特別な事情がある場合は、法第21条第4項第1号及び第2号に基づき利用目的を公表する義務がないと考え得る⁽⁵⁶⁾。

しかし、当該条文は例外規定であり、その適用範囲は限定されるため、本条に基づき利用目的の通知公表を行わないこととするには、慎重な判断を要する。

(5) 要配慮個人情報について

法第2条第3項

この法律において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、**犯罪の経歴**、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報という。

施行令第2条

法第二条第三項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。

一 身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。

（略）

四 本人を被疑者又は被告人として、逮捕、搜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。

五 本人を少年法（昭和二十三年法律第百六十八号）第三条第一項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。

法第20条第2項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

（略）

二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

（略）

八 その他前各号に掲げる場合に準ずるものとして政令で定める場合

施行令第9条

法第二十条第二項第八号の政令で定める場合は、次に掲げる場合とする。

一 本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合

（略）

要配慮個人情報を取得する場合には、あらかじめ本人の同意を得なければならない（法第20条第2項）が、顔識別機能付きカメラシステムにおいて要配慮個人情報を取り扱うことが想定される。

まず、顔識別機能付きカメラにより撮影した画像に、犯罪行為が写りこむ可能性があるが、単に防犯カメラの映像等で、犯罪行為が疑われる映像が映ったのみでは、犯罪の経歴にも、刑事事件に関する手続が行われたことにも当たらないため、要配慮個人情報に該当しない。

照合用データベースに登録するために要配慮個人情報を取得する場合も、原則として、あらかじめ本人の同意を得なければならない（法第20条第2項）。ただし、その例外として、人の生命、身体又は財産の保護のために必要がある場合（法第20条第2項第2号）に該当することもあり得るが、これに該当するかは、慎重な判断を要する。

(6) 従来型防犯カメラについての考え方

従来型防犯カメラにより個人情報を取り扱っており、「取得の状況からみて利用目的が明らか」（法第21条第4項第4号）であることが認められる場合は、利用目的の通知公表は不要となる⁽⁵⁷⁾。

この場合であっても、防犯カメラが作動中であることを施設等の入口などに掲示する等、防犯カメラにより自らの個人情報が取得されていることを被撮影者において容易に認識可能となっていなければならない（法第20条第1項）。外観上カメラであることが明らかであり、個人情報が取得されていることが被撮影者において容易に認識可能な場合は、防犯カメラが作動中であることの掲示がなくとも法第20条第1項の求めを満たしているといえる。

なお、従来型防犯カメラを利用し、従来型防犯カメラとしての利用目的を特定している場合、事後的に顔特徴データを抽出し、他の情報と照合したり、分析することは、目的外利用⁽⁵⁸⁾に当たる。

3 運用基準の在り方及び当該内容に関する透明性の確保

法第22条

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

照合用データベースについては、システムの運用に先立ち明確な運用基準を定め、当該運用基準に従って運用することで、個人データを正確かつ最新の内容に保ち、利用する必要がなくなった個人データを遅滞なく消去するよう努めなければならない⁽⁵⁹⁾。

(1) 登録基準

照合用データベースに個人情報を登録するための登録基準を作成するに当たっては、対象とする犯罪行為等をあらかじめ明確にし、当該行為の性質に応じ、利用目的の達成のために必要最小限の範囲内の情報が登録されるような基準となるよう努めなければならない。

例えば、犯罪行為等の防止を目的とするときは、登録基準の内容（登録対象者）は、当該犯罪行為等を行う蓋然性が高い者に厳格に限定し、登録時にも当該犯罪行為等を行う蓋然性があることを厳格に判断することが望ましい。

また、不審な行動など特定の行動をもって登録する場合には、利用目的との関係で本来登録する必要がないにもかかわらず、身体的・精神的障害により特定の行動をとる者が登録されるおそれがある。仮に、特定の属性の者に対し、利用目的に照らして過大な不利益を課したりする等の不当な差別的取扱いが生じた場合、法第19条違反になり得るため、登録基準に差別的な取扱いを生じさせる原因がないか検証することが望ましい。また、利用目的との関係で本来登録する必要がない者の登録が生じた場合には、その原因が登録基準にないかについても検証を行うことが望ましい。

さらに、登録事務を行ういずれの担当者においても同様の判断を行うことができる統一的な基準を作成したり、当該基準に従って一定の運用を行うことができる体制を整備したりすることも重要である⁽⁶⁰⁾。

(2) 対応手順

検知対象者が検知された場合の適切な対応方法について手順を定め、当該手順に従って対応を行う体制を整備しておくことが望ましい。対応手順は、顔識別機能付きカメラシステムの利用により実現しようとする目的に対する警戒段階に応じ、複数作成しておくことも考えられる⁽⁶¹⁾。

また、顔識別機能付きカメラシステムは、あくまでも被撮影者と検知対象者の同一性を推測するものであることから（第3章1(1)参照）、被検知者が本当に検知対象者であるかを、システムだけでなく目視により確認するなど、慎重な対応をすることが望ましい。

(3) 保存期間

個人情報取扱事業者は、法第22条に基づき個人データをその利用目的を達成する範囲内において保有することとされている。そのため、利用目的の達成に必要な最小限の範囲内で保存期間を設定するよう努めなければならない。

顔識別機能付きカメラシステムでは以下ア、イの二つの個人情報を取得することが考えられる。それぞれについて、保存期間を設定する観点を示す。

ア 照合用データベースに登録した情報

保存期間を設定するに当たっては、対象とする犯罪行為等の再犯傾向や、登録対象者が再来訪するまでの一般的に想定される期間等を考慮することが考えられる。

また、複数の登録基準が設定されている場合、各基準の性質を考慮した保存期間をそれぞれ設定するよう努めなければならない。

イ 顔識別機能付きカメラで撮影した画像から抽出した顔特徴データで照合をした結果、検知対象者ではなかった者の情報

顔識別機能付きカメラで撮影した顔画像及び顔画像から抽出した顔特徴データのうち、検知対象者でない者の顔画像及び顔特徴データは、利用目的達成のために利用する必要がないと考えられるため、遅滞なく消去するよう努めなければならない。

(4) 登録消去

ア 保存期間満了時の対応

照合用データベースに登録された情報は、その情報が登録されている期間について管理をし、保存期間満了後に直ちに消去することを原則とし、保存期間を延長する場合は利用目的を達成するために必要な範囲に限るよう努めなければならない。

イ 保存期間中における登録要件の喪失への対応

保存期間中であっても、登録要件が喪失した場合には、当該登録情報は直ちに消去されるよう努めなければならない。そこで、登録消去の基準を設定し、登録要件を喪失した情報を直ちに消去するための体制を整えておくよう努めなければならない。

また、登録要件に関する情報が最新のものになっていることを担保できる仕組みを整えておくことが望ましい⁽⁶²⁾。

ウ 登録されたデータの検証

照合用データベースに登録された情報は、一定の期間ごとに、利用目的の達成に必要最小限の情報のみが登録されているか、保存期間が満了した情報や登録要件を喪失した情報及び誤登録された情報の消去が完了しているか等の検証を行うことが望ましい。

(5) 運用基準に関する透明性の確保

個人情報の適正な取扱いの観点から適正な運用基準を定めるとともに、運用基準についての透明性を確保することも望ましい。

運用基準を作成するに当たっては、肖像権・プライバシー、個人情報保護法や顔識別機能付きカメラシステムに関する専門的な知見を有する有識者等の意見を踏まえることが望ましい。

また、透明性の確保の観点から、運用基準について、Web サイト等に掲示することが考えられる。登録基準については、利用目的の達成を妨げない範囲で、どのような基準に該当する者が登録の対象となっているかや、登録される情報の取得元、誤登録防止措置、保存期間等を明らかにすることが望ましい。

4 安全管理措置

法第23条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

個人情報取扱事業者には、法第23条に基づき、個人データについて安全管理措置を講ずることが義務付けられている。カメラ画像や顔特徴データなどの個人データについては、当該個人データの漏えい、滅失又は毀損の防止その他の安全管理のために必要かつ適切な措置を講じる必要がある。具体的には組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置及び外的環境の把握を行う必要があり、例えば以下のような措置が考えられる。

① 組織的安全管理措置	カメラ画像や顔特徴データを取り扱う情報システムを使用できる従業員を限定、事業者内の責任者を定める、管理者及び情報の取扱いに関する規程等を整備、システムログその他の個人データの取扱いに係る記録の整備等を通じて個人データの取扱いの検証。等
② 人的安全管理措置	従業員に対する適切な研修（個人情報保護法の適用範囲・義務規定、カメラ画像や顔特徴データの取扱いに関する講義等）等を実施する。等
③ 物理的安全管理措置	カメラ及び画像データ・顔特徴データを保存する電子媒体等の盗難又は紛失等を防止するために、設置場所に応じた適切な安全管理を行う。等
④ 技術的安全管理措置	情報システムを使用してカメラ画像や顔特徴データを取り扱う場合や、IPカメラ（ネットワークカメラ、Webカメラ）のようにネットワークを介してカメラ画像等を取り扱う場合に、必要とされる当該システムへの技術的なアクセス制御や漏えい防止策等を講ずる（パスワード設定等の措置がアクセス制御に適切な場合はかかる措置も含む。）、アクセスログの取得分析により不正利用の有無を監視する。等
⑤ 外的環境の把握	外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講ずること。等 ⁽⁶³⁾

カメラ画像がデータベースを構築していない場合には、個人データとして法第23条の安全管理措置を講ずる義務が直接適用される対象ではないものの、当該画像が漏えい等することがないよう、上記の各種安全管理措置を参考として適切に取り扱うことが望ましい。

5 他の事業者等に対する個人データの提供

照合用データベースに登録された情報等の個人データを第三者に提供する場合、例外事由に該当しない限り、原則としてあらかじめ本人の同意を得なければならない。しかし、防犯目的で顔識別機能付きカメラシステムを利用する場合、かかる同意を取得することは困難であると想定される。

そこで、顔識別機能付きカメラシステムに係る個人データを提供できるのは、法第27条第1

項各号や、同第5項各号に該当する場合に限定される。この該当性や、そもそも個人データを提供する必要の有無については、慎重な判断を要する。

(1) 法令に基づく場合

法第27条第1項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一 法令に基づく場合
(略)

令状、捜査関係事項照会、弁護士会照会、法令に基づく調査等は、「法令に基づく場合」に該当するため、これらに応じて個人データを提供する際に、本人の同意を得る必要はない。

ただし、かかる請求や照会があった場合、顔特徴データは不変性が高く、追跡が可能となる情報であることに鑑み、特に照会事項と関係のない情報を提供することになっていないか等について個人情報取扱事業者自身が確認を行うことが重要である⁽⁶⁴⁾⁽⁶⁵⁾。

(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき及び公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

法第27条第1項

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

(略)
二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
(略)

人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるときや公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるときは、あらかじめ本人の同意を得ることなく個人データを第三者に提供することが可能である。

ただし、本号に基づく個人データの提供については、個別の提供行為ごとに本号の適用の可

否を判断しなければならない。あらかじめ、本号に基づき特定の場合に特定の者に対し、顔特徴データを提供することが想定されている場合は、具体的にどのような場合に本号を根拠に情報提供するかについて、事業者間で運用基準を定めておくことにより、恣意的な判断がなされないようにすることが望ましい。

(3) 委託

法第27条第5項

次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

一 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合

顔識別機能付きカメラシステムを利用する際、カメラ画像の分析やシステムの運用を、警備会社等の事業者委託することがあり得る。個人データの取扱いの全部又は一部を委託することに伴い、当該個人データが提供される場合は、当該提供先は第三者に該当しないため、あらかじめ本人の同意を得ることなく、個人データを提供することができる。

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない（法第25条）。

なお、委託元から委託先への監督義務を含め、顔識別機能付きカメラシステムについて委託を行う際の留意事項については、55頁（本誌209頁）以下も参照のこと。

(4) 共同利用

法第27条第5項

次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

（略）

三 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的並びに当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

複数の事業者間で被登録者の情報を共有する場合、共同利用により個人データを提供するこ

とが考えられる。この場合には、当該提供先は第三者に該当しないため、あらかじめ本人の同意を得ることなく、個人データを提供することができる。

顔特徴データの性質に鑑み、共同利用する者の範囲は、その範囲を同一業種内に限定したとしても、全国や、ある地域全体といった広い範囲で共同利用することが安易に認められるものではない。例えば、組織的な窃盗の防止を目的とする場合、盗難被害にあった商品や、当該商品に関する全国的あるいは地域全体における組織的な窃盗の発生状況をもとに、登録対象者が共同利用する者の範囲において同様の犯行を行うことの蓋然性を踏まえて、共同利用する者の範囲を利用目的の達成に照らして真に必要な範囲に限定することが適切であると考えられる。

また、共同利用を行う場合には、どの事業者においても同様の対応を行うことができる統一的な運用基準を作成し、登録情報などを含めて適切に管理することが望ましい。また、共同利用の目的は犯罪予防や安全確保に限り、他の目的で用いないようにすることが望ましい。

【一事業者内での個人データの取扱い範囲】

一事業者内のエリアが異なる複数の施設間で同じ登録情報を利用する場合も、利用目的の達成に照らして真に必要な範囲に限定した利用とすることが適切であると考えられる。

なお、安全管理措置義務（法第23条）においても、適切な範囲で個人データを取り扱うことが求められている。

6 保有個人データに係る情報の公表等及び開示等の請求や相談への対応

(1) 保有個人データについて

法第16条第4項

この章において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの以外のものをいう。

施行令第5条

法第十六条第四項の政令で定めるものは、次に掲げるものとする。

- 一 当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの
- 二 当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの
- 三 当該個人データの存否が明らかになることにより、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利を被るおそれがあるもの

四 当該個人データの存否が明らかになることにより、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

個人情報保護法においては、個人情報取扱事業者は、保有個人データに関する事項の公表をするとともに、本人から保有個人データの開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の請求（以下「開示等の請求」という。）を受けたときは、同法に従って、開示等の請求に応じなければならない。

保有個人データとは、個人データである照合用データベースに登録された情報等のうち、個人情報取扱事業者が開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことのできる権限を有するものであって、施行令第5条で定めるもの以外のものをいう。

なお、施行令第5条で定めるものとして、「当該個人データの存否が明らかになることにより、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの」（施行令第5条第1号）や「当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し、又は誘発するおそれがあるもの」（施行令第5条第2号）があり、これに当たる場合、保有個人データには該当しない。

例えば、テロ防止を目的としているとき、登録基準を施設内で危険物を所持している者と定め、登録時に被登録者が危険物を所持していることを少なくともカメラ画像を通じて確認し、危険物を所持しているという情報を取り扱っている場合には、上記各号により保有個人データに該当しないとも考えられる⁽⁶⁶⁾。

ただし、施行令第5条各号は例外的な場合であるため、慎重な判断を要する。

(2) 保有個人データに係る情報の公表等

法第32条第1項

個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

一 当該個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

二 全ての保有個人データの利用目的（第二十一条第四項第一号から第三号までに該当する場合を除く。）

三 次項の規定による求め又は次条第一項（同条第五項において準用する場合を含む。）、第三十四条第一項若しくは第三十五条第一項、第三項若しくは第五項の規定による請求に応じる手続（第三十八条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。）

四 前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

施行令第10条

法第三十二条第一項第四号の政令で定めるものは、次に掲げるものとする。

- 一 法第二十三条の規定により保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くことにより当該保有個人データの安全管理に支障を及ぼすおそれがあるものを除く。）
- 二 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
- 三 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

顔識別機能付きカメラシステムに係る情報が保有個人データであるとき、保有個人データに関する事項を、本人の知り得る状態に置かなければならない。例えば、Web サイトへの掲載を行っておくこと等が考えられる（2(2)イも参照のこと。）。

特に、開示等の請求に応じる手続については、具体的にどのような請求を行うことができるか及び手続の方法を、単に法令上の用語を用いるだけでなく、分かりやすく説明することが望ましい。例えば、「自分の個人データが照合用データベースに登録されているか確認することを請求できる」⁽⁶⁷⁾や「誤って照合用データベースに登録された自分の個人データを消去することを請求できる」⁽⁶⁸⁾のように示すことが考えられる。

また、(3)のように、当該本人が識別される保有個人データの特定に必要な事項として顔画像の提出を求める等、顔識別機能付きカメラシステムに特有の手続が必要となる場合は、特に手続の方法として示しておくことが望ましい。

(3) 開示等の請求や相談への対応**法第33条**

1 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の個人情報保護委員会規則で定める方法による開示を請求することができる。

2 個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、同項の規定により当該本人が請求した方法（当該方法による開示に多額の費用を要する場合その他の当該方法による開示が困難である場合にあっては、書面の交付による方法）により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

- 一 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
 - 二 当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
 - 三 他の法令に違反することとなる場合
- （略）

法第34条

1 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの内容が事実でないときは、当該保有個人データの内容の訂正、追加又は削除（以下この条において「訂正等」という。）を請求することができる。

2 個人情報取扱事業者は、前項の規定による請求を受けた場合には、その内容の訂正等に関して他の法令の規定により特別の手續が定められている場合を除き、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

（略）

法第35条

1 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第十八条若しくは第十九条の規定に違反して取り扱われているとき、又は第二十条の規定に違反して取得されたものであるときは、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を請求することができる。

2 個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第二十七条第一項又は第二十八条の規定に違反して第三者に提供されているときは、当該保有個人データの第三者への提供の停止を請求することができる。

4 個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

5 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る第二十六条第一項本文に規定する事態が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる。

6 個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない。

ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する場合その他の利用停止等又は第三者への提供の停止を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

(略)

法第40条

- 1 個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。
- 2 個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

個人情報取扱事業者は、原則として本人からの開示等の請求（開示、訂正等、利用停止等の請求）に応じなければならない。

一般に、照合用データベースには、照合に必要最小限の情報である顔特徴データしか含まれていない場合があり得る。こうした場合の対応として、例えば請求者に顔画像の提出を求め、当該顔画像から顔特徴データを抽出し、登録情報と照合するなどして開示等の請求に応じることが考えられる⁽⁶⁹⁾。

開示等の請求に応じる義務がない保有個人データ又は個人データ（法第33条第2項各号又は施行令第5条に該当する場合（6(1)参照）が生じることがあらかじめ想定される場合は、各条に該当する場合を整理して基準を定め、恣意的な運用がなされないようにしておくことが望ましい。

法令上の開示等の請求に該当しないような法令上対応する義務がない問合せについても、信頼醸成の観点から、できる限り丁寧に対応していくことが重要である。そのために開示等の請求への対応も含め、相談窓口を設置しておくことが望ましい。

また、自らの個人情報が誤登録されていると考える者から、開示等の請求やその他問合せがあった際に、請求者の請求に応じた対応や、誤登録の有無を直ちに確認し、誤登録の場合には消去するための体制をあらかじめ整えておくことが望ましい。

(参考) 顔識別機能付きカメラシステムに関する委託

本報告書が対象とする空間において顔識別機能付きカメラシステムを利用する場合、施設を運営する事業者（以下「施設運営事業者」という。）が顔識別機能付きカメラシステムの導入を決定した上、警備会社等にカメラ画像の分析やシステムの運用を委託する等、顔識別機能付きカメラシステムに関し個人データの取扱いを委託することが想定される⁽⁷⁰⁾。

この場合、本報告書で対応が望ましいと示す事項については、事業者間の個別の関係により対応は異なり得るが、対応が望ましいとする趣旨に合っている限り委託元と委託先のいずれの事業者が対応しても差し支えない。

本項では、本報告書で示す事項のうち、特に対応が複雑になると思われるものについて考え方を示す。

1. 利用目的等の通知公表等（2(2)参照）

2(2)アにおいて、施設内において掲示することが考えられる事項として①顔識別機能付きカメラシステムの運用主体、②顔識別機能付きカメラシステムで取り扱われる個人情報の利用目的、③問合せ先、④ Web サイトの URL 及び QR コード等を挙げた。

①について、委託の場合は委託元である施設運営事業者を運用主体として記載することになる。

②については、個人データの取扱いを委託しているか否かにかかわらず記載内容は同様である。

③については、当該顔識別機能付きカメラシステムについて実質的に応答できる者を記載することが望ましく、施設運営事業者か委託先の警備会社等のいずれでもよい。ただし、委託先の警備会社等を問合せ先とする場合、顔識別機能付きカメラシステムの運用について委託を受けていることを明らかにすることが望ましい。

④については、施設運営事業者の Web サイト等を示すことが望ましい⁽⁷¹⁾。

2. 運用基準の作成（3 参照）

運用基準はいずれの事業者が作成してもよいが、委託元である施設運営事業者が、最終的に確認して責任を持たなければならない。

3. 安全管理措置（4 参照）

法第25条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

委託元が個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない（法第25条）。

顔識別機能付きカメラシステムに関する個人データの取扱いを委託する場合、従来型防犯カメラとは異なる性質を有する個人データを取り扱っており、固有の留意事項があることを委託先と共有して、委託先に対する監督を行わなければならない。

4. 漏えい等報告

顔識別機能付きカメラシステムにおける個人データの漏えい等が生じた場合に個人情報保護委員会に報告しなければならない場合として、（１）要配慮個人情報が含まれる個人データの漏えい等、（２）不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（３）不正の目的をもって行われたおそれがある個人データの漏えい等、（４）個人データに係る本人の数が千人を超える漏えい等が発生した場合又は発生したおそれがある事態が生じた場合（以下「報告対象事態」という。）がある（法第26条第1項、規則第7条）。

施設運営事業者が警備会社等に委託を行っている場合、委託先である警備会社等は委託元である施設運営事業者に規則第8条第1項各号に定める事項を通知すれば、個人情報保護委員会への報告義務が免除される（法第26条第1項ただし書、規則第9条）。この場合、委託元である施設運営事業者が、個人情報保護委員会に対し報告を行わなければならない。なお、委託先である警備会社等が自ら個人情報保護委員会に報告を行った場合であっても、委託元である施設運営事業者も個人情報保護委員会への報告を行わなければならない。

なお、個人情報取扱事業者は報告対象事態を知ったときは、本人への通知を行わなければならない（法第26条第2項）。しかし、保有する個人データの中に本人の連絡先が含まれていない場合等、本人への通知が困難である場合は、事案の公表や問合せ窓口を用意してその連絡先を公表し、本人が自らの個人データが対象となっているか否かを確認できるようにすること等の本人の権利利益を保護するために必要な代替措置を講ずることによる対応が認められる（通則ガイドライン3-5-4-5）。

5. 開示等の請求への対応（6参照）

施設運営事業者が警備会社等に個人データの取扱いを委託している場合、開示等の請求に応じる権限は施設運営事業者が有していると考えられ、この場合、施設運営事業者が開示等の請求に応じなければならない。

第6章 事業者の自主的な取組として考えられる事項

近年、駅や列車内での事件が増加する中で、不特定多数の人が行き来する駅や空港などにおける安全への関心が高まっていること等により、今後、顔識別機能付きカメラシステムの利用ニーズが増えていくことが見込まれる。そのような中で、顔識別機能付きカメラシステムを導入しても、適正に個人情報が取り扱われ、個人の権利利益が保護されることや、導入の必要性等について被撮影者や社会から理解を得ることが重要となっている。

こうした観点から、本章においては、事業者の自主的な取組として考えられる事項について紹介する⁽⁷²⁾。

1 実現しようとする内容の明確化・適切な手段の選択

第3章1(2)及び(3)で述べたものをはじめ、犯罪予防や安全確保のために様々な手段がある。そこで、犯罪予防や安全確保のための方策を選定するに当たっては、実現しようとする内容を明確にして検討し、その内容に照らして必要かつ適切な手段を選択することが重要である。こうした観点から、以下の順に沿って検討することが望ましい。

(1) 実現しようとする内容の明確化

まず、犯罪予防や安全確保として実現しようとする内容を明確にする。このとき、抽象的に「犯罪予防」とするのではなく、具体的に特定することが望ましい⁽⁷³⁾。

(2) 重大性・緊急性の検討

実現しようとする内容で明確にした予防したい犯罪等の、当該施設や類似施設における発生実態（発生事実・可能性の有無、発生頻度、犯罪の態様）や被害が生じた場合の大きさ等の観点から重大性や緊急性を検討する。

(3) 有効な手段の検討

第3章1(2)及び(3)を参考に、実現しようとする内容や重大性・緊急性に照らして有効な手段をリストアップする。

(4) 適切な手段の選択

(3)でリストアップした手段の中から、実現しようとする内容を十分に実現でき、かつ個人の権利利益をより侵害しない適切な手段を選択する。

2 導入前の影響評価

不特定多数の者が出入りする大規模な空間に顔識別機能付きカメラシステムの導入を検討するに当たっては、企画・設計段階から導入に当たっての個人の権利利益の侵害リスクを把握し

て適切に対策を講じるためにも、システムの運用に伴い想定されるリスク要因や、被撮影者・被検知者の権利利益の侵害や差別的取扱いリスク等を考慮しながら影響評価を行うことが望ましい。

また、突然の導入に対する批判や、導入検討段階では想定していなかった問題が生じるおそれがあるため、一定期間を設けて試験的实施を行うことが望ましい。また、その結果も踏まえて再度影響評価を行ったり、リスク要因への対応を行うことが望ましい⁽⁷⁴⁾。

【PIA（Privacy Impact Assessment、個人情報保護評価・プライバシー影響評価）】

顔識別機能付きカメラシステムの利用は、個人情報保護法の遵守だけでなく、肖像権やプライバシー侵害についても留意を要する。そこで、事後における対症療法的な対応ではなく、個人情報等の保護を含む個人の権利利益の保護を事業の設計段階で組み込み、事業全体を通じて計画的にプライバシー保護の取組を実施する「プライバシー・バイ・デザイン」の考え方が重要である。それを実践する手法として、別紙2 顔識別機能付きカメラシステムの検討の観点リストを参考にしながら PIA を実施することが望ましい⁽⁷⁵⁾。

3 被撮影者への十分な説明

個人情報取扱事業者は、試験的实施の際やシステムの本格的な利用開始前からシステムを導入することについて広報を行うことが考えられる。

例えば、カメラを設置する施設にあらかじめ掲示を行うことや、HP 上で周知するなど様々な広報の手段を活用することが望ましい。

4 他の事業者との連携

他の事業者との連携を図ることによって、顔識別機能付きカメラシステムの必要性や有用性を広報するとともに、相互に導入事例の情報交換を行うことで知見を集積し、個々の事業者の取組の改善を行うことが望ましい。

また、認定個人情報保護団体の制度を活用して、業界全体として個人情報の適正な取扱いに取り組むことも期待される。

【認定個人情報保護団体】

認定個人情報保護団体とは、業界等の民間による個人情報の保護の推進を図るために、自主的な取組を行うことを目的として、個人情報保護委員会の認定を受けた民間団体である（法第47条第1項）。令和2年改正法により、事業者の特定分野（部門）を対象とする団体も認定を受けられることとなった（同条第2項）ところ、顔識別機能付きカメラシステムに関連する特定分野団体が設立されることも期待される。

認定個人情報保護団体においては、対象事業者から個別の事案について相談を受けることにより知見を集積し、さらに当該知見を対象事業者に還元していくことが期待される。具体

的には以下の役割が期待される⁽⁷⁶⁾。

- ① 自主ルールの整備⁽⁷⁷⁾
- ② 対象事業者が実施する PIA についての助言
- ③ 対象事業者における運用のチェック
- ④ 対象事業者における利害関係者への意見聴取や第三者委員会設置のサポート
- ⑤ 対象事業者による被撮影者等の対応（開示等の請求、苦情処理等）のサポート⁽⁷⁸⁾

5 導入後の検証

顔識別機能付きカメラシステムの利用開始後、運用基準に従って適切な運用が行われているか定期的に確認していくことが求められるが、顔識別機能付きカメラシステムの運用担当者以外の者による内部監査を行う体制も整えておくことが望ましい。これは、システムの規模や目的に応じて通常の業務監査やシステム監査の一環として行うことも考えられる⁽⁷⁹⁾⁽⁸⁰⁾。

別紙1：顔識別機能付きカメラシステムの利用を巡る国際的な議論

顔識別機能付きカメラシステムの利用を巡っては、国際的に様々な議論がなされているところ、ここでは概観について述べる（欧州の議論についての詳細は本検討会第5回資料2「欧州主要国における顔識別機能付カメラの利用に関する法制度の調査」⁽⁸¹⁾を参考にされたい。）。

EU一般データ保護規則（General Data Protection Regulation（GDPR））においては、生体データが特別なカテゴリーのデータとして位置づけられており、原則としてその処理が禁止されている（GDPR 第9条第1項）。ただし、「データ主体が物理的又は法的に同意を与えることができない場合で、データ主体又はその他の自然人の生命に関する利益を保護するために取扱いが必要となるとき」（GDPR 第9条第2項(c)）や、「求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める EU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合。」（GDPR 第9条第2項(g)）には生体データの処理を行うことができる例外とされている。

また、欧州委員会（European Commission）は、2021年4月、顔認識技術をも含む AI 技術の利用に関する規制案を公表し、現在 EU 内で審議中である。これは、AI 技術によってもたらされるリスクを①受諾不可、②高リスク、③低リスクに区分しリスクに応じた措置を要請する案となっている。ただし、①受諾不可に分類されているものは、公的空間での法執行目的の遠隔生体認証等（公的空間で犯罪捜査のためにリアルタイムで遠隔顔認識技術が使用される場合など）であり、②公共交通機関等で使用されるリアルタイム顔認識技術は高リスクに分類され、適合性評価といくつかの安全要件への準拠を条件として許可される可能性があると考えられている。

なお、英国一般データ保護規則（General Data Protection Regulation（英国 GDPR））においても、GDPR と同様に生体データの処理は原則として禁止されているが、同趣旨の例外が規定されている。

また、2022年10月に、世界プライバシー会議（Global Privacy Assembly（GPA））において「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」にかかる決議が行われた。この決議の中で推奨事項として6つの原則が示されている。具体的には、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。）である。これらの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されている。

別紙2：顔識別機能付きカメラシステムの検討の観点リスト

本報告書で紹介した検討の観点を以下に一覧する。なお、顔識別機能付きカメラシステムを導入するに当たり、下記に掲げる事項については、法令上義務付けられたものを除き、全て実施しなければならないわけではない。

また、下記に掲げていない事項を実施することが望ましい場合もあることに留意して、個別の事案に応じて各個人情報取扱事業者において実施すべき対応を検討することが重要である。

確認欄	対応事項	関連条文	関連箇所
システム導入前	適切な手段の検討		
	顔識別機能付きカメラシステムを導入して実現しようとする内容を明確にし、適切な手段であるかの検討	望ましい対応	第6章1
	利用目的の特定		
	利用目的の特定	法第17条第1項	第5章2(1)
	運用基準		
	登録基準の作成	法第22条（努力義務）	第5章3(1)
	・利用目的の達成のために必要最小限の情報が登録される基準か		
	・差別的取扱いを誘発する基準でないか	法第19条	第5章3(1)
	対応手順の作成	法第22条参照	第5章3(2)
	保存期間の定め	法第22条（努力義務）	第5章3(3)
	登録消去の基準の定め		第5章3(4)イ
	運用基準に従った対応が行われる体制の整備	法第22条、法第23条参照	第5章3(1)、(4)
	情報共有について		
	（法第27条第1項第2号又は第3号に基づき個人データの提供を行うことがあらかじめ想定されている場合）情報提供の運用基準を定めること	望ましい対応	第5章5(2)
	（登録情報を共有する場合）共有する範囲が利用目的の達成に照らして真に必要な範囲であることかの検討	法第27条第5項3号参照	第5章5(4)
	安全管理措置		
	安全管理措置を実施	法第23条	第5章4
	開示等の請求		
	開示等の請求等への対応窓口の設置、対応体制の整備	法第22条（努力義務）、法第33条～第40条参照	第5章6(3)
	その他		
	肖像権・プライバシー侵害の観点からの検討	法第19条、法第20条第1項参照	第5章2(3)ウ
	影響評価の実施	望ましい対応	第6章2
	被撮影者への十分な説明	望ましい対応	第6章3

	確認欄	対応事項	根拠条文	関連箇所
システム導入時	利用目的等の通知公表等			
		カメラにより個人情報を取得していることの 掲示又はカメラが作動していることが外観から 明らかになっている	法第20条第1項	第5章2(3)ア
		施設内に以下の事項の掲示を行った	望ましい対応	第5章2(2)ア
		・顔識別機能付きカメラシステムの運用 主体		
		・個人情報の利用目的		
		・問合せ先		
		・WebサイトのURL及びQRコード等		
		Webサイト等で以下の事項を公表した		第5章2(2)イ
		・顔識別機能付きカメラシステムを導入 する必要性	望ましい対応	
		・顔識別機能付きカメラシステムの仕組 み		
		・個人情報の利用目的	法第21条第1項、法第 32条第1項第2号	第5章2(2)イ
		・運用基準（登録基準、登録される情報 の取得元、誤登録防止措置、保存期間 等）	望ましい対応	第5章3
		・他の事業者への提供（委託、共同利用 等）	法第27条第5項第3号	第5章5(4)
		・安全管理措置	法第32条第1項第4 号、施行令第10条1号	第5章4、6(2)
		・開示等の請求に応じる手続	法第32条第1項第3号	第5章6(2)
システム導入後	運用基準			
		登録情報及び登録基準の検証を行った。		
		・保存期間満了、登録要件の喪失、誤登 録した登録情報の確認・消去	法第22条参照	第5章3(4)ウ
		・利用目的との関係で本来登録する必要 がない者を登録したことの原因が登録 基準にないかの検討		第5章3(1)
		保存期間が満了したもの及び登録要件を喪失 した登録情報並びに誤登録された情報の消去	法第22条（努力義務）	第5章3(4)ア、 イ
		内部監査等により運用基準に従って適切な運 用が行われているかの検証	望ましい対応	第6章5

別紙3：施設内での掲示案

顔 識 別 機 能 付 き
カ メ ラ シ ス テ ム
作 動 中

顔識別機能付き
カメラシステムにより
どのようなことが
行われているか
一見してわかるような図

犯罪予防のために顔識別機能付きカメラシステムを利用しています。

※取得した顔画像及びそこから抽出した顔特徴データについて、必要最小限の範囲内において、当社の照合用データベースに登録して利用します。

本件についての詳細は下記URL又はQRコードから当社ウェブサイトをご覧ください。

<https://△◇○△.com>

QR

お問合せ先 ○○株式会社お客様ご相談窓口
○○○@△△△

(参考資料) 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**1. 構成員****【構成員（五十音順）】**

生 貝 直 人	一橋大学大学院法学研究科准教授
石 井 夏生利	中央大学国際情報学部教授
遠 藤 史 啓	神奈川大学法学部准教授
菊 池 浩 明	明治大学総合数理学部専任教授
宍 戸 常 寿	東京大学大学院法学政治学研究科教授
新 保 史 生	慶應義塾大学総合政策学部教授
巽 智 彦	東京大学大学院法学政治学研究科准教授
星 周一郎	東京都立大学法学部教授
森 亮 二	英知法律事務所弁護士
山 本 龍 彦	慶應義塾大学大学院法務研究科教授

2. 議事内容**【第1回（令和4年1月28日(金)）】**

- ・顔識別機能付き防犯カメラの利用に関する法的整理＜事務局＞
- ・顔識別技術について＜日本電気株式会社＞

【第2回（令和4年3月9日(水)）】

- ・顔識別機能付き防犯カメラの特性に関する国内外の評価について＜事務局＞
- ・カメラ画像の利用に関する不法行為法上の評価について＜森構成員、遠藤構成員＞

【第3回（令和4年4月14日(木)）】

- ・これまでの検討事項についての振り返り
- ・プライバシー権からのコメント＜山本構成員＞
- ・渋谷書店万引対策共同プロジェクトの概要について＜全国万引犯罪防止機構＞
- ・認定個人情報保護団体の活動内容等について＜日本万引防止システム協会＞

【第4回（令和4年5月23日(月)）】

- ・防犯カメラに対する不安とその対策等について＜全国消費生活相談員協会＞
- ・防犯目的のためにカメラ設置する際に事業者へ求める事項について
＜日本消費生活アドバイザー・コンサルタント・相談員協会＞
- ・透明性の確保や説明責任に関する検討、検討会報告書の骨子案について＜事務局＞

【第5回（令和4年6月20日（月））】

- ・ 検討会報告書の素案について＜事務局＞
- ・ 欧州主要国における顔識別機能付カメラの利用に関する法制度の調査について
＜渥美坂井法律事務所・外国法共同事業＞

【第6回（令和4年9月7日（水））】

- ・ 検討会報告書のとりまとめに向けた論点整理

【第7回（令和4年12月22日（木））】

- ・ 検討会報告書（案）について

【注】

- (1) なお、顔識別機能付きカメラシステムについては、AI倫理等の課題も存在している。本報告書においては、第3章2(2)エで述べるほかは、第4章から第6章までで述べる観点を中心に検討することとする。
- (2) 顔識別機能付きカメラシステムを利用することによって取り扱う個人情報の項目は、顔画像及び顔特徴データに加えて、発生日時、内容、特徴などといった文字情報も考えられる。
- (3) なお、第5章2(6)は、従来型防犯カメラについても述べている。
- (4) 個人情報保護法上、顔画像や顔特徴データを取得する際に原則としてあらかじめ本人の同意を得る必要はない。
- (5) 本報告書が対象とするのは、顔識別機能付きカメラシステムを運用する者と当該システムで個人情報を取り扱われる者との間に関係性がなく、事前に同意を得ることが困難な場合を想定している。事前に同意を得ることが容易な場合として、例えば、事業所の入退館のために事前に本人の同意を取得して顔認証機能付きカメラシステムを利用する場合がある。
- (6) 安全確保とは、行方不明者等の搜索等個人の安全確保を想定している。
- (7) 商用目的での利用については「カメラ画像利活用ガイドブック ver3.0」(IoT推進コンソーシアム、総務省、経産省、2022年3月)(以下「カメラ画像利活用ガイドブック」という。)を参照することができる。なお、商用目的で設置したカメラを、犯罪予防や安全確保のために顔識別機能付きカメラシステムのために転用する場合は、本報告書の対象となる。
- (8) 法第58条参照
- (9) 行政機関が顔識別機能付きカメラシステムを利用するに当たっては、「個人情報等の適正な取扱いに関する政策の基本原則」(個人情報保護委員会、2022年5月)にも留意する必要がある。
- (10) ただし、不法行為法等との関係については個別の検討が必要である。
- (11) 被検知者と検知対象者の同一性を人が確認するために、顔特徴データだけでなく、顔画像を登録しているのが一般的である。
- (12) これらの対策が、顔識別機能付きカメラシステムの利用と比べ、必ず個人の権利利益を侵害するおそれが低いと示すものではない。
- (13) これらの対策は、映像分析技術と組み合わせて実施することも考えられる。
- (14) 記載に当たっては、以下の文献等を参考にした。
 - ・ カメラ画像利活用ガイドブック
 - ・ 「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扱いに関するガイドブック」(2020年3月、国土交通省)
 - ・ Information Commissioner's Office, "Information Commissioner's Opinion : The use of live facial recognition

technology in public places”, June 2021

- ・ Global Privacy Assembly, “Adopted Resolution On Facial Recognition Technology”, October 2020
- ・ European Data Protection Board, “Guidelines 3/2019 on processing of personal data through video devices”, January 2020
- ・ Commission Nationale de l’Informatique et des Libertés, “Reconnaissance faciale : pour un débat à la hauteur des enjeux”, novembre 2019

- (15) 以下の懸念点があるから、顔識別機能付きカメラシステムは利用すべきでないとするものではなく、これらの懸念点を踏まえた対応を第4章から第6章まで等を参考にしながら検討することが重要である。
- (16) 本項で紹介する活用事例であっても、個別の事情によっては、個人情報保護法違反や不法行為が成立するおそれがある。
- (17) なお、顔識別機能付きカメラシステムを商用目的で利用することもあり得るが、その場合の留意点について、カメラ画像利活用ガイドブックを参照することができる。
- (18) 本報告書において検討した裁判例は以下のとおり。
 - ① 最判昭和44年12月24日刑集23巻12号1625頁
 - ② 最判平成17年11月10日民集59巻9号2428頁
 - ③ 東京地判平成18年3月31日判タ1209号60頁
 - ④ 東京地判平成19年3月26日 LEX/DB28132442
 - ⑤ 東京地判平成21年5月11日判時2055号85頁
 - ⑥ 東京地判平成22年9月27日判タ1343号153頁
 - ⑦ 東京地判平成27年11月5日判タ1425号318頁
 - ⑧ 東京地判平成31年3月14日 LEX/DB25559868
 - ⑨ 名古屋地判令和元年9月5日 LEX/DB25564163
 - ⑩ 東京地判令和2年1月27日 LEX/DB25584266
 - ⑪ 最大判平成29年3月15日刑集71巻3号13頁
 - ⑫ 東京地判平成13年2月6日判時1748号144頁
 - ⑬ 最判平成20年3月6日民集62巻3号665頁
 - ⑭ 大阪地判平成6年4月27日判タ860号160頁
- (19) なお、事案の概要及び判旨は、本検討会での議論を踏まえ、個人情報保護委員会において、顔識別機能付きカメラシステムを利用する場合の肖像権・プライバシーの観点から留意点を整理するために判決文を一部抜粋又は要約したものであるため、詳細については判決文を参照されたい。
- (20) 海老原震一「判解」最判解刑事篇昭和44年度491頁
- (21) 本判例は、防犯カメラによる撮影ではなく、警察官によるカメラ撮影についての事案である。また、本判例では、上記自由を肖像権とは称していない。
- (22) ただし肖像権という語は用いられていない。
- (23) 本判例は、写真週刊誌のカメラマンが刑事事件の法廷において被疑者の容ぼう、姿態を撮影した行為が不法行為法上違法とされた事例である。
- (24) なお、脚注(8)の裁判例には、撮影が問題となった事案と撮影した画像が第三者に提供されたことが問題となった事案が含まれているが、本報告書では主に撮影についての考慮要素を整理する。
- (25) また、③は損害額の算定において、マスコミが防犯カメラにより撮影された画像を目的外利用に当たることを認識しながら記事に用いたことが、防犯カメラの目的外利用を助長及び促進させることとなる点で悪質だと指摘する。
- (26) これらの点について、防犯カメラや顔画像に関する事例ではなく、また、顔識別機能付きカメラシステムの利用においても直ちに適用されるものではないが、顔識別機能付きカメラシステムによる、追跡性について検討する際に参考になる裁判例がある。
 - ①最大判平成29年3月15日刑集71巻3号13頁は、捜査の一環として、約6か月半の間、被告人、共犯者のほか、

被告人の知人女性も使用する蓋然性があった自動車等合計19台に、同人らの承諾なく、かつ、令状を取得することなく、GPS 端末を取り付けた上、その所在を検索して移動状況を把握するという方法により行われた GPS 捜査が、強制処分当たるか争われた事案である。裁判所は「このような捜査手法は、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から、個人のプライバシーを侵害し得るものであり、また、そのような侵害を可能とする機器を個人の所持品に秘かに装着することによって行う点において、公道上の所在を肉眼で把握したりカメラで撮影したりするような手法とは異なり、公権力による私的領域への侵入を伴うものというべきである」と判示した。

また、⑫東京地判平成13年2月6日判時1748号144頁は、国が本全国の道路上に設置、管理している自動車ナンバー自動読み取りシステム（以下「Nシステム」という。）の端末によって、車両の搭乗者の容ぼう等が写っている可能性がある画像が撮影された上、車両ナンバープレートを判読されて、当該ナンバープレートの文字データとして抽出されたナンバーデータを記録、保存されたことについての事案であるが、裁判所は「Nシステムによって、走行車両のナンバーデータを記録、保存していることが、憲法一三条の趣旨に反して、原告らの権利もしくは私生活上の自由を違法に侵害するものとは認められない」と判断したが、その検討過程において「仮に、Nシステムの端末が道路上の至る所に張りめぐらされ、そこから得られる大量の情報が集積、保存されるような事態が生じれば、運転者の行動や私生活の内容を相当程度詳細に推測し得る情報となり、原告らの主張するような国民の行動に対する監視の問題すら生じ得るという点で、Nシステムによって得られる情報が、目的や方法の如何を一切問わず収集の許される情報とはいえないことも明らかである」と指摘した。

データベースの管理に関する判例として、最判平成20年3月6日民集62巻3号665頁がある。

- (27) 「パーソナルデータの利活用に関する制度改正大綱」（平成26年6月24日、IT 総合戦略本部決定）
- (28) 判タ242号119頁
- (29) 海老原震一「判解」最判解刑事篇昭和44年度491頁
- (30) 民集59巻9号2428頁
- (31) ③から⑩までの事案の概要及び判旨は、本検討会第2回資料3 遠藤史啓構成員「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資料（2022.3.09）」をもとに作成した。
- (32) 刑集71巻3号13頁
- (33) 判時1748号145頁
- (34) 民集62巻3号665頁
- (35) 判タ860号160頁
- (36) 被害日時、被害商品、犯行が疑われる者の特徴、車両ナンバーなどのそれ単体では特定の個人を識別することができない情報であっても個人データに該当する。
- (37) 犯罪行為等の類型を例示するに当たっては、刑事法上の犯罪名である必要はなく、どのような犯罪行為等を念頭に顔識別機能付きカメラシステムが利用されているかを、被撮影者が認識できるように示すことが望ましい。なお、第6章3において述べるとおり、顔識別機能付きカメラシステムを利用する必要性についての広報を行うことが望ましい。このような広報も含め、被撮影者が自らの個人情報が取り扱われることを理解できるような対応を行うことが重要である。
- (38) なお、顔識別機能付きカメラシステムにおいては、カメラの撮影により取得した顔画像、そこから抽出した顔特徴データと、照合用データベースに登録された顔特徴データが取り扱われる。照合用データベースに登録された顔特徴データには、カメラの撮影により取得した顔画像から抽出したものと、他のデータベース（例えば報道等）から取得した顔画像から抽出した顔特徴データが含まれる。これらの個人情報それぞれについて利用目的を検討しなければならない。ただし、検討の結果、利用目的がいずれも同様に特定されることもあり得る。
- (39) なお、本項で述べる事項と個人情報保護法の適用関係については、別紙2 顔識別機能付きカメラシステムの検討の観点リストも参照されたい。
- (40) 被撮影者が撮影前に掲示を目にする可能性のある場所（例えば、大規模な入口等）での掲示を望ましいとするものであって、施設内であればどこで掲示してもよいというものではない。また、カメラの設置場所での掲示を妨げるものではない。

- (41) 設置されているカメラによって取得した顔画像及びそこから抽出した顔特徴データ（個人情報／個人識別符号）を、取得後に直ちに廃棄する等してデータベースとして保有していないのか（例えば、属性や人流の分析等）、データベースとして保有する（原則として保有個人データになる）かがわかるように記載することも考えられる。
- (42) 掲示場所を施設内とすること自体は義務ではなく望ましい対応であるものの、通常、顔識別機能付きカメラシステムの運用主体及び問合せ先に当たる事項は、法第32条第1項第1号及び第3号に基づき、本人の知り得る状態に置かなければならず、カメラ画像及び顔特徴データの利用目的は、法第21条第1項に基づき、本人に通知又は公表しなければならない。
- (43) 法第32条第1項第1号は「当該個人情報取扱事業者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名」を本人の知り得る状態に置かなければならないとするが、施設内における掲示では、個人情報取扱事業者の名称等、顔識別機能付きカメラシステムの運用主体が誰か分かる程度の情報を明らかにすることを望ましいとするものである。
- (44) 施設内の掲示自体に問合せ先を記載しない場合であっても、問合せ先が記載された Web サイトの QR コード等を掲示する等、問合せをしたい者が容易に問合せを行うことができる情報を記載しておくことが望ましい。
- (45) 当該 Web サイトに容易にアクセスすることができる手段であればよく、当該 Web サイトを容易に検索することができるキーワードを示すことも考えられる。
- (46) これらのほか、マーケティング目的で利用していないこと、法第27条第1項各号に該当する場合等を除き第三者提供を行っていないこと及び検知されても直ちに退去を求めることはないこと等、被撮影者の不安を取り除くために有益な情報を記載することも考えられる。
- (47) 第6章1で検討した事項等を参考に記載することが考えられる。
- (48) 法第21条第1項に基づき、本人に通知し、又は公表しなければならない。
- (49) 法第27条第5項第3号に基づき、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。
- (50) 法第32条第1項第4号及び施行令第10条第1号に基づき、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
- (51) 法第32条第1項第3号並びに法第32条第1項第4号及び施行令第10条第2号、同条第3号に基づき、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。
- (52) 不当な差別的取扱いを生じさせ得る運用基準については、3(1)も参照のこと。
- (53) 利用目的等の通知公表等を実施内で行うことにより、本条との関係でも義務を果たすことができる。掲示の具体的方法は、(2)アと同様に考えることができる。
- (54) 外観上カメラであることが明らかであり、個人情報が取得されていることが被撮影者において容易に認識可能な場合は、カメラが作動中であることの掲示等を行わなくとも、法第20条第1項の求めは満たしている。他方、顔識別機能付きカメラシステムを利用する場合、外観上カメラであることがわかるか否かにかかわらず、(2)アのとおり施設内において顔識別機能付きカメラシステムに関する掲示を行うことが望ましい。
- (55) 例えば、撮影の場所に関してはトイレや更衣室など通常撮影されることが想定されないような場所にカメラを設置して撮影することや、商用的な観点から特定の個人を追跡して監視する場合には法第19条及び法第20条第1項違反になり得る。
- (56) なお、顔識別機能付きカメラシステムにより個人情報を取り扱う場合は、取得の状況からみて利用目的が明らかであるとは認められない（法第21条第4項第4号）。
- (57) 今後、従来型防犯カメラ以外の機能を有する防犯カメラの普及や、防犯以外の目的で利用されるカメラの普及によっては、従来型防犯カメラにより個人情報を取り扱うことが「取得の状況からみて利用目的が明らか」（法第21条第4項第4号）と言えなくなる可能性がある。また、顔特徴データの抽出を想定しない場合であっても、どのようなカメラが設置され、どのような運用がなされているのか被撮影者が理解できるようにするために、カメラの性質や、利用目的、取得する情報等について掲示を行うことが考えられる。
- (58) 目的外利用を行う場合には、原則として、あらかじめ本人の同意を得なければならない（法第18条第1項）。ただし、その例外として、法令に基づく場合や、人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき等は、本人の同意は不要である（法第18条第3項）。

- (59) なお、一定の刑事手続を受けた者を照合用データベースに登録する場合は、被登録者の更生を妨げないように適切な保存期間となるように考慮することも望ましいと考えられる。
- (60) 共同利用の場合において、共同利用する者のいずれもが同様の判断ができるように登録基準を作成し、体制を整備することが望ましいことについて、5(4)も参照のこと。
- (61) 例えば、テロ防止を目的とする場合、大規模イベントや外国の要人が来日する等の強い警戒が必要と考えられる場合と、平時でそれぞれ対応手順を作成しておくことが考えられる。
- (62) 例えば、ある施設において犯罪行為を行った疑いで刑事手続を受けた者を登録要件とする場合において、当該登録者が犯罪行為を行ったとはいえないと判断されたときは、登録要件は喪失していることとなる。そのような登録要件に係る最新情報を収集する仕組みを担保することが望ましい。
- (63) なお、一部の事業者によれば、駅や空港等に設置した顔識別機能付きカメラシステムに関する個人情報はローカルネットワークにおいて取り扱われていることが多く、外国において取り扱われることはセキュリティ面で大きなリスクがあるとのことである。
- (64) 弁護士会からの照会請求に対して、行政区長が前科及び犯罪経歴等を回答した最判昭和56年4月14日民集第35巻3号620頁のように、弁護士会照会に応じて前科及び犯罪経歴等を第三者に提供した場合であっても、不法行為が成立した事例がある。
- (65) なお、顔識別機能付きカメラで単に撮影した映像を本号に基づき提供する場合は、従来型防犯カメラにより撮影した映像を本号に基づき提供する場合と同様である。
- (66) なお、保有個人データに該当しない個人データについて開示等の請求があった場合、本人に対しては、保有個人データが存在しない旨を通知することになる（Q&A9-15参照）。
- (67) 法第33条第1項に基づく開示請求として、このような請求ができる。
- (68) 法第35条第5項に基づき、「本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合」の利用停止等請求として、このような請求ができる。
- (69) 顔特徴データのみ保有している場合には、当該顔特徴データをもとに、開示等の請求に応じられるよう対応することが望ましいと示すものである。犯罪予防や安全確保のために必要がないにもかかわらず、開示等の請求に応じる目的のためだけに、顔特徴データ以外の情報（例えば氏名等）を取得、保有することを求めるものではない。
- (70) 顔識別機能付きカメラシステムの運用について警備会社等に委託している場合、少なくとも委託元である施設運営事業者と委託先である警備会社等がいずれも登録情報を閲覧できる場合が多いと思われる。この場合、個人データの取扱いを委託しているといえ、法第25条及び法第27条第5項第1号が適用される。
- (71) なお、利用目的の通知公表義務（法第21条第1項）は、委託元及び委託先のいずれもが負う。
- (72) 個人情報保護委員会においても、本章で述べる事項が普及するよう取り組みを進めることが重要である。
- (73) 例えば、常習性の高い犯罪と、常習性は低いが甚大な被害が予想される犯罪では、その予防のために用いるべき手段も異なり得る。
- (74) 特に、これまで他の事業者においても行われていなかったような新規性がある事案については、第三者委員会を設置することも考えられる。
- (75) 「PIAの取組の推進について—PIAの意義と実施手順に沿った留意点—」（2021年6月、個人情報保護委員会）（https://www.ppc.go.jp/files/pdf/pia_promotion.pdf）も参照のこと。
- (76) 「個人情報の保護に関する基本方針」6(3)（2022年4月1日閣議決定）も参照のこと。
- (77) 認定個人情報保護団体は、個人情報保護指針を作成するよう努めなければならない（法第54条第1項）。なお、ここでいう自主ルールは個人情報保護指針でなくてもよい。
- (78) 対象事業者は被撮影者からの開示等の請求や苦情に対して真摯に対応することが求められるが、対応が困難な者からの請求等も想定される。このような者への対応が事業者にとって過度な負担となり、問合せ対応自体を忌避することにならないよう、対応のための専門的な知見の提供等の対応支援をすることも重要である。
- (79) 導入前の影響評価と同様、特に、これまで他の事業者においても行われていなかったような新規性がある事案については、第三者委員会を設置することも考えられる。
- (80) 特に大規模な駅や空港等で顔識別機能付きカメラシステムを利用する場合は、他の代替手段を選択することが困

難であり生活に不可欠な空間であることや、また、個人情報を大規模かつ網羅的に取得することが可能であることに鑑み、透明性レポートを作成・公表することも考えられる。透明性レポートとは、法第27条第1項第1号等に基づき本人の同意なく個人データの提供を行った場合の透明性を図るために作成するレポートであり、法令に基づき個人データの提供を求められた件数や、求めに応じ個人データの提供を行った件数のほか、顔識別機能付きカメラシステムによる効果等を公表することが考えられる。

- (81) 同資料は、渥美坂井法律事務所・外国法共同事業「欧州主要国における顔識別機能付カメラの利用に関する法制度に関する調査」(2022年3月)

(https://www.ppc.go.jp/files/pdf/major_european_countries_camera_report_R403.pdf) に基づき報告されたものであり、令和4年3月31日時点の情報である。