

「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の更新

令和5年3月30日に「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」を公表したこと等を踏まえて、『「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』について、以下のとおり更新いたしました。

1 ガイドライン（通則編）

1-1 定義

（個人情報）

Q 1-412 カメラ画像から抽出した性別や年齢といった属性情報や、人物を全身のシルエット画像等に置き換えて作成した店舗等における移動軌跡データ（人流データ）は、個人情報に該当しますか。

A 1-412 個人情報とは、特定の個人を識別することができる情報をいいます。性別や年齢といった属性情報や、又は全身のシルエット画像等に置き換えて作成した店舗等における移動軌跡データ（人流データ）のみであれば、抽出元の本人を判別可能なカメラ画像や個人識別符号等特定の個人本人を識別することができる情報と容易に照合することができる場合を除き、個人情報には該当しません。

（令和5年5月更新）

（個人情報）

Q 1-13 店舗や、駅・空港等に従来型防犯カメラ（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）を設置し、撮影したカメラ画像を防犯目的で利用することを考えています。個人情報保護法との関係で、どのような点に留意する必要がありますか。

A 1-13 個人情報取扱事業者は、カメラにより特定の個人を識別することができる画像を取得する場合、個人情報を取り扱うことになるため、利用目的をできる限り特定し、当該利用目的の範囲内でカメラ画像を利用しなければなりません。

また、個人情報の利用目的を本人に通知し、又は公表しなければなりません。カメラの設置状況等から利用目的が防犯目的であることが明らかである場合には、「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」（法第21条第4項第4号）に当たり、利用目的の通知・公表は不要と考えられます。

さらに、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ため、カメラの設置状況等から、カメラにより自らの個人情報が取得されていることを本人において容易に認識可能といえない場合には、容易に認識可能とするための措置を講じなければなりません（法第20条第1項）。例えば、防犯カメラが作動中であることを店舗や駅・空港等の入口や、カメラの設置場所等に掲示する等の措置を講じることが考えられます。また、外観上、カメラであることが明らかである等、カメラにより自らの個人情報が取得されていることを本人において容易に認識可能であったとしても、上記例で示した掲示等の措置を講じることにより、より容易に認識可能とすることが望ましいと考えられます。

（令和5年5月追加）

（個人情報）

Q1-1214 店舗や、駅・空港等に防犯カメラを設置し、撮影したカメラにより画像やを取得し、そこから得られた顔認証特徴データを抽出して、これを防犯目的で利用する（顔識別機能付きカメラシステムを利用する。）ことを考えています。個人情報保護法との関係で、どのような措置を講ずる従来型防犯カメラを利用する場合の留意点（Q1-13）に加えて、どのような点に留意する必要があるですか。

A1-1214 個人情報取扱事業者は、顔識別機能付きカメラシステムにより特定の個人本人を判別可能な識別することができるカメラ画像やそこから得られた顔認証特徴データを取り扱う場合、個人情報を取り扱うことになるため、利用目的をできる限り特定し、当該利用目的の範囲内でカメラ画像や顔特徴認証データ等を利用しなければなりません。また、個人情報の利用目的をあらかじめ公表するか、又は個人情報の取得後速やかに本人に通知若しくは公表する必要があります。

具体的には、店舗等に設置した防犯カメラによりカメラ画像を取得し、そこから顔認証データを抽出してこれを防犯目的で利用する場合、本人においてかかる取扱いが行われるとは合理的に予測・想定できないと考えられ、また、顔認証データはマーケティング等他の目的にも利用され得る個人情報であることから、防犯のためにカメラ画像及び顔認証技術を用いた顔認証データの取扱いが行われることを本人が予測・想定できるように利用目的を特定し、これをあらかじめ公表又はその取得後速やかに通知・公表する必要があると考えられます。具体的には、どのような個人情報の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ため、従来型防犯カメラの場合と異なり、犯罪防止目的であることだけでなく、顔識別機能を用いていることも明らかにして、利用目的を特定しなければなりません。

また、防犯カメラが作動中であることを店舗等の入口や設置場所等に掲示する等、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本人において容易に認識可能とするための措置を講ずる必要があります。顔識別機能付きカメラシステムを利用する場合

は、設置されたカメラの外観等から犯罪防止目的で顔識別機能が用いられていることを認識することが困難であるため、「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」(法第 21 条第 4 項第 4 号) に当たらず、個人情報の利用目的を本人に通知し、又は公表しなければなりません。また、顔識別機能付きカメラシステムに登録された顔特徴データ等が保有個人データに該当する場合には、保有個人データに関する事項の公表等 (法第 32 条) をしなければなりません。なお、法第 20 条第 1 項に関する留意点は Q 1-13 のとおりです。

加えて、上記のとおり利用目的の通知・公表をしなければならず、また、本人から理解を得るためできる限り分かりやすく情報提供を行うため、顔識別機能付きカメラシステムの運用主体、同システムで取り扱われる個人情報さらに、カメラ画像の取得主体、カメラ画像の内容、カメラ画像及び顔認証データの利用目的、問い合わせ先等を本人が確認できるよう、これらを店舗等の入口や設置場所等に明示するか、又は、これら、さらに詳細な情報を掲載した WEBWeb サイトの URL 又は QR コード等を示す店舗や駅・空港等の入口や、カメラの設置場所等に掲示することが望ましいと考えられます。

カメラ画像や顔認証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、個々のカメラ画像や顔認証データを含む情報は個人データに該当するため、個人情報保護法に基づく適切な取扱いが必要です。

なお、カメラ画像を取得してこれを防犯目的のみに利用し、顔認証データは取り扱わない、従来型の防犯カメラの場合には、「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) であることから、利用目的の通知・公表は不要と考えられますが、かかる場合であっても、防犯カメラが作動中であることを店舗等の入口や設置場所等に掲示する等、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本人において容易に認識可能とするための措置を講ずることが望ましいと考えられます。

—さらに、照合のためのデータベース (検知対象者のデータベース) 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、利用目的の達成に必要な範囲を超えて、個人情報が登録されることのないような登録基準としなければなりません (法第 18 条第 1 項)。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と考えられます。また、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文書化された統一的な基準を作成するとともに、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することも重要です。

駅・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については、「犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について」（個人情報保護委員会、2023年3月）も参照のこと。

（令和4.5年4.5月更新）

（個人情報）

Q 1 - ~~13~~15 防犯目的のために取得したカメラ画像やそこから得られた顔認証特徴データをマーケティング等の商業目的に利用することを考えています。個人情報保護法との関係で、どのような措置を講ずる必要がありますか。

A 1 - ~~13~~15 当初防犯目的のために取得したカメラ画像やそこから得られた顔認証特徴データを、マーケティング等の商業目的のために利用する場合には、あらかじめ本人の同意を得なければなりません（法第18条第1項）。

なお、当初から商業目的のためにカメラ画像や顔認証特徴データを取得する場合については、Q 1 - ~~12~~13、Q 1 - 14 及び Q 1 - 16 を参照のこと。

（令和3.5年9.5月更新）

~~（個人情報）~~

~~Q 1 - 15 防犯目的のために、万引き・窃盗等の犯罪行為や迷惑行為に対象を限定した上で、顔認証システムを導入しようとする場合にどのような注意が必要とされますか。~~

~~A 1 - 15 本人を判別可能なカメラ画像や顔認証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、個々のカメラ画像や顔認証データを含む情報は個人データに該当するため、個人情報保護法に基づく適切な取扱いが必要です。~~

~~防犯目的のために、万引き・窃盗等の犯罪行為や迷惑行為に対象を限定した上で、顔認証システムを導入して顔認証データを含む個人データを用いようとする場合には、特定された利用目的の達成のために必要最小限の範囲内において顔認証システムへの登録を行い、個人データを正確かつ最新の内容に保つ必要があります。~~

~~具体的には、各事業者においてどのような基準でデータベースに登録するか社内ルールを設定し、誤登録等を防ぐための適切な措置として、例えば被害届の有無により判断を行うなど客観的に犯罪・迷惑行為が確認されるケース等に限定するとともに、事業者内で責任を有する者により登録の必要性和正確性について確認が行われる体制を整えること等が重要です。~~

~~（令和3年9月更新）~~

(個人情報)

Q 1-16 電光掲示板等に内蔵したカメラで撮影した本人の顔画像から、性別や年齢といった属性情報を抽出し、当該本人向けにカスタマイズした広告を電光掲示板等に表示しています。属性情報を抽出した後、顔画像は即座に削除しています。個人情報保護法上、どのような措置を講ずる必要がありますか。

A 1-16 個人情報取扱事業者は、カメラにより特定の個人を識別することが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り取得してはなりません。そのため、カメラの設置状況等から、カメラにより自らの個人情報が取得されていることを本人において容易に認識可能といえない場合には、容易に認識可能とするための措置を講じなければなりません。一般に、電光掲示板等に内蔵したカメラで撮影する場合には、掲示等がなければ、自らの個人情報が取得されていることを本人において容易に認識可能といえないと考えられるため、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本人において容易に認識可能とするための措置を講ずる必要がありますと講ずる必要がありません。

また、個人情報取扱事業者が、一連の取扱いにおいて、特定の個人を識別することができる顔画像を取得した後、顔画像から属性情報を抽出した上で、当該属性情報に基づき当該本人向けに直接カスタマイズした広告を配信する場合、当該顔画像を直ちに削除廃棄したとしても、個人情報を取り扱って当該顔画像について、特定の個人を識別した上で、広告配信を行っていると解されます。このため、個人情報取扱事業者は、顔画像から抽出した属性情報に基づき広告配信が行われることを本人が予測・想定できるように利用目的を特定し、これを通知・公表するとともに、当該利用目的の範囲内で顔画像を利用しなければなりません。

(令和3年5月更新)

(個人情報データベース等)

Q 1-41 防犯カメラやビデオカメラなどで記録された映像情報は、特定の個人を識別することが本人が判別できる映像であれば、個人情報データベース等に該当しますか。

A 1-41 本人が判別特定の個人を識別することができる映像情報であれば、個人情報に該当しますが、特定の個人情報を検索することができるように「体系的に構成」されたものでない限り、個人情報データベース等には該当しないと解されます。すなわち、記録した日時について検索することは可能であっても、特定の個人に係る映像情報について検索することができない場合には、個人情報データベース等には該当しないと解されます。

(令和5年5月更新)

1-5 個人データの管理（法第 22 条～第 25 条関係）

（データ内容の正確性の確保等）

Q 5-4 防犯カメラにおけるカメラ画像や顔認証特徴データ等などの個人データの保有期間についてはどのように考えれば良いですか。

A 5-4 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おり、その保有期間については、利用する必要がある最小限の期間とする必要があります。利用目的の達成に必要な範囲内において、保存期間の設定等を行う必要があります。利用の必要性を考慮して保存期間を設定し、個人データを利用する必要がなくなったときは、遅滞なく消去するよう努めなければなりません。

（令和 5-3年 5-9月更新）

1-7 個人データの第三者への提供（法第 27 条～第 30 条関係）

（第三者に該当しない場合）

Q 7-50 防犯目的のために取得したカメラ画像・顔認証特徴データ等について、防犯目的の達成に照らして真に必要な範囲内で共同利用をすることは可能ですか。その場合には、どのような点に注意する必要がありますか。

A 7-50 一般に個人データを共同利用しようとする場合には、法第 27 条第 5 項第 3 号に基づき、①共同利用をする旨、②共同して利用される個人データの項目、③共同して利用する者の範囲、④利用する者の利用目的、⑤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、その代表者の氏名をあらかじめ本人に通知又は容易に知りうる状態に置かなければなりません。

防犯目的のために取得したカメラ画像・顔認証特徴データ等を共同利用しようとする場合には、共同利用されるカメラ画像・顔認証特徴データ等の範囲や、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ます。防犯目的の達成に照らし、共同利用される個人データを必要な範囲に限定することを確保する観点からは、例えば共同利用するデータベースへの登録条件を整備して犯罪行為や迷惑行為に関わらない者の情報については登録・共有しないことが必要です。例えば、カメラ画像・顔特徴データ等を、組織的な窃盗の防止を目的として共同利用する場合、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、共同利用されるカメラ画像・顔特徴データ等の範囲や、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ます。

また、共同利用は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することを認める制度です。このため、共同利用する者の範囲は、本人がどの事業者まで現在あるいは将来利用されるか判断できる程度に明確にする必要があります。

さらに、個人データの開示等の請求及び苦情を受け付けその処理に尽力するとともに、個人データの内容等について開示、訂正、利用停止等の権限を有し安全管理等個人データの管理について責任を有する管理責任者を明確に定めて、必要な対応を行うことが求められます。

加えて、カメラ画像・顔特徴データ等を共同利用する場合には、共同利用する全ての者が同様の取扱いを行うための統一的な運用基準（登録基準や保存期間等）を作成することが望ましいと考えられます。共同利用するカメラ画像・顔特徴データ等の登録基準については、Q1-14を参照のこと。

（令和5-3年9-5月更新）

1-9 保有個人データに関する事項の公表等、保有個人データの開示・訂正等・利用停止等（法第32条～第39条関係）、個人情報取扱いに関する苦情処理（法第40条関係）

（保有個人データの開示）

Q9-13 防犯目的のために、万引き・窃盗等の犯罪行為や迷惑行為に対象を限定した上で、顔識別機能付きカメラシステム等に顔認証特徴データ等を登録して保有個人データとした場合には、個人情報保護法に基づきどのように開示請求、内容の訂正、利用停止の請求等に対応する必要がありますか。

A9-13 防犯目的のために顔識別機能付きカメラシステム等に登録された顔認証特徴データ等が保有個人データであるに該当する場合、法令に基づき開示請求等に適切に対応する必要がありませんしなればなりません。すなわち、開示請求がなされた場合には、保有個人データの開示義務の例外事由に該当しない限り、開示請求に適切に対応する必要がありませんしなればなりません。また、訂正等請求や利用停止等の請求が行われた際にも、法令に基づき適切に対応する必要がありませんしなればなりません。

—（平成30年12月追加・令和5年5月更新）

（全般）

Q10-8 防犯カメラを設置してカメラ画像・顔特徴データ等個人データを取り扱う場合には、安全管理措置として特にどのような点に注意すれば良いよいですか。

A10-8 個人情報取扱事業者は、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ます。カメラ画像・や顔認証特徴データ等などが個人デー

タに該当する場合には、の個人データについてはその性質（特に、顔特徴データは不変性が高く、個人の行動の追跡が可能となること等）も踏まえ、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なければならない必要がある、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、外的環境の把握として、例えば以下のような措置が考えられます。

- ①組織的安全管理措置：カメラ画像・顔特徴データ等を取り扱う情報システムを使用できる従業者を限定、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する 等
- ②人的安全管理措置：従業者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・顔特徴データ等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・顔特徴データ等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・顔特徴データ等を取り扱う場合や、IP カメラ（ネットワークカメラ、WEBWeb 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のためには適切な場合にはパスワード設定等のかかる措置も含む。）一、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

また、カメラ画像・顔特徴データ等が保有個人データに該当する場合には、保有個人データの安全管理のために講じた措置の内容を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。）に置かなければなりません←必要があります。ただし、本人の知り得る状態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については、本人の知り得る状態に置く必要はありません（法第 32 条第 1 項第 4 号、施行令第 10 条第 1 号）。

なお、カメラ画像・顔特徴データ等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に、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と考えられます。

（平成 30 年 12 月追加・令和 5-4年 5-4月更新）

以上