

## 【講演レポート】

### 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を利用する際の留意点

個人情報保護委員会事務局 企画官 大星 光弘 氏

本講演では、「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」※（以下、「本文書」という。）の概要について、従来型の防犯カメラにも触れつつ、紹介します。

※[https://www.ppc.go.jp/files/pdf/kaoshikibetsu\\_camera\\_system.pdf](https://www.ppc.go.jp/files/pdf/kaoshikibetsu_camera_system.pdf)

## ○ 前提となる個人情報保護法の知識

### 個人情報とは

個人情報保護法における個人情報とは、生存する個人に関する情報であり、以下のいずれかに該当するものです。

- ① 当該情報に含まれる氏名、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  
この具体例は、名前、顔写真（特定の個人を識別することができるもの）、防犯カメラの映像（特定の個人を識別することができるもの）等です。なお、履歴書などに名前と住所が組み合わせて書いてある場合は、住所も個人情報に該当します。
- ② 個人識別符号が含まれるもの  
政令・規則で指定された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は個人識別符号です。例えば、DNA、顔、虹彩、声紋、歩行の態様等を電子計算機の用に供するために変換した符号がこれに該当します。また、政令・規則で指定された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も個人識別符号です。例えば旅券番号や免許証の番号、マイナンバーがこれに該当します。  
なお、個人識別符号単体であっても個人情報に該当します。

個人情報保護法上、個人情報を取り扱う場合には、取得・利用に関するルール、例えば、利用目的をできる限り特定し、利用目的を達成するために必要な範囲でのみ利用することができる等の遵守が必要です。

### 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「個人データ」と言います。例えば、防犯カメラに映った顔画像1枚1枚を整理したデータベースの顔画像などです。

個人情報保護法上、個人データについては、取得・利用に関するルールに加えて、保管・管理や第三者提供に関するルールをさらに遵守する必要があります。

### 保有個人データとは

さらに、開示、訂正、利用停止、消去等を行うことのできる権限を有する個人データを「保有個人データ」と言います。例えば、委託契約で委託先が個人データの加工だけを行い、委託先には開示、訂正、利用停止、消去等の権限がない場合には、委託先にとっては、当該個人データは「保有個人データ」とはなりません。

個人情報保護法上、保有個人データについては、公表事項・開示請求等への対応に関するルールを遵守する必要があります。

このように、単なる個人情報からデータベース化する場合には遵守すべきルールが増えるとお考えください。

## 要配慮個人情報

要配慮個人情報は、原則として、あらかじめ本人の同意を得ないで取得してはなりません。要配慮個人情報は特に配慮が必要なものとして政令で指定された記述等が含まれる個人情報であり、例えば、人種、信条、社会的身分、病歴、犯罪の経歴、犯罪による被害を被った事実などです。

## 防犯カメラにおける個人情報保護法のルール

防犯カメラで、特定の個人を識別することができる映像を撮影した場合は、個人情報を取り扱うこととなるため、個人情報保護法上、利用目的の特定等が必要となります。ただし、利用目的を特定すれば、どのような取得や利用でも認められるということにはならず、偽りその他不正の手段による取得の禁止、不適正利用の禁止について注意が必要です。

また、防犯カメラで犯罪等の事象が撮影された場合に、下記のとおり、その犯罪等を行った人の画像をキャプチャーショットなどで切り取り、顔画像、事象が発生した日時、発生状況、その人の特徴等をまとめることができますが、顔画像等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、これに含まれる一つひとつの個人情報が「個人データ」となります。


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
...	...	...	...	...

図1. 顔画像とそれに関する情報の例

例えば、「個人データ」の一部である「男性、スーツ、40代」といったその人の特徴だけ抜き出して第三者提供する場合であっても、「原則本人の同意が必要」というルールを守らなければなりません。他の事業者等での犯罪等の被害を防ぐための第三者提供に適用できる可能性がある例外規定がありますが、原則として第三者提供のためには同意を得なければならないことに注意してください。

「個人情報データベース等」とされていない場合は個人データに該当しないため、第三者提供の規律はわかりませんが、第三者提供等については、肖像権・プライバシーにも留意が必要です。

さらに、規則で定める個人データの重大な漏えい等が発生した場合は、個人情報保護委員会への報告及び本人への通知が必要となるため、注意が必要です。

## ○「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」の解説

## 本文書の構成

本文書は個人情報保護委員会が2022年1月に設置した「犯罪予防や安全確保のための画像利用に関する有識者検討会」（座長：東京大学大学院 宍戸 常寿教授）で議論され、取り纏められた報告書を、個人情報保護委員会で審議し、2023年3月29日に公表されたものです。

本文書では、本文書の背景、用語の定義、顔識別機能付きカメラシステムについての説明と、顔識別機能付きカメラシステムを導入する際の3つの留意点

- ① 肖像権・プライバシーに関する留意点
- ② 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
- ③ 事業者の自主的な取組として考えられる事項

を整理しています。

## 顔識別機能付きカメラシステムとは

顔識別機能付きカメラシステム（以下、「カメラシステム」という。）は、従来の防犯カメラと違い、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ベースを作成しています。カメラシステムの仕組みは、図2のとおりです。

## 顔識別機能付きカメラシステムについて

- 本文書が前提とする「顔識別機能付きカメラシステム」は、以下の仕組みを持つシステムである。

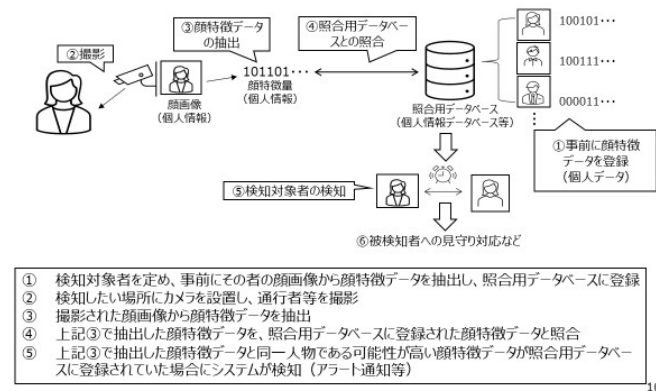


図2. 顔識別機能付きカメラシステムの仕組み

カメラシステムは、例えば施設内で犯罪行為や迷惑行為を行った人物を事前登録し、カメラを施設入口等に設置して通行者等の顔を撮影し、その顔画像から顔特徴データを抽出、登録されているデータベースと照合し、一致すれば警報が鳴るシステムです。ただし、警報が鳴った場合でも、検知対象者が必ずしも事前登録した者と一致しているとは限らないため、通常は目視による確認も行います。

カメラシステムの利点は、顔特徴データの不変性が高いことから、犯罪予防や安全確保に高い効果を有している点です。例えば、体格や服装を手がかりに警備員等が目視で確認するよりも、高い精度で効率的に検知、追跡できる、といった点が挙げられます。

懸念点としては、長期・広範囲にわたり個人の行動を追跡できてしまう可能性がある点です。また、施設入口にカメラが設置されている場合、施設に入ったすべての人のデータが取得されることとなり、自動的、

無差別かつ大量の取得がなされる点も懸念されます。さらに、カメラシステムは通常の防犯カメラと見た目が変わらないため、顔特徴データを取得していることがわかりにくい点があり、利用目的の予測が困難です。そして差別的効果（例えば、どのような基準に基づいて登録するかを決める際に、特定の属性の者への偏見や差別が含まれる等）や、行動の萎縮効果（例えば本人が撮影されることを嫌がり、施設に来なくなってしまう、といった可能性）も考えられます。

## 対象範囲

本文書の対象範囲は顔画像および顔特徴データが用いられる場合が中心となります。対象となる空間的範囲は、例えば、駅や空港などの、カメラシステムで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、不特定多数の人が出入りするような大規模な空間を想定しています。

利用目的は、犯罪予防や安全確保、主体的範囲は、個人情報取扱事業者が中心となります。

### 本文書の対象範囲

- 本文書は、以下のいずれの条件も満たす場合を対象範囲としている。

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 <b>顔特徴データ</b> が <b>用いられる</b> 場合を中心とする。
空間的範囲	a. 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 <b>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</b> > 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想定される。 b. 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する場合等、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、aでの取扱いと同視できる場合
目的	<b>犯罪予防や安全確保</b> （行方不明者等の捜索等）のため。
主体的範囲	<b>個人情報取扱事業者</b> を中心とする。 > 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においても参考にできる。

14

図3. 「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」の対象範囲

## 肖像権・プライバシーに関する留意点

### 肖像権・プライバシー侵害を争点とする裁判例

肖像権・プライバシー法という法律自体はありませんが、最判平成 17 年 11 月 10 日民集 59 巻 9 号 2428 頁において「人はみだりに自己の容貌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」と認められました。同判例では、ある者の容貌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的に考慮して、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、とされました。

本文書では、カメラ関係の判例や裁判例をまとめて紹介しているので、参考にしてください。特に、防犯カメラで撮影した映像を第三者に提供する場合、肖像権・プライバシーの観点から特に注意が必要になると考えます。なお、顔画像等を「個人情報データベース等」としており、当該「個人情報データベース等」に含まれる個人データを第三者提供する場合には、個人情報保護法に基づき、原則として、あらかじめ本人の同意を得る必要があります。

また、本文書では、不法行為の成否を評価するに当たり考慮される要素については、個人情報保護法の不適正利用の禁止（法 19 条）や適正取得（法 20 条 1 項）の解釈においても考慮すべきであると指摘しています。（図 4）

### 肖像権・プライバシー侵害の観点からの留意点②

- 本文書では、不法行為の成否を評価するに当たり考慮される要素（前ページの①～⑦の要素等）については、個人情報保護法の不適正利用の禁止（法 19 条）、適正取得（法 20 条 1 項）の解釈においても考慮すべきであると指摘している。

<前ページの①～⑦の要素>

①被撮影者の社会的地位、②撮影された被撮影者の活動内容、③撮影の場所（範囲）、④撮影の目的、⑤撮影の態様、⑥撮影の必要性、⑦撮影された画像の管理方法

（不適正な利用の禁止）

第十九条 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。

（適正な取得）

第二十条 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。

19

図 4. 肖像権・プライバシー侵害の観点からの留意点

## カメラシステムを利用する際の個人情報保護法上での留意点

### 基本的な考え方

カメラシステムを利用する場合、①利用目的の特定、②利用目的の通知・公表をしなければなりません。また、③不適正取得とならないようにしなければなりません。

#### ① 利用目的の特定

防止したい事項とともに、顔識別機能を用いていることの特定が必要です。防止したい事項については少なくとも犯罪予防や行方不明者の捜索等としなければなりません。また、より具体的に犯罪行為の種類、例えばテロ防止や万引防止と特定することも考えられます。

#### ② 利用目的の通知・公表

上記で特定した利用目的は、原則として、通知又は公表しなければなりません。ホームページに掲示したり、施設の中で掲示する等して通知・公表することが考えられます。カメラシステムを利用する場合には、利用目的を通知・公表をしなければなりません。従来型の防犯カメラの場合、利用目的が防犯目的であることが明らかな場合には通知・公表は不要となる場合があります。

また、本人からの理解を得るためにも、カメラシステムの運用主体等について施設内で掲示したり、カメラシステムを導入する必要性等を Web サイト等で掲示することも望ましいです。本文書では具体的な施設内での掲示例を示しています。掲示例においては、顔画像の取得・照合用データベースについて述べるとともに、より詳細な説明をしているサイトの URL や QR コードを掲示するなどの例を挙げているので、参考にしてください。

#### ③ 不適正取得の禁止

カメラの小型化などにより設置状況から個人情報が取得されていることを本人が容易に認識できない場合には、容易に認識可能とする措置を講じなければなりません。例えば、「カメラ撮影中」などの掲示をすることが考えられます。

## 運用基準

カメラシステムの運用に先立ち、顔画像や顔特徴データをどのような場合に登録するか、検知対象者が来店した場合にどういった対応を取るか、保存期間、登録消去の方法について明確な運用基準を定めて、運用することとなります。運用基準の作成にあたっては、有識者等から意見聴取をするなども望ましいでしょう。

### ① 登録基準

顔特徴データ等を登録する基準（登録基準）は、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基準としなければなりません。登録対象者を、当該犯罪行為等を行う蓋然性が高い者と明確に限定するような登録基準とすることが求められます。

「蓋然性が高い者に厳格に限定するとは、どのような基準にすればよいのか」との質問がありましたが、私がヒアリングした企業では、例えば、そのカメラ画像に犯罪行為がきちんと映っている場合のみを登録している場合が多く、おそらくこの人が万引きをしたのだらうと考えられる場合でも、きちんと画像にそれが映っていない場合は登録していないケースが多いようです。カメラ画像に犯罪行為がきちんと映っている場合に限る、などを基準にするのも一案ではないでしょうか。

### ② 対応手順

次に検知対象者が検知された場合に、適切な対応ができるように、事前の手順を定めておくことが望ましいです。対象者が検知された場合でも 100%確実に一致しているとは言えないため、事業者は通常、目視で確認しています。次にその本人が検知対象者であった場合、多くの場合は見守るといった形で警備の体制を強化し、次のステップとして、声がけをする、など、慎重な対応を取っているケースが多いようです。

### ③ 保存期間

保存期間は、利用の必要性を考慮して保存期間を設定し、利用の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。保存期間の設定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ますが、施設ごとに対応が異なるため、個別に考慮、検討が必要です。

### ④ 保存期間満了時の対応（登録消去）

照合用データベースに登録された情報は、保存期間満了後、遅滞なく消去することを原則とし、保存期間延長にあたっては、利用する必要がある期間の範囲内に限るよう努めなければなりません。また、登録消去の基準を設定し、保存期間中であっても登録要件を喪失した場合は遅滞なく消去するための体制を整備しておくよう努めなければなりません。

## 他の事業者への個人データの提供

個人データを第三者に提供する場合、例えば警察からの捜査関係事項照会などの場合は、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、確認することが重要です。また文書内容について、

肖像権・プライバシーの観点などから、もし不安や疑問に思う点等があれば、警察に質問することなどを行った方がよいでしょう。

また、「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」に該当するとして、本人の同意なく、個人データを第三者提供することが認められる場合もあります。もっとも、例えば地域内の事業者間で、これに基づいて個人データを共有することが事前に想定されている場合には、具体的にどのような場合にこれを根拠に第三者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で恣意的な判断がなされないようにすることが望ましいでしょう。

共同利用の場合も、個人データの提供にあたって本人の同意は不要ですが、共同利用する者の範囲については、その範囲を同一業種内に限定したとしても、全国、又は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、真に必要な範囲に限定することが適切です。共同利用を行う際には、どの事業者も同様の対応ができるよう、文書化された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でしょう。

### 開示等の請求への対応

本人から開示請求がなされた場合、個人情報保護法に従い、原則として、開示しなければなりません。当該個人データの存否が明らかになることで、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や、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場合については例外として、開示が不要となりますが、できる限り丁寧に対応していくことが重要です。

### 委託の場合の対応

本文書では、施設運用事業者が警備会社等にカメラシステムの運用を委託している場合の対応事項や委託の場合の考え方などもまとめています（図5）。例えば、委託先から個人データの漏えい等が発生した場合、委託先は委託元に対して、法に定められた事項を通知すれば個人情報保護委員会への報告や本人への通知は免除となりますが、委託元には、通知の有無にかかわらず報告義務が生じる、といったことなどを整理しています。

#### (参考) 委託

- 施設運営事業者が、本システムの導入を決定した上で、警備会社等にカメラ画像の分析やシステムの運用等、個人データの取扱いの委託をすることが想定される。

対応事項	委託の場合の考え方（法25条、法27条5項1号）	
施設内での 掲示事項例	運用主体	委託元である施設運営事業者
	利用目的	委託の有無にかかわらず記載内容は同様
	問合せ先	本システムについて実質的に応答できる者。委託先を問合せ先とする場合、本システムの運用の委託を受けていることを明らかにすることが望ましい。
	Webサイト等のURL及びQRコード等	委託元である施設運営事業者のWebサイト等が望ましい。
運用基準の作成	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。	
安全管理措置	委託元は委託先の監督義務がある（法25条）。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。	
漏えい等報告	<ul style="list-style-type: none"> <li>● 報告対象事態（法26条、規則7条）が生じた場合は、原則として、漏えい等の概要等を個人情報保護委員会に対して報告するとともに、本人に通知しなければならない。</li> <li>● 委託先は委託元に規則8条1項で定める事項を通知すれば、報告義務及び通知義務は免除。委託元は、通知の有無にかかわらず、報告義務及び通知義務がある。</li> <li>● 本人通知については、漏えい等した保有する個人データに本人の連絡先が含まれていない等、本人への通知が困難である場合は、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。</li> </ul>	
開示等請求	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、この場合には、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。	

34

図5. カメラシステムの運用委託における委託元／委託先の対応事項と役割

## 事業者の自主的な取組として考えられる事項

事業者の自主的な取組みとして、実現しようとする内容を明確化して適切な手段かを検討する、PIA（個人情報保護評価・プライバシー影響評価）など導入前の影響評価の実施や一定期間を設けての試験的实施、新規性のある事案に対する第三者委員会による意見聴取等が挙げられます。

また、被撮影者への十分な説明として、本格的利用開始前からの広報、他事業者との連携による広報（カメラシステムの必要性や有用性について、一社単独ではなく業界全体として広報）を行うことが考えられます。加えて、他事象者との間で導入事例の情報交換を行うことで知見を集積したり、認定個人情報保護団体を活用する等して、業界として取り組むことも考えられます。

導入後は、カメラシステムの運用担当者以外の者による内部監査や、第三者委員会設置での確認、透明性レポートの作成公表などが考えられます。

## 実現しようとする内容の明確化と適切な手段の選択

実現しようとする内容の確認については、抽象的に犯罪予防とするのではなく、具体的にどういった犯罪が想定され、防止したいのかを特定し、当該施設や類似施設における発生の実態等も踏まえたうえで、有効な手段（例えばカメラシステムがいいのか手荷物検査がいいのか、等）を考えて、適切な手段を選択するのがよいでしょう。

## 最後に

本文書中では、「顔識別機能付きカメラシステムの検討の観点リスト」を掲載しており、各項目に関連する法令・ガイドライン等の箇所も案内しています。また、個人情報保護法に関連した相談受付用の 24 時間チャットボットサービス、個人情報保護法相談ダイヤル、PPC ビジネスサポートデスクなども設置していますので、ぜひご活用ください。

- ・PPC 質問チャット

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

- ・個人情報保護法相談ダイヤル

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

- ・PPC ビジネスサポートデスク（要予約）

[https://www.ppc.go.jp/personalinfo/business\\_support/](https://www.ppc.go.jp/personalinfo/business_support/)



個人情報保護委員会事務局 企画官 大星 光弘 氏

2004 年経済産業省入庁、2022 年 7 月から現職



本内容は、2023 年 5 月 26 日に開催された JIPDEC セミナー「企業におけるカメラ画像利活用の際の実務ポイント～防犯利用から商用利用まで」講演内容を取りまとめたものです。