

防犯カメラと個人情報保護法の取扱い
～改訂版～

2023年10月

 公益社団法人 日本防犯設備協会

映像監視分科会

改訂版発行に当たって

個人情報保護委員会は、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」を、令和5年5月25日に更新しました。

また、「令和3年改正法」では、令和5年4月1日から、民間事業者、国の行政機関、独立行政法人等に加え、地方公共団体についても個人情報保護法が適用されることになりました。

これを受け当協会では、本「防犯カメラと個人情報保護法の取扱い」の内容をこれに適合すべく改訂することとし、解説部分も含め必要な加除訂正等を行いました。

なお、当協会は、令和5年3月8日付で個人情報保護委員会から、認定個人情報保護団体に認定されました。現在の対象事業者数は、68社・団体です。

はじめに

「個人情報の保護に関する法律」（以下「個人情報保護法」）は平成15年5月に公布され、平成17年4月に全面施行されました（以下「旧法」という。以下同じ。）。その後、情報通信技術の急速な発展や事業活動のグローバル化等により個人情報保護法が制定された当時には想定されなかったほど膨大かつ多様に個人情報が利活用されるようになりました。

このような状況の中、平成26年に大手企業による大規模な個人情報漏洩事件が発生し、個人情報保護への関心が一気に高まりました。そこで国際的な法制定の動向等も踏まえ、「個人情報保護法」は「定義の明確化」「個人情報の適切な活用・流通の確保」「グローバル化への対応」等を目的とした改正が実施されました。改正された「個人情報保護法」は、平成27年9月に「改正個人情報保護法」として公布され、平成29年5月30日に全面施行されました（以下「27年改正法」という。以下同じ。）。また、近年では防犯カメラの高画質化も進んでいます。高画質な防犯カメラで撮影された画像は、個人を十分に識別することができるため、個人情報として取り扱わなければならないことが改正法の中で明確にされています。

防犯に対する意識の高まりなどから防犯カメラの需要が益々高まっている現在において、防犯カメラの設置等に携わる総合防犯設備士及び防犯設備士の方々にとって「個人情報保護法」の理解は必須となっています。「個人情報保護法」を知らずに防犯カメラを設置したことによって法に抵触するようなことになってはなりません。また、防犯カメラの管理者に対して、その管理・運用についての指導をすることもあると思います。

こうした中、映像監視分科会では、個人情報保護委員会による「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（令和3年9月10日更新）から防犯カメラに係る部分を抜粋し、より判り易く理解していただくために必要な解説を追加し、「防犯カメラと個人情報の保護法の取扱い」を制作しました。

防犯カメラの取扱いに関しては「個人情報の保護」だけではなく「プライバシーの保護」についての配慮も必要となります。このことについては東京都立大学法学部 星周一郎教授の解説を掲載致しました。

「防犯カメラと個人情報保護法の取扱い」が「個人情報保護法」を遵守した防犯カメラの設置・運用の一助となればと考えております。

公益社団法人 日本防犯設備協会
映像監視分科会
主査 大野 眞裕

目次

改訂版発行に当たって

はじめに

目次

1 個人情報保護法を理解する	・・・ 1
1.1 個人情報の定義	・・・ 1
1.2 個人情報取扱事業者の定義	・・・ 1
1.3 防犯カメラに関する用語の定義	・・・ 4
2 防犯カメラ等に関する「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（令和 5 年 5 月 25 日更新）の抜粋項目と解説	・・・ 5
1-1 定義（個人情報） Q1-12, Q1-13, Q1-14, Q1-15、Q1-16 （個人識別符号） Q1-22 （要配慮個人情報） Q1-31 （個人情報 データベース等） Q1-41 （個人情報取扱事業者） Q1-50、Q1-51、 Q1-53、Q1-54 （保有個人データ） Q1-56, Q1-57	・・・ 6
1-2 個人情報の利用目的（利用目的の特定） Q2-1、Q2-3、	・・・ 15
1-5 個人データの管理（データ内容の正確性の確保等） Q5-2、Q5-3、 Q5-4、（従業者の監督） Q5-6、Q5-7（委託先の監督） Q5-11	・・・ 17
1-7 個人データの第三者への提供（第三者提供の制限の原則） Q7-1、Q7-16、 Q7-17（第三者に該当しない場合） Q7-49、Q7-50、Q7-51、Q7-52	・・・ 20
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） Q9-10、 Q9-13	・・・ 25
1-10 講ずべき安全管理措置の内容（全般） Q10-7、Q10-8（人的安全管理措置） Q10-13	・・・ 26
4-1 仮名加工情報（令和 3 年 9 月追加） Q14-1	・・・ 29
4-2 匿名加工情報 Q15-6、Q15-8、Q15-14	・・・ 29
3 防犯カメラに関するガイドライン	・・・ 31
3.1 個人情報保護法と自治体の「防犯カメラ設置と管理に関するガイドライン」	・・・ 31
3.2 宮城県の「防犯カメラの設置及び運用に関するガイドライン」	・・・ 31
4 高機能防犯カメラの適法・適正な利用にあたって	・・・ 33
東京都立大学法学部教授：星 周一郎	
5 解像度と画像使用目的	・・・ 45
6 顔識別機能付き防犯カメラシステム	・・・ 46
7 防犯設備士と個人情報保護法	・・・ 46
参考文献	・・・ 47

1 個人情報保護法を理解する

個人情報保護法は3年毎に、「個人情報」の定義や「個人情報取扱事業者」の義務などが必要に応じて改正されます。そのため、最初に組み立てを理解する必要があります。

1.1 個人情報の定義

27年改正法では「個人情報」の定義が明確化されました。防犯設備士が個人情報について考える場合、防犯カメラ等（「防犯カメラとデジタルレコーダ」を言う。以下同じ。）の取り扱いについては、明確化された内容を理解して対応する必要があります。

防犯カメラ等の機能や性能が向上したことで、NTSC方式（アナログ）主流の旧法時代では考えなかったことが、27年改正法では直接影響するので、慎重な対応が必要です。

個人情報の定義については、旧法と27年改正法を比較しながら解説します。

旧法の定義：

第2条①この法律において「個人情報」とは、生存する個人に関する情報であつて、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できることとなるものを含む。）をいう。

27年改正法の定義：

第2条①この法律において「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。

- 1 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第2号において同じ。）で作られる記録をいう。以下同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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。）

- 2 個人識別符号がふくまれるもの

防犯カメラで撮影し記録された画像は、旧法では「その他の記述等」に含まれていましたが、タイムラプスVTRやデジタルレコーダなどに記録された画像がその言葉に該当すると理解していた防犯設備士は少なかったのではないかと思います。

27年改正法では「電磁的方式で作られる記録」と、それらの画像の規定が明確になっています。さらに、第2項で「個人識別符号がふくまれるもの」には、防犯カメラ画像から得られた顔特徴データや音声と動作等については声紋認証と歩容認証などの手法などにより、特定の個人を識別できるものとして、個人情報としています。

防犯カメラ等から考えると、アナログ（NTSC方式）の場合、初期の頃の記録はVHSなどのテープ方式が、平成16年頃から現在まではデジタルレコーダが使われています。

VHSテープにタイムラプスモードで記録していた時の解像度は非常に低く、よほど被写体を近くで撮影しないと、個人を識別できると言える画像ではありませんでした。

その後デジタルレコーダが主流になっても、アナログ（NTSC方式）防犯カメラは2：1インターレースで撮影しますが、デジタルレコーダはその片フィールド画像+擬似補完画像での記録方式が多く、結局、記録された情報は半分程度になっていました。テープ方式よりは解像度は良いが、被写体の目鼻とか文字や模様など、細かい部分は情報の欠落により判別が難しかったのが現実でした。

現在では、防犯カメラの撮像素子はプログレッシブが大半になり、解像度もハイビジョンやフルハイビジョンの機器が多くなりました。そのため、被写体の画角が「画角A」（人物全身が画面の半分）程度でも、撮影した画像から個人の特徴が分かるようになりました。解像度が良くなりかつ走査での情報欠落が無くなったおかげです。

したがって、現在の防犯カメラ等により撮影し記録した画像等は、ほとんどの場合で本人が判別できる映像となり、個人情報に該当し、個人情報保護法の適用対象となります。

個人情報保護法にはあらゆる分野の個人情報が含まれていますが、防犯カメラ等に関係が薄いものもあるので、個人情報保護委員会が作成した「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（令和5年5月25日更新）の中から、防犯カメラ等に関連する項目を当分科会で選抜して第2章に掲載しました。

「個人情報」に関しては、Q1-12、Q1-13、Q-1-14、Q1-15、Q1-16、Q1-22、Q1-31を確認してください。

1.2 個人情報取扱事業者の定義

27年改正法では営利非営利を問わず、個人情報を事業の用に供している事業者は個人情報取扱事業者となり、定められた義務が課せられます。防犯カメラ等を取り扱う防犯設備士は、個人情報保護法を正しく理解して、特に画像に関係する管理について適切に対応しなければなりません。

「個人情報取扱事業者」に該当するかどうかと義務に関しては、Q1-50、Q1-51、Q1-53、Q1-54を確認してください。なお、Q1-50に記載されていますが、旧法において、取り扱う個人情報の数が5,000を超えない事業者は個人情報取扱事業者から除外されていましたが、27年改正法には除外規定は無いので注意してください。

さらに、27年改正法では、個人データにおいて6か月を超えて保有すると保有個人データになり、それを取り扱う個人情報取扱事業者には、更なる義務が発生することになっていましたが、令和2年改正法では、この保有期間の除外規定は無くなりましたので注意してください。（施行は令和4年4月）なお、保有個人データに関する事項の公表などは、1-9に記載されています。

個人情報取扱事業者の義務

項目	令和3年改正法
利用目的の特定	第17条第1項
利用目的の変更	第17条第2項
原則利用目的による制限	第18条
不適正な利用の禁止	第19条第2項
適正な取得	第20条第1項
要配慮個人情報の取得	第20条第2項
取得に際しての利用目的の通知等	第21条
データ内容の正確性の確保等	第22条
安全管理措置	第23条
従業者の監督	第24条
委託先の監督	第25条
漏えい等の報告等	第26条
第三者提供の制限	第27条第1項
オプトアウト(*)による第三者提供	第27条第2項～第4項
「第三者」に該当しない場合	第27条第5項、第6項
外国にある第三者への提供の制限	第28条
第三者提供者に係る記録の作成等	第29条
第三者提供を受ける際の確認等	第30条
個人関連情報の第三者提供の制限等	第31条
保有個人データに関する事項の公表等	第32条
開示	第33条
訂正等	第34条
利用停止等	第35条
理由の説明	第36条
開示等の請求等に応じる手続き	第37条
手数料	第38条
事前の請求	第39条
個人情報取扱事業者による苦情の処理	第40条
仮名加工情報の第三者提供の制限等	第42条
匿名加工情報の作成等	第43条
匿名加工情報の提供	第44条

識別行為の禁止	第 45 条
安全管理の措置等	第 46 条

(注) オプトアウトとは、個人情報の第三者提供に関し、個人データの第三者への提供を本人の求めに応じて停止すること。大手企業による顧客情報の流出事件が起きたこともあり、27 年改正法では個人情報をオプトアウト手続きで第三者提供する場合には「個人情報保護委員会」への届け出が必要となりました。個人情報保護法、「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（令和 3 年 9 月 10 日更新）については、参考文献を参照してください。

1.3 防犯カメラに関する用語の定義

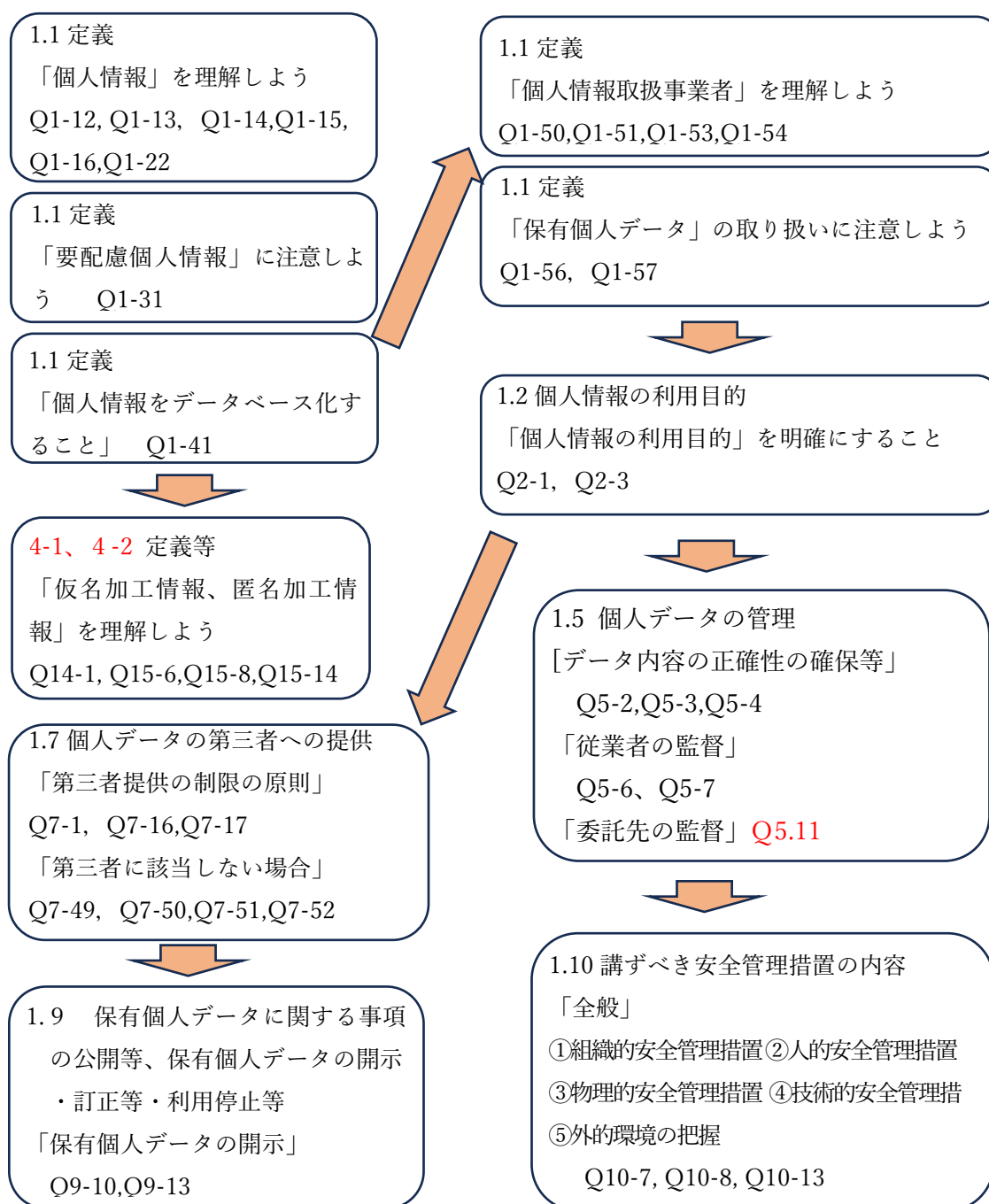
「個人情報の保護に関する法律についてのガイドライン」に関する Q&A（令和 5 年 5 月 25 日更新）より抜粋

用語	定義
防犯カメラ	防犯目的で設置しているカメラ
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
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
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

2 防犯カメラ等に係る「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 (令和 5 年 5 月 25 日更新) の抜粋項目と解説

防犯カメラ等に係る個人情報保護法を理解するには、1-1 定義に記載の「個人情報」や「要配慮個人情報」「個人情報データベース等」「個人情報取扱事業者」「保有個人データ」を読んで、言葉を理解してください。次に、1-1「個人情報取扱事業者」の項目に戻り、個人情報取扱事業者になったつもりで、1-2 以降の実施内容の理解に進んでください。

全体を理解する項目は、下記フローの四角内の Q&A に掲載しています。



1-1 定義 P6 (「ガイドライン」に関する Q&A 掲載ページ 以下同じ。)

(個人情報)

Q 1-12 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 1-12 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、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、抽出元のカメラ画像や個人識別符号等特定の個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しない場合には、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)

Q 1-14 店舗や、駅・空港等に設置したカメラにより画像を取得し、そこから顔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、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りますか。

A1-14 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を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データ等を利用しなければなりません。

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。

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Q1-13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の利用目的、問い合わせ先、さらに詳細な情報を掲載したWebサイトのURL又はQRコード等を店舗や駅・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5年5月更新)

(個人情報)

Q 1-15 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 1-15 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特徴データを取得する場合については、Q 1-13、Q 1-14 及び Q 1-16 を参照のこと。

(令和5年5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、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じなければなりません。

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したとしても、個人情報を取り扱って広告配信を行っているとして解されます。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5年5月更新)

(個人識別符号)

Q 1-22 施行令第1条第1号に規定された個人識別符号に関するガイドライン(通則編)の記載において、「本人を認証することができるようにしたもの」とありますが、これは具体的にどのようなことを想定しているのですか。

A 1-22 「本人を認識することができるようにしたもの」とは、登録された顔の容貌やDNA、指紋等の生体情報がある人物の生体情報と照合することで、特定の個人を識別することができる水準である符号を想定しています。

【当協会の解説】

1. 防犯カメラで撮影し記録した画像は個人情報として取り扱います。
2. 防犯カメラ及び防犯カメラシステムの取扱いは、従来型防犯カメラの場合と、顔識別機能付きカメラシステムの場合に分けて行う必要があります。
3. 従来型防犯カメラは、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。
4. 顔識別機能付きカメラシステムは、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。従来型防犯カメラに、顔特徴データを抽出し顔識別ができるデジタルレコーダなどや外部システムを接続したのも含みます。
5. 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。
6. 従来型防犯カメラで撮影した画像を防犯目的のみのために使用する場合は、取得した防犯カメラ画像の利用目的の通知や掲示するなどの措置は必要ありません（法第21条第4項第4号）。しかし、防犯カメラが設置されている場所に入る人が、個人情報を取得されていることを容易に認識できるように、「防犯カメラ稼働中」や「設置管理者」などを明記することが望まれます。
なお、自治体の防犯カメラに関するガイドラインでは、犯罪抑止効果及びプライバシー保護の観点から、「防犯カメラ設置」等の表示を求めているところもあります。
7. 顔識別機能付きカメラシステムの場合は、防犯カメラが設置されている場所に入る人が、撮影した顔画像から顔特徴データを抽出し顔識別を行っていることを容易に認識できるように、その利用目的の通知・公表をしなければなりません。また、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、問い合わせ先等を入り口などに明示するか、これらを掲載したWEBサイトのURL又はQRコード等を示すことが望まれます。
8. 防犯カメラの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、画像の管理者や団体は個人情報取扱事業者となります。
9. 従来型防犯カメラ画像から抽出した性別、全身のシルエット画像等による移動軌跡データのみであれば個人情報には該当しません。（本人が特定できる情報と照合することが可能な場合は除きます。）

1-1 定義 P9

(要配慮個人情報)

Q 1-31 ある人の犯罪行為を撮影した防犯カメラ映像は、要配慮個人情報に該当しますか。

A 1-31 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き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ません。

【当協会の解説】

この項目は要配慮個人情報について説明します。

個人情報にはその個人が不当な差別、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要配慮個人情報があります。一般に人種、信条、犯罪歴、病歴等を言います。要配慮個人情報の取扱いについては行政、民間、業界団体等において個別の法令やガイドラインに規定されていますので個別に確認の上、対応する必要があります。

犯罪をしても捜査の対象にならなかった場合（謝罪の上、警察への通報や捜査に至らなかった場合など）は要配慮個人情報には該当しません。未だ刑事事件に関する手続きが行われていないからです。同様の事例として、思想や信仰等の信条は要配慮個人情報に該当しますが、それを推知させる情報は該当しないものとされています。

1-1 定義 P11

(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 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)

【当協会の解説】

この項目は個人情報データベース等について説明します。

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されています。

従来型防犯カメラの映像情報を、単にデジタルレコーダやコンピュータ等に記録・集約するだけでは、個人情報データベース等には該当しないものとされています。

顔識別機能付きカメラシステムの場合は、顔の抽出ができるので、撮影した顔のナンバー管理と時間管理等ができます。顔識別や検出ソフト等を使うと、特定の個人に係る映像情報の検索ができるので、個人情報データベース等になります。

なお、コンピュータ等を使わずに、顔画像を含む印刷物の場合、五十音順、年月日などで整理されており、目次や、索引を用いて容易に特定の個人情報を検索できる形であれば、個人情報データベース等になります。

1-1 定義 P13

(個人情報取扱事業者)

Q 1-50 個人情報を取り扱う件数が少ない事業者も個人情報取扱事業者に該当しますか。

A 1-50 個人情報データベース等を事業の用に供している者であれば、当該個人情報データベース等を構成する個人情報によって識別される特定の個人の数の多寡にかかわらず、個人情報取扱事業者に該当します。

なお、平成 27 年改正の施行（平成 29 年 5 月 30 日）前においては、5000 人分以下の個人情報しか取り扱っていない者は、個人情報取扱事業者から除外されていましたが、施行後はこれらの者も個人情報取扱事業者に該当することとなりますので、注意が必要です。

(個人情報取扱事業者)

Q 1-51 個人情報を「事業の用に供している」とは、どのような意味ですか。加工、分析などをせず、データベースとして利用しているのみであれば、該当しませんか。

A 1-51 「事業の用に供している」とは、事業者がその行う事業のために個人情報を利用していることをいい、特にその方法は限定されません。事業のために個人情報データベース等を作成、加工、分析、提供することだけでなく、事業を行う上で必要となる顧客情報、従業員情報、配達先情報などをデータベースとして利用していることなども含みます。

(個人情報取扱事業者)

Q 1-53 委託業務として、委託元の個人情報データベース等を利用していますが、この場合も、個人情報取扱事業者に該当しますか。

A 1-53 委託元の個人情報データベース等を加工・分析等をせずにそのまま利用する場合でも、委託された業務を行うために利用するのであれば「事業の用に供している」ことになり、委託先も個人情報取扱事業者に該当します。

(個人情報取扱事業者)

Q 1-54 NPO 法人や自治会・町内会、同窓会、PTA のような非営利の活動を行っている団体も、個人情報取扱事業者として、個人情報保護法の規制を受けるのですか。

A 1-54 個人情報保護法における「事業」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であって、かつ社会通念上事業と認められるものをいい、営利・非営利の別は問いません。したがって、非営利の活動を行っている団体であっても、個人情報データベース等を事業の用に供している場合は、個人情報取扱事業者に該当します。NPO 法人や自治会・町内会、同窓会、PTA のほか、サークルやマンション管理組合なども個人情報取扱事業者に該当し得ます。

(平成 30 年 7 月更新)

【当協会の解説】

27年改正法では、防犯カメラ等の画像は基本的に個人情報となるので、防犯カメラを取扱う会社や団体などは、その画像が個人情報データベース等に該当し、それを事業の用に供している場合は、個人情報取扱事業者となります。

防犯設備士が、防犯カメラの設置や管理をする会社、団体にアドバイスするポイントを下表にまとめましたので確認ください。

番号	個人情報取扱事業者の実施項目	防犯設備士がアドバイスするポイント
1	利用目的を明確にすること	対象の建物や地域の防犯上の脆弱性を改善できることに資する目的であること。
2	利用目的内の利用とすること	撮影対象範囲と画像の活用範囲が利用目的に合っていること。防犯目的以外には利用しないこと。
3	適切な取得を行うこと	防犯カメラの隠し撮影配置は不適切。特に公共空間に設置する場合には、防犯カメラは住民が見える位置に設置すること。また、自治体が決めた「防犯カメラの設置と管理に関するガイドライン」等に適合していること。
4	適切な表示を行うこと	建物入口や設置電柱などに、防犯カメラを表示する看板などを設置し、看板には設置者か管理者の名称を記載すること。 1-1 定義（個人情報）当協会の解説の 6 及び 7 に、従来型防犯カメラの場合と、顔識別機能付きカメラシステムの場合の解説が記載されているので参照のこと。
5	画像の閲覧を適切に行うこと	ライブ画像を定められた関係者以外には簡単に見えないようにすること。
6	画像の管理と画像の取り出しを適切に行うこと	組織的安全管理措置のため、事業者内の責任者と従事者を決めること。 記録画像の第三者への貸し出しは、定められた警察などの関係者のみとして、貸し出す際には、責任者に連絡して、従事者が必要な画像を取り出して記録を残すこと。（参考 A7-17、A10-8）

1-1 定義 P15

(保有個人データ)

Q 1-56 個人データの取扱いが委託される場合、当該個人データは委託元と委託先のどちらの保有個人データとなりますか。

A 1-56 特に定めのない限り、委託元の保有個人データになると考えられますが、具体的には個別の事例ごとに判断することになります。

委託元が、個人データを受託処理する個人情報取扱事業者である委託先に対し、自らの判断で当該個人データの開示等を行う権限を付与していないとき（委託元、委託先間で何ら取り決めがなく委託先が自らの判断で開示等を行うことができない場合も含む。）は、本人に対する開示等の権限を有しているのは委託元であるため、当該個人データは委託元の「保有個人データ」となります。

(保有個人データ)

Q 1-57 ガイドライン（通則編）2-7の「(4) 当該個人データの存在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安全と秩序の維持に支障が及ぶおそれがあるもの」の事例1について、「警察から捜査関係事項照会等がなされることにより初めて取得した個人データ」とありますが、これは具体的にはどのような意味ですか。

A 1-57 例えば、ある事業者が、ある人物に関し、警察から刑事訴訟法第197条第2項に基づき、顧客情報の提供依頼を受けたが、依頼がなされた時点では、当該事業者が当該人物の個人データを保有していない場合、当該照会によって当該事業者は初めて当該人物の個人データを入手することになります。このような個人データの存否が明らかになれば、犯罪の予防、鎮圧、捜査又は公共安全と秩序の維持に支障が及ぶおそれがあるため、「保有個人データ」からは除外されます。したがって、この事例では、当該人物の個人データは、開示請求の対象外となります。

【当協会の解説】

保有個人データとは、個人情報取扱事業者が、開示、内容の修正、追加または削除、利用の停止、消去および第三者への提供の停止を行うことができる権限を有する個人データです。

防犯設備士は、個人情報取扱事業者に、該当している個人データが、保有個人データの場合には、法令に基づき適切に対応するようアドバイスをしてください。

なお、27年改正法では、個人データについて6か月を超えて保有すると保有個人データになっていましたが、令和2年の改正（施行は令和4年4月）では、6ヶ月の除外規定が削除されているので注意してください。

（利用目的の特定）

Q 2-1 個人情報取扱事業者は、個人情報の利用目的を「できる限り特定しなければならない」とされていますが、どの程度まで特定する必要がありますか。

A 2-1 利用目的を「できる限り」特定するとは、個人情報取扱事業者が、個人情報をどのような目的で利用するかについて明確な認識を持つことができ、また本人において、自らの個人情報がどのような事業の用に供され、どのような目的で利用されるのかについて一般的かつ合理的に予測・想定できる程度に、利用目的を特定することをいいます。このため、特定される利用目的は、具体的で本人にとって分かりやすいものであることが望ましく、例えば、単に「お客様のサービスの向上」等のような抽象的、一般的な内容を利用目的とすることは、できる限り具体的に特定したことにはならないと解されます。

また、一連の個人情報の取扱いの中で、本人が合理的に予測・想定できないような個人情報の取扱いを行う場合には、かかる取扱いを行うことを含めて、利用目的を特定する必要があります。例えば、いわゆる「プロファイリング」といった、本人に関する行動・関心等の情報を分析する処理を行う場合には、分析結果をどのような目的で利用するかのみならず、前提として、かかる分析処理を行うことを含めて、利用目的を特定する必要があります。具体的には、以下の様な事例においては、分析処理を行うことを含めて、利用目的を特定する必要があります。

事例 1) ウェブサイトの閲覧履歴や購買履歴等の情報を分析して、本人の趣味・嗜好に応じた広告を配信する場合

事例 2) 行動履歴等の情報を分析して信用スコアを算出し、当該スコアを第三者へ提供する場合

（令和 3 年 9 月更新）

（利用目的の特定）

Q 2-3 「利用」とは何を意味しまか。

A 2-3 特段の定義があるわけではありませんが、取得及び廃棄を除く取扱い全般を意味すると考えられます。したがって、保管しているだけでも利用に該当します。

【当協会の解説】

個人情報の利用目的について説明します。

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、利用目的を特定する義務があります。防犯カメラで取得した個人情報をどのような目的で利用するかを明確にすることは、個人情報を取得した者にとっても利用目的が明確となり、また個人情報を取得された本人にとっても自分の個人情報がどのような目的で利用されるのかが明確となります。このため防犯カメラで取得した個人情報の利用は、生命や財産を守るなどの防犯目的に特定し、その目的達成に必要な範囲に限定することが必要です。

A1-13 のように、防犯カメラにより、防犯目的のためにのみ撮影して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は、取得の状況からみて利用目的が明確なので、利用目的を明示する必要はありません。

また、防犯カメラで取得した個人情報は、これを破棄するまでの間が「利用」と定義されます。このため、単に保管しているだけでも利用に該当します。

1-5 個人データの管理（法第 22 条～第 25 条関係） P32

（データ内容の正確性の確保等）

Q 5-2 取得した個人情報は、いつ廃棄しなければなりませんか。

A 5-2 個人情報保護法では、個人情報の保存期間や廃棄すべき時期について規定していません。もっとも、個人情報取扱事業者は、その取扱いに係る個人データを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りません。（法第 22 条）

（データ内容の正確性の確保等）

Q 5-3 「遅滞なく消去する」とは、具体的にどのような期間で消去することを求めていますか。

A 5-3 「遅滞なく」が示す具体的な期間は、個人データの取扱状況等により異なり得ますが、業務の遂行上の必要性や引き続き当該個人データを保管した場合の影響等も勘案し、必要以上に長期にわたることのないようにする必要があると解されます。他方で、事業者のデータ管理のサイクル等、実務上の都合に配慮することは認められます。

（データ内容の正確性の確保等）

Q 5-4 カメラ画像や顔特徴データ等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よいですか。

A 5-4 個人情報取扱事業者は、法第 22 条に基づき、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 年 5 月更新）

【当協会の解説】

データ内容の正確性の確保等にある記録画像の保存に関する説明をします。

防犯カメラで撮影した画像を記録するのはデジタルレコーダを使います。内蔵 HDD（ハードディスク）はコンピュータの進化に伴い記憶容量が増えて、現在では 2TB タイプが一般的になっており、利用目的に適した保存が可能になってきました。記録は一定期間で上書き消去する使い方を基本とします。

例えばマンションの場合では、管理組合の会合が月 1 回ならばそれまでは記録を残しておくことが必要になります。

また、通学路などについては、自治体が生している「防犯カメラ設置と管理に関するガイドライン」などに、「必要最小限の期間（概ね 1 か月以内）など」と記載されていますので確認して対応してください。

1-5 個人データの管理 P33

(従業者の監督)

Q5-6 町内会やマンション管理組合等において、監督が必要となる「従業者」には、どのような者が該当しますか。

A5-6 町内会やマンション管理組合等の形態や管理の実態にもよりますが、例えば、町内会やマンション管理組合の運営を担う理事等は、個人情報保護法における「従業者」に該当するものと考えられます。

(従業者の監督)

Q5-7 従業者に対する監督の一環として、個人データを取り扱う従業者を対象とするビデオやオンライン等による監視（モニタリング）を実施する際の留意点について教えてください。

A5-7 個人データの取扱いに関する従業者の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリングを実施する場合は、次のような点に留意することが考えられます。なお、モニタリングに関して、個人情報の取扱いに係る重要事項等を定めるときは、あらかじめ労働組合等に通知し必要に応じて協議を行うことが望ましく、また、その重要事項等を定めたときは、従業者に周知することが望ましいと考えられます。

- モニタリングの目的をあらかじめ特定した上で、社内規定等に定め、従業者に開示すること
- モニタリングの実施に関する責任者及びその権限を定めること
- あらかじめモニタリングの実施に関するルールを策定し、その内容を運用者に徹底すること
- モニタリングがあらかじめ定めたルールに従って適正に行われているか、確認を行うこと

(委託先の監督)

Q5-11 外部事業者に定型的業務を委託する場合、必ず、当該外部事業者が用意している約款等に加えて、自己の社内内規を遵守するよう求める覚書を追加的に締結する等の対応が必要となりますか。

A5-11 個人データの取扱いを委託する場合の委託先の監督については、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等を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、委託する事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）などに起因するリスクに応じて行うべきものと考えられます。当該約款等を吟味した結果、当該約款等を遵守することにより当該個人データの安全管理が図られると判断される場合には、当該定型的業務を委託することについて必ずしも追加的に覚書を締結する必要まではないと考えられます。

【当協会の解説】

マンションの防犯カメラについては、平成18年「防犯に配慮した共同住宅に係る設計指針」と「防犯優良マンション標準設置基準」が警察庁と国土交通省から発出され、それ以降のマンションで設置が行われました。マンション管理組合が設置した防犯カメラの場合、マンション所有者である管理組合が個人情報取扱事業者になり、その役員は従業者になります。また、防犯カメラを含む施設管理業務などを委託したマンション管理会社や警備会社は委託先になります。

特にエレベータかご内の防犯カメラは、必ず設置することが指導されており、未設置の既設の建築物には、エレベータ会社などが追加で設置した場合もありました。エレベータ会社は、防犯カメラをエレベータ管理のために、全国規模の管理センターで管理しますので、マンション管理会社などから再委託される場合も発生します。

マンションなどの防犯カメラの管理には、再委託が発生する可能性がありますので、従業者は委託先との約款等を吟味し、再委託関係にも注意をして、個人データが漏えい等をした場合のリスクが無いように、安全管理を行うことが大切です。

防犯カメラ等の個人データは、防犯カメラが撮影してモニターで見える映像と、デジタルレコーダに収納した記録画像です。従業者は委託先との約款等を吟味し、個人データが漏えい等をした場合のリスクが無いように、以下の対応を含めて安全管理を行うことが大切です。

通常、デジタルレコーダにはモードロックという機能があり、画面切り替えや記録取り出しなどの様々な機能や性能の操作について、管理ランク別にそれらを制限する登録を事前に行うことができます。業務委託する際にも、委託先にどのランクまで操作できる権限を認めるかを約款等に記載しておくこととともに、防犯カメラ等の操作権限の事前登録が必要です。

店舗や事業所の場合、防犯カメラ等には社員である従業者が撮影されて記録されます。したがって、モニタリングについてもA5-7のように適切に対処する必要があります。また、防犯カメラを含む施設管理業務などを委託した場合の対応は、マンションの事例と同様に対応してください。

1-7 個人データの第三者への提供（法第 27 条～30 条関係） P42

（第三者提供の制限の原則）

Q 7-1 「第三者」とはどのような者をいうのですか。

A 7-1 「第三者」とは、一般に①当該個人データによって特定される本人、②当該個人データを提供しようとする個人情報取扱事業者以外の者をいい、自然人、法人、その他の団体を問いません。

なお、第三者提供の制限（法第 27 条）、外国にある第三者への提供の制限（法第 28 条）、確認・記録義務（法第 29 条及び第 30 条）の各条において、①及び②に加えて「第三者」から除外される者が規定されていますので、各ガイドラインの「第三者」に係る記載を確認してください。

ガイドライン（通則編）3-6-3

ガイドライン（外国にある第三者への提供編）2-2、3、4

ガイドライン（第三者提供時の確認・記録義務編）2-1-2、2-1-3

（第三者提供の制限の原則）

Q 7-16 弁護士法第 23 条の 2 に基づき、当社の従業員の情報について弁護士会から照会があった場合、当該従業員の同意を得ずに弁護士会に当該従業員の情報を提供してもよいですか。

A 7-16 弁護士法第 23 条の 2 に基づく弁護士会からの照会に対する回答は、「法令に基づく場合」（法第 27 条第 1 項第 1 号）に該当するため、照会に応じて提供する際に本人の同意を得る必要はありません。

（第三者提供の制限の原則）

Q 7-17 刑事訴訟法第 197 条第 2 項に基づき、警察から顧客に関する情報について照会があった場合、顧客本人の同意を得ずに回答してもよいですか。同法第 507 条に基づき、検察官から裁判の執行に関する照会があった場合はどうですか。

A 7-17 警察や検察等の捜査機関からの照会（刑事訴訟法第 197 条第 2 項）や、検察官及び裁判官等からの裁判の執行に関する照会（同法第 507 条）に対する回答は、「法令に基づく場合」（法第 27 条第 1 項第 1 号）に該当するため、これらの照会に応じて個人情報を提供する際に本人の同意を得る必要はありません。要配慮個人情報を提供する際も同様です。

なお、これらの照会は、いずれも、捜査や裁判の執行に必要な場合に行われるもので、相手方に回答すべき義務を課すものと解されており、また、上記照会により求められた顧客情報を本人の同意なく回答することが民法上の不法行為を構成することは、通常考えにくいいため、これらの照会には、一般に回答をすべきであると考えられます。ただし、本人との間の争いを防止するために、照会に応じ警察等に対し顧客情報を提供する場合には、当該情報提供を求めた捜査官等の役職、氏名を確認するとともに、その求めに応じ提供したことを後日説明できるようにしておくことが必要と考えられます。

【当協会の解説】

(第三者提供の制限)

第 27 条① 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。

- 1 法に基づく場合
- 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。
- 3 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。
- 4 国の機関若しくは地方公共団体又はその委託を受けた者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、本人の同意を得ることにより当該事務の遂行に支障を及ぼす恐れがあるとき。

個人情報保護委員会の Q & A 15 分類には、「第三者提供」に関係する項目が非常に多くあります。これは、27 年改正法には個人情報を管理統制するだけでなく、活用できるようにするという側面があるのではと思っています。

防犯設備士が個人情報を第三者に提供する時には、目的×提供者×提供条件などの様々なケースのパターンのどれに該当するかを検討して、条件が合う場合は提供を考えるが、それ以外では提供しないとするかなどの明確な判断が大切です。

そもそも、防犯設備士がアドバイスする防犯カメラに関する個人情報取扱事業者は、防犯を目的に設置し管理しているのですから、提供する第三者と提供条件は法第 27 条第 1 項第 1 号、第 2 号又は第 4 号の規定により、弁護士法や刑事訴訟法などにもとづき、弁護士会や捜査機関、裁判所からの照会などに絞られます。

マンション管理組合が設置した防犯カメラ等の記録画像を、自ら定めたルールにもとづき確認することは、個人情報取扱事業者の当然の行為であって、「第三者」への提供には該当しません。しかし、管理人室のモニター画面が、マンション出入りの宅配業者等にも見える向きになっていると、「第三者」への個人データの提供になる可能性があるので注意が必要です。また、1-5 に記載の様にマンション管理組合が、マンション管理会社にデジタルレコーダの管理を任せる場合は、委託先の監督が必要になります。

防犯設備士は、デジタルレコーダのモードロック機能(*)の管理者権限を使い、画像流出のトラブルを防止する方法をマンション管理組合などに指導してください。

(*) モードロック機能は、デジタルレコーダの操作権限(ランク)を登録する機能。モニター画面を表示する、表示するチャンネル(防犯カメラ)を制限する、記録画面を見る、機器内の機能を登録する、記録取り出し権限を登録するなど、機器取扱いの操作権限(ランク)ごとに、操作者を決めて制限する機能。コンビニエンスストアなどでは、防犯カメラ画像を従業員が見ることができないように設定するところもある。

1-7 第三者に該当しない場合（共同利用） P58

（第三者に該当しない場合）

Q 7-49 各共同利用者を「責任を有する者」とし、それぞれが開示等の請求権や苦情を受け付けることとすることはできますか。

A 7-49 可能ですが、法第 27 条第 5 項第 3 号の規定に基づき、各共同利用者を「責任を有する者」としていることが明確にされていることが必要です。

（第三者に該当しない場合）

Q 7-50 防犯目的のために取得するカメラ画像・顔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。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、Q 1-14 を参照のこと。

（令和 5 年 5 月更新）

(第三者に該当しない場合)

Q 7-51 過去に取得した個人データを特定の事業者との間で共同利用することは可能ですか。

A 7-51 一般に、個人データを共同して利用する場合には、①共同利用する旨、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、その代表者の氏名について、個人データの共同利用を開始する前に、本人に対して通知するか、本人が容易に知り得る状態に置く必要があります(ガイドライン(通則編)3-6-3(3)参照)。これに加えて、既に事業者が取得している個人データについて共同利用を検討する際には、当該個人データの内容や性質等に応じて共同利用の是非を判断した上で、当該個人データを取得する際に当該事業者が法第17条第1項の規定により特定した利用目的の範囲内であることを確認する必要があります。

(令和3年9月更新)

(第三者に該当しない場合)

Q 7-52 既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合について、「社会通念上、共同して利用する者の範囲や利用目的等が当該個人データの本人が通常予期しうると客観的に認められる範囲内」に含まれる場合とは、どのような場合ですか。

A 7-52 取得の際に通知・公表している利用目的の内容や取得の経緯等にかんがみて、既に特定の事業者が取得している個人データを他の事業者と共同で利用すること、共同して利用する者の範囲、利用する者の利用目的等が、当該個人データの本人が通常予期しうると客観的に認められる場合をいいます。

(平成30年12月追加)

【当協会の解説】

(第三者提供の制限)

第27条⑤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、前各号の規定の適用について、第三者に該当しないものとする。

3 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、共同利用して利用する者の範囲、利用する者の利用目的及び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。

ショッピングセンターや空港などでは、敷地や建物の防犯のために防犯カメラ等をビル管理会社などが設置します。各テナントや関連会社は独自に設置した防犯カメラ画像とビル管理会社の防犯カメラから分岐して提供される画像を使う場合もあります。

防犯カメラの画像は個人情報ですので、複数団体が1台の防犯カメラの画像を共用すると、法第27条の第三者提供の制限に抵触する恐れがあります。その場合に、上記の法第27条第5項第3号の規定にもとづき、必要な事項を本人に通知などを実施すれば対応できます。マンションのエレベータかご内の防犯カメラ画像をエレベータ会社から分岐して提供されている場合などでも、条件が適しているか注意が必要と思います。

(なお、同規定の下線部分は、令和4年4月施行)

1-9 保有個人データに関する事項の公表等（法第 32 条～第 39 条関係）、など P70

（保有個人データの開示）

Q9-10 電磁的記録の提供による方法で保有個人データを開示する場合において、本人が指定したファイル形式や提供方法による開示が技術的に困難な場合には、どう対応すべきですか。

A9-10 個人情報取扱事業者は、本人が保有個人データの電磁的記録の提供による方法による開示を請求した場合には、当該方法による開示が困難である場合を除き、電磁的記録の提供による方法（本人が請求した方法）でこれを開示する必要があります。

この場合、個人情報取扱事業者は、電磁的記録のファイル形式（PDF形式、Word形式等）や電磁的記録の提供方法（電磁的記録を記録媒体に保存してこれを郵送する、電磁的記録を電子メールに添付して送信する、ウェブサイト上で電磁的記録をダウンロードさせる等）を定めることができ、本人がファイル形式等を指定した場合であっても、これに応じる必要はありません。

このため、個人情報取扱事業者は、本人が指定したファイル形式等による開示が困難な場合には、個人情報取扱事業者において対応可能なファイル形式等で開示すれば足りる。もっとも、本人の利便性向上の観点から、できる限り本人の要望に沿った形で対応することが望ましいと考えられます。

（令和3年9月追加）

（保有個人データの開示）

Q9-13 顔識別機能付きカメラシステム等に顔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 顔識別機能付きカメラシステム等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、法令に基づき開示請求等に適切に対応しなければなりません。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しなければなりません。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しなければなりません。

（平成 30 年 12 月追加・令和 5 年 5 月更新）

【当協会の解説】

保有個人データの扱いは、14 頁 Q1-56、Q1-57 の解説を参照してください。

1-10 講ずべき安全管理措置の内容 P79

(全般)

Q10-7 標的型メール攻撃や、その他不正アクセス等による個人データの漏えい等の被害を防止するために、安全管理措置に関して、どのような点に注意すればよいですか。 A10-7 ガイドライン（通則編）に記載されている技術的安全管理措置の各項目を遵守することや、それらについて従業者に対して必要な研修・注意喚起を行うことに加え、次のような措置を講ずることが考えられます。

- 不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用すること。
- 巧妙化する攻撃の傾向を把握し、適宜必要な対策を従業者に周知すること。
- 個人データを端末に保存する必要がある場合、パスワードの設定又は暗号化により秘匿すること（なお、データの暗号化又はパスワードによる保護に当たっては、不正に入手した者が容易に解読できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮することも有効な取組と解されます）。

また、内閣サイバーセキュリティセンター（NISC）や独立行政法人情報処理推進機構（IPA）等がホームページで公表しているセキュリティ対策等を参考にすることも考えられます。

（令和5年3月更新）

(全般)

Q10-8 カメラを設置してカメラ画像・顔特徴データ等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・顔特徴データ等が個人データに該当する場合には、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ず、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、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、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のため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

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。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 年 5 月更新）

（人的安全管理措置）

Q 1 0—13 従業者との雇用契約において守秘義務を定めたり、派遣社員の派遣元との間の契約において派遣社員の守秘義務を定めることは義務付けられますか。

A 1 0—13 人的安全管理措置として、義務付けられるわけではありません。ただし、人的安全管理措置及び従業者の監督（法第 24 条）の一環として、従業者との雇用契約において守秘義務を定める等の対応を取ること、有効な取り組みと考えられます。なお、関係業法において守秘義務が定められている場合もあるため、留意が必要です。

【当協会の解説】

1-10 講ずべき安全管理措置には、特に防犯カメラ等については A 1 0—8 に①組織的安全管理措置、②人的安全管理措置、③物理的安全管理措置、④技術的安全管理措置、⑤外的環境の把握として具体的内容が示されています。

①組織的安全管理措置、②人的安全管理措置、③物理的安全管理措置については、各都道府県などが定めている「防犯カメラの設置及び運営に関するガイドライン」（名称が若干違う場合もあります）などを参考にして、「防犯カメラの設置・運用要領」などを事前に作成してください。

ネットワークに関連することは、個人情報保護委員会のガイドライン Q&A の、（別添）講ずべき安全管理措置の内容のうち④技術的安全管理措置の各項目に、様々な内容が記載されています。

平成 28 (2016) 年ロシアのウェブサービス「INSECAM」のサイト上に日本の防犯カメラのマンションエントランス、飲食店の厨房、葬儀会場などの画像と、それ以外のウェブカメラの画像と合わせて約 6000 台強のカメラの画像が流出しました。設置時にパスワード登録ができていない、デフォルトパスワードを変更しないで使用したためでした。

また、海外製特定デジタルレコーダがマルウェア Mirai によりボット化され、米国政府機関に向けた大規模 DDos 攻撃が発生しました。このデジタルレコーダは日本にも存在し、関係機関から警告が出されました。

防犯設備士は、④技術的安全管理措置に対応するために、当協会が発行している「防犯カメラシステムネットワーク構築ガイドⅡ」の内容を理解してください。設置時にはネットワーク網の設計と管理に気を付け、日常的に脆弱性がある防犯カメラ等と無線ルータ及びスイッチングハブなどの情報に対応して、定期点検を行うなど、個人情報の漏えい等が起きない様に、万全の対応をしてください。

4-1 仮名加工情報と 4-2 匿名加工情報

「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（令和 3 年 9 月 10 日更新）には、4.1 仮名加工情報と 4.2 匿名加工情報についての記述があります。

「防犯カメラ」とか、「画像」とかの文字は見当たりませんが、個人情報をマスキング等によって仮名化するとか匿名化する、という表現がありますので、参考のために、関係が考えられる項目を紹介します。

4-1 仮名加工情報（令和 3 年 9 月追加）

4-1-1 定義

Q 1 4-1 匿名加工情報と仮名加工情報の違いは何ですか。
A 1 4-1 匿名加工情報は、特定の個人を識別することができないよう個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたもの（法第 2 条第 6 項）です。「個人情報」（法第 2 条第 1 項）に該当せず、本人の同意を得ずに第三者に提供することが可能です（匿名加工情報の取扱いに係る義務等については、ガイドライン（仮名加工情報・匿名加工情報編）3-2 参照）。
これに対し、仮名加工情報は、他の情報と照合しない限り特定の個人を識別できないよう加工した個人に関する情報（法第 2 条第 5 項）であり、仮名加工情報を作成した個人情報取扱事業者においては、通常、当該仮名加工情報の作成の元となった個人情報や当該仮名加工情報に係る削除情報等を保有していると考えられることから、原則として「個人情報」（法第 2 条第 1 項）に該当するものです。変更前の利用目的と関連性を有すると合理的に認められる範囲を超える利用目的の変更が可能ですが（法第 41 条第 9 項）、原則として第三者への提供が禁止されています（法第 41 条第 6 項）（仮名加工情報の取扱いに係る義務等については、ガイドライン（仮名加工情報・匿名加工情報編）2-2 参照）。

4-2 匿名加工情報

4-2-2 匿名加工情報の適正な加工

Q 1 5-6 個人情報を、安全管理措置の一環等としてマスキング等によって匿名化した場合、匿名加工情報として取り扱う必要がありますか。
A 1 5-6 匿名加工情報を作成するためには、匿名加工情報作成の意図をもって、法第 43 条第 1 項に基づき、施行規則第 34 条各号で定める基準に従い加工する必要があります。
したがって、匿名加工情報の加工基準に基づかずに、個人情報を安全管理措置の一環等としてマスキング等によって匿名化した場合には、匿名加工情報としては扱われません。また、客観的に匿名加工情報の加工基準に沿った加工がなされている場合であっても、引き続き個人情報の取扱いに係る規律が適用されるものとして取り扱う意図で加工された個人に関する情報については、匿名加工情報の取扱いに係る規律は適用されません。
(令和 3 年 9 月更新)

Q 1 5-8 匿名加工情報を作成するときに施行規則第 34 条各号に定める基準で求められている措置を全て行う必要がありますか。
A 1 5-8 匿名加工情報を作成するためには、法第 43 条第 1 項に基づき、施行規則第 34 条各号で定める基準に従い加工する必要がありますが、各号に定める措置を選択的に講ずれば良いものでなく、各号全ての措置を行う必要があります（ただし、該当情報が無い場合は当該措置を講じる必要はありません）。なお、プライバシー保護等の観点から追加的に措置を講じていただくことを妨げるものではありません。

Q 1 5—14 匿名加工情報を作成する過程において氏名等を仮 ID に置き換えた場合における氏名と仮 ID の対応表は、匿名加工情報の作成後は破棄する必要がありますか。また、氏名等の仮 ID への置き換えに用いた置き換えアルゴリズムに用いられる乱数等のパラメータについてはどうですか。

A 1 5—14 匿名加工情報の作成の過程において、氏名等を仮 ID に置き換えた場合における氏名と仮 ID の対応表は、匿名加工情報と容易に照合ができ、それにより匿名加工情報の作成の元となった個人情報の本人を識別することができるものであることから、匿名加工情報の作成後は破棄する必要があります。

また、匿名加工情報を作成した個人情報取扱事業者が、氏名等を仮 ID に置き換えるために用いた置き換えアルゴリズムと乱数等のパラメータの組合せを保有している場合には、当該置き換えアルゴリズム及び当該乱数等のパラメータを用いて再度同じ置き換えを行うことによって、匿名加工情報とその作成の元となった個人情報とを容易に照合でき、それにより匿名加工情報の作成の元となった個人情報の本人を識別することができることから、匿名加工情報の作成後は、当該パラメータを破棄する必要があります。

(令和 3 年 9 月更新)

【当協会の解説】

防犯カメラの顔認証機能がこれから急発展するように思います。また、プライバシー保護を求めのご意見も今後増えてくると思っています。これらは、防犯カメラシステムの記録機能が良くなっても解決できない場合があり、ライブ画像の見方や見せ方を適切にすることも重要になります。

防犯設備士にとっては、防犯カメラシステムの機能を適切に選び設置するだけでなく、現場での運用方法についても適切なアドバイスをすることが重要になっていると思います。さらに、現場によっては、匿名加工の方法の検討も必要になると思います。

3 防犯カメラに関するガイドライン

3.1 個人情報保護法と自治体の「防犯カメラ設置と管理に関するガイドライン」

平成 12 年警察庁は「安全安心まちづくり推進要綱」を発出しました。それを受けて、平成 13 年の大阪府から平成 20 年の福岡県まで、全都道府県で「安全安心まちづくり条例」（名称が若干違う場合もあります）が制定されました。

さらに防犯カメラについては、多くの都道府県で「防犯カメラの設置と管理に係るガイドライン」（名称が若干違う場合もあります）が示されました。

制定当時の防犯カメラと記録装置（テープ方式含む）は解像度が悪く、被写体が防犯カメラにかなり近くないと人物の特徴が分かりませんでした。しかし、現在設置される防犯カメラと記録装置（デジタルレコーダ）はハイビジョンやフルハイビジョンの高解像度が大半になってきました。

1-1 に記載の様に、27 年改正法では、防犯カメラで撮影し記録された画像は、電磁的記録として明確化され、特定の個人が識別できる場合には、個人情報に該当します。

3.2 宮城県の「防犯カメラの設置と運用に関するガイドライン」

平成 28 年（2016 年）10 月宮城県から示された「防犯カメラの設置と運用に関するガイドライン」には、27 年改正法の内容を踏まえて以下の内容が記載されています。

- ・対象となるカメラ（1）設置目的について

ガイドラインの対象に、防火・防災等を主目的にするカメラであっても、防犯目的を併せ持つカメラも含まれることを明記しています。

- ・撮影範囲、設置場所等について

27 年改正法第 16 条（利用目的による制限）に対応した撮影範囲の制限を記載していません。

- ・設置の表示について

「防犯カメラ設置」の表示と設置者等の名称を、犯罪抑止効果及びプライバシー保護の観点から求めています。

- ・管理責任者、操作取扱者について

防犯上必要な業務を遂行できる管理責任者と操作取扱者を指定することとしています。

- ・設置者等の責務及び撮影された画像等の適正な管理について

27 年改正法第 20 条（安全管理措置）及びその具体的に講ずべき措置を定めています。

- ・撮影された画像等の閲覧・提供の制限について

法令に基づく場合以外に、迷子や認知症等の行方不明の安否確認に必要な場合や災害発生時の被害状況の情報提供する場合など、県民等の生命、身体及び財産の安全の確保その他公共の利益のために緊急性がある場合等も対象としていて、提供方法についても細かく記載しています。

- ・防犯カメラの保守点検について

日常的な点検に加えて、定期的に保守点検を指示しています。また、パソコン等を使用する場合は、最新のウイルス対策ソフトの使用も指摘しています。

- ・業務委託について

防犯カメラの設置、施設管理業務、警備業務に加えて、動線分析等の業務を含めて、業務委託する際の具体的な注意事項を示しています。

- ・個人情報保護法の遵守について

記録された画像の中で個人情報に該当する場合は、個人情報保護法に基づき適正に取り扱うことを指示しています。

防犯設備士と防犯設備士（業）協会の方々は、関連するガイドラインを確認して、旧法時代に作成されたもの場合には、27年改正法に沿った考え方について関係部署と相談して、適切に対応するように努めてください。

なお、これらの内容は、当協会の **SES 標準 防犯用映像装置一般基準 SES E 3001-3** の **A.4 防犯カメラ管理規定「事例」** に詳しく掲載しています。

4 高機能防犯カメラの適法・適正な利用にあたって

執筆：東京都立大学法学部教授 星 周一郎

街頭設置カメラについては、その画質の向上をはじめとする機能の高度化に伴い、その法的な設置根拠や許容限界についても、新たな観点から議論をする必要があります。

1. 映像等情報の個人情報該当性

従来のアナログ技術で人物を撮影したカメラ映像は、「個人を容易に識別できないので個人情報にはあたらないが、警察での捜査の過程での他の情報との突合により、個人情報にあたる可能性があるもの」という、ややあいまいな位置づけだったといえます。

これに対し、高精細・高画質のデジタル画像では、画角等にもよりますが、それ自体で、個人を識別できる映像となる場合が圧倒的に多くなっています。個人情報該当性の判断では、個人の氏名まで識別できる必要はありません。「他の誰でもない、その人」であることがわかる情報、言い換えれば、本人と紐付けが可能な情報であれば、「個人情報」に該当します。そういった情報が悪用されれば、それと紐付いた本人に不利益が及びかねないため、個人情報として保護する必要が生ずるからです。そのため、そういった映像は、個人情報にあたることとなります。また、顔認証などに用いる対照データも、個人識別符号として個人情報にあたります（個人情報保護法 2 条・以下、個人情報保護法の条文番号は令和 3 年 4 月現在のものです）。

映像や識別符号が個人情報に該当するならば、カメラの設置者が個人情報取扱事業者であれば、個人情報保護法上の、(1)個人情報である段階での諸責務、(2)個人情報データベース等を構成する個人データとされた段階での諸責務、(3)個人データを保有する保有個人データに該当する段階での諸責務を、それぞれ遵守する必要が生じます。

2. 個人情報とプライバシー

カメラ映像が個人情報にあたるとなると、「えっ！　じゃあ、もう使ってはダメなの？」といった反応を示す向きもあるかもしれません。しかし、この認識は誤りです。個人情報保護法は「個人情報利用禁止法」ではありません。2017 年 9 月に表面化した「年金支給漏れ事件」などに象徴されるように、個人情報の適正な利活用は、むしろ有用・必須で、個人に利益をもたらすものなのです。個人情報保護法自体も、適正な利活用を推奨しています（個人情報保護法 1 条）。

では、個人情報保護法は、こういった法律なのでしょうか。その内容をごく単純化しますと、個人情報を利用する場合には、①その利用目的をできる限り特定した上で（同法 15 条）、②その利用目的の達成に必要な範囲でのみ（同法 16 条）、本人に利用目的を通知しつつ利用（同法 18 条）すること、③個人情報を取得する際には適正な手段で行うこと

(同法 17 条)、をそれぞれ求めるというのが、基本的な構図となっています。また、個人情報データを整理した場合には、④個人データの第三者への提供は、原則として本人の同意なく行ってはいけない(同法 23 条)、という点が重要になります。よく出くわす、「個人情報だから教えられません」という場面は、この「第三者提供の制限」に関係します。

以上が遵守されるならば、映像が個人情報にあたるとしても、その利用は、個人情報保護法上、まったく問題なく可能なのです。

- ①利用目的の特定
- ②目的達成のために必要な範囲での利用・本人への通知
- ③適正な取得
- ④個人データの本人の同意を得ない第三者提供の制限

ところが、実は、個人情報保護法が定めるのはここまでです。それ以上の、①特定される利用目的の許容限界や、②「目的達成に必要な範囲」の具体的基準などについては、何も定めていないことに注意する必要があります。極論すれば、たとえば、いやがらせ目的で隣人の動向監視のために隣人宅を撮影しようとした場合、カメラの設置に際して、①「隣人の監視」として目的を特定し、②その目的達成に必要な範囲でのみ映像を利用し、その利用目的を本人に通知し、③隠し撮りでなく撮影し、④第三者提供もしないのであれば、個人情報保護法上は「適法」であることとなります。

もちろん、その隣人は抗議するでしょうし、社会一般の常識としても、そういった利用は許されないと考えます。この、「そういった利用は許されない」という常識的判断の根拠となるのが、「プライバシーの保護」なのです。個人情報保護法との関係では、①特定された利用目的の適切さの有無や程度、②「目的達成に必要な範囲」とはどこまでをいうのかの具体的な解釈が、「プライバシーを不当に侵害しないか否か」という観点で判断されるわけです。その意味で、利用態様の限界を最終的に画するのは、「プライバシー保護」なのです。このように、「個人情報の保護」と「プライバシーの保護」は、次元を異にする問題です。しかし、もちろん、両者は密接に関係します。少なくとも、個人情報保護法の認める利用枠組みが遵守されていなければ、不当なプライバシー侵害が発生することになります。

ただし、プライバシーは、きわめて錯綜した概念です。その議論は非常に難しいのですが、防犯カメラの設置の許容性という文脈では、個人の一定領域の情報をみだりに取得・利用されないことで、私生活の平穏を確保する、という意味合いで理解しておけば十分でしょう。

そして、目的が不当、あるいは、利用が必要な範囲を超え不適切と判断された場合、プライバシーの不当な侵害が生じていることとなります。その場合、公序良俗違反(民法 90 条)となり、不法行為(同法 709 条)による損害賠償責任等が生ずることとなります。

そもそも、民間の防犯カメラの設置・使用の根拠は、民法上の所有権(同法 206 条)や

施設管理権などに求められます。個人情報保護法は、個人情報を取り扱うことの「根拠」規定ではなく、扱い方のルールを定めたものです。そういった点も含め、カメラ映像が個人情報に該当することになるといっても、従来からの適切な利用態様であれば、基本的には適法性が認められ、従来どおり許容されるのです。

3. 生体認証機能の利用・許容限界

顔認証など生体認証機能を備えた防犯カメラシステムの許容性についても、個人情報保護法の次元とプライバシー保護の次元とで考えることになります。

プライバシー保護の観点から検討しましょう。顔認証機能付きのカメラシステムには、「プライバシーに対する影響が懸念される」とする指摘が、よくなされます。ただその場合、具体的にどういう事態が懸念されるのかは、実は明らかではありません。たとえば、万引き常習犯と疑われる者が来店した際、それを記憶している「警備員の目」で認証すると、顔認証システムで認証することで、ただちにプライバシーへの影響に差が生ずるわけでもないでしょう。また、「行動監視につながる」という懸念であれば、生体認証システムの利用そのものではなく、認証用のデータ（個人識別符号）の共同利用が許されるか、という問題であるようにも思います。本来、重要なのは、抽象的な印象論ではなく、利用実例毎の具体的な法的判断であるはずなのですが、どうしても議論が曖昧になってしまう傾向があります。

こういった曖昧さは、個人情報保護法上の適法性判断にも影響を及ぼします。生体認証機能付きであっても、それを防犯に使うのであれば、①防犯での利用という、利用目的の特定については、従来のシステムと変わるところはないはずです。他方で、②従来のシステムに加えて、生体認証機能を備えたシステムの利用が、防犯目的の達成に必要な範囲での利用と認められるか、という点については、プライバシーの観点での議論が曖昧であることもあり、その具体的内容は、必ずしも明確ではありません。また、かつては、防犯目的での生体認証システムの利用については、社会一般のコンセンサスが必ずしも得られているとはいえない状況にもありましたが、現在では、その利用への理解も広まりつつあります。こういった、プライバシー概念の不明確さに加えて、国民一般の認識に時代や社会状況による変化もあることが、具体的な許容限界が画一的に明確にならない、1つの要因であるともいえます。

生体認証システムの利用に理解が広まりつつあるとはいえ、それに不安を感じる消費者等も一定数存することも否定できません。そういった方たちに関しては、たとえば、認定個人情報保護団体制度（個人情報保護法 47 条以下）に基づき、苦情に対して丁寧に対応し、不安を払拭する枠組みを構築することが望まれます。その際には、不安や苦情の文脈も様々ですから、より関連性の高い認定個人情報保護団体に関する情報の提供や、当該団体の紹介といった対応も有効であると思われます。

4. マルチ・ユースへの要望と対応

また、生体認証機能等を備えたカメラシステムを、防犯のみではなく、商用に使うという「マルチ・ユース」へのニーズも、今後増加が予想されます。

こういった利用の許容性も、基本的には、防犯カメラの場合と同じ枠組みで判断されます。個人情報保護法上は、①「商用」のより具体的な目的を特定し、②その目的達成に必要な範囲であれば、基本的には許容されることとなります。ただ、現時点では商用での街頭設置カメラ映像の利用は、まだ「社会常識」とまでは必ずしもなっていないため、設置表示などにより、利用目的の通知やそのための情報の取り扱いに関する情報提供は、より丁寧に行うことが求められるでしょう。

また、②特定された目的が、個人識別性がなくても、たとえば、単なる人数分析や年齢・性別と行った属性分析でも達成できるのであれば、個人識別性を除去した映像データを用いるべきこととなります。その場合、その意味で、マルチ・ユースに用いる場合のカメラシステムは、技術面も含め、より複雑になる可能性があります。たとえば、実画像を録画データとして残しつつ、普段の商用利用等としては、復元できない形で個人識別性を除去した匿名加工情報（個人情報保護法2条9項）、または、特定の個人との対応関係が完全に排斥された統計情報（個人情報保護委員会『匿名加工ガイドライン』参照）としての利用のみを行うようにする一方で、防犯目的等での利用の必要がある場合には、個人識別性のある映像データを利用するといった枠組みを設定し、その適正な利用の枠組みを、弁護士などの第三者の立ち会いなどにより保障することなどが考えられます。この点については、個別の事情に応じた慎重な検討が望まれるところです。

さらに、プライバシー保護の観点で考えると、現状では、防犯目的での個人情報の利用に比較して、商用での利用については、世論の抵抗感はより強い状態にあるように思われます。そうであれば、その利用についても、相応の慎重な検討が必要となるでしょう。

5. 防犯活動としての映像の利用

窃盗が疑われる者の映像を、顔にモザイクをかけてインターネット上に公開し、そのモザイクを除去しないこととの引き換えに盗品の返還を求める、といった事案が散見された時期がありました。

こういった手法は、防犯カメラ映像の利用としては、許容されるものではありません。犯人の検挙や盗品の取り戻しを自ら行うのは、現代の法治国家では原則として認められない「実力行使」「自力救済」にあたりかねません。個人情報保護法上も、「窃盗が疑われる者」の個人情報を、本人の同意を得ないで第三者提供（公開）することは、法令に基づく捜査の一環、その他警察からの問い合わせへの対応としての警察への提供以外は、基本的に認められません。防犯カメラ映像の「防犯という利用目的の達成に必要な範囲」としては、それが基本となります。

他方で、窃盗が発生しないようにする「戸締まり用心」は、私人が自ら行うべき事項です。防犯カメラ映像を不審者の早期発見、警戒のために設置者自ら使うことは、従来からある「鍵掛け」による防犯を、さらに進めたものとして認められることとなります。とりわけ、転売の容易性や換金性が高まる中、被害額が1億円単位に達するような組織的集団窃盗など、「万引き」という範疇にはとどまらない甚大な被害も生じていますし、「自ら行う犯罪対策」への店舗側の要請も強まる一方です。

その要請に応えるため、たとえば顔認証機能の利用が認められるかの判断は、個人情報保護法上許容できる枠組みでも、最終的には、それを世間が納得するかという社会の常識に求められます。それは、プライバシー保護、言い換えれば、私生活の平穩確保に関する社会常識がどこに求められるかの判断です。

もっとも、何が適正な判断であるかは、具体的な場面ごとに即した個別的なものになります。たとえば、隣人トラブルで、一方が他方の家の私有地を撮影できるカメラを設置するような場合は、たとえ防犯目的があつたとしても、撮影される側にとって「社会通念上受忍すべき不利益の程度を超え」る影響を及ぼすもので、違法であるとされます（東京地裁平成21年5月11日判決）。住宅建設の際の施行上のトラブルで、和解に基づき、施工業者が、当該住宅の解体工事期間中に、現場への不審者の侵入や資材の盗難防止のために解体現場を撮影する防犯カメラを設置した場合には、プライバシー侵害はないとされた例もあります（東京地裁平成28年9月14日判決）。さらに、撮影された映像の取扱いについても、たとえば、店内での万引きの様子を撮影した映像をメディアに提供して放映させるような行為には、万引きの増加に警鐘を鳴らす番組での利用であれば公益目的があり、適法ですが、当該カメラの納入・設置会社が防犯効果を宣伝するために、自社のホームページで宣伝することは違法とされています（東京地裁平成22年9月27日判決）。いずれも、大方の理解の得られる常識的判断といえると思いますが、こういった、個別の事情に基づいた具体的な判断が必要となります。

また、この「社会の常識」は、先にも言及したように、時代や社会状況によっても変化します。平成20（2008）年にスタートしたGoogleのストリートビュー・サービスは、当初はプライバシー侵害を懸念する声も大きかったのですが、現在では、広く受け入れられています（福岡高裁平成24年7月13日判決参照）。また、店頭での顔認証機能付きカメラシステムの導入には、「行動監視されたり、趣味・趣向が丸裸にされたりするのでは」との懸念が一部でなされますが、他方で、店舗での購買履歴等が記録されるポイントカードの利用や、あるいは、ネット通販等の閲覧・利用履歴が事業者によって把握されることについて、躊躇の声は少ないようです。

社会の常識、納得感の見極めには、たしかに困難な面があります。それが、この問題の解決の方向を見えにくくしているのです。なお、文末に、カメラの設置や撮影データの利用の是非が実際に裁判で争われた事例のいくつかを列挙しましたので、参考にしていただければと思います。

6. 個人情報保護ガイドラインや防犯カメラ条例・ガイドラインの意義

顔認証機能なども含め、現在の高機能化したカメラシステムの設置・利用がどこまで認められるかについては、2つの次元で考えるべきことになります。

第1は、撮影される映像や個人識別符号に個人情報該当性が認められることを前提に、個人情報保護法の規定を遵守することです。そうであれば、個人情報保護法の枠組みにおいても、その利用は適法なものとなります。これが、必要最低限です。

第2に、個人情報保護法上許容されるとしても、その利用が社会的に許容されるかは、社会がプライバシー保護として何を求めるか、という「社会の常識」にかかってきます。それは、犯罪状況にも左右されるし、プライバシーとして具体的に何を求めるのか、現実空間とサイバー空間とでの認識の相違など、より複雑な方程式になっています。

その判断は、最終的には、④高機能なカメラシステム等を利用することに得られる利益、⑤それがプライバシーの利益に及ぼす影響がどの程度なのか、それを丁寧に説明するという透明性の確保が何より重要です。ストリートビューが受容されたのも、撮影された者が撮影内容を確認できるという意味で透明性がより確保されやすく、被撮影者自身も他の場所の撮影データを利用することで利益を享受できるシステムであった面も大きかったと考えられます。

そして、その両者の比較衡量から、⑤があるとしても一定程度にとどまり、④がより優越することに、社会一般の理解が得られるかという点に、そのシステムの利用が許容されるかの判断がかかってきます。

もっとも、一般論としてはそう言えるとしても、具体的な判断はやはり困難です。そういった場合に手がかりになるのが、個人情報保護法を所管する個人情報保護委員会の公表したガイドラインです。本冊子は、そのガイドラインの内容を、防犯カメラに即してさらに詳しく説明したものとして非常に有用です。また、自治体によって制定されていることのある防犯カメラ条例や防犯カメラ利用ガイドラインも参考になります。それらを参照しつつ、防犯カメラシステムの適切な設置・運用に努めることが、システムに対する信頼を確保し、防犯目的をより適切に達成するために必要となるのです。

【参考】民間部門でのカメラの設置・映像データの利用をめぐる判例・裁判例一覧

1. カメラの設置・映像の利用が適法とされた事例

・名古屋高裁平成 17 年 3 月 30 日判決（裁判所ウェブサイト）

コンビニエンスストアにおける防犯ビデオカメラによる店内の撮影、録画には、目的の相当性、必要性、方法の相当性が認められ、被控訴人（コンビニエンスストア経営者）が警察にビデオテープを提供したことは、違法なものとは認められないとした事例

・福井地裁平成 21 年 4 月 22 日判決（労働判例 985 号 23 頁）

病院が設置した防犯カメラは勤務する医師の行動を監視するために設置されたとは認められず、映す範囲からすれば医師に何らかの損害が生じているとも認められないから、カメラの設置行為が勤務する医師に対するパワーハラスメントに当たり、医師のプライバシーないし人格権を侵害したとは認められないとした事例

・京都地裁平成 21 年 9 月 25 日判決（判例時報 2066 号 81 頁）

学生向けの単身者用マンション（本件建物）の所有者が、防犯目的及び入居者の使用状況を確認する目的で防犯カメラを設置することは正当な管理業務の範囲内であるということができ、また、設置態様としても、1 階玄関前天井部分に 1 個設置したものであって、所有者が本件防犯カメラの映像で知り得るのは、本件建物への出入りのみであるから、入居者のプライバシーを過度に侵害するということもなく、所有者の監視行為が不法行為となるということとはできないとした事例

・東京地裁平成 22 年 7 月 28 日判決（判例時報 2092 号 99 頁）

介護付有料老人ホームの入居者が食事中誤燕事故で死亡した事案で、老人ホーム開設者が、本件事故の原因究明のために最も重要である食堂の様子を録画していたビデオテープを本件事故発生後 10 日後に消去したとしても、不法行為を構成するものではないとされた事例

・東京地裁平成 24 年 12 月 20 日判決（D1-Law.com 判例体系：29022899）

原告が自らの所有する建物に隣接する建物の所有者である被告に対し、被告所有の建物に設置された防犯カメラ及び構築物によって、原告及び原告の家族の平穩に生活する権利及び原告の建物所有権が妨害されているとして、これらの物件の撤去を求めるなどしたが、本件防犯カメラは、原告建物の 2 階及び 3 階の窓を撮影することができるものの、現在では、原告建物の窓はその隅が映る程度にカメラの角度が設定されていること、他方、

被告において、防犯のために本件防犯カメラを設置しておく必要性がないとはいえないことの各事情を総合考慮すれば、本件防犯カメラが、原告の相隣関係における受忍限度を超えるものであるとまではいえず、被告にこれを撤去する義務があるとはいえないとされた事例

・東京高裁平成 28 年 9 月 14 日判決 (D1-Law.com 判例体系：28243686)

原告が、被告に対して、別件訴訟における和解に基づいて被告が住宅の解体工事を行った際に、原告に無断で、現場を不在にする約 2 週間弱の期間、不審者の侵入、現場に置いてある資材の盗難防止のため防犯カメラを設置したことが違法であることの確認を求めるとともに、当該違法行為により精神的苦痛を被ったとして、不法行為に基づく損害賠償請求を行った件に関し、実際にプライバシーが侵害された訳ではなく、本件防犯カメラの設置に当たっては、原告との間で事前に協議をすることが望ましかったとはいえるものの、本件防犯カメラの設置目的、設置状況、設置期間からすると、被告による本件防犯カメラの設置行為が、直ちに、不法行為に該当する行為と認めることもできないとして、原告の確認の訴えを却下して、損害賠償請求を棄却した原判決が維持され、控訴が棄却された事例

・東京高裁平成 29 年 9 月 28 日判決 (D1-Law.com 判例体系：28253770)

学校法人である一審被告の設置する病院にて、統合失調症と診断され、医療保護入院となった一審原告が、当該病院の医師の行った診断は誤診であり、また一審原告に対し、監視カメラのある部屋に入院させなければならない理由を説明しなかったという説明義務違反により精神的苦痛を被ったとして、一審被告に対して、民法 715 条に基づき損害賠償請求を行った件に関し、監視カメラは隔離室における自傷他害行為の防止、行動制限中の行動把握、安全管理等という正当な目的で設置されており、原告は、本件病院で診察を受けた当時、早急な入院加療が必要であるが、本人に病識がなく、現実検討能力が低下している状態であったのであるから、原告に対して監視カメラがある部屋に入院となることを説明した場合には、不穏となり、上記設置目的を達成できない蓋然性があったと考えられるため、本件において、被告には、原告に対し監視カメラがある部屋に入院させなければならない理由を説明すべき義務があったということとはできず、被告がそうした説明をしなかったとしても、その対応が不法行為に当たるとはいえないとして原告の請求を棄却した原判決が維持され、控訴が棄却された事例

・【参考】横浜地裁令和元年 10 月 10 日判決 (労働判例 1216 号 5 頁)

被告が経営するスーパーマーケットで勤務していた原告が、商品を会計せずに持ち帰ったことを理由になされた懲戒解雇について、これが無効であると主張して争った事案において、本件懲戒解雇の有効性については、本件懲戒解雇及び予備的に行った本件予備的解

雇意思表示は、いずれも、客観的合理的理由を欠き、社会通念上相当であると認められず無効であるとされたものの、同店精肉部門のチーフが、従業員から、原告が何か持ち帰った疑いがある旨の報告を受け、防犯カメラの映像をチェックし、原告が発泡スチロールを抱えて帰宅したこと、同日原告がレジで精算を行っていないことをそれぞれ確認して懲戒解雇自由の存在を確認したことについて、当該防犯カメラの設置・利用の是非は争点とされていない。

・【参考】福岡高裁平成 24 年 7 月 13 日判決（判例時報 2234 号 44 頁）

インターネット上で提供されている「ストリートビュー」と題するサービスにより、ベランダに干していた洗濯物を撮影・公表されたため強迫神経症及び知的障害が悪化した上、転居を余儀なくされたとして、控訴人（1 審原告）が、プライバシー侵害等を理由に損害賠償を請求した事案について、本件画像が、本件居室やベランダの様子を特段に撮影対象としたものではなく、公道から周囲全体を撮影した際に写り込んだもので、ベランダに掛けられている物については判然としないから、一般人を基準とした場合には、私生活の平穏が侵害されたとは認められないとして、1 審判決（請求棄却）に対する控訴を棄却した事例（最決平成 26 年 3 月 4 日〔D1-Law.com 判例体系：28270813〕で控訴人の上告棄却〔上告不受理〕）

2. カメラの設置・映像の利用が違法とされた事例

・福岡地裁平成 17 年 3 月 29 日判決（裁判所ウェブサイト）

原告が、道路を挟んで向かい合った所に住んでいる被告から、原告宅にゴミを投げ込まれたので人格権を侵害されたとして、ゴミの投げ込み禁止とゴミによって壊れた原告宅の補修費用、慰謝料を請求したのに対し、被告は、ゴミの投げ込みの一部を否認し、原告からカメラで被告宅を監視され、人格権の侵害を受けたとして、カメラの撤去などと共に、慰謝料を請求した事案で、双方の慰謝料の請求の一部を認容し、原告にカメラを被告宅に向けないよう命じた事例

・松山地裁平成 21 年 3 月 25 日判決（労働判例 983 号 5 頁）

観光バス会社による配車差別及び事務室への監視カメラ等の設置は、同社労働組合に対する不当労働行為に該当し、その構成員らに心理的圧迫及び経済的打撃が加えられ、労働組合としての人格的利益の中核である自由な組合活動の萎縮ないし抑制という損害を被ったことが認められ、不法行為を構成するが、組合員のプライバシー権が侵害されたとまでは認められないとした事例

・東京地裁平成 21 年 5 月 11 日判決（判例時報 2055 号 85 頁）

近隣の住人同士であるYらとXらとの間でトラブルが激化し、Yらが、Xらに対する監視目的をもって、テレビカメラを設置し、Xら居宅（駐輪場と玄関付近）及び居宅前の私道を継続的に撮影してきたことを認定した上で、私道部分はXら居宅の敷地ではないものの、Xらが居宅から外出する際には必ず通る部分であって、Xらの日常生活に密着した空間であることが認められるから、Xらは、私道部分においても、その敷地内におけるのと同様にプライバシー権の保護を受けることができるとし、また、Xらが自らの生活状況をテレビカメラの監視対象とされることを承諾したものと認められないとして、Yらのテレビカメラによる継続的撮影行為は、Xらのプライバシー権を侵害するものとして違法であるとした事例

・東京地裁平成27年11月5日判決（判例タイムズ1425号318頁）

原告らが、被告が共有する区分所有建物の共用部分である庇等の屋外にカメラ4台（以下「本件全カメラ」という。）を設置して原告らを監視しているとし、これらの行為が原告らのプライバシーを侵害していると主張して、不法行為に基づき、被告に対し、本件全カメラの撤去及び損害賠償を求めたところ、本件カメラの1台の撮影が、常に行われており、原告らの外出や帰宅等という日常生活が常に把握されるという原告らのプライバシー侵害としては看過できない結果となっていること、他方、被告は、当該カメラの設置について、被告所有建物の1階居室の南側窓とその窓付近を撮影して防犯を図るものであるとするが、窓の防犯対策としては二重鍵を設置するなどのその他の代替手段がないわけではないこと、その他上記の種々の事情を考慮すると、当該カメラの設置及びこれによる撮影に伴う原告らの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、その撤去請求及び損害賠償請求の一部を認めたが、本件全カメラを設置する行為は、階段室をエレベータ室に改造することや屋根・廊下の一部を管理人室に改造することのような、形状又は効用を確定的に変える行為ということではできないから、共用部分の「変更」には当たらず、本件全体建物の区分所有者の過半数ではなく、また、議決権の過半数を有する者でもない原告が、本件全体建物の区分所有権に基づいて、これらのカメラの妨害排除請求をすることはできないとされた事例

・東京地裁平成29年10月18日（LLI/DB判例秘書：L07230402・D1-Law.com判例体系：29037989）

被告ら共有の土地の一部を賃借し、同土地に建物を所有し居住している原告らが、被告Y1に対し、各カメラの撤去等及び損害賠償などを求めた事案で、本件各カメラの設置は、原告自宅からの外出や帰宅等のため本件通路を通行する度に本件各カメラに写り込むなどし、原告らの生活実態が把握され得るものであって、原告らのプライバシーを侵害するものであり、本件各カメラの設置の必要性は原告らのプライバシー侵害を正当化し得るものではないから、そのプライバシーに基づき、各カメラの撤去を求めることができると

したうえで、精神的苦痛を慰謝するために不法行為に基づく損害賠償を認容した事例

・名古屋地裁令和元年9月5日判決（裁判所ウェブサイト）

原告らの住所地付近の土地に分譲マンションの建設計画を立て、本件マンションの建設を行った被告らが、本件マンションの建設中、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原告らが各住居に出入りする様子等を撮影したことにより、原告らの肖像権、プライバシー権、表現の自由である本件マンションの建設現場付近でマンション建設に反対する反対運動を行う自由及び集会の自由である同反対運動のため集会を開催する自由が侵害されたとして、原告ら各自が、被告らに対し、民法709条、719条の共同不法行為に基づく損害賠償請求として、連帯して、慰謝料及びこれに対する遅延損害金の支払を求めた事案で、ある者の容ぼう等をその承諾なく撮影することなど、原告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、原告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、原告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いうべきであるとしたうえで、防犯カメラの1台はダミーカメラであって、ある原告宅の撮影は行われていなかったものの、合理的な理由なく、撮影機能があるカメラと同一形状の防犯カメラ1台を当該原告宅の方向に向けて設置することは、当該原告の平穏な生活を害するものであり、被告らが当該原告に対する嫌がらせ目的であるとまでの認定はできないとしても、少なくとも当該原告の平穏な生活を害することになることは理解したうえで設置していると認められるから、不法行為に該当するとして、当該原告の請求を一部認容した事例。

3. 防犯カメラの設置・撮影は適法であるが映像の利用について（一部）違法とされた事例

・東京地裁平成18年3月31日判決（判例タイムズ1209号60頁）

防犯ビデオの映像を写真週刊誌に掲載した場合に、防犯ビデオの設置目的を超えて違法に肖像権を侵害するものであるとされた事例

・東京地裁平成22年9月27日判決（判例タイムズ1343号153頁）

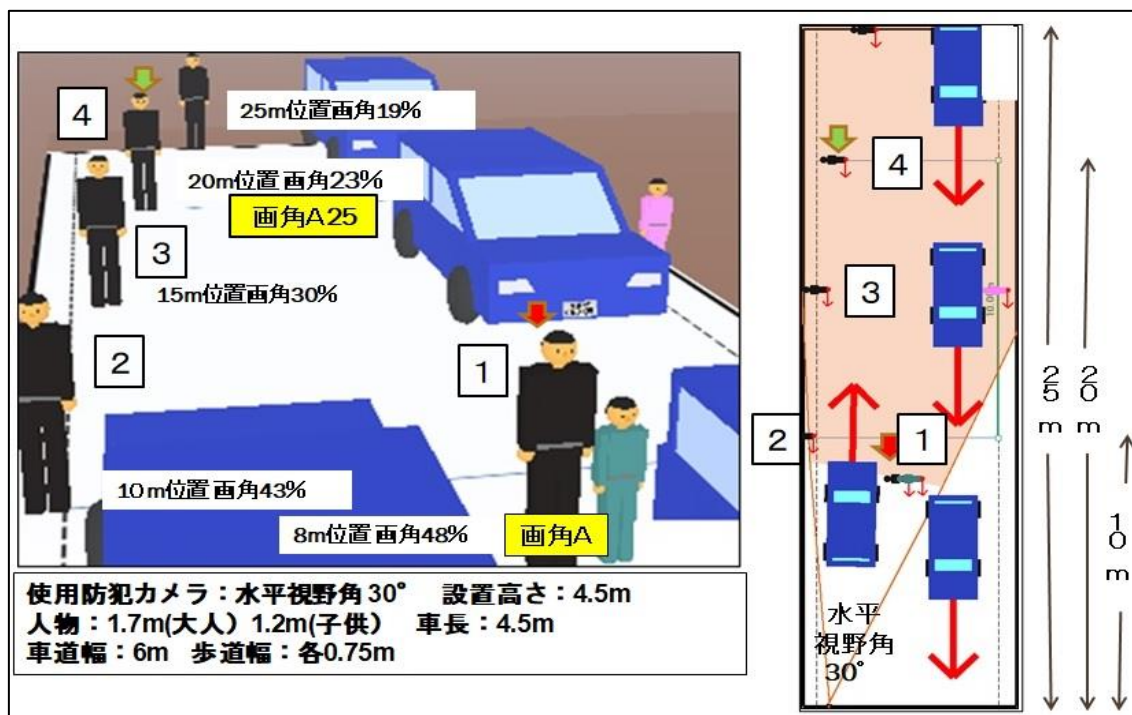
コンビニエンスストアの防犯カメラによる店舗内の客の撮影が不法行為法上違法でなく、当該カメラにより撮影された個人の映像を報道機関に提供して公表したことは、公益を図る目的があり、カメラの設置目的等に間接的ながらそうものであるから、不法行為法上違法でないが、カメラ設置会社が、自社製品の販売促進を目的として、映像の放映及び配布をする行為には、専ら公益を図る目的があったとは認められず、不法行為法上違法であるとされた事例

・東京地裁平成 31 年 1 月 16 日判決 (LEX/DB インターネット : 29052263 ・ D1-Law.com 判例体系 : 29052263)

被告が、報道機関に対し、被告のタクシーに乗車中の音楽活動等を行っている原告を撮影したドライブレコーダーの動画 (本件映像) が収録された記録媒体を、原告に無断で提供した行為は、原告の人格的利益及びプライバシー権を侵害するものであり、本件映像がテレビ番組で放映され、また、インターネット上でも拡散したことにより、精神的苦痛を被ったと主張して、被告に対し、不法行為による損害の賠償として、慰謝料及び弁護士費用の合計 1100 万円の支払等を求めた事案において、本件提供行為の目的に公益性が認められず、本件映像が必ずしも秘匿性・プライバシー性の低い情報とはいえ、本件提供行為に至る経緯にやむを得ない事情が認められないことからすれば、本件提供行為として違法性を阻却されることはないとし、原告の請求額を減額して一部認容した事例

5 解像度と画像使用目的

下図は、6mの歩車道一体型の道路に人物と車を配置して、4.5mの高さに設置した街頭防犯カメラを使って撮影した条件でシミュレーションした3D画像です。



使用ソフト：3D画角シミュレーションソフト TOA (株)

防犯カメラ方式 解像度と使用目的	画角C (バストショット)	画角B (全身)	画角A (50%)	画角A25 (25%)
アナログ	人相の認識	人物の特定	行動把握	全体把握
フルハイビジョン	人相の認識	人相の認識	人物の特定	行動把握

NTSC(アナログ)防犯カメラでもフルハイビジョン防犯カメラでも撮影する範囲は同じです。しかし画像中の人物や車などがどこまで鮮明に撮影し記録されるかは、使用する防犯カメラの方式と解像度によって大きく異なります。

当協会は、基準身長1.7m人物が撮影範囲に占める大きさを「画角」として、防犯カメラの方式ごとに、各々の画角ごとの最適な使用目的を決めています。

上図では人物①は「画角A」で、アナログでは動きが分かる行動把握ですが、フルハイビジョンなら人物の特定が分かります。人物④は「画角A25」で、アナログでは人数が分かる程度の全体把握ですが、フルハイビジョンなら人物の行動が把握できます。

防犯設備士は、防犯カメラの設置をする時には、防犯カメラの解像度と撮影できる視野角から、撮影目的に合う設置場所と撮影範囲を見極めてください。もし、人物の特定や人相の認識に関係する画角であれば、個人情報保護法の対応を検討してください。

6 顔識別機能付き防犯カメラシステム

従来型防犯カメラにも、動体検知や不動態検知及び車番検知などの検知と分析ができるシステムがありますが、令和5年5月に更新された個人情報保護法についてのガイドラインに関するQ&Aでいう顔識別機能付きカメラシステムとは、1.3で示されているように「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判別を行うシステムのこと」です。人数カウント機能があるから、文字判別機能があるからと言っても、顔識別機能付き防犯カメラシステムになるわけではありません。

顔画像から顔特徴データを抽出して顔判別を行う方法は、防犯カメラ単独で実施する場合、デジタルレコーダなどの自前のサーバ機能との組み合わせで実施する場合、クラウドなどの外部サーバと連携して実施する場合などの色々な方法があります。それぞれの実施方法によって、その後の対処方法が異なります。

顔識別機能付き防犯カメラシステムを使用する場合には、そのシステムが受け持つ機能などと、受け持つ管理者や運用、利用する組織などを事前に明確に把握して、個人データの漏えいや滅失などの問題が発生することのないよう必要な安全管理措置をとるとともに、問題発生時の混乱防止にも特段の注意が必要です。

7 防犯設備士と個人情報保護法

最近事件や事故が起きると、現場付近の防犯カメラの画像を利用した新聞報道やテレビ報道が行われます。

その場合、事件等の解決に役立てるため、「個人情報取扱事業者」である防犯カメラ（システム）所有者や管理者は、防犯カメラ画像確認や適切な画像提出が求められます。

防犯設備士は、防犯カメラの設計・設置にあたっては適切な防犯カメラの種類や解像度の選定とともに死角を極力少なくする配置と撮影範囲について指導して、さらに記録するデジタルレコーダの選定や、記録コマ数などのアドバイスも行っていると思います。

今後は、さらに、多くの「個人情報取扱事業者」と日常的な情報交換や防犯カメラシステムの整備と管理運用の協力を行い、「個人情報保護法」に関する対応についても、積極的にアドバイスできるように準備してください。

参考文献

- ① 個人情報保護法
<https://www.ppc.go.jp/personalinfo/>
- ② 「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
<https://www.ppc.go.jp/personalinfo/contact/>
- ③ 「防犯カメラの設置と管理に関するガイドライン」(宮城県)
<https://www.pref.miyagi.jp/soshiki/kyosha/gaidorain.html>
- ④ 防犯用映像装置一般基準 SES E 3001-3 (2019年9月21日改正)
(公社) 日本防犯設備協会
- ⑤ 防犯カメラシステムネットワーク構築ガイドⅡ (公社) 日本防犯設備協会
- ⑥ 2017AUTUMN 日防設ジャーナル No.118 爽秋号 (公社) 日本防犯設備協会
防犯カメラの高度化と法的規制の新たな動向 東京都立大学 教授 星 周一郎

執筆者

編集委員会：映像監視分科会

執筆担当委員	氏名	会員・会社名
主査	大野 眞裕	アイホン株式会社
委員	寺沢 慶一	NECプラットフォームズ株式会社
委員	松村 祐弥	TOA株式会社
委員	仁子 泰輔	TOA株式会社
委員	池上 貴則	東芝テリー株式会社
委員	古藤 晴洋	株式会社日立国際電気
特別委員	三澤 賢洋	(公社)日本防犯設備協会 特別講師 (起案担当)

事務局 公益社団法人 日本防犯設備協会
担当部長 関根晨貴、上原 実
< 2021年10月20日現在 >

なお、4章の「高機能防犯カメラの適法・適正な利用にあたって」については、東京都立大学 法学部 星 周一郎 教授によって執筆して頂いたものです。

防犯カメラと個人情報保護法の取扱い ～改訂版～

発行 2023年10月

編集 公益社団法人 日本防犯設備協会 映像監視分科会

この冊子は、著作権法で保護対象となっている著作物です。本書に記載の内容を転載される場合は、事前に(公社)日本防犯設備協会の承諾を得てください。この冊子についての意見又は質問は、(公社)日本防犯設備協会 事務局にご連絡ください。

発行所 公益社団法人 日本防犯設備協会

〒105-0013 東京都港区浜松町1-12-4 (第2長谷川ビル)

TEL:03-3431-7301 FAX:03-3431-7304 E-mail:info@ssaj.or.jp