防犯カメラや画像認識システムの安全利用のお勧め

万引防止システムをお使いいただきありがとうございます。日本万引防止システム協会の加入会員企業ではその製品の品質・機能において万全を期して設置・導入を進めております。

今後の重点施策として、未然防止や不審者発見のトリガーとしてのＥＡＳ機器導入による不明ロスの削減効果の向上に加え、新たに犯罪行為の再発防止につながる防犯画像技術などの新技術の利用を推進して参ります。その際、考慮しなければいけないことは、防犯データ〈文字・画像〉は、対象者の個人情報保護、肖像権、プライバシーの侵害等への法的な配慮が必要である点です。

新たに改正個人情報保護法が平成29年5月30日に全面施行されました。これにより、カメラで撮影した顔画像及びその画像から抽出した画像データで個人を識別できるものを個人情報と定義しており、防犯カメラ画像は、基本的に個人情報にあたることを前提に、来店者の理解を得る対応が必要となっています。具体的な対応としては、店頭や店内に「防犯カメラ設置（一例）」の告知POP掲示を徹底することなどが求められています。

（参考例）

また、個人情報保護法上は、例えば、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る顔認証データについて防犯以外の他の目的に利用する場合は本人の同意が必要であるほか、顔認証データなどの個人データを６か月以上保有する保有個人データとする場合、保有個人データに関する事項の公表、開示等請求対応、苦情の処理等に対応する必要があります。なお、個人情報保護法の概要や詳しい改正のポイントは個人情報保護委員会のホームページ（http://www.ppc.go.jp/）で確認できますので、本部担当者の皆様はチェックされますようお願いします。

万引を防止するために、できる限りの措置を講じることは、店舗の財産権を守るうえで当然の権利であるとともに、犯罪を抑止するという社会の要請に合致するものです。いわば、社会的責任であると言えます。防犯カメラに録画された防犯画像を活用することについても同様に考えられるべきであり、それが万引防止等に有効であり、かつ、個人情報保護法を遵守し、人権を侵害することのない範囲で、これを積極的に活用することが望ましいと考えます。

本書の概要

JEAS 日本万引防止システム協会

1 ルール

❶ 防犯カメラ管理規定（例）

防犯カメラの設置店は、防犯カメラ管理規定（例）に沿った運用をお願いします。

1．当店における防犯カメラの設置目的は、設置場所内の安全管理及び盗難防止に関して使用する物であり、記録を残す場合においてもこの目的のみに使用を限定する。
2．上記に基づき、店内には「防犯カメラ設置」や「防犯カメラ稼働中」の表示を行うことで、防犯目的であることを明示する。
3．記録に関しては、管理責任者を○○○○○、管理副責任者を○○○○○と定め、両名を管理者とする。管理者以外は記録内容に触れないものとする。
4．記録保持期間は、概ね○○とし、以後上書きを行う。（記録内容によって若干前後する。）
5．記録内容の確認及び、印刷等については管理者が行い、従業員に注意を促すものについては、守秘義務を結びセキュリティ教育を受けた従業員のみの閲覧とし、決して第三者に漏らさないこととする。
6．記録内容において第三者への提供を行う場合は必ず、記録されている映像の本人に同意を得ることとする。同意が得られない場合は第三者への提供を行わない。
なお、本人から本人の情報開示を要求された場合は、原則、それに応じなければならない。
7．上記につき、下記項目においてはこれを除外することができる。
① 法令に基づく場合：令状による捜査、任意協力等
② 人の生命身体又は財産の保護（本人の同意を得ることが困難であるとき）
③ 公衆衛生の向上等（同上）
④ 国の機関等への協力（本人の同意を得ることにより業務の遂行に支障を及ぼすおそれがあるとき）
なお、記録内容の提供にあたっては、提供日時や提供先、提供した画像の内容、提供目的、理由などを記録する。
8．管理者は防犯カメラの設置運用に関する苦情を受けた際は、誠実かつ迅速に対応し、必要な措置を講じる。
9．録画媒体等にメンテナンスを要する場合は、メンテナンス過程における録画データ漏洩を防止するため、保守委託先と秘密保持契約を締結する。また、録画用ハードディスクを交換する場合は、交換したディスクの廃棄方法・責任者を明確にすること。

【それ以外の推奨事項】

10．レコーダーは施錠できる部屋又は施錠できるケースに設置され、鍵の管理が行われている。管理者が鍵の管理をしていること。
11．管理者は上記の規定を定期的にチェックすること。

❷ 運用管理規定（例）

防犯データ〈文字・画像〉を利用する際は、運用管理規程（例）を参考にされ防犯データの安全利用をお願いします。

1．「防犯カメラ管理規定」を定め、理解し遵守すること。
2．防犯画像の活用の対象となる蓄積された個人情報は、店舗の万引防止の目的のために利用するものであり、犯罪を防止するという目的外の利用は絶対に行わないこと。
① 防犯画像及び業務上知り得た情報のSNS書込み禁止。
② 防犯画像及び業務上知り得た情報の口外禁止。

3．「個人情報保護」や「組織における情報漏洩防止」に関する教育を受けた管理者（以下、管理者という。）を配置すること。

4．データをサーバーやネットワーク上で管理する場合は、アクセス権限の明確化やアクセス・ログの記録保存やウィルス対策を確実に行ない情報漏洩や目的外の利用の防止に努めること。加えてデータを保存するコンピューター及びメモリーないしハードディスク等の記録媒体はワイヤーでロックするなど、持ち出しができないような物理的措置を講じること。
5．紙媒体は施錠できる部屋又は施錠できるケースに保管し、鍵の管理者が管理、管理者以外の持ち出しを禁止すること。
6．利用される情報の確認、印刷等については管理者が行うこと。また、情報を利用する従業員に対しては、必要な範囲でのみ情報を提供すること。
7．システムに登録したのち一定期間を経過してもシステムの対象とならない画像はこれを削除すること。またシステムに登録をしておく必要が無くなった対象はその期限に関係なく消去すること。
8．管理者を含め、関係する従業員等には、就業規則や或いは誓約書等で秘密保持のルールを守らせるとともに、セキュリティ教育を施すこと。

【管理責任者が異なる小売店の関係者間で情報を共同利用する場合】※

9．自社及び情報共有先会社に、防犯カメラ管理規定があり、遵守されていること、また、各店舗に「個人情報保護」や「組織における情報漏洩防止」に関する教育を受けた管理者が配置されていることを確認し合っておくこと。
10．相互に提供する画像は、警察への被害届けの際に警察に提示し、万引犯人に関する画像であること。または商品隠匿などの画像確認可能な映像がある確実な事犯であり、店長や総務部長によって確認されたものに限定すること。「疑わしい」だけの情報の共有はしない。
11．共有する画像は一定期間を経過してもシステムの対象とならない画像はこれを削除すること。またシステムに登録をしておく必要が無くなった対象はその期限に関係なく消去すること。
12．情報リスク対策のためにも共有する情報は防犯上必要最小限に限定し、法令に準拠した各社間の取り決めの範囲内に留めること。

※個人情報保護法上、共同利用を行う際には、① 共同利用をする旨、② 共同利用される個人データの項目、③ 共同利用する者の範囲、④ 利用目的、⑤ 責任を有する者の氏名又は名称を予め本人に通知し又は本人が容易に知り得る状態（例：ホームページの掲載やパンフレットの配布など）に置くこと、が必要です。詳細は、個人情報保護法第23条5項3号、同ガイドライン（52-55頁）、同Q&A（A5-28～A5-32）をご確認下さい。

2 考え方

❶ システム利用上の基本的考え方

システムが登録画像を検知した際も、お客様として、丁寧な対応に努めていただくよう徹底をお願いします。

1．画像認識システムや不審動作検知システム等でのアラートはその時点では犯人ではないこと、アラートの正確性が100%正しいものではないことなどを踏まえ、アラート対象者を犯人と決め付けない対応に終始すること。
2．防犯画像利用は万引防止策の一つとしてとらえ、これのみに依存しようとせず、その他の対策を十分講じつつ、これを補完するものと考えて活用すること。
3．社内ルールが不明確な状態で、画像情報が、個人を特定する他の情報と一体となった運用はなされないように配慮すること。

3 参考

❶ カメラ画像の取扱いに関する個人情報保護法Q&A

Q 1-11 **【防犯目的のためのカメラ画像や顔認証データの利用】**
店舗に防犯カメラを設置し、撮影した顔画像やそこから得られた顔認証データ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、どのような措置を講ずる必要がありますか。

A 1-11 本人を判別可能なカメラ画像やそこから得られた顔認証データを取扱う場合、個人情報の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認証データを利用しなければなりません。本人を判別可能なカメラ画像を撮影録画する場合は、個人情報の取得となりますので、個人情報の利用目的をあらかじめ公表しておくか、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ことが必要です。

防犯カメラにより、防犯目的のみのために撮影する場合、「取得の状況からみて利用目的が明らか（法第18条第4項第4号）」であることから利用目的の通知・公表は不要と解されますが、防犯カメラが作動中であることを店舗の入口に掲示する等、本人に対して自身の個人情報が取得されていることを認識させるための措置を講ずることが望ましいと考えられます。

また、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。

Q 1-12 **【商業目的のためのカメラ画像や顔認証データの利用】**
店舗にカメラを設置し、撮影した顔画像やそこから得られた顔認証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 1-12 本人を判別可能なカメラ画像やそこから得られた顔認データを取扱う場合、個人情報の利用目的をできる限り特定し、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とともに、当該利用目的の範囲内でカメラ画像や顔認証データを利用しなければなりません。

なお、防犯目的のみ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データについて、他の目的に利用しようとする場合、本人の同意を得る必要があります。

Q 1-13 **【カメラ画像から抽出した属性情報や移動軌跡データ（人流データ）】**
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に置き換えて作成した移動軌跡データ（人流データ）は、個人情報に該当しますか。

A 1-13 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、年齢、又は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、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。

結びになりますが、大規模チェーン店やグループ企業間などのように組織が大きくなれば、おのずと情報漏洩やデータの目的外利用のリスクが高まります。同一組織内であったとしても、①データの項目、②利用の範囲の明確化、③利用目的、④責任者を決めておくことをお勧めします。

【発行日】平成28年12月【改訂日】平成29年12月
【制　作】日本万引防止システム協会（略称：JEAS）
防犯データ〈文字・画像〉安全利用推進委員会
【連絡先】日本万引防止システム協会　事務局
〒160-0004　東京都新宿区四谷1-2-8
TEL：03-3355-2322　FAX：03-3355-2344
http://www.jeas.gr.jp　E-mail：info@jeas.gr.jp

JEAS-20171206