防犯カメラの取扱いに関する注意事項

佐倉市　危機管理課
＜平成２８年１１月＞

①防犯カメラの取扱いに関する注意事項

②防犯カメラの設置・運用するにあたっての注意

③防犯カメラの管理方法チェック表

① 防犯カメラの取扱いに関する注意事項

１．はじめに

佐倉市では、市民や地域コミュニティによる防犯意識の向上と防犯活動の増加により、市内の犯罪発生件数は、年々、減少傾向を示しています。

しかし、その一方で、「侵入盗難」、「乗り物盗難」、「不審者による声掛け」など、私たち市民の生活を脅かす身近な犯罪が依然として発生しており、市民が安全で安心して暮らせるまちづくりのため、さらなる防犯対策が必要となってきています。

２．防犯カメラの有用性

犯罪者は、犯行に及ぶ際、人に見られることを嫌うと言われています。

防犯カメラは、人の目が行き届かない場所や時間帯においても24時間の撮影ができるため、犯罪の抑止効果が期待されるとともに、万が一犯罪が発生した場合には犯罪者の特定にも役立つなど、その有用性は広く認識されています。

３．防犯カメラとプライバシー

一方で、防犯カメラは不特定多数の方が通行する公共の場所に設置されることが多いため、撮影される個人のプライバシーを侵害することがないよう、その取扱いには十分注意する必要があります。

また、人には自分の姿をみだりに撮影されたり、公表されたりすることのない自由があり、プライバシーの権利の一つとして、憲法第13条（個人の自由と幸福を求める権利）により保障されています。

防犯カメラは、犯罪の抑止や犯罪者の特定を目的とするものですが、撮影された個人の映像は、特定の人を識別することができる個人情報にあたる可能性があるため、個人のプライバシーを侵害しないよう、映像データやその関連機器は適切に管理しましょう。

４．個人情報について

様々な面から個人のプロフィールを表現したものが「個人情報」であり、犯罪者にとってはターゲットを選定するための格好のネタです。もし個人情報が流出すれば、犯罪に悪用されるおそれがあります。

個人情報が悪用された例は全国各地にあり、こうした犯罪への悪用を防ぐためにも、防犯カメラの映像データ等の個人情報は適切な管理が必要です。

【参考】個人情報保護に関する法律（抜粋）

（定義）
第２条　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って、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、それにより個人を識別することとなるものを含む。）をいう。

【参考】個人情報に該当する例

- 本人の氏名
- 生年月日、連絡先、（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
- 防犯カメラに記録された情報等本人が判別できる映像情報
- 特定の個人を識別できる情報が記載されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報
- 雇用管理情報（会社が従業員を評価した情報を含む。）

（出典）個人情報保護に関する法律についての経済産業分野を対象とするガイドライン

② 防犯カメラを設置・運用するにあたっての注意

１．設置運用基準の作成・遵守

防犯カメラの映像データや記録媒体について、漏えい、盗難、毀損、紛失などを防止するため、防犯カメラの設置及び運用に関する基準（設置運用基準）を作成し、自治会・商店会等で遵守していただくことになります。

２．防犯カメラの設置の場所と撮影の範囲

公共の場所に防犯カメラを設置する場合は、設置場所の所有者の許可が必要になります。どのような目的で設置するのかを明らかにし、その地域の関係者（住民、自治会、商店会等）や警察等と十分に話し合いましょう。

また、防犯カメラの撮影方向や角度を調整するなどして、撮影範囲を必要最小限にし、個人の住宅内などの私的空間（プライバシー）が映らないように注意しましょう。

３．防犯カメラの設置の表示

防犯カメラを設置した場合は、その周辺を通行する人に対し、あらかじめ防犯カメラが設置されていることを表示していただきます。

また、犯罪の抑止効果を高めるために、防犯カメラの設置場所付近に、防犯カメラを設置していることをわかりやすく表示し、表示には設置者の名称（団体名等）を記載してください。

４．管理責任者の設置、取扱担当者の指定

防犯カメラは、その取扱いを間違えれば個人のプライバシーの侵害につながりますので、管理・運用にあたって責任者を明らかにするため、管理責任者を指定することになります。

また、関連機器の操作や映像データの確認などを取扱う者を限定するため、取扱担当者を選びましょう。基本的に、防犯カメラや映像データは管理責任者や取扱担当者以外の者が取扱うことのないように、厳重な注意が必要です。

５．映像データの保存・廃棄方法

映像データを録画した記録媒体（CD、DVD、ＳＤカード、ＵＳＢメモリ、ハードディスクなど）や映像を閲覧するパソコン等については、管理責任者や取扱担当者以外の者の閲覧や盗難の防止のため、不特定多数の者が扱うことのできない施錠された場所の中で厳重に保管してください。

消費者庁によると、平成２５年（２０１３年）に発生した漏えい事故のうち紙媒体が１９１件（５２．２%）、電子媒体が１６８件（４５．９%）となっており、日常的に取り扱う文書の保護だけでなく、パソコン等や映像データを録画した記録媒体の保護が大変重要となります。

保管場所から個人情報が盗難される例もありますが、盗難・紛失事故の多くは、保管場所から外部に持ち出したときに発生しています。未然防止には個人情報を持ち出さないことが一番です。

映像データ等は施錠可能な場所に保管することは当然ですが、個人情報持ち出しの原則禁止と例外的に保管場所から持ち出すときの手続きと注意事項などのルールを定め、周知徹底することをお勧めします。

【参考】データ化された個人情報の漏えい事故例

- メールの一斉送信や誤送信に関する個人情報漏えい事故
- ＵＳＢメモリやパソコンに記録した個人情報の紛失・盗難事故
- インターネット上に個人情報が流出した事故
- 個人情報の廃棄や消去、再利用などに関する事故
- 不正アクセス・不正ログインによる個人情報の漏えい事故

【参考】自治会内で統一したルールを策定することが望ましい事案例

- 映像データを録画した記録媒体（CD、DVD、ＳＤカード、ＵＳＢメモリ、ハードディスクなど）や映像を閲覧するパソコン等などのウィルス感染の予防・防止
- 映像データを保存しているパソコン等のパスワード設定
- 防犯カメラの事務に携わらない人が、映像データを閲覧できないような措置

また、保存期間を過ぎた映像データや必要のなくなった映像データは、そのまま放置しておくと、個人情報が流出する危険性が高まりますので、映像が閲覧できないよう物理的に破砕、溶解等の処理を行うなど、速やかに廃棄してください。

【参考】自治会・商店会等でルールを策定することが望ましい例

データの保存方法	事案	廃棄の方法（例）
紙	不要になったり、書き損じたメモを廃棄するとき	シュレッダー処理後に廃棄
パソコン（ハードディスク）	パソコンを廃棄するとき	内蔵されているハードディスクを物理的に破壊した後に廃棄
	パソコンを買い替えるため、使用中のパソコンを下取りに出したり、中古販売店に売ったりするとき	データ消去ソフトなどを使ってデータを読み取れなくした後に、使用していたパソコンを手放す データが消去できていることを業者に確認してもらうなど
	リース契約等、使用中のパソコンを返却し、新しいパソコンを借りることになった	
映像データの記録媒体	録画された映像データの記録媒体（CD、DVD、ＳＤカード、ハードディスクなど）を廃棄するとき	物理的に破壊した後に廃棄

☆廃棄の経過をメモなどに残しておくこともポイントです。

個人情報の記録媒体は、シュレッダー処理や溶解処理など確実に廃棄しましょう。何の処理もせずに、一般ゴミや資源ゴミとして捨てられたことにより個人情報が外部に流出した例や個人情報等を保存したパソコンを適切に廃棄しなかったことによる個人情報漏えい事故の例も少なくありません。

６．映像データの保存期間

映像データの漏えい、盗難、紛失又は流出等の防止及びその他の安全管理を徹底するために、保存期間はできるだけ短期間とすることが望ましいです。長くても３０日以内を目安に必要な保存期間を定め、不要な映像データの保存はやめましょう。

７．映像データの利用・提供の制限

映像データを利用するため、パソコン等で映像データを取扱う際は、インターネット回線のない環境で取扱いましょう。また、映像データは他の記録媒体（CD、DVD、ＳＤカード、ＵＳＢメモリ、ハードディスクなど）に必要以上に複製することは避け、ＩＤやパスワードを使用してセキュリティ対策をしましょう。

また、防犯カメラの映像データを提供する場合は、プライバシーが侵害されることのないよう、次の場合を例外として、設置目的以外の目的に利用したり、第三者に提供してはなりません。

なお、提供については、提供日時や提供先、提供した映像の内容、提供目的、理由を記録するなどの基準を定め、適正に運用してください。

① 法令等に定めがあるとき。
② 人の生命、身体又は財産を保護するため、緊急かつやむを得ないと認められるとき。

他にも、メールやインターネットを日常的に使用することにより、データが漏えいするリスクも増大しています。電子媒体による漏えいの最大の特色は、事故１件あたりの漏えい人数・件数の大きさです。このことは、事故にかかわる事後処理コストの増大を意味します。また、不注意による漏えいも多く、文書の盗難・紛失と同様に、日常的な注意喚起が重要です。

８．守秘義務

管理責任者や取扱担当者等は、映像データそのものはもちろん、映像データから知り得た情報は絶対に他人に漏らしてはなりません。

また、管理責任者や取扱担当者等の立場でなくなった後についても、引き続き守秘義務があります。

９．苦情の対応

防犯カメラの設置・運用に対する苦情やお問合せに対しては、あらかじめ対応要領を定めておくなど、誠実かつ迅速に対応しましょう。

③ 防犯カメラ管理方法チェック表

１　設置運用基準の作成と遵守
- 防犯カメラの設置及び運用に関する基準を作成していますか　……　□

２　防犯カメラの設置場所と撮影範囲
- 防犯カメラの設置場所は所有者の許可をとっていますか　……　□
- 周辺住民（自治会、商店会等）や警察等と話し合いましたか　……　□
- 個人の住宅内などの私的空間が映っていませんか　……　□

３　防犯カメラの設置表示
- 防犯カメラの設置場所付近に設置者の名称を表示していますか　……　□

４　管理責任者の設置、取扱担当者の指定
- 防犯カメラの管理責任者を決めましたか　……　□
- 防犯カメラの取扱担当者を決めましたか　……　□

５　映像データの保存・廃棄方法
- 記録媒体やパソコン等は施錠して保管していますか　……　□
- 保存期間を過ぎた映像データ廃棄はしていますか　……　□

６　映像データの保存期間
- 映像データの保存期間は３０日以内にしていますか　……　□

７　映像データの利用・提供の制限
- 映像データはインターネット回線のない環境で取扱っていますか　…　□
- 映像データを必要以上に複製していませんか
- 映像データはセキュリティ対策をしていますか　……　□
- 映像データを提供する場合の基準を定めていますか　……　□

８　守秘義務
- 映像データ等の情報を他人に漏らしていませんか　……　□

９　苦情の対応
- 苦情やお問合せに対しての対応要領をきめていますか　……　□