【個人情報・プライバシーについて】

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１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るとされています。また、防犯カメラに記録された個人が識別できるような画像は、個人情報の保護に関する法律においても保護の対象となっています。

地域防犯カメラは犯罪の防止や犯罪者の特定を目的とし、不特定多数の方が通行する公共の場所に設置するものですが、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する必要があります。

また、個人情報が流出した場合には、犯罪に悪用される恐れがあります。犯罪への悪用を防ぐためにも、防犯カメラ等の個人情報は適切な管理が必要です。

ポイント①

防犯カメラの設置場所と撮影範囲

設置場所の選定については、鴻巣警察署生活安全課及び自治振興課立ち会いのもと確認してください。地域の犯罪発生状況等について警察から効果的な設置場所について助言をもらうことができます。

撮影範囲については、以下の空間が含まれないよう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する必要があります。

・ 住宅の玄関、窓その他日常生活の様子がうかがえる私的空間
・ 個人を認識することができる距離（顔が認識できなくても、人物が鮮明に映ることで個人が特定されうる場合も含みます。）の範囲内にある私的空間

また、防犯カメラのマスキング機能により私的空間が映らないようにすることも重要です。ただし、防犯カメラに映り込む住宅の住人などからそのことについて書面による同意が得られた場合は、マスキング機能による画像の黒塗りを外すことができます。

ポイント②

設置運用規程の策定と遵守

撮影された画像を自由に見ることができ、画像データを取り出せる状況は、プライバシーを侵害する恐れがあります。

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規程（設置運用規程）を策定し、自治会内で遵守していただくことが重要です。

ポイント③

管理責任者、運用責任者、画像取扱者の指定

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る可能性があるため、管理・運用にあたっては責任者を明らかにするため、管理責任者を指定することが重要です。

また、関連機器の操作や映像データの確認などを取り扱う者を限定するため、運用責任者、画像取扱者を選定してください。基本的に、防犯カメラや映像データは運用責任者・画像取扱者以外の方が取り扱うことのないように、厳重な注意が必要です。

防犯カメラの操作方向や画像の管理方法について、マニュアル等を作成することも大切です。

ポイント④

地域の合意

どのような目的で設置するのかを明らかにし、ポイント②で策定した設置運用規程をもとに自治会の総会等において十分に話し合いましょう。

また、防犯カメラを設置する建造物の所有者や設置場所の所有者、設置場所付近の方や撮影範囲に含まれる方に事前に説明し、同意を得ておくことが重要です。

ポイント⑤

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ください。

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（自治会（町内会）名）を記載してください。

ポイント⑥

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、管理責任者等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。

また、映像を閲覧するパソコン等などのウイルス感染の予防・防止や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も重要です。

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。廃棄の経過をメモなどに残しておくことも重要です。

ポイント⑦

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控えましょう。

ポイント⑧

映像データの利用・提供の制限

自治会内で、不法投棄と思われることや違法駐車と思われる事象が発生した場合に違反者特定のために映像データを利用することはできません。

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り扱う際は、インターネット回線のない環境で取り扱いましょう。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するほか、第三者に提供してはいけません。

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、提供の内容について記録簿に残す等適正に運用してください。

【提供する必要性があると考えられる場合】
１、法令等に定めがあるとき。
２、捜査機関から犯罪または事故の捜査目的で、文書により画像提供の要請を受けた場合。
３、個人の生命、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。

ポイント⑨

守秘義務

管理責任者や運用責任者等は、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を絶対に他人に漏らしてはなりません。

また、管理責任者や運用責任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。

ポイント⑩

苦情の対応

防犯カメラの設置・運用に対する苦情やお問い合わせに対しては、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てください。