連　載

新技術調査レポート

建築物の防犯・入退室管理設備の現況について

（一財）建築コスト管理システム研究所・新技術調査検討会

1　はじめに

令和３年は、無差別に他人へ危害を加える痛ましい事件が相次ぎました。鉄道関係では10月京王線、11月九州新幹線での車内放火事件があり、他方、12月大阪北新地のクリニックでも放火事件が起きました。これらの事件が起きる度に、監視カメラ(映像記録)の役割に対する意識が更に高まりました。また、コロナ禍が依然続く中、企業ではセキュリティの強化に加え、入室時にサーモカメラにより体温計測を行うなど、入室管理が日常化しています。

このような状況を踏まえ、建築物の防犯設備、監視カメラ設備、入退室管理設備について現況を紹介します。

2　防犯設備

防犯設備は「侵入者」による犯罪を阻止する目的で設置され、保護対象は人命と財産となります。

（1）防犯対策の基本

（公社）日本防犯設備協会発行『あなたのまちの安全対策』の冊子によると、防犯対策の基本は、犯罪企図者が嫌う四つの点、目、音、光、時間に留意することとあります（**表１**）。

表１　防犯対策の基本

視点	犯罪者の心理	防犯機材
目	見られていることを恐れる。	防犯カメラ テレビドアホン
音	音により露見することを恐れる。	サイレン 警報ベル
光	照明により、人目にさらされていることを恐れる。	LED防犯灯 サイレン付き人感ライト
時間	侵入までに時間がかかることを嫌う。	CP鍵 防犯ガラス

（2）防犯設備と監視カメラ設備の役割

防犯設備は検知センサにより侵入者を検知し、非常ベルなどで、建物内部の入居者・管理者へ異常を知らせます。これに監視カメラ設備を設ければ、犯罪者の監視・記録ができるようになります。

監視カメラは防犯カメラとも呼ばれますが、機器の違いはなく、受け止め方による表現方法の違いによるものです。**図１**に、防犯設備と監視カメラ設備のシステム概念を示します。なお、監視カメラ設備の詳細は、以降の別項目で説明します。

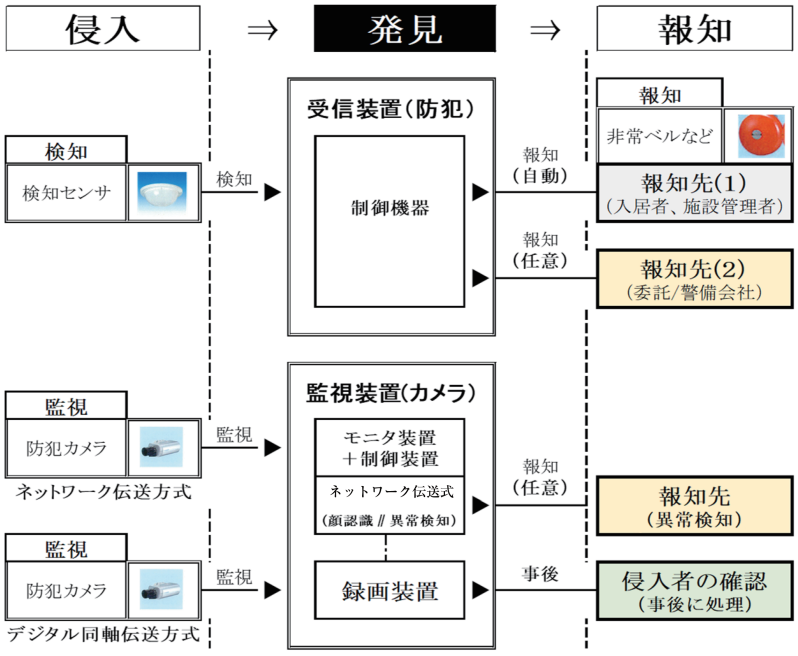


図１　防犯設備と監視カメラ設備の概念図

（3）防犯センサ

防犯センサは使用目的に応じて、多くの種類があり、センサの特徴を理解した上で取付け場所（窓、ドア、屋外フェンスなど）に応じた選定が必要になります。**表2**に各種の防犯センサの概要を示します。

表2　各種の防犯センサ

名　称	概　要
パッシブセンサ（受動型）	壁・家具の背景物体と侵入者などの表面から放射されている遠赤外線エネルギー変化（温度差）を検知するセンサである。
赤外線センサ（能動型）	可視光に近い領域（0.72−1.5μm）の近赤外線を利用している。投光部と受光部が分離した対向型などがある。
マグネットスイッチ	ドアや窓などに設置し、その戸の開閉を検知するセンサである。
ガラス破壊センサ	侵入者が窓ガラスを破壊した時に、その振動や音を検知するセンサである。 なお、音検知のものは、集音マイク付きでガラス破壊音センサと呼ばれる。
マイクロ波センサ	屋外の警戒用センサとして、特に雪や雨、霧などの悪天候時に信頼性の高い、対向型のセンサである。 赤外線センサの補助的なセンサとして使用されている。
フェンスセンサ	外周フェンスに終端ボックスから検知ケーブル（センサ）をコントローラまで配線して、フェンス全体で侵入者を検知して警備する方法である。

（4）その他の関連事項

警備会社による機械警備には、警備業法上の機械警備（警備員駆けつけ対応）と自主機械警備（事前登録者へ通報対応）があります。

機械警備では、「機械警備に関する努力義務」があり、「警備会社がセンサ等で異常発生を覚知してから遅くとも25分以内に警備員を現場に到着……」とされています。なお、北海道のように土地が広大な場合は、25分以内ではなく、30分以内となり、地域により異なる場合があります。

自主機械警備とは、異常時に通報する登録者を事前に決め、侵入者を検知した時に携帯電話などへ通報する仕組みです。なお、自動通報機能の装置が必要となります。

3　監視カメラ設備

監視カメラ設備は監視の目的で設置され、記録装置を備えれば犯罪状況の記録ができ、後の現況確認に役立ちます。更に、AIカメラのハードと関連ソフトを用いれば、不審者の検知、顔の認証など、セキュリティの強化に役立ちます。

設備構成は監視カメラ、モニタ装置、録画装置で構成されます。

（1）監視カメラ

1）監視カメラの種類

監視カメラの種別は、ボックス型、ボックス型のハウジング一体型、ドーム型、PTZ型（パン・チルト・ズーム）があります。

PTZ型はカメラ機器の遠隔操作が可能であり、Pan（左右上下）、Tilt（傾ける）、Zoom（望遠）の略称です。また、PTZ型は別名で「スピードドームカメラ」とも呼ばれます。**図2**に監視カメラの一例を示します。

図2　監視カメラの一例

出典：パナソニック㈱のホームページ

2）監視カメラ設備の伝送方式

監視カメラ設備の伝送方式は、ネットワーク伝

送方式とデジタル同軸伝送方式の二つがあります。

ネットワーク伝送方式は、構内LANを用い、画像データを圧縮して、LANケーブルで伝送します。また、デジタル同軸伝送方式は、画像データを圧縮しないで、同軸ケーブルで伝送します。**図３**に伝送方式による通信ケーブルを示します。

これらの監視カメラへの電源供給で留意する点は、PoE機能付き支線用スイッチ（Ｌ２）を使用する場合において、タイプにより電力消費量が異なることです。PoE Type 1 では12.95W、PoE Type 2では25.5Wとなります。

（注）PoE（Power over Ethernet）とはイーサネットの規格であり、LANケーブルを経由して、データ通信と同時に電力を供給することができます。

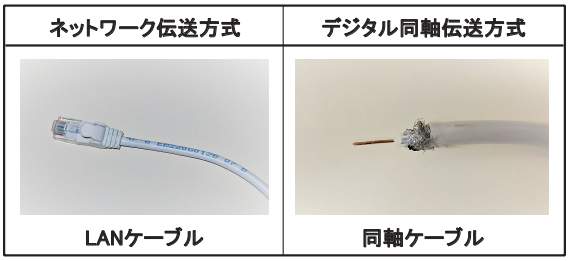


図３　伝送方式による通信ケーブル

（２）モニタ装置

モニタ装置は、監視カメラで撮った映像を視るための装置です。モニタサイズは、監視者とモニタの監視距離、画面分割数等により選定されます。

（３）録画装置

録画装置は、録画時間、画質（解像度ほか）等を実情に合わせ、デジタルレコーダなどが必要となります。

録画装置のデジタル記憶媒体の容量は、「デジタル記憶媒体の容量＞カメラ１台当たりの容量×カメラ台数」で計算されます。例えば、カメラ１台当たりは、「画像圧縮方式H.264」、「10日間」の場合に概ね「34GB」となります。

表３にデジタル記憶媒体の容量（参考例）を示します。

（注）「H.264」とは、2003年５月にITU（国際電気通信連合）によって勧告された、動画データの圧縮符号化方式の標準の一つです。

表３　デジタル記憶媒体の容量（参考例）

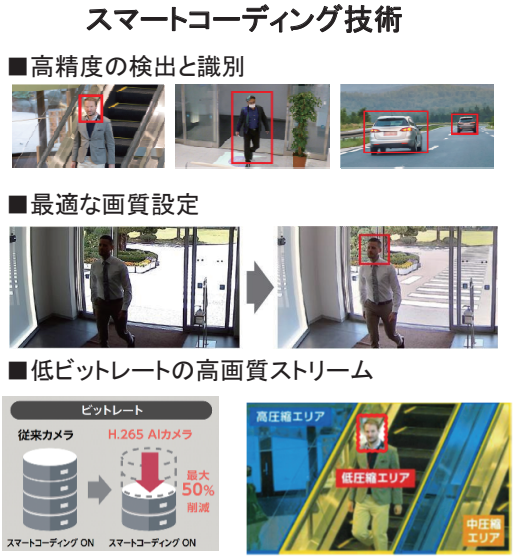
カメラ１台当たりの容量（参考）		
計算条件	カメラ台数	１台
	解像度	640×480
	伝送レート	300［kbps］
	録画時間	10日間
記憶媒体の容量		約34［GB］

（４）監視カメラの技術向上

１）AIネットワークカメラ

AIネットワークカメラでは、従来難しかった映像の分析・解析等の高負荷をカメラ内に「AIプロセッサ」を組み込むことにより、受信サーバの処理が分散され効率が向上されました。これらは、スマートコーディング技術、インテリジェントオート（iA）機能により、適正な画像圧縮、最適な撮影を向上させています。**図４**にAIネットワークカメラの技術の内容を示します。

（注）インテリジェントオート（iA）機能とは、カメラがシーンに応じて自動認識し、最適な撮影モードへ自動で切り換わり、更に背景のボケを調節できる機能です。



スマートコーディング技術とは
検知物体以外の領域の圧縮率を上げ、検知物体の有無に応じてリフレッシュ間隔及びフレームレートを最適化することにより大幅に帯域削減する技術。

（注）
1. フレッシュ間隔は、カメラの映像を1枚ずつ取り込んでいき、全カメラの取込みが終わる（1周する）までの時間。
2. フレームレート（fps）とは、1秒間に何コマの静止画が記録されているかという数値。
3. ビットレートとは「1秒間で送受信可能なデータ量」を示し、単位はbps（bit per second）と表記。

図４　AIネットワークカメラの技術

出典：パナソニック㈱のホームページ

2）監視カメラの検知機能

最近では、AIネットワークカメラでAIカメラとソフトウェアを用いて、不審者の動体検知、置き去り・持ち去りの物体検知、コロナ禍の体温検知などが可能となり、更なる研究・開発がなされています。

（5）その他の関連事項

1）クラウド活用の長所と短所

以前はSDカードや録画装置に画像データを保存して確認していましたが、最近ではインターネットなどのネットワークを経由した、クラウドサービスを活用し、遠隔地での確認が可能になりました。**表4**にクラウドの特徴を示します。

表4　クラウドの特徴

長所	短所
・遠隔地からの映像確認が可能である。 ・導入及び管理コストの削減が可能である。 ・検知・検索などの処理が可能である。	・インターネット回線の不具合時に映像確認、データ保存が不確実である。 ・サービス利用費が設定条件により影響が大きい。（カメラ台数及び保存期間など） ・外部LANの接続による情報漏洩のリスクがある。（セキュリティの脆弱性、データ消失など）

2）不審者検知の事例

人間は緊張すると、顔の皮膚に精神的なストレスによる一過性の“ふるえ”が現れます。これらを検知するソフトウェアが不審者事前検知システムです。2014年に行われたソチオリンピック、国内では2018年の伊勢志摩サミットなどでも採用されました。

4　入退室管理設備

入退室管理設備は建物内への「不法侵入者」を抑止する目的で設置され、様々な個人識別方法を用い、入退室の許可権限を付与されることにより、入退室ができます。本設備に、防犯設備、監視カメラ設備を加えると、セキュリティが更に強化されます。また、入退室記録を用いて、業務管理の効率化が図られます。

（1）建物内部のセキュリティ

1）セキュリティ区域の設定

入退室管理設備の計画では、最初にセキュリティレベルに応じた区域を、特定ゾーン、専用ゾーン、共用ゾーンとして定めます。**表5**にセキュリティレベル区域を示します。

表5　セキュリティレベル区域（室名）

区域	室名等
特定ゾーン	金庫、サーバ室など特に重要な場所
専用ゾーン	事務室など入居者が使用する場所
共用ゾーン	エントランス、通用口廊下など入居者も外来者も利用する場所

2）通行制限の環境

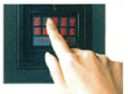
入退室者の通行制限には、セキュリティゲートの設置と電気錠付き扉・自動扉があります。これらはICカード、生体認証などの個人を特定する識別方法により入退室の制限が解除されます。

各ゾーン内の各室はセキュリティ内容に応じ、通常のカギ付き扉または電気錠付き扉・自動扉のいずれかを選択します。

（2）個人の識別方法

個人の識別方法には、**表6**に示す暗証番号、生体認証、ICカード、ハンズフリータグなどがあり、それぞれの認証装置を用い、登録された内容と合致すれば、電気錠・自動扉が解錠されます。

表6　個人の識別方法

識別方法	概　要	外　観
暗証番号	既設定の番号入力により解錠。	 パナソニック㈱
生体認証	体の特徴を認識し、既登録と認証装置で照合して解錠。	照合装置 （顔認証、指認証など）
ICカード	ICカードによる解錠。 （接触型、非接触型） （注）既存の社員証（ICカード）に識別チップを組込み可能	 非接触型 パナソニック㈱
ハンズフリータグ	小さな「タグ」を体や荷物につけ、「タグ」を認証して解錠。	 タグ  アンテナ ㈱日立パワーソリューションズ

出典：パナソニック㈱、㈱日立パワーソリューションズのホームページ

（3）生体認証

生体認証は個人の生体情報を「鍵」として扱うため、「なりすまし、カードの偽造」を防止できる効果があり、重要な場所に採用されます。

生体認証（バイオメトリクス）には、顔、虹彩、指紋、掌紋、指静脈、声紋などがあり、更なる生体認証技術の研究・開発が行われています。

これらを利用するためにはそれぞれの読取り装置とソフトウェア製品で運用でき、一例として、**表７**に一部の認証装置（指･顔の例）を示します。

表７　認証装置（指・顔の例）

装置名	外観
指静脈照合装置	 ㈱日立産業制御ソリューションズ
顔照合装置	 パナソニック システムソリューションズ ジャパン㈱

出典：㈱日立産業制御ソリューションズ、パナソニック システムソリューションズ ジャパン㈱のホームページ

5　生体認証

生体認証のうち、顔認証について述べます。

（1）顔認証の長所と留意点

顔認証とは、顔の「目・鼻・口・輪郭」などの特徴をカメラで読み取り、データベースに予め登録済の顔データと照合して、本人認証を行う、生体認証の一つとなります。顔認証装置は、顔検出機能（カメラ／認識部）と顔照合機能（ソフト／照合部）で構成されています。

表８及び**表９**に顔認証について利用者側の長所と管理者側の留意点を示します。

表８　顔認証の長所（利用者側）

長　所	備　考
１．パスワード忘れや紛失の心配がない。	暗証番号、ICカードは忘れや紛失が生じやすいが、生体情報は心配がない。
２．なりすましが防止できる。	ICカードやIDカードはそれ自体で盗用されるが、生体情報は心配がない。
３．利用者の処理時間の負担が少ない。	顔の識別から判定までの時間が短い。
４．両手が塞がっても認証できる。	ハンズフリーである。
５．非接触式なので衛生的である。	感染症リスクを低減できる。

表９　顔認証の留意点（管理者側）

留意点	備　考
１．顔認証システムによって認証精度に差がある。	・顔の経年変化や髪型の変化の認識精度に注意する。 ・マスクやメガネの着用の認識精度に注意する。
２．環境によって認証精度が落ちる。	・認証時に一定の照度が必要である。 ・屋外設置では雨天や逆光など屋外環境に対応したタイプを選定する。
３．顔データの取扱いは、細心の注意が必要である。	顔は個人情報の対象である。

（2）生体認証データの管理

個人情報保護法の一部改正が、令和２年６月に公布され、令和４年４月１日より施行となります。

改正内容の一部を紹介すると、「情報漏洩等が発生し、個人の権利利益を害するおそれが大きい場合」、以前は事業者による委員会への報告でしたが、新たに本人への通知が必要となります。漏洩等が生じると、対応処置の業務量が増加します。

個人情報管理への理解を深めるために、改めて、個人情報保護法における生体認証の位置づけを述べます。なお、詳細は、個人情報保護法を参照してください。

１）生体認証の位置づけ

個人情報保護法では、個人識別符号は大別して２種類に分けられています。これらは、個人情報の保護に関する法律施行令第１条第１号（イ～ト）の生体認証、第１条第２号～第８号のマイナンバー、基礎年金番号などがあります。

表10に個人識別符号（生体認証）を示します。

表10　個人識別符号（生体認証）

個人情報の保護に関する法律施行令（第１条第１号）

細胞のDNA	歩行の姿勢
顔の画像・動画	手の静脈の形状
瞳の虹彩	指紋・掌紋
声の特徴	

◆「第1条第1号」に示される個人識別符号は、身体の一部の 特徴を変換したデータが該当します。

・1 号個人識別符号は、ICTの進展によって生体認証に利用することが考えられる情報に対応しています。

出典：総務省ホームページ「ICTスキル総合習得教材」

2）個人情報の安全管理

現在、個人情報を保有するすべての事業所は「安全管理措置」の対策を講じる必要があります（第20条）。同法ガイドラインでは、「８　（別添）講ずべき安全管理措置の内容」に具体的な措置や手法が示されています。**表11**に一例として物理的安全管理措置の概要を示します。

表11　個人情報取扱事業者の安全管理措置等

物理的安全管理措置
①　**入退館（室）管理の実施**
（例）入退館（室）管理を実施している物理的に保護された室内での個人データを取り扱う業務など
②　**盗難等の防止**
（例）個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止
③　**機器装置等の物理的な保護**
（例）盗難、破壊、破損、漏水、火災、停電等からの物理的な保護など

出典：経済産業省ホームページ「個人情報取扱事業者の皆さんへ」

（3）その他の関連事項

1）非常時の電気錠動作

建物火災時の避難対策として、パニックオープン（非常時開放システム）があり、電気錠の施錠・解錠のあり方の検討が必要となります。また、これらのほか、長期停電時の電源確認も重要です。

6　おわりに

ここまで防犯設備、監視カメラ設備、入退室管理設備について、一般的なことを述べてきました。

防犯設備は「侵入者」の防止、入退室管理設備は「不法侵入者」の抑止、更に監視カメラ設備は監視・記録及び不審者の検知ができ、これらを組み合わせてセキュリティの強化ができます。

生体認証は「なりすまし・偽造」を防止するために設けられ、事前に生体情報の登録が必要となります。更に、生体認証は、個人情報保護法第１条第１号の個人識別符号に該当し、事業者は同法第20条により「安全管理措置」の対策を講じることとされています。

今後、生体認証技術の向上、システム間の連携、IoT（Internet of Things）への接続が進むことで、セキュリティ・利便性が更に向上すると考えられますが、生体情報の情報漏洩がないように充分な注意が必要となります。

本レポートが読者の防犯・入退室管理設備に対する理解に役立てば幸いです。

最後に、「建築物の防犯・入退室管理設備の現況について」をまとめるにあたり、パナソニック㈱ エレクトリックワークス社様には多大なご協力をいただきました。

ここに感謝の意を表します。

（参考文献）
1）（公社）日本防犯設備協会『あなたのまちの安全対策』（Ⅱ防犯対策の基本　1．犯罪者心理）
2）竹中エンジニアリング㈱カタログHP
3）パナソニック㈱カタログ（入退室管理システム：総合型セキュリティ eX-SGのご紹介）HP
4）国土交通省大臣官房官庁営繕部監修「建築設備設計基準」（令和３年版）（第９章監視カメラ設備）pp.316-321,（一社）公共建築協会，2021
5）㈱日立パワーソリューションズHPハンズフリータグ
6）㈱日立産業制御ソリューションズHP指静脈照合装置
　２―４【2】個人情報・個人データベース・個人データ
7）総務省「ICTスキル総合習得教材」
8）経済産業省「個人情報パンフレット（平成27年９月）個人情報取扱事業者の皆さんへ」
9）（一社）日本電設工業協会「特集最新のセキュリティ技術」『電設技術』平成28年５月号
10）KODANSHA「電車内の犯罪を防げ！不審者検知「ディフェンダー X」のスゴイ実力」FRIDAYデジタル，2021/11/15