ビル建築設備としてのセキュリティシステム

Security System for Building Management

藤森　敦　■FUJIMORI Atsushi
菅野　麻衣子　■KANNO Maiko
立川　寛　■TACHIKAWA Kan

入退室管理を行う場合，セキュリティポリシーの検討と運用は重要である。

ビルにおけるセキュリティポリシーには，利便性とセキュリティとを両立すべき対象向けのものと，セキュリティを重視すべき対象向けのものがある。前者に対しては非接触認証が可能な“顔照合技術”が，また，後者に対しては扉の工夫で一人ずつの正しい通行を実現する手法や，顔照合と人物監視を組み合わせた“モニタリングシステム”が有効である。

Security policy is important for access control in building management. There are two main objectives in applying security policy in building management. One is to secure compatibility of security and the occupants' convenience, for which a personal identification system using facial recognition is effective. The other is to give priority to security over other considerations. For this latter objective, Toshiba proposes not only a specially developed door system that allows only one person to enter at a time, but also a monitoring system that recognizes individual faces and is equipped with a video recording system.

1　まえがき

東芝は企業のビルを中心にセキュリティ機器を納入してきた。事業化を開始した十数年前は，磁気カードや接触式ICカードを用いた入退室管理システムが中心であった。その後，技術の進歩とセキュリティニーズの高まりがあいまって，入退室管理システムでは非接触式ICカードを用いたものが主流になり，更にバイオメトリクス（生体認証）を併用するケースも珍しくなくなった。一方で，監視カメラもあらゆるシーンで見受けられるようになり，犯罪捜査に効果を現したという話を数多く聞くようになってきた。

しかし，こうしたセキュリティ機器の普及やセキュリティ意識の高まりのなかで，世の中全般に目を向けてみると，必ずしも犯罪発生件数が減少してきているわけではない。特に企業においては個人情報の流出事件が多数発生しており，企業でのセキュリティ運用上に“セキュリティホール”の存在が疑われる。

ここでは，セキュリティシステム導入にあたって必須であるセキュリティポリシーの策定手順と，セキュリティ管理を適切に実現し運用するための技術について述べる。

2　ビル建築設備におけるセキュリティの考え方

2.1　セキュリティポリシー―何から何を守るのか

セキュリティ機器を導入するにあたってまず分析しておかなければならないのが，「何から何を守りたいのか」ということである。「今はセキュリティ対策を何もやっていないので何かやりたい」という話や，「他社が入退室管理をやっているのでうちもやりたい」という話を聞くこともあるが，そういう場合であっても，むやみにセキュリティ機器を勧めることはしない。それは，単にセキュリティ機器を導入すればセキュリティが確保されるものではなく，守りたいものと防ぎたい犯罪（特に侵入）の方法によって，導入すべきシステムが大きく異なってくるからである。

ビルにおける犯罪の種類とその対象，及び犯行手口の例を**表1**に示す。多くの場合は侵入者が犯行に及ぶ場合がもっとも脅威になるが，たとえ侵入者を完全にシャットアウトできても，関係者による犯行の余地が残されていては不十分である。関係者と部外者との適切な識別を行うとともに，関係者の中でも誰がどこに出入りしてよいのか明確に定めることが必要である。そのうえで，必要にして十分なセキュリ

表1．ビルにおける犯罪の種類と考えられる手口の例
Examples of various criminal techniques in buildings

犯罪の分類	対象		犯行手口の例
	オフィス	住居	
傷害，暴行，誘拐，痴漢	役員，職員，従業員，来訪者	居住者，来訪者	• 部外者又は関係者が侵入後，みずからの手であるいは凶器を用いて
破壊	建物，設備		• 部外者又は関係者が侵入後，みずからの手によりあるいは爆発物などにより
窃盗	金品（財産），設備，情報		• 部外者又は関係者が侵入後，みずからの手で持去り，あるいは盗聴，あるいは盗撮 • ネットワーク経由での情報持出し
騒乱	法人や団体の信用・名誉・経営，個人の信用・名誉	個人の信用・名誉	• 部外者又は関係者が侵入又は接近のうえ，掲示物・配布物・拡声器などにより

ティ機器を配置していく。また，監視カメラを設置することは犯罪抑止力の観点からも非常に有効であるが，監視したいものによって適切なカメラやレンズ，及び設置場所を選定する必要があり，画像を誰がどこで監視するのか，録画画像の保管期間についても定めなければ無用の長物となってしまう。

何から何を守るのか，すなわちセキュリティポリシーを定めたうえで的確なセキュリティ機器を導入することが重要である。当社では，防犯設備士(注1)の資格を持ったシステムエンジニアが顧客の要望をヒアリングしたうえで，目的にふさわしい機器を推奨している。

2.2 たまねぎ構造

守るべきセキュリティレベル（程度）が同一の空間をセキュリティゾーンと呼ぶ。このセキュリティゾーンは隣り合わせのゾーンとの境界が壁，仕切り，出入り口などによって明確に分けられたものでなければならない。また，セキュリティゾーンは，セキュリティレベルがより高いゾーンを，より低いゾーンが囲むように配置される“たまねぎ構造”が望ましい（**図1**）。たまねぎ構造を実現することにより，周りを囲んでいる低いセキュリティレベルのゾーンに対する警備対策が，高いセキュリティレベルのゾーンの防護に役だつからである。この構造は，工場や計算機センターから大規模なビルのセキュリティに至るまで，一般的に適用可能である。

2.3 セキュリティゾーンごとに必要とされる考え方

最近の大規模なビルでは複数の業種・業態の企業が同居しているケースが多い。業種・業態が異なれば「何から何を守るのか」は必然的に異なるが，各テナントのセキュリティポリシーはテナント入口以降（たまねぎ構造のレベル3，4）に反映される。一方で，不特定多数の出入りを管理する共有部である，レベル0（外周監視），レベル1（ロビー，共通会議室），レベル2（各テナント入口）はビル管理者の意向に沿った共通のポリシーが用いられる。

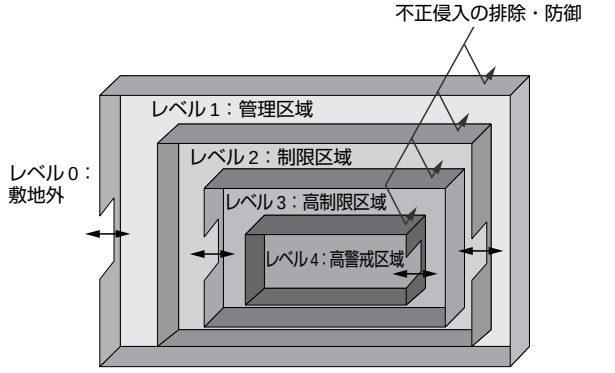

図1．たまねぎ構造のセキュリティゾーン— セキュリティレベルがより高いゾーンを，より低いゾーンが囲むように配置するたまねぎ構造が望ましい。
Basic structure of security zone

(注1) 警察庁所管の公益法人である（社）日本防犯設備協会が認定する資格で，防犯警報設備の設計，施工，維持管理を行うとともに，防犯診断や地域安全活動などへの参画を行う。

このような共有部におけるセキュリティに必要とされる考え方とは何であろうか。それは利便性とセキュリティとを両立させることによりセキュリティポリシーを正しく運用させることである。多人数の通行に耐えると同時に，大人数通行，荷物運搬なども妨げないシステムが必要とされる。

一方，大企業が所有する自社ビルや専用の建築物（計算機センター，研究棟など）においては，社員どうしという気軽さから運用がルーズとなるため，外部のいろいろな人間による侵入だけでなく，内部犯行に配慮した考え方が必要となる。計算機室，重要物（現金，重要情報，危険物など）の保管庫，コントロールルームなど，レベル3，4にあたるゾーンへのアクセス権限は限られた人物のみに与え，厳正に運用し，外部及び内部の犯行に備えるべきである。このようなケースにおいて重要となる考え方として，ひとり一通行を確実に実施することが挙げられる。ひとり一通行により，アクセス違反となる伴連れや逆流の防止が可能となる。また，アクセスを許可された者による犯罪を抑止したり検知するために，入室時間を管理する，室内外での挙動を監視するという考え方も重要視されはじめている。

3 セキュリティ運用を徹底する技術

ここでは，前節で示された考え方を実現する技術について述べる。

3.1 利便性とセキュリティを両立させる技術

利便性とセキュリティを両立させる一つの解は“非接触認証”である。非接触タイプのセキュリティ装置としては，非接触ICカードや非接触式バイオメトリクス装置が挙げられるが，ここでは後者の例として，当社が開発した“顔照合セキュリティシステム FacePass™”（**図2**）を紹介する。

顔照合には様々な利点がある。まず，カードと比較して，常に携帯する必要がない，貸し借りができないという利点である。また，顔照合は非接触式認証であり，扉の前に立てば自動的に本人を確認するので，高度のセキュリティを保ったうえで，荷物を持っていても煩わしくないといった利便性が得られる点である。もう一つは，照合時に装置のモニタに顔を映すとともに，顔画像が通行履歴に残るため，犯罪抑止効果を期待できる点である。通常，犯罪者は自分の顔が映されているという時点で犯行をあきらめる，と言われている。また，通行時の顔画像が履歴に残るため，特に内部犯行予備者への抑止効果も期待できる。FacePass™は，管理すべき扉が複数の場合には，1か所で登録した利用者の顔情報を，ほかの照合機に配信して運用するシステムを構築することも可能である。

図2．顔照合セキュリティシステム FacePass$_{TM}$ の外観 ― あらかじめ登録された顔とカメラからの顔を照合して扉を制御する装置である。
FacePass$_{TM}$ facial recognition security system

3.2　セキュリティ重視の技術

セキュリティ重視の考えを実現する技術として，扉設備を工夫することによりひとり一通行を実現する手法と，ひとり一通行の実現に加えて内部犯行の抑止と検知にも効果のある“顔照合モニタリングシステム”を紹介する。

3.2.1　扉設備によりひとり一通行を守る手法

セキュリティゾーンは壁，仕切り，出入り口などによって分けられる。通常の通行では出入り口によって人の出入りを制限することになるわけで，この出入り口でいかに厳密に有資格者と無資格者とを識別し，いかに厳密に無資格者の入場を排除するかがセキュリティ構築の成否を握っている。ところが安易な運用を許してしまえば，せっかくのセキュリティシステムもそこの部分がセキュリティホールになってしまうことがある。例えば，管理されたゲート（扉）を有資格者が通行した後から，続いて来た人がいっしょに通行してしまう伴連れや，退出するためにゲート（扉）を開けたとき，ほかの人が入場してしまう逆流がそれである。これらはもちろんセキュリティシステムの正しい運用ではないが，残念ながら多くの場面で目にする現実である。

ひとり一通行を実現させる一つの方法がインターロックである。前室を設けることとセンサにより人数をカウントすることにより，ひとり一通行といえども複数の有資格者を通行させることができるのが特長である（**図3**）。

これに対して，正しい運用をしつけることにより，必然的にひとり一通行を実現する方法がアンチパスバックとアンチフォワードである。**図4**に示すように連続した複数の扉がある場合，一つ目の扉から入場していないにもかかわらず一つ目の扉から出ようとした場合，通行違反として通行不可となる（アンチパスバック）。また，一つ目の扉から入場していないにもかかわらず，二つ目の扉から入場しようとした場合，通行違反として通行不可となる（アンチフォワード）。この仕組みは通常の扉を使って構築することができるため，既設の建屋にも比較的簡単に導入できる。

3.2.2　セキュリティが高く導入が容易な顔照合モニタリングシステム

前節で扉設備を工夫することによりひとり一通行を実現する手法を紹介したが，ここでは，顔照合

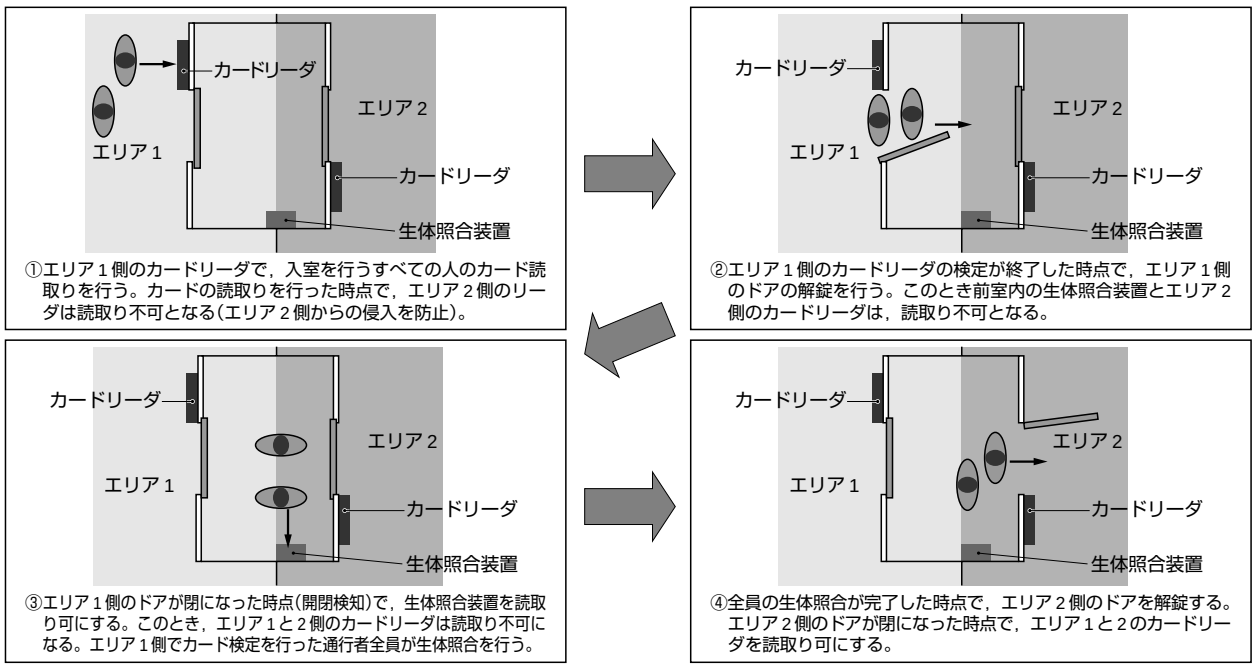

図3．インターロックの通行手順 ― 前室を設けることとセンサによる人数カウントにより，有資格者を通行させることができる。
Controlled access sequence using interlock system

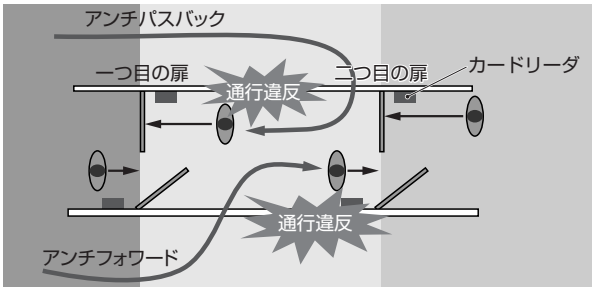

図4．アンチパスバック・アンチフォワードの通行違反例 ― 一つ目の扉から入場していないにもかかわらず一つ目の扉を出ようとした場合，通行違反として通行不可となり(アンチパスバック)，一つ目の扉から入場していないにもかかわらず，二つ目の扉から入場しようとした場合，通行違反として通行不可となる(アンチフォワード)。

Examples of access prevention by "anti-passback door" and "anti-forward door"

装置と監視カメラを連動させて，不審行動及び滞留時間をモニタで監視するシステムを紹介する。このシステムでは，顔照合セキュリティシステム FacePass$_{TM}$と"ウェブカメラによる照合時監視映像解析"とを組み合わせ，使用抵抗感が少なく，かつ確実な入室管理を提供できる(**図5**)。

このシステムの主な特長は，次の3点である。

(1) 顔照合での入室をトリガとして所在管理が可能

(2) 顔照合入退室前後の画像を監視可能

(3) 顔画像を検知・照合した場合だけ画像の蓄積が可能

このシステムでは，入退出時に顔画像が保存され，所在の管理，更には滞留時間の管理が的確に行われる。したがって，入室有資格者にも常に監視されていることを意識させるため，有資格者への抑止効果，つまりは内部犯行への抑止効果が絶大である。更には監視映像も，従来の監視システムのようにただ収集して保存する方法と違い，顔照合前後の画像が保存されるため，後で不審者や不審行動の検索が容易にできるメリットがある。また，前節で紹介した扉設備によりセキュリティを高める手法に比べ，付帯設備が少なく導入しやすい高セキュリティ実現の手法とも言える。

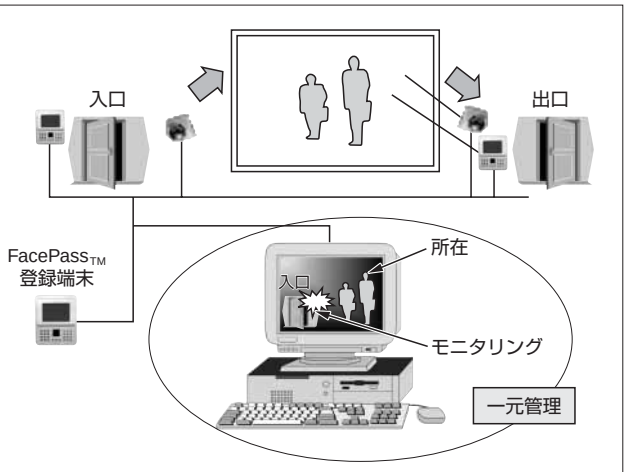

図5．顔照合モニタリングシステム ― 顔照合と監視カメラでモニタリングし，導入が容易で確実な入退室管理を実施する。

Monitoring system using facial recognition and video surveillance

4 あとがき

入退出管理においてセキュリティポリシーが重要であることを述べ，ビル設備としてのセキュリティシステムにおいて，このポリシーを正しく運用するために用いるソリューションを提案した。

まず入退出管理全般について，対象に応じて適切に策定されたセキュリティポリシー，すなわち何から何を守るのかを明確にして設備を構築することが重要である点を主張した。また，ビルのセキュリティシステムにおいては，一般に複数業種・業態の同居する空間(ゾーン)と，自社ビルや専用建築物のような空間とではそのポリシーが異なり，前者については利便性とセキュリティとの両立が求められるが，後者についてはセキュリティを特に重視すべきであることを示した。

それらを受けて，利便性とセキュリティとの両立をポリシーとする運用のために，非接触認証が行える顔照合セキュリティシステム FacePass$_{TM}$の有効性を示した。一方，セキュリティ重視のポリシーに従った運用のために，いわゆる伴連れ防止を実現する扉の設置手法を示した。更に，顔照合と画像監視を組み合わせたモニタリングシステムを用いて，付帯設備が少ない構成で伴連れを抑止する入退出管理を実現できることを示した。

今後は，引き続きセキュリティポリシーの遵守を継続しつつ，当社の特長の一つである顔や人物の認識技術を用いたセキュリティシステムの展開を進めることで，より安全で利便性の高いビル設備の供給を目指す。

藤森　敦　FUJIMORI Atsushi

社会ネットワークインフラ社 システムコンポーネンツ事業部 ターミナル機器営業部主務。セキュリティ及びバイオメトリクスシステムのエンジニアリングに従事。

System Components Div.

菅野　麻衣子　KANNO Maiko

社会ネットワークインフラ社 システムコンポーネンツ事業部 ターミナル機器営業部。セキュリティ及びバイオメトリクスシステムのエンジニアリングに従事。

System Components Div.

立川　寛　TACHIKAWA Kan

社会ネットワークインフラ社 システムコンポーネンツ事業部 ターミナル機器営業部主務。セキュリティ及びバイオメトリクスシステムのエンジニアリングに従事。

System Components Div.