

入退出管理システム

“人の動き”をコントロールするオフィスのセキュリティ対策

人(社員)、財産(金品)、情報、信用——企業が守るべきものは、今も昔も変わらない。しかし近年、社会情勢の著しい変化により、企業のセキュリティソリューションに対するニーズが高まるとともに、その手法も細分化・高度化が進行している。今号では、それらのセキュリティ対策を、主として物理的な側面から捉え、特にテナントビル入居企業にとって必要性が高いと考えられる「入退出管理システム」に関して、(株)日立ビルシステムに取材。具体的導入事例も交えて、その導入メリットを紹介する。

企業を取り巻くリスクの変化

現在、セキュリティ対策は、企業規模の大小や立地環境を問わず、早急に対応すべき課題として重要視されている。いわゆる事務所荒らしといった不法侵入によるリスクは昔から存在するが、なぜ今、セキュリティに対する問題意識が急速に高まってきているのだろうか。その背景には、次のような企業を取り巻く社会情勢の変化が挙げられる。

①内部から発生するトラブル誘因の増加

●雇用環境の変化

社内就業人口における契約・派遣社員等、「会社」に対して帰属意識が比較的低い従業員が増加し、またフレックス勤務の定着・グローバル化する取引先への対応により勤務形態の24時間化が近年急速に加速している。結果、個人々人に対して情報の取扱いを周知・徹底することや、仕事の必要性に応じ

た情報へのアクセスに対して個々に管理することが困難な状況となってきている。

●IT化の進展

顧客情報等、機密情報の電子化が進行した結果、膨大な情報を取り出しやすい環境となった。さらに、すぐに印刷したりコンパクトに社外へ持ち出せるようになり、故意・過失を問わず、内部からの情報漏洩というトラブルを助長しているものと考えられ、近年においては、高度な技術を必要とする情報漏洩よりも、紙媒体やパソコン・記録媒体を経由した情報漏洩の割合が増加している(図表1)。

②外部侵入によるトラブル誘因の増加

数年来多くの企業で実施されてきた、人的コスト・ファシリティコスト削減策の結果、営業拠点等において、人員の少ない小規模オフィスが増加した。特に昼間、在席しているのが女性アシスタントのみといったオフィスも増えており、主に夜間に発生する事務

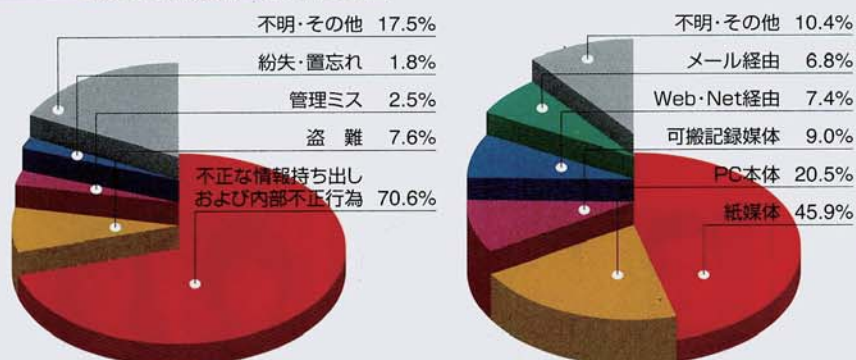
所荒らしに限らず、不特定多数が入館する日中の不法侵入を脅威と感じる企業が増加している(図表2)。

③法による義務化

2005年4月1日から全面施行された「個人情報保護法」により、個人情報取扱事業者(過去6ヵ月で一度でも5千件以上の個人情報を扱った企業:企業活動を行うほとんどの会社が該当)は、個人情報の取扱いについて、利用目的による制限、適正な取得、安全管理措置等を義務付けられることとなった。すなわち、個人(顧客)情報漏洩を防止することは、自らの財産を守るのみならず、コンプライアンス(法令遵守)の面からも必須となったのである。

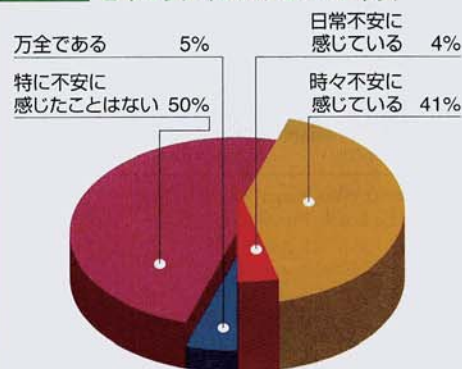
個人情報漏洩事故が起こった場合、企業は、損害賠償や復旧コスト、社会的信用失墜という莫大なダメージを被ることは言うまでもない。個人情報漏洩事件が大きく報道されるようになったことも、信用失墜リスク増大・

図表1 個人情報漏洩の原因別被害者数比率と個人情報漏洩経路の件数割合



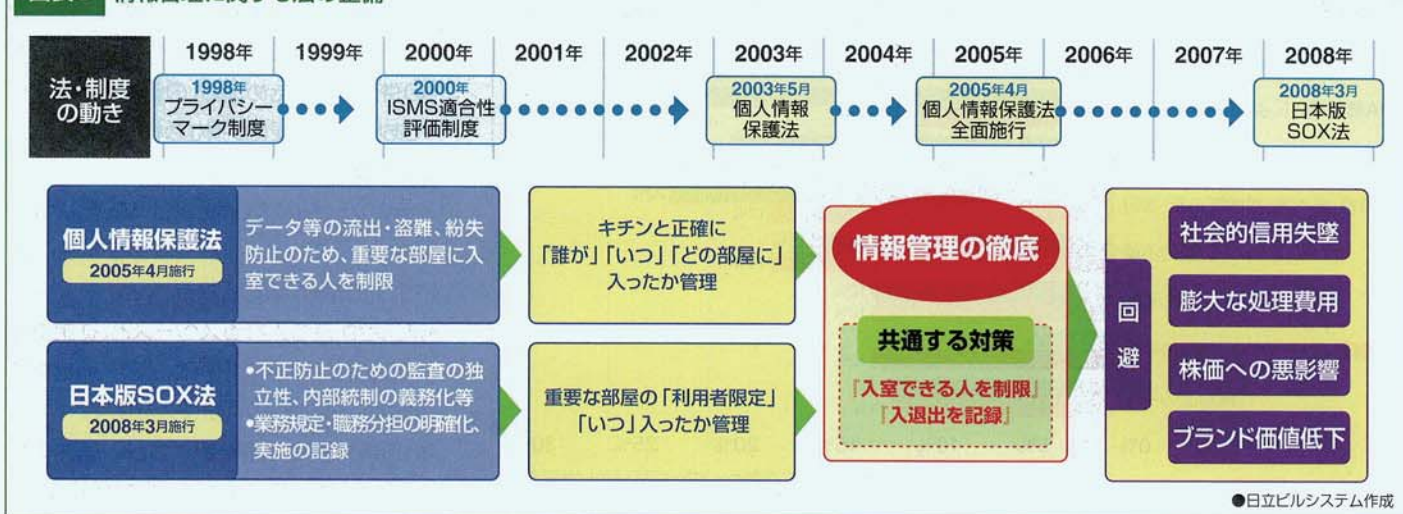
●出典:「2004年度情報セキュリティインシデントに関する調査報告書」NPO日本ネットワークセキュリティ協会

図表2 入居ビルのセキュリティシステムへの不安



●出典:「オフィスセキュリティ意識調査」2004年日立ビルシステム・生駒データサービスシステム共同調査

図表3 情報管理に関する法の整備



企業ブランド価値低下に拍車をかけている。これらの報道を見ると、情報漏洩は、インターネット経由の不正アクセスといった外部からの攻撃によって起こるものよりも、内部の従業員による情報取扱い上の不注意や意図的な持ち出しといった、物理的な「人の動き」に伴う事件が多いことが分かる。こうした事態に備え、企業は、万一の事件発生に際し、速やかな原因究明と立証を行うために、「人の動き」を記録として残す等の一定レベル以上の社内セキュリティ対策を構築することが必要となった。

さらに、2008年3月の施行が検討されている「日本版SOX法」は、上場企業に対し内部統制強化を義務付けており、その一つに情報漏洩対策強化も盛り込まれている。これら上場企業は、取引する中小企業に対しても一層厳格な情報取扱いを要求することとなり、セキュリティ対策が脆弱な企業はシャットアウトされる可能性も出てくる。同時に、社会的信用を高めるうえで必要となるプライバシーマークやISMS認証取得*のために、セキュリティポリシーを策定し実践する企業は、一層増加していくものと予測される(図表3)。

以上のように、情報漏洩対策および個人情報保護法・日本版SOX法等の法的規制の対応に共通して必要となるのは、情報や契約書類等を保管する重要な部屋や執務室に対して、「入れる人を明確にする」「必要な

人だけ入れる」「いつ誰が入ったか記録する」ことを満足するセキュリティ対策である。多くの企業にとって、今後、人の出入りを管理するセキュリティに対する取り組みが、企業のステイタスを表す指標の一つとして重要視されることは間違いないだろう。

*プライバシーマーク:個人情報取扱いに関する認定制度で、審査基準はJIS Q 15001(個人情報保護に関するコンプライアンス・プログラムの要求事項)に準拠し、認定された事業者はPマークの使用許諾を得る。
 *ISMS認証:情報セキュリティマネジメントシステムを構築し、適切に運用していると評価された事業者に対し与えられる、情報セキュリティ認証。

人の動きを制限する物理的セキュリティ対策

このような状況において、テナントビルでは、ビルオーナー、入居企業各々がどのような対策を講じるべきだろうか。複数テナントが入居する一般的なオフィスビルを想定し、

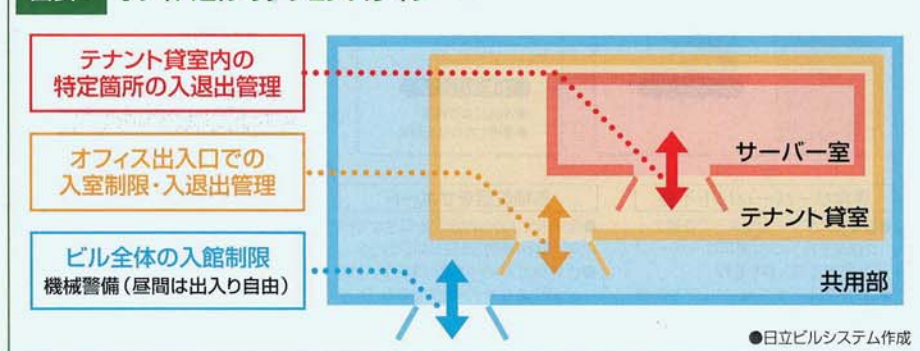
入館・入室制限、入退出管理といった物理的セキュリティ対策について考える(図表4)。

①ビルオーナー

図表5は、(株)生駒データサービスシステムが、テナント企業に対して行った移動動機に関する調査を集計したものである。グラフを見ると、「管理・セキュリティ体制の不備」を移転理由として挙げている企業が、ここ数年で著しく増加していることが分かる。既存ビルのオーナーは、テナントの流出防止策として、次のような対応を実施し、新築ビルとのセキュリティ面の格差を縮小させることが必要となる。

- 機械警備によるビル出入口の入館制限はもちろん、ビル全体のセキュリティを維持するシステムを検討する。また、テナント貸室出入口の入室制限まで、ニーズに応じてオーナー側で用意する。
- テナント側が用意した貸室内セキュリティシステムと併用する場合、携帯性を考慮し

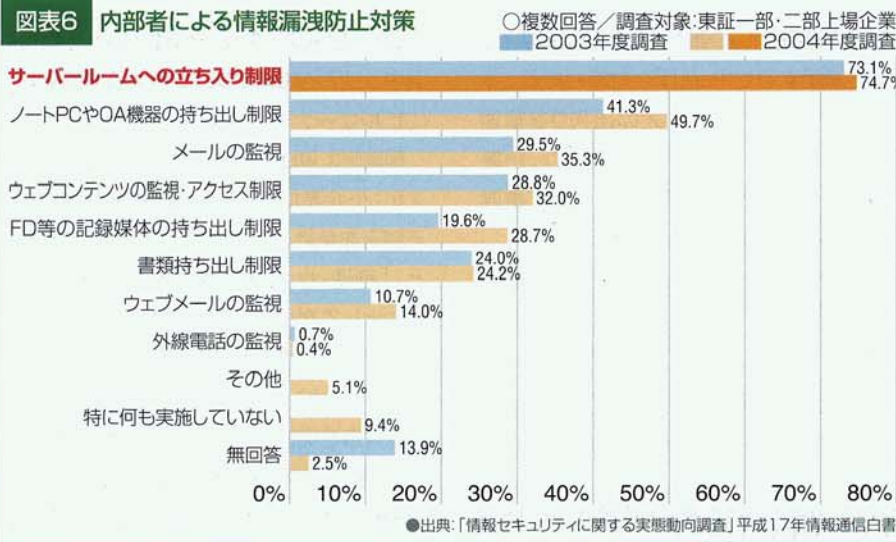
図表4 オフィスビルのデフェンスライン



図表5 テナントの移転動機



図表6 内部者による情報漏洩防止対策



図表7 ネットACSのシステム構成図と特長



て非接触ICカードを利用したシステムを導入することが望ましい。従来のキーボックスシステムの場合、鍵とテナント用カードの併用となるため、個人の管理には不向きであり、かつ利便性が損なわれることがある。

②テナント

テナントビルの入居企業は、前述したような内外からのリスクを低減させるために、次のような対策が求められる。

- 来訪者が立ち入れるスペースと、従業員のみの執務スペースを明確に区分し、営業時間中の外部からの不法侵入を防ぐ。
- 内部情報漏洩や盗難を防ぐため、室内の特定箇所（サーバーールーム、書類保管室、金庫室、更衣室等）に、特定の従業員のみアクセス可能とし、また、アクセス可能な時間帯を従業員個別に設定する。
- 従業員の誰が、いつ、どのエリアに入退出したかを記録し、データとして蓄積する。

これらの対策を実施するには、今までのビルのセキュリティ≒機械警備では不十分である。入室を制限するだけでなく、出入りの履歴を取る物理的セキュリティ対策、すなわち入退出管理システムが必要となる(図表6)。

システム導入時のハードル

従来の入退出管理システムには、テナント企業が導入を考える際、以下のような課題があった。

- イニシャル面では、サーバー設置費用等の高額なシステム導入コストがかかるため、貸室内の1ないし2カ所のみで入退出管理を実施する場合はコストメリットが低下する。また、セキュリティ投資に限界がある小規模企業等では、導入が困難となる。
- ランニング面では、サーバー管理・システム運用業務が発生するが、これら業務のための専門の管理者を置くことは現実的ではない。そのため、特に社員の異動による認証用カードの更新、オフィスレイアウトの変更、セキュリティ機器の障害対応時等に負荷がかかり、担当者の本来の業務を圧迫する場合がある。

●テナントビルであるため、既設ドアの交換といった大掛かりな工事ができない。

現在は、こうした課題を踏まえ、入居ビルの既存設備や、テナント企業の規模にフレキシブルに対応した入退出管理システムが提供されている。その一例として、オフィスに普及したインターネットを利用した、株式会社日立ビルシステムの入退出管理システム「ネットACS」を紹介する。

インターネット型入退出管理システム「ネットACS」

同システムは、「特定の箇所に、安価で、簡単に」をテーマに開発された入退出管理システムである。認証コントローラーを日立カスタマーセンターと電話回線やインターネットを通じて接続することで、管理用のサーバーを個々のユーザー内に設置することを不要とし、導入コストの大幅な低廉化を実現した(図表7)。同時に、日々の運用や認証用IDカードの発行・抹消といった作業も、日立カスタマーセンターからサポートすることで、ランニング面のユーザー負荷軽減を図っている。また、既設ドアに取り付け可能な面付電気錠を採用しているため、テナントビルのドアを交換する必要がないため、導入工事が簡単に済むことも特長の一つとなっている。

認証用の非接触IDカードについては、現在、社員証や多目的機能等を持たせたカードが普及しているため、日立の入退出管理システムでは、ニーズに合わせた多様なシステムのカード選択が可能。さらに、基本システムに「指静脈認証装置」による生体認証を加えた、より高度なセキュリティシステムも提供している。

「ネットACS」を導入している企業は、貸室出入口1ヵ所を対象とする小規模企業から、複数拠点を全国展開する大企業まで幅広い。拠点毎にサーバーを持つ必要がなく、全拠点・全従業員の入退出を本社で一元管理でき、また拠点の増設に低コストで対応可能というメリットから、全国展開型企業での導入実績が多くなっているということである。

社員のセキュリティ意識向上も実現「ネットACS」導入事例



野村リビングサポート株式会社

野村リビングサポート株式会社は、野村不動産グループのマンション管理会社。今年1月に竣工した新宿5丁目の長府新宿ビルに本社を構え、現在、4～7階の4フロアに約200名が勤務している。

同社では、個人情報保護法施行を契機に、顧客の個人情報をいかに適正に取り扱うかについて検討を重ねてきた。そして、顧客の信頼を得るためには、審査の厳しいプライバシーマークの取得が必要であると考え、入退出管理システムの導入を決定した。

「従前のオフィスでも、テンキー入力と記帳による入退出管理を実施しており、共用スペースと執務スペースを完全に遮断してフロアセキュリティを強化していました。しかし、使い勝手や履歴の正確性を考慮し、1月の本社移転を機に、非接触型IDカードを使用するシステムに変更しました」(同社総務部長 駒橋正雄氏)。

現在、同オフィスでは、セキュリティレベルを①来訪者が入室可能な専有部内の共用部、②社員が入室可能な執務スペース、③限定社員のみ入室可能な重要度の高い部屋、の3段階に分け、②

と③のドアに「ネットACS」設備を設置している。

「ネットACS」は、社員全員の認証用カードを総務で一括管理することで、レイアウト変更や人事異動にスムーズに対応できる多様性を持ち、また、



導入コスト・運用コストともに他社システムと比較して低廉であったことが評価された。

同ビルでも、一般のビルと同様に警備会社のシステムが導入されているが、警備会社のシステムは夜間無人の際には有効であるが、昼間のセキュリティには効果を発揮しないということも、「ネットACS」を導入するに至った大きな理由の一つである。通常、ビル側の提供する警備会社のシステムと、テナントが用意するセキュリティシステムが別系統の場合、利便性という面で問題となる場合がある。その点、同ビルの入館・専有部入室用非接触IDカードと「ネットACS」のカードは、一つのケースに入れ重ねた状態で使用可能となっており、使い勝手という点に関しては全くストレスを感じていないということである。

「情報漏洩事故の原因の大部分は人間の「うっかり」にあり、これを完全に防止することは、技術を極めたシステムでも限界があるでしょう。しかし、物理的な管理を実施することによって、社員のメンタルな面で、セキュリティに対する意識が高まっていく。これが、入退出管理システムを導入した大きなメリットであると考えています」(同 駒橋氏)

同社では、2年後のプライバシーマーク更新に備えるため、より効果的なセキュリティ構築を目指していくとしている。