2011年7月版

オフィスのセキュリティ構築

ー自社の最適な守り方ー

ビジネス環境は変化し続けています。日本においても、マーケットやビジネスプロセス、経営層や従業員の組織に対する意識変化など、一つのパターンではくくることのできない多種多様のスタイルが出現しています。

そうなると、当然のことながら事業活動におけるリスクも多様化することになり、そっくりそのまま隣の真似をしてみても、同じようにリスクを取り払うことは困難だといえるでしょう。

当マニュアルでは、各社各様のリスクをどのように軽減または除去していくべきか、学術的ではなく実務的にオフィスにおけるセキュリティに焦点を絞り検討します。もちろん、オフィス以外の研究開発・製造・物流拠点での活動においても、基本的な考え方に大きな違いはありませんので、この中で有益となるものはご活用いただけるのではないかと考えています。

CBRE

CHAPTER.1
オフィスセキュリティの考え方

一口にオフィスセキュリティといっても、一体、どのようなリスクに対して、何を、どのように守るのか……。まず初めに、これまで漠然と捉えられていた、このリスクと守るべき資産をしっかりと把握しておく必要があるでしょう。

■オフィスに起こり得るリスク

まず、オフィスに起こり得るリスクをセキュリティの視点で理解するため、人的リスク、物的リスク、情報リスクの三点から考えてみたいと思います。

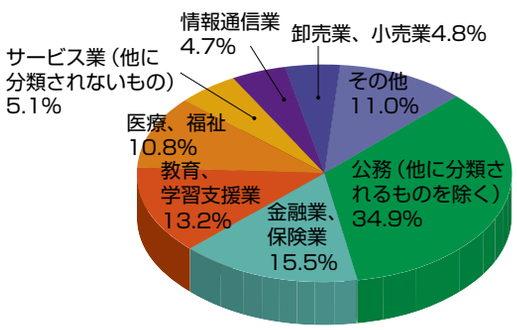
人的リスクとは、経営者を含む従業員の体にかかわる危険ということ。オフィス内の事故や災害による人的被害を別にすれば、ここで真っ先に挙げられるのは、オフィス内に不法に侵入してくる“招かれざる客”による社員への危害・暴行のリスクです。一昔前までは、社外の人間が自由に出入りできるオフィスというのは、珍しくありませんでした。隣の席の同僚が、自席で自分の全く知らない人と打ち合わせをしている。そんな風景も見受けられたものです。ただ、これでは、人的リスクに対して無防備であることはいうまでもありません。昨今、オフィスへの入室は、非接触カードリーダーといった最新のセキュリティシステムによってガードされることが一般化してきており、中には生体認証を取り入れる企業も出てきました。しかし、これを過信することが、かえってオフィスにおける人的リスクを増加させてしまう面もあるのです。不法侵入者に一度オフィスに入られてしまうと、正社員に加え契約社員、アルバイトまたパートナー企業からの一定期間の常駐者などさまざまな就業者が存在している現在のオフィスでは、その特定はこれまでより困難なものになります。またネット社会に象徴されるように、メールやWEBがビジネスツールの中心で他の社員の顔を知る必要がない業種では、侵入者はまさしく自由です。このような状態では経営者や従業員を守れているとはいい難いでしょう。立哨がいながら、気付いたら残業時間中にすぐそばまで部外者が入り込んでいた、トイレ等に侵入されたという事例も起こっています。これらに対抗するために、建物のエントランスにフラッパーゲート（入退室管理システム）を設置したり、オフィスへの入室だけでなく退出も管理するということが行われているわけですが、アポイントの確認も満足にせずゲートを通してしまい、全く設置の意味をなさないようなところも見受けられます。

次に物的リスクですが、たとえば施設に対しては、内部からも外部からも被害を受ける可能性があります。内部的には建物やオフィスの破壊、ネットワーク等の破断、金品・貴重品・美術品の盗難など、外部的には建物外周部やインフラ導入部の破壊、社有車へのいたずらなどが挙げられます。内部被害については前出の不法侵入者によるものと、従業員以外でオフィスに入る作業関係者の突発的な犯行、残念ながら会社に対して悪

意を持つ従業員などによるものがあります。外部被害は計画的な犯行だけでなく、予知不能な通りすがりによるものもあるでしょう。一九七〇年代のオフィスビルや九〇年代にいくつか発生した爆破テロ等では、物的被害以上に大きな人的被害をもたらしました。

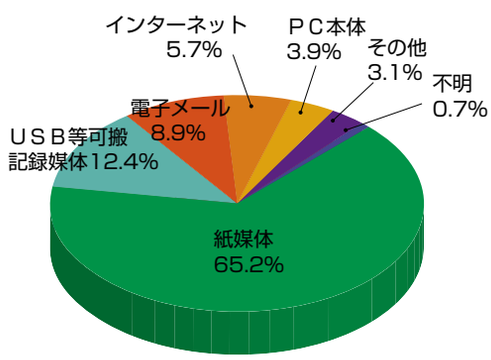
情報リスクは、漏洩（盗難）とデータそのものの破壊が挙げられ、ご存知の通り企業価値そのものにもダイレクトに影響を及ぼします。NPO日本ネットワークセキュリティ協会が発表した「情報セキュリティインシデントに関する調査報告書」によると二〇〇九年の業種別の個人情報漏洩件数は「金融業・保険業」がトップで、次いで「公務」、「教育、学習支援業」で全体の約七〇%でした。二〇一〇年上半期のデータでも、この三業種で約六四%を占めています（図❶）。漏洩媒体・経路としては、紙ベースが圧倒的に多く、次いでUSB等可搬記憶媒体、電子メールという順になっています（図❷）。各企業でペーパーレス化、ペーパーストックレス化をはじめ、認証や監視のシステム、シンクライアント等の導入が進んでいるにもかかわらず、こうした実態となっているのはなぜでしょうか。原因として挙げられているのは、「管理ミス」「誤操作」「紛失・置き忘れ」で八割以上に上ります。移転時の書類紛失や手違いでの流出、重要書類やデータ媒体、PCを外部に置き忘れたことによる情報漏洩、郵便物の誤送やメールの誤送信等々。また、統計データには反映されていませんが、オフィス外やエレベーター内での社員同士の立ち話から機密情報が漏れてしまうといったケースも考えられます。「盗難」や「不正な情報持ち出し」は、さほど高い割合ではありませんが、情報は人が扱う以上、どのような形態であれ悪意があれば可能であると認識しておく必要があります。

1 2010年上半期 業種別の個人情報漏洩件数



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

2 2010年上半期の漏洩媒体・経路別の漏洩件数



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

オフィスのセキュリティ構築

ー自社の最適な守り方ー

シービーアールイー

■企業にとって守るべき経営資産とは

セキュリティを計画する上では、守るべき資産を特定する必要があります。当然のことですが、これが特定されていないと、適切なセキュリティレベルが維持されているかどうかの判断はできません。一般的には次のようなものが挙げられます。

- **人（経営者、従業員、来訪者）**
- **情報（顧客情報、従業員情報、技術・経営・財務・営業等の企業情報）**
- **施設（生産拠点、物流拠点、オフィス、インフラ、各種設置物）**
- **モノ（所有機器、金品・貴重品・美術品、社有車）**
- **価値（企業価値・競争力、社会的信用）**

これらに各社特有のものを加えたものが、自社の守るべき資産となります。サービス業等では、不特定多数の来客、テナントビルオーナー等は、入居されている各テナント等も加わるでしょう。人口に対して犯罪被害者数の割合が少ないといわれる日本ですが、具体的に守るべき資産を特定していくと、意外と危険にさらされているものがあることに気が付くと思います。しかも、これらは恒久的なものではなく時間とともに変化しますから、事あるごとに見直しをすべきだといえるでしょう。資産を特定できたら、できるだけリスクの発生確率と影響度を定量化して対応方針を決定します。

オフィスのセキュリティ構築

ー自社の最適な守り方ー

シービーアールイー

■企業のオフィスセキュリティへの取り組み状況

オフィスセキュリティで一般的に想定されるのは「入退出管理」、「情報へのアクセス・取り扱い制限」、「書類やPCの持ち出し制限」ですが、これらの施策はそれぞれ独立して行われていることが多いようです。その理由の一つが、とにかく物理的にオフィスや情報へのアクセスを制限すればOKという単純なアプローチにあります。

たとえば入退出管理では、「マシンルームの出入り口に生体認証システムを設置し、入室も退室も万全に管理している」として、システム担当者も施設担当者もこれで安心というところも少なくありません。しかし、もう少し俯瞰的に見てみると、マシンルーム付近へのアクセスが容易だったり、逆に人がめったに来ないような場所でありながら壁などは簡易な構造体で構成されていることがあります。また、保守作業時などに外部パートナーが頻繁に出入りするという理由で、扉を開けっ放しにされているケースも見受けられます。PC等についても、金融機関のように持ち出しをさせないようバッグなどの私物は一切オフィス内に持ち込み禁止という職務に合わせた対応をしているところがある一方、持ち出し禁止にもかかわらずノート型PCを盗難防止策もせず採用し、退社時にはデスク上に放置というあえて盗難を誘発するような運用をされているところもあります。これらは、個別の対応や物理的な面だけを考え、全体的な対応や運用面を考えていないオフィスでは多かれ少なかれ見られる例です。弊社がかかわる多くの企業・団体の中でも、総合的に考えられた安全かつ投資効果の高いセキュリティ施策をとっているところは、まだまだ少ないと認識しています。

Point

▼オフィスには人的リスク、物的リスク、情報リスクがある

▼まずは自社の守るべき資産を特定、把握する

▼全体的かつ運用まで含めたオフィス計画が作られているところは少ない

CBRE

CHAPTER.2
自社にマッチしたオフィスセキュリティ構築のフロー

オフィスセキュリティの重要性を意識しない企業は少ないと思いますが、問題は、いかに合理的かつ効果的に構築していくかです。自社にもっとも適したセキュリティを作り上げる際の基本的な手順を見ていくことにしましょう。

■短絡的、個別の打ち手は無駄

では、どのように各社各様のニーズにあったセキュリティを構築していけばよいのでしょうか。当然のことながら、できるだけ早く効率的に実施できればベターなのですが、前述の通り個別にやってしまえということでは百害あって一利なし。たとえば、経営トップから「知らない人間がオフィス内にいるのを見掛けた。出入り口を制限して立哨を立てるように」と指示されたとしても、たとえばISO27001認証機関から「関係者以外、情報にアクセスできないようしっかり制限してください」と指導されたとしても、短絡的に機器を設置したり鍵をつけるのではなく、これらの指示やアドバイスをクリアしつつ、使い勝手を損なわないような策を取る必要があります。従業員の生産性を阻害するような安易な施策は、結局、やり直しをすることになります。

こんな例があります。雇用形態が多様化した従業員の識別と社員同士のコミュニケーション活性化をねらい、人事部門が主導で社員章を作成することにした某企業。導入に向けいろいろと検討していくうちに食堂などの経費精算や勤怠管理も一枚でということになり、専門ベンダーでICカードを作成、顔写真も入れ、地方拠点にまでこのICカードが配布されました。ところが、人事部門の知らないところで管理部門がICカードを利用したセキュリティ構築を検討しており、加えて、これがタイプの異なるICカードであったため相互利用ができず、結局配布済みカードは回収、新たなカードを作成し再配布することとなりました。コストだけでなく、人事部門の作業負荷、配布回収に伴う従業員の手間暇まで考えると相当の無駄が発生したといえるでしょう。これに輪をかけて、経営企画部門等でセキュリティ方式の固定化されたテナントビルへの移転などを検討していたなどとなったら、それこそ一からやり直しとなってしまうのです。しかしこの企業の場合、すべてを終える前に気付いただけよかったのかもしれません。なぜなら、このまま進めていたら「ここはこのカード」「あそこはこのカード」となって、従業員の利便性は格段に落ちることになったでしょう。

■俯瞰的な検討を

新たなオフィスセキュリティ構築に向け検討を始めるにあたっては、まず、所管部門が経営陣を含めた社内関係者に確認をとることが前提となります。ただし、セキュリティ構築という業務の性格上、一部のメンバーで秘密裏に進めるということも多く、その場合はやはり経営トップのかかわりと認識が重要となるでしょう。

また、検討のベースとなる条件はまちまちであり、オフィスが所有施設なのか賃貸なのか、都心か郊外か、高層か低層か、大規模か小規模か、来訪者が多いのか少ないのか、正社員が多いのか非正社員が多いのか、定型業務かプロジェクト型業務か等々、これだけでも相当数の組み合わせになります（図❸）。それに加え、生産性を阻害しない具体策と、ステークホルダーへの投資に対する説明責任まで考えたら、一足飛びに実施できないという理由がおわかりいただけると思います。当然のことながら、運用段階になってからボロボロとセキュリティホールが見つかったのでは取り返しがつきません。今回の計画停電などのように、電気が途絶えたら完全フリーとなってしまうようではまずいですし、脆弱となる部分のカバーができるかという視点も重要となります。

自社の置かれている状況をきちんと把握し、関係者全員が想像力を働かせ全方位的な捉え方で検討を進めていくこと。これにあたっては、セキュリティ機器ベンダーや設備設計者など、専門家のアドバイスが参考になるでしょう。ただし、これらは特定分野に限定されますから、全体感は自社のことをいちばんよく理解している社内メンバーが責任を持って進めていくべきです。もちろん、特定分野に限定されずにサポートできる、セキュリティコンサルを利用するというのも有効な手段です。

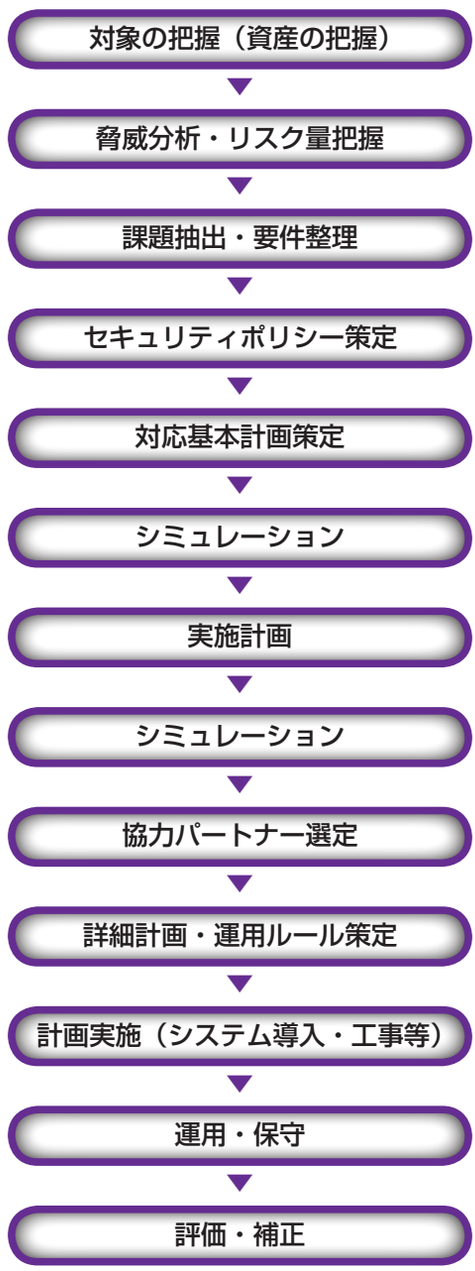
3 セキュリティ検討のベースとなる条件

■オフィスにおけるセキュリティ構築のフロー

セキュリティ構築のためのフローは前出のような条件によってさまざまですが、私どもシービー・リチャードエリスにおける基本的な考え方を一例としてご紹介します（図❹）。おおよそ図❹のような流れですが、新築テナントビルなどに移転をする場合などは建築工程や入居時期などの時間的制約を加味し、各プロセスに強弱をつけたり簡略化したりすることになります。また、企業や事業所の規模によっては、問題ないところは簡略化しシンプルかつスピーディーに進められると考えます。

オフィスセキュリティ構築は自社の置かれている状況や条件によると前述しましたが、中でも自社施設か、賃借施設かという点は大きく影響する要素です。具体的に問題になるのは、ビルオーナーや管理会社とテナントとのセキュリティに関する考え方の温度差です。ビル側がよかれと思って導入しているセキュリティシステムが、逆にテナント特有の対応へのネックとなることがよく見受けられます。逆にビル側の認識レベルが低く、陳腐化したシステムで万全と考え、テナント工事に制限をかけるといったケースも見受けられます。また、いつ退去するかわからない普通借家契約でのテナントビル入居では、セキュリティシステムにどこまで投資すべきかという判断基準が自社施設の場合よりも難しくなるでしょう。

4 オフィスにおけるセキュリティ構築のフロー



Point

▼短絡的なシステムや機器の導入は無駄である
▼個別対応ではなく俯瞰的かつ想像力を働かせて計画を立てる
▼基本的なフローをベースに条件を加味して構築していく

CHAPTER.3
オフィスセキュリティ構築の具体策

セキュリティの考え方も構築のフローも理解した、そうなると次なるステップは、いよいよその具体的な構築手法です。シービー・リチャードエリスが考えるセキュリティ構築のフレームで各項目別のアプローチのポイントを解説します。

■どこまでやるか

オフィスセキュリティ構築のフローは理解したとして、計画段階で、いきなりセキュリティシステム機器のベンダーや設備設計者といった社外パートナーに依頼してしまうといったケースを多々目にします。緊急な対応が必要な場合、早目に専門家のアドバイスを取り入れることは決して間違いではありません。ただし、そうなると、どうしても物理的なシステムや機器の導入、警備方法などディテールの計画に傾注していってしまいます。その弊害は、第二章でご説明した通り「短絡的、個別の打ち手は無駄」につながりやすいということ。トライ&エラーを繰り返し、より良い形へとブラッシュアップしていけばいいという余裕のある企業はいいかもしれませんが、現実的な取り組みとはいえません。お金と時間、人的リソースは無尽蔵にあるわけではないですから、最初にいかに汗をかいて的確なプランを立ち上げられるかが鍵となります。オフィスセキュリティ構築の陣頭指揮をとられる方（一般的には総務部門や社内プロジェクトのリーダー）が、どんなことを、いつ頃までに、どのようにやっていくかをプランニングするわけですが、その際、検討のフレームがあると具体的に考えやすいと思います。どのようにアプローチしていくかのガイドラインといってもいいかもしれません。

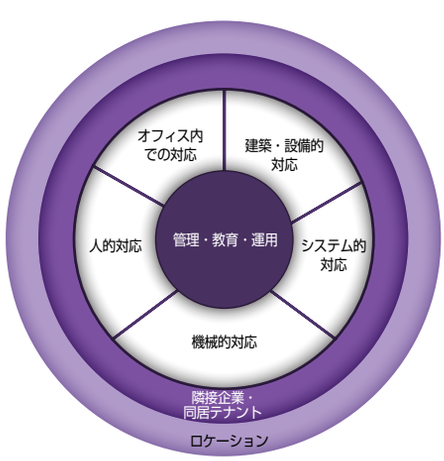
■具体的なアプローチの仕方

専門とする領域によってアプローチの仕方に差はあると思いますが、ファシリティに関するサービスプロバイダーであるシービー・リチャードエリスのアプローチは次の通りです。

①ロケーション ②隣接企業・同居テナント ③建築・設備的対応 ④システム的対応 ⑤機械的対応 ⑥人的対応 ⑦オフィス内での対応 ⑧管理・教育・運用

このアプローチは、人的リスク、物的リスク、情報リスクのすべてにかかわるものであると認識しており、多少の前後はあるものの基本的には大枠からディテールへと並んでいます。この順序で検討していくことにより、手戻りや過剰な投資を抑えることができると考えています（図❺）。

5 具体的アプローチのイメージ



オフィスのセキュリティ構築

ー自社の最適な守り方ー

シービーアールイー

1 ロケーション

現在のオフィスで構築するのか、移転を機に構築するのかにかかわらず、オフィスセキュリティには地域性やロケーションを考える必要があります。都心部と郊外部で違うのはもちろん、たとえば同じ東京都心部でも、丸の内エリアと渋谷エリアでは街としての特性や周辺施設も大きく異なっています。各企業は事業戦略に併せて拠点立地を検討するわけですが、セキュリティもその特性に併せて、個別に構築する必要があるでしょう。

このとき注意したいのが、日中と夜間の地域イメージの変化。昼間は整然としているにもかかわらず、実は盛り場への通り道となっていて夜は酔った人がごったがえしているとか、昼間は周辺住民でにぎわっているものの、夜は閑散としていて暗い道を女性社員が帰らなければならないエリアであるなど、時間による差は案外気が付きにくい点です。その他、東京の本社が主導でセキュリティ構築を推進する場合、各都市のビル管理に対する慣習の差を認識しておく必要もあります。東京のオフィスビルでは、土日祭日は正面玄関が閉鎖され、従業員しかビル内に入れないのが一般的ですが、たとえば観光都市の大通り沿いのビルなどでは、かなりの確率で休日であっても正面玄関はオープンになっています。このような点を考慮せずにセキュリティ体制を構築してしまっては、的確さを欠くのは明らかです。

また、主題とは少し外れますが、BCP（Business Continuity Plan ／事業継続計画）という観点で、液状化や水害が予測されるのかといったことも確認が必要です。行政発行の災害マップなどで確認をすることができますので対策に含めるといいでしょう。

2 隣接企業・同居テナント

自社施設や一棟借りの賃貸施設では隣接する企業や周辺の商業店舗、賃借オフィスビルのフロアや区画借りでは他の入居企業・団体など、近隣や同居する相手がどういった業種なのか、どういった施設を所有・運営しているのかということを知っておいた方がベターでしょう。反社会的勢力といったわかりやすいケースの場合は、当然、会社として適切な判断がされると思いますが、たとえば二四時間営業をする店舗の夜間の状況や、二四時間業務を行うテナントと同居するような場合は、建物の入退館にどのような影響が出るか知っておかなければなりません。

テナントビルの場合、特殊な機器や薬品などを使用する施設となっていれば、それが適切に扱われているのか、管理会社などを通して確認すべきでしょう。ひっきりなしに物流業者が出入りしたり、不特定多数の方を対象にしたセミナーが頻繁に実施されるという場合も、エントランスやエレベーター、廊下やトイレなど共用部への影響を考える必要があります。

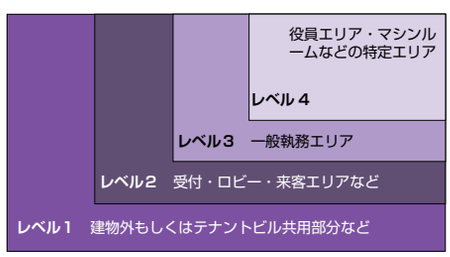
3 建築・設備的対応

建築面で挙げられるポイントは、まずスタッキング（複数階の場合の何階にどの機能、どの部門が入るかといった垂直上のゾーニング計画）やレイアウトプランに関してです（図❻）。

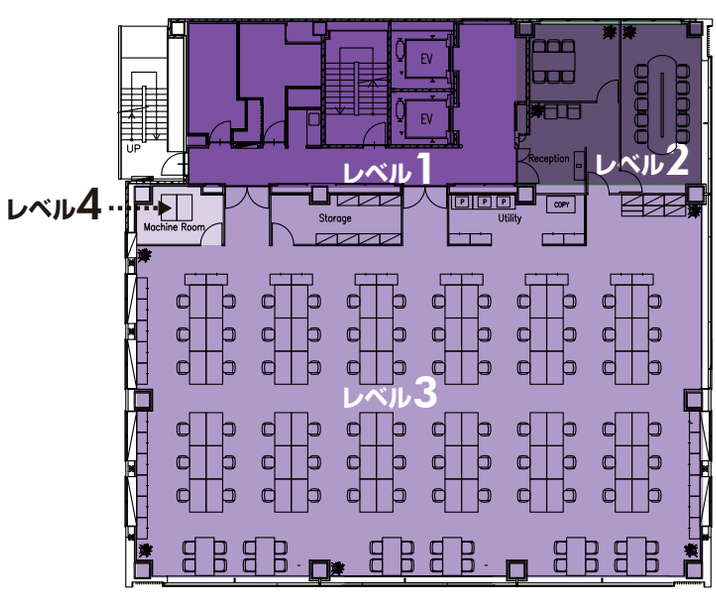
来客エリアをワンフロアに集中させ、一般の執務エリアへの侵入を制限するといった手法はよく活用されますが、役員フロアは災害時に避難しやすいよう低層階に、逆に、外部の侵入者から守るために高層階に設置といった考え方もあります。その他、安全でわかりやすいオフィス内動線計画、避難経路、外部からの侵入を防ぐ建物設計や死角の少ないオフィスレイアウト、トイレ内天井への点検口の有無（入り待ち防止のチェック）、ガラスによる個室やエレベーター内の可視化なども建築的な工夫となります。業種によっては、特定部署へのファイヤーウォール（チャイニーズウォール）としての隔壁設置などもこれに含まれるでしょう。

設備的には、照明の適切な配置や自動点灯などによる暗がりの防止、空調設備や給水設備への容易なアクセスの防止（有害物質混入などの抑止）、電源やネットワーク設備への施錠や電磁波対策などが挙げられます。

6 セキュリティゾーニング例



※レベルの分け方は、それぞれで異なります



4 システム的対応

主に各種認証サーバーやファイヤーウォールの仕組みなどです。これらはシステムインテグレーターやITコンサルタントにより計画されるものですから詳細は割愛いたしますが、その計画を実行するためには、建築・設備工事、機械警備との連動が必要です。関係者間でよく協議していくことが必須となります。

5 機械的対応

文字通り、機械設備の設置によって警備を行うものであり、入退出管理（建物エントランス、オフィス、マシンルーム・金庫室などの重要施設など）、監視カメラ（建物エントランス、オフィス内、マシンルーム・金庫室等重要施設、通路、エレベーター内など）、各種センサー（オフィス内、共用部、窓面など）などが挙げられます。

ご承知の通り、入退出管理などは、細かく設定すればするほど従業員や来客対応の利便性が損なわれる側面もあり、たとえば、トイレに行くだけでも三回、四回とカードを読ませ扉を開けなくてはならないといったケースも見受けられます。バランスは各社・各部門でさまざまですが、必要なものだけを適切に設置するというのが基本スタンスとなるでしょう。業態的に来客が多い企業では、一般的に建物エントランスでのフラッパーゲートによる入館規制は敬遠される傾向にあります。その場合、各階までは誰でも上がれるようにした上で、来客ゾーンと執務ゾーンの切り分けで対応することになるでしょう。また、誘導用途となっている建物に入居する場合などは、「人のにぎわいを創出する」と「不特定多数のアクセスを避ける」という、相反する要素が出てきますので、その両面を融合させるオフィス作りを実現させなければなりません。そのためにも、③の建築・設備的対応で軽減させる、適正化させるという視点が大事なのですが、場合によっては逆に意外なところに付加すべき点が出てくることもあるので注意が必要です。機械警備は、種別によって警備会社によるものと設備メーカーによるものとがありますので、適切な情報収集が大切です。

なお、多くの方がご経験されていると思いますが、入退出管理の導入・運用の際、従業員以外の一時的な就業者、来訪者、清掃や警備業者、郵便や宅急便など、オフィスに出入りするさまざまな方たちを、いかにリスクなく混乱なく整理していくかという課題は必ず出てきますので、妥協することなく議論していただきたいと思います。

6 人的対応

いわゆる警備会社による常駐、立哨や巡回です。監視室があったり出入り口に立哨がいることは、犯罪を未然に防ぐ一定の抑止効果があります。また、従業員が常時見ていることのできない部分を巡回でカバーすることも可能です。ただし、建築・設備の対応、そして機械的対応を考慮した上で、それらをカバーするという視点で計画をしないと、人件費が膨大になる可能性もありますので注意してください。警備会社を選定する際には、スクリーニングやその予定者の経歴を確認できればなお良いでしょう。テナントビルの場合は、ビル側の警備と兼ねてオフィス内の依頼をすることも有効な方法です。

7 オフィス内での対応

オフィス内でのアクセスコントロールという面では、⑤のICカード利用の入退出管理と連動させた仕組みがあります。ICカードを読ませ入室した人でないと自席のPCにもアクセスできず、複合機などのプリントもできないというようなものです。その他、プリンタメーカー各社で提供しているカードリーダーのプリント制御の仕組みは、セキュリティ面以外にも部署単位、チーム単位で使用している共用プリンターでの書類混入防止に有効ですし、そもそも余計なプリントアウトをしないということは適切な書類廃棄方法に加えて情報流出などの低減につながります。また、整然と書類を保管・利用することは流出防止につながりますし、意図的な持ち出しの抑止にも効果があると思われます。

ノートPCを利用している場合はワイヤーロックをつけたり、帰宅時には施錠できる場所に保管するなどの運用で盗難を抑止することができます。オフィス内の施策については、オフィス家具メーカーなどでも有効な情報を提供していますので、そうしたものを参考とするのも良いと思います。また、残業者に対する安全性確保や、これはDRP（Disaster Recovery Program ／災害復旧計画）につながる話ですが、災害時要援護者（視力や歩行に障害のある方、外国人など）への適切な席の確保や有事の際の案内なども、事前に検討しておくべきでしょう。

8 管理・教育・運用

これまで、主にハード面やセキュリティ施策について解説してきましたが、これを導入・実行していくだけで万全というわけでは決してありません。どんな有効な策を整えたところで、正しく管理・運用されなければセキュリティホールは生まれてきますし、扱う人が目的や効果を正しく認識していなければ、単なる面倒な仕組みとなってしまいます。

詳しくは第四章で触れますが、定期的なモニタリング・教育を、ぜひ実施していっていただきたいと思います。また、退職者やレイアウト変更への対応など、計画・導入時点とは条件が常に変化していきますので、手抜かりなく対応案を講じることが必要です。

オフィスセキュリティの運用において特に気を付けたいのは、来訪者に対してのホスピタリティです。非常に多いのが、セキュリティを強くしたばかりに受付がいつも込み合ってしまっているという例です。込み合っていてもきちんとした待ち受けスペースが確保されていればいいのですが、椅子もないロビーで来訪者が所在なく立って待っている光景をよく目にします。さらに、皆が待っているところに受付担当が企業名を大きな声で呼び掛けたりすることもあり、これでは来訪者同士が困惑してしまうこともあるでしょう。最近、一部の企業では、待ち受けスペースのない受付階には多数の受付担当を配置し来訪者に素早く対応し、その後、エレベーターで待ち受けスペースや打ち合わせブースのある来客フロアに案内するといった二段階受付を実施しているところもあります。二回目の受付では個人名で呼び掛けるといった配慮がなされており、ビジネスマナーや個人情報を守るといった点でも、また、ホスピタリティの面でも非常に気持ちが良いものです。

Point

▼構築へのアプローチは視野を広く
▼適切な順序での検討は過剰な投資を抑えることができる
▼正しく管理・運用していくために定期的なモニタリングと教育を
▼会社内だけではなく外部の方へのホスピタリティも忘れずに

CHAPTER.4
継続していくための体制作り・教育

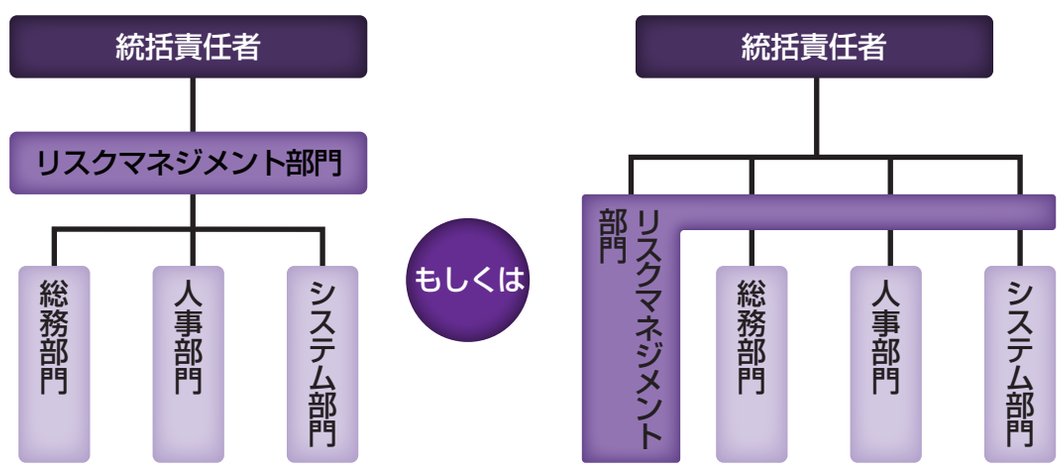
オフィスセキュリティは、ハードや仕組みさえ出来上がればそれで終わりというものではありません。肝心なのは、それを行う会社や従業員のスタンスや気持ちです。最後に、この肝心なところをお伝えします。

■会社側の施策

オフィスセキュリティの仕組みが出来上がったら、それを継続、チェックしていくための体制や教育が必要です。管理体制を作り、従業員にわかりやすい社内規則と定常的に意識できる仕組み、ミスを防ぐ教育・訓練が必要不可欠。加えて、不正行為をしづらい環境作りと適切な監査も同時に行っていかなければなりませんし、場合によっては、ペナルティを課すというルール作りをしなければならないケースも出てくるでしょう。

欧米ではCRE（コーポレートリアルエステート／企業不動産）という、不動産戦略の全体最適を目指す組織を持つ企業が多いのですが、日本では地域ごとだったり、不動産部門、総務部門、財務部門とバラバラの組織で不動産利用が行われており、部分最適の域を脱していないところがまだまだ多いと認識しています。私どもでは、オフィスセキュリティについても同様だと考えています。セキュリティを全体統括する組織（図❼）があれば、それぞれの施策の間での漏れや重複がなくなり、過剰な投資を抑え、生産性も阻害しない、組織や事業の変化にも経営に直結した情報で素早く適切に変更対応できるなど、全体最適目線での構築が可能となるでしょう。管掌範囲は少しずつ異なるようですが、金融機関や総合商社以外の業種でもリスク統括といった組織を持つ企業が増えてきていますので、事業活動を停滞させない活動に期待したいところです。

7 セキュリティを全体統括する組織の例



■従業員の取り組み

会社側の施策を生かすも殺すも、それを利用する従業員次第です。「自分くらいはいいだろう」、「自分には関係ないだろう」といった考えはもはや通用しません。意図的に何かをするということは論外ですが、自分で気が付かないうちにリスクを引き起こしている、またはリスクにさらされているという現実、経済社会におけるさまざまな活動はリスクと表裏一体であるという認識をすることが大切ではないでしょうか。もちろん四六時中「これはリスクか?」と考えているわけにはいきませんし、ビジネスを拡大させるためにはリスクを負って飛び込んでいく必要もあるでしょう。ただ、きちんとリスクを認識しておくこと、そのような場面に出くわしたとき、これは危ないぞと回避策を考えるというような感覚を育てることも大切だと思います。こうした社内啓蒙的なことについてのコンサルティングサービスも存在しており、相談されてみるのも一案です。日常的には、リスクと安全に対する認識を高めるための声掛けや、セキュリティに対する情報共有をはかり、より良い仕組みを作っていくためのリスクコミュニケーションがますます必要になっていくでしょう。

■発生時の対応とDRP、BCP、EHS&Sとの関連性

きちんとプロセスを踏んだ計画を着実に実行していけば、より適切な高いレベルでのセキュリティが期待できるわけですが、オフィスにおけるリスクは多種多様であり、現実には完全に払拭することはできません。そうだとすれば、事故や間違いは起きるという前提で、そのときの対応を準備しておくことも重要です。

リスクマネジメントの概念・定義は人により若干差があるようですが、基本的には「回避」、「転嫁（移転）」、「軽減（低減）」、「受容（保有）」という概念になります。たとえば、物的被害であれば交換・修繕等でそれなりの費用がかかってきますし、一人当たり一万円～四万円程度といわれる情報漏洩による損害賠償も、場合によっては一人当たり一〇〇万円超にも及ぶケースもあるようです。これについては保険等での転嫁の準備が必要でしょう。

また第二章で述べたように、リスクの影響度により回避だけでなく軽減策も考慮しておく必要がありますし、リスクをそのまま受け入れることもあるでしょう。コンティンジェンシープラン（不測の事態への想定・対応計画）を立てるためには、どのようなことが起き得るかを関係者全員が想像力を働かせて出し尽くすことが大事ではないかと考えます。これは、大局的に捉えればDRPやBCPにつながるものです。本稿ではその内容については触れませんが、この三月の震災ではDRPがないことが従業員の安否確認や拠点・資産の被害状況確認を進められない原因となった事例も多いようです。BCPはあるものの、想定以上の影響の大きさに見直しを余儀なくされたというところもあったようです。今後はあらゆる分野で、英知を結集し有事に備える計画がなされるものと期待します。

また、ファシリティマネジメントにおける概念で、EHS&Sというものがあります。Environment、Health、Safety、Security の略で、FM推進連絡協議会の文献によれば、環境・健康・安全・セキュリティに関する基本方針と、そのマネジメントシステムを表します。企業や団体の活動において、顕在化するリスクを排除し、ステークホルダーに対する健康・安全の尊重、地球資源の持続的利用（サスティナビリティ）、法令遵守、環境保全などに努める、米国を中心として広まっているリスクマネジメントシステムの手法です。セキュリティだけでなく、事業活動におけるリスクマネジメントを考え始める際のガイドラインとして活用いただけるのではないかと思います。

■最後に

弊社で携わるさまざまなファシリティ戦略やプロジェクトにおけるリアルな経験を基に、オフィスにおけるセキュリティについてお伝えしてきましたが、何度も申し上げる通り、自社のリスクは自社の方々が本来もっともよく知っているはずで、知らなくてはならないと思います。そして、その対策を講じるための動きに着手するのも、やはり自社にほかならないでしょう。企業によって守るべき経営資源は異なり、対策も当然のことながら違ってきます。そんな中、一から十まで専門家に丸投げということではなく、自社でなくてはできないところ、自らやらなくてはいけないところと、外部のリソースを使うべきところとをしっかりと見極め、オフィスのセキュリティ構築をされることをおすすめします。

Point

▼セキュリティに関する統括組織は効果的
▼従業員のリスクに対する認識向上も重要
▼リスク発生時の対応もきちんと計画しておく

●執筆
シービーアールイー・ジャパン株式会社
プロジェクトマネジメント部 ディレクター　田村 貴之
E-mail:takayuki.tamura@cbre.co.jp

お問い合わせ先
シービーアールイー株式会社　東京本社
TEL:03-5470-8769　FAX:03-5470-8745　E-mail: info@officite.jp