

FACILITY SCIENCES

連載第 7 回
セキュリティの科学

ファシリティマネジャーのための科学的基礎知識
ファシリティ・サイエンス

業務をストップさせないためには 総合的なセキュリティ対策が大切

ハッキングや窃盗だけでなく、地震、火災など、オフィスはあらゆる危険性に晒されています。このような数多くのリスクに対して、予防のための計画を立案し、実行していくのもファシリティマネジャーの重要な役割の一つでしょう。リスク管理は、個々の対策だけを行えば効果をあげられるものではありません。そこにはトータル・セキュリティ・ソリューションという発想が必要になります。今回は、世界で唯一、国際的なセキュリティ規格である BS7799 を取得した建設会社である大成建設において、多くのオフィスビルや事業用施設の設計に携わってきた専門家に、ファシリティマネジャーが考えるべきセキュリティの知識についてお話を伺いました。



大成建設株式会社
設計本部 理事
副本部長

荒井和弘氏



大成建設株式会社
設計本部
設備グループ
グループリーダー

山森 桂氏



大成建設株式会社
設計本部
企画推進部
チーフ・アーキテクト

山木 茂氏



大成建設株式会社
1 施設計画室長
技術士(電気・電子部門)

荒幡芳雄氏

「ファシリティ・サイエンス」下記バックナンバーは <http://www.websanko.com> にアクセスください。

02年 11月号 第6回 消防用設備(スプリンクラー)の科学
02年 9月号 第5回 エレベーター(昇降機)の科学
02年 7月号 第4回 リスクマネジメント(地震対策)の科学

02年 5月号 第3回 水(トイレ)の科学
02年 3月号 第2回 温感(空調)の科学
02年 1月号 第1回 あかり(照明)の科学

いくら堅牢な「錠前」をつけても
火事にあっつしまえば意味はない

.....オフィスにおける「セキュリティ」とは、簡単に言えばどういうことになるのでしょうか?

山森 セキュリティというと、ついつい、ネットワークにおけるハッカー対策だとか、オフィスに入退室管理といった「各論」ばかりに話が先行がちです。しかし、オフィスにおける安全性を確保するためには、対症療法だけでは不十分なのです。もっと総合的にリスクの排除を行わなければなりません。このような考えから、私たちは「トータル・セキュリティ・ソリューション」という名称で、企業に対するセキュリティのコンサルタントから設計、工事(建築、設備)管理まで幅広いサービスを提供しています。

.....部分的にセキュリティを強化しても意味がないということですか?

荒幡 簡単に言えばそうなりますね。たとえば、ファイアーウォールの導入といった「的」なセキュリティ対策をいくら行っても、もし建物に侵入されてコンピュータを操作されれば情報は漏れてしまいます。

あるいは、ハードディスクを複数にしてデータを分散させても、電源がストップしてしまえばシステムはダウンする。つまりビジネスの安全性を確保するには、トータルなセキュリティを考えなければ意味がないのです。

.....つまり、玄関に強力な錠前をいくつもつけても勝手口が開いていればそこから泥棒に入られたり、防火対策がなければ火事ですべてを失ってしまうというのと同じでしょうか。

山森 その通りですね。私たちは企業におけるリスク管理の研究を早くから始め、想定されるリスクを、物的要因によるものと人的要因によるもの2つに大別し、それぞれの項目を詳細に検討してきました。その結果、ざっと40近いリスク項目がある。このうち、どれを優先して対策を講じるかは企業の方針によりますが、オフィスの管理を担当するファシリティマネジャーがセキュリティを考えるのであれば、すべてについてひと通り検討し、守るべき対象は何か、それをどのような状態に保持するかなどを考慮し、そのうえで独自のセキュリティの方針を決める必要があるのです。そして、セキュリティ性能の高い施設を実現しなければなりません。

建物用途に応じた技術シート

建物用途: 研究所	建物用途: 工場	建物用途: 銀行	建物用途: 事務所ビル	
トータルセキュリティパッケージ技術シート				
想定されるリスク	対策種別	セキュリティレベル	対策例	採用の有無
物的要因によるリスク 自然災害 地震 台風 豪雨・洪水 豪雪 地滑り・断層 落雷 設備・建屋の災害・障害 火災 停電 電気工事 回線故障 電磁波ノイズ 電気の質 温湿度 塵埃 断水 ガス供給停止 漏水 振動・騒音 設備機器故障 劣化・腐食 システム故障	1 抑制対策 リスクを予め除去・軽減させる対策	1	発電機、UPS 燃料備蓄、配線計画(強電配線との分離)建築資材の選定、配材材質の選定、配管計画、防振計画・施行、早期更新、可燃物の排除、サーバルームの配置、操作ガイダンス、建築ゾーニング(セキュリティレベル)アメニティ充実、室名の非表示、メンテナンスの容易性、システムのアクセス管理(個人認証)	
	2 防火対策 リスクの実現を阻止する対策	1-2	免震構造、免震床(フリーアクセス)耐震構造、防火仕様、風雨対策(開口部遮断、ガラス厚等)排水計画、計画地の地質(洪水対策)、避雷システム(能動的)落雷時の等電位対策、ノイズフィルター、電磁シールド、高調波対策、高性能フィルター、建築躯体(壁厚等)入退室管理、ファイアーウォール	
	3 検知対策 リスクの発生を迅速に検知する対策	1-3	火災の早期発見(超感度センサー)漏水センサー、超感度センサー、監視システム、火災放置設備、ウイルスチェック	
	4 予備対策 リスクの発生を他の方法でカバーする対策	1-4	電源の二重化、電源引込の多重化、通信回線引込の多重化、空調システムの二重化、上水の備蓄、システムの二重化、搬送ポンプの電源バックアップ、データバックアップ	
	5 復旧対策 リスクの発生時に損失を最小限にし、早期に復旧させる対策	1-5	特殊消火(新ガス)防火区画、汎用品の利用	
人的要因によるリスク 過失 失火 爆発 車の事故 衝突物 誤作動 利益を目的とする行為 プログラムデータ・用品の窃盗 金品の盗難 機密の漏洩 ダメージを与えることを目的とする行為 放火 データ・資料の改ざん ハード・ソフトの破壊 建物の破壊・爆破 不法侵入 労働闘争・サボタージュ				

セキュリティ性能が高い施設とは 総合的な安全性を配慮した建物

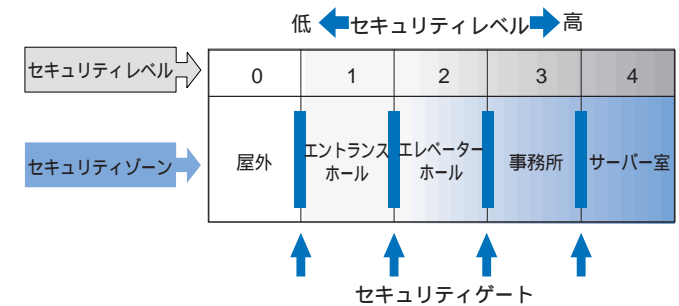
.....セキュリティ性能が高い施設とは、実際にはどういうものを示すのでしょうか?

山森 企業によってセキュリティに求められる内容やレベルは違いますが、もっとも厳しいレベルで言えば、24時間365日止まらない高性能なシステムを稼働させて業務を継続できる施設ということになるでしょうね。

.....その条件を満たすために、さまざまな設備を付けるのですね。

山森 そうなりますね。システムの安定性や堅牢性を高めるのはあたりまえですが、最初に説明したように、リスクにつながるあらゆる要素を排除しなければなりません。このため、入退室管理も厳しくなります。

多重ゲートシステム

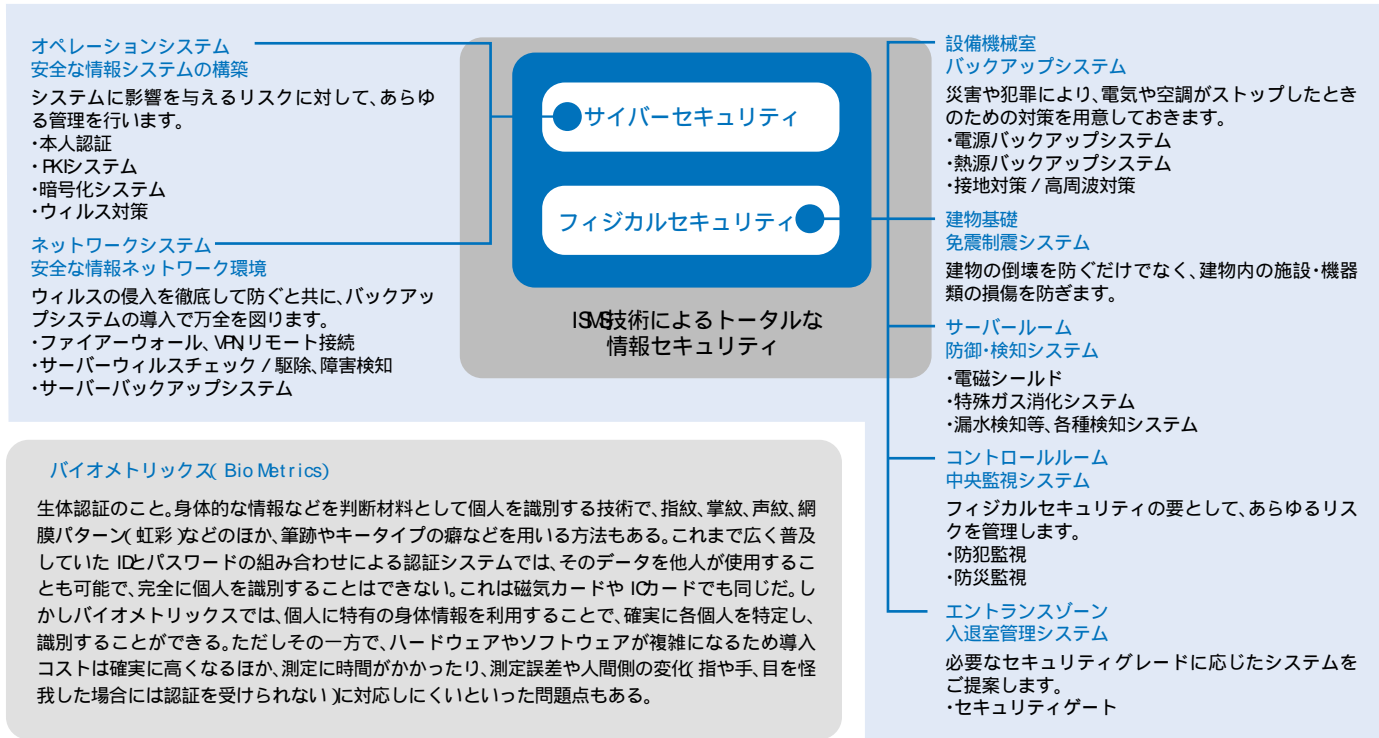


各所に監視カメラを設置

……カード式のキーを利用したりする方法ですか？

山森　それは管理のためのツールの一つにすぎません。まず大事なのは、オフィスをゾーニングし、ゲートによって入室できる人のレベルを分けることなのです。具体的にば「外周部　エレベーター乗り場フロア内」などで三段階以上のゾーニングがなされていれば、セキュリティについてはかなりレベルの高い施設といえるでしょう。そしてその管理のために磁気カードや、最近では非接触の ICカード、あるいは指紋や網膜パターンによるバイオメトリックス(下記コラム参照)を導入するケースが増えてきています。

荒幡　ここで一つ考えなければいけないのは、セキュリティのレベルを高めるのと、セキュリティ性能の高い「いい施設」をつくるのは少し違うということです。たとえば入退室管理のための一つとしてガードマンを置く方法がありますが、もともと建物を設計する段階で人の動線を十分に検討していないと何力所ものチェックポイントを設けなければならず、それこそ「ロビーがガードマンだらけ」になってしまいます。これでは建物の印象も悪くなるし、使いにくいだけでなく人件費もかさむでしょう。あるいは、いくら最新式のバイオメトリックスを導入しても、ゾーニングがシンプルではなく、誰かと打ち合わ



世界的なセキュリティの規格取得が総合的な安全性を考えるきっかけに

……大成建設がトータル・セキュリティ・ソリューションに関心を持ったきっかけはどのようなことだったのですか？

山木　私たちは顧客企業の依頼を受けて施設の建設を行いますが、そのときには多くの機密事項に触れることとなります。たとえば生産工場の新設プロジェクトでは、どんな製品をどのくらいの量、製造するのかといった、メーカーにとって最重要の極秘情報まで事前に聞かされるのです。したがって、データの管理についてはもともと高い意識を持っていましたし、当然、プロジェクトごとに守秘義務契約を締結します。その姿勢を明確にするため、昨年、情報セキュリティ管理の国際的規格である「BS7799」の認証を取得しました。

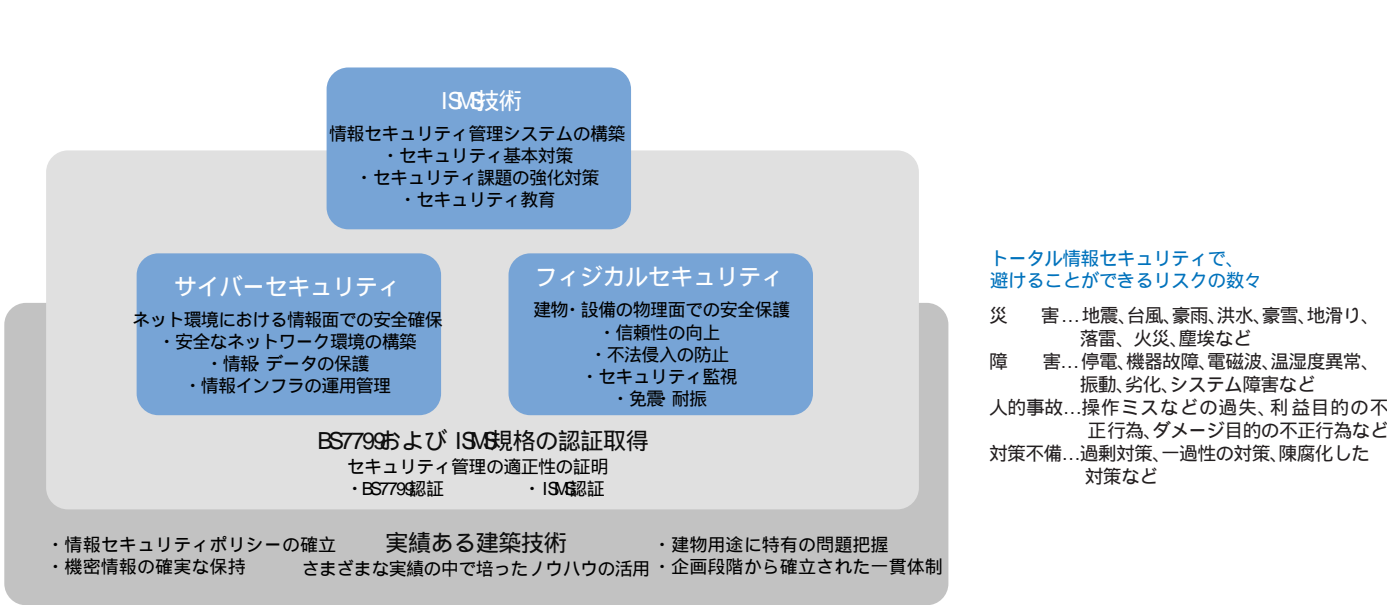
……BS7799とはどんな規格なのですか？

山木　英国規格協会（BSI）が策定した情報セキュリティに関する国際規格で、「サーバなど情報機器の安全性を確保し、適切に管理する」といった要件を12以上満たすことで初めて合格できます。ちなみに建設会社でBS7799の認証を取得したのは、今回が世界で最初であるだけでなく、現在でも他に例はありません。

せをしに行くだけでいくつものゲートを通り抜けなければならないビルでは、たとえ安全性は守れても仕事の効率が落ちてしまう。つまり、本当の意味でセキュリティ性能の高い施設をつくるには、建物の設計段階から、「どんなテナントが入り、どんなセキュリティレベルを必要とするのか？」と考え、安全で使いやすいビルにしなければならないのです。私たちがトータル・セキュリティ・ソリューションのサービスを始めた理由も、まさにここにあります。

……ICカードやバイオメトリックスといったアイテムだけにこだわるのではなく、施設全体の機能を考えるべきですね。

荒幡　そうですね。これは半分笑い話なんですけど、地方都市のあるオフィスビルを訪ねたとき、何の入退室管理もしていなかったので、「セキュリティはどうなっているのですか？」と聞いたら、「ここでは全員の顔を知っているので不審者がいれはずぐにわかります」という答えだった(笑)。つまり、アイテムだけにこだわるのではなく、総合的に「何をどうやって守るのか？」というテーマを最初に考えるべきなんです。またもちろん、そのためにどのくらいのコストをかけられるのかも重要になります。



ファシリティマネジャーは安全に無関心ではられない

……日本でも最近は、企業の安全意識がかなり高まっているようですが、山森　やはり「9.11」のテロ事件の影響は大きいようですね。もちろん、あれほどの攻撃に耐えるビルを建てるのは実際には難しいでしょうが、「非常事態による危機管理」という考えが知られるようになってきましたし、その前提となる予防管理、つまりリスクマネジメントの意識も高まってきました。

……テロとか大規模な災害が起きたら、通信システムを二重化するだけでは安全とは言えませんからね。

山森　そうですね。例えばコンピュータシステムを稼働するには、通信だけでなく電源の安全性も考えなければ不十分だということは、すでに多くの企業が認識しています。このため、オフィスビルにおいてもバックアップ電源の有無が、テナント企業にとって大きな関心事になってきました。

……電源のセキュリティにも、入退室管理と同じようにさまざまなレベルがありますね。

山森　首都圏でもっとも恐れられている災害は大地震でしょう。もし東京に震災が起きた場合、電力などのライフラインが回復するまで最短でも3日、もしかするともっと長くなるのではないかとわれています。その間、業務を継続するにはそれだけのバックアップ電源を持っていなければなりません。つまり予備の発電設備と十分な燃料、冷却水を備えたビルはセキュリティ性能が高いといえるでしょう。ただ実際にはそこまでコストをかけるのはなかなか難しいので、サーバと端末だけを2〜3時間動かすバックアップ電源を用意したり、最低限、データを保護するだけの時間、コンピュータを稼働できる予備電源を備えたビルもある。どの程度のセキュリティが必要か、損失額、発生確率と対策費用を費用対効果の面からそれぞれの企業が考えたうえで、オフィスを計画するべきでしょう。

建物からシステム、業務までのトータルセキュリティサービス

セキュリティは総合的に考えなければいけないのですが、現実問題として、建物からシステム、そして業務支援まで幅広いコンサルティングサービスを一つの企業で行うのは決して簡単ではありません。このような考えから、大成建設では野村総合研究所（NRI）と共同で「トータルセキュリティサービス」の事業を開始しました。このサービスは、企業に対して、セキュリティポリシーの策定からセキュリティシステムおよび施設の構築、そして運営までを一元的に提供するもので、リスクマネジメントのアウトソーシング化を可能にしています。

……大地震以外の原因で電力がストップすることはあるのですか？

山森　大きなビルの場合、電力の引き込み線は二重化されていますし、電力会社のほうでも複数の系統から給電できるようにしている場合もあるので、ビル全体が停電するということは実際にはほとんどありません。しかし、高性能なシステムを持つ企業ではより高い安全性を確保するために、スポットネットワーク受電といって、常時、複数の系統から並列に電力を供給してもらい、事故や工事計画停電時に系統切換による瞬時停電を防ぐというシステムもあります。

……こうやってお話を伺っていると、セキュリティを実現するにも、多くの知識が必要だということがわかりますね。

荒幡　最終的に、企業のセキュリティ計画を立案するのはファシリティマネジャーなので、正しい知識を持つ必要はあるでしょう。大事なのは、流行だけに惑わされず、総合的で中長期的視野に立ったセキュリティ対策をすることなのです。最近ば「無線LANを導入したい」と話すオフィス管理者がいます。たしかに無線LANは便利ですが、そのメリットだけを考えて導入すると電波が外に漏れ、ハッキングの恐れがあります。「じゃあ、建物を電磁シールドすればいい」と簡単に考えることもできない。その結果、オフィスで携帯電話が使えなくなり、業務に支障が生じたケースだってあるのですから。

山森　セキュリティ対策の多くは利便性と相反しますから、それも含めてトータルな方針が欠かせないのです。これは明らかにファシリティマネジメントの分野でしょうね。

荒幡　安全意識の高い外資系企業では、入居するビルのセキュリティ性能を、ファシリティマネジャーなどのリスク管理担当者が事前に厳しくチェックします。これに対して日本企業はまだ十分とはいえません。情報通信技術を駆使して企業活動を行うIT社会においては、経営戦略に沿ってファシリティを有効な経営資源として活用することが求められてきます。それだけに、これからの企業は、もっともっと高い安全意識を持ち、セキュリティ対策を進めてほしいですね。