松崎 正利氏
エンジニアリング事業本部 情報ソリューション本部上席エンジニア

# 物理セキュリティに求められるもの

## ブロードバンドの普及とセキュリティガイドライン

基調講演の冒頭、松崎氏は近年の急速なブロードバンドの普及とそれに伴うハイテク犯罪の増加について言及した。

まず、情報機器の世帯普及率10%までの所用年数をみると、電話は76年、携帯電話は15年、パソコンは13年を要したが、インターネットはわずか5年で到達している。この急激な発展に伴い、インターネット相互接続点を流れる情報量も、ここ10年で1,000倍へと急増したという。また、ハイテク犯罪の検挙件数をみても、平成9年度の262件に対して、平成19年度は5473件(警視庁資料)と爆発的に増えている。もちろんこれは検挙された件数であって、その背後にはもっと多くの犯罪が潜んでいることは言うまでもない。

その対策として、2000年には不正アクセス禁止法、2005年には個人情報保護法が施行されるなど、セキュリティに対する法体系も徐々に整備されてはいるが、必ずしも充分とは言えないのが実情のようだ。

このような現状を踏まえ、内閣官房の情報セキュリティ対策推進会議からは「情報セキュリティポリシーに関するガイドライン」として情報セキュリティの定義が提示されている。そこには「情報資産の機密性・完全性・可用性」を維持することが大切であると謳われている。機密性とは「許可されている人間だけが情報にアクセスできる状態」であり、完全性とは「情報の正確性と完全性が維持されている状態」、可用性とは「必要な時に確実に情報にアクセスできる状態」である。

一方、世界基準の情報セキュリティ認証規格としてはISO/IEC27001が挙げられるが、2008年度現在、国内では約2800社がその認証を取得しているという。同様に、倉庫・物流施設に求められるセキュリティの認証制度として、監視カメラのシステムを重視したTAPAがあるが2007年度現在、世界1224件の取得企業の中で、アジアが約半数の610件を占めている。

## 何を、どのように守るのか セキュリティ計画の必要性

情報資産に対するリスクとしては、前述した情報資産の機密性・完全性・可用性が維持できなくなったケースが考えられる。つまり、盗難・盗聴・盗撮、不正アクセスなどによって情報が漏えいするという「機密性が失われるリスク」、内部不正や紛失、ウイルスなどによって情報が改ざんされる「完全性が失われるリスク」、停電やテロ、ネットワーク故障などによって情報が使えなくなる「可用性が失われるリスク」が存在する。

このようなリスクをしっかりと把握・分析し、それを許容・回避・低減・転嫁(保険等)にジャンル分けして正しく評価する「リスクアセスメント」の考え方が重要になってくる。その上で、それぞれについての「リスク対策」を考え、「セキュリティ環境の構築」へと向かうことが大切だ。

さて、このセキュリティ環境の構築には4つの基本原則がある。周囲からの見通しと照明を確保する「監視性の確保」、適切な維持管理とコミュニティ形成を図る「領域性の強化」、犯罪企図者の動きを限定し接近を妨げる「接近の制御」、部材や設備等を破壊されにくいものとする「被害対象の強化」などである。

この4つの基本原則を踏まえた上で、執務室や役員室など個別のセキュリティレベルを設定し、社員、来客、宅配業者などへのアクセス権限をしっかりと振り分け管理する。そして、区域ごとの基本方針の策定(監視策としての巡回警備やカメラの設置、入退管理策としてのICカードや生体認証の導

入の検討)を実施することが重要だという。

## 入退管理システムの基本は確実な本人認証と監視カメラ

セキュリティ対策の中核となるのは入退管理システムであり、入退管理の基本となるのが、確実な本人認証である。これまでは、暗証番号やパスワードによる記憶認証、鍵やIDカード、証明書などの物理認証によって本人認証が行われてきた。しかし、忘却による煩わしさの問題、紛失や盗難によるなりすまし等の被害の問題が課題とされている。この課題を克服するための方策として、いま生体認証(バイオメトリクス)方式が注目されている。生体認証は、個人特有の生体情報を利用して本人確認を行う認証方式であり、指紋などのように個人の生体的特徴を利用するため、原理的にはなりすましなどの問題が起きにくいといわれている。指紋の他に静脈、掌形、顔、虹彩などがあり、署名や声紋までが含まれるが、現時点ではFeliCaなどのICカードと併用して使われるケースが多くなっている。

また、この入退管理システムと監視カメラの連携が近年のトレンドとして注目されている。特に大型の案件ではネットワークカメラの採用が増えてきているという。これまでのアナログカメラに代表されるCCTVシステムはいわゆる「閉じたシステム」であったのに対し、ネットワークカメラは既存のインターネット回線に接続さえすれば、誰もがパソコンを通じて監視映像を閲

覧し、監視システムをコントロールすることができる。もちろん、遠隔地での操作も可能だ。特に、ICカード等を利用した入退管理システムと連携した場合、ICカードの氏名やナンバーを入力するだけで、いつ、誰が、どの部屋に入退したかを瞬時に検索し、その映像を呼び出すこともできる。事故が発生した時の事後検証に大きな力を発揮することは言うまでもない。

現在、監視カメラは業種や業態を問わず、様々な分野で利用されている。また、監視用途ばかりでなく、商業施設の動線分析や流通施設の車両誘導、さらには工場や生産設備の工程管理などにも活用されている。それだけに、監視カメラのさらなる普及・拡大やセキュリティ施策の一般化に資するためにも、性能基準や評価手法を標準化し、用語の統一を図るなどの業界内連携が必要となってきているという。

基調講演の最後に松崎氏は「物理セキュリティは、本来建築計画に負うところが大きい。しかし、利用者の日常の利便性に配慮すると、出入口を増やすなど、妥協せざるを得ない部分がぜい弱性として生まれる。そこを補うのがセキュリティシステムであり、清水建設がセキュリティビジネスに参入している理由もそこにある」との理念を語った。200年に及ぶ歴史の中で、絶えず「堅固で安全な施設を造る」ことを理想としてきた清水建設の「セキュリティ」に対する大きな自負と責任が感じられた。

GDSF JAPANの各セッション取材レポートは、次号以降２セッションずつ紹介します。