クロール　日本企業に求められるセキュリティー対策

有事対応は平時の準備から

２００１年に発生した米国の同時多発テロ事件をきっかけに、日本企業のセキュリティー意識は急速に高まった。以降、世界各地でテロや自然災害が発生するたびに各社は対応を強化しているが、世界的リスクコンサルティングファームのクロールでアジア太平洋地区統括責任者を務める影山正氏は「有事対応は平時からの備えが最も重要。セキュリティーで考えるべきは、体制と情報と臨機応変に対応できる意思決定機能だ」と指摘する。

影山氏（左）と村崎氏

社員のＩＴリテラシー向上が鍵

クロールは世界55都市、26カ国に拠点を展開するリスク・コンサルティングファーム。同社は40年以上にわたって企業や政府機関など、さまざまな顧客のリスクマネジメントと有事対応を行ってきた。

近年では、政治的な思想に基づく大規模テロが世界各地で多発していることを受けて、グローバル展開する日本企業からの相談も増えているというが、実際に有効な対策に至るケースはまだ少ないのが現状だ。その理由について影山氏は〝パッチワーク的アプローチ〟を挙げる。例えば、ある国で大規模テロが発生した場合、その国の現地法人のセキュリティーのみを強化したり、ある国で洪水被害が出ればその国にある自社工場のＢＣＰ対策に走るといった場当たり的な対応が散見されるという。中には「汎用的なセキュリティーマニュアルを売ってほしい」と要望する企業もあるという。こうした状況につい同氏は「リスク対策はその企業全体に関わるものであり、個社ごとにその内容は異なる。自社の体制に合ったセキュリティープログラムを構築するためにも、グローバルに展開する企業には、社内のセキュリティーに責任を持って司令塔となるセキュリティーオフィサーが必要だ」と強調する。

企業のリスクは大きく二つに分けることができる。一つは、投資や情報管理、防災、不正など、いわば〝見えるリスク〟。もう一つは、情報の抜き取りやウイルスを使ったシステムの乗っ取りといったインターネット上の〝見えないリスク〟だ。どちらのリスクも日を追うごとに巧妙化しているため、企業が全てのリスクに完全に対応したマニュアルを作ることは不可能に近い。そこで同社ではリスクの芽を早い段階で摘み取る方法として①危機管理に関する内部の仕組みづくり②定期的な情報収集③人材のバックグラウンドチェックーの3点を提案している。社内の仕組みづくりの基本は、有事の動きを考える机上シミュレーション訓練。同社アソシエイト・マネジング・ディレクター日本支社代表の村崎直子氏は「まずはシミュレーションで自社のセキュリティーの欠点を見つけることが重要だ」と訓練の意義を説明する。

海外の現地法人については、その地域の状況を定期的に観測し、情勢に変化がないか確認する必要がある。また、人材についても、採用前の身元調査や退職後の進路、思想の変化などを定期的に確認することが求められる。社内の情報を熟知した従業員が自社の敵となる人間の協力者になった場合のリスクに備えるためだ。

このようにさまざまな対策を提供している同社だが、村崎氏は、企業がリスクマネジメントを考える上での基本は、社員一人一人がリスクに対する想像力を持つことだという。最近ではＳＮＳで自分の居場所や交友関係を無防備に公開する人が増えているが、こうした情報は犯罪組織に利用される恐れがある。「多くの企業は社員のＩＴリテラシーの向上に努め、一定の秩序を整えることから始める必要がある」と指摘する。