第３３１回産業事情検討会（3 月 29 日）

企業のグローバル展開と IT セキュリティリスク

㈱カスペルスキー　営業統括責任者　宮橋一郎氏

本日のテーマの意義について

企業が海外に進出するに当たって、さまざまなリスクを考慮しなければならない。リスクによってビジョンの実現が阻まれることは不本意である。できるはずであった準備や対策を怠ったために事業がリスクにさらされた場合にはなおさらである。まさに、「情報セキュリティリスク」はそれである。また、情報セキュリティ事故では大きな金銭的な損害をこうむるだけでなく、事業を前進させることとは逆方向の後ろ向きの力が膨大にかかり、組織も人員も大きく疲弊する。

企業で起こる情報セキュリティ事故は、高度な技術を用いたサイバー犯罪によるものばかりではなく、不注意によるデータ紛失や漏洩は跡を絶たない。下請け会社の従業員はなぜ社用の PC を家族に譲渡できたのか。なぜその PC を娘が使用する際にセキュリティ対策がなされていなかったのか。なぜ PC を家族に譲渡する際に、プロジェクト関連データを消しておかなかったのか等、多くは、明確なルールを設定して対策を打てば解決できるもの、被害を最小限に抑えることができるものばかりである。

情報漏洩事故への対応

一度情報漏洩事故が起こると、膨大なマンパワーと時間、費用をかけた対応が求められることになる。事故対応で行われる主な作業。

１．「初動」流出元の捜査と流出内容の調査

どこから流出したのか流出元を突き止める捜査から始まる。そして、どの程度の情報が流出したのか流出内容を確認しなければならない。携わった担当者ですでに別の会社に移っている者もいる。当時のプロジェクト関連資料を見返しながら、インターネットにどの部分が流出したのかを確認する膨大な作業がある。この間にも悪意ある犯人は、波状攻撃をしかけ情報流出の範囲は広がっていく。

２．お客様への報告と公表

正確な報告が求められるとともに、進行中の捜査で十分に確認が取れていないことでもいち早く報告をしなければいけない。当時の契約でどのような責任分担があったのかも再確認する必要。経営者からの対応も求められる。社会的立場によっては記者会見への対応も求められる。何が正確なことなのかわからないままにその場対応を余儀なくされ、また、プレスが正しく報じてくれる保証もない。

３．被害者への対応

「被害者への通知」、「相談窓口の設置」、「個別訪問」など。役員クラスの対応が求められることも多い。

海外セキュリティ環境と日本企業のリスク

世界各国と比較して日本は IT セキュリティリスクが比較的低い国である。さまざまなタイプのウィルスやスパム、マルウェアによる感染事故で見て、日本は他の国よりも事故の体験率が少ない。それに対して、インド・中国など日本企業の多くが進出するアジアの新興国の感染率は日本の数十倍である。そういう地

域に進出する日本企業の最大のリスクは、1. 自身のリスク感性が鈍いこと、且つ、2.「鈍感」だという自覚が薄いこと、そして、3. 金を出し惜しんで逆に膨大な損失に至ることだ。

海外進出リスクへの対策

最低限やっておかなければならないことは、1. 進出先のリスク度合いを知る。2. 情報セキュリティに関するルールを明示し教育する。3. 最低限の IT セキュリティ防衛装備を導入する。4. 最低限のコントロールプロセスを実施する。5. いざ事故が起こったときのルールを決める、である。

「セキュリティ・ポリシー」を作成し、パートナーを含めたすべての関係者とルールの共有をする。会社として「どの情報を最重要保護対象とするのか」その方針を明確にし、保護対象の情報についてはアクセスコントロール、職務権限分離によってアクセスできる主体を限定する。「起こしてはいけない」のはもちろんだが、「起こった場合にどうするのか」対応のルールを定め、被害が拡大しないための体制を整えることが重要である。