必要性高まる標的型メールへの対策

◆増加する標的型メールの攻撃とその被害

2016年6月に旅行大手のJTBは「最大約793万人分の顧客情報が流出したおそれがある」と発表した。その理由は、関連会社の社員が取引先を装ったメールに添付されたファイルを開き、パソコンやサーバがウイルスに感染したからである。3月19日に不審な通信に気づいてから同25日に通信を完全に遮断するまでに6日かかったことが、顧客の氏名、住所などの個人情報流出のリスクを拡大させた。

今回JTBに届いたメールは、特定の組織や個人を狙った「標的型メール」である。この標的型メールによる攻撃がここ数年増加しており、警視庁が把握する15年の件数は過去最多の3,828件になった。その中には125万件の年金情報が流出した日本年金機構の事件など大きな被害が出たものもある。JTBの発表は16年も標的型メールによる攻撃が続いており、その対策が急務であることを示している。

◆対策は組織全体で、予防措置の他に事後対策も定めておくことが必要

15年の標的型メールによる攻撃は、同じ内容を送るばらまき型が92%を占めた。標的型メールの9割近くがインターネット上では公開していないアドレスに送信され、8割弱が受信者の信用しやすい偽装したアドレスから送信されていたことから、犯人が入念な調査と周到な準備をしたうえで攻撃していることがわかる。

この標的型メールへの対策には、メールの発信元や添付ファイルをチェックするシステム面の対策と、不審なメールを開かない、重要機密は暗号化してやり取りするなどの運用面の対策がある。どちらも組織全体の問題としてしかるべき予算をとり、情報システムの管理部門が中心となり、経営トップから現場の社員まで教育、運用を徹底すれば予防措置として大きな効果をもたらす。

ただし、上記の対策をとっても、年々手口が巧妙になり、見破りにくくなっている攻撃を100%防ぐことは難しい。そのリスクも考慮して重要データは暗号化しておくこと、そして、ウイルスに感染した場合の事後のルールとして、通信の遮断やウイルスの除去、被害の洗い直し、警察への連絡、発表の仕方などを定めて、被害の大きさを最小にとどめる準備もしておく必要がある。　　【藤井和則】