手口巧妙、水際対策に限界

標的型メールの脅威 ▶上

不審察知ＡＩ活用急ぐ

ＪＴＢから最大679万人分にのぼる顧客情報が流出した可能性があることが先月発覚した。昨年6月の日本年金機構の125万件を超える大規模流出は、犯罪者が日本から個人情報を盗み出す動きが活発になっている実態を映す。明るみに出る被害の大半は攻撃対象を調べ尽くして送りつける標的型メールと呼ぶ手法だ。日本企業はどう対処すればいいのか。

中東の政府系情報機関で数年前まで非友好国に対するサイバー攻撃に携わった元ハッカーが6月下旬、都内で日本経済新聞の取材に応じた。「侵入できない標的は一つもなかった」と振り返る。

国家運用の軍や情報機関のサイバー部隊のように豊富な資金と人材があれば企業の情報システムへの侵入は容易という。「水際対策は無意味。実際に不正侵入を繰り返した私が言うのだから間違いない」

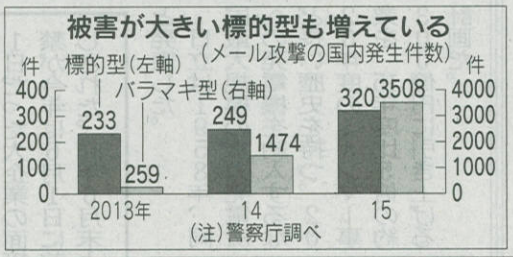
日常業務にワナ

ＪＴＢは社内システムへの不正侵入を防ぐ水際対策に余念がなかった。システムの入り口にファイアウオールと呼ぶ監視機器を設置、不審な通信を遮断する体制を整えていた。不審メールを開封しないよう毎月2度は抜き打ち訓練も実施。それでも不正侵入を防げなかったのは、ありふれた日常業務の中にワナが仕掛けられていたからだ。

3月15日。ＪＴＢ子会社の社員が「航空券控え添付のご連絡」という件名の電子メールを受け取った。「eチケットの控え」と題する添付ファイルを開くとウイルスが作動し始めた。

ＪＴＢの金子和彦取締役は「通常業務のようなメールが送られ、担当者は添付ファイルを開いてしまった」と釈明する。

ＪＴＢから多くの個人情報が流出した可能性がある（6月、国交省）



差出人のアドレスは取引先である全日本空輸のものに改ざんしていた。件名や添付ファイルのタイトルも日常業務を模していた。犯人がＪＴＢの業務内容を調査したうえで送信したのは明白だ。

弱点調べ執拗に

特定の組織を狙うサイバー攻撃は標的型攻撃と呼ばれる。警察庁によると、ウイルスを仕込んだ電子メールを送る標的型メール攻撃の発生件数は2015年に前年比3割増えた。不特定多数を狙うバラマキ型と異なり、犯人は狙った組織のシステムの弱点を調べ、目的の情報が得られるまで執拗に攻撃を繰り返す。

標的型メールは年を追うごとに巧妙になる。企業のメールを傍受して本物そっくりに作成し、社員がフェイスブックなどに書いた内容を盛り込むこともある。

「情報セキュリティー業界で、水際対策の限界が叫ばれるようになったのは2年ほど前から」（アズジェントの中山貴禎セキュリティ・サービス部部長）という。犯人は乗っ取ったパソコンから目的の情報を探そうと社内システムを回遊する。各社はこうした不審な動きを察知する事後対策システムの開発を進める。

注目を集めるのが人工知能（ＡＩ）だ。社内の膨大なデータの中で一握りだけ存在する攻撃者の通信を人力で特定するのは難しい。ＡＩに社内システムの正常な状態を学習させ、逸脱した動きを察知する。ソフトバンクグループは昨年、ＡＩに強い米サイバーリーズンに出資。ＡＩを使うセキュリティー技術は富士通やＮＥＣも開発を急ぐ。

企業の取り組みは現段階で水際対策が中心。情報処理推進機構によるとサイバー攻撃に対し陣頭指揮を執る最高情報セキュリティー責任者（ＣＩＳＯ）を置く日本企業は4割。欧州の7割や米国の6割を下回る。日本企業は防御に加え有事への備えが求められている。