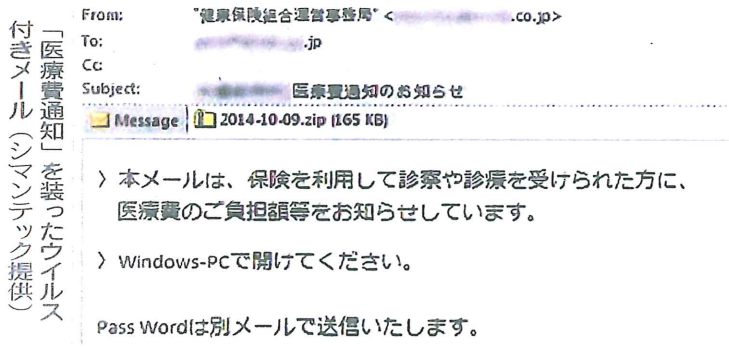
産経新聞　【月ぎめ定価3093円（本体価格2864円＋消費税229円）】1部売り130円　（第3種郵便物認可）

クラウド悪用 標的型メール

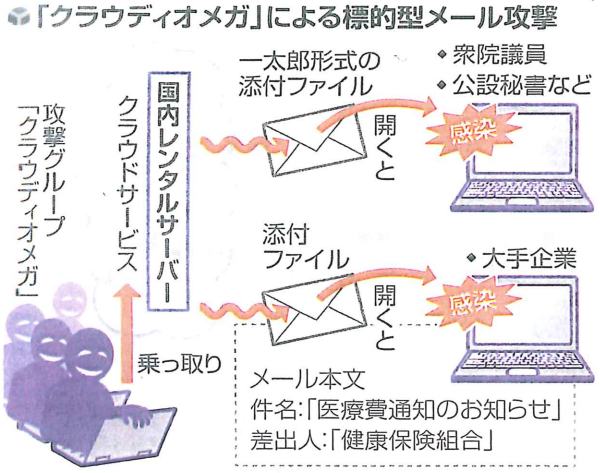
サーバー乗っ取り 衆院関係者に

中国系？周到準備か

国や大手企業から機密情報などを盗み取ろうと、同じグループの関与が疑われるサイバー攻撃が相次いでいる。ウイルスを送りつける標的型メール攻撃の一種で、日本国内のレンタルサーバーを乗っ取り、文書ソフトの弱点を突いて攻撃するなど、手口は巧妙化している。2014年の標的型メール攻撃は前年の5倍を超えており、国などは注意を呼び掛けている。



「医療費通知」を装ったウイルス付きメール（シマンテック提供）



昨年から攻撃増加

14年11月上旬、当時の衆院議員や公設秘書、衆院事務局職員合わせて約40人のメールアドレスにウイルス付きメールが集中的に送られた。

同事務局によると、ほとんどがジャストシステムの文書ソフト「一太郎」の弱点を利用した手口で、一太郎の文書に見せかけた添付ファイルを開くとウイルスに感染し、外部から遠隔操作される仕組みだった。情報の外部流出は確認されなかったが、中央省庁では広く一太郎が使われており、同社は同月中旬に修正ソフトを配布した。

情報セキュリティー会社のシマンテックによると、このウイルス付きメールは、企業などが借りる国内のレンタルサーバーの一部が乗っ取られ、そこから送られていた。レンタルサーバーを使う「クラウドサービス」を悪用していることから、同社は、この攻撃グループを「クラウディオメガ」と名付けた。

同グループによる攻撃は11年に確認され、13年までは年数件程度だったが、14年は1年間だけで約100件と急増した。今年に入ってからも攻撃は続いており、グループの一部は、中国に拠点を持つ集団が関与する可能性があるという。

大手企業も被害

クラウディオメガによる標的型メール攻撃は、大手企業も受けている。

「保険を利用して診察や診療を受けられた方に、医療費のご負担額等をお知らせしています」

三菱商事や、富士重工業の関連会社の社員らに14年9～10月、「医療費通知のお知らせ」と題するメールが相次いで届いた。差出人名は「健康保険組合」となっており、添付ファイルを開くよう指示していた。開いた社員は「医療費などを確認しなければならない年末調整の時期だったので、つい開けてしまった」と話す。

このメールでパソコン2台が感染した三菱商事は約600人の氏名や電話番号などが流出した。同種の攻撃を受けた伊藤忠商事も、約400人分の個人情報が流出している。

こうした添付ファイルのウイルスは、衆院関係者向けとほぼ同じだった。シマンテックの林薫主任研究員は「ウイルスの種類から同一犯なのは間違いない。高度な技術を使い、3年以上かけて周到に準備し、標的を絞って攻撃しているのではないか」と分析する。

独立行政法人の情報処理推進機構が確認した標的型メール攻撃は、13年に97件だったが、昨年は5・2倍の509件と激増した。同機構は「信じてしまいそうな巧妙なタイトルや文面となっているので、安易に添付ファイルを開かないでほしい」と注意を促している。