「標的型攻撃メールの例と見分け方」: IPA テクニカルウォッチ(編集版)

特定の組織や人から機密情報を窃取する「標的型サイバー攻撃」が深刻な脅威となっているが、その中でも「標的型攻撃メール」が依然として猛威を振るっている。

標的型攻撃メールは、不特定多数に大量に送られるウイルスメールとは異なり、特定の組織や人にしか送られないため、セキュリティソフトの定義ファイルに登録される前に標的とするメール受信者まで届いてしまう。そのため、受信者がセキュリティソフトを利用していても、被害を防ぐことが難しい。

また、メール受信者が不審をいだかないように様々な騙しのテクニックが駆使されているため、メール受信者は本物のメールと勘違いしてしまい、ウイルス感染の仕掛けが施された添付ファイルを開いたり、本文に記載されたウイルス感染の仕掛けが施されたサイトへのリンクをクリックしたりしてしまう可能性が高い。

添付ファイルの開封や本文のリンク先にアクセスすると、遠隔操作ウイルス（RAT：Remote Access Trojan／Remote Administration Tool）に感染し、新たなウイルスの感染、組織システム内へのウイルス拡散、情報収集、機密情報の外部への漏えい、システムの破壊といった大きな被害へ発展することになる。

標的型攻撃メールについては、国内でも 2005 年頃から報道されるようになったが、特に 2011 年 9 月に大手重工の被害が報道されてからは、多数のメディアで取り上げられるようになり、ここ数年は実際のメールが報道されることも多くなったため、目にする機会は増えたともいえよう。このような標的型攻撃メールは、大手企業や官公庁だけでなく、それらの組織と関係のある業界団体や中小企業に対して行われることにも留意が必要である。加えて、プライベートで利用しているメールアドレスを一時的に業務メールで使用している、またはしていた場合には、プライベートのメール利用環境でも不審なメールに注意する必要がある。

― 標的型攻撃メールの例 ―

標的型攻撃メールの例を用いて不審か否かを見分けるための着眼点については以下の URL からのダウンロード資料に記載する“2.2 標的型攻撃メールの例(5 ページ)”を参照してください。

http://www.ipa.go.jp/security/technicalwatch/20150109.html

― 標的型攻撃メールと注意すべき対応方法 ―

次の表はIPAに情報提供があった標的型攻撃メールや公開情報から得た知見を基に標的型攻撃メールの特徴をまとめたものである。 これらの特徴に複数合致するメールを受信した場合は、標的型攻撃メールの可能性があるため、注意して対応する必要がある。対応方法については、以下のURLからのダウンロード資料に記載する“3. 標的型攻撃メールへの対応(22ページ)”を参照してください。

http://www.ipa.go.jp/security/technicalwatch/20150109.html

(ア) メールのテーマ	① 知らない人からのメールだが、メール本文の URL や添付ファイルを開かざるを得ない内容 (例 1) 新聞社や出版社からの取材申込や講演依頼 (例 2) 就職活動に関する問い合わせや履歴書送付 (例 3) 製品やサービスに関する問い合わせ、クレーム (例 4) アンケート調査
	② 心当たりのないメールだが、興味をそそられる内容 (例 1) 議事録、演説原稿などの内部文書送付 (例 2) VIP 訪問に関する情報
	③ これまで届いたことがない公的機関からのお知らせ (例 1) 情報セキュリティに関する注意喚起 (例 2) インフルエンザ等の感染症流行情報 (例 3) 災害情報
	④ 組織全体への案内 (例 1) 人事情報 (例 2) 新年度の事業方針 (例 3) 資料の再送、差替え
	⑤ 心当たりのない、決裁や配送通知 (英文の場合が多い) (例 1) 航空券の予約確認 (例 2) 荷物の配達通知
	⑥ ID やパスワードなどの入力を要求するメール (例 1) メールボックスの容量オーバーの警告 (例 2) 銀行からの登録情報確認

(イ) 差出人のメールアドレス	① フリーメールアドレスから送信されている ② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
(ウ) メールの本文	① 日本語の言い回しが不自然である
	② 日本語では使用されない漢字（繁体字、簡体字）が使われている
	③ 実在する名称を一部に含む URL が記載されている
	④ 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる（HTML メールの場合）
	⑤ 署名の内容が誤っている (例 1) 組織名や電話番号が実在しない (例 2) 電話番号が FAX 番号として記載されている
(エ) 添付ファイル	① ファイルが添付されている
	② 実行形式ファイル(exe / scr / cpl など)が添付されている
	③ ショートカットファイル(lnk など)が添付されている
	④ アイコンが偽装されている (例 1) 実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
	⑤ ファイル拡張子が偽装されている (例 1) 二重拡張子となっている (例 2) ファイル拡張子の前に大量の空白文字が挿入されている (例 3) ファイル名に RLO が使用されている