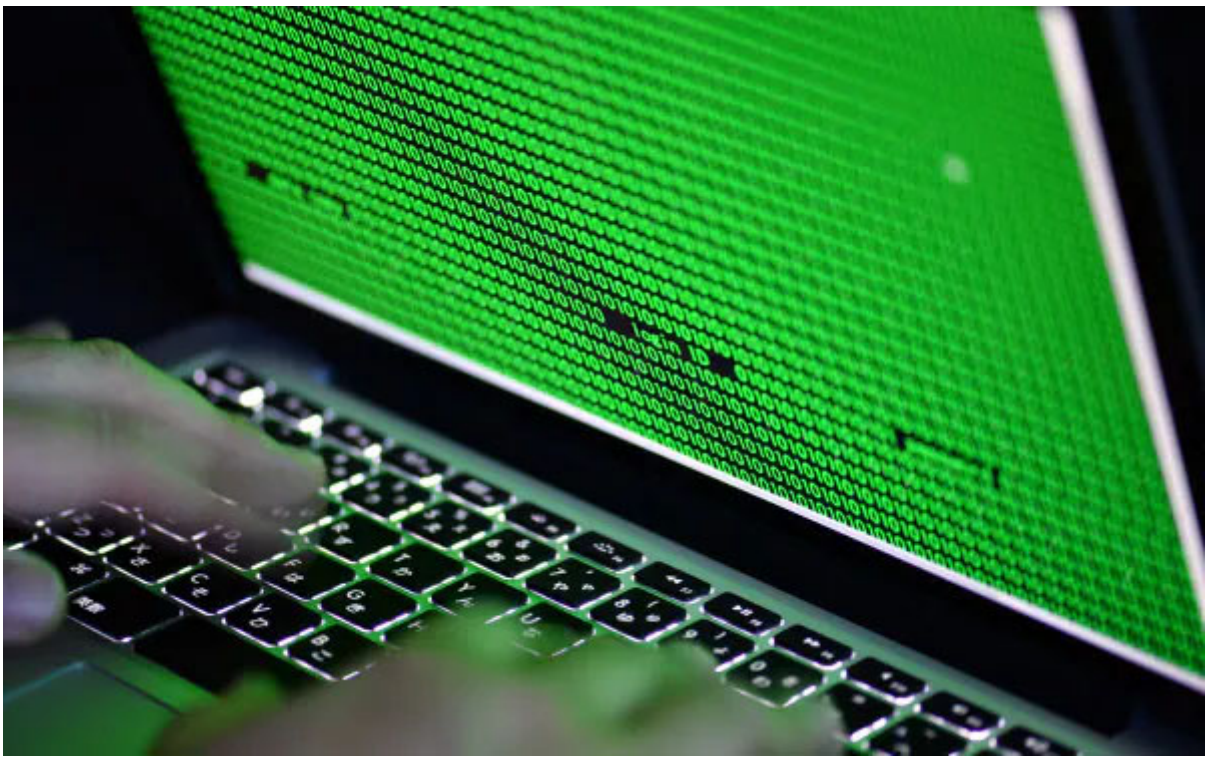
なりすましメール拡散のウイルス、日本に本格上陸

2019/11/29 15:35|日本経済新聞　電子版

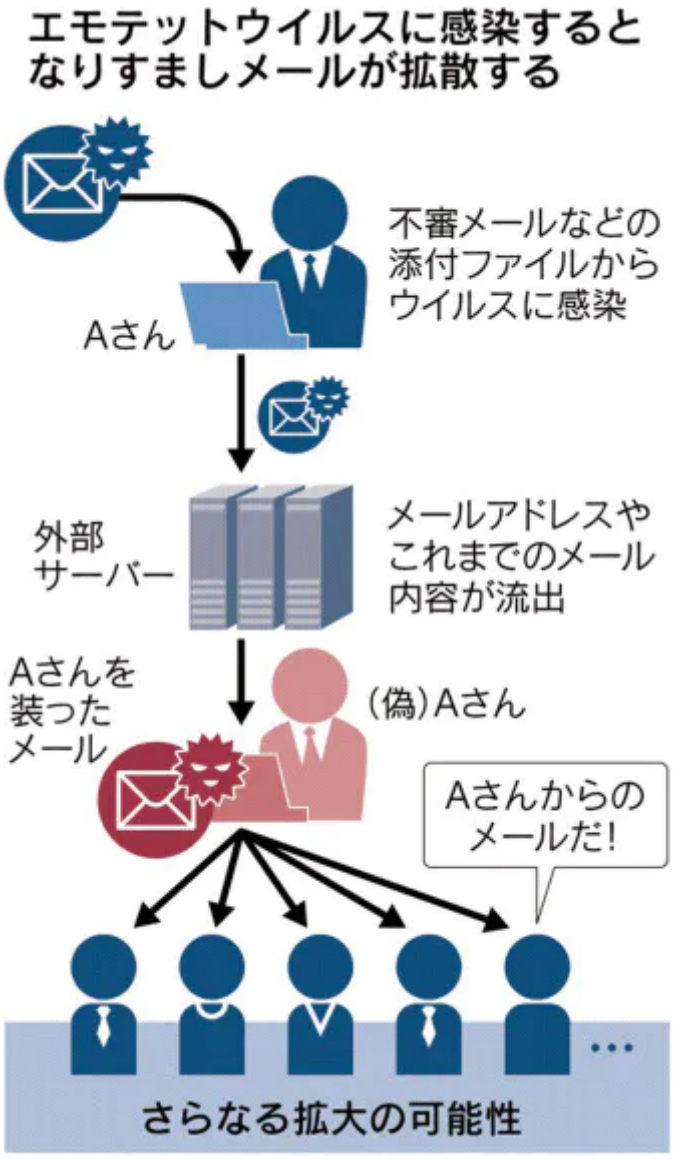


ウイルスは、感染したパソコンからメールアドレスやパスワード、メール本文などを盗み出す

欧米で流行しているコンピューターウイルス「Emotet（エモテット）」が日本に本格上陸し、被害が出始めた。感染するとメールアドレスや本文を盗まれ、本人になりすましたメールが次々と関係者に送られる。首都大学東京や京都市観光協会など少なくとも400以上の団体・企業で被害が出ているとされ、民間団体などが注意を呼びかけている。

10月18日、首都大学東京の教員に海外の雑誌社からメールが届いた。過去にやりとりがあったため、教員は疑問を持たずに添付ファイルを開いた。すると複数の教職員になりすましたメールが関係者に相次いで送信されるようになった。

教職員は自分の意思でメールを送っていないため、同大学は外部に調査を依頼、エモテットの被害だと判明した。添付ファイルやパスワードの外部流出、サーバーデータの暗号化の被害がなかったかどうか調べている。



エモテットは、感染パソコンから別のなりすましメールを作るパンデミック型のウイルスだ。受信メールに添付されたウイルス付きのファイルを開き、ファイルに含まれるプログラムを作動させると感染する。ウイルスは、パソコンからメールアドレスやパスワードなどを盗む。盗まれたアドレスなどは外部のサーバーを経由して流出し、別のパソコンからウイルス付きのなりすましメールを拡散する。

エモテットの感染被害	
首都大学東京 (11/1)	教員が受信したメールの添付ファイルを開封しＰＣが感染。相次いで教職員などへ不審メールが届いた。
双葉電子工業 (11/8)	フィリピン子会社のＰＣがウイルスに感染。子会社の従業員とメールでやりとりした一部のアドレスが盗まれた。
京都市観光協会 (11/25)	同協会の職員のＰＣがウイルスに感染。職員を装ったメールが相次いで送信された。
(注) 日付はウイルスへの感染を発表した日	

京都市観光協会でも、職員が取引先の1社とメールを交わしている最中に、その取引先を装ったウイルス付きの返信メールが紛れ込んだ。エモテットとみられるウイルスが埋め込まれた添付ファイルを開いたという。双葉電子工業はフィリピン子会社で被害にあった。

ウイルスソフト大手のトレンドマイクロによると、エモテットは2014年に確認され、金融機関が標的だった。最近は日本語のウイルス付きメールが送られるようになり、日本で被害が表面化した。トレンドマイクロが対策ソフトで検出した国内のエモテットは9月までは月数十件程度だったが、10月だけで1700件に上った。

サイバー対策のS&J（東京・港）の三輪信雄社長はエモテットについて「メールそのものが盗まれる点が脅威」と話す。ファイルを暗号化して送信しても、別のメールに記載されたパスワードも漏れるので開封されてしまう可能性が高い。

エモテットでメールなどが盗まれると、ランサムウエア（身代金要求ウイルス）の起点として使われる可能性もある。ランサムウエアでサーバーのデータが暗号化されると企業は業務ができなくなる。米国土安全保障省によれば、復旧費用などに1件当たり最大100万ドル（1億円強）かかるという。サイバー防御に詳しい伊藤忠商事の佐藤元彦氏は「日本でもランサムウエアの被害に、エモテットが関与した可能性がある」と指摘する。

民間団体のJPCERTコーディネーションセンター（東京・中央）は「不審なメールの添付ファイルを開封しない」「万が一ファイルを開いた時はプログラムの動作を許可しないようにすべきだ」と呼びかけている。

（島津忠承、河端里咲、林英樹）

本サービスに関する知的財産権その他一切の権利は、日本経済新聞社またはその情報提供者に帰属します。また、本サービスに掲載の記事・写真等の無断複製・転載を禁じます。

Nikkei Inc. No reproduction without permission.