



日本郵政を騙った偽メールが急増！！

昨年末から、

**差出人欄が「日本郵政」や「JAPAN POST」等
となった偽メール**

が急増しています。

この偽メールにはファイルが添付されていて、このファイルをクリックすると自動的に不正プログラムがインストールされ、インターネットバンキングの認証情報が詐取されます。

特徴として、

- ・ 送信者のメールアドレスが日本郵政と異なる「×××@rambler.ru」などのフリーメールとなっている
- ・ 添付されているファイルの拡張子(ファイル名の末尾)が「.zip」、「.exe」など、クリックすると実行する形式になっている

などといったものがあります。

〈偽メール本文の事例〉



拝啓

配達員が注文番号×××の商品を配達するため電話で連絡を差し上げたのですが、つながりませんでした。従ってご注文の品はターミナルに返送されました。

ご注文登録時に入力していただいた電話番号に誤りがあったことが分かりました。

このメールに添付されている委託運送状を印刷して、最寄りのJAPANPOST取り扱い郵便局までお問い合わせください。

敬具

JAPAN POST ジャパンの宛先：

〒〇〇〇-〇〇〇〇

東京都×××××

※ 日本郵政株式会社等のホームページには、この様なメールを送付することはないと明記されています。

※※ 被害防止策 ※※

- 不審なメールは開かずに送信者に確認するほか、添付されているファイル(「.zip」や「.exe」など)を開いたり、リンク先にアクセスしたりしない。
- ウイルス対策ソフトを導入し、常にパターンファイルを更新する。
- OSやブラウザなどを常に最新の状態にする。

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は・・・

石川県警察本部生活環境課サイバー犯罪対策室



076-225-0110



cyber@police.pref.ishikawa.lg.jp