

実在する企業を装った不審メール（ウイルス付きメール）にご注意ください！

実在する企業を装って、ウイルスを仕込んだファイルを添付したり、不審なURLを記載したりしたメールが多数出回っていると警視庁が注意喚起を行っています。

不審メールによってウイルスに感染すると、インターネットバンキングのログイン情報（パスワードなど）が盗まれたり、普段とは異なる偽の画面が表示されて偽のサイトへ誘導されたりすることがあります。

これまでに確認されている不審メールの例として、次のようなものがあります。

○【不審メール例】見積書送付の業務連絡を装ったメール

見積書送付の業務連絡を装ったメールで、メールに添付されているファイルを開くとウイルスに感染するメールが確認されています。

（不審メール例 イメージ）

件名 添付写真について
宛先 ●●●●

いつもお世話になります。
添付写真と同じの御見積をいただけませんか。
よろしく願いいたします。

容量が大きい為、分けて送信致します。

● 添付ファイル：XX_20161031_XXXXXXX.JPG.zip

○【不審メール例】日本郵政グループを装ったメール

日本郵政（郵便局）を装った、ウイルスを仕込んだファイルを添付したり、不審なURLを記載したりしたメールが確認されています。（メールの差出人が部分的に「JAPAN POST」あるいは「日本郵政」等と表示され、メール本文には「JAPAN POST ジャパン」等と記載されているものが確認されています。）

（不審メール例 イメージ）

送信者 ●●●● XXXXXXXX@XXXXXXXX.XX.XX
件名 番号××××××××の下で小包の配達

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

〒●●●●—●●●●●
東京都港区●● ●—●—●
●●ビル

Post Japan Co., Ltd.

○【不審メール例】実在する企業を装ったメール

実在する企業を装った、請求書の送付やFAXの受信通知などといった内容で、メールに添付されているファイルを開くとウイルスに感染するメールが確認されています。

(不審メール例 イメージ)

差出人	●●●●株式会社
件名	●●宛請求書をお送りします。
宛先	●●●●
お疲れ様です。遅くなりました。 ご依頼の請求書をお送りします。	
ご確認の上、お手配よろしく申し上げます。	
● 添付ファイル：2016-06-23-123456.doc 34.0KB	

👉 今後もこのような不審メールが出回る可能性がありますので、以下の点に十分ご注意ください。

■ 身に覚えのないメールや不審な添付ファイルは開かないでください

メールや添付ファイルにウイルスが仕込まれていた場合、メールや添付ファイルを開くとウイルスに感染しますので、身に覚えのないメールや不審な添付ファイルは絶対に開かず削除してください。

■ パソコン動作の異常が発生したら、すぐにパソコンの利用を中止してください

万一、不審な添付ファイルを開いてしまい、パソコンの動作が不安定になる等の異常が少しでも発生した場合は「不正送金ウイルス」に感染している可能性が極めて高いと思われますので、すぐにパソコンの利用を中止してください。

■ インターネットバンキング利用時には細心の注意を

インターネットバンキングを利用される際に、普段と異なる画面が表示されたり、必要のない場面でお客様 ID や各種パスワード、合言葉などを入力させる画面が表示されたりした場合は、絶対にパスワードなどは入力せず、当金庫までお問い合わせください。

■ ウイルス対策ソフトをご利用ください

インターネットバンキングを利用される前には、ウイルス対策ソフトでパソコン内をスキャンすることをお奨めします。万一、不審な添付ファイルを開いたことによりウイルスに感染してしまったら、ウイルス対策ソフトでスキャンするなどして駆除してください。

■ 被害に遭わないために、当金庫の推奨するセキュリティ対策の実施をお願いいたします

詳しくは次のリンクをご参照ください。

「インターネットバンキングを安全にご利用いただくための重要なお願い」

<http://www.chushin.co.jp/attention/outline.html>

以上