
「ウイルスメール駆除」「迷惑メールフィルタ」 仕様について

コスモメディア株式会社

2010. 6. 8

ウイルス駆除

ウイルスメールが届いた場合には、下記のように、通知メールだけが届きます。本文にも、怪しいリンク先などが書かれている場合が多いためです。

件名: Undelivered mail: Your transaction has been processed

メール受信者の方へ、

あなた宛に assentsq@routes.com (虚偽の可能性あり)から送られた以下のメールは、感染オブジェクトを含んでいたために配信されませんでした。

受信者 = hogehoge@jah.jp
件名 = Your transaction has been processed

--- Dr.Web report ---
以下のウイルスが検出されました:
BackDoor.Siggen.17777

検査の詳細:
[29802] /var/drweb/msgs/in/9/01BD5F79/.p2.body archive ZIP
[29802] >/var/drweb/msgs/in/9/01BD5F79/.p2.body/setup.exe
infected with BackDoor.Siggen.17777

検査の統計:
Known viruses: 1

--- Dr.Web report ---

メッセージは以下のレコード名でアーカイブに保存されました:
drweb/drweb.quarantine.fstw8m

元のメールを受信するためには
postmaster, に連絡してください(上記のレコード名が必要です)。

Antivirus service provided by
Dr.Web (R) for Unix mail servers
(<http://www.drweb.com>)

迷惑メールフィルタ

迷惑メールの場合は、件名の最初に[SPAM]と言う文字列を追加してお届けします。次ページからのメールフィルタ設定を参考にお試しください。

件名: [SPAM] Twitter 587-60

<http://open**.googlegroups*.com/web/Twittersecuritymodel_setup.zip>

Hi, mur@jah.jp
Attention! We detected that someone was trying to steal your Twitter account password.
We strongly recommended you to download our secure module to protect account!
Please click on the link below:
<http://open.googlegroups*.com/web/Twittersecuritymodel_setup.zip><http://twitter.com/Twittersecuritymodelsetup.zip>
The Twitter Team
If you received this message in error and did not sign up for a Twitter account, click not my account.
Please do not reply to this message; it was sent from an unmonitored email address. This message is a service email related to your use of Twitter. For general inquiries or to request support with your Twitter account, please visit us at
<http://open.googlegroups*.com/web/Twittersecuritymodelsetup.zip>[Twitter Support](http://twitter.com/TwitterSupport).

この迷惑メールは、Twitterを装い、ウイルス感染するファイルをダウンロードさせる、フィッシングメールです。(本メールはテキストですが、アウトルック等のソフトでは、赤字の部分が見えず、青字部分をクリックするように誘導されます。)

赤色にしている部分が、ウイルスを含むファイルで、そのままクリックすると感染する恐れがあります。

このメールの場合、弊社の迷惑メールエンジンが、迷惑メールと判断していますので、お客さまも、まずは、疑いを持って臨めると思います。

※本メール中の赤字のURLは、途中に「*」を付加するとともに、幾つかの文字を削除しておりますので、クリックしても該当のウイルスには到達しませんので、ご安心ください。