

【NEZU システム通信】

(Vol.0007)

発行日 06.5.31

ごあいさつ

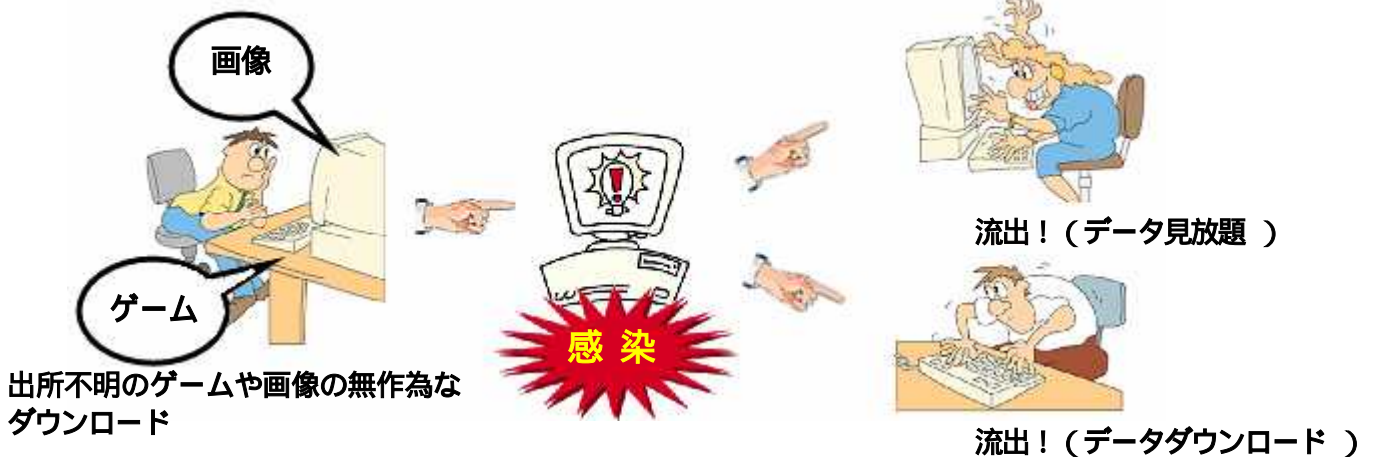
日頃は根津グループとお取引頂きまして、誠にありがとうございます。
今回のシステム通信は、情報流出問題で話題の『ウィニー』の“番外編”です。

『ウィニー』を使ってないのに・・・情報が外部に洩れた！？

それは、「山田オルタナティブ」ウイルスに感染した事が原因かもしれません！

山田オルタナティブ

「山田オルタナティブ」は、インターネット上で写真データやゲームデータになりすまします。被害者が目的のデータと思い、ダウンロードしたデータを実行（写真の表示やゲームの実行）した時点で感染します。被害内容は数分毎にパソコンのデスクトップ画面を画像として記録し、その画像をインターネットに流出させます。デスクトップの画像が流出する事で、被害者がどのような作業をパソコンで行っているか、他人に閲覧されてしまいます。また、他のパソコンから被害者のパソコンの中身（マイドキュメント等）を直接閲覧することができる様にしまい、その中身（大事なデータ）をダウンロードされてしまう可能性もあります。



出所不明のデータや怪しいホームページのデータをダウンロードしてパソコンで実行した場合には、感染している恐れも十分にあります。過去に、芸能人の画像にウイルスソフトが密かに付いていて、画像をダウンロードした際にウイルスソフトがインストールされてしまった！という報告もあります。

では、どうすれば感染しているか判断できるか？ 暴露ウイルスの簡単な確認方法をご紹介します。

暴露ウイルスに感染したかどうかの確認は簡単です。インターネットエクスプローラのアドレス欄に以下の文字を入力して [Enter] キーを押します。入力する文字は半角英数字で、<http://127.0.0.1:80/> 又は <http://127.0.0.1:8080/> と入力します。両方試しても構いません。



(拡大)

上記文字を入力し [Enter] キーを押した後に、「ページを表示できません」等の表示がされましたら感染の可能性はありません。(図 - 1)



もし、画面上にファイル名や「Index of /」の文字(図-2参照)が表示されましたら、暴露ウイルスに感染している可能性があります。速やかにパソコンのインターネットの線を外し、ウイルス駆除を行ってください。無線接続の場合には無線カードをパソコンから外します。インターネットに接続されていなければ、データの漏洩はありません。

確認結果は、以下の何れかの画面が表示されます。



(図 - 1 感染なしの場合)



(図 - 2 感染ありの場合)

上記はあくまで簡易的な確認方法です。感染の有無の判断と駆除は専用ウイルス対策ソフトの使用をお願いします

暴露ウイルス等ウイルスの駆除(悪意のあるソフトウェアの削除ツール)

マイクロソフトのホームページより、ウイルス発見駆除ソフトが無料で公開されています。このソフトは毎月定期的に更新されますので、定期的に行えば、仮に暴露ウイルス等ウイルスの感染があっても発見駆除してくれます。

このソフトは手動実行となります。

マイクロソフト(株) 悪意のあるソフトウェアの削除ツール 以下アドレスより無料ダウンロードできます。

<http://www.microsoft.com/japan/security/malwareremove/default.msp>

(株)シマンテック ウイルス発見・駆除ソフト関連

<http://www.symantec.com/ja/jp/index.jsp>

トレンドマイクロ(株) ウイルス発見・駆除ソフト関連

<http://www.trendmicro.co.jp/home/>

「山田オルタナティブ」とは、その前身に「山田ウイルス」というウイルスが存在し、ある掲示板で「友人の山田からのメールを開いたら感染した」と言う書き込みから「山田ウイルス」と名付けられたそうです。また「山田オルタナティブ」は、感染者の殆どが、「XXオルタナティブ」というゲームをダウンロード又は所有していた事からこの名前が付けられたようです。ファイル交換共有ソフトで不正に公開されている映画・音楽・パソコン用ソフト等は著作権法違反にあたり、公開取得しますと罰せられます。

編集後記

情報システムの添田です。発注システムの Moses(モーゼ)導入ではお会いしている方も多いと思います。私の自宅のパソコンの調子がおかしい。。もしかして?と思い、ウイルススキャンを行ってみました。ウイルス感染ではありませんでした。私たちシステムに携わっている者でも「ウイルス感染」には敏感に反応してしまいますね。

最近、紅茶、ハーブティー、中国茶といろんな種類の茶葉を購入し、その日の気分によってお茶を選びリラックスしています。お気に入りのミルクティーを飲んで次の根津システム通信の構想を練りたいと思います。



発行: 根津鋼材 株式会社 住所: 〒116-0014 東京都荒川区東日暮里2-2-3 (TEL)03-3805-5555

メール: hp_master@nezu-g.co.jp ホームページ: <http://www.nezu-g.co.jp/>

発行人: 根津訓光 / 監修 樋口良成 / 編集長

編集: 情報システム事業部

根津鋼材システム通信に掲載された記事の転載はご遠慮願います。

このメールマガジンは、弊社とお取引があり配信依頼がありましたお客様にのみ発行しております。配信中止の場合は、お手数ですが hp_master@nezu-g.co.jp までご一報ください。その際には、御社名、御社(配信先)メールアドレス、御担当者様名を暗記くださいます様よろしくお願ひ致します。