



## ごあいさつ

今回のNEZU システム通信は、

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。

鉄鋼関連情報(社団法人鉄鋼連盟 2011年11月24日発表)

特定の相手へウイルス添付メールを送付する『標的型攻撃』

についてお届け致します。

## 鉄鋼関連情報

下記 URL より社団法人鉄鋼連盟が発表した『鉄鋼需要 2011年11月』の資料を閲覧することが出来ます。(次回公表は12月下旬予定です。)

<http://www.jisf.or.jp/data/jyukyu/documents/jyukyu1111.pdf>

### 特定の相手へウイルス添付メールを送付する『標的型攻撃』

10月末に衆議院のパソコンがウイルス感染したニュースが報じられて間もなく、11月4日には総務省でもウイルス感染が報じられました。この2件は、これまでのウイルス感染事件とは異なる特徴があります。

それは、いずれも『標的型攻撃』を受けていたことです。

#### 何故開いてしまったのか

『標的型攻撃』の特徴として、知人や既知の団体からのメールが来たと思わせる手口があります。衆議院の件では「**お願い事**」という件名のメールでした。総務省の件では

「平成23年(2011年)東北地方太平洋沖地震(東日本大震災)について[略]:緊急災害対策本部発表資料)」という件名のメールでした。**実在する人を装い**、取材の申し込みや資料添付等の**緊急性を煽る件名**で、**反射的にメールを開かせ**感染させるという手口でした。

普段、件名が英語のメールに対しては警戒しますが、自分に関連のありそうな日本語のメールに対しては警戒が緩みがちです。添付ファイルへの警戒も小さくなるため、感染リスクが高くなります。

#### ウイルス対策ソフトも突破

各社のウイルス対策ソフトは、頻繁にウイルス定義ファイルを更新することで新種のウイルスでも検知出来る様な仕組みになっていますが、その更新よりも新しいウイルスは完全な防備が出来ません。今回のウイルスは、まだ名前さえも付いていないウイルスだった様です。それは正に『標的型攻撃』の特徴でもあり、**最新のウイルス定義ファイルを使っても検知されませんでした。**

従来の不特定多数を狙った手口の場合、大勢にウイルスが送り付けられるのでウイルス対策ソフトの会社もその情報を入手し易いのですが、今回の様な標的型の場合、特定少数の場所にものみ送り付けられる為、他



からの異常が発見され難く、定義ファイルの更新もされなかったのです。その結果、添付ファイルを開く際にウイルスと判定されず感染し、被害が広がってしまいました。

## ウイルス感染を防ぐには

少しでも怪しいと思った添付ファイルは開かない。

送信者が取引会社や知人でも添付ファイルやメールを開く前にウイルスチェックを行う。重要なメールの真偽は直接本人に電話で確認する。

銀行やクレジットカードのパスワードの変更要請等の内容の場合、一旦メールを閉じ、ホームページを確認したり電話をかけて確認したりする等、一呼吸置くようにする。また、対策として定期的に暗証番号を変更する。

メールに記載されたインターネットのアドレス(URL)をクリックしない。  
ホームページやメールに、攻撃者に特定されるような個人情報を容易に記入しない。

ウイルス対策ソフトは常に最新の定義ファイルをダウンロードする様に設定する。

OS やソフトウェアのアップデートは常に最新の状態に保つ。



標的型攻撃では、ターゲットを絞り、最新のウイルスで、心理の裏を突いて攻撃をします。攻撃が進化する世の中では、これまで以上にセキュリティ対策への心構えが求められます。これからは企業で徹底したルールを設けることや、一人ひとりの心がけが重要になってくるでしょう。

### 参考 URL

YOMIURI ONLINE サイバー護身術 完全防備、ほぼ不可能な「標的型メール」

[http://www.yomiuri.co.jp/net/security/goshinjyutsu/20111028\\_0YT8T00882.htm](http://www.yomiuri.co.jp/net/security/goshinjyutsu/20111028_0YT8T00882.htm)

@IT 企業を狙う標的型攻撃 その手口と抜本的な対策とは

<http://www.atmarkit.co.jp/fsecurity/rensai/appsec04/appsec01.html>

@IT これが標的型攻撃の実態だ

<http://www.atmarkit.co.jp/fsecurity/column/kawaguchi/034.html>

## 編集後記

こんにちは、情報システム事業部の添田です。暦は小雪、陽射しの暑さも弱く、寒い季節になりましたね。7年前の2004年10月にこのNEZUシステム通信の第1回を配信してから今回の配信で40回目の配信となりました。時にはお客様へご迷惑をお掛けしてしまったこともありましたが、ご丁寧に返信を頂くほとんどのお客様から『いつも勉強をさせてもらっています』『貴重な情報をありがとう』と仰って頂いたり、直接お会いした方には『いつも配信ありがとうございます』と温かいお言葉をかけて頂いたりするので、大変心強い思いをしております。私たちも日々勉強で、いろんな情報を入手し、これからも益々皆様のお役に立てる情報を配信し続けて行きたいと思っておりますのでよろしく申し上げます。



発行：根津鋼材 株式会社

住所：〒116-0014 東京都荒川区東日暮里1-32-5 (TEL)03-3805-5555

メール：[hp\\_master@nezu.g.co.jp](mailto: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

NEZU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](mailto:hp_master@nezu.g.co.jp) までご連絡ください。その際には、御社名、御社（配信先）メールアドレス、担当者様名を明記くださいます様よろしくお願ひ致します。