

# パソコン便利帳 IV

## 1、掲示板をもっと楽しむために

～1、現存する掲示板を楽しく見る方法

～2、簡単なHTML(CPU言語)を活用しよう

## 2、益々巧妙化する詐欺の手口(注意しましょう！)

ランサムウェア、フィッシングメール、悪質サイト

## 3、ネット詐欺の代表的7つの手口

# 1 掲示板をもっと楽しむために

## ～1、現存する掲示板を楽しく見る方法

手間をなるべく防ぐため掲示板を削減しようという動きがありますが現存する掲示板を少しでも楽しく見て活用できる様に解説します。

掲示板は色々な表現が出来る様に工夫されています。

- \* 自己紹介の掲示板：入力補助、タグの利用、携帯で使う、等
- \* Newおしゃべりの部屋：ツリー表示、一覧表示、トピックス表示、記事検索、記事修正・削除、記事検索等
- \* 旧お喋りの部屋：トピック表示、アルバム、留意事項、ワード検索、過去ログ、その他色々
- \* テーマ写真館、楽しい写真掲示板：ワード検索、フォトアルバム、書き込みのアシストタグ
- \* 俳句・川柳の掲示板：一覧表示、ツリー表示、トピック表示、記事検索、記事修正・削除、携帯用URL等
- \* 出欠連絡掲示板：上記と同じ、プラス絵文字表示

## ～2、簡単なHTML(CPU言語)を活用しよう

- \* 文字のサイズ : <font size=5>文字</font> 1～7位まで
- \* 文字の色 : <font color=green>文字</font> #ff00ff でも良い  
上の2つを合わせて両立も可能<font size=5 color=green>
- \* リンクを使う : <a href="http://blog.goo.ne.jp/4syakai">ここ</a>を  
クリック！
- \* 画像挿入 : 
- \* 書いたまま、改行禁止 <pre>自動改行しないように長く表示！ </pre>
- \* 改行する : <br>
- \* 文字などを点滅させる : <blink>文字</blink>
- \* 他にも色々あります、詳しくはここを参照してください  
<a href="http://www.urban.ne.jp/home/kibochan/html.htm">ここ</a>

## 2 益々巧妙化する詐欺の手口

### ～1、ランサムウェア

#### ランサムウェアとは?

ランサムウェアとは、ユーザーの同意なくユーザーのコンピューターに違法にインストールされるマルウェア (悪意のあるソフトウェア) の一種です。ランサムウェアは、犯罪者がユーザーのコンピューターを遠隔地からロックします。次に、「あなたのコンピューターはロックされています、支払いを行うまでアクセスできません」という警告を含んだポップアップ ウィンドウが表示されます。



(ランサムウェアの画面の例。日本人を狙う場合は日本語表示のものが使われる)

# ランサムウェアの対処方法

## パソコンを感染させない



### ■ 不審なメールの添付ファイルやリンクを開かない

一見正常なメールに見えても心当たりのない添付ファイルは開かない、あるいは送信者に確認する。

参考：IPA 独立行政法人情報処理推進機構

[【注意喚起】ランサムウェア感染を狙った攻撃に注意](#)



### ■ パソコンへのウイルス対策ソフト導入や最新パターンファイルの適用

※ただし、パターンファイルに登録されていない新種のウイルスは防げない場合があります。

### ■ WindowsOS搭載製品の場合、WindowsUpdateを実施しOSを最新状態に保つ。

※ WannaCry対策では本対応が重要です。詳細は[こちら](#)

### ■ WEBブラウザ、JavaやFlash等のブラウザプラグインを更新し最新状態に保つ。

## ランサムウェアによるデータの暗号化に備える

### ■ パソコンはこまめにバックアップを取り、そのバックアップファイルにパソコンが直接アクセスできないようにする。

ランサムウェアの被害は、ファイルが暗号化され開けなくなってしまうことです。暗号化されてしまったファイルの復元は困難なことから、重要なファイルについてはいつでも復元できるよう、定期的なバックアップを行うことが対策となります。

参照：IPA 独立行政法人情報処理推進機構 [IPAテクニカルウォッチ「ランサムウェアの脅威と対策」](#)



Back UP

## 2 益々巧妙化する詐欺の手口

### ～2、フィッシングメール

#### フィッシングメールとは？

フィッシングとは英語で「釣る」の意で、メールをきっかけに読み手を騙し、金銭などを巻き上げる。つまり、被害に遭う人や、ウィルスに感染させて乗っ取るパソコンを「魚」に見立て、『メール』という釣り針を使って獲物を獲得することから、『フィッシングメール』という呼び名が付けられました。

獲物(主には金銭)を獲得することが目的であるため、フィッシングメールは、単にウィルスに感染させることだけが目的のものとは違う。ということになります。

オンラインバンキングを乗っ取ることを狙い、銀行になりすまして送られてくるメールなどは、お金という獲物を獲得することを狙っているので、フィッシングメールの代表格と言えます。

### ～3、悪質サイトの種類

**ワンクリック詐欺で高額請求**

**機密情報を搾取するスパイウェア**

**偽サイト誘導で個人情報搾取するサイト**

# 色々な悪質メールの実例～1

## 1、支払い確認

この E-Mail はお客様のお支払い情報とお客様のご注文が処理されることを確認するためのものです。ご注文が完了すると、別送で E-Mail を送信します。

このメッセージの最後に記載されている請求書をご確認ください。何かご不明な点、ご質問等ございましたら、この E-mail に返信して下さい

ご利用ありがとうございます。 添付: エクセル invoice

## 2、本日、添付の請求書を郵送します

お世話になります。大変失礼しました。

本日、添付の請求書を郵送します。 添付: ファイル

## 3、ご注文有難う御座いました お客様のご注文有難う御座いました

注文内容をご確認下さい 添付: エクセルファイル

## 4、お金のヒミツ.net <fukugyou\_qizu@yahoo.co.jp>新時代の究極の副業を開催させていただきます動画4本視聴するだけで、毎月100万円が手に入るチャンス！

⇒ <http://1234.tw/ux-baaabQ> この副業を実践すると、あなたは会社に勤める必要はありません！

毎月安定して、100万円稼げていたら会社に行く必要ないですよ？ そんな究極の副業を、先着100名限定でご紹介します

## 5、注意！！OFFICEのプロダクトキーが不正コピーされています

セキュリティ警告！

お使いになっているオフィスソフトの授權が終了されてしまう可能性があります！日本マイクロソフトセキュリティチームはお使いのオフィスソフトのプロダクトキーが違法コピー

された可能性があることを発見しています。攻撃者はお使いのオフィスソフトのプロダクトキーを利用して他のオフィスソフトを起動しようと

試みています、ご本人の捜査なのか確定できない為、お手数ですが、直ちに検証作業をして下さいますようお願いいたします。

検証作業をしていただけない場合、日本マイクロソフトはお使いのオフィスソフトの授權状態を終了させていただきますのでご了承下さい

「今すぐ認証」

\*ライセンス認証(マイクロソフトプロダクトアクチベーション)とは不正コピーを防止するための技術で、手続きは、短時間に簡単な実行できますまた、

この手続きは匿名で行われるのでお客様の個人情報 は 保護されております。

# 色々な悪質メールの実例～2

## 6、重要書類

お世話になります。昨日お話しした重要書類です。

添付ファイル:6W03553043. Xls

## 7、口座振替払い

御依頼の登記が完了しましたので、お手数ですが、費用のお振り込みをお願いします。

よろしく申し上げます。 添付ファイル:サービス請求書. xls

\*\*\*\*\*

(東京法律事務所内)

電 話:03-3355-0941

FAX:03-3357-1072

※2016年6月9日から事務所住所が変わりました。

\*\*\*\*\*

## 8、宿泊予約確認

この度お客様の予約を確認しました、添付資料ご確認下さい

添付ファイル:エクセル

## 9、写真送付しました

先日の写真ですファイルになっているのでご覧ください

添付ファイル:ファイ



# 3、ネット詐欺の代表的7つの手口

## ～1、オンライン銀行口座の不正送金(フィッシング詐欺)

最近出てきたインターネットバンキングを狙った新しい手口の一つ。

高度な技術が利用されており、被害が出るまで見破るのが難しい手口です。

## ～2、アダルトサイト詐欺(ワンクリック詐欺)

現在もっとも多い手口の一つです。ワンクリック詐欺、不当請求詐欺とも言われます

## ～3、偽ブランド品詐欺、偽販売サイト詐欺

インターネットサイトで購入したブランド品が偽物であったり、商品を送ってこない。

クレジットカード情報を盗まれるなど、数多くの被害が報告されている詐欺です。

## ～4、偽セキュリティソフト詐欺

ウェブサイトにアクセスした際に、「このPCはウイルスに感染している」などといった注意を促し、

全く効果のないセキュリティソフトをインストールさせる手法です。

## ～5、ウェブサイト改ざんウイルス被害

ウェブサイトを改ざんして、閲覧者をウイルスに感染させる手法です。「ガンプラー」などが有名。

## ～6、Facebookアカウント乗っ取り

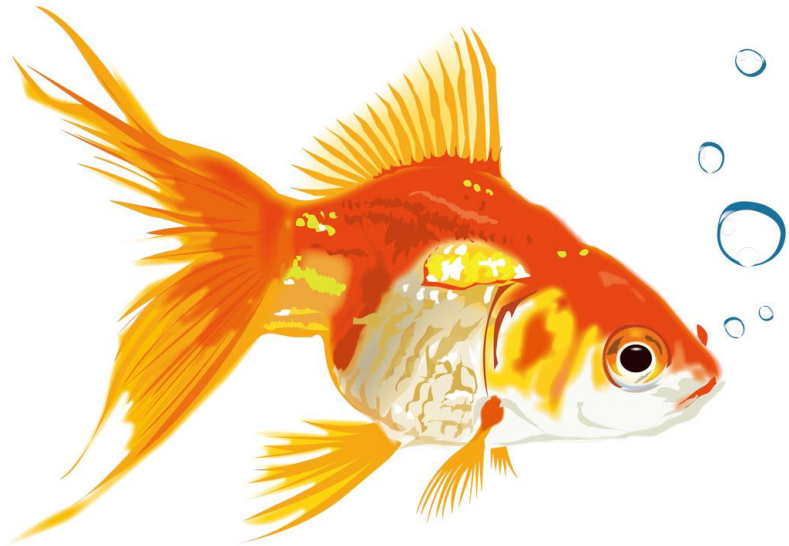
アカウントを乗っ取るために友達申請の仕組みを利用して行う詐欺行為。

## ～7、Twitter詐欺、アカウント乗っ取り

ダイレクトメッセージ(DM)にフィッシング詐欺のURLを送付したり、スパムメールの文言を送りつける迷惑行為です。

以上で説明はおわりです

ご清聴を感謝いたします



2017年7月31日

吉岡伴明