MYStaffからのお知らせ

2015年6月5日
MYStaff清瀬
（有限会社マイスタッフ）


清瀬市内の風景

平素はMYStaff をご利用頂きありがとうございます。

各地で夏日を記録している5月を終え、梅雨時の6月に入りましたが、
皆様いかがお過ごしでしょうか？

話題の Windows 10 がいよいよ 2015年07月29日にリリースされる事が、
Microsoft から発表になりました。

また日本年金機構の個人情報流出事件が大々的に報道されております。

早速弊社ユーザー様からお問合せを頂きましたので、
3ヶ月ぶりに「MYStaffからのお知らせ」を作成させて頂く事としました。

皆様のご参考となれば幸いです。

Windows 7 と Windows 8.1 から Windows 10 へのアップグレードについて

Windows 8.1 の後継となる Windows 10 が、2015年07月29日にリリースされることがMicrosoft のホームページにおいて発表されました。
Windows 10 には新しいインターネットブラウザをはじめ、多くの新機能が搭載されています。
また操作性について、Windows 7 と Windows 8 の良い点を統合されており、現在 Windows 7 と Windows 8.1 のどちらをご利用されている方でも容易に移行できる様設計されております。

Windows 10 の機能の詳細につきましては、Microsoft ホーム―ページ内の次のURLをご覧ください。

http://www.microsoft.com/ja-jp/windows/

ここでは、現在ご利用中 Windows 7 と Windows 8.1 の Windows 10 へのアップグレードについて記載させて頂きます。

**なお一部のWebサイト、周辺機器およびソフトウェアは、Windows 10 に対応していない場合があります。
また操作性についても Windows 7 や Windows 8.1 と異なる部分がありますので、
Windows 10 へのアップグレード前に十分な確認と検討を行う必要があります。**

期間限定の無償アップグレードについて

Microsoft では、現在 Windows 7 と Windows 8.1 をご利用の方に、Windows 10 に無償でアップグレードできるサービスを期間限定で実施すると発表しております。
期間については現在の発表では、Windows 10 リリース後1年間となっております。

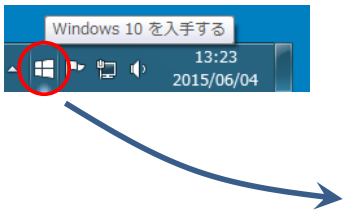
ただし次の製品は無償アップグレード対象外となっております。

Windows 7 Enterprise	Windows 8 Enterprise	Windows 8.1 Enterprise
Windows RT	Windows RT 8.1	Windows Phone（通信事業者により異なります）

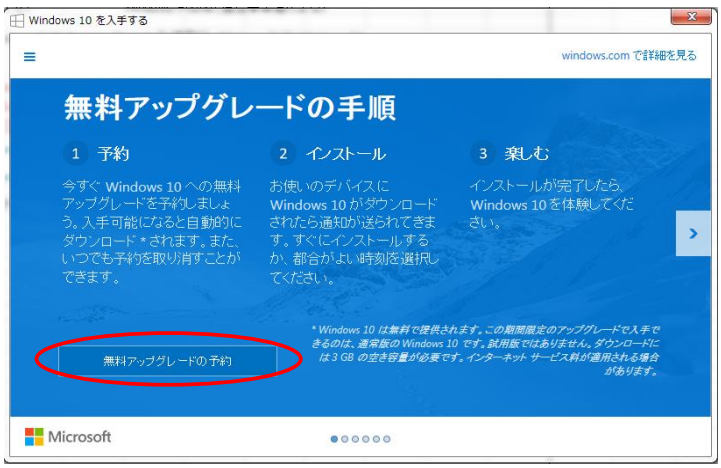
また Windows 10 へのアップグレードには、事前に Windows 7 は Service Pack 1 の適用が、Windows 8 は Windows 8.1 へのアップグレードが必要となります。

無償アップグレードの方法

Windows Update が適切に実行されている場合、無償アップグレードの対象となる Windows では、インジケーター領域に次のようなアイコンが表示されます。



このアイコンをクリックすると右のような「Windows 10 を入手する」という画面が表示されます。



「無料アップグレードの予約」をクリックして、表示される手順に従って、
無料アップグレードの予約を行います。

これで Windows 10 がリリースされると、
自動的にアップグレードが実行されます。

怪しいメールの見分け方について

2015年05月末から06月に掛けて、日本年金機構の個人情報流出事件が大々的に報道されております。
今回のケースは、年金情報を閲覧可能なパソコンがウィルスに感染し、外部からの遠隔操作により情報が流出したもので、
ウィルのへの感染経路は電子メールの添付ファイルからと報道されております。

今回のケースでは巧妙な偽装が行われており、セキュリティ対策ソフトウェアも通過しているようなので、
最新の注意を払わなければウィルスメールである事を見破る事は困難であったと思われます。

セキュリティ対策ソフトウェアを通過してしまった場合、はたしてどのようにウィルスメールである事を見破ればいいのか？
ここではウィルスメールを見破る方法の一例をご紹介します。
「怪しい！」と思ったら、安易に開かずに以下の操作ができる方に確認をお願いするというのも一案かと思います。

怪しいメールのチェックポイント

今回のようなケースに該当するウィルスメールには概ね次の3種類があります。

(1) 埋め込み型
　メール自体にウィルスとなるコードを埋め込んで送られて来るもの。
(2) 添付ファイル型
　メールの添付ファイルにウィルスとなるコードを埋め込んで送られて来るもの。
(3) 外部リンク型
　メール自体にはウィルスとなるコードは無く、リンクだけが記載されており、リンクを開かせてウィルスに感染させるもの。

「(1)埋め込み型」と「(2)添付ファイル型」については、概ねウィルス対策ソフトウェアで駆除が出来ますが、
「(3)外部リンク型」については、ウィルス対策ソフトウェアで駆除できない場合があり、最近被害が多く報告されております。
ここでは「(3)外部リンク型」を例として記載させて頂きます。

残念ながら今回の事件ほど巧妙なサンプルではなく、目的もウィルス感染させるものではなくIDとパスワードを盗むタイプのものですが、
「(1)埋め込み型」や「(2)添付ファイル型」にも応用できますので対策手法の参考になれば幸いです。

メールを開いた時点で簡単に見破れるのポイントを記載しておきます。

記載したポイントの内①の書体、③の自分が登録したメールアドレスおよび⑤の電子署名でこのメールが偽装メールである事は見分けられます。
もしここがもっともらしく偽装されていた場合は、②の送信者のメールアドレスと④のリンク先URLがあたかもセブン銀行さんのように偽装されていますので、誤ってリンク先URLを開いてしまう可能性があります。

メールアドレス偽装は、メールソフトウェアによっては簡単に偽装できます。
リンク先URLの偽装も容易で、メール本文中をはじめ、PDFファイル等の添付ファイルで可能ですので注意して下さい。
例として、パソコンでこの文書をご覧になっている場合、次のGoogleのURLをクリックすると弊社のホームページが表示されます。

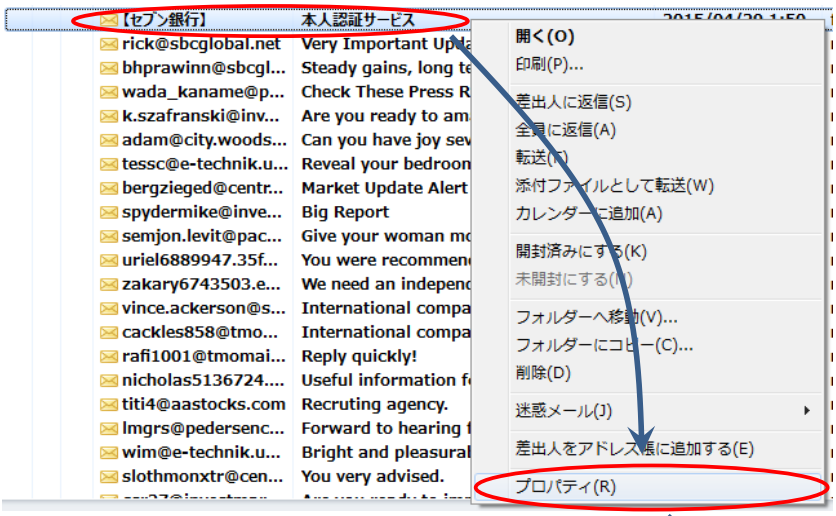
http://www.google.co.jp/

PDFを開くソフトウェアに依っては確認メッセージが表示されるものもありますが、そのまま開いてしまう場合もあります。

メッセージのソースを確認する方法

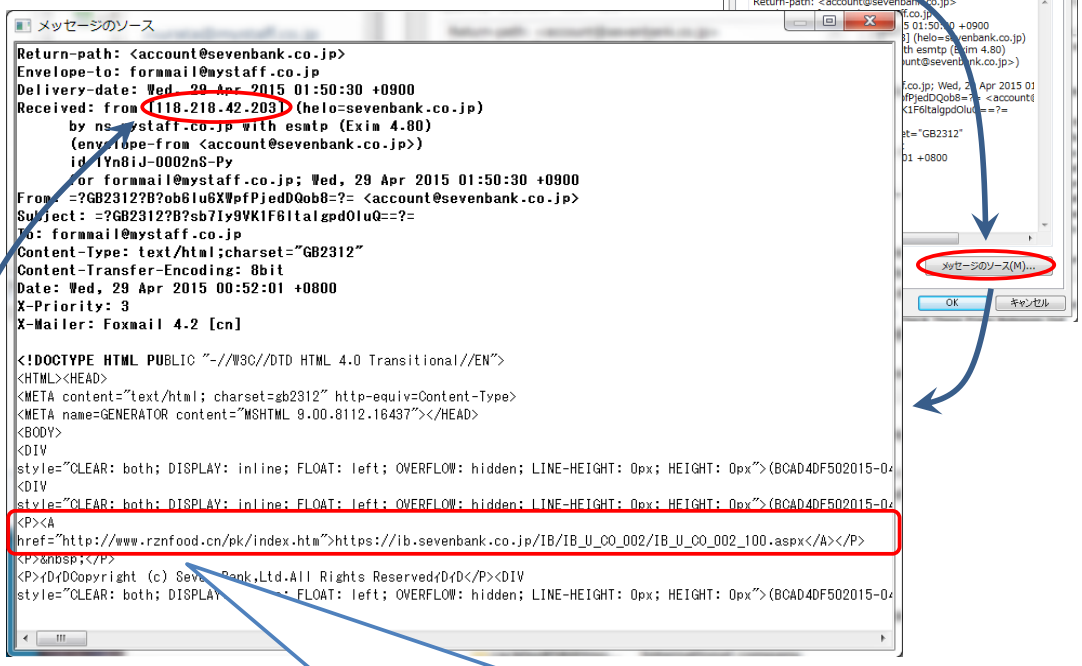
偽装を見破る方法としてメールメッセージのソースを確認する方法があります。
ちょっと難しい操作と思われるかもしれませんが、この操作によってパソコンやデータが壊れることはありません。

(1) メール一覧で対象のメールにマウスカーソルを合せて右クリックして、メニューから「プロパティ(R)」をクリックします。



(2) 「詳細」タブをクリックして「メッセージソース(M)」をクリックします。

(3) 以下のようなメッセージソースが開きますので、チェックポイントを記載します。



①表示は「https://ib.sevenbank.co.jp/IB/IB_U_CO_002/IB_U_CO_002_100.aspx」になっていますが、
実際のリンク先は「http://www.rznfood.cn/pk/index.htm」です。

②このIPアドレスは韓国で利用されているもので、
セブン銀行さんが韓国からメールを発信するとは考えられません。

①の判定についてはHTMLの知識が若干必要になります。
この例では「<A href="(URL1)">(URL2)</A>」の文で、(URL1)と(URL2)が異なる事から偽装と判断できます。
②の判定についてはインターネットの知識が若干必要になります。
この例では「118.218.42.203」を「APNIC WHOIS」(アジアのIPアドレスを管理している組織のIP検索機能)で検索すると、
「118.216.0.0～118.223.255.255」のIPアドレスは韓国の「Hanaro Telecom」で利用している事が判明しました。

セキュリティチェックポイント

前回（2015年03月06日版）の「MYStaffからのお知らせ」にも掲載させて頂いた内容に若干追加させて頂きましたが、
今一度次の注意事項徹底をお願いします。

(1) パソコンを長時間使用してないときは必ず電源を切る。
　電源の入っていないパソコンを遠隔操作される事はありません。
　ただし「LAN Wake Up（LAN経由起動）」の設定を行っている場合はこの限りではありません。
(2) 必ずセキュリティ対策ソフトウェアを利用し、更新機能を利用して最新の状態にする。
　必ずウィルス対策とファイアーウォールを有効にして下さい。
(3) 必ず Windows Update を実施し、Windowsを最新の状態にする。
(4) 怪しいと思われるサイトはできる限り閲覧しない。
　キーワードは「無料」です。「無料動画閲覧」「無料ダウンロード」には十分注意して下さい。
(5) 無料のソフトウェアをダウンロードする場合は注意書きを良く読む。
　必ず「余分なソフトウェアをダウンロードしないか？」、「パソコンのデータが送られる事はないか？」等の確認をして下さい。
(6) 送信者に心当たりのないメールは開かない。
(7) 送信者が明確でないメールの添付ファイルは開かない。
(8) 送信者が明確でないメール内に記載されているURLは絶対クリックしない。
　「配信停止依頼」を装った誘導もありますので注意して下さい。
(9) システムメンテナンス等の名目でパスワード入力を求めて来る場合は、安易に入力しないで電話等で真意を確認する。
　振込、情報変更等をこちらから依頼をしていないのに、銀行やショッピングサイトがパスワード入力を求めて来ることはありません。
(10) 銀行サイト、ショッピングサイトでID、パスワード、クレジットカード情報を入力する場合はURLを確認してから行う。

便乗商法や便乗詐欺に注意して下さい！

早速「流出したあなたの個人情報が、ショッピングサイトのデータベースに載ってしまったので削除業者を紹介します。」
という電話が消費者センターを名乗るものから架かって来たという、便乗詐欺の報道がありました。

もしこのような電話が架かって来た場合は、

　「必要ありません！」

とキッパリ断って下さい。

「それでは気が済まない！」と言う方は、

　「ここでは電話できないのでこちらから折り返しかけなおします。」

と言って、組織名、電話番号および担当者名を聞き出し、警察の方に相談するのも一案です。

これから予想されるのは「セキュリティを万全にする為、ファイアーウォールの導入をお奨めします！」と言う便乗商法です。

ファイアーウォールはセキュリティ対策には有効な装置ですが、詳細な管理を行わないと有効に機能しません。
またファイアウォールで先に記載させて頂いた「外部リンク型」のウィルスメールに完全に対応しようとすると、
ほぼ常駐に近い専属の技術者やある程度の知識を有する管理者が必要になります。

最後に前回（2015年03月06日版）の繰り返しとなってしまいますが、電話セールへの対応についての注意を記載させて頂きます。

多くの電話セールスは、テレアポ代行業者が行っている場合があります。
テレアポ代行業者電話先の情報を独自のデータベースで管理しており、興味深い対応をすると「電話効果あり」として、
データベースに登録されます。
このデータベースを利用して他の商品についても電話セールスを行ってきます。

電話セールスで一度興味深い対応をすると、いろんな電話セールスが架かってくると言うケースをお聞きする事があります。

逆に「キッパリ断り続けると、電話セールスの件数が減ってくる。」とのお話をお聞きする事もあります。

興味がある場合でも電話セールスではなく、該当する商品のホームページやその会社に直接電話して確認する方が安全です。

おわりに・・・

Windows 10 リリース開始日決定や、
日本年金機構の個人情報流出問題を機に、
お客さ様からのお問合せを何件か頂きましたので、
「MYStaffからのお知らせ」第２弾を作成させて頂きました。

今回からはメールでの配信も実施させて頂きます。

各地で梅雨入りの発表も聞かれるようになりました。

気温の定まらない不安定な天気の日が続いておりますが、
皆様お体に気を付けてお過ごしください。

なお今後このような資料の送付がご不用でしたら
ご一報頂けれ送付を打ち切らせて頂きます。

ご不明な点がありましたら、お気軽にお問合せ下さい。

【作成者】
MYStaff清瀬（有限会社マイスタッフ）
〒204-0003
東京都清瀬市中里6-54-7ﾗﾋﾞｵﾝ協和4-F
Tel 042-493-5871 Fax 042-493-5872
e-mail : front@mystaff.jp
http://mystaff.jp/　http://mystaff.info/