Topic

平成 26 年 9 月 25 日

金融機関等のフィッシングサイトの増加について（第2報）

金融機関等のフィッシングサイトが9月下旬から再び増加しています。

1　金融機関等のフィッシングサイトの増加

警察庁では、平成 26 年6月 30 日に金融機関等のフィッシングサイト増加について、注意喚起[i]を実施しましたが、9月下旬以降、金融機関等のフィッシングサイトの増加を再び観測しています。下の図は、警察庁で観測した日本国内の金融機関等のフィッシングサイトの件数を表したものです。

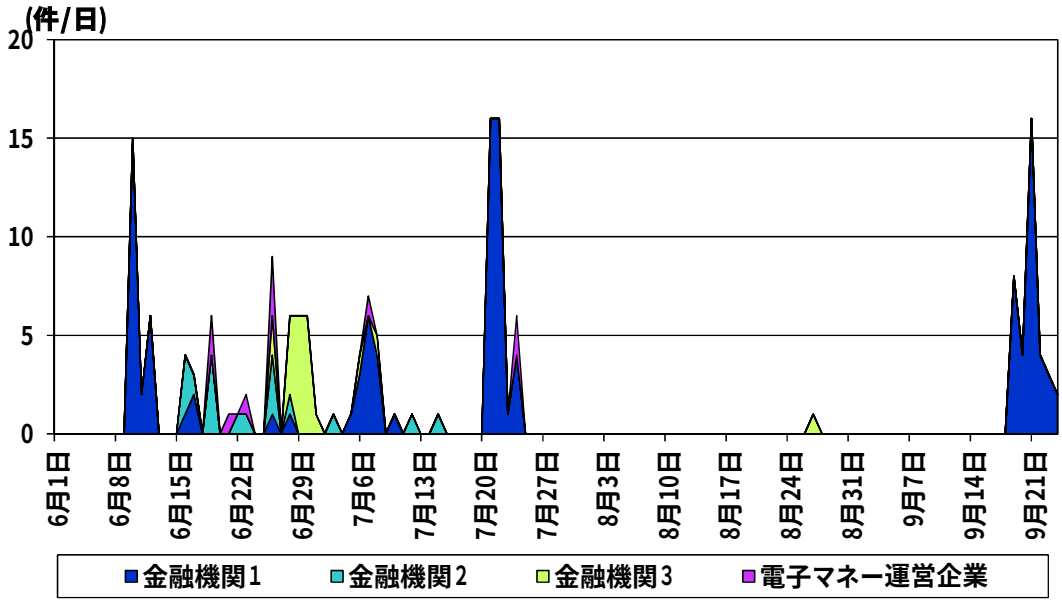

図　金融機関等のフィッシングサイトの観測状況（6月1日～9月24日）

金融機関のフィッシングサイトの観測状況は、7 月下旬に観測されて以来、ほとんど観測されていませんでしたが、9月下旬以降、再び観測しています。

フィッシングサイトは、減少と増加を繰り返していることから、オンラインバンキング等を利用する場合には、常に注意を払う必要があります。

[i] 「金融機関等のフィッシングサイトの増加について」（平成 26 年 6 月 30 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20140630.pdf

2 フィッシング被害に遭わないための対策について（前回の再掲）

フィッシングサイトへの誘導は、主に電子メールによって行われることから以下のような対策が考えられます。

- 正規のサイト管理者が電子メールで口座番号や暗証番号の入力を促すことは無いことから、そのような電子メール内のリンク先は安易にクリックしない。
- 認証を必要とするサイトには、正規の URL を直接入力するなどして、表示されているメニューから操作する。

閲覧しているサイトが正規のものであることを確認するためには、以下の項目全てを確認して下さい。

- ブラウザに表示されている URL が正規のものであるか確認する。
- 個人情報等を入力する場合は、サイトが SSL/TLS（URL が「https」から始まっています。）により、暗号化されていることを確認する。
- サイトの証明書を表示し、証明書の発行先が金融機関等の正規のサイト管理者であることを確認する。

また、正規のサイトであっても、ウィルスに感染したパソコンで閲覧すると、ログイン情報を窃取されたり、不正送金が行われたりする場合もあるので、以下のような基本的なセキュリティ対策も重要です。

- ウィルス対策ソフトをインストールし、パターンファイルを最新のものにしておく。
- OS やソフトウェアのセキュリティ修正プログラムを適用しておく。
- インターネット上のファイルやメールの添付ファイルで不審なものは実行しない。