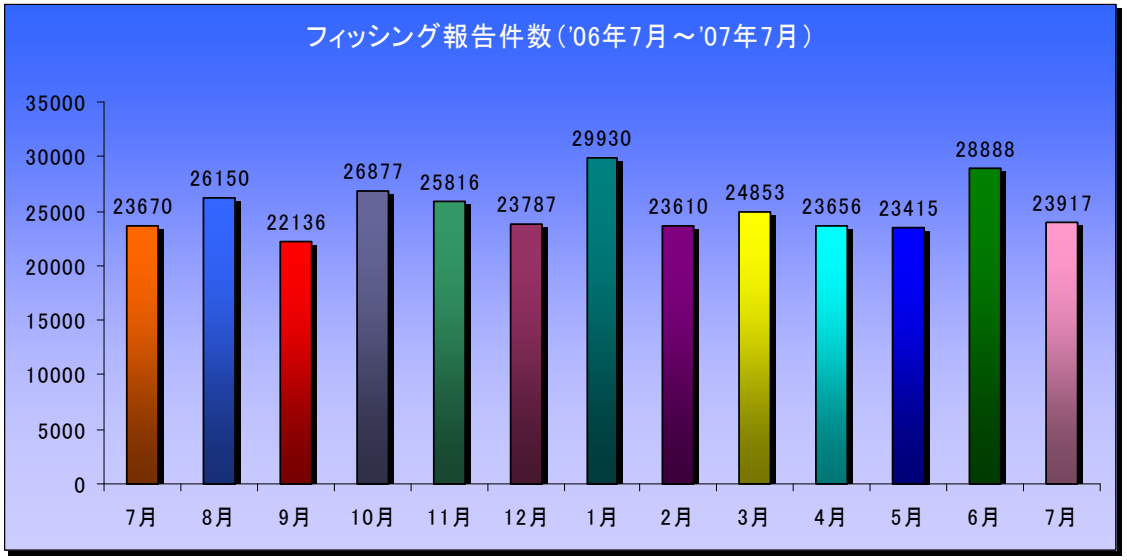
フィッシング対策協議会４半期レポート
2007 年 7-9 月期

2007 年 7-9 月期におけるフィッシングに関する動向やフィッシング対策協議会の活動を報告します。

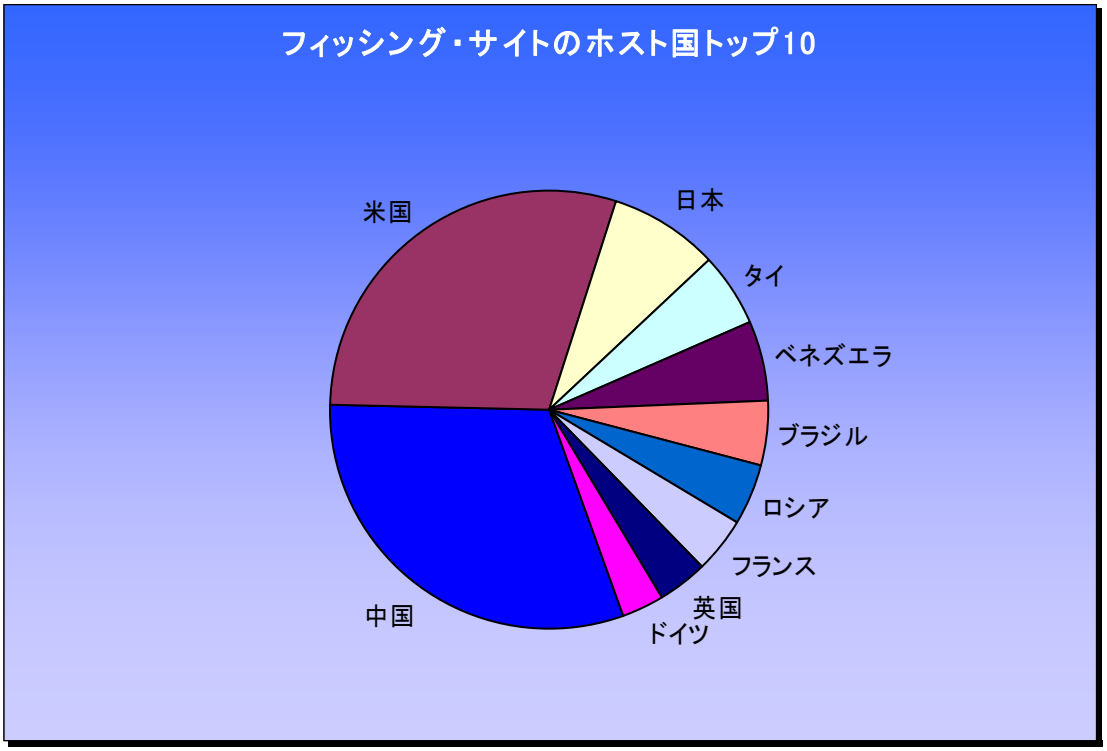
１．海外のフィッシング状況

APWG Phishing Activity Trends Report 2007 年 7 月によれば、7 月期のフィッシングに関する報告件数　23,917 件となっており、金融サービスが引き続き最も標的となった産業分野となり、全攻撃の 94.4%を占めることになりました。APWG 会長の David Jevans は、「2007 年 7 月は上位の銀行の標的に攻撃が集中しました。主要な標的のおよそ半分はヨーロッパの金融機関である」とし、「IRS および英国の税務当局の名を騙ったフィッシングが行われていることを引き続き確認している。ヨーロッパおよび日本における国際的なフィッシングに関する報告が増加しているよだ。また、非常に多くの米国の信用組合および小規模銀行に対する低レベルの攻撃が続いている。」と述べています。



フィッシング行為報告件数（月単位／2006 年 7 月～2007 年 7 月）

フィッシング・サイトのホストとなった国を見ると、2007 年 7 月期は、中国がアメリカを上回り、23.74%でフィッシング用サイトのホスト国のトップとなりました。中国がアメリカを上回ってフィッシング用サイトのホスト国のトップとなったのはこの 7 月期が初めてです。

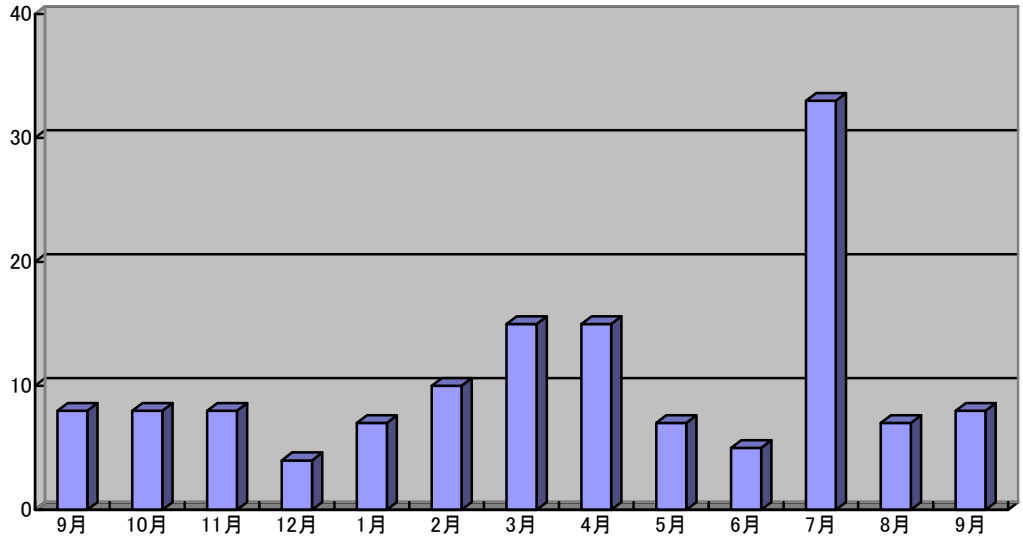


フィッシング・サイトのホスト国（2007 年 7 月）,APWG

２．国内のフィッシング状況

6-9 月においては、日本の銀行のブランドを語るフィッシング事象が発生しました。７月に新生銀行をかたるフィッシング事例が２波にわたり発生しました。いずれも英語の e-mail によって、英語版のログイン画面を真似たサイトで口座番号や暗証番号を搾取しようとするものでした。このフィッシングメールは本協議会関係者や報道機関係部門も直接受信するほど、数多くの発信が行われたものと想定されます。ほぼ同時期に複数種類の URL が用いられ、サイトはアメリカ、イギリス、トルコなど複数の国に置かれていました。このように同時期に複数の URL やサイトを用意する手口は欧米では以前より行われており、日本の企業ブランドを使ったものとしては、今回がフィッシング対策協議会で観測している限り初めてものと考えられます。新生銀行のかたるフィッシングの第２派では、英語で複数 URL が用いられる点は同様ですが、新たに乱数表を表す画面が追加され、そこに加入者が持つ乱数表（セキュリティカード）の値を全て入力させようとするものとなりました。

９月にはインターネット専業銀行「イーバンク銀行」をかたるフィッシングに関する事象が認められました。日本の金融機関を標的にした日本語によるフィッシングということで、その影響の大きさが懸念されます。この一連の攻撃は 8 月の中旬から始まっており、偽サイトが閉鎖される度に新しいサイトが立ち上げられ、繰り返し攻撃が行われた模様です。



フィッシングサイトの件数（2006年9月～2007年9月）

３．活動状況

（１）APWG 会議参加報告書に公開（９月末）

2007 年５月 30 日－31 日に行われた APWG 主催の The 2007 Counter-eCrime Operations Summit への参加報告をホームページにて公開いたしました。会議後、現地においてセキュリティに取り組む企業への訪問インタビューを行いその内容も同報告書に記載しました。

（２）リーフレット配布

フィッシング啓発リーフレット配布についてホームページを通じて希望募集開始しました。

情報セキュリティ関係の教育・研修会やイベント等の配布に利用可能であり、無料でご提供しております。

詳しくは「啓発リーフレットの無料提供について」を参照ください。

４．スタッフより　　～フィッシング事象を発見したら

フィッシング対策協議会ではフィッシング事象の情報提供を募集しています。　フィッシングの e-mail を受信したり、フィッシング事象の発生を顧客等から連絡を受ける等で認知した場合、フィッシング対策協議会にそれら情報を提供ください。

提供いただいた情報を元に、分析整理するとともに事例情報として公開することにより注意喚起や啓発等に活用させていただきます。

フィッシング事象を発見したら
info@antiphishing.jp 宛にフィッシングの e-mail やその内容を送付（転送）してください。

この案内は、フィッシング対策協議会のトップページから、左の灰色のフレーム内（MAIN MENU）の下の方にある『フィッシングメールを受け取ったら』をクリックすることにより参照いただけます。

以上