月次報告書（2007年7月分）

フィッシング情報届出状況

2007 年 8 月 20 日

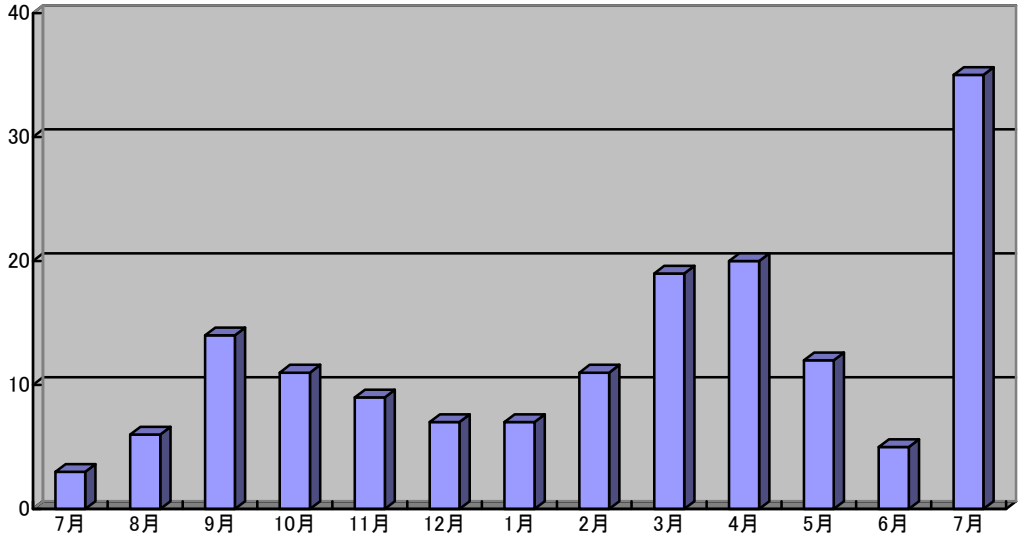
目次

1. フィッシング情報届出状況

1.1. フィッシング情報届出状況

・ **フィッシング情報の届出件数**： 35 件

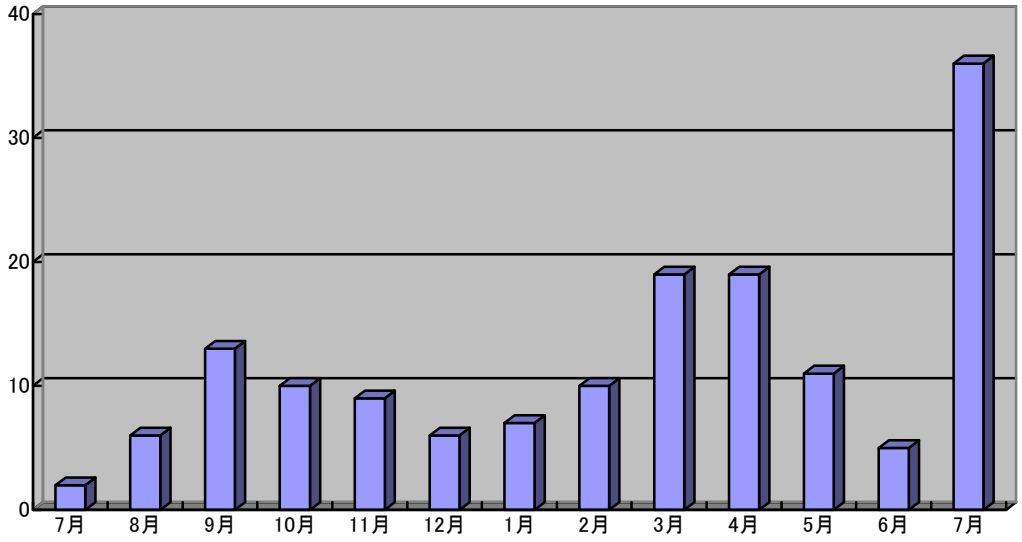
2007 年 7 月度に報告されたフィッシング情報は、前月度よりも大幅に増加して、過去 2 番目に多い 35 件となりました。



フィッシング情報の届出件数（2006年7月～2007年7月）

・ **フィッシングメールの件数**： 36 件

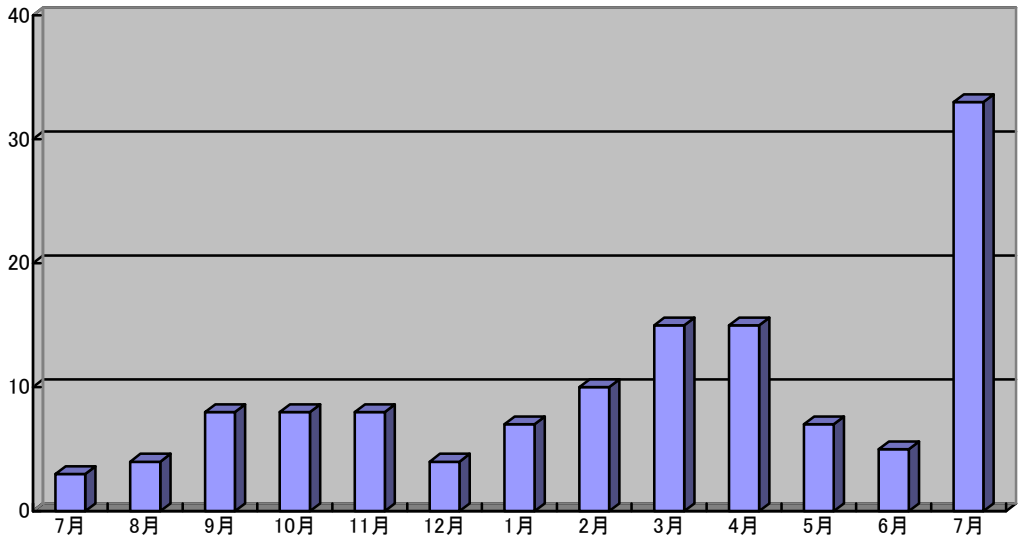
2007 年 7 月度に報告されたフィッシングメールは、前月度よりも大幅に増加して、過去 2 番目に多い 36 件となりました。



フィッシングメールの件数（2006年7月～2007年7月）

・ **フィッシングサイトの件数**： 33 件

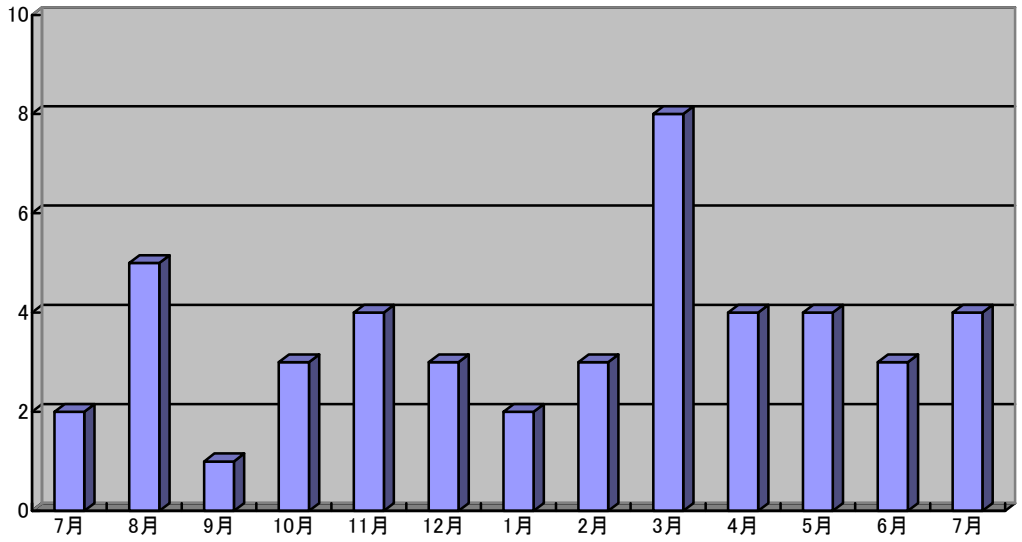
2007 年 7 月度に報告されたフィッシングサイトは、前月度よりも大幅に増加して、過去最多の 33 件となりました。



フィッシングサイトの件数（2006年7月～2007年7月）

・ **フィッシングによりブランド名を悪用された企業の件数**： 4 件

2007 年 7 月度にブランド名を悪用された企業の件数は、前月度より 1 件多い 4 件でした。

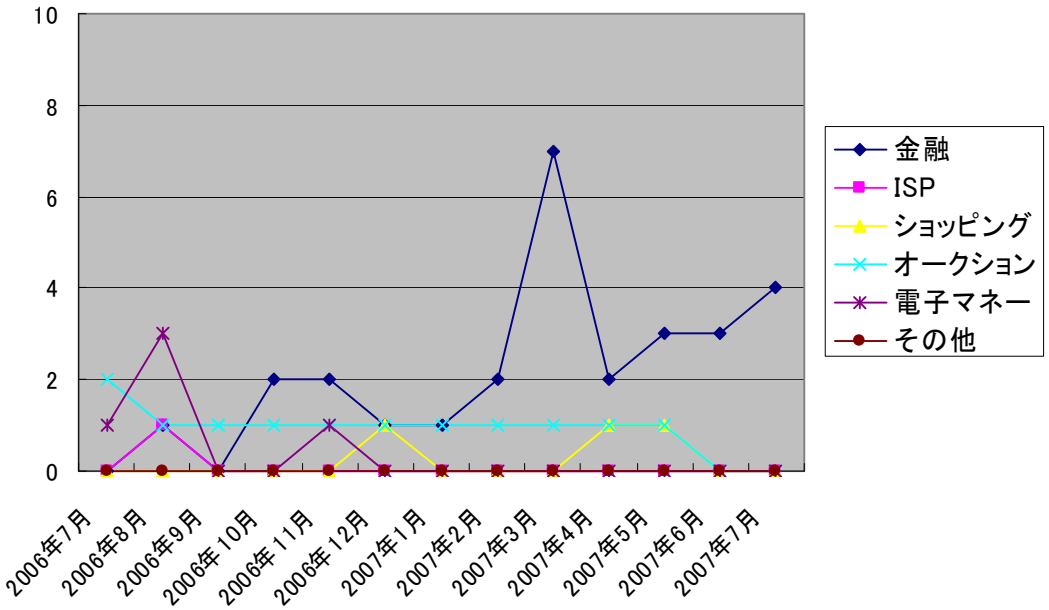


フィッシングによりブランド名を悪用された企業の件数（2006年7月～2007年7月）

・ **もっともフィッシングに利用されるWEBサイトが多かった国**： アメリカ（21 件）

1.2.　業種別の状況

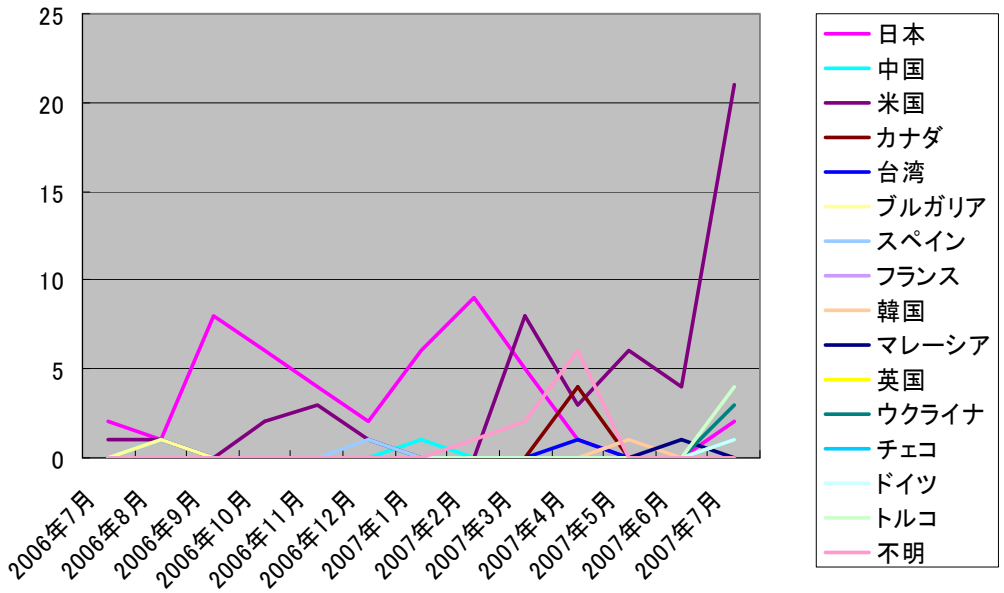
2007 年 7 月度に標的となった業種は、金融関係が 4 件でした。



業種別の状況（2006年7月～2007年7月）

1.3. フィッシングサイトのホスト国

2007 年 7 月度に報告されたフィッシングサイトは、アメリカで 21 件、トルコで 4 件、ウクライナで 3 件、日本で 2 件、イギリス、チェコ、ドイツでそれぞれ 1 件ホスティングされていました。



フィッシングサイトのホスト国(2006年7月～2007年7月)

1.4. フィッシングメールの動向

7 月度には、新生銀行をかたるフィッシングメールに関する報告が非常に多数寄せられ、25 通のフィッシングメールが確認されました。フィッシングメールは、2 回の異なる時期に発生し、1 度目は 11 日から 12 日にかけて、2 度目は 24 日から 25 日にかけて大量送信されました。メールは英語で記載され、「口座情報の確認ができないため、サイトを訪れて情報の更新を行って欲しい」として偽サイトに誘導しようとします。フィッシングメールの件名は「Lock your Shinsei Bank Online Access!」、「Illegaly accessed by 3rd party」、「Suspend your account!」などで、差出人は「no_reply@shinseibank.co.jp」、「security@shinseibank.co.jp」、「support@shinseibank.co.jp」を詐称しています。HTML 形式で作成され、本文には「https://direct03.shinseibank.co.jp/」から始まる URL が記載されていますが、クリックすると本物とは全く異なる URL のサイトに誘導されるようになっています。

その他、日本語のキャッシング融資メールも引き続き確認されており、9 通のメールに関する

報告がありました。

1.5. フィッシングサイトの動向

7 月度は、新生銀行のフィッシングサイトに関する報告が多数寄せられました。上記のフィッシングメールが大量送信されたのに合わせて、非常に多くのサイトが登場し、21 のサイトが確認されました。フィッシングサイトは、同行のロゴマークを使って「新生パワーダイレクト」の英語のログインサイトを模倣したもので、口座番号や暗証番号の入力を促します。ドメイン名は新生銀行のものとは全く異なり、SSL も使用されていません。1 回目に確認された 10 のサイトのアドレスはどれも、「http://（任意のドメイン）/b7e/LiveConnect.htm」というもので、アメリカ、イギリス、トルコ、ウクライナ、チェコでホスティングされていました。2 度目のメール発生時に登場したフィッシングサイトは、1 回目とは手口が若干異なり、口座番号、暗証番号、パワーダイレクトのパスワードを入力してログインした後に、「セキュリティ・カード」の内容の入力を促す画面を表示して、乱数表の全文字を入力させようとします。アドレスはいずれも、「http://（任意のドメイン）/shinseybank.com.jp/login.html」で、こちらは 11 件のサイトが確認され、米国もしくはドイツのサーバーにホスティングされていました。

その他、キャッシング融資サイトが 10 件、「PayPal」、「North Fork Bank」を騙るサイトがそれぞれ 1 件確認されました。

1.6. フィッシング関連の不正プログラム情報

特にありません。

1.7. その他の動向

特にありません。

1.8. 総括

日本の金融機関を標的にした大規模なフィッシングはここ最近確認されていませんでしたが、今月度は新生銀行をかたるフィッシングが発生しました。それにより、今月度のフィッシング情報届出数は大幅に増加して過去 2 番目に多い 35 件となり、新生銀行に関するものはそのうち 24

件を占めました。

今回の新生銀行をかたるフィッシングは、手口が洗練されており、大々的に行われました。サイトは巧妙に作られ、メールに合わせて一度に多くのサイトを出現させているあたり用意も周到で、2回目には同行がセキュリティ対策として導入している乱数表の情報まで盗み取ろうとするなど非常に危険度の高いものでした。今回は英語によるものでしたが、もし日本語が使われていたとしたら、国内の利用者への影響はさらに大きかったものであると思われます。すでに2回続けてフィッシングが起きています。今後も同様の事例が発生する可能性があり、引き続き注意が必要です。

今回英語が使われたことや、URLに「shinseybank.com.jp」という表記が見られること、また手口の巧妙さなどから、外国の犯罪組織による犯行の可能性も考えられます。もし彼らが日本の金融機関をターゲットにし始めたとすると、今後他の日本の金融機関が狙われる可能性もあります。