特集　サイバー攻撃防衛のための取り組み

インターネット・バンキングへの攻撃手口と考えられる対応策

一般社団法人 全国銀行協会
企画部次長　大坂　元一

1．インターネット・バンキングとは

インターネット・バンキング（以下、ネットバンキング）は、文字どおりインターネットを経由して、銀行預金の残高照会や取引明細の確認、振込などの取引をすることができるサービスです。銀行によっては、法人のお客さま向けに、海外送金や売掛金の消し込みサービスなどを提供しているところもあります。

従来は、銀行の窓口や最寄りのATMに行かなければできなかったこれらの取引も、ネットバンキングによってご自宅や勤務先のパソコンやスマートフォンなどから、時間や場所を気にせずに行えるようになっています。日中は働いていたり、育児や介護をしていたりして、銀行の窓口が開いている時間帯に十分な時間を取ることが難しい人には、とても便利なサービスです。

ネットバンキングの契約口座数は、6,580万口座を超えているとされており[1]、わが国で一定程度定着したサービス、社会的なインフラということができそうです。

2．ネットバンキングにおける不正利用被害

一方、こうした利便性の向上・利用者数の増加に比例するように、近年、ネットバンキングの不正利用被害が急増しています。

全国銀行協会の調べによりますと、平成25年度には、１年間で約14億３千万円強の被害が発生しました。平成26年度も上半期の６か月間だけで約10億４千万円弱の被害が発生しており、不正利用の被害が増加し続けています（図１）。

平成24年度以前は、多くても１年間で２億円強程度の被害であったことに照らせば、平成25年度以降の被害急増は際立っています。

ネットバンキングは、インターネットを経由して銀行取引に関する情報をやり取りすることから、「なりすまし」[1]や、「送金情報の改ざん」等の手口による犯罪が生じる可能性があります。そして、そのような不正利用の手口は、日々高度化・巧妙化しています。

もちろん、銀行では様々な対策を講じていますが、便利なネットバンキングをより安全に・安心して利用するためには、利用者も犯罪の手口を知り、それを踏まえた対策を講じておくことが重要です。

3．ネットバンキングにおける不正利用の手口

ネットバンキングの不正利用手口は、犯人側が以下のような方法でログイン時や取引時の認証に

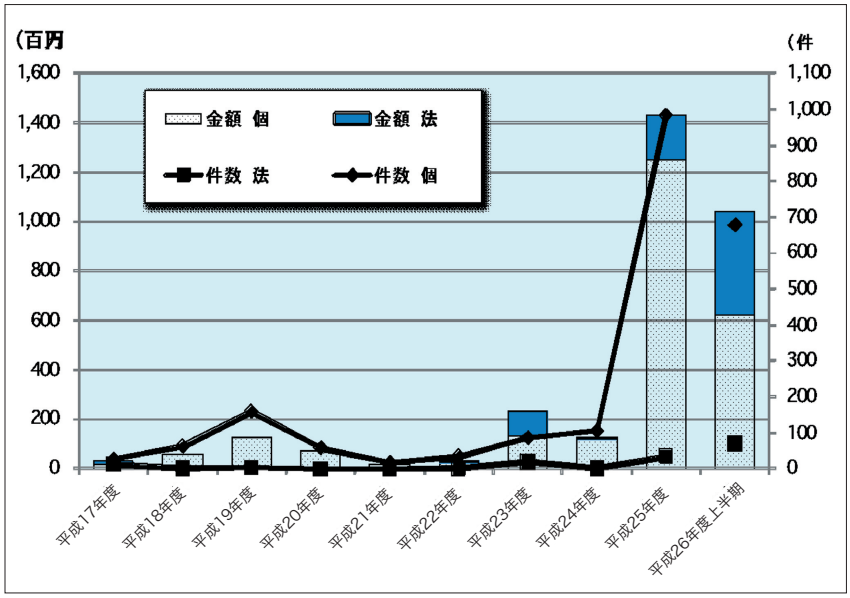

図１　ネットバンキングによる預金等の不正払戻し件数・金額

必要な情報[2]（パスワード等）を盗取し、利用者（預金者）本人に「なりすまし」して不正に取引を行うというものです。

（1）フィッシング詐欺

犯人側は、銀行を騙る偽の電子メールを不特定多数のメールアドレスに送信し、その銀行の利用者を偽の銀行サイトに誘導。ＩＤやパスワード、乱数表などの認証情報を入力させ、その入力された情報を盗取して不正送金に利用するという手口です。

過去には、わが国におけるフィッシング詐欺によるネットバンキング不正利用被害は限定的でした。これは、英語で記述された偽のサイトや、日本語であっても用語や文体に著しく違和感を覚えるものが多く、偽サイトであると見破ることが容易であったためと考えられます。しかし、近年は、フィッシング詐欺の手口の知識があっても見破ることが難しい、巧妙な偽サイトが増加しています。また、銀行を騙る偽の電子メールも、タイトルに「【重要】」や「【緊急】」といった表現を盛り込み、メール本文に「パスワード等を入力しなければ、システム変更によりアカウントがロックされる」などといった表現で、利用者の焦燥感を煽って情報の入力を促すものが見られます。被害増加の背景には、このような手口の巧妙化があると推察されます。

（2）スパイウェア

犯人側は、サイトの脆弱な部分を改ざんしてスパイウェア[3]を忍び込ませるなどし、当該サイトを閲覧した利用者のパソコンをスパイウェアに感染させます。スパイウェアに感染したパソコンでネットバンキングを利用すると、第三者から、１）キーボードで入力した情報を盗取される、２）ＩＤやパスワード、乱数表などの認証情報の入力を求める偽画面が表示される、３）電子メールの内容を盗み見られる、などの危険があります。さらに、スパイウェアの中には、利用者がネットバンキングにアクセスする挙動を常時監視しており、正規の銀行サイトのログイン時に偽のポップアップ画面を表示して、パスワード等の情報の入力を促すタイプも存在しています。

銀行ではスパイウェア対策として、１）については可変パスワード（パスワード生成機や乱数表などを用いて、確認の度に異なる情報の入力を要求する認証方法）を提供しています。

しかし、最近では、２）や３）の手口が発生しており、乱数表や電子メールで通知されるパスワードを利用していても注意が必要となっています。

（3）スパイウェアによる電子証明書の窃取

平成26年に入り、法人向けのネットバンキングにおいて、ネットバンキングに利用するパソコンに格納された電子証明書が窃取されてしまう、という新たな手口も確認されています。具体的な窃取の方法としては、取引銀行から提供されたネットバンキング利用のための電子証明書をパソコンのブラウザ（Internet Explorerなど）内に保存している場合、犯人側が、１）ブラウザのエクスポート機能を悪用し、電子証明書と秘密鍵を全てエクスポートして、犯人側の管理するサーバに送信してしまう、２）ブラウザ内の電子証明書を削除または破壊し、銀行から電子証明書が再発行されるタイミングで盗取またはコピーを保存し、犯人側の管理するサーバに送信してしまう、というものです。

以上のような不正利用の手口ですが、これらは主としてネットバンキングを利用するパソコンなどの端末のセキュリティ対策が不十分であることを原因として発生しているものと考えられます。そのため、銀行ではネットバンキングの利用者に対し、セキュリティ対策を複数組み合わせて採用・実施することにより、不正利用被害に遭遇する可能性を低減させることが重要であることを呼びかけています（図２）。

図２　法人のお客さま向け注意喚起チラシ

４．利用者が注意すべきこと、取るべき対策等

（１）注意点・対策

ネットバンキングを安全に・安心して利用するためには、以下の三つの観点から注意し、対策を講じることが重要です。

観点１：パソコンなどのネットバンキング利用端末を安全に管理する

ａ．セキュリティ対策ソフトを導入するとともに、最新の状態に更新しておく

上述のとおり、通常のWebサイトを見ているだけで、パソコンがスパイウェアに感染してしまうこともあります。パソコンでインターネットを利用していれば、スパイウェアに感染してしまう機会は「必ず」と言ってよいほどあると考えて、対策を講じましょう。銀行がネットバンキングの利用者向けにセキュリティ対策ソフトを提供している場合、それを活用しましょう。

ｂ．パソコンのOSやインストールされている各種ソフトウェアを最新の状態に更新しておく

スパイウェアは、パソコンにインストールされているソフトウェアの未修正の脆弱性を悪用して感染すると考えられています。OSはもちろん、ブラウザ、その他のインターネット上のファイル開封・閲覧に利用するソフトウェア（Adobeなど）も、最新の状態にしておきましょう。

観点２：パスワード等を安全に管理する

ａ．パスワード等の入力は慎重に行う

銀行が電子メールでパスワード等の入力を求めることは絶対にありません。また、偽画面や偽サイトにパスワード等を入力しないよう気をつけましょう。

ｂ．銀行が提供しているセキュリティ対策を活用する

銀行が、より安全な認証方法（現時点では、パスワード生成機など）を提供している場合は、可能な限り、銀行が推奨する方法[4]に従って活用しましょう。

観点３：不正利用手口や対策を知る

銀行のホームページに掲載されている注意喚起を確認し、それに従ってネットバンキングを利用しましょう。

ホームページで偽画面、偽のサイトや、銀行を騙る電子メールの例を図示して、注意喚起している銀行もあります。それを確認していれば、同様の手口を警戒することができます。

家族や友人、他の利用者などと不正利用の手口や対策の情報を共有すれば、身近な方の被害の未然防止や早期発見につながるかもしれません。

その他の対策として、振込や振替等の資金移動を伴う取引について、あらかじめ利用限度額を必要な範囲内でできるだけ低く設定しておくことも考えられます。不正利用の手口は、巧妙化のスピードが極めて速く、様々な対策を講じても、絶対安全とはなりません。万が一の場合にも、被害を最小限に抑えることができるように対策を講じておくことも重要です。

（２）被害に遭ったと思ったら

万が一、ネットバンキングの不正利用に遭ったと思ったら、できるだけ早く、最寄りの警察へ通報して事情を説明するとともに、取引銀行へも連絡をしましょう。

なお、全銀協の会員銀行[2]は、次のような申し合わせを行っています。

ａ．個人のお客さまについて

預金者保護法等[3]の趣旨を踏まえ、ネットバンキングによる預金等の不正な払戻しが発生した際には、銀行に過失がない場合でも、利用者自身の責任によらずに遭われた被害については[5]、１）金融機関への速やかな通知、２）金融機関への十分な説明、および３）捜査当局への被害事実等の事情説明（真摯な協力）の３点を充たしていれば、原則として補償[6]を行うことを申し合わせています[4]。

ｂ．法人のお客さまについて

全銀協の申し合わせ[5]では、銀行と被害者である法人のお客さまの双方が、一般的に必要とされるセキュリティ対策を行っていても、なお発生した不正な払戻しについて、個別銀行がその経営判断として補償することを検討することとしています。

なお、各銀行が被害補償の検討をするにあたっ

ては、１）法人のお客さま側に、セキュリティ対策の不作為をはじめとする一定の事象が発生している場合、銀行は補償を減額または補償をしないという判断をすることがあり得ること、２）法人のお客さまの属性(例：大、中小、零細企業、等)や、セキュリティ対策への対応力(例：当該法人がIT業種など)に応じて、「補償の対象先」(＝補償するか否か)や、(補償金額の)「上限」等を個別銀行が個別の事象に応じて判断することがあり得ること、に留意が必要です。

５．おわりに

銀行界では、お客さまに安心してネットバンキングを利用していただけるよう、セキュリティ対策の強化に努めているほか、最新の不正利用手口について銀行のサイトや電子メールなどを使って注意喚起しています。その他、ネットバンキングの不正送金先口座に悪用されることのないよう、口座開設時の本人確認や開設目的の確認を厳格に実施するなどして、不審な預金口座が開設されることのないように努めています。さらに、警察当局等からの通報があれば、振込先口座の入出金を一時停止（口座凍結）するなどの対応も行っています。

利用者の方におかれても、ネットバンキング不正利用の手口を知り、銀行が提供・導入しているセキュリティ対策を着実に実施するなどして、被害抑止に努めていただくようお願いしたいと思います(7)。

注

(1)正当な利用者になりすました第三者が、不正にネットバンキングの操作を行うことです。

(2)ＩＤやパスワード等。本文では以下「パスワード等」と表記します。

(3)パソコンに感染し、（情報の盗取に限らず）パソコン利用者本人が意図しない動作を引き起こす、悪意のあるソフトウェアを総称して「コンピュータウイルス（または単に「ウイルス」）」や、「マルウェア」と呼ばれることもありますが、本稿ではわかりやすさの観点から「スパイウェア」と呼びます。

(4)例えば、銀行から電子メールで通知されるパスワードをパソコンで受け取っていると、万が一、そのパソコンがスパイウェアに感染していれば、電子メールが犯人側に盗み見られてしまうかもしれません。それを防ぐために、電子メールでパスワードを通知する銀行は、パスワードの通知先をネットバンキングに利用するパソコンとは別の機器（携帯電話等）でしか閲覧できないメールアドレスに設定することを推奨していることが一般的です。

(5)これに対して、利用者に過失があると考えられる場合の対応については、「インターネットの技術やその世界における犯罪手口は日々高度化しており、そうした中で、各行が提供するサービスは、そのセキュリティ対策を含め一様ではないことから、重過失・過失の類型や、それに応じた補償割合を定型的に策定することは困難である。したがって、補償を行う際には、被害に遭ったお客さまの態様やその状況等を加味して判断する。」とされています。

(6)ただし、金融機関への通知が被害発生日の30日後まで行われなかった場合、親族等による払戻の場合、虚偽の説明を行った場合、戦争・暴動等の社会秩序の混乱に乗じてなされた場合は補償を行わない、とされています。

(7) 本文中の意見にわたる部分は、筆者の個人的な見解であり、全銀協の公式的な見解を示すものではありません。

参考文献および関連URL

[1] 公益財団法人金融情報システムセンター(編)：平成26年版金融情報システム白書. 平成25年12月９日初版発行, 平成25年３月31日基準.

[2] 全銀協の会員（下記リンク先参照）のうち、正会員・準会員・特例会員。
全銀協のホームページ
http://www.zenginkyo.or.jp/abstract/outline/organization/member_01.html

[3]「偽造カード等及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律」（平成18年２月10日施行）. 同法附則および附帯決議.

[4]全銀協のホームページ
http://www.zenginkyo.or.jp/news/2008/02/19160000.html

[5]全銀協のホームページ
http://www.zenginkyo.or.jp/news/2014/07/17174000.html