「安全で安心なインターネットの利用のために」
～フィッシングの概要と基本的な対策について～

警察庁生活安全局情報技術犯罪対策課
官民連携推進室　課長補佐　後藤　太作

■はじめに

インターネットは国民生活や社会経済活動に必要不可欠な社会基盤として定着していることに加え、新型コロナウイルス感染症対策として「新しい生活様式」が求められていることなども相まって、今後、更なる普及・発展を遂げていくものと考えられます。

他方で、新型コロナウイルス感染症の発生に乗じたものを含め、国内外において様々なサイバー犯罪等が発生しており、それらへの対処は重要な課題となっています。

本稿では、個々の利用者がインターネットを安全に利用する観点から、インターネットバンキングに係る不正送金等に用いられるサイバー犯罪等の手口であるフィッシングの概要や基本的な対策などについて紹介します。

なお、文中の意見にわたる部分は私見であることをあらかじめお断りいたします。

■フィッシングの概況

フィッシングとは、ID・パスワード等の入力を求める偽のサイト（フィッシングサイト）によって、それらの情報を窃取するといった行為であり、利用者をフィッシングサイトに誘導するため、正規の事業者等を装ったリンク付きの電子メール等を広くばら撒くなどの行為が併せて行われます。

フィッシングは、以前から様々なサイバー犯罪等に用いられている典型的な手口ですが、近年、増加・巧妙化している傾向にあり、例えば、インターネットバンキングに係る不正送金事犯（以下単に「不正送金」という。）では令和元年9月からフィッシングによるものとみられる被害が急増し、警察庁から注意喚起※1を実施しています。

令和2年において、不正送金に関しては被害が急増した令和元年と比べると減少してはいるものの、同様の被害が引き続き多数発生しているほか、その他のインターネットサービスのID・パスワード等やクレジットカード情報などを狙ったフィッシングが多数確認されています。

これらのフィッシングでは、正規の事業者からのサービス利用手続に関する連絡を装ったり、特別定額給付金に関する通知を装ったりと、あの手この手で利用者をだまそうとする様々なものが確認されていますので、内容等にかかわらず警戒する必要がある情勢といえます。

このような情勢等の詳細については、警察庁が令和3年3月4日に発表した「令和2年におけるサイバー空間をめぐる脅威の情勢等について」※2や、令和2年11月5日に開催された消費者委員会（第330回・本会議）における警察庁、フィッシング対策協議会及び総務省の説明資料（内閣府Webサイトで公開※3）などで確認できます。

■フィッシングの手口～不正送金における事例～

令和元年9月から被害が急増したフィッシングによる不正送金の手口の全体像は図1のとおりですが、主な特徴としては、

－電子メールのほか、SMS（ショートメッセージ）を用いてフィッシングサイトへ誘導する

－ID・パスワードに加えて、ワンタイムパスワード等や口座情報等をフィッシングサイトで窃取する

ことがあげられます。

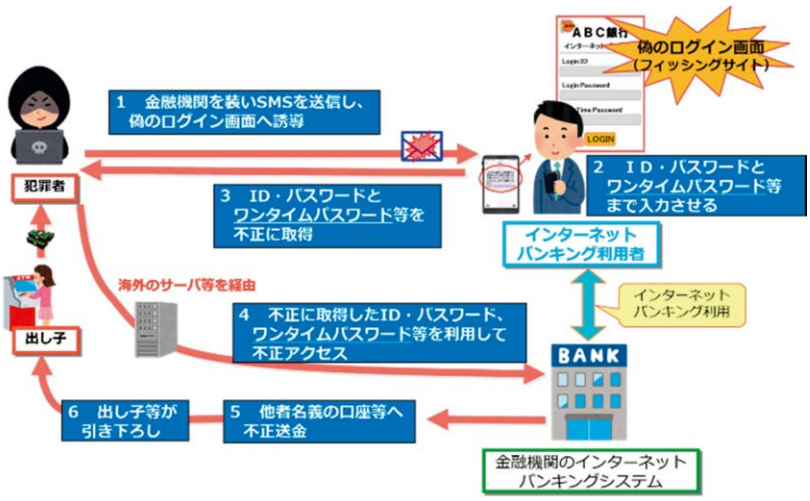

図1　フィッシング(スミッシング)による不正送金の手口

また、SMSを用いたフィッシング（スミッシング）では、

- 電子メールと比べてフィルタリング等の対策が困難であり、利用者への到達率が高い
- 送信元（送信者ID）の詐称により、正規の事業者等からのメッセージと同一スレッドに表示させることが可能である（図2）

といった傾向・特徴もみられるため、特に注意が必要です。

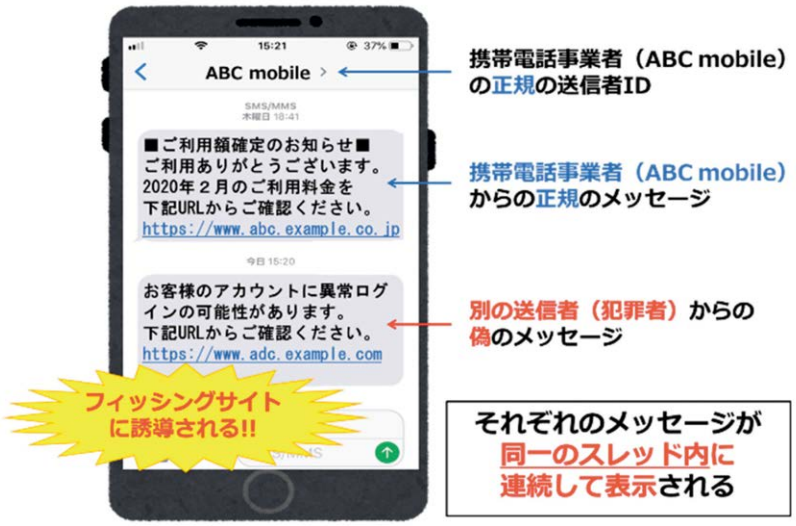

図2　同一スレッドに表示されるSMS
（携帯電話事業者を装った場合のイメージ）

近年のスミッシングの中でも特に警戒が必要と考えられる事例としては、「荷物の配送連絡を装ったSMS」があげられます。

具体的には、荷物の配送連絡を装ったSMSによってリンク先URLへのアクセスを促し、

- iOS端末からアクセスした場合は、実在する金融機関を装った偽の警告メッセージをポップアップ表示した上で、当該金融機関を装ったフィッシングサイトを表示する
- Android端末からアクセスした場合は、ブラウザの更新を装ったポップアップを表示して不正なアプリを端末にインストールするように仕向け、その後、当該アプリが実在する金融機関を装った偽の警告メッセージをポップアップ表示し、金融機関を装ったフィッシングサイトへ誘導する

といったものです。不正なアプリをインストールしてしまった場合には、不正な送金等の被害のほか、端末内の情報を窃取される、SMSをばらまく踏み台とされるなどの被害が生じるおそれがあります。

この事例については、(一財)日本サイバー犯罪対策センター(JC3)が「運送系企業を装ったSMSから銀行のフィッシングサイトへ誘導されるまでの流れ」と題した分かりやすい動画を公開※4していますので、ぜひ一度御覧ください。また、警察庁Webサイトの「インターネット安全・安心相談」ページ※5に「荷物の配送連絡を装ったSMSに関する相談事例」を掲載していますので、疑わしいSMSを受信した際などには、まず御確認ください。

なお、荷物の配送連絡を装ったSMSが代表的ですが、SMS等の内容が異なる同様のケースも多種ありますので、御注意ください。

このような手法でフィッシングサイトへ誘導され、ID・パスワード等が窃取された後には、

- 窃取したワンタイムパスワード等を用いて送金上限額などの設定を不正に変更する
- 窃取した口座情報等を用いて金融機関の公式アプリを不正に有効化する（図3）

などされた上で不正な送金がされるケースも多く、これによって、被害が増大する傾向もみられます。

また、ID・パスワード等の窃取から不正な送金・出金等までが極めて短時間で行われることから、不正な送金のような具体被害を防止するためには、フィッシングによる情報窃取を回避することと、情報を窃取されてしまった場合に可能な限り迅速に対処することが極めて重要といえます。

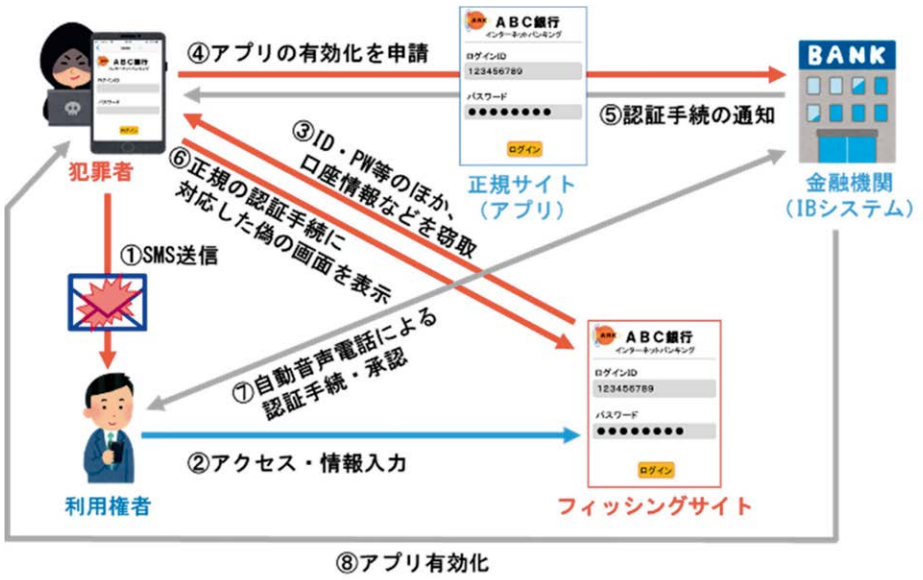

図3　公式アプリの不正な有効化の概要

■フィッシングによる情報窃取の回避

フィッシングによる情報窃取を回避するための対策は、一言で言えば「フィッシングの手口にだまされないようにする」ことです。具体的には、

- リンク先URLへのアクセスを促す電子メール・SMS全般を警戒する
- 利用しているサービス等へのアクセスはブラウザのブックマーク等や、公式アプリから行う（SMS等に記載されたリンクからのアクセスは避ける）
- SMS等に記載されたリンクからのアクセスが避けられない場合には、正規サイトのドメインであるかを確実に確認する
- 安易にID・パスワード等を入力したり、アプリをインストール（権限を許可）したりしない

ことなどがあげられます。

昨今のフィッシングは極めて巧妙であるため、まずはSMS等に記載されたリンクからのアクセス等を極力避けることが有効です。その上で、どうしてもアクセスが必要と考える場合には、SMS等の文面やサイトの

見た目などでの判別は困難であることに留意し、正規サイトと見分けづらい紛らわしいURLが用いられている可能性や電子メールに記載されているリンク先URLの表記が偽装されている可能性なども念頭に置いて、アクセス先のURL（ドメイン）が正規サイトのものであるか細心の注意を払って確実に確認する必要があります。

また、相談事例の中には、だまされて情報を入力してしまった後に不安になってインターネットで調べた結果、注意喚起情報を見付けて自ら被害に気が付いたケースもありますので、不審と感じたか否かにかかわらず、このような情報を事前に確認することも効果的な対策であると考えられます。

■フィッシング被害後の迅速な対処

フィッシングの被害にあった場合には、入力してしまったパスワード等を変更する、正規の事業者（金融機関やクレジットカード会社など）へ連絡して利用を停止するなどの被害防止措置をすぐに実施することが重要です。

利用サービスの設定を不正に変更されたり、公式アプリを不正に有効化されたりすることによって、正規の利用者がログインやパスワード等の変更をできなくなるケースや、パスワードの変更のみを行っても不正な送金等の被害が生じるケースもありますので、放置せずに迅速・確実に対応を行ってください。また、不正なアプリをインストールしてしまった場合には、アンインストールすることも忘れないようにしてください。

なお、万が一、他のサービスでパスワードを使い回している場合は、他のサービスのパスワードも適切に変更してください。フィッシングによる場合に限らず、一度漏えいしたID・パスワードはリスト化されて他のサービス等の侵害にも用いられることから、パスワードの使い回しは禁物です。心当たりがある場合は事前に見直しを行うことを強く推奨します。

また、不正な送金等の被害が判明（発生）した場合に備えて、受信したSMS等や入力してしまった情報、時系列などについてなるべく詳細に記録しておくことも重要です。こういった記録は金融機関や警察における調査・捜査や被害防止対策に役立つのみならず、早期の被害回復等につながることも期待されますので、記憶の新しいうちに行うようにしてください。

■おわりに

本稿で紹介した対策に目新しいものはありませんが、新型コロナウイルス感染症対策における三密を避ける、マスク等の着用や手指の消毒を徹底するといった対策と同様に、個人として必要かつ実施可能な対策を理解し、意識的に徹底することが重要です。

我が国では、例年、2月1日から3月18日を「サイバーセキュリティ月間」に設定し、セイバーセキュリティに関する普及啓発活動を集中的に実施しています。月間中に警察が開催するイベント情報なども含む関連情報については、内閣官房の内閣サイバーセキュリティセンター（NISC）のWebサイト※6で公開されていますので、まずはこのような機会に関心を持って調べてみることも効果的であると思います。

また、警察庁のWebサイト「サイバーポリスエージェンシー※7」では、サイバー犯罪、サイバー攻撃による被害の防止を図るため、サイバー犯罪・サイバー攻撃の手口や情勢に係る情報等を公開しているので、こちらもご覧ください。

本稿で紹介したこれらの情報がインターネット利用者の安全・安心の一助となれば幸いです。

※1　https://www.npa.go.jp/cyber/policy/caution1910.html
※2　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_cyber_jousei.pdf
※3　https://www.cao.go.jp/consumer/iinkai/2020/330/shiryou/index.html
※4　https://www.jc3.or.jp/info/movie.html
※5　https://www.npa.go.jp/cybersafety/
※6　https://www.nisc.go.jp/security-site/
※7　https://www.npa.go.jp/cybersecurity/index.html