特集

消費者のための情報セキュリティ入門

特集1

ネットを悪用した手口に騙されないために4つの代表的な罠を知ろう

神谷 健司 Kamiya Kenshi
独立行政法人情報処理推進機構(IPA)
セキュリティセンター セキュリティ普及啓発・振興部 セキュリティ相談・支援グループ

パソコンやスマートフォン(以下、スマホ)を使ったインターネットサービスは、生活に欠くことができないものになりました。その一方で、インターネットには個人を狙う罠が仕掛けられている場合があります。

罠のほとんどは、偽の警告などの嘘で利用者を巧みに「騙す仕掛け」です。こうした仕掛け(=手口)を知ることが、騙されないための対策になります。そこで、本稿では、IPAが開設している「情報セキュリティ安心相談窓口」に数多くの相談が寄せられている騙しの手口について解説します。

罠 その1 偽のセキュリティ警告を使用したサポート詐欺

パソコンでウェブサイトを閲覧中に突然、「パソコンがウイルスに感染して個人情報が漏えいしている」などの警告が表示されることがあります。警告が画面いっぱいに表示され、電話番号が表示されているなどの場合、それは偽の警告です(図1)。パソコンから、けたたましい警告の音声が鳴りやまないこともあります。

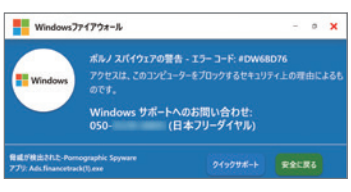
これは、警告を消せず焦った利用者に、偽のサポート窓口に電話をさせ、サポート料金と称して高額の金銭を騙し取る、「サポート詐欺」と呼ばれる手口です(図2)。

電話をすると、片言の日本語を話す外国人のオペレーターにつながります。相手は、マイクロソフト社などの著名な企業のサポート技術者であると偽り、パソコンに遠隔操作ソフトをダウンロードさせます。

遠隔操作ソフトを使用すると、遠隔地にあるパソコンから、操作対象のパソコンの画面を見ながらマウスやキーボードの操作が可能になります。相手はこの機能を悪用して次々と画面を開き、パソコンに問題があるという嘘の説明を繰り返します。被害者がこの説明を信じると、ウイルスの除去やセキュリティサポートサービスと称して高額な金銭を要求します。

図1 偽のセキュリティ警告の例

図2 偽のサポート窓口



偽警告の被害にあわないために

偽の警告で被害者を焦らせ、不安をあおり、そのうえで言葉巧みに信用させ、金銭を騙し取るやり方は、オレオレ詐欺などの特殊詐欺にも共通する手口と言えます。ところが、特殊詐欺の手口に関する知識があり、日頃から注意をしていてもサポート詐欺に騙されてしまうことがあります。「ウェブサイト閲覧中のウイルス感染」など、経験したことがない騙しの手口を使われると、従来の知識が通用せず、嘘が見破れないことがあるためだと考えられます。騙されないためには、こうした手口を知ることが重要です。

加えて、普段目にしない警告が突然表示された場合、それは正しいものなのかを立ち止まって考えることも重要です。

正規のウイルス対策ソフトがウイルス感染を検知した際も警告が出ますが、今すぐ電話をするように求めることは基本的にありません。

現在のパソコンはセキュリティが強化されています。個人の利用では、基本的なセキュリティ対策を行っている場合[*1]、ウイルスに感染することは非常に少なくなりました。

そのため、正規のウイルス対策ソフトが動作した際の表示を見る機会がないため、突然表示された「偽のウイルス警告」を本物と勘違いしてしまうことが考えられます。

偽の警告が表示された際の対処

パソコンに偽の警告が表示された際の対処は、所定のキー操作を行い、ウェブブラウザーを閉じるだけで問題ありません。詳細は「IPA安心相談窓口だより『偽のセキュリティ警告に表示された番号に電話をかけないで！』」[*2]の5項をご参照ください。

電話をかけて、パソコンを遠隔操作されてしまった場合は、Windowsの「システムの復元」機能を使用して、遠隔操作ソフトをインストールする前の状態にシステムを戻すことを推奨します。システムの復元ができない場合、遠隔操作の及ぼす影響について判断ができないため、パソコンの初期化を推奨します。詳細は前出の資料[*2]の3項をご参照ください。

罠 その2 フィッシング

フィッシングとは、実在する企業・団体名をかたり、その企業・団体の公式サイトにそっくりな「偽サイト」に誘導し、利用者を騙して情報を入力させて、その情報を奪う手口のことです。フィッシングを目的とした、メール、ショートメッセージサービス（以下、SMS）、ソーシャルネットワーキングサービス（以下、SNS）の投稿などに記載されたURLをクリックし、パスワードやクレジットカード番号などを入力すると被害が発生します。

逆の見方をすると、フィッシングメールを受信しても、URLのクリックさえしなければ被害は発生しません。そのため攻撃者は、さまざまな騙しのテクニックを使ってURLをクリックさせようとします。主な手口は次のとおりです。

- アカウントが凍結されるなどの、受信者に不安を抱かせる内容を記載
- 偽の当選や還付金の通知など、思わずURLをクリックしたくなる内容を記載
- 新型コロナウイルスワクチンの接種予約など、その時々の社会情勢に乗じた内容を記載
- メールの送信元やロゴマークを偽装して公式からの通知であると錯覚させる　など

＊1 独立行政法人情報処理推進機構「日常における情報セキュリティ対策」（2023年4月20日）「2-2. 利用者向け」 https://www.ipa.go.jp/security/anshin/measures/everyday.html

＊2 IPA安心相談窓口だより「偽のセキュリティ警告に表示された番号に電話をかけないで！−パソコンにおける最近の手口と対策を解説−」（2021年11月16日） https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211116.html

フィッシングの被害にあわないために

フィッシングメールは、本物らしい文面を使用し、送信元などを偽装しているため、真偽の判断が難しいことが多くなっています[*3]。本物かどうかの判断に迷った場合は、公式サイトなど確かな情報源を使ってご確認ください。真偽がはっきりしないメールについては、次の対応をしてください。

- URLをクリック、タップしない
- 添付ファイルを開かない
- 記載の電話番号に電話をしない
- 返信しない

罠 その3 SMSを悪用した手口

従来、フィッシングサイトへの誘導は、主にメールで行われていました。近年は、新たな手口として、SMSを悪用したものが増えています。その代表例が、宅配事業者をかたる偽の不在通知SMSです(図3)。

フィッシングメールに関する知識があり、不審なメールに注意をしていても、この偽のSMSに騙されてしまうことがあります。SMSでもフィッシングが可能であることを知らない場合に、荷物の配達予定日にたまたまこうしたSMSが届くと、思わずURLをタップしてしまうことがあるためです。

偽のSMSは、宅配事業者をかたるものに加えて、通信キャリアや公的機関をかたる架空請求、金融機関をかたるフィッシングなど、複数のバリエーションがあります(図4)。

悪意の攻撃者は、SMSに偽の不在連絡や、支払い請求などを記載し、受け取った人を驚かせて、SMSのURLをタップさせようとします。URLをタップしてしまうと、スマホの種別や偽SMSのタイプによって、次に示すさまざまな被害が発生します(図5)。

- Androidでは多くの場合、不正アプリのインストールに誘導される
- iPhoneではフィッシングサイトに誘導され、「Apple IDとパスワード」や「クレジットカードの情報」を入力させられ、それらを奪われる
- 架空請求SMSでは、フィッシングサイトへ誘導され、コンビニで買ったプリペイドカードで支払うように指示され、フィッシングサイトに「プリペイドカードの発行番号」を

図3 偽の不在通知SMSの例

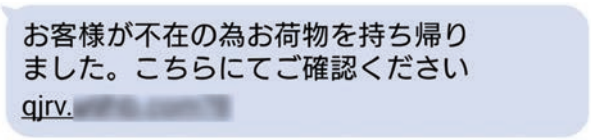


図4 国税庁をかたる架空請求SMSの例

図5 URLをタップすると発生する被害

＊3 IPA安心相談窓口だより「メールの見かけ上の送信元情報を安易に信じないで」(2021年9月21日)
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20210921.html

入力させられて金銭を奪われる。クレジットカード番号を窃取されることもある

● 偽SMSの被害にあわないために

不審なSMSのURLをタップしない限り前記の被害にあうことはありません。不審なSMSが届いた際は削除し、URLはタップしないようにしてください。

Androidに不正なアプリをインストールしてしまうと、そのスマホから、同じ内容の偽SMSが見知らぬ宛先に多数送信されてしまいます。偽SMSの発信元には、不正なアプリをインストールしてしまった被害者の電話番号が使われます。そのため、荷物の問い合わせの電話が複数の人からかかってくるようになり、この時点で異常に気がつくことがあります。

被害者に不正なアプリをインストールさせる際も、騙しのテクニックが使われます。Androidには不正なアプリを誤ってインストールしないための保護機能があります。ところが、攻撃者は、利用者を騙してこの機能を解除させようとします。

SMSのURLをクリックすると、「使っているアプリが古いため更新が必要」などの偽の警告を表示して、不正なアプリをインストールすることを求めます。アプリの更新に見せ掛けて、利用者に保護機能を解除して不正なアプリをインストールさせようとするのです。このような不審な警告が出た場合は、指示には従わないでください。

この手口の詳細や、不正なアプリをインストールしてしまった際の対処方法は、IPA安心相談窓口だより[*4] [*5]をご参照ください。

罠 その4 性的な映像をばらまくと恐喝し、暗号資産で金銭を要求する迷惑メール

「あなたのパソコンをハッキングしてアダルトサイトを閲覧している姿をウェブカメラで撮影した。家族や同僚にばらまかれたくなければ暗号資産で金銭を支払え」というメールを受信したという相談が寄せられています。この手口では、ハッキングなどの言葉で相手を不安にさせたうえで、性的な映像をばらまくと脅しています[*6]。こうした脅しに騙されてはいけません。

このメールは同じような文面で不特定多数にばらまかれています。実際の動画へのリンクや添付などがないことから、このメールの内容について根拠はないと考えられます。そのため、メールを無視して削除するだけで問題ありません。

● 手口を知る、立ち止まって考える

インターネットを悪用して個人を狙う代表的な騙しの手口についてご説明しました。こうした手口を知ることで、安全にネットを楽しむことができます。より多くの手口を知りたい場合は、警察庁、IPA、国民生活センターなどの注意喚起情報をご参照ください。

もう1つ、騙されないためのポイントをご紹介します。前述のとおり、騙しの手口には、落ち着いて考えると通常は発生しない不自然な点が多々あります。そのため、初めて見る警告、もしくは不自然な状況に遭遇した場合、それらは偽物である可能性が高いです。従来と異なる状況に遭遇した際に、これは騙しの手口ではないかを「立ち止まって考える」ことが重要です。

どうしたらよいかが分からない場合は、相手の指示には従わず、近くの詳しい人やIPAなどの窓口に相談するようにしてください。

＊4 IPA安心相談窓口だより「宅配便業者に加えて通信事業者をかたる偽ショートメッセージサービス（SMS）が増加中」（2021年12月22日）
https://www.ipa.go.jp/security/anshin/attention/2021/mgdayori20211222.html

＊5 IPA安心相談窓口だより「国税庁をかたる偽ショートメッセージサービス（SMS）や偽メールに注意」（2022年10月31日）
https://www.ipa.go.jp/security/anshin/attention/2022/mgdayori20221031.html

＊6 IPA安心相談窓口だより「性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意」（2018年10月10日）
https://www.ipa.go.jp/security/anshin/attention/2018/mgdayori20181010.html