インターネット詐欺や騙しの事例と安心・安全対策

大久保 貴世 ●一般財団法人インターネット協会 主幹研究員

なりすましからフィッシングまで、対策をしていれば防ぐことができたトラブルだが、どう対策していいのか分からない利用者も多い。「情報セキュリティ対策9カ条」など安心・安全対策の周知が求められる。

■インターネット利用「トラブル不安」が68％

内閣府が2018年11月に公表した「インターネットの安全・安心に関する世論調査」[1]で、インターネット利用をめぐるトラブルへの不安が「ある」「どちらかといえばある」と答えた人は合わせて68％となった。

不安の内容（複数回答）は「個人情報が流出する」が80％で最多。「詐欺などにあって金品などを取られる」52％、「子供や家族が危険な目に遭う」45％、「SNSやブログなどで誹謗中傷を受ける」37％と続く。対策を「行いたいが、できていない」と「行っていない」は計17％。その理由（複数回答）は、「何を行ってよいかわからない」が最多で60％、「費用がかかる」13％や「時間がない」13％と続く。調査は18歳以上の3000人を対象に面接方式で行い、1666人が回答したデータである。

■セキュリティ関連の事例

それでは、具体的なトラブルにはどんなものがあるか。2018年のセキュリティ関連の事例を振り返ってみよう（資料4-5-1）。注意すれば防げたトラブルが多いが、利用者からみれば、どのような対策をしていればよかったのか、分かりにくかったのではないかと考えられる。

■インターネット利用者ができる対策の啓発

なりすましメールやフィッシングメールは、インターネット関連団体のメールアドレス宛にも多数届いており、明らかにあやしい迷惑メールだと判断できるものもある。一方で、文中に本当のパスワードが記載されているなど、もしかしたら利用者自身が何か間違ったことをしたのではないかとメールの内容を信じかねないものもある。

そこで、「何を行ってよいかわからない」という利用者に向けて、そのような場面に遭遇する時に備え、地域、学校などへの注意啓発の例を場面別に紹介したい。

●場面１：宅配業者を騙るショートメッセージ（SMS）

「佐川急便をかたるSMSから偽のサイトに誘導され、スマートフォンに不審なアプリをインストールしてしまった」

佐川急便の偽サイトにはAndroidスマートフォ

資料4-5-1　2018年のセキュリティ関連事例

内容	詳細
なりすましメール	佐川急便を装うショートメッセージ（SMS）が突然スマートフォンに届き、不審なアプリのインストール誘導や、フィッシングサイトへ誘導される手口が2018年7月から急増している。記載のアドレスにアクセスしてアプリをインストールしたり、フィッシングサイトに情報を入力すると、不特定多数の人に偽のSMSを大量に送られたり、キャリア決済を不正使用される場合がある。佐川急便は宅配サービスでSMSを使っておらず、注意を呼びかけている。
脅迫メール	仮想通貨「ビットコイン」による支払いを要求する複数パターンによる脅迫メールが出回っている。メールの内容は、「アダルト動画を閲覧している姿をウェブカメラで撮影した」「拡散されたくなければ仮想通貨を支払え」などと脅迫する内容だった。 またメールの件名や本文に受信者が実際に使用していた可能性のあるパスワードを記載。外部のサービスから何らかの原因でデータが漏えいし、送信者はそれをもとに記載をしていると考えられる。
不正アクセス	ある大学は2018年10月24日、メールシステムに不正アクセスを受けていたと発表。教職員など3人のメールアカウントが第三者に乗っ取られ、メールの送受信データから3アカウント合計で1147人の個人情報が漏洩していた。さらに、3アカウントから合計6972件のスパムメールが送信された。 3アカウントが乗っ取られ、スパムメールが送信されたのは2018年7月28日から8月28日にかけて。漏洩した個人情報は、教職員や学生、卒業生の氏名やメールアドレス、電話番号などである。 米マイクロソフトのクラウドサービス「Office 365」を利用し、IDとパスワードが第三者に推測され、不正にログインされた。大学側は、個人情報が漏洩した対象者に対して、個別に状況の説明と謝罪をしている。 再発防止策として、一定期間パスワードを変更していない利用者のアカウントをロックするほか、システムのセキュリティを強化したり、利用者向けの講習会を開催したりするという。
フィッシングメール	「あなたのアカウントは閉鎖されます」Amazonかたるフィッシングメール出回る。Amazonのロゴ入りHTMLメールで、本文には「大変申し訳ございません、あなたのアカウントは閉鎖されます。あなたのアカウントAmazonを更新できませんでした」などと書かれ、「アカウント検証」と書かれたリンクも添えられている。リンクをクリックすると、フィッシングサイトに誘導される。 2018年6月、セキュリティ団体が、リンクをクリックしたり、フィッシングサイトに個人情報やクレジットカード情報などを入力しないよう注意が必要と呼びかけている。

出典：各種資料を基に筆者作成

ン向けの不審なアプリをダウンロードさせるリンクが仕込まれている。これをAndroidスマートフォンにインストールした場合、自分のスマートフォンからも佐川急便をかたるSMSが不特定多数（自分のアドレス帳にない宛先）に向けて送信されてしまう事象が確認されている。

対策は2つある

1.不審なSMSのURLをタップしない

2.提供元不明のアプリのインストール許可を“オフ”にしておく

Androidスマートフォンのセキュリティ設定で、「提供元不明のアプリ」をオフにしておく。今回の不審なアプリは、公式のアプリマーケット（Google Playなど）からは配信されていない。公式マーケット以外からアプリをインストールしようとする場合、許可をオフにしていると、インストールをブロックする警告が一旦表示されるが、そこから先の設定には進まず、インストールをキャンセルする。

その後、2018年8月以降、iPhoneやiPad等のiOS端末でアクセスした場合に、「電話番号と認証コード」や「Apple IDとパスワード」などの詐取を狙ったフィッシングサイトが表示される事例が確認された。その手口は、偽SMSに記載のURLから偽サイトにアクセスし、携帯電話会社が提供するキャリア決済サービスの悪用やApple IDを狙ったフィッシングサイトに誘導されるというもの。フィッシングサイトでは、「アップル社から送られた製品はセキュリティの許可が必要」などのもっともらしい文言で、入力を促されてしまうものだ。

対策は3つある。

1.偽サイトや、フィッシングサイトが表示された場合は、画面を閉じる。

2.電話番号と認証コードを入力してしまった場合は、すぐに携帯電話会社に不正なキャリア決済が発生していないか確認する。

3.キャリア決済が発生していた場合は、携帯電話

会社や、キャリア決済が利用されたサービスの提供会社に相談する。それでも問題が解決せず、契約関連について公的機関への相談が必要な場合は、最寄りの消費生活センターに相談する。

【参考資料】

独立行政法人情報処理推進機構セキュリティセンター「宅配便業者をかたる偽ショートメッセージに関する相談が急増中～誘導されるままAndroid端末にアプリをインストールしないように！～」（2018年 8月 8日）
https://www.ipa.go.jp/security/anshin/mgdayori20180808.html

「宅配便業者をかたる偽ショートメッセージに関する新たな手口が出現し、iPhoneも標的に
～不審アプリのインストールに加えて、フィッシングにも注意！ ～」（2018年 11月 29日）
https://www.ipa.go.jp/security/anshin/mgdayori20181129.html

●場面２：仮想通貨で金銭を要求する迷惑メール

「アダルトサイトを閲覧しているあなたの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仮想通貨で金銭を支払え」というメールを受信した。

メール文中には、本来あるべき映像へのURLリンクや、映像ファイルの添付がないもの（資料4-5-2）。よって、単なる迷惑メールの可能性が非常に高いと考えられる。また、当初はすべて英語で書かれていたが、その後は日本語で書かれたメールも増えている。日本語は不自然で、英文を翻訳サイトなどの機械翻訳にかけたものであろう。

実際に受信者がウェブサービス等で設定したことのあるパスワードが1つ、メールの件名や本文冒頭に記載されている場合がある。「これがあなたのパスワードであることを知っている」というような説明がされ、そのパスワードは、現在使用中のものである場合と、そうではなく古いものの場合とがあった。これは、外部のサービスから何らかの原因でデータが漏えいし、それをもとに記載されていると考えられるが、流出経路とその原因は不明である。

「撮影されたあなたの映像を家族や同僚にばらまかれたくなかったら、ビットコインで5,000ドル（金額はケースによって異なります。）を支払え」「支払えば、撮影した映像は即座に消去する」と記載され、ビットコインを利用する際の口座番号に相当するビットコインアドレスなどが記載されている。

迷惑メールによくあることだが、送信先と送信元が両方とも自分の同じアドレスになっている場合があり、実際の送信元はメールのヘッダ情報を見ないとわからないことがあり、さらに複雑な発信ルートを辿っていたり身元を隠すために巧妙な手口を使ったりする場合もある。

対策は2つある

1.受信したメールは無視する。

迷惑メールの一種にすぎず、メールは無視して、仮想通貨の支払いは行わない。

2.記載されていたパスワードは変更する。

メールに記載されていたパスワードを現在も使用している場合は、パスワードの変更を行う。

【参考資料】

出典：独立行政法人情報処理推進機構セキュリティセンター「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/mgdayori20181010.html

資料4-5-2　仮想通貨で金銭を要求する迷惑メールの例

Subject:あなたのパスワードが侵害されました
Date: Wed, 28 Nov 2018 22:41:16 +0800
From: *****l@******.org　**←Fromアドレスが Toと同じアドレス**
To: newuser <*****l@******.org>

こんにちは!
私は数ヶ月前にあなたの電子メールとデバイスをクラックしたハッカーです。
あなたが訪問したサイトの1つにパスワードを入力君た。それを傍受しました。
これは、ハッキングの瞬間にからのあなたのパスワードです: **********
(中略)
だから、あなたがサイトで楽しむとき(あなたは私が何を意味するか知っています!)
あなたのカメラのプログラムを使用してスクリーンショットを作成しました。
その後、私はそれらを現在閲覧されているサイトのコンテンツに結合しました。
(中略)
したがって、私は沈黙のためにあなたからの支払いを期待しています。
私は$600が良い価格だと思います!
Bitcoin経由で支払う。私のBTCウォレット: 1AZ3wUazMgpCg3y**********
(中略)
ばかなことしないで!警察や友人はあなたを確実に助けません...
p.s. 私はあなたに将来のアドバイスを与えることができます。安全でないサイトにはパスワードを入力しないでください。
私はあなたの慎重さを願っています。お別れ。

出典：一般財団法人インターネット協会

■推奨するパスワード作成方法の一例

パスワードを利用されないためには、まずはパスワードを長く複雑にするなど推測されにくいものにして、さらに複数サービス間で使い回しをしないことが重要。使い回しを回避するパスワード作成方法の1つとして、『コアパスワード』を使った方法を紹介する。

まず、自分の趣味や興味のあることなどから決めた短いフレーズを基に、任意の変換ルールを適用して、憶えやすく、強度の高いパスワードを作成。これを全てのパスワードに共通して使用する『コアパスワード』とする。

例えば、「テレビが好き」というフレーズを決めた場合、このフレーズをローマ字「terebigasuki(12文字)」に変換し、これだけである程度の長さ(桁数)を確保した憶えやすいパスワードが作成できる。

次に、ローマ字に置き換えた文字列の一部を大文字、記号、数字に置き換えたり、数字や記号を追加したりするなど、任意の変換ルールを適用する。

次に、サービス名の略称や頭文字、URLの一部などから、サービス毎に任意の短い文字列を決める。これをサービス毎の識別子として、コアパスワードの前または後に追加する。

【参考資料】

独立行政法人情報処理推進機構セキュリティセンター「不正ログイン被害の原因となるパスワードの使い回しはNG〜ちょっとした工夫でパスワードの使い回しを回避〜」(2016年8月3日)
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

■これだけは知っておきたいこと

あらためて、内閣サイバーセキュリティセンターが、インターネットを安全に利用するための対策をまとめた「情報セキュリティ対策9カ条」を紹介したい。

このような対策をしたり心構えを持っていれば、大切な個人情報の流出や、詐欺などにあって金品などを取られるという事態を避けることができる。すぐにでもできるわかりやすい対策なので、ぜひ対応してもらいたい。

（1）OSやソフトウェアは常に最新の状態にしておこう

製造元から無料で配布される最新の改良プログラムにアップデートしましょう。

（2）パスワードは貴重品のように管理しよう

パスワードは他人に知られないように、メモをするなら人目に触れない場所に保管しましょう。

（3）ログインID・パスワード　絶対教えない用心深さ

金融機関を名乗り、銀行口座番号や暗証番号、ログインIDやパスワード、クレジットカード情報の入力を促すような身に覚えのないメールが届いた場合、入力せず無視しましょう。

（4）見に覚えのない添付ファイルは開かない

メールに添付されたファイルを開いたり、URL（リンク先）をクリックしないようにしましょう。

（5）ウイルス対策ソフトを導入しよう

コンピュータにウイルス対策ソフトを導入しましょう。

（6）ネットショッピングでは信頼できるお店を選ぼう

詐欺などの被害に遭わないように信頼できるお店を選びましょう。身近な人からお勧めのお店を教わるのも安心です。

（7）大切な情報は失う前に複製しよう

思い出の写真など、大切な情報がパソコンの故障によって失われることのないよう、別のハードディスクなどに複製して保管しておきましょう。

（8）外出先では紛失・盗難に注意しよう

機器やファイルにパスワードを設定し、なくしたり盗まれないように注意して持ち歩きましょう。

（9）困ったときはひとりで悩まず各種相談窓口に相談しよう

1. 内閣府2018年11月インターネットの安全・安心に関する世論調査
https://survey.gov-online.go.jp/tokubetu/h30/h30-net.pdf

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2019年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp