わたしは ダマサレナイ!!

第51話

インターネットバンキング＆ＡＴＭ セキュリティ対策で口座を不正利用から守る！

ATTENTION

このコーナーで紹介するマンガは、実際に起きた事件を基に、「だましのシーン」を再現したものです。「私だけは大丈夫」なんて甘く考えていませんか？ 実はそう考える人こそ被害にあいやすいのです。

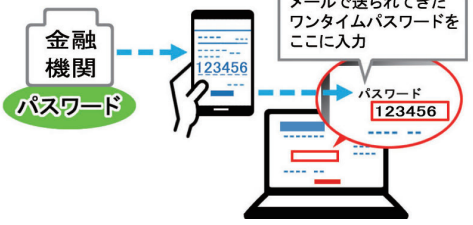
監修／NACS（公益社団法人日本消費生活アドバイザー・コンサルタント・相談員協会）消費者相談室／大井菜子　　マンガ／まきのこうじ

ネットバンキングのセキュリティ対策例

※金融機関によって異なります。

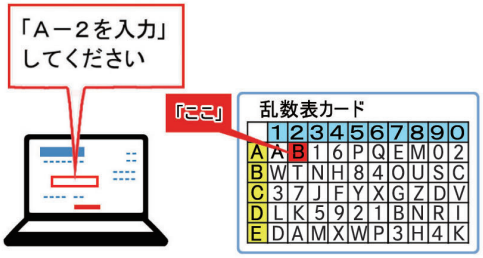
▶ワンタイムパスワード

事前に登録しているメールアドレスやスマートフォンアプリなどに、金融機関から送られてくる一度しか使えない使い捨てパスワード。



▶乱数表認証

法則性のない文字列の表が記載されたカードが金融機関から発行され、ネットバンキングを利用する際、指定された表位置の文字や数字を入力する。



POINT! SAGI 1 ネットバンキングとＡＴＭの主なセキュリティ対策

インターネットバンキング（以下、ネットバンキング）やＡＴＭは、便利な金融サービスとして普及してきましたが、ＩＤやパスワードなどの認証情報を詐取されて不正利用される危険性もあります。実際、過去には不正送金や成りすまし詐欺といった被害が多発しました。金融機関では、そうした被害からユーザーを守るために、さまざまなセキュリティ対策の導入や注意喚起を行い、被害が大幅に減少しましたが、２０１９年秋ごろより、ネットバンキングの不正送金の被害が再び急増しています。

〈ネットバンキングの主なセキュリティ対策〉

●ワンタイムパスワード

認証のたびに１度限りのパスワードが発行される。発行方法は、「事前に登録したメールアドレスに送信」、「事前にダウンロードしたスマートフォンアプリに通知」、「金融機関が貸し出す小型の端末（トークン）で生成」などがある。

●乱数表認証

ユーザーごとに乱数表を記載したカードが発行され、認証時に指定される文字や記号を、乱数表を基に入力。指定される内容は認証のたびに変わる。

〈ＡＴＭの主なセキュリティ対策〉

●指静脈認証

人それぞれ違う手指の静脈パターンを、自分のＩＣキャッシュカードに登録する生体認証型のセキュリティ。ＡＴＭに搭載されたセンサーに指を触れて認証させる。

POINT! SAGI 2 ネットバンキングの不正送金 その新たな手口とは？

ネットバンキングの不正送金における従来の主な手

口は、「フィッシングメールやフィッシング広告によって消費者を偽のＷＥＢサイトに誘導し、認証情報を詐取する」でしたが、現在横行している手口はさらに巧妙です。まず、金融機関や宅配業者などを装ったメールで、消費者のパソコンを不正送金ウイルスに感染させます。スマートフォンなら、ゲームアプリなどに偽装した不正送金アプリをインストールさせます。そして、消費者が正規のネットバンキングにアクセスすると、不正送金ウイルスや不正送金アプリが起動。正規のネットバンキングのページの上に重ねるように、偽のページをポップアップという仕組みで表示させるのです。消費者は偽のページと気づかずに、パスワードやＩＤ、乱数表などの認証情報を入力してしまい、自分の預貯金口座（以下、口座）から不正送金をされてしまいます。安全性が高いとされるワンタイムパスワードでも、被害にあったケースが確認されています。

表示されるＵＲＬが正規ページと同じなため、見破ることは極めて困難です。まずは、不正送金のウイルスやアプリの潜入を防ぐために、怪しいメールの添付ファイルやリンクを不用意に開かないこと、アプリをインストールする際は、開発元が信頼できるか確認することが大切です。そして、セキュリティのソフトやアプリを常にアップデートして最新の状態に保つようにしましょう。

POINT! SAGI 3 口座を守るためにはセキュリティ対策とセキュリティ意識が大切

セキュリティ対策を破る手口があるからといって、セキュリティ対策は決して無駄ではありません。金融機関が提供するさまざまなセキュリティサービスを活用することは、口座を守るための必要最低限な対策という認識を持ってほしいと考えます。

金融機関のセキュリティサービスは、前頁でご紹介した以外にもいろいろあります。例えば、「取引通知

メール」は、口座の入出金や振込などの手続きがあった場合に、登録済みのメールアドレスにその都度、内容を通知してくれます。さらに「利用限度額設定」も活用して1日の利用限度額を設定することで、万が一、不正な送金や出金をされても早期発見し、被害金額を抑えることができます（どちらのサービスもネットバンキングとATMで利用可能です）。また、ネットバンキングの「IP制限」は、事前に登録したIPアドレス（インターネットに接続される機器を識別する番号）からのアクセスのみ取引を可能とし、第三者による悪用や不正取引の被害を防止します。セキュリティサービスの内容や名称は金融機関によって異なるので、問い合わせてみてください。

こうしたセキュリティ対策に加えて、日常生活の中でセキュリティ意識を高めることも非常に大切です。「口座の取引内容や残高を定期的に確認する」、「パスワードを使いまわさない」、「インターネットカフェやフリーWi－Fiの環境でネットバンキングを利用しない」など、認証情報詐取の危険性を常に意識しましょう。

ネットバンキングの使用中に不審な点や違和感を感じたら、操作をすぐ中止して、口座の金融機関へ連絡してください。万一被害にあってしまった場合は、口座の金融機関や消費者ホットライン、最寄りの警察や警察相談ダイヤルに相談しましょう。

関連情報

・国民生活センター
「偽ウェブサイトとインターネットバンキングをねらった攻撃」
http://www.kokusen.go.jp/wko/pdf/wko-201809_07.pdf

万一の相談先

・消費者ホットライン
☎188（いやや）（「いやや!」と覚える）
※最寄りの消費生活センターや消費生活相談窓口につながります。相談受付時間は相談受付先によって異なります。

・警察相談専用電話
☎#9110
※受付時間は各都道府県警察本部で異なります。