Information-technology
Promotion
Agency, Japan

第 13-32-299 号
2013 年 9 月 2 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 インターネットバンキング利用時の勘所を理解しましょう！ 」

警察庁からは 8 月 8 日に、「2013 年 1 月から 7 月までのインターネットバンキングの不正送金による被害額が、過去最悪だった 2011 年の年間被害額を超えた」との発表がありました。

IPA に寄せられる相談においても“インターネットバンキングの不正送金”に関する相談の件数が、6 月以降目立っています（図 1 参照）。

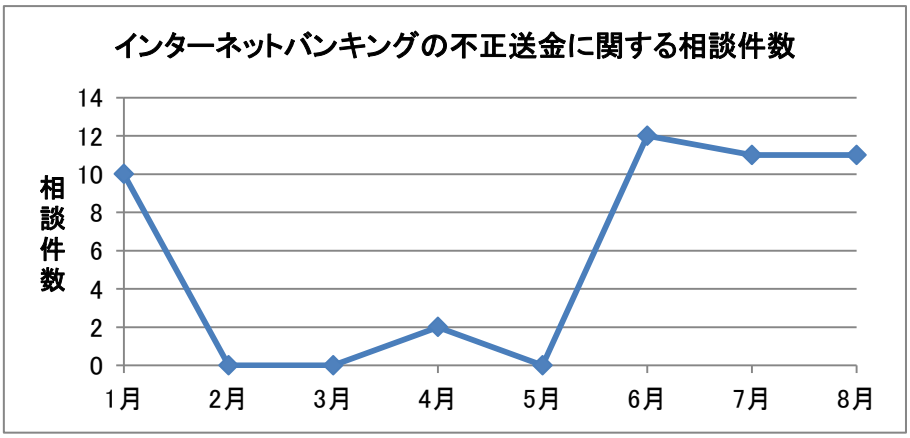

図 1：インターネットバンキングの不正送金に関する相談件数

また、報道された内容から、これまで有効とされていたワンタイムパスワードを用いた認証が破られる新たな手口が出現していることがうかがえます。この手口では、従来の ID、パスワード、暗証番号、乱数表、合言葉を盗み取る機能をもつウイルスが更に、ウェブメールサービスのログイン情報を盗み取る機能を備えていることがわかっています。そのためワンタイムパスワードの発行をウェブメールに送信するよう設定している場合、攻撃者がウェブメールにログインすることでワンタイムパスワードが漏えいしてしまう、というものです。こうした背景からインターネットバンキング利用者の中から新たな被害が発生していると考えられます。

そのため、今回の呼びかけでは、インターネットバンキングでの不正送金を目的とした攻撃の手口について解説するとともに、インターネットバンキングを利用する際の注意点など、一般利用者ができる対策について整理をしてまとめます。

(1) 従来の手口

基本的な手口は以下の流れで、利用者のパソコンをウイルスに感染させることで不正なポップアップを画面に表示させ、インターネットバンキングの ID、パスワード、暗証番号、乱数表、合言葉を盗み取るものです。これは 2012 年 12 月の呼びかけで解説したものと同様です（図 2、図 3 参照）。

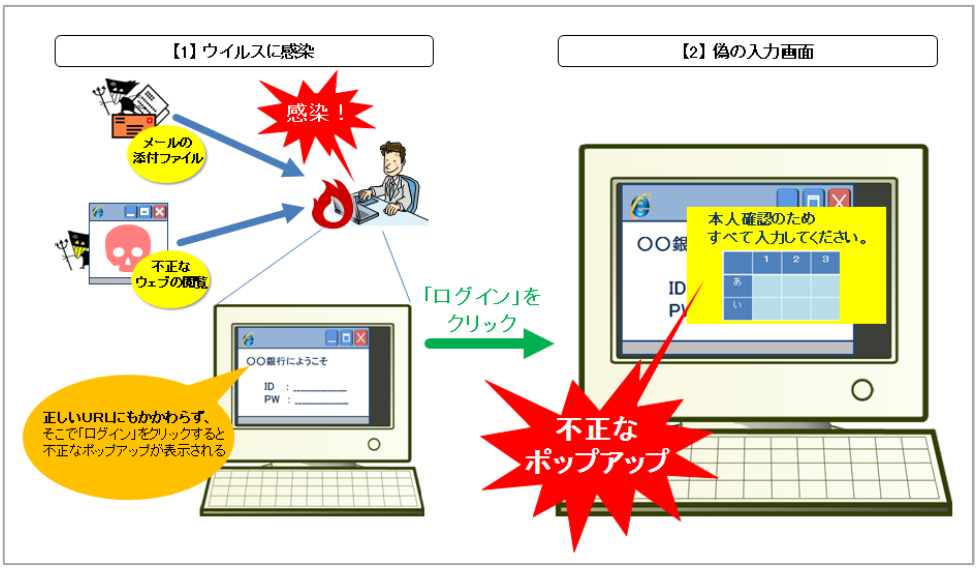

図 2：不正なポップアップ画面を表示させる手口のイメージ図

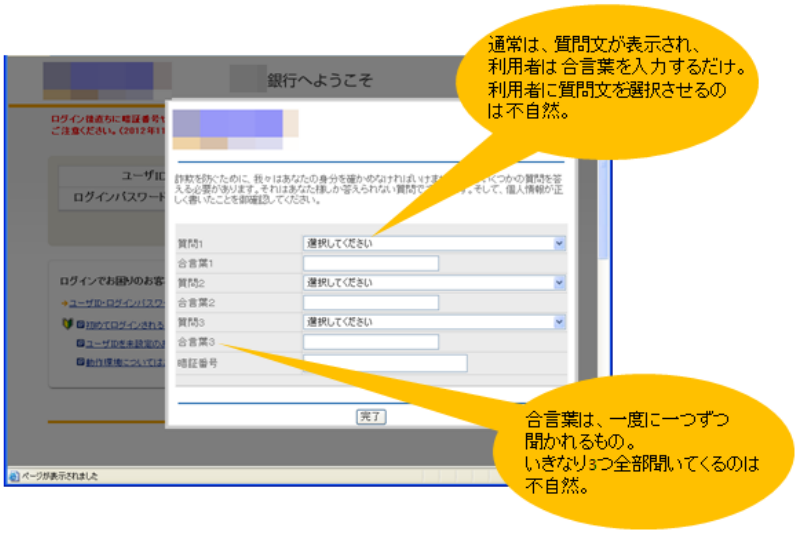

図 3：合言葉の入力を求める不正なポップアップ画面

従来の手口は、インターネットバンキングの ID、パスワード、乱数表、合言葉などの固定の認証情報のすべてを盗み取る手口でした。本来、乱数表や合言葉などによる認証は、事前に通知されている、または登録している固定の認証情報のうち、要求された一部分のみを入力することで認証を行う仕組みです。そのため、攻撃者にそれら固定の認証情報のすべてが盗み取られてしまうと、認証が機能しなくなってしまいます。

これらの手口への有効な対策は、ワンタイムパスワードと呼ばれる、都度使い捨てのパスワード（固定の認証情報でない）を用いる認証を利用することでした。

しかし、現在では、ワンタイムパスワードを用いた認証を利用していても、メールで受け取るタイプのワンタイムパスワードで、その受信を広く利用されているウェブメールに設定している場合には、認証が破られてしまう、という手口が新たに出てきました。

(2) ワンタイムパスワードを破る新たな手口

新たな手口では、認証情報などを盗み取る「第 1 ステージ」と盗み取った認証情報を悪用する「第 2 ステージ」が存在すると考えられます。

第 1 ステージ（認証情報の窃取）

新たな手口では、攻撃に用いられるウイルスが「1.従来の手口」で述べたインターネットバンキングの ID、パスワード、暗証番号、乱数表、合言葉を盗み取る機能に加えて、**広く利用されているウェブメールサービスのログイン情報を盗み取る機能を持っています。**そのため、「メールで受け取るタイプのワンタイムパスワード」を利用し、その受信を広く利用されているウェブメールに設定している場合には、認証が破られてしまう可能性があります。

「メールで受け取るタイプのワンタイムパスワード」では、以下の【1】～【2】の流れで、ワンタイムパスワードが発行され、利用者にメールで通知されます（図 4 参照）。

万が一、ウイルスに感染しているパソコンでインターネットバンキングを利用してしまうと、インターネットバンキングの ID、パスワードなどの情報だけでなく、ワンタイムパスワードを受信するためのウェブメールサービスの ID、パスワードも盗み取られてしまいます。

【1】ログイン操作、送金操作（図 4：①）
利用者は、インターネットバンキングへのログイン操作や送金操作を行います。

【2】ワンタイムパスワードの通知（図 4：②）
事前に登録したメールアドレスへワンタイムパスワードが送られます。

【3】ワンタイムパスワードの確認（図 4：③、④）
利用者は、メールで通知されたワンタイムパスワードを確認するために、ウェブメールサービスへ ID、パスワードを入力してログインし、ワンタイムパスワードを確認します。

【4】ウイルスによる認証情報の窃取（図 4：⑤）
利用者のパソコンがウイルスに感染していると、インターネットバンキングの ID、パスワード、乱数表、合言葉に加えて、ウェブメールサービスの ID、パスワードをも攻撃者に盗み取られてしまいます。

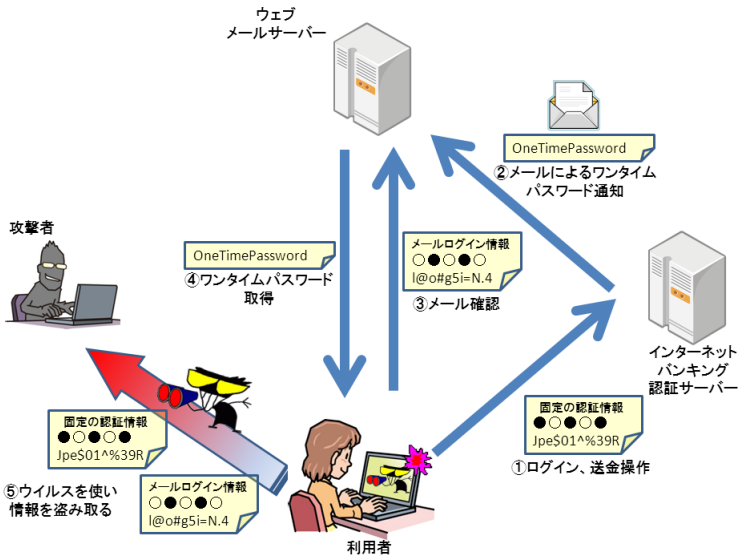

図 4：メールで受け取るワンタイムパスワードの仕組みのイメージ図

第 2 ステージ（認証情報の悪用）

攻撃者は、第 1 ステージでインターネットバンキングの ID、パスワード、乱数表、合言葉及びウェブメールサービスの ID、パスワードを盗み取ったことで、以下の【1】～【4】の流れで、利用者に気づかれないうちに、不正なログインや送金などが可能となります。

【1】ログイン操作、送金操作（図 5：①）

攻撃者は、盗み取った認証情報を使い、インターネットバンキングへのログイン操作や送金操作を行います。

【2】ワンタイムパスワードの通知（図 5：②）

事前に登録したメールアドレスへワンタイムパスワードが送られます。

【3】ワンタイムパスワードの確認（図 5：③、④）

攻撃者は、盗み取ったウェブメールサービスの ID、パスワードを使い、ウェブメールサービスへ不正にログインし、ワンタイムパスワードを確認します。

【4】窃取した認証情報を使い不正にログイン、送金（図 5：⑤、⑥）

攻撃者は、利用者に気づかれないうちに不正にネットバンキングにログインし、不正な送金を行います。

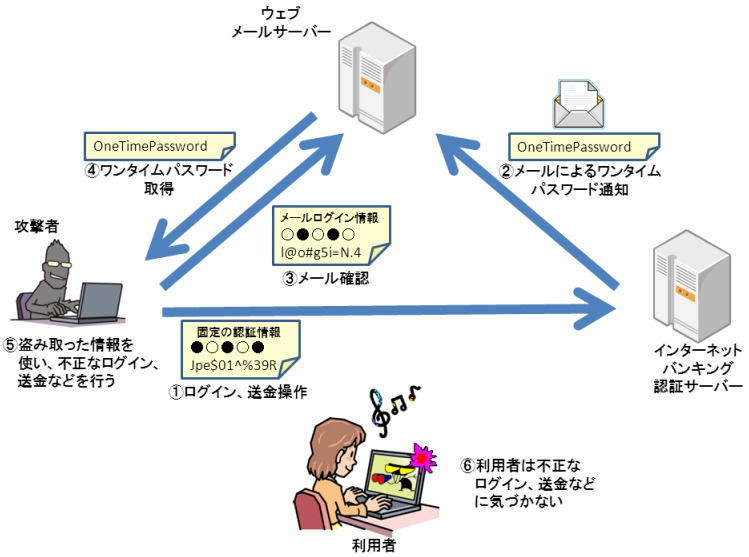

図 5：攻撃者によるインターネットバンキングの不正利用のイメージ図

なお、ワンタイムパスワードには、ハードウェアトークンよるワンタイムパスワード生成器（図 6 参照）や従来型携帯電話やスマートフォンのソフトウェア（アプリ）トークンによるワンタイムパスワード生成器（図 7 参照）もあり、これらは今回の攻撃に対して安全です。

図 6：ハードウェアトークンよるワンタイムパスワード生成器

図 7：従来型携帯電話やスマートフォンのソフトウェア（アプリ）トークンによる
ワンタイムパスワード生成器

(3) 対策

対策としては、一般的なウイルスに感染しないための対策と、インターネットバンキング特有の対策があります。

●対策 1 ウイルス感染を防ぐ

・使用しているパソコンの OS やアプリケーションなどの脆弱性を解消する

使用しているパソコンの OS やアプリケーションなどの脆弱性（ぜいじゃくせい：セキュリティ上の弱点）を悪用されると、ウェブサイトを閲覧しただけで、ウイルスに感染する可能性があります。OS や、インストールされているアプリケーションソフトウェアに、最新の更新プログラムが公開されたら速やかに適用して、脆弱性を解消してください。

IPA では、利用者のパソコンにインストールされている主なソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認できるツール「MyJVN バージョンチェッカ」を公開しています。是非ご利用ください。

（ご参考）

・MyJVN バージョンチェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/vccheck.html

・セキュリティソフトを導入し、ウイルス定義ファイルを最新に保ち、使用する

セキュリティソフトは万能ではありませんが、重要な対策の一つです。セキュリティソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入してしまったウイルスを駆除することができます。近年のウイルスは、パソコン画面の見た目や動作からでは感染していることが分からないものも多いため、ウイルスの発見と駆除には、セキュリティソフトが有効です。

一般利用者向けのセキュリティソフトとしては、ウイルスの発見と駆除だけでなく、危険なウェブサイトを閲覧しようとした時にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

●対策 2 インターネットバンキング特有の対策

・ワンタイムパスワードを適切に利用する

各行のセキュリティサービスの 1 つとして、ワンタイムパスワードが提供されている場合があります。ワンタイムパスワードを適切に利用することで、過去のフィッシングや不正なポップアップを用いた手口などによる不正送金の被害をほとんど防げたと考えられます。ご利用のインターネットバンキングでワンタイムパスワードが提供されていれば、積極的に利用しましょう。ただし、ワンタイムパスワードをメールで受け取る場合には、携帯電話会社から提供されているメールアドレスの利用を推奨します。携帯電話会社のメールアドレスは、ウェブメールなどとは異なり、ID、パスワードによる認証でないため不正にメールを取得することが難しくなっています（図 8 参照）。

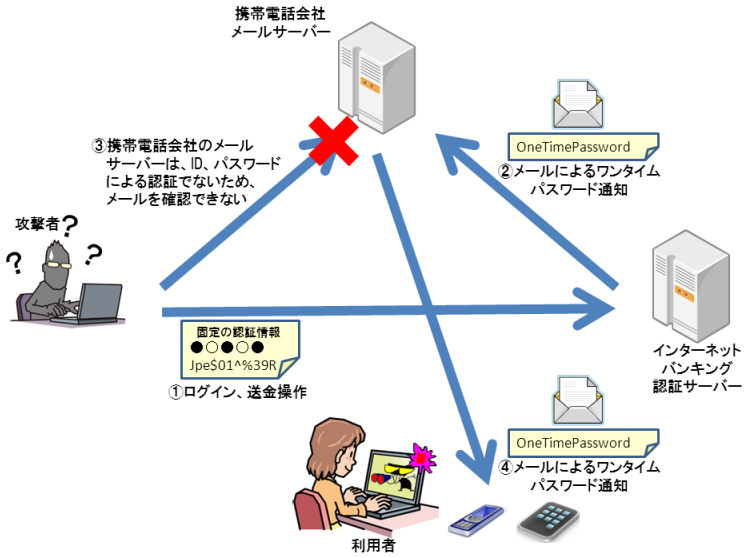

図 8：携帯電話のメールでワンタイムパスワードを受け取る場合のイメージ図

・乱数表、合言葉などをすべて入力しない

インターネットバンキングなどの金融機関が第二認証情報（乱数表や合言葉など）のすべての入力を求めることは通常ありません。第二認証情報「すべて」の入力を促す画面が表示された場合は、絶対に情報を入力しないようにしてください。

通常利用時と異なる入力の要求があった場合は、入力せずに、サービス提供元に確認をしてください。

・メール通知サービスを携帯電話宛に設定する

各行のセキュリティサービスの 1 つとして、振込み完了通知等のメール通知サービスが提供されている場合があります。メール通知サービスを利用することで、万が一、第三者が不正送金などを行ったとしても、すぐに気づくことができるため被害を最小限に抑えることができますので、積極的に利用しましょう。その際は、常にメールでの通知を確認できるように、携帯電話などモバイル端末で受信できるメールアドレスを登録しましょう。

・ブックマーク、バンキングアプリを利用する

フィッシング対策として、インターネットバンキングなどの重要な情報を扱うサイトへアクセスする際には、ウェブページの検索結果やメールのリンクからアクセスするのではなくて、予めそれらのサイトをブックマークに登録しておき、ブックマークからアクセスを行うようにしましょう。

また、従来型携帯電話やスマートフォンであれば、インターネットバンキングを利用するための専用のアプリケーションが各行より公開されている場合があります。公式のバンキングアプリを利用することでフィッシングの被害に遭う危険性を低減できますので、公式のバンキングアプリが公開されていないか確認しましょう（図 9 参照）。

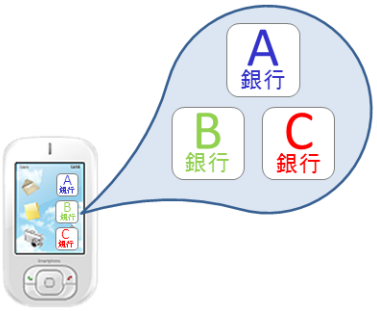

図 9：スマートフォン向けバンキングアプリ

■お問い合わせ先
IPA 技術本部セキュリティセンター 加賀谷／田中
Tel:03-5978-7591 Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp