Information-technology
Promotion
Agency, Japan

第 12-32-267 号
2012 年 12 月 3 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 ネット銀行を狙った不正なポップアップに注意！ 」
～ “乱数表”や“合言葉”の正しい使われ方を知り、自己防衛を ～

パソコンでインターネットバンキングにログインしようとすると、ウイルスが不正なポップアップ画面を表示して、合言葉や乱数表を利用者に入力させ、これらの情報を窃取しようとする新たな手口の犯行が発生しているとして、警察庁と各金融機関が注意を呼び掛けています。

従来のフィッシング詐欺は、利用者を「見た目はそっくりだが完全に別の偽サイト」へ巧みに誘導して、個人情報や金銭に関わる情報を窃取するケースが大部分でした。また 2011 年 9 月には、銀行を装った偽メールにウイルスが添付されていて、そのウイルスを実行するとログイン情報や乱数表の内容の入力を促す偽の画面が表示されるといった手口も出現しました。

今回の新たな手口では、「本物のサイトにアクセスしたら、“途中から”偽の画面が出現する」という点で、今までのフィッシング詐欺の手口と決定的に異なります。本物のサイトのログイン後の表示であるために利用者が信用してしまい、情報を入力して被害が広がったと推測されます。

IPA ではこのウイルスの動作確認を行いました。その手口と動作を解説し、被害に遭わないための対策を紹介します。

（1） 不正行為の手口

本物のサイトに不正なポップアップ画面を出現させる手口を以下に示します。

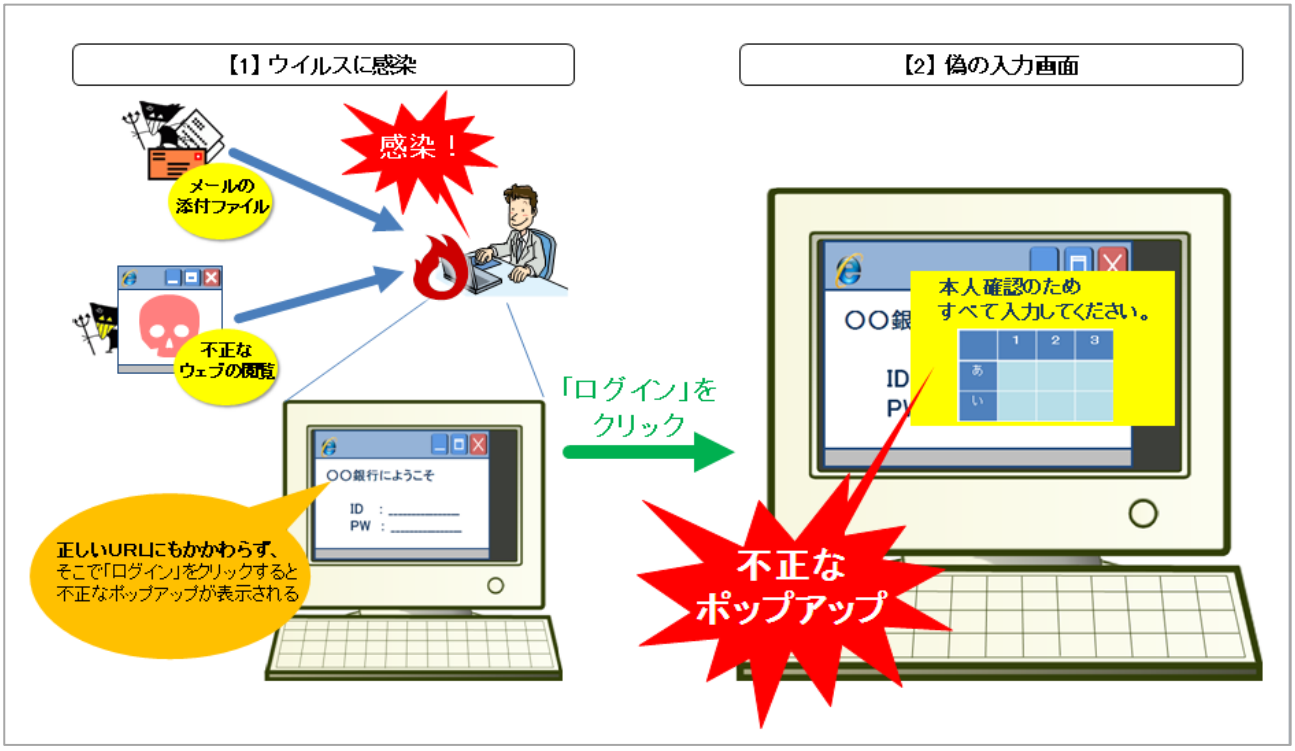

図 1：不正なポップアップ画面を出現させる手口のイメージ図

【1】ウイルスに感染させる

悪意ある者が、一般利用者のパソコンをウイルスに感染させる方法としては、以下のものが考えられます。

・ウイルスを添付したメールを送りつける。

・迷惑メールや SNS 上のコメントや投稿にウイルス配布サイトの URL を記載して、誘導する。
・本物のウェブサイトを改ざんして、別のウイルス配布サイトへ誘導する。

【2】不正なポップアップ画面で入力画面を表示させる

そのパソコンでインターネットバンキングのサイトにログインする際に、乱数表や合言葉などの入力を促す、不正なポップアップ画面が表示されます。

【3】パソコン利用者が情報を入力してしまう

利用者は、本物のサイトが入力を促しているものと思い、乱数表や合言葉などを入力してしまいます。（その後、入力された情報が悪意ある者へ渡ってしまう仕組みになっていると考えられます。）

この手口では、本物のサイトの利用中に、本物の画面にかぶさるような形で不正なポップアップ画面が表示されるため、ブラウザに表示されている URL からは、それが偽の画面であることを判別することができません。また、インターネットバンキングサイトが SSL に対応している場合でも、SSL による本物のサイトの利用中に不正なポップアップ画面が出現※1 します。

※1 「SSL による本物のサイトの利用中に不正なポップアップ画面が出現」:
SSL（Secure Socket Layer）とは、インターネット上での通信を暗号化や、ウェブサイトの「身元保証」を提供する技術です。
SSL であればアクセス先ウェブサイトの「身元が保証」されるので、ブラウザに表示される鍵マーク等を確認することでフィッシング被害を防ぐことが可能です。しかし今回のウイルスは、利用者が SSL により「本物の」ウェブサイトにアクセスした後に、その画面自体をパソコン内部で改ざんしてしまう機能を備えています。

（2） ウイルスの動作検証結果

IPA は、今回問題になっている、不正なポップアップ画面を表示させるタイプのウイルスと思われるプログラムを入手しました。
このプログラムを検証したところ、特定の銀行にログインする際に、実際に不正なポップアップ画面が表示されることを確認しました。

【1】通常のログイン画面

下記図 2 は、あるインターネットバンキングサイトの通常のログイン画面です。

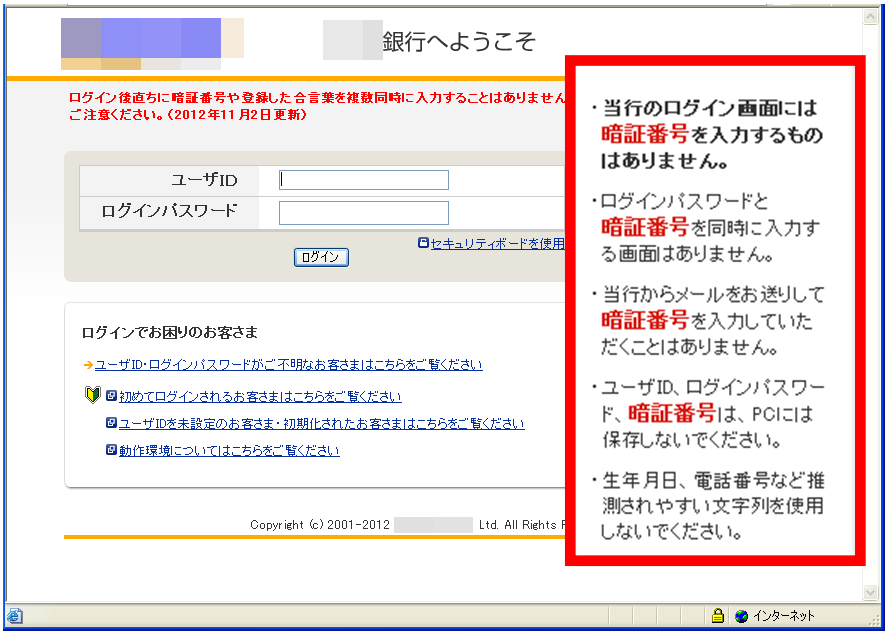

図 2：通常のログイン画面（注意書き部分を拡大）

【2】ウイルスによって改ざんされた偽の画面（偽のログイン画面と情報入力画面）

パソコンがこのウイルスに感染している状態で【1】と同じログイン画面にアクセスすると、少し異なる画面が表示されます（図 3）。この時の URL は【1】と同じであるため、URL からこれを不正なページと判断することはできません。

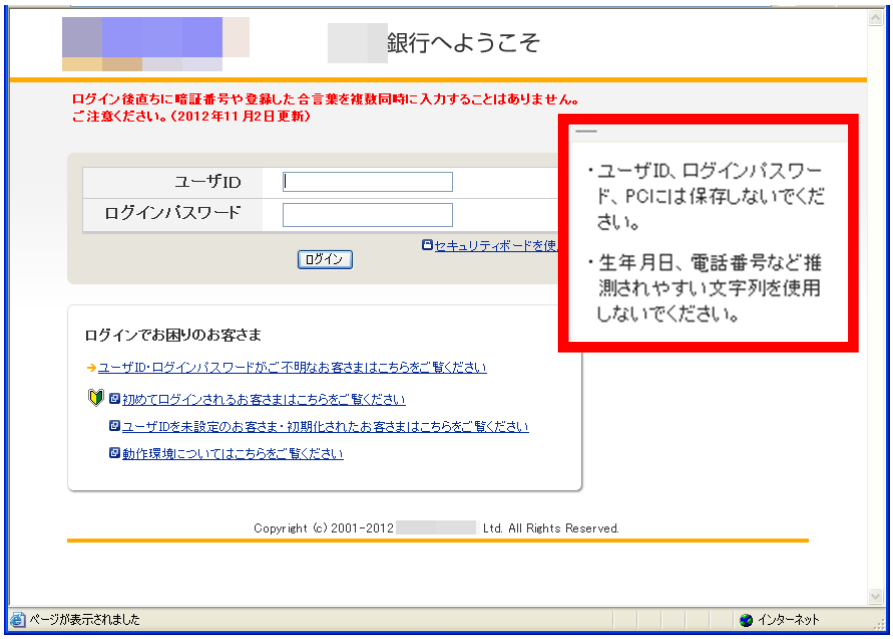

図 3：偽のログイン画面（注意書き部分を拡大）

この状態で「ユーザ ID」と「ログインパスワード」を入力し、「ログイン」ボタンをクリックすると、以下図 4 のように、利用者が**既に設定してある「質問」と「合言葉」の入力を要求**する不正なポップアップ画面が表示されます。ここで「質問」と「合言葉」を入力してしまうと、これらの情報が悪意ある者へと窃取されてしまうと考えられます。

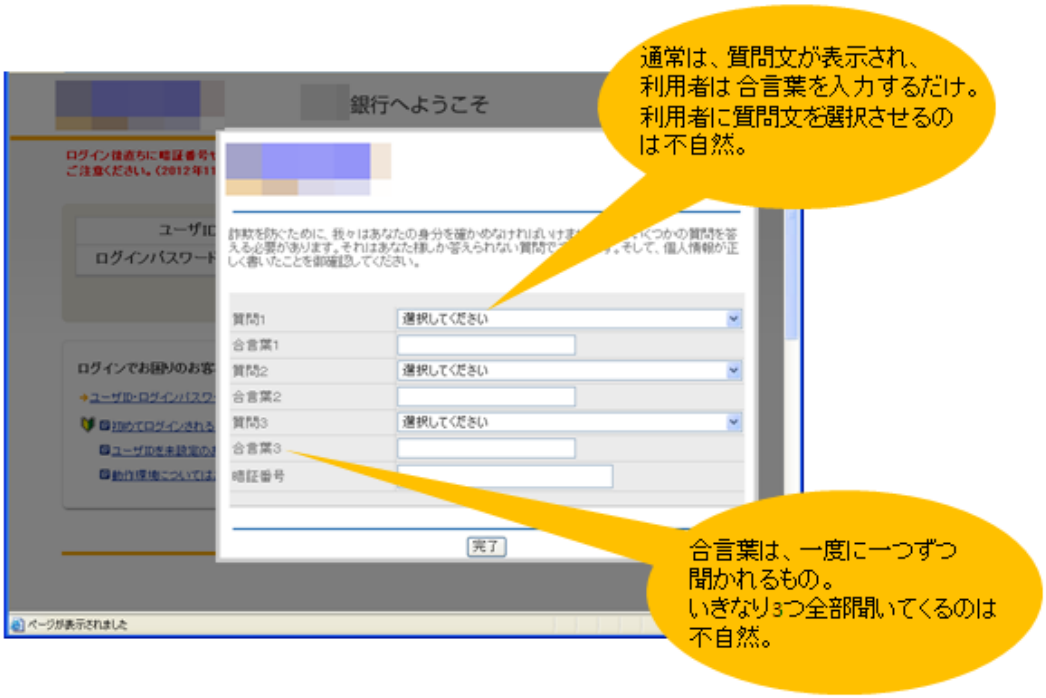

図 4：不正なポップアップ画面

（3）対策

一般利用者がこのようなウイルスに感染させられた経緯は不明ですが、パソコンをウイルス感染から防御しつつ、インターネットバンキング利用時に注意を払うことで、被害に遭わずに済んだ可能性が高いと考えられます。

●対策１　ウイルスに感染しないために

・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は、最新の更新プログラムを適用して、脆弱性を解消してください。定期あるいは緊急に更新プログラムが公開されますので、公開された場合にはすぐに更新プログラムを適用してください。

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。

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

・ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保ちながら使用する

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。ウイルス対策ソフトを導入し、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、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、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利用時の注意点

・乱数表や合言葉などを一度にすべて入力しない

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）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。

通常利用する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。

第二認証情報について

第二認証情報とは、利用者がインターネットバンキングサイト利用時において、送金などの重要な操作を行う際に要求されるものです。多くの数字が記載された乱数表が事前に送付されてそれを用いるケースや、複数の質問に対する回答（合言葉）を事前に登録しておくケースが多いようです。

乱数表には多くの数字が記載されており、本人確認時には、インターネットバンキングサイトがランダムに指定した箇所の数字のみを入力します。また合言葉は、「利用者だけが知り得る情報」を、質問と合言葉の組み合わせとして事前に複数登録しておくもので、本人確認時には、その中から一部の質問に関する合言葉を入力します。

つまり、第二認証情報とは、インターネットバンキング側と利用者の二者だけが共通で知っている複数の情報のうち、インターネットバンキング側がその中の一部の情報だけを利用者に入力させることで、本人確認を行うものです。

この乱数表や合言葉の使われ方を理解することで、すべての情報の入力を促された時に「怪しい」と気付き、情報の入力を思い留まることが期待できます。

●対策３　一歩進んだお勧めの対策

・パーソナルファイアウォール※2 を適切に設定して使用する

パーソナルファイアウォールを導入し、設定を厳しくして自分が許可したプログラムだけを通信可能とすることにより、**万が一ウイルスに感染してしまっても、そのウイルスが外部と通信することを防ぎ、さらにはウイルスの存在に気付くことができる可能性があります。**

※2 パーソナルファイアウォール：
個々の端末（パソコンやモバイル機器など）に導入するもので、端末と外部ネットワークの間の通信を制御するソフトウェアです。通常、“事前に許可した通信以外を通過させない”、“許可するプログラムを事前に登録しておき、未許可のプログラムの通信を遮断する”といった機能を持ちます。
製品単体としても販売されていますが、「統合型ウイルス対策ソフト」と呼ばれる製品の中にパーソナルファイアウォール機能を合わせ持つものもあります。

・ワンタイムパスワードのサービスを利用する

インターネットバンキングやオンラインゲームなどでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを窃取するウイルスに感染していても、一度きりのパスワードのため、仮に窃取されてもその後悪用されることはありません。また、フィッシングの手口に引っ掛かり、ID やパスワードを窃取されたとしても、同様に、悪用されることはありません。ただし、ワンタイムパスワード生成器を他人に渡さない、信頼できるサイトに対してのみパスワード入力する、などの基本的対策は必須です。

上記対策のほか、日ごろから、**こうした便利なサービスを利用する際にはリスクをともなう**という意識を持つことも大切です。

（4）こんなときは…

今回ご紹介した不正なポップアップ画面を表示させるウイルスを検知してしまった、ウイルスに感染しているかもしれない、などといったご心配やご相談がありましたら、IPA 安心相談窓口までご連絡ください。

まずは、ご相談ください。

	安心相談窓口の問合せ先
電話	03-5978-7509 （オペレータ対応は、平日の 10:00～12:00 および 13:30～17:00）
E-mail	anshin@ipa.go.jp ※このメールアドレスに特定電子メールを送信しないでください。
FAX	03-5978-7518
郵送	〒113-6591 東京都文京区本駒込 2-28-8 文京グリーンコート　センターオフィス 16 階 IPA セキュリティセンター「情報セキュリティ安心相談窓口」宛

■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／青木
Tel:03-5978-7591　Fax:03-5978-7518
E-mail: isec-info@ipa.go.jp