第 14-11-316 号
2014 年 7 月 1 日
独立行政法人情報処理推進機構

今月の呼びかけ

「 オンラインバンキングの正しい画面を知って、金銭被害から身を守りましょう！ 」

オンラインバンキングにおける不正送金の被害が増加傾向にあります。警察庁によれば 2014 年の国内における被害額は、5 月 9 日の時点で 14 億円を超え、既に昨年の被害総額を超えたとあります※1。

IPA への相談件数は下図のとおりです（図 1 参照）。

図 1：IPA に寄せられたオンラインバンキング関連の相談件数（過去 1 年半）

IPA では過去 3 回に渡り「今月の呼びかけ」※2においてもオンラインバンキングに関する注意喚起を行っています。しかし前述のとおり被害が後を絶たず、手口にも変化がみられることから、改めて呼びかけを行います。

金銭被害を食い止めるには、**騙されないための注意深さと知識が必要で、利用者自身で何が正しいのかを「知る」ことが必要**です。具体的には、オンラインバンキングの「正しい画面」を知ることです。それさえ知っていれば、パソコンが万が一ウイルスに感染しても、異常に気付くことができます。

今月の呼びかけでは、オンラインバンキングを狙ったウイルスを使った巧妙な手口、および金銭被害に遭わないための対策について説明します。

---

[1] 警察庁：インターネットバンキングに係る不正送金事犯に関連する不正プログラム等の感染端末の特定及びその駆除について　http://www.npa.go.jp/cyber/goz/index.html

[2] 2011 年 9 月の呼びかけ：「あなたの銀行口座も狙われている！？」― SpyEye（スパイアイ）ウイルスに注意！ ―
http://www.ipa.go.jp/security/txt/2011/09outline.html
2012 年 12 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！」
http://www.ipa.go.jp/security/txt/2012/12outline.html
2013 年 9 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！」
http://www.ipa.go.jp/security/txt/2013/09outline.html

（1） 従来の手口と新しい手口

オンラインバンキングにおける不正送金の手口は巧妙化しています。ここでは従来の手口と、巧妙になった新しい手口を説明します。

オンラインバンキングにおける不正送金の従来の手口は、次の通りです（図 2 の「従来の手口」）。

① 利用者のパソコンにウイルスを感染させることで、不正なポップアップ画面を表示させる。
② その画面に、送金に必要な情報（ID、パスワード、乱数表の数字など）を利用者に入力させる。
③ その結果、**送金に必要な情報が第三者に渡ってしまう**。
④ 第三者は、窃取した情報を悪用して手動で不正送金を行う。

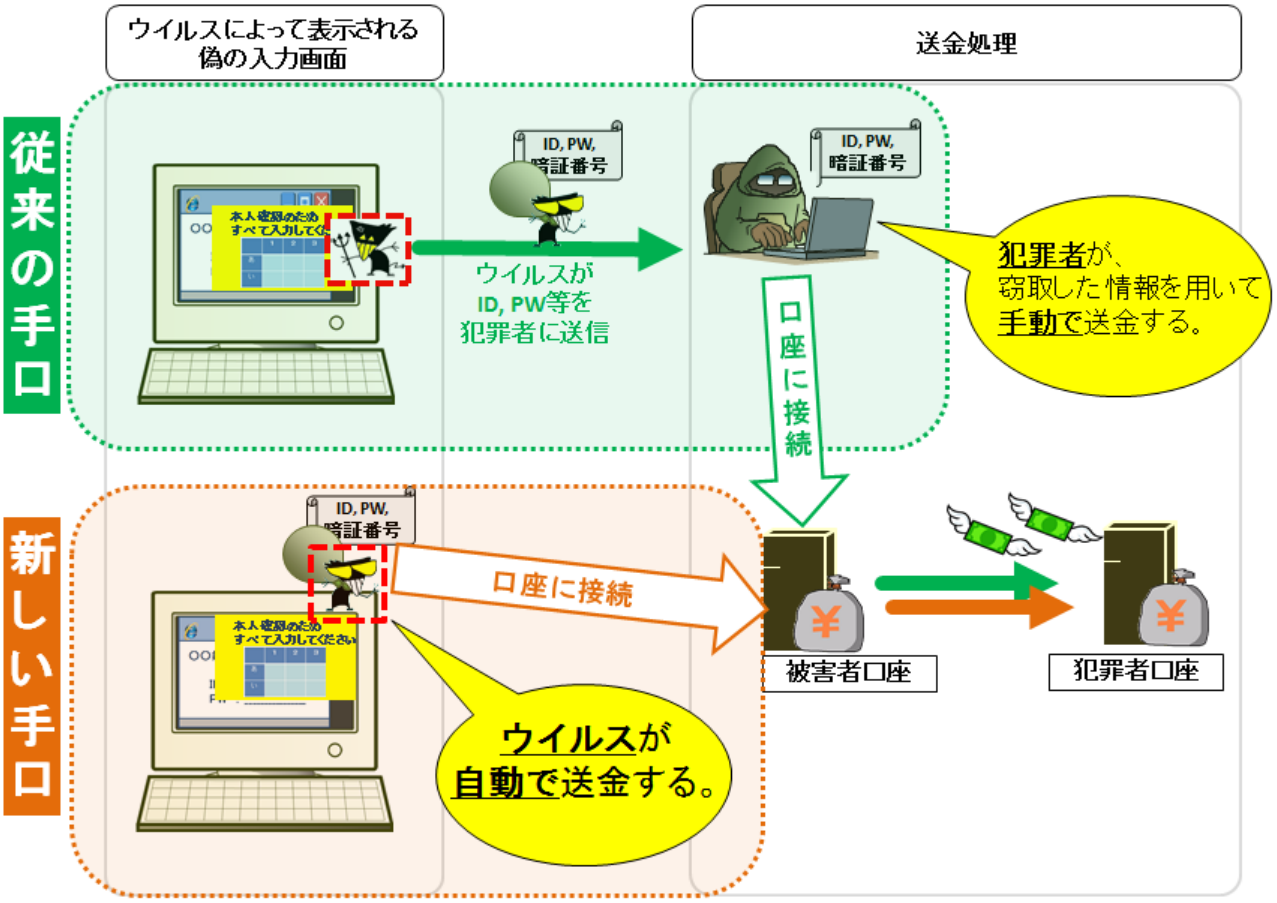

図 2：オンラインバンキングを狙ったウイルスの「従来の手口」と「新しい手口」

しかし 2014 年 3 月に、窃取した情報を悪用して、その場でリアルタイムに送金処理を行う新たなウイルスが確認されました[※3]。新たなウイルスによる手口は次の通りです（図 2 の「新しい手口」）。

---

[3] 日本経済新聞「三井住友銀、新手のネット不正送金被害を発表」
http://www.nikkei.com/article/DGXNASFL120SX_S4A510C1000000/
msn 産経ニュース「ネットバンキング入力と同時に不正送金　新種ウイルス確認　三井住友銀、数十件被害」
http://sankei.jp.msn.com/affairs/news/140512/crm14051220160015-n1.htm
朝日新聞 DIGITAL「ネットバンク不正深刻　三井住友銀、最新対策後も被害」
http://www.asahi.com/articles/DA3S11131726.html

① 利用者のパソコンにウイルスを感染させることで、不正なポップアップ画面を表示させる。
② その画面に、送金に必要な情報（ID、パスワード、乱数表の数字など）を利用者に入力させる。
③ 入力させた情報が即座に悪用され、**第三者の口座への不正送金がリアルタイムに行われてしまう**。

新たなウイルスは送金に必要な情報の入力と同時に送金を完結させてしまうものでした。この件を受けて金融機関側も利用者に対して注意喚起をしています※4。

この手口は犯罪者にとって手っ取り早く金銭を収受できるよう工夫が図られています。一方利用者にとってはうかつな認証情報の入力が、不正送金被害に直結することを意味します。

しかし**“パソコンにウイルスを感染させ”、その後“そのウイルスに不正な画面を表示させる”という点で従来の手口と共通**しています。つまり不正な画面であることに気が付けば、金銭被害に遭わずに済みます。

（２） 「正しい画面」と「不正な画面」の見分け方

オンラインバンキングのサイトには、利用者への情報として「正しい画面」と「不正な画面」を示しているところがあります。いまや利用者がオンラインバンキングの利用に際し、この**「正しい画面」と画面遷移を把握しておくことは必須といえます**。

「不正な画面」は既知のウイルスによって表示されるもので、ウイルスや手口が異なれば、出現する「不正な画面」も多種多様になると考えられます。そのため「正しい画面」を知っていることは、それと異なる画面が現れた際に異変に気付くことができ、金銭被害から身を守ることができます。

図３は、実際にみずほ銀行がサイト上で掲載している「正しい画面」です※5。

---

4 三井住友銀行
「インターネットバンキングの情報を盗み取ろうとするコンピューターウイルスを使った新たな手口について」
http://www.smbc.co.jp/news/j600880_01.html
「インターネットバンキング（SMBC ダイレクト）の情報を盗み取ろうとするコンピュータウイルスにご注意ください」
http://www.smbc.co.jp/security/popup.html

5 みずほ銀行
「当行が合言葉の入力をお願いする正規の流れ」
http://www.mizuhobank.co.jp/crime/info121028.html#nagare

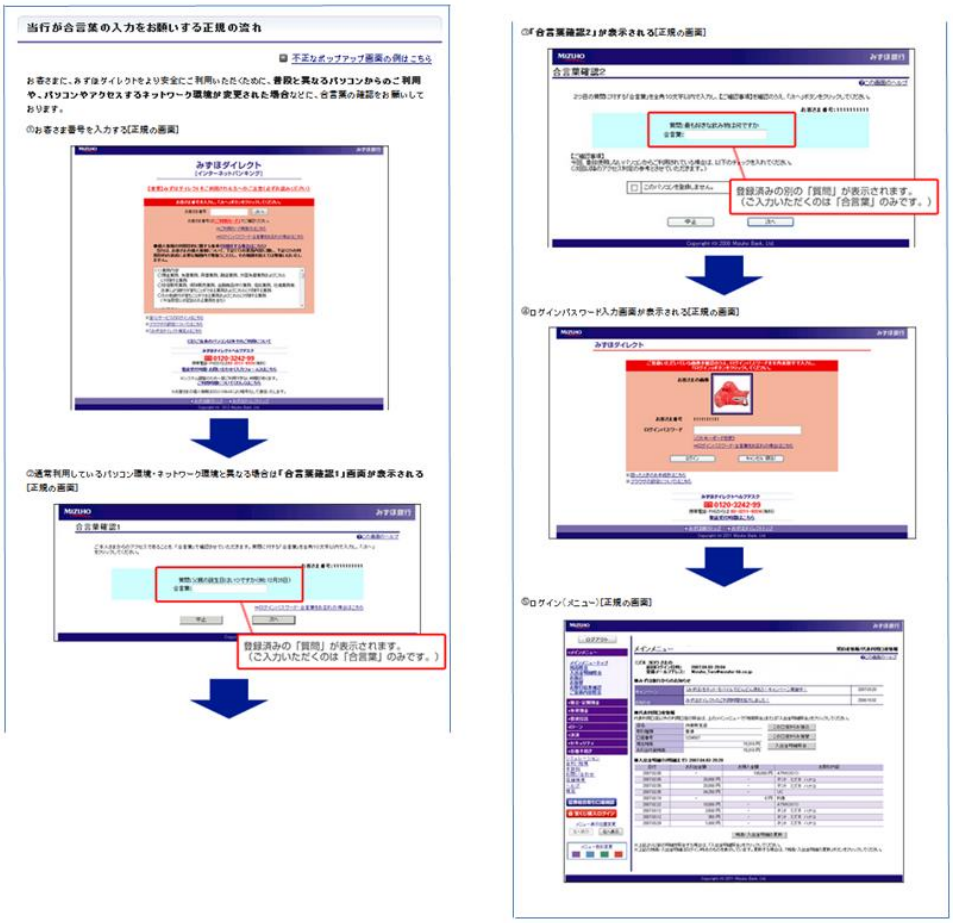

図３：みずほ銀行が掲載している「正しい画面」

またオンラインバンキングのサイトによっては、実際の「正しい」取引を体験できるデモページを用意している金融機関もあります※6。

オンラインバンキングでは、このように利用者に「正しい画面」を提示している場合がありますので、利用中のオンラインバンキングのサイトで「正しい画面」が掲載されているかを確認してください。掲載されていた場合は、**画面のスクリーンショットをパソコンに保存しておくかプリントアウトしておき、オンラインバンキング利用時には常に正しい画面と画面遷移に照らし合わせながら利用してください**。

もしオンラインバンキング利用時に「正しい画面」と異なる画面が現れた場合、ウイルス感染が原因の場合以外にも、オンラインバンキング側のシステム変更の可能性があるため、以下の対応を取ってください。

- 金融機関本体のサイトを確認し、オンラインバンキングの画面の変更の有無を確認する。もしくは問い合わせ窓口に確認する。
- もしシステム変更によるものではない場合、ウイルス感染が疑われますのですぐにオンラインバンキングの利用を停止し、セキュリティソフトによる駆除や後述する感染を防ぐための対策を行ってください。

---

[6] 三井住友銀行：インターネットバンキング（SMBC ダイレクト）体験版
http://www.smbc.co.jp/kojin/direct/demo.html
大垣共立銀行：スーパーOK ダイレクト体験版
https://www.okb.co.jp/okdirect/demo.html

（３） ウイルスに感染しないために

ウイルス感染の手口には、ウェブサイトに仕掛けをし、閲覧しただけで感染させる手法をはじめ、いくつもありますが、利用者にとって必須の基本対策に変わりはありません。一方で、利用者がきちんと対策を行っていても、以下の要因によりパソコンがウイルスに感染する場合があり、ウイルスに感染する可能性を完全に排除できないのも現実です。

・いわゆる「ゼロデイ攻撃」という修正プログラムが提供される前に、ソフトウェアの脆弱性を悪用されて、ウイルスに感染してしまう。
・企業のサーバーが不正アクセスを受け、サーバー上のファイルがウイルスに置き換えられる※7。それを一般利用者がウイルスと知らずにダウンロードし、ウイルスに感染してしまう。

しかし下記の対策を確実に実施することは、オンラインバンキングに関するウイルスのみならず、多くのウイルスからパソコンを守るのに有効な手段となります。

【1】使用しているパソコンの OS とソフトウェアの脆弱性を解消する

OS やインストールされているソフトウェアに、最新の更新プログラムが公開された際には、速やかに適用し、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。利用してください。

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

【2】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感染していることが分かりづらいものも多く、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。

オンラインバンキングの普及により、窓口や ATM に出向く必要がなくなるなど、利便性は大幅に向上しましたが、それと相まってリスクも増大しています。ぜひ、他人事と思わずにこれらの対策を実施し、被害防止に努めてください。

■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

---

7 最近の事例：
株式会社シーディーネットワークス・ジャパン「セキュリティ侵害に関するお知らせ」
http://www.cdnetworks.co.jp/pressrelease/2254/
シマンテック社：「脆弱性を悪用しないマルウェア Bankeiya が日本のユーザーを狙う」
http://www.symantec.com/connect/blogs/bankeiya