フィッシング対策協議会
ガイドライン策定ワーキンググループ

インターネットバンキングの
不正送金被害にあわないためのガイドライン

あなたも狙われている！

●インターネットバンキングを狙った不正送金が急増しています！

警察庁の発表[1]によれば、インターネットバンキング利用者の情報を盗み取り、利用者の口座から不正送金する事案の被害が急増しています。

平成 24 年にはわずか 64 件、約 4,800 万円だった被害額が、平成 27 年には 1,495 件、約 30 億 7300 万円の被害額に達しています。

●不正送金の手口

同種の詐欺事件の手口としては「フィッシング（phishing）」という方法を用いるものがよく知られています。これは金融機関をかたった巧妙な電子メールにより金融機関の HP そっくりなページに誘導し、ID・パスワードや乱数表などの情報を入力させて盗み取るものです。

これに加え、最近、利用者のパソコンをウイルスやマルウエア（スパイウエアなど）に感染させて、それらの情報を盗み取る手口も多発しています。

平成 26 年には後者の手口によって、多くの金融機関で被害が発生しました。これらの手口の急速な巧妙化を背景に不正送金被害が増加しており、注意が必要です。

不正送金防止、2 つの鉄則！

第一の鉄則：第二認証情報（乱数表・ワンタイムパスワードなど）の入力は慎重に！

【ポイント】

絶対に乱数表に記載された全ての乱数を同時に入力してはいけません。また、乱数の一部だけ入力させたり、それを複数回繰り返したりする巧妙な手口もあります。銀行のサイトで偽画面の具体例を掲載して注意を呼びかけていることがあります。そのような注意喚起も活用・参照して、乱数表などの入力は慎重に行いましょう。

最近はワンタイムパスワードの利用が増えています。ワンタイムパスワードは、スマートフォンのアプリやハードウエアトークン、メールでの通知によるものなどがあります。なお、ワンタイムパスワードをメールで通知する方式の場合、メールの通知先として普段インターネットバンキングに利用しているパソコンのアドレスとは別のアドレスを登録することも有効です。

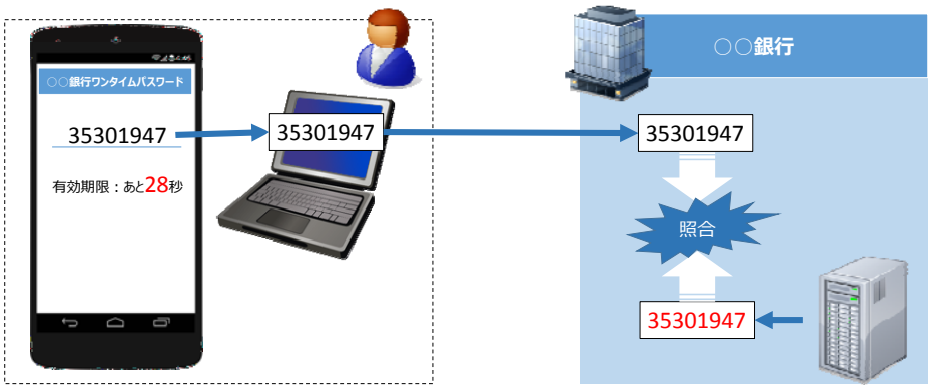
【説明】

インターネットバンキングでは、利用者と銀行が直接対面せずに取り引きすることから、本人による利用であることを、様々な方法（「認証方式」）で確認しています。

最近利用の増えているワンタイムパスワードにはいろいろな方式がありますが、代表

[1] http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf

的なものには、スマートフォンのアプリを利用するものがあります。取り引きの都度、アプリに表示される一回限りのパスワードを銀行サイトの画面入力することで安全に取り引きを行うことができます。アプリと銀行のそれぞれで、同じ計算方式でパスワードを計算することにより、両者が計算したパスワードが同じであれば正しい利用者であると認証できます。この計算には時刻や利用者の固有情報を用いるため、時刻毎・ユーザー毎に異なるパスワードが都度生成されます。



スマホアプリによるワンタイムパスワードの例

偽アプリも出回っているため、アプリは取り引き先の銀行のホームページなど必ず信用できる先からダウンロードしてください。

また ID と固定パスワード（第一認証情報）による認証に加え、資金移動等などのタイミングで乱数表等などの第二認証情報の入力を求める方式がしばしば見られます。

	ア	イ	ウ	エ
1	23	78	92	91
2	61	49	83	11
3	12	33	10	27
4	85	56	08	69

乱数表の例

乱数表を用いた認証で大事なことは、乱数表を他人に知られないようにしっかりと保管することです。

しかし、乱数表そのものの保管だけでは十分ではありません。パソコンで入力する際の情報管理にも注意が必要です。昨今の情報を盗み取る手口においては、利用者を巧みに偽画面へ誘導した後、乱数表に記載された数字を入力させて詐取する実例があります。乱数表の情報が第三者に盗まれてしまうと、利用者本人になりすました第三者に不正送金されてしまう危険があります。平成 25 年には、そのような手口で多数の被害が発生しました。

金融機関では、パソコンのウイルス感染により、パソコン内のデータだけでなく、そのパソコンを利用したネットワーク上のサービスも乗っ取られることで、第三者に ID／パスワードを詐取されて不正送金される被害が発生しています。金融機関のインターネットバンキングなどの ID／パスワードをパソコン、スマートフォン、Ｅメール、クラウドサーバー、ネットワーク上のサービス等に保存しないでください。

第二の鉄則：インターネット利用機器を最新の状態に保とう！

ニセの画面表示などで、あなたの口座情報を盗もうとする手口に対抗するには、インターネット利用をしている機器のソフトウエアやアプリを最新の状態に保つことが重要です。

以下の鉄則を参考に利用している機器を最新な状態に保ち、被害にあわないようにしましょう。

パソコン編

- **ソフトウエアのこまめなアップデートで常に最新状態に！**
  - Java や Adobe Reader、Web ブラウザなどのアップデートは、更新案内に従いできるだけできるだけ早く行い、最新の状態を保ちましょう。利用している Java が最新状態かチェックできる無償サービスもありますので活用しましょう。＊注意参照
- **ウイルス対策ソフトを利用！ 検知用データは常に最新に！！**
  - ウイルス検知用データは、アップデートを自動更新にするなどして、常に最新の状態にしましょう。
- **基本ソフト（OS）のアップデートも忘れずに！！！**
  - アップデートの自動更新を有効に設定しておくことがお勧めです。常に最新の状態に保ちましょう。
  - セキュリティのサポートがされなくなった古いパソコンの基本ソフト（OS）（例：Windows XP など）の使用はやめて、新しい基本ソフト（OS）を使いましょう。
- **怪しいサイトへのアクセスは避けましょう！**
  - 見慣れないメールからの Web アクセスや、怪しい情報を掲示したサイトからのアクセスはやめましょう。

注意：

●Java 最新バージョン利用の簡易チェック【MyJVN バージョンチェッカによる脆弱性対策チェック】
MuJVN サイト　http://jvndb.jvn.jp/apis/myjvn/　より利用可能。

スマホ・タブレット編

- **アプリのこまめなアップデートで常に最新状態に！**
  - インストールされているアプリのアップデートは、更新案内に従いできるだけできるだけ早く行い、最新の状態を保ちましょう。
- **セキュリティソフトを利用！ 検知用データは常に最新に！！**
  - 検知用データは、アップデートを自動更新にするなどして、常に最新の状態にしましょう。
- **基本ソフト（OS）のアップデートも忘れずに！！！**
  - アップデートの自動更新を有効に設定しておくことがお勧めです。常に最新の状態に保ちましょう。
- **アプリは正規アプリマーケットからインストールしましょう！**
  - 金融機関とは関係のない、第三者が作成したアプリなどは十分に注意して安易なインストールを避ける（特に無料アプリ）ようにしましょう。
  - Android 端末の場合、設定の中の「セキュリティ」の「不明な提供元 - Play ストア以外で購入したアプリケーションのインストールを許可する」を有効にしないようにしましょう。

チェックリスト

怪しいメールを受け取ったら落ち着いて以下のチェックリストで確認しましょう！

★金融機関からのメールを受け取った場合

□ 自分と取り引きのある金融機関ですか?

→取り引きがない場合は、開封せず削除を推奨します。取り引きのある金融機関が電子署名を採用している場合は署名を確認しましょう。（※1）

□ いつも受け取る内容と比較して、書式や言い回し・トーンなどに違いや違和感はないですか?

→偽メールかどうか判断がつかない場合は、取り引きのある銀行のホームページの注意喚起を確認しましょう。偽画面の具体例を掲載していることがあります。それでも判断がつかない場合は、銀行に問い合わせましょう。

□ メールの内容が、「緊急」「重要」「セキュリティ」などを強調し、該当金融機関の Web ページにログインする情報の確認や入力を求めていないですか?

→この場合、偽メールである可能性が極めて高いです。

□ メール文中にある Web サイトへのリンク先 URL は見覚えがありますか?

→メール文面中の URL と実際に飛ぶ先の URL が異なるように細工をすることが可能です。これを見破るためには、リンクまたは URL 部分にマウスカーソルを乗せてみます。表示されたリンク先の URL が利用者カードや毎月の請求書などに記載の URL と同じことを確認しましょう。

★取り引きのある金融機関の Web サイトにアクセスする場合

□ URL はいつもと同じですか?

→ブラウザの URL 欄が確認できる場合は、見覚えのある URL か確認します。

□ 画面の見た目に違和感はないですか？いつもと見慣れない入力項目はないですか?

→偽画面かどうか判断がつかない場合は、取り引きのある銀行のホームページの注意喚起を確認しましょう。偽画面の具体例を掲載していることがあります。それでも判断がつかない場合は、銀行に問い合わせましょう。（※2）

□ パソコンの場合、ブラウザの URL 欄が正当性を示す緑色表示になっていますか?

→これからログインしようとする Web サイトが、正当性を示す EV-SSL を使用しておりブラウザの URL 欄が緑色表示になるか、事前に取り引きのある金融機関の注意喚起 Web ページを確認します。

＜InternetExplorer の場合＞

□ パスワードをメールで受信する場合、パソコンとは別の機器・端末のメールアドレスで受信するように設定していますか?

→一部の銀行は、１ 回限りの使い捨てパスワード（ワンタイムパスワード）をメールで通知するサービスを提供しています。しかし、マルウエアなどに感染しているパソコンでパスワード通知メールを受信すると、それが盗み見られてしまう危険性があります。パスワード通知メールを携帯電話キャリア各社のメールアドレ

スなどで受信するように設定すれば、より安全です。

★パソコン・スマホを安全に保つ

□ お使いのパソコンは Windows XP 以外ですか?

→Windows XP のサポートは 2014 年 4 月で終了しています。
Windows XP に新たなセキュリティ上の問題が見つかっても、修正された更新プログラムは提供されません。

□ Windows、iOS、android などの OS やブラウザ、メールソフト、Java、Flash などのアプリケーション類は最新の状態に保っていますか?

→古いバージョンのままだと、不正プログラムであるマルウエアに感染する可能性が高まります。
感染すると、上述のチェック項目に関わらず、不正ログイン、不正送金の被害に逢う可能性があります。

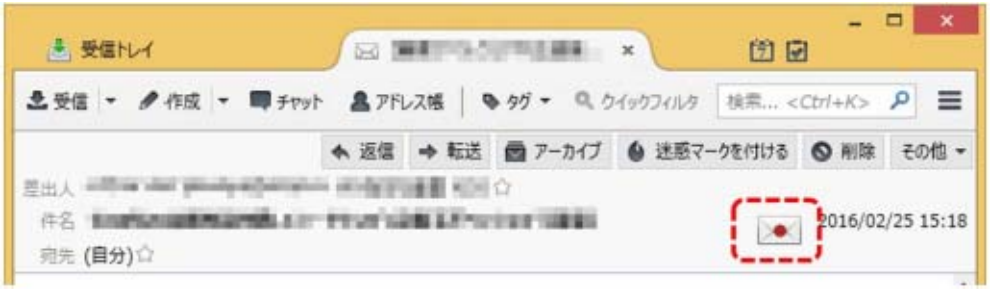
＜参考：Java が最新かどうかを確認できる Web ページ＞
http://www.java.com/ja/download/installed.jsp

※1 【参考情報】電子署名の確認方法

金融機関の中には、お客様にメールの正当性を示す電子署名という技術を採用しているところもあります。電子署名がされたメールをメールソフトで受信すると、該当のメールにマークが表示されます。

＜Outlook の場合＞

＜Thunderbird の場合＞



※2 【参考情報】偽メールや偽画面の誘導文言について

偽画面では、「あなたのコンピュータをシステムが認識できませんでした」「機能アップデート後の当行サイトを利用するためには、再度の登録が必要です」「お客さまの合言

葉は簡単すぎるため、変更が必要です」などとして、巧妙に銀行の画面であることを装って、不正に情報の入力を促すものがあります。

偽メールでは、「アカウントが凍結されないように」「アカウントがロックされないように」などと、利用者の焦燥感を煽るような言葉で、不正に情報の入力を促すものがあります。（その際、「システムをアップグレードしたため」などと、もっともらしい理由をつけていることもあります）

インターネットバンキング不正送金被害、もしもの時の相談先

フィッシング詐欺やオンライン銀行不正送金、ウイルス感染、不正アクセスなどのサイバー犯罪の不安がある場合、巻き込まれた場合には、速やかに下記の窓口に相談しましょう。

１）金融機関への連絡

ご利用のサービスの相談窓口へ連絡し、銀行からの案内をふまえて必要な手続きを取りましょう。また、相談窓口では、犯罪手口の解明のために、手掛かりとなる情報を聞かれることがありますので、できるかぎり協力するようにしましょう。

連絡先：各金融機関の相談窓口

※ご利用のインターネットバンキングの問い合わせ先・連絡先を、あらかじめ確認しておきましょう。

２）警察への相談、通報など

インターネットバンキング不正利用にあったり、あいそうになったときは、事実関係を整理し、警察のサイバー犯罪相談窓口に相談、通報しましょう。

連絡先：都道府県警察本部 サイバー犯罪相談窓口

http://www.npa.go.jp/cyber/soudan.htm

３）コンピューターウイルス感染に関する相談

ID、パスワードを盗むウイルスに感染した場合、パソコンの中には、犯人や手口解明への重要な手掛かりが残っている可能性もあります。OS の再インストールやウイルス駆除については、銀行や警察からの案内や指示も踏まえて対応しましょう。ウイルス駆除など具体的な対処方法については、IPA やご使用のセキュリティソフトベンダへ相談しましょう。

連絡先：IPA 情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html

連絡先：セキュリティソフトベンダ各社サイト

株式会社カスペルスキー　http://www.kaspersky.co.jp/

キングソフト株式会社　http://www.kingsoft.jp/

株式会社シマンテック　http://jp.norton.com/

ソースネクスト株式会社 http://www.sourcenext.com/

トレンドマイクロ株式会社　http://www.trendmicro.co.jp/
マカフィー株式会社　http://www.mcafee.com/japan/

4）フィッシング詐欺に関する相談

フィッシング詐欺と思われるメールを受信した場合は、フィッシング対策協議会へ連絡しましょう。提供された情報はフィッシング詐欺被害の防止に役立てられます。

連絡先：フィッシング対策協議会報告窓口

https://www.antiphishing.jp/registration.html