インターネット・バンキングの

セキュリティ対策 2019年度版

CONTENTS

本書の内容は一般的なセキュリティ対策の事例を紹介しています。
特定の銀行、サービスや機器の内容を掲載しているわけではありません。

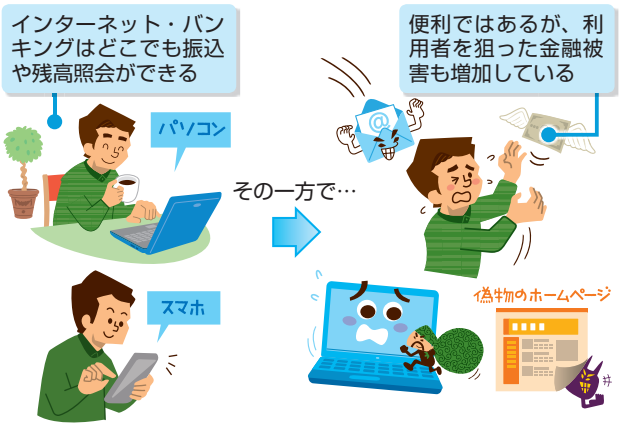
1 金融被害に遭わないようにするには

セキュリティ対策

インターネット・バンキングは、インターネットを使って預金の残高・取引明細の確認や、振込などができます。しかし、インターネット・バンキングによる不正送金などの金融被害も増えているのでセキュリティ対策が必要です。

インターネット・バンキングの利用者を狙った犯罪が増加している

インターネット・バンキングは、銀行に出向くことなく残高・取引明細の確認や振込などができるため、大変便利です。一方で、便利ゆえにインターネット・バンキングの利用者を狙った金融犯罪による被害も増えていて、偽物のホームページに誘導されてIDやパスワードが盗まれるなどの事例が報告されています。



ヒント スマートフォンやタブレットでのセキュリティ対策はどうするの？

インターネット･バンキングを、スマートフォン（以下「スマホ」と表記）やタブレットから利用する人も増えてきています。スマホやタブレットも、パソコンと同様の危険にさらされています。パソコンと同じように万全のセキュリティ対策をしましょう。特に、発行元の不確かな無料アプリをダウンロードすると、思わぬ被害を受けることがあるので、注意しましょう。

ヒント 銀行ではどんなセキュリティ対策がされているの？

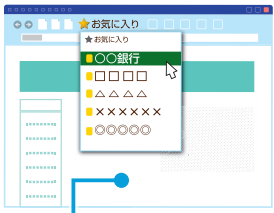
利用者が安心してインターネット・バンキングを使えるように、SSL（暗号化した通信）や電子証明書など、銀行のシステムごとにさまざまなセキュリティ対策が講じられています。しかし、利用者側のパソコンやスマホに悪質なスパイウェアが入っていたり、他人にパスワードを知られたりしては、口座を守ることが難しくなります。銀行が提供している各種のセキュリティ対策を活用するなど、利用者側もしっかりと対策を取りましょう。

セキュリティ対策を万全にしてインターネット・バンキングを安全に利用する

インターネット・バンキングによる不正送金などの金融被害の多くは、利用時のセキュリティ対策の甘さから起こります。次ページ以降を参考にして、インターネット・バンキングを安心して利用できるよう、しっかりセキュリティ対策をしましょう。また、常日頃から銀行のホームページをよく確認して、金融犯罪の手口や実際の被害などを把握しておくことも大切です。

セキュリティ対策ソフトを導入し、常に最新版にする

銀行のホームページに掲載されているセキュリティに関する「お知らせ」などの情報をよく読む



銀行のホームページは「お気に入り」に登録しておき、そこから開く癖をつける

使っているソフトウェアを最新版にする

2 IDやパスワードを安全に管理するには

ID、パスワード

インターネット・バンキングを利用するには、IDやパスワードが必要です。これは通帳やキャッシュカードの暗証番号と同じように大切なものです。警察や銀行、市役所、年金事務所などの職員であっても訊ねることはないので、他人に教えてはいけません。

「ID」や「パスワード」ってなに？

IDとは、契約者を識別する文字列です。「アカウント」や「お客さま番号」といった名称で呼ばれていることもあります。一方、パスワードは認証を得るための合言葉のようなものです。IDやパスワードなどの入力する情報は、各銀行のシステムによって異なります。

ID
通帳やキャッシュカードのように、契約者を識別するための身分証明書のようなもの

パスワード
銀行のATMで入力する暗証番号と同じような役割で、認証を得るための合言葉のようなもの

ヒント パスワードはIDと対になっている

取引銀行から送られてくるIDとパスワードは2つ揃うことで意味をもちます。どちらか一方でも忘れてしまうと、インターネット・バンキングを利用することはできません。

ヒント IDやパスワードはクラウドサービスに保管しない

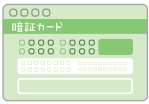
メモや写真を保存できるクラウドサービスに、IDやパスワード、暗証カードを撮影した写真などを保管しないでください。何者かがクラウドサービスを狙って攻撃し、保存したそれらの情報を盗んでしまう恐れがあるからです。

パスワードの種類っていろいろあるの？

各銀行によって、導入しているパスワードは異なります。例えば、「第2パスワード」は、通常のログイン時とは異なるパスワードで、重要な取引の際に求められることがあります。「ワンタイムパスワード」は一定時間ごとに変わるパスワードで、一度しか使えません。

第2パスワード

IDやパスワードとは別の画面で入力する場合や「暗証カード」から入力する場合などがある



ワンタイムパスワード

メールで送られてくるものを入力する場合やパスワード生成機に表示される数字を入力する場合などがある

IDやパスワードの管理に気をつける

パスワードは他人に知られないように、推測されにくい文字や数字を用いましょう。家族の名前、電話番号、生年月日は、推測されやすくなります。また、パソコンやスマホ内のファイル（ワード・テキストなど）に保存したり、ブラウザーに記憶させたりしたID･パスワードが漏えいし、詐取される事例が増えていますので注意しましょう。

推測されやすいパスワードは使用しない

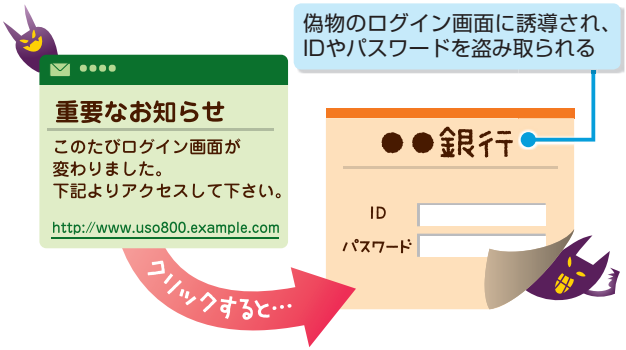
3 IDやパスワードを盗まれないようにするには

フィッシング詐欺

フィッシング詐欺とは、銀行や契約会社の名を騙って、IDやパスワードを盗み取る犯罪です。偽物のホームページに誘導し、ID・パスワードや、カード番号を利用者自身に入力させる手口が代表的です。

メールやSMSで偽物のホームページに誘導されることもある

取引銀行からのメール※だと思ってリンクをクリックしたところ、偽物のホームページに誘導され、そこで入力したIDやパスワードなどの情報を盗み取られる「フィッシング詐欺」の被害が増えています。また、「キャンペーン」や「ポイントを付与」など、お得な情報の通知を装ったメールを送りつけて、そこから偽物のホームページに誘導する手口もあります。



「キャンペーン」や「ポイントを付与」などのお得な情報の通知を装って、偽物のホームページへ誘導する

宅配業者を装いSMSで不在通知を送り付け、偽サイトに誘導してIDやパスワードを窃取するフィッシング詐欺が増えている。送信者をよく確認し、むやみにURLをクリックしないようにする

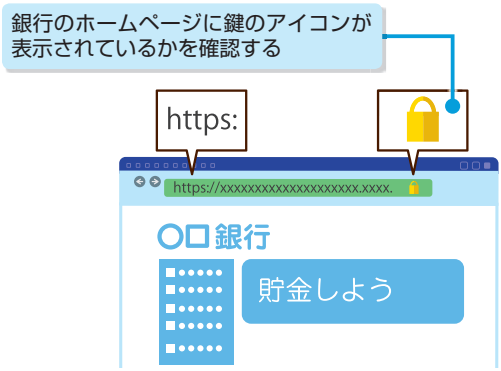
※メールだけでなく、スマホや携帯電話のショートメッセージサービス（SMS）、アプリを利用したフィッシング詐欺の手口が増えています。

ヒント なりすましに騙されないように注意！

銀行員や公的機関の職員などになりすまして、「還付金を振り込む」などと言葉巧みにインターネット・バンキングの申し込みを勧め、届いた会員カードのIDやパスワードなどを聞き出そうとする「ボイスフィッシング」の事例が増えています。インターネット・バンキングの申し込みで届いた各種資料は、誰にも見せたり渡したりしないようにしましょう。

フィッシング詐欺にひっかからないために

銀行のホームページへアクセスしたつもりが、偽物のホームページだったということがないように、必ずブラウザーに登録した「お気に入り」からアクセスしましょう。また、「https」から始まる通信を暗号化する仕組み（SSL）が導入されているホームページは、アドレスバーに鍵のアイコンが表示されたり、アドレスバーが緑色に表示される場合があります。パソコンのブラウザーで鍵のアイコンをクリックし、証明書を取得した会社の情報を確認すると、より安心です。



フィッシング詐欺の対策

- インターネット・バンキングへのログインは、「お気に入り（ブックマーク）」からトップページ経由でアクセスする
- キャンペーン情報などは、銀行のホームページや店頭で確認する
- あまりに条件が良すぎる情報など、メールに違和感がある場合はアクセスしない
- 検索サイトで表示された銀行のリンク先とURLをよく確認してから開く

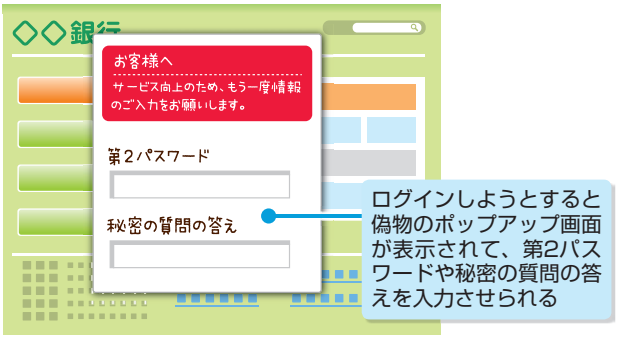
4 悪意のあるソフトウェアからパソコンやスマホを守るには

ウイルス対策

「スパイウェア」などの悪意のあるソフトウェアに感染すると、IDやパスワードなどの重要な情報を盗み取られることがあります。こうしたコンピューターウイルスに感染しないためには、対策ソフトの導入が必須です。

コンピューターウイルスに感染するとどうなるの？

「コンピューターウイルス」に感染すると、正規のインターネット・バンキングのページにアクセスしているにも関わらず、偽物のポップアップ画面が表示され、IDやパスワードなどが盗み取られることがあります。一度感染すると、自分自身をコピーして、さらに感染・増殖するのも特徴です。また、「スパイウェア」に感染すると、キーボード入力の内容や画面操作の様子、パソコンやスマホに保存されているファイルなどが盗み見られ、情報が流出する恐れがあります。これらの被害に遭わないように、適切な対策が必要です。

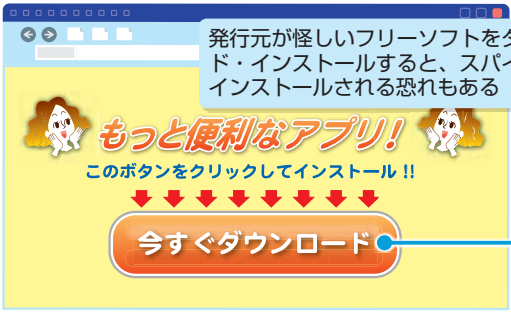


ヒント 最新のOSでもセキュリティ対策ソフトは必要

最新のWindows 10は、セキュリティ対策として「Windows Defender」などで保護されています。ただし、市販のセキュリティ対策ソフトはもっと多機能なので、万全を期すならば市販のソフトを導入するとよいでしょう。

メールの添付ファイルやフリーソフトのダウンロード時に注意する

メールの添付ファイルを開いたり、記載リンクをクリックすることによって、スパイウェアに感染することがあります。心当たりのないメールには十分注意し、安易に開封・クリックしないようにしましょう。また、発行元が怪しいフリーソフトのダウンロードは、感染の危険を伴います。できるだけ控えましょう。



ウイルスからパソコンやスマホを守る

パソコンはセキュリティ対策ソフトやファイアウォールを使うことで守れます。そうしたソフトなどを必ず導入し、常に最新の状態にしましょう。また、スマホのセキュリティ対策も忘れないでください。通信事業者や銀行では、スマホのセキュリティを高めるセキュリティ対策アプリを配布しています。それらをインストールすることで、スマホでも安全にインターネット・バンキングを使えます。

セキュリティ対策ソフトを導入し、常に最新の状態にしておく

通信事業者や銀行が配布しているウイルス対策アプリを導入する

ファイアウォール
不正なアクセスが通過しないようにブロックする仕組み

※セキュリティ対策ソフトは、市販されているソフトのほか、銀行や通信事業者が不正送金対策用のソフトを提供している場合もあります。

セキュリティ対策ソフトがウイルスを検知したらどうするの？

セキュリティ対策ソフトからウイルスの検知が通知されたら、すぐに隔離･駆除しましょう。そのウイルスによって、すでにIDやパスワードなどが盗み取られている恐れもあります。速やかに、口座に不審な取引がないかを確認してください。引き続き同じIDやパスワードを利用するのは、とても危険です。銀行にIDの再発行を依頼したり、パスワードを変更したりしましょう。

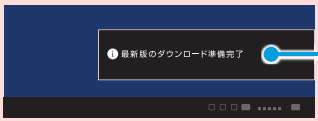
ヒント スマホのアプリはアップデートしよう

アプリのアップデートは、新機能の追加や使い勝手の向上だけなく、セキュリティを向上する機能も含まれていることがあります。常に最新版にアップデートし、スマホを安全に使いましょう。

アップデートの通知が表示されたら、アプリをアップデートする

ヒント ソフトは最新版にアップデートしよう

パソコンを使っていたり、再起動したりすると、JavaやAdobe Reader、Adobe Flash Playerなどがアップデートを通知してくることがあります。これらのアップデートにより、スパイウェアに感染する機会が減るため、毎回必ず更新しておきましょう。



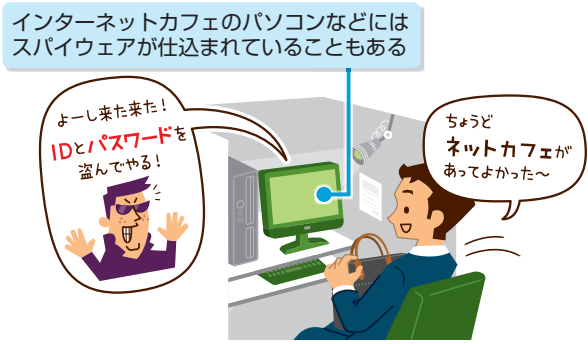
アップデートの通知を促された場合は、クリックしてアップデートする

ヒント 自分のパソコンやスマホだからといって安心はできない

公衆無線LANに接続してインターネット・バンキングを利用するときは、パソコンやモバイル機器から無線LANアクセスポイントまでの通信が暗号化されているかをよく確認しましょう。暗号化なしの場合、通信内容を盗聴される危険性があります。

外出先で利用するときは特に注意する

インターネット・バンキングは、安全であると確信できるパソコンや回線から利用しましょう。最近では、インターネットカフェなど、自由に利用できるパソコンが増えています。便利な反面、悪意のある人によってスパイウェアが仕込まれている可能性もあるので注意してください。自分の管理下にないパソコンは非常に危険です。自分のパソコン以外からはインターネット・バンキングを利用しないでください。



悪意のあるソフトウェアへの対策

- セキュリティ対策ソフトを必ず導入する（不正送金対策用のソフトは、銀行が無償提供している場合もある）
- セキュリティ対策ソフトを最新版にしておく
- 怪しいサイトやフリーソフトを利用しない
- 信頼できるサイト以外からファイルやフリーソフトをダウンロードしない
- 自分の管理下にないパソコンではインターネット・バンキングを利用しない
- 安易に添付ファイルを開封したり、リンクをクリックしたりしない

5 インターネット・バンキングを正しく運用するには

金融被害防止策

インターネット・バンキングは手軽で便利な反面、インターネットならではの危険もあります。日頃から以下のことに注意しておきましょう。

セキュリティ対策ソフトやファイアウォールの設定を確認する

インターネット・バンキングを利用するパソコンやスマホには、必ずセキュリティ対策ソフトをインストールしておきましょう。IDやパスワードは、人の目につく場所やパソコンおよびスマホ内で管理してはいけません。また、パソコンでは、ファイアウォールの設定が有効になっているかを確認しておきましょう。

セキュリティ対策ソフトやOSは最新版にバージョンアップする

セキュリティ対策ソフトやOS、各種ソフトは、最新版にアップデートするように心がけましょう。特にサポートが終了したOSやソフトを使うのは避けましょう。

ワンタイムパスワードを使ってセキュリティを強固にする

銀行によっては、セキュリティ対策として「ワンタイムパスワード」の導入が進んでいます。アプリや専用カード、パスワード生成機などで、一定時間ごとに更新されるパスワードが表示され、そのパスワードを入力することで認証します。安全性が高まるので、積極的に利用しましょう。

ヒント Microsoft Edgeはインターネット・バンキングで使えない場合もある

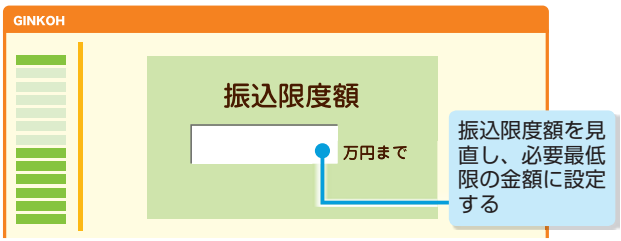
Windows 10では、ホームページを見る標準のブラウザーとして、「Microsoft Edge」がインストールされています。しかし、Microsoft Edgeは新しいブラウザーであるため、すべての銀行のホームページに対応しているとは限りません。機能が使えなかったり、Webページがきちんと表示されない場合は、Internet ExplorerやGoogle Chromeを使いましょう。

メールに添付されているファイルを開いたり、不審なホームページにアクセスしない

心当たりのないメールに添付されているファイルを開いたり、不審なホームページにアクセスしたりしないようにしましょう。クリックする前に、銀行のホームページなどで注意喚起が行われていないか、あらかじめ情報を確認しましょう。

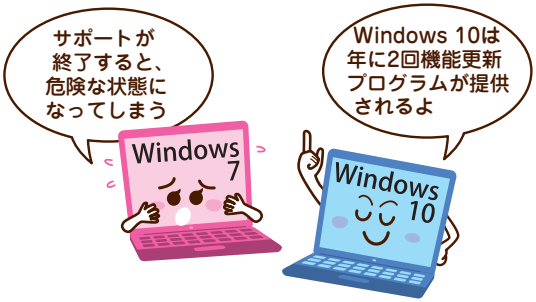
振込限度額などを見直す

振込限度額や各種料金の払込限度額は、契約者自身が変更できます。普段の取引に必要なだけの金額を設定することで、万が一の事態でも被害を最小限に抑えられます。



OSのサポート期間に注意しよう

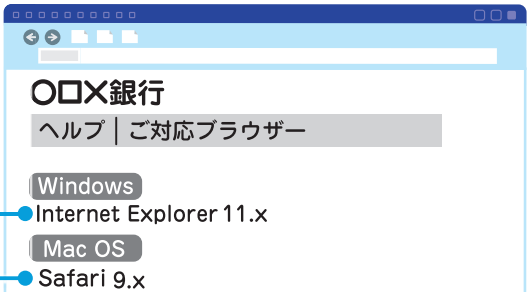
パソコンやスマホのOSにはサポート期間があります。サポート期間が終了したOSは、セキュリティ更新プログラムが提供されなくなるため、悪意のある攻撃に対して無防備となり、ウイルスに侵入されやすくなります。たとえば、Windows 7は2020年1月14日にサポート期間が終了します。早めに最新のWindows 10環境への移行を検討しましょう。Windows 10は、大規模な機能更新プログラムが年2回ごとに提供されますが、機能更新プログラムを毎回適用すればサポート切れになる心配がありません。



対応ブラウザーが最新版になっているかを確認しよう

インターネット・バンキングを使う場合、ブラウザーが銀行のホームページに対応しているか、最新版になっているかを確認しましょう。古いブラウザーでは、セキュリティの問題が発生することがあります。

使用しているブラウザーが銀行のホームページに対応しているかを確認する



ヒント サポート切れのサーバーは使わない

社内などでサーバーを利用している場合、そのサーバーのOSが古くないかを注意してください。サポートが終了した古いOSのサーバーは、サーバー自身が危険なだけでなく、ネットワークにつながっている他のパソコンにもセキュリティ上の悪影響を与えることがあります。実際に、英国の国民保健サービス（NHS）がサイバー攻撃を受けて、身代金を支払うなどの被害が起きています。サーバーもパソコンやスマホと同様、OSを常に最新版に保ち、古いOSは使わないようにしましょう。

古いパソコンやスマホは今後どうすればいいの？

古いOSのパソコンやスマホは、新しいOSにバージョンアップするか、新しいOSが搭載されているパソコンやスマホに買い換えましょう。またOSだけでなく、使用しているソフトも随時アップデートを確認し、最新版にしておきましょう。

パソコンやスマホのOSやアプリは、最新版にアップデートする

金融被害防止の対策

- パソコンやスマホには、セキュリティ対策ソフトを必ず導入する
- セキュリティ対策ソフトを最新版にアップデートしておく
- サポートが終了したOSのパソコンやスマホでインターネット・バンキングを利用しない
- ワンタイムパスワードを使用する
- 不審なホームページや発行元が不確かなフリーソフトを使用しない
- 怪しい添付ファイルやリンクを安易にクリックしない
- 必要最低限の振込限度額に設定する
- OSやソフトは銀行の推奨環境であることを確認して利用する

6 法人がインターネット・バンキングの被害に遭わないようにするには

法人における金融被害防止策

法人が被害を受けると、被害額が大きくなるばかりか、会社の信頼を損ねる結果にもつながりかねません。銀行が提供・注意喚起しているセキュリティ対策を実施し、対策を徹底しましょう。

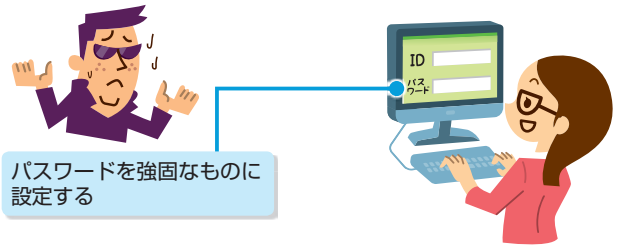
取引のデータを作成する人と承認する人のパソコンを分ける

振込などの取引を、「入力する人」と「承認する人」に分けて、別々のパソコンで行うようにすれば、複数のパソコンにアクセスしなければ不正送金を行えなくなるため、不正取引を防止する対策として有効です。

強固なパスワードを設定する

パスワードは推測されにくく、当てずっぽうで合致することがない強固なものを設定しましょう。会社情報である「設立年月日」「社長の名前」「代表電話番号」などは推測されやすくなります。また、数字だけのパスワードは推測されやすいので避けてください。パスワードは、十分な長さがあり、英数字と記号を含めたものとすることで推測されにくくなります。さらに、英字は大文字と小文字を適度に混ぜると強度が高まります。

インターネット・バンキングで使うパスワードは、他のサイトで使うパスワードとは違うものにし、万一、パスワードの漏えいが起きても、インターネット・バンキングへの影響がないようにしましょう。



ヒント アップデートする前にチェックしよう

顧客管理などの社内システムは、最新OSでは動かないことがあります。アップデート前に、管理者などに確認しましょう。

振込限度額などを必要最低限の金額に設定する

きちんと対策をとっていたつもりでも、インターネット・バンキングの被害に遭ってしまうことがあります。そこで万が一に備えて、振込限度額や各種料金の払込限度額を、通常の業務に必要な最低限の金額に設定して、被害を最小限に抑えられるようにしましょう。

不正なログインや送金がないか定期的に確認する

インターネット・バンキングを利用しないときでも定期的にログインし、身に覚えのない操作がされていないか確認しましょう。長期間にわたってログインしていないと、不正なアクセスや送金に気づかず、被害が増大する恐れがあります。

業務を装った標的型攻撃メールに注意する

送信者や宛先を偽装し、メールにマルウェアを添付する「標的型攻撃」によって企業の機密情報や個人情報が盗まれる被害が増えています。業務に関係があるようなメールに見えても添付ファイルをすぐに開いたり、文中のリンクを不用意にクリックしないようにしましょう。

7 万が一金融被害に遭ったときは

銀行に連絡、警察に連絡

用心に用心を重ねていても、身に覚えのない取引が発生してしまうかもしれません。インターネット・バンキングを利用していて、何かおかしいなと感じたら、すぐに銀行に連絡しましょう。

身に覚えのない振込メールが届いたら異常がないか確認する

インターネット・バンキングで操作すると、「振込」「振替」「ログインパスワードの変更」「メールアドレスの変更」など操作に応じたメールが届きます。操作の覚えがないのに、これらのメールが届いたときは、被害が発生しているかもしれません。インターネット・バンキングにログインして異常がないか確認しましょう。

ヒント いつでも確認可能なスマホまたは携帯メールなどを登録する

銀行からの通知メールは、警報のようなものです。異変を見逃してしまわないように、銀行からのメールはスマホまたは携帯メールなど確認しやすい端末で受け取り、必ず確認する癖をつけましょう。もし身に覚えのない「パスワード、メールアドレスの変更」や「振込・振替のお知らせ」など、異変を感じるメールを受け取ったら、すぐに銀行に連絡しましょう。
2018年10月には、24時間365日稼動のシステムに参加する銀行間で、振込可能時間が拡大されました。スマホまたは携帯メールアドレスを登録しておけば、パソコンで受信するのに比べて、異変に早く気づける確率が高まります。

金融被害に遭ったらすぐに銀行に連絡する

金融被害に遭ってしまったら、早急に銀行に連絡しましょう。連絡が早ければ、被害が大きくなる前に食い止められることもあります。いざという時のために、銀行の連絡先を、スマホや携帯電話、スケジュール帳、自宅のパソコン周りなど、複数の箇所に控えておきましょう。銀行によっては、時間帯によって連絡先が異なることもあります。また、銀行に連絡したら、警察にも連絡しましょう。「おかしいな」と感じたら、すぐに銀行に相談しましょう。

❶銀行に連絡	異変を感じたら、すぐに銀行に連絡しましょう。戸惑っている間にも被害が大きくなります。
❷警察に連絡	銀行に連絡したあと、忘れずに警察にも連絡しましょう。銀行に連絡したら、間をあけずに速やかに連絡してください。

金融被害に遭った場合

- 「振込」「振替」「ログインパスワードの変更」「メールアドレスの変更」などで、操作の覚えのないメールが届いたら、被害に遭ったことを疑う
- 銀行の連絡先を控えておき、被害に遭ったらすぐに銀行に連絡する
- 銀行に連絡したあと、警察にも連絡する

インターネット・バンキングを使用する前にチェック！

□ID・パスワードは適切に管理していますか？
□ワンタイムパスワードを利用していますか？
□パスワードは推測されにくく、強固なものを設定していますか？
□セキュリティ対策は行っていますか？
□最新のOSとブラウザーを使用していますか？
□登録の電子メールアドレスはスマホ・携帯電話で受け取れるようにしていますか？
□振込限度額、各種料金の払込限度額は見直していますか？

●本書に掲載されている情報について

本書に掲載されている情報は、2019年7月現在のものです。本書で紹介している内容は、一般的なセキュリティ対策の一例です（特定の銀行、サービスや機器の内容を掲載しているわけではありません）。このため、すべての環境や対策方法は本書の記載と同様に行えることを保証するものではありません。また、金融被害の手口は日々変化しており、本書の対策ですべてのトラブルを解決できるものではありません。

●免責

本書は無償で提供されるものであり、本書の使用または使用不能により生じたお客様の損害に対して、当行では一切の責任を負いかねます。また、本書に関するお問い合わせはお受けしておりません。あらかじめご了承ください。

七十七銀行