

# ご注意下さい！

偽造・盗難キャッシュカード、盗難通帳、偽造印鑑等による不正な預金払出しや、いわゆるヤミ金融業者等による預金口座への不正な振込請求、さらにはフィッシングやスパイウェアといった事件が発生しています。

お客様におかれましては、そうした被害に遭われぬよう、十分にご注意下さい。

**ご注意！**

## 偽造・盗難キャッシュカード、盗難通帳、偽造印鑑等による不正な預金払出し等

通帳・印鑑はもちろんのこと、キャッシュカードや本人であることを示す各種資料(運転免許証・パスポート等)についても、別々にかつ厳重に保管して下さい。

キャッシュカードの暗証番号は他人に知られないようにして下さい。また、他人に知られ易い暗証番号(生年月日、電話番号等)はすみやかに変更されることをお勧めします。銀行員や警察官が銀行店舗外や電話等で暗証番号をお尋ねすることはありません。預金の引出しの際に、暗証番号を後ろから盗み見られたり、他人に知られたりしないようご注意ください。

ATMコーナーにおいて暗証番号を盗み見るためと思われる隠しカメラが設置される事件が発生していますので、ご注意ください。ATMコーナーにおいて不審な機器等を見かけた場合には、ATM設置金融機関、または警察署にご連絡下さい。

預金の引出し、入金の際の現金を狙ったすりやひったくり等には十分ご注意ください。スキミング(注)等によりキャッシュカードが偽造され、預金が払い出されるといった被害が発生しています。このような被害に遭わないために、キャッシュカードを入れた財布等を長時間手元から離すことのないようご注意ください。

(注) スキミングとは、他人のカードの磁気記録を不正に読み出してコピーを作成することです。

スキマーと呼ばれるカード情報の読み取り装置によりカード情報が盗み取られます。

キャッシュカードの暗証番号は他のサービスの暗証番号として使うことは避けましょう。キャッシュカードを偽造して他のサービスの暗証番号を盗み取り、預金が引き出された事件が発生しました。

万一、通帳・印鑑・キャッシュカードのいずれか一つでも紛失・盗難された場合や何か不審に思われる場合は、直ちにお取引銀行および警察署にご連絡下さい。例えば、通帳のみを紛失された場合であっても、印影から印鑑が偽造されるおそれがあります。

また、空き巣や車上盗難の被害に遭ったときは、スキミング等が行われている可能性もありますので、キャッシュカードが盗まれていなくても、念のためお取引銀行および警察署にご連絡下さい。

カード・通帳・印鑑をなくされたときの銀行の連絡先は[こちら](#)をご覧ください(全国銀行協会「モアバンク」へのリンク)。

**ご注意！**

## 預金口座への不正な振込請求等

振り込み詐欺(注)や電子メール等による身に覚えのない利用料等の請求の被害が拡大しています。お振込になる前に事実かどうかを必ずご確認ください。

(注) 振り込み詐欺とは、親戚あるいは警察官等を装って電話をかけ、事故・喧嘩の示談金や賠償金、借金返済金が必要であると偽って多額の現金を振り込ませる詐欺行為です。

ヤミ金融業者等による法外・強引な返済請求があった場合には、安易に振込等を行わないで下さい。

銀行の預金規定では、第三者による預金口座の利用を禁止させていただいておりますので、預金口座を売ることや貸すことはできません。

「金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律」により、他人になりすます目的で預金通帳やキャッシュカードを譲り受けたり、相手になりすまし目的があることを知りながら、預金通帳やキャッシュカードを譲り渡した場合等は、50万円以下の罰金が科されます。

不審に思われる場合には、最寄りの警察署、財務局、都道府県の相談窓口等にご相談下さい。

**ご注意!**

## 「貸します詐欺」

ニセダイレクトメール・広告等にご注意

最近、金融機関などを装って、「お金を貸します」といった内容のニセのダイレクトメール・携帯メールなどを送りつけて、保証金や保険金名目でお金を騙し取る新手の手口が急増しています(このような詐欺行為を「貸します詐欺」といいます)。

被害に遭わないよう、十分ご注意下さい。

### 「騙されないための心構え三か条」

取引関係のないところから突然送られてくる、「お金貸します」とのダイレクトメール・携帯メール等に注意

(低金利で、しかも高額を貸し付けるかのような広告にご注意下さい)

融資をする前に、様々な口実でお金を振り込まそうとする手口に注意

(保証料、保険料等の名目でお金を要求します)

「貸します詐欺」かもしれないと感じたら、すぐに問い合わせ

「貸します詐欺」被害ホットライン

03 - 5320 - 4775 (東京都貸金業対策課)

「金融機関等詐称被害に関する連携会議」

**ご注意!**

## フィッシング

フィッシング(注)により口座番号、インターネットバンキングのID、パスワード、キャッシュカードの暗証番号等を詐取し、これらの情報を用いて悪用する事件が発生していますので、十分にご注意下さい。

(注)フィッシング(Phishing)とは、金融機関等を偽装したEメールを送信し、Eメールの受信者に偽のホームページにアクセスするよう仕向け、そのホームページにおいて、預金の口座番号、インターネットバンキングのID、パスワード、キャッシュカードの暗証番号等を入力させることにより個人の金融情報を不正に入手するような行為のことです。

金融機関が預金の口座番号、インターネットバンキングのID、パスワード、キャッシュカードの暗証番号等の確認を目的とするEメールを送信することはありません。

不審なEメールを受信した場合には、送信元のEメールアドレスや指定されたホームページのアドレスをよく確認するとともに、メールを送信してきたとされる金融機関等に確認するなど、安易に指定されたホームページにアクセスしたり、預金の口座番号、インターネットバンキングのID、パスワード、キャッシュカードの暗証番号等を入力することのないようご注意下さい。

- ・ 万一、不審先と思われるホームページ等において、預金の口座番号、インターネットバンキングのID、パスワード、キャッシュカードの暗証番号等を入力してしまった場合には、直ちにお取引銀行にご連絡下さい。
- ・ 各都道府県警察では、サイバー犯罪相談窓口を設置し、フィッシングに関する情報提供を受け付けています。

**ご注意!**

## スパイウェア

預金者のパソコンに侵入させたスパイウェアソフト(注)を利用して、そのパソコンからインターネットバンキングのIDやパスワードを搾取した上で、預金者の口座から預金を不正に引き出すという事件が発生しておりますので、十分にご注意下さい。

(注)スパイウェアとは、預金者がインターネットバンキングを利用する際に入力したIDやパスワードを、悪意の第三者のアドレスに自動的に送信するソフトです。

スパイウェアの侵入経路は、心当たりのない電子メールの開封時や提供先がはっきりしないフリーソフトのダウンロード時が一般的(悪意のあるホームページを閲覧するだけで侵入するものもあります)ですので、例えば、不審なメールを受信した場合には、送信元のアドレスを確認するなど、不用意に開封しないよう、十分にご注意下さい。

**最近、金融機関からの郵送物であると偽装して、スパイウェアを仕込んだCD-ROMを送りつける手口の事件が発生しました。**

預金者のパソコンにスパイウェア対策ソフトをインストールしておくことも有効と考えられますが、絶えずアップデートして最新の状態にしておく必要があります。なお、対策ソフトによっては検知できないスパイウェアもありますので、ご留意願います。

取引履歴の確認や通帳の記帳を頻繁に行っていただくことにより、身に覚えのない取

引を早期に発見することができます。また、振込限度額等の設定を少額なものに変更することも被害を減らす方法としてお勧めします。

- ・ 万一、スパイウェアを発見した場合、あるいは身に覚えのない取引履歴があった場合には、直ちにお取引銀行にご連絡下さい。
- ・ 金融機関名で普段から郵送されているものと違うCD-ROMが届いた場合には、真正のものであるかどうか、お取引銀行にご確認下さい。
- ・ 各都道府県警察では、サイバー犯罪相談窓口を設置し、サイバー犯罪に関する情報提供を受け付けています。

銀行では、預金口座の開設等にあたり、法律に従った本人確認をいたしておりますが、上記のような盗難通帳・偽造印鑑等による預金の不正な払出しや預金口座の不正利用等を防止するため、預金のお支払い時等に改めてご本人の確認をさせていただくことや、預金口座のご利用目的等をお伺いすることがございますので、ご理解とご協力をお願い申し上げます。

なお、預金規定に違反する場合には、預金口座のご利用を停止させていただいたり、解約させていただく場合もございます。

「預金の不正な払出し」・「預金口座への不正な振込請求」等に関するご相談やご照会等ございましたら、当協会の「皆様の相談所」(電話番号:03-3262-2182)もご利用下さい。