平成２６年　６月　９日
株式会社新銀行東京

インターネットバンキングにおける不正利用にご注意ください

インターネットバンキングを通じて預金を不正に引き出される被害が国内で急増していますので、下記のような点にご注意の上、ご利用ください。

1. OS、ブラウザは常に最新の状態に更新する

ご利用環境（OS、ブラウザ）は推奨環境のものをご利用ください。その上で、最新のセキュリティパッチを適用してください。

特に、WindowsXP は 2014 年 4 月 9 日でマイクロソフトのサポートが停止しており、それ以降の新たなセキュリティの脅威に対応できない状態にありますので、WindowsVista 以降の OS をご利用ください。

2. セキュリティ対策ソフトを導入し最新の状態に更新する

お取引に使用するパソコンは、セキュリティ対策ソフトを導入し、最新の状態にアップデートした上でご利用ください。また、定期的にウィルスチェックと駆除を行ってください。

3. パスワードを変更する

パスワードは、定期的に更新してください。

4. 振込限度額を必要な範囲内で出来るだけ低く設定する

振込限度額を必要最低限に設定することで、万一、被害にあった場合でも最小限に抑えることができます。振込限度額の設定を見直し、必要以上に高額設定しないでください。

なお、法人インターネットバンキングでは、事前登録先振込と都度指定振込でそれぞれ 1 日あたりの振込限度額が設定できます。

5. 不正なログイン履歴がないか確認する

当行のインターネットバンキングは、ログイン直後の画面に直近３回分のログイン履歴が表示されています。この履歴の中に利用した憶えのない履歴がないかご確認ください。

もし、利用した憶えのないログイン履歴が確認された場合には、預金残高や、取引履歴などをご確認の上、不正な出金が無いかをご確認ください。また、パスワード、確認暗証番号なども即時変更してください。

6. 契約者番号、パスワードを不用意に入力しない

当行のインターネットバンキングは、

- ログイン時
- 振込（総・給振、代金回収含む）や定期預金の預入、解約等資金の移動を伴うお取引時
- パスワード、確認暗証番号変更時

以外で契約者番号やパスワード、確認暗証番号の入力を求めることはありません。

もし、ログイン後に、ポップアップ画面が表示されて、パスワード等の入力を求められるなど、通常とは異なるタイミングで契約者番号、パスワード、確認暗証番号の入力を求められたときには、絶対に入力を行わないでください。

また、お電話やメール、書面などで、当行からお客様へ契約者番号、パスワードなどをお問合せすることも一切ありません。万一、お心当たりがある場合には、早急に当行コールセンターまでご連絡ください。

7. 不審なメールのリンク先をクリックしない

当行からお客様へリンクをクリックすることを促すようなメールを送信することはありません。不審なメールが送付されてきた場合には、リンク先をクリックしないで、早急に当行コールセンターまでご連絡ください。

もし被害に遭われた、もしくは当行からの不審な照会、メールなどがあった場合は、当行のコールセンターへご連絡ください。

■ 本件に関するご連絡・お問い合わせ先 ■

新銀行東京コールセンター

0120−289−226

個人インターネットバンキング、モバイルバンキングに関するお問合せ：
ガイダンスの後、電話機の【１】をプッシュしてください。
法人インターネットバンキングに関するお問合せ：
ガイダンスの後、電話機の【４】をプッシュしてください。

受付時間：９：００～１７：００（銀行窓口休業日を除く）