

平成27年4月20日

インターネットバンキングをご利用中のお客さまへ

インターネットバンキングの不正アクセス対策について

現在、インターネットバンキングの ID やパスワード等を第三者が不正に取得し、お客さまに成りすまして不正にアクセス・資金の移動を行う等の被害が全国の金融機関で多発しています。

お客さまにおかれましては、不正アクセスによる被害に遭わないため、以下の点にご注意いただきますようお願いいたします。

1 OS・ブラウザは推奨環境にあったものを使用してください。

サポートが終了し、セキュリティ更新プログラム等の提供が行われていないOSやブラウザを使用したり、推奨環境以外でのご利用は控えてください。また、OSやブラウザは最新の状態に更新してください。

2 セキュリティ対策ソフトを導入してください。

セキュリティ対策ソフトを導入していないパソコンはウィルス感染する危険性が高くなります。セキュリティ対策ソフトを導入するとともに、常に最新の状態に更新し定期的にウィルススキャンを実施してください。

3 インターネットバンキング専用セキュリティ対策ソフト「Rapport（ラポルト）」をご利用ください。

Rapport（ラポルト）はインターネットバンキングを狙ったウィルスの検知・駆除および通信情報の改ざん防止を行うソフトです。パソコンにインストールするだけで自動的に機能し、他のセキュリティソフトとの併用も可能です。また、無料でご利用いただけます。

4 パスワード等の情報を不正に入力させる画面に注意してください。

インターネットバンキングにログインした後に、ウィルスが不正な入力画面を表示し、お客さまの情報を入力させようとする事象を確認しております。「あなたのコンピューターをシステムが認識できませんでした。」というメッセージではじまるパスワード等の入力を要求された場合、絶対に入力しないでください。また、「確認用パスワード」の数字すべてを入力いただくことはありませんので、絶対に入力しないでください。

5 パスワードや「お客様カード」は厳重に管理してください。

パスワードを記載したメモや「お客様カード」が第三者に不正利用され、悪用されることのないよう、厳重な管理をお願いいたします。また、パスワードは定期的に変更することをお奨めします。

6 電子証明書をご利用ください。(法人 | Bが対象)

電子証明書は、実社会でいう運転免許証や印鑑証明書などに相当するもので、当金庫が発行する電子的な身分証明書です。電子証明書にはインターネットバンキングの契約者であることを証明する情報などが記録されています。電子証明書が入っていないパソコンからはログインできないため、第三者による不正アクセス対策として有効です。「ID・パスワード方式」をご利用のお客さまは「電子証明書方式」に変更されることをお奨めします。

7 利用者ワンタイムパスワードをご利用ください。(法人 | Bが対象)

資金移動時に入力する「確認暗証番号」に加えて、入力する暗証番号がその都度変更となる「利用者ワンタイムパスワード」をご利用ください。特に「ID・パスワード方式」を利用のお客さまはぜひご利用ください。

8 ソフトウェアトークンによるワンタイムパスワード認証をご利用ください。(個人 | Bが対象)

ワンタイムパスワードとは、「ソフトウェアトークン」と呼ばれる生成アプリに表示される6桁の数字で、30秒毎に更新されるパスワードです。IDとパスワードの入力によるログイン認証に加えて、ワンタイムパスワードを入力することで、より安全にインターネットバンキングをご利用いただけます。

9 ログイン後に表示されるご利用の履歴を確認してください。

ログイン直後の画面に表示される過去のログイン履歴をご確認ください。また、残高照会・入出金明細照会や通帳記帳を行い、身に覚えのない取引がないか等をご確認ください。

