

お客様各位へ

関信用金庫

WEB-FB、WEBバンキング、でんさいサービスを  
ご利用のお客様のセキュリティ対策について

現在、本年に入ってから他金融機関のインターネットバンキングにおいて、不正送金被害が急増しております。当金庫において、現在まで不正送金被害は発生しておりませんが、WEB-FB、WEBバンキング、でんさいサービス（以下「IBサービス」と言います。）をご利用のお客様におかれましては、以下のセキュリティ対策を実施していただきますよう、お願い申し上げます。

なお、IBサービスにログインした際に不審な入力画面等が表示された場合、ID・パスワード等の情報を入力せず、当金庫にご連絡ください。

※IBサービスのご利用者は、以下の対策の実施をお願いします。

IBサービスのご利用者へ実施していただくセキュリティ対策	
①	IBサービスに使用するパソコン（以下、単に「パソコン」という。）に関し、基本ソフト（OS）やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新する。
②	パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を中止する。 （例：WindowsXPを搭載しているパソコンを引続き使用している等）
③	パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新し、当金庫のIBサービス専用セキュリティソフト「Rapport」を導入する。
④	電子証明書やワンタイムパスワードをご利用いただく。若しくはIBサービスに係るパスワードを定期的に変更する。
⑤	当金庫が指定した正規の手順以外で電子証明書を利用しない。
IBサービスのご利用者へ推奨するセキュリティ対策	
①	パソコンの利用目的として、インターネット接続時の利用はIBサービスに限定する。
②	パソコンや無線LANのルータ等について、未利用時は可能な限り電源を切断する。
③	WEB-FB、でんさいサービス等は、取引の申請者と承認者とで異なるパソコンを利用する。
④	振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定する。
⑤	不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかをその都度確認する。

**重要**：過去の不正送金事故において、大半のケースが電子証明書やワンタイムパスワードの未導入先です。事故防止の観点からも導入をご検討いただきますようお願い申し上げます。ご不明な点はヘルプデスクまでご連絡ください。

以上