お 客 様 各 位

２０２０年１１月１１日

遠　軽　信　用　金　庫

偽画面を表示させてＷＥＢ－ＦＢサービスの情報を盗み取ろうとする事例について

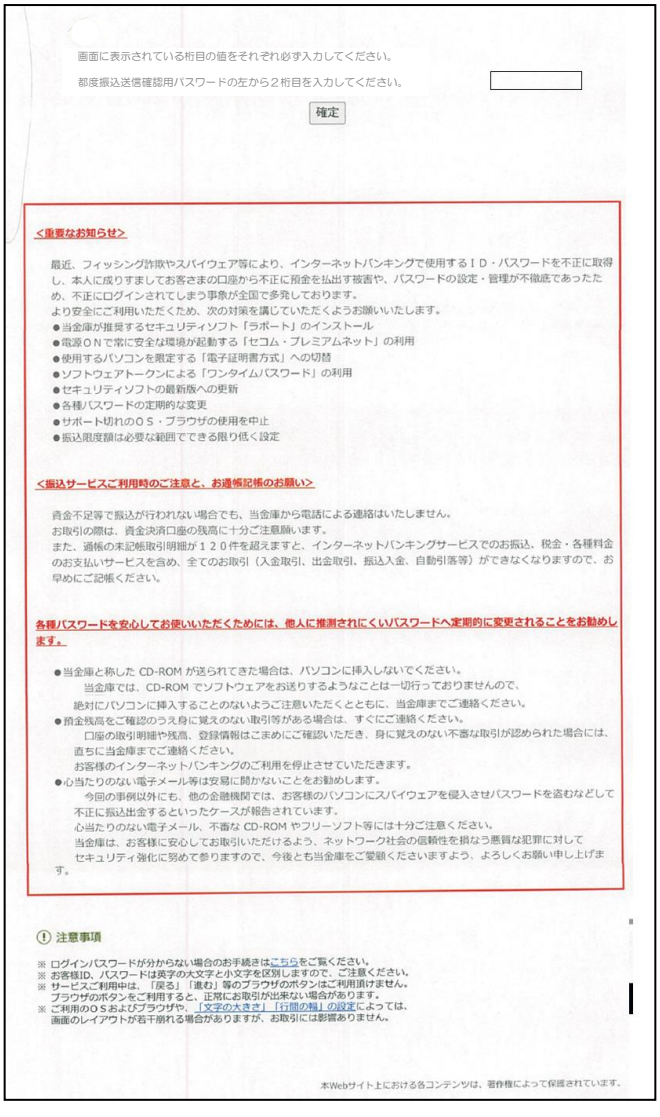
日頃より当金庫のＷＥＢ－ＦＢサービスをご利用いただき誠にありがとうございます。

一部の信用金庫におきまして、ＷＥＢ－ＦＢサービスの偽画面を表示させて、お取引に必要なＩＤ・パスワードを盗み取る事例が確認されております。

ＷＥＢ－ＦＢサービスでは、ログイン直後にパスワードを入力していただくことはありません。

もし、このような画面が表示されても入力は絶対に行わないでください。

実際に確認された偽画面のイメージ画像



①ログイン画面で ID とパスワードを入力すると、左のような画面が表示されます。

②この画面では、都度振込送信確認用パスワードについて、桁数指定で入力を求めてきます。入力すると、次は別の桁数を指定してきます。この繰り返しでパスワード情報を入手します。

③画面中央にある〈重要なお知らせ〉以下の文章は、当金庫のものではありません。

④偽画面の URL は本物と同じものが表示されています。

被害を防ぐために

偽画面の表示は、お客様のパソコンがウイルスに感染したことが原因である可能性があります。ＷＥＢ－ＦＢサービスをご利用のお客様は、ウイルス感染からの情報流出を防ぐために、以下の点にご注意をお願いします。

・ウイルス対策ソフトを導入する。

常に最新版にアップデートして利用し、定期的にウイルスチェックを行ってください。

インターネットバンキングを狙ったウイルスの検知・駆除には、セキュリティソフト「Rapport」が効果的です。

・OS やブラウザ、ソフトウェア（アプリケーション）は常に最新の状態に更新する。

これらの脆弱性情報は日々更新されていますので、最新の状態を保つことが脆弱性対策になります。

・ウイルス感染の原因となる行動をしない。

不審なウェブサイトや、送信元が不明な E メールは開かないでください。また、インターネットカフェなど不特定多数が利用するパソコンでは、USB メモリ等の使用を避けてください。

・各種暗証番号等の管理方法を見直す。

スマートフォンやパソコン、クラウドサービスへの保存はお控えください。ウイルス感染時の情報流出リスクが高まります。

・ワンタイムパスワードを利用する。

ワンタイムパスワードは一定時間で自動的に変更されることから、第三者に搾取されたとしても、不正送金のリスクを低減させることができます。実際に不正送金被害にあったお客様は、ワンタイムパスワードを利用していないケースが多く見受けられます。

以　上