

令和2年11月

お客さま 各位

北星信用金庫

## 偽画面を表示させてインターネットバンキングの情報を 盗み取ろうとする事例について

平素は格別のお引き立てを賜り、ありがたく厚く御礼申し上げます。

さて、標記につきまして、一部の他信用金庫におきまして、WEB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。

つきましては、今後も同様の事例が発生する恐れがありますので、別紙「ID・  
パスワードを盗み取る事例について」をご参照頂き、ID・パスワードの管理には十分御  
注意頂きますようお願い申し上げます。

以上



## I D・パスワードを盗み取る事例について

一部の他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I D・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には絶対に行わないでください。

### 1. 実際に確認された偽画面のイメージ画像

画面に表示されている桁目の値をそれぞれ必ず入力してください。  
都度振込送信確認用パスワードの左から2桁目を入力してください。

[確定]

**<重要なお知らせ>**

最近、フィッシング詐欺やスパイウェア等により、インターネットバンキングで使用するI D・パスワードを不正に取得し、本人に成りすましてお客様の口座から不正に預金を払出す被害や、パスワードの設定・管理が不徹底であったため、不正にログインされてしまう事例が全国で多発しております。  
より安全にご利用いただくため、次の対策を講じていただくようお願いいたします。

- 当金庫が推奨するセキュリティソフト「ラボート」のインストール
- 電源ONで常に安全な環境が起動する「セコム・プレミアムネット」の利用
- 使用するパソコンを限定する「電子証明書方式」への切替
- ソフトウェアトークンによる「ワンタイムパスワード」の利用
- セキュリティソフトの最新版への更新
- 各種パスワードの定期的な変更
- サポート切れのOS・ブラウザの使用を中止
- 振込限度額は必要な範囲でできる限り低く設定

**<振込サービスご利用時のご注意と、お進捗情報をお願い>**

資金不足等で振込が行われない場合でも、当金庫から電話による連絡はいたしません。  
お取引の際は、資金決済口座の残高に十分ご注意ください。  
また、通帳の未記帳取引明細が120件を超えますと、インターネットバンキングサービスでのお振込、税金・各種料金のお支払いサービスを含め、全てのお取引（入金取引、出金取引、振込入金、自動引落等）ができなくなりますので、お早めにご確認ください。

**各種パスワードを安心してお使いいただくためには、他人に推測されにくいパスワードへ定期的に変更されることをお勧めします。**

- 当金庫と称したCD-ROMが送られてきた場合は、パソコンに挿入しないでください。  
当金庫では、CD-ROMでソフトウェアをお送りするようなことは一切行っておりませんので、絶対にパソコンに挿入することのないようご注意くださいとともに、当金庫までご連絡ください。
- 預金残高をご確認のうえ身に覚えのない取引等がある場合は、すぐにご連絡ください。  
口座の取引明細や残高、登録情報はごまかにご確認いただき、身に覚えのない不審な取引が認められた場合には、直ちに当金庫までご連絡ください。  
お客様のインターネットバンキングのご利用を停止させていただきます。
- 心当たりのない電子メール等は安易に開かないことをお勧めします。  
今回の事例以外にも、他の金融機関では、お客様のパソコンにスパイウェアを侵入させパスワードを盗むなどして不正に振込出金するといったケースが報告されています。  
心当たりのない電子メール、不審なCD-ROMやフリーソフト等には十分ご注意ください。  
当金庫は、お客様に安心してお取引いただけるよう、ネットワーク社会の信頼性を損なう悪質な犯罪に対してセキュリティ強化に努めて参りますので、今後とも当金庫をご愛顧くださいませう、よろしくお申し上げます。

**① 注意事項**

- ※ ログインパスワードが分からない場合のお手続きはこちらをご覧ください。
- ※ お客様ID、パスワードは英字の大文字と小文字を区別しますので、ご注意ください。
- ※ サービスご利用中は、「戻る」「進む」等のブラウザのボタンはご利用頂けません。ブラウザのボタンをご利用すると、正常にお取引が出来ない場合があります。
- ※ ご利用のOSおよびブラウザや、「文字の大きさ」「行間の数」の設定によっては、画面のレイアウトが若干崩れる場合がありますが、お取引には影響ありません。

本Webサイト上における各コンテンツは、著作権によって保護されています。

#### -偽画面の特徴-

- (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力します。
- (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。

## 2. 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。

### **(1) 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。

### **(2) 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。

### **(3) 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。

### **(4) 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。

### **(5) 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