

お客さま各位

## ビジネス WEB－FB の偽画面表示によるパスワード搾取について

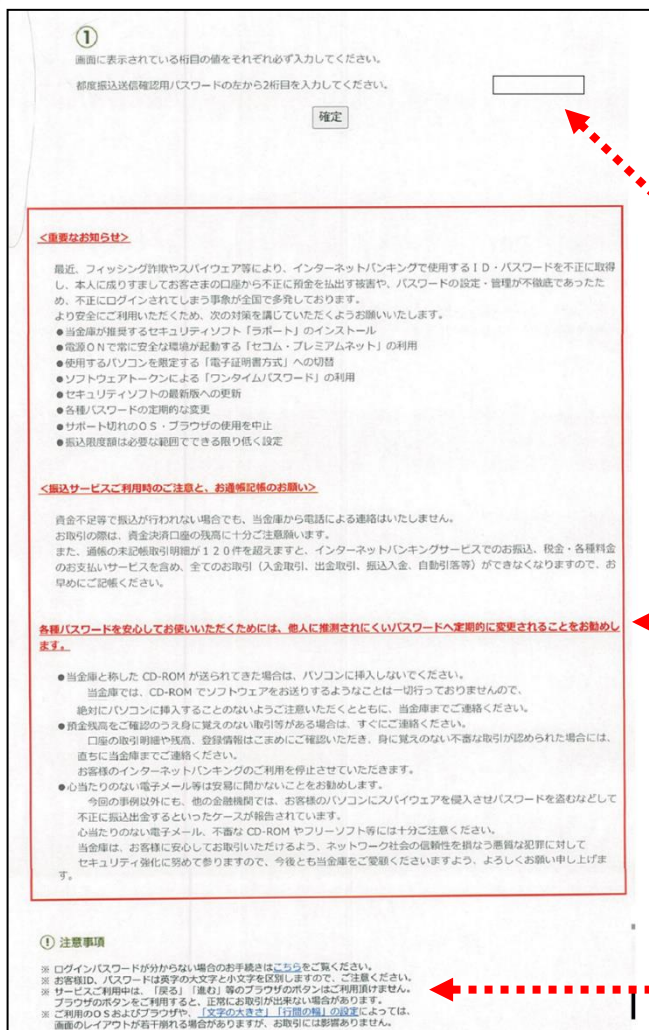
一部の信用金庫におきまして、ビジネス WEB－FB の偽画面を表示させ、お取引に必要な ID・パスワードを盗み取る事例が確認されております。（※11 月現在、当金庫において同様の事案は発生しておりません。）

ビジネス WEB－FB では、ログイン直後に、振込用のパスワードを入力していただくことはありません。

（※初回開通操作、パスワード再設定操作を行う場合のみ、ログイン直後にパスワード変更画面が表示されます。）

普段とは異なる、見慣れない画面でパスワード入力を求められた場合は、絶対にパスワードの入力は行わず、当金庫までご連絡ください。

### 実際に確認された偽画面のイメージ画像



① 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ID・パスワードを不正に取得し、本人に成りすましてお客さま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「ラポート」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固定する「電子証明書方式」への切替
- ソフトウェアアタックによる「ワーム」/「トロイの木馬」/「スパイウェア」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、お迷惑のお願い>**

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、通常の未記帳取引明細が120件を超えたと、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、他人に盗取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。また、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、すぐにご確認ください。  
口座の取引明細や残高、登録情報はごまめに確認いただき、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みなどして不正に振込を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、お客様に安心してご利用いただけるよう、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おりますので、今後とも当金庫をご愛顧ください。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いただけません。  
ブラウザのボタンをご利用すると、正常にお取引いただける場合があります。
- ※ ご利用のOSおよびブラウザは、「文字の大きさ」「画面の幅」の設定によっては、画面のレイアウトが若干異なる場合がありますが、お取引には影響ありません。

① ログイン画面でIDとパスワードを入力すると、左図のような偽画面が表示されます。  
偽画面のURLは本物と同じURLが表示されています。

② 左図では、都度振込送信確認用パスワードの2桁目の入力を要求しています。  
入力を行うと、次は別の桁数の入力を要求してきます。  
この繰り返しにより、犯人はパスワード情報を不正に入手します。

③ 画面中央の<重要なお知らせ>以下は、犯人側が作成した文章です。  
表示されているリンク先へは絶対にアクセスしないでください。

## 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ィルスに感染したことが原因である可能性があります。  
インターネットバンキングをご利用のお客様は、ウィ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。

### ・ウィ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、定期的にウィ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ィルスの検知・駆除には、セキュリティソフト「Rapport」が効果的です。「Rapport」は無料でご利用いただけます。詳細は下記 URL よりご確認ください。

Rapport のご案内 : <http://www.shinkin.co.jp/info/kyotsu/oshirase/20141010/>

### ・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利用者は、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。詳細は下記 URL よりご確認ください。

ワンタイムパスワードのご案内 : [https://hamamatsu-iwata.jp/netbank/business/post\\_5.html](https://hamamatsu-iwata.jp/netbank/business/post_5.html)

### ・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。

### ・ウィ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。

### ・パスワードの管理方法を見直す

パソコンやスマートフォン、クラウドサービスへのパスワード保存はお控えください。ウィルス感染時に情報流出のリスクが高まります。

以 上

【本件に関するお問い合わせ】

浜松いわた信用金庫 ITサポートセンター

0120-186-131

音声ガイダンス【2】をプッシュしてください

受付時間 平日 9:00～17:00

