

インターネットバンキングを安全にご利用頂くためのお願い

最近、ID・パスワード方式で法人インターネットバンキングをご利用のお客さまを狙った不正送金の被害（残高が全て送金される）が多発しています。（「電子証明書」や「ワンタイムパスワード」をご利用されているお客さまでの被害は発生しておりません。）

インターネットバンキングご利用の際には当金庫が提供しております「電子証明書」や「ワンタイムパスワード」を至急お申し込みいただきますようお願いいたします。

詳しくは窓口または下記お問い合わせ先までご連絡ください。

記

1. 被害に遭わないための対策

（１）ID やパスワードは厳重に管理

パスワードは第三者に教えないでください。警察官や当金庫の職員であってもお客さまにパスワードをお尋ねすることはございません。

また、パスワードは定期的に変更してください。

なお、ID やパスワードをメモ等に残したり、パソコン内に電子ファイルで保存しますと、盗み見られるおそれがありますのでご注意ください。

（２）セキュリティ対策ソフトやソフトウェアを最新に

インターネットバンキングをご利用するパソコンには必ずセキュリティ対策ソフトウェアをインストールされ、常に最新の状態に更新してください。

また、OS やブラウザを含む各種ソフトウェアも最新のものに更新して下さい。

（３）身に覚えのないメールや SMS は開かない

スマートフォンやパソコンには毎日多くのメールが届きますが、身に覚えのないメールや SMS は開かないでください。最近は宅配便業者や金融機関を騙った偽のメールが増えています。心当たりがない場合はフィッシングメールの可能性があるのでメールを開かずに削除されることを推奨いたします。

（４）口座の残高をこまめに確認

インターネットバンキングを利用した犯罪はどんどん巧妙になっており、不正送金されても気付けないケースも増えています。知らないうちに被害に遭っていることもございますので、口座の残高はこまめにチェックしてください。

（５）当金庫から届くメールを確認

インターネットバンキングで振込やメールアドレスの変更を行うと、メールにて通知されますので、覚えのない取引が無いか確認してください。当金庫の法人インターネットバンキングシステムから届くメールアドレスは `hib_shinkin@ssc.facetoface.ne.jp` で、当金庫から届くメールアドレスは `〇〇@takaoka-shinkin.co.jp` です。

(6) サポート詐欺に注意

パソコンの画面に「ウイルスに感染しました」「システムエラーが発生しました」等のメッセージが表示され、そこに記載されている番号に電話をかけさせ「ウイルスを除去します」「ソフトのインストールが必要です」等の名目で金銭を詐取する被害が発生しておりますので以下の点にご注意ください。

- ①メッセージで表示された番号には絶対に電話をかけないでください。
- ②ID、パスワード等の大切な情報は他人に伝えないでください。
- ③知らない相手に言われるままにPCを操作しないでください。

2. 当金庫が提供している対策

(1) 電子証明書によるログイン

電子証明書とは電子的に作られた身分証明書のようなものです。電子証明書をパソコンに保存し、電子証明書をインストールしたパソコン以外からはログインできない仕組みとすることにより、不正利用の防止が図れます。

※電子証明書をご利用の場合は申込書の提出をお願いいたします。

(2) ワンタイムパスワードの利用

ワンタイムパスワードとは、振込実行時に都度発行される1度限りのパスワード(30秒間有効)です。ワンタイムパスワードの利用で、パスワードが盗み取られる不正取引を防ぐことができます。

ワンタイムパスワードには、①専用のアプリ生成器に、パスワードを表示させるハードウェアトークンと②スマートフォンにアプリをインストールいただきパスワードを表示させるソフトウェアトークンの2種類がございます。どちらも同様の機能を有しております。

①ハードウェアトークンをご利用の際は申込書の提出をお願いいたします。ハードウェアトークンのご購入には1個につき消費税込みで1,100円(2024年11月1日現在の手数料)が必要となります。

また、ハードウェアトークンの電池寿命は約5年となります。電池切れや故障、紛失等の場合、再度ご購入いただく必要がありますので、当金庫までお申し込みください。

ハードウェアトークンの一例



②ソフトウェアトークンをご利用の場合は以下の二次元コードより無料でインストールいただけます。ご利用開始にあたり、当金庫へのお申し込みは不要です。スマートフォンの機種変更時にもお客さまご自身で変更可能となりますが、新旧のスマートフォンをご準備ください。

ソフトウェアトークンの一例

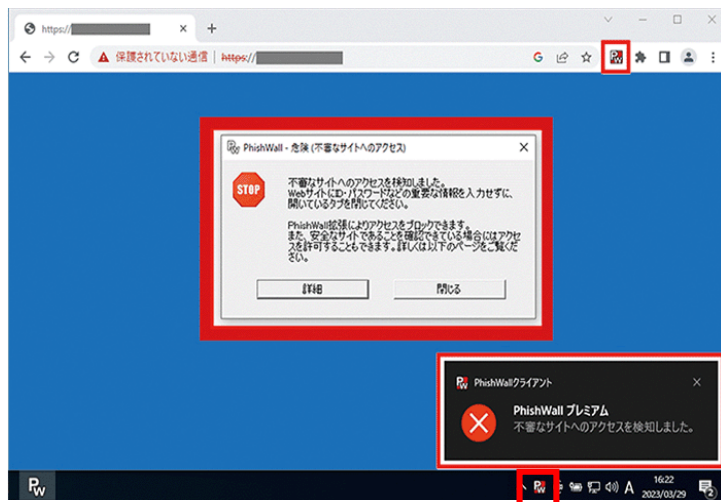


(3) 不正送金・フィッシングサイトを検知する「PhishWall プレミアム」

高岡信用金庫の正規の Web ページにお客さまが接続する際、緑のシグナルを表示して、接続中の Web ページが本物であることを簡単にご確認いただけます。



金融機関のサイトを装って情報詐取等を行うような不審なサイトを対象に、不審なサイトへのアクセスを検知します。検知した場合には警告メッセージが表示されます。



PhishWall プレミアムをインストールするには当金庫インターネットバンキング（個人・法人）の以下のバナーをクリックしてください。



3. 毎月の利用料

電子証明書、ワンタイムパスワード（ハードウェアトークン・ソフトウェアトークン）および PhishWall プレミアムに係る毎月の利用料は必要ありません。

以上

お問い合わせ先
高岡信用金庫 システム部
電話 0766-24-0226