

インターネットバンキングの不正利用にご注意ください。

金融機関を装ったメールを送付し金融機関の偽のホームページへ誘導して、IDやパスワード等の重要情報を入力させ、取得するという詐欺事件「フィッシング詐欺」が発生しております。また、スパイウェアやウイルスなどにより、お客さまから暗証番号（パスワード）などを不正に盗み出し、お客さまになりすまして、お客さまの口座から不正に預金を引き出す被害も発生しております。

本被害に遭われぬよう以下の点にご注意のうえ、インターネットバンキング（WEB-FB・WEBバンキング）サービスをご利用いただきますようお願いいたします。

1. 当金庫はメールのリンクからログインページへの誘導やパスワード等の問合せはいたしません。不審な電子メールに掲載されたリンクはクリックしないことや、身に覚えのないメールは開かないようご注意ください。
2. OSやブラウザは最新版にアップデートしていただき、セキュリティ対策ソフトをご利用ください。
3. インターネットカフェなど、不特定多数の方が利用できるパソコンからのご利用はお控えください。
4. 不審なホームページの閲覧やフリーソフト等をインストールされる際はご注意ください。
5. 身に覚えのないCD-ROMが送られてきた場合は、読み込まないようご注意ください。
6. パソコン内に契約者（お客様）IDや暗証番号（パスワード）などを保存しますと、外部に流出するおそれがありますのでご注意ください。
7. ファイル共有ソフトは利用しないでください。
8. ログイン履歴をご確認いただき、定期的に残高照会、取引履歴照会等を行い、操作された内容であるかご確認ください。また、お取引通知をしておりますので、Eメールアドレスの登録を推奨します。
9. 契約者（お客様）IDや暗証番号（パスワード）は、本人確認するうえで非常に重要な情報です。次の点に注意して、厳重に管理していただきますようお願いいたします。
 - (1) 暗証番号（パスワード）は第三者に絶対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、お客さまに暗証番号（パスワード）をおたずねすることはございません。
 - (2) 暗証番号（パスワード）は推測しづらいものにして、適宜変更してください。
 - (3) IDや暗証番号（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、盗まれるおそれがありますのでご注意ください。
 - (4) パソコンを破棄する際は、専用ソフト等を使用してパソコン内のデータを完全に消去することを推奨します。
 - (5) 他のサイト等で使用している暗証番号（パスワード）は使用しないことを推奨します。
 - (6) 暗証番号（パスワード）の入力時には、キーボードからの直接入力ではなく、ソフトウェアキーボードを利用してください。

不正利用を発見された場合は、速やかに当金庫までご連絡ください。