

金融犯罪にご注意ください

金融機関を装った電子メール等により、二セのホームページにアクセスさせたり、パソコンをウイルス感染させ、二セのログインページに暗証番号やパスワードを入力させることによりお取引に必要な情報を不正に取得し、その情報を使って不正な送金を行うといった事件が発生しています。

◎被害にあわないために

- 最新の状態に更新したウイルス対策ソフトでウイルスチェックを行ったうえで、インターネットバンキングをご利用ください。また、パソコン起動時にはウイルス対策ソフトのスキャン機能でパソコン内をチェックしてからご使用になることをお勧めします。(当行では無料でご利用いただけるセキュリティツールも提供しております)
- OSやブラウザの更新を行い、最新の状態でインターネットバンキングをご利用ください。
- ネットカフェなど不特定多数の方が使用するパソコンでのご利用はお避けください。
- 暗証番号は生年月日や電話番号、「0000」や「9999」といった連番など、他人に類推されやすい番号は使用しないでください。また、暗証番号やパスワードは定期的に変更してください。
- 暗証番号を、貴重品ボックスやロッカー等の他のサービスの暗証番号に使用しないでください。
- 契約者番号やお取引確認番号、確認用パスワード等はパソコン・スマートフォン本体や各種クラウドサービスに保存しないでください。
- 不審な電子メールを不用意に開いたり、通常とは異なる不審なサイトへのアクセスやソフトウェア等のダウンロードはおやめください。(スパイウェア・ウイルスの感染の原因となります)
- ワンタイムパスワードをご利用ください。
- 都度指定振込限度額の引下げをご検討ください。振込限度額を必要最低限に設定することで、被害額を最小限に抑えることができます。
- 金融機関職員が、電話や電子メールで、暗証番号やパスワードを照会することはありません。不審なことがありましたら、お近くの〈ひろぎん〉窓口または〈ひろぎん〉ダイレクトマーケティングセンターにご連絡ください。

◎被害を早期に発見するために

- インターネットバンキングのログイン履歴をご確認ください。(ログイン履歴はインターネットバンキングのホーム画面で直近3回分がご確認いただけます)
- お取引後に金融機関が送付する取引完了メールをご確認ください。すぐに確認できるよう、登録するメールアドレスは、携帯電話・スマートフォンのメールアドレスをお勧めします。