
インターネットバンキングにおける フィッシング詐欺にご注意ください

インターネットバンキングにおけるフィッシング詐欺とは、実在する金融機関等を装う偽メールなどから、本物と酷似した偽のサイト（フィッシングサイト）へ誘導し、IDやパスワードの入力を促し情報を盗み取り、その情報を基に本物のサイトからログインし、不正送金を行うという手口です。他にも、メールの不正な添付ファイルや改ざんされたWEBサイトを閲覧することでウイルスに感染させ、正規のサイトへのアクセスを検知すると、偽のログインページをポップアップ画面で表示させ、IDやパスワードの入力を促すといった手口があります。

これらのフィッシング詐欺を防止するために、以下の点にご注意いただきますようお願い申し上げます。

1. 心当たりのないメールは開かないでください。
当金庫から、個人情報やパスワードなどの重要情報について、メールで問い合わせをしたり、回答をお願いするようなことはありませんので、当金庫を装った不審なメール等を受信した場合は、直ちに当金庫までご連絡ください。
また、万一メールを開いてしまった場合は、以下の操作をしないようご注意ください。
 - ・メールに添付されたファイルを開くこと
 - ・メールに記載されているリンクをクリックすること
 - ・個人情報やパスワード等の重要情報を入力すること
2. OSやブラウザは、推奨環境をご参照のうえ、最新の状態でご利用ください。
なお、Windows7等のサポートが終了したOSやブラウザ等を使用しないでください。
3. セキュリティソフトを導入していただくとともに、最新の状態で更新したうえで定期的にウイルスチェックを行ってください。
また、当金庫が推奨する以下のセキュリティ対策も併せてご利用ください。
 - ・ウイルス対策ソフト「ラポート」
 - ・ワンタイムパスワード（個人インターネットバンキング）
 - ・電子証明書（法人インターネットバンキング）
4. 1回あたり、1日あたりの取引限度額は必要最低限の金額に設定してください。

その他の注意事項につきましては以下のページをご参照ください。

- ・インターネットバンキングを安全にご利用いただくために
http://www.shinkin.co.jp/info/security_02/index.html