2026年6月30日

お客さま 各位

株式会社 荘内銀行

インターネット取引サービスへの不正アクセス・不正取引による被害を防ぐために

インターネットバンキングへのアクセスに必要な ID やパスワード等の情報が第三者に盗み取られ、それらの情報を不正に利用し、他人名義の銀行口座へ不正送金が行われる被害が発生しております。

その手口として、金融機関担当者になりすまし、お客さまの情報を聞き出す不審な電話（ボイスフィッシング）や、遠隔操作ソフトをインストールさせ企業側の端末を遠隔操作する事例が確認されています。

このような被害に遭わないために、ご自身の対策状況について、以下のチェックをお勧めいたします。

〈チェック項目〉

☐ インターネットバンキングの ID やパスワードなどは、決して第三者に教えない。

☐ 銀行を騙る不審な電話を受けた場合は、銀行の取引店・代表電話に折り返し電話するなど慎重に対応する。

☐ パソコン利用中に警告画面や警告音が出ても、画面に表示された連絡先には連絡しない。

☐ パソコン利用中に不審な表示（普段と違うログイン画面、不自然なポップアップ、追加の個人情報入力要求など）が出て情報の入力を求められても、それに応じない。

☐ 不審なメールや SMS、添付ファイル、リンクを開かない。

☐ パスワードは、推測が容易な単純なものを用いない。また、同じパスワードを使い回さない。

☐ OS やソフトウェアは、常に最新の状態に更新する。

☐ ソフトウェアは、必ず公式サイトや正規のアプリストアからダウンロードする。

☐ セキュリティソフトを導入し、定期的なセキュリティスキャンを実施する。

※セキュリティソフトは、振る舞い検知機能やウェブ保護機能を持つ総合セキュリティソフトの利用を推奨します。定義ファイル（マルウェア検出用ファイル）は常に最新の状態に更新してください。

☐ マルウェア感染防止のため、ブラウザから通常行わないキーボード操作を求められても実行しない。
（特にマルウェア感染に悪用される「Ctrl + V」等のショートカット実行）

☐ 不正送金・フィッシング対策ソフト「Phish Wall プレミアム」を利用する。

※お使いのパソコンにインストールすることで、アクセスしている当行サイトが本物かどうかを確認いただけます。当行ホームページで無償提供しておりますので、ご利用ください。

荘内銀行ホームページ　https://www.shonai.co.jp/information/phishwall/

マルウェアには、通信乗っ取りにより画面上の表示を偽装しながら裏側で第三者の口座に送金を実行するタイプ、画面録画やスクリーンキャプチャによりユーザーが入力した情報や画面上の認証情報を盗み出すタイプなどさまざまなものがあります。防止にあたっては、上記のチェック項目を徹底することに加え、日頃からインターネットの利用に十分な注意を払うことが重要です。

チェック項目にあるリスクの高い行為を実施してしまった、不審な事象があったなど、ご相談がある場合は下記センターまでご連絡ください。

以　上

＜本件に関するお問い合わせ先＞

荘内銀行コンタクトセンター　フリーダイヤル：0120-1032-39

【受付時間】平日 9：00～19：00