【重要】

MITB攻撃にご注意ください

２０２０年７月以降からＭＩＴＢ（Man-in-the-Browser）攻撃による不正送金犯罪が増加している旨の情報がありましたので十分にご注意ください。

MITB（Man-in-the-Browser）攻撃とは、パソコンがマルウェアに感染することで発生します。インターネットバンキングユーザーの端末上の Web ブラウザを乗っ取りアカウント情報を盗み見たり、ブラウザ上の画面を書き換え送金情報を変更することでユーザーの預金を不正に送金します。

不正送金被害防止の対策について

インターネットバンキングのＩＤ、各種パスワード、各種暗証番号の情報等が第三者に知られた場合、インターネットバンキングで不正送金される被害につながる恐れがありますので十分にご注意ください。

■ 最新状態のウィルス対策ソフトを利用してください。

■ 不正送金対策ソフト「PhishWall プレミアム」（無料）を導入してください。

■ 当組合から電子メールやＳＭＳ（ショートメッセージサービス）でログイン画面やパスワード変更画面等に誘導することはありません。

■ 不審な電子メールやＳＭＳ（ショートメッセージサービス）を受信した場合はすぐに削除し、記載されたリンク先へのアクセスやパスワード等の入力は絶対にしないでください。

■ 必ず URL を確認して、不審なサイトにはアクセスしないでください。

【正しい URL】

https://www.nozomi.shinkumi.jp/～　（のぞみ信用組合ホームページ）

https://www.nozomi.shinkumi.net/～　（のぞみ信用組合ホームページ［ミラーサイト］※1）

※1【通常サイトアクセス不能時の接続先 URL】

https://www.parasol.anser.ne.jp/～（個人向けインターネットバンキング）

https://www.bizsol.anser.ne.jp/～　（法人向けインターネットバンキング）

のぞみ信用組合