

【重要】

フィッシング攻撃に対する警戒のお願い

令和4年8月下旬から9月にかけて、金融機関を騙ったフィッシングメールによりフィッシングサイトへ誘導され、インターネットバンキングのパスワード等の情報が窃取されることにより、不正送金が行われる手口による被害が急増して以来、一旦被害は減少傾向となったものの、令和5年2月以降、被害が急増している状況です。

次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出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。

インターネットバンキングのID、各種パスワード、各種暗証番号等

- 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に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