偽Ｅメール　偽ショートメッセージ（ＳＭＳ）等による情報搾取に注意！！

現在、金融機関を名乗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おります。

「カード・通帳の利用停止、再開のお手続の設定をして下さい」

「あなたの預金口座はリスクが検出されましたので、この口座を制限します。解除するためには、下記のリンクから再登録をお願いいたします」

この様な身に覚えのない内容の偽メールが送られ、偽メールのリンク先画面へ誘導され、ワンタイムパスワードを入力させて盗み取る等の手口です。

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://kimishin.jp/（君津信用組合ホームページ）

https://www.parasol.anser.ne.jp/ib/index.do?PT=BS&CCT0080=2190

（インターネットバンキング（個人向け））

https://www.bizsol.anser.ne.jp/2190c/rblgi01/I1RBLGI01-S01.do

（インターネットバンキング（法人向け））

いつも ずっと あなたのそばに

君津信用組合