お客様各位

令和２年２月

フィッシング攻撃に対する警戒のお願い

2019 年 9 月頃から、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おります。

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】

http://www.kyouritsu.shinkumi.co.jp/～（共立信用組合ホームページ）

https://www.parasol.anser.ne.jp/～（共立信用組合インターネットバンキング）

☆ 当組合ではフィッシング詐欺への対策として、ホームページの常時ＳＳＬ化を行う予定です。ＳＳＬ化後は URL が下記のように変更になりますのでご注意ください。

※ＳＳＬとはデータのやり取りを暗号化し盗聴や改ざんを防ぐ仕組みです。

【ＳＳＬ化後の正しい URL】（「共立信用組合ホームページ」URL の先頭が「https://」に変わります）

https://www.kyouritsu.shinkumi.co.jp/～（共立信用組合ホームページ）

共立信用組合