

金融機関を騙った、偽Eメールや偽ショートメッセージ（SMS）等にご注意下さい

現在、金融機関を騙ったEメールやショートメッセージ（SMS）を配信して、正規の金融機関のホームページに似せた不審なサイト（フィッシングサイト）に誘導させて、お客様のインターネットバンキングのパスワード等の情報を盗み取り、不正に送金を行う手口による被害が急増しています

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、十分ご注意くださいようお願いいたします。

- ・インターネットバンキングのログインIDやパスワード
- ・ワンタイムパスワード
- ・各種暗証番号
- ・各種パスワード

- 当組合からEメールやショートメッセージ（SMS）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Eメールやショートメッセージ（SMS）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。
- 当組合のホームページおよび大信インターネットバンキング・大信ビジネスバンキングの正しいURLは以下の通りです。
※～以降は閲覧しているサイトによって変更されます。

〈大東京信用組合ホームページ〉

<http://www.daisin.co.jp/>～

〈大信インターネットバンキング〉

<https://www.parasol.anser.ne.jp/>～

〈大信ビジネスバンキング〉

<https://www.bizsol.anser.ne.jp/>～

不正送金被害防止のため、当組合ホームページよりセキュリティ対策ソフト「PhishWallプレミアム」（偽サイト判定ソフト）をご利用ください。

インターネットバンキングに関するお問い合わせ先
大信インターネットバンキングヘルプデスク
TEL：0120-828-139
平日9：00～24：00 土日祝9：00～17：00