

## マネロン等対策を騙ったフィッシングメールにご注意ください

金融機関を装い、マネー・ローンダリングおよびテロ資金供与対策（以下、マネロン等対策）の名目で、キャッシュカードの暗証番号、インターネットバンキングのログインID・パスワード、クレジットカード番号等を不正に入手しようとするフィッシングメール（金融機関等になりすましたメール）が確認されています。

当行では、マネロン等対策の一環として、お取引の内容や状況等に応じて、過去に確認した氏名、住所、生年月日、ご職業や取引の目的等について、窓口等で再度確認をさせていただき取り組みを行っておりますが、お客さまの「暗証番号」、インターネットバンキングの「ログインID・パスワード」等を、メールやSMSでお問い合わせすることも、メールやSMSでウェブサイトに誘導した上で入力を求めるようなことはございません。

こうしたフィッシングの被害に遭わないために、次の対策をとるなど、十分にご注意をお願いいたします。

- ・心当たりのないメールやSMSに掲載されたリンク等は開かないでください。
- ・当行からの不審なメールやSMS等を受信した場合には、当行に電話で問い合わせてください。
- ・当行のウェブサイトへのアクセスに際しては、事前に正しいウェブサイトのURLをブックマーク登録しておき、ブックマークからアクセスしてください。
- ・パソコンのセキュリティ対策ソフトを最新版にしてください。
- ・お客さまの「暗証番号」、インターネットバンキングの「ログインID・パスワード」は他人に教えないでください。また、紙等書き留めたりしないでください。

## 《フィッシングメール・SMSの例》

### 重要なお知らせ

当行では金融庁によるマネー・ローンダリング及びテロ資金供与対策に関するガイドライン等を踏まえ、お客さまが当行にご登録されている各種情報等について、メール、DMなどの方法で、現在の情報に更新されているかどうかのご確認をさせていただいております。

お客さまにはお手数をおかけすることとなりますが、ご理解、ご協力のほど、よろしくお願い申し上げます。

#### ■対象項目

・氏名/住所/自宅電話番号/口座番号/暗証番号/ID・パスワード 等

#### ■ご利用確認はこちら

<http://〇〇〇〇・・・> (偽サイトのURL)

誠に勝手ながら本メールは発信専用アドレスより配信しております。

本メールにご返信いただきましてもお答えすることができませんのでご了承ください。

以 上

(参考)

- ・ [フィッシング 110 番](#) (警察庁ウェブサイト)
- ・ [金融犯罪の手口ーフィッシング詐欺ー](#) (全国銀行協会ウェブサイト)