

## **当社を偽装した不審メール・SMSにご注意ください**

実在する金融機関を偽装した不審メール・SMS による被害が多発しています。不正な添付ファイルやリンクを開くことで、コンピュータウイルスに感染したり、偽のウェブサイト（フィッシングサイト）で個人情報を入力させられ、悪用される恐れがあります。不審なメール・SMS が届いた場合は、添付ファイルやリンクを開かず、そのメール・SMS をすぐに削除してください。また、不審なウェブサイトでは決して個人情報を入力しないよう十分にご注意ください。

### **不審なメール・SMS を受信した場合**

昨今の不審なメール・SMS や偽のウェブサイトは非常に巧妙に作られており、一見しただけでは不正なものであると気づきにくくなっています。

#### **<偽のメール・SMS の特徴>**

- お客さまの個人情報（ID・パスワード・氏名・生年月日等）の入力を要求している
- 記載されている URL が当社の正規ウェブサイトと異なっている
- 身に覚えのない手続きを要求している

### **ウェブサイト上不審な点を見つけた場合**

不審なリンクを開いてしまったり、ウェブサイトの操作中に不審な表示（普段と違うログイン画面、不自然なポップアップ画面、追加の個人情報入力要求など）を見つけた場合は、決して個人情報等（ID・パスワード・氏名・生年月日等）を入力せず、すぐにブラウザを閉じてください。万が一、個人情報等を入力してしまった場合は、速やかにパスワードを変更してください。

### **日常の備え（セキュリティ対策）**

日常のセキュリティ対策が不足していると、知らぬ間にウイルスに感染し、正規のウェブサイト进行操作していても個人情報が窃取されてしまう恐れがあります。以下の対策を心がけてください。

- 推測されやすいパスワードは使用しない
- 同じパスワードを使い回さない
- ウイルス対策ソフトをインストールする
- ソフトウェアを常に最新の状態にアップデートする

以 上