

# インターネット犯罪対抗チェックポイント

インターネットバンキング犯罪に合わないために、必ず確認と実施していただきたいこと

## 電話を使った不正犯罪防止のための注意事項

- 金融機関や警察・役所を騙り、電話で個人情報(ログインIDやパスワード・暗証番号・口座番号等)を聞き出し、不正を行う手口が蔓延しています。
- 金融機関が電話でログインIDやパスワードを聞くことはありません。「ログインIDやパスワードを教えてください」と言う電話は全て詐欺です。
- 役所職員や金融機関・警察官等が絡んだ複数人による電話や、機械音声による督促など手口が巧妙化しています。少しでも不審と感じられた場合は当該金融機関または警察にご連絡ください。

## ウイルス感染防止のための注意事項

- 不審なメールの開封や添付ファイルのクリック等には十分注意してください。
- 金融機関を名乗る手口も増えていきますので少しでも不審と感じられた場合は当該金融機関にご確認ください。

## ご利用パソコンの挙動について

- パソコンの立ち上がりが異常に遅い、インターネットの閲覧がよく途切れるようになった等、普段と異なる挙動は感染の可能性があります。
- ウイルス検索を実行し、発見した場合はウイルス駆除を行ってください。

## 不正利用の確認

- ログイン履歴、お取引の照会を行い、見覚えのない取引がないか確認してください。また、残高の確認も実施ください。

## ログイン時の注意事項

- ワンタイムパスワードをご利用ください。格段に安全性が高まります。ご採用を検討ねがいます。  
個人のお客様 ; ソフトウェアトークン  
法人のお客様 ; ソフトウェアトークンまたはハードウェアトークン
- 電子証明書方式をご利用ください。  
※法人のお客様

## 不審なメール等から誘導された当組合ログイン画面にはご注意ください。

- 巧妙に偽装されたメールが蔓延しています。  
利用実績のあるブックマークや当組合ホームページログイン画面からのログインを推奨します。
- 少しでも疑問を持たれるような画面が表示された場合は当組合までご連絡ください。

## 資金移動関連について

- 必要以上の限度額申込を行っていないか確認のうえ適正な金額への見直しをお願いいたします。

## 【近年増加しているインターネットバンキング被害について】

最近、以下のような被害事例が増加しております。十分ご注意ください、安全対策を徹底してください。

### 1. フィッシング詐欺

【事例】: 信頼できる企業や金融機関を装ったメールや SMS が送られてきて、偽のウェブサイトに誘導し、個人情報やログイン情報を入力させる手口です。

【対策】

- メールや SMS のリンクをクリックする前に、その正当性を確認してください。
- 公式サイトに直接アクセスしてログイン情報を入力してください。
- 疑わしいメールや SMS は削除し、情報を提供しないでください。

### 2. マルウェア感染

【事例】: 悪意のあるソフトウェア(マルウェア)をパソコンやスマートフォンに感染させ、キー入力を記録するキーロガーや、スクリーンショットを撮るスパイウェアなどにより情報を盗まれる手口です。

【対策】

- 最新のウイルス対策ソフトをインストールし、定期的に更新してください。
- 信頼できないウェブサイトからファイルをダウンロードしないでください。
- 不審なリンクや添付ファイルを開かないでください。

### 3. スミッシング(SMS フィッシング)

【事例】: SMS を利用して、金融機関や宅配業者を装い、偽のウェブサイトに誘導して情報を盗む手口です。

【対策】

- SMS 内のリンクをクリックする前に、送信元を確認してください。
- 不審な SMS は無視し、必要に応じて金融機関に直接連絡してください。

### 4. ソーシャルエンジニアリング

【事例】: 人間の心理的な隙を突いて情報を盗む手口です。例えば、電話やメールで正規のサポート担当者を装い、個人情報やログイン情報を聞き出します。

【対策】

- 電話やメールで個人情報を求められても、安易に提供しないでください。
- 正規のサポート担当者であるかどうか確認するために、公式の連絡先を使用してください。

### 5. 公共 Wi-Fi の利用による情報漏えい

【事例】: 公共の Wi-Fi を利用してインターネットバンキングにアクセスし、通信が盗聴されて情報が漏洩する手口です。

**【対策】**

- 公共の Wi-Fi を利用してインターネットバンキングにアクセスしないでください。
- 信頼できるネットワークを使用し、VPN(仮想プライベートネットワーク)を利用してください。