

インターネット・バンキングをご利用のお客さまのセキュリティ対策について

最近、マスコミで報道されておりますように、インターネット・バンキングにおいて、不正送金被害が増加しています。ご利用者におかれましては、以下のセキュリティ対策を実施していただきますようお願いいたします。

なお、お心当たりのないお振込み等がありましたら、速やかにお取引信用組合までご連絡ください。

1. インターネット・バンキングのご利用者は、以下の対策を実施していただきますようお願いいたします。

(1) ウイルスの感染防止・・・パスワード等を漏えいさせない。

不審なサイト、メールは開かず、パソコンには必ずセキュリティソフトを導入して、ウイルス定義ファイル等を最新版へアップデートする。

また、パソコンがウイルスに感染していないことを定期的を確認する。

(2) パスワードの定期的な変更・・・漏えいしたパスワードを無効化する。

類推され易いパスワードは使用せず、パスワードも定期的に変更する。

また、インターネットカフェ等のパソコンで、インターネットバンキングは利用しない。

2. 特に法人向けインターネット・バンキングのご利用者におかれましては、上記1の対策を実施していただくとともに、以下の対策を実施していただきますようお願いいたします。

(1) 電子証明書のセキュリティ強化やインターネット・バンキング専用のセキュリティ対策ソフトの導入など、当組合が提供しているセキュリティ対策を実施する。

※取扱組合が指定した正規の手順以外で電子証明書を利用しない。

(2) 不正アクセスの検知・・・不正送金を未然に察知する。

インターネットバンキングの利用有無に関わらず、随時、残高照会、利用履歴を確認して、不審な取引がないかを確認する。

※取引通知メールの宛先を携帯電話等に設定し、退社後の不正アクセスについても検知する。

(3) 振込上限金額は必要最低限を設定する。

(4) PCを利用していないときは、PC電源をオフにする。

(5) メール通知・ワンタイムパスワードを利用する場合、メール送信先のアドレスを、携帯電話等のPCとは別媒体に設定する。

(6) 操作者と承認者の権限を設定し、別々のパソコンで利用する。