

重要：必ずお読みください

インターネットバンキングを安全にご利用いただくために

- 当組合は、全国銀行協会による申し合わせの主旨を踏まえ、不正な払戻し被害の拡大抑止に努めています。
- しかしながら、最近は犯罪の手口が高度化・巧妙化し、被害が拡大しております。そのため、当組合ではセキュリティ対策事例を複数組み合わせて講じていくことが必要であるとの認識にたち、引き続きインターネットバンキングにおけるセキュリティ対策の強化の取り組みを進めてまいります。
- お客様におかれましては、インターネットバンキングを安全にご利用いただくため、当組合が導入し、推奨しているセキュリティ対策を積極的にご利用いただくとともに、「(別紙1)」に記載した事項を実施いただきますよう、ご協力をお願いいたします。
- なお、当組合はインターネットバンキングにおける預金等の不正な払戻しが発生した場合には、お客様が被害に遭われた状況等を踏まえ、個別の事案ごとに補償いたします。ただし、補償を減額する、もしくは補償をしない取扱いをする場合がございます。事例について「(別紙2)」のとおりまとめましたので、あらかじめご承知くださいますようお願いいたします。

(別紙1) お客様に講じていただくセキュリティ対策事例

(別紙2) 補償減額または補償せずの取扱いとなりうるケースについて

【お問合せ先】

神奈川県医師信用組合 インターネットバンキング担当

電話番号 045-640-5000

または、お取引店にお問合せください。

受付時間 平日 9:00 ~ 17:00

(土・日・祝日・年末年始を除く)

お客さまに講じていただくセキュリティ対策事例

お客さまにインターネットバンキングを安心してご利用していただくために、以下のセキュリティ対策の実施をお願いいたします。

1. お客さまに実施していただくセキュリティ対策

- (1) 組合が導入しているセキュリティ対策を着実に実施していただくこと
- (2) インターネットバンキングに使用するパソコン(以下、「パソコン」という。)に関し、基本ソフト(OS)やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新していただくこと
- (3) パソコンにインストールされている各種ソフトウェアで、メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を止めていただくこと
- (4) パソコン上にセキュリティ対策ソフトを導入するとともに、最新の状態に更新したうえで、稼働していただくこと
- (5) インターネットバンキングに係るパスワードを定期的に変更していただくこと
- (6) 当組合が指定した正規の手順以外でのワンタイムパスワードの利用は止めていただくこと

2. お客さまに推奨するセキュリティ対策

- (1) パソコンの利用目的として、インターネット接続時の利用はインターネットバンキングに限定していただくこと
- (2) パソコンや無線LANのルータ等について、未利用時は可能な限り電源を切断していただくこと
- (3) 振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定していただくこと
- (4) 不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかを定期的に確認していただくこと

補償減額または補償せずの取扱いとなりうるケースについて

以下のようなケースでは、当組合はそれぞれの事情を個別に判断したうえで、補償を減額する、もしくは補償をしない取り扱いとする場合があります。

1. 以下のような対応がお客さまに実施されていないケース

- (1) 「(別紙1) 1.」のセキュリティ対策の導入
- (2) 身に覚えのない残高変動や不正取引が発生した場合の、一定期間内の当組合への通報
- (3) 不正取引が発生した場合の、一定期間内の警察への通報
- (4) 不正取引が発生した場合の、当組合による調査および警察による捜査への協力

2. お客さまに過失があると考えられる以下のような事象が認められたケース

- (1) 正当な理由なく、他人にID・パスワード等を回答してしまった、あるいはトークン等を渡してしまった場合
- (2) パソコンや携帯電話等が盗難に遭った場合において、ID・パスワード等をパソコンや携帯電話等に保存していた場合
- (3) 当組合が注意喚起しているにも関わらず、注意喚起された方法で、メール型のフィッシングに騙される等、不用意にID・パスワード等を入力してしまった場合

3. その他、以下のような事例に相当するケース

- (1) お客さまの関係者の犯行であることが判明した場合
- (2) その他、上記2.の場合と同程度の注意義務違反が認められた場合