

令和5年11月1日

お客様各位

北伊勢上野信用金庫

法人向けインターネットバンキングの被害補償について

平素より弊庫WEB-FBサービス、WEBバンキングサービスをご利用いただきありがとうございます。

弊庫では、平成26年7月17日付全国銀行協会による申し合わせ（法人向け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に関する補償の考え方）の主旨を踏まえ、法人向けインターネットバンキングの不正利用被害について、下記のとおり被害補償を行いますのでご連絡申し上げます。

また、**電子証明書方式およびワンタイムパスワードをご利用でないお客様（*1）におかれましては、被害補償額の減額対象となります。**不正利用被害防止のため、当金庫が推奨しているセキュリティ対策を実施いただきますようお願いいたします。

記

1. 対象のお客様

以下のサービスをご契約されている法人のお客様となります。

- ・WEB-FBサービス（基本契約、一般契約）
- ・WEBバンキングサービス

2. 補償対象

第三者がID・パスワード等を盗用し、お客様が上記サービスを不正利用されたことにより被った損害を対象とします。

3. 補償限度額

1契約につき上限1,000万円

4. 補償条件

当金庫は、法人のお客様が不正利用被害に遭われた状況等を踏まえ、個別の案件ごとに補償いたします。

- (1) 不正利用被害に遭った翌日から30日以内に当金庫への通知が行われていること。
- (2) 不正利用被害に遭った状況等について、当金庫が行う調査に対し、お客様から遅延なく十分な説明が行われていること。
- (3) お客様が警察に被害届を提出し捜査に協力していること。

5. 補償の対象とならない場合

ご利用状況によっては、補償の対象にならない場合がございます。

- (1) 不正な資金移動等が行われたことについて当金庫が善意かつ無過失であり、かつ、次のいずれかに該当する場合
 - ① お客様の配偶者、二等親内の親族、同居の親族、その他の同居人、または家事使用人によって行われた場合。
 - ② 法人の場合、役員、従業員または使用人等（パート、アルバイト、派遣社員等を含みます）によって行われた場合、もしくはそれらの者が加担した盗用によって行われた場合。
 - ③ お客様が、被害状況についての当金庫に対する説明において、重要な事項について偽りの説明を行った場合。
 - ④ お客様が正当な理由なく、他人の各種IDやパスワード等を知らせた場合。
 - ⑤ お客様がパソコンや携帯電話の盗難に遭った場合または廃棄処分をした場合に、各種IDやパスワード等をパソコンや携帯電話に保存していた場合。
 - ⑥ 当金庫が注意喚起しているメール型のフィッシングにだまされる等、不用意に各種IDやパスワード等を入力していた場合。
 - ⑦ 他人に譲渡・貸与または担保に差入れられたパソコン等の不正利用によって生じた損害の場合。
 - ⑧ 不正利用被害が当金庫への通知日の30日以前に発生していた場合。
 - ⑨ その他、お客様に故意または重大な過失があると考えられるような事象が認められた場合。
- (2) 戦争、暴動等による著しい社会秩序の混乱に乗じてまたはこれに付随して不正な資金移動等が行われた場合

6. 補償を減額する場合

ご利用状況によっては、補償を減額する場合がございます。

- (1) 電子証明書方式を利用していない場合。
- (2) ワンタイムパスワードを利用していない場合。
- (3) ウイルス対策ソフト等（当金庫が導入しているセキュリティ対策ソフト（Rapport）を含む（*2））のセキュリティ機能を利用していない場合。
- (4) ウイルス対策ソフト等を最新の状態で利用していない場合。
- (5) 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が最新の状態に更新されていない場合。
- (6) 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がサポート期限終了後も使用されている場合。
- (7) 各種IDやパスワード等が適切に管理されていない場合。
- (8) その他お客様に過失があると考えられるような事象が認められた場合。

7. 当金庫が推奨しているセキュリティ対策

当金庫では、次のセキュリティ対策を推奨しております。被害を未然に防ぐためにご確認のうえ対策を講じていただきますようお願い申し上げます。

- (1) 電子証明書方式の利用
- (2) ワンタイムパスワードの利用
- (3) セキュリティソフトによる定期的なウイルスチェック、基本ソフト（OS）やウェブブラウザは最新の状態へ。
- (4) 金融機関などを装った電子メールや金融機関などのホームページ（偽サイト）へ誘導して、IDやパスワードなどの重要情報を入力させて搾取するフィッシング詐欺に注意。
- (5) 重要な取引が行われた際の取引通知メール、ログインログアウト履歴を確認。
- (6) 定期的に残高照会、取引履歴照会、入出金履歴照会を行い、不正利用・不正引き出しの有無を確認。

〔注記〕

*1：お客様には、法人の役員、従業員や家族等の関係者、退職者を含みます。

*2：お客様のご利用環境により、本ソフトがご利用できない場合を除きます。

<本件に関するお問い合わせ先>

北伊勢上野信用金庫E Bサービスセンター

電話：0120-497-004

(平日9:00～17:00)