

法人インターネットバンキングを
ご利用のお客さま 各位

法人インターネットバンキングの不正利用に係る被害補償について

蒲郡信用金庫では、法人のお客さま向けのインターネットバンキング（以下、「法人 I B」といいます）を安心してご利用いただくため、不正利用に係る被害補償を下記のとおりとさせていただきます。

記

1. 対象のお客様

法人 I Bをご契約されているお客様

2. 法人 I Bの不正利用に係る被害補償について

- (1) お客様の「過失」等については、被害に遭われた状況等を踏まえ、個別の事案ごとに補償の判断をさせていただきます。
- (2) 被害補償額は、1口座につき年間1,000万円を上限とします。

3. 被害補償を受けるための注意点

- (1) 法人 I Bを使用するにあたって、下記「5. お客様に講じていただくセキュリティ強化策について」を実施して下さい。
- (2) 不正利用が発生した場合、発生日の翌日から30日以内に当金庫へ被害の届出をして下さい。
- (3) 不正利用が発生した場合、当金庫による調査および警察による捜査への協力をして下さい。

4. 被害額の全部に関して補償しかねる場合について

- (1) 会社関係者の犯行であることが判明した場合。
- (2) お客様の配偶者、二親等内のご親族、同居のご親族、その他のご同居人、または家事使用人(家事全般を行っている家政婦など)の犯行であることが判明した場合。
- (3) 被害状況についての当金庫に対するお客様のご説明において、重要な事項に関し偽りがあった場合。
- (4) 戦争、暴動などによる著しい社会秩序の混乱に乗じまたはこれに付随して法人 I Bが不正に使用された場合。
- (5) その他、重大な注意義務違反が認められた場合。

5. お客さまに講じていただくセキュリティ強化策について

- (1) お客さまに実施していただくセキュリティ強化策
 - ① 当金庫が提供しているセキュリティ強化策（電子証明書、ワンタイムパスワード、ウイルス対策ソフト「**Rappport**（ラポート）」）等を確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」といいます）に関し、推奨の基本ソフト（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を使用しないこと。
- ④ パソコンにウイルス対策ソフトを導入するとともに、パターンファイル（ウイルスを特定して駆除するために必要なファイル）を最新の状態に更新したうえで、稼動していただくこと。
- 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 当金庫が指定した正規の手順で電子証明書を利用していただくこと。
- ⑦ 下記「6. ID・パスワード管理について」を実施していただくこと。

(2) お客様に推奨するセキュリティ強化策

- 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 取引の申請者と承認者とで異なるパソコンを利用していただくこと。
- ④ 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。
- ⑤ 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を確認していただくこと。

6. ID・パスワードの管理について

- (1) ID・パスワード等は他人に知らせないでください。
- (2) 生年月日、電話番号、住所・地番、自動車等のナンバーなど他人に推測されやすい番号をパスワードに使用しないでください。
- (3) ID・パスワード等をパソコンのファイルやメール等に保存しないでください。
- (4) ID・パスワード等は、メモ等の紙に残さないようにしてください。
- (5) インターネットカフェなど不特定多数の人が利用する場所のパソコン等で、インターネットバンキング取引を行わないでください。
- (6) 当金庫からメール等でお客様の ID・パスワードをお聞きすることはありませんので、ご注意ください。
- (7) パスワード入力の際は、ソフトウェアキーボードをご利用ください。

以上