

平成27年12月1日

お客さま各位

「法人インターネットバンキング」の不正利用による被害の補償について

平素は格別のご高配を賜り、厚く御礼申し上げます。

宮城第一信用金庫では、法人のお客さま向けのインターネットバンキングを安心してご利用いただくため、平成27年12月1日（火）から、「宮城第一信用金庫 法人インターネットバンキング」により不正な預金払戻しに遭われた場合の被害補償を下記のとおりといたします。

また、当面の間、法人・個人のインターネットバンキングの新規契約を見合わせていただきますので、ご理解のほど宜しくお願いいたします。

記

1. 補償開始日

平成27年12月1日（火）

2. 対象となるお客さま

「宮城第一信用金庫 法人インターネットバンキング」にて預金の不正な払戻しの被害に遭われたお客さま

3. 補償限度額

1 ご契約あたり年間1,000万円まで

4. 補償金額について

当金庫が提供しているセキュリティ対策（ウイルス対策ソフト等）を行っていない場合や、パスワードの管理に問題があった場合など、個別の事案ごとにお客さまのお話をお伺いしたうえで内容によっては被害補償の対象外または補償額を減額させていただくことがございますのでご了承ください。詳細は別紙の内容をご参照ください。

5. 被害に遭われた場合

身に覚えのない不審なお取引、パスワードなどが他人に知られた、または、知られた恐れがある場合には下記相談センターまたはお取引店まで至急ご連絡ください。

本件に関するお問い合わせ先
宮城第一信用金庫 お客さま相談センター
022-722-3842
(受付時間：平日9：00～17：00)
担当：工藤、高橋

(別紙1)

被害補償の対象外または減額となりうる主な事例

- 当金庫が提供しているセキュリティ対策(ウイルス対策ソフト「Rapport(ラポート)」等)を利用していない場合
- インターネットバンキングに利用するパソコンの基本ソフト(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が最新の状態に更新されていない場合
- 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を使用している場合
- パソコンにセキュリティ対策ソフトを導入し、最新の状態に更新していない場合
- 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ない場合
- ID・パスワード等が管理不十分により他人が知りえる状態になった場合
- パソコン等が盗難された場合においてID・パスワード等をパソコン等に保存していた場合
- 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
- 警察へ被害届を提出していない場合
- 不正な払戻しの発生した翌日から30日以内に当庫への届出がない場合
- 被害調査にご協力いただけない場合や重要な事項について偽りの説明を行った場合
- お客さま、お客さまの従業員、そのご家族等の行為もしくは加担によって生じた不正払戻しの場合
- 他人に強要されたインターネットバンキングの不正使用による損害である場合
- 戦争、地震等により著しい秩序の混乱時の不正利用による損害である場合
- その他当金庫が注意喚起しているにも関わらず、注意義務違反があると認められる場合

(別紙2)

当金庫の推奨するセキュリティ対策

1. セキュリティ対策ソフトは最新版で利用してください。

コンピューターウイルス感染防止のためにウイルス対策ソフトの導入やフィッシングによる被害防止のためフィッシング対策ソフトを利用してください。

また、常に最新の状態に更新し、定期的にウイルスチェックと駆除を行ってください。当庫ホームページよりウイルス対策ソフト(Rapport(ラポート))を無料でインストールいただけます。

2. 電子証明書を利用してください。

現在、準備中(1月上旬予定)ですが、電子証明書をパソコンに保存することにより、利用パソコンを特定し他のパソコンからのログオンを抑止することができます。

無料で利用いただけますのでお申込みください。

なお、詳細については準備ができ次第案内いたします。

3. 当日振込指定の資金移動取引停止について。

現在、準備中(1月上旬予定)ですが、不正に預金を引き出す被害を防止するため、法人インターネットバンキングを利用した当日指定の資金移動(振込、振替)の取扱いを中止することといたします。

当日振込みを希望されるお客さまは、「事前登録方式」により可能となりますが、届出書の提出が必要となりますので、お取引店へお申ください。

なお、詳細については準備ができ次第案内いたします。

※「事前登録方式」とは

お客さまからお申込みいただくことにより、振込先の口座情報を当金庫にて登録する方式です。「事前登録方式」により登録された振込先については、当日指定の資金移動のお取引が可能となります。(「事前登録方式」により登録された口座については、お客さまで変更・削除をすることはできません)

※「事前登録方式」と「都度指定方式(現在の方式)」の違い

		事前登録方式	都度指定方式(現在の方式)
振込先の登録方法		当金庫へお申込	インターネットバンキング画面上でお客さまが登録
振込指定日	当日指定	○(通常通り)	×(取り扱いできません)
	翌日以降の指定	○(通常通り)	○(通常通り)

4. OS、ブラウザの管理を徹底してください。

貴社で使用しているパソコンのOS等のソフトウェアやブラウザを常に最新の状態に更新してください。

5. パスワードは定期的に更新してください。

インターネット暗証番号や利用者暗証番号等のパスワードを定期的(随時)に更新してください。

6. 事務担当者(利用者)と管理者(承認者)で別々のパソコンを利用してください。

フィッシング等を防止するため、事務担当者と管理者で同一のパソコンを使用しないでください。また、権限認証機能を利用いただき、振込等の資金移動業務における登録者と送信者を分けて使用してください。

※フィッシングとは

実際の金融機関やクレジット会社等を装った電子メールを送付し、これらのホームページと類似の偽サイトに誘導して、重要情報を詐取するもの。

7. 振込限度額は必要最低限に設定してください。

万一被害にあった場合の被害額を最小限に抑えるために、再度見直しを行い、振込限度額を必要最低限に引き下げてください。

8. 操作履歴をこまめにチェックしてください。

管理者は、当日の業務を開始する際や退社される前に、必ずインターネットバンキングにログオンし、入出金明細表等により適切な操作であるか操作履歴の確認を行ってください。

9. 不審なメールに注意してください。

心あたりのない電子メール、不審な電子メールに記載されているインターネットのアドレス(URL)をクリックすることや添付ファイルを開封することはウイルス感染やフィッシングの危険がありますので、絶対に行わないでください。

10. パソコンの利用目的を限定してください。

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使用してください。

11. インターネットバンキングを利用しない時や接続の必要がないときの留意点。

インターネットバンキングを利用しない時や、インターネット接続の必要がない場合は、使用のパソコンをネットワークから遮断したり、無線LANを切断するなど、パソコンをインターネット環境から隔離し、常時接続はしないようにしてください。

以上