

平成 28 年 4 月 18 日

お客さま各位

株式会社 名古屋銀行

法人インターネットバンキング不正送金等被害補償について

1. 対象となるサービスとお客さま

名古屋ビジネスダイレクトをご契約の法人のお客さま

2. 補償の概要

法人インターネットバンキングをご利用中のお客さまが第三者により盗取された番号(ID・パスワード)等を用いて行われた不正な振込等により生じた被害の補償を検討いたします。

3. 補償の上限額

1,000 万円とします。

4. 補償開始日

平成 27 年 1 月 3 日(土)より

5. 補償の対象とならない場合

- (1) 不正送金が発生した翌日から 30 日以内に当行および警察への届出がなかった場合
- (2) 不正送金が発生した場合における銀行による調査及び警察による捜査への協力がなかった場合
- (3) 不正送金が第三者との共謀またはお客さまの故意または「重大な過失」により行われた場合
- (4) 会社関係者の犯行であることが判明した場合
- (5) お客さまが、被害状況についての当行または警察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
- (6) 番号(ID・パスワード)等の盗用等が、天変地異、戦争、暴動等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行われた場合
- (7) ワンタイムパスワード(ハードウェアトークン並びにソフトウェアトークン)をご利用のお客さまにおいて、ワンタイムパスワード(ハードウェアトークン並びにソフトウェアトークン)を当行所定の方法でご利用いただいていない場合。
- (8) ワンタイムパスワード(ハードウェアトークン並びにソフトウェアトークン)を他人に貸与または譲渡していた場合。
- (9) ワンタイムパスワード(ハードウェアトークン並びにソフトウェアトークン)を紛失した際、直ちに当行へのお届け出がなされなかった場合。

「重大な過失」となりうる場合

- ① ウイルス対策ソフト等セキュリティ対策を実施しなかった場合
- ② 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場合
- ③ インターネットバンキングに使用するパソコンにおいて、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とせず長期間放置されていた場合
- ④ 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(OS)やウェブブラウザ等を使用していた場合

- ⑤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。
- ⑥銀行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
- ⑦お客さまが日本国外にお住まい、または日本国外で利用している場合
- ⑧その他、上記と同程度の著しい注意義務違反が認められた場合

6. 補償の減額となりうる場合

- (1) パソコンに関し、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なかった場合
- (2) ウイルス対策ソフトを導入しているが、最新の状態に更新したうえで稼働していない場合
- (3) 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
- (4) インターネットバンキングの申請者と承認者と異なるパソコンを利用していなかった場合
- (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なかった場合
- (6) その他、上記と同程度の注意義務違反が認められた場合

以上の状況を判定することについては、お客さまの申告、または当行の調査（調査会社による調査を含みます）により、当行が検討・判定した結果に基づきます。

不正送金にあわれた場合

万が一、不正送金被害にあわれた場合は、直ちにお取引店までご連絡をお願いします。