

# インターネット・バンキング不正送金対策のお願い

平成 29 年 11 月吉日

平素より東日本銀行をご利用いただき誠にありがとうございます。

平成 29 年 9 月 7 日付警察庁公表資料(※)によりますと、平成 29 年上期のインターネット・バンキングに係る不正送金事犯による被害の発生件数・被害額は 214 件・5 億 6,400 万円と平成 28 年上期比で被害件数は 645 件、被害金額は 3 億 3,300 万円下回ったとされております。

当行ではインターネット・バンキングに関しまして、従来からホームページ等でセキュリティについてご案内しておりますが、今一度以下のセキュリティ対策を行っていただきますようお願い申し上げます。

(※)警察庁ウェブサイト

([http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29\\_kami\\_cyber\\_jousei.pdf](http://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf))

## 1. お客さまに必ず行っていただきたいセキュリティ対策

### (1) サポートのある「OS」・「ブラウザ」の最新の状態で利用

当行ホームページ上に「動作確認状況」を提示しておりますが、その中に記載のある「対象 OS」ごとの「対象ブラウザ」を常に最新の状態を維持したうえでご利用ください。

法人のお客さまの動作環境

[http://www.higashi-nipponbank.co.jp/juridical/pdf/ib\\_kankyo.pdf](http://www.higashi-nipponbank.co.jp/juridical/pdf/ib_kankyo.pdf)

個人のお客さまの動作環境

[http://www.higashi-nipponbank.co.jp/direct/direct\\_kankyo.pdf](http://www.higashi-nipponbank.co.jp/direct/direct_kankyo.pdf)

### (2) ウィルス対策ソフトおよびセキュリティ対策ソフト等の導入および最新の状態で利用

市販されておりますウィルス対策ソフトおよび当行が提供しておりますセキュリティ対策ソフト「Phish Wall(フィッシュウォール)プレミアム」を必ず導入し、最新の状態を維持したうえでご利用ください。

### (3) ID・パスワード等の適切な管理

ID・パスワード等はお客さまがご本人であることを確認するための重要な情報です。以下の点にご留意いただき、お客さま以外の第三者に知られることのないよう慎重に管理してください。

- ① ID・パスワード等を、パソコン、スマートフォンやクラウドサービス等にファイルや画像(写真)などで入力・保存しない。
- ② パスワード等は定期的に変更するとともに、第三者から類推されやすいものに設定しない。
- ③ ID・パスワード等の入力を求めるメールを当行が送ることはありません。そのようなメールを受信しても無視してください。
- ④ ダイレクトバンキングサービスご利用時に、ダイレクトバンキングカードの利用者番号(カード裏面記載の 1 桁目～12 桁目までの番号)全ての入力を当行が求めることはありません。そのようなウイ

ンドウが出たら、直ちに操作を中断し、すみやかに当行に通知してください。

なお、ID・パスワード等が偽造・盗難・紛失等により、他人に使用されるおそれが生じた場合または他人に使用されたことを認知した場合にはすみやかに当行に通知してください。

(4) 電子証明書(クライアント証明書)の利用について(法人のお客さまのみ)

銀行が指定した正規の手順以外での電子証明書の利用は止めてください。

(5) 電子メールアドレスの設定について

振込依頼および振替依頼の受付結果、その他告知等(法人・個人のお客さま共通)、メール通知パスワード(個人のお客さま(任意))のメールを受信するメールアドレスの設定を、東日本ビジネス IB サービス、東日本ダイレクトバンキングサービスご利用 PC ではご覧になれない別端末(携帯電話やスマートフォン等のアドレス)に設定してください。

(6) 当行が導入しているセキュリティ対策の実施および新たな対策を講じた場合の同対策の導入

当行が導入しているセキュリティ対策を必ず実施していただくとともに、今後も当行はセキュリティ対策の向上に努めてまいりますので、新たな対策を講じた場合には必ず利用してください。

法人のお客さま向けのセキュリティ対策の詳細

<http://www.higashi-nipponbank.co.jp/juridical/ib.html>

個人のお客さま向けのセキュリティ対策の詳細

<http://www.higashi-nipponbank.co.jp/direct/>

## 2. お客さまに推奨するセキュリティ対策

- ・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
- ・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
- ・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。**特に個人のお客さまにおかれましては限度額を 20 万円以下に設定していただくことを推奨いたします。**
- ・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
- ・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(法人のお客さまのみ)
- ・インターネットカフェやホテルなど複数の人が利用する共用のパソコンを使用したり、公衆 Wi-Fi を使用して、インターネット・バンキングを利用することは極力避けること

## 3. 不審な事象が発生した場合

以下のような不審な事象が発生した場合、直ちにインターネット・バンキングの停止をご連絡ください。

- ・パソコン内の電子証明書が消失する
- ・知らないうちにパスワードがロックされている
- ・(通常とは違う)シャットダウンやフリーズが意図しないで起こる

以上