インターネットバンキングのセキュリティについて

サービスを安全にご利用になるために、以下の点をいま一度ご確認ください。

- ウイルス対策ソフトを必ず導入し、ウイルスを検知・駆除した状態で東日本ビジネス IB サービスをご利用ください。また、ウイルス対策ソフト、ウイルス定義ファイルは、常に最新の状態に更新するとともに、定期的にウイルススキャンをおこなってください。
- 東日本銀行では、不正送金・フィッシング対策ソフト『PhishWall プレミアム』を提供しています。市販のウイルス対策ソフトとあわせて、必ずご利用ください。
- 基本ソフト（OS）やブラウザ等、インストールされている各種ソフトウェアは、常に最新の状態に更新してください。
- 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は使用しないでください。
- パスワード等を記載したワード・エクセル等のファイルをパソコン内に保存しないでください。
- 不審であったり信頼性が不明なサイトの閲覧、不審なメールは開封しないよう、利用者さま全員に徹底してください。
- パソコンの外部からの不正操作を防止するため、東日本ビジネス IB サービスを利用しない時や、インターネット接続の必要がない時は、ご利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、常時接続は避けてください。
- パソコンを利用しない場合は、パソコンの電源を落とすよう徹底をお願いします。
- パスワードは定期的に変更してください。
- 承認機能をご利用ください。また、作成者と承認者では異なるパソコンをご利用ください。

- 1 取引あたりの限度額は適切な金額に設定してください。また、1 日あたりの限度額についても、日頃の取引金額をご確認のうえ、適切な金額の設定をお願いします。
- トランザクション認証用トークンを第三者に渡さないでください。
- ID･パスワード等を第三者に教えないでください。銀行員・警察官などがお客さまに ID･パスワードをお尋ねすることはありません。
- パスワードは、第三者の目に容易に触れるところや運転免許証・通帳・キャッシュカード・ご契約カードなど、類推される恐れのある物には絶対に書き留めないでください。
- パスワードをパソコンやスマートフォンから入力される場合、第三者から見えないようにしてください。
- パスワードを第三者に知られてしまった、もしくは知られてしまったと思われる時は、直ちにお客さま自身でパスワードの変更手続きをおこなってください。
- お客さまご自身が所有、管理する端末以外からやむを得ず操作された場合は、事後速やかにパスワードを変更してください。
- 他のサイトで利用しているパスワードは使用しないことをお勧めします。
- 他人に推測されやすいパスワード（生年月日・電話番号・住所）は使用しないでください。
- インターネット・バンキングを利用するパソコンは、過去の入力履歴を用いて、入力しようとする内容を予め表示するキーボード入力補助（オートコンプリート）機能は解除して使用してください。
- 不特定多数の方が使用するパソコンでのご利用は避けてください。
- インターネット・バンキングにログインした際に不審な入力画面等が表示された場合、IDやパスワード等の情報は入力せず、速やかに銀行にご連絡ください。
- パスワード（暗証番号）をキャッシュカードの暗証番号等他のサービスの暗証番号として使うこと、あるいは、ロッカー、貴重品ボックス、携帯電話　等の金融機関との取引以外で使うことは避けてください。
- 「ログイン ID」「ログインパスワード」「確認用パスワード」「承認パスワード」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。これらは第三者に知られることのないように、また、お忘れにならないようにご注意ください。パスワードは定期的に変更していただくことにより安全性が高まります。
- 東日本ビジネス IB サービスでは、お客さまのパソコンと当行のコンピュータ間のデータ通信について、本サービスを安心してご利用いただけるよう最新式の暗号化技術の 256 ビット SSL 暗号化方式を利用し、情報の盗聴・書き換え等を防止しています。

- パソコンのキーボード情報を盗み第三者に送信するスパイウェアに対するセキュリティ対策として、画面上で開いたソフトウェアキーボード画面の文字ボタンをマウスでクリックし、パスワードを入力するソフトウェアキーボードを導入しています。
- 外部からのインターネットを通じた不正利用を抑止するため、ご利用時のユーザーおよびパソコンとホストコンピュータを認証する証明書（電子証明書）を導入しています。なお、OS・ブラウザの環境によっては証明書のご利用がいただけない場合がございます。
- トランザクション認証は、相手先の口座番号や振込金額等の情報を元に生成された二次元コードを専用のトークンで読み取ることで生成されるパスワード（トランザクション認証番号）により認証を行うことで第三者の不正利用を防止する機能です。

法人のお客様は以下の対策をおこなうと、万一、不正な振り込みがあっても早期発見につながります。

- 東日本ビジネス IB サービスの操作履歴により、不自然な動きがないか常に確認してください。
- 帰社時やパソコンの切電時には、身に覚えのない取引・予約取引がないことを必ずご確認ください。
- 遠隔操作により E メールアドレス自体が削除されると思われる事例も報告されています。東日本ビジネス IB サービスに登録する E メールアドレスは携帯電話メールアドレスなど、東日本ビジネス IB サービスを利用するパソコンとは完全に隔離された E メールアドレスを登録することも効果的です。なお、E メールアドレスの登録にあたっては、フリーメールを中心とした、ブラウザで閲覧するタイプの E メールアドレスはお勧めしません。