

「ほくぎんダイレクトA」を安全にご利用いただくために

最近、インターネットバンキングでお客さまの預金口座に不正にアクセスし、犯人の口座へ送金するという犯罪が相次いで発生しています。

手口としては、お客さまのパソコンをコンピュータ・ウィルスに感染させ、お客さまのご預金を引き出し送金するというものが多くなっております。

また、銀行に成りすまして不審なメールを送信し、お客さまのログインIDやパスワード情報を盗み取る手口（いわゆるフィッシング詐欺）も報道されています。

本紙では、そのような犯罪に対するほくぎんダイレクトAのセキュリティ対策や、お客さまご自身に対策していただきたい事項について記載しておりますので、本紙をご参考にほくぎんダイレクトAを安全にご利用ください。

ほくぎんダイレクトAのセキュリティ

1. 「ワンタイムパスワード」のご利用

ワンタイムパスワードは一度だけ有効な使い捨てのパスワードです。1分ごとにパスワードが更新されるため、パスワードを盗まれたり、推測されたりすることがありません。（スマートフォンまたは携帯電話にアプリをダウンロードして利用するソフトウェアトークン方式と、専用装置によるハードウェアトークン方式があります。）

2. ソフトウェアキーボードによるパスワード入力

画面上に表示されるキーボードの文字をクリックすることで文字入力を可能にします。これはキーボードの操作履歴を盗み取るタイプのスパイウェアに有効です。

3. そのほか、下記のセキュリティ対策を行っております。各セキュリティ対策の詳細については、北陸銀行ホームページでご確認ください。

・リスクベース認証

第三者のなりすましによる不正アクセスを防止するために、通常と異なるご利用環境と判断した場合、合言葉（質問と回答）による追加認証を行います。

・EV SSL証明書

フィッシング詐欺への対策として、日本ベリサイン株式会社のEV SSL証明書を採用しています。

・IBロック

モバイルバンキング（携帯電話からの利用）で、インターネットバンキング（パソコンやスマートフォンからの利用）によるほくぎんダイレクトAの利用可否を設定することができます。

・ログインID、パスワード等の管理について

お取引に応じて複数のパスワードを確認する本人認証システムを採用しています。

・256bitSSL暗号化方式

インターネット回線上で情報が盗まれないための暗号方式のうち、より解読が困難な方式を採用しています。

・利用端末変更

ほくぎんダイレクトAを利用できる端末を任意のタイミングで変更できます。

・お取引等のご案内メール

ご登録のEメールアドレスにお取引結果の通知を送信します。

・緊急利用停止

パスワード等が盗まれたときにお客さまご自身でご利用を停止できます。

お客さまにお願いしたいセキュリティ対策

1. 「ウイルス対策ソフト」を使用

インターネットに接続するパソコンにはウイルス対策ソフトを導入してください。

- (1) ウィルスパターンは最新の状態に更新してください。
- (2) 定期的にコンピュータのウィルスチェックを行ってください。

2. 「パスワード」の管理

- (1) ログインパスワード、確認パスワードは定期的に変更してください。
- (2) ログインID、パスワードをワード・エクセル等のファイルに記載してパソコン内に保存することは絶対にお止めください。

3. 「フィッシング詐欺」に注意

- (1) 心当たりのない不審な電子メールをお受け取りになった場合は、電子メール内にあるホームページにアクセスし、パスワード等の個人情報を入力したり、電子メールにて回答なさらないようご注意ください。(当行から電子メールでパスワード等の情報をお聞きすることは一切ございません)
- (2) インターネットバンキングにアクセスするURL「<http://www.hokugin.co.jp/>」をブラウザの「お気に入り」「ブックマーク」に追加することをお勧めします。

4. 「疑わしい取引」に注意

- (1) インターネットカフェのパソコン等の不特定の人が利用するパソコンでは、インターネットバンキングのご利用はお控えください。
- (2) 不審なWebサイトにアクセスしないでください。

5. その他の注意

- (1) インターネットバンキングをご利用されているパソコンでのファイル交換ソフト(「Winny」「WinMX」「LimeWire」等)のご利用はお控えください。
- (2) 不審なCD-ROM等が当行名等で送付された場合には、パソコンには挿入せず当行までご連絡ください。(インターネットバンキングをご利用のお客さまに当行がCD-ROMをお送りすることはございません)
- (3) 無線LANをご利用される場合は、利用機器の制限、暗号化機能を利用するなどセキュリティ設定には十分注意してください。
- (4) フリーソフトをみだりにダウンロード・インストールしないでください。
- (5) お取引内容を都度ご確認ください。
 - ◎ 前回ログイン履歴、取引確認メールを都度チェックしてください。
 - ◎ 電子メールアドレスについては、常に最新の正しいものをご登録ください。2つまで登録可能です。2つ目の電子メールアドレスの登録は、メニュー画面の「各種手続き」－「お客さま登録内容確認・変更」－「お客さま情報」－「セレクトEメールサービス」よりご登録ください。

以上

広 (800) 1527 平成30年7月現在