セキュリティについて

〈ひろぎん〉ダイレクトバンキングサービスでは、本サービスを安心してご利用いただけるよう、インターネット上での情報の盗聴、データの偽造や改ざん、第三者の不正使用などを防ぐため、以下の対策を実施しています。

■厳重な本人確認

●申込書により、ご契約いただいた印鑑を照合しています。また、オンライン申込の場合は、キャッシュカードの暗証番号等により申込者ご本人であることを確認しています。

●サービス利用の際には、ダイレクトバンキング暗証番号等により契約者ご本人であることを確認しています。

●ダイレクトバンキング暗証番号等を複数回誤って入力された場合、サービスのご利用を停止いたします。

※利用停止の解除は、当行所定の方法により届出が必要です。

●お客さまが普段とは異なる環境よりインターネットバンキングをご利用されているとシステム的に判断した場合には、あらかじめご登録いただいた合言葉を使用し申込者ご本人であることを確認しています。

■ご利用履歴の表示

直近3回分までのログイン日時をインターネットバンキングホーム画面に表示しますので、ログイン履歴をご確認いただけます。

※お客さま以外の第三者の利用を防ぐため、ログイン中はパソコンから離れないでください。

■ソフトウェアキーボード

キーロガー（キーボードでの入力情報を盗みとる）対策として、お取引確認番号やダイレクトバンキング暗証番号を入力する際には、画面上に表示された擬似キーボード（ソフトウェアキーボード）をマウスでクリックすることで安全にご入力いただけます。

■自動ログアウト

ログインしたまま一定の時間内に操作がない場合、自動的にログアウトし、お取引を終了いたします。

■ご確認電子メールの送信

インターネットバンキングでは、振込・振替のお取引、パスワード等の登録情報を変更される都度、電子署名付の電子メールにてご連絡いたします。なお、当行から電子メール等でパスワード等をお客さまにおたずねすることは一切ありません。

※心当たりのないメールが届いた場合は、すぐに、当行までご連絡ください。

広島銀行から送信する電子メールアドレスの発信元は以下のとおりです。

ibmail@ib.hirogin.co.jp（取引結果通知メール、入出金通知メール等）
ibmail.hirogin@otp-auth.net（ワンタイムパスワード生成アプリ利用案内メール）
dbguide@po.hirogin.co.jp（商品・サービスお知らせメール）
ibmail@po.hirogin.co.jp（商品・サービスお知らせメール）

受信制限等の設定をされる場合は、上記アドレス（またはドメイン）を指定受信していただきますようお願いします。

■お客さま情報の暗号化

お客さまのパソコンと当行のサーバー間におけるデータの送受信において現在最もセキュリティレベルが高いといわれている暗号化方式「128ビットSSL（Secure Socket Layer）」を採用し、お客さまの情報を保護しています。
この128ビットSSLによって暗号化された情報は2の128乗通りの符合を組み合わせてできており、現時点では解読はほぼ不可能とされています。

■システム監視体制

インターネットから銀行のコンピュータへの不正なアクセスを防止するため、ファイアーウォールを設けています。