

インターネットバンキングの セキュリティについて

琉球銀行の取組み



1 セキュリティ環境

- ① 128bit SSL暗号化方式を採用
 - 現時点で最も解読困難とされる暗号化方式で、情報漏えい・改ざんを防止します。
- ② 自動ログオフ機能
 - 不正使用を防ぐため、一定時間利用がない場合自動的にログオフされます。
- ③ 前回ご利用日時の表示
 - インターネットバンキングの画面上で、不審な使用がないか確認できます。

2 フィッシング対策

- ① 各種パスワードでお客さまを特定
 - ログオンパスワードほか数種類のパスワードでお客さまを厳密に特定いたします。
- ② 一部パスワードに「可変方式」を採用
 - ログオン時(法人)、重要取引時(個人)には都度変更される2桁の「確認パスワード」を使用します。
- ③ ソフトウェアキーボードの採用
 - ソフトウェアキーボードの利用により、操作履歴がパソコンに残りません。
- ④ EV SSLサーバー証明書の導入
 - 当行インターネットバンキングのサイトは認証局の証明書を取得しています。
- ⑤ ウィルス対策ソフト「Rapport(ラポート)」の無償提供*
 - 不正なウィルスから大切な資金をお守りいたします。
- ⑥ ワンタイムパスワードの導入*
 - 60秒毎に変わる使い捨てパスワードの利用で、セキュリティが格段に向上します。
※ソフトやアプリのインストールなど、お客さま側の対応が必要となります。

3 被害発生防止対策

- ① 「1日あたりの振込・払込限度額」の設定
 - お客様ご自身で、適正な「1日あたりの限度額」を設定いただけます。
- ② 電子メールの送信
 - 重要な取引を行った場合、当行から電子メールで内容を知りたくします。

4 万一の際の補償

- ① 万一不正送金被害が発生した場合の補償を用意しています。
 - ※補償内容は各々の事例やお客様のセキュリティ対策内容に応じて算定されます。
 - ※セキュリティ対策については当行の「セキュリティガイド」をご参照ください。

セキュリティガイドは右記二次元コードより、りゅうぎんホームページからご確認ください▲
<https://www.ryugin.co.jp/others/pamphlet/>



インターネットバンキング のセキュリティ対策

お客様に
お願い
したいこと

-  ☐ パソコンをご利用の方は、ウィルス対策ソフト「Rapport（ラポート）」を導入してください。
- ☐ ワンタイムパスワードをご利用ください。
- ☐ パスワードは推測されにくい文字や数字を組み合わせをご利用ください。
- ☐ パスワードやID等は、パソコンやスマートフォン内、またはクラウドなどに絶対に保存しないでください。
また、電子メールでの送受信、メール下書き等への保存も行わないでください。
- ☐ OSやソフトなどは常に最新の状態にしてください。
- ☐ 銀行職員や警察官、役所職員等がお客様のパスワード等を訊ねることは決してありません。
万一不信な電話等を受けた場合は、お取引店または下記お問い合わせ先へご連絡ください。
- ☐ メールアドレスは、携帯電話・スマートフォンなど通知後すぐに確認できるアドレスをご登録ください。
- ☐ 振込・払込限度額は必要な範囲内に設定してください。
- ☐ 不審なログインや送金がないか、定期的にご確認ください。
- ☐ 使用しないときはパソコンの電源を切ってください。
- ☐ 偽画面と思われる画面が現れた場合、あるいはウィルスに感染したと思われる場合は、すぐに利用を中止し、お取引店または下記当行お問い合わせ先まで連絡願います。

お問い合わせ先

りゅうぎんEBセンター

通話料
無料

0800-300-3927

受付時間/平日9:00~24:00、土・日・祝日8:00~24:00

