琉球銀行

りゅうぎんインターネットバンキング

セキュリティガイド

個人・法人のお客さま共通

インターネットバンキングの
ご利用を開始する前に必ずご覧ください

第5版
2022年8月現在

Internet Banking

はじめに

〈琉球銀行インターネットバンキング〉をお申込みいただき誠にありがとうございます。

便利なインターネットバンキングをより安全にご利用いただくために、セキュリティ対策についてご案内いたします。

当行がご案内するセキュリティ対策ツールはすべて無料です。ご利用開始前にお使いのパソコンやスマートフォンへの導入をお願いします。

目次

お問い合わせ先については37ページをご覧ください

セキュリティ対策レベルチェック

あなたは大丈夫？ 大切な預金を守るための環境をチェック。

対策の前に、まずはセルフチェック！
当てはまる項目にチェックしてください。

- ☐ インターネットバンキングを使うパソコン・スマートフォンに**セキュリティソフト（またはセキュリティブラウザやアプリ等）を導入**している
- ☐ **ログオンパスワードを定期的に変更**している
- ☐ インターネットバンキングに**メールアドレスを登録**し、**お取引確認メールの受信・確認**をしている。
- ☐ インターネットバンキングを使うパソコン・スマートフォンの基本ソフト（OS）やソフトウェアは**最新のバージョン**にアップデートしている
- ☐ 振込限度額を**必要な範囲内**で設定している

いくつ当てはまりましたか？

チェックが少ないほど、セキュリティレベルが低く
大切なあなたの預金が狙われる可能性が高くなってしまいます。

インターネットバンキングを狙う詐欺の手口

フィッシング詐欺 …… **金融機関を装った偽のメールやショートメール（SMS）等**を利用者に送り、実在するインターネットバンキングのログオンページを装う**偽サイトに誘導**する。
誘導した画面でIDやパスワードを盗み取る。

ウィルス感染 …… 金融機関の**正規のサイトにそっくりの画面**や、**偽のポップアップ画面**を表示させて、パスワード（乱数表）や合い言葉などを盗み取る。

上記の手口は一例です。まるで金融機関から送られてきたような偽のメールや、本物そっくりの偽画面など、よく確認しないと騙される可能性が高くて危険です。
このようなメールや画面に騙されないように、セキュリティを強化して大切な預金を守りましょう。

セキュリティ対策ツールを導入し、
ご利用環境のセキュリティを強化しましょう！
対策方法は次のページへ

あなたがインターネットバンキングを利用するのは パソコン？スマートフォン？必要なセキュリティツールを確認しましょう。

パソコンをご利用の方

Personal computer

ウィルス対策ソフト
Rapport〈ラポート〉

インターネットバンキングに特化したセキュリティ対策ソフトで、インストールしていただくとインターネットバンキング取引時の安全性が格段に向上します。インストールするだけで機能し、ウィルスを検知すると自動的にウィルスの停止・駆除を行います。

- 簡単インストールでウィルスを検知&停止・駆除
- 市販のウィルス対策ソフトと併用OK※

※一部のウィルス対策ソフトとは併用できない場合があります。

スマートフォンをご利用の方

Smartphone

セキュリティブラウザアプリ
Trusteer Mobile〈トラスティーア・モバイル〉

Trusteer Mobileアプリを使用してインターネットバンキングにアクセスすることで、偽のWebサイトではなく、正規のインターネットバンキングのサイトに確実にアクセスできます。ブラウザ内はウィルスが侵入することができないので、不正取引を防ぐために有効です。

- 専用ブラウザでウェブサイトの検証
- 外部からの攻撃を防ぐ

＋

ワンタイムパスワード

従来のパスワードは、好きな英数字を指定して設定できますが、パスワードを推測されやすいため、セキュリティを保つためにはこまめにパスワードを変更する必要があります。

ワンタイムパスワードは、60秒ごとに専用のアプリ※で自動的に発行される使い捨てのパスワードです。1回限りの使い捨てパスワードのため、万一誰かに盗み見られても悪用される心配がありません。

※アプリのダウンロードは、スマートフォンか携帯電話のみ可能です。

※画面はイメージです。

＋

Rapport（ラポート）、Trusteer Mobile（トラスティーア・モバイル）、ワンタイムパスワードのご利用手数料は 無料

フィッシング詐欺やウィルス感染を防ぐのに 有効

Rapport
インストール方法 … P4へ

Trusteer Mobile
インストール方法 … P8へ

ワンタイムパスワード
お申込み方法 … P14へ

さっそくインストールしましょう ▶

セキュリティ対策ソフト「Rapport（ラポート）」インストール方法

パソコン専用

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

りゅうぎんインターネットバンキングに ログオンしていない場合

1

琉球銀行ホームページ上部にある「**インターネットバンキング〈会員登録はこちら〉**」を選択。

「セキュリティ対策ツール」の「**パソコンをご利用の方はこちら**」を選択。

2

「個人のお客さま ダウンロード」または「法人・個人事業主のお客さま ダウンロード」を選択。

りゅうぎんインターネットバンキングに ログオンしている場合

1

【個人のお客さま】
インターネットバンキング：画面右側

【法人のお客さま】
Biz ネット：画面左側メニュー内

当行インターネットバンキングトップ画面右側（法人は左側）の、「**Rapport（ラポート）ウィルス対策ソフト**」を選択。

2

「**ラポートダウンロードはこちら**」を選択。

Rapport（ラポート） ダウンロードページへ ▸

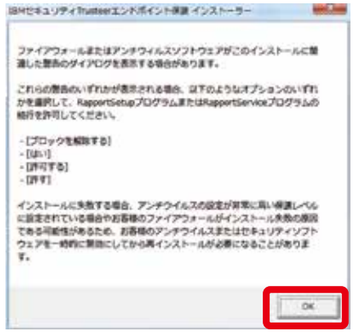
3

「**Rapport のダウンロード**」を選択。

4

「**保存**」または「**名前を付けて保存**」を選択した後、「**実行**」を選択。
※エラーが出る場合は、パソコンのデスクトップ等に保存して実行してください。（デスクトップ等に Trusteer の緑のアイコンのファイルが現れます。）
※ユーザーアカウント制御が表示される場合は「**はい**」を選択してください。

5



内容を確認後、「**OK**」を選択。

ダウンロードが開始されますので、完了するまでお待ちください。（約 5 分〜20 分程度）
※セキュリティ警告が表示される場合は「**実行する**」を選択してください。

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

6

ダウンロード終了後、ソフトウェア使用許諾契約の内容をご確認のうえ「**使用許諾契約の条項に同意します**」にチェックをいれて「**インストール**」を選択。
インストールが始まりますのでしばらくお待ちください。

インストール中…

7

インストール完了後、「**完了**」を選択。

Rapport でウェブサイトの検証

① 右下のタスクバー

② アドレスバーの横

①右下のタスクバー
②アドレスバーの横
に**緑のアイコン**が表示されていたら、Rapport（ラポート） が導入されています。
（琉球銀行以外のページでは②のアイコンがグレーになることがありますが、琉球銀行ホームページへアクセス時に緑色になっていたら、安心してインターネットバンキングをご利用いただけます。）

このマークが表示されていたら
ラポートが導入されています。

正規のページではアイコンが緑で表示されます。
Rapport にて保護されていないページにアクセスするとグレーになります。

その他ご留意事項

・「Rapport」は IBM 社が提供するソフトウェアであり、当行が提供するものではありません。
・本ソフトウェアの利用にあたっては、IBM 社が定める使用許諾契約に同意する必要があります。
・本ソフトウェアが提供するサービスは、IBM 社により予告なく変更または廃止される場合があります。
・本ソフトウェアを利用しても、ウィルスによる被害を受ける可能性が完全になくなるわけではありません。
・本ソフトウェアを利用した結果、お客さまが何らかの被害を受けた場合でも、当行は責任を負いかねます。

スマートフォンでもご利用の方は
こちらもインストールしましょう

Rapportの導入が済んだら
ワンタイムパスワードの利用手続きへ！

Rapport
インストール方法 … P4へ

Trusteer Mobile
インストール方法 … P8へ

ワンタイムパスワード
お申込み方法 … P14へ

セキュリティブラウザ「Trusteer Mobile（トラスティーア・モバイル）」インストール方法

スマートフォン専用

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

1

琉球銀行スマートフォン用サイトより、「**インターネットバンキング**」→「**インターネットバンキング（ログオンページへ）**」を選択し、ログオンページを表示する。

2

お客さまご自身の「**ご契約番号**」「**ログオンパスワード**」を入力し、ログオンボタンを選択。

画面左上の「**メニュー**」を選択。

表示されたメニューの中にある「**ウイルス対策ソフト trusteer mobile**」を選択。

3

「Trusteer Mobileのインストールはこちら」を選択。

Android OSの方（Google Play）とiOSの方（iTunes Store）ではリンクボタンが異なりますのでご注意ください。

Android OSをご利用の方

「Play ストア」を選択。

「インストール」を選択。

「同意する」を選択。

iOS（iPhone）をご利用の方

「入手」を選択。

「インストール」を選択。

「**パスワード**」にお客さま自身の Apple ID のパスワードを入力し「**OK**」を選択。

セキュリティブラウザ「Trusteer Mobile（トラスティーア・モバイル）」インストール方法

スマートフォン専用

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

Android OSをご利用の方

7

「開く」が表示されたらインストールは完了。
引き続き「設定」を行うため「開く」を選択。

8

ソフトウェア使用許諾契約の内容をご確認のうえ、「同意する」を選択。

iOS（iPhone）をご利用の方

7

「開く」が表示されたらインストールは完了。
引き続き「設定」を行うため「開く」を選択。

8

ソフトウェア使用許諾契約の内容をご確認のうえ、「同意する」を選択。

9

画面右下の「メニューボタン」を選択。
※機種によってはメニューボタンを長押ししてください。

10

「サイトを追加」を選択。

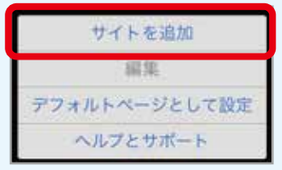
11

「サイトのリスト」より、
「琉球Internet Banking」を選択。
※「琉球銀行」を選ぶこともできます。その場合は、当行のスマートフォン用ホームページ（トップ）からのログオンになります。

9

「Trusteerのアイコン」を選択。

10



「サイトを追加」を選択。

11

「サイトのリスト」より、
「琉球Internet Banking」を選択。
※「琉球銀行」を選ぶこともできます。その場合は、当行のスマートフォン用ホームページ（トップ）からのログオンになります。

セキュリティブラウザ「Trusteer Mobile（トラスティーア・モバイル）」インストール方法

スマートフォン専用

12

「琉球 Internet Banking」のアイコンが追加されたら設定完了。

「**デフォルトページとして設定**」にチェックを入れて、「**今すぐ移動**」を選択。

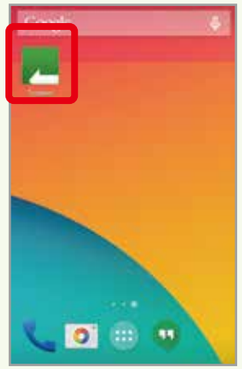
13

Trusteer のアイコンが緑色で表示されていることを確認し、ご利用ください。
（緑色で表示されているページは安心してご利用いただけます。）

セキュリティブラウザ「Trusteer Mobile（トラスティーア・モバイル）」ご利用方法

スマートフォン専用

1



【Android OS】画面イメージ

【iOS（iPhone）】画面イメージ

Trusteer

ホーム画面の「Trusteer」を選択し、アプリを起動する。

自動的にりゅうぎん（スマートフォン用）インターネットバンキングログオン画面へ移動。

2

画面上部に Trusteer の緑のマークが表示されていることを確認できたら、インターネットバンキングを安全にご利用いただけます。
（Trusteer によって保護されていないページの場合はマークが灰色で表示されます。）

※「Trusteer Mobile」をインストールしただけでは、セキュリティ対策にはなりません。アプリを起動してからログオンすることで、安全にご利用いただけます。

その他ご留意事項

- 「Trusteer Mobile」は IBM 社が提供するソフトウェアであり、当行が提供するものではありません。
- 本ソフトウェアの利用にあたっては、IBM 社が定める使用許諾契約に同意する必要があります。
- 本ソフトウェアが提供するサービスは、IBM 社により予告なく変更または廃止される場合があります。
- 本ソフトウェアを利用しても、ウィルスによる被害を受ける可能性が完全になくなるわけではありません。
- 本ソフトウェアを利用した結果、お客さまが何らかの被害を受けた場合でも、当行は責任を負いかねます。

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

りゅうぎんインターネットバンキング ワンタイムパスワード

ワンタイムパスワードは、スマートフォンまたは携帯電話に「ソフトウェアトークン（アプリ）」をインストールしてご利用いただくことで、端末（スマートフォンや携帯電話）にパスワードを発行する機能が追加されます。
個人のお客さまも、法人・個人事業主のお客さまもご利用可能です。ご利用いただくには右記 3 ステップのお手続きが必要です。本ガイドを参考にしながらステップ順にお申込み・設定を進めて、ご利用を開始してください。
通常のパスワードに「ワンタイムパスワード」をプラスすることで、セキュリティを強化しましょう。

お申込みの際に必要なもの

- ☑ ご自身のメールアドレス
（アプリをダウンロードして使用するスマートフォンまたは携帯電話のメールアドレス）
- ☑ 筆記用具
（次のページに書き込み用のメモ欄があります）
- ☑ インターネットバンキングご利用カード

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

Step1〈お申込み〉　スマートフォンまたはパソコン

1

事前準備

お申込みにはメールアドレスが必要です。
また、アプリの設定には、「利用開始パスワード」「サービス ID」「ユーザ ID」が必要になります。
下のメモ欄に必要情報のメモをとりながら、お申込み～設定を行うとスムーズです。

メールアドレス	
利用開始パスワード	※Step1-❹で入力した 6 桁の数字
サービス ID	※Step2-❶のメールに記載してある数字
ユーザ ID	※Step2-❶のメールに記載してある数字

2

※画面イメージは個人向けインターネットバンキングのものです。

インターネットバンキングに**ログオン**。

◆個人のお客さま
メニューの「各種変更・申込」を選択し、「**ワンタイムパスワードの申込み**」を選択。

◆法人（Biz ネット）のお客さま
左側メニューの「メンテナンス」を選択、「**ワンタイムパスワードの申込み**」を選択。

3

ご留意事項を確認し、「**上記事項を理解し了承しました。**」をチェックした後、「**確認**」ボタンを選択。

4

「ワンタイムパスワードアプリ」をダウンロードするスマートフォンまたは携帯電話の**メールアドレスを入力**。
※パソコンのメールアドレスは入力しないでください。
パソコンにはダウンロードできません。

利用開始パスワード（6桁）の数字を決めて入力。
※初期登録処理で1回のみ使用するパスワードです。忘れないように16ページのメモ欄に書き込んでおきましょう。
⇒利用開始パスワード

「**確認**」ボタンを選択。

5

「メールアドレス」、「利用開始パスワード」を確認し、問題なければ確認パスワードを入力。

◆個人のお客さま
「確認パスワード（2 桁）」を入力し、「実行」を選択。

◆法人（Biz ネット）のお客さま
「確認パスワード（7 桁）」を入力し、「実行」を選択。

6

※受信したメールはStep3が
完了するまで削除しないでください。

受付完了です。

入力したメールアドレス宛てにメールが届きます。ご確認のうえ Step2 へお進みください。（メールのドメインは「@otp-auth.net」です。）

Step2〈アプリのダウンロード〉　スマートフォンまたは携帯電話

1

1 Step1-6でスマートフォンまたは携帯電話で受信した「**ワンタイムパスワードのご案内**」の電子メールを開く。

2 （2）に記載されている「**サービスID**」と「**ユーザID**」をメモしておくと便利です。（⇒16ページ T2・T3）

3 （1）の「**ダウンロード用URL**」をタップし、ページの指示に従い「**ワンタイムパスワードアプリ**」を**インストール**してください。

※スマートフォンへアプリをインストールする手順については、9ページ〈「Trusteer Mobile」インストール方法〉と同じです。ご参照ください。
※携帯電話へのインストールについては、画面の指示に従って進めてください。

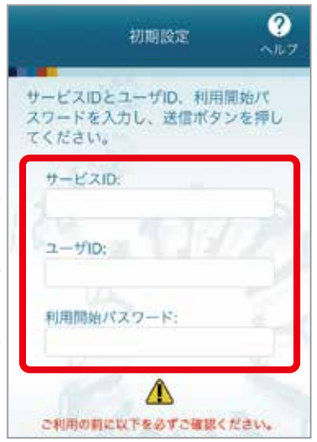
〈利用申込受付確認メール〉▶
※個人向けインターネットバンキングをご利用の方向けのメール（例）です。

Step3〈アプリの設定処理〉

1

アプリを起動

T2 T3 T1



初期設定　スマートフォンまたは携帯電話

アプリのインストールが完了すると、スマートフォンの画面に「ワンタイムパスワード」のアイコンが追加される。
アイコンを選択して**アプリを起動**。

「**サービスID**」、「**ユーザID**」、「**利用開始パスワード**」を入力。
※16ページのメモを参考に入力してください。

入力内容を確認のうえ、「**送信**」を選択。

※携帯電話をご利用の場合も同じ手順でお進みください。

2

初期設定が完了。
「**次へ**」を選択し、トークン表示名を確認後「**登録**」を選択。利用開始登録へお進みください。
※トークン表示名に任意の文言を追加されたい時は、「**変更後の追加文言**」に入力してください。

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

3

利用開始登録　スマートフォンまたはパソコン

1 「Copy」を選択し、ワンタイムパスワードをコピー。

2 琉球銀行のロゴをタップし、インターネットバンキングの画面に移動。

3 コピーしておいたワンタイムパスワードを貼り付け（ペースト）、「登録」を選択。

※パソコンから利用開始登録を行う場合は、①インターネットバンキングへログオン ②利用開始登録画面にワンタイムパスワードを入力し「登録」を選択していただくと設定が完了します。

4

ワンタイムパスワードの利用開始登録が完了しました。

次回のログオン時からは、ワンタイムパスワードを使用したログオン方式に変更されます。
※ワンタイムパスワードアプリを起動し、ワンタイムパスワードを入力しないとログオンできません。

利用開始登録が完了したら「**トークン利用開始登録完了**」のメールが、登録のメールアドレスに送付されますので、ご確認ください。

ワンタイムパスワードのご利用方法

ワンタイムパスワードは通常ログオンと併せてご利用いただきます。ログオン方法は３パターンありますので、右記の案内に沿ってご確認ください。

スマートフォンでログオンする場合
ワンタイムパスワードアプリからログオン P21
（トラスティーア・モバイル）Trusteer Mobileでログオン P22
パソコンでログオンする場合 P23

スマートフォンでログオンする場合〈ワンタイムパスワードアプリからログオン〉※個人のお客さまのみ

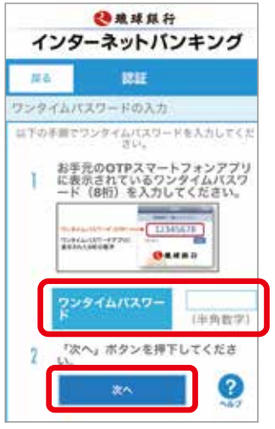
1

アプリを起動

ワンタイムパスワード**アプリを起動**。

「Copy」を選択してパスワードをコピー。
コピー後、**琉球銀行のロゴマーク**をタップして、インターネットバンキングのログオンページを表示。

2



「**ご契約者番号（10桁）**」と「**ログオンパスワード（6桁）**」を入力し、「**ログオン**」を選択。

ワンタイムパスワードの入力欄に、1でコピーしたパスワードを**貼り付け（ペースト）**して、「次へ」を選択。

トップページが表示され、**ログオン完了**。

※ブラウザや環境によって、画面イメージが異なる場合がございます。ご了承ください。

スマートフォンでログオンする場合〈Trusteer Mobile（トラスティーア・モバイル）でログオン〉 ※個人のお客さまのみ

1

アプリを起動

「Trusteer Mobile」を起動。

ログオン画面で「ご契約者番号（10桁）」と「ログオンパスワード（6桁）」を入力し、「ログオン」を選択。

※Trusteer Mobile のご利用方法については
13 ページをご参照ください。

2

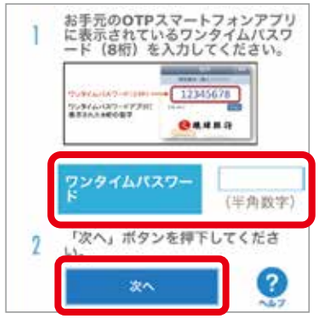
アプリを起動

ワンタイムパスワードアプリを起動し、「Copy」を選選択。
コピーが完了したら「Trusteer Mobile」アプリの画面に戻る。

※スマートフォンの詳しい操作方法については
各携帯電話会社のマニュアルをご参照ください。

3

アプリを起動



ワンタイムパスワードの入力欄に、2でコピーしたパスワードを**貼り付け（ペースト）**して、「次へ」を選択。

トップページが表示され、**ログオン完了。**

パソコンでログオンする場合〈スマートフォンまたは携帯電話でアプリを使用〉

1

「契約者番号（10 桁）」、「ログオンパスワード（6 桁）」を入力し「ログオン」を選選択。

※法人（Bizネット）のお客さまは、「管理者」コードでのログオンの時にワンタイムパスワードが必要になります。（「利用者」コードでのログオン時には必要ありません。）ログオン後に「可変パスワード（2 桁）」の入力がありますので、お手元に「ご利用カード」をご準備ください。

2

▲スマートフォン画面イメージ

▲携帯電話画面イメージ

スマートフォンまたは携帯電話でワンタイムパスワード**アプリを起動。**

表示されたワンタイムパスワードを、パソコン画面のワンタイムパスワード欄に入力し、「次へ」を選択。

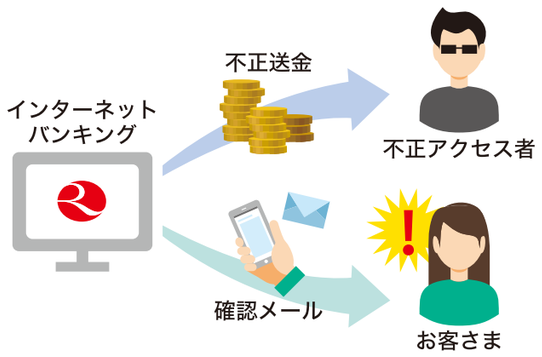
トップページが表示され、**ログオン完了。**

ログオンイメージ

初めてログオンする時には メールアドレスの登録が必要です。

重要なお知らせを確認するために

初めてインターネットバンキングにログオンされる時には、メールアドレスのご登録が必要です。
これはお取引内容の確認メールの受信のほかに、**不正利用による送金被害の拡大防止のためにも大変重要です。**携帯電話やスマートフォンなど、いつでもすぐにメールの内容が確認できるアドレスをご登録いただき、お取引後には必ずメールが受信されていることをご確認ください。



メールアドレス登録時に必要なもの

下記をご準備のうえ、メールアドレスのご登録へお進みください。

- ☑ **ご自身のメールアドレス ／ 2つのアドレスまで登録できます**
  （※携帯電話やスマートフォン等ですぐに確認できるアドレスを登録してください。）
- ☑ **りゅうぎんインターネットバンキングご利用カード**

メールアドレスの変更・受信設定について

メールアドレスの登録・変更後、ご指定のメールアドレス宛に『メールアドレス変更完了』の通知が発信されます。受信できない場合は、正しいメールアドレスに修正してください。メールアドレスの変更は、ログオン後、メインメニューの「**各種変更・申込（個人のお客さまの場合）**」または「**メンテナンス（法人のお客さまの場合）**」の「**メールアドレスの登録・変更**」よりお手続きいただけます。
また、**迷惑メール対策等で受信の制限をされている場合は、右記メールアドレスからのメールを受信できるよう設定を変更してください。**

個人のお客さま
direct@ryugin.co.jp

法人・個人事業主のお客さま
eb@ryugin.co.jp

1

インターネットバンキングにログオン。（初回）
メールアドレスを入力し必要事項を入力後「**登録**」ボタンを選択。

2

入力内容を確認し、**確認パスワードを入力して「実行」**ボタンを選択。

この場合は「**ご利用カード**」の確認番号「③の下」「⑤の下」に記載された番号「54」を入力。

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
確認番号	3	5	5	4	4	6	8	7	1	0

ご利用カード

3

登録完了。「**次へ**」を選択。
メインメニューより各種サービスがご利用いただけます。

メールアドレスの登録方法　〈スマートフォン・携帯電話編〉

1

インターネットバンキングにログオン。（初回ログオン）
メールアドレスを入力し必要事項を入力後「**登録**」ボタンを選択。

入力内容を確認し、**確認パスワードを入力して「実行」**ボタンを選択。

この場合は「**ご利用カード**」の確認番号「①の下」と「③の下」に記載された番号「35」を入力。

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
確認番号	3	5	5	4	4	6	8	7	1	0

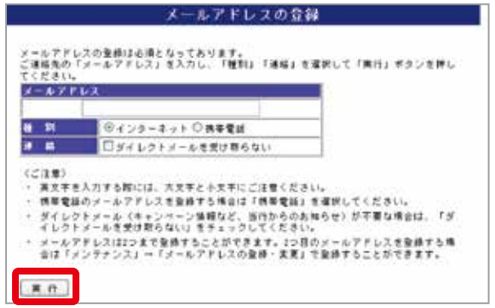
ご利用カード

2

登録完了。「**次へ**」を選択。
メインメニューより各種サービスがご利用いただけます。

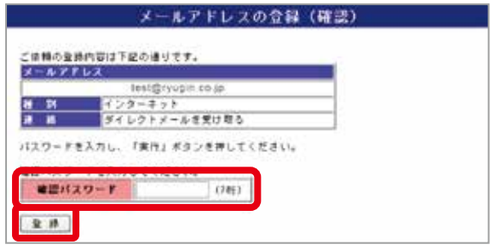
メールアドレスの登録方法　〈法人向け『Bizネット』編〉

1



「りゅうぎん Biz ネット」にログオン。（初回ログオン）
メールアドレスを入力し「**実行**」ボタンを選択。

2



※確認パスワード（7 桁）は、ご利用カードお受取り時の設定（初期値）は①～⑦までの数字です。ご自身で変更を行われた場合は、変更後の確認パスワードをご使用ください。

入力内容を確認し、**確認パスワードを入力して「登録」**ボタンを選択。

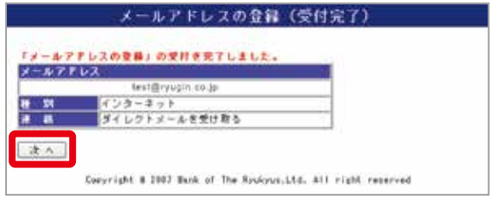
確認パスワード（7 桁）は、「**ご利用カード**」の①～⑦までの下の数字です。下記の場合は「3554468」を入力。

	①	②	③	④	⑤	⑥	⑦	⑧	⑨	⑩
確認番号	3	5	5	4	4	6	8	7	1	0

確認パスワード（7 桁）

ご利用カード

3



メールアドレスの登録（受付完了）画面で「**次へ**」を選択して登録完了。
メインメニューより各種サービスがご利用いただけます。

セキュリティ対策ツールの導入以外にも 設定の見直しやパスワードの管理が必要です。

振込限度額の設定

振込限度額を必要な範囲内で設定することで、インターネットバンキングを利用した不正送金が発生した場合の被害額をおさえることができます。
インターネットバンキングで「振込」をご利用されない場合は、振込限度額を「0 円」に設定することも可能です。下記設定から振込限度額が必要な範囲内に設定されているか確認しましょう。

パソコンで設定	ログオン	個人の方 各種変更・申込 法人の方 メンテナンス	振込限度額の照会・変更
スマートフォン・携帯電話で設定	ログオン	6. 各種変更・申込	3. 振込限度額

※「ワンタイムパスワード」をご利用いただいているお客さまは、引き上げの設定変更も可能です。（個人上限 500 万円、法人上限 10 億円）。それ以外の方は「窓口」でのお手続きが必要になります。

基本ソフト（OS）やソフトウェアは常に最新のものを使用する

古いバージョンのOSやサポートが切れているOSは、最新の手口（スパイウェアに感染）に引っかかりやすくて危険です。アップデート情報を見逃さないように気をつけて、常に最新のものを使うようにしましょう。

心あたりのないメールや、怪しいサイトは開かない

金融機関がお客さまのIDやパスワードについてメールでお問い合わせすることはございません。心あたりのないメールに記載されているURLや、怪しいサイトにはアクセスしないようにお気をつけください。アクセスすると、ウィルスを感染させるサイトへ誘導させられる可能性が高く危険です。

パスワードの徹底管理

パスワードの管理を徹底することで、不正利用されるリスクを減らすことができます。

- **単純な文字列**は使用しない（「1111111」や「1234567」、「password」など）
- **推測されやすい文字列**（生年月日や携帯番号等）を使用しない
- パスワードを**定期的に変更**する
- 他人に**パスワードを教えない**
- 他サイトの**パスワードの使い回しをしない**

「ログオンパスワードを忘れてしまった！」そんな時は…

お客さまのセキュリティを守るために、当行の行員がお客さまのパスワードを調べることはできません。パスワードを再登録するには、**窓口**で「**ご利用カードの再発行手続き**」をしていただくか、「**インターネットバンキング Light（要会員登録）**」にログオン後、インターネットバンキングのログオンパスワード再発行の手続きをしていただく必要があります。
なお、「インターネットバンキング Light」でのお手続きは、個人のお客さまのみとなっております。

窓口でお手続き ※個人・法人のお客さま

窓口に下記３点をお持ちいただき、お手続きをお願いいたします。

- ご利用カード
- お届け印
- 本人確認書類（免許証、パスポート他）

※ご利用の再開は、郵送にて届出住所にカードが到着後となります。

WEB でお手続き ※個人のお客さまのみ

「インターネットバンキング Light（ライト）」に会員登録されている方は、ログオン後にお手続きが可能です。

1. ログオン
2. 「インバンログオンパスワード再登録」を選択
3. 画面の案内に従って再登録

規定回数以上ログオンパスワードを間違えた場合も上記の方法でお手続きが可能です。

※ご利用カードに記載されている〈個人〉確認パスワード、〈法人〉可変パスワード・確認パスワードを規程回数以上間違えた場合は「窓口」でのお手続きのみとなりますのでご注意ください。

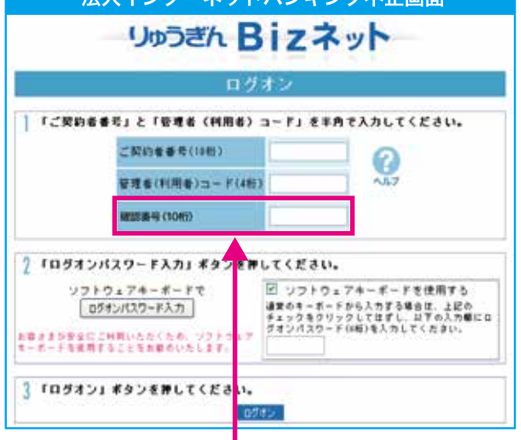
重要

偽のログオン画面にご注意ください！

「偽画面」表示によるパスワード等の詐取が発生しています。

当行ではインターネットバンキングのログオン時に「確認番号」を入力いただくことはありません。
ログオン時に入力するのは、りゅうぎん Biz ネット（法人）の場合「ご契約者番号（10桁）」と「管理者（利用者）コード（4桁）」、「ログオンパスワード（6 桁）」の 3 種類、りゅうぎんインターネットバンキング（個人）の場合は「ご契約者番号（10桁）」と「ログオンパスワード（6 桁）」の 2 種類のみです。下の画面のように、ログオン時に「ご利用カード」に記載の「確認番号（10桁）」の入力が表示される場合は、パソコンがウィルスに感染している可能性があります。
万一「下の画面が表示された」、「偽画面へ情報を入力してしまった」場合は速やかに右記お問合せ先までご連絡ください。

法人インターネットバンキング不正画面



個人インターネットバンキング不正画面

ログオン画面で「確認番号」の入力を求めることはありません。
絶対に入力しないでください。

その他ご注意すべき点

1 「ログオンパスワード（6桁）」「確認パスワード（7桁、法人向け）」は定期的に変更してください。
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おいてください。

2 **不審なメールは開けずに削除してください。**メール内の不審なリンクや添付ファイルも開かないでください。
不審なウェブサイトへは接続しないでください。

3 メールアドレスの登録は、**携帯電話のアドレス等、メールの受信を直ちに確認できるものを登録してください。**お振込等の都度、取引内容をお知らせしますので、**万一不正送金等があっても早期の発見につながります。**
※メールアドレスの登録・変更後は必ずメールが受信されていることを確認してください。

4 迷惑メール対策でメール受信の制限をされている場合は
eb@ryugin.co.jp（法人向け）、direct@ryugin.co.jp（個人向け）
からのメール受信を許可するように設定をお願いします。

5 **振込・払込限度額は必要な範囲内で適切な金額に設定してください。**限度額の引下げはインターネットバンキング上のメニュー「メンテナンス（法人向け）」「各種変更・申込み（個人向け）」から行うことが出来ます。但し、引き上げについては「ワンタイムパスワード」をご利用のお客さまは上記メニューから、それ以外のお客さまは営業店（法人は代表口座店）の窓口にて書面でお申込みください。

お問い合わせ先 通話料無料

夜12時までのご連絡は
りゅうぎんEBセンター **0800-300-3927** 平日 9時～24時 / 土・日・祝日 8時～24時

上記以外の時間帯で緊急時のご連絡は
ATMほっとライン フリーコール **0120-49-8689** 24時間

セキュリティ対策は万全ですか？
セルフチェックで最終確認しましょう！

チェック！

ご利用端末に セキュリティ 対策ツールを導入 ⇒P2参照	ウィルス対策ソフト「Rapport（ラポート）」のインストール　パソコンを ご利用の方	☐
	セキュリティブラウザ「Trusteer Mobile（トラスティーア・モバイル）」のインストール　スマートフォンを ご利用の方	☐
	ワンタイムパスワードの利用　パソコンをご利用の方 スマートフォンをご利用の方	☐
インターネットバンキングの 設定	**メールアドレス**の登録 ⇒P24参照	☐
	振込限度額を確認し、必要範囲内に設定する ⇒P28参照	☐
インターネットバンキングの ご利用にあたり 気をつけること ⇒P29参照	**パスワードの管理**を徹底する	☐
	心あたりのないメールを開いたり、**怪しいサイト**にアクセスしない	☐
ご利用端末の環境について ⇒P28参照	ご利用端末の基本ソフト（OS）やソフトウェアを **最新のものにアップデート**している	☐

チェックの数を確認！

チェックの数を数えて、あなたのセキュリティレベルを確認しましょう。

0～3	低	ウィルスに感染したりフィッシング詐欺の被害に合う可能性が高くなっています。まずはセキュリティ対策ツールの導入や、設定の見直しをしましょう。
4～6	中	セキュリティ対策をしていただいているようですが、まだ少し脅威に対して脆弱性があります。よりセキュリティを強化するため、本ガイドを確認しながら対策をお願いします。
7～8	高	セキュリティレベルが高く、安心してお使いいただけます。しかし、金融詐欺の新たな手口が出てくる可能性もありますので、琉球銀行ホームページにアップされる注意喚起情報に気を配り、万が一「怪しい」と思ったらすぐにお電話などでお問い合わせください。

Q1.Rapport（ラポート）や Trusteer Mobile（トラスティーア・モバイル）の利用手数料は無料ですか？

ご利用手数料は無料でご利用いただけます。追加でかかる手数料や更新のための費用等もございません。
※インターネットに接続するためのプロバイダ料金および通信料は、お客さま負担となりますのでご了承ください。

Q2. ワンタイムパスワードを使わなくてもいいですか？

ワンタイムパスワードの導入は任意ですが、セキュリティ強化のために導入を推奨しています。
万が一「ログオンパスワード」や「確認パスワード」の情報が盗まれた場合でも、ワンタイムパスワードを導入していることで不正送金を未然に防げることが可能になります。
より安心・安全にインターネットバンキングをご利用いただくためにも、導入をご検討ください。

Q3. スマートフォン（携帯電話）を機種変更する予定だけど、ワンタイムパスワードはそのまま使えるの？

ワンタイムパスワードアプリをダウンロードしたスマートフォンや携帯電話の機種変更や修理などを行う場合は「利用停止」の申請が必要になります。インターネットバンキング Light もしくはお取引店窓口からお手続きをお願いいたします。ご利用を再開される場合は、お使いになる機種で再度「ワンタイムパスワードのお申込」→「ワンタイムパスワードアプリのダウンロード」→「ワンタイムパスワードアプリの設定処理」を行ってください。
※「利用停止」を行わずにスマートフォンや携帯電話を変更されると、インターネットバンキングをご利用いただけなくなりますのでご注意ください。

個人のお客さま向け

▼パソコンで申請

琉球銀行ホームページ ▶ インターネットバンキングLightログオン ▶ ワンタイムパスワード利用停止

▼スマートフォンで申請

琉球銀行ホームページ ▶ インターネットバンキングLight ▶ インターネットバンキングLightログオン ▶ OTP利用停止申請

個人・法人向け

▼窓口で申請

ご利用カード　代表口座のご印鑑　ご本人確認書類　左記３点をご準備のうえ、お取引店窓口へご来店ください。

Q4. 登録後にメールアドレスを変更したけど、手続きは必要ですか？

「お取引確認メール」を受信していただくために、「各種変更・申込」メニュー（法人は「メンテナンス」）より必ず変更登録のお手続きをお願いいたします。
※メールアドレスは２つまで登録が可能です。

Q5. パスワードに有効期限ってあるの？

「ログオンパスワード」の有効期限は90日です。期限が到来したら、変更・継続使用の選択が可能です。また、パスワードは随時変更可能ですので、セキュリティ対策のためにも定期的かつ必要なタイミングで変更してください。

Q6. 設定を変更した覚えがないのに振込限度額が「０円」になっています。

平成27年6月28日（日）、長期間※インターネットバンキングをご利用いただいていないお客さまの「振込限度額」を「0円」に引き下げさせていただきました。インターネットバンキングのセキュリティ向上の観点から、振込限度額を引き下げることでお客さまが不正送金被害に遭われる可能性を低減いたしました。ただし、残高照会や入出金明細照会、お振替等は従来通りご利用いただけます。
「振込限度額」の引き上げは、インターネットバンキング（ワンタイムパスワードをご利用の方のみ）または窓口からお手続きいただけます。

※長期間とは…
〈個人のお客さま〉 … 平成25年12月31日までに会員登録のあるお客さまで、平成26年1月1日以降に「お振込」「お振替」「定期預金の預入・支払い」「投資信託の購入・解除等」のご利用が一度もないお客さま。

〈法人のお客さま〉 … 平成25年12月31日までに会員登録のあるお客さまで、平成26年1月1日以降に管理者コードまたは利用者コードで一度も「ログオン実績」のないお客さま。

Q7. インストールしたセキュリティ対策ソフト（またはアプリ）は削除していいですか？

「ワンタイムパスワード」のアプリについては、削除前に「利用停止」のお手続きが必要です。お手続きをせずにアプリを削除するとインターネットバンキングにログオンできなくなるため、必ずお手続き後に削除してください。
詳しいお手続き方法については 33 ページの Q3 をご覧ください。
「Rapport」と「Trusteer Mobile」については、削除前のお手続き等は不要です。ご利用を再開するには、再度インストールをお願いします。

Q8. 市販のウィルス対策ソフトや会社で独自のセキュリティ対策ソフトを入れているが、Rapport を導入する必要はありますか？

Rapportはインターネットバンキングを狙ったウィルスに特化したソフトです。市販のウィルス対策ソフトと検知の方法が違うため、併用することでウィルスに対する保護力が高まります。ぜひ、導入をご検討ください。

Q9.Rapport をインストールしたら、パソコンの動きが遅くなったので外して（アンインストールして）しまったけど…

お使いになっているパソコンの環境や条件により、動きが遅くなるケースが発生する場合がございます。37ページに記載のあるIBM Trusteerカスタマーサポートへご連絡し、ご相談ください。

Q10.Trusteer Mobile ではウイルスは駆除しないの？

Trusteer Mobileはインターネット専用のブラウザ（閲覧アプリ）です。ウィルスの駆除は行いませんが、ご利用時にウィルスの危険性がないかお使いの端末状況を確認し、リスクがある場合は、警告と修復ガイダンスが表示されます。万が一警告が表示されましたら、内容を確認しガイダンスにそって修復してください。

Q11.「ワンタイムパスワード」を申し込んだけど、キーホルダーやカード型の機械（ハードウェアトークン）は送られてこないの？

当行のワンタイムパスワードはソフトウェアトークンと言われるアプリケーション（アプリ）を、スマートフォンや携帯電話にインストールして使用します。（当行から郵送等でお届けするものはございません。）
キーホルダーやカード型の機械（＝パスワード自動発行機械）の役割をお客さまがいつも身近で使用されているスマートフォンや携帯電話が行います。
お申込み操作によりアプリをダウンロードすることで、その日からすぐにご利用することができます。アプリのアイコンを選択するだけでワンタイムパスワードが表示されますので、とても便利です。ぜひ、ご利用ください。

Q12.「ワンタイムパスワード」のパスワードはメールで送られてこないのですか？

当行のワンタイムパスワードは、スマートフォンや携帯電話にダウンロード（導入）したアプリのアイコンを選択するだけでパスワードが表示されますので、パスワードがメールで送られることはございません。
お使いになるパソコンと別の端末（スマートフォンや携帯電話）でパスワードが発行されますので、万が一お使いのパソコンから契約者番号（ID）やログオンパスワードの情報が漏れたとしても、ワンタイムパスワードをご利用することにより第三者からの不正なログオンを防ぐことができます。

Q13. いつも検索サイトで「琉球銀行」や「りゅうぎんインターネットバンキング」などを検索してアクセスしているけど…

GoogleやYahoo!等の検索サイトは便利ですが、時に偽サイトに誘導される可能性があります。
検索サイトを使用されるときは、当行ホームページ（http://www.ryugin.co.jp）が正しく表示されているか確認してから、ログオンボタンよりログオンしてください。

Q14. インターネットバンキングのログオン画面以外でログオンパスワードの入力を求められたけど問題ないですか？

インターネットバンキングのログオン画面以外での、ログオンパスワードの入力はお勧めできません。
一部アプリ（ソフト）等（例：家計簿アプリ）をご利用されている場合、アプリにより自動的にインターネットバンキングへアクセスし、入出金の明細等をダウンロードする仕組みになっております。家計簿を自動的に作成するアプリ（ソフト）等は便利なように思われますが、お客さまの契約者番号（ID）やログオンパスワード等の個人情報の登録が必要となっているため、不正利用防止の観点から当行では推奨しておりません。
万が一、他のサイト等で入力した情報が原因となり不正送金等の被害に遭われた場合は、補償の対象外となるケースもあります。ご利用の際には充分にご注意ください。

Q15. もっと詳しくウィルス対策ツールの情報を知りたい

ウィルス対策ツールの情報やセキュリティ対策については、当行ホームページにも掲載していますので、ぜひご参照ください。また、最新の情報も随時掲載いたしますので、ログオン前にはぜひご確認ください。

お問い合わせ

下記連絡先またはお近くの琉球銀行窓口へお気軽にお問い合わせください。

操作に関するお問い合わせ 通話料無料

りゅうぎんEBセンター　**0800-300-3927**

受付時間　平日 9時～24時
土・日・祝日 8時～24時

ご利用カードの紛失・盗難に関するお問い合せ

お取引店へご連絡ください。

受付時間　平日 9時～17時
土・日・祝日 休業

銀行営業時間外および休日のご利用カード紛失・盗難に関するお問い合わせ 通話料無料

ATMほっとライン　フリーコール **0120-49-8689**

受付時間　24時間

Rapport（ラポート）や Trusteer Mobile（トラスティーア・モバイル）に関するお問い合せ 通話料無料

IBM Trusteer カスタマーサポート
0120-925-283（インターネットバンキング会員のみ利用可能）
http://www.trusteer.com/

受付時間　平日 9時～21時
土・日・祝日 休業

または上記ホームページURLより「カスタマーサポート」を選ぶ事で
①チャット　②メール　③折り返しの電話（コールバック）のご利用もできます。