

よくあるご質問

Q.1 [契約者ID][初回ログインパスワード][資金移動用パスワード][ワнтаイムパスワード]は、どのような場面で使うのですか？ また、ログインパスワードの「初回」とはどういう意味ですか？

A.1 ご利用場面毎の使用ID・パスワードは次の通りです。なお、初回ログインパスワードは、お申込後の初回ログイン時に正式なログインパスワードに変更してご利用いただけますので、次回ログイン以降は登録したログインパスワードをご利用いただけます。

[契約者ID][ログインパスワード]: ログイン時
[資金移動用パスワード]: ワンタイムパスワード利用開始登録時
[ワンタイムパスワード]: ログイン時*、振込、振込予約取消、利用限度額変更等
※ログイン時については、利用者の設定によっては不要。

Q.2 パスワードを変更したいのですが？

A.2 ログインパスワードは「メインメニュー」⇒「サービス一覧」⇒「ログインパスワード変更」にて変更できます。

[資金移動用パスワード]は、営業店窓口での変更となりますので、お問い合わせ先までご連絡ください。

Q.3 規定の回数を超え、連続で入力を間違えてしまったため、パスワードがロックされてしまいました。どうすればいいのですか？

A.3 各パスワードのロックの解除については、当金庫所定の手続きが必要ですが、詳細につきましては、お問い合わせ先までご連絡ください。

Q.4 ワンタイムパスワードをインストールしたスマートフォンを買い替えますが、何か手続きは必要ですか？

A.4 ■お手元に新旧両方のスマートフォンがある場合は、新旧スマートフォンを利用して「ワンタイムパスワードの交換」を実施してください。詳細につきましては、当金庫ホームページでご確認ください。

■お手元に旧スマートフォンしか無い場合は、旧スマートフォンで「ワンタイムパスワードの利用中止」を実施してください。新スマートフォンがお手元に届き次第、再度「ワンタイムパスワードの利用開始」を実施してください。詳細につきましては、当金庫ホームページでご確認ください。

■お手元に新スマートフォンしか無い場合、旧スマートフォンのワンタイムパスワードアプリをアンインストールしたなど、旧スマートフォンでワンタイムパスワードが表示できない場合は、当金庫所定の手続きが必要です。詳細につきましては、お問い合わせ先までご連絡ください。

※「ワンタイムパスワード利用開始」及び「ワンタイムパスワード利用中止」には、数字10桁の資金移動用パスワードが必要となります。

ご注意事項

契約者ID、各パスワードの管理について

お申込書（お客様控）は、通帳、印鑑およびキャッシュカードと同様に非常に大切なものです。以下の点にご注意のうえ、お客様ご自身で厳重に管理してください。

■お申込書（お客様控）は他人の目に容易に触れるところに放置しないでください。

■各パスワードは、他人には絶対に教えないでください。

※当金庫職員が、お客様にパスワードを確認させていただくことはありません。

■[ログインパスワード]は、定期的に変更していただくことをお奨めします。

■契約者IDや各パスワードが他人に知られたと思う場合は、「IB取引中止」操作またはすみやかに当金庫までご連絡ください。

■ログイン時に、不正な入力画面（ポップアップ画面）を表示させ、パスワード情報を入力させようとするウィルスが発生しています。IBシステムが、「資金移動用パスワード」を3箇所以上同時に入力要求することはありませんので、絶対に入力しないでください。

■IBシステムがパスワード等の重要情報のコピーをアップロード要求することはありませんので、絶対にアップロードしないでください。

セキュリティに注意してください

最近、マルウェア、ウィルス、フィッシング詐欺等により、お客様から暗証番号（パスワード）などを不正に取得し、お客様に成りすまして、お客様の口座から不正に預金を引き出す（振り込む）被害が発生しております。本サービスをより安全にご利用いただくために、以下の点にご注意のうえ、本サービスをご利用いただきますようお願いいたします。

■ウィルス対策ソフト等は最新の状態に保つ

ウィルス対策ソフト「Rapport（ラポート）」等を導入し、パターンファイル、ブラウザ・OSのセキュリティパッチの更新をこまめに行い、パソコンやスマートフォンのセキュリティ水準を最新の状態に保ってください。更新を自動的にしてくれる機能も提供されていますので、有効に活用してください。

■不審な電子メールの開封、不審なソフトのダウンロード、不審なリンクのクリックは行わない

コンピュータウィルスやスパイウェアは、電子メール開封時やフリーソフト等のダウンロード、不審なホームページを開いたときなどに、気付かれないままパソコンやスマートフォンに入り込む可能性があります。心当たりのない電子メールの開封や不審なフリーソフト等のダウンロードには十分ご注意ください。また、ウィルス等に感染した疑いのある場合は、すぐにセキュリティ対策ソフトなどでウィルスチェックを行ってください。

■実在の人物・企業・組織になりました電子メールやSNSに注意

実在の人物・企業・組織になりました電子メールを送付する、または請求書や不在通知等の受信者が開きやすい電子メール・SNSメッセージを送付してウィルスに感染させる例が増えていますので、ご注意ください。

■パスワード等をPC、スマートフォン等内に保存しない

パスワード等の重要情報は、絶対にPCおよびスマートフォン内に保存しないでください。コンピュータウィルスやスパイウェアによってそれらが流出した場合、深刻な被害に遭うおそれがあります。同様に、ネットワーク上のサービス（例：クラウドサーバー）等にこれらの重要情報を保存することもやめてください。