

セキュリティ

●二要素認証

U I 銀行では、取引において複数の認証要素を用いることで、なりすましや乗っ取りなどのリスクに対応しています。

取引の種類に応じて、端末認証や SMS 認証などの「所有認証」、パスワードや PIN 番号などの「記憶認証」、指紋や顔などの「生体認証」の認証要素を組み合わせることで、セキュリティの強化を行なっています。

●不正アクセス防止

不正アクセスに備えて、ログインパスワード等の各種認証は、一定回数以上誤って入力されるとロックがかかります。

●メール通知

普通預金口座からのお振り替えやメールアドレスの変更などの手続きがあった場合、登録済みのメールアドレス宛に取引・手続き内容を通知します。お取引に覚えのない場合は当社までご連絡ください。

●通信の暗号化

ネット上を流れるすべての情報は SSL/TLS(128bit)により暗号化し、保護されます。SSL/TLS は、通信データを暗号化することで、第三者にその内容を知られないようにする規格です。

●情報の保護

U I 銀行では、お客さまの情報の保護について細心の注意を払っております。U I 銀行アプリには、ご利用時に入力いただいた重要な情報は保存されません。

また、U I 銀行が取り扱うお客さまの情報は、暗号化や、社員のアクセス権限の厳正な管理などの安全対策を行ったうえで保存されています。

●サイバーセキュリティ監視体制

お客さまの情報を預かり、サービスを提供する U I 銀行のシステムは、24 時間 365 日セキュリティ監視を行い、外部からの不正な侵入やサイバー攻撃の予兆を早期発見し、未然に防ぐ体制をとっております。

また、ファイアウォールなどのさまざまな対策によって、不正侵入や DDoS 攻撃などのサイバー攻撃を防止しています。

●取引端末の限定

口座開設後は、登録した端末以外からのご利用はできません。第三者によるなりすまし等の不正利用を防ぐことができます。

●お引出し限度額の設定

U I 銀行アプリで以下の設定が可能です。設定の内容は即時で反映します。

- ・提携 ATM について、1 日あたりのお引出し限度額の変更が可能です。
- ・お振込について、限度額の変更が可能です。

●ワンタイムパスワード

モバイルアプリでお取引（振込、定期預金お預入れなど）をする際に、スマートフォンで生成する 1 回限りの使い捨てパスワードが表示されます。再利用できないため、不正送金被害等に遭うリスクの低減が図れます。

尚、ワンタイムパスワードご入力後、お取引が成立します。

以上