２．セキュリティについて

概要

本サービスでは以下のセキュリティ対策を行っています。セキュリティ保全の観点から、以下の内容はお客さまに対して一部公表しません。

（１）システム環境

① 128bit SSL 暗号化方式を採用

② EVSSL サーバー証明書の採用（フィッシング犯罪への対策として EVSSL サーバー証明書を採用しています。）

③ サーバー検知型ウイルス対策ソフト TrusteerPinpoint の採用

ご契約者さまが本サービスを利用する際に、契約者が操作する端末がｺﾝﾋﾟｭｰﾀｰｳｨﾙｽ（ﾏﾙｳｪｱ）等に感染していないかを検知し、感染が認められる場合はﾛｸﾞｵﾝﾊﾟｽﾜｰﾄﾞを利用不可とすると同時に振込限度額を強制的に「0 円」とします。実質的に資金移動が不可能となります。ご契約者さまの意図とは関係なく稼働し、本機能の解除等はできません。

④ 一定時間操作がなかった場合の自動ログオフ機能の導入

⑤ ソフトウェアキーボードの導入

（２）不正利用防止、リスク低減のための仕組み

① 最大 4 種類の ID/パスワードでお客さまのご本人確認をします。(「ご契約者様番号」「ログオンパスワード」「確認パスワード」「ワンタイムパスワード（任意）」)

② リスクベース認証

ご契約者さまが本サービスを利用する際の基本パターン（IP アドレスや端末種類や時間帯など）を記憶し、それらを逸脱するアクセスが検知された場合に、ログオン時に ID/パスワード以外の追加質問項目（好きな食べ物は？などの合言葉）が提示されます。上記、追加質問項目の回答は初回ログオン時にご契約者さま自身が設定します。セキュリティの観点からも照会には応じられません。ご契約者さまの意図とは関係なく稼働し、リスクベース認証機能の解除等はできません。なお、設定できるのは全角（ひらがな、カタカナ、英字、数字）２０字以内です。

③ 振込・払込限度額の設定（第三者の不正アクセスによる不正送金被害の低減）

④ 前回ご利用日時の表示（第三者による不正アクセスの自己チェックが可能）

⑤ 受付内容や受付結果等の電子メール送信（第三者による不正アクセスの自己チェックが可能です。）

（３）その他

① セキュリティソフト「SaAT Netizen（サートネチズン）」の配布

② スマートフォン専用セキュリティアプリ「SecureStarter」の配布