セキュリティ

●本人確認方法
「JAネットバンク」では、ログインID、ログインパスワード、確認用パスワード、メール通知パスワード、ワンタイムパスワードによって、ご本人であることを確認します。
※携帯電話からのご利用の場合は、携帯電話固有のID番号を使用します。

●128ビットSSL（Secure Sockets Layer）暗号化方式
「JAネットバンク」では、お客様のパソコンと当JAのコンピュータ間のデータ通信について、安心してご利用いただけるよう最新式の暗号化技術の128ビットSSL暗号化方式を採用し、情報の盗聴・書換え等を防止します。

●ソフトウェアキーボード（パソコンご利用時のみ）
「JAネットバンク」の画面上に表示されたキーボードをマウスでクリックすることにより、パスワードを入力します。キーボードで入力しないため、キーボードの入力情報を盗み取るキーロガーを防ぎます。

●ワンタイムパスワード
ワンタイムパスワードとは、1分毎に変化する1回限りで無効となる使い捨てのパスワードです。ログインID、ログインパスワードに加え、携帯電話やスマートフォンに表示されるパスワードを入力して本人確認を行います。
ワンタイムパスワードはお客様の携帯電話やスマートフォンにインストールしたトークン（トークンアプリ）により生成され、携帯電話やスマートフォンの画面上に表示されます。
万一、ウイルス等によりパスワードが盗まれたとしても、パスワードは1分毎に更新され、1度使用したパスワードはその時点で使用できなくなることから、不正利用の防止に有効な対策です。
※スマートフォンをご利用の場合は、ワンタイムパスワードのご利用が必須となります。

●メール通知パスワード（取引認証パスワード）
振込、各種料金の払込み、お客様情報の変更等の取引時に、お客様にご登録いただいたメールアドレスに、取引の都度、取引内容とパスワードを記載したメールを送信します。取引内容を確認できるとともに、通知されたパスワードを確認用パスワードに加えて入力することにより、第三者に不正利用されることを防ぎます。

●リスクベース認証（追加認証）
「JAネットバンク」では、第三者からの不正利用を防止するため、お客様のご利用環境を分析させていただいております。万一、通常と異なる環境と判断した場合には、ご登録いただいた「質問」と「回答」による追加認証を行います。
※携帯電話からのご利用の場合は、携帯電話固有のID番号で端末認証を行うため、追加認証は行いません。

●不正送金対策ソフト

JAバンクでは偽サイト誘導防止対策、ウイルス攻撃対策等の観点で「PhishWallプレミアム」を無償で提供しております。JAネットバンクのホームページからダウンロードいただきますようお願いします。

●EV-SSL証明書（Extended Validation SSL）

フィッシング詐欺への対策として「EV-SSL証明書」を採用してセキュリティの強化を行っております。

EV-SSL証明書で保護されている「JAネットバンク」にアクセスすると、パソコンのアドレスバーが緑色に変わります。

※ブラウザのバージョンによっては、ご確認いただけない場合があります。

●振込限度額の変更

ワンタイムパスワード未利用時に限度額を引き上げた場合、3日後から変更されます。

ワンタイムパスワードご利用時、ネットバンクご利用開始4日目以降に限度額を引き上げた場合、もしくは限度額を引き下げる場合は、操作完了後すぐに変更されます。

●直近のご利用履歴

「JAネットバンク」にログインした際、パソコンの場合は直近3回のご利用履歴、スマートフォンの場合は前回のご利用履歴が確認できます。

第三者の成りすましによる不正アクセスをチェックできます。

●電子メールによる取引通知

ご利用のお取引に応じて、電子メールで確認メールをお送りします。

スマートフォンまたは携帯電話のメールアドレスを登録される方で、インターネット経由のメールを、受信拒否に設定されている場合は、スマートフォンまたは携帯電話の「ドメイン指定受信機能」により、「webcenter.anser.or.jp」「otp-auth.net」のドメインが受信できるよう設定を行ってください。

●自動ログアウト

ログインしたまま離席された場合等、画面の盗み見等を防止するため、一定時間操作をせずに放置していると、自動的にログアウトします。