



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、ワンタイムパスワード等により、ご本人であることを確認します。

●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ワンタイムパスワードアプリ(トークンアプリ)で生成され、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。

※都度振込、ペイジー(民間)のお取引には、ワンタイムパスワードのご利用が必須となります。

●生体認証ログイン

スマートフォンのワンタイムパスワードアプリ(トークンアプリ)からログインする際に、スマートフォンに搭載された生体認証(指紋認証・顔認証)を利用することにより、ログインID・ログインパスワードを入力することなくログインすることができます。

●ソフトウェアトークン取引認証

振込・振替処理が行われた都度、スマートフォン上のワンタイムパスワードアプリ(トークンアプリ)で、お客様ご自身が「振込先・振込金額」等をご確認のうえ認証を行うセキュリティです。認証がなければ振込が完了しないため、不正ログインや振込内容改ざんによる不正送金を防ぎます。

●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きます。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。

●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いたします。

●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の場合(JA窓口で事前登録した口座への振込・振替のみ可能)、限度額引上げは3日後に変更されます。

ワンタイムパスワードご利用の場合、ワンタイムパスワード利用開始日を含め3日間は、限度額引上げは即時に変更されません(同期間経過後に変更されます)。同期間経過後の限度額引上げは、操作完了後即時に変更されます。

限度額引下げは、ワンタイムパスワードの利用に関わらず、操作完了後即時に変更されます。

●直近のログイン履歴

「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回のログイン履歴、スマートフォンの場合は前回のログイン日時が確認できます。

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」「janetbank.jp」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。

●届出電話番号認証

お届け済みの「ご登録電話番号」から「認証先電話番号」へ発信することで、本人認証を行うことができます。