セキュリティに関する注意事項

日頃のセキュリティ対策について、以下のような点にもご注意ください。

NG 心当たりのないメールやサイトは開かないでください。

お客さまの情報を盗みとろうとする偽Eメールを開いたり、メールに記載されているリンク先へアクセスしただけでお客さまのパソコンがウィルスに感染する場合もあります。

NG ID・パスワードのお取扱いにはご注意ください。

パスワードはご本人さまを確認する大切な情報です。定期的に変更していただくようお願いします。なお、職員がEメールや電話等でIDやパスワード等を照会することはありません。絶対に、他人に教えることがないようご注意ください。

NG パソコンのOSやインストールされているセキュリティソフトは最新の状態へ更新してください。

常に最新版を適用することで、不正送金被害の防止に役立ちます。また、製造元のサポートが終了しているバージョンのOS等の使用は避けていただき、サポートされているバージョンを使用することを、強くおすすめします。※WindowsXPは平成26年4月9日（水）に、マイクロソフト社によるサポートが終了となりました。

NG 不特定多数の方が使用するパソコンでログインしないでください。

インターネットカフェなど不特定多数の方が使用するパソコンでインターネットバンキング利用した場合、入力したID・パスワードや閲覧した情報がパソコン内に残ってしまう危険があります。

セキュリティ対策のご利用方法や操作方法については、
下記のお問い合わせ先までご連絡ください。

JAネットバンク ヘルプデスク

《ネットバンクに関するサービスおよび各種操作方法について》

0120-058-098

音声ガイダンスに沿って、1番をプッシュしてください。

［平日］9:00～21:00　［土日祝］9:00～17:00 ※1月1日は終日、受付けしておりません

万一、不正送金の被害に遭ってしまったら・・・

《緊急時のサービスの利用停止について》

0120-058-098

音声ガイダンスに沿って、3番をプッシュしてください。

24時間 365日 ※フリーダイヤルは携帯電話、スマートフォン、IP電話からもご利用いただけますが、一部ご利用いただけない場合があります。

ネットバンキング犯罪から お客さまの口座を守るために

不正送金の被害が発生しています

JAネットバンクをご利用のお客さまにおいても、不正取引の被害が発生しています。
JAネットバンクでは、お客さまに安心してインターネットバンキングをご利用いただけるよう、
最新のセキュリティ対策を用意しています。大切な貯金を守るためにも、導入を強くおすすめします。

お心当たりはありませんか？

こんな手口であなたのIDやパスワードが狙われています。

CASE 1

スパイウェア

電子メールなどを介して、知らないうちにパソコンに侵入し、パスワード等の個人情報を第三者に転送するプログラムを使ったケースです。

CASE 2

ウイルス感染

ウイルス感染により、不正なポップアップ画面等を表示して、パスワードなどを入力させることで個人情報を盗み取るケースです。

CASE 3

フィッシング詐欺

金融機関になりすまして電子メール等を送付し、偽のサイトへ誘導することで、のID・パスワードなどの個人情報を不正に取得するケースです。

これらの不正送金の手口に遭わないためには？

詳しい対処方法については中面をお読みください。▶

JAネットバンク

大切な貯金を守るために

ぜひ、ご利用いただきたい 3つの対策

不正送金を初めとしたネットバンキング犯罪の手口は、日々巧妙化しています。被害に遭うリスクを最小限にするためには、下記のセキュリティ対策ツールを複合的に使用することを、強くおすすめいたします。

対策 1

ネットバンキング専用の不正送金対策ソフト

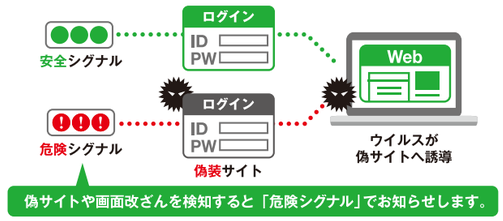
PhishWallプレミアム（無料）をぜひご利用ください。

アンチウイルスソフトも無償提供していますので、ぜひご利用ください。

偽サイトへの誘導やウィルスによる画面改ざんを検知し、不正送金を防止します。

ウイルス感染による偽装サイトへの誘導や、画面改ざん（MITB攻撃）を検知し、不正送金を防止する不正送金対策ソフト「PhishWall（フィッシュウォール）プレミアム」および「アンチウイルスソフト」を無償提供しています。インストールすると、JAネットバンクにアクセスした際、ブラウザのツールバーにシグナルを表示させることで、正式なサイトであることを確認できるようになります。

● PhishWall プレミアムが不正取引を防止する仕組



対策 2

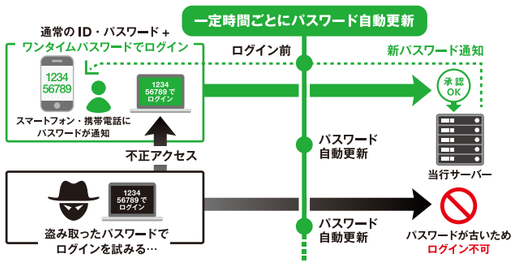
不正ログインを防ぐために

ワンタイムパスワードをぜひご利用ください。

ワンタイムパスワードはセキュリティの高いパスワードです。

一度お取引で利用したワンタイムパスワードや一定時間経過したワンタイムパスワードは無効になるため、第三者が不正に再利用することができません。そのため、高いセキュリティを確保できますので、ご利用を強くおすすめいたします。

● ワンタイムパスワードの仕組



対策 3

不正取引を防ぐために

メール通知パスワード（取引認証パスワード）をぜひご利用ください。

※すでに、ワンタイムパスワードをご利用の方は、取引認証パスワードをご利用ください。

メール通知パスワードは、お取引を選択いただくとその取引専用のパスワードがメールで通知されるシステムです。

不正な振込等身に覚えのない取引が行われた場合には、Eメールで取引内容が通知されるため、第三者による不正振込を防止できますので、ご利用を強くおすすめいたします。ご利用されるパソコンとは別のスマートフォンや携帯電話等のアドレスをご登録ください。また、フリーメールアドレスのご利用は避けてください。

● メール通知パスワードにより不正取引を防止する仕組

その他にも様々なセキュリティ対策をご用意しております。

セレクトEメールサービス（追加メールアドレス）

あらかじめ登録されているメールアドレスとは別に、追加メールアドレスを設定いただき、振込・振替や各種設定変更時等の受付メールを受信することができます。

インターネットバンキングロック（IBロック）

通常時はパソコンからインターネットバンキングができないようにロックをかけておき、取引する際に携帯電話にてそのロックを解除する機能です。

限度額の変更

パソコンまたはスマートフォン・携帯電話から振込振替限度額の引き下げが可能です。万一、不正送金の被害に合った際に、被害を最小限に抑えるための手段として有効です。

リスクベース認証（追加認証）機能

普段と異なる環境からアクセスした際に、本人確認のため、あらかじめ設定していただいた「一問一答の合言葉」の入力をすることで不正取引を防止します。