

平成22年12月3日

J Aネットバンクご利用のお客様へ

秋川農業協同組合

## インターネットを利用した金融犯罪防止について（お知らせ）

昨今インターネットを利用した犯罪が増加しており、インターネットバンキングについても簡単な文字列の組み合わせにより不正なアクセスを繰り返す、口座から預金を引き出す例が複数の金融機関において発生しています。

つきましては、改めて以下の点にご留意いただき、J Aネットバンクをご利用ください。特に、ログインID・パスワードにつきましては、同一の英数字や連番等の推測されやすい文字列のご使用はお控えいただくとともに、定期的な変更をお勧めいたします。

また、身に覚えのないお取引がございましたら、お取引のある店舗にご連絡ください。

### **J Aネットバンクのご利用にあたっては、以下の点にご留意ください。**

#### **1 推測されやすいパスワードのご使用はお控えください**

（推測されやすいパスワードの例）

- ・ 同一の英数字や連番
- ・ 生年月日、自宅の住所地番や電話番号、勤務先の電話番号、自動車のナンバーなど
- ・ パソコンや携帯電話の電子メールアドレス
- ・ その他のインターネットバンキングで使用しているパスワード、キャッシュカードの暗証番号など

#### **2 パスワードは定期的に変更してください**

第三者による不正使用を防止するため、パスワードは定期的に変更してください。ログインID・パスワードはメニュー画面のメニューバーで「ログインID変更」「パスワード変更」をお選びいただくと、24時間いつでもご変更いただけます。

#### **3 目につくところにパスワードをメモしないでください**

第三者にパスワードを不正に取得される恐れがあります。また、ID、パスワード等を記録したファイルをパソコン内に保存しないでください。

#### **4 インターネットバンキングロックのご利用をお勧めします**

J Aネットバンクでは、通常はパソコンによるJ Aネットバンク取引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を提供していますので、ご利用を推奨します。

（詳しくはJ Aネットバンクホームページ画面「セキュリティ」をご覧ください）

**5 入出金明細は定期的を確認してください**

入出金明細は定期的を確認してください。不正使用の早期発見にもつながります。

**6 インターネットバンキングの利用後は必ずログアウトをしてください**

インターネットバンキングの利用後、ログアウトをしないままパソコンを放置することは、第三者に利用される恐れがあり危険です。インターネットバンキングの利用後は、必ずログアウトしてください。

**7 振込限度額を見直してください**

インターネットバンキングの1日当たり振込限度額を見直し、お客様に必要な金額を設定してください。万一、不正使用の被害が発生した場合でも、被害金額を抑えることができます。また、1回当たり振込限度額はJAの窓口で変更できます。

**8 電子メールアドレスをご確認ください**

インターネットバンキングで振込や振替などを受け付けた場合は、お客様が登録された電子メールアドレスに受付メールをお送りしています。電子メールアドレスが誤っている場合は、メールが届きませんので、必ず受信可能な電子メールアドレスを登録してください。JAネットバンクからの電子メールについては、閲覧可能な設定としてください。

**9 不特定多数の人が操作できるパソコンでのJAネットバンクの操作は避けてください**

図書館やインターネットカフェ等、不特定多数の人が操作できるパソコンでのJAネットバンクのご利用は避けてください。

**10 セキュリティ対策ソフトは最新のものを使用してください**

アンチウイルスソフトを導入いただくとともに導入後もウイルス定義ファイルを最新のものにアップデートし定期的にウイルスチェックを行うなど、高いセキュリティ水準を維持してください。

**11 心当たりのないメールは開かないでください**

心当たりのないメールは開かないでください。添付されているファイルについても同様です。メールを開いただけで、スパイウェアがインストールされてしまうものもあります。JAネットバンクでは、電子メールを使ってパスワード等をご照会することはございません。

また、心当たりのないメール中のリンクはクリックしないようご注意ください。

**12 外部から入手したCD-ROMや、インターネットでのソフトのダウンロードにご注意ください**

郵送されてきたり、無料で配布されているCD-ROMやインターネットで配布されているソフト、怪しいホームページへのアクセス、ウィニーなどのファイル交換ソフトを経由したファイルなどには、気づかぬうちにスパイウェアをインストールするものがありますので、ご注意ください。JAネットバンクでは、CD-ROMの郵送やソフトのダウンロードを要請することはありません。

### 13 フィッシングサイトにご注意ください

偽の web サイトに認証情報等を入力するように誘導し、インターネットバンキングサービスにログインするために必要な ID やパスワードを詐取する不正行為があります。ID、パスワードを詐取されてしまいますと、お客様になりすまして不正に振込出金が行われる恐れがあります。

また、JA ネットバンクでは EV SSL 証明書にて正しいサイトであることを表示しています。アドレスバーが赤色であれば、フィッシングサイトの可能性がありますので、ご注意ください。

#### 【Internet Explorer7 以降の PC ブラウザ】

アドレスバー全体の背景が緑色となり、アドレスバーの横にサイトを運営する組織名 (NTT DATA CORPORATION[JP]) と認証局 (VeriSign によって識別) が交互に表示されます。

#### 【Firefox3.6 以降の PC ブラウザ】

アドレスバーの左側が緑色になり、サイトを運営する組織名 (NTT DATA Corporation) が表示されます。

#### 【Safari4.0 以降の PC ブラウザ】

タイトルの右側が緑色になり、サイトの運営主体の組織名が表示されます。