セキュリティについて

当ウェブサイトでは、商品・サービスの拡充とともに、より安定したシステムの構築や、セキュリティの強化を推進しています。当社システムを安心してご利用いただくために、また、お客様ご自身が「金融犯罪被害」等に遭わないために、以下の点に十分にご注意くださいますようお願いいたします。

お各様の情報等を不正入手する「詐欺サイト」「詐欺メール」にご注意ください。

フィッシング

フィッシングとは、本物そっくりのウェブサイトを作成し、金融機関等のホームページを装い、お客様のパスワードや個人情報を不正に入手する詐欺行為です。たとえばウェブサイトの URL が当社の URL（www.xxxxxx.jp）及びプロバンの URL（https://projectbank.jp/）に似せてあったり、ウェブサイトのデザインや画像素材、さらには画面そのものが流用してあったり、フィッシングサイトは巧妙につくられていることが多く、注意が必要です。

なりすまし

電子メール等で差出人名を偽装したり、本物の名前を騙って文章が書かれていたりする詐欺行為です。たとえば当社の名前でお客様にご案内を送り、個人情報を聞き出そうとしたり、上記のフィッシングサイトに誘導をはかったりします。

また、メール以外でも、当社の名前で CD-ROM を配布したり、関係のないアプリケーションをダウンロードさせたり、不正な目的でソフトウエアをインストールさせようとするケースも報告されています。

通常、当社からお送りするメールはすべて、「●●●@projectbank.jp」というメールアドレスから配信されます（●●●は任意）。

ただし、送信者のメールアドレスが偽装されていることもありますので、下記の点にもご注意なさってください。

1. メールからウェブサイトにリンクがはられている場合は、リンク先のウェブサイトが正当なものであるかをご確認ください。詳細は前述の「フィッシング」をご参照ください。

スパイウエア

スパイウエアとは、お客様のパソコンに保存された情報や、パソコンの操作履歴を本人に気付かれないように収集し、第三者に送信する等の行為をおこなう不正なソフトウエアです。

スパイウエアの被害に遭わないためには

1. 不特定多数の人が使う共用 PC（たとえばインターネットカフェ等）ではログインやお取引をおこなわない。

2. セキュリティソフトを利用し、常に最新版にアップデートしておく。

3. 不審なウェブサイトの閲覧や電子メールの開封をむやみにおこなわない。また、信頼できないソフトのダウンロードやインストールもむやみにおこなわない。