

セキュリティについて

安心してご利用いただくために

長野銀行では、インターネットバンキングのサービスを提供するにあたり、お客さまに安心してご利用いただくために、情報を保護するセキュリティ対策に細心の注意を払い、以下のような方法で安全対策をとっております。

SSL128bit 暗号化方式

ネットスケープ社が開発した、インターネット上を流れるお客さまの情報を暗号化するシステムで、現時点では極めて解読が困難であるとされる方法です。当行では、お客さまの情報の送受信にこのSSL128bit 暗号化方式を採用しています。

※SSL(Secure Socket Layer)とは、ブラウザに搭載されている暗号通信機能のことで、世界各国の金融機関が採用しております。

フィッシング詐欺対策「EV SSL 証明書」

当行では、フィッシング詐欺対策として合同会社シマンテックウェブサイトセキュリティの「EV SSL 証明書」を導入し、セキュリティの強化を行っています。これにより、お客さまが対象のインターネットサービスをアクセスする際には、当行の正当なウェブサイトであることが容易にご確認いただけます。

「EV SSL証明書」の詳細については合同会社シマンテックウェブサイトセキュリティのホームページ(<https://www.verisign.co.jp/>)をご確認ください。

対応ブラウザについて

Windows XP SP2 Internet Explorer7.0 以降(Windows Vista 以降は、標準装備されています)

上記以外のバージョンのブラウザの場合はアドレスバーは緑色になりませんが、SSL暗号化通信は行われます。

確認方法について

インターネットバンキングのログイン画面で、アドレスバーが緑色に表示されていること、および運営組織名(NTT DATA CORPORATION)が表示されていることを確認し

ます。

アドレスバーが赤く表示された場合は、当行の正規のサイトではなくフィッシングサイトである可能性がありますので、ログインIDやログインパスワードの入力をしないでください。



※運営組織名の欄は、運営組織名 (NTT DATA CORPORATION) と認証組織名 (VeriSign によって認証) が交互に表示されます。

電子証明書(クライアント証明書)

お客様のお申し込みにより、当行で電子証明書を発行しお客さまの特定のパソコンにインストールしてご利用いただく方法です。電子証明書をインストールしたパソコン(1ユーザーにつき1台)以外からはご利用できなくなり、第三者による不正利用のリスクが軽減されますので、ぜひご利用ください。

ソフトウェアキーボード

ソフトウェアキーボードをご利用いただくことにより、キーボードで入力した内容を第三者が不正に取得することができなくなりますので、ぜひご利用ください。

ログイン ID(パソコン利用の場合)

インターネットバンキング利用画面に接続する(ログイン)ための ID で、お客さまのお名前に相当するものです。初回ログイン時にお客さまにお決めいただきます(ログイン ID 取得)。

本人確認のためのパスワード

取引を行うにあたって、ログインパスワード、確認用パスワード、承認パスワードを入力いただくことにより、お客さまの本人確認行うなどの本人確認方法を採用しています。

ログインパスワード

インターネットバンキング利用画面に接続(ログイン)するために必要なパスワードです。

確認用パスワード

ペイジーなどの資金移動を伴うお取引、ログイン ID の変更、メールアドレスの変更などのお取引内容をご確認いただくために必要なパスワードです。

承認パスワード

作成した振込、請求または納付データを当行に送信していただく際に入力していただくパスワードです。(一括伝送サービスをご利用する場合)

※ログイン ID、ログインパスワード、確認用パスワード、承認パスワードは操作画面でいつでも変更することができます。セキュリティ確保のため、定期的に変更することをお勧めいたします。

※ログイン ID、ログインパスワード、確認用パスワード、承認パスワードを当行所定の回数を連続または累積して誤って入力されますと、サービスの利用を停止させていただきます。

暗証番号、確認暗証番号

振込・振替を行う際に入力していただく暗証番号です。操作画面から変更することはできません。変更する場合は、支店窓口でお手続きをお願いいたします。

ワンタイムパスワード

キーホルダー大の「トークン」に表示される1回限りの使い捨てパスワードです。

※使い捨てパスワードは60秒ごとに切り替わるため、万一、パスワードを盗み取られても有効なパスワードは切り替わっているため、悪用される心配がありません。

※一度使用したワンタイムパスワードは無効となりますので、万一、フィッシングなどでワンタイムパスワードが盗まれたとしても、不正に取引されることはありません。

ログイン履歴の表示

インターネットバンキングでは、ログイン後のメインメニューに過去3回のログイン履歴が表示されますので、ログイン時に必ずご確認ください。

自動ログアウト

一定時間操作がなかった場合、自動的にログアウト(回線の切断)を行い、第三者の不正使用を防ぐよう、配慮しております。

メール通知による確認

振込・振替、一括伝送サービス、税金・各種料金の払込(ペイジー)などの資金の移動を伴うお取引、ログインID、各パスワードの変更など重要なお取引を行った場合に、初期設定で登録されたメールアドレスに受付の結果を送信いたします。