ＳＢＩさくらんぼ支店　セキュリティ対策

ＥＶ－ＳＳＬについて
お客さまのパソコンにて当行ホームページのお問い合わせ画面ならびにインターネットバンキングにアクセスすると、アドレスバーが緑色に変わり、アクセスしたサイトが当行の正規サイトであることを簡易に確認出来ます。（※現在、Internet Explorer 7.0のみ対象）
アドレスバーに表示されたURLの横に、ウェブサイトを運営する組織（Kirayaka Bank, Ltd.またはNTT DATA）とＥＶ ＳＳＬ証明書を発行した認証局名（VeriSign）が交互に表示されますので、ウェブサイトの運営組織とサーバー証明書発行認証局が一目で確認出来ます。

フィッシング対策（PhishWall）
金融機関などを装った電子メールを送信して電子メールのリンクから偽のサイトに誘導し、そこで「ログインＩＤ」や「ログインパスワード」、「住所・氏名」などの個人情報を詐欺する行為を「フィッシング詐欺」といいます。
当行が、電子メールで口座番号や暗証番号、各種パスワード等、重要なお客さまの情報をお尋ねすることはありません。
PhishWallは、株式会社セキュアブレインが提供しているフィッシング対策ソフトで、インストール・ご利用は無料となっております。
当行ホームページにお客さまがアクセスする際、ブラウザのツールバーに緑のシグナルを表示して、アクセス中の当行ホームページが本物であることを簡単にご確認いただけます。

128 ビットSSL（Secure Socket Layer）暗号化方式
SBIさくらんぼ支店では、お客さまのパソコンと当行のコンピュータ間のデータ通信について、本サービスを安心してご利用して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。

ログインID、パスワード等の管理について
「ログインID」「ログインパスワード」「確認用パスワード」は、お客さまがご本人であることを確認するための重要な情報です。これらは第三者に知られることのないように、またお忘れにならないようにご注意ください。
定期的にパスワードを変更していただくとより安全性が高まります。
「ログインID」「ログインパスワード」「確認用パスワード」はパソコンに保存しないでください。

取引のご確認
ご依頼いただいたお取引の受付確認や処理結果等の重要なご通知やご案内をスピーディに電子メールでご案内いたします。
お客さまが振込・定期預金等のお取引を実施したにもかかわらず受付確認メールを受信しない場合、またはお心当たりのない電子メールが届いた場合は「SBIさくらんぼ支店」までご連絡ください。

ワンタイムパスワードについて
従来の固定式パスワードに加え、１分ごとに自動発行される使い捨てのパスワード（ワンタイムパスワード）を使用して、お取引のたびにご本人の確認を行い取引の安全性を更に高める機能です。
インターネットバンキングご利用のお客様がパスワード自動作成用のアプリ（ソフトウェアトークン)をお客様のスマートフォンにダウンロードしていただき、インターネットバンキングご利用の際はそのアプリを起動していただくことが必要になります。
ご利用は無料ですが、ワンタイムパスワードアプリのダウンロードには別途通信料（パケット料）がかかります。

※ワンタイムパスワードの詳細については「スマートフォン・ワンタイムパスワードについて」をご覧ください。
※ワンタイムパスワードサービスに対応したスマートフォンが必要です。

リスクベース認証について
「リスクベース認証」とは、第三者のなりすましによる犯罪などの不正利用を防ぐためのセキュリティ対策です。お客様がインターネットにアクセスされるパソコン環境やネットワーク環境を分析し、普段と異なる環境からのアクセスと判断した場合に、ご本人であることを確認し、ご本人を特定するための認証機能です。
※リスクベース認証についての詳細については「リスクベース認証（合言葉認証）機能」 をご覧ください。

サービスの休止について
システムの更新・メンテナンス等により一時的にサービスを休止することがありますのであらかじめご了承ください。

画面移動および終了時
ブラウザ上の「戻る」、「進む」ボタンは使用しないでください。
SBIさくらんぼ支店では、終了時には画面上の「ログアウト」ボタンをクリックしてください。
（ブラウザ上の「バツ」ボタンはクリックしないでください。）