セキュリティについて

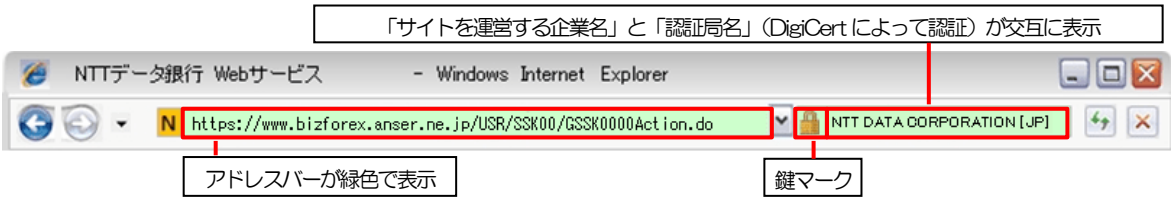
■256 ビット SSL（Secure Socket Layer）暗号化方式

NCB 外為スーパーダイレクトでは、本サービスを安心してご利用いただけるよう、お客さまのパソコンと NCB 外為スーパーダイレクトのコンピュータ間のデータ通信について、暗号化技術の 256 ビット SSL 暗号化方式を採用し、情報の漏えい・書換え等を防止します。

■EVSSL 証明書（Extended Validation）の採用

NCB 外為スーパーダイレクトでは、フィッシング詐欺への対策として EVSSL 証明書を採用し、セキュリティの強化を行っています。
EVSSL 証明書は、実在する運営者の正当なサイトであることを証明する規格で、当行の正当なサイトへアクセスするとアドレスバーが緑色で表示されます。

（Internet Explorer の場合）



※Internet Explorer 以外のブラウザをご利用の場合は、以下のとおり表示されます。

①Firefox の場合

アドレスバーの左側が緑色になり、「サイトを運営する企業名」が緑色の文字で表示されます。
また、緑色の部分にポインタを置くと認証局名が表示され、クリックすると証明書の内容が表示されます。

②Safari の場合

鍵マークの隣に「サイトを運営する企業名」が緑色の文字で表示されます。
また、「サイトを運営する企業名」をクリックすると証明書の内容が表示されます。

⚠ 注意

- アドレスバーが赤色に変わった場合は、当行に見せかけたフィッシング（不正）サイトですので絶対にログインしないようご注意ください。

■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。これらを第三者に知られること、またお忘れになることのないようご注意ください。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。

⚠ 注意

- パスワードは絶対に第三者へ教えないでください。当行職員がお客さまにパスワードをお尋ねしたり、電子メールなどでパスワードの入力をお願いしたりすることはありません。
- パスワードを第三者へ知られた、もしくは知られたと思われる場合、直ちにお客さまご自身でパスワードの変更手続きを行ってください。

>>>> パスワードの変更方法については P.162 参照

■電子証明書の採用

あらかじめお客さまのパソコンに当行が発行する電子証明書を取得・格納し、ログイン時に電子証明書、およびログインパスワードによりお客さま本人であることを確認するものです。
ID・パスワード情報が漏えいした場合でも、電子証明書が格納されたパソコンを使用しない限りサービスを利用することができないため、第三者による不正利用のリスクを軽減し、セキュリティ面の強化がはかれます。NCB 外為スーパーダイレクトでは、電子証明書の取得・格納を必須とさせていただいております。

■ソフトウェアキーボードについて

パスワード入力時に、ソフトウェアキーボードを利用することにより、キーボードの入力情報を盗みとるタイプのスパイウェアからパスワードを守ることができます。

⚠ 注意

- ソフトウェアキーボードを使用されても、スパイウェアによる被害を受ける恐れが完全に無くなるわけではありません。
- スパイウェア対応のウィルスソフトをご利用ください。また、ウィルス対策ソフトは常に最新の状態に更新し、定期的にウィルスチェックを実施していただきますようお願いします。

■取引のご確認

ご依頼いただいたお取引の受付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。
お客さまがお取引を実施したにもかかわらず電子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お取引店または当行ヘルプデスクまでご連絡ください。

■ご利用履歴の表示

ヘッダ（画面右上）に直近３回のご利用日時を表示し、不正に利用されていないかを確認できます。
ご利用日時にお心当たりのない場合は、お取引店または当行ヘルプデスクまでご連絡ください。

■タイムアウトについて

ログアウトをしないで長時間席を離れた場合のセキュリティ対策として、最後の操作から一定時間が経過すると操作が継続できなくなる設定を行っています。
操作が継続できなくなった場合は、一度ログイン画面に戻ってから再度ログインしてください。
また、NCB 外為スーパーダイレクトを終了する際に、ブラウザの「×（閉じる）」ボタンを使用すると一定時間利用ができなくなりますので、必ず「ログアウト」ボタンをクリックしてください。