セキュリティ

〈OK メイト・WEB〉では、インターネット上での情報の盗聴、データの偽造や改ざん、第三者の不正使用などを防ぐため、万全なセキュリティ対策を実施しています。

■128 ビット SSL 暗号化通信を採用

SSL（Secure Socket Layer）とは、インターネット上を流れるお客さまの情報を、お客さまのパソコンのブラウザと OKB のコンピュータの間で暗号化する仕組みです。

〈OK メイト・WEB〉で採用している 128 ビット SSL により暗号化された情報は、2 の 128 乗通りの符号を組み合わせてできています。

■厳重な本人確認

○サービス利用の際には、各種パスワード・暗証番号により契約者ご本人であることを確認しています。

○各種パスワード・暗証番号を一定回数誤って入力すると、サービス利用をいったん停止します。

○ログインパスワードなどはインターネット上で変更可能です。セキュリティ確保のため、90 日間パスワードの変更がない場合にはお知らせします。

■ワンタイムパスワード

都度振込・振替の操作時などに、ハードトークンに表示されるワンタイムパスワードを入力して本人認証を行うセキュリティの高い認証方式です。万が一、ログイン ID、ログインパスワードなどを第三者に取得された場合でも、ワンタイムパスワードはお客さまにしかわからないため、第三者による不正な預金の引き出しなどを防止することができます。

■電子証明書方式による本人認証

電子証明書とは、電子的な身分証明書です。電子証明書がインストールされている端末（パソコン）からのみにアクセスを制限し、第三者による不正使用のリスクを軽減します。

■不正送金対策ソフト（PhishWall プレミアム）

OKB ホームページやインターネットバンキングにアクセスした際、ブラウザのツールバーやシステムトレイにシグナルが表示され、真正な Web サイトであることを確認できるようになります。

また、インターネットバンキングの利用中に不正な偽画面などを表示させることによって認証情報などを盗み取る攻撃を検知した場合は、警告画面を表示し、お客さまにお知らせします。

・動作環境やパソコンの設定方法、インストール方法などについては OKB ホームページをご覧ください。

■利用履歴の表示

過去の直近 3 回までのログイン日時をトップ画面に表示しますので、ログイン履歴をチェックできます。

■電子メールによるご連絡

総合振込、給与振込、地方税納入のデータ確定依頼、または承認、振込振替のお取引、パスワードなどの登録情報を変更される都度、電子メールでご連絡します。

■ソフトウェアキーボード

スパイウェア対策として画面上に「ソフトウェアキーボード」を表示しています。ソフトウェアキーボードのご利用により、スパイウェアによる各種パスワード・暗証番号の情報盗用を防止します。

■電子署名付きメールによるご連絡

〈OK メイト・WEB〉で OKB からお送りする電子メールには、電子署名を付与しています。電子署名を付与することで、以下の点を確認できるため、有効な「フィッシング詐欺」対策となります。

・電子メールの送信者が「大垣共立銀行」である。

・電子メールの内容が途中で改ざんされていない。

■システム構成・監視体制

〈OK メイト・WEB〉では、複数のファイアーウォールを設け、インターネットからの不正なアクセスを防いでいます。

インターネットからの攻撃を常時監視し、不測の事態に備えています。

■EV SSL 証明書の採用

Internet Explorer7.0 以降を使用して、〈OK メイト・WEB〉の取引画面にアクセスすると、アドレスバーが緑色に変わります。さらに、アドレスバーの横に Web サイトを運営している組織名として NTT DATACORPORATION[JP]（株式会社 NTT データ）と、証明書を発行した認証局名として VeriSign（日本ベリサイン株式会社）が表示されます。アドレスバーが緑色に変化するということは、Web サイトを運営している組織の実在性を第三者認証局が検証し、その上で証明書が正式に発行されたことを意味します。

・〈OK メイト・WEB〉は、株式会社 NTT データが運営するサービスを利用しています。