

「ちば興銀コスモス WEB」セキュリティについて

ちば興銀コスモス WEB サービスでは、本サービスを安心してご利用いただけるよう、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、以下の対策を実施しています。

128 ビット SSL (Secure Socket Layer) 暗号化通信方式の採用

SSL とは、ネットスケープ社が開発した、インターネット回線を通るお客様の情報を、お客様のパソコンのブラウザと当行のサーバーの間で暗号化する仕組みです。現在、最もセキュリティ度の高い暗号化技術である米国ベリサイン社による 128 ビット暗号化システムによりお客様の情報を保護しています。これによって暗号化された情報は、2 の 128 乗通りの符合を組み合わせてできていますので、現時点で、解読はほとんど不可能とされています。

※記載されている会社名・製品名は各社の商標または登録商標です。

厳重な本人確認

- ・ 申込書により、ご契約いただいた印鑑を照合しています。
- ・ サービス利用の際には、パスワード等により契約者ご本人であることを確認しています。
- ・ パスワード等を複数回誤って入力された場合、サービスのご利用を一定時間停止いたします。

ご利用履歴の表示

過去の直近 3 回までのログイン日時をメインメニュー画面に表示しますので、ログイン履歴を確認いただけます。

自動ログアウト

ログインしたまま一定の時間内に操作がない場合、自動的にログアウトし、お取引を終了いたします。

※お客様以外の第三者の利用を防ぐため、ログイン中にパソコンから離れないでください。

パスワード変更通知

各種パスワードは、60 日間変更がない場合、ログインされたときにお知らせいたします。

ご確認電子メールの送信

総合振込等のデータの確定依頼・承認、振込・振替のお取引、パスワード等の登録情報を変更される都度、電子メールにてご連絡いたします。

なお、当行から電子メール等でパスワード等をお客さまにおたずねすることは一切ありません。

※取引内容に心当たりのない場合は、すぐに、当行までご連絡ください。

システム監視体制

インターネットから銀行のコンピュータへの不正なアクセスを防止するため、ファイアーウォールを設けています。

お客さまへのお願い事項

- ・当行では、お客さまがインターネットバンキングをご利用になるパソコンを特定する「電子証明書ログイン方式」の導入をお勧めしております。現在「ID・パスワードログイン方式」をご利用されている方につきましては、よりセキュリティの高い「電子証明書ログイン方式」への切替えをご検討ください。
- ・パスワード等は契約者ご本人を確認させていただくために大変重要なものです。必ず契約者ご本人が責任をもって管理し、他人に内容を知られないようご注意ください。
- ・パスワード等は定期的に変更することをお勧めします。
- ・ちば興銀コスモス WEB サービスのご利用は、契約者ご本人が管理するパソコンを使用してください。第三者が不正な装置等を取り付けている可能性のあるパソコンでのご利用はおやめください。
- ・ちば興銀コスモス WEB の、ご利用を開始する前にウィルスチェックソフト等の組み込みをお勧めします。また、ご利用に際し不審な電子メールを開封しないようにしてください。

ソフトウェアキーボード入力機能

従来のログイン ID パスワードに加え、お取引実行時等に入力する確認暗証番号の入力時にも利用が可能となり、これまで以上に安全なインターネットバンキングをご利用いただけます。

(1)ログインパスワードの入力画面および確認用暗証番号の入力画面に表示される“ソフトウェアキーボードを開く”というリンクボタンをクリック。

The screenshot shows a login page titled "ログイン" (Login) with the ID "BL0001". It contains two main sections:

- 電子証明書方式のお客様** (Electronic Certificate Method): Includes a "電子証明書ログイン" (Electronic Certificate Login) button and a "電子証明書発行" (Electronic Certificate Issuance) button. A note below states: "証明書を取得されていない方、もしくは証明書を再取得される方は、「電子証明書発行」ボタンより証明書の発行を行ってください。" (For those who have not obtained a certificate or need to re-obtain one, please use the 'Electronic Certificate Issuance' button to issue the certificate.)
- ID・パスワード方式のお客様** (ID/Password Method): Includes input fields for "ログインID" (Login ID) and "ログインパスワード" (Login Password). A link "ソフトウェアキーボードを開く" (Open Software Keyboard) is located next to the password field and is circled in black. A "ログイン" (Login) button is at the bottom.

(2)画面上にキーボード画面が開き、文字をクリックしパスワード等をマウスで入力。

The screenshot shows a software keyboard interface titled "ソフトウェアキーボード" (Software Keyboard) with the ID "0504204". It features:

- A "ログインパスワード" (Login Password) input field with "戻る" (Back) and "次へ" (Next) buttons.
- A numeric keypad (数字) with digits 0-9 and a decimal point.
- A QWERTY keyboard (英字 (小文字)) for lowercase letters.
- A numeric keypad (英字 (大文字)) for uppercase letters.
- Buttons for "閉じる" (Close) and "決定" (Enter/Confirm).

セキュリティ対策ソフト

当行では、「ちば興銀コスモス WEB」、「ちば興銀コスモス外為 WEB」を安全にご利用いただくために無料のセキュリティソフト「saat netizen」および「PhishWall プレミアム」を提供しています。

セキュリティソフトをインストールいただき、是非ともご利用ください。

※「saat netizen」をインストールしている場合、当行のホームページをご利用の間、「netizen」が対応しているウイルスについて常に最新の状態でチェックし、ウイルスが発見された場合には駆除いたします。

【ご利用に関する注意事項】

・ご利用には、ソフトウェアのインストールが必要です。

※本ソフトはお客様がお使いのパソコン環境によっては、ご利用いただけない場合がございますのであらかじめご了承ください。

※他社のセキュリティ製品がインストールされているパソコンでもご利用が可能です。ただし、他社のセキュリティ製品との相性によっては、正常に作動しないこともございます。

・本サービスは、当行のホームページを立ち上げた場合に自動的に起動し、ホームページを閉じると自動的に終了します。

※手動起動をご希望の場合は、タスクトレイメニューより「自動的に起動する」を無効にしてご利用ください。

・本サービスはウィルスからの脅威を全て防ぐことを保証するものではありません。

・安全にインターネットをご利用いただくためにはお客様自ら十分なセキュリティ対策を行っていただきますようお願いいたします。

●本サービスに関するお問い合わせは「 saat (サート) サポートセンター」までお問い合わせください。本サービスの問い合わせは、お取引店およびちば興銀 EB サービスセンターではお受けしておりません。

「 saat (サート) サポートセンター」

電話 : 03-3570-5286 (通話料はお客様負担)

受付時間 月～金曜日 8 : 00～22 : 00

土～日曜日 8 : 00～19 : 00

※祝日、年末年始 (12/29～翌 1/3 は休業となります)

※「Phishwall (フィッシュウォール) プレミアム」は、フィッシング・不正なポップアップなどでログイン ID やパスワードを盗む MITB 攻撃 (マン・イン・ザ・ブラウザ) 対策ソフトです。「PhishWall プレミアム」をお客様のパソコンにインストールしている場合、お客様がアクセスしたウェブサイトが偽装されていないか確認を行い、真正なサイトである場合は、ブラウザのツールバー (画面左上) に緑色の信号が点灯し、アクセスしているウェブサイトが本物であることが確認できます。(利用料金は無料です) また、不正にポップアップ画面を表示させてパスワードなどを盗み取ろうとする MITB 攻撃型ウィルスに感染している場合、警告メッセージを表示して不正な画面への入力を防ぐことができます。

【ご利用に関する注意事項】

・ご利用には、ソフトウェアのインストールが必要です。

※本ソフトはお客さまがお使いのパソコン環境によっては、ご利用いただけない場合がございますのであらかじめご了承ください。

※他社のセキュリティ製品がインストールされているパソコンでもご利用が可能です。ただし、他社のセキュリティ製品との相性によっては、正常に作動しないこともございます。

※本サービスはウィルスからの脅威を全て防ぐことを保証するものではありません。安全にインターネットをご利用いただくためにはお客さま自ら十分なセキュリティ対策を行っていただきますようお願いいたします。

●本サービスに関するお問い合わせは、「セキュアブレインテクニカルサポートセンター」までお問い合わせください。本サービスの問い合わせは、お取引店およびちば興銀 EB サービスセンターではお受けしておりません。

フリーダイヤル：0120-988-131

受付時間 月～金曜日 9：00～12：00、13：00～17：00

※土日祝日、年末年始（12/29～翌1/4は休業となります）

ワンタイムパスワード

一度だけ有効な使い捨てのパスワードで、60秒ごとに変更されます。万一、パソコンがウイルスに感染し、ID・パスワード等が盗まれた場合でも、ワンタイムパスワードを表示する機器までも盗むことは難しいため、不正取引の防止に有効です。ワンタイムパスワードをご利用になる場合には、ソフトウェアトークンまたはハードウェアトークンのどちらかをお選びいただき、お申込が必要になります。

(1) ソフトウェアトークン

スマートフォンまたは携帯電話に専用アプリをダウンロードして、ワンタイムパスワードを表示させる仕組みです。1台のスマートフォンで複数のユーザ様にご利用できます。1台の携帯電話では1名のユーザ様のご利用となります。

お申込につきましては、[こちら](#)の申込書にご記入のうえ、お取引店にご提出ください。

ソフトウェアトークンにご利用可能な携帯電話の機種は[こちら](#)をご覧ください。また、ご利用可能なスマートフォンの機種は[こちら](#)をご覧ください。

(2) ハードウェアトークン

キーホルダー型のワンタイムパスワード生成機で、液晶画面にワンタイムパスワードが表示されます。1つのハードウェアトークンで、複数のユーザ様にご利用できます。

お申込につきましては、[こちら](#)の申込書にご記入のうえ、お取引店にご提出ください。

二経路認証

都度指定方式の振込・振替取引を実施する際に、パソコン（第一経路）で取引データを作成し、スマートフォン（第二経路）で承認を行うことで取引を成立させる認証方式です。

仮にパソコンがウイルスに感染して取引内容が改ざんされた場合でも、別ルート（スマートフォン）で取引内容確認、承認を行うため、不正取引に気付くことができます。

お申込につきましては、[こちら](#)の申込書にご記入のうえ、お取引店にご提出ください。

二経路認証にご利用可能なスマートフォンの機種は[こちら](#)をご覧ください。