安心してお取引いただくために

セキュリティ対策一覧

項　　目	セキュリティ対策・ご注意
キャッシュカードの被害防止対策	**・キャッシュカードご利用限度額の変更** お客さまのご希望に応じて、１日あたりのご利用限度額の範囲で任意に変更していただけます。 **・暗証番号の変更** 簡単な画面操作により、ＡＴＭでキャッシュカードの暗証番号を変更していただけます。 **・生体認証機能を搭載したＩＣキャッシュカードの発行** 一人ひとり異なる「指静脈」パターンでご本人を確認する生体認証機能により、厳格な本人認証ができる「ＩＣキャッシュカード」および「バンクカードＶｉｓａ」をご希望により発行しております。 **・その他の対策** キャッシュカード・通帳等の紛失や盗難に遭われた場合のお届けおよびキャッシュカードのご利用停止の受付は24時間体制で対応しておりますので、出来る限りすみやかに当行までご連絡ください。
インターネットバンキングの被害防止対策	**（個人のお客さま・法人のお客さま共通）** **・EV SSL証明書** フィッシング詐欺等への対策として、インターネットバンキングをご利用のお客さまが、現在閲覧しているウェブサイトが正当なウェブサイトかどうかを簡単にご確認いただけます。 **・振込限度額変更** お振込の上限金額を設定していただけます。 **・電子メールによる取引通知** お取引の確認メールを送信します。 お振込・お振替等の取引を行われた場合は、お届けいただいているメールアドレスに、ご依頼内容の確認メールを送信いたします。 **・ソフトウェアキーボード** パソコンの画面上にキーボードを表示して、マウスで各種パスワード・暗証番号を入力することにより、キーボードで入力した情報を盗み取るキーロガーを防ぎます。 **・ワンタイムパスワード** 1分毎に変化する1回限りで無効となる使い捨てのパスワードです。 ログインID（または電子証明書※法人のお客さまのみ）、ログインパスワードに加え、スマートフォン、携帯電話に表示されるパスワードを入力して本人確認を行います。 法人のお客さまは二経路認証のご利用が必須となります。 **・セキュリティ対策ソフト「ＳａＡＴ Netizen（サート・ネチズン）」** 但馬銀行のホームページやインターネットバンキングをご利用いただいている間、マルウェアやウイルスの活動等を監視し、必要に応じて検知･駆除･遮断を行うセキュリティソフトです。当行ホームページより無料でインストールいただけます。 **（個人のお客さま）** **・追加認証（合言葉認証）** 第三者のなりすましによる不正なログインを防止するセキュリティ対策です。 通常とは異なるご利用環境であると判断した場合等に、ご本人さまのご利用であることを確認するため、「合言葉」による追加認証を行います。 **・メール通知パスワード・取引認証パスワード** 振込・振替等の取引時に、お客さまにご登録いただいたメールアドレスに、取引の都度、取引の内容とパスワードを記載したメールを送信します。 取引内容を確認できるとともに、通知されたパスワードを確認用パスワードに加えて入力することにより第三者に不正利用されることを防ぎます。 **・IBロック** 携帯電話から利用停止を設定することで、パソコンからの利用を制御し、第三者に不正利用されることを防ぎます。 **・ログイン緊急利用停止** 第三者による不正利用等のおそれがある場合に、お客さまご自身でインターネットバンキングの利用を停止できます。 **（法人のお客さま）** **・電子証明書** お客さまのパソコンに当行が発行する電子証明書をインストールしていただくことにより、ご利用のパソコンを特定したうえでパスワードによる本人確認を行いますので、第三者による不正使用の防止等セキュリティ強化が図れます。 **・二経路認証** 都度指定方式の振込・振替を実施する際に、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。 仮にウイルス等に感染し、不正な振込操作をされた場合でも、別経路での承認取引が必要となるため、不正な取引を防ぐことができます。 ※二経路認証をご利用の場合は、ワンタイムパスワードの利用が必須となります。
被害防止のためのご注意	**・警察官などを騙ってキャッシュカードをだまし取り預金を引き出す詐欺についてのご注意** 百貨店の社員や警察官などを騙って電話をかけ、キャッシュカードの暗証番号を聞き出し、キャッシュカードをだまし取り預金を引き出す犯罪（カード手交型）や、封筒にキャッシュカードを入れさせ、隙を見て別の封筒にすり替えてキャッシュカードを盗みとる犯罪（カードすり替え型）が全国で発生していますので、十分にご注意ください。 銀行協会職員や銀行員、警察官などが電話で暗証番号をお尋ねしたり、キャッシュカードをお預かりすることはありません。 **・キャッシュカード暗証番号についてのご注意** キャッシュカードの暗証番号は、他人から類推されやすい番号の利用はお避けいただくとともに、現在類推されやすい番号をご利用のお客さまは、すみやかにATMで変更されることをお勧めします。 また、暗証番号をキャッシュカードに書き込んだり、手帳やメモ等に記入してカードと共に保管・携帯しないようにしてください。 なお、暗証番号を誤入力された場合、当行所定の回数に達した時点で当該キャッシュカードは使用できなくなりますので、ご注意ください。 **・フィッシング詐欺についてのご注意** 金融機関や運送会社等を装い、ファイルを添付したメールを送信しウイルスに感染させたり、偽の画面を表示し、ＩＤやパスワード等の重要情報を入力させるなどのフィッシング詐欺が急増しております。 お心当たりのない電子メールを開封されたり、不審な画面にＩＤやパスワード等を入力されないようご注意ください。 当行では、電子メールによりＩＤやパスワード、暗証番号などの重要情報をお尋ねすることは一切ありません。 **・マルウェアについてのご注意** マルウェアの侵入を防ぐため、みだりにフリー・ソフトをダウンロードしたり、心当たりのない先からの電子メールを不用意に開封したりされないようご注意ください。 マルウェア対応のセキュリティ対策ソフトをご利用され、常に最新の状態にされることをお勧めします。 なお、各種パスワード・暗証番号はできるだけ「ソフトウェアキーボード」を用いてマウスで入力してください。 **・パソコンのご利用についてのご注意** ご使用のパソコンのＯＳ、ブラウザやマルウェア対応のセキュリティ対策ソフトは、常に最新の状態に更新されることをお勧めします。