Miyazaki Taiyo Bank

# 宮崎太陽銀行ダイレクトセキュリティ対策のご案内

宮崎太陽銀行のセキュリティ対策の中には、お客さまご自身がご活用いただくことで
より高いセキュリティを確保できるサービス機能がありますので、是非ご活用ください。

## セキュリティの高い『本人認証方式』で、第三者による不正利用を防止します

### ワンタイムパスワード

1分毎に更新する使い捨てのパスワードで、一度使用したパスワードは再利用できないため安全性が高い認証方式です。ログインの際、固定の本人認証情報（ログインID、ログインパスワード）に加えて使用します。


ワンタイムパスワードはスマートフォンまたは携帯電話にダウンロードした「トークンアプリ（※）」で生成・表示される使い捨てのパスワードです。
パスワードは1分ごとに更新されるため、不正利用を防ぐ仕組みとして有効です。

※トークンアプリ:ワンタイムパスワードを生成・表示するプログラムのこと。


### ワンタイムパスワードを推奨しています!

当行は不正送金を防止するため、「ワンタイムパスワード」のご利用を強くお勧めしています。
振込や、お客さま情報の更新などの重要なお取引には、ワンタイムパスワードが必須です。

**⚠注意** ワンタイムパスワードを利用しない場合は振込手続きや税金・各種料金払い込み手続きが出来ません。

## 『EV SSL証明書』で当行の正当なサイトを容易に確認できます


## 『ソフトウェアキーボード』でスパイウェア対策を実施しています

取引操作画面上に表示されたキーボードをマウスでクリックすることでパスワード等を入力することができます。
この場合、入力情報がパソコン上に残らないため、キーボードの入力情報を不正に取得しようとするキーロガータイプの「スパイウェア」に対する有効な対策となります。


## 『128bitSSL』による情報暗号化で情報の送受信を守ります

インターネットでの情報の漏洩、盗聴、データの偽造・改ざんを防ぐため、お客さまの情報の送受信に128bitSSL（Secure Socket Layer）による暗号化方式を採用しています。


## 不正送金対策ソフト「PhishWallプレミアム」をご利用ください

不正送金・フィッシングの脅威からお客さまを守る、無料のセキュリティソフトウェアで、他社のセキュリティ製品とも一緒に使えます。当行のホームページより入手できます。

【「PhishWallプレミアム」に関するお問い合わせ】
株式会社日立システムズ セキュアブレイン テクニカルサポートセンター

電話番号:0120-988-131（通話料無料）
※ダイヤル後、アナウンスに従いお使いいただいている製品の番号を押してください。
※営業時間:月～金曜日 9:00～12:00 13:00～18:00（土日祝祭日・年末年始（12/29～1/4）を除く）
メール:tech.support.fn@hitachi-systems.com
※製品名、ご利用のOSを記載のうえ、ご連絡くださいますようお願いします。

## ログイン画面URLのご案内

「宮崎太陽ダイレクト」にログインされる際、お客さまの端末設定環境や当行ホームページ（サイト）の影響等で【ログイン】ボタンからログイン画面を表示できない事象が発生した場合は、下記URLから直接ログイン画面を表示し、ログインを行ってください。

https://www.parasol.anser.ne.jp/ib/index.do?PT=BS&CCT0080=0591

当行が加盟する「全国銀行協会」では、金融犯罪を防止するため、専用のセキュリティ対策の啓蒙サイトがあります。
金融犯罪の概要・手口・防止策・事例等が詳しく解説されておりますので、是非ご覧ください。

検索キーワード 〉 金融犯罪の手口


お問い合わせ先

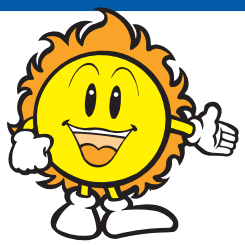
●宮崎太陽銀行EBサポートセンター
【受付時間】銀行営業日9:00～17:00
0120-47-3456
WEB https://www.taiyobank.co.jp

●時間外の不正取引に係るサービス利用停止依頼窓口
ATMセンター 0985-23-1168
※「サービス利用停止依頼」以外のお問い合わせには対応できませんので、あらかじめご了承ください。

宮崎太陽銀行

2025年3月現在

# 『宮崎太陽ダイレクト』を安全にご利用いただくために



宮崎太陽銀行では、『宮崎太陽ダイレクト』を、お客さまに安心してお使いいただくために、さまざまなセキュリティ対策を実施しております。

**当行がご提供いたしますセキュリティ対策を積極的にご活用いただくとともに、お客さまご自身でも下記のようなセキュリティ対策を万全に実施いただきますようお願いいたします。**

## 当行からお客さまへのお願い

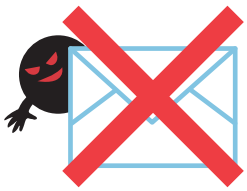
### ご利用の端末に関するお願い

- **市販のウィルス対策ソフト**を導入するとともに、常に**最新の状態に更新**し、定期的にパソコン・スマートフォンをチェック（スキャン）してください。


- パソコン・スマートフォンのOSやブラウザ等を**最新の状態に更新**してください。
- メーカーの**サポート期間が経過したOSやブラウザ、セキュリティ対策ソフト**は絶対に**使用しない**でください。
- インターネットカフェ、図書館、ホテルなど**不特定多数の人が利用するパソコン**でのご利用はお止めください。

※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避けていただき、ご自身で管理するパソコンを利用してください。

- お心当たりのない電子メールの**添付ファイル**は**開かない**ようにしてください。



- **不自然なフリーソフト**のダウンロード、**不審なWebサイト**へはアクセスしないでください。
- インターネット・バンキングに使用する**パソコンや無線LANルータ**などは利用時以外は**可能な限り電源を切断**するようにしてください。

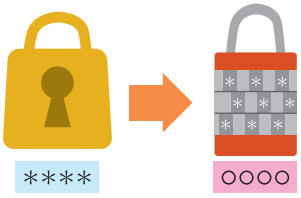
### パスワード管理に関するお願い

- パスワード類は**厳重に管理**してください。

※メモやパソコンのファイル、メール等に保存することは、避けてください。

- パスワード類は**定期的に変更**してください。

※変更がないまま1年が経過すると、パスワード変更画面が自動的に表示されます。




- **他人に類推される恐れのあるパスワード類**の登録は避けてください。

※生年月日、電話番号、勤務先の電話番号、自宅の住所・番地、自動車ナンバー、同一数字、連続数字等

- パスワード類は他人に**絶対に教えない**でください。

※当行行員であっても、お客さまにパスワード類をお尋ねすることはございません。


- **電子メールのリンク先**で、安易にパスワード等を**入力しない**ようご注意ください。

※当行がお送りする電子メールで、サービスのご案内、セキュリティ対策のため等と称して直接お客さまにパスワード等の入力をお願いすることは一切ございません。


### サービスご利用に関するお願い

- **振込限度額**は必要な範囲内で**低く設定**してください。

※万が一、ウィルスに感染した場合にも、被害を最小限に抑えることができるようにしてください。
※サービス画面上で変更することができます。変更後の振込限度額は引き上げの場合4日後、引き下げの場合即時で適用されます。


- **ログイン履歴**や**入出金明細**をご確認ください。

※定期的にログインしていただき、ログイン履歴や入出金明細をご確認ください。
※ログイン後のトップページには、ログイン履歴が表示されていますので、ログインの際に確認してください。
※身に覚えのないログインやお取引を確認した場合は、すみやかにEBサポートセンターまでご連絡ください。


- 各種取引後の**メール通知**をご確認ください。

※振込・振替のご依頼や登録情報のご変更等を行われた場合は、電子メールにて受付結果をお知らせいたします。
※万が一、身に覚えのない取引のメール通知があった場合は、すみやかにEBサポートセンターまでご連絡ください。
※また、各種取引後にメール通知が受信できない場合には登録誤り等が考えられますので、ご確認ください。
※フリーメールアドレス（無料でメールアカウントを取得できるアドレス）は第三者に悪用されてしまう可能性がありますので、フリーメールアドレスでのご登録を避け、スマートフォンのメールアドレスをご登録ください。