



インターネットバンキングをより安全にご利用いただくために

インターネットバンキングによる金融被害に遭わないためには日頃のセキュリティ対策が重要です。

被害に遭わないためには…

1 ウイルス対策ソフトをご利用ください

- 最新の状態に更新したウイルス対策ソフトでウイルスチェックを行ったうえで、インターネットバンキングをご利用ください。また、パソコン起動時にはウイルス対策ソフトのスキャン機能でパソコン内をチェックしてからご使用になることをお勧めします。
- OSやブラウザの更新を行い最新の状態でご利用ください。
(ひろぎん)では無料でご使用いただけるセキュリティツールを提供していますのでご利用ください。

無料で提供している
セキュリティツール

[スマートフォン用]

- セキュリティ機能付「ひろぎんアプリ」

[パソコン用]

- ウイルス対策セキュリティツール「SaAT Netizen(サートネチズン)」
- フィッシング対策ツール「Phish Wall(フィッシュウォール)プレミアム」

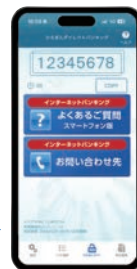
詳しくはP.5をご覧ください

2 ワンタイムパスワードをご利用ください

インターネットバンキングで、お振込、税金・各種料金払込み(Pay-easy(ペイジー)) (民間払込)、自動送金、組戻、振込先口座登録(事前登録)、振込限度額変更、オンライン入金、住所変更・電話番号変更のお取引の際は、アプリ上で取引内容を確認する取引認証(トランザクション認証)または、60秒ごとに更新されるワンタイムパスワードを必須としています。
(ご利用手数料は無料で、ご希望の場合はインターネットバンキングからお申込みいただけます。お申込時に「パスワード生成アプリ」と「パスワード生成機」の2種類からご選択ください。)



↑パスワード生成機
(キーホルダー型/約6cm)



パスワード生成アプリ→
(スマートフォン)

3 振込限度額の引下げをご検討ください

振込限度額を必要最低限に設定することで、被害額を最小限に抑えることができます。必要以上に高額に設定しないことをお勧めします。(振込限度額の引下げは、店頭もしくはインターネットバンキングでお手続きいただけます。)

4 当行からお送りする電子メールをご確認ください

(ひろぎん)ダイレクトバンキングサービスでは、お振込等の取引、またパスワード、メールアドレスの変更の都度、電子メールでお知らせする仕組みとなっております。

ご登録の電子メールアドレスは、すぐにご確認いただけるスマートフォンの電子メールアドレスをご登録ください。

フリーメール(無料でアカウントが取得できる電子メールサービス)は、ID・パスワードを不正に利用される可能性も高いため、ご登録されないようお願いいたします。

スマートフォンからは「ひろぎんアプリ」をご利用ください



●ひろぎんアプリはセキュリティチェックが自動的に実行され、お持ちのスマートフォン端末が安全な環境にあるかどうか簡単にチェックできるセキュリティ機能を備えたアプリです。

※ご利用の端末によって、ご利用いただけない場合やOSのアップデート等が必要となる場合がありますので、あらかじめご了承ください。

ご利用方法



〈ひろぎん〉が提供するパソコン用セキュリティツール(無償)

ウイルス対策ツール「SaAT Netizen(サートネチズン)」

(提供:ネットムーブ社)

- 「SaAT Netizen(サートネチズン)」は不正送金やウイルスからパソコンを守る、無料のセキュリティツールです。
- 当行のインターネットバンキングやホームページをご利用いただいている間、スパイウェアの侵入やウイルス活動等を監視し、必要に応じ検知・駆除・遮断を行います。(セキュリティの観点から、一部機能については、パソコン起動とともに有効となります)

〈主な機能〉

- ・プロセス監視: プロセスを監視し、動作中およびシステムにアクセスするウイルスをリアルタイムで検知・駆除します。
 - ・システムスキャナー: パソコン内部に潜伏するウイルスを検知・駆除します。
 - ・不正実行遮断: ブラウザの脆弱性を利用したウイルスの事項を事前に検知し遮断します。
- その他の機能および詳細は〈ひろぎん〉ホームページの「SaAT Netizen(サートネチズン)」専用サイトでご確認ください。



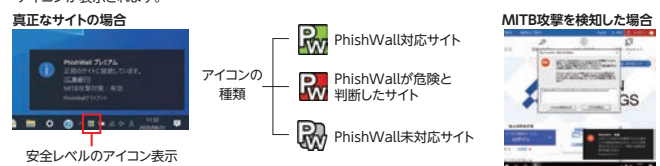
フィッシング詐欺対策・MITB攻撃対策ツール「Phish Wall(フィッシュウォール)プレミアム」

(提供:日立システムズ社)

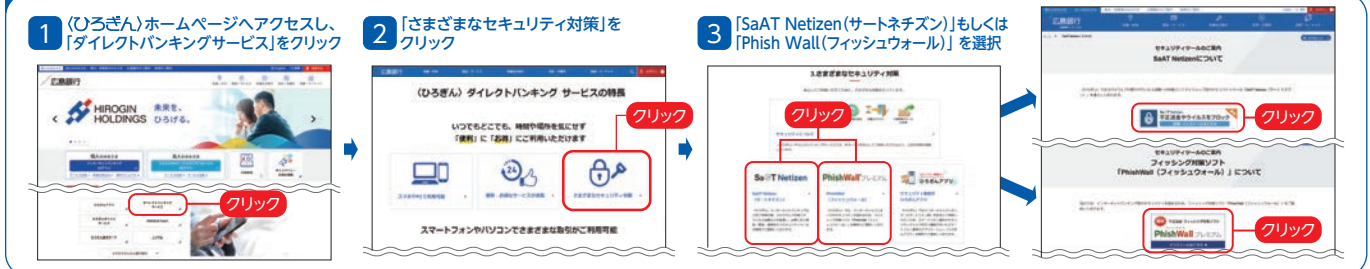
- 「Phish Wallプレミアム」は、アクセスしているサイトが安全(正当な〈ひろぎん〉のサイト)であることを一目で確認できるセキュリティツールです。
- フィッシング詐欺(金融機関を装った偽のメールに記載のあるURLリンクをクリックさせ偽のウェブサイトに誘導し、パスワードや暗証番号を入力させ情報を搾取る犯罪)やMITB [マン・イン・ザ・ブラウザ] 攻撃(不正にポップアップ画面を表示させてパスワードを盗み取ろうとする犯罪)に有効です。

Phish Wall(フィッシュウォール)通知領域への表示(例)

PhishWall(フィッシュウォール)プレミアムをインストールすると、システムトレイ(通知領域)へ以下のようなアイコンが表示されます。



ダウンロード方法



お問い合わせ先

SaAT Netizen(サートネチズン)について

サート・サポートセンター ネットズン専用窓口 【受付時間】 月～金曜日 8:00～22:00、土・日曜日 8:00～19:00
TEL 0120-987-903 ※祝休日、年末年始(12/29～翌1/3)は休業となります。
 携帯電話・PHSから、もしくは上記電話がつながりにくい場合は**03-3570-5286**

Phish Wall(フィッシュウォール)プレミアムについて

セキュアブライン テクニカルサポートセンター 【受付時間】 月～金曜日 9:00～12:00、13:00～18:00
TEL 0120-988-131 ※土・日・祝休日、年末年始(12/29～翌1/4)は休業となります。