筑波銀行 NEWS RELEASE

平成 30 年 3 月 30 日

スマートフォン向けアプリ「Ｓｅｃｕｒｅ　Ｓｔａｒｔｅｒ」バージョンアップのお知らせ

～生体認証でつくばインターネットバンキングのログオンが簡単に！！～

筑波銀行（頭取：藤川　雅海、本店：茨城県土浦市）は、スマートフォン向けアプリ「Ｓｅｃｕｒｅ Ｓｔａｒｔｅｒ（セキュアスターター)」のバージョンアップを行ないましたので、お知らせいたします。

バージョンアップ後のアプリは、各アプリストアにて順次アップデート可能となります。アップデート後は、スマートフォンに搭載されている生体認証機能等を利用した「かんたんログオン機能」をご利用いただけるようになります。これによって、つくばインターネットバンキングのご利用が更に安全・簡単・便利になります。

当行は今後も、お客さまが最初に相談したい銀行「Ｆｉｒｓｔ　Ｃａｌｌ　Ｂａｎｋ（ファースト・コール・バンク)」の実現に向け、顧客保護（セキュリティ）を確保する観点を踏まえながら、お客さま第一主義、お客さまのライフスタイルに寄り添ったサービスが提供できるよう取り組んでまいります。

記

１．ご利用開始可能日

平成３０年３月３０日（金）

※順次、各アプリストアにてアップデート可能となります。(Google Play/App Store)

２．「かんたんログオン機能」の概要

契約者番号およびログオンパスワードを都度入力せずに指紋認証や顔認証のみでインターネットバンキングへのログオンが完了します。

※契約者番号およびログオンパスワードの初期登録が必要です。

※「かんたんログオン機能」は、スマートフォンに搭載されている端末（画面）ロックのセキュアな認証方式を利用しています。利用可能な認証方式はご利用のスマートフォンによって異なります。

３．「Ｓｅｃｕｒｅ　Ｓｔａｒｔｅｒ」のセキュリティ機能（従来の提供機能）

機能	内容
「端末初期化警告」	ＯＳの不正利用の問題を検知した場合に表示されます。
「悪性コード検知警告」	ウイルスなどの悪性コードが混入した、不正アプリを検知した場合に表示されます。（Ａｎｄｒｏｉｄ ＯＳ）
「ＤＮＳチェック警告」	アクセス先の情報に問題を検知した場合に表示されます。
「Ｗｉ－Ｆｉ接続警告」	インターネットバンキングなどへのアクセス時、Ｗｉ－Ｆｉネットワークに接続している場合に表示されます。

※上記のセキュリティ機能は引き続き提供されます。対応方法など、詳細はアプリの紹介ページをご覧ください。【https://web.saat.jp/s-starter/tsukubabank/】

以　上

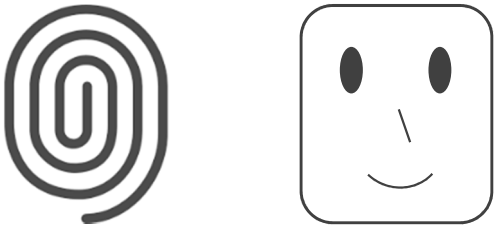
報道機関のお問合せ先
筑波銀行　　総合企画部広報室　　鴨志田　　内線3730
℡　029－859－8111

スマートフォン専用無料アプリ「Secure Starter」

つくばインターネットバンキングの

ログオンを生体認証で

指紋認証　　顔認証



セキュアに！簡単に！

※画像はiOSのサンプルイメージです。実際のものとは異なる場合があります。　2018/3/30時点

アプリＴＯＰ画面のイメージ

2018/3/30時点

旧

「Secure Starter」紹介Webページ

↓

【https://web.saat.jp/s-starter/tsukubabank/】

または、当行ホームページ(スマホ用)の下段にある
リンクバナーからアクセスしてください。

新

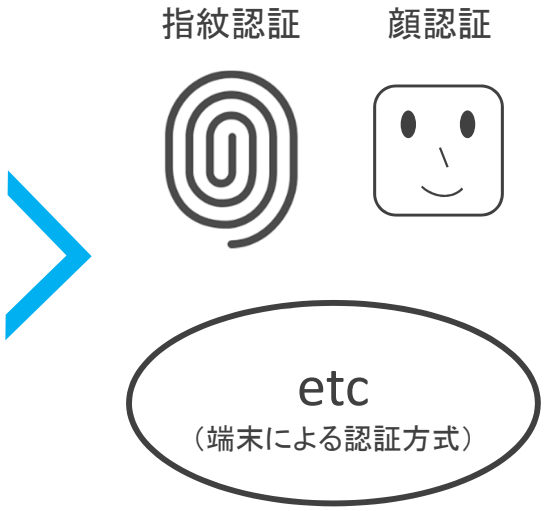
※画像はiOSのサンプルイメージです。実際のものとは異なる場合があります。

「かんたんログオン」のイメージ

2018/3/30時点

かんたんログオンを タップ

かんたんログオン（認証）



つくばインターネットバンキング TOPページ

初回の登録は必要ですが、
ログオンの都度、契約者番号やパスワードを入力する必要はありません。

「かんたんログオン」の設定方法

「かんたんログオンの設定はこちら」をタップ

「かんたんログオン」をタップ

設定したい方の「登録」をタップ

ログオン情報（契約者番号やパスワードなど）を入力し「登録」をタップして端末認証を実施

※設定が完了したらホーム画面の「かんたんログオン」をタップしてログオンしてください。
※端末自体に生体情報を登録していない場合、端末への生体情報登録を要求される場合があります。
※画像はiOSのサンプルイメージです。ご利用端末によって、表示される文言等が異なる場合があります。

ご利用可能端末

2018/3/30時点

OS種類	端末	かんたんログオン 利用可否	認証方式
Android 5.0以上	Android	○	・端末ロック認証 端末に装備されている指紋、パスワード、パターン、ロックNo.等で認証します。（端末毎に異なります）
iOS 9.0以上	iPhone5S以降	○	・Touch ID / Face ID 指紋認証または顔認証で認証します。
	iPhone5以前	×	

ご注意事項

1. 「かんたんログオン」は、スマートフォンに搭載された端末（画面）ロックのセキュアな認証機能を利用します。ご利用の機種により認証方法が異なりますのでご了承ください。（お客さまが選択することはできません。）
2. 生体認証が利用できる機種は、Android OS 5.0以上、iPhone iOS 9.0以上の生体認証機能付き端末となります。 Android OS 5.0以上で生体認証機能が無い端末では、パターン認証やロックNo. 認証になります。対象機種以外のお客さまは「かんたんログオン」はご利用いただけません。
3. Android 5.0未満及びiOS9.0未満の端末では、新アプリのダウンロードはできませんが、旧アプリをご利用中のお客さまはそのまま継続利用することができます。ただし、旧アプリの再ダウンロードはできませんのでご注意ください。
4. 生体認証等が苦手な方向けに、つくばインターネットバンキングの契約者番号保存ログオン機能も搭載しております。アプリ内のセキュアな環境に契約者番号を保存しておくことで、2回目以降のログオン時にパスワードのみの入力でログオン可能となります。
5. つくばインターネットバンキングのログオン時に、リスクベース認証が発生し追加の合言葉を要求されることがあります。その場合は、継続してご利用いただくことでシステムが正当なログインだと学習し、追加の合言葉は要求されなくなります。
6. ワンタイムパスワードをご利用中の方は、ログオンの都度入力が必要になります。
7. 「Secure Starter」についての詳細は専用Webページからご確認ください。
【https://web.saat.jp/s-starter/tsukubabank/】

「Secure Starter」のセキュリティ機能（従来の提供機能）

「端末初期化警告」の表示　（メッセージコード1001）

OSの不正利用（Root権限の奪取／Jailbreak）の問題を検知した場合に表示されます。対処には、お客さまによる端末の初期化（工場出荷時状態への復元）が必要です。初期化方法は、通信事業者やメーカーのサポート窓口からお問い合わせください。

〈Android〉

各通信事業者のｻﾎﾟｰﾄ連絡先やｼｮｯﾌﾟ、端末の購入店へお問い合わせください。

〈iOS〉

Appleのサポートページをご参照ください。ご不明な点につきましては、Appleのサポート連絡先からお問い合わせください。

※通信事業者やメーカーのサポート窓口では「工場出荷時状態への復元手順」につきまして、お問い合わせください。

※初期化により、端末のデータが消去されます。事前に必ずデータのバックアップをお取りください。

「悪性コード検知警告」の表示　（メッセージコード1102）

ウイルスなどの悪性コードが混入した、不正アプリを検知した場合に表示されます（Android OS）。対処には、お客さまによる不正アプリの削除が必要です。画面の指示に従い、削除を完了してください。

「DNSチェック警告」の表示　（メッセージコード1002）

アクセス先の情報に問題を検知した場合（DNSチェック）に表示されます。画面の指示に従い、端末のネットワーク設定を確認・変更の上、利用続行の可否を選択してください。

※警告の表示は、アプリの設定に応じて行われます。

「Wi-Fi接続警告」の表示　（メッセージコード1003）

つくばインターネットバンキングなどへのアクセス時、Wi-Fiネットワークに接続している場合に表示されます。画面の指示に従い、Wi-Fiネットワークの信頼性を確認のうえ、利用続行の可否を選択してください。