



2018年11月14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 ～生体認証で法人向けインターネットバンキング「つくばビジネスNet」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いますので、お知らせいたします。
今回のバージョンアップは、法人向けインターネットバンキング（以下「つくばビジネスNet」）の「かんたんログオン機能」に対応するもので**全国初**の取り組みとなります。

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、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

2018年11月15日（木）

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

2. アップデート概要

(1) 対象サービス

つくばビジネスNet

(2) 対応内容

生体認証機能（指紋認証や顔認証等）を利用した「かんたんログオン機能」対応
※個人向けインターネットバンキングと同様の機能を提供します。

(3) ご利用になる際の注意点

- ① 契約者番号、管理者（利用者）コード、ログオンパスワードの初期登録が必要です。
- ② 「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）ロックのセキュリティの高い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 セキュリティの観点から、可変パスワード・ワンタイムパスワードにつきましては、都度入力が必要となりますのでご了承ください。

「Secure Starter」の機能詳細については以下の紹介ページをご覧ください。

<https://web.saar.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
TEL 029-859-8111			

スマートフォン専用無料アプリ 「Secure Starter」

個人のお客さまも 

法人のお客さまも 



筑波銀行 Tsukuba Bank

個人のお客さま 法人のお客さま

インターネットバンキング
ログイン

契約者番号

パスワード

契約者番号を保存

インターネットバンキング
かんたんログイン(生体認証)

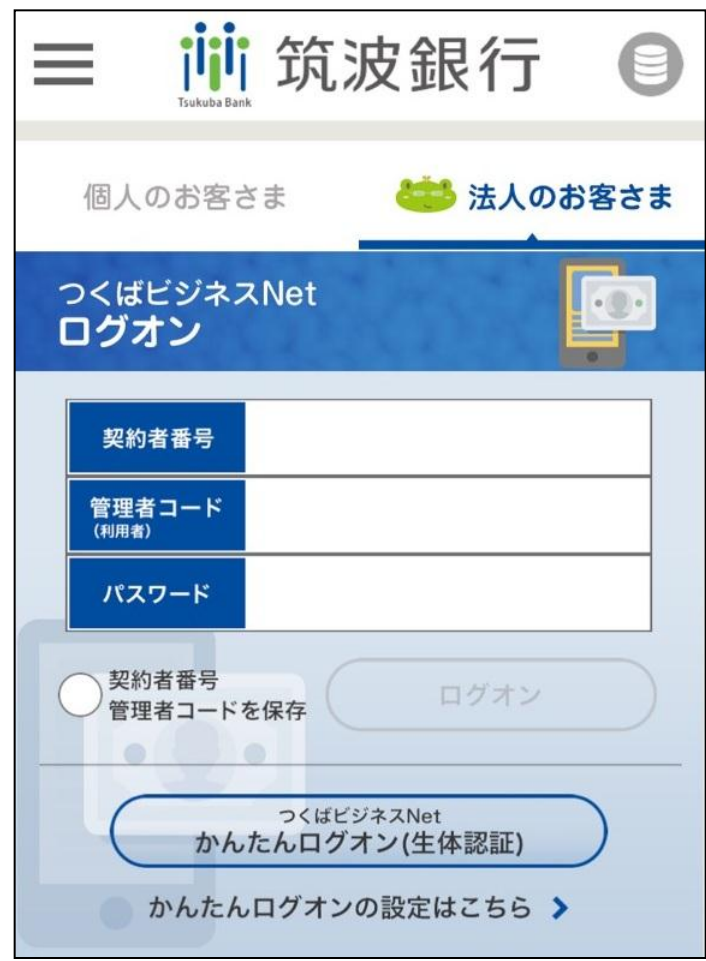
かんたんログインの設定はこちら >

Light WEB照会サービス・
インターネットバンキングのご契約

Light WEB照会(残高照会)
インターネットバンキングのご契約はこちら

Light WEB照会
かんたんログイン(生体認証)

かんたんログインの設定はこちら >



筑波銀行 Tsukuba Bank

個人のお客さま 法人のお客さま

つくばビジネスNet
ログイン

契約者番号

管理者コード
(利用者)

パスワード

契約者番号
管理者コードを保存

つくばビジネスNet
かんたんログイン(生体認証)

かんたんログインの設定はこちら >

インターネットバンキングの ログインを生体認証で

セキュアに！簡単に！

指紋
認証



顔認証



※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。 2018/11/15時点

旧

個人のお客さま用メニュー



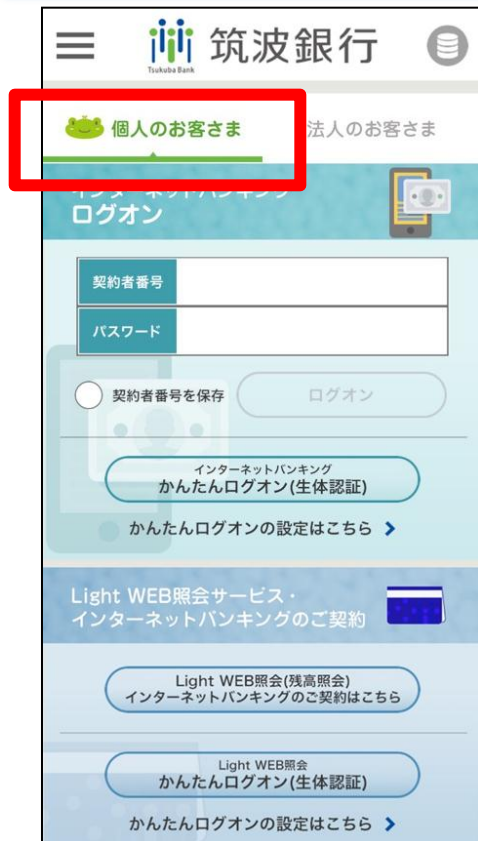
従来の個人用メニュー
+
法人用メニュー
を新規に追加!

お客さまの用途に
合わせてタブを
切り替えてご利用
いただけるように
なりました!

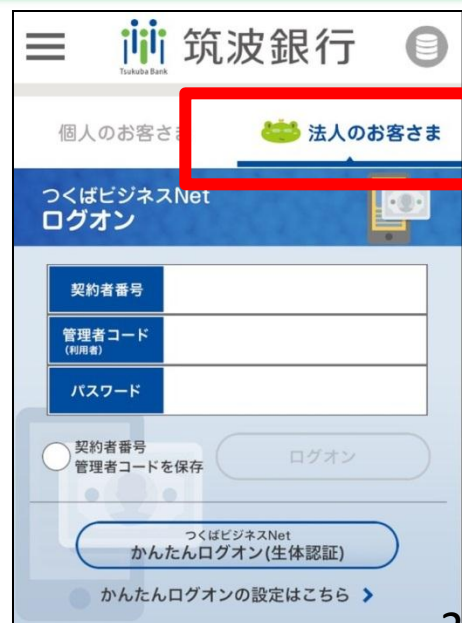


新

個人のお客さま用タブ



法人のお客さま用タブ



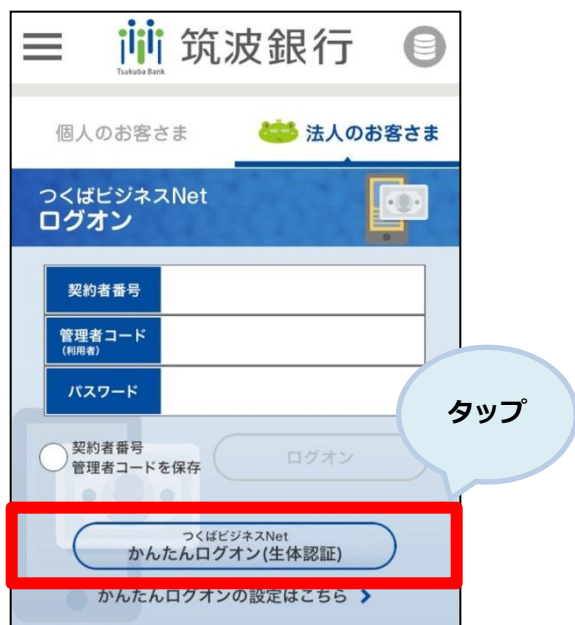
「Secure Starter」紹介Webページ



<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。

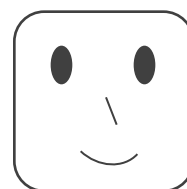
①かんたんログオン ボタンをタップ



②かんたんログオン (認証)

指紋認証

顔認証



etc
(端末による認証方式)

※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。

③可変パスワード/ (ワンタイムパスワード)の入力

可変パスワードの入力

	1	2	3	4	5	6	7	8	9	10
確認番号			○					○		
可変パスワード	<input type="text"/> (2桁)									

ワンタイムパスワードの入力(※)

ワンタイムパスワード

お手元のパスワードカード(表面)の「①」ボタンを押すと画面に表示される6桁の数字

ワンタイムパスワード

④つくばビジネスNet へログオン!

メッセージ

メッセージ 未読0件 [一覧へ](#)

承認状況

権限が付与されていない場合は「-」が表示されます

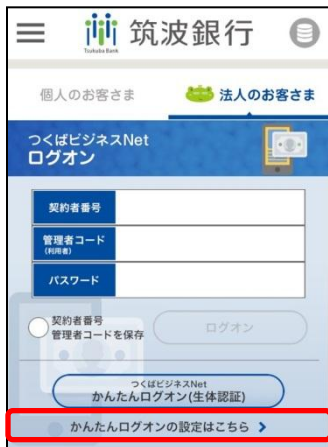
	承認待ち取引 (括弧内は本日承認期限)	作成済み取引 (未承認)	作成中取引
振込	0件 (0件)	0件	0件

※お客さまの権限設定によりワンタイムパスワードは入力が必要な場合もあります。

【法人のお客さま】かんたんログオンの設定方法

2018/11/15時点

「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



つくばビジネスNetの「登録」をタップ



ログオン情報（契約者番号、管理者（利用者）コード、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。

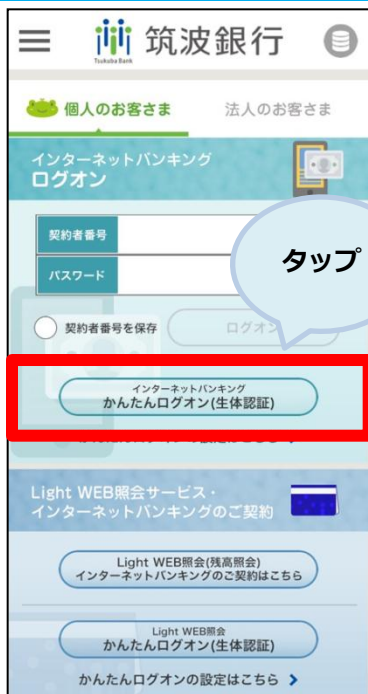
【個人のお客さま】かんたんログオンのイメージ

2018/11/15時点

①かんたんログオンを
タップ

②かんたんログオン
(認証)

③つくばインターネット
バンキングへログオン！



指紋認証 顔認証



etc

(端末による認証方式)

※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。



【個人のお客さま】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



つくばインターネットバンキングLight Web照会
サービスも設定できます。

※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。

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

- 「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。)
- 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。
- 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。
- 生体認証等が苦手な方向けに、個人のお客さまの場合契約者番号、法人のお客さまの場合契約者番号、管理者(利用者)コードの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ログオン情報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入力のみでログオン可能となります。
- 法人のお客さまは、ログオンの都度可変パスワードの入力が必要になります。
- 法人のお客さまで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。
- 「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/>】

「端末初期化警告」の表示

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〉

各通信事業者のサポート連絡先やショップ、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

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

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。

「Wi-Fi接続警告」の表示

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。

※警告の表示は、アプリの設定に応じて行われます。