

2022年3月2日

各 位

住信SBIネット銀行株式会社

スマート認証 NEO のセキュリティ強化について

～中継型（リアルタイム）フィッシング詐欺にも有効～

住信 SBI ネット銀行株式会社（本社：東京都港区、代表取締役社長（CEO）：円山 法昭、以下「住信 SBI ネット銀行」という）は、2022 年 3 月 2 日より、アプリ「住信 SBI ネット銀行」における認証機能「スマート認証 NEO」の登録時に必要な SMS 認証（ショートメッセージ認証）のセキュリティを強化しました。

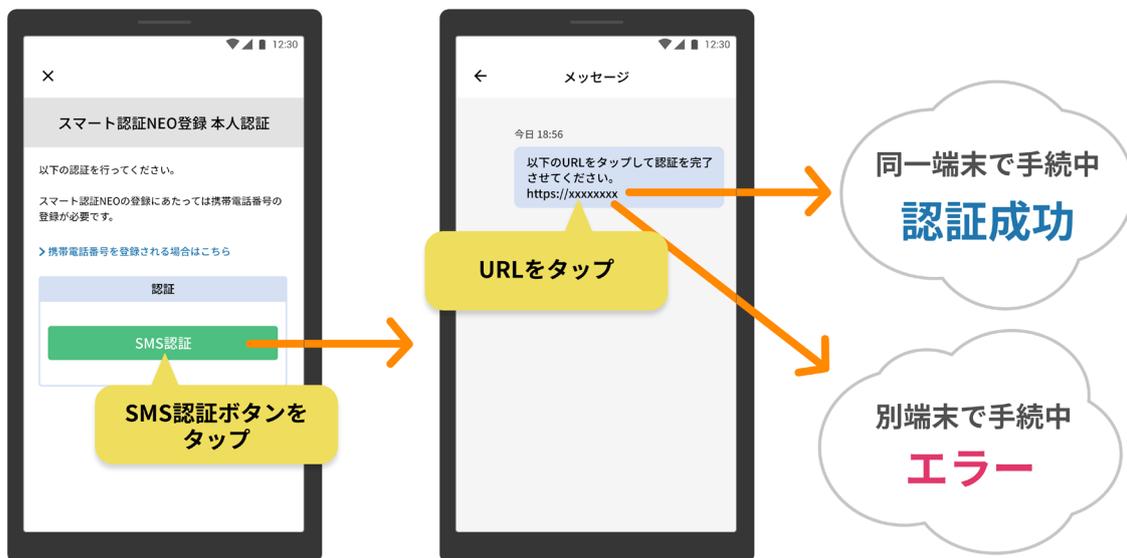
従来の二要素認証である SMS 認証では、当社から認証コードを SMS で送信し、それをお客さまが画面に入力することで認証しますが、今回開発した「アプリ連動型 SMS 認証」では認証コードのかわりに URL を送信し、お客さまがその URL をタップすると、自動的に当社アプリが起動して認証します。

認証コードの入力が不要であることに加え、SMS 認証手続き中のアプリと SMS を受信した端末が同一である必要があり、従来の SMS 認証に比べて、利便性とセキュリティレベルが大幅に向上します。

・アプリ連動型 SMS 認証フローイメージ

SMS認証手続き中のアプリ

メッセージアプリ



この「アプリ連動型 SMS 認証」は、当社の独自開発によるもので、現在特許出願中です。

・当社のセキュリティ対策

住信 SBI ネット銀行では、お客さまに安心してご利用いただけるよう、以下のようなセキュリティ対策を実施しています。

24 時間 365 日体制の振込モニタリング

当社の基準に照らし、第三者が操作した可能性があると思われる取引は、一時的にお取扱いを停止し、お客さまへ電話やメール等にてご連絡をさせていただきます。

セキュリティ対策ツールの無償提供

スマートフォンを利用した取引認証機能「スマート認証 NEO」や、セキュリティ対策ソフトの「SaAT Netizen」を無償で提供しています。

スマート認証 NEO について詳しくはこちら

<https://www.netbk.co.jp/contents/lineup/smartauth-neo/>

SaAT Netizen について詳しくはこちら

<https://www.netbk.co.jp/contents/security/software/>

不審なログイン環境のチェック

犯罪者などによる不審なログインにいち早く気付いていただけるよう、お客さまの口座に異なるご利用環境からログインが行われた場合、メールなどでお知らせしています。

ウイルス感染のチェック

お客さまが当社 WEB サイトにアクセスした際に、お使いの PC がコンピューターウイルスに感染していないかをチェックしています。

ウイルスの感染兆候を検知した場合には、ブラウザを遮断しご利用を停止します。

住信 SBI ネット銀行は、お客さま中心主義のもと最先端のテクノロジーを活用することで金融サービスを変革し、社会をより快適で便利なものに変えていくことを目指してまいります。

以上

本プレスリリースに関するお問い合わせ先：住信 SBI ネット銀行 企画部 広報担当 03-6229-1247