法人口座を狙ったフィッシング詐欺の新たな手口にご注意ください
― 遠隔操作ソフトを悪用する手口が確認されています―

2026 年 6 月吉日
株式会社 SBI 新生銀行

警視庁から法人口座を狙ったインターネットバンキングの不正送金被害が多発しているとの注意喚起がありましたので、銀行を騙った不審なメール・電話にご注意ください。

近時、銀行を装った自動音声の電話の後、対人対応に切り替え、従前のように偽サイトへ誘導して認証情報等を入力させるだけでなく、「PC 環境の更新」、「セキュリティ強化」、「電子証明書の更新」、「利用制限の解除」などを口実に、遠隔操作ソフトをインストールさせ、お客さまの端末を犯罪者が遠隔操作して不正送金を実行する事例が確認されています。 詳細は（別紙）を参照ください。

本手口では、代表者、経理・財務・総務担当者、代表電話受付、インターネットバンキング操作担当者が狙われる危険があります。被害にあわないために本注意喚起の内容を、必ず社内でご共有ください。

【次の行為は絶対に行わないでください】

- ログイン ID、ログインパスワード、暗証番号、ワンタイムパスワード等の認証情報を第三者に伝えること
- メールや SMS に記載されたリンクからインターネットバンキングにログインすること
- 案内された遠隔操作アプリや不審なソフトをインストールすること
- 電話をつないだまま、相手の指示に従ってパソコンを操作すること
- 画面共有や遠隔操作を許可すること

当行は絶対に電話、メール、FAX、SMS 等のいかなる方法によってもお客さまの認証情報（ログイン ID、ログインパスワード、暗証番号、ワンタイムパスワード等）をお伺いすることはありません。また、インターネットバンキングのお手続きのために、お客さまに遠隔操作ソフトのインストールや画面共有を依頼することはありません。

なお、不審な電話、メール、FAX、SMS 等があった場合は、相手の担当者の部署・氏名等を聞いた上で、折り返し連絡するなど慎重にご対応いただくか、もしくは「ご照会窓口 SBI 新生コーポレートコールセンター（法人ご契約者さま専用）」にお問い合わせください。万一、認証情報（ログイン ID、ログインパスワード、暗証番号、ワンタイムパスワード等）を入力または回答してしまった場合は、「ご照会窓口 SBI 新生コーポレートコールセンター（法人ご契約者さま専用）」へ速やかにご連絡いただくとともに、お客さまの所在地管轄の警察署へご相談ください。

〈本件に関するお問い合わせ先〉
SBI 新生コーポレートコールセンター
電話番号：0120-511-025（銀行営業日 9:00～17:00）
※メニュー番号「4」をご利用ください。

（別紙）

＜新たな手口による発生事例＞　遠隔操作による不正送金被害の発生

お客さまへ見慣れない番号から電話がかかってきて次のような自動音声が流れる（複数のパターンが確認されていますので、以下に限りません）

こちらは●●銀行法人窓口です。インターネットバンキングを利用している方は1を押してください

↓

番号を押すと有人対応に切り替わり、以下のようなパターンで誘導されメールアドレスを聞かれる（複数のパターンが確認されていますので、以下に限りません）

セキュリティ強化のための更新が済んでいないため、電話しました	電子証明書の更新が済んでいないため、電話しました	現在、取引の制限を行っています。更新方法をご案内します

↓

送られてきたメールのリンクをクリックすると「必ずご確認いただきたいお知らせ」画面が表示され、更新に必要と称してアプリのインストールを促される

インストールするとお客さまのパソコンを犯罪者が遠隔操作します

お客さまの表示画面と犯罪者側の表示画面は異なっています

↓

インストールすると以下文言が記載された画面が表示される（以下に限りません）

現在セキュリティ保護強化に伴うシステム更新実施しております。処理完了までの間、一時的に画面が遅延または停止する場合がありますが、正常な処理となりますのでそのままお待ちくださいますようお願い申し上げます

↓

「手続きを進めるにはショートメール（またはEメール）による認証が必要です」と言われ、携帯電話の番号（またはメールアドレス）を聞かれる

↓

送られてきたショートメール（またはEメール）のリンクをクリックして「ログインパスワード、取引実行パスワード、ワンタイムパスワード」等をスマートフォンの画面に入力するよう促される

↓

パソコンを遠隔操作され、騙し取られた認証情報を利用した不正な振込を実行される

犯罪者はお客さまのパソコンを遠隔操作し、裏側で不正送金を実行