口座・アカウントの不正アクセス・不正取引にご注意ください

2025年8月5日

昨今、証券口座の乗っ取りを通じた不正アクセス・不正取引被害が急増しております。その手口としては、主に、メールやSMSなどによって実在する組織のウェブサイトを装ったフィッシングサイトなどに顧客を誘導して顧客情報（ログインIDやパスワード等）を窃取し、口座に不正にアクセスするものや、攻撃者が顧客端末をマルウェアに感染させ、リアルタイムで当該端末を監視するとともに操作し、顧客情報を窃取するものなどが想定されております。

昨年12月にはJFマリンバンクを装った不審な電子メールが送付され、フィッシングサイトに誘導される事案も確認されており、当会をご利用いただいておりますお客様におかれましても改めて下記対策内容をご確認いただき、不正サイトへのアクセス等を行わないようご注意願います。

万一、誤ってネットバンクのログインID・パスワードなどの情報を入力してしまった場合、不正送金などの被害にあう可能性がありますので、利用停止や最寄りの店舗へのご相談をお願いいたします。

＜不正アクセス・不正取引にかかる対策について＞

- ✓ 不審なメール又はSMSや添付ファイル、リンクを開かないこと。
- ✓ パスワードは推測が容易な単純なものを用いず、また、同じパスワードを使いまわさないこと。
- ✓ OS・ソフトウェアを最新に保つこと。
- ✓ ソフトウェアは、信頼できないサイトからダウンロードしないこと、必ず公式サイトや正規のアプリストアからダウンロードするよう徹底すること。
- ✓ セキュリティソフトを導入し、定期的なセキュリティスキャンを実施すること。セキュリティソフトを更新し、定義ファイル（セキュリティソフトがマルウェアを検出するのに使用するファイル）を常に最新の状態に保つこと。セキュリティソフトには、振る舞い検知機能やウェブ保護機能を持つ総合セキュリティソフトの利用が推奨されること。
- ✓ 利用者自身のPCやスマートフォンで、自社のサイト利用中に不審な表示（普段と違うログイン画面、不自然なポップアップ、追加の個人情報入力要求など）が出て情報の入力を求められた場合はそれに応じないこと。
- ✓ マルウェア感染防止のため、ブラウザから通常行わないキーボード操作（特にCtrl＋V等のショートカット実行）を求められても実行しないこと。
