サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

多要素認証を設定しよう

近年、証券口座やＳＮＳなどのアカウントの乗っ取り被害が多発しています。
証券口座については、多要素認証の設定必須化が、日本証券業協会から発表されましたが証券口座以外にも多要素認証に対応しているサービス（ＬＩＮＥ、Ｉｎｓｔａｇｒａｍ Ａｍａｚｏｎなど）がありますので、これを機に設定を検討してください。

多要素認証の種類

●ＳＭＳ/Ｅメール認証（安全性★）
事前に登録された電話番号やＥメールアドレスに対して送信されるワンタイムパスワード（ＯＴＰ）を入力する認証方式。
利便性と普及率は高いが、多要素認証のなかでは最も脆弱であるが、設定することによりセキュリティは大幅に向上する。

●認証アプリ（安全性★★）
認証アプリで生成されたＯＴＰを入力する方式。
ＳＭＳ/Ｅメール認証よりも脆弱性が少なく、セキュリティが高い。

●パスキー（安全性★★★）
「持っているもの（端末と秘密鍵）」と「本人であること（生体情報やＰＩＮ）」を組み合わせた認証方式で、セキュリティ面では最も強固なので、利用しているサービスや端末がパスキーに対応している場合、**最優先で設定することを推奨。**
パスキーの設定後は、ログイン認証が簡易になることから、利便性にも優れている。

多要素認証の脅威別耐性

脅威名	ＳＭＳ/メール	認証アプリ	パスキー
フィッシング詐欺	○	○	○
パスワードリスト攻撃	○	○	○
総当たり攻撃	○	○	○
ＳＩＭスワップ	×	○	○
マルウェア	×	△	○
リアルタイム型フィッシング	×	×	○

まとめ

多要素認証については、安全性の高いものを優先して設定しましょう。

また、多要素認証の設定だけではなく、**機器やアプリのアップデート、パスワードは可能な限り長く複雑にして使い回さない、セキュリティソフトを導入する**などの基本的なセキュリティ対策を合わせて行うようにしてください。