二段階認証と二要素認証

二段階認証は、二要素で組み合わせるべき

三種類の要素
- 本人しか知らないパスワード
- 本人所有物に依存するパスワード
- 指紋や虹彩認証などの生体認証

・複数要素を組み合わせて二要素認証

・生体認証は、ブルートフォース攻撃から守り、コピーされにくい

スマートフォンなどを使用した二段階認証は、電子決済など金融分野等のアプリで当たり前になっています。
アクセスをしようとしている人が、正当なアクセスできる権利を有している人かどうかを判断するためには、適正な認証システムが必要です。
お金を扱うアプリでなくても、会員として登録する場面で、登録されたメールアドレスやショートメッセージサービス（SMS）を使ってアプリがパスワードを送り、それを利用してログインをする手法がありますが、これは本人を確認するためのもので、二段階認証とは別物です。
二段階認証は、通常の ID、パスワードでのログインの他に、もう一つ別のパスワードやセキュリティコード等を使って二段階に分けて認証手続きをする方法です。
多くの二段階認証では、Google 認証システムのような一定時間でパスワードを自動更新するワンタイムパスワードを使用しているものが多いです。これにより、万が一パスワードが漏れても安心度が高まります。
仮想通貨取引所へのログインや、オンライン銀行での振込処理などで多く使用されていますが、これを電子マネーなどの個々の買い物などのモバイル決済で使用するには、面倒すぎて採用されていません。モバイル決済では、利便性を優先してパスワード入力さえしなくてよいように、プリペイドなどでリスク軽減しているものが流行っています。
その際、ログイン時に二段階認証を義務付け、その後はスマートフォンアプリ上でログインされたままになるものが多く、どの程度の期間使用していないと強制的に再度認証させるかは利便性とのバランスで、各社の方針は異なるようです。
二段階認証に似た言葉で、二要素認証というセキュリティ用語があります。
二要素認証では、2 つ以上の別の認証要素を利用して、アクセスする人の確認をします。
一般的には、ID、パスワードという本人しか知らないはずのデータを利用するもの、スマートフォンやワンタイムパスワードキーなど本人が所有するハードウェアに依存するデータ、そして指紋や虹彩認証などの生体認証の 3 種類の要素があります。二段階認証とかぶるものが多いですが、基本的にパスワードなど文字データに頼るものは、ブルートフォース攻撃の対象になりやすいので、生体認証と組み合わせる方がよいでしょう。