２０２５年5月２２日発行　第５６４号

2025
5

ふじさん

fujijoho group monthly magazine

富士情報

～ ２０２５年指針 ～

開　点

［今月のひとこと］

パスキー

・情報処理試験合格者

・今年の夏至は６月21日

・書店無店舗自治体

清八山のミツバツツジ　　写真提供：都留市　産業課

今月のひとこと

パスキー

社　長　渡　辺　直　企

証券会社のインターネット口座が相次いで乗っ取られ、株式を不正に売買される被害が急増しています。金融庁によりますと、今年の 3 月から急増し 4 月には単月で 4,852 件の不正アクセス、2,746 件の不正取引があり、約 1,481 億円の不正売却、約 1,308 億円の不正買付があったそうです。多くはフィッシング詐欺などで ID やパスワードが抜き取られているとして、日本証券業協会は「メールや SMS（ショートメッセージ）などに表示されているリンクを絶対に使わないでください。」と呼びかけています。

5 月 1 日には著名投資家のテスタさんが楽天証券で保有する自身の口座が乗っ取り被害にあったと X に投稿しました。二段階認証を使用していたそうですが、朝に二段階認証の確認メールが来て気付いたそうです。あわてて確認したところ、前日夜に注文した履歴があり発覚したとのことです。二段階認証は当該サービス(この場合は楽天証券)の ID とパスワードに加えて、スマホに届く認証コード、生体認証などの追加の認証を行うものです。テスタさんの場合二段階認証を何らかの方法で突破されてしまったそうです。幸いにも取引所開始前に発覚し、口座をロックしたため金銭的な被害を免れたそうです。SBI 証券は ID とパスワードだけでログインが可能なバックアップサイトを 5 月 30 日に閉鎖予定でしたが、急遽 5 月 2 日に閉鎖しています。このお知らせのページで「デバイス認証」「FIDO 認証」の利用を呼びかけています。

FIDO(ファイド)は生体認証や PIN といったローカルな認証と、公開鍵暗号方式の署名機能を組み合わせた認証技術です。ユーザー側の端末には秘密鍵を格納し秘密鍵で署名されたトークンをサーバに送信し、サーバが秘密鍵に紐づいた公開鍵を用いて署名を検証します。生体情報や PIN は送信されずトークンを傍受されても秘密鍵がなければ対応するトークンを作成することはできません。生体認証と秘密鍵を格納する認証器は端末に内蔵されているので端末を物理的に持ち出されない限り安全です。Windows11 には TPM（Trusted Platform Module）が必須になりましたが、これも認証器です。

FIDO は端末固有の秘密鍵を用いるため、端末の紛失、機種変更が有った場合は新たにサーバに登録する必要があります。FIDO アライアンスは新しい認証方式としてパスキーを策定しています。パスキーには同期パスキーといって、複数端末で同じ秘密鍵を暗号化して同期して使用できる方式が有ります。Google パスワードマネージャーや iCloud キーチェーンを用いて端末間で秘密鍵の共有が可能になっています。この秘密鍵は暗号化されていて端末内でしか復号できないので利便性も安全性も兼ね備えた方式といえます。

これらの認証や暗号化は公開鍵暗号方式を用いています。1977 年に MIT の 3 人の研究者が開発しました。素数 p,q が与えられたとき n =pq は簡単に計算できますが、n を素因数分解して p や q を得ることが困難な性質を利用しています。公開鍵暗号で用いられる RSA 暗号は一般に約 300 桁の 2 つの素数を秘密鍵とし、2 つの素数を掛け合わせた約 600 桁(2048 ビット)の合成数を公開鍵としています。公開鍵は秘密鍵の所有者しか復号できない暗号を作成することができ、秘密鍵の署名は公開鍵によって検証ができます。

公開鍵暗号方式はインターネットの暗号化通信(https)をはじめ、マイナンバーカードやビットコインなど多くの場で活用されています。パスキーなどのインフラが整備されることで、より安全なデジタル環境が整うよう期待しています。