要旨

１．はじめに

近年、様々なシステムへのログイン認証に、ID とパスワードを求められるようになった。しかし、パスワードの使いまわしや安易なパスワード利用など、パスワードの流出による不正アクセスの原因のひとつとなっている。また、管理者側では、パスワードを忘れたことによるパスワード初期化の問合せ対応が負担となっている。そこで、パスワードを覚える必要のない、かつ、セキュアな認証に焦点を当て、パスワードの忘却問題への解決の糸口を探ることにした。

２．パスワードを利用しない認証とは

認証方式は、本人しか知りえない情報を利用する『知識認証』と、本人だけが所持しているものを利用する『所有物認証』、身体的な特徴を利用する『生体認証』の３つに分類される。パスワードは、その本人しか知りえない情報の為、『知識認証』に当たり、『所有物認証』と『生体認証』はパスワードを覚える必要が無い。よってパスワードを覚える必要が無く、『所有物認証』か『生体認証』、または、その両方を利用する認証が、パスワードの忘却問題を解決してくれる認証であることがわかった。

３．『所有物認証』か『生体認証』、または、その両方を利用する認証とは

調査を実施したところ、パスワードを覚える必要が無く、『所有物認証』と『生体認証』の両方を利用する『FIDO（Fast IDentity Online: ファイド）』という認証があることがわかった。FIDO は、「利用機器（パソコンやスマートフォンなど）の所持認証 + 利用機器での生体認証」を行える。つまり、生体認証を使って、利用機器にログイン後、秘密鍵でログイン要求を暗号化し、暗号化されたデータを送ると、送信先（サーバー）には対応した公開鍵があり、その公開鍵で復号化して認証する。これにより、送信先では、登録された機器からのアクセスかどうかの検知ができ、また、ユーザー情報は、インターネット回線に送信されない安全な認証と言える。（図１参照）

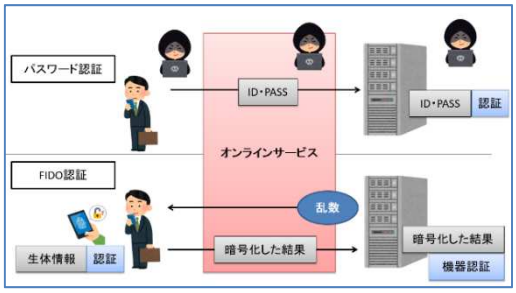

図 1. FIDO の仕組みの図解

４．課題・仮説

当研究グループでは、FIDO の認証技術の理解を深め、安全な認証方式かどうかを検証し、安全性を高めることができないかを検討した。

FIDO で利用できる利用機器（パソコンやスマートフォンなど）には、既に生体認証機能が備わっているが、指紋認証では、ゼラチン等で偽造できることがあり、顔認証では、双子が見分けらないなど、様々な問題を抱えている。そこで、本人を特定できる新たな

要旨

認証を利用機器側に設けることができないかと考えた。

５．検証

ウィルス対策セキュリティソフトには、「ふるまい検知」と呼ばれる機能が実装されつつあり、普段とは異なる挙動を検知できることにヒントを得て、個人のキーボード入力の癖に着目し、その癖を判別できるようにならないか、実際にアプリケーションを作成し検証してみた。キーストロークアプリケーションは、登録時のストローク情報と認証時のストローク情報を比較し、どれだけ類似しているかを判定し認証する仕組みである。ストローク情報を取得する為に入力する“パスコード”は、認証時の画面に表示されており、記憶する必要は無く、“パスコード”を見ながら入力(タイピング)が可能となっている。

研究メンバーそれぞれが、ユーザー登録時に同じパスコードを登録し、自分のユーザー時の本人受入率と、他のユーザー時の他人拒否率を算出する方法をとり、キーボード入力の癖を見分けられるのかを検証した。

他のユーザーの認証画面で、同じパスコードを入力した時のストローク情報を下図(図 2)に示す。同じパスコードを入力したにも関わらず、キーを押している、離している時間がそれぞれ異なっていることがわかる。

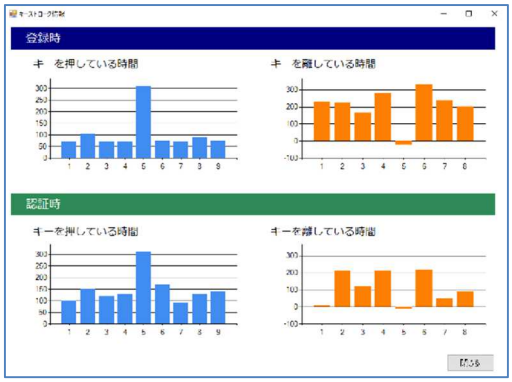

図 2. 他人拒否時のストローク情報

６．考察・今後の展望

『所有物認証』と『生体認証』の両方を利用したパスワードを覚える必要の無い FIDO の認証技術を利用し、FIDO でも防げない偽造認証、誤認については、キーストロークアプリケーションを組み合わせた多重認証で、セキュリティを強化することができる。これによりパスワードを覚える必要が無い為、パスワードの忘却問題を解決できると考えた。

近年の技術躍進から、“癖”で本人特定する認証技術を、AI と共同で開発、発展させることで、完全なパスワードレス時代がくることに期待する。

※「FIDO」は、FIDO Alliance の商標です。

※文章内の記載の会社名および製品名は、各社の登録商標または各社に帰属する標章もしくは商号です。