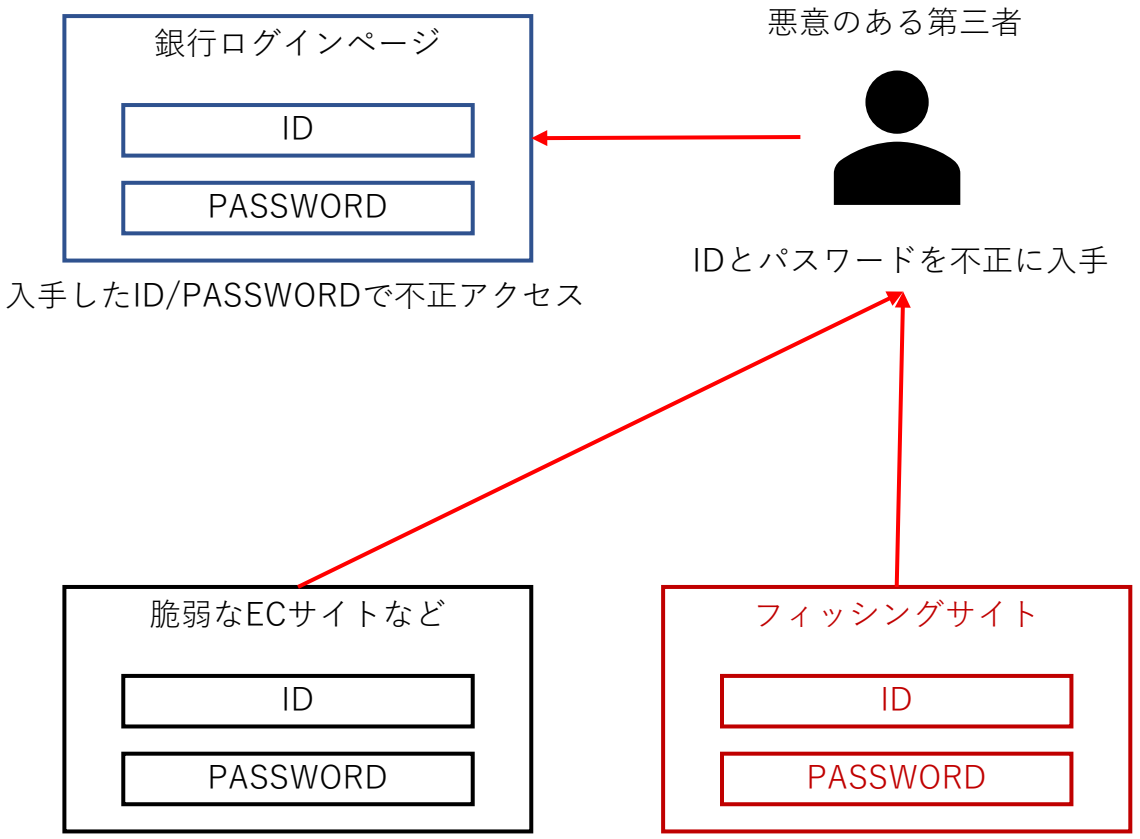
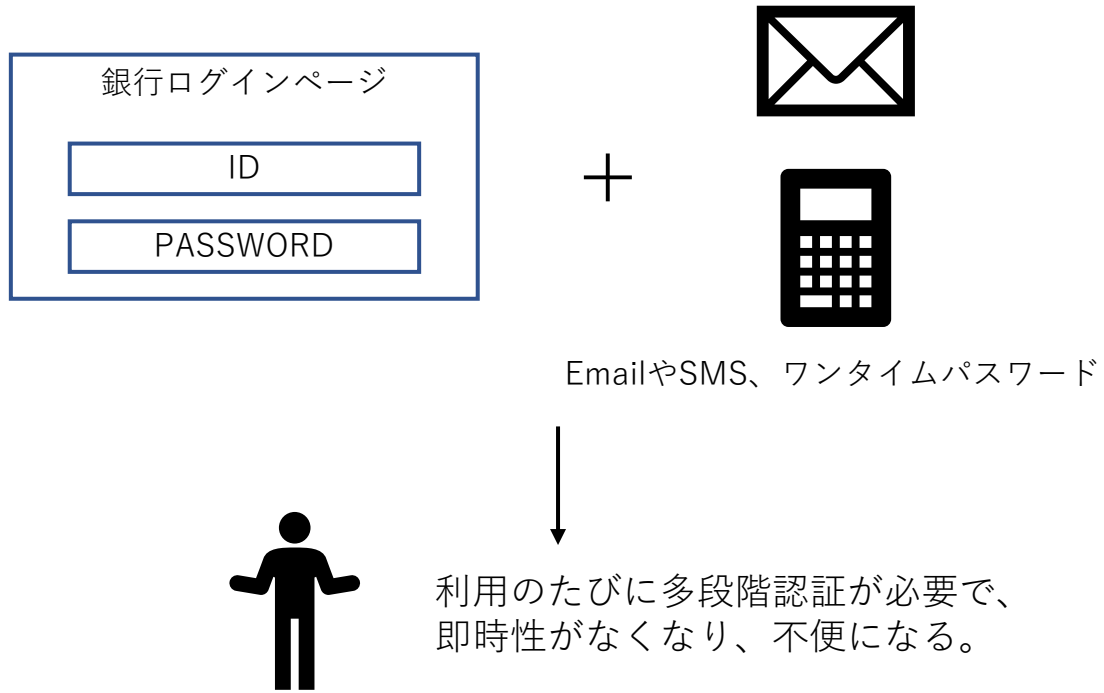
ID/PASSWORDを利用したセキュリティの問題点

IDとパスワードのみを使用した認証方式



ID/PASSWORD方式では、自社のサイトのセキュリティが万全であっても、他のサイトからID/PASSWORDが流出する可能性がある。また、スマホに不慣れなユーザーは、フィッシング詐欺でのID/PASSWORDの抜き取られや、内部者の顧客情報漏れがあれば、不正アクセスを許してしまう。

EmailやSMS、ワンタイムパスワードを利用した多段階認証



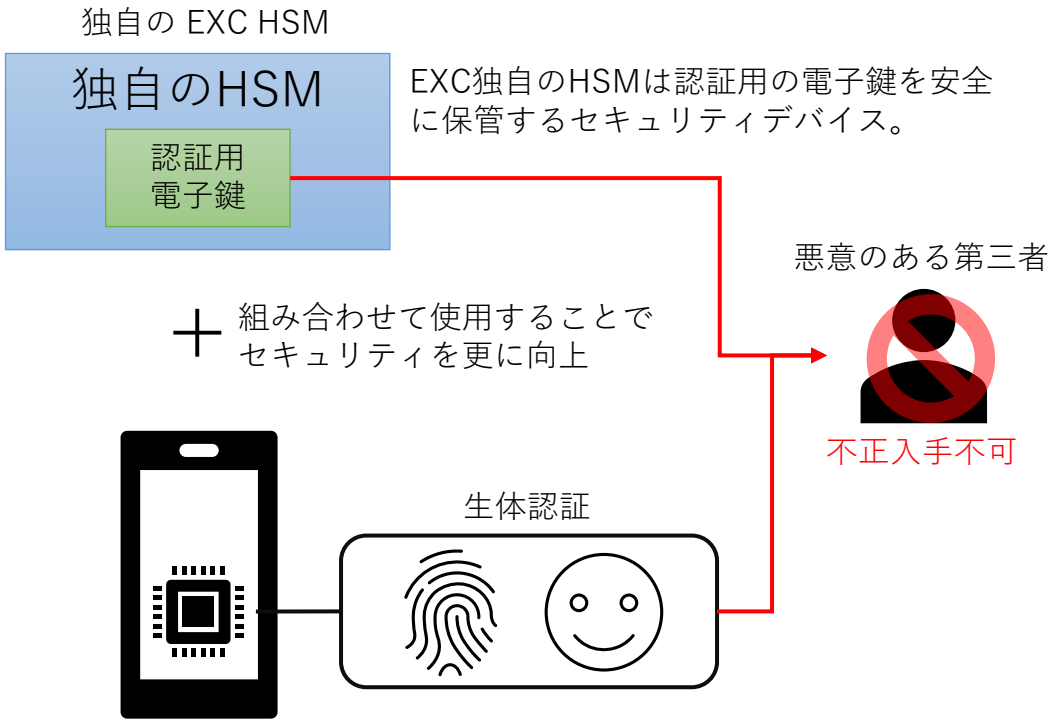
利用のたびに多段階認証が必要で、即時性がなくなり、不便になる。

従来のID/PASSWORD方式に、ワンタイムパスワードを加えても、ワンタイムパスワード自身がフィッシングされる可能性がある。

また、EmailやSMSを併用した多段階認証を導入すると、決済の即時性がなくなり、スマホに不慣れなユーザーにとっての利便性は大きく低下する。

独自のHSMと生体認証を組み合わせたCBDCのセキュリティー

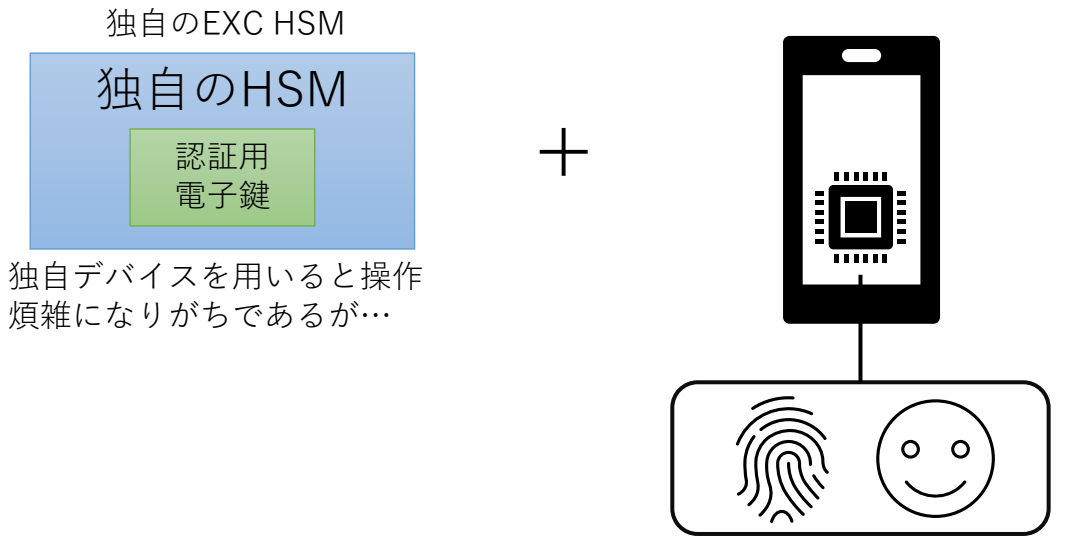
EXC HSMと生体認証を組み合わせた高いセキュリティ



生体認証情報はスマホのセキュリティチップに安全に保管されているので、不正に入手することは不可能。

GVEのCBDCプラットフォームでは、独自のEXC HSMとスマホの生体認証を組み合わせた安全な認証方式を導入。HSMの認証用電子鍵と生体認証の認証情報は安全に保管されているためハッキングやフィッシングサイトを用いても第三者が入手することは不可能。

EXC HSMと生体認証との組み合わせで利便性を向上



独自デバイスを用いると操作煩雑になりがちであるが…

生体認証を組み合わせることで1秒未満で認証可能

スマホの生体認証は、誰でも簡単に使用できるため、スマートフォンの操作になれていない方にとっても、非常に便利。

スマホの生体認証は、1秒以下で手軽に認証が行えるため、HSMのような専用デバイスを使用したときの操作の煩雑さを補い、利便性を大きく向上。

アップルとグーグルは、それぞれのiOSとアンドロイドでの、指紋認証でのエラーは5万分の1、顔認証では百万分の１の精度が既に確保済みと発表。この2つの組み合わせで、エラーは5億分の１。
クラウド音声認証を加えれば、セキュリテイーは更に向上。