GMO トラスト・ログイン

第 1 回

多要素認証ってなに?

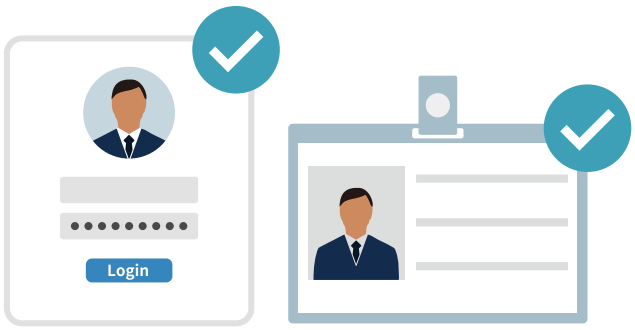
セキュリティを高めるテクノロジーとして多要素認証が注目されています。これは、従来のパスワードに加えてもう一つの方法で認証を行いセキュリティレベルを高めることを可能にします。今回より全 6 回の予定で多要素認証について連載していきます。

パスワードの課題

本 BLOG も含めて様々なセキュリティ関連の情報でパスワードの危険性について説明されています。例えばパスワードの使い回しや簡単に想像されてしまう単語を含めたパスワードは悪意を持つ第三者に不正にアクセスを許してしまう原因となってしまいます。また、パスワードの文字数が短い場合や英数字特殊記号などを組み合わせていない場合簡単に解読されてしまうこともレポートされています。また、解読に使われるマシンも以前は物理的に用意する必要がありましたが、現在クラウドサービスを使用すると簡単に大量の CPU を持つサーバを何台も使用することができるためより攻撃者に有利な環境がそろってきているということが言えます。

そこで企業では重要な情報へアクセスするのにパスワードポリシーを強固なものとしてユーザに義務付けると、今度はユーザがパスワードを頻繁に忘れてしまって業務に影響が出てきます。また付箋やメモ用紙にパスワードを書いて近くに貼っているという光景も目にするようになってしまいます。

パスワードを複雑にする以外の認証強度を高める方法



ID パスワードと社員証を使ってログイン

パスワードが解読されてしまっても情報へアクセスをさせない方法はないでしょうか。例えばシステムにアクセスするときにパスワードを入力し、さらに自分の社員証をかざしてはじめてアクセスできるようにしたらどうでしょう。社員証はいつも社員が自分の首から下げて持ち歩いているものですのでこれをかざすことができるのは本人以外にあり得ないことになります。

この場合、自分の知っている パスワードと自分が持っている社員証の両方が正しいことが確認されてシステムへのアクセスが許可されることになります。

このようにパスワードと社員証の二つの方法を使って認証させることを「多要素認証」または「二段階認証」と呼ばれています。これからは総じて「多要素認証」と呼ぶことにします。このパスワードや社員証はそれぞれ認証の「要素」と呼ばれます。

多要素認証の身近な例

もう少し身近なところで多要素認証について見ていきましょう。

1. 銀行のキャッシュディスペンサー

IC チップキャッシュカードと暗証番号

みなさんが銀行の ATM に行って預金を引き出す時のことを考えてください。キャッシュカードを使いますね。最近のキャッシュカードには IC 対応のキャッシュカードが普及しています。このキャッシュカードに IC チップが埋め込まれています。この IC チップは偽造が非常に困難な物理的な仕組みが施されています。預金を引き出す時にこの IC 対応キャッシュカードを ATM に挿入し、事前に登録している暗証番号を入力します。これは IC 対応キャッシュカードを持っていること、暗証番号を知っていることの二つの要素で認証しているので多要素認証の一つです。

2. オンラインバンキングのトークン


ネット送金ができるオンラインバンキング
ID パスワードとトークンに表示される
番号を入力

オンラインバンキングを活用している人の中には、銀行からトークンと呼ばれる小さなキーホルダーみたいなガジェットが送付されてきて使用している人もいるのではないでしょうか。このトークンには小さな液晶があり表示されている数字が常に定期的に更新されています。オンラインバンキングのシステムにログインするときに自分の ID とパスワードを入力し、そのあとトークンに表示されている番号を入力してログインできるようになります。このトークンの定期的に変わる数字列は「ワンタイムパスワード」と呼ばれ入力しているときにハッカーに知られてしまっても、次にログインするときにはその時にトークンに表示されている数字列でないとログインできないため安全であると言えます。
この例では事前に登録しているオンラインバンキングの ID とパスワードを知っていること、トークンを持っていてトークンに表示される現在の数字列を入力できることの二つの要素で認証しているのでこれも多要素認証の一つです。

3. iPhone の App Store でアプリの購入・インストール

App Store でアプリ購入時に
Touch ID による指紋認証

スマホで iPhone を使用している人はたくさんいらっしゃると思います。特に国内では海外とくらべ iPhone のシェアが高いので皆さんの周りにもたくさんの方が iPhone を使用しているのではないでしょうか。iPhone を初めて使用するときには必ず最初に Apple ID の登録が必要になります。これは自分のメールアドレスと自分で指定したパスワードで作成されます。また、最近の iPhone ではロックしたiPhone にアクセスするのにTouch IDと呼ばれる指紋情報で認証することができます。iPhone ではさまざまなサービスを利用するのに Apple ID が使用されます。App Store の設定の中でも Apple ID とパスワードを覚えておいてくれます。
さて、App Store で何かアプリをインストールするときはどうするでしょうか。まずは App Store のアイコンをクリックしてApp Storeを立ち上げます。その後インストールしたいアプリを検索して選択します。アプリのページを開きそこで

インストールを選ぶと Touch ID による指紋認証を要求されます。Touch ID が確認されて初めてそのアプリがインストールされます。これは最初に App Store アプリを起動したときに、事前に設定した Apple ID とパスワードが自動的に送信されています。そしてアプリをインストールするときに Touch ID による指紋認証が実行されます。有料のアプリの場合この時点で Apple ID に紐づく課金方法で課金が行われます。この App Store でも Apple ID とパスワードによる認証と Touch ID による指紋認証の二つの要素で認証しているので多要素認証の一つです。

4. クレジットカードでの支払い

みなさんもレストランなどの支払いにクレジットカードを使用することがあるかと思います。以前はサインをして決済するのが一般的でしたが最近は店頭で端末にクレジットカードを挿入し４桁の PIN と呼ばれる番号を入力するだけでサインレスで決済することができるようになってきています。これはクレジットカードに IC チップが内蔵されており、IC チップ対応のクレジットカードを持っていること、PIN 番号を知っていることの二つの要素で認証してクレジットカード決済を行っていますのでこれも多要素認証の一つとなります。

ユーザの記憶に頼らない安全な本人確認方法

多要素認証の身近な例をいくつか見てきました。ここで気が付いた人もいると思いますが、パスワードや暗証番号は使用する人が記憶している必要があるのですが、もう一つの要素は IC 対応キャッシュカードそのものであったり、トークンに表示される数字列をそのまま入力していたり、Touch ID に指で指紋を押し付けているだけだったりとこれらはすべて人の記憶は関与 しません。覚えていなくてもよいので忘れる心配はありません。これはパスワードのように推測できないように難しいものや使いまわさないように気を付ける必要がないのです。
多要素認証を使用するシステムでは認証を複数回行うため認証強度は非常に高くなりますが、ユーザがもう一つ複雑なパスワードを覚えておく必要はない ためユーザの負担はそれほど高くなるものではありません。これはセキュリティ上非常に有効な手段であると言えます。

今後の多要素認証の普及

この多要素認証はこれまでは銀行の取引や何かを購入するといった金銭のやり取りが伴うシステムにおいて不正取引が行われないために導入されてきました。しかしこれからは情報そのものを守るためにも多要素認証を使ったセキュリティを高める仕組みが使用されるようになってきます。さまざまな情報漏洩事件からも情報が洩れることの被害は甚大なものとなってきています。これらの情報漏洩リスクを防ぐためにも多要素認証は一つの有効かつリーズナブルな手段となることは確実です。

今回は 身近な例で多要素認証とはどんなものなのかをわかってもらえましたでしょうか。
今後の連載でもう少し詳しく多要素認証について解説していきます。

お問い合わせ
(GMOグローバルサイン株式会社)
03-4545-2303
support-jp@globalsign.com