パスワード

パスワードとは

パスワード（password）は文字通り、関門を通るための「合言葉」です。情報システムの分野だけでなく、社会活動の様々な分野でパスワードによる認証方式が使われています。例えばキャッシュカードやクレジットカードの暗証番号などもパスワードの一種です。

情報システム分野でのパスワードは、パソコンやスマートフォンなどの端末機器や特定の機能・サービスを利用する際に、利用者が本人であることを認証するためのもので、一般的にはユーザーID と対にして使用されます。

パスワードは、本人のみが知るということが前提で、一般的には文字と数字を組み合わせた文字列です。パスワードに用いることができる文字の種類や文字列の長さは、利用する機能や情報サービスによって異なりますが、近年は、数字だけでなく、アルファベット（大文字・小文字を区別）や記号（+-/!"#|_ など）を組み合わせ、より複雑なものを設定するよう求めることが多くなっています。

ちなみに、数字だけのパスワードは、暗証番号あるいは PIN（Personal Identification Number）とも呼ばれます。金融機関の暗証番号は 4 桁が通常ですが、これだと 1 万通りの組み合わせしかありませんので、試行錯誤を繰り返してパスワードが見破られるおそれが高いと言わざるを得ません。このように短いパスワードの場合は、入力の試行回数は 3 回まで、というような少ない試行回数を上限とすることが普通ですが、それでも危険性は残ります。

明らかに、パスワードは複雑なものほど、なりすまし対策として有効なのです。

ユーザーID とアカウント ID

上述で何気なくユーザーID という言葉を使いましたが、最近はアカウント ID という言葉をよく目にされると思います。ユーザーID とアカウント ID はほぼ同じことと考えて差し支えありません。

アカウント（account）とは、直訳すると取引先とか口座という意味で、主に会計的な意味での顧客のことを言います。すなわち、アカウント ID という時のアカウントは、情報

サービスの提供者が、有料であるか無料であるかを問わず、顧客を管理するために開設した口座を意味します。通常、そこには取り引きに関わる諸情報ー氏名その他の会員情報、クレジットカード番号などの利用料の支払いに関わる情報、などが紐づけれています。顧客側から見ると、アカウントを持つということはその業者が提供するサービスを利用する権利がある、ということになります。

強いてユーザーID とアカウント ID とのニュアンスの違いを言えば、ユーザーID は利用者を識別するだけのもの、アカウント ID は取り引きのある利用者を識別するためのもの、ということができるかもしれません。また、ユーザーID は一般にサービス提供者側が付与し、1 つのアカウントに複数のユーザーID を付与することもあるのに対して、アカウント ID は利用者（取引先=支払者）にひとつで、どちらかと言えば利用者のメールアドレスなどをそのままアカウント ID としていることが多い、ということでしょうか。

ということで、以下の解説においては、特に必要のない限り、ユーザーID を用いることにします。

パスワードの決め方と管理の仕方

パスワードが悩みの種であるのは、他人に類推されないような複雑なものであるべきながら、覚えやすいものでないと、実際には使いにくいからです。皆様もこんな思いをされたことがあるのでは？

- 同じパスワードを使わないこと → だからどのパスワードを使ったか分からなくなる
- パスワードは定期的に変更すること → ますますどのパスワードを使ったか混乱する
- 自分や家族の名前、住所、電話番号、誕生日などは使わない → だから覚えられない
- 長いパスワードにしましょう → ますます覚えられない、入力も面倒だ
- パスワードを手帳などに記載しないこと → そうはいっても覚えていられない

実際、利用するすべてのサービスに、別の、ランダムな組み合わせの、長いパスワードを付け、定期的に変更する、ということを守ろうとしたら、パスワード管理ソフト（あるいはサービス）でも使わないと無理です。パスワード管理システムを使うことのデメリット（有料である、それ自体がセキュリティリスクになるなど）もありますので、ここでは、パスワード管理システムに頼らないで、上記悩みを解決する方法はないか考えることにします。

ここから先は、筆者の個人的な考え方です。異論もあるかと思います（特にセキュリティの専門家からは）が、こんな考え方もあるんだ、程度にお読みください。

1. どんなに複雑なパスワードに設定しても、流失やハッキングされたら意味がなく、ユーザーID とパスワードでの認証方式である限り、なりすましされる危険性は残る。銀行系のウェブサイトなど、なりすましされた時に直接的に被害を被るおそれのあるサイトに対してはワンタイムパスワード（後述）を使う。
2. そうはいっても、パスワードを簡単に類推されるのでは問題である。少なくとも文字種の組み合わせと長さには配慮する。
3. 文字列として、自分の覚えやすい事柄や数字列を使うのは構わないことにする。ただし、それを単純に組み合わせるのではなく、自分のルール（その 1）で組み合わせ・加工することで、複雑度を高める。
4. パスワードの使い回しはしない。自分のルール（その 1）の中にサービス事業者の区別の付け方を組み込む。
5. 利用サービス、ユーザーID、パスワード、パスワード設定日、などを一覧表の形で登録したパスワード管理リストを Excel で作成し、その Excel ブックをパスワード付きで保存する。この Excel ブックのパスワードだけはメモを取らず覚えこむ。
6. パスワード管理リストに記載するパスワードはパスワードそのものでなく、パスワードの一部を伏せるなど、自分のルール（その2）で加工したものとする。
7. Excel ブックはオンラインストレージサービスを利用して、バックアップとするとともに、家のパソコンでも、スマートフォンでも見れるようにする。

ポイントとなるのは、3 の「覚えやすい事柄や数字を、自分のルール（その 1）で組み合わせ・加工する」ということです。パスワードは覚えられなくても、自分で決めたルールは忘れないでいられるでしょう。
ルールは以下のような観点で考えると良いでしょう。

- 事柄を何にするか
- 数字列を何にするか
- いくつを大文字にして何文字目にするか
- 記号は何を使い何文字目にするか、記号を使えない場合はどうするか
- サービス事業者の区別をどうつけるか
- 組み合わせ方をどうするか
- パスワード文字数が短い場合にはどうするか
- 定期的に変えなければいけない時はどうするか

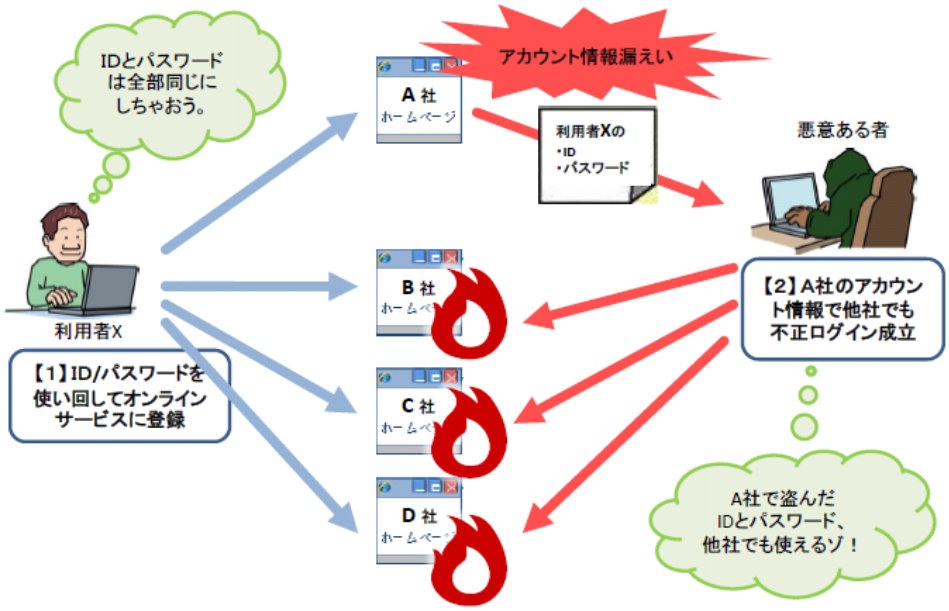
インターネットで「パスワード　決め方」などで検索すると、参考になる例が見つかると思います。

5 のパスワード管理リスト上のパスワードを「自分のルール（その 2）で加工」することと、Excel ブックにパスワードを付けて保存するのは、盗難や紛失への対策です。Windows の「メモ帳」ではパスワード付きの保存はできませんので、Excel の利用をお勧めします。

パスワード使い回しの危険性

悪意のある者が、何らかの方法で事前に入手した ID とパスワードのリストを流用し、自動的に連続入力するプログラムなど使って、色々なウェブサイトに不正ログインを試みる手口をパスワードリスト攻撃と言います。ここでログインが成立した ID とパスワードの組み合わせはその後、他の不正アクセスに悪用され、最終的には直接金銭的被害に結びついてしまうこともあります。

注意すべき点は、パスワードリスト攻撃においては、その元となる ID とパスワードは、個人のパソコンからではなくインターネットサービスのサーバから盗み取られている場合が多い、ということです。つまり、利用者側で強固なパスワードを設定し、かつパソコン上でセキュリティソフトを利用して守っていても、同一のパスワードを使い回している限り、パスワードリスト攻撃の被害を防ぐことはできません。



パスワードリスト攻撃 （出典：IPA）

ワンタイムパスワード

ワンタイムパスワードとは、文字通り 1 回しか使えない「使い捨てパスワード」、およびそれを採用した認証の仕組みのことです。

ワンタイムパスワードでは、認証を行うたびに毎回異なるパスワードを使用し、一度使用したパスワードは再利用せずに使い捨てにします。万が一、ワンタイムパスワードを窃取されたとしても、すでに使われたワンタイムパスワードは再度使うことはできないので、安全性が向上します。
それに加えて、一般的に有効期間が 30 秒～1 分程度で、とても短いのも特徴です。不正を目論む者にパスワードを破る時間的な余裕を与えないことも有効な対策となっています。

ワンタイムパスワードは、不正アクセスを防ぐ有効な手法として、主に金融機関のインターネットバンキングなどに普及していて、徐々にオンラインゲームなどの他のサービスにも広がっています。インターネットバンキングでは、各種サービスへのログインだけでなく、口座からの送金など、慎重さが求められる操作する際にもワンタイムパスワードでの認証がされます。

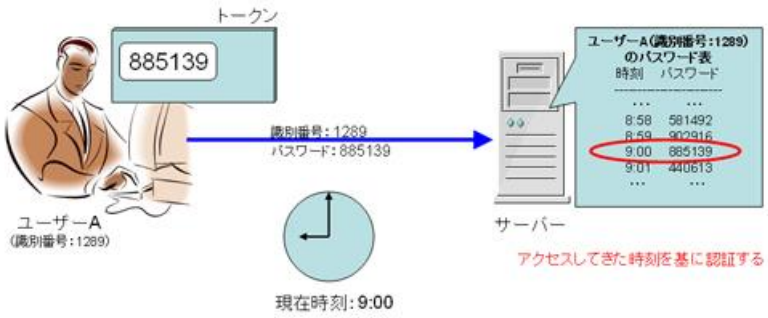
ワンタイムパスワードを生成する方式には、タイムスタンプ方式（タイムシンクロナス方式、時刻同期方式ともいいます）とチャレンジ・レスポンス方式の 2 通りがあります。ここでは、銀行系で一般的なタイムスタンプ方式についてのみ解説します。

タイムスタンプ方式

タイムスタンプ方式では、トークン（token）というツールを利用して、ワンタイムパスワード（一般的には 6 桁の数字）を生成します。認証を行う際には、ユーザーはユーザーID とトークンに表示されたワンタイムパスワードを送信します。認証サーバ側では、あらかじめ把握してあるユーザーとトークンの情報および時刻を判断して、送られてきたワンタイムパスワードが、本人のものであるかどうかを判断する仕組みです。

この方式は、タイムスタンプという名の通り、ワンタイムパスワードを生成するための情報として時刻を使います。そのため、認証サーバとトークンの間で時刻の同期がとれていることが必要です。ただし物理的に別のものですので、時刻の厳密な同期はできません。そのため認証サーバには時刻のずれを吸収するような仕組みも備えられています。

トークンという用語は、もともとの意味が「しるし」「証拠」「記念品」「引換券」「形ばかりの」などであることから、例えば、地下鉄やバスなどの代用通貨とか、商品券・図書券などのことを指したり、通信や仮想通貨の分野でも使われたりします。ワンタイムパスワードでのトークンは、正確には「セキュリティトークン」のことで、ワンタイムパスワードを発行する器具（ハードウェアトークン）またはアプリ（ソフトウェアトークン）を指します。



タイムスタンプ方式の仕組み　（出典：日経 X TECH）

ワンタイムパスワードで利用されるハードウェアトークンは、主にキーホルダー型とカード型の 2 種類です。

【キーホルダー型】
小さく、ボタンも一つしかないため、使いやすい

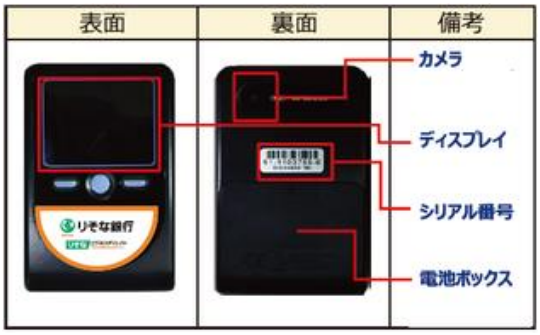
キーホルダー型トークン　（SQUARE ENIX）

【カード型】
薄く、お財布やカード入れなどに入れて持ち運びやすい。10 キーのキーボードが付いているものが多い。

カード型トークン　（浜松信用金庫）

銀行系などでは、もともとキーホルダー型の専用トークンを採用していましたが、トークンの紛失・盗難時の不正取引の防止強化のため、振り込みをする際に相手の口座番号などを入力してパスワードを生成することのできる、カード型のトークンに移行しています。

りそな銀行では、キーボードの代わりにカメラを内蔵したカード型トークンを発行しています。



カメラ内蔵型トークン （りそな銀行）

ソフトウェアトークンは、ワンタイムパスワードをパソコンやスマートフォン等の画面上に表示するアプリケーションのことです。ハードウェアトークンという専用機器を配布しないで済むので、スマートフォンの利用拡大に伴って各銀行では積極的にこのアプリの利用を呼び掛けています。

ソフトウェアトークン画面例

（Google Play Store）