

ともに学ぶ。考える。 情報セキュリティ対策

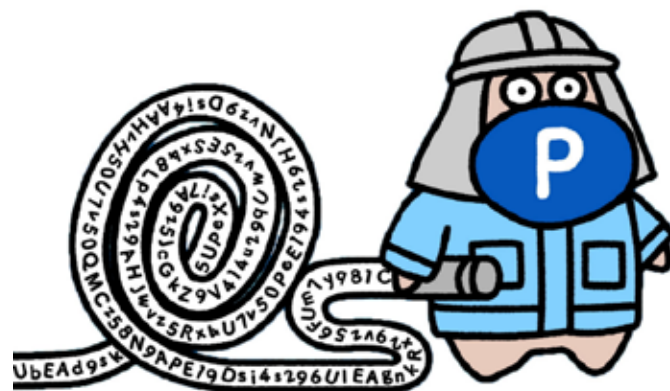
～大人もこどもも一緒に学び、考える。インターネットとのつきあい方～

【3】パスワード



あなたはID,パスワードを 作成したことがありますか？

心の中で
教えてください♪



インターネットの様々なサービスを利用するときに、多くの人がIDやパスワードを作成した経験があるのではないのでしょうか？
ではあらためてIDやパスワードとは何か？を考えてみましょう

インターネット上でいろいろなサービスを利用する場合の権利



アカウントとはインターネット上でいろいろなサービスを利用する場合の権利、といえます。利用者の区別と個別情報の管理などに必要なものです。
もちろんアカウントを簡単に作成することは推奨できません。
サービス内容、本当に必要か、信頼できる提供元か、などをきちんと確認する必要があります。

ID（アイディー）とは

インターネット上でいろいろなサービスを利用する場合、個人を特定するために必要なモノ



IDとは「Identifier」の略称です。
ユーザー名、アカウント名などと呼ぶこともあります。
インターネット上でサービスを利用する場合、「このサービスを使うのは私です」と
しっかり特定するために必要なモノになります。
メールアドレス、ニックネーム、本名、ランダムな文字列などが使われます。

利用者本人を識別するための確認手法

IDとパスワードを組み合わせて確認する方法が一般的



認証とは「本当にその人か？」を確実に確認するための手法です。IDの本人であることを確認する手段として、当初同時に登録したパスワードを合わせて認証する方法が一般的です。

IDもパスワードもそれぞれ「自分であること」を示すために必要なものであり、他の人に知られてはいけません。

お手軽パスワード？



IDやパスワード情報が漏れると、第三者が自分になりすまし、パソコンやスマホでインターネット上のサービスに不正ログイン、個人情報漏洩など被害にあう可能性があります。第三者に簡単に割り出すことができる「お手軽パスワード」も危険です。パスワードは長く、複雑にして、使いまわさないことが大切です。

危険なパスワードとは

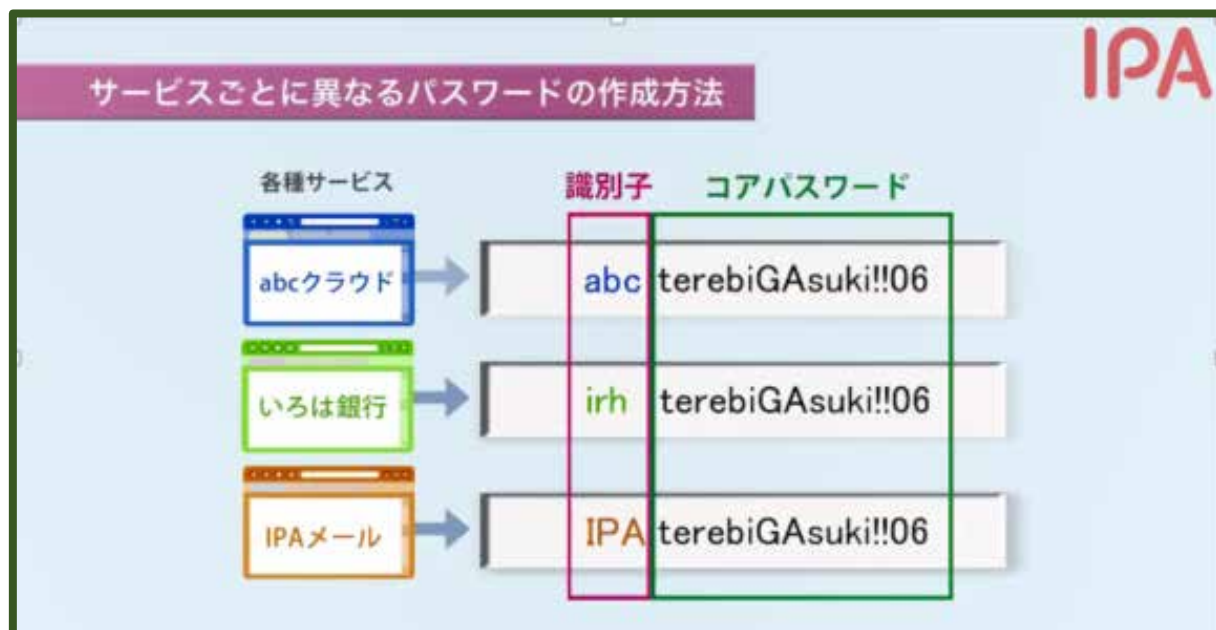
- ・ IDとパスワードが同じ
- ・ 名前・電話番号・誕生日をそのまま使用
- ・ 「1234」や「abcd」や「1111」など
単純な羅列
- ・ 様々なサービスで同じパスワードを使う
- ・ パスワードを人に教える



危険なパスワードとして、上記にあげたようなパスワードを使用していないでしょうか？使用しているパスワードが、簡単に推測されないか、今一度、確認してみましょう。

推奨されるパスワード設定例

- 私だけの「コアパスワード」の設定。
- サービスごとの識別子をプラス。



推奨されるパスワード設定例として、コアパスワードを作成することがあげられます。例えば「テレビが好き」といった言葉をローマ字表記にし、記号や数字を付けて自分のコアパスワードとして作成します。サービスごとに異なる識別子、例えばサービスの頭文字などを、コアパスワードの頭や最後に付けると、パスワードの使いまわしを防ぐことになります。

コアパスワードと識別子を別々に管理

- コアパスワードは暗記がベスト
- 暗記できなければメモを保存
- サービスごとの識別子は電子ファイルか紙で保存

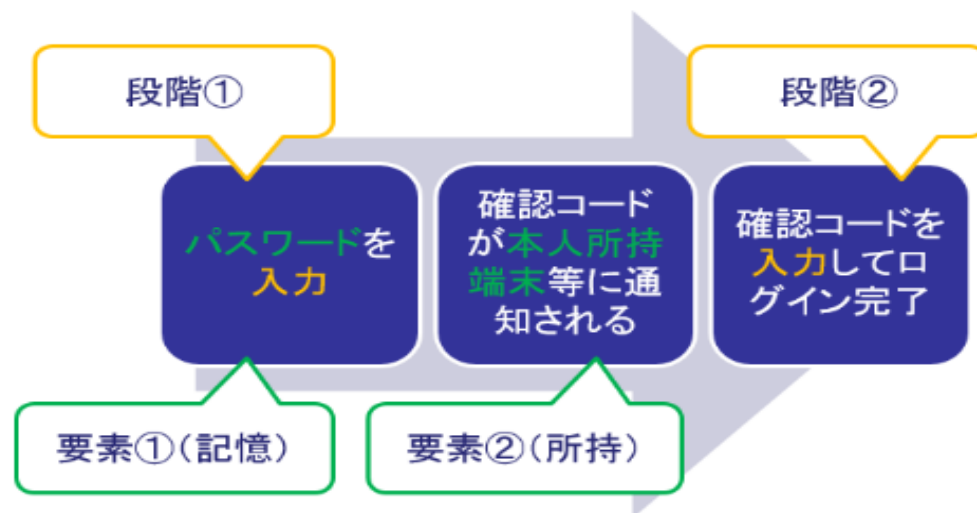


パスワードの管理方法として、コアパスワードと識別子を別々に管理することが大切です。特にコアパスワードは暗記がベスト。サービスごとの識別子は電子ファイルか紙に書いて保存しましょう。

多要素認証とは

認証の3要素である、①パスワードなどの「記憶」、②キャッシュカードなどの「所持」、③指紋などの「生体情報」のうち、2つ以上の要素で認証する方式

「多要素認証」 イメージ



最近ではパスワードだけでなく、もう一つの要素（ワンタイムパスワード、指紋や顔）などを使って、初めてサービスが利用できる「多要素認証」方式も増えています。

「多要素認証」を利用している場合、仮にIDおよび1つ目のパスワードを不正利用されてもログインはできないことから、不正ログイン防止に効果があります。多要素認証を提供しているサービスは積極的にその設定を行ってください。

秘密の質問の答えにも工夫を

- これまでの質問と答え

Q.好きな食べ物は？

A.ラーメン

Q.母親の旧姓は？

A.藤井

Q.ペットの名前は？

A.コロ

- 共通フレーズを追加する

Q.好きな食べ物は？

A.ラーメン **カモしれない**

Q.母親の旧姓は？

A.藤井 **カモしれない**

Q.ペットの名前は

A.コロ **カモしれない**

初めに設定した秘密の質問に対する答えを確認する認証方法もあります。その場合の答えにも工夫をしましょう。アンサーに共通フレーズを追加するだけで、あなたのオリジナルの認証になります。

IDとパスワードの設定や管理の大切さを知り、不正ログインによる被害やトラブルに遭わないようにする。

私たちがインターネットを活用する上で、自分自身を守るセキュリティの意識が大切です。

IDとパスワードの設定や管理の大切さを知り、不正ログインによる被害やトラブルに遭わないようにしましょう。

確認テスト 問題

(3)パスワード

Q3-1

パスワードを設定する際に推奨されるものはどれでしょう。

選択肢	
	1. できる限り長く複雑に、同じパスワードを使い回さない
	2. 自分や家族の名前や誕生日などにパスワードを設定すると覚えやすい
	3. 複数サービスで同じパスワードに設定すると忘れにくい

次のページで正解と
解説を確認しましょう

確認テスト 正解と解説

Q3－1

パスワードを設定する際に推奨されるものはどれでしょう。

正解	選択肢
●	1. できる限り長く複雑に、同じパスワードを使い回さない
	2. 自分や家族の名前や誕生日などにパスワードを設定すると覚えやすい
	3. 複数サービスで同じパスワードに設定すると忘れにくい

【解説】

パスワードは長く、複雑にして、使いまわさないことが大切です。

危険なパスワードは以下になります。

- ・IDとパスワードが同じ
- ・名前・電話番号・誕生日をそのまま使用
- ・「1234」や「abcd」や「1111」など単純な羅列
- ・様々なサービスで同じパスワードを使う
- ・パスワードを人に教える

使用しているパスワードが、簡単に推測されないか、今一度、確認してみましょう。

確認テスト 問題

(3)パスワード

Q3-2

「多要素認証」の説明で間違っている内容はどれでしょう。

選択肢


- | | |
|--|--|
| | 1. インターネットサービスにログインする際の、複数の要素(記憶、所持、生体情報)を用いた認証方式である |
| | 2. 仮にIDおよび1つ目のパスワードを不正利用されてもログインはできないことから、不正ログイン防止に効果がある |
| | 3. 「コアパスワード」を設定し、サービスごとに識別子をプラスすることで管理が楽である |

次のページで正解と
解説を確認しましょう

確認テスト 正解と解説

Q3-2

「多要素認証」の説明で間違っている内容はどれでしょう。

正解	選択肢
	1. インターネットサービスにログインする際の、複数の要素(記憶、所持、生体情報)を用いた認証方式である
	2. 仮にIDおよび1つ目のパスワードを不正利用されてもログインはできないことから、不正ログイン防止に効果がある
	3. 「コアパスワード」を設定し、サービスごとに識別子をプラスすることで管理が楽である

【解説】

多要素認証とは、
認証の3要素である

- ①パスワードなどの「記憶」
- ②キャッシュカードなどの「所持」
- ③指紋などの「生体情報」

のうち、2つ以上の要素で認証する方式です。