

多要素認証って何？

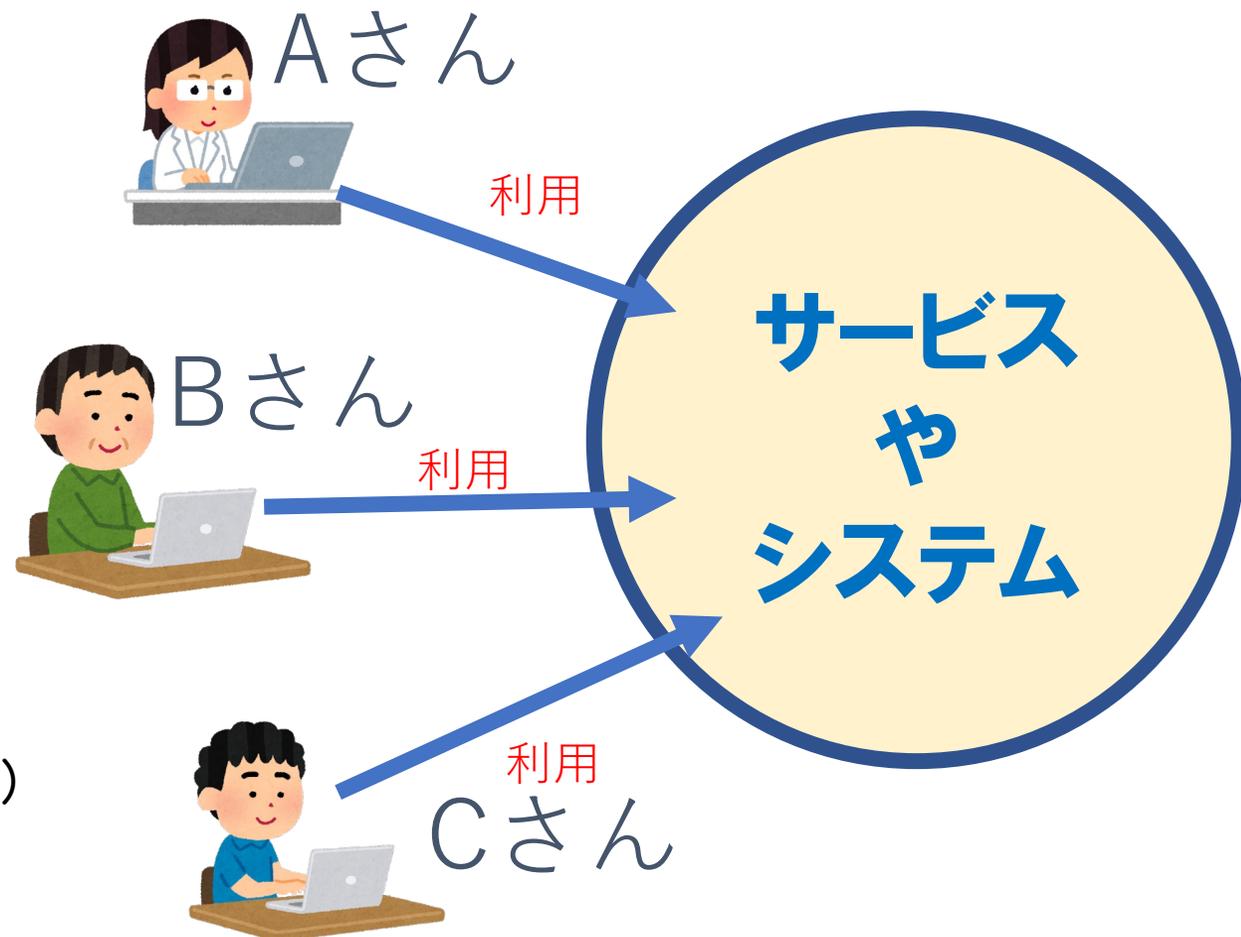
どうして必要なの？

情報戦略機構

認証って何？

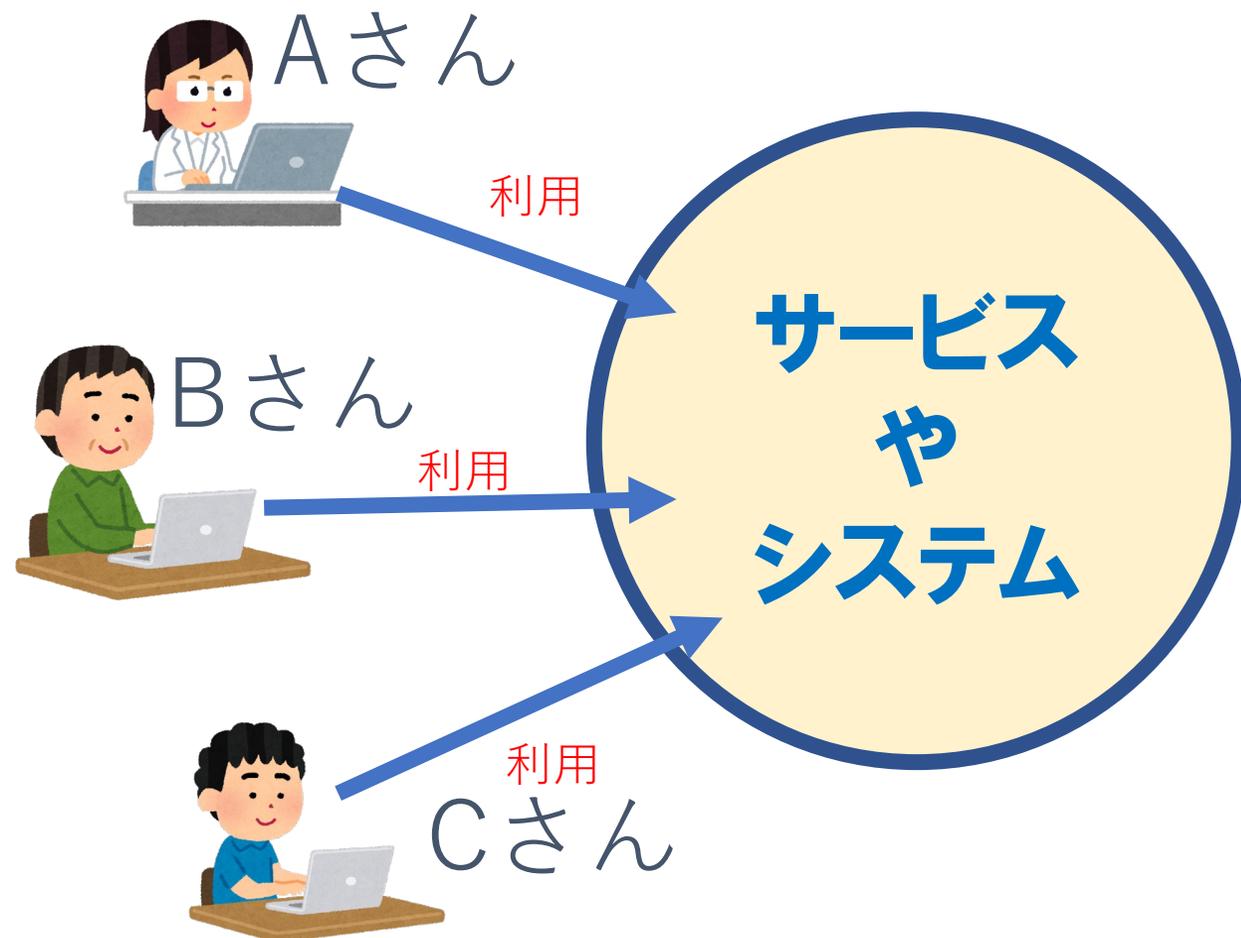
- システムやサービスを利用するときに、IDとパスワードを入力します。
- この手順を「認証」と言います。
- サービスやシステムを、**利用する権利がある人だけ**に使ってもらうために必要です。

以下のようなときには必須です
使う人を区別して動くもの（例：メールサービス）
使う人を限定するもの（例：文書庫）



認証って何？

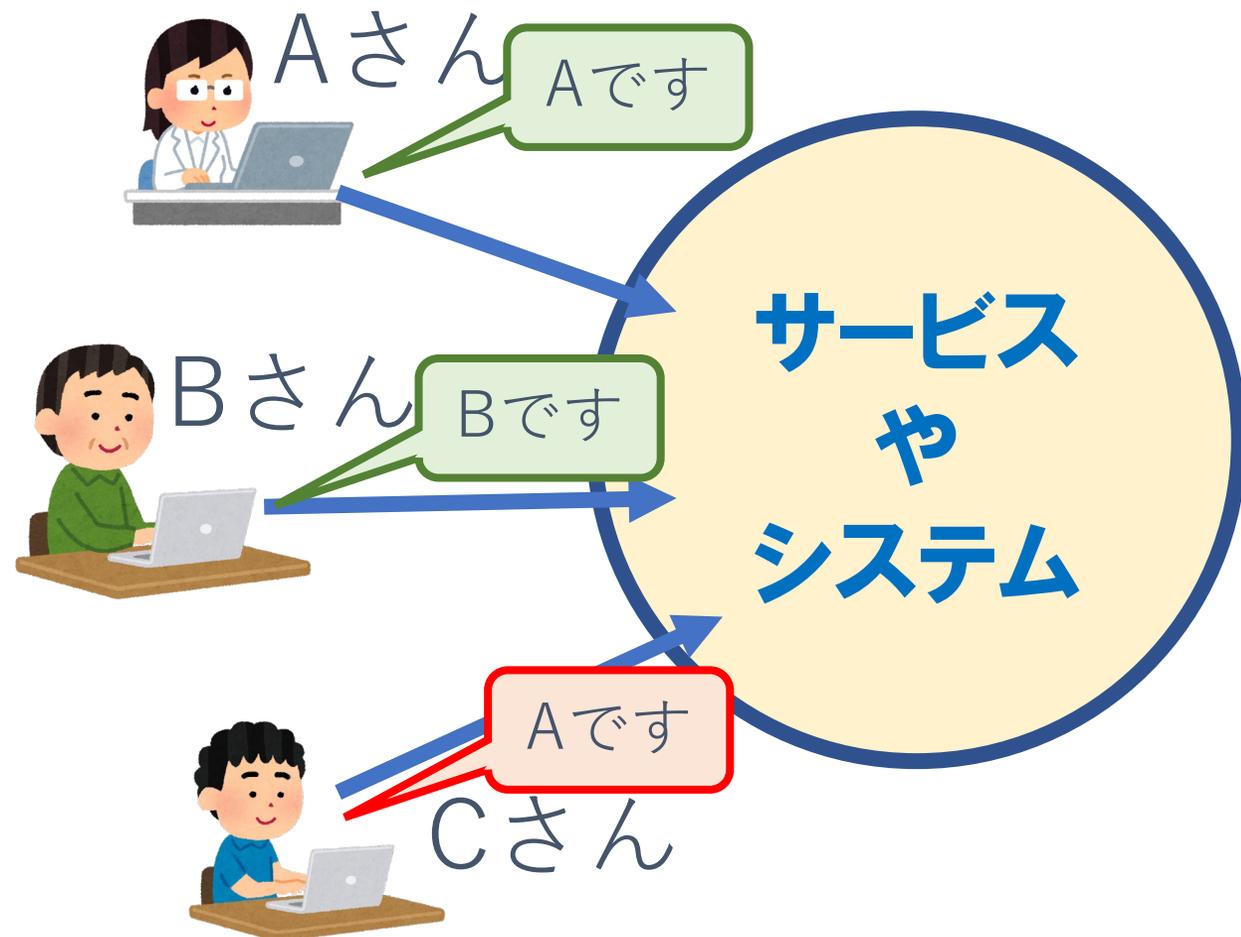
- 正確にいうと、「**認証**」とはサービスやシステムを使おうとしている人が**誰なのか**を**チェック**すること。



認証って何？

誰なのかをチェックする

- 「誰なのか」は名乗ってもらわないとわかりません。
これが「ID」の入力です。
- でも他人の名をかたることもできますよね。



認証って何？

誰なのかをチェックする

- 「確かに本人であること」をチェックするには？
 - 本人だけが知っていることを本当に知っているかチェック
(例：合言葉)
 - 本人だけが持っているものを本当に持っているかチェック
(例：身分証の提示)
 - 本人かどうかを直接チェック
(例：顔パス)

認証の要素

チェック方法には様々な方法がありますが、大きく3つに分類できます。

知識情報：パスワード、合言葉、秘密の質問

所持情報：身分証、スマホ（携帯電話）

生体情報：顔、指紋、静脈、虹彩



茨城大学

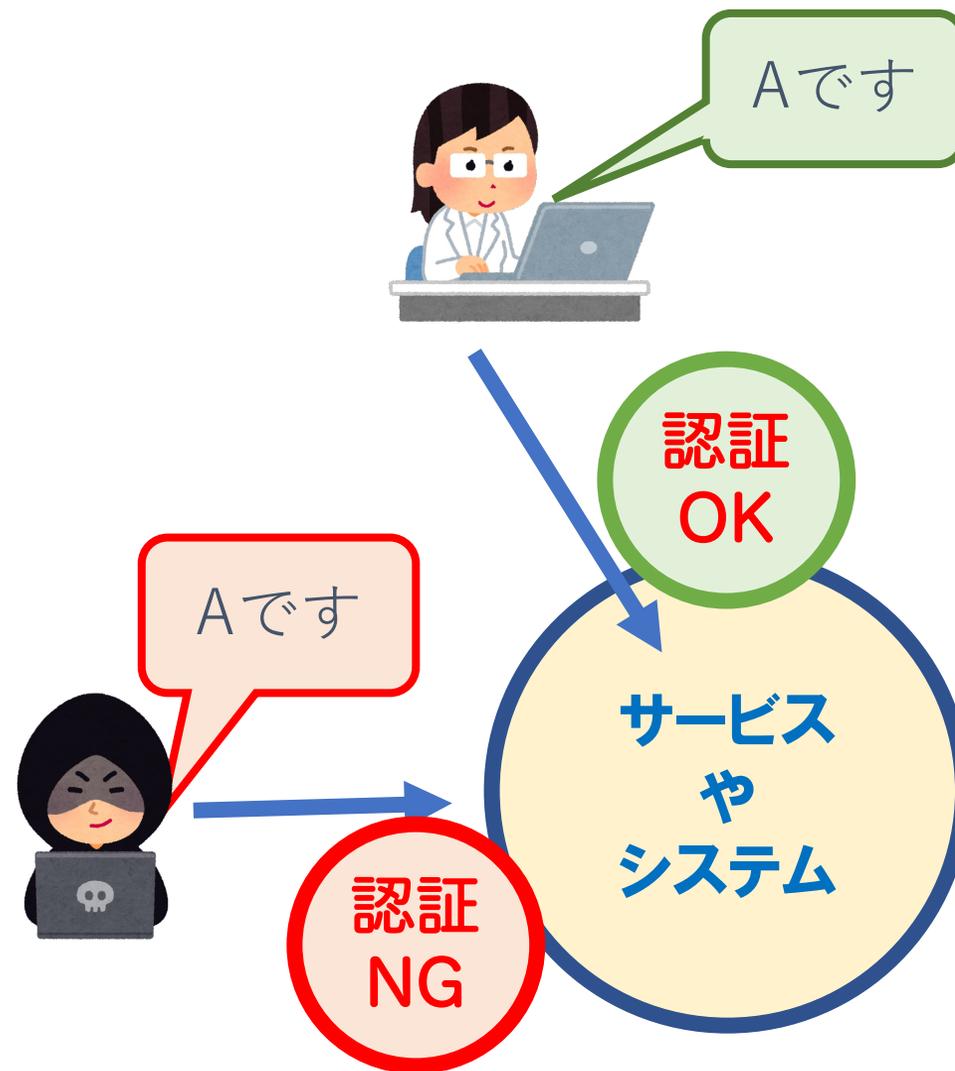
組織アカウントを使用してサインインしてください

yourID

パスワード

サインイン

認証の目的は
システムやサービスの
不正利用を防ぐこと
です。

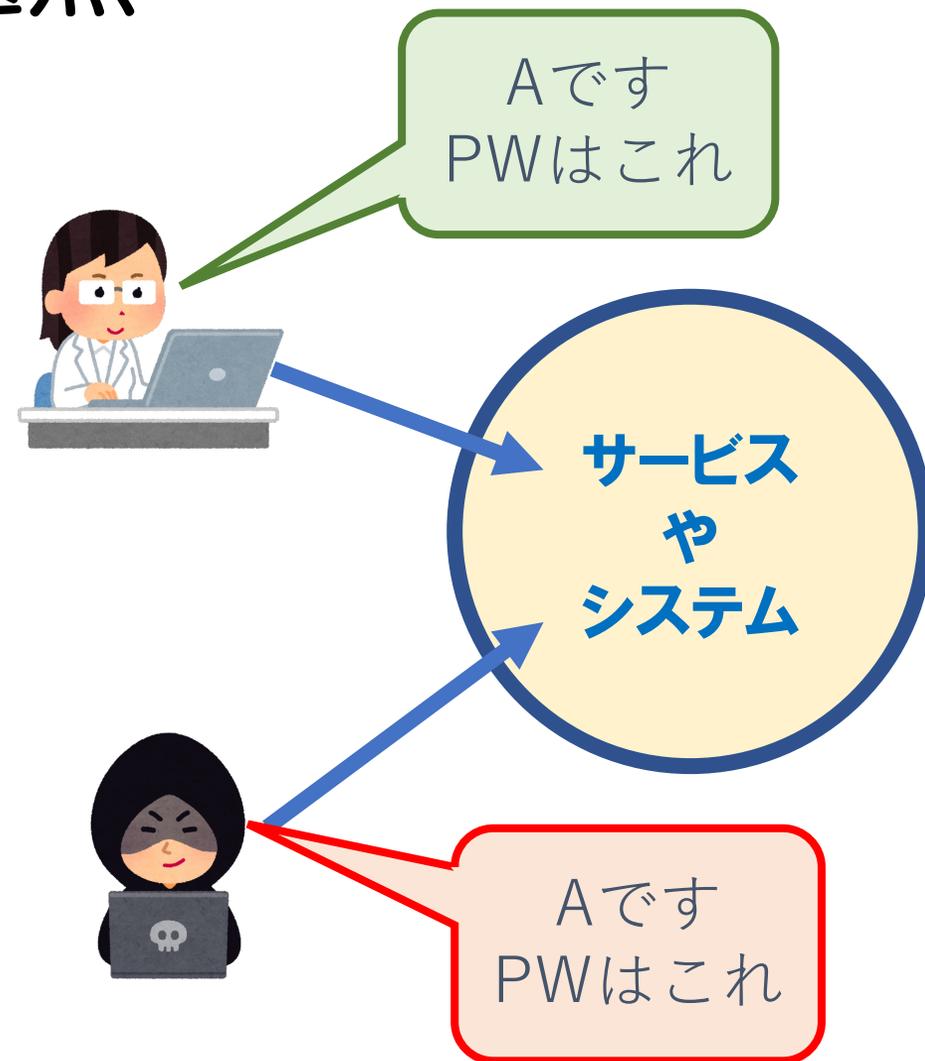


パスワード認証方式の問題点

- IDとパスワードが一致すれば、
本人でなくとも
サービスやシステムが利用できる。



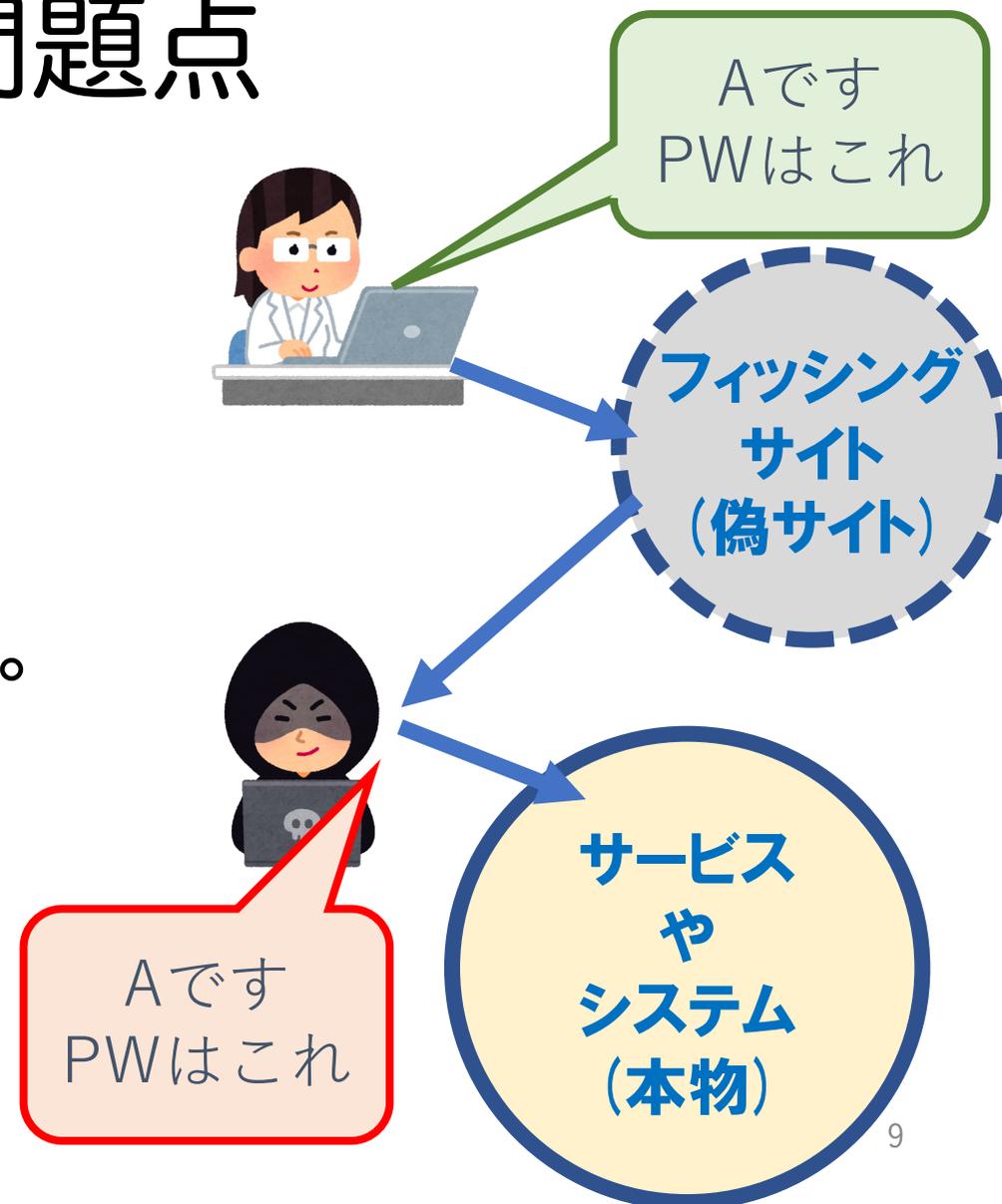
- パスワード認証方式では、
パスワードをしっかりと管理し、
他人に漏らさないことが重要。



パスワード認証方式の問題点

個人の注意だけでは防げない時代です

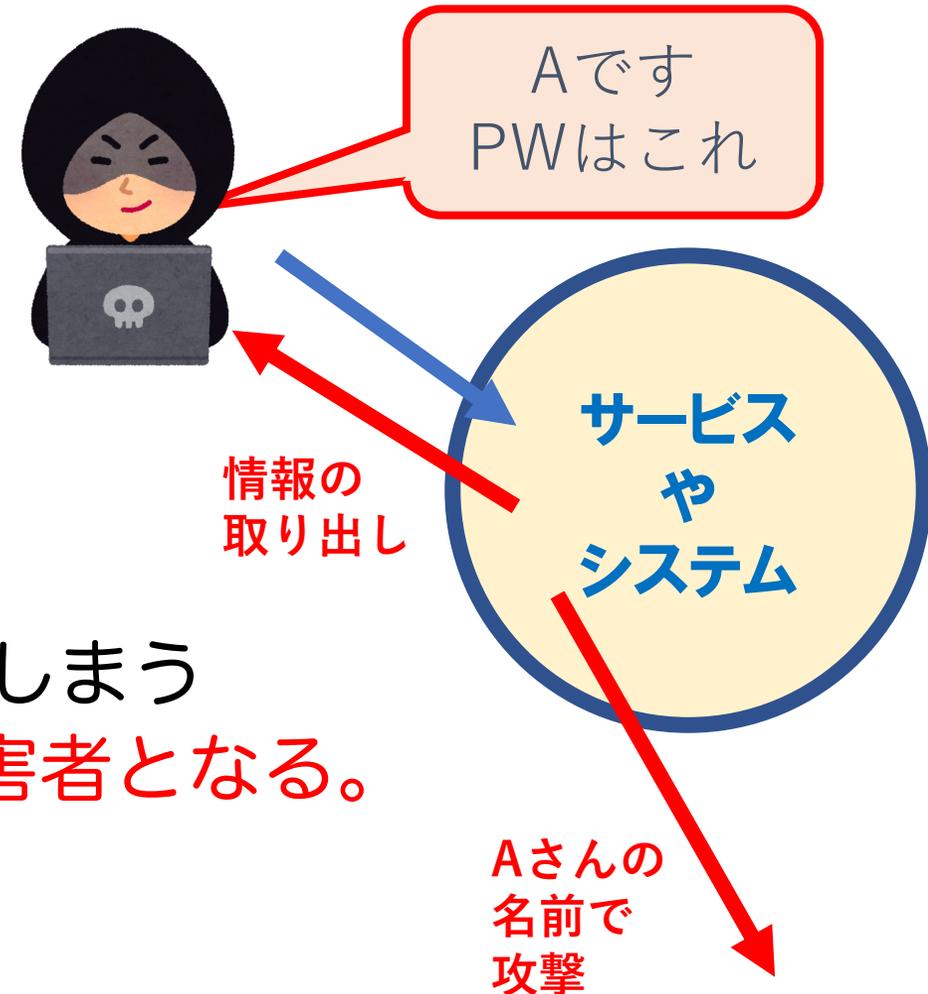
- フィッシングにひっかかって、自ら攻撃者に漏らしてしまう。
(ひっかかった人には自覚がない)
- 攻撃者が適当に試したら偶然一致した。
(プログラムを使うので、いくらでも試せる)
- 複数のサービスで同じパスワードを使っていて、他所で漏洩した。
(個人にできる防衛は同じパスワードにしないこと)



システムに侵入されたら

攻撃者に悪用された場合、

- システムに格納されている情報を取り出されてしまう
→情報漏えい
(内容によっては莫大な損害賠償)
- 外部への攻撃の踏み台として利用されてしまう
→Aさん (や本学) がサイバー攻撃の加害者となる。



多要素認証って何？

- 本人チェックのときに、**複数の要素**を使うこと。

知識情報：パスワード、合言葉、秘密の質問

所持情報：身分証、**スマホ**（携帯電話）

生体情報：顔、指紋、指静脈、虹彩

登録された**パスワード**を
知っているか

+

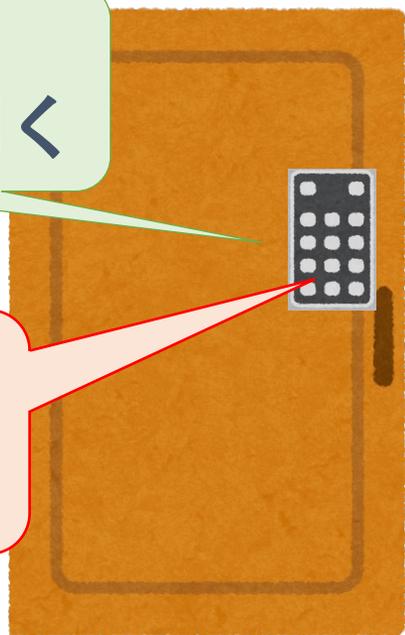
登録された**スマホ**を
持っているか

多要素認証って何？

扉の鍵を増やすイメージ

暗証番号を
知っていれば開く

正解を知らなくても
誰でも試せる。
偶然開くかも。



パスワード認証のみ

両方使うことで、
強度アップ

鍵を持って
いれば開く

鍵を拾った人も
開けられる

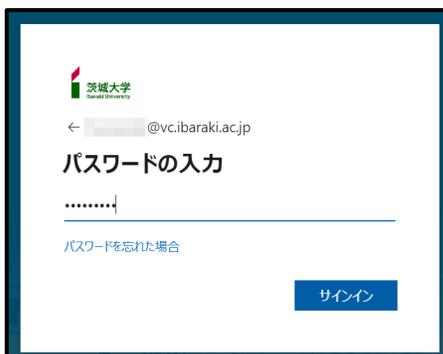


多要素認証

多要素認証の流れ（一例）

登録されたパスワードを
知っているか

登録されたスマホを
持っているか



Aです
PWはこれ



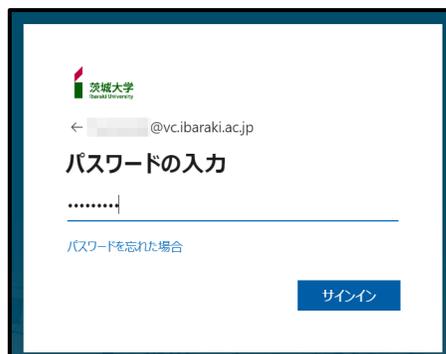
登録されたスマホに
承認要求が届く。
PCの画面に表示され
ているコードを
スマホに入力



多要素認証を攻撃者からみると（一例）

登録されたパスワードを
知っているか

登録された携帯電話を
持っているか



認証
NG



Aです
PWはこれ

登録されたスマホを
持っていないので
コードを入力する
承認画面がない。



多要素認証の流れ（一例）

登録されたパスワードを
知っているか

登録されたスマホを
持っているか



Aです
PWはこれ



登録されたスマホに
承認要求が届く。
PCの画面に表示され
ているコードを
スマホに入力



茨城大学の多要素認証に利用できる機器

認証方法	必要な条件	例	認証時に利用者が行うこと
認証アプリに入力	アプリが動きかつ通信ができること	スマホ、WiFiで接続されたタブレット	PCなどの認証画面に表示されるコード(数字)を認証アプリの承認画面に入力する。
認証アプリでコード取得	アプリが動く機器(通信は不要)	スマホ、タブレットなど	認証アプリに表示されるコード(数字)をPCなどの認証画面に入力する
SMSでコード取得	SMSが受信できる機器	スマホ、タブレット(回線契約付)、携帯電話など	SMS(ショートメッセージ)で届いたコード(数字)をPCなどの認証画面に入力する
電話	通話を受けられる電話	スマートフォン 携帯電話 固定電話 (非推奨)	登録した電話機で通話を受け、音声案内に従い、「#」を押す

認証の目的は、
システムやサービスの
不正利用を防ぐこと
です。

- みなさんのアカウントはシステムへの入り口です。
- 効果を発揮するには全利用者が設定することが必要です。

