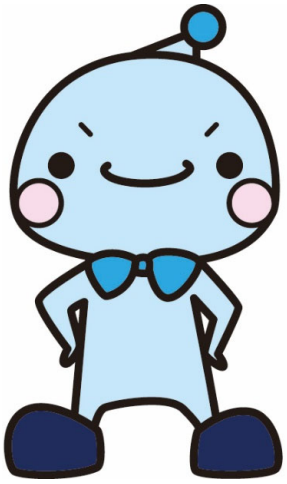
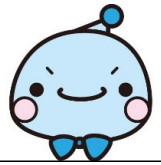
Java



盛岡情報ビジネス&デザイン専門学校

★☆★本日の内容★☆★

1. ハッシュとは
2. ユーザ登録処理の流れ



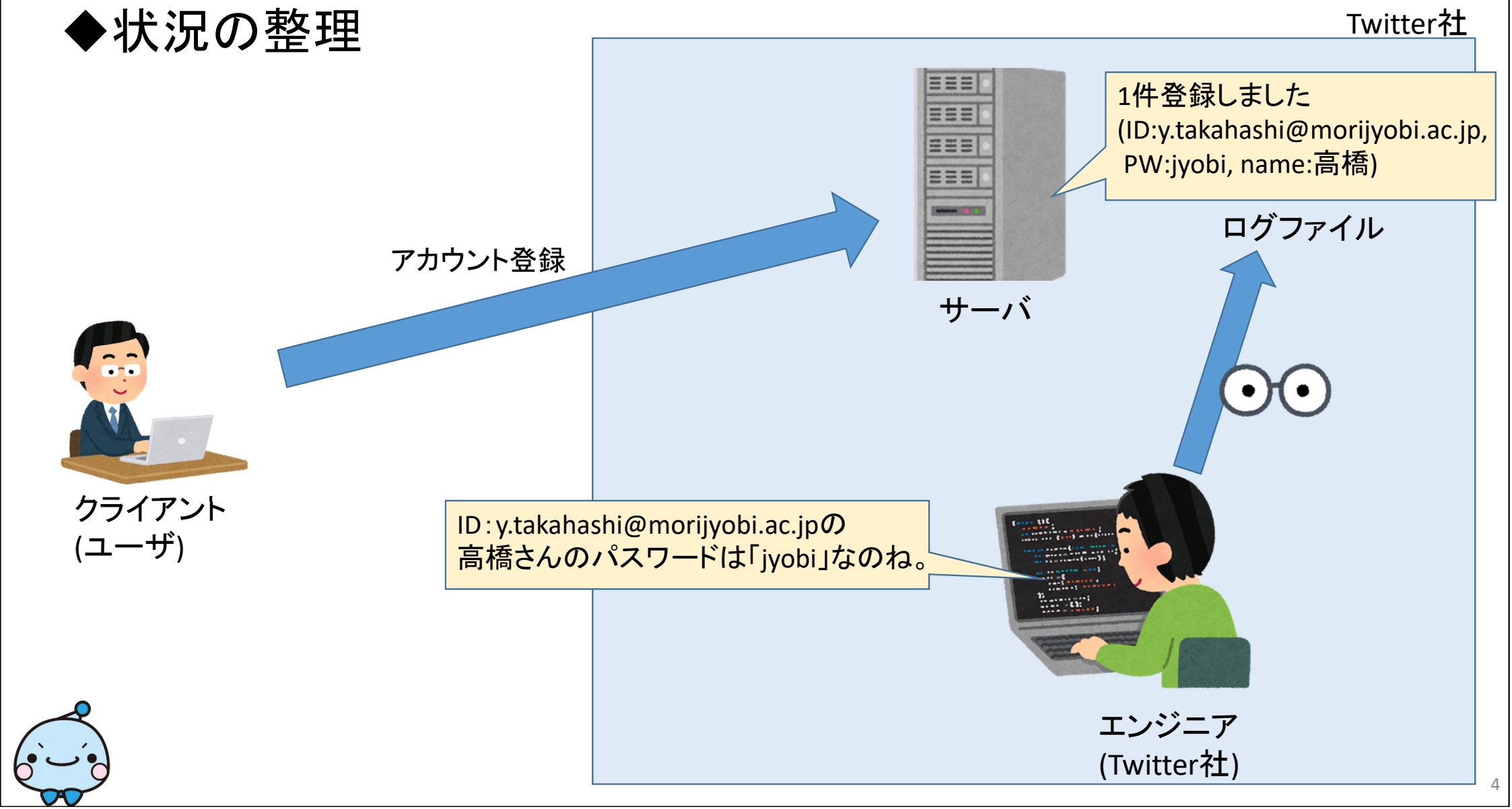
2018/5/4
とある事件が起きました。
Twitter社の発表

パスワードを
「平文」で
ログに出力していました。

When you set a password for your Twitter account, we use technology that masks it so no one at the company can see it. We recently identified a bug that stored passwords unmasked in an internal log.

つまり、社員はシステムのログであなたのPWを見ることができてしまっていました！

◆状況の整理


Twitter社
1件登録しました
(ID:y.takahashi@morijyobi.ac.jp,
PW:jyobi, name:高橋)
ログファイル
アカウント登録
サーバ
クライアント
(ユーザ)
ID:y.takahashi@morijyobi.ac.jpの
高橋さんのパスワードは「jyobi」なのね。
エンジニア
(Twitter社)

◆理想の姿

ログファイル、DBの中身等どこにも平文のパスワードが存在しない状態になっていること。

クライアント
(ユーザ)

アカウント登録

Webサーバ

1件登録しました
(ID:y.takahashi@morijyobi.ac.jp,
PW:34a64d0c169485eaf1ef7b60a10866802a9aac137b9baab18ade68c5b7cf6a32, name:高橋)

ログファイル

DB登録処理(INSERT)

Twitter社

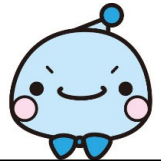
DBサーバ

ID	PW	名前
001	34a64d0c1・・・a32	高橋
002	a10866802d・・・e68	髙田
003	7b9bab18ad・・・7cf	細川

なるほど。
ID:y.takahashi@morijyobi.ac.jpの
高橋さんが新規で会員登録したのね。
PWはハッシュ化されて分からないね。
ヨシ！

エンジニア
(Twitter社)

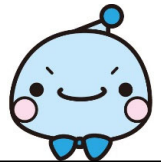
SELECTしてテーブルの中身を見てもPWはハッシュ化されていて分からないね。ヨシ！



◆パスワードハッシュとは

PWの文字列をハッシュ関数を使って意味を持たない16進数の固定長の文字の羅列に変換すること。(下記の例は16進64桁にハッシュ)

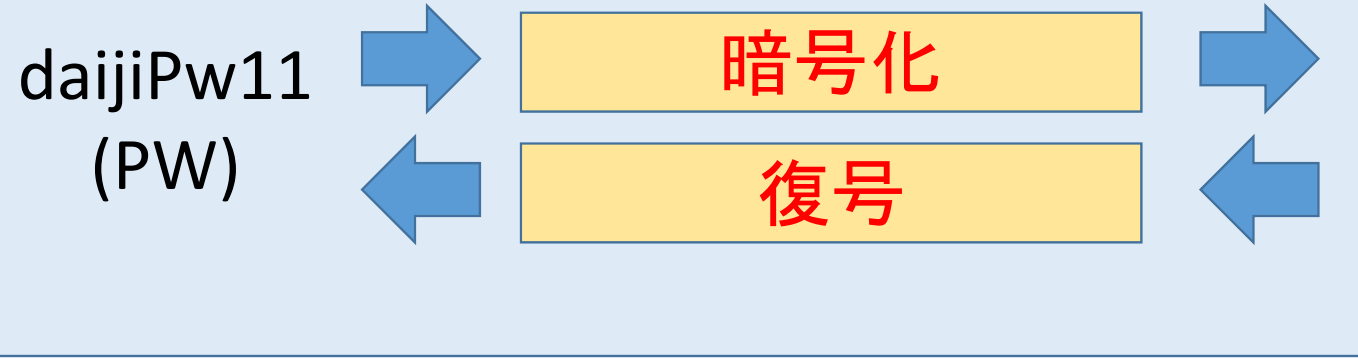
ハッシュ関数は出力値から入力値を得ることが困難であるという特性(**一方向性、不可逆性**)を持っている。



◆ハッシュと暗号化の違い

ハッシュ(復元できない)

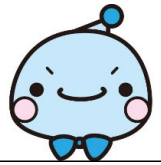
暗号化(復元できる)



◆有名なハッシュアルゴリズム

MD5　(Message Digest Algorythm 5)

入力値から128bit(16進数32桁)のハッシュ値を出力するアルゴリズム
衝突耐性が低いため、現在はセキュリティ用途ではなく、ファイルの
チェックサムなどに利用するのが主な目的です。



◆有名なハッシュアルゴリズム

SHA-2

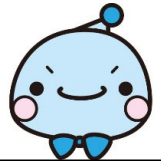
・SHA256

入力値から256bit(16進数64桁)のハッシュ値を出力するアルゴリズム

・SHA512

入力値から512bit(16進数128桁)のハッシュ値を出力するアルゴリズム

セキュリティ強度はSHA512の方が高いですが、出力するための負荷が高いため、負荷と強度のバランスを考えてSHA256が良く使われています。SHA256でも現在のCPUの計算能力では現実的な時間でハッシュ値から元の値を計算することができません。



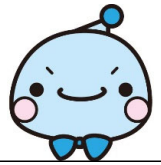
◆さらに安全なPWの保存方法

実は単純にハッシュするだけではまだまだ安全とは言えません。

さらにセキュリティ強度を高めるには下記の2つの対策も加えて採用する必要があります。

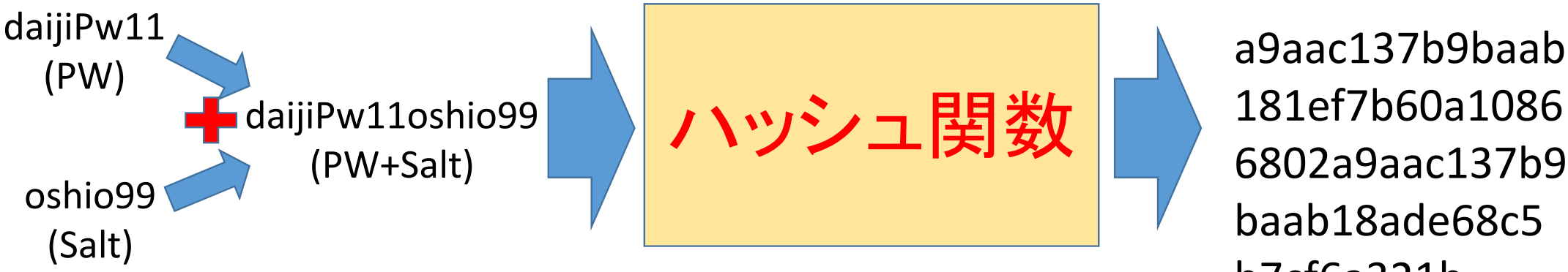
・ソルト

・ストレッチング



◆ソルトとは

ハッシュ値を算出す際は「ソルト」と呼ばれるものを加えてハッシュするのが一般的です。



ソルトを使用する際は下記に注意して実装しましょう。

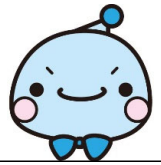
・ユーザごとに異なるソルトを使用する。

・ある程度の長さのソルトを使用する。(20文字以上推奨)

そうすることによって、下記の効果を得ることができます。

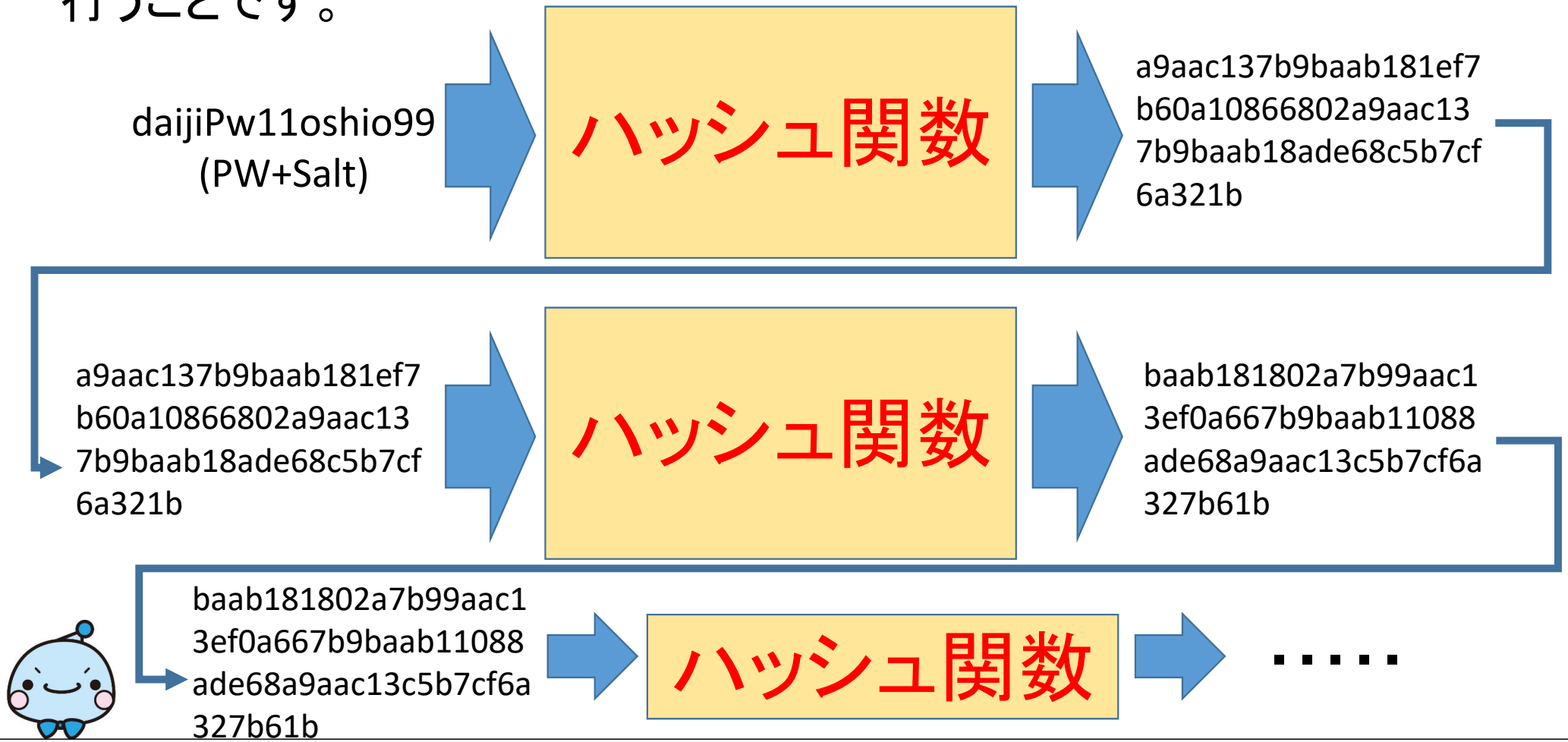
・同じPWでも異なるハッシュ値を算出する。

・入力文字列を長くし、逆引きの計算量を増加させる。



◆ストレッチングとは

ストレッチングとはハッシュ値の計算を何回も(1000～数万回程度)繰り返し行うことです。

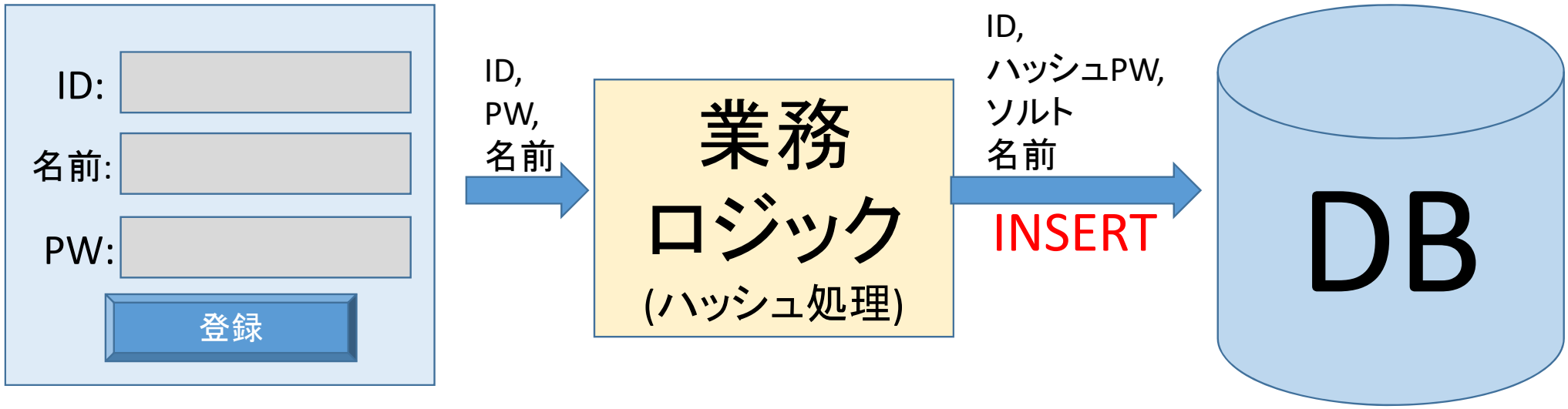


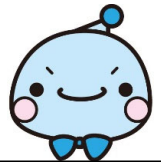
◆ユーザ登録処理

まずはユーザ情報をDBに登録する仕組みを学びましょう。

登録フォームから入力された情報とハッシュ化したPW、ハッシュに使ったソルトをDBへ登録します。

この際に絶対にPWは平文で登録してはいけません。



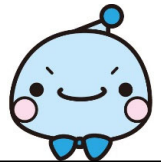


◆練習問題　(必須課題)　2点

問1：下記の項目を含んだ会員登録フォームを作成せよ。
今後の課題でログインロジックを実装するため、DBアクセスまで実装する事。

登録項目：　※オリジナル要素として増やしても構いません。

- 氏名
- 年齢
- 性別
- 電話番号
- メールアドレス　(重複不可にすること)
- パスワード　※PWはハッシュしてソルトとともにDBに保存すること

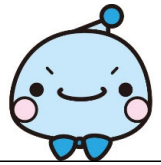


◆チャレンジ問題　2点

問2：問1で登録した会員の一覧を表示する機能を実装せよ。

表示項目：

- 氏名
- 年齢
- 性別
- 電話番号
- メールアドレス　(重複不可にすること)



◆チャレンジ問題　2点

問3：問1で登録した会員を削除する機能を実装せよ。
ただし、削除に使用するキーはメールアドレスとすること。