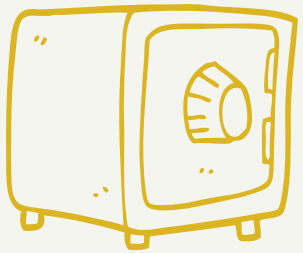
A U T H

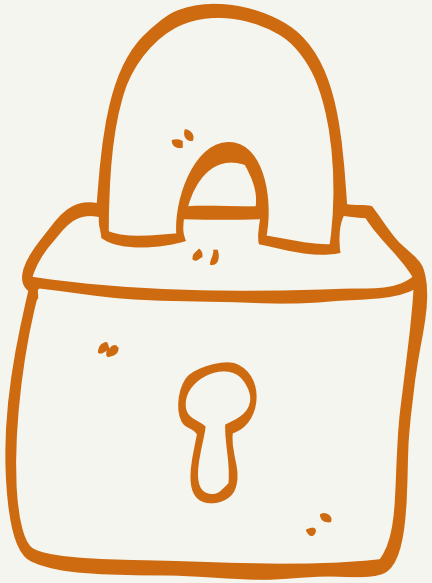


WEB DEVELOPER
BOOTCAMP

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.



認証

AUTHENTICATION

認証とは、ユーザーが「誰であるか」を確認するプロセス。

多くの場合ユーザー名とパスワードの組み合わせで認証を行うが、セキュリティ質問や顔認証などを組み合わせることもできる。

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

認可

AUTHORIZATION

認可とは、ユーザーが「何ができるか」を確認する確認するプロセス。

一般的には、ユーザーが認証された後に認可を行う。
「あなたが誰なのかわかったので、 何ができるか教えるね」というイメージ。

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

ルール #1

パスワードはそのまま保存しない！

DEEP BREATH. IT'S TIME FOR AUTH.

ルール #1

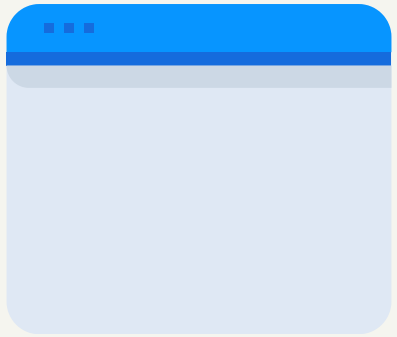
パスワードはそのまま保存しない！

```
{
    username: 'kittycatluvr',
    password: 'meowmeow999!'
},
{
    username: 'geckoGuy',
    password: 'lizard987'
}
```


DEEP BREATH. IT'S TIME FOR AUTH.

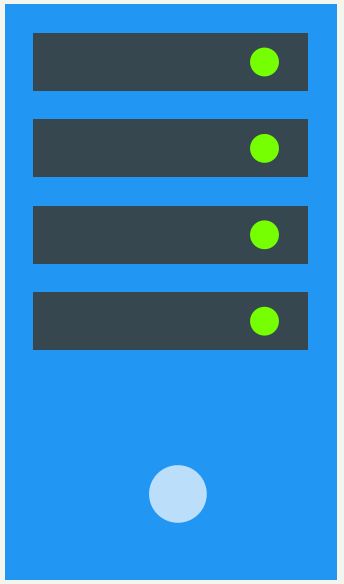
DEEP BREATH. IT'S TIME FOR AUTH.

CLIENT



↓でログインしたい:
Username: 'geckoGuy'
Password: 'lizard987'

SERVER



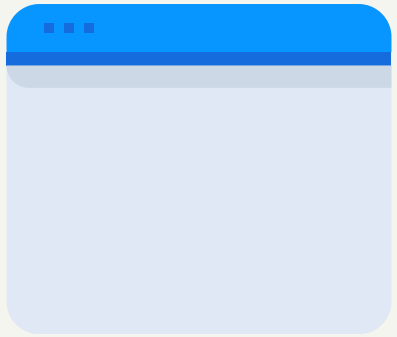
DATABASE

```
{
    username: 'kittycatluvr',
    password: 'meowmeow999!'
},
{
    username: 'geckoGuy',
    password: 'lizard987'
}
```

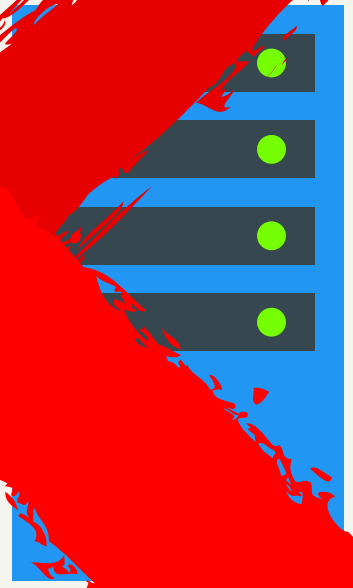
DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

CLIENT



↓でログインし
Username: 'geck
Password: 'lizard



DATABASE

{

username: 'kittycatluvr',
password: 'meowmeow999!'

},
{

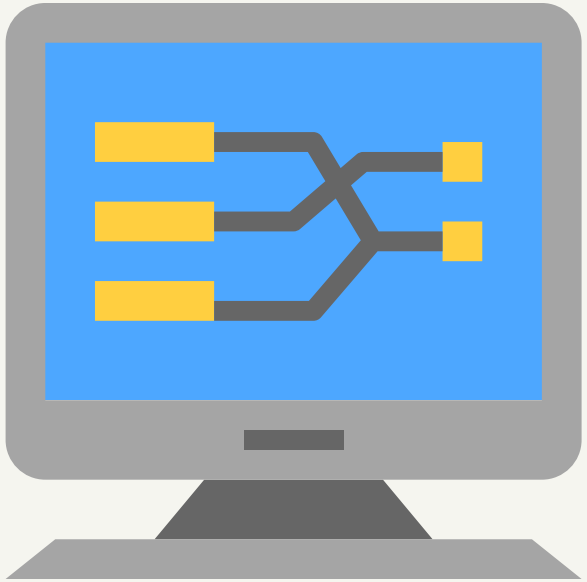
username: 'geckoGuy',
password: 'lizard987'

}

DEEP BREATH. IT'S TIME FOR AUTH.

N  !

DEEP BREATH. IT'S TIME FOR AUTH.



ハッシュ化

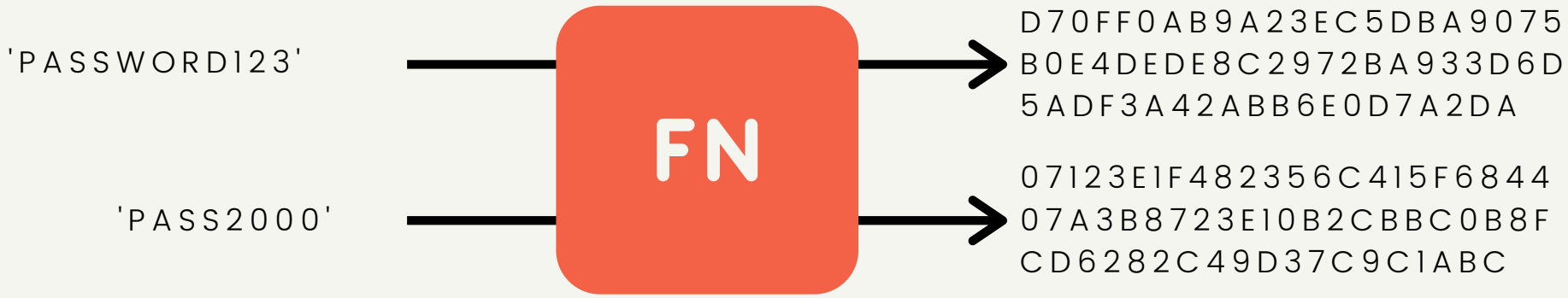
HASHING

パスワードをデータベースにそのまま保存するのではなく、まずパスワードをハッシュ関数にかけ、その結果をデータベースに保存する。

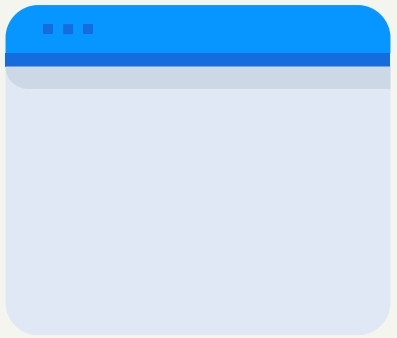
DEEP BREATH. IT'S TIME FOR AUTH.

ハッシュ関数

ハッシュ関数とは、任意のサイズの入力データを
固定サイズの出力値に変換する関数。

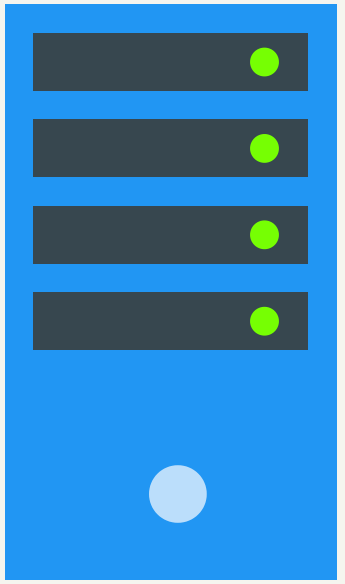


CLIENT



↓でログインしたい:
Username: 'geckoGuy'
Password: 'lizard987'

SERVER



DATABASE

{

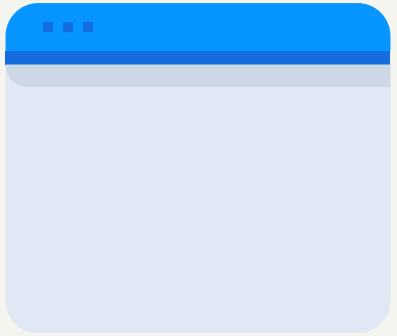
username: 'kittycatluvr',
password:'d70ffoab9a23ec5dba9075b0e4de
de8c2972ba933d6d5adf3a42abb6e0d7a2da'

},
{

username: 'geckoGuy',
password:'07123e1f482356c415f684407a3b87
23e10b2cbbc0b8fcd6282c49d37c9c1abc'

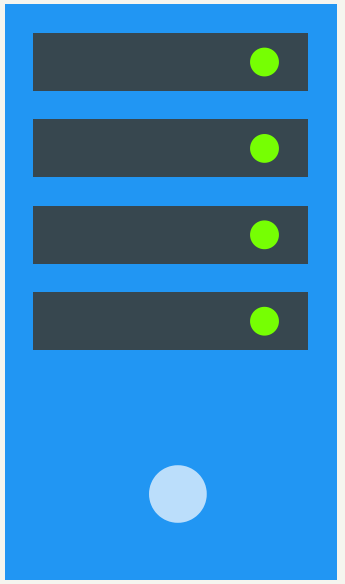
}

CLIENT



↓でログインしたい:
Username: 'geckoGuy'
Password: 'lizard987'

SERVER



DATABASE

{

username: 'kittycatluvr',
password:'d70ffoab9a23ec5dba9075b0e4de
de8c2972ba933d6d5adf3a42abb6e0d7a2da'

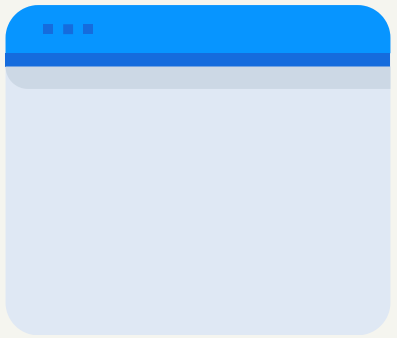
},
{

username: 'geckoGuy',
password:'07123e1f482356c415f684407a3b87
23e10b2cbbc0b8fcd6282c49d37c9c1abc'

}

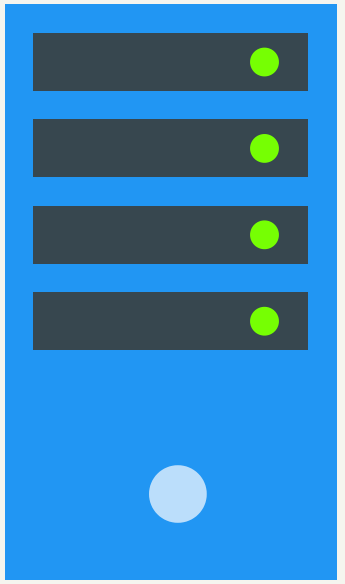
'LIZARD987' → FN →

CLIENT



↓でログインしたい:
Username: 'geckoGuy'
Password: 'lizard987'

SERVER



DATABASE

{

username: 'kittycatluvr',
password:'d70ffoab9a23ec5dba9075b0e4de
de8c2972ba933d6d5adf3a42abb6e0d7a2da'

},
{

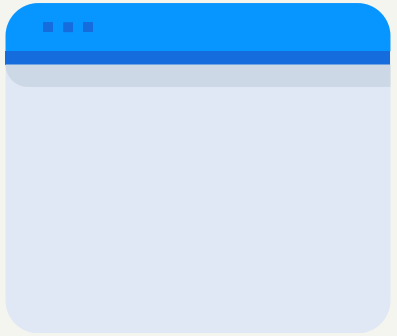
username: 'geckoGuy',
password:'07123e1f482356c415f684407a3b87
23e10b2cbbc0b8fcd6282c49d37c9c1abc'

}

'LIZARD987' → FN →

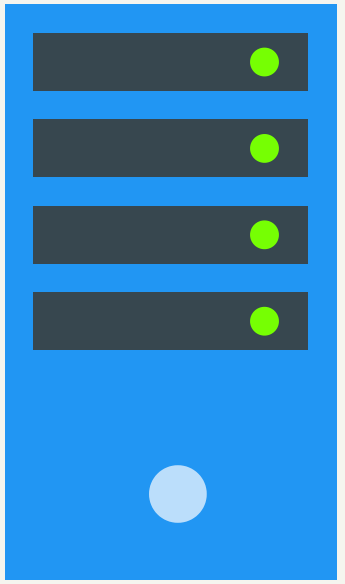
07123E1F482356C415F6844
07A3B8723E10B2CBBC0B8F
CD6282C49D37C9C1ABC

CLIENT



↓でログインしたい:
Username: 'geckoGuy'
Password: 'lizard987'

SERVER



DATABASE

{

username: 'kittycatluvr',
password:'d70ffoab9a23ec5dba9075b0e4de
de8c2972ba933d6d5adf3a42abb6e0d7a2da'

},
{

username: 'geckoGuy',
password:'07123e1f482356c415f684407a3b87
23e10b2cbbc0b8fcd6282c49d37c9c1abc'

}

一致！！

'LIZARD987' → FN →

07123E1F482356C415F6844
07A3B8723E10B2CBBC0B8F
CD6282C49D37C9C1ABC

暗号学的ハッシュ関数

1. 一方向性の関数である。元に戻せない。
2. 入力のちょっとした変化で、出力が大きく変化する。
3. 同じ入力に対して必ず同じ出力となる。
4. 異なる入力から同じ出力が生成される確率が極めて低い。
5. 関数の実行が意図的に遅い。

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

S A L T

セキュリティの強化

DEEP BREATH. IT'S TIME FOR AUTH.

DEEP BREATH. IT'S TIME FOR AUTH.

SALT

ソルト

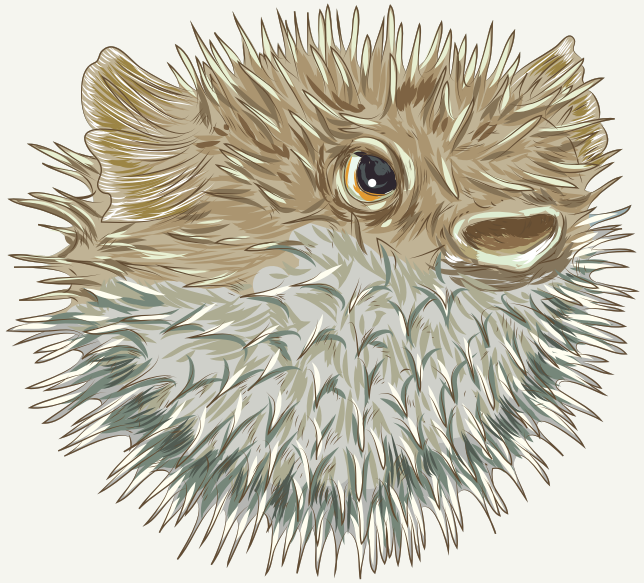
ソルトとは、ハッシュ化する前にパスワードに加える任意の値のこと。

ソルトは、他では容易に作られない、一意なハッシュを保証し、多くのセキュリティ攻撃を軽減するのに役立つ。

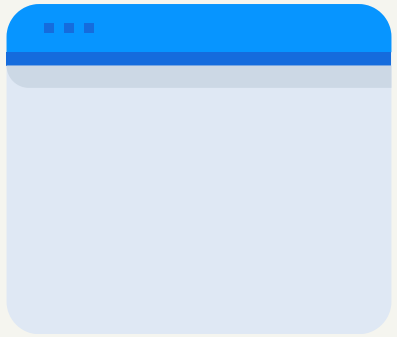
DEEP BREATH. IT'S TIME FOR AUTH.

B C R Y P T

パスワードハッシュ化関数

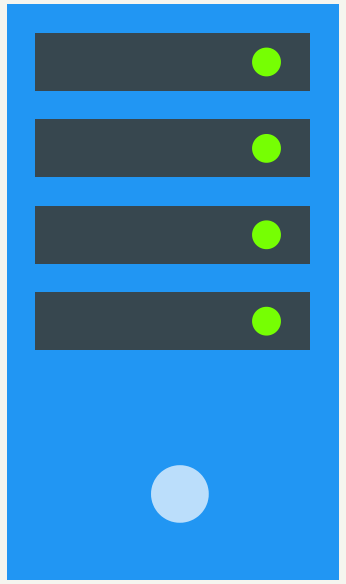


クライアント



クッキーもってますよ
セッションIDは4

サーバー



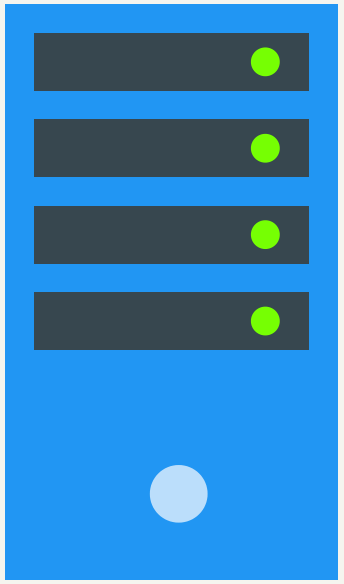
データストア

```
{
    id: 4,
    shoppingCart: [
        {item: 'carrot', qty:2},
        {item: 'celery', qty:5},
        {item: 'potatoe;', qty:4},
    ]
}
```

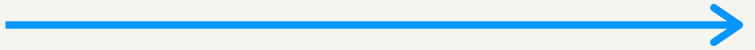
データストア

```
{
    id: 3,
    shoppingCart: [
        {item: 'lime', qty:1},
        {item: 'la croix', qty:99},
        {item: 'lemon', qty:2},
    ]
},
{
    id: 4,
    shoppingCart: [
        {item: 'carrot', qty:2},
        {item: 'celery', qty:5},
        {item: 'potatoe;', qty:4},
    ]
},
{
    id: 5,
    shoppingCart: [
        {item: 'apple', qty:2},
        {item: 'onion', qty:5},
        {item: 'pear;', qty:9},
    ]
}
```

サーバー



あなたのセッションIDは4



クライアント