


# 盗まれにくく、忘れにくい 面影の選択による認証手法 おもかげパスワード

研究駆動コース 35R 村上あさひ


## はじめに



0613かな



パスワード  
のぞき見られている  
気がする...



パスワードまた忘れてしまった!  
再設定面倒だな...  
パスワードマネージャの使い方も  
よくわからない...

はじめに

本研究で目指すのは

のぞかれても盗まれにくい  
覚えやすく忘れにくい

個人認証

- 1 おもかげパスワードの概要**  
おもかげパスワードとは?どんな課題を解決する?
- 2 のぞかれても盗まれにくい理由とは?**  
おもかげパスワードはのぞき見耐性ある?
- 3 覚えやすく忘れにくい理由とは?**  
おもかげパスワードは覚えやすくて忘れにくい?
- 4 おもかげパスワードの社会実装**  
メーカーの製品セキュリティの方とのお話を通して
- 5 おもかげパスワードの今後について**  
おもかげパスワードの後は?

- 1 おもかげパスワードの概要**  
おもかげパスワードとは?どんな課題を解決する?
- 2 のぞかれても盗まれにくい理由とは?  
おもかげパスワードはのぞき見耐性ある?
- 3 覚えやすく忘れにくい理由とは?  
おもかげパスワードは覚えやすくて忘れにくい?
- 4 おもかげパスワードの社会実装  
メーカーの製品セキュリティの方とのお話を通して
- 5 おもかげパスワードの今後について  
おもかげパスワードの未来は?

## おもかげパスワードの概要

本研究で目指すのは

のぞかれても盗まれにくい  
覚えやすく忘れにくい

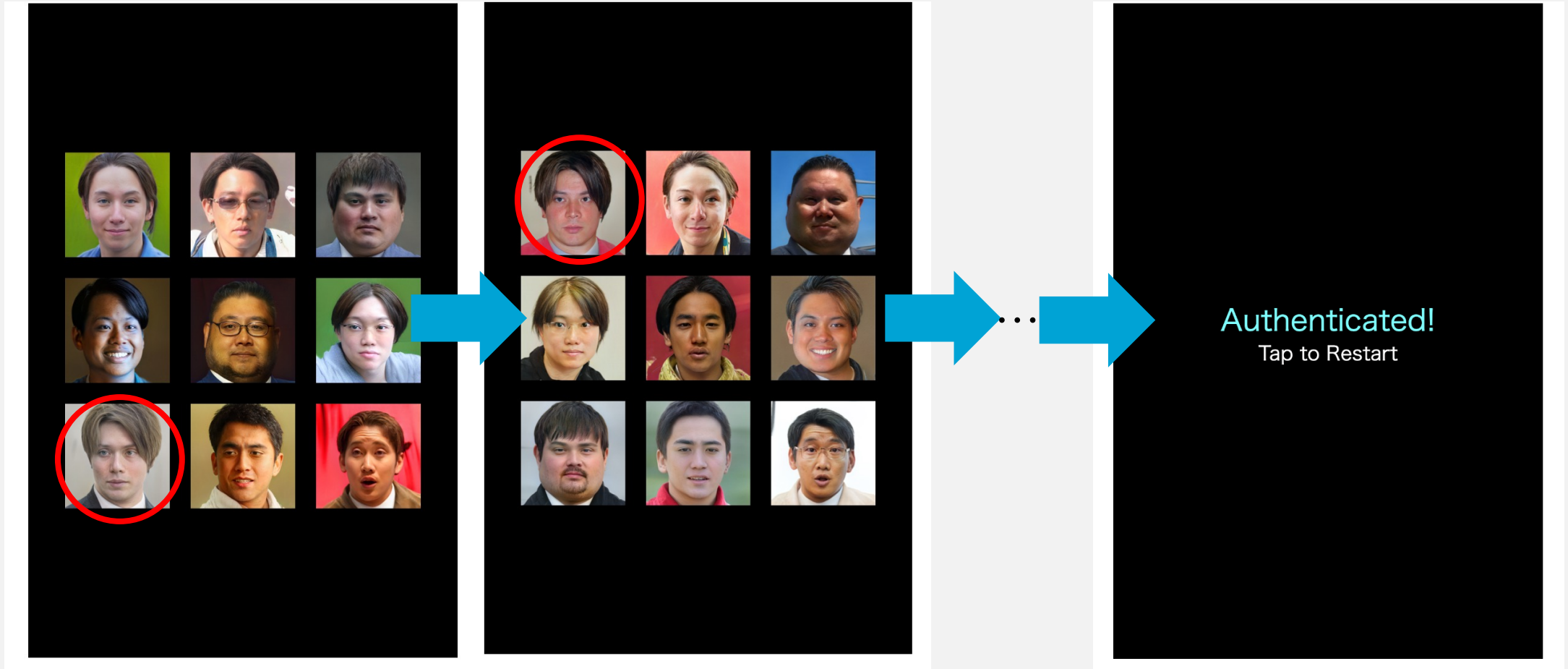
個人認証

pc.fm.senshu-u.ac.jp



# Graphical Authentication

Tap to Start



設定したパスワード顔画像の面影が見える「おもかげ画像」を4回選択するとロック解除できる個人認証方式



# 認証画面の画像構成について



パスワード顔画像

そうではない  
8枚の顔画像



⋮



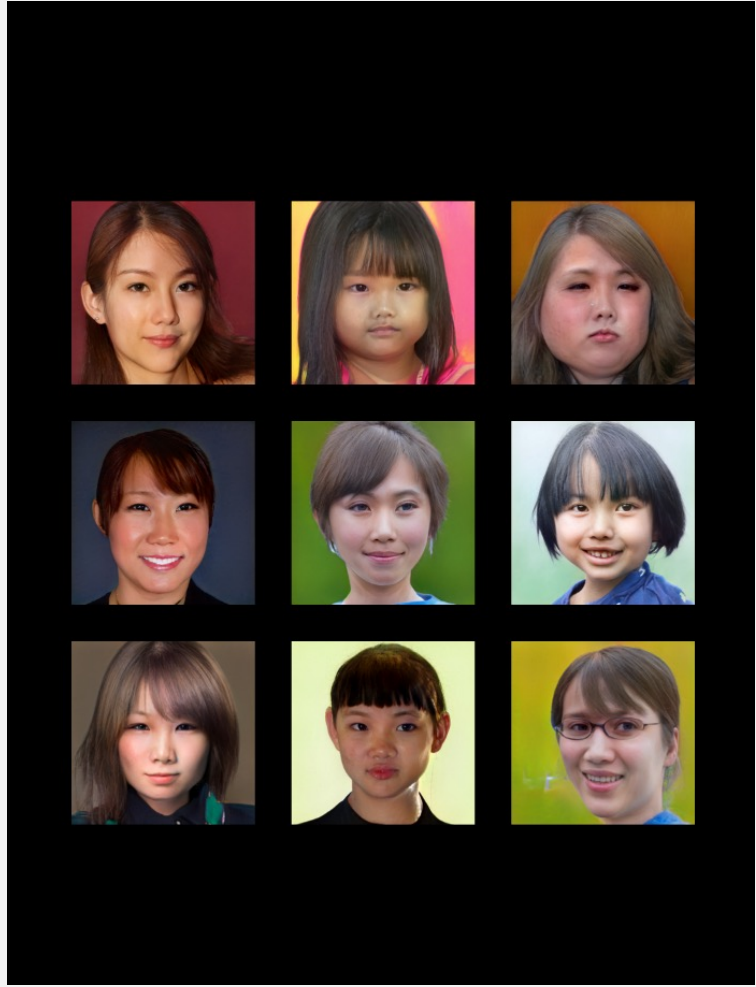
正解画像

おもかげ画像

不正解画像



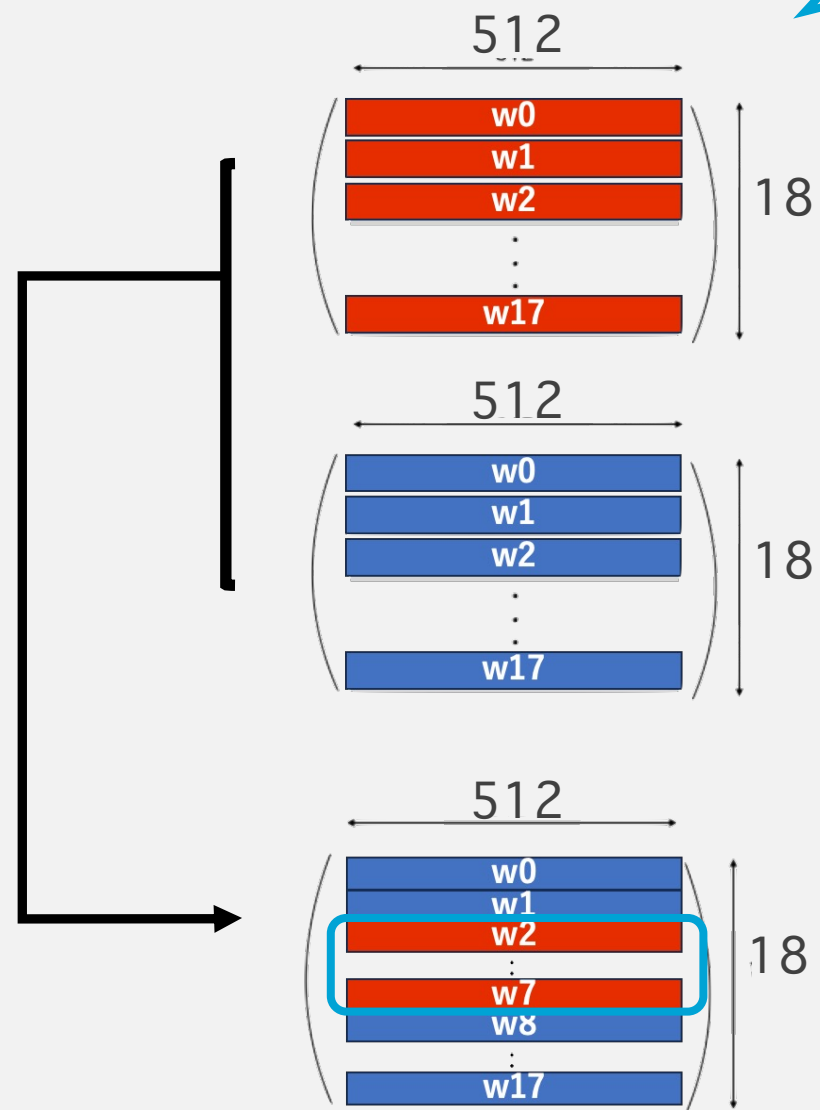
⋮



認証画面

# おもかげ画像の生成

512次元のベクトルの集合である潜在変数に変換



← エンコード



パスワード顔画像

ユーザが設定する

→



ランダム生成顔画像

GANが生成する

GANの Style mixingで生成

⇒



面影を持つおもかげ画像

1 おもかげパスワードの概要  
おもかげパスワードとは?どんな課題を解決する?

2 のぞかれても盗まれにくい理由とは?  
おもかげパスワードはのぞき見耐性ある?

3 覚えやすく忘れにくい理由とは?  
おもかげパスワードは覚えやすくて忘れにくい?

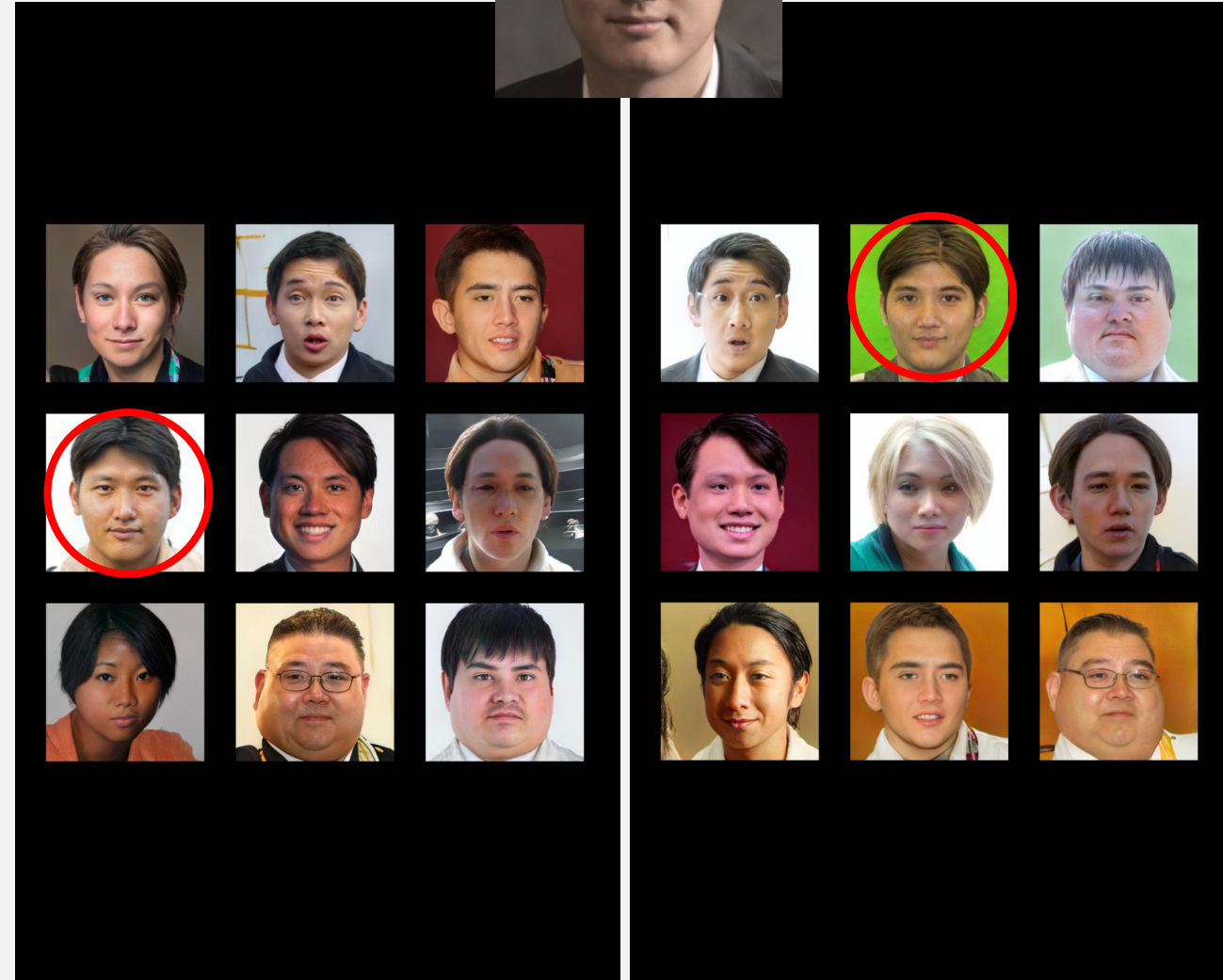
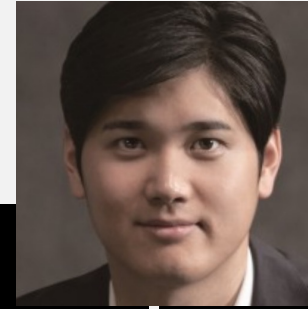
4 おもかげパスワードの社会実装  
メーカーの製品セキュリティの方とのお話を通して

5 おもかげパスワードの今後について  
おもかげパスワードの未来は?

## なぜのぞかれても盗まれにくい？

- ・パスワード顔画像  
そのものは**提示されない**
- ・認証時に提示される画像が  
**毎回異なる**

パスワード顔画像



## 評価実験1の評価観点

- 1 正規ユーザ(パスワードを知っているユーザ)の評価  
初めての利用者が本システムを正しく利用できる?
- 2 非正規ユーザ(パスワードを知らないユーザ)の評価  
悪意のある人ののぞき見による認証成功はどれくらい?
- 3 本システムの使いやすさ  
SUSスコアを使い、定量的に本システムの使いやすさを評価

スコア50未満:注意が必要

スコア50-79 :中程度

スコア80以上:非常に優れている

※SUS : System Usability Scale

## 評価実験1 (おもかげパスワードの性能評価)

- ・正規ユーザ(パスワードを知っているユーザ)の役割

- ①パスワード顔画像を設定
- ②認証問題を解く作業を3回繰り返す

- ・非正規ユーザ(パスワードを知らないユーザ)の役割

- ①他者が認証問題を解いている動画を見る
- ②同じ認証問題を解く作業を3回繰り返す

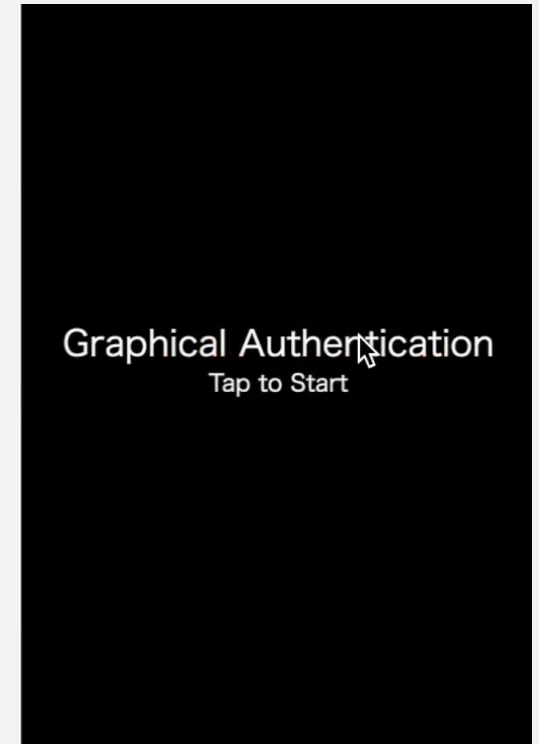
- ・実験参加者

計16名の20代の大学生に実施

本システムを操作するのは初めてであり、

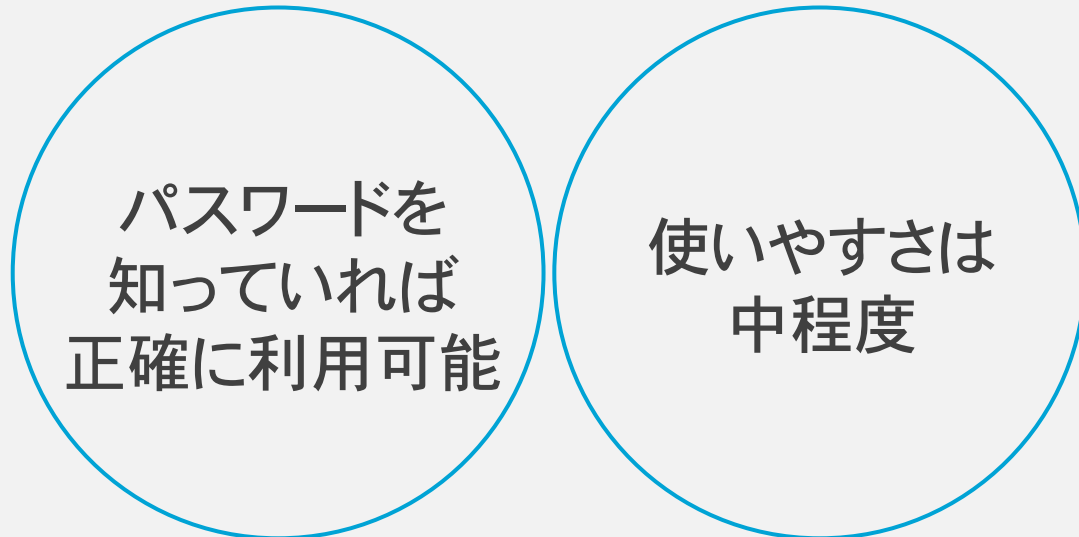
情報技術系の理工学を専攻:14名、理工学以外を専攻:2名

男性:8名、女性:8名



## 結果(全体)

正規ユーザ	
認証成功率	SUSスコア
100%	66.3



非正規ユーザ
認証成功率
45.8%



## 他の認証システムとの比較

	おもかげ	図形	ランダムアート	顔画像	パスコード認証	パターン認証
認証成功率 (正規)	100.0%	100.0%	100.0%	88.9%	100.0%	100.0%
認証成功率 (非正規)	45.8%	27.8%	61.1%	50.0%	100.0%	72.2%

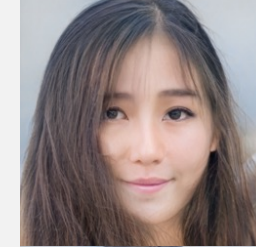
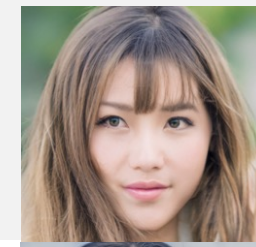
ここを目指す

(石井ら[2019])



## ユーザ調査

パスワード  
顔画像



ランダム生成  
顔画像

濃い



薄い

目的: 面影度合いを薄くするため、正規ユーザがどのくらいの面影であると認識できるのか調査

手法: 15通りのベクトルの組み合わせでおもかげ画像を生成し、ランダムで画像を表示しアンケートを実施

## ユーザ調査結果

実施人数: 大学2年生～4年生までの14名

実験結果: 同じ面影度合いでも回答が反転している

写真番号	Aさんの評価	Bさんの評価	Cさんの評価	Dさんの評価
8	2	1	2	1
9	1	3	1	1
10	1	3	2	1
11	3	3	3	1



面影の認識は人によって大きく異なり、一様に面影度合いを薄くすることはできない  
個人個人がわかる面影度合いにチューニングしたら良いのでは

## 評価実験2

目的: 個人個人の面影度合いを調整した上でのぞき見できるかを評価

手法:

- ① 1名の実験参加者が認識可能な、最も薄い面影度合いでチューニング
- ② 認証問題を解いている動画を作成
- ③ 原理を知っている他の実験参加者10名に動画を見てもらい同じ認証問題を解いてもらう

結果: 非正規ユーザののぞき見による認証成功率は**6.7%**



**目標の数値まで非正規ユーザの認証成功率を下げることができた**

- 1 おもかげパスワードの概要  
おもかげパスワードとは?どんな課題を解決する?
- 2 のぞかれても盗まれにくい理由とは?  
おもかげパスワードはのぞき見耐性ある?
- 3 覚えやすく忘れにくい理由とは?  
おもかげパスワードは覚えやすくて忘れにくい?
- 4 おもかげパスワードの社会実装  
メーカーの製品セキュリティの方とのお話を通して
- 5 おもかげパスワードの今後について  
おもかげパスワードの後は?

## 21 なぜ覚えやすく忘れにくい?

パスワード顔画像として設定



設定した人を思い浮かべるだけで  
認証問題を解くことができる



## 面影を用いることの効果に対する評価実験

目的: 面影を用いることで、長期間使用していなくても、パスワードを忘れていないかを評価

手法: 性能評価実験の実験参加者が忘れていないかを評価  
評価は4フェーズに分けて行う(各フェーズ5回中3回認証成功で終了)

段階	評価方法
第1フェーズ	何も見せずに解いてもらう 解くことができなかつたら2へ
第2フェーズ	パスワードに設定した人の名前だけを教える 解くことができなかつたら3へ
第3フェーズ	設定したパスワード顔画像を見せる 解くことができなかつたら4へ
第4フェーズ	おもかげ画像を見せる

## 結果

実験参加者: 性能評価実験に参加していただいたうちの15名(男性:7名、女性:8名)

評価実験から開いた期間は平均154日(5ヶ月弱)、標準偏差17日

段階	評価方法	結果
第1フェーズ	何も見せずに解いてもらう 解くことができなかつたら2へ	13名
第2フェーズ	パスワードに設定した人の名前だけを教える 解くことができなかつたら3へ	2名
第3フェーズ	設定したパスワード顔画像を見せる 解くことができなかつたら4へ	0名
第4フェーズ	おもかげ画像を見せる	0名

長い期間空いていても全体の87%が何も見ずにパスワード顔画像を思い出すことができたことから、覚えやすく忘れにくいことが言える

1 おもかげパスワードの概要  
おもかげパスワードとは?どんな課題を解決する?

2 のぞかれても盗まれにくい理由とは?  
おもかげパスワードはのぞき見耐性ある?

3 覚えやすく忘れにくい理由とは?  
おもかげパスワードは覚えやすくて忘れにくい?

4 おもかげパスワードの社会実装  
メーカー製品セキュリティの方とのお話を通して

5 おもかげパスワードの今後について  
おもかげパスワードの未来は?



# おもかげパスワードの社会実装

おもかげパスワード  
独自の脅威

顔の類似度から  
機械が突破できる？

法的な観点から

実在する人物の  
顔画像を扱うこと  
への課題整理

## 機械によっておもかげパスワードは突破できる？

おもかげパスワードの脅威：ツールによる自動解析  
面影を用いているゆえ、顔の類似度から機械で自動的に正解画像を  
判別できてしまうのでは？

認証画面に提示される画像を  
顔の類似度で9人に分類できれば  
おもかげパスワードの突破が現実的になる



攻撃可能性を探るミニマムな実験として  
顔認識モデルを使いペアごとの類似度の算出を行い  
面影を識別できるのかを検証した

## 顔認識モデルを使った実験

手法: 顔認識モデル(ArcFace)を使用し、ペアごとのコサイン類似度(0に近いほど似ていない、1に近いほど似ている)を評価

結果: 同じパスワード顔画像から生成されたおもかげ画像同士(正解画像同士)は比較的高い値を示す  
ただし、正解画像と不正解画像同士でも高い値を示すものもある

考察: 簡単に識別可能という結論にはならないが、識別不可能とも言えない

	1.00	0.22	0.27	0.40	0.03	0.18	0.19	0.08
	0.22	1.00	0.61	0.27	0.02	0.42	0.10	0.07
	0.27	0.61	1.00	0.38	0.00	0.37	0.10	0.13
	0.40	0.27	0.38	1.00	0.07	0.14	0.07	0.13
	0.03	0.02	0.00	0.07	1.00	0.00	0.12	0.00
	0.18	0.42	0.37	0.14	0.00	1.00	0.07	0.09
	0.19	0.10	0.10	0.07	0.12	0.07	1.00	0.22
	0.08	0.07	0.13	0.13	0.00	0.09	0.22	1.00

※ ペアごとの類似度の算出をしているだけのため、誰のおもかげであるかを特定できるかはこの実験の範囲外

## 顔をを使うことのメリット・センシティブさについて

### メリット

面影を用いることで「覚えやすく忘れにくく」なっている

### 北條トレーナーより肖像権と個人情報の問題について

肖像権は、法律上の明文はなく、みだりに自己の容ぼう等を撮影され、これを公表されない人格的利益

おもかげパスワードの態様で実施されている場合には、肖像権に対する侵害とは考えられない

おもかげパスワードで使用する顔画像データの特徴点が個人識別符号に該当し、個人情報として取り扱うことになるため、おもかげパスワードのサーバ管理者は個人情報取扱事業者として対応する必要がある

- 1 おもかげパスワードの概要  
おもかげパスワードとは?どんな課題を解決する?
- 2 のぞかれても盗まれにくい理由とは?  
おもかげパスワードはのぞき見耐性ある?
- 3 覚えやすく忘れにくい理由とは?  
おもかげパスワードは覚えやすくて忘れにくい?
- 4 おもかげパスワードの社会実装  
パナソニック製品セキュリティの方とのお話を通して
- 5 おもかげパスワードの今後について  
おもかげパスワードの後は?

まとめと今後～盗まれにくく、忘れにくいことに対して～

のぞかれても  
盗まれにくい



のぞき見耐性の  
向上

覚えやすく  
忘れにくい



面影を用いる  
効果についての  
評価実験

社会実装



独自の脅威  
顔情報を扱う  
ことについて

今後も更なる検討を進めていく

専修大学無人コンビニプロジェクトや小学校を対象に社会実装を目指す