

オンライン試験における 不正行為防止技術

日本テスト学会記念講演 2021.3.28

成蹊大学 小方 博之

1

COVID-19の世界的流行の大学への影響

- 2019年に確認されたCOVID-19は、世界各地に感染拡大、翌年3月にWHOがパンデミック宣言
- 全国の大学で卒業式や入学式が中止
- 4月に7都府県、次いで全国に緊急事態宣言が発令
 - 授業開始日の延期、オンライン化へ移行

2

国内大学の授業実施形態（2020年7月1日時点）

	対面授業	対面・遠隔を併用	遠隔授業
国立大学(86校)	1.2%	64.0%	34.9%
公立大学(102校)	7.8%	70.6%	21.6%
私立大学(824校)	17.6%	59.7%	22.7%
高等専門学校(57校)	33.3%	40.4%	26.3%
全体(1069校)	16.2%	60.1%	23.8%

文部科学省「新型コロナウイルス感染症の状況を踏まえた大学等の授業の実施方法」より

- 海外でも同様に対面を制限し、オンライン授業を拡大

3

国内大学の定期試験形態（2020年度夏学期）

- 全国141大学を抽出し、各大学のホームページから前期定期試験の実施方法を調査（各都道府県から3大学ずつ抽出）

前期試験方法	地域区分	北海道	東北	関東	中部	関西	中国	四国	九州・沖縄	計
課題		100%	22%	52%	52%	52%	53%	25%	42%	44%
対面		-	-	5%	4%	5%	-	17%	21%	7%
オンライン試験		-	-	-	-	-	-	-	-	0%
対面・課題		-	-	-	15%	24%	13%	17%	12%	11%
課題・オンライン試験		-	-	19%	7%	-	7%	-	-	5%
提示なし		-	78%	24%	22%	19%	27%	41%	25%	33%
計		3	18	21	27	21	15	12	24	141

成蹊大学 小方研究室 調べ

4

オンライン試験の不正行為事例

- 国内の報道は少ない
- 海外（特に韓国）ではいくつか不正行為事例が報道されている

大学名	不正行為	受験人数	不正人数	科目又は学部	対応策
成均館大学	問題を有料サイトに投稿	-	一部の学生	物理学	テレビ会議システムを用いて受験生の身分を確認
仁荷大学	109人中91人が1箇所に集まって問題共有（電話・会員制交流サイト）	109	91	医学部	対面式に変更
西江大学	一同に集まり答えの共有・替え玉	-	20	数学・電子工学	-
建国大学	替え玉	-	-	-	-
韓国外国語大学	カカオトーク（メッセージアプリケーション）を用いた回答の共有	998	約700	-	-
延世大学	答案を共有	約300	-	-	-
漢陽大学	-	-	-	-	-
ソウル市立大学	-	-	-	-	-

成蹊大学 小方研究室 調べ

5

オンライン試験での不正行為への対応

試験監督サービス

- 遠隔監視、いわゆるAI技術による不正行為検出など
- 不正行為検出については現行のサービス間では機能にあまり差はない

試験監督サービス	アイトラッキング(目線・角度)	人数推定	同一人物判定	音声認識	年齢推定	試験監督機能	指紋認識	即時解析
Check PointZ	Yes	Yes	Yes	—	Yes	Yes	No	Yes
Remote Testing AI アナリスト	Yes	Yes	Yes	Yes	—	Yes	No	Yes
Remoty AI+	Yes	Yes	Yes	—	Yes	Yes	No	Yes
Excert	試験監督が確認	No	Yes	No	—	Yes	No	No
Examity	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Proctor U	Yes	Yes	—	—	—	Yes	—	Yes
Proctorio	Yes	Yes	Yes	—	Yes	No	—	Yes
On VUE	Yes	Yes	Yes	—	Yes	No	Yes	Yes

成蹊大学 小方研究室 調べ

6

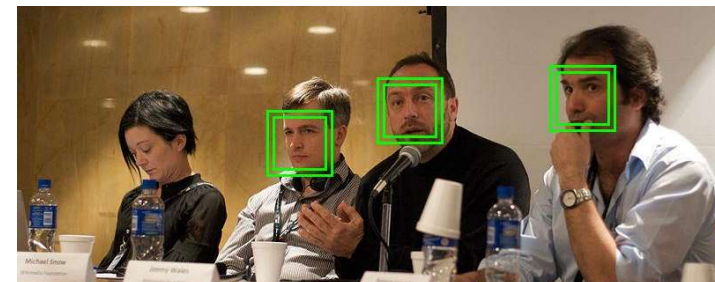
現行の試験監督サービスに見られる不正行為検出技術

- 人数推定
- 視線方向の検出（アイトラッキング）
- 同一人物判定
- 年齢推定
- 指紋認識
- など

7

人数推定

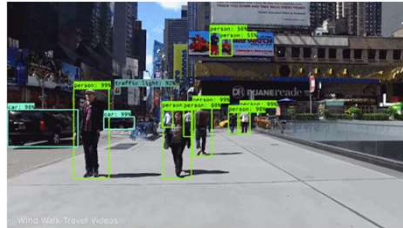
- 顔検出か人物検出
- 顔検出：Viola-Jones法(2001)が代表的



8

人数推定

- 最近の顔（人物）検出手法：
深層ニューラルネットワーク(DNN)
- RCNN, YOLO, SSDなど
- より柔軟な顔・人物検出
- 顔検出の場合、横顔、俯き顔などにも対応



<https://sgu.ac.id/id/computer-vision-artificial-intelligence-why-is-it-important/>

9

人数推定

- 技術を体験できるサイト
<https://azure.microsoft.com/ja-jp/services/cognitive-services/face/#demo>



10

アイトラッキング

- もともとは眼球運動の測定技術を指す
- 瞳孔が赤外線で容易に検出できる性質を利用
- 精度は高いが、赤外線照射が必要



<https://steakrecords.com/ja/668163-eye-pupil-tracking-using-hough-circle-transform-python-27-opencv-eye-tracking.html>

11

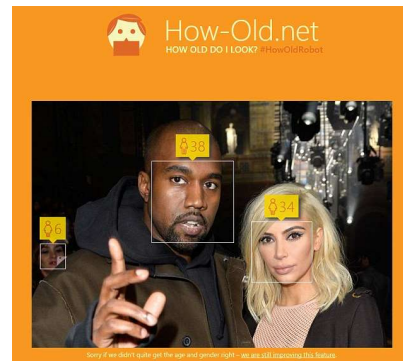
アイトラッキング

- PC内蔵カメラによる簡易な方法
 - 両眼の向きから視線方向を算出
 - PC、スマホなどで手軽に使用可能
 - 視線方向の検出精度やサンプリング周波数は専用装置に劣る

12

年齢推定

- DNNで可能
- 技術的には顔認識を緻密化したものとみなせる
- 深層学習時に、年齢推定に有用な特徴を引き出すのに工夫が必要

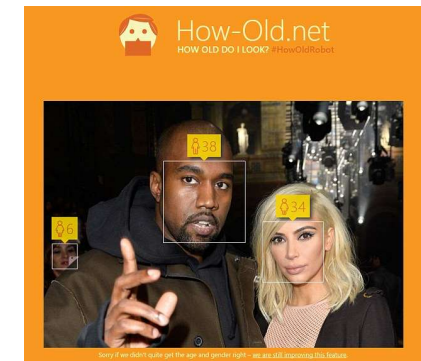


<https://www.dailymail.co.uk>

13

年齢推定

- 技術を体験できるサイト
"How Old Do I Look?"
<https://www.how-old.net>



<https://www.dailymail.co.uk>

14

指紋認証

- 指紋センサ付きマウスなどの製品があり、継続的認証も技術的には可能

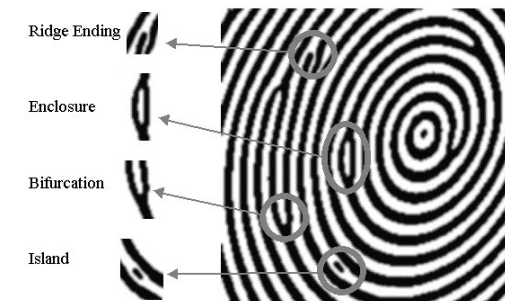


<https://www.sanwa.co.jp/product/syohin.asp?code=M-A-IRFP139BK>

15

指紋認証

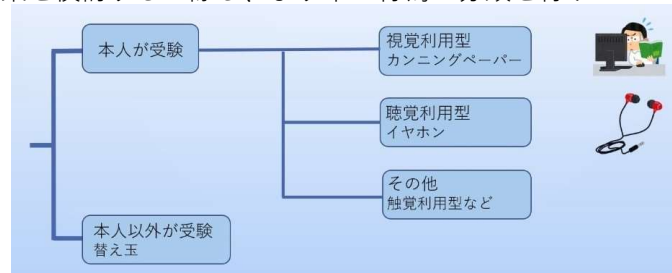
- マイニューシャ方式
 - すべてが一致する確率は640億分の1
 - 照合数は10～12点とも20～40点とも



16

不正行為の分類 (小方他2017)

- 会場外オンライン試験の実用化には網羅的に不正行為対策をすることが必要
- 対策を検討するに際し、まず不正行為の分類を行う



17

不正行為対策

- 防止
 - 不正行為を無効にする対策
 - 外部情報の遮断・妨害など
 - 不正行為の検出より確実
- 検出
 - 不正行為を発見する対策
 - 受験者の本人確認・ふるまい監視など
 - 推定の要素が入るため、不確実な側面がある

18

不正行為の防止技術

部屋レベル

- 持ち込み不許可物の排除
- 試験会場での携帯電話等通信抑止装置
- サウンドマスキング

身体レベル

- VR機器（例：VRゴーグル）
 - VR機器が臨場感を高めるために外部情報を遮断する性質を利用
 - 別途、ゴーグルのブラックボックス化、着脱の検知も必要
 - 実用性は別にして不正行為防止に利用が考えられるのはVRゴーグルに限らない（ヘッドホン：聴覚遮断、VRスーツ：触覚遮断など）

19

不正行為検出の要件 (橋本他2013)

不正行為の検出技術の研究・開発にあたっては、いくつかの制約を考慮する必要がある。

- 継続性
 - 不正行為を継続的に監視できる
- 透過性
 - 受験者の解答の妨げにならない
- 同一性
 - 監視している対象が本人だと保証される
- 耐攻撃性
 - 対抗策に対して頑健である

20

要件を満たす検出技術

- 替え玉の検出
 - 本人認証の手法を応用
- 受験者本人の不正行為の検出
 - 持ち込み許可物以外のものを所持
 - (PCなどを通じて) 参照許可物以外のものを参照
 - (上述のものを検出することが困難な場合) 行動判別

21

本人認証手法の分類と要件充足性

認証手法	メリット	デメリット	具体例
知識認証	コストが安く導入しやすい	パスワードなどの漏洩	パスワード・合言葉
所有物認証	認証が簡単	譲渡による偽装 認証時に所有している必要がある	IDカード・本人証明書
生体認証	身体的特徴	認証が簡単	指紋・虹彩・DNA
	行動的特徴	怪我などの身体変化の影響を受けやすい 漏洩がない	筆跡・タッチジェスチャ

- 知識認証：継続性を満たさない
- 所有物認証：同一性を満たさない
- 生体認証（バイオメトリクス）：ものによっては条件を満たす

22

試験形態と本人認証

- 筆記
 - ペン持ち方認証（橋本他2013）
 - 筆記認証（米谷他2010）
- キーボードとマウス
 - 指紋認証
 - キーストローク認証



23

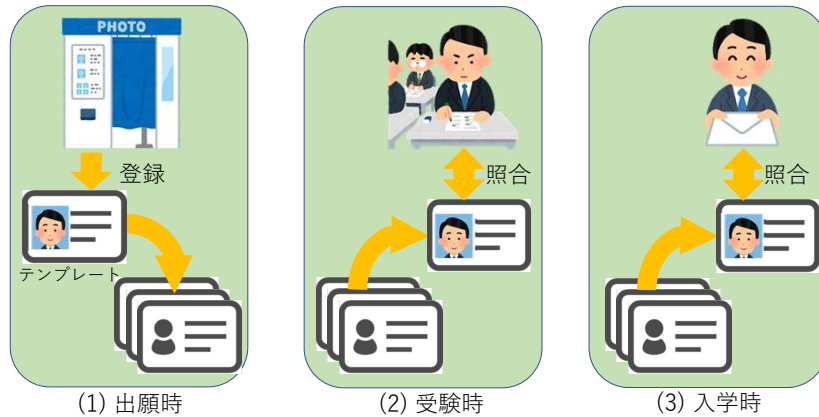
試験形態と本人認証

- タブレット
 - タッチジェスチャ認証（安田他2021）
- 汎用
 - 顔認証、虹彩認証（ただし、入力デバイスとリンクしていないため、同一性が保証されない可能性）



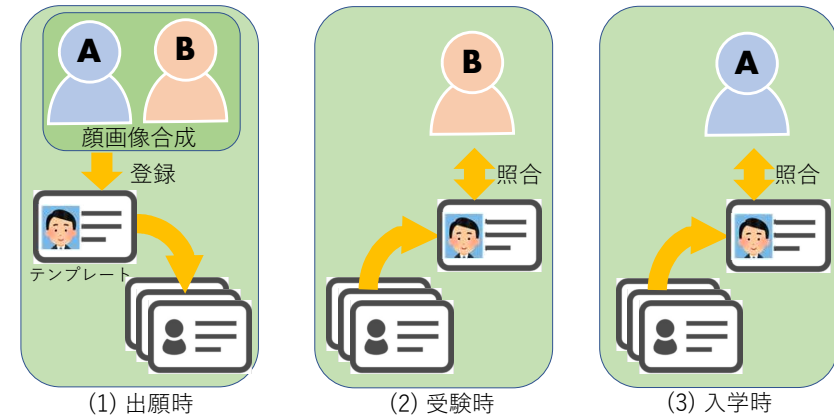
24

本人認証の手順（顔認証の場合）



25

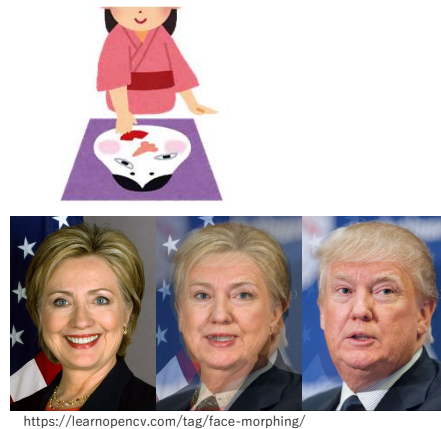
テンプレート改変による不正事例



26

顔画像合成の方法

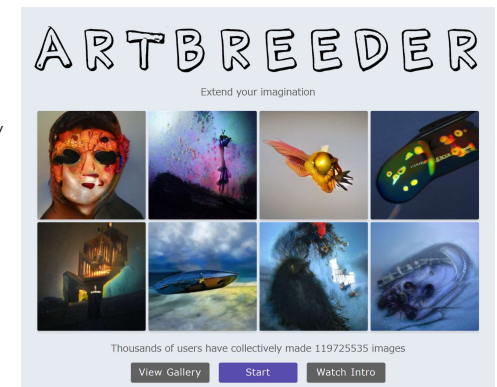
- 手作業による方法
 - 画像加工ソフト等を利用
 - 作業者のスキルに依存
- モーフィング
 - 2画像間を線形補間
 - 合成度合いを調整可能
 - 比較的合成と分かりやすい
- AIによる合成
 - 顔特性を考慮した非線形補間
 - 合成度合いを調整可能
 - 自然な合成



27

顔画像合成の方法

- 技術を体験できるサイト
<https://www.artbreeder.com/>



28

StyleGAN(Karras+2018)

- GAN（敵対的生成ネットワーク）の一種
- 高精細・写真的な顔画像生成が可能
- 潜在ベクトルをGANに入力することで、画像生成
- 生成画像に対応する潜在ベクトルを算出することで、合成画像生成が可能



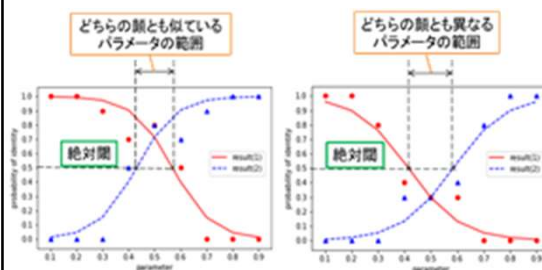
29

合成顔画像による本人照合攻撃性の評価

- 混合率と人間の受ける印象は必ずしも線形関係にない
- 恒常法により両合成元人物との弁別閾を求める

30

合成顔画像による本人照合攻撃のリスク評価



- 両弁別閾の値によって混同度を評価
- 66名の男女に合成画像について2肢強制選択法で判断してもらう
- 結果、9組中7組で混同度が正となった（どちらも判断できる合成画像が存在）

31

顔写真AI照合による耐攻撃性の評価

- 人間より認証精度が高いといわれるDNNによる評価を実施
- インターネットから20～30代の有名人男女各30名の画像を各10枚程度収集し、男女各435組の合成顔画像を作成
- FaceNetとone-class SVMを使用して評価
- 870組中、両方と同一人物判定した合成顔画像が存在したのは17組のみ（暫定値）

32