プレスリリース 2012/12/12

人間とデバイスの感度の違いを利用した プライバシー保護技術

-カメラの写りこみによるプライバシー侵害を被撮影者側から防止-

国立情報学研究所
越前 功
iechizen@nii.ac.jp

本発表の流れ

1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～ プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

本発表の流れ

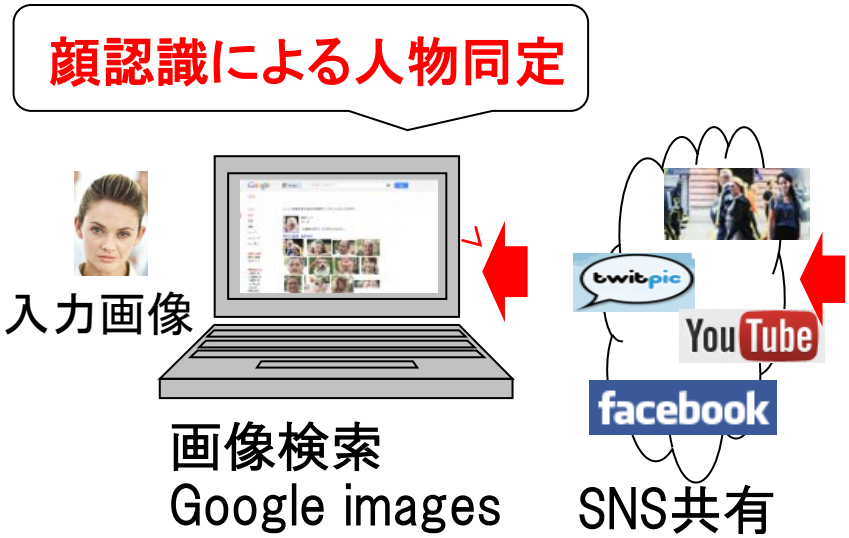
1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～ プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

研究背景

カメラ付き携帯端末の普及, SNSや画像検索技術の進展

- カメラの写りこみによるプライバシー侵害
  - 意図せずカメラに写りこみ
  - TwitterやSNSを通じて写真公開 (位置・時間情報)

- Google imagesなどの画像検索技術により，撮影者がいつ・どこにいたか暴露



位置情報送信
lat　：緯度
lon,：経度
geo,：測地系
x-acc：測位レベル

➡ 意図しない写り込みによるプライバシーの侵害が社会問題化

顔認識技術とプライバシー侵害

- **カーネギー・メロン大学による Facebook の実験**(2011)
  - 写真撮影に合意した匿名の被験者のうち 1/3 が Facebook 上の写真と比較することで人物を同定される
  - 被験者の個人的な興味関心事や社会保障番号の一部なども判明

- **EU　Facebookから顔認識技術を排除**(2012)

米フェイスブックはプライバシーを懸念する欧州連合(EU)当局の要請に従い、欧州ユーザー向けに顔認識機能を無効化

- **Google Project Glass**(2012)
- **Apple iGlass**(2012)

–カメラとヘッドマウントディスプレイで構成されたAR(拡張現実)アプリケーション

–カメラに写りこんだ人物の名前，所属組織や役職を，検索エンジンを通してリアルタイムに特定される可能性 → 人物がリアルタイムに同定される

- **国内：商業施設内で無断で顔撮影，顧客分析**(2012)

客に無断で撮影した顔映像から性別と年代を推測，週1万～2万人分のデータ

➡ **顔認識技術がプライバシー侵害につながる危険性**

従来対策

- **顔面への着色や髪形の変更により人物の顔検出を失敗させる手法**
  顔面への特殊パターンの着色や髪形を特殊な形状にすることで顔認識の前処理である顔検出を失敗させ，人物の同定を防止

- **顔面を物理的に隠し人物のプライバシーを保護する手法**
  Wearable Privacy Shellと呼ばれる伸縮可能なShell状素材を用いてユーザのプライバシーを物理的に保護

引用：Wearable Privacy Shells：
http://www.toxel.com/tech/2011/08/20/wearable-privacy-shells/

引用：How to camouflage yourself from facial recognition technology,
http://venturebeat.com/2010/07/02/facial-recognition-camouflage/

➡ 物理空間における人対人のコミュニケーションに支障をきたす恐れ

本発表の流れ

1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

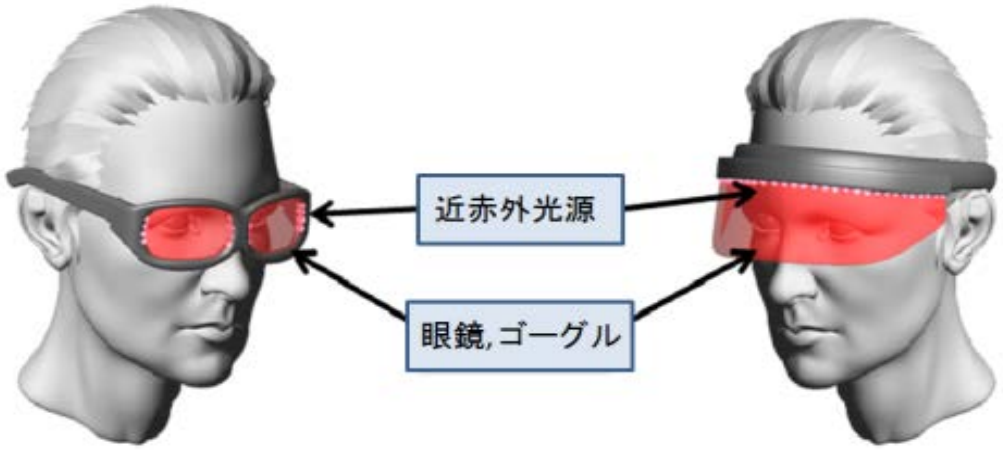
目的と手段

目的:

物理空間における人対人のコミュニケーションに支障をきたすことなく，カメラの写りこみによるプライバシー侵害を被撮影者側から防止する方法の確立

手段:

ウェアラブルデバイス（プライバシーバイザー）の顔面への装着により，人の視覚に影響を与えず，カメラの撮像デバイスのみに反応するノイズ（近赤外線）を顔面から照射し，顔検出を失敗させる



➡ ノイズ光源をどのように配置すれば未検出となるか？

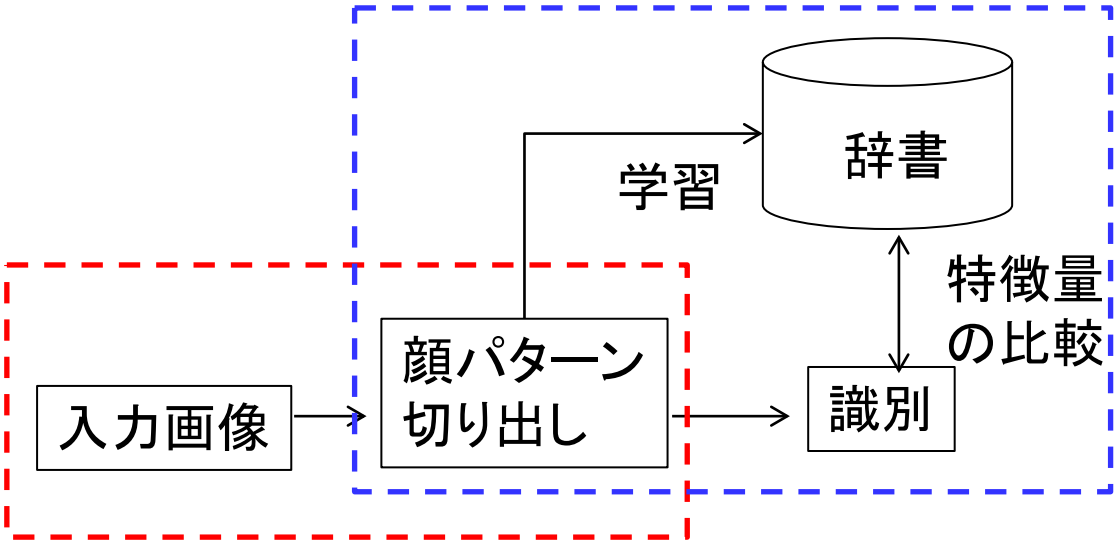
顔検出と顔認識

顔検出：

入力画像の中から，顔の位置を検出する技術

顔認識：

顔検出された画像の中から特定の人間の顔を認識する技術



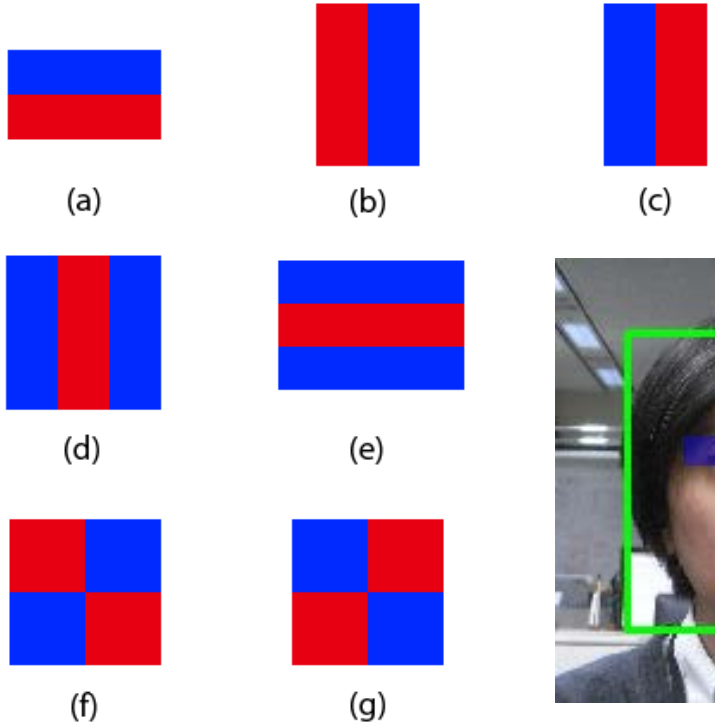
・顔検出の後に顔認識が行われる

・ 代表的手法：Viola-Jones法
・ 人の顔がもつ特徴量利用

➡ **Viola-Jones法に着目し，顔検出を失敗させる**

Viola-Jones法

- Haar-like特徴による特徴抽出
- マルチスケール検出アルゴリズム
- 複数の弱判別器から強判別器を構成（Boosting）
- 高い精度と高速な検出処理を実現



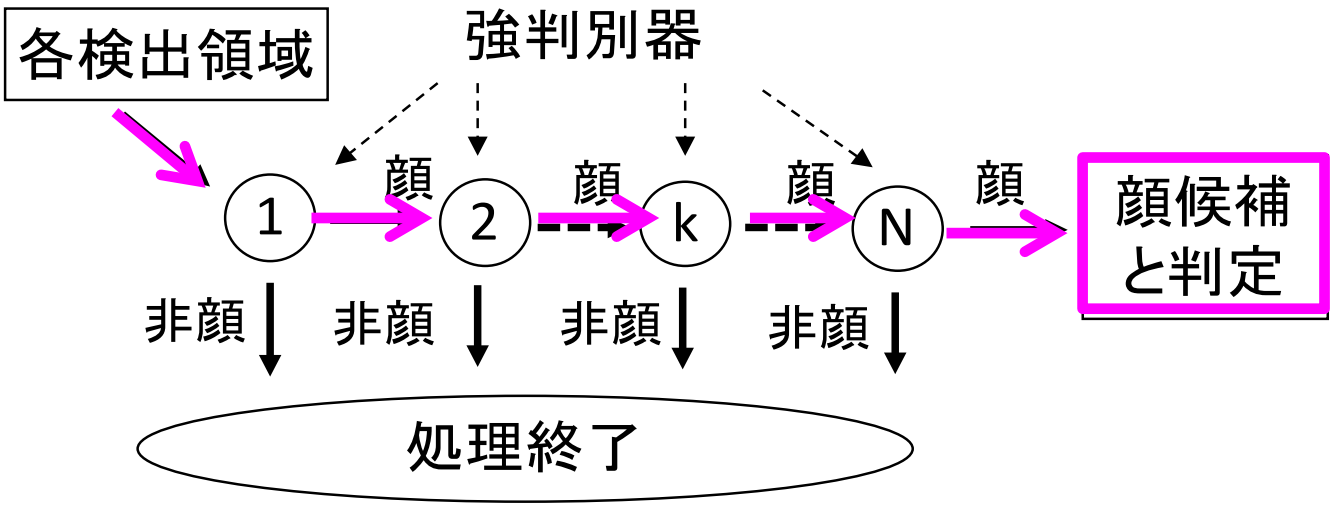
Haar-like特徴の例

検出領域と矩形特徴の重ね合わせの例

Viola-Jones法の原理

・Haar-like特徴量と閾値を比較し，特徴を判別する複数の弱判別器から成る強判別器を順に並べた多段のステージから構成

・教師あり学習により，顔検出に有効な矩形特徴の選択，強判別器内の弱識別器の構成，強識別器の連結順序を事前に決定



顔候補判定の手順：

・各検出領域に対して，順に“顔・非顔”の判別を行い，“非顔”の場合は 処理を終了

・全ての強判別器で“顔”と判定された場合，

➡ **当該領域における処理を終了**

ノイズ光源の配置

Haar-like特徴による特徴抽出を失敗させる効果的な配置の分析

・配置の特定：

- 学習後の Haar-like 特徴の重合せ

  赤い矩形内の数値：+1

  青い矩形内の数値：−1

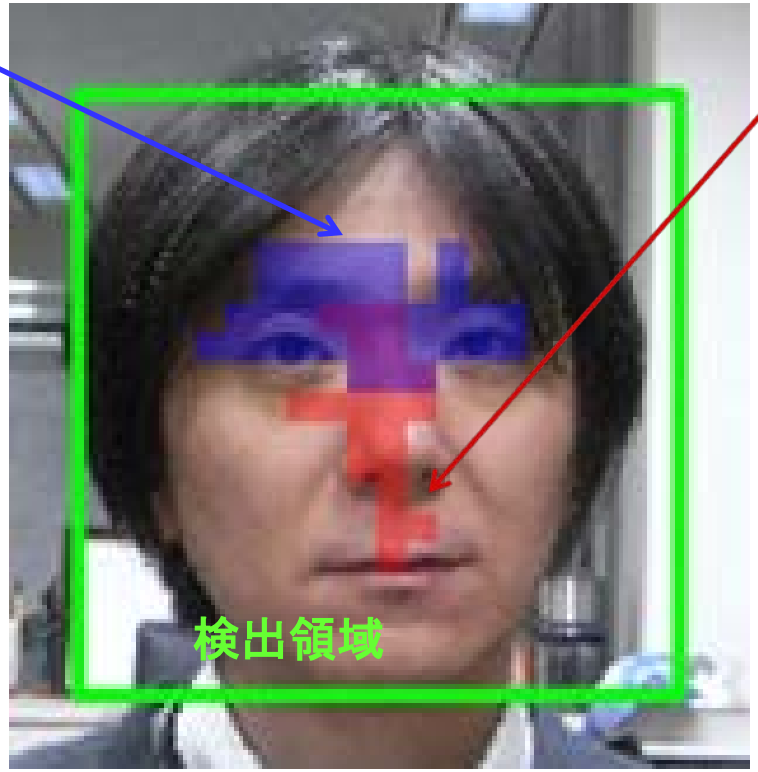
  として検出領域上に足し合わせる

・解析結果：

- **赤領域：鼻の周囲**
- **青領域：目の周辺**および**鼻筋**

青い矩形： 顔の輝度が暗い箇所→ 明るくすることで，特徴破壊

赤い矩形：：顔の輝度が明るい箇所→ 暗くすることで，特徴破壊



ノイズ光源の配置 ➡ 目の周辺および鼻筋

本発表の流れ

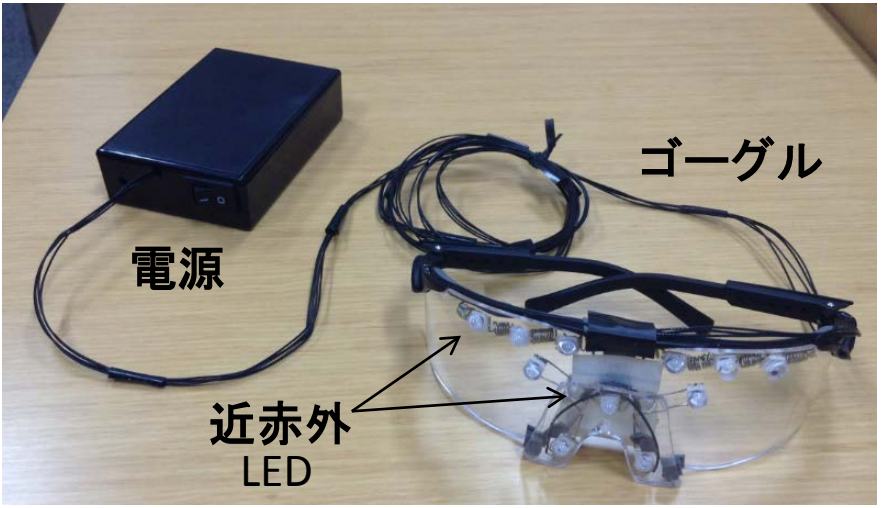
1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～ プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

プライバシーバイザー

市販ゴーグルに11個の近赤外LEDを取付け

顔検出を不能にするノイズ光源の配置

- **目の周辺　8個**(瞼両側:6個，瞳両側:2個)
  最内側2個:0°,その内側2個:20°　外側2個:30°
- **鼻筋周辺　3個**（鼻両側:2個，眉間:1個）



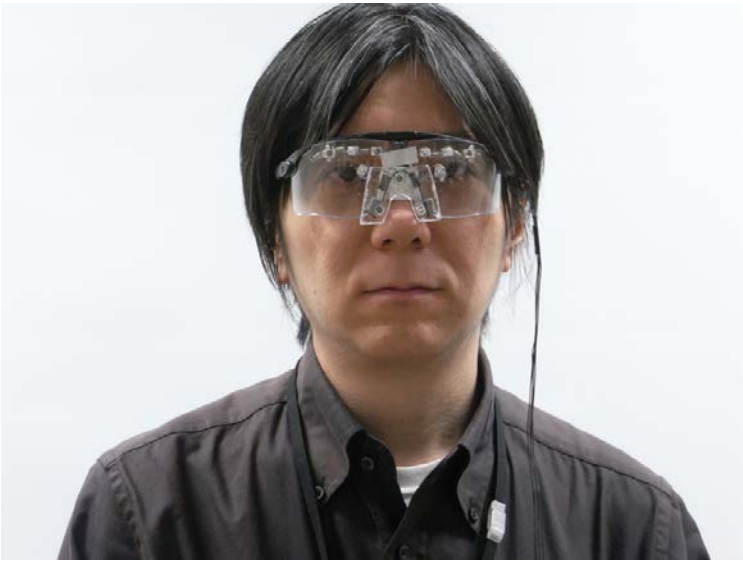
プライバシーバイザーの概観

プライバシーバイザーの仕様

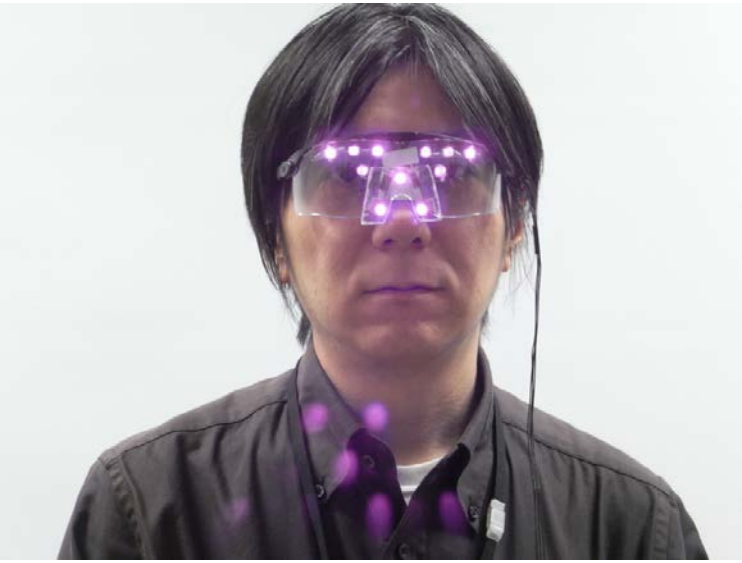
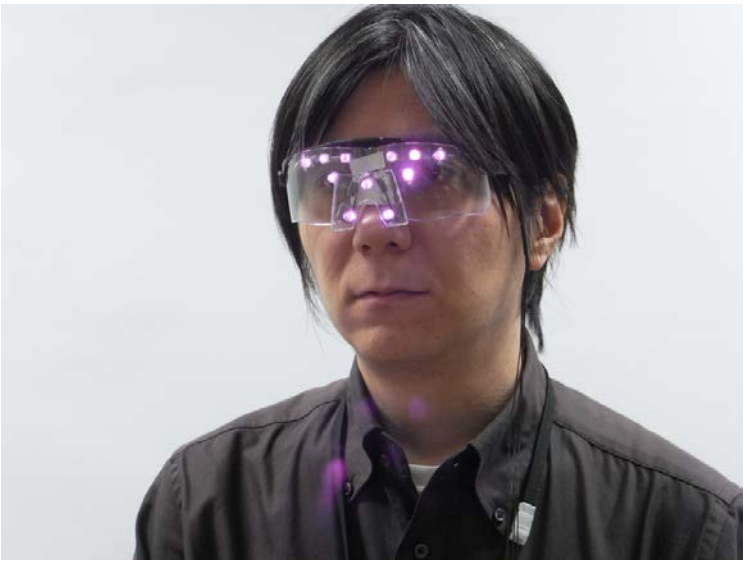
近赤外LED	個数: 11個, ピーク波長:870 nm, 放射強度:600mW/sr，放射角:±15° 定格電流:1A, 定格消費電力:2.1W
ゴーグル	フレーム材料:プラスティック, レンズ:ポリカーボネート,
電源	リチウムイオン電池 (3.7V×3) 2000mA/h

顔面上の違和感少なく，撮影時の顔検出を失敗させる

装着イメージ



ノイズなし

ノイズあり

本発表の流れ

1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

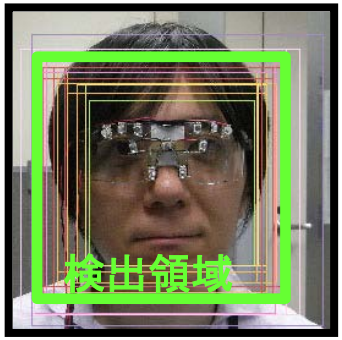
評価実験

- 被写体の条件ごとに写り込み画像を撮影し，Viola-Jones法に基づく顔検出を行い評価

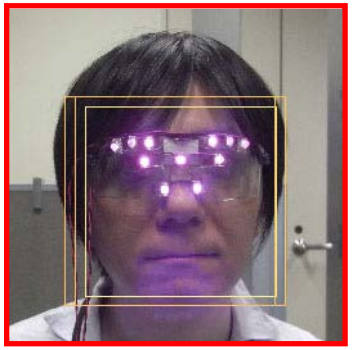
	被写体の条件
（ｉ）	プライバシーバイザー非装着
（ii）	プライバシーバイザー装着(ノイズ無し)
（iii）	プライバシーバイザー装着(ノイズ有り)

- **評価方法：**
  - 評価者：10人
  - 撮影距離：１－22 m
  - 撮影角度：　0°，10°，20°
  - Open CV（強判別器：個数N=20)よる顔検出ライブラリを使用
  - 10人の評価者の検出人数の分布図より評価

- **OpenCVによる顔検出：**
  - 全ての強判別器を通過した検出領域は“顔候補”となる
  - “顔候補”が含まれると判定された領域内に，その他の“顔候補”が含まれると判定された（近接するサイズの）検出領域の数 M（個）が



M≧２：顔検出



M<2：顔非検出

M≧2 →当該領域に顔があると判定し検出

M＜2 →当該領域に顔がないと判定し非検出

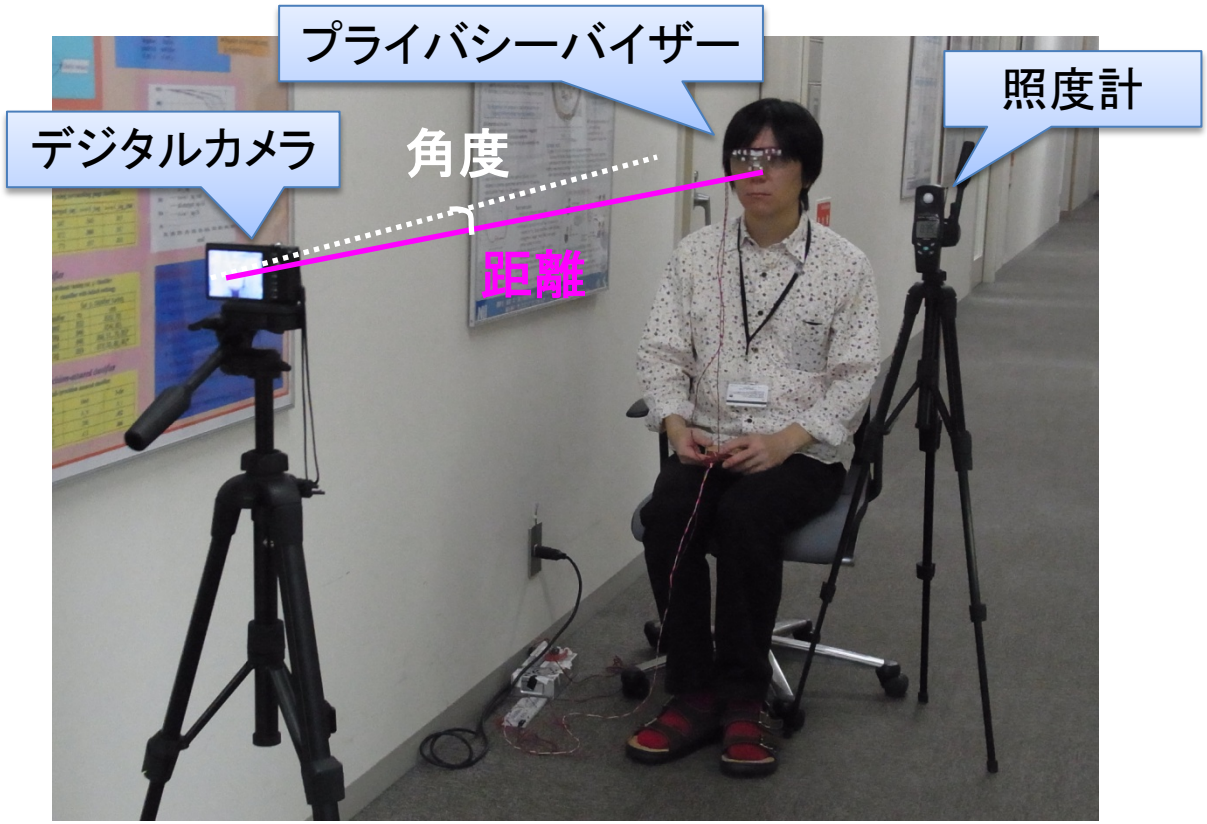
評価環境

デジタルカメラ

型番: Ricoh R10
画素数: 3264 x 2448 (8M)
フォーカス: スポットAF
測光: マルチ
絞り値: f/3.3 ※自動設定
露出時間: 1/10秒 ※自動設定

撮影環境

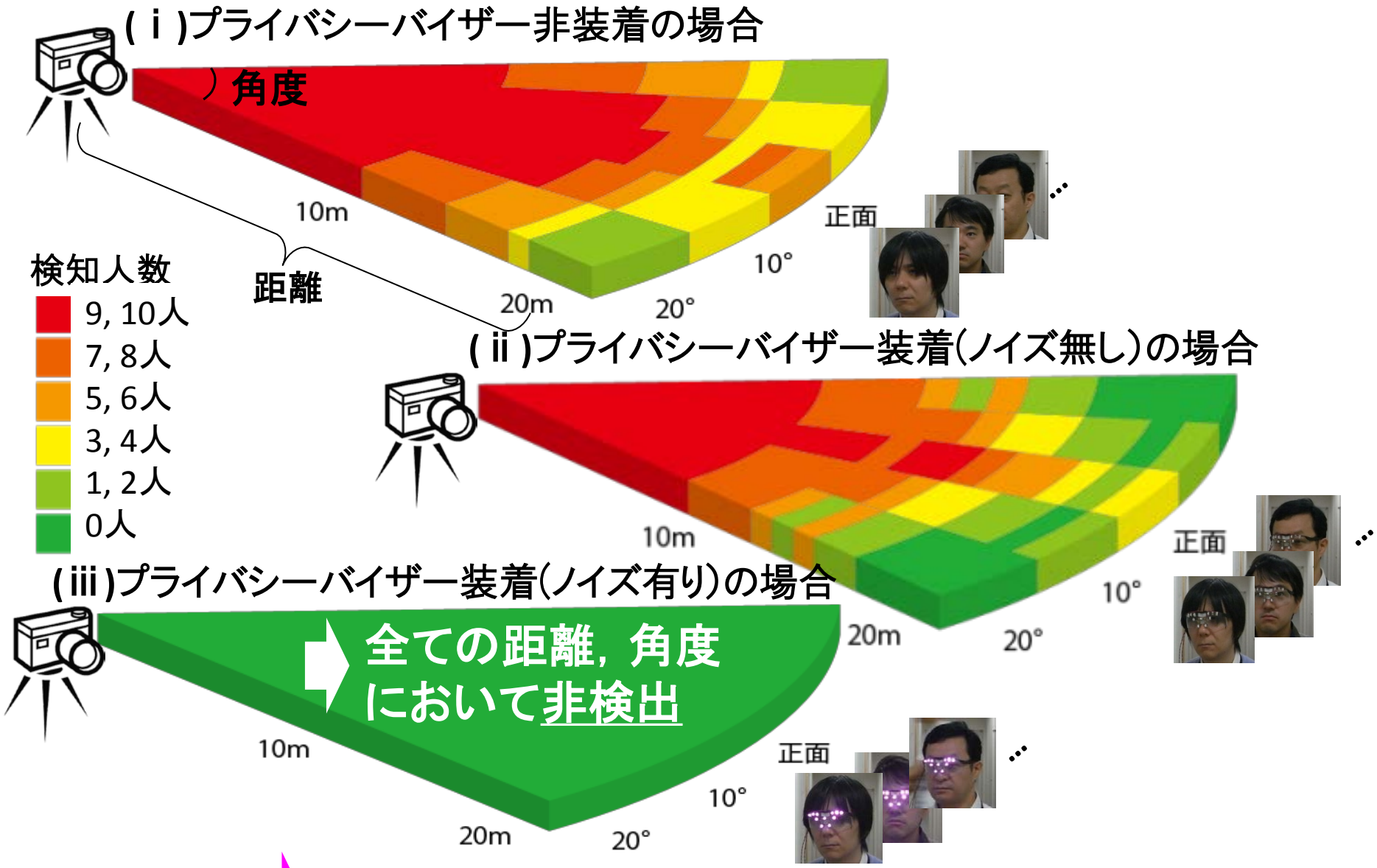
距離: 1～22m（1m刻み）
角度: 0°　／10°　／20°
照明: 蛍光灯 、67.5 Lux



➡ 評価者10人を異なる撮影**角度**及び**距離**で撮影

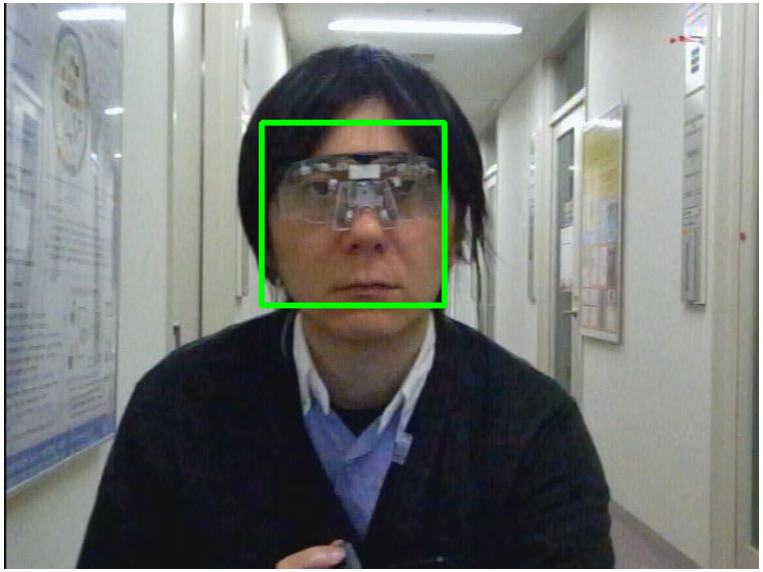
評価環境 (19mの距離から撮影)

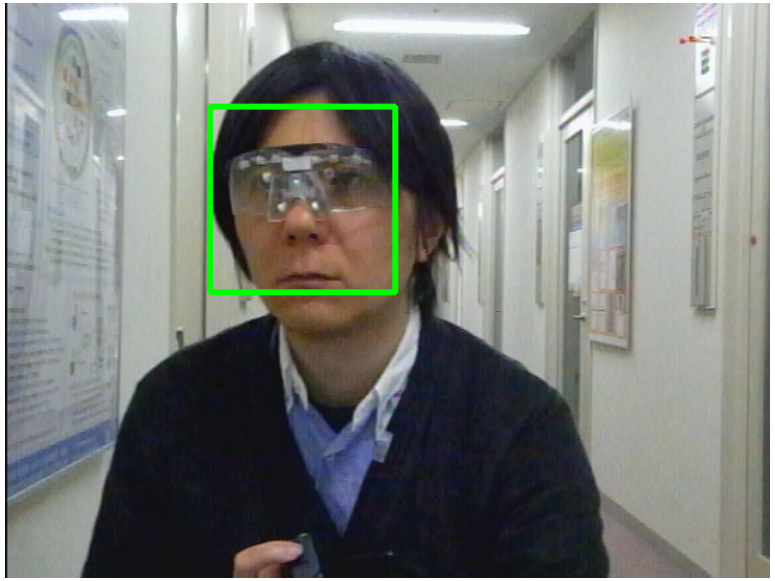
評価結果（検出人数の分布図）



提案手法：➡ 顔検出によるプライバシー侵害を効果的に防止可能

検出結果

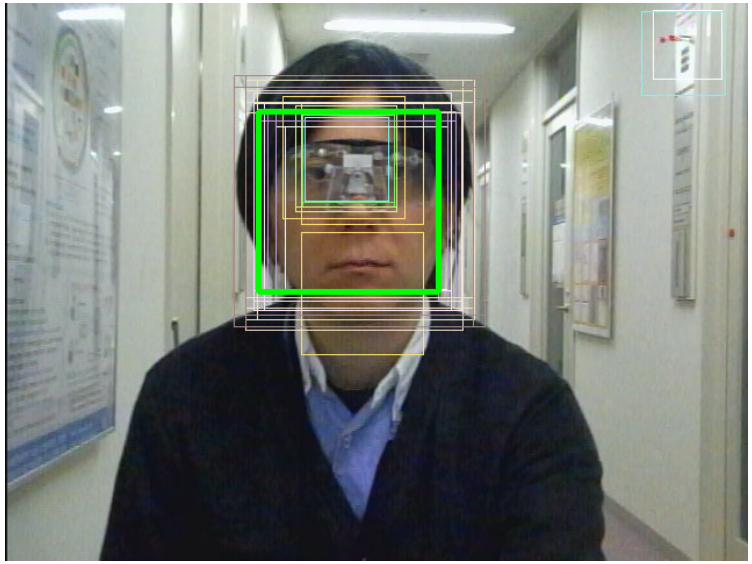


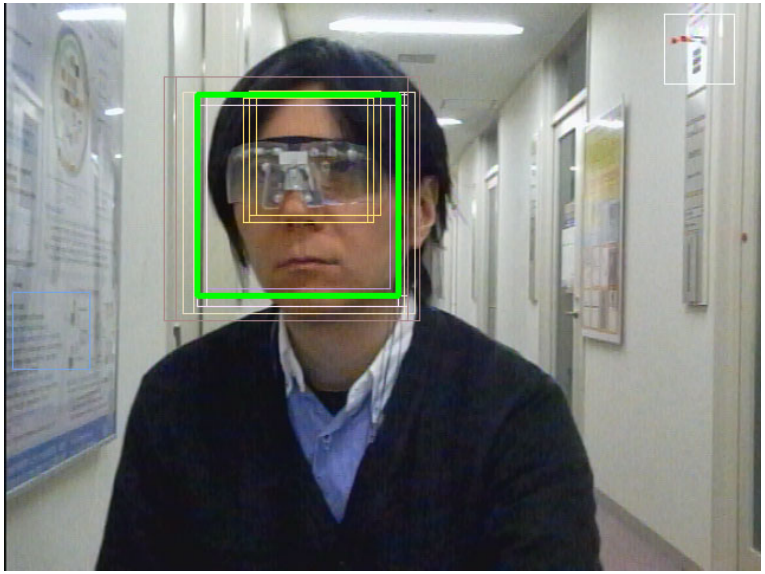


ノイズなし

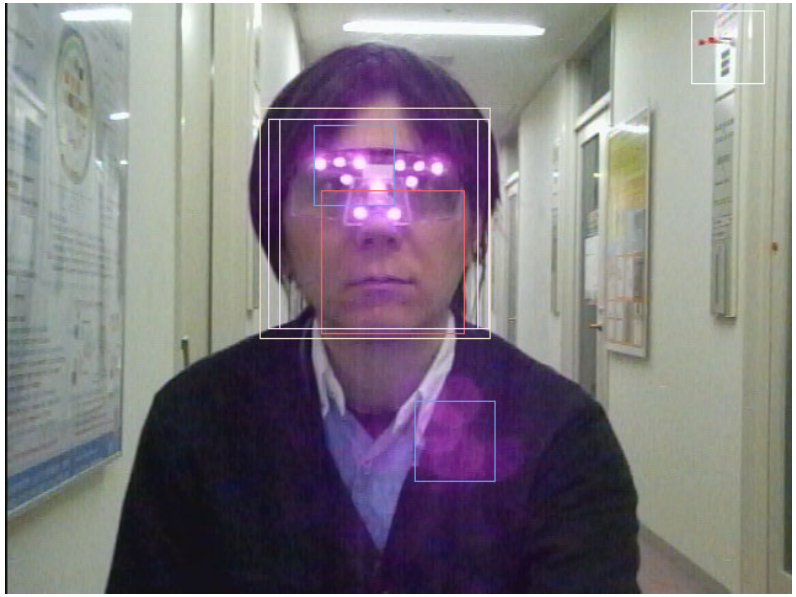
ノイズあり

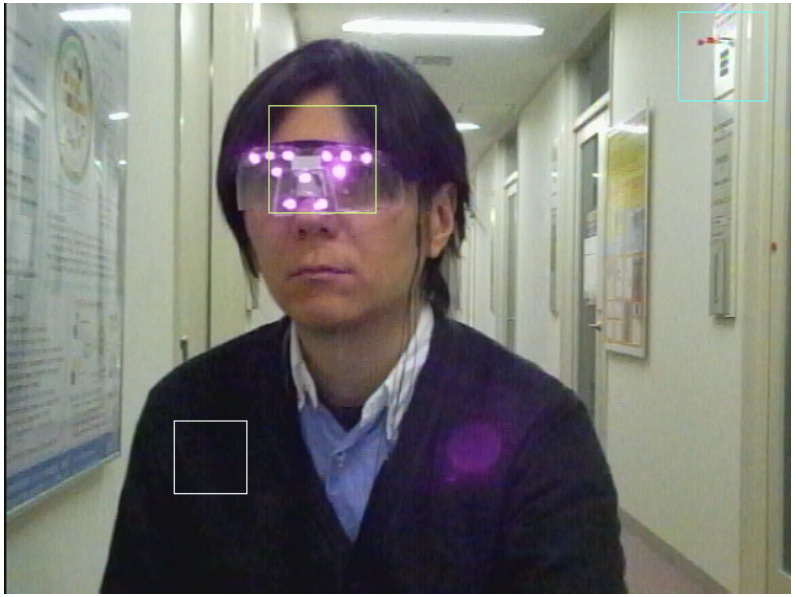
検出結果（詳細モード）





ノイズなし





ノイズあり

本発表の流れ

1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション

まとめ

- カメラ付き携帯端末の普及, SNSや画像検索技術の進展
  → プライバシー侵害
- 従来手法
  – 顔面への着色, 髪形の変更, 顔面を物理的に隠す方法
  → 物理空間における人対人のコミュニケーションに支障をきたす問題
- 写り込み防止の要件
  顔面上の違和感少なく, 撮影時の顔検出を失敗させる
- 代表的な顔検出法(Viola-Jones法)を解析
  顔面上の違和感少なく, 特徴を 破壊する箇所
  → 目の周辺および鼻筋周辺にノイズ光源を配置
- 写りこみ防止方式の実装(プライバシーバイザー)
  Viola-Jones法の解析に基づき市販ゴーグルに11個の近赤外LEDを取付け
- 評価実験
  プライバシーバイザー装着(ノイズ有り):(撮影範囲 1-22m, ±20°)顔非検出

➡ 顔検出によるプライバシー侵害を効果的に防止可能

今後の検討：電源が不要なプライバシーバイザー

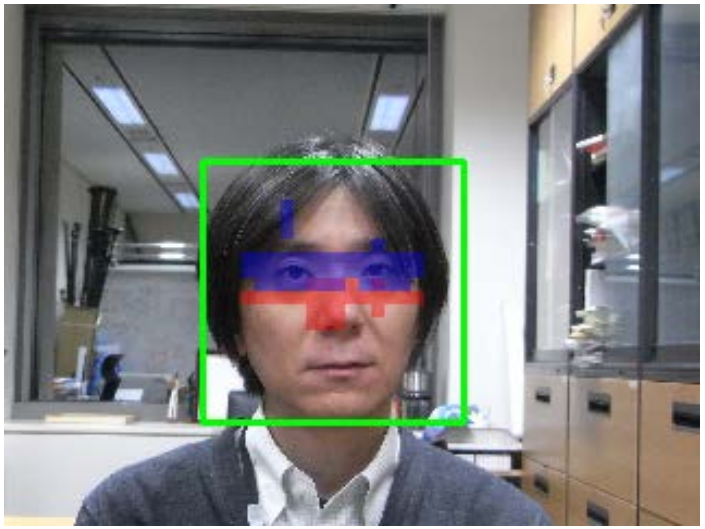
Haar-like特徴の低輝度部分または高輝度部分の特徴を崩すように下記部材を貼付

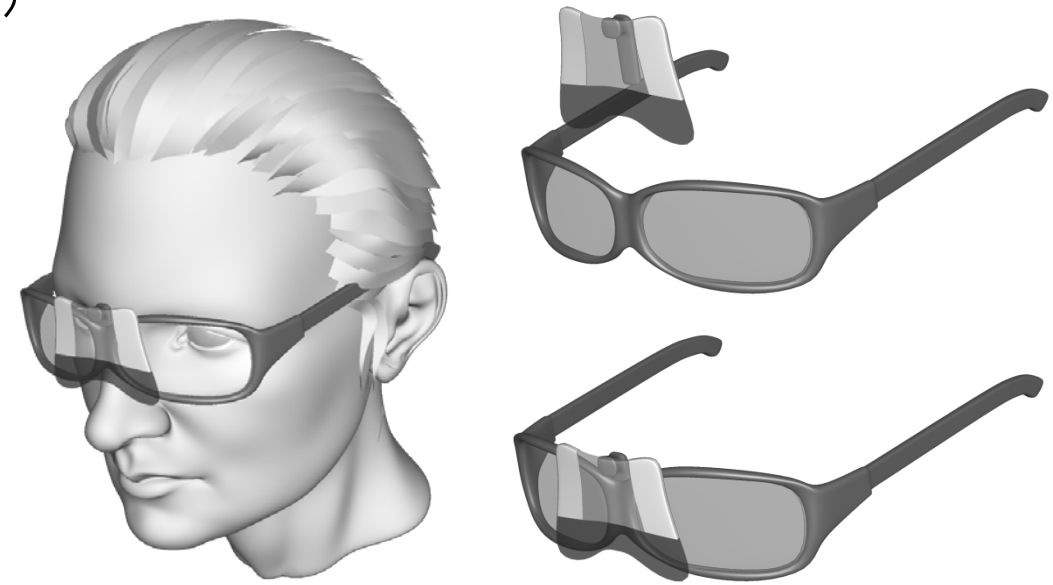
低輝度部分：

1. 入射光の特定波長または全波長を**一定方向に反射する部材**で構成される特徴を持つ高輝度化部材（例：光学フィルター）

高輝度部分：

2. 入射光の特定波長または全波長を**吸収する部材**で構成される特徴を持つ低輝度化部材（例：光学フィルター）
3. 一定角度以上かつ一定距離以上からの視認に対して，**当該領域を低輝度化する部材**（例：プライバシーフィルター）





参考：サングラスでは顔認識を失敗させることはできない

サングラス（5種類）をかけた入力画像は，Google Picasa(Google社の写真管理ソフト）の顔認識機能により，全て登録画像の人物として認識

サングラスでは顔検出を妨害することはできない

本発表の流れ

1. 研究背景
2. 提案方式
   ～カメラによる写りこみを被撮影者側から防止する方式 ～
3. 提案方式の実装
   ～プライバシーバイザーの実装 ～
4. 評価実験
5. まとめ
6. デモンストレーション