プライバシーバイザー
「追跡されない自由」

国立情報学研究所
越前 功

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

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 Glass(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

➡ **顔認識技術がプライバシー侵害につながる危険性**

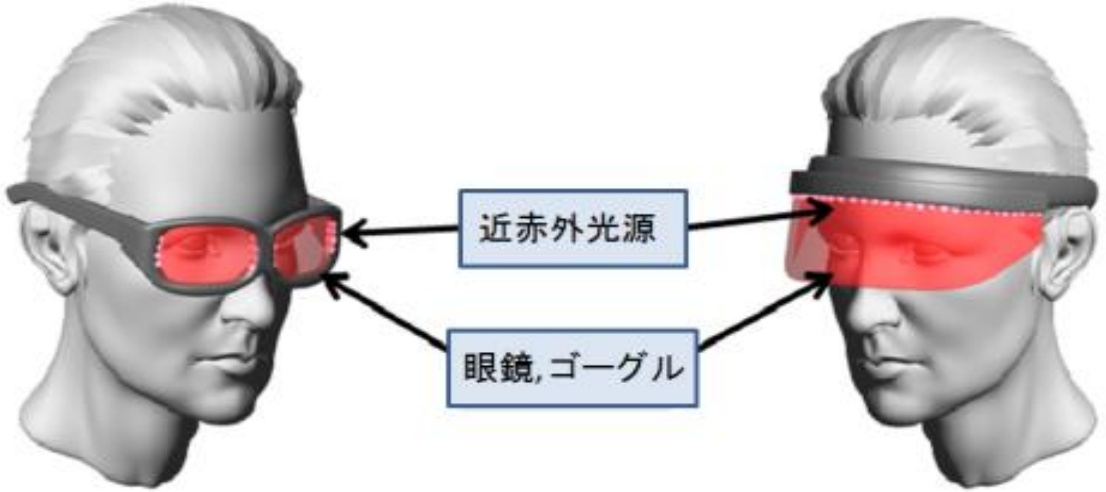
目的と手段

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:

人の視覚に影響を与えず，カメラの撮像デバイスに反応するノイズ（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？

ノイズ光源の配置

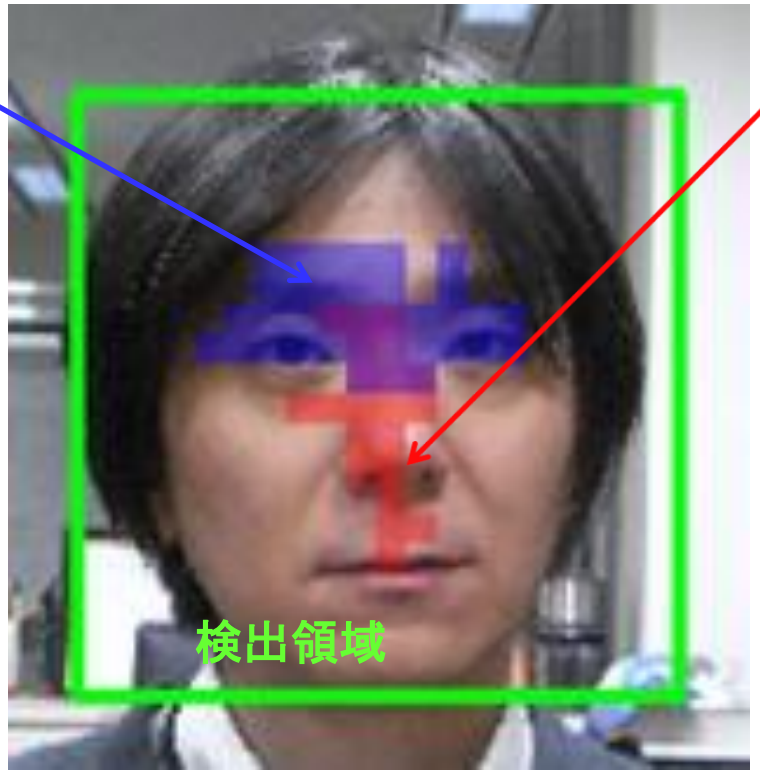
Haar-like 特徴量の特徴抽出を失敗させる効果的な配置の分析

- **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



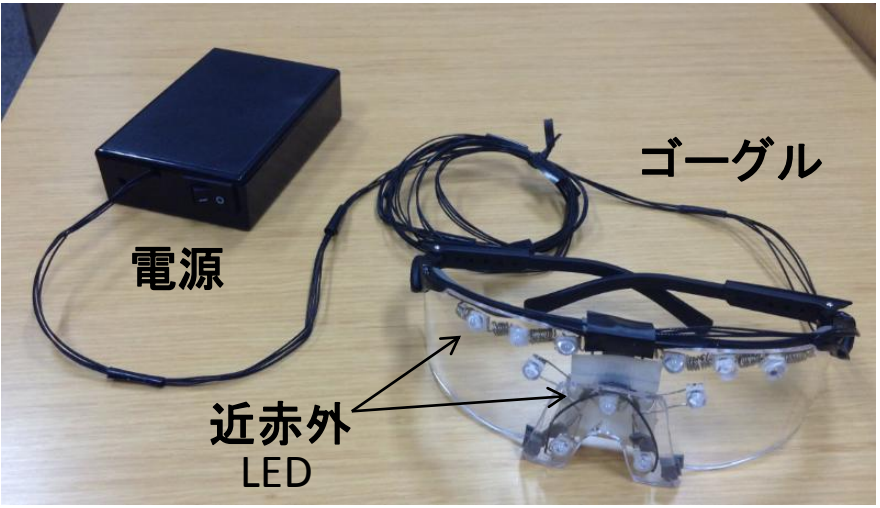
ノイズ光源の配置 ➡ **目の周辺および鼻筋**

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に基づき

- **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）



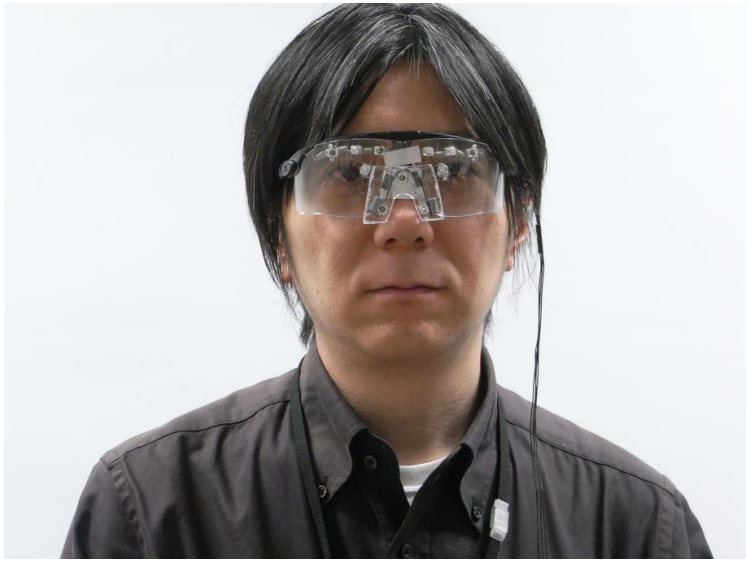
プライバシーバイザーの概観

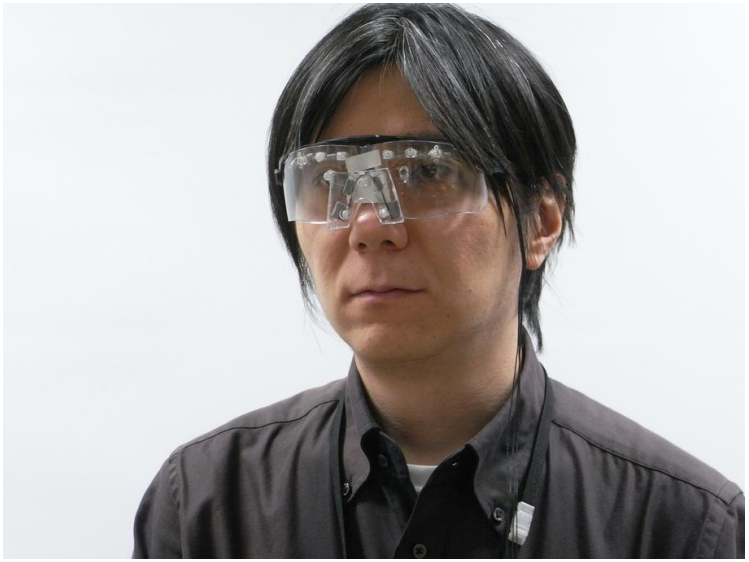
プライバシーバイザーの仕様

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

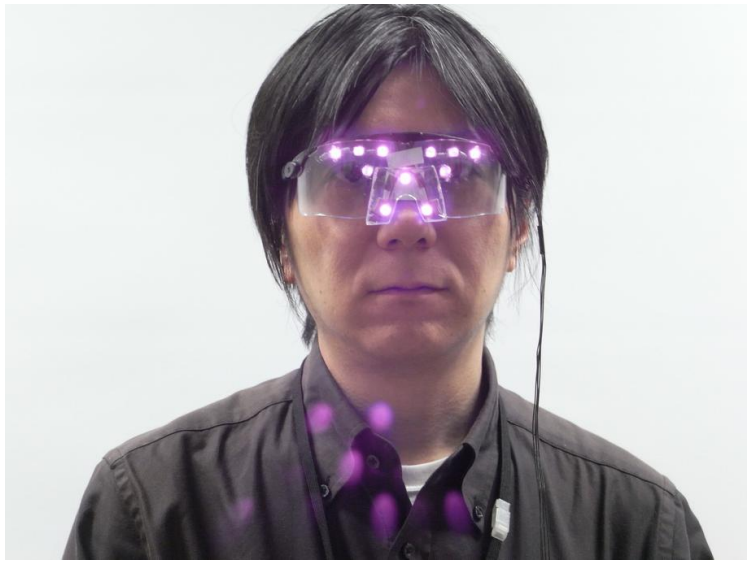
顔面上の違和感少なく，撮影時の顔検出を失敗させる

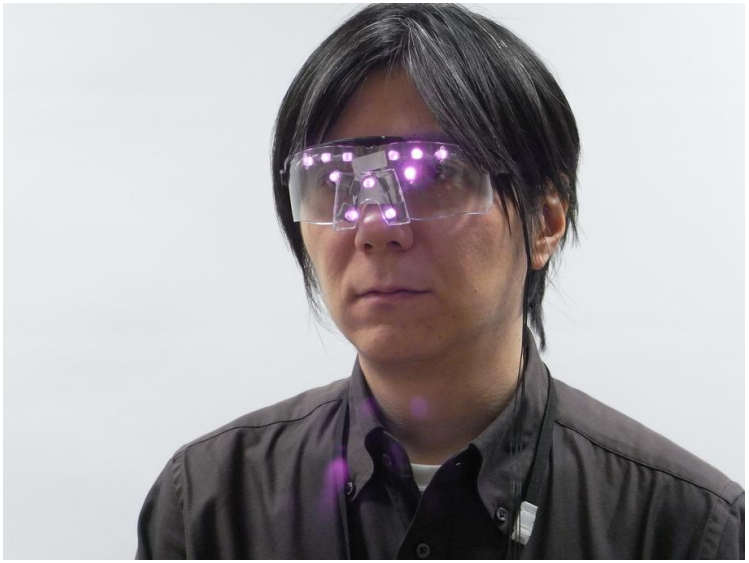
装着イメージ





ノイズなし





ノイズあり

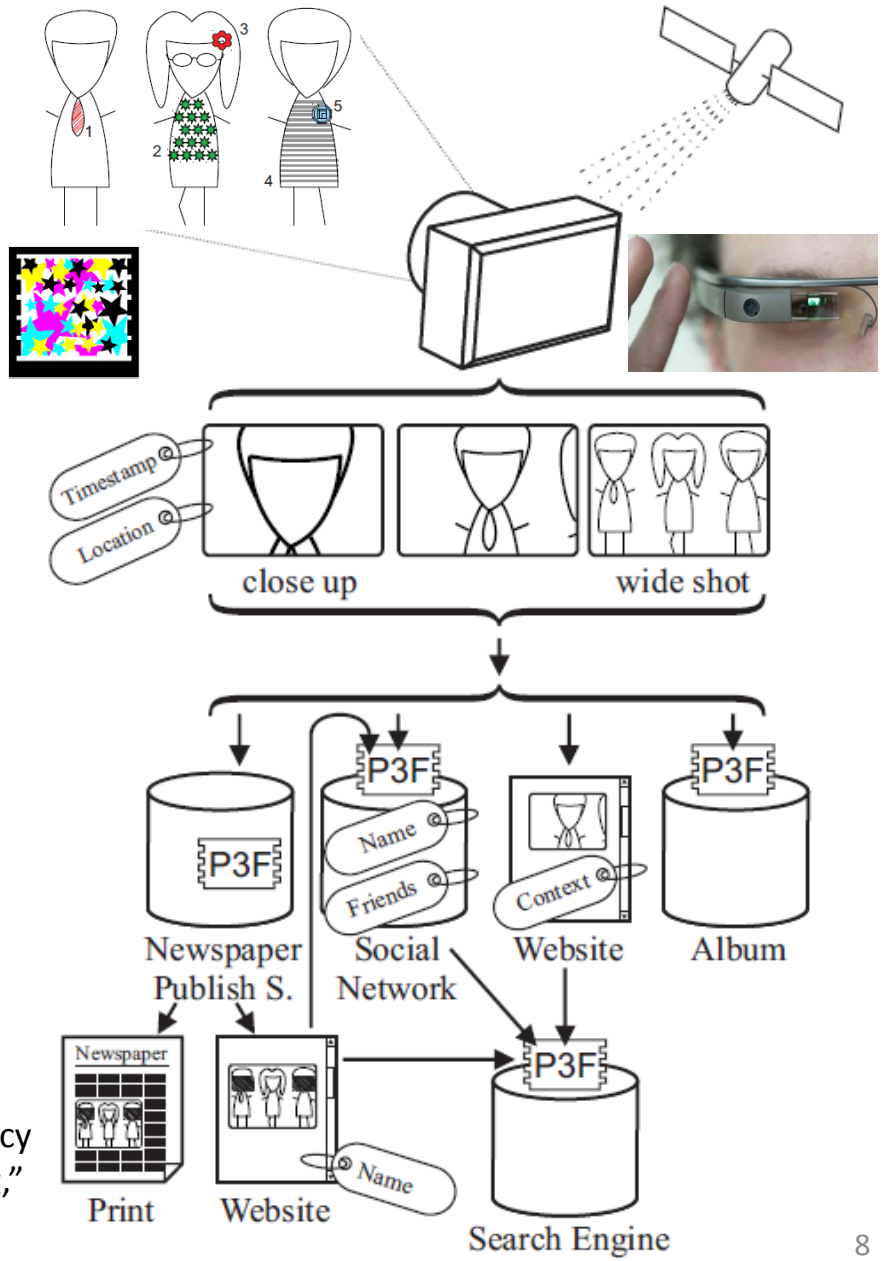
Personal Picture Policy Framework (P3F)[2]

写りこみや撮影時における個人のプライバシーポリシーを衣服やアクセサリなどに埋め込み

ISPに当該バーコードの検出器の実装を義務付け，写りこみや撮影を経由した個人のプライバシーを保護

TABLE I
PERSON-RELATED PRIVACY POLICY OPTIONS AND USAGE MATRIX

Personal Flag	Publish	Name, Identify	Index, Search
No Restriction (SIP)	✓	✓	✓
Do not Search (S)	✓	✓	✗
Do not Identify (I)	✓	✗	✗
Do not Publish (P)	blur face	✗	✗



[2] A. Dabrowski, E. Weippl, I. Echizen, “Framework based on Privacy Policy Hiding for Preventing Unauthorized Face Image Processing,” 7 pages, under review for IEEE SMC 2013.