

～写真共有によるプライバシー侵害を防止するには～ PrivacyTag: SNS投稿ユーザの主観的な判断基準のみに 依存しない被写体のプライバシー保護

町田 史門¹, 越前 功^{1, 2}

¹ 総合研究大学院大学, ² 国立情報学研究所

どんな研究？

多くの人々がSNSを通して、家族や友人などとのコミュニケーションを楽しんでいます。その一方で、友人やその他ユーザによる不用意なSNS投稿により、大小様々なプライバシー漏洩が発生しています。本研究では、SNSを安心・安全に楽しめるように、SNSユーザのプライバシーを効果的に守る手法を研究しています。本発表は、SNS投稿メッセージに含まれる**写真に写る/写り込む人物のプライバシー**に注目します。

何がわかる？

SNS投稿ユーザは、自身が持つ主観的な判断基準をもとに、投稿するか否かを判断しており、被写体となる人物のプライバシーポリシーを考慮していません。そこで、投稿時に被写体のポリシーを反映させる手法を検討します。具体的には、SNSへ写真投稿時に被写体が身に付けるプライバシータグを検知・解析し、そのポリシーに基づき被写体の顔領域を非特定化します。そして、タグごとにコミュニティを定義し、投稿の公開対象者を限定することで、被写体のプライバシーを保護します。

研究背景

Facebook, TwitterなどのSNSが幅広いユーザ層へ浸透

- 18才以上のインターネットユーザの72%がSNSを利用
- 画像投稿: Facebook 3億5000万枚/日, Instagram 7000万枚/日

<http://www.pewinternet.org/2013/08/05/72-of-online-adults-are-social-networking-site-users/>

➡ 不用意なSNS投稿によるセンシティブデータ漏洩のリスク

- 子供の可愛い、可笑しい写真を友人などのコミュニティへ共有したい願望、良い母・幸せな家族を演じたい願望 [P. Kumar et al. 2015]
- 他人が写った写真をSNSに公開することに問題意識がない傾向 [2014年度情報セキュリティに対する意識調査, 2015]
- 自身は適切な投稿判断の基準を持ち、常に正しい判断ができると考える → 喜怒哀楽などの感情に変化がある時、投稿判断を誤る傾向がある [Y. Wang et al. 2011]

大型連休前のSNS投稿注意喚起

SNS投稿時のトラブルを防ぐために：

- 位置情報等のメタ情報の削除
- 写真の被写体から事前に投稿許可を得る
- 不要な写り込みは特定出来ないように加工



<http://www.ipa.go.jp/security/txt/2015/05outline.html>

コミュニティ・状況に応じたプライバシーポリシー

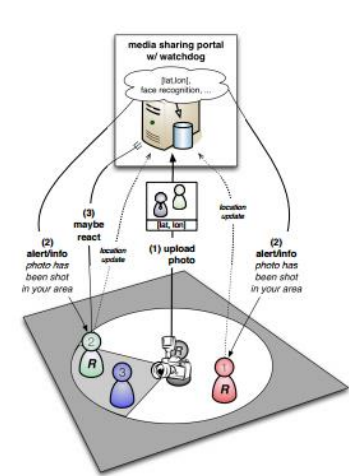
[P.Kumar et al. 2015]

- 写真などの投稿内容から自身の行動が他人に知られることを不快に感じる
- 特定の個人や興味を持つコミュニティへの限定公開要望 [M.Sleeper et al. 2013]

➡ 写真に写る/写り込む人物のコミュニティに応じたプライバシーに注目

従来手法

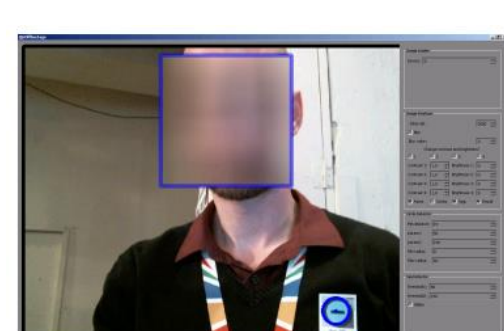
顔認識用いる手法



顔情報と位置情報をシステム上に登録し、他ユーザによる写真投稿時に顔認識を行い、当該ユーザに通知する手法

[Benjamin et al. 2013]

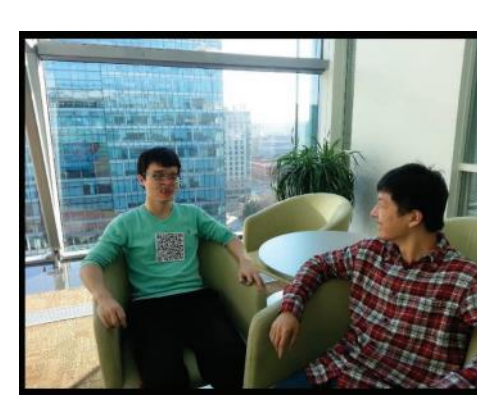
タグ認識用いる手法



[F.Pallas et al. 2014]

機械のみでなく、人間も容易に判断可能なプライバシーポリシー・タグを身につけ、撮影者にアピールする手法

QRコードベースのプライバシーポリシー・タグを利用してプライバシーをコントロールする手法



[C.Bo et al. 2014]

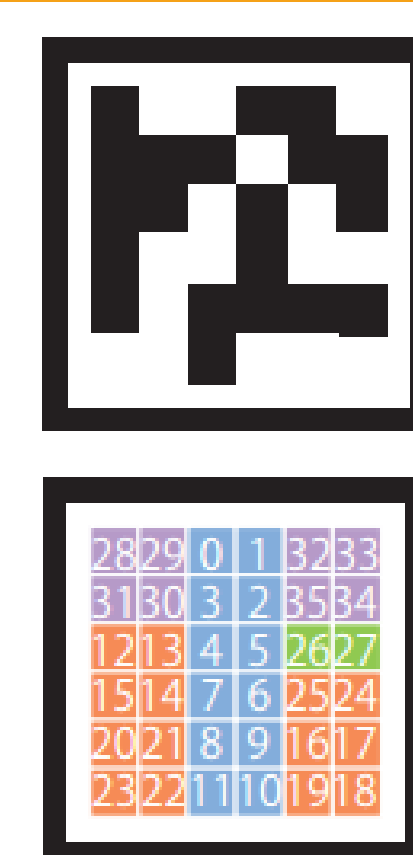
顔情報とプライバシーポリシーをモバイルデバイスに登録し、他ユーザによる写真撮影時にその撮影デバイスにポリシーを転送・適用する手法



[Papachan et al. 2014]

提案手法

ユーザのプライバシーポリシー、および属するコミュニティ情報をビットパターンとして埋め込み、顔領域の公開可否とそのSNS公開範囲をコントロールする



パターン配置 (計36 bit)

- コミュニティID: 14 bit
- 公開ポリシー: 2 bit
- エラー訂正: 8 bit
 - リードソロモン符号
 - 1情報シンボル(4 bit)の訂正



1. 写真撮影



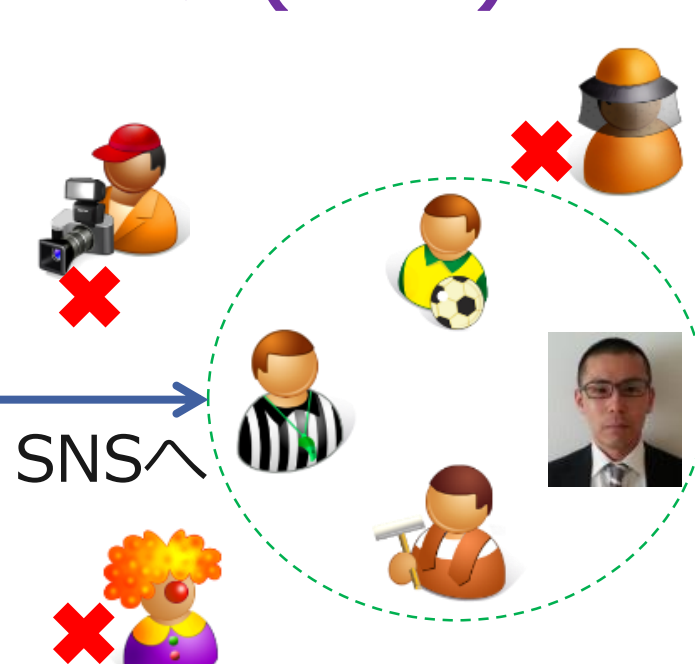
2. 顔検知

3. タグ検知・解析

4. 顔の非特定化



5. SNSへ



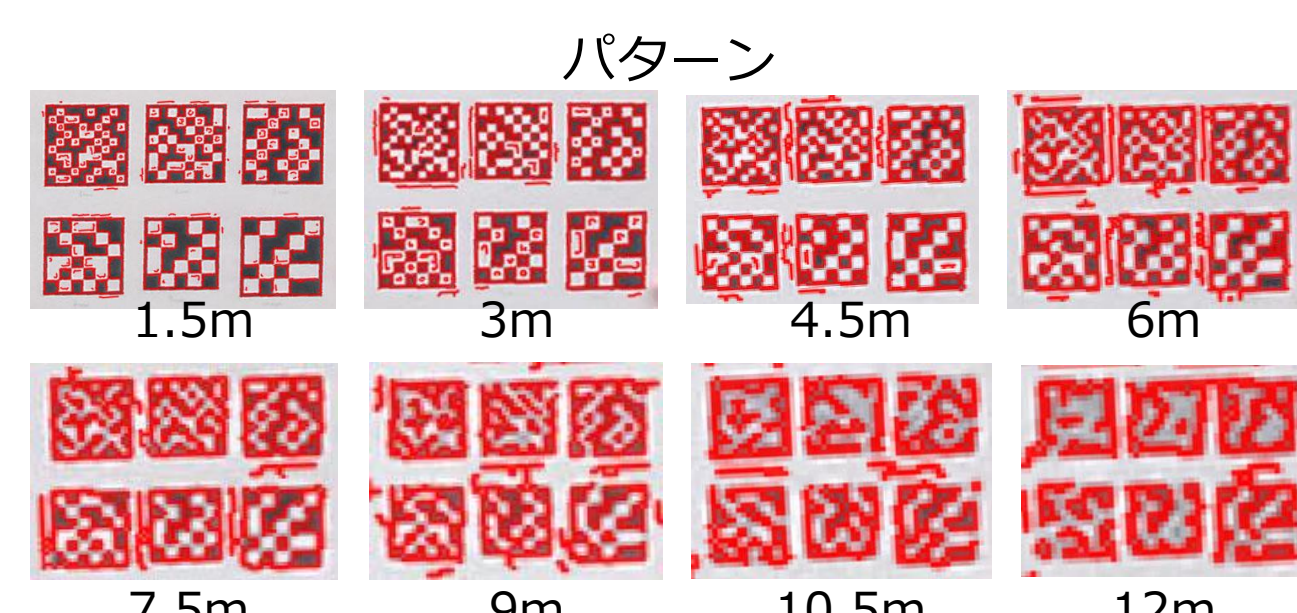
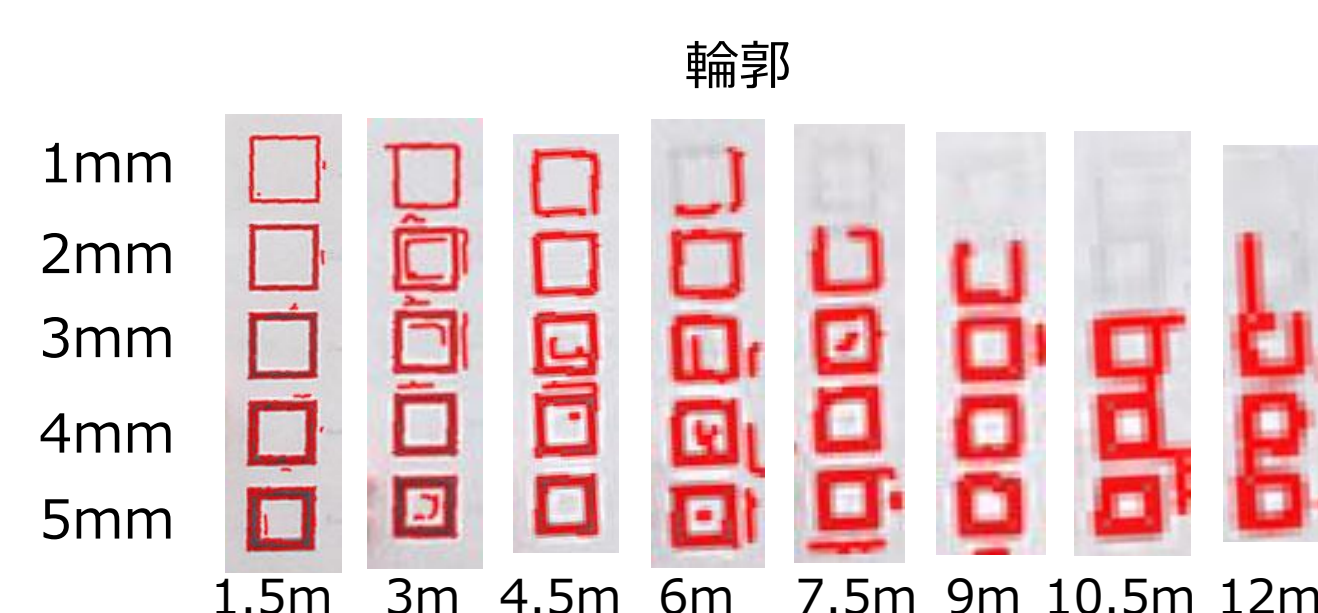
評価

予備評価：タグデザイン・検知手法検討

提案手法：プライバシータグ



幅3mm, 距離6m以下で概ね検知可



評価：被写体までの距離とタグサイズの検討

実用的なサイズ: 5cm以下で社会距離（～350cm）公共距離の一部までは検知可能

提案タグ

サイズ/距離	45 cm	82.5 cm	120 cm	235 cm	350 cm	450 cm	550 cm	650 cm	750 cm	850 cm	950 cm	1050 cm
2 cm	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA	NA	NA
3 cm	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA	NA
5 cm	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA	NA
7.5 cm	✓	✓	✓	✓	✓	✓	✗	NA	NA	NA	NA	NA
10 cm	✓	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA

密接距離 個人距離 社会距離 公共距離 Hallによるパーソナルスペースの分類, 1966



従来手法：QRコード



被斜体との距離制約が課題



QRコードタグ

サイズ/距離	45 cm	82.5 cm	120 cm	235 cm	350 cm	450 cm	550 cm	650 cm	750 cm	850 cm	950 cm	1050 cm
2 cm	✓	✓	✓	NA	NA	NA	NA	NA	NA	NA	NA	NA
3 cm	✓	✓	✓	✓	NA	NA	NA	NA	NA	NA	NA	NA
5 cm	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA	NA	NA
7.5 cm	✓	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA	NA
10 cm	✓	✓	✓	✓	✓	✓	✓	✓	NA	NA	NA	NA

SNSに投稿される写真の撮影距離として考えられる社会距離がカバーできていない

