プライバシータグによるコミュニティを考慮した被写体のプライバシー保護手法

町田 史門† 越前 功†‡

†総合研究大学院大学
101-8430 東京都千代田区一ツ橋 2-1-2
‡国立情報学研究所
101-8430 東京都千代田区一ツ橋 2-1-2
{shmachid, iechizen}@nii.ac.jp

あらまし SNSが幅広い年代に普及し，友人・知人と画像を含むメッセージを介したオンラインコミュニケーションが日常化している．ユーザが手軽に撮影・投稿できる一方で，不用意な投稿によるセンシティブデータ漏洩が問題となっている．本稿では，このようなセンシティブデータ漏洩のうち，写真に写る/写り込む人物に注目する．写真に写る人物のプライバシーを保護するために，当該人物が属するコミュニティ内外におけるプライバシーの振舞いをポリシとして埋め込んだタグを用いて，コミュニティ内外で当該人物の顔領域を適応的に保護する手法を提案し，本手法の主要機能であるプライバシータグの評価，およびプロトタイプアプリケーションの開発を行った．

A method of privacy protection based on community by privacy tag for photographic subject

Shimon Machida† Isao Echizen†‡

†The Graduate University for Advanced Studies
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, JAPAN
‡National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, JAPAN
{shmachid, iechizen}@nii.ac.jp

Abstract People of all ages are using Social Networking Services on a daily basis in these days. SNS users can take a photo and post a message easily. On the other hand, this raises leakage of sensitive data by unintentional posting. In this paper, we focus a photographic subject in a photo within like this leakage of sensitive data. In order to protect the privacy of a photographic subject, we proposed a method of protecting the subject's face area adaptively using privacy tag that contains one's privacy behavior within and without a community as privacy policy. Moreover, we evaluated the privacy tag and developed prototype application based on the method.

1 はじめに

Facebook, Instagram に代表される Social Networking Service (SNS) が幅広い年代に普及し，友人・知人と写真や動画を含むメッセージを介したオンラインコミュニケーションが日常化している．これら SNS において 1 日あたりに投稿される写真は Facebook が 3 億 5000 万枚, Instagram は 7000 万枚におよび，SNS ユーザは日常の出来事をスマートフォン等のカメラ付きデバイスを用い手軽に撮影し，メッセージを添えて SNS へ投稿している．

手軽に撮影・投稿できる一方，ユーザの不用意な投稿によるセンシティブデータの漏洩が問題となっている[1, 2]．情報セキュリティの倫理に対する意識調査[3]では，70%の調査対象者が他人の写った写真を SNS に公開することに対し，問題意識がない傾向であった．このような状況を受け，SNS 投稿時の不要なトラブルを避けるための注意喚起[4]として，投稿前に (1) 位置情報等のメタ情報の削除，(2) 写真の被写体から事前に投稿許可，(3) 不要な写り込みに対して特定ができないよう加工が推奨されている．しかし，投稿の都度，適切な対応を施すことは困難であるため，簡易に対処する手段が必要である．

実生活において，人々はそれぞれ異なるプライバシーポリシを持ち，同様に，同一人物であっても，自身が属するコミュニティ等の状況に応じた異なるポリシを持っている[5]．SNS においても，投稿メッセージに対して，アクセス可/不可とする友人をサブセット化したリストを用いて，ユーザが属するコミュニティを複数定義し，投稿内容に応じて，これらのコミュニティを使い分けている[6]．自身のコミュニティ内においては，投稿内容に応じて特定個人や興味を持つコミュニティに対して，公開・共有したい願望を持つ [7, 8]．一方，コミュニティ外において，自身が意図するプライバシーポリシと異なる場合は，写真や投稿メッセージに含まれる，誰が何をしているかといった行動内容を他人に知られることを不快に感じている[9]．このように SNS が提供する保護機能以外に，コミュニティに応じたプライバシーポリシを反映する機能が必要である．本論文では，このようなセンシティブデータ漏洩のうち，写真に写る/写り込む人物のプライバシーに注目する．

写真に写る人物のプライバシー保護を目的とした従来手法において，撮影者が容易に判断可能な単純化されたタグ[10]や，多くのポリシを埋め込んだ QR コードベースのタグ[5]が提案されている．しかし，単純化されたタグはコミュニティに応じたプライバシーの振舞いを表現できない．また，QR コードのように多くの情報を含む複雑なタグは，被写体までの距離が理由による検知・解析精度に課題がある．

本論文では，写真に写る人物のプライバシーを保護するために，当該人物が属するコミュニティ内外におけるプライバシーの振舞いをポリシとして埋め込んだタグを用いて，コミュニティ内外で当該人物の顔領域を適応的に保護する手法を提案する．さらに，本手法で用いるプライバシータグの評価として，従来手法で用いられる QR コードベースのタグと我々が提案するタグを比較・評価するとともに，本手法を適用したプロトタイプアプリケーションを開発する．本手法を適用することにより，SNS 投稿ユーザ，または写真の撮影者の主観的な判断基準に依存することなく，被写体のプライバシーポリシに基づいたプライバシー保護を行うことが可能となる．

2 被写体のプライバシー保護

2.1 SNS ユーザのプライバシー保護

SNS 提供者側では，ユーザのセンシティブデータの漏洩を防ぐために，様々なプライバシー設定機能を提供している．しかし，プライバシー管理は複雑性があり，その維持に多くの労力が必要とされる[6]．そのため，投稿の公開範囲設定など，情報の開示境界に関する研究[6, 11, 12]が活発に行われている．ただし，多くの従来研究は，投稿ユーザ自身のプライバシー保護を主目的としており，投稿内容に含まれる他ユーザのプライバシーには注目していない．具体的には，SNS へ投稿する写真に写る/写り込む人物を含む被写体のプラ

イバシーを考慮する必要がある．そこで，投稿ユーザの判断基準に依存したプライバシー保護ではなく，被写体のプライバシーポリシを反映させる手法を検討する．

2.2 被写体のプライバシーポリシ適用

SNS 投稿時に被写体のプライバシーポリシを反映させるためには，被写体のポリシを投稿ユーザに参照させる必要がある．その際，考え得る手法としては，以下が挙げられる．

- 顔認識を用いる手法： 予め，顔の特徴量とプライバシーポリシを紐付け登録し，投稿時の顔認識により被写体のポリシを適用
- タグ認識を用いる手法： 自身のポリシを埋め込んだタグを身につけ，投稿時にタグ解析を行い，被写体のポリシを適用

顔認識を用いる手法として，Benjamin らは，予め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[13]を提案する．また，自身の顔情報とプライバシーポリシをスマートフォン上に登録しておき，他人による写真撮影時に，その撮影デバイスへ自身のポリシを転送・適用させる手法[14]が提案されている．これらの手法の場合，タグを常に身に付ける煩雑さがないものの，システム上に顔の特徴量等の人体特性を登録する必要があるため，プライバシー懸念を理由にユーザから利用を拒否される可能性がある[15].

一方，タグ認識を用いる手法では，機械のみでなく，人間も容易に判断可能な単純化されたタグを身に付け，周囲にアピールする手法[10]や，QR コードに多くのポリシを埋め込み，プライバシーをコントロールする手法[5]が提案されている．しかし，単純化されたタグは，コミュニティや状況に応じたプライバシーの振舞いを表現し難い．また，QR コードのように多くの情報を含む複雑なタグは，被写体までの距離が理由による検知・解析精度に課題がある．

2.3 プライバシーアピール

タグ認識を用いる手法により，プライバシーポリシを含むタグを身に付ける場合，自身のプライバシーポリシを周囲にアピールすることになる．自身のポリシをセンシティブデータの 1 つと捉え，隠すべきとする考え方もあるが，撮影者にプライバシーアピールをすることで，被写体のポリシ尊重を促す効果がある[14].

そこで，本提案では，システム上に人体特性の登録を必要としないタグ認識を用いる手法を採用し，撮影時に被写体が身に付けたタグから取得したポリシを適用させることとした．

3 被写体のプライバシー保護スキームの提案

写真に写る/写り込む人物のプライバシーを保護するために，当該人物が属するコミュニティ内外におけるプライバシーの振舞いをポリシとして埋め込んだタグを用いて，コミュニティ内外で当該人物の顔領域を適応的に保護する手法を提案する．本手法を適用すると，SNS へ写真投稿時に，写真に写る人物が身に付けたタグを検知･解析し，その結果得られるポリシに基づき，当該人物の顔領域を暈して非特定化する．また，タグに含まれるコミュニティ情報を用いて，予め，ユーザが属するコミュニティの定義と，そのコミュニティに属するその他ユーザを紐付ける．これにより，ユーザはコミュニティごとに異なるポリシを持つタグを身に付けることで，状況に応じたプライバシーの振舞いが可能となる．さらに，コミュニティの所属ユーザを投稿の公開対象者として利用することで，投稿メッセージの公開範囲を限定し，センシティブデータの漏洩を防ぐ．

本提案スキームは，(1) プライバシータグ，(2) Photo Privacy Realizer，(3) Privacy Wall の 3 つの主要機能から構成される．次節では，これら機能の説明，提案スキームの流れを説明する．

3.1　プライバシータグ

プライバシータグとは，インターネット上で自身の情報を公開/非公開といったプライバシーの振舞いと，その振舞いを適用するコミュニティ情報をプライバシーポリシとしてシンボル化したタグである．ユーザは，衣服やアクセサリ等，ファッションの一部として本タグを身に付け，周囲に自身のプライバシーポリシをアピールする．プライバシータグのデザインおよび評価については，4 章で説明する．

3.2　Photo Privacy Realizer

Photo Privacy Realizer (PPR) は，SNS 投稿時に，写真から人物の検知，当該人物が身に付けるプライバシータグの検知および，解析を行い，取得したポリシに基づき，その人物の顔領域の保護を実現する Web アプリケーションである．ユーザがスマートフォン等から利用することを想定しており，(1) コミュニティ管理，(2) 写真撮影および SNS 投稿 の 2 機能から構成される．PPR は，取得したポリシに従い，被写体の顔領域に暈しを入れて非特定化する．そして，非特定化後の写真とメッセージをコミュニティメンバのみに限定公開する．5 章でこれら機能を実現したプロトタイプの PPR を説明する．

3.3　Privacy Wall

Privacy Wall とは，PPR 以外のデバイスで撮影・投稿される際に，プライバシータグを身に付けた被写体のプライバシー保護を行う機能である．本機能は，SNS 提供者の機能の一部として構築され，投稿時にタグ検知のみを行い，タグを身に付けた全被写体の顔領域を非特定化する．なお，本論文では機能の提案のみとし，今後検討を行う．

3.4　提案スキームの流れ

提案スキームのプロセスフローを図 1 に示す．

1. タグの入手

プライバシータグは，タグを取り扱う店から，共通のコミュニティ ID を含む全公開/コミュニティ内公開/非公開を示す 3 種のタグを束ねたタグパックとして購入，または，ユーザ自身によるタグのプリントが可能である．

2. タグのアクティベートとコミュニティ登録

タグを入手後，PPR を利用して，タグのアクティベートと新たなコミュニティを登録する．また，コミュニティに所属するメンバを Facebook の友人リストから選択して紐付ける．各コミュニティメンバは，自身のプライバシーポリシに合致するタグを身に付ける．

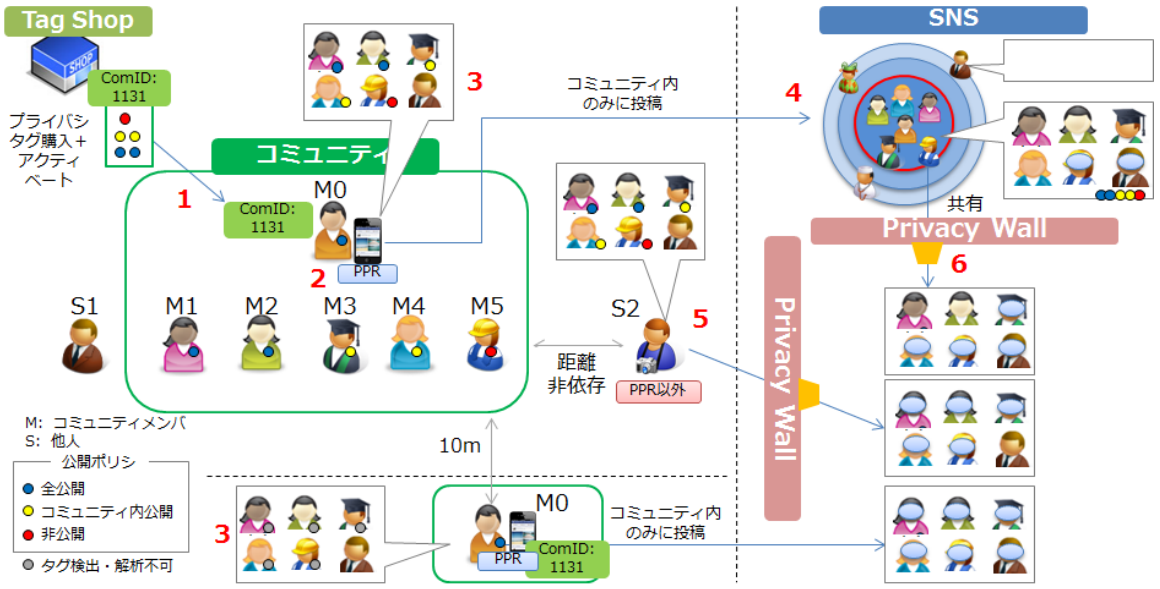


図 1　提案スキームのプロセスフロー

3. 写真撮影と非特定化

PPR を利用して写真を撮影するが，その際，被写体が身に付けたタグを解析する．この時，被写体のポリシが“非公開”の場合は，顔領域に暈しを入れる．また，当該写真にコミュニティメンバ外の他人が写り込んでいる場合，タグを身に付けていないためポリシを取得できないが，プライバシーを尊重して非特定化する．同様に，被写体からの距離等が原因により，タグを検知したが，解析ができない場合も当該被写体を非特定化する．

4. SNS 投稿

保護処理後の写真にメッセージを添え，SNS へ投稿する．その際，当該コミュニティのメンバを対象に限定公開する．

5. PPR 以外のデバイスによる撮影・投稿

コミュニティメンバ外の他人が PPR 以外のデバイスで撮影・投稿したとする．この場合，SNS 提供者側に構築される Privacy Wall により，タグの検知のみを行い，タグを身に付けた全被写体の顔領域を非特定化する．

6. コミュニティ外へ再投稿

既に投稿されたメッセージの共有等，投稿メッセージがコミュニティ外に再投稿される場合は，写真のメタ情報からポリシを取得し，そのポリシに基づき非特定化する．

3.5 撮影者と距離による保護

図 2 に，撮影者（コミュニティメンバ，他人）と距離（至近距離，遠距離）による顔領域の保護処理の対応を示す．コミュニティのメンバが M0～M5 の 6 名存在する．また，コミュニティメンバ外の他人として S1，S2 がいる．このうち，M0 と S2 が撮影者となる．

M0 が PPR を利用して，コミュニティメンバを撮影した．その際，M5 はポリシ：非公開を身に付けていたため，顔領域に暈し処理を入れる．また，他人である S1 が写り込んでいるが，タグを身に付けていないため，S1 のプライバシーを尊重し，暈し処理を入れる．また，M0 が 10m 離れた場所で撮影を行った際に，タグの検知はできたが，ポリシ解析ができなかった．この場合は，全ての被写体を非特定化する．他人である S2 が PPR 以外のデバイスで撮影を行った場合，SNS 提供者側の Privacy Wall により，タグを身に付けたユーザのみ非特定化が行われる．

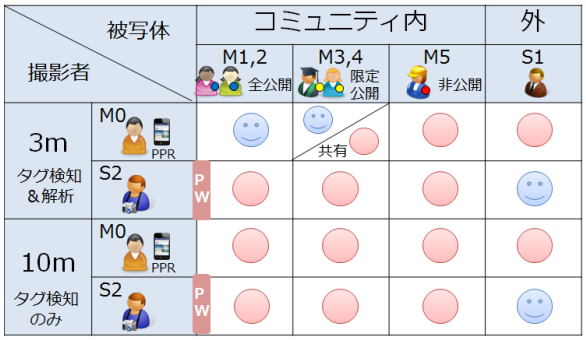


図 2　撮影者と距離による保護処理の対応

4　プライバシータグ

我々が提案するプライバシータグのデザインと写真内の被写体が身に付けたタグの検知・解析アルゴリズムを説明する．また，従来手法で用いられる QR コードベースのタグとの比較，評価を行い，課題であった被写体までの距離による検知・解析精度の改善を示す．

4.1　デザイン

従来手法では，撮影者が容易に判断可能な単純化されたタグ [10]や，QR コードをベースとしたタグ[5]が提案されている．しかし，単純化されたタグは，コミュニティ等に応じたプライバシーの振舞いを表現し難い．また，QR コードのように多くの情報を含む複雑なタグは，被写体までの距離による検知・解析精度に課題がある．そこで，状況に応じたプライバシーの振舞いが可能，かつ，距離によるタグの検知・解析精度が改善するデザインを提案する．

公開ポリシ

SNS 写真投稿時の公開ポリシを検討した．写真のセンシティブデータ漏洩を防ぐために，複雑な設定は必要なく，顔情報やタグ付け，位置情報等

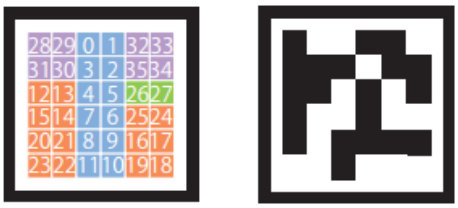
の公開・非公開を表す数ビットで対応可能とされる[16]．我々の提案スキームは，コミュニティを考慮した被写体の顔領域保護を行うため，公開ポリシとして，(1)非公開，(2)コミュニティ内公開，(3)全公開の 3 種を定義した．表 1 に提案タグにおける公開ポリシを示す．

表 1　提案タグにおける公開ポリシ

公開ポリシ	ポリシ説明
非公開	コミュニティ内外問わず，自身の顔領域を非公開
コミュニティ内公開	特定コミュニティ内であれば，自身の顔領域を公開可能
全公開	コミュニティに関わらず，自身の顔領域を公開可能

ビットパターン

定義した公開ポリシや適用対象となるコミュニティ情報を，タグ内にビットとして配置するため，タグ内のビットパターンを検討した．本タグ内のビットパターンとタグサンプルを図 3 に示す．



(a)　ビットパターン　(b)　タグサンプル

図 3　プライバシータグ

本タグに求められる要件として，タグの向きに依存しないビット可読性，バースト誤りを考慮したエラー訂正がある．これらに対応するため，タグ上でバースト誤りが発生しやすい領域を，左右・上部→左右・下部→中央の順であると仮定した．この仮定のもと，タグ検知および，タグの向きを判定するために，位置決めビットパターンをヘッダ部として中央に配置した（図 3-(a), bit: 0-11）．次に，被写体のプライバシーポリシとなるコミュニティ ID と公開ポリシを左右・下部へ配置した（図 3-(a)，bit: 12-25, 26-27）．誤り訂正符号にリード・ソロモン符号を採用し，1 シンボル=4 ビットごとにエラー訂正が可能である．但し，ヘッダ部はエラー訂正の対象外とする．このエラー訂正符号を左右・上部に配置した（図 3-(a), bit: 28-34）．

4.2　検知と解析

写真から被写体が身に付けたタグの検知・解析フローを図 4 に示す．検知・解析フローは，顔検知とタグ検知・解析を並列に実行する．顔検知は，顔検出アルゴリズム: Viola-Jones 法をベースとした手法[17]を適用した．次に，タグ検知・解析は，最初にタグのフレーム境界を検出する．次に，タグの傾き等への対応として画像補正を行い，タグ内のビットパターンを読み取る．最後に，位置決めパターンであるヘッダ部とのマッチングにより，プライバシータグであるかの確認を行う．なお，読取り不可ビットがある場合は，エラー訂正符号を用い，ビットを補完する．

タグ検知・解析後，タグの持ち主となる被写体を判別する．被写体は当該タグを上半身に身に付けている，かつ，検知した顔の幅(W)，高さ(H)を用い，顔直下の 3W×4H の領域にタグが存在すると仮定して，マッチング処理を行う．最後に，取得したポリシに従い，暈し処理を行う．

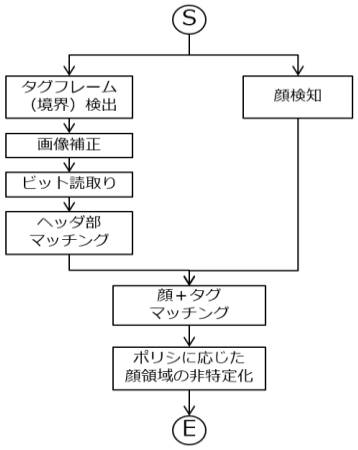


図 4　プライバシータグの検知・解析フロー

4.3　評価

従来手法で用いられる QR コードのタグと我々のタグの比較評価として，各タグにおいて，タグサイズ:2 cm～15cm かつ, 被写体までの距離:1.5m～12m の検知・解析精度を評価した．なお，QR コードはバージョン 1，評価実験は屋外で約 2090 万画素のデジタルカメラを利用して撮影した．図 5 に提案タグと QR コードベースタグの評価実験

の例，図 6 に実験結果を示す．評価の結果，タグサイズ 15cm 以外の全サイズにおいて，検知・解析可能な距離が向上した．特に，提案タグの 2～5cm において，QR コードは距離：1.5m～3m までが読取り上限であったが，提案タグは，4.5m まで読取り可能であった．図 5-(b)は，サイズ：3cm，距離：4.5m において，QR コードは各ビットが暈けており，読み取ることができなかったが，提案タグはタグの検知とビット解析が可能であった．この結果を受け，本提案のタグサイズを実用的なサイズ，距離と考えられる約 3cm 四方とした．

(a) タグ:3cm，距離:1.5m（両タグとも解析可能）

(b) タグ:3cm，距離:4.5m（QR タグは解析不可）

図 5　提案タグと QR コードの比較評価の例

提案タグ　○：タグ検知＋解析，△：タグ検知のみ，X：タグ検知不可

サイズ/距離	1.5m	3m	4.5m	6m	7.5m	9m	10.5m	12m
2cm	○	○	△	X	X	X	X	X
3cm	○	○	○	X	X	X	X	X
5cm	○	○	○	△	X	X	X	X
7.5cm	○	○	○	○	△	X	X	X
10cm	○	○	○	○	△	X	X	X
15cm	○	○	○	○	△	X	X	X

QRコード　○：解析，X：タグ解析不可

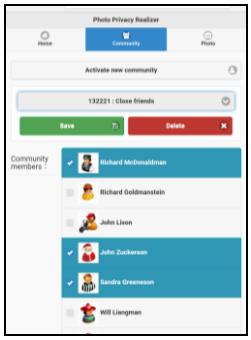
サイズ/距離	1.5m	3m	4.5m	6m	7.5m	9m	10.5m	12m
2cm	X	X	X	X	X	X	X	X
3cm	○	X	X	X	X	X	X	X
5cm	○	○	X	X	X	X	X	X
7.5cm	○	○	○	X	X	X	X	X
10cm	○	○	○	○	X	X	X	X
15cm	○	○	○	○	○	X	X	X

図 6　提案タグと QR コードの評価結果

5　Photo Privacy Realizer

5.1　概要

プライバシータグを身に付けた人物の顔領域を保護するために，4 章で提案したタグをベースに，Facebook を対象としたプロトタイプの PPR を開発した．PPR は，(1) コミュニティ管理，(2) 写真撮影および SNS 投稿の 2 機能から構成される．PPR のユーザインターフェースを図 7 に示す．



(a) コミュニティ管理

(b) 顔領域の保護

図 7　PPR のユーザインターフェース

5.2　コミュニティ管理

コミュニティ管理機能を図 7-(a)に示す．本機能では，コミュニティのアクティベート，コミュニティに属するユーザの決定を行う．最初に Facebook へログインが必要となる．ログイン後，自身の Facebook 上の友人が一覧で表示される．次に，コミュニティのアクティベートを行うために，“Activate”ボタンを押下し，購入したタグパックに付帯するコミュニティ ID を登録する．そして，登録したコミュニティ ID に対して，属するユーザを画面タップで選択/解除を行い，最後に，コミュニティ情報を保存する．また，コミュニティのプルダウンリストより，登録済みのコミュニティを切り替えることで，コミュニティに属する友人のメンテナンスが可能となる．

5.3　写真撮影/SNS 投稿

本機能では新たに写真撮影，または既に撮影済み写真に対して，顔検知および，タグ検知・解析

を行い，取得したポリシと PPR で指定されたコミュニティに応じて顔領域に暈し処理を行う．最初に投稿メッセージの入力，写真撮影を行う．次に，“Anonymize”ボタンを押下し，撮影された写真に含まれるタグの解析を行い，その結果に応じた非特定化を行う．また，タグのコミュニティが合致しない場合も，非特定化を行う．ユーザのポリシに基づいた顔領域の暈し処理を図 7-(b)に示す．最後に“Post”ボタンを押下し，SNS へメッセージと保護処理後の写真を投稿し，コミュニティメンバのみに限定公開する．

6 おわりに

写真に写る/写り込む人物のプライバシーを保護するために，当該人物が属するコミュニティ内外におけるプライバシーの振舞いをポリシとして埋め込んだタグを用いて，コミュニティ内外で当該人物の顔領域を適応的に保護する手法を提案した．また，本手法で用いるプライバシータグの評価として，従来手法で用いられる QR コードベースのタグと我々のタグをタグサイズ，被写体までの距離の観点で比較，評価を行い，これまでの課題であった被写体までの距離が理由による検知・解析精度の改善を示した．さらに，本タグをベースに Facebook を対象としたプロトタイプアプリケーション: Photo Privacy Realizer を開発した．

謝辞

本研究の写真における顔検知およびタグ解析に多くのご支援頂いた国立情報学研究所越前功研究室の大金建夫氏に感謝申し上げる．

参考文献

[1] The Twitter Typo That Exposed Anthony Weiner, http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html

[2] Twitter user says vacation tweets led to burglary, http://news.cnet.com/8301-1009_3-10260183-83.html

[3] 2014 年度 情報セキュリティの倫理に対する意識調査, https://www.ipa.go.jp/files/000044094.pdf

[4] ゴールデンウィーク（GW）の行楽写真を投稿する際はご注意を, http://www.ipa.go.jp/security/txt/2015/05outline.html

[5] C Bo, G Shen, J Liu, XY Li, YG Zhang and F Zhao: Privacy. tag: Privacy concern expressed and respected, *Proc. SenSys*'14, pp. 163-176 (2014)

[6] M Mondal, Y Liu, B Viswanath, KP Gummadi and A Mislove: Understanding and Specifying Social Access Control Lists, *Proc. SOUPS*'14 (2014)

[7] M Sleeper, R Balebako, S Das, AL McConahy, J Wiese and LF Cranor: The post that wasn't: exploring self-censorship on facebook, *Proc. CSCW*'13, pp.793-802 (2013)

[8] A Besmer and HR Lipford: Privacy Perceptions of Photo Sharing in Facebook, *Proc. SOUPS*'08 (2008)

[9] P Kumar and S Schoenebeck: The Modern Day Baby Book: Enacting Good Mothering and Stewarding Privacy on Facebook, Proc. CSCW'15 (2015)

[10] F Pallas, MR Ulbricht, LJ Parasi and U Hoppner: Offlinetags: A novel privacy approach to online photo sharing, *Proc. CHI*'14, pp. 2179-2184, (2014)

[11] 町田史門, 梶山朋子, 嶋田茂, 越前功: SNS におけるセンシティブデータの漏洩検知に基づく公開範囲の設定方式, 情報処理学会論文誌 55(9) (2014)

[12] S Egelman, A Oates and S Krishnamurthi: Oops, I did it again: Mitigating repeated access control errors on Facebook, *Proc. CHI*'11, pp. 2295-2304 (2011)

[13] B Henne, C Szongott and M Smith: SnapMe if You Can: Privacy Threats of Other Peoples' Geo-Tagged Media and What We Can Do About it, *Proc. WiSec*'13, pp.95-106 (2013)

[14] P Pappachan, R Yus, PK Das, T Finin, E Mena and A Joshi: A Semantic Context-Aware Privacy Model for Facebook, *Proc. PrivOn*'14 (2014)

[15] Y Li, K Xu, Q Yan, Y Li and RH Deng: Understanding OSN-Based Facial Disclosure Against Face Authentication Systems, *Proc. ASIACCS*'14

[16] A Ashok, et.al, V Nguyen, M Gruteser, N Mandayam, W Yuan and K Dana: Do Not Share! Invisible Light Beacons for Signaling Preferences to Privacy-Respecting Cameras, *Proc. VLCS'14* (2014)

[17] P. Viola and M. Jones: Robust Real-Time Face Detection, IJCV, Vol.57, No.2, pp.134-157 (2004)