ウェアラブルカメラによるSNS記事投稿時に発生するプライバシー侵害の特徴分析

大本 茂史† 岸本 拓也† 髙田 美樹† 高田 さとみ† 奈良 育英† 周 子胤† 嶋田 茂†
越前 功‡

† 首都大学東京 産業技術大学院大学 〒140-0011 東京都品川区東大井 1-10-40

‡ 国立情報学研究所コンテンツ科学研究系 〒101-8430 東京都千代田区一ツ橋 2-1-2

E-mail: †{a1207so, a1216tk, a1132mt, a1034st, a1230in, a1224zz, shimada-shigeru}@aiit.ac.jp, ‡ iechizen@nii.ac.jp

あらまし Google Glass などウェアラブルカメラによるプライバシー侵害を危惧する意見が増えつつあり，その利便性が否定されかねない．そこでプライバシー侵害の要因分析を目的とし，Google Glass に関する YouTube 記事から機微な意見の抽出や感情分析により，プライバシー侵害に関する記事を収集した．その中でプライバシー侵害に関する意見が多く寄せられている記事に含まれるビデオのシーンをキャプション分析により抽出し，その特徴をベクトル化して，学習することでプライバシー侵害を予知する学習型のアルゴリズムを開発した．

キーワード ウェアラブルカメラ，プライバシー侵害，SNS，ビデオ投稿，感情分析，特徴分析

Feature Analysis Of Privacy Invasion That Occur When Posting Photos and Videos to SNS by Wearable Camera

Shigefumi OOMOTO† Takuya KISHIMOTO† Miki TAKATA† Satomi TAKADA†
Ikuhide NARA† Ziyin ZHOU† Shigeru SHIMADA† Isao ECHIZEN‡

† Tokyo Metropolitan University AIIT Higashi Ohi 1-10-40 , Shinagawa-ku, Tokyo, 140-0011 Japan

‡ National Institute of Informatics 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, 101-8430 Japan

E-mail: †{a1207so, a1216tk, a1132mt, a1034st, a1230in, a1224zz, shimada-shigeru}@aiit.ac.jp, ‡ iechizen@nii.ac.jp

Abstract Opinion to fear the invasion of privacy by wearable camera like Google Glass is getting increasingly, the convenience might be denied. And we collected articles on privacy infringement from YouTube articles related Google Glass to purpose for factor analysis of privacy invasion, by extracting sensitive opinion and emotion analysis. We have developed the learning algorithm for determining the invasion of privacy by learning the feature vector that is extracting caption analysis from the video scene that has many opinions of privacy invasion.

Keyword Wearable Camera, Privacy Invasion, SNS, Video Posting, Emotion Analysis, Feature Analysis

1. 研究背景と目的

1.1 研究背景

Twitter や Facebook に代表される SNS への投稿は，テキストのみの投稿に対して，写真やビデオによる投稿の割合が増加しており，Facebook には 1 日あたり約 3 億 5000 万件の写真がアップロードされている[1]. このような状況は，携帯電話からスマートフォンへの進化に伴い，モバイル（携帯可能）デバイスに搭載されたカメラで撮影した写真やビデオを簡単に SNS へ投稿できる環境が整ったことに因るが，最近はさらに利便性を高めたウェアラブル（着用可能）なデバイスへと進化している．Google Glass に代表されるようなウェアラブルデバイスに装備されたカメラ（以降、ウェアラブルカメラと略称する）は，着用したまま常時撮影が可能で，撮影されていること自体が被撮影者や他のユーザーから気付かれにくい．撮影者自身もプライバシー侵害の可能性を意識せずに常時撮影を行い，SNS へ投稿してしまうリスクが高い．

今後商品化が予定されている Google Glass の機能は現時点ではかなり制限されているものの，プライバシーとセキュリティが同製品の 2 つの懸念点として取り上げられており，米国のバーやカジノでは製品として投入される前にも関わらず，使用が禁止される事態が起きている[2]．また，カナダ，オーストラリアなど 6

カ国のプライバシー関連当局が，データ保護の観点から Google に対して個人のプライバシー権尊重のための対策について質問の書簡を送付するなど国際的にもプライバシーの問題が指摘されている．

ウェアラブルカメラの利用は，プライバシー侵害リスクを助長しやすく,社会問題となることが危惧され，着用による携帯性の向上やハンズフリーによる操作性の向上といった製品自体の利便面[3]が否定されかねない．

1.2 目的

本研究は，Google Glass などウェアラブルカメラからの SNS 投稿時に発生するプライバシー侵害を予知する機能を開発し，それを用いたプライバシー保護サービスを実用化することを目的とする．本稿では，ウェアラブルカメラに関する投稿記事から，プライバシー関心度の高い SNS コンテンツを抽出し，SNS コンテンツの分析からプライバシー侵害のパターンを学習し，プライバシー侵害を自動的に予知する方式を提案する．この方式により，ウェアラブルカメラを利用して撮影した写真やビデオを SNS へアップロードする前にプライバシー侵害を予知し、投稿者へ警告として通知することで，侵害を事前に保護する Opt-in のサービスシステムの実用化を提案する．

以降，2 章で SNS における Opt-in サービスについて述べ，3 章で分析対象とした SNS の記事の選定方法を説明する．選定した記事から抽出したプライバシー侵害の問題が発生している場面（以下、プライシー侵害シーンとする）の特徴抽出の方法について 4 章で説明し，5 章でその特徴を利用したプライバシー侵害の予知方式の提案とその評価を行う．

2. SNS における Opt-in サービス

2.1 Opt-in サービスの必要性

SNS への画像投稿時に発生するプライバシー侵害に関する調査として，町田らによる，「SNS に投稿される写真のプライバシー調査」がある[4]．同調査によると，SNS 利用ユーザーは，自分自身の痴態となる顔画像よりも，行動時間や位置情報といった時空間情報を意識しており，画像内に他人の顔が含まれている画像を投稿する場合は，投稿前の了解の有無をプライバシー侵害の重要な指標としている．了解の有無が重要であり，投稿前の対応（Opt-in）が求められている．

SNS 利用ユーザーが意図せずプライバシーを侵害してしまう要因として,「不用意な公開」,「設定の不備」,「知識不足」,「アプリケーションによる公開」,「“友達”による情報の公開」,「他の情報との関連付け」,「SNS のポリシー変更」などが挙げられる[5]．これらの要因を防ぐには，投稿前に関係者の事前合意（Opt-in）を得ることが望ましいが，SNS サービスを提供する各社は，対応方針を示すプライバシーポリシーや投稿記事の公開範囲の設定の推奨等を記述提示する事後の対応策（Opt-out）を採っている[6]．そのため，対応は SNS 利用ユーザーの判断に委ねられることになり，投稿前に適切な対応が採られない場合はプライバシー侵害が発生する．

プライバシー侵害を未然に防ぐためには事前の対応（Opt-in）が必要である．

2.2 関連研究

SNS への画像投稿時に発生するプライバシー侵害から保護を行う Opt-in 方式に関する研究として，Anna Squicciarini らによるプライバシー保護ポリシー予測(A3P)システムの提案がある[7]．同システムは，新たに SNS へ投稿される記事に対して，その画像と画像に関連付けられたメタデータから動的にプライバシー保護ポリシーを予測するものである．システムのユーザーは，システムが予測して提示したプライバシー保護ポリシーに対して,自らが適切と判断する設定を行い，システムはそれを学習する．ユーザーによる設定の学習方式であるため，ユーザーが適切な設定を行わない場合や，学習の初期段階においては予測精度が必ずしも保証されず，予測したプライバシー保護ポリシーをユーザーが必ずしも実施しない可能性もある．

学習の初期段階からプライバシー保護ポリシーの予測精度を向上させる方式として，小山らのプライバシー侵害予知サービスの提案がある[8]．投稿記事に被害者の情報が含まれているかを判定し，プライバシー侵害コミュニティに該当した場合には，投稿者に対して投稿が問題となることを提示する Opt-in のサービスである．しかし，同サービスは写真（静止画）を対象にしており，ビデオ特有の問題が検討されていない．

ウェアラブルデバイスとプライバシーに関連する研究として，越前による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が挙げられる[9]．意図しない写り込みを被撮影者側から防止する方式の提案で，プライバシーバイザーと呼ばれるウェアラブルデバイスを顔面に装着し，同デバイスよりカメラの撮像デバイスのみに反応するノイズ（近赤外線）を顔面に照射することで顔検出を失敗させることができる．しかし，これは被撮影者を対象としたハードウェアからのアプローチであり，撮影者側によるプライバシー侵害行為を防止するものではない．

以上，前例の中で，本稿では，小山らの提案について，写真以外にビデオも対象としたプライバシー侵害の予知方式を考える．

3. SNS 記事の分析

3.1 分析対象とする SNS 記事

分析の対象とする SNS 記事は前研究[10]から継続してアーカイブしている Google Glass に関する YouTube 記事である．

YouTube 記事を自動収集するため，Google が提供している『YouTube Data API』を利用する[11]．YouTube にて検索キーワード『google+glass』でヒットするビデオは約 9,900,000 件であるが，同 API は，1 度で取得できるデータ件数が上位 1000 件までと制限があるため，一定間隔のポーリング収集を行い，クローリングを行った．分析に利用する記事は，過去 7 ヶ月間（2013/06 - 2013/12）に蓄積した YouTube 記事アーカイブで，その記事から分析対象としたのは，Google Glass で撮影されたビデオや，製品レビュー・ニュース・製品デモ等の Google Glass に関する話題の英語の記事である．日本語の記事はほとんど収集できないため，分析対象外とした．

3.2 SNS 記事の構成

YouTube 記事は，次の 3 つのメディアで構成される（図 1）．

1. ユーザー間での共有対象となるビデオ
2. ビデオの音声を約 4 秒ごとにテキスト化したキャプション
3. 投稿ユーザーや閲覧者がビデオに対する所感を入力するコメント

図 1 YouTube 記事の構成

ビデオは静止画像列の集合体であり，キャプションはその静止画像列に対応する音声部分と紐付く．コメントはビデオに対する意見で，ビデオ全体と紐付く．各メディアの関係を図 2 に示す．

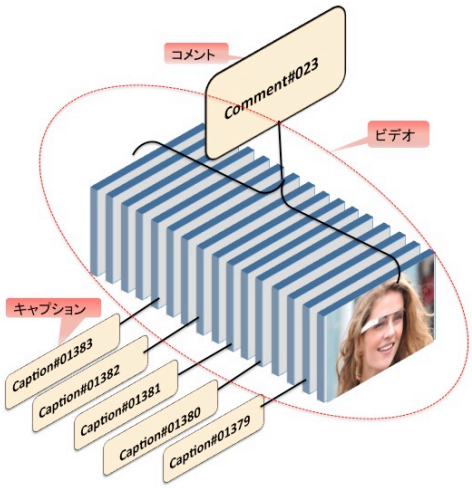


図 2 各メディアの関係

3.3 プライバシー関連ビデオの選定

プライバシーの問題に触れている記事の選定は，前研究と同様にコメントを利用する手法を用いる．選定にはプライバシー侵害に抵触するような表現を持つキーワード群である PS(Privacy Sensitive)ワード[12]と，6 つの感情因子に分類された 65 項目の単語である POMS(Profile of Mood States)を利用した感情分析[13]の組み合わせを適用する．この手法により選定したビデオをプライバシー関連ビデオとする．

4. プライバシー侵害シーンの特徴分析

4.1 特徴抽出の方法

プライバシー侵害を予知するには，プライバシー侵害が発生する状況や場面（シーン）を事前に捉える必要がある．そのため，コメントの感情分析により選定したプライバシー関連ビデオ 412 本について，プライバシー侵害の疑いのあるシーンが含まれているかどうかを視聴して確認し，プライバシー侵害の疑いのあるシーンが含まれている 77 本のビデオからプライバシー侵害シーンの抽出を行う．シーンはビデオの静止画像列とそれに対応するキャプションの集合体と定義する．抽出したシーンは，Google Glass の着用者を撮影した客観的な内容のものと，Google Glass の着用者が撮影した主観的なものに分けられる．プライバシー侵害から保護する対象は，Google Glass などウェアラブルカメラを利用して撮影し投稿する，撮影者による主観的な内容のものであるが，プライバシーの問題を指摘する機微な意見は，Google Glass の機能を紹介したものや，パロディ，ニュース番組など客観的な内容のものに多く寄せられているため，それらもプライバシー侵害シーンの抽出対象とする．Google Glass の着用者が撮影した主観的な内容のビデオのキャプションには，撮影者と被撮影者による感嘆を表すものが多く含

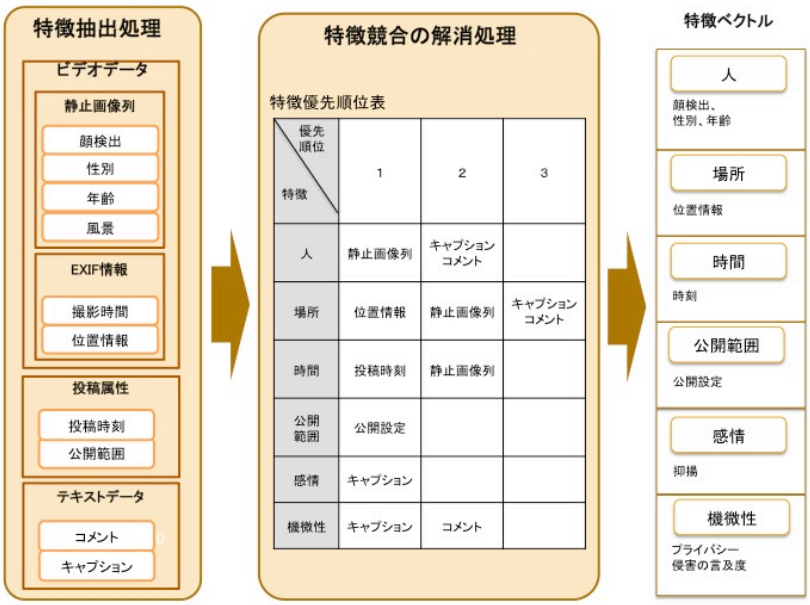


図 3 特徴の抽出フロー

まれ，その感情の抑揚がシーンの特徴となる．また，コメントにはビデオの視聴者がプライバシーの問題を指摘する意見が含まれ，視聴者の立場や環境などを反映した機微な意見が，プライバシー侵害の要因を特徴付ける重要なファクターとなる．

特徴の抽出フローを図 3 に示す．

各メディアから得られるデータを利用して，特徴を人，場所，時間，公開範囲，感情，機微性の 6 つのカテゴリーに分類する．各メディアのデータは，次のように解析して定量化を行い，プライバシー侵害シーンを表す特徴ベクトルとする．

1) ビデオ

ビデオの静止画像を 1 秒単位に保存した静止画像列を，画像解析ソフトウェアパッケージである OKAO Vision[14]を利用して解析し，顔領域の認識のほかに性別，年齢，シーン識別の検出結果を人に関する特徴とする．今回は検出結果から人数を算出し，特徴ベクトルとする．シーン識別で昼夜の識別ができる場合は，時間帯[15]の分類（表 1）を時間の特徴とする．静止画像上の文字認識により場所を示す単語から場所が特定できる場合は，場所の特徴とすることができる．場所の特定には，場所を表す単語を階層的に分類できるようコード化した辞書を作成し，該当の場所に一致するコードを場所の特徴ベクトルとする．今回は，収集したビデオに寄せられているコメントの中にプライバシーの問題が発生する場所として指摘されている，場所に関する単語と位置情報に任意にコードを設定して作成した．例えば，室内のトイレは”11”，店舗であるショッピングセンターは”64”というコードを設定した．

表 1 時刻を時間帯で分類

時刻	時間帯分類	分類値
3:00～9:00	朝，明け方	0
9:00～18:00	昼，夕方	1
18:00～3:00	夜，未明	2

2) キャプション

キャプションは,対応する静止画像列と組み合わせることでシーンの特徴とする．キャプションの投稿者や撮影者が撮影時に発する感情である当事者感情に着目した前研究[16]より，当事者感情が興奮状態の時にプライバシー侵害が発生しやすい傾向があるため，キャプションに英語の標準的な感情表現をスコア化した ANEW[17]の単語が含まれる場合は，含まれる単語のスコアの平均値を感情に関する特徴ベクトルとする．

キャプションから人，場所，時間に関する単語が抽出できる場合はそれぞれを特徴とすることができる．しかし，特定するためには音声認識の精度が求められるため，今回は対象外とした．

3) コメント

ビデオに対して寄せられる意見であるコメントには，ビデオのシーンがプライバシーに触れているかどうかについて言及した機微な意見が含まれている可能性がある．プライバシーの問題に関す

る言及ついての具体的な表現を捉えるために，前述の PS ワードによる単語抽出を行い，PS ワード数を機微性に関する特徴ベクトルとする．

SNS への投稿時は，各 SNS サービスで定義された公開範囲を設定できるため，特徴ベクトルとして考慮する．公開範囲は，各 SNS サービスで設定範囲が異なるが[18]，非公開とすべき情報の重要度による公開範囲として，町田ら[19]による SNS エゴネットワークにおける開示レベルを今回は適用する．収集した YouTube ビデオには公開範囲が設定されていないため，開示レベルへの置き換え方法は検討せず，すべて同一とする．

4.2 特徴の競合解消

各メディアから同じ特徴のデータが抽出できるため，特徴とするデータの競合が発生する．そのため，特徴競合の解消処理を行う．

例えば，静止画像から顔が検出できる場合やキャプションやコメント，投稿する際に入力したテキストの内容から人の存在が確認できる場合は，人に関する特徴データの競合が発生する．この場合は，静止画像から人の映り込みを特定できる確率が高いため，静止画像列のデータを特徴として優先的に採用するなど，データの優先順位付けを行うことで特徴の競合解消を行う．場所の特徴では，位置情報や静止画像，キャプション，コメントから場所が特定できる場合に特徴の競合が発生するため，位置情報を優先するなど各特徴カテゴリーでのデータの競合解消を行い，採用したデータを特徴ベクトルとする．

5. プライバシー侵害の予知方式

5.1 予知方式の概要

プライバシー侵害シーンの特徴ベクトルデータを機械学習処理し，プライバシー侵害の判定を行う．

図 4 に侵害判定の処理フローを示す．

学習フローでは，YouTube データアーカイブから選定したプライバシー関連ビデオのプライバシー侵害シーンを抽出し，その特徴ベクトルデータを利用して機械学習を行い，プライバー侵害シーンのパターン化を行う．

予知フローでは，ウェアラブルカメラを利用して撮影し SNS へ投稿された写真やビデオに含まれるシーンの抽出を行い，その特徴ベクトルデータに対して，学習フローで得たパターンとの比較でプライバシー侵害の予知を行う．プライバシー侵害シーンに適合した場合は，投稿者へ警告通知を行う．

5.2 評価

YouTube データアーカイブから選定したプライバシー関連ビデオの静止画像 4,312 枚を特徴ベクトル化したデータセットを用い，プライバシー侵害の判定評価を行った．静止画像は事前評価を行い，プライバシー侵害のデータ 2,992 件，プライバシー侵害ではないデータ 1,320 件の正解情報を付与した．また，特徴ベクトルのデータ欠損による学習結果の拡散を防ぐため，欠損部分には各特徴カテゴリーのデータセット全体での平均値を設定した．

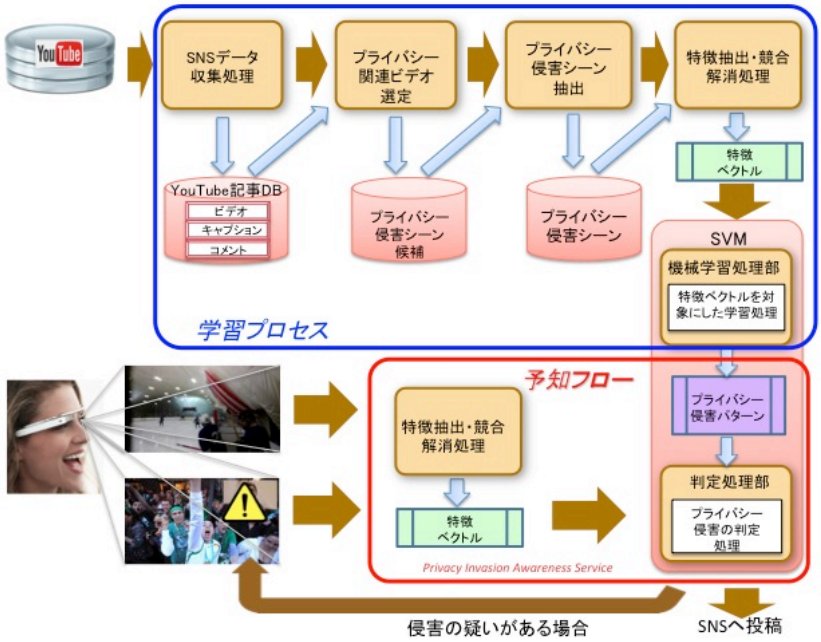


図 4 侵害判定の処理フロー

特徴ベクトルの事例を以下に示す．

＜プライバシー侵害の事例＞

事例 1

ショッピングセンターで顔あり

事例 2

トイレ
顔なし

事例 3

電車内
顔なし

事例 4

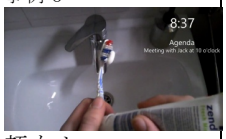
複数の顔あり

事例 5

繁華街での逮捕現場

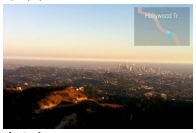
＜プライバシー侵害ではない事例＞

事例 6



顔なし

事例 7



顔なし

事例 8

顔なし

事例 9

顔あり
公開範囲限定

事例 10

顔あり
公開範囲限定

特徴ベクトル

特徴 / データ	人	場所	時間	公開範囲	感情	機微性
事例 1	1	64:shopping center	1:昼	5:他人	5.41	23
事例 2	0	11:toilet	1:昼	5:他人	0	30
事例 3	0	75:subway	2:夜	5:他人	0	9
事例 4	9	74:square	1:昼	5:他人	5.24	6
事例 5	4	72:downtown	2:夜	5:他人	0	67
事例 6	0	12:home	0:朝	5:他人	0	0
事例 7	0	74:field	2:夜	5:他人	0	0
事例 8	0	75:subway	2:夜	5:他人	0	0
事例 9	1	53:skating rink	1:昼	4:知人	0	1
事例 10	1	73:street	1:昼	2:友人	0	6

公共の場で撮影された静止画像列から顔が識別できる場合はプライバシー侵害の可能性があり，感情や機微性にも数値で特徴が表れている（事例 1，4，5）．顔が識別されていなくても，トイレ（事例 2）や電車内（事例 3）といったセンシティブな場所で撮影された静止画像列はプライバシー侵害の可能性がある．

一方，顔が識別できない静止画像列（事例 6～8）や，顔が識別できても，公開範囲が限定されていればプライバシー侵害にはあたらない（事例 9，10）．

特徴ベクトルデータの機械学習には，SVM，NaiveBayes，NeuralNetwork の 3 つ分類器を用い，判定率の比較を行った．評価は，同数の学習用，テスト用のデータを無作為に抽出して行った．分類器別の判定結果を図 5 に示す．

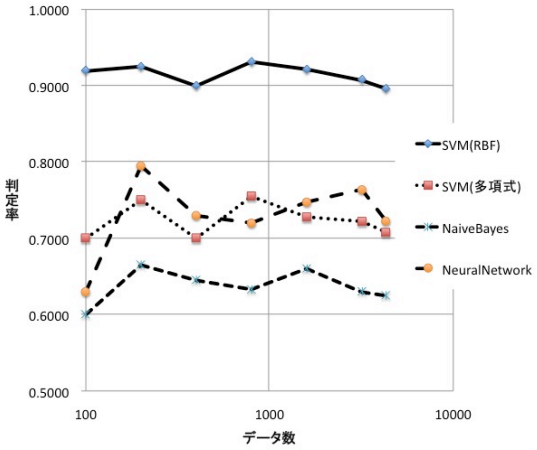


図 5 分類器別判定結果

判定率の高い SVM で，10 交差検定を行ったところ，92.14%の判定率が得られた．

6. まとめ

SNS 上の意見をもとに，Google Glass に関する YouTube 記事からプライバシー侵害シーンを抽出し，その特徴を学習することでプライバシー侵害を予知する方式を開発し，評価を行った．今後は，プライバシー侵害予知サービスを想定した評価を行うことが課題である．また，今回は特徴競合の解消処理として特徴採用の優先順位をあらかじめ設定したが，これを自動的に行うことも今後の課題である．

謝辞

画像解析ソフトウェアパッケージ OKAO Vision を提供いただいたオムロン株式会社に感謝申し上げます．

参　考　文　献

[1] BUSINESS INSIDER, "Facebook Users Are Uploading 350 Million New Photos Each Day", http://www.businessinsider.com/facebook-350-million-photos-each-day-2013-9 (2013/12/29)

[2] CNET, "Privacy officials from 6 countries request details on Google Glass", http://news.cnet.com/8301-1023_3-57589973-93/privacy(2013/12/30)

[3] MM 総研,"日米におけるウェアラブル端末の市場展望――日米消費者調査の結果から", http://www.m2ri.jp/newsreleases/main.php?id=010120131225500 (2014/1/5)

[4] 町田史門, 小山貴之, 宋洋, 高田さとみ, 嶋田茂, 越前功, "SNS 写真投稿に起因するプライバシー侵害の類型化とその保護策", 電子情報通信学会 EMM 研究会技術報告, 2012

[5] JNSA, "SNS の安全な歩き方～セキュリティとプライバシーの課題と対策～", http://www.jnsa.org/result/2012/sns.html(2014/1/1)

[6] Facebook ヘルプセンター, https://www.facebook.com/help/(2014/1/1)

[7] Anna Squicciarini, Smitha Sundareswaran, Dan Lin, "A3P:Adaptive Policy Prediction for Shared Images over Popular Content Sharing Sites", ACM New York, 2011

[8] 小山貴之, 宋洋, 町田史門, 嶋田茂, 越前功, ″SNS 画像投稿時のプライバシー侵害予知サービスの提案", DEIM Forum,2013

[9] 越前功, "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-", NII プレスリリース 2012/12/12

[10] 奈良育英, 高田さとみ, 髙田美樹, 大本茂史, 岸本拓也, 周子胤, 嶋田茂, "SNS 画像投稿時に発生するプライバシー侵害の要因分析", 電子情報通信学会 HCS 研究会技術報告, 2013

[11] YouTube Data API, https://developers.google.com/youtube/(2014/2/22)

[12] 高田さとみ, 小山貴之, 町田史門, 宋洋, 嶋田茂, "SNS 画像投稿時に発生するプライバシー侵害の要因分析", 電子情報通信学会 EMM 研究会技術報告,2012

[13] J.Bollen, A.Pepe, and H. Mao, "Modeling public mood and emotion: Twitter sentiment and socio-economic phenomena, " CoRR, vol. abs/0911.1583, 2009.

[14] OMRON, OKAO Vision, http://www.omron.co.jp/ecb/products/mobile/ (2014/1/1)

[15] 気象庁, "時間細分図", http://www.jma.go.jp/jma/kishou/know/yougo_hp/saibun.html(2014/1/13)

[16] 高田さとみ, 周子胤, 髙田美樹, 大本茂史, 岸本拓也, 奈良育英, 嶋田茂, "キャプションテキスト感情の分析によるプライバシー侵害シーン抽出",情報処理学会自然言語処理研究会報告, 2014

[17] M. M. Bradley and P. J. Lang. Affective Norms for English Words (ANEW): Stimuli, instruction manual, and affective ratings. (Tech. Report C-1), 1999

[18] 日経プラスワン, "思わぬ社会制裁も SNS で異なる公開範囲に注意", http://www.nikkei.com/article/DGXDZO61259000Y3A011C1W05001/(2014/1/5)

[19] S. Machida, S. Shimada, and I. Echizen, "Settings of Access Control by Detecting Privacy Leaks in SNS", In Proceedings of The 9th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS 2013), pp.660-666, Kyoto, Japan, Dec. 2013