Vol.2014-SPT-8 No.14
2014/3/27

SNS ユーザ協力型の不正アカウント報告システム

津田 侑[1,a)]　遠峰 隆史[1]　井上 大介[1]

概要：個人情報やプライバシーに係る情報がユーザ自身により書き込まれる SNS では，攻撃者にそれらの情報を窃取される恐れがある．実際に，情報窃取用の不正なアカウントを作成しユーザと友達関係を構築することで，公開されたプロフィール情報以外に友達のみに限定公開されたものまでも窃取する方法が存在する．本研究では SNS の特性を活かし，SNS 上のユーザらが協力して不正アカウントを報告し合うシステムを提案する．本システムでは，友達申請を受けた時点でそのアカウントが不正なものかどうかの判定基準をユーザに示し，不正アカウントの報告を促す．報告された不正アカウントは他のユーザにも共有され，ユーザ同士で注意喚起することを可能とする．本研究の最後では，実際に 7 人の Facebook ユーザが本システムを用いて収集した不正アカウントを分析し，それらのプロフィール情報の特徴やそれらが行う友達申請行為に着目した考察を述べる．

A System for Sharing and Alerting to Fake Profiles among Online Social Networks Users

Yu Tsuda[1,a)]　Takashi Tomine[1]　Daisuke Inoue[1]

Abstract: On online social networks (OSNs) which store huge personal data and privacy information by OSNs users, those information can be stolen by attackers. Actually, attackers create their accounts called “fake profiles” for collecting information. Then, the accounts connect to targeted users on OSNs in order that they aim at limited-access information only for targeted users’ friends. In this paper, we propose a system for sharing and alerting to fake profiles among OSNs users, in which users can collaborate with their friends. This system shows a sence of fake profiles to users and encourages users to report the profiles to their friends as attackers. In addition, 7 existing Facebook users collect fake profiles using this system. The authors analyze these fake profiles. At last, we discuss features of their profile information and their friend-request actions.

1. はじめに

インターネット上で他者との友達関係を構築したり，特定の事柄に興味を持つ者たちでのコミュニティを形成することなどを目的としたソーシャル・ネットワーキング・サービス（SNS: Social Networking Service）の利用が人々の生活に浸透してきた．SNS の形体は多様で，たとえば 140 文字以下の短文を投稿する Twitter[1] や実名を含む詳細なプロフィールを作成することで実際の交友関係をオンラインでも形成する Facebook[2]，職歴や技能を登録するビジネス上での利用に特化した LinkedIn[3] などがある．

SNS を利用する際に，ユーザには実名，住所，勤務先などの個人情報の入力が求められることがある．また，利用を進めるとそのユーザの行動や発言，現在地の情報といったプライバシーに関する情報を投稿することもある．．これには，実在する人物と SNS ユーザを強く紐付け，日常生活の延長でインターネット上でも交流を継続しやすくする利点がある．しかし，このことが様々なユーザのプライバシー情報が SNS に集約される一因となり，多くの既存研究でプライバシー情報が攻撃者に窃取されうることが懸念されている [4], [5], [6].

ユーザのプライバシー情報を狙う攻撃者の中には，SNS

1 独立行政法人 情報通信研究機構 サイバー攻撃対策総合研究センター
Cybersecurity Research Center, National Institute of Information and Communications Technology, Koganei, Tokyo, 184–8795, JAPAN
a) tsuda@nict.go.jp

© 2014 Information Processing Society of Japan

上の友達限定の情報を狙うために友達関係を結ぼうとするものも存在する．攻撃用のユーザを作成し，不特定多数に手当たり次第に，ときには特定の標的を狙い定めて友達申請を送信する．その申請をユーザが承認すれば，友達のみに限定公開するように設定していた情報も閲覧，窃取されてしまう．本研究では，このような攻撃者がスパム行為や情報窃取のために作成したと思われるユーザを総じて**不正アカウント**と呼ぶ．

本研究では，このような不正アカウントからの友達申請をユーザらで自衛できる仕組みとして，SNS の特性を活かしたユーザ協力型の不正アカウント報告システムを構築する．SNS はユーザらが友達関係を構築して利用することが想定される．そのため，ユーザが不正アカウントであると思われるものを友達同士で共有できれば，ユーザ同士で互いに不正アカウントに対して注意を払うことができると考えられる．

本研究で開発するユーザ協力型の不正アカウント報告システムは，代表的な SNS である Facebook を対象とする．先行研究 [7] で調査した不正アカウントの特徴に基づき算出された不正アカウントの判定基準をユーザに提示することで，ユーザらに不正アカウントの報告機会を与える．そこでユーザが不正アカウントとして報告すればその情報がユーザの友達たちの間で共有され，注意喚起できる．

本研究では，実際に 7 人の Facebook ユーザが本システムを利用して不正アカウント収集作業を実施した．不正アカウントは，本システムが提示した不正アカウント判定基準からユーザ自身の判断で選択した．本稿の最後では，これらの収集した不正アカウントが持つプロフィール情報や友達申請の行為自体について特徴を挙げ，考察を述べる．

2. 関連研究

2.1 不正アカウント対策に関する既存研究

SNS 上の不正アカウントを検知する研究は様々なアプローチから行われている．

Conti らは，ユーザらが構築する友達関係グラフの傾向から不正アカウントの検知を試みている [8]．文献 [8] では，まず，Facebook を対象に収集したデータを用いて，Facebook における友達関係グラフを構築する．そして，そのグラフにおけるノードの平均次数や孤立したノードの数に注目することで不正アカウントを検知する．Nazir らは，Facebook 上のゲームアプリケーションを対象として，事例分析を通して不正アカウントの特徴を抽出している [9]．正規のユーザアカウントと不正アカウントの間には友達の数や投稿数といった属性には差が見られないが，アプリケーション内での振る舞いに差が見られる．この特徴を活かして，SVM を用いて正規アカウントと不正アカウントを分類している．

また，不正アカウントからユーザのプライバシー情報を保護する SNS の仕組みも提案されている．

Cutillo らは不正アカウントによる攻撃をプライバシー・完全性・可用性に対する危険性の観点から整理した上で，プライバシー保護を目的とした SNS，Safebook を提案している [10]．Safebook では P2P を用いた SNS を構築することでユーザ情報の分散管理を実現している．Guha らの NOYB[11] では，プロフィール情報の暗号化機能を Web ブラウザのプラグインとして実装することでプライバシー保護を実現している．

これらの研究は SNS 上でのユーザの活動を観測することで不正アカウントを検知したり，不正アカウントからプライバシー情報そのものを保護するための仕組みとして提案されている．一方，本研究では Facebook のような既存の SNS における友達申請のイベントに着目し，友達申請者の公開されたプロフィール情報のみを用いて不正アカウントの判定を試みる．これにより，正規のユーザアカウントが不正アカウントと友達関係を結ばないようにし，攻撃者が不正アカウント経由でユーザの詳細なプライバシー情報を窃取することを防ぐ．

2.2 ユーザ協力型の不正アカウント検知

著者らはこれまでに Facebook 上に現れた不正アカウントを調査し，その特徴を利用した不正アカウントの検知手法を提案してきた [7]．

この手法では Facebook が実名登録を前提としていることを活かし，以下の公開された情報を基に不正アカウントかどうかを判定し，その判断基準を算出する．

- 登録名（漢字・カタカナ・ローマ字表記）
- プロフィール画像
- 共通の友達の数
- 友達申請時刻とアカウントの作成時刻

不正アカウントであるかどうかの判断基準をユーザに提示することで，ユーザに不正アカウントの報告を促す．ユーザによって不正アカウントであると報告されたものは他のユーザにも共有される．さらに，不正アカウントと報告されたものの中でユーザ自身のプロフィールを模倣したものがあれば，それを他のユーザに周知することができる．

本研究では文献 [7] で述べられた手法を Facebook と連携した Web アプリケーションとして実装し，7 人の Facebook ユーザで実際に不正アカウントを収集した．第 3 章では，本研究で開発したシステムの概要と実装について述べ，第 5 章では，本システムを利用して実際に収集した不正アカウントの情報と事例を述べる．そして第??章では，収集した不正アカウントの情報を基に考察を述べる．

3. ユーザ協力型不正アカウント報告システム

3.1 システム概要

文献 [7] で提案した手法を基に不正アカウントの情報を

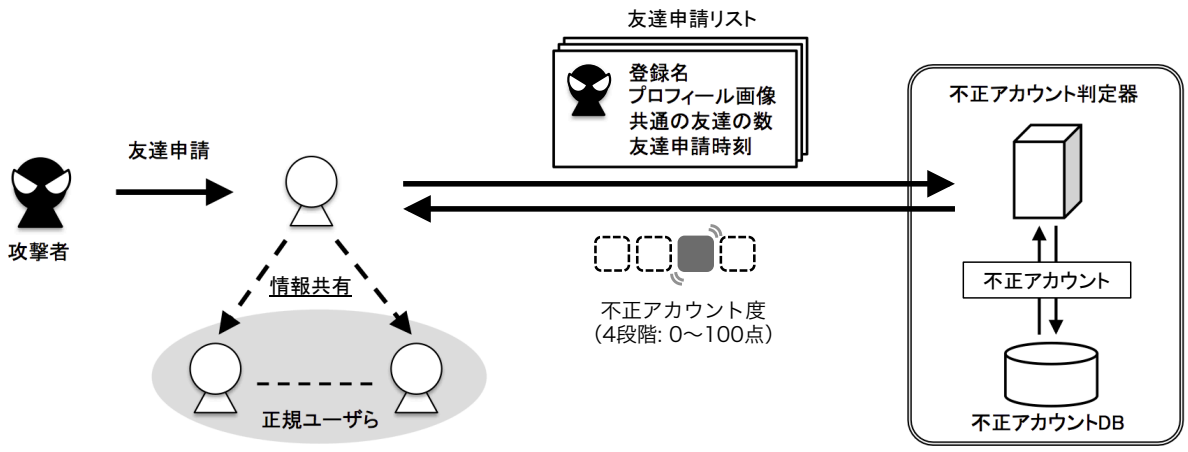


図 1 不正アカウント報告システムの概要

SNS 上の友達と報告し合える仕組みについて述べる．システムの概要を図 1 に示す．

SNS ユーザは，SNS を利用する上で他のユーザから友達申請を受けることになる．このとき，ユーザには友達申請をしてきたユーザの登録名，プロフィール画像，ユーザとの共通の友達の数といった公開された情報が提示される．それ以外に，ユーザが友達申請を受け取った時刻も取得できる場合もある．

これらのユーザから閲覧できる友達申請者のプロフィール情報を不正アカウント判定器に送信する．そうすると，文献 [7] で挙げた不正アカウントの特徴を基に算出された不正アカウント度がユーザに提示される．不正アカウント度は 0 から 100 の間の数値になり，数値によって 4 段階に色分けされる．

ユーザはシステムに提示された不正アカウント度を確認し，そのアカウントが不正なものであると判断できれば，既に友達関係を結んでいるユーザに対してその情報を報告できる．ここで不正アカウントであると報告されたものは，不正アカウント DB に蓄積されていく．不正アカウント DB に蓄積された不正アカウントのプロフィール情報は，他のユーザが同様の友達申請を受けたときに不正アカウント度の算出に利用される．

3.2 実装

本システムは Facebook と連携した Web アプリケーションとして実装する．友達申請リストやユーザのプロフィールは，Facebook Graph API[12] を用いて取得する．

図 2 に本システムのインタフェースを示す．ユーザから得た友達申請リストを基に不正アカウント度を算出し，ユーザに提示する．

ユーザは提示された不正アカウント度を基に，「友達承認/保留」または「不正アカウント共有」を選択できる．「不正アカウント共有」ボタンを押下することで，そのアカウントの情報が自身の友達に共有され，不正アカウントとして DB に格納される．「友達承認/保留」ボタンは Facebook で実装されている機能で，不正アカウントではないとユーザが判断すればこのボタンを押下することで友達として承認できる．本システムでは，これらのどちらのボタンを押下するかはユーザの判断に任せられる．

図 2 不正アカウント報告システムの画面

また，ユーザ自身のプロフィールを模倣した「なりすましアカウント」についても一覧できる．なりすましアカウントは，あるユーザのプロフィール情報を模倣し，そのユーザの友達に対して友達申請を行う．この性質を利用し，友達が報告した不正アカウントの中にユーザ自身のプロフィール情報，特に登録名が類似したものがあれば，それをなりすましアカウントとして提示する．

4. 不正アカウントの収集

4.1 実施概要

2013 年 7 月 1 日から 2013 年 10 月 31 日の 4 ヶ月にかけて，本研究で構築したシステムを用いて不正アカウントの収集を実施した．不正アカウトの収集には 7 人が参加し，

表 1 収集した不正アカウント

収集期間	2013 年 7 月 1 日 〜 2013 年 10 月 31 日
収集者数	7 人
件数	187 件 男性: 132 件 女性: 55 件
友達申請数	のべ 279 回

それぞれが Facebook 上で友達関係を築いている．不正アカウントを収集する際に本システムは 7 人のユーザそれぞれに対して不正アカウントの判定基準を与えるが，その判定基準から不正アカウントとして報告するかどうかはユーザ個人の判断に任せた．

不正アカウント収集の実施および収集した不正アカウントの概要を表 1 にまとめる．7 人が報告した不正アカウントからの友達申請はのべ 279 回で，不正アカウントのユニーク数は 187 件であった．そのうち性別で男性と設定されているものは 132 件，女性と設定されているものは 55 件であった．

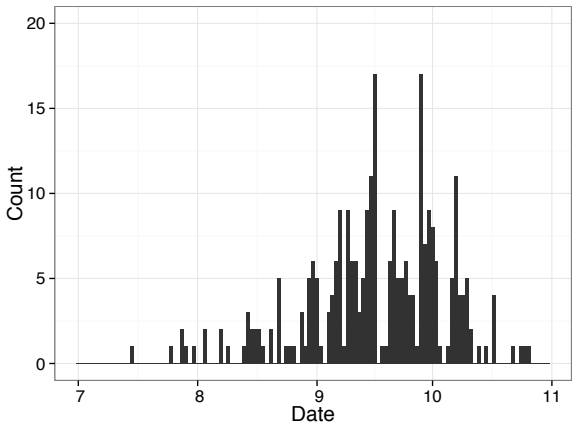
次に，不正アカウントによる友達申請をユーザが受信した日時を日別・時間帯別の集計で図 3 に示す．日別集計（図 3(a)）では，9 月上旬から 10 月上旬にかけて不正アカウントの件数が急激に増加したものの，それ以降は減少傾向にあったことがわかる．時間帯別集計（図 3(b)）では時間帯によっては多少の差はあるものの，時間帯に関係なく概ね一定して友達申請があったことが見られる．これらのことから，不正アカウントによる友達申請には時期によって傾向に差が見られるが，その申請の時間帯についてはあまり偏りが見られないことがわかる．なお，これらの友達申請時刻の差異は今回収集できた不正アカウントに依存するものであると考えられる．

4.2 収集した不正アカウントの例

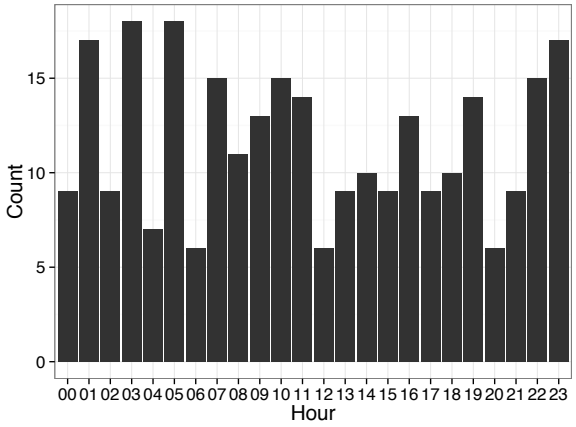
本節では，今回の実際に収集できた不正アカウントの例を紹介する．これらの不正アカウントは既に削除されており，Facebook 上のプロフィール掲載ページにもアクセスできなくなっている．

表 2 は，不正アカウント収集に参加したうちの 1 人のみが報告した不正アカウントのプロフィール情報である．これには，登録名の漢字表記とカタカナ表記で不整合がある．また，登録名は女性の名付けに利用されることが多いものであるにもかかわらず，性別は男性と設定されている．プロフィール画像は Facebook で用いられる性別ごとの初期画像をそのまま利用している．

表 3 は，不正アカウント収集に参加した 7 人のうち 5 人に友達申請を送信した不正アカウントのプロフィール情報である．前述した例とは異なり，登録名の漢字・カタカナ・ローマ字の表記には整合性がある．また，性別が女性と設定され，プロフィール画像にも女性が一人が被写体となった写真が利用されている．そして，プロフィール情報の最終更新時刻から友達申請時刻までに約 200 秒から約 400 秒ほど要している．



(a) 日別の友達申請数



(b) 時間帯別の友達申請数

図 3 友達申請の集計

表 2 不正アカウントの例 (1)

属性	内容
登録名（漢字）	立田 双葉
登録名（カタカナ）	アベ アリス
登録名（ローマ字）	Tatsuta Futaba
性別	男性
プロフィール画像	男性用初期画像
友達申請受信者数	1 人
友達申請時刻 − 最終更新時刻	414 秒

5. 考察

5.1 不正アカウントによる友達申請の特徴

本節では，不正アカウントの友達申請の行為自体に着目し，友達申請の仕方やその時刻に注目した考察を述べる．

5.1.1 友達申請の送信相手

不正アカウントが友達申請を送信相手は大半が 1 人で，

表 3 不正アカウントの例 (2)

属性	内容
登録名（漢字）	宍戸 友紀
登録名（カタカナ）	シシド トモノリ
登録名（ローマ字）	Shishido Tomonori
性別	女性
プロフィール画像	女性一人の写真
友達申請受信者数	5 人
友達申請時刻 − 最終更新時刻	最小: 206 秒
	最大: 414 秒
	平均: 298.8 秒

複数ユーザに対して送信した不正アカウントは 187 件中 59 件であった．複数人に対して友達申請をした不正アカウントは 7 人中 5 人に送信したものが最大で，これが 3 件あった．また，友達申請を受けたユーザの組み合わせには規則性はなく，各々が友達申請を受けた順番もユーザの ID や登録名などに関連性は見られなかった．この傾向は複数ユーザに友達申請を送信している他の不正アカウントにも見られる．

このように，複数ユーザに対して友達申請を送信する不正アカウントも収集したもののうち 31.6%（187 件中 59 件）の割合で存在する．このことから不正アカウントを友達同士で共有し注意喚起し合えることは有効であると考えられる．

一方で，スパム行為のような複数ユーザに対して友達申請を送信するのではなく特定のユーザに狙いを定めて友達申請を送信する場合も考えられる．この場合はユーザの友達からの注意喚起以外にも，友達申請を送信してきたユーザが不正アカウントであるかどうかをユーザ自身で判断できることが求められる．

実際に，今回の不正アカウント収集で得た 1 人のユーザにのみ友達申請を送信したものは全体のうち 68.4%（187 件中 128 件）であることから，文献 [7] の提案で算出した判定基準でもユーザにとっては不正アカウントと判断するある程度の指標となっていると考えられる．しかし，このような不正アカウントの特徴をそのまま利用するだけではユーザに不正アカウントの判断基準を与えることができなくなることが懸念される．そのため，プロフィール情報以外にも公開された情報を用いたり，それを利用して学習するといったことが必要であると考えられ，これは今後の研究課題となる．

5.1.2 友達申請時刻

ユーザに友達申請を送信した時刻とプロフィールの最終更新時刻の差を計算すると，その差が最も小さいアカウントで 25 秒，差が最も大きいもので 767 秒，平均すると 256.6 秒であった．これは不正アカウントがプロフィールを編集・作成してから 5 分前後で友達申請をユーザに送信していることを意味している．

また，複数人が同じ不正アカウントを報告していることや不正アカウントがプロフィールの最終更新時刻から短時間で友達申請を送信していることから伺える．このことから，不特定多数に対してスパムのような目的で友達申請を送信する以外にも，何らかの方法で入手した友達リストやコミュニティ関係を狙って友達申請を送信していると推察される．

5.2 不正アカウントのプロフィール情報の特徴

本節では，収集した不正アカウントのプロフィール情報に注目する．不正アカウントのプロフィール情報には文献 [7] で挙げたような特徴がいくつか存在する．ここでは，今回収集した不正アカウトにおいて見られた特徴的な点について述べ，議論する．

5.2.1 登録名

表 2 で例示したように，登録名の漢字・カタカナ・ローマ字表記が不整合なものが全 187 件中 35 件あった．Facebook は利用規約 [13] で実名および実在の情報が登録されていることが定められており，多くの正規ユーザらはこれらを正しく入力していると考えられる．

しかし，不正アカウントを作成する攻撃者にとっては，登録名の表記は名前の辞書を利用すれば簡単に整合性をとることができる．今回収集した不正アカウントの登録名に整合性がとれているものが全体の 8 割以上を占めることから，その他の特徴と組み合わせて不正アカウント判定基準を算出する必要がある．

5.2.2 プロフィール画像

今回収集した不正アカウントのプロフィール画像の分類を表 4 に示す．プロフィール画像を分類するにあたり，著者が目視でプロフィール画像を確認した．表 4 では前述の登録名の整合性も合わせて分類している．

不正アカウントに利用されているプロフィール画像のうち，女性一人・集合の写真のような Facebook の初期画像ではないものを Web 検索エンジンで類似画像検索したところ，多くが他の Web サイトでも利用されていることがわかった．このことから，不正アカウントを作成する際に Web 上のリソースが流用されることが確認できた．

また，今回収集できた不正アカウントのうち，多くが男性用初期画像と女性一人の写真を設定していた．そして，これらの画像を設定していた不正アカウントにのみ登録名が不整合なものが見られた．

5.3 なりすましアカウントへの対応

ユーザの友達のような親しい他のユーザになりすますしてアカウントを作成する，特に対象となる SNS 上に既に存在するユーザや別の SNS に存在するユーザのプロフィール情報を用いてなりすましアカウントを作成することが攻撃者にとって効果的であることは既存研究でも示されてい

表 4　プロフィール画像と登録名の整合性による分類

	登録名		
	整合	不整合	合計
男性用初期画像	55	26	81
女性用初期画像	3	-	3
女性一人の写真	86	9	95
女性の集合写真	3	-	3
キャラクター画像	2	-	2
風景・物の写真	3	-	3
合計	152	35	187

る [14]．また，別の研究では SNS 上のユーザらは不容易に見ず知らずのユーザからの友達申請を許可してしまう傾向があることが示されている [15]．

今回の不正アカウント収集では参加した 7 人の Facebook ユーザをなりすましたアカウントは発見できなかった．しかし，一方でこのような他人になりすました不正アカウントを発見し他のユーザと情報共有することへの要求はあると考えられる．

なりすましアカウントへの対応としては，安易に友達申請を許可しない，友達申請を許可する前に他の手段を用いて本人確認をするといったより高いソーシャルメディアに対するリテラシーがユーザには求められる．しかしながら，そのような高いリテラシーを備えたユーザばかりでなく不注意で友達申請を承認するユーザも多く存在するため，そのようなユーザに注意を促せる仕組みが必要となる．

この点，本研究のシステムではユーザ同士が協力して不正アカウントを報告し合うことができ，なりすましアカウントが発見されたことを本システムを介してなりすまされたユーザ本人に伝えることができる．

6. おわりに

本研究では，SNS のユーザらが不正アカウントと友達関係を構築しないように注意喚起する仕組みとして，ユーザらが協力して不正アカウントの情報を報告し合うシステムを構築した．友達申請を受けた際にそのアカウントが不正アカウントの可能性があるかどうかをユーザらに提示し，不正アカウントの報告を促す．不正アカウントの判定基準は，プロフィール情報や友達申請時刻といった公開された情報のみで算出する．

本システムを用いて 7 人の Facebok ユーザで不正アカウントの収集をしたところ，のべ 279 件の友達申請を受信した．収集した不正アカウントのユニーク数では 187 件あった．これらの不正アカウントを分析したところ，プロフィール情報として登録されている名前や画像に特徴があった．また，友達申請行為に着目すると，不特定多数に友達申請をスパムのように送信する以外にも友達リストや SNS 上の関係性を用いたと思われるある程度範囲を絞った友達申請も散見された．

今回の研究では Facebook を対象とした不正アカウントを収集したが，今後は LinkedIn や Twitter のような他の SNS のリソースも活用し，利用者規模を拡大して不正アカウントを収集する．さらに，友達同士で不正アカウントを報告し合うことの有効性の評価を行う．この際，ユーザによって誤って不正アカウントと判断されたり，意図的に不正アカウントと認定されるといったことが起こりうる．そのため，このような行動に影響しないような仕組みを導入する必要があると考えている．

参考文献

[1] Twitter. `http://www.twitter.com/`.
[2] Facebook. `http://www.facebook.com/`.
[3] LinkedIn. `http://www.linkedin.com/`.
[4] Ralph Gross, Alessandro Acquisti, and H John Heinz Iii. Information Revelation and Privacy in Online Social Networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pp. 71–80, 2005.
[5] Joshua Fogel and Elham Nehmad. Internet social network communities : Risk taking , trust , and privacy concerns. *Computers in Human Behavior*, Vol. 25, No. 1, pp. 153–160, 2009.
[6] Balachander Krishnamurthy and Craig E Wills. Characterizing Privacy in Online Social Networks. In *Proceedings of the first workshop on Online social networks*, pp. 37–42, 2008.
[7] 津田侑, 遠峰隆史, 井上大介. SNS の特性を活かした不正アカウント検知手法. コンピュータセキュリティシンポジウム 2013（CSS2013）, 2013.
[8] Mauro Conti, Radha Poovendran, and Marco Secchiero. FakeBook : Detecting Fake Profiles in On-line Social Networks. In *Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2012)*, pp. 1071–1078, 2012.
[9] Atif Nazir, Saqib Raza, Chen-nee Chuah, and Burkhard Schipper. Ghostbusting Facebook : Detecting and Characterizing Phantom Profiles in Online Social Gaming Applications. In *Proceedings of the 3rd Workshop on Online Social Networks (WSON 2010)*, 2010.
[10] Leucio Antonio Cutillo, Refik Molva, and Thorsten Strufe. Safebook : A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust. *IEEE Communications Magazine*, No. December, pp. 94–101, 2009.
[11] Saikat Guha, Kevin Tang, and Paul Francis. NOYB : Privacy in Online Social Networks. In *Proceedings of the first workshop on Online social networks*, pp. 49–54, 2008.
[12] Facebook Graph API. `http://developers.facebook.com/docs/reference/api/`（2014 年 2 月 24 日閲覧）.
[13] Facebook 利用規約. `http://www.facebook.com/legal/terms/`（2014 年 2 月 24 日閲覧）.
[14] Leyla Bilge, Thorsten Strufe, Davide Balzarotti, Engin Kirda, and Sophia Antipolis. All Your Contacts Are Belong to Us : Automated Identity Theft Attacks on Social Networks. In *Proceedings of the 18th international conference on World wide web*, pp. 551–560, 2009.
[15] Yazan Boshmaf, Ildar Muslukhov, Konstantin Beznosov, and Matei Ripeanu. The Socialbot Network : When Bots Socialize for Fame and Money. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pp. 93–102, 2011.

© 2014 Information Processing Society of Japan