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～

第 0.7 版

2012 年 11 月 1 日

NPO 日本ネットワークセキュリティ協会

SNS セキュリティワーキンググループ

目次

JNSA SNS セキュリティワーキンググループ (2012/11/1 現在)

ワーキンググループリーダー

高橋 正和	日本マイクロソフト株式会社

メンバー（五十音順）

足立 靖子	日本マイクロソフト株式会社
池上 美千代	東芝ソリューション株式会社
泉原 克人	NHN Japan 株式会社
一之宮 美紀	株式会社インフォセック
稲葉 悠夏	株式会社インフォセック
宇崎 俊介	NHN Japan 株式会社
岡庭 素之	キヤノン IT ソリューションズ株式会社
小川 博久	みずほ情報総研株式会社
奥村 博信	キヤノン IT ソリューションズ株式会社
木村 仁美	セコムトラストシステムズ株式会社
郷間 佳市郎	株式会社日立システムズ
久保 啓司	JPCERT コーディネーションセンター
斉藤 雅浩	富士通株式会社
坂本 慶	サイバーソリューション株式会社
塩田 英二	TIS 株式会社
高橋 伸和	日本ベリサイン株式会社
高橋 誠	NHN Japan 株式会社
田中 淳一	トレンドマイクロ株式会社
田中 洋	株式会社インフォセック
玉井 睦	セコム株式会社
手塚 信之	SCSK 株式会社
中井 尚子	JPCERT コーディネーションセンター
中司 年哉	グローバルセキュリティエキスパート株式会社
則武 智	エヌ・ティ・ティ・コミュニケーションズ株式会社
長谷川 長一	株式会社ラック
服部 真	富士通株式会社
福田 尚弘	パナソニック株式会社
本多 規克	アルプスシステムインテグレーション株式会社
丸山 司郎	株式会社ラック
南 芳明	日本ベリサイン株式会社
三村 智彦	富士通株式会社

守屋 英一　　日本アイ・ビー・エム株式会社
柳澤 智　　富士通株式会社
渡辺 仙吉　　日本アイ・ビー・エム株式会社

1 はじめに

2011 年に入り、SNS (Social Networking Service) という言葉が急激に広まり、注目を集めるようになった。一方で、SNS の概念はとても広く、Wikipedia の「ソーシャル・ネットワーキング・サービスの一覧[1]」では、360 を超える実に多様な SNS が紹介されている(2012/6/18 現在）。加えて、ソーシャル・ネットワークという概念は、インターネットの黎明期から存在し、Netnews やメールもソーシャル・ネットワークと考えることもでき、なぜ、SNS という言葉が急速に広がっているのか理解しにくい面がある。

また、SNS の利用が急速に広がる一方で、SNS のセキュリティやプライバシーにかかわる問題も表面化している。これまで、ネットワークセキュリティは、技術的なセキュリティやセキュリティマネジメントが中心となっていたが、SNS においては、プライバシーにかかわる問題が大きな比重を占めることになり、プライバシーに対する侵害への懸念から、SNS の利用を危険視する考えも根強いものがある。

本稿では、まず SNS の概要とビジネスモデルを解説し、そして、SNS に関わるセキュリティとプライバシーの問題について取り上げる。

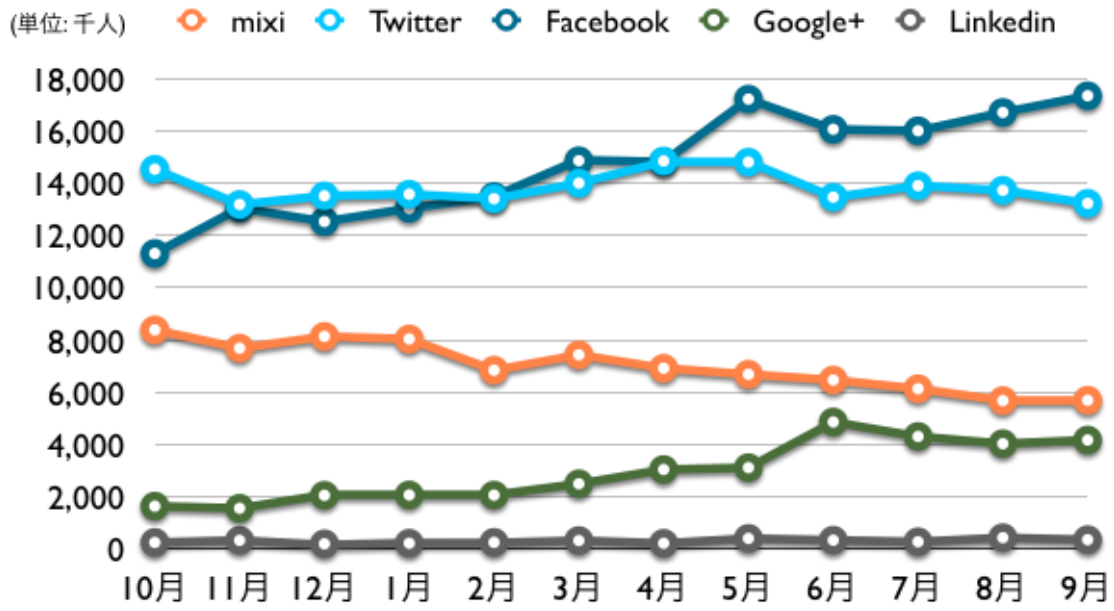
2 SNS: ソーシャル・ネットワーキング・サービスとは

ニールセンが公表している「日本の主要 SNS サイトの動向」では、mixi, Twitter, Facebook, Google+, Linkedin が取り上げられており、2012 年 9 月の調査では、図 1 の結果となっている。

この資料を見ると、Twitter, mixi, Facebook が主要な SNS として使われており、Twitter, mixi が横ばいであるのに対して、Facebook が利用者を伸ばしている。

また、この資料では取り上げられていないが、YouTube、USTREAM、ニコニコ動画などの動画サービス、GREE やモバゲーなどのゲーム系のサービスも、SNS として扱われることが多い。

■ PC訪問者数推移



(単位: 千人)

	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
mixi	8,385	7,684	8,135	8,037	6,839	7,428	6,914	6,682	6,463	6,127	5,671	5,686
Twitter	14,551	13,199	13,529	13,593	13,419	14,017	14,866	14,824	13,479	13,920	13,741	13,243
Facebook	11,319	13,061	12,543	13,049	13,508	14,877	14,831	17,241	16,083	16,027	16,730	17,369
Google+	1,622	1,541	2,038	2,051	2,045	2,480	3,028	3,099	4,852	4,295	4,019	4,159
Linkedin	228	310	176	199	231	302	197	384	315	255	412	335

図 1 2012/9 mixi, Twitter, Facebook, Google+, Linkedin PC ネット視聴データ[2]

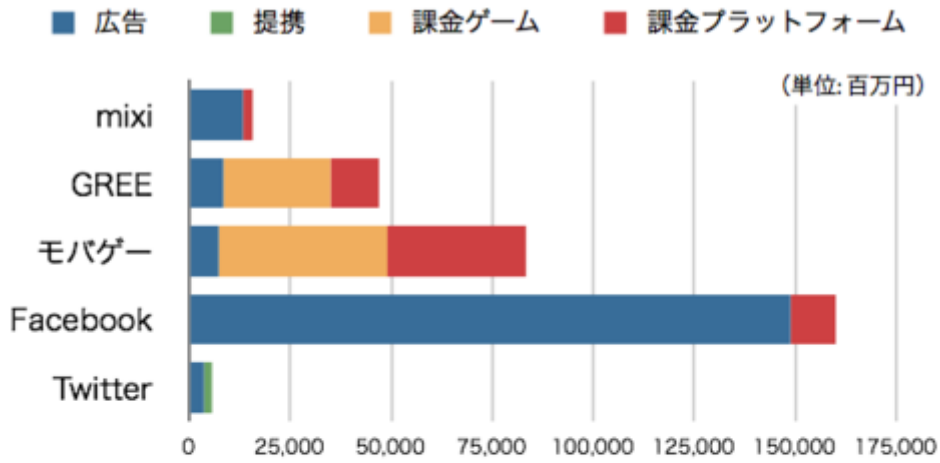
2.1. 広告媒体としての SNS

SNS のビジネスモデルについて、斉藤 徹氏が 2011 年 4 月に Alternative Blog に書いている「国内外主要 SNS のビジネスモデル比較 ～ mixi、GREE、Mobage、Facebook、Twitter[3]」に詳しくまとめられている。SNS は、変化の激しい分野で、既にサービス内容や企業形態が変わってしまっている部分もあるのだが、SNS ビジネスを俯瞰するうえで、重要かつ十分な情報がまとめられている。

この資料によれば、SNS の収益は、主に「広告」、「提携」、「課金ゲーム」、「課金プラットフォーム」で構成される。国内の SNS では、mixi が「広告」、GREE は「課金ゲーム」、モバゲーは「課金ゲーム」と「課金プラットフォーム」を主要な収益源としている。これは、GREE、モバゲーが自社で運用するゲーム関連の売り上げを主体としているのに対して、mixi は、プラットフォームの提供に徹していることが要因となっているようだ。

海外の SNS に目を向けると、Facebook の 2010 年の売上の 93%が広告売上で、7%が課金売上と推定されており、mixi と近い収益構造となっている。

Twitter は、検索エンジンサイトにツイートをインデックス化することを認める提携契約という、他の SNS では見られない形態の収益が 36%を占めており、64%を占める広告と並ぶ主要な収益の柱となっている。



	2010年度 (1-12月) 売上構成			
	広告売上	提携売上	課金売上 ゲーム	課金売上 プラットフォーム
mixi	13,262	0	0	2,413
GREE	8,410	0	26,549	11,963
モバゲー	7,264	0	41,754	34,302
Facebook	148,800	0	0	11,200
Twitter	3,600	2,000	0	0

注: 1ドル80円として換算

図 2 **【Fig5. 2010 年 1-12 月期 mixi、GREE、モバゲー、Facebook、Twitter のビジネスモデルの比較】** 出典：国内外主要 SNS のビジネスモデル比較

この分析で明らかなように、SNS の多くは広告を主要な収益源としており、新しいオンライン広告形態として定着している。インターネットにおけるオンライン広告の推移を振り返ると、Yahoo などのポータルサイトにおけるバナー広告、検索エンジンによる検索連動型広告、そして、ソーシャルメディア（SNS）による口コミ広告と、推移していると考えられている

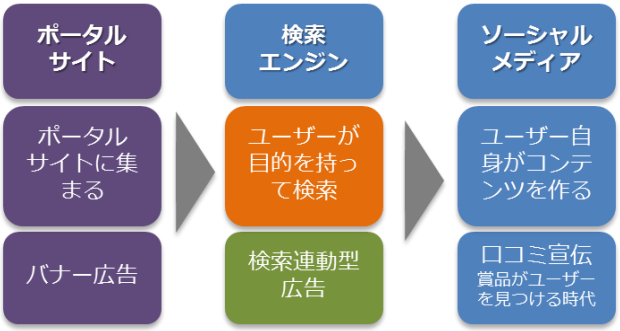


図 3 オンライン広告の推移 出典：ソーシャルネットワーク革命がみるみるわかる本

オンラインにおける消費行動は、電通が提唱する AISAS モデルが利用されることが多い。AISAS モデルは、「商品に気づき（Attention）、興味を持って（Interest）、情報を収集して（Search）、気に入ったら購入し（Action）、その後インターネットなどを通じて感想、意見を共有する（Share）」というフェーズで消費者の購買行動をモデル化したものである[4]。

オンライン広告としてのソーシャルメディア（SNS）は、AISAS モデルの Attention から Interest へと押し上げる効果と、それぞれのフェーズを下流方向に拡散していく効果があると考えられている。なおソーシャルメディア(SNS)を使った広告は、バナー広告や検索連動型広告を置き換えるものではなく、それぞれが連動する形で利用されている。

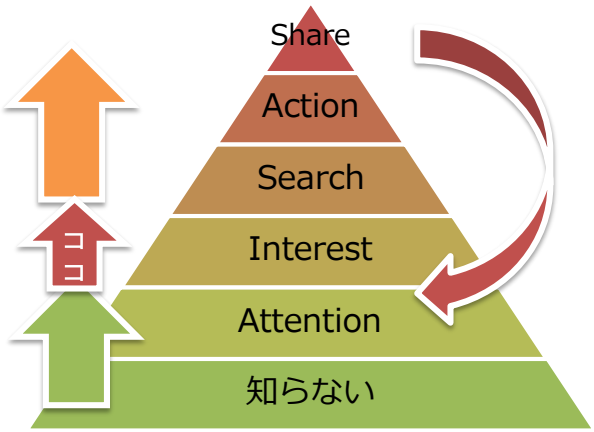


図 4 電通 AISAS での SNS の位置付

3 SNS のプライバシーとセキュリティの問題と対策

SNS にかかわるセキュリティやプライバシーにかかわる様々な事件が報道されている一方で、ちょっとした問題は起きているが、本当に懸念するような問題はないと指摘する声もある。当ワーキンググループで、SNS に関わる実被害について調査したところ、次のような事例が見つかっている。

- “友達”の解除が殺人事件に発展[5]
- 求職者に対する、SNS アカウントのパスワード開示要求[6]
- 偽装アカウントからの”友達”申請[7]
- 研究者によるユーザーデータ収集の実験[8]
- ハッカーが SNS と BLOG のデータにより割り出され逮捕される[9]
- SNS への写真投稿によるトラブル（チェックイン機能でウソバレ事件が続出！[10]）
- 動画再生を装った”いいね！”ボタンによる意図しない情報開示[11]
- ソーシャルハラスメント[12]

また、当ワーキンググループのメンバーでもある、日本 IBM 守屋氏の「フェイスブックが危ない」[13]では、次のような事例と懸念が紹介されている。

- 位置情報による自宅や勤務先がわかってしまう問題、タイムラインによる時間と場所の記録
- 16 歳の少女の誕生パーティに 15,000 人が”参加”、140 人以上が押し掛ける
- ストーカーアプリの存在[14]
- アカウントの乗っ取りによる個人情報の詐取
- 偽アカウントによる偽りの情報の発信
- 意図しない知人からの発見（ドメスティックバイオレンスに絡んだ事例など）
- 炎上
- 投稿による解雇や処分

これらの、事例を分類すると、「プライバシーにかかわる情報集積」に関わる問題、「マルウエアや詐欺のプラットフォームとしての利用」に関わる問題、「偽アカウント、アカウントの乗っ取り」による問題、「不適切な発言や行為」による問題、に分類することができる。そして、これらの問題は、相互に関連しながら、「サイバー犯罪」や「実社会における被害」へとつながっているものと考えられる（図 5）。

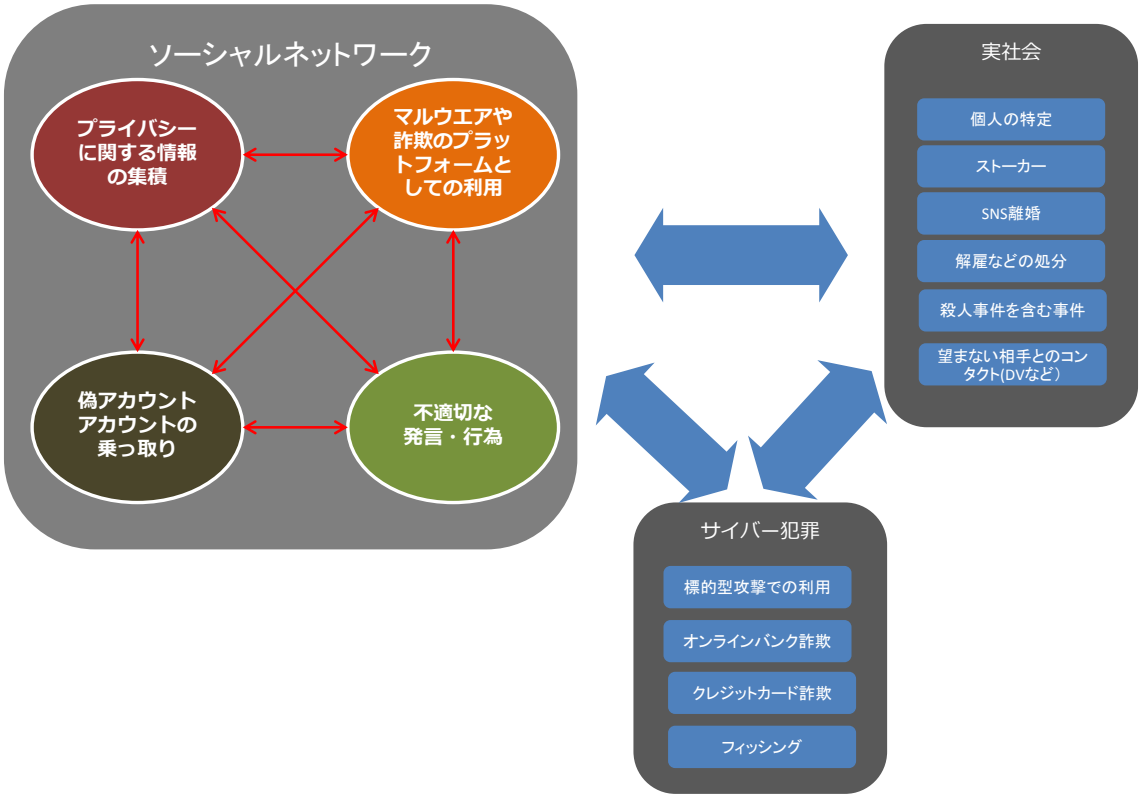


図 5 SNS の問題と、サーバー犯罪、実社会の関連

3.1. プライバシーに関する情報の集積

プライバシーに関する情報の集積と、それらの情報の意図しない公開や利用は、SNS のセキュリティとプライバシーに関する主要な問題となっている。

利用者自らが、意図せず公開をしてしまうケースとしては「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」などが要因としてあげられる。

3.1.1. 不用意な公開

「不用意な公開」は、公開されるとは知らずに、プロフィールに住所や電話番号などを記載する場合や、自らの生活や家族構成を投稿してしまうような場合で、詐欺行為や実社会での嫌がらせに利用される可能性がある。加えて、旅行などの投稿、Twitter のナウ発言、チェックインなどから留守にしている事がわかってしまい、空き巣に入られる危険性が指摘されている。また、これらの情報が蓄積されることで、将来的な問題につながることも懸念される。特に若年層においては、すべての情報を公開することをポリシーとしている場合が見受けられる

が、公開した情報は半永久的にインターネット上に残ることになる。このため、現在は問題のない内容でも、将来的には問題となる可能性を、利用者自身が認識して公開する内容を選択する必要がある。

なお公開の範囲として“友達の友達”というカテゴリーがあるが、“友達”の平均を 130 名、それぞれの友達の半分が重複していると考えると、“友達の友達”は、およそ 8,500 名になる。この中には、信頼ができないアカウントが含まれる可能性が高く、“友達の友達”は、無制限の“公開”とあまり変わりがないと考えた方が無難である。

3.1.2. 設定の不備

SNS の多くは、広告やデータの使用権から収益を得ていることから、基本的に情報を公開する方向で運用されている。日本における個人情報の収集は、オプトイン（事前確認）が主流であるが、SNS ではオプトアウト（停止等が求められたときに対応する）が主流となっている。

プロフィールなどに記載した利用者の住所や電話番号が、意図せず公開されている場合も少なくないが、これはデフォルトの設定が制限なしの“公開”とされていることが原因となっている。投稿や写真などについても、デフォルトの設定が”公開”となっているものが多いので、公開範囲に注意する必要がある。

「タグ付け」と呼ばれる写真に写っている人物を特定する機能も用意されているが、「タグ付け」の設定が適切でない場合、「友人」にタグ付けされ事により、「いつ・どこで・だれと・何をしていたか」といったプライバシーに関わる情報が意図せずに広範囲に公開されてしまうことがある。

3.1.3. 知識不足

利用者の知識不足から、意図せず、もしくは、危険性を認識していないことから意図的に、自らの情報を公開している場合が少なくない。「公開範囲に関する問題」、「位置情報に関する問題」、「詐欺行為の存在」、「オンライン広告に対する認識」などに対する知識が問題となる場合が多い。

① 公開範囲に関する問題

もっとも基本的な問題として、プロフィールなどに記載した情報、自らの投稿やコメント、“いいね！”などのリアクションが公開される範囲が正しく認識されていない事が問題となっている場合がある。

多くの SNS は、利用者情報を広告などに利用することでビジネスが成り立っていることから、デフォルトの設定が情報を公開する設定になっている場合が多い。つまり、なにも設定をしなければ、情報の閲覧は制限されないと考える必要がある。

例えば、Facebook では、“基本データ”として住所や電話番号などを記載するのだが、これらの項目はデフォルトでは“公開”、つまり誰でも閲覧できる状態になっている。

② 位置情報に関する問題

GPS 機能の付いたスマートフォンで撮影した写真を、BLOG や Twitter に掲載した場合、利用者が明示的な設定を行わない限り、写真に位置情報が埋め込まれており、自宅が特定されるなどの問題が懸念されて

いる[15]。先に紹介したハッカーが逮捕された事例も、写真に埋め込まれた位置情報から犯人が特定されたと考えられている[9]。

また、Facebook の“地図”では、チェックインや写真の位置情報に基づいて、利用者がいた時刻と場所が地図上に表示される。わざわざ写真の位置情報を調べるまでもなく、居住場所、勤務先、行きつけの店等が一目瞭然でわかってしまう。

図 6 Facebook の”地図”による表示

③ 詐欺行為の存在

SNS 上でも詐欺行為は行われている。SNS を通じた詐欺や詐欺的なメッセージは、“友達”を通じて発信されるため信用されることが多いようで、SNS を使った詐欺行為は、スパムなどのメールを使った詐欺行為と比較して、騙される可能性が高いと考えられている。

「偽装アカウントからの”友達”申請[7]」の例のように、架空の人物や、実在する人物を装ったアカウントからの友達申請が大量に行われた事例がある。この事例は、個人情報の詐取に加えて、“友達”をからの情報を装うことで、アフィリエイトによる収益を狙ったものではないかと考えられている。

また、動画などの再生ボタンに対する“いいね！”ボタンの埋め込みも行われている。例えば、アダルトサイトや反社会的なサイトにアクセスした際に、そうとは知らずに“いいね！”ボタンを押してしまい、その結果として、そのサイトをアクセスしたことが周知されてしまうという事件も起きている[16]。なお、この手法を悪用すれば、利用者がまったく覚えのないサイトを、あたかも閲覧したように見せることもできてしまう。

④ オンライン広告に対する認識

SNS では、数多くのオンライン広告が表示されるが、一般的に、これらのオンライン広告に対する審査は行われていない。つまり、誰もが広告を出すことができる（図 7）。このため、偽セキュリティソフトと思われるソフトウェアや、詐欺の可能性が高いと一目でわかる広告まで、無審査で広告として表示される。

日本的な感覚では問題と思える運用だが、問題のある広告を報告する仕組みが用意されており、問題のある広告は迅速に対処するというポリシーで運営が行われているものと考えられる。広告は審査が行われていると考える利用者とは、大きな認識のギャップが存在するといえる。

図 7 Facebook での広告の掲載画面

3.1.4. アプリケーションによる公開

Facebook ではアプリケーションと呼ばれるサードパーティソフトウェアが利用できるのだが、このアプリケーションは、基本データ、プロフィール情報、写真、他の人と共有した情報へのアクセス、自分の名前を使った Facebook への投稿を行うことができる。つまり、アプリケーションは、Facebook を使って利用者ができることは、ほぼ全て実施することができることになる。この機能が必ずしも問題となるわけではないのだが、利用される範囲が不明確な点と、「他の人と共有した情報」に対してアクセスができる点が問題となる。例えば、「研究者たちが Facebook に 102 体のボットを送り込んで 250GB のユーザーデータを収集」[8] のように、大量の個人情報を収集することができてしまう。

mixi やゲーム系の SNS でもアプリケーションの利用が可能だが、同様にサードパーティで運営されている場合が多いことを認識する必要がある。

図 8 アプリの許可画面の例

3.1.5. ”友達”による情報の公開

「SNS への写真投稿によるトラブル（チェックイン機能でウソバレ事件が続出！[10]）」のように、SNS 上の“友達”による情報の公開が問題となるケースもある。典型的なケースは、ここで紹介されているように、”友達“による SNS への投稿で、秘密にしておいたことが露呈してしまうようなものである。

また、“タグ付け“と呼ばれる、写真に写っている人物を SNS のアカウントに結び付ける機能も、同じ問題をはらんでいる。例えば、筆者の”地図“（図 9）では、3 つの情報が記載されている。どれも筆者が投稿したものではなく、筆者が登壇したセミナーの写真に”タグ付け“されたものと、一緒に食事をした”友達”が”チェックイン“[17]したものである。

ある意味、楽しい機能で、仲間内で使っている分には良いのだが、思わぬところで情報が利用・悪用される可能性がある。つまり、SNS におけるプライバシーの問題は、本人・友人・SNS プロバイダーそれぞれの方針や設定に依存していることを認識する必要がある。

図 9 筆者の"地図" 3 件とも"友達"によって登録されている

なお、"タグ付け"については、「あなたがタグ付けされたタイムライン上の投稿の公開範囲」と、「あなたがタグ付けされたコンテンツをタイムラインに掲載するかどうかを確認する」を設定することで、公開される範囲を制御することができる。

図 10 タイムラインとタグ付けの設定

また、先ほど述べたアプリケーションについても同様の問題がある。利用者が設定を行わない限り、以下の項目について、"友達"が許可をしたアプリケーションからのアクセスを許してしまい、アプリケーションを通じて、自分の情報を収集されてしまう懸念がある。

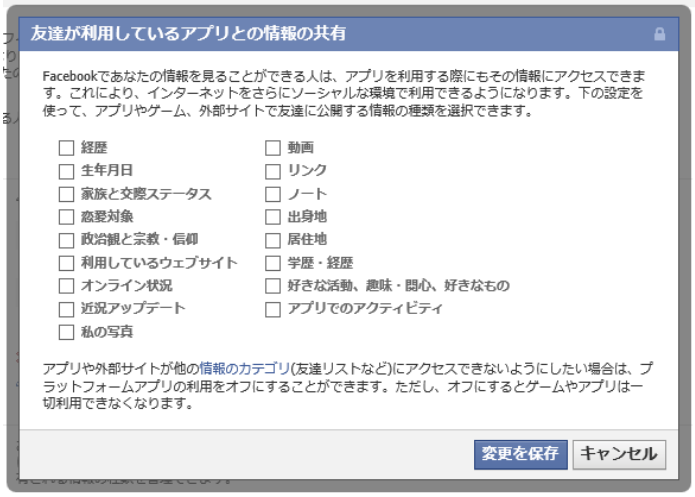


図 11 友達が利用しているアプリとの情報の共有

3.1.6. 他の情報との関連付け

複数の SNS、Web メールサービス、BLOG などの情報が関連付けられることにより、思わぬプライバシー情報が露呈することがある。「ハッカーが SNS と BLOG のデータにより割り出され逮捕される [9]」でも、Twitter で侵入したことを公表したした際に利用したサイトに写真が掲載されており、その写真に位置情報が残っていたことから人物の特定につながった。

これほど複雑な例ではなくとも、店員の方がつけている名札や、レシートに印刷される担当者名から、SNS のアカウントを特定できる場合もある。また、入社試験の際に、SNS の情報の公開が求められるケースや、応募書類と SNS などのインターネット上のデータを照合されるといったことも起きている。

3.1.7. SNS のポリシー変更

一般に、SNS ではデフォルトの設定が、時間と共に公開されるものが増える傾向にあり、なかには利用者への明確な通知なしに変更され、これまで非公開であったものが突然、公開されてしまった事例もある。SNS を利用する上では、このような点についても注意をしていく必要がある（図 12）[18]。

例えば、Facebook では、2011 年 11 月にタイムラインと呼ばれるインターフェースに変更され、後述する ”地図“が追加されたことにより、「②位置情報に関する問題」で触れたように、利用者の位置情報の履歴が見られることになった。”地図“は、明示的な設定をしない限り、制限のない”公開“の設定になっていたことから、知らぬ間に自宅や職場を公開している状況が存在した。

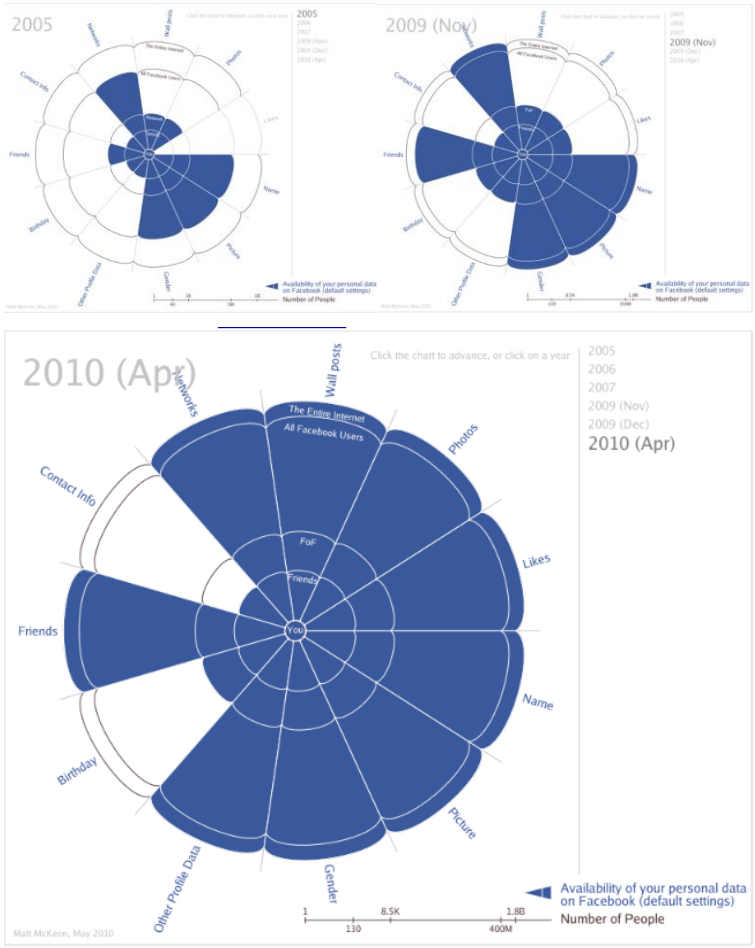


図 12 The Evolution of Privacy on Facebook

3.2. マルウエア感染や詐欺行為のプラットフォームとしての利用

SOPHOS の「セキュリティ脅威レポート 2012」[19]では、2012 年の新しいトレンドとして、「ソーシャルメディアと Web」に対する攻撃が増加するものと予想している。また、G Data Software の Eddy Willems 氏は、「SNS でのウイルス感染の危険度はメールより 10 倍も高い[20]」との発言をしている。

SNS 上の”友達“を通じた情報は信頼関係があるため、一般的なスパムと比較して騙されてしまう可能性が高い。マルウエアの拡散や詐欺行為においても、この信頼関係が利用されるようになっている。

また、短縮 URL、画像からのリンクや、画像そのものを使った攻撃など、SNS の特徴を活かした攻撃が可能である点も、マルウエアを感染させるための手段として悪用される背景となっている。

3.3. 偽アカウント・アカウントの乗っ取り

SNS のアカウントの乗っ取りも頻繁に行われている。SOPHOS の Graham Cluley 氏が、Facebook が公表したセキュリティに関する資料から、「一日当たり 60 万件の不正なログインが行われている[21]」と分析をしている。また、この BLOG を紹介している TechCrunch[22]の記事では、この資料から次のような分析も行っている。

- Facebook 上で共有されるコンテンツのうち、スパムは 4%未満（メールは 89.1%がスパム）
- Facebook のユーザでスパムを経験する人は 1 日の全ユーザ数の 5%未満
- 1 日にログインするユーザ数は Facebook の 7 億 5000 万あまりのユーザの 50%
- 一人のユーザのフレンド数は平均 130 人
- Facebook 上のユーザの 1 か月の総滞留時間は 7000 億分

一方で、アカウントを作成していない場合は、別の問題が起きる可能性がある。例えば、Twitter で鳩山首相（当時）の偽アカウントを作り、発言を繰り返した例がある[23]。2009 年 7 月の JCAST ニュースの記事では、Twitter のなりすましが疑われる例として、小室哲哉氏、サイバーエージェント社長の藤田晋氏、作家の村上春樹を挙げている[24]。

偽アカウントの有効性について、前述の守屋氏の書籍 [13] では、UOLDiveo が行った実験を紹介している[25]。この実験では、ターゲットの上司の ID を複製（クローン化）して偽の Facebook アカウントを作成。そのアカウントから、この上司の友人の友人 432 人に友達リクエストを送信したところ、1 時間で 24 通のリクエストが承認された。なお、ほとんどの人は、既にその上司と“友達”の関係にあった。そして上司の直接の友人 436 人にリクエストを送信し、1 時間で 14 人の承認を得て、最終的にターゲットとも“友達”になることに成功している。

3.4. 不適切な発言・行為

不適切な発言による炎上事件は、SNS に限ったものではないが、SNS でもよく発生している。「炎上事例まとめ〈ツイッター/ブログ/amazon レビュー/iPhone アプリなど〉[26]」では、牛丼店のアルバイトの動画、地下鉄職員が利用客の個人情報を BLOG に公開、コーヒー飲料の Twitter を使ったキャンペーン、遅刻した社員に反省文を読ませた動画などが紹介されている。

また、ホテル内のレストランの従業員が著名人の来店を公表した例や、カンニングや違法性の高い行為を自ら公表したことで社会的な問題となった例もある。

個人の投稿はともかく、企業のサイトや投稿が炎上するのは避けなければならない。「「炎上」させないための「べからず集」[27]」では、企業のキャンペーンなどが炎上した事例を紹介し、炎上を防ぐためアプローチが紹介されている。そして、“炎上させないための「べからず集」”として次の項目を挙げている。

炎上させないための「べからず集」：出典「炎上」させないための「べからず集」 [27]

◦運営者の身分や企業との関係性を隠すべからず
◦不誠実、不公平な対応はするべからず
◦各種法令を違反するべからず（道交法や薬事法など）
◦不謹慎な発言はするべからず
◦他社批判をするべからず
◦オンライン・オフラインの対応を区別するべからず

それぞれ、ある意味当たり前のことではあるのだが、従来の一方的な情報発信では問題視されることの少ない項目が多い点に注意する必要がある。

4 むすび

SNS＝ソーシャル・ネットワーキング・サービスの利用は、今後とも拡大していく可能性が高い。便利なシステムであり、生活空間を格段に広げることができる反面、プライバシーにかかわる問題が表面化している。

これらの問題は、SNS の特性を理解し、適切な設定を行うことで、回避できるものが少なくない。JNSA SNS セキュリティ WG では、SNS に関わるトラブルを避けるための措置として、以下の項目を挙げている。

SNS を安全に歩くための 10 項目：JNSA SNS セキュリティ WG

1. 常に公開・引用・記録されることを意識して利用する
2. 複雑なパスワードを利用し、セキュリティを高める設定を利用する
3. 公開範囲を設定し、不必要な露出を避ける
4. 知らない人とむやみに“友達”にならない、知っている人でも真正の確認をする
5. “友達”に迷惑をかけない設定を行う
6. “友達”から削除は慎重に、制限リストなどの利用も考慮する
7. 写真の位置情報やチェックインなど、技術的なリスクを理解し正しく利用する
8. むやみに“友達”のタグ付けや投稿を行わない
9. 対策ソフトを利用し、危険なサイトを利用するリスクを低減する
10. 企業などの組織においては、SNS ガイドラインを策定し遵守する

今日でも、「メールはいらない」と発言されるビジネスマンもいるように、SNS は個人や企業にとって必ずしも必要なものとは限らない。一方で、SNS による利用者間のコミュニケーション、BtoC のコミュニケーションは多くの可能性を持っており、適切に利用することで、それぞれの潜在能力を引き出していくことができるものだと考えている。 本稿が、SNS を安全に歩くうえで、何らかの参考になれば幸いである。

なお、Facebook では、以下のページからアカウントの管理やプライバシーについて解説を行っている。Facebook ユーザは、一度目を通しておくことをお勧めする。

Facebook ヘルプセンター：基本情報
https://www.facebook.com/help/?page=260315770650470&ref=bc

付録：Facebook の設定項目 (2012/5/31 調べ)

基本データ	職歴と学歴			基本的な公開設定（公開、友達の友達、友達、カスタム）
	自己紹介			基本的な公開設定（公開、友達の友達、友達、カスタム）
	基本データ	性別		タイムラインに性別を表示する・しない
		生年月日		生年月日をタイムラインに表示する 月と日のみタイムラインに表示する 生年月日をタイムラインに表示しない
		血液型		表示に関する選択なし
		恋愛対象		基本的な公開設定（公開、友達の友達、友達、カスタム）
		言語		基本的な公開設定（公開、友達の友達、友達、カスタム）
		宗教・信仰		基本的な公開設定（公開、友達の友達、友達、カスタム）
		政治感		基本的な公開設定（公開、友達の友達、友達、カスタム）
		住んだことのある場所	居住地	基本的な公開設定（公開、友達の友達、友達、カスタム）
			出身地	基本的な公開設定（公開、友達の友達、友達、カスタム）
		交際関係と家族	交際ステータス	以下の項目について選択可能 独身、交際中、婚約中、既婚、複雑な関係、オープンな関係、配偶者と死別、別居、離婚 基本的な公開設定（公開、友達の友達、友達、カスタム）
			家族	基本的な公開設定（公開、友達の友達、友達、カスタム）
		連絡先情報	携帯番号	基本的な公開設定（公開、友達の友達、友達、カスタム）
			住所	基本的な公開設定（公開、友達の友達、友達、カスタム）
			スクリーン名（ＩＭスクリーンネーム）	基本的な公開設定（公開、友達の友達、友達、カスタム）
			ウェブサイト	基本的な公開設定（公開、友達の友達、友達、カスタム）
			メールアドレス	基本的な公開設定（公開、友達の友達、友達、カスタム）
		好きな言葉		基本的な公開設定（公開、友達の友達、友達、カスタム）
プライバシー設定	投稿時のプライバシー管理：デフォルト設定の管理			基本的な公開設定（公開、友達の友達、友達、カスタム）
	つながりの設定	あなたのタイムラインを氏名で検索できる人		基本的な公開設定（公開、友達の友達、友達、カスタム）
		メールアドレスまたは電話番号であなたを検索できる人		基本的な公開設定（公開、友達の友達、友達、カスタム）
		あなたに友達リクエストを送信できる人		基本的な公開設定（公開、友達の友達、友達、カスタム）

		あなたに Facebook メッセージを送信できる人		基本的な公開設定（公開、友達の友達、友達、カスタム）
	タイムラインとタグ付け	あなたのタイムラインに投稿できる人		基本的な公開設定（公開、友達の友達、友達、カスタム）
		ほかの人があなたのタイムラインに投稿したコンテンツの共有範囲		基本的な公開設定（公開、友達の友達、友達、カスタム）
		あなたがタグ付けされたコンテンツをタイムラインに掲載するかどうかを確認する		オン・オフ
		あなたがタグ付けされたタイムライン上の投稿の公開範囲		基本的な公開設定（公開、友達の友達、友達、カスタム）
		あなたの投稿へのタグ付けを確認する		オン・オフ
		あなただと思われる写真がアップロードされたときにタグ付けの提案が表示される人		非公開・友達
	広告、アプリ、ウェブサイト	利用しているアプリ		アプリの一覧が表示される
		他のユーザーが利用しているアプリとの情報の共有		以下の項目についてのチェックボックス 経歴、生年月日、家族と交際ステータス、恋愛対象、政治と宗教・信仰、オンライン状況、近況のアップデート、私の写真、動画、リンク、ノート、出身地、居住区、学歴・経歴、好きな活動、趣味、関心、好きなもの、アプリでのアクティビティ
		インスタントパーソナライゼーション		有効・無効
		一般検索		有効・無効
		広告	外部広告の設定を編集	友達のみ・非公開
			ソーシャル広告を編集の設定	友達のみ・非公開
	タイムラインの過去の投稿の共有範囲を制限			全体の投稿に対しする公開範囲の設定。わかりにくい設定
ウォール	友達	編集　（友達の公開範囲の編集）		基本的な公開設定（公開、友達の友達、友達、カスタム）

[1] ソーシャル・ネットワーキング・サービスの一覧
http://ja.wikipedia.org/wiki/%E3%82%BD%E3%83%BC%E3%82%B7%E3%83%A3%E3%83%AB%E3%83%BB%E3%83%8D%E3%83%83%E3%83%88%E3%83%AF%E3%83%BC%E3%82%AD%E3%83%B3%E3%82%B0%E3%83%BB%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%AE%E4%B8%80%E8%A6%A7

[2] 2012/9 mixi, Twitter, Facebook, Google+, Linkedin PC ネット視聴データ : Nelsen Netview
http://media.looops.net/sekine/2012/10/25/neilsen-netview-201209/

[3] 国内外主要 SNS のビジネスモデル比較 ～ mixi、GREE、Mobage、Facebook、Twitter
http://blogs.itmedia.co.jp/saito/2011/04/sns-mixigreemob-d05d.html

[4] デジタル化による生活者の購買プロセス変化～AIDMA から AISAS®へ
http://www.dentsu.co.jp/ir/data/pdf/dentsu-br157.pdf#page=9

[5] Gunned down over a Facebook snub: The couple 'shot dead by a father... because they defriended his daughter on social networking site'
http://www.dailymail.co.uk/news/article-2098583/Father-60-charged-murder-shot-dead-couple-defriended-daughter-Facebook.html#ixzz1yOWmh840http://www.dailymail.co.uk/news/article-2098583/Father-60-charged-murder-shot-dead-couple-defriended-daughter-Facebook.html

[6] Facebook を監視する雇用主--従業員採用で判断材料に
http://japan.cnet.com/news/commentary/35014891/

[7] 拝啓 Facebook 殿 日本の Facebook で恥かしい汚染が広まっております（永江一石の IT マーケティング日記）
http://www.landerblue.co.jp/blog/?p=1005

[8] 研究者たちが Facebook に 102 体のボットを送り込んで 250GB のユーザーデータを収集
http://jp.techcrunch.com/archives/20111101researchers-flood-facebook-with-bots-collect-250gb-of-user-data/

[9] セキュリティは楽しいかね？ CabinCr3w のメンバーはなぜ FBI に逮捕されたのか?
http://d.hatena.ne.jp/ukky3/20120416/1334533781

[10] Facebook チェックイン機能でウソバレ事件が続出！
http://nikkan-spa.jp/199462/bkr_120501_01

[11] エロサイトに「いいね」した人がエロサイトを見ていたとは限らない
http://blog.maripo.org/2012/05/like-trap/

[12] 出典 すべての投稿に即「いいね！」こんな「ソーハラ」オヤジは嫌われる
http://www.j-cast.com/kaisha/2012/04/10128386.html

[13] フェイスブックが危ない、守屋英一著、文藝春秋 ISBN978-4-16-660867-6

[14] 周囲の女性を表示するアプリ「Girls Around Me」、開発元が批判に反論
http://japan.cnet.com/news/service/35015733/?ref=rss
iPhone のナンパアプリ「Girls Around Me」（エイプリルフールネタじゃないです）
http://blogs.itmedia.co.jp/burstlog/2012/04/iphonegirls-aro-3376.html?ref=rssall
Facebook の友だちをストーカーできるアプリ Friend-Watch–あの Andy の懲りない第二作
http://jp.techcrunch.com/archives/20110823new-friend-watch-app-lets-you-stalk-your-facebook-friends/

[15] iPhone、情報流出の「落とし穴」 ブログや Twitter に掲載した写真から自宅が特定される？
http://pc.nikkeibp.co.jp/article/trend/20091204/1021023/?rt=nocnt

[16] 知らない間にアダルトサイトを「いいね」 Facebook 知人、同僚に性的嗜好がバレる http://www.j-cast.com/2012/04/28130346.html

[17] Facebook: いつ、誰と、何を、そして「どこで」
https://www.facebook.com/note.php?note_id=159535824058810

[18] The Evolution of Privacy on Facebook
http://mattmckeon.com/facebook-privacy/

[19] SOPHOS の「セキュリティ脅威レポート 2012」
http://www.sophos.com/ja-jp/security-news-trends/reports/security-threat-report.aspx

[20] SNS でのウイルス感染の危険度はメールより 10 倍も高い
http://itpro.nikkeibp.co.jp/article/NEWS/20101126/354594/

[21] 600,000+ compromised account logins every day on Facebook, official figures reveal
http://nakedsecurity.sophos.com/2011/10/28/compromised-facebook-account-logins/

[22] Facebook の 1 日の不正ログインは 60 万件−アカウントがハックされている
http://jp.techcrunch.com/archives/20111028facebook-sees-600000-comprised-logins-per-day/

[23] Twitter で鳩山首相になりすました男性が謝罪 「有名人でコントやってみたかった」
http://www.itmedia.co.jp/news/articles/0912/28/news014.html

[24] 著名人の「なりすまし」 Twitter で相次ぐ
http://www.j-cast.com/2009/07/22045839.html

[25] Facebook の誰とでも、24 時間以内に「友達」になれる方法 （WIRED.jp）
http://itpro.nikkeibp.co.jp/article/NEWS/20111212/376362/
É possível ficar amigo de qualquer um no Facebook em até 24 horas, alerta especialista
http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/11/16/e-possivel-ficar-amigo-de-qualquer-um-no-facebook-em-ate-24-horas-alerta-especialista.jhtm

[26] 「炎上事例まとめ〈ツイッター/ブログ/amazon レビュー/iPhone アプリなど〉
http://matome.naver.jp/odai/2128581417617980001

[27] 「炎上」させないための「べからず集」
http://marketingis.jp/archives/1938

