JPCERT CC®

法人における SNS 利用に伴うリスクと対策

一般社団法人 JPCERT コーディネーションセンター

2013 年 03 月 28 日

JPCERT CC®

目次

1. はじめに

SNS（ソーシャル・ネットワーク・サービス）は、インターネット利用者が情報を発信するメディアのひとつであり、人と人とのつながりを促進・サポートする機能を有するコミュニティ型の会員制サービスとして、世界中で利用者を増やしている。利用者の増加に伴い、法人においても、新しいコミュニケーション・ツールとして、SNS を利用して、顧客や SNS 利用者からのストレートな声を体系的に集め、商品やサービスの改善の参考にしようとする動きも見られる。その一方で、利用上の不注意が発端で、ネガティブな法人イメージを与えることになった失敗事例もあれば、法人としては SNS を利用していなくても、従業員が個人として行った SNS 上での発言が発端で、法人が非難の的になる事例もある。

本レポートでは、日本国内および諸外国における SNS に起因するリスクとセキュリティ対策の現状について、公表されている情報（文献・Web）を収集するとともに、国内 SNS 提供事業者およびセキュリティベンダへインタビューを行い、それらの情報を基礎として考察を加え、SNS の利用に関して法人が取るべき対策についてまとめた。

SNS の利用に関して法人が被るリスクには、次の 2 つがある。

- 法人の従業員が個人として SNS を利用することから生じるリスク
- 法人が自ら SNS を利用することから生じるリスク

前者のリスクについては、法人として SNS を利用するか否かにかかわらず、すべての法人において対策を検討しておく必要があるといえる。

本レポートでは、第 2 章で SNS の利用実態を概観し、第 3 章で SNS の特性とそれが招く危険性についてまとめる。第 4 章では、個々のリスクと具体的なトラブル事例について述べ、そうしたトラブルをできる限り回避し、また、不運にもトラブルが生じた際の影響を最小限に抑えるために法人としてあらかじめ取っておくべき対策を第 5 章で述べる。

2. SNS の利用実態

近年、SNS の利用者数が急速に増加している。種々の SNS が無料で提供されており、利用者は、目的ごとに、例えば、友達や同僚とのコミュニケーションには、様々な情報交換機能などを有する Facebook や mixi を、ゲーム愛好者とのコミュニケーションには Gree や Mobage を、簡易な情報収集・発信手段としては Twitter をといったように、複数の SNS サービスを、それぞれのシステムの特徴に応じて使い分けている。

図 1 に、インターネットメディア総合研究所の調査によるソーシャルメディア人口推計値を示す。SNS 利用者数は 2008 年にすでに 1000 万人を超えており、2010 年以降はその数が急増しており、2012 年 5 月には延べ 5000 万人に達している。

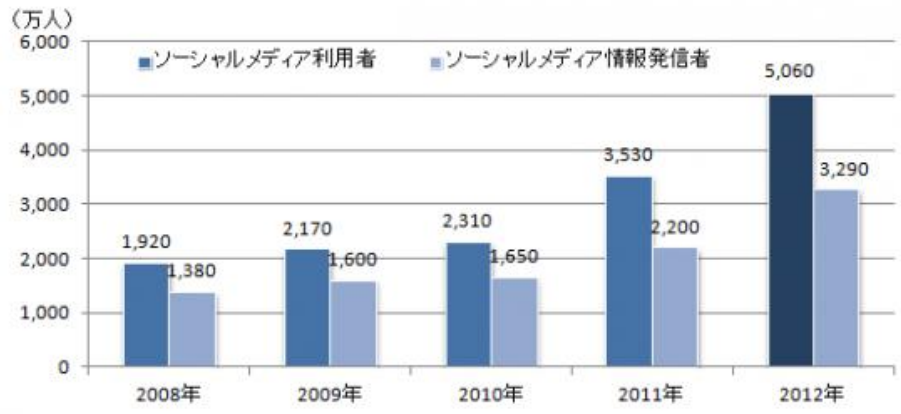

図 1: ソーシャルメディア人口推計値
(2012 年 5 月時点での日本のソーシャルメディア人口)

出典：『ソーシャルメディア調査報告書 2012』株式会社インプレス R&D

総務省の平成 23 年度版情報通信白書に掲載された SNS の利用目的についてのアンケート結果、図 2 によれば、多くの利用者が「もともとの知人とのコミュニケーション」と「情報収集」、「同じ趣味・嗜好を持つ人との出会い」を利用目的に挙げており、4 番目に「自分の交友関係を広げたい」が挙っている。SNS を、実社会における交友の場を補完する「ネット上の場」として利用することを基本としつつ、ネットの特性を活用して、実社会では出会う機会の少ない人々との出会いを求めていると言えそうだ。インターネットを利用した通信メディアとして、公開性と広域性を特徴とする掲示板やブログと、受信者をアドレスで特定することで管理可能な電子メールとのちょうど中間に位置する、快い帰属感をともなったグループ内コミュニケーションを手軽に実現できるツールとし

て歓迎され、利用者の急増につながっているとものと考えられる。

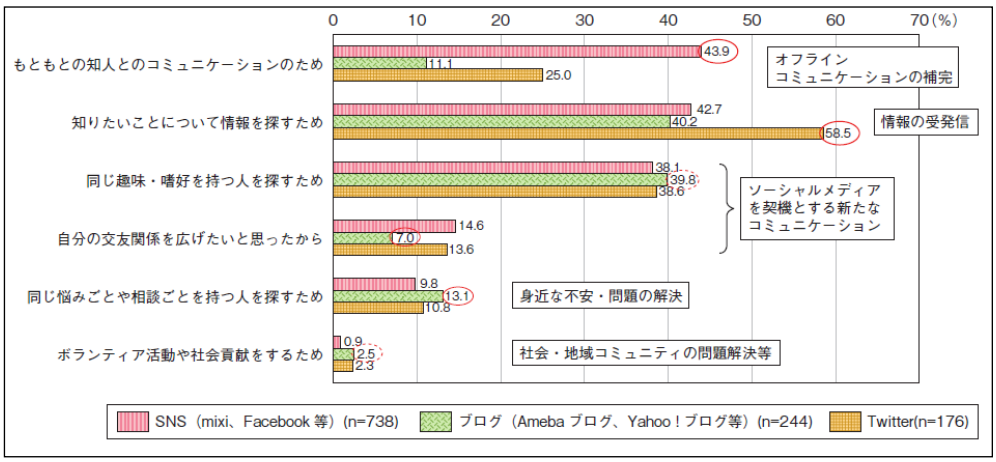

図 2: 個人の利用目的

出典：「平成 23 年度版情報通信白書」総務省

こうした SNS の個人利用者の増加傾向に対応して、個人向けの事業を営む法人を中心に、従来であれば葉書やダイレクトメール、自社のホームページを利用することが一般的だった、新製品やサービスの広告活動に利用するなど、事業活動の中で SNS を積極的に活用しようとする動きが増えてきている。インプレス R&D による「企業のソーシャルメディア利用実態調査 2011」によれば、法人による SNS の利用目的は、図 3 に示すとおり、

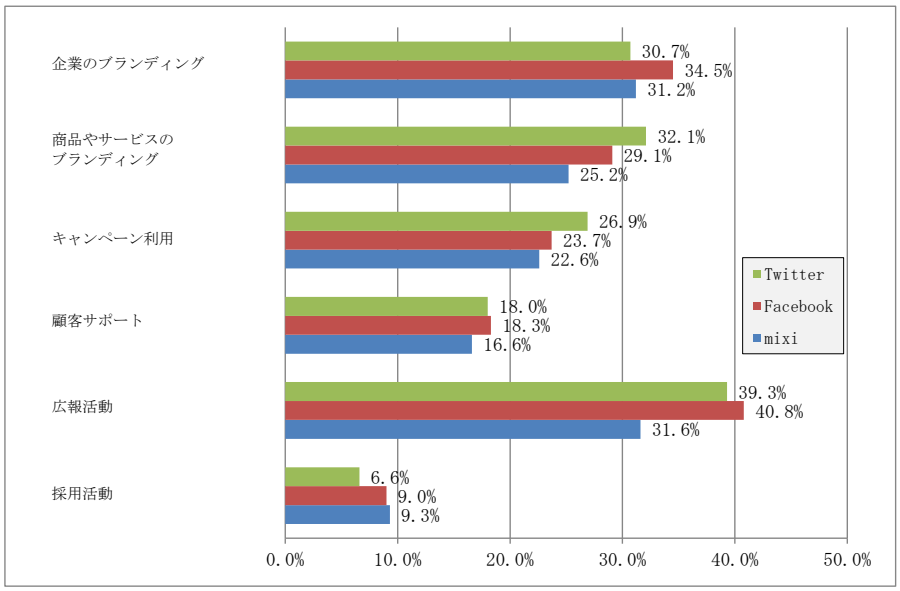

図 3: SNS の利用における効果

出典：「企業のソーシャルメディア利用実態調査 2011」インプレス R&D のデータをもとに作図

「広報活動」が最も多く、「企業のブランディング」や「商品やサービスのブランディング」が続いている。SNS の中に形成されているコミュニティの特性に合わせたメッセージをタイムリーに届けられる SNS の特性を活用した広報活動を狙っており、また、企業ホームページを通じた企業や商品、サービスのブランディング発信を補完する通信メディアとして SNS を活用しようとしていることが見て取れる。また、広告活動に対して専任の従業員や経費を充てることのできない法人にとっては、SNS といったプラットフォームを利用することで、情報伝達媒体を利用する広告費を抑えることが可能な点も魅力だと考えられる。

以下に、法人による SNS の活用例をあげる。

(1) 法人用の SNS アカウントを取得しての利用

一部の法人は、SNS の法人用アカウントを取得し、これを使って SNS 利用者への広告・宣伝メッセージを送り届けている。大手の法人の場合には、製品や部署ごとに SNS の公式アカウントを作成・運用するケースもある。

以下に、正式アカウントを公開している法人の例を列挙する。

（参考） 正式アカウント一覧 50 音順

味の素株式会社
SNS 公式アカウント一覧
http://www.ajinomoto.co.jp/socialmedia_account/

株式会社ベネッセコーポレーション
ソーシャルメディア公式アカウント一覧
http://www.benesse.co.jp/campaign/socialmedia.html

サントリーホールディングス株式会社
ソーシャルメディア アカウント一覧
http://www.suntory.co.jp/enjoy/socialmedia/

シャープ株式会社
ソーシャルメディア公式アカウント
http://www.sharp.co.jp/corporate/socialmedia/

トヨタ自動車株式会社
ソーシャルメディア公式アカウント
http://www.toyota.co.jp/jpn/company/links/social/index.html

(2) SNS 上での法人の評判(レピュテーション)測定

今後の製品開発やサービスの改善のための分析材料として活用される、製品やサービスに対する評判(レピュテーション)を収集するための手段として SNS が使われている。SNS では利用者の本音が吐露されやすい場所であり、その投稿には法人の製品やサービスの評価や評判も多く含まれる。また、Facebook のようなサービスに投稿された情報は、投稿者のプロフィールと併せて分析することが可能であり、性別、年齢、居住地域などの情報と関連付けた立体的な評判を評価することができる。Twitter では、自社名や自社製品名を検索すると、それらに関係のある Tweet を抽出してリストアップすることができる。

3. SNS の特性とそれが招く危険性

SNS は、電子メールやブログなどの旧来のインターネット上の通信メディアと比べて、次に述べるような特性をもち、そうした特性ゆえに発生する危険性を伴っていると考えられる。

3.1. 個人情報の公開とそれが招く危険性

SNS 上では、コミュニケーションを拡大するため、同窓生や同郷の人など共通の体験や趣味をもつ利用者を検索して見つけ出し、SNS 上での自分のコミュニティに加えるための機能が提供されている。こうした機能により他の利用者から発見してもらえるよう、SNS 利用者は登録時に一定の個人情報の提示を求められる。Facebook や LinkedIn など一部の SNS では、実在する個人を特定できるような情報も求められる。Facebook では実名を公開することが条件であり、LinkedIn においては実名のみならず、勤務先の法人名や学歴に関しても公開される。SNS により細かな差異はあるものの、SNS を利用するにあたっては、多かれ少なかれ個人情報を提示することと引き換えに、気を許した発言ができる「仲間内のコミュニケーションの場」が実現されているのである。

SNS 利用の前提となっている個人情報の開示が、本人が想定していた以上の公開性を帯びてしまう可能性があることに注意をしておく必要がある。その原因の一つは、開示した情報の閲覧範囲の制御に関する利用者の誤解や操作ミスである。その中には、閲覧範囲のデフォールト設定が途中で SNS 提供事業者により変更され、利用者がその影響に気付いていない場合も含まれる。

さらに、開示した複数の情報を組み合わせることにより、あるいは、それらをインターネット上の公開情報や SNS などを通じて入手できる他の情報と組み合わされることにより、対応する物理的な存在を一人に絞り込むことができるなど、本人が元々想定していた以上に立ち入った個人情報を他人に知られる可能性がある。

3.2. 利用者がもつ種々の人間関係の表現とそれが招く危険性

SNS 上でのコミュニケーションでは、「同じ SNS 利用者の A さんと私は B 大学の同窓生である」とか「私は C 社でアルバイトをし始めた」などのように、しばしば利用者相互間や特定の法人との関係が記述される。発信者は他人に知られても構わないとの判断

を行った上で、こうした関係性を公表するのであるが、その記述の中で言及される他人や組織にとっては公表されたくない内容が含まれている場合があり得る。

さらに、関係性の記述を引用したメッセージを他の利用者が発信することにより、元の記述を行った利用者が意図していた範囲の外側にいる利用者にまで情報が伝わる可能性もある。

3.3. 利用者間の信頼関係とそれが招く危険性

SNS 上でのコミュニケーションでは、通信相手が友人またはその知人に限られているとの安心感があり、そのために、受け取ったメッセージを善意に基づくものと信じ、機微な情報についても大胆に表明するといったように、警戒感の水準を下げて行動する傾向がある。しかしながら、種々の要因により、SNS 上のコミュニティ内にも悪意を持った者が入り込んでいる可能性がある。

利用者が気心の知れた仲間ならばと考えて SNS で公開している情報も、悪意をもった部外者にとっては、普通では簡単に入手しがたい攻撃相手の周辺の人間関係を掌握できる

表 1: SNS で公開している情報が悪用される例

情報		情報の悪用（例）
基本プロフィール	氏名	標的型攻撃
	顔写真	誘拐、ストーキング
	住所	誘拐、空き巣、ストーキング
	生年月日	パスワードの推測
	電話番号	パスワードの推測
	メールアドレス	IDの推測、標的型攻撃
	勤務先	標的型攻撃
	出身校	同窓生を詐称
	家族構成	誘拐、空き巣、炎上
	交際	炎上、ストーキング
	趣味・関心	標的型攻撃
	友達	標的型攻撃
時系列で表示される情報		誘拐、空き巣、ストーキング、標的型攻撃
友達へ送信する情報		マルウエア・フィッシングのURL
利用者全員へ公開する情報		マルウエア・フィッシングのURL、炎上
アプリケーション		標的型攻撃
位置情報		誘拐、空き巣、ストーキング
お気に入り		マルウエア・フィッシングのURL

という意味で、ソーシャルエンジニアリング攻撃を仕掛けるための貴重な参考情報になり得る。例えば、基本プロフィールで公開している法人名や所属部署をもとに、攻撃者が法人情報や関係者情報を収集し、利用者プロフィールを公開している本人や同僚に成りすまして、ソーシャルエンジニアリングを仕掛ける恐れがある。また、公表されている生年月日や電話番号などの情報は、ログイン・パスワードを推測するヒントになり得、推測に成功すれば不正アクセスにつながる恐れがある。多くの SNS で公開されている情報のうち悪用される可能性が考えられるものを、それぞれの悪用のシナリオを添えて表 1 に掲げる。

悪意をもった者が、他人によって投稿された情報にアクセスして入手するだけの場合にも生ずるリスクについて上で述べたが、さらに、能動的に情報発信を行う場合について考えられる危険性について次に述べる。利用者は、SNS で送られてきたメッセージを無条件に信用する傾向がある。図 に示した「ソーシャルネットワークサービス利用に関するセキュリティ意識調査」では、面識のある友人・知人からのメッセージを「特に気にせずクリックする」と回答した人は、「同意する」・「やや同意する」を合わせると約

80%に達している。このため、SNS 上で友達や仕事関係者を騙る攻撃者からメッセージが届けば、利用者は特に注意することなくメッセージに書かれているリンク先にアクセスしたり、添付ファイルを開いたりすると考えられ、マルウエアに感染するリスクが著しく高いと言える。

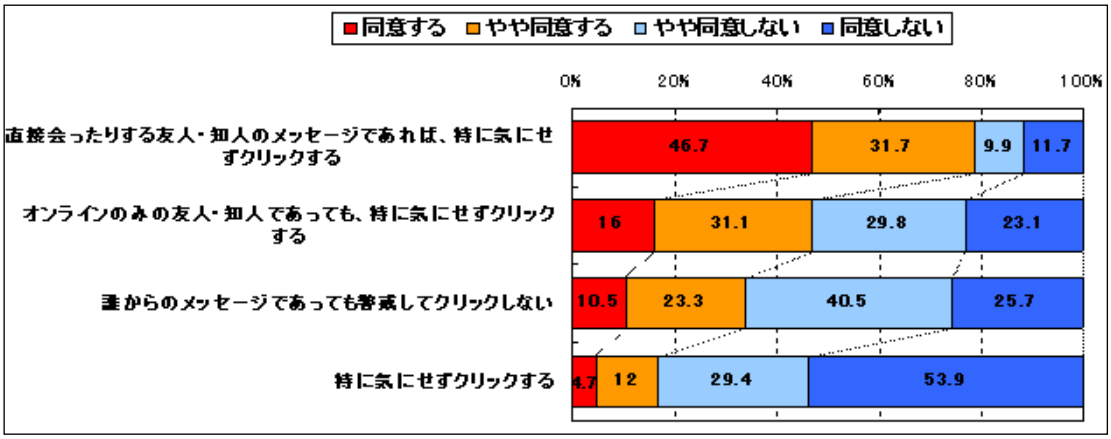

図 4: SNS 利用中のメッセージ内のリンクに対する意識

出典：「ソーシャルネットワークサービス利用に関するセキュリティ意識調査」[1]トレンドマイクロ

3.4. サービスの連携とそれが招く危険性

昨今の SNS で提供されるサービスは、様々な外部サービスと連携している。たとえば、GPS の位置情報をもとに現在地情報を提供する「foursquare」や、ランニングやサイクリングの記録を管理し、SNS 上で共有・提供できる「RunKeeper」などがある。このようなサービスは、単独でもサービスの提供が可能ではあるが、付加価値を高めるなどの目的で SNS と連携して実現されているものもあり、利用者の情報が SNS 提供事業者以外のサービス事業者に提供されている場合がある。

SNS の機能は年々進化し、かつ複数の事業者が提供している様々なサービスとの連携を始めている。攻撃者は、サービスが連携している点を悪用し、次に例示したような攻撃を仕掛けてくるかもしれない。

● チェックイン機能を悪用した攻撃例

Facebook のチェックイン機能「スポット」のような現在の位置情報を提供するサービスを使うことで、SNS 上にリアルタイムで位置情報を表示することができる。SNS 利用者

[1] http://jp.trendmicro.com/jp/about/news/pr/article/20110819013710.html

がこのようなサービスを利用していた場合、攻撃者は利用者の位置情報を SNS から把握し、現在地や行動パターン、更には仕事上の取引先などをも把握するかもしれない。

● **短縮 URL**

短縮 URL とは、URL の文字列を短く変換する機能[2]である。Twitter のような投稿文字数に制限があるサービスでは、文字列の長い URL を貼り付けると本文を書き込めなくなってしまうことがあるため、短縮 URL が利用される。

短縮 URL は、リンク先の Web サイトのドメインが表示されないため、悪用されやすく、短縮 URL から不正な Web サイトに誘導され、マルウエア感染やフィッシング攻撃を受ける可能性がある。シマンテック社が SNS 上の不正な Web サイトに繋がる URL を調査したところ、その 65%は短縮 URL であった。[3]

● **顔認識機能**

顔認識機能は、顔写真の画像データから人物を特定する機能で、すでにソフトウエア製品として市販されている。こういった顔認識機能は、昨今では、犯罪者やテロリストを逮捕する手段として捜査当局に採用されたり、一部の SNS においてサービスに組み込まれたりしている。また、法人において、顔情報がパスワード代わりのセキュリティトークンとして利用されている例もある。

> シマンテック社へ取材したところ、「最近は写真だけで誰かを特定するアプリケーションがある。それがあれば、街中にいる人物を撮影し、SNS を悪用し、個人情報を収集するというストーキングのような活動も可能になってしまう」と、将来的に顔写真が悪用される可能性もあるという。加えて、同社のブログでは、顔認識ソフトウエアを使った悪用事例も紹介されている。

カーネギーメロン大学の研究論文「Faces of Facebook: Privacy in the Age of Augmented Reality」によると、安価なハードウエア（35 ドルの Web カメラとスマートフォン）を使用するだけで、出会い系サイトに登録されている利用者の身元を特定したり、カーネギーメロン大学のキャンパスを歩く人々を SNS 上で特定したりすることができた。また、市販の顔認識ソフトウエアを使用して、ある人の社会保障番号を割り出すことさえ

---

2 http://en.wikipedia.org/wiki/URL_shortening

3 出典：「シマンテックインターネットセキュリティ脅威レポート - 2010 年版 2011 年 4 月発行」シマンテック http://www.symantec.com/content/ja/jp/enterprise/white_papers/istr16_wp_201104.pdf

できた。この研究は、今後大きなプライバシーの問題が生じる可能性を示唆している。

4. 法人が留意すべき SNS によるリスク

本章では、先に述べた SNS の利用が招く可能性のある危険性を踏まえて、法人が留意すべきリスクを、事例を紹介しつつ、整理する。

4.1 すべての法人が留意すべき SNS によるリスク

本節では、組織として積極的に SNS を活用しているか否かにかかわらず、すべての法人に生じ得る、SNS の利用に由来するリスクについて述べる。

(1) SNS における従業員の言動によって引き起こされるトラブル

SNS 利用者は、公の場での発言であるとの認識なしに、仲間内の井戸端会議のつもりで SNS へメッセージを投稿していることが多い。しかしながら、前章で述べたような原因で、投稿者が想定していた以上に広範囲の読者の目に触れることになるケースがある。また、投稿に際してメッセージに含まれる人や組織を匿名化したつもりであっても、プロファイルや他の利用者を含む他の投稿と情報を重ね合わせることにより、メッセージ中で言及された人や組織が特定できるケースも考えられる。

したがって、法人の従業員(アルバイト職員なども含む。)が無邪気に投稿したメッセージが、思わぬ読者の注意を惹き、メッセージ中で言及された雇用主である法人が非難の標的になったり、法人の顧客や取引先のプライバシーや秘密事項が曝されたりする事態にもなりかねない。SNS のようなネットワーク・メディアでは、非難が爆発的に広まる「炎上」と呼ばれる状況に到るケースも時々見られるし、ネットワーク上に流布してしまったプライバシーや秘密事項等に関する情報は消去し難い状態で存在し続けることになる。

法人は、従業員の個人的な SNS 利用から、ブランドの毀損や風評被害といったリスクを被る可能性があると考えられる。以下に実際に起きた例を挙げる。

● 法人ブランドの広告塔に従業員が SNS の投稿で泥を塗る

ある大手スポーツ用品メーカーが，ある著名なプロスポーツ選手と広告契約を結んでいた。そのメーカーの直営店に勤務する一人の社員が、その選手が妻とともに来店したのを見かけ、その様子を夫妻の容姿についての侮辱を込めて Twitter に投稿した。この社員は、それまでも不適切な内容の投稿を行っていた模様であるが、この Twitter 投稿をきっかけに、インターネット掲示板において、いわゆる「炎上」が発生した。さらに、同社

社員は、Twitter とは別の SNS 上で自身のプロフィールを公表していたため、氏名・顔写真・出身校・所属法人・交際相手のプロフィールなどが容易に特定され、さらには勤務先の法人も特定されて、社会常識の欠けた従業員の行動を放置していると言った多数の非難の声が法人にも届くようになった。

ブランドのシンボルとも言うべき広告契約選手を自社の従業員がこきおろし、名誉を棄損していたことが公になり、さらにそれを放置していたとの非難の声が巻き起こり拡大する事態に、当該法人は、自社従業員が契約選手の情報を流出させたことを認め、再発防止を徹底する旨の「お詫びとご報告」を法人ホームページに掲載し、謝罪せざるを得なくなった。

● 従業員の私的な投稿に端を発する騒ぎで所属法人までが謝罪

架空の設定ではあったが、あるインターネット関連法人の社員が、被面接者に対する侮辱的な内容を含んだ採用面接の模様を Google+に投稿した。読者は、これを作り話とは受け取らず、不届きな投稿だとして、インターネット掲示板などで「炎上」するところまで騒ぎが拡大した。実名で Google+を利用していたため、ネットワーク内だけでなく、実社会でも非難を浴びることになり、さらには、所属している法人までが批判される事態に到った。

この事態を収拾するため、当該法人は「書き込まれた面接の実況中継は架空のもの」との声明を出した上で謝罪し、さらに翌日には、経緯と原因、対応策、再発防止策を公表した。

(2) 標的型攻撃

昨今では、多くの法人が、情報窃取あるいは遠隔操作用の機能を備えたマルウエアを用いた、標的型のサイバー攻撃を多かれ少なかれ受けているとされている。この種の攻撃では多くの場合、巧妙な標的型メールを従業員や役員に送り付けて、添付したファイルを開かせることによって、マルウエアに感染させて、その後の執拗な攻撃の橋頭保が作られる。攻撃者が、SNS 上で知り得た知人の名前を装ったり、SNS を用いてメッセージを送ったりすれば、標的にされた人は知人からのものと誤認して安易に添付ファイルを開く確率が高くなるのだ。

メールの受信者が受け取った時に怪しいものと疑わないような巧妙な内容のメールを作るには、法人の組織構造や指揮系統(上司－部下の関係)、組織内事情にある程度通じている必要がある。かつては、こうした情報を組織外の人間が収集することは、容易でなかった。ところが、SNS が広く利用されるようになった今日では、所属組織、経歴、

誕生日、友人・知人関係、趣味・趣向などを容易に入手し、SNS 上の投稿を注意深く収集して追うことにより組織内情報さえしばしば垣間見ることができることができるようになっているのである。

一部の SNS では、プロファイルの中で利用者名だけでなく所属組織や所属部門についても実名で登録することになっている。交換されるメッセージからは、組織内の人間関係や関心事をうかがい知ることができる。こうした情報をもとに標的型攻撃のシナリオが作成されていると考えられる。以下に実際に起きた例を紹介する。

S1：EMC 社 RSA 事業本部に対する標的型攻撃

2011 年 3 月に EMC 社の RSA 事業本部が標的型攻撃の被害を受け、RSA 製品の SecurID[4] の情報が漏えいする事件があった。この事件に係る一連の攻撃の流れを、アンラボ社が図 に示したようにまとめている。

1) 2日間隔で「2011 Recruitment Plan」というタイトルメールをそれぞれ別のチームに所属する職員に送信。ターゲットの職員の個人情報は、ソーシャルネットワークサービスを利用して収集。
2) メールには「2011 Recruitment plan.xls」という添付ファイルが存在。このファイルは、3月 15日に公開された Adobe Flash Player のゼロデイ (Zero Day) 脆弱性 (CVE-2011-0609) を悪用した SWF ファイルが存在。
3) 脆弱性を悪用して Poison Ivy (リモートコントロールタイプのトロイの木馬) マルウェア感染
4) 感染したシステムを悪用して内部ネットワークにアクセスし、目標のシステムの管理者権限への権限上昇。
5) 目標のシステムのデータを別のシステムにコピーし、圧縮および暗号化。
6) 圧縮および暗号化したデータを再び RAR でパスワードをかけて圧縮し、FTP を利用して外部に存在するハッキングされた第 3 のシステムに転送。

図 5: RSA が受けた標的型攻撃の一連の流れ

出典：「ASEC Report 2011 年 4 月号」アンラボ

また、F-Secure 社によれば、この事件では図 のような標的型メール「2011 Recruitment plan」が使われた。このメールに添付されている、図 に掲げたファイル 「2011 Recruitment plan.xls」 を受信者が開き、そのマシンに Adobe Flash Player の脆弱性（CVE-2011-0609）が存在した場合には、Poison Ivy(遠隔操作用のトロイの木馬)マルウエアに感染する。攻撃がなされた当時は、当該脆弱性に対するパッチがない、いわゆるゼロディ(Zero Day)攻撃であった。このマルウエアに感染したマシンには、「バックドア」といわれる攻撃者が侵入するための裏口が設けられ、いつでも不正に侵入できるようになる。

[4] http://japan.rsa.com/node.aspx?id=1156

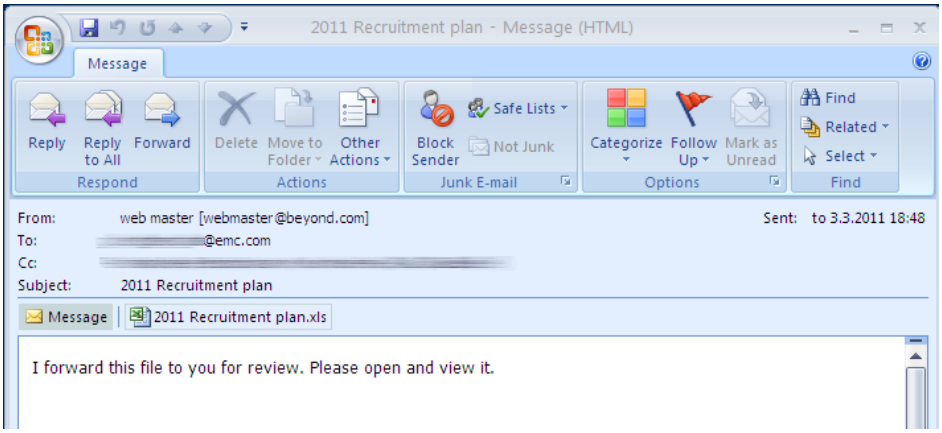

図 6: 標的型メール

出典：「How We Found the File That Was Used to Hack RSA」F-Secure 社

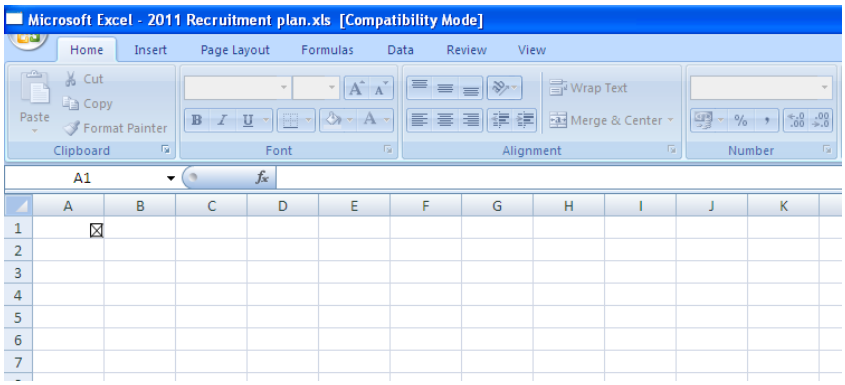

図 7: 標的型メールの添付ファイル

出典：「How We Found the File That Was Used to Hack RSA」F-Secure 社

アンラボ社によれば、この事例で攻撃者は、RSA 事業本部に勤める従業員を SNS で探し出し、その従業員に上述のような標的型メールを送り添付ファイルを開かせることに成功した。SNS から収集した情報を駆使したソーシャルエンジニアリング攻撃だったのである。

また、今回のインタビュー調査において、次のように指摘したセキュリティベンダもあった。

LinkedIn を用いて大まかな企業内の組織図もしくは人物をもとに同業種内の相関図を作成されてしまう可能性がある

(3) 第三者による法人を騙った SNS を用いた情報発信

SNS のアカウントは、特別な本人確認や身元確認をすることなく、求めに応じて発行されることが一般的なので、第三者が勝手に法人ないし法人の関係者を名乗って SNS 上で情報を発信することがありうる。その中には、悪意のないケースや単なる SNS 上での仮名として名前を使っているケースもあるが、悪意をもってなされた場合には、知らないうちに法人に対する不本意な評判が SNS 内に作り出されかねないリスクがある。特に、SNS 利用者が多い人口層を主な顧客としている企業にとっては、法人としての IT リテラシーを疑われることになりかねない。そうした事例を次に紹介する。

● 関係者を騙った不適切な投稿

大手法人 A 社の取締役を騙り、障害者を誹謗する非社会的な発言や虚偽の発言を繰り返している者がいた。A 社はそれに気づいていなかったが、そのうちに他社の経営者を揶揄する Tweet が投稿されたことを契機に、いわゆるネット上での「炎上」が発生して、A 社も事態に気づいて調査した結果、それまで多数の投稿が A 社に成りすました第三者によってなされていたことが判明した。

騙られた A 社は、その後に取得した正規アカウントを用いて、一連の Tweet が A 社および A 社の取締役とは無関係であるとの声明を発して事態の収拾を図った。

4.2 SNS を活用する法人が留意すべきリスク

組織として積極的に SNS を活用しようとしている法人が留意すべきセキュリティ・リスクとしては、公式の SNS 法人アカウントの管理が不十分であったために、正規のアカウントが第三者に不正に利用される可能性が挙げられる。第三者に勝手に不適切な内容の投稿をされた場合、投稿内容によっては、ブランドの毀損や風評被害の発生も考えられる。実際に起きた例を次に挙げる。

● 第三者によるアカウント窃取の実例

熊本県のゆるキャラ「くまモン」の Twitter アカウントが乗っ取られ、フォロワーのアカウントを「くまモン」がブロックするという事態が発生した。「くまモン」オフィシャル

ページによると、正規 Twitter アカウントに対して悪意の第三者がログインしていることが発覚。熊本県庁では、新たに「くまモン」のアカウントを作成し、旧アカウントのフォロワーを新アカウントへ移行してもらうよう呼びかける対応を行った。

5. 法人がとるべき対策

5.1 すべての法人がとるべき対策

本節では、すべての法人において検討すべき対策を述べる。

(1) 従業員の言動によって引き起こされるリスクへの対策

インタビュー調査において、あるセキュリティベンダは、SNS を利用もしくは SNS に係わらざるを得ない法人は SNS にどう接するべきかについて次のように述べている。

> インタビューより
>
> Q：SNS を利用する法人は何に気を付ければ良いか？
>
> A：部署によっては PR 部署等、IT に詳しくない担当がうっかりやってしまうという事があり、気を付けなければならない。その意味で、SNS 利用について社内ガイドラインを定める事も必要である。(シマンテック社)
>
> A: ソーシャルメディアポリシー/ガイドラインを策定し、従業者の意識を高める努力。
>
> 一律で SNS サイトをブロックする、業務時間帯のみブロックする（昼休み時間帯などは許可する）などの「社内から SNS を触らせない」対策はもはや限界にきていると思われる。新しいメディアを積極的に取り入れることのメリットを尊重することで、企業のブランディング、組織に対する帰属意識向上につながる可能性があると思われます。(某セキュリティ会社)
>
> A: 社内でのソーシャルメディアポリシーの策定が必要である。(マカフィー社)

すなわち、法人として SNS の活用を考えていない場合にも、法人の従業員による SNS の利用に鑑み、従業員向けに SNS 利用に伴うリスクを教え、SNS の利用に関するガイドラインを策定することが推奨される。

SNS の利用に関するガイドラインで規定すべき内容について一例を示す。

- 利用する目的・範囲の明確化
  SNS の利用目的を、新製品やキャンペーン情報などの発信、お客様からの問い合わせへの返信など業務目的に限定し、目的以外での情報発信をしないように規定する。

- 利用部門
  業務で SNS を利用できる部門（広報、商品企画、カスタマーサポートなど）を限定し、情報を管理する。

- フォロワーの管理
  法人の公式アカウントをフォローしているフォロワーからのコメントに十分な注意を払い、必要に応じて適切な対応を行えるように、対応方針、担当窓口を明確化する。

- 禁止事項の明確化
  社内の機密情報、他者の誹謗中傷、違法行為または公序良俗に反する行為等の禁止事項を明確にする。

- 投稿内容のチェック体制
  SNS に投稿する情報は、あらかじめ社内のレビューを受け、前項の禁止事項が含まれないかなどの確認を行った上で、投稿するようにする。

- 炎上時の対応方針
  炎上が生じた場合に備えて、あらかじめ対応の方針を策定しておく。

次に国内企業にて実際に運用されているガイドラインを例示する。

(参考)　国内企業の SNS ガイドライン　　五十音順

インテル株式会社
インテル・ソーシャルメディア・ガイドライン
http://www.intel.co.jp/content/www/jp/ja/legal/intel-social-media-guidelines.html

日本アイ・ビー・エム株式会社
IBM　ソーシャル・コンピューティングのガイドライン
http://www-06.ibm.com/ibm/jp/about/partner/scg.html

日本コカ・コーラ株式会社
コカ・コーラシステム　ソーシャルメディアの利用に関する行動指針
http://www.cocacola.co.jp/info/social_guide01.html

日本電気株式会社
NEC グループ　ソーシャルメディアポリシー
http://jpn.nec.com/site/ja/socialpolicy.html

(2) 標的型攻撃などの想定外な事態に対する対策

SNS に登録されている情報は単独で、あるいは、インターネット上で公開されている情報と組み合わされることで、標的型攻撃に利用されることも考えられる。SNS のようなネットワーク・メディアの普及は、それ以前の時代には外部からうかがい知ることの難しかった組織内の状況を垣間見ることができるようになっていることを意味し、そうした状況に置かれていること理解して、法人は標的型攻撃に備えておく必要がある。
また、標的型攻撃を水際で完全に遮断することは事実上不可能であるとの認識を持ち、標的型攻撃に遭遇することを想定して、CSIRT(Computer Security Incident Response Team)などのセキュリティ事象に対処するための組織体制を構築することも法人にできる重要な対策であると言える。

5.2 SNS を活用している法人がとるべき対策

(1) 公式アカウントの不十分な管理から生じるリスクへの対策

第 4 章で紹介した事例でも見られたように、法人の SNS アカウントを使って不適切な内容の投稿が行われれば、一気にその法人の信用の失墜やブランド価値の毀損につながる。法人は、公開している SNS のアカウントを適切に管理することで、そうしたリスクの低減に努める必要がある。次に管理項目の一例を示す。

- SNS アカウントのパスワードとして強固なものを選ぶ。

- SNS アカウントの ID・パスワードの共有範囲を最小限に抑えることによりパスワード拡散を防ぐ。
- 法人用アカウントで SNS にアクセスするためのマシンに基本的なセキュリティ対策を実施し、マルウエア感染によって起きる情報窃取を防ぐ。
- SNS アカウントからメッセージを発する担当者、時間帯、発する対象時事などの制限を決め投稿状態を管理する。
- 複数の SNS アカウントを運用している場合は、全てのアカウントを一元管理するのか、SNS アカウントを運用しているサービスや事業部ごとに管理するのか規定を策定する。

また、正規な法人の SNS アカウントを、法人の公開ウェブサイトで明示しておくことは、悪意ある第三者にて作成された法人に類似した SNS アカウントへ利用者を導かせないための対策ともなる。

6. まとめ

日本における SNS の利用者数は 2010 年以降急増しており、2012 年には延べ 5000 万人に達し、現在も増加の一途をたどっている。法人の従業員においても相当数が SNS を個人利用していると考えるべきであろう。また、SNS の利用者数の増加に伴い、法人も SNS を広報活動のメディアとして利用し始めた。このような SNS の普及や利用の拡大傾向に伴い、従業員による不適切な言動に起因したいわゆる「炎上」や、第三者による成りすまし行為に起因するブランド毀損も発生している。さらには、法人に対する標的型攻撃のための情報収集源として SNS が利用されることもある。

SNS の利用に起因するリスクを法人が軽減するには、SNS の利用に関するガイドラインを策定し、広報担当者を含む従業員一人一人に周知徹底させる必要がある。加えて、公式アカウントの管理や想定外の事態に対する法人内の対応体制なども必要である。

ガイドラインを策定する際の参考情報として本資料が一助となる事を願う。

謝辞

本レポートの作成にあたり、インタビューにご協力頂きました SNS 提供事業者のグリー株式会社など他数社、自治体、セキュリティベンダの株式会社カスペルスキー、株式会社シマンテック、トレンドマイクロ株式会社、マカフィー株式会社の皆様に感謝いたします。